Lenovo

Lenovo XClarity Management Hub
คู่มือการติดตั้งและคู่มือผู้ใช้

เวอร์ชัน 2.1

หมายเหตุ

ก่อนที่จะใช้ข้อมูลนี้และผลิตภัณฑ์ที่รองรับ โปรดอ่าน คำประกาศทั่วไปและคำประกาศทางกฎหมายในเอกสารแบบออนไลน์ของ XClarity Orchestrator

ตีพิมพ์ครั้งที่สอง (กรกฎาคม 2024)

สารบัญ

บทที่ 1. การวางแผนสำหรับ Lenovo XClarity Management Hub

ตรวจสอบข้อควรพิจารณาและข้อกำหนดเบื้องต้นต่อไปนี้ เพื่อช่วยคุณวางแผนสำหรับการติดตั้งของ Lenovo XClarity Management Hub

ฮาร์ดแวร์และซอฟต์แวร์ที่รองรับ

ตรวจสอบให้แน่ใจว่าสภาพแวดล้อมของคุณตรงกับข้อกำหนดของฮาร์ดแวร์และซอฟต์แวร์สำหรับ Lenovo XClarity Management Hub

ระบบโฮสต์

ข้อกำหนดสำหรับไฮเปอร์ไวเซอร์

รองรับไฮเปอร์ไวเซอร์ต่อไปนี้สำหรับการติดตั้ง Lenovo XClarity Management Hub

- VMware ESXi 7.0, U1, U2 และ U3
- VMware ESXi 6.7, U1, U2[1] และ U3

สำหรับ VMware ESXi, อุปกรณ์เสมือนคือเทมเพลต OVF

ข้อสำคัญ:

- สำหรับ VMware ESXi 6.7 U2 คุณต้องใช้อิมเมจ ISO ของ VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso หรือใหม่กว่า

ข้อกำหนดด้านฮาร์ดแวร์

ตารางต่อไปนี้แสดงรายการการกำหนดค่า *ขั้นต่ำที่แนะนำ* สำหรับ XClarity Management Hub ตามจำนวนของอุปกรณ์ Edge-Client ที่มีการจัดการ อาจต้องมีทรัพยากรเพิ่มเติมเพื่อให้ได้รับประสิทธิภาพสูงสุด ทั้งนี้ขึ้นอยู่กับสภาพแวดล้อมของคุณ

จำนวนอุปกรณ์ Edge-Client ที่มีการจัดการ	**โปรเซสเซอร์**	**หน่วยความจำ**	**ที่จัดเก็บ**
0 - 100 อุปกรณ์	6	32 GB	340 GB
100 - 200 อุปกรณ์	8	34 GB	340 GB

จำนวนอุปกรณ์ Edge-Client ที่มีการจัดการ	โปรเซสเซอร์	หน่วยความจำ	ที่จัดเก็บ
200 - 400 อุปกรณ์	10	36 GB	340 GB
400 - 600 อุปกรณ์	12	40 GB	340 GB
600 - 800 อุปกรณ์	14	44 GB	340 GB
800 - 1,000 อุปกรณ์	16	48 GB	340 GB

1. นี่คือปริมาณที่จัดเก็บขั้นต่ำสำหรับใช้งานโดยอุปกรณ์เสมือน XClarity Management Hub เช่น ที่เก็บข้อมูล SSD

ข้อกำหนดด้านซอฟต์แวร์

ต้องใช้ซอฟต์แวร์ต่อไปนี้สำหรับ XClarity Management Hub

- **เซิร์ฟเวอร์ NTP** ต้องใช้เซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย (NTP) เพื่อตรวจสอบให้แน่ใจว่าการประทับเวลาสำหรับเหตุการณ์และการแจ้งเตือนทั้งหมดที่ได้รับจากตัวจัดการทรัพยากรและอุปกรณ์ที่ได้รับการจัดการถูกซิงโครไนซ์กับ XClarity Management Hub ตรวจสอบให้แน่ใจว่าสามารถเข้าถึงเซิร์ฟเวอร์ NTP ได้บนเครือข่ายการจัดการ (ปกติบนอินเทอร์เฟซ Eth0)

อุปกรณ์ที่สามารถจัดการได้

XClarity Management Hub สามารถจัดการ ตรวจสอบ และเตรียมใช้งานอุปกรณ์ ThinkEdge Client สูงสุด 10,000 เครื่อง (โดยไม่มี Baseboard Management Controller)

คุณสามารถค้นหารายการอุปกรณ์ ThinkEdge Client และตัวเลือกที่รองรับทั้งหมด (เช่น I/O, DIMM และอะแดปเตอร์จัดเก็บข้อมูล) ระดับเฟิร์มแวร์ขั้นต่ำที่จำเป็น และข้อควรพิจารณาเกี่ยวกับข้อจำกัดได้จาก เซิร์ฟเวอร์ XClarity Management Hub

สำหรับข้อมูลทั่วไปเกี่ยวกับการกำหนดค่าและตัวเลือกฮาร์ดแวร์สำหรับอุปกรณ์ที่ระบุ โปรดดู เว็บเพจ Lenovo Server Proven

เว็บเบราเซอร์

เว็บอินเทอร์เฟซ XClarity Management Hub จะทำงานกับเว็บเบราเซอร์ต่อไปนี้

- Chrome 80.0 ขึ้นไป
- Firefox ESR 68.6.0 ขึ้นไป
- Microsoft Edge 40.0 ขึ้นไป

- Safari 13.0.4 ขึ้นไป (ทำงานบน macOS 10.13 ขึ้นไป)

ไฟร์วอลและเซิร์ฟเวอร์พร็อกซี

การบริการและการสนับสนุนบางฟังก์ชัน รวมถึง Call Home และสถานะการรับประกัน จำเป็นต้องมีการเข้าถึงอินเทอร์เน็ต หากคุณมีไฟร์วอลล์ในเครือข่าย ให้กำหนดค่าไฟร์วอลล์เพื่อเปิดใช้งาน XClarity Orchestrator และตัวจัดการทรัพยากรให้ดำเนินการเหล่านี้ หาก Lenovo XClarity Orchestrator และตัวจัดการทรัพยากรไม่มีสิทธิ์เข้าถึงอินเทอร์เน็ตได้โดยตรง ให้กำหนดค่าเพื่อให้ใช้เซิร์ฟเวอร์พร็อกซี

ไฟร์วอลล์

ตรวจสอบว่าชื่อ DNS และพอร์ตต่อไปนี้เปิดอยู่บนไฟร์วอลล์สำหรับ XClarity Orchestrator และตัวจัดการทรัพยากรที่เกี่ยวข้อง (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub และ Lenovo XClarity Administrator) หากมี แต่ละ DNS จะแสดงแทนระบบที่กระจายตามทางภูมิศาสตร์ด้วยที่อยู่ IP แบบไดนามิก

หมายเหตุ: ที่อยู่ IP อาจมีการเปลี่ยนแปลง ใช้ชื่อ DNS หากเป็นไปได้

ชื่อ DNS	**พอร์ต**	**โปรโตคอล**
ดาวน์โหลดอัปเดตต่างๆ (เซิร์ฟเวอร์การจัดการ อัปเดตเฟิร์มแวร์ UpdateXpress System Packs (ไดรเวอร์อุปกรณ์ของ OS) และแพคที่เก็บข้อมูล)		
download.lenovo.com	443	https
support.lenovo.com	443 และ 80	https และ http
ส่งข้อมูลบริการไปยังฝ่ายสนับสนุนของ Lenovo (Call Home) – XClarity Orchestrator เท่านั้น		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 และใหม่กว่า) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 และก่อนหน้า)	443	https
ส่งข้อมูลเป็นครั้งคราวไปให้ Lenovo – XClarity Orchestrator เท่านั้น		

ชื่อ DNS	พอร์ต	โปรโตคอล
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 และใหม่กว่า) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 และก่อนหน้า)	443	https
รับข้อมูลการรับประกัน		
supportapi.lenovo.com	443	https และ http

เซิร์ฟเวอร์พร็อกซี

หาก XClarity Orchestrator หรือตัวจัดการทรัพยากรไม่มีสิทธิ์เข้าถึงอินเทอร์เน็ตได้โดยตรง ให้ตรวจสอบว่ามีการกำหนดค่าให้ใช้เซิร์ฟเวอร์พร็อกซี HTTP (ดู การกำหนดค่าเครือข่ายใน XClarity Orchestrator เอกสารแบบออนไลน์)

- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีให้ใช้การการตรวจสอบความถูกต้องพื้นฐาน
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีที่ไม่สิ้นสุด
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีส่งต่อ
- ตรวจสอบให้แน่ใจว่ามีการกำหนดค่าให้โหลดบาลานเซอร์เก็บเซสชันไว้กับเซิร์ฟเวอร์พร็อกซีหนึ่งตัว และไม่มีการสลับไปมา

ข้อควรพิจารณา: XClarity Management Hub ต้องมีการเข้าถึงอินเทอร์เน็ตโดยตรง ในขณะนี้ยังไม่มีการรองรับพร็อกซีเซิร์ฟเวอร์ HTTP

ความพร้อมใช้งานของพอร์ต

Lenovo XClarity Orchestrator และตัวจัดการทรัพยากรกำหนดให้ต้องเปิดพอร์ตบางพอร์ตเพื่ออำนวยความสะดวกในการสื่อสาร หากพอร์ตที่จำเป็นถูกบล็อกหรือกระบวนการอื่นใช้พอร์ตนั้นอยู่ ฟังก์ชันบางอย่างอาจทำงานไม่ถูกต้อง

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub และ Lenovo XClarity Administrator เป็นแอปพลิเคชัน RESTful ที่สื่อสารอย่างปลอดภัยผ่าน TCP บนพอร์ต 443

XClarity Orchestrator

XClarity Orchestrator จะรับข้อมูลและตอบสนองผ่านพอร์ตที่แสดงในตารางต่อไปนี้ หาก XClarity Orchestrator และทรัพยากรที่มีการจัดการทั้งหมดอยู่หลังไฟร์วอลล์ และคุณต้องการเข้าถึงทรัพยากรเหล่านั้นจากเบราเซอร์ที่อยู่*นอก*ไฟร์วอลล์ คุณต้องตรวจสอบว่าพอร์ตที่จำเป็นเปิดอยู่

หมายเหตุ: XClarity Orchestrator สามารถเลือกที่จะได้รับการกำหนดค่าเพื่อทำการเชื่อมต่อขาออกกับบริการภายนอกได้ เช่น LDAP, SMTP หรือ syslog การเชื่อมต่อเหล่านี้อาจต้องการพอร์ตเพิ่มเติมที่มักจะกำหนดค่าโดยผู้ใช้ได้และไม่ได้รวมอยู่ในรายการนี้ นอกจากนี้การเชื่อมต่อเหล่านี้ยังอาจต้องการการเข้าถึงเซิร์ฟเวอร์บริการชื่อโดเมน (DNS) บน TCP หรือ UDP พอร์ต 53 เพื่อแก้ไขปัญหาเรื่องชื่อเซิร์ฟเวอร์ภายนอก

Service	**ขาออก (พอร์ตเปิดบนระบบภายนอก)**	**ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Orchestrator)**
อุปกรณ์ XClarity Orchestrator	• DNS – TCP/UDP บนพอร์ต **53**	• HTTPS – TCP บนพอร์ต **443**
เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายนอก	• LDAP– TCP บนพอร์ต **389**[1]	ไม่สามารถใช้ได้
บริการส่งต่อเหตุการณ์	• เซิร์ฟเวอร์อีเมล (SMTP) – UDP บนพอร์ต **25**[1] • บริการเว็บ REST (HTTP) – UPD บนพอร์ต **80**[1] • Splunk – UDP บนพอร์ต **8088**[11], **8089**[1] • Syslog – UDP บนพอร์ต **514**[1]	ไม่สามารถใช้ได้
Lenovo Services (รวมถึง Call Home)	• HTTPS (Call Home) – TCP บนพอร์ต **443**	ไม่สามารถใช้ได้

1. นี่คือพอร์ตเริ่มต้น คุณสามารถกำหนดค่าพอร์ตนี้ได้จากอินเทอร์เฟซผู้ใช้ XClarity Orchestrator

