Lenovo XClarity Administrator
คู่มือการวางแผนและการติดตั้ง
สำหรับสภาพแวดล้อม Docker

เวอร์ชัน 4.0.0

หมายเหตุ

ก่อนที่จะใช้ข้อมูลนี้และผลิตภัณฑ์ที่รองรับ โปรดอ่าน คำประกาศทั่วไปและคำประกาศทางกฎหมายในเอกสารแบบออนไลน์ของ XClarity Administrator

ฉบับตีพิมพ์ครั้งที่หนึ่ง (กุมภาพันธ์ 2023)

สารบัญ

รูปภาพ

ตาราง

ข้อมูลสรุปของการเปลี่ยนแปลง

รุ่นที่ตามมาของซอฟต์แวร์การจัดการ Lenovo XClarity Administrator ให้การสนับสนุนสำหรับฮาร์ดแวร์ใหม่ การปรับปรุงซอฟต์แวร์ และการแก้ไขต่างๆ

โปรดดูข้อมูลเกี่ยวกับการแก้ไขในไฟล์ประวัติการเปลี่ยนแปลง (*.chg) ที่ให้มาในแพคเกจการอัปเดต

สำหรับข้อมูลเกี่ยวกับฮาร์ดแวร์ที่รองรับทั้งหมด (รวมทั้งเซิร์ฟเวอร์ ตัวเครื่อง และสวิตช์ Flex) ดู ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

สำหรับข้อมูลเกี่ยวกับการเปลี่ยนแปลงในรุ่นก่อนหน้า โปรดดู มีอะไรใหม่ ในเอกสารแบบออนไลน์ของ XClarity Administrator

ฮาร์ดแวร์ต่อไปนี้ได้รับการรองรับในรุ่นนี้

- **เซิร์ฟเวอร์และอุปกรณ์**
  - ThinkAgile HX630 V3 (7D6M)
  - ThinkAgile HX645 V3 (7D9M)
  - ThinkAgile HX650 V3 (7D6N)
  - ThinkAgile HX665 V3 (7D9N)
  - ThinkAgile MX630 V3 (7D6U)
  - ThinkAgile MX650 V3 (7D6S)
  - ThinkAgile VX630 V3 (7D6X, 7Z63)
  - ThinkAgile VX635 V3 (7D9V)
  - ThinkAgile VX645 V3 (7D9K)
  - ThinkAgile VX650 V2-DPU (7Z63)
  - ThinkAgile VX650 V3 (7D6W)
  - ThinkAgile VX650 V3-DPU (7D6W)
  - ThinkAgile VX655 V3 (7D9W)
  - ThinkAgile VX665 V3 (7D9L)
  - ThinkAgile VX850 V3 (7DDK)
  - ThinkEdge SE350 V2 (7DA9)
  - ThinkEdge SE455 V3 (7DBY)
  - ThinkEdge SE360 V2 (7DAM)
  - ThinkSystem SD555 V3 (7DDP, 7DDQ)

  - ThinkSystem SD650 V3 (7D7M)
  - ThinkSystem SD650-I V3 (7D7L)
  - ThinkSystem SD650-N V3(7D7L)
  - ThinkSystem SD665 V3 (7D9P)
  - ThinkSystem SD665-N V3 (7DAZ)
  - ThinkSystem SR630 V3 (7D72, 7D73, 7D74)
  - ThinkSystem SR635 V3 (7D9G, 7D9H)
  - ThinkSystem SR645 V3 (7D9C, 7D9D)
  - ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
  - ThinkSystem SR655 V3 (7D9E, 7D9F)
  - ThinkSystem SR665 V3 (7D9B, 7D9A)
  - ThinkSystem SR675 V3 (7D9Q, 7D9R)
  - ThinkSystem SR850 V3 (7D96, 7D97, 7D98)
  - ThinkSystem SR860 V3 (7D93, 7D94, 7D95)
  - ThinkSystem SR950 V3 (7DC4, 7DC5, 7DC6)
  - ThinkSystem ST650 V3 (7D7A, 7D7B)
- **อุปกรณ์จัดเก็บ**
  - แฟลชอาร์เรย์ทั้งหมด ThinkSystem DE6400F (7DB6)
  - แฟลชอาร์เรย์ไฮบริด ThinkSystem DE6400H (7DB6)
  - แฟลชอาร์เรย์ทั้งหมด ThinkSystem DE6600F (7DB7)
  - แฟลชอาร์เรย์ไฮบริด ThinkSystem DE6600H (7DB7)
- **สวิตช์**
  - สวิตช์ ThinkSystem DB730S FC SAN (7D9J)
  - ThinkSystem DB400D FC SAN Director (6684)
  - ThinkSystem DB800D FC SAN Director (6682)

เวอร์ชันนี้รองรับการวางแผนหรือการปรับปรุงการติดตั้งต่อไปนี้สำหรับซอฟต์แวร์การจัดการ

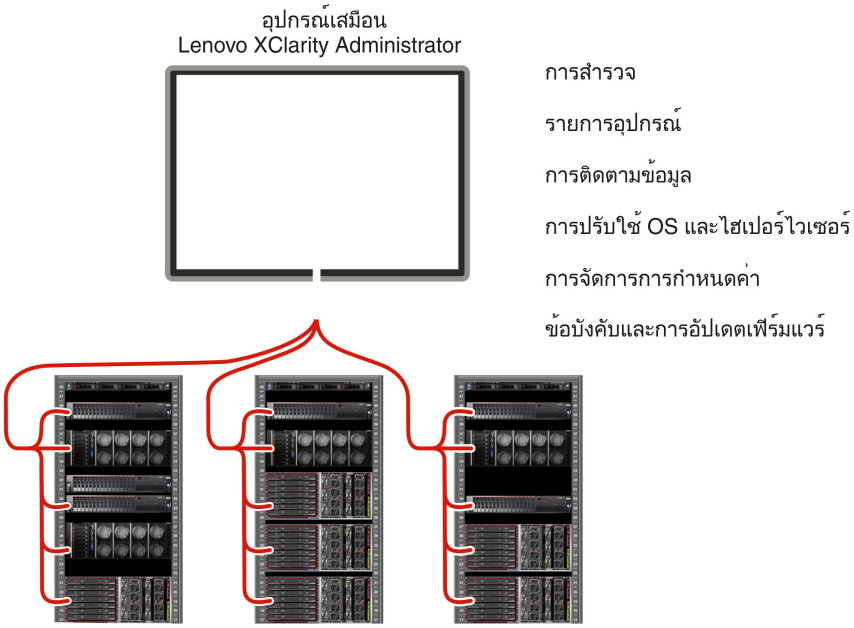
ฟังก์ชัน	**รายละเอียด**
การวางแผนและติดตั้ง	นำ ssh-rsa ออกและเพิ่ม ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 และ ecdsa-sha2-nistp521 ลงในรายการอัลกอริทึมคีย์โฮสต์ที่รองรับ (ดู การจัดการการเข้ารหัส)

บทที่ 1. Lenovo XClarity Administrator ภาพรวม

Lenovo XClarity Administrator คือโซลูชั่นการจัดการทรัพยากรแบบรวมศูนย์ที่ทำให้การจัดการโครงสร้างพื้นฐานทำได้ง่ายขึ้น การตอบสนองเร็วขึ้น และปรับปรุงความพร้อมใช้งานของระบบเซิร์ฟเวอร์และโซลูชั่นของ Lenovo® ซึ่งทำหน้าที่เป็นอุปกรณ์เสมือนที่ทำการค้นหา ดูแลรายการอุปกรณ์ ติดตาม ตรวจสอบ และเตรียมใช้งานเซิร์ฟเวอร์ เครือข่าย และฮาร์ดแวร์การจัดเก็บข้อมูลในสภาพแวดล้อมที่ปลอดภัยโดยอัตโนมัติ

เรียนรู้เพิ่มเติม:

- XClarity Administrator: การจัดการฮาร์ดแวร์เหมือนกับเป็น ซอฟต์แวร์
- XClarity Administrator: ภาพรวม



XClarity Administrator มีอินเทอร์เฟซกลางในการเรียกใช้ฟังก์ชันต่อไปนี้สำหรับอุปกรณ์ที่ได้รับการจัดการทั้งหมด

การจัดการฮาร์ดแวร์

XClarity Administrator มีการจัดการฮาร์ดแวร์โดยไม่ต้องใช้เอเจนต์ โดยสามารถค้นหาอุปกรณ์ที่ได้รับการจัดการได้โดยอัตโนมัติ รวมทั้งเซิร์ฟเวอร์ เครือข่าย และฮาร์ดแวร์การจัดเก็บข้อมูล ข้อมูลรายการอุปกรณ์จะถูกรวบรวมสำหรับอุปกรณ์ที่ได้รับการจัดการ เพื่อให้มองเห็นภาพรวมของรายการฮาร์ดแวร์ที่มีการจัดการและสถานะ

มีงานการจัดการต่างๆ สำหรับแต่ละอุปกรณ์ที่รองรับ รวมทั้งการดูสถานะและคุณสมบัติ และการกำหนดค่าการตั้งค่าระบบและเครือข่าย การเปิดใช้อินเทอร์เฟซการจัดการ การเปิดเครื่องและปิดเครื่อง และการควบคุมจากระยะไกล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการอุปกรณ์ โปรดดู การจัดการตัวเครื่อง, การจัดการเซิร์ฟเวอร์ และ การจัดการสวิตช์ ในเอกสารแบบออนไลน์ของ XClarity Administrator

เคล็ดลับ: เซิร์ฟเวอร์ เครือข่าย และฮาร์ดแวร์การจัดเก็บข้อมูลที่สามารถจัดการได้โดย XClarity Administrator เรียกว่า *อุปกรณ์* ฮาร์ดแวร์ที่อยู่ภายใต้การจัดการของ XClarity Administrator เรียกว่า *อุปกรณ์ที่ได้รับการจัดการ*

คุณสามารถใช้มุมมองแร็คใน XClarity Administrator เพื่อจัดกลุ่มอุปกรณ์ที่ได้รับการจัดการของคุณให้แสดงการติดตั้งจริงบนแร็คในศูนย์ข้อมูลของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับแร็ค โปรดดู การจัดการแร็ค ในเอกสารแบบออนไลน์ของ XClarity Administrator

เรียนรู้เพิ่มเติม:

- XClarity Administrator: การสำรวจ
- XClarity Administrator: รายการอุปกรณ์
- XClarity Administrator: การควบคุมระยะไกล

การตรวจสอบฮาร์ดแวร์

XClarity Administrator แสดงมุมมองแบบรวมศูนย์ของเหตุการณ์และการแจ้งเตือนทั้งหมด ซึ่งอุปกรณ์ที่ได้รับการจัดการสร้างขึ้น เหตุการณ์หรือการแจ้งเตือนจะถูกส่งไปยัง XClarity Administrator และแสดงในบันทึกเหตุการณ์หรือการแจ้งเตือน สรุปเหตุการณ์และการแจ้งเตือนทั้งหมดแสดงอยู่ในแดชบอร์ดและแถบสถานะ เหตุการณ์และการแจ้งเตือนสำหรับแต่ละอุปกรณ์แสดงอยู่ในหน้ารายละเอียดการแจ้งเตือนและเหตุการณ์สำหรับอุปกรณ์นั้นๆ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบฮาร์ดแวร์ โปรดดู การทำงานกับเหตุการณ์ และ การทำงานกับการแจ้งเตือน ในเอกสารแบบออนไลน์ของ XClarity Administrator

เรียนรู้เพิ่มเติม: XClarity Administrator: การตรวจสอบ

การจัดการการกำหนดค่า

คุณสามารถกำหนดเงื่อนไขและเงื่อนไขล่วงหน้าสำหรับเซิร์ฟเวอร์ทั้งหมดของคุณโดยใช้การกำหนดค่าที่สอดคล้องกัน การตั้งค่าการกำหนดค่า (เช่น อุปกรณ์การจัดเก็บข้อมูลภายใน อะแดปเตอร์ I/O การตั้งค่าการบูท เฟิร์มแวร์ พอร์ต และตัวควบคุมการจัดการ และการตั้งค่า UEFI) จะถูกบันทึกไว้ในรูปแบบเซิร์ฟเวอร์ที่สามารถนำไปใช้กับเซิร์ฟเวอร์ที่ได้รับการจัดการได้หลายเครื่อง เมื่อรูปแบบเซิร์ฟเวอร์ได้รับการอัปเดต ความเปลี่ยนแปลงที่มีจะถูกนำไปใช้กับเซิร์ฟเวอร์ที่มีการนำรูปแบบเครื่องไปใช้โดยอัตโนมัติ

รูปแบบเซิร์ฟเวอร์ยังรวมการสนับสนุนสำหรับการจำลองที่อยู่ I/O เพื่อให้คุณสามารถจำลองการเชื่อมต่อ Flex System Fabric หรือเปลี่ยนวัตถุประสงค์เซิร์ฟเวอร์โดยไม่ทำให้ฟาบริกหยุดชะงัก

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์ ดูการกำหนดค่าเซิร์ฟเวอร์โดยใช้ XClarity Administrator ในเอกสารแบบออนไลน์ของ XClarity Administrator

เรียนรู้เพิ่มเติม:

- XClarity Administrator: Bare Metal ไปยังคลัสเตอร์

- XClarity Administrator: รูปแบบการกำหนดค่า

ข้อบังคับและการอัปเดตเฟิร์มแวร์

การจัดการเฟิร์มแวร์ถูกปรับปรุงให้ง่ายขึ้นด้วยการกำหนดนโยบายด้านการปฏิบัติตามข้อบังคับเกี่ยวกับเฟิร์มแวร์ให้กับอุปกรณ์ที่ได้รับการจัดการ เมื่อคุณสร้างและกำหนดนโยบายด้านการปฏิบัติตามข้อบังคับให้กับอุปกรณ์ที่ได้รับการจัดการ XClarity Administrator จะตรวจสอบการเปลี่ยนแปลงที่มีต่อรายชื่ออุปกรณ์สำหรับอุปกรณ์เหล่านั้นและระบุอุปกรณ์ใดก็ตามที่ไม่เป็นไปตามข้อบังคับ

เมื่ออุปกรณ์ไม่เป็นไปตามข้อบังคับ คุณสามารถใช้ XClarity Administrator เพื่อใช้และเปิดใช้งานอัปเดตเฟิร์มแวร์สำหรับอุปกรณ์ทั้งหมดในอุปกรณ์นั้นจากที่เก็บข้อมูลการอัปเดตเฟิร์มแวร์ที่คุณจัดการ

หมายเหตุ: การรีเฟรชที่เก็บและการดาวน์โหลดอัปเดตเฟิร์มแวร์ต้องมีการเชื่อมต่ออินเทอร์เน็ต หาก XClarity Administrator ไม่มีการเชื่อมต่ออินเทอร์เน็ต คุณสามารถนำเข้าอัปเดตเฟิร์มแวร์ไปยังที่เก็บนั้นด้วยตนเอง

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการอัปเดตเฟิร์มแวร์ โปรดดู การอัปเดตเฟิร์มแวร์บนอุปกรณ์ที่มีการจัดการ ในเอกสารแบบออนไลน์ของ XClarity Administrator

เรียนรู้เพิ่มเติม:

- XClarity Administrator: Bare Metal ไปยังคลัสเตอร์
- XClarity Administrator: การอัปเดตเฟิร์มแวร์
- XClarity Administrator: การเตรียมใช้งานการอัปเดตด้านการรักษาความปลอดภัยของ เฟิร์มแวร์

การปรับใช้ระบบปฏิบัติการ

คุณสามารถใช้ XClarity Administrator เพื่อจัดการที่เก็บไฟล์อิมเมจระบบปฏิบัติการ และปรับใช้ไฟล์อิมเมจระบบปฏิบัติการกับเซิร์ฟเวอร์ที่ได้รับการจัดการได้สูงสุด 28 เครื่องพร้อมกัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการปรับใช้ระบบปฏิบัติการ โปรดดู การปรับใช้อิมเมจระบบปฏิบัติการ ในเอกสารแบบออนไลน์ของ XClarity Administrator

เรียนรู้เพิ่มเติม:

- XClarity Administrator: Bare Metal ไปยังคลัสเตอร์
- XClarity Administrator: การปรับใช้ระบบปฏิบัติการ

การจัดการผู้ใช้

XClarity Administrator มีเซิร์ฟเวอร์ตรวจสอบความถูกต้องแบบรวมศูนย์เพื่อสร้างและจัดการบัญชีผู้ใช้ และเพื่อจัดการและตรวจสอบความถูกต้องของข้อมูลประจำตัวผู้ใช้ เซิร์ฟเวอร์ตรวจสอบความถูกต้องถูกสร้างขึ้นโดยอัตโนมัติเมื่อคุณเริ่มต้นเซิร์ฟเวอร์การจัดการเป็นครั้งแรก บัญชีผู้ใช้ที่คุณสร้างขึ้นสำหรับ XClarity Administrator ยังสามารถใช้เข้าระบบในตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการได้ในโหมดการตรวจสอบความถูกต้องที่มีการจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับผู้ใช้ โปรดดู การจัดการบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ XClarity Administrator

XClarity Administrator รองรับเซิร์ฟเวอร์ตรวจสอบความถูกต้องสามประเภทดังนี้

- **เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายใน** ตามค่าเริ่มต้น XClarity Administrator ถูกกำหนดค่าเพื่อใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายใน ซึ่งอยู่บนโหนดการจัดการ
- **เซิร์ฟเวอร์ LDAP ภายนอก** ขณะนี้ รองรับเฉพาะ Microsoft Active Directory เซิร์ฟเวอร์เครื่องนี้จะต้องอยู่บนเซิร์ฟเวอร์ Microsoft Windows ภายนอกที่เชื่อมต่อกับเครือข่ายการจัดการเมื่อใช้เซิร์ฟเวอร์ LDAP ภายนอก จะต้องปิดใช้งานเซิร์ฟเวอร์ตรวจสอบความถูกต้องภายใน
- **SAML 2.0 ภายนอก ผู้ให้บริการข้อมูลประจำตัว** ขณะนี้ รองรับเฉพาะ Microsoft Active Directory Federation Services (AD FS) นอกจากการป้อนชื่อผู้ใช้และรหัสผ่านแล้ว ยังสามารถตั้งค่าการตรวจสอบความถูกต้องแบบหลายปัจจัยได้ เพื่อเปิดใช้งานการรักษาความปลอดภัยเพิ่มเติม โดยต้องใช้รหัส PIN การอ่านสมาร์ทการ์ด และใบรับรองไคลเอ็นต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับประเภทการตรวจสอบความถูกต้อง โปรดดู การจัดการเซิร์ฟเวอร์การตรวจสอบความถูกต้อง ในเอกสารแบบออนไลน์ของ XClarity Administrator

เมื่อคุณสร้างบัญชีผู้ใช้ คุณจะกำหนดกลุ่มบทบาทที่กำหนดไว้ล่วงหน้าหรือกำหนดเองให้กับบัญชีผู้ใช้ เพื่อควบคุมระดับการเข้าถึงผู้ใช้ดังกล่าว สำหรับข้อมูลเพิ่มเติมเกี่ยวกับกลุ่มบทบาท โปรดดู การสร้างกลุ่มบทบาท ในเอกสารแบบออนไลน์ของ XClarity Administrator

XClarity Administrator รวมบันทึกการตรวจสอบที่แสดงบันทึกประวัติการดำเนินการของผู้ใช้ เช่น การเข้าระบบ การสร้างผู้ใช้รายใหม่ หรือการเปลี่ยนรหัสผ่านของผู้ใช้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบันทึกการตรวจสอบ โปรดดู การทำงานกับเหตุการณ์ ในเอกสารแบบออนไลน์ของ XClarity Administrator

การตรวจสอบความถูกต้องอุปกรณ์

XClarity Administrator ใช้วิธีการต่อไปนี้ในการตรวจสอบความถูกต้องกับตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการ

- **การตรวจสอบความถูกต้องที่ได้รับการจัดการ** เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการ บัญชีผู้ใช้ที่คุณสร้างขึ้นใน XClarity Administrator จะถูกใช้เพื่อตรวจสอบความถูกต้องตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการ

  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับผู้ใช้ โปรดดู การจัดการบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ XClarity Administrator
- **การตรวจสอบความถูกต้องภายใน** เมื่อปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการ ข้อมูลประจำตัวที่จัดเก็บไว้ที่กำหนดไว้ใน XClarity Administrator จะถูกใช้เพื่อตรวจสอบความถูกต้องของเซิร์ฟเวอร์ที่ได้รับการจัดการ ข้อมูลประจำตัวที่จัดเก็บไว้จะต้องตรงกับบัญชีผู้ใช้ที่ใช้งานบนอุปกรณ์หรือใน Active Directory

  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับข้อมูลประจำตัวที่จัดเก็บไว้ โปรดดู การจัดการข้อมูลประจำตัวที่จัดเก็บไว้ ในเอกสารแบบออนไลน์ของ XClarity Administrator

การรักษาความปลอดภัย

หากระบบของคุณต้องสอดคล้องกับมาตรฐาน NIST SP 800-131A XClarity Administrator สามารถช่วยให้คุณได้รับระบบที่มีความสอดคล้องกันอย่างสมบูรณ์ได้

XClarity Administrator รองรับใบรับรอง SSL แบบลงนามด้วยตัวเอง (ซึ่งออกโดยหน่วยงานด้านใบรับรองภายใน) และใบรับรอง SSL ภายนอก (ซึ่งออกโดย CA เอกชนหรือเชิงพาณิชย์)

สามารถกำหนดค่าไฟร์วอลล์บนตัวเครื่องและเซิร์ฟเวอร์ให้รับคำขอที่เข้ามาจาก XClarity Administrator เท่านั้นได้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรักษาความปลอดภัย โปรดดู การใช้สภาพแวดล้อมที่ปลอดภัย ในเอกสารแบบออนไลน์ของ XClarity Administrator

การบริการและการสนับสนุน

XClarity Administrator สามารถตั้งค่าให้รวบรวมและส่งไฟล์การวินิจฉัยโดยอัตโนมัติให้กับผู้ให้บริการที่คุณต้องการเมื่อเกิดเหตุการณ์ที่สามารถให้บริการได้ใน XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ คุณสามารถเลือกที่จะส่งไฟล์การวินิจฉัยให้กับ Lenovo Support โดยใช้ Call Home หรือผู้ให้บริการรายอื่นโดยใช้ SFTP นอกจากนี้ คุณยังสามารถรวบรวมไฟล์การวินิจฉัย เปิดบันทึกปัญหา และส่งไฟล์การวินิจฉัยด้วยตนเองไปยัง Lenovo Support Center

เรียนรู้เพิ่มเติม: XClarity Administrator: การบริการและการสนับสนุน

การสร้างการทำงานอัตโนมัติโดยใช้สคริปต์

XClarity Administrator สามารถผนวกรวมกับการจัดการระดับสูงจากภายนอกและแพลตฟอร์มระบบอัตโนมัติ โดยผ่านอินเทอร์เฟซการโปรแกรมแอปพลิเคชัน (APIs) REST ที่เปิดอยู่ สามารถใช้ REST API XClarity Administrator เพื่อบูรณาการกับโครงสร้างพื้นฐานการจัดการที่มีอยู่ของคุณ

ชุดเครื่องมือ PowerShell ให้ไลบรารี cmdlet เพื่อสร้างการทำงานอัตโนมัติสำหรับการเตรียมใช้งานและการจัดการทรัพยากรจากเซสชัน Microsoft PowerShell ชุดเครื่องมือ Python มีไลบรารีที่ใช้ Python สำหรับคำสั่งและ API เพื่อสร้างการทำงานอัตโนมัติสำหรับการเตรียมใช้งานและการจัดการทรัพยากรจากระบบที่ใช้ OpenStack เช่น Ansible หรือ Puppet ชุดเครื่องมือทั้งสองชุดนี้มีอินเทอร์เฟซที่ใช้ร่วมกับ REST API ของ XClarity Administrator เพื่อให้ฟังก์ชันต่างๆ ทำงานแบบอัตโนมัติ เช่น

- การเข้าสู่ระบบ XClarity Administrator
- การจัดการและการถอนการจัดการตัวเครื่อง เซิร์ฟเวอร์ อุปกรณ์การจัดเก็บข้อมูล และสวิตช์บนสุดของแร็ค (อุปกรณ์)
- การรวบรวมและการดูข้อมูลรายการอุปกรณ์สำหรับอุปกรณ์และส่วนประกอบต่างๆ
- การปรับใช้ไฟล์อิมเมจระบบปฏิบัติการกับเซิร์ฟเวอร์หนึ่งหรือหลายเครื่อง
- การกำหนดค่าเซิร์ฟเวอร์ผ่านการใช้รูปแบบการกำหนดค่า

- การนำอัปเดตเฟิร์มแวร์ไปใช้กับอุปกรณ์

การบูรณาการกับซอฟต์แวร์ที่ได้รับการจัดการอื่น ๆ

โมดูล XClarity Administrator ผสานรวม XClarity Administrator กับซอฟต์แวร์การจัดการของบุคคลที่สามเพื่อให้ฟังก์ชันในการค้นหา การตรวจสอบ การกำหนดค่า และการจัดการ เพื่อลดต้นทุนและความซับซ้อนของการดูแลระบบเป็นประจำสำหรับอุปกรณ์ที่รองรับ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ XClarity Administrator ดูเอกสารต่อไปนี้

- Lenovo XClarity Integrator สำหรับ Microsoft System Center
- Lenovo XClarity Integrator สำหรับ VMware vCenter

สำหรับข้อควรพิจารณาเพิ่มเติม ดู ข้อควรพิจารณาด้านการจัดการ

เรียนรู้เพิ่มเติม:

- Lenovo XClarity Integrator สำหรับภาพรวม Microsoft System Center
- Lenovo XClarity Integrator สำหรับ VMware vCenter

เอกสารคู่มือ

เอกสาร XClarity Administrator ได้รับการอัปเดตทางออนไลน์ในภาษาอังกฤษเป็นประจำ ดู เอกสารแบบออนไลน์ของ XClarity Administrator สำหรับข้อมูลและขั้นตอนล่าสุด

เอกสารแบบออนไลน์มีในภาษาดังต่อไปนี้:

- ภาษาเยอรมัน (de)
- ภาษาอังกฤษ (en)
- ภาษาสเปน (es)
- ภาษาฝรั่งเศส (fr)
- ภาษาอิตาลี (it)
- ภาษาญี่ปุ่น (ja)
- ภาษาเกาหลี (ko)
- ภาษาโปรตุเกสบราซิล (pt_BR)
- ภาษารัสเซีย (ru)
- ภาษาไทย (th)
- ภาษาจีนตัวย่อ (zh_CN)
- ภาษาจีนตัวเต็ม (zh_TW)

คุณสามารถเปลี่ยนภาษาของเอกสารแบบออนไลน์ได้ด้วยวิธีต่อไปนี้:

- เปลี่ยนการตั้งค่าภาษาในเว็บเบราเซอร์

- ต่อท้าย URL ด้วย **?lang=*<language_code>*** ตัวอย่างเช่น ในการแสดงเอกสารแบบออนไลน์เป็นภาษาจีนตัวย่อ:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**`?lang=zh_CN`**

บทที่ 2. การวางแผนสำหรับ XClarity Administrator

ก่อนการติดตั้ง Lenovo XClarity Administrator ให้ตรวจสอบข้อควรพิจารณาต่อไปนี้เพื่อช่วยคุณวางแผนสำหรับการติดตั้งและการจัดการประจำวัน

สิทธิ์การใช้งานและการทดลองใช้ฟรี 90 วัน

Lenovo XClarity Administrator ให้สิทธิ์ทดลองใช้ฟรี 90 วัน ที่ให้คุณสามารถใช้คุณลักษณะที่มีอยู่ทั้งหมดได้ในช่วงระยะเวลาจำกัด

คุณสามารถดูสถานะสิทธิ์การใช้งาน รวมถึงจำนวนวันที่เหลือของสิทธิ์การใช้งานเวอร์ชันทดลองใช้ได้โดยคลิกเมนูการดำเนินการของผู้ใช้ (

) บนแถบชื่อเรื่อง XClarity Administrator แล้วคลิก **เกี่ยวกับ**

XClarity Administrator รองรับสิทธิ์การใช้งานต่อไปนี้

- **Lenovo XClarity Pro** สิทธิ์การใช้งานแต่ละอันมีใบอนุญาตดังต่อไปนี้สำหรับอุปกรณ์ตัวเดียว
  - บริการและการสนับสนุนสำหรับ Lenovo XClarity Integrator
  - บริการและการสนับสนุนสำหรับ XClarity Administrator
  - ฟังก์ชันขั้นสูงภายใน XClarity Administrator:
    - การกำหนดค่าเซิร์ฟเวอร์โดยใช้รูปแบบการกำหนดค่า
    - การปรับใช้ระบบปฏิบัติการ
    - การรายงานปัญหาเกี่ยวกับ XClarity Administrator โดยใช้ Call Home (Call Home สำหรับการแจ้งเตือนฮาร์ดแวร์จะไม่ได้รับผลกระทบ)

คุณต้องซื้อสิทธิ์การใช้งานสำหรับอุปกรณ์ที่ได้รับการจัดการแต่ละเครื่องที่รองรับฟังก์ชันขั้นสูง สิทธิ์การใช้งานไม่ได้ผูกกับอุปกรณ์เฉพาะเครื่อง

การปฏิบัติตามข้อกำหนดของสิทธิ์การใช้งานขึ้นอยู่กับจำนวนของอุปกรณ์ที่ได้รับการจัดการที่รองรับฟังก์ชันขั้นสูง จำนวนอุปกรณ์ที่ได้รับการจัดการต้องไม่เกินจำนวนสิทธิ์การใช้งานทั้งหมดในคีย์สิทธิ์การใช้งานที่ใช้งานอยู่ทั้งหมด หาก XClarity Administrator ไม่สอดคล้องกับสิทธิ์การใช้งานที่ติดตั้ง (ตัวอย่างเช่น หากสิทธิ์การใช้งานหมดอายุหรือหากจัดการอุปกรณ์เพิ่มเติมจนจำนวนเกินจำนวนสิทธิ์การใช้งานที่ใช้งานอยู่ทั้งหมด) คุณมีระยะเวลาผ่อนผัน 90 วันเพื่อติดตั้งสิทธิ์การใช้งานที่เหมาะสม ในแต่ละครั้งที่ XClarity Administrator ไม่เป็นไปตามข้อบังคับ ระยะเวลาผ่อนผันจะรีเซ็ตเป็น 90 วัน หากระยะปลอดหนี้ (รวมถึงการทดลองใช้ฟรี) สิ้นสุดก่อนที่สิทธิ์การใช้งานจะเป็นไปตามข้อกำหนด ฟังก์ชันขั้นสูงจะปิดใช้งานสำหรับอุปกรณ์ทั้งหมด

หมายเหตุ:

- การกำหนดค่าเซิร์ฟเวอร์และคุณลักษณะการปรับใช้ระบบปฏิบัติการจะถูกปิดใช้งานเมื่อหมดระยะเวลาผ่อนผัน
- Call Home สำหรับปัญหาเกี่ยวกับ XClarity Administrator (คุณลักษณะ Call Home ของซอฟต์แวร์) จะปิดใช้งานเมื่อสิทธิ์การใช้งานไม่เป็นไปตามข้อกำหนด ไม่มีระยะเวลาผ่อนผันสำหรับคุณลักษณะนี้ แต่ Call Home สำหรับการแจ้งเตือนฮาร์ดแวร์ไม่ได้รับผลกระทบ

หากมีการติดตั้งสิทธิ์การใช้งานอยู่แล้ว *ไม่*จำเป็นต้องใช้สิทธิ์การใช้งานสิทธิ์ใหม่เมื่อทำการอัปเกรดเป็นXClarity Administratorเวอร์ชันใหม่

สำหรับข้อมูลเกี่ยวกับการซื้อสิทธิ์การใช้งาน Lenovo XClarity Pro โปรดติดต่อตัวแทนจำหน่ายหรือคู่ค้าธุรกิจที่ได้รับอนุญาตของ Lenovo

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการติดตั้งใบอนุญาต โปรดดู การติดตั้งใบอนุญาตการเปิดใช้งานเต็มรูปแบบ ในเอกสารแบบออนไลน์ของ XClarity Administrator

---

ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

อุปกรณ์การจัดการ Lenovo XClarity Administrator ทำงานในเครื่องเสมือนบนระบบโฮสต์

ข้อกำหนดสำหรับไฮเปอร์ไวเซอร์

สภาพแวดล้อมคอนเทนเนอร์

รองรับสภาพแวดล้อมคอนเทนเนอร์ต่อไปนี้ในการใช้ XClarity Administrator เป็นคอนเทนเนอร์

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

ไฮเปอร์ไวเซอร์

รองรับไฮเปอร์ไวเซอร์ต่อไปนี้ในการใช้ XClarity Administrator เป็นอุปกรณ์เสมือน

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 7 และ 8[1]
- Microsoft Windows Server 2022 ที่ติดตั้ง Hyper-V
- Microsoft Windows Server 2019 ที่ติดตั้ง Hyper-V
- Microsoft Windows Server 2016 ที่ติดตั้ง Hyper-V
- Microsoft Windows Server 2012 R2 ที่ติดตั้ง Hyper-V

- Microsoft Windows Server 2012 ที่ติดตั้ง Hyper-V
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat v8.x ที่ติดตั้งเครื่องเสมือนที่ใช้ kernel (KVM) v2.12.0
- Red Hat v7.x ที่ติดตั้ง KVM v1.2.17
- Ubuntu 20.04.2 LTS ที่มีการติดตั้ง KVM v4.2.3
- VMware ESXi 7.0, U1, U2 และ U3
- VMware ESXi 6.7, U1, U2[2] และ U3

หมายเหตุ:

1. CentOS Linux ไม่ได้อัปเดตโดย Red Hat อีกต่อไป ลองย้ายไปใช้ Red Hat Enterprise Linux แทน (ดู Red Hat: วิธีการแปลงจากเว็บเพจ LCentOS หรือ Oracle Linux เป็นเว็บเพจ RHEL)
2. สำหรับ VMware ESXi 6.7 U2 คุณต้องใช้อิมเมจ ISO ของ VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso หรือใหม่กว่า

สำหรับ VMware และ Citrix สามารถใช้เครื่องเสมือนเป็นเทมเพลต OVF ได้ สำหรับ Hyper-V และ Nutanix AHV เครื่องเสมือนคืออิมเมจดิสก์เสมือน (VHD) สำหรับ CentOS และ KVM เครื่องเสมือนใช้งานได้โดยเป็นรูปแบบ qcow2

ข้อสำคัญ: สำหรับระบบ Hyper-V ที่ทำงานบนเกสต์ Linux ที่มีฐานเคอร์เนล 2.6 และใช้หน่วยความจำในปริมาณสูงสำหรับอุปกรณ์เสมือน คุณต้องปิดใช้งานการเข้าถึงหน่วยความจำในรูปแบบไม่เหมือนกัน (NUMA) บนแผงการตั้งค่า Hyper-V จากโปรแกรมจัดการ Hyper-V การเปลี่ยนการตั้งค่าดังกล่าวกำหนดให้คุณต้องรีสตาร์ทบริการ Hyper-V ซึ่งจะรีสตาร์ทเครื่องเสมือนที่กำลังทำงานทั้งหมดอีกด้วย หากไม่ได้ปิดใช้งานการตั้งค่านี้ อุปกรณ์เสมือน XClarity Administrator อาจประสบปัญหาระหว่างการเริ่มทำงานครั้งแรก

ข้อกำหนดด้านฮาร์ดแวร์

XClarity Administrator จะต้องเป็นไปตาม*ข้อกำหนดขั้นต่ำ*ดังต่อไปนี้ อาจต้องมีทรัพยากรเพิ่มเติมเพื่อให้ได้รับประสิทธิภาพที่เหมาะสม ขึ้นอยู่กับขนาดของระบบของคุณและการใช้ รูปแบบการกำหนดค่า ของคุณ

- ไมโครโปรเซสเซอร์เสมือนสองตัว
- หน่วยความจำ 8 GB
- ที่จัดเก็บข้อมูล 192 GB เพื่อการใช้งานโดยอุปกรณ์เสมือน XClarity Administrator
- แสดงความละเอียดต่ำสุดกว้าง 1024 พิกเซล (XGA)

ตารางต่อไปนี้แสดงรายการการกำหนดค่าที่แนะนำขั้นต่ำตามจำนวนอุปกรณ์ โปรดทราบว่าหากคุณรันโดยใช้การกำหนดค่าต่ำสุด เวลาการดำเนินการสิ้นสุดที่คาดการณ์ไว้สำหรับงานการจัดการอาจนานขึ้น สำหรับงานการเตรียมใช้งาน เช่น การปรับใช้ระบบปฏิบัติการ การอัปเดตเฟิร์มแวร์และการกำหนดค่าเซิร์ฟเวอร์ คุณอาจจำเป็นต้องเพิ่มทรัพยากรชั่วคราว

จำนวนอุปกรณ์ที่มีการจัดการ	การกำหนดค่า CPU/หน่วยความจำเสมือน
0 - 100 อุปกรณ์	2 vCPU, 8 GB RAM
100 - 200 อุปกรณ์	4 vCPU, 10 GB RAM
200 - 400 อุปกรณ์	6 vCPU, 12 GB RAM
400 - 600 อุปกรณ์	8 vCPU, 16 GB RAM
600 - 800 อุปกรณ์	10 vCPU, 20 GB RAM
800 - 1,000 อุปกรณ์	12 vCPU, 24 GB RAM

หมายเหตุ:

- อินสแตนซ์ XClarity Administrator เดียวสามารถรองรับอุปกรณ์ได้สูงสุด 1,000 เครื่อง
- สำหรับคำแนะนำล่าสุดและข้อควรพิจารณะด้านประสิทธิภาพเพิ่มเติม โปรดดู XClarity Administrator: คู่มือประสิทธิภาพ (เอกสาร วิชาการ)
- คุณอาจต้องเพิ่มทรัพยากรเพื่อรักษาประสิทธิภาพในระดับที่ยอมรับได้ ทั้งนี้ขึ้นอยู่กับขนาดของสภาพแวดล้อมที่ได้รับการจัดการและรูปแบบการใช้งานในการติดตั้งของคุณ หากคุณเห็นการใช้งานโปรเซสเซอร์ในแดชบอร์ดทรัพยากรระบบแสดงค่าสูงหรือสูงมาก ให้พิจารณาเพิ่มแกนโปรเซสเซอร์เสมือน 1-2 ตัว หากการใช้หน่วยความจำคงอยู่ที่ 80% ขณะว่าง ให้พิจารณาเพิ่ม RAM 1-2 GB หากระบบไม่ตอบสนองการกำหนดค่าที่กำหนดไว้ในตาราง ให้พิจารณาการรัน VM เป็นระยะเวลายาวนานขึ้นเพื่อประเมินประสิทธิภาพของระบบ
- สำหรับข้อมูลเกี่ยวกับวิธีการเพิ่มพื้นที่ดิสก์โดยการลบทรัพยากร XClarity Administrator ที่ไม่ได้ใช้งานอีกต่อไป ดู การจัดการพื้นที่ดิสก์ ในเอกสารแบบออนไลน์ของ XClarity Administrator

ข้อกำหนดด้านซอฟต์แวร์

- **เซิร์ฟเวอร์** Orchestrator

  หากคุณจัดการอุปกรณ์จำนวนมากโดยใช้ XClarity Administrator หลายอินสแตนซ์ คุณสามารถทำการตรวจสอบการจัดการ การเตรียมใช้งาน และการวิเคราะห์ได้จากส่วนกลางโดยใช้ Lenovo XClarity OrchestratorXClarity Orchestrator สามารถรองอินสแตนซ์ XClarity Administrator ได้โดยไม่จำกัดจำนวน ซึ่งจัดการอุปกรณ์ที่ไม่ใช่ ThinkEdge Client จำนวนสูงสุด 10,000 เครื่องพร้อมกัน

  หากต้องการจัดการอินสแตนซ์ XClarity Administrator v4.0 หรือใหม่กว่าโดยใช้ Lenovo XClarity Orchestrator จะต้องใช้ XClarity Orchestrator v2.0 หรือใหม่กว่า

- **เซิร์ฟเวอร์ตรวจสอบความถูกต้อง**

  หากคุณเลือกที่จะใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายนอก รองรับเฉพาะ Microsoft Active Directory ที่ทำงานบน Windows Server 2008 ขึ้นไปเท่านั้น

หากคุณเลือกที่จะใช้ผู้ให้บริการข้อมูลประจำตัว SAML รองรับเฉพาะ Microsoft Active Directory Federation Services (AD FS) เวอร์ชัน 2.0 ขึ้นไปที่ทำงานบน Windows Server 2012 เท่านั้น

- **เซิร์ฟเวอร์** NTP

  ต้องใช้เซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย (NTP) เพื่อตรวจสอบให้แน่ใจว่าเวลาประทับสำหรับเหตุการณ์และการแจ้งเตือนทั้งหมดที่ได้รับจากอุปกรณ์ที่ได้รับการจัดการถูกปรับให้ตรงกับ XClarity Administrator ตรวจสอบให้แน่ใจว่าสามารถเข้าถึงเซิร์ฟเวอร์ NTP ได้บนเครือข่ายการจัดการ (ปกติบนอินเทอร์เฟซ Eth0)

  เคล็ดลับ: พิจารณาใช้ระบบโฮสต์ที่ติดตั้ง XClarity Administrator เป็นเซิร์ฟเวอร์ NTP หากคุณดำเนินการเช่นนั้น ตรวจสอบให้แน่ใจว่าระบบโฮสต์เข้าถึงได้บนเครือข่ายการจัดการ

ทรัพยากรที่สามารถจัดการได้

อินสแตนซ์ XClarity Administrator เดี่ยวสามารถจัดการ ตรวจสอบ และเตรียมใช้งานอุปกรณ์จริงได้สูงสุด 1,000 เครื่อง

คุณสามารถค้นหารายการอุปกรณ์และตัวเลือกที่รองรับทั้งหมด (เช่น I/O, DIMM และอะแดปเตอร์ที่จัดเก็บ) ระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำ และข้อควรพิจารณาเกี่ยวกับข้อจำกัดต่างๆ ได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกที่แท็บ **ความเข้ากันได้** แล้วคลิกลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

สำหรับข้อมูลทั่วไปเกี่ยวกับการกำหนดค่าและตัวเลือกฮาร์ดแวร์สำหรับอุปกรณ์ที่ระบุ โปรดดู เว็บเพจ Lenovo Server Proven

ข้อจำกัด: หากระบบโฮสต์ที่ติดตั้ง XClarity Administrator เป็นแร็คเซิร์ฟเวอร์หรือโหนดคอมพิวท์ที่มีการจัดการ คุณจะไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับระบบโฮสต์ดังกล่าวหรือตัวเครื่องทั้งหมดในเวลาเดียวกัน เมื่อใช้การอัปเดตเฟิร์มแวร์กับระบบโฮสต์ จะต้องรีสตาร์ทโฮสต์อัปเดต การรีสตาร์ทระบบโฮสต์จะรีสตาร์ท XClarity Administrator ด้วย ทำให้ XClarity Administrator ใช้งานไม่ได้ เพื่อทำการอัปเดตบนระบบโฮสต์

เว็บเบราเซอร์ที่รองรับ

เว็บอินเทอร์เฟซ XClarity Administrator จะทำงานกับเว็บเบราเซอร์ต่อไปนี้

- Chrome™ 48.0 หรือใหม่กว่า (55.0 หรือสูงกว่าสำหรับคอนโซลระยะไกล)
- Firefox® ESR 38.6.0 หรือใหม่กว่า
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 หรือใหม่กว่า (IOS7 หรือใหม่กว่าและ OS X)

ไฟร์วอลและเซิร์ฟเวอร์พร็อกซี

บางฟังก์ชันของLenovo XClarity Administrator รวมถึงการอัปเดตเซิร์ฟเวอร์การจัดการ การอัปเดตเฟิร์มแวร์ บริการและการสนับสนุน ต้องใช้การเข้าถึงอินเทอร์เน็ต หากคุณมีไฟร์วอลล์ในเครือข่าย ให้กำหนดค่าไฟร์วอลล์เพื่อเปิดใช้งาน

XClarity Administrator ให้เซิร์ฟเวอร์การจัดการสามารถดำเนินการเหล่านี้ได้ หากเซิร์ฟเวอร์การจัดการไม่สามารถเข้าถึงอินเทอร์เน็ตได้โดยตรง ให้กำหนดค่าXClarity Administrator ให้ใช้เซิร์ฟเวอร์พร็อกซี

ไฟร์วอลล์

ตรวจดูว่าชื่อ DNS และพอร์ตต่อไปนี้เปิดอยู่บนไฟร์วอลล์

หมายเหตุ: ที่อยู่ IP อาจมีการเปลี่ยนแปลง ใช้ชื่อ DNS หากเป็นไปได้

ตาราง 1. จำเป็นต้องมีการเชื่อมต่ออินเทอร์เน็ต

ชื่อ DNS	**ที่อยู่** IPv4	**ที่อยู่** IPv6	**พอร์ต**	**โปรโตคอล**
ดาวน์โหลดคีย์เปิดใช้งานสิทธิ์การใช้งาน				
fod.lenovo.com	ไม่ระบุ	ไม่ระบุ	443	https
ดาวน์โหลดข่าวสารด้านบริการ				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
ดาวน์โหลดอัปเดตต่างๆ (เซิร์ฟเวอร์การจัดการ อัปเดตเฟิร์มแวร์ UpdateXpress System Packs (ไดรเวอร์อุปกรณ์ของ OS) และแพคที่เก็บข้อมูล)				
datacentersupport.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
download.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
filedownload.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
support.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https และ http
supportapi.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
ดาวน์โหลดเฟิร์มแวร์ (Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, บางสวิตช์ Flex และ CMM รุ่นแรกเท่านั้น)				

ตาราง 1. จำเป็นต้องมีการเชื่อมต่ออินเทอร์เน็ต (มีต่อ)

ชื่อ DNS	**ที่อยู่** IPv4	**ที่อยู่** IPv6	**พอร์ต**	**โปรโตคอล**
www.ibm.com	129.42.56.21-6, 129.42.58.21-6, 129.42.60.21-6, 129.42.160.5-1, 207.25.252.1-97	ไม่ระบุ	443 และ 80	https และ http
www-03.ibm.com	204.146.30.17	ไม่ระบุ	443 และ 80	https และ http
download3.boulder.ibm.com	170.225.126.-24	ไม่ระบุ	443	https
download4.boulder.ibm.com	170.225.126.-43	ไม่ระบุ	443 และ 80	https และ http
delivery04-bld.dhe.ibm.com	170.225.126.-45	ไม่ระบุ	443 และ 80	https และ http
delivery04-mul.dhe.ibm.com	170.225.126.-46	ไม่ระบุ	443 และ 80	https และ http
delivery04.dhe.ibm.com	170.225.126.-44	ไม่ระบุ	443 และ 80	https และ http
อัปโหลดข้อมูลบริการไปยังฝ่ายสนับสนุนของ Lenovo (Call Home)				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	ไม่ระบุ	443	https
logupload.lenovo.com/BLL/Logupload.ashx	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
อัปโหลดข้อมูลบริการไปยังการอำนวยการอัปเดต Lenovo				

ตาราง 1. จำเป็นต้องมีการเชื่อมต่ออินเทอร์เน็ต (มีต่อ)

ชื่อ DNS	ที่อยู่ IPv4	ที่อยู่ IPv6	พอร์ต	โปรโตคอล
logupload.lenovo.com/BLL/Logupload.ashx	ไม่ระบุ	ไม่ระบุ	443 และ 80	https
ดาวน์โหลดข้อมูลการรับประกัน				
ibase.lenovo.com (ทั่วโลก)	ไม่ระบุ	ไม่ระบุ	443 และ 80	https และ http
service.lenovo.com.cn (เฉพาะประเทศจีน)	114.247.140.-212 (เฉพาะประเทศจีน)	ไม่ระบุ	83	http
supportapi.lenovo.com	ไม่ระบุ	ไม่ระบุ	443 และ 80	https และ http

ข้อควรพิจารณา: สำหรับการรับข้อมูลการรับประกันของอุปกรณ์ที่มีการจัดการโดยใช้ XClarity Administrator ของผู้ใช้ในประเทศจีน คุณต้องอัปเกรดเป็น XClarity Administrator v1.3.1 ขึ้นไป

เซิร์ฟเวอร์พร็อกซี

หากเซิร์ฟเวอร์การจัดการไม่สามารถเข้าถึงอินเทอร์เน็ตได้โดยตรง ให้ตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์การจัดการได้กำหนดค่าให้ใช้เซิร์ฟเวอร์พร็อกซี HTTP หรือไม่ (โปรดดู การกำหนดค่าการเข้าถึงเครือข่าย)

- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีให้ใช้การการตรวจสอบความถูกต้องพื้นฐาน
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีที่ไม่สิ้นสุด
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีส่งต่อ
- ตรวจสอบให้แน่ใจว่ามีการกำหนดค่าให้โหลดบาลานเซอร์เก็บเซสชันไว้กับเซิร์ฟเวอร์พร็อกซีหนึ่งตัว และไม่มีการสลับไปมา

ความพร้อมใช้งานของพอร์ต

อาจมีหลายพอร์ตพร้อมใช้งาน ทั้งนี้ขึ้นอยู่กับวิธีใช้งานไฟร์วอลล์ในสภาพแวดล้อมของคุณ หากพอร์ตที่ต้องการถูกบล็อกหรือกระบวนการอื่นใช้พอร์ตนั้นอยู่ ฟังก์ชัน Lenovo XClarity Administrator บางอย่างอาจไม่ทำงาน

ในการระบุพอร์ตที่ต้องเปิดตามสภาพแวดล้อมของคุณ ให้ตรวจดูส่วนต่อไปนี้ ตารางในส่วนต่อไปนี้ประกอบด้วยข้อมูลเกี่ยวกับการใช้งานพอร์ตแต่ละพอร์ตใน XClarity Administrator อุปกรณ์ที่ได้รับการจัดการที่ได้รับผลกระทบ โปรโตคอล (TCP หรือ UDP) และทิศทางโฟลว์การรับส่งข้อมูล การรับส่งข้อมูล*ขาเข้า*จะกำหนดลำดับการส่งต่อจากอุปกรณ์ที่ได้รับ

การจัดการหรือระบบภายนอกไปยัง XClarity Administrator ดังนั้น พอร์ตบนอุปกรณ์ XClarity Administrator จะต้องเปิด โฟลว์การรับส่งข้อมูล*ขาออก*จาก XClarity Administrator ไปยังอุปกรณ์ที่ได้รับการจัดการ

- เข้าถึงเซิร์ฟเวอร์ XClarity Administrator
- การเข้าถึงระหว่าง XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ
- การเข้าถึงระหว่าง XClarity Administrator และเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์

เข้าถึงเซิร์ฟเวอร์ XClarity Administrator

หากเซิร์ฟเวอร์ XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการทั้งหมดอยู่หลังไฟร์วอลล์ และคุณต้องการเข้าถึงอุปกรณ์เหล่านั้นจากเบราเซอร์ที่อยู่นอกไฟร์วอลล์ คุณต้องตรวจสอบว่าพอร์ต XClarity Administrator เปิดอยู่ หากคุณกำลังใช้ SNMP และ SMTP สำหรับการจัดการเหตุการณ์ คุณอาจต้องตรวจสอบให้แน่ใจว่าพอร์ตที่ใช้โดยเซิร์ฟเวอร์ XClarity Administrator สำหรับการส่งต่อเหตุการณ์เปิดอยู่

เซิร์ฟเวอร์ XClarity Administrator จะรับข้อมูลและตอบสนองผ่านพอร์ตที่แสดงในตารางต่อไปนี้

หมายเหตุ:

- XClarity Administrator เป็นแอปพลิเคชัน RESTful ที่สื่อสารอย่างปลอดภัยผ่าน TCP บนพอร์ต 443
- XClarity Administrator สามารถเลือกที่จะได้รับการกำหนดค่าเพื่อทำการเชื่อมต่อขาออกกับบริการภายนอกได้ เช่น LDAP, SMTP หรือ syslog การเชื่อมต่อเหล่านี้อาจต้องการพอร์ตเพิ่มเติมที่มักจะกำหนดค่าโดยผู้ใช้ได้และไม่ได้รวมอยู่ในรายการนี้ นอกจากนี้การเชื่อมต่อเหล่านี้ยังอาจต้องการการเข้าถึงเซิร์ฟเวอร์บริการชื่อโดเมน (DNS) บน TCP หรือ UDP พอร์ต 53 เพื่อแก้ไขปัญหาเรื่องชื่อเซิร์ฟเวอร์ภายนอก

การสื่อสาร	อุปกรณ์ XClarity Administrator	เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายนอก	บริการส่งต่อเหตุการณ์	Lenovo Services (รวมถึง Call Home)
ขาออก (พอร์ตเปิดบนระบบภายนอก)	• DNS – TCP/UDP บนพอร์ต 53	• LDAP– TCP บนพอร์ต 389[1] • LDAPS – TCP บนพอร์ต 636 • การตรวจสอบความถูกต้องของ SAML – TCP บนพอร์ต 3268, 3269	• เซิร์ฟเวอร์ FTP – TCP บนพอร์ต 21[1] • เซิร์ฟเวอร์อีเมล (SMTP) – UDP บนพอร์ต 25[1] • บริการเว็บ REST (HTTP) – UDP บนพอร์ต 80[1] • ตัวจัดการ SNMP – UDP บนพอร์ต 161[2], 162[1] • MS Azure – UDP บนพอร์ต 443[1] • Syslog – UDP บนพอร์ต 514[1] • พุช Apple[3] – TCP บนพอร์ต 443, 2195, 5223 • พุช Google[4] – TCP บนพอร์ต 443, 5288, 5299, 5230	• การรับประกัน (เฉพาะประเทศจีน) – TCP บนพอร์ต 83[5] • HTTPS (Call Home) – TCP บนพอร์ต 443
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	• HTTPS – TCP บนพอร์ต 443	ไม่สามารถใช้ได้	• SNMP – UDP บนพอร์ต 161	ไม่สามารถใช้ได้

1. นี่คือพอร์ตเริ่มต้น คุณสามารถกำหนดค่าพอร์ตนี้ได้จากอินเทอร์เฟซผู้ใช้
2. ใช้พอร์ตนี้เมื่อมีการกำหนดค่าการส่งต่อเหตุการณ์ SNMP ที่มีการตรวจสอบความถูกต้องของผู้ใช้
3. เปิดพอร์ตนี้เมื่อ Wi-Fi อยู่ด้านหลังไฟร์วอลล์หรือชื่อจุดเข้าใช้งานส่วนตัว (APN) สำหรับข้อมูลเซลลูลาร์ จำเป็นต้องใช้การเชื่อมต่อโดยตรงแบบ unproxied กับเซิร์ฟเวอร์ APN บนพอร์ตนี้ พอร์ตนี้ใช้เป็นการย้อนโหนดเมื่อเกิด

ข้อผิดพลาดบน Wi-Fi เท่านั้น เมื่ออุปกรณ์ไม่สามารถเข้าถึงบริการการแจ้งเตือนแบบพุชของ Apple บนพอร์ต 5223 ช่วงที่อยู่ IP คือ 17.0.0.0/8

4. สำหรับช่วงที่อยู่ IP โปรดดู Google ASN 15169 โดเมน android.googleapis.com
5. แม้ว่าไม่จำเป็นสำหรับประเทศอื่นๆ นอกเหนือจากประเทศจีน แต่ XClarity Administrator อาจพยายามเชื่อมต่อกับบริการนี้ในประเทศอื่นๆ

การเข้าถึงระหว่าง XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ

หากอุปกรณ์ที่ได้รับการจัดการ (เช่น โหนดคอมพิวท์ หรือเซิร์ฟเวอร์ในแร็ค) อยู่หลังไฟร์วอลล์ และหากคุณต้องการจัดการอุปกรณ์เหล่านั้นจากเซิร์ฟเวอร์ XClarity Administrator ที่อยู่นอกไฟร์วอลล์ คุณต้องตรวจสอบว่าพอร์ตทั้งหมดที่เกี่ยวข้องกับการสื่อสารระหว่าง XClarity Administrator และตัวควบคุมการจัดการแผงวงจรในแต่ละอุปกรณ์ที่ได้รับการจัดการเปิดอยู่

หากคุณต้องการติดตั้งระบบปฏิบัติการบนอุปกรณ์ที่ได้รับการจัดการโดยใช้ XClarity Administrator อย่าลืมตรวจดูรายการพอร์ตใน การเข้าถึงระหว่าง XClarity Administrator และเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์

- **CMM ของตัวเครื่องแบบ Flex**

การสื่อสาร	**CMM ของตัวเครื่องแบบ Flex**
ขาออก (พอร์ตเปิดบนระบบภายนอก)	– SLP – UDP/TCP บนพอร์ต **427** – CIM HTTP – TCP บนพอร์ต **5988**[2] – CIM HTTPS – TCP บนพอร์ต **5989** – คำสั่ง TCP – TCP บนพอร์ต **6090**[2] – คำสั่ง TCP แบบปลอดภัย – TCP บนพอร์ต **6091**
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	– SFTP – TCP บนพอร์ต **22**[1] – ตัวชี้วัด CIM HTTPS – TCP **9090** – LDAPS – TCP บนพอร์ต **50637**

1. พอร์ตนี้ใช้ในการถ่ายโอนการอัปเดตเฟิร์มแวร์โดยใช้ SFTP
2. ตามค่าเริ่มต้น การจัดการจะทำผ่านพอร์ตที่มีความปลอดภัย พอร์ตที่ไม่ปลอดภัยเป็นตัวเลือกเสริม

- **เซิร์ฟเวอร์และโหนดคอมพิวท์**

การสื่อสาร	ThinkSystem และ ThinkAgile	System x	Flex System	ThinkServer
ขาออก (พอร์ตเปิดบนระบบภายนอก)	– SFTP – TCP บนพอร์ต 115 – SLP – UDP/TCP บนพอร์ต 427 – HTTPS – TCP บนพอร์ต 443 – การค้นหา SSDP – UDP บนพอร์ต 1900 – การควบคุมระยะไกล – TCP บนพอร์ต 3888[4] – KVM ระยะไกล – TCP บนพอร์ต 3889[4] – CIM HTTPS – TCP บนพอร์ต 5989 – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต 6990[5]	– SLP – UDP/TCP บนพอร์ต 427 – HTTPS – TCP บนพอร์ต 443 – IPMI – TCP บนพอร์ต 623 – การควบคุมระยะไกล – TCP บนพอร์ต 3888[4] – KVM ระยะไกล – TCP บนพอร์ต 3889[4] – CIM HTTP – TCP บนพอร์ต 5988[3] – CIM HTTPS – TCP บนพอร์ต 5989[3] – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต 6990[5]	– SLP – UDP/TCP บนพอร์ต 427 – การควบคุมระยะไกล – TCP บนพอร์ต 3888[4] – KVM ระยะไกล – TCP บนพอร์ต 3889[1, 4] – CIM HTTP – TCP บนพอร์ต 5988[3] – CIM HTTPS – TCP บนพอร์ต 5989[3] – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต 6990[5]	– SNMP Traps – UDP บนพอร์ต 162 – IPMI – UDP บนพอร์ต 623
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	– SFTP – TCP บนพอร์ต 22[2] – HTTPS – TCP บนพอร์ต 443 – การค้นหา SSDP – UDP บนพอร์ต 1900 – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต	– SFTP – TCP บนพอร์ต 22[2] – HTTPS – TCP บนพอร์ต 443 – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต 6990[5] – ตัวชี้วัด CIM HTTPS – TCP	– SFTP – TCP บนพอร์ต 22[2] – HTTPS – TCP บนพอร์ต 443 – กา รอัปเดตเฟิร์มแวร์ - TCP บนพอร์ต 6990[5] – ตัวชี้วัด CIM HTTPS – TCP	– SNMP Traps – UDP บนพอร์ต 162

