VMware vCenter 対応 Lenovo XClarity Integrator

インストールおよびユーザー・ガイド

バージョン 8.6.0

注

本書および本書で紹介する製品をご使用になる前に、77 ページの 付録 D「特記事項」 に記載されている情報をお読みください。

第 30 版 (2024 年 12 月)

目次

図

表

本書について

本書では、VMware vCenter 対応 Lenovo XClarity Integrator, *バージョン 8.6.0* をインストールして使用する方法について説明します。

この手順では、機能を使用したシステム情報の取得、ファームウェアの更新、電源使用量の監視、システム設定の構成、VMware vCenter 管理環境の仮想マシン用の移行ルールの作成に関する情報を説明します。

規則および用語

太字の「**注**」、「**重要**」、または「**注意**」で始まっているパラグラフは、重要な情報を強調する特定の意味を持つ注意書きです。

注：これらの特記事項は重要なヒント、ガイダンス、またはアドバイスを提供します。

重要：これらの特記事項は、不都合なまたは困難な状態を避けるために役立つ情報またはアドバイスを提供します。

注意：これらの特記事項は、プログラム、デバイス、またはデータへの考えられる損傷を示します。損傷が起こりうる指示または状態の前には警告通知が表示されます。

本書で使用されている用語、頭字語、および省略語のいくつかについて、下の表で説明します。

表 1. 頻繁に使用される用語と頭字語

用語/頭字語	定義
BMC	ベースボード管理コントローラー
LXCA	Lenovo XClarity Administrator
LXCI	Lenovo XClarity Integrator
PFA	障害予知アラート
UXSP	UpdateXpress System Packs

Web リソース

以下の Web サイトでは、System x、Flex System、BladeCenter サーバー、およびシステム管理ツールの理解、使用、およびトラブルシューティングに役立つリソースが提供されています。

VMware vCenter 対応 Lenovo XClarity Integrator サイト

VMware vCenter 対応 Lenovo XClarity Integrator 用の最新のダウンロードがあります。

- VMware 対応 Lenovo XClarity Integrator Web サイト

Lenovo XClarity ソリューションを使用したシステム管理

この Web サイトでは、Lenovo XClarity ソリューションの概要について説明します。このソリューションは、System x および Flex System ハードウェアに統合され、システム管理機能を提供します。

- Lenovo XClarity Solution を使用したシステム管理についての Web サイト

Lenovo テクニカル・サポート・ポータル

この Web サイトは、ハードウェアおよびソフトウェアのサポートを見つける役に立ちます。

- Lenovo サポート・ポータル Web サイト

ServerProven Web サイト

次の Web サイトは、BladeCenter、Flex System、System x、および xSeries ® ハードウェアのハードウェア互換性の概要を示します。

- Lenovo ServerProven: BladeCenter 製品の互換性
- Lenovo ServerProven: Flex System シャーシの互換性
- Lenovo ServerProven: System x ハードウェア、アプリケーション、およびミドルウェアの互換性

VMware Web サイト

この Web サイトは、VMware 製品の検索に役立ちます。

- VMware Web サイト

第 1 章　VMware vCenter 対応 Lenovo XClarity Integrator

VMware vCenter 対応 Lenovo XClarity Integrator は VMware vCenter 対応 LXCI の拡張機能です。システム管理者に System x サーバー、BladeCenter サーバー、および Flex System サーバー用の拡張管理機能を提供します。VMware vCenter 対応 Lenovo XClarity Integrator は Lenovo ハードウェア管理機能を統合することで VMware vCenter の管理機能を拡張し、以下の機能を提供します。

VMware vCenter 対応 Lenovo XClarity Integrator は、以下の機能を提供します。

ダッシュボード

ダッシュボードには、以下の情報が表示されます。

- システム情報の要約、システム正常性メッセージなど、選択されたホストおよびクラスター・ステータスの概要。
- 全体リソース使用状況、ホスト正常性メッセージ、接続情報などの要約情報。
- 各ホストの BMC 情報およびユーザーが直接 BMC コンソールを許可できます。

ファームウェア更新

ファームウェア更新機能は、Lenovo UpdateXpress System Packs (UXSPs) と個別の更新を取得して、ご利用の ESXi システムに適用します。ローリング・システム更新 機能は、ダウン時間ゼロで中断を伴わないシステム更新を可能にし、クラスター環境でのホスト更新プロセスをワークロードの中断を伴わずに自動化します。また、複数のホストの同時更新をサポートして時間を節約します。

電力メトリック

電力メトリックは、電力使用量、熱使用の履歴、およびファン速度を監視して、その要約を提供します。また、管理対象ホストの傾向グラフも示します。電源キャッピング対応ホストの電源キャッピングを設定して、サーバーの電力使用量を制限することもできます。

Advanced Settings Utility

ASU は、BMC、Unified Extensible Firmware Interface (UEFI)、ブート順序の設定など、ホストの現在のシステム設定を管理します。

障害予知管理

障害予知管理は、サーバー・ハードウェア・ステータスを監視して、障害予知アラートを受け取ります。障害予知アラートに基づいてサーバーの管理ポリシーを設定し、障害予知アラートに応答して仮想マシンを自動的に退避させ、ユーザーのワークロードを保護するか、ユーザーに通知を送信します。障害予知管理は、ホスト上で手動で有効または無効にします。

ローリング・システム更新機能

ローリング・システム更新 (RSU) 機能は、システムを実行し続けながら、ファームウェアを 1 つのバッチで更新します。その際、サーバー・ホストでアプリケーション・サービスの中断は発生しません。RSU 機能は、無停止ファームウェア更新のアプローチを提供します。VMware クラスター内でワークロード中断なしの動的仮想マシン移動と自動ホスト再起動を利用することでファームウェアの完全な管理を可能にします。

ローリング・システム・リブート

ローリング・システム・リブート (RSR) 機能は、定義された VMware クラスター内でワークロード中断なしの動的仮想マシン移動と自動ホスト再起動を利用することで自動ローリング再起動メカニズムを提供します。

ThinkAgile VX アプライアンス・サーバーのハードウェア・トポロジー・ビュー

ハードウェア・トポロジー機能は、ThinkAgile VX アプライアンス・サーバーに組み込みグラフィカル・ビューを提供します。このページには、サーバーのレイアウト、詳細なハードウェア・インベントリー、および正常性情報が表示され、vSAN ディスクを管理するためのウィザードが提供されます。

Lenovo XClarity Administrator 統合

Lenovo XClarity Integrator は Lenovo XClarity Administrator と統合されており、Lenovo サーバーの検出の自動化、管理対象サーバーのインベントリー・マップ・ビューの視覚化、構成パターンを使用したサーバーの構成、ローリング・ファームウェア・ポリシー展開の調整を行う便利な方法を提供します。

vSphere Lifecycle Manager (vLCM) の統合

vSphere 7.0 で導入された vSphere Lifecycle Manager (vLCM) と統合された Lenovo XClarity Integrator は、定義されたクラスター全体のイメージを使用して、ファームウェア更新を管理する便利な方法を提供します。

第 2 章　VMware vCenter 向け LXCI の計画およびインストール

VMware vCenter 対応 Lenovo XClarity Integrator を計画してインストールするには、この手順を使用します。

システム要件

このセクションでは、VMware vCenter 対応 Lenovo XClarity Integrator のシステム要件について説明します。

VMware vCenter Server のサポートされるバージョン

VMware vCenter 対応 Lenovo XClarity Integrator は、VMware vCenter Server の拡張機能です。

バージョン 6.0.0 以降の Lenovo XClarity Integrator では、VMware vCenter 6.5 (U2) 以上のバージョンのみサポートされ、vSphere HTML クライアントを通じてのみアクセスできます。vSphere Flex クライアントはサポートされなくなりました。

VMware vCenter のバージョンとクラスターが使用されている vSphere Client に応じて、以下のマトリックスに従って適切な Lenovo XClarity Integrator バージョンを選択します。

表 2. VMware vCenter のバージョン・サポート・マトリックス

VMware vCenter バージョン	Lenovo XClarity Integrator バージョン		
	5.5.0 (Flex クライアントのみサポート)	7.7.0 (HTML クライアントのみサポート)	8.6.0
8.0 (U1、U2、U3)	X	X	√
8.0 GA	X	X	√
7.0 (U3)	X	√	√
7.0 (U1、U2)	X	√	X
7.0 GA	X	√	X
6.7 (U1、U2、U3)	√	√	X
6.5 (U2、U3)	√	√	X
6.5 (U1)	√	X	X
6.5	√	X	X
バージョン 6.0 以前	√	X	X

注：
- ターゲット VMware vCenter のバージョンが、6.5 (U2) 以前のバージョンであるか、ユーザーが vSphere Flex クライアントがある LXCI を使用する場合、LXCI を 6.0.0 にアップグレードしないでください。
- ターゲット VMware vCenter のバージョンが 7.0 (U1) 以降の場合、LXCI を 8.0.0 にアップグレードしないでください。

Lenovo XClarity Administrator のサポート・バージョン

表 3. Lenovo XClarity Administrator バージョン・サポート・マトリックス

LXCA	LXCI のバージョン										
	7.4.0	7.5.0	7.6.0	7.7.0	8.0.0	8.1.0	8.2.0	8.3.0	8.4.0	8.5.0	8.6.0
4.2	X	X	X	X	X	X	X	X	X	X	√
4.1	X	X	X	X	X	X	X	X	X	√	X
4.0	X	X	X	X	X	√	√	√	√	√	X
3.6	X	X	√	√	√	√	√	√	√	X	X
3.5	X	√	√	√	√	√	√	√	√	X	X

サポートされる ESXi バージョン

VMware vCenter 対応 Lenovo XClarity Integrator は、Lenovoカスタマイズされた VMware vSphere Hypervisor (ESXi) カスタム・イメージおよび VMware ESXi 標準イメージの両方をサポートします。以下のバージョンがサポートされています。

- 8.0
- 7.0
- 6.7
- 6.5
- 6.0

Lenovo カスタマイズされた ESXi イメージは、VMWare 製品からダウンロードできます。ダウンロード Web サイト: https://my.vmware.com/web/vmware/downloads。VMware vSphere を見つけて、「**Download Product** (製品のダウンロード)」リンクをクリックします。次に「**Custom ISOs** (カスタム ISO)」タブをクリックして、ESXi の Lenovo カスタム・イメージを見つけます。

サポートされるサーバー・モデル

このトピックでは、VMware vCenter 対応 Lenovo XClarity Integrator でサポートされるサーバー・モデルに関する情報を記載しています。

XClarity Integrator プラグインにはサーバー・モデルの制限はありません。ただし、プラグインが管理するハードウェアは、以下の表にある Lenovo サーバー・モデルに限定されます。

表 4. サポートされている Lenovo サーバー

シリーズ	サーバー・モデル	
ThinkSystem	• SD530 (7X20、7X21、7X22) • SD530 V3 (7DD3、7DDA) • SD535 V3 (7DD1、7DD8) • SD550 V3 (7DD2、7DD9) • SD630 V2 (7D1K) • SE350 (7Z46、7D1X、7D27) • SN550 (7X16) • SN550 V2 (7Z69) • SN850 (7X15) • SR150 (7Y54) (中国のみ) • SR158 (7Y55) • SR250 (7Y51、7Y52) (インドを除く全世界) • SR250 (7Y72、7Y73) (インドのみ) • SR250 V2 (7D7Q、7D7R、7D7S) • SR258 (7Y53) • SR530 (7X07、7X08)	• SR650 (7X05、7X06) • SR650 V2 (7Z72、7Z73) • SR650 V3 (7D75、7D76、7D77) • SR655 (7Y00、7Z01) • SR655 V3 (7D9E、7D9F) • SR665 (7D2V、7D2W) • SR665 V3 (7D9A、7D9B) • SR670 (7Y36、7Y37、7Y38) • SR670 V2 (7Z22、7Z23) • SR675 V3 (7D9Q、7D9R) • SR850 (7X18、7X19) • SR850 V2 (7D31、7D32、7D33) • SR850 V3 (7D96、7D97、7D98) • SR850P (7D2F、7D2G、7D2H) • SR860 (7X69、7X70) • SR860 V2 (7Z59、7Z60、7D42)

表 4. サポートされている Lenovo サーバー (続き)