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 ต้องเปิดพอร์ตบางพอร์ตเพื่ออำนวยความสะดวกในการสื่อสาร หากพอร์ตที่จำเป็นถูกบล็อกหรือกระบวนการอื่นใช้พอร์ตนั้นอยู่ ฟังก์ชันฮับการจัดการบางอย่างอาจทำงานไม่ถูกต้อง

หากอุปกรณ์อยู่หลังไฟร์วอลล์ และหากคุณต้องการจัดการอุปกรณ์เหล่านั้นจากฮับการจัดการที่อยู่นอกไฟร์วอลล์ดังกล่าว คุณต้องตรวจสอบว่าพอร์ตทั้งหมดที่เกี่ยวข้องกับการสื่อสารระหว่างฮับการจัดการและ Baseboard Management Controller ในอุปกรณ์แต่ละเครื่องเปิดอยู่

การบริการหรือส่วนประกอบ	ขาออก (พอร์ตเปิดไปยังระบบภายนอก)	ขาเข้า (พอร์ตเปิดอยู่บนอุปกรณ์เป้าหมาย)
XClarity Management Hub 2.0	• DNS - UDP บนพอร์ต 53 • NTP - UDP บนพอร์ต 123 • HTTPS - TCP บนพอร์ต 443 • SSDP - UDP บนพอร์ต 1900 • DHCP - UDP บนพอร์ต 67	• HTTPS - TCP บนพอร์ต 443 • SSDP - UDP บนพอร์ต 32768-65535
เซิร์ฟเวอร์ ThinkSystem และ ThinkAgile	• HTTPS – TCP บนพอร์ต 443 • การค้นหา SSDP – UDP บนพอร์ต 1900	• HTTPS – TCP บนพอร์ต 443

XClarity Management Hub

XClarity Management Hub จะรับข้อมูลและตอบสนองผ่านพอร์ตที่แสดงในตารางต่อไปนี้

การบริการหรือส่วนประกอบ	ขาออก (พอร์ตเปิดบนระบบภายนอก)	ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Management Hub)
อุปกรณ์ XClarity Management Hub[1]	• DNS – TCP/UDP บนพอร์ต 53[2]	• HTTPS – TCP บนพอร์ต 443 • MQTT – TCP บนพอร์ต 8883
อุปกรณ์ ThinkEdge Client[3]	ไม่สามารถใช้ได้	• MQTT – TCP บนพอร์ต 8883

1. เมื่อใช้ XClarity Management Hub ในการจัดการอุปกรณ์ผ่าน XClarity Orchestrator พอร์ตบางตัวจะต้องเปิดเพื่ออำนวยความสะดวกในการสื่อสาร หากพอร์ตที่ต้องการถูกบล็อกหรือกระบวนการอื่นใช้พอร์ตนั้นอยู่ ฟังก์ชัน XClarity Orchestrator บางอย่างอาจทำงานไม่ถูกต้อง
2. XClarity Management Hub สามารถเลือกที่จะได้รับการกำหนดค่าเพื่อทำการเชื่อมต่อขาออกกับบริการภายนอกได้ นอกจากนี้การเชื่อมต่อเหล่านี้ยังอาจต้องการการเข้าถึงเซิร์ฟเวอร์บริการชื่อโดเมน (DNS) บน TCP หรือ UDP พอร์ต 53 เพื่อแก้ไขปัญหาเรื่องชื่อเซิร์ฟเวอร์ภายนอก
3. หากอุปกรณ์ที่สามารถจัดการได้อยู่หลังไฟร์วอลล์ และหากคุณต้องการจัดการอุปกรณ์เหล่านั้นจาก XClarity Management Hub ที่อยู่นอกไฟร์วอลล์ คุณต้องตรวจสอบว่าพอร์ตทั้งหมดที่เกี่ยวข้องกับการสื่อสารระหว่าง XClarity Management Hub และอุปกรณ์ Edge เปิดอยู่

XClarity Administrator

เมื่อใช้ Lenovo XClarity Administrator ในการจัดการอุปกรณ์ผ่าน Lenovo XClarity Orchestrator พอร์ตบางตัวจะต้องเปิดเพื่ออำนวยความสะดวกในการสื่อสาร หากพอร์ตที่ต้องการถูกบล็อกหรือกระบวนการอื่นใช้พอร์ตนั้นอยู่ ฟังก์ชัน XClarity Orchestrator บางอย่างอาจทำงานไม่ถูกต้อง

สำหรับข้อมูลเกี่ยวกับพอร์ตต่างๆ ที่ต้องเปิดสำหรับ XClarity Administrator โปรดดู ความพร้อมใช้งานของพอร์ต ใน XClarity Administrator เอกสารแบบออนไลน์

ข้อควรพิจารณาเกี่ยวกับเครือข่าย

คุณสามารถกำหนดค่า Lenovo XClarity Management Hub ให้ใช้อินเทอร์เฟซเครือข่ายเดี่ยว (eth0) หรืออินเทอร์เฟซเครือข่ายที่แยกต่างหากสองตัว (eth0 และ eth1) สำหรับการสื่อสารได้

Lenovo XClarity Management Hub สื่อสารผ่านเครือข่ายต่อไปนี้

- *เครือข่ายการจัดการ* จะใช้เพื่อการสื่อสารระหว่าง Lenovo XClarity Management Hub กับอุปกรณ์ที่มีการจัดการ
- *เครือข่ายข้อมูล* จะใช้สำหรับการสื่อสารระหว่างระบบปฏิบัติการที่ติดตั้งบนเซิร์ฟเวอร์และอินทราเน็ตของบริษัท อินเทอร์เน็ต หรือทั้งคู่

อินเทอร์เฟซเดี่ยว (eth0)

เมื่อใช้อินเทอร์เฟซเครือข่ายเดี่ยว (eth0) การสื่อสารด้านการจัดการ การสื่อสารด้านข้อมูล และการปรับใช้ระบบปฏิบัติการจะเกิดขึ้นผ่านเครือข่ายเดียวกัน

เมื่อคุณตั้งค่า Lenovo XClarity Management Hub ให้กำหนดอินเทอร์เฟซเครือข่าย eth0 โดยคำนึงถึงเงื่อนไขต่อไปนี้

- ต้องกำหนดค่าอินเทอร์เฟซเครือข่ายเพื่อรองรับการค้นพบและการจัดการอุปกรณ์ (รวมถึงการอัปเดตเฟิร์มแวร์) Lenovo XClarity Management Hub ต้องสามารถสื่อสารกับอุปกรณ์ทั้งหมดที่จะจัดการจากเครือข่ายการจัดการ Lenovo XClarity Management Hub ต้องสามารถสื่อสารกับอุปกรณ์ทั้งหมดที่จะจัดการจากเครือข่าย
- หากต้องการปรับใช้อิมเมจ OS อินเทอร์เฟซ eth0 ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเซิร์ฟเวอร์เครือข่ายที่ใช้เพื่อเข้าถึงระบบปฏิบัติการโฮสต์
- **สิ่งสำคัญ**: การใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่ใช้งานร่วมกันอาจทำให้เกิดการหยุดชะงักในการรับส่งข้อมูล เช่น แพ็คเก็ตที่ถูกยกเลิก หรือปัญหาการเชื่อมต่อเครือข่ายการจัดการ โดยขึ้นอยู่กับการกำหนดค่าเครือข่ายของคุณ (ตัวอย่างเช่น หากการรับส่งข้อมูลจากเซิร์ฟเวอร์มีลำดับความสำคัญสูงและการรับส่งข้อมูลจากตัวควบคุมการจัดการมีลำดับความสำคัญต่ำ) เครือข่ายการจัดการใช้การรับส่งข้อมูล UDP ใน TCP เพิ่มเติม การรับส่งข้อมูล UDP อาจมีลำดับความสำคัญต่ำเมื่อการรับส่งข้อมูลของเครือข่ายอยู่ในลำดับสูง

อินเทอร์เฟซแบบแยกสองตัว (eth0 และ eth1)

เมื่อใช้อินเทอร์เฟซเครือข่ายสองตัว (eth0 และ eth1) คุณจะสามารถตั้งค่าเครือข่ายในเครือข่ายแบบแยกกันทางกายภาพหรือแบบเสมือนจริงได้

ตรวจสอบข้อควรพิจารณาต่อไปนี้เมื่อต้องทำการกำหนดอินเทอร์เฟซเครือข่าย eth0 และ eth1

- อินเทอร์เฟซเครือข่าย eth0 ต้องเชื่อมต่อกับเครือข่ายการจัดการและต้องมีการกำหนดค่าเพื่อรองรับการค้นพบและการจัดการอุปกรณ์ Lenovo XClarity Management Hub ต้องสามารถสื่อสารกับอุปกรณ์ทั้งหมดที่จะจัดการจากเครือข่ายการจัดการ
- สามารถกำหนดค่าอินเทอร์เฟซเครือข่าย eth1 ให้สื่อสารกับเครือข่ายข้อมูลภายใน เครือข่ายข้อมูลสาธารณะ หรือทั้งสองเครือข่ายได้
- ในการปรับใช้อิมเมจระบบปฏิบัติการ อินเทอร์เฟซเครือข่าย eth1 ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเครือข่ายเซิร์ฟเวอร์ที่ใช้ในการเข้าถึงระบบปฏิบัติการโฮสต์
- สามารถใช้ฟังก์ชันได้บนเครือข่ายใดเครือข่ายหนึ่ง
- สำหรับเครือข่ายแบบแยกเสมือนจริง แพ็คเก็ตจากเครือข่ายการจัดการและแพ็คเก็ตจากเครือข่ายข้อมูลถูกส่งผ่านการเชื่อมต่อทางกายภาพเดียวกัน จะมีการใช้การแท็ก VLAN บนแพ็คเก็ตข้อมูลเครือข่ายการจัดการทั้งหมดเพื่อแยกการรับส่งข้อมูลระหว่างสองเครือข่ายออกจากกัน

ข้อควรพิจารณาเกี่ยวกับที่อยู่ IP

ตรวจสอบข้อควรพิจารณาเกี่ยวกับที่อยู่ IP ต่อไปนี้ก่อนทำการกำหนดค่าเครือข่าย

- การเปลี่ยนที่อยู่ IP ของอุปกรณ์เสมือนหลังจาก XClarity Management Hub เริ่มทำงานแล้วจะทำให้เกิดปัญหาการเชื่อมต่อกับ XClarity Orchestrator และอุปกรณ์ที่ได้รับการจัดการทั้งหมด หากคุณต้องเปลี่ยนที่อยู่ IP ให้ยกเลิกการเชื่อมต่อ XClarity Management Hub จาก XClarity Orchestrator และถอนการจัดการอุปกรณ์ที่มีการจัดการทั้งหมดก่อนเปลี่ยนที่อยู่ IP จากนั้นจัดการอุปกรณ์ใหม่และเชื่อมต่อ XClarity Management Hub ไปยัง XClarity Orchestrator อีกครั้งหลังจากเปลี่ยนที่อยู่ IP เสร็จสิ้นแล้ว
- กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) หากใช้ DHCP การเปลี่ยนแปลงที่อยู่ IP ต้องน้อยที่สุด เช่น อ้างอิงที่อยู่ DHCP ตามที่อยู่ MAC หรือกำหนดค่า DHCP เพื่อให้สัญญาเช่าไม่หมดอายุหากที่อยู่ IP ของอุปกรณ์ที่มีการจัดการ (นอกเหนือจากอุปกรณ์ ThinkEdge Client) มีการเปลี่ยนแปลง คุณจะต้องยกเลิกการจัดการอุปกรณ์ แล้วจึงทำการจัดการอีกครั้ง
- ไม่รองรับ Network Address Translation (NAT) ซึ่งเปลี่ยนการแมปพื้นที่ที่อยู่ IP
- ต้องกำหนดค่าอินเทอร์เฟซเครือข่ายด้วยที่อยู่ IPv4 เพื่อจัดการอุปกรณ์ต่อไปนี้ ไม่รองรับที่อยู่ IPv6
  - เซิร์ฟเวอร์ ThinkServer
  - อุปกรณ์ Lenovo Storage

- ไม่รองรับการจัดการอุปกรณ์ RackSwitch โดยใช้ IPv6 Link Local ผ่านทางพอร์ตข้อมูลหรือพอร์ตการจัดการ