การสื่อสาร	ThinkSystem และ ThinkAgile	System x	Flex System	ThinkServer
	6990[5] – ตัวชี้วัด CIM HTTPS – TCP 9090 – LDAPS – TCP บนพอร์ต 50636[6],50637	9090 – LDAPS – TCP บนพอร์ต 50636[6],50637	9090 – LDAPS – TCP บนพอร์ต 50636[6],50637	

1. ต้องเปิดพอร์ตนี้เฉพาะเซิร์ฟเวอร์ที่มี IMM2 เท่านั้น
2. พอร์ตนี้ใช้ในการถ่ายโอนการอัปเดตเฟิร์มแวร์โดยใช้ SFTP
3. ตามค่าเริ่มต้น การจัดการจะทำผ่านพอร์ตที่มีความปลอดภัย พอร์ตที่ไม่ปลอดภัยเป็นตัวเลือกเสริม
4. เปิดใช้งานระบบควบคุมระยะไกลและ KVM ระยะไกลจากเว็บเบราว์เซอร์ ไม่ใช่เซิร์ฟเวอร์ XClarity Administrator
5. พอร์ตนี้ใช้ในการเชื่อมต่อกับระบบปฏิบัติการ BMU เพื่อถ่ายโอนไฟล์และเรียกใช้สั่งการอัปเดต
6. พอร์ตนี้จำเป็นสำหรับการกำหนดค่าเซิร์ฟเวอร์โดยใช้รูปแบบการกำหนดค่า

- **สวิตช์** Rack **และ** Flex

การสื่อสาร	**สวิตช์** Rack	**สวิตช์** Flex
ขาออก (พอร์ตเปิดบนระบบภายนอก)	– SSH – TCP บนพอร์ต 22[1,3] – SNMP - UDP บนพอร์ต 161[2] – SLP – UDP/TCP บนพอร์ต 427[6] – HTTPS – TCP บนพอร์ต 443[7]	– SSH – TCP บนพอร์ต 22[3] – SNMP - UDP บนพอร์ต 161[5]
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	– SFTP – TCP บนพอร์ต 22[4] – SNMP Traps – TCP บนพอร์ต 162[2]	– SFTP – TCP บนพอร์ต 22[4] – SNMP Traps- TCP บนพอร์ต 162[2]

1. สำหรับสวิตช์ Rack ของ ENOS พอร์ตนี้ใช้ในการกำหนดค่าข้อมูลประจำตัวหัวของสแต็ก (HoS), ใช้ระหว่างสวิตช์ CMM และ Flex, เปิดใช้งานช่องเฟิร์มแวร์ และล้างข้อมูลคีย์โฮสต์ SSH ก่อนที่จะถ่ายโอนไฟล์ SFTP
2. ต้องเปิดพอร์ตนี้บนอุปกรณ์เครื่องมือ XClarity Administrator (ขาเข้า) เมื่อสวิตช์อยู่บนเครือข่ายอื่นที่ไม่ใช่ XClarity Administrator เพื่อให้ XClarity Administrator สามารถรับเหตุการณ์สำหรับอุปกรณ์เหล่านั้นได้

3. พอร์ตนี้ใช้ในการจัดการ (SSH)
4. พอร์ตนี้ใช้ในการถ่ายโอนการอัปเดตเฟิร์มแวร์โดยใช้ SFTP
5. สำหรับสวิตช์ Rack ของ ENOS พอร์ตนี้ใช้ในการถ่ายโอนข้อมูลรายการอุปกรณ์
6. พอร์ตนี้ใช้ในการค้น
7. พอร์ตนี้ใช้ในการปรับใช้การอัปเดตเฟิร์มแวร์

- **อุปกรณ์จัดเก็บ**

การสื่อสาร	อุปกรณ์จัดเก็บ
ขาออก (พอร์ตเปิดบนระบบภายนอก)	– FTP – TCP พอร์ต **21** – SFTP- TCP บนพอร์ต **22**[2] – SLP – UDP/TCP บนพอร์ต **427** – HTTPS – TCP บนพอร์ต **443**[1]
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	– HTTPS – TCP บนพอร์ต **443**[2] – SNMP Traps- UDP บนพอร์ต **115**

1. พอร์ตนี้ใช้ในการถ่ายโอนการอัปเดตเฟิร์มแวร์
2. พอร์ตนี้ใช้ในการถ่ายโอนและปรับใช้การอัปเดตเฟิร์มแวร์

การเข้าถึงระหว่าง XClarity Administrator และเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์

การสื่อสาร	การปรับใช้ OS [1, 2, 3]	การอัปเดตไดรเวอร์อุปกรณ์ OS [2]
ขาออก (พอร์ตเปิดบนระบบภายนอก)		• WinRM ผ่าน HTTP – TCP บนพอร์ต **5985**[5] • WinRM ผ่าน HTTPS – TCP บนพอร์ต **5986**[6]
ขาเข้า (พอร์ตเปิดบนอุปกรณ์ XClarity Administrator)	• การสื่อสาร SMB – TCP บนพอร์ต **445**[4] • HTTPS (ยกเว้น ThinkServer) – TCP บนพอร์ต **8443**[6]	• การสื่อสาร SMB – TCP บนพอร์ต **445**[4]

1. หากคุณกำหนดค่า XClarity Administrator ให้ใช้งานเครือข่ายการปรับใช้ระบบปฏิบัติการ ต้องเปิดพอร์ตบนเครือข่ายนั้น
2. สำหรับรายการพอร์ตที่ต้องพร้อมใช้งานในการปรับใช้ระบบปฏิบัติการ โปรดดู ความพร้อมใช้งานของพอร์ตสำหรับระบบปฏิบัติการที่ใช้งาน ในเอกสารแบบออนไลน์ของ XClarity Administrator ตัวอย่างเช่น หากมีการกำหนดค่าการปรับใช้ระบบปฏิบัติการ ให้ใช้เครือข่ายข้อมูล (eth1) แต่ต้องเปิดพอร์ตเหล่าบนเครือข่ายนั้น
3. อินสแตนซ์ XClarity Administrator แต่ละรายการจะมีหน่วยงานด้านใบรับรอง (CA) ที่ไม่ซ้ำกัน ซึ่งใช้สำหรับการปรับใช้ OS เท่านั้น CA ดังกล่าวจะลงนามในใบรับรองที่ใช้สำหรับเซิร์ฟเวอร์เป้าหมายในพอร์ต 8443 เมื่อเริ่มการปรับใช้ OS ระบบจะรวมใบรับรอง CA นั้นในอิมเมจ OS ที่พุชไปยังเซิร์ฟเวอร์เป้าหมาย ในฐานะส่วนหนึ่งของกระบวนการปรับใช้ เซิร์ฟเวอร์นั้นจะเชื่อมโยงกลับไปยังพอร์ต 8443 รวมทั้งยืนยันใบรับรองที่ได้รับจากพอร์ต 8443 ระหว่างการทำแฮนด์เชค เนื่องจากพอร์ตทั้งสองมีใบรับรอง CA
4. พอร์ตนี้ใช้ในการถ่ายโอนไฟล์ไดรเวอร์ Windows
5. พอร์ตนี้ใช้ในการเชื่อมต่อกับ WinRM ของเซิร์ฟเวอร์เป้าหมาย
6. พอร์ตนี้ใช้ในการแลกเปลี่ยนข้อมูลระหว่าง OS เป้าหมายกับ XClarity Administrator รวมถึงอิมเมจและสถานะ OS

ข้อควรพิจารณาด้านการจัดการ

การจัดการอุปกรณ์มีให้เลือกหลายวิธี คุณอาจต้องใช้โซลูชั่นการจัดการหลายตัวที่ทำงานในเวลาเดียวกัน ขึ้นอยู่กับอุปกรณ์ที่ได้รับการจัดการ

สามารถจัดการอุปกรณ์หนึ่งได้โดยอินสแตนซ์เดียวของ Lenovo XClarity Administrator เท่านั้น อย่างไรก็ตาม คุณสามารถใช้ซอฟต์แวร์การจัดการอื่น (เช่น VMware vRealize Operations Manager) ร่วมกับ Lenovo XClarity Administrator เพื่อ*ติดตาม*อุปกรณ์ที่ XClarity Administrator จัดการ

ข้อควรพิจารณา: ต้องใช้ความระมัดระวังเป็นพิเศษ เมื่อใช้เครื่องมือการจัดการหลายตัวในการจัดการอุปกรณ์ของคุณ เพื่อป้องกันความขัดแย้งที่คาดไม่ถึง ตัวอย่างเช่น การส่งการเปลี่ยนแปลงสถานะพลังงานโดยใช้เครื่องมืออื่น อาจขัดแย้งกับงานการกำหนดค่าหรือการอัปเดตที่กำลังทำงานใน XClarity Administrator

อุปกรณ์ ThinkSystem, ThinkServer และ System x

หากคุณต้องการใช้ซอฟต์แวร์การจัดการในการตรวจสอบอุปกรณ์ที่ได้รับการจัดการของคุณ ให้สร้างผู้ใช้ภายในใหม่ด้วยการตั้งค่า SNMP หรือ IPMI ที่ถูกต้องจากอินเทอร์เฟซ IMM ตรวจสอบให้แน่ใจว่าคุณให้สิทธิ์ SNMP หรือ IPMI แล้วแต่ความต้องการของคุณ

อุปกรณ์ Flex System

หากคุณต้องการใช้ซอฟต์แวร์การจัดการอื่นเพื่อตรวจสอบอุปกรณ์ที่ได้รับการจัดการของคุณ และดูว่าซอฟต์แวร์การจัดการดังกล่าวใช้การสื่อสาร SNMPv3 หรือ IPMI หรือไม่ คุณต้องเตรียมระบบของคุณโดยปฏิบัติตามขั้นตอนต่อไปนี้สำหรับ CMM ที่จัดการแต่ละเครื่องดังนี้

1. เข้าระบบในเว็บอินเทอร์เฟซของตัวควบคุมการจัดการสำหรับตัวเครื่องโดยใช้ชื่อผู้ใช้และรหัสผ่านของ `RECOVERY_ID`
2. หากนโยบายการรักษาความปลอดภัยถูกตั้งค่าเป็น **การรักษาความปลอดภัย** ให้เปลี่ยนวิธีการตรวจสอบความถูกต้องของผู้ใช้
   a. คลิก **การจัดการโมดูลการจัดการ ➡ บัญชีผู้ใช้**
   b. คลิกแท็บ **บัญชี**
   c. คลิก **การตั้งค่าการเข้าสู่ระบบแบบส่วนกลาง**
   d. คลิกแท็บ **ทั่วไป**
   e. เลือก **ภายนอกก่อน แล้วจึงการตรวจสอบความถูกต้องภายใน** สำหรับวิธีการตรวจสอบความถูกต้องของผู้ใช้
   f. คลิก **ตกลง**
3. สร้างผู้ใช้ภายในใหม่ด้วยการตั้งค่า SNMP หรือ IPMI ที่ถูกต้องจากเว็บอินเทอร์เฟซของตัวควบคุมการจัดการ
4. หากนโยบายการรักษาความปลอดภัยถูกตั้งค่าเป็น **การรักษาความปลอดภัย** ให้ออกจากระบบ แล้วเข้าระบบในเว็บอินเทอร์เฟซของตัวควบคุมการจัดการ โดยใช้ชื่อผู้ใช้ใหม่และรหัสผ่าน เมื่อได้รับข้อความแจ้ง ให้เปลี่ยนรหัสผ่านสำหรับผู้ใช้ใหม่

ตอนนี้ คุณสามารถใช้ผู้ใช้ใหม่เป็นผู้ใช้ SNMP หรือ IPMI ที่ใช้งาน

หมายเหตุ: หากคุณถอนการจัดการตัวเครื่องแล้วกลับมาจัดการอีกครั้ง บัญชีผู้ใช้ใหม่นี้จะถูกล็อคและปิดใช้งาน ในกรณีนี้ ทำขั้นตอนดังกล่าวซ้ำเพื่อสร้างบัญชีผู้ใช้ใหม่

ข้อควรพิจารณาด้านเครือข่าย

เมื่อวางแผนการติดตั้ง Lenovo XClarity Administrator ให้พิจารณาโทโพโลยีเครือข่ายที่นำมาใช้งานในระบบของคุณ และ XClarity Administrator เข้ากับโทโพโลยีดังกล่าวอย่างไร

ข้อสำคัญ: กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) ถ้าใช้ DHCP ต้องแน่ใจว่ามีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด

ข้อจำกัดของการกำหนดค่า IP

สำหรับฟังก์ชันและอุปกรณ์ที่ได้รับการจัดการต่อไปนี้ จะต้องกำหนดค่าอินเทอร์เฟซเครือข่ายด้วยที่อยู่ IPv4 ไม่รองรับที่อยู่ IPv6

- อัปเดตเฟิร์มแวร์สำหรับอุปกรณ์ Lenovo Storage
- เซิร์ฟเวอร์ ThinkServer
- อุปกรณ์ Lenovo Storage

ไม่รองรับการจัดการอุปกรณ์ RackSwitch โดยใช้ IPv6 Link Local ผ่านทางพอร์ตข้อมูลหรือพอร์ตการจัดการ

ไม่รองรับ Network Address Translation (NAT) ซึ่งเปลี่ยนการแมปพื้นที่ที่อยู่ IP

ประเภทเครือข่าย

โดยทั่วไปแล้ว สภาพแวดล้อมส่วนใหญ่จะใช้งานประเภทเครือข่ายต่อไปนี้ คุณอาจใช้งานเครือข่ายเหล่านี้เพียงเครือข่ายเดียวหรืออาจใช้ทั้งสามเครือข่าย ขึ้นอยู่กับความต้องการของคุณ

- **เครือข่ายการจัดการ**

  โดยปกติแล้วเครือข่ายการจัดการจะสำรองไว้สำหรับการสื่อสารระหว่าง Lenovo XClarity Administrator และหน่วยประมวลผลการจัดการสำหรับอุปกรณ์ที่ได้รับการจัดการ ตัวอย่างเช่น อาจมีการกำหนดค่าเครือข่ายการจัดการเพื่อให้รวม XClarity Administrator, CMM สำหรับแต่ละตัวเครื่องที่ได้รับการจัดการ และตัวควบคุมการจัดการแผงวงจรของแต่ละเซิร์ฟเวอร์ที่ XClarity Administrator จัดการ

- **เครือข่ายข้อมูล**

  โดยปกติแล้วเครือข่ายข้อมูลจะใช้สำหรับการสื่อสารระหว่างระบบปฏิบัติการที่ติดตั้งบนเซิร์ฟเวอร์และอินทราเน็ตของบริษัท อินเทอร์เน็ต หรือทั้งคู่

- **เครือข่ายการปรับใช้ระบบปฏิบัติการ**

  ในบางกรณี มีการตั้งค่าเครือข่ายการปรับใช้ระบบปฏิบัติการให้แยกการสื่อสารออก ซึ่งจำเป็นต่อการปรับใช้ระบบปฏิบัติการบนเซิร์ฟเวอร์ หากใช้งาน โดยปกติแล้วเครือข่ายนี้จะรวม XClarity Administrator และโฮสต์เซิร์ฟเวอร์ทั้งหมด

  แทนที่จะใช้งานเครือข่ายการปรับใช้ระบบปฏิบัติการแยกต่างหาก คุณอาจเลือกที่จะผสานรวมฟังก์ชันการทำงานนี้ในเครือข่ายการจัดการหรือเครือข่ายข้อมูลก็ได้

การกำหนดค่าเครือข่าย

คุณสามารถกำหนดค่า Lenovo XClarity Administrator ให้ใช้อินเทอร์เฟซเครือข่ายหนึ่งหรือสองรายการได้

ข้อควรพิจารณา:

- การเปลี่ยนที่อยู่ IP ของ XClarity Administrator หลังจากจัดการอุปกรณ์อาจทำให้อุปกรณ์อยู่ในสถานะออฟไลน์ใน XClarity Administrator ตรวจสอบให้แน่ใจว่าอุปกรณ์ทั้งหมดไม่ได้รับการจัดการก่อนที่จะเปลี่ยนที่อยู่ IP

- คุณสามารถเปิดใช้งานหรือปิดใช้งานการตรวจสอบที่อยู่ IP ที่ซ้ำกันในซับเน็ตเดียวกันได้โดยคลิกปุ่มสลับ **การตรวจสอบที่อยู่ IP ที่ซ้ำกัน** ส่วนนี้จะปิดใช้งานตามค่าเริ่มต้น เมื่อเปิดใช้งาน XClarity Administrator จะแสดงการแจ้งเตือนหากคุณพยายามแก้ไขที่อยู่ IP ของ XClarity Administrator หรือจัดการอุปกรณ์ที่มีที่อยู่ IP เดียวกันกับอุปกรณ์อื่นที่ได้รับการจัดการ หรืออุปกรณ์อื่นที่พบในซับเน็ตเดียวกัน

  หมายเหตุ: เมื่อเปิดใช้งาน XClarity Administrator จะเรียกใช้การสแกน ARP เพื่อค้นหาอุปกรณ์ IPv4 ที่ใช้งานอยู่บนซับเน็ตเดียวกัน หากต้องการป้องกันไม่ให้ทำการสแกน ARP ให้ปิดใช้งาน **การตรวจสอบที่อยู่ IP ที่ซ้ำกัน**
- เมื่อใช้ XClarity Administrator เป็นอุปกรณ์เสมือน หากอินเทอร์เฟซเครือข่ายสำหรับเครือข่ายการจัดการถูกกำหนดค่าให้ใช้ Dynamic Host Configuration Protocol (DHCP) ที่อยู่ IP ของอินเทอร์เฟซการจัดการอาจเปลี่ยนแปลงได้เมื่อการเช่า DHCP หมดอายุลง หากที่อยู่ IP เปลี่ยน คุณต้องถอนการจัดการตัวเครื่อง เซิร์ฟเวอร์ในแร็คและเซิร์ฟเวอร์แบบทาวเวอร์ แล้วจึงกลับมาจัดการอีกครั้ง เพื่อหลีกเลี่ยงปัญหาดังกล่าว ให้เปลี่ยนอินเทอร์เฟซการจัดการเป็นที่อยู่ IP แบบคงที่ หรือไม่ก็ตรวจสอบให้แน่ใจว่าการกำหนดค่าเซิร์ฟเวอร์ DHCP ได้รับการตั้งค่าตามที่อยู่ DHCP เป็นไปตามที่อยู่ MAC หรือการเช่า DHCP ยังไม่หมดอายุ
- หากคุณ*ไม่*ต้องการใช้ XClarity Administrator เพื่อปรับใช้ระบบปฏิบัติการหรืออัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถปิดใช้งานเซิร์ฟเวอร์ Samba และ Apache ได้โดยการเปลี่ยนอินเทอร์เฟซเครือข่ายให้ใช้ตัวเลือก **ค้นหาและจัดการฮาร์ดแวร์เท่านั้น** โปรดทราบว่าเซิร์ฟเวอร์การจัดการจะรีสตาร์ทหลังจากการเปลี่ยนแปลงอินเทอร์เฟซเครือข่าย
- เมื่อใช้ XClarity Administrator เป็นคอนเทนเนอร์
  - คุณสามารถเปิดหรือปิดใช้งานการตรวจสอบที่อยู่ IP ที่ซ้ำกัน แก้ไขบทบาทของอินเทอร์เฟซเครือข่าย และแก้ไขการตั้งค่าพร็อกซีได้เท่านั้น การตั้งค่าเครือข่ายอื่นๆ ทั้งหมด (รวมถึงที่อยู่ IP, เกตเวย์ และ DNS) จะถูกกำหนดไว้ในการตั้งค่าคอนเทนเนอร์
  - ตรวจสอบให้แน่ใจว่ามีการตั้งค่าเครือข่าย macvlan บนระบบโฮสต์

XClarity Administrator มีอินเทอร์เฟซเครือข่ายต่างหากสองส่วนที่สามารถกำหนดให้กับระบบของคุณได้ ขึ้นอยู่กับโทโพโลยีเครือข่ายที่คุณนำมาใช้ สำหรับอุปกรณ์เสมือน เครือข่ายเหล่านี้มีจะชื่อเป็น eth0 และ eth1 สำหรับคอนเทนเนอร์ คุณสามารถเลือกชื่อที่กำหนดเองได้

- กรณีที่มีเพียงอินเทอร์เฟซเครือข่ายเดียว (eth0):
  - ต้องกำหนดค่าอินเทอร์เฟซเพื่อสนับสนุนการค้นหาและการจัดการอุปกรณ์ (เช่น การอัปเดตการกำหนดค่าและเฟิร์มแวร์) โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการแผงวงจรในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
  - หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้นคุณต้องนำเข้าการอัปเดตลงในที่เก็บ

- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์ของ OS อินเทอร์เฟซเครือข่ายจะต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเครือข่ายเซิร์ฟเวอร์ที่ใช้ในการเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

- ในกรณีที่มีอินเทอร์เฟซเครือข่ายสองตัว (eth0 และ eth1):
  - อินเทอร์เฟซเครือข่ายแรก (โดยปกติคืออินเทอร์เฟซ Eth0) จะต้องเชื่อมต่อกับเครือข่ายการจัดการ และกำหนดค่าให้สนับสนุนการค้นหาและการจัดการอุปกรณ์ (รวมถึงการกำหนดค่าเซิร์ฟเวอร์และการอัปเดตเฟิร์มแวร์ โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
  - อินเทอร์เฟซเครือข่ายที่สอง (โดยทั่วไปคืออินเทอร์เฟซ eth1) จะสามารถกำหนดค่าให้สื่อสารกับเครือข่ายข้อมูลภายใน เครือข่ายข้อมูลสาธารณะ หรือทั้งสองเครือข่าย
  - หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้นคุณต้องนำเข้าการอัปเดตลงในที่เก็บ
  - หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
  - หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์อุปกรณ์ คุณสามารถเลือกที่จะใช้อินเทอร์เฟซ eth1 หรือ eth0 ได้ อย่างไรก็ตาม อินเทอร์เฟซที่คุณใช้ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเซิร์ฟเวอร์เครือข่ายที่ใช้เพื่อเข้าถึงระบบปฏิบัติการโฮสต์

    หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

ตารางต่อไปนี้แสดงการกำหนดค่าที่เป็นไปได้สำหรับอินเทอร์เฟซเครือข่าย XClarity Administrator ตามประเภทของโทโพโลยีเครือข่ายที่นำมาใช้งานในระบบของคุณ ใช้ตารางนี้เพื่อระบุวิธีการกำหนดอินเทอร์เฟซเครือข่ายแต่ละรายการ

ตาราง 2. บทบาทของอินเทอร์เฟซเครือข่ายแต่ละรายการตามโทโพโลยีเครือข่าย

โทโพโลยีเครือข่าย	**บทบาทของอินเทอร์เฟซ** 1 (eth0)	**บทบาทของอินเทอร์เฟซ** 2 (eth1)
เครือข่าย Converged (การจัดการและเครือข่ายข้อมูลที่รองรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS)	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS	ไม่มี
แยกเครือข่ายการจัดการที่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS และเครือข่ายข้อมูล	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS	เครือข่ายข้อมูล • ไม่มี
แยกเครือข่ายการจัดการและเครือข่ายข้อมูลที่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	เครือข่ายข้อมูล • การค้นหาและการจัดการ • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS

ตาราง 2. บทบาทของอินเทอร์เฟซเครือข่ายแต่ละรายการตามโทโพโลยีเครือข่าย (มีต่อ)

โทโพโลยีเครือข่าย	**บทบาทของอินเทอร์เฟซ** 1 (eth0)	**บทบาทของอินเทอร์เฟซ** 2 (eth1)
แยกเครือข่ายการจัดการและเครือข่ายข้อมูลที่ไม่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	เครือข่ายข้อมูล • ไม่มี
เฉพาะเครือข่ายการจัดการเท่านั้น (ไม่สนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS)	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	ไม่มี

เครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว

ในโทโพโลยีเครือข่ายนี้ การสื่อสารด้านการจัดการ การสื่อสารด้านข้อมูล และการปรับใช้ระบบปฏิบัติการจะเกิดขึ้นผ่านเครือข่ายเดียวกัน โทโพโลยีนี้เรียกว่าเครือข่าย *converged*

ข้อสำคัญ: การใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่ใช้งานร่วมกัน อาจทำให้เกิดการหยุดชะงักในการรับส่งข้อมูล เช่น แพ็คเก็ตที่ถูกยกเลิก หรือปัญหาการเชื่อมต่อเครือข่ายการจัดการ โดยขึ้นอยู่กับการกำหนดค่าเครือข่ายของคุณ (ตัวอย่างเช่น หากการรับส่งข้อมูลจากเซิร์ฟเวอร์มีลำดับความสำคัญสูงและการรับส่งข้อมูลจากตัวควบคุมการจัดการมีลำดับความสำคัญต่ำ) เครือข่ายการจัดการใช้การรับส่งข้อมูล UDP ใน TCP เพิ่มเติม การรับส่งข้อมูล UDP อาจมีลำดับความสำคัญต่ำเมื่อการรับส่งข้อมูลของเครือข่ายอยู่ในลำดับสูง

เมื่อคุณติดตั้ง Lenovo XClarity Administrator จะกำหนดอินเทอร์เฟซเครือข่าย eth0 โดยคำนึงถึงเงื่อนไขต่อไปนี้:

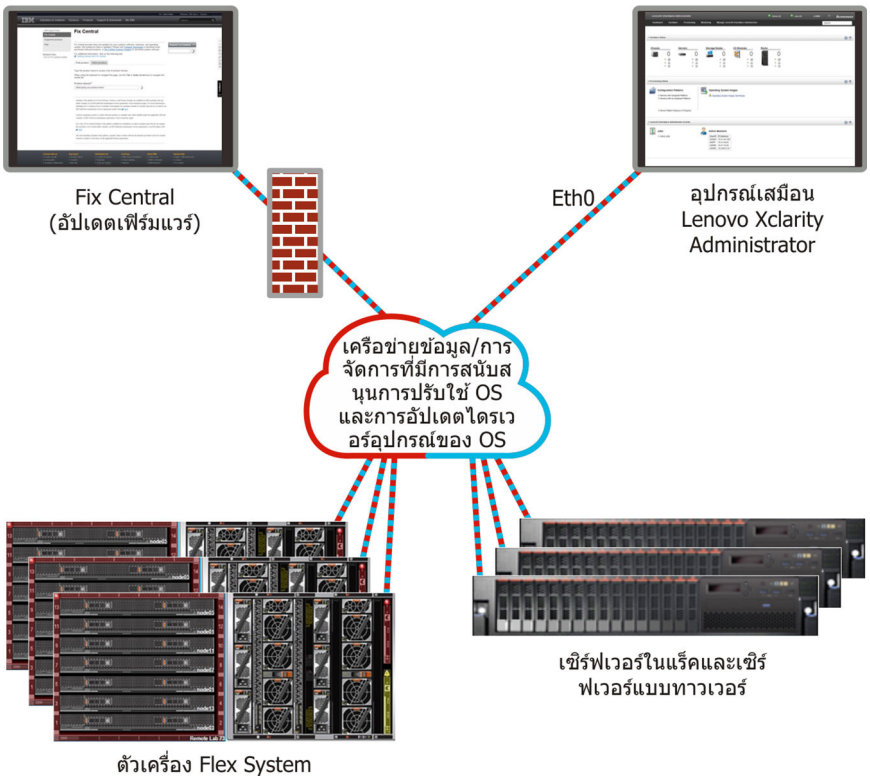
- ต้องกำหนดค่าอินเทอร์เฟซเพื่อสนับสนุนการค้นหาและการจัดการอุปกรณ์ (เช่น การอัปเดตการกำหนดค่าและเฟิร์มแวร์) โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการแผงวงจรในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง

- หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้น คุณต้องนำเข้าการอัปเดตลงในที่เก็บ
- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์ของ OS อินเทอร์เฟซเครือข่ายจะต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเครือข่ายเซิร์ฟเวอร์ที่ใช้ในการเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น
- คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่ตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการเฉพาะเมื่อคุณใช้งานโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง อย่างไรก็ตาม คุณไม่สามารถใช้ XClarity Administrator เพื่อนำการอัปเดตเฟิร์มแวร์ไปใช้กับเซิร์ฟเวอร์ที่ได้รับการจัดการ แม้ว่าจะมีการนำเฟิร์มแวร์บางรายการเท่านั้นไปใช้กับการเปิดใช้งานทันที และ XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ท ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อนำไปใช้กับการเปิดใช้งานแบบเลื่อน เฉพาะบางเฟิร์มแวร์เท่านั้นที่นำไปใช้เมื่อรีสตาร์ทโฮสต์ XClarity Administrator

นอกจากนี้ คุณยังสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองสำหรับเชื่อมต่อกับเครือข่ายเดียวกันจาก XClarity Administrator เพื่อรองรับการสำรองซ้ำซ้อน

ภาพต่อไปนี้แสดงตัวอย่างการใช้งานสำหรับโทโพโลยีเครือข่าย Converged



รูปภาพ 1. ตัวอย่างการใช้งานของเครือข่ายเดี่ยวสำหรับการจัดการ ข้อมูล และการปรับใช้ระบบปฏิบัติการ

เครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

ในโทโพโลยีเครือข่ายนี้ เครือข่ายการจัดการและเครือข่ายข้อมูลเป็นเครือข่ายที่แยกจากกันทางกายภาพ และเครือข่ายการปรับใช้ระบบปฏิบัติการได้รับการกำหนดค่าเป็นส่วนหนึ่งของเครือข่ายการจัดการหรือเครือข่ายข้อมูล

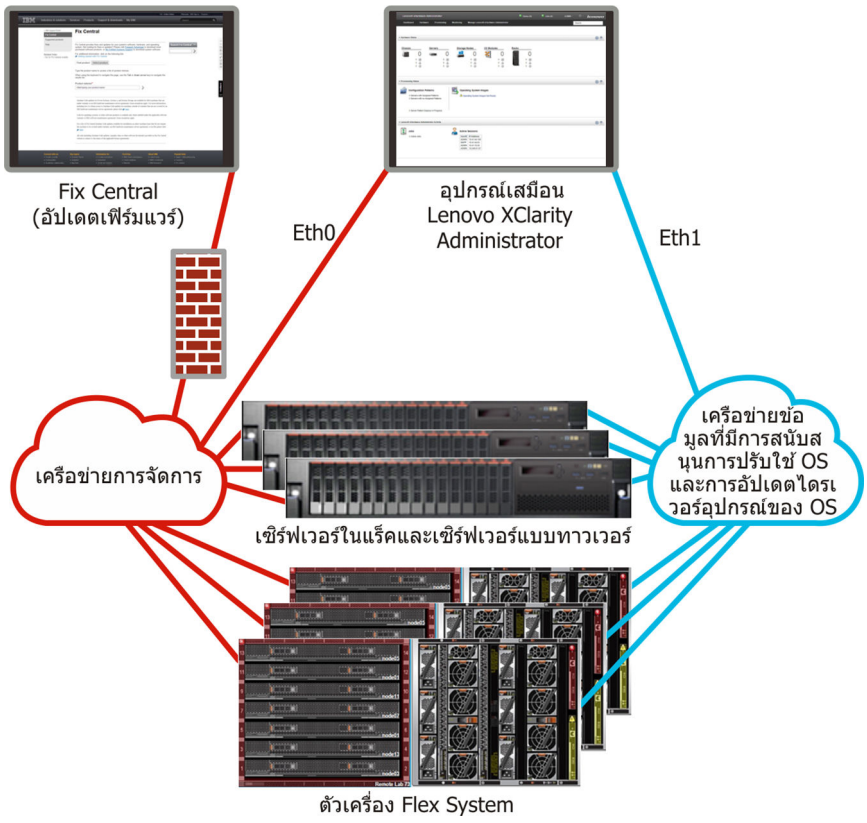
เมื่อคุณติดตั้ง Lenovo XClarity Administrator จะกำหนดการตั้งค่าเครือข่ายโดยใช้ข้อควรพิจารณาต่อไปนี้:

- อินเทอร์เฟซเครือข่ายแรก (โดยปกติคืออินเทอร์เฟซ Eth0) จะต้องเชื่อมต่อกับเครือข่ายการจัดการ และกำหนดค่าให้สนับสนุนการค้นหาและการจัดการอุปกรณ์ (รวมถึงการกำหนดค่าเซิร์ฟเวอร์และการอัปเดตเฟิร์มแวร์ โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
- อินเทอร์เฟซเครือข่ายที่สอง (โดยทั่วไปคืออินเทอร์เฟซ eth1) จะสามารถกำหนดค่าให้สื่อสารกับเครือข่ายข้อมูลภายใน เครือข่ายข้อมูลสาธารณะ หรือทั้งสองเครือข่าย
- หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้น คุณต้องนำเข้าการอัปเดตลงในที่เก็บ

- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์อุปกรณ์ คุณสามารถเลือกที่จะใช้อินเทอร์เฟซ eth1 หรือ eth0 ได้ อย่างไรก็ตาม อินเทอร์เฟซที่คุณใช้ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเซิร์ฟเวอร์เครือข่ายที่ใช้เพื่อเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

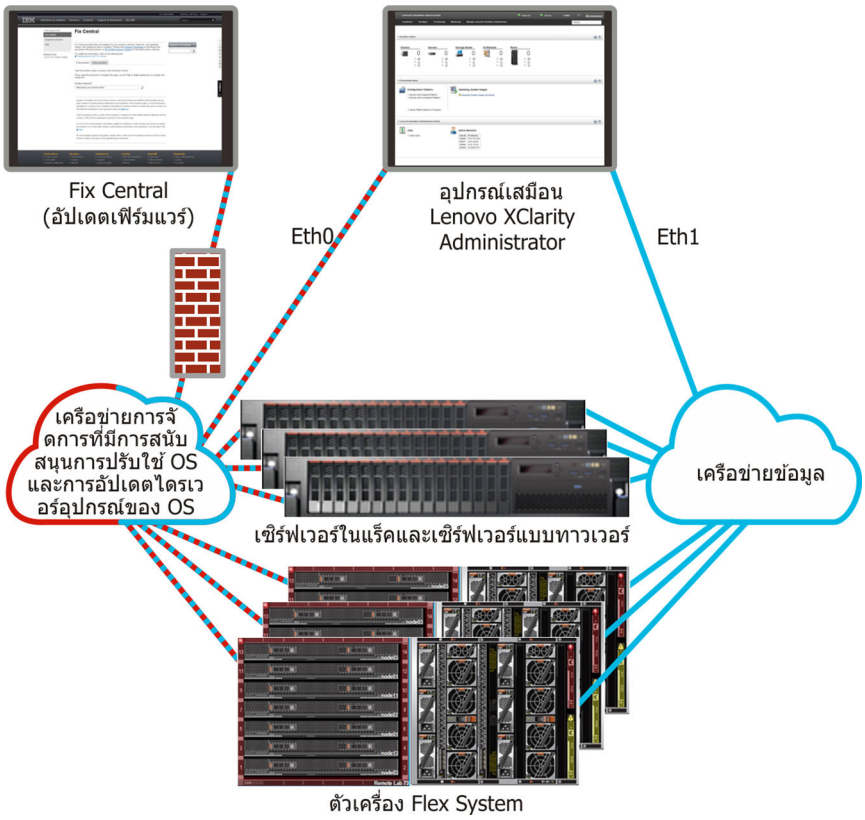
รูปภาพ2 “ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล” บนหน้าที่ 33 แสดงตัวอย่างการใช้งานเครือข่ายการจัดการและเครือข่ายข้อมูลแยกจากกัน ซึ่งมีการกำหนดค่าเครือข่ายการปรับใช้ระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล



รูปภาพ 2. ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล

รูปภาพ3 “ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ” บนหน้าที่ 34 แสดงอีกตัวอย่างหนึ่งของการใช้งานเครือข่ายการจัดการและเครือข่ายข้อมูลแยกจากกัน ซึ่งมีการกำหนดค่าเครือข่ายการปรับใช้ระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ ในการใช้งานนี้ XClarity Administrator ไม่จำเป็นต้องมีการเชื่อมต่อกับเครือข่ายข้อมูล

หมายเหตุ: หากเครือข่ายการปรับใช้ระบบปฏิบัติการไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูล หากจำเป็น



รูปภาพ 3. ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ

เครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือน

ในโทโพโลยีนี้ เครือข่ายข้อมูลและเครือข่ายการจัดการจะแยกจากกันแบบเสมือนจริง แพ็คเก็ตจากเครือข่ายข้อมูลและแพ็คเก็ตจากเครือข่ายการจัดการถูกส่งผ่านการเชื่อมต่อทางกายภาพเดียวกัน ระบบจะใช้การแท็ก VLAN บนแพ็คเก็ตข้อมูลเครือข่ายการจัดการทั้งหมดเพื่อแยกการรับส่งข้อมูลระหว่างสองเครือข่ายออกจากกัน

หมายเหตุ: หากมีการติดตั้ง Lenovo XClarity Administrator บนโฮสต์ที่รันเซิร์ฟเวอร์ที่ได้รับการจัดการในตัวเครื่อง คุณจะไม่สามารถใช้ XClarity Administrator เพื่อนำการอัปเดตเฟิร์มแวร์ไปใช้กับทั้งตัวเครื่องพร้อมกัน เมื่อนำการอัปเดตเฟิร์มแวร์ไปใช้ ต้องรีสตาร์ทระบบโฮสต์

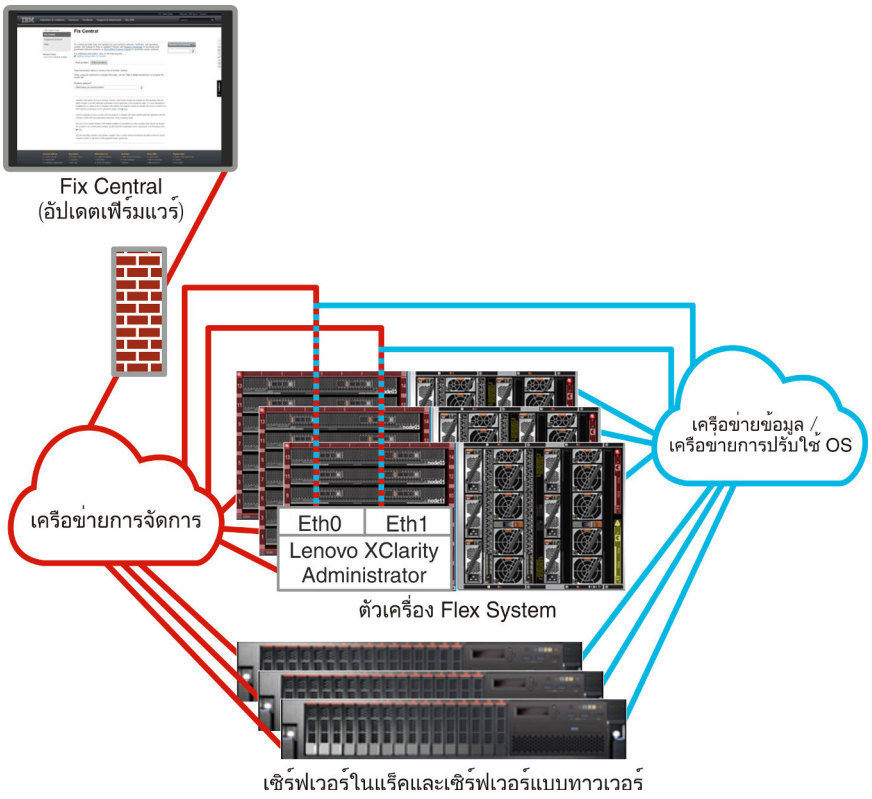
เมื่อคุณติดตั้ง XClarity Administrator จะกำหนดการตั้งค่าเครือข่ายโดยใช้ข้อควรพิจารณาต่อไปนี้:

- อินเทอร์เฟซเครือข่ายแรก (โดยปกติคืออินเทอร์เฟซ Eth0) จะต้องเชื่อมต่อกับเครือข่ายการจัดการ และกำหนดค่าให้สนับสนุนการค้นหาและการจัดการอุปกรณ์ (รวมถึงการกำหนดค่าเซิร์ฟเวอร์และการอัปเดตเฟิร์มแวร์ โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
- อินเทอร์เฟซเครือข่ายที่สอง (โดยทั่วไปคืออินเทอร์เฟซ eth1) จะสามารถกำหนดค่าให้สื่อสารกับเครือข่ายข้อมูลภายใน เครือข่ายข้อมูลสาธารณะ หรือทั้งสองเครือข่าย

- หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้น คุณต้องนำเข้าการอัปเดตลงในที่เก็บ
- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์อุปกรณ์ คุณสามารถเลือกที่จะใช้อินเทอร์เฟซ eth1 หรือ eth0 ได้ อย่างไรก็ตาม อินเทอร์เฟซที่คุณใช้ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเซิร์ฟเวอร์เครือข่ายที่ใช้เพื่อเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น
- คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่ตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการเฉพาะเมื่อคุณใช้งานโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง อย่างไรก็ตาม คุณไม่สามารถใช้ XClarity Administrator เพื่อนำการอัปเดตเฟิร์มแวร์ไปใช้กับเซิร์ฟเวอร์ที่ได้รับการจัดการ แม้ว่าจะมีการนำเฟิร์มแวร์บางรายการเท่านั้นไปใช้กับการเปิดใช้งานทันที และ XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ท ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อนำไปใช้กับการเปิดใช้งานแบบเลื่อน เฉพาะบางเฟิร์มแวร์เท่านั้นที่นำไปใช้เมื่อรีสตาร์ทโฮสต์ XClarity Administrator

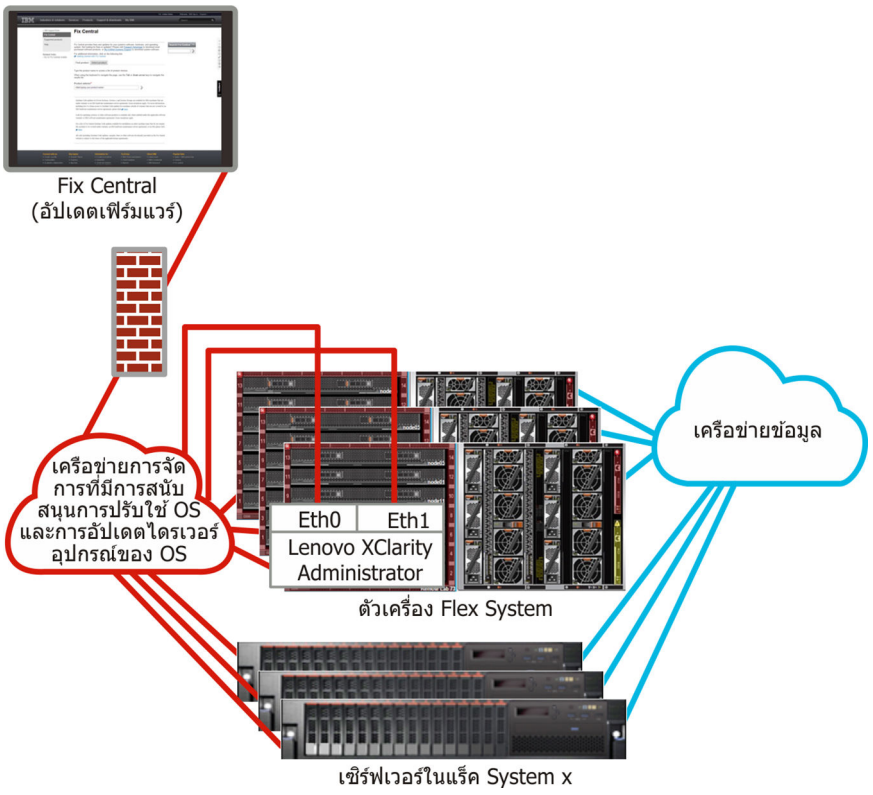
รูปภาพ4 “ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล” บนหน้าที่ 36 แสดงตัวอย่างการใช้งานเครือข่ายการจัดการและเครือข่ายข้อมูลที่แยกจากกันแบบเสมือนจริง ซึ่งมีการกำหนดค่าเครือข่ายการปรับใช้ระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล ในตัวอย่างนี้ XClarity Administrator ได้รับการติดตั้งบนเซิร์ฟเวอร์ที่ได้รับการจัดการในตัวเครื่อง



รูปภาพ 4. ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายข้อมูล

รูปภาพ5 “ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ” บนหน้าที่ 37 แสดงตัวอย่างการใช้งานเครือข่ายการจัดการและเครือข่ายข้อมูลที่แยกจากกันแบบเสมือนจริง ซึ่งมีการกำหนดค่าเครือข่ายการปรับใช้ระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ และ XClarity Administrator ได้รับการติดตั้งบนเซิร์ฟเวอร์ที่ได้รับการจัดการในตัวเครื่อง ในการใช้งานนี้ XClarity Administrator ไม่จำเป็นต้องมีการเชื่อมต่อกับเครือข่ายข้อมูล

หมายเหตุ: หากเครือข่ายการปรับใช้ระบบปฏิบัติการไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูล หากจำเป็น



รูปภาพ 5. ตัวอย่างการใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง ที่มีเครือข่ายระบบปฏิบัติการเป็นส่วนหนึ่งของเครือข่ายการจัดการ

เครือข่ายการจัดการอย่างเดียว

ในโทโพโลยีนี้ Lenovo XClarity Administrator สามารถเข้าถึงเครือข่ายการจัดการได้อย่างเดียว โดยไม่สามารถเข้าถึงเครือข่ายข้อมูลได้ อย่างไรก็ตาม XClarity Administrator ต้องมีสิทธิ์เข้าถึงเครือข่ายการปรับใช้ระบบปฏิบัติการ หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการจาก XClarity Administrator ถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ

เมื่อคุณติดตั้ง XClarity Administrator และกำหนดการตั้งค่าเครือข่าย จะต้องกำหนดค่าอินเทอร์เฟซเครือข่าย eth0 เป็น

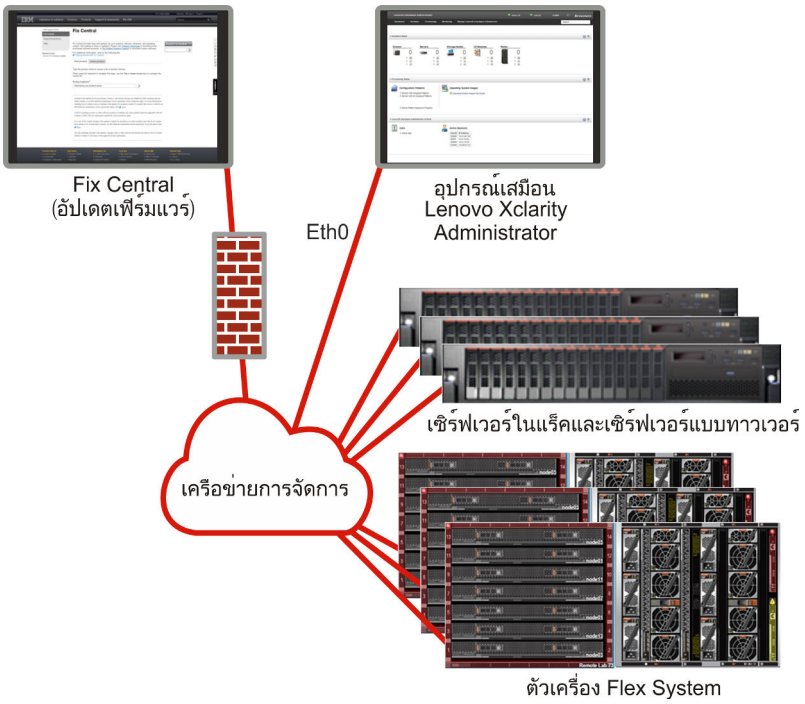
- ต้องกำหนดค่าอินเทอร์เฟซเพื่อสนับสนุนการค้นหาและการจัดการอุปกรณ์ (เช่น การอัปเดตการกำหนดค่าและเฟิร์มแวร์) โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการแผงวงจรในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
- หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้น คุณต้องนำเข้าการอัปเดตลงในที่เก็บ
- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้

- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์ของ OS อินเทอร์เฟซเครือข่ายจะต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเครือข่ายเซิร์ฟเวอร์ที่ใช้ในการเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

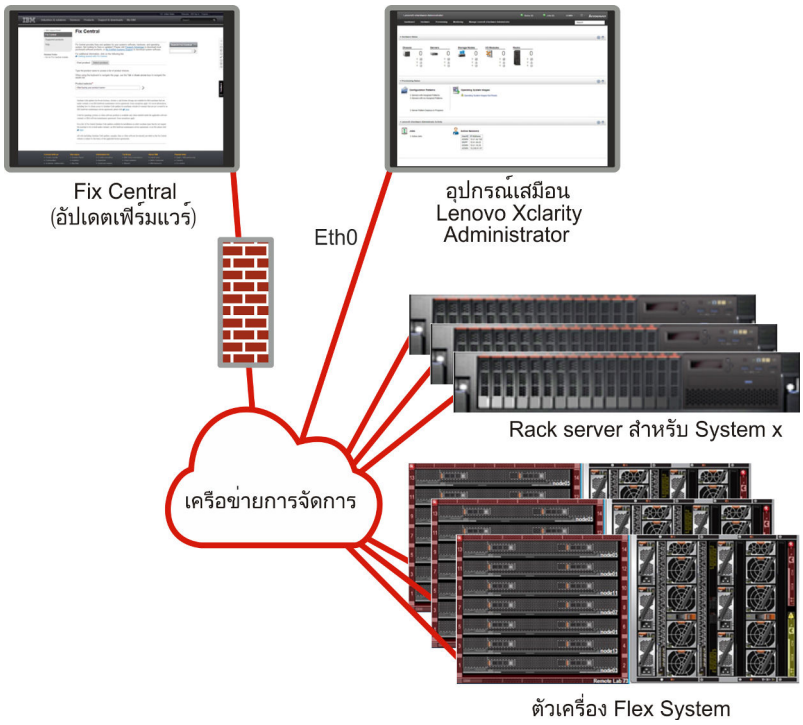
นอกจากนี้ คุณยังสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองสำหรับเชื่อมต่อกับเครือข่ายเดียวกันจาก XClarity Administrator เพื่อรองรับการสำรองซ้ำซ้อน

รูปภาพ6 “ตัวอย่างการนำมาใช้งานของเครือข่ายการจัดการอย่างเดียวที่ไม่มีการรองรับสำหรับการปรับใช้ระบบปฏิบัติการ” บนหน้าที่ 38 แสดงตัวอย่างการนำมาใช้งานสำหรับเครือข่ายการจัดการอย่างเดียวที่ไม่รองรับการปรับใช้ระบบปฏิบัติการจาก XClarity Administrator



รูปภาพ 6. ตัวอย่างการนำมาใช้งานของเครือข่ายการจัดการอย่างเดียวที่ไม่มีการรองรับสำหรับการปรับใช้ระบบปฏิบัติการ

รูปภาพ6 “ตัวอย่างการนำมาใช้งานของเครือข่ายการจัดการอย่างเดียวที่ไม่มีการรองรับสำหรับการปรับใช้ระบบปฏิบัติการ” บนหน้าที่ 38 แสดงตัวอย่างการนำมาใช้งานสำหรับเครือข่ายการจัดการอย่างเดียวที่รองรับการปรับใช้ระบบปฏิบัติการจาก XClarity Administrator



รูปภาพ 7. ตัวอย่างการนำมาใช้งานของเครือข่ายการจัดการอย่างเดียวที่มีการรองรับสำหรับการปรับใช้ระบบปฏิบัติการ

ข้อควรพิจารณาด้านการรักษาความปลอดภัย

แผนสำหรับการรักษาความปลอดภัยของ Lenovo XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการทั้งหมด

การจัดการ Encapsulation

เมื่อคุณจัดการตัวเครื่องและเซิร์ฟเวอร์ Lenovo ใน Lenovo XClarity Administrator คุณสามารถกำหนดค่า Lenovo XClarity Administrator เพื่อเปลี่ยนกฎไฟร์วอลล์สำหรับอุปกรณ์เพื่อให้รับคำขอที่เข้ามาจาก Lenovo XClarity Administrator เท่านั้น ซึ่งเรียกว่า *Encapsulation* คุณยังสามารถเปิดใช้งานหรือปิดใช้งาน Encapsulation บนตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการแล้วโดย Lenovo XClarity Administrator

เมื่อเปิดใช้งานบนอุปกรณ์ที่รองรับ Encapsulation Lenovo XClarity Administrator จะเปลี่ยนโหมด Encapsulation ของอุปกรณ์เป็น “encapsulationLite” และเปลี่ยนกฎไฟร์วอลล์บนอุปกรณ์เพื่อจำกัดคำขอที่เข้ามาจาก Lenovo XClarity Administrator นี้เท่านั้น

เมื่อปิดใช้งาน โหมด Encapsulation จะตั้งค่าเป็น “ปกติ” หากเปิดใช้งาน Encapsulation บนอุปกรณ์ก่อนหน้านี้ ระบบจะนำกฎไฟร์วอลล์สำหรับ Encapsulation ออก

ข้อควรพิจารณา: หากเปิดใช้งาน Encapsulation และ XClarity Administrator ไม่สามารถใช้งานได้ก่อนที่อุปกรณ์จะได้รับการถอนการจัดการ ต้องดำเนินการขั้นตอนที่จำเป็นในการปิดใช้งาน Encapsulation เพื่อสร้างการสื่อสารกับ

อุปกรณ์ สำหรับขั้นตอนการกู้คืน โปรดดู การกู้คืนการจัดการตัวเครื่องด้วย CMM ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว และ การกู้คืนการจัดการแร็คเซิร์ฟเวอร์หรือเซิร์ฟเวอร์แบบทาวเวอร์ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว ในเอกสารแบบออนไลน์ของ XClarity Administrator

หมายเหตุ:

- ไม่รองรับ Encapsulation บนสวิตช์ อุปกรณ์จัดเก็บข้อมูล และตัวเครื่องและเซิร์ฟเวอร์ที่ไม่ใช่ของ Lenovo
- เมื่อมีการกำหนดค่าอินเทอร์เฟซเครือข่ายการจัดการเพื่อใช้ Dynamic Host Configuration Protocol (DHCP) และเมื่อ Encapsulation เปิดใช้งาน การจัดการเซิร์ฟเวอร์ในแร็คอาจใช้เวลานาน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Encapsulation โปรดดู การเปิดใช้งาน Encapsulation ในเอกสารแบบออนไลน์ของ XClarity Administrator

การจัดการการเข้ารหัส

การจัดการการเข้ารหัสประกอบด้วยโหมดการสื่อสารและโปรโตคอลที่ควบคุมวิธีในการควบคุมการสื่อสารที่ปลอดภัยระหว่าง Lenovo XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ (เช่น ตัวเครื่อง เซิร์ฟเวอร์ และสวิตช์ Flex)

อัลกอริทึมการเข้ารหัส

XClarity Administrator รองรับ TLS 1.2 และอัลกอริทึมการเข้ารหัสที่รัดกุมมากขึ้นสำหรับการเชื่อมต่อเครือข่ายที่ปลอดภัย

รองรับการเข้ารหัสที่มีความรัดกุมสูงเท่านั้น เพื่อการรักษาความปลอดภัยที่ดียิ่งขึ้น ระบบปฏิบัติการไคลเอ็นต์และเว็บเบราเซอร์ต้องรองรับชุดการเข้ารหัสชุดใดชุดหนึ่งต่อไปนี้

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

โหมดการเข้ารหัสสำหรับเซิร์ฟเวอร์การจัดการ

การตั้งค่านี้จะกำหนดโหมดที่จะใช้สำหรับการสื่อสารที่มีความปลอดภัยจากเซิร์ฟเวอร์การจัดการ

- **ความเข้ากันได้ของ** นี่คือโหมดเริ่มต้น โหมดนี้เข้ากันได้กับเฟิร์มแวร์เวอร์ชันที่เก่ากว่า เบราเซอร์ และไคลเอ็นต์เครือข่ายอื่นๆ ที่ไม่ได้ใช้งานมาตรฐานการรักษาความปลอดภัยที่เข้มงวด ซึ่งจำเป็นเพื่อให้สอดคล้องตาม NIST SP 800-131A
- NIST SP 800-131A โหมดนี้ได้รับการออกแบบมาเพื่อให้สอดคล้องตามมาตรฐาน NIST SP 800-131A XClarity Administrator ได้รับการออกแบบมาให้ใช้การเข้ารหัสที่ปลอดภัยภายในระบบและที่ที่สามารถใช้ได้เสมอ เพื่อใช้การเชื่อมต่อเครือข่ายการเข้ารหัสที่ปลอดภัย อย่างไรก็ตาม ในโหมดนี้ ไม่อนุญาตให้มีการเชื่อมต่อเครือข่ายที่ใช้การเข้ารหัสที่ไม่ได้รับการอนุมัติโดย NIST SP 800-131A รวมถึงการปฏิเสธใบรับรอง Transport Layer Security (TLS) ที่ได้รับการลงนามด้วย SHA-1 หรือแฮชที่ประสิทธิภาพน้อยกว่า

  หากคุณเลือกโหมดนี้:

  - สำหรับพอร์ตทั้งหมดนอกเหนือจากพอร์ต 8443 การเข้ารหัส TLS CBC ทั้งหมดและการเข้ารหัสทั้งหมดที่ไม่รองรับ Perfect Forward Secrecy จะถูกปิดใช้งาน
  - ระบบอาจพุชการแจ้งเตือนเหตุการณ์ไปยังการสมัครรับข้อมูลอุปกรณ์เคลื่อนที่บางรายการไม่สำเร็จ (โปรดดู การส่งต่อเหตุการณ์ไปยังอุปกรณ์เคลื่อนที่ ในเอกสารแบบออนไลน์ของ XClarity Administrator) บริการภายนอก เช่น Android และ iOS จะแสดงใบรับรองที่ได้รับการลงนามด้วย SHA-1 ซึ่งเป็นอัลกอริทึมที่ไม่สอดคล้องตามข้อกำหนดของโหมด NIST SP 800-131A ที่เข้มงวดกว่า ดังนั้น การเชื่อมต่อไปยังบริการเหล่านี้อาจล้มเหลวเนื่องจากการยกเว้นด้านใบรับรองหรือความล้มเหลวของแฮนด์เชค

  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการปฏิบัติตาม NIST SP 800-131A โปรดดู การปฏิบัติตามข้อบังคับ NIST 800-131A ในเอกสารแบบออนไลน์ของ XClarity Administrator

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าโหมดการรักษาความปลอดภัยบนเซิร์ฟเวอร์การจัดการ โปรดดู การตั้งค่าโหมดการเข้ารหัสและโปรโตคอล การสื่อสาร ในเอกสารแบบออนไลน์ของ XClarity Administrator

โหมดการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ที่มีการจัดการ

การตั้งค่านี้จะกำหนดโหมดที่จะใช้สำหรับการสื่อสารที่มีความปลอดภัยจากเซิร์ฟเวอร์ที่มีการจัดการ