シリーズ	サーバー・モデル	
	• SR550 (7X03、7X04) • SR570 (7Y02、7X03) • SR590 (7X98、7X99) • SR250 V3 (7DCM、7DCL) • SR630 (7X01、7X02) • SR630 V2 (7Z70、7Z71) • SR630 V3 (7D72、7D73、7D74) • SR635 (7Y98、7Y99) • SR635 V3 (7D9G、7D9H) • SR645 (7D2X, 7D2Y) • SR645 V3 (7D9C、7D9D)	• SR860 V3 (7D93、7D94、7D95) • SR950 (7X11、7X12、7X13) • SR950 V3 (7DC4、7DC5、7DC6) • ST250 (7Y45、7Y46) • ST250 V2 (7D8F、7D8G) • ST250 V3 (7DCF、7DCE) • ST258 (7Y47) • ST258 V2 (7D8H) • ST550 (7X09、7X10) • ST558 (7Y15、7Y16) (中国のみ) • ST650 V2 (7Z74、7Z75) • ST650 V3 (7D7A、7D7B) • ST658 V2 (7Z76)
ThinkServer	• SR588 V2 (7D53) • SR590 V2 (7D53)	• SR660 V2 (7D6L) • SR668 V2 (7D6L)
ThinkEdge	• SE350 V2 (7DA9) • SE360 V2 (7DAM)	• SE450 (7D8T) • SE455 V3 (7DBY)
解決策	• ThinkAgile HX シリーズ・アプライアンス (7D20、7D2T、7D1Z、7X82、7X83、7X84、7Y95、7Z08、7Z29、7Z44、8689、8693、8695、5462) • ThinkAgile HX シリーズ認定ノード (7D20、7D29、7Y88、7Y89、7Y90、7Y96、7Z03、7Z04、7Z05、7Z09、7Z45) • ThinkAgile VX 統合システム (7D43、7D6X、7D6W、7D82、7D9K、7D9L、7D9V、7D9W)	• ThinkAgile VX シリーズ・アプライアンス (7Y11、7Y12、7Y13、7Y14、7Y91、7Y92、7Y93、7Y94、7Z13、7Z58、7Z62、7Z63) • ThinkAgile VX シリーズ認定ノード (7D6W、7D6X、7D9L、7D9K、7D9V、7D9W、7Y92、7Y93、7Y94、7Z12、7Z58、7Z63、7DDK)
System x	• nx360 M5 (5465) • nx360 M5 DWC (5467、5468、5469) • x240 計算ノード (7162、2588) • x240 M5 計算ノード (2591、9532) • x280、x480、x880 X6 計算ノード (7196、4258) • x440 計算ノード (7167、2590) • x3250 M6 (3633)	• x3500 M5 (5464) • x3550 M4 (7914) • x3550 M5 (5463) • x3630 M4 (7158) • x3650 M4 (7915) • x3650 M5 (5462、8871) • x3750 M4 (8753) • x3850 X6/x3950 X6 (6241)
レガシー ThinkServer	• RD350 • RD450 • RD550 • RD650	• RS160 • SD350 (5493) • TD350 • TS460

注：

- vSphere Lifecycle Manager では以下のサーバーのみサポートされています。
  - Lenovo ThinkAgile VX シリーズ・アプライアンス
  - Lenovo ThinkAgile VX シリーズ認定ノード
  - Lenovo ThinkAgile VX 統合システム
  - Lenovo ThinkSystem SD630 V2、SE350、SE350 V2、SE450、SR630、SR630 V2、SR630 V3、SR645、SR645 V3、SR650、SR650 V2、SR650 V3、SR665、SR665 V3、SR850P、SR850 V2、SR850 V3、および SR950、SR950 V3。
- ハードウェア・トポロジーでは、次のサーバーのみサポートされています。
  - ThinkAgile VX アプライアンス:
    - 7Y93: ThinkAgile VX2320/VX3320/VX7320N アプライアンス
    - 7Y94: ThinkAgile VX5520/VX7520/VX3520G アプライアンス
    - 7Z62: ThinkAgile VX2330/VX3330/VX7330-N アプライアンス
    - 7Z63: ThinkAgile VX3530-G/VX5530/VX7530 アプライアンス
  - ThinkAgile VX 認定ノード:

表 4. サポートされている Lenovo サーバー (続き)

シリーズ	サーバー・モデル
	– 7DDK: ThinkAgile VX850 V3/VX850 V3-DPU CN – 7D43: ThinkAgile VX7576 ノード – 7D6X: ThinkAgile VX630 V3 CN – 7D6W: ThinkAgile VX650 V3/VX650 V3-DPU CN – 7D82: ThinkAgile VX3376 ノード – 7D9L: ThinkAgile VX665 V3 CN – 7D9K: ThinkAgile VX645 V3 CN – 7D9V: ThinkAgile VX635 V3 CN – 7D9W: ThinkAgile VX655 V3 CN – 7Z62: ThinkAgile VX3331 ノード – 7Z63: ThinkAgile VX7531 認定ノード – 7Y94: ThinkAgile VX 2U 認定ノード/VX 2U 認定ノード (SAP HANA 用) – ThinkAgile VX 統合システム: – 7D43: ThinkAgile VX3575-G/VX5575/VX7575 IS – 7D6X: ThinkAgile VX630 V3 IS – 7D6W: ThinkAgile VX650 V3/VX650 V3-DPU IS – 7D82: ThinkAgile VX2375/VX3375/VX7375-N IS – 7D9K: ThinkAgile VX645 V3 IS – 7D9L: ThinkAgile VX665 V3 IS – 7D9V: ThinkAgile VX635 V3 IS – 7D9W:ThinkAgile VX655 V3 IS • ThinkServer サーバーは、インベントリー、監視、およびローリング再起動のみをサポートし、一部のインベントリー情報は「NA」として表示されます。 • ThinkServer SR588 V2/SR590 V2 (7D53) の場合、BMC のバージョンは 5.30 以降である必要があります。 • ThinkServer SR660 V2/SR668 V2 (7D6L) の場合、BMC のバージョンは 5.33 以降である必要があります。

表 5. サポートされている IBM サーバー

シリーズ	サーバー・モデル	
System x	• dx360 M2 (7321、7323) • dx360 M3 (6391) • dx360 M4 (7912、7913、7918、7919) • HS22 (7870、7809、1911、1936) • HS22V (7871、1949) • HS23 (7875、1882、1929) • HS23E (8038、8039) • HX5 (7872、7873、1909、1910) • nx360 M4 (5455) • Smart Analytics System (7949) • x220 計算ノード (7906、2585) • x222 計算ノード (7916) • x240 計算ノード (8956、8737、8738、7863) • x280 X6 計算ノード / x480 X6 計算ノード / x880 計算ノード X6 (4259、7903) • x440 計算ノード (7917) • x3100 M4 (2582、2586) • x3100 M5 (5457) • x3200 M2 (4367、4368) • x3200 M3 (7327、7328) • x3250 M2 (7657、4190、4191、4194) • x3250 M3 (4251、4252、4261) • x3250 M4 (2583)	• x3250 M5 (5458) • x3300 M4 (7382) • x3400 M2 (7836、7837) • x3400 M3 (7378、7379) • x3500 M2 (7839) • x3500 M3 (7380) • x3500 M4 (7383) • x3530 M4 (7160) • x3550 M2 (7946、4198) • x3550 M3 (7944、4254) • x3550 M4 (7914) • x3620 M3 (7376) • x3630 M3 (7377) • x3630 M4 (7158、7518、7519) • x3650 M2 (7947、4199) • x3650 M3 (7944、7945、4254、4255、5454) • x3650 M4 (7915) • x3650 M4 HD (5460) • x3650 M4 BD (5466) • x3750 M4 (8722、8733) • x3755 M4 (7164) • x3690 X5 (7148、7149、7147、7192) • x3850 X5/X3950 X5 (7145、7146、7143、7191) • x3850 X6 / x3950 X6 (3837、3839)
注：		

表 5. サポートされている IBM サーバー (続き)

シリーズ	サーバー・モデル
• IBM サーバーでは、ファームウェア更新はサポートされていません。 • Lenovo でカスタマイズした ESXi 6.5 以降は、IBM サーバーではサポートされません。 • System x3250 M4 (2583) は、ダッシュボードと Lenovo Dynamic System Analysis の一部の機能のみをサポートします。更新、電源、およびシステム構成機能はサポートされません。	

ハードウェア要件

このセクションでは、VMware vCenter 対応 Lenovo XClarity Integrator のハードウェア要件について説明します。デフォルトでは、VMware vCenter 対応 Lenovo XClarity Integrator 仮想アプライアンスは、以下のハードウェア構成に事前構成されています。

- メモリー: 16 GB RAM
- ディスク・スペース: 128 GB のハードディスク・ドライブの空きスペース
- プロセッサー: 4 つのプロセッサー

ネットワーク要件

このセクションでは、ポート、ファイアウォール、プロキシー要件を含むネットワーク要件を説明します。

利用可能なポート

環境でファイアウォールがどのように実装されているかに応じて、いくつかのポートを利用できる必要があります。必要なポートがブロックされているか、別のプロセスによって使用されている場合は、一部の Lenovo XClarity Integrator の機能が動作しないことがあります。

環境に基づいて、どのポートを開く必要があるかを確認するには、次のセクションを参照してください。これらのセクションのテーブルには、各ポートが XClarity Integrator でどのように使用されているか、vCenter、影響のある管理対象デバイス、プロトコル (TCP または UDP) およびトラフィック・フローの方向に関する情報が含まれます。

*インバウンド・トラフィック*は、管理対象デバイスまたは外部システムから XClarity Integrator へのフローを特定するので、ポートは、 XClarity Integrator アプライアンスで開く必要があります。*アウトバウンド・トラフィック*は、XClarity Integrator から管理対象デバイスまたは外部システムに流れます。

- 7 ページの 「XClarity Integrator サーバーへのアクセス」
- 8 ページの 「XClarity Integrator と管理対象デバイス間のアクセス」

XClarity Integrator サーバーへのアクセス

XClarity Integrator サーバーとすべての管理対象デバイスがファイアウォールで保護されていて、ユーザーが、ファイアウォールの外側にあるブラウザーからこれらのデバイスにアクセスしようとする場合、XClarity Integrator ポートが開いていることを確認する必要があります。

XClarity Integrator サーバーは、次のテーブルで一覧されているポートを介してリッスンし、応答します。

注：XClarity Integrator は、ポート 443 上の TCP を介して安全に通信する RESTful アプリケーションです。

表 6. インターネット接続要件

通信	XClarity Integrator アプライアンス	vCenter	XClarity Administrator [1]	Lenovo Services [2]
アウトバウンド (外部システムで開くポート)	DNS – ポート 53 の TCP/UDP	HTTPS – ポート 443 の TCP	HTTPS – ポート 443 の TCP	HTTPS – ポート 443 の TCP
インバウンド (XClarity Integrator アプライアンスで開いたポート)	HTTPS – ポート 443 の TCP	HTTPS – ポート 443 の TCP	該当なし	該当なし

1. XClarity Administrator を XClarity Integrator に登録するには、https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/plan_openports.html を参照してください。
2. 特定の Lenovo Services Web サイトにアクセスするには、「8 ページの 「ファイアウォール」」 を参照してください。

XClarity Integrator と管理対象デバイス間のアクセス

計算ノードやラック・サーバーなどの管理対象デバイスがファイアウォールで保護されており、ユーザーが、ファイアウォールの外側にある XClarity Integrator サーバーからこれらデバイスを管理する場合は、XClarity Integrator と各管理対象デバイスのベースボード管理コントローラー間の通信関連するすべてのポートが開いていることを確認します。

注：XClarity Integrator と サーバー BMC 間で ICMP プロトコルも許可する必要があります。Lenovo XClarity Integrator は、ファームウェア更新中に ICMP (ping) を使用して BMC の接続を確認します。

表 7. サーバーと計算ノード

通信	ThinkSystem および ThinkAgile	System x
アウトバウンド (外部システムで開くポート)	• SLP – ポート 427 の UDP • HTTPS – ポート 443 の TCP • CIM HTTPS – ポート 5989 の TCP [2] • ファームウェア更新 - ポート 6990 の TCP [4] • SLP – ポート 427 の UDP	• HTTPS – ポート 443 の TCP • IPMI – ポート 623 のTCP [1] • CIM HTTP – ポート 5988 の TCP [3] • CIM HTTPS – ポート 5989 の TCP [3] • ファームウェア更新 - ポート 6990 の TCP [4]
インバウンド (XClarity Integrator アプライアンスで開いたポート)	• HTTPS – ポート 443 の TCP • ファームウェア更新 - ポート 6990 の TCP [4]	• HTTPS – ポート 443 の TCP • ファームウェア更新 - ポート 6990 の TCP [4]

1. XClarity Integrator は、サーバー構成とファームウェア更新にこのポートを使用します。
2. デフォルトでは、このポートは一部の新しいサーバーでは無効になっています。この場合、このポートを開く必要はありません。XClarity Integrator は管理に REST Over HTTPS を使用します。このポートは、CIM を使用して XClarity Integrator で管理されているサーバーでのみ開く必要があります。
3. デフォルトでは、管理はセキュア・ポートを介して実行されます。非セキュア・ポートはオプションです。
4. このポートは、BMU OS に接続してファイルを転送し、更新コマンドを実行するために使用されます。