ข้อควรพิจารณาด้านความพร้อมใช้งานสูง

ใช้คุณลักษณะความพร้อมใช้งานสูงที่เป็นส่วนหนึ่งของระบบปฏิบัติการโฮสต์เพื่อตั้งค่าความพร้อมใช้งานสูงสำหรับ Lenovo XClarity Orchestrator

Microsoft Hyper-V

ใช้ฟังก์ชันความพร้อมใช้งานสูงที่จัดให้สำหรับสภาพแวดล้อม Hyper-V

VMware ESXi

ในระบบความพร้อมใช้งานสูงของ VMware สามารถกำหนดค่าหลายโฮสต์รวมกันเป็นคลัสเตอร์ได้ โดยใช้ที่จัดเก็บข้อมูลร่วมกันในการสร้างอิมเมจดิสก์ของเครื่องเสมือน (VM) ที่พร้อมใช้งานสำหรับโฮสต์ในคลัสเตอร์ VM ทำงานบนโฮสต์เดียวเท่านั้นในแต่ละครั้ง เมื่อมีปัญหากับ VM อินสแตนซ์อื่นของ VM นั้นจะเริ่มทำงานบนโฮสต์สำรอง

VMware High Availability ต้องมีส่วนประกอบต่อไปนี้

- โฮสต์ขั้นต่ำสองตัวที่มีการติดตั้ง ESXi โฮสต์เหล่านี้จะกลายเป็นส่วนหนึ่งของคลัสเตอร์ VMware
- โฮสต์ที่สามที่มีการติดตั้ง VMware vCenter

  เคล็ดลับ: ตรวจสอบให้แน่ใจว่าคุณติดตั้ง VMware vCenter ในเวอร์ชันที่เข้ากันได้กับเวอร์ชันของ ESXi ที่ติดตั้งบนโฮสต์ที่จะใช้ในคลัสเตอร์

  สามารถติดตั้ง VMware vCenter บนโฮสต์ใดโฮสต์หนึ่งที่จะใช้ในคลัสเตอร์ได้ อย่างไรก็ตาม หากโฮสต์นั้นปิดเครื่องหรือใช้งานไม่ได้ คุณจะสูญเสียการเข้าถึงอินเทอร์เฟซ VMware vCenter ไปด้วย
- ที่จัดเก็บข้อมูลร่วม (ที่จัดเก็บข้อมูล) ที่โฮสต์ทุกตัวในคลัสเตอร์สามารถเข้าถึงได้ คุณสามารถใช้ที่จัดเก็บข้อมูลร่วมประเภทใดก็ได้ที่ VMware รองรับ ที่จัดเก็บข้อมูลจะถูกใช้โดย VMware เพื่อระบุว่า VM ควรจะเปลี่ยนไปยังโฮสต์อื่นหรือไม่ในกรณีล้มเหลว (การตรวจสอบการทำงาน)

บทที่ 2. การกำหนดค่า XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

เมื่อคุณเข้าใช้ Lenovo XClarity Management Hub เป็นครั้งแรก คุณต้องดำเนินการหลายขั้นตอนเพื่อเริ่มต้นตั้งค่า XClarity Management Hub

ขั้นตอน

ดำเนินการตามขั้นตอนต่อไปนี้ในการตั้งค่าเบื้องต้น XClarity Management Hub

ขั้นตอนที่ 1. เข้าสู่ระบบเว็บอินเทอร์เฟซ XClarity Management Hub

ขั้นตอนที่ 2. อ่านและยอมรับข้อตกลงการอนุญาตให้ใช้สิทธิ

ขั้นตอนที่ 3. สร้างบัญชีผู้ใช้เพิ่มเติม

ขั้นตอนที่ 4. กำหนดการเข้าถึงเครือข่าย รวมถึงที่อยู่ IP สำหรับเครือข่ายข้อมูลและการจัดการ

ขั้นตอนที่ 5. กำหนดค่าวันที่และเวลา

ขั้นตอนที่ 6. ลงทะเบียน XClarity Management Hub กับเซิร์ฟเวอร์ Orchestrator

การเข้าสู่ระบบ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถเปิดเว็บอินเทอร์เฟซ XClarity Management Hub จากคอมพิวเตอร์ที่มีการเชื่อมต่อเครือข่ายกับเครื่องเสมือน XClarity Management Hub ได้

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าคุณกำลังใช้หนึ่งในเว็บเบราเซอร์ที่รองรับต่อไปนี้

- Chrome 80.0 ขึ้นไป
- Firefox ESR 68.6.0 ขึ้นไป
- Microsoft Edge 40.0 ขึ้นไป
- Safari 13.0.4 ขึ้นไป (ทำงานบน macOS 10.13 ขึ้นไป)

การเข้าถึงเว็บอินเทอร์เฟซจะดำเนินการผ่านการเชื่อมต่อที่มีความปลอดภัย ตรวจสอบให้แน่ใจว่าคุณใช้ **https**

หากคุณกำหนดค่า XClarity Management Hub จากระยะไกล คุณต้องมีการเชื่อมต่อกับเครือข่ายเลเยอร์ 2 เครือข่ายเดียวกัน ซึ่งต้องเข้าถึงจากที่อยู่ที่ไม่มีการกำหนดเส้นทางจนกว่าการตั้งค่าเริ่มต้นจะเสร็จสมบูรณ์ ดังนั้น ให้พิจารณาการ

เข้าถึงXClarity Management Hubจาก VM อื่นที่มีการเชื่อมต่อกับ XClarity Management Hub ตัวอย่างเช่น คุณสามารถเข้าถึง XClarity Management Hub จาก VM อื่นบนโฮสต์ที่มีการติดตั้ง XClarity Management Hub

XClarity Management Hub ให้เซสชันผู้ใช้ออกจากระบบโดยอัตโนมัติหลังจากผ่านไป 60 นาที โดยไม่คำนึงถึงกิจกรรมของผู้ใช้

ขั้นตอน

ดำเนินการตามขั้นตอนต่อไปนี้เพื่อเข้าสู่ระบบเว็บอินเทอร์เฟซ XClarity Management Hub

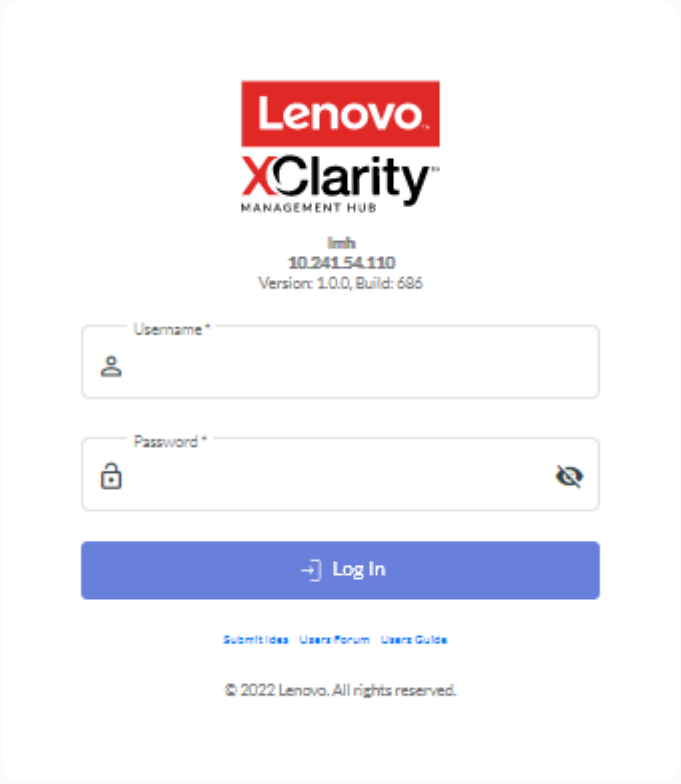
ขั้นตอนที่ 1. ชี้เบราเซอร์ของคุณไปยังที่อยู่ IP XClarity Management Hub
`https://<IPv4_address>`

ตัวอย่าง:
`https://192.0.2.10`

ที่อยู่ IP ที่คุณใช้ขึ้นอยู่กับการตั้งค่าสภาพแวดล้อมของคุณ

- หากคุณระบุที่อยู่ IPv4 ใน eth0_config ใช้ที่อยู่ IPv4 นั้นในการเข้าถึง XClarity Management Hub
- หากเซิร์ฟเวอร์ DHCP ได้รับการตั้งค่าในโดเมนการเผยแพร่เดียวกันกับ XClarity Management Hub ให้ใช้ที่อยู่ IPv4 ที่ปรากฏในคอนโซลเครื่องเสมือน XClarity Management Hub เพื่อเข้าถึง XClarity Management Hub
- หากคุณมีเครือข่าย eth0 และ eth1 บนซับเน็ตที่แยกต่างหาก และหากมีการใช้ DHCP บนทั้งสองซับเน็ต ให้ใช้ที่อยู่ IP ของ *eth1* เมื่อเข้าถึงเว็บอินเทอร์เฟซสำหรับการตั้งค่าเริ่มต้น เมื่อ XClarity Management Hub เริ่มต้นเป็นครั้งแรก ทั้ง eth0 และ eth1 จะได้รับที่อยู่ IP ที่กำหนด DHCP และเกตเวย์เริ่มต้นของ XClarity Management Hub จะได้รับการตั้งค่าเป็นเกตเวย์ที่กำหนด DHCP สำหรับ *eth1*

หน้าการเข้าสู่ระบบเริ่มต้นของ XClarity Management Hub จะแสดง:



ขั้นตอนที่ 2. เลือกภาษาที่ต้องการจากรายการ **ภาษา** แบบดรอปดาวน์

หมายเหตุ: การตั้งค่าและค่าการกำหนดค่าที่ระบุโดยอุปกรณ์ที่มีการจัดการอาจมีเฉพาะภาษาอังกฤษเท่านั้น

ขั้นตอนที่ 3. ป้อนข้อมูลประจำตัวของคุณ แล้วคลิก **เข้าสู่ระบบ**

หากคุณเข้าสู่ระบบ XClarity Management Hub เป็นครั้งแรก ให้ป้อนข้อมูลประจำตัวเริ่มต้น USERID และ PASSW0RD (โดยที่ 0 เป็นศูนย์)

ขั้นตอนที่ 4. อ่านและยอมรับข้อตกลงการอนุญาตให้ใช้สิทธิ

ขั้นตอนที่ 5. หากคุณเข้าสู่ระบบเป็นครั้งแรกโดยใช้ข้อมูลประจำตัวเริ่มต้น ระบบจะแจ้งให้เปลี่ยนรหัสผ่าน ตามค่าเริ่มต้น รหัสผ่านต้องประกอบด้วยอักขระ 8 – 256 ตัวและต้องเป็นไปตามเกณฑ์ต่อไปนี้

ข้อสำคัญ: ขอแนะนาให้ใช้รหัสผ่านที่รัดกุมซึ่งใช้อักขระมากกว่า 16 ตัว

- (1) ต้องมีตัวอักษรพิมพ์ใหญ่อย่างน้อยหนึ่งตัว
- (2) ต้องมีตัวอักษรพิมพ์เล็กอย่างน้อยหนึ่งตัว
- (3) ต้องประกอบด้วยตัวเลขอย่างน้อยหนึ่งตัว
- (4) ต้องประกอบด้วยอักขระพิเศษอย่างน้อยหนึ่งตัว
- (5) ต้องไม่เหมือนกับชื่อผู้ใช้

ขั้นตอนที่ 6. หากคุณเข้าสู่ระบบเป็นครั้งแรก ระบบจะแจ้งให้เลือกว่าจะใช้ใบรับรองที่ลงนามด้วยตนเองปัจจุบัน หรือใช้ใบรับรองที่ลงนามโดย CA ภายนอก หากคุณเลือกใช้ใบรับรองที่ลงนามภายนอก หน้าใบรับรองเซิร์ฟเวอร์จะปรากฏขึ้น

ข้อควรพิจารณา: ใบรับรองที่ลงนามด้วยตนเองไม่ปลอดภัย แนะนำให้สร้างและติดตั้งใบรับรองที่ลงนามภายนอกของคุณเอง

ดูข้อมูลเกี่ยวกับการใช้ใบรับรองที่ลงนามภายนอกได้ที่ การติดตั้งใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกที่เชื่อถือได้ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