- **การรักษาความปลอดภัยแบบเข้ากันได้** เลือกโหมดนี้เมื่อบริการและไคลเอ็นต์ต้องการใช้การเข้ารหัสที่ไม่สอดคล้องตามมาตรฐาน CNSA/FIPS โหมดนี้รองรับอัลกอริทึมการเข้ารหัสที่หลากหลาย และอนุญาตให้มีการเปิดใช้งานบริการทั้งหมด
- NIST SP 800-131A เลือกโหมดนี้เพื่อให้สอดคล้องตามมาตรฐาน NIST SP 800-131A ซึ่งรวมถึงการจำกัดคีย์ RSA ไว้ที่ 2048 บิตหรือมากกว่า การจำกัดแฮชที่ใช้สำหรับลายเซ็นดิจิตอลให้เป็น SHA-256 หรือยาวกว่า และใช้เฉพาะอัลกอริทึมการเข้ารหัสแบบสมมาตรที่ NIST รับรองเท่านั้น โหมดนี้กำหนดให้ตั้งค่าโหมด SSL/TLS เป็น **TLS 1.2 Server Client**

  โหมดนี้ยัง*ไม่*รองรับบนเซิร์ฟเวอร์ที่มี XCC2

- **การรักษาความปลอดภัยมาตรฐาน** (เซิร์ฟเวอร์ที่มี XCC2 เท่านั้น) โหมดนี้เป็นโหมดการรักษาความปลอดภัยเริ่มต้นสำหรับ เซิร์ฟเวอร์ที่มี XCC2 เลือกโหมดนี้เพื่อให้สอดคล้องตามมาตรฐาน FIPS 140-3 เพื่อให้ XCC ดำเนินการในโหมดที่ผ่านมาตรฐาน FIPS 140-3 จะต้องเปิดใช้งานบริการที่รองรับการเข้ารหัสระดับ FIPS 140-3 เท่านั้น บริการที่ไม่รองรับการเข้ารหัสระดับ FIPS 140-2/140-3 ถูกปิดใช้งานตามค่าเริ่มต้น แต่สามารถเปิดใช้งานได้หากจำเป็นต้องใช้ หากมีการเปิดใช้งานบริการใดๆ ที่ใช้การเข้ารหัสที่ไม่ใช่ระดับ FIPS 140-3 XCC จะไม่สามารถดำเนินการในโหมดที่ผ่านมาตรฐาน FIPS 140-3 ได้ โหมดนี้ต้องใช้ใบรับรองระดับ FIP
- **การรักษาความปลอดภัยที่รัดกุมสำหรับองค์กร** (เซิร์ฟเวอร์ที่มี XCC2 เท่านั้น) โหมดนี้เป็นโหมดที่ปลอดภัยที่สุด เลือกโหมดนี้เพื่อให้สอดคล้องตามมาตรฐาน CNSA อนุญาตเฉพาะบริการที่รองรับการเข้ารหัสระดับ CNSA เท่านั้น บริการที่ไม่ปลอดภัยจะถูกปิดใช้งานตามค่าเริ่มต้นและไม่สามารถเปิดใช้งานได้ โหมดนี้ต้องใช้ใบรับรองระดับ CNSA

  XClarity Administrator ใช้ลายเซ็นใบรับรอง RSA-3072/SHA-384 ในเซิร์ฟเวอร์ในโหมด**การรักษาความปลอดภัยที่รัดกุมสำหรับองค์กร**

  ข้อสำคัญ:

  – ต้องติดตั้งคีย์คุณลักษณะตามต้องการของ XCC2 ในแต่ละ เซิร์ฟเวอร์ที่มี XCC2 ที่เลือกเพื่อใช้โหมดนี้

  – ในโหมดนี้ หาก XClarity Administrator ใช้ใบรับรองที่ลงนามด้วยตนเอง XClarity Administrator ต้องใช้ใบรับรองหลักและใบรับรองเซิร์ฟเวอร์ที่ใช้ RSA3072/SHA384 หาก XClarity Administrator ใช้ใบรับรองที่ลงนามภายนอก XClarity Administrator ต้องสร้าง CSR ที่ใช้ RSA3072/SHA384 based CSR และติดต่อภายนอกเพื่อลงนามใบรับรองเซิร์ฟเวอร์ใหม่ตาม RSA3072/SHA384

  – เมื่อ XClarity Administrator ใช้ใบรับรองที่ใช้ RSA3072/SHA384 XClarity Administrator อาจยกเลิกการเชื่อมต่ออุปกรณ์อื่นๆ นอกเหนือจากตัวเครื่อง Flex System (CMMS) และเซิร์ฟเวอร์, เซิร์ฟเวอร์ ThinkSystem, เซิร์ฟเวอร์ ThinkServer, เซิร์ฟเวอร์ System x M4 และ M5, สวิตช์ Lenovo ThinkSystem DB Series, Lenovo RackSwitch, สวิตช์ Flex System, สวิตช์ Mellanox, อุปกรณ์จัดเก็บ ThinkSystem DE/DM, ไลบรารีเทปเทป IBM และเซิร์ฟเวอร์ ThinkSystem SR635/SR655 ที่แฟลชด้วยเฟิร์มแวร์เวอร์ชันก่อน 22C หากต้องการจัดการอุปกรณ์ที่ถูกตัดการเชื่อมต่อต่อไป ให้ตั้งค่าอินสแตนซ์ XClarity Administrator อื่นด้วยใบรับรองที่ใช้ RSA2048/SHA384

พิจารณาความเกี่ยวข้องของการเปลี่ยนแปลงโหมดการเข้ารหัสต่อไปนี้

- ไม่รองรับการเปลี่ยนจากโหมด **การรักษาความปลอดภัยแบบเข้ากันได้** หรือโหมด **การรักษาความปลอดภัยมาตรฐาน** เป็นโหมด **การรักษาความปลอดภัยที่รัดกุมสำหรับองค์กร**
- หากคุณอัปเกรดจากโหมด **การรักษาความปลอดภัยแบบเข้ากันได้** เป็นโหมด **การรักษาความปลอดภัยมาตรฐาน** คุณจะได้รับการแจ้งเตือน หากใบรับรองที่นำเข้าหรือคีย์สาธารณะ SSH ไม่สอดคล้องตามมาตรฐาน แต่คุณยังคงสามารถอัปเกรดเป็นโหมด **การรักษาความปลอดภัยมาตรฐาน** ได้
- หากคุณดาวน์เกรดจากโหมด **การรักษาความปลอดภัยที่รัดกุมสำหรับองค์กร** เป็นโหมด **การรักษาความปลอดภัยแบบเข้ากันได้** หรือโหมด **การรักษาความปลอดภัยมาตรฐาน**:

  - เซิร์ฟเวอร์จะรีสตาร์ทโดยอัตโนมัติเพื่อให้โหมดการรักษาความปลอดภัยมีผล
  - หากคีย์ FoD โหมดรัดกุมขาดหายไปหรือหมดอายุใน XCC2 และหาก XCC2 ใช้ใบรับรอง TLS ที่ลงนามด้วยตนเอง XCC2 จะสร้างใบรับรอง TLS ที่ลงนามด้วยตนเองขึ้นมาใหม่โดยอ้างอิงจากอัลกอริทึมที่สอดคล้องตามมาตรฐานแบบรัดกุม XClarity Administrator แสดงความล้มเหลวในการเชื่อมต่อเนื่องจากข้อผิดพลาดของใบรับรอง ในการแก้ไขปัญหาข้อผิดพลาดของใบรับรองที่ไม่น่าเชื่อถือ โปรดดู การแก้ปัญหาใบรับรองเซิร์ฟเวอร์ที่ไม่น่าเชื่อถือ ในเอกสารแบบออนไลน์ของ XClarity Administrator หาก XCC2 ใช้ใบรับรอง TLS ที่กำหนดเอง XCC2 จะอนุญาตให้ดาวน์เกรด และเตือนคุณว่าคุณต้องนำเข้าใบรับรองเซิร์ฟเวอร์ที่ใช้การเข้ารหัสโหมด **การรักษาความปลอดภัยมาตรฐาน**
- โหมด NIST SP 800-131A ไม่รองรับบนเซิร์ฟเวอร์ที่มี XCC2
- หากมีการตั้งค่าโหมดการเข้ารหัสสำหรับ XClarity Administrator เป็น TLS v1.2 และหากเซิร์ฟเวอร์ที่มีการจัดการที่ใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการมีการตั้งค่าโหมดการรักษาความปลอดภัยเป็น TLS v1.3 การเปลี่ยนโหมดการรักษาความปลอดภัยของเซิร์ฟเวอร์เป็น TLS v1.3 โดยใช้ XClarity Administrator หรือ XCC จะทำให้เซิร์ฟเวอร์ออฟไลน์แบบถาวร
- หากมีการตั้งค่าโหมดการเข้ารหัสสำหรับ XClarity Administrator เป็น TLS v1.2 และคุณพยายามจัดการเซิร์ฟเวอร์ด้วย XCC ที่มีการตั้งค่าโหมดการรักษาความปลอดภัยเป็น TLS v1.3 คุณจะไม่สามารถจัดการเซิร์ฟเวอร์โดยใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการได้

คุณสามารถเปลี่ยนการตั้งค่าการรักษาความปลอดภัยของอุปกรณ์ต่อไปนี้ได้

- เซิร์ฟเวอร์ Lenovo ThinkSystem ที่มีโปรเซสเซอร์ Intel หรือ AMD (ยกเว้น SR635 / SR655)
- เซิร์ฟเวอร์ Lenovo ThinkSystem V2
- เซิร์ฟเวอร์ Lenovo ThinkSystem V3 ที่มีโปรเซสเซอร์ Intel หรือ AMD
- เซิร์ฟเวอร์ Lenovo ThinkEdge SE350 / SE450
- เซิร์ฟเวอร์ Lenovo System x

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าโหมดการรักษาความปลอดภัยบนเซิร์ฟเวอร์ที่มีการจัดการ โปรดดู การกำหนดค่าการตั้งค่าการรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์ ในเอกสารแบบออนไลน์ของ XClarity Administrator

ใบรับรองด้านความปลอดภัย

Lenovo XClarity Administrator ใช้ใบรับรอง SSL ในการสร้างการสื่อสารที่ปลอดภัยและน่าเชื่อถือระหว่าง XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ (เช่น ตัวเครื่องและโปรเซสเซอร์การบริการในเซิร์ฟเวอร์ System x) รวมถึงการสื่อสารกับ XClarity Administrator โดยผู้ใช้ หรือกับบริการอื่นๆ ตามค่าเริ่มต้น XClarity Administrator, CMM และตัวควบคุมการจัดการจะใช้ใบรับรองที่สร้างโดย XClarity Administrator ที่ลงนามด้วยตนเองและออกให้โดยหน่วยงานด้านใบรับรองภายใน

ใบรับรองเซิร์ฟเวอร์ที่ลงนามด้วยตนเองเริ่มต้น ซึ่งถูกสร้างขึ้นโดยไม่ซ้ำกันในทุกอินสแตนซ์ของ XClarity Administrator จะมอบการรักษาความปลอดภัยที่เพียงพอสำหรับสภาพแวดล้อมต่างๆ มากมาย คุณสามารถเลือกที่จะให้ XClarity Administrator จัดการใบรับรองให้คุณ หรือคุณสามารถรับบทบาทที่ใช้งานอยู่เพิ่มเติมและเปลี่ยนหรือกำหนดใบรับรองเซิร์ฟเวอร์เอง XClarity Administrator จะให้ตัวเลือกสำหรับการกำหนดใบรับรองเองสำหรับสภาพแวดล้อมของคุณ ตัวอย่างเช่น คุณสามารถเลือก:

- สร้างคีย์คู่ใหม่โดยการสร้างผู้ให้บริการออกใบรับรองภายในและ/หรือใบรับรองเซิร์ฟเวอร์ปลายทางขึ้นมาใหม่ที่ใช้ค่าที่เฉพาะเจาะจงกับองค์กรของคุณ
- สร้างคำขอการลงนามใบรับรอง (CSR) ที่สามารถส่งไปยังผู้ให้บริการออกใบรับรองที่คุณเลือกเพื่อลงนามใบรับรองที่กำหนดเอง ซึ่งสามารถอัปโหลดไปยัง XClarity Administrator เพื่อใช้เป็นใบรับรองเซิร์ฟเวอร์ปลายทางสำหรับบริการที่โฮสต์ทั้งหมด
- ดาวน์โหลดใบรับรองเซิร์ฟเวอร์ไปยังระบบภายในเพื่อให้คุณสามารถนำเข้าใบรับรองนั้นลงในรายการใบรับรองที่เชื่อถือได้ของเว็บเบราเซอร์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับใบรับรอง โปรดดู การทำงานกับใบรับรองด้านความปลอดภัย ในเอกสารแบบออนไลน์ของ XClarity Administrator

การตรวจสอบความถูกต้อง

เซิร์ฟเวอร์ตรวจสอบความถูกต้องที่รองรับ

เซิร์ฟเวอร์ตรวจสอบความถูกต้อง คือรีจิสทรีผู้ใช้ที่ใช้ในการตรวจสอบความถูกต้องของข้อมูลประจำตัวผู้ใช้ Lenovo XClarity Administrator รองรับเซิร์ฟเวอร์ตรวจสอบความถูกต้องต่อไปนี้

- **เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายใน** ตามค่าเริ่มต้น XClarity Administrator ได้รับการกำหนดค่าให้ใช้เซิร์ฟเวอร์ Lightweight Directory Access Protocol (LDAP) ที่อยู่ในเซิร์ฟเวอร์การจัดการ
- **เซิร์ฟเวอร์ LDAP ภายนอก** ปัจจุบัน รองรับเฉพาะ Microsoft Active Directory และ OpenLDAP เท่านั้น เซิร์ฟเวอร์เครื่องนี้จะต้องอยู่บนเซิร์ฟเวอร์ Microsoft Windows ภายนอกที่เชื่อมต่อกับเครือข่ายการจัดการ เมื่อใช้เซิร์ฟเวอร์ LDAP ภายนอก จะต้องปิดใช้งานเซิร์ฟเวอร์ตรวจสอบความถูกต้องภายใน

  ข้อควรพิจารณา: เพื่อกำหนดค่าวิธีการผูก Active Directory โดยใช้ข้อมูลประจำตัว ตัวควบคุมการจัดการแผงวงจรสำหรับเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่องจะต้องใช้เฟิร์มแวร์ตั้งแต่เดือนกันยายน 2016 ขึ้นไป
- **ระบบการจัดการข้อมูลประจำตัวภายนอก** ขณะนี้ ระบบรองรับเฉพาะ CyberArk เท่านั้น

  หากบัญชีผู้ใช้สำหรับเซิร์ฟเวอร์ ThinkSystem หรือ ThinkAgile ถูกออนบอร์ดลงบน CyberArk คุณสามารถเลือกที่จะให้ XClarity Administrator เรียกใช้ข้อมูลประจำตัวจาก CyberArk เพื่อเข้าสู่ระบบเซิร์ฟเวอร์เมื่อตั้งค่าเซิร์ฟเวอร์สำหรับการจัดการครั้งแรก (ด้วยการตรวจสอบความถูกต้องที่ได้รับการจัดการหรือแบบภายในเครื่อง) ก่อนที่จะสามารถดึงข้อมูลประจำตัวจาก CyberArk ได้ ต้องกำหนดพาธ CyberArk ใน XClarity Administrator และต้อง

สร้างความน่าเชื่อถือร่วมระหว่าง CyberArk และ XClarity Administrator โดยใช้การตรวจสอบความถูกต้องร่วมของ TLS ผ่านใบรับรองไคลเอ็นต์

- **SAML ภายนอก ผู้ให้บริการข้อมูลประจำตัว** ขณะนี้ รองรับเฉพาะ Microsoft Active Directory Federation Services (AD FS) นอกจากการป้อนชื่อผู้ใช้และรหัสผ่านแล้ว ยังสามารถตั้งค่าการตรวจสอบความถูกต้องแบบหลายปัจจัยได้ เพื่อเปิดใช้งานการรักษาความปลอดภัยเพิ่มเติม โดยต้องใช้รหัส PIN การอ่านสมาร์ทการ์ด และใบรับรองไคลเอ็นต์ เมื่อใช้ SAML ผู้ให้บริการข้อมูลประจำตัว เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายในไม่ถูกปิดใช้งาน จำเป็นต้องใช้บัญชีผู้ใช้ภายในระบบเพื่อเข้าสู่ระบบตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการโดยตรง (เว้นแต่จะมีการเปิดใช้งาน Encapsulation บนอุปกรณ์) สำหรับการตรวจสอบความถูกต้องของ PowerShell และ REST API และสำหรับการกู้คืน หากไม่มีการตรวจสอบความถูกต้องภายนอก

  คุณสามารถเลือกใช้ได้ทั้งเซิร์ฟเวอร์ LDAP ภายนอกและ ผู้ให้บริการข้อมูลประจำตัว ภายนอก หากเปิดใช้งานทั้งคู่ เซิร์ฟเวอร์ LDAP ภายนอกจะใช้ในการเข้าสู่ระบบอุปกรณ์ที่ได้รับการจัดการโดยตรง และ ผู้ให้บริการข้อมูลประจำตัว จะใช้ในการเข้าสู่ระบบเซิร์ฟเวอร์การจัดการ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเซิร์ฟเวอร์ตรวจสอบความถูกต้อง โปรดดู การจัดการเซิร์ฟเวอร์การตรวจสอบความถูกต้อง ในเอกสารแบบออนไลน์ของ XClarity Administrator

การตรวจสอบความถูกต้องอุปกรณ์

ตามค่าเริ่มต้น อุปกรณ์ได้รับการจัดการโดยใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการ XClarity Administrator ในการเข้าสู่ระบบอุปกรณ์ เมื่อจัดการเซิร์ฟเวอร์ในแร็คและตัวเครื่อง Lenovo คุณสามารถเลือกใช้การตรวจสอบความถูกต้องภายในเครื่องหรือการตรวจสอบความถูกต้องที่ได้รับการจัดการในการเข้าสู่ระบบอุปกรณ์

- เมื่อใช้*การตรวจสอบความถูกต้องภายในเครื่อง*สำหรับเซิร์ฟเวอร์ในแร็ค ตัวเครื่อง Lenovo และสวิตช์ในแร็คของ Lenovo XClarity Administrator จะใช้ข้อมูลประจำตัวที่จัดเก็บไว้เพื่อตรวจสอบความถูกต้องกับอุปกรณ์ *ข้อมูลประจำตัวที่จัดเก็บไว้*อาจเป็นบัญชีผู้ใช้ที่ใช้งานบนอุปกรณ์หรือบัญชีผู้ใช้ใน Active Directory

  คุณต้องสร้างข้อมูลประจำตัวที่จัดเก็บไว้ใน XClarity Administrator ที่ตรงกับบัญชีผู้ใช้ที่ใช้งานอยู่บนอุปกรณ์ หรือบัญชีผู้ใช้ในเซิร์ฟเวอร์ Active Directory ก่อนจัดการอุปกรณ์โดยใช้การตรวจสอบความถูกต้องภายในเครื่อง (โปรดดู การจัดการข้อมูลประจำตัวที่จัดเก็บไว้ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

  หมายเหตุ:

  – อุปกรณ์ RackSwitch รองรับเฉพาะข้อมูลประจำตัวที่จัดเก็บไว้สำหรับการตรวจสอบความถูกต้อง ทั้งนี้ ข้อมูลประจำตัวผู้ใช้ของ XClarity Administrator จะไม่ได้รับการสนับสนุน
- การใช้*การตรวจสอบความถูกต้องที่ได้รับการจัดการ* ช่วยให้คุณสามารถจัดการ และตรวจสอบอุปกรณ์หลายเครื่องได้โดยใช้ข้อมูลประจำตัวในเซิร์ฟเวอร์ตรวจสอบความถูกต้อง XClarity Administrator แทนข้อมูลประจำตัวภายในเครื่อง เมื่อมีการใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ (นอกเหนือจากเซิร์ฟเวอร์ ThinkServer, System x M4, และสวิตช์) XClarity Administrator จะกำหนดค่าอุปกรณ์และส่วนประกอบที่ติดตั้งเพื่อใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator สำหรับการจัดการส่วนกลาง

- เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการ คุณจะสามารถจัดการอุปกรณ์โดยใช้ข้อมูลประจำตัวที่ป้อนเองหรือข้อมูลประจำตัวที่จัดเก็บไว้ก็ได้ (โปรดดู การจัดการบัญชีผู้ใช้ และ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

  ข้อมูลประจำตัวที่จัดเก็บไว้จะถูกใช้จนกว่า XClarity Administrator จะกำหนดค่าการตั้งค่า LDAP บนอุปกรณ์ หลังจากนั้น การเปลี่ยนแปลงใดๆ กับข้อมูลประจำตัวที่จัดเก็บไว้จะไม่ส่งผลต่อการจัดการหรือการตรวจสอบของอุปกรณ์นั้น

  หมายเหตุ: เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ คุณจะไม่สามารถแก้ไขข้อมูลประจำตัวที่จัดเก็บไว้สำหรับอุปกรณ์นั้นโดยใช้ XClarity Administrator
- หากมีการใช้เซิร์ฟเวอร์ LDAP ภายในหรือภายนอกเป็นเซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator จะใช้บัญชีผู้ใช้ที่กำหนดไว้ในเซิร์ฟเวอร์ตรวจสอบความถูกต้องในการเข้าสู่ระบบ XClarity Administrator, CMM และตัวควบคุมการจัดการแผงวงจรในโดเมน XClarity Administrator บัญชีผู้ใช้ CMM และตัวควบคุมการจัดการภายในจะถูกปิดใช้งาน
- หากมีการใช้ผู้ให้บริการข้อมูลประจำตัว SAML 2.0 เป็นเซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator บัญชี SAML จะไม่สามารถเข้าถึงอุปกรณ์ที่ได้รับการจัดการ อย่างไรก็ตาม เมื่อใช้ทั้งผู้ให้บริการข้อมูลประจำตัว SAML และเซิร์ฟเวอร์ LDAP ร่วมกัน หากผู้ให้บริการข้อมูลประจำตัวใช้บัญชีที่มีอยู่ในเซิร์ฟเวอร์ LDAP บัญชีผู้ใช้ LDAP สามารถใช้ในการเข้าสู่ระบบอุปกรณ์ที่ได้รับการจัดการ ขณะที่วิธีการตรวจสอบความถูกต้องขั้นสูงเพิ่มเติมที่มีให้โดย SAML 2.0 (เช่น การตรวจสอบความถูกต้องแบบหลายปัจจัยและการลงชื่อเข้าใช้ครั้งเดียว) สามารถใช้ในการเข้าสู่ระบบ XClarity Administrator
- การเข้าสู่ระบบแบบครั้งเดียวอนุญาตให้ผู้ใช้ที่เข้าสู่ระบบ XClarity Administrator อยู่แล้ว เข้าสู่ระบบตัวควบคุมการจัดการแผงวงจรโดยอัตโนมัติ การเข้าสู่ระบบแบบครั้งเดียวจะเปิดใช้งานตามค่าเริ่มต้นเมื่อเซิร์ฟเวอร์ ThinkSystem หรือ ThinkAgile ถูกนำเข้าสู่การจัดการโดย XClarity Administrator (เว้นแต่เซิร์ฟเวอร์จะจัดการด้วยรหัสผ่าน CyberArk) คุณสามารถกำหนดค่าการตั้งค่าส่วนกลางเพื่อเปิดใช้งานหรือปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวกับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ที่มีการจัดการทั้งหมดได้ การเปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวสำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile บางเครื่องจะแทนที่การตั้งค่าส่วนกลางของเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ทั้งหมด (ดู การจัดการเซิร์ฟเวอร์ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

  หมายเหตุ: การเข้าสู่ระบบแบบครั้งเดียวจะถูกปิดใช้งานโดยอัตโนมัติเมื่อใช้ระบบการจัดการข้อมูลประจำตัวของ CyberArk สำหรับการตรวจสอบความถูกต้อง
- เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับเซิร์ฟเวอร์ ThinkSystem SR635 และ SR655:
  - เฟิร์มแวร์ของตัวควบคุมการจัดการแผงวงจรรองรับบทบาทผู้ใช้ LDAP สูงสุดห้าบทบาท XClarity Administrator เพิ่มบทบาทผู้ใช้ LDAP เหล่านี้ไปยังเซิร์ฟเวอร์ระหว่างการจัดการ: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** และ **lxc-os-admin**

ผู้ใช้ต้องได้รับการกำหนดบทบาทผู้ใช้ LDAP ที่ระบุอย่างน้อยหนึ่งบทบาทเพื่อสื่อสารกับเซิร์ฟเวอร์ ThinkSystem SR635 และ SR655

  - เฟิร์มแวร์ของตัวควบคุมการจัดการไม่รองรับผู้ใช้ LDAP ที่มีชื่อผู้ใช้เดียวกันกับผู้ใช้ภายในของเซิร์ฟเวอร์

- สำหรับเซิร์ฟเวอร์ ThinkServer และ System x M4 จะไม่ใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator แต่บัญชี IPMI จะถูกสร้างขึ้นบนอุปกรณ์ที่มีคำนำหน้า “LXCA_” ตามด้วยสตริงแบบสุ่ม (บัญชีผู้ใช้ IPMI ในระบบที่มีอยู่ไม่ถูกปิดใช้งาน) เมื่อคุณถอนการจัดการเซิร์ฟเวอร์ ThinkServer ระบบจะปิดการใช้งานบัญชีผู้ใช้ “LXCA_” และคำนำหน้า “LXCA_” จะถูกแทนที่ด้วย “DISABLED_” ในการระบุว่าเซิร์ฟเวอร์ ThinkServer ได้รับการจัดการโดยอินสแตนซ์อื่นหรือไม่ XClarity Administrator จะตรวจหาบัญชี IPMI ที่มีคำนำหน้า “LXCA_” หากคุณเลือกบังคับการจัดการของเซิร์ฟเวอร์ ThinkServer ที่ได้รับการจัดการ ระบบจะปิดการใช้งานและเปลี่ยนชื่อบัญชี IPMI ทั้งหมดบนอุปกรณ์ที่มีคำนำหน้า “LXCA_” พิจารณาล้างข้อมูลบัญชี IPMI ที่ไม่ได้ใช้งานอีกต่อไปด้วยตนเอง

  หากคุณใช้ข้อมูลประจำตัวที่ป้อนเอง XClarity Administrator จะสร้างข้อมูลประจำตัวสำหรับที่จัดเก็บไว้โดยอัตโนมัติ และใช้ข้อมูลประจำตัวที่จัดเก็บไว้นั้นเพื่อจัดการอุปกรณ์

  หมายเหตุ: เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ คุณจะไม่สามารถแก้ไขข้อมูลประจำตัวที่จัดเก็บไว้สำหรับอุปกรณ์นั้นโดยใช้ XClarity Administrator

  - ทุกครั้งที่คุณจัดการอุปกรณ์โดยใช้ข้อมูลประจำตัวที่ป้อนด้วยตนเอง ข้อมูลประจำตัวสำหรับจัดเก็บใหม่จะถูกสร้างขึ้นสำหรับอุปกรณ์นั้น แม้ว่าได้สร้างข้อมูลประจำตัวสำหรับจัดเก็บสำหรับอุปกรณ์นั้นแล้วระหว่างกระบวนการจัดการก่อนหน้า
  - เมื่อคุณถอนการจัดการอุปกรณ์ XClarity Administrator จะไม่ลบข้อมูลประจำตัวที่จัดเก็บไว้ซึ่งถูกสร้างขึ้นโดยอัตโนมัติสำหรับอุปกรณ์นั้นในระหว่างกระบวนการจัดการ

บัญชีผู้ใช้ในการกู้คืน

หากคุณระบุรหัสผ่านในการกู้คืน XClarity Administrator จะปิดการใช้งานบัญชีผู้ใช้ CMM ภายในหรือบัญชีผู้ใช้ตัวควบคุมการจัดการ และสร้างบัญชีผู้ใช้ในการกู้คืนใหม่ (`RECOVERY_ID`) บนอุปกรณ์สำหรับการตรวจสอบความถูกต้องในอนาคต หากเซิร์ฟเวอร์การจัดการล้มเหลว คุณสามารถใช้บัญชี `RECOVERY_ID` ในการเข้าสู่ระบบอุปกรณ์สำหรับดำเนินการกู้คืนเพื่อคืนค่าฟังก์ชันการจัดการบัญชีบนอุปกรณ์ได้ จนกว่าโหนดการจัดการจะได้รับการจัดการหรือแทนที่

หากคุณถอนการจัดการอุปกรณ์ที่มีบัญชีผู้ใช้ `RECOVERY_ID` ระบบจะเปิดใช้งานบัญชีผู้ใช้ภายในทั้งหมด และบัญชี `RECOVERY_ID` จะถูกลบ

- หากคุณเปลี่ยนบัญชีผู้ใช้ภายในที่ปิดใช้งานอยู่ (เช่น เปลี่ยนรหัสผ่าน) การเปลี่ยนแปลงเหล่านั้นจะไม่มีผลต่อบัญชี `RECOVERY_ID` ในโหมดการตรวจสอบความถูกต้องที่ได้รับการจัดการ บัญชี `RECOVERY_ID` เป็นเพียงบัญชีผู้ใช้เดียวที่เปิดใช้งานและทำงานได้
- ใช้บัญชี `RECOVERY_ID` เฉพาะในกรณีฉุกเฉินเท่านั้น ตัวอย่างเช่น หากเซิร์ฟเวอร์การจัดการล้มเหลว หรือหากปัญหาด้านเครือข่ายป้องกันไม่ให้อุปกรณ์สื่อสารกับ XClarity Administrator เพื่อตรวจสอบความถูกต้องของผู้ใช้

- มีการระบุรหัสผ่าน `RECOVERY_ID` เมื่อคุณค้นหาอุปกรณ์ ตรวจสอบว่าคุณบันทึกรหัสผ่านสำหรับการใช้งานในภายหลัง

สำหรับข้อมูลเกี่ยวกับการกู้คืนการจัดการอุปกรณ์ โปรดดู การกู้คืนการจัดการตัวเครื่องด้วย CMM ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว และ การกู้คืนการจัดการแร็คเซิร์ฟเวอร์หรือเซิร์ฟเวอร์แบบทาวเวอร์ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว ในเอกสารแบบออนไลน์ของ XClarity Administrator

บัญชีผู้ใช้และกลุ่มบทบาท

บัญชีผู้ใช้ จะใช้ในการเข้าสู่ระบบและจัดการ Lenovo XClarity Administrator และตัวเครื่องและเซิร์ฟเวอร์ที่ได้รับการจัดการทั้งหมด บัญชีผู้ใช้ XClarity Administrator อยู่ภายใต้กระบวนการที่พึ่งพากันสองกระบวนการ: การตรวจสอบความถูกต้องและการอนุญาต

การตรวจสอบความถูกต้อง เป็นกลไกด้านการรักษาความปลอดภัยที่มีการตรวจสอบข้อมูลประจำตัวของผู้ใช้ กระบวนการตรวจสอบความถูกต้องจะใช้ข้อมูลประจำตัวของผู้ใช้ที่จัดเก็บในเซิร์ฟเวอร์ตรวจสอบความถูกต้องที่กำหนดค่าไว้ ซึ่งยังป้องกันไม่ให้เซิร์ฟเวอร์การจัดการที่ไม่ได้รับอนุญาตหรือแอปพลิเคชันระบบที่ได้รับการจัดการอย่างหลอกลวงเข้าถึงทรัพยากร หลังการตรวจสอบความถูกต้อง ผู้ใช้สามารถเข้าถึง XClarity Administrator ได้ อย่างไรก็ตาม ในการเข้าถึงทรัพยากรเฉพาะหรือดำเนินงานเฉพาะ ผู้ใช้ยังต้องมีการตรวจสอบความถูกต้องที่เหมาะสม

การอนุญาต จะตรวจสอบสิทธิ์ของผู้ใช้ที่ได้รับการตรวจสอบความถูกต้อง และควบคุมการเข้าถึงทรัพยากรโดยยึดตามความเป็นสมาชิกของผู้ใช้ในกลุ่มบทบาท *กลุ่มบทบาท* ใช้ในการกำหนดบทบาทเฉพาะให้กับชุดบัญชีผู้ใช้ที่กำหนดและได้รับการจัดการในเซิร์ฟเวอร์ตรวจสอบความถูกต้อง ตัวอย่างเช่น หากผู้ใช้เป็นสมาชิกของกลุ่มบทบาทที่มีสิทธิ์ระดับผู้ควบคุม ผู้ใช้รายนั้นสามารถสร้าง แก้ไข และลบบัญชีผู้ใช้ออกจาก XClarity Administrator หากผู้ใช้มีสิทธิ์ระดับผู้ดำเนินการ ผู้ใช้รายนั้นสามารถดูข้อมูลบัญชีผู้ใช้ได้เท่านั้น

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับบัญชีผู้ใช้และกลุ่มบทบาท โปรดดู การจัดการบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ XClarity Administrator

การรักษาความปลอดภัยบัญชีผู้ใช้

การตั้งค่าบัญชีผู้ใช้จะควบคุมความซับซ้อนของรหัสผ่าน การล็อคบัญชี และการหมดเวลาของเว็บเซสชันที่ไม่ใช้งาน คุณสามารถเปลี่ยนค่าของการตั้งค่าการรักษาความปลอดภัยบัญชี:

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าการรักษาความปลอดภัยบัญชี โปรดดู การเปลี่ยนการตั้งค่าการรักษาความปลอดภัยของบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ Lenovo XClarity Administrator

ข้อควรพิจารณาด้านความพร้อมใช้งานสูง

เพื่อตั้งค่าความพร้อมใช้งานสูงสำหรับ Lenovo XClarity Administrator ให้ใช้คุณลักษณะความพร้อมใช้งานสูงที่เป็นส่วนหนึ่งของระบบปฏิบัติการโฮสต์ หรือสภาพแวดล้อมของคอนเทนเนอร์

Docker

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ XClarity Administrator ที่ใช้ Docker Engine สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

Citrix

ใช้ฟังก์ชันความพร้อมใช้งานสูงที่จัดให้สำหรับสภาพแวดล้อม Citrix สำหรับข้อมูลเพิ่มเติม โปรดดู การใช้งานความพร้อมใช้งานสูง (Citrix) ในเอกสารแบบออนไลน์ของ XClarity Administrator

KVM (CentOS, RedHat และ Ubuntu)

คุณสามารถใช้ OpenStack หรือหากคุณมีระบบความพร้อมใช้งานสูงอยู่แล้ว ให้คุณใช้กระบวนการภายในของคุณต่อไปได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ OpenStack โปรดดู การใช้งานความพร้อมใช้งานสูง (KVM) ในเอกสารแบบออนไลน์ของ XClarity Administrator

Microsoft Hyper-V

ใช้ฟังก์ชันความพร้อมใช้งานสูงที่จัดให้สำหรับระบบ ESXi สำหรับข้อมูล โปรดดู การนำความพร้อมใช้งานสูงมาใช้งาน (Microsoft Hyper-V) ในเอกสารแบบออนไลน์ของ XClarity Administrator

Nutanix AHV

ใช้ฟังก์ชันความพร้อมใช้งานสูงของเครื่องเสมือนที่จัดให้สำหรับระบบ Nutanix AHV สำหรับข้อมูลเพิ่มเติม โปรดดู การใช้งานความพร้อมใช้งานสูง (Nutanix) ในเอกสารแบบออนไลน์ของ XClarity Administrator

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 บนโฮสต์ที่จะใช้ในคลัสเตอร์ได้ อย่างไรก็ตาม หากโฮสต์นั้นปิดเครื่องหรือใช้งานไม่ได้ คุณจะเสียการเข้าถึงอินเทอร์เฟซ VMware vCenter ไปด้วย

- ที่จัดเก็บข้อมูลร่วม (ที่จัดเก็บข้อมูล) ที่โฮสต์ทุกตัวในคลัสเตอร์สามารถเข้าถึงได้ คุณสามารถใช้ที่จัดเก็บข้อมูลร่วมประเภทใดก็ได้ที่ VMware รองรับ ที่จัดเก็บข้อมูลจะถูกใช้โดย VMware เพื่อระบุว่า VM ควรจะเปลี่ยนไปยังโฮสต์อื่นหรือไม่ในกรณีล้มเหลว (การตรวจสอบการทำงาน)

สำหรับรายละเอียดเกี่ยวกับการตั้งค่าคลัสเตอร์ของ VMware High Availability โปรดดู การนำความพร้อมใช้งานสูงมาใช้งาน (VMware ESXi) ในเอกสารแบบออนไลน์ของ XClarity Administrator

---

คุณลักษณะตามต้องการ

คุณลักษณะตามต้องการ เปิดใช้งานคุณลักษณะโดยไม่จำเป็นต้องติดตั้งฮาร์ดแวร์หรือซื้ออุปกรณ์ใหม่ การเปิดใช้งานดังกล่าวทำได้โดยการขอรับและติดตั้งคีย์ คุณลักษณะตามต้องการ ที่เกี่ยวข้อง

หากต้องการใช้การควบคุมระยะไกลและการดำเนินการปรับใช้ระบบปฏิบัติการใน Lenovo XClarity Administrator คุณต้องเปิดใช้งานการอัปเกรดขั้นสูงระดับ XClarity Controller ระดับองค์กร หรือ MM สำหรับเซิร์ฟเวอร์ที่ไม่ได้มาพร้อมกับคุณลักษณะเหล่านี้ที่เปิดการใช้งานแล้วตามค่าเริ่มต้น และการดำเนินการเหล่านี้ยังกำหนดอีกว่าต้องติดตั้งคีย์คุณลักษณะตามต้องการ สำหรับ Remote Presence บนเซิร์ฟเวอร์ ThinkSystem, Converged และ System x ด้วย คุณสามารถกำหนดได้ว่าให้เปิดใช้งาน ปิดใช้งาน หรือไม่ติดตั้ง Remote Presence บนเซิร์ฟเวอร์จากหน้าเซิร์ฟเวอร์ (โปรดดู การดูสถานะของเซิร์ฟเวอร์ที่มีการจัดการ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

ฟังก์ชันขั้นสูงของเซิร์ฟเวอร์บางอย่างเปิดใช้งานโดยใช้คีย์ คุณลักษณะตามต้องการ หากคุณลักษณะมีการตั้งค่าที่กำหนดค่าได้ที่แสดงระหว่างการตั้งค่า UEFI คุณสามารถกำหนดค่าการตั้งค่าได้โดยใช้ รูปแบบการกำหนดค่า อย่างไรก็ตาม กำหนดค่าที่ได้รับจะยังไม่เปิดใช้งานจนกว่าจะติดตั้งคีย์ คุณลักษณะตามต้องการ ที่เกี่ยวข้อง

หมายเหตุ: คุณไม่สามารถติดตั้งหรือจัดการคีย์ คุณลักษณะตามต้องการ จาก XClarity Administrator อย่างไรก็ตาม คุณสามารถดูรายการคีย์ คุณลักษณะตามต้องการ ที่กำลังติดตั้งอยู่บนเซิร์ฟเวอร์ที่ได้รับการจัดการได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการดูคีย์ คุณลักษณะตามต้องการ ที่ติดตั้ง โปรดดู การดูคีย์คุณลักษณะตามต้องการ ในเอกสารแบบออนไลน์ของ XClarity Administrator

การขอรับและติดตั้งคีย์ คุณลักษณะตามต้องการ:

1. ซื้อการอัปเกรด คุณลักษณะตามต้องการ โดยใช้หมายเลขชิ้นส่วนที่เหมาะสม

   คุณสามารถซื้อคีย์ได้จาก เว็บพอร์ทัลคุณลักษณะตามต้องการ เมื่อทำการซื้อเสร็จสิ้นแล้ว คุณจะได้รับรหัสการอนุญาตทางอีเมล

2. บน เว็บพอร์ทัลคุณลักษณะตามต้องการ ป้อนรหัสการอนุญาตที่คุณได้รับ รวมทั้งตัวระบุระบบที่ไม่ซ้ำกันของเซิร์ฟเวอร์ที่คุณต้องการอัปเกรด
3. ดาวน์โหลดคีย์การเปิดใช้งานในรูปแบบของไฟล์ .KEY
4. อัปโหลดคีย์การเปิดใช้งานไปยังตัวควบคุมการจัดการสำหรับเซิร์ฟเวอร์
5. เริ่มระบบเซิร์ฟเวอร์อีกครั้ง เมื่อรีสตาร์ทเรียบร้อยแล้ว คุณลักษณะจะถูกเปิดใช้งาน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับคีย์ คุณลักษณะตามต้องการ โปรดดู การใช้งานคุณลักษณะตามต้องการของ Lenovo

บทที่ 3. การติดตั้ง Lenovo XClarity Administrator

มีอยู่ด้วยกันหลายวิธีเพื่อเชื่อมต่ออุปกรณ์ที่สามารถจัดการได้กับเครือข่าย และเพื่อตั้งค่าในอุปกรณ์เสมือน Lenovo XClarity Administrator เพื่อจัดการอุปกรณ์เหล่านั้น ใช้ข้อมูลในส่วนนี้เพื่อเป็นคู่มือการตั้งค่าอุปกรณ์ที่สามารถจัดการได้และติดตั้ง XClarity Administrator

ส่วนนี้อธิบายวิธีการตั้งค่าโทโพโลยีทั่วไปต่างๆ ส่วนนี้ไม่ครอบคลุมโทโพโลยีเครือข่ายทุกอย่างที่ใช้ได้

ข้อควรพิจารณา: ในการจัดการอุปกรณ์ XClarity Administrator ต้องสามารถเข้าถึงเครือข่ายการจัดการ

เรียนรู้เพิ่มเติม:

-  การติดตั้ง Lenovo XClarity Administrator บน VMware vCenter
-  การติดตั้ง Lenovo XClarity Administrator บน VMware vSphere
-  การติดตั้ง Lenovo XClarity Administrator บน Windows Hyper-V
-  การติดตั้ง Lenovo XClarity Administrator บน Red Hat KVM

เครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว

ในโทโพโลยีเครือข่ายนี้ ทั้งเครือข่ายข้อมูลและเครือข่ายการจัดการจะเป็นเครือข่ายเดียวกัน

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

โปรดตรวจสอบว่าเฟิร์มแวร์ขั้นต่ำที่จำเป็นติดตั้งอยู่บนอุปกรณ์แต่ละเครื่องที่คุณต้องการจัดการโดยใช้ XClarity Administrator คุณสามารถดูระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกแท็บ **ความเข้ากันได้** แล้วคลิกที่ลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

ข้อสำคัญ: กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) ถ้าใช้ DHCP ต้องแน่ใจว่ามีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด

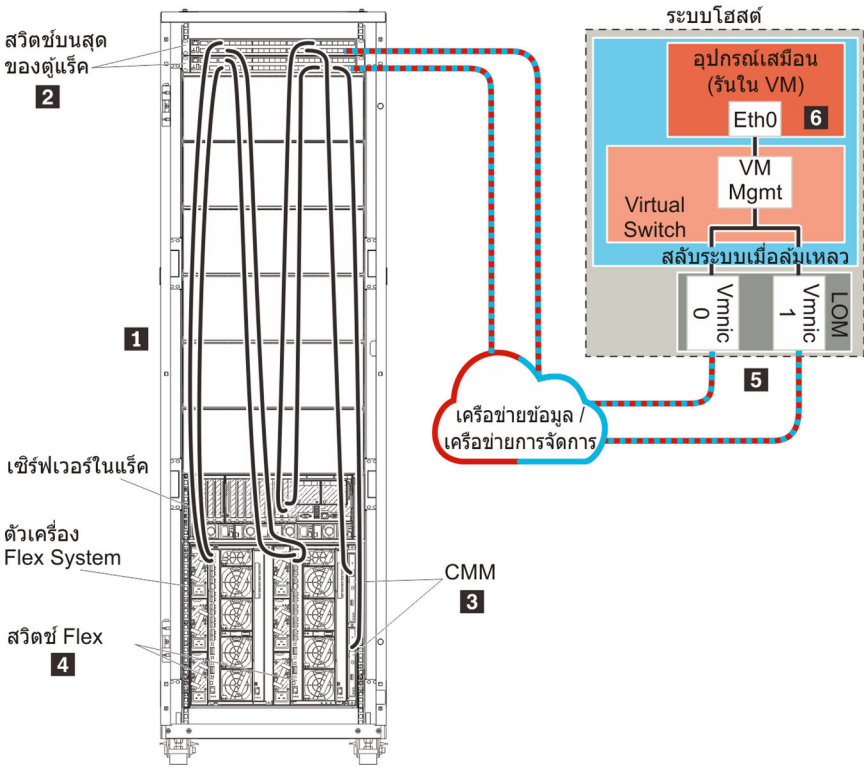
เกี่ยวกับงานนี้

สำหรับอุปกรณ์เสมือน การสื่อสารทั้งหมดระหว่าง XClarity Administrator และเครือข่ายเกิดขึ้นผ่านอินเทอร์เฟซเครือข่าย eth0 บนโฮสต์ สำหรับคอนเทนเนอร์ คุณสามารถใช้ชื่อที่กำหนดเองได้ อย่างไรก็ตาม ในสถานการณ์นี้จะใช้ eth0

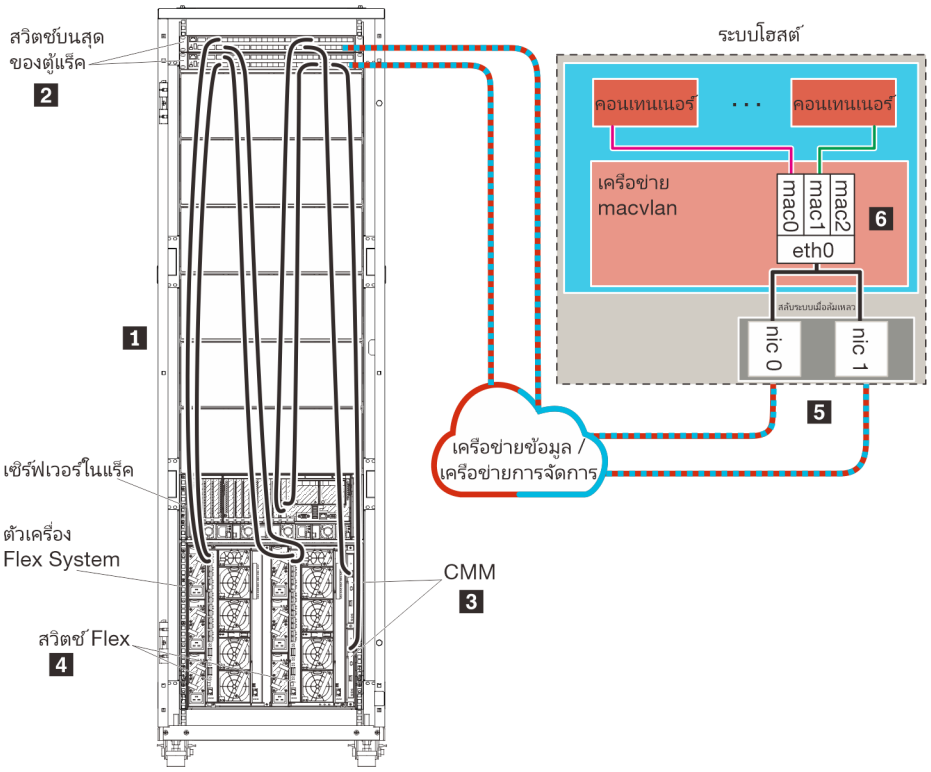
ข้อสำคัญ: การใช้งานเครือข่ายข้อมูลและเครือข่ายการจัดการที่ใช้งานร่วมกัน อาจทำให้เกิดการหยุดชะงักในการรับส่งข้อมูล เช่น แพ็คเก็ตที่ถูกยกเลิก หรือปัญหาการเชื่อมต่อเครือข่ายการจัดการ โดยขึ้นอยู่กับการกำหนดค่าเครือข่ายของคุณ (ตัวอย่างเช่น หากการรับส่งข้อมูลจากเซิร์ฟเวอร์มีลำดับความสำคัญสูงและการรับส่งข้อมูลจากตัวควบคุมการจัดการมีลำดับความสำคัญต่ำ) เครือข่ายการจัดการใช้การรับส่งข้อมูล UDP ใน TCP เพิ่มเติม การรับส่งข้อมูล UDP อาจมีลำดับความสำคัญต่ำเมื่อการรับส่งข้อมูลของเครือข่ายอยู่ในลำดับสูง

ภาพต่อไปนี้อธิบายวิธีหนึ่งในการตั้งค่าสภาพแวดล้อมของคุณหากเครือข่ายข้อมูลและเครือข่ายการจัดการเป็นเครือข่ายเดียวกัน หมายเลขในรูปภาพแสดงถึงขั้นตอนตามตามเลขในส่วนต่อไปนี้

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับเซิร์ฟเวอร์ในแร็ค สวิตช์ในแร็ค สวิตช์ Flex และ CMM ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูล/เครือข่ายการจัดการเดี่ยว



รูปภาพ 8. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลเดี่ยวและการจัดการสำหรับอุปกรณ์เสมือน



รูปภาพ 9. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลเดี่ยวและการจัดการสำหรับคอนเทนเนอร์

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator
- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➞ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

หากคุณต้องการติดตั้ง XClarity Administrator เพื่อจัดการตัวเครื่องและเซิร์ฟเวอร์ในแร็คที่มีอยู่และได้รับการกำหนดค่าแล้ว ให้ไปต่อที่ ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการวางแผนสำหรับโทโพโลยีนี้ รวมถึงข้อมูลเกี่ยวกับการตั้งค่าเครือข่าย และการกำหนดค่า Eth1 และ Eth0 โปรดดู เครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว

ขั้นตอนที่ 1: เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ Lenovo XClarity Administrator ไปยังสวิตช์บนสุดของแร็ค

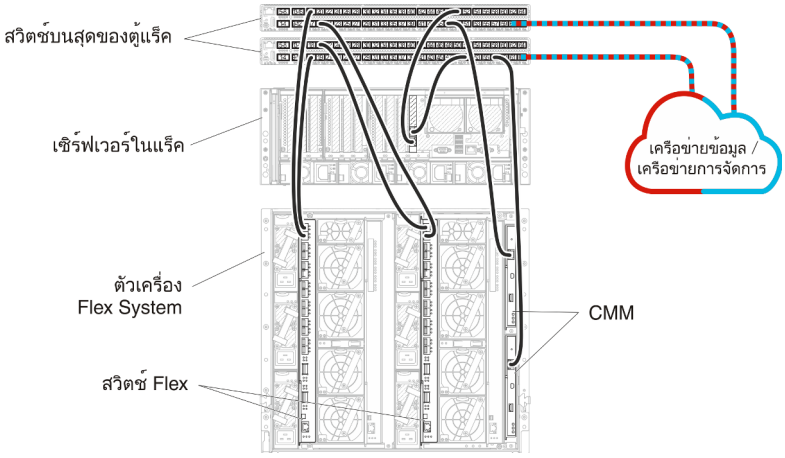
เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คเพื่อให้สามารถสื่อสารระหว่างอุปกรณ์เครือข่ายของคุณได้

ขั้นตอน

เดินสายสวิตช์ Flex และ CMM แต่ละรายการในแต่ละตัวเครื่อง เซิร์ฟเวอร์ในแร็คแต่ละตัว และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คทั้งสองตัว คุณสามารถเลือกพอร์ตใดก็ได้ในสวิตช์บนสุดของแร็ค

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการเดินสายออกจากตัวเครื่อง (สวิตช์ Flex และ CMM) เซิร์ฟเวอร์ในแร็ค และสวิตช์บนสุดของแร็คของ XClarity Administrator

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับเซิร์ฟเวอร์ในแร็ค สวิตช์ในแร็ค สวิตช์ Flex และ CMM ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูล/เครือข่ายการจัดการเดี่ยว



รูปภาพ 10. ตัวอย่างการเดินสายสำหรับเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว

ขั้นตอนที่ 2: กำหนดค่าสวิตช์บนสุดของแร็ค

กำหนดค่าสวิตช์บนสุดของแร็ค

ก่อนจะเริ่มต้น

นอกเหนือจากข้อกำหนดการกำหนดค่าทั่วไปสำหรับสวิตช์บนสุดของแร็คแล้ว โปรดตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมดแล้ว รวมถึงพอร์ตภายนอกไปยัง สวิตช์ Flex, เซิร์ฟเวอร์ในแร็ค และเครือข่าย และพอร์ตภายในไปยัง CMM, เซิร์ฟเวอร์ในแร็ค และเครือข่าย

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของสวิตช์แร็คที่ติดตั้ง

สำหรับข้อมูลเกี่ยวกับการกำหนดค่าสวิตช์บนสุดของแร็คของ Lenovo โปรดดู สวิตช์แร็คในเอกสารแบบออนไลน์ของ System x หากมีการติดตั้งสวิตช์บนสุดของแร็ครุ่น โปรดอ่านเอกสารที่มาพร้อมกับสวิตช์นั้น

ขั้นตอนที่ 3: กำหนดค่า Chassis Management Module (CMM)

กำหนดค่า Chassis Management Module (CMM) หลักในตัวเครื่องของคุณเพื่อจัดการอุปกรณ์ทั้งหมดในตัวเครื่อง

เกี่ยวกับงานนี้

สำหรับข้อมูลโดยละเอียดเกี่ยวกับการกำหนดค่า CMM โปรดดู การกำหนดค่าส่วนประกอบตัวเครื่องในเอกสารแบบออนไลน์ ของ Flex System

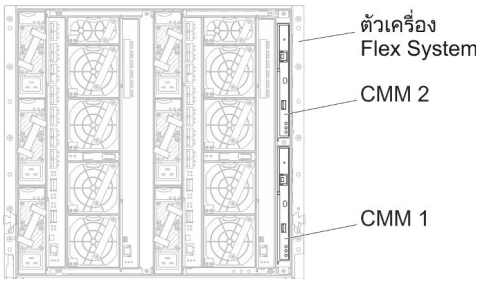
นอกจากนี้ โปรดดูขั้นตอน 4.1 - 4.5 บนโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้ในการกำหนดค่า CMM

หากมีการติดตั้ง CMM สองตัว ให้กำหนดค่าเฉพาะ CMM *หลัก* ซึ่งจะซิงโครไนซ์การกำหนดค่ากับ CMM สแตนด์บายโดยอัตโนมัติ

ขั้นตอนที่ 1. เชื่อมต่อสายอีเทอร์เน็ตจาก CMM ในช่อง 1 กับเวิร์กสเตชันไคลเอ็นต์เพื่อสร้างการเชื่อมต่อโดยตรง



สำหรับการเชื่อมต่อกับ CMM เป็นครั้งแรก คุณอาจต้องเปลี่ยนคุณสมบัติของอินเทอร์เน็ตโปรโตคอลในเวิร์กสเตชันไคลเอ็นต์

ข้อสำคัญ: ตรวจสอบให้แน่ใจว่าซับเน็ตเวิร์กสเตชันไคลเอ็นต์เป็นซับเน็ตเดียวกับซับเน็ต CMM (ซับเน็ต CMM เริ่มต้นคือ 255.255.255.0) ที่อยู่ IP ที่เลือกสำหรับเวิร์กสเตชันไคลเอ็นต์ต้องอยู่บนเครือข่ายเดียวกันกับ CMM (ตัวอย่างเช่น 192.168.70.0 - 192.168.70.24)

ขั้นตอนที่ 2. ในการเปิดอินเทอร์เฟซการจัดการ CMM ให้เปิดเว็บเบราเซอร์บนเวิร์กสเตชันไคลเอ็นต์ และกำหนดให้ไปยังที่อยู่ IP ของ CMM

หมายเหตุ:

- ตรวจสอบว่าคุณใช้การเชื่อมต่อที่ปลอดภัย และรวม **https** ไว้ใน URL (ตัวอย่างเช่น https://192.168.70.100) หากคุณไม่รวม https คุณจะได้รับข้อผิดพลาด ไม่พบเพจ
- หากคุณใช้ที่อยู่ IP เริ่มต้น 192.168.70.100 อินเทอร์เฟซการจัดการ CMM อาจใช้เวลาสักครู่กว่าจะใช้ได้ ความล่าช้านี้เกิดขึ้นเนื่องจาก CMM พยายามรับที่อยู่ DHCP เป็นเวลาสองนาทีขึ้นไปก่อนที่จะกลับมาเป็นที่อยู่คงที่เริ่มต้น

ขั้นตอนที่ 3. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ ID ผู้ใช้เริ่มต้น `USERID` และรหัสผ่าน `PASSWORD` หลังจากเข้าสู่ระบบ คุณต้องเปลี่ยนรหัสผ่านเริ่มต้น

ขั้นตอนที่ 4. ดำเนินการตัวช่วยสร้างการตั้งค่าเริ่มต้นของ CMM เพื่อระบุรายละเอียดสำหรับสภาพแวดล้อมของคุณ ตัวช่วยสร้างการตั้งค่าเริ่มต้นมีตัวเลือกดังต่อไปนี้:

- ดูรายการอุปกรณ์และสถานภาพของตัวเครื่อง
- นำเข้าการกำหนดค่าจากไฟล์การกำหนดค่าที่มีอยู่
- กำหนดค่าการตั้งค่า CMM ทั่วไป
- กำหนดค่าวันที่และเวลาของ CMM

  คำแนะนำ: เมื่อคุณติดตั้ง XClarity Administrator คุณจะกำหนดค่า XClarity Administrator และตัวเครื่องทั้งหมดที่ได้รับการจัดการโดย XClarity Administrator ให้ใช้เซิร์ฟเวอร์ NTP
- กำหนดค่าข้อมูล IP ของ CMM
- กำหนดค่านโยบายการรักษาความปลอดภัยของ CMM
- กำหนดค่า Domain Name System (DNS)
- กำหนดค่าระบบส่งต่อเหตุการณ์

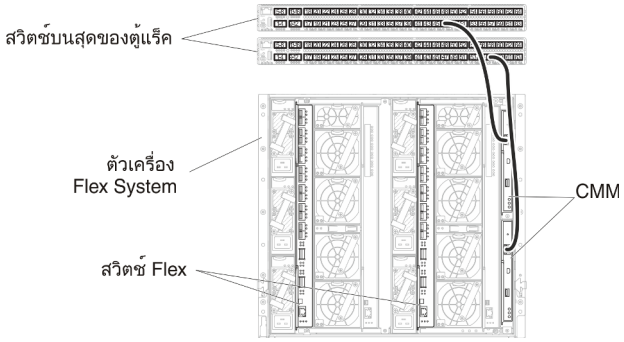
ขั้นตอนที่ 5. หลังจากบันทึกการตั้งค่าของตัวช่วยสร้างการตั้งค่าและใช้การเปลี่ยนแปลงแล้ว ให้กำหนดค่าที่อยู่ IP สำหรับส่วนประกอบทั้งหมดในตัวเครื่อง

โปรดดูขั้นตอน 4.6 ในโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

หมายเหตุ: คุณต้องรีเซ็ตหน่วยประมวลผลการจัดการระบบสำหรับโหนดคอมพิวท์แต่ละโหนด และรีสตาร์ทสวิตช์ Flex เพื่อแสดงที่อยู่ IP ใหม่