ファイアウォール

管理サーバーの更新およびファームウェア更新をダウンロードするには、インターネットにアクセスする必要があります。ご使用のネットワークでファイアウォール (該当する場合) を構成し、LXCI 管理サーバーがこれらの操作を実行できるようにします。管理サーバーがインターネットに直接アクセスできない場合、LXCI を構成してプロキシー・サーバーを使用します。

ファイアウォールで次の FQDN と ポートが利用できることを確認したら、プロキシーで許可します。

表 8. インターネット接続要件

DNS 名	ポート	プロトコル
datacentersupport.lenovo.com	443	https
download.lenovo.com	443	https
filedownload.lenovo.com	443	https
support.lenovo.com	443	https
supportapi.lenovo.com	443	https

プロキシー

vCenter でプロキシーを設定し、vLCM 機能を使用してファームウェアを更新するには、ユーザーが vCenter から Lenovo XClarity Integrator (プロトコル HTTPS、ポート 443) への接続を、ユーザーの会社のプロキシー構成で許可する必要があります。

プロキシー・サーバーは、以下の要件を満たしている必要があります。
- プロキシー・サーバーが基本認証を使用するようにセットアップされている。
- プロキシー・サーバーが終了しないプロキシーとしてセットアップされている。
- プロキシー・サーバーが、転送プロキシーとして設定されている。
- ロード・バランサーは、1 つのプロキシー・サーバーでのみセッションを保持するように構成されている。

VMware vCenter 対応 Lenovo XClarity Integrator のインストール

このセクションでは、VMware vCenter 対応 Lenovo XClarity Integrator 仮想アプライアンスのインストール手順について説明します。

注：VMware vCenter 対応 Lenovo XClarity Integrator 仮想アプライアンスは、VMware ESXi ベースの環境にのみインストールできます。

始める前に

インストールする前に、以下の点に注意してください。
- ESXi ホストに VMware vCenter 対応 Lenovo XClarity Integrator 仮想アプライアンス用の十分なフリー・ディスク・スペースとメモリーがあること。
- ネットワークが DHCP または静的 IP アドレスを使用するように設定されていること。

手順

vSphere Client から ESXi ホストに VMware vCenter 対応 Lenovo XClarity Integrator 仮想アプライアンスをインストールするには、次の手順を実行します。

ステップ 1. vSphere Client にログインします。

ステップ 2. ターゲット ESXi ホストを右クリックし、「**Deploy OVF Template** (OVF テンプレートのデプロイ)」をクリックします。「Deploy OVF Template (OVF テンプレートのデプロイ)」ウィザードが表示されます。

ステップ 3. 「**Select an OVF template** (OVF テンプレートの選択)」ページで、ソースの場所として「**URL**」または「**Local file** (ローカル・ファイル)」を選択します。ローカル・ファイルの場合、「**Choose Files (ファイルの選択)**」をクリックして OVF ファイルの場所を入力してから、「**NEXT (次へ)**」をクリックします。

ステップ 4. 「**Select a name and folder (名前とフォルダーの選択)**」ページで、仮想マシン固有の名前とターゲットの場所を入力し、「**NEXT (次へ)**」をクリックします。

ステップ 5. 「**Select a computer resource (コンピューター・リソースの選択)**」ページで、宛先コンピューターのリソースを選択し、「**NEXT (次へ)**」をクリックします。

ステップ 6. 「**Review details (詳細の確認)**」ページで、詳細を確認して「**NEXT (次へ)**」をクリックします。

ステップ 7. 「**License agreements (ライセンス契約)**」ページで、ライセンス契約を読み、「**I accept all license agreements. (すべてのライセンス契約に同意します。)**」を選択し、「**NEXT (次へ)**」をクリックします。

ステップ 8. 「**Select storage (ストレージの選択)**」ページで、構成とディスク・ファイルのストレージを選択し、「**NEXT (次へ)**」をクリックします。

ステップ 9. 「**Select networks (ネットワークの選択)**」ページで、そのターゲット仮想サーバーのネットワークを選択し、「**NEXT (次へ)**」をクリックします。

注：「**IP Allocation Settings** (IP 割り当て設定)」セクションに表示されている設定をスキップします。IP 割り当て設定は、次の手順で構成します。

ステップ 10. 「**Customize template (テンプレートのカスタマイズ)**」ページで、ネットワーク構成を設定して、「**NEXT (次へ)**」をクリックします。

注：ユーザーは、vCenter のアドレス、ユーザー名、およびパスワードを「**vCenter Registration (vCenter の登録)**」領域に入力できます。

ステップ 11. 「**Ready to Complete** (実行する準備ができました)」ページで、詳細を確認して「**Finish** (終了)」をクリックします。

ステップ 12. 仮想マシンの電源を入れます。仮想マシンの電源がオンになると、「Lenovo XClarity Integrator」のアプライアンス管理ページにアクセスするための URL が VM コンソールに表示されます。

たとえば、次の図はアプライアンスの管理に使用する URL が表示されます。

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

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

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

ステップ 13. 「Lenovo XClarity Integrator」のアプライアンス管理ページに移動します。たとえば、次のような場合です。`https://192.0.2.10/admin`

ステップ 14. 「**Account Configuration** (アカウント構成)」ページで、「Lenovo XClarity Integrator」のアプライアンス管理ページにログインするための管理者アカウントを設定し、「**Submit** (送信)」をクリックします。

ステップ 15. 「**Lenovo XClarity Integrator appliance administration** (Lenovo XClarity Integrator アプライアンス管理)」ログイン・ページで、ウィザードで作成した管理者アカウントを入力し、「**Login** (ログイン)」をクリックします。「**vCenter Connection** (vCenter 接続)」ページが表示されます。

ステップ 16. 「**vCenter Connection** (vCenter 接続)」ページで、「**Register** (登録)」をクリックして、Lenovo XClarity Integrator を vCenter Server に登録します。詳しくは、53 ページの 「vCenter 接続の構成」 を参照してください。

vSphere Lifecycle Manager の有効化/無効化

LXCI は、vSphere Lifecycle Manager (vLCM) のハードウェア・サポート・マネージャーとして機能し、ベース ESXi、Lenovo ドライバーのアドオン、およびファームウェアのアドオンで構成されるクラスター全体のイメージを使用して Lenovo ESXi サーバーを管理する vLCM を有効にします。

始める前に

ターゲット・サーバーがサポートされていることを確認します。サポートされるマシン・タイプについての詳しくは、4 ページの 表 4「サポートされている Lenovo サーバー」 を参照してください。

手順

ユーザーは、VLCM のハードウェア・サポート・マネージャーとして LXCI を有効または無効にできます。

「**vCenter Connection** (vCenter 接続)」ページで、「**vSphere Lifecycle Manager**」列で「**Disable** (無効)」または「**Enable** (有効)」をクリックして、必要なサーバーの vLCM ステータスを変更します。

VLCM を使用したファームウェア更新の管理について詳しくは、37 ページの 「vSphere Lifecycle Manager 機能の使用」 を参照してください 。

次に行うこと

VMware vCenter 対応 Lenovo XClarity Integrator にログインして構成します (15 ページの 第 3 章「Lenovo XClarity Integrator の構成」を参照)。

事前対応ハードウェア管理の有効化/無効化

LXCI は、事前対応ハードウェア管理 (PHM) のハードウェア・サポート・マネージャーとして機能します。

始める前に

ターゲット・サーバーがサポートされていることを確認します。サポートされるマシン・タイプについての詳しくは、4 ページの 表 4「サポートされている Lenovo サーバー」 を参照してください。

手順

ユーザーは、PHM のハードウェア・サポート・マネージャーとして LXCI を有効または無効にできます。

「**vCenter Connection (vCenter 接続)**」ページで、「**Proactive Hardware Management (事前対応ハードウェア管理)**」列で「**Disable (無効)**」または「**Enable (有効)**」をクリックして、必要なサーバーの PHM ステータスを変更します。

PHM を使用したファームウェア更新の管理について詳しくは、41 ページの 「事前対応ハードウェア管理機能の使用」を参照してください 。

次に行うこと

VMware vCenter 対応 Lenovo XClarity Integrator にログインして構成します (15 ページの 第 3 章「Lenovo XClarity Integrator の構成」を参照)。

Lenovo XClarity Integrator の高可用性の実装

Lenovo XClarity Integrator の高可用性を実装するには、ESXi 環境で vSphere 高可用性 (HA) 機能を使用します。ESXi ホストでの実行に失敗すると、代替ホスト上で Lenovo XClarity Integrator が再起動されます。

始める前に

vSphere HA クラスターが使用可能であることを確認します。VSphere HA クラスターの作成について詳しくは、「Creating a vSphere HA Cluster (vSphere 高可用性クラスターの作成)」を参照してください。

手順

Lenovo XClarity Integrator の高可用性を実装するには、以下の手順を実行します。

ステップ 1. vSphere HA クラスターに Lenovo XClarity Integrator をデプロイします。

ステップ 2. 「**Restart VMs (VM の再起動)**」を選択し、Respond to Host Failure (ホスト障害時の対応) のステップに基づいて、ホストの障害時の対応を構成します。

ステップ 3. 「VM 監視を有効化」のステップに基づいて、VM 監視を有効にします。

VMware vCenter 対応 Lenovo XClarity Integrator のアップグレード

VMware ESXi ベースの完了に、すでに VMware vCenter 対応 Lenovo XClarity Integrator があるインストールされている場合は、アップグレードします。

VMware ESXi ベースの環境での VMware vCenter 用 LXCI のアップグレード

このセクションでは、Lenovo XClarity Integrator 仮想アプライアンスが既に ESXi ベースの環境にインストールされている場合に更新する方法について説明します。

始める前に

更新を実行するには、まず更新パッケージを入手する必要があります。通常、更新パッケージには 4 つのファイルが含まれています。

- **.chg ファイル**: 変更履歴ファイル
- **.tgz ファイル**: 更新ペイロード
- **.txt ファイル**: 特定の更新パッケージの Readme ファイル
- **.xml ファイル**: 更新に関するメタデータ

注：Lenovo XClarity Integrator v5.0.2 または v5.1.0 を使用するには、更新パッケージを適用する前に、修正パッチ `lnvgy_sw_lxci_upload_fixpatch_1.0.0_anyos_noarch` を適用してください。次の手順でステップ 2 ー 7 を実行して、修正パッチを適用します。2 つのメッセージがプラグイン登録に関する情報とともに表示されます。このメッセージは無視してください。パッチは、VMware 対応 Lenovo XClarity Integrator Web サイト からダウンロードできます。

手順

ステップ 1. (オプション) Lenovo XClarity Integrator を VMware vCenter から登録解除します。

ステップ 2. Lenovo XClarity Integrator Web インターフェースから、ページの左パネルにある「**Version and upgrade** (バージョンとアップグレード)」をクリックします。

ステップ 3. 「**Import** (インポート)」をクリックします。「Import (インポート)」ダイアログが表示されます。

ステップ 4. 「**Browse (参照)**」をクリックし、ターゲット・ファイルを選択したら、「**Open (開く)**」をクリックします。選択したファイルが「Import (インポート)」ダイアログに表示されます。

注：TXT、CHG、XML、および TGZ ファイルが選択されている必要があります。

ステップ 5. 「**Import** (インポート)」をクリックして選択されたファイルをインポートします。

注：

- 更新パッケージと基本ネットワークのサイズに応じて、インポート処理に数分から数時間かかることがあります。ネットワークに接続されていることを確認し、進行状況表示バーが完了してダイアログが閉じるまで待ちます。
- `Invalid session` エラーが表示された場合、セッションが期限切れです。Lenovo XClarity Integrator Web インターフェースからログアウトして再度ログインし、インポート操作を再試行します。高速なネットワークに更新パッケージを置くことを検討してください。

ステップ 6. 更新パッケージがインポートされたら、表で更新パッケージを選択し、「**Perform Update** (更新の実行)」をクリックします。プロンプト・ダイアログが表示されます。情報をよく読みます。

注：
- 更新プロセスを完了するには、Lenovo XClarity Integrator の再起動が必要になることがあります。再起動した場合、構成接続と他のすべてのアクティブ・ジョブが停止します。
- 更新の進行状況は、vSphere Client または vCenter Web クライアントで仮想アプライアンス・コンソールから監視できます。

ステップ 7. アプライアンス・コンソールが開いたら、「**OK**」をクリックすると、更新リクエストがサーバーに送信されます。更新の進行状況メッセージがコンソールに表示されます。コンソールに、`update finished` と表示され、エラーが表示されなかったら、正常に更新されたことを示します。