หลังจากดำเนินการเสร็จ

คุณสามารถดำเนินการต่อไปนี้ได้จากเมนู **บัญชีผู้ใช้** ( ) ที่มุมขวาบนของเว็บอินเทอร์เฟซ XClarity Management Hub

- ออกจากเซสชันปัจจุบันโดยคลิก **ออกจากระบบ** หน้าเข้าสู่ระบบ XClarity Management Hub จะปรากฏขึ้น
- ถามคำถามและค้นหาคำตอบโดยใช้ เว็บไซต์กระดานสนทนาชุมชน Lenovo XClarity
- ส่งแนวคิดต่างๆ เกี่ยวกับ XClarity Management Hub โดยคลิก **ส่งแนวคิดต่างๆ** จากเมนู **บัญชีผู้ใช้** ( ) ในเว็บอินเทอร์เฟซมุมบนขวา หรือโดยไปที่ เว็บไซต์ Lenovo XClarity Ideation โดยตรง
- ดูเอกสารแบบออนไลน์ โดยคลิกที่ **คู่มือผู้ใช้**
- ดูข้อมูลเกี่ยวกับรุ่นของ XClarity Management Hub โดยคลิก **เกี่ยวกับ**
- เปลี่ยนภาษาของส่วนติดต่อผู้ใช้ได้โดยคลิก **เปลี่ยนภาษา** รองรับภาษาต่อไปนี้
  - ภาษาอังกฤษ (en)
  - ภาษาจีนตัวย่อ (zh-CN)
  - ภาษาจีนตัวเต็ม (zh-TW)
  - ภาษาฝรั่งเศส (fr)
  - ภาษาเยอรมัน (de)
  - ภาษาอิตาลี (it)
  - ภาษาญี่ปุ่น (ja)
  - ภาษาเกาหลี (ko)
  - ภาษาโปรตุเกสบราซิล (pt-BR)
  - ภาษารัสเซีย (ru)
  - ภาษาสเปน (es)
  - ภาษาไทย (th)

การสร้างบัญชีผู้ใช้ของ Lenovo XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถสร้างบัญชีผู้ใช้ได้สูงสุด 10 บัญชีสำหรับ Lenovo XClarity Management Hub

ขั้นตอน

ในการสร้างบัญชีผู้ใช้นั้น ให้ดำเนินการขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. จากแถบเมนู Lenovo XClarity Management Hub ให้คลิก **การรักษาความปลอดภัย** (⚙) ➔ **ผู้ใช้ภายใน** เพื่อแสดงการ์ด ผู้ใช้ภายใน

ขั้นตอนที่ 2. คลิกไอคอน **สร้าง** (⊕) เพื่อสร้างผู้ใช้ กล่องโต้ตอบ สร้างผู้ใช้ใหม่ จะปรากฏขึ้น

ขั้นตอนที่ 3. กรอกข้อมูลต่อไปนี้ลงในกล่องโต้ตอบ

- ป้อนชื่อผู้ใช้ที่ไม่ซ้ำกัน คุณสามารถระบุอักขระได้สูงสุด 32 ตัว รวมถึงอักขระที่เป็นตัวอักษรและตัวเลขคละกัน จุด (.) ขีดกลาง (-) และขีดล่าง (_)

  หมายเหตุ: ชื่อผู้ใช้ไม่จำเป็นต้องตรงตามตัวพิมพ์ใหญ่-เล็ก

- ป้อนรหัสผ่านใหม่ แล้วยืนยัน ตามค่าเริ่มต้น รหัสผ่านต้องประกอบด้วยอักขระ 8 – 256 ตัวและต้องเป็นไปตามเกณฑ์ต่อไปนี้

  ข้อสำคัญ: ขอแนะนาให้ใช้รหัสผ่านที่รัดกุมซึ่งใช้อักขระมากกว่า 16 ตัว
  - (1) ต้องมีตัวอักษรพิมพ์ใหญ่อย่างน้อยหนึ่งตัว
  - (2) ต้องมีตัวอักษรพิมพ์เล็กอย่างน้อยหนึ่งตัว
  - (3) ต้องประกอบด้วยตัวเลขอย่างน้อยหนึ่งตัว
  - (4) ต้องประกอบด้วยอักขระพิเศษอย่างน้อยหนึ่งตัว
  - (5) ต้องไม่เหมือนกับชื่อผู้ใช้

ขั้นตอนที่ 4. คลิก **สร้าง**

เพิ่มบัญชีผู้ใช้ในตาราง

หลังจากดำเนินการเสร็จ

จากการ์ด ผู้ใช้ภายใน คุณสามารถดำเนินการต่อไปนี้ได้

- แก้ไขรหัสผ่านและคุณสมบัติสำหรับบัญชีผู้ใช้ของคุณโดยคลิกไอคอน **แก้ไข** (✎) โปรดทราบว่ารหัสผ่านไม่มีวันหมดอายุ
- ลบผู้ใช้ที่เลือกได้โดยคลิกไอคอน **ลบ** (🗑)

การกำหนดค่าการตั้งค่าเครือข่ายของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถกำหนดค่าการตั้งค่าอินเทอร์เฟซเครือข่าย IPv4 เดียวและการกำหนดเส้นทางอินเทอร์เน็ต

ก่อนจะเริ่มต้น

ตรวจสอบข้อควรพิจารณาเกี่ยวกับเครือข่ายก่อนทำการกำหนดค่าเครือข่าย (โปรดดู ข้อควรพิจารณาเกี่ยวกับเครือข่าย)

ขั้นตอน

หากต้องการกำหนดค่าการตั้งค่าเครือข่าย ให้คลิก **การดูแลระบบ** (⚙) ➔ **เครือข่าย** จากแถบเมนู XClarity Management Hub แล้วดำเนินการขั้นตอนต่อไปนี้อย่างน้อยหนึ่งขั้นตอน

- **กำหนดค่าการตั้งค่า IP**สำหรับอินเทอร์เฟซ eth0 ให้คลิกแท็บ **อินเทอร์เฟซ Eth0** กำหนดค่าการตั้งค่าที่อยู่ IPv4 ที่ใช้ได้ แล้วคลิก **ใช้**

  ข้อควรพิจารณา:

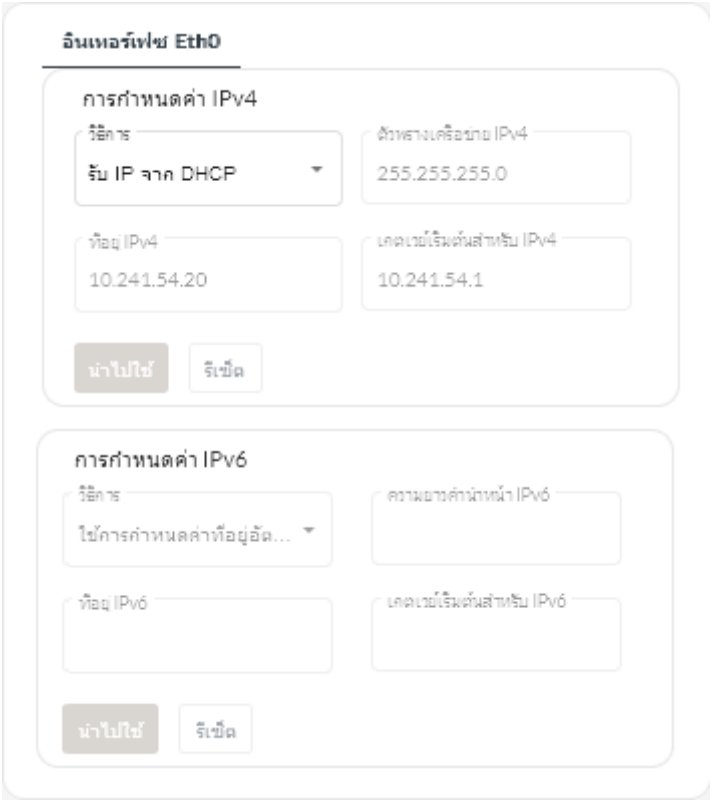
  – การเปลี่ยนที่อยู่ IP ของอุปกรณ์เสมือนหลังจาก XClarity Management Hub เริ่มทำงานแล้วจะทำให้เกิดปัญหาการเชื่อมต่อกับ XClarity Orchestrator และอุปกรณ์ที่ได้รับการจัดการทั้งหมด หากคุณต้องเปลี่ยนที่อยู่ IP ให้ยกเลิกการเชื่อมต่อ XClarity Management Hub จาก XClarity Orchestrator และถอนการจัดการอุปกรณ์ที่มีการจัดการทั้งหมดก่อนเปลี่ยนที่อยู่ IP จากนั้นจัดการอุปกรณ์ใหม่และเชื่อมต่อ XClarity Management Hub ไปยัง XClarity Orchestrator อีกครั้งหลังจากเปลี่ยนที่อยู่ IP เสร็จสิ้นแล้ว

  ปัจจุบันรองรับเฉพาะที่อยู่ IPv4 เท่านั้น

  – **การตั้งค่า IPv4** คุณสามารถกำหนดค่าวิธีการกำหนด IP, ที่อยู่ IPv4, ตัวพรางเครือข่าย และเกตเวย์เริ่มต้น สำหรับวิธีการกำหนด IP คุณสามารถเลือกที่จะใช้ที่อยู่ IP ที่กำหนดแบบคงที่หรือเลือกรับที่อยู่ IP จากเซิร์ฟเวอร์ DHCP เมื่อใช้ที่อยู่ IP แบบคงที่ คุณต้องระบุที่อยู่ IP, ตัวพรางเครือข่าย และเกตเวย์เริ่มต้น

เกตเวย์เริ่มต้นจะต้องเป็นที่อยู่ IP ที่ถูกต้องและต้องใช้มาสก์เครือข่ายเดียวกัน (ซับเน็ตเดียวกัน) กับอินเทอร์เฟซที่เปิดใช้งาน (eth0)

หาอินเทอร์เฟซตัวใดตัวหนึ่งใช้ DHCP เพื่อรับที่อยู่ IP เกตเวย์เริ่มต้นจะใช้ DHCP ด้วย

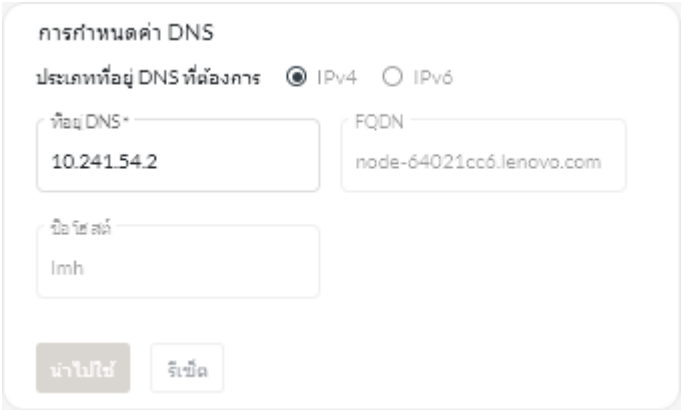


- **กำหนดค่าการตั้งค่าการกำหนดเส้นทางอินเทอร์เน็ต**เลือกที่จะกำหนดค่าการตั้งค่าระบบชื่อโดเมน (DNS) จากการ์ด การกำหนดค่า DNS จากนั้นคลิก **ใช้**

  ปัจจุบันรองรับเฉพาะที่อยู่ IPv4 เท่านั้น

  คุณสามารถเปลี่ยนที่อยู่ IP ของเซิร์ฟเวอร์ DNS ได้

  ชื่อโดเมนที่มีคุณสมบัติครบถ้วน (FQDN) และชื่อโฮสต์ของเซิร์ฟเวอร์ DNS เหมือนกับเซิร์ฟเวอร์ XClarity Management Hub และไม่สามารถเปลี่ยนแปลงได้



การกำหนดค่าวันที่และเวลาของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณต้องตั้งค่าเซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย (NTP) อย่างน้อยหนึ่งเครื่อง (สูงสุดสี่) ในการซิงโครไนซ์ประทับเวลาระหว่าง XClarity Management Hub และอุปกรณ์ที่มีการจัดการทั้งหมด