ขั้นตอนที่ 6. รีสตาร์ท CMM โดยใช้อินเทอร์เฟซการจัดการ CMM

ขั้นตอนที่ 7. ขณะที่ CMM กำลังรีสตาร์ท ให้เชื่อมต่อสายเคเบิลจากพอร์ตอีเทอร์เน็ตบน CMM กับเครือข่ายของคุณ



ขั้นตอนที่ 8. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ที่อยู่ IP ใหม่

หลังจากดำเนินการเสร็จ

คุณยังสามารถกำหนดค่า CMM ให้สนับสนุนการสำรองด้วย ใช้ระบบวิธีใช้ CMM เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับฟิลด์ที่มีอยู่ในแต่ละหน้าต่อไปนี้

- กำหนดค่าการทำงานล้มเหลวสำหรับ CMM ในกรณีฮาร์ดแวร์ทำงานล้มเหลวใน CMM หลัก จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **คุณสมบัติ** ➔ **การทำงานล้มเหลวขั้นสูง**
- กำหนดค่าการทำงานล้มเหลวเป็นผลมาจากปัญหาของเครือข่าย (อัปลิงค์) จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **เครือข่าย** คลิกแท็บ **อีเทอร์เน็ต** จากนั้นคลิก **อีเทอร์เน็ตขั้นสูง** ในระดับต่ำที่สุด โปรดตรวจสอบให้แน่ใจว่าคุณเลือก **ทำงานล้มเหลวเนื่องจากไม่มีลิงก์เครือข่าย**

ขั้นตอนที่ 4: กำหนดค่า สวิตช์ Flex

กำหนดค่า สวิตช์ Flex (โมดูล I/O) ในตัวเครื่องแต่ละตัว

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตภายนอกจากสวิตช์ Flex ไปยังสวิตช์บนสุดของแร็ค และพอร์ตภายในไปยัง CMM

หากตั้งค่าสวิตช์ Flex ให้รับการตั้งค่าเครือข่ายแบบไดนามิก (ที่อยู่ IP, เน็ตมาสก์, เกตเวย์ และที่อยู่ DNS) ผ่าน DHCP โปรดตรวจสอบให้แน่ใจว่าสวิตช์ Flex มีการตั้งค่าที่สอดคล้องกัน (ตัวอย่างเช่น ตรวจสอบให้แน่ใจว่าที่อยู่ IP อยู่ในซับเน็ตเดียวกันกับ CMM)

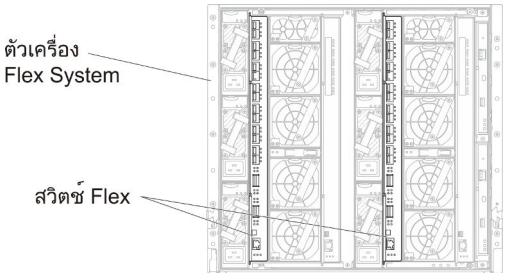
ข้อสำคัญ: สำหรับตัวเครื่อง Flex System แต่ละเครื่อง ตรวจสอบให้แน่ใจว่าประเภทโครงสร้างของการ์ดขยายในเซิร์ฟเวอร์แต่ละตัวในตัวเครื่องเข้ากันได้กับประเภทโครงสร้างของสวิตช์ Flex ทั้งหมดในตัวเครื่องเดียวกัน ตัวอย่างเช่น หากมีการติดตั้งสวิตช์อีเทอร์เน็ตในตัวเครื่อง เซิร์ฟเวอร์ทั้งหมดในตัวเครื่องนั้นต้องมีการเชื่อมต่ออีเทอร์เน็ตผ่านทางขั้วต่อ LAN-on-motherboard หรือการ์ดขยายอีเทอร์เน็ต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าสวิตช์เครือข่าย Flex โปรดดู การกำหนดค่าโมดูล I/O ในเอกสารแบบออนไลน์ของ Flex Systems

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของ สวิตช์ Flex ที่ติดตั้ง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับสวิตช์ Flex, ดู สวิตช์เครือข่าย Flex System ในเอกสารแบบออนไลน์ของ Flex Systems ที่ได้รับการสนับสนุนแต่ละรายการ

ตามปกติแล้ว คุณต้องกำหนดค่าสวิตช์ Flex ในช่องใส่สวิตช์ Flex 1 และ 2

คำแนะนำ: ช่องใส่สวิตช์ Flex 2 คือช่องใส่โมดูลที่สามเมื่อดูที่ด้านหลังของตัวเครื่อง



รูปภาพ 11. ตำแหน่งของ สวิตช์ Flex ในตัวเครื่อง

ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

คุณสามารถติดตั้ง Docker ในเซิร์ฟเวอร์ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ Lenovo XClarity Administrator

ก่อนจะเริ่มต้น

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ XClarity Administrator ที่ใช้ Docker Engine สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

ตรวจสอบให้แน่ใจว่าโฮสต์ที่มีคุณสมบัติตรงตามข้อกำหนดเบื้องต้นที่กำหนดไว้ใน ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator
- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➔ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

ขั้นตอน

ติดตั้งและกำหนดค่า Docker บนโฮสต์โดยใช้คำแนะนำที่มาพร้อมการจัดจำหน่าย Docker

ขั้นตอนที่ 6. ติดตั้งและกำหนดค่า XClarity Administrator

ติดตั้งและกำหนดค่าคอนเทนเนอร์ Lenovo XClarity Administrator บนโฮสต์ Docker ที่เพิ่งติดตั้ง

ก่อนจะเริ่มต้น

ตรวจสอบว่าระบบโฮสต์ของคุณมีคุณสมบัติฮาร์ดแวร์และซอฟต์แวร์ตรงตามข้อกำหนดขั้นต่ำของระบบ (โปรดดู ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น)

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ตรวจสอบให้แน่ใจว่า OS ของโฮสต์และ XClarity Administrator ใช้เซิร์ฟเวอร์ NTP เดียวกัน

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูล การจัดการฮาร์ดแวร์ และการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้จะใช้ eth0

ตรวจสอบให้แน่ใจว่ามีการโหลดเครือข่าย macvlan ลงในเคอร์เนลบนระบบโฮสต์ ใช้คำสั่ง **lsmod | grep macvlan** เพื่อตรวจสอบการโหลด ใช้คำสั่ง **modprobe macvlan** เพื่อโหลด macvlan ลงในเคอร์เนล

ตรวจสอบให้แน่ใจว่าคุณใช้ชื่อและที่อยู่ IP ที่ไม่ซ้ำกันสำหรับแต่ละคอนเทนเนอร์เมื่อใช้งานหลายคอนเทนเนอร์ XClarity Administrator บนโฮสต์เดียวกัน

หากคุณต้องการจัดการ ThinkServer และอุปกรณ์แบบดั้งเดิมอื่นๆ ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน Docker เพื่อรองรับ IPv6

1. แก้ไขไฟล์ /etc/docker/daemon.json ตั้งค่าคีย์ **ipv6** เป็นจริง และตั้งค่าคีย์ **fixed-cidr-v6** เป็นเครือข่ายย่อย IPv6 ของคุณ ข้อมูลต่อไปนี้คือตัวอย่างไฟล์ Daemon
   ```
   {
      "ipv6": true,
      "fixed-cidr-v6": "2001:db8:1::/64",
      "experimental": true,
      "ip6tables": true
   }
   ```
2. โหลดไฟล์การกำหนดค่า Docker อีกครั้งโดยเรียกใช้คำสั่งต่อไปนี้
   ```
   systemctl reload docker
   ```

หมายเหตุ: XClarity Administrator *ไม่ได้*รันเป็นคอนเทนเนอร์ที่มีสิทธิ์

ขั้นตอน

หากต้องการติดตั้งคอนเทนเนอร์ XClarity Administrator โดยใช้ Docker-compose ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ดาวน์โหลดอิมเมจอุปกรณ์เสมือน XClarity Administrator ไฟล์สภาพแวดล้อม และไฟล์ YAML จาก เว็บเพจการดาวน์โหลด XClarity Administrator ไปยังเวิร์กสเตชันไคลเอ็นต์ เข้าสู่ระบบเว็บไซต์ แล้วใช้คีย์การเข้าถึงที่กำหนดให้คุณใช้ดาวน์โหลดอิมเมจ

ขั้นตอนที่ 2. นำเข้าอิมเมจคอนเทนเนอร์ XClarity Administrator ลงในโฮสต์ Docker โดยการเรียกใช้คำสั่งต่อไปนี้
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

ขั้นตอนที่ 3. แก้ไขไฟล์ **docker_compose.env** และอัปเดตตัวแปรสภาพแวดล้อมต่อไปนี้

- CONTAINER_NAME ชื่อคอนเทนเนอร์ที่ไม่ซ้ำกัน ใช้เพื่อสร้างโวลุ่ม Docker สำหรับแต่ละอินสแตนซ์ XClarity Administrator (ตัวอย่างเช่น **CONTAINER_NAME=LXCA-203**)
- ADDRESS ที่อยู่ IPv4 แบบคงที่สำหรับคอนเทนเนอร์ (ตัวอย่างเช่น **ADDRESS=192.0.2.0**)
- BACKUP_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เพื่อจัดเก็บข้อมูลสำรองของ XClarity Administrator นี่ต้องเป็น **/mnt/backup_share**
- FIRMWARE_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เป็นที่เก็บข้อมูลระยะไกลสำหรับการอัปเดตเฟิร์มแวร์ นี่ต้องเป็น **/mnt/fw_share**

ข้อมูลต่อไปนี้คือตัวอย่างไฟล์สภาพแวดล้อม

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

ขั้นตอนที่ 4. แก้ไข **docker_compose.yml** และอัปเดตคุณสมบัติต่อไปนี้

- ตั้งค่าคุณสมบัติ **อิมเมจ** เป็นชื่อของไฟล์อิมเมจการติดตั้งที่ใช้ในขั้นตอนที่ 2

  หมายเหตุ: คุณสามารถเปลี่ยนชื่อไฟล์อิมเมจ (ตัวอย่างเช่น “ล่าสุด”) โดยใช้คำสั่ง `docker tag`
- หากคุณต้องการใช้การแชร์ระยะไกลเป็นที่เก็บข้อมูลเฟิร์มแวร์ระยะไกลและเพื่อจัดเก็บข้อมูลสำรอง XClarity Administrator ให้ตั้งค่าจุดติดตั้งโฮสต์สำหรับการแชร์ระยะไกลแต่ละรายการในคุณสมบัติ **โวลุ่ม**
- ตั้งค่าคุณสมบัติ **dns** เป็นที่อยู่ IP ของเซิร์ฟเวอร์ DNS
- คอนเทนเนอร์แชร์พูลของทรัพยากรโปรเซสเซอร์และหน่วยความจำที่โฮสต์ใช้งานได้ หรือเลือกที่จะกำหนดขีดจำกัดในการใช้ทรัพยากรโดยการตั้งค่าคุณสมบัติ CPU และ **หน่วยความจำ**
- ตั้งค่าคุณสมบัติ **หลัก** เป็นชื่ออินเทอร์เฟซเครือข่ายบนระบบโฮสต์ที่จะใช้เป็นอินเทอร์เฟซหลักของอินเทอร์เฟซ macvlan ในคอนเทนเนอร์ อินเทอร์เฟซนี้ต้องมีสิทธิ์การเข้าถึงเครือข่ายย่อยที่กำหนดให้กับคอนเทนเนอร์โดยตรง
- ตั้งค่า **subnet** และ **gateway** ตามโทโพโลยีเครือข่ายของคุณ โดยปกแล้วติ เครือข่ายย่อยและเกตเวย์จะใช้สำหรับเครือข่ายการจัดการ ซึ่งใช้ ${ADDRESS}
- หากคุณต้องการรองรับ IPv6 ให้ตั้งค่าคุณสมบัติ **enable_ipv6** เป็นจริง ตั้งค่าคุณสมบัติ **ipv6_address** เป็นที่อยู่ IPv6 และเพิ่มคุณสมบัติ **subnet** และ **gateway** อีกชุดตามโทโพโลยีเครือข่ายของคุณ (โดยปกติจะใช้กับเครือข่ายการจัดการซึ่งมีที่อยู่ IPv6 อยู่)

หมายเหตุ: XClarity Administrator ใช้ macvlan ในการกำหนดค่าเครือข่ายคอนเทนเนอร์ สำหรับข้อมูลเพิ่มเติม โปรดดู ใช้เว็บเพจเครือข่าย macvlan

ต่อไปนี้คือตัวอย่างไฟล์ YML ที่เปิดใช้งาน IPv6

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
```

```
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

ขั้นตอนที่ 5. ปรับใช้อิมเมจใน Docker โดยการเรียกใช้คำสั่งต่อไปนี้ โดยที่ *<ENV_FILENAME>* คือชื่อของไฟล์ตัวแปรสภาพแวดล้อมที่สร้างขึ้นในขั้นตอนที่ 2

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

หลังจากดำเนินการเสร็จ

เข้าสู่ระบบและกำหนดค่า XClarity Administrator (โปรดดู การเข้าถึงเว็บอินเทอร์เฟซ Lenovo XClarity Administrator เป็นครั้งแรก และ การกำหนดค่า Lenovo XClarity Administrator)

เครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

ในโทโพโลยีนี้ เครือข่ายข้อมูลและเครือข่ายการจัดการเป็นเครือข่ายที่แยกจากกัน การสื่อสารการจัดการระหว่าง Lenovo XClarity Administrator และเครือข่ายเกิดขึ้นผ่านอินเทอร์เฟซเครือข่าย Eth0 บนโฮสต์ การสื่อสารข้อมูลจะเกิดขึ้นผ่านอินเทอร์เฟซเครือข่าย Eth1

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

โปรดตรวจสอบว่าเฟิร์มแวร์ขั้นต่ำที่จำเป็นติดตั้งอยู่บนอุปกรณ์แต่ละเครื่องที่คุณต้องการจัดการโดยใช้ XClarity Administrator คุณสามารถดูระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกแท็บ **ความเข้ากันได้** แล้วคลิกที่ลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

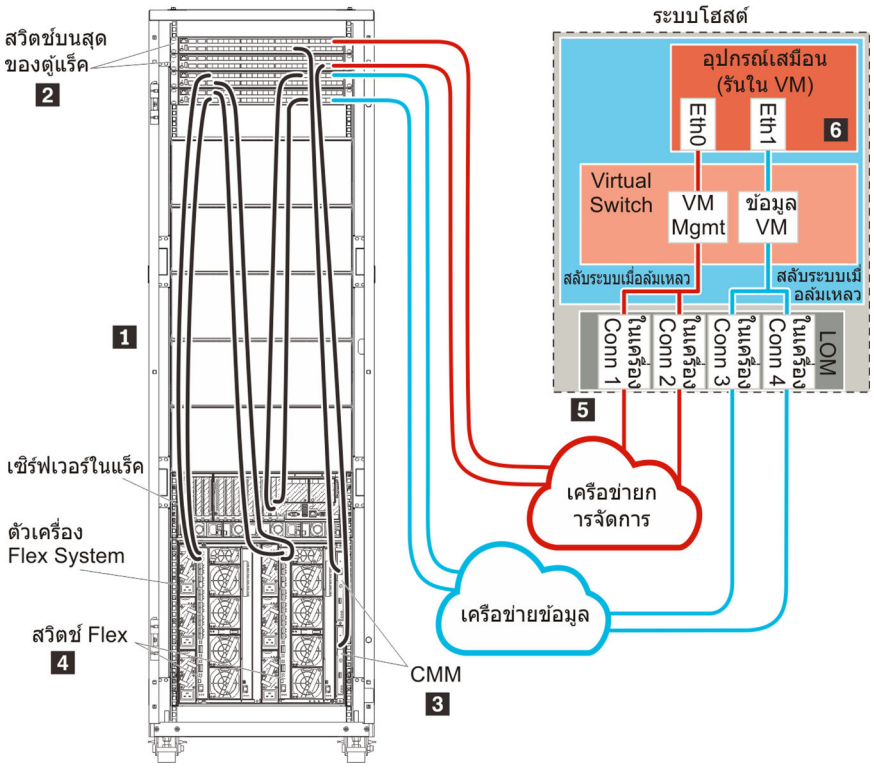
ข้อสำคัญ: กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) ถ้าใช้ DHCP ต้องแน่ใจว่ามีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด

เกี่ยวกับงานนี้

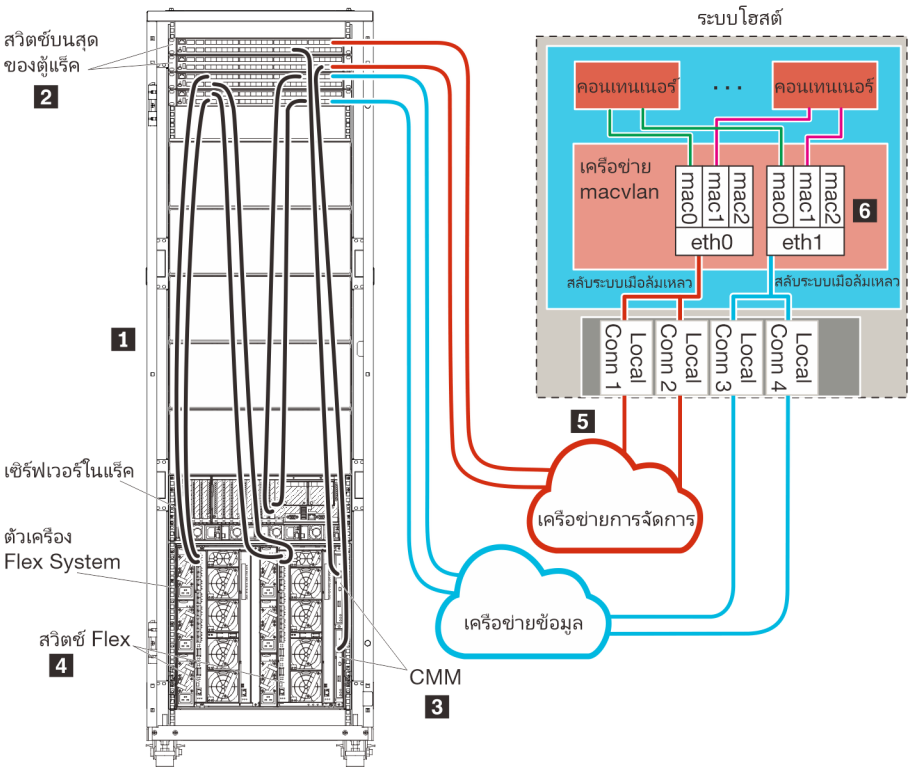
ภาพต่อไปนี้อธิบายวิธีหนึ่งในการตั้งค่าสภาพแวดล้อมของคุณหากเมื่อเครือข่ายข้อมูลและเครือข่ายการจัดการเป็นเครือข่ายที่แยกจากกัน หมายเลขในรูปภาพแสดงถึงขั้นตอนตามตามเลขในส่วนต่อไปนี้

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

คำแนะนำ: แทนที่จะตั้งค่าสวิตช์จริงสองตัวที่เชื่อมต่อกับแต่ละเครือข่ายเพื่อการสำรอง (สำหรับสวิตช์ทั้งหมดสี่ตัว) คุณสามารถตั้งค่าสวิตช์จริงตัวเดียวที่เชื่อมต่อกับแต่ละเครือข่าย (สำหรับสวิตช์ทั้งหมดสองตัว) ในกรณีนั้น สวิตช์แต่ละตัวจะเชื่อมต่อกับทั้งสองเครือข่าย และคุณจะใช้งาน VLAN สองตัว: ตัวหนึ่งสำหรับเครือข่ายข้อมูล และอีกตัวสำหรับเครือข่ายการจัดการ ทั้งนี้เพื่อแยกการรับส่งข้อมูลออกจากกัน



รูปภาพ 12. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลและการจัดการที่แยกจากกันทางกายภาพสำหรับอุปกรณ์เสมือน



รูปภาพ 13. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลและการจัดการที่แยกจากกันทางกายภาพสำหรับคอนเทนเนอร์

หากคุณต้องการติดตั้ง XClarity Administrator เพื่อจัดการตัวเครื่องและเซิร์ฟเวอร์ในแร็คที่มีอยู่และได้รับการกำหนดค่าแล้ว ให้ไปต่อที่ ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการวางแผนสำหรับโทโพโลยีนี้ รวมถึงข้อมูลเกี่ยวกับการตั้งค่าเครือข่าย และการกำหนดค่า Eth1 และ Eth0 โปรดดู เครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

ขั้นตอนที่ 1: เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ Lenovo XClarity Administrator ไปยังสวิตช์บนสุดของแร็ค

เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คเพื่อให้สามารถสื่อสารระหว่างอุปกรณ์เครือข่ายของคุณได้

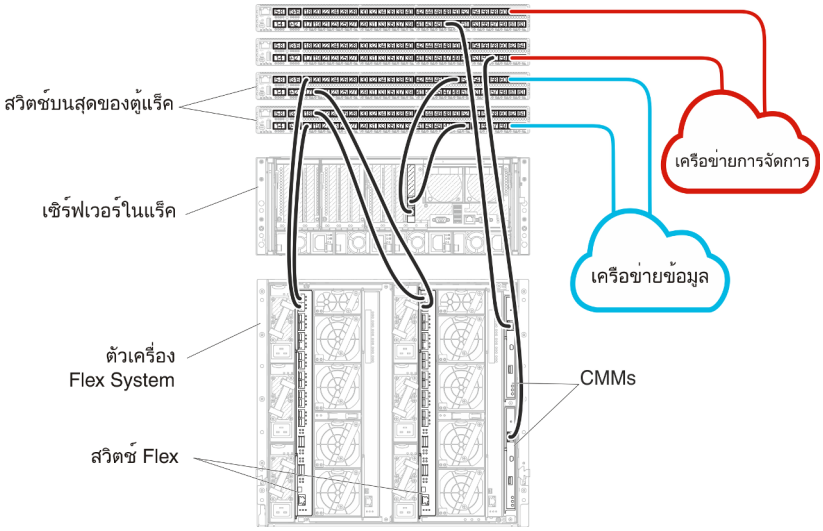
ขั้นตอน

เดินสายสวิตช์ Flex และ CMM แต่ละรายการในแต่ละตัวเครื่อง เซิร์ฟเวอร์ในแร็คแต่ละตัว และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คทั้งสองตัว คุณสามารถเลือกพอร์ตใดก็ได้ในสวิตช์บนสุดของแร็ค

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการเดินสายออกจากตัวเครื่อง (สวิตช์ Flex และ CMM) เซิร์ฟเวอร์ในแร็ค และสวิตช์บนสุดของแร็คของ XClarity Administrator

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

คำแนะนำ: แทนที่จะตั้งค่าสวิตช์จริงสองตัวที่เชื่อมต่อกับแต่ละเครือข่ายเพื่อการสำรอง (สำหรับสวิตช์ทั้งหมดสี่ตัว) คุณสามารถตั้งค่าสวิตช์จริงตัวเดียวที่เชื่อมต่อกับแต่ละเครือข่าย (สำหรับสวิตช์ทั้งหมดสองตัว) ในกรณีนั้น สวิตช์แต่ละตัวจะเชื่อมต่อกับทั้งสองเครือข่าย และคุณจะใช้งาน VLAN สองตัว: ตัวหนึ่งสำหรับเครือข่ายข้อมูล และอีกตัวสำหรับเครือข่ายการจัดการ ทั้งนี้เพื่อแยกการรับส่งข้อมูลออกจากกัน



รูปภาพ 14. ตัวอย่างการเดินสายสำหรับเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันทางกายภาพ

ขั้นตอนที่ 2: กำหนดค่าสวิตช์บนสุดของแร็ค

กำหนดค่าสวิตช์บนสุดของแร็ค

ก่อนจะเริ่มต้น

นอกเหนือจากข้อกำหนดการกำหนดค่าทั่วไปสำหรับสวิตช์บนสุดของแร็คแล้ว โปรดตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมดแล้ว รวมถึงพอร์ตภายนอกไปยัง สวิตช์ Flex, เซิร์ฟเวอร์ในแร็ค และเครือข่าย และพอร์ตภายในไปยัง CMM, เซิร์ฟเวอร์ในแร็ค และเครือข่าย

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของสวิตช์แร็คที่ติดตั้ง

สำหรับข้อมูลเกี่ยวกับการกำหนดค่าสวิตช์บนสุดของแร็คของ Lenovo โปรดดู สวิตช์แร็คในเอกสารแบบออนไลน์ของ System x หากมีการติดตั้งสวิตช์บนสุดของแร็ครุ่น โปรดอ่านเอกสารที่มาพร้อมกับสวิตช์นั้น

ขั้นตอนที่ 3: กำหนดค่า Chassis Management Module (CMM)

กำหนดค่า Chassis Management Module (CMM) หลักในตัวเครื่องของคุณเพื่อจัดการอุปกรณ์ทั้งหมดในตัวเครื่อง

เกี่ยวกับงานนี้

สำหรับข้อมูลโดยละเอียดเกี่ยวกับการกำหนดค่า CMM โปรดดู การกำหนดค่าส่วนประกอบตัวเครื่องในเอกสารแบบออนไลน์ ของ Flex System

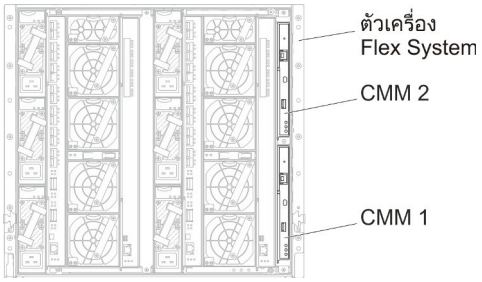
นอกจากนี้ โปรดดูขั้นตอน 4.1 - 4.5 บนโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้ในการกำหนดค่า CMM

หากมีการติดตั้ง CMM สองตัว ให้กำหนดค่าเฉพาะ CMM *หลัก* ซึ่งจะซิงโครไนซ์การกำหนดค่ากับ CMM สแตนด์บายโดยอัตโนมัติ

ขั้นตอนที่ 1. เชื่อมต่อสายอีเทอร์เน็ตจาก CMM ในช่อง 1 กับเวิร์กสเตชันไคลเอ็นต์เพื่อสร้างการเชื่อมต่อโดยตรง



สำหรับการเชื่อมต่อกับ CMM เป็นครั้งแรก คุณอาจต้องเปลี่ยนคุณสมบัติของอินเทอร์เน็ตโปรโตคอลในเวิร์กสเตชันไคลเอ็นต์

ข้อสำคัญ: ตรวจสอบให้แน่ใจว่าซับเน็ตเวิร์กสเตชันไคลเอ็นต์เป็นซับเน็ตเดียวกับซับเน็ต CMM (ซับเน็ต CMM เริ่มต้นคือ 255.255.255.0) ที่อยู่ IP ที่เลือกสำหรับเวิร์กสเตชันไคลเอ็นต์ต้องอยู่บนเครือข่ายเดียวกันกับ CMM (ตัวอย่างเช่น 192.168.70.0 - 192.168.70.24)

ขั้นตอนที่ 2. ในการเปิดอินเทอร์เฟซการจัดการ CMM ให้เปิดเว็บเบราเซอร์บนเวิร์กสเตชันไคลเอ็นต์ และกำหนดให้ไปยังที่อยู่ IP ของ CMM

หมายเหตุ:

- ตรวจสอบว่าคุณใช้การเชื่อมต่อที่ปลอดภัย และรวม **https** ไว้ใน URL (ตัวอย่างเช่น https://192.168.70.100) หากคุณไม่รวม https คุณจะได้รับข้อผิดพลาด ไม่พบเพจ
- หากคุณใช้ที่อยู่ IP เริ่มต้น 192.168.70.100 อินเทอร์เฟซการจัดการ CMM อาจใช้เวลาสักครู่กว่าจะใช้ได้ ความล่าช้านี้เกิดขึ้นเนื่องจาก CMM พยายามรับที่อยู่ DHCP เป็นเวลาสองนาทีขึ้นไปก่อนที่จะกลับมาเป็นที่อยู่คงที่เริ่มต้น

ขั้นตอนที่ 3. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ ID ผู้ใช้เริ่มต้น `USERID` และรหัสผ่าน `PASSWORD` หลังจากเข้าสู่ระบบ คุณต้องเปลี่ยนรหัสผ่านเริ่มต้น

ขั้นตอนที่ 4. ดำเนินการตัวช่วยสร้างการตั้งค่าเริ่มต้นของ CMM เพื่อระบุรายละเอียดสำหรับสภาพแวดล้อมของคุณ ตัวช่วยสร้างการตั้งค่าเริ่มต้นมีตัวเลือกดังต่อไปนี้:

- ดูรายการอุปกรณ์และสถานภาพของตัวเครื่อง
- นำเข้าการกำหนดค่าจากไฟล์การกำหนดค่าที่มีอยู่
- กำหนดค่าการตั้งค่า CMM ทั่วไป
- กำหนดค่าวันที่และเวลาของ CMM

  คำแนะนำ: เมื่อคุณติดตั้ง XClarity Administrator คุณจะกำหนดค่า XClarity Administrator และตัวเครื่องทั้งหมดที่ได้รับการจัดการโดย XClarity Administrator ให้ใช้เซิร์ฟเวอร์ NTP
- กำหนดค่าข้อมูล IP ของ CMM
- กำหนดค่านโยบายการรักษาความปลอดภัยของ CMM
- กำหนดค่า Domain Name System (DNS)
- กำหนดค่าระบบส่งต่อเหตุการณ์

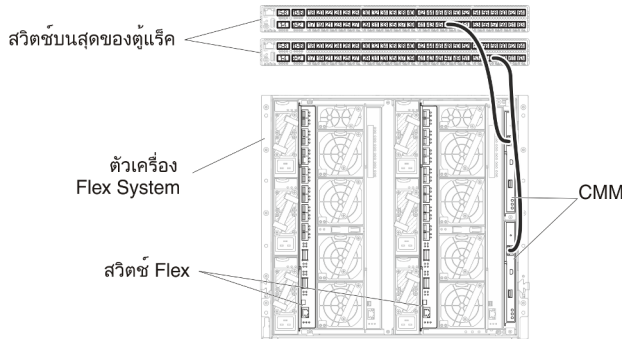
ขั้นตอนที่ 5. หลังจากบันทึกการตั้งค่าของตัวช่วยสร้างการตั้งค่าและใช้การเปลี่ยนแปลงแล้ว ให้กำหนดค่าที่อยู่ IP สำหรับส่วนประกอบทั้งหมดในตัวเครื่อง

โปรดดูขั้นตอน 4.6 ในโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

หมายเหตุ: คุณต้องรีเซ็ตหน่วยประมวลผลการจัดการระบบสำหรับโหนดคอมพิวท์แต่ละโหนด และรีสตาร์ทสวิตช์ Flex เพื่อแสดงที่อยู่ IP ใหม่

ขั้นตอนที่ 6. รีสตาร์ท CMM โดยใช้อินเทอร์เฟซการจัดการ CMM

ขั้นตอนที่ 7. ขณะที่ CMM กำลังรีสตาร์ท ให้เชื่อมต่อสายเคเบิลจากพอร์ตอีเทอร์เน็ตบน CMM กับเครือข่ายของคุณ



ขั้นตอนที่ 8. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ที่อยู่ IP ใหม่

หลังจากดำเนินการเสร็จ

คุณยังสามารถกำหนดค่า CMM ให้สนับสนุนการสำรองด้วย ใช้ระบบวิธีใช้ CMM เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับฟิลด์ที่มีอยู่ในแต่ละหน้าต่อไปนี้

- กำหนดค่าการทำงานล้มเหลวสำหรับ CMM ในกรณีฮาร์ดแวร์ทำงานล้มเหลวใน CMM หลัก จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **คุณสมบัติ** ➔ **การทำงานล้มเหลวขั้นสูง**
- กำหนดค่าการทำงานล้มเหลวเป็นผลมาจากปัญหาของเครือข่าย (อัปลิงค์) จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **เครือข่าย** คลิกแท็บ **อีเทอร์เน็ต** จากนั้นคลิก **อีเทอร์เน็ตขั้นสูง** ในระดับต่ำที่สุด โปรดตรวจสอบให้แน่ใจว่าคุณเลือก **ทำงานล้มเหลวเนื่องจากไม่มีลิงก์เครือข่าย**

ขั้นตอนที่ 4: กำหนดค่า สวิตช์ Flex

กำหนดค่า สวิตช์ Flex ในแต่ละตัวเครื่อง

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตภายนอกจากสวิตช์ Flex ไปยังสวิตช์บนสุดของแร็ค และพอร์ตภายในไปยัง CMM

หากตั้งค่าสวิตช์ Flex ให้รับการตั้งค่าเครือข่ายแบบไดนามิก (ที่อยู่ IP, เน็ตมาสก์, เกตเวย์ และที่อยู่ DNS) ผ่าน DHCP โปรดตรวจสอบให้แน่ใจว่าสวิตช์ Flex มีการตั้งค่าที่สอดคล้องกัน (ตัวอย่างเช่น ตรวจสอบให้แน่ใจว่าที่อยู่ IP อยู่ในซับเน็ตเดียวกันกับ CMM)

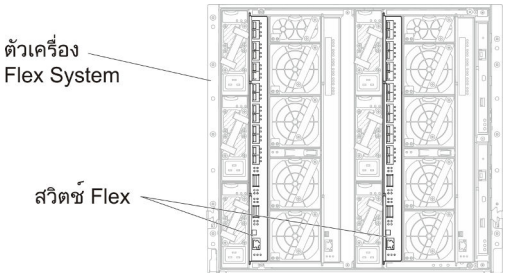
ข้อสำคัญ: สำหรับตัวเครื่อง Flex System แต่ละเครื่อง ตรวจสอบให้แน่ใจว่าประเภทโครงสร้างของการ์ดขยายในเซิร์ฟเวอร์แต่ละตัวในตัวเครื่องเข้ากันได้กับประเภทโครงสร้างของสวิตช์ Flex ทั้งหมดในตัวเครื่องเดียวกัน ตัวอย่างเช่น หากมีการติดตั้งสวิตช์อีเทอร์เน็ตในตัวเครื่อง เซิร์ฟเวอร์ทั้งหมดในตัวเครื่องนั้นต้องมีการเชื่อมต่ออีเทอร์เน็ตผ่านทางขั้วต่อ LAN-on-motherboard หรือการ์ดขยายอีเทอร์เน็ต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าสวิตช์เครือข่าย Flex โปรดดู การกำหนดค่าโมดูล I/O ในเอกสารแบบออนไลน์ของ Flex Systems

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของ สวิตช์ Flex ที่ติดตั้ง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับสวิตช์ Flex, ดู สวิตช์เครือข่าย Flex System ในเอกสารแบบออนไลน์ของ Flex Systems ที่ได้รับการสนับสนุนแต่ละรายการ

ตามปกติแล้ว คุณต้องกำหนดค่าสวิตช์ Flex ในช่องใส่สวิตช์ Flex 1 และ 2

คำแนะนำ: ช่องใส่สวิตช์ Flex 2 คือช่องใส่โมดูลที่สามเมื่อดูที่ด้านหลังของตัวเครื่อง



รูปภาพ 15. ตำแหน่งของ สวิตช์ Flex ในตัวเครื่อง

ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

คุณสามารถติดตั้ง Docker ในเซิร์ฟเวอร์ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ Lenovo XClarity Administrator

ก่อนจะเริ่มต้น

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ XClarity Administrator ที่ใช้ Docker Engine สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

ตรวจสอบให้แน่ใจว่าโฮสต์ที่มีคุณสมบัติตรงตามข้อกำหนดเบื้องต้นที่กำหนดไว้ใน ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator
- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➔ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

ขั้นตอน

ติดตั้งและกำหนดค่า Docker บนโฮสต์โดยใช้คำแนะนำที่มาพร้อมการจัดจำหน่าย Docker

ขั้นตอนที่ 6. ติดตั้งและกำหนดค่า XClarity Administrator

ติดตั้งและกำหนดค่าคอนเทนเนอร์ Lenovo XClarity Administrator บนโฮสต์ Docker ที่เพิ่งติดตั้ง

ก่อนจะเริ่มต้น

ตรวจสอบว่าระบบโฮสต์ของคุณมีคุณสมบัติฮาร์ดแวร์และซอฟต์แวร์ตรงตามข้อกำหนดขั้นต่ำของระบบ (โปรดดู ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น)

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ตรวจสอบให้แน่ใจว่า OS ของโฮสต์และ XClarity Administrator ใช้เซิร์ฟเวอร์ NTP เดียวกัน

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูล การจัดการฮาร์ดแวร์ และการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้จะใช้ eth0

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูลและฮาร์ดแวร์ และเครือข่ายที่จะใช้สำหรับการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้ใช้ eth0 และ eth1 ตามลำดับ

ตรวจสอบให้แน่ใจว่ามีการโหลดเครือข่าย macvlan ลงในเคอร์เนลบนระบบโฮสต์ ใช้คำสั่ง **lsmod | grep macvlan** เพื่อตรวจสอบการโหลด ใช้คำสั่ง **modprobe macvlan** เพื่อโหลด macvlan ลงในเคอร์เนล

ตรวจสอบให้แน่ใจว่าคุณใช้ชื่อและที่อยู่ IP ที่ไม่ซ้ำกันสำหรับแต่ละคอนเทนเนอร์เมื่อใช้งานหลายคอนเทนเนอร์ XClarity Administrator บนโฮสต์เดียวกัน

หากคุณต้องการจัดการ ThinkServer และอุปกรณ์แบบดั้งเดิมอื่นๆ ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน Docker เพื่อรองรับ IPv6

1. แก้ไขไฟล์ /etc/docker/daemon.json ตั้งค่าคีย์ **ipv6** เป็นจริง และตั้งค่าคีย์ **fixed-cidr-v6** เป็นเครือข่ายย่อย IPv6 ของคุณ ข้อมูลต่อไปนี้คือตัวอย่างไฟล์ Daemon
   ```
   {
      "ipv6": true,
      "fixed-cidr-v6": "2001:db8:1::/64",
      "experimental": true,
      "ip6tables": true
   }
   ```
2. โหลดไฟล์การกำหนดค่า Docker อีกครั้งโดยเรียกใช้คำสั่งต่อไปนี้
   ```
   systemctl reload docker
   ```

หมายเหตุ: XClarity Administrator *ไม่ได้*รันเป็นคอนเทนเนอร์ที่มีสิทธิ์

ขั้นตอน

หากต้องการติดตั้งคอนเทนเนอร์ XClarity Administrator โดยใช้ Docker-compose ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ดาวน์โหลดอิมเมจอุปกรณ์เสมือน XClarity Administrator ไฟล์สภาพแวดล้อม และไฟล์ YAML จาก เว็บเพจการดาวน์โหลด XClarity Administrator ไปยังเวิร์กสเตชันไคลเอ็นต์ เข้าสู่ระบบเว็บไซต์ แล้วใช้คีย์การเข้าถึงที่กำหนดให้คุณใช้ดาวน์โหลดอิมเมจ

ขั้นตอนที่ 2. นำเข้าอิมเมจคอนเทนเนอร์ XClarity Administrator ลงในโฮสต์ Docker โดยการเรียกใช้คำสั่งต่อไปนี้
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

ขั้นตอนที่ 3. แก้ไขไฟล์ **docker_compose.env** และอัปเดตตัวแปรสภาพแวดล้อมต่อไปนี้

- CONTAINER_NAME ชื่อคอนเทนเนอร์ที่ไม่ซ้ำกัน ใช้เพื่อสร้างโวลุ่ม Docker สำหรับแต่ละอินสแตนซ์ XClarity Administrator (ตัวอย่างเช่น **CONTAINER_NAME=LXCA-203**)
- ADDRESS ที่อยู่ IPv4 แบบคงที่สำหรับคอนเทนเนอร์ (ตัวอย่างเช่น **ADDRESS=192.0.2.0**)
- BACKUP_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เพื่อจัดเก็บข้อมูลสำรองของ XClarity Administrator นี่ต้องเป็น **/mnt/backup_share**
- FIRMWARE_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เป็นที่เก็บข้อมูลระยะไกลสำหรับการอัปเดตเฟิร์มแวร์ นี่ต้องเป็น **/mnt/fw_share**

ข้อมูลต่อไปนี้คือตัวอย่างไฟล์สภาพแวดล้อม

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

ขั้นตอนที่ 4. แก้ไข **docker_compose.yml** และอัปเดตคุณสมบัติต่อไปนี้

- ตั้งค่าคุณสมบัติ **อิมเมจ** เป็นชื่อของไฟล์อิมเมจการติดตั้งที่ใช้ในขั้นตอนที่ 2

  หมายเหตุ: คุณสามารถเปลี่ยนชื่อไฟล์อิมเมจ (ตัวอย่างเช่น “ล่าสุด”) โดยใช้คำสั่ง `docker tag`
- หากคุณต้องการใช้การแชร์ระยะไกลเป็นที่เก็บข้อมูลเฟิร์มแวร์ระยะไกลและเพื่อจัดเก็บข้อมูลสำรอง XClarity Administrator ให้ตั้งค่าจุดติดตั้งโฮสต์สำหรับการแชร์ระยะไกลแต่ละรายการในคุณสมบัติ **โวลุ่ม**
- ตั้งค่าคุณสมบัติ **dns** เป็นที่อยู่ IP ของเซิร์ฟเวอร์ DNS
- คอนเทนเนอร์แชร์พูลของทรัพยากรโปรเซสเซอร์และหน่วยความจำที่โฮสต์ใช้งานได้ หรือเลือกที่จะกำหนดขีดจำกัดในการใช้ทรัพยากรโดยการตั้งค่าคุณสมบัติ CPU และ **หน่วยความจำ**
- ตั้งค่าคุณสมบัติ **หลัก** เป็นชื่ออินเทอร์เฟซเครือข่ายบนระบบโฮสต์ที่จะใช้เป็นอินเทอร์เฟซหลักของอินเทอร์เฟซ macvlan ในคอนเทนเนอร์ อินเทอร์เฟซนี้ต้องมีสิทธิ์การเข้าถึงเครือข่ายย่อยที่กำหนดให้กับคอนเทนเนอร์โดยตรง
- ตั้งค่า **subnet** และ **gateway** ตามโทโพโลยีเครือข่ายของคุณ โดยปกแล้วติ เครือข่ายย่อยและเกตเวย์จะใช้สำหรับเครือข่ายการจัดการ ซึ่งใช้ ${ADDRESS}
- หากคุณต้องการรองรับ IPv6 ให้ตั้งค่าคุณสมบัติ **enable_ipv6** เป็นจริง ตั้งค่าคุณสมบัติ **ipv6_address** เป็นที่อยู่ IPv6 และเพิ่มคุณสมบัติ **subnet** และ **gateway** อีกชุดตามโทโพโลยีเครือข่ายของคุณ (โดยปกติจะใช้กับเครือข่ายการจัดการซึ่งมีที่อยู่ IPv6 อยู่)

ต่อไปนี้คือตัวอย่างไฟล์ YML ที่เปิดใช้งาน IPv6

```
version: '3.8'

services:

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

```
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

```
      - subnet: 192.0.122.0/24
      - subnet: "2001:8003:7d51:2005::/80"
```

ขั้นตอนที่ 5. ปรับใช้อิมเมจใน Docker โดยการเรียกใช้คำสั่งต่อไปนี้ โดยที่ *<ENV_FILENAME>* คือชื่อของไฟล์ตัวแปรสภาพแวดล้อมที่สร้างขึ้นในขั้นตอนที่ 2

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

หลังจากดำเนินการเสร็จ

เข้าสู่ระบบและกำหนดค่า XClarity Administrator (โปรดดู การเข้าถึงเว็บอินเทอร์เฟซ Lenovo XClarity Administrator เป็นครั้งแรก และ การกำหนดค่า Lenovo XClarity Administrator)

โทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง

ในโทโพโลยีนี้ เครือข่ายข้อมูลและเครือข่ายการจัดการจะแยกจากกันแบบเสมือนจริง แพ็คเก็ตจากเครือข่ายข้อมูลและแพ็คเก็ตจากเครือข่ายการจัดการถูกส่งผ่านการเชื่อมต่อทางกายภาพเดียวกัน ระบบจะใช้การแท็ก VLAN บนแพ็คเก็ตข้อมูลเครือข่ายการจัดการทั้งหมดเพื่อแยกการรับส่งข้อมูลระหว่างสองเครือข่ายออกจากกัน

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

โปรดตรวจสอบว่าเฟิร์มแวร์ขั้นต่ำที่จำเป็นติดตั้งอยู่บนอุปกรณ์แต่ละเครื่องที่คุณต้องการจัดการโดยใช้ XClarity Administrator คุณสามารถดูระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกแท็บ **ความเข้ากันได้** แล้วคลิกที่ลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

ตรวจสอบให้แน่ใจว่าได้ตั้งค่า VLAN ID สำหรับเครือข่ายข้อมูลและเครือข่ายการจัดการแล้ว หรือสามารถเปิดใช้งานการแท็ก VLAN จาก สวิตช์ Flex หากคุณใช้งานการแท็กจาก สวิตช์ Flex หรือเปิดใช้งานจากสวิตช์บนสุดของแร็คหากคุณใช้งานการแท็กจากสวิตช์บนสุดของแร็ค

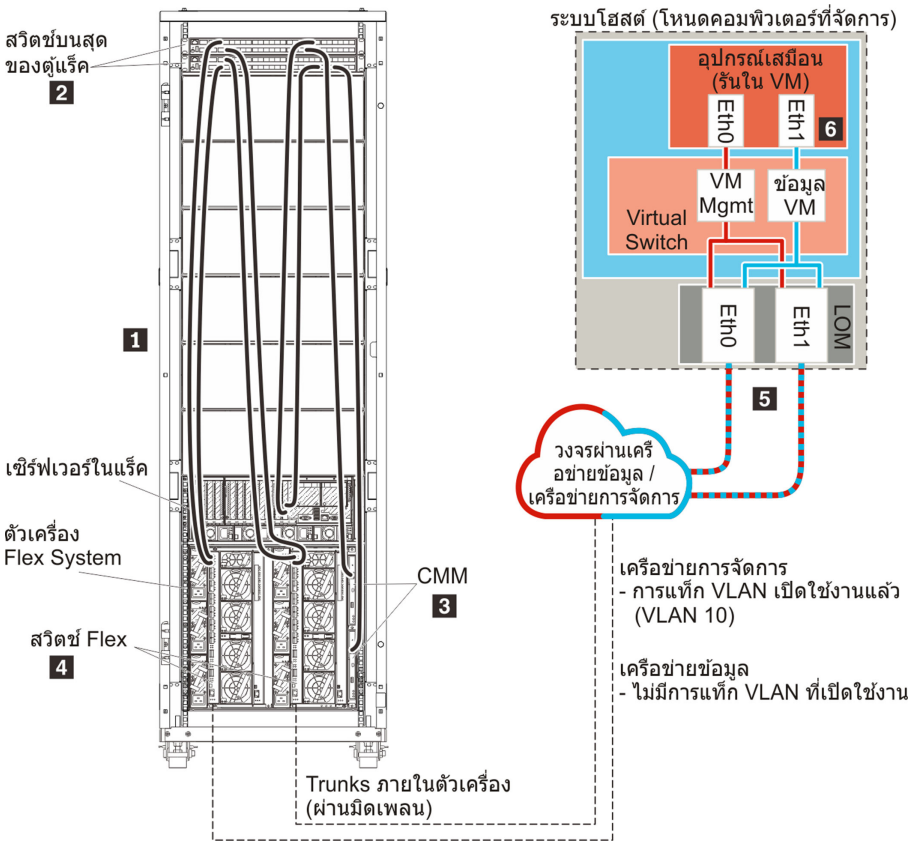
ตรวจสอบให้แน่ใจว่าคุณกำหนดพอร์ตที่ CMM เชื่อมต่อในฐานะที่เป็นของ VLAN การจัดการ

ข้อสำคัญ: กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) ถ้าใช้ DHCP ต้องแน่ใจว่ามีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด

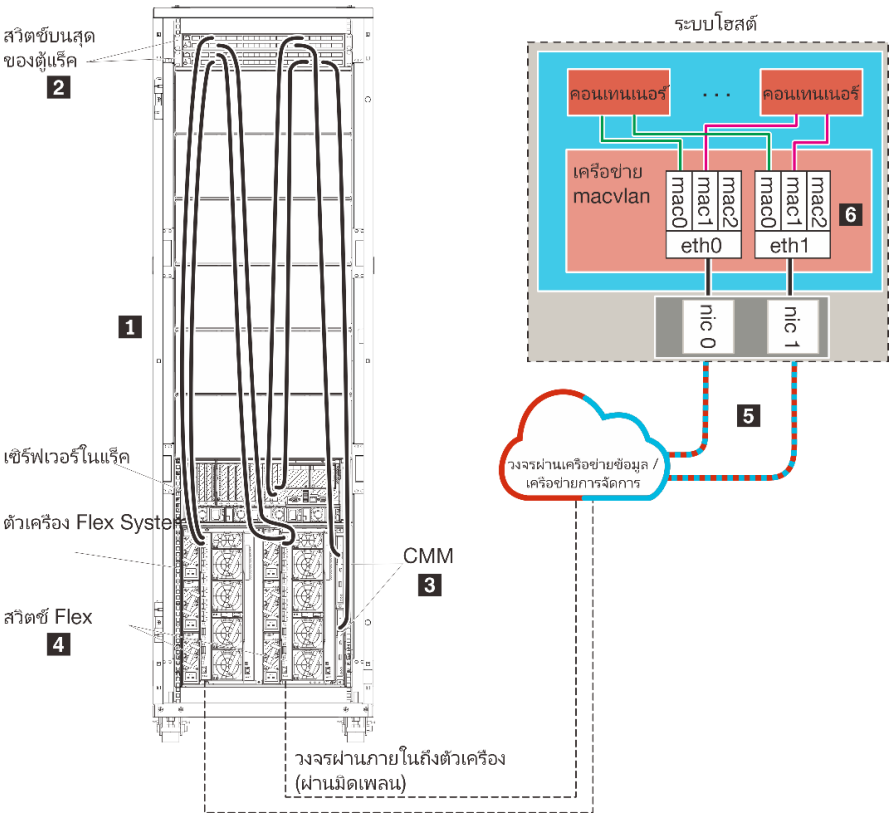
เกี่ยวกับงานนี้

ภาพต่อไปนี้อธิบายวิธีหนึ่งในการตั้งค่าสภาพแวดล้อมของคุณเพื่อให้เครือข่ายการจัดการแยกออกจากเครือข่ายเสมือนจริง หมายเลขในรูปภาพแสดงถึงขั้นตอนตามตามเลขในส่วนต่อไปนี้

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง



รูปภาพ 16. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลและการจัดการที่แยกจากกันแบบเสมือนสำหรับอุปกรณ์เสมือน



รูปภาพ 17. ตัวอย่างโทโพโลยีเครือข่ายข้อมูลและการจัดการที่แยกจากกันแบบเสมือนสำหรับคอนเทนเนอร์

ในกรณีนี้ จะมีการติดตั้งXClarity Administrator บนเซิร์ฟเวอร์ในตัวเครื่อง Flex System ที่ได้รับการจัดการโดย XClarity Administrator

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator
- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➞ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

และในกรณีนี้ ข้อมูลทั้งหมดจะถูกส่งผ่านการเชื่อมต่อทางกายภาพเดียวกันด้วย การแยกเครือข่ายการจัดการออกจากเครือข่ายข้อมูลทำได้ผ่านการแท็ก VLAN ซึ่งแท็กเฉพาะที่สอดคล้องกับเครือข่ายการจัดการจะเพิ่มในแพ็คเก็ตข้อมูลขาเข้าเพื่อให้แน่ใจว่ามีการกำหนดเส้นทางไปยังอินเทอร์เฟซที่เหมาะสม แท็กจะถูกถอดออกจากแพ็คเก็ตข้อมูลขาออก

สามารถเปิดใช้งานการแท็ก VLAN ได้ในหนึ่งในอุปกรณ์ดังต่อไปนี้:

- **สวิตช์บนสุดของแร็ค** แท็ก VLAN ที่สอดคล้องกับเครือข่ายการจัดการจะถูกเพิ่มไปยังแพ็คเก็ตเมื่อเข้าสู่สวิตช์บนสุดของแร็ค และส่งผ่าน สวิตช์ Flex ไปยังเซิร์ฟเวอร์ในตัวเครื่อง Flex System ในเส้นทางการส่งคืน แท็ก VLAN จะถูกถอดออกขณะที่ส่งมาจากสวิตช์บนสุดของแร็คไปยังตัวควบคุมการจัดการ
- **สวิตช์ Flex** แท็ก VLAN ที่สอดคล้องกับเครือข่ายการจัดการจะถูกเพิ่มไปยังแพ็คเก็ตเมื่อเข้าสู่ สวิตช์ Flex และส่งผ่านไปยังเซิร์ฟเวอร์ในตัวเครื่อง Flex System ในเส้นทางการส่งคืน แท็ก VLAN จะถูกเพิ่มโดยเซิร์ฟเวอร์ และส่งไปยัง สวิตช์ Flex ซึ่งจะถอดออกเมื่อส่งต่อไปยังตัวควบคุมการจัดการ

ตัวเลือกว่าจะใช้งานการแท็ก VLAN หรือไม่ จะขึ้นอยู่กับความต้องการและความซับซ้อนในสภาพแวดล้อมของคุณ

หากคุณต้องการติดตั้ง XClarity Administrator เพื่อจัดการตัวเครื่องและเซิร์ฟเวอร์ในแร็คที่มีอยู่และได้รับการกำหนดค่าแล้ว ให้ไปต่อที่ ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการวางแผนสำหรับโทโพโลยีนี้ รวมถึงข้อมูลเกี่ยวกับการตั้งค่าเครือข่าย และการกำหนดค่า Eth1 และ Eth0 โปรดดู เครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือน

ขั้นตอนที่ 1: เดินสายตัวเครื่องและเซิร์ฟเวอร์ในแร็คไปยังสวิตช์บนสุดของแร็ค

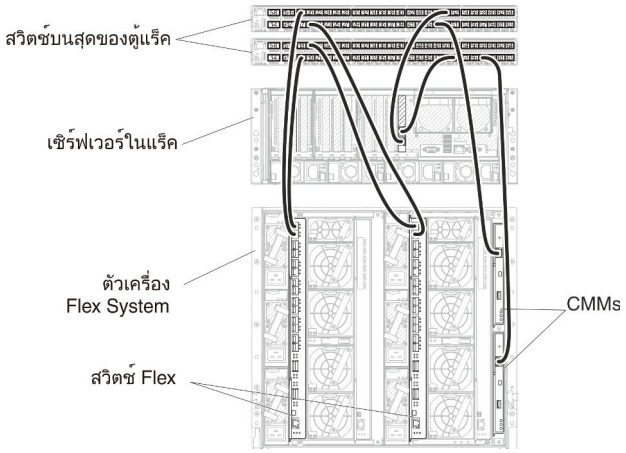
เดินสายตัวเครื่องและเซิร์ฟเวอร์ในแร็คไปยังสวิตช์บนสุดของแร็คเดียวกันเพื่อให้สามารถสื่อสารระหว่างอุปกรณ์ของคุณได้

ขั้นตอน

เดินสายสวิตช์ Flex และ CMM แต่ละรายการในแต่ละตัวเครื่องและเซิร์ฟเวอร์ในแร็คแต่ละตัว ไปยังสวิตช์บนสุดของแร็คทั้งสองตัว คุณสามารถเลือกพอร์ตใดก็ได้ในสวิตช์บนสุดของแร็คนั้น

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการเดินสายไฟออกจากตัวเครื่อง (สวิตช์ Flex และ CMM) และเซิร์ฟเวอร์ในแร็คไปยังสวิตช์บนสุดของแร็คเมื่อติดตั้ง Lenovo XClarity Administrator บนเซิร์ฟเวอร์ในตัวเครื่องที่จะได้รับการจัดการโดย XClarity Administrator

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง



รูปภาพ 18. ตัวอย่างการเดินสายสำหรับเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง

ขั้นตอนที่ 2: กำหนดค่าสวิตช์บนสุดของแร็ค

กำหนดค่าสวิตช์บนสุดของแร็ค

ก่อนจะเริ่มต้น

นอกเหนือจากข้อกำหนดการกำหนดค่าทั่วไปสำหรับสวิตช์บนสุดของแร็คแล้ว โปรดตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมดแล้ว รวมถึงพอร์ตภายนอกไปยัง สวิตช์ Flex, เซิร์ฟเวอร์ในแร็ค และเครือข่าย และพอร์ตภายในไปยัง CMM, เซิร์ฟเวอร์ในแร็ค และเครือข่าย

คุณสามารถใช้งานการแท็ก VLAN ในสวิตช์ Flex หรือสวิตช์บนสุดของแร็ค ทั้งนี้ขึ้นอยู่กับความต้องการและความซับซ้อนในสภาพแวดล้อมของคุณ หากคุณใช้งานการแท็กจากสวิตช์บนสุดของแร็ค ให้เปิดใช้งานการแท็ก VLAN จากสวิตช์บนสุดของแร็ค

ตรวจสอบให้แน่ใจว่าได้ตั้งค่า VLAN ID สำหรับเครือข่ายการจัดการและเครือข่ายข้อมูลแล้ว

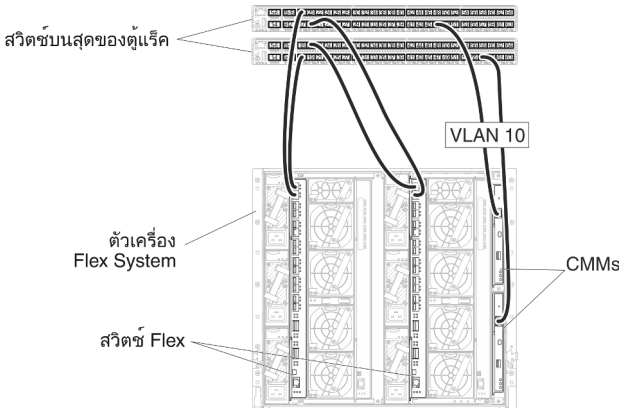
ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของสวิตช์แร็คที่ติดตั้ง

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการแท็ก VLAN ที่ใช้งานในสวิตช์บนสุดของแร็ค และเปิดใช้งานเฉพาะในเครือข่ายการจัดการ VLAN การจัดการได้รับการตั้งค่าเป็น VLAN 10

ในกรณีนี้ คุณต้องกำหนดพอร์ตที่ CMM เชื่อมต่อในฐานะที่เป็นของ VLAN การจัดการ

หมายเหตุ: คุณยังสามารถเปิดใช้งานการแท็ก VLAN บนเครือข่ายข้อมูลเพื่อกำหนดค่า VLAN ข้อมูล



รูปภาพ 19. ตัวอย่างการกำหนดค่าสำหรับ สวิตช์ Flex ในเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง (VMware ESXi) ที่เปิดใช้งานการแท็ก VLAN ในเครือข่ายการจัดการ

สำหรับข้อมูลเกี่ยวกับการกำหนดค่าสวิตช์บนสุดของแร็คของ Lenovo โปรดดู สวิตช์แร็คในเอกสารแบบออนไลน์ของ System x หากมีการติดตั้งสวิตช์บนสุดของแร็ครุ่น โปรดอ่านเอกสารที่มาพร้อมกับสวิตช์นั้น

ขั้นตอนที่ 3: กำหนดค่า Chassis Management Module (CMM)

กำหนดค่า Chassis Management Module (CMM) หลักในตัวเครื่องของคุณเพื่อจัดการอุปกรณ์ทั้งหมดในตัวเครื่อง