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

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


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

ステップ 8. (オプション) Lenovo XClarity Integrator を VMware vCenter に登録します。

VMware vCenter 対応 Lenovo XClarity Integrator のアンインストール

このセクションでは、VMware vCenter 対応 Lenovo XClarity Integrator のアンインストール方法について説明します。

手順

以下の手順を実行して VMware vCenter 対応 Lenovo XClarity Integrator をアンインストールします。

1. 「**Lenovo XClarity Integrator appliance administration** (Lenovo XClarity Integrator アプライアンス管理)」ページにログインします。
2. アプライアンスのバックアップを作成します。
3. vCenter からプラグインを登録解除します。詳しくは、53 ページの 「vCenter 接続の構成」を参照してください。
4. vSphere Client でアプライアンスをオフにし、インベントリーから削除します。
5. vSphere Client サービスを停止します。
6. vCenter サーバーから、`/etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/` 以下の `com.lenovo.lxci-*.*` ディレクトリーを削除します。

   注：vCenter サーバーのバージョンによっては、`/etc/vmware` パスが異なることがあります。
7. vSphere Client サービスを起動します。

第 3 章　Lenovo XClarity Integratorの構成

このセクションのトピックには、ターゲット・サーバーでの Lenovo XClarity Integrator の構成に関する情報があります。

BMC の検出と管理

Lenovo XClarity Integrator を使用すると、BMC を検出して BMC を ESXi ホストに関連付けることができるため、vSphere 環境でターゲット・サーバーのアウト・オブ・バンド (OOB) 管理を有効にできます。

Lenovo XClarity Integrator では、BMC を検出および管理するための 2 つの方法がサポートされています。

- BMC の直接的な検出と管理

  注：これは、以下のサーバーに適用されません。
  - ThinkServer サーバー
  - ThinkSystem SR635
  - ThinkSystem SR655
- Lenovo XClarity Administrator を使用した BMC の検出と管理

注：ThinkSystem サーバーでは、CIM サービスはデフォルトで無効になっています。ファームウェア・レベルによっては、LXCI によって CIM サービスがサーバーを管理できる場合があります。

BMC の直接検出と管理

BMC のアドレスと資格情報を入力することで、BMC を直接検出して管理できます。

手順

ステップ 1. 「vSphere Client」 Web ページで、「**Menu (メニュー)**」ドロップダウン・リストをクリックして、「**Lenovo XClarity Integrator**」を選択します。「Lenovo XClarity Integrator」管理ページが表示されます。

ステップ 2. 「**Discover servers (サーバーを検出)**」セクションをクリックします。サーバー検出ページが表示されます。

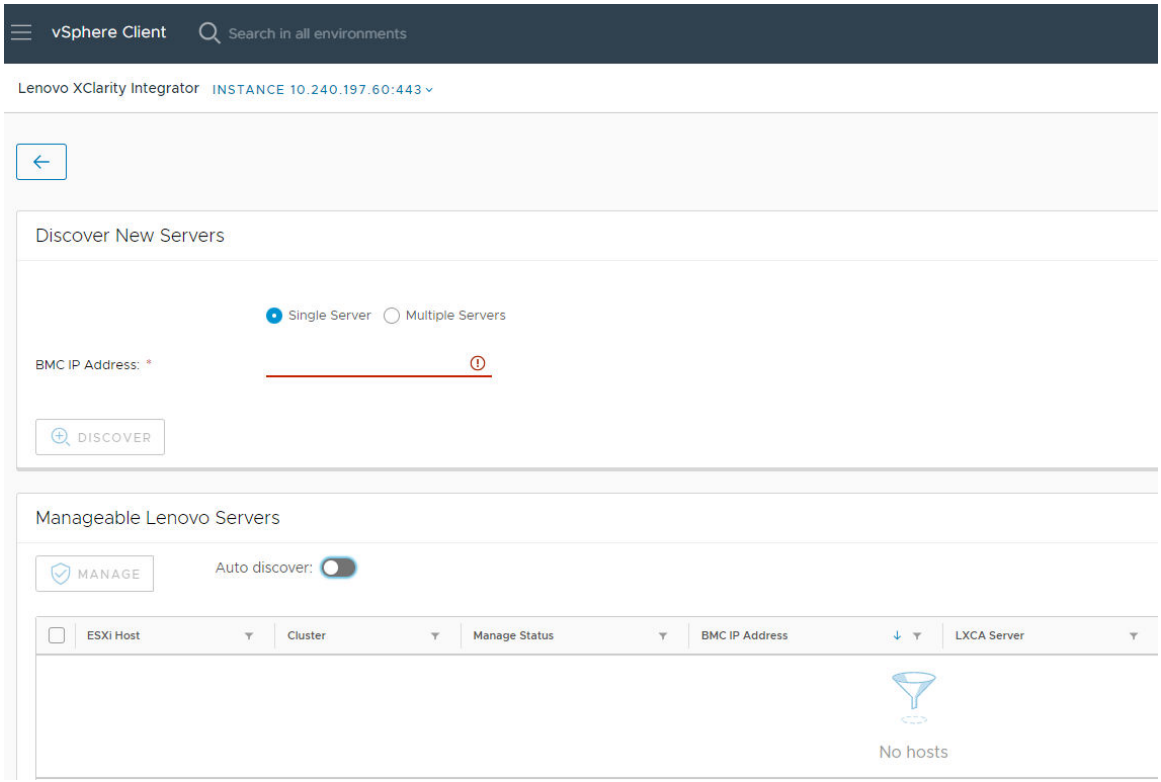


図 1. BMC の検出と管理

注：管理可能だが Lenovo XClarity Integrator によって管理されていない vCenter 管理 ESXi ホストがすべて「**Manageable Lenovo Servers** (管理可能な Lenovo Server)」セクションにリストされます。BMC が Lenovo XClarity Integrator によって検出されていないホストの場合、このホストの管理ステータスが「**Manage Status** (ステータスの管理)」列に「Not Ready (作動不能)」と表示されます。

ステップ 3. 「**Discover New Servers (新しいサーバーの検出)**」セクションで、単一の BMC IP アドレスか複数サーバー用の IP アドレス範囲を入力したら、「**Discover (検出)**」をクリックします。

注：

- IP アドレス範囲に含まれる IP アドレスが 60 未満にすることをお勧めします。
- 1 つの BMC が検出され、1 つのESXi ホストに関連付けることができる場合、BMC IP アドレスが、「**Manageable Lenovo Servers (管理可能 Lenovo Server)**」テーブルの「**BMC IP address (BMC IP アドレス)**」列に表示され、ESXi ホストの管理ステータスが「**Manage Status (ステータス管理)**」列で「**Ready (準備完了)**」に変更されます。

ステップ 4. 「Manageable Lenovo Servers (管理可能 Lenovo Server)」領域で、以下のいずれかを実行します。

- サーバーを管理するには、「**Ready (準備完了)**」ステータスのターゲット・サーバーを 1 つ以上選択し、「**MANAGE (管理)**」をクリックします。その後、ポップアップ・ウィンドウで、BMC ユーザー名とパスワードを入力し、「**OK**」をクリックします。

  サーバーが適切に管理されている場合、成功メッセージが表示されます。サーバーの管理ステータスが、「**Manage Status (ステータス管理)**」**列で、**「**Managing (管理中)**」に変わり、サーバーが、「**Managed Servers (管理対象サーバー)**」セクションに表示されます。
- 自動検出機能を有効化または無効化するには、トグル・アイコンをクリックし、「**Yes (はい)**」をクリックして、すぐにプロセスを開始するか、「**NO (いいえ)**」をクリックして、LXCI が有効化された後、24 時間以内にプロセスを開始するようにします。

注：自動検出サービスを実行する前に、SSDP プロトコルを有効にする必要があります。自動検出機能が有効な場合は、1 日に 1 回実行されます。

LXCA を使用した BMC の検出と管理

Lenovo XClarity Administrator がすでに利用可能で、Lenovo XClarity Administratorが、ESXi サーバーを管理している場合、Lenovo XClarity Integrator でサーバーを検出または管理する必要はありません。Lenovo XClarity Administrator を Lenovo XClarity Integrator に登録するだけで、Lenovo XClarity Integrator が Lenovo XClarity Administrator を介して、BMC を自動検出・管理します。Lenovo XClarity Administrator の登録方法については、17 ページの 「Lenovo XClarity Administrator の構成」 を参照してください。

注：LXCA を LXCI に登録する際は、LXCA アカウントに LXCI が管理するすべてのターゲット・サーバーを管理する言々が付与されているかを確認します。これらのサーバーは、LXCA の**ローカル認証**ではなく、**管理対象認証**が管理する必要があります。詳細については、https://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html を参照してください。

Lenovo XClarity Administrator の構成

Lenovo XClarity Integrator は Lenovo XClarity Administrator を使用してターゲット・サーバーをまとめて管理するための統合手段を提供します。Lenovo XClarity Administrator が Lenovo XClarity Integrator に登録されると、Lenovo XClarity Integrator はサーバーを自動的に検出および管理できるようになります。vSphere Client でサーバーを管理するには、シャーシ・マップ、構成パターン、ファームウェア・ポリシー展開などの Lenovo XClarity Administrator の機能を使用します。

始める前に

Lenovo XClarity Administrator を Lenovo XClarity Integrator に登録する前に、以下を確認してください。

- Lenovo XClarity Administrator は現在の環境で動作しています。
- *Lenovo XClarity Integrator Administration* 権限を持っていること。

手順

ステップ 1. 「vSphere Client」Web ページで、上部の「**Menu (メニュー)**」ドロップダウン・リスト・ボックスをクリックし、「**Lenovo XClarity Integrator**」を選択します。「Lenovo XClarity Integrator」管理ページが表示されます。

ステップ 2. 「**Service Status (サービス状況)**」セクションで、「**ADD LENOVO XCLARITY ADMINISTRATOR (Lenovo XClarity Administrator を追加)**」をクリックします。「Registration Wizard (登録ウィザード)」ページが表示されます。

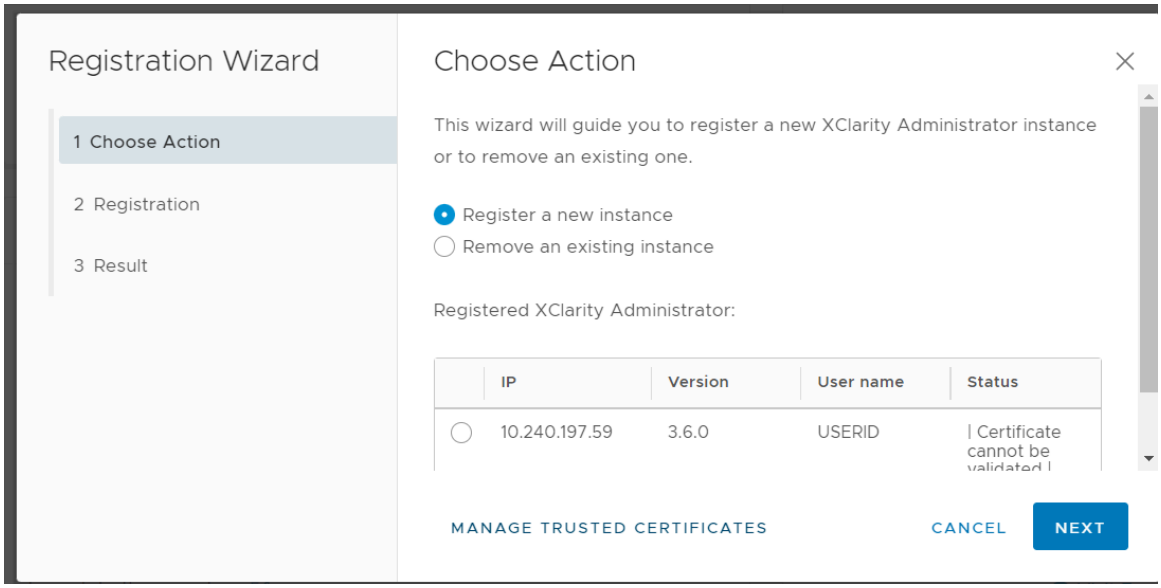


図 2. 「Registration Wizard (登録ウィザード)」ページ

ステップ 3. 次のいずれかを行います。

- 新規インスタンスの登録:
  1. 「Choose Action (操作の選択)」ページで、「**Register a new instance (新規インスタンスの登録)**」「**Next (次へ)**」の順に選択します。
  2. 「Registration (登録)」ページで、以下のいずれかを実行します。
     - 「**Use an existing account (既存アカウントの使用)**」を選択して、ホスト名または IP アドレス、ユーザー名およびパスワードを入力したら、「**Next (次へ)**」をクリックします。

