Lenovo

คู่มือผู้ใช้

XClarity Controller 2

หมายเหตุ: ก่อนใช้ข้อมูลนี้ โปรดอ่านข้อมูลทั่วไปใน ภาคผนวก B “คำประกาศ” บนหน้าที่ 303

ฉบับตีพิมพ์ครั้งที่หนึ่ง (พฤษภาคม 2021)

สารบัญ

บทที่ 1. ข้อมูลเบื้องต้น

Lenovo XClarity Controller 2 (XCC2) คือระบบควบคุมการจัดการที่ทันสมัย ซึ่งแทนที่ตัวควบคุมการจัดการแผงวงจรฐาน (BMC) สำหรับเซิร์ฟเวอร์ Lenovo ThinkSystem

ซึ่งสืบเนื่องมาจากโปรเซสเซอร์การบริการ Integrated Management Module II (IMM2) รุ่นที่สองที่รวมฟังก์ชันการทำงานของโปรเซสเซอร์การบริการ Super I/O ตัวควบคุมวิดีโอ และความสามารถในการแสดงตนระยะไกลไว้ในชิปตัวเดียวบนแผงระบบของเซิร์ฟเวอร์ โดยมอบคุณลักษณะดังต่อไปนี้:

- ตัวเลือกในการเชื่อมต่ออีเทอร์เน็ตแบบเฉพาะหรือแบบที่ใช้ร่วมกันสำหรับการจัดการระบบ
- รองรับ HTML5
- รองรับการเข้าถึงผ่านทาง XClarity Mobile
- XClarity Provisioning Manager
- การกำหนดค่าระยะไกลที่ใช้ XClarity Essentials หรือ XClarity Controller CLI
- ช่วยให้แอปพลิเคชันและเครื่องมือสามารถเข้าถึง XClarity Controller ได้ทั้งจากภายในและระยะไกล
- ปรับปรุงคุณสมบัติ Remote Presence
- REST API (สคีมา Redfish) รองรับบริการและแอปพลิเคชันซอฟต์แวร์เกี่ยวกับเว็บเพิ่มเติม

  หมายเหตุ: ขณะนี้ XClarity Controller รองรับข้อกำหนด Redfish Scalable Platforms Management API Specification 1.0.2 และสคีมา 2016.2

หมายเหตุ:

- ในเว็บอินเทอร์เฟซของ XClarity Controller BMC จะใช้สำหรับอ้างอิงไปยัง XCC
- พอร์ตเครือข่ายแบบเฉพาะสำหรับการจัดการระบบอาจใช้ไม่ได้กับเซิร์ฟเวอร์ ThinkSystem บางตัว สำหรับเซิร์ฟเวอร์เหล่านี้ การเข้าถึง XClarity Controller จะทำได้ผ่านทางพอร์ตเครือข่ายที่ใช้ร่วมกับระบบปฏิบัติการเซิร์ฟเวอร์เท่านั้น
- สำหรับเซิร์ฟเวอร์ Flex นั้น Chassis Management Module (CMM) จะเป็นโมดูลการจัดการหลักสำหรับฟังก์ชันต่างๆ ในการจัดการระบบ การเข้าถึง XClarity Controller จะทำได้ผ่านทางพอร์ตเครือข่ายบน CMM

เอกสารนี้จะอธิบายวิธีใช้ฟังก์ชันต่างๆ ของ XClarity Controller ในเซิร์ฟเวอร์ ThinkSystem XClarity Controller ทำงานกับ XClarity Provisioning Manager และ UEFI เพื่อมอบความสามารถในการจัดการระบบให้กับเซิร์ฟเวอร์ ThinkSystem

ในการตรวจสอบการอัปเดตเฟิร์มแวร์ ให้ดำเนินการตามขั้นตอนต่อไปนี้

หมายเหตุ: เมื่อคุณเข้าถึง Support Portal เป็นครั้งแรก คุณต้องเลือกหมวดหมู่ผลิตภัณฑ์ กลุ่มผลิตภัณฑ์ และหมายเลขรุ่นสำหรับเซิร์ฟเวอร์ของคุณ ในครั้งต่อไปที่คุณเข้าใช้ Support Portal เว็บไซต์จะโหลดผลิตภัณฑ์ที่คุณเลือกไว้ในตอนแรกให้เลยล่วงหน้า และจะแสดงเฉพาะลิงก์สำหรับผลิตภัณฑ์ของคุณเท่านั้น หากต้องการเปลี่ยนหรือเพิ่มผลิตภัณฑ์ในรายการ ให้คลิกลิงก์ **จัดการรายการผลิตภัณฑ์ของฉัน** มีการเปลี่ยนแปลงข้อมูลเว็บไซต์เป็นระยะ ขั้นตอนในการระบุเฟิร์มแวร์และเอกสารอาจแตกต่างจากที่อธิบายไว้ในเอกสารนี้เล็กน้อย

1. ไปที่ http://datacentersupport.lenovo.com
2. ภายใต้ Support (**การสนับสนุน**) ให้เลือก Data Center (**ศูนย์ข้อมูล**)
3. เมื่อเนื้อหาโหลดขึ้นมาแล้ว ให้เลือก Servers (**เซิร์ฟเวอร์**)
4. ในส่วน Select Series (**เลือกซีรี่ย์**) ให้เลือกซีรี่ย์ฮาร์ดแวร์ของเซิร์ฟเวอร์ที่ต้องการก่อน ตามด้วย Select Sub-Series (**เลือกซีรี่ย์ย่อย**) เพื่อเลือกซีรี่ย์ย่อยของผลิตภัณฑ์เซิร์ฟเวอร์ และสุดท้ายในส่วน Select Machine Type (**เลือกประเภทเครื่อง**) ให้เลือกประเภทเครื่องที่ต้องการ

คุณลักษณะระดับ Standard และ Platinum ของ XClarity Controller

XClarity Controller มีคุณลักษณะต่างๆ ให้เลือกทั้งระดับ Standard และระดับ Platinum ดูข้อมูลเพิ่มเติมเกี่ยวกับระดับคุณลักษณะของ XClarity Controller ที่ติดตั้งในเซิร์ฟเวอร์ของคุณได้จากเอกสารประกอบการใช้งานเซิร์ฟเวอร์ ทุกระดับจะประกอบด้วยคุณลักษณะต่อไปนี้:

- การเข้าใช้งานและจัดการเซิร์ฟเวอร์จากระยะไกลได้ตลอดเวลา
- สามารถจัดการจากระยะไกลได้ไม่ว่าเซิร์ฟเวอร์นั้นจะมีสถานะได้รับการจัดการหรือไม่
- การควบคุมฮาร์ดแวร์และระบบปฏิบัติการได้จากระยะไกล

หมายเหตุ: คุณลักษณะบางอย่างอาจใช้ไม่ได้กับเซิร์ฟเวอร์ Flex System

ด้านล่างนี้คือรายการคุณลักษณะระดับมาตรฐานของ XClarity Controller

คุณลักษณะระดับมาตรฐานของ XClarity Controller

ด้านล่างนี้คือรายการคุณลักษณะระดับมาตรฐานของ XClarity Controller:

อินเทอร์เฟซการจัดการระดับมาตรฐานอุตสาหกรรม

- อินเทอร์เฟซ IPMI 2.0
- Redfish
- DCMI 1.5
- SNMPv3

อินเทอร์เฟซการจัดการอื่น ๆ

- เว็บ
- Legacy CLI
- USB แผงด้านหน้า - แผงตัวดำเนินการเสมือนผ่านอุปกรณ์เคลื่อนที่

การควบคุมการเปิดปิดเครื่อง/รีเซ็ต

- การเปิดเครื่อง
- ฮาร์ดชัตดาวน์/ซอฟต์ชัตดาวน์
- การควบคุมการเปิด/ปิดเครื่องตามกำหนดการ
- รีเซ็ตระบบ
- การควบคุมลำดับการบูต

บันทึกเหตุการณ์

- IPMI SEL
- บันทึกที่ผู้ใช้สามารถอ่านได้
- บันทึกการตรวจสอบ
- บันทึกขนาดเล็ก

การตรวจสอบสภาพแวดล้อม

- การตรวจสอบแบบไม่ต้องใช้ตัวแทน
- การตรวจสอบเซนเซอร์
- ตัวควบคุมพัดลม
- ตัวควบคุมไฟ LED
- ข้อผิดพลาดเกี่ยวกับชิปเซ็ต (Caterr, IERR, เป็นต้น...)
- การระบุสถานะของระบบ
- การตรวจสอบประสิทธิภาพ OOB สำหรับอะแดปเตอร์ I/O
- การแสดงและการส่งออกรายการอุปกรณ์

RAS

- NMI เสมือน

- การกู้คืนเฟิร์มแวร์อัตโนมัติ
- การเลื่อนระดับอัตโนมัติของเฟิร์มแวร์ที่สำรองข้อมูล
- POST Watchdog
- OS Loader Watchdog
- OS Watchdog
- การจับภาพหน้าจอสีน้ำเงิน (ความบกพร่องของระบบปฏิบัติการใน FFDC)
- เครื่องมือวินิจฉัยแบบฝังตัว
- Call Home

การกำหนดค่าเครือข่าย

- IPv4
- IPv6
- ที่อยู่ IP, ตัวพรางเครือข่ายย่อย, เกตเวย์
- โหมดการกำหนดที่อยู่ IP
- ชื่อโฮสต์
- ที่อยู่ MAC แบบตั้งโปรแกรมได้
- การเลือก MAC แบบคู่ (หากฮาร์ดแวร์เซิร์ฟเวอร์รองรับ)
- การกำหนดพอร์ตเครือข่ายใหม่
- การแท็ก VLAN

โปรโตคอลเครือข่าย

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- ไคลเอ็นต์ LDAP

- NTP
- SSDP
- LLDP

การแจ้งเตือน

- PET Traps
- SNMP TRAPs
- อีเมล
- เหตุการณ์ Redfish

Remote Presence

- ดิสก์ระยะไกลบนการ์ด (RDOC)

การเปลี่ยนเส้นทางแบบอนุกรม

- IPMI SOL
- การกำหนดค่าพอร์ตอนุกรม รวมถึงสิทธิ์และความเร็ว
- บัฟเฟอร์คอนโซลอนุกรม (120 วินาที)

การรักษาความปลอดภัย

- CRTM ของโปรเซสเซอร์ที่ไม่ใช่โฮสต์
- การอัปเดตเฟิร์มแวร์ที่ลงนามแบบดิจิตอล
- Role Based Access Control (RBAC)
- บัญชีผู้ใช้ภายใน
- บัญชีผู้ใช้ LDAP/AD
- การย้อนกลับของเฟิร์มแวร์ที่ปลอดภัย
- NIST SP 800–131a
- Chassis Intrusion Detection (หากฮาร์ดแวร์เซิร์ฟเวอร์รองรับ)
- เปิดใช้งานเฉพาะโปรโตคอลที่ปลอดภัยและเข้ารหัสเท่านั้น
- การบันทึกการตรวจสอบของการเปลี่ยนแปลงการกำหนดค่าและการดำเนินการบนเซิร์ฟเวอร์
- การตรวจสอบความถูกต้องของคีย์สาธารณะ (PK)

- รีไทร์/กำหนดวัตถุประสงค์ของระบบใหม่
- การสนับสนุน PFR
- FIPS 140–3
- โหมด Security และแดชบอร์ด Security
- การจัดเก็บรหัสผ่านที่ปลอดภัย

การจัดการพลังงาน

- มาตรวัดพลังงานแบบเรียลไทม์

Features on Demand

- ที่เก็บคีย์การเปิดใช้งาน

การใช้งานและการกำหนดค่า

- การค้นพบกลุ่มข้างเคียง
- การกำหนดค่าระยะไกล
- การส่งผ่านระบบปฏิบัติการ
- เครื่องมือการใช้งานและการกำหนดค่าแบบฝังตัวและชุดไดรเวอร์
- สำรองข้อมูลและคืนค่าการกำหนดค่า
- ขนาด RDOC แบบขยาย (พร้อมการ์ด MicroSD)
- โปรไฟล์ความร้อนที่กำหนดค่าได้

การอัปเดตเฟิร์มแวร์

- การอัปเดตแบบไม่ต้องใช้ตัวแทน
- การอัปเดตระยะไกล

คุณลักษณะระดับ Platinum ของ XClarity Controller

ด้านล่างนี้คือรายการคุณลักษณะระดับ Platinum ของ XClarity Controller:

คุณลักษณะระดับมาตรฐานของ XClarity Controller ทั้งหมด และ:

บันทึกเหตุการณ์

- บันทึกของการเปลี่ยนส่วนประกอบ

RAS

- Boot Capture
- การจับภาพวิดีโอขัดข้อง

การแจ้งเตือน

- Syslog

Remote Presence

- Remote KVM
- การติดตั้งของไฟล์ IO/IMG ไคลเอ็นต์ภายใน
- การควบคุมคุณภาพ/แบนด์วิดท์
- การทำงานร่วมกันบนคอนโซลเสมือน (ผู้ใช้ 6 ราย)
- การสนทนาบนคอนโซลเสมือน
- บันทึกวิดีโอ/เล่นซ้ำ
- การติดตั้งสื่อเสมือนของ ISO/IMG files http, Samba และ NFS ระยะไกล
- ไคลเอนต์ Java คอนโซลระยะไกล

การเปลี่ยนเส้นทางแบบอนุกรม

- การเปลี่ยนทิศทางอนุกรมโดยใช้ Telnet/SSH

การรักษาความปลอดภัย

- การลงชื่อเข้าใช้ครั้งเดียว
- Security Key Lifecycle Manager (SKLM)
- การบล็อกที่อยู่ IP
- โหมดการรักษาความปลอดภัยระดับองค์กรแบบรัดกุม (เป็นไปตาม CNSA)
- System Guard

การจัดการพลังงาน

- การจำกัดพลังงาน

- การตรวจสอบประสิทธิภาพ OOB — เมตริกประสิทธิภาพของระบบ
- กราฟิกด้านพลังงานแบบเรียลไทม์
- ชุดตัวนับพลังงานในอดีต
- กราฟิกแสดงอุณหภูมิ

การใช้งานและการกำหนดค่า

- การติดตั้งระบบปฏิบัติการจากระยะไกล

การอัปเดตเฟิร์มแวร์

- ซิงค์กับพื้นที่เก็บข้อมูล
- การอัปเดตอัตโนมัติ
- การอัปเดตชุดเฟิร์มแวร์
- การย้อนกลับเฟิร์มแวร์จากที่เก็บข้อมูลในเครื่องในการ์ด MicroSD

ฟังก์ชันการจัดการอื่น ๆ

- การจัดการกลุ่มข้างเคียง

การอัปเกรด XClarity Controller

หากเซิร์ฟเวอร์ของคุณมาพร้อมฟังก์ชันของเฟิร์มแวร์ XClarity Controller ในระดับมาตรฐานหรือขั้นสูง คุณอาจจะสามารถอัปเกรดฟังก์ชัน XClarity Controller ในเซิร์ฟเวอร์ของคุณได้ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับระดับการอัปเกรดที่มีและวิธีการสั่งซื้อ ให้ดู บทที่ 8 “การจัดการสิทธิ์การใช้งาน” บนหน้าที่ 133

ข้อกำหนดเกี่ยวกับเว็บเบราเซอร์และระบบปฏิบัติการ

ใช้ข้อมูลในหัวข้อนี้เพื่อดูรายการของเบราเซอร์ ชุดรหัส และระบบปฏิบัติการที่ได้รับการรองรับสำหรับเซิร์ฟเวอร์ของคุณ

เว็บอินเทอร์เฟซของ XClarity Controller ต้องใช้เว็บเบราเซอร์รายการใดรายการหนึ่งต่อไปนี้:

- Chrome 48.0 หรือสูงกว่า (55.0 หรือสูงกว่าสำหรับคอนโซลระยะไกล)
- Firefox ESR 38.6.0 หรือสูงกว่า
- Microsoft Edge
- Safari 9.0.2 หรือสูงกว่า (iOS 7 หรือใหม่กว่า และ OS X)

หมายเหตุ: การรองรับคุณลักษณะคอนโซลระยะไกลไม่พร้อมใช้งานผ่านเบราเซอร์บนระบบปฏิบัติการของอุปกรณ์เคลื่อนที่

เบราเซอร์ที่แสดงรายการข้างต้นตรงกับเบราเซอร์ที่ได้รับการรองรับโดยเฟิร์มแวร์ XClarity Controller ในขณะนี้ เฟิร์มแวร์ XClarity Controller อาจได้รับการปรับปรุงเป็นระยะๆ เพื่อรวมการรองรับเบราเซอร์อื่นๆ

การรองรับเว็บเบราเซอร์อาจแตกต่างจากเบราเซอร์ที่แสดงรายการในส่วนนี้ โดยขึ้นอยู่กับเวอร์ชันของเฟิร์มแวร์ใน XClarity Controller หากต้องการดูรายการเบราเซอร์ที่รองรับสำหรับเฟิร์มแวร์ที่อยู่ใน XClarity Controller ในปัจจุบัน ให้คลิกรายการเมนู **เบราเซอร์ที่รองรับ** จากหน้าการเข้าสู่ระบบ XClarity Controller

สำหรับการรักษาความปลอดภัยที่เพิ่มขึ้น ในตอนนี้มีเฉพาะรหัสที่มีประสิทธิภาพสูงเท่านั้นที่ได้รับการรองรับเมื่อใช้งาน HTTPS เมื่อใช้งาน HTTPS การใช้งานระหว่างระบบปฏิบัติการไคลเอ็นต์และเบราเซอร์ต้องรองรับชุดรหัสรายการใดรายการหนึ่งต่อไปนี้:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

แคชของเบราเซอร์อินเทอร์เน็ตจะจัดเก็บข้อมูลเกี่ยวกับเว็บเพจที่คุณเยี่ยมชม เพื่อให้เว็บเพจเหล่านั้นโหลดได้รวดเร็วยิ่งขึ้นในอนาคต หลังการอัปเดตแฟลชของเฟิร์มแวร์ XClarity Controller เบราเซอร์ของคุณอาจใช้ข้อมูลจากแคชต่อไป แทนการรับข้อมูลจาก XClarity Controller หลังการอัปเดตเฟิร์มแวร์ XClarity Controller ขอแนะนำให้ล้างข้อมูลแคชของเบราเซอร์ เพื่อให้แน่ใจว่าเว็บเพจที่ทำหน้าที่โดย XClarity Controller จะแสดงผลอย่างถูกต้อง

การสนับสนุนหลายภาษา

ใช้ข้อมูลในหัวข้อนี้เพื่อดูรายการภาษาที่ XClarity Controller สนับสนุน

ตามค่าเริ่มต้น ภาษาที่เลือกไว้สำหรับเว็บอินเทอร์เฟซ XClarity Controller คือภาษาอังกฤษ อินเทอร์เฟซสามารถแสดงผลได้หลายภาษา ซึ่งรวมถึงภาษาต่างๆ ต่อไปนี้:

- ภาษาฝรั่งเศส
- ภาษาเยอรมัน
- ภาษาอิตาลี
- ภาษาญี่ปุ่น
- ภาษาเกาหลี
- ภาษาโปรตุเกส (บราซิล)
- ภาษารัสเซีย
- ภาษาจีนตัวย่อ
- ภาษาสเปน (สากล)
- ภาษาจีนตัวเต็ม

ในการเลือกภาษาที่คุณต้องการ ให้คลิกลูกศรด้านข้างภาษาที่เลือกในปัจจุบัน เมนูแบบดรอปดาวน์จะปรากฏขึ้นเพื่อให้คุณเลือกภาษาที่ต้องการ

สตริงข้อความที่สร้างโดยเฟิร์มแวร์ XClarity Controller จะแสดงในภาษาที่สั่งโดยเบราเซอร์ หากเบราเซอร์ระบุภาษาอื่นนอกเหนือจากภาษาที่แปลตามที่แสดงรายการข้างต้น ข้อความจะแสดงในภาษาอังกฤษ นอกจากนี้ สตริงข้อความใดๆ ที่แสดงโดยเฟิร์มแวร์ XClarity Controller แต่ไม่ได้สร้างโดย XClarity Controller (ตัวอย่างเช่น ข้อความที่สร้างโดย UEFI, อะแดปเตอร์ PCIe เป็นต้น...) จะแสดงในภาษาอังกฤษ

อินพุตของข้อความที่เป็นภาษาเฉพาะนอกเหนือจากภาษาอังกฤษ เช่น *ข้อความการบุกรุก* ยังไม่ได้รับการรองรับในขณะนี้ เฉพาะข้อความที่พิมพ์ในภาษาอังกฤษเท่านั้นที่ได้รับการรองรับ

ข้อมูลเบื้องต้นเกี่ยวกับ MIB

ใช้ข้อมูลในหัวข้อนี้เพื่อเข้าถึง Management Information Base

สามารถดาวน์โหลด SNMP MIB ได้จาก https://support.lenovo.com/ (ค้นหาตามประเภทเครื่องบนพอร์ทัล) ซึ่งประกอบด้วยสี่ MIB ดังต่อไปนี้:

- **SMI MIB** อธิบายโครงสร้างข้อมูลการจัดการสำหรับ Lenovo Data Center Group
- **Product MIB** อธิบายเกี่ยวกับตัวระบุออบเจ็กต์สำหรับผลิตภัณฑ์ Lenovo
- **XCC MIB** ให้ข้อมูลเกี่ยวกับรายการอุปกรณ์และการตรวจสอบสำหรับ Lenovo XClarity Controller

- XCC Alert MIB กำหนด trap สำหรับเงื่อนไขการแจ้งเตือนที่ Lenovo XClarity Controller ตรวจพบ

หมายเหตุ: ลำดับการนำเข้าสำหรับ MIB ทั้งสี่คือ SMI MIB → Product MIB → XCC MIB → XCC Alert MIB

คำประกาศที่ใช้ในเอกสารนี้

ใช้ข้อมูลนี้เพื่อทำความเข้าใจเกี่ยวกับคำประกาศที่ใช้ในเอกสารนี้

เอกสารนี้จะใช้คำประกาศดังต่อไปนี้:

- **หมายเหตุ**: คำประกาศนี้แสดงคำแนะนำต่างๆ ที่สำคัญ
- **สำคัญ**: คำประกาศนี้แสดงข้อมูลหรือคำแนะนำที่อาจช่วยคุณเลี่ยงสถานการณ์ที่ก่อให้เกิดปัญหา หรือความไม่สะดวก
- **ข้อคำนึง**: คำประกาศนี้ระบุเกี่ยวกับความเสียหายที่อาจเกิดขึ้นได้กับโปรแกรม อุปกรณ์ หรือข้อมูล คำประกาศเกี่ยวกับข้อคำนึงจะเขียนไว้ก่อนหน้าคำแนะนำ หรือสถานการณ์ที่อาจก่อให้เกิดความเสียหาย

บทที่ 2. การเปิดและใช้งานเว็บอินเทอร์เฟซ XClarity Controller

หัวข้อนี้จะอธิบายขั้นตอนการเข้าใช้งานและการดำเนินการที่ทำได้จากเว็บอินเทอร์เฟซ XClarity Controller

XClarity Controller รวมฟังก์ชันโปรเซสเซอร์การบริการ ตัวควบคุมวิดีโอ และฟังก์ชัน Remote Presence เข้าไว้ด้วยกันในชิปเดียว ในการเข้าใช้ XClarity Controller จากระยะไกลผ่านเว็บอินเทอร์เฟซ คุณต้องลงชื่อเข้าใช้งานก่อน บทนี้จะอธิบายขั้นตอนการเข้าใช้งานและการดำเนินการที่ทำได้จากเว็บอินเทอร์เฟซ XClarity Controller

การเข้าถึงเว็บอินเทอร์เฟซ XClarity Controller

ข้อมูลในหัวข้อนี้จะอธิบายวิธีเข้าถึงเว็บอินเทอร์เฟซ XClarity Controller

XClarity Controller รองรับการกำหนดที่อยู่ IPv4 แบบคงที่และ Dynamic Host Configuration Protocol (DHCP) ที่อยู่ IPv4 แบบคงที่ตามค่าเริ่มต้นที่ระบุให้กับ XClarity Controller คือ 192.168.70.125 ในตอนแรก XClarity Controller ได้รับการกำหนดค่าให้พยายามรับที่อยู่จากเซิร์ฟเวอร์ DHCP และหากไม่สามารถทำได้ ก็จะใช้ที่อยู่ IPv4 แบบคงที่

นอกจากนี้ XClarity Controller ยังรองรับ IPv6 แต่จะไม่มีที่อยู่ IP แบบ IPv6 คงที่ ตามค่าเริ่มต้น ตอนแรก ในการเข้าถึง XClarity Controller ในระบบ IPv6 คุณสามารถใช้ที่อยู่ IP แบบ IPv4 หรือที่อยู่ Link Local แบบ IPv6 ก็ได้ XClarity Controller จะสร้างที่อยู่ Link Local แบบ IPv6 โดยใช้ MAC address มาตรฐาน IEEE 802 และแทรกด้วย Octet สองตัว โดยมีค่าเลขฐานสิบหก 0xFF และ 0xFE ตรงกลาง MAC address แบบ 48 บิต ดังที่อธิบายไว้ใน RFC4291 และสลับตำแหน่งบิตที่ 2 จากทางขวาในเลขแปดหลักชุดแรกของที่อยู่ MAC ตัวอย่างเช่น หาก MAC address คือ 08-94-ef-2f-28-af ที่อยู่ Link Local จะเป็นดังนี้:

```
fe80::0a94:efff:fe2f:28af
```

เมื่อคุณเข้าถึง XClarity Controller เงื่อนไข IPv6 ต่อไปนี้จะถูกตั้งเป็นค่าเริ่มต้น:

- การกำหนดค่าที่อยู่ IPv6 อัตโนมัติเปิดใช้งาน
- การกำหนดค่าที่อยู่ IP แบบคงที่ของ IPv6 ปิดใช้งาน
- DHCPv6 เปิดใช้งาน
- การกำหนดค่าอัตโนมัติแบบสุ่มเปิดใช้งาน

XClarity Controller ให้คุณเลือกได้ว่าจะใช้การเชื่อมต่อเครือข่ายกับเซิร์ฟเวอร์แบบ *เฉพาะ* (ถ้าใช้ได้) หรือแบบ *ใช้ร่วมกัน* สำหรับการจัดการระบบ โดยค่าเริ่มต้น เซิร์ฟเวอร์แบบติดตั้งอยู่บนตู้แร็คและแบบทาวเวอร์จะใช้การเชื่อมต่อเครือข่ายแบบ*เฉพาะ*สำหรับการจัดการระบบ

การเชื่อมต่อเครือข่ายแบบเฉพาะสำหรับการจัดการระบบบนเซิร์ฟเวอร์ส่วนใหญ่ จะมาพร้อมกับตัวควบคุมอินเทอร์เฟซเครือข่ายแบบ 1Gbit แยกต่างหาก อย่างไรก็ตาม ในบางระบบ อาจมีการเชื่อมต่อเครือข่ายสำหรับการจัดการระบบเฉพาะโดยใช้ Network Controller Sideband Interface (NCSI) กับพอร์ตเครือข่ายหนึ่งพอร์ตของตัวควบคุมอินเทอร์เฟซเครือข่ายแบบหลายพอร์ต ในกรณีนี้ การเชื่อมต่อเครือข่ายสำหรับการจัดการระบบเฉพาะจะจำกัดความเร็วของอินเทอร์เฟซ Sideband อยู่ที่ 10/100 สำหรับข้อมูลและข้อจำกัดเกี่ยวกับการติดตั้งใช้งานพอร์ตการจัดการในระบบ โปรดดูในเอกสารระบบของคุณ

หมายเหตุ: พอร์ตเครือข่ายแบบ *เฉพาะ* สำหรับการจัดการระบบอาจใช้ไม่ได้กับเซิร์ฟเวอร์ของคุณ หากฮาร์ดแวร์ของคุณไม่มีพอร์ตเครือข่ายแบบ *เฉพาะ* XClarity Controller จะใช้ได้เฉพาะการตั้งค่าเครือข่ายแบบ *ใช้ร่วมกัน* เท่านั้น

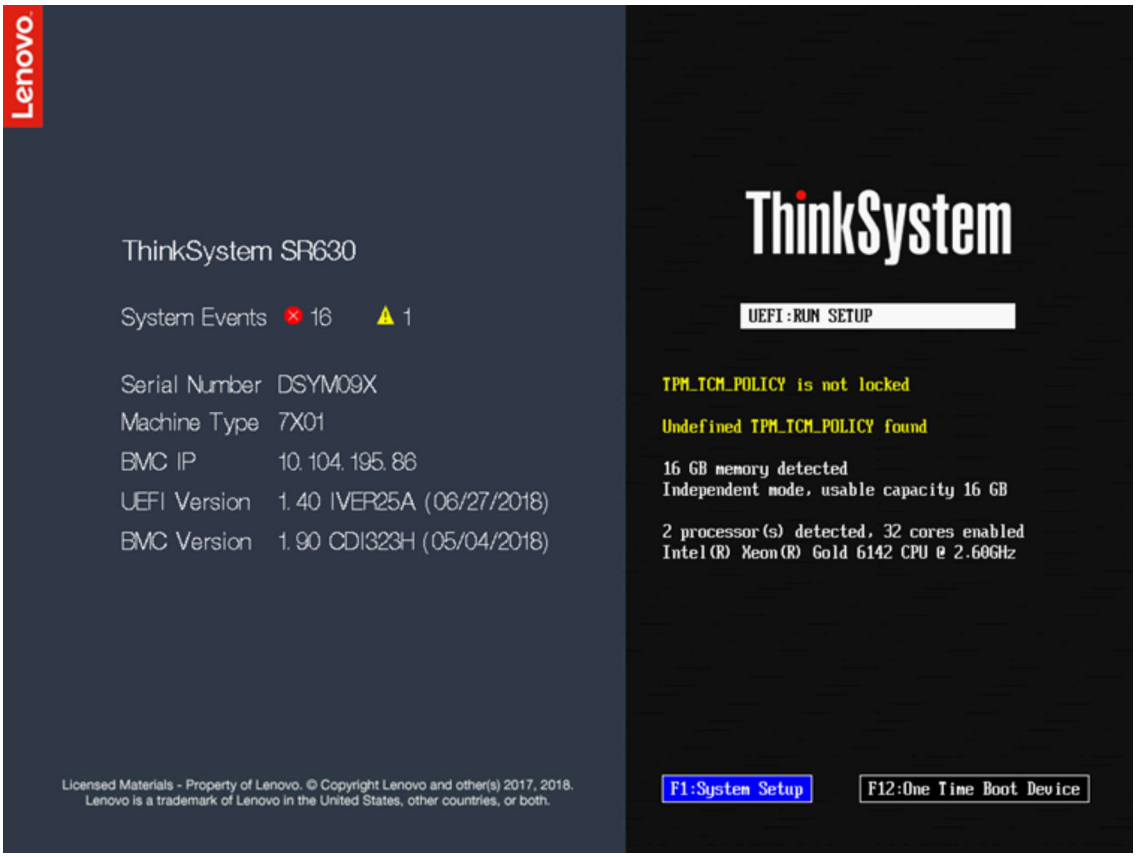
การตั้งค่าการเชื่อมต่อเครือข่าย XClarity Controller ผ่าน XClarity Provisioning Manager

ใช้ข้อมูลในหัวข้อนี้เพื่อตั้งค่าการเชื่อมต่อเครือข่าย XClarity Controller ผ่าน XClarity Provisioning Manager

หลังจากคุณเริ่มเซิร์ฟเวอร์ คุณสามารถใช้ XClarity Provisioning Manager ในการกำหนดค่าการเชื่อมต่อเครือข่าย XClarity Controller เซิร์ฟเวอร์ที่มี XClarity Controller ต้องเชื่อมต่อกับเซิร์ฟเวอร์ DHCP หรือต้องกำหนดค่าเครือข่ายเซิร์ฟเวอร์ให้ใช้ที่อยู่ IP แบบคงที่ของ XClarity Controller ในการตั้งค่าการเชื่อมต่อเครือข่าย XClarity Controller ผ่าน Setup Utility ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. เปิดเซิร์ฟเวอร์ หน้าต้อนรับ ThinkSystem จะปรากฏขึ้น

> **หมายเหตุ**: หลังจากเซิร์ฟเวอร์ต่อเข้ากับไฟ AC แล้ว กว่าที่ปุ่มควบคุมการเปิด/ปิดจะทำงานอาจใช้เวลาถึง 40 วินาที



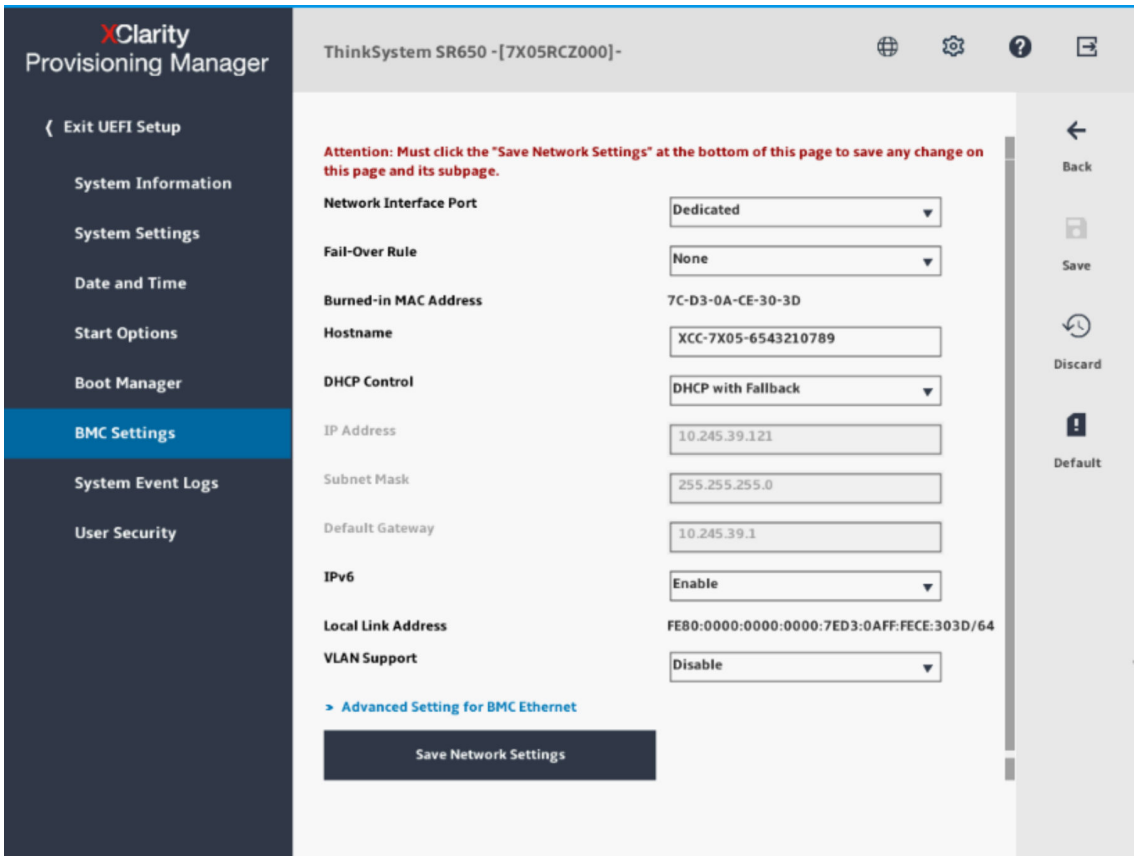
ขั้นตอนที่ 2. เมื่อระบบแสดงพร้อมท์ **<F1> System Setup** ให้กด F1 หากคุณได้ตั้งค่าทั้งรหัสผ่านในการเปิดเครื่องและรหัสผ่านผู้ดูแลระบบ คุณต้องพิมพ์รหัสผ่านผู้ดูแลระบบเพื่อเข้าถึง XClarity Provisioning Manager

ขั้นตอนที่ 3. จากเมนูหลักของ XClarity Provisioning Manager ให้เลือก **UEFI Setup**

ขั้นตอนที่ 4. บนหน้าจอถัดไป ให้เลือก **BMC Settings** จากนั้นคลิก **Network Settings**

ขั้นตอนที่ 5. มีตัวเลือกการเชื่อมต่อเครือข่าย XClarity Controller 3 ตัวเลือกในฟิลด์ **DHCP Control**:

- IP แบบคงที่
- เปิดใช้งาน DHCP
- DHCP พร้อมการใช้แทน



ขั้นตอนที่ 6. เลือกหนึ่งในตัวเลือกการเชื่อมต่อเครือข่าย

ขั้นตอนที่ 7. หากคุณเลือกใช้ที่อยู่ IP แบบคงที่ คุณต้องระบุที่อยู่ IP, ตัวพรางเครือข่ายย่อย และเกตเวย์ตามค่าเริ่มต้น

ขั้นตอนที่ 8. คุณยังสามารถใช้ Lenovo XClarity Controller Manager เพื่อเลือกการเชื่อมต่อเครือข่ายเฉพาะ (หากเซิร์ฟเวอร์ของคุณมีพอร์ตเครือข่ายเฉพาะ) หรือการเชื่อมต่อเครือข่าย XClarity Controller ที่ใช้ร่วมกัน

หมายเหตุ:

- พอร์ตเครือข่ายการจัดการระบบเฉพาะอาจใช้ไม่ได้กับเซิร์ฟเวอร์ของคุณ หากฮาร์ดแวร์ของคุณไม่มีพอร์ตเครือข่ายเฉพาะ XClarity Controller จะใช้ได้เฉพาะการตั้งค่าเครือข่ายที่ *ใช้ร่วมกัน* เท่านั้น บนหน้าจอ **Network Configuration** ให้เลือก **Dedicated** (หากมี) หรือ **Shared** ในฟิลด์ **Network Interface Port**
- ในการค้นหาตำแหน่งของขั้วต่ออีเทอร์เน็ตบนเซิร์ฟเวอร์ที่ XClarity Controller ใช้งาน ให้ดูเอกสารที่มาพร้อมเซิร์ฟเวอร์ของคุณ

ขั้นตอนที่ 9. คลิก **บันทึก**

ขั้นตอนที่ 10. ออกจาก XClarity Provisioning Manager

หมายเหตุ:

- คุณต้องรอประมาณ 1 นาทีเพื่อให้การเปลี่ยนแปลงมีผลก่อนที่เฟิร์มแวร์ของเซิร์ฟเวอร์จะกลับมาทำงานได้อีกครั้ง
- คุณยังสามารถกำหนดค่าการเชื่อมต่อเครือข่าย XClarity Controller ผ่านเว็บอินเทอร์เฟซ XClarity Controller หรืออินเทอร์เฟซบรรทัดคำสั่ง (CLI) ในเว็บอินเทอร์เฟซ XClarity Controller สามารถกำหนดค่าการเชื่อมต่อเครือข่ายโดยคลิก **การกำหนดค่า** BMC จากแผงการนำทางด้านซ้าย แล้วเลือก **เครือข่าย** ใน CLI ของ XClarity Controller การเชื่อมต่อเครือข่ายได้รับการกำหนดค่าโดยใช้คำสั่งต่างๆ หลายคำสั่ง ซึ่งขึ้นอยู่กับการกำหนดค่าการติดตั้งของคุณ

การเข้าสู่ระบบ XClarity Controller

ใช้ข้อมูลในหัวข้อนี้เพื่อเข้าถึง XClarity Controller ผ่านเว็บอินเทอร์เฟซ XClarity Controller

ข้อสำคัญ: XClarity Controller จะได้รับการตั้งค่าเริ่มต้นด้วยชื่อผู้ใช้ `USERID` และรหัสผ่าน `PASSWORD` (ที่มีเลขศูนย์ ไม่ใช่ตัวอักษร O) การตั้งค่าผู้ใช้ตามค่าเริ่มต้นนี้มีสิทธิ์การเข้าถึงระดับผู้ควบคุม เปลี่ยนชื่อผู้ใช้และรหัสผ่านนี้ระหว่างการกำหนดค่าเริ่มต้นเพื่อการรักษาความปลอดภัยที่ดียิ่งขึ้น หลังจากทำการเปลี่ยนแปลง คุณจะไม่สามารถตั้งค่า `PASSWORD` เป็นรหัสผ่านสำหรับเข้าสู่ระบบได้อีกครั้ง

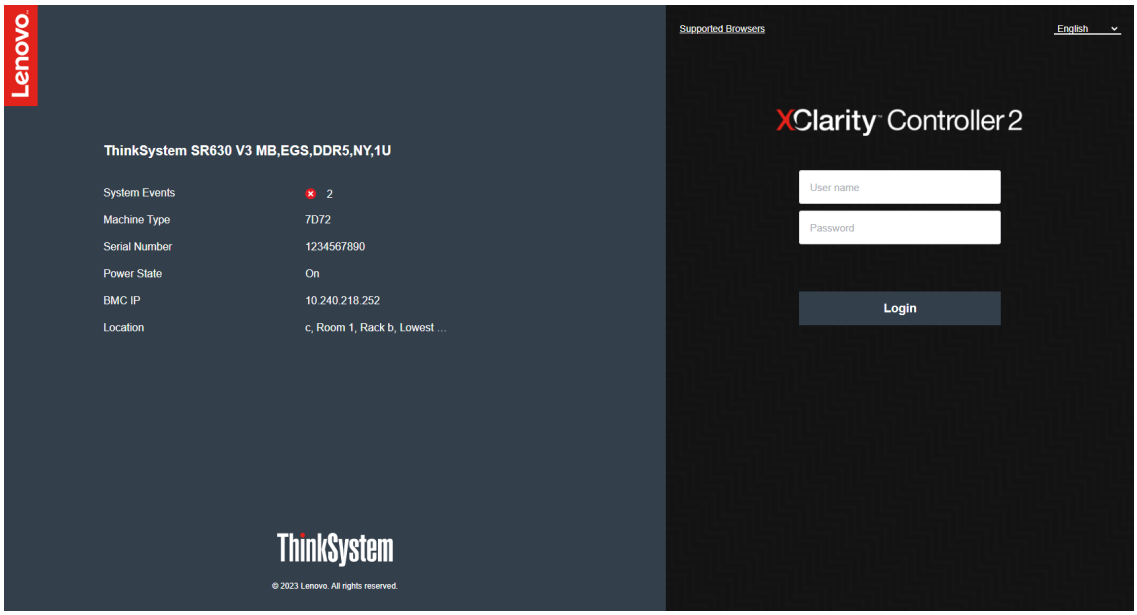
หมายเหตุ: ใน Flex System สามารถจัดการบัญชีผู้ใช้ XClarity Controller ได้โดย Flex System Chassis Management Module (CMM) และอาจแตกต่างจากการผสมระหว่าง USERID/PASSW0RD ที่อธิบายข้างต้น

ในการเข้าถึง XClarity Controller ผ่านเว็บอินเทอร์เฟซ XClarity Controller ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. เปิดเว็บเบราเซอร์ ในฟิลด์ที่อยู่หรือ URL ให้พิมพ์ที่อยู่ IP หรือชื่อโฮสต์ของ XClarity Controller ที่คุณต้องการเชื่อมต่อ

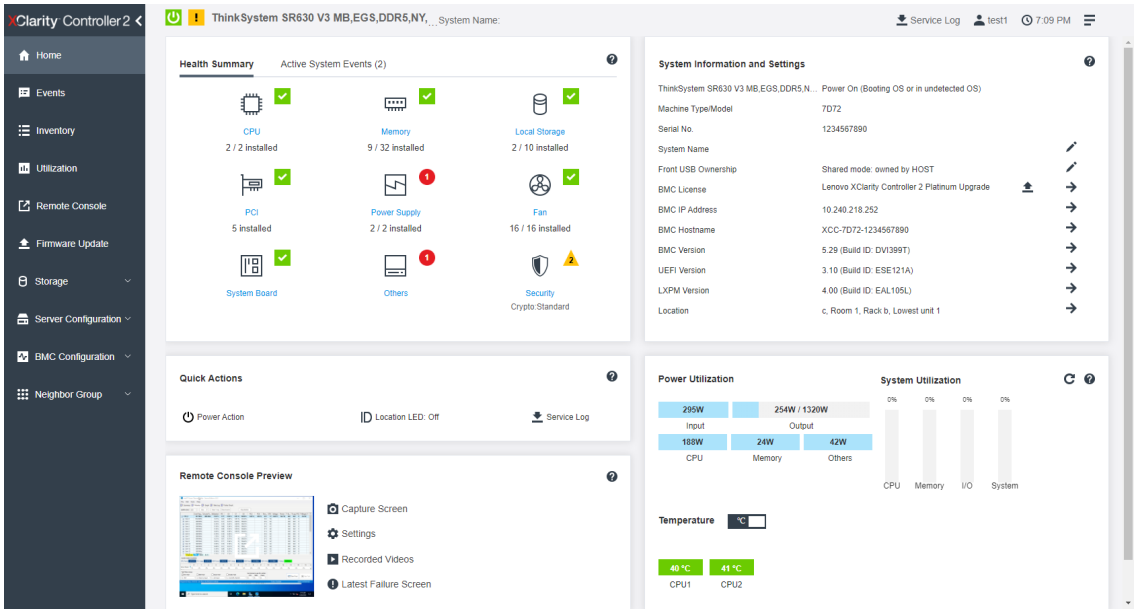
ขั้นตอนที่ 2. เลือกภาษาที่ต้องการจากรายการภาษาแบบดรอปดาวน์

หน้าต่างการเข้าสู่ระบบจะแสดงในภาพประกอบต่อไปนี้



ขั้นตอนที่ 3. พิมพ์ชื่อผู้ใช้และรหัสผ่านของคุณในหน้าต่างการเข้าสู่ระบบ XClarity Controller หากคุณกำลังใช้ XClarity Controller เป็นครั้งแรก คุณสามารถรับชื่อผู้ใช้และรหัสผ่านจากผู้ดูแลระบบของคุณ ความพยายามในการเข้าสู่ระบบทั้งหมดจะถูกบันทึกลงในบันทึกเหตุการณ์ คุณอาจต้องป้อนรหัสผ่านใหม่หลังจากเข้าสู่ระบบ ทั้งนี้ขึ้นอยู่กับว่าผู้ดูแลระบบของคุณกำหนดค่า ID ผู้ใช้ไว้อย่างไร

ขั้นตอนที่ 4. คลิก **เข้าสู่ระบบ** เพื่อเริ่มต้นเซสชัน เบราเซอร์จะเปิดหน้าแรกของ XClarity Controller ตามที่แสดงในภาพประกอบต่อไปนี้ หน้าแรกจะแสดงข้อมูลเกี่ยวกับระบบที่ XClarity Controller จัดการ และไอคอนที่ระบุจำนวนข้อผิดพลาดร้ายแรง 1 และจำนวนคำเตือน 1 ที่ปรากฏในระบบ ณ ปัจจุบัน



หน้าแรกจะแบ่งออกเป็นสองส่วนสำคัญ ส่วนแรกคือแผงการนำทางด้านซ้าย ซึ่งเป็นชุดหัวข้อที่ทำให้คุณสามารถดำเนินการดังต่อไปนี้:

- ตรวจสอบสถานะเซิร์ฟเวอร์
- กำหนดค่าเซิร์ฟเวอร์
- กำหนดค่า XClarity Controller หรือ BMC
- ปรับปรุงเฟิร์มแวร์

ส่วนที่สองคือข้อมูลแบบกราฟิกที่อยู่ทางด้านขวาของแผงการนำทาง รูปแบบที่แบ่งแยกย่อยจะแสดงมุมมองด่วนของสถานะเซิร์ฟเวอร์ และการดำเนินการด่วนบางส่วนที่สามารถดำเนินการได้

รายละเอียดเกี่ยวกับฟังก์ชัน XClarity Controller ในเว็บอินเทอร์เฟซ

นี่คือตารางที่อธิบายฟังก์ชันต่างๆ ของ XClarity Controller ในแผงการนำทางด้านซ้าย

หมายเหตุ: ขณะที่ใช้งานส่วนต่างๆ ในเว็บอินเทอร์เฟซ คุณยังสามารถคลิกที่ไอคอนเครื่องหมายคำถามเพื่อดูวิธีใช้แบบออนไลน์ได้ด้วย

ตาราง 1. ฟังก์ชัน XClarity Controller

ตารางสามคอลัมน์ที่แสดงรายละเอียดการดำเนินการที่ทำได้จากเว็บอินเทอร์เฟซ XClarity Controller

แท็บ	รายการที่เลือก	รายละเอียด
หน้าแรก	ข้อมูลสรุปสถานะ/เหตุการณ์ของระบบที่ดำเนินอยู่	แสดงสถานะปัจจุบันของส่วนประกอบฮาร์ดแวร์หลักภายในระบบ
	ข้อมูลและการตั้งค่าระบบ	แสดงข้อมูลสรุปทั่วไปของระบบ
	การดำเนินการด่วน	แสดงลิงก์ด่วนสำหรับควบคุมการเปิด/ปิดเครื่องเซิร์ฟเวอร์และไฟ LED ตำแหน่ง รวมทั้งปุ่มในการดาวน์โหลดข้อมูลการซ่อมบำรุง
	การใช้พลังงาน/การใช้งานระบบ/อุณหภูมิ	แสดงภาพรวมด่วนเกี่ยวกับการใช้พลังงาน การใช้งานระบบ และอุณหภูมิเซิร์ฟเวอร์โดยรวมในปัจจุบัน

ตาราง 1. ฟังก์ชัน XClarity Controller (มีต่อ)

แท็บ	รายการที่เลือก	รายละเอียด
	การแสดงตัวอย่างคอนโซลระยะไกล	ควบคุมเซิร์ฟเวอร์ในระดับระบบปฏิบัติการ คุณสามารถดูและใช้งานคอนโซลเซิร์ฟเวอร์ได้จากคอมพิวเตอร์ของคุณ ส่วนคอนโซลระยะไกลในหน้าแรกของ XClarity Controller จะแสดงภาพหน้าจอพร้อมปุ่มเรียกใช้ แถบเครื่องมือด้านขวาประกอบด้วยการดำเนินการด่วนต่อไปนี้: • จับภาพหน้าจอ • การตั้งค่า • วิดีโอที่บันทึก • หน้าจอความบกพร่องล่าสุด
เหตุการณ์	บันทึกเหตุการณ์	แสดงรายการเหตุการณ์เกี่ยวกับฮาร์ดแวร์และการจัดการที่ผ่านมาทั้งหมด
	บันทึกการตรวจสอบ	แสดงบันทึกการดำเนินการที่ผ่านมาของผู้ใช้ เช่น การล็อกอินเข้าใช้ Lenovo XClarity Controller การสร้างผู้ใช้ใหม่ และการเปลี่ยนรหัสผ่านของผู้ใช้ คุณสามารถใช้บันทึกการตรวจสอบเพื่อติดตามและลงบันทึกการให้สิทธิ์และการควบคุมต่างๆ ในระบบไอที
	ประวัติการบำรุงรักษา	แสดงประวัติการอัปเดตเฟิร์มแวร์ การกำหนดค่า และการเปลี่ยนฮาร์ดแวร์ที่ผ่านมาทั้งหมด
	ผู้รับการแจ้งเตือน	ระบุตัวผู้ที่จะได้รับแจ้งเกี่ยวกับเหตุการณ์ต่างๆ ในระบบ ช่วยให้คุณสามารถกำหนดค่าผู้รับแจ้งแต่ละคน รวมทั้งจัดการการตั้งค่าที่มีผลกับผู้รับแจ้งเหตุการณ์ทั้งหมด นอกจากนี้ คุณยังสามารถสร้างเหตุการณ์ทดสอบเพื่อยืนยันว่าการตั้งค่าการแจ้งเตือนของคุณใช้ได้ผลจริงหรือไม่
รายการอุปกรณ์		แสดงส่วนประกอบทั้งหมดในระบบ พร้อมทั้งสถานะและข้อมูลสำคัญ คุณสามารถคลิกที่อุปกรณ์เพื่อแสดงข้อมูลเพิ่มเติม **หมายเหตุ**: โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับสถานะเปิด/ปิดเครื่องในเว็บอินเทอร์เฟซ SMM2
การใช้		แสดงข้อมูลอุณหภูมิโดยรอบ/ส่วนประกอบ, การใช้พลังงาน, ระดับแรงดันไฟฟ้า, การใช้งานระบบย่อยภายในระบบ และความเร็วพัดลมของเซิร์ฟเวอร์รวมถึงส่วนประกอบของเซิร์ฟเวอร์ในรูปแบบกราฟิกหรือแบบตาราง

ตาราง 1. ฟังก์ชัน XClarity Controller (มีต่อ)

แท็บ	รายการที่เลือก	รายละเอียด
ที่จัดเก็บข้อมูล	รายละเอียด	แสดงโครงสร้างทางกายภาพของอุปกรณ์จัดเก็บข้อมูลและการกำหนดค่าพื้นที่จัดเก็บข้อมูล
	การตั้งค่า RAID	ดูหรือแก้ไขการกำหนดค่า RAID ในปัจจุบัน ซึ่งรวมถึงข้อมูลดิสก์เสมือนและอุปกรณ์จัดเก็บตามจริง
คอนโซลระยะไกล		ให้สิทธิ์เข้าถึงฟังก์ชันการทำงานของคอนโซลระยะไกล คุณสามารถใช้คุณลักษณะสื่อเสมือนเพื่อเมาท์ไฟล์ ISO หรือ IMG ที่อยู่ในระบบของคุณ หรือบนเครือข่ายที่เข้าถึงได้โดย BMC ที่ใช้โปรโตคอล CIFS, NFS, HTTPS หรือ SFTP ดิสก์ที่เมาท์จะปรากฏเป็นไดรฟ์ USB ที่เชื่อมต่อกับเซิร์ฟเวอร์
กา รอัปเดตเฟิร์มแวร์		• แสดงระดับของเฟิร์มแวร์ • อัปเดตเฟิร์มแวร์ของ XClarity Controller และเฟิร์มแวร์ของเซิร์ฟเวอร์ • อัปเดตเฟิร์มแวร์ของ XClarity Controller จากที่เก็บข้อมูล
การกำหนดค่าเซิร์ฟเวอร์	อะแดปเตอร์	แสดงข้อมูลอะแดปเตอร์เครือข่ายที่ติดตั้งไว้ รวมทั้งการตั้งค่าที่สามารถกำหนดค่าได้ทาง XClarity Controller
	ตัวเลือกการบูต	• เลือกอุปกรณ์สำหรับบูตที่จะใช้ในการบูตแบบครั้งเดียวในการเริ่มระบบเซิร์ฟเวอร์ใหม่ครั้งต่อไป • เปลี่ยนการตั้งค่าโหมดการบูตและลำดับการบูต
	นโยบายพลังงาน	• กำหนดค่าการสำรองพลังงานที่จะใช้เมื่อเกิดเหตุการณ์แหล่งจ่ายไฟขัดข้อง • กำหนดค่านโยบายการจำกัดพลังงาน • กำหนดค่านโยบายการจ่ายไฟกลับเข้าระบบ **หมายเหตุ**: โปรดดูรายละเอียดเพิ่มเติมเกี่ยวกับสถานะเปิด/ปิดเครื่องในเว็บอินเทอร์เฟซ SMM2

ตาราง 1. ฟังก์ชัน XClarity Controller (มีต่อ)

แท็บ	รายการที่เลือก	รายละเอียด
	คุณสมบัติของเซิร์ฟเวอร์	• เฝ้าดูคุณสมบัติ สถานะ และการตั้งค่าเซิร์ฟเวอร์ • จัดการไทม์เอาต์ในการเริ่มระบบเซิร์ฟเวอร์เพื่อตรวจจับและกู้คืนจากอาการเซิร์ฟเวอร์ค้าง • สร้างข้อความการบุกรุก ข้อความการบุกรุกคือข้อความที่คุณสามารถสร้างขึ้นเพื่อให้ผู้ใช้เห็นเมื่อพวกเขาเข้าสู่ระบบ XClarity Controller
การกำหนดค่า BMC	การสำรองและกู้คืนข้อมูล	รีเซ็ตการกำหนดค่า XClarity Controller เพื่อใช้การตั้งค่าเริ่มต้นจากโรงงาน สำรองข้อมูลการกำหนดค่าปัจจุบัน หรือเรียกคืนการกำหนดค่าจากไฟล์
	สิทธิ์การใช้งาน	จัดการคีย์เปิดการทำงานสำหรับคุณลักษณะ XClarity Controller ที่เป็นตัวเลือกเสริม
	เครือข่าย	กำหนดค่าคุณสมบัติ สถานะ และการตั้งค่าเครือข่ายสำหรับ XClarity Controller
	การรักษาความปลอดภัย	กำหนดค่าคุณสมบัติ สถานะ และการตั้งค่าการรักษาความปลอดภัยสำหรับ XClarity Controller
	ผู้ใช้/LDAP	• กำหนดค่าโปรไฟล์การเข้าใช้งาน XClarity Controller และการตั้งค่าล็อกอินกลาง • ดูบัญชีผู้ใช้ที่กำลังเข้าใช้งาน XClarity Controller อยู่ในขณะนี้ • แท็บ LDAP จะกำหนดค่าการตรวจสอบความถูกต้องของผู้ใช้เพื่อใช้ร่วมกับเซิร์ฟเวอร์ LDAP อย่างน้อยหนึ่งเซิร์ฟเวอร์ นอกจากนี้ ยังช่วยให้สามารถเปิดใช้งานหรือปิดใช้งานการรักษาความปลอดภัย LDAP และจัดการใบรับรองได้
	Call Home	กำหนดค่าตัวเลือก Call Home เพื่อรวบรวมข้อมูลเกี่ยวกับระบบและส่งไปยัง Lenovo สำหรับการบริการ

บทที่ 3. การกำหนดค่า XClarity Controller

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจเกี่ยวกับตัวเลือกต่างๆ ที่ใช้ได้ในการกำหนดค่า XClarity Controller

เมื่อกำหนดค่า XClarity Controller จะสามารถใช้ตัวเลือกสำคัญๆ ต่อไปนี้ได้:

- การสำรองและกู้คืนข้อมูล
- สิทธิ์การใช้งาน
- เครือข่าย
- การรักษาความปลอดภัย
- ผู้ใช้/LDAP

การกำหนดค่าบัญชีผู้ใช้/LDAP

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีการจัดการบัญชีผู้ใช้

คลิก **ผู้ใช้**/LDAP ภายใต้ **การกำหนดค่า** BMC เพื่อสร้าง แก้ไข และดูบัญชีผู้ใช้ และกำหนดการตั้งค่า LDAP

แท็บ **ผู้ใช้ภายในระบบ** แสดงบัญชีผู้ใช้ที่ได้รับการกำหนดค่าใน XClarity Controller และมีการเข้าสู่ระบบ XClarity Controller ในปัจจุบัน

แท็บ **LDAP** แสดงการกำหนดค่า LDAP สำหรับการเข้าถึงบัญชีผู้ใช้ที่เก็บไว้บนเซิร์ฟเวอร์ LDAP

วิธีการตรวจสอบความถูกต้องของผู้ใช้

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจเกี่ยวกับโหมดการทำงานแบบต่างๆ ที่ XClarity Controller สามารถใช้เพื่อตรวจสอบความถูกต้องสำหรับความพยายามในการเข้าสู่ระบบ

คลิก **ยินยอมการเข้าสู่ระบบจาก** เพื่อเลือกวิธีการตรวจสอบความถูกต้องสำหรับความพยายามในการเข้าสู่ระบบ คุณสามารถเลือกใช้วิธีการตรวจสอบความถูกต้องวิธีใดวิธีหนึ่งดังต่อไปนี้:

- **ภายในเท่านั้น**: ผู้ใช้จะได้รับการตรวจสอบความถูกต้องโดยการค้นหาบัญชีผู้ใช้ภายในที่มีการกำหนดค่าใน XClarity Controller หากไม่มี ID ผู้ใช้และรหัสผ่านที่ตรงกัน การเข้าถึงจะถูกปฏิเสธ
- LDAP **เท่านั้น**: XClarity Controller จะพยายามตรวจสอบความถูกต้องของผู้ใช้ด้วยข้อมูลประจำตัวที่เก็บไว้ภายในเซิร์ฟเวอร์ LDAP การใช้วิธีการตรวจสอบนี้จะ*ไม่*มีการค้นหาบัญชีผู้ใช้ภายในระบบจากใน XClarity Controller

- **ภายในและตามด้วย** LDAP: ระบบจะพยายามใช้การตรวจสอบความถูกต้องภายในก่อน หากการตรวจสอบความถูกต้องภายในล้มเหลว ระบบจะใช้การตรวจสอบความถูกต้องแบบ LDAP
- LDAP **ก่อน แล้วตามด้วยผู้ใช้ภายในระบบ**: ระบบจะพยายามใช้การตรวจสอบความถูกต้อง LDAP ก่อน หากการตรวจสอบความถูกต้องแบบ LDAP ล้มเหลว ระบบจะใช้การตรวจสอบความถูกต้องภายใน

หมายเหตุ:

- เฉพาะบัญชีที่ได้รับการดูแลภายในเท่านั้นที่มีการแบ่งปันกับอินเทอร์เฟซ IPMI และ SNMP อินเทอร์เฟซดังกล่าวไม่รองรับการตรวจสอบความถูกต้องแบบ LDAP
- ผู้ใช้ IPMI และ SNMP จะสามารถเข้าสู่ระบบโดยใช้บัญชีที่ได้รับการดูแลภายใน เมื่อฟิลด์ **ยินยอมการเข้าสู่ระบบจาก** ตั้งค่าเป็น LDAP **เท่านั้น**

การสร้างบทบาทใหม่

ใช้ข้อมูลในหัวข้อนี้เพื่อสร้างบทบาทใหม่

สร้างบทบาท

คลิกแท็บ **บทบาท** และคลิกที่ **สร้าง** เพื่อสร้างบทบาทแบบปรับแต่งเอง

กรอกข้อมูลในฟิลด์ต่อไปนี้: **ชื่อบทบาท** และ **ระดับอำนาจหน้าที่** สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับระดับสิทธิ์ โปรดดูที่หัวข้อถัดไป

บทบาทที่สร้างขึ้นมีให้กับผู้ใช้ในเมนูแบบดรอปดาวน์ตรงบทบาทในส่วนผู้ใช้

หมายเหตุ: บทบาทที่ใช้ในผู้ใช้และ LDAP ไม่ได้รับอนุญาตให้แก้ไขและลบชื่อบทบาท แต่มีสิทธิ์เข้าถึงเพื่อแก้ไขการอนุญาตที่กำหนดเองที่เกี่ยวข้อง

ระดับสิทธิ์

บทบาทแบบปรับแต่งสามารถเปิดใช้งานกลุ่มสิทธิพิเศษต่างๆ ต่อไปนี้:

การกำหนดค่า - เครือข่ายและการรักษาความปลอดภัย BMC
ผู้ใช้สามารถแก้ไขพารามิเตอร์การกำหนดค่าภายในหน้าการรักษาความปลอดภัย BMC และหน้าเครือข่าย

การจัดการบัญชีผู้ใช้
ผู้ใช้สามารถเพิ่ม แก้ไข หรือลบผู้ใช้ รวมทั้งเปลี่ยนการตั้งค่าการเข้าสู่ระบบแบบส่วนกลางได้

การเข้าถึงคอนโซลระยะไกล
ผู้ใช้สามารถเข้าถึงคอนโซลระยะไกลได้

การเข้าถึงคอนโซลระยะไกลและดิสก์ระยะไกล

ผู้ใช้สามารถเข้าถึงคอนโซลระยะไกลและคุณลักษณะสื่อเสมือนได้

การเปิด/รีสตาร์ทเซิร์ฟเวอร์จากระยะไกล

ผู้ใช้สามารถใช้งานฟังก์ชันการเปิดเครื่องและรีสตาร์ทเซิร์ฟเวอร์ได้

การกำหนดค่า - พื้นฐาน

ผู้ใช้สามารถแก้ไขพารามิเตอร์การกำหนดค่าภายในหน้าคุณสมบัติเซิร์ฟเวอร์และเหตุการณ์ได้

ความสามารถในการล้างข้อมูลบันทึกเหตุการณ์

ผู้ใช้สามารถล้างข้อมูลบันทึกเหตุการณ์ ผู้ใช้ทุกรายสามารถดูบันทึกเหตุการณ์ได้ แต่จะต้องมีระดับสิทธิ์นี้เพื่อล้างบันทึก

การกำหนดค่า - ขั้นสูง (การอัปเดตเฟิร์มแวร์, รีสตาร์ท BMC, กู้คืนการกำหนดค่า)

ผู้ใช้ไม่มีข้อจำกัดเมื่อกำหนดค่า XClarity Controller นอกจากนี้ ผู้ใช้งานจะมีสิทธิ์การเข้าถึงด้านการดูแลเพื่อใช้งาน XClarity Controller สิทธิ์การเข้าถึงด้านการดูแล ประกอบด้วยฟังก์ชันขั้นสูงดังต่อไปนี้: การอัปเดตเฟิร์มแวร์, การบูตเครือข่าย PXE, การกู้คืน XClarity Controller เป็นค่าเริ่มต้นจากโรงงาน, การแก้ไขและกู้คืนการตั้งค่า XClarity Controller จากไฟล์การกำหนดค่า และการรีสตาร์ทและรีเซ็ต XClarity Controller

การกำหนดค่า - การรักษาความปลอดภัย UEFI

ผู้ใช้สามารถแก้ไขการตั้งค่าการรักษาความปลอดภัย UEFI ได้

บทบาทที่กำหนดค่าล่วงหน้า

บทบาทต่อไปนี้ได้รับการกำหนดค่าล่วงหน้าและไม่สามารถแก้ไขหรือลบได้:

ผู้ดูแลระบบ

บทบาทผู้ดูแลระบบไม่มีข้อจำกัดและสามารถดำเนินการได้ทั้งหมด

อ่านอย่างเดียว

บทบาท Read Only (อ่านอย่างเดียว) สามารถแสดงข้อมูลเซิร์ฟเวอร์ได้ แต่ไม่สามารถดำเนินการที่ส่งผลต่อสถานะของระบบได้ เช่น บันทึก แก้ไข ล้าง รีบูต อัปเดตเฟิร์มแวร์

ผู้ปฏิบัติงาน

ผู้ใช้ที่มีบทบาทผู้ปฏิบัติงานมีสิทธิ์ดังต่อไปนี้:

- การกำหนดค่า - เครือข่ายและการรักษาความปลอดภัย BMC
- การเปิด/รีสตาร์ทเซิร์ฟเวอร์จากระยะไกล
- การกำหนดค่า - พื้นฐาน
- ความสามารถในการล้างข้อมูลบันทึกเหตุการณ์

- การกำหนดค่า - ขั้นสูง (การอัปเดตเฟิร์มแวร์, รีสตาร์ท BMC, กู้คืนการกำหนดค่า)

การสร้างบัญชีผู้ใช้ใหม่

ใช้ข้อมูลในหัวข้อนี้เพื่อสร้างผู้ใช้ใหม่ภายในระบบ

การสร้างผู้ใช้

คลิกที่ **สร้าง** เพื่อสร้างบัญชีผู้ใช้ใหม่

กรอกข้อมูลในฟิลด์ต่อไปนี้: **ชื่อผู้ใช้**, **รหัสผ่าน**, **ยืนยันรหัสผ่าน** และเลือก **บทบาท** จากเมนูดรอปดาวน์ สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับ **บทบาท** โปรดดูที่หัวข้อถัดไป

บทบาท

บทบาทต่อไปนี้ถูกกำหนดไว้ล่วงหน้าในขณะที่สามารถสร้างบทบาทแบบกำหนดเองใหม่ได้ตามความต้องการของผู้ใช้:

ผู้ดูแลระบบ
บทบาทผู้ดูแลระบบไม่มีข้อจำกัดและสามารถดำเนินการได้ทั้งหมด

อ่านอย่างเดียว
บทบาท Read Only (อ่านอย่างเดียว) สามารถแสดงข้อมูลเซิร์ฟเวอร์ได้ แต่ไม่สามารถดำเนินการที่ส่งผลต่อสถานะของระบบได้ เช่น บันทึก แก้ไข ล้าง รีบูต อัปเดตเฟิร์มแวร์

ผู้ปฏิบัติงาน
ผู้ใช้ที่มีบทบาทผู้ปฏิบัติงานมีสิทธิ์ดังต่อไปนี้:

- การกำหนดค่า - เครือข่ายและการรักษาความปลอดภัย BMC
- การเปิด/รีสตาร์ทเซิร์ฟเวอร์จากระยะไกล
- การกำหนดค่า - พื้นฐาน
- ความสามารถในการล้างข้อมูลบันทึกเหตุการณ์
- การกำหนดค่า - ขั้นสูง (การอัปเดตเฟิร์มแวร์, รีสตาร์ท BMC, กู้คืนการกำหนดค่า)

การตั้งค่า SNMPv3

ในการเปิดใช้งานการเข้าถึง SNMPv3 ให้กับผู้ใช้ ให้เลือกกล่องตัวเลือกที่อยู่ถัดจาก **การตั้งค่า SNMPv3** คำอธิบายตัวเลือกการเข้าถึงของผู้ใช้งานมีดังนี้:

ประเภทการเข้าถึง

รองรับเฉพาะการดำเนินการ **GET** เท่านั้น XClarity Controller ไม่รองรับการดำเนินการ **SET** ของ SNMPv3 SNMP3 สามารถทำได้เฉพาะการสอบถามเท่านั้น

ที่อยู่สำหรับ trap

ระบุเป้าหมายของ trap สำหรับผู้ใช้ ค่านี้สามารถเป็นที่อยู่ IP หรือชื่อโฮสต์ก็ได้ การใช้งาน trap ช่วยให้ตัวแทน SNMP แจ้งไปยังสถานีการจัดการเกี่ยวกับเหตุการณ์ต่างๆ (เช่น เมื่ออุณหภูมิของโปรเซสเซอร์สูงเกินกว่ากำหนด)

โปรโตคอลการตรวจสอบความถูกต้อง

รองรับเฉพาะ **HMAC-SHA** เป็นโปรโตคอลการตรวจสอบความถูกต้องเท่านั้น อัลกอริทึมนี้ใช้โดยโมเดลการรักษาความปลอดภัยของ SNMPv3 สำหรับการรับรองความถูกต้อง

โปรโตคอลความเป็นส่วนตัว

คุณสามารถป้องกันข้อมูลที่ถ่ายโอนระหว่างไคลเอ็นต์ของ SNMP และตัวแทนได้ด้วยการเข้ารหัส วิธีการที่สนับสนุนได้แก่ **CBC-DES** และ **AES**

หมายเหตุ: แม้ว่าผู้ใช้ SNMPv3 จะใช้สตริงของรหัสผ่านที่ซ้ำกัน ระบบจะยังคงอนุญาตให้เข้าถึง XClarity Controller ได้ ตัวอย่างสองตัวอย่างต่อไปนี้แสดงเพื่อเป็นข้อมูลให้คุณใช้อ้างอิง

- หากมีการตั้งค่ารหัสผ่านเป็น “*11111111*” (ตัวเลขแปดหลักที่มีเลข 1 แปดตัว) ผู้ใช้ยังคงสามารถเข้าถึง XClarity Controller ได้หากรหัสผ่านที่ป้อนเข้ามี 1 มากกว่าแปดตัวโดยไม่ตั้งใจ ตัวอย่างเช่น หากมีการป้อนรหัสผ่านเป็น “*1111111111* (ตัวเลขสิบหลักที่มีเลข 1 สิบตัว) ระบบจะยังคงให้สิทธิ์ในการเข้าถึงเช่นกัน สตริงที่ทำซ้ำจะถือว่ามีคีย์เดียวกัน
- หากมีการตั้งค่ารหัสผ่านเป็น “*bertbert*” ผู้ใช้ยังคงสามารถเข้าถึง XClarity Controller ได้หากป้อนรหัสเป็น “*bertbertbert*” โดยไม่ตั้งใจ รหัสผ่านทั้งสองจะถือว่ามีคีย์เดียวกัน

สำหรับรายละเอียดเพิ่มเติม โปรดดูหน้า 72 ในมาตรฐานอินเทอร์เน็ตของเอกสาร RFC 3414 (https://tools.ietf.org/html/rfc3414)

คีย์ SSH

XClarity Controller สนับสนุน SSH Public Key Authentication (ประเภทคีย์ RSA) ในการเพิ่มคีย์ SSH ไปยังบัญชีผู้ใช้ภายในระบบ ให้เลือกกล่องตัวเลือกที่อยู่ถัดจาก **คีย์ SSH** มีตัวเลือกสองรายการ ดังต่อไปนี้:

เลือกไฟล์คีย์

เลือกไฟล์คีย์ SSH ที่จะนำเข้าไปยัง XClarity Controller จากเซิร์ฟเวอร์ของคุณ

ป้อนคีย์ลงในฟิลด์ข้อความ

วางหรือป้อนข้อมูลจากคีย์ SSH ของคุณลงในฟิลด์ข้อความ

หมายเหตุ:

- เครื่องมือของ Lenovo บางอย่างอาจสร้างบัญชีผู้ใช้ชั่วคราวเพื่อเข้าถึง XClarity Controller เมื่อมีการเรียกใช้เครื่องมือบนระบบปฏิบัติการเซิร์ฟเวอร์ บัญชีชั่วคราวนี้จะไม่สามารถดูได้ และไม่ใช้ตำแหน่งใดๆ ของบัญชีผู้ใช้ภายในระบบ 12 ตำแหน่ง บัญชีถูกสร้างด้วยชื่อผู้ใช้ (ตัวอย่างเช่น “20IuN4SB”) และรหัสผ่านแบบสุ่ม สามารถใช้บัญชีในการเข้าถึง XClarity Controller บนอินเทอร์เฟซ Ethernet over USB ภายในเท่านั้น และเฉพาะสำหรับอินเทอร์เฟซ Redfish และ SFTP เท่านั้น การสร้างและการลบบัญชีชั่วคราวนี้ออกจะถูกบันทึกลงในบันทึกการตรวจสอบ เช่นเดียวกับการกระทำใดๆ ที่ดำเนินการโดยเครื่องมือที่มีข้อมูลประจำตัวเหล่านี้ด้วย
- สำหรับ SNMPv3 Engine ID ทาง XClarity Controller จะใช้สตริง HEX เพื่อระบุ ID สตริง HEX นี้ถูกแปลงมาจากชื่อโฮสต์ XClarity Controller เริ่มต้น ดูตัวอย่างด้านล่าง:

  ในขั้นแรก ชื่อโฮสต์ “XCC-7X06-S4AHJ300” จะถูกแปลงเป็นรูปแบบ ASCII: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  สตริง HEX จะถูกสร้างขึ้นโดยใช้รูปแบบ ASCII (โดยไม่สนใจช่องว่าง): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

การลบบัญชีผู้ใช้

ใช้ข้อมูลในหัวข้อนี้เพื่อลบบัญชีผู้ใช้ภายใน

ในการลบบัญชีผู้ใช้ภายในระบบ ให้คลิกไอคอนถังขยะบนแถวบัญชีที่คุณต้องการลบ หากคุณได้รับอนุญาต คุณสามารถลบบัญชีของคุณเองหรือบัญชีของผู้ใช้อื่นๆ ได้ แม้ว่าพวกเขาจะเข้าสู่ระบบอยู่ก็ตาม เว้นแต่จะเป็นเพียงบัญชีเดียวที่เหลืออยู่พร้อมสิทธิ์การจัดการบัญชีผู้ใช้ เซสชันที่กำลังดำเนินอยู่เมื่อมีการลบบัญชีผู้ใช้จะไม่สิ้นสุดโดยอัตโนมัติ

การใช้รหัสผ่านที่แฮชสำหรับการตรวจสอบความถูกต้อง

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีใช้การใช้รหัสผ่านที่แฮชสำหรับการตรวจสอบความถูกต้อง

นอกเหนือจากการใช้รหัสผ่านและบัญชีผู้ใช้ LDAP/AD XClarity Controller ยังสนับสนุนรหัสผ่านที่แฮชของบุคคลภายนอกสำหรับการตรวจสอบความถูกต้อง รหัสผ่านพิเศษจะใช้รูปแบบการเข้ารหัสด้วยฟังก์ชันแฮชแบบทางเดียว (SHA256) และได้รับการรองรับจากเว็บอินเทอร์เฟซ XClarity Controller, OneCLI และ CLI แต่อย่างไรก็ตาม โปรดตระหนักว่าการตรวจสอบความถูกต้องของอินเทอร์เฟซ XCC SNMP, IPMI และ CIM ไม่สนับสนุนรหัสผ่านที่แฮชของบุคคลภายนอก มีเพียงเครื่องมือ OneCLI และอินเทอร์เฟซ XCC CLI เท่านั้นที่สามารถสร้างบัญชีใหม่โดยใช้รหัสผ่านที่แฮชหรือทำการอัปเดตรหัสผ่านที่แฮชได้ XClarity Controller ยังช่วยให้เครื่องมือ OneCLI และอินเทอร์เฟซ XClarity Controller CLI เรียกใช้รหัสผ่านที่แฮชได้หากเปิดใช้ความสามารถในการอ่านรหัสผ่านที่แฮช

การตั้งค่ารหัสผ่านที่แฮชผ่านเว็บ XClarity Controller

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า** BMC และเลื่อนไปที่ส่วน Security Password Manager เพื่อเปิดใช้หรือปิดใช้ฟังก์ชันรหัสผ่านของบริษัทภายนอก หากเปิดใช้ ระบบจะใช้รหัสผ่านที่แฮชของบุคคลภายนอกสำหรับการ

ตรวจสอบความถูกต้องในการเข้าสู่ระบบ นอกจากนี้คุณยังสามารถเปิดใช้งานการเรียกใช้รหัสผ่านที่แฮชของบุคคลภายนอกจาก XClarity Controller ได้เช่นกัน

หมายเหตุ: ตามค่าเริ่มต้น ฟังก์ชัน *รหัสผ่านของบุคคลภายนอก* และ *การอนุญาตให้เรียกใช้รหัสผ่านที่แฮชของบุคคลภายนอก* จะถูกปิดใช้งานอยู่

หากต้องการตรวจสอบว่ารหัสผ่านของผู้ใช้เป็นแบบ *ดั้งเดิม* หรือเป็น *รหัสผ่านของบุคคลภายนอก* ให้คลิก **ผู้ใช้**/LDAP ภายใต้ **การตั้งค่า** BMC สำหรับรายละเอียดเพิ่มเติม ข้อมูลจะอยู่ภายใต้คอลัมน์ **แอตทริบิวต์ขั้นสูง**

หมายเหตุ:

- ผู้ใช้จะไม่สามารถเปลี่ยนรหัสผ่านหากเป็นรหัสผ่านของบุคคลภายนอก และฟิลด์ **รหัสผ่าน** และ **ยืนยันรหัสผ่าน** จะแสดงเป็นสีเทา
- หากรหัสผ่านของบุคคลภายนอกหมดอายุ ข้อความแจ้งเตือนจะแสดงขึ้นในระหว่างขั้นตอนการเข้าสู่ระบบของผู้ใช้

ตั้งค่ารหัสผ่านที่แฮชผ่านฟังก์ชัน OneCLI

- การเปิดใช้งานคุณลักษณะ

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- การสร้างรหัสผ่านที่แฮช (ไม่ใช้ Salt) ตัวอย่างต่อไปนี้จะแสดงการเข้าสู่ระบบ XClarity Controller โดยใช้รหัสผ่าน *password123*

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
  $ sudo OneCli config set IMM.Loginid.2 admin
  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash
  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- การสร้างผู้ใช้ด้วยรหัสผ่านที่แฮช (ใช้ Salt) ตัวอย่างต่อไปนี้จะแสดงการเข้าสู่ระบบ XClarity Controller โดยใช้รหัสผ่าน *password123* Salt=abc

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  $ sudo OneCli config set IMM.Loginid.3 Admin
  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash
  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- การเรียกใช้รหัสผ่านที่แฮชและ salt

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
  $ sudo OneCli config show IMM.SHA256Password.3
  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- การลบรหัสผ่านที่แฮชและ salt

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""
  ```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- การตั้งค่ารหัสผ่านที่แฮชในบัญชีที่มีอยู่

```
$ sudo OneCli config set IMM.Loginid.2 admin
$ sudo OneCli config set IMM.Password.2 Passw0rd123abc
$ sudo OneCli config set IMM.SHA256Password.2 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

หมายเหตุ: ในขณะที่มีการตั้งรหัสผ่านที่แฮชไว้ รหัสผ่านนี้จะมีผลทันที รหัสผ่านมาตรฐานเดิมจะไม่สามารถใช้งานได้อีกต่อไป ในตัวอย่างนี้ รหัสผ่านมาตรฐานเดิม *Passw0rd123abc* จะไม่สามารถใช้อีกต่อไปได้จนกว่ารหัสผ่านที่ถูกแฮชจะถูกลบ

ตั้งค่ารหัสผ่านที่แฮชผ่านฟังก์ชัน CLI

- การเปิดใช้งานคุณลักษณะ

```
> hashpw -sw enabled
```

- การสร้างรหัสผ่านที่แฮช (ไม่ใช้ Salt) ตัวอย่างต่อไปนี้จะแสดงการเข้าสู่ระบบ XClarity Controller โดยใช้รหัสผ่าน *password123*

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

- การสร้างผู้ใช้ด้วยรหัสผ่านที่แฮช (ใช้ Salt) ตัวอย่างต่อไปนี้จะแสดงการเข้าสู่ระบบ XClarity Controller โดยใช้รหัสผ่าน *password123* Salt=abc

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
-ssalt 'abc' -a super
```

- การเรียกใช้รหัสผ่านที่แฮชและ salt

```
> hashpw -re enabled
> users -3 -ghp -gsalt
```

- การลบรหัสผ่านที่แฮชและ salt

```
> users -3 -shp "" -ssalt ""
```

- การตั้งค่ารหัสผ่านที่แฮชในบัญชีที่มีอยู่

```
> users -2 -n admin -p Passw0rd123abc -shp
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

หมายเหตุ: ในขณะที่มีการตั้งรหัสผ่านที่แฮชไว้ รหัสผ่านนี้จะมีผลทันที รหัสผ่านมาตรฐานเดิมจะไม่สามารถใช้งานได้อีกต่อไป ในตัวอย่างนี้ รหัสผ่านมาตรฐานเดิม *Passw0rd123abc* จะไม่สามารถใช้อีกต่อไปได้จนกว่ารหัสผ่านที่ถูกแฮชจะถูกลบ

หลังจากที่มีการตั้งค่ารหัสผ่านที่แฮชแล้ว โปรดจำไว้ว่าอย่าใช้รหัสผ่านนี้เพื่อเข้าสู่ระบบ XClarity Controller เมื่อเข้าสู่ระบบ คุณจะต้องใช้รหัสผ่านแบบข้อความธรรมดา ในตัวอย่างที่แสดงด้านล่าง รหัสผ่านแบบข้อความธรรมดาคือ “password123”

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

การกำหนดค่าการตั้งค่าการเข้าสู่ระบบส่วนกลาง

ใช้ข้อมูลในหัวข้อนี้ในการกำหนดค่าการตั้งค่านโยบายการเข้าสู่ระบบและรหัสผ่านที่นำไปใช้กับผู้ใช้ทั้งหมด

การหมดเวลาเซสชันเมื่อไม่มีการใช้งานบนเว็บ

ใช้ข้อมูลในหัวข้อนี้เพื่อตั้งค่าตัวเลือกระยะเวลาการหมดเวลาของเซสชันเว็บจากการไม่ใช้งาน

ในฟิลด์ **การหมดเวลาเซสชันเมื่อไม่มีการใช้งานบนเว็บ** คุณสามารถระบุระยะเวลาเป็นนาทีที่ XClarity Controller จะรอก่อนตัดการเชื่อมต่อเซสชันบนเว็บที่ไม่มีการใช้งาน ระยะเวลารอสูงสุดคือ 1,440 นาที หากตั้งค่าไว้ที่ 0 เซสชันบนเว็บจะไม่หมดอายุ

เฟิร์มแวร์ XClarity Controller สามารถรองรับเซสชันบนเว็บได้พร้อมกันสูงสุด 6 เซสชัน เพื่อเพิ่มเซสชันว่างสำหรับการใช้งานโดยผู้ใช้อื่นๆ ขอแนะนำให้คุณออกจากระบบเซสชันบนเว็บเมื่อเสร็จสิ้นการใช้งาน แทนที่จะรอให้การหมดเวลาเซสชันเมื่อไม่มีการใช้งานปิดเซสชันให้คุณโดยอัตโนมัติ

หมายเหตุ: หากคุณออกจากเบราเซอร์ที่เปิดอยู่บนเว็บเพจ XClarity Controller ที่รีเฟรชโดยอัตโนมัติ เซสชันบนเว็บของคุณจะไม่ปิดโดยอัตโนมัติจากการที่ไม่มีการใช้งาน

การตั้งค่านโยบายการรักษาความปลอดภัยของบัญชี

ใช้ข้อมูลนี้เพื่อทำความเข้าใจและตั้งค่านโยบายการรักษาความปลอดภัยของบัญชีสำหรับเซิร์ฟเวอร์ของคุณ

หมายเหตุ: ใน Flex System การตั้งค่านโยบายการรักษาความปลอดภัยของบัญชีจะได้รับการจัดการโดย Flex System Chassis Management Module (CMM) และไม่สามารถแก้ไขผ่าน XCC ได้ เมื่อใช้ CMM เพื่อกำหนดค่านโยบายการรักษาความปลอดภัยของบัญชี โปรดทราบข้อมูลต่อไปนี้:

- ต่างจาก XCC ตรงที่ CMM ไม่มีการตั้งค่า *ระยะเวลาการแจ้งเตือนรหัสผ่านหมดอายุ (วัน)* เมื่อมีการกำหนดค่า *ระยะเวลาหมดอายุของรหัสผ่าน* ให้เป็น 5 วันขึ้นไปใน CMM ทาง XCC จะตั้งค่าระยะเวลาการแจ้งเตือนรหัสผ่านหมดให้เป็น 5 วัน ในทางกลับกัน หากมีการตั้งค่าให้เป็นน้อยกว่า 5 วัน ระยะเวลาการแจ้งเตือนรหัสผ่านหมดอายุจะเป็นค่าที่ระบุใน *ระยะเวลาหมดอายุของรหัสผ่าน*

- สำหรับการตั้งค่า *จำนวนสูงสุดของการเข้าสู่ระบบล้มเหลว (ครั้ง)* ช่วงที่กำหนดไว้ใน CMM คือ 0-100 ครั้ง อย่างไรก็ตาม ช่วงที่กำหนดไว้ใน XCC คือ 0-10 ครั้ง ดังนั้นเมื่อผู้ใช้เลือกค่าที่เกินกว่า 10 ครั้งใน CMM ทาง XCC จะยังคงตั้งค่าจำนวนสูงสุดของการเข้าสู่ระบบล้มเหลวให้เป็น 10 ครั้งอยู่ดี
- สำหรับการตั้งค่า *กรอบเวลาขั้นต่ำสำหรับการเปลี่ยนรหัสผ่าน (ชั่วโมง)* ช่วงที่กำหนดไว้ใน CMM คือ 0-1440 ชั่วโมง อย่างไรก็ตาม ช่วงที่กำหนดไว้ใน XCC คือ 0-240 ชั่วโมง ดังนั้นเมื่อผู้ใช้เลือกค่าที่เกินกว่า 240 ชั่วโมงใน CMM ทาง XCC จะยังคงตั้งค่ากรอบเวลาขั้นต่ำสำหรับการเปลี่ยนรหัสผ่านให้เป็น 240 ชั่วโมงอยู่

ข้อมูลต่อไปนี้คือรายละเอียดของฟิลด์สำหรับการตั้งค่าการรักษาความปลอดภัย

กำหนดให้เปลี่ยนรหัสผ่านเมื่อเข้าใช้งานครั้งแรก

หลังจากตั้งค่าผู้ใช้ใหม่ด้วยรหัสผ่านตามค่าเริ่มต้น การเลือกกล่องตัวเลือกนี้จะกำหนดให้ผู้ใช้ดังกล่าวเปลี่ยนรหัสผ่านของตนเมื่อผู้ใช้เข้าสู่ระบบเป็นครั้งแรก ค่าเริ่มต้นสำหรับฟิลด์นี้คือเปิดใช้กล่องตัวเลือก

ต้องใช้รหัสผ่านที่ซับซ้อน

มีการเลือกกล่องตัวเลือกตามค่าเริ่มต้นและรหัสผ่านที่ซับซ้อนต้องเป็นไปตามกฎต่อไปนี้:

- มีได้เฉพาะอักขระต่อไปนี้ (ไม่อนุญาตให้มีช่องว่างขาว): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- ต้องมีตัวอักษรอย่างน้อยหนึ่งตัว
- ต้องมีตัวเลขอย่างน้อยหนึ่งตัว
- ต้องประกอบด้วยการผสมผสานต่างๆ อย่างน้อยสองรายการต่อไปนี้:
  - มีอักษรตัวพิมพ์ใหญ่อย่างน้อยหนึ่งตัว
  - มีอักษรตัวพิมพ์เล็กอย่างน้อยหนึ่งตัว
  - ต้องมีอักขระพิเศษอย่างน้อยหนึ่งตัว
- ไม่สามารถใช้อักขระอื่นๆ ได้ (โดยเฉพาะอย่างยิ่งช่องว่างหรือช่องว่างสีขาว)
- รหัสผ่านต้องไม่มีอักขระตัวเดียวกันมากกว่าสองตัวติดกัน (เช่น “aaa”)
- รหัสผ่านต้องเป็นชื่อผู้ใช้ ซ้ำชื่อผู้ใช้อย่างน้อยหนึ่งครั้ง หรือเป็นชื่อผู้ใช้เรียงกลับด้าน
- รหัสผ่านต้องมีความยาวอย่างน้อย 8 อักขระและไม่เกิน 32 อักขระ