เกี่ยวกับงานนี้

สำหรับข้อมูลโดยละเอียดเกี่ยวกับการกำหนดค่า CMM โปรดดู การกำหนดค่าส่วนประกอบตัวเครื่องในเอกสารแบบออนไลน์ ของ Flex System

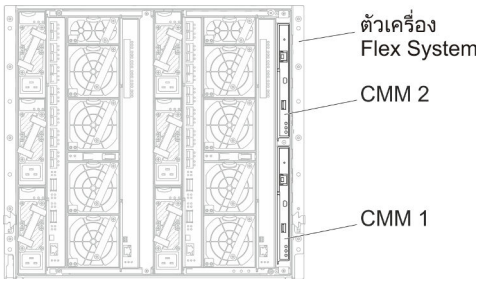
นอกจากนี้ โปรดดูขั้นตอน 4.1 - 4.5 บนโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้ในการกำหนดค่า CMM

หากมีการติดตั้ง CMM สองตัว ให้กำหนดค่าเฉพาะ CMM *หลัก* ซึ่งจะซิงโครไนซ์การกำหนดค่ากับ CMM สแตนด์บายโดยอัตโนมัติ

ขั้นตอนที่ 1. เชื่อมต่อสายอีเทอร์เน็ตจาก CMM ในช่อง 1 กับเวิร์กสเตชันไคลเอ็นต์เพื่อสร้างการเชื่อมต่อโดยตรง



สำหรับการเชื่อมต่อกับ CMM เป็นครั้งแรก คุณอาจต้องเปลี่ยนคุณสมบัติของอินเทอร์เน็ตโปรโตคอลในเวิร์กสเตชันไคลเอ็นต์

ข้อสำคัญ: ตรวจสอบให้แน่ใจว่าซับเน็ตเวิร์กสเตชันไคลเอ็นต์เป็นซับเน็ตเดียวกับซับเน็ต CMM (ซับเน็ต CMM เริ่มต้นคือ 255.255.255.0) ที่อยู่ IP ที่เลือกสำหรับเวิร์กสเตชันไคลเอ็นต์ต้องอยู่บนเครือข่ายเดียวกันกับ CMM (ตัวอย่างเช่น 192.168.70.0 - 192.168.70.24)

ขั้นตอนที่ 2. ในการเปิดอินเทอร์เฟซการจัดการ CMM ให้เปิดเว็บเบราเซอร์บนเวิร์กสเตชันไคลเอ็นต์ และกำหนดให้ไปยังที่อยู่ IP ของ CMM

หมายเหตุ:

- ตรวจสอบว่าคุณใช้การเชื่อมต่อที่ปลอดภัย และรวม **https** ไว้ใน URL (ตัวอย่างเช่น https://192.168.70.100) หากคุณไม่รวม https คุณจะได้รับข้อผิดพลาด ไม่พบเพจ
- หากคุณใช้ที่อยู่ IP เริ่มต้น 192.168.70.100 อินเทอร์เฟซการจัดการ CMM อาจใช้เวลาสักครู่กว่าจะใช้ได้ ความล่าช้านี้เกิดขึ้นเนื่องจาก CMM พยายามรับที่อยู่ DHCP เป็นเวลาสองนาทีขึ้นไปก่อนที่จะกลับมาเป็นที่อยู่คงที่เริ่มต้น

ขั้นตอนที่ 3. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ ID ผู้ใช้เริ่มต้น `USERID` และรหัสผ่าน `PASSWORD` หลังจากเข้าสู่ระบบ คุณต้องเปลี่ยนรหัสผ่านเริ่มต้น

ขั้นตอนที่ 4. ดำเนินการตัวช่วยสร้างการตั้งค่าเริ่มต้นของ CMM เพื่อระบุรายละเอียดสำหรับสภาพแวดล้อมของคุณ ตัวช่วยสร้างการตั้งค่าเริ่มต้นมีตัวเลือกดังต่อไปนี้:

- ดูรายการอุปกรณ์และสถานภาพของตัวเครื่อง
- นำเข้าการกำหนดค่าจากไฟล์การกำหนดค่าที่มีอยู่
- กำหนดค่าการตั้งค่า CMM ทั่วไป
- กำหนดค่าวันที่และเวลาของ CMM

  คำแนะนำ: เมื่อคุณติดตั้ง XClarity Administrator คุณจะกำหนดค่า XClarity Administrator และตัวเครื่องทั้งหมดที่ได้รับการจัดการโดย XClarity Administrator ให้ใช้เซิร์ฟเวอร์ NTP
- กำหนดค่าข้อมูล IP ของ CMM
- กำหนดค่านโยบายการรักษาความปลอดภัยของ CMM

- กำหนดค่า Domain Name System (DNS)
- กำหนดค่าระบบส่งต่อเหตุการณ์

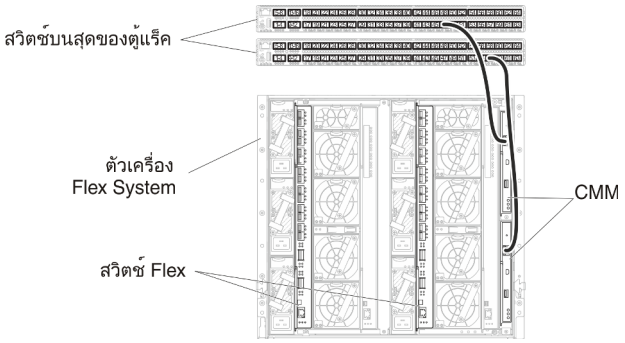
ขั้นตอนที่ 5. หลังจากบันทึกการตั้งค่าของตัวช่วยสร้างการตั้งค่าและใช้การเปลี่ยนแปลงแล้ว ให้กำหนดค่าที่อยู่ IP สำหรับส่วนประกอบทั้งหมดในตัวเครื่อง

โปรดดูขั้นตอน 4.6 ในโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

หมายเหตุ: คุณต้องรีเซ็ตหน่วยประมวลผลการจัดการระบบสำหรับโหนดคอมพิวท์แต่ละโหนด และรีสตาร์ทสวิตช์ Flex เพื่อแสดงที่อยู่ IP ใหม่

ขั้นตอนที่ 6. รีสตาร์ท CMM โดยใช้อินเทอร์เฟซการจัดการ CMM

ขั้นตอนที่ 7. ขณะที่ CMM กำลังรีสตาร์ท ให้เชื่อมต่อสายเคเบิลจากพอร์ตอีเทอร์เน็ตบน CMM กับเครือข่ายของคุณ



ขั้นตอนที่ 8. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ที่อยู่ IP ใหม่

หลังจากดำเนินการเสร็จ

คุณยังสามารถกำหนดค่า CMM ให้สนับสนุนการสำรองด้วย ใช้ระบบวิธีใช้ CMM เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับฟิลด์ที่มีอยู่ในแต่ละหน้าต่อไปนี้

- กำหนดค่าการทำงานล้มเหลวสำหรับ CMM ในกรณีฮาร์ดแวร์ทำงานล้มเหลวใน CMM หลัก จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล Mgt ➔ คุณสมบัติ ➔ การทำงานล้มเหลวขั้นสูง**
- กำหนดค่าการทำงานล้มเหลวเป็นผลมาจากปัญหาของเครือข่าย (อัปลิงค์) จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล Mgt ➔ เครือข่าย** คลิกแท็บ **อีเทอร์เน็ต** จากนั้นคลิก **อีเทอร์เน็ตขั้นสูง** ในระดับต่ำที่สุด โปรดตรวจสอบให้แน่ใจว่าคุณเลือก **ทำงานล้มเหลวเนื่องจากไม่มีลิงก์เครือข่าย**

ขั้นตอนที่ 4: กำหนดค่า สวิตช์ Flex

กำหนดค่า สวิตช์ Flex ในแต่ละตัวเครื่อง

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตภายนอกจากสวิตช์ Flex ไปยังสวิตช์บนสุดของแร็ค และพอร์ตภายในไปยัง CMM

คุณสามารถใช้งานการแท็ก VLAN ในสวิตช์ Flex หรือสวิตช์บนสุดของแร็ค ทั้งนี้ขึ้นอยู่กับความต้องการและความซับซ้อนในสภาพแวดล้อมของคุณ หากคุณใช้งานการแท็กจากสวิตช์ Flex ให้เปิดใช้งานการแท็ก VLAN จากสวิตช์ Flex

ตรวจสอบให้แน่ใจว่าได้ตั้งค่า VLAN ID สำหรับเครือข่ายการจัดการและเครือข่ายข้อมูลแล้ว

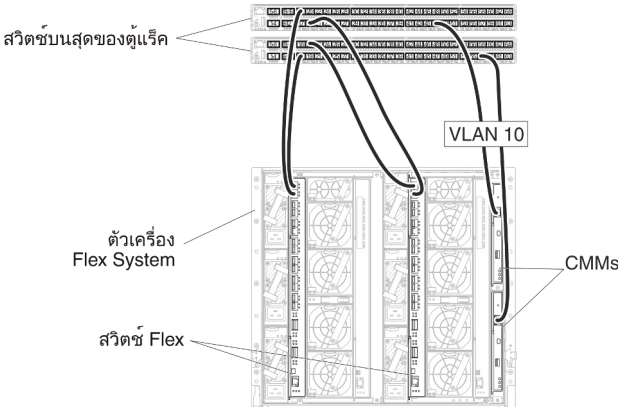
ข้อสำคัญ: สำหรับตัวเครื่อง Flex System แต่ละเครื่อง ตรวจสอบให้แน่ใจว่าประเภทโครงสร้างของการ์ดขยายในเซิร์ฟเวอร์แต่ละตัวในตัวเครื่องเข้ากันได้กับประเภทโครงสร้างของสวิตช์ Flex ทั้งหมดในตัวเครื่องเดียวกัน ตัวอย่างเช่น หากมีการติดตั้งสวิตช์อีเทอร์เน็ตในตัวเครื่อง เซิร์ฟเวอร์ทั้งหมดในตัวเครื่องนั้นต้องมีการเชื่อมต่ออีเทอร์เน็ตผ่านทางขั้วต่อ LAN-on-motherboard หรือการ์ดขยายอีเทอร์เน็ต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าสวิตช์เครือข่าย Flex โปรดดู การกำหนดค่าโมดูล I/O ในเอกสารแบบออนไลน์ของ Flex Systems

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของ สวิตช์ Flex ที่ติดตั้ง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับสวิตช์ Flex, ดู สวิตช์เครือข่าย Flex System ในเอกสารแบบออนไลน์ของ Flex Systems ที่ได้รับการสนับสนุนแต่ละรายการ

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการแท็ก VLAN ที่ใช้งานในสวิตช์ Flex และเปิดใช้งานเฉพาะในเครือข่ายการจัดการ VLAN การจัดการได้รับการตั้งค่าเป็น VLAN 10

หมายเหตุ: คุณสามารถกำหนดค่า VLAN ข้อมูลด้วยการเปิดใช้งานการแท็ก VLAN บนเครือข่ายข้อมูล



รูปภาพ 20. ตัวอย่างการกำหนดค่าสำหรับ สวิตช์ Flex ในเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง (VMware ESXi) ที่เปิดใช้งานการแท็ก VLAN ในเครือข่ายการจัดการ

ดำเนินการตามขั้นตอนต่อไปนี้เพื่อกำหนดค่าสวิตช์ Flex สำหรับกรณีนี้:

ขั้นตอนที่ 1. กำหนดค่าสวิตช์ Flex ในช่องใส่สวิตช์ Flex 1:

a. กำหนด VLAN การจัดการ (ในตัวอย่างนี้ เราเลือก VLAN 10) ให้มีพอร์ตภายนอกที่เดินสายไปยังสวิตช์การจัดการบนสุดของแร็ค (Ext1)

b. กำหนดพอร์ตภายในเป็นส่วนหนึ่งของ VLAN 10 (VLAN การจัดการ) ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน VLAN Trunking บนพอร์ตนั้น

ขั้นตอนที่ 2. กำหนดค่าสวิตช์ Flex ในช่องใส่สวิตช์ Flex 2:

คำแนะนำ: ช่องใส่สวิตช์ Flex 2 คือช่องใส่โมดูลที่สาม หากคุณดูที่ด้านหลังของตัวเครื่อง:

a. กำหนด VLAN การจัดการ (ในตัวอย่างนี้ เราเลือก VLAN 10) ให้มีพอร์ตภายนอกที่เดินสายไปยังสวิตช์การจัดการบนสุดของแร็ค

b. กำหนดพอร์ตภายในเป็นส่วนหนึ่งของ VLAN 10 (VLAN การจัดการ) ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน VLAN Trunking บนพอร์ตนั้น

ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

คุณสามารถติดตั้ง Docker ในระบบที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ Lenovo XClarity Administrator

ก่อนจะเริ่มต้น

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ XClarity Administrator ที่ใช้ Docker Engine สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

ตรวจสอบให้แน่ใจว่าโฮสต์ที่มีคุณสมบัติตรงตามข้อกำหนดเบื้องต้นที่กำหนดไว้ใน ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรี

สตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator

- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➔ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

ขั้นตอน

ติดตั้งและกำหนดค่า Docker บนโฮสต์โดยใช้คำแนะนำที่มาพร้อมการจัดจำหน่าย Docker

ขั้นตอนที่ 6. ติดตั้งและกำหนดค่า XClarity Administrator

ติดตั้งและกำหนดค่าคอนเทนเนอร์ Lenovo XClarity Administrator บนโฮสต์ Docker ที่เพิ่งติดตั้ง

ก่อนจะเริ่มต้น

ตรวจสอบว่าระบบโฮสต์ของคุณมีคุณสมบัติฮาร์ดแวร์และซอฟต์แวร์ตรงตามข้อกำหนดขั้นต่ำของระบบ (โปรดดู ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น)

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ตรวจสอบให้แน่ใจว่า OS ของโฮสต์และ XClarity Administrator ใช้เซิร์ฟเวอร์ NTP เดียวกัน

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูล การจัดการฮาร์ดแวร์ และการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้จะใช้ eth0

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูลและฮาร์ดแวร์ และเครือข่ายที่จะใช้สำหรับการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้ใช้ eth0 และ eth1 ตามลำดับ

ตรวจสอบให้แน่ใจว่ามีการโหลดเครือข่าย macvlan ลงในเคอร์เนลบนระบบโฮสต์ ใช้คำสั่ง **lsmod | grep macvlan** เพื่อตรวจสอบการโหลด ใช้คำสั่ง **modprobe macvlan** เพื่อโหลด macvlan ลงในเคอร์เนล

ตรวจสอบให้แน่ใจว่าคุณใช้ชื่อและที่อยู่ IP ที่ไม่ซ้ำกันสำหรับแต่ละคอนเทนเนอร์เมื่อใช้งานหลายคอนเทนเนอร์ XClarity Administrator บนโฮสต์เดียวกัน

หากคุณต้องการจัดการ ThinkServer และอุปกรณ์แบบดั้งเดิมอื่นๆ ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน Docker เพื่อรองรับ IPv6

1. แก้ไขไฟล์ /etc/docker/daemon.json ตั้งค่าคีย์ **ipv6** เป็นจริง และตั้งค่าคีย์ **fixed-cidr-v6** เป็นเครือข่ายย่อย IPv6 ของคุณ ข้อมูลต่อไปนี้คือตัวอย่างไฟล์ Daemon
   ```
   {
      "ipv6": true,
      "fixed-cidr-v6": "2001:db8:1::/64",
      "experimental": true,
      "ip6tables": true
   }
   ```
2. โหลดไฟล์การกำหนดค่า Docker อีกครั้งโดยเรียกใช้คำสั่งต่อไปนี้
   ```
   systemctl reload docker
   ```

หมายเหตุ: XClarity Administrator *ไม่ได้*รันเป็นคอนเทนเนอร์ที่มีสิทธิ์

ขั้นตอน

หากต้องการติดตั้งคอนเทนเนอร์ XClarity Administrator โดยใช้ Docker-compose ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ดาวน์โหลดอิมเมจอุปกรณ์เสมือน XClarity Administrator ไฟล์สภาพแวดล้อม และไฟล์ YAML จาก เว็บเพจการดาวน์โหลด XClarity Administrator ไปยังเวิร์กสเตชันไคลเอ็นต์ เข้าสู่ระบบเว็บไซต์ แล้วใช้คีย์การเข้าถึงที่กำหนดให้คุณใช้ดาวน์โหลดอิมเมจ

ขั้นตอนที่ 2. นำเข้าอิมเมจคอนเทนเนอร์ XClarity Administrator ลงในโฮสต์ Docker โดยการเรียกใช้คำสั่งต่อไปนี้
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

ขั้นตอนที่ 3. แก้ไขไฟล์ **docker_compose.env** และอัปเดตตัวแปรสภาพแวดล้อมต่อไปนี้

- CONTAINER_NAME ชื่อคอนเทนเนอร์ที่ไม่ซ้ำกัน ใช้เพื่อสร้างโวลุ่ม Docker สำหรับแต่ละอินสแตนซ์ XClarity Administrator (ตัวอย่างเช่น **CONTAINER_NAME=LXCA-203**)
- ADDRESS ที่อยู่ IPv4 แบบคงที่สำหรับคอนเทนเนอร์ (ตัวอย่างเช่น **ADDRESS=192.0.2.0**)
- BACKUP_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เพื่อจัดเก็บข้อมูลสำรองของ XClarity Administrator นี่ต้องเป็น **/mnt/backup_share**
- FIRMWARE_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เป็นที่เก็บข้อมูลระยะไกลสำหรับการอัปเดตเฟิร์มแวร์ นี่ต้องเป็น **/mnt/fw_share**

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

ขั้นตอนที่ 4. แก้ไข **docker_compose.yml** และอัปเดตคุณสมบัติต่อไปนี้

- ตั้งค่าคุณสมบัติ **อิมเมจ** เป็นชื่อของไฟล์อิมเมจการติดตั้งที่ใช้ในขั้นตอนที่ 2

  หมายเหตุ: คุณสามารถเปลี่ยนชื่อไฟล์อิมเมจ (ตัวอย่างเช่น “ล่าสุด”) โดยใช้คำสั่ง `docker tag`
- หากคุณต้องการใช้การแชร์ระยะไกลเป็นที่เก็บข้อมูลเฟิร์มแวร์ระยะไกลและเพื่อจัดเก็บข้อมูลสำรอง XClarity Administrator ให้ตั้งค่าจุดติดตั้งโฮสต์สำหรับการแชร์ระยะไกลแต่ละรายการในคุณสมบัติ **โวลุ่ม**
- ตั้งค่าคุณสมบัติ **dns** เป็นที่อยู่ IP ของเซิร์ฟเวอร์ DNS
- คอนเทนเนอร์แชร์พูลของทรัพยากรโปรเซสเซอร์และหน่วยความจำที่โฮสต์ใช้งานได้ หรือเลือกที่จะกำหนดขีดจำกัดในการใช้ทรัพยากรโดยการตั้งค่าคุณสมบัติ CPU และ **หน่วยความจำ**
- ตั้งค่าคุณสมบัติ **หลัก** เป็นชื่ออินเทอร์เฟซเครือข่ายบนระบบโฮสต์ที่จะใช้เป็นอินเทอร์เฟซหลักของอินเทอร์เฟซ macvlan ในคอนเทนเนอร์ อินเทอร์เฟซนี้ต้องมีสิทธิ์การเข้าถึงเครือข่ายย่อยที่กำหนดให้กับคอนเทนเนอร์โดยตรง
- ตั้งค่า **subnet** และ **gateway** ตามโทโพโลยีเครือข่ายของคุณ โดยปกแล้วติ เครือข่ายย่อยและเกตเวย์จะใช้สำหรับเครือข่ายการจัดการ ซึ่งใช้ ${ADDRESS}
- หากคุณต้องการรองรับ IPv6 ให้ตั้งค่าคุณสมบัติ **enable_ipv6** เป็นจริง ตั้งค่าคุณสมบัติ **ipv6_address** เป็นที่อยู่ IPv6 และเพิ่มคุณสมบัติ **subnet** และ **gateway** อีกชุดตามโทโพโลยีเครือข่ายของคุณ (โดยปกติจะใช้กับเครือข่ายการจัดการซึ่งมีที่อยู่ IPv6 อยู่)

ต่อไปนี้คือตัวอย่างไฟล์ YML ที่เปิดใช้งาน IPv6

```
version: '3.8'

services:

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

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

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

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

ขั้นตอนที่ 5. ปรับใช้อิมเมจใน Docker โดยการเรียกใช้คำสั่งต่อไปนี้ โดยที่ *<ENV_FILENAME>* คือชื่อของไฟล์ตัวแปรสภาพแวดล้อมที่สร้างขึ้นในขั้นตอนที่ 2

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

หลังจากดำเนินการเสร็จ

เข้าสู่ระบบและกำหนดค่า XClarity Administrator (โปรดดู การเข้าถึงเว็บอินเทอร์เฟซ Lenovo XClarity Administrator เป็นครั้งแรก และ การกำหนดค่า Lenovo XClarity Administrator)

โทโพโลยีเครือข่ายการจัดการอย่างเดียว

ในโทโพโลยีนี้ Lenovo XClarity Administrator จะมีเฉพาะเครือข่ายการจัดการอย่างเดียว และจะไม่มีเครือข่ายข้อมูล

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมพอร์ตทั้งหมด รวมถึง:

- พอร์ตที่ XClarity Administrator ต้องมี (โปรดดู ความพร้อมใช้งานของพอร์ต)
- พอร์ตภายนอกไปยังเครือข่าย
- พอร์ตภายในไปยัง CMM

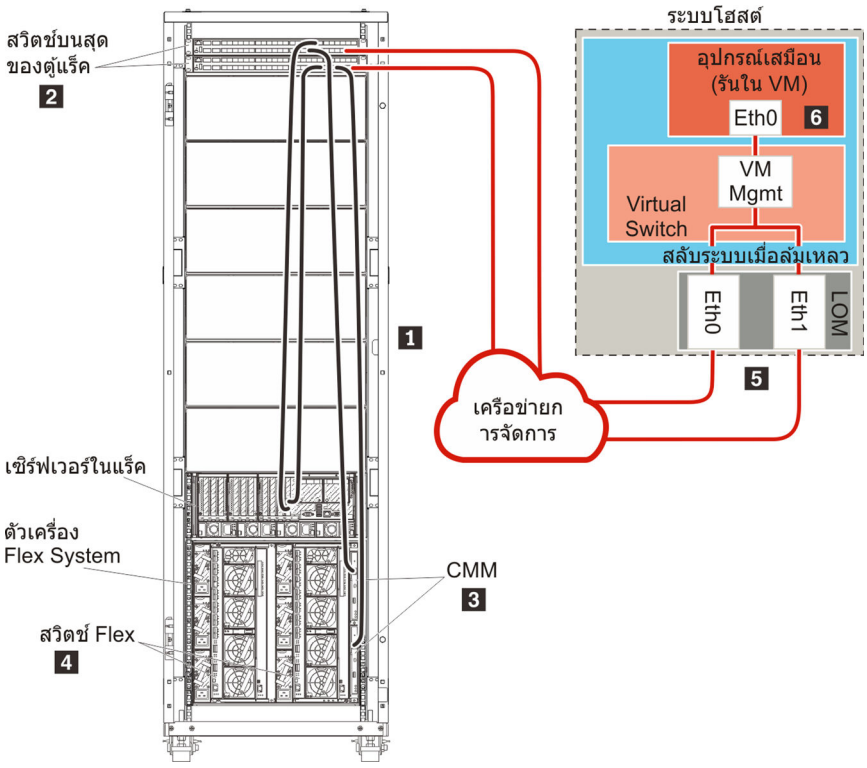
โปรดตรวจสอบว่าเฟิร์มแวร์ขั้นต่ำที่จำเป็นติดตั้งอยู่บนอุปกรณ์แต่ละเครื่องที่คุณต้องการจัดการโดยใช้ XClarity Administrator คุณสามารถดูระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกแท็บ **ความเข้ากันได้** แล้วคลิกที่ลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

ข้อสำคัญ: กำหนดค่าอุปกรณ์และส่วนประกอบในลักษณะที่มีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด พิจารณาใช้ที่อยู่ IP แบบคงที่แทน Dynamic Host Configuration Protocol (DHCP) ถ้าใช้ DHCP ต้องแน่ใจว่ามีการเปลี่ยนแปลงที่อยู่ IP น้อยที่สุด

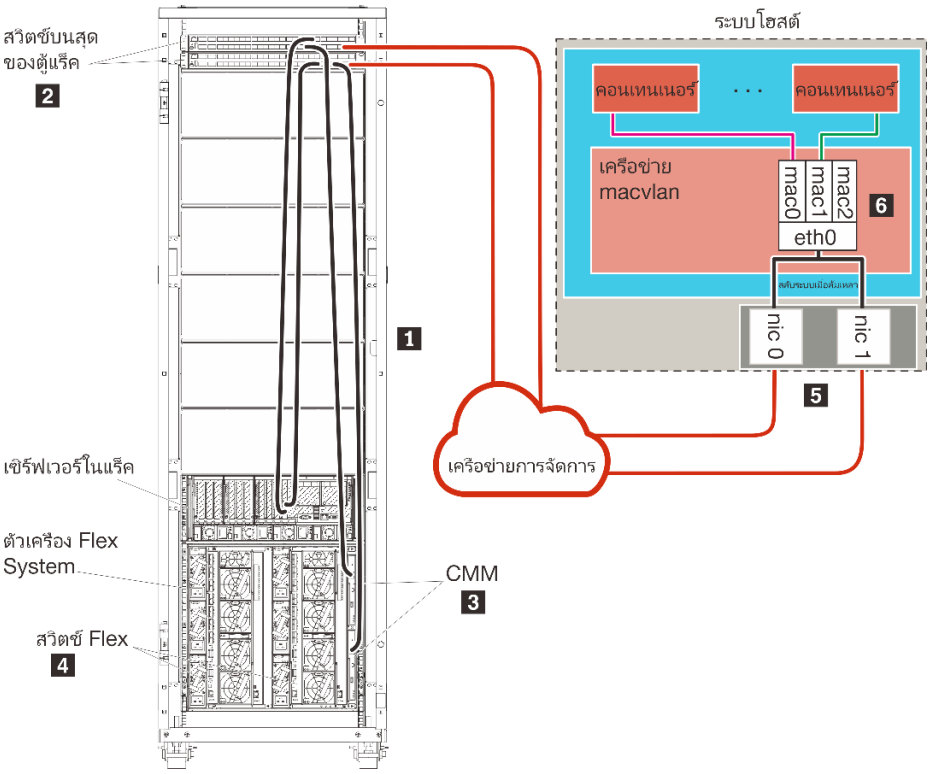
เกี่ยวกับงานนี้

ภาพต่อไปนี้อธิบายวิธีหนึ่งในการตั้งค่าสภาพแวดล้อมของคุณหาก Lenovo XClarity Administrator มีเพียงเครือข่ายการจัดการอย่างเดียว (และไม่มีเครือข่ายข้อมูล) หมายเลขในรูปภาพแสดงถึงขั้นตอนตามตามเลขในส่วนต่อไปนี้

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายการจัดการอย่างเดียว



รูปภาพ 21. ตัวอย่างโทโพโลยีเครือข่ายการจัดการอย่างเดียวสำหรับอุปกรณ์เสมือน



รูปภาพ 22. ตัวอย่างโทโพโลยีเครือข่ายการจัดการอย่างเดียวสำหรับคอนเทนเนอร์

หากคุณต้องการติดตั้ง XClarity Administrator เพื่อจัดการตัวเครื่องและเซิร์ฟเวอร์ในแร็คที่มีอยู่และได้รับการกำหนดค่าแล้ว ให้ไปต่อที่ ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการวางแผนสำหรับโทโพโลยีนี้ รวมถึงข้อมูลเกี่ยวกับการตั้งค่าเครือข่าย และการกำหนดค่า Eth1 และ Eth0 โปรดดู เครือข่ายการจัดการอย่างเดียว

ขั้นตอนที่ 1: เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ Lenovo XClarity Administrator ไปยังสวิตช์บนสุดของแร็ค

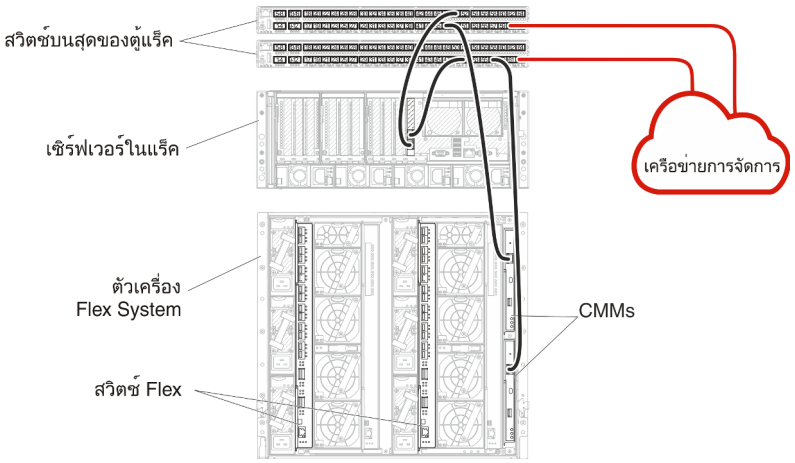
เดินสายตัวเครื่อง เซิร์ฟเวอร์ในแร็ค และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คเพื่อให้สามารถสื่อสารระหว่างอุปกรณ์เครือข่ายของคุณได้

ขั้นตอน

เดินสายสวิตช์ Flex และ CMM แต่ละรายการในแต่ละตัวเครื่อง เซิร์ฟเวอร์ในแร็คแต่ละตัว และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็คทั้งสองตัว คุณสามารถเลือกพอร์ตใดก็ได้ในสวิตช์บนสุดของแร็ค

ภาพต่อไปนี้เป็นตัวอย่างที่แสดงการเดินสายไฟออกจากตัวเครื่อง (สวิตช์ Flex และ CMM), เซิร์ฟเวอร์ในแร็ค และโฮสต์ XClarity Administrator ไปยังสวิตช์บนสุดของแร็ค

หมายเหตุ: ภาพนี้แสดงตัวเลือกในการเดินสายทั้งหมดที่อาจจำเป็นสำหรับสภาพแวดล้อมของคุณ แต่รูปนี้แสดงเฉพาะข้อกำหนดตัวเลือกการเดินสายสำหรับสวิตช์ Flex, CMM และเซิร์ฟเวอร์ในแร็ค ตามที่เกี่ยวข้องกับการตั้งค่าเครือข่ายการจัดการอย่างเดียว



รูปภาพ 23. ตัวอย่างการเดินสายสำหรับเครือข่ายการจัดการอย่างเดียว

ขั้นตอนที่ 2: กำหนดค่าสวิตช์บนสุดของแร็ค

กำหนดค่าสวิตช์บนสุดของแร็ค

ก่อนจะเริ่มต้น

นอกเหนือจากข้อกำหนดการกำหนดค่าทั่วไปสำหรับสวิตช์บนสุดของแร็คแล้ว โปรดตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมดแล้ว รวมถึงพอร์ตภายนอกไปยัง สวิตช์ Flex, เซิร์ฟเวอร์ในแร็ค และเครือข่าย และพอร์ตภายในไปยัง CMM, เซิร์ฟเวอร์ในแร็ค และเครือข่าย

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของสวิตช์แร็คที่ติดตั้ง

สำหรับข้อมูลเกี่ยวกับการกำหนดค่าสวิตช์บนสุดของแร็คของ Lenovo โปรดดู สวิตช์แร็คในเอกสารแบบออนไลน์ของ System x หากมีการติดตั้งสวิตช์บนสุดของแร็ครุ่น โปรดอ่านเอกสารที่มาพร้อมกับสวิตช์นั้น

ขั้นตอนที่ 3: กำหนดค่า Chassis Management Module (CMM)

กำหนดค่า Chassis Management Module (CMM) หลักในตัวเครื่องของคุณเพื่อจัดการอุปกรณ์ทั้งหมดในตัวเครื่อง

เกี่ยวกับงานนี้

สำหรับข้อมูลโดยละเอียดเกี่ยวกับการกำหนดค่า CMM โปรดดู การกำหนดค่าส่วนประกอบตัวเครื่องในเอกสารแบบออนไลน์ ของ Flex System

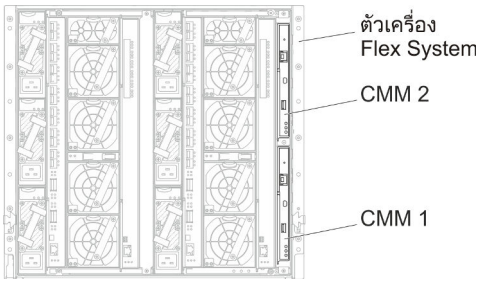
นอกจากนี้ โปรดดูขั้นตอน 4.1 - 4.5 บนโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้ในการกำหนดค่า CMM

หากมีการติดตั้ง CMM สองตัว ให้กำหนดค่าเฉพาะ CMM *หลัก* ซึ่งจะซิงโครไนซ์การกำหนดค่ากับ CMM สแตนด์บายโดยอัตโนมัติ

ขั้นตอนที่ 1. เชื่อมต่อสายอีเทอร์เน็ตจาก CMM ในช่อง 1 กับเวิร์กสเตชันไคลเอ็นต์เพื่อสร้างการเชื่อมต่อโดยตรง



สำหรับการเชื่อมต่อกับ CMM เป็นครั้งแรก คุณอาจต้องเปลี่ยนคุณสมบัติของอินเทอร์เน็ตโปรโตคอลในเวิร์กสเตชันไคลเอ็นต์

ข้อสำคัญ: ตรวจสอบให้แน่ใจว่าซับเน็ตเวิร์กสเตชันไคลเอ็นต์เป็นซับเน็ตเดียวกับซับเน็ต CMM (ซับเน็ต CMM เริ่มต้นคือ 255.255.255.0) ที่อยู่ IP ที่เลือกสำหรับเวิร์กสเตชันไคลเอ็นต์ต้องอยู่บนเครือข่ายเดียวกันกับ CMM (ตัวอย่างเช่น 192.168.70.0 - 192.168.70.24)

ขั้นตอนที่ 2. ในการเปิดอินเทอร์เฟซการจัดการ CMM ให้เปิดเว็บเบราเซอร์บนเวิร์กสเตชันไคลเอ็นต์ และกำหนดให้ไปยังที่อยู่ IP ของ CMM

หมายเหตุ:

- ตรวจสอบว่าคุณใช้การเชื่อมต่อที่ปลอดภัย และรวม **https** ไว้ใน URL (ตัวอย่างเช่น https://192.168.70.100) หากคุณไม่รวม https คุณจะได้รับข้อผิดพลาด ไม่พบเพจ

- หากคุณใช้ที่อยู่ IP เริ่มต้น 192.168.70.100 อินเทอร์เฟซการจัดการ CMM อาจใช้เวลาสักครู่กว่าจะใช้ได้ ความล่าช้านี้เกิดขึ้นเนื่องจาก CMM พยายามรับที่อยู่ DHCP เป็นเวลาสองนาทีขึ้นไปก่อนที่จะกลับมาเป็นที่อยู่คงที่เริ่มต้น

ขั้นตอนที่ 3. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ ID ผู้ใช้เริ่มต้น `USERID` และรหัสผ่าน `PASSWORD` หลังจากเข้าสู่ระบบ คุณต้องเปลี่ยนรหัสผ่านเริ่มต้น

ขั้นตอนที่ 4. ดำเนินการตัวช่วยสร้างการตั้งค่าเริ่มต้นของ CMM เพื่อระบุรายละเอียดสำหรับสภาพแวดล้อมของคุณ ตัวช่วยสร้างการตั้งค่าเริ่มต้นมีตัวเลือกดังต่อไปนี้:

- ดูรายการอุปกรณ์และสถานภาพของตัวเครื่อง
- นำเข้าการกำหนดค่าจากไฟล์การกำหนดค่าที่มีอยู่
- กำหนดค่าการตั้งค่า CMM ทั่วไป
- กำหนดค่าวันที่และเวลาของ CMM

  คำแนะนำ: เมื่อคุณติดตั้ง XClarity Administrator คุณจะกำหนดค่า XClarity Administrator และตัวเครื่องทั้งหมดที่ได้รับการจัดการโดย XClarity Administrator ให้ใช้เซิร์ฟเวอร์ NTP
- กำหนดค่าข้อมูล IP ของ CMM
- กำหนดค่านโยบายการรักษาความปลอดภัยของ CMM
- กำหนดค่า Domain Name System (DNS)
- กำหนดค่าระบบส่งต่อเหตุการณ์

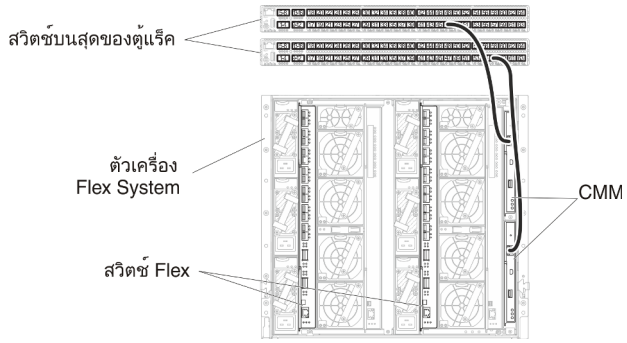
ขั้นตอนที่ 5. หลังจากบันทึกการตั้งค่าของตัวช่วยสร้างการตั้งค่าและใช้การเปลี่ยนแปลงแล้ว ให้กำหนดค่าที่อยู่ IP สำหรับส่วนประกอบทั้งหมดในตัวเครื่อง

โปรดดูขั้นตอน 4.6 ในโปสเตอร์คำแนะนำที่ให้มาพร้อมกับตัวเครื่องของคุณ

หมายเหตุ: คุณต้องรีเซ็ตหน่วยประมวลผลการจัดการระบบสำหรับโหนดคอมพิวท์แต่ละโหนด และรีสตาร์ทสวิตช์ Flex เพื่อแสดงที่อยู่ IP ใหม่

ขั้นตอนที่ 6. รีสตาร์ท CMM โดยใช้อินเทอร์เฟซการจัดการ CMM

ขั้นตอนที่ 7. ขณะที่ CMM กำลังรีสตาร์ท ให้เชื่อมต่อสายเคเบิลจากพอร์ตอีเทอร์เน็ตบน CMM กับเครือข่ายของคุณ



ขั้นตอนที่ 8. เข้าสู่ระบบอินเทอร์เฟซการจัดการ CMM โดยใช้ที่อยู่ IP ใหม่

หลังจากดำเนินการเสร็จ

คุณยังสามารถกำหนดค่า CMM ให้สนับสนุนการสำรองด้วย ใช้ระบบวิธีใช้ CMM เพื่อดูข้อมูลเพิ่มเติมเกี่ยวกับฟิลด์ที่มีอยู่ในแต่ละหน้าต่อไปนี้

- กำหนดค่าการทำงานล้มเหลวสำหรับ CMM ในกรณีฮาร์ดแวร์ทำงานล้มเหลวใน CMM หลัก จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **คุณสมบัติ** ➔ **การทำงานล้มเหลวขั้นสูง**
- กำหนดค่าการทำงานล้มเหลวเป็นผลมาจากปัญหาของเครือข่าย (อัปลิงค์) จากอินเทอร์เฟซการจัดการ CMM ให้คลิก **การจัดการโมดูล** Mgt ➔ **เครือข่าย** คลิกแท็บ **อีเทอร์เน็ต** จากนั้นคลิก **อีเทอร์เน็ตขั้นสูง** ในระดับต่ำที่สุด โปรดตรวจสอบให้แน่ใจว่าคุณเลือก **ทำงานล้มเหลวเนื่องจากไม่มีลิงก์เครือข่าย**

ขั้นตอนที่ 4: กำหนดค่า สวิตช์ Flex

กำหนดค่า สวิตช์ Flex ในแต่ละตัวเครื่อง

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตภายนอกจากสวิตช์ Flex ไปยังสวิตช์บนสุดของแร็ค และพอร์ตภายในไปยัง CMM

หากตั้งค่าสวิตช์ Flex ให้รับการตั้งค่าเครือข่ายแบบไดนามิก (ที่อยู่ IP, เน็ตมาสก์, เกตเวย์ และที่อยู่ DNS) ผ่าน DHCP โปรดตรวจสอบให้แน่ใจว่าสวิตช์ Flex มีการตั้งค่าที่สอดคล้องกัน (ตัวอย่างเช่น ตรวจสอบให้แน่ใจว่าที่อยู่ IP อยู่ในซับเน็ตเดียวกันกับ CMM)

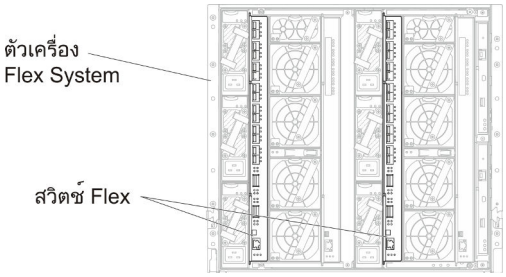
ข้อสำคัญ: สำหรับตัวเครื่อง Flex System แต่ละเครื่อง ตรวจสอบให้แน่ใจว่าประเภทโครงสร้างของการ์ดขยายในเซิร์ฟเวอร์แต่ละตัวในตัวเครื่องเข้ากันได้กับประเภทโครงสร้างของสวิตช์ Flex ทั้งหมดในตัวเครื่องเดียวกัน ตัวอย่างเช่น หากมีการติดตั้งสวิตช์อีเทอร์เน็ตในตัวเครื่อง เซิร์ฟเวอร์ทั้งหมดในตัวเครื่องนั้นต้องมีการเชื่อมต่ออีเทอร์เน็ตผ่านทางขั้วต่อ LAN-on-motherboard หรือการ์ดขยายอีเทอร์เน็ต สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการกำหนดค่าสวิตช์เครือข่าย Flex โปรดดู การกำหนดค่าโมดูล I/O ในเอกสารแบบออนไลน์ของ Flex Systems

ขั้นตอน

ขั้นตอนการกำหนดค่าอาจแตกต่างกัน โดยขึ้นอยู่กับประเภทของ สวิตช์ Flex ที่ติดตั้ง สำหรับข้อมูลเพิ่มเติมเกี่ยวกับสวิตช์ Flex, ดู สวิตช์เครือข่าย Flex System ในเอกสารแบบออนไลน์ของ Flex Systems ที่ได้รับการสนับสนุนแต่ละรายการ

ตามปกติแล้ว คุณต้องกำหนดค่าสวิตช์ Flex ในช่องใส่สวิตช์ Flex 1 และ 2

คำแนะนำ: ช่องใส่สวิตช์ Flex 2 คือช่องใส่โมดูลที่สามเมื่อดูที่ด้านหลังของตัวเครื่อง



รูปภาพ 24. ตำแหน่งของ สวิตช์ Flex ในตัวเครื่อง

ขั้นตอนที่ 5: ติดตั้งและกำหนดค่าโฮสต์

คุณสามารถติดตั้ง Docker ในระบบที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ Lenovo XClarity Administrator

ก่อนจะเริ่มต้น

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ XClarity Administrator ที่ใช้ Docker Engine สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

ตรวจสอบให้แน่ใจว่าโฮสต์ที่มีคุณสมบัติตรงตามข้อกำหนดเบื้องต้นที่กำหนดไว้ใน ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ข้อสำคัญ: คุณสามารถตั้งค่า XClarity Administrator บนระบบใดๆ ที่มีคุณสมบัติตรงตามข้อกำหนดสำหรับ XClarity Administrator รวมถึงเซิร์ฟเวอร์ที่ได้รับการจัดการ หากคุณใช้เซิร์ฟเวอร์ที่ได้รับการจัดการสำหรับโฮสต์ของ XClarity Administrator:

- คุณต้องโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการที่แยกจากกันแบบเสมือนจริง หรือโทโพโลยีเครือข่ายข้อมูลและเครือข่ายการจัดการเดี่ยว
- คุณไม่สามารถใช้ XClarity Administrator เพื่อใช้การอัปเดตเฟิร์มแวร์กับเซิร์ฟเวอร์ที่ได้รับการจัดการนั้นได้ แม้ว่าจะมีเฉพาะเฟิร์มแวร์บางตัวเท่านั้นที่ใช้กับการเปิดใช้งานทันที XClarity Administrator จะบังคับให้เซิร์ฟเวอร์เป้าหมายรีสตาร์ทใหม่ ซึ่งจะเป็นการรีสตาร์ท XClarity Administrator ด้วยเช่นกัน เมื่อใช้กับการเปิดใช้งานแบบเลื่อน ระบบจะใช้เฟิร์มแวร์บางอย่างเท่านั้นเมื่อมีการรีสตาร์ทโฮสต์ของ XClarity Administrator
- หากคุณใช้กับเซิร์ฟเวอร์ในตัวเครื่อง Flex System ตรวจสอบให้แน่ใจว่าได้ตั้งค่าให้เซิร์ฟเวอร์เปิดเครื่องเองโดยอัตโนมัติ คุณสามารถตั้งค่าตัวเลือกนี้จากเว็บอินเทอร์เฟซของ CMM โดยคลิก **การจัดการตัวเครื่อง ➜ โหนดคอมพิวท์** แล้วเลือกเซิร์ฟเวอร์ และเลือก **เปิดอัตโนมัติ** สำหรับ **โหมดเปิดอัตโนมัติ**

ขั้นตอน

ติดตั้งและกำหนดค่า Docker บนโฮสต์โดยใช้คำแนะนำที่มาพร้อมการจัดจำหน่าย Docker

ขั้นตอนที่ 6. ติดตั้งและกำหนดค่า XClarity Administrator

ติดตั้งและกำหนดค่าคอนเทนเนอร์ Lenovo XClarity Administrator บนโฮสต์ Docker ที่เพิ่งติดตั้ง

ก่อนจะเริ่มต้น

ตรวจสอบว่าระบบโฮสต์ของคุณมีคุณสมบัติฮาร์ดแวร์และซอฟต์แวร์ตรงตามข้อกำหนดขั้นต่ำของระบบ (โปรดดู ข้อกำหนดฮาร์ดแวร์และซอฟต์แวร์เบื้องต้น)

ตรวจสอบให้แน่ใจว่าได้เปิดใช้งานพอร์ตที่เหมาะสมทั้งหมด รวมถึงพอร์ตที่ XClarity Administrator ต้องการ (โปรดดู ความพร้อมใช้งานของพอร์ต)

ตรวจสอบให้แน่ใจว่าระบบโฮสต์อยู่ในเครือข่ายเดียวกันกับอุปกรณ์ที่คุณต้องการจัดการ

ตรวจสอบให้แน่ใจว่า OS ของโฮสต์และ XClarity Administrator ใช้เซิร์ฟเวอร์ NTP เดียวกัน

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูล การจัดการฮาร์ดแวร์ และการปรับใช้ OS (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้จะใช้ eth0

XClarity Administrator อนุญาตให้ใช้ชื่อที่กำหนดเองสำหรับเครือข่ายที่จะใช้สำหรับการจัดการข้อมูลและฮาร์ดแวร์ (ดู การกำหนดค่าเครือข่าย) ตัวอย่างในขั้นตอนต่อไปนี้จะใช้ eth0

ตรวจสอบให้แน่ใจว่ามีการโหลดเครือข่าย macvlan ลงในเคอร์เนลบนระบบโฮสต์ ใช้คำสั่ง **lsmod | grep macvlan** เพื่อตรวจสอบการโหลด ใช้คำสั่ง **modprobe macvlan** เพื่อโหลด macvlan ลงในเคอร์เนล

ตรวจสอบให้แน่ใจว่าคุณใช้ชื่อและที่อยู่ IP ที่ไม่ซ้ำกันสำหรับแต่ละคอนเทนเนอร์เมื่อใช้งานหลายคอนเทนเนอร์ XClarity Administrator บนโฮสต์เดียวกัน

หากคุณต้องการจัดการ ThinkServer และอุปกรณ์แบบดั้งเดิมอื่นๆ ตรวจสอบให้แน่ใจว่าได้เปิดใช้งาน Docker เพื่อรองรับ IPv6

1. แก้ไขไฟล์ /etc/docker/daemon.json ตั้งค่าคีย์ **ipv6** เป็นจริง และตั้งค่าคีย์ **fixed-cidr-v6** เป็นเครือข่ายย่อย IPv6 ของคุณ ข้อมูลต่อไปนี้คือตัวอย่างไฟล์ Daemon
   ```
   {
      "ipv6": true,
      "fixed-cidr-v6": "2001:db8:1::/64",
      "experimental": true,
      "ip6tables": true
   }
   ```
2. โหลดไฟล์การกำหนดค่า Docker อีกครั้งโดยเรียกใช้คำสั่งต่อไปนี้
   ```
   systemctl reload docker
   ```

หมายเหตุ: XClarity Administrator *ไม่ได้*รันเป็นคอนเทนเนอร์ที่มีสิทธิ์

ขั้นตอน

หากต้องการติดตั้งคอนเทนเนอร์ XClarity Administrator โดยใช้ Docker-compose ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ดาวน์โหลดอิมเมจอุปกรณ์เสมือน XClarity Administrator ไฟล์สภาพแวดล้อม และไฟล์ YAML จาก เว็บเพจการดาวน์โหลด XClarity Administrator ไปยังเวิร์กสเตชันไคลเอ็นต์ เข้าสู่ระบบเว็บไซต์ แล้วใช้คีย์การเข้าถึงที่กำหนดให้คุณใช้ดาวน์โหลดอิมเมจ

ขั้นตอนที่ 2. นำเข้าอิมเมจคอนเทนเนอร์ XClarity Administrator ลงในโฮสต์ Docker โดยการเรียกใช้คำสั่งต่อไปนี้
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

ขั้นตอนที่ 3. แก้ไขไฟล์ **docker_compose.env** และอัปเดตตัวแปรสภาพแวดล้อมต่อไปนี้

- CONTAINER_NAME ชื่อคอนเทนเนอร์ที่ไม่ซ้ำกัน ใช้เพื่อสร้างโวลุ่ม Docker สำหรับแต่ละอินสแตนซ์ XClarity Administrator (ตัวอย่างเช่น **CONTAINER_NAME=LXCA-203**)
- ADDRESS ที่อยู่ IPv4 แบบคงที่สำหรับคอนเทนเนอร์ (ตัวอย่างเช่น **ADDRESS=192.0.2.0**)
- BACKUP_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เพื่อจัดเก็บข้อมูลสำรองของ XClarity Administrator นี่ต้องเป็น **/mnt/backup_share**
- FIRMWARE_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เป็นที่เก็บข้อมูลระยะไกลสำหรับการอัปเดตเฟิร์มแวร์ นี่ต้องเป็น **/mnt/fw_share**

ข้อมูลต่อไปนี้คือตัวอย่างไฟล์สภาพแวดล้อม

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

ขั้นตอนที่ 4. แก้ไข **docker_compose.yml** และอัปเดตคุณสมบัติต่อไปนี้

- ตั้งค่าคุณสมบัติ **อิมเมจ** เป็นชื่อของไฟล์อิมเมจการติดตั้งที่ใช้ในขั้นตอนที่ 2

  หมายเหตุ: คุณสามารถเปลี่ยนชื่อไฟล์อิมเมจ (ตัวอย่างเช่น “ล่าสุด”) โดยใช้คำสั่ง `docker tag`
- หากคุณต้องการใช้การแชร์ระยะไกลเป็นที่เก็บข้อมูลเฟิร์มแวร์ระยะไกลและเพื่อจัดเก็บข้อมูลสำรอง XClarity Administrator ให้ตั้งค่าจุดติดตั้งโฮสต์สำหรับการแชร์ระยะไกลแต่ละรายการในคุณสมบัติ **โวลุ่ม**
- ตั้งค่าคุณสมบัติ **dns** เป็นที่อยู่ IP ของเซิร์ฟเวอร์ DNS
- คอนเทนเนอร์แชร์พูลของทรัพยากรโปรเซสเซอร์และหน่วยความจำที่โฮสต์ใช้งานได้ หรือเลือกที่จะกำหนดขีดจำกัดในการใช้ทรัพยากรโดยการตั้งค่าคุณสมบัติ CPU และ **หน่วยความจำ**
- ตั้งค่าคุณสมบัติ **หลัก** เป็นชื่ออินเทอร์เฟซเครือข่ายบนระบบโฮสต์ที่จะใช้เป็นอินเทอร์เฟซหลักของอินเทอร์เฟซ macvlan ในคอนเทนเนอร์ อินเทอร์เฟซนี้ต้องมีสิทธิ์การเข้าถึงเครือข่ายย่อยที่กำหนดให้กับคอนเทนเนอร์โดยตรง
- ตั้งค่า **subnet** และ **gateway** ตามโทโพโลยีเครือข่ายของคุณ โดยปกแล้วติ เครือข่ายย่อยและเกตเวย์จะใช้สำหรับเครือข่ายการจัดการ ซึ่งใช้ ${ADDRESS}
- หากคุณต้องการรองรับ IPv6 ให้ตั้งค่าคุณสมบัติ **enable_ipv6** เป็นจริง ตั้งค่าคุณสมบัติ **ipv6_address** เป็นที่อยู่ IPv6 และเพิ่มคุณสมบัติ **subnet** และ **gateway** อีกชุดตามโทโพโลยีเครือข่ายของคุณ (โดยปกติจะใช้กับเครือข่ายการจัดการซึ่งมีที่อยู่ IPv6 อยู่)

ต่อไปนี้คือตัวอย่างไฟล์ YML ที่เปิดใช้งาน IPv6

```
version: '3.8'

services:

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

```
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

ขั้นตอนที่ 5. ปรับใช้อิมเมจใน Docker โดยการเรียกใช้คำสั่งต่อไปนี้ โดยที่ *<ENV_FILENAME>* คือชื่อของไฟล์ตัวแปรสภาพแวดล้อมที่สร้างขึ้นในขั้นตอนที่ 2

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

หลังจากดำเนินการเสร็จ

เข้าสู่ระบบและกำหนดค่า XClarity Administrator (โปรดดู การเข้าถึงเว็บอินเทอร์เฟซ Lenovo XClarity Administrator เป็นครั้งแรก และ การกำหนดค่า Lenovo XClarity Administrator)

การใช้งานความพร้อมใช้งานสูง

คุณสามารถใช้ Docker Datacenter ตั้งค่าสภาพแวดล้อมความพร้อมใช้งานสูงสำหรับคอนเทนเนอร์ Lenovo XClarity Administrator ที่ใช้ Docker Engine

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความพร้อมใช้งานสูงของ Docker Datacenter โปรดดู เว็บเพจสถาปัตยกรรมและแอปความพร้อมใช้งานสูงด้วย Docker Datacenter

บทที่ 4. การกำหนดค่า Lenovo XClarity Administrator

เมื่อคุณเข้าใช้ Lenovo XClarity Administrator เป็นครั้งแรก คุณต้องดำเนินการหลายขั้นตอนเพื่อเริ่มต้นตั้งค่า XClarity Administrator

เรียนรู้เพิ่มเติม: XClarity Administrator: การกำหนดค่า ครั้งแรก

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อตั้งค่า XClarity Administrator เป็นครั้งแรก

ขั้นตอนที่ 1. การเข้าถึงเว็บอินเทอร์เฟซ XClarity Administrator

ขั้นตอนที่ 2. อ่านและยอมรับข้อตกลงการอนุญาตให้ใช้สิทธิ

ขั้นตอนที่ 3. สร้างบัญชีผู้ใช้ที่มีสิทธิ์ระดับผู้ควบคุม

คำแนะนำ: ลองสร้างบัญชีผู้ใช้ที่มีสิทธิ์ระดับผู้ควบคุมอย่างน้อยสองบัญชีเพื่อให้คุณมีบัญชีสำรอง หากต้องการ กับที่จัดเก็บของผู้ควบคุมเพื่อให้มีการสำรอง หากจำเป็นต้องใช้งาน

ขั้นตอนที่ 4. กำหนดการเข้าถึงเครือข่าย รวมถึงที่อยู่ IP สำหรับเครือข่ายข้อมูลและการจัดการ

ขั้นตอนที่ 5. กำหนดค่าวันที่และเวลา

ขั้นตอนที่ 6. กำหนดค่าการตั้งค่าบริการและการสนับสนุน รวมถึงคำชี้แจงสิทธิ์ส่วนบุคคล ข้อมูลการใช้งานและฮาร์ดแวร์ บริการสนับสนุนของ Lenovo (Call Home) การอำนวยการอัปโหลด Lenovo และการรับประกันผลิตภัณฑ์

ขั้นตอนที่ 7. กำหนดค่าการตั้งค่าความปลอดภัย รวมถึง เซิร์ฟเวอร์ตรวจสอบความถูกต้อง, กลุ่มผู้ใช้, ใบรับรองเซิร์ฟเวอร์ และโหมดการเข้ารหัส

ขั้นตอนที่ 8. จัดการตัวเครื่อง, เซิร์ฟเวอร์, สวิตช์ และอุปกรณ์การจัดเก็บข้อมูล

การเข้าถึงเว็บอินเทอร์เฟซ Lenovo XClarity Administrator เป็นครั้งแรก

คุณสามารถเปิดเว็บอินเทอร์เฟซ XClarity Administrator จากคอมพิวเตอร์ที่มีการเชื่อมต่อเครือข่ายกับเครื่องเสมือน XClarity Administrator ได้

ก่อนจะเริ่มต้น

ตรวจสอบให้แน่ใจว่าคุณกำลังใช้หนึ่งในเว็บเบราเซอร์ที่รองรับต่อไปนี้:

- Chrome™ 48.0 หรือใหม่กว่า (55.0 หรือสูงกว่าสำหรับคอนโซลระยะไกล)
- Firefox® ESR 38.6.0 หรือใหม่กว่า
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 หรือใหม่กว่า (IOS7 หรือใหม่กว่าและ OS X)

หมายเหตุ: ไม่รองรับการเปิดใช้อินเทอร์เฟซ Management Controller จาก XClarity Administrator โดยใช้เว็บเบราเซอร์ Safari

ตรวจสอบให้แน่ใจว่าคุณได้เข้าสู่ระบบเว็บอินเทอร์เฟซ XClarity Administrator จากระบบที่มีการเชื่อมต่อเครือข่ายกับโหนดการจัดการ XClarity Administrator

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อเข้าใช้เว็บอินเทอร์เฟซ XClarity Administrator เป็นครั้งแรก

ขั้นตอนที่ 1. ชี้เบราเซอร์ของคุณไปยังที่อยู่ IP ของ XClarity Administrator

เคล็ดลับ: การเข้าถึงเว็บอินเทอร์เฟซจะดำเนินการผ่านการเชื่อมต่อที่มีความปลอดภัย ตรวจสอบให้แน่ใจว่าคุณใช้ https

- **สำหรับคอนเทนเนอร์** ให้ใช้ที่อยู่ IPv4 ที่ระบุไว้สำหรับตัวแปร ${ADDRESS} เพื่อเข้าถึง XClarity Administrator โดยใช้ URL ต่อไปนี้:
  `https://<IPv4_address>/ui/login.html`

  ตัวอย่าง:
  `https://192.0.2.10/ui/login.html`
- **สำหรับอุปกรณ์เสมือน** ที่อยู่ IP ที่คุณใช้ขึ้นอยู่กับการตั้งค่าสภาพแวดล้อมของคุณ

  หากคุณมีเครือข่าย Eth0 และ Eth1 บนซับเน็ตที่แยกต่างหาก และหากมีการใช้ DHCP บนทั้งสองซับเน็ต ให้ใช้ที่อยู่ IP ของ *Eth1* เมื่อเข้าถึงเว็บอินเทอร์เฟซสำหรับการตั้งค่าเริ่มต้น เมื่อ XClarity Administrator เริ่มต้นเป็นครั้งแรก ทั้ง Eth0 และ Eth1 จะได้รับที่อยู่ IP ที่กำหนด DHCP และเกตเวย์เริ่มต้นของ XClarity Administrator จะได้รับการตั้งค่าเป็นเกตเวย์ที่กำหนด DHCP สำหรับ *Eth1*

  ใช้ที่อยู่ IPv4 แบบคงที่

  หากคุณกำหนดที่อยู่ IPv4 ใน eth0_config ให้ใช้ที่อยู่ IPv4 นั้นในการเข้าถึง XClarity Administrator โดยใช้ URL ต่อไปนี้:
  `https://<IPv4_address>/ui/login.html`

ตัวอย่าง:
`https://192.0.2.10/ui/login.html`

ให้ใช้เซิร์ฟเวอร์ DHCP ในโดเมนบรอดแคสต์เดียวกันกับ XClarity Administrator

หากเซิร์ฟเวอร์ DHCP ได้รับการตั้งค่าโดเมนบรอดแคสต์เดียวกันกับ XClarity Administrator ให้ใช้ที่อยู่ IPv4 ที่แสดงใน XClarity Administrator คอนโซลเครื่องเสมือนเพื่อเข้าถึง XClarity Administrator โดยใช้ URL ต่อไปนี้:
`https://<IPv4_address>/ui/login.html`

ตัวอย่าง:
`https://192.0.2.10/ui/login.html`

ให้ใช้เซิร์ฟเวอร์ DHCP ในโดเมนบรอดแคสต์ต่างกันกับ XClarity Administrator

หากเซิร์ฟเวอร์ DHCP *ไม่ได้* รับการตั้งค่าในโดเมนบรอดแคสต์เดียวกัน ให้ใช้ที่อยู่ IPv6 Link Local (LLA) ที่แสดงบน eEth0 (เครือข่ายการจัดการ) ใน XClarity Administrator คอนโซลเครื่องเสมือนเพื่อเข้าถึง XClarity Administrator ตัวอย่างเช่น:

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

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

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

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

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

เคล็ดลับ: ที่อยู่ IPv6 Link Local (LLA) จะมาจากที่อยู่ MAC ของอินเทอร์เฟซ

ข้อควรพิจารณา: หากคุณกำหนดค่า XClarity Administrator จากระยะไกล คุณต้องมีการเชื่อมต่อกับเครือข่ายเลเยอร์ 2 เครือข่ายเดียวกัน ซึ่งต้องเข้าถึงจากที่อยู่ที่ไม่มีการกำหนดเส้นทางจนกว่าการตั้งค่าเริ่มต้นจะเสร็จสมบูรณ์ ดังนั้น ให้พิจารณาการเข้าถึงXClarity Administratorจาก VM อื่นที่มีการเชื่อมต่อกับ XClarity Administrator ตัวอย่างเช่น คุณสามารถเข้าถึง XClarity Administrator จาก VM อื่นบนโฮสต์ที่มีการติดตั้ง XClarity Administrator

– Firefox:

ในการเข้าถึงเว็บอินเทอร์เฟซ XClarity Administrator จากเบราเซอร์ Firefox ให้เข้าสู่ระบบโดยใช้ URL ต่อไปนี้ โปรดสังเกตว่าจำเป็นต้องมีวงเล็บเมื่อป้อนที่อยู่ IPv6

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

ตัวอย่างเช่น จากตัวอย่างก่อนหน้าที่แสดงสำหรับ Eth0 ให้ป้อน URL ต่อไปนี้ในเว็บเบราเซอร์ของคุณ:

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

- Internet Explorer:

  ในการเข้าถึงเว็บอินเทอร์เฟซ XClarity Administrator จากเบราเซอร์ Internet Explorer ให้เข้าสู่ระบบโดยใช้ URL ต่อไปนี้ โปรดสังเกตว่าจำเป็นต้องมีวงเล็บเมื่อป้อนที่อยู่ IPv6

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

  โดยที่ *<zone_index>* คือตัวระบุสำหรับอะแดปเตอร์อีเทอร์เน็ตที่เชื่อมต่อกับเครือข่ายการจัดการจากคอมพิวเตอร์ที่คุณเปิดใช้เว็บเบราเซอร์ หากคุณใช้เบราเซอร์บน Windows ให้ใช้คำสั่ง `ipconfig` เพื่อค้นหาดัชนีโซนซึ่งแสดงต่อจากเครื่องหมายเปอร์เซ็นต์ (%) ในฟิลด์ **ที่อยู่** IPv6 Link Local สำหรับอะแดปเตอร์ ในตัวอย่างต่อไปนี้ ดัชนีโซนคือ “30”