       注：以下を確認してください。
       - このアカウントには、「lxc-supervisor」役割グループまたは「lxc-operator、lxc-fw-admin、lxc-hw-admin および lxc-os-admin」の組わせ役割グループがあります。
       - リソース・アクセス制御が XClarity Administrator で有効になっている場合、このアカウントはサーバーにアクセスできます
     - 「**Create a new account by connecting with this administrative account (この管理者アカウントに接続して新しいアカウントを作成する)**」を選択して、ホスト名または IP アドレス、ユーザー名およびパスワードを入力し、「**Next (次へ)**」をクリックします。

       注：
       - 新しいアカウントに、「lxc-operator、lxc-fw-admin、lxc-hw-admin および lxc-os-admin」の役割グループが付与されていることを確認します。
       - リソース・アクセス制御が XClarity Administrator で有効になっている場合、このアカウントはサーバーにアクセスできることを確認します。
       - LDAP が XClarity Administrator で使用されているか、ローカル・アカウントが無効になっている場合は、このオプションを選択しないでください。
  3. (オプション) 「View Certificate (証明書の表示)」ページで、「**Next (次へ)**」をクリックして、証明書を許可します。
  4. 「Result (結果)」ページで、「**FINISH (終了)**」をクリックします。
- 既存のインスタンスの削除:

1. 「Choose Action (操作の選択)」ページで、「**Remove an existing instance (既存のインスタンスの削除)**」を選択して、テーブルからターゲット・インスタンスを選択したら、「**Next (次へ)**」をクリックします。
2. 「Unregister (登録抹消)」ページで、「**Next (次へ)**」をクリックします。
3. 「Result (結果)」ページで、「**FINISH (終了)**」をクリックします。

- トラステッド証明書の管理:
  1. 「Choose Action (操作の選択)」ページで、「**MANAGE TRUSTED CERTIFICATES (トラステッド証明書を管理)**」をクリックして、「VMware vCenter」ページにアクセスします。
  2. 67 ページの 「トラステッド証明書の管理」の手順を実行します。

アクセス制御の構成

Lenovo XClarity Integratorは、役割ベースのアクセスをサポートしています。

さまざまな機能へのアクセスを制御するため、以下の 4 つの権限が定義されています。

権限	許可された機能
システム一覧	• ホストのインベントリー、イベント、使用状況情報の表示 • BMC インターフェースの起動
ファームウェア更新	ファームウェアの更新
構成	システム設定の構成と KVM の起動
管理	LXCI 管理ページへのアクセス: • LXCI/vCenter 接続の編集 • LXCA 接続の追加 • サーバーの検出と管理 • サーバーを介した管理の無効化

デフォルトでは、vCenter 管理者の役割は Lenovo XClarity Integrator により定義されたすべての権限を持っています。vCenter 管理者は、必要に応じてこれらの権限を他の vCenter ユーザーに付与できます。

Lenovo XClarity Integrator 証明書を Web ブラウザーにインポート

Lenovo XClarity Integrator を使用する証明書が信頼できるサードパーティによって署名されておらず、ファームウェア更新、シャーシ・マップ、システム設定などの機能を使用する場合、表示ページがブロックされます。この場合、ユーザーは、Lenovo XClarity Integrator ルート証明書をダウンロードして、それを、作業しているブラウザーに応じて、トラステッド証明書の Web ブラウザー・リストにインポートするか、セキュリティーの例外に追加します。

手順

- Internet Explorer および Chrome の場合:
  1. 「Lenovo XClarity Integrator (Lenovo XClarity Integrator アプライアンス管理)」ページにログインします。
  2. 「**Security Settings** (セキュリティー設定)」をクリックし、「**Certificate Authority** (証明機関)」をクリックします。
  3. 「**Download Certification Authority Root Certificate** (証明機関ルート証明書のダウンロード)」をクリックして、証明書をダウンロードします。
  4. `downloadded.ca.cer` ファイルをダブルクリックします。
  5. 「**General** (全般)」タブで「**Install Certificate** (証明書のインストール)」をクリックします。
  6. 「**Local Machine (ローカル・マシン)**」を選択し、「**Next** (次へ)」をクリックします。
  7. 「**Certificate Store** (証明書ストア)」ページで、「**Place all certificates in the following store** (すべての証明書を次のストアに配置する)」を選択し、「**Browse** (参照)」をクリックします

8. 「**Trusted Root Certificate Authorities** (信頼されたルート証明機関)」を選択し、「**OK**」をクリックします。
9. 「**Finish** (終了)」をクリックします。
10. Internet Explorer の場合、ブラウザーを閉じてもう一度開き、変更を有効にします。

- Firefox の場合:
  1. ブラウザーを開いた状態で、「**Firefox**」 ➙ 「**Options (オプション)**」 ➙ 「**Privacy&Security (プライバシーとセキュリティ)**」 ➙ 「**Certificates (証明書)**」 ➙ 「**View Certificates (証明書を表示)**」 ➙ 「**Servers (サーバー証明書)**」 ➙ 「**Add Exception (例外を追加)**」をクリックします。
  2. 「**Location (ロケーション)**」フィールドに、Lenovo XClarity Integrator でインストールしたホストの完全修飾ドメイン・ネームまたは IP アドレスを入力します。
  3. 「**Get Certificate** (証明書の取得)」をクリックします。
  4. 「**Confirm Security Exception (セキュリティー例外の確認)**」をクリックして、ブラウザーを更新します。

第 4 章　環境概要の表示

このセクションでは、Lenovo XClarity Integrator ダッシュボードの概要を説明します。Lenovo XClarity Integrator ダッシュボードは、管理対象サーバー、管理可能サーバー、サービス・ステータス、製品情報の概要を示します。

手順

Lenovo XClarity Integrator ダッシュボードを表示するには、以下の手順を実行します。
1. 「vSphere Client」Web ページから、上部にある「**Menu** (メニュー)」ドロップダウン・リスト・ボックスをクリックします。
2. 「**Lenovo XClarity Integrator**」をクリックします。Lenovo XClarity Integrator 管理ページが表示されます。

ダッシュボードで以下のセクションのいずれかを選択します。
- 「**Discover Servers** (サーバーの検出)」: 21 ページの 「「Discover Servers (サーバーの検出)」セクション」を参照してください。
- 「**Managed Servers** (管理対象サーバー)」: 21 ページの 「「Managed Servers (管理対象サーバー)」セクション」を参照してください。
- 「**Service Status** (サービス状況)」: 22 ページの 「「Service Status (サービス・ステータス)」セクション」を参照してください。
- 「**Product Information** (製品情報)」: 22 ページの 「「Product Information (製品情報)」セクション」を参照してください。

「Discover Servers (サーバーの検出)」セクション

このセクションでは、管理可能な Lenovo Server の数を表示できます。「**Manageable Lenovo Servers (管理可能な Lenovo Server)**」または「**Discover New Servers (新しいサーバーの検出)**」をクリックすると、サーバーの検出や管理など、詳細な操作ペインを操作できます。

「**Manageable Lenovo Servers** (管理可能な Lenovo Server)」セクションには、管理可能サーバーの以下の詳細がリストされた表があります。
- ESXi ホスト
- クラスター
- ステータス管理
- BMC IP アドレス
- LXCA サーバー
- モデル
- シリアル番号
- 製品名
- vCenter

「Managed Servers (管理対象サーバー)」セクション

このセクションでは、管理対象 Lenovo Server 数と、これらのサーバー上にある仮想マシンの数を、サーバー・ステータスごとにグループ分けして表示できます。数の情報をクリックすると、「**Managed Servers (管理対象サーバー)**」操作ペインを表示できます。

「**Managed Servers** (管理対象サーバー)」操作ペインには、管理可能サーバーの以下の詳細がリストされた表があります。
- ESXi ホスト
- クラスター
- ステータス
- 電源

- BMC IP アドレス
- LXCA サーバー
- モデル
- シリアル番号
- vCenter

次のいずれかを実行します。
- 管理対象サーバーのインベントリー情報を更新するには、「**REFRESH INVENTORY** (インベントリーの最新表示)」ボタンをクリックします。
- 必要に応じて管理対象サーバーの BMC ユーザー名およびパスワードを更新するには、「**EDIT CREDENTIALS (資格情報の編集)**」ボタンをクリックします。
- 管理対象サーバーを介して管理を無効にするには、「**UNMANAGE** (管理対象から除外)」ボタンをクリックします。

  注：このサーバーのすべての Lenovo XClarity Integrator 機能が無効になり、このサーバーが「**Manageable Lenovo Servers** (管理可能な Lenovo Server)」セクションに表示されます。

「Service Status (サービス・ステータス)」セクション

このセクションには、Lenovo XClarity Integrator が提供するサービスのステータスが表示されます。

このセクションには、以下の 3 種類のサービスが表示されます。
- XClarity Integrator サービス

  Lenovo XClarity Integrator バックエンド・サービスの IP アドレスとステータスが表示されます。「**EDIT (編集)**」をクリックすると、Lenovo XClarity Integratorサービスに接続するための IP アドレス、ユーザー名、パスワードを編集できます。
- vCenter サーバー

  XClarity Integrator が登録されている vCenter サーバーが表示されます。「**EDIT (編集)**」をクリックすると、VMware vCenter 対応 Lenovo XClarity Integrator 管理者 Web ページを表示できます。詳しくは、53 ページの 「vCenter 接続の構成」 を参照してください。
- XClarity Administrator

  XClarity Integrator に登録されている XClarity Administrators が表示されます。「**EDIT (編集)**」または「**LAUNCH (起動)**」をクリックすると、XClarity Administrators を編集または起動できます。

「Product Information (製品情報)」セクション

このセクションでは、Lenovo XClarity Integrator の製品情報を表示できます。

以下のリンクをクリックすると、製品の詳細を参照したり、製品の改善に役立つフィードバックを送信したりすることができます。
- Lenovo ライセンス契約書の表示
- サード・パーティ・ライセンスの表示
- サード・パーティ・ライセンスの表示
- オンライン資料
- 製品の Web サイト
- フォーラムにアクセス
- アイデアを送信

第 5 章　サーバーの管理

Lenovo XClarity Integrator は、System x、BladeCenter および Flex サーバーのプラットフォーム管理を行います。このセクションのトピックでは、Lenovo XClarity Integrator を使用したサーバーの管理方法について説明します。

以下の前提条件を満たしていることを確認してください。
- 同じ LXCI インスタンスに登録されている vCenter が管理する Lenovo Server の数は 1,000 を超えないようにしてください。超える場合は、これらの Lenovo Server に対して複数の LXCI インスタンスをデプロイする必要があります。
- VMware vCenter Server が、管理対象 ESXi サーバーの BMC にアウト・オブ・バンド (OOB) ネットワーク接続できる。
- 「**Cluster Overview (クラスターの概要)**」ページでは、BMC を確認し、BMC への要求済みアクセスを維持できます。
- 以下のサーバーが Lenovo XClarity Administrator によって管理され、Lenovo XClarity Administrator が Lenovo XClarity Integrator に登録されている必要があります (17 ページの 「Lenovo XClarity Administrator の構成」 を参照)。
  - ThinkServer サーバー
  - ThinkSystem SR635
  - ThinkSystem SR655

手順

ステップ 1. インベントリー・ツリーから vCenter ホストを選択します。

ステップ 2. 「**Monitor (監視)**」タブをクリックします。
左側のナビゲーション・ペインで、必要に応じて「**Lenovo XClarity**」から以下のいずれかの機能を選択します。
- システム概要
- イベント
- システム一覧
- 使用状況
- シャーシ・マップ
- ハードウェア・トポロジー

ステップ 3. 「**Configure (構成)**」タブをクリックします。
左側のナビゲーション・ペインで、必要に応じて「**Lenovo XClarity**」から以下のいずれかの機能を選択します。
- ファームウェア更新
- 電源ポリシー
- 構成

ステップ 4. インベントリー・ツリーから vCenter ホストを右クリックします。表示された「**Actions (操作)**」ドロップダウン・リスト・ボックスでカーソルを「**Lenovo XClarity**」に移動します。以下のいずれかの機能を選択します。
- リモート・コンソールの起動
- BMC インターフェースの起動

システム情報の表示

「System Overview (システム概要)」ページには、現在のシステムのスナップショット・ビューが表示されます。マシン・タイプ、オペレーティング・システム、バージョン、BMC ファームウェア・バージョン、UEFI ファームウェア・バージョンなどの基本的なシステム情報を表示できます。また、システムのハードウェア・イベント要約を表示し、完全な診断データを収集することもできます。