หากไม่ได้เลือกกล่องตัวเลือกนี้ ตัวเลขที่ระบุในความยาวขั้นต่ำของรหัสผ่านสามารถกำหนดได้เป็น 0–32 อักขระ รหัสผ่านของบัญชีอาจเว้นว่างได้ หากมีการตั้งค่าความยาวขั้นต่ำของรหัสผ่านเป็น 0

ระยะเวลาหมดอายุของรหัสผ่าน (วัน)

ฟิลด์นี้มีอายุรหัสผ่านสูงสุดที่ได้รับอนุญาตก่อนจะต้องเปลี่ยนรหัสผ่าน

ระยะเวลาการแจ้งเตือนรหัสผ่านหมดอายุ (วัน)

ฟิลด์นี้มีจำนวนวันที่ผู้ใช้ได้รับคำเตือนก่อนที่รหัสผ่านของตนจะหมดอายุ

ความยาวขั้นต่ำสำหรับรหัสผ่าน

ฟิลด์นี้มีความยาวสูงสุดของรหัสผ่าน

จำนวนรอบการใช้รหัสผ่านซ้ำ

ฟิลด์นี้มีจำนวนรหัสผ่านก่อนหน้าที่ไม่สามารถใช้ซ้ำได้

กรอบเวลาขั้นต่ำสำหรับการเปลี่ยนรหัสผ่าน (ชั่วโมง)

ฟิลด์นี้มีระยะเวลาที่ผู้ใช้ต้องรอระหว่างการเปลี่ยนรหัสผ่าน

จำนวนสูงสุดของการเข้าสู่ระบบล้มเหลว (ครั้ง)

ฟิลด์นี้มีจำนวนความพยายามในการเข้าสู่ระบบที่ล้มเหลวที่อนุญาตก่อนที่ผู้ใช้จะถูกกันไม่ให้เข้าสู่ระบบเป็นระยะเวลาหนึ่ง

ระยะเวลาการล็อคผู้ใช้จากระบบเมื่อเข้าใช้งานล้มเหลวครบจำนวนครั้งสูงสุด (นาที)

ฟิลด์นี้ระบุระยะเวลา (เป็นนาที) ที่ระบบย่อย XClarity Controller จะทำให้ไม่สามารถเข้าสู่ระบบระยะไกลเมื่อเข้าสู่ระบบล้มเหลวครบจำนวนครั้งสูงสุด

การกำหนดค่า LDAP

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือเปลี่ยนการตั้งค่า LDAP ของ XClarity Controller

การสนับสนุน LDAP ประกอบด้วย:

- การสนับสนุนสำหรับโปรโตคอล LDAP เวอร์ชัน 3 (RFC-2251)
- การสนับสนุนสำหรับ API มาตรฐานของไคลเอ็นต์ LDAP (RFC-1823)
- การสนับสนุนสำหรับรูปแบบคำสั่งตัวกรองการค้นหา LDAP มาตรฐาน (RFC-2254)
- การสนับสนุนสำหรับ Lightweight Directory Access Protocol (v3) Extension สำหรับ Transport Layer Security (RFC-2830)

การใช้งาน LDAP รองรับเซิร์ฟเวอร์ LDAP ต่อไปนี้:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)

- เซิร์ฟเวอร์ Novell eDirectory เวอร์ชัน 8.7, 8.8 และ 9.4
- เซิร์ฟเวอร์ OpenLDAP 2.1, 2.2, 2.3 และ 2.4

คลิกแท็บ **LDAP** เพื่อดูหรือแก้ไขการตั้งค่า LDAP ของ XClarity Controller

XClarity Controller สามารถตรวจสอบการเข้าถึงของผู้ใช้จากระยะไกลผ่านเซิร์ฟเวอร์ LDAP แทนหรือเพิ่มเติมจากบัญชีผู้ใช้ภายในที่จัดเก็บไว้ในตัวของ XClarity Controller เอง สามารถกำหนดสิทธิพิเศษให้กับบัญชีผู้ใช้แต่ละบัญชีโดยใช้สตริง IBMRBSPermissions คุณยังสามารถใช้เซิร์ฟเวอร์ LDAP ในการกำหนดผู้ใช้ให้กับกลุ่มและตรวจสอบความถูกต้องเป็นกลุ่ม นอกเหนือจากการตรวจสอบความถูกต้องของผู้ใช้ตามปกติ (การตรวจสอบรหัสผ่าน) ตัวอย่างเช่น คุณสามารถเชื่อมโยง XClarity Controller กับกลุ่มอย่างน้อยหนึ่งกลุ่ม ผู้ใช้จะผ่านการตรวจสอบความถูกต้องเป็นกลุ่มก็ต่อเมื่อผู้ใช้อยู่ในกลุ่มที่เชื่อมโยงกับ XClarity Controller อย่างน้อยหนึ่งกลุ่ม

ในการกำหนดค่าเซิร์ฟเวอร์ LDAP ให้ดำเนินการขั้นตอนต่อไปนี้:

1. ภายใต้ **ข้อมูลเซิร์ฟเวอร์ LDAP** จะมีตัวเลือกจากรายการดังต่อไปนี้:
   - **ใช้เซิร์ฟเวอร์ LDAP สำหรับการตรวจสอบความถูกต้องเท่านั้น (พร้อมการอนุญาตภายใน)**: การเลือกนี้จะกำหนดให้ XClarity Controller ใช้ข้อมูลประจำตัวเฉพาะในการตรวจสอบเซิร์ฟเวอร์ LDAP และรับข้อมูลความเป็นสมาชิกของกลุ่ม คุณสามารถกำหนดชื่อและสิทธิพิเศษของกลุ่มในส่วนการตั้งค่า Active Directory
   - **ใช้เซิร์ฟเวอร์ LDAP สำหรับการตรวจสอบความถูกต้องและการอนุญาต**: การเลือกนี้จะกำหนดให้ XClarity Controller ใช้ข้อมูลประจำตัวทั้งในการตรวจสอบเซิร์ฟเวอร์ LDAP และระบุสิทธิ์ของผู้ใช้

   หมายเหตุ: คุณสามารถกำหนดค่าเซิร์ฟเวอร์ LDAP ที่จะใช้สำหรับการตรวจสอบความถูกต้องได้ด้วยตนเอง หรือค้นหาผ่านระเบียน DNS SRV แบบไดนามิก

   - **ใช้เซิร์ฟเวอร์ที่กำหนดค่าไว้ล่วงหน้า**: คุณสามารถกำหนดค่าเซิร์ฟเวอร์ LDAP สูงสุดสี่เซิร์ฟเวอร์โดยป้อนที่อยู่ IP หรือชื่อโฮสต์ของแต่ละเซิร์ฟเวอร์ หากเปิดใช้งาน DNS หมายเลขพอร์ตสำหรับแต่ละเซิร์ฟเวอร์จะระบุหรือไม่ก็ได้ หากฟิลด์นี้เว้นว่างไว้ ระบบจะใช้ค่าเริ่มต้นที่ 389 สำหรับการเชื่อมต่อ LDAP ที่ไม่มีการรักษาความปลอดภัย สำหรับการเชื่อมต่อที่มีการรักษาความปลอดภัย ค่าพอร์ตเริ่มต้นคือ 636 คุณต้องกำหนดค่าเซิร์ฟเวอร์ LDAP อย่างน้อยหนึ่งเซิร์ฟเวอร์
   - **ใช้ DNS เพื่อค้นหาเซิร์ฟเวอร์**: คุณสามารถเลือกค้นหาเซิร์ฟเวอร์ LDAP แบบไดนามิก กลไกที่อธิบายใน RFC2782 (DNS RR สำหรับระบุตำแหน่งที่ตั้งของบริการ) จะใช้ในการค้นหาเซิร์ฟเวอร์ LDAP ซึ่งเรียกว่า DNS SRV คุณต้องระบุชื่อโดเมนที่มีคุณสมบัติครบถ้วน (FQDN) ที่จะใช้เป็นชื่อโดเมนในคำขอ DNS SRV
     - **ฟอเรสต์** AD: ในสภาพแวดล้อมที่มีกลุ่มสากลข้ามโดเมน ต้องกำหนดค่าชื่อฟอเรสต์ (ชุดโดเมน) เพื่อค้นหา Global Catalogs (GC) ที่ต้องการ ในสภาพแวดล้อมที่ไม่มีการสมัครสมาชิกกลุ่มข้ามโดเมน ฟิลด์นี้สามารถเว้นว่างไว้ได้

– **โดเมน AD**: คุณต้องระบุชื่อโดเมนที่มีคุณสมบัติครบถ้วน (FQDN) ที่จะใช้เป็นชื่อโดเมนในคำขอ DNS SRV

หากคุณต้องการเปิดใช้งาน LDAP ที่มีความปลอดภัย ให้คลิกกล่องตัวเลือก **เปิดใช้งาน LDAP ที่มีความปลอดภัย** เพื่อรองรับ LDAP ที่มีความปลอดภัย ต้องมีการใช้ใบรับรอง SSL ที่ถูกต้องและต้องนำเข้าใบรับรองที่เชื่อถือได้ของไคลเอ็นต์ SSL ใน XClarity Controller เซิร์ฟเวอร์ LDAP ของคุณต้องรองรับ Transport Layer Security (TLS) เวอร์ชัน 1.2 เพื่อให้เข้ากันได้กับไคลเอ็นต์ LDAP ที่มีความปลอดภัยของ XClarity Controller ดูข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมดูแลใบรับรองได้ที่ "การควบคุมดูแลใบรับรอง SSL" บนหน้าที่ 56

2. กรอกข้อมูลภายใต้ **พารามิเตอร์เพิ่มเติม** ด้านล่างนี้คือคำอธิบายของพารามิเตอร์

วิธีการ Binding

ก่อนที่คุณจะสามารถค้นหาหรือสืบค้นเซิร์ฟเวอร์ LDAP คุณต้องส่งคำขอสำหรับการผูก ฟิลด์นี้จะควบคุมวิธีการดำเนินการผูกเริ่มต้นกับเซิร์ฟเวอร์ LDAP วิธีการผูกมีดังต่อไปนี้:

- **ไม่จำเป็นต้องใช้ข้อมูลประจำตัว**

  ใช้วิธีนี้ในการผูกโดยไม่ต้องมีชื่อที่ใช้ระบุ (DN) หรือรหัสผ่าน ไม่แนะนำให้ใช้วิธีนี้เนื่องจากเซิร์ฟเวอร์ส่วนใหญ่ได้รับการกำหนดค่าไม่ให้อนุญาตคำขอค้นหาบนระเบียนผู้ใช้ที่เฉพาะเจาะจง

- **ใช้ข้อมูลประจำตัวที่กำหนดค่า**

  ใช้วิธีนี้ในการผูกกับ DN ของไคลเอ็นต์หรือรหัสผ่านที่กำหนดค่า

- **ใช้ข้อมูลประจำตัวสำหรับการเข้าสู่ระบบ**

  ใช้วิธีนี้ในการผูกกับข้อมูลประจำตัวที่ให้มาระหว่างขั้นตอนการเข้าสู่ระบบ สามารถระบุ ID ผู้ใช้ผ่าน DN, DN บางส่วน, ชื่อโดเมนที่มีคุณสมบัติครบถ้วน หรือผ่าน ID ผู้ใช้ที่ตรงกับแอตทริบิวต์การค้นหา UID ที่ได้รับการกำหนดค่าบน XClarity Controller หากข้อมูลประจำตัวที่ปรากฏคล้ายคลึงกับ DN บางส่วน (เช่น cn=joe) DN บางส่วนนี้จะขึ้นต้นด้วย DN รูทที่กำหนดค่าในความพยายามที่จะสร้าง DN ที่ตรงกับระเบียนของผู้ใช้ หากความพยายามในการผูกล้มเหลว ระบบจะดำเนินความพยายามครั้งสุดท้ายเพื่อทำการผูกโดยเติม cn= นำหน้าข้อมูลประจำตัวสำหรับการเข้าสู่ระบบ และเติมสตริงผลลัพธ์นำหน้า DN รูทที่กำหนดค่า

หากการผูกเริ่มต้นเสร็จสิ้น ระบบจะดำเนินการค้นหาเพื่อหารายการบนเซิร์ฟเวอร์ LDAP ที่เป็นของผู้ใช้ที่เข้าสู่ระบบ หากจำเป็น ระบบจะดำเนินความพยายามในการผูกครั้งที่สอง ครั้งนี้จะผูกกับ DN ที่เรียกใช้จากระเบียน LDAP ของผู้ใช้ และรหัสผ่านที่ป้อนระหว่างขั้นตอนการเข้าสู่ระบบ หากความพยายามในการผูกครั้งที่สองล้มเหลว ผู้ใช้จะถูกปฏิเสธการเข้าถึง ระบบจะดำเนินการผูกครั้งที่สองเฉพาะเมื่อใช้วิธีการผูกแบบ **ไม่จำเป็นต้องใช้ข้อมูลประจำตัว** หรือ **ใช้ข้อมูลประจำตัวที่กำหนดค่า** เท่านั้น

ชื่อที่ใช้ระบุรูท (DN)

นี่คือชื่อที่ใช้ระบุ (DN) ของรายการรูทของโครงสร้างไดเรกทอรีบนเซิร์ฟเวอร์ LDAP (ตัวอย่างเช่น dn= mycompany,dc=com) DN นี้จะใช้เป็นออบเจกต์ฐานสำหรับคำขอค้นหาทั้งหมด

แอตทริบิวต์การค้นหา UID

เมื่อตั้งค่าวิธีการผูกเป็น **ไม่จำเป็นต้องใช้ข้อมูลประจำตัว** หรือ **ใช้ข้อมูลประจำตัวที่กำหนดค่า** การผูกกับเซิร์ฟเวอร์ LDAP เริ่มต้นจะตามด้วยคำขอการค้นหาที่เรียกใช้ข้อมูลเฉพาะเกี่ยวกับผู้ใช้ รวมถึง DN ของผู้ใช้ สิทธิ์การเข้าสู่ระบบ และสมาชิกกลุ่ม คำขอค้นหานี้ต้องระบุชื่อแอตทริบิวต์ที่แสดงแทน ID ผู้ใช้บนเซิร์ฟเวอร์ ชื่อแอตทริบิวต์นี้ได้รับการกำหนดค่าในฟิลด์นี้ บนเซิร์ฟเวอร์ Active Directory โดยปกติแล้ว ชื่อแอตทริบิวต์คือ **sAMAccountName** บนเซิร์ฟเวอร์ Novell eDirectory และ OpenLDAP ชื่อแอตทริบิวต์คือ **uid** หากฟิลด์นี้เว้นว่างไว้ ค่าเริ่มต้นคือ **uid**

ตัวกรองกลุ่ม

ฟิลด์ **ตัวกรองกลุ่ม** จะใช้สำหรับการตรวจสอบความถูกต้องเป็นกลุ่ม ระบบจะพยายามทำการตรวจสอบความถูกต้องเป็นกลุ่มหลังจากมีการตรวจสอบข้อมูลประจำตัวของผู้ใช้เสร็จสิ้นแล้ว หากการตรวจสอบความถูกต้องเป็นกลุ่มล้มเหลว ความพยายามของผู้ใช้ในการเข้าสู่ระบบจะถูกปฏิเสธ เมื่อมีการกำหนดค่าตัวกรองกลุ่ม ตัวกรองจะใช้ระบุว่า XClarity Controller อยู่ในกลุ่มใด นั่นหมายความว่าการดำเนินการนี้จะสำเร็จได้ก็ต่อเมื่อผู้ใช้ต้องอยู่ในกลุ่มที่ได้รับการกำหนดค่าสำหรับการตรวจสอบความถูกต้องเป็นกลุ่มอย่างน้อยหนึ่งกลุ่ม หากฟิลด์ **ตัวกรองกลุ่ม** เว้นว่างไว้ การตรวจสอบความถูกต้องเป็นกลุ่มจะสำเร็จโดยอัตโนมัติ หากกำหนดค่าตัวกรองกลุ่ม ระบบจะพยายามจับคู่กลุ่มในรายการอย่างน้อยหนึ่งกลุ่มกับกลุ่มที่ผู้ใช้อยู่ หากไม่มีกลุ่มที่ตรงกัน ผู้ใช้จะไม่สามารถตรวจสอบความถูกต้องและการเข้าถึงจะถูกปฏิเสธ หากมีกลุ่มที่ตรงกันอย่างน้อยหนึ่งกลุ่ม การตรวจสอบความถูกต้องเป็นกลุ่มจะเสร็จสมบูรณ์
การเปรียบเทียบจะพิจารณาตัวพิมพ์เล็ก-ใหญ่ ตัวกรองจะถูกจำกัดไว้ที่ 511 อักขระ และสามารถประกอบด้วยชื่อกลุ่มอย่างน้อยหนึ่งกลุ่ม ต้องใช้อักขระเครื่องหมายโคลอน (:) คั่นชื่อกลุ่มหลายรายการ ช่องว่างด้านหน้าและด้านหลังจะถูกละเว้น แต่ช่องว่างในส่วนอื่นๆ จะถือว่าเป็นส่วนหนึ่งของชื่อกลุ่ม

หมายเหตุ: อักขระตัวแทน (*) จะไม่ถือว่าเป็นอักขระตัวแทนอีกต่อไป แนวคิดของอักขระตัวแทนถูกยกเลิกแล้วเพื่อป้องกันไม่ให้เกิดความเสี่ยงด้านการรักษาความปลอดภัย สามารถระบุชื่อกลุ่มเป็น DN แบบเต็มหรือโดยใช้เฉพาะส่วน *cn* เท่านั้น ตัวอย่างเช่น กลุ่มที่มี DN เป็น cn=adminGroup, dc=mycompany, dc=com สามารถระบุได้โดยใช้ DN ตามจริงหรือพร้อมกับ adminGroup

ความเป็นสมาชิกกลุ่มที่ซ้อนกันได้รับการรองรับเฉพาะในสภาพแวดล้อม Active Directory เท่านั้น ตัวอย่างเช่น หากผู้ใช้เป็นสมาชิกของ GroupA และ GroupB แล้ว GroupA ยังเป็นสมาชิกของ GroupC ด้วย จะถือว่าผู้ใช้เป็นสมาชิกของ GroupC เช่นกัน การค้นหาที่ซ้อนกันจะหยุด หากค้นหากลุ่มครบ 128 กลุ่ม กลุ่มในหนึ่งระดับจะถูกค้นหาก่อนกลุ่มในระดับที่ต่ำกว่า การวนซ้ำจะไม่ถูกตรวจพบ

แอตทริบิวต์การค้นหากลุ่ม

ในสภาพแวดล้อม Active Directory หรือ Novell eDirectory ฟิลด์ **แอตทริบิวต์การค้นหากลุ่ม** จะระบุชื่อแอตทริบิวต์ที่ใช้ในการระบุกลุ่มที่ผู้ใช้อยู่ ในสภาพแวดล้อม Active Directory ชื่อแอตทริบิวต์คือ **memberOf**

ในสภาพแวดล้อม eDirectory ชื่อแอตทริบิวต์คือ **groupMembership** ในสภาพแวดล้อมของเซิร์ฟเวอร์ OpenLDAP โดยปกติแล้ว ผู้ใช้จะถูกกำหนดไปยังกลุ่มที่มี objectClass เท่ากับ PosixGroup ในบริบทดังกล่าว ฟิลด์นี้จะระบุชื่อแอตทริบิวต์ที่ใช้ในการระบุสมาชิกของ PosixGroup โดยเฉพาะ ชื่อแอตทริบิวต์นี้คือ **memberUid** หากฟิลด์นี้เว้นว่างไว้ ชื่อแอตทริบิวต์ในตัวกรองจะกลับไปเป็น **memberOf** ตามค่าเริ่มต้น

แอตทริบิวต์สิทธิ์การเข้าใช้งาน

เมื่อผู้ใช้ได้รับการตรวจสอบความถูกต้องผ่านเซิร์ฟเวอร์ LDAP เสร็จสมบูรณ์แล้ว ต้องเรียกใช้สิทธิ์การเข้าสู่ระบบสำหรับผู้ใช้ ในการเรียกใช้สิทธิ์การเข้าสู่ระบบ ตัวกรองการค้นหาที่ส่งไปยังเซิร์ฟเวอร์ต้องระบุชื่อแอตทริบิวต์ที่เกี่ยวข้องกับสิทธิ์การเข้าสู่ระบบ ฟิลด์ **Login Permission Attribute** ระบุชื่อแอตทริบิวต์ หากฟิลด์นี้เว้นว่างไว้ ผู้ใช้จะถูกกำหนดสิทธิ์แบบอ่านอย่างเดียวตามค่าเริ่มต้น โดยถือว่าผู้ใช้ผ่านการตรวจสอบความถูกต้องของผู้ใช้และกลุ่ม

ค่าแอตทริบิวต์ที่ส่งกลับโดยเซิร์ฟเวอร์ LDAP จะค้นหาสตริงคำสำคัญ IBMRBSPermissions= สตริงคำสำคัญนี้ต้องตามด้วยสตริงบิตโดยป้อนเป็นเลข 0 หรือ 1 ติดต่อกัน 12 ตัว แต่ละบิตจะแสดงแทนชุดของฟังก์ชัน บิตจะกำกับด้วยตัวเลขตามตำแหน่งของบิต บิตด้านซ้ายสุดคือตำแหน่งบิต 0 และบิตด้านขวาสุดคือตำแหน่งบิต 11 ค่าของ 1 ที่ตำแหน่งบิตจะเปิดใช้งานฟังก์ชันที่เกี่ยวข้องกับตำแหน่งบิตนั้น ค่าของ 0 ที่ตำแหน่งบิตจะปิดใช้งานฟังก์ชันที่เกี่ยวข้องกับตำแหน่งบิตนั้น

สตริง IBMRBSPermissions=010000000000 คือตัวอย่างที่ถูกต้อง คำสำคัญ IBMRBSPermissions= ใช้เพื่ออนุญาตให้วางคำสำคัญนี้ไว้ที่ตำแหน่งใดก็ได้ในฟิลด์นี้ ซึ่งทำให้ผู้ดูแลระบบ LDAP สามารถใช้แอตทริบิวต์ที่มีอยู่ซ้ำ ซึ่งเป็นการป้องกันการต่อขยายสคีม่า LDAP และยังทำให้สามารถใช้แอตทริบิวต์เพื่อวัตถุประสงค์ดั้งเดิมของแอตทริบิวต์ คุณสามารถเพิ่มสตริงคำสำคัญที่ตำแหน่งใดก็ได้ในฟิลด์นี้ แอตทริบิวต์ที่คุณใช้สามารถอนุญาตให้ใช้สตริงที่มีรูปแบบอิสระ เมื่อเรียกใช้แอตทริบิวต์เสร็จสมบูรณ์แล้ว ระบบจะตีความค่าที่ส่งกลับโดยเซิร์ฟเวอร์ LDAP ตามข้อมูลในตารางต่อไปนี้

ตาราง 2. บิตที่อนุญาต

ตารางสามคอลัมน์ที่มีคำอธิบายเกี่ยวกับตำแหน่งบิต

ตำแหน่งบิต	ฟังก์ชัน	คำอธิบาย
0	ปฏิเสธเสมอ	ผู้ใช้จะไม่ผ่านการตรวจสอบความถูกต้องเสมอ สามารถใช้ฟังก์ชันนี้เพื่อบล็อกผู้ใช้เฉพาะราย หรือผู้ใช้ที่เกี่ยวข้องกับกลุ่มๆ หนึ่งโดยเฉพาะ
1	สิทธิ์การเข้าถึงระดับผู้ควบคุม	ผู้ใช้ได้รับสิทธิพิเศษของผู้ดูแลระบบ ผู้ใช้มีสิทธิ์เข้าถึงทุกฟังก์ชันแบบอ่าน/เขียน หากคุณตั้งค่าบิตนี้ คุณไม่ต้องตั้งค่าบิตอื่นๆ แต่ละบิต

ตาราง 2. บิตที่อนุญาต (มีต่อ)

ตำแหน่งบิต	ฟังก์ชัน	คำอธิบาย
2	สิทธิ์การเข้าถึงแบบอ่านอย่างเดียว	ผู้ใช้มีสิทธิ์การเข้าถึงแบบอ่านอย่างเดียว และไม่สามารถดำเนินการกระบวนการบำรุงรักษา (ตัวอย่างเช่น รีสตาร์ท การดำเนินการระยะไกล หรือการอัปเดตเฟิร์มแวร์) หรือทำการแก้ไข (ตัวอย่างเช่น บันทึก ล้างข้อมูล หรือคืนค่าฟังก์ชัน) ตำแหน่งบิตที่ 2 และบิตอื่นๆ ทั้งหมดจะไม่เกิดขึ้นพร้อมกัน โดยที่ตำแหน่งบิตที่ 2 มีลำดับความสำคัญต่ำสุด เมื่อตั้งค่าบิตอื่นๆ ทั้งหมด บิตนี้จะถูกละทิ้ง
3	การเชื่อมโยงเครือข่ายและการรักษาความปลอดภัย	ผู้ใช้สามารถแก้ไขการรักษาความปลอดภัย โปรโตคอลเครือข่าย อินเทอร์เฟซเครือข่าย การกำหนดพอร์ต และการกำหนดค่าพอร์ตอนุกรม
4	การจัดการบัญชีผู้ใช้	ผู้ใช้สามารถเพิ่ม แก้ไข หรือลบผู้ใช้ รวมทั้งเปลี่ยนการตั้งค่าการเข้าสู่ระบบแบบส่วนกลางในหน้าต่างโปรไฟล์การเข้าสู่ระบบ
5	การเข้าถึงคอนโซลระยะไกล	ผู้ใช้สามารถเข้าถึงคอนโซลเซิร์ฟเวอร์ระยะไกลได้
6	การเข้าถึงคอนโซลระยะไกลและดิสก์ระยะไกล	ผู้ใช้สามารถเข้าถึงคอนโซลเซิร์ฟเวอร์ระยะไกลและฟังก์ชันของดิสก์ระยะไกลสำหรับเซิร์ฟเวอร์ระยะไกล
7	การเข้าถึงการเปิด/รีสตาร์ทเซิร์ฟเวอร์จากระยะไกล	ผู้ใช้สามารถเข้าถึงฟังก์ชันการเปิดเครื่องและรีสตาร์ทเซิร์ฟเวอร์จากระยะไกล
8	การกำหนดค่าอะแดปเตอร์พื้นฐาน	ผู้ใช้สามารถแก้ไขพารามิเตอร์การกำหนดค่าในหน้าต่าง System Settings และ Alerts
9	ความสามารถในการล้างข้อมูลบันทึกเหตุการณ์	ผู้ใช้สามารถล้างข้อมูลบันทึกเหตุการณ์ **หมายเหตุ**: ผู้ใช้ทุกรายสามารถดูบันทึกเหตุการณ์ได้ แต่จะต้องมีสิทธิ์ในระดับนี้จึงจะล้างข้อมูลบันทึกเหตุการณ์ได้

ตาราง 2. บิตที่อนุญาต (มีต่อ)

ตำแหน่งบิต	ฟังก์ชัน	คำอธิบาย
10	การกำหนดค่าอะแดปเตอร์ขั้นสูง	ผู้ใช้ไม่มีข้อจำกัดเมื่อกำหนดค่า XClarity Controller นอกจากนี้ ผู้ใช้จะมีสิทธิ์การเข้าถึงด้านการดูแลเพื่อใช้งาน XClarity Controller ผู้ใช้สามารถดำเนินการฟังก์ชันขั้นสูงดังไปนี้: อัปเกรดเฟิร์มแวร์, บูตเครือข่าย PXE, คืนค่า XClarity Controller เป็นค่าเริ่มต้นจากโรงงาน, แก้ไขและคืนค่าการกำหนดค่าอะแดปเตอร์จากไฟล์การกำหนดค่า และรีสตาร์ทและรีเซ็ต XClarity Controller
11	สงวนไว้	ตำแหน่งบิตนี้สงวนไว้สำหรับการใช้งานในอนาคต หากไม่มีการตั้งค่าบิต ผู้ใช้จะมีสิทธิ์แบบอ่านอย่างเดียว ระบบจะให้ความสำคัญกับสิทธิ์การเข้าสู่ระบบที่เรียกใช้จากระเบียนของผู้ใช้โดยตรง หากแอตทริบิวต์ของสิทธิ์การเข้าสู่ระบบไม่อยู่ในระเบียนของผู้ใช้ ระบบจะพยายามเรียกใช้สิทธิ์จากกลุ่มที่ผู้ใช้อยู่ ซึ่งดำเนินการโดยเป็นส่วนหนึ่งของระยะการตรวจสอบความถูกต้องเป็นกลุ่ม ระบบจะกำหนด inclusive OR ของบิตทั้งหมดสำหรับกลุ่มทุกกลุ่มให้ผู้ใช้ บิต สิทธิ์การเข้าถึงแบบอ่านอย่างเดียว (ตำแหน่ง 2) ได้รับการตั้งค่าเฉพาะเมื่อมีการตั้งค่าบิตอื่นๆ ทั้งหมดเป็น 0 เท่านั้น หากมีการตั้งค่าบิตปฏิเสธเสมอ (ตำแหน่ง 0) สำหรับกลุ่มใดๆ ผู้ใช้จะถูกปฏิเสธการเข้าถึง บิต ปฏิเสธเสมอ (ตำแหน่ง 0) มีความสำคัญเหนือกว่าบิตอื่นๆ ทั้งหมดเสมอ

หากไม่มีการตั้งค่าบิต ระบบจะตั้งค่าเริ่มต้นเป็น **อ่านอย่างเดียว** ให้กับผู้ใช้

โปรดทราบว่าระบบจะให้ความสำคัญกับสิทธิ์การเข้าสู่ระบบที่เรียกใช้จากระเบียนของผู้ใช้โดยตรง หากผู้ใช้ไม่มีแอตทริบิวต์สิทธิ์การเข้าใช้งานในระเบียน ระบบจะพยายามเรียกใช้สิทธิ์จากกลุ่มที่ผู้ใช้อยู่ และตรงกับตัวกรองกลุ่ม หากมีการกำหนดค่า ในกรณีนี้ ระบบจะกำหนด inclusive OR ของบิตทั้งหมดสำหรับกลุ่มทุกกลุ่มให้ผู้ใช้ในทำนองเดียวกัน บิต **สิทธิ์การเข้าถึงแบบอ่านอย่างเดียว** จะได้รับการตั้งค่าเฉพาะเมื่อบิตอื่นๆ ทั้งหมดเป็น 0 เท่านั้น นอกจากนี้ โปรดทราบว่าหากมีการตั้งค่าบิต **ปฏิเสธเสมอ** สำหรับกลุ่มใดๆ ผู้ใช้จะถูกปฏิเสธการเข้าถึง บิต **ปฏิเสธเสมอ** มีความสำคัญเหนือกว่าบิตอื่นๆ ทุกบิต

หมายเหตุ: หากคุณมอบความสามารถในการแก้ไขพารามิเตอร์การกำหนดค่าอะแดปเตอร์ที่เกี่ยวข้องกับข้อมูลพื้นฐาน เครือข่าย และ/หรือการรักษาความปลอดภัยให้ผู้ใช้ คุณควรพิจารณามอบความสามารถในการรีสตาร์ท XClarity Controller (บิตตำแหน่ง 10) ให้กับผู้ใช้รายเดียวกันนี้ด้วย หากไม่มีความสามารถนี้ ผู้ใช้อาจจะ

เปลี่ยนแปลงพารามิเตอร์ได้ (ตัวอย่างเช่น ที่อยู่ IP ของอะแดปเตอร์) แต่จะไม่สามารถทำให้พารามิเตอร์มีผลใช้งานได้

3. เลือกว่าจะ **เปิดใช้งานการรักษาความปลอดภัยตามบทบาทที่ปรับปรุงสำหรับผู้ใช้** Active Directory ภายใต้ **การตั้งค่า** Active Directory (หากใช้โหมด **ใช้เซิร์ฟเวอร์** LDAP **สำหรับการตรวจสอบความถูกต้องและการอนุญาต**) หรือกำหนดค่า **กลุ่มสำหรับการอนุญาตภายใน** (หากใช้โหมด **ใช้เซิร์ฟเวอร์** LDAP **สำหรับการตรวจสอบความถูกต้องเท่านั้น** (**พร้อมการอนุญาตภายใน**))

   - **เปิดใช้งานการรักษาความปลอดภัยตามบทบาทที่ปรับปรุงสำหรับผู้ใช้** Active Directory

     หากเปิดใช้งานการตั้งค่าการรักษาความปลอดภัยตามบทบาทที่ปรับปรุง ต้องกำหนดค่าชื่อเซิร์ฟเวอร์ที่มีรูปแบบอิสระให้ทำหน้าที่เป็นชื่อเป้าหมายสำหรับ XClarity Controller โดยเฉพาะนี้ ชื่อเป้าหมายสามารถเชื่อมโยงกับบทบาทอย่างน้อยหนึ่งรายการบนเซิร์ฟเวอร์ Active Directory ผ่านเครื่องมือ Snap-In ของระบบการรักษาความปลอดภัยตามบทบาท (RBS) ซึ่งสามารถดำเนินการได้โดยสร้างเป้าหมายที่มีการจัดการ ระบุชื่อที่เฉพาะเจาะจง แล้วเชื่อมโยงกับบทบาทที่เหมาะสม หากมีการกำหนดค่าชื่อในฟิลด์นี้ ก็จะให้ความสามารถในการกำหนดบทบาทเฉพาะสำหรับผู้ใช้และ XClarity Controller (เป้าหมาย) ที่เป็นสมาชิกของบทบาทเดียวกัน เมื่อผู้ใช้เข้าสู่ระบบ XClarity Controller และได้รับการตรวจสอบความถูกต้องผ่าน Active Directory ระบบจะเรียกใช้บทบาทที่ผู้ใช้เป็นสมาชิกจากไดเรกทอรี สิทธิ์ที่กำหนดให้กับผู้ใช้จะถูกแยกออกจากบทบาทที่มีในฐานะสมาชิกเป้าหมายที่ตรงกับชื่อเซิร์ฟเวอร์ที่ได้รับการกำหนดค่าที่นี่ หรือเป้าหมายที่ตรงกับ XClarity Controller ใดๆ XClarity Controller หลายตัวสามารถใช้ชื่อเป้าหมายเดียวกันได้ ซึ่งสามารถใช้เพื่อจัดกลุ่ม XClarity Controller หลายรายการเข้าด้วยกัน และกำหนดให้กับบทบาทเดียวกัน (หรือหลายบทบาท) โดยใช้เป้าหมายเดี่ยวที่มีการจัดการ ในทางกลับกัน สามารถตั้งชื่อที่ไม่ซ้ำกันให้กับ XClarity Controller แต่ละรายการได้

   - **กลุ่มสำหรับการอนุญาตภายใน**

     มีการกำหนดค่าชื่อกลุ่มเพื่อให้ข้อมูลจำเพาะเกี่ยวกับการอนุญาตภายในสำหรับกลุ่มของผู้ใช้ คุณสามารถกำหนดสิทธิ์ (บทบาท) ที่เหมือนกับที่อธิบายไว้ในตารางข้างต้นให้กับชื่อกลุ่มแต่ละรายการ เซิร์ฟเวอร์ LDAP เชื่อมโยงผู้ใช้กับชื่อกลุ่ม เมื่อผู้ใช้เข้าสู่ระบบ ระบบจะกำหนดสิทธิ์ที่เชื่อมโยงกับกลุ่มที่ผู้ใช้อยู่ให้กับผู้ใช้คนดังกล่าว สามารถกำหนดค่ากลุ่มเพิ่มเติมได้โดยคลิกไอคอน “+” หรือลบโดยคลิกไอคอน “x”

การกำหนดค่าโปรโตคอลเครือข่าย

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือสร้างการตั้งค่าเครือข่ายสำหรับ XClarity Controller

การกำหนดค่าการตั้งค่าอีเทอร์เน็ต

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือเปลี่ยนวิธีที่ XClarity Controller สื่อสารด้วยวิธีการเชื่อมต่ออีเทอร์เน็ต

หมายเหตุ: เซิร์ฟเวอร์ AMD ไม่รองรับฟังก์ชันการป้องกันการทำงานล้มเหลวของอีเทอร์เน็ต

XClarity Controller ใช้ตัวควบคุมเครือข่ายจำนวนสองชุด โดยตัวควบคุมเครือข่ายชุดหนึ่งจะเชื่อมต่อกับพอร์ตการจัดการแบบเฉพาะ และตัวควบคุมอีกตัวหนึ่งทำหน้าที่เชื่อมต่อกับพอร์ตที่ใช้ร่วมกัน ตัวควบคุมเครือข่ายแต่ละชุดจะมีการระบุ Burned-in MAC Address ของตนเอง หากมีการใช้ DHCP เพื่อกำหนดที่อยู่ IP ให้กับ XClarity Controller เมื่อผู้ใช้สลับระหว่างพอร์ตเครือข่าย หรือหากเกิดการทำงานล้มเหลวจากพอร์ตเครือข่ายแบบเฉพาะไปยังพอร์ตเครือข่ายที่ใช้งานร่วมกัน เซิร์ฟเวอร์ DHCP อาจกำหนดที่อยู่ IP ที่แตกต่างกันให้กับ XClarity Controller หากมีการใช้งาน DHCP ขอแนะนำให้ผู้ใช้เลือกใช้ชื่อโฮสต์เพื่อเข้าถึง XClarity Controller แทนการใช้งานที่อยู่ IP แม้ว่าพอร์ตเครือข่าย XClarity Controller จะไม่เปลี่ยนแปลง แต่เซิร์ฟเวอร์ DHCP อาจกำหนดที่อยู่ IP ที่แตกต่างกันให้กับ XClarity Controller เมื่อสิ้นสุดระยะการเช่า DHCP หรือเมื่อรีบูต XClarity Controller หากผู้ใช้จำเป็นต้องเข้าถึง XClarity Controller โดยใช้ที่อยู่ IP ที่ไม่เปลี่ยนแปลง ควรกำหนดค่า XClarity Controller สำหรับที่อยู่ IP แบบคงที่แทนการใช้งาน DHCP

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อแก้ไขการตั้งค่าอีเทอร์เน็ตของ XClarity Controller

การกำหนดค่าชื่อโฮสต์ของ XClarity Controller

ชื่อโฮสต์ของ XClarity Controller ตามค่าเริ่มต้นถูกสร้างขึ้นโดยใช้การผสมผสานสตริง “XCC -”ตามด้วยประเภทเครื่องเซิร์ฟเวอร์และหมายเลขประจำเครื่องของเซิร์ฟเวอร์ (ตัวอย่างเช่น “XCC-7X03-1234567890”) คุณสามารถเปลี่ยนชื่อโฮสต์ของ XClarity Controller โดยป้อนอักขระความยาวไม่เกิน 63 ตัวในฟิลด์นี้ ชื่อโฮสต์ต้องไม่มีเครื่องหมายมหัพภาค (.) และมีได้เฉพาะอักขระที่เป็นตัวอักษร ตัวเลข ยัติภังค์ และขีดล่างเท่านั้น

พอร์ตอีเทอร์เน็ต

การตั้งค่านี้จะควบคุมพอร์ตอีเทอร์เน็ตที่ใช้โดยตัวควบคุมการจัดการ รวมถึงพอร์ตที่ใช้ร่วมกันและพอร์ตเฉพาะ

เมื่อ **ปิดใช้งาน** พอร์ตอีเทอร์เน็ตทั้งหมดจะไม่ได้รับการกำหนดที่อยู่ IPv4 หรือ IPv6 และจะป้องกันไม่ให้มีการเปลี่ยนแปลงการกำหนดค่าอีเทอร์เน็ตใดๆ เพิ่มเติม

หมายเหตุ: การตั้งค่านี้จะไม่มีผลกระทบต่ออินเทอร์เฟซ USB LAN หรือพอร์ตการจัดการ USB ที่ด้านหน้าของเซิร์ฟเวอร์ อินเทอร์เฟซดังกล่าวมีการตั้งค่าการเปิดใช้งานเฉพาะของตนเอง

การกำหนดค่าการตั้งค่าเครือข่าย IPv4

ในการใช้การเชื่อมต่ออีเทอร์เน็ต IPv4 ให้ดำเนินการขั้นตอนต่อไปนี้:

1. เปิดใช้งานตัวเลือก **IPv4**

   หมายเหตุ: การปิดใช้งานอินเทอร์เฟซอีเทอร์เน็ตจะป้องกันการเข้าถึง XClarity Controller จากเครือข่ายภายนอก

2. จากฟิลด์ **วิธีการ** ให้เลือกตัวเลือกใดตัวเลือกหนึ่งต่อไปนี้:

   - **รับ IP จาก DHCP**: XClarity Controller จะรับที่อยู่ IPv4 จากเซิร์ฟเวอร์ DHCP
   - **ใช้ที่อยู่ IP แบบคงที่**: XClarity Controller จะใช้ค่าที่ระบุโดยผู้ใช้สำหรับที่อยู่ IPv4

- **DHCP ก่อน แล้วตามด้วยที่อยู่ IP แบบคงที่**: XClarity Controller จะพยายามรับที่อยู่ IPv4 จากเซิร์ฟเวอร์ DHCP แต่หากความพยายามดังกล่าวล้มเหลว XClarity Controller จะใช้ค่าที่ระบุโดยผู้ใช้สำหรับที่อยู่ IPv4

3. ในฟิลด์ **ที่อยู่แบบคงที่** ให้พิมพ์ที่อยู่ IP ที่คุณต้องการกำหนดให้กับ XClarity Controller

   หมายเหตุ: ที่อยู่ IP ต้องมีจำนวนเต็มสี่ตัวตั้งแต่ 0 ถึง 255 โดยไม่มีช่องว่างและแยกด้วยเครื่องหมายมหัพภาค ฟิลด์นี้จะไม่ได้รับการกำหนดค่าหากตั้งค่าวิธีการเป็น **รับ IP จาก DHCP**

4. ในฟิลด์ **ตัวพรางเครือข่าย** ให้พิมพ์ตัวพรางเครือข่ายย่อยที่ใช้โดย XClarity Controller

   หมายเหตุ: ตัวพรางเครือข่ายย่อยต้องมีจำนวนเต็มสี่ตัวตั้งแต่ 0 ถึง 255 โดยไม่มีช่องว่างหรือเครื่องหมายมหัพภาคติดต่อกัน และแยกด้วยเครื่องหมายมหัพภาค การตั้งค่าเริ่มต้นคือ 255.255.255.0 ฟิลด์นี้จะไม่ได้รับการกำหนดค่าหากตั้งค่าวิธีการเป็น **รับ IP จาก DHCP**

5. ในฟิลด์ **เกตเวย์เริ่มต้น** ให้พิมพ์เราเตอร์เกตเวย์เครือข่ายของคุณ

   หมายเหตุ: ที่อยู่เกตเวย์ต้องมีจำนวนเต็มสี่ตัวตั้งแต่ 0 ถึง 255 โดยไม่มีช่องว่างหรือเครื่องหมายมหัพภาคติดต่อกัน และแยกด้วยเครื่องหมายมหัพภาค ฟิลด์นี้จะไม่ได้รับการกำหนดค่าหากตั้งค่าวิธีการเป็น **รับ IP จาก DHCP**

การกำหนดค่าการตั้งค่าอีเทอร์เน็ตขั้นสูง

คลิกแท็บ **อีเทอร์เน็ตขั้นสูง** เพื่อตั้งค่าอีเทอร์เน็ตเพิ่มเติม

หมายเหตุ: ใน Flex System การตั้งค่า VLAN จะได้รับการจัดการโดย Flex System CMM และไม่สามารถแก้ไขใน XClarity Controller

ในการเปิดใช้งานการแท็ก Virtual LAN (VLAN) ให้เลือกกล่องตัวเลือก **เปิดใช้งาน VLAN** เมื่อเปิดใช้งาน VLAN และกำหนดค่า VLAN ID แล้ว XClarity Controller จะยอมรับเฉพาะแพ็กเก็ตที่มี VLAN ID ที่ระบุเท่านั้น สามารถกำหนดค่า VLAN ID ด้วยค่าตัวเลขตั้งแต่ 1 ถึง 4094

จากรายการ **การเลือก MAC** ให้เลือกการเลือกใดการเลือกหนึ่งต่อไปนี้:

- ใช้ Burned-in MAC Address

  ตัวเลือก Burned-in MAC Address คือที่อยู่จริงที่ไม่ซ้ำกัน ซึ่งถูกกำหนดให้กับ XClarity Controller โดยผู้ผลิต ที่อยู่คือฟิลด์แบบอ่านอย่างเดียว

- ใช้ที่อยู่ MAC แบบกำหนดเอง

  หากมีการระบุค่า ที่อยู่ที่ได้รับการดูแลภายในจะแทนที่ Burned-in MAC Address ที่อยู่ที่ได้รับการดูแลภายในต้องเป็นค่าฐานสิบหกตั้งแต่ **000000000000** ถึง **FFFFFFFFFFFF** ค่านี้ต้องอยู่ในรูปแบบ *xx:xx:xx:xx:xx:xx* โดยที่ *x* เป็นตัวเลขฐานสิบหกตั้งแต่ 0 ถึง 9 หรือ “a” ถึง “f” XClarity Controller ไม่รองรับการใช้ที่อยู่ Multicast ไบต์แรกของที่อยู่ Multicast เป็นเลขคี่ (Least Significant Bit ถูกตั้งค่าไว้ที่ 1) ดังนั้น ไบต์แรกต้องเป็นเลขคู่

ในฟิลด์ **หน่วยการส่งข้อมูลสูงสุด** ให้ระบุหน่วยการส่งข้อมูลสูงสุดของแพ็คเก็ต (เป็นไบต์) สำหรับอินเทอร์เฟซเครือข่ายของคุณ ช่วงของหน่วยการส่งข้อมูลสูงสุดเริ่มตั้งแต่ 60 ถึง 1500 ค่าเริ่มต้นสำหรับฟิลด์นี้คือ 1500

ในการใช้การเชื่อมต่ออีเทอร์เน็ต IPv6 ให้ดำเนินการขั้นตอนต่อไปนี้:

การกำหนดค่าการตั้งค่าเครือข่าย IPv6

1. เปิดใช้งานตัวเลือก **IPv6**
2. กำหนดที่อยู่ IPv6 ให้กับอินเทอร์เฟซโดยใช้การกำหนดวิธีใดวิธีหนึ่งต่อไปนี้:
   - ใช้การกำหนดค่าที่อยู่อัตโนมัติที่ไม่เกี่ยวข้องกับสถานะ
   - ใช้การกำหนดค่าที่อยู่แบบมีสถานะ (DHCPv6)
   - ใช้ที่อยู่ IP ที่กำหนดแบบคงที่

     หมายเหตุ: เมื่อเลือก **ใช้ที่อยู่ IP ที่กำหนดแบบคงที่** ระบบจะขอให้คุณพิมพ์ข้อมูลต่อไปนี้:

     – ที่อยู่ IPv6

     – ความยาวคำนำหน้า

     – เกตเวย์

การกำหนดค่า DNS

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือเปลี่ยนการตั้งค่า Domain Name System (DNS) ของ XClarity Controller

หมายเหตุ: ใน Flex System จะไม่สามารถแก้ไขการตั้งค่า DNS ใน XClarity Controller ได้ การตั้งค่า DNS ได้รับการจัดการโดย CMM

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่า DNS ของ XClarity Controller

หากคุณคลิกกล่องตัวเลือก **ใช้เซิร์ฟเวอร์ที่อยู่ DNS เพิ่มเติม** ให้ระบุที่อยู่ IP ของเซิร์ฟเวอร์ Domain Name System สูงสุดสามเซิร์ฟเวอร์บนเครือข่ายของคุณ ที่อยู่ IP แต่ละรายการต้องมีจำนวนเต็มตั้งแต่ 0 ถึง 255 โดยแยกด้วยเครื่องหมายมหัพภาค ที่อยู่เซิร์ฟเวอร์ DNS เหล่านี้ถูกเพิ่มในรายการค้นหาบนสุด ดังนั้นจะมีการค้นหาชื่อโฮสต์บนเซิร์ฟเวอร์เหล่านี้ก่อนชื่อโฮสต์ที่ถูกกำหนดโดยเซิร์ฟเวอร์ DHCP โดยอัตโนมัติ

การกำหนดค่า DDNS

ใช้ข้อมูลในหัวข้อนี้เพื่อเปิดใช้งานหรือปิดใช้งานโปรโตคอล Dynamic Domain Name System (DDNS) บน XClarity Controller

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่า DDNS ของ XClarity Controller

คลิกกล่องตัวเลือก **เปิดใช้งาน DDNS** เพื่อเปิดใช้งาน DDNS เมื่อเปิดใช้งาน DDNS แล้ว XClarity Controller จะแจ้งให้ Domain Name Server เปลี่ยนการกำหนดค่า Domain Name Server ที่ใช้งานอยู่ของชื่อโฮสต์ที่กำหนดค่า XClarity Controller, ที่อยู่หรือข้อมูลอื่นๆ ที่จัดเก็บไว้ใน Domain Name Server แบบเรียลไทม์

เลือกตัวเลือกจากข้อมูลในรายการเพื่อกำหนดวิธีเลือกชื่อโดเมนของ XClarity Controller ที่คุณต้องการ

- **ใช้ชื่อโดเมนที่กำหนดเอง**: คุณสามารถระบุชื่อโดเมนที่มี XClarity Controller
- **ใช้ชื่อโดเมนที่ได้รับจากเซิร์ฟเวอร์ DHCP**: ชื่อโดเมนที่มี XClarity Controller ถูกระบุโดยเซิร์ฟเวอร์ DHCP

การกำหนดค่า Ethernet over USB

ใช้ข้อมูลในหัวข้อนี้เพื่อควบคุมอินเทอร์เฟซ Ethernet over USB ที่ใช้สำหรับการสื่อสารภายในระหว่างเซิร์ฟเวอร์และ XClarity Controller

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่า Ethernet over USB ของ XClarity Controller

ระบบจะใช้ Ethernet over USB เพื่อการสื่อสารภายในกับ XClarity Controller คลิกที่กล่องตัวเลือกเพื่อเปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซ Ethernet over USB

ข้อสำคัญ: หากคุณปิดใช้งาน Ethernet over USB คุณจะไม่สามารถดำเนินการอัปเดตภายในของเฟิร์มแวร์ XClarity Controller หรือเฟิร์มแวร์ของเซิร์ฟเวอร์โดยใช้ยูทิลิตีแบบแฟลชของ Linux หรือ Windows

เลือกวิธีการที่ XClarity Controller ใช้ในการกำหนดที่อยู่ไปยังปลายทางของอินเทอร์เฟซ Ethernet over USB

- **ใช้ที่อยู่ IPv6 Link-local สำหรับ Ethernet over USB**: วิธีการนี้จะใช้ที่อยู่ IPv6 ที่อิงตามที่อยู่ MAC ซึ่งได้รับการจัดสรรให้กับปลายทางของอินเทอร์เฟซ Ethernet over USB โดยปกติแล้วจะมีการสร้างที่อยู่ IPv6 Link Local โดยใช้ที่อยู่ MAC (RFC 4862) แต่ระบบปฏิบัติการ Windows 2008 และเวอร์ชัน 2016 ที่ใหม่กว่าไม่รองรับที่อยู่ IPv6 Link Local แบบคงที่บนปลายทางโฮสต์ของอินเทอร์เฟซ แต่ลักษณะการทำงานของ Windows ตามค่าเริ่มต้นจะสร้างที่อยู่ Link Local แบบสุ่มขณะทำงานแทน หากอินเทอร์เฟซ Ethernet over USB ของ XClarity Controller ได้รับการกำหนดค่าให้ใช้โหมดที่อยู่ IPv6 Link Local ฟังก์ชันต่างๆ ที่ใช้งานอินเทอร์เฟซนี้จะไม่ทำงานเนื่องจาก XClarity Controller ไม่รู้จักที่อยู่ที่ Windows กำหนดให้กับอินเทอร์เฟซ หากเซิร์ฟเวอร์กำลังใช้งาน Windows ให้วิธีการกำหนดค่าที่อยู่ Ethernet over USB วิธีอื่น หรือปิดใช้งานลักษณะการทำงานของ Windows ตามค่าเริ่มต้นโดยใช้คำสั่งนี้: *netsh interface ipv6 set global randomizeidentifiers=disabled*
- **ใช้ที่อยู่ภายในที่ลิงก์กับ IPv4 สำหรับ Ethernet over USB**: ที่อยู่ IP ในช่วง 169.254.0.0/16 ถูกกำหนดให้กับ XClarity Controller และฝั่งเซิร์ฟเวอร์ของเครือข่าย

- **กำหนดการตั้งค่า IPv4 สำหรับ Ethernet over USB**: การใช้วิธีการนี้จะเป็นการระบุที่อยู่ IP และตัวพรางเครือข่ายที่ถูกกำหนดให้กับ XClarity Controller และฝั่งเซิร์ฟเวอร์ของอินเทอร์เฟซ Ethernet over USB

หมายเหตุ:

1. การกำหนดค่า OS IP ไม่ได้ใช้เพื่อตั้งค่าที่อยู่ OS IP ของอินเทอร์เฟซ Ethernet Over USB แต่จะใช้เพื่อแจ้ง BMC ว่ามีการเปลี่ยนแปลงที่อยู่ OS IP ของ Ethernet Over USB
2. ก่อนที่คุณจะกำหนดการตั้งค่า IP สามรายการสำหรับ Ethernet over USB คุณต้องกำหนดค่าที่อยู่ OS IP ของ Ethernet over USB ในระบบปฏิบัติการของคุณด้วยตนเอง

การแมปหมายเลขพอร์ตอีเทอร์เน็ตภายนอกกับหมายเลขพอร์ต Ethernet over USB ถูกควบคุมโดยการคลิกกล่องตัวเลือก **เปิดใช้งานการส่งต่อพอร์ตอีเทอร์เน็ตภายนอกไปยัง Ethernet over USB** และกรอกข้อมูลการแมปสำหรับพอร์ตที่คุณต้องการส่งต่อจากอินเทอร์เฟซเครือข่ายการจัดการไปยังเซิร์ฟเวอร์

การกำหนดค่า SNMP

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่า SNMP Agent

ดำเนินการขั้นตอนต่อไปนี้เพื่อกำหนดการตั้งค่าการแจ้งเตือน SNMP ของ XClarity Controller

1. คลิก Network ภายใต้ **การกำหนดค่า BMC**
2. เลือกกล่องตัวเลือกที่เกี่ยวข้องเพื่อเปิดใช้งาน **SNMPv1 Trap**, **SNMPv2 Trap** และ/หรือ **SNMPv3 Trap**
3. หากเปิดใช้งาน **SNMPv1 Trap** หรือ **SNMPv2 Trap** ให้กรอกข้อมูลในฟิลด์ต่อไปนี้:
   a. ในฟิลด์ **ชื่อกลุ่ม** ให้ป้อนชื่อกลุ่ม ต้องระบุชื่อ
   b. ในฟิลด์ **โฮสต์** ให้ป้อนที่อยู่โฮสต์
4. หากเปิดใช้งาน **SNMPv3 Trap** ให้กรอกข้อมูลในฟิลด์ต่อไปนี้:
   a. ในฟิลด์ **รหัสเอนจิน** ให้ป้อนรหัสเอนจิน ต้องระบุรหัสเอนจิน
   b. ในฟิลด์ **พอร์ตรับ Trap** ให้ป้อนหมายเลขพอร์ต หมายเลขพอร์ตเริ่มต้นคือ 162
5. หากเปิดใช้งาน SNMP Trap ให้เลือกประเภทเหตุการณ์ที่คุณต้องการแจ้งเตือนต่อไปนี้:
   - **ร้ายแรง**
   - **ข้อคำนึง**
   - **ระบบ**

   หมายเหตุ: คลิกที่ประเภทหลักแต่ละประเภทเพื่อเลือกประเภทกิจกรรมย่อยเพิ่มเติมที่คุณต้องการรับการแจ้งเตือน

การเปิดใช้งานหรือปิดใช้งานการเข้าถึงเครือข่าย IPMI

ใช้ข้อมูลในหัวข้อนี้เพื่อควบคุมการเข้าถึงเครือข่าย IPMI ไปยัง XClarity Controller

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่า IPMI ของ XClarity Controller กรอกข้อมูลในฟิลด์ต่อไปนี้เพื่อดูหรือแก้ไขการตั้งค่า IPMI:

การเข้าถึง IPMI ผ่าน LAN

คลิกสวิตช์เพื่อเปิดใช้งานหรือปิดใช้งานการเข้าถึงเครือข่าย IPMI ไปยัง XClarity Controller

ข้อสำคัญ:

- หากคุณไม่ได้ใช้เครื่องมือหรือแอปพลิเคชันใดๆ ที่เข้าถึง XClarity Controller ผ่านเครือข่ายโดยใช้โปรโตคอล IPMI ขอแนะนำให้คุณปิดการใช้งานการเข้าถึงเครือข่าย IPMI เพื่อความปลอดภัยที่ดียิ่งขึ้น
- การเข้าถึง IPMI ผ่าน LAN ใน XClarity Controller ถูกปิดใช้งานตามค่าเริ่มต้น

การกำหนดค่าการตั้งค่าเครือข่ายด้วยคำสั่ง IPMI

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่าการตั้งค่าเครือข่ายโดยใช้คำสั่ง IPMI

เนื่องจากแต่ละการตั้งค่าเครือข่าย BMC ได้รับการกำหนดค่าโดยใช้คำขอ IPMI ที่แยกกัน และไม่เรียงตามลำดับ BMC ไม่มีมุมมองโดยสมบูรณ์ของการตั้งค่าเครือข่ายทั้งหมดจนกว่าจะมีการรีสตาร์ท BMC เพื่อนำการเปลี่ยนแปลงเครือข่ายที่รอดำเนินการไปใช้ คำขอเปลี่ยนแปลงการตั้งค่าเครือข่ายอาจสำเร็จได้ เมื่อมีการดำเนินการตามคำขอนั้น แต่จะถือว่าคำขอดังกล่าวไม่ถูกต้องเมื่อมีคำขอเปลี่ยนแปลงเพิ่มเติมในภายหลัง หากการตั้งค่าเครือข่ายที่รอดำเนินการใช้งานร่วมกันไม่ได้เมื่อรีสตาร์ท BMC การตั้งค่าใหม่จะไม่ถูกนำไปใช้ หลังจากรีสตาร์ท BMC คุณควรพยายามเข้าถึง BMC โดยใช้การตั้งค่าใหม่เพื่อให้แน่ใจว่ามีการนำการตั้งค่าเหล่านั้นไปใช้ตามที่คาดการณ์

การเปิดใช้งานบริการและการกำหนดพอร์ต

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือเปลี่ยนหมายเลขพอร์ตที่บริการบางส่วนบน XClarity Controller ใช้งาน

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการกำหนดพอร์ตของ XClarity Controller กรอกข้อมูลในฟิลด์ต่อไปนี้เพื่อดูหรือแก้ไขการกำหนดพอร์ต:

เว็บ

หมายเลขพอร์ตคือ 80 ฟิลด์นี้ไม่สามารถกำหนดค่าได้โดยผู้ใช้

Web over HTTPS

ในฟิลด์นี้จะระบุหมายเลขพอร์ตสำหรับ Web Over HTTPS ค่าเริ่มต้นคือ 443

REST over HTTPS

หมายเลขพอร์ตจะเปลี่ยนเป็นหมายเลขที่ระบุในฟิลด์ Web over HTTPS โดยอัตโนมัติ ฟิลด์นี้ไม่สามารถกำหนดค่าได้โดยผู้ใช้

Remote Presence

ในฟิลด์นี้จะระบุหมายเลขพอร์ตสำหรับ Remote Presence ค่าเริ่มต้นคือ 3900

IPMI ผ่าน LAN

หมายเลขพอร์ตคือ 623 ฟิลด์นี้ไม่สามารถกำหนดค่าได้โดยผู้ใช้

หมายเหตุ: IPMI จะปิดใช้งานตามค่าเริ่มต้น

SFTP

ในฟิลด์นี้จะระบุหมายเลขพอร์ตที่ใช้สำหรับ SSH File Transfer Protocol (SFTP) หมายเลขพอร์ตคือ 115 ฟิลด์นี้ไม่สามารถกำหนดค่าได้โดยผู้ใช้

หมายเหตุ: ต้องมี IMM.SFTPPortControl=open สำหรับการอัปเดต OneCLI ภายใน

SSDP

หมายเลขพอร์ตคือ 1900 ฟิลด์นี้ไม่สามารถกำหนดค่าได้โดยผู้ใช้

SSH

ในฟิลด์นี้จะระบุหมายเลขพอร์ตที่ถูกกำหนดค่าให้เข้าถึงอินเทอร์เฟซบรรทัดคำสั่งผ่านโปรโตคอล SSH ค่าเริ่มต้นคือ 22

SNMP Agent

ในฟิลด์นี้จะระบุหมายเลขพอร์ตสำหรับ SNMP Agent ที่ทำงานบน XClarity Controller ค่าเริ่มต้นคือ 161 หมายเลขพอร์ตที่ถูกต้องเริ่มตั้งแต่ 1 ถึง 65535

SNMP Traps

ในฟิลด์นี้จะระบุหมายเลขพอร์ตที่ใช้สำหรับ SNMP Traps ค่าเริ่มต้นคือ 162 หมายเลขพอร์ตที่ถูกต้องเริ่มตั้งแต่ 1 ถึง 65535

การกำหนดค่าข้อจำกัดการเข้าถึง

ใช้ข้อมูลในหัวข้อนี้เพื่อดูหรือเปลี่ยนการตั้งค่าที่บล็อกการเข้าถึงจากที่อยู่ IP หรือที่อยู่ MAC ไปยัง XClarity Controller

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่าการควบคุมการเข้าถึง XClarity Controller

รายการบล็อกและการจำกัดเวลา

ตัวเลือกเหล่านี้ช่วยให้คุณบล็อกที่อยู่ IP/Mac เฉพาะเป็นระยะเวลาที่กำหนดได้

- **รายการที่อยู่ IP ที่บล็อก**
  - คุณสามารถป้อนที่อยู่ IPv4 สูงสุดสามรายการหรือช่วงค่าและที่อยู่ IPv6 สามรายการหรือช่วงค่า โดยคั่นด้วยเครื่องหมายจุลภาค ซึ่งไม่อนุญาตให้เข้าถึง XClarity Controller โปรดดูตัวอย่าง IPv4 ด้านล่าง:
  - ตัวอย่างที่อยู่ IPv4 เดี่ยว: 192.168.1.1
  - ตัวอย่างที่อยู่ IPv4 ซุปเปอร์เน็ต: 192.168.1.0/24
  - ตัวอย่างช่วง IPv4: 192.168.1.1–192.168.1.5
- **รายการที่อยู่ MAC ที่บล็อก**
  - คุณสามารถป้อนที่อยู่ MAC สูงสุดสามรายการโดยคั่นด้วยเครื่องหมายจุลภาค ซึ่งไม่อนุญาตให้เข้าถึง XClarity Controller ตัวอย่าง: 11:22:33:44:55:66
- **การเข้าถึงแบบจำกัด (หนึ่งครั้ง)**
  - คุณสามารถวางกำหนดช่วงเวลาแบบครั้งเดียว เพื่อให้ไม่สามารถเข้าถึง XClarity Controller ได้ระหว่างช่วงดังกล่าว สำหรับช่วงเวลาที่คุณระบุ:
  - วันที่และเวลาเริ่มต้นจะต้องอยู่หลังจากเวลาปัจจุบันของ XCC
  - วันที่และเวลาสิ้นสุดจะต้องอยู่หลังจากวันที่และเวลาเริ่มต้น
- **การเข้าถึงแบบจำกัด (รายวัน)**
  - คุณสามารถวางกำหนดช่วงเวลาในแต่ละวัน เพื่อให้ไม่สามารถเข้าถึง XClarity Controller ได้ระหว่างช่วงดังกล่าว สำหรับแต่ละช่วงเวลาที่คุณระบุ:
  - วันที่และเวลาสิ้นสุดจะต้องอยู่หลังจากวันที่และเวลาเริ่มต้น

รายการบล็อกที่ทริกเกอร์ภายนอก

ตัวเลือกเหล่านี้ช่วยให้คุณตั้งค่าการบล็อคที่อยู่ IP เฉพาะ (IPv4 และ IPv6) โดยอัตโนมัติซึ่งพยายามเข้าสู่ระบบ XClarity Controller ด้วยชื่อผู้ใช้หรือรหัสผ่านที่ไม่ถูกต้องหลายครั้งติดต่อกัน

การบล็อกอัตโนมัติจะตรวจจับว่ามีการเข้าสู่ระบบล้มเหลวมากเกินไปจากที่อยู่ IP ใด IP หนึ่ง และบล็อกที่อยู่นั้นจากการเข้าถึง XClarity Controller ตามระยะเวลาที่กำหนดไว้ล่วงหน้า

- **จำนวนสูงสุดของการเข้าสู่ระบบล้มเหลวจาก IP ใด IP หนึ่ง**
  - จำนวนครั้งสูงสุดระบุจำนวนของการเข้าสู่ระบบล้มเหลวที่อนุญาตสำหรับผู้ใช้ที่มีรหัสผ่านไม่ถูกต้องจากที่อยู่ IP เฉพาะ ก่อนที่จะถูกล็อค

- หากตั้งค่าเป็น 0 ที่อยู่ IP จะไม่ถูกล็อคเมื่อเข้าสู่ระบบล้มเหลว
- ตัวนับการเข้าสู่ระบบล้มเหลวสำหรับที่อยู่ IP เฉพาะจะถูกรีเซ็ตเป็นศูนย์ หลังจากที่อยู่ IP นั้นเข้าสู่ระบบสำเร็จ

• **ระยะเวลาการล็อคสำหรับการบล็อค IP**

- ระยะเวลาขั้นต่ำ (เป็นนาที) ที่ต้องผ่านไปก่อนผู้ใช้จะสามารถพยายามเข้าสู่ระบบได้อีกครั้งจากที่อยู่ IP ที่ถูกล็อค
- หากตั้งค่าเป็น 0 ระบบจะบล็อกการเข้าถึงจากที่อยู่ IP ที่ถูกล็อคไปจนกว่าผู้ดูแลระบบจะปลดล็อคให้

• **รายการบล็อก**

- รายการบล็อกตารางจะแสดงที่อยู่ IP ที่ถูกล็อคทั้งหมด คุณสามารถปลดล็อคที่อยู่ IP หนึ่งรายการหรือทั้งหมดได้จากรายการบล็อค

การกำหนดค่าพอร์ต USB บนแผงด้านหน้าไปยังการจัดการ

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่าพอร์ต USB บนแผงด้านหน้าของ XClarity Controller ไปยังการจัดการ

บนบางเซิร์ฟเวอร์ พอร์ต USB บนแผงด้านหน้าสามารถสลับเพื่อเชื่อมต่อกับเซิร์ฟเวอร์หรือ XClarity Controller ได้ การเชื่อมต่อกับ XClarity Controller มีจุดประสงค์หลักในการใช้งานกับอุปกรณ์เคลื่อนที่ที่ใช้งานแอป Lenovo XClarity Mobile เมื่อเชื่อมต่อสาย USB ระหว่างอุปกรณ์เคลื่อนที่และแผงด้านหน้าของเซิร์ฟเวอร์ ระบบจะสร้างการเชื่อมต่อ Ethernet over USB ระหว่างแอปบนอุปกรณ์เคลื่อนที่ที่ใช้งานบนอุปกรณ์และ XClarity Controller

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อดูหรือแก้ไขการตั้งค่าพอร์ต USB บนแผงด้านหน้าของ XClarity Controller ไปยังการจัดการ

มีการตั้งค่าที่คุณสามารถเลือกได้ 4 ประเภท:

โหมดโฮสต์เท่านั้น
พอร์ต USB บนแผงด้านหน้าจะเชื่อมต่อกับเซิร์ฟเวอร์เท่านั้นเสมอ

โหมด BMC เท่านั้น
พอร์ต USB บนแผงด้านหน้าจะเชื่อมต่อกับ XClarity Controller เท่านั้น

โหมดแบบใช้งานร่วมกัน : BMC เป็นเจ้าของ
มีการใช้พอร์ต USB บนแผงด้านหน้าร่วมกันทั้งเซิร์ฟเวอร์และ XClarity Controller แต่พอร์ตจะถูกสลับไปเป็น XClarity Controller

โหมดแบบใช้งานร่วมกัน: โฮสต์เป็นเจ้าของ
มีการใช้พอร์ต USB บนแผงด้านหน้าร่วมกันทั้งเซิร์ฟเวอร์และ XClarity Controller แต่พอร์ตจะถูกสลับไปเป็นโฮสต์

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับแอปบนอุปกรณ์เคลื่อนที่ โปรดดูไซต์ต่อไปนี้:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

หมายเหตุ:

- หากมีการกำหนดค่าพอร์ต USB บนแผงด้านหน้าสำหรับโหมดแบบใช้งานร่วมกัน พอร์ตจะถูกเชื่อมต่อกับ XClarity Controller เมื่อไม่มีพลังงาน และเชื่อมต่อกับเซิร์ฟเวอร์เมื่อมีพลังงาน เมื่อมีพลังงาน การควบคุมของพอร์ต USB บนแผงด้านหน้าสามารถสลับไปมาระหว่างเซิร์ฟเวอร์และ XClarity Controller ได้ ในโหมดแบบใช้งานร่วมกัน ยังสามารถสลับพอร์ตระหว่างโฮสต์และ XClarity Controller ได้ โดยกดปุ่มการระบุบนแผงด้านหน้า (อาจเป็นปุ่มการจัดการ USB สำหรับโหนดคอมพิวเตอร์) ค้างไว้ 3 วินาที
- เมื่อกำหนดค่าในโหมดแบบใช้งานร่วมกันและพอร์ต USB เชื่อมต่อกับเซิร์ฟเวอร์ในปัจจุบัน XClarity Controller สามารถรองรับคำขอให้สลับพอร์ต USB บนแผงด้านหน้ากลับไปยัง XClarity Controller ได้ เมื่อมีการดำเนินการตามคำขอนี้ พอร์ต USB บนแผงด้านหน้าจะยังคงเชื่อมต่อกับ XClarity Controller จนกว่าจะไม่มีการใช้งาน USB กับ XClarity Controller ตามระยะเวลาที่ระบุในการหมดเวลาเมื่อไม่มีการใช้งาน

การกำหนดค่าการตั้งค่าการรักษาความปลอดภัย

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่าโปรโตคอลการรักษาความปลอดภัย

หมายเหตุ: การตั้งค่าเวอร์ชัน TLS ต่ำสุดเริ่มต้นคือ TLS 1.2 แต่คุณสามารถกำหนดค่า XClarity Controller ให้ใช้ TLS เวอร์ชันอื่นๆ ได้ หากจำเป็นสำหรับเบราเซอร์หรือแอปพลิเคชันการจัดการของคุณ สำหรับข้อมูลเพิ่มเติม โปรดดู “คำสั่ง tls” บนหน้าที่ 223

คลิก Security ภายใต้ **การกำหนดค่า** BMC เพื่อเข้าถึงและกำหนดค่าคุณสมบัติ สถานะ และการตั้งค่าการรักษาความปลอดภัยสำหรับ XClarity Controller ของคุณ

แดชบอร์ดรักษาความปลอดภัย

หัวข้อนี้จะอธิบายเกี่ยวกับภาพรวมของแดชบอร์ดรักษาความปลอดภัย

แดชบอร์ดรักษาความปลอดภัยจะช่วยในการประเมินระบบรักษาความปลอดภัยโดยรวมและสถานะของระบบ

- **เหตุการณ์การรักษาความปลอดภัย** BMC จะรายงานเหตุการณ์ที่เกิดจากปัญหาด้านความปลอดภัย เช่น การบุกรุกตัวเครื่อง, ความเสียหายเมื่อตรวจพบ PFR, ความไม่สอดคล้องของฮาร์ดแวร์ System Guard, จัมเปอร์การรักษาความปลอดภัยที่เปิดอยู่บน Planar เป็นต้น
- **โหมดรักษาความปลอดภัยของ** BMC แสดงสถานะโดยรวมเกี่ยวกับการปฏิบัติตามข้อบังคับของโหมดการรักษาความปลอดภัย

- **บริการและพอร์ตของ BMC** จะค้นหาบริการ/พอร์ตที่ไม่ปลอดภัยทั้งหมดที่เปิดใช้งานแต่ไม่สอดคล้องกับโหมดการรักษาความปลอดภัยปัจจุบัน
- **ใบรับรอง BMC** แสดงรายการใบรับรองที่ไม่สอดคล้องทั้งหมดที่ใช้โดย XCC
- **บัญชีผู้ใช้ BMC** จะให้คำแนะนำทั่วไปเกี่ยวกับวิธีทำให้บัญชีและการจัดการรหัสผ่านปลอดภัยยิ่งขึ้น

หมายเหตุ: แดชบอร์ดจะแสดงไอคอนคำเตือนหากมีความเสี่ยงในพื้นที่ความปลอดภัยเหล่านี้ที่สแกนโดย XCC ลิงก์รายละเอียดในแต่ละหมวดหมู่จะนำผู้ใช้ไปยังหน้าการตั้งค่าเพื่อแก้ไขปัญหา

โหมดรักษาความปลอดภัย

หัวข้อนี้จะอธิบายเกี่ยวกับภาพรวมของโหมดรักษาความปลอดภัย

สิทธิ์การใช้งาน XCC Standard ช่วยให้ผู้ใช้สามารถกำหนดค่าเซิร์ฟเวอร์ของตนในโหมดความปลอดภัยหนึ่งในสองโหมด: โหมดมาตรฐานและโหมดการทำงานร่วมกัน มีให้ใช้งานในเซิร์ฟเวอร์ V3 ทั้งหมด

สิทธิ์การใช้งาน XCC Platinum มาพร้อมกับโหมดรักษาความปลอดภัยที่สาม: โหมดองค์กรแบบรัดกุม โหมดนี้เหมาะสมที่สุดสำหรับข้อกำหนดด้านการรักษาความปลอดภัยในระดับสูง

โหมดการรักษาความปลอดภัยระดับองค์กรแบบรัดกุม

- โหมดการรักษาความปลอดภัยระดับองค์กรแบบรัดกุมเป็นโหมดที่ปลอดภัยที่สุด
- อัลกอริทึมการเข้ารหัสทั้งหมดที่ BMC ใช้จะสอดคล้องตามมาตรฐานระดับองค์กรแบบรัดกุม
- BMC ทำงานในโหมดที่ผ่านการตรวจสอบความถูกต้องมาตรฐาน
- ต้องมีใบรับรองระดับองค์กรแบบรัดกุม
- อนุญาตเฉพาะบริการที่รองรับการเข้ารหัสระดับองค์กรแบบรัดกุมเท่านั้น
- ต้องมีคีย์ Feature on Demand ในการเปิดใช้งาน

โหมดการรักษาความปลอดภัยมาตรฐาน

- โหมดมาตรฐานเป็นโหมดการรักษาความปลอดภัยตามค่าเริ่มต้น
- อัลกอริทึมการเข้ารหัสทั้งหมดที่ BMC ใช้จะสอดคล้องตามมาตรฐานของระดับ Standard
- BMC ทำงานในโหมดที่ผ่านการตรวจสอบความถูกต้องมาตรฐาน
- ต้องมีใบรับรองระดับ Standard
- บริการที่ต้องใช้การเข้ารหัสที่ไม่รองรับการเข้ารหัสระดับ Standard จะถูกปิดใช้งานตามค่าเริ่มต้น

โหมดการรักษาความปลอดภัยแบบเข้ากันได้

- โหมดความเข้ากันได้คือโหมดที่จะใช้เมื่อบริการและไคลเอ็นต์ต้องการใช้การเข้ารหัสที่ไม่สอดคล้องตามมาตรฐานระดับองค์กรแบบรัดกุม/มาตรฐาน
- ระบบจะรองรับอัลกอริทึมการเข้ารหัสหลากหลายรูปแบบมากขึ้น
- เมื่อโหมดนี้เปิดใช้งาน BMC จะไม่ดำเนินการในโหมดที่ผ่านมาตรฐานระดับ Standard
- อนุญาตให้เปิดใช้งานบริการทั้งหมด

เมทริกซ์การบริการในโหมดรักษาความปลอดภัยสามโหมด:

คุณลักษณะ/บริการ	**ใช้การเข้ารหัส**	**สถานะ Default** **พร้อมใช้งาน**	**รองรับใน** **โหมด** Strict	**รองรับใน** **โหมด** Standard	**รองรับใน** **โหมดความเข้ากันได้**
IPMI-over-KCS	ไม่	เปิดใช้งาน	ใช่	ใช่	ใช่
IPMI-over-LAN	ใช่	ปิดใช้งาน	ไม่	ใช่	ใช่
SNMPv1 traps	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
SNMPv3 traps	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่ หากเปิดใช้งาน จะแจ้งเตือนสำหรับการใช้การเข้ารหัสแบบ non-FIPS	ใช่
SNMPv3 agent	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่ หากเปิดใช้งาน จะแจ้งเตือนสำหรับการใช้การเข้ารหัสแบบ non-FIPS	ใช่

คุณลักษณะ/บริการ	**ใช้การเข้ารหัส**	**สถานะ Default** **พร้อมใช้งาน**	**รองรับใน** **โหมด** Strict	**รองรับใน** **โหมด** Standard	**รองรับใน** **โหมดความเข้ากันได้**
การแจ้งเตือนด้วยอีเมล	ใช่	ไม่มีการกำหนดค่า	ใช่ ไม่สามารถเปิดใช้งานด้วย CRAM-MD5 Authentication	ใช่ หากจำเป็นองมี CRAM-MD5 จะแจ้งเตือนสำหรับการใช้การเข้ารหัสแบบ non-FIPS	ใช่
การแจ้งเตือน Syslog	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
TLS 1.2	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
TLS 1.3	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
Web over HTTPS	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
Redfish over HTTPS	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
SSDP	ไม่	เปิดใช้งาน	ใช่	ใช่	ใช่
SSH-CLI	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
SFTP	ใช่	ปิดใช้งาน	ใช่	ใช่	ใช่
LDAP	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
Secure LDAP	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
การจัดการคีย์การรักษาความปลอดภัย	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่

คุณลักษณะ/บริการ	ใช้การเข้ารหัส	สถานะ Default พร้อมใช้งาน	รองรับใน โหมด Strict	รองรับใน โหมด Standard	รองรับใน โหมดความเข้ากันได้
คอนโซลระยะไกล	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
สื่อเสมือน - CIFS	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
สื่อเสมือน - NFS	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
สื่อเสมือน - HTTPFS	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
RDOC - Local	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
RDOC - CIFS	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
RDOC - HTTP	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
RDOC - HTTPS	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
RDOC - FTP	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
RDOC - SFTP	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
การอัปโหลด FFDC (SFTP)	ใช่	เปิดใช้งาน	ใช่	ใช่	ใช่
การอัปโหลด FFDC (TFTP)	ไม่	เปิดใช้งาน	ไม่	ใช่	ใช่

คุณลักษณะ/บริการ	ใช้การเข้ารหัส	สถานะ Default พร้อมใช้งาน	รองรับใน โหมด Strict	รองรับใน โหมด Standard	รองรับใน โหมดความเข้ากันได้
อัปเดตจากที่เก็บข้อมูล – CIFS	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
อัปเดตจากที่เก็บข้อมูล - NFS	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
อัปเดตจากที่เก็บข้อมูล – HTTP	ไม่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
อัปเดตจากที่เก็บข้อมูล – HTTPS	ใช่	ไม่มีการกำหนดค่า	ใช่	ใช่	ใช่
Call Home	ใช่	ปิดใช้งาน	ใช่	ใช่	ใช่
รหัสผ่านบุคคลที่สาม	ใช่	ไม่มีการกำหนดค่า	ไม่	ใช่	ใช่
การฟอร์เวิร์ดพอร์ต	ไม่ระบุ	ปิดใช้งาน	ใช่	ใช่	ใช่

การสลับโหมดรักษาความปลอดภัย

ใช้ข้อมูลในหัวข้อนี้เพื่อสลับและตรวจสอบโหมดรักษาความปลอดภัย

โหมดมาตรฐานเป็นโหมดการรักษาความปลอดภัยตามค่าเริ่มต้น

โดยทั่วไปแล้ว หาก XCC ตรวจพบการตั้งค่าที่ไม่สอดคล้องกับโหมดมาตรฐาน XCC จะแสดงการแจ้งเตือน แต่ผู้ใช้ไม่จำเป็นต้องเปลี่ยนโหมด ในกรณีนี้ XCC จะเข้าสู่โหมดรักษาความปลอดภัยมาตรฐานพร้อมการแทนที่ (ไม่เป็นไปตามข้อกำหนด)

ผู้ใช้สามารถเปิดเมนูแบบเลื่อนลงเพื่อเลือกโหมดต่างๆ และใช้ฟังก์ชัน “ตรวจสอบความถูกต้อง” เพื่อกำหนดจำนวนรายการที่ไม่เป็นไปตามข้อกำหนดที่ตรวจพบโดย XCC

เมื่อผู้ใช้คลิกที่ “Apply” XCC จะตรวจสอบความถูกต้องของรายการไม่เป็นไปตามข้อกำหนดด้วย

ภาพรวมของ SSL

หัวข้อนี้จะอธิบายเกี่ยวกับภาพรวมของโปรโตคอลการรักษาความปลอดภัย SSL

SSL คือโปรโตคอลการรักษาความปลอดภัยที่มีความเป็นส่วนตัวในการติดต่อสื่อสาร SSL ช่วยให้แอปพลิเคชันไคลเอ็นต์/เซิร์ฟเวอร์สามารถสื่อสารในลักษณะที่ช่วยป้องกันการลอบฟัง การแทรกแซง และปลอมแปลงข้อความ คุณสามารถกำหนดค่า XClarity Controller ให้ใช้งานการสนับสนุน SSL สำหรับการเชื่อมต่อประเภทต่างๆ อาทิ เว็บเซิร์ฟเวอร์แบบปลอดภัย (HTTPS), การเชื่อมต่อ LDAP แบบปลอดภัย (LDAPS), CIM over HTTPS และเซิร์ฟเวอร์ SSH รวมถึงเพื่อจัดการใบรับรองที่จำเป็นสำหรับ SSL

การควบคุมดูแลใบรับรอง SSL

หัวข้อนี้จะแสดงข้อมูลเกี่ยวกับการดูแลจัดการใบรับรองที่สามารถใช้กับโปรโตคอลการรักษาความปลอดภัย SSL

คุณสามารถใช้ SSL กับใบรับรองที่ลงนามด้วยตนเองหรือกับใบรับรองที่ลงนามโดยหน่วยงานผู้ออกใบรับรองบุคคลที่สาม การใช้ใบรับรองที่ลงนามด้วยตนเองคือวิธีที่ง่ายที่สุดสำหรับการใช้ SSL แต่ก็เป็นการสร้างความเสี่ยงด้านการรักษาความปลอดภัยเล็กน้อย ความเสี่ยงเกิดขึ้นเนื่องจากไคลเอ็นต์ SSL ไม่มีวิธีการตรวจสอบความถูกต้องข้อมูลประจำตัวของเซิร์ฟเวอร์ SSL สำหรับการเชื่อมต่อที่พยายามเป็นครั้งแรกระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ ตัวอย่างเช่น อาจมีโอกาสที่บุคคลที่สามจะปลอมแปลงเว็บเซิร์ฟเวอร์ XClarity Controller และขัดขวางกระแสข้อมูลระหว่างเว็บเซิร์ฟเวอร์ XClarity Controller จริงและเว็บเบราเซอร์ของผู้ใช้ หากมีการนำเข้าใบรับรองที่ลงนามด้วยตนเองในที่เก็บใบรับรองของเบราเซอร์ในขณะที่มีการเชื่อมต่อเริ่มต้นระหว่างเบราเซอร์และ XClarity Controller การสื่อสารในอนาคตทั้งหมดจะได้รับการรักษาความปลอดภัยสำหรับเบราเซอร์นั้น (โดยถือว่าการเชื่อมต่อเริ่มต้นไม่ถูกบุกรุกจากการโจมตี)

คุณสามารถใช้ใบรับรองที่ลงนามโดยหน่วยงานผู้ออกใบรับรอง (CA) เพื่อการรักษาความปลอดภัยที่สมบูรณ์ยิ่งขึ้น หากต้องการขอรับใบรับรองที่ลงนาม คุณจะต้องเลือก **สร้างคำขอการลงนามใบรับรอง (CSR)** เลือก **ดาวน์โหลดคำขอการลงนามใบรับรอง (CSR)** และส่งคำขอการลงนามใบรับรอง (CSR) ไปยัง CA เพื่อขอรับใบรับรองที่ลงนาม เมื่อได้รับใบรับรองที่ลงนาม ให้เลือก **นำเข้าใบรับรองที่ลงนาม** เพื่อนำเข้าใน XClarity Controller

ฟังก์ชันของ CA คือการตรวจสอบข้อมูลประจำตัวของ XClarity Controller ใบรับรองมีลายเซ็นดิจิตอลสำหรับ CA และ XClarity Controller หาก CA ที่เป็นที่รู้จักออกใบรับรอง หรือหากใบรับรองของ CA ได้รับการนำเข้าในเว็บเบราเซอร์แล้ว เบราเซอร์จะสามารถตรวจสอบความถูกต้องของใบรับรอง และระบุเว็บเบราเซอร์ XClarity Controller ได้อย่างชัดเจน

XClarity Controller ต้องการใบรับรองสำหรับใช้กับเซิร์ฟเวอร์ HTTPS, CIM over HTTPS และไคลเอ็นต์ LDAP ที่ปลอดภัย นอกจากนี้ ไคลเอ็นต์ LDAP ที่ปลอดภัยยังต้องการใบรับรองที่เชื่อถือได้ที่จะนำเข้าอย่างน้อยหนึ่งใบรับรอง ไคลเอ็นต์ LDAP ที่ปลอดภัยจะใช้ใบรับรองที่เชื่อถือได้เพื่อระบุเซิร์ฟเวอร์ LDAP โดยชัดเจน ใบรับรองที่เชื่อถือได้คือใบรับรองของ CA ที่ลงนามใบรับรองของเซิร์ฟเวอร์ LDAP หากเซิร์ฟเวอร์ LDAP ใช้ใบรับรองที่ลงนามด้วยตนเอง ใบรับรองที่เชื่อถือได้สามารถเป็นใบรับรองของเซิร์ฟเวอร์ LDAP เองได้ ต้องนำเข้าใบรับรองที่เชื่อถือได้เพิ่มเติม หากมีการใช้งานเซิร์ฟเวอร์ LDAP ในการกำหนดค่าของคุณมากกว่าหนึ่งเซิร์ฟเวอร์

การจัดการใบรับรอง SSL

หัวข้อนี้จะแสดงข้อมูลเกี่ยวกับการดำเนินการบางรายการ ซึ่งสามารถเลือกได้เพื่อจัดการใบรับรองโดยใช้โปรโตคอลการรักษาความปลอดภัย SSL

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า BMC** เพื่อกำหนดค่าการจัดการใบรับรอง SSL

ระหว่างทำการจัดการใบรับรองของ XClarity Controller คุณจะพบตัวเลือกการดำเนินการต่อไปนี้:

ดาวน์โหลดใบรับรองที่ลงนาม

ใช้ลิงก์นี้ เพื่อดาวน์โหลดสำเนาของใบรับรองที่ติดตั้งในปัจจุบัน ใบรับรองสามารถดาวน์โหลดได้ในรูปแบบ PEM หรือ DER ก็ได้ สามารถดูเนื้อหาของใบรับรองโดยใช้เครื่องมือของบริษัทภายนอก อาทิ OpenSSL (www.openssl.org) ตัวอย่างของบรรทัดคำสั่งสำหรับเรียกดูเนื้อหาของใบรับรองด้วย OpenSSL จะมีลักษณะคล้ายกับตัวอย่างต่อไปนี้:

```
openssl x509 -in cert.der -inform DER -text
```

ดาวน์โหลดคำขอการลงนามใบรับรอง (CSR)

ใช้ลิงก์นี้ เพื่อดาวน์โหลดสำเนาคำขอการลงนามใบรับรอง เอกสาร CSR สามารถดาวน์โหลดได้ในรูปแบบ PEM หรือ DER ก็ได้

สร้างใบรับรองที่ลงนาม

สร้างใบรับรองที่ลงนามเอง เมื่อดำเนินการเรียบร้อยแล้ว คุณสามารถเปิดใช้งาน SSL ได้โดยใช้ใบรับรองใหม่

หมายเหตุ: เมื่อดำเนินการ **สร้างใบรับรองที่ลงนามด้วยตนเอง** หน้าต่างการสร้างใบรับรองที่ลงนามด้วยตนเองสำหรับ HTTPS จะเปิดขึ้น คุณจะได้รับการขอให้กรอกข้อมูลลงในฟิลด์ที่จำเป็นและฟิลด์เสริมจนเสร็จสิ้น คุณ*ต้อง*กรอกข้อมูลลงในฟิลด์ที่จำเป็นจนครบ เมื่อป้อนข้อมูลเรียบร้อยแล้ว ให้คลิก **สร้าง** เพื่อดำเนินขั้นตอนให้เสร็จสิ้น

สร้างคำขอการลงนามใบรับรอง (CSR)