ก่อนจะเริ่มต้น

เซิร์ฟเวอร์ NTP แต่ละเครื่องต้องสามารถเข้าถึงผ่านเครือข่ายได้ ลองพิจารณาการตั้งค่าเซิร์ฟเวอร์ NTP บนระบบภายในที่ XClarity Management Hub กำลังทำงาน

หากคุณเปลี่ยนเวลาในเซิร์ฟเวอร์ NTP อาจใช้เวลาสักครู่กว่าที่ XClarity Management Hub จะซิงโครไนซ์กับเวลาใหม่

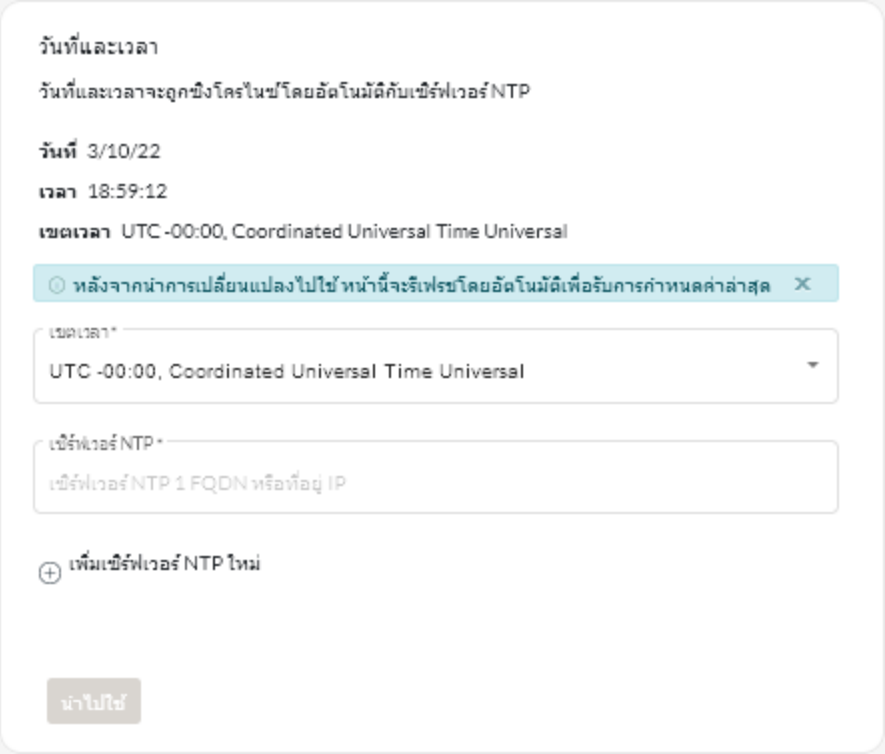
ข้อควรพิจารณา: อุปกรณ์เสมือน XClarity Management Hub และโฮสต์ต้องได้รับการตั้งค่าให้ซิงโครไนซ์เวลาจากแหล่งเดียวกัน เพื่อป้องกันการซิงค์เวลาผิดพลาดระหว่าง XClarity Management Hub และโฮสต์โดยไม่ได้ตั้งใจ โดยปกติ โฮสต์จะได้รับการกำหนดค่าเพื่อให้อุปกรณ์เสมือนซิงค์เวลากับโฮสต์ หาก XClarity Management Hub ได้รับการกำหนดค่าให้ซิงโครไนซ์กับแหล่งอื่นนอกเหนือจากโฮสต์ของตนเอง คุณต้องปิดใช้งานการซิงโครไนซ์เวลากับโฮสต์ระหว่างอุปกรณ์เสมือน XClarity Management Hub กับโฮสต์ของอุปกรณ์เสมือนนั้น

- สำหรับ ESXi ให้ทำตามคำแนะนำใน เว็บเพจ VMware – การปิดใช้งานการซิงโครไนซ์เวลา

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อตั้งค่าวันที่และเวลาสำหรับ XClarity Management Hub

ขั้นตอนที่ 1. จากแถบเมนู XClarity Management Hub ให้คลิก **การดูแลระบบ** (⚙) ➔ **วันที่และเวลา** เพื่อแสดงการ์ด วันที่และเวลา



ขั้นตอนที่ 2. เลือกโซนเวลาที่โฮสต์สำหรับ XClarity Management Hub อยู่

หากโซนเวลาที่เลือกเป็นไปตามเวลาออมแสง (DST) เวลาจะถูกปรับสำหรับ DST โดยอัตโนมัติ

ขั้นตอนที่ 3. ระบุชื่อโฮสต์หรือที่อยู่ IP ของเซิร์ฟเวอร์ NTP แต่ละเครื่องภายในเครือข่ายของคุณ คุณสามารถกำหนดเซิร์ฟเวอร์ NTP สูงสุดสี่เครื่อง

ขั้นตอนที่ 4. คลิก **ใช้**

การจัดการใบรับรองด้านความปลอดภัยของ Lenovo XClarity Management Hub ขสำหรับอุปกรณ์ Edge-Client

Lenovo XClarity Management Hub ใช้ใบรับรอง SSL ในการสร้างการสื่อสารที่ปลอดภัยและน่าเชื่อถือระหว่าง Lenovo XClarity Management Hub และอุปกรณ์ที่มีการจัดการ รวมไปถึงการสื่อสารกับ Lenovo XClarity Management Hub โดยผู้ใช้หรือบริการอื่นๆ ตามค่าเริ่มต้น Lenovo XClarity Management Hub และ XClarity Orchestrator ใช้ XClarity Orchestrator ที่ลงนามด้วยตนเองและออกให้โดยหน่วยงานด้านใบรับรองภายใน

ก่อนจะเริ่มต้น

ส่วนนี้มีไว้สำหรับผู้ดูแลระบบที่มีความเข้าใจพื้นฐานเกี่ยวกับมาตรฐาน SSL และใบรับรอง SSL รวมถึงความหมายและวิธีจัดการมาตรฐานและใบรับรองเหล่านี้ สำหรับข้อมูลทั่วไปเกี่ยวกับใบรับรองคีย์สาธารณะ โปรดดู เว็บเพจ X.509 ใน

Wikipedia และ เว็บเพจ Internet X.509 Public Key Infrastructure Certificate และ Certificate Revocation List (CRL) Profile (RFC5280)

เกี่ยวกับงานนี้

ใบรับรองเซิร์ฟเวอร์เริ่มต้น ซึ่งถูกสร้างขึ้นโดยไม่ซ้ำกันในทุกอินสแตนซ์ของ Lenovo XClarity Management Hub จะมอบการรักษาความปลอดภัยที่เพียงพอสำหรับสภาพแวดล้อมต่างๆ มากมาย คุณสามารถเลือกที่จะให้ Lenovo XClarity Management Hub จัดการใบรับรองให้คุณ หรือคุณสามารถรับบทบาทที่ใช้งานอยู่เพิ่มเติมได้โดยกำหนดใบรับรองเซิร์ฟเวอร์เองและแทนที่ใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub จะให้ตัวเลือกสำหรับการกำหนดใบรับรองเองสำหรับสภาพแวดล้อมของคุณ ตัวอย่างเช่น คุณสามารถเลือก:

- สร้างคีย์คู่ใหม่โดยการสร้างผู้ให้บริการออกใบรับรองภายในและ/หรือใบรับรองเซิร์ฟเวอร์ปลายทางขึ้นมาใหม่ที่ใช้ค่าที่เฉพาะเจาะจงกับองค์กรของคุณ
- สร้างคำขอการลงนามใบรับรอง (CSR) ที่สามารถส่งไปยังผู้ให้บริการออกใบรับรองที่คุณเลือกเพื่อลงนามใบรับรองที่กำหนดเอง ซึ่งสามารถอัปโหลดไปยัง Lenovo XClarity Management Hub เพื่อใช้เป็นใบรับรองเซิร์ฟเวอร์ปลายทางสำหรับบริการที่โฮสต์ทั้งหมด
- ดาวน์โหลดใบรับรองเซิร์ฟเวอร์ไปยังระบบภายในเพื่อให้คุณสามารถนำเข้าใบรับรองนั้นลงในรายการใบรับรองที่เชื่อถือได้ของเว็บเบราเซอร์

Lenovo XClarity Management Hub ให้บริการหลายอย่างที่ยอมรับการเชื่อมต่อ SSL/TLS ขาเข้า เมื่อไคลเอ็นต์ เช่น เว็บเบราเซอร์ เชื่อมต่อกับบริการใดบริการหนึ่งเหล่านี้ Lenovo XClarity Management Hub จะระบุ *ใบรับรองเซิร์ฟเวอร์* เพื่อให้ไคลเอนต์ที่พยายามเชื่อมต่อระบุเซิร์ฟเวอร์ได้ ไคลเอ็นต์ควรเก็บรักษารายการใบรับรองที่ตัวเองเชื่อถือ หากใบรับรองเซิร์ฟเวอร์ของ Lenovo XClarity Management Hub ไม่รวมอยู่ในรายการของไคลเอ็นต์ ไคลเอ็นต์จะตัดการเชื่อมต่อจาก Lenovo XClarity Management Hub เพื่อหลีกเลี่ยงการแลกเปลี่ยนข้อมูลที่มีความละเอียดอ่อนด้านการรักษาความปลอดภัยกับแหล่งที่ไม่น่าเชื่อถือ

Lenovo XClarity Management Hub ทำหน้าที่เป็นไคลเอ็นต์เมื่อสื่อสารกับอุปกรณ์ที่ได้รับการจัดการและบริการภายนอก เมื่อเกิดกรณีเช่นนี้ขึ้น อุปกรณ์ที่มีการจัดการหรือบริการภายนอกจะให้ใบรับรองของเซิร์ฟเวอร์เพื่อที่จะรับการตรวจสอบโดย Lenovo XClarity Management Hub Lenovo XClarity Management Hub จะเก็บรักษารายการใบรับรองที่ตัวเองเชื่อถือ หาก *ใบรับรองที่เชื่อถือได้* ที่อุปกรณ์ที่ได้รับการจัดการหรือบริการภายนอกนั้นระบุไม่มีรวมอยู่ในรายการ Lenovo XClarity Management Hub จะตัดการเชื่อมต่อกับอุปกรณ์ที่ได้รับการจัดการหรือบริการภายนอก เพื่อหลีกเลี่ยงการแลกเปลี่ยนข้อมูลที่มีความละเอียดอ่อนด้านการรักษาความปลอดภัยกับแหล่งที่ไม่น่าเชื่อถือ

ประเภทของใบรับรองต่อไปนี้ใช้โดยบริการ Lenovo XClarity Management Hub และควรได้รับการเชื่อถือโดยไคลเอ็นต์ที่เชื่อมต่อกับใบรับรอง

- **ใบรับรองเซิร์ฟเวอร์** ระหว่างการบูตเริ่มต้น ระบบจะสร้างคีย์และใบรับรองที่ลงนามด้วยตนเองที่ไม่ซ้ำกัน รายการเหล่านี้จะใช้เป็นผู้ให้บริการออกใบรับรองรูท ซึ่งสามารถจัดการได้ในหน้าหน่วยงานด้านใบรับรองในการตั้งค่าการรักษาความปลอดภัย Lenovo XClarity Management Hub ไม่จำเป็นต้องสร้างใบรับรองรูทนี้ใหม่ เว้นแต่คีย์จะถูกบุกรุก หรือหน่วยงานของคุณมีนโยบายที่กำหนดให้เปลี่ยนใบรับรองทั้งหมดเป็นระยะ (ดูที่ การสร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองใหม่ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client)นอกจากนี้ ระหว่างการตั้งค่าเริ่มต้น จะมีการสร้างคีย์ที่แยกต่างหากและใบรับรองเซิร์ฟเวอร์ที่สร้างและลงนามโดยหน่วยงานด้านใบรับรองภายใน ใบรับรองนี้จะใช้เป็นใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ตามค่าเริ่มต้น ซึ่งจะสร้างใหม่โดยอัตโนมัติในแต่ละครั้งที่ Lenovo XClarity Management Hub ตรวจพบว่าที่อยู่เครือข่าย (ที่อยู่ IP หรือ DNS) เปลี่ยนแปลงเพื่อทำให้แน่ใจว่าใบรับรองมีที่อยู่ที่ถูกต้องสำหรับเซิร์ฟเวอร์ ซึ่งสามารถกำหนดเองและสร้างตามความต้องการ (ดูที่ การสร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองใหม่ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client)