  ```
  PS C:> ipconfig
  การกำหนดค่า Windows IP

  อะแดปเตอร์อีเทอร์เน็ต vEthernet (teamVirtualSwitch):

     ส่วนต่อท้าย DNS เฉพาะการเชื่อมต่อ  . :
     ที่อยู่ IPv6 Link Local . . . . . : 2001:db8:56ff:fe80:bea3%30
     ที่อยู่ IPv4 การกำหนดค่าอัตโนมัติ. . : 192.0.2.30
     เกตเวย์เริ่มต้น . . . . . :
  ```

  หากคุณใช้เบราเซอร์บน Linux ให้ใช้คำสั่ง `ifconfig` เพื่อค้นหาดัชนีโซน คุณยังสามารถใช้ชื่อของอะแดปเตอร์ (โดยทั่วไปคือ Eth0) เป็นดัชนีโซนได้ด้วย

  ตัวอย่างเช่น จากตัวอย่างที่แสดงสำหรับ Eth0 และดัชนีโซน ให้ป้อน URL ต่อไปนี้ในเว็บเบราเซอร์ของคุณ:

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

ขั้นตอนที่ 2. คุณอาจได้รับคำเตือนเกี่ยวกับความปลอดภัยหรือใบรับรองในครั้งแรกที่คุณเข้าใช้ Lenovo XClarity Administrator คุณสามารถละเว้นคำเตือนนั้น

ผลลัพธ์

หน้า การตั้งค่าเริ่มต้น จะแสดงขึ้น

หลังจากดำเนินการเสร็จ

ดำเนินการขั้นตอนการตั้งค่าเริ่มต้นเพื่อกำหนดค่า XClarity Administrator (โปรดดู การกำหนดค่า Lenovo XClarity Administrator)

การสร้างบัญชีผู้ใช้

บัญชีผู้ใช้ที่ใช้เพื่อจัดการการตรวจสอบความถูกต้องและการเข้าถึง Lenovo XClarity Administrator และอุปกรณ์ที่อยู่ภายใต้การตรวจสอบความถูกต้องที่ได้รับการจัดการ

เกี่ยวกับงานนี้

บัญชีผู้ใช้บัญชีแรกที่คุณสร้างต้องมีบทบาทผู้ควบคุมและเปิดการใช้งานอยู่

เนื่องจากมาตรการรักษาความปลอดภัยที่เข้มงวดขึ้น ให้สร้างบัญชีผู้ใช้อย่างน้อย 2 บัญชีที่มีบทบาท **ผู้ควบคุม** อย่าลืมบันทึกรหัสผ่านสำหรับบัญชีผู้ใช้เหล่านี้และเก็บไว้ในที่ปลอดภัย เผื่อไว้ในกรณีที่ต้องกู้คืน Lenovo XClarity Administrator

ขั้นตอน

ในการสร้างบัญชีผู้ใช้ ให้ดำเนินการขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. กรอกข้อมูลต่อไปนี้ในกล่องโต้ตอบสร้างผู้ใช้ระดับผู้ควบคุมใหม่

- ป้อนชื่อผู้ใช้และรายละเอียดของผู้ใช้
- ป้อนรหัสผ่านใหม่และยืนยัน กฎสำหรับรหัสผ่านขึ้นอยู่กับการตั้งค่าการรักษาความปลอดภัยบัญชีในปัจจุบัน
- เลือกกลุ่มบทบาทอย่างน้อยหนึ่งกลุ่มเพื่ออนุญาตให้ผู้ใช้ดำเนินงานที่เหมาะสมได้

  สำหรับข้อมูลเกี่ยวกับกลุ่มบทบาทและวิธีการสร้างกลุ่มบทบาทที่กำหนดเอง โปรดดู การสร้างกลุ่มบทบาท ในเอกสารแบบออนไลน์ของ XClarity Administrator
- (ไม่บังคับ) ตั้งค่า **เปลี่ยนรหัสผ่านเมื่อเข้าใช้งานครั้งแรก** เป็น `Yes` ถ้าคุณต้องการบังคับให้ผู้ใช้เปลี่ยนรหัสผ่านในครั้งแรกที่ผู้ใช้เข้าสู่ระบบ XClarity Administrator

ขั้นตอนที่ 2. คลิก **สร้าง**

ขั้นตอนที่ 3. คลิกไอคอน **สร้าง** ( ) และทำซ้ำขั้นตอนก่อนหน้าเพื่อสร้างผู้ใช้เพิ่มเติม

ขั้นตอนที่ 4. คลิก **กลับไปที่การตั้งค่าเริ่มต้น**

การกำหนดค่าการเข้าถึงเครือข่าย

ในการกำหนดค่าการเข้าถึงเครือข่าย คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายได้สูงสุดสองชุด ชื่อโฮสต์สำหรับ Lenovo XClarity Administrator และเซิร์ฟเวอร์ DNS ที่จะใช้

เกี่ยวกับงานนี้

XClarity Administrator มีอินเทอร์เฟซเครือข่ายต่างหากสองส่วนที่สามารถกำหนดให้กับระบบของคุณได้ ขึ้นอยู่กับโทโพโลยีเครือข่ายที่คุณนำมาใช้ สำหรับอุปกรณ์เสมือน เครือข่ายเหล่านี้มีจะชื่อเป็น eth0 และ eth1 สำหรับคอนเทนเนอร์ คุณสามารถเลือกชื่อที่กำหนดเองได้

- กรณีที่มีเพียงอินเทอร์เฟซเครือข่ายเดียว (eth0):
  - ต้องกำหนดค่าอินเทอร์เฟซเพื่อสนับสนุนการค้นหาและการจัดการอุปกรณ์ (เช่น การอัปเดตการกำหนดค่าและเฟิร์มแวร์) โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการแผงวงจรในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง

- หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้นคุณต้องนำเข้าการอัปเดตลงในที่เก็บ
- หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
- หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์ของ OS อินเทอร์เฟซเครือข่ายจะต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเครือข่ายเซิร์ฟเวอร์ที่ใช้ในการเข้าถึงระบบปฏิบัติการโฮสต์

  หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเทอร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

- ในกรณีที่มีอินเทอร์เฟซเครือข่ายสองตัว (eth0 และ eth1):
  - อินเทอร์เฟซเครือข่ายแรก (โดยปกติคืออินเทอร์เฟซ Eth0) จะต้องเชื่อมต่อกับเครือข่ายการจัดการ และกำหนดค่าให้สนับสนุนการค้นหาและการจัดการอุปกรณ์ (รวมถึงการกำหนดค่าเซิร์ฟเวอร์และการอัปเดตเฟิร์มแวร์ โดยจะต้องสามารถสื่อสารกับ CMM และสวิตช์ Flex ได้ในแต่ละตัวเครื่องที่มีการจัดการ ตัวควบคุมการจัดการในเซิร์ฟเวอร์ที่ได้รับการจัดการแต่ละเครื่อง และสวิตช์ของ RackSwitch แต่ละเครื่อง
  - อินเทอร์เฟซเครือข่ายที่สอง (โดยทั่วไปคืออินเทอร์เฟซ eth1) จะสามารถกำหนดค่าให้สื่อสารกับเครือข่ายข้อมูลภายใน เครือข่ายข้อมูลสาธารณะ หรือทั้งสองเครือข่าย
  - หากคุณต้องการขอรับอัปเดตเฟิร์มแวร์และไดรเวอร์อุปกร์ของ OS โดยใช้ XClarity Administrator อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องมีการเชื่อมต่อกับอินเทอร์เน็ตด้วย โดยผ่านไฟร์วอลล์หากทำได้ มิฉะนั้นคุณต้องนำเข้าการอัปเดตลงในที่เก็บ
  - หากคุณต้องการเก็บข้อมูลบริการ หรือใช้การแจ้งเตือนปัญหาอัตโนมัติ (รวมถึง Call Home และการอำนวยการอัปโหลด Lenovo) อินเทอร์เฟซเครือข่ายอย่างน้อยหนึ่งรายการจะต้องเชื่อมต่อกับอินเทอร์เน็ต โดยผ่านไฟร์วอลล์หากทำได้
  - หากคุณต้องการปรับใช้อิมเมจระบบปฏิบัติการและการอัปเดตไดรเวอร์อุปกรณ์ คุณสามารถเลือกที่จะใช้อินเทอร์เฟซ eth1 หรือ eth0 ได้ อย่างไรก็ตาม อินเทอร์เฟซที่คุณใช้ต้องมีการเชื่อมต่อเครือข่าย IP กับอินเทอร์เฟซเซิร์ฟเวอร์เครือข่ายที่ใช้เพื่อเข้าถึงระบบปฏิบัติการโฮสต์

    หมายเหตุ: หากคุณใช้เครือข่ายต่างหากในการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ OS คุณสามารถกำหนดค่าอินเทอร์เฟซเครือข่ายที่สองเพื่อให้เชื่อมต่อกับเครือข่ายนั้นได้ แทนที่จะเชื่อมต่อกับเครือข่ายข้อมูล อย่างไรก็ตาม หากระบบปฏิบัติการบนเซิร์ฟเวอร์แต่ละตัวไม่มีสิทธิ์เข้าถึงเครือข่ายข้อมูล ให้กำหนดค่าอินเท

อร์เฟซเพิ่มเติมบนเซิร์ฟเวอร์เพื่อสร้างการเชื่อมต่อจากระบบปฏิบัติการโฮสต์บนเซิร์ฟเวอร์ไปยังเครือข่ายข้อมูลสำหรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ หากจำเป็น

ตารางต่อไปนี้แสดงการกำหนดค่าที่เป็นไปได้สำหรับอินเทอร์เฟซเครือข่าย XClarity Administrator ตามประเภทของโทโพโลยีเครือข่ายที่นำมาใช้งานในระบบของคุณ ใช้ตารางนี้เพื่อระบุวิธีการกำหนดอินเทอร์เฟซเครือข่ายแต่ละรายการ

ตาราง 3. บทบาทของอินเทอร์เฟซเครือข่ายแต่ละรายการตามโทโพโลยีเครือข่าย

โทโพโลยีเครือข่าย	**บทบาทของอินเทอร์เฟซ** 1 (eth0)	**บทบาทของอินเทอร์เฟซ** 2 (eth1)
เครือข่าย Converged (การจัดการและเครือข่ายข้อมูลที่รองรับการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS)	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS	ไม่มี
แยกเครือข่ายการจัดการที่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS และเครือข่ายข้อมูล	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS	เครือข่ายข้อมูล • ไม่มี

ตาราง 3. บทบาทของอินเทอร์เฟซเครือข่ายแต่ละรายการตามโทโพโลยีเครือข่าย (มีต่อ)

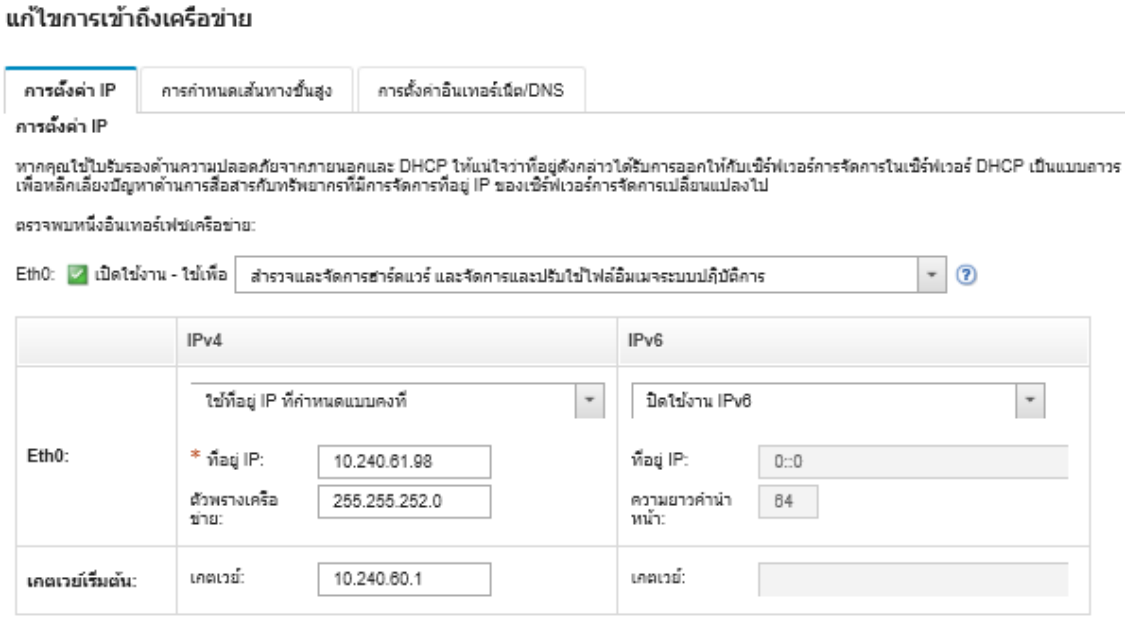
โทโพโลยีเครือข่าย	**บทบาทของอินเทอร์เฟซ** 1 (eth0)	**บทบาทของอินเทอร์เฟซ** 2 (eth1)
แยกเครือข่ายการจัดการและเครือข่ายข้อมูลที่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	เครือข่ายข้อมูล • การค้นหาและการจัดการ • การปรับใช้ OS • การอัปเดตไดรเวอร์ OS
แยกเครือข่ายการจัดการและเครือข่ายข้อมูลที่ไม่มีการสนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	เครือข่ายข้อมูล • ไม่มี
เฉพาะเครือข่ายการจัดการเท่านั้น (ไม่สนับสนุนการปรับใช้ OS และการอัปเดตไดรเวอร์อุปกรณ์ของ OS)	เครือข่ายการจัดการ • การค้นหาและการจัดการ • การกำหนดค่าเซิร์ฟเวอร์ • การอัปเดตเฟิร์มแวร์ • การรวบรวมข้อมูลบริการ • การแจ้งเตือนปัญหาอัตโนมัติ (เช่น Call Home และการอำนวยการอัปโหลด Lenovo) • การดึงข้อมูลการรับประกัน	ไม่มี

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอินเทอร์เฟซเครือข่ายของ XClarity Administrator โปรดดู ข้อควรพิจารณาด้านเครือข่าย

ขั้นตอน

ในการกำหนดค่าการเข้าถึงเครือข่าย ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. จากหน้า การตั้งค่าเริ่มต้น ให้คลิก **กำหนดการเข้าถึงเครือข่าย** หน้า แก้ไขการเข้าถึงเครือข่าย จะแสดงขึ้น



ขั้นตอนที่ 2. หากคุณต้องการปรับใช้ระบบปฏิบัติการและอัปเดตไดรเวอร์อุปกรณ์ของ OS โดยใช้ XClarity Administrator ให้เลือกอินเทอร์เฟสเครือข่ายที่จะใช้สำหรับการจัดการระบบปฏิบัติการ

- หากมีการกำหนดอินเทอร์เฟซเพียงหนึ่งรายการสำหรับ XClarity Administrator ให้เลือกว่าจะใช้อินเทอร์เฟซนั้นเพื่อค้นหาและจัดการฮาร์ดแวร์เท่านั้น หรือจะใช้เพื่อจัดการระบบปฏิบัติการด้วย
- หากกำหนดอินเทอร์เฟซสองรายการให้กับ XClarity Administrator (Eth0 และ Eth1) ให้กำหนดว่าจะใช้อินเทอร์เฟซใดในการจัดการระบบปฏิบัติการ หากคุณเลือก “ไม่มี” คุณจะ*ไม่*สามารถปรับใช้อิมเมจระบบปฏิบัติการ หรืออัปเดตไดรเวอร์อุปกรณ์ OS กับเซิร์ฟเวอร์ที่ได้รับการจัดการจาก XClarity Administrator

ขั้นตอนที่ 3. ระบุการตั้งค่า IP

a. สำหรับอินเทอร์เฟซแรก ให้ระบุที่อยู่ IPv4, ที่อยู่ IPv6 หรือทั้งคู่

- **IPv4** คุณต้องกำหนดที่อยู่ IPv4 ให้กับอินเทอร์เฟซ คุณสามารถเลือกที่จะใช้ที่อยู่ IP ที่กำหนดแบบคงที่ หรือเลือกรับที่อยู่ IP จากเซิร์ฟเวอร์ DHCP
- **IPv6** หรือคุณสามารถกำหนดที่อยู่ IPv6 ให้กับอินเทอร์เฟซโดยใช้การกำหนดวิธีใดวิธีหนึ่งต่อไปนี้:
  - ใช้ที่อยู่ IP ที่กำหนดแบบคงที่
  - ใช้การกำหนดค่าที่อยู่แบบมีสถานะ (DHCPv6)
  - ใช้การกำหนดค่าที่อยู่อัตโนมัติแบบสุ่ม

  หมายเหตุ: สำหรับข้อมูลเกี่ยวกับการจำกัดที่อยู่ IPv6 โปรดดู ข้อจำกัดของการกำหนดค่า IP

b. หากมีอินเทอร์เฟซที่สอง ให้ระบุที่อยู่ IPv4, ที่อยู่ IPv6 หรือทั้งคู่

หมายเหตุ: ที่อยู่ IP ที่กำหนดให้กับอินเทอร์เฟซนี้ต้องอยู่ในซับเน็ตอื่นที่ไม่ได้มาจากที่อยู่ IP ที่กำหนดให้กับอินเทอร์เฟซแรก หากคุณเลือกที่จะใช้ DHCP ในการกำหนดที่อยู่ IP ของอินเทอร์เฟซทั้งสอง (Eth0 และ Eth1) เซิร์ฟเวอร์ DHCP ต้องกำหนดซับเน็ตเดียวกันสำหรับที่อยู่ IP ของอินเทอร์เฟซสองรายการ

- **IPv4** คุณสามารถเลือกที่จะใช้ที่อยู่ IP ที่กำหนดแบบคงที่ หรือเลือกรับที่อยู่ IP จากเซิร์ฟเวอร์ DHCP
- **IPv6** หรือคุณสามารรถกำหนดที่อยู่ IPv6 ให้กับอินเทอร์เฟซโดยใช้การกำหนดวิธีใดวิธีหนึ่งต่อไปนี้:
  - ใช้ที่อยู่ IP ที่กำหนดแบบคงที่
  - ใช้การกำหนดค่าที่อยู่แบบมีสถานะ (DHCPv6)
  - ใช้การกำหนดค่าที่อยู่อัตโนมัติแบบสุ่ม

c. ระบุเกตเวย์เริ่มต้น

หากคุณระบุเกตเวย์เริ่มต้น เกตเวย์นั้นจะต้องเป็นที่อยู่ IP ที่ถูกต้องและต้องใช้มาสก์เครือข่ายเดียวกัน (ซับเน็ตเดียวกัน) กับที่อยู่ IP สำหรับหนึ่งในอินเทอร์เฟซเครือข่าย (Eth0 หรือ Eth1) หากคุณใช้อินเทอร์เฟซเดียว เกตเวย์เริ่มต้นจะต้องอยูบนซับเน็ตเดียวกันกับอินเทอร์เน็ตเครือข่าย

หาอินเทอร์เฟซตัวใดตัวหนึ่งใช้ DHCP เพื่อรับที่อยู่ IP เกตเวย์เริ่มต้นจะใช้ DHCP ด้วย หากต้องการป้อนที่อยู่เกตเวย์เริ่มต้นด้วยตนเอง ซึ่งแทนที่ที่อยู่ที่ได้รับจากเซิร์ฟเวอร์ DHCP ให้เลือกช่องทำเครื่องหมาย **แทนที่เกตเวย์**

เคล็ดลับ:

- ตรวจสอบให้แน่ใจว่าเกตเวย์ตรงกับเครือข่ายย่อยของอินเทอร์เฟซเครือข่ายตัวใดตัวหนึ่ง เกตเวย์เริ่มต้นจะได้รับการตั้งค่าผ่านอินเทอร์เฟซเครือข่ายโดยอัตโนมัติ
- หากต้องการกลับสู่เกตเวย์ที่ DHCP ระบุไว้ ให้ล้างช่องทำเครื่องหมาย **แทนที่เกตเวย์**

ข้อควรระวัง:
หากคุณเลือกที่จะแทนที่เกตเวย์ โปรดใช้ความระมัดระวังในการป้อนที่อยู่เกตเวย์ที่ถูกต้อง มิฉะนั้นเซิร์ฟเวอร์การจัดการนี้จะไม่สามารถเข้าถึงได้ และไม่สามารถเข้าสู่ระบบจากระยะไกลเพื่อแก้ไขได้

d. คลิก **บันทึกการตั้งค่า IP**

ขั้นตอนที่ 4. **ตัวเลือก**: กำหนดค่าการตั้งค่าขั้นสูง

a. คลิกแท็บ **การกำหนดเส้นทางขั้นสูง**

b. ระบุรายการเส้นทางอย่างน้อยหนึ่งรายการในตาราง **การตั้งค่าเส้นทางขั้นสูง** ที่อินเทอร์เฟซนี้จะใช้

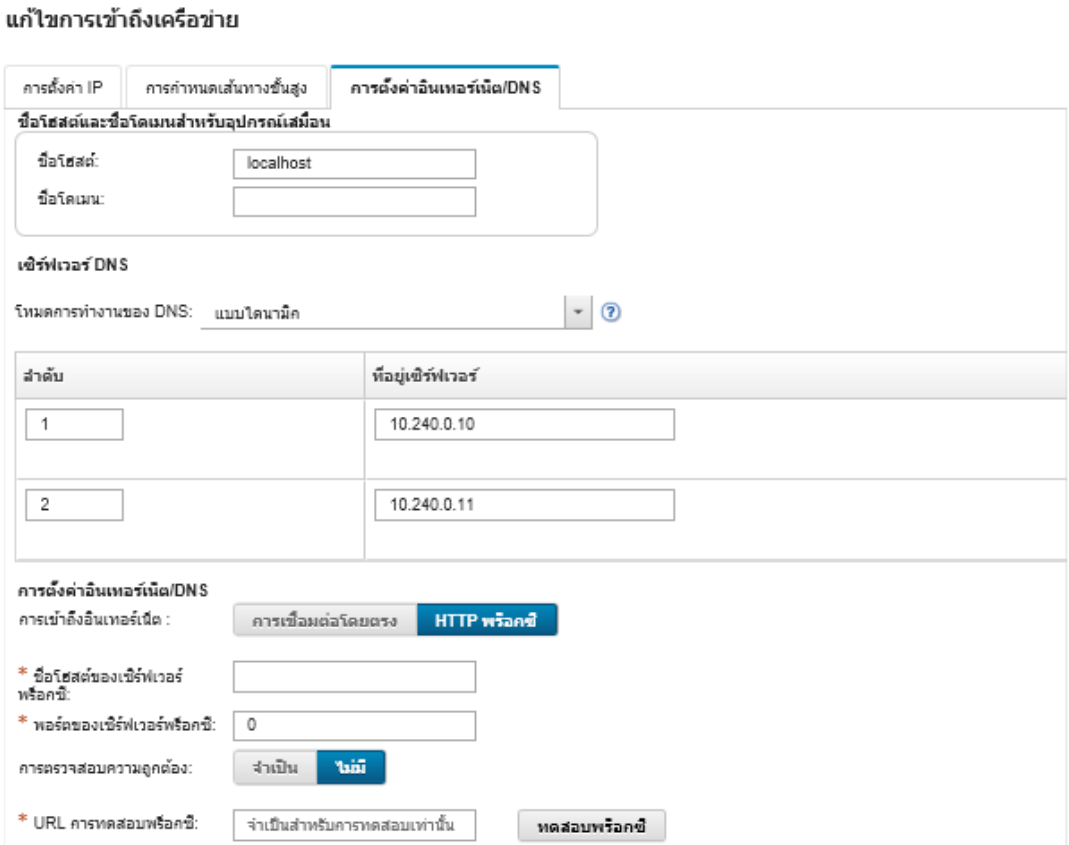
ในการกำหนดรายการเส้นทางอย่างน้อยหนึ่งรายการ ให้ดำเนินการขั้นตอนต่อไปนี้

1. เลือกอินเทอร์เฟซ
2. ระบุประเภทเส้นทาง ซึ่งสามารถเป็นเส้นทางไปยังโฮสต์อื่นหรือไปยังเครือข่าย
3. ระบุโฮสต์ปลายทางหรือที่อยู่เครือข่ายที่คุณจะกำหนดเส้นทางไป
4. ระบุซับเน็ตมาสก์สำหรับที่อยู่ปลายทาง
5. ระบุที่อยู่เกตเวย์ที่จะกำหนดที่อยู่แพ็คเก็ตให้

c. คลิก **บันทึกการกำหนดเส้นทางขั้นสูง**

ขั้นตอนที่ 5. สามารถเลือกที่จะปรับเปลี่ยนการตั้งค่า DNS และพร็อกซีได้

a. คลิกแท็บ **DNS และพร็อกซี**



b. ระบุชื่อโฮสต์และชื่อโดเมนที่จะใช้สำหรับ XClarity Administrator

c. เลือกโหมดการทำงานของ DNS โดยสามารถระบุเป็น **แบบคงที่** หรือ DHCP

ข้อควรพิจารณา: คุณต้องเริ่มระบบเซิร์ฟเวอร์การจัดการใหม่เมื่อคุณเปลี่ยนโหมดการดำเนินการ DNS

หมายเหตุ: หากคุณเลือกที่จะใช้เซิร์ฟเวอร์ DHCP เพื่อรับที่อยู่ IP การเปลี่ยนแปลงใดๆ ที่คุณทำกับฟิลด์ **เซิร์ฟเวอร์ DNS** จะถูกเขียนทับในครั้งถัดไปที่ XClarity Administrator ต่ออายุการเช่า DHCP

d. ระบุที่อยู่ IP ของ Domain Name System (DNS) อย่างน้อยหนึ่งรายการที่จะใช้และลำดับความสำคัญสำหรับแต่ละรายการ

e. ระบุว่าการเข้าถึงอินเทอร์เน็ตโดยใช้การเชื่อมต่อโดยตรงหรือพร็อกซี HTTP (หาก XClarity Administrator มีการเข้าถึงอินเทอร์เน็ต)

หมายเหตุ: ให้ใช้พร็อกซี HTTP ตรวจสอบให้แน่ใจว่าเป็นไปตามข้อกำหนดต่อไปนี้
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีให้ใช้การการตรวจสอบความถูกต้องพื้นฐาน
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีที่ไม่สิ้นสุด
- ตรวจสอบให้แน่ใจว่าได้ตั้งค่าเซิร์ฟเวอร์พร็อกซีเป็นพร็อกซีส่งต่อ
- ตรวจสอบให้แน่ใจว่ามีการกำหนดค่าให้โหลดบาลานเซอร์เก็บเซสชันไว้กับเซิร์ฟเวอร์พร็อกซีหนึ่งตัว และไม่มีการสลับไปมา

หากคุณเลือกที่จะใช้พร็อกซี HTTP ให้กรอกฟิลด์ที่จำเป็นต่อไปนี้
1. ระบุชื่อโฮสต์เซิร์ฟเวอร์พร็อกซีและพอร์ต
2. เลือกว่าจะใช้การตรวจสอบความถูกต้องหรือไม่ และระบุชื่อผู้ใช้และรหัสผ่านหากจำเป็น
3. ระบุ URL ทดสอบพร็อกซี
4. คลิก **ทดสอบพร็อกซี** เพื่อตรวจสอบว่าการตั้งค่าพร็อกซีได้รับการกำหนดค่าและทำงานอย่างถูกต้องหรือไม่

f. คลิก **บันทึก DNS และพร็อกซี**

g. พุชชื่อโดเมนแบบเต็ม (FQDN) ของเซิร์ฟเวอร์การจัดการ XClarity Administrator และข้อมูล DNS เพื่อไปยังเซิร์ฟเวอร์ที่มีการจัดการ ซึ่งมี IMM2, XCC และ XCC2 เพื่อให้เซิร์ฟเวอร์ที่มีการจัดการสามารถค้นหาเซิร์ฟเวอร์การจัดการโดยใช้ข้อมูลนี้

1. คลิก **พุช FQDN / DNS ไปยัง BMC**
2. เลือกวิธีการจัดการรายการ DNS ที่มีอยู่ในตัวควบคุมการจัดการแผงวงจร
   - เก็บรายการ DNS ที่มีอยู่ไว้ และต่อท้ายรายการ DNS ของเซิร์ฟเวอร์การจัดการลงในช่องว่างถัดไป
   - เปลี่ยนรายการ DNS ที่มีอยู่ทั้งหมดด้วยรายการ DNS ของเซิร์ฟเวอร์การจัดการ

3. พิมพ์ YES ในฟิลด์แก้ไข
4. คลิก **ใช้**

มีการสร้างงานขึ้นเพื่อการดำเนินการนี้ คุณสามารถตรวจสอบความคืบหน้าของงานจากการ์ด **การตรวจสอบ ➔ งาน** หากงานไม่เสร็จสมบูรณ์ ให้คลิกลิงก์งานเพื่อแสดงรายละเอียดเกี่ยวกับงาน (ดู การทำงานกับงาน ในเอกสารแบบออนไลน์ของ XClarity Administrator)

คุณยังสามารถลบข้อมูล FQDN ของเซิร์ฟเวอร์การจัดการและ DNS ออกจากเซิร์ฟเวอร์ที่มีการจัดการซึ่งมี IMM2, XCC และ XCC2 ได้ด้วยการคลิก **นำ FQDN / DNS ออกจาก BMC** คุณสามารถเลือกเก็บรายการ DNS ที่มีอยู่อื่นๆ ไว้, ลบรายการ DNS ทั้งหมด หรือลบเฉพาะรายการที่ตรงกับข้อมูลเซิร์ฟเวอร์การจัดการ

ขั้นตอนที่ 6. คลิก **ย้อนกลับ**

ขั้นตอนที่ 7. คลิก **ทดสอบการเชื่อมต่อ** เพื่อตรวจสอบการตั้งค่าเครือข่าย

การกำหนดค่าวันที่และเวลา

แม้ว่าคุณจะสามารถตั้งค่าวันที่และเวลาสำหรับ Lenovo XClarity Administrator ด้วยตนเองได้ แต่วิธีที่ดีกว่าคือการตั้งค่าเซิร์ฟเวอร์ Network Time Protocol (NTP) ที่สามารถใช้เพื่อซิงโครไนซ์การลงเวลาระหว่าง XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการทั้งหมด

ก่อนจะเริ่มต้น

คุณต้องใช้เซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย (NTP) อย่างน้อยหนึ่งเครื่อง (สูงสุดสี่) ในการซิงโครไนซ์ประทับเวลาสำหรับเหตุการณ์ทั้งหมดที่ได้รับจากอุปกรณ์ที่มีการจัดการกับ XClarity Administrator

เคล็ดลับ: เซิร์ฟเวอร์ NTP ต้องสามารถเข้าถึงผ่านเครือข่ายการจัดการ (ตามปกติจะเป็นอินเทอร์เฟซ Eth0) ลองพิจารณาการตั้งค่าเซิร์ฟเวอร์ NTP บนโฮสต์ที่ XClarity Administrator กำลังทำงาน

หากคุณเปลี่ยนเวลาในเซิร์ฟเวอร์ NTP อาจใช้เวลาสักครู่กว่าที่ XClarity Administrator จะซิงโครไนซ์กับเวลาใหม่

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

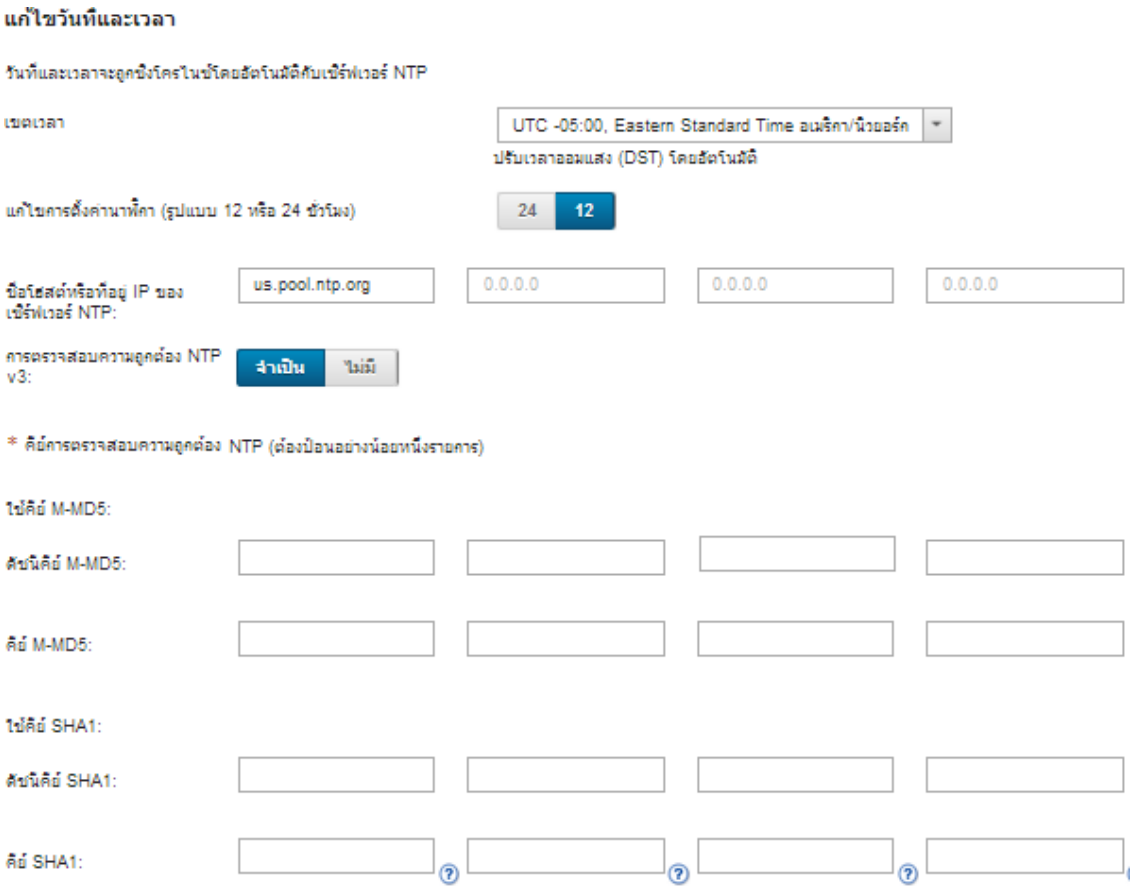
- สำหรับ ESXi ให้ทำตามคำแนะนำใน เว็บเพจ VMware – การปิดใช้งานการซิงโครไนซ์เวลา

- สำหรับ Hyper-V จาก Hyper-V Manager ให้คลิกขวาเครื่องเสมือน XClarity Administrator แล้วคลิก **Settings** ในกล่องโต้ตอบ ให้คลิก **Management** > **Integration Services** ในแถบการนำทาง แล้วล้าง **Time synchronization**.

ขั้นตอน

ในการตั้งค่าเซิร์ฟเวอร์ NTP สำหรับ XClarity Administrator ให้ดำเนินการขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. จากหน้าการตั้งค่าเริ่มต้น คลิก **กำหนดลักษณะวันที่และเวลา** หน้า แก้ไขวันที่และเวลา จะแสดงขึ้น



ขั้นตอนที่ 2. กรอกข้อมูลในกล่องโต้ตอบวันที่และเวลา

1. เลือกโซนเวลาที่โฮสต์สำหรับ XClarity Administrator อยู่

   หากโซนเวลาที่เลือกเป็นไปตามเวลาออมแสง (DST) เวลาจะถูกปรับสำหรับ DST โดยอัตโนมัติ
2. เลือกใช้นาฬิกาแบบ 12 ชั่วโมงหรือ 24 ชั่วโมง
3. ระบุชื่อโฮสต์หรือที่อยู่ IP ของเซิร์ฟเวอร์ NTP แต่ละเครื่องภายในเครือข่ายของคุณ คุณสามารถกำหนดเซิร์ฟเวอร์ NTP สูงสุดสี่เครื่อง
4. เลือก**จำเป็น** เพื่อเปิดใช้งานการตรวจสอบความถูกต้อง NTP v3 หรือเลือก**ไม่มี** เพื่อใช้การตรวจสอบความถูกต้อง NTP v1 ระหว่าง XClarity Administrator และเซิร์ฟเวอร์ NTP ในเครือข่ายของคุณ

คุณสามารถใช้การตรวจสอบความถูกต้อง v3 หาก CMM ของ Flex System ที่ได้รับการจัดการและตัวควบคุมการจัดการแผงวงจรมีเฟิร์มแวร์ที่ต้องการการตรวจสอบความถูกต้อง v3 และหากต้องการการตรวจสอบความถูกต้อง NTP v3 ระหว่าง XClarity Administrator และเซิร์ฟเวอร์ NTP อย่างน้อยหนึ่งเครื่องในเครือข่ายของคุณ

5. หากคุณเปิดใช้งานการตรวจสอบความถูกต้อง NTP v3 แล้ว ให้ตั้งค่าคีย์การตรวจสอบความถูกต้องและดัชนีสำหรับเซิร์ฟเวอร์ NTP ที่ใช้ได้แต่ละเครื่อง คุณสามารถระบุคีย์ M-MD5, คีย์ SHA1 หรือทั้งคู่ได้ หากมีการระบุทั้งคีย์ M-MD5 หรือ SHA1 XClarity Administrator จะส่งคีย์ M-MD5 หรือ SHA1 ให้กับ CMM ของ Flex System ที่ได้รับการจัดการและตัวควบคุมการจัดการที่รองรับ คีย์ดังกล่าว XClarity Administrator ใช้คีย์ดังกล่าวเพื่อตรวจสอบความถูกต้องของเซิร์ฟเวอร์ NTP

   - สำหรับคีย์ M-MD5 ให้ระบุสตริง ASCII ที่ประกอบด้วยเฉพาะตัวอักษรตัวพิมพ์ใหญ่และตัวพิมพ์เล็ก (a-z, A-Z) ตัวเลข (0–9) และอักขระพิเศษต่อไปนี้ @#
   - สำหรับคีย์ SHA1 ให้ระบุสตริง ASCII ที่เป็นอักขระ 40 ตัว ที่มีเฉพาะ 0–9 และ a-f เท่านั้น
   - ดัชนีคีย์และคีย์ตรวจสอบความถูกต้องที่ระบุต้องตรงกับค่า ID และรหัสผ่านของคีย์ที่ตั้งไว้บนเซิร์ฟเวอร์ NTP ตัวอย่างเช่น หากดัชนีคีย์ของคีย์ SHA1 ที่ป้อนในเซิร์ฟเวอร์ NTP คือ 5 แล้วดัชนีคีย์ที่ระบุของคีย์ SHA1 ของ XClarity Administrator ก็จะเป็น 5 ด้วย สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่า ID และรหัสผ่านของคีย์ โปรดดูเอกสารสำหรับเซิร์ฟเวอร์ NTP ของคุณ
   - คุณต้องระบุคีย์สำหรับเซิร์ฟเวอร์ NTP แต่ละเครื่องที่ใช้การตรวจสอบความถูกต้อง v3 แม้ว่าเซิร์ฟเวอร์ NTP อย่างน้อยสองเครื่องใช้คีย์เดียวกัน
   - หากคุณเปิดใช้งานการตรวจสอบความถูกต้อง v3 แต่ไม่ได้กำหนดคีย์การตรวจสอบความถูกต้อง และดัชนีสำหรับเซิร์ฟเวอร์ NTP จะมีการใช้การตรวจสอบความถูกต้อง v1 ตามค่าเริ่มต้น
   - หากคุณระบุเซิร์ฟเวอร์ NTP หลายเครื่อง เซิร์ฟเวอร์ NTP จะต้องเป็นการตรวจสอบความถูกต้อง v3 ทั้งหมดหรือการตรวจสอบความถูกต้อง v1 ทั้งหมดอย่างใดอย่างหนึ่ง ไม่รองรับการใช้เซิร์ฟเวอร์ NTP การตรวจสอบความถูกต้อง v3 หรือการตรวจสอบความถูกต้อง v1 ผสมรวมกัน
   - หากคุณระบุเซิร์ฟเวอร์ NTP หลายเครื่องที่มีการตรวจสอบความถูกต้อง v3 ตัวดัชนีคีย์ต้องไม่เหมือนกันหากคีย์ทั้งหลายไม่เหมือนกัน ตัวอย่างเช่น เซิร์ฟเวอร์ NTP 1 และ 2 ไม่สามารถมีดัชนีคีย์ SHA1 เท่ากับ 1 หากมีคีย์ SHA1 แตกต่างกันในเซิร์ฟเวอร์ NTP 1 และ 2 คุณต้องกำหนดค่าเซิร์ฟเวอร์ NTP เครื่องใดเครื่องหนึ่งให้ยอมรับคีย์ที่มีดัชนีคีย์ที่แตกต่างจากเซิร์ฟเวอร์ NTP อื่นๆ มิเช่นนั้น จะมีการกำหนดค่าดัชนีคีย์ตัวเดียวกันให้กับคีย์ที่ถูกกำหนดครั้งสุดท้ายที่เชื่อมโยงกับดัชนีคีย์กับเซิร์ฟเวอร์ NTP ทั้งหมด

ขั้นตอนที่ 3. คลิก **บันทึก**

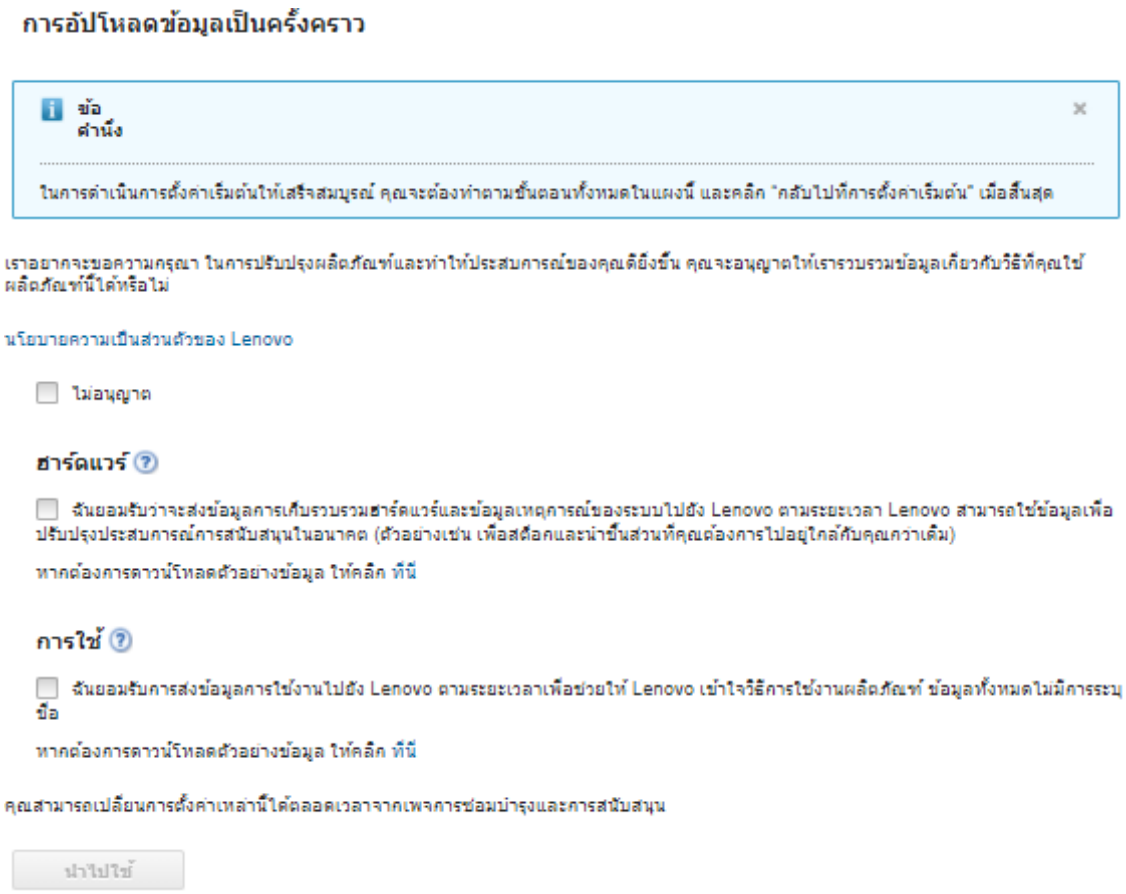
การกำหนดค่าบริการและการสนับสนุน

คุณสามารถกำหนดค่าบริการและการตั้งค่าการสนับสนุน รวมถึง ข้อมูลการใช้งาน, บริการสนับสนุนของ Lenovo (การเรียกเลขหมายโทรศัพท์บ้าน), การอำนวยการอัปโหลด Lenovo และการรับประกันผลิตภัณฑ์

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อกำหนดค่าการรักษาความปลอดภัย

ขั้นตอนที่ 1. จากหน้าการตั้งค่าเริ่มต้น คลิก **กำหนดค่าบริการและการตั้งค่าการสนับสนุน** หน้า บริการและการสนับสนุน จะแสดงขึ้น



ขั้นตอนที่ 2. อ่านและยอมรับ คำชี้แจงสิทธิ์ส่วนบุคคลของ Lenovo

หมายเหตุ: คุณไม่สามารถรวบรวมและส่งข้อมูลไปยัง Lenovo โดยไม่ยอมรับ คำชี้แจงสิทธิ์ส่วนบุคคลของ Lenovo ก่อน หากคุณเลือกที่จะปฏิเสธคำชี้แจงสิทธิ์ส่วนบุคคล คุณสามารถตรวจสอบและยอมรับคำชี้แจงสิทธิ์ส่วนบุคคลได้ภายหลังจากหน้า **การบริการและการสนับสนุน** ➔ **การกำหนดค่า** Call Home

ขั้นตอนที่ 3. หรือสามารถเลือกเพื่ออนุญาตให้ Lenovo XClarity Administrator รวบรวมข้อมูลการใช้งานและฮาร์ดแวร์และคลิก **นำไปใช้**

คุณสามารถรวบรวมและส่งข้อมูลประเภทต่อไปนี้ไปให้ Lenovo ได้

- **ข้อมูลการใช้งาน**

  เมื่อคุณตกลงที่จะส่งข้อมูลการใช้งานให้กับ Lenovo ข้อมูลต่อไปนี้จะถูกรวบรวมและส่งเป็นรายสัปดาห์ ข้อมูลนี้*ไม่มีการระบุชื่อ* ไม่มีการรวบรวมข้อมูลส่วนตัว (รวมถึงหมายเลขประจำเครื่อง, UUID, ชื่อโฮสต์, ที่อยู่ IP และชื่อผู้ใช้) หรือส่งไปยัง Lenovo
  - บันทึกการดำเนินการที่ดำเนินการ
  - รายการเหตุการณ์ที่ถูกยกระดับ และประทับเวลาเมื่อยกระดับ
  - รายการเหตุการณ์การตรวจสอบที่ยกระดับ และประทับเวลาเมื่อยกระดับ
  - รายการงานที่ดำเนินการไปแล้ว และข้อมูลความสำเร็จหรือความล้มเหลวของแต่ละงาน
  - เมตริกของ XClarity Administrator รวมถึงการใช้งานหน่วยความจำ การใช้งานโปรเซสเซอร์ และเนื้อที่ดิสก์
  - ข้อมูลรายการอุปกรณ์จำกัดเกี่ยวกับอุปกรณ์ที่มีการจัดการทั้งหมด
- **ข้อมูลฮาร์ดแวร์**

  เมื่อคุณตกลงที่จะส่งข้อมูลฮาร์ดแวร์ไปให้ Lenovo ข้อมูลต่อไปนี้จะถูกรวบรวมและส่งเป็นระยะ ข้อมูลนี้*มีการระบุชื่อ* ข้อมูลฮาร์ดแวร์ประกอบด้วยแอตทริบิวต์ เช่น UUID และหมายเลขประจำเครื่อง ไม่รวมที่อยู่ IP หรือชื่อโฮสต์

  - **ข้อมูลฮาร์ดแวร์รายวัน** ข้อมูลต่อไปนี้มีไว้สำหรับการเปลี่ยนแปลงในรายการอุปกรณ์แต่ละรายการ
    - เหตุการณ์การเปลี่ยนแปลงรายการอุปกรณ์ (FQXHMDM0001I)
    - การเปลี่ยนแปลงที่เกิดขึ้นกับข้อมูลรายการอุปกรณ์สำหรับอุปกรณ์ที่เกี่ยวข้องกับเหตุการณ์นั้น
  - **ข้อมูลฮาร์ดแวร์รายสัปดาห์** ข้อมูลรายการอุปกรณ์มีไว้สำหรับอุปกรณ์ที่มีการจัดการทั้งหมด

เมื่อมีการส่งข้อมูลการใช้งานและฮาร์ดแวร์ไปยัง Lenovo ระบบจะบันทึกเหตุการณ์ในบันทึกการตรวจสอบ

คุณสามารถเปลี่ยนการตั้งค่านี้เมื่อใดก็ได้ และดาวน์โหลดไฟล์เก็บถาวรล่าสุดที่ถูกรวบรวมและส่งไปให้ Lenovo โดยใช้ลิงก์จากการคลิกแท็บ **การดูแลระบบ ➔ การบริการและการสนับสนุน** แล้วคลิก **การอัปโหลดข้อมูลเป็นครั้งคราว**

ขั้นตอนที่ 4. หรือคลิก **การกำหนดค่าการเรียกเลขหมายโทรศัพท์บ้าน** เพื่อตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติเป็นบริการสนับสนุนของ Lenovo (การเรียกเลขหมายโทรศัพท์บ้าน) แล้วคลิก **นำไปใช้และเปิดใช้งาน** เพื่อ

สร้างระบบส่งต่อบริการการเรียกเลขหมายโทรศัพท์บ้านเริ่มต้น หรือคลิก **นำไปใช้เท่านั้น** เพื่อบันทึกข้อมูลติดต่อ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติเป็นบริการสนับสนุนของ Lenovo โปรดดู การตั้งค่าการเรียกเลขหมายโทรศัพท์บ้าน ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 5. หรือคลิก **การอำนวยการอัปโหลด Lenovo** เพื่อตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติเป็น การอำนวยการอัปโหลด Lenovo แล้วคลิก **นำไปใช้และเปิดใช้งาน** เพื่อสร้างระบบส่งต่อบริการการอำนวยการอัปโหลด Lenovo เริ่มต้น หรือคลิก **นำไปใช้เท่านั้น** เพื่อบันทึกข้อมูลการตั้งค่า

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติเป็นการอำนวยการอัปโหลด Lenovo โปรดดู การตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติให้แก่ การอำนวยการอัปโหลด Lenovo ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 6. หรือคลิก **การรับประกัน** เพื่อเปิดใช้งานการเชื่อมต่อภายนอกที่จำเป็นในการรวบรวมข้อมูลการรับประกันของอุปกรณ์ได้รับการจัดการของคุณ

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการดูสถานะการรับประกัน (รวมถึงการรับประกันเพิ่มเติม) ของอุปกรณ์ได้รับการจัดการ โปรดดู การดูข้อมูลการรับประกัน ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 7. เลือกที่จะคลิก **ข่าวสารด้านบริการของ Lenovo** เพื่ออนุญาตให้ Lenovo ส่งข่าวสารด้านบริการไปที่ XClarity Administrator แล้วคลิก **ใช้**

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับประเภทข่าวสารด้านบริการที่ Lenovo ส่ง โปรดดู การรับข่าวสารจาก Lenovo ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 8. ระบุรหัสผ่านการกู้คืนบริการที่คุณใช้เพื่อรวบรวมและดาวน์โหลดข้อมูลและบันทึกบริการ หาก XClarity Administrator ไม่ตอบสนองและไม่สามารถกู้คืนได้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับรหัสผ่านการกู้คืนบริการ โปรดดู การเปลี่ยนรหัสผ่านการกู้คืนบริการ ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 9. คลิก **กลับไปที่การตั้งค่าเริ่มต้น**

การกำหนดค่าการรักษาความปลอดภัย

คุณสามารถกำหนดค่าการรักษาความปลอดภัย รวมถึง กลุ่มบทบาท, เซิร์ฟเวอร์ตรวจสอบความถูกต้อง, การตั้งค่าการรักษาความปลอดภัยของบัญชีผู้ใช้ และใบรับรอง

ขั้นตอน

ดำเนินการขั้นตอนต่อไปนี้เพื่อกำหนดค่าการรักษาความปลอดภัย

ขั้นตอนที่ 1. จากหน้าการตั้งค่าเริ่มต้น คลิก **กำหนดการตั้งค่าการรักษาความปลอดภัยเพิ่มเติม** หน้า การรักษาความปลอดภัย จะแสดงขึ้น

ขั้นตอนที่ 2. สร้างกลุ่มบทบาทที่กำหนดเองเพื่อจัดการการตรวจสอบความถูกต้อง และการเข้าถึงทรัพยากร (โปรดดู การสร้างกลุ่มบทบาท ในเอกสารแบบออนไลน์ของ XClarity Administrator)

กลุ่มบทบาท คือชุดรวมหนึ่งหรือหลายบทบาท และใช้ในการกำหนดบทบาทเหล่านั้นให้กับผู้ใช้หลายราย บทบาทที่คุณกำหนดค่าสำหรับกลุ่มบทบาทจะกำหนดระดับสิทธิ์เข้าถึงที่มอบให้กับผู้ใช้แต่ละรายที่เป็นสมาชิกของกลุ่มบทบาทนั้น ผู้ใช้ XClarity Administrator แต่ละรายจะต้องเป็นสมาชิกของอย่างน้อยหนึ่งกลุ่มบทบาท

ขั้นตอนที่ 3. กำหนดค่าเซิร์ฟเวอร์ตรวจสอบความถูกต้อง (โปรดดู การจัดการเซิร์ฟเวอร์การตรวจสอบความถูกต้อง ในเอกสารแบบออนไลน์ของ XClarity Administrator)

เซิร์ฟเวอร์ตรวจสอบความถูกต้อง คือเซิร์ฟเวอร์ Microsoft Active Directory (LDAP) ที่ใช้เพื่อตรวจสอบความถูกต้องของข้อมูลประจำตัวของผู้ใช้ XClarity Administrator จะใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องเดียวสำหรับการจัดการผู้ใช้ส่วนกลางของอุปกรณ์ที่ได้รับการจัดการทั้งหมด (ยกเว้นสวิตช์ Flex) เมื่ออุปกรณ์ได้รับการจัดการโดย XClarity Administrator อุปกรณ์ที่ได้รับการจัดการและส่วนประกอบที่ติดตั้ง (ยกเว้นสวิตช์ Flex) จะได้รับการกำหนดค่าให้ใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator บัญชีผู้ใช้ที่กำหนดไว้ในเซิร์ฟเวอร์ตรวจสอบความถูกต้องจะถูกใช้เพื่อเข้าสู่ระบบ XClarity Administrator, CMM และตัวควบคุมการจัดการแผงวงจร

คุณสามารถเลือกให้ใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องภายนอกแทนเซิร์ฟเวอร์ตรวจสอบความถูกต้องภายในในโหมดการจัดการ

ขั้นตอนที่ 4. กำหนดค่าการตั้งค่าการรักษาความปลอดภัยบัญชีผู้ใช้ ซึ่งจะควบคุมความซับซ้อนของรหัสผ่าน การล็อคบัญชี และการหมดเวลาของเว็บเซสชันที่ไม่ใช้งาน (โปรดดู การเปลี่ยนการตั้งค่าการรักษาความปลอดภัยของบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

ขั้นตอนที่ 5. กำหนดค่าการตั้งค่าการเข้ารหัสที่จะกำหนดโหมดการสื่อสารและโปรโตคอลที่ควบคุมวิธีจัดการการสื่อสารที่ปลอดภัยระหว่าง XClarity Administrator และอุปกรณ์ที่ได้รับการจัดการ (โปรดดู การตั้งค่าโหมดการเข้ารหัสและโปรโตคอล การสื่อสาร ในเอกสารแบบออนไลน์ของ XClarity Administrator)

ขั้นตอนที่ 6. หากคุณวางแผนที่จะจัดการเซิร์ฟเวอร์ในแร็คโดยใช้การตรวจสอบความถูกต้องภายในแทนที่จะใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการของ XClarity Administrator ให้สร้างข้อมูลประจำตัวที่จัดเก็บไว้อย่างน้อยหนึ่งรายการที่สอดคล้องกับบัญชีผู้ใช้ที่ใช้งานบนอุปกรณ์หรือใน Active Directory ที่สามารถใช้ในการเข้าสู่ระบบอุปกรณ์ในระหว่างกระบวนการจัดการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับข้อมูลประจำตัวที่จัดเก็บไว้ โปรดดู การจัดการข้อมูลประจำตัวที่จัดเก็บไว้ ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 7. หากคุณวางแผนที่จะใช้ใบรับรองเซิร์ฟเวอร์ที่กำหนดเองที่ประกอบด้วยข้อมูลของคุณเอง หรือใช้ใบรับรองที่ลงนามภายนอก ให้สร้างและปรับใช้ใบรับรองใหม่ก่อนที่คุณเริ่มต้นการจัดการระบบ สำหรับข้อมูลเกี่ยวกับการสร้างใบรับรองด้านความปลอดภัยของคุณเอง โปรดดู การทำงานกับใบรับรองด้านความปลอดภัย ในเอกสารแบบออนไลน์ของ XClarity Administrator

ขั้นตอนที่ 8. จากเมนูแนวตั้งในหน้าการรักษาความปลอดภัย ให้คลิก **กลับไปที่การตั้งค่าเริ่มต้น**

การจัดการอุปกรณ์

Lenovo XClarity Administratorสามารถจัดการระบบได้หลายประเภท รวมถึงตัวเครื่อง Flex System เซิร์ฟเวอร์ในแร็คและเซิร์ฟเวอร์แบบทาวเวอร์ สวิตช์ของ RackSwitch และอุปกรณ์การจัดเก็บข้อมูล คุณสามารถค้นหาและจัดการอุปกรณ์จำนวนมากที่อยู่ในสภาพแวดล้อมของคุณได้อย่างง่ายดาย โดยนำเข้าข้อมูลเกี่ยวกับอุปกรณ์ของคุณโดยใช้ไฟล์การนำเข้าเป็นกลุ่ม

ก่อนจะเริ่มต้น

ข้อสำคัญ:

- คุณสามารถจัดการอุปกรณ์ได้สูงสุด 300 อุปกรณ์ในครั้งเดียว ห้ามรวมอุปกรณ์ในไฟล์การนำเข้าเป็นกลุ่มเกิน 300 รายการ
- หลังจากที่คุณเริ่มดำเนินการจัดการอุปกรณ์ รอให้งานการจัดการทั้งหมดเสร็จสมบูรณ์ก่อนที่จะเริ่มดำเนินการจัดการอุปกรณ์อื่น

ระบบจะมองเห็นและจัดการส่วนประกอบตัวเครื่อง (เช่น CMM, โหนดคอมพิวท์, สวิตช์ และอุปกรณ์การจัดเก็บข้อมูล) โดยอัตโนมัติเมื่อคุณจัดการตัวเครื่องมีส่วนประกอบเหล่านี้ คุณไม่สามารถสำรวจและจัดการส่วนประกอบตัวเครื่องแยกจากตัวเครื่อง

ต้องมีพอร์ตบางตัวเพื่อสื่อสารกับ CMM ในตัวเครื่องและตัวควบคุมการจัดการแผงวงจรในเซิร์ฟเวอร์ ตรวจสอบให้แน่ใจว่าพอร์ตเหล่านี้สามารถใช้งานได้ก่อนที่จะพยายามจัดการระบบ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับพอร์ต โปรดดู ความพร้อมใช้งานของพอร์ต

โปรดตรวจสอบว่ามีเฟิร์มแวร์ขั้นต่ำที่จำเป็นติดตั้งอยู่บนแต่ละระบบที่คุณต้องการจัดการโดยใช้ XClarity Administrator คุณสามารถดูระดับเฟิร์มแวร์ที่จำเป็นขั้นต่ำได้จาก เว็บเพจฝ่ายสนับสนุนของ XClarity Administrator – ความเข้ากันได้ โดยคลิกแท็บ **ความเข้ากันได้** แล้วคลิกที่ลิงก์สำหรับประเภทอุปกรณ์ที่เหมาะสม

ตรวจสอบว่ามีการตั้งค่าเซสชันโหมดคำสั่ง TCP อย่างน้อย 3 เซสชันสำหรับการสื่อสารภายนอกกับ CMM สำหรับข้อมูลเกี่ยวกับการตั้งค่าจำนวนเซสชัน โปรดดู คำสั่ง tcpcmdmode ในเอกสารแบบออนไลน์ของ CMM

พิจารณาปรับใช้ที่อยู่ IPv4 *หรือ* IPv6 สำหรับ CMM และสวิตช์ Flex ทั้งหมดที่ได้รับการจัดการโดย XClarity Administrator หากคุณปรับใช้ IPv4 สำหรับ CMM และสวิตช์ Flex บางรายการ และ IPv6 สำหรับรายการอื่นๆ ระบบอาจไม่ได้รับเหตุการณ์บางอย่างในบันทึกการตรวจสอบ (หรือเป็น trap การตรวจสอบ)

ตรวจสอบว่าคุณเปิดใช้งานการส่งต่อ SLP แบบ Multicast บนสวิตช์บนสุดของแร็ค และเราเตอร์ในสภาพแวดล้อมของคุณ ดูเอกสารที่มาพร้อมกับสวิตช์หรือเราเตอร์เฉพาะของคุณเพื่อระบุว่ามีการเปิดใช้งานการส่งต่อ SLP แบบ Multicast หรือไม่ และเพื่อค้นหาวิธีการเปิดใช้งาน หากปิดใช้งานไว้

ข้อสำคัญ:

- คุณอาจต้องเปิดใช้งานการส่งต่อ SLP มัลติแคสต์และ SSH บนสวิตช์ RackSwitch แต่ละตัวด้วยตัวเองโดยใช้คำสั่งต่อไปนี้ก่อน XClarity Administrator จึงจะมองเห็นและจัดการสวิตช์ดังกล่าวได้ ทั้งนี้ขึ้นอยู่กับเวอร์ชันเฟิร์มแวร์สำหรับสวิตช์ของ RackSwitch สำหรับข้อมูลเพิ่มเติม โปรดดู สวิตช์แร็คในเอกสารแบบออนไลน์ของ System x
- ต้องเปิดใช้งานการส่งต่อ SLP แบบ Multicast ในแต่ละอุปกรณ์การจัดเก็บข้อมูลแต่ละเครื่องก่อนที่จะสามารถตรวจพบโดย XClarity Administrator
- หากคุณวางแผนที่จะใช้ใบรับรองเซิร์ฟเวอร์ที่กำหนดเองที่ประกอบด้วยข้อมูลของคุณเอง หรือใช้ใบรับรองที่ลงนามภายนอก ให้สร้างและปรับใช้ใบรับรองใหม่ก่อนที่คุณเริ่มต้นการจัดการระบบ สำหรับข้อมูลเกี่ยวกับการสร้างใบรับรองด้านความปลอดภัยของคุณเอง โปรดดู การทำงานกับใบรับรองด้านความปลอดภัย ในเอกสารแบบออนไลน์ของ XClarity Administrator
- หากคุณต้องการใช้งานซอฟต์แวร์การจัดการอื่นๆ นอกเหนือจาก Lenovo XClarity Administrator ในการตรวจสอบตัวเครื่อง และหากซอฟต์แวร์การจัดการนั้นใช้การสื่อสาร SNMPv3 ก่อนอื่นคุณต้องสร้าง ID ผู้ใช้ CMM ภายในที่กำหนดค่าด้วยข้อมูล SNMPv3 ที่เหมาะสม แล้วจึงเข้าสู่ระบบ CMM โดยใช้ ID ผู้ใช้ดังกล่าวและเปลี่ยนรหัสผ่าน สำหรับข้อมูลเพิ่มเติม โปรดดู ข้อควรพิจารณาด้านการจัดการ ในเอกสารแบบออนไลน์ของ XClarity Administrator
- โปรโตคอลการค้นพบบริการ เช่น SLP และ SSDP เปิดใช้งาน XClarity Administrator เพื่อค้นหาประเภทของอุปกรณ์ที่กำลังจะจัดการโดยอัตโนมัติ จากนั้นจะใช้วิธีที่เหมาะสมในการจัดการอุปกรณ์ อุปกรณ์บางประเภทไม่รองรับโปรโตคอลการค้นหาบริการ และโปรโตคอลการค้นหาบริการจะถูกปิดโดยเจตนาในบางสภาพแวดล้อม ไม่ว่าในกรณีใด คุณต้องเลือกประเภทอุปกรณ์ที่เหมาะสมเพื่อเสร็จสิ้นกระบวนการจัดการ ประเภทอุปกรณ์ต่อไปนี้ต้องได้รับการระบุอย่างชัดเจน
  - สวิตช์ Lenovo ThinkSystem DB ซีรีส์
  - สวิตช์ NVIDIA Mellanox

เกี่ยวกับงานนี้

XClarity Administrator สามารถค้นหาระบบในสภาพแวดล้อมของคุณ โดยการตรวจหาอุปกรณ์ที่สามารถจัดการได้ที่อยู่บนซับเน็ต IP เดียวกันกับ XClarity Administrator โดยใช้ที่อยู่ IP ที่ระบุ หรือช่วงของที่อยู่ IP หรือด้วยการนำเข้าข้อมูลจากสเปรดชีต

ตามค่าเริ่มต้น อุปกรณ์ได้รับการจัดการโดยใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการ XClarity Administrator ในการเข้าสู่ระบบอุปกรณ์ เมื่อจัดการเซิร์ฟเวอร์ในแร็คและตัวเครื่อง Lenovo คุณสามารถเลือกใช้การตรวจสอบความถูกต้องภายในเครื่องหรือการตรวจสอบความถูกต้องที่ได้รับการจัดการในการเข้าสู่ระบบอุปกรณ์

- เมื่อใช้*การตรวจสอบความถูกต้องภายในเครื่อง*สำหรับเซิร์ฟเวอร์ในแร็ค ตัวเครื่อง Lenovo และสวิตช์ในแร็คของ Lenovo XClarity Administrator จะใช้ข้อมูลประจำตัวที่จัดเก็บไว้เพื่อตรวจสอบความถูกต้องกับอุปกรณ์ *ข้อมูลประจำตัวที่จัดเก็บไว้*อาจเป็นบัญชีผู้ใช้ที่ใช้งานบนอุปกรณ์หรือบัญชีผู้ใช้ใน Active Directory

  คุณต้องสร้างข้อมูลประจำตัวที่จัดเก็บไว้ใน XClarity Administrator ที่ตรงกับบัญชีผู้ใช้ที่ใช้งานอยู่บนอุปกรณ์ หรือบัญชีผู้ใช้ในเซิร์ฟเวอร์ Active Directory ก่อนจัดการอุปกรณ์โดยใช้การตรวจสอบความถูกต้องภายในเครื่อง (โปรดดู การจัดการข้อมูลประจำตัวที่จัดเก็บไว้ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

  หมายเหตุ:

  – อุปกรณ์ RackSwitch รองรับเฉพาะข้อมูลประจำตัวที่จัดเก็บไว้สำหรับการตรวจสอบความถูกต้อง ทั้งนี้ ข้อมูลประจำตัวผู้ใช้ของ XClarity Administrator จะไม่ได้รับการสนับสนุน

- การใช้*การตรวจสอบความถูกต้องที่ได้รับการจัดการ* ช่วยให้คุณสามารถจัดการ และตรวจสอบอุปกรณ์หลายเครื่องได้โดยใช้ข้อมูลประจำตัวในเซิร์ฟเวอร์ตรวจสอบความถูกต้อง XClarity Administrator แทนข้อมูลประจำตัวภายในเครื่อง เมื่อมีการใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ (นอกเหนือจากเซิร์ฟเวอร์ ThinkServer, System x M4, และสวิตช์) XClarity Administrator จะกำหนดค่าอุปกรณ์และส่วนประกอบที่ติดตั้งเพื่อใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator สำหรับการจัดการส่วนกลาง

  – เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการ คุณจะสามารถจัดการอุปกรณ์โดยใช้ข้อมูลประจำตัวที่ป้อนเองหรือข้อมูลประจำตัวที่จัดเก็บไว้ก็ได้ (โปรดดู การจัดการบัญชีผู้ใช้ และ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

    ข้อมูลประจำตัวที่จัดเก็บไว้จะถูกใช้จนกว่า XClarity Administrator จะกำหนดค่าการตั้งค่า LDAP บนอุปกรณ์ หลังจากนั้น การเปลี่ยนแปลงใดๆ กับข้อมูลประจำตัวที่จัดเก็บไว้จะไม่ส่งผลต่อการจัดการหรือการตรวจสอบของอุปกรณ์นั้น

    หมายเหตุ: เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ คุณจะไม่สามารถแก้ไขข้อมูลประจำตัวที่จัดเก็บไว้สำหรับอุปกรณ์นั้นโดยใช้ XClarity Administrator

  – หากมีการใช้เซิร์ฟเวอร์ LDAP ภายในหรือภายนอกเป็นเซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator จะใช้บัญชีผู้ใช้ที่กำหนดไว้ในเซิร์ฟเวอร์ตรวจสอบความถูกต้องในการเข้าสู่ระบบ XClarity Administrator, CMM และตัวควบคุมการจัดการแผงวงจรในโดเมน XClarity Administrator บัญชีผู้ใช้ CMM และตัวควบคุมการจัดการภายในจะถูกปิดใช้งาน

  – หากมีการใช้ผู้ให้บริการข้อมูลประจำตัว SAML 2.0 เป็นเซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator บัญชี SAML จะไม่สามารถเข้าถึงอุปกรณ์ที่ได้รับการจัดการ อย่างไรก็ตาม เมื่อใช้ทั้งผู้ให้บริการข้อมูลประจำตัว SAML และเซิร์ฟเวอร์ LDAP ร่วมกัน หากผู้ให้บริการข้อมูลประจำตัวใช้บัญชีที่มีอยู่ในเซิร์ฟเวอร์ LDAP บัญชีผู้ใช้ LDAP สามารถใช้ในการเข้าสู่ระบบอุปกรณ์ที่ได้รับการจัดการ ขณะที่วิธีการตรวจ

สอบความถูกต้องขั้นสูงเพิ่มเติมที่มีให้โดย SAML 2.0 (เช่น การตรวจสอบความถูกต้องแบบหลายปัจจัยและการลงชื่อเข้าใช้ครั้งเดียว) สามารถใช้ในการเข้าสู่ระบบ XClarity Administrator

- การเข้าสู่ระบบแบบครั้งเดียวอนุญาตให้ผู้ใช้ที่เข้าสู่ระบบ XClarity Administrator อยู่แล้ว เข้าสู่ระบบตัวควบคุมการจัดการแผงวงจรโดยอัตโนมัติ การเข้าสู่ระบบแบบครั้งเดียวจะเปิดใช้งานตามค่าเริ่มต้นเมื่อเซิร์ฟเวอร์ ThinkSystem หรือ ThinkAgile ถูกนำเข้าสู่การจัดการโดย XClarity Administrator (เว้นแต่เซิร์ฟเวอร์จะจัดการด้วยรหัสผ่าน CyberArk) คุณสามารถกำหนดค่าการตั้งค่าส่วนกลางเพื่อเปิดใช้งานหรือปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวกับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ที่มีการจัดการทั้งหมดได้ การเปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวสำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile บางเครื่องจะแทนที่การตั้งค่าส่วนกลางของเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ทั้งหมด (ดู การจัดการเซิร์ฟเวอร์ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

  หมายเหตุ: การเข้าสู่ระบบแบบครั้งเดียวจะถูกปิดใช้งานโดยอัตโนมัติเมื่อใช้ระบบการจัดการข้อมูลประจำตัวของ CyberArk สำหรับการตรวจสอบความถูกต้อง

- เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับเซิร์ฟเวอร์ ThinkSystem SR635 และ SR655:

  - เฟิร์มแวร์ของตัวควบคุมการจัดการแผงวงจรรองรับบทบาทผู้ใช้ LDAP สูงสุดห้าบทบาท XClarity Administrator เพิ่มบทบาทผู้ใช้ LDAP เหล่านี้ไปยังเซิร์ฟเวอร์ระหว่างการจัดการ: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** และ **lxc-os-admin**

    ผู้ใช้ต้องได้รับการกำหนดบทบาทผู้ใช้ LDAP ที่ระบุอย่างน้อยหนึ่งบทบาทเพื่อสื่อสารกับเซิร์ฟเวอร์ ThinkSystem SR635 และ SR655

  - เฟิร์มแวร์ของตัวควบคุมการจัดการไม่รองรับผู้ใช้ LDAP ที่มีชื่อผู้ใช้เดียวกันกับผู้ใช้ภายในของเซิร์ฟเวอร์

- สำหรับเซิร์ฟเวอร์ ThinkServer และ System x M4 จะไม่ใช้เซิร์ฟเวอร์ตรวจสอบความถูกต้องของ XClarity Administrator แต่บัญชี IPMI จะถูกสร้างขึ้นบนอุปกรณ์ที่มีคำนำหน้า “LXCA_” ตามด้วยสตริงแบบสุ่ม (บัญชีผู้ใช้ IPMI ในระบบที่มีอยู่ไม่ถูกปิดใช้งาน) เมื่อคุณถอนการจัดการเซิร์ฟเวอร์ ThinkServer ระบบจะปิดการใช้งานบัญชีผู้ใช้ “LXCA_” และคำนำหน้า “LXCA_” จะถูกแทนที่ด้วย “DISABLED_” ในการระบุว่าเซิร์ฟเวอร์ ThinkServer ได้รับการจัดการโดยอินสแตนซ์อื่นหรือไม่ XClarity Administrator จะตรวจหาบัญชี IPMI ที่มีคำนำหน้า “LXCA_” หากคุณเลือกบังคับการจัดการของเซิร์ฟเวอร์ ThinkServer ที่ได้รับการจัดการ ระบบจะปิดการใช้งานและเปลี่ยนชื่อบัญชี IPMI ทั้งหมดบนอุปกรณ์ที่มีคำนำหน้า “LXCA_” พิจารณาล้างข้อมูลบัญชี IPMI ที่ไม่ได้ใช้งานอีกต่อไปด้วยตนเอง

  หากคุณใช้ข้อมูลประจำตัวที่ป้อนเอง XClarity Administrator จะสร้างข้อมูลประจำตัวสำหรับที่จัดเก็บไว้โดยอัตโนมัติ และใช้ข้อมูลประจำตัวที่จัดเก็บไว้นั้นเพื่อจัดการอุปกรณ์

  หมายเหตุ: เมื่อเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับอุปกรณ์ คุณจะไม่สามารถแก้ไขข้อมูลประจำตัวที่จัดเก็บไว้สำหรับอุปกรณ์นั้นโดยใช้ XClarity Administrator

- ทุกครั้งที่คุณจัดการอุปกรณ์โดยใช้ข้อมูลประจำตัวที่ป้อนด้วยตนเอง ข้อมูลประจำตัวสำหรับจัดเก็บใหม่จะถูกสร้างขึ้นสำหรับอุปกรณ์นั้น แม้ว่าได้สร้างข้อมูลประจำตัวสำหรับจัดเก็บสำหรับอุปกรณ์นั้นแล้วระหว่างกระบวนการจัดการก่อนหน้า
- เมื่อคุณถอนการจัดการอุปกรณ์ XClarity Administrator จะไม่ลบข้อมูลประจำตัวที่จัดเก็บไว้ซึ่งถูกสร้างขึ้นโดยอัตโนมัติสำหรับอุปกรณ์นั้นในระหว่างกระบวนการจัดการ

หลังจากที่ระบบได้รับการจัดการโดย XClarity Administrator XClarity Administrator จะสำรวจระบบที่ได้รับการจัดการแต่ละระบบเป็นระยะเพื่อรวบรวมข้อมูล เช่น รายการอุปกรณ์ ข้อมูลผลิตภัณฑ์ที่สำคัญ (VPD) และสถานะ คุณสามารถดูและตรวจสอบแต่ละระบบที่ได้รับการจัดการ และดำเนินการจัดการ (เช่น การกำหนดค่าการตั้งค่าระบบ การปรับใช้อิมเมจระบบปฏิบัติการ และการเปิดและปิดเครื่อง)

สามารถจัดการระบบโดย XClarity Administrator ทีละรายการเท่านั้น ไม่รองรับการจัดการโดยตัวจัดการหลายรายการ หากระบบได้รับการจัดการโดย XClarity Administrator หนึ่งรายการ และคุณต้องการจัดการระบบกับ XClarity Administrator อื่น คุณต้องถอนการจัดการระบบใน XClarity Administrator ปัจจุบันก่อน จากนั้นคุณจะสามารถจัดการระบบกับ XClarity Administrator อื่นได้ สำหรับข้อมูลเกี่ยวกับการถอนการจัดการระบบ โปรดดู การถอนการจัดการตัวเครื่อง, การเลิกการจัดการเซิร์ฟเวอร์, การถอนการจัดการสวิตช์ของ RackSwitch และ การถอนการจัดการระบบที่จัดเก็บ Lenovo Storage ในเอกสารแบบออนไลน์ของ XClarity Administrator

หมายเหตุ: XClarity Administrator ไม่แก้ไขการตั้งค่าการรักษาความปลอดภัยหรือการตั้งค่าการเข้ารหัส (โหมดการเข้ารหัสและโหมดที่ใช้สำหรับการสื่อสารที่มีความปลอดภัย) ระหว่างกระบวนการจัดการ คุณสามารถแก้ไขการตั้งค่าการเข้ารหัสหลังจากระบบได้รับการจัดการ (โปรดดู การตั้งค่าโหมดการเข้ารหัสและโปรโตคอล การสื่อสาร ในเอกสารแบบออนไลน์ของ XClarity Administrator)

หมายเหตุ: สามารถติดตั้ง XClarity Administrator ล่วงหน้าด้วยรายการอุปกรณ์ฮาร์ดแวร์สำหรับตัวเครื่องสาธิต (รวมถึง CMM, โหนดคอมพิวท์ และสวิตช์) และเซิร์ฟเวอร์ในแร็คหรือเซิร์ฟเวอร์แบบทาวเวอร์สำหรับสาธิต อุปกรณ์สาธิตจะถูกสร้างขึ้นหน้าเว็บอินเทอร์เฟซ และสามารถใช้เพื่อสาธิตการดำเนินการด้านการจัดการ อย่างไรก็ตาม การดำเนินการด้านการจัดการดังกล่าวจะล้มเหลว ตัวอย่างเช่น คุณสามารถสร้างรูปแบบการกำหนดค่า และปรับใช้รูปแบบกับเซิร์ฟเวอร์สาธิต แต่การปรับใช้นั้นจะล้มเหลว คุณสามารถนำอุปกรณ์สาธิตออกด้วยการยกเลิกการจัดการกับอุปกรณ์ (โปรดดู การถอนการจัดการตัวเครื่อง และ การเลิกการจัดการเซิร์ฟเวอร์ ในเอกสารแบบออนไลน์ของ XClarity Administrator) หลังจากลบอุปกรณ์สาธิตแล้ว อุปกรณ์จะไม่สามารถได้รับการจัดการได้อีกครั้ง

ขั้นตอน

ในการค้นหาและจัดการระบบของคุณใน XClarity Administrator โดยใช้ไฟล์การนำเข้าเป็นกลุ่ม ให้ดำเนินการตามขั้นตอนต่อไปนี้

หมายเหตุ: เมื่อสวิตช์ที่จัดการใช้การนำเข้าเป็นกลุ่ม HTTPS จะได้รับการเปิดใช้งานบนสวิตช์ และไคลเอ็นต์ NTP บนสวิตช์จะได้รับการกำหนดค่าให้ใช้การตั้งค่า NTP จากเซิร์ฟเวอร์การจัดการ ในการเปลี่ยนการตั้งค่าเหล่านี้ คุณต้องจัดการสวิตช์ด้วยตนเอง

1. จากแถบเมนู XClarity Administrator ให้คลิก **ฮาร์ดแวร์ ➔ สำรวจและจัดการอุปกรณ์เครื่องใหม่** หน้าสำรวจและจัดการ จะปรากฏขึ้น
2. คลิกกล่องตัวเลือก **เปิดใช้งาน Encapsulation ในอุปกรณ์ที่ได้รับการจัดการในอนาคตทั้งหมด** เพื่อเปลี่ยนกฎไฟร์วอลล์บนอุปกรณ์ทั้งหมดระหว่างกระบวนการจัดการ เพื่อให้รับคำขอที่เข้ามาจาก XClarity Administrator เท่านั้น

   หมายเหตุ:

   - ไม่รองรับ Encapsulation บนสวิตช์ อุปกรณ์จัดเก็บข้อมูล และตัวเครื่องและเซิร์ฟเวอร์ที่ไม่ใช่ของ Lenovo
   - เมื่อมีการกำหนดค่าอินเทอร์เฟซเครือข่ายการจัดการเพื่อใช้ Dynamic Host Configuration Protocol (DHCP) และเมื่อ Encapsulation เปิดใช้งาน การจัดการเซิร์ฟเวอร์ในแร็คอาจใช้เวลานาน

   สามารถเปิดใช้งานหรือปิดใช้งาน Encapsulation บนอุปกรณ์เฉพาะหลังจากมีการจัดการอุปกรณ์

   ข้อควรพิจารณา: หากเปิดใช้งาน Encapsulation และ XClarity Administrator ไม่สามารถใช้งานได้ก่อนที่อุปกรณ์จะได้รับการถอนการจัดการ ต้องดำเนินการขั้นตอนที่จำเป็นในการปิดใช้งาน Encapsulation เพื่อสร้างการสื่อสารกับอุปกรณ์ สำหรับขั้นตอนการกู้คืน โปรดดู การกู้คืนการจัดการตัวเครื่องด้วย CMM ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว และ การกู้คืนการจัดการแร็คเซิร์ฟเวอร์หรือเซิร์ฟเวอร์แบบทาวเวอร์ภายหลัง เซิร์ฟเวอร์การจัดการล้มเหลว ในเอกสารแบบออนไลน์ของ XClarity Administrator
3. คลิก **นำเข้าเป็นกลุ่ม** ตัวช่วยสร้างการนำเข้าเป็นกลุ่มจะปรากฏขึ้น

4. คลิกลิงก์ **ใน Excel** หรือ **ใน CSV** ในหน้า นำเข้าไฟล์ข้อมูล เพื่อดาวน์โหลดไฟล์นำเข้าเป็นกลุ่มแบบเทมเพลตในรูปแบบ Excel หรือ CSV

   ข้อสำคัญ: ไฟล์เทมเพลตอาจเปลี่ยนแปลงจากรุ่นหนึ่งไปยังอีกรุ่นหนึ่ง ตรวจสอบให้แน่ใจว่าคุณใช้เทมเพลตล่าสุดเสมอ
5. กรอกข้อมูลในเวิร์กชีตข้อมูลในไฟล์เทมเพลต และบันทึกไฟล์ในรูปแบบ CSV *ที่คั่นด้วยเครื่องหมายจุลภาค*

เคล็ดลับ: ไฟล์เทมเพลต Excel ประกอบด้วยเวิร์กชีต **ข้อมูล** และเวิร์กชีต **Readme** ใช้เวิร์กชีต **ข้อมูล** เพื่อกรอกข้อมูลอุปกรณ์ เวิร์กชีต **Readme** ประกอบด้วยข้อมูลเกี่ยวกับวิธีกรอกข้อมูลในแต่ละฟิลด์ในเวิร์กชีต **ข้อมูล** (รวมถึงฟิลด์ที่จำเป็น) และตัวอย่างต่างๆ

ข้อสำคัญ:

- อุปกรณ์จะได้รับการจัดการตามลำดับที่แสดงในไฟล์นำเข้าเป็นกลุ่ม
- XClarity Administrator จะใช้ข้อมูลการกำหนดแร็คที่กำหนดไว้ในการกำหนดค่าอุปกรณ์เมื่ออุปกรณ์ได้รับการจัดการ หากคุณเปลี่ยนการกำหนดแร็คใน XClarity Administrator แล้ว XClarity Administrator ก็จะอัปเดตการกำหนดค่าของอุปกรณ์ หากคุณอัปเดตการกำหนดค่าอุปกรณ์หลังจากที่อุปกรณ์ได้รับการจัดการ การเปลี่ยนแปลงจะแสดงใน XClarity Administrator
- ขอแนะนำให้สร้างแร็คในสเปรดชีตอย่างชัดเจนก่อนกำหนดแร็คให้กับอุปกรณ์ แต่ทั้งนี้ก็ไม่จำเป็นต้องทำก็ได้ หากแร็คไม่ได้รับการกำหนดw;hอย่างชัดเจน และแร็คไม่มีอยู่แล้วใน XClarity Administrator ระบบจะใช้ข้อมูลการกำหนดแร็คที่ระบุไว้สำหรับอุปกรณ์เพื่อสร้างแร็คที่มีความสูงเริ่มต้นเป็น 52U

  หากคุณต้องการใช้ความสูงอื่นสำหรับแร็ค คุณต้องกำหนดแร็คในสเปรดชีตอย่างชัดเจนก่อนกำหนดให้กับอุปกรณ์

ในการกำหนดอุปกรณ์ในไฟล์นำเข้าเป็นกลุ่ม ให้ดำเนินการตามคอลัมน์ต่อไปนี้

- (คอลัมน์ A - C) สำหรับการค้นหาพื้นฐาน คุณจะต้องระบุประเภทอุปกรณ์ และที่อยู่ IP ปัจจุบันหรือหมายเลขประจำเครื่องของอุปกรณ์ รองรับประเภทต่อไปนี้:
  - **แผงครอบ** ตัวยึดสำหรับอุปกรณ์ที่ไม่ได้จัดการ ในมุมมองแร็ค อุปกรณ์นี้จะแสดงเป็นกราฟิกแผงครอบทั่วไป โปรดดูเวิร์กชีต **Readme** ในเทมเพลต Excel สำหรับประเภทแผงครอบเพิ่มเติม
  - **flexchassis**. ตัวเครื่อง Flex System 10U
  - **เซิร์ฟเวอร์** เซิร์ฟเวอร์ในแร็คและเซิร์ฟเวอร์แบบทาวเวอร์ได้รับการรองรับโดย XClarity Administrator
  - **แร็ค** แร็ค 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U และ 52U ไม่รองรับความสูงของแร็คอื่นๆ ระบบจะใช้ 52U เป็นค่าเริ่มต้น