สร้างคำขอการลงนามใบรับรอง (CSR) เมื่อดำเนินการเรียบร้อยแล้ว คุณสามารถดาวน์โหลดไฟล์ CSR และส่งไปยังหน่วยงานด้านใบรับรอง (CA) เพื่อลงนามได้

หมายเหตุ: เมื่อดำเนินการ **สร้างคำขอการลงนามใบรับรอง (CSR)** หน้าต่างสร้างคำขอการลงนามใบรับรองสำหรับ HTTPS จะเปิดขึ้น คุณจะได้รับการขอให้กรอกข้อมูลลงในฟิลด์ที่จำเป็นและฟิลด์เสริมจนเสร็จสิ้น คุณ*ต้อง*กรอกข้อมูลลงในฟิลด์ที่จำเป็นจนครบ เมื่อป้อนข้อมูลเรียบร้อยแล้ว ให้คลิก **สร้าง** เพื่อดำเนินขั้นตอนให้เสร็จสิ้น

นำเข้าใบรับรองที่ลงนาม

ใช้เพื่อนำเข้าใบรับรองที่ลงนาม หากต้องการขอรับใบรับรองที่ลงนาม คุณจะต้องสร้างคำขอการลงนามใบรับรอง (CSR) ก่อน จากนั้นจึงส่งคำขอไปยังหน่วยงานด้านใบรับรอง (CA)

การกำหนดค่าเซิร์ฟเวอร์ Secure Shell

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจและเปิดใช้งานโปรโตคอลการรักษาความปลอดภัย SSH

คลิก Network ภายใต้ **การกำหนดค่า BMC** เพื่อกำหนดค่าเซิร์ฟเวอร์ Secure Shell

ในการใช้โปรโตคอล SSH จำเป็นต้องสร้างคีย์เพื่อเปิดใช้งานเซิร์ฟเวอร์ SSH ก่อน

หมายเหตุ:

- ไม่จำเป็นต้องมีการจัดการใบรับรองในการใช้ตัวเลือกนี้
- XClarity Controller จะสร้างคีย์เซิร์ฟเวอร์ SSH เริ่มต้น หากคุณต้องการสร้างคีย์เซิร์ฟเวอร์ SSH ใหม่ ให้คลิก **เครือข่าย** ภายใต้ **การกำหนดค่า BMC**; แล้วคลิก **สร้างคีย์**
- หลังจากดำเนินการเสร็จสิ้น คุณต้องรีสตาร์ท XClarity Controller เพื่อให้การเปลี่ยนแปลงมีผล

การเข้าถึง IPMI ผ่าน Keyboard Controller Style (KCS)

ใช้ข้อมูลในหัวข้อนี้เพื่อควบคุมการเข้าถึง IPMI ผ่าน Keyboard Controller Style (KCS) ไปยัง XClarity Controller

XClarity Controller มีอินเทอร์เฟซ IPMI ผ่านช่อง KCS ที่ไม่จำเป็นต้องมีการตรวจสอบความถูกต้อง

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า BMC** เพื่อเปิดใช้งานหรือปิดใช้งานการเข้าถึง IPMI ผ่าน KCS

หมายเหตุ: หลังจากเปลี่ยนการตั้งค่า คุณต้องรีสตาร์ท XClarity Controller เพื่อให้การเปลี่ยนแปลงมีผล

ข้อสำคัญ: หากคุณไม่ได้ใช้งานเครื่องมือหรือแอปพลิเคชันบนเซิร์ฟเวอร์ใดๆ ที่เข้าถึง XClarity Controller ผ่านโปรโตคอล IPMI ขอแนะนำให้คุณปิดการใช้งานการเข้าถึง IPMI KCS เพื่อความปลอดภัยที่ดียิ่งขึ้น XClarity Essentials ใช้งานอินเทอร์เฟซ IPMI ผ่าน KCS ไปยัง XClarity Controller หากคุณปิดใช้งานอินเทอร์เฟซ IPMI ผ่าน KCS ให้เปิด

ใช้งานอีกครั้งก่อนที่จะเรียกใช้ XClarity Essentials บนเซิร์ฟเวอร์ แล้วจึงปิดใช้งานอินเทอร์เฟซหลังจากคุณดำเนินการเสร็จสิ้น

การรวบรวมบันทึก IPMI SEL

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่าบันทึก IPMI SEL

XClarity Controller มีตัวเลือกการรวบรวมบันทึก IPMI SEL

คลิกสวิตช์มุมบนขวาเพื่อเปิดหรือปิดใช้งานการรวบรวมบันทึก IPMI SEL

คุณลักษณะนี้ช่วยให้สามารถทำการเรกคอร์ดบันทึก IPMI SEL ได้ เรกคอร์ด SEL ใหม่จะมีการต่อท้ายเสมอ และเรกคอร์ดที่เก่าที่สุดจะถูกทิ้งเมื่อบันทึก IPMI SEL เต็ม

หมายเหตุ: การใช้การตั้งค่านี้จำเป็นต้องรีบูต BMC

ป้องกันการลดระดับเฟิร์มแวร์ของระบบ

ใช้ข้อมูลในหัวข้อนี้เพื่อป้องกันไม่ให้เฟิร์มแวร์ของระบบเปลี่ยนเป็นระดับเฟิร์มแวร์ที่เก่ากว่า

คุณลักษณะนี้ทำให้คุณสามารถกำหนดว่าจะอนุญาตให้เฟิร์มแวร์ของระบบกลับไปยังระดับเฟิร์มแวร์ที่เก่ากว่าหรือไม่

คลิก **Network** ภายใต้ **การกำหนดค่า BMC** เพื่อป้องกันไม่ให้เฟิร์มแวร์ของระบบลดระดับ

ในการเปิดใช้งานหรือปิดใช้งานคุณลักษณะนี้ ให้คลิก **Network** ภายใต้ **การกำหนดค่า BMC** การเปลี่ยนแปลงใดๆ ที่ดำเนินการจะมีผลในทันทีโดยไม่จำเป็นต้องรีสตาร์ท XClarity Controller

การกำหนดค่าเซิร์ฟเวอร์การจัดการคีย์ความปลอดภัย (SKM)

ใช้ข้อมูลในหัวข้อนี้เพื่อสร้างและจัดการคีย์ความปลอดภัย

คุณลักษณะนี้ใช้เซิร์ฟเวอร์การจัดการคีย์จากส่วนกลางเพื่อมอบคีย์ที่ปลดล็อคฮาร์ดแวร์การจัดเก็บข้อมูล เพื่อเข้าถึงข้อมูลที่จัดเก็บบน SED ในเซิร์ฟเวอร์ ThinkSystem เซิร์ฟเวอร์การจัดการคีย์ประกอบ SKLM - เซิร์ฟเวอร์การจัดการคีย์ IBM SED และ KMIP - เซิร์ฟเวอร์การจัดการคีย์ Thales/Gemalto SED (KeySecure และ CipherTrust)

XClarity Controller ใช้เครือข่ายเพื่อรับคีย์จากเซิร์ฟเวอร์การจัดการคีย์ ดังนั้นเซิร์ฟเวอร์การจัดการคีย์จะต้องสามารถเข้าถึง XClarity Controller ได้ XClarity Controller ทำหน้าที่เป็นช่องทางการสื่อสารระหว่างเซิร์ฟเวอร์การจัดการคีย์และ

เซิร์ฟเวอร์ ThinkSystem ที่ส่งคำขอ เฟิร์มแวร์ของ XClarity Controller จะพยายามเชื่อมต่อกับเซิร์ฟเวอร์การจัดการคีย์ที่กำหนดค่าไว้แต่ละชุด และจะหยุดเมื่อสามารถเชื่อมต่อได้โดยสมบูรณ์

XClarity Controller จะติดต่อสื่อสารกับเซิร์ฟเวอร์การจัดการคีย์ หากตรวจสอบว่าได้ทำตามเงื่อนไขต่อไปนี้แล้ว:

- มีการกำหนดค่าชื่อโฮสต์/ที่อยู่ IP ของเซิร์ฟเวอร์การจัดการคีย์อย่างน้อยหนึ่งรายการภายใน XClarity Controller
- มีการติดตั้งใบรับรองสองชุด (ของไคลเอ็นต์และเซิร์ฟเวอร์) สำหรับการสื่อสารกับเซิร์ฟเวอร์การจัดการคีย์ภายใน XClarity Controller

หมายเหตุ: กำหนดค่าเซิร์ฟเวอร์การจัดการคีย์อย่างน้อยสองชุด (เซิร์ฟเวอร์หลักและรอง) ที่มีโปรโตคอลเดียวกันสำหรับอุปกรณ์ของคุณ หากเซิร์ฟเวอร์การจัดการคีย์หลักไม่ตอบสนองความพยายามในการเชื่อมต่อจาก XClarity Controller จะมีการเริ่มต้นการพยายามเชื่อมต่อกับเซิร์ฟเวอร์การจัดการคีย์เสริมจนกว่าจะเชื่อมต่อได้สำเร็จ

จะต้องมีการเชื่อมต่อ Transport Layer Security (TLS) ระหว่าง XClarity Controller และเซิร์ฟเวอร์การจัดการคีย์ XClarity Controller จะตรวจสอบความถูกต้องของเซิร์ฟเวอร์การจัดการคีย์โดยเปรียบเทียบใบรับรองเซิร์ฟเวอร์ที่ส่งมาโดยเซิร์ฟเวอร์การจัดการคีย์กับใบรับรองเซิร์ฟเวอร์การจัดการคีย์ที่มีการนำเข้าไปไว้ในพื้นที่จัดเก็บที่น่าเชื่อถือของ XClarity Controller ก่อนหน้านี้ เซิร์ฟเวอร์การจัดการคีย์จะตรวจสอบความถูกต้อง XClarity Controller แต่ละชุดที่สื่อสารกับตนเอง และตรวจสอบเพื่อยืนยันว่า XClarity Controller นั้นได้รับอนุญาตให้เข้าถึงเซิร์ฟเวอร์การจัดการคีย์ได้ การตรวจสอบความถูกต้องนี้ดำเนินการโดยเปรียบเทียบใบรับรองของไคลเอ็นต์ ซึ่งส่งมาจาก XClarity Controller เข้ากับรายการใบรับรองที่น่าเชื่อถือ ซึ่งจัดเก็บอยู่ภายในเซิร์ฟเวอร์การจัดการคีย์

เซิร์ฟเวอร์การจัดการคีย์อย่างน้อยหนึ่งชุดจะเชื่อมต่อ และกลุ่มอุปกรณ์จะถูกพิจารณาเป็นตัวเลือก จำเป็นต้องมีการนำเข้าใบรับรองเซิร์ฟเวอร์การจัดการคีย์ในขณะที่ใบรับรองของไคลเอ็นต์จะต้องมีการระบุ โดยค่าเริ่มต้น ระบบจะใช้ใบรับรอง HTTPS หากต้องการเปลี่ยนใบรับรอง คุณสามารถสร้างใบรับรองใหม่แทน

หมายเหตุ: ในการเชื่อมต่อเซิร์ฟเวอร์ KMIP (KeySecure และ CipherTrust) ต้องสร้างคำขอการลงนามใบรับรอง (CSR) และชื่อทั่วไปต้องตรงกับชื่อผู้ใช้ที่กำหนดในเซิร์ฟเวอร์ KMIP แล้วจึงนำเข้าใบรับรองที่ลงนามโดยหน่วยงานผู้ออกใบรับรอง (CA) ที่เซิร์ฟเวอร์ KMIP เชื่อถือสำหรับ CSR

การกำหนดค่าเซิร์ฟเวอร์การจัดการคีย์

ใช้ข้อมูลในหัวข้อนี้เพื่อสร้างชื่อโฮสต์หรือที่อยู่ IP และข้อมูลพอร์ตที่เกี่ยวข้องสำหรับเซิร์ฟเวอร์การจัดการคีย์

ส่วนการกำหนดค่าเซิร์ฟเวอร์การจัดการคีย์ประกอบด้วยฟิลด์ดังต่อไปนี้:

ชื่อโฮสต์หรือที่อยู่ IP

ป้อนชื่อโฮสต์ (หากเปิดใช้งานหรือมีการกำหนดค่า DNS ไว้) หรือที่อยู่ IP ของเซิร์ฟเวอร์การจัดการคีย์ลงในฟิลด์นี้ สามารถเพิ่มเซิร์ฟเวอร์ได้สูงสุดสี่ชุด

พอร์ต

ป้อนหมายเลขพอร์ตสำหรับเซิร์ฟเวอร์การจัดการคีย์ลงในฟิลด์นี้ หากฟิลด์นี้เว้นว่างไว้ ระบบจะใช้ค่าเริ่มต้นที่ 5696 แทน ค่าของหมายเลขพอร์ตที่ใช้งานได้คือ 1 ถึง 65535

การกำหนดค่ากลุ่มอุปกรณ์

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่ากลุ่มอุปกรณ์ที่ใช้ในเซิร์ฟเวอร์ SKLM

ในเซิร์ฟเวอร์ SKLM กลุ่มอุปกรณ์ช่วยให้ผู้ใช้สามารถจัดการคีย์ไดรฟ์แบบเข้ารหัสด้วยตนเอง (SED) บนหลายเซิร์ฟเวอร์แบบเป็นกลุ่ม คุณจำเป็นต้องสร้างกลุ่มอุปกรณ์โดยใช้ชื่อเดียวกันบนเซิร์ฟเวอร์ SKLM ด้วย

ส่วนกลุ่มอุปกรณ์ประกอบด้วยฟิลด์ต่างๆ ดังนี้:

กลุ่มอุปกรณ์

กลุ่มอุปกรณ์ช่วยให้ผู้ใช้จัดการคีย์สำหรับ SED ภายในเซิร์ฟเวอร์หลายชุดได้ในรูปแบบกลุ่ม คุณจำเป็นต้องสร้างกลุ่มอุปกรณ์โดยใช้ชื่อเดียวกันบนเซิร์ฟเวอร์ SKLM ด้วย ค่าเริ่มต้นสำหรับฟิลด์นี้คือ IBM_SYSTEM_X_SED

การสร้างการจัดการใบรับรอง

หัวข้อนี้แสดงข้อมูลเกี่ยวกับการจัดการใบรับรองของไคลเอ็นต์และเซิร์ฟเวอร์

ใบรับรองของไคลเอ็นต์และเซิร์ฟเวอร์จะใช้เพื่อรับรองความถูกต้องของการสื่อสารระหว่างเซิร์ฟเวอร์ SKLM และ XClarity Controller ซึ่งอยู่ภายในเซิร์ฟเวอร์ ThinkSystem ส่วนนี้จะอธิบายถึงการจัดการใบรับรองของไคลเอ็นต์และเซิร์ฟเวอร์

การจัดการใบรับรองของไคลเอ็นต์

หัวข้อนี้แสดงข้อมูลเกี่ยวกับการจัดการใบรับรองของไคลเอ็นต์

ใบรับรองของไคลเอ็นต์จะจัดอยู่ในประเภทใดประเภทหนึ่งดังต่อไปนี้

- ใบรับรอง XClarity Controller แบบลงนามด้วยตนเอง
- ใบรับรองที่สร้างขึ้นจากคำขอการลงนามใบรับรอง (CSR) ของ XClarity Controller และมีการลงนาม (ภายนอก) โดย CA ซึ่งเป็นบุคคลที่สาม

ใบรับรองของไคลเอ็นต์ที่จำเป็นสำหรับการสื่อสารกับเซิร์ฟเวอร์ SKLM ใบรับรองของไคลเอ็นต์ประกอบด้วยลายเซ็นดิจิตอลของ CA และ XClarity Controller

หมายเหตุ:

- ใบรับรองจะมีการจัดเก็บไว้ในการอัปเดตเฟิร์มแวร์

- หากไม่มีการสร้างใบรับรองของไคลเอ็นต์เพื่อใช้สื่อสารกับเซิร์ฟเวอร์ SKLM จะมีการใช้ใบรับรองเซิร์ฟเวอร์ HTTPS ของ XClarity Controller แทน
- ฟังก์ชันของ CA คือการตรวจสอบข้อมูลประจำตัวของ XClarity Controller

ในการสร้างใบรับรองของไคลเอ็นต์ ให้คลิกไอคอนเครื่องหมายบวก ( ) และเลือกรายการใดรายการหนึ่งต่อไปนี้:

- สร้างคีย์และใบรับรองที่ลงนามเองใหม่
- สร้างคีย์และคำขอการลงนามใบรับรองใหม่ (CSR)

ตัวเลือกการดำเนินการ **สร้างคีย์และใบรับรองที่ลงนามเองใหม่** จะสร้างคีย์การเข้ารหัสชุดใหม่และใบรับรองที่ลงนามเอง ในหน้าต่าง สร้างคีย์และใบรับรองที่ลงนามเองใหม่ ให้ป้อนหรือเลือกข้อมูลในฟิลด์ที่จำเป็นและฟิลด์เสริมอื่นๆ ซึ่งใช้กับการกำหนดค่าของคุณ (ดูตารางถัดไป) คลิก **ตกลง** เพื่อสร้างคีย์การเข้ารหัสและใบรับรอง หน้าต่างการดำเนินการจะปรากฏขึ้น ระหว่างที่ระบบสร้างใบรับรองที่ลงนามเอง หน้าต่างยืนยันจะปรากฏขึ้นเมื่อติดตั้งใบรับรองเรียบร้อยแล้ว

หมายเหตุ: คีย์การเข้ารหัสใหม่และใบรับรองจะแทนที่คีย์และใบรับรองเดิมที่มีอยู่

ตาราง 3. สร้างคีย์และใบรับรองที่ลงนามเองใหม่

ตารางแบบสองคอลัมน์พร้อมส่วนหัว แสดงรายละเอียดฟิลด์บังคับและฟิลด์เสริมของการดำเนินการ สร้างคีย์และใบรับรองที่ลงนามเองใหม่ แถวล่างสุดจะขยายครอบคลุมพื้นที่ทั้งสองคอลัมน์

ฟิลด์	รายละเอียด
ประเทศ[1]	จากในรายการ ให้เลือกประเทศที่เป็นที่อยู่ทางกายภาพของ BMC
รัฐหรือจังหวัด[1]	ป้อนชื่อรัฐหรือจังหวัดซึ่งเป็นที่อยู่ทางกายภาพของ BMC
เมืองหรือท้องถิ่น[1]	ป้อนชื่อเมืองหรือท้องถิ่นซึ่งเป็นที่อยู่ทางกายภาพของ BMC
ชื่อของหน่วยงาน[1]	ป้อนชื่อบริษัทหรือหน่วยงานที่เป็นเจ้าของ BMC
ชื่อโฮสต์ BMC[1]	ป้อนชื่อโฮสต์ของ BMC ที่ปรากฏบนแถบที่อยู่เว็บ
ชื่อผู้ติดต่อ	ป้อนชื่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC
ที่อยู่อีเมล	ป้อนที่อยู่อีเมลของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC
แผนกขององค์กร	ป้อนชื่อแผนกภายในบริษัท ซึ่งเป็นเจ้าของ BMC
นามสกุล	ป้อนนามสกุลของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ

ตาราง 3. สร้างคีย์และใบรับรองที่ลงนามเองใหม่ (มีต่อ)

ฟิลด์	รายละเอียด
ชื่อ	ป้อนชื่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
ชื่อย่อ	ป้อนชื่อย่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 20 อักขระ
ตัวที่มีคุณสมบัติ DN	ป้อนตัวที่มีคุณสมบัติชื่อที่ใช้ระบุของ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
1. ฟิลด์นี้ต้องระบุข้อมูล	

หลังจากสร้างใบรับรองของไคลเอ็นต์แล้ว คุณสามารถดาวน์โหลดใบรับรองเพื่อจัดเก็บภายใน XClarity Controller โดยเลือกที่การดำเนินการ **ดาวน์โหลดใบรับรอง**

ตัวเลือกการดำเนินการ **สร้างคีย์และคำขอการลงนามใบรับรองใหม่** (CSR) จะสร้างคีย์การเข้ารหัสชุดใหม่และ CSR ในหน้าต่าง สร้างคีย์และคำขอการลงนามใบรับรองใหม่ ให้ป้อนหรือเลือกข้อมูลในฟิลด์ที่จำเป็นและฟิลด์เสริมอื่นๆ ซึ่งใช้กับการกำหนดค่าของคุณ (ดูตารางถัดไป) คลิก **ตกลง** เพื่อสร้างคีย์การเข้ารหัสใหม่และ CSR

หน้าต่างการดำเนินการจะปรากฏขึ้นระหว่างที่ระบบสร้าง CSR เมื่อการดำเนินการเสร็จสมบูรณ์ หน้าต่างการยืนยันจะปรากฏขึ้น หลังจากสร้าง CSR แล้ว คุณจะต้องส่ง CSR ไปยังหน่วยงานด้านใบรับรอง (CA) เพื่อการลงนามแบบดิจิตอล เลือก **ดาวน์โหลดคำขอการลงนามใบรับรอง** (CSR) แล้วคลิก **ตกลง** เพื่อบันทึก CSR ลงในเซิร์ฟเวอร์ของคุณ จากนั้นให้คุณส่ง CSR ไปยังหน่วยงาน CA ของคุณเพื่อลงนาม

ตาราง 4. สร้างคีย์และคำขอการลงนามใบรับรองใหม่

ตารางแบบสองคอลัมน์พร้อมส่วนหัว แสดงรายละเอียดฟิลด์บังคับและฟิลด์เสริมของการดำเนินการ สร้างคีย์และคำขอการลงนามใบรับรองใหม่ แถวล่างสุดจะขยายครอบคลุมพื้นที่ทั้งสองคอลัมน์

ฟิลด์	รายละเอียด
ประเทศ[1]	จากในรายการ ให้เลือกประเทศที่เป็นที่อยู่ทางกายภาพของ BMC
รัฐหรือจังหวัด[1]	ป้อนชื่อรัฐหรือจังหวัดซึ่งเป็นที่อยู่ทางกายภาพของ BMC
เมืองหรือท้องถิ่น[1]	ป้อนชื่อเมืองหรือท้องถิ่นซึ่งเป็นที่อยู่ทางกายภาพของ BMC
ชื่อของหน่วยงาน[1]	ป้อนชื่อบริษัทหรือหน่วยงานที่เป็นเจ้าของ BMC

ตาราง 4. สร้างคีย์และคำขอการลงนามใบรับรองใหม่ (มีต่อ)

ฟิลด์	รายละเอียด
ชื่อโฮสต์ BMC[1]	ป้อนชื่อโฮสต์ของ BMC ที่ปรากฏบนแถบที่อยู่เว็บ
ชื่อผู้ติดต่อ	ป้อนชื่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC
ที่อยู่อีเมล	ป้อนที่อยู่อีเมลของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC
แผนกขององค์กร	ป้อนชื่อแผนกภายในบริษัท ซึ่งเป็นเจ้าของ BMC
นามสกุล	ป้อนนามสกุลของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
ชื่อ	ป้อนชื่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
ชื่อย่อ	ป้อนชื่อย่อของผู้ติดต่อซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 20 อักขระ
ตัวที่มีคุณสมบัติ DN	ป้อนตัวที่มีคุณสมบัติชื่อที่ใช้ระบุของ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
รหัสผ่านทดสอบ	ป้อนรหัสผ่านของ CSR ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 30 อักขระ
ชื่อแบบไม่มีโครงสร้าง	ป้อนข้อมูลเพิ่มเติม เช่น ชื่อแบบไม่มีโครงสร้างแน่นอน ซึ่งกำหนดให้กับ BMC ฟิลด์นี้สามารถกรอกข้อมูลได้ไม่เกิน 60 อักขระ
1. ฟิลด์นี้ต้องระบุข้อมูล	

คำขอ CSR จะได้รับการลงนามแบบดิจิตอลโดยหน่วยงาน CA โดยใช้เครื่องมือการดำเนินการด้านใบรับรองของผู้ใช้ เช่น *OpenSSL* หรือเครื่องมือบรรทัดคำสั่ง *Certutil* ใบรับรองของไคลเอ็นต์ทั้งหมดที่ลงนามโดยใช้เครื่องมือการดำเนินการด้านใบรับรองของผู้ใช้จะมีใบรับรอง *พื้นฐาน* ที่เหมือนกัน ใบรับรอง *พื้นฐาน* นี้จะต้องนำเข้าไปยังเซิร์ฟเวอร์ SKLM ด้วย เพื่อให้เซิร์ฟเวอร์ทั้งหมดที่ลงนามแบบดิจิตอลโดยผู้ใช้ได้รับการยอมรับจากเซิร์ฟเวอร์ SKLM

หลังจากใบรับรองได้รับการลงนามโดย CA แล้ว คุณจะต้องนำเข้าใบรับรองไปยัง BMC ให้เลือกรายการการดำเนินการ **นำเข้าใบรับรองที่ลงนาม** แล้วเลือกไฟล์ที่ต้องการอัปโหลดเป็นใบรับรองของไคลเอ็นต์ จากนั้นให้คลิก **ตกลง** หน้าต่างการดำเนินการจะปรากฏขึ้น ระหว่างที่ใบรับรองที่ลงนามโดย CA ถูกอัปโหลด หากการอัปโหลดเสร็จสมบูรณ์ หน้าต่าง

การอัปโหลดใบรับรองจะปรากฏขึ้น หากการอัปโหลดไม่เสร็จสมบูรณ์ หน้าต่างข้อผิดพลาดการอัปโหลดใบรับรองจะปรากฏขึ้น

หมายเหตุ:

- เพื่อเพิ่มการรักษาความปลอดภัย ควรใช้ใบรับรองที่ได้รับการลงนามแบบดิจิตอลโดย CA
- ใบรับรองที่นำเข้าไปยัง XClarity Controller จะต้องสอดคล้องกับ CSR ที่สร้างขึ้นก่อนหน้า

หลังจากนำเข้าใบรับรองที่ลงนามโดย CA ไปยัง BMC แล้ว ให้เลือก **ดาวน์โหลดใบรับรอง** เมื่อคุณเลือกการดำเนินการนี้ ระบบจะดาวน์โหลดใบรับรองที่ลงนามโดย CA จาก XClarity Controller เพื่อจัดเก็บไว้ภายในระบบของคุณ

การจัดการใบรับรองของเซิร์ฟเวอร์

หัวข้อนี้แสดงข้อมูลเกี่ยวกับการจัดการใบรับรองของเซิร์ฟเวอร์

ใบรับรองของเซิร์ฟเวอร์จะสร้างขึ้นภายในเซิร์ฟเวอร์ของ SKLM และจะต้องนำเข้าไปใน XClarity Controller ก่อนคุณสมบัติการเข้าถึงไดรฟ์แบบปลอดภัยจึงจะสามารถทำงานได้ ในการนำเข้าใบรับรองซึ่งทำหน้าที่รับรองความถูกต้องของเซิร์ฟเวอร์ SKLM ให้กับ BMC ให้คลิก **นำเข้าใบรับรอง** จากในส่วนสถานะใบรับรองของเซิร์ฟเวอร์ภายในหน้าการเข้าถึงไดรฟ์ ตัวบ่งชี้การดำเนินการจะแสดงขึ้น ระหว่างที่ไฟล์ถูกถ่ายโอนไปยังที่จัดเก็บข้อมูลบน XClarity Controller

หลังจากที่ใบรับรองมีการถ่ายโอนไปยัง XClarity Controller สำเร็จเรียบร้อยแล้ว พื้นที่สถานะใบรับรองของเซิร์ฟเวอร์จะแสดงเนื้อหาต่อไปนี้: `A server certificate is installed`

หากคุณต้องการเอาใบรับรองที่น่าเชื่อถือออก ให้คลิกที่ปุ่ม **นำออก** ของใบรับรองที่เกี่ยวข้อง

Security Password Manager

ใช้ข้อมูลในหัวข้อนี้เพื่ออนุญาตรหัสผ่านของบุคคลที่สาม

คุณลักษณะนี้ช่วยให้ผู้ใช้ตัดสินใจได้ว่าจะอนุญาตให้ใช้รหัสผ่านของบุคคลที่สามหรือไม่

- **รหัสผ่านของบุคคล** : เมื่อเปิดใช้งานแล้ว BMC จะสามารถใช้แฮชรหัสผ่านที่ผู้ใช้ให้ไว้สำหรับการตรวจสอบสิทธิ์
- **อนุญาตการดึงรหัสผ่านของบุคคลที่สาม** : ผู้ใช้ยังสามารถเปิดหรือปิดการดึงแฮชรหัสผ่านของบุคคลที่สามจาก BMC ได้

บันทึกการตรวจสอบเพิ่มเติม

ใช้ข้อมูลในหัวข้อนี้เพื่อควบคุมบันทึกการตรวจสอบเพิ่มเติม

คุณลักษณะนี้จะช่วยให้คุณสามารถตัดสินใจว่าจะรวมรายการบันทึกของคำสั่งการตั้งค่า IPMI (ข้อมูลดิบ) จากช่อง LAN และ KCS ลงในบันทึกการตรวจสอบหรือไม่

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า** BMC บนเว็บ XCC เพื่อเปิดใช้งาน/ปิดใช้งานบันทึกการตรวจสอบเพิ่มเติม

หมายเหตุ: หากคำสั่งการตั้งค่า IPMI มาจากช่อง LAN ชื่อผู้ใช้และที่อยู่ IP ต้นทางจะรวมอยู่ในข้อความบันทึก และคำสั่ง IPMI ทั้งหมดที่มีข้อมูลการรักษาความปลอดภัยที่ละเอียดอ่อน (เช่น รหัสผ่าน) จะถูกแยกออก

จำกัดการเข้าสู่ระบบที่เกิดขึ้นพร้อมกันต่อบัญชีผู้ใช้

ใช้ข้อมูลในหัวข้อนี้เพื่อจำกัดเซสชันที่เกิดพร้อมกันต่อบัญชีผู้ใช้

คุณลักษณะนี้ช่วยให้ผู้ใช้กำหนดจำนวนเซสชันที่เกิดพร้อมกันที่อนุญาตต่อบัญชีผู้ใช้ได้

- **จำนวนเซสชันที่เกิดขึ้นพร้อมกันบนเว็บ** : กำหนดเอาไว้ได้ตั้งแต่ 1 ถึง 10 ครั้ง
- **จำนวนเซสชันที่เกิดขึ้นพร้อมกันของบรรทัดสั่ง** : สามารถตั้งค่าได้ 1 หรือ 2 เซสชัน
- **จำนวนเซสชันที่เกิดขึ้นพร้อมกันบน** Redfish : กำหนดเอาไว้ได้ตั้งแต่ 1 ถึง 16 ครั้ง

หมายเหตุ: หากจำนวนเซสชันทั้งหมดเกินจำนวนที่ตั้งไว้ ผู้ใช้จะสร้างเซสชันใหม่ไม่ได้อีกต่อไป

System Guard

หัวข้อนี้แสดงภาพรวมของ System Guard

คุณลักษณะ System Guard จะถ่ายภาพสแน็ปช็อตของคลังส่วนประกอบฮาร์ดแวร์เป็นข้อมูลอ้างอิงที่เชื่อถือได้ จากนั้นจะตรวจสอบหาค่าความคลาดเคลื่อนใดๆ จากภาพสแน็ปช็อตอ้างอิง เมื่อเกิดความคลาดเคลื่อน เซิร์ฟเวอร์จะสามารถรายงานเหตุการณ์ให้ผู้ใช้ทราบ นอกจากนี้ ยังสามารถป้องกันไม่ให้เซิร์ฟเวอร์บูตเข้าสู่ระบบปฏิบัติการและแจ้งให้ผู้ใช้ตอบกลับ

ผู้ใช้สามารถถ่ายภาพสแน็ปช็อตได้ตลอดเวลา แม้ในขณะที่ปิดใช้งานคุณลักษณะนี้ก็ตาม การสร้างภาพสแน็ปช็อตใช้เวลาประมาณหนึ่งนาที ผู้ใช้สามารถเลือกชุดย่อยของส่วนประกอบฮาร์ดแวร์เพื่อบังคับใช้ และเลือกการดำเนินการที่เกี่ยวข้องเมื่อตรวจพบความคลาดเคลื่อน

หมายเหตุ: การตรวจจับความคลาดเคลื่อนจะดำเนินการเมื่อเซิร์ฟเวอร์เปิด (POST) หรือรีบูตระบบ ตัวอย่างเช่น ในขณะที่ระบบปฏิบัติการยังคงทำงานอยู่ หากดิสก์ไดร์ฟถูกดึงออกมาแล้วเสียบกลับเข้าไปใหม่ในภายหลัง System Guard จะไม่บันทึกเหตุการณ์หรือดำเนินการใดๆ หากดิสก์ไดร์ฟที่ดึงออกมาไม่ได้มีการเสียบกลับไปจนกว่าจะรีบูตครั้งถัดไป กรณีนี้ System Guard จะทำงาน

การเปิดใช้งาน System Guard

ใช้ข้อมูลในหัวข้อนี้เพื่อเปิดใช้งานระบบ System Guard

คุณลักษณะ System Guard ถูกปิดใช้งานตามค่าเริ่มต้น เปิดใช้งานก่อนจัดส่งตามความต้องการของผู้ใช้ปลายทาง

นอกจากนี้ ตัวเลือกการรีเซ็ตเป็นค่าเริ่มต้นของ XCC ยังปิดใช้งาน System Guard และล้างการตั้งค่าด้วย ยกเว้นประวัติภาพ

ขณะเปิดใช้งาน System Guard ผู้ใช้จะถูกขอให้ยืนยันการตั้งค่า ใช้ภาพที่เชื่อถือได้ที่มีอยู่แล้ว หรือถ่ายภาพคลังข้อมูลใหม่ที่เชื่อถือได้ก่อนที่จะเปิดการป้องกัน System Guard เมื่อเปิดใช้งานแล้ว:

- หากระบบปิดอยู่ System Guard จะเริ่มกลบล้างรายการฮาร์ดแวร์ทันที
- หากระบบเปิดอยู่ System Guard จะเปรียบเทียบข้อมูลในคลังข้อมูลของส่วนประกอบกับภาพที่เชื่อถือได้

หากผลลัพธ์ของการเปรียบเทียบบ่งชี้ว่ามีความคลาดเคลื่อนจากภาพที่เชื่อถือได้ XCC จะแสดงคำเตือน **ไม่เป็นไปตามข้อกำหนดเนื่องจากการกำหนดค่าฮาร์ดแวร์ไม่ตรงกัน** รายละเอียดของรายการที่ไม่ตรงกันแต่ละองค์ประกอบฮาร์ดแวร์ที่ขาดหายไป/เปลี่ยนแปลง/ใหม่ พร้อมแอตทริบิวต์ตำแหน่ง/ตัวระบุ/คำอธิบาย เปรียบเทียบกับภาพที่เชื่อถือได้

ผู้ใช้สามารถกำหนดค่าขอบเขตและการดำเนินการของ System Guard และตัดสินใจว่าจะดำเนินการใดเมื่อระบบไม่เป็นไปตามข้อกำหนดผ่านแผง Scope and Action

การตั้งค่าการเข้ารหัส

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจการตั้งค่าการเข้ารหัสแบบต่างๆ

โหมดการรักษาความปลอดภัยสูง

- รองรับเฉพาะรหัสแบบใหม่และแบบมีประสิทธิภาพเท่านั้น
- สอดคล้องตามมาตรฐาน NIST
- สอดคล้องตามมาตรฐาน PFS (Perfect Forward Secrecy)

โหมดความเข้ากันได้

- รองรับชุดรหัสที่หลากหลายเพื่อความเข้ากันได้สูงสุด
- ไม่สอดคล้องตามมาตรฐาน PFS และ NIST

โหมดสอดคล้องตามมาตรฐาน NIST

- รองรับชุดรหัสที่หลากหลายเพื่อความเข้ากันได้สูงสุด
- สอดคล้องตามมาตรฐาน NIST
- สอดคล้องตามมาตรฐาน PFS

เวอร์ชัน TLS ที่รองรับ

- TLS 1.0 ขึ้นไป
- TLS 1.1 ขึ้นไป
- TLS 1.2 ขึ้นไป
- TLS 1.3

การตั้งค่าการเข้ารหัส TLS คือการจำกัดชุดรหัส TLS ที่รองรับสำหรับบริการ BMC

โปรดดูตารางต่อไปนี้สำหรับการตั้งค่าต่างๆ ที่รองรับชุดรหัส TLS

โหมดรักษาความปลอดภัย	**เวอร์ชัน TLS**	**ชุดรหัส TLS**
โหมดการรักษาความปลอดภัยสูง	TLS 1.3	• TLS_AES_256_GCM_SHA384
โหมดการรักษาความปลอดภัยสูง	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
โหมดสอดคล้องตามมาตรฐาน NIST	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256

โหมดรักษาความปลอดภัย	**เวอร์ชัน TLS**	**ชุดรหัส TLS**
โหมดสอดคล้องตามมาตรฐาน NIST	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
โหมดความเข้ากันได้	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256

โหมดรักษาความปลอดภัย	เวอร์ชัน TLS	ชุดรหัส TLS
โหมดความเข้ากันได้	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
โหมดความเข้ากันได้	TLS 1.1 TLS 1.0	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

การกำหนดค่า Call Home

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่า Call Home

คุณสามารถสร้างระบบส่งต่อบริการที่ส่งข้อมูลบริการสำหรับอุปกรณ์ที่ได้รับการจัดการใดๆ ไปยังฝ่ายสนับสนุนของ Lenovo โดยอัตโนมัติโดยใช้ฟังก์ชัน Call Home

Lenovo มีความมุ่งมั่นต่อการรักษาความปลอดภัยเป็นอย่างยิ่ง เมื่อเปิดใช้งาน Call Home จะติดต่อ Lenovo เพื่อเปิดทิคเก็ตบริการและส่งข้อมูลบริการจากอุปกรณ์ที่ได้รับการจัดการ เมื่ออุปกรณ์นั้นรายงานฮาร์ดแวร์ทำงานขัดข้อง ข้อมูลบริการที่คุณมักจะอัปโหลดด้วยตนเองไปยังฝ่ายสนับสนุนของ Lenovo จะถูกส่งไปยังศูนย์บริการสนับสนุนของ Lenovo

โดยอัตโนมัติผ่านทาง HTTPS โดยใช้ TLS 1.2 ขึ้นไป ระบบจะไม่ส่งข้อมูลทางธุรกิจของคุณ การเข้าถึงข้อมูลบริการในศูนย์บริการสนับสนุนของ Lenovo จะจำกัดเฉพาะเจ้าหน้าที่บริการที่ได้รับอนุญาตเท่านั้น

การเข้าสู่หน้า Call Home เป็นครั้งแรก

เมื่อเข้าสู่หน้า Call Home เป็นครั้งแรก คุณจะเห็นหน้าต่างคำเตือน ให้คลิก “ดูข้อกำหนดและเงื่อนไข” เพื่อดำเนินการต่อ

ข้อคำนึง: คุณต้องยอมรับ **คำชี้แจงเรื่องความเป็นส่วนตัวของ Lenovo** ก่อนที่คุณจะสามารถถ่ายโอนข้อมูลไปยังฝ่ายสนับสนุนของ Lenovo ได้ การดำเนินการนี้จะต้องทำเพียงครั้งเดียวเมื่อเข้าสู่หน้าครั้งแรก

หมายเหตุ: คุณสามารถอ่าน “ดูข้อกำหนดและเงื่อนไข” และ **คำชี้แจงเรื่องความเป็นส่วนตัวของ Lenovo** ได้ที่ด้านบนของหน้าทุกเมื่อ

กำหนดค่า Call Home

ต้องกรอกข้อมูลในเก้าฟิลด์ที่จำเป็นต่อไปนี้:

- ประเทศ
- ชื่อผู้ติดต่อ
- หมายเลขโทรศัพท์
- อีเมล
- รหัสไปรษณีย์
- ชื่อบริษัท
- ที่อยู่
- เมือง
- รัฐ/จังหวัด

ข้อคำนึง: ต้องกรอกข้อมูลในฟิลด์ที่จำเป็นทั้งหมด ไม่เช่นนั้นคุณจะไม่สามารถใช้การเปลี่ยนแปลงและเปิดใช้งาน**การรายงานไปยังฝ่ายบริการของ Lenovo** ได้

สถานะทิคเก็ต

แต่ละทิคเก็ตสามารถมีสถานะหนึ่งในห้าสถานะต่อไปนี้ได้:

- **รอดำเนินการ**: กำลังส่งข้อมูลบริการหรือรอการตอบกลับ
- **ดำเนินการอยู่**: ส่งข้อมูลบริการเรียบร้อยแล้ว และกำลังดำเนินการแก้ไขปัญหา
- **ล้มเหลว**: ส่งข้อมูลบริการไม่สำเร็จ

- **ปิด**: ปัญหาได้รับการดำเนินการ และปิดทิคเก็ตแล้ว
- **ยกเลิก**: ปัญหาได้รับการดำเนินการ และยกเลิกทิคเก็ตแล้ว

ทดสอบ Call Home

คุณสามารถทดสอบฟังก์ชัน Call Home ได้โดยคลิกที่ “ทดสอบ Call Home” ข้อความจะแสดงที่ด้านบนของหน้าเพื่อระบุว่าการดำเนินการสำเร็จหรือไม่ และคุณจะสามารถตรวจสอบบันทึกเหตุการณ์ด้านล่างเพื่อดูผลการทดสอบได้

- **การดำเนินการ — ยกเลิก**: หากสถานะของทิคเก็ตเป็น “ดำเนินการอยู่” คุณสามารถคลิกไอคอน “เลิกทำ” ในคอลัมน์ “การดำเนินการ” เพื่อยกเลิกทิคเก็ต
- **การดำเนินการ — หมายเหตุ**: เมื่อคุณคลิกไอคอน “หมายเหตุ” ในคอลัมน์ “การดำเนินการ” ระบบจะแสดงพร้อมท์ให้คุณระบุหมายเหตุสำหรับเหตุการณ์ที่เกี่ยวข้อง

  หมายเหตุ: ต้องกรอกข้อมูลชื่อและเนื้อหาข้อความเพื่อส่งหมายเหตุ ฟังก์ชันนี้**จะส่งข้อมูลไปยังเซิร์ฟเวอร์เท่านั้น** ไม่ได้ใช้สำหรับการบันทึกและแสดงข้อมูล หากคลิกหมายเหตุอีกครั้ง คุณจะได้รับพร้อมท์ที่แสดงหน้าต่างหมายเหตุใหม่เพื่อระบุข้อความอีกรายการ

ข้อคำนึง: หากต้องการเรียกใช้ Call Home โปรดตรวจสอบให้แน่ใจว่าการตั้งค่า DNS นั้นถูกต้องและมีการเชื่อมต่อกับอินเทอร์เน็ตที่ Call Home ใช้ได้ หาก XClarity Controller เข้าถึงอินเทอร์เน็ตผ่านทางพร็อกซี HTTP ให้ตรวจสอบว่ามีการกำหนดค่าพร็อกซีเซิร์ฟเวอร์ให้ใช้การตรวจสอบความถูกต้องพื้นฐาน และตั้งค่าเป็นพร็อกซีที่ไม่มีการยกเลิก

พร็อกซี HTTP

พร็อกซี HTTP ทำหน้าที่เป็นตัวกลางสองบทบาท ได้แก่ ไคลเอ็นต์ HTTP และเซิร์ฟเวอร์ HTTP สำหรับการรักษาความปลอดภัย การจัดการ และฟังก์ชันการทำงานสำหรับการแคช พร็อกซี HTTP กำหนดเส้นทางคำขอของไคลเอ็นต์ HTTP จากเว็บเบราเซอร์ไปยังอินเทอร์เน็ต ในขณะที่สนับสนุนการแคชข้อมูลจากอินเทอร์เน็ต

- **ที่อยู่เซิร์ฟเวอร์พร็อกซี**: ฟิลด์นี้จำเป็นสำหรับการเปิดใช้งานพร็อกซี HTTP สามารถกรอกข้อมูลได้ไม่เกิน 63 อักขระในฟิลด์นี้ ช่วยให้ผู้ใช้ระบุที่อยู่ IP หรือชื่อโฮสต์ได้ ชื่อโฮสต์ต้องประกอบด้วยตัวอักษรและตัวเลข เครื่องหมายขีดกลาง ('-') และขีดล่าง ('_')
- **พอร์ต**: ฟิลด์นี้จำเป็นสำหรับการระบุพอร์ตของพร็อกซี HTTP สามารถกรอกหมายเลขได้ตั้งแต่ 1-65535 ในฟิลด์นี้เท่านั้น
- **ทดสอบพร็อกซี**: หากต้องการเปิดใช้งานคุณลักษณะนี้ คุณจำเป็นต้องกรอกข้อมูลตำแหน่งพร็อกซีและพอร์ตพร็อกซีที่ถูกต้องเพื่อทดสอบว่ามีฟังก์ชันพร็อกซี HTTP ปัจจุบันพร้อมใช้งานหรือไม่
- **ชื่อผู้ใช้**: หากเลือกตัวเลือก **ต้องมีการตรวจสอบความถูกต้อง** คุณจะต้องระบุชื่อผู้ใช้และแสดงข้อมูลรับรองพร็อกซี สามารถกรอกข้อมูลได้ไม่เกิน 30 อักขระในฟิลด์นี้ และใช้ช่องว่างไม่ได้
- **รหัสผ่าน**: ฟิลด์นี้ไม่บังคับและจะแสดงหากเลือกตัวเลือก 'ต้องมีการตรวจสอบความถูกต้อง' สามารถกรอกข้อมูลได้ไม่เกิน 15 อักขระในฟิลด์นี้ และใช้ช่องว่างไม่ได้

การสำรองข้อมูลและคืนค่าการกำหนดค่า BMC

ข้อมูลในหัวข้อนี้จะอธิบายวิธีคืนค่าหรือแก้ไขการกำหนดค่า BMC

เลือก **สำรองข้อมูลและคืนค่า** ภายใต้ **การกำหนดค่า BMC** เพื่อดำเนินการต่างๆ ต่อไปนี้:

- ดูข้อมูลสรุปเกี่ยวกับการกำหนดค่าตัวควบคุมการจัดการ
- สำรองข้อมูลหรือคืนค่าการกำหนดค่าตัวควบคุมการจัดการ
- ดูสถานะการสำรองข้อมูลและคืนค่า
- รีเซ็ตการกำหนดค่าตัวควบคุมการจัดการเป็นการตั้งค่าเริ่มต้นจากโรงงาน
- เข้าถึงตัวช่วยสร้างการตั้งค่าเริ่มต้นของตัวควบคุมการจัดการ

การสำรองข้อมูลการกำหนดค่า BMC

ข้อมูลในหัวข้อนี้จะอธิบายวิธีสำรองข้อมูลการกำหนดค่า BMC

เลือก **สำรองข้อมูลและคืนค่า** ภายใต้ **การกำหนดค่า BMC** ที่ด้านบนสุดคือส่วน **สำรองข้อมูลการกำหนดค่า BMC**

หากมีการสำรองข้อมูลก่อนหน้านี้ คุณจะเห็นรายละเอียดในฟิลด์ **การสำรองข้อมูลล่าสุด**

ในการสำรองข้อมูลการกำหนดค่า BMC ปัจจุบัน ให้ดำเนินการตามขั้นตอนที่แสดงไว้ด้านล่าง:

1. ระบุรหัสผ่านสำหรับไฟล์สำรองข้อมูล BMC
2. เลือกว่าคุณต้องการเข้ารหัสทั้งไฟล์หรือเฉพาะข้อมูลที่เป็นความลับเท่านั้น
3. เริ่มต้นกระบวนการสำรองข้อมูลโดยคลิก **เริ่มการสำรองข้อมูล** ระหว่างกระบวนการ คุณจะไม่สามารถดำเนินการคืนค่า/รีเซ็ต
4. เมื่อกระบวนการเสร็จสมบูรณ์ จะมีปุ่มปรากฏขึ้นเพื่อให้คุณดาวน์โหลดและบันทึกไฟล์ได้

หมายเหตุ: เมื่อผู้ใช้ตั้งค่าผู้ใช้/รหัสผ่านของ XClarity Controller ใหม่และทำการสำรองข้อมูลการกำหนดค่า บัญชี/รหัสผ่านเริ่มต้น (`USERID/PASSWORD`) ถูกสำรองข้อมูลไว้ด้วย การลบบัญชี/รหัสผ่านเริ่มต้นจากการสำรองข้อมูลจะทำให้ระบบแสดงข้อความแจ้งเตือนผู้ใช้ว่าเกิดความล้มเหลวในการกู้คืนบัญชี/รหัสผ่าน XClarity Controller ผู้ใช้สามารถละเว้นข้อความนี้ได้

การคืนค่าการกำหนดค่า BMC

ข้อมูลในหัวข้อนี้จะอธิบายวิธีคืนค่าการกำหนดค่า BMC

เลือก **สำรองข้อมูลและคืนค่า** ภายใต้ **การกำหนดค่า BMC** ทางด้านล่าง **สำรองข้อมูลการกำหนดค่า BMC** คือ ส่วน **คืนค่า BMC จากไฟล์การกำหนดค่า**

ในการคืนค่า BMC เป็นการกำหนดค่าที่บันทึกไว้ก่อนหน้า ให้ดำเนินการตามขั้นตอนที่แสดงไว้ด้านล่าง:

1. เรียกดูเพื่อเลือกไฟล์สำรองข้อมูลและป้อนรหัสผ่านเมื่อได้รับข้อความ
2. ตรวจสอบไฟล์โดยคลิก **ดูเนื้อหา** เพื่อดูรายละเอียด
3. หลังจากตรวจสอบเนื้อหา ให้คลิก **เริ่มการคืนค่า**

การรีเซ็ต BMC เป็นค่าเริ่มต้นจากโรงงาน

ข้อมูลในหัวข้อนี้จะอธิบายวิธีรีเซ็ต BMC เป็นการตั้งค่าเริ่มต้นจากโรงงาน

เลือก **สำรองข้อมูลและคืนค่า** ภายใต้ **การกำหนดค่า BMC** ทางด้านล่าง **คืนค่า BMC จากไฟล์การกำหนดค่า** คือ ส่วน **รีเซ็ต BMC เป็นค่าเริ่มต้นจากโรงงาน**

ในการรีเซ็ต BMC เป็นค่าเริ่มต้นจากโรงงาน ให้ดำเนินการตามขั้นตอนที่แสดงไว้ด้านล่าง:

1. คลิก **เริ่มการรีเซ็ต BMC เป็นค่าเริ่มต้นจากโรงงาน**

   หมายเหตุ:

   - เฉพาะผู้ใช้ที่มีสิทธิ์ผู้ใช้ระดับผู้ควบคุมสามารถดำเนินการนี้ได้
   - การเชื่อมต่ออีเทอร์เน็ตถูกตัดการเชื่อมต่อชั่วคราว คุณต้องเข้าสู่ระบบเว็บอินเทอร์เฟซ XClarity Controller อีกครั้ง หลังจากการดำเนินการรีเซ็ตเสร็จสมบูรณ์
   - เมื่อคุณคลิก **เริ่มรีเซ็ต BMC ให้เป็นค่าเริ่มต้นจากโรงงาน** หน้าต่างยืนยันจะปรากฏขึ้น และคุณจะสามารถเลือกช่องกาเครื่องหมายเพื่อรักษาการตั้งค่าต่อไปนี้:
     - **รักษาการตั้งค่าผู้ใช้ภายในระบบ**
     - **รักษาการตั้งค่าเครือข่าย**
   - เมื่อคุณคลิก ตกลง การเปลี่ยนแปลงการกำหนดค่าก่อนหน้านี้ทั้งหมดจะหายไป ยกเว้นการเปลี่ยนแปลงที่คุณเลือกที่จะคงไว้
   - หากคุณต้องการเปิดใช้งาน LDAP เมื่อมีการกู้คืนการกำหนดค่า BMC คุณจะต้องนำเข้าใบรับรองการรักษาความปลอดภัยที่น่าเชื่อถือเสียก่อน
   - หากคุณกำลังทำงานจากระบบภายในของ BMC คุณจะสูญเสียการเชื่อมต่อ TCP/IP คุณจะต้องกำหนดค่าอินเทอร์เฟซเครือข่าย BMC ใหม่เพื่อกู้คืนการเชื่อมต่อ
   - หลังจากกระบวนการเสร็จสมบูรณ์ ระบบจะรีสตาร์ท XClarity Controller
   - การรีเซ็ต BMC เป็นค่าเริ่มต้นจากโรงงานจะไม่ส่งผลกระทบต่อการตั้งค่า UEFI

การรีสตาร์ท XClarity Controller

ข้อมูลในหัวข้อนี้จะอธิบายวิธีรีสตาร์ท XClarity Controller ของคุณ

ดูรายละเอียดเกี่ยวกับวิธีการรีสตาร์ท XClarity Controller ได้ที่ “การดำเนินการด้านพลังงาน” บนหน้าที่ 94

บทที่ 4. การติดตามข้อมูลสถานะเซิร์ฟเวอร์

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจในวิธีการดูและติดตามข้อมูลเซิร์ฟเวอร์ที่คุณกำลังเข้าถึง

เมื่อคุณเข้าสู่ระบบ XClarity Controller หน้าสถานะของระบบจะแสดงขึ้น จากหน้านี้ คุณสามารถดูสถานะฮาร์ดแวร์ของเซิร์ฟเวอร์ บันทึกเหตุการณ์และบันทึกการตรวจสอบ สถานะระบบ ประวัติการบำรุงรักษา และผู้รับการแจ้งเตือน

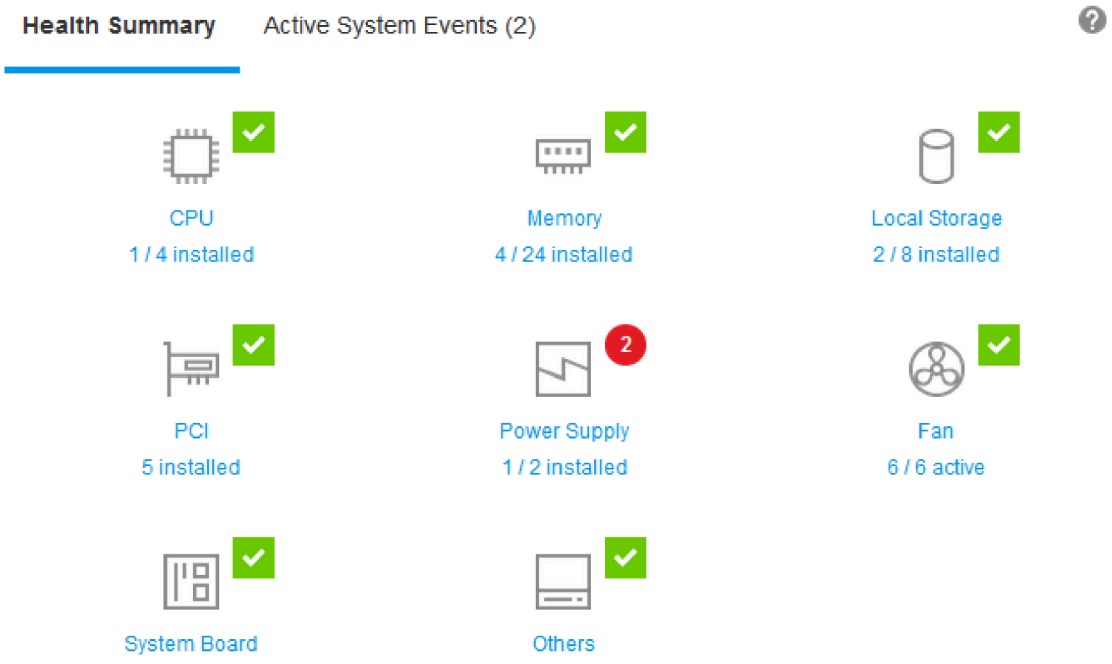
การดูข้อมูลสรุปสถานะ/เหตุการณ์ของระบบที่ดำเนินอยู่

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีการดูข้อมูลสรุปสถานะ/เหตุการณ์ของระบบที่ดำเนินอยู่

เมื่อคุณเข้าถึงหน้าแรกของ XClarity Controller ระบบจะแสดง **ข้อมูลสรุปสถานะ** ตามค่าเริ่มต้น จะมีการแสดงข้อมูลกราฟิก ซึ่งแสดงจำนวนของส่วนประกอบฮาร์ดแวร์ที่มีการติดตั้ง รวมถึงสถานะการทำงานของส่วนประกอบเหล่านั้น ส่วนประกอบฮาร์ดแวร์ที่มีการติดตามสถานะมีดังนี้

- โปรเซสเซอร์ (CPU)
- หน่วยความจำ
- ที่จัดเก็บภายใน
- อะแดปเตอร์ PCI
- แหล่งจ่ายไฟ
- พัดลม
- แผงระบบ
- อื่นๆ

หมายเหตุ: **ที่จัดเก็บภายใน** อาจแสดงสถานะ “ไม่พร้อมใช้งาน” บนไอคอนสถานะบนระบบที่มีการติดตั้งแบ็คเพลนแบบ Simple-swap



หากส่วนประกอบฮาร์ดแวร์ใดๆ เหล่านี้ทำงานผิดปกติ จะมีการแสดงเครื่องหมายด้วยไอคอนวิกฤติหรือการเตือน ภาวะวิกฤติจะแสดงเป็นไอคอนวงกลมสีแดง ขณะที่ภาวะการเตือนจะแสดงเป็นไอคอนสามเหลี่ยมสีเหลือง เมื่อเคลื่อนไอคอนเมาส์ไว้เหนือสัญลักษณ์วิกฤติหรือการเตือน ระบบจะแสดงเหตุการณ์ปัจจุบันสำหรับส่วนประกอบนั้นสูงสุดสามรายการ

หากต้องการเรียกดูเหตุการณ์อื่นๆ ให้คลิกที่แท็บ **เหตุการณ์ของระบบที่ดำเนินอยู่** หน้าต่างจะปรากฏขึ้น พร้อมแสดงเหตุการณ์ที่ดำเนินอยู่ในระบบ ณ ปัจจุบัน คลิก **ดูบันทึกเหตุการณ์ทั้งหมด** เพื่อดูทั้งประวัติเหตุการณ์

หากส่วนประกอบฮาร์ดแวร์แสดงเครื่องหมายถูกสีเขียว แสดงว่าส่วนประกอบทำงานเป็นปกติและไม่มีเหตุการณ์ปัจจุบัน

ข้อความด้านล่างส่วนประกอบฮาร์ดแวร์จะระบุจำนวนของส่วนประกอบที่ติดตั้ง หากคุณคลิกที่ข้อความดังกล่าว ระบบจะนำคุณไปยังหน้า **รายการอุปกรณ์**

การดูข้อมูลของระบบ

หัวข้อนี้จะอธิบายวิธีการขอรับรายการสรุปข้อมูลเซิร์ฟเวอร์โดยทั่วไป

แผง **ข้อมูลเกี่ยวกับระบบและการตั้งค่า** ทางด้านซ้ายของหน้าโฮมเพจ ช่วยมอบข้อมูลสรุปเกี่ยวกับข้อมูลทั่วไปของเซิร์ฟเวอร์ ซึ่งรวมถึงข้อมูลต่อไปนี้:

- ชื่อเครื่อง, สถานะพลังงานและระบบปฏิบัติการ
- ประเภทและรุ่นเครื่อง
- หมายเลขประจำเครื่อง
- ชื่อระบบ
- การเป็นเจ้าของ USB ด้านหน้า
- สิทธิ์การใช้งาน BMC
- ที่อยู่ IP สำหรับ BMC
- ชื่อโฮสต์ BMC
- เวอร์ชันของ UEFI
- เวอร์ชันของ BMC
- เวอร์ชันของ LXPM
- ตำแหน่ง

เซิร์ฟเวอร์อาจอยู่ในสถานะระบบสถานะใดสถานะหนึ่งที่แสดงรายการในตารางต่อไปนี้

ตาราง 5. รายละเอียดสถานะระบบ

ตารางสองคอลัมน์ที่มีส่วนหัวสำหรับบันทึกสถานะระบบของเซิร์ฟเวอร์

สถานะ	**รายละเอียด**
ปิดระบบ/ไม่ทราบสถานะ	เซิร์ฟเวอร์ปิดอยู่
เปิดระบบ/เริ่มต้น UEFI	เซิร์ฟเวอร์เปิดอยู่ แต่ UEFI ไม่ทำงาน
ระบบทำงานใน UEFI	เซิร์ฟเวอร์เปิดอยู่ และ UEFI กำลังทำงาน
ระบบหยุดทำงานใน UEFI	เซิร์ฟเวอร์เปิดอยู่; UEFI ตรวจพบปัญหาและหยุดการทำงานแล้ว

ตาราง 5. รายละเอียดสถานะระบบ (มีต่อ)

สถานะ	รายละเอียด
การบูตระบบปฏิบัติการหรือในระบบปฏิบัติการที่ไม่รองรับ	เซิร์ฟเวอร์อาจอยู่ในสถานะนี้ด้วยเหตุผลใดเหตุผลหนึ่งต่อไปนี้: • ตัวโหลดระบบปฏิบัติการเริ่มต้นแล้ว แต่ระบบปฏิบัติการไม่ทำงาน • อินเทอร์เฟซ BMC Ethernet over USB ถูกปิดใช้งาน • ระบบปฏิบัติการไม่โหลดไดรเวอร์ที่รองรับอินเทอร์เฟซ Ethernet over USB
บูตระบบปฏิบัติการแล้ว	ระบบปฏิบัติการของเซิร์ฟเวอร์กำลังทำงานอยู่
Suspend to RAM	เซิร์ฟเวอร์ถูกกำหนดให้อยู่ในสถานะสแตนด์บายหรือโหมดสลีป
การรันระบบในการทดสอบหน่วยความจำ	เซิร์ฟเวอร์เปิดอยู่และเครื่องมือการวินิจฉัยหน่วยความจำกำลังทำงาน
การรันระบบในการตั้งค่า	เซิร์ฟเวอร์เปิดอยู่ และระบบได้บูตไปยังเมนูการ F1 Setup ของ UEFI หรือเมนู LXPM
การรันระบบในโหมดการบำรุงรักษา LXPM	เซิร์ฟเวอร์เปิดอยู่ และระบบได้บูตไปยังโหมดการบำรุงรักษา LXPM ซึ่งผู้ใช้ไม่สามารถเลื่อนไปตามเมนู LXPM

หากคุณต้องการเปลี่ยนชื่อระบบ ให้คลิกที่ไอคอนรูปดินสอ ป้อนชื่อระบบที่คุณต้องการใช้งาน แล้วคลิกเครื่องหมายถูกสีเขียว

หากคุณต้องการเปลี่ยนความเป็นเจ้าของ USB ด้านหน้า ให้คลิกที่ไอคอนรูปดินสอแล้วเลือกโหมด **การเป็นเจ้าของ USB ด้านหน้า** ที่ต้องการจากเมนูแบบดรอปดาวน์ จากนั้น คลิกที่เครื่องหมายถูกสีเขียว

หากเซิร์ฟเวอร์ของคุณมีสิทธิ์การใช้งานอื่นนอกเหนือจากสิทธิ์การใช้งาน XClarity Controller แบบ Enterprise คุณอาจสามารถซื้ออัปเกรดสิทธิ์การใช้งานเพื่อเปิดใช้งานคุณลักษณะเสริมได้ ในการติดตั้งสิทธิ์การใช้งานแบบอัปเกรดหลังจากได้รับสิทธิ์การใช้งานดังกล่าว ให้คลิกที่ไอคอนลูกศรชี้ขึ้น

ในการเพิ่ม ลบ หรือส่งออกสิทธิ์การใช้งาน ให้คลิกที่ไอคอนลูกศรชี้ด้านขวา

ในการเปลี่ยนการตั้งค่าที่เกี่ยวข้องสำหรับที่อยู่ IP ของ BMC, ชื่อโฮสต์ของ BMC, เวอร์ชันของ UEFI, เวอร์ชันของ BMC และรายการตำแหน่งที่ตั้ง ให้คลิกที่ไอคอนลูกศรชี้ขวา

- สำหรับที่อยู่ IP และชื่อโฮสต์ ระบบจะนำคุณไปยังส่วน **การกำหนดค่าอีเทอร์เน็ต** ภายใต้ Network
- สำหรับรายการเวอร์ชันของ UEFI และ BMC ระบบจะนำคุณไปยังหน้า **การอัปเดตเฟิร์มแวร์**
- สำหรับรายการตำแหน่งที่ตั้ง ระบบจะนำคุณไปยังส่วน **คุณสมบัติของเซิร์ฟเวอร์** ในหน้า **การกำหนดค่าเซิร์ฟเวอร์**

การดูการใช้งานของระบบ

เมื่อคลิกที่ **การใช้งาน** บนแผงด้านซ้ายมือ ระบบจะแสดงรายการสรุปข้อมูลการใช้งานเซิร์ฟเวอร์ทั่วไป

การใช้งานระบบคือตัววัดแบบรวมที่อ้างอิงข้อมูลการใช้งานโปรเซสเซอร์ หน่วยความจำ และระบบย่อย I/O แบบเรียลไทม์ ข้อมูลการใช้งานทั้งหมดมาจากฝั่ง ME(Node manager) และสามารถดูได้ทั้งในมุมมองกราฟิกหรือมุมมองตาราง ซึ่งรวมถึงข้อมูลต่อไปนี้:

- **อุณหภูมิ**
  - แสดงอุณหภูมิแวดล้อมตามเวลาจริงและอุณหภูมิส่วนประกอบหลัก
  - การวางเคอร์เซอร์ของเมาส์เหนือโมดูลหน่วยความจำจะทำให้เห็นอุณหภูมิปัจจุบัน
  - แท็บประวัติจะแสดงแผนภูมิอุณหภูมิย้อนหลังได้สูงสุด 24 ชั่วโมงที่ผ่านมา
- **การใช้พลังงาน**
  - แสดงแผนภูมิวงกลมที่มีข้อมูลการใช้พลังงานปัจจุบัน ตลอดจนแผนภูมิการใช้พลังงานย้อนหลังสูงสุด 24 ชั่วโมงที่ผ่านมา
  - การวางเคอร์เซอร์ของเมาส์เหนือแผนภูมิวงกลมจะทำให้เห็นการใช้พลังงานในปัจจุบัน

- แผนภูมิวงกลมที่แสดงข้อมูลการใช้พลังงานปัจจุบันประกอบด้วยสี่ประเภท ได้แก่ CPU, หน่วยความจำ, อื่นๆ และอะไหล่ “อื่นๆ” หมายถึง การใช้พลังงานของระบบทั้งหมดลบด้วยการใช้พลังงานของ CPU และหน่วยความจำ “อะไหล่” หมายถึง พลังงานที่จัดสรรไว้ทั้งหมดลบด้วยการใช้พลังงานของระบบทั้งหมด
- แท็บแรงดันไฟฟ้าจะแสดงค่าแรงดันไฟฟ้าปัจจุบันและสถานะบนเซ็นเซอร์แรงดันไฟฟ้าทั้งหมดที่ฮาร์ดแวร์รองรับ

- **การใช้งานของระบบ**
  - แสดงภาพการใช้งานปัจจุบันของระบบ โปรเซสเซอร์ หน่วยความจำ และระบบย่อย I/O
  - ใช้ฟังก์ชันรีเฟรชหรือรีโหลดเบราว์เซอร์เพื่ออัปเดตข้อมูลการใช้งานปัจจุบัน
  - การใช้งานระดับระบบย่อยของ CPU แสดงเปอร์เซ็นต์ของแบนด์วิดท์ของ CPU ทั้งหมดที่ใช้งานอยู่ในปัจจุบัน โดยวัดจากตัวนับประสิทธิภาพที่สร้างขึ้นใน CPU (อาจแตกต่างเล็กน้อยจากการใช้งาน CPU ที่รายงานโดยระบบปฏิบัติการ)
  - การใช้งานระดับระบบย่อยของหน่วยความจำแสดงถึงเปอร์เซ็นต์ของแบนด์วิดท์ตัวควบคุมช่องทางหน่วยความจำทั้งหมดที่ใช้งานอยู่ในปัจจุบัน (ไม่ได้แสดงจำนวนหน่วยความจำที่ใช้อยู่ในปัจจุบัน)
  - การใช้งานระดับระบบย่อยของ I/O แสดงถึงเปอร์เซ็นต์ของแบนด์วิดท์ทราฟฟิก PCIe ทั้งหมดที่ใช้งานอยู่ในปัจจุบัน
  - ค่าแบนด์วิธที่วัดจะคำนวณเป็นเปอร์เซ็นต์จากปริมาณแบนด์วิธหน่วยความจำที่ใช้งาน และหน่วยความจำสูงสุดที่ใช้งานได้ (ต่อวินาที)
- **ความเร็วพัดลม** (RPM)
  - ส่วนความเร็วพัดลมจะแสดงข้อมูลความเร็วพัดลมเป็นเปอร์เซ็นต์ของความเร็วสูงสุด
  - ผู้ใช้สามารถคลิกที่ไอคอนรูปเฟืองเพื่อเข้าถึงตัวเลือก **การเพิ่มความเร็ว**
    - การตั้งค่านี้ช่วยให้เซิร์ฟเวอร์ระบายความร้อนเพิ่มเติมตามอุณหภูมิแวดล้อม สามารถเพิ่มความเร็วพัดลมได้มากกว่าความเร็วปกติโดยอัลกอริธึมควบคุมความร้อน จะไม่มีการเปลี่ยนแปลงหากพัดลมทำงานที่ความเร็วเต็มที่แล้ว

การดูบันทึกเหตุการณ์

บันทึกเหตุการณ์ จะมีรายการประวัติของฮาร์ดแวร์ทั้งหมดและเหตุการณ์เกี่ยวกับการจัดการ

เลือกแท็บ **บันทึกเหตุการณ์** ใน **เหตุการณ์** เพื่อแสดงหน้า **บันทึกเหตุการณ์** เหตุการณ์ทั้งหมดในบันทึกจะถูกประทับเวลา โดยใช้การตั้งค่าวันที่และเวลาของ XClarity Controller นอกจากนี้ บางเหตุการณ์จะยังสร้างการแจ้งเตือนเมื่อเหตุการณ์เกิดขึ้น หากมีการกำหนดค่าให้ดำเนินการเช่นนั้นใน **แจ้งเตือนผู้รับ** คุณสามารถจัดเรียงและกรองเหตุการณ์ในบันทึกเหตุการณ์ได้

ต่อไปนี้คือรายละเอียดเกี่ยวกับการดำเนินการที่ทำได้ในหน้า **บันทึกเหตุการณ์**

- **กำหนดตารางเอง**: เลือกรายการการดำเนินการนี้เพื่อเลือกประเภทของข้อมูลที่คุณต้องการแสดงในตาราง สามารถแสดงหมายเลขลำดับเพื่อช่วยในการกำหนดลำดับของเหตุการณ์ เมื่อเหตุการณ์มากกว่าหนึ่งเหตุการณ์มีการประทับเวลาเดียวกัน

  หมายเหตุ: มีการใช้หมายเลขลำดับบางหมายเลขโดยกระบวนการ BMC ภายใน ดังนั้นจึงเป็นเรื่องปกติที่อาจมีช่องว่างระหว่างหมายเลขลำดับเมื่อมีการจัดเรียงเหตุการณ์ตามหมายเลขลำดับ
- **ล้างข้อมูลบันทึก**: เลือกรายการการดำเนินการนี้เพื่อลบบันทึกเหตุการณ์
- **รีเฟรช**: เลือกรายการการดำเนินการนี้เพื่ออัปเดตการแสดงผลด้วยรายการบันทึกเหตุการณ์ใดๆ ที่อาจเกิดขึ้นตั้งแต่มีการแสดงหน้าครั้งล่าสุด
- **ประเภท**: เลือกประเภทเหตุการณ์ที่จะแสดง ซึ่งรวมถึงประเภทเหตุการณ์ต่างๆ ต่อไปนี้:

   แสดงรายการข้อผิดพลาดในบันทึก

   แสดงรายการคำเตือนในบันทึก

   แสดงรายการข้อมูลในบันทึก

  คลิกแต่ละไอคอนเพื่อปิดหรือเปิดประเภทข้อผิดพลาดที่จะแสดง การคลิกไอคอนติดต่อกันจะสลับระหว่างการแสดงและไม่แสดงเหตุการณ์ กล่องสีน้ำเงินรอบไอคอนจะระบุประเภทของเหตุการณ์ที่จะแสดง
- **การกรองประเภทที่มา**: เลือกรายการจากเมนูดรอปดาวน์เพื่อแสดงเฉพาะประเภทรายการบันทึกเหตุการณ์ที่คุณต้องการให้แสดง
- **การกรองเวลา**: เลือกรายการการดำเนินการนี้เพื่อระบุช่วงเวลาของเหตุการณ์ที่คุณต้องการแสดง
- **ค้นหา**: เพื่อค้นหาประเภทเหตุการณ์หรือคำสำคัญที่เฉพาะเจาะจง คลิกไอคอนแว่นขยายและพิมพ์คำที่จะค้นหาในกล่อง **ค้นหา** โปรดทราบว่าอินพุตจะพิจารณาตัวพิมพ์เล็ก-ใหญ่

หมายเหตุ: จำนวนสูงสุดของบันทึกเหตุการณ์คือ 1024 เมื่อบันทึกเหตุการณ์เต็ม รายการบันทึกใหม่จะเขียนทับรายการที่เก่าที่สุดโดยอัตโนมัติ

การดูบันทึกการตรวจสอบ

บันทึกการตรวจสอบจะแสดงบันทึกการดำเนินการที่ผ่านมาของผู้ใช้ เช่น การเข้าสู่ระบบ XClarity Controller การสร้างผู้ใช้ใหม่ และการเปลี่ยนรหัสผ่านของผู้ใช้

คุณสามารถใช้บันทึกการตรวจสอบเพื่อติดตามและลงบันทึกการให้สิทธิ์ การเปลี่ยนแปลง และการดำเนินการต่างๆ ในระบบได้

ทั้งบันทึกเหตุการณ์และบันทึกการตรวจสอบต่างก็รองรับการบันทึกการดำเนินการเกี่ยวกับการบำรุงรักษาและการดูข้อมูลเหมือนๆ กัน หากต้องการดูรายละเอียดเกี่ยวกับการดำเนินการสำหรับการแสดงผลและการกรองที่ทำได้ในหน้าบันทึกการตรวจสอบ โปรดดูที่ “การดูบันทึกเหตุการณ์” บนหน้าที่ 82

หมายเหตุ:

- หลังจากเรียกใช้เครื่องมือของ Lenovo บนระบบปฏิบัติการเซิร์ฟเวอร์ของคุณ บันทึกการตรวจสอบอาจมีระเบียนที่แสดงการกระทำที่ดำเนินการโดยชื่อผู้ใช้ (ตัวอย่างเช่น ผู้ใช้ “20luN4SB”) ซึ่งคุณอาจไม่รู้จัก เมื่อมีการเรียกใช้เครื่องมือบางอย่างบนระบบปฏิบัติการเซิร์ฟเวอร์ เครื่องมือเหล่านั้นอาจสร้างบัญชีผู้ใช้ชั่วคราวเพื่อเข้าถึง XClarity Controller บัญชีถูกสร้างด้วยชื่อผู้ใช้และรหัสผ่านแบบสุ่ม และสามารถใช้ในการเข้าถึง XClarity Controller บนอินเทอร์เฟซ Ethernet over USB ภายในเท่านั้น สามารถใช้บัญชีในการเข้าถึงอินเทอร์เฟซ Redfish และ SFTP ของ XClarity Controller เท่านั้น การสร้างและการลบบัญชีชั่วคราวนี้ออกจะถูกบันทึกลงในบันทึกการตรวจสอบ เช่นเดียวกับการกระทำใดๆ ที่ดำเนินการโดยเครื่องมือที่มีข้อมูลประจำตัวเหล่านี้ด้วย
- จำนวนสูงสุดของบันทึกการตรวจสอบคือ 1024 เมื่อบันทึกการตรวจสอบเต็ม รายการบันทึกใหม่จะเขียนทับรายการที่เก่าที่สุดโดยอัตโนมัติ

การดูประวัติการบำรุงรักษา

หน้า **ประวัติการบำรุงรักษา** จะรวมข้อมูลเกี่ยวกับการอัปเดตเฟิร์มแวร์ การกำหนดค่า และประวัติการเปลี่ยนฮาร์ดแวร์

สามารถกรองเนื้อหาของประวัติการบำรุงรักษาเพื่อให้แสดงเหตุการณ์บางประเภทหรือเวลาบางช่วงได้

หมายเหตุ: จำนวนสูงสุดของบันทึกประวัติการบำรุงรักษาคือ 250 เมื่อบันทึกประวัติการบำรุงรักษาเต็ม รายการบันทึกใหม่จะเขียนทับรายการที่เก่าที่สุดโดยอัตโนมัติ

การกำหนดค่าผู้รับการแจ้งเตือน

ใช้ข้อมูลในหัวข้อนี้เพื่อเพิ่มและแก้ไขอีเมลและการแจ้งเตือน Syslog หรือผู้รับ SNMP TRAP

ต่อไปนี้คือรายละเอียดเกี่ยวกับการดำเนินการที่ทำได้ในแท็บ **ผู้รับการแจ้งเตือน**

รายการของการดำเนินการต่อไปนี้สามารถทำได้ในส่วนผู้รับ **อีเมล/Syslog**

- **สร้าง**: เลือกรายการของการดำเนินการนี้เพื่อสร้างผู้รับอีเมลและผู้รับ Syslog ใหม่เพิ่มเติม สามารถกำหนดค่าผู้รับอีเมลและ Syslog ได้สูงสุด 12 ราย
  - **สร้างผู้รับอีเมล**: เลือกรายการของการดำเนินการนี้เพื่อสร้างผู้รับอีเมล
    - ป้อนชื่อและที่อยู่อีเมลของผู้รับ

- เลือกว่าจะเปิดใช้งานหรือปิดใช้งานการแจ้งเตือนเหตุการณ์ หากเลือกปิดใช้งาน บัญชีจะยังคงได้รับการกำหนดค่า แต่จะไม่มีการส่งอีเมล
- เลือกประเภทเหตุการณ์ที่ผู้รับจะได้รับการแจ้งเตือน หากคุณคลิกดรอปดาวน์ถัดจากป้ายประเภทร้ายแรง ข้อคำนึง หรือระบบ คุณสามารถเลือกหรือยกเลิกการเลือกการแจ้งเตือนสำหรับประเภทส่วนประกอบที่เฉพาะเจาะจงได้
- คุณสามารถเลือกว่าจะรวมเนื้อหาของบันทึกเหตุการณ์ไว้ในการแจ้งเตือนทางอีเมลหรือไม่
- ดัชนีจะระบุว่ามีการกำหนดช่องผู้รับช่องใดใน 12 ช่อง
- คุณสามารถกำหนดค่าเซิร์ฟเวอร์อีเมลที่จะส่งต่อเหตุการณ์ไปถึงได้ที่นี่ หรือโดยคลิกการดำเนินการของเซิร์ฟเวอร์ SMTP ที่ด้านบนของส่วนนี้ ดูรายละเอียดการกำหนดค่าเซิร์ฟเวอร์ SMTP ด้านล่าง

- **สร้างผู้รับ** Syslog: เลือกรายการของการดำเนินการนี้เพื่อสร้างผู้รับ Syslog
  - ป้อนชื่อและที่อยู่ IP หรือชื่อโฮสต์ของเซิร์ฟเวอร์ Syslog
  - เลือกว่าจะเปิดใช้งานหรือปิดใช้งานการแจ้งเตือนเหตุการณ์ หากเลือกปิดใช้งาน บัญชีจะยังคงได้รับการกำหนดค่า แต่จะไม่มีการส่งอีเมล
  - ดัชนีจะระบุว่ามีการกำหนดช่องผู้รับช่องใดใน 12 ช่อง
  - เลือกประเภทเหตุการณ์ที่จะส่งไปยังเซิร์ฟเวอร์ Syslog หากคุณคลิกเมนูดรอปดาวน์ถัดจากป้ายประเภทร้ายแรง ข้อคำนึง หรือระบบ คุณสามารถเลือกหรือยกเลิกการเลือกการแจ้งเตือนสำหรับประเภทส่วนประกอบที่เฉพาะเจาะจงได้

- **เซิร์ฟเวอร์** SMTP: เลือกรายการการดำเนินการนี้เพื่อกำหนดค่าการตั้งค่าที่เกี่ยวข้องสำหรับเซิร์ฟเวอร์อีเมล SMTP สามารถกำหนดค่าเซิร์ฟเวอร์อีเมลได้เพียงเซิร์ฟเวอร์เดียวเท่านั้น ระบบจะใช้การกำหนดค่าอีเมลที่เหมือนกันเมื่อส่งการแจ้งเตือนไปยังผู้รับอีเมลที่กำหนดค่าทั้งหมด BMC จะสลับจากการเชื่อมต่อที่ปลอดภัยเป็นการเชื่อมต่อที่เข้ารหัสโดยอัตโนมัติสำหรับการถ่ายโอนเมลโดยใช้คำสั่ง STARTTLS อย่างสม่ำเสมอผ่านพอร์ต 587 หากเซิร์ฟเวอร์เมลเป้าหมายรองรับได้
  - ป้อนชื่อโฮสต์หรือที่อยู่ IP และหมายเลขพอร์ตเครือข่ายของเซิร์ฟเวอร์อีเมล
  - หากเซิร์ฟเวอร์อีเมลต้องมีการตรวจสอบความถูกต้อง ให้เลือกกล่องตัวเลือก **ต้องมีการตรวจสอบความถูกต้อง** และป้อนชื่อผู้ใช้และรหัสผ่าน เลือกประเภทการตรวจสอบความถูกต้องที่เซิร์ฟเวอร์อีเมลกำหนด ไม่ว่าจะเป็นวิธีการแบบถาม-ตอบ (CRAM-MD5) หรือข้อมูลประจำตัวแบบง่าย (**เข้าสู่ระบบ**)
  - บางเครือข่ายอาจบล็อกอีเมลขาออก หากค่าของพาธย้อนกลับไม่ตรงตามที่คาดการณ์ ตามค่าเริ่มต้น XClarity Controller จะใช้ alertmgr@domain โดยที่โดเมนคือชื่อโดเมนตามที่ระบุในส่วน DDNS ของเว็บเพจเครือข่าย XClarity Controller คุณสามารถระบุข้อมูลผู้ส่งของคุณเองแทนที่ค่าเริ่มต้น
  - คุณสามารถทดสอบการเชื่อมต่อเซิร์ฟเวอร์อีเมลเพื่อให้แน่ใจว่าการตั้งค่าอีเมลได้รับการกำหนดค่าอย่างถูกต้อง XClarity Controller จะแสดงข้อความที่ระบุว่าการเชื่อมต่อสำเร็จหรือไม่

- **ลองใหม่และหน่วงเวลา**: เลือกรายการการดำเนินการนี้เพื่อกำหนดค่าการตั้งค่าที่เกี่ยวข้องสำหรับตัวเลือกการลองใหม่และหน่วงเวลา
  - ขีดจำกัดการลองใหม่จะระบุจำนวนครั้งที่ XClarity Controller จะพยายามส่งการแจ้งเตือน หากความพยายามในครั้งแรกไม่สำเร็จ
  - การหน่วงเวลาระหว่างรายการจะระบุระยะเวลาที่ XClarity Controller จะรอหลังจากส่งการแจ้งเตือนไปยังผู้รับรายหนึ่ง ก่อนที่จะส่งการแจ้งเตือนไปยังผู้รับถัดไป
  - การหน่วงเวลาระหว่างความพยายามจะระบุระยะเวลาที่ XClarity Controller จะรอหลังจากความพยายามล้มเหลว ก่อนที่จะลองส่งการแจ้งเตือนใหม่
- **โปรโตคอล**: เลือกรายการการดำเนินการนี้เพื่อกำหนดค่าการตั้งค่าที่เกี่ยวข้องสำหรับโปรโตคอลการเชื่อมต่อ
  - คุณสามารถเลือกได้ระหว่าง **โปรโตคอล** TCP หรือ **โปรโตคอล** UDP โปรดทราบว่าการตั้งค่านี้จะนำไปใช้กับผู้รับ Syslog ทั้งหมด
- หากมีการสร้างผู้รับอีเมลหรือผู้รับ Syslog แล้ว ผู้รับเหล่านั้นจะปรากฏในรายการของส่วนนี้
  - ในการแก้ไขการตั้งค่าสำหรับผู้รับอีเมลหรือผู้รับ Syslog ให้คลิกไอคอนดินสอด้านล่างส่วนหัวการดำเนินการตรงแถวถัดจากผู้รับที่คุณต้องการกำหนดค่า
  - ในการลบผู้รับอีเมลหรือผู้รับ Syslog ให้คลิกไอคอนถังขยะ
  - ในการส่งการแจ้งเตือนทดสอบไปยังผู้รับอีเมลหรือผู้รับ Syslog ให้คลิกไอคอนเครื่องบินกระดาษ

การดำเนินการต่อไปนี้สามารถทำได้ในส่วนผู้ใช้ SNMPv3

- **สร้าง**: เลือกรายการของการดำเนินการนี้เพื่อสร้างผู้รับ SNMPv3 TRAP
  - เลือกบัญชีผู้ใช้ที่จะเชื่อมโยงกับ SNMPv3 TRAP บัญชีผู้ใช้ต้องเป็นหนึ่งในบัญชีผู้ใช้ภายในระบบ 12 บัญชี
  - ระบุชื่อโฮสต์หรือที่อยู่ IP ของตัวจัดการ SNMPv3 ที่จะได้รับ SNMPv3 TRAP
  - XClarity Controller ใช้อัลกอริทึมแฮช HMAC-SHA ในการตรวจสอบความถูกต้องด้วยตัวจัดการ SNMPv3 ซึ่งเป็นอัลกอริทึมเดียวที่ได้รับการรองรับ
  - รหัสผ่านความเป็นส่วนตัวใช้ร่วมกับโปรโตคอลความเป็นส่วนตัวเพื่อเข้ารหัสลับข้อมูล SNMP
  - **การตั้งค่าส่วนกลางของ SNMPv3** นำไปใช้กับผู้รับ SNMPv3 TRAP ทั้งหมด การตั้งค่าเหล่านี้สามารถกำหนดค่าขณะสร้างผู้รับ SNMPv3 TRAP หรือโดยคลิกการดำเนินการตั้งค่า SNMPv3 ที่ด้านบนของส่วนผู้ใช้ SNMPv3
    - เลือกว่าจะเปิดใช้งานหรือปิดใช้งาน SNMPv3 TRAP หากปิดใช้งาน การตั้งค่าจะยังคงได้รับการกำหนดค่าแต่จะไม่มีการส่ง SNMPv3 TRAP
    - จำเป็นต้องมีและกำหนดค่าข้อมูลตำแหน่งที่ตั้งและที่ติดต่อ BMC บนเว็บเพจคุณสมบัติของเซิร์ฟเวอร์ โปรดดูข้อมูลเพิ่มเติมที่ “การตั้งค่าตำแหน่งที่ตั้งและที่ติดต่อ” บนหน้าที่ 116

– เลือกประเภทเหตุการณ์ที่จะทำให้ TRAP ส่งไปยังตัวจัดการ SNMPv3 หากคุณคลิกเมนูดรอปดาวน์ถัดจากป้ายประเภทร้ายแรง ข้อคำนึง หรือระบบ คุณสามารถเลือกหรือยกเลิกการเลือกการแจ้งเตือนสำหรับประเภทส่วนประกอบที่เฉพาะเจาะจงได้

หมายเหตุ: คุณสามารถป้องกันข้อมูลที่ถ่ายโอนระหว่างไคลเอ็นต์ของ SNMP และตัวแทนได้ด้วยการเข้ารหัส วิธีการที่สนับสนุนสำหรับ**โปรโตคอลความเป็นส่วนตัว** ได้แก่ CBC-DES และ AES

- หากมีการสร้างผู้รับ SNMPv3 TRAP แล้ว ผู้รับเหล่านั้นจะปรากฏในรายการของส่วนนี้
  - ในการแก้ไขการตั้งค่าสำหรับผู้รับ SNMPv3 ให้คลิกไอคอนดินสอด้านล่างส่วนหัวการดำเนินการบนแถวถัดจากผู้รับที่คุณต้องการกำหนดค่า
  - ในการลบผู้รับ SNMPv3 ให้คลิกไอคอนถังขยะ

การจับภาพข้อมูลหน้าจอความบกพร่องของระบบปฏิบัติการล่าสุด

ใช้ข้อมูลในหัวข้อนี้เพื่อจับภาพและดูหน้าจอความบกพร่องของระบบปฏิบัติการ

ระบบจะจับภาพหน้าจอระบบปฏิบัติการโดยอัตโนมัติเมื่อเกิดการหมดเวลาของ OS Watchdog หากเกิดเหตุการณ์ที่ทำให้ระบบปฏิบัติการหยุดทำงาน ระบบจะเปิดคุณลักษณะ OS Watchdog และจับภาพเนื้อหาบนหน้าจอ XClarity Controller จะเก็บภาพหน้าจอเพียงภาพเดียวเท่านั้น เมื่อเกิดการหมดเวลาของ OS Watchdog ภาพหน้าจอใหม่จะเขียนทับภาพหน้าจอก่อนหน้า ต้องเปิดใช้งานคุณลักษณะ OS Watchdog เพื่อจับภาพหน้าจอความบกพร่องของระบบปฏิบัติการ ในการตั้งค่าเวลา OS Watchdog โปรดดูข้อมูลเพิ่มเติมได้ที่ “การตั้งค่าการหมดเวลาของเซิร์ฟเวอร์” บนหน้าที่ 117 คุณลักษณะการจับภาพหน้าจอความบกพร่องของระบบปฏิบัติการจะพร้อมใช้งานเมื่อมีฟังก์ชันการทำงานของ XClarity Controller ในระดับขั้นสูงหรือระดับองค์กรเท่านั้น ดูข้อมูลเกี่ยวกับระดับฟังก์ชันการทำงานของ XClarity Controller ที่ติดตั้งในเซิร์ฟเวอร์ของคุณได้จากเอกสารประกอบการใช้งานเซิร์ฟเวอร์