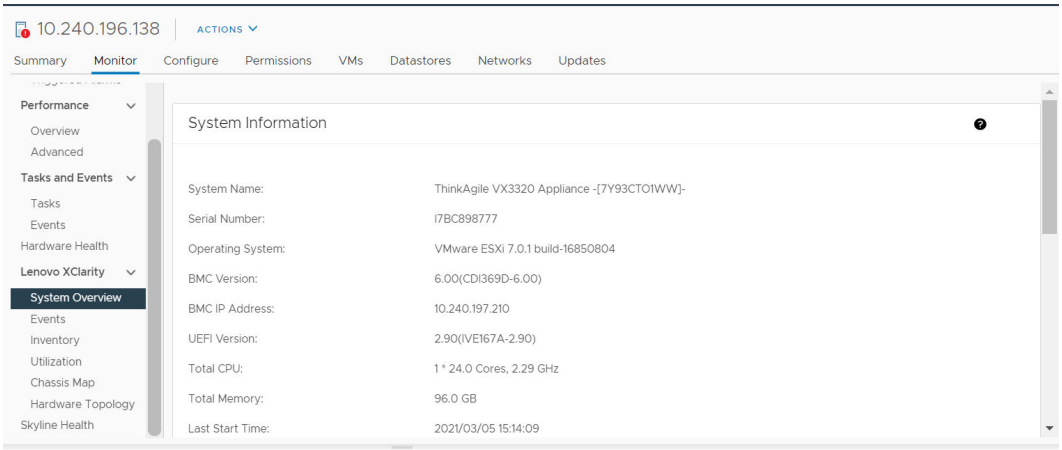


図 3. 「System Overview (システム概要)」ページ

システム診断収集機能の起動

手順

完全なシステム診断データを収集するには、以下の手順を実行します。

ステップ 1. 「System Overview (システム概要)」ページの下部セクションにある「**Collect (収集)**」をクリックします。

注：この収集プロセスには最大で 5 分かかります。完了すると、前回の収集時間が「**System Overview (システム概要)**」ページに表示されます。

ステップ 2. 最新のシステム診断データをダウンロードするには、「**Download log (ログのダウンロード)**」をクリックします。

サーバー・イベントの表示

現在のサーバーのハードウェア・イベントの詳細を表示できます。

以下のアイコンは、各イベントの重大度を示しています。

- : クリティカル
- : 警告
- : 通知

このページでは、次の操作について説明しています。

- 「**Type (タイプ)**」をクリックしてイベントをフィルタリングする
- 「**Refresh (最新表示)**」をクリックしてイベントを最新表示する
- 表の見出しをクリックしてシステム・イベントをソートする

サーバー・インベントリーの表示

「**Inventory (インベントリー)**」ページには、現在のサーバー・インベントリーのスナップショット・ビューが表示されます。このページでは、システム・ボード、マイクロプロセッサー、メモリー、ファン、センサー、NIC、PCI アダプター、ファームウェア情報を表示できます。

ページの右側にある「**Quick Link (クイック・リンク)**」を使用すると、目的のセクションにアクセスできます。特定のセクションで、+ 記号をクリックして詳細を表示します。

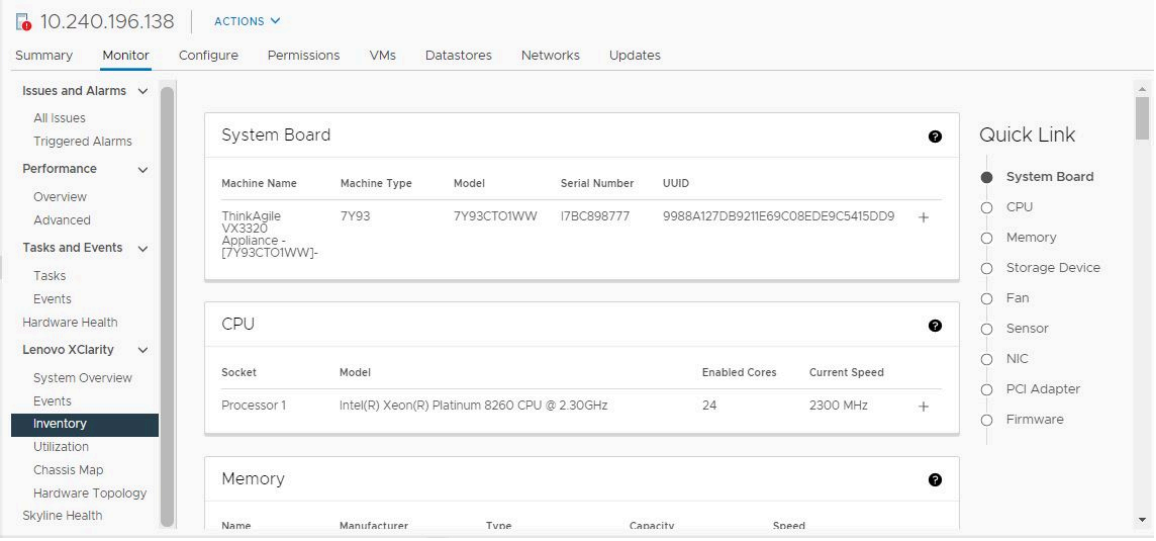


図 4. 「Inventory (インベントリー)」ページ

サーバーの使用状況の表示

「**Utilization (使用状況)**」ページには、周辺温度、システム電源入力、ファン速度の最新の使用状況情報と履歴が表示されます。

情報を見やすくするため、このページには情報のビューが 2 つあります (グラフィック・ビューと・テーブル・ビュー)。

図 5. 「Utilization (使用状況)」ページ

項目	最新情報	履歴情報
「Ambient Temperature (周辺温度)」	温度計グラフ	折れ線グラフ/リスト (直近 6 時間、12 時間、24 時間)
「Power Utilization (電力使用量)」	ドーナツ・グラフ	折れ線グラフ/リスト (直近 1、6 時間、12 時間、24 時間)
「Fan Speed (ファン回転数)」	リスト	該当なし

注：「Fan Speed (ファン回転数)」は「Table View (テーブル・ビュー)」でのみ使用できます。

ハードウェア・トポロジーの操作

ハードウェア・トポロジー機能は、ThinkAgile VX アプライアンス・サーバーに組み込みグラフィカル・ビューを提供します。このインターフェイスは、サーバー・レイアウト、詳細なハードウェア・インベントリーおよび正常性情報の表示および vSAN ディスクの管理をサポートします。

ホスト・ハードウェア・トポロジー

ホスト・ハードウェア・トポロジーは、ホストに関する全体的な情報を提供し、ユーザーがトポロジー上で操作を実行できます。

注：ホストが vCenter によってサポートされている必要があります。vCenter でサポートされていないホストの場合、ユーザーはページのプロンプトに従って LXCI またはブラウザーからハードウェア定義パッケージを確認してインストールできます。

「Hardware Topology (ハードウェア・トポロジー)」ページにアクセスするには、以下を行います。

1. vCenter ホストのインベントリー・ツリーからホストを選択し、右側のペインで「Monitor (モニター)」タブをクリックします。
2. 「Lenovo XClarity」で「Hardware Topology (ハードウェア・トポロジー)」をクリックします。ハードウェア・トポロジー・ビュー・ページが表示されます。
3. 次のいずれかを行います。
   - 一般的なホスト情報については、26 ページの「一般的なホスト情報の表示」を参照してください。
   - vSAN ディスク情報を表示するには、27 ページの「vSAN ディスク情報の表示」を参照してください。
   - パワー・サプライの情報については、「28 ページの「パワー・サプライ・ユニット (PSU) のヘルス・ステータスの表示」」を参照してください。
   - vSAN ディスクを削除する方法については、29 ページの「vSAN ディスクの削除」を参照してください。
   - vSAN ディスクを交換するには、30 ページの「vSAN ディスクの交換」を参照してください。

一般的なホスト情報の表示

ハードウェア・トポロジー・ページでは、ホストに関する一般情報の表示がサポートされています。

一般情報

「Hardware Topology (ハードウェア・トポロジー)」ページの上部ペインで、ユーザーはホストに関する一般情報を表示できます。

- 「Machine Name (マシン名)」
- 「Machine Type (マシン・タイプ)」
- 「Front Panel LED (前面パネル LED)」
  -  : 電源状態
  -  : ロケーション LED の状態
  -  : 障害 LED 状態
- 「Hardware Health (ハードウェア・ヘルス)」

  - 正常
  - 警告
  - クリティカル

注：詳細を表示するには、「**Hardware Health (ハードウェア・ヘルス)**」列の展開アイコン ⌄ をクリックします。

操作

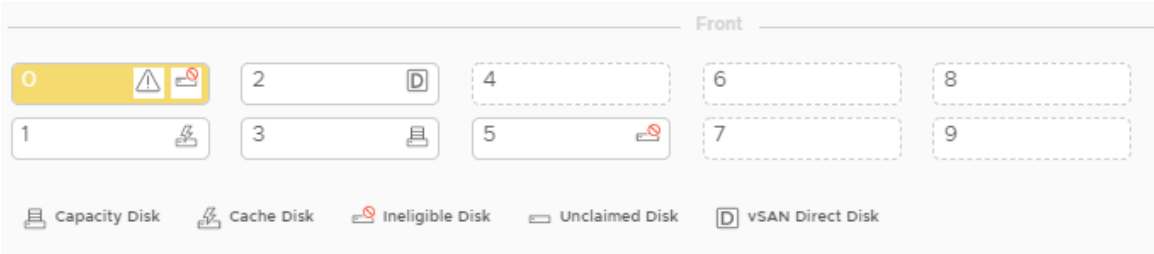
このペインの右側で、「**VIEW ACTIONS (操作の表示)**」および「**HOST ACTIONS (ホストの操作)**」をクリックすることもできます。

- 「**VIEW ACTIONS (操作の表示)**」で、
  - **View Detail Inventory (詳細インベントリーの表示)**: クリックして、「**Inventory (インベントリー)**」ページにアクセスします。
  - **View Reference Photo (参照写真の表示)**: クリックして、製品リファレンス・ページにアクセスします。このページには、このマシンの実際の前面図および背面図が記載されており、「Lenovo Press の製品ガイド」へのアクセスについての説明があります。
  - **Refresh Hardware Topology (ハードウェア・トポロジーを最新の情報に更新)**: クリックして、ハードウェア・トポロジー情報を更新します。
- 「**HOST ACTIONS (ホストの操作)**」で、
  - **Host LED (ホスト LED)**: クリック**Host LED: ON (ホスト LED: オン)**、**Host LED: OFF (ホスト LED: オフ)**、または**Host LED: BLINK (ホスト LED: 点滅)**をクリックして LED のステータスを変更します。
  - **Launch BMC Interface (BMC インターフェースの起動)**: クリックして、Lenovo XClarity Controller Web サイトにアクセスします。
  - **Launch Remote Console (リモート・コンソールの起動)**: クリックして、Lenovo XClarity Controller Web サイトのリモート・コンソール・ページにアクセスします。

vSAN ディスク情報の表示

ハードウェア・トポロジー・ページには、実際のサーバー・スロットに取り付け済みのディスクの仮想ビューが表示されます。

図 6. ハードウェア・トポロジー



注：背面バックプレーンを備えるサーバーの場合は「**Front (前面)**」トポロジーと「**Rear (背面)**」トポロジーの両方が表示されます。

ハードウェア・トポロジーは以下を示します。

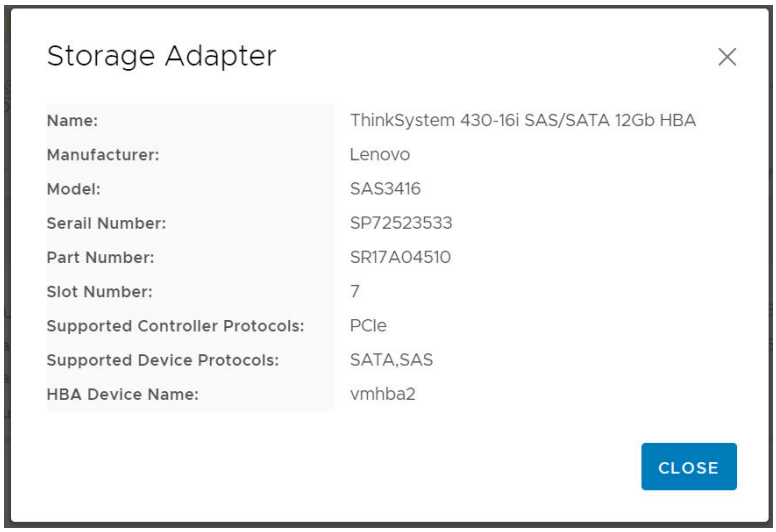
- ディスクの位置: ディスクがインストールされていないスロットが、ドット・ラインで表示されます。
- ディスクのステータス: 色ごとにディスク・ステータスが異なります。
  - 白色: 正常な状態
  - イエロー: 警告状態
  - レッド: クリティカル状態
- ディスク・タイプ: 各スロットの右側に、容量ディスク、キャッシュ・ディスク、非仮想ディスク、未宣言ディスク、および vSAN ダイレクト・ディスクのディスク・タイプ・アイコンが表示されます。