  คุณสามารถเลือกใช้ใบรับรองเซิร์ฟเวอร์ที่ลงนามภายนอกแทนใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองเริ่มต้นโดยสร้างคำขอการลงนามใบรับรอง (CSR) ให้ CSR ลงนามโดยผู้ให้บริการออกใบรับรองรูทในเชิงพาณิชย์หรือส่วนตัว จากนั้นนำเข้ากลุ่มใบรับรองทั้งหมดลงใน Lenovo XClarity Management Hub (ดู การติดตั้งใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกที่เชื่อถือได้ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

  หากคุณเลือกที่จะใช้ใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองเริ่มต้น ขอแนะนำให้คุณนำเข้าใบรับรองเซิร์ฟเวอร์ในเว็บเบราเซอร์เป็นหน่วยงานด้านใบรับรองรูทที่เชื่อถือได้ เพื่อหลีกเลี่ยงข้อความแสดงข้อผิดพลาดของใบรับรองในเบราเซอร์ของคุณ (ดู การนำเข้าใบรับรองของเซิร์ฟเวอร์ลงในเว็บเบราเซอร์ของ Lenovo XClarity Management Hub สำหรับอุปกรณ์ Edge-Client
- **ใบรับรองการปรับใช้** OS บริการการปรับใช้ระบบปฏิบัติการจะใช้ใบรับรองที่แยกต่างหาก เพื่อทำให้แน่ใจว่าโปรแกรมติดตั้งระบบปฏิบัติการสามารถเชื่อมต่อกับบริการการปรับใช้ได้อย่างปลอดภัยในระหว่างขั้นตอนการปรับใช้ หากคีย์ถูกบุกรุก คุณสามารถสร้างคีย์ใหม่โดยรีสตาร์ท Lenovo XClarity Management Hub

การสร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองใหม่ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถสร้างใบรับรองเซิร์ฟเวอร์ใหม่เพื่อแทนที่ใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ที่ลงนามด้วยตนเองปัจจุบัน หรือนำใบรับรองที่สร้างโดย XClarity Management Hub กลับมาใช้อีก หาก XClarity Management Hub ใช้ใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกที่กำหนดเองอยู่ในปัจจุบัน XClarity Management Hub ใช้ใบรับรองของเซิร์ฟเวอร์ที่ลงนามด้วยตนเองใหม่สำหรับการเข้าถึง HTTPS

ก่อนจะเริ่มต้น

ข้อควรพิจารณา: หากคุณสร้างใบรับรองเซิร์ฟเวอร์ XClarity Management Hub โดยใช้ใบรับรองรูท CA ใหม่ XClarity Management Hub จะสูญเสียการเชื่อมต่อกับอุปกรณ์ที่มีการจัดการ และคุณต้องจัดการอุปกรณ์อีกครั้ง หากคุณสร้างใบรับรองเซิร์ฟเวอร์ XClarity Management Hub โดยไม่เปลี่ยนรูท CA (ตัวอย่างเช่น เมื่อใบรับรองหมดอายุ) คุณจะไม่ต้องจัดการอุปกรณ์ใหม่

เกี่ยวกับงานนี้

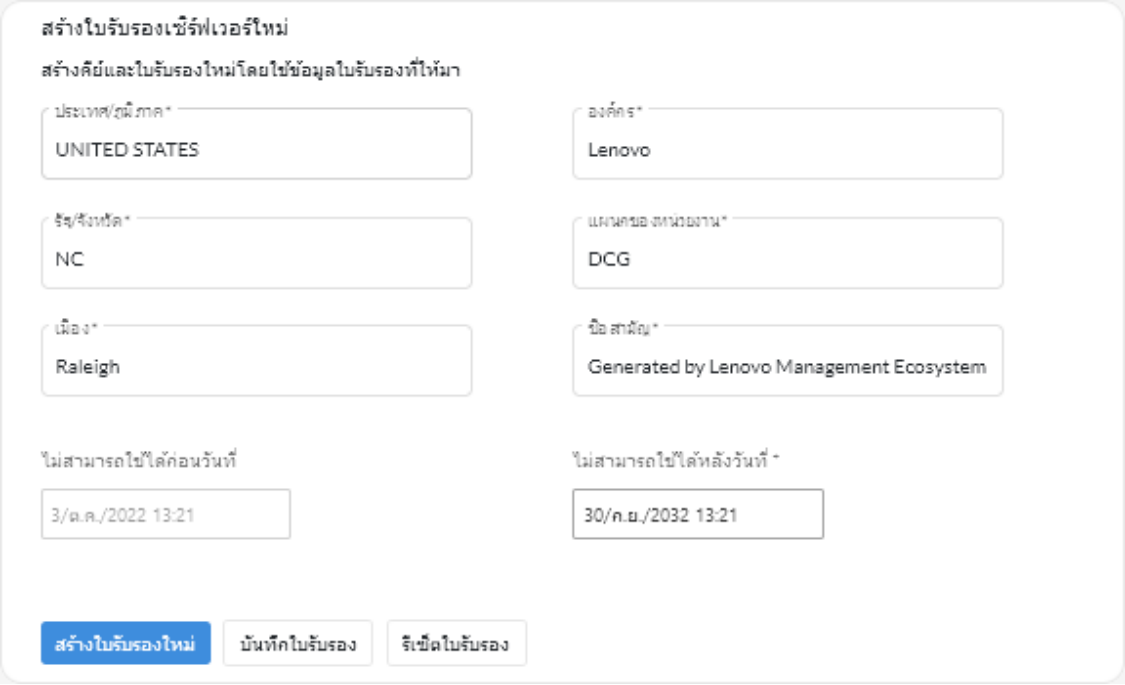
ใบรับรองเซิร์ฟเวอร์ที่มีการใช้งานอยู่ในปัจจุบันบน ไม่ว่าจะเป็นแบบลงนามด้วยตัวเองหรือลงนามจากภายนอกจะยังคงมีการใช้งานอยู่ จนกว่าจะมีการสร้างใบรับรองเซิร์ฟเวอร์ใหม่ ลงนาม และติดตั้ง

ข้อสำคัญ: เมื่อใบรับรองเซิร์ฟเวอร์ถูกแก้ไข อับการจัดการจะรีสตาร์ท และเซสชันของผู้ใช้ทั้งหมดจะสิ้นสุดลง ผู้ใช้ต้องเข้าสู่ระบบอีกครั้งเพื่อใช้งานเว็บอินเทอร์เฟซต่อ

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อสร้างใบรับรองเซิร์ฟเวอร์ XClarity Management Hub ที่ลงนามด้วยตัวเอง

ขั้นตอนที่ 1. จากแถบเมนู XClarity Management Hub ให้คลิก **การรักษาความปลอดภัย** (⚙) ➔ **ใบรับรองเซิร์ฟเวอร์** เพื่อแสดงการ์ด **สร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองใหม่**



ขั้นตอนที่ 2. จากการ์ด **สร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตัวเองใหม่** ให้กรอกข้อมูลในฟิลด์สำหรับคำขอ

- รหัส ISO 3166 สองตัวอักษรสำหรับประเทศและภูมิภาคต้นทางที่เชื่อมโยงกับหน่วยงานด้านใบรับรอง (เช่น US สำหรับสหรัฐอเมริกา)
- ชื่อเต็มของรัฐหรือจังหวัดที่จะเชื่อมโยงกับใบรับรอง (เช่น แคลิฟอร์เนียหรือนิวบรันสวิก)
- ชื่อเต็มของเมืองที่จะเชื่อมโยงกับใบรับรอง (ตัวอย่างเช่น San Jose) ความยาวของค่าต้องไม่เกิน 50 อักขระ

- องค์กร (บริษัท) ซึ่งเป็นเจ้าของใบรับรอง โดยทั่วไปแล้วคือชื่อตามกฎหมายของบริษัท ควรใส่ส่วนต่อท้ายใดๆ เช่น Ltd., Inc., หรือ Corp (เช่น ACME International Ltd.) ความยาวของค่านี้ต้องไม่เกิน 60 อักขระ
- (ไม่บังคับ) หน่วยงานที่เป็นเจ้าของใบรับรอง (เช่น ABC Division) ความยาวของค่านี้ต้องไม่เกิน 60 อักขระ
- ชื่อทั่วไปของเจ้าของใบรับรอง โดยทั่วไปแล้วคือชื่อโดเมนแบบเต็ม (FQDN) หรือที่อยู่ IP ของเซิร์ฟเวอร์ที่ใช้ใบรับรอง (เช่น **www.domainname.com** หรือ **192.0.2.0**) ความยาวของค่านี้ต้องไม่เกิน 63 อักขระ

  หมายเหตุ: ในขณะนี้ แอตทริบิวต์นี้ไม่มีผลกระทบกับใบรับรอง
- วันที่และเวลาที่ใบรับรองเซิร์ฟเวอร์ไม่ถูกต้องอีกต่อไป

  หมายเหตุ: ในขณะนี้ แอตทริบิวต์เหล่านี้ไม่มีผลกระทบกับใบรับรอง

หมายเหตุ: คุณไม่สามารถเปลี่ยนชื่อแสดงแทนบุคคลที่ได้รับการรับรองเมื่อสร้างใบรับรองเซิร์ฟเวอร์ใหม่

ขั้นตอนที่ 3. คลิก **สร้างใบรับรองที่ลงนามด้วยตัวเองใหม่** เพื่อสร้างใบรับรองที่ลงนามด้วยตัวเองใหม่ แล้วคลิก **สร้างใบรับรองใหม่** เพื่อยืนยัน
ฮับการจัดการจะรีสตาร์ท และเซสชันผู้ใช้ที่เกิดขึ้นทั้งหมดจะสิ้นสุดลง

ขั้นตอนที่ 4. เข้าสู่ระบบเว็บเบราเซอร์ใหม่

หลังจากดำเนินการเสร็จ

จากการ์ด สร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตัวเองใหม่ คุณสามารถดำเนินการต่อไปนี้ได้

- บันทึกใบรับรองเซิร์ฟเวอร์ปัจจุบันไปยังระบบภายในของคุณในรูปแบบ PEM โดยคลิก **บันทึกใบรับรอง**
- สร้างใบรับรองเซิร์ฟเวอร์ใหม่โดยใช้การตั้งค่าเริ่มต้นโดยคลิก **รีเซ็ตใบรับรอง** เมื่อได้รับข้อความแจ้ง ให้กด Ctrl+F5 เพื่อรีเฟรชเบราเซอร์ จากนั้นสร้างการเชื่อมต่อกับเว็บอินเทอร์เฟซอีกครั้ง

การติดตั้งใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกที่เชื่อถือได้ของ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถเลือกใช้ใบรับรองเซิร์ฟเวอร์ที่เชื่อถือได้ที่มีการลงนามโดยหน่วยงานด้านใบรับรอง (CA) เอกชนหรือพาณิชย์ในการใช้ใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอก ให้สร้างคำขอการลงนามใบรับรอง (CSR) แล้วนำเข้าใบรับรองเซิร์ฟเวอร์ที่ได้มาเพื่อแทนที่ใบรับรองเซิร์ฟเวอร์ที่มีอยู่

ก่อนจะเริ่มต้น

ข้อควรพิจารณา:

- หากคุณติดตั้งใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ที่ลงนามจากภายนอกโดยใช้ใบรับรองรูท CA ใหม่ XClarity Management Hub จะสูญเสียการเชื่อมต่อกับอุปกรณ์ที่มีการจัดการ และคุณต้องจัดการอุปกรณ์อีกครั้ง หากคุณติดตั้งใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ที่ลงนามจากภายนอกโดยไม่เปลี่ยนรูท CA (ตัวอย่างเช่น เมื่อใบรับรองหมดอายุ) คุณจะไม่ต้องจัดการอุปกรณ์ใหม่
- หากมีการเพิ่มอุปกรณ์ใหม่หลังจากสร้าง CSR และก่อนที่จะนำเข้าใบรับรองเซิร์ฟเวอร์ที่ลงนาม ต้องรีสตาร์ทอุปกรณ์เหล่านั้นเพื่อรับใบรับรองเซิร์ฟเวอร์ใหม่