คลิกการดำเนินการ **หน้าจอความบกพร่องล่าสุด** ในส่วน **คอนโซลระยะไกล** ที่หน้าแรกของ XClarity Controller เพื่อดูภาพของหน้าจอระบบปฏิบัติการที่มีการจับภาพเมื่อเกิดการหมดเวลาของ OS Watchdog นอกจากนี้ ยังสามารถดูการจับภาพได้โดยคลิก **บริการ** ตามด้วย **หน้าจอความบกพร่องล่าสุด** ในส่วน **การดำเนินการด่วน** ของหน้าแรก หากระบบยังไม่เคยพบการหมดเวลาของ OS Watchdog และไม่เคยจับภาพหน้าจอระบบปฏิบัติการ ข้อความที่ระบุว่ายังไม่มีการสร้างภาพหน้าจอความบกพร่องจะปรากฏขึ้น

บทที่ 5. การกำหนดค่าเซิร์ฟเวอร์

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจเกี่ยวกับตัวเลือกต่างๆ ที่ใช้ได้ในการกำหนดค่าเซิร์ฟเวอร์

เมื่อกำหนดค่าเซิร์ฟเวอร์ จะสามารถใช้ตัวเลือกต่อไปนี้ได้:

- อะแดปเตอร์
- ตัวเลือกการบูต
- นโยบายพลังงาน
- คุณสมบัติของเซิร์ฟเวอร์

การดูข้อมูลอะแดปเตอร์และการตั้งค่าการกำหนดค่า

ใช้ข้อมูลในหัวข้อนี้เพื่อดูรายละเอียดเกี่ยวกับอะแดปเตอร์ต่างๆ ที่ติดตั้งภายในเซิร์ฟเวอร์

คลิกที่ **อะแดปเตอร์** ในส่วน **การกำหนดค่าเซิร์ฟเวอร์** เพื่อดูข้อมูลเกี่ยวกับอะแดปเตอร์ที่ติดตั้งภายในเซิร์ฟเวอร์

หมายเหตุ:

- หากอะแดปเตอร์ไม่รองรับการติดตามสถานะ อะแดปเตอร์จะไม่แสดงผลสำหรับการติดตามหรือกำหนดค่า สำหรับข้อมูลที่เกี่ยวข้องกับรายการอุปกรณ์ของอะแดปเตอร์ PCI ที่ติดตั้งทั้งหมด โปรดดูได้ที่หน้า **รายการอุปกรณ์**

การกำหนดค่าโหมดและลำดับการบูทระบบ

ในการกำหนดค่าโหมดและลำดับการบูตระบบ ให้ใช้ข้อมูลในหัวข้อนี้

เมื่อคุณเลือก **ตัวเลือกการบูต** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** คุณสามารถกำหนดค่าโหมดและลำดับการบูตระบบได้

หมายเหตุ: ไม่อนุญาตให้ใช้วิธีการภายในที่ไม่มีการตรวจสอบยืนยันตัวตนในการเปลี่ยนการตั้งค่าระบบที่เกี่ยวข้องกับการรักษาความปลอดภัย ตัวอย่างเช่น ไม่สามารถกำหนดค่าการบูตที่ปลอดภัยผ่าน API ภายในที่ไม่มีการตรวจสอบยืนยันตัวตนจาก OS หรือ UEFI Shell ได้ ซึ่งรวมถึง OneCLI ที่ทำงานภายในและรับข้อมูลประจำตัวชั่วคราวโดยใช้ IPMI หรือเครื่องมือและ API ใดๆ ในการกำหนดค่าการบูตที่ปลอดภัย, TPM, การตั้งค่าที่เกี่ยวข้องกับรหัสผ่านการตั้งค่า UEFI การตั้งค่าที่เกี่ยวข้องกับการรักษาความปลอดภัยทั้งหมดต้องมีการตรวจสอบยืนยันตัวตนที่เหมาะสมพร้อมสิทธิพิเศษที่เพียงพอ

สำหรับโหมดการบูตระบบ จะมีตัวเลือกสองตัวเลือกต่อไปนี้:

UEFI Boot
: เลือกตัวเลือกนี้เพื่อกำหนดค่าเซิร์ฟเวอร์ที่รองรับ Unified Extensible Firmware Interface (UEFI) หากคุณบูตระบบปฏิบัติการที่เปิดใช้งาน UEFI ตัวเลือกนี้อาจลดระยะเวลาในการบูตโดยปิดใช้งาน Legacy Option ROM

Legacy Boot
: เลือกตัวเลือกนี้หากคุณกำหนดค่าเซิร์ฟเวอร์เพื่อให้บูตระบบปฏิบัติการที่ต้องการเฟิร์มแวร์ Legacy (BIOS) เลือกตัวเลือกนี้เฉพาะเมื่อคุณบูตระบบปฏิบัติการที่เปิดใช้งานที่ไม่ใช่ UEFI เท่านั้น

ในการกำหนดค่าลำดับการบูตระบบ ให้เลือกอุปกรณ์จากรายการของ **อุปกรณ์ที่มี** และคลิกลูกศรขวาเพื่อเพิ่มอุปกรณ์ในลำดับการบูต ในการลบอุปกรณ์ออกจากลำดับการบูต ให้เลือกอุปกรณ์จากรายการลำดับการบูตและคลิกลูกศรซ้ายเพื่อย้ายอุปกรณ์กลับไปยังรายการของอุปกรณ์ที่มี ในการเปลี่ยนลำดับการบูต ให้เลือกอุปกรณ์และคลิกลูกศรขึ้นหรือลงเพื่อย้ายอุปกรณ์ขึ้นหรือลงตามลำดับความสำคัญ

เมื่อคุณเปลี่ยนลำดับการบูต คุณต้องเลือกตัวเลือกการรีสตาร์ทก่อนนำการเปลี่ยนแปลงไปใช้ มีตัวเลือกดังต่อไปนี้:

- **รีสตาร์ทเซิร์ฟเวอร์ในทันที**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก และเซิร์ฟเวอร์จะรีสตาร์ทในทันทีโดยไม่ปิดระบบปฏิบัติการ
- **รีสตาร์ทเซิร์ฟเวอร์ตามปกติ**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก และระบบปฏิบัติการจะปิดก่อนรีสตาร์ทเซิร์ฟเวอร์
- **รีสตาร์ทด้วยตนเองในภายหลัง**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก แต่จะไม่มีผลจนกว่าจะมีการรีบูตเซิร์ฟเวอร์ครั้งถัดไป

การกำหนดค่าการบูทแบบครั้งเดียว

ใช้ข้อมูลในหัวข้อนี้เพื่อละเว้นการบูตที่กำหนดค่าชั่วคราว และบูตไปยังอุปกรณ์ที่ระบุครั้งเดียวแทน

คลิก **ตัวเลือกการบูต** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** และเลือกอุปกรณ์จากเมนูดรอปดาวน์เพื่อกำหนดค่าอุปกรณ์ที่ระบบจะบูตไปยังอุปกรณ์นั้นครั้งเดียว เมื่อรีสตาร์ทเซิร์ฟเวอร์ครั้งถัดไป มีตัวเลือกดังต่อไปนี้:

เครือข่าย PXE
: ตั้งค่าเซิร์ฟเวอร์ของคุณให้พยายามบูตเครือข่าย Preboot Execution Environment

สื่อแบบถอดได้หลัก
: ระบบจะบูตเซิร์ฟเวอร์จากอุปกรณ์ USB เริ่มต้น

CD/DVD **เริ่มต้น**

ระบบจะบูตเซิร์ฟเวอร์จากไดรฟ์ CD/DVD เริ่มต้น

การตั้งค่าระบบ F1

ระบบจะบูตเซิร์ฟเวอร์ไปยัง Lenovo XClarity Provisioning Manager

พาร์ทิชันการวินิจฉัย

ระบบจะบูตเซิร์ฟเวอร์ไปยังส่วนการวินิจฉัยของ Lenovo XClarity Provisioning Manager

ฮาร์ดดิสก์เริ่มต้น

ระบบจะบูตเซิร์ฟเวอร์จากดิสก์ไดรฟ์เริ่มต้น

สื่อระยะไกลหลัก

ระบบจะบูตเซิร์ฟเวอร์จากสื่อเสมือนที่เมาท์

ไม่มีการบูตแบบครั้งเดียว

ระบบจะใช้ลำดับการบูตที่กำหนดค่าไว้ ไม่มีการแทนที่ลำดับการบูตที่กำหนดค่าไว้ด้วยการบูตแบบครั้งเดียว

เมื่อคุณเปลี่ยนประเภทของการบูตให้ดำเนินการด้วยอุปกรณ์สำหรับบูตแบบครั้งเดียว คุณยังสามารถระบุการบูตให้เป็นการบูตระบบแบบดั้งเดิมหรือการบูต UEFI ได้ด้วย คลิกกล่องตัวเลือก **Prefer Legacy Boot** หากคุณต้องการให้การบูตเป็นแบบ Legacy BIOS Boot ยกเลิกการทำเครื่องหมายกล่องนี้ หากต้องการใช้การบูต UEFI เมื่อคุณเลือกที่จะเปลี่ยนจากการบูตแบบครั้งเดียวเป็นลำดับการบูต คุณต้องเลือกตัวเลือกการรีสตาร์ทก่อนนำการเปลี่ยนแปลงไปใช้

- **รีสตาร์ทเซิร์ฟเวอร์ในทันที**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก และเซิร์ฟเวอร์จะรีสตาร์ทในทันทีโดยไม่ปิดระบบปฏิบัติการ
- **รีสตาร์ทเซิร์ฟเวอร์ตามปกติ**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก และระบบปฏิบัติการจะปิดก่อนรีสตาร์ทเซิร์ฟเวอร์
- **รีสตาร์ทด้วยตนเองในภายหลัง**: การเปลี่ยนแปลงลำดับการบูตจะได้รับการบันทึก แต่จะไม่มีผลจนกว่าจะมีการรีบูตเซิร์ฟเวอร์ครั้งถัดไป

การจัดการพลังงานของเซิร์ฟเวอร์

ใช้ข้อมูลในหัวข้อนี้เพื่อดูรายละเอียดการจัดการพลังงานและใช้งานฟังก์ชันการจัดการพลังงานต่างๆ

เลือก **นโยบายพลังงาน** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** เพื่อดูข้อมูลการจัดการพลังงานและดำเนินการฟังก์ชันการจัดการพลังงาน

หมายเหตุ: ในตัวเครื่องที่มีเบลดหรือโหนดเซิร์ฟเวอร์ความหนาแน่นสูง การระบายความร้อนของตัวเครื่องและพลังงานจะถูกควบคุมโดยตัวควบคุมการจัดการตัวเครื่องแทน XClarity Controller

การกำหนดค่าการสำรองพลังงาน

ใช้ข้อมูลในหัวข้อนี้ หากต้องการกำหนดค่าการสำรองพลังงาน

หมายเหตุ: **ปัจจุบัน ผู้ใช้ไม่สามารถเปลี่ยนแปลงนโยบายการใช้พลังงานภายในระบบ AMD ได้**

เมื่อติดตั้งชุดแหล่งจ่ายไฟ 2 ชุด โหมดการสำรองจะถูกตั้งค่าเป็น Redundant (N+N) เมื่อกำหนดค่าชุดแหล่งจ่ายไฟ 2 ชุดนี้แล้ว หากชุดแหล่งจ่ายไฟชุดใดชุดหนึ่งทำงานล้มเหลว ไฟ AC ไม่เข้า หรือถูกถอดออก จะมีการรายงานเหตุการณ์ขาดการสำรองในบันทึกเหตุการณ์ XCC

หากมีการติดตั้งชุดแหล่งจ่ายไฟเพียง 1 ชุดหลังจากจัดส่งไปแล้ว โหมดการสำรองจะถูกตั้งค่าเป็นโหมดไม่สำรองโดยอัตโนมัติ

ฟิลด์ที่มีในส่วนการสำรองพลังงาน รวมถึงฟิลด์ต่อไปนี้:

- **Redundant (N+N)**: มีแหล่งพลังงานอิสระตั้งแต่สองแหล่งขึ้นไปที่สามารถจ่ายพลังงานให้กับระบบได้พร้อมกัน ซึ่งหมายความว่าหากแหล่งพลังงานอย่างน้อยหนึ่งแหล่งล้มเหลว แหล่งพลังงานอื่นๆ จะสามารถจ่ายพลังงานให้กับระบบต่อไปได้โดยไม่หยุดชะงัก ความซ้ำซ้อน N+N ช่วยให้ทนทานต่อข้อผิดพลาดในระดับสูง และรับประกันว่าระบบจะยังคงทำงานได้แม้ในกรณีที่เกิดความล้มเหลวหลายครั้ง
  - **โหมด Zero Output**: เมื่อเปิดใช้งานภายใต้การกำหนดค่าสำรอง PSU บางตัวจะเข้าสู่สถานะสแตนด์บายโดยอัตโนมัติภายใต้สภาวะโหลดน้อย ในการทำงานเช่นนี้ PSU ที่เหลือจะจ่ายกำลังไฟทั้งหมดเพื่อเพิ่มประสิทธิภาพ
- **Redundant (N+1)**: มีแหล่งพลังงานหลักหนึ่งแห่งที่สามารถจ่ายพลังงานให้กับระบบได้ นอกจากนี้ ยังมีแหล่งพลังงานสำรองอย่างน้อยหนึ่งแหล่งที่ในการพร้อมใช้งานหากแหล่งพลังงานหลักล้มเหลว แหล่งพลังงานสำรองได้รับการออกแบบเพื่อให้มีพลังงานมากเพียงพอที่จะให้ระบบทำงานต่อไปได้ จนกว่าจะสามารถซ่อมแซมหรือเปลี่ยนแหล่งพลังงานหลักได้ Redundant N+1 มีระดับความทนทานต่อข้อผิดพลาดที่ต่ำกว่าเมื่อเทียบกับความซ้ำซ้อน N+N
- **โหมดไม่มีการสำรอง**: ในโหมดนี้ ไม่รับประกันว่าเซิร์ฟเวอร์จะยังคงทำงานต่อ หากสูญเสียพลังงานจากแหล่งจ่ายไฟ เซิร์ฟเวอร์จะจำกัดเพื่อพยายามให้เซิร์ฟเวอร์ยังคงทำงานได้อยู่ หากแหล่งจ่ายไฟล้มเหลว

คลิก **นำไปใช้** หลังจากเปลี่ยนแปลงการกำหนดค่า

การกำหนดค่านโยบายการจำกัดพลังงาน

โปรดใช้ข้อมูลในหัวข้อนี้ หากต้องการกำหนดค่านโยบายการจำกัดพลังงาน

หมายเหตุ: เซิร์ฟเวอร์โปรเซสเซอร์ AMD ไม่รองรับการกำหนดค่าฟังก์ชันนโยบายการจำกัดพลังงานของผู้ใช้

คุณสามารถเลือกเปิดใช้งานหรือปิดใช้งานฟังก์ชันการจำกัดพลังงาน หากเปิดใช้งานการจำกัดพลังงาน สามารถทำการเลือกเพื่อจำกัดปริมาณพลังงานที่ใช้โดยเซิร์ฟเวอร์ หากปิดใช้งานการจำกัดพลังงาน พลังงานสูงสุดที่ใช้โดยเซิร์ฟเวอร์จะถูกกำหนดโดยนโยบายการสำรองพลังงาน ในการเปลี่ยนการตั้งค่า ให้คลิก **รีเซ็ต** ก่อน เลือกการตั้งค่าที่คุณต้องการ จากนั้น คลิก **นำไปใช้**

สามารถเปิดใช้งานการจำกัดพลังงานโดยใช้มาตรการการใช้กระแสไฟ AC หรือมาตรการการใช้กระแสไฟ DC จากเมนูแบบดรอปดาวน์ ให้เลือกประเภทมาตรการที่จะใช้กำหนดขีดจำกัดของการจำกัดพลังงาน เมื่อสลับระหว่าง AC และ DC ตัวเลขบนแถบเลื่อนจะเปลี่ยนแปลงให้สอดคล้องกัน

มีวิธีเปลี่ยนการจำกัดพลังงานด้วยกันสองวิธี ดังนี้:

- **วิธีที่** 1: ย้ายเครื่องหมายแถบเลื่อนไปยังกำลังไฟฟ้าที่ต้องการเพื่อกำหนดขีดจำกัดพลังงานเซิร์ฟเวอร์โดยรวม
- **วิธีที่** 2: ป้อนค่าลงในช่องอินพุต เครื่องหมายแถบเลื่อนจะย้ายไปยังตำแหน่งที่สอดคล้องโดยอัตโนมัติ

คลิก **นำไปใช้** หลังจากเปลี่ยนแปลงการกำหนดค่า

หมายเหตุ: ตัวเลือก **นโยบายพลังงาน** จะไม่พร้อมใช้งานเมื่อ XClarity Controller อยู่ในตัวเครื่องที่มีเบลดหรือโหนดเซิร์ฟเวอร์ความหนาแน่นสูง นโยบายพลังงานจะถูกควบคุมโดยตัวควบคุมการจัดการตัวเครื่องแทน XClarity Controller

การกำหนดค่านโยบายการจ่ายไฟกลับเข้าระบบ

ใช้ข้อมูลในหัวข้อนี้ในการกำหนดค่าวิธีการที่เซิร์ฟเวอร์ตอบสนองเมื่อมีการจ่ายไฟกลับเข้าระบบหลังจากสูญเสียพลังงาน

เมื่อกำหนดค่านโยบายการจ่ายไฟกลับเข้าระบบ ตัวเลือกสามตัวเลือกต่อไปนี้จะพร้อมใช้งาน:

ปิดเสมอ

เซิร์ฟเวอร์จะยังคงปิดอยู่ แม้ว่าจะมีการจ่ายไฟกลับเข้าระบบแล้วก็ตาม

การคืนค่า

เซิร์ฟเวอร์จะเปิดโดยอัตโนมัติเมื่อมีการจ่ายไฟกลับเข้าระบบ หากมีการเปิดเซิร์ฟเวอร์ไว้ในเวลาที่เกิดไฟฟ้าขัดข้อง หรือเซิร์ฟเวอร์จะยังคงปิดอยู่ เมื่อมีการจ่ายไฟกลับเข้าระบบ

เปิดเสมอ

เซิร์ฟเวอร์จะเปิดโดยอัตโนมัติ เมื่อมีการจ่ายไฟกลับเข้าระบบ

คลิก **นำไปใช้** หลังจากเปลี่ยนแปลงการกำหนดค่า

หมายเหตุ: ตัวเลือก **นโยบายการจ่ายไฟกลับเข้าระบบ** จะไม่พร้อมใช้งานในตัวเครื่องที่มีเบลดหรือโหนดเซิร์ฟเวอร์ความหนาแน่นสูง นโยบายการจ่ายไฟกลับเข้าระบบจะถูกควบคุมโดยตัวควบคุมการจัดการตัวเครื่องแทน XClarity Controller

การดำเนินการด้านพลังงาน

ดูข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจการดำเนินการด้านพลังงานที่สามารถใช้ได้กับเซิร์ฟเวอร์

คลิก **การดำเนินการด้านพลังงาน** ในส่วน **การดำเนินการด่วน** ของหน้าแรก XClarity Controller

ตารางต่อไปนี้มีรายละเอียดของการดำเนินการด้านพลังงานและการรีสตาร์ทที่สามารถดำเนินการได้บนเซิร์ฟเวอร์

ตาราง 6. การดำเนินการด้านพลังงานและรายละเอียด

ตารางสองคอลัมน์ที่มีรายละเอียดของการดำเนินการด้านพลังงานและการรีสตาร์ทของเซิรฟ์เวอร์

การดำเนินการด้านพลังงาน	**รายละเอียด**
เปิดเซิร์ฟเวอร์	เลือกรายการการดำเนินการนี้เพื่อเปิดเซิร์ฟเวอร์ และบูตระบบปฏิบัติการ
ปิดเซิร์ฟเวอร์ตามปกติ	เลือกรายการการดำเนินการนี้เพื่อปิดระบบปฏิบัติการ แล้วปิดเซิร์ฟเวอร์
ปิดเซิร์ฟเวอร์ในทันที	เลือกรายการการดำเนินการนี้เพื่อปิดเซิร์ฟเวอร์โดยไม่ต้องปิดระบบปฏิบัติการก่อน
รีสตาร์ทเซิร์ฟเวอร์ตามปกติ	เลือกรายการการดำเนินการนี้เพื่อปิดระบบปฏิบัติการ แล้วเริ่มต้นเซิร์ฟเวอร์ใหม่
รีสตาร์ทเซิร์ฟเวอร์ในทันที	เลือกรายการการดำเนินการนี้เพื่อเริ่มต้นเซิร์ฟเวอร์ใหม่ในทันทีโดยไม่ต้องปิดระบบปฏิบัติการก่อน
บูตเซิร์ฟเวอร์ไปยังการตั้งค่าระบบ	เลือกรายการนี้เพื่อเปิดเครื่องหรือรีบูตเซิร์ฟเวอร์ และบูตไปยังการตั้งค่าระบบโดยอัตโนมัติโดยไม่จำเป็นต้องกด F1 ระหว่างการบูต

ตาราง 6. การดำเนินการด้านพลังงานและรายละเอียด (มีต่อ)

การดำเนินการด้านพลังงาน	**รายละเอียด**
ทริกเกอร์สัญญาณขัดจังหวะความสำคัญสูง (NMI)	เลือกรายการของการดำเนินการนี้เพื่อบังคับให้เกิดสัญญาณขัดจังหวะความสำคัญสูง (NMI) บนระบบที่มี “อาการค้าง” การเลือกรายการของการดำเนินการนี้จะทำให้ระบบปฏิบัติการของแพลตฟอร์มสามารถดำเนินการถ่ายโอนข้อมูลหน่วยความจำ ซึ่งสามารถใช้เพื่อวัตถุประสงค์ในการแก้ไขข้อบกพร่องจากอาการค้างของระบบ การรีบูตอัตโนมัติในการตั้งค่า NMI จากเมนูการตั้งค่าระบบ F1 จะกำหนดว่า XClarity Controller จะรีบูตเซิร์ฟเวอร์หลังจาก NMI หรือไม่
กำหนดเวลาดำเนินการด้านพลังงาน	เลือกรายการการดำเนินการนี้เพื่อกำหนดเวลาการดำเนินการด้านพลังงานและการรีสตาร์ทสำหรับเซิร์ฟเวอร์รายวันและรายสัปดาห์
รีสตาร์ทตัวควบคุมการจัดการ	เลือกรายการการดำเนินการนี้เพื่อรีสตาร์ท XClarity Controller
เซิร์ฟเวอร์เริ่มต้นระบบกำลังไฟ AC	เลือกการดำเนินการนี้เพื่อเริ่มต้นเซิร์ฟเวอร์ใหม่
หมายเหตุ: หากระบบปฏิบัติการอยู่ในโหมดการพักหน้าจอหรือโหมดล็อคเมื่อพยายามปิดระบบปฏิบัติการ XClarity Controller อาจไม่สามารถเริ่มต้นการปิดเครื่องได้ตามปกติ XClarity Controller จะดำเนินการฮาร์ดรีเซ็ตหรือปิดเครื่องหลังจากช่วงการหน่วงเวลาปิดเครื่องหมดอายุ ขณะที่ระบบปฏิบัติการอาจยังคงทำงานอยู่	

การจัดการและการติดตามผลการใช้พลังงานด้วยคำสั่ง IPMI

ใช้ข้อมูลในหัวข้อนี้เพื่อจัดการและติดตามผลการใช้พลังงานโดยใช้คำสั่ง IPMI

หัวข้อนี้จะอธิบายวิธีใช้ Intel Intelligent Power Node Manager และ Data Center Manageability Interface (DCMI) เพื่อมอบการตรวจสอบพลังงานและความร้อน และการจัดการพลังงานตามนโยบายสำหรับเซิร์ฟเวอร์ที่ใช้คำสั่งการจัดการพลังงาน Intelligent Platform Management Interface (IPMI)

สำหรับเซิร์ฟเวอร์ที่ใช้ Intel Node Manager SPS 3.0, ผู้ใช้ XClarity Controller สามารถใช้คำสั่งการจัดการพลังงาน IPMI ที่มีให้บริการโดย Management Engine (ME) ของ Intel ในการควบคุมคุณลักษณะ Node Manager และตรวจสอบการใช้พลังงานของเซิร์ฟเวอร์ นอกจากนี้ ยังสามารถดำเนินการการจัดการพลังงานของเซิร์ฟเวอร์ได้โดยใช้คำสั่งการจัดการพลังงาน DCMI ตัวอย่าง Node Manager และคำสั่งการจัดการพลังงาน DCMI มีระบุไว้ในหัวข้อนี้

การจัดการพลังงานของเซิร์ฟเวอร์โดยใช้คำสั่ง Node Manager

ใช้ข้อมูลในหัวข้อนี้เพื่อจัดการพลังงานของเซิร์ฟเวอร์โดยใช้ตัวจัดการโหนด

เฟิร์มแวร์ Intel Node Manager ไม่มีอินเทอร์เฟซภายนอก ดังนั้น XClarity Controller ต้องได้รับคำสั่ง Node Manager ก่อน แล้วจึงส่งไปยัง Intel Node Manager XClarity Controller จะทำหน้าที่เป็นรีเลย์และอุปกรณ์ส่งคำสั่ง IPMI โดยใช้การบริดจ์ IPMI มาตรฐาน

หมายเหตุ: การเปลี่ยนนโยบาย Node Manager โดยใช้คำสั่ง Node Manager IPMI อาจสร้างข้อขัดแย้งกับฟังก์ชันการจัดการพลังงานของ XClarity Controller ตามค่าเริ่มต้น การบริดจ์ของคำสั่ง Node Manager จะถูกปิดใช้งานเพื่อป้องกันข้อขัดแย้ง

สำหรับผู้ใช้ที่ต้องการจัดการพลังงานของเซิร์ฟเวอร์โดยใช้ Node Manager แทน XClarity Controller มีคำสั่ง OEM IPMI ที่ประกอบด้วย (ฟังก์ชันเครือข่าย: *0x3A*) และ (คำสั่ง: *0xC7*) ให้ใช้งาน

ในการเปิดใช้งานคำสั่ง Node Manager IPMI ดั้งเดิม ให้พิมพ์:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01`

ในการปิดใช้งานคำสั่ง Node Manager IPMI ดั้งเดิม ให้พิมพ์:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00`

ข้อมูลต่อไปนี้เป็นตัวอย่างของคำสั่งการจัดการพลังงาน Node Manager

หมายเหตุ:

- โดยการระบุ IPMI *ช่อง 0* และที่อยู่เป้าหมาย *0x2c* คุณสามารถใช้ IPMITOOL ในการส่งคำสั่งไปยัง Intel Node Manager เพื่อการประมวลผล ข้อความคำขอถูกใช้เพื่อเริ่มต้นการดำเนินการ และข้อความการตอบสนองจะถูกส่งกลับไปยังผู้ร้องขอ
- คำสั่งจะแสดงในรูปแบบต่อไปนี้เนื่องจากมีพื้นที่จำกัด

การตรวจสอบพลังงานโดยใช้ Get Global System Power Statistics, (**รหัสคำสั่ง** 0xC8): คำขอ:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00` การตอบสนอง:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

การจำกัดพลังงานโดยใช้ Set Intel Node Manager Policy, (**รหัสคำสั่ง** 0xC1): คำขอ:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00`การตอบสนอง:57 01 00

การประหยัดพลังงานโดยใช้ Set Intel Node Manager Policy, (**รหัสคำสั่ง** 0xC1): คำขอ:`ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00`

รับฟังก์ชัน ID อุปกรณ์โดยใช้ Get Intel Management Engine Device ID:คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* -b *0x00* -t *0x2c* raw *0x06 0x01*การตอบสนอง:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

สำหรับคำสั่ง Intel Node Manager เพิ่มเติม โปรดดูเอกสารฉบับล่าสุดของ *ข้อมูลจำเพาะสำหรับอินเทอร์เฟซภายนอกของ Intel Intelligent Power Node Manager ที่ใช้ IPMI* ที่ https://businessportal.intel.com

การจัดการพลังงานของเซิร์ฟเวอร์โดยใช้คำสั่ง DCMI

ใช้ข้อมูลในหัวข้อนี้เพื่อจัดการพลังงานของเซิร์ฟเวอร์โดยใช้คำสั่ง DCMI

DCMI มีฟังก์ชันการตรวจสอบและการควบคุมที่สามารถแสดงผ่านอินเทอร์เฟซของซอฟต์แวร์การจัดการมาตรฐาน นอกจากนี้ ยังสามารถดำเนินการฟังก์ชันการจัดการพลังงานของเซิร์ฟเวอร์ได้โดยใช้คำสั่ง DCMI

ข้อมูลต่อไปนี้เป็นตัวอย่างของฟังก์ชันและคำสั่งการจัดการพลังงาน DCMI ที่ใช้งานทั่วไป ข้อความคำขอถูกใช้เพื่อเริ่มต้นการดำเนินการ และข้อความการตอบสนองจะถูกส่งกลับไปยังผู้ร้องขอ

หมายเหตุ: คำสั่งจะแสดงในรูปแบบต่อไปนี้เนื่องจากมีพื้นที่จำกัด

รับการอ่านค่าพลังงาน: คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x02 0xdc 0x01 0x00 0x00* การตอบสนอง:dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

ตั้งค่าขีดจำกัดพลังงาน: คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *PASSWORD* raw *0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03* การตอบสนอง:dc

รับค่าตัวเก็บประจุพลังงาน: คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x03 0xdc 0x00 0x00* การตอบสนอง:dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

เปิดใช้งานขีดจำกัดพลังงาน: คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x05 0xdc 0x01 0x00 0x00* การตอบสนอง:dc

ปิดใช้งานกำจัดพลังงาน: คำขอ:ipmitool -H *<$XClarity_Controller_IP>* -U *<USERID>* -P *<PASSWORD>* raw *0x2c 0x05 0xdc 0x00 0x00 0x00* การตอบสนอง:dc

หมายเหตุ: ในบางเซิร์ฟเวอร์ การดำเนินการยกเว้นสำหรับคำสั่ง **ตั้งค่าขีดจำกัดพลังงาน**: อาจไม่ได้รับการรองรับ ตัวอย่างเช่น พารามิเตอร์ *Hard Power Off system and log events to SEL* อาจไม่ได้รับการรองรับ

สำหรับรายการคำสั่งทั้งหมดที่ได้รับการรองรับโดยข้อมูลจำเพาะ DCMI โปรดดูเอกสารฉบับล่าสุดของ *ข้อมูลจำเพาะของ Data Center Manageability Interface* ที่ https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf

---

ฟังก์ชันคอนโซลระยะไกล

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีการดูและโต้ตอบกับคอนโซลเซิร์ฟเวอร์ระยะไกล

คุณสามารถใช้ฟังก์ชันคอนโซลระยะไกลในเว็บอินเทอร์เฟซ XClarity Controller เพื่อดูและโต้ตอบกับคอนโซลเซิร์ฟเวอร์ คุณสามารถกำหนดดิสก์อิมเมจ (ไฟล์ ISO หรือ IMG) เป็นไดรฟ์เสมือนบนเซิร์ฟเวอร์ ฟังก์ชันคอนโซลระยะไกลมีให้ใช้งานร่วมกับคุณลักษณะขั้นสูงของ XClarity Controller และคุณลักษณะระดับองค์กรของ XClarity Controller และพร้อมใช้งานผ่านเว็บอินเทอร์เฟซเท่านั้น คุณต้องเข้าสู่ระบบ XClarity Controller ด้วย ID ผู้ใช้ที่มีสิทธิ์ระดับผู้ควบคุมหรือสิทธิ์การเข้าถึงคอนโซลระยะไกล เพื่อใช้งานคุณลักษณะคอนโซลระยะไกล สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการอัปเกรดจาก XClarity Controller ระดับมาตรฐานเป็น XClarity Controller ขั้นสูงหรือ XClarity Controller ระดับองค์กร โปรดดู “การอัปเกรด XClarity Controller” บนหน้าที่ 8

ใช้คุณลักษณะคอนโซลระยะไกลในการทำสิ่งต่างๆ ต่อไปนี้:

- การดูวิดีโอจากระยะไกลด้วยความละเอียดกราฟิกสูงสุด 1280 x 1024 ที่ 72 หรือ 75Hz โดยไม่คำนึงถึงสถานะของเซิร์ฟเวอร์
- การเข้าถึงเซิร์ฟเวอร์จากระยะไกลโดยใช้แป้นพิมพ์และเมาส์จากไคลเอ็นต์ระยะไกล
- การติดตั้งไฟล์ ISO และ IMG ที่อยู่บนระบบภายในของคุณ หรือบนระบบระยะไกลเป็นไดรฟ์เสมือนที่พร้อมให้เซิร์ฟเวอร์ใช้งาน
- อัปโหลดอิมเมจ IMG หรือ ISO ไปยังหน่วยความจำของ XClarity Controller และติดตั้งกับเซิร์ฟเวอร์เป็นไดรฟ์เสมือน ไฟล์สูงสุดสองไฟล์ที่มีขนาดรวมสูงสุด 50 MB อาจถูกอัปโหลดลงในหน่วยความของ XClarity Controller

หมายเหตุ:

- เมื่อเริ่มต้นคุณลักษณะคอนโซลระยะไกลในโหมดผู้ใช้หลายราย (XClarity Controller ที่มีชุดคุณลักษณะระดับองค์กรของ XClarity Controller จะรองรับเซสชันพร้อมกันสูงสุดหกเซสชัน) จะสามารถใช้คุณลักษณะดิสก์ระยะไกลได้ครั้งละหนึ่งเซสชันเท่านั้น
- คอนโซลระยะไกลสามารถแสดงผลเฉพาะวิดีโอที่สร้างโดยตัวควบคุมวิดีโอบนแผงระบบเท่านั้น หากมีการติดตั้งอะแดปเตอร์ตัวควบคุมวิดีโอแยกต่างหากและใช้แทนที่ตัวควบคุมวิดีโอของระบบ คอนโซลระยะไกลของ XClarity Controller จะไม่สามารถแสดงผลเนื้อหาวิดีโอจากอะแดปเตอร์ที่เพิ่มได้
- หากคุณมีไฟร์วอลล์ในเครือข่าย คุณต้องเปิดพอร์ตเครือข่ายเพื่อรองรับคุณลักษณะคอนโซลระยะไกล ในการดูหรือเปลี่ยนหมายเลขพอร์ตเครือข่ายที่ใช้โดยคุณลักษณะคอนโซลระยะไกล โปรดดู “การเปิดใช้งานบริการและการกำหนดพอร์ต” บนหน้าที่ 46

- คุณลักษณะคอนโซลระยะไกลจะใช้ HTML5 สำหรับแสดงผลวิดีโอเซิร์ฟเวอร์บนเว็บเพจ ในการใช้คุณลักษณะนี้ เบราเซอร์ของคุณต้องรองรับการแสดงผลเนื้อหาวิดีโอที่ใช้องค์ประกอบ HTML5
- หากคุณใช้ใบรับรองที่ลงนามด้วยตนเองและที่อยู่ IPv6 ในการเข้าถึง BMC ด้วยเบราเซอร์ Internet Explorer เซสชันคอนโซลระยะไกลอาจไม่สามารถเริ่มได้ เนื่องจากข้อผิดพลาดของใบรับรอง เพื่อหลีกเลี่ยงปัญหานี้ สามารถเพิ่มใบรับรองที่ลงนามด้วยตนเองไปยังผู้อนุมัติใบรับรอง Trust Root ของ Internet Explorer:
  - เลือก Security ภายใต้ **การกำหนดค่า BMC** และดาวน์โหลดใบรับรองที่ลงนามด้วยตนเอง
  - เปลี่ยนนามสกุลไฟล์ของใบรับรองเป็น *.crt และดับเบิลคลิกไฟล์ใบรับรองเว็บ
  - ล้างแคชของเบราว์เซอร์ IE11
  - คลิก **ติดตั้งใบรับรอง** เพื่อติดตั้งใบรับรองในที่เก็บใบรับรองโดยดำเนินการตามขั้นตอนของตัวช่วยสร้างการนำเข้าใบรับรอง

การเปิดใช้งานฟังก์ชันคอนโซลระยะไกล

หัวข้อนี้แสดงข้อมูลเกี่ยวกับฟังก์ชันคอนโซลระยะไกล

ดังที่ระบุไว้ก่อนหน้านี้ ฟังก์ชันคอนโซลระยะไกล XClarity Controller จะพร้อมใช้งานเฉพาะในคุณลักษณะขั้นสูงของ XClarity Controller และคุณลักษณะระดับองค์กรของ XClarity Controller เท่านั้น หากคุณไม่มีสิทธิ์ในการดำเนินการคอนโซลระยะไกล คุณจะเห็นไอคอนกุญแจ

หลังจากคุณซื้อและได้รับคีย์เปิดการทำงานสำหรับการอัปเกรดขั้นสูงของ XClarity Controller ให้ติดตั้งการอัปเกรดนั้นโดยใช้คำแนะนำภายใต้ “การติดตั้งคีย์เปิดการทำงาน” บนหน้าที่ 133

ในการใช้ฟังก์ชันคอนโซลระยะไกล ให้ดำเนินการขั้นตอนต่อไปนี้:

1. คลิกรูปภาพที่มีลูกศรชี้แนวทแยงมุมสีขาวในส่วนคอนโซลระยะไกลของหน้าแรก XClarity Controller หรือเว็บเพจคอนโซลระยะไกล
2. เลือกโหมดใดโหมดหนึ่งต่อไปนี้:
   - เริ่มคอนโซลระยะไกลในโหมดผู้ใช้รายเดียว
   - เริ่มคอนโซลระยะไกลในโหมดผู้ใช้หลายราย

   หมายเหตุ: XClarity Controller ที่มีชุดคุณลักษณะ XClarity Controller ระดับองค์กรรองรับเซสชันวิดีโอพร้อมกันสูงสุดหกเซสชันในโหมดผู้ใช้หลายราย
3. เลือกว่าจะอนุญาตให้ผู้อื่นสามารถร้องขอการส่งคำขอยกเลิกการเชื่อมต่อไปยังผู้ใช้คอนโซลระยะไกลหรือไม่ เมื่อมีผู้ที่ต้องการใช้คุณลักษณะคอนโซลระยะไกล และมีการใช้งานคุณลักษณะดังกล่าวในโหมดผู้ใช้รายเดียว หรือเมื่อมีผู้ใช้งานคุณลักษณะคอนโซลระยะไกลในโหมดผู้ใช้หลายรายครบจำนวนสูงสุดแล้ว **ช่วงเวลาที่ไม่มีการตอบ**

สนอง ระบุระยะเวลาที่ให้ XClarity Controller รอก่อนจะยกเลิกการเชื่อมต่อผู้ใช้โดยอัตโนมัติ หากไม่ได้รับการตอบสนองต่อคำขอยกเลิกการเชื่อมต่อ

4. เลือกว่าจะอนุญาตให้บันทึกวิดีโอการบูตเซิร์ฟเวอร์สามรายการล่าสุดหรือไม่
5. เลือกว่าจะอนุญาตให้บันทึกวิดีโอเซิร์ฟเวอร์ล่มสามรายการล่าสุดหรือไม่
6. เลือกว่าจะอนุญาตให้ถ่ายภาพหน้าจอระบบปฏิบัติการล้มเหลวที่มีข้อผิดพลาด HW หรือไม่
7. คลิก **เปิดใช้คอนโซลระยะไกล** เพื่อเปิดหน้าคอนโซลระยะไกลในอีกแท็บหนึ่ง เมื่อเซสชันคอนโซลระยะไกลที่เป็นไปได้ทั้งหมดอยู่ระหว่างใช้งาน กล่องโต้ตอบจะปรากฏขึ้นมา จากกล่องโต้ตอบนี้ ผู้ใช้สามารถส่งคำขอยกเลิกการเชื่อมต่อไปยังผู้ใช้คอนโซลระยะไกล ซึ่งได้เปิดใช้งานการตั้งค่าเป็น **อนุญาตให้ผู้อื่นร้องขอการยกเลิกการเชื่อมต่อเซสชันระยะไกลของฉัน** ผู้ใช้สามารถยอมรับหรือปฏิเสธคำขอยกเลิกการเชื่อมต่อได้ หากผู้ใช้ไม่ตอบสนองภายในระยะเวลาที่ระบุโดยการตั้งค่า **ช่วงเวลาที่ไม่มีการตอบสนอง** XClarity Controller จะสิ้นสุดเซสชันของผู้ใช้โดยอัตโนมัติ

การควบคุมการเปิด/ปิดเครื่องระยะไกล

หัวข้อนี้จะอธิบายวิธีส่งคำสั่งเปิด/ปิดเครื่องและเริ่มระบบใหม่ไปยังเซิร์ฟเวอร์จากหน้าต่างคอนโซลระยะไกล

คุณสามารถส่งคำสั่งเปิด/ปิดเครื่องและเริ่มระบบใหม่ไปยังเซิร์ฟเวอร์จากหน้าต่างคอนโซลระยะไกลโดยไม่ต้องกลับไปยังเว็บเพจหลัก ในการควบคุมพลังงานของเซิร์ฟเวอร์ด้วยคอนโซลระยะไกล ให้คลิก **พลังงาน** และเลือกคำสั่งใดคำสั่งหนึ่งต่อไปนี้:

เปิดเซิร์ฟเวอร์
เลือกรายการการดำเนินการนี้เพื่อเปิดเซิร์ฟเวอร์ และบูตระบบปฏิบัติการ

ปิดเซิร์ฟเวอร์ตามปกติ
เลือกรายการการดำเนินการนี้เพื่อปิดระบบปฏิบัติการ แล้วปิดเซิร์ฟเวอร์

ปิดเซิร์ฟเวอร์ในทันที
เลือกรายการการดำเนินการนี้เพื่อปิดเซิร์ฟเวอร์โดยไม่ต้องปิดระบบปฏิบัติการก่อน

รีสตาร์ทเซิร์ฟเวอร์ตามปกติ
เลือกรายการการดำเนินการนี้เพื่อปิดระบบปฏิบัติการ แล้วเริ่มต้นเซิร์ฟเวอร์ใหม่

รีสตาร์ทเซิร์ฟเวอร์ในทันที
เลือกรายการการดำเนินการนี้เพื่อเริ่มต้นเซิร์ฟเวอร์ใหม่ในทันทีโดยไม่ต้องปิดระบบปฏิบัติการก่อน

บูตเซิร์ฟเวอร์ไปยังการตั้งค่าระบบ
เลือกรายการนี้เพื่อเปิดเครื่องหรือรีบูตเซิร์ฟเวอร์ และบูตไปยังการตั้งค่าระบบโดยอัตโนมัติโดยไม่จำเป็นต้องกด F1 ระหว่างการบูต

การจับภาพหน้าจอคอนโซลระยะไกล

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีใช้คุณลักษณะการจับภาพหน้าจอคอนโซลระยะไกล

คุณลักษณะการจับภาพหน้าจอในหน้าต่างคอนโซลระยะไกลจะจับภาพเนื้อหาบนจอแสดงผลภาพของเซิร์ฟเวอร์ ในการจับภาพและบันทึกภาพหน้าจอ ให้ดำเนินการตามขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. ในหน้าต่างคอนโซลระยะไกล ให้คลิก **จับภาพหน้าจอ**

ขั้นตอนที่ 2. ในหน้าต่างป็อปอัป ให้คลิก**บันทึกไฟล์** และกด **ตกลง** ไฟล์จะถูกตั้งชื่อเป็น rpviewer.png และบันทึกไปยังโฟลเดอร์การดาวน์โหลดเริ่มต้นของคุณ

หมายเหตุ: รูปภาพของการจับภาพหน้าจอจะได้รับการบันทึกเป็นประเภทไฟล์ PNG

การสนับสนุนแป้นพิมพ์คอนโซลระยะไกล

ในหน้าต่างคอนโซลระยะไกล ภายใต้ **แป้นพิมพ์** จะมีตัวเลือกให้ใช้งานดังต่อไปนี้:

- คลิก **แป้นพิมพ์เสมือน** เพื่อเปิดใช้งานแป้นพิมพ์เสมือน คุณลักษณะนี้มีประโยชน์หากคุณกำลังใช้งานอุปกรณ์แท็บเล็ตที่ไม่มีแป้นพิมพ์จริง สามารถใช้ตัวเลือกต่อไปนี้ในการสร้างมาโครและการกดแป้นพิมพ์พร้อมกัน ซึ่งสามารถส่งไปยังเซิร์ฟเวอร์ ระบบปฏิบัติการบนระบบไคลเอ็นต์ที่คุณกำลังใช้งานอาจพิมพ์ทับการกดแป้นพิมพ์พร้อมกันบางส่วน (ตัวอย่างเช่น Ctrl+Alt+Del) แทนที่จะส่งไปยังเซิร์ฟเวอร์ ปุ่มอื่นๆ เช่น F1 หรือ Esc อาจถูกขัดขวางโดยโปรแกรมหรือเบราเซอร์ที่คุณกำลังใช้งาน มาโครจะให้กลไกในการส่งการกดปุ่มไปยังเซิร์ฟเวอร์ที่ผู้ใช้อาจไม่สามารถส่งได้
- คลิก **มาโครของเซิร์ฟเวอร์** เพื่อใช้มาโครที่เซิร์ฟเวอร์กำหนด มาโครของเซิร์ฟเวอร์บางส่วนได้รับการกำหนดค่าไว้ล่วงหน้าโดยเฟิร์มแวร์ของ XClarity Controller สามารถกำหนดมาโครที่เซิร์ฟเวอร์กำหนดอื่นๆ โดยใช้ Lenovo XClarity Essentials และดาวน์โหลดได้จาก XClarity Controller มาโครเหล่านี้ถูกกำหนดไว้สำหรับผู้ใช้ทั้งหมดของคุณลักษณะคอนโซลระยะไกล
- คลิก **กำหนดค่า** เพื่อเพิ่มหรือลบมาโครที่ผู้ใช้กำหนด มาโครที่ผู้ใช้กำหนดจะถูกกำหนดเฉพาะสำหรับผู้ใช้คอนโซลระยะไกลในปัจจุบันเท่านั้น ผู้ใช้คอนโซลระยะไกลคนอื่นๆ จะไม่เห็นมาโครที่ผู้ใช้กำหนดของกันและกัน
  - คลิกไอคอนเพิ่มมาโครและกดลำดับปุ่มที่คุณต้องการ แล้วคลิก **เพิ่ม** เพื่อเพิ่มมาโครใหม่
  - ในการลบมาโครที่ผู้ใช้กำหนด ให้เลือกมาโครจากรายการและคลิกไอคอนถังขยะ
  - ในการส่งมาโครที่ผู้ใช้กำหนดไปยังเซิร์ฟเวอร์ ให้เลือกตัวเลือก **มาโครที่ผู้ใช้กำหนด** และคลิกบนมาโครที่คุณต้องการส่ง

การสนับสนุนเมาส์คอนโซลระยะไกล

ใช้ข้อมูลนี้เพื่อทำความเข้าใจตัวเลือกต่างๆ สำหรับการควบคุมเมาส์ระยะไกล

หน้าต่างคอนโซลระยะไกลมีตัวเลือกต่างๆ มากมายสำหรับการสนับสนุนเมาส์ รวมถึงการควบคุมเมาส์แบบ Absolute, การควบคุมเมาส์แบบ Relative (ไม่มีการเร่ง) และการควบคุมเมาส์ (RHEL, Linux ที่เก่ากว่า)

ระบบควบคุมเมาส์แบบ Absolute และ Relative

ใช้ข้อมูลนี้เพื่อเข้าถึงตัวเลือกแบบ Absolute และ Relative สำหรับการควบคุมเมาส์

ในการเข้าถึงตัวเลือกแบบ Absolute และ Relative สำหรับการควบคุมเมาส์ ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. ในหน้าต่างคอนโซลระยะไกล ให้คลิก **เมาส์**

ขั้นตอนที่ 2. คลิก **การตั้งค่าเมาส์** จากเมนูแบบดรอปดาวน์

ขั้นตอนที่ 3. เลือกโหมด **การเร่งประสิทธิภาพเมาส์** โหมดใดโหมดหนึ่งต่อไปนี้:

การจัดตำแหน่งแบบ Absolute (Windows, Linux เวอร์ชันใหม่ และ Mac OS X)
ไคลเอ็นต์จะส่งข้อความแสดงตำแหน่งเมาส์ไปยังเซิร์ฟเวอร์ที่สัมพันธ์กับจุดเริ่มต้น (พื้นที่ด้านซ้ายบน) ของพื้นที่การดู

การจัดตำแหน่งแบบ Relative โดยไม่มีการเร่งประสิทธิภาพ
ไคลเอ็นต์จะส่งตำแหน่งเมาส์ค่าชดเชยจากตำแหน่งเมาส์ก่อนหน้า

การจัดตำแหน่งแบบ Relative (Linux เวอร์ชันเก่า)
โหมดนี้จะนำปัจจัยการเร่งประสิทธิภาพไปใช้ในการปรับแนวเมาส์ได้ดียิ่งขึ้นบนเป้าหมายบน Linux บางเป้าหมาย มีการเลือกการตั้งค่าการเร่งประสิทธิภาพเพื่อเพิ่มขีดความสามารถในการเข้ากันได้กับ Linux Distribution เวอร์ชันเก่ากว่า

บันทึก/เล่นซ้ำวิดีโอหน้าจอ

ใช้ข้อมูลในหัวข้อนี้เพื่อบันทึกหรือเล่นซ้ำวิดีโอหน้าจอระยะไกล

เว็บอินเทอร์เฟซ XClarity Controller มีคุณลักษณะที่คล้ายกับ DVR เพื่อรองรับการบันทึกและการเล่นวิดีโอหน้าจอระยะไกล ฟังก์ชันนี้รองรับการบันทึกวิดีโอลงในโฟลเดอร์เครือข่ายเท่านั้น ขณะนี้ระบบรองรับแค่โปรโตคอล NFS และ CIFS ต่อไปนี้คือขั้นตอนในการใช้ฟังก์ชันการบันทึกและเล่นซ้ำ

1. บนเว็บเพจคอนโซลระยะไกล ให้คลิก**การบันทึกหน้าจอ**เพื่อเปิดหน้าต่างการตั้งค่า
2. ในหน้าต่างการตั้งค่า อาจจำเป็นต้องระบุข้อมูลต่อไปนี้

- หากมีการเลือกประเภทการเมาท์ “CIFS” ให้ระบุพารามิเตอร์**โฟลเดอร์ระยะไกล ชื่อผู้ใช้** และ**รหัสผ่าน** รูปแบบสำหรับโฟลเดอร์ระยะไกลของ CIFS คือ “//**<ที่อยู่ IP ระยะไกล>**/**<ชื่อโฟลเดอร์>**” ตัวอย่างเช่น: //xxx.xxx.xxx.xxx/folder
- หากมีการเลือกประเภทการเมาท์ “NFS” ให้ระบุพารามิเตอร์**โฟลเดอร์ระยะไกล** รูปแบบสำหรับโฟลเดอร์ระยะไกลของ NFS คือ “**<ที่อยู่ IP ระยะไกล>**:/**<ชื่อโฟลเดอร์>**” ตัวอย่างเช่น: xxx.xxx.xxx.xxx:/folder
- ระบุชื่อไฟล์วิดีโอหากจำเป็น หากมีการระบุชื่อไฟล์แล้ว กล่องข้อความแสดงข้อผิดพลาดจะแสดงขึ้น หากต้องการเขียนทับชื่อไฟล์ที่มีอยู่ ให้เลือก “เขียนทับชื่อไฟล์” หากมีการเลือกกล่อง “อัตโนมัติ” ระบบจะตั้งชื่อไฟล์วิดีโอโดยอัตโนมัติ
- “ขนาดไฟล์สูงสุด” แสดงขนาดไฟล์วิดีโอสูงสุดก่อนที่การบันทึกวิดีโอจะหยุดทำงานโดยอัตโนมัติ
- “ระยะเวลาการบันทึกสูงสุด” แสดงระยะเวลาการบันทึกวิดีโอสูงสุดก่อนที่การบันทึกวิดีโอจะหยุดทำงานโดยอัตโนมัติ

3. คลิก **เริ่มการบันทึกวิดีโอ** เพื่อเริ่มบันทึกวิดีโอ
4. คลิก **หยุดการบันทึกวิดีโอ** เพื่อหยุดบันทึกวิดีโอ หน้าต่างป๊อปอัปที่บอกว่า “การบันทึกวิดีโอเสร็จสมบูรณ์” จะปรากฏขึ้นและแสดงข้อมูลการบันทึกวิดีโอที่เกี่ยวข้อง
5. ดาวน์โหลดวิดีโอที่บันทึกจาก NFS หรือ CIFS ไปยังโฟลเดอร์ภายในเครื่องของคุณ ในส่วนการแสดงตัวอย่างคอนโซลระยะไกลของหน้าแรกของ XClarity Controller ให้คลิก **วิดีโอที่บันทึกไว้** และเลือกไฟล์วิดีโอที่จะเล่นซ้ำ

โหมดหน้าจอคอนโซลระยะไกล

ใช้ข้อมูลในหัวข้อนี้เพื่อกำหนดค่าโหมดหน้าจอคอนโซลระยะไกล

ในการกำหนดค่าโหมดหน้าจอคอนโซลระยะไกล ให้คลิก **โหมดหน้าจอ**

ตัวเลือกเมนูมีดังต่อไปนี้:

เต็มหน้าจอ

โหมดนี้จะเติมเดสก์ท็อปของไคลเอ็นต์ด้วยจอแสดงผลภาพ การกดปุ่ม Esc ในโหมดนี้จะออกจากโหมดเต็มหน้าจอ เนื่องจากเมนูคอนโซลระยะไกลจะไม่ปรากฏให้เห็นในโหมดเต็มหน้าจอ คุณจะต้องออกจากโหมดเต็มหน้าจอเพื่อใช้คุณลักษณะใดๆ ที่มีให้ใช้งานผ่านเมนูคอนโซลระยะไกล เช่น มาโครแป้นพิมพ์

พอดีหน้าจอ

ตัวเลือกนี้เป็นการตั้งค่าเริ่มต้นเมื่อเปิดใช้งานคอนโซลระยะไกล ในการตั้งค่านี้ เดสก์ท็อปเป้าหมายจะแสดงผลโดยสมบูรณ์โดยไม่มีแถบเลื่อน ระบบจะรักษาอัตราส่วนกว้างยาวไว้

หน้าจอแบบปรับมาตราส่วน

เมื่อมีการเปิดใช้งานการปรับมาตราส่วน ขนาดวิดีโอจะถูกปรับขนาดเพื่อให้ภาพทั้งภาพถูกปรับมาตราส่วนให้เติมหน้าต่างคอนโซลได้

หน้าจอขนาดเดิม

ภาพวิดีโอมีขนาดเท่ากับฝั่งเซิร์ฟเวอร์ แถบเลื่อนจะปรากฏหากจำเป็นเพื่อทำให้สามารถดูพื้นที่ของภาพวิดีโอที่ไม่พอดีกับภายในหน้าต่างได้

โหมดสี

ปรับความคมชัดของสีสำหรับหน้าต่างคอนโซลระยะไกล โหมดสีมีด้วยกันสองตัวเลือก ดังนี้:

- สี: 7, 9, 12, 15 และ 23 บิต
- ระดับสีเทา: 16, 32, 64 และ 128 เฉด

หมายเหตุ: มักจะมีการปรับโหมดสีหากการเชื่อมต่อไปยังเซิร์ฟเวอร์ระยะไกลมีแบนด์วิธจำกัด และคุณต้องการลดความต้องการใช้แบนด์วิธ

วิธีการติดตั้งสื่อ

โปรดใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจวิธีการเมาท์สื่อ

มีตัวเลือกกลไกให้สามชุด สำหรับติดตั้งไฟล์ ISO และ IMG เพื่อใช้เป็นไดรฟ์แบบเสมือน

- สามารถเพิ่มไดรฟ์เสมือนไปยังเซิร์ฟเวอร์จากเซสชันคอนโซลระยะไกลโดยคลิก **สื่อ**
- จากเว็บเพจคอนโซลระยะไกลโดยตรง โดยไม่ต้องสร้างเซสชันของคอนโซลระยะไกล
- เครื่องมือแบบสแตนด์อโลน

ผู้ใช้ต้องมีสิทธิ์ **การเข้าถึงคอนโซลระยะไกลและดิสก์ระยะไกล** เพื่อใช้คุณลักษณะสื่อเสมือน

ผู้ใช้สามารถติดตั้งไฟล์เป็นสื่อแบบเสมือนได้จากระบบภายในหรือจากเซิร์ฟเวอร์ระยะไกล และสามารถเข้าถึงได้ผ่านเครือข่าย หรืออัปโหลดลงในหน่วยความจำของ XClarity Controller โดยใช้คุณสมบัติ RDOC กลไกเหล่านี้อธิบายไว้ทางด้านล่าง

- สื่อภายในเป็นไฟล์ ISO หรือ IMG ซึ่งอยู่ในระบบที่คุณกำลังใช้เพื่อเข้าถึง XClarity Controller กลไกนี้จะพร้อมใช้งานผ่านเซสชันคอนโซลระยะไกลเท่านั้น ไม่ใช่จากเว็บเพจคอนโซลระยะไกลโดยตรง และมีให้ใช้งานร่วมกับคุณลักษณะระดับองค์กรของ XClarity Controller เท่านั้น ในการเมาท์สื่อภายใน ให้คลิก**เปิดใช้งาน** ในส่วน **เมาท์สื่อภายใน** คุณสามารถติดตั้งไฟล์บนเซิร์ฟเวอร์ได้สูงสุดสี่ไฟล์พร้อมกัน

  หมายเหตุ:

- เมื่อใช้งานเบราเซอร์ Google Chrome คุณสามารถใช้งานตัวเลือกการติดตั้งเสริมที่เรียกว่า **เมาท์ไฟล์/โฟลเดอร์** เพื่อลากและวางไฟล์/โฟลเดอร์ได้
- หากมีเซสชันคอนโซลระยะไกลดำเนินอยู่พร้อมกันหลายเซสชันด้วย XClarity Controller ฟีเจอร์นี้สามารถเปิดใช้งานได้โดยเซสชันใดเซสชันหนึ่งเท่านั้น

• ไฟล์ที่อยู่ในระบบระยะไกลสามารถเมาท์เป็นสื่อเสมือนได้ สามารถติดตั้งไฟล์เป็นสื่อเสมือนพร้อมกันได้สูงสุดสี่ไฟล์ XClarity Controller รองรับการทำงานร่วมกับโปรโตคอลการแบ่งปันไฟล์ต่อไปนี้:

- CIFS - Common Internet File System:
  - ป้อน URL ที่ค้นหาไฟล์ในระบบระยะไกล
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง
  - ป้อนข้อมูลประจำตัวที่จำเป็นสำหรับ XClarity Controller เพื่อเข้าถึงไฟล์ในระบบระยะไกล

    หมายเหตุ: XClarity Controller ไม่รองรับช่องว่างในชื่อผู้ใช้ รหัสผ่าน หรือ URL ตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์ CIFS ไม่มีข้อมูลประจำตัวสำหรับการเข้าสู่ระบบที่กำหนดค่าโดยมีช่องว่างในชื่อผู้ใช้หรือรหัสผ่าน และ URL ไม่มีช่องว่าง
  - ตัวเลือกการเมาท์จะมีหรือไม่ก็ได้ และกำหนดโดยโปรโตคอล CIFS
  - หากเซิร์ฟเวอร์ระยะไกลอยู่ในคอลเลกชันของเซิร์ฟเวอร์ ซึ่งมีการจัดการการรักษาความปลอดภัยจากส่วนกลาง ให้ป้อนชื่อโดเมนที่มีเซิร์ฟเวอร์ระยะไกลอยู่
- NFS - Network File System:
  - ป้อน URL ที่ค้นหาไฟล์ในระบบระยะไกล
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง
  - ตัวเลือกการเมาท์จะมีหรือไม่ก็ได้ และกำหนดโดยโปรโตคอล NFS รองรับทั้ง NFSv3 และ NFSv4 ตัวอย่างเช่น หากต้องการใช้ NFSv3 คุณจะต้องระบุตัวเลือกเป็น ‘nfsvers=3’ หากเซิร์ฟเวอร์ NFS ใช้ลักษณะเฉพาะด้านการรักษาความปลอดภัย AUTH_SYS เพื่อตรวจสอบยืนยันการดำเนินการ NFS คุณต้องระบุตัวเลือก ‘sec=sys’
- HTTPFS – HTTP Fuse-based File System:
  - ป้อน URL ที่ค้นหาไฟล์ในระบบระยะไกล
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง

  หมายเหตุ: อาจมีข้อผิดพลาดเกิดขึ้นระหว่างขั้นตอนการติดตั้ง สำหรับใบรับรองการรักษาความปลอดภัยที่สร้างโดย Microsoft IIS หากเกิดกรณีนี้ โปรดดู “ปัญหาข้อผิดพลาดการติดตั้งสื่อ” บนหน้าที่ 114

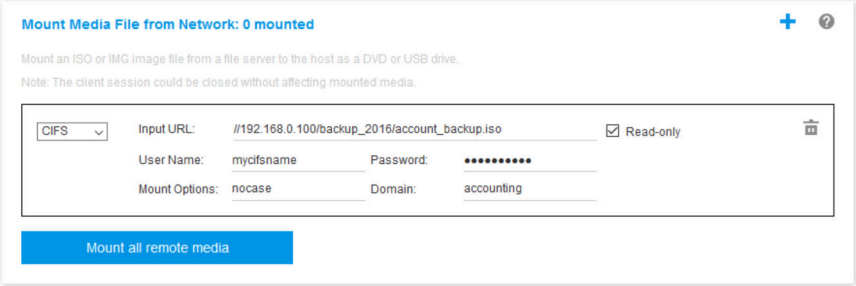
คลิก **เมาท์สื่อระยะไกลทั้งหมด** เพื่อเมาท์ไฟล์เป็นสื่อเสมือน ในการถอดสื่อเสมือน ให้คลิกไอคอนถังขยะทางด้านขวาของสื่อที่เมาท์

- สามารถอัปโหลดไฟล์ลงในหน่วยความจำของ XClarity Controller ได้สูงสุดสองไฟล์ และเมาท์เป็นสื่อเสมือนโดยใช้คุณลักษณะ RDOC ของ XClarity Controller ขนาดรวมของไฟล์ทั้งสองไฟล์ต้องไม่เกิน 50 MB ไฟล์เหล่านี้จะอยู่ในหน่วยความจำ XClarity Controller จนกว่าจะถูกลบออก แม้ว่าจะสิ้นสุดเซสชันการควบคุมจากระยะไกลแล้วก็ตาม คุณลักษณะ RDOC รองรับกลไกดังต่อไปนี้เมื่ออัปโหลดไฟล์:

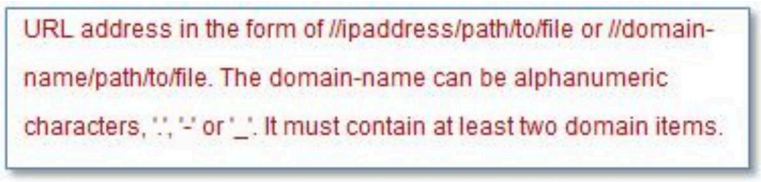
  – CIFS - Common Internet File System: ดูคำอธิบายด้านบนเพื่อดูรายละเอียด

    ตัวอย่าง:

    หากต้องการติดตั้งไฟล์ ISO ที่ชื่อ account_backup.iso ที่อยู่ภายในไดเร็กทอรี backup_2016 ของเซิร์ฟเวอร์ CIFS ที่ที่อยู่ IP 192.168.0.100 เป็นไดรฟ์เสมือนแบบอ่านอย่างเดียวไปยังเซิร์ฟเวอร์ คุณจะต้องป้อนข้อมูลลงในฟิลด์ตามที่แสดงในภาพประกอบด้านล่าง ในตัวอย่างนี้ เซิร์ฟเวอร์ซึ่งตั้งอยู่ที่ 192.168.0.100 เป็นสมาชิกของคอลเล็กชันเซิร์ฟเวอร์ภายใต้โดเมนชื่อ “accounting” ชื่อโดเมนเป็นตัวเลือกเสริม หากเซิร์ฟเวอร์ CIFS ของคุณไม่ได้เป็นส่วนหนึ่งของโดเมน ให้เว้นว่างในฟิลด์ Domain ตัวเลือกการติดตั้ง CIFS แบบ “nocase” ซึ่งมีการระบุไว้ภายในฟิลด์ Mount Options ในตัวอย่างนี้ ระบุให้เซิร์ฟเวอร์ละเว้นการตรวจสอบตัวพิมพ์เล็ก/ใหญ่สำหรับชื่อไฟล์ ฟิลด์ Mount Options เป็นตัวเลือกเสริม ข้อมูลที่ป้อนลงในฟิลด์นี้โดยผู้ใช้จะไม่ถูกใช้งานโดย BMC และจะถูกส่งผ่านไปยังเซิร์ฟเวอร์ CIFS เมื่อมีการยื่นขอติดตั้งสื่อ โปรดดูเอกสารสำหรับการใช้งานเซิร์ฟเวอร์ CIFS ของคุณ เพื่อตรวจสอบว่าเซิร์ฟเวอร์ CIFS ของคุณรองรับตัวเลือกใดบ้าง

    BMC จะให้คำแนะนำเมื่อทำการระบุ URL หาก URL ที่ป้อนไม่ถูกต้อง ปุ่มการติดตั้งจะแสดงเป็นสีเทา และจะมีข้อความสีแดงปรากฏด้านล่างของฟิลด์ URL เพื่อแสดงรูปแบบการป้อนค่า URL ที่ระบบต้องการ

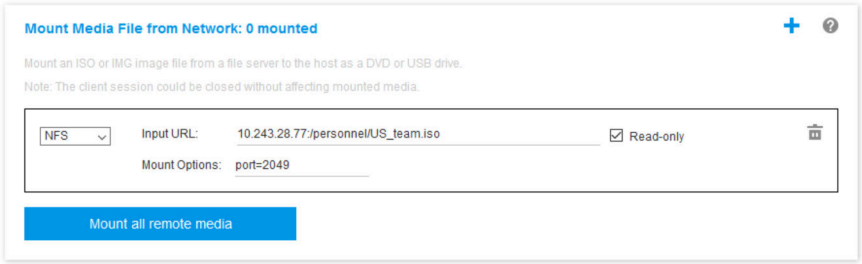
    

  – NFS - Network File System: ดูคำอธิบายด้านบนเพื่อดูรายละเอียด

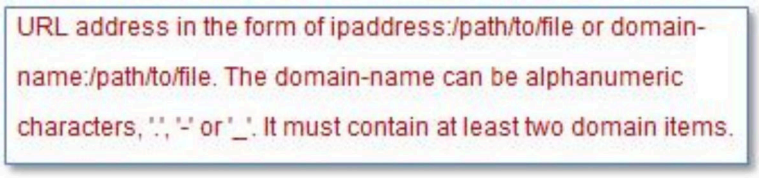
    ตัวอย่าง:

    หากต้องการติดตั้งไฟล์ ISO ชื่อ US_team.iso ที่อยู่ภายในไดเร็กทอรี่ชื่อ “personnel” ของเซิร์ฟเวอร์ NFS บนที่อยู่ IP 10.243.28.77 โดยติดตั้งเป็นไดรฟ์เสมือนแบบอ่านอย่างเดียวลงบนเซิร์ฟเวอร์ คุณจะต้องกรอกข้อมูลในฟิลด์ตามที่แสดงในตัวอย่างด้านล่าง ตัวเลือกการติดตั้ง “port=2049” ของ NFS ระบุว่าควรใช้งานพอร์ตเครือข่าย 2049 เพื่อการถ่ายโอนข้อมูล ฟิลด์ Mount Options เป็นตัวเลือกเสริม ข้อมูลที่ป้อนลงในฟิลด์นี้โดยผู้

ใช้จะถูกส่งผ่านไปยังเซิร์ฟเวอร์ NFS เมื่อมีการยื่นขอติดตั้งสื่อ โปรดดูเอกสารสำหรับการใช้งานเซิร์ฟเวอร์ NFS ของคุณ เพื่อตรวจสอบว่าเซิร์ฟเวอร์ NFS ของคุณรองรับตัวเลือกใดบ้าง



BMC จะให้คำแนะนำเมื่อทำการระบุ URL หาก URL ที่ป้อนไม่ถูกต้อง ปุ่มการติดตั้งจะแสดงเป็นสีเทา และจะมีข้อความสีแดงปรากฏด้านล่างของฟิลด์ URL เพื่อแสดงรูปแบบการป้อนค่า URL ที่ระบบต้องการ

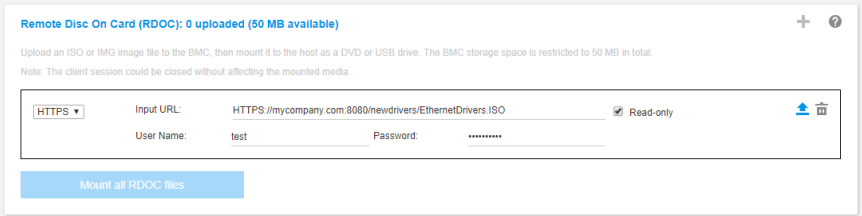


- HTTPS – Hypertext Transfer Protocol Secure:
  - ป้อน URL ที่ค้นหาไฟล์ในระบบระยะไกล
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง
  - ป้อนข้อมูลประจำตัวที่จำเป็นสำหรับ XClarity Controller เพื่อเข้าถึงไฟล์ในระบบระยะไกล

หมายเหตุ:

- อาจมีข้อผิดพลาดเกิดขึ้นระหว่างขั้นตอนการติดตั้ง สำหรับใบรับรองการรักษาความปลอดภัยที่สร้างโดย Microsoft IIS หากเกิดกรณีนี้ โปรดดู “ปัญหาข้อผิดพลาดการติดตั้งสื่อ” บนหน้าที่ 114
- XClarity Controller ไม่รองรับช่องว่างในชื่อผู้ใช้ รหัสผ่าน หรือ URL ตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์ CIFS ไม่มีข้อมูลประจำตัวสำหรับการเข้าสู่ระบบที่กำหนดค่าโดยมีช่องว่างในชื่อผู้ใช้หรือรหัสผ่าน และ URL ไม่มีช่องว่าง **ตัวอย่าง**:

  หากต้องการติดตั้งไฟล์ ISO ที่ชื่อ EthernetDrivers.ISO ที่อยู่ภายในไดเร็กทอรี “newdrivers” ของเซิร์ฟเวอร์ HTTPS ที่มีชื่อโดเมนว่า “mycompany.com” ผ่านพอร์ตเครือข่าย 8080 เป็นไดรฟ์เสมือนแบบอ่านอย่างเดียวไปยังเซิร์ฟเวอร์ คุณจะต้องป้อนข้อมูลลงในฟิลด์ตามที่แสดงในภาพประกอบด้านล่าง



BMC จะให้คำแนะนำเมื่อทำการระบุ URL หาก URL ที่ป้อนไม่ถูกต้อง ปุ่มการติดตั้งจะแสดงเป็นสีเทา และจะมีข้อความสีแดงปรากฏด้านล่างของฟิลด์ URL เพื่อแสดงรูปแบบการป้อนค่า URL ที่ระบบต้องการ

URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- SFTP – SSH File Transfer Protocol
  - ป้อน URL ที่ค้นหาไฟล์ในระบบระยะไกล
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง
  - ป้อนข้อมูลประจำตัวที่จำเป็นสำหรับ XClarity Controller เพื่อเข้าถึงไฟล์ในระบบระยะไกล

  หมายเหตุ:

  - XClarity Controller ไม่รองรับช่องว่างในชื่อผู้ใช้ รหัสผ่าน หรือ URL ตรวจสอบให้แน่ใจว่าเซิร์ฟเวอร์ CIFS ไม่มีข้อมูลประจำตัวสำหรับการเข้าสู่ระบบที่กำหนดค่าโดยมีช่องว่างในชื่อผู้ใช้หรือรหัสผ่าน และ URL ไม่มีช่องว่าง
  - เมื่อ XClarity Controller เชื่อมต่อกับเซิร์ฟเวอร์ HTTPS หน้าต่างป็อปอัปจะปรากฏพร้อมแสดงข้อมูลของใบรับรองด้านความปลอดภัยที่ใช้โดยเซิร์ฟเวอร์ HTTPS XClarity Controller ไม่สามารถตรวจสอบความถูกต้องของใบรับรองด้านความปลอดภัย
- LOCAL - Common Internet File System:
  - เรียกดูระบบของคุณเพื่อหาไฟล์ ISO หรือ IMG ที่คุณต้องการเมาท์
  - หากคุณต้องการให้ไฟล์ปรากฏต่อเซิร์ฟเวอร์เป็นสื่อเสมือนแบบอ่านอย่างเดียว ให้ทำเครื่องหมายลงในกล่อง

คลิก **เมาท์ไฟล์** RDOC **ทั้งหมด** เพื่อเมาท์ไฟล์เป็นสื่อเสมือน หากต้องการถอดสื่อแบบเสมือนออก ให้คลิกที่ไอคอนถังขยะทางด้านขวาของสื่อที่ติดตั้งอยู่

เครื่องมือแบบสแตนด์อโลน

สำหรับผู้ใช้ที่ต้องการเมาท์อุปกรณ์หรืออิมเมจ (.iso/.img) โดยใช้ XClarity Controller ผู้ใช้สามารถใช้ส่วนรหัสแบบสแตนด์อโลน rdmount ของแพ็กเกจ OneCLI ได้ rdmount จะเปิดการเชื่อมต่อกับ XClarity Controller และจะเมาท์อุปกรณ์หรืออิมเมจไปยังโฮสต์

rdmount มีรูปแบบคำสั่งต่อไปนี้:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

ตัวอย่างในการเมาท์ไฟล์ iso:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

ดิสก์ระยะไกลโดยใช้ไคลเอ็นต์ Java

ส่วนนี้จะอธิบายวิธีการเมาท์สื่อภายในโดยใช้ไคลเอ็นต์ Java

คุณสามารถใช้ไคลเอ็นต์ Java เพื่อกำหนดให้กับไดรฟ์ CD หรือ DVD ไดรฟ์ดิสก์ แฟลชไดรฟ์ USB ที่อยู่บนคอมพิวเตอร์หรือคุณสามารถระบุดิสก์อิมเมจบนคอมพิวเตอร์เพื่อเซิร์ฟเวอร์ใช้งาน คุณสามารถใช้ไดรฟ์สำหรับฟังก์ชันต่างๆ เช่น การรีสตาร์ท (บูต) เซิร์ฟเวอร์ การอัปเดตรหัส การติดตั้งซอฟต์แวร์ใหม่บนเซิร์ฟเวอร์ และการติดตั้งหรืออัปเดตระบบปฏิบัติการบนเซิร์ฟเวอร์ คุณสามารถเข้าถึงดิสก์ระยะไกลได้ ไดรฟ์และดิสก์อิมเมจจะแสดงเป็นไดรฟ์ USB บนเซิร์ฟเวอร์

หมายเหตุ: Java คอนโซลระยะไกลรองรับสภาพแวดล้อมแบบ Java อย่างใดอย่างหนึ่งต่อไปนี้ และสามารถเปิดได้เฉพาะในกรณีที่ไคลเอนต์ HTML5 ไม่ได้ทำงานอยู่เท่านั้น

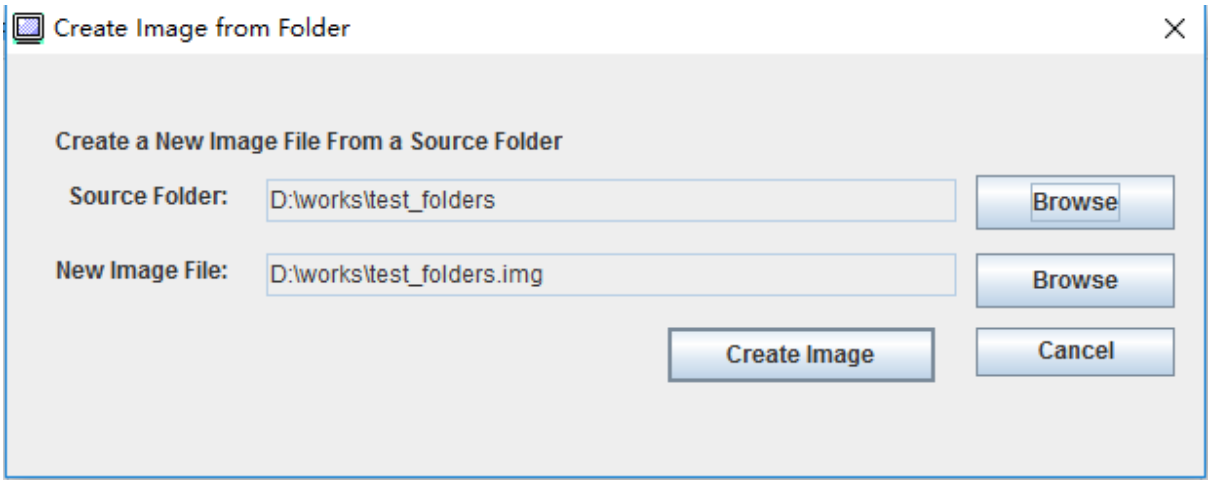
1. สภาพแวดล้อมรันไทม์ของ Oracle Java 1.8/Java SE 8 หรือเวอร์ชันที่ใหม่กว่า
2. รองรับ OpenJDK 8. Distribution of AdoptOpenJDK ที่มี HotSpot JVM

หากคุณใช้ AdoptOpenJDK คุณต้องใช้ https://openwebstart.com/ ภายใต้ OSX, Windows และ Linux

การสร้างไฟล์อิมเมจ

หากต้องการสร้างไฟล์อิมเมจใหม่จากโฟลเดอร์ต้นทางที่ระบุ ให้ทำตามขั้นตอนต่อไปนี้:

1. คลิกตัวเลือก **สร้างอิมเมจ** ภายใต้แท็บ **สื่อเสมือน** ในหน้าต่าง Virtual Media Java Client หน้าต่างสร้างอิมเมจจากโฟลเดอร์จะปรากฏขึ้น
2. คลิกปุ่ม **เรียกดู** ที่เกี่ยวข้องกับฟิลด์ **โฟลเดอร์ต้นทาง** เพื่อเลือกโฟลเดอร์ต้นทาง
3. คลิกปุ่ม **เรียกดู** ที่เกี่ยวข้องกับฟิลด์ **ไฟล์อิมเมจใหม่** เพื่อเลือกไฟล์อิมเมจที่จะใช้
4. คลิกปุ่ม **สร้างอิมเมจ**

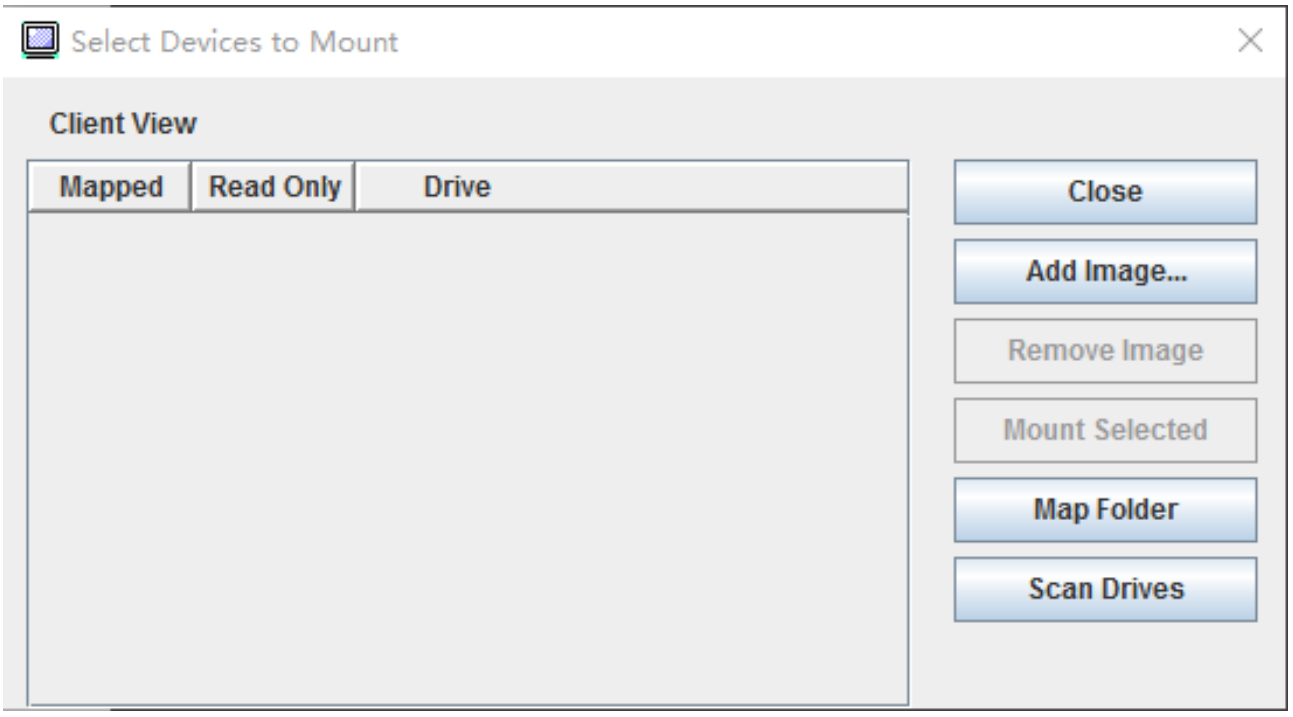


รูปภาพ 1. การสร้างไฟล์อิมเมจ

การเลือกอุปกรณ์ที่จะเมาท์

หากต้องการเมาท์อิมเมจ โฟลเดอร์ และไดรฟ์ CD/DVD/USB ภายในเครื่อง ให้ทำตามขั้นตอนต่อไปนี้:

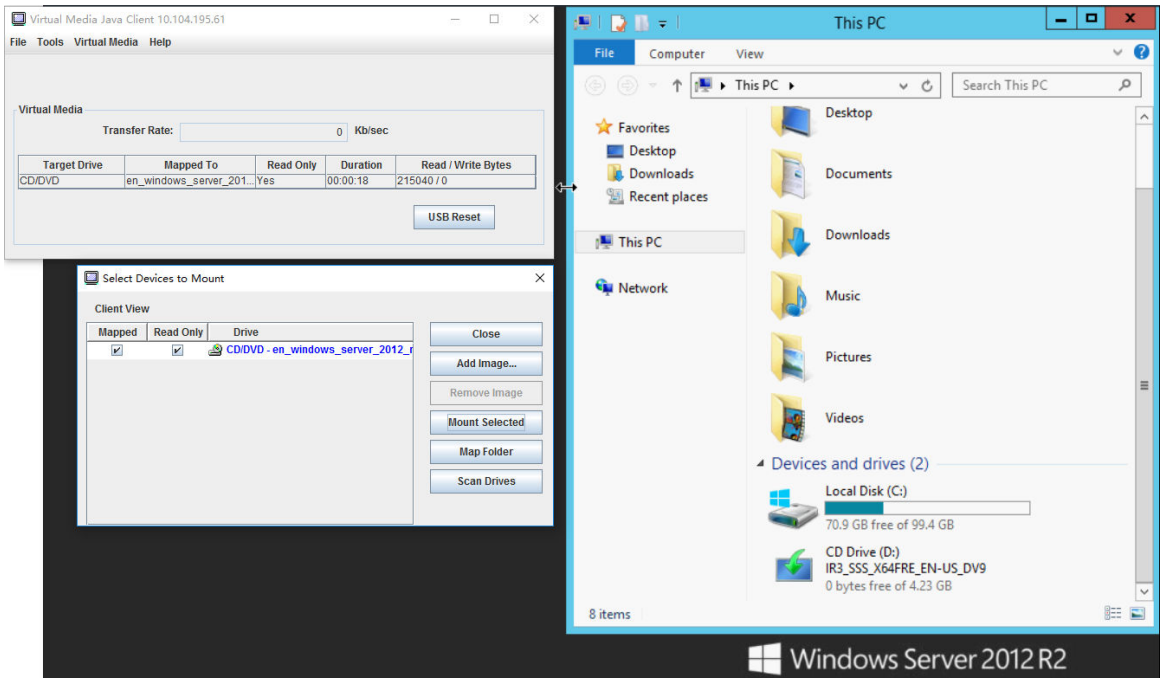
คลิกตัวเลือก **เลือกอุปกรณ์ที่จะเมาท์** ภายใต้แท็บ **สื่อเสมือน** ในหน้าต่าง Virtual Media Java Client หน้าต่างเลือกอุปกรณ์ที่จะเมาท์จะปรากฏขึ้น



รูปภาพ 2. หน้าต่างเลือกอุปกรณ์ที่จะเมาท์

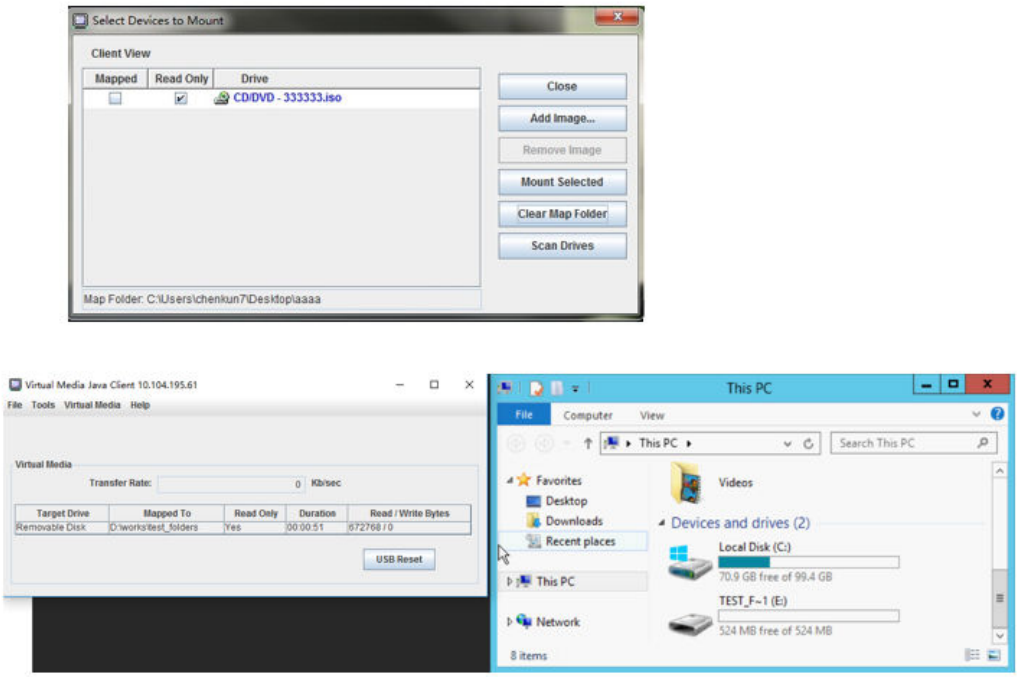
คุณสามารถเมาท์อิมเมจ โฟลเดอร์ และไดรฟ์ CD/DVD/USB ภายในเครื่องได้โดยทำตามขั้นตอนต่อไปนี้:

- **เมาท์อิมเมจภายในเครื่อง**:
    1. คลิกปุ่ม **เพิ่มอิมเมจ** เพื่อเลือกอิมเมจที่คุณต้องการเมาท์
    2. ตรวจสอบตัวเลือก**แม็ป**
    3. ตรวจสอบตัวเลือก**อ่านอย่างเดียว**เพื่อเปิดใช้งานฟังก์ชัน หากจำเป็น
    4. คลิกปุ่ม **เมาท์รายการที่เลือก** และคุณจะเมาท์อิมเมจภายในเครื่องได้สำเร็จ



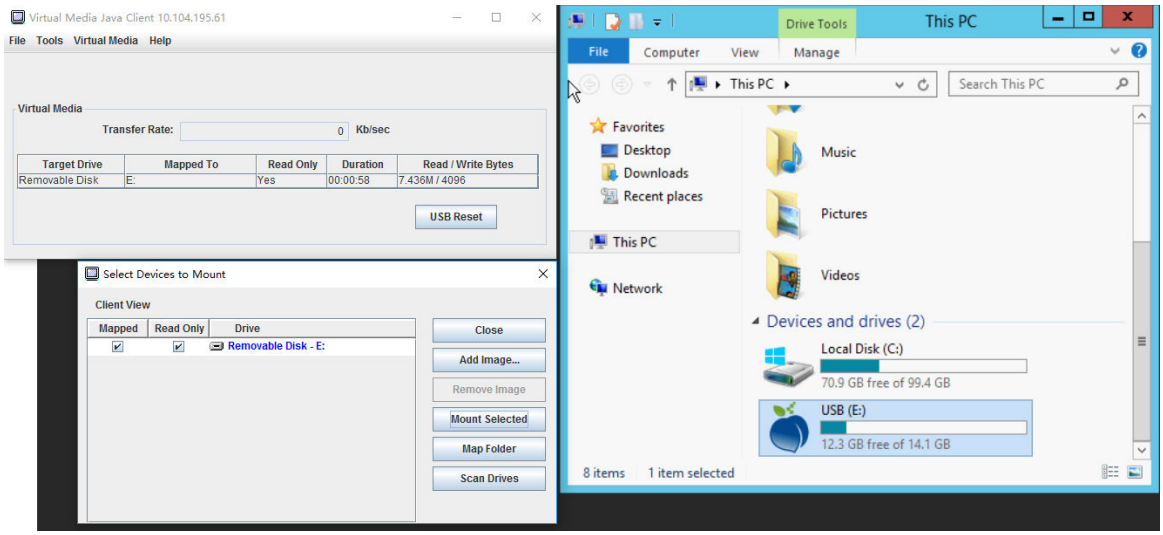
รูปภาพ 3. เมาท์อิมเมจภายในเครื่อง

- **เมาท์โฟลเดอร์ภายในเครื่อง**:
    1. คลิกปุ่ม **แม็ปโฟลเดอร์** เพื่อเลือกโฟลเดอร์ภายในเครื่องที่คุณต้องการเมาท์
    2. คลิกปุ่ม **เมาท์รายการที่เลือก** และคุณจะเมาท์โฟลเดอร์ภายในเครื่องเครื่องได้สำเร็จ