トポロジー上のいずれかのディスクをクリックできます。

- 選択したディスクが vSAN グループに属している場合、同じ vSAN グループ内の他のディスクが黒い実線で強調表示されます。
- 「VIEW ACTIONS (操作の表示)」で、
  - 「Show Icons Legend (アイコンの凡例の表示)」: このオプションには、トポロジー・ビューのディスクのディスク・タイプを表すのに使用するアイコン (キャッシュ・ディスク、容量ディスク、非仮想ディスク、未設定ディスク、vSAN ダイレクト・ディスク、空のベイなど) が表示されます。アイコンの凡例を非表示するには、「Show Icon Legends (アイコンの凡例の表示)」を再度クリック します。
  - 「Show Disk Groups (ディスク・グループの表示)」: このオプションでは、ディスク詳細テーブルに新規の列「Disk Group (ディスク・グループ)」が追加され、ディスクのグループがトポロジー・ビューに表示されます。ディスク・グループを非表示するには、「Show Disk Groups (ディスク・グループの表示)」を再度クリックします。
- 選択したディスクが下の表で強調表示され、「Bay (ベイ)」、「Drive Type (ドライブ・タイプ)」、「Controller (コントローラー)」、「Status (ステータス)」、「Capacity (容量)」、および「Media (メディア)」などの物理ディスクおよび論理ディスクの詳細情報がリストされます。
- トポロジー・ビュー「Disk Group (ディスク・グループ)」リンクをクリックすると、そのディスク・グループに関連付けられているすべてのディスクがディスク・テーブルで強調表示されます。

  注: コントローラー名をクリックすると、詳細が表示されます。

図 7. コントローラー詳細



パワー・サプライ・ユニット (PSU) のヘルス・ステータスの表示

ハードウェア・トポロジー・ページには、サーバーにインストール済みのパワー・サプライ・ユニット (PSU) のヘルス・ステータスの仮想ビューが表示されます。

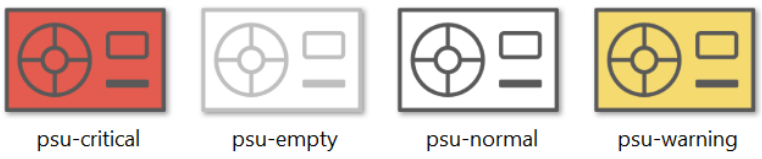


図 8. PSU のヘルス・ステータス

色ごとに以下を含む PSU の異なるヘルス・ステータスを示します。

- レッド: クリティカル状態

- ホワイトとライト・グレーのライン: 空の状態
- ホワイトとダーク・グレーのライン: 正常な状態
- イエロー: 警告状態

vSAN ディスクの削除

ディスク削除オプションを使用すると、ユーザーは vSAN ディスクをディスク・グループから削除し、ディスク・ベイから物理的に取り外すことができます。

注：
- キャッシュ・ディスクを削除する前に、必ずデータをバックアップしてください。そうしないと、動作中の仮想マシンが中断される場合があります。
- vSAN ホストで重複排除と圧縮が有効にされ、キャッシュ・ディスクまたは最後の容量ディスクがディスク・グループから削除されると、ディスク・グループ全体が削除されます。必要に応じて、ディスク・グループを手動で再作成する必要があります。
- 物理ディスクがベイから取り外されると、ディスクはドット・ラインで示され、そのステータスは空になります。

手順

ステップ 1. ハードウェア・トポロジー・ページで、トポロジー・ビューからターゲット・ディスクを選択します。

ステップ 2. 右側のペインの「**DISK ACTIONS (ディスク操作)**」 → 「**Remove Disk (ディスクの削除)**」をクリックします。「Remove Disk (ディスクの削除)」ウィザードが表示されます。

ステップ 3. 検証ページでは、選択したディスクが強調表示され、関連情報が表示されます。

ステップ 4. 「**NEXT (次へ)**」をクリックします。データの移行ページが表示されます。

ステップ 5. データの移行ページの「**vSAN Data Migration (vSAN データ移行)**」ドロップダウン・リストから、以下のいずれかの希望するモードを選択してディスク・データを移行します。

表 9. vSAN データ移行オプション

オプション	サポートされる機能		
	事前チェック	同じクラスター内の他の vSAN ディスクへのデータの移行	ディスク/ディスク・グループの削除
「No data migration (データ移行なし)」	√		√
「Ensure accessibility (アクセシビリティーの確認)」	√	√	√
「Full data migration (完全データ移行)」	√	√	√

ステップ 6. 「**DO IT NOW (今、行う)**」をクリックしてディスク・グループからディスクを削除します。

ステップ 7. プロセスが完了したら、「**NEXT (次へ)**」をクリックします。「Remove Disk (ディスクを削除)」ページにリダイレクトされます。

ステップ 8. ディスクの削除ページで、「**Disk LED (ディスク LED)**」または「**Host LED (ホスト LED)**」をクリックして、ディスクまたはホスト上の LED をオン/オフします。リモート・ユーザーは正しいディスクまたはホストを識別することができます。

ステップ 9. 「**FINISH (終了)**」をクリックしてディスクの削除プロセスを完了します。

vSAN ディスクの交換

ディスクの交換オプションを使用すると、選択したディスクをディスク・グループから新しいディスクに物理的に交換することができます。

注：キャッシュ・ディスクまたは最後の容量ディスクを交換した場合、ディスク・グループ全体が再構築されます。キャッシュ・ディスクを交換する前に、必ずデータをバックアップしてください。しないと、動作中の仮想マシンが機能しなくなる場合があります。

手順

ステップ 1. ハードウェア・トポロジー・ページで、トポロジー・ビューからターゲット・ディスクを選択します。

ステップ 2. 右側のペインの「**DISK ACTIONS (ディスク操作)**」 → 「**Replace Disk (ディスクの交換)**」 をクリックします。「Replace Disk (ディスクの交換)」ウィザードが表示されます。

ステップ 3. 検証ページでは、選択したディスクが強調表示され、関連情報が表示されます。

ステップ 4. 「**NEXT (次へ)**」をクリックします。データの移行ページが表示されます。

ステップ 5. データの移行ページの「**vSAN Data Migration (vSAN データ移行)**」ドロップダウン・リストから、以下のいずれかの希望するモードを選択してディスク・データを移行します。

表 10. vSAN データ移行オプション

オプション	サポートされる機能		
	事前チェック	同じクラスター内の他の vSAN ディスクへのデータの移行	ディスク/ディスク・グループの削除
「No data migration (データ移行なし)」	√		√
「Ensure accessibility (アクセシビリティーの確認)」	√	√	√
「Full data migration (完全データ移行)」	√	√	√

ステップ 6. 「**DO IT NOW (今、行う)**」をクリックしてディスク・グループからディスクを削除します。

ステップ 7. プロセスが完了したら、「**NEXT (次へ)**」をクリックします。「Remove Disk (ディスクを削除)」ページにリダイレクトされます。

ステップ 8. 「ディスクの交換」ページで、新しいディスクを同じベイに挿入した後に「**DETECT NEW DISK (新規ディスクの検出)**」をクリックします。このページに新しいディスク情報が表示されます。

ステップ 9. 「**Auto Claim New Disk (新規ディスクの自動要求)**」をオンにし、新しいディスクをディスク・グループに自動的に追加します。

ステップ 10.「**FINISH (終了)**」をクリックしてディスクの交換プロセスを完了します。

クラスター・ハードウェア・トポロジー

クラスター・ハードウェア・トポロジーを使用すると、クラスターのすべてのホストのトポロジーを 1 つの場所で表示できます。

「**Hardware Topology (ハードウェア・トポロジー)**」ページにアクセスするには、以下を行います。

1. vCenter ホストのインベントリー・ツリーからクラスターを選択し、右側のペインで「**Monitor (モニター)**」タブをクリックします。

2. 「Lenovo XClarity」で「Hardware Topology (ハードウェア・トポロジー)」をクリックします。
「Hardware Topology (ハードウェア・トポロジー)」ビュー・ページが表示されます。ユーザーは、クラスターに関する一般情報を表示できます。

一般情報

「Hardware Topology (ハードウェア・トポロジー)」で、ユーザーはテーブル内のホストに関するハードウェア全体の正常性情報を表示できます。

- Total (合計): ホスト、ディスク、またはディスク・グループの数を表示します。
- Normal (正常) : 正常な状態のホスト、ディスク、またはディスク・グループの数を表示します。
- Warning (警告) : 警告状態のホスト、ディスク、またはディスク・グループの数を表示します。
- Critical (クリティカル) : クリティカルな状態のホスト、ディスク、またはディスク・グループの数を表示します。

操作

以下の操作がサポートされています。

- ホストを検索するには、右上の検索ボックスにホスト名または IP アドレスを入力し、「Enter」キーを押します。
- クラスターの下のホストの情報を表示するには、「Total (合計)」/「Normal (正常)」/「Warning (警告)」/「Critical (クリティカル)」列の任意の番号をクリックして、各ホストのトポロジーを展開します。
- 各ホストの詳細を表示するには、各ホスト・トポロジーの右側にある「HOST DETAILS (ホストの詳細)」をクリックします。ユーザーは、「Host Topology (ホスト・トポロジー)」ページにリダイレクトされます。
- 詳細インベントリーを表示したり、写真を参照したり、ハードウェア・トポロジーを更新したりするには「VIEW ACTIONS (操作の表示)」をクリックします。詳しくは、27 ページの 「操作」 を参照してください。
- LED ステータスを変更するには、BMC インターフェースを起動するか、リモート・コンソールを起動して「HOST ACTIONS (ホストの操作)」をクリックします。詳しくは、27 ページの 「操作」 を参照してください。

BMC Web インターフェースの起動

Lenovo XClarity Integrator で特定のサーバーのベースボード管理コントローラー (BMC) Web インターフェースを起動できます。

手順

サーバーの BMC インターフェースを起動するには、以下の手順を実行します。

ステップ 1. インベントリー・ツリーから vCenter ホストを右クリックします。
「Actions (操作)」ドロップダウン・リスト・ボックスが表示されます。

ステップ 2. 「Lenovo XClarity」 ➡ 「Launch BMC Interface (BMC インターフェースの起動)」をクリックします。
確認ダイアログ・ボックスが表示されます。

ステップ 3. 「OK」をクリックします。
サーバーの BMC Web インターフェースが表示されます。

ステップ 4. BMC 資格情報を使用して BMC インターフェースにログインします。

リモート・コンソールの起動

管理対象サーバーのリモート制御セッションを開始し、ローカル・コンソールのように、サーバーの電源オン/オフやローカルまたはリモート・ドライブの論理マウントなどの操作をこのサーバーで実行できます。

手順

管理対象サーバーのリモート・コンソールを起動するには、以下の手順を実行します。

ステップ 1. インベントリー・ツリーから vCenter ホストを右クリックします。
「**Actions (操作)**」ドロップダウン・リスト・ボックスが表示されます。

ステップ 2. 「**Lenovo XClarity**」 ➡ 「**Launch Remote Console (リモート・コンソールの起動)**」をクリックします。
確認ダイアログ・ボックスが表示されます。

ステップ 3. 「**OK**」をクリックして、Web ブラウザーで表示されるセキュリティー警告を許可します。
サーバーのリモート制御セッションが開始されます。

ファームウェア更新機能の操作

「 Firmware Updates (ファームウェア更新)」機能は、UpdateXpress System Pack (UXSP) または、個別のファームウェア更新を取得して、現在起動している ESXi サーバーにデプロイします。

単一の ESXi サーバーの更新は、ローリング・システム更新機能を使用したサーバーの更新に似ています。唯一の違いとして、更新タスクが作成されている際は、現在の ESXi が表示され、選択できることが挙げられます。設定の更新および更新タスクの管理方法について詳しくは、41 ページの「ローリング・システム更新機能の操作」 を参照してください。

電源ポリシー機能の操作

「Power Policy (電源ポリシー)」機能を使用すると、ファームウェアが電源キャッピング設定をサポートして有効になっている場合は、電力削減と冷却がシステムでサポートされます。この機能は、データセンターのインフラストラクチャーのコスト軽減や、既存のインフラストラクチャーへのサーバー増設の検討に役立ちます。

電源キャッピングの値は、ファームウェアによってキャップされるラックまたはブレード・サーバーに対して設定する値です。電源キャッピング値は、ラックとブレード・サーバーの両方ですべての電源サイクルに対して不変です。電源キャッピング値が設定されている場合、システム電力消費量は定義された値を超えません。

電源キャッピングがサポートされていてサーバーで有効になっている場合、サーバーの最小および最大電源キャッピング値を Lenovo XClarity Integrator が取得し、サーバーの電力消費量範囲として表示できます。以下の例では、最小値が 0 で最大値が 750 です。

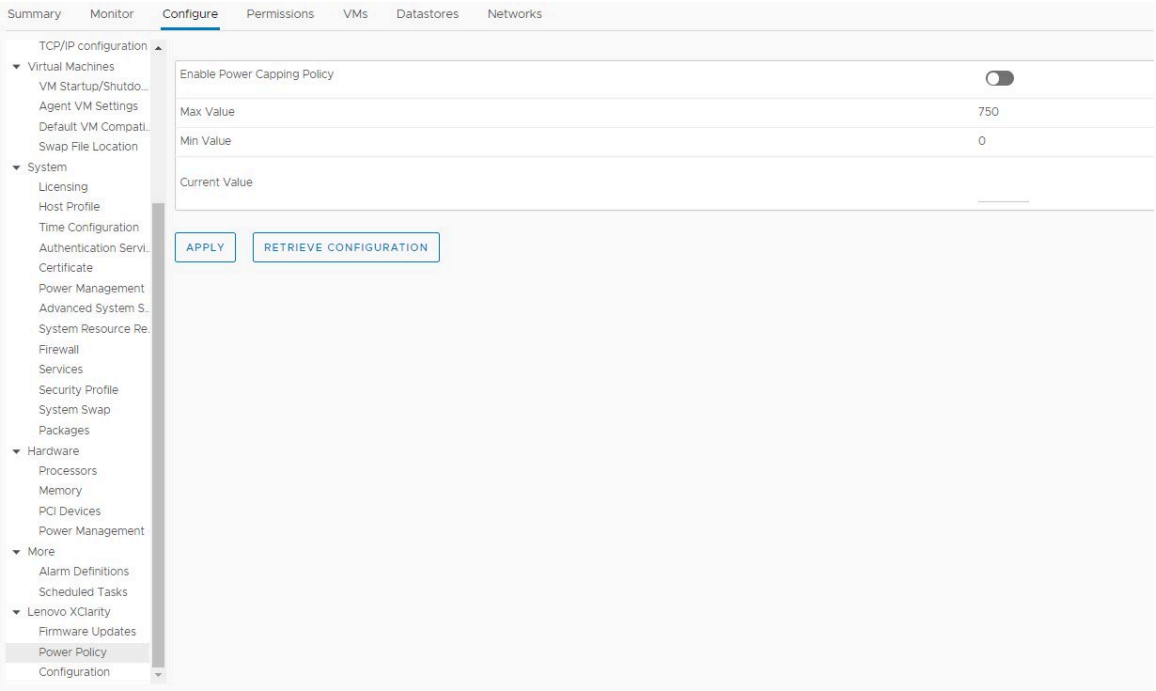


図 9. 「Power Policy (電源ポリシー)」構成ページ

システム設定機能の操作

「System settings (システム設定)」機能を使用すると、ホストのシステム設定の管理をサポートします。Lenovo XClarity Administrator がサーバーを管理しており、Lenovo XClarity Administrator が Lenovo XClarity Integrator に登録されている場合、ユーザーは、構成パターンをホストにデプロイできます。その他の場合は、ブート・オプションとホストのシステム設定のみを表示できます。

サーバーへの構成パターンのデプロイ

Lenovo XClarity Administrator を Lenovo XClarity Integrator に登録したら、Lenovo XClarity Administrator で管理されている各サポート済みサーバーで構成パターンをデプロイまたは非アクティブ化できます。サーバー・パターンは、事前 OS サーバー構成を表します。これには、ローカル・ストレージ構成、I/O アダプター構成、ブート設定、その他の BMC および UEFI ファームウェア設定が含まれます。サーバー・パターンは、複数のサーバーを同時にすばやく構成するための全体的なパターンとして使用されます。

このタスクについて

Lenovo XClarity Administrator に事前定義済みパターンがない場合は、リンクをクリックして Lenovo XClarity Administrator を開き、サーバー・パターンを作成できます。このタスクは「**Configuration Pattern (構成パターン)**」ページで実行します。

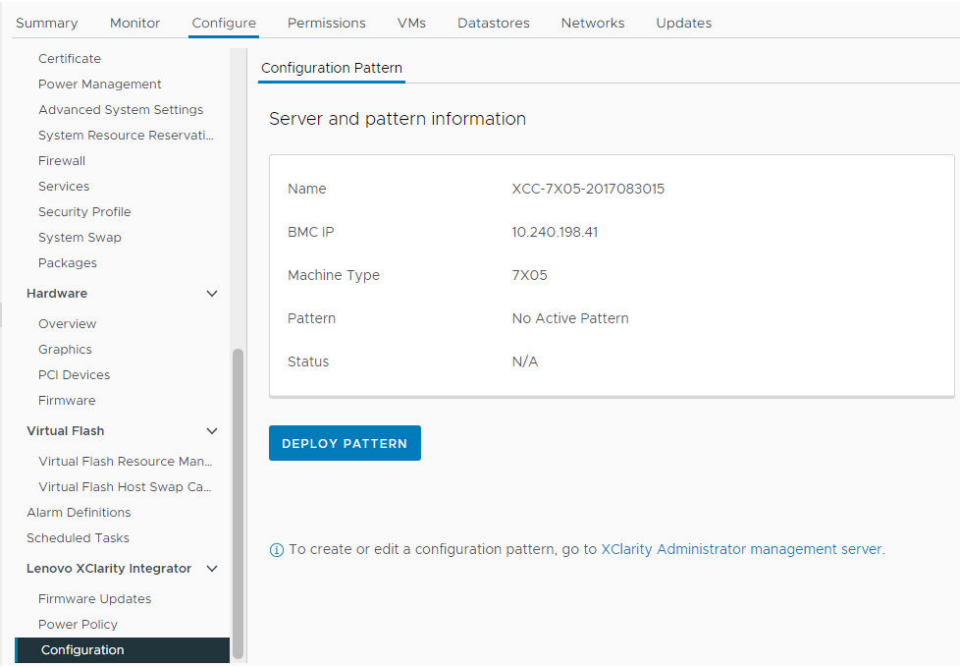


図 10. 「Configuration Pattern (構成パターン)」ページ

手順

ステップ 1. 目的のホストを選択し、「**Configure (構成する)**」 ➔ 「**Lenovo XClarity Integrator**」 ➔ 「**Configuration (構成)**」の順に選択します。

ステップ 2. 「**Configuration Pattern (構成パターン)**」ページで、構成パターンを選択します。
- **デプロイ・パターン**。選択済みパターンをターゲット・サーバーにデプロイします。
- **非アクティブ化パターン**。パターンをターゲット・サーバーから非アクティブ化します。

ステップ 3. 「**Deploy Pattern (パターンのデプロイ)**」ページのドロップダウン・リストでターゲット・パターンを選択し、「**Next (次へ)**」をクリックします。

ステップ 4. 「**Confirm Action (操作の確認)**」ページで、アクティベーション・タイムを選択し「**DONE (完了)**」をクリックします。

注：
- **即時アクティベーション**。パターンをデプロイし、サーバーを再起動して、即時に変更を有効にます。
- **遅延アクティベーション**。パターンをデプロイしますが、サーバーを再起動しません。変更は次の再起動で有効になります。
- サーバー構成によっては、デプロイメント・プロセスに約 30 分かかる場合があります。
- 始動パスワードまたはシステム・ガードにより、サーバーの再起動が停止します。始動パスワードまたはシステム・ガードが有効になっていて、更新中にターゲット・サーバーの再起動が必要な場合、ユーザーはプロンプト・メッセージに従ってアクションを実行する必要があります。

ブート・オプション機能の操作

「**Boot Options (ブート・オプション)**」ペインでは、左から右にオプション・デバイスと現在のブート順序が表示されます。順序を変更するには、「boot order (ブート順序)」オプションを上下に移動するか、2 つの列の間で対応する矢印ボタンをクリックして移動します。

前回の更新日時の日付スタンプが、「**RETRIEVE CONFIGURATION (構成の取得)**」ボタンの右側に表示されます。「**RETRIEVE CONFIGURATION (構成の取得)**」をクリックし、最新のブート・オプション設定値を取得します。変更を加えた場合は、「**Save (保存)**」をクリックして、新しいブート・オプション設定を保存します。

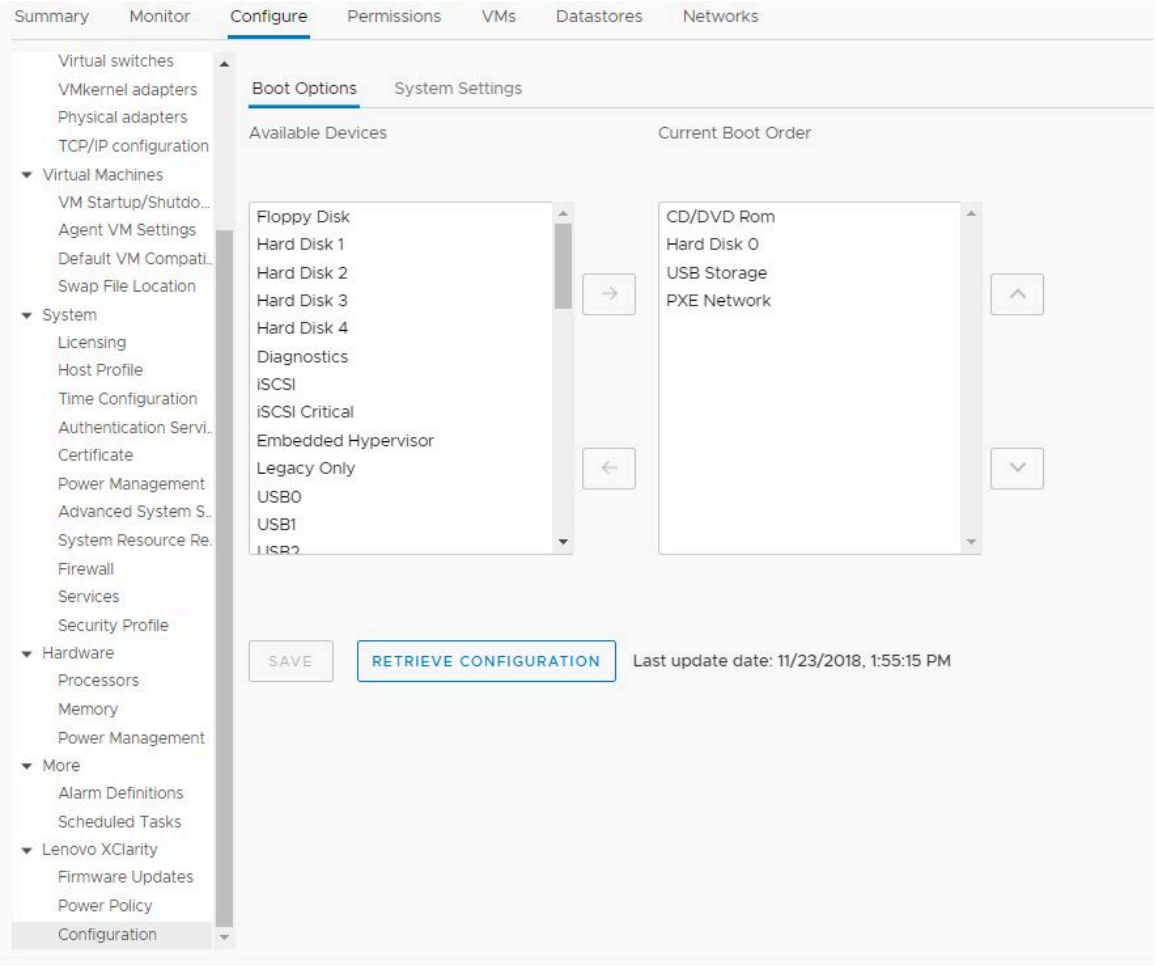


図 11. 「Boot Options (ブート・オプション)」ペイン

システム設定の表示とエクスポート

以下の手順を使用して、ThinkSystem サーバー、Lenovo System x、BladeCenter、または Flex サーバーのシステム設定を表示およびエクスポートできます。

手順

システム設定を表示およびエクスポートするには、以下の手順を実行します。

ステップ 1. 「**Configure (構成)**」ペインで、「**Lenovo XClarity**」の「**Configuration (構成)**」をクリックし、右ペインの「**System Settings (システム設定)**」タブをクリックします。
「**System Settings (システム設定)**」ペインでは、「**EXPORT TO CSV (CSV へのエクスポート)**」ボタンと「**RETRIEVE CONFIGURATION (構成の取得)**」ボタンの下にシステム設定がリストされます。前回の更新日時の日付スタンプが、「**RETRIEVE CONFIGURATION (構成の取得)**」ボタンの右側に表示されます。