เกี่ยวกับงานนี้

แนวทางปฏิบัติที่ดีที่สุดคือให้ใช้ใบรับรองที่ลงนาม v3 เสมอ

ต้องสร้างใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกจากคำขอการลงนามใบรับรองที่สร้างขึ้นล่าสุดโดยใช้ปุ่ม **สร้างไฟล์ CSR**

เนื้อหาของใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกต้องเป็นชุดใบรับรองที่ประกอบด้วยสายการลงนาม CA ทั้งหมด รวมทั้งใบรับรองรูทของ CA, ใบรับรองระดับกลางใดๆ และใบรับรองเซิร์ฟเวอร์

หากใบรับรองเซิร์ฟเวอร์ใหม่ไม่ได้รับการลงนามโดยบุคคลที่สามที่เชื่อถือได้ ครั้งถัดไปที่คุณเชื่อมต่อกับ Lenovo XClarity Management Hub เบราเซอร์ของคุณจะแสดงข้อความเกี่ยวกับการรักษาความปลอดภัยและกล่องโต้ตอบที่แจ้งให้คุณยอมรับใบรับรองใหม่ลงในเบราเซอร์ เพื่อหลีกเลี่ยงข้อความเกี่ยวกับการรักษาความปลอดภัย คุณสามารถนำเข้าใบรับรองเซิร์ฟเวอร์ลงในรายการใบรับรองที่เชื่อถือได้ของเว็บเบราเซอร์ (โปรดดู การนำเข้าใบรับรองของเซิร์ฟเวอร์ลงในเว็บเบราเซอร์ของ Lenovo XClarity Management Hub สำหรับอุปกรณ์ Edge-Client)

XClarity Management Hub เริ่มต้นใช้งานใบรับรองเซิร์ฟเวอร์ใหม่โดยไม่ต้องสิ้นสุดเซสชันปัจจุบัน ระบบจะสร้างเซสชันใหม่โดยใช้ใบรับรองใหม่ เมื่อต้องการใช้ใบรับรองใหม่ที่ใช้งานอยู่ ให้รีสตาร์ทเว็บเบราเซอร์ของคุณ

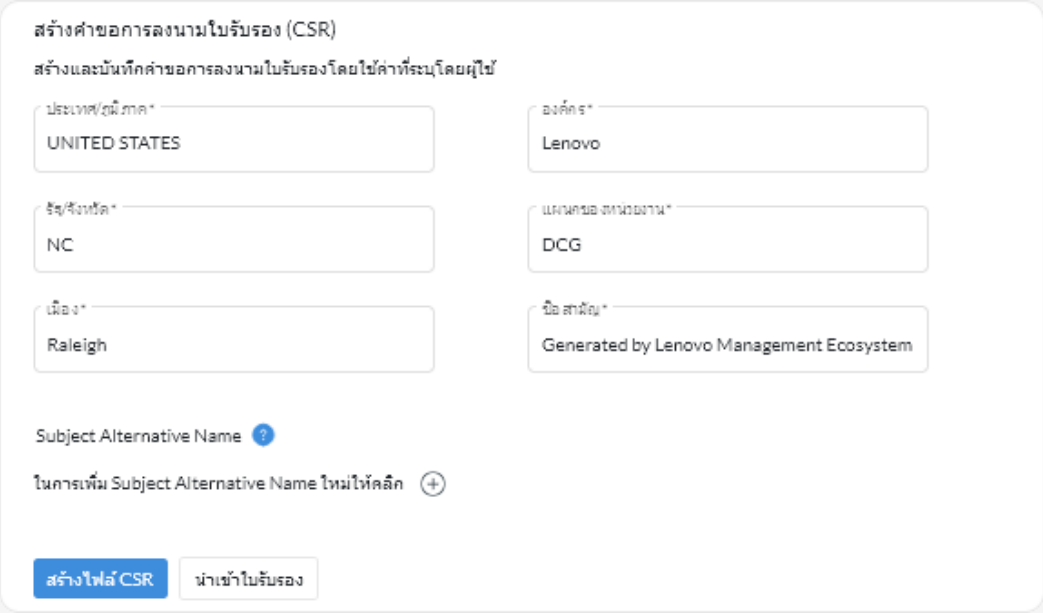
ข้อสำคัญ: เมื่อมีการแก้ไขใบรับรองของเซิร์ฟเวอร์ เซสชันผู้ใช้ที่สร้างขึ้นทั้งหมดต้องยอมรับใบรับรองใหม่โดยคลิก Ctrl +F5 เพื่อรีเฟรชเว็บเบราเซอร์ แล้วจึงสร้างการเชื่อมต่อกับ XClarity Management Hub อีกครั้ง

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อสร้างและติดตั้งใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอก

ขั้นตอนที่ 1. สร้างคำขอการลงนามใบรับรองและบันทึกไฟล์ไปยังระบบภายในของคุณ

1. จากแถบเมนู XClarity Management Hub ให้คลิก **การรักษาความปลอดภัย** (⚙) ➔ **ใบรับรองเซิร์ฟเวอร์** เพื่อแสดงการ์ดข้อมูล สร้างคำขอการลงนามใบรับรอง



2. จากการ์ดสร้างคำขอการลงนามใบรับรอง (CSR) ให้กรอกข้อมูลในฟิลด์สำหรับคำขอ

   - รหัส ISO 3166 สองตัวอักษรสำหรับประเทศหรือภูมิภาคต้นทางที่เชื่อมโยงกับหน่วยงานด้านใบรับรอง (เช่น US สำหรับสหรัฐอเมริกา)
   - ชื่อเต็มของรัฐหรือจังหวัดที่จะเชื่อมโยงกับใบรับรอง (เช่น แคลิฟอร์เนียหรือนิวบรันสวิก)
   - ชื่อเต็มของเมืองที่จะเชื่อมโยงกับใบรับรอง (ตัวอย่างเช่น San Jose) ความยาวของค่าต้องไม่เกิน 50 อักขระ
   - องค์กร (บริษัท) ซึ่งเป็นเจ้าของใบรับรอง โดยทั่วไปแล้วคือชื่อตามกฎหมายของบริษัท ควรใส่ส่วนต่อท้ายใดๆ เช่น Ltd., Inc., หรือ Corp (เช่น ACME International Ltd.) ความยาวของค่านี้ต้องไม่เกิน 60 อักขระ
   - (ไม่บังคับ) หน่วยงานที่เป็นเจ้าของใบรับรอง (เช่น ABC Division) ความยาวของค่านี้ต้องไม่เกิน 60 อักขระ
   - ชื่อทั่วไปของเจ้าของใบรับรอง ส่วนนี้ต้องเป็นชื่อโฮสต์ของเซิร์ฟเวอร์ที่ใช้ใบรับรอง ความยาวของค่านี้ต้องไม่เกิน 63 อักขระ

     หมายเหตุ: ในขณะนี้ แอตทริบิวต์นี้ไม่มีผลกระทบกับใบรับรอง
   - (ไม่บังคับ) Subject Alternative Name ที่ปรับแต่ง ลบ และเพิ่มไปยังส่วนขยาย X.509 "subjectAltName" เมื่อสร้าง CSR Subject Alternative Name ที่ระบุจะได้รับการตรวจสอบ (ตามประเภทที่ระบุ) และจะเพิ่มไปยัง CSR เฉพาะหลังจากที่คุณสร้าง CSR เท่านั้น ตามค่าเริ่มต้น XClarity Management Hub จะกำหนดชื่อแสดงแทนบุคคลที่ได้รับการรับรองสำหรับ CSR โดยอัตโนมัติตามที่อยู่ IP และชื่อโฮสต์ที่ค้นพบโดยอินเทอร์เฟสเครือข่ายสำหรับระบบปฏิบัติการเกสต์ของ XClarity Management Hub

ข้อควรพิจารณา: Subject Alternative Name ต้องมีชื่อโดเมนแบบเต็ม (FQDN) หรือที่อยู่ IP ของฮับการจัดการ และต้องตั้งค่า Subject Name เป็น FQDN ของฮับการจัดการ ตรวจสอบว่ากรอกข้อมูลในฟิลด์ที่จำเป็นเหล่านี้แล้วและมีความถูกต้องก่อนเริ่มกระบวนการ CSR เพื่อให้แน่ใจว่าใบรับรองจะเสร็จสมบูรณ์ ข้อมูลใบรับรองที่ขาดหายไปอาจส่งผลให้เกิดการเชื่อมต่อที่ไม่น่าเชื่อถือเมื่อพยายามเชื่อมต่อฮับการจัดการกับ Lenovo XClarity Orchestrator

ชื่อที่คุณระบุต้องถูกต้องสำหรับประเภทที่เลือก

- **DNS** (ใช้ FQDN ตัวอย่างเช่น hostname.labs.company.com)
- **ที่อยู่ IP** (เช่น 192.0.2.0)
- **อีเมล** (เช่น example@company.com)

ขั้นตอนที่ 2. จัดหา CSR ให้กับหน่วยงานด้านใบรับรอง (CA) ที่น่าเชื่อถือ CA ลงนาม CSR และส่งกลับใบรับรองเซิร์ฟเวอร์

ขั้นตอนที่ 3. นำเข้าใบรับรองเซิร์ฟเวอร์ที่ลงนามจากภายนอกและใบรับรอง CA ลงใน XClarity Management Hub และแทนที่ใบรับรองเซิร์ฟเวอร์ปัจจุบัน

1. จากการ์ดสร้างคำขอการลงนามใบรับรอง (CSR) ให้คลิก **นำเข้าใบรับรอง** เพื่อแสดงกล่องโต้ตอบ นำเข้าใบรับรอง
2. คัดลอกและวางใบรับรองเซิร์ฟเวอร์และใบรับรอง CA ในรูปแบบ PEM คุณต้องระบุสายใบรับรองทั้งหมด โดยเริ่มต้นด้วยใบรับรองเซิร์ฟเวอร์และลงท้ายด้วยใบรับรอง CA รูท
3. คลิก **นำเข้า** เพื่อจัดเก็บใบรับรองเซิร์ฟเวอร์ในพื้นที่จัดเก็บที่น่าเชื่อถือของ XClarity Management Hub

ขั้นตอนที่ 4. ยอมรับใบรับรองใหม่โดยกด Ctrl+F5 เพื่อรีเฟรชเบราเซอร์ จากนั้นสร้างการเชื่อมต่อกับเว็บอินเทอร์เฟซอีกครั้ง ซึ่งต้องดำเนินการโดยเซสชันผู้ใช้ที่สร้างขึ้นทั้งหมด

การนำเข้าใบรับรองของเซิร์ฟเวอร์ลงในเว็บเบราเซอร์ของ Lenovo XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

คุณสามารถบันทึกสำเนาของใบรับรองเซิร์ฟเวอร์ปัจจุบันในรูปแบบ PEM ลงในระบบภายในของคุณ จากนั้นคุณสามารถนำเข้าใบรับรองลงในรายการใบรับรองที่เชื่อถือได้ของเว็บเบราเซอร์หรือแอปพลิเคชันอื่นๆ เพื่อหลีกเลี่ยงข้อความแจ้งเตือนด้านการรักษาความปลอดภัยจากเว็บเบราเซอร์เมื่อคุณเข้าถึง Lenovo XClarity Management Hub

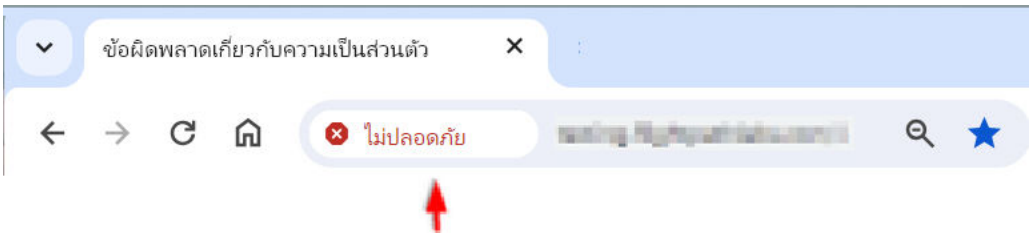
ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อนำเข้าใบรับรองเซิร์ฟเวอร์ลงในเว็บเบราเซอร์