รูปภาพ 4. เมาท์โฟลเดอร์ภายในเครื่อง

- **เมาท์** CD/DVD **หรือไดรฟ์** USB:
  1. คลิกปุ่ม **สแกนไดรฟ์** เพื่อตรวจหา CD/DVD หรือไดรฟ์ USB Drive ที่เสียบอยู่
  2. ตรวจสอบตัวเลือก**แม็ป**
  3. ตรวจสอบตัวเลือก**อ่านอย่างเดียว**เพื่อเปิดใช้งานฟังก์ชัน หากจำเป็น
  4. คลิกปุ่ม **เมาท์รายการที่เลือก** และคุณจะเมาท์อิมเมจภายในเครื่องได้สำเร็จ



รูปภาพ 5. เมาท์ CD/DVD หรือไดรฟ์ USB

หน้าต่างเลือกอุปกรณ์ที่จะเมาท์แสดงรายการอุปกรณ์ภายในเครื่องปัจจุบันที่พร้อมใช้งานสำหรับการเมาท์ หน้าต่างนี้ประกอบด้วยฟิลด์และปุ่มต่อไปนี้:

- ฟิลด์**แม็ป**มีกล่องตัวเลือกที่ช่วยให้คุณสามารถเลือกอุปกรณ์ที่จะเมาท์หรือแม็ปได้
- ฟิลด์**อ่านอย่างเดียว**มีกล่องตัวเลือกที่ช่วยให้คุณสามารถเลือกอุปกรณ์ที่แม็ปหรือเมาท์ที่จะเป็นแบบ*อ่านอย่างเดียว*บนเซิร์ฟเวอร์โฮสต์ได้
- ฟิลด์**ไดรฟ์**มีพาธอุปกรณ์ในเครื่อง
- คลิกปุ่ม **ปิด** เพื่อปิดหน้าต่างเลือกอุปกรณ์ที่จะเมาท์
- คลิกปุ่ม **เพิ่มอิมเมจ** เพื่อเรียกดูดิสก์อิมเมจและไฟล์อิมเมจ ISO ในระบบไฟล์ภายในเครื่องที่คุณต้องการเพิ่มลงในรายการอุปกรณ์
- คลิกปุ่ม **ลบอิมเมจ** เพื่อลบอิมเมจที่เคยเพิ่มลงในรายการอุปกรณ์
- คลิกปุ่ม **เมาท์รายการที่เลือก** เพื่อเมาท์หรือแม็ปอุปกรณ์ทั้งหมดที่ได้รับการตรวจสอบสำหรับการเมาท์และแม็ปในฟิลด์**แม็ป**

  หมายเหตุ: ระบบจะเมาท์โฟลเดอร์เป็นแบบอ่านอย่างเดียว
- คลิกปุ่ม **สแกนไดรฟ์** เพื่อรีเฟรชรายการอุปกรณ์ภายในเครื่อง

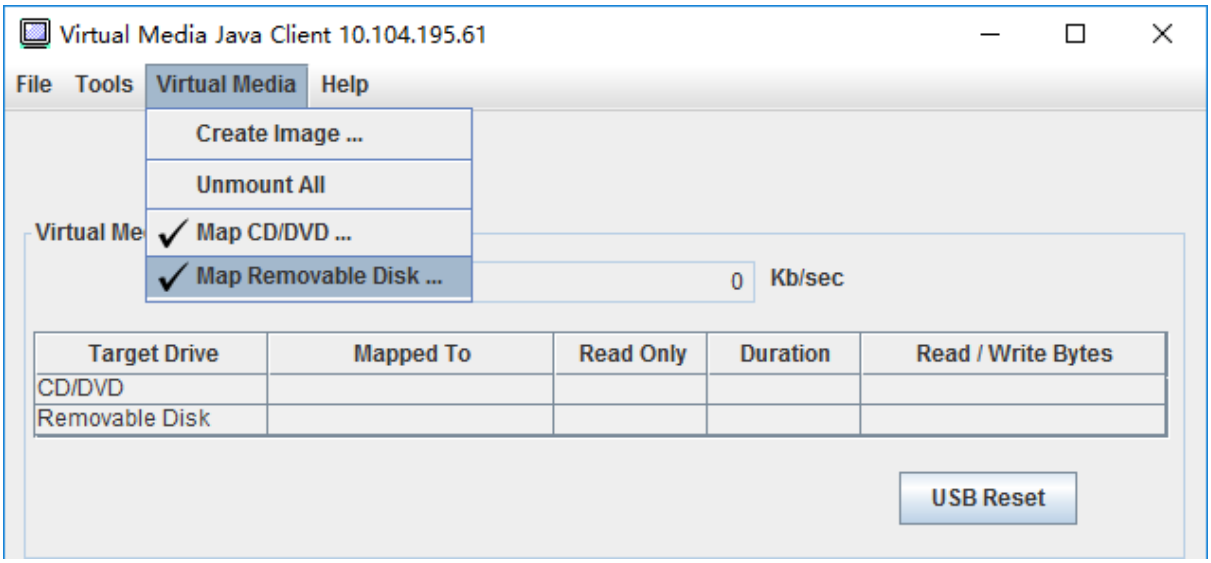
การเลือกอุปกรณ์ที่จะยกเลิกการเมาท์

หากต้องการยกเลิกการเมาท์เซิร์ฟเวอร์โฮสต์ ให้ทำตามขั้นตอนต่อไปนี้:

1. คลิกตัวเลือก **ยกเลิกการเมาท์ทั้งหมด** ภายใต้แท็บ **สื่อเสมือน** ในหน้าต่าง Virtual Media Java Client

2. หลังจากเลือกตัวเลือก **ยกเลิกการเมาท์ทั้งหมด** ระบบจะแสดงหน้าต่างยืนยันการยกเลิกการเมาท์ทั้งหมด หากคุณยอมรับ อุปกรณ์เซิร์ฟเวอร์โฮสต์*ทั้งหมด*บนเซิร์ฟเวอร์จะถูกยกเลิกการเมาท์

   หมายเหตุ: คุณไม่สามารถยกเลิกการเมาท์ของไดรฟ์ทีละตัวได้



รูปภาพ 6. ยกเลิกการเมาท์ทั้งหมด

ปัญหาข้อผิดพลาดการติดตั้งสื่อ

ใช้ข้อมูลในหัวข้อนี้เพื่อการแก้ไขปัญหาเกี่ยวกับข้อผิดพลาดในการติดตั้งสื่อ

เมื่อใช้งานใบรับรองการรักษาความปลอดภัยที่สร้างโดย Microsoft IIS คุณอาจพบข้อผิดพลาดระหว่างขั้นตอนการติดตั้งได้ หากเกิดเหตุการณ์เช่นนี้ ให้แทนที่ใบรับรองการรักษาความปลอดภัยด้วยใบรับรองใหม่ที่สร้างโดย openssl แทน ไฟล์ pfx ที่สร้างขึ้นใหม่จะถูกโหลดลงในเซิร์ฟเวอร์ Microsoft IIS โดยเฉพาะ

ด้านล่างคือตัวอย่างซึ่งแสดงวิธีการสร้างใบรับรองการรักษาความปลอดภัยใหม่ด้วย openssl ภายในระบบปฏิบัติการ Linux

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
```

```
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

การออกจากเซสชันคอนโซลระยะไกล

หัวข้อนี้จะอธิบายวิธีสิ้นสุดเซสชันคอนโซลระยะไกล

หากต้องการออกจากเซสชันคอนโซลระยะไกล ให้ปิดหน้าต่างคอนโซลระยะไกลและสื่อเสมือน

บันทึกของการดาวน์โหลดข้อมูลบริการ

ใช้ข้อมูลในหัวข้อนี้ในการรวบรวมข้อมูลบริการเกี่ยวกับเซิร์ฟเวอร์ของคุณ โดยปกติแล้ว กระบวนการนี้จะดำเนินการตามคำขอของผู้ให้บริการเพื่อแก้ไขปัญหาของเซิร์ฟเวอร์

ในหน้าแรกของ XClarity Controller ให้คลิกตัวเลือก **บันทึกของบริการ** ในส่วน **การดำเนินการด่วน** และเลือก **บันทึกของข้อมูลบริการ**

ตามค่าเริ่มต้น บันทึกของบริการจะมีข้อมูลต่อไปนี้: ข้อมูลระบบ, คลังของระบบ, การใช้งานระบบ, ตาราง SMBIOS, การอ่านเซ็นเซอร์, บันทึกเหตุการณ์, คีย์ FOD, คีย์ SLP, การกำหนดค่า UEFI และการกำหนดค่า XClarity Controller 2

ผู้ใช้สามารถวางเมาส์เหนือตัวเลือกข้อมูลพื้นฐานและคลิกที่หน้าต่างลอยเพื่อดูข้อมูลจริงที่จะส่งออก

แม้ว่าข้อมูลพื้นฐานจะเป็นข้อมูลที่จำเป็นต้องมี ผู้ใช้มีตัวเลือกในการส่งออกข้อมูลต่อไปนี้:

- ข้อมูลเครือข่าย (IP, ชื่อโฮสต์)
- การวัดและส่งข้อมูลทางไกล (ข้อมูลตลอด 24 ชั่วโมง)
- บันทึกการตรวจสอบ (มีชื่อผู้ใช้)
- หน้าจอความบกพร่องล่าสุด

คลิก **ส่งออก** เพื่อดาวน์โหลดบันทึกของข้อมูลบริการ

กระบวนการของการรวบรวมข้อมูลบริการและการสนับสนุนอาจใช้เวลาสองถึงสามนาทีเพื่อดำเนินการให้เสร็จสมบูรณ์ ไฟล์จะได้รับการบันทึกไปยังโฟลเดอร์การดาวน์โหลดเริ่มต้นของคุณ ข้อตกลงการตั้งชื่อสำหรับไฟล์ข้อมูลบริการจะเป็นไปตามข้อตกลงนี้:`<machine type and model>_<serial number>_xcc_mini-log_<date>-<time>.zip`

ตัวอย่างเช่น: 7X2106Z01A_2345678_xcc_mini-log_170511-175656.zip

นอกเหนือจากรูปแบบ zip แล้ว คุณยังสามารถดาวน์โหลดข้อมูลการซ่อมบำรุงได้โดยใช้รูปแบบ tzz ผ่าน **เรียกดูประวัติ**... tzz ใช้เวลาในการเตรียมพร้อม ดังนั้นจะไม่ปรากฏขึ้นทันทีหลังจากส่งออกไฟล์ zip Tzz ใช้อัลกอริธึมการบีบอัดที่แตกต่างกันและสามารถแยกได้ด้วยยูทิลิตี เช่น “Izop”

เรียกดูประวัติ... จะเก็บบันทึกของบริการที่ส่งออกล่าสุดด้วย

คุณสมบัติของเซิร์ฟเวอร์

ใช้ข้อมูลในหัวข้อนี้เพื่อเปลี่ยนแปลงหรือดูคุณสมบัติของเซิร์ฟเวอร์ที่เกี่ยวข้อง

การตั้งค่าตำแหน่งที่ตั้งและที่ติดต่อ

ใช้ข้อมูลในหัวข้อนี้ในการตั้งค่าพารามิเตอร์ต่างๆ เพื่อช่วยระบุระบบสำหรับเจ้าหน้าที่ฝ่ายปฏิบัติการและสนับสนุน

เลือก **คุณสมบัติของเซิร์ฟเวอร์** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** เพื่อกำหนดค่าข้อมูล **ตำแหน่งที่ตั้งและที่ติดต่อ**

ที่ติดต่อ

ทำให้คุณสามารถระบุชื่อและหมายเลขโทรศัพท์ของบุคคลที่ควรติดต่อหากระบบประสบปัญหา

หมายเหตุ: ฟิลด์นี้เหมือนกับฟิลด์ที่ติดต่อในการกำหนดค่า SNMPv3 และจำเป็นต้องมีเพื่อเปิดใช้งาน SNMPv3

ชื่อแร็ค

ทำให้คุณสามารถค้นหาตำแหน่งเซิร์ฟเวอร์ได้ง่ายดายยิ่งขึ้นโดยระบุแร็คที่มีเซิร์ฟเวอร์อยู่

หมายเหตุ: ฟิลด์นี้จะระบุหรือไม่ก็ได้ และกำหนดค่าไม่ได้ในโหนด Flex

หมายเลขห้อง

ทำให้คุณสามารถค้นหาตำแหน่งเซิร์ฟเวอร์ได้ง่ายดายยิ่งขึ้นโดยระบุห้องที่มีเซิร์ฟเวอร์อยู่

อาคาร

ทำให้คุณสามารถค้นหาตำแหน่งเซิร์ฟเวอร์ได้ง่ายดายยิ่งขึ้นโดยระบุอาคารที่มีเซิร์ฟเวอร์อยู่

U ต่ำสุด

ทำให้คุณสามารถค้นหาตำแหน่งเซิร์ฟเวอร์ได้ง่ายดายยิ่งขึ้นโดยระบุตำแหน่งในแร็ค

หมายเหตุ: ฟิลด์นี้จะระบุหรือไม่ก็ได้ และกำหนดค่าไม่ได้ในโหนด Flex

ที่อยู่

ทำให้คุณสามารถระบุที่อยู่สำหรับส่งไปรษณีย์แบบเต็มที่มีเซิร์ฟเวอร์อยู่

หมายเหตุ: เมื่อมีการป้อนข้อมูลที่เกี่ยวข้องแล้ว ข้อมูลจะปรากฏแบบบรรทัดเดียวในฟิลด์ **ตำแหน่งที่ตั้ง** ในส่วน SNMPv3 และหน้าแรกของ XClarity Controller

การตั้งค่าการหมดเวลาของเซิร์ฟเวอร์

ใช้ข้อมูลในหัวข้อนี้ในการตั้งค่าเวลาใช้งานเซิร์ฟเวอร์

เวลาใช้งานเหล่านี้ใช้เพื่อคืนค่าการทำงานให้กับเซิร์ฟเวอร์ที่มีอาการค้าง

เลือก **คุณสมบัติของเซิร์ฟเวอร์** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** เพื่อกำหนดค่าเวลาใช้งานเซิร์ฟเวอร์ มีการเลือกเวลาใช้งานเซิร์ฟเวอร์ ดังต่อไปนี้:

OS Watchdog

OS Watchdog ใช้ในการตรวจสอบระบบปฏิบัติการเพื่อให้แน่ใจว่าระบบไม่มีอาการค้าง ต้องเปิดใช้งานอินเทอร์เฟซ Ethernet over USB สำหรับคุณลักษณะนี้ ดูรายละเอียดได้ที่ “การกำหนดค่า Ethernet over USB” บนหน้าที่ 44 XClarity Controller จะติดต่อระบบปฏิบัติการตามช่วงเวลาที่กำหนดค่าในการเลือก **เวลา OS Watchdog** หากระบบปฏิบัติการไม่ตอบสนองก่อนถึงเวลาการตรวจสอบครั้งถัดไป XClarity Controller จะถือว่าระบบปฏิบัติการมีอาการค้าง XClarity Controller จะจับภาพหน้าจอเนื้อหาของเซิร์ฟเวอร์ แล้วรีบูตเซิร์ฟเวอร์เพื่อพยายามคืนค่าการทำงาน XClarity Controller จะรีบูตเซิร์ฟเวอร์เพียงครั้งเดียวเท่านั้น หากระบบปฏิบัติการยังมีอาการค้างอยู่หลังจากรีบูต แทนที่จะดำเนินการรีบูตเซิร์ฟเวอร์ต่อไป เซิร์ฟเวอร์จะถูกปล่อยให้อยู่ในอาการค้างเพื่อให้สามารถดำเนินการตรวจสอบและแก้ไขปัญหาได้ ในการทำให้ OS watchdog กลับมาทำงานอีกครั้ง ให้ปิดแล้วเปิดเซิร์ฟเวอร์ ในการเปิดใช้งาน OS watchdog ให้เลือกช่วงเวลาจากรายการดรอปดาวน์ของเวลา OS Watchdog และคลิก **นำไปใช้** ในการปิดใช้งาน OS watchdog ให้เลือก **ไม่มี** บนเมนูดรอปดาวน์ของเวลา OS Watchdog

โปรแกรมเฝ้าระวังตัวโหลด

โปรแกรมเฝ้าระวังตัวโหลดจะตรวจสอบช่วงเวลาระหว่างความเสร็จสมบูรณ์ของ POST และขณะที่ระบบปฏิบัติการกำลังทำงานอยู่ ต้องเปิดใช้งานอินเทอร์เฟซ Ethernet over USB สำหรับคุณลักษณะนี้ ดูรายละเอียดได้ที่ “การกำหนดค่า Ethernet over USB” บนหน้าที่ 44 เมื่อ POST ดำเนินการเสร็จสมบูรณ์ XClarity Controller จะเริ่มตัวจับเวลา และเริ่มต้นติดต่อระบบปฏิบัติการ หากระบบปฏิบัติการไม่ตอบสนองตามเวลาที่กำหนดค่าไว้ในการเลือกของโปรแกรมเฝ้าระวังตัวโหลด XClarity Controller จะถือว่าการบูตระบบปฏิบัติการมีอาการค้าง แล้ว XClarity Controller จะรีบูตเซิร์ฟเวอร์เพื่อพยายามคืนค่าการทำงาน XClarity Controller จะรีบูตเซิร์ฟเวอร์เพียงครั้งเดียวเท่านั้น หากการบูตระบบปฏิบัติการยังมีอาการค้างอยู่หลังจากรีบูต แทนที่จะดำเนินการรีบูตเซิร์ฟเวอร์ต่อไป เซิร์ฟเวอร์จะถูกปล่อยให้อยู่ในอาการค้างเพื่อให้สามารถดำเนินการตรวจสอบและแก้ไขปัญหาได้ โปรแกรมเฝ้าระวังตัวโหลดจะกลับมาทำงานอีกครั้งเมื่อปิดแล้วเปิดเซิร์ฟเวอร์ หรือเมื่อเซิร์ฟเวอร์บูตไปยังระบบปฏิบัติการสำเร็จ ในการเปิดใช้งานโปรแกรมเฝ้าระวังตัวโหลด ให้เลือกช่วงเวลาจากรายการดรอปดาวน์ของโปรแกรมเฝ้าระวังตัวโหลด และคลิก **นำไปใช้** ในการปิดใช้งานโปรแกรมเฝ้าระวังตัวโหลด ให้เลือก **ไม่มี** บนรายการดรอปดาวน์ของโปรแกรมเฝ้าระวังตัวโหลด

เปิดใช้งานการหน่วงเวลาปิดเครื่อง

ใช้ฟิลด์การหน่วงเวลาปิดเครื่องเพื่อระบุระยะเวลาเป็นนาทีที่ระบบย่อยของ XClarity Controller จะรอให้ระบบปฏิบัติการปิดเองก่อนที่จะบังคับให้ปิดเครื่อง ในการตั้งค่าการหมดเวลาของการหน่วงเวลาปิดเครื่อง ให้เลือกช่วงเวลาจากรายการดรอปดาวน์และคลิก **นำไปใช้** ในการทำให้ XClarity Controller ไม่สามารถบังคับปิดเครื่องได้ ให้เลือก **ไม่มี** จากการเลือกแบบดรอปดาวน์

ข้อความการบุกรุก

ใช้ข้อมูลในหัวข้อนี้เพื่อสร้างข้อความที่จะแสดงเมื่อผู้ใช้เข้าสู่ระบบ XClarity Controller

เลือก **คุณสมบัติของเซิร์ฟเวอร์** ภายใต้ **การกำหนดค่าเซิร์ฟเวอร์** ใช้ตัวเลือก **ข้อความการบุกรุก** เพื่อกำหนดค่าข้อความที่คุณต้องการแสดงต่อผู้ใช้ เมื่อดำเนินการเสร็จแล้ว ให้คลิก **นำไปใช้**

ข้อความจะแสดงขึ้นในพื้นที่ข้อความของหน้าการเข้าสู่ระบบ XClarity Controller เมื่อผู้ใช้เข้าสู่ระบบ

การตั้งค่าวันที่และเวลาของ XClarity Controller

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจเกี่ยวกับการตั้งค่าวันที่และเวลาของ XClarity Controller มีคำแนะนำให้เพื่อกำหนดค่าวันที่และเวลาของ XClarity Controller วันที่และเวลาของ XClarity Controller จะใช้เพื่อประทับเวลาเหตุการณ์ทั้งหมดที่ถูกบันทึกไว้ในบันทึกเหตุการณ์ และการแจ้งเตือนที่ถูกส่ง

ที่หน้าแรกของ XClarity Controller ให้คลิกไอคอนนาฬิกาที่มุมบนขวาเพื่อดูหรือเปลี่ยนวันที่และเวลาของ XClarity Controller XClarity Controller ไม่มีนาฬิกาแบบเรียลไทม์ของตนเอง คุณสามารถกำหนดค่า XClarity Controller ให้ซิงค์เวลาและวันที่กับเซิร์ฟเวอร์โปรโตคอลเวลาของเครือข่าย หรือซิงค์กับฮาร์ดแวร์นาฬิกาแบบเรียลไทม์ของเซิร์ฟเวอร์

การซิงค์กับ NTP

ดำเนินการขั้นตอนต่อไปนี้เพื่อซิงโครไนซ์นาฬิกาของ XClarity Controller กับเซิร์ฟเวอร์ NTP

- เลือก **ซิงค์เวลากับ NTP** และระบุที่อยู่เซิร์ฟเวอร์ NTP
- สามารถระบุเซิร์ฟเวอร์ NTP เพิ่มเติมโดยคลิกไอคอน “+”
- ระบุความถี่ที่คุณต้องการให้ XClarity Controller ซิงค์กับเซิร์ฟเวอร์ NTP
- เวลาที่ได้รับจากเซิร์ฟเวอร์ NTP จะอยู่ในรูปแบบเวลามาตรฐานสากล (UTC)
  - หากคุณต้องการให้ XClarity Controller ปรับเวลาและวันที่สำหรับภูมิภาคท้องถิ่นของคุณ ให้เลือกค่าชดเชยโซนเวลาสำหรับตำแหน่งกระทำการของคุณจากเมนูดรอปดาวน์
  - หากที่ตั้งของคุณเป็นไปตามเวลาออมแสง ให้ทำเครื่องหมายในกล่องตัวเลือก **ปรับเป็นเวลาออมแสง** (DST) **โดยอัตโนมัติ**
- เมื่อเปลี่ยนแปลงการกำหนดค่าเสร็จสิ้นแล้ว ให้คลิก **นำไปใช้**

การซิงค์กับโฮสต์

เวลาที่เก็บไว้ในฮาร์ดแวร์นาฬิกาแบบเรียลไทม์ของเซิร์ฟเวอร์อาจอยู่ในรูปแบบเวลามาตรฐานสากล (UTC) หรืออาจมีการปรับและจัดเก็บไว้ในรูปแบบเวลาท้องถิ่น ระบบปฏิบัติการบางระบบจัดเก็บนาฬิกาแบบเรียลไทม์ในรูปแบบ UTC ขณะที่ระบบอื่นๆ จัดเก็บเวลาเป็นเวลาท้องถิ่น นาฬิกาแบบเรียลไทม์ของเซิร์ฟเวอร์ไม่ได้ระบุรูปแบบของเวลา ดังนั้น เมื่อมีการกำหนดค่าให้ XClarity Controller ซิงค์กับนาฬิกาแบบเรียลไทม์ของโฮสต์ ผู้ใช้สามารถเลือกวิธีที่ XClarity Controller ใช้เวลาและวันที่ที่รับจากนาฬิกาแบบเรียลไทม์ได้

- ท้องถิ่น (ตัวอย่าง: Windows): ในโหมดนี้ XClarity Controller จะพิจารณาว่าเวลาและวันที่ที่รับมาจากนาฬิกาแบบเรียลไทม์เป็นเวลาท้องถิ่น ซึ่งมีการนำค่าชดเชยโซนเวลาและค่าชดเชย DST ที่เกี่ยวข้องไปใช้แล้ว

- UTC (ตัวอย่าง: Linux): ในโหมดนี้ XClarity Controller จะพิจารณาว่าเวลาและวันที่ที่รับมาจากนาฬิกาแบบเรียลไทม์เป็นเวลามาตรฐานสากล ซึ่งไม่มีการนำค่าชดเชยโซนเวลาและค่าชดเชย DST ที่เกี่ยวข้องไปใช้ ในโหมดนี้ คุณสามารถเลือกปรับเวลาและวันที่สำหรับภูมิภาคท้องถิ่นของคุณ โดยเลือกค่าชดเชยโซนเวลาสำหรับตำแหน่งกระทำการของคุณจากเมนูดรอปดาวน์ หากที่ตั้งของคุณเป็นไปตามเวลาออมแสง คุณยังสามารถทำเครื่องหมายในกล่องตัวเลือก **ปรับเป็นเวลาออมแสง** (DST) **โดยอัตโนมัติ**
- เมื่อเปลี่ยนแปลงการกำหนดค่าเสร็จสิ้นแล้ว ให้คลิก **นำไปใช้**

หมายเหตุ:

- เมื่อเกิดเวลาออมแสง การกระทำใดๆ ที่กำหนดเวลาไว้เพื่อให้ XClarity Controller ดำเนินการระหว่างช่วงเวลาที่นาฬิกาข้ามเวลาไปข้างหน้าจะไม่มีการดำเนินการ ตัวอย่างเช่น หากเวลาออมแสงของสหรัฐอเมริกาเริ่มต้นเวลา 2:00 น. ของวันที่ 12 มีนาคม และการดำเนินการด้านพลังงานถูกกำหนดเวลาไว้ที่ 2:10 น. ของวันที่ 12 มีนาคม การดำเนินการนี้จะไม่เกิดขึ้น เมื่อเวลาไปถึง 2:00 น. XClarity Controller จะอ่านเวลาเป็น 3:00 น. แทน
- ไม่สามารถแก้ไขการตั้งค่าเวลาและวันที่ของ XClarity Controller ใน Flex System

บทที่ 6. การกำหนดค่าที่จัดเก็บข้อมูล

ใช้ข้อมูลในหัวข้อนี้เพื่อทำความเข้าใจเกี่ยวกับตัวเลือกต่างๆ ที่ใช้ได้ในการกำหนดค่าที่จัดเก็บข้อมูล

เมื่อกำหนดค่าที่จัดเก็บข้อมูล จะสามารถใช้ตัวเลือกต่อไปนี้ได้:

- รายละเอียด
- การตั้งค่า RAID

รายละเอียด RAID

โปรดใช้ข้อมูลในหัวข้อนี้สำหรับการใช้ฟังก์ชันรายละเอียด RAID

ฟังก์ชันนี้จะแสดงโครงสร้างทางกายภาพของอุปกรณ์จัดเก็บข้อมูลและการกำหนดค่าพื้นที่จัดเก็บข้อมูล พร้อมด้วยรายละเอียด อย่างเช่น ตำแหน่ง ผู้ผลิต ชื่อผลิตภัณฑ์ สถานะ ความจุ อินเทอร์เฟซ สื่อ ฟอร์มแฟคเตอร์ และข้อมูลอื่นๆ

การตั้งค่า RAID

โปรดใช้ข้อมูลในหัวข้อนี้ หากต้องการใช้งานฟังก์ชันการตั้งค่า RAID

ใช้ข้อมูลในหัวข้อนี้เพื่อดูและกำหนดค่าพูลที่จัดเก็บ ดิสก์และไดรฟ์เสมือนที่เกี่ยวข้องสำหรับอะแดปเตอร์ RAID หากระบบปิดอยู่ ให้เปิดระบบเพื่อดูข้อมูล RAID

การดูและกำหนดค่าไดรฟ์เสมือน

ใช้ข้อมูลในหัวข้อนี้เพื่อดูและกำหนดค่าไดรฟ์เสมือน

เมื่อคุณเลือก **RAID Setup** ภายใต้ **Server Configuration** แท็บ **Array Configuration** จะถูกเลือก และดิสก์เสมือนที่มีอยู่จะแสดงตามค่าเริ่มต้น ไดรฟ์แบบลอจิคัลถูกจัดเรียงตามดิสก์อาร์เรย์และตัวควบคุม ข้อมูลโดยละเอียดเกี่ยวกับดิสก์เสมือน เช่น ขนาดการแบ่งส่วนดิสก์เสมือนและข้อมูลที่สามารถบูตได้จะปรากฏขึ้น

ในการกำหนดค่าการตั้งค่า RAID ให้คลิก **เปิดใช้งานโหมดแก้ไข**

ในโหมดแก้ไข คุณสามารถคลิกเมนูการดำเนินการของตัวควบคุม ดูดิสก์เสมือน RAID ในปัจจุบัน และสร้างดิสก์เสมือน RAID ใหม่

จากเมนูการดำเนินการของตัวควบคุม คุณสามารถดำเนินการต่อไปนี้ได้:

ล้างการกำหนดค่า RAID

ล้างการกำหนดค่าและข้อมูลทั้งหมดบนตัวควบคุมที่เลือก

จัดการการกำหนดค่าภายนอก

นำเข้าไดรฟ์ภายนอกใดๆ ที่ตรวจพบ ไดรฟ์ภายนอกเป็นไดรฟ์ที่ย้ายจากการกำหนดค่า RAID อื่นไปยังตัวควบคุม RAID ปัจจุบัน

หมายเหตุ: คุณจะได้รับแจ้ง หากตรวจไม่พบไดรฟ์ภายนอก

ข้อมูลของดิสก์เสมือน RAID ปัจจุบันสำหรับตัวควบคุมเฉพาะจะแสดงเป็น “การ์ดดิสก์เสมือน” ที่เกี่ยวข้อง แต่ละการ์ดจะแสดงข้อมูล เช่น ชื่อดิสก์เสมือน สถานะ ความจุ และการดำเนินการ ไอคอนรูปดินสอทำให้คุณสามารถแก้ไขข้อมูล และไอคอนถังขยะทำให้คุณสามารถลบ “การ์ดดิสก์เสมือน” ได้

หมายเหตุ: ไม่สามารถเปลี่ยนความจุและระดับ RAID ได้

หากคุณคลิกชื่อดิสก์เสมือน หน้าต่างคุณสมบัติของดิสก์เสมือนจะปรากฏขึ้น

ในการสร้างดิสก์เสมือน RAID ใหม่ ให้ดำเนินการตามขั้นตอนที่แสดงไว้ด้านล่าง:

หมายเหตุ: หากความจุที่จัดเก็บไม่เหลือพื้นที่ คุณจะไม่สามารถสร้างดิสก์เสมือนใหม่ได้

1. **เลือกไดรฟ์หรือดิสก์อาร์เรย์ที่มีความจุที่จัดเก็บที่ว่างอยู่**
   a. เมื่อสร้างดิสก์เสมือนในดิสก์อาร์เรย์ใหม่ คุณต้องระบุระดับ RAID หากมีไดรฟ์ให้เลือกไม่พอ และคุณคลิก **ถัดไป** ข้อความแสดงข้อผิดพลาดจะปรากฏภายใต้ฟิลด์ระดับ RAID

      สำหรับระดับ RAID บางระดับ จำเป็นต้องมีสแปน นอกจากนี้ ยังต้องมีจำนวนไดรฟ์ต่ำสุดในสแปนด้วย

      1) สำหรับประเภทของสถานการณ์เหล่านี้ เว็บอินเทอร์เฟซจะแสดง **สแปน 1** ตามค่าเริ่มต้น
      2) เลือกไดรฟ์และคลิก **เพิ่มสมาชิก** เพื่อเพิ่มไดรฟ์ไปยัง **สแปน 1** เมื่อ **สแปน 1** มีไดรฟ์ไม่พอ ให้ปิดใช้งานลิงก์ **เพิ่มสแปน**
      3) คลิก **เพิ่มสแปน** เพื่อเพิ่ม **สแปน 2** เลือกไดรฟ์และคลิก **เพิ่มสมาชิก** เพื่อเพิ่มไปยัง **สแปน 2**
      4) คลิก **เพิ่มสมาชิก** เพื่อเพิ่มไดรฟ์ไปยังสแปนล่าสุด หากคุณต้องการเพิ่มไดรฟ์ไปยัง **สแปน 1** อีกครั้ง คุณต้องคลิก สแปน 1 และเลือกไดรฟ์เพื่อเพิ่มไปยัง **สแปน 1**
      5) หากมีสแปนถึงจำนวนสูงสุดแล้ว ให้ปิดใช้งาน **เพิ่มสแปน**

   b. ในการสร้างดิสก์เสมือนในดิสก์อาร์เรย์ที่มีอยู่ คุณต้องเลือกดิสก์อาร์เรย์ที่มีความจุที่ว่างอยู่
2. **การสร้างดิสก์เสมือน**

a. ตามค่าเริ่มต้นจะสร้างดิสก์เสมือนที่ใช้ความจุที่จัดเก็บทั้งหมด ไอคอน **เพิ่ม** ถูกปิดใช้งานเมื่อมีการใช้ที่จัดเก็บทั้งหมด คุณสามารถคลิกไอคอนรูปดินสอเพื่อเปลี่ยนความจุหรือคุณสมบัติอื่นๆ

b. เมื่อคุณแก้ไขดิสก์เสมือนดิสก์แรกเพื่อให้ใช้ความจุที่จัดเก็บเฉพาะบางส่วนเท่านั้น ไอคอน **เพิ่ม** จะถูกเปิดใช้งาน คลิกไอคอนเพื่อแสดงหน้าต่าง **เพิ่มดิสก์เสมือน**

c. หากมีดิสก์เสมือนมากกว่าหนึ่งดิสก์ ไอคอน **ถอดออก** จะถูกเปิดใช้งาน ไอคอนนี้จะไม่แสดง หากมีดิสก์เสมือนเพียงดิสก์เดียว เมื่อคุณคลิกไอคอน **ถอดออก** แถวที่เลือกจะถูกลบในทันที หน้าต่างการยืนยันจะไม่ปรากฏ เนื่องจากยังไม่มีการสร้างดิสก์เสมือน

d. คลิก **เริ่มการสร้างดิสก์เสมือน** เพื่อเริ่มกระบวนการ

หมายเหตุ: เมื่อตัวควบคุมไม่ได้รับการรองรับ ข้อความจะปรากฏขึ้น

การดูและกำหนดค่ารายการที่จัดเก็บข้อมูล

ใช้ข้อมูลในหัวข้อนี้เพื่อดูและกำหนดค่ารายการที่จัดเก็บข้อมูล

ภายใต้แท็บ **รายการที่จัดเก็บข้อมูล** คุณสามารถดูและกำหนดค่าดิสก์อาร์เรย์ ไดรฟ์เสมือนที่เกี่ยวข้อง และไดรฟ์สำหรับตัวควบคุม RAID

- **สำหรับอุปกรณ์จัดเก็บที่รองรับการกำหนดค่า** RAID:
  1. หากตัวควบคุมมีดิสก์อาร์เรย์ที่กำหนดค่า ตัวควบคุมจะแสดงไดรฟ์ที่ติดตั้งตามดิสก์อาร์เรย์ ข้อมูลต่อไปนี้จะอธิบายรายการที่ปรากฏในหน้าต่าง
     - **ชื่อตาราง**: แสดง ID ดิสก์อาร์เรย์, ระดับ RAID และจำนวนของไดรฟ์ทั้งหมด
     - **สารบัญ**: แสดงรายการคุณสมบัติพื้นฐาน - ชื่อไดรฟ์, สถานะ RAID, ประเภท, หมายเลขประจำเครื่อง, หมายเลขชิ้นส่วน, หมายเลข FRU และการดำเนินการ คุณสามารถไปยังหน้า **รายการอุปกรณ์** เพื่อดูคุณสมบัติทั้งหมดที่ XClarity Controller สามารถตรวจหาได้
     - **การดำเนินการ**: ข้อมูลต่อไปนี้แสดงรายการการดำเนินการที่สามารถทำได้ การดำเนินการบางอย่างจะไม่พร้อมใช้งานเมื่อไดรฟ์อยู่ในสถานะอื่น
       - **กำหนด Hot Spare**: ระบุไดรฟ์เป็น Hot Spare ส่วนกลาง หรือ Hot Spare เฉพาะ
       - **ถอด Hot Spare ออก**: ถอดไดรฟ์ออกจาก Hot Spare
       - **ทำให้ดิสก์ไดรฟ์ออฟไลน์**: ตั้งค่าให้ไดรฟ์ออฟไลน์
       - **ทำให้ดิสก์ไดรฟ์ออนไลน์**: ตั้งค่าให้ไดรฟ์ออนไลน์
       - **ทำให้ดิสก์ไดรฟ์เป็นแบบนำกลับมาใช้ใหม่ได้**: ตั้งค่าไดรฟ์เป็นแบบนำกลับมาใช้ใหม่ได้
       - **ทำให้ดิสก์ไดรฟ์เป็นรายการที่หายไป**: ตั้งค่าไดรฟ์เป็นรายการที่หายไป
       - **ทำให้ไดรฟ์พร้อมสำหรับ JBOD**: เพิ่มไดรฟ์ในการจัดเตรียมดิสก์ JBOD

- **ทำให้ไดรฟ์อยู่ในสภาพดีที่ไม่มีการกำหนดค่า**: ทำให้ไดรฟ์พร้อมใช้งานสำหรับการกำหนดค่าลงในอาร์เรย์ หรือสำหรับใช้เป็น Hot Spare ฉุกเฉิน
- **ทำให้ไดรฟ์อยู่ในสภาพไม่เหมาะสมที่ไม่มีการกำหนดค่า**: ทำเครื่องหมายว่าไดรฟ์อยู่ในสภาพไม่เหมาะสม เพื่อป้องกันไม่ให้นำไปใช้ในอาร์เรย์ หรือใช้เป็น Hot Spare ฉุกเฉิน
- **ทำให้ดิสก์ไดรฟ์เป็นรายการที่เตรียมถอดออก**: ตั้งค่าไดรฟ์สำหรับการถอดออก

2. หากตัวควบคุมมีไดรฟ์ที่ยังไม่ได้รับการกำหนดค่า ไดรฟ์เหล่านั้นจะปรากฏในตาราง **ไดรฟ์ที่ไม่ใช่** RAID โดยการคลิกตัวเลือก **แปลง** JBOD **เป็นพร้อมกำหนดค่า** หน้าต่างจะปรากฏพร้อมแสดงไดรฟ์ทั้งหมดที่รองรับรายการดำเนินการนี้ คุณสามารถเลือกไดรฟ์ที่จะแปลงได้อย่างน้อยหนึ่งไดรฟ์

สำหรับอุปกรณ์จัดเก็บที่ไม่รองรับการกำหนดค่า RAID: XClarity Controller อาจไม่สามารถตรวจหาคุณสมบัติของไดรฟ์บางรายการได้

บทที่ 7. การอัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์

ในการอัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์ ให้ใช้ข้อมูลในหัวข้อนี้

ภาพรวม

ข้อมูลทั่วไปเกี่ยวกับการอัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์

ตัวเลือก**การอัปเดตเฟิร์มแวร์**บนแผงการนำทางมี 4 คุณลักษณะ:

- **เฟิร์มแวร์ระบบ**: ภาพรวมของสถานะและเวอร์ชันของเฟิร์มแวร์ระบบ และใช้สำหรับการดำเนินการอัปเดตเฟิร์มแวร์ระบบ
- **เฟิร์มแวร์อะแดปเตอร์**: ภาพรวมของเฟิร์มแวร์อะแดปเตอร์ที่ติดตั้ง รวมถึงสถานะและเวอร์ชัน และใช้สำหรับการดำเนินการอัปเดตเฟิร์มแวร์อะแดปเตอร์
- **เฟิร์มแวร์** PSU: ภาพรวมของเวอร์ชันของเฟิร์มแวร์แหล่งจ่ายไฟ และใช้สำหรับการดำเนินการอัปเดตเฟิร์มแวร์ PSU
- **อัปเดตจากที่เก็บข้อมูล**: ซิงค์เฟิร์มแวร์ของเซิร์ฟเวอร์ให้ตรงกับที่เก็บข้อมูล CIFS/NFS ระยะไกลสำหรับการอัปเดตเป็นแบทช์

สถานะและเวอร์ชันของเฟิร์มแวร์ปัจจุบันสำหรับไดรเวอร์ BMC, UEFI และ LXPM และอะแดปเตอร์จะแสดงขึ้น รวมถึงเวอร์ชันหลักและเวอร์ชันสำรองของ BMC สถานะของเฟิร์มแวร์มีด้วยกันสี่ประเภท:

- **ใช้งานอยู่**: มีการใช้งานเฟิร์มแวร์อยู่
- **ไม่มีการใช้งาน**: ไม่มีการใช้งานเฟิร์มแวร์
- **กำลังรอ**: เฟิร์มแวร์กำลังรอเปลี่ยนมาใช้งาน
- N/A: ไม่มีการติดตั้งเฟิร์มแวร์สำหรับส่วนประกอบนี้

ข้อควรพิจารณา:

- XCC และ IMM ต้องได้รับการอัปเดตเป็นเวอร์ชันล่าสุดก่อนอัปเดต UEFI การอัปเดตในลำดับที่แตกต่างกันอาจส่งผลให้เกิดพฤติกรรมการทำงานที่แปลกหรือไม่ถูกต้อง
- การติดตั้งการอัปเดตเฟิร์มแวร์ที่ไม่ถูกต้องอาจทำให้เซิร์ฟเวอร์ทำงานผิดปกติ ก่อนที่คุณจะติดตั้งเฟิร์มแวร์หรืออัปเดตโปรแกรมควบคุมอุปกรณ์ ควรอ่านไฟล์ Readme และประวัติการเปลี่ยนแปลงที่มาพร้อมกับการอัปเดตที่ดาวน์โหลด ไฟล์เหล่านี้มีข้อมูลสำคัญเกี่ยวกับการอัปเดตและขั้นตอนการติดตั้งการอัปเดต รวมถึงขั้นตอนพิเศษในการอัปเดต ตั้งแต่เฟิร์มแวร์หรือโปรแกรมควบคุมอุปกรณ์รุ่นก่อนหน้าไปจนถึงรุ่นล่าสุด เนื่องจากเว็บเบราเซอร์อาจมีข้อมูลแคชของ XCC ขอแนะนำให้โหลดเว็บเพจอีกครั้งหลังจากอัปเกรดเฟิร์มแวร์ XCC

- เซิร์ฟเวอร์โปรเซสเซอร์ AMD ไม่รองรับการอัปเดตเฟิร์มแวร์ของอะแดปเตอร์ภายนอก ยกเว้นของอะแดปเตอร์ M.2 SATA
- การอัปเดตเฟิร์มแวร์บางรายการต้องมีการรีสตาร์ทระบบ ซึ่งจะเป็นการเปิดใช้งานเฟิร์มแวร์หรือการอัปเดตภายในกระบวนการนี้ในการบูทระบบเรียกว่า "โหมดการบำรุงรักษาระบบ" ซึ่งไม่อนุญาตให้ผู้ใช้ปิดเครื่องชั่วคราว นอกจากนี้โหมดดังกล่าวจะเปิดใช้งานระหว่างการอัปเดตเฟิร์มแวร์ด้วย ผู้ใช้จะต้องไม่ตัดการเชื่อมต่อไฟฟ้า AC เมื่อระบบเข้าสู่โหมดการบำรุงรักษา

การอัปเดตเฟิร์มแวร์ระบบ อะแดปเตอร์ และ PSU

ขั้นตอนในการอัปเดตเฟิร์มแวร์ระบบ เฟิร์มแวร์อะแดปเตอร์ และเฟิร์มแวร์ PSU

ในการนำการอัปเดตไปใช้กับ**เฟิร์มแวร์ระบบ เฟิร์มแวร์อะแดปเตอร์** และ**เฟิร์มแวร์** PSU ด้วยตนเอง ให้ทำตามขั้นตอนต่อไปนี้:

1. คลิก **อัปเดตเฟิร์มแวร์** ภายในแต่ละคุณลักษณะ หน้าต่างอัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์จะเปิดขึ้น
2. คลิก **เรียกดู** เพื่อเลือกไฟล์การอัปเดตเฟิร์มแวร์ที่คุณต้องการใช้
3. เลื่อนไปยังไฟล์ที่คุณต้องการเลือกและคลิก **เปิด** ระบบจะนำคุณกลับไปยังหน้าต่างอัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์โดยมีไฟล์ที่เลือกแสดงอยู่
4. คลิก **ถัดไป** > เพื่อเริ่มต้นการอัปโหลดและตรวจสอบกระบวนการในไฟล์ที่เลือก มาตรวัดความคืบหน้าจะแสดงขณะกำลังอัปโหลดและตรวจสอบไฟล์ คุณสามารถดูหน้าต่างสถานะนี้เพื่อตรวจสอบว่าไฟล์ที่คุณเลือกอัปเดตเป็นไฟล์ที่ถูกต้องหรือไม่ สำหรับ**เฟิร์มแวร์ระบบ** หน้าต่างสถานะจะมีข้อมูลเกี่ยวกับประเภทไฟล์ของเฟิร์มแวร์ที่จะอัปเดต เช่น BMC, UEFI หรือ LXPM หลังจากอัปโหลดไฟล์เฟิร์มแวร์และตรวจสอบเสร็จสิ้นแล้ว ให้คลิก **ถัดไป** เพื่อเลือกอุปกรณ์ที่คุณต้องการอัปเดต
5. คลิก **อัปเดต** เพื่อเริ่มการอัปเดตเฟิร์มแวร์ มาตรวัดความคืบหน้าจะแสดงความคืบหน้าของการอัปเดต เมื่อดำเนินการอัปเดตเฟิร์มแวร์เสร็จสมบูรณ์แล้ว ให้คลิก **เสร็จสิ้น** หากการอัปเดตกำหนดให้ต้องรีสตาร์ท XClarity Controller เพื่อให้มีผล ข้อความแจ้งเตือนจะปรากฏขึ้น ดูรายละเอียดเกี่ยวกับวิธีการรีสตาร์ท XClarity Controller ได้ที่ “การดำเนินการด้านพลังงาน” บนหน้าที่ 94

อัปเดตจากที่เก็บข้อมูล

อัปเดตเฟิร์มแวร์ของเซิร์ฟเวอร์จากที่เก็บข้อมูลระยะไกล

หมายเหตุ: *ฟังก์ชัน CIFS/NFS/HTTPS/Onboard Firmware History ต้องมีสิทธิ์การใช้งาน XCC Platinum*

ภาพรวม

XCC ได้เปิดตัวการอัปเดตเฟิร์มแวร์บนเซิร์ฟเวอร์โดยใช้แพ็คเกจ Update Bundles (Service Packs) คุณลักษณะนี้ทำให้กระบวนการง่ายขึ้นโดยใช้ API หนึ่งรายการหรือเครื่องมือไคลเอ็นต์ Redfish เพื่ออัปเดตเฟิร์มแวร์ทั้งหมดในระบบ รวมทั้งแพ็คเกจเฟิร์มแวร์ OOB และ IB ด้วย กระบวนการดังกล่าวเกี่ยวข้องกับการค้นหาแพ็คเกจเฟิร์มแวร์ที่เกี่ยวข้อง ดาวน์โหลดและแตกไฟล์จากเซิร์ฟเวอร์ HTTP/HTTPS ระยะไกล หรืออัปโหลดไปยังที่เก็บข้อมูลภายใน BMC ผ่านเว็บเบราว์เซอร์ หรือติดตั้งจากไดเร็กทอรีที่ใช้ร่วมกันของ CIFS หรือ NFS

ไฟล์ข้อมูลเมตาต้องอยู่ในไดเร็กทอรีระดับรากของระบบไฟล์ที่ใช้ร่วมกันของเครือข่าย หากใช้การเมาต์ CIFS หรือ NFS โดยมีการระบุเพย์โหลดของเฟิร์มแวร์ในข้อมูลเมตา อุปกรณ์ microSD ของเซิร์ฟเวอร์สามารถจัดเก็บที่เก็บข้อมูลประวัติ ทำให้ผู้ใช้สามารถย้อนกลับระดับเฟิร์มแวร์ได้

หากแพ็กเกจเฟิร์มแวร์มีเพย์โหลดที่ไม่รองรับการอัปเดตเฟิร์มแวร์นอกแบนด์ BMC จะเริ่มเซิร์ฟเวอร์และกำหนดค่าให้บูตจากอิมเมจของระบบปฏิบัติการแบบฝังที่ติดตั้งใน BMC ก่อนดำเนินการอัปเดต

Update Bundle และข้อมูลเมตา

Update Bundle (Service Packs) เป็นไฟล์บีบอัดของชุดเฟิร์มแวร์ ประกอบด้วยแพ็คเกจเฟิร์มแวร์ตั้งแต่หนึ่งแพ็คเกจขึ้นไปสำหรับส่วนประกอบในระบบ คุณลักษณะการอัปเดตจาก Repository ของ XCC จะใช้ไฟล์ Update Bundle ไฟล์ชุดที่คลายซิปมีข้อมูลเมตาและไบนารีเพย์โหลด ไฟล์ข้อมูลเมตา JSON ให้ข้อมูลแก่ XCC เกี่ยวกับประเภทของอิมเมจเฟิร์มแวร์ที่ไฟล์ชุดมีอยู่ และไบนารีเพย์โหลดจะจัดเตรียมอิมเมจเฟิร์มแวร์

ที่เก็บข้อมูลเฟิร์มแวร์ภายใน XCC

Update Bundle สามารถมีแพ็คเกจเฟิร์มแวร์ได้หลายชุด และ XCC (อุปกรณ์อิเล็กทรอนิกส์) จะสงวนพื้นที่ 2GB ในแฟลชสำหรับคุณลักษณะใหม่ เมื่อได้รับชุดใหม่แล้ว XCC จะล้างข้อมูลเก่า บางแพลตฟอร์มใช้การ์ด MicroSD เพื่อให้พื้นที่เก็บข้อมูลเพิ่มเติม และ XCC จะย้าย Updated Bundle ล่าสุดไปยังที่เก็บข้อมูลในอดีตของการ์ด SD ที่เก็บข้อมูลในอดีตของเฟิร์มแวร์สามารถจัดเก็บได้สูงสุดสามชุด และผู้ใช้สามารถใช้คุณลักษณะ Firmware Rollback เพื่อเปลี่ยนกลับเป็นชุดก่อนหน้าได้

หมายเหตุ:

- หาก Update Bundle รวมเฉพาะแพ็คเกจเฟิร์มแวร์ OOB ที่มีในระบบ XCC จะไม่เปลี่ยนสถานะพลังงานของระบบในการอัปเดตเฟิร์มแวร์อุปกรณ์ PCI จะต้องมีการเปิดระบบเสียก่อน
- หาก Update Bundle มีแพ็คเกจเฟิร์มแวร์ IB ที่มีอยู่ในระบบ XCC จะจัดเก็บสถานะพลังงานของระบบก่อนที่จะอัปเดตและกู้คืนสถานะพลังงานหลังจากอัปเดต Update Bundle แล้ว ในระหว่างกระบวนการอัปเดต XCC จะรีบูตโฮสต์เป็นระบบปฏิบัติการแบบฝัง
- หาก Update Bundle มีระดับข้อกำหนดเบื้องต้นของเฟิร์มแวร์ UEFI และถ้าเวอร์ชัน UEFI ที่ติดตั้งในปัจจุบันไม่ตรงตามหรือต่ำกว่าระดับนั้น XCC จะปิดระบบเพื่อทำการอัปเดตเฟิร์มแวร์ UEFI ก่อน

- หาก Update Bundle มีระดับข้อกำหนดเบื้องต้นของเฟิร์มแวร์ XCC และถ้าเวอร์ชัน XCC ที่ติดตั้งปัจจุบันไม่เป็นไปตามหรือต่ำกว่าระดับนั้น XCC จะรีบูตก่อนหลังจากอัปเกรดตัวเอง

อัปเดตด้วย WebGUI

ด้วย**การอัปเดตจากที่เก็บข้อมูล** ผู้ใช้สามารถกำหนดค่า XCC เพื่อซิงค์เฟิร์มแวร์ของเซิร์ฟเวอร์ให้ตรงกับที่เก็บข้อมูลเฟิร์มแวร์ CIFS/NFS ระยะไกลได้ ที่เก็บข้อมูลเฟิร์มแวร์ควรประกอบด้วยแพ็คเกจต่างๆ ซึ่งรวมถึงไฟล์ไบนารี่และข้อมูลเมตา หรือ Update Bundle Metadata JSON และไฟล์ไบนารีอื่นๆ ที่เกี่ยวข้อง XCC แยกวิเคราะห์ไฟล์ Metadata JSON เพื่อเลือกแพ็คเกจเฟิร์มแวร์ที่รองรับการอัปเดต OOB สำหรับฮาร์ดแวร์ระบบเฉพาะนี้ แล้วจึงเริ่มการอัปเดตเป็นแบทช์

มีสถานะการอัปเดต 5 สถานะ:

- **เครื่องหมายถูกสีเขียว** : การอัปเกรดเฟิร์มแวร์เสร็จสมบูรณ์แล้ว
- **เครื่องหมาย X สีแดง** : การอัปเกรดเฟิร์มแวร์ล้มเหลว
- **กำลังอัปเดต**: กำลังอยู่ระหว่างการอัปเกรดเฟิร์มแวร์
- **ยกเลิก**: การอัปเกรดเฟิร์มแวร์ถูกยกเลิก
- **รอดำเนินการ**: กำลังรอปรับใช้การอัปเกรดเฟิร์มแวร์

เมื่อผู้ใช้คลิก**หยุดการอัปเดต** จะเป็นการยกเลิกการอัปเกรดในคิวหลังจากการอัปเดตแบบแพคเกจการติดตั้งปัจจุบันเสร็จสมบูรณ์แล้ว

ในการอัปเดตจากที่เก็บข้อมูล ให้ดำเนินการขั้นตอนต่อไปนี้:

1. คลิก **เชื่อมต่อ** กับที่เก็บข้อมูลระยะไกลหลังจากป้อนข้อมูลที่เก็บข้อมูลระยะไกล
2. คลิก **อัปเดต** เพื่อเริ่มการอัปเดตเป็นแบทช์
3. คลิก **ดูรายละเอียด** เพื่อดูสถานะการอัปเดต โดยสถานะจะมีทั้งหมด 5 หมวดหมู่ตามที่กล่าวไปข้างต้น
4. คลิก **หยุดการอัปเดต** จะเป็นการยกเลิกการอัปเกรดในคิวหลังจากการอัปเดตแบบแพคเกจการติดตั้งปัจจุบันเสร็จสมบูรณ์แล้ว
5. คลิก **ตัดการเชื่อมต่อ** เพื่อตัดการเชื่อมต่อจากที่เก็บข้อมูลระยะไกล
6. หากการอัปเดตกำหนดให้ต้องรีสตาร์ท XClarity Controller เพื่อให้มีผล ข้อความแจ้งเตือนจะปรากฏขึ้น ดูรายละเอียดเกี่ยวกับวิธีการรีสตาร์ท XClarity Controller ได้ที่ “การดำเนินการด้านพลังงาน” บนหน้าที่ 94

หมายเหตุ: หากระบบติดตั้งการ์ด MicroSD คุณสามารถดูประวัติการอัปเดตของ Update Bundle และเลือกดัชนีของ Update Bundle เพื่อดำเนินการย้อนกลับเฟิร์มแวร์ได้ กระบวนการนี้คล้ายกับการอัปเดตจากที่เก็บข้อมูล ยกเว้น Update Bundle ในอดีตจะอยู่ใน MicroSD

อัปเดตด้วย Redfish

อินเทอร์เฟซ Redfish ใช้เพย์โหลดรูปแบบ JSON เพื่อให้คนสามารถอ่านและเขียนสคริปต์ได้ง่าย XCC Redfish มี API มาตรฐาน (SimpleUpdate) เพื่อดึงไฟล์ Update Bundle จาก URI ผ่าน HTTP/HTTPS/SFTP/TFTP เช่นเดียวกับ Multipart HTTP Push Update เพื่อทำการพุชไฟล์ Update Bundle UpdateService คุณสามารถใช้คำสั่งหรือเครื่องมือไคลเอ็นต์ Redfish รายการเดียวเพื่อทำการอัปเดตเฟิร์มแวร์และสถานะการอัปเดตคิวรี

คำสั่งตัวอย่างเพื่อพุชไฟล์ชุดไปยัง XCC และสร้างงานสำหรับการถ่ายโอนและการตรวจสอบไฟล์:

```
curl -s -k -u USERID:PASSWORD-F 'UpdateParameters={"Targets":[]};type=application/json' -F
 'UpdateFile=@./NY7D72-IB-320.zip;type=application/octet-stream' https://10.240.218.157:443/mfwupdate
{
  "ld": "f2fd6e9d-c0a6-4b11-b9f6-69a17a1 ,
  "Name": "Task f2fd6e9d-c0a6-4b11-b9f6-69a17a1 e579c",
  "@odata.type": "#Task.v1_5_1. Task",
  "@odata.id': "[redfish/v 1 fTaskServicefTasks/f2fd6e9d-c0a6-4b11-b9f6-69a 17a1 e579c",
  "Messages": [l
  "Description": "This resource represents a task for a Redfish implementation."
  "StartTime": "2022-03-21 TOT 16:41 +00:00",
  "TaskMonitor": "/redfish/v1fTaskSen.'ice/c069ed4a-e754-4970-ab9a-922e8a3e076b",
  "@odata.context": "'redfish/v1/$metadata#Task.Task",
  "@odata.etag":
  "PercentCompIete": 0,
  "HidePayload": true,
  "TaskState": "New"
}
```

คำสั่งตัวอย่างไปยัง API ของงานตอบสนองด้วยรหัสงานสำหรับการอัปเดตเฟิร์มแวร์หลังจากการถ่ายโอนและการตรวจสอบอิมเมจเสร็จสิ้น:

```
https://10.240.218.157/
redfish/v1/TaskService/Tasks/f2fd6e9d c0a6 4b11 b9f6 69a17a1e579c
{
  "@odata.etag": ,
  "Name-: "Task f2fd6e9d-c0a6-4b11-b9f6-69a17a1e579c",
  Task",
  "IredfishNI/TaskSemcenasksff2fd6e9d-c0a6-4bI I-b9f6-69aI 7a1e579c",
  "Messages": [
    {
      "Resolution": "Follow the referenced job and monitor the job for further updates.",
    "@odata.type":
    'MessageSeverity": "OK",
    "MessageArgs": [
    "IredfishtvI/JobService/JObs/JObROOOOOI-lJPdate"
  ],
  "Messageld": "Update. 1 .O.OperationTransitionedToJob",
  "Message": "The update operation has transitioned to the job at URI 'Iredfsh/vl
 IJobService/Jobs/JobROOOOO1-Update'."
  }
  ],
  "Description": "This resource represents a task for a Redfish implementation.",
  "HidePayIoad": true,
  "StartTime":
  "TaskMonitor: "'redfish1v1/TaskseNice/c069ed4a-e754-4970-ab9a-922e8a3e076b",
  "TaskStatus": "OK",
  "@odata.context-: "'redfish/v1/$metadata#Task.Task",
```

```
  "Id": "f2fd6e9d-c0a6-4b11-b9f6-6ga17a 1 e579c",
  "Percentcomplete": 100,
  "EndTime": 2022-03-21
  "TaskState": "Completed"
}
```

โดยการคิวรีรหัสงาน XCC จะส่งคืนขั้นตอนงานสำหรับแพ็คเกจเฟิร์มแวร์ทั้งหมดใน Update Bundle ดังที่แสดงด้านล่าง:

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-Update


```
{
"@odata.etag": "\"1647847200776\"", "PercentComplete": 100, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update", "Messages": [
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"HardDiskDrive"
],
"MessageId": "Update.1.0.UpdateSuccessful ",
"Message": " Device 'HardDiskDrive' successfully updated with image 'NY7D72-IB-320.zip'."
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/UEFI"
],
"MessageId": "Update.1.0.UpdateSuccessful",
"Message": "Device '/redfish/v1/UpdateService/FirmwareInventory/UEFI' successfully
 updated with image 'NY7D72-IB-320.zip'. "
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "Critical",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary"
],
"MessageId": "Update.1.0.ApplyFailed",
"Message": "Installation of image 'NY7D72-IB-320.zip' to '/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary' failed."
}
],
"Description": "This resource is used to represent a job for a Redfish implementation.",
"StartTime": "2022-03-21T07:16:58+00:00",
"Id": "JobR000001-Update",
"EndTime": "2022-03-21T07:20:00+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job", "Steps": {
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps"
},
"Name": "JobR000001-Update", "StepOrder": [
"lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "lnvgy_fw_uefi_ese103a-1.00_anyos_comp.uxz",
 "lnvgy_fw_xcc_esx301p-0.01_anyos_comp.uxz"
],
"JobState": "Completed"
```


เมื่อมีการคิวรีขั้นตอนงาน XCC จะส่งคืนข้อมูลเพิ่มเติมไปยังการอัปเดตเฟิร์มแวร์แต่ละรายการ:

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt


```
{
"@odata.etag": "\"1647847202778\"", "PercentComplete": 1, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-
```

```
 cq37_anyos_comp.lvt",
"Messages": [],
"Description": "This resource is used to represent a job for a Redfish implementation.", "StartTime":
 "2022-03-21T07:16:58+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job",
"Id": "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "Name":
 "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "EndTime": "2022-03-21T07:20:02+00:00",

"JobState": "Completed"
```

ทำการดาวน์โหลดจากที่เก็บข้อมูลระยะไกลและอัปเดตตามที่แสดงด้านล่าง:

```
system> syncrep
syncrep [options] Launch firmware sync from remote repository options:
-t protocol to connect repository. The local type will reboot host immediately.
 (eg: syncrep -t samba -l url -u user -p password; syncrep -t local -l /bulk/bundle.tgz;
syncrep -t http -l http://IP/bundle.tgz)
-l location of remote repository (URL format)
-u User
-p Password
-o option (extra option string for samba and nfs mounts)
-d domain (domain for samba mount)
-q query current update status
-c cancel the sync process
-r <> firmware rollback
-gl get repository list
```

บทที่ 8. การจัดการสิทธิ์การใช้งาน

การจัดการสิทธิ์การใช้งานของ Lenovo XClarity Controller ช่วยให้คุณสามารถติดตั้งและจัดการคุณลักษณะการจัดการเซิร์ฟเวอร์และระบบต่างๆ ที่เป็นตัวเลือกเสริม

เซิร์ฟเวอร์ของคุณสามารถใช้ฟังก์ชันและคุณลักษณะเฟิร์มแวร์ของ XClarity Controller ได้หลายระดับ ระดับของคุณสมบัติเฟิร์มแวร์ที่ติดตั้งบนเซิร์ฟเวอร์ของคุณอาจแตกต่างกันไป ทั้งนี้ขึ้นอยู่กับประเภทฮาร์ดแวร์

คุณสามารถอัปเกรดฟังก์ชัน XClarity Controller ได้โดยการซื้อและติดตั้งคีย์เปิดการทำงาน

หากต้องการสั่งซื้อคีย์เปิดการทำงาน โปรดติดต่อตัวแทนขายหรือพาร์ทเนอร์ทางธุรกิจของคุณ

ใช้เว็บอินเทอร์เฟซ XClarity Controller หรือ XClarity Controller CLI เพื่อติดตั้งคีย์เปิดการทำงานด้วยตนเอง ซึ่งจะทำให้คุณใช้คุณลักษณะที่เป็นตัวเลือกเสริมที่ซื้อไว้ได้ ก่อนที่จะเปิดการทำงานด้วยคีย์:

- คีย์เปิดการทำงานต้องอยู่ในระบบที่คุณกำลังใช้เข้าสู่ระบบ XClarity Controller
- คุณต้องสั่งซื้อคีย์สิทธิ์การใช้งานและรับรหัสอนุญาตทางไปรษณีย์หรืออีเมล

โปรดดู “การติดตั้งคีย์เปิดการทำงาน” บนหน้าที่ 133, “การลบคีย์เปิดการทำงาน” บนหน้าที่ 134 หรือ “การส่งออกคีย์เปิดการทำงาน” บนหน้าที่ 134 สำหรับข้อมูลเกี่ยวกับการจัดการคีย์เปิดการทำงานโดยใช้เว็บอินเทอร์เฟซ XClarity Controller โปรดดู “คำสั่ง keycfg” บนหน้าที่ 188 สำหรับข้อมูลเกี่ยวกับการจัดการคีย์เปิดการทำงานโดยใช้ XClarity Controller CLI

หากต้องการลงทะเบียน ID ในการดูแลจัดการสิทธิ์การใช้งานของ XClarity Controller ให้คลิกลิงก์ต่อไปนี้: http://thinksystem.lenovofiles.com/help/index.jsp

ดูข้อมูลเพิ่มเติมเกี่ยวกับการจัดการสิทธิ์การใช้งานสำหรับเซิร์ฟเวอร์ Lenovo ได้ที่เว็บไซต์ **Lenovo Press** ต่อไปนี้:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

ข้อควรพิจารณา: คุณไม่สามารถอัปเกรดฟังก์ชัน XClarity Controller ระดับมาตรฐานเป็นระดับองค์กรโดยตรง อันดับแรกคุณจะต้องอัปเกรดเป็นฟังก์ชันขั้นสูงก่อนจึงจะสามารถเปิดใช้งานฟังก์ชันระดับองค์กรได้

การติดตั้งคีย์เปิดการทำงาน

ใช้ข้อมูลในหัวข้อนี้เพื่อเพิ่มคุณลักษณะเสริมในเซิร์ฟเวอร์ของคุณ

ในการติดตั้งคีย์เปิดการทำงาน ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. คลิก **สิทธิ์การใช้งาน** ภายใต้ **การกำหนดค่า** BMC

ขั้นตอนที่ 2. คลิก **อัปเกรดสิทธิ์การใช้งาน**

ขั้นตอนที่ 3. ในหน้าต่าง **เพิ่มสิทธิ์การใช้งานใหม่** คลิก **เรียกดู** แล้วเลือกไฟล์คีย์เปิดการทำงานที่จะเพิ่มในหน้าต่าง อัปโหลดไฟล์ และคลิก **เปิด** เพื่อเพิ่มไฟล์ หรือคลิก **ยกเลิก** เพื่อหยุดการติดตั้ง หากต้องการเสร็จสิ้นการเพิ่มคีย์ ให้คลิก **ตกลง** ในหน้าต่าง เพิ่มคีย์เปิดการทำงาน หรือคลิก **ยกเลิก** เพื่อหยุดการติดตั้ง

หน้าต่าง สำเร็จ จะระบุว่าคีย์เปิดการทำงานได้รับการติดตั้ง

หมายเหตุ:

- หากคีย์เปิดการทำงานไม่ถูกต้อง หน้าต่างแสดงข้อผิดพลาดจะปรากฏขึ้น

ขั้นตอนที่ 4. คลิก **ตกลง** เพื่อปิดหน้าต่าง สำเร็จ

การลบคีย์เปิดการทำงาน

ใช้ข้อมูลในหัวข้อนี้เพื่อลบคุณลักษณะแบบเสริมออกจากเซิร์ฟเวอร์ของคุณ

ในการลบคีย์เปิดการทำงาน ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. คลิก **สิทธิ์การใช้งาน** ภายใต้ **การกำหนดค่า** BMC

ขั้นตอนที่ 2. เลือกคีย์เปิดการทำงานที่จะลบออก แล้วคลิก **ลบ**

ขั้นตอนที่ 3. ในหน้าต่าง ยืนยันการลบคีย์เปิดการทำงาน ให้คลิก **ตกลง** เพื่อยืนยันการลบคีย์เปิดการทำงาน หรือคลิก **ยกเลิก** เพื่อเก็บไฟล์คีย์ไว้
คีย์เปิดการทำงานที่เลือกจะถูกลบออกจากเซิร์ฟเวอร์ และจะไม่ปรากฏในหน้าการจัดการสิทธิ์การใช้งานอีกต่อไป

การส่งออกคีย์เปิดการทำงาน

ใช้ข้อมูลในหัวข้อนี้เพื่อส่งออกคุณลักษณะแบบเสริมจากเซิร์ฟเวอร์ของคุณ

หากต้องการส่งออกคีย์เปิดการทำงาน โปรดดำเนินการขั้นตอนต่อไปนี้

ขั้นตอนที่ 1. คลิก **สิทธิ์การใช้งาน** ภายใต้ **การกำหนดค่า** BMC

ขั้นตอนที่ 2. ในหน้าการจัดการสิทธิ์การใช้งาน ให้เลือกคีย์เปิดการทำงานที่ต้องการส่งออก แล้วคลิก **ส่งออก**

ขั้นตอนที่ 3. ในหน้าต่าง **ส่งออกสิทธิ์การใช้งานที่เลือก** ให้คลิก **ส่งออก** เพื่อยืนยันการส่งออกคีย์เปิดการทำงาน หรือคลิก **ยกเลิก** เพื่อยกเลิกคำขอการส่งออกคีย์

ขั้นตอนที่ 4. เลือกไดเร็กทอรี่สำหรับบันทึกไฟล์
คีย์เปิดการทำงานที่เลือกจะถูกส่งออกจากเซิร์ฟเวอร์

บทที่ 9. การจัดการกลุ่มข้างเคียง

การจัดการกลุ่มข้างเคียงของ Lenovo XClarity Controller เป็นกลุ่มการจัดการเสมือนจริงในเซิร์ฟเวอร์ Lenovo ThinkSystem ซึ่งจัดการเซิร์ฟเวอร์หลายเครื่องใน XCC เดียว

Lenovo XClarity Controller (XCC) เป็นโปรเซสเซอร์บริการแบบผสานรวมที่มาแทนที่ Baseboard Management Controller (BMC) ที่รู้จักกันดีสำหรับเซิร์ฟเวอร์ Lenovo ThinkSystem เพื่อฟังก์ชันการกำหนดค่าเซิร์ฟเวอร์ การจัดการ และการตรวจสอบ

โดยปกติแล้ว XCC จะสามารถจัดการเซิร์ฟเวอร์ได้เพียงเครื่องเดียวเท่านั้น อย่างไรก็ตาม ซอฟต์แวร์การจัดการแบบรวมศูนย์ของ Lenovo XClarity Administrator (LXCA) จะช่วยอำนวยความสะดวกในการจัดการการปรับขยายไปยังเซิร์ฟเวอร์หลายเครื่อง หากไม่ได้ปรับใช้ LXCA ในภาคสนาม โดยเฉพาะอย่างยิ่งสำหรับผู้ใช้ SMB แต่ละโหนดจะต้องได้รับการกำหนดค่าทีละโหนด ซึ่งเป็นกระบวนการที่ไม่มีประสิทธิภาพ เพื่อจัดการกับสถานการณ์นี้ คุณลักษณะของกลุ่มข้างเคียง XCC ได้รับการออกแบบมาเพื่อสร้างกลุ่มการจัดการเสมือนจริงระหว่างเซิร์ฟเวอร์ Lenovo ThinkSystem ซึ่งจะจัดการเซิร์ฟเวอร์หลายเครื่องใน XCC เดียว ซึ่งเป็นวิธีที่ยืดหยุ่นในการเริ่มต้นการปรับใช้อย่างรวดเร็วสำหรับเซิร์ฟเวอร์หลายเครื่องภายในส่วนเครือข่ายท้องถิ่น

คุณลักษณะที่รองรับ

ข้อมูลทั่วไปเกี่ยวกับคุณลักษณะที่กลุ่มข้างเคียงรองรับ

The **กลุ่มข้างเคียง XCC** มีคุณลักษณะต่อไปนี้:

- ค้นพบโหนดข้างเคียงที่อยู่ในส่วนเครือข่ายท้องถิ่นเดียวกัน
- ตรวจสอบความสมบูรณ์ของระบบและสถานะพลังงานของโหนดข้างเคียง
- กำหนดค่ากลุ่มข้างเคียงในโหนดผู้นำ
- โคลนการกำหนดค่าระบบให้กับสมาชิกหลายคนของกลุ่มข้างเคียง
- เริ่มการอัปเดตเฟิร์มแวร์พร้อมกันกับสมาชิกหลายคนของกลุ่มข้างเคียง
- โหนดผู้นำ XCC รองรับสูงสุด 200 โหนด

เซิร์ฟเวอร์ ThinkSystem ที่รองรับคุณลักษณะกลุ่มข้างเคียง XCC

เซิร์ฟเวอร์	ประเภทเครื่อง
ThinkSystem SR630 V3	7D72, 7D73
ThinkSystem SR650 V3	7D75, 7D76
Lenovo ThinkSystem ST650 V3	7D7A,7D7B,7D7C
Lenovo ThinkSystem SD650 V3	7D7M
Lenovo ThinkSystem SD650–I V3	7D7L
Lenovo ThinkSystem SR635 V3	7D9G,7D9H
Lenovo ThinkSystem SR645 V3	7D9C,7D9D
Lenovo ThinkSystem SR655 V3	7D9E,7D9F
Lenovo ThinkSystem SR665 V3	7D9A,7D9B
ThinkSystem SD665 V3	7D9P
ThinkSystem SR675 V3	7D9Q,7D9R

หมายเหตุ: คุณลักษณะ XCC Neighbor Group จะรวมอยู่ในเซิร์ฟเวอร์ Lenovo ThinkSystem รุ่นต่อๆ ไป

การค้นหาโหนดข้างเคียง

ใช้ข้อมูลในหัวข้อนี้เพื่อค้นหาโหนดข้างเคียง

อินสแตนซ์ XCC แต่ละรายการจะค้นพบเซิร์ฟเวอร์ข้างเคียงในกลุ่มเครือข่ายท้องถิ่นเดียวกันโดยใช้ข้อความมัลติคาสต์ Simple Service Discovery Protocol (SSDP)

สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับเซิร์ฟเวอร์ที่จะค้นพบโดยอินสแตนซ์ XCC:

1. พอร์ต 1900 สำหรับ Simple Service Discovery Protocol (SSDP) 1900 เปิดใช้งานใน XCC (**การกำหนดค่า BMC –> Network –> SSDP**)
2. การจัดการกลุ่มข้างเคียงจะถูกกำหนดค่าให้เปิดใช้งาน (ปิดใช้งานตามค่าเริ่มต้น)

หน้า Discovery จะช่วยตรวจสอบข้อมูลระบบ สถานะพลังงานและสถานภาพแบบเรียลไทม์ของโหนดที่ค้นหาทั้งหมด คอลัมน์ **Last Time Alive** ระบุการประทับเวลาของการได้รับข้อความ SSDP ล่าสุดจากโหนดข้างเคียง มีการอัปเดตเป็นประจำเว้นแต่โหนดข้างเคียงจะออฟไลน์อยู่ หรือการตั้งค่า SSDP/การจัดการกลุ่มข้างเคียงถูกปิดใช้งาน

การตั้งค่ากลุ่มข้างเคียง

ใช้ข้อมูลในหัวข้อนี้เพื่อตั้งค่ากลุ่มข้างเคียง

กลุ่มข้างเคียงถูกสร้างขึ้นบนหน้าเว็บ XCC โดยระบุชื่อกลุ่ม

ตรวจสอบให้แน่ใจว่าชื่อกลุ่มใหม่ไม่ซ้ำกันและไม่มีอยู่ในส่วนเครือข่ายท้องถิ่น

หลังจากสร้างกลุ่มใหม่แล้ว:

- อินสแตนซ์ XCC ปัจจุบันจะถูกเพิ่มเข้าไปโดยอัตโนมัติ
- อินสแตนซ์ XCC ปัจจุบันกลายเป็นโหนดผู้นำของกลุ่มข้างเคียง XCC ใหม่
- อินสแตนซ์ XCC อื่นๆ ทั้งหมดในกลุ่มเครือข่ายท้องถิ่นเดียวกันจะได้รับแจ้งทันที และหน้าเว็บการค้นพบ XCC ข้างเคียงของแต่ละเซิร์ฟเวอร์จะได้รับการอัปเดต
- โหนดผู้นำของกลุ่มสามารถเลือกเซิร์ฟเวอร์ข้างเคียงหนึ่งเซิร์ฟเวอร์หรือเซิร์ฟเวอร์ข้างเคียงหลายเซิร์ฟเวอร์ได้ เพื่อเข้าร่วมกลุ่มโดยระบุข้อมูลประจำตัวผู้ดูแลระบบ XCC ของเซิร์ฟเวอร์ข้างเคียง
- เมื่อโหนดข้างเคียงตรวจสอบข้อมูลรับรองผู้ใช้สำเร็จ โหนดข้างเคียงจะยอมรับคำขอจากโหนดผู้นำ จากนั้นจึงเข้าร่วมกลุ่มนี้ในฐานะสมาชิกใหม่

การเตรียมใช้งานกลุ่มข้างเคียง

ใช้ข้อมูลในหัวข้อนี้เพื่อเตรียมใช้งานกลุ่มข้างเคียง

การเตรียมใช้งานกลุ่มข้างเคียงเป็นคุณลักษณะที่กระจายการกำหนดค่าไปยังสมาชิกกลุ่มหลายคน ประกอบด้วย **Clone Configuration** และ **Update Firmware from Repository**

Clone Configuration ใช้เพื่อเผยแพร่การกำหนดค่าของระบบ XCC ปัจจุบันไปยังสมาชิกที่เลือกของประเภทเครื่องเดียวกัน การกำหนดค่าที่ถูกโคลนรวมถึง:

1. การกำหนดค่าเซิร์ฟเวอร์: Boot Options, Power Policy, Server Properties

2. การกำหนดค่า BMC: เครือข่าย (ยกเว้นที่อยู่ IP และการตั้งค่าที่เกี่ยวข้อง), การรักษาความปลอดภัย, ผู้ใช้/LDAP (รวมถึงบัญชีผู้ใช้และรหัสผ่าน), Call Home

Update Firmware from Repository จะเริ่มต้นการอัปเดตเฟิร์มแวร์พร้อมกันสำหรับสมาชิกที่เลือก โดยระบุที่เก็บข้อมูลเฟิร์มแวร์ที่ใช้ร่วมกันผ่านโปรโตคอล Common Internet File System (CIFS) หรือ Network File System (NFS) สามารถใช้การอัปเดตเฟิร์มแวร์กับเครื่องหลายประเภทพร้อมกันได้ ตราบใดที่มีอิมเมจเฟิร์มแวร์ที่เกี่ยวข้องอยู่ในที่เก็บข้อมูลที่ใช้ร่วมกัน

เมื่อมีการอัปเดตเฟิร์มแวร์ของกลุ่มข้างเคียง คุณสามารถตรวจสอบความคืบหน้าได้ในคอลัมน์ Status & Details

บทที่ 10. Lenovo XClarity Controller Redfish REST API

Lenovo XClarity Controller ประกอบด้วยชุด REST API ใช้งานได้ง่ายที่สอดคล้องตาม Redfish ซึ่งสามารถนำไปใช้เพื่อเข้าถึงข้อมูลและบริการของ Lenovo XClarity Controller ได้จากแอปพลิเคชันซึ่งใช้งานภายนอกเฟรมเวิร์กของ Lenovo XClarity Controller

คุณสมบัตินี้ช่วยมอบความสะดวกสบายในการผสานความสามารถของ Lenovo XClarity Controller เข้ากับซอฟต์แวร์อื่นๆ ไม่ว่าซอฟต์แวร์ดังกล่าวจะทำงานบนระบบเดียวกันกับเซิร์ฟเวอร์ Lenovo XClarity Controller หรือบนเซิร์ฟเวอร์ระยะไกลภายในเครื่องข่ายเดียวกัน API เหล่านี้พัฒนาจาก REST API มาตรฐานอุตสาหกรรมของ Redfish และเข้าถึงได้ผ่านโปรโตคอล HTTPS

ดูคู่มือผู้ใช้ XClarity Controller Redfish REST API ได้ที่นี่: https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf

Lenovo มีสคริปต์ Redfish โอเพนซอร์สตัวอย่าง ซึ่งสามารถใช้เป็นข้อมูลอ้างอิงสำหรับการพัฒนาซอฟต์แวร์ที่สื่อสารกับ Lenovo Redfish REST API ดูสคริปต์ตัวอย่างเหล่านี้ได้ที่:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

ดูข้อมูลจำเพาะของ DMTF ที่เกี่ยวข้องกับ Redfish API ได้ที่: https://redfish.dmtf.org/ เว็บไซต์นี้มีข้อมูลจำเพาะทั่วไปและเอกสารอ้างอิงอื่นๆ เกี่ยวกับ Redfish REST API

บทที่ 11. อินเทอร์เฟซบรรทัดคำสั่ง

ใช้ข้อมูลในหัวข้อนี้เพื่อป้อนคำสั่งสำหรับจัดการและเฝ้าตรวจสอบการทำงานของ XClarity Controller โดยไม่ต้องใช้เว็บอินเทอร์เฟซของ XClarity Controller

ใช้อินเทอร์เฟซบรรทัดคำสั่ง (CLI) เพื่อเข้าใช้งาน XClarity Controller โดยไม่ต้องใช้เว็บอินเทอร์เฟซ โดยประกอบด้วยฟังก์ชันการจัดการชุดย่อยที่มีในเว็บอินเทอร์เฟซ

คุณสามารถเข้าถึง CLI ได้ทางเซสชัน SSH คุณต้องได้รับการตรวจสอบความถูกต้องจาก XClarity Controller ก่อนจึงจะออกคำสั่งใน CLI ได้

การเข้าถึงอินเทอร์เฟซบรรทัดคำสั่ง

ใช้ข้อมูลในหัวข้อนี้เพื่อเข้าถึง CLI

ในการเข้าถึง CLI ให้เริ่มเซสชัน SSH ไปยังที่อยู่ IP ของ XClarity Controller (ดูข้อมูลเพิ่มเติมได้ที่ “การกำหนดค่าการเปลี่ยนเส้นทางแบบอนุกรมไปยัง SSH” บนหน้าที่ 143)

การเข้าสู่ระบบเซสชันบรรทัดคำสั่ง

ใช้ข้อมูลในหัวข้อนี้เพื่อเข้าสู่ระบบเซสชันบรรทัดคำสั่ง

ในการเข้าสู่ระบบบรรทัดคำสั่ง ให้ดำเนินการขั้นตอนต่อไปนี้:

ขั้นตอนที่ 1. ทำการเชื่อมต่อกับ XClarity Controller

ขั้นตอนที่ 2. พิมพ์ ID ผู้ใช้ เมื่อได้รับข้อความให้ป้อนชื่อผู้ใช้

ขั้นตอนที่ 3. พิมพ์รหัสผ่านที่คุณใช้ในการเข้าสู่ระบบ XClarity Controller เมื่อได้รับข้อความให้ป้อนรหัสผ่าน

คุณเข้าสู่ระบบบรรทัดคำสั่ง พร้อมท์บรรทัดคำสั่งคือ `system>` เซสชันบรรทัดคำสั่งจะดำเนินต่อไปจนกว่าคุณจะพิมพ์ `exit` ที่บรรทัดคำสั่ง คุณออกจากระบบและเซสชันสิ้นสุดแล้ว

การกำหนดค่าการเปลี่ยนเส้นทางแบบอนุกรมไปยัง SSH

หัวข้อนี้แสดงข้อมูลเกี่ยวกับการใช้ XClarity Controller เป็นเซิร์ฟเวอร์ปลายทางอนุกรม

การเปลี่ยนเส้นทางแบบอนุกรมไปยัง SSH จะทำให้ผู้ดูแลระบบสามารถใช้ XClarity Controller เป็นเซิร์ฟเวอร์ปลายทางอนุกรมได้ สามารถเข้าถึงพอร์ตอนุกรมของเซิร์ฟเวอร์ได้จากการเชื่อมต่อ SSH เมื่อเปิดใช้งานการเปลี่ยนเส้นทางแบบอนุกรม

หมายเหตุ: คำสั่ง **console 1** ของ CLI ถูกใช้เพื่อเริ่มเซสชันการเปลี่ยนเส้นทางแบบอนุกรมด้วยพอร์ต COM

เซสชันตัวอย่าง

```
$ ssh USERID@10.240.1.12
Password:

system>
```

การรับส่งข้อมูลทั้งหมดจากเซสชัน SSH ถูกเปลี่ยนเส้นทางไปยัง COM2

```
ESC (
```

พิมพ์ลำดับคีย์ออกเพื่อกลับไปยัง CLI ในตัวอย่างนี้ กด Esc แล้วพิมพ์วงเล็บซ้าย พร้อมท์ CLI จะแสดงขึ้นเพื่อระบุการกลับไปยัง IMM CLI

```
system>
```

รูปแบบคำสั่ง

ดูหลักเกณฑ์ในหัวข้อนี้เพื่อทำความเข้าใจวิธีป้อนคำสั่งใน CLI

โปรดอ่านหลักเกณฑ์ต่อไปนี้ก่อนที่จะใช้คำสั่ง:

- แต่ละคำสั่งมีรูปแบบต่อไปนี้:
  `command [arguments] [-options]`
- รูปแบบคำสั่งจะพิจารณาตัวพิมพ์เล็ก-ใหญ่
- ชื่อคำสั่งเป็นตัวพิมพ์เล็กทั้งหมด
- อาร์กิวเมนต์ทั้งหมดต้องตามหลังคำสั่งทันที ตัวเลือกต้องตามหลังอาร์กิวเมนต์ทันที
- แต่ละตัวเลือกจะมีเครื่องหมายขีดกลาง (-) นำหน้าเสมอ ตัวเลือกอาจเป็นแบบย่อ (ตัวอักษรตัวเดียว) หรือแบบยาว (ตัวอักษรหลายตัว) ก็ได้
- หากตัวเลือกมีอาร์กิวเมนต์ จะต้องระบุอาร์กิวเมนต์ เช่น:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  โดยที่ **ifconfig** คือคำสั่ง eth0 คืออาร์กิวเมนต์ ขณะที่ -i, -g และ -s คือตัวเลือก ในตัวอย่างนี้ ตัวอย่างทั้งสามมีอาร์กิวเมนต์

- วงเล็บเป็นการระบุว่าอาร์กิวเมนต์หรือตัวเลือกนั้นๆ ไม่บังคับ วงเล็บไม่ใช่ส่วนหนึ่งของคำสั่งที่คุณพิมพ์

คุณลักษณะและข้อจำกัด

หัวข้อนี้ประกอบด้วยข้อมูลเกี่ยวกับคุณลักษณะและข้อจำกัดของ CLI

CLI ประกอบด้วยคุณลักษณะและข้อจำกัดต่อไปนี้:

- อนุญาตให้มีเซสชัน CLI ที่เกิดขึ้นพร้อมกันหลายเซสชันผ่าน SSH
- ป้อนได้หนึ่งคำสั่งต่อบรรทัด (จำกัดความยาว 1024 อักขระ รวมเว้นวรรค)
- ไม่มีการใช้อักขระต่อเนื่องสำหรับคำสั่งแบบยาว ฟังก์ชันแก้ไขเพียงอย่างเดียวที่ใช้ได้คือปุ่ม Backspace ซึ่งใช้ลบอักขระที่คุณเพิ่งพิมพ์ไป
- คุณสามารถใช้ปุ่มลูกศรขึ้นและลงเพื่อเลือกคำสั่งที่ป้อนล่าสุดได้ 8 คำสั่ง คำสั่ง **history** จะแสดงคำสั่ง 8 รายการล่าสุดที่คุณสามารถใช้เป็นปุ่มลัดในการรันคำสั่งได้ ดังตัวอย่างต่อไปนี้:

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- ใน CLI จะมีการจำกัดบัฟเฟอร์เอาต์พุตที่ 2 KB ไม่มีการบัฟเฟอร์ เอาต์พุตของแต่ละคำสั่งต้องมีอักขระไม่เกิน 2048 ตัว ขีดจำกัดนี้ไม่มีผลกับโหมดเปลี่ยนเส้นทางพอร์ตอนุกรม (มีการบัฟเฟอร์ข้อมูลระหว่างการเปลี่ยนเส้นทางพอร์ตอนุกรม)
- โดยจะใช้ข้อความธรรมดาในการระบุสถานะการรันคำสั่ง ดังตัวอย่างต่อไปนี้:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- รูปแบบคำสั่งจะพิจารณาตัวพิมพ์เล็ก-ใหญ่

- ต้องมีช่องว่างอย่างน้อยหนึ่งช่องระหว่างตัวเลือกกับอาร์กิวเมนต์ ตัวอย่างเช่น `ifconfig eth0 -i192.168.70.133` ถือเป็นรูปแบบคำสั่งที่ไม่ถูกต้อง รูปแบบคำสั่งที่ถูกต้องคือ `ifconfig eth0 -i 192.168.70.133`
- คำสั่งทั้งหมดจะมีตัวเลือก `-h`, `-help` และ `?` ซึ่งแสดงวิธีใช้รูปแบบคำสั่ง ตัวอย่างต่อไปนี้จะให้ผลลัพธ์แบบเดียวกัน:
```
system> power -h
system> power -help
system> power ?
```
- บางคำสั่งที่อธิบายไว้ในส่วนต่อไปนี้อาจใช้ไม่ได้กับการกำหนดค่าระบบของคุณ ในการดูรายการคำสั่งที่การกำหนดค่าของคุณรองรับ ให้ใช้ตัวเลือก `help` หรือ `?` ดังที่แสดงในตัวอย่างต่อไปนี้:
```
system> help
system> ?
```
- ใน Flex System การตั้งค่าบางอย่างจะได้รับการจัดการโดย CMM และไม่สามารถแก้ไขใน XClarity Controller ได้