  - **ที่จัดเก็บ** อุปกรณ์จัดเก็บ
  - **สวิตช์** สวิตช์ของ RackSwitch

  หมายเหตุ: โหนดคอมพิวท์ สวิตช์ และอุปกรณ์การจัดเก็บข้อมูล Flex System ถือว่าเป็นส่วนหนึ่งของการสำรวจและกระบวนการจัดการตัวเครื่อง
- (คอลัมน์ D - H) หากคุณเลือกใช้ข้อมูลประจำตัวที่ป้อนด้วยตนเองแทนข้อมูลประจำตัวที่จัดเก็บไว้ (คอลัมน์ Z) (Columns Z) หรือข้อมูลประจำตัว (คอลัมน์ AF – AJ) ให้ระบุชื่อผู้ใช้และรหัสผ่านปัจจุบัน ข้อมูลประจำตัวที่ป้อนด้วยตนเองมีประโยชน์หากข้อมูลประจำตัวสำหรับอุปกรณ์บางเครื่องแตกต่างกัน หากคุณไม่ระบุข้อมูลประจำตัวสำหรับอุปกรณ์อย่างน้อยหนึ่งตัวในไฟล์นำเข้าเป็นกลุ่ม ระบบจะใช้ข้อมูลประจำตัวส่วนกลาง

ที่คุณระบุในกล่องโต้ตอบ นำเข้าเป็นกลุ่ม แทน สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการป้อนผู้ใช้และการตรวจสอบความถูกต้องที่ได้รับการจัดการด้วยตนเอง โปรดดู การจัดการบัญชีผู้ใช้ ในเอกสารแบบออนไลน์ของ XClarity Administrator

หมายเหตุ:

- หากต้องการใช้ข้อมูลประจำตัวที่ป้อนด้วยตนเอง คุณต้องเลือกการตรวจสอบความถูกต้องที่ได้รับการจัดการสำหรับ XClarity Administrator
- บางฟิลด์ไม่ได้นำไปใช้กับอุปกรณ์บางตัว
- (สำหรับตัวเครื่อง) หากคุณเลือกการตรวจสอบความถูกต้องที่ได้รับการจัดการ (ในคอลัมน์ AA หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม) คุณต้องระบุรหัสผ่าน `RECOVERY_ID` ในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่ม หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม หากคุณเลือกการตรวจสอบความถูกต้องในเครื่อง จะไม่อนุญาตให้ใช้รหัสผ่านในการกู้คืน ไม่ต้องระบุรหัสผ่านในการกู้คืนในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่ม หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม
- (สำหรับเซิร์ฟเวอร์ในแร็ค) หากคุณเลือกการตรวจสอบความถูกต้องที่ได้รับการจัดการ (ในคอลัมน์ AA หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม) คุณสามารถเลือกระบุรหัสผ่านในการกู้คืนในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่ม หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม หากคุณเลือกการตรวจสอบความถูกต้องในเครื่อง จะไม่อนุญาตให้ใช้รหัสผ่านในการกู้คืน ไม่ต้องระบุรหัสผ่านในการกู้คืนในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่ม หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม
- (สำหรับสวิตช์บนแร็ค) อุปกรณ์ RackSwitch จะรองรับเฉพาะข้อมูลประจำตัวที่จัดเก็บไว้ (ในคอลัมน์ Z) สำหรับการรับรองความถูกต้องกับสวิตช์ ทั้งนี้ จะไม่รองรับข้อมูลประจำตัวของผู้ใช้แบบกำหนดเอง

- (คอลัมน์ I -U) คุณสามารถเลือกระบุข้อมูลเพิ่มเติมหากคุณต้องการนำการเปลี่ยนแปลงไปใช้กับอุปกรณ์เมื่อการจัดการเสร็จสมบูรณ์

  หมายเหตุ: บางฟิลด์ไม่ได้นำไปใช้กับอุปกรณ์บางตัว ฟิลด์เหล่านี้ไม่ได้นำไปใช้กับสวิตช์ของ RackSwitch
- (คอลัมน์ V- Z) คุณสามารถเลือกที่จะให้ข้อมูลสำหรับการสร้างแร็คและการกำหนดได้ โดยประกอบด้วย ชื่อแร็ค ตำแหน่ง ห้อง หน่วยแร็คล่างสุด และความสูง

  หมายเหตุ:

  - ขณะสร้างแร็ค คุณต้องระบุชื่อแร็คและความสูงของแร็ค รองรับความสูงของแร็คต่อไปนี้: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U และ 52U ไม่รองรับความสูงของแร็คอื่นๆ
  - ขณะสร้างแผงครอบทั่วไป คุณต้องระบุชื่อแร็คและความสูงของแผงครอบ รองรับความสูงของแผงครอบต่อไปนี้: 1U, 2U และ 4U
  - ขณะสร้างแผงครอบที่ระบุเฉพาะ ระบบจะละเว้นความสูงของแผงครอง XClarity Administrator นั้น ทราบข้อมูลความสูงของแผงครอบแต่ละประเภท ดูสเปรดชีตเทมเพลตสำหรับประเภทและความสูงของแผงครอบ

- ขณะกำหนดอุปกรณ์ให้กับแร็ค ระบบจะละเว้นความสูงของอุปกรณ์ โดยจะดึงข้อมูลความสูงของอุปกรณ์จากรายการอุปกรณ์

- (คอลัมน์ AA) หากการจัดการไม่สำเร็จเนื่องจากเงื่อนไขข้อผิดพลาดต่อไปนี้ ให้ทำซ้ำขั้นตอนนี้โดยใช้ตัวเลือกการจัดการแบบบังคับ

  - หาก XClarity Administrator การจัดการล้มเหลวและไม่สามารถกู้คืนได้

    หมายเหตุ: หากอินสแตนซ์ XClarity Administrator ทดแทนใช้ที่อยู่ IP เดียวกันกับ XClarity Administrator ที่ล้มเหลว คุณสามารถจัดการอุปกรณ์อีกครั้งโดยใช้บัญชีและรหัสผ่าน RECOVERY_ID (หากมี) และตัวเลือกการจัดการแบบบังคับ

  - หากมีการนำ XClarity Administrator การจัดการออกก่อนถอนการจัดการอุปกรณ์

  - หากอุปกรณ์ไม่ได้ถูกถอนการจัดการโดยเสร็จสมบูรณ์

  สามารถจัดการอุปกรณ์โดยอินสแตนซ์ XClarity Administrator ทีละรายการเท่านั้น ไม่รองรับการจัดการโดยอินสแตนซ์ XClarity Administrator หลายรายการ หากอุปกรณ์การจัดเก็บข้อมูลได้รับการจัดการโดย XClarity Administrator หนึ่งรายการ แล้วคุณต้องการจัดการกับ XClarity Administrator อื่น คุณต้องถอนการจัดการอุปกรณ์ก่อนจาก XClarity Administrator เดิม แล้วจัดการกับ XClarity Administrator ใหม่

  ข้อสำคัญ: หากคุณเปลี่ยนแปลงที่อยู่ IP ของเซิร์ฟเวอร์หลังจากเซิร์ฟเวอร์ได้รับการจัดการโดย XClarity Administrator XClarity Administrator จะจดจำที่อยู่ IP ใหม่ และดำเนินการจัดการเซิร์ฟเวอร์ต่อ อย่างไรก็ตาม XClarity Administrator จะไม่รู้จักการเปลี่ยนแปลงที่อยู่ IP สำหรับเซิร์ฟเวอร์บางประเภท หาก XClarity Administrator แสดงว่าเซิร์ฟเวอร์ออฟไลน์หลังจากที่อยู่ IP ถูกเปลี่ยนแปลง ให้จัดการเซิร์ฟเวอร์อีกครั้งโดยใช้ตัวเลือกการจัดการแบบบังคับ

- (คอลัมน์ AB) หากคุณเลือกใช้ข้อมูลประจำตัวที่จัดเก็บไว้แทนการป้อนข้อมูลประจำตัวด้วยตนเอง (คอลัมน์ D – H) หรือข้อมูลประจำตัว (คอลัมน์ AF – AJ) ให้ระบุ ID ข้อมูลประจำตัวที่จัดเก็บไว้ คุณสามารถค้นหา ID ข้อมูลประจำตัวที่จัดเก็บไว้ในหน้าข้อมูลประจำตัวที่จัดเก็บไว้โดยคลิก **การดูแล ➔ การรักษาความปลอดภัย** จากเมนู XClarity Administrator แล้วคลิก **ข้อมูลประจำตัวที่จัดเก็บไว้** จากแผงการนำทางด้านซ้าย สำหรับข้อมูลเพิ่มเติมเกี่ยวข้อมูลประจำตัวและการตรวจสอบความถูกต้องภายในเครื่อง โปรดดู การจัดการข้อมูลประจำตัวที่จัดเก็บไว้ ในเอกสารแบบออนไลน์ของXClarity Administrator

  หมายเหตุ:

  - อุปกรณ์ RackSwtich รองรับเฉพาะข้อมูลประจำตัวที่จัดเก็บไว้เท่านั้นสำหรับการตรวจสอบความถูกต้อง ทั้งนี้ จะไม่รองรับข้อมูลประจำตัวของผู้ใช้แบบกำหนดเอง (ในคอลัมน์ D)

  - หากคุณจัดการอุปกรณ์โดยใช้ข้อมูลประจำตัวที่จัดเก็บไว้ และเปิดใช้งานการตรวจสอบความถูกต้องที่ได้รับการจัดการ คุณจะไม่สามารถแก้ไขข้อมูลประจำตัวที่จัดเก็บไว้ดังกล่าวได้

- (คอลัมน์ AC) สำหรับตัวเครื่องและเซิร์ฟเวอร์ในแร็ค หากคุณเลือกที่จะใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการ คุณสามารถระบุรหัสผ่าน RECOVERY_ID ในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่มหรือในกล่อง

โต้ตอบนำเข้าเป็นกลุ่ม หากคุณเลือกการตรวจสอบความถูกต้องในเครื่อง จะไม่อนุญาตให้ใช้รหัสผ่านในการกู้คืน ไม่ต้องระบุรหัสผ่านในการกู้คืนในคอลัมน์ G ของไฟล์นำเข้าเป็นกลุ่ม หรือในกล่องโต้ตอบนำเข้าเป็นกลุ่ม

- (คอลัมน์ AD) สำหรับเซิร์ฟเวอร์ในตู้แร็ค คุณสามารถเลือกใช้การตรวจสอบความถูกต้องในเครื่องแทนการตรวจสอบความถูกต้องที่ได้รับการจัดการของ XClarity Administrator โดยระบุ FALSE ในคอลัมน์นี้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตรวจสอบความถูกต้องที่ได้รับการจัดการและการตรวจสอบความถูกต้องในเครื่อง โปรดดู การจัดการเซิร์ฟเวอร์การตรวจสอบความถูกต้อง ในเอกสารแบบออนไลน์ของ XClarity Administrator
- (คอลัมน์ AE) คุณสามารถเลือกที่จะระบุรายการกลุ่มบทบาทที่ได้รับอนุญาตให้ดูและจัดการอุปกรณ์ คุณสามารถระบุเฉพาะกลุ่มบทบาทที่ผู้ใช้ปัจจุบันอยู่

  หมายเหตุ: หากคุณเพิ่มอุปกรณ์ให้กับตัวเครื่องที่ได้รับการจัดการ อุปกรณ์ใหม่อยู่ในกลุ่มบทบาทเดียวกันกับตัวเครื่อง
- (คอลัมน์ AF – AJ) หากคุณเลือกใช้ระบบการจัดการข้อมูลประจำตัวแทนข้อมูลประจำตัวที่ป้อนด้วยตนเอง (คอลัมน์ D – H) หรือข้อมูลประจำตัวที่จัดเก็บไว้ (คอลัมน์ AB) ให้ระบุที่อยู่ IP หรือชื่อโฮสต์ของเซิร์ฟเวอร์ที่มีการจัดการ ชื่อผู้ใช้ และเลือกที่จะระบุ ID แอปพลิเคชัน ที่จัดเก็บ และโฟลเดอร์

  หากคุณระบุ ID แอปพลิเคชัน คุณต้องระบุที่จัดเก็บและโฟลเดอร์ด้วย หากมี

  หากคุณไม่ระบุ ID แอปพลิเคชัน XClarity Administrator จะใช้พาธที่กำหนดไว้เมื่อคุณตั้งค่า CyberArk เพื่อระบุบัญชีที่ออนบอร์ดใน CyberArk

  หมายเหตุ: รองรับเฉพาะเซิร์ฟเวอร์ ThinkSystem หรือ ThinkAgile เท่านั้น ต้องกำหนดค่าระบบการจัดการข้อมูลประจำตัวใน XClarity Administrator และ Lenovo XClarity Controller สำหรับเซิร์ฟเวอร์ ThinkSystem ที่มีการจัดการหรือ ThinkAgile ต้องรวมเข้ากับ CyberArk

ภาพต่อไปนี้แสดงตัวอย่างไฟล์นำเข้าเป็นกลุ่ม:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9	2002:939:	2002:9:	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. จากตัวช่วยสร้าง นำเข้าเป็นกลุ่ม ให้ป้อนชื่อไฟล์ CSV เพื่ออัปโหลดไฟล์สำหรับการประมวลผล คุณสามารถคลิก **เรียกดู** เพื่อช่วยค้นหาไฟล์ได้
7. คลิก **อัปโหลด** เพื่ออัปโหลด และตรวจสอบไฟล์
8. คลิก **ถัดไป** เพื่อแสดงหน้า สรุปอินพุต ที่มีรายการอุปกรณ์ที่ได้รับการจัดการ

นำเข่าเป็นกลุ่ม

สรุปการป้อนข้อมูล

สิ่งที่แสดงคือรายการอุปกรณ์ที่จะได้รับการจัดการ คุณอาจต้องการตรวจสอบข้อมูลก่อนสิ้นสุดตัวช่วยสร้าง คุณสามารถกลับไปอัปโหลดไฟล์ที่ถูกต้องใหม่เสมอถ้าจำเป็น

☐ แสดงเฉพาะแถวที่อาจมีปัญหา

อุปกรณ์ที่จะได้รับการจัดการทั้งหมด 4 เครื่อง: ตัวเครื่อง 1 ตัว, สวิตช์ 1 ตัว, เซิร์ฟเวอร์ 2 ตัว, ที่จัดเก็บ 0 ตัว

CSV Row	Name	Current IP	Credentials	Type
2	Server_1	192.0.2.0	จำเป็นต้องมีอินพุต	server
3	Chassis_1		จำเป็นต้องมีอินพุต	flexchassis
4	Rack_2		จำเป็นต้องมีอินพุต	rack
5	Filler		จำเป็นต้องมีอินพุต	filler

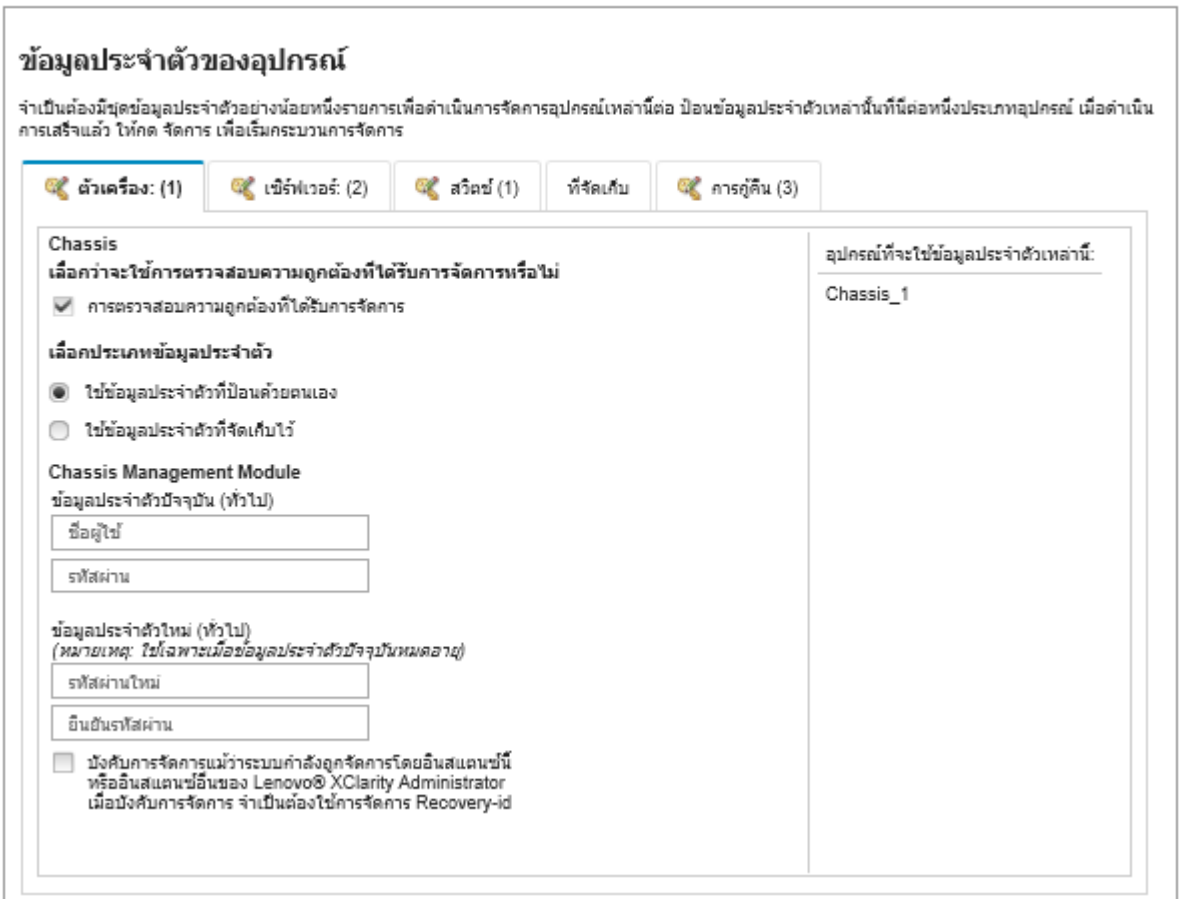
9. ตรวจดูข้อมูลสรุปของอุปกรณ์ที่คุณต้องการจัดการ

   เลือก **แสดงเฉพาะแถวอาจมีปัญหา** เพื่อแสดงแถวที่มีข้อมูลไม่ครบถ้วน แก้ปัญหาใดๆ ในไฟล์นำเข้าเป็นกลุ่ม แล้วคลิก **ย้อนกลับ** เพื่ออัปโหลดไฟล์ CSV ที่แก้ไขแล้ว

หมายเหตุ:

- หากไม่ได้ให้ข้อมูลที่จำเป็นในไฟล์นำเข้าเป็นกลุ่ม อุปกรณ์ที่เกี่ยวข้องจะไม่ได้รับการจัดการ
- หน้า สรุปอินพุต จะระบุแถวที่ไม่มีข้อมูลประจำตัว หากคุณไม่ระบุข้อมูลประจำตัวในไฟล์นำเข้าเป็นกลุ่ม ระบบจะใช้ข้อมูลประจำตัวส่วนกลางที่คุณระบุในตัวช่วยสร้าง นำเข้าเป็นกลุ่ม แทน

10. คลิก **ถัดไป** เพื่อแสดงหน้า ข้อมูลประจำตัวของอุปกรณ์



11. **ตัวเลือกเสริม**: คลิกที่แท็บแต่ละแท็บ และเลือกที่จะระบุการตั้งค่าและข้อมูลประจำตัวส่วนกลางสำหรับใช้กับอุปกรณ์ตามประเภทที่ระบุทั้งหมด อุปกรณ์จะใช้การตั้งค่าและข้อมูลประจำตัวส่วนกลางที่แสดงอยู่ทางด้านขวาของแท็บแต่ละแท็บ

    หากคุณเลือกใช้ข้อมูลประจำตัวส่วนกลาง ข้อมูลประจำตัวสำหรับประเภทอุปกรณ์ประเภทใดประเภทหนึ่งจะต้องเหมือนกันกับอุปกรณ์ประเภทเดียวกันนั้นทั้งหมด ที่ไม่ได้มีการป้อนข้อมูลประจำตัวในไฟล์นำเข้าเป็นกลุ่ม ตัวอย่างเช่น ข้อมูลประจำตัว CMM ต้องเหมือนกันสำหรับตัวเครื่องทั้งหมด และข้อมูลประจำตัวการจัดการที่จัดเก็บต้องเหมือนกันสำหรับอุปกรณ์การจัดเก็บข้อมูลทั้งหมด หากข้อมูลประจำตัวไม่เหมือนกัน คุณต้องป้อนข้อมูลประจำตัวในไฟล์นำเข้าเป็นกลุ่ม

- **ตัวเครื่อง** ระบุโหมดการตรวจสอบความถูกต้องและประเภทข้อมูลประจำตัว ระบุข้อมูลประจำตัวปัจจุบันสำหรับการเข้าสู่ระบบตัวเครื่องทั้งหมดที่กำหนดในไฟล์นำเข้าเป็นกลุ่ม ระบุรหัสผ่านใหม่ที่จะใช้หากข้อมูลประจำตัว CMM ปัจจุบันหมดอายุแล้ว

  หากคุณบังคับการจัดการตัวเครื่อง ให้ระบุบัญชีและรหัสผ่าน RECOVERY_ID สำหรับข้อมูลประจำตัวของอุปกรณ์

- **เซิร์ฟเวอร์** ระบุโหมดการตรวจสอบความถูกต้องและประเภทข้อมูลประจำตัว ระบุข้อมูลประจำตัวปัจจุบันสำหรับการเข้าสู่ระบบเซิร์ฟเวอร์ในแร็คและเซิร์ฟเวอร์แบบทาวเวอร์ทั้งหมดที่กำหนดในไฟล์นำเข้าเป็นกลุ่ม ระบุรหัสผ่านใหม่ที่จะใช้หากข้อมูลประจำตัว ตัวควบคุมการจัดการแผงวงจร ปัจจุบันหมดอายุแล้ว

  หากคุณบังคับการจัดการเซิร์ฟเวอร์ ให้ระบุบัญชีและรหัสผ่าน RECOVERY_ID สำหรับข้อมูลประจำตัวของอุปกรณ์

- **สวิตช์** ระบุข้อมูลประจำตัวที่จัดเก็บไว้สำหรับการเข้าสู่ระบบสวิตช์ของ RackSwitch ทั้งหมดที่กำหนดในไฟล์นำเข้าเป็นกลุ่ม หากตั้งค่าไว้ ให้ระบุรหัสผ่าน “enable” ที่ใช้เพื่อเข้าสู่โหมด Privileged Exec บนสวิตช์นั้น
- **ที่จัดเก็บ** ระบุข้อมูลประจำตัวปัจจุบันสำหรับการเข้าสู่ระบบอุปกรณ์การจัดเก็บข้อมูลทั้งหมดที่กำหนดในไฟล์นำเข้าเป็นกลุ่ม
- **การกู้คืน** ระบุรหัสผ่านในการกู้คืนสำหรับการเข้าสู่ระบบเซิร์ฟเวอร์และตัวเครื่องทั้งหมดที่กำหนดในไฟล์นำเข้าเป็นกลุ่ม

  คุณสามารถเลือกใช้ได้ทั้งบัญชีผู้ใช้ภายในหรือข้อมูลประจำตัวการกู้คืนที่จัดเก็บไว้ ไม่ว่าจะเลือกใช้ตัวเลือกใด ชื่อผู้ใช้จะต้องเป็น `RECOVERY_ID` เสมอ

  เมื่อระบุรหัสผ่าน ระบบจะสร้างบัญชี `RECOVERY_ID` บนอุปกรณ์ และบัญชีผู้ใช้ภายในระบบทั้งหมดจะถูกปิดใช้งาน

  - สำหรับตัวเครื่อง จำเป็นต้องใช้รหัสผ่านในการกู้คืน
  - สำหรับเซิร์ฟเวอร์ รหัสผ่านในการกู้คืนเป็นตัวเลือกที่ระบุหรือไม่ก็ได้หากคุณเลือกที่จะใช้การตรวจสอบความถูกต้องที่ได้รับการจัดการ และไม่สามารถใช้ได้หากคุณเลือกใช้การตรวจสอบความถูกต้องในเครื่อง
  - ตรวจสอบให้แน่ใจว่ารหัสผ่านเป็นไปตามนโยบายการรักษาความปลอดภัยและรหัสผ่านสำหรับอุปกรณ์นโยบายการรักษาความปลอดภัยและรหัสผ่านอาจแตกต่างกันไป
  - ตรวจสอบว่าคุณบันทึกรหัสผ่านในการกู้คืนสำหรับการใช้งานในอนาคต
  - ไม่รองรับบัญชีการกู้คืนสำหรับเซิร์ฟเวอร์ ThinkServer และ System x M4

ข้อมูลที่คุณระบุไว้ในไฟล์นำเข้าเป็นกลุ่มจะแทนที่ข้อมูลที่คล้ายคลึงกันที่คุณระบุในหน้า ข้อมูลประจำตัวของอุปกรณ์

คุณสามารถเลือกบังคับการจัดการอุปกรณ์แต่ละประเภทได้ ถ้า:

- ขณะนี้อุปกรณ์ได้รับการจัดการโดยระบบการจัดการอื่น เช่น อินสแตนซ์ XClarity Administrator อื่น หรือ IBM Flex System Manager

- มีการนำ XClarity Administrator ออก แต่ยังไม่ได้ถอนการจัดการอุปกรณ์ก่อนเลิกใช้งาน
- อุปกรณ์ไม่ได้รับการถอนการจัดการอย่างถูกต้อง และยังไม่ได้ล้างการสมัครรับข้อมูล CIM

หมายเหตุ: หากอุปกรณ์ได้รับการจัดการโดยอินสแตนซ์ XClarity Administrator อื่น อุปกรณ์จะได้รับการจัดการโดยอินสแตนซ์เดิมเป็นระยะเวลาหนึ่งหลังจากเกิดการจัดการแบบบังคับ คุณสามารถถอนการจัดการอุปกรณ์เพื่อนำอุปกรณ์ออกจากอินสแตนซ์ XClarity Administrator เดิม

12. คลิก **จัดการ** หน้า ผลลัพธ์การตรวจสอบ จะแสดงข้อมูลเกี่ยวกับสถานะการจัดการของอุปกรณ์แต่ละอุปกรณ์ในไฟล์นำเข้าเป็นกลุ่ม

    ระบบจะสร้างงานสำหรับกระบวนการจัดการ หากคุณปิดตัวช่วยสร้างการนำเข้าเป็นกลุ่ม กระบวนการจัดการจะดำเนินการต่อในพื้นหลัง คุณสามารถตรวจสอบสถานะของกระบวนการจัดการได้จากบันทึกงาน สำหรับข้อมูลเกี่ยวกับบันทึกงาน โปรดดู การติดตามข้อมูลงาน ในเอกสารแบบออนไลน์ของ XClarity Administrator

    หาก XClarity Administrator ไม่สามารถเข้าสู่ระบบอุปกรณ์โดยใช้ข้อมูลประจำตัวที่ระบุในไฟล์นำเข้าเป็นกลุ่ม หรือข้อมูลประจำตัวส่วนกลางที่ระบุในกล่องโต้ตอบ การจัดการอุปกรณ์ล้มเหลว และ XClarity Administrator ย้ายไปยังอุปกรณ์ถัดไปในไฟล์นำเข้าเป็นกลุ่ม

    หมายเหตุ: หากการจัดการไม่สำเร็จเนื่องจากเงื่อนไขข้อผิดพลาดต่อไปนี้ ให้ทำซ้ำขั้นตอนนี้โดยใช้ตัวเลือก**การจัดการแบบบังคับ**

    - หาก XClarity Administrator การจัดการล้มเหลวและไม่สามารถกู้คืนได้

      หมายเหตุ: หากอินสแตนซ์ XClarity Administrator ทดแทนใช้ที่อยู่ IP เดียวกันกับ XClarity Administrator ที่ล้มเหลว คุณสามารถจัดการอุปกรณ์อีกครั้งโดยใช้บัญชีและรหัสผ่าน RECOVERY_ID (หากมี) และตัวเลือก **การจัดการแบบบังคับ**

    - หากมีการนำ XClarity Administrator การจัดการออกก่อนถอนการจัดการอุปกรณ์
    - หากอุปกรณ์ไม่ได้ถูกถอนการจัดการโดยเสร็จสมบูรณ์

    ข้อควรพิจารณา: สามารถจัดการอุปกรณ์โดยอินสแตนซ์ XClarity Administrator ทีละรายการเท่านั้น ไม่รองรับการจัดการโดยอินสแตนซ์ XClarity Administrator หลายรายการ หากอุปกรณ์ได้รับการจัดการโดย XClarity Administrator หนึ่งรายการ แล้วคุณต้องการจัดการกับ XClarity Administrator อื่น คุณต้องถอนการจัดการอุปกรณ์จาก XClarity Administrator เดิมก่อนแล้วจัดการกับ XClarity Administrator ใหม่

13. หากไฟล์นำเข้าเป็นกลุ่มรวมตัวเครื่องใหม่ไว้ด้วย ให้ตรวจสอบและเปลี่ยนการตั้งค่าเครือข่ายการจัดการสำหรับทั้งตัวเครื่อง (รวมถึงโหนดคอมพิวท์และสวิตช์ Flex) และเพื่อกำหนดค่าข้อมูลโหนดคอมพิวท์ อุปกรณ์การจัดเก็บข้อมูลภายใน อะแดปเตอร์ I/O, เป้าหมายการบูต และการตั้งค่าเฟิร์มแวร์ โดยการสร้างและปรับใช้รูปแบบเซิร์ฟเวอร์ สำหรับข้อมูลเพิ่มเติม โปรดดู การแก้ไขการตั้งค่า IP การจัดการสำหรับตัวเครื่อง และ การกำหนดค่าเซิร์ฟเวอร์โดยใช้ XClarity Administrator ในเอกสารแบบออนไลน์ของ XClarity Administrator

หลังจากดำเนินการเสร็จ

หลังจากที่จัดการระบบแล้ว คุณสามารถดำเนินการดังต่อไปนี้:

- ค้นหาและจัดการระบบเพิ่มเติม (โปรดดู การจัดการตัวเครื่อง, การจัดการแร็ค, การจัดการเซิร์ฟเวอร์, การจัดการอุปกรณ์จัดเก็บ และ การจัดการสวิตช์ ในเอกสารแบบออนไลน์ของ Lenovo XClarity Administrator)
- กำหนดค่าข้อมูลระบบ, อุปกรณ์การจัดเก็บข้อมูลภายใน, อะแดปเตอร์ I/O, การตั้งค่าการบูต และการตั้งค่าเฟิร์มแวร์ โดยสร้างและปรับใช้รูปแบบเซิร์ฟเวอร์ (โปรดดู การกำหนดค่าเซิร์ฟเวอร์โดยใช้ XClarity Administrator ในเอกสารแบบออนไลน์ของ Lenovo XClarity Administrator)
- ปรับใช้อิมเมจระบบปฏิบัติการกับเซิร์ฟเวอร์ที่ยังไม่ได้ติดตั้งระบบปฏิบัติการ (โปรดดู การปรับใช้อิมเมจระบบปฏิบัติการ ในเอกสารแบบออนไลน์ของ XClarity Administrator)
- อัปเดตเฟิร์มแวร์บนอุปกรณ์ที่ไม่เป็นไปตามนโยบายปัจจุบัน (โปรดดู การอัปเดตเฟิร์มแวร์บนอุปกรณ์ที่มีการจัดการ ในเอกสารแบบออนไลน์ของ XClarity Administrator)
- เพิ่มระบบที่เพิ่งได้รับการจัดการไปยังแร็คที่เหมาะสมเพื่อแสดงสภาพแวดล้อมจริง (โปรดดู การจัดการแร็ค ในเอกสารแบบออนไลน์ของ XClarity Administrator)
- ตรวจสอบสถานะและรายละเอียดของฮาร์ดแวร์ (โปรดดู การดูสถานะของเซิร์ฟเวอร์ที่มีการจัดการ ในเอกสารแบบออนไลน์ของ XClarity Administrator)
- ตรวจสอบเหตุการณ์และการแจ้งเตือน (โปรดดู การทำงานกับเหตุการณ์ และ การทำงานกับการแจ้งเตือน ในเอกสารแบบออนไลน์ของ XClarity Administrator)
- ปิดใช้งานหรือเปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวสำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ที่มีการจัดการ
  - สำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ทั้งหมดที่มีการจัดการ (ส่วนกลาง) ให้คลิก **การดูแลระบบ ➔ การรักษาความปลอดภัย** จากแถบเมนู XClarity Administrator คลิก **เซสชันที่กำลังทำงาน** แล้วเปิดใช้งานหรือปิดใช้งาน **การเข้าสู่ระบบแบบครั้งเดียว**
  - สำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile บางเครื่อง ให้คลิก **ฮาร์ดแวร์ ➔ เซิร์ฟเวอร์** จากแถบเมนู XClarity Administrator แล้วคลิก **การดำเนินการทั้งหมด ➔ การรักษาความปลอดภัย ➔ เปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียว** หรือ **การดำเนินการทั้งหมด ➔ การรักษาความปลอดภัย ➔ ปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียว**.

หมายเหตุ: การเข้าสู่ระบบแบบครั้งเดียวอนุญาตให้ผู้ใช้ที่เข้าสู่ระบบ XClarity Administrator อยู่แล้ว เข้าสู่ระบบตัวควบคุมการจัดการแผงวงจรโดยอัตโนมัติ การเข้าสู่ระบบแบบครั้งเดียวจะเปิดใช้งานตามค่าเริ่มต้นเมื่อเซิร์ฟเวอร์ ThinkSystem หรือ ThinkAgile ถูกนำเข้าสู่การจัดการโดย XClarity Administrator (เว้นแต่เซิร์ฟเวอร์จะจัดการด้วยรหัสผ่าน CyberArk) คุณสามารถกำหนดค่าการตั้งค่าส่วนกลางเพื่อเปิดใช้งานหรือปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวกับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ที่มีการจัดการทั้งหมดได้ การเปิดใช้งานการเข้าสู่ระบบแบบครั้งเดียวสำหรับเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile บางเครื่องจะแทนที่การตั้งค่าส่วนกลางของเซิร์ฟเวอร์ ThinkSystem และ ThinkAgile ทั้งหมด

บทที่ 5. การลงทะเบียน XClarity Administrator

การลงทะเบียนอินสแตนซ์ของ Lenovo XClarity Administrator ทำให้คุณสามารถใช้คุณสมบัติพื้นฐานโดยไม่ได้รับคำเตือนซ้ำๆ เกี่ยวกับการหมดอายุของการทดลองใช้และสิทธิ์การใช้งานที่ไม่เป็นไปตามข้อกำหนด หลังจากลงทะเบียนแล้ว คำเตือนสำหรับการไม่เป็นไปตามข้อกำหนดจะไม่แสดงอีกต่อไป อย่างไรก็ตาม ฟังก์ชันทั้งหมดที่ต้องมีสิทธิ์การใช้งานจะยังคงปิดใช้งานอยู่ จนกว่าคุณจะซื้อและติดตั้งสิทธิ์การใช้งานตามจำนวนอุปกรณ์ที่มีการจัดการ

เกี่ยวกับงานนี้

การลงทะเบียนอินสแตนซ์ XClarity Administrator ไม่จำเป็นต้องเปิดเผยข้อมูลติดต่อของคุณ Lenovo ไม่เปิดเผยข้อมูลที่คุณให้ไว้กับหน่วยงานภายนอกอื่นๆ

หากคุณติดตั้งสิทธิ์การใช้งานฟังก์ชันขั้นสูงไปแล้ว คุณไม่จำเป็นต้องลงทะเบียนอินสแตนซ์ XClarity Administrator ดูข้อมูลเพิ่มเติมเกี่ยวกับสิทธิ์การใช้งานและฟังก์ชันขั้นสูง โปรดดู การติดตั้งใบอนุญาตการเปิดใช้งานเต็มรูปแบบ

ขั้นตอน

ในการลงทะเบียน XClarity Administrator ให้ทำตามขั้นตอนต่อไปนี้

- หาก XClarity Administrator เชื่อมต่อกับอินเทอร์เน็ต
    1. จากแถบเมนู Lenovo XClarity Administrator ให้คลิก **การดูแลระบบ ➔ การลงทะเบียน** เพื่อแสดงหน้าการลงทะเบียน
    2. คลิก **ลงทะเบียน** เพื่อลงทะเบียนอินสแตนซ์ของ XClarity Administrator
    3. กรอกชื่อบริษัท จำนวนอุปกรณ์ที่จะจัดการโดย XClarity Administrator และประเทศที่ XClarity Administrator ตั้งอยู่
    4. คลิก **ส่ง**
- หาก XClarity Administrator ไม่ได้เชื่อมต่อกับอินเทอร์เน็ต
    1. ลงทะเบียน XClarity Administrator
        a. ในเว็บเบราเซอร์ ให้เปิด เว็บพอร์ทัลการลงทะเบียน Lenovo XClarity
        b. กรอกชื่อบริษัท จำนวนอุปกรณ์ที่จะจัดการโดย XClarity Administrator และประเทศที่ XClarity Administrator ตั้งอยู่
        c. คลิก **ส่ง** เพื่อรับโทเค็นการลงทะเบียน
    2. จากแถบเมนู Lenovo XClarity Administrator ให้คลิก **การดูแลระบบ ➔ การลงทะเบียน** เพื่อแสดงหน้าการลงทะเบียน

3. คลิก **นำเข้า** เพื่อนำเข้าโทเค็นการลงทะเบียน
4. กรอกข้อมูลโทเค็นการลงทะเบียนที่คุณได้รับในขั้นตอนที่ 1
5. คลิก **ส่ง**

บทที่ 6. การติดตั้งใบอนุญาตการเปิดใช้งานเต็มรูปแบบ

หลังจากการทดลองใช้ฟรี 90 วัน หมดอายุ คุณต้องซื้อและติดตั้งสิทธิ์การใช้งาน Lenovo XClarity Pro สำหรับทุกอุปกรณ์ที่ได้รับการจัดการ ที่รองรับฟังก์ชันขั้นสูง เพื่อใช้การปรับใช้ระบบปฏิบัติการ และคุณลักษณะการกำหนดค่าอุปกรณ์ใน Lenovo XClarity Administrator คุณต้องมี Lenovo XClarity Pro สิทธิ์การใช้งานสำหรับอุปกรณ์ที่ได้รับการจัดการ *ทั้งหมด* เพื่อรับ XClarity Administrator บริการและการสนับสนุน

เรียนรู้เพิ่มเติม: XClarity Administrator: การติดตั้งใบอนุญาต

ก่อนจะเริ่มต้น

ตรวจสอบข้อควรพิจารณาสิทธิ์การใช้งานต่อไปนี้

- สิทธิ์การใช้งาน*ไม่ได้*ผูกกับอุปกรณ์เฉพาะเครื่อง
- สิทธิ์การใช้งานตัวเครื่องให้สิทธิ์การใช้งานสำหรับอุปกรณ์ 14 เครื่อง
- สำหรับเซิร์ฟเวอร์ที่ซับซ้อนและปรับขนาดได้ System x3850 X6 (6241) แต่ละเซิร์ฟเวอร์ต้องมีสิทธิ์การใช้งานแยกโดยไม่คำนึงถึงพาร์ติชัน
- สำหรับเซิร์ฟเวอร์ที่ซับซ้อนและปรับขนาดได้ System x3950 X6 (6241) หากไม่มีพาร์ติชัน แต่ละเซิร์ฟเวอร์ต้องมีสิทธิ์การใช้งานแยกกัน หากมีพาร์ติชัน แต่ละพาร์ติชันต้องมีสิทธิ์การใช้งานแยกกัน
- อุปกรณ์ต่อไปนี้*ไม่รองรับ*ฟังก์ชันขั้นสูงและ*ไม่จำเป็นต้องมี*สิทธิ์การใช้งานสำหรับคุณลักษณะเหล่านี้ แต่อย่างไรก็ตาม คุณต้องซื้อสิทธิ์การใช้งานสำหรับอุปกรณ์เหล่านี้แต่ละเครื่องเพื่อรับการบริการและการสนับสนุนของ XClarity Administrator
  - เซิร์ฟเวอร์ ThinkServer
  - เซิร์ฟเวอร์ System x M4
  - เซิร์ฟเวอร์ System x X5
  - เซิร์ฟเวอร์ System x3850 X6 และ x3950 X6 (3837)
  - อุปกรณ์จัดเก็บ
  - สวิตช์

คุณต้องมีสิทธิ์ระดับ **lxc-supervisor** หรือ **lxc-security-admin** จึงจะสามารถติดตั้งสิทธิ์การใช้งานเหล่านี้ได้

เกี่ยวกับงานนี้

XClarity Administrator รองรับสิทธิ์การใช้งานต่อไปนี้

- **Lenovo XClarity Pro** สิทธิ์การใช้งานแต่ละอันมีใบอนุญาตดังต่อไปนี้สำหรับอุปกรณ์ตัวเดียว
  - บริการและการสนับสนุนสำหรับ Lenovo XClarity Integrator
  - บริการและการสนับสนุนสำหรับ XClarity Administrator
  - ฟังก์ชันขั้นสูงภายใน XClarity Administrator:
    - การกำหนดค่าเซิร์ฟเวอร์โดยใช้รูปแบบการกำหนดค่า
    - การปรับใช้ระบบปฏิบัติการ
    - การรายงานปัญหาเกี่ยวกับ XClarity Administrator โดยใช้ Call Home (Call Home สำหรับการแจ้งเตือนฮาร์ดแวร์จะไม่ได้รับผลกระทบ)

ระยะเวลาการเปิดใช้งานสำหรับสิทธิ์การใช้งานจะเริ่มต้นเมื่อซื้อสิทธิ์การใช้งานและสร้างรหัสการอนุญาต

การปฏิบัติตามข้อกำหนดของสิทธิ์การใช้งานขึ้นอยู่กับจำนวนของอุปกรณ์ที่ได้รับการจัดการที่รองรับฟังก์ชันขั้นสูง จำนวนอุปกรณ์ที่ได้รับการจัดการต้องไม่เกินจำนวนสิทธิ์การใช้งานทั้งหมดในคีย์สิทธิ์การใช้งานที่ใช้งานอยู่ทั้งหมด หาก XClarity Administrator ไม่สอดคล้องกับสิทธิ์การใช้งานที่ติดตั้ง (ตัวอย่างเช่น หากสิทธิ์การใช้งานหมดอายุหรือหากจัดการอุปกรณ์เพิ่มเติมจนจำนวนเกินจำนวนสิทธิ์การใช้งานที่ใช้งานอยู่ทั้งหมด) คุณมีระยะเวลาผ่อนผัน 90 วันเพื่อติดตั้งสิทธิ์การใช้งานที่เหมาะสม ในแต่ละครั้งที่ XClarity Administrator ไม่เป็นไปตามข้อบังคับ ระยะเวลาผ่อนผันจะรีเซ็ตเป็น 90 วัน หากระยะปลอดหนี้ (รวมถึงการทดลองใช้ฟรี) สิ้นสุดก่อนที่สิทธิ์การใช้งานจะเป็นไปตามข้อกำหนด ฟังก์ชันขั้นสูงจะปิดใช้งานสำหรับอุปกรณ์ทั้งหมด

ตัวอย่างเช่น หากคุณจัดการเซิร์ฟเวอร์ ThinkSystem เพิ่มอีก 100 เซิร์ฟเวอร์และสวิตช์ Rack 20 สวิตช์ในอินสแตนซ์ XClarity Administrator ที่มีอยู่ คุณมีเวลา 90 วันในการซื้อและติดตั้งสิทธิ์การใช้งานเพิ่มเติม 100 สิทธิ์ก่อนที่ฟังก์ชันขั้นสูงจะถูกปิดใช้งานในส่วนอินเทอร์เฟซผู้ใช้ (สำหรับอุปกรณ์ทั้งหมด) สิทธิ์ใช้งานสำหรับสวิตช์ Rack ทั้ง 20 สิทธิ์ไม่จำเป็นต้องใช้ฟังก์ชันขั้นสูง อย่างไรก็ตาม จะต้องมีสิทธิ์ใช้งานเหล่านี้หากคุณต้องการบริการและการสนับสนุน หากมีการปิดใช้งานฟังก์ชันขั้นสูง จะมีการเปิดใช้งานฟังก์ชันขั้นสูงอีกครั้งหลังจากที่คุณติดตั้งสิทธิ์การใช้งานที่เพียงพอที่จะกลับไปเป็นตามข้อกำหนด

หากคุณใช้สิทธิ์การใช้งานแบบทดลองใช้ฟรีหรือคุณมีระยะเวลาผ่อนผันเพื่อให้สอดคล้องกับข้อบังคับ และคุณอัปเกรด XClarity Administrator เป็นเวอร์ชันใหม่กว่า สิทธิ์การใช้งานแบบทดลองใช้หรือระยะเวลาผ่อนผันจะรีเซ็ตเป็น 90 วัน

หมายเหตุ:

- การกำหนดค่าเซิร์ฟเวอร์และคุณลักษณะการปรับใช้ระบบปฏิบัติการจะถูกปิดใช้งานเมื่อหมดระยะเวลาผ่อนผัน
- Call Home สำหรับปัญหาเกี่ยวกับ XClarity Administrator (คุณลักษณะ Call Home ของซอฟต์แวร์) จะปิดใช้งานเมื่อสิทธิ์การใช้งานไม่เป็นไปตามข้อกำหนด ไม่มีระยะเวลาผ่อนผันสำหรับคุณลักษณะนี้ แต่ Call Home สำหรับการแจ้งเตือนฮาร์ดแวร์ไม่ได้รับผลกระทบ

หากมีการติดตั้งสิทธิ์การใช้งานอยู่แล้ว *ไม่*จำเป็นต้องใช้สิทธิ์การใช้งานสิทธิ์ใหม่เมื่อทำการอัปเกรดเป็นXClarity Administratorเวอร์ชันใหม่

คุณสามารถดูสถานะสิทธิ์การใช้งาน รวมถึงจำนวนวันที่เหลือของสิทธิ์การใช้งานเวอร์ชันทดลองใช้ได้โดยคลิกเมนูการดำเนินการของผู้ใช้ (

) บนแถบชื่อเรื่อง XClarity Administrator แล้วคลิก **เกี่ยวกับ**

การขอรับความช่วยเหลือ

- หากคุณประสบกับปัญหาและใช้บริการจากคู่ค้าธุรกิจ โปรดติดตั้งกับคู่ค้าธุรกิจของคุณเพื่อตรวจสอบความถูกต้องของธุรกรรมและสิทธิ์การใช้งาน
- หากคุณไม่ได้รับหลักฐานยืนยันสิทธิ์การใช้งานอิเล็กทรอนิกส์ รหัสการอนุญาต หรือคีย์เปิดใช้งาน หรือหากมีการส่งให้ผิดคน โปรดติดต่อตัวแทนในภูมิภาคตามที่ตั้งประเทศของคุณ
  - ESDNA@lenovo.com (ประเทศในอเมริกาเหนือ)
  - ESDAP@lenovo.com (ประเทศในเอเชียแปซิฟิก)
  - ESDEMEA@lenovo.com (ประเทศในยุโรป ตะวันออกกลาง และเอเชีย)
  - ESDLA@lenovo.com (ประเทศในลาตินอเมริกา)
  - ESDChina@Lenovo.com (ประเทศจีน)
- หากข้อมูลเกี่ยวกับการให้สิทธิ์การใช้งานของฉันไม่ถูกต้อง โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ SW_override@lenovo.com พร้อมข้อมูลต่อไปนี้:
  - หมายเลขใบสั่ง
  - ข้อมูลติดต่อของคุณ รวมถึงที่อยู่อีเมล
  - ที่อยู่จริงของคุณ
  - การเปลี่ยนแปลงที่คุณต้องการทำ
- หากคุณมีปัญหาหรือคำถามเกี่ยวกับการดาวน์โหลดสิทธิ์การใช้งาน โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ eSupport_-_Ops@lenovo.com

---

การติดตั้งสิทธิ์การใช้งานแบบเปิดใช้งานครบทุกฟังก์ชันแบบโดยใช้เว็บอินเทอร์เฟซ XClarity Administrator

หาก XClarity Administrator มีการเข้าถึงอินเทอร์เน็ต คุณสามารถใช้เว็บอินเทอร์เฟซ XClarity Administrator เพื่อแลกและรับสิทธิ์การใช้งานสำหรับการอนุญาตที่มีอยู่ แล้วนำเข้าและติดตั้งสิทธิ์การใช้งานที่แลกได้

ก่อนจะเริ่มต้น

โปรดติดต่อตัวแทน Lenovo หรือคู่ค้าธุรกิจที่ได้รับอนุญาตเพื่อซื้อสิทธิ์การใช้งาน Lenovo XClarity Pro ตามฟังก์ชันที่คุณต้องการเปิดใช้งานและจำนวนอุปกรณ์ที่คุณต้องการจัดการ หลังจากที่ซื้อสิทธิ์การใช้งานแล้ว จะมีการส่งรหัสการ

อนุญาตไปให้คุณทางอีเมล*หลักฐานยืนยันสิทธิ์การใช้งานอิเล็กทรอนิกส์* รหัสการอนุญาตเป็นสตริงตัวอักษรและตัวเลข 22 อักขระ ซึ่งคุณต้องใช้เพื่อแลกและติดตั้งสิทธิ์การใช้งาน หากคุณไม่ได้รับอีเมลและคุณได้สั่งซื้อสิทธิ์การใช้งานผ่านทางคู่ค้าธุรกิจแล้ว โปรดติดต่อคู่ค้าธุรกิจของคุณเพื่อขอรหัสการอนุญาต

นอกจากนี้คุณยังสามารถเรียกดูรหัสการอนุญาตจาก เว็บพอร์ทัลคุณลักษณะตามต้องการ โดยคลิกที่ **เรียกดูรหัสการอนุญาต**

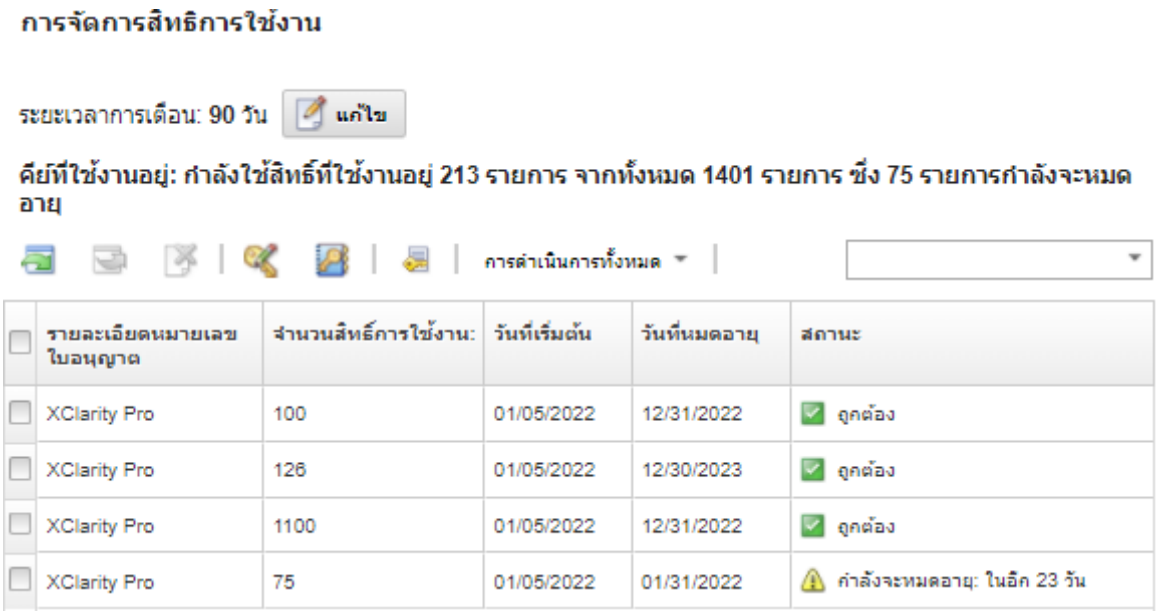
ขั้นตอน

หากต้องการติดตั้งสิทธิ์การใช้งาน Lenovo XClarity Pro ในเซิร์ฟเวอร์การจัดการ ให้ทำตามขั้นตอนใดขั้นตอนหนึ่งต่อไปนี้

- **การแลกและติดตั้งสิทธิ์การใช้งานที่เหลือทั้งหมดหรือสิทธิ์การใช้งานชุดย่อยจากรหัสการอนุญาตเดียว**

  คุณสามารถแลกสิทธิ์ใช้งานทั้งหมดหรือสิทธิ์ใช้งานชุดย่อยสำหรับรหัสการอนุญาตเดียวเพื่อสร้างรหัสเปิดใช้งานสิทธิ์การใช้งาน ซึ่งเป็นไฟล์ที่มีข้อมูลเกี่ยวกับสิทธิ์การใช้งานที่แลกแต่ละรายการ จากนั้นคุณสามารถติดตั้งสิทธิ์การใช้งานที่แลกโดยใช้ไฟล์คีย์เปิดใช้งานสิทธิ์การใช้งานนั้น

  1. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ ➔ สิทธิ์การใช้งาน** เพื่อแสดงหน้า การจัดการสิทธิ์การใช้งาน

  2. คลิกไอคอน **ร้องขอคีย์เปิดใช้งาน** ( ) เพื่อแสดงกล่องโต้ตอบ ร้องขอคีย์เปิดใช้งาน
  3. คลิก **รหัสการอนุญาตเดียว**
  4. ป้อนรหัสการอนุญาต 22 อักขระ และคลิก **ค้นหา** เพื่อดึงข้อมูลเกี่ยวกับสิทธิ์การใช้งานที่ซื้อไว้สำหรับรหัสการอนุญาตที่ระบุจากเว็บไซต์คุณลักษณะตามต้องการ

     หากระบบไม่ยอมรับรหัสการอนุญาตที่คุณได้รับ โปรดติดต่อฝ่ายสนับสนุนของ Lenovo

5. ป้อนหมายเลขลูกค้าของ Lenovo 10 หลักในฟิลด์ **หมายเลขลูกค้า** Lenovo
6. ป้อนจำนวนสิทธิ์การใช้งานที่คุณต้องการแลกใช้ในฟิลด์ **จำนวนการแลกใช้** แล้วคลิก **ดำเนินการต่อ**

   เพื่อแลกใช้สิทธิ์การใช้งานทั้งหมดที่ใช้ได้ในรหัสการอนุญาตนี้ ให้ตรวจสอบว่าจำนวนในฟิลด์ **สิทธิ์การใช้งานที่ใช้ได้** ตรงกัน

   หากต้องการแลกใช้สิทธิ์การใช้งานชุดย่อยที่ใช้ได้ คุณสามารถแลกสิทธิ์การใช้งานที่เหลือในภายหลังโดยใช้รหัสการอนุญาตเดียวกัน

   เคล็ดลับ: XClarity Administrator แต่ละเครื่องรองรับอุปกรณ์ที่มีการจัดการสูงสุด 1,000 เครื่อง ดังนั้น ด้วยคีย์เปิดใช้งานสิทธิ์การใช้งานเดียวที่คุณติดตั้งในอินสแตนซ์ XClarity Administrator ไม่ควรมีสิทธิ์การใช้งานมากกว่า 1,000 สิทธิ์
7. ตรวจสอบข้อมูลการติดต่อเพื่อความถูกต้องและทำการแก้ไขหากจำเป็น
8. คลิก **ส่งคำขอ** เพื่อแลกสิทธิ์การใช้งานและสร้างคีย์เปิดใช้งานสิทธิ์การใช้งาน
9. เลือกคีย์เปิดใช้งานสิทธิ์การใช้งานที่มีสิทธิ์การใช้งานที่จะติดตั้ง
10. คลิก **ติดตั้ง** เพื่อติดตั้งสิทธิ์การใช้งานในเซิร์ฟเวอร์การจัดการ
11. คลิก **ปิด**

- **แลกและติดตั้งสิทธิ์การใช้งานที่เหลือทั้งหมดจากรหัสการอนุญาตหลายรหัส**

  คุณสามารถแลกและติดตั้งสิทธิ์การใช้งานที่เหลือทั้งหมดจากรหัสการอนุญาตหลายรหัส ระบบจะสร้างคีย์เปิดใช้งานสิทธิ์การใช้งานขึ้นสำหรับรหัสการอนุญาตแต่ละรหัส จากนั้นคุณสามารถติดตั้งสิทธิ์การใช้งานที่แลกโดยใช้คีย์เปิดใช้งานสิทธิ์การใช้งาน ต้องระบุรหัสการอนุญาตในไฟล์รูปแบบ CSV โดยใช้เทมเพลทที่มีให้

  1. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ ➔ สิทธิ์การใช้งาน** เพื่อแสดงหน้า การจัดการสิทธิ์การใช้งาน
  2. คลิกไอคอน **ร้องขอคีย์เปิดใช้งาน** (🔑) เพื่อแสดงกล่องโต้ตอบ ร้องขอคีย์เปิดใช้งาน
  3. คลิก **รหัสการอนุญาตหลายรหัส**
  4. คลิกลิงก์ **ดาวน์โหลดเทมเพลท** เพื่อเปิดไฟล์ Excel เพิ่มรหัสการอนุญาตแต่ละรหัสลงในไฟล์ และบันทึกไฟล์ในรูปแบบ CSV ลงในระบบภายในของคุณ
  5. คลิก **เรียกดู** เพื่อค้นหาและเลือกไฟล์ CSV สำหรับรหัสอนุญาต แล้วคลิก **ค้นหา** เพื่อดึงข้อมูลเกี่ยวกับรหัสการอนุญาตจากเว็บไซต์บริการสนับสนุนของ Lenovo
  6. ตรวจสอบข้อมูลเกี่ยวกับสิทธิ์การใช้งานที่ซื้อและรหัสเปิดใช้งานสิทธิ์การใช้งานที่ใช้ได้ซึ่งเชื่อมโยงกับรหัสการอนุญาตแต่ละรหัส
  7. ป้อนหมายเลขลูกค้าของ Lenovo 10 หลักในฟิลด์ **หมายเลขลูกค้า** Lenovo
  8. ตรวจสอบข้อมูลการติดต่อเพื่อความถูกต้องและทำการแก้ไขหากจำเป็น แล้วคลิก **ดำเนินการต่อ**

9. เลือก **ใช่ ฉันต้องการแลกรหัสการอนุญาตที่ใช้ได้ทั้งหมด** แล้วคลิก **ส่งคำขอ** เพื่อสร้างคีย์เปิดใช้งานสิทธิ์การใช้งาน
10. เลือกคีย์เปิดใช้งานสิทธิ์การใช้งานที่คุณต้องการติดตั้ง
11. คลิก **ติดตั้ง** เพื่อติดตั้งคีย์เปิดใช้งานสิทธิ์การใช้งานในเซิร์ฟเวอร์การจัดการ
12. คลิก **ปิด**

- **ดึงข้อมูลและติดตั้งสิทธิ์การใช้งานที่แลก**

  คุณสามารถดาวน์โหลดคีย์เปิดใช้งานสิทธิ์การใช้งานไปยังระบบภายในจากอินสแตนซ์ XClarity Administrator ที่มีสิทธิ์เข้าถึง เว็บพอร์ทัลคุณลักษณะตามต้องการ แล้วนำเข้าและติดตั้งคีย์เปิดใช้งานสิทธิ์การใช้งานเหล่านั้นในอินสแตนซ์ XClarity Administrator การดำเนินการนี้มีประโยชน์ในกรณีที่คุณต้องการติดตั้งสิทธิ์การใช้งานบนอินสแตนซ์ XClarity Administrator ที่ไม่สามารถเข้าถึงอินเทอร์เน็ต หรือเมื่อคุณทำการติดตั้ง XClarity Administrator ใหม่และต้องกู้คืนสิทธิ์การใช้งานที่ติดตั้ง

  1. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ ➔ สิทธิ์การใช้งาน** เพื่อแสดงหน้า การจัดการสิทธิ์การใช้งาน
  2. คลิกไอคอน **เรียกดูประวัติ** () เพื่อแสดงกล่องโต้ตอบเรียกดูประวัติ
  3. ป้อนหมายเลขลูกค้า Lenovo หรือรหัสการอนุญาต 22 อักขระ
  4. คลิก **ค้นหา** เพื่อดึงข้อมูลเกี่ยวกับสิทธิ์การใช้งานที่แลกและพร้อมใช้งาน

     หากระบบไม่ยอมรับรหัสการอนุญาตที่คุณได้รับ โปรดติดต่อฝ่ายสนับสนุนของ Lenovo
  5. เลือกไฟล์คีย์สิทธิ์การใช้งานที่คุณต้องการติดตั้ง
  6. คลิก **ติดตั้ง** เพื่อติดตั้งคีย์เปิดใช้งานสิทธิ์การใช้งานใน XClarity Administrator
  7. คลิก **ปิด**

- **นำเข้าและติดตั้งสิทธิ์การใช้งานที่แลกบนอินสแตนซ์ XClarity Administrator อื่น**

  หากคุณแลกสิทธิ์การใช้งานโดยใช้อินสแตนซ์ XClarity Administrator หนึ่งและต้องการติดตั้งสิทธิ์การใช้งานนั้นบนอีกอินสแตนซ์ XClarity Administrator หรือหากเกิดเงื่อนไขข้อผิดพลาดที่ทำให้คุณต้องกู้คืนสิทธิ์การใช้งานที่ติดตั้งไว้ คุณสามารถนำเข้าไฟล์คีย์สิทธิ์การใช้งานจากระบบภายในไปยังอินสแตนซ์ XClarity Administrator อื่นได้

  1. จากอินสแตนซ์ XClarity Administrator ที่มีสิทธิ์เข้าถึง เว็บพอร์ทัลคุณลักษณะตามต้องการ ให้ดึงข้อมูลคีย์เปิดใช้งานสิทธิ์การใช้งานจาก เว็บพอร์ทัลคุณลักษณะตามต้องการ แล้วบันทึกคีย์เปิดใช้งานสิทธิ์การใช้งานเป็นไฟล์ลงในระบบภายในของคุณ

     a. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ ➔ สิทธิ์การใช้งาน** เพื่อแสดงหน้าการจัดการสิทธิ์การใช้งาน

     b. คลิกไอคอน **เรียกดูประวัติ** () เพื่อแสดงกล่องโต้ตอบเรียกดูประวัติ

     c. ป้อนรหัสการอนุญาต 22 อักขระ

d. คลิก **ค้นหา** เพื่อดึงข้อมูลเกี่ยวกับสิทธิ์การใช้งานที่แลกและพร้อมใช้งานสำหรับรหัสการอนุญาตดังกล่าว

   หากระบบไม่ยอมรับรหัสการอนุญาตที่คุณได้รับ โปรดติดต่อฝ่ายสนับสนุนของ Lenovo

e. เลือกไฟล์คีย์เปิดใช้งานสิทธิ์การใช้งานที่คุณต้องการติดตั้ง

f. คลิก **ดาวน์โหลด** เพื่อบันทึกไฟล์คีย์สิทธิ์การใช้งานไปยังระบบภายใน

2. จากอินสแตนซ์ XClarity Administrator ที่คุณต้องการติดตั้งคีย์เปิดใช้งานสิทธิ์การใช้งาน:

   a. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ ➔ สิทธิ์การใช้งาน** เพื่อแสดงหน้าการจัดการสิทธิ์การใช้งาน

   b. คลิกไอคอน **นำเข้าและนำไปใช้** () เพื่อนำเข้าและติดตั้งสิทธิ์การใช้งาน

   c. คลิก **เรียกดู** เพื่อเลือกคีย์เปิดใช้งานสิทธิ์การใช้งานสำหรับสิทธิ์การใช้งานที่คุณต้องการติดตั้ง

      หากต้องการนำเข้าคีย์เปิดใช้งานสิทธิ์การใช้งานหลายรายการ ให้บีบอัดไฟล์ .KEY ลงในไฟล์ ZIP และเลือกไฟล์ ZIP เพื่อนำเข้า

   d. คลิก **ยอมรับสิทธิ์การใช้งาน** เพื่อนำเข้าและนำสิทธิ์การใช้งานไปใช้

      เมื่อติดตั้งเสร็จสมบูรณ์แล้ว คีย์เปิดใช้งานสิทธิ์การใช้งานจะแสดงอยู่ในตารางที่มีจำนวนสิทธิ์การใช้งานที่ติดตั้งและระยะเวลาการเปิดใช้งาน (วันที่เริ่มต้นและวันหมดอายุ)

หลังจากดำเนินการเสร็จ

จากหน้า สิทธิ์การใช้งาน คุณสามารถดำเนินการต่อไปนี้ได้

- ดาวน์โหลดคีย์เปิดใช้งานสิทธิ์การใช้งานที่เฉพาะเจาะจงอย่างน้อยหนึ่งรายการไปยังระบบภายในโดยคลิกไอคอน **ส่งออก** ()

  หมายเหตุ: เมื่อคุณส่งออกคีย์เปิดใช้งานสิทธิ์การใช้งานหลายรายการ ไฟล์จะถูกดาวน์โหลดเป็นไฟล์ ZIP รายการเดียว

- ลบคีย์เปิดใช้งานสิทธิ์การใช้งานที่ระบุ โดยคลิกไอคอน **ลบ** ()
- กำหนดค่าระยะเวลาเตือนสิทธิ์การใช้งานโดยคลิกปุ่ม **แก้ไข** ที่ด้านบนของหน้า ระยะเวลาเตือนสิทธิ์การใช้งานคือจำนวนวันก่อนที่สิทธิ์การใช้งานจะหมดอายุเมื่อ XClarity Administrator ทริกเกอร์คำเตือน

การขอรับความช่วยเหลือ

- หากคุณประสบกับปัญหาและใช้บริการจากคู่ค้าธุรกิจ โปรดติดตั้งกับคู่ค้าธุรกิจของคุณเพื่อตรวจสอบความถูกต้องของธุรกรรมและสิทธิ์การใช้งาน

- หากคุณไม่ได้รับหลักฐานยืนยันสิทธิ์การใช้งานอิเล็กทรอนิกส์ รหัสการอนุญาต หรือคีย์เปิดใช้งาน หรือหากมีการส่งให้ผิดคน โปรดติดต่อตัวแทนในภูมิภาคตามที่ตั้งประเทศของคุณ
  - ESDNA@lenovo.com (ประเทศในอเมริกาเหนือ)
  - ESDAP@lenovo.com (ประเทศในเอเชียแปซิฟิก)
  - ESDEMEA@lenovo.com (ประเทศในยุโรป ตะวันออกกลาง และเอเชีย)
  - ESDLA@lenovo.com (ประเทศในลาตินอเมริกา)
  - ESDChina@Lenovo.com (ประเทศจีน)
- หากข้อมูลเกี่ยวกับการให้สิทธิ์การใช้งานของฉันไม่ถูกต้อง โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ SW_override@lenovo.com พร้อมข้อมูลต่อไปนี้:
  - หมายเลขใบสั่ง
  - ข้อมูลติดต่อของคุณ รวมถึงที่อยู่อีเมล
  - ที่อยู่จริงของคุณ
  - การเปลี่ยนแปลงที่คุณต้องการทำ
- หากคุณมีปัญหาหรือคำถามเกี่ยวกับการดาวน์โหลดสิทธิ์การใช้งาน โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ eSupport_-_Ops@lenovo.com

---

การติดตั้งสิทธิ์การใช้งานแบบเปิดใช้งานครบทุกฟังก์ชันแบบโดยใช้เว็บพอร์ทัลคุณลักษณะตามต้องการ

หาก XClarity Administrator *ไม่*สามารถเข้าถึงอินเทอร์เน็ตได้ คุณสามารถแลกและรับสิทธิ์การใช้งานสำหรับรหัสการอนุญาตที่มีอยู่โดยใช้ เว็บพอร์ทัลคุณลักษณะตามต้องการ จากระบบอื่นที่มีการเข้าถึงเครือข่ายกับ XClarity Administrator จากนั้นคุณสามารถใช้เว็บอินเทอร์เฟซ XClarity Administrator เพื่อนำเข้าและติดตั้งสิทธิ์การใช้งานที่แลกมาได้

ขั้นตอน

หากต้องการติดตั้งสิทธิ์การใช้งาน Lenovo XClarity Pro ในเซิร์ฟเวอร์การจัดการ ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ซื้อสิทธิ์การใช้งาน Lenovo XClarity Pro ให้กับอุปกรณ์ที่มีการจัดการแต่ละเครื่อง

โปรดติดต่อตัวแทน Lenovo หรือคู่ค้าธุรกิจที่ได้รับอนุญาตเพื่อซื้อสิทธิ์การใช้งาน Lenovo XClarity Pro ตามฟังก์ชันที่คุณต้องการเปิดใช้งานและจำนวนอุปกรณ์ที่คุณต้องการจัดการ หลังจากที่ซื้อสิทธิ์การใช้งานแล้ว จะมีการส่งรหัสการอนุญาตไปให้คุณทางอีเมล*หลักฐานยืนยันสิทธิ์การใช้งานอิเล็กทรอนิกส์* รหัสการอนุญาตเป็นสตริงตัวอักษรและตัวเลข 22 อักขระ ซึ่งคุณต้องใช้เพื่อแลกและติดตั้งสิทธิ์การใช้งาน หากคุณไม่ได้รับอีเมลและคุณได้สั่งซื้อสิทธิ์การใช้งานผ่านทางคู่ค้าธุรกิจแล้ว โปรดติดต่อคู่ค้าธุรกิจของคุณเพื่อขอรหัสการอนุญาต

นอกจากนี้คุณยังสามารถเรียกดูรหัสการอนุญาตจาก เว็บพอร์ทัลคุณลักษณะตามต้องการ โดยคลิกที่ **เรียกดูรหัสการอนุญาต**

ขั้นตอนที่ 2. แลกสิทธิ์การใช้งานทั้งหมดหรือบางส่วนโดยใช้รหัสการอนุญาต เมื่อแลกสิทธิ์การใช้งานแล้ว ระบบจะสร้างไฟล์คีย์เปิดใช้งานสิทธิ์การใช้งานขึ้น

1. เปิด เว็บพอร์ทัลคุณลักษณะตามต้องการ จากเว็บเบราเซอร์ แล้วเข้าสู่ระบบพอร์ทัลโดยใช้ที่อยู่อีเมลของคุณเป็นรหัสผู้ใช้
2. คลิก **ร้องขอคีย์การเปิดใช้าน**
3. เลือก **ป้อนรหัสการอนุญาตแบบครั้งเดียว**
4. ป้อนรหัสการอนุญาต 22 อักขระ แล้วคลิก **ดำเนินการต่อ**
5. ป้อนหมายเลขลูกค้าของ Lenovo ในฟิลด์ **หมายเลขลูกค้า** Lenovo
6. ป้อนจำนวนสิทธิ์การใช้งานที่คุณต้องการแลกใช้ในฟิลด์ **จำนวนการแลกใช้** แล้วคลิก **ดำเนินการต่อ**

   เพื่อแลกใช้สิทธิ์การใช้งานทั้งหมดที่ใช้ได้ในรหัสการอนุญาตนี้ ให้ตรวจสอบว่าจำนวนในฟิลด์ **สิทธิ์การใช้งานที่ใช้ได้** ตรงกัน

   หากต้องการแลกใช้สิทธิ์การใช้งานชุดย่อยที่ใช้ได้ คุณสามารถแลกสิทธิ์การใช้งานที่เหลือในคีย์เปิดใช้งานสิทธิ์การใช้งานอื่นโดยใช้รหัสการอนุญาตเดียวกัน

   เคล็ดลับ: XClarity Administrator แต่ละเครื่องรองรับอุปกรณ์ที่มีการจัดการสูงสุด 1,000 เครื่อง ดังนั้น ด้วยคีย์เปิดใช้งานสิทธิ์การใช้งานเดียวที่คุณติดตั้งในอินสแตนซ์ XClarity Administrator ไม่ควรมีสิทธิ์การใช้งานมากกว่า 1,000 สิทธิ์
7. ทำตามข้อความแจ้งเตือนเพื่อป้อนรายละเอียดผลิตภัณฑ์และข้อมูลการติดต่อ แล้วคลิก **ดำเนินการต่อ** เพื่อสร้างคีย์เปิดใช้งานสิทธิ์การใช้งาน
8. เลือกผู้รับเพิ่มเติมโดยเฉพาะเพื่อรับคีย์เปิดใช้งานสิทธิ์การใช้งานด้วยก็ได้
9. คลิก **ส่ง** เพื่อส่งคีย์เปิดใช้งานสิทธิ์การใช้งาน

   บุคคลที่ได้รับมอบหมายคำสั่งซื้อและผู้รับเพิ่มเติมจะได้รับอีเมลพร้อมคีย์เปิดใช้งานสิทธิ์การใช้งาน คีย์คือไฟล์ในรูปแบบ .KEY

   หมายเหตุ: นอกจากนี้คุณยังสามารถดาวน์โหลดคีย์เปิดใช้งานสิทธิ์การใช้งาน (แยกกันหรือเป็นชุด) ได้จาก เว็บพอร์ทัลคุณลักษณะตามต้องการ โดยคลิก **เรียกดูประวัติ** และใช้หมายเลขลูกค้า Lenovo เพื่อค้นหาโหลดคีย์เปิดใช้งานสิทธิ์การใช้งาน จากนั้นดาวน์โหลดคีย์ทั้งหมดหรือคีย์ชุดย่อย แล้วคลิก **อีเมล** เพื่อส่งคีย์ไปให้คุณทางอีเมลหรือคลิก **ดาวน์โหลด** เพื่อดาวน์โหลดคีย์ไปยังระบบภายใน

ขั้นตอนที่ 3. นำเข้าและติดตั้งสิทธิ์การใช้งานใน XClarity Administrator

1. จากแถบเมนู XClarity Administrator ให้คลิก **การดูแลระบบ** ➔ **สิทธิ์การใช้งาน** เพื่อแสดงหน้า การจัดการสิทธิ์การใช้งาน
2. คลิกไอคอน **นำเข้าและนำไปใช้** () เพื่อติดตั้งสิทธิ์การใช้งาน
3. คลิก **เรียกดู** เพื่อเลือกไฟล์คีย์เปิดใช้งานสิทธิ์การใช้งานสำหรับสิทธิ์การใช้งานที่คุณต้องการติดตั้ง

   เคล็ดลับ: หากต้องการนำเข้าคีย์เปิดใช้งานสิทธิ์การใช้งานหลายรายการ ให้บีบอัดไฟล์ .KEY ลงในไฟล์ ZIP และเลือกไฟล์ ZIP เพื่อนำเข้า
4. คลิก **ยอมรับสิทธิ์การใช้งาน** เพื่อนำเข้าและนำสิทธิ์การใช้งานไปใช้

   เมื่อติดตั้งเสร็จสมบูรณ์แล้ว คีย์เปิดใช้งานสิทธิ์การใช้งานจะแสดงอยู่ในตารางที่มีจำนวนสิทธิ์การใช้งานที่ติดตั้งและระยะเวลาการเปิดใช้งาน (วันที่เริ่มต้นและวันหมดอายุ)

หลังจากดำเนินการเสร็จ

จากหน้า สิทธิ์การใช้งาน คุณสามารถดำเนินการต่อไปนี้ได้

- ดาวน์โหลดคีย์เปิดใช้งานสิทธิ์การใช้งานที่เฉพาะเจาะจงอย่างน้อยหนึ่งรายการไปยังระบบภายในโดยคลิกไอคอน **ส่งออก** ()

  หมายเหตุ: เมื่อคุณส่งออกคีย์เปิดใช้งานสิทธิ์การใช้งานหลายรายการ ไฟล์จะถูกดาวน์โหลดเป็นไฟล์ ZIP รายการเดียว
- ลบคีย์เปิดใช้งานสิทธิ์การใช้งานที่ระบุ โดยคลิกไอคอน **ลบ** ()
- กำหนดค่าระยะเวลาเตือนสิทธิ์การใช้งานโดยคลิกปุ่ม **แก้ไข** ที่ด้านบนของหน้า ระยะเวลาเตือนสิทธิ์การใช้งานคือจำนวนวันก่อนที่สิทธิ์การใช้งานจะหมดอายุเมื่อ XClarity Administrator ทริกเกอร์คำเตือน

การขอรับความช่วยเหลือ

- หากคุณประสบกับปัญหาและใช้บริการจากคู่ค้าธุรกิจ โปรดติดตั้งกับคู่ค้าธุรกิจของคุณเพื่อตรวจสอบความถูกต้องของธุรกรรมและสิทธิ์การใช้งาน
- หากคุณไม่ได้รับหลักฐานยืนยันสิทธิ์การใช้งานอิเล็กทรอนิกส์ รหัสการอนุญาต หรือคีย์เปิดใช้งาน หรือหากมีการส่งให้ผิดคน โปรดติดต่อตัวแทนในภูมิภาคตามที่ตั้งประเทศของคุณ
  - ESDNA@lenovo.com (ประเทศในอเมริกาเหนือ)
  - ESDAP@lenovo.com (ประเทศในเอเชียแปซิฟิก)
  - ESDEMEA@lenovo.com (ประเทศในยุโรป ตะวันออกกลาง และเอเชีย)
  - ESDLA@lenovo.com (ประเทศในลาตินอเมริกา)
  - ESDChina@Lenovo.com (ประเทศจีน)

- หากข้อมูลเกี่ยวกับการให้สิทธิ์การใช้งานของฉันไม่ถูกต้อง โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ SW_override@lenovo.com พร้อมข้อมูลต่อไปนี้:
  - หมายเลขใบสั่ง
  - ข้อมูลติดต่อของคุณ รวมถึงที่อยู่อีเมล
  - ที่อยู่จริงของคุณ
  - การเปลี่ยนแปลงที่คุณต้องการทำ
- หากคุณมีปัญหาหรือคำถามเกี่ยวกับการดาวน์โหลดสิทธิ์การใช้งาน โปรดติดต่อฝ่ายสนับสนุนของ Lenovo ที่ eSupport_-_Ops@lenovo.com

บทที่ 7. การอัปเดต XClarity Administrator เป็น

เมื่อใช้ Lenovo XClarity Administrator เป็นคอนเทนเนอร์ ให้ใช้ขั้นตอนการอัปเดตนี้ในการติดตั้งซอฟต์แวร์ล่าสุดเป็นคอนเทนเนอร์ใหม่ และผูกโวลุ่มของคอนเทนเนอร์เดิมกับคอนเทนเนอร์ใหม่

ก่อนจะเริ่มต้น

คุณสามารถอัปเดต XClarity Administrator v4.0 หรือใหม่กว่าได้จากอินสแตนซ์ XClarity Administrator v3.0 หรือใหม่กว่าเท่านั้น หากคุณใช้ XClarity Administrator เวอร์ชันที่เก่ากว่า v3.0 คุณต้องอัปเกรดเป็น v3.0 หรือใหม่กว่าก่อนที่จะอัปเกรดเป็น v4.0

หากต้องการจัดการอินสแตนซ์ XClarity Administrator v4.0 หรือใหม่กว่าโดยใช้ Lenovo XClarity Orchestrator จะต้องใช้ XClarity Orchestrator v2.0 หรือใหม่กว่า หากคุณอัปเดตเป็น XClarity Administrator v4.0 หรือใหม่กว่า ตรวจสอบให้แน่ใจว่า XClarity Orchestrator เป็น v2.0 หรือใหม่กว่า

เกี่ยวกับงานนี้

ไฟล์ `docker-compose.yml` ใช้ตัวแปรสภาพแวดล้อมต่อไปนี้ ซึ่งคุณตั้งค่าไว้ระหว่างการติดตั้งคอนเทนเนอร์*เดิม* คอนเทนเนอร์ใหม่จะใช้ตัวแปรสภาพแวดล้อมเหล่านี้ด้วย

- CONTAINER_NAME ชื่อคอนเทนเนอร์ที่ไม่ซ้ำกัน ใช้เพื่อสร้างโวลุ่ม Docker สำหรับแต่ละอินสแตนซ์ XClarity Administrator (ตัวอย่างเช่น `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator ใช้ชื่อคอนเทนเนอร์เพื่อสร้างโวลุ่มสำหรับคอนเทนเนอร์ หากคุณใช้ชื่อคอนเทนเนอร์เดียวกันสำหรับคอนเทนเนอร์ใหม่ อินสแตนซ์ XClarity Administrator ใหม่จะใช้โวลุ่มเดียวกัน ดังนั้นจึงมีสิทธิ์เข้าถึงข้อมูลและการตั้งค่าระบบเดียวกันกับอินสแตนซ์ XClarity Administrator เดิม (คอนเทนเนอร์)

  หากคุณเปลี่ยนชื่อคอนเทนเนอร์ จะมีการสร้างโวลุ่มใหม่สำหรับคอนเทนเนอร์นั้น อินสแตนซ์ XClarity Administrator ใหม่จะไม่มีสิทธิ์เข้าถึงข้อมูลและการตั้งค่าระบบเดียวกันกับอินสแตนซ์ XClarity Administrator เดิม (คอนเทนเนอร์) หากคุณจำเป็นต้องเปลี่ยนชื่อคอนเทนเนอร์หรือที่อยู่ IP ให้สำรองข้อมูลและการตั้งค่าระบบสำหรับอินสแตนซ์ XClarity Administrator เดิมก่อนที่จะติดตั้งคอนเทนเนอร์ใหม่ แล้วใช้ข้อมูลสำรองนั้นเพื่อกู้คืนข้อมูลระบบและการตั้งค่าในคอนเทนเนอร์ใหม่
- ADDRESS ที่อยู่ IPv4 หรือ IPv6 แบบคงที่สำหรับคอนเทนเนอร์ (ตัวอย่างเช่น `ADDRESS=192.0.2.0`)

  การเปลี่ยนที่อยู่ IP ของ XClarity Administrator หลังจากจัดการอุปกรณ์อาจทำให้อุปกรณ์อยู่ในสถานะออฟไลน์ใน XClarity Administrator ตรวจสอบให้แน่ใจว่าอุปกรณ์ทั้งหมดไม่ได้รับการจัดการก่อนที่จะเปลี่ยนที่อยู่ IP

- BACKUP_MOUNT และ FIRMWARE_MOUNT (ไม่บังคับ) พาธสำหรับการแชร์ระยะไกลที่สามารถใช้เพื่อเก็บข้อมูลสำรองของ XClarity Administrator หรือใช้เป็นที่เก็บข้อมูลระยะไกลสำหรับการอัปเดตเฟิร์มแวร์ พาธนี้ต้องเป็น `/mnt/backup_share` และ `/mnt/fw_share` ตามลำดับ

หมายเหตุ: XClarity Administrator *ไม่ได้*รันเป็นคอนเทนเนอร์ที่มีสิทธิ์

ขั้นตอน

หากต้องการอัปเดตคอนเทนเนอร์ XClarity Administrator ให้ทำตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ดาวน์โหลดอิมเมจคอนเทนเนอร์ XClarity Administrator จาก เว็บเพจการดาวน์โหลด XClarity Administrator ไปยังเวิร์กสเตชันไคลเอ็นต์ เข้าสู่ระบบเว็บไซต์ แล้วใช้คีย์การเข้าถึงที่กำหนดให้คุณใช้ดาวน์โหลดอิมเมจ

ขั้นตอนที่ 2. นำเข้าอิมเมจคอนเทนเนอร์ XClarity Administrator ลงในโฮสต์ Docker โดยการเรียกใช้คำสั่งต่อไปนี้
```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```

ขั้นตอนที่ 3. แก้ไขไฟล์ **docker-compose.yml** เดียวกันกับที่ใช้สำหรับคอนเทนเนอร์เดิม อัปเดตคุณสมบัติของอิจเมจที่ด้านบนของไฟล์เพื่อชี้ไปยังอิมเมจ Docker ใหม่จากขั้นตอนที่ 2 คุณสามารถเปลี่ยนแท็กอิมเมจได้ด้วยคำสั่ง `docker tag`

ต่อไปนี้แสดงตัวอย่างไฟล์ yml ที่เปิดใช้งาน IPv6

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
```

```
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

ขั้นตอนที่ 4. ปิดคอนเทนเนอร์*เดิม* โดยใช้คำสั่งต่อไปนี้

```
docker-compose -p ${CONTAINER_NAME} down
```

ขั้นตอนที่ 5. ปรับใช้อิมเมจใน Docker *ใหม่*โดยการเรียกใช้คำสั่งต่อไปนี้ โดยที่ *<ENV_FILENAME>* คือชื่อของไฟล์ตัวแปรสภาพแวดล้อม

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

บทที่ 8. การถอนการติดตั้ง XClarity Administrator

ให้ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อถอนการติดตั้งอุปกรณ์เสมือน Lenovo XClarity Administrator หรือคอนเทนเนอร์

ขั้นตอน

ในการถอนการติดตั้งอุปกรณ์เสมือนของ XClarity Administrator ให้ดำเนินการตามขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. ถอนการจัดการอุปกรณ์ทั้งหมดที่มีการจัดการโดย XClarity Administrator (ดู การจัดการตัวเครื่อง, การจัดการเซิร์ฟเวอร์ และ การจัดการสวิตช์ ในเอกสารแบบออนไลน์ของ XClarity Administrator)

ขั้นตอนที่ 2. ถอนการติดตั้ง XClarity Administrator โดยขึ้นอยู่กับระบบปฏิบัติการ:

- Docker-composeเรียกใช้คำสั่งต่อไปนี้เพื่อหยุดคอนเทนเนอร์และลบเครือข่ายและโวลุ่ม
  `docker-compose down -v`
- CentOS, Red Hat, Rocky และ Ubuntu
  1. เชื่อมต่อกับโฮสต์ใช้โปรแกรมจัดการเครื่องเสมือน
  2. คลิกขวาที่เครื่องเสมือน และคลิก **ปิดเครื่อง ➔ บังคับปิด**
  3. คลิกขวาที่เครื่องเสมือนอีกครั้ง และเลือก **ลบ** กล่องโต้ตอบ ยืนยันการลบ จะปรากฏขึ้น
  4. เลือกช่องทำเครื่องหมายทั้งหมด แล้วคลิก **ลบ**
- ESXi
  1. เชื่อมต่อกับโฮสต์ผ่าน VMware vSphere Client
  2. คลิกขวาที่เครื่องเสมือน และคลิก **เปิด/ปิดเครื่อง ➔ ปิดเครื่อง**
  3. คลิกขวาที่เครื่องเสมือนอีกครั้ง และเลือก **ลบออกจากดิสก์**
- Hyper-V
  1. จากแดชบอร์ดโปรแกรมจัดการเซิร์ฟเวอร์ ให้คลิก Hyper-V
  2. คลิกขวาที่เซิร์ฟเวอร์ แล้วคลิก **โปรแกรมจัดการ** Hyper-V
  3. คลิกขวาที่เครื่องเสมือน และคลิก **ปิดเครื่อง**
  4. คลิกขวาที่เครื่องเสมือนอีกครั้ง และเลือก **ลบ**