- Chrome

1. ส่งออกใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub

a. คลิกไอคอนคำเตือน “ไม่ปลอดภัย” ในแถบที่อยู่ด้านบน เช่น:



b. คลิก **ใบรับรองไม่ถูกต้อง** เพื่อแสดงกล่องโต้ตอบใบรับรอง

c. คลิกแท็บ **รายละเอียด**

d. คลิก **ส่งออก**

e. ระบุชื่อและตำแหน่งของไฟล์ใบรับรอง แล้วคลิก **บันทึก** เพื่อส่งออกใบรับรอง

f. ปิดกล่องโต้ตอบตัวแสดงใบรับรอง

2. นำเข้าใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ลงในรายการใบรับรองรูทจากหน่วยงานที่เชื่อถือสำหรับเบราเซอร์ของคุณ

a. จากเบราเซอร์ Chrome ของคุณ ให้คลิกจุดสามจุดที่มุมขวาบนของหน้าต่าง แล้วคลิก **การตั้งค่า** เพื่อเปิดหน้า การตั้งค่า

b. คลิก **ความเป็นส่วนตัวและการรักษาความปลอดภัย** แล้วคลิก **การรักษาความปลอดภัย** เพื่อแสดงหน้า การรักษาความปลอดภัย

c. เลื่อนไปยังส่วน **ขั้นสูง** แล้วคลิก **จัดการใบรับรองของอุปกรณ์**

d. คลิก **นำเข้า** แล้วคลิก **ถัดไป**

e. เลือกไฟล์ใบรับรองที่คุณส่งออกก่อนหน้านี้ แล้วคลิก **ถัดไป**

f. เลือกตำแหน่งที่จัดเก็บใบรับรอง แล้วคลิก **ถัดไป**

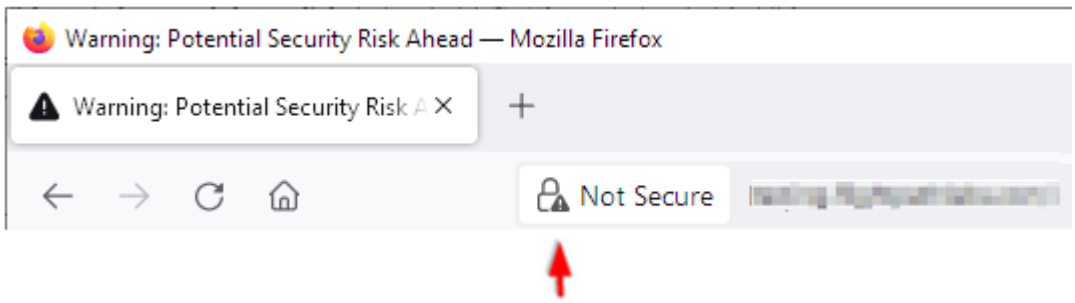
g. คลิก **เสร็จ**

h. ปิดและเปิดเบราว์เซอร์ Chrome แล้วเปิด Lenovo XClarity Management Hub ใหม่

- Firefox

1. ส่งออกใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub

a. คลิกไอคอนคำเตือน “ไม่ปลอดภัย” ในแถบที่อยู่ด้านบน เช่น:



b. คลิก **การเชื่อมต่อไม่ปลอดภัย** แล้วคลิก **ข้อมูลเพิ่มเติม**

c. คลิก **ดูใบรับรอง**

d. เลื่อนลงไปยังส่วน **เบ็ดเตล็ด** และคลิกลิงก์ PEM **(ใบรับรอง)** เพื่อบันทึกไฟล์ไปยังระบบภายใน

2. นำเข้าใบรับรองเซิร์ฟเวอร์ Lenovo XClarity Management Hub ลงในรายการใบรับรองรูทจากหน่วยงานที่เชื่อถือสำหรับเบราเซอร์ของคุณ

a. เปิดเบราเซอร์ แล้วคลิก **เครื่องมือ ➔ การตั้งค่า** แล้วคลิก **ความเป็นส่วนตัวและการรักษาความปลอดภัย**

b. เลื่อนลงไปยังส่วน **การรักษาความปลอดภัย**

c. คลิก **ดูใบรับรอง** เพื่อแสดงกล่องโต้ตอบ ตัวจัดการใบรับรอง

d. คลิกแท็บ **ใบรับรองของคุณ**

e. คลิก **นำเข้า** และเรียกดูตำแหน่งที่ตั้งที่ดาวน์โหลดใบรับรอง

f. เลือกใบรับรอง แล้วคลิก **เปิด**

g. ปิดกล่องโต้ตอบ ตัวจัดการใบรับรอง

การเชื่อมต่อ XClarity Management Hub สำหรับอุปกรณ์ Edge-Client กับ XClarity Orchestrator

หลังจากลงทะเบียน (เชื่อมต่อ) Lenovo XClarity Management Hub กับ Lenovo XClarity Orchestrator คุณสามารถเริ่มต้นการจัดการและตรวจสอบอุปกรณ์ได้

ก่อนจะเริ่มต้น

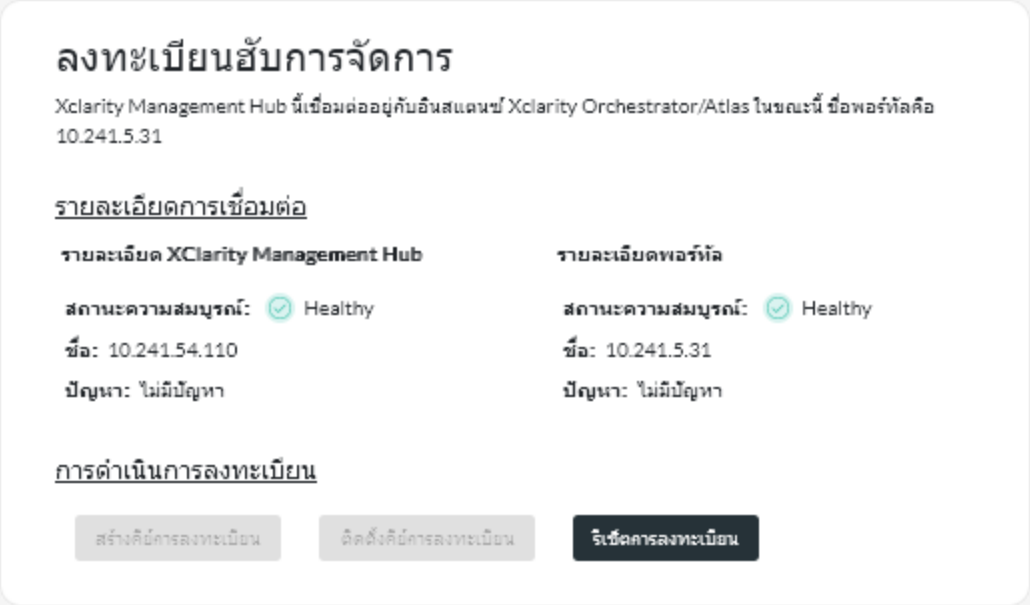
ตรวจสอบว่า XClarity Management Hub สามารถเข้าถึงได้ในเครือข่ายจาก XClarity Orchestrator และตรวจสอบว่า XClarity Orchestrator สามารถเข้าถึงได้ในเครือข่ายจาก XClarity Management Hub

ขั้นตอน

ในการลงทะเบียน XClarity Management Hub ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. สร้างคีย์การลงทะเบียนฮับการจัดการ

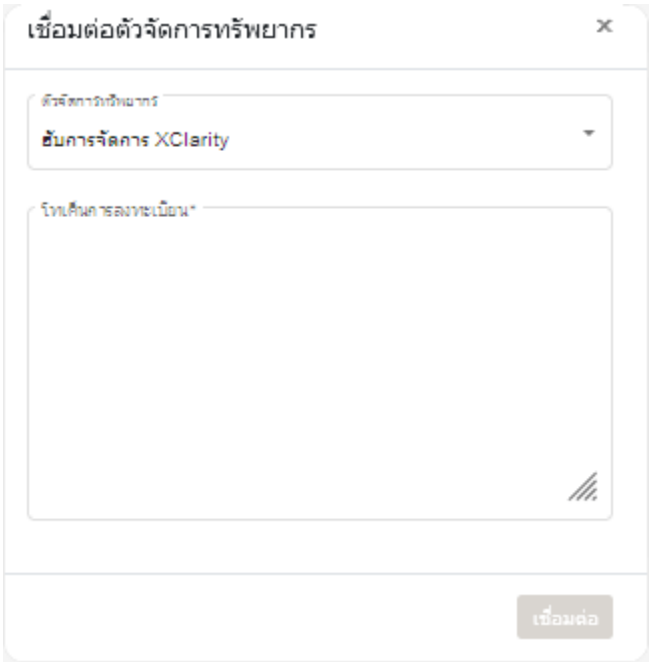
1. จากแถบเมนู Management Hub ให้คลิก **การลงทะเบียน** เพื่อแสดงหน้า การลงทะเบียน



2. สร้าง **สร้างคีย์การลงทะเบียน**
3. คลิก **คัดลอกไปยังคลิปบอร์ด** เพื่อคัดลอกคีย์การลงทะเบียน แล้วปิดกล่องโต้ตอบ

ขั้นตอนที่ 2. เพิ่มคีย์การลงทะเบียนฮับการจัดการไปยัง XClarity Orchestrator

1. จากแถบเมนู XClarity Orchestrator ให้คลิก **ทรัพยากร** (⚙) ➔ **ตัวจัดการทรัพยากร** เพื่อแสดงการ์ด ตัวจัดการทรัพยากร
2. คลิกไอคอน **เชื่อมต่อ** (+) เพื่อแสดง ตัวจัดการทรัพยากร กล่องโต้ตอบ เชื่อมต่อตัวจัดการทรัพยากร



3. เลือก **XClarity Management Hub** เป็นตัวจัดการทรัพยากร
4. คัดลอกคีย์การลงทะเบียนลงในฟิลด์ **โทเค็นการลงทะเบียน**
5. คลิก **เชื่อมต่อ** เพื่อแสดงกล่องโต้ตอบ เชื่อมต่อตัวจัดการทรัพยากร ที่มีคีย์การลงทะเบียน XClarity Orchestrator
6. คลิก **คัดลอกไปยังคลิปบอร์ด** เพื่อคัดลอกคีย์การลงทะเบียน แล้วปิดกล่องโต้ตอบ

ขั้นตอนที่ 3. เพิ่มคีย์การลงทะเบียน XClarity Orchestrator ไปยังฮับการจัดการ

1. จากแถบเมนู Management Hub ให้คลิก **การลงทะเบียน** เพื่อแสดงหน้า การลงทะเบียน
2. คลิก **ติดตั้งคีย์การลงทะเบียน**
3. คัดลอกคีย์การลงทะเบียนลงในฟิลด์ **โทเค็นการลงทะเบียน**
4. คลิก **เชื่อมต่อ**

หลังจากดำเนินการเสร็จ

- จัดการอุปกรณ์โดยใช้ฮับการจัดการ (ดู การจัดการอุปกรณ์ ThinkEdge Client ใน XClarity Orchestrator เอกสารแบบออนไลน์)
- ลบคีย์การลงทะเบียนฮับการจัดการปัจจุบันโดยคลิก **รีเซ็ตการลงทะเบียน**

บทที่ 3. การถอนการติดตั้ง XClarity Management Hub สำหรับอุปกรณ์ Edge-Client

ให้ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อถอนการติดตั้งอุปกรณ์เสมือน XClarity Management Hub

ขั้นตอน

ในการถอนการติดตั้งอุปกรณ์เสมือนของ XClarity Management Hub ให้ดำเนินการตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ถอนการจัดการอุปกรณ์ทั้งหมดที่จัดการโดย XClarity Management Hub ในขณะนี้

ขั้นตอนที่ 2. ถอนการติดตั้ง XClarity Management Hub โดยขึ้นอยู่กับระบบปฏิบัติการ

- ESXi
    1. เชื่อมต่อกับโฮสต์ผ่าน VMware vSphere Client
    2. คลิกขวาที่เครื่องเสมือน และคลิก **เปิด/ปิดเครื่อง ➔ ปิดเครื่อง**
    3. คลิกขวาที่เครื่องเสมือนอีกครั้ง และเลือก **ลบออกจากดิสก์**

Lenovo