รายการคำสั่งตามตัวอักษร

หัวข้อนี้จะแสดงรายการคำสั่งใน CLI ตามลำดับตัวอักษร โดยแต่ละคำสั่งจะมีลิงก์ไปยังหัวข้อนั้นๆ แต่ละหัวข้อจะแสดงข้อมูลเกี่ยวกับคำสั่ง ฟังก์ชัน รูปแบบคำสั่ง และการใช้งาน

รายการคำสั่งใน XClarity Controller CLI ทั้งหมดตามลำดับตัวอักษรมีดังนี้:

คำสั่งยูทิลิตี้

หัวข้อนี้จะแสดงรายการคำสั่งยูทิลิตี้ใน CLI ตามตัวอักษร

คำสั่งยูทิลิตี้มี 3 คำสั่งดังนี้:

คำสั่ง exit

ใช้คำสั่งนี้เพื่อออกจากระบบเซสชัน CLI

ใช้คำสั่ง **exit** เพื่อออกจากระบบและสิ้นสุดเซสชัน CLI

คำสั่ง help

คำสั่งนี้จะแสดงรายการคำสั่งทั้งหมด

ใช้คำสั่ง **help** เพื่อแสดงรายการคำสั่งทั้งหมด พร้อมรายละเอียดสั้นๆ ของแต่ละคำสั่ง นอกจากนี้ คุณยังสามารถพิมพ์ ? ใน Command Prompt ได้ด้วย

คำสั่ง history

คำสั่งนี้จะแสดงรายการคำสั่งที่เคยใช้ไป

ใช้คำสั่ง **history** เพื่อแสดงรายการประวัติคำสั่งที่ใช้ไป 8 รายการล่าสุดที่จัดทำดัชนีไว้ ดัชนีเหล่านี้สามารถใช้เป็นทางลัด (นำหน้าด้วย !) เพื่อออกคำสั่งเดิมซ้ำจากรายการประวัติ

ตัวอย่าง:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
```

```
-l 00:00:00:00:00:00
system>
```

คำสั่งการตรวจสอบ

หัวข้อนี้จะแสดงรายการคำสั่งการตรวจสอบใน CLI ตามตัวอักษร

คำสั่งการตรวจสอบมี 11 คำสั่งดังนี้:

คำสั่ง clearlog

คำสั่งนี้จะใช้เพื่อล้างข้อมูลในบันทึกเหตุการณ์ IMM

ใช้คำสั่ง **clearlog** เพื่อล้างข้อมูลในบันทึกเหตุการณ์ของ IMM ในการใช้คำสั่งนี้ คุณจะต้องมีสิทธิ์ล้างข้อมูลในบันทึกเหตุการณ์

หมายเหตุ: คำสั่งนี้มีไว้เพื่อรองรับการใช้งานส่วนบุคคลเท่านั้น

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 7. คำสั่ง clearlog

ตารางต่อไปนี้เป็นตารางแบบบรรทัดเดียวสองคอลัมน์ซึ่งประกอบด้วยตัวเลือกและคำอธิบายตัวเลือก

ตัวเลือก	รายละเอียด
-t <all | platform | audit>	ประเภทของเหตุการณ์ เลือกประเภทเหตุการณ์ที่ต้องการล้างข้อมูล หากไม่ได้ระบุ ประเภทเหตุการณ์ทั้งหมดจะถูกเลือก

คำอธิบายประเภทของเหตุการณ์

- ทั้งหมด: ประเภทของเหตุการณ์ทั้งหมด รวมถึงเหตุการณ์แพลตฟอร์มและเหตุการณ์การตรวจสอบ
- แพลตฟอร์ม: เหตุการณ์ประเภทแพลตฟอร์ม
- ตรวจสอบ: เหตุการณ์ประเภทการตรวจสอบ

ตัวอย่างเช่น:

```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
```

```
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

คำสั่ง fans

คำสั่งนี้ใช้เพื่อแสดงข้อมูลความเร็วพัดลมเซิร์ฟเวอร์

ใช้คำสั่ง **fans** เพื่อแสดงความเร็วพัดลมเซิร์ฟเวอร์แต่ละตัว

ตัวอย่าง:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

คำสั่ง ffdc

คำสั่งนี้ใช้ในการสร้างไฟล์ข้อมูลการบริการใหม่

ใช้คำสั่ง First Failure Data Capture (**ffdc**) เพื่อสร้างและถ่ายโอนข้อมูลการบริการไปยังการสนับสนุน

รายการต่อไปนี้ประกอบด้วยคำสั่งที่ใช้ร่วมกับคำสั่ง **ffdc**

- **generate** ใช้เพื่อสร้างไฟล์ข้อมูลการบริการใหม่
- **status** ใช้เพื่อตรวจสอบสถานะไฟล์ข้อมูลการบริการ
- **copy** ใช้คัดลอกข้อมูลการบริการที่มีอยู่
- **delete** ใช้ลบข้อมูลการบริการที่มีอยู่

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 8. คำสั่ง ffdc

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 8. คำสั่ง ffdc (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-t	หมายเลขประเภทข้อมูล	1 (การถ่ายโอนโปรเซสเซอร์) และ 4 (ข้อมูลการบริการ) การถ่ายโอนข้อมูลโปรเซสเซอร์ประกอบด้วยบันทึกและไฟล์ที่มีทั้งหมด ข้อมูลบริการประกอบด้วยชุดย่อยของบันทึกและไฟล์ ค่าเริ่มต้นคือ 1
-f [1]	ชื่อไฟล์ระยะไกล หรือ ไดเร็กทอรี่เป้าหมายของ sftp	สำหรับ sftp ให้ใช้พาธแบบเต็มหรือ/ปิดท้ายสำหรับชื่อไดเร็กทอรี่ (~/ หรือ /tmp/) ค่าเริ่มต้นคือชื่อที่สร้างโดยระบบ
-ip [1]	ที่อยู่ของเซิร์ฟเวอร์ tftp/sftp	
-pn [1]	หมายเลขพอร์ตของเซิร์ฟเวอร์ tftp/sftp	ค่าเริ่มต้นคือ 69/22
-u [1]	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ sftp	
-pw [1]	รหัสผ่านสำหรับเซิร์ฟเวอร์ sftp	
1. อาร์กิวเมนต์เพิ่มเติมสำหรับคำสั่ง generate และ copy		

รูปแบบคำสั่ง:
```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

ตัวอย่างเช่น:
```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
```

```
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

คำสั่ง hreport

ใช้คำสั่งนี้ในการแสดงรายงานสถานภาพที่ฝังตัว

ตารางต่อไปนี้จะแสดงคำสั่ง hreport

ตาราง 9. คำสั่ง hreport

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยรายละเอียดคำสั่ง hreport ต่างๆ

ตัวเลือก	**รายละเอียด**
generate	สร้างรายงานสถานภาพใหม่
status	ตรวจสอบสถานะ
copy	คัดลอกรายงานสถานภาพที่มีอยู่
delete	ลบรายงานสถานภาพที่มีอยู่

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือก generate และ copy

ตาราง 10. คำสั่ง generate และ copy

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกคำสั่ง generate และ copy และรายละเอียดตัวเลือก

ตัวเลือก	**รายละเอียด**
-f	ชื่อไฟล์ระยะไกลหรือไดเร็กทอรี่เป้าหมาย sftp (ค่าเริ่มต้นคือชื่อที่สร้างโดยระบบ ((สำหรับ sftp, ให้ใช้พาธแบบเต็มหรือ/ปิดท้ายสำหรับชื่อไดเร็กทอรี่ (~/ หรือ /tmp/))
-ip	ที่อยู่ของเซิร์ฟเวอร์ tftp/sftp

ตาราง 10. คำสั่ง generate และ copy (มีต่อ)

ตัวเลือก	รายละเอียด
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ tftp/sftp (ค่าเริ่มต้น 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ sftp
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ sftp

คำสั่ง mhlog

ใช้คำสั่งนี้เพื่อแสดงรายการในบันทึกกิจกรรมของประวัติการบำรุงรักษา

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 11. คำสั่ง mhlog

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด
-c <count>	แสดงรายการ 'จำนวน' (1-250)
-i <index>	แสดงรายการเริ่มต้นที่ดัชนี (1-250)
-f	ชื่อไฟล์ระยะไกลของไฟล์บันทึก
-ip	ที่อยู่ของเซิร์ฟเวอร์ tftp/sftp
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ tftp/sftp (ค่าเริ่มต้น 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ sftp
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ sftp

ตัวอย่าง

การแสดงผลจะมีลักษณะดังนี้:

```
Type            Message                                                    Time
-------------   ------------                                               ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.                  05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
```

```
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                          05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.      05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T .              05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C0075) is added.                             05/08/2020,06:43:28
```

คำสั่ง led

ใช้คำสั่งนี้เพื่อแสดงผลและตั้งค่าสถานะไฟ LED

คำสั่ง **led** จะแสดงผลและตั้งค่าสถานะไฟ LED ของเซิร์ฟเวอร์

- การเรียกใช้คำสั่ง **led** โดยไม่มีตัวเลือกจะแสดงสถานะของไฟ LED ในแผงด้านหน้า
- ตัวเลือกคำสั่ง **led -d** ต้องใช้กับตัวเลือกคำสั่ง **led -identify on**

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 12. คำสั่ง led

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-l	เรียกดูสถานะไฟ LED ทั้งหมดในระบบและส่วนประกอบย่อย	
-chklog	ปิดไฟ LED ของบันทึกการตรวจสอบ	off
-identify	เปลี่ยนสถานะของไฟ LED ระบุสถานะช่องใส่	off, on, blink
-d	เปิดไฟ LED ระบุสถานะในระยะเวลาที่กำหนด	ระยะเวลา (วินาที)

รูปแบบคำสั่ง:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

ตัวอย่าง:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
```

```
Power                   Off

system> led -l
Label                   Location                State          Color
Battery                 Planar                  Off
BMC Heartbeat           Planar                  Blink          Green
BRD                     Lightpath Card          Off
Channel A               Planar                  Off
Channel B               Planar                  Off
Channel C               Planar                  Off
Channel D               Planar                  Off
Channel E               Planar                  Off
Chklog                  Front Panel             Off
CNFG                    Lightpath Card          Off
CPU                     Lightpath Card          Off
CPU 1                   Planar                  Off
CPU 2                   Planar                  Off
DASD                    Lightpath Card          Off
DIMM                    Lightpath Card          Off
DIMM 1                  Planar                  Off
DIMM 10                 Planar                  Off
DIMM 11                 Planar                  Off
DIMM 12                 Planar                  Off
DIMM 13                 Planar                  Off
DIMM 14                 Planar                  Off
DIMM 15                 Planar                  Off
DIMM 16                 Planar                  Off
DIMM 2                  Planar                  Off
DIMM 3                  Planar                  Off
DIMM 4                  Planar                  Off
DIMM 5                  Planar                  Off
DIMM 6                  Planar                  Off
DIMM 7                  Planar                  Off
DIMM 8                  Planar                  Off
DIMM 9                  Planar                  Off
FAN                     Lightpath Card          Off
FAN 1                   Planar                  Off
FAN 2                   Planar                  Off
FAN 3                   Planar                  Off
Fault                   Front Panel (+)         Off
Identify                Front Panel (+)         On             Blue
LINK                    Lightpath Card          Off
LOG                     Lightpath Card          Off
NMI                     Lightpath Card          Off
OVER SPEC               Lightpath Card          Off
PCI 1                   FRU                     Off
PCI 2                   FRU                     Off
PCI 3                   FRU                     Off
PCI 4                   FRU                     Off
Planar                  Planar                  Off
Power                   Front Panel (+)         Off
PS                      Lightpath Card          Off
RAID                    Lightpath Card          Off
Riser 1                 Planar                  Off
Riser 2                 Planar                  Off
SAS ERR                 FRU                     Off
SAS MISSING             Planar                  Off
SP                      Lightpath Card          Off
TEMP                    Lightpath Card          Off
VRM                     Lightpath Card          Off
system>
```

คำสั่ง readlog

คำสั่งนี้จะแสดงบันทึกเหตุการณ์ IMM

ใช้คำสั่ง **readlog** เพื่อแสดงรายการในบันทึกเหตุการณ์ IMM ระบบจะแสดงบันทึกเหตุการณ์พร้อมกัน 5 รายการ รายการจะแสดงจากใหม่สุดไปยังเก่าสุด

readlog จะแสดง 5 รายการแรกในบันทึกเหตุการณ์ เริ่มตั้งแต่รายการล่าสุดจากการเรียกใช้ครั้งแรก ตามด้วย 5 รายการในลำดับต่อมา

readlog -a จะแสดงรายการทั้งหมดในบันทึกเหตุการณ์ เริ่มตั้งแต่รายการล่าสุด

readlog -f จะรีเซ็ตตัวนับและแสดง 5 รายการแรกในบันทึกเหตุการณ์ เริ่มตั้งแต่รายการล่าสุด

readlog -date *วันที่* จะแสดงรายการในบันทึกเหตุการณ์ในวันที่ระบุด้วยรูปแบบ ดด/วว/ปป สามารถคั่นรายการวันที่ด้วยเครื่องหมายขีดแนวตั้ง (|)

readlog -sev *ระดับความร้ายแรง* จะแสดงรายการในบันทึกเหตุการณ์ในระดับความร้ายแรงที่ระบุ (E, W, I) สามารถคั่นรายการระดับความร้ายแรงด้วยเครื่องหมายขีดแนวตั้ง (|)

readlog -i *ip_address* จะตั้งค่าที่อยู่ IP แบบ IPv4 หรือIPv6 ของเซิร์ฟเวอร์ TFTP หรือ SFTP ซึ่งจะใช้จัดเก็บบันทึกเหตุการณ์ ตัวเลือกคำสั่ง **-i** และ **-l** จะใช้ร่วมกันเพื่อระบุที่ตั้ง

readlog -l *ชื่อไฟล์* จะตั้งค่าชื่อไฟล์บันทึกเหตุการณ์ ตัวเลือกคำสั่ง **-i** และ **-l** จะใช้ร่วมกันเพื่อระบุที่ตั้ง

readlog -pn *port_number* จะแสดงหรือตั้งค่าหมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP หรือ SFTP (ค่าเริ่มต้นคือ 69/22)

readlog -u *ชื่อผู้ใช้* จะระบุชื่อผู้ใช้ของเซิร์ฟเวอร์ SFTP

readlog -pw *รหัสผ่าน* จะระบุรหัสผ่านของเซิร์ฟเวอร์ SFTP

รูปแบบคำสั่ง:
```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

ตัวอย่าง:
```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
```

```
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

คำสั่ง syshealth

คำสั่งนี้ให้ข้อมูลสรุปของสถานะหรือเหตุการณ์ที่ดำเนินอยู่

ใช้คำสั่ง syshealth ในการแสดงข้อมูลสรุปของสถานะหรือเหตุการณ์ที่ดำเนินอยู่ของเซิร์ฟเวอร์ สถานะพลังงาน สถานะระบบ สถานะฮาร์ดแวร์ (รวมถึงพัดลม แหล่งจ่ายไฟ ที่จัดเก็บ โปรเซสเซอร์ หน่วยความจำ) จำนวนการรีสตาร์ท และสถานะซอฟต์แวร์ IMM จะแสดงขึ้น

รูปแบบคำสั่ง:

```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

ตัวอย่าง:

```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

คำสั่ง temps

คำสั่งนี้จะแสดงข้อมูลอุณหภูมิและเกณฑ์อุณหภูมิทั้งหมด

ใช้คำสั่ง temps ในการแสดงข้อมูลอุณหภูมิและเกณฑ์อุณหภูมิทั้งหมด อุณหภูมิชุดเดียวกันจะแสดงเหมือนในเว็บอินเทอร์เฟซ

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T      SS      HS
-----------------------------------------------
CPU1     N/A     N/A   80/27     N/A     N/A
CPU2     N/A     N/A   80/27     N/A     N/A
DASD1  66/19   73/23   82/28   88/31   92/33
Amb    59/15   70/21   83/28   90/32   95/35
system>
```

หมายเหตุ:

1. ผลลัพธ์มีส่วนหัวคอลัมน์ต่อไปนี้:

   WR: รีเซ็ตคำเตือน (ค่าฮิสเทอรีซิสของเกณฑ์ที่ไปในทางบวก)

   W: คำเตือน (สูงกว่าเกณฑ์ที่ไม่ร้ายแรง)

   T: อุณหภูมิ (ค่าปัจจุบัน)

   SS: ซอฟต์ชัตดาวน์ (สูงกว่าเกณฑ์ที่ร้ายแรง)

   HS: ฮาร์ดชัตดาวน์ (สูงกว่าเกณฑ์ที่ไม่สามารถกู้คืนได้)
2. ค่าอุณหภูมิทั้งหมดอยู่ในหน่วยองศาฟาห์เรนไฮต์/เซลเซียส
3. N/A หมายถึง ไม่สามารถใช้ได้

คำสั่ง volts

ใช้คำสั่งนี้ในการแสดงข้อมูลแรงดันไฟฟ้าของเซิร์ฟเวอร์

ใช้คำสั่ง **volts** ในการแสดงข้อมูลแรงดันไฟฟ้าและเกณฑ์แรงดันไฟฟ้าทั้งหมด แรงดันไฟฟ้าชุดเดียวกันจะแสดงเหมือนในเว็บอินเทอร์เฟซ

```
Example:
system> volts

      i HSL    SSL    WL     WRL    V      WRH    WH     SSH     HSH
-------------------------------------------------------------------
5v     5.02   4.00   4.15   4.50   4.60   5.25   5.50   5.75    6.00
3.3v   3.35   2.80   2.95   3.05   3.10   3.50   3.65   3.70    3.85
12v   12.25  11.10  11.30  11.50  11.85  12.15  12.25  12.40   12.65
-5v   -5.10  -5.85  -5.65  -5.40  -5.20  -4.85  -4.65  -4.40   -4.20
-3.3v -3.35  -4.10  -3.95  -3.65  -3.50  -3.10  -2.95  -2.80   -2.70
VRM1                             3.45
VRM2                             5.45
system>
```

หมายเหตุ: ผลลัพธ์มีส่วนหัวคอลัมน์ต่อไปนี้:

HSL: ฮาร์ดชัตดาวน์ ต่ำ (ต่ำกว่าเกณฑ์ที่ไม่สามารถกู้คืนได้)

SSL: ซอฟต์ชัตดาวน์ ต่ำ (ต่ำกว่าเกณฑ์ที่ร้ายแรง)

WL: คำเตือน ต่ำ (ต่ำกว่าเกณฑ์ที่ไม่ร้ายแรง)

WRL: รีเซ็ตคำเตือน ต่ำ (ค่าฮิสเทอรีซิสของเกณฑ์ที่ไปในทางบวก)

V: แรงดันไฟฟ้า (ค่าปัจจุบัน)

WRH: รีเซ็ตคำเตือน สูง (ค่าฮิสเทอรีซิสของเกณฑ์ไปในทางบวก)

WH: คำเตือน สูง (สูงกว่าเกณฑ์ที่ไม่ร้ายแรง)

SSH: ซอฟต์ชัตดาวน์ สูง (สูงกว่าเกณฑ์ที่ร้ายแรง)

HSH: ฮาร์ดชัตดาวน์ สูง (สูงกว่าเกณฑ์ที่ไม่สามารถกู้คืนได้)

คำสั่ง vpd

คำสั่งนี้จะแสดงการกำหนดค่าและข้อมูล (ข้อมูลผลิตภัณฑ์ที่สำคัญ) ที่เกี่ยวข้องกับฮาร์ดแวร์และซอฟต์แวร์ของเซิร์ฟเวอร์

ใช้คำสั่ง **vpd** เพื่อแสดงข้อมูลผลิตภัณฑ์ที่สำคัญสำหรับระบบ (sys), IMM (bmc), BIOS เซิร์ฟเวอร์ (uefi), Lenovo XClarity Provisioning Manager (lxpm), เฟิร์มแวร์ของเซิร์ฟเวอร์ (fw), ส่วนประกอบของเซิร์ฟเวอร์ (comp) และอุปกรณ์ PCIe (pcie) ข้อมูลเดียวกันจะแสดงเหมือนในเว็บอินเทอร์เฟซ

รูปแบบคำสั่ง:
```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

ตัวอย่าง:
```
system> vpd bmc
Type            Status      Version     Build     ReleaseDate
----            -------       -----       ------
BMC (Primary)   Active      0.00        DVI399T    2017/06/06
BMC (Backup)    Inactive    1.00        TEI305J    2017/04/13

system>
```

คำสั่งควบคุมการเปิด/ปิดและเริ่มระบบเครื่องเซิร์ฟเวอร์ใหม่

หัวข้อนี้จะแสดงรายการคำสั่งเปิด/ปิดและเริ่มระบบเครื่องเซิร์ฟเวอร์ใหม่ใน CLI ตามตัวอักษร

คำสั่งเปิด/ปิดและเริ่มระบบเครื่องเซิร์ฟเวอร์ใหม่มี 4 คำสั่งดังนี้:

คำสั่ง power

คำสั่งนี้จะกำหนดวิธีควบคุมการเปิด/ปิดเครื่องเซิร์ฟเวอร์

ใช้คำสั่ง **power** เพื่อควบคุมการเปิด/ปิดเครื่องเซิร์ฟเวอร์ ในการใช้คำสั่ง **power** คุณจะต้องมีสิทธิ์เปิด/ปิดเครื่องหรือเริ่มระบบใหม่สำหรับเซิร์ฟเวอร์ระยะไกลในระดับสิทธิ์ที่กำหนด

ตารางต่อไปนี้ประกอบด้วยชุดย่อยของคำสั่งที่ใช้ได้กับคำสั่ง **power**

ตาราง 13. คำสั่ง power

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยคำสั่งเปิด/ปิดเครื่อง รายละเอียดคำสั่ง และค่าของคำสั่งที่เกี่ยวข้อง

คำสั่ง	**รายละเอียด**	**ค่า**
การเปิดเครื่อง	ใช้คำสั่งนี้ในการเปิดเครื่องเซิร์ฟเวอร์	on, off
power off	ใช้คำสั่งนี้ในการปิดเครื่องเซิร์ฟเวอร์ **หมายเหตุ**: ตัวเลือก **-s** จะเป็นการปิดระบบปฏิบัติการก่อนที่เซิร์ฟเวอร์จะปิดเครื่อง	on, off
power cycle	ใช้คำสั่งนี้เพื่อปิดเครื่องเซิร์ฟเวอร์แล้วจึงเปิดเครื่องอีกครั้ง **หมายเหตุ**: ตัวเลือก **-s** จะเป็นการปิดระบบปฏิบัติการก่อนที่เซิร์ฟเวอร์จะปิดเครื่อง	
power enterS3	ใช้คำสั่งนี้เพื่อให้ระบบปฏิบัติการเข้าสู่โหมด S3 (โหมดสลีป) **หมายเหตุ**: คำสั่งนี้จะใช้เมื่อระบบปฏิบัติการเปิดอยู่เท่านั้น โหมด S3 อาจไม่รองรับในเซิร์ฟเวอร์บางรุ่น	
power rp	ใช้ตัวเลือกนี้เพื่อระบุนโยบายการจ่ายไฟกลับเข้าระบบของโฮสต์	alwayson|alwaysoff|restore

ตาราง 13. คำสั่ง power (มีต่อ)

คำสั่ง	รายละเอียด	ค่า
power S3resume	ใช้คำสั่งนี้เพื่อให้ระบบปฏิบัติการออกจากโหมด S3 (โหมดสลีป) **หมายเหตุ**: คำสั่งนี้จะใช้เมื่อระบบปฏิบัติการเปิดอยู่เท่านั้น โหมด S3 อาจไม่รองรับในเซิร์ฟเวอร์บางรุ่น	
power state	ใช้คำสั่งนี้เพื่อแสดงสถานะการเปิด/ปิดเครื่องเซิร์ฟเวอร์ และสถานะปัจจุบันของเซิร์ฟเวอร์	on, off

ตารางต่อไปนี้ประกอบด้วยตัวเลือกสำหรับคำสั่ง **power on**, **power off** และ **power cycle**

ตาราง 14. คำสั่ง power

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-s	ใช้ตัวเลือกนี้เพื่อปิดระบบปฏิบัติการก่อนที่เซิร์ฟเวอร์จะปิดเครื่อง **หมายเหตุ**: ตัวเลือก **-s** จะถูกใช้โดยปริยายเมื่อมีการใช้ตัวเลือก **-every** สำหรับคำสั่ง **power off** และ **power cycle**	
-every	ใช้ตัวเลือกนี้กับคำสั่ง **power on**, **power off** และ **power cycle** เพื่อควบคุมการเปิด/ปิดเครื่องเซิร์ฟเวอร์ คุณสามารถตั้งค่าวันที่ เวลา และความถี่ (ทุกวันหรือทุกสัปดาห์) ในการเปิด ปิด หรือเริ่มระบบเซิร์ฟเวอร์ใหม่	**หมายเหตุ**: ค่าต่างๆ ของตัวเลือกนี้จะแสดงแบบแยกบรรทัดกันเนื่องจากมีพื้นที่จำกัด Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-t	ใช้ตัวเลือกนี้เพื่อระบุเวลาเป็นชั่วโมงและนาทีเพื่อเปิดเครื่องเซิร์ฟเวอร์ ปิดระบบปฏิบัติการ และปิดหรือเริ่มระบบเซิร์ฟเวอร์ใหม่	ใช้รูปแบบต่อไปนี้: hh:mm (h ชม., m นาที)

ตาราง 14. คำสั่ง power (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-d	ใช้ตัวเลือกนี้เพื่อระบุวันที่ในการเปิดเครื่องเซิร์ฟเวอร์ นี่เป็นตัวเลือกเพิ่มเติมสำหรับคำสั่ง power on **หมายเหตุ**: ตัวเลือก -d และ -every ไม่สามารถใช้ร่วมกันในคำสั่งเดียวกันได้	ใช้รูปแบบต่อไปนี้: mm/dd/yyyy (m เดือน, d วัน, y ปี)
-clear	ใช้ตัวเลือกนี้เพื่อล้างข้อมูลวันที่เปิดเครื่องที่วางกำหนดการไว้ นี่เป็นตัวเลือกเพิ่มเติมสำหรับคำสั่ง power on	

รูปแบบคำสั่ง:
```
power on
power off [-s]
power state
power cycle [-s]
```

ข้อมูลต่อไปนี้เป็นตัวอย่างของคำสั่ง power

หากต้องการปิดระบบปฏิบัติการและปิดเครื่องเซิร์ฟเวอร์ทุกวันอาทิตย์เวลา 1.30 น. ให้ป้อนคำสั่งต่อไปนี้:
```
system> power off
-every Sun -t 01:30
```

หากต้องการปิดระบบปฏิบัติการและเริ่มระบบเซิร์ฟเวอร์ใหม่ทุกวันเวลา 1.30 น. ให้ป้อนคำสั่งต่อไปนี้:
```
system> power cycle
-every Day -t 01:30
```

หากต้องการเปิดเครื่องเซิร์ฟเวอร์ทุกวันจันทร์เวลา 1.30 น. ให้ป้อนคำสั่งต่อไปนี้:
```
system> power on
-every Mon -t 13:00
```

หากต้องการเปิดเครื่องเซิร์ฟเวอร์ในวันที่ 31 ธันวาคม 2013 เวลา 23.30 น. ให้ป้อนคำสั่งต่อไปนี้:
```
system> power on
-d 12/31/2013 -t 23:30
```

หากต้องการล้างข้อมูลการเริ่มระบบใหม่ทุกสัปดาห์ ให้ป้อนคำสั่งต่อไปนี้:
```
system> power cycle
-every clear
```

คำสั่ง reset

คำสั่งนี้จะกำหนดวิธีรีเซ็ตเครื่องเซิร์ฟเวอร์

ใช้คำสั่ง **reset** เพื่อเริ่มระบบเครื่องเซิร์ฟเวอร์ใหม่ ในการใช้คำสั่งนี้ คุณจะต้องมีสิทธิ์เปิด/ปิดเครื่องหรือเริ่มระบบใหม่

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 15. คำสั่ง reset

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-s	ปิดระบบปฏิบัติการก่อนที่จะรีเซ็ตเซิร์ฟเวอร์	
-d	หน่วงเวลาการรีเซ็ตไว้ตามเวลาที่กำหนด (เป็นวินาที)	0 - 120
-nmi	สร้างสัญญาณขัดจังหวะความสำคัญสูง (NMI) บนเซิร์ฟเวอร์	

รูปแบบคำสั่ง:
```
reset [option]
option:
-s
-d
-nmi
```

คำสั่ง fuelg

คำสั่งนี้ใช้สำหรับแสดงผลข้อมูลเกี่ยวกับพลังงานของเซิร์ฟเวอร์

ใช้คำสั่ง **fuelg** เพื่อแสดงข้อมูลเกี่ยวกับการใช้พลังงานของเครื่องเซิร์ฟเวอร์ และกำหนดค่าการจัดการพลังงานของเซิร์ฟเวอร์ นอกจากนี้ คำสั่งนี้ยังใช้กำหนดค่านโยบายต่างๆ สำหรับการสูญเสียการสำรองพลังงานด้วย ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 16. คำสั่ง fuelg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 16. คำสั่ง fuelg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-pme	เปิดใช้งานหรือปิดใช้งานการจัดการพลังงานและการจำกัดพลังงานของเซิร์ฟเวอร์	on, off
-pcapmo-de	กำหนดโหมดการจำกัดพลังงานของเซิร์ฟเวอร์	อินพุต, เอาต์พุต
-pcap	ค่าตัวเลขซึ่งอยู่ระหว่างช่วงค่าของการจำกัดพลังงาน ซึ่งจะแสดงเมื่อเรียกใช้คำสั่ง fuelg โดยไม่ระบุตัวเลือกกับเป้าหมาย	ค่าตัวเลขกำลังไฟฟ้า
-history	แสดงประวัติการใช้พลังงานหรือประวัติประสิทธิภาพ	pc, perf
-period	ค่าตัวเลขสำหรับการแสดงประวัติ (1, 6, 12, 24 ชั่วโมง)	ค่าตัวเลขเป็นชั่วโมง
-pm	กำหนดโหมดนโยบายสำหรับการสูญเสียการสำรองพลังงาน	• **bt**- แบบพื้นฐานพร้อมการจำกัดพลังงาน • **rt**- แบบซ้ำซ้อนและไม่มีการจำกัดพลังงาน (ค่าเริ่มต้น) • **ort**- N_1 แบบซ้ำซ้อนและไม่มีการจำกัดพลังงาน
-zm	เปิดใช้งานหรือปิดใช้งานโหมด Zero Output การตั้งค่านี้สามารถตั้งค่าได้เมื่อมีการตั้งค่าโหมดนโยบายเป็นแบบซ้ำซ้อนและไม่มีการจำกัดพลังงาน	on, off
-perf	แสดงการใช้งานการประมวลผลปัจจุบัน รวมถึงระบบ ไมโครโปรเซสเซอร์ และ I/O	เปอร์เซ็นต์
-pc	แสดงผลการใช้พลังงานปัจจุบัน	• **output**- แสดงผลการใช้พลังงาน DC ปัจจุบัน สำหรับเซิร์ฟเวอร์ทาวเวอร์และตู้แร็ค คำสั่งนี้จะรวมการใช้พลังงานของระบบ, CPU, หน่วยความจำ และส่วนประกอบอื่นๆ แต่สำหรับเบลดเซิร์ฟเวอร์ ITE คำสั่งนี้จะรวมการใช้พลังงานของระบบเท่านั้น • **input**- แสดงผลการใช้พลังงานขาเข้าปัจจุบัน รวมถึงการใช้พลังงานของระบบ

รูปแบบคำสั่ง:
```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

ตัวอย่าง:
```
system> fuelg
-pme: on
system>
```

คำสั่ง pxeboot

คำสั่งนี้จะแสดงและตั้งค่าเงื่อนไขของ Preboot eXecution Environment

การเรียกใช้คำสั่ง **pxeboot** โดยไม่มีตัวเลือกจะแสดงการตั้งค่า Preboot eXecution Environment ในปัจจุบัน ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 17. คำสั่ง pxeboot

ตารางต่อไปนี้เป็นตารางแถวเดียวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าที่เกี่ยวข้องกับตัวเลือกนั้นๆ

ตัวเลือก	รายละเอียด	ค่า
-en	ตั้งค่าเงื่อนไข Preboot eXecution Environment สำหรับการเริ่มระบบครั้งต่อไป	enabled, disabled

รูปแบบคำสั่ง:
```
pxeboot [options]
option:
  -en state
```

ตัวอย่าง:
```
system> pxeboot
-en disabled
system>
```

คำสั่ง Serial Redirect

หัวข้อนี้ประกอบด้วยคำสั่ง Serial Redirect

มีคำสั่ง Serial Redirect เพียงหนึ่งคำสั่ง นั่นคือ: “คำสั่ง console” บนหน้าที่ 167

คำสั่ง console

ใช้คำสั่งนี้เพื่อเริ่มเซสชันคอนโซลการเปลี่ยนเส้นทางพอร์ตอนุกรม

ใช้คำสั่ง **console** เพื่อเริ่มเซสชันคอนโซลการเปลี่ยนเส้นทางพอร์ตอนุกรมไปยังพอร์ตอนุกรม IMM ที่กำหนดไว้

รูปแบบคำสั่ง:
```
console 1
```

คำสั่งการกำหนดค่า

หัวข้อนี้จะแสดงรายการคำสั่งการกำหนดค่าใน CLI ตามตัวอักษร

คำสั่งการกำหนดค่ามี 41 คำสั่งดังนี้:

คำสั่ง accseccfg

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดการตั้งค่าการรักษาความปลอดภัยของบัญชี

การเรียกใช้คำสั่ง **accseccfg** โดยไม่มีตัวเลือกจะแสดงข้อมูลการรักษาความปลอดภัยบัญชีทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 18. คำสั่ง accseccfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 18. คำสั่ง accseccfg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-am	ตั้งค่าวิธีการตรวจสอบความถูกต้องผู้ใช้	local, ldap, localldap, ldaplocal
-lp	ระยะเวลาการล็อคผู้ใช้จากระบบเมื่อเข้าใช้งานล้มเหลวครบจำนวนครั้งสูงสุด (นาที)	ระหว่าง 0 ถึง 2880, 0 = ระยะเวลาการล็อคผู้ใช้จากระบบไม่หมดอายุ
-pe	ระยะเวลาสิ้นอายุของรหัสผ่าน (วัน)	ระหว่าง 0 ถึง 365, 0 = ไม่หมดอายุ
-pew	ระยะเวลาการแจ้งเตือนรหัสผ่านหมดอายุ **หมายเหตุ**: ระยะเวลาการแจ้งเตือนรหัสผ่านหมดอายุต้องน้อยกว่าระยะเวลาการหมดอายุรหัสผ่าน	ระหว่าง 0 ถึง 30, 0 = ไม่แจ้งเตือน
-pc	เปิดใช้งานกฎความซับซ้อนของรหัสผ่านแล้ว	on, off
-pl	ความยาวรหัสผ่าน	หากมีการเปิดใช้งานกฎความซับซ้อนของรหัสผ่าน ความยาวของรหัสผ่านต้องอยู่ระหว่าง 8 ถึง 32 ตัว หากไม่เปิดใช้งานจะอยู่ระหว่าง 0 ถึง 32 ตัว
-ci	กรอบเวลาขั้นต่ำสำหรับการเปลี่ยนรหัสผ่าน (ชั่วโมง)	ระหว่าง 0 ถึง 240, 0 = เปลี่ยนทันที
-lf	จำนวนครั้งสูงสุดของการเข้าใช้งานล้มเหลว	ระหว่าง 0 ถึง 10, 0 = ไม่ล็อค
-chgnew	เปลี่ยนรหัสผ่านผู้ใช้ใหม่หลังจากเข้าสู่ระบบครั้งแรก	on, off
-rc	จำนวนรอบการใช้รหัสผ่านซ้ำ	ระหว่าง 0 ถึง 10, 0 = ใช้ซ้ำทันที
-wt	การหมดเวลาเซสชันเมื่อไม่มีการใช้งานบนเว็บและ Secure Shell (นาที)	ระหว่าง 0 ถึง 1440

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication methoc
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

ตัวอย่าง:

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgnew off
-rc 0
-wt user
system>
```

คำสั่ง alertcfg

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าพารามิเตอร์การแจ้งเตือนระยะไกลส่วนกลางของ IMM

การเรียกใช้คำสั่ง alertcfg โดยไม่มีตัวเลือกจะแสดงพารามิเตอร์การแจ้งเตือนระยะไกลแบบร่วมทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 19. คำสั่ง alertcfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 19. คำสั่ง alertcfg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-dr	ตั้งค่าเวลารอระหว่างการลองใหม่แต่ละครั้งก่อนที่ IMM จะส่งการแจ้งเตือนซ้ำ	0 ถึง 4.0 นาที โดยเพิ่มขึ้นครั้งละ 0.5 นาที
-da	ตั้งค่าเวลารอก่อนที่ IMM จะส่งการแจ้งเตือนไปยังผู้รับคนถัดไปในรายชื่อ	0 ถึง 4.0 นาที โดยเพิ่มขึ้นครั้งละ 0.5 นาที
-rl	ตั้งค่าจำนวนครั้งเพิ่มเติมที่จะให้ IMM พยายามส่งการแจ้งเตือนต่อไป หากความพยายามก่อนหน้าล้มเหลว	0 ถึง 8

รูปแบบคำสั่ง:
```
alertcfg [options]
  options:
    -rl retry_limit
    -dr retry_delay
    -da agent_delay
```

ตัวอย่าง:
```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

คำสั่ง asu

คำสั่งนี้ใช้ในการกำหนดการตั้งค่า UEFI

คำสั่ง Advanced Settings Utility (ASU) ใช้สำหรับกำหนดการตั้งค่า UEFI เพื่อให้การเปลี่ยนแปลงการตั้งค่า UEFI ใดๆ เริ่มต้นทำงาน จำเป็นต้องรีบูตระบบโฮสต์

ตารางต่อไปนี้ประกอบด้วยชุดย่อยของคำสั่งที่ใช้ได้กับคำสั่ง **asu**

ตาราง 20. คำสั่ง asu

ตารางต่อไปนี้เป็นตารางหลายแถวแบบ 3 คอลัมน์ ซึ่งประกอบด้วยคำสั่งย่อยที่ใช้ร่วมกับคำสั่ง **asu** ได้ ข้อมูลคำอธิบายและค่าที่เกี่ยวข้องกับคำสั่งจะมีการอธิบายไว้ภายในตาราง

ตาราง 20. คำสั่ง asu (มีต่อ)

คำสั่ง	รายละเอียด	ค่า
delete	ใช้คำสั่งนี้เพื่อลบอินสแตนซ์หรือบันทึกของการตั้งค่า การตั้งค่าจะต้องเป็นอินสแตนซ์ที่ยินยอมให้ลบได้ เช่น iSCSI.AttemptName.1	*setting_instance*
ความช่วยเหลือ	ใช้คำสั่งนี้เพื่อแสดงข้อมูลช่วยเหลือสำหรับการตั้งค่าหนึ่งรายการหรือมากกว่า	*setting*
set	ใช้คำสั่งนี้เพื่อเปลี่ยนแปลงค่าของการตั้งค่า กำหนดการตั้งค่า UEFI เป็นค่าอินพุต **หมายเหตุ**: • กำหนดคู่ของการตั้งค่า/ค่าอย่างน้อยหนึ่งรายการ • การตั้งค่านี้สามารถใช้อักขระตัวแทนได้หากขยายไปยังการตั้งค่ารายการเดียว • ค่าจะต้องอยู่ในเครื่องหมายอัญประกาศหากมีช่องว่าง • ค่าของรายการแบบเรียงลำดับจะต้องคั่นด้วยสัญลักษณ์เท่ากับ (=) เช่น set B*.Bootorder“CD/DVD Rom=Hard Disk 0=PXE Network.”	*setting value*
showgroups	ใช้คำสั่งนี้เพื่อแสดงผลกลุ่มการตั้งค่าที่ใช้งานได้ คำสั่งนี้จะแสดงผลชื่อของกลุ่มที่เป็นที่รู้จัก ชื่อกลุ่มอาจแตกต่างกันไปขึ้นอยู่กับอุปกรณ์ที่ติดตั้ง	*setting*
show	ใช้คำสั่งนี้เพื่อแสดงค่าปัจจุบันของการตั้งค่าอย่างน้อยหนึ่งรายการ	*setting*

ตาราง 20. คำสั่ง asu (มีต่อ)

คำสั่ง	รายละเอียด	ค่า
showvalues	ใช้คำสั่งนี้เพื่อแสดงค่าที่เป็นไปได้ทั้งหมดของการตั้งค่าอย่างน้อยหนึ่งรายการ **หมายเหตุ**: • คำสั่งนี้จะแสดงข้อมูลเกี่ยวกับค่าที่ยินยอมให้สำหรับการตั้งค่า • คำสั่งนี้จะแสดงจำนวนอินสแตนซ์ต่ำสุดและสูงสุดที่ยอมให้สำหรับการตั้งค่านี้ • ค่าเริ่มต้นจะแสดง หากมี • ค่าเริ่มต้นจะอยู่ในวงเล็บมุมเปิดและปิด (< และ >) • ค่าแบบข้อความจะแสดงความยาวต่ำสุดและสูงสุด และนิพจน์แบบทั่วไป	*setting*

หมายเหตุ:

- ในรูปแบบของคำสั่ง *setting* คือชื่อของการตั้งค่าที่คุณต้องการเรียกดูหรือเปลี่ยนแปลง และ *value* คือค่าที่คุณกำลังป้อนลงในการตั้งค่า
- *Setting* อาจประกอบด้วยชื่อมากกว่าหนึ่งชื่อ ยกเว้นเมื่อใช้คำสั่ง **set**
- *Setting* สามารถประกอบด้วยอักขระตัวแทน เช่น ดอกจัน (*) หรือปรัศนี (?)
- *Setting* อาจเป็นได้ทั้งกลุ่ม ชื่อการตั้งค่า หรือ **all**

ตัวอย่างของรูปแบบคำสั่งสำหรับคำสั่ง **asu** จะแสดงในรายการด้านล่างต่อไปนี้:

- หากต้องการแสดงตัวเลือกทั้งหมดสำหรับคำสั่ง asu ให้ป้อนคำสั่ง `asu –help`
- หากต้องการดูรายละเอียดความช่วยเหลือสำหรับคำสั่งทั้งหมด ให้ป้อนคำสั่ง `asu -v –help`
- หากต้องการแสดงรายละเอียดความช่วยเหลือสำหรับคำสั่งเพียงชุดเดียว ให้ป้อนคำสั่ง `asu -v set –help`
- หากต้องการเปลี่ยนค่า ให้ป้อนคำสั่ง `asu set setting value`
- หากต้องการแสดงค่าปัจจุบัน ให้ป้อนคำสั่ง `asu show setting`
- หากต้องการแสดงผลการตั้งค่าในแบบแบทช์ยาว ให้ป้อนคำสั่ง `asu show -l -b all`
- หากต้องการแสดงผลค่าที่เป็นไปได้ทั้งหมดสำหรับการตั้งค่า ให้ป้อนคำสั่ง `asu showvalues setting` ตัวอย่างคำสั่ง show values:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 21. ตัวเลือก asu

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-b	แสดงผลในรูปแบบแบทช์	
–help[1]	แสดงวิธีการใช้คำสั่งและตัวเลือก ตัวเลือก –help จะต้องวางไว้ด้านหน้าของคำสั่ง เช่น **asu –help show**	
–help[1]	แสดงความช่วยเหลือสำหรับคำสั่ง ตัวเลือก –help จะต้องวางไว้ด้านหลังของคำสั่ง เช่น **asu show –help**	
-l	ชื่อการตั้งค่ารูปแบบยาว (รวมชุดการกำหนดค่า)	
-m	ชื่อการตั้งค่ารูปแบบผสม (ใช้ ID การกำหนดค่า)	
-v[2]	เอาต์พุตรายละเอียด	

1. ตัวเลือก –help สามารถใช้กับคำสั่งใดก็ได้
2. ตัวเลือก -v ใช้เฉพาะระหว่าง **asu** และคำสั่งเท่านั้น

รูปแบบคำสั่ง:

```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

หมายเหตุ: ดูที่คำสั่งแต่ละรายการเพื่อดูตัวเลือกคำสั่งเพิ่มเติม

ใช้คำสั่งการดำเนินการ asu เพื่อกำหนดการตั้งค่า UEFI หลายรายการ แล้วสร้างและเรียกใช้คำสั่งโหมดแบบแบตช์ ใช้คำสั่ง **tropen** และ **trset** เพื่อสร้างไฟล์การดำเนินการที่ประกอบด้วยการตั้งค่าหลายรายการสำหรับนำไปใช้ การดำเนินการที่มีการระบุ ID สามารถเปิดใช้ได้ด้วยคำสั่ง **tropen** สามารถใช้คำสั่ง **trset** เพื่อเพิ่มการตั้งค่าลงในชุด สามารถยืนยัน

การดำเนินการที่เสร็จสมบูรณ์ได้ โดยใช้คำสั่ง **trcommit** เมื่อคุณดำเนินการเสร็จเรียบร้อยแล้ว คุณสามารถลบการดำเนินการได้โดยใช้คำสั่ง **trrm**

หมายเหตุ: กระบวนการคืนค่าการตั้งค่า UEFI จะสร้างการดำเนินการพร้อมด้วย ID โดยใช้หมายเลขลำดับแบบสุ่มสามหลัก

ตารางต่อไปนี้ประกอบด้วยคำสั่งการดำเนินการที่ใช้ได้กับคำสั่ง **asu**

ตาราง 22. คำสั่งการดำเนินการ asu

ตารางต่อไปนี้เป็นตารางหลายแถวแบบ 3 คอลัมน์ที่ประกอบด้วยคำสั่งการดำเนินการ รายละเอียดคำสั่ง และค่าของคำสั่งที่เกี่ยวข้อง

คำสั่ง	**รายละเอียด**	**ค่า**
tropen *id*	คำสั่งนี้จะสร้างไฟล์การดำเนินการใหม่ ซึ่งประกอบด้วยการตั้งค่าหลายรายการเพื่อกำหนดค่า	*Id* คือสตริงสำหรับใช้ระบุ ประกอบด้วยตัวอักษรและตัวเลข 1 - 3 หลัก
trset *id*	คำสั่งนี้จะเพิ่มการตั้งค่า หรือคู่ของค่าอย่างน้อยหนึ่งรายการให้กับการดำเนินการ	*Id* คือสตริงสำหรับใช้ระบุ ประกอบด้วยตัวอักษรและตัวเลข 1 - 3 หลัก
trlist *id*	คำสั่งนี้จะแสดงเนื้อหาของไฟล์การดำเนินการก่อนเป็นลำดับแรก ซึ่งมีประโยชน์หากมีการสร้างไฟล์การดำเนินการภายใน CLI Shell	*Id* คือสตริงสำหรับใช้ระบุ ประกอบด้วยตัวอักษรและตัวเลข 1 - 3 หลัก
trcommit *id*	คำสั่งนี้ใช้ยืนยันและดำเนินการเนื้อหาของไฟล์การดำเนินการ ผลลัพธ์และข้อผิดพลาดของการดำเนินการจะแสดงขึ้น	*Id* คือสตริงสำหรับใช้ระบุ ประกอบด้วยตัวอักษรและตัวเลข 1 - 3 หลัก
trrm *id*	คำสั่งนี้ใช้ลบไฟล์การดำเนินการออกหลังจากยืนยันการดำเนินการแล้ว	*Id* คือสตริงสำหรับใช้ระบุ ประกอบด้วยตัวอักษรและตัวเลข 1 - 3 หลัก

ตัวอย่างของการสร้างการตั้งค่า UEFI หลายรายการ:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

คำสั่ง backup

ใช้คำสั่งนี้เพื่อสร้างไฟล์สำรองข้อมูลที่ประกอบด้วยการตั้งค่าการรักษาความปลอดภัยระบบในปัจจุบัน

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 23. คำสั่ง backup

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-f	ชื่อไฟล์สำรองข้อมูล	ชื่อไฟล์ที่ถูกต้อง
-pp	รหัสผ่านหรือวลีรหัสผ่านที่ใช้เข้ารหัสในไฟล์สำรองข้อมูล	รหัสผ่าน หรือวลีรหัสผ่านที่คั่นด้วยอัญประกาศเดี่ยว
-ip	ที่อยู่ IP ของเซิร์ฟเวอร์ TFTP/SFTP	ที่อยู่ IP ที่ถูกต้อง
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP	หมายเลขพอร์ตที่ถูกต้อง (ค่าเริ่มต้นคือ 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP	ชื่อผู้ใช้ที่ถูกต้อง
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP	รหัสผ่านที่ถูกต้อง
-fd	ชื่อไฟล์สำหรับรายละเอียด XML ของคำสั่งสำรองข้อมูลใน CLI	ชื่อไฟล์ที่ถูกต้อง

รูปแบบคำสั่ง:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

ตัวอย่าง:

```
system> backup f xcc-back.cli pp xxxxxx ip 192.168.70.200
```

```
ok
system>
```

คำสั่ง dhcpinfo

ใช้คำสั่งนี้เพื่อดูการกำหนดค่า IP ที่ระบุโดยเซิร์ฟเวอร์ของ DHCP สำหรับ eth0

ใช้คำสั่ง **dhcpinfo** เพื่อดูการกำหนดค่า IP ที่ระบุโดยเซิร์ฟเวอร์ DHCP สำหรับ eth0 หากอินเทอร์เฟซได้รับการกำหนดค่าโดยอัตโนมัติจากเซิร์ฟเวอร์ DHCP คุณสามารถใช้คำสั่ง **ifconfig** เพื่อเปิดหรือปิดใช้งาน DHCP

รูปแบบคำสั่ง:
```
dhcpinfo eth0
```

Example:
```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

ตารางต่อไปนี้จะอธิบายเอาต์พุตจากตัวอย่าง

ตาราง 24. คำสั่ง dhcpinfo

ตารางต่อไปนี้เป็นตารางหลายแถวแบบ 2 คอลัมน์ที่อธิบายตัวเลือกต่างๆ ที่ใช้ในตัวอย่างก่อนหน้า

ตัวเลือก	รายละเอียด
-server	เซิร์ฟเวอร์ DHCP ที่ระบุการกำหนดค่า
-n	ชื่อโฮสต์ที่ระบุ
-i	ที่อยู่ IPv4 ที่ระบุ
-g	ที่อยู่เกตเวย์ที่ระบุ
-s	ซับเน็ตมาสก์ที่ระบุ
-d	ชื่อโดเมนที่ระบุ

ตาราง 24. คำสั่ง dhcpinfo (มีต่อ)

ตัวเลือก	รายละเอียด
-dns1	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv4
-dns2	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv4
-dns3	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv4
-i6	ที่อยู่ IPv6
-d6	ชื่อโดเมน IPv6
-dns61	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv6
-dns62	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv6
-dns63	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv6

คำสั่ง dns

ใช้คำสั่งนี้เพื่อดูและตั้งค่าการกำหนดค่า DNS ของ IMM

หมายเหตุ: ใน Flex System จะไม่สามารถแก้ไขการตั้งค่า DNS ใน IMM การตั้งค่า DNS ได้รับการจัดการโดย CMM

การเรียกใช้คำสั่ง **dns** โดยไม่มีตัวเลือกจะแสดงข้อมูลการกำหนดค่า DNS ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 25. คำสั่ง dns

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-state	สถานะ DNS	on, off
-ddns	สถานะ DDNS	enabled, disabled
-i1	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv4	ที่อยู่ IP ในรูปแบบจุดทศนิยม
-i2	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv4	ที่อยู่ IP ในรูปแบบจุดทศนิยม

ตาราง 25. คำสั่ง dns (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-i3	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv4	ที่อยู่ IP ในรูปแบบจุดทศนิยม
-i61	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv6	ที่อยู่ IP ในรูปแบบ IPv6
-i62	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv6	ที่อยู่ IP ในรูปแบบ IPv6
-i63	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv6	ที่อยู่ IP ในรูปแบบ IPv6
-p	ลำดับความสำคัญของ IPv4/IPv6	ipv4, ipv6

รูปแบบคำสั่ง:
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

หมายเหตุ: ตัวอย่างต่อไปนี้แสดงการกำหนดค่า IMM ที่มีการปิดใช้งาน DNS

ตัวอย่างเช่น:
```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled

system>
```
ตารางต่อไปนี้จะอธิบายตัวเลือกต่างๆ ที่ใช้ในตัวอย่างก่อนหน้า

ตาราง 26. เอาต์พุตคำสั่ง dns

ตารางต่อไปนี้เป็นตารางหลายแถวแบบ 2 คอลัมน์ที่อธิบายตัวเลือกต่างๆ ที่ใช้ในตัวอย่างก่อนหน้า

ตัวเลือก	รายละเอียด
-state	สถานะของ DNS (**on** หรือ **off**)
-i1	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv4
-i2	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv4
-i3	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv4
-i61	ที่อยู่ IP หลักของเซิร์ฟเวอร์ DNS แบบ IPv6
-i62	ที่อยู่ IP ลำดับ 2 ของเซิร์ฟเวอร์ DNS แบบ IPv6
-i63	ที่อยู่ IP ลำดับ 3 ของเซิร์ฟเวอร์ DNS แบบ IPv6
-ddns	สถานะของ DDNS (**enabled** หรือ **disabled**)
-dnsrc	ชื่อโดเมน DDNS ที่ต้องการ (**dhcp** หรือ **manual**)
-ddn	DDN ที่ระบุด้วยตนเอง
-ddncur	DDN ปัจจุบัน (อ่านอย่างเดียว)
-p	เซิร์ฟเวอร์ DNS ที่ต้องการ (**ipv4** หรือ **ipv6**)

คำสั่ง encaps

ใช้คำสั่งนี้เพื่อให้ BMC ออกจากโหมดปกปิด

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 27. คำสั่ง encaps

ตารางต่อไปนี้เป็นตารางหนึ่งแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด
ปิดโหมด Lite	ให้ BMC ออกจากโหมดปกปิดและเปิดการเข้าถึงส่วนกลางไปยังผู้ใช้ทั้งหมด

คำสั่ง ethtousb

ใช้คำสั่ง **ethtousb** เพื่อแสดงและกำหนดค่าการแมปพอร์ตอีเทอร์เน็ตกับ Ethernet-over-USB

คำสั่งนี้ทำให้คุณสามารถแมปหมายเลขพอร์ตอีเทอร์เน็ตภายนอกกับหมายเลขพอร์ตอื่นที่เป็นแบบ Ethernet-over-USB

การเรียกใช้คำสั่ง **ethtousb** โดยไม่มีตัวเลือกจะแสดงข้อมูล Ethernet-over-USB ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 28. คำสั่ง ethtousb

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-en	สถานะ Ethernet-over-USB	enabled, disabled
-m*x*	กำหนดค่าการแมปพอร์ตสำหรับดัชนี *x*	คู่พอร์ต คั่นด้วยเครื่องหมายโคลอน (:) ในรูปแบบ *port1:port2* ที่ซึ่ง: • หมายเลขดัชนีพอร์ต *x* คือเลขจำนวนเต็มตั้งแต่ 1 ถึง 10 ในตัวเลือกคำสั่ง • *port1* ของคู่พอร์ต คือหมายเลขพอร์ตอีเทอร์เน็ตภายนอก • *port2* ของคู่พอร์ต คือหมายเลขพอร์ต Ethernet-over-USB
-rm	ลบการแมปพอร์ตสำหรับดัชนีที่ระบุ	1 ถึง 10 การเรียกใช้คำสั่ง **ethtousb** โดยไม่มีตัวเลือกจะแสดงดัชนีการแมปพอร์ต

รูปแบบคำสั่ง:

```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

ตัวอย่าง:

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
```

system>

คำสั่ง firewall

ใช้คำสั่งนี้เพื่อกำหนดค่าไฟร์วอลล์เพื่อจำกัดการเข้าถึงจากที่อยู่ที่ระบุและเลือกที่จะจำกัดกรอบเวลาการเข้าถึง หากไม่มีการระบุตัวเลือก การตั้งค่าปัจจุบันจะปรากฏขึ้น

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 29. คำสั่ง firewall

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสามคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด	ค่า
-bips	บล็อคที่อยู่ IP 1-3 รายการ (คั่นด้วยเครื่องหมายจุลภาค, CIDR หรือช่วง)	ที่อยู่ IP ที่ถูกต้อง **หมายเหตุ**: ที่อยู่ IPv4 และ IPv6 สามารถใช้รูปแบบ CIDR เพื่อบล็อกช่วงของที่อยู่ได้
-bmacs	บล็อคที่อยู่ MAC 1-3 รายการ (คั่นด้วยเครื่องหมายจุลภาค)	ที่อยู่ MAC ที่ถูกต้อง **หมายเหตุ**: การกรองที่อยู่ MAC จะใช้ได้กับที่อยู่เฉพาะเท่านั้น
-bbd	บล็อควันที่เริ่มต้น	วันที่มีรูปแบบ <YYYY-MM-DD>
-bed	บล็อควันที่สิ้นสุด	วันที่มีรูปแบบ <YYYY-MM-DD>
-bbt	บล็อคเวลาเริ่มต้น	เวลาที่มีรูปแบบ <HH:MM>
-bet	บล็อคเวลาสิ้นสุด	เวลาที่มีรูปแบบ <HH:MM>
-bti	บล็อกช่วงเวลา 1-3 ช่วง (คั่นด้วยเครื่องหมายจุลภาค) เช่น *firewall - bti 01:00–02:00,05:05–10:30* จะบล็อกการเข้าถึงระหว่างช่วงเวลา 01:00-02:00 และ 05:05-10:30 ทุกวัน	ช่วงเวลาที่มีรูปแบบ <HH:MM-HH:MM>
-clr	ล้างข้อมูลกฎของไฟร์วอลล์สำหรับประเภทที่ระบุ	ip, mac, datetime, interval, all
ตัวเลือกต่อไปนี้ใช้สำหรับการบล็อกที่อยู่ IP		

ตาราง 29. คำสั่ง firewall (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-iplp	ระยะเวลาการล็อคที่อยู่ IP เป็นนาที	ตัวเลขตั้งแต่ 0 ถึง 2880, 0 = ไม่หมดอายุ
-iplf	จำนวนสูงสุดของการเข้าสู่ระบบล้มเหลวก่อนที่ที่อยู่ IP จะถูกล็อค **หมายเหตุ**: หากไม่ใช่ 0 ค่านี้จะต้องมากกว่าหรือเท่ากับ <จำนวนสูงสุดของการเข้าสู่ระบบล้มเหลว> ซึ่งตั้งค่าโดย *<accseccfg -lf>*	ตัวเลขตั้งแต่ 0 ถึง 32, 0 = ไม่ล็อค
-ipbl	แสดง/กำหนดค่ารายการที่อยู่ IP ที่ถูกล็อค	del, clrall, show • **-del**: ลบที่อยู่ IPv4 หรือ IPv6 ออกจากรายการบล็อก • **-clrall**: ล้าง IP ที่ถูกบล็อกทั้งหมด • **-show**: แสดง IP ที่ถูกบล็อกทั้งหมด

ตัวอย่าง:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

คำสั่ง gprofile

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าโปรไฟล์แบบกลุ่มสำหรับ IMM

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 30. คำสั่ง gprofile

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 30. คำสั่ง gprofile (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-clear	ลบกลุ่ม	enabled, disabled
-n	ชื่อของกลุ่ม	สตริงที่มีความยาวไม่เกิน 63 อักขระสำหรับ *group_name* ค่า *group_name* จะต้องไม่ซ้ำกัน
-a	ระดับหน่วยงานแบบอิงบทบาท	supervisor, operator, rbs <role list>: nsc|am|rca| rcvma|pr|bc|cel|ac ค่ารายการบทบาทจะมีการระบุโดยใช้การคั่นด้วย เครื่องหมายขีดแนวตั้ง
-h	แสดงวิธีการใช้คำสั่งและตัวเลือก	

รูปแบบคำสั่ง:

```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

คำสั่ง hashpw

ใช้คำสั่งนี้ร่วมกับคำสั่งเสริม -sw เพื่อเปิดใช้งาน/ปิดใช้งานฟังก์ชันรหัสผ่านของบริษัทภายนอก หรือคำสั่งเสริม -re เพื่อเปิดใช้งาน/ปิดใช้งานการอนุญาตให้เรียกรหัสผ่านของบริษัทภายนอก

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 31. คำสั่ง hashpw

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 31. คำสั่ง hashpw (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-sw	สถานะสวิตช์รหัสผ่านของบริษัทภายนอก	enabled, disabled
-re	สถานะการอ่านรหัสผ่านของบริษัทภายนอก **หมายเหตุ**: สามารถตั้งค่าการอ่านได้ หากเปิดใช้งานสวิตช์	enabled, disabled

ตัวอย่าง:

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute               Role             Password Expires
 -------      --------      ------------------               ------             ----------------
    1           USERID                   Native                  Administrator      Password doesn't expire
5           guest5    Third-party Password              Administrator                   90 day(s)
```

คำสั่ง ifconfig

ใช้คำสั่งนี้เพื่อกำหนดค่าอินเทอร์เฟซอีเทอร์เน็ต

พิมพ์ **ifconfig eth0** เพื่อแสดงการกำหนดค่าอินเทอร์เฟซอีเทอร์เน็ตในปัจจุบัน หากต้องการเปลี่ยนการกำหนดค่าอินเทอร์เฟซอีเทอร์เน็ต ให้พิมพ์ตัวเลือกต่างๆ ตามด้วยค่าที่เกี่ยวข้อง หากต้องการเปลี่ยนการกำหนดค่าอินเทอร์เฟซ อย่างน้อยคุณต้องมีสิทธิ์ในการกำหนดค่าการเชื่อมโยงเครือข่ายและการรักษาความปลอดภัยสำหรับอะแดปเตอร์

หมายเหตุ: ใน Flex System การตั้งค่า VLAN จะได้รับการจัดการโดย Flex System CMM และไม่สามารถแก้ไขใน IMM ได้

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 32. คำสั่ง ifconfig

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 32. คำสั่ง ifconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-b	Burned-in MAC Address (อ่านอย่างเดียว ไม่สามารถกำหนดค่าได้)	
-state	สถานะอินเทอร์เฟซ	disabled, enabled
-c	วิธีการกำหนดค่า	dhcp, static, dthens (dthens จะใช้กับตัวเลือก **ลองใช้เซิร์ฟเวอร์ dhcp หากล้มเหลว ให้ใช้การกำหนดค่าแบบคงที่** บนเว็บอินเทอร์เฟซ)
-i	ที่อยู่ IP แบบคงที่	ที่อยู่ในรูปแบบที่ถูกต้อง
-g	ที่อยู่เกตเวย์	ที่อยู่ในรูปแบบที่ถูกต้อง
-s	ซับเน็ตมาสก์	ที่อยู่ในรูปแบบที่ถูกต้อง
-n	ชื่อโฮสต์	สตริงที่มีความยาวไม่เกิน 63 อักขระ สตริงนี้อาจประกอบด้วยตัวอักษร ตัวเลข จุด ขีดล่าง และขีดกลาง
-r	อัตราข้อมูล	10, 100, auto
-d	โหมด Duplex	full, half, auto
-m	MTU	ตัวเลขตั้งแต่ 60 ถึง 1500
-l	LAA	รูปแบบของ MAC address ไม่อนุญาตให้ใช้ Multicast address (ไบต์แรกต้องเป็นเลขคู่)
-dn	ชื่อโดเมน	ชื่อโดเมนในรูปแบบที่ถูกต้อง
-auto	การตั้งค่า Autonegotiation ซึ่งจะกำหนดว่าการตั้งค่าอัตราข้อมูลและเครือข่าย Duplex สามารถกำหนดค่าได้หรือไม่	true, false
-ghn	รับชื่อโฮสต์จาก DHCP	disabled, enabled
-nic	สลับโหมด NIC[1]	shared, dedicated, shared:nixX[2]
-failover[2]	โหมดการทำงานล้มเหลว	none, shared, shared:nicX
-nssync[3]	การซิงโครไนซ์การตั้งค่าเครือข่าย	enabled, disabled

ตาราง 32. คำสั่ง ifconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-address_table	ตารางที่อยู่ IPv6 ที่สร้างขึ้นโดยอัตโนมัติ พร้อมทั้งค่า Prefix length ของที่อยู่ **หมายเหตุ**: ตัวเลือกนี้จะแสดงเฉพาะในกรณีที่เปิดใช้งาน IPv6 และการกำหนดค่าอัตโนมัติแบบสุ่ม	ค่านี้เป็นแบบอ่านอย่างเดียวและไม่สามารถกำหนดค่าได้
-ipv6	สถานะ IPv6	disabled, enabled
-lla	Link-local address **หมายเหตุ**: Link-local address จะแสดงเฉพาะในกรณีที่เปิดใช้งาน IPv6	Link-local address จะกำหนดโดย IMM ค่านี้เป็นแบบอ่านอย่างเดียวและไม่สามารถกำหนดค่าได้
-ipv6static	สถานะ IPv6 แบบคงที่	disabled, enabled
-i6	ที่อยู่ IP แบบคงที่	ที่อยู่ IP แบบคงที่สำหรับอีเทอร์เน็ตช่อง 0 ในรูปแบบ IPv6
-p6	Prefix length ของที่อยู่	ตัวเลขตั้งแต่ 1 ถึง 128
-g6	เกตเวย์หรือเส้นทางที่เป็นค่าเริ่มต้น	ที่อยู่ IP ของเกตเวย์หรือเส้นทางที่เป็นค่าเริ่มต้นสำหรับอีเทอร์เน็ตช่อง 0 ในรูปแบบ IPv6
-dhcp6	สถานะ DHCPv6	enabled, disabled
-sa6	สถานะการกำหนดค่าอัตโนมัติแบบสุ่มของ IPv6	enabled, disabled
-vlan	เปิดหรือปิดใช้งานการแท็ก VLAN	enabled, disabled

ตาราง 32. คำสั่ง ifconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-vlanid	แท็กการระบุแพคเก็ตเครือข่ายสำหรับ IMM	ตัวเลขตั้งแต่ 1 ถึง 4094

หมายเหตุ:

1. -nic ยังจะแสดงสถานะของ nic ด้วย [ใช้งานอยู่] แสดงว่ากำลังใช้งาน nic XCC อยู่ในขณะนี้

   ตัวอย่าง:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   ระบุว่า nic3 อยู่ในโหมดแบบใช้งานร่วมกันในช่องเสียบ 5, nic2 อยู่ในช่องเสียบ 3, nic1 เป็นพอร์ตสำหรับ XCC โดยเฉพาะ และ XCC กำลังใช้ nic3
2. ค่า shared:nicX ใช้ได้กับเซิร์ฟเวอร์ที่มีการ์ดเครือข่าย Mezzanine ที่เป็นตัวเลือกเสริมติดตั้งอยู่ การ์ดเครือข่าย Mezzanine นี้สามารถใช้ได้โดย IMM
3. หาก IMM ถูกกำหนดค่าให้ใช้พอร์ตเครือข่ายการจัดการเฉพาะ ตัวเลือก -failover จะสั่งให้ IMM เปลี่ยนไปใช้พอร์ตเครือข่ายที่ใช้ร่วมกัน หากมีการปลดการเชื่อมต่อพอร์ตเฉพาะออก
4. หากเปิดใช้งานโหมดการทำงานล้มเหลว ตัวเลือก -nssync จะสั่งให้ IMM ใช้การตั้งค่าเครือข่ายเดียวกันกับพอร์ตเครือข่ายการจัดการเฉพาะสำหรับพอร์ตเครือข่ายที่ใช้ร่วมกัน

รูปแบบคำสั่ง:
```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
```

```
  -g6 ipv6_gateway_address
  -p6 length
  -vlan state
  -vlanid VLAN ID
```

ตัวอย่าง:

```
system> ifconfig eth0
-state    :   enabled
-c        :   dthens
-ghn      :   disabled
-i        :   192.168.70.125
-g        :   0.0.0.0
-s        :   255.255.255.0
-n        :   IMM00096B9E003A
-auto     :   true
-r        :   auto
-d        :   auto
-vlan     :   disabled
-vlanid  :   1
-m        :   1500
-b        :   00:09:6B:9E:00:3A
-l        :   00:00:00:00:00:00
-dn       :
-ipv6     :  enabled
-ipv6static :  disabled
-i6       :  ::
-p6       :  64
-g6       :  ::
-dhcp6   :  enabled
-sa6      :  enabled
-lla      :  fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
      nic1: dedicate
      nic2: ext card slot #3
      nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

คำสั่ง keycfg

ใช้คำสั่งนี้เพื่อแสดง เพิ่ม หรือลบคีย์เปิดการทำงาน

สิทธิ์ควบคุมคีย์เปิดการทำงานฟังก์ชัน IMM เสริม

หมายเหตุ:

- เมื่อเรียกใช้คำสั่ง keycfg โดยไม่ระบุตัวเลือก ระบบจะแสดงรายการคีย์เปิดการทำงานที่ติดตั้งไว้ ข้อมูลคีย์ที่แสดงจะประกอบด้วยหมายเลขดัชนีของคีย์เปิดการทำงานแต่ละรายการ ประเภทของคีย์เปิดการทำงาน ช่วงวันที่ที่คีย์ใช้ได้ จำนวนการใช้คงเหลือ สถานะคีย์ และรายละเอียดคีย์
- เพิ่มคีย์เปิดการทำงานใหม่ผ่านการถ่ายโอนไฟล์

- ลบคีย์เก่าโดยระบุหมายเลขคีย์หรือประเภทคีย์ เมื่อลบคีย์ตามประเภท ระบบจะลบเฉพาะคีย์แรกที่พบในประเภทดังกล่าวเท่านั้น

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 33. คำสั่ง keycfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-add	เพิ่มคีย์เปิดการทำงาน	ค่าสำหรับตัวเลือกคำสั่ง -ip, -pn, -u, -pw และ -f
-ip	ที่อยู่ IP ของเซิร์ฟเวอร์ TFTP ซึ่งต้องการเพิ่มคีย์เปิดการทำงาน	ที่อยู่ IP ที่ถูกต้องสำหรับเซิร์ฟเวอร์ TFTP
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP ซึ่งต้องการเพิ่มคีย์เปิดการทำงาน	หมายเลขพอร์ตที่ถูกต้องของเซิร์ฟเวอร์ TFTP/SFTP (ค่าเริ่มต้นคือ 69/22)
-u	ชื่อผู้ใช้ของเซิร์ฟเวอร์ SFTP ซึ่งต้องการเพิ่มคีย์เปิดการทำงาน	ชื่อผู้ใช้ที่ถูกต้องสำหรับเซิร์ฟเวอร์ SFTP
-pw	รหัสผ่านของเซิร์ฟเวอร์ SFTP ซึ่งต้องการเพิ่มคีย์เปิดการทำงาน	รหัสผ่านที่ถูกต้องสำหรับเซิร์ฟเวอร์ SFTP
-f	ชื่อไฟล์ของคีย์เปิดการทำงานที่ต้องการเพิ่ม	ชื่อไฟล์ที่ถูกต้องของไฟล์คีย์เปิดการทำงาน
-del	ลบคีย์เปิดการทำงานตามหมายเลขดัชนี	หมายเลขดัชนีของคีย์เปิดการทำงานที่ถูกต้องจากรายการ **keycfg**
-deltype	ลบคีย์เปิดการทำงานตามประเภทคีย์	ค่าประเภทคีย์ที่ถูกต้อง

รูปแบบคำสั่ง:
```
keycfg [options]
option:
```

```
-add
   -ip tftp/sftp server ip address
   -pn pn port number of tftp/sftp server (default 69/22)
   -u  username for sftp server
   -pw password for sftp server
   -f  filename
   -del   n ( where n is a valid ID number from listing)
   -deltype x ( where x is a Type value)
```

ตัวอย่าง:

```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5               "valid"   "IMM remote presence"
2   3     10/20/2010      2               "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

หมายเหตุ: ฟิลด์**รายละเอียด**ของ ID หมายเลข 3 จะแสดงแยกบรรทัดกันเนื่องจากมีพื้นที่จำกัด

คำสั่ง ldap

ใช้คำสั่งนี้เพื่อแสดงและตั้งค่าพารามิเตอร์การกำหนดค่าโปรโตคอล LDAP

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 34. คำสั่ง ldap

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-a	วิธีการตรวจสอบความถูกต้องของผู้ใช้	local only, LDAP only, local first then LDAP, LDAP first then local
-aom	โหมดตรวจสอบความถูกต้องเท่านั้น	enabled, disabled
-b	วิธีการ Binding	anonymous, bind with ClientDN and password, bind with Login Credential
-c	ชื่อที่ใช้ระบุไคลเอ็นต์	สตริงที่มีความยาวไม่เกิน 127 อักขระสำหรับ *client_dn*
-d	โดเมนการค้นหา	สตริงที่มีความยาวไม่เกิน 63 อักขระสำหรับ *search_domain*
-f	ตัวกรองกลุ่ม	สตริงที่มีความยาวไม่เกิน 127 อักขระสำหรับ *group_filter*

ตาราง 34. คำสั่ง ldap (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-fn	ชื่อฟอเรสต์	สำหรับการทำงานในระบบ Active Directory สตริงที่มีความยาวไม่เกิน 127 อักขระ
-g	แอตทริบิวต์การค้นหากลุ่ม	สตริงที่มีความยาวไม่เกิน 63 อักขระสำหรับ *group_search_attr*
-l	แอตทริบิวต์สิทธิ์การเข้าใช้งาน	สตริงที่มีความยาวไม่เกิน 63 อักขระสำหรับ *string*
-p	รหัสผ่านไคลเอ็นต์	สตริงที่มีความยาวไม่เกิน 15 อักขระสำหรับ *client_pw*
-pc	ยืนยันรหัสผ่านไคลเอ็นต์	สตริงที่มีความยาวไม่เกิน 15 อักขระสำหรับ *confirm_pw* วิธีการใช้คำสั่งคือ: ldap -p *client_pw* -pc *confirm_pw* คุณต้องใช้ตัวเลือกนี้ในกรณีที่เปลี่ยนรหัสผ่านไคลเอ็นต์ โดยจะเปรียบเทียบอาร์กิวเมนต์ *confirm_pw* กับอาร์กิวเมนต์ *client_pw* คำสั่งนี้จะทำงานไม่สำเร็จหากอาร์กิวเมนต์ไม่ตรงกัน
-ep	รหัสผ่านแบบเข้ารหัส	สำรอง/กู้คืนรหัสผ่าน (ใช้ภายในเท่านั้น)
-r	ชื่อที่ใช้ระบุ (DN) รายการรูท	สตริงที่มีความยาวไม่เกิน 127 อักขระสำหรับ *root_dn*
-rbs	ระบบการรักษาความปลอดภัยตามบทบาท (RBS) ที่ปรับปรุงใหม่สำหรับผู้ใช้ Active Directory	enabled, disabled
-s1ip	ชื่อโฮสต์/ที่อยู่ IP ของเซิร์ฟเวอร์ 1	สตริงที่มีความยาวไม่เกิน 127 อักขระหรือที่อยู่ IP สำหรับ *host name/ip_addr*
-s2ip	ชื่อโฮสต์/ที่อยู่ IP ของเซิร์ฟเวอร์ 2	สตริงที่มีความยาวไม่เกิน 127 อักขระหรือที่อยู่ IP สำหรับ *host name/ip_addr*
-s3ip	ชื่อโฮสต์/ที่อยู่ IP ของเซิร์ฟเวอร์ 3	สตริงที่มีความยาวไม่เกิน 127 อักขระหรือที่อยู่ IP สำหรับ *host name/ip_addr*
-s4ip	ชื่อโฮสต์/ที่อยู่ IP ของเซิร์ฟเวอร์ 4	สตริงที่มีความยาวไม่เกิน 127 อักขระหรือที่อยู่ IP สำหรับ *host name/ip_addr*
-s1pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ 1	หมายเลขพอร์ตไม่เกิน 5 หลักสำหรับ *port_number*

ตาราง 34. คำสั่ง ldap (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-s2pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ 2	หมายเลขพอร์ตไม่เกิน 5 หลักสำหรับ *port_number*
-s3pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ 3	หมายเลขพอร์ตไม่เกิน 5 หลักสำหรับ *port_number*
-s4pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ 4	หมายเลขพอร์ตไม่เกิน 5 หลักสำหรับ *port_number*
-t	ชื่อเป้าหมายของเซิร์ฟเวอร์	เมื่อเปิดใช้งานตัวเลือก RBS ฟิลด์นี้จะระบุชื่อเป้าหมายที่สามารถเชื่อมโยงกับบทบาทอย่างน้อยหนึ่งรายการบนเซิร์ฟเวอร์ Active Directory ผ่านเครื่องมือ Snap-In ของระบบการรักษาความปลอดภัยตามบทบาท (RBS)
-u	แอตทริบิวต์การค้นหา UID	สตริงที่มีความยาวไม่เกิน 63 อักขระสำหรับ *search_attrib*
-v	เรียกที่อยู่เซิร์ฟเวอร์ LDAP ผ่านทาง DNS	off, on
-h	แสดงวิธีการใช้คำสั่งและตัวเลือกต่างๆ	

รูปแบบคำสั่ง:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
```

```
-t name
-u search_attrib
-v off|on
-h
```

คำสั่ง ntp

ใช้คำสั่งนี้เพื่อแสดงและกำหนดค่าโปรโตคอลเวลาเครือข่าย (NTP)

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 35. คำสั่ง ntp

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-en	เปิดหรือปิดใช้งานโปรโตคอลเวลาเครือข่าย	enabled, disabled
-i[1]	ชื่อหรือที่อยู่ IP ของเซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย นี่คือหมายเลขดัชนีของเซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย	ชื่อของเซิร์ฟเวอร์ NTP ที่จะใช้ในการซิงโครไนซ์นาฬิกา หมายเลขดัชนีของเซิร์ฟเวอร์ NTP จะอยู่ในช่วง -i1 ถึง -i4
-f	ความถี่ (เป็นนาที) ที่นาฬิกา IMM ได้รับการซิงโครไนซ์กับเซิร์ฟเวอร์โปรโตคอลเวลาเครือข่าย	3 - 1440 นาที
-synch	ร้องขอการซิงโครไนซ์กับเซิร์ฟเวอร์โปรโตคอลเวลาเครือข่ายทันที	ไม่มีค่าที่จะใช้กับพารามิเตอร์นี้

1. -i จะมีผลเหมือนกับ i1

รูปแบบคำสั่ง:

```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

ตัวอย่าง:

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

คำสั่ง portcfg

ใช้คำสั่งนี้เพื่อกำหนดค่า IMM สำหรับคุณลักษณะการเปลี่ยนเส้นทางอนุกรม

IMM ต้องได้รับการกำหนดค่าให้ตรงกับการตั้งค่าพอร์ตอนุกรมภายในของเซิร์ฟเวอร์ หากต้องการเปลี่ยนการกำหนดค่าพอร์ต ให้พิมพ์ตัวเลือกต่างๆ ตามด้วยค่าที่เกี่ยวข้อง หากต้องการเปลี่ยนการกำหนดค่าพอร์ตอนุกรม อย่างน้อย คุณต้องมีสิทธิ์ในการกำหนดค่าการเชื่อมโยงเครือข่ายและการรักษาความปลอดภัยสำหรับอะแดปเตอร์

หมายเหตุ: สำหรับฟังก์ชัน IPMI นั้น IMM จะใช้ได้เฉพาะพอร์ตอนุกรมภายนอกของเซิร์ฟเวอร์เท่านั้น ไม่รองรับ CLI เมื่อใช้พอร์ตอนุกรม ไม่รองรับตัวเลือก **serred** และ **cliauth** ที่เดิมมีอยู่ใน Remote Supervisor Adapter II CLI

การเรียกใช้คำสั่ง **portcfg** โดยไม่มีตัวเลือกจะแสดงข้อมูลการกำหนดค่าพอร์ตอนุกรม ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

หมายเหตุ: จำนวนบิตข้อมูล (8) ถูกตั้งค่าไว้ในฮาร์ดแวร์และไม่สามารถเปลี่ยนแปลงได้

ตาราง 36. คำสั่ง portcfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-b	อัตรา Baud	9600, 19200, 38400, 57600, 115200
-p	Parity	none, odd, even
-s	บิต Stop	1, 2
-climode	โหมด CLI	0, 1, 2 ที่ซึ่ง: • 0 = none: CLI ถูกปิดใช้งาน • 1 = cliems: CLI เปิดใช้งานพร้อมลำดับการกดปุ่มที่ใช้ได้กับ EMS • 2 = cliuser: CLI เปิดใช้งานพร้อมลำดับการกดปุ่มที่ผู้ใช้กำหนด

รูปแบบคำสั่ง:

```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

ตัวอย่าง:

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

คำสั่ง portcontrol

ใช้คำสั่งนี้เพื่อเปิดหรือปิดพอร์ตการบริการเครือข่าย

ณ ปัจจุบัน คำสั่งนี้รองรับเฉพาะการควบคุมพอร์ตของโปรโตคอล IPMI เท่านั้น พิมพ์ **portcontrol** เพื่อแสดงสถานะของพอร์ต IPMI หากต้องการเปิดใช้งานหรือปิดใช้งานพอร์ตเครือข่าย IPMI ให้ป้อนตัวเลือก **-ipmi** ตามด้วยค่า **on** หรือ **off**

ตาราง 37. คำสั่ง portcontrol

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-all	เปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซและโปรโตคอลทั้งหมด	on, off
-cim	เปิดใช้งานหรือปิดใช้งานการค้นหา CIM	on, off
-ipmi	เปิดใช้งานหรือปิดใช้งานการเข้าถึง ipmi ผ่าน LAN	on, off
-ipmi-kcs	เปิดใช้งานหรือปิดใช้งานการเข้าถึง ipmi จากเซิร์ฟเวอร์	on, off
-rest	เปิดใช้งานหรือปิดใช้งานการค้นหา REST	on, off

ตาราง 37. คำสั่ง portcontrol (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-slp	เปิดใช้งานหรือปิดใช้งานการค้นหา SLP	on, off
-snmp	เปิดใช้งานหรือปิดใช้งานการค้นหา SNMP	on, off
-ssdp	เปิดใช้งานหรือปิดใช้งานการค้นหา SSDP	on, off
-cli	เปิดใช้งานหรือปิดใช้งานการค้นหา CLI	on, off
-web	เปิดใช้งานหรือปิดใช้งานการค้นหา WEB	on, off

รูปแบบคำสั่ง:
```
portcontrol [options]
 options:
   -ipmi on/off
```

ตัวอย่าง:
```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

คำสั่ง ports

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าพอร์ต IMM

การเรียกใช้คำสั่ง **ports** โดยไม่มีตัวเลือกจะแสดงข้อมูลสำหรับพอร์ต IMM ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 38. คำสั่ง ports

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-open	แสดงพอร์ตที่เปิดอยู่	
-reset	รีเซ็ตพอร์ตเป็นการตั้งค่าเริ่มต้น	
-httpp	หมายเลขพอร์ต HTTP	หมายเลขพอร์ตเริ่มต้น: 80
-httpsp	หมายเลขพอร์ต HTTPS	หมายเลขพอร์ตเริ่มต้น: 443
-sshp	หมายเลขพอร์ต CLI เดิมของ SSH	หมายเลขพอร์ตเริ่มต้น: 22
-snmpap	หมายเลขพอร์ตเอเจนต์ SNMP	หมายเลขพอร์ตเริ่มต้น: 161
-snmptp	หมายเลขพอร์ต SNMP traps	หมายเลขพอร์ตเริ่มต้น: 162
-rpp	หมายเลขพอร์ต Remote Presence	หมายเลขพอร์ตเริ่มต้น: 3900
-cimhp	หมายเลขพอร์ต CIM over HTTP	หมายเลขพอร์ตเริ่มต้น: 5988
-cimhsp	หมายเลขพอร์ต CIM over HTTPS	หมายเลขพอร์ตเริ่มต้น: 5989

รูปแบบคำสั่ง:
```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

ตัวอย่างเช่น:
```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
```

```
-cimhp 5988
-cimhsp 5989
system>
```

คำสั่ง rdmount

ใช้คำสั่งนี้เพื่อเมาท์อิมเมจดิสก์ระยะไกลหรือการแชร์เครือข่าย

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 39. คำสั่ง rdmount

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

หมายเหตุ:

- สามารถอัปโหลดไฟล์ลงในหน่วยความจำของ XClarity Controller ได้สูงสุดสองไฟล์ และเมาท์เป็นสื่อเสมือนโดยใช้คุณลักษณะ RDOC ของ XClarity Controller ขนาดรวมของไฟล์ทั้งสองไฟล์ต้องไม่เกิน 50 MB อิมเมจที่อัปโหลดจะเป็นแบบอ่านอย่างเดียว เว้นแต่จะใช้ตัวเลือก –rw
- เมื่อใช้โปรโตคอล HTTP, SFTP หรือ FTP เพื่อเมาท์หรือแม็ปอิมเมจ ขนาดรวมของอิมเมจทั้งหมดจะต้องไม่เกิน 50 MB จะไม่มีการจำกัดขนาด หากใช้โปรโตคอล NFS หรือ SAMBA

ตาราง 39. คำสั่ง rdmount (มีต่อ)

ตัวเลือก	รายละเอียด
-r	rdoc operation (หากใช้จะต้องเป็นตัวเลือกแรก) -r -map: เมาท์อิมเมจ RDOC -r -unmap<filename>: ยกเลิกการเมาท์อิมเมจ RDOC ที่เมาท์ไป -r -maplist: แสดงอิมเมจ RDOC ที่เมาท์ผ่านเว็บเบราเซอร์ XClarity Controller และอินเทอร์เฟซ CLI
-map	-t <samba|nfs|http|sftp|ftp> ประเภท filesystem -ro อ่านอย่างเดียว -rw อ่านและเขียน -u ผู้ใช้ -p รหัสผ่าน -l ตำแหน่งที่ตั้งไฟล์ (รูปแบบ URL) -o ตัวเลือก (สตริงตัวเลือกพิเศษสำหรับเมาท์ samba และ nfs) -d โดเมน (โดเมนสำหรับเมาท์ samba)
-maplist	แสดงอิมเมจที่แม็ป
-unmap <id|fname>	ใช้ ID ที่มีอิมเมจเครือข่าย ไฟล์ที่มีชื่อ rdoc
-mount	เมาท์อิมเมจที่แม็ป
-unmount	ยกเลิกการเมาท์อิมเมจที่เมาท์ไป

คำสั่ง restore

ใช้คำสั่งนี้เพื่อคืนค่าการตั้งค่าระบบจากไฟล์สำรองข้อมูล

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 40. คำสั่ง restore

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-f	ชื่อไฟล์สำรองข้อมูล	ชื่อไฟล์ที่ถูกต้อง
-pp	รหัสผ่านหรือวลีรหัสผ่านที่ใช้เข้ารหัสในไฟล์สำรองข้อมูล	รหัสผ่าน หรือวลีรหัสผ่านที่คั่นด้วยอัญประกาศเดี่ยว
-ip	ที่อยู่ IP ของเซิร์ฟเวอร์ TFTP/SFTP	ที่อยู่ IP ที่ถูกต้อง
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP	หมายเลขพอร์ตที่ถูกต้อง (ค่าเริ่มต้นคือ 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP	ชื่อผู้ใช้ที่ถูกต้อง
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP	รหัสผ่านที่ถูกต้อง

รูปแบบคำสั่ง:
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

ตัวอย่าง:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

คำสั่ง restoredefaults

ใช้คำสั่งนี้เพื่อคืนค่าการตั้งค่า IMM ทั้งหมดเป็นค่าเริ่มต้นจากโรงงาน

- ไม่มีตัวเลือกสำหรับคำสั่ง restoredefaults
- ระบบจะขอให้คุณยืนยันคำสั่งก่อนที่จะประมวลผล

รูปแบบคำสั่ง:
```
restoredefaults
```

ตัวอย่าง:

```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

คำสั่ง roles

ใช้คำสั่งนี้เพื่อแสดงผลหรือกำหนดค่าบทบาท

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 41. คำสั่ง roles

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 41. คำสั่ง roles (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-n	บทบาทที่ต้องการกำหนดค่า	ความยาวไม่เกิน 32 อักขระ
-p	ตั้งค่าสิทธิพิเศษ	custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: การเข้าถึงการจัดการบัญชีผู้ใช้ • **rca**: การเข้าถึงคอนโซลระยะไกล • **rcvma**: การเข้าถึงคอนโซลระยะไกลและดิสก์ระยะไกล (สื่อเสมือน) • **pr**: การเข้าถึงการเปิด/รีสตาร์ทเซิร์ฟเวอร์จากระยะไกล • **cel**: ความสามารถในการล้างข้อมูลบันทึกเหตุการณ์ • **bc**: การกำหนดค่าอะแดปเตอร์ (พื้นฐาน) • **nsc**: การกำหนดค่าอะแดปเตอร์ (เครือข่ายและการรักษาความปลอดภัย) • **ac**: การกำหนดค่าอะแดปเตอร์ (ขั้นสูง) • **us**: การรักษาความปลอดภัย UEFI **หมายเหตุ**: สามารถใช้แฟล็กสิทธิ์แบบกำหนดเองข้างต้นร่วมกันในแบบใดก็ได้
d	ลบแถว	

รูปแบบคำสั่ง

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

ตัวอย่าง

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok


system> roles
Account              Role                              Privilege                    Assigned To
------- ----------------------------------   -------------------------     -------------------------------
    0                    Administrator                      all                        USERID
    1                         ReadOnly                        none
    2                         Operator                custom:pr|cel|bc|nsc
    3                            test1                 custom:am|rca|rcvma
```

คำสั่ง seccfg

ใช้คำสั่งนี้เพื่อดำเนินการย้อนกลับเฟิร์มแวร์

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 42. คำสั่ง seccfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด	ค่า
-fwrb	อนุญาตการย้อนกลับเฟิร์มแวร์เป็นเวอร์ชันก่อนหน้า	yes, no
-aubp	เปิดหรือปิดฟังก์ชันการสำรองข้อมูลอัตโนมัติไปยังโปรโมชันหลัก	enabled, disabled

คำสั่ง set

ใช้คำสั่งนี้เพื่อเปลี่ยนแปลงการตั้งค่า IMM บางอย่าง

- การตั้งค่า IMM บางอย่างสามารถเปลี่ยนแปลงได้ด้วยการใช้แค่คำสั่ง **set** พื้นฐาน
- การตั้งค่าบางอย่างในนี้ เช่น ตัวแปรสภาพแวดล้อม จะใช้โดย CLI

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 43. คำสั่ง set

ตารางต่อไปนี้เป็นตารางแถวเดียวจำนวน 3 คอลัมน์ที่ประกอบด้วยรายละเอียดคำสั่งและข้อมูลที่เกี่ยวข้อง

ตาราง 43. คำสั่ง set (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
ค่า	กำหนดค่าสำหรับพาธหรือการตั้งค่าที่ระบุ	ค่าที่เหมาะสมสำหรับพาธหรือการตั้งค่าที่ระบุ

รูปแบบคำสั่ง:
```
set [options]
option:
  value
```

คำสั่ง smtp

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดการตั้งค่าสำหรับอินเทอร์เฟซ SMTP

การเรียกใช้คำสั่ง **smtp** โดยไม่มีตัวเลือกจะแสดงข้อมูลอินเทอร์เฟซ SMTP ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 44. คำสั่ง smtp

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-auth	รองรับการตรวจสอบความถูกต้องของ SMTP	enabled, disabled
-authepw	รหัสผ่านแบบเข้ารหัสสำหรับการตรวจสอบความถูกต้องของ SMTP	สตริงรหัสผ่านที่ถูกต้อง
-authmd	วิธีการตรวจสอบความถูกต้องของ SMTP	CRAM-MD5, LOGIN
-authn	ชื่อผู้ใช้ในการตรวจสอบความถูกต้องของ SMTP	สตริง (ความยาวไม่เกิน 256 อักขระ)
-authpw	รหัสผ่านสำหรับการตรวจสอบความถูกต้องของ SMTP	สตริง (ความยาวไม่เกิน 256 อักขระ)
-pn	หมายเลขพอร์ต SMTP	หมายเลขพอร์ตที่ถูกต้อง
-s	ที่อยู่ IP หรือชื่อโฮสต์ของเซิร์ฟเวอร์ SMTP	ที่อยู่ IP หรือชื่อโฮสต์ที่ถูกต้อง (ความยาวไม่เกิน 63 อักขระ)

รูปแบบคำสั่ง:
```
smtp [options]
```

```
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

ตัวอย่าง:

```
system> smtp
-s test.com
-pn 25
system>
```

คำสั่ง snmp

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าข้อมูลอินเทอร์เฟซ SNMP

การเรียกใช้คำสั่ง **snmp** โดยไม่มีตัวเลือกจะแสดงข้อมูลอินเทอร์เฟซ SNMP ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 45. คำสั่ง snmp

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-a3	SNMPv3 agent	on, off **หมายเหตุ**: ในการเปิดใช้งาน SNMPv3 agent จะต้องมีคุณสมบัติตามเกณฑ์ต่อไปนี้: • ผู้ติดต่อ IMM ที่ระบุโดยใช้ตัวเลือกคำสั่ง -cn • ตำแหน่งที่ตั้ง IMM ที่ระบุโดยใช้ตัวเลือกคำสั่ง -l
-t1	SNMPv1 traps	on, off
-t2	SNMPv2 traps	on, off
-t	SNMPv3 traps	on, off

ตาราง 45. คำสั่ง snmp (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-l	ตำแหน่งที่ตั้ง IMM	สตริง (ความยาวไม่เกิน 47 อักขระ) **หมายเหตุ**: • อาร์กิวเมนต์ที่มีช่องว่างต้องล้อมรอบด้วยเครื่องหมายคำพูด ไม่อนุญาตให้มีช่องว่างนำหน้าหรือต่อท้ายอาร์กิวเมนต์ • ล้างข้อมูลตำแหน่งที่ตั้ง IMM โดยไม่ระบุอาร์กิวเมนต์ใดเลย หรือระบุสตริงว่างเป็นอาร์กิวเมนต์ เช่น “”
-cn	ชื่อผู้ติดต่อ IMM	สตริง (ความยาวไม่เกิน 47 อักขระ) **หมายเหตุ**: • อาร์กิวเมนต์ที่มีช่องว่างต้องล้อมรอบด้วยเครื่องหมายคำพูด ไม่อนุญาตให้มีช่องว่างนำหน้าหรือต่อท้ายอาร์กิวเมนต์ • ล้างข้อมูลชื่อผู้ติดต่อ IMM โดยไม่ระบุอาร์กิวเมนต์ใดเลย หรือระบุสตริงว่างเป็นอาร์กิวเมนต์ เช่น “”
-c	ชื่อ SNMP community	สตริง (ความยาวไม่เกิน 15 อักขระ) **หมายเหตุ**: • อาร์กิวเมนต์ที่มีช่องว่างต้องล้อมรอบด้วยเครื่องหมายคำพูด ไม่อนุญาตให้มีช่องว่างนำหน้าหรือต่อท้ายอาร์กิวเมนต์ • ล้างชื่อ SNMP community โดยไม่ระบุอาร์กิวเมนต์ใดเลย หรือระบุสตริงว่างเป็นอาร์กิวเมนต์ เช่น“”
-ct	ชื่อกลุ่ม SNMPv2 trap	สตริง (ความยาวไม่เกิน 15 อักขระ) **หมายเหตุ**: • อาร์กิวเมนต์ที่มีช่องว่างต้องล้อมรอบด้วยเครื่องหมายคำพูด ไม่อนุญาตให้มีช่องว่างนำหน้าหรือต่อท้ายอาร์กิวเมนต์ • ล้างข้อมูลชื่อผู้ติดต่อ IMM โดยไม่ระบุอาร์กิวเมนต์ใดเลย หรือระบุสตริงว่างเป็นอาร์กิวเมนต์ เช่น ""

ตาราง 45. คำสั่ง snmp (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-ci	ที่อยู่ IP หรือชื่อโฮสต์ของ SNMP community	ที่อยู่ IP หรือชื่อโฮสต์ที่ถูกต้อง (ความยาวไม่เกิน 63 อักขระ) **หมายเหตุ**: • ที่อยู่ IP หรือชื่อโฮสต์สามารถมีจุด ขีดล่าง ขีดกลาง ตัวอักษร และตัวเลขได้เท่านั้น ไม่อนุญาตให้มีช่องว่างหรือจุดต่อกัน • ล้างข้อมูลที่อยู่ IP หรือชื่อโฮสต์ของ SNMP Community โดยไม่ระบุอาร์กิวเมนต์ใดเลย
-cti	ชื่อโฮสต์/ที่อยู่ IP กลุ่ม SNMPv2 trap	ที่อยู่ IP หรือชื่อโฮสต์ที่ถูกต้อง (ความยาวไม่เกิน 63 อักขระ) **หมายเหตุ**: • ที่อยู่ IP หรือชื่อโฮสต์สามารถมีจุด ขีดล่าง ขีดกลาง ตัวอักษร และตัวเลขได้เท่านั้น ไม่อนุญาตให้มีช่องว่างหรือจุดต่อกัน • ล้างข้อมูลที่อยู่ IP หรือชื่อโฮสต์ของ SNMP Community โดยไม่ระบุอาร์กิวเมนต์ใดเลย
-eid	รหัสเอนจิน SNMP	สตริง (ความยาวไม่เกิน 1 ถึง 27 อักขระ)

รูปแบบคำสั่ง:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

ตัวอย่าง:
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
```

```
-eid XCC-7Z70-DSYM09X
system>
```

คำสั่ง snmpalerts

ใช้คำสั่งนี้เพื่อจัดการการแจ้งเตือนที่ส่งทาง SNMP

การเรียกใช้ **snmpalerts** โดยไม่มีตัวเลือกจะแสดงการตั้งค่าการแจ้งเตือน SNMP ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 46. คำสั่ง snmpalerts

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-status	สถานะการแจ้งเตือน SNMP	on, off
-crt	ตั้งค่าเหตุการณ์ร้ายแรงที่จะส่งการแจ้งเตือน	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot ระบุการตั้งค่าการแจ้งเตือนร้ายแรงที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **snmpalerts -crt custom:te|vo** ส่วนที่เป็นค่าที่กำหนดเองคือ: • te: อุณหภูมิเกินเกณฑ์ร้ายแรงที่กำหนด • vo: แรงดันไฟฟ้าเกินเกณฑ์ร้ายแรงที่กำหนด • po: ระบบไฟฟ้าขัดข้องร้ายแรง • di: ฮาร์ดดิสก์ไดรฟ์ขัดข้อง • fa: พัดลมขัดข้อง • cp: ไมโครโปรเซสเซอร์ขัดข้อง • me: หน่วยความจำขัดข้อง • in: ฮาร์ดแวร์ใช้ร่วมกันไม่ได้ • re: การสำรองพลังงานขัดข้อง • ot: เหตุการณ์ร้ายแรงอื่นๆ
-crten	ส่งการแจ้งเตือนเหตุการณ์ร้ายแรง	enabled, disabled

ตาราง 46. คำสั่ง snmpalerts (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-wrn	ตั้งค่าเหตุการณ์ระดับคำเตือนที่จะส่งการแจ้งเตือน	all, none, custom:rp|te|vo|po|fa|cp|me|ot ระบุการตั้งค่าการแจ้งเตือนระดับคำเตือนที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **snmpalerts -wrn custom:rp|te** ส่วนที่เป็นค่าที่กำหนดเองคือ: • rp: คำเตือนเรื่องการสำรองพลังงาน • te: อุณหภูมิเกินเกณฑ์ระดับคำเตือนที่กำหนด • vo: แรงดันไฟฟ้าเกินเกณฑ์ระดับคำเตือนที่กำหนด • po: พลังงานเกินเกณฑ์ระดับคำเตือนที่กำหนด • fa: เหตุการณ์ที่ไม่ร้ายแรงเกี่ยวกับพัดลม • cp: ไมโครโปรเซสเซอร์มีประสิทธิภาพลดลง • me: คำเตือนเกี่ยวกับหน่วยความจำ • ot: เหตุการณ์ระดับคำเตือนอื่นๆ
-wrnen	ส่งการแจ้งเตือนเหตุการณ์ระดับคำเตือน	enabled, disabled
-sys	ตั้งค่าเหตุการณ์ประจำที่จะส่งการแจ้งเตือน	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne ระบุการตั้งค่าการแจ้งเตือนประจำที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **snmpalerts -sys custom:lo|tio** ส่วนที่เป็นค่าที่กำหนดเองคือ: • lo: การเข้าใช้งานระยะไกลสำเร็จ • tio: ระบบปฏิบัติการถึงเวลาไทม์เอาต์ • ot: เหตุการณ์อื่นๆ เกี่ยวกับข้อมูลและระบบ • po: เปิด/ปิดพลังงานของระบบ • bf: การบูตระบบปฏิบัติการขัดข้อง • til: โปรแกรมเฝ้าระวังตัวโหลดระบบปฏิบัติการถึงเวลาไทม์เอาต์ • pf: ความขัดข้องที่คาดการณ์ไว้ (PFA) • el: บันทึกเหตุการณ์ใช้ไปแล้ว 75% • ne: เปลี่ยนเครือข่าย
-sysen	ส่งการแจ้งเตือนเหตุการณ์ประจำ	enabled, disabled

รูปแบบคำสั่ง:
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

คำสั่ง srcfg

ใช้คำสั่งนี้เพื่อระบุลำดับการกดปุ่มเพื่อเข้าสู่ CLI จากโหมดการเปลี่ยนเส้นทางพอร์ตอนุกรม

หากต้องการเปลี่ยนการกำหนดค่าการเปลี่ยนเส้นทางพอร์ตอนุกรม ให้พิมพ์ตัวเลือกต่างๆ ตามด้วยค่าที่เกี่ยวข้อง หากต้องการเปลี่ยนการกำหนดค่าการเปลี่ยนเส้นทางพอร์ตอนุกรม อย่างน้อย คุณต้องมีสิทธิ์ในการกำหนดค่าการเชื่อมโยงเครือข่ายและการรักษาความปลอดภัยสำหรับอะแดปเตอร์

หมายเหตุ: ฮาร์ดแวร์ IMM ไม่มีความสามารถในการสอดผ่านพอร์ตอนุกรม ดังนั้น จึงไม่รองรับตัวเลือก `-passthru` และ `entercliseq` ซึ่งมีอยู่ใน Remote Supervisor Adapter II CLI

การเรียกใช้คำสั่ง **srcfg** โดยไม่มีตัวเลือกจะแสดงลำดับการกดปุ่มเปลี่ยนเส้นทางพอร์ตอนุกรมปัจจุบัน ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกคำสั่ง `srcfg -entercliseq`

ตาราง 47. คำสั่ง srcfg

ตารางต่อไปนี้เป็นตารางแถวเดียวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และข้อมูลค่าของตัวเลือกนั้นๆ

ตัวเลือก	รายละเอียด	ค่า
-entercliseq	ป้อนลำดับการกดปุ่ม CLI	ลำดับการกดปุ่มที่ผู้ใช้กำหนดในการเข้าสู่ CLI **หมายเหตุ**: ลำดับนี้ต้องมีอักขระอย่างน้อยหนึ่งตัวและไม่เกิน 15 ตัว สัญลักษณ์ Caret (^) มีความหมายพิเศษในลำดับนี้ โดยจะใช้แทนปุ่ม Ctrl ที่ตรงกับลำดับการกดปุ่ม Ctrl (เช่น ^[ใช้แทนการกด Esc และ ^M ใช้แทนการขึ้นบรรทัดใหม่แบบ CR) ระบบจะตีความ ^ ในทุกตำแหน่งว่าเป็นลำดับการกด Ctrl โปรดดูตารางการแปลง ASCII-to-key เพื่อดูรายการลำดับการกด Ctrl ทั้งหมด ค่าเริ่มต้นของฟิลด์นี้คือ ^[(ซึ่งก็คือ Esc ตามด้วย (

รูปแบบคำสั่ง:

```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

ตัวอย่าง:

```
system> srcfg
-entercliseq ^[Q
system>
```

คำสั่ง sshcfg

ใช้คำสั่งนี้เพื่อแสดงและกำหนดค่าพารามิเตอร์ SSH

การเรียกใช้คำสั่ง **sshcfg** โดยไม่มีตัวเลือกจะแสดงพารามิเตอร์ SSH ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 48. คำสั่ง sshcfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-cstatus	สถานะของ SSH CLI	enabled, disabled
-hk gen	สร้างคีย์ส่วนตัวของเซิร์ฟเวอร์ SSH	
-hk rsa	แสดงคีย์สาธารณะ RSA ของเซิร์ฟเวอร์	

รูปแบบคำสั่ง:

```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

ตัวอย่าง:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

คำสั่ง ssl

ใช้คำสั่งนี้เพื่อแสดงและกำหนดค่าพารามิเตอร์ SSL

ในการเปิดใช้งานไคลเอ็นต์ SSL ต้องติดตั้งใบรับรองของไคลเอ็นต์ การเรียกใช้คำสั่ง **ssl** โดยไม่มีตัวเลือกจะแสดงพารามิเตอร์ SSL ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 49. คำสั่ง ssl

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-ce	เปิดใช้งานหรือปิดใช้งานไคลเอ็นต์ SSL	on, off
-se	เปิดใช้งานหรือปิดใช้งานเซิร์ฟเวอร์ SSL	on, off
-cime	เปิดใช้งานหรือปิดใช้งาน CIM ผ่าน HTTPS บนเซิร์ฟเวอร์ SSL	on, off

รูปแบบคำสั่ง:
```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

พารามิเตอร์: พารามิเตอร์ต่อไปนี้ปรากฏอยู่ในการแสดงสถานะตัวเลือกสำหรับคำสั่ง **ssl** และเป็นผลลัพธ์จาก CLI เท่านั้น:

เปิดใช้งานการส่งที่ปลอดภัยผ่านเซิร์ฟเวอร์

การแสดงสถานะนี้เป็นแบบ read-only และไม่สามารถตั้งค่าได้โดยตรง

สถานะคีย์เซิร์ฟเวอร์เว็บ/CMD

การแสดงสถานะนี้เป็นแบบ read-only และไม่สามารถตั้งค่าได้โดยตรง ค่าผลลัพธ์บรรทัดคำสั่งที่เป็นไปได้มีดังต่อไปนี้:

คีย์ส่วนตัวและ Cert/CSR ไม่พร้อมใช้งาน

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามโดย CA แล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองที่สร้างขึ้นโดยอัตโนมัติแล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองแล้ว

จัดเก็บคีย์ส่วนตัวแล้ว, CSR พร้อมให้ดาวน์โหลด

สถานะคีย์ CSR **ของเซิร์ฟเวอร์** SSL

การแสดงสถานะนี้เป็นแบบ read-only และไม่สามารถตั้งค่าได้โดยตรง ค่าผลลัพธ์บรรทัดคำสั่งที่เป็นไปได้มีดังต่อไปนี้:

คีย์ส่วนตัวและ Cert/CSR ไม่พร้อมใช้งาน

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามโดย CA แล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองที่สร้างขึ้นโดยอัตโนมัติแล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองแล้ว

จัดเก็บคีย์ส่วนตัวแล้ว, CSR พร้อมให้ดาวน์โหลด

สถานะคีย์ LDAP **ของไคลเอ็นต์** SSL

การแสดงสถานะนี้เป็นแบบ read-only และไม่สามารถตั้งค่าได้โดยตรง ค่าผลลัพธ์บรรทัดคำสั่งที่เป็นไปได้มีดังต่อไปนี้:

คีย์ส่วนตัวและ Cert/CSR ไม่พร้อมใช้งาน

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามโดย CA แล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองที่สร้างขึ้นโดยอัตโนมัติแล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองแล้ว

จัดเก็บคีย์ส่วนตัวแล้ว, CSR พร้อมให้ดาวน์โหลด

สถานะคีย์ CSR **ของไคลเอ็นต์** SSL

การแสดงสถานะนี้เป็นแบบ read-only และไม่สามารถตั้งค่าได้โดยตรง ค่าผลลัพธ์บรรทัดคำสั่งที่เป็นไปได้มีดังต่อไปนี้:

คีย์ส่วนตัวและ Cert/CSR ไม่พร้อมใช้งาน

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามโดย CA แล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองที่สร้างขึ้นโดยอัตโนมัติแล้ว

ติดตั้งคีย์ส่วนตัวและใบรับรองที่ลงนามด้วยตนเองแล้ว

จัดเก็บคีย์ส่วนตัวแล้ว, CSR พร้อมให้ดาวน์โหลด

คำสั่ง sslcfg

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่า SSL สำหรับ IMM และจัดการใบรับรอง

การเรียกใช้คำสั่ง **sslcfg** โดยไม่มีตัวเลือกจะแสดงข้อมูลการกำหนดค่า SSL ทั้งหมด คำสั่ง **sslcfg** ใช้เพื่อสร้างคีย์การเข้ารหัสลับใหม่ และใบรับรองที่ลงนามด้วยตนเองหรือคำขอลงนามใบรับรอง (CSR) ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 50. คำสั่ง sslcfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-server	สถานะเซิร์ฟเวอร์ SSL	enabled, disabled **หมายเหตุ**: สามารถเปิดใช้งานเซิร์ฟเวอร์ SSL เฉพาะเมื่อมีใบรับรองที่ถูกต้องเท่านั้น
-client	สถานะของไคลเอ็นต์ SSL	enabled, disabled **หมายเหตุ**: สามารถเปิดใช้งานไคลเอ็นต์ SSL เฉพาะเมื่อมีเซิร์ฟเวอร์หรือใบรับรองไคลเอ็นต์ที่ถูกต้องเท่านั้น
-cim	สถานะ CIM ผ่าน HTTPS	enabled, disabled **หมายเหตุ**: สามารถเปิดใช้งาน CIM ผ่าน HTTPS เฉพาะเมื่อมีเซิร์ฟเวอร์หรือใบรับรองไคลเอ็นต์ที่ถูกต้องเท่านั้น
-cert	สร้างใบรับรองที่ลงนามด้วยตนเอง	server, client, sysdir, storekey **หมายเหตุ**: • ต้องใช้ค่าสำหรับตัวเลือกคำสั่ง **-c**, **-sp**, **-cl**, **-on** และ **-hn** เมื่อสร้างใบรับรองที่ลงนามด้วยตนเอง • ค่าสำหรับตัวเลือกคำสั่ง **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** และ **-dq** จะมีหรือไม่ก็ได้ เมื่อสร้างใบรับรองที่ลงนามด้วยตนเอง
-csr	สร้าง CSR	server, client, sysdir, storekey **หมายเหตุ**: • ต้องใช้ค่าสำหรับตัวเลือกคำสั่ง **-c**, **-sp**, **-cl**, **-on** และ **-hn** เมื่อสร้าง CSR • ค่าสำหรับตัวเลือกคำสั่ง **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** และ **-un** จะมีหรือไม่ก็ได้ เมื่อสร้าง CSR

ตาราง 50. คำสั่ง sslcfg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-i	ที่อยู่ IP สำหรับเซิร์ฟเวอร์ TFTP/SFTP	ที่อยู่ IP ที่ถูกต้อง **หมายเหตุ**: ต้องระบุที่อยู่ IP สำหรับเซิร์ฟเวอร์ TFTP หรือ SFTP เมื่ออัปโหลดใบรับรอง หรือดาวน์โหลดใบรับรองหรือ CSR
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP	หมายเลขพอร์ตที่ถูกต้อง (ค่าเริ่มต้นคือ 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP	ชื่อผู้ใช้ที่ถูกต้อง
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP	รหัสผ่านที่ถูกต้อง
-l	ชื่อไฟล์ใบรับรอง	ชื่อไฟล์ที่ถูกต้อง **หมายเหตุ**: ต้องมีชื่อไฟล์เมื่อดาวน์โหลดหรืออัปโหลดใบรับรองหรือ CSR หากไม่มีการระบุชื่อไฟล์สำหรับดาวน์โหลด ระบบจะใช้และแสดงชื่อสำหรับไฟล์ตามค่าเริ่มต้น
-dnld	ดาวน์โหลดไฟล์ใบรับรอง	ตัวเลือกนี้ไม่รับอาร์กิวเมนต์ แต่ยังต้องระบุค่าสำหรับตัวเลือกคำสั่ง **-cert** หรือ **-csr** (โดยขึ้นอยู่กับประเภทใบรับรองที่กำลังดาวน์โหลด) ตัวเลือกนี้ไม่รับอาร์กิวเมนต์ แต่ยังต้องระบุค่าสำหรับตัวเลือกคำสั่ง **-i** และตัวเลือกคำสั่ง **-l** (มีหรือไม่ก็ได้)
-upld	นำเข้าไฟล์ใบรับรอง	ตัวเลือกนี้ไม่รับอาร์กิวเมนต์ แต่ยังต้องระบุค่าสำหรับตัวเลือกคำสั่ง **-cert**, **-i** และ **-l**
-tc*x*	ใบรับรองที่เชื่อถือได้ *x* สำหรับไคลเอ็นต์ SSL	นำเข้า, ดาวน์โหลด, ลบออก **หมายเหตุ**: หมายเลขใบรับรองที่เชื่อถือได้ *x* คือเลขจำนวนเต็มตั้งแต่ 1 ถึง 3 ในตัวเลือกคำสั่ง
-c	ประเทศ	รหัสประเทศ (2 ตัวอักษร) **หมายเหตุ**: ต้องมีเมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-sp	รัฐหรือจังหวัด	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: ต้องมีเมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-cl	เมืองหรือท้องถิ่น	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 50 อักขระ) **หมายเหตุ**: ต้องมีเมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR

ตาราง 50. คำสั่ง sslcfg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-on	ชื่อหน่วยงาน	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: ต้องมีเมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-hn	ชื่อโฮสต์ IMM	สตริง (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: ต้องมีเมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-cp	ชื่อผู้ติดต่อ	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-ea	ที่อยู่อีเมลผู้ติดต่อ	ที่อยู่อีเมลที่ถูกต้อง (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-ou	แผนกของหน่วยงาน	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-s	นามสกุล	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-gn	ชื่อ	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-in	ชื่อย่อ	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 20 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-dq	ตัวที่มีคุณสมบัติชื่อโดเมน	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้างใบรับรองที่ลงนามด้วยตนเองหรือ CSR
-cpwd	รหัสผ่านทดสอบ	สตริง (ความยาวไม่น้อยกว่า 6 อักขระ ไม่เกิน 30 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้าง CSR
-un	ชื่อแบบไม่มีโครงสร้าง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 60 อักขระ) **หมายเหตุ**: มีหรือไม่ก็ได้เมื่อสร้าง CSR

รูปแบบคำสั่ง:
```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
```

```
  -i ip_address
-pn portnumber
-u username
  -pw password
  -l filename
  -dnld
  -upld
  -tc xaction
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn bmc_hostname
  -cp contact_person
  -ea email_address
  -ou organizational_unit
  -s surname
  -gn given_name
  -in initials
  -dq dn_qualifier
  -cpwd challenge_password
  -un unstructured_name
```

ตัวอย่าง:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

ตัวอย่างใบรับรองของไคลเอ็นต์:

- ในการสร้าง CSR สำหรับคีย์ที่จัดเก็บ ให้ป้อนคำสั่งต่อไปนี้:

  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

ตัวอย่างข้างต้นจะแสดงผลแบบหลายบรรทัดเนื่องจากมีพื้นที่จำกัด

- ในการดาวน์โหลดใบรับรองจาก IMM ลงในเซิร์ฟเวอร์อื่น ให้ป้อนคำสั่งต่อไปนี้:

  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```

- ในการอัปโหลดใบรับรองที่ประมวลผลโดยหน่วยงานผู้ออกใบรับรอง (CA) ให้ป้อนคำสั่งต่อไปนี้:
```
system> sslcfg
-cert storekey -upld -i 192.168.70.230 -l tklm.der
```
- ในการสร้างใบรับรองที่ลงนามด้วยตนเอง ให้ป้อนคำสั่งต่อไปนี้:
```
system> sslcfg
-cert storekey -c US -sp NC -cl rtp -on Lenovo -hn XCC-5cf3fc6e0c9d
-cp Contact -ea "" -ou "
ok
```
ตัวอย่างข้างต้นจะแสดงผลแบบหลายบรรทัดเนื่องจากมีพื้นที่จำกัด

ตัวอย่างใบรับรองของเซิร์ฟเวอร์ SKLM:

- ในการนำเข้าใบรับรองของเซิร์ฟเวอร์ SKLM ให้ป้อนคำสั่งต่อไปนี้:
```
system> storekeycfg
-add -ip 192.168.70.200 -f tklm-server.der
ok
```

คำสั่ง storekeycfg

ใช้คำสั่งนี้เพื่อกำหนดค่าชื่อโฮสต์หรือที่อยู่ IP และพอร์ตเครือข่ายสำหรับเซิร์ฟเวอร์ SKLM

คุณสามารถกำหนดค่าเป้าหมายของเซิร์ฟเวอร์ SKLM ได้สูงสุดสี่รายการ นอกจากนี้ คำสั่ง **storekeycfg** ยังใช้เพื่อติดตั้งและลบใบรับรองที่ใช้งานโดย IMM เพื่อการตรวจสอบความถูกต้องไปยังเซิร์ฟเวอร์ SKLM ด้วย

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 51. คำสั่ง storekeycfg

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-add	เพิ่มคีย์เปิดการทำงาน	ค่าตัวเลือกคือคำสั่ง -ip, -pn, -u, -pw และ -f
-ip	ชื่อโฮสต์หรือที่อยู่ IP ของเซิร์ฟเวอร์ TFTP/SFTP	ชื่อโฮสต์หรือที่อยู่ IP ที่ถูกต้องของเซิร์ฟเวอร์ TFTP/SFTP
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP หรือ SFTP	หมายเลขพอร์ตที่ถูกต้องของเซิร์ฟเวอร์ TFTP หรือ SFTP (ค่าเริ่มต้นคือ 69/22)
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP	ชื่อผู้ใช้ที่ถูกต้องสำหรับเซิร์ฟเวอร์ SFTP

ตาราง 51. คำสั่ง storekeycfg (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP	รหัสผ่านที่ถูกต้องสำหรับเซิร์ฟเวอร์ SFTP
-f	ชื่อไฟล์ของคีย์เปิดการทำงาน	ชื่อไฟล์ที่ถูกต้องของชื่อไฟล์คีย์เปิดการทำงาน
-del	ใช้คำสั่งนี้เพื่อลบคีย์เปิดการทำงานตามหมายเลขดัชนี	หมายเลขดัชนีของคีย์เปิดการทำงานที่ถูกต้องจากรายการ keycfg
-dgrp	เพิ่มกลุ่มของอุปกรณ์	ชื่อกลุ่มอุปกรณ์
-sxip	เพิ่มชื่อโฮสต์หรือที่อยู่ IP ของเซิร์ฟเวอร์ SKLM	ชื่อโฮสต์หรือที่อยู่ IP ที่ถูกต้องของเซิร์ฟเวอร์ SKLM ค่าตัวเลขระหว่าง 1, 2, 3 หรือ 4
-sxpn	เพิ่มหมายเลขพอร์ตของเซิร์ฟเวอร์ SKLM	หมายเลขพอร์ตที่ถูกต้องของเซิร์ฟเวอร์ SKLM ค่าตัวเลขระหว่าง 1, 2, 3 หรือ 4
-testx	ทดสอบการกำหนดค่าและการเชื่อมต่อไปยังเซิร์ฟเวอร์ SKLM	ค่าตัวเลขระหว่าง 1, 2, 3 หรือ 4
-h	แสดงวิธีการใช้คำสั่งและตัวเลือก	

รูปแบบคำสั่ง:
```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

ตัวอย่าง:

ในการนำเข้าใบรับรองของเซิร์ฟเวอร์ SKLM ให้ป้อนคำสั่งต่อไปนี้:
```
system> storekeycfg
```

```
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

ในการกำหนดค่าที่อยู่เซิร์ฟเวอร์ SKLM และหมายเลขพอร์ต ให้ป้อนคำสั่งดังต่อไปนี้:

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

ในการกำหนดชื่อกลุ่มอุปกรณ์ ให้ป้อนคำสั่งดังต่อไปนี้:

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

คำสั่ง syncrep

ใช้คำสั่งนี้เพื่อเรียกใช้การซิงค์เฟิร์มแวร์จากที่เก็บข้อมูลระยะไกล

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 52. คำสั่ง syncrep

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-t	โปรโตคอลในการเชื่อมต่อกับที่เก็บข้อมูล	samba, nfs
-l	ตำแหน่งของที่เก็บข้อมูลระยะไกล	ในรูปแบบ URL
-u	ผู้ใช้	
-p	รหัสผ่าน	
-o	ตัวเลือก	สตริงตัวเลือกพิเศษสำหรับเมาท์ samba และ nfs
-d	โดเมน	โดเมนสำหรับเมาท์ samba
-q	สืบค้นสถานะการอัปเดตปัจจุบัน	
-c	ยกเลิกกระบวนการซิงค์	

รูปแบบคำสั่ง

```
syncrep [options]  Launch firmware sync from remote repository
options:
```

```
-t <samba|nfs> protocol to connect repository
-l location of remote repository (URL format)
-u User
-p Password
-o option (extra option string for samba and nfs mounts)
-d domain (domain for samba mount)
-q query current update status
-c cancel the sync process
```

ตัวอย่าง

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

คำสั่ง thermal

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่านโยบายโหมดความร้อนของระบบโฮสต์

การเรียกใช้คำสั่ง thermal โดยไม่มีตัวเลือกจะแสดงนโยบายโหมดความร้อน ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 53. คำสั่ง thermal

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-mode	แสดงนโยบายโหมดระบายความร้อนและกำหนดค่าตารางความร้อนของระบบโฮสต์ (อ่านอย่างเดียว)	ปกติ, ประสิทธิภาพ, ขั้นต่ำ, ประหยัด, ปรับแต่งเอง
-table <vendorID_deviceID><table_number>	<vendorID_deviceID> ระบุผู้จัดจำหน่ายและรหัสอุปกรณ์ของส่วนประกอบที่ต้องการการระบายความร้อนสำรอง	อักขระฐานสิบหก 8 ตัว

ตาราง 53. คำสั่ง thermal (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
	<table_number> ระบุตารางความร้อนสำรองที่จะใช้	1 = ต่ำ: เพิ่มความเร็วพัดลมเล็กน้อย 2 = กลาง: เพิ่มความเร็วพัดลมระดับกลาง 3 = สูง: เพิ่มความเร็วพัดลมอย่างมาก 0 = ปกติ: ไม่มีการเพิ่มความเร็วพัดลม

รูปแบบคำสั่ง:
```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

ตัวอย่าง:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

คำสั่ง timeouts

ใช้คำสั่งนี้เพื่อแสดงหรือเปลี่ยนค่าการหมดเวลา

- ในการแสดงการหมดเวลา ให้พิมพ์ `timeouts`
- ในการเปลี่ยนค่าการหมดเวลา ให้พิมพ์ตัวเลือกตามด้วยค่า
- ในการเปลี่ยนค่าการหมดเวลา คุณต้องมีสิทธิ์ในการกำหนดค่าอะแดปเตอร์เป็นอย่างน้อย

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับค่าการหมดเวลา ค่าเหล่านี้จะตรงกับตัวเลือกแบบดึงลงไล่ระดับสเกลสำหรับการหมดเวลาของเซิร์ฟเวอร์บนเว็บอินเทอร์เฟซ

ตาราง 54. คำสั่ง timeouts

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 4 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าสำหรับตัวเลือกที่เกี่ยวข้อง

ตาราง 54. คำสั่ง timeouts (มีต่อ)

ตัวเลือก	การหมดเวลา	หน่วย	ค่า
-f	การหน่วงเวลาปิดเครื่อง	นาที	ปิดใช้งาน, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	การหมดเวลาของตัวโหลด	นาที	ปิดใช้งาน, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	การหมดเวลาของระบบปฏิบัติการ	นาที	ปิดใช้งาน, 2.5, 3, 3.5, 4
-s	การถ่ายภาพหน้าจอระบบปฏิบัติการล้มเหลวที่มีข้อผิดพลาด HW	/	disabled, enabled

รูปแบบคำสั่ง:
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

ตัวอย่าง:
```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

คำสั่ง tls

ใช้คำสั่งนี้เพื่อกำหนดระดับต่ำสุดของ TLS

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 55. คำสั่ง tls

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 55. คำสั่ง tls (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-min	เลือกระดับต่ำสุดของ TLS	1.1, 1.2[1], 1.3
-h	แสดงการใช้งานและตัวเลือก	
หมายเหตุ: 1. หากโหมดการเข้ารหัสถูกกำหนดเป็นโหมด NIST-800-131A Compliance จะต้องตั้งค่าเวอร์ชันของ TLS เป็น 1.2		

การใช้งาน:

```
tls [-options] - configures the minimum TLS level
   -min <1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

ตัวอย่าง:

หากต้องการดูการใช้งานของคำสั่ง tls ให้ป้อนคำสั่งดังต่อไปนี้:

```
system> tls
-h
system>
```

หากต้องการรับเวอร์ชันล่าสุดของ tls ให้ป้อนคำสั่งดังต่อไปนี้:

```
system> tls
-min 1.2
system>
```

หากต้องการเปลี่ยนเวอร์ชันปัจจุบันของ tls เป็นเวอร์ชัน 1.2 ให้ป้อนคำสั่งดังต่อไปนี้:

```
system> tls
-min 1.2
ok
system>
```

คำสั่ง trespass

ใช้คำสั่งนี้เพื่อกำหนดค่าและแสดงข้อความการบุกรุก

คำสั่ง **trespass** สามารถใช้เพื่อกำหนดค่าและแสดงข้อความการบุกรุกได้ ข้อความการบุกรุกจะแสดงต่อผู้ใช้ที่เข้าสู่ระบบผ่านอินเทอร์เฟซ WEB หรือ CLI

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 56. คำสั่ง uefipw

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด
-s	กำหนดค่าข้อความการบุกรุก
-h	แสดงการใช้งานและตัวเลือก

รูปแบบคำสั่ง:
```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

ตัวอย่าง:

หมายเหตุ: ข้อความการบุกรุกไม่มีช่องว่าง

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

คำสั่ง uefipw

ใช้คำสั่งนี้เพื่อกำหนดค่ารหัสผ่านผู้ดูแลระบบ UEFI รหัสผ่านเป็นแบบเขียนอย่างเดียว

คำสั่ง **uefipw** สามารถใช้ร่วมกับคำสั่งเสริม “-p” เพื่อกำหนดค่ารหัสผ่านผู้ดูแลระบบ UEFI สำหรับ XCC หรือคำสั่งเสริม “-ep” สำหรับ LXCA เพื่อกำหนดค่ารหัสผ่านผู้ดูแลระบบ UEFI ด้วยอินเทอร์เฟซ CLI รหัสผ่านเป็นแบบเขียนอย่างเดียว

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 57. คำสั่ง uefipw

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตาราง 57. คำสั่ง uefipw (มีต่อ)

ตัวเลือก	รายละเอียด
-cp	รหัสผ่านปัจจุบัน (ต้องมีความยาวไม่เกิน 20 อักขระ)
-p	รหัสผ่านใหม่ (ต้องมีความยาวไม่เกิน 20 อักขระ)
-cep	เข้ารหัสรหัสผ่านปัจจุบัน
-ep	เข้ารหัสรหัสผ่านใหม่

รูปแบบคำสั่ง:
```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
   -cep     - current password encrypted
   -ep      - new password encrypted
```

คำสั่ง usbeth

ใช้คำสั่งนี้ในการเปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซ LAN over USB ภายใน

รูปแบบคำสั่ง:
```
usbeth [options]
options:
-en <enabled|disabled>
```

ตัวอย่าง:
```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

คำสั่ง usbfp

ใช้คำสั่งนี้เพื่อควบคุมการใช้ BMC ของพอร์ต USB บนแผงด้านหน้า

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 58. คำสั่ง usbfp

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตาราง 58. คำสั่ง usbfp (มีต่อ)

ตัวเลือก	รายละเอียด
-mode <bmc | server | shared>	ตั้งค่าโหมดการใช้งานเป็น BMC, เซิร์ฟเวอร์ หรือแบบใช้งานร่วมกัน
-it <minutes>	การหมดเวลาเมื่อไม่มีการใช้งานเป็นนาที (โหมดแบบใช้งานร่วมกัน)
-btn <on | off>	เปิดใช้งานการใช้ปุ่ม ID เพื่อสลับเจ้าของ (โหมดแบบใช้งานร่วมกัน)
-own <bmc | server >	ตั้งค่าเจ้าของเป็น BMC หรือเซิร์ฟเวอร์ (โหมดแบบใช้งานร่วมกัน)

คำสั่ง user

ใช้คำสั่งนี้เพื่อเข้าถึงบัญชีผู้ใช้ทั้งหมดและระดับสิทธิ์ของบัญชีเหล่านั้น

คำสั่ง **users** ยังใช้เพื่อสร้างบัญชีผู้ใช้ใหม่และแก้ไขบัญชีที่มีอยู่แล้ว การเรียกใช้คำสั่ง **users** โดยไม่มีตัวเลือกจะแสดงรายการผู้ใช้และข้อมูลผู้ใช้พื้นฐานบางส่วน ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 59. คำสั่ง user

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-user_index	หมายเลขดัชนีของบัญชีผู้ใช้	1 ถึง 12 หรือ **all** สำหรับผู้ใช้ทั้งหมด
-n	ชื่อบัญชีผู้ใช้	สตริงที่ไม่ซ้ำกันประกอบด้วยตัวเลข ตัวอักษร จุด และขีดล่างเท่านั้น ความยาวไม่น้อยกว่า 4 อักขระ และไม่เกิน 16 อักขระ
-p	รหัสผ่านของบัญชีผู้ใช้	สตริงที่ประกอบด้วยตัวอักษรอย่างน้อยหนึ่งตัวและอักขระที่ไม่ใช่ตัวอักษรหนึ่งตัว ความยาวไม่น้อยกว่า 6 อักขระ และไม่เกิน 20 อักขระ ค่านัลจะสร้างบัญชีโดยไม่มีรหัสผ่าน ซึ่งผู้ใช้ต้องตั้งค่าระหว่างการเข้าสู่ระบบครั้งแรก
-r	ชื่อบทบาท	ตามที่แสดงในคำสั่ง “คำสั่ง roles” บนหน้าที่ 201
-ep	รหัสผ่านการเข้ารหัสลับ (สำหรับสำรอง/คืนค่า)	รหัสผ่านที่ถูกต้อง

ตาราง 59. คำสั่ง user (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-clear	ลบบัญชีผู้ใช้ที่ระบุ หากคุณได้รับอนุญาต คุณสามารถลบบัญชีของคุณเองหรือบัญชีของผู้ใช้อื่นๆ ได้ แม้ว่าพวกเขาจะเข้าสู่ระบบอยู่ก็ตาม เว้นแต่จะเป็นเพียงบัญชีเดียวที่เหลืออยู่พร้อมสิทธิ์การจัดการบัญชีผู้ใช้ เซสชันที่กำลังดำเนินอยู่เมื่อมีการลบบัญชีผู้ใช้จะไม่สิ้นสุดโดยอัตโนมัติ	ต้องระบุหมายเลขดัชนีของบัญชีผู้ใช้ที่จะลบตามรูปแบบต่อไปนี้: `users -clear -user_index`
-curr	แสดงผู้ใช้ที่เข้าสู่ระบบในปัจจุบัน	
-sauth	โปรโตคอลการตรวจสอบความถูกต้องของ SNMPv3	HMAC-SHA, none
-spriv	โปรโตคอลความเป็นส่วนตัวของ SNMPv3	CBC-DES, AES, none
-spw	รหัสส่วนตัวของ SNMPv3	รหัสผ่านที่ถูกต้อง
-sepw	รหัสส่วนตัวของ SNMPv3 (เข้ารหัสลับ)	รหัสผ่านที่ถูกต้อง
-sacc	ประเภทการเข้าถึง SNMPv3	get, set
-strap	ชื่อโฮสต์ SNMPv3 Trap	ชื่อโฮสต์ที่ถูกต้อง

ตาราง 59. คำสั่ง user (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-pk	แสดงคีย์สาธารณะ SSH สำหรับผู้ใช้	หมายเลขดัชนีของบัญชีผู้ใช้ **หมายเหตุ**: • คีย์ SSH ที่กำหนดให้กับผู้ใช้แต่ละคีย์จะแสดงขึ้น พร้อมด้วยหมายเลขดัชนีของคีย์การระบุ • เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก -***userindex***) ของรูปแบบ: **users -2 -pk** • คีย์ทั้งหมดอยู่ในรูปแบบ OpenSSH • สำหรับโหนด Flex คำสั่งของผู้ใช้จะจำกัดเฉพาะบัญชี IPMI และ SNMP ภายในเท่านั้น ไม่รองรับตัวเลือก **-pk** สำหรับ Flex System
-e	แสดงคีย์ SSH ทั้งหมดในรูปแบบ OpenSSH *(ตัวเลือกคีย์สาธารณะ SSH)*	ตัวเลือกนี้ไม่รับอาร์กิวเมนต์ และต้องใช้แยกจากตัวเลือก **users -pk** อื่นๆ ทั้งหมด **หมายเหตุ**: เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก -***userindex***) ของรูปแบบ: **users -2 -pk -e**
-remove	ลบคีย์สาธารณะ SSH จากผู้ใช้ *(ตัวเลือกคีย์สาธารณะ SSH)*	ต้องระบุหมายเลขดัชนีของคีย์สาธารณะที่จะลบออกเป็น -***key_index*** หรือ **-all** ที่เฉพาะเจาะจงสำหรับคีย์ทั้งหมดที่กำหนดให้กับผู้ใช้ **หมายเหตุ**: • เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก -***userindex***) ของรูปแบบ: **users -2 -pk -remove -1** • สำหรับโหนด Flex คำสั่งของผู้ใช้จะจำกัดเฉพาะบัญชี IPMI และ SNMP ภายในเท่านั้น ไม่รองรับตัวเลือก **-remove** สำหรับ Flex System

ตาราง 59. คำสั่ง user (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-add	เพิ่มคีย์สาธารณะ SSH สำหรับผู้ใช้ *(ตัวเลือกคีย์สาธารณะ SSH)*	คีย์ที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยวในรูปแบบ OpenSSH **หมายเหตุ**: • ระบบจะใช้ตัวเลือก **-add** โดยไม่รวมตัวเลือกคำสั่ง **users -pk** อื่นๆ ทั้งหมด • เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก -***userindex***) ของรูปแบบ: **users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/ aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="** • สำหรับโหนด Flex คำสั่งของผู้ใช้จะจำกัดเฉพาะบัญชี IPMI และ SNMP ภายในเท่านั้น ไม่รองรับตัวเลือก **-add** สำหรับ Flex System
-upld	อัปโหลดคีย์สาธารณะ SSH *(ตัวเลือกคีย์สาธารณะ SSH)*	กำหนดให้ตัวเลือก **-i** และ **-l** ต้องระบุตำแหน่งคีย์ **หมายเหตุ**: • ระบบจะใช้ตัวเลือก **-upld** โดยไม่รวมตัวเลือกคำสั่ง **users -pk** อื่นๆ ทั้งหมด (ยกเว้น **-i** และ **-l**) • ในการเปลี่ยนคีย์ด้วยคีย์ใหม่ คุณต้องระบุ -***key_index*** ในการเพิ่มคีย์ลงในท้ายรายการของคีย์ปัจจุบัน ไม่ต้องระบุดัชนีของคีย์ • เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก -***userindex***) ของรูปแบบ: **users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key** • สำหรับโหนด Flex คำสั่งของผู้ใช้จะจำกัดเฉพาะบัญชี IPMI และ SNMP ภายในเท่านั้น ไม่รองรับตัวเลือก **-upld** สำหรับ Flex System

ตาราง 59. คำสั่ง user (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-dnld	ดาวน์โหลดคีย์สาธารณะ SSH ที่ระบุ *(ตัวเลือกคีย์สาธารณะ SSH)*	กำหนดให้ **-*key_index*** ต้องระบุคีย์ที่จะดาวน์โหลด และตัวเลือก **-i** และ **-l** ต้องระบุตำแหน่งการดาวน์โหลดบนคอมพิวเตอร์เครื่องอื่นที่ใช้งานเซิร์ฟเวอร์ TFTP **หมายเหตุ**: • ระบบจะใช้ตัวเลือก **-dnld** โดยไม่รวมตัวเลือกคำสั่ง **users -pk** อื่นๆ ทั้งหมด (ยกเว้น **-i**, **-l** และ **-*key_index***) • เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก **-pk** หลังดัชนีผู้ใช้ (ตัวเลือก **-*userindex***) ของรูปแบบ: **users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key**
-i	ที่อยู่ IP ของเซิร์ฟเวอร์ TFTP/SFTP สำหรับการอัปโหลดหรือดาวน์โหลดไฟล์คีย์ *(ตัวเลือกคีย์สาธารณะ SSH)*	ที่อยู่ IP ที่ถูกต้อง **หมายเหตุ**: ต้องใช้ตัวเลือก **-i** ตามที่กำหนดโดยตัวเลือกคำสั่ง **users -pk -upld** และ **users -pk -dnld**
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP *(ตัวเลือกคีย์สาธารณะ SSH)*	หมายเลขพอร์ตที่ถูกต้อง (ค่าเริ่มต้นคือ 69/22) **หมายเหตุ**: พารามิเตอร์เสริมสำหรับตัวเลือกคำสั่ง **users -pk -upld** และ **users -pk -dnld**
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP *(ตัวเลือกคีย์สาธารณะ SSH)*	ชื่อผู้ใช้ที่ถูกต้อง **หมายเหตุ**: พารามิเตอร์เสริมสำหรับตัวเลือกคำสั่ง **users -pk -upld** และ **users -pk -dnld**
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP *(ตัวเลือกคีย์สาธารณะ SSH)*	รหัสผ่านที่ถูกต้อง **หมายเหตุ**: พารามิเตอร์เสริมสำหรับตัวเลือกคำสั่ง **users -pk -upld** และ **users -pk -dnld**
-l	ชื่อไฟล์สำหรับการอัปโหลดหรือดาวน์โหลดไฟล์คีย์ผ่าน TFTP หรือ SFTP *(ตัวเลือกคีย์สาธารณะ SSH)*	ชื่อไฟล์ที่ถูกต้อง **หมายเหตุ**: ต้องใช้ตัวเลือก **-l** ตามที่กำหนดโดยตัวเลือกคำสั่ง **users -pk -upld** และ **users -pk -dnld**

ตาราง 59. คำสั่ง user (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-af	ยอมรับการเชื่อมต่อจากโฮสต์ *(ตัวเลือกคีย์สาธารณะ SSH)*	รายการชื่อโฮสต์และที่อยู่ IP ที่คั่นด้วยเครื่องหมายจุลภาค ความยาวไม่เกิน 511 อักขระ อักขระที่ถูกต้อง ได้แก่: ตัวอักษรและตัวเลข เครื่องหมายจุลภาค ดอกจัน เครื่องหมายคำถาม เครื่องหมายอัศเจรีย์ จุลภาค ยัติภังค์ โคลอน และสัญลักษณ์เปอร์เซ็นต์
-cm	ความเห็น *(ตัวเลือกคีย์สาธารณะ SSH)*	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว ความยาวไม่เกิน 255 อักขระ **หมายเหตุ**: เมื่อใช้ตัวเลือกคีย์สาธารณะ SSH ต้องใช้ตัวเลือก `-pk` หลังดัชนีผู้ใช้ (ตัวเลือก *`-userindex`*) ของรูปแบบ: `users -2 -pk -cm "This is my comment."`

รูปแบบคำสั่ง:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )
   -r       - role name as listed in roles command
   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                   - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

ตัวอย่าง:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------      ------------------              ------             ----------------
    1           USERID                  Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute             Role               Password Expires
 -------      --------      ------------------             ------             ----------------
    1           USERID                  Native            Administrator                   90 day(s)
2           sptest                  Native                 Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r  Admini
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
```

คำสั่งควบคุม IMM

หัวข้อนี้จะแสดงรายการคำสั่ง CLI การควบคุม IMM ตามตัวอักษร

คำสั่งการควบคุม IMM มี 7 คำสั่งดังนี้:

คำสั่ง alertentries

ใช้คำสั่งนี้เพื่อจัดการผู้รับการแจ้งเตือน

- การเรียกใช้ **alertentries** โดยไม่มีตัวเลือกจะแสดงการตั้งค่ารายการแจ้งเตือนทั้งหมด
- **alertentries -number -test** จะสร้างการแจ้งเตือนทดสอบตามหมายเลขดัชนีผู้รับที่กำหนด
- **alertentries -number** (number คือหมายเลข 0 - 12) จะแสดงการตั้งค่ารายการแจ้งเตือนตามหมายเลขดัชนีผู้รับที่ระบุ หรือให้คุณแก้ไขการตั้งค่าการแจ้งเตือนสำหรับผู้รับดังกล่าว

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 60. คำสั่ง alertentries

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 60. คำสั่ง alertentries (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-number	หมายเลขดัชนีผู้รับที่จะแสดง เพิ่ม แก้ไข หรือลบ	1 ถึง 12
-status	สถานะผู้รับการแจ้งเตือน	on, off
-type	ประเภทการแจ้งเตือน	email, syslog
-log	รวมบันทึกเหตุการณ์ในอีเมล การแจ้งเตือนด้วย	on, off
-n	ชื่อผู้รับการแจ้งเตือน	สตริง
-e	ที่อยู่อีเมลผู้รับการแจ้งเตือน	ที่อยู่อีเมลที่ถูกต้อง
-ip	ที่อยู่ IP หรือชื่อโฮสต์ของ Syslog	ที่อยู่ IP หรือชื่อโฮสต์ที่ถูกต้อง
-pn	หมายเลขพอร์ตของ Syslog	หมายเลขพอร์ตที่ถูกต้อง
-del	ลบหมายเลขดัชนีผู้รับที่ระบุ	
-test	สร้างการแจ้งเตือนทดสอบ ตามหมายเลขดัชนีผู้รับที่ระบุ	

ตาราง 60. คำสั่ง alertentries (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-crt	ตั้งค่าเหตุการณ์ร้ายแรงที่จะส่งการแจ้งเตือน	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot ระบุการตั้งค่าการแจ้งเตือนร้ายแรงที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **alertentries -crt custom:te|vo** ส่วนที่เป็นค่าที่กำหนดเองคือ: • te: อุณหภูมิเกินเกณฑ์ร้ายแรงที่กำหนด • vo: แรงดันไฟฟ้าเกินเกณฑ์ร้ายแรงที่กำหนด • po: ระบบไฟฟ้าขัดข้องร้ายแรง • di: ฮาร์ดดิสก์ไดรฟ์ขัดข้อง • fa: พัดลมขัดข้อง • cp: ไมโครโปรเซสเซอร์ขัดข้อง • me: หน่วยความจำขัดข้อง • in: ฮาร์ดแวร์ใช้ร่วมกันไม่ได้ • re: การสำรองพลังงานขัดข้อง • ot: เหตุการณ์ร้ายแรงอื่นๆ
-crten	ส่งการแจ้งเตือนเหตุการณ์ร้ายแรง	enabled, disabled
-wrn	ตั้งค่าเหตุการณ์ระดับคำเตือนที่จะส่งการแจ้งเตือน	all, none, custom:rp|te|vo|po|fa|cp|me|ot ระบุการตั้งค่าการแจ้งเตือนระดับคำเตือนที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **alertentries -wrn custom:rp|te** ส่วนที่เป็นค่าที่กำหนดเองคือ: • rp: คำเตือนเรื่องการสำรองพลังงาน • te: อุณหภูมิเกินเกณฑ์ระดับคำเตือนที่กำหนด • vo: แรงดันไฟฟ้าเกินเกณฑ์ระดับคำเตือนที่กำหนด • po: พลังงานเกินเกณฑ์ระดับคำเตือนที่กำหนด • fa: เหตุการณ์ที่ไม่ร้ายแรงเกี่ยวกับพัดลม • cp: ไมโครโปรเซสเซอร์มีประสิทธิภาพลดลง • me: คำเตือนเกี่ยวกับหน่วยความจำ • ot: เหตุการณ์ระดับคำเตือนอื่นๆ

ตาราง 60. คำสั่ง alertentries (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-wrnen	ส่งการแจ้งเตือนเหตุการณ์ระดับคำเตือน	enabled, disabled
-sys	ตั้งค่าเหตุการณ์ประจำที่จะส่งการแจ้งเตือน	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne ระบุการตั้งค่าการแจ้งเตือนประจำที่กำหนดเอง โดยใช้รายการค่าที่คั่นด้วยเครื่องหมายขีดแนวตั้งในรูปแบบ **alertentries -sys custom:lo|tio** ส่วนที่เป็นค่าที่กำหนดเองคือ: • lo: การเข้าใช้งานระยะไกลสำเร็จ • tio: ระบบปฏิบัติการถึงเวลาไทม์เอาต์ • ot: เหตุการณ์อื่นๆ เกี่ยวกับข้อมูลและระบบ • po: เปิด/ปิดพลังงานของระบบ • bf: การบูตระบบปฏิบัติการขัดข้อง • til: โปรแกรมเฝ้าระวังตัวโหลดระบบปฏิบัติการถึงเวลาไทม์เอาต์ • pf: ความขัดข้องที่คาดการณ์ไว้ (PFA) • el: บันทึกเหตุการณ์ใช้ไปแล้ว 75% • ne: เปลี่ยนเครือข่าย
-sysen	ส่งการแจ้งเตือนเหตุการณ์ประจำ	enabled, disabled

รูปแบบคำสั่ง:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
      -sysen state
```

ตัวอย่าง:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

คำสั่ง batch

ใช้คำสั่งนี้เพื่อเรียกใช้คำสั่งใน CLI อย่างน้อยหนึ่งรายการที่อยู่ในไฟล์

- บรรทัดความเห็นในไฟล์แบทช์จะขึ้นต้นด้วย #
- เมื่อเรียกใช้ไฟล์แบทช์ ระบบจะแสดงคำสั่งที่ล้มเหลวพร้อมกับรหัสแสดงข้อผิดพลาด
- คำสั่งไฟล์แบทช์ที่มีตัวเลือกคำสั่งที่ไม่รู้จักอาจได้รับคำเตือน

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 61. คำสั่ง batch

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-f	ชื่อไฟล์แบทช์	ชื่อไฟล์ที่ถูกต้อง
-ip	ที่อยู่ IP ของเซิร์ฟเวอร์ TFTP/SFTP	ที่อยู่ IP ที่ถูกต้อง
-pn	หมายเลขพอร์ตของเซิร์ฟเวอร์ TFTP/SFTP	หมายเลขพอร์ตที่ถูกต้อง (ค่าเริ่มต้นคือ 69/22)

ตาราง 61. คำสั่ง batch (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-u	ชื่อผู้ใช้สำหรับเซิร์ฟเวอร์ SFTP	ชื่อผู้ใช้ที่ถูกต้อง
-pw	รหัสผ่านสำหรับเซิร์ฟเวอร์ SFTP	รหัสผ่านที่ถูกต้อง

รูปแบบคำสั่ง:
```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 username
  -pw password
```

ตัวอย่างเช่น:
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

คำสั่ง clearcfg

ใช้คำสั่งนี้เพื่อกำหนดการตั้งค่า IMM เป็นค่าเริ่มต้นจากโรงงาน

ในการใช้คำสั่งนี้ อย่างน้อยคุณต้องมีสิทธิ์ในการกำหนดค่าอะแดปเตอร์ขั้นสูง หลังจากล้างข้อมูลการกำหนดค่า IMM แล้ว IMM จะรีสตาร์ท

คำสั่ง clock

ใช้คำสั่งนี้เพื่อแสดงวันที่และเวลาปัจจุบัน คุณสามารถตั้งค่าค่าชดเชย UTC และเวลา Daylight Saving

BMC รับเวลาจากเซิร์ฟเวอร์โฮสต์หรือเซิร์ฟเวอร์ NTP

เวลาที่รับจากโฮสต์อาจเป็นเวลาภายในท้องถิ่นหรือเวลา UTC ควรตั้งค่าตัวเลือกโฮสต์เป็น UTC หากไม่มีการใช้ NTP และโฮสต์ใช้รูปแบบ UTC ค่าชดเชย UTC อาจอยู่ในรูปแบบ +0200, +2:00, +2 หรือ 2 สำหรับค่าบวก และ -0500, -5:00 หรือ -5 สำหรับค่าลบก็ได้ ค่าชดเชย UTC และเวลา Daylight Saving จะใช้กับ NTP หรือเมื่อโหมดโฮสต์เป็น UTC

สำหรับค่าชดเชย UTC เท่ากับ +2, -7, -6, -5, -4 และ -3 จำเป็นต้องมีการตั้งค่า Daylight Saving แบบพิเศษ

- สำหรับค่า +2 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, ee (ยุโรปตะวันออก), tky (ตุรกี), bei (เบรุต), amm (อัมมาน), jem (เยรูซาเล็ม)
- สำหรับค่า -7 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, mtn (เมาน์เทน), maz (มาซาตลัน)
- สำหรับค่า -6 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, mex (เม็กซิโก), cna (อเมริกาเหนือตอนกลาง)
- สำหรับค่า -5 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, cub (คิวบา), ena (อเมริกาเหนือฝั่งตะวันออก)
- สำหรับค่า -4 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, asu (อาซุนซีออน), cui (กูยาบา), san (ซานเตียโก), cat (แคนาดา - แอตแลนติก)
- สำหรับค่า -3 จะต้องใช้ตัวเลือก Daylight Saving ดังนี้: off, gtb (กอตฮอบ), bre (บราซิล - ตะวันออก)

รูปแบบคำสั่ง:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

ตัวอย่างเช่น:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

คำสั่ง identify

ใช้คำสั่งนี้เพื่อเปิดหรือปิดไฟ LED ระบุสถานะบนตัวเครื่อง หรือตั้งให้ไฟกะพริบ

ตัวเลือก **-d** สามารถใช้กับตัวเลือก **-s on** เพื่อเปิดไฟ LED แค่ไม่กี่วินาทีตามที่ระบุด้วยตัวเลือก **-d** ไฟ LED จะปิดหลังครบกำหนดเวลาที่ระบุไว้

รูปแบบคำสั่ง:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

ตัวอย่าง:
```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

คำสั่ง info

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าข้อมูลเกี่ยวกับ IMM

การเรียกใช้คำสั่ง **info** โดยไม่มีตัวเลือกจะแสดงข้อมูลตำแหน่งที่ตั้งและผู้ติดต่อ IMM ทั้งหมด ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 62. คำสั่ง info

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-name	ชื่อ IMM	สตริง
-contact	ชื่อของผู้ติดต่อ IMM	สตริง
-location	ตำแหน่งที่ตั้ง IMM	สตริง
-room[1]	ตัวระบุห้อง IMM	สตริง
-rack[1]	ตัวระบุแร็ค IMM	สตริง
-rup[1]	ตำแหน่งของ IMM ในแร็ค	สตริง
-ruh	ความสูงในหน่วยแร็ค	อ่านอย่างเดียว
-bbay	ที่ตั้ง Blade Bay	อ่านอย่างเดียว
1. ค่านี้เป็นแบบอ่านอย่างเดียวและไม่สามารถรีเซ็ตได้หาก IMM อยู่ใน Flex System		

รูปแบบคำสั่ง:

```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

คำสั่ง spreset

ใช้คำสั่งนี้เพื่อรีสตาร์ท IMM

ในการใช้คำสั่งนี้ อย่างน้อยคุณต้องมีสิทธิ์ในการกำหนดค่าอะแดปเตอร์ขั้นสูง

คำสั่ง Service Advisor

หัวข้อนี้จะแสดงรายการคำสั่ง Service Advisor ใน CLI ตามตัวอักษร

คำสั่ง Service Advisor มี 3 คำสั่งดังนี้:

คำสั่ง chconfig

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดการตั้งค่า Service Advisor

- คุณต้องยอมรับข้อกำหนดและเงื่อนไขของ Service Advisor โดยใช้ตัวเลือกคำสั่ง **chconfig -li** ก่อนที่จะกำหนดค่าพารามิเตอร์อื่นๆ
- จำเป็นต้องระบุฟิลด์ข้อมูลผู้ติดต่อทั้งหมด รวมทั้งฟิลด์ **Service Support Center** (โดยใช้ตัวเลือกคำสั่ง chconfig -sc) ก่อน จึงจะเปิดใช้งาน Support of Service Advisor ได้
- ต้องมีการตั้งค่าฟิลด์พร็อกซี HTTP ทั้งหมด หากจำเป็นต้องใช้พร็อกซี HTTP

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 63. คำสั่ง chconfig

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 63. คำสั่ง chconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-li	ดูหรือยอมรับข้อกำหนดและเงื่อนไขของ Service Advisor **หมายเหตุ**: ต้องยอมรับข้อกำหนดและเงื่อนไขก่อนกำหนดค่าพารามิเตอร์อื่นๆ	view, accept
-sa	สถานะการสนับสนุนของ Service Advisor **หมายเหตุ**: ในการเปิดใช้งาน Service Advisor จะต้องมีคุณสมบัติตามเกณฑ์ต่อไปนี้: • ต้องระบุรหัสประเทศ • ต้องระบุตัวเลือกทั้งหมดในข้อมูลผู้ติดต่อ Service Advisor	enabled, disabled
-sc	รหัสประเทศสำหรับ Service Support Center	รหัสประเทศ ISO จำนวนสองอักขระ
ตัวเลือกข้อมูลผู้ติดต่อ Service Advisor:		
-cn	ชื่อของผู้ติดต่อหลัก	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-cph	หมายเลขโทรศัพท์ของผู้ติดต่อหลัก	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาว 5 - 30 อักขระ)
-ce	ที่อยู่อีเมลของผู้ติดต่อหลัก **หมายเหตุ**: userid หรือชื่อโฮสต์ใช้ตัวอักษร หรือตัวเลข รวมทั้งเครื่องหมาย '.', '-' หรือ '_' ได้ ที่อยู่อีเมลต้องมีรายการโดเมนอย่างน้อยสองรายการ และรายการโดเมนสุดท้ายควรเป็นตัวอักษร 2-4 ตัว	ที่อยู่อีเมลที่ถูกต้องในรูปแบบ `userid@hostname` (ความยาวไม่เกิน 30 อักขระ)
-co	ชื่อหน่วยงานหรือบริษัทของผู้ติดต่อหลัก	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-ca	ที่อยู่ของที่ตั้งเครื่อง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)

ตาราง 63. คำสั่ง chconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-cci	เมืองของที่ตั้งเครื่อง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-cs	รัฐของที่ตั้งเครื่อง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-cz	รหัสไปรษณีย์ของที่ตั้งเครื่อง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 9 อักขระ)
ตัวเลือกข้อมูลผู้ติดต่อ Service Advisor สำรอง:		
-an	ชื่อสำรองของผู้ติดต่อหลัก	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-aph	หมายเลขโทรศัพท์สำรองของผู้ติดต่อหลัก	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาว 5 - 30 อักขระ)
-ae	ที่อยู่อีเมลสำรองของผู้ติดต่อหลัก **หมายเหตุ**: userid หรือชื่อโฮสต์ใช้ตัวอักษร หรือตัวเลข รวมทั้งเครื่องหมาย '.', '-' หรือ '_' ได้ ที่อยู่อีเมลต้องมีรายการโดเมนอย่างน้อยสองรายการ และรายการโดเมนสุดท้ายควรเป็นตัวอักษร 2-4 ตัว	ที่อยู่อีเมลที่ถูกต้องในรูปแบบ `userid@hostname` (ความยาวไม่เกิน 30 อักขระ)
-ao	ชื่อหน่วยงานหรือบริษัทของผู้ติดต่อสำรอง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-aa	ที่อยู่ของที่ตั้งเครื่องสำรอง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-aci	เมืองของที่ตั้งเครื่องสำรอง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-as	รัฐของที่ตั้งเครื่องสำรอง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-az	รหัสไปรษณีย์ของที่ตั้งเครื่องสำรอง	สตริงที่คั่นด้วยเครื่องหมายอัญประกาศเดี่ยว (ความยาวไม่เกิน 9 อักขระ)

ตาราง 63. คำสั่ง chconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
ตัวเลือกการตั้งค่าพร็อกซี HTTP:		
-loc	ที่ตั้งพร็อกซี HTTP	ชื่อโฮสต์หรือที่อยู่ IP ที่มีคุณสมบัติครบถ้วนสำหรับพร็อกซี HTTP (ความยาวไม่เกิน 63 อักขระ)
-po	พอร์ตพร็อกซี HTTP	หมายเลขพอร์ตที่ถูกต้อง (1 - 65535)
-ps	สถานะพร็อกซี HTTP	enabled, disabled
-pw	รหัสผ่านพร็อกซี HTTP	รหัสผ่านที่ถูกต้องที่คั่นด้วยอัญประกาศเดี่ยว (ความยาวไม่เกิน 15 อักขระ)
-epw	รหัสผ่านที่เข้ารหัสพร็อกซี HTTP	รหัสผ่านที่ถูกต้องที่คั่นด้วยอัญประกาศเดี่ยว (ความยาวไม่เกิน 15 อักขระ)
-u	ชื่อผู้ใช้พร็อกซี HTTP	ชื่อผู้ใช้ที่ถูกต้องที่คั่นด้วยอัญประกาศเดี่ยว (ความยาวไม่เกิน 30 อักขระ)
-test	ทดสอบพร็อกซี HTTP	

รูปแบบคำสั่ง:

```
chconfig [options]
option:
  -li view|accept
  -sa enable|disable
  -sc service_country_code
  -ce contact_email
  -cn contact_name
  -co company_name
  -cph contact_phone
  -cpx contact_extension_phone
  -an alternate_contact_name
  -ae alternate_contact_email
  -aph alternate_contact_phone
  -apx alternate_contact_extension_phone
  -mp machine_phone_number
  -loc hostname/ip_address
  -po proxy_port
  -ps proxy_status
  -pw proxy_pw
  -ccl machine_country_code
  -u proxy_user_name
```

คำสั่ง chmanual

ใช้คำสั่งนี้เพื่อสร้างคำขอ Call Home ด้วยตนเอง

หมายเหตุ: กำหนดค่าผู้รับข้อความ Call Home โดยใช้คำสั่ง **chconfig**

- คำสั่ง **chmanual -test** จะสร้างข้อความทดสอบ Call Home

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 64. คำสั่ง chmanual

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-test	สร้างข้อความทดสอบเพื่อส่งไปยังผู้รับ Call Home	

รูปแบบคำสั่ง:
```
chmanual [options]
Generates a manual Call Home or a Test Call Home
  -test: Generate a test Call Home.
```

คำสั่ง chlog

ใช้คำสั่งนี้เพื่อแสดง 5 เหตุการณ์ Call Home ล่าสุดและยกเลิกเคสที่เกี่ยวข้องกับเหตุการณ์ตาม caseNumber

คำสั่ง **chlog** จะแสดง 5 รายการล่าสุดจากบันทึกกิจกรรม Call Home ที่สร้างขึ้นโดยเซิร์ฟเวอร์หรือผู้ใช้ โดยจะแสดงรายการ Call Home ล่าสุดก่อน เซิร์ฟเวอร์จะไม่ส่งเหตุการณ์ซ้ำ หากเหตุการณ์นั้นไม่ได้รับการรับรู้ว่าแก้ไขแล้วในบันทึกกิจกรรม

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 65. คำสั่ง chconfig

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 65. คำสั่ง chconfig (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-c	ยกเลิกเคสที่เกี่ยวข้องกับเหตุการณ์ตาม caseNumber	

รูปแบบคำสั่ง:

```
chlog[-options]
      Displays the last five call home events that were generated either by
      the system or the user (most recent call home entry first.)

      -c: cancel the case associated with the event by caseNumber
```

คำสั่งแบบไม่ต้องใช้ตัวแทน

หัวข้อนี้จะแสดงรายการคำสั่งแบบไม่ต้องใช้ตัวแทนตามตัวอักษร

คำสั่งแบบไม่ต้องใช้ตัวแทนมี 3 คำสั่งดังนี้:

คำสั่ง storage

ใช้คำสั่งนี้เพื่อแสดงผลและกำหนดค่าข้อมูล (หากรองรับโดยแพลตฟอร์ม) ที่เกี่ยวกับอุปกรณ์จัดเก็บของเซิร์ฟเวอร์ ซึ่งมีการจัดการโดย IMM

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 66. คำสั่ง storage

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-list	แสดงรายการเป้าหมายการจัดเก็บที่จัดการโดย IMM	*controllers*|*pools*|*volumes*|*drives* เมื่อ *target* คือ: • *controllers*: แสดงรายการตัวควบคุม RAID ที่สนับสนุน[1] • *pools*: แสดงรายการพูลที่จัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID[1] • *volumes*: แสดงรายการโวลุ่มจัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID[1] • *drives*: แสดงรายการไดรฟ์จัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID[1]
-list -target *target_id*	แสดงรายการ *เป้าหมาย* การจัดเก็บที่จัดการโดย IMM ตาม *target_id*	*pools*|*volumes*|*drives ctrl[x]*|*pool[x]* เมื่อ *target* และ *target_id* คือ: • *pools ctrl[x]*: แสดงรายการพูลที่จัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID อ้างอิงจาก target_id[1] • *volumes ctrl[x]*|*pool[x]*: แสดงรายการโวลุ่มจัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID อ้างอิงจาก target_id[1] • *drives ctrl[x]*|*pool[x]*: แสดงรายการไดรฟ์จัดเก็บซึ่งเกี่ยวข้องกับตัวควบคุม RAID อ้างอิงจาก target_id[1]
-list flashdimms	แสดงรายการ Flash DIMM ที่จัดการโดย IMM	
-list devices	แสดงสถานะของดิสก์และ Flash DIMM ทั้งหมดที่จัดการโดย IMM	
-show *target_id*	แสดงข้อมูลของเป้าหมายที่เลือก ซึ่งจัดการโดย IMM	เมื่อ *target_id* คือ: *ctrl[x]*|*vol[x]*|*disk[x]*|*pool[x]* |*flashdimm[x]* 3

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-show *target_id* info	แสดงข้อมูลโดยละเอียดของเป้าหมายที่เลือก ซึ่งจัดการโดย IMM	เมื่อ *target_id* คือ: *ctrl[x]|vol[x]|disk[x]|pool[x]* *|flashdimm[x]* [3]
-show *target_id firmware*[3]	แสดงข้อมูลเฟิร์มแวร์ของเป้าหมายที่เลือก ซึ่งจัดการโดย IMM	เมื่อ *target_id* คือ: *ctrl[x]|disk[x]|flashdimm[x]*[2]
-showlog *target_id<m:n|all>*[3]	แสดงบันทึกเหตุการณ์ของเป้าหมายที่เลือก ซึ่งจัดการโดย IMM	เมื่อ *target_id* คือ: *ctrl[x]*[4] *m:n|all* เมื่อ *m:n* คือหนึ่งถึงจำนวนสูงสุดของบันทึกเหตุการณ์ เมื่อ *all* คือบันทึกเหตุการณ์ทั้งหมด
-config ctrl -scanforgn -target *target_id*[3]	ตรวจหาการกำหนดค่า RAID แปลกปลอม	เมื่อ *target_id* คือ: *ctrl[x]*[5]
-config ctrl -imptforgn -target *target_id*[3]	นำเข้าการกำหนดค่า RAID แปลกปลอม	เมื่อ *target_id* คือ: *ctrl[x]*[5]
-config ctrl -clrforgn -target *target_id*[3]	ล้างการกำหนดค่า RAID แปลกปลอม	เมื่อ *target_id* คือ: *ctrl[x]*[5]
-config ctrl -clrcfg -target *target_id*[3]	ล้างการกำหนดค่า RAID	เมื่อ *target_id* คือ: *ctrl[x]*[5]
-config drv -mkoffline -target *target_id*[3]	เปลี่ยนแปลงสถานะของไดรฟ์จากออนไลน์เป็นออฟไลน์	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -mkonline -target *target_id*[3]	เปลี่ยนแปลงสถานะของไดรฟ์จากออฟไลน์เป็นออนไลน์	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -mkmissing -target *target_id*[3]	ทำเครื่องหมายไดรฟ์ออฟไลน์เป็นไดรฟ์สภาพดีที่ไม่มีการกำหนดค่า	เมื่อ *target_id* คือ: *disk[x]*[5]

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-config drv -prprm -target *target_id*[3]	เตรียมไดรฟ์สภาพดีที่ไม่มีการกำหนดค่าสำหรับการนำออก	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -undoprprm -target *target_id*[3]	ยกเลิกการจัดเตรียมไดรฟ์สภาพดีที่ไม่มีการกำหนดค่าสำหรับการนำออก	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -mkbad -target *target_id*[3]	เปลี่ยนไดรฟ์สภาพดีที่ไม่มีการกำหนดค่าเป็นไดรฟ์ไม่เหมาะสมที่ไม่มีการกำหนดค่า	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -mkgood -target *target_id*[3]	เปลี่ยนไดรฟ์ไม่เหมาะสมที่ไม่มีการกำหนดค่าเป็นไดรฟ์สภาพดีที่ไม่มีการกำหนดค่า หรือ แปลงไดรฟ์แบบ Just a Bunch of Disks (JBOD) เป็นไดรฟ์สภาพดีที่ไม่มีการกำหนดค่า	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -addhsp *-[dedicated pools]* -target *target_id*[3]	ระบุไดรฟ์ที่เลือกให้เป็น Hot Spare สำหรับตัวควบคุมหรือพูลจัดเก็บที่มีอยู่	เมื่อ *target_id* คือ: *disk[x]*[5]
-config drv -rmhsp -target *target_id*[3]	ถอด Hot Spare ออก	เมื่อ *target_id* คือ: *disk[x]*[5]
-config vol -remove -target *target_id*[3]	ถอดโวลุ่มออกหนึ่งชุด	เมื่อ *target_id* คือ: *vol[x]*[5]

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[3]	แก้ไขคุณสมบัติของโวลุ่มหนึ่งชุด	• [-N *volume_name*] คือชื่อของโวลุ่ม • [-w <*0*|*1*|*2*>] คือนโยบายการเขียนแคช: – ป้อน *0* สำหรับนโยบาย Write Through – ป้อน *1* สำหรับนโยบาย Write Back – ป้อน *2* สำหรับนโยบาย Write With Battery Backup Unit (BBU) • [-r <*0*|*1*|*2*>] คือนโยบายการอ่านแคช: – ป้อน *0* สำหรับนโยบาย No Read Ahead – ป้อน *1* สำหรับนโยบาย Read Ahead – ป้อน *2* สำหรับนโยบาย Adaptive Read Ahead • [-i <*0*|*1*>] คือนโยบาย I/O ของแคช: – ป้อน *0* สำหรับนโยบาย Direct I/O – ป้อน *1* สำหรับนโยบาย Cached I/O • [-a <*0*|*2*|*3*>] คือนโยบายการเข้าถึง: – ป้อน *0* สำหรับนโยบาย Read Write – ป้อน *2* สำหรับนโยบาย Read Only – ป้อน *3* สำหรับนโยบาย Blocked • [-d <*0*|*1*|*2*>] คือนโยบายแคชของดิสก์: – ป้อน *0* หากไม่มีการเปลี่ยนแปลงนโยบาย – พิมพ์ *1* เพื่อเปิดใช้งานนโยบาย[6] – พิมพ์ *2* เพื่อปิดใช้งานนโยบาย • [-b <*0*|*1*>] คือการเริ่มต้นบนพื้นหลัง: – ป้อน *0* เพื่อเปิดใช้งานการเริ่มต้น – ป้อน *1* เพื่อปิดใช้งานการเริ่มต้น • *-target_id* คือ *vol[x]*[5]
-config vol -add<[-R]	สร้างโวลุ่มหนึ่งชุดสำหรับพูลจัดเก็บ	• [-R <*0*|*1*|*5*|*1E*|*6*|*10*|*50*|*60*|*00*|*1ERLQ0*|

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
[-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3,7]	ใหม่เมื่อเป้าหมายคือตัวควบคุม หรือ สร้างโวลุ่มด้วยพูลที่จัดเก็บที่มีอยู่เมื่อเป้าหมายคือพูลที่จัดเก็บ	*1E0RLQ0>*] ตัวเลือกนี้ใช้กำหนดระดับ RAID และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • [-D disk *[id11]:disk[id12]:..disk[id21]:disk [id22]:..*] ตัวเลือกนี้ใช้กำหนดกลุ่มไดรฟ์ (รวมถึงสแปน) และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • [-H disk *[id1]:disk[id2]:..*]ตัวเลือกนี้ใช้กำหนดกลุ่ม Hot Spare และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • [-1 hole] ตัวเลือกนี้ใช้กำหนดหมายเลขดัชนีของพื้นที่ว่างของพูลจัดเก็บที่มีอยู่ • [-N *volume_name*] คือชื่อของโวลุ่ม • [-w <*0*|*1*|*2*>] คือนโยบายการเขียนแคช: – ป้อน *0* สำหรับนโยบาย Write Through – ป้อน *1* สำหรับนโยบาย Write Back – ป้อน *2* สำหรับนโยบาย Write With Battery Backup Unit (BBU) • [-r <*0*|*1*|*2*>] คือนโยบายการอ่านแคช : – ป้อน *0* สำหรับนโยบาย No Read Ahead – ป้อน *1* สำหรับนโยบาย Read Ahead – ป้อน *2* สำหรับนโยบาย Adaptive Read Ahead
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[3]	สร้างโวลุ่มหนึ่งชุดสำหรับพูลจัดเก็บใหม่เมื่อเป้าหมายคือตัวควบคุม หรือ สร้างโวลุ่มด้วยพูลที่จัดเก็บที่มีอยู่เมื่อเป้าหมายคือพูลที่จัดเก็บ	• [-i <*0*|*1*>] คือนโยบาย I/O ของแคช: – ป้อน *0* สำหรับนโยบาย Direct I/O – ป้อน *1* สำหรับนโยบาย Cached I/O • [-a <*0*|*2*|*3*>] คือนโยบายการเข้าถึง: – ป้อน *0* สำหรับนโยบาย Read Write – ป้อน *2* สำหรับนโยบาย Read Only – ป้อน *3* สำหรับนโยบาย Blocked • [-d <*0*|*1*|*2*>] คือนโยบายแคชของดิสก์:

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
		– ป้อน *0* หากไม่มีการเปลี่ยนแปลงนโยบาย – ป้อน *1* เพื่อเปิดใช้งานนโยบาย[6] – ป้อน *2* เพื่อปิดใช้งานนโยบาย • [-f <*0/1/2*>] คือประเภทการเริ่มต้น: – ป้อน *0* หากไม่ต้องการใช้การเริ่มต้น – ป้อน *1* หากต้องการเริ่มต้นแบบด่วน – ป้อน *2* หากต้องการเริ่มต้นแบบเต็ม • [-S *volume_size*] คือขนาดของโวลุ่มใหม่ โดยมีหน่วยเป็น MB • [-P *strip_size*] คือขนาดการแบ่งส่วนของโวลุ่ม เช่น 128K หรือ 1M • -target *target_id* คือ: – *ctrl[x]* (พูลที่จัดเก็บใหม่)[5] – *pool[x]* (พูลที่จัดเก็บที่มีอยู่)[5]
-config vol -getfreecap [-R] [-D disk] [-H disk] -target *target_id*[3]	เรียกดูปริมาณความจุที่ว่างอยู่ของกลุ่มไดรฟ์	• [-R <*0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0*>] ตัวเลือกนี้ใช้กำหนดระดับ RAID และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • [-D disk *[id11]:[id12]:..[id21]:[id22]:..*] ตัวเลือกนี้ใช้กำหนดกลุ่มไดรฟ์ (รวมถึงสแปน) และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • [-H disk *[id1]:[id2]:..*]ตัวเลือกนี้ใช้กำหนดกลุ่ม Hot Spare และใช้กับพูลที่จัดเก็บใหม่เท่านั้น • -target *target_id* คือ: – *ctrl[x]*[5]

ตาราง 66. คำสั่ง storage (มีต่อ)

ตัวเลือก	รายละเอียด	ค่า
-help	แสดงวิธีการใช้คำสั่งและตัวเลือก	

หมายเหตุ:

1. คำสั่งนี้ได้รับการรองรับเฉพาะบนเซิร์ฟเวอร์ที่ IMM สามารถเข้าถึงตัวควบคุม RAID
2. โดยจะมีการแสดงข้อมูลเฟิร์มแวร์เฉพาะสำหรับตัวควบคุม ดิสก์ และ Flash DIMM เท่านั้น และจะไม่แสดงข้อมูลเฟิร์มแวร์สำหรับพูลและโวลุ่มที่เกี่ยวข้อง
3. ข้อมูลจะแสดงผลแบบหลายบรรทัดเนื่องจากมีพื้นที่จำกัด
4. คำสั่งนี้รองรับการทำงานร่วมกับเซิร์ฟเวอร์ที่สนับสนุนบันทึก RAID เท่านั้น
5. คำสั่งนี้รองรับการทำงานร่วมกับเซิร์ฟเวอร์ที่สนับสนุนการกำหนดค่า RAID เท่านั้น
6. ค่า *Enable* ไม่สนับสนุนการกำหนดค่า RAID ระดับ 1
7. รายการบางส่วนของตัวเลือกที่ใช้งานได้มีการแสดงไว้ด้านล่าง ตัวเลือกที่เหลือสำหรับคำสั่ง storage -config vol -add จะแสดงในแถวถัดไป

รูปแบบคำสั่ง:

```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

ตัวอย่าง:

```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
```

```
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>
system> storage
-config drv -mkgood -target disk[0-0]
ok
system>
system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>
system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>
system> storage
-config drv -mkonline -target disk[0-0]
ok
system>
system> storage
-config drv -prprm -target disk[0-0]
ok
system>
system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>
system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>
system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage
-config vol -remove -target vol[0-1]
ok
system>
system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>
```

```
system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
```

```
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
storage[0-0]    Pool 0
storage[0-1]    Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
```

```
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
```

```
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

คำสั่ง adapter

คำสั่งนี้ใช้เพื่อแสดงผลข้อมูลรายการอุปกรณ์อะแดปเตอร์ PCIe

หากเซิร์ฟเวอร์ไม่สนับสนุนคำสั่ง adapter เซิร์ฟเวอร์จะตอบกลับด้วยข้อความต่อไปนี้เมื่อมีการป้อนคำสั่ง:
`Your platform does not support this command.`
หากคุณนำออก แทนที่ หรือกำหนดค่าอะแดปเตอร์ใดๆ คุณจะต้องทำการเริ่มระบบเซิร์ฟเวอร์ใหม่ (อย่างน้อยหนึ่งครั้ง) เพื่อดูข้อมูลที่อัปเดตแล้วของอะแดปเตอร์

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 67. คำสั่ง adapter

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

ตัวเลือก	รายละเอียด	ค่า
-list	แสดงรายการอะแดปเตอร์ PCIe ทั้งหมดภายในเซิร์ฟเวอร์	
-show *target_id*	แสดงข้อมูลแบบละเอียดของอะแดปเตอร์ PCIe เป้าหมาย	*target_id [info|firmware|ports|chips]* ที่ซึ่ง: • *info*: แสดงข้อมูลฮาร์ดแวร์ของอะแดปเตอร์ • *firmware*: แสดงข้อมูลเฟิร์มแวร์ทั้งหมดของอะแดปเตอร์ • *ports*: แสดงข้อมูลพอร์ตอีเทอร์เน็ตทั้งหมดของอะแดปเตอร์ • *chips*: แสดงข้อมูลชิป GPU ทั้งหมดของอะแดปเตอร์
-h	แสดงวิธีการใช้คำสั่งและตัวเลือก	

รูปแบบคำสั่ง:

```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

ตัวอย่าง:

```
system> adapter
list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
```

```
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

คำสั่ง mvstor

ใช้คำสั่งนี้เพื่อรับข้อมูลรายการอุปกรณ์ที่เกี่ยวข้องกับ M.2 และจัดการโวลุ่มเสมือน

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 68. คำสั่ง mvstor

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	รายละเอียด
-h/?	พิมพ์ข้อมูลวิธีใช้สำหรับคำสั่งนี้
-version	แสดงข้อมูลเฟิร์มแวร์ของตัวควบคุม
-disks	แสดงข้อมูลดิสก์สื่อ
-volumes	แสดงข้อมูลโวลุ่มเสมือน
-create	สร้างโวลุ่มเสมือน สามารถระบุ VD_Name RaidLevel และ StripeSize ได้
-delete	ลบโวลุ่มเสมือน
-import	นำเข้าโวลุ่มเสมือนใหม่ หลังจากนำเข้าโวลุ่มเสมือน การรีบูตระบบจะสร้างโวลุ่มเสมือนโดยอัตโนมัติ

การใช้งาน

```
   mvstor [-options] - raid configuration for SATA/NVMe RAID boot solution.
options:
   -version                    - displays controller firmware version.
   -disks                       - displays information of media disks.
   -volumes                     - displays information of virtual disks
```

```
   -create -slot <slot_no> -name <vd name> -level <0|1> -stripe <32|64|128|256|512> - create virtual volume.
       Marvell SATA RAID: stripe size can only be 32k or 64k
       Marvell NVMe RAID: vd name is unapplicable. The name will always be VD_0.
   -delete -slot <slot_no> -id <0|1>          - delete the virtual volume
   -import -slot <slot_no> -id <0|1>          - import a foreign virtual volume
```

ตัวอย่าง

```
system> mvstor -version
    Controller Slot      Device Name                                              Version
1                ThinkSystem M.2 SATA 2-Bay RAID Enablement Kit        2.3.20.1203


system> mvstor -disks
  Controller Slot 1    M.2 Bay0         128GB M.2 SATA SSD     LEN
  Controller Slot 1    M.2 Bay1         128GB M.2 SATA SSD     LEN

system> mvstor -volumes
Controller Slot 1:
    VD_ID:         0
    VD_Name:       VD_Test
    PD_Member:     0,1
    RaidLevel:     1
    StripSize:     64k
    VD_Capacity:   117 GB
    VD_Status:     Optimal
       1              64k           29 GB            Optimal

system> mvstor -delete –slot 1 -id 0
VD_ID 0 is deleted

system> mvstor -create –slot 1 -name M2RAID -level 1 -strip 64
New volume is created

system> mvstor -import –slot 1 -id 0
VD_ID 0 is imported
```

คำสั่งการสนับสนุน

หัวข้อนี้จะแสดงรายการคำสั่งการสนับสนุนตามตัวอักษร

มีคำสั่งการสนับสนุนเพียงหนึ่งคำสั่ง นั่นคือ: “คำสั่ง dbgshimm” บนหน้าที่ 261

คำสั่ง dbgshimm

ใช้คำสั่งนี้เพื่อปลดล็อคการเข้าถึงเครือข่ายเชลล์การแก้ไขข้อบกพร่องที่มีความปลอดภัย

หมายเหตุ: คำสั่งนี้มีไว้เพื่อรองรับการใช้งานส่วนบุคคลเท่านั้น

ตารางต่อไปนี้จะแสดงอาร์กิวเมนต์สำหรับตัวเลือกต่างๆ

ตาราง 69. คำสั่ง dbgshimm

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวนสองคอลัมน์ที่ประกอบด้วยตัวเลือกและรายละเอียดของตัวเลือก

ตัวเลือก	**รายละเอียด**
สถานะ	แสดงสถานะ
เปิดใช้งาน	เปิดใช้งานการเข้าถึงการแก้ไขข้อบกพร่อง (เป็นค่าเริ่มต้น หากไม่มีการระบุตัวเลือก)
ปิดใช้งาน	ปิดใช้งานการเข้าถึงการแก้ไขข้อบกพร่อง

บทที่ 12. อินเทอร์เฟซ IPMI

บทนี้จะอธิบายข้อมูลเกี่ยวกับอินเทอร์เฟซ IPMI ที่ XClarity Controller รองรับ

สำหรับรายละเอียดของคำสั่ง IPMI มาตรฐาน โปรดดูเอกสารข้อมูลจำเพาะของ Intelligent Platform Management Interface (IPMI) (เวอร์ชัน 2.0 ขึ้นไป) เอกสารนี้จะแสดงรายละเอียดเกี่ยวกับพารามิเตอร์ OEM ที่ใช้กับคำสั่ง IPMI และคำสั่ง OEM IPMI มาตรฐานที่เฟิร์มแวร์ XClarity Controller รองรับ

การจัดการ XClarity Controller ด้วย IPMI

ใช้ข้อมูลในหัวข้อนี้เพื่อจัดการ XClarity Controller โดยใช้ Intelligent Platform Management Interface (IPMI)

XClarity Controller มาพร้อม ID ผู้ใช้ที่ตั้งค่าเริ่มต้นด้วยชื่อผู้ใช้ USERID และรหัสผ่าน PASSW0RD (ที่มีเลขศูนย์ ไม่ใช่ตัวอักษร O) ผู้ใช้นี้มีสิทธิ์การเข้าถึงระดับผู้ควบคุม

ข้อสำคัญ: เปลี่ยนชื่อผู้ใช้และรหัสผ่านนี้ระหว่างการกำหนดค่าเริ่มต้นเพื่อการรักษาความปลอดภัยที่ดียิ่งขึ้น

ใน Flex System ผู้ใช้สามารถกำหนดค่า Flex System CMM ให้จัดการบัญชีผู้ใช้ IPMI ของ XClarity Controller จากส่วนกลาง ในสถานการณ์นี้ คุณอาจไม่สามารถเข้าถึง XClarity Controller โดยใช้ IPMI ได้จนกว่า CMM จะกำหนดค่า ID ผู้ใช้ IPMI แล้ว

หมายเหตุ: ข้อมูลประจำตัวของ ID ผู้ใช้ที่กำหนดค่าโดย CMM อาจแตกต่างจากการผสม USERID/PASSW0RD ที่อธิบายข้างต้น หากไม่มีการกำหนดค่า ID ผู้ใช้ IPMI โดย CMM พอร์ตเครือข่ายที่เกี่ยวข้องกับโปรโตคอล IPMI จะถูกปิด

นอกจากนี้ XClarity Controller ยังให้ความสามารถในการจัดการเซิร์ฟเวอร์ระยะไกลของ IPMI ต่อไปนี้:

อินเทอร์เฟซบรรทัดคำสั่ง IPMI

อินเทอร์เฟซบรรทัดคำสั่ง IPMI ให้การเข้าถึงฟังก์ชันการจัดการเซิร์ฟเวอร์โดยตรงผ่านโปรโตคอล IPMI 2.0 คุณสามารถใช้ IPMItool เพื่อออกคำสั่งควบคุมพลังงานของเซิร์ฟเวอร์ ดูข้อมูลของเซิร์ฟเวอร์ และระบุเซิร์ฟเวอร์ ดูข้อมูลเพิ่มเติมเกี่ยวกับ IPMItool ได้ที่ “การใช้ IPMItool” บนหน้าที่ 264

อนุกรมผ่าน LAN

ในการจัดการเซิร์ฟเวอร์จากตำแหน่งที่ตั้งระยะไกล ให้ใช้ IPMItool เพื่อสร้างการเชื่อมต่ออนุกรมผ่าน LAN (SOL) ดูข้อมูลเพิ่มเติมเกี่ยวกับ IPMItool ได้ที่ “การใช้ IPMItool” บนหน้าที่ 264

การใช้ IPMItool

ใช้ข้อมูลในหัวข้อนี้เพื่อเข้าถึงข้อมูลเกี่ยวกับ IPMItool

IPMItool ให้เครื่องมือต่างๆ ที่คุณสามารถใช้ในการจัดการและกำหนดค่าระบบ IPMI คุณสามารถใช้ IPMItool ทั้งภายในหรือภายนอกเพื่อจัดการและกำหนดค่า XClarity Controller

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ IPMItool หรือหากต้องการดาวน์โหลด IPMItool ให้ไปที่ https://github.com/ipmitool/ipmitool

คำสั่ง IPMI ที่มีพารามิเตอร์ OEM

ดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN

เพื่อสะท้อนถึงความสามารถที่ได้รับจาก XCC สำหรับการตั้งค่าเครือข่ายบางส่วน ค่าสำหรับข้อมูลพารามิเตอร์บางค่าจะถูกกำหนดตามที่แสดงด้านล่าง

DHCP

นอกเหนือจากวิธีการทั่วไปในการรับที่อยู่ IP แล้ว ทาง XCC จะมีโหมดที่พยายามรับที่อยู่ IP จากเซิร์ฟเวอร์ DHCP ในระยะเวลาที่กำหนดและเมื่อไม่สามารถใช้ที่อยู่ IP แบบคงที่ได้

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
ที่มาของที่อยู่ IP	4	ข้อมูล 1 [7:4] – สงวนไว้ [3:0] – ที่มาของที่อยู่ 0h = ไม่ระบุ 1h = ที่อยู่แบบคงที่ (กำหนดค่าด้วยตนเอง) 2h = ที่อยู่ที่ได้รับจาก XCC ที่ใช้ DHCP 3h = ที่อยู่ที่ได้รับจาก BIOS หรือซอฟต์แวร์ระบบ 4h = ที่อยู่ที่ได้รับจาก XCC ที่ใช้โปรโตคอลการกำหนดที่อยู่อื่นๆ XCC ใช้ค่า 4h เพื่อระบุโหมดที่อยู่ของ DHCP ที่ใช้ที่อยู่แบบคงที่ไม่ได้

การเลือกอินเทอร์เฟซอีเทอร์เน็ต

ฮาร์ดแวร์ XCC มี Mac อีเทอร์เน็ต 10/100 คู่ที่มีอินเทอร์เฟซ RMII ฮาร์ดแวร์ XCC ยังมี Mac อีเทอร์เน็ต 1Gbps คู่ที่มีอินเทอร์เฟซ RGMII ด้วย Mac ตัวหนึ่งมักจะเชื่อมต่อกับเซิร์ฟเวอร์ NIC ที่ใช้งานร่วมกันและ MAC อีกตัวหนึ่งจะถูกใช้เป็นพอร์ตการจัดการระบบเฉพาะ จะมีพอร์ตอีเทอร์เน็ตแค่หนึ่งพอร์ตบนเซิร์ฟเวอร์ที่ทำงานในเวลาที่กำหนดเท่านั้น พอร์ตทั้งสองจะไม่มีการเปิดใช้งานพร้อมๆ กัน

บนเซิร์ฟเวอร์ ผู้ออกแบบระบบอาจเลือกที่จะเชื่อมต่อกับอินเทอร์เฟซอีเทอร์เน็ตตัวใดตัวหนึ่งต่อไปนี้บน Planar ระบบ ในระบบดังกล่าว XCC จะรองรับเพียงอินเทอร์เฟซอีเทอร์เน็ตที่เชื่อมต่อกับ Planar เท่านั้น คำขอใช้พอร์ตที่ไม่ได้เชื่อมต่อจะส่งคืนรหัสการเสร็จสมบูรณ์ CCh

ID แพคเกจสำหรับการ์ดเครือข่ายเสริมทั้งหมดมีลำดับเลขดังนี้:

- การ์ดเสริม #1, ID แพคเกจ = 03h (eth2),
- การ์ดเสริม #2, ID แพคเกจ = 04h (eth3),

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อระบุพอร์ตอีเทอร์เน็ตที่ควรใช้ (แพคเกจแบบลอจิคัล) พารามิเตอร์นี้ในคำสั่งดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์หรือ 4 ไบต์ หากอุปกรณ์อยู่ในแพคเกจ NCSI ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h สำหรับ eth0, สำหรับ 01h สำหรับ eth1 เป็นต้น ไบต์ 4 = (ตัวเลือกเสริม) หมายเลขช่อง หากอุปกรณ์เป็นแพคเกจ NCSI	C0h	ข้อมูล 1 00h = eth0 01h = eth1 02h = eth2 เป็นต้น (FFh = ปิดใช้งานพอร์ตเครือข่ายภายนอกทั้งหมด) XCC รองรับไบต์ข้อมูลเสริมเสริมที่ 2 เพื่อระบุว่ามีการใช้ช่องใดบ้างในแพคเกจ data2 00h = ช่อง 0 01h = ช่อง 1 เป็นต้น หากไม่มีการระบุข้อมูล 2 ในคำขอ ระบบจะถือว่าใช้ช่อง 0

ไบต์ข้อมูล 1 ใช้ในการระบุว่าเป็นแพจเกจแบบลอจิคัล อาจเป็นการกำหนดให้เฉพาะ NIC การจัดการระบบหรืออินเทอร์เฟซ NCSI ใน NIC ที่ใช้ร่วมกันกับเซิร์ฟเวอร์

ไบต์ข้อมูล 2 ใช้เพื่อระบุช่องสำหรับแพคเกจแบบลอจิคัล หากแพคเกจเป็นอุปกรณ์ NCSI หากไม่มีการระบุข้อมูล 2 ในคำขอและแพคเกจแบบลอจิคัลเป็นอุปกรณ์ NCSI ระบบจะถือว่าใช้ช่อง 0 หากไม่มีการระบุข้อมูล 2 ในคำขอ แต่แพคเกจแบบลอจิคัลไม่เป็นอุปกรณ์ NCSI ระบบจะละเว้นข้อมูลช่อง

ตัวอย่าง:

ภาคผนวก A หากช่อง 2 ของ NIC ที่ใช้ร่วมกันบน Planar (ID แพคเกจ = 0, eth0) จะถูกใช้เป็นพอร์ตการจัดการ ข้อมูลอินพุตจะเป็น: 0xC0 0x00 0x02

ภาคผนวก B: หากช่องแรกของเครือข่ายแรกที่มีการใช้การ์ด Mezzanine ข้อมูลอินพุตจะเป็น: 0xC0 0x02 0x0

การเปิดใช้งาน/ปิดใช้งานอีเทอร์เน็ตผ่าน USB

พารามิเตอร์ด้านล่างใช้เพื่อเปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซภายใน XCC

ตารางต่อไปนี้เป็นตารางหลายแถวจำนวน 3 คอลัมน์ที่ประกอบด้วยตัวเลือก รายละเอียดตัวเลือก และค่าของตัวเลือกที่เกี่ยวข้อง

พารามิเตอร์	**#**	**ข้อมูลพารามิเตอร์**
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อเปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซอีเทอร์เน็ตผ่าน USB) พารามิเตอร์นี้ในคำสั่งดูพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h (ปิดใช้งาน) หรือ 01h (เปิดใช้งาน)	C1h	ข้อมูล 1 0x00 = ปิดใช้งาน 0x01 = เปิดใช้งาน

ไบต์ข้อมูล 1 ใช้ในการระบุว่าเป็นแพจเกจแบบลอจิคัล อาจเป็นการกำหนดให้เฉพาะ NIC การจัดการระบบหรืออินเทอร์เฟซ NCSI ใน NIC ที่ใช้ร่วมกันกับเซิร์ฟเวอร์

ไบต์ข้อมูล 2 ใช้เพื่อระบุช่องสำหรับแพคเกจแบบลอจิคัล หากแพคเกจเป็นอุปกรณ์ NCSI หากไม่มีการระบุข้อมูล 2 ในคำขอและแพคเกจแบบลอจิคัลเป็นอุปกรณ์ NCSI ระบบจะถือว่าใช้ช่อง 0 หากไม่มีการระบุข้อมูล 2 ในคำขอ แต่แพคเกจแบบลอจิคัลไม่เป็นอุปกรณ์ NCSI ระบบจะละเว้นข้อมูลช่อง

ตัวอย่าง:

ภาคผนวก A หากช่อง 2 ของ NIC ที่ใช้ร่วมกันบน Planar (ID แพคเกจ = 0, eth0) จะถูกใช้เป็นพอร์ตการจัดการ ข้อมูลอินพุตจะเป็น: 0xC0 0x00 0x02

ภาคผนวก B: หากช่องแรกของเครือข่ายแรกที่มีการใช้การ์ด Mezzanine ข้อมูลอินพุตจะเป็น: 0xC0 0x02 0x0

ตัวเลือก IPMI สำหรับการดู DUID-LLT

ค่าแบบอ่านอย่างเดียวเพิ่มเติมที่จำเป็นต้องแสดงผ่าน IPMI คือ DUID ตาม RFC3315 รูปแบบของ DUID จะอ้างอิงจาก Link Layer Address Plus Time

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อเปิดใช้งานหรือปิดใช้งานอินเทอร์เฟซอีเทอร์เน็ตผ่าน USB) พารามิเตอร์นี้ในคำสั่งดูพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทานพารามิเตอร์ (ตามข้อมูลจำเพาะ IPMI) ไบต์ 3 = ความยาวของไบต์ที่ตามมา (16 ไบต์ในปัจจุบัน) ไบต์ 4-n DUID_LLT	C2h	

พารามิเตอร์การกำหนดค่าอีเทอร์เน็ต

พารามิเตอร์ต่อไปนี้อาจใช้สำหรับกำหนดค่าการตั้งค่าอีเทอร์เน็ตเฉพาะ

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อเปิดใช้งานหรือปิดใช้งานตั้งค่าการแลกเปลี่ยนข้อมูลกันโดยอัตโนมัติให้กับอินเทอร์เฟซอีเทอร์เน็ต) ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h (ปิดใช้งาน) หรือ 01h (เปิดใช้งาน)	C3h	ข้อมูล 1 0x00 = ปิดใช้งาน 0x01 = เปิดใช้งาน หมายเหตุ: บนระบบ Flex และ Stark สิ้นสุดการตั้งค่าการแลกเปลี่ยนข้อมูลกันโดยอัตโนมัติจะไม่เปลี่ยนแปลงเนื่องจากอาจทำให้พาธการสื่อสารทางเครือข่ายผ่าน CMM และ SMM เสียหายได้
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อดูหรือตั้งค่าอัตราข้อมูลของอินเทอร์เฟซอีเทอร์เน็ต) ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h (10Mb) หรือ 01h (100Mb)	C4h	ข้อมูล 1 0x00 = 10Mbit 0x01 = 100Mbit

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อดูหรือตั้งค่าการตั้งค่า Duplex ของอินเทอร์เฟซอีเทอร์เน็ต) ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h (Half Duplex) หรือ 01h (Full Duplex)	C5h	ข้อมูล 1 0x00 = Half Duplex 0x01 = Full Duplex
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อดูหรือตั้งค่าหน่วยการส่งข้อมูลสูงสุด (MTU) ของอินเทอร์เฟซอีเทอร์เน็ต) ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3-4 = ขนาดของ MTU	C6h	ข้อมูล 1 ขนาดของ MTU
พารามิเตอร์ OEM (XCC ใช้หมายเลขพารามิเตอร์นี้เพื่อดูหรือตั้งค่าที่อยู่ MAC ที่ได้รับการดูแลภายใน) ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์	C7h	ข้อมูล 1 - 6 ที่อยู่ Mac

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
ไบต์ 2 = การตรวจทาน ไบต์ 3– 8 = ที่อยู่ Mac		

ตัวเลือก IPMI สำหรับการดูที่อยู่ Link-Local

นี่คือพารามิเตอร์แบบอ่านอย่างเดียวเพื่อเรียกดูที่อยู่ IPV6 Link Local

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ใช้เพื่อดูที่อยู่ Link-Local ของ XCC: ข้อมูลการตอบสนองจะส่งคืนค่าต่อไปนี้: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทานพารามิเตอร์ (ตามข้อมูลจำเพาะ IPMI) ไบต์ 3 = ความยาวคำนำหน้าของที่อยู่ IPV6 ไบต์ 4-19 ที่อยู่ Local Link ในรูปแบบเลขฐานสอง	C8h	

ตัวเลือก IPMI สำหรับการเปิดใช้งาน/ปิดใช้งาน IPv6

นี่คือพารามิเตอร์อ่าน/เขียนเพื่อเปิดใช้งาน/ปิดใช้งาน IPV6 ใน XCC

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ใช้เพื่อเปิดใช้งาน/ปิดใช้งาน IPv6 ใน XCC ข้อมูลการตอบสนองจะส่งคืนค่าต่อไปนี้: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทานพารามิเตอร์ (ตามข้อมูลจำเพาะ IPMI) ไบต์ 3 = 00h (ปิดใช้งาน) หรือ 01h (เปิดใช้งาน)	C9h	ข้อมูล 1 0x00 = ปิดใช้งาน 0x01 = เปิดใช้งาน

ส่งผ่านอีเทอร์เน็ตผ่าน USB ไปยังเครือข่ายภายนอก

พารามิเตอร์ด้านล่างนี้ใช้เพื่อกำหนดค่าการส่งผ่านอีเทอร์เน็ตผ่าน USB ไปยังอีเทอร์เน็ตภายนอก

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ในคำสั่งดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h ข้อมูลการตอบสนองการดูจะส่งคืนค่าต่อไปนี้: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = สำรอง (00h) ไบต์ 4:5 = หมายเลขพอร์ตอีเทอร์เน็ตผ่าน USB (LSByte เป็นอันดับแรก) ไบต์ 6:7 = หมายเลขพอร์ตอีเทอร์เน็ตภายนอก (LSByte เป็นอันดับแรก) จำนวนไบต์ที่ตามมาอาจแตกต่างกัน (1, 4 หรือ 16 ไบต์) ทั้งนี้ขึ้นอยู่กับโหมดที่อยู่: • ไบต์ 8 = โหมดที่กำหนดไว้ล่วงหน้า: 00h = การส่งผ่านถูกปิดใช้งาน 01h = ใช้ที่อยู่ IP ของ CMM ไบต์ 8:11 = ที่อยู่ IP ของเครือข่ายภายนอกของ IPv4 ในรูปเลขฐานสอง Bytes 8:23 = ที่อยู่ IP ของเครือข่ายภายนอกของ IPv6 ในรูปเลขฐานสอง รหัสการเสร็จสมบูรณ์: 00h – สำเร็จ 80h – ไม่รองรับพารามิเตอร์ C1h – ไม่รองรับคำสั่ง	CAh	ตั้งค่าพารามิเตอร์การกำหนดค่า LAN: ข้อมูล 1 สงวนไว้ (= 00h) ข้อมูล 2:3 หมายเลขพอร์ตอีเทอร์เน็ตผ่าน USB, LSByte เป็นอันดับแรก ข้อมูล 4:5 หมายเลขพอร์ตอีเทอร์เน็ตภายนอก, LSByte เป็นอันดับแรก จำนวนไบต์ที่ตามมาอาจแตกต่างกัน (1, 4 หรือ 16 ไบต์) ทั้งนี้ขึ้นอยู่กับโหมดที่อยู่: ข้อมูล 6 00h = ปิดใช้งานการส่งผ่าน 01h = ใช้ที่อยู่ IP ของ CMM ข้อมูล 6:9 ที่อยู่ IP ของเครือข่ายภายนอกของ IPv4 ในรูปเลขฐานสอง ข้อมูล 6:21 ที่อยู่ IP ของเครือข่ายภายนอกของ IPv6 ในรูปเลขฐานสอง

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
C7h – ความยาวของข้อมูลการร้องขอไม่ถูกต้อง		
พารามิเตอร์ OEM พารามิเตอร์นี้ใช้สำหรับตั้งค่าและรับที่อยู่ IP และตัวพรางเครือข่าย Lan over USB ของ XCC: ข้อมูลการตอบสนองจะส่งคืนค่าต่อไปนี้: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทานพารามิเตอร์ (ตามข้อมูลจำเพาะ IPMI) ไบต์ 3:10 = ที่อยู่ IP และค่าตัวพรางเครือข่าย (MS-byte) เป็นอันดับแรก	CBh	ข้อมูล 1:4 ที่อยู่ IP ของอินเทอร์เฟซ Lan over USB ในด้านของ XCC ข้อมูล 5:8 ตัวพรางเครือข่ายของอินเทอร์เฟซ Lan over USB ในด้านของ XCC
พารามิเตอร์ OEM พารามิเตอร์นี้ใช้สำหรับตั้งค่าและรับที่อยู่ IP Lan over USB ของ Host OS: ข้อมูลการตอบสนองจะส่งคืนค่าต่อไปนี้: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทานพารามิเตอร์ (ตามข้อมูลจำเพาะ IPMI) ไบต์ 3:6 = ที่อยู่ IP (MS-byte) เป็นอันดับแรก	CCh	ข้อมูล 1:4 ที่อยู่ IP ของอินเทอร์เฟซ Lan over USB ในด้านของโฮสต์

สืบค้นรายการอุปกรณ์แพคเกจแบบลอจิคัล

พารามิเตอร์ด้านล่างใช้ในการสืบค้นรายการอุปกรณ์แพคเกจ NCSI

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ในคำสั่งดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h การดำเนินการสืบค้นรายการอุปกรณ์แพคเกจ การดำเนินการสืบค้นข้อมูลแพคเกจจะดำเนินการโดยการออกคำขอโดยใช้ไบต์ข้อมูล 0x00 สองรายการนอกเหนือจากหมายเลขพารามิเตอร์ D3h สืบค้นรายการอุปกรณ์แพคเกจ : –> 0x0C 0x02 0x00 0xD3 0x00 0x00 การตอบสนองของ XCC ประกอบด้วยไบต์ของข้อมูลสำหรับแต่ละแพคเกจที่มีอยู่: บิต 7:4 = จำนวนของช่อง NCSI ในแพคเกจ บิต 3:0 = หมายเลขแพคเกจแบบลอจิคัล การตอบสนอง –> 0x00 0x00 0x40 0x01 0x32 ระบุว่ามีแพคเกจแบบลอจิคัลอยู่ 3 แพคเกจ:	D3h	ดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN:

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
แพคเกจ 0 มีช่อง NCSI 4 ช่อง แพคเกจ 1 ไม่ใช่ NCSI NIC จึงไม่รองรับช่อง NCSI แพคเกจ 2 มีช่อง NCSI 3 ช่อง		

ดู/ตั้งค่าข้อมูลแพคเกจแบบลอจิคัล

พารามิเตอร์ด้านล่างใช้เพื่ออ่านและกำหนดลำดับความสำคัญที่กำหนดให้กับแต่ละแพคเกจ

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ในคำสั่งดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h คำสั่งรองรับการดำเนินการ 2 อย่างดังนี้: • อ่านลำดับความสำคัญของแพคเกจ • ตั้งค่าลำดับความสำคัญของแพคเกจ การดำเนินการอ่านลำดับความสำคัญของแพคเกจ การดำเนินการอ่านลำดับความสำคัญของแพคเกจจะดำเนินการโดยการออกคำขอโดยใช้ไบต์ข้อมูล 0x00 สองรายการนอกเหนือจากหมายเลขพารามิเตอร์ D4h อ่านลำดับความสำคัญของแพคเกจ: –> 0x0C 0x02 0x01 0xD4 0x00 0x00 การตอบสนอง –> 0x00 0x00 0x00 0x12 0x23 แพคเกจแบบลอจิคัล 0 = ลำดับความสำคัญ 0 แพคเกจแบบลอจิคัล 2 = ลำดับความสำคัญ 1	D4	ดู/ตั้งค่าพารามิเตอร์การกำหนดค่า LAN: บิต [7-4] = ลำดับความสำคัญของแพคเกจแบบลอจิคัล (1 = สูงสุด, 15 = ต่ำสุด) บิต [3-0] = หมายเลขแพคเกจแบบลอจิคัล

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
แพคเกจแบบลอจิคัล 3 = ลำดับความสำคัญ 2 การดำเนินการตั้งค่าลำดับความสำคัญของแพคเกจ การดำเนินการตั้งค่าลำดับความสำคัญของแพคเกจจะดำเนินการโดยการออกคำขอโดยใช้พารามิเตอร์อย่างน้อยหนึ่งรายการนอกเหนือจากหมายเลขพารามิเตอร์ D4h ตั้งค่าลำดับความสำคัญของแพคเกจ: –> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 ตั้งค่าแพคเกจแบบลอจิคัล 0 = ลำดับความสำคัญ 0 ตั้งค่าแพคเกจแบบลอจิคัล 2 = ลำดับความสำคัญ 1 ตั้งค่าแพคเกจแบบลอจิคัล 3 = ลำดับความสำคัญ 2 การตอบสนอง: รหัสเสร็จสมบูรณ์เท่านั้น ไม่มีข้อมูลเพิ่มเติม		

ดู/ตั้งค่าสถานะการซิงโครไนซ์เครือข่าย XCC

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM ไบต์ใช้ในการกำหนดค่าเพื่อซิงโครไนซ์การตั้งค่าเครือข่ายระหว่างโหมดกำหนดให้เฉพาะและโหมด NIC ที่ใช้ร่วมกัน พารามิเตอร์นี้ในคำสั่งดูพารามิเตอร์การกำหนดค่า LAN ไม่ได้ใช้ตัวระบุการตั้งค่าหรือจำเป็นต้องมีตัวเลือกบล็อก ดังนั้นควรตั้งค่าฟิลด์เหล่านี้เป็น 00h ข้อมูลการตอบสนองจะส่งคืน 3 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = 00h (เปิดใช้งาน) หรือ 01h (ปิดใช้งาน)	D5h	ข้อมูล 1 0x00 = การซิงโครไนซ์ 0x01 = อิสระ

ไบต์ใช้ในการกำหนดค่าเพื่อซิงโครไนซ์การตั้งค่าเครือข่ายระหว่างโหมดกำหนดให้เฉพาะและโหมด NIC ที่ใช้ร่วมกัน มีค่าเริ่มต้นเป็น 0h ซึ่งหมายความว่า XCC จะอัปเดตการตั้งค่าเครือข่ายโดยอัตโนมัติระหว่างการเปลี่ยนโหมดและใช้ NIC ที่ใช้ร่วมกัน (บนแผง) เป็นการอ้างอิงหลัก หากตั้งค่าเป็น 1h ระบบจะทำการตั้งค่าเครือข่ายแต่ละรายการแยกจากกันที่นี่ ซึ่งเราสามารถกำหนดค่าการตั้งค่าเครือข่ายที่แตกต่างกันระหว่างโหมดต่างๆ เช่น เปิดใช้งาน VLAN ในโหมดกำหนดให้เฉพาะและตั้งค่า VLAN เป็นปิดใช้งานในโหมด NIC ที่ใช้ร่วมกัน

ดู/ตั้งค่าโหมดเครือข่าย XCC

พารามิเตอร์	#	ข้อมูลพารามิเตอร์
พารามิเตอร์ OEM พารามิเตอร์นี้ใช้ในการดู/ตั้งค่าโหมดเครือข่าย NIC การจัดการ XCC ข้อมูลการตอบสนองจะส่งคืน 4 ไบต์: ไบต์ 1 = รหัสการเสร็จสมบูรณ์ ไบต์ 2 = การตรวจทาน ไบต์ 3 = โหมดเครือข่ายที่ใช้/ระบุ ไบต์ 4 = ID แพคเกจของโหมดเครือข่ายที่ใช้ ไบต์ 5 = ID ช่องของโหมดเครือข่ายที่ใช้	D6h	ตั้งค่าพารามิเตอร์การกำหนดค่า LAN: ข้อมูล 1 โหมดเครือข่ายที่จะตั้งค่า ดูพารามิเตอร์การกำหนดค่า LAN: ข้อมูล 1 โหมดเครือข่ายที่จะดู นี่เป็นข้อมูลเสริมและเป็นค่าเริ่มต้นในการสืบค้นโหมดเครือข่ายปัจจุบัน

คำสั่ง OEM IPMI

XCC สนับสนุนคำสั่ง OEM IPMI ต่อไปนี้ แต่ละคำสั่งจะต้องใช้สิทธิ์พิเศษระดับต่างๆ ตามที่ระบุไว้ด้านล่าง

รหัส	คำสั่ง Netfn 0x2E	สิทธิ์พิเศษ
0xCC	รีเซ็ต XCC เป็นค่าเริ่มต้น	PRIV_USR

รหัส	คำสั่ง Netfn 0x3A	สิทธิ์พิเศษ
0x00	สืบค้นเวอร์ชันเฟิร์มแวร์	PRIV_USR
0x0D	ข้อมูลแผง	PRIV_USR
0x1E	ตัวเลือกการหน่วงเวลาการคืนค่าการจ่ายไฟกลับเข้าตัวเครื่อง	PRIV_USR
0x38	NMI และรีเซ็ต	PRIV_USR

รหัส	คำสั่ง Netfn 0x3A	สิทธิ์พิเศษ
0x49	เริ่มต้นการรวบรวมข้อมูล	PRIV_USR
0x4A	ดันไฟล์	PRIV_USR
0x4D	สถานะการรวบรวมข้อมูล	PRIV_USR
0x50	ดูข้อมูล Build	PRIV_USR
0x55	ดู/ตั้งค่าชื่อโฮสต์	PRIV_USR
0x6B	สืบค้นระดับการตรวจทานเฟิร์มแวร์ FPGA	PRIV_USR
0x6C	สืบค้นระดับการตรวจทานฮาร์ดแวร์ของแผง	PRIV_USR
0x6D	สืบค้นระดับการตรวจทานเฟิร์มแวร์ PSoC	PRIV_USR
0x98	การควบคุมพอร์ต FP USB	PRIV_USR
0xC7	สวิตช์ Native NM IPMI	PRIV_ADM

รีเซ็ต XCC เป็นคำสั่งเริ่มต้น

คำสั่งนี้จะรีเซ็ตการตั้งค่าการกำหนดค่า XCC เป็นค่าเริ่มต้น

ฟังก์ชันเครือข่าย = 0x2E			
รหัส	**คำสั่ง**	**ข้อมูลคำขอและการตอบสนอง**	**รายละเอียด**
0xCC	รีเซ็ต XCC เป็นค่าเริ่มต้น	**คำขอ**: ไบต์ 1 – 0x5EByte 2 – 0x2B ไบต์ 3 – 0x00 ไบต์ 4 – 0x0AByte 5 – 0x01 ไบต์ 6 – 0xFF ไบต์ 7 – 0x00Byte 8 – 0x00 ไบต์ 9 – 0x00 **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2 – 0x5EByte 3 – 0x2B ไบต์ 4 – 0x00 ไบต์ 5 – 0x0AByte 6 – 0x01 ไบต์ 7 – ข้อมูลการตอบสนอง 0 = สำเร็จ ไม่ใช่ศูนย์ = ล้มเหลว	คำสั่งนี้จะรีเซ็ตการตั้งค่าการกำหนดค่า XCC เป็นค่าเริ่มต้น

คำสั่งข้อมูลแผง/เฟิร์มแวร์

ส่วนนี้แสดงรายการคำสั่งต่างๆ สำหรับการสืบค้นข้อมูลแผงและเฟิร์มแวร์

ฟังก์ชันเครือข่าย = 0x3A			
รหัส	**คำสั่ง**	**ข้อมูลคำขอและการตอบสนอง**	**รายละเอียด**
0x00	สืบค้นเวอร์ชันเฟิร์มแวร์	**คำขอ**: ไม่มีข้อมูลตามคำขอ **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2 – เวอร์ชันหลัก ไบต์ 3 – เวอร์ชันรอง	คำสั่งนี้จะส่งคืนหมายเลขเวอร์ชันหลักและรองของเฟิร์มแวร์ หากคำสั่งทำงานร่วมกับข้อมูลการร้องขอเพิ่มเติม 1 ไบต์ การตอบสนองของ XCC จะส่งคืนฟิลด์ที่สาม (การตรวจทาน) ของเวอร์ชันด้วย (Major.Minor.Revision)
0x0D	สืบค้นข้อมูลแผง	**คำขอ**: N/A **การตอบสนอง**: ไบต์ 1 – ID ระบบ ไบต์ 2 – การตรวจทานแผง	คำสั่งนี้จะส่งคืน ID บอร์ดและการตรวจทาน Planar
0x50	สืบค้นข้อมูล Build	**คำขอ**: N/A **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2:10 – ชื่อ Build ASCIIZ ไบต์ 11:23 – วันที่ Build ASCIIZ ไบต์ 24:31 – เวลา Build ASCII	คำสั่งนี้จะส่งคืนชื่อ Build วันที่ Build และเวลา Build สตริงชื่อ Build และวันที่ Build จะมีการใช้ศูนย์เพื่อแสดงจุดสิ้นสุด รูปแบบของวันที่ Build คือ YYYY-MM-DD เช่น “ZUBT99A ” “2005-03-07” “23:59:59”

ฟังก์ชันเครือข่าย = 0x3A			
รหัส	**คำสั่ง**	**ข้อมูลคำขอและการตอบสนอง**	**รายละเอียด**
0x6B	สืบค้นระดับการตรวจทานเฟิร์มแวร์ FPGA	**คำขอ**: ไบต์ 1 – ประเภทอุปกรณ์ FPGA * ประเภทอุปกรณ์ FPGA 0 = ในเครื่อง (ระดับที่ใช้งานอยู่) 1 = การ์ด CPU 1 (ระดับที่ใช้งานอยู่) 2 = การ์ด CPU 2 (ระดับที่ใช้งานอยู่) 3 = การ์ด CPU 3 (ระดับที่ใช้งานอยู่) 4 = การ์ด CPU 4 (ระดับที่ใช้งานอยู่) 5 = ROM หลักในเครื่อง 6 = ROM การกู้คืนในเครื่อง **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2 – ระดับการตรวจทานหลัก ไบต์ 3 – ระดับการตรวจทานรอง ไบต์ 4 – ระดับการตรวจทานรองย่อย	คำสั่งนี้จะส่งคืนระดับการตรวจทานของเฟิร์มแวร์ FPGA หากไบต์ 1 ถูกตัดออก ระบบจะเลือกอุปกรณ์ภายในเครื่อง (ระดับที่ใช้งานอยู่)

ฟังก์ชันเครือข่าย = 0x3A			
รหัส	**คำสั่ง**	**ข้อมูลคำขอและการตอบสนอง**	**รายละเอียด**
		(ทดสอบไบต์บนแพลตฟอร์ XCC)	
0x6C	สืบค้นระดับการตรวจทานฮาร์ดแวร์ของแผง	**คำขอ**: ไม่มีข้อมูล **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2 – ระดับการตรวจทาน	คำสั่งนี้จะส่งคืนระดับการตรวจทานของฮาร์ดแวร์แผงที่ FPGA อยู่
0x6D	สืบค้นระดับการตรวจทานเฟิร์มแวร์ PSoC	**คำขอ**: ไม่มี **การตอบสนอง**: ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2 – bin# ไบต์ 3 – APID ไบต์ 4 – Rev ไบต์ 5-6 – FRU ID ไบต์ 6:N – ซ้ำไบต์ 2-6 สำหรับแต่ละ PSoC ที่ตรวจพบ	คำสั่งนี้จะส่งคืนระดับการตรวจทานของอุปกรณ์ PSoC ที่ตรวจพบทั้งหมด หมายเหตุ: bin# แสดงเป็นตำแหน่งจริง ดูรายละเอียดได้ที่ข้อมูลจำเพาะของระบบ

คำสั่งควบคุมระบบ

ข้อมูลจำเพาะ IPMI มีข้อมูลการเปิด/ปิดและรีเซ็ตพื้นฐาน Lenovo เพิ่มฟังก์ชันการควบคุมเพิ่มเติม

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x2E</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td>0x1E</td><td>ตัวเลือกการหน่วงเวลาการคืนค่าการจ่ายไฟกลับเข้าตัวเครื่อง</td><td>คำขอ:

<table><tr><td>ไบต์ 1</td><td>ประเภทคำขอ:

0x00 = ตั้งค่าตัวเลือกการหน่วงเวลา

0x01 = ตัวเลือกการหน่วงเวลาของการสืบค้น</td></tr><tr><td>ไบต์ 2</td><td>(หากไบต์ 1 = 0x00)

0x00 = ปิดใช้งาน (ค่าเริ่มต้น)

0x01 = สุ่ม

0x02 - 0xFF สงวนไว้</td></tr></table>
การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์

ไบต์ 2 – ตัวเลือกการหน่วงเวลา (สำหรับคำขอสืบค้นเท่านั้น)</td><td>การตั้งค่านี้จะใช้เมื่อมีการตั้งค่านโยบายการจ่ายไฟกลับเข้าระบบตัวเครื่องเป็นเปิดเครื่องอยู่ตลอดเวลา หรือคืนค่าเป็นเปิดเครื่อง (หากมีการเปิดเครื่องก่อนหน้านี้) หลังระบบใช้/คืนค่า AC มี 2 ทางเลือก: ปิดใช้งาน (การตั้งค่าเริ่มต้น ไม่มีการหน่วงเวลาเมื่อเปิดเครื่อง) และสุ่ม การตั้งค่าการหน่วงเวลาแบบสุ่มให้การหน่วงเวลาระหว่าง 1 ถึง 15 วินาที จากเวลาที่ระบบจะใช้/คืนค่า AC เมื่อเซิร์ฟเวอร์เปิดใช้งานโดยอัตโนมัติ

XCC รองรับคำสั่งนี้บนเซิร์ฟเวอร์ในแร็คเท่านั้น</td></tr>
<tr><td>0x38</td><td>NMI และรีเซ็ต</td><td>คำขอ:

ไบต์ 1 – จำนวนวินาที</td><td>คำสั่งนี้ใช้ในการทำ NMI ระบบ อาจมีการรีเซ็ตระบบ (รีบูต) หรือปิด/เปิดเครื่องใหม่หลัง NMI</td></tr>
</table>

ฟังก์ชันเครือข่าย = 0x2E			
รหัส	**คำสั่ง**	**ข้อมูลคำขอและการตอบสนอง**	**รายละเอียด**
		0 = NMI เท่านั้น ไบต์ 2 – ประเภทการรีเซ็ต 0 = ซอฟต์รีเซ็ต 1 = ปิด/เปิดเครื่องใหม่ **การตอบสนอง** : ไบต์ 1 – รหัสการเสร็จสมบูรณ์	หากฟิลด์ “จำนวนวินาที” ไม่เป็น 0 ระบบจะรีเซ็ตหรือปิด/เปิดเครื่องใหม่หลังจากจำนวนวินาทีที่ระบุ ไบต์ 2 ของคำขอจะระบุหรือไม่ก็ได้ หากไม่มีการระบุไบต์ 2 หรือหากมีค่าเป็น 0x00 ระบบจะทำการซอฟต์รีเซ็ต หากไบต์ 2 เป็น 0x01 ระบบจะปิด/เปิดเครื่องใหม่

คำสั่งอื่นๆ

ส่วนนี้เป็นคำสั่งที่ไม่เข้ากับส่วนอื่นๆ

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr>
<td>0x55</td>
<td>ดู/ตั้งค่าชื่อโฮสต์</td>
<td>ความยาวของคำขอ = 0:

ข้อมูลคำขอว่างเปล่า

การตอบสนอง:

<table>
<tr><td>ไบต์ 1</td><td>รหัสการเสร็จสมบูรณ์</td></tr>
<tr><td>ไบต์ 2-65</td><td>ชื่อโฮสต์ปัจจุบัน

ASCIIZ, สตริงที่มี Null บอกจุดสิ้นสุด</td></tr>
</table>

ความยาวของคำขอ 1-64:

<table>
<tr><td>ไบต์ 1-64</td><td>ชื่อโฮสต์ DHCP

ASCIIZ ลงท้ายด้วย 00h</td></tr>
</table>
</td>
<td>ใช้คำสั่งนี้เพื่อดู/ตั้งค่าชื่อโฮสต์

เมื่อตั้งค่าชื่อโฮสต์ ต้องลงท้ายค่าที่ต้องการด้วย 00h ชื่อโฮสต์ถูกจำกัดไว้ที่ 63 อักขระและลงท้ายด้วย Null</td>
</tr>
<tr>
<td>0x98</td>
<td>การควบคุมพอร์ต FP USB</td>
<td>คำขอ:

ไบต์ 1

<table>
<tr><td>01h:</td><td>ดูเจ้าของปัจจุบันของพอร์ต USB บนแผงด้านหน้า</td></tr>
</table>
</td>
<td>คำสั่งนี้ใช้สำหรับสถานะการสืบค้น/การกำหนดค่าพอร์ต FP USB, กำหนดค่าโหมด/การหมดเวลาของพอร์ต FP USB และสลับเจ้าของพอร์ต USB ระหว่างโฮสต์และ BMC

ในการกำหนดค่า FP USB สามารถมีได้ 3 โหมด – กำหนดให้เฉพาะโฮสต์ กำหนดให้เฉพาะ BMC หรือโหมดแบบใช้งานร่วมกันซึ่งอนุญาต</td>
</tr>
</table>

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td></td><td></td><td>การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์

ไบต์ 2

<table><tr><td>00h</td><td>โฮสต์เป็นเจ้าของ</td></tr><tr><td>01h:</td><td>BMC เป็นเจ้าของ</td></tr></table>
คำขอ:

ไบต์ 1

<table><tr><td>02h:</td><td>ดูการกำหนดค่าของพอร์ต USB บนแผงด้านหน้า</td></tr></table>
การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์

ไบต์ 2

<table><tr><td>00h</td><td>กำหนดให้เฉพาะโฮสต์</td></tr><tr><td>01h:</td><td>กำหนดให้เฉพาะ BMC</td></tr><tr><td>02h:</td><td>โหมดแบบใช้งานร่วมกัน</td></tr></table></td><td>ให้สลับเจ้าของไปมาระหว่างโฮสต์และ BMC ได้

หากเปิดใช้งานโหมดแบบใช้งานร่วมกัน พอร์ต USB จะเชื่อมต่อกับ BMC เมื่อเซิร์ฟเวอร์ปิดและเชื่อมต่อกับเซิร์ฟเวอร์เมื่อเซิร์ฟเวอร์เปิด

เมื่อเปิดใช้งานโหมดแบบใช้งานร่วมกันและเปิดเครื่องเซิร์ฟเวอร์ BMC จะส่งคืนพอร์ต USB กลับไปยังเซิร์ฟเวอร์ หลังจากเกิดการหมดเวลาเมื่อไม่มีการใช้งานในการกำหนดค่า

หากเซิร์ฟเวอร์มีปุ่มระบุสถานะ ผู้ใช้สามารถเปิดใช้งาน/ปิดใช้งานปุ่ม ID เพื่อสลับเจ้าของพอร์ต FP USB ได้ โดยกดปุ่ม ID ค้างไว้นานกว่า 3 วินาที

ระบบจะตั้งค่าฮิสเทอรีซิสเป็นวินาทีเมื่อสลับพอร์ตโดยอัตโนมัติระหว่างการปิด/เปิดเครื่อง นี่เป็นพารามิเตอร์เสริม

เซิร์ฟเวอร์ SD530

พอร์ตนี้จะเป็นตัวเลือกเสริมบนแพลตฟอร์มเซิร์ฟเวอร์ SD530 และจะแสดงเมื่อมีการเชื่อมต่อโดยตรงกับ XCC และเฉพาะกับ XCC เท่านั้น การสลับพอร์ตไปยังโฮสต์ไม่พร้อมใช้งาน

• เมื่อป้อนคำสั่งด้วยไบต์ 1 = 1 XCC จะตอบสนองว่าพอร์ตเป็น</td></tr>
</table>

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td></td><td></td><td>ไบต์ 3:4 – การหมดเวลาเมื่อไม่มีการใช้งานเป็นนาที (MSB เป็นอันดับแรก)

ไบต์ 5 – เปิดใช้งานปุ่ม ID

<table><tr><td>00h</td><td>ปิดใช้งาน</td></tr><tr><td>01h:</td><td>เปิดใช้งาน</td></tr></table>
ไบต์ 6 – ฮิสเทอรีซิส (ตัวเลือกเสริม) เป็นวินาที

คำขอ:

ไบต์ 1

03h: ตั้งค่าการกำหนดค่าของพอร์ต USB บนแผงด้านหน้า

ไบต์ 2

<table><tr><td>00h</td><td>กำหนดให้เฉพาะโฮสต์</td></tr><tr><td>01h:</td><td>กำหนดให้เฉพาะ BMC</td></tr><tr><td>02h:</td><td>โหมดแบบใช้งานร่วมกัน</td></tr></table>
ไบต์ 3:4 – การหมดเวลาเมื่อไม่มีการใช้งานเป็นนาที (MSB เป็นอันดับแรก)</td><td>ของ BMC เสมอ
• เมื่อป้อนคำสั่งด้วยไบต์ 1 = 2 XCC จะตอบสนองว่าพอร์ตกำหนดให้เฉพาะ BMC เสมอ
• เมื่อป้อนคำสั่งด้วยไบต์ 1 = 3 หรือไบต์ 1 = 4 XCC จะตอบสนองด้วยรหัสการเสร็จสมบูรณ์ D6h

เซิร์ฟเวอร์ที่ไม่ใช่ SD530

บนแพลตฟอร์มที่ไม่เซิร์ฟเวอร์ SD530 การใช้งานของพอร์ต USB บนแผงด้านหน้าของ XCC สามารถปิดใช้งานได้โดยเปลี่ยนเป็นโหมด “โฮสต์เท่านั้น”

เมื่อป้อนคำสั่งด้วยไบต์ 1 = 5 หรือไบต์ 1 = 6 XCC จะตอบสนองด้วยรหัสการเสร็จสมบูรณ์ D6h</td></tr>
</table>

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td></td><td></td><td>ไบต์ 5 – เปิดใช้งานปุ่ม ID

<table><tr><td>00h</td><td>ปิดใช้งาน</td></tr><tr><td>01h:</td><td>เปิดใช้งาน</td></tr></table>
ไบต์ 6 – ฮิสเทอรีซิส (ตัวเลือกเสริม) เป็นวินาที

การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์ ไบต์ 2

<table><tr><td>00h</td><td>สลับไปเป็นโฮสต์</td></tr><tr><td>01h:</td><td>สลับไปเป็น BMC</td></tr></table>
การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์

ไบต์ 1

<table><tr><td>05h:</td><td>เปิดใช้งาน/ปิดใช้งานพอร์ต USB บนแผงด้านหน้า</td></tr></table>
ไบต์ 2</td><td></td></tr>
</table>

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td></td><td></td><td><table><tr><td>00h</td><td>ปิดใช้งาน</td></tr><tr><td>01h:</td><td>เปิดใช้งาน</td></tr></table>
การตอบสนอง:

ไบต์ 1 – รหัสการเสร็จสมบูรณ์

คำขอ:

ไบต์ 1

<table><tr><td>06h:</td><td>อ่านสถานะการเปิดใช้งาน/ปิดใช้งานของพอร์ต USB บนแผงด้านหน้า</td></tr></table>
การตอบสนอง:

ไบต์ 1 - รหัสการเสร็จสมบูรณ์

ไบต์ 2</td><td></td></tr>
<tr><td>0xC7</td><td>สวิตช์ Native NM IPMI</td><td>ความยาวของคำขอ = 0:

ข้อมูลคำขอว่างเปล่า

การตอบสนอง:

<table><tr><td>ไบต์ 1</td><td>รหัสการเสร็จสมบูรณ์</td></tr></table></td><td>คำสั่งนี้ใช้ในการเปิดใช้งาน/ปิดใช้งานฟังก์ชันการบริดจ์ของ XCC สำหรับคำสั่ง Native Intel IPMI</td></tr>
</table>

<table>
<tr><th colspan="4">ฟังก์ชันเครือข่าย = 0x3A</th></tr>
<tr><th>รหัส</th><th>คำสั่ง</th><th>ข้อมูลคำขอและการตอบสนอง</th><th>รายละเอียด</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>ไบต์ 2</td><td>สถานะเปิดใช้งาน/ปิดใช้งานปัจจุบัน</td></tr>
</table>
ความยาวของคำขอ= 1:
<table>
<tr><td>ไบต์ 1</td><td>แอตทริบิวต์การเปิดใช้งาน/การปิดใช้งานอินเทอร์เฟซ Native NM IPMI

00h – ปิดใช้งาน

01h – เปิดใช้งาน</td></tr>
</table>
การตอบสนอง:
<table>
<tr><td>ไบต์ 1</td><td>รหัสการเสร็จสมบูรณ์</td></tr>
</table>
</td><td></td></tr>
</table>

บทที่ 13. เซิร์ฟเวอร์แบบ Edge

หัวข้อนี้จะอธิบายฟังก์ชันเฉพาะสำหรับเซิร์ฟเวอร์แบบ Edge

หมายเหตุ:

1. ระบบจะขอให้คุณเปลี่ยนรหัสผ่าน XCC ครั้งแรกที่คุณเข้าสู่ระบบ
2. IPMI ผ่าน LAN ถูกปิดใช้งานตามค่าเริ่มต้น
3. IPMI ผ่าน KCS ถูกปิดใช้งานตามค่าเริ่มต้น

โหมดจำกัดการเข้าถึงระบบ

เมื่อ**โหมดจำกัดการเข้าถึงระบบ**อยู่ในสถานะเปิดใช้งาน หมายความว่าระบบอยู่ในโหมดจำกัดการเข้าถึงระบบ คุณสามารถเปิดใช้งานระบบและปลดล็อค มิฉะนั้นระบบโฮสต์จะบูตไม่ได้

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า** BMC และเลื่อนไปที่ **โหมดจำกัดการเข้าถึงระบบ**

โหมดจำกัดการเข้าถึงระบบ

หากต้องการเปิดใช้งานระบบและออกจาก**โหมดจำกัดการเข้าถึงระบบ** ให้ทำตามขั้นตอนต่อไปนี้

1. คลิกปุ่ม **ไม่มีการใช้งาน** และหน้าต่าง Key Vault Activation จะปรากฏขึ้นเพื่อแสดง **ข้อความคำถาม**
2. ติดต่อผู้ดูแลระบบ IT และแสดง**ข้อความคำถาม**
3. รับข้อมูล**ถาม-ตอบ**จากผู้ดูแลระบบ IT และป้อนลงในหน้าต่าง Key Vault Activation
4. คลิกปุ่ม **ตกลง** แล้วคลิก **ใช้**
5. หากการตั้งค่าทั้งหมดทำงานอย่างถูกต้องแล้ว คุณจะเห็น**โหมดจำกัดการเข้าถึงระบบ**เปลี่ยนเป็น**ไม่มีการใช้งาน**

หมายเหตุ: เมื่อโหมดจำกัดการเข้าถึงระบบอยู่ในสถานะเปิดใช้งาน การเข้าถึงความลับของระบบจะ**ถูกปฏิเสธ** เช่น SED Authentication Key

หากต้องบังคับให้ระบบเข้าสู่โหมดจำกัดการเข้าถึงระบบ ให้ทำตามขั้นตอนต่อไปนี้

1. คลิกปุ่ม **เปิดใช้งาน**
2. คลิกปุ่ม **ตกลง** แล้วคลิก **ใช้**

การตรวจจับการเคลื่อนไหว

คุณสามารถเปิดใช้งานฟังก์ชันนี้เพื่อป้องกันเซิร์ฟเวอร์โดยการตรวจจับการเคลื่อนไหวทางกายภาพของเซิร์ฟเวอร์

หากมีการเปิดใช้งานการตรวจจับความเคลื่อนไหว คุณสามารถตั้งค่ารายการต่อไปนี้ได้ทั้งนี้ขึ้นอยู่กับการกำหนดลักษณะและการติดตั้งของคุณ

- **ระดับความไว**: เลือกระดับความไวจาก**ต่ำ ปานกลาง** และ**สูง**ตามความต้องการของคุณ
- **แนวตำแหน่ง**: เลือกการติดตั้งจาก**แท่นวางตั้งโต๊ะ โครงยึดแบบติดผนัง (แนวนอน) โครงยึดแบบติดผนัง (แนวตั้ง) ชั้นวาง** และ**โครงยึดแบบติดเพดาน**

หมายเหตุ: การตรวจจับการเคลื่อนไหวจะถูกปิดใช้งานโดยอัตโนมัติเมื่อระบบเข้าสู่โหมดจำกัดการเข้าถึง

การตรวจจับการบุกรุกตัวเครื่อง

คุณสามารถเปิดใช้งานฟังก์ชันนี้เพื่อป้องกันเซิร์ฟเวอร์โดยการตรวจจับการเคลื่อนไหวทางกายภาพของฝาครอบด้านบน

การกำหนดค่าเพิ่มเติม

หากมีการติดตั้งแพคเกจ LOM แบบเปิดใช้งานระบบไร้สาย คุณสามารถเลือกการตั้งค่าสำหรับเหตุการณ์การงัดแงะที่ตรวจพบได้สามรายการ

ในบางกรณี**ข้อความคำถาม**อาจไม่สามารถตรวจสอบได้โดย ThinkShield Key Vault Portal และอาจจำเป็นต้องรีเซ็ตตัวนับภายในอุปกรณ์ก่อนที่จะเปิดใช้งานอุปกรณ์ภายใต้คำขอของผู้ดูแลระบบ IT

ผู้จัดการ SED Authentication Key (AK)

หากต้องการติดตั้งระบบด้วย SED (ไดรฟ์แบบเข้ารหัสด้วยตนเอง) คุณลักษณะนี้จะควบคุม BMC เพื่อปรับใช้ SED Authentication Key คุณสามารถใช้ SED Authentication Key เพื่อเข้ารหัสไดรฟ์บูตและข้อมูลและบูตระบบโดยไม่ต้องเข้ามาจัดการด้วยตัวเอง

หมายเหตุ: ไม่อนุญาตให้ดำเนินขั้นตอนนี้เมื่อระบบไม่ได้เปิดใช้งาน (อยู่ในโหมดจำกัดการเข้าถึงระบบ) หรือผู้ใช้ปัจจุบันไม่มีสิทธิ์ในการจัดการ SED Authentication Key

คลิก **การรักษาความปลอดภัย** ภายใต้ **การกำหนดค่า** BMC และเลื่อนไปที่ **ผู้จัดการ** SED Authentication Key (AK)

เปลี่ยน SED AK

สร้าง SED AK **จากวลีรหัสผ่าน**: ตั้งรหัสผ่านและป้อนรหัสผ่านอีกครั้งเพื่อยืนยัน คลิก **สร้างใหม่** เพื่อรับ SED AK ใหม่

สร้าง SED AK **แบบสุ่ม**: คลิก **สร้างใหม่** เพื่อรับ SED AK แบบสุ่ม

สำรองข้อมูล SED AK: ตั้งรหัสผ่านและป้อนรหัสผ่านใหม่เพื่อยืนยัน คลิก **เริ่มสำรองข้อมูล** เพื่อสำรองข้อมูล SED AK จากนั้นให้ดาวโหลดไฟล์ SED AK และเก็บรักษาไว้เพื่อใช้ในอนาคต

หมายเหตุ: หากคุณใช้ไฟล์ SED AK สำรองเพื่อกู้คืนข้อมูลการกำหนดค่า ระบบจะขอให้คุณใส่รหัสผ่านที่ตั้งไว้ที่นี่

กู้คืนข้อมูล SED AK: คุณสามารถดำเนินการขั้นตอนนี้ได้ก็ต่อเมื่อ SED ทำงานไม่ถูกต้อง การกู้คืนข้อมูล SED AK สามารถทำได้สองวิธีด้วยกันคือ:

- **กู้คืนข้อมูล** SED AK **โดยใช้วลีรหัสผ่าน**: ใช้รหัสผ่านที่ตั้งในโหมด **สร้าง** SED AK **จากวลีรหัสผ่าน** เพื่อกู้คืนข้อมูล SED AK
- **กู้คืนข้อมูล** SED AK **จากไฟล์สำรอง**: อัปโหลดไฟล์สำรองข้อมูลที่สร้างขึ้นในโหมด **สำรองข้อมูล** SED AK และป้อนรหัสผ่านไฟล์สำรองเพื่อกู้คืน SED AK

เครือข่ายแบบ Edge

ระบบจะรองรับหน้าฟังก์ชันนี้เฉพาะขณะที่มีการติดตั้งแพคเกจ LOM แบบเปิดใช้งานระบบไร้สาย

สำหรับตารางการกำหนดค่าเริ่มต้นเครือข่ายโทโพโลยี โปรดดูข้อมูลเพิ่มเติมที่ https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html

การเชื่อมต่อ Wi-Fi

คลิก **เปิดใช้งาน** และคุณจะกำหนดค่าการตั้งค่าตามการกำหนดค่า Wi-Fi ได้

การเชื่อมต่อ LTE

ช่วยให้คุณสามารถควบคุมการเชื่อมต่อ LTE สำหรับแผงเครือข่ายแบบ Edge ได้

ที่อยู่แผงเครือข่ายแบบ Edge

สถานะ IPv4 **หรือ** IPv6	**สถานะเซิร์ฟเวอร์** DHCP	**วิธีการ**
ปิดใช้งาน	**ปิดใช้งาน**	**รับ** IP **จาก** DHCP
เปิดใช้งาน	**เปิดใช้งาน**	**ใช้ที่อยู่** IP **แบบคงที่**
เปิดใช้งาน	**ปิดใช้งาน**	**รับ** IP **จาก** DHCP **หรือ ใช้ที่อยู่** IP **แบบคงที่** ขึ้นอยู่กับการใช้งานของคุณ

บริดจ์เครือข่าย BMC

คุณสามารถเข้าถึง BMC ผ่าน **พอร์ตดาวน์ลิงก์**, **พอร์ต** Wi-Fi, **พอร์ตอัปลิงก์** หรือ **ไม่มี**

หมายเหตุ: เลือก **ไม่มี** เพื่อปิดใช้งานฟังก์ชันนี้

การแก้ไขปัญหาแผงเครือข่ายแบบ Edge

รีสตาร์ททันที: คุณสามารถรีสตาร์ทแผงระบบเครือข่ายได้โดยใช้ปุ่มนี้

รีเซ็ตเป็นค่าเริ่มต้นจากโรงงาน: คุณสามารถรีเซ็ตแผงเครือข่ายเป็นการตั้งค่าเริ่มต้นโดยใช้ปุ่มนี้

ภาคผนวก A. การขอความช่วยเหลือและความช่วยเหลือด้านเทคนิค

หากคุณต้องการความช่วยเหลือ การบริการ หรือความช่วยเหลือด้านเทคนิค หรือเพียงแค่ต้องการข้อมูลเพิ่มเติมเกี่ยวกับผลิตภัณฑ์ Lenovo คุณจะพบว่า Lenovo นั้นมีแหล่งข้อมูลมากมายที่พร้อมจะให้ความช่วยเหลือคุณ

บน World Wide Web ข้อมูลล่าสุดเกี่ยวกับระบบ อุปกรณ์เสริม การให้บริการ และการสนับสนุนของ Lenovo มีให้บริการที่:

http://datacentersupport.lenovo.com

หมายเหตุ: หัวข้อนี้มีข้อมูลอ้างอิงถึงเว็บไซต์ IBM และข้อมูลเกี่ยวกับการขอรับการบริการ IBM คือผู้ให้บริการ ThinkSystem ของ Lenovo

ก่อนโทรศัพท์ติดต่อ

ก่อนที่คุณจะโทรศัพท์ติดต่อ มีขั้นตอนต่างๆ ดังต่อไปนี้ที่คุณสามารถทดลองเพื่อพยายามแก้ปัญหาด้วยตัวคุณเองก่อน อย่างไรก็ตาม หากคุณจำเป็นต้องโทรศัพท์ติดต่อเพื่อขอรับความช่วยเหลือ โปรดรวบรวมข้อมูลที่จำเป็นสำหรับช่างเทคนิคบริการ เพื่อให้เราสามารถแก้ไขปัญหาให้คุณได้อย่างรวดเร็ว

พยายามแก้ไขปัญหาด้วยตัวเอง

คุณอาจสามารถแก้ไขปัญหาได้โดยไม่ต้องขอรับความช่วยเหลือจากภายนอกโดยการทำตามขั้นตอนการแก้ไขปัญหาที่ Lenovo เตรียมไว้ให้ในวิธีใช้แบบออนไลน์หรือในเอกสารเกี่ยวกับผลิตภัณฑ์ Lenovo เอกสารเกี่ยวกับผลิตภัณฑ์ Lenovo ยังอธิบายข้อมูลเกี่ยวกับการทดสอบการวินิจฉัยซึ่งคุณสามารถนำไปดำเนินการเองได้ เอกสารข้อมูลเกี่ยวกับระบบ ระบบปฏิบัติการ และโปรแกรมส่วนใหญ่จะมีขั้นตอนการแก้ไขปัญหาและคำอธิบายเกี่ยวกับข้อความแสดงข้อผิดพลาดและรหัสข้อผิดพลาด หากคุณสงสัยว่าเป็นปัญหาเกี่ยวกับซอฟต์แวร์ โปรดดูเอกสารข้อมูลเกี่ยวกับระบบปฏิบัติการหรือโปรแกรม

คุณสามารถอ่านเอกสารเกี่ยวกับผลิตภัณฑ์ ThinkSystem ของคุณได้จาก:

http://thinksystem.lenovofiles.com/help/index.jsp

คุณสามารถดำเนินการตามขั้นตอนดังต่อไปนี้เพื่อพยายามแก้ปัญหาด้วยตัวคุณเองก่อน:

- ตรวจสอบสายเคเบิลทั้งหมดเพื่อให้แน่ใจว่าสายทั้งหมดเชื่อมต่อเรียบร้อยแล้ว
- ตรวจสอบสวิตช์เปิดปิดเพื่อให้แน่ใจว่าระบบและอุปกรณ์เสริมเปิดอยู่

- ตรวจสอบว่าผลิตภัณฑ์ Lenovo ของคุณมีซอฟต์แวร์ เฟิร์มแวร์ และไดรเวอร์อุปกรณ์ระบบปฏิบัติการที่อัปเดตแล้ว ข้อกำหนดและเงื่อนไขของ Lenovo Warranty ระบุให้คุณซึ่งเป็นเจ้าของผลิตภัณฑ์ Lenovo เป็นผู้รับผิดชอบในการบำรุงรักษาและอัปเดตซอฟต์แวร์และเฟิร์มแวร์ทั้งหมดให้กับผลิตภัณฑ์ (เว้นแต่ผลิตภัณฑ์ครอบคลุมโดยสัญญาการบำรุงรักษาเพิ่มเติม) ช่างเทคนิคบริการจะร้องขอให้คุณอัปเกรดซอฟต์แวร์และเฟิร์มแวร์ของคุณ หากปัญหาที่พบมีวิธีแก้ไขที่บันทึกไว้ในเอกสารเกี่ยวกับการอัปเกรดซอฟต์แวร์
- หากคุณได้ติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใหม่ในสภาพแวดล้อมระบบของคุณ โปรดตรวจสอบ http://www.lenovo.com/serverproven/ เพื่อให้แน่ใจว่าผลิตภัณฑ์รองรับฮาร์ดแวร์และซอฟต์แวร์ดังกล่าว
- โปรดไปที่ http://datacentersupport.lenovo.com เพื่อตรวจสอบข้อมูลเพื่อช่วยคุณแก้ไขปัญหา
  - คลิกที่กระดานสนทนา Lenovo ที่ https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg เพื่อดูว่ามีบุคคลอื่นที่กำลังประสบปัญหาที่คล้ายคลึงกันหรือไม่

คุณอาจสามารถแก้ไขปัญหาได้โดยไม่ต้องขอรับความช่วยเหลือจากภายนอกโดยการทำตามขั้นตอนการแก้ไขปัญหาที่ Lenovo เตรียมไว้ให้ในวิธีใช้แบบออนไลน์หรือในเอกสารเกี่ยวกับผลิตภัณฑ์ Lenovo เอกสารเกี่ยวกับผลิตภัณฑ์ Lenovo ยังอธิบายข้อมูลเกี่ยวกับการทดสอบการวินิจฉัยซึ่งคุณสามารถนำไปดำเนินการเองได้ เอกสารข้อมูลเกี่ยวกับระบบ ระบบปฏิบัติการ และโปรแกรมส่วนใหญ่จะมีขั้นตอนการแก้ไขปัญหาและคำอธิบายเกี่ยวกับข้อความแสดงข้อผิดพลาดและรหัสข้อผิดพลาด หากคุณสงสัยว่าเป็นปัญหาเกี่ยวกับซอฟต์แวร์ โปรดดูเอกสารข้อมูลเกี่ยวกับระบบปฏิบัติการหรือโปรแกรม

รวบรวมข้อมูลที่จำเป็นในการโทรขอรับการสนับสนุน

หากคุณเชื่อว่าจำเป็นต้องขอรับบริการตามการรับประกันสำหรับผลิตภัณฑ์ Lenovo ของคุณ ช่างเทคนิคบริการจะสามารถช่วยเหลือคุณได้อย่างมีประสิทธิภาพมากขึ้นหากคุณเตรียมความพร้อมก่อนที่จะโทรศัพท์ติดต่อ คุณยังสามารถดูที่ http://datacentersupport.lenovo.com/warrantylookup สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการรับประกันผลิตภัณฑ์ของคุณ

รวบรวมข้อมูลต่อไปนี้เพื่อมอบให้กับช่างเทคนิคบริการ ข้อมูลนี้จะช่วยให้ช่างเทคนิคบริการสามารถแก้ไขปัญหาได้อย่างรวดเร็ว และมั่นใจว่าคุณจะได้รับการบริการตามที่ระบุไว้ในสัญญา

- หมายเลขของสัญญาข้อตกลงเกี่ยวกับการบำรุงรักษาฮาร์ดแวร์และซอฟต์แวร์ หากมี
- หมายเลขประเภทเครื่อง (ตัวระบุเครื่อง 4 หลักของ Lenovo)
- หมายเลขรุ่น
- หมายเลขประจำเครื่อง
- UEFI และระดับของเฟิร์มแวร์ของระบบในปัจจุบัน
- ข้อมูลที่เกี่ยวข้องอื่นๆ เช่น ข้อความแสดงข้อผิดพลาด และบันทึก

อีกทางเลือกหนึ่งนอกจากการโทรติดต่อฝ่ายสนับสนุนของ Lenovo คุณสามารถไปที่ https://www-947.ibm.com/support/servicerequest/Home.action เพื่อเพื่อยื่นคำขอรับบริการอิเล็กทรอนิกส์ การยื่นคำขอรับบริการอิเล็กทรอนิกส์จะ

เป็นการเริ่มกระบวนการกำหนดวิธีแก้ไขปัญหาโดยการให้ข้อมูลที่เกี่ยวข้องอื่นๆ แก่ช่างเทคนิคบริการ ช่างเทคนิคบริการของ Lenovo สามารถเริ่มหาวิธีแก้ปัญหาให้กับคุณทันทีที่คุณได้กรอกและยื่นคำขอรับบริการอิเล็กทรอนิกส์เรียบร้อยแล้ว

การรวบรวมข้อมูลการซ่อมบำรุง

เพื่อระบุต้นตอของปัญหาเกี่ยวกับเซิร์ฟเวอร์หรือตามที่มีการร้องขอโดยฝ่ายสนับสนุนของ Lenovo คุณอาจต้องทำการรวบรวมข้อมูลการซ่อมบำรุงที่สามารถนำไปใช้ในการวิเคราะห์ต่อไปได้ ข้อมูลการซ่อมบำรุงประกอบด้วยข้อมูล อาทิเช่น บันทึกเหตุการณ์และรายการฮาร์ดแวร์

ข้อมูลการซ่อมบำรุงสามารถรวบรวมโดยใช้เครื่องมือดังต่อไปนี้:

- Lenovo XClarity Controller

  คุณสามารถใช้เว็บอินเทอร์เฟซ Lenovo XClarity Controller หรือ CLI ในการรวบรวมข้อมูลการซ่อมบำรุงสำหรับเซิร์ฟเวอร์ ไฟล์นี้สามารถบันทึกข้อและส่งกลับมายังฝ่ายสนับสนุนของ Lenovo

  - สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้เว็บอินเทอร์เฟซในการรวบรวมข้อมูลการซ่อมบำรุง โปรดดู http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/NN1ia_c_servicesandsupport.html
  - สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ CLI ในการรวบรวมข้อมูลการซ่อมบำรุง โปรดดู http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/nn1ia_r_ffdccommand.html

- Lenovo XClarity Administrator

  สามารถตั้งค่า Lenovo XClarity Administrator ให้เก็บรวบรวมและส่งไฟล์การวินิจฉัยไปที่ฝ่ายสนับสนุนของ Lenovo โดยอัตโนมัติ เมื่อเกิดเหตุการณ์ที่สามารถซ่อมบำรุงได้บางเหตุการณ์ใน Lenovo XClarity Administrator และปลายทางที่มีการจัดการ คุณสามารถเลือกที่จะส่งไฟล์การวินิจฉัยไปที่ บริการสนับสนุนของ Lenovo โดยใช้ Call Home หรือไปที่ผู้ให้บริการรายอื่นโดยใช้ SFTP นอกจากนี้ คุณยังสามารถเก็บรวบรวมไฟล์การวินิจฉัย เปิดบันทึกปัญหา และส่งไฟล์การวินิจฉัยไปที่ศูนย์ฝ่ายสนับสนุนของ Lenovo ด้วยตนเอง

  คุณสามารถค้นหาข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าการแจ้งเตือนปัญหาอัตโนมัติภายใน Lenovo XClarity Administrator ที่ http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html

- Lenovo XClarity Provisioning Manager

  ใช้ฟังก์ชันรวบรวมข้อมูลการซ่อมบำรุงของ Lenovo XClarity Provisioning Manager เพื่อรวบรวมข้อมูลการซ่อมบำรุงระบบ คุณสามารถรวบรวมข้อมูลบันทึกระบบที่มีอยู่ หรือเรียกใช้การวินิจฉัยใหม่เพื่อรวบรวมข้อมูลใหม่

- Lenovo XClarity Essentials

สามารถเรียกใช้ Lenovo XClarity Essentials ภายในจากระบบปฏิบัติการ นอกเหนือจากข้อมูลการซ่อมบำรุงฮาร์ดแวร์ Lenovo XClarity Essentials สามารถรวบรวมข้อมูลเกี่ยวกับระบบปฏิบัติการ เช่น บันทึกเหตุการณ์ของระบบปฏิบัติการ

ในการรับข้อมูลการซ่อมบำรุง คุณสามารถเรียกใช้คำสั่ง `getinfor` สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการเรียกใช้ `getinfor` โปรดดู http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/onecli_r_getinfor_command.html

---

การติดต่อฝ่ายสนับสนุน

คุณสามารถติดต่อฝ่ายสนับสนุนเพื่อรับความช่วยเหลือสำหรับปัญหาของคุณ

คุณสามารถรับการบริการด้านฮาร์ดแวร์ผ่านผู้ให้บริการที่ได้รับอนุญาตจาก Lenovo หากต้องการค้นหาผู้ให้บริการที่ได้รับอนุญาตจาก Lenovo ในการให้บริการรับประกัน โปรดไปที่ https://datacentersupport.lenovo.com/us/en/serviceprovider และใช้การค้นหาด้วยตัวกรองสำหรับแต่ละประเทศ โปรดดูหมายเลขโทรศัพท์ของฝ่ายสนับสนุนของ Lenovo ที่ https://datacentersupport.lenovo.com/us/en/supportphonelist สำหรับรายละเอียดการสนับสนุนในภูมิภาคของคุณ

ภาคผนวก B. คำประกาศ

Lenovo อาจจะไม่สามารถจำหน่ายผลิตภัณฑ์ บริการ หรือคุณลักษณะที่กล่าวไว้ในเอกสารนี้ได้ในทุกประเทศ กรุณาติดต่อตัวแทน Lenovo ประจำท้องถิ่นของคุณเพื่อขอข้อมูลเกี่ยวกับผลิตภัณฑ์และบริการที่มีอยู่ในปัจจุบันในพื้นที่ของคุณ

การอ้างอิงใดๆ ถึงผลิตภัณฑ์, โปรแกรม หรือบริการของ Lenovo ไม่มีเจตนาในการกล่าว หรือแสดงนัยที่ว่าอาจใช้ผลิตภัณฑ์, โปรแกรม หรือบริการของ Lenovo เท่านั้น โดยอาจใช้ผลิตภัณฑ์, โปรแกรม หรือบริการที่ทำงานได้เทียบเท่าที่ไม่เป็นการละเมิดสิทธิเกี่ยวกับทรัพย์สินทางปัญญาของ Lenovo แทน อย่างไรก็ตาม ผู้ใช้มีหน้าที่ในการประเมิน และตรวจสอบความถูกต้องในการทำงานของผลิตภัณฑ์, โปรแกรม หรือบริการอื่น

Lenovo อาจมีสิทธิบัตร หรือแอปพลิเคชันที่กำลังจะขึ้นสิทธิบัตรที่ครอบคลุมเรื่องที่กล่าวถึงในเอกสารนี้ การมอบเอกสารฉบับนี้ให้ไม่ถือเป็นการเสนอและให้สิทธิการใช้ภายใต้สิทธิบัตรหรือแอปพลิเคชันที่มีสิทธิบัตรใดๆ คุณสามารถส่งคำถามเป็นลายลักษณ์อักษรไปยังส่วนต่างๆ ต่อไปนี้:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO จัดเอกสารฉบับนี้ให้ “ตามที่แสดง” โดยไม่ได้ให้การรับประกันอย่างใดทั้งโดยชัดเจน หรือโดยนัย รวมถึงแต่ไม่จำกัดเพียงการรับประกันโดยนัยเกี่ยวกับการไม่ละเมิด, การขายสินค้า หรือความเหมาะสมสำหรับวัตถุประสงค์เฉพาะทาง บางขอบเขตอำนาจไม่อนุญาตให้ปฏิเสธการรับประกันโดยชัดเจน หรือโดยนัยในบางกรณี ดังนั้นข้อความนี้อาจไม่บังคับใช้ในกรณีของคุณ

ข้อมูลนี้อาจมีส่วนที่ไม่ถูกต้อง หรือข้อความที่ตีพิมพ์ผิดพลาดได้ จึงมีการเปลี่ยนแปลงข้อมูลในที่นี้เป็นระยะ โดยการเปลี่ยนแปลงเหล่านี้รวมไว้ในเอกสารฉบับตีพิมพ์ครั้งใหม่ Lenovo อาจดำเนินการปรับปรุง และ/หรือเปลี่ยนแปลงผลิตภัณฑ์ และ/หรือโปรแกรมที่อธิบายไว้ในเอกสารฉบับนี้เมื่อใดก็ได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

ผลิตภัณฑ์ที่กล่าวถึงในเอกสารนี้ไม่ได้มีเจตนาเอาไว้ใช้ในแอปพลิเคชันที่เกี่ยวข้องกับการฝังตัวหรือการช่วยชีวิตรูปแบบอื่น ซึ่งหากทำงานบกพร่องอาจก่อให้เกิดการบาดเจ็บ หรือเสียชีวิตของบุคคลได้ ข้อมูลที่ปรากฏในเอกสารนี้ไม่มีผลกระทบหรือเปลี่ยนรายละเอียด หรือการรับประกันผลิตภัณฑ์ Lenovo ไม่มีส่วนใดในเอกสารฉบับนี้ที่จะสามารถใช้งานได้เสมือนสิทธิโดยชัดเจน หรือโดยนัย หรือชดใช้ค่าเสียหายภายใต้สิทธิทรัพย์สินทางปัญญาของ Lenovo หรือบุคคลที่สาม ข้อมูลทั้งหมดที่ปรากฏอยู่ในเอกสารฉบับนี้ได้รับมาจากสภาพแวดล้อมเฉพาะและนำเสนอเป็นภาพประกอบ ผลที่ได้รับในสภาพแวดล้อมการใช้งานอื่นอาจแตกต่างออกไป

Lenovo อาจใช้ หรือเผยแพร่ข้อมูลที่คุณได้ให้ไว้ในทางที่เชื่อว่าเหมาะสมโดยไม่ก่อให้เกิดภาระความรับผิดต่อคุณ

ข้อมูลอ้างอิงใดๆ ในเอกสารฉบับนี้เกี่ยวกับเว็บไซต์ที่ไม่ใช่ของ Lenovo จัดให้เพื่อความสะดวกเท่านั้น และไม่ถือเป็นการรับรองเว็บไซต์เหล่านั้นในกรณีใดๆ ทั้งสิ้น เอกสารในเว็บไซต์เหล่านั้นไม่ถือเป็นส่วนหนึ่งของเอกสารสำหรับผลิตภัณฑ์ Lenovo นี้ และการใช้เว็บไซต์เหล่านั้นถือเป็นความเสี่ยงของคุณเอง

ข้อมูลเกี่ยวกับการทำงานที่ปรากฏอยู่ในที่นี้ถูกกำหนดไว้ในสถานการณ์ที่ได้รับการควบคุม ดังนั้น ผลที่ได้รับจากสภาพแวดล้อมในการใช้งานอื่นอาจแตกต่างกันอย่างมาก อาจมีการใช้มาตรการบางประการกับระบบระดับขั้นการพัฒนา และไม่มีการรับประกันว่ามาตรการเหล่านี้จะเป็นมาตรการเดียวกันกับที่ใช้ในระบบที่มีอยู่ทั่วไป นอกจากนั้น มาตรการบางประการอาจเป็นการคาดการณ์ตามข้อมูล ผลลัพธ์ที่เกิดขึ้นจริงจึงอาจแตกต่างไป ผู้ใช้เอกสารฉบับนี้ควรตรวจสอบความถูกต้องของข้อมูลในสภาพแวดล้อมเฉพาะของตน

เครื่องหมายการค้า

Lenovo, โลโก้ของ Lenovo, ThinkSystem, Flex System, System x, NeXtScale System และ x Architecture เป็นเครื่องหมายการค้าของ Lenovo ในสหรัฐอเมริกา ประเทศอื่น หรือทั้งสองกรณี

Intel และ Intel Xeon เป็นเครื่องหมายการค้าของ Intel Corporation ในสหรัฐอเมริกา ประเทศอื่น หรือทั้งสองกรณี

Internet Explorer, Microsoft และ Windows เป็นเครื่องหมายการค้าของกลุ่มบริษัท Microsoft

Linux เป็นเครื่องหมายค้าจดทะเบียนของ Linus Torvalds

ชื่อบริษัท ชื่อผลิตภัณฑ์ หรือชื่อบริการอื่นๆ อาจเป็นเครื่องหมายการค้าหรือเครื่องหมายบริการของผู้นั้น

คำประกาศที่สำคัญ

ความเร็วของโปรเซสเซอร์จะระบุความเร็วนาฬิกาภายในไมโครโปรเซสเซอร์ นอกจากนี้ปัจจัยอื่นๆ ยังส่งผลต่อการทำงานของแอปพลิเคชัน

ความเร็วของไดรฟ์ซีดีหรือดีวีดีจะมีอัตราการอ่านที่ไม่แน่นอน แต่ความเร็วที่แท้จริงจะแตกต่างกันไปและมักมีอัตราน้อยกว่าความเร็วสูงสุดที่เป็นไปได้

ในส่วนของความจุของโปรเซสเซอร์ สำหรับความจุจริงและความจุเสมือน หรือปริมาณความจุของช่องหน่วยความจำ KB มีค่าเท่ากับ 1,024 ไบต์, MB มีค่าเท่ากับ 1,048,576 ไบต์ และ GB มีค่าเท่ากับ 1,073,741,824 ไบต์

ในส่วนของความจุไดรฟ์ฮาร์ดดิสก์หรือปริมาณการสื่อสาร MB มีค่าเท่ากับ 1,000,000 ไบต์ และ GB มีค่าเท่ากับ 1,000,000,000 ไบต์ ความจุโดยรวมที่ผู้ใช้สามารถเข้าใช้งานได้จะแตกต่างกันไป ขึ้นอยู่กับสภาพแวดล้อมในการใช้งาน

ความจุไดรฟ์ฮาร์ดดิสก์ภายในสูงสุดสามารถรับการเปลี่ยนชิ้นส่วนไดรฟ์ฮาร์ดดิสก์แบบมาตรฐาน และจำนวนช่องใส่ไดรฟ์ฮาร์ดดิกส์ทั้งหมดพร้อมไดรฟ์ที่รองรับซึ่งมี ขนาดใหญ่ที่สุดในปัจจุบันและมีให้ใช้งานจาก Lenovo

หน่วยความจำสูงสุดอาจต้องใช้การเปลี่ยนหน่วยความจำมาตรฐานพร้อมโมดูลหน่วยความจำเสริม

เซลหน่วยความจำโซลิดสเตทแต่ละตัวจะมีจำนวนรอบการเขียนข้อมูลในตัวที่จำกัดที่เซลสามารถสร้างขึ้นได้ ดังนั้น อุปกรณ์โซลิดสเตทจึงมีจำนวนรอบการเขียนข้อมูลสูงสุดที่สามารถเขียนได้ ซึ่งแสดงเป็น **total bytes written** (TBW) อุปกรณ์ที่เกินขีดจำกัดนี้ไปแล้วอาจไม่สามารถตอบสนองต่อคำสั่งที่ระบบสร้างขึ้นหรืออาจไม่สามารถเขียนได้ Lenovo จะไม่รับผิดชอบต่อการเปลี่ยนชิ้นส่วนอุปกรณ์ที่มีจำนวนรอบโปรแกรม/การลบที่รับประกันสูงสุดเกินกว่าที่กำหนดไว้ ตามที่บันทึกในเอกสารข้อกำหนดเฉพาะที่พิมพ์เผยแพร่อย่างเป็นทางการสำหรับอุปกรณ์

Lenovo ไม่ได้ให้การเป็นตัวแทนหรือการรับประกันที่เกี่ยวกับผลิตภัณฑ์ที่ไม่ใช่ของ Lenovo การสนับสนุน (หากมี) สำหรับผลิตภัณฑ์ที่ไม่ใช่ของ Lenovo มีให้บริการโดยบุคคลที่สาม แต่ไม่ใช่ Lenovo

ซอฟต์แวร์บางอย่างอาจมีความแตกต่างกันไปตามรุ่นที่ขายอยู่ (หากมี) และอาจไม่รวมถึงคู่มือผู้ใช้หรือฟังก์ชันการทำงานของโปรแกรมทั้งหมด

การปนเปื้อนของอนุภาค

ข้อคำนึง: อนุภาคที่ลอยในอากาศ (รวมถึงเกล็ดหรืออนุภาคโลหะ) และกลุ่มก๊าซที่มีความไวในการทำปฏิกิริยาเพียงอย่างเดียวหรือร่วมกันกับปัจจัยด้านสิ่งแวดล้อมอื่นๆ เช่น ความชื้นหรืออุณหภูมิ อาจเป็นต้นเหตุที่ทำให้อุปกรณ์เกิดความเสี่ยงดังที่อธิบายไว้ในเอกสารฉบับนี้

ความเสี่ยงที่เกิดจากการมีระดับอนุภาคสูงจนเกินไปหรือมีปริมาณความเข้มข้นของก๊าซที่เป็นอันตราย สร้างความเสียหายที่อาจทำให้อุปกรณ์ทำงานผิดปกติหรือหยุดทำงาน ข้อกำหนดนี้จึงระบุถึงข้อจำกัดสำหรับอนุภาคและก๊าซ ซึ่งมีไว้เพื่อหลีกเลี่ยงจากความเสียหายดังกล่าว อย่างไรก็ดี ข้อจำกัดนี้จะต้องไม่นำไปพิจารณาหรือใช้เป็นข้อกำหนดขั้นสุดท้าย เนื่องจากยังมีปัจจัยอื่นๆ มากมาย เช่น อุณหภูมิหรือปริมาณความชื้นของอากาศ ที่อาจส่งผลกระทบต่อการแพร่ของอนุภาคหรือสารกัดกร่อนทางสิ่งแวดล้อมและสิ่งปนเปื้อนที่เป็นก๊าซ หากข้อกำหนดที่เฉพาะเจาะจงนี้ไม่มีระบุไว้ในเอกสารฉบับนี้ คุณจำเป็นต้องนำแนวปฏิบัติมาใช้เพื่อรักษาระดับอนุภาคและก๊าซให้สอดคล้องกับข้อกำหนดในการป้องกันสุขภาพและความปลอดภัยของมนุษย์ หาก Lenovo พิจารณาว่าระดับของอนุภาคหรือก๊าซในสภาพแวดล้อมระบบของคุณทำให้อุปกรณ์เกิดความเสียหาย Lenovo อาจกำหนดเงื่อนไขการซ่อมแซมหรือเปลี่ยนอุปกรณ์หรือชิ้นส่วนเพื่อดำเนินมาตรการแก้ไขที่เหมาะสมในการบรรเทาการปนเปื้อนทางสิ่งแวดล้อมดังกล่าว โดยการดำเนินมาตรการแก้ไขที่เหมาะสมดังกล่าวนั้นเป็นความรับผิดชอบของลูกค้า

ตาราง 70. ข้อกำหนดสำหรับอนุภาคและก๊าซ

สิ่งปนเปื้อน	ข้อกำหนด
อนุภาค	• อากาศภายในห้องจะต้องได้รับการกรองอย่างต่อเนื่องตามข้อกำหนด 40% Atmospheric dust spot efficiency (MERV 9) ตามมาตรฐาน ASHRAE 52.2[1] • อากาศที่ลอยเข้าสู่ศูนย์ข้อมูลต้องได้รับการกรอง 99.97% หรือมากกว่า โดยใช้แผ่นกรองอากาศแบบ High-efficiency particulate air (HEPA) ที่สอดคล้องตามมาตรฐาน MIL-STD-282 • ความชื้นสัมพัทธ์ที่ทำให้อนุภาคที่ปนเปื้อนอยู่ในอากาศละลายต้องมีค่ามากกว่า 60%[2] • ห้องจะต้องปราศจากการปนเปื้อนจากสารนำไฟฟ้า เช่น เส้นสังกะสี
ก๊าซ	• ทองแดง: ประเภท G1 ตาม ANSI/ISA 71.04-1985[3] • เงิน: อัตราการกัดกร่อนต่ำกว่า 300 Å ใน 30 วัน

[1] ASHRAE 52.2-2008 - *วิธีการทดสอบอุปกรณ์ทำความสะอาดการระบายอากาศทั่วไปเพื่อตรวจสอบประสิทธิภาพการกรองตามขนาดอนุภาค* Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] ความชื้นสัมพัทธ์ที่ทำให้อนุภาคที่ปนเปื้อนอยู่ในอากาศละลาย คือ ความชื้นสัมพัทธ์ในระดับที่ฝุ่นดูดซับน้ำมากเพียงพอที่จะเกิดการเปียกชื้นและทำให้เกิดการนำไฟฟ้าโดยไอออน

[3] ANSI/ISA-71.04-1985 *สภาพแวดล้อมในการวัดกระบวนการและระบบการควบคุม: สารปนเปื้อนทางอากาศ* Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

คำประกาศกฎข้อบังคับด้านโทรคมนาคม

ในประเทศของคุณ ผลิตภัณฑ์นี้อาจไม่ได้รับการรับรองให้เชื่อมต่อเข้ากับอินเทอร์เฟสของเครือข่ายโทรคมนาคมสาธารณะไม่ว่าด้วยวิธีใดก็ตาม คุณอาจจำเป็นต้องมีใบรับรองเพิ่มเติมตามที่กฎหมายกำหนดก่อนจะทำการเชื่อมต่อดังกล่าว หากมีข้อสงสัยใดๆ โปรดติดต่อตัวแทนจำหน่ายหรือเจ้าหน้าที่ของ Lenovo

ประกาศเกี่ยวกับการแผ่คลื่นอิเล็กทรอนิกส์

เมื่อคุณเชื่อมต่อจอภาพกับอุปกรณ์ คุณต้องใช้สายของจอภาพที่กำหนดและอุปกรณ์ตัดสัญญาณรบกวนๆ ใดที่ให้มาพร้อมกับจอภาพ

สามารถดูคำประกาศเกี่ยวกับการแผ่คลื่นอิเล็กทรอนิกส์เพิ่มเติมได้ที่:

http://thinksystem.lenovofiles.com/help/index.jsp

การประกาศเกี่ยวกับ BSMI RoHS ของไต้หวัน

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

ข้อมูลติดต่อเกี่ยวกับการนำเข้าและส่งออกสำหรับไต้หวัน

ผู้ติดต่อพร้อมให้ข้อมูลเกี่ยวกับการนำเข้าและส่งออกสำหรับไต้หวัน

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

ดรรชนี

จ

ช

น

บ

ป

ผ

พ

Lenovo

หมายเลขชิ้นส่วน: SP47A30085

Printed in China

(1P) P/N: SP47A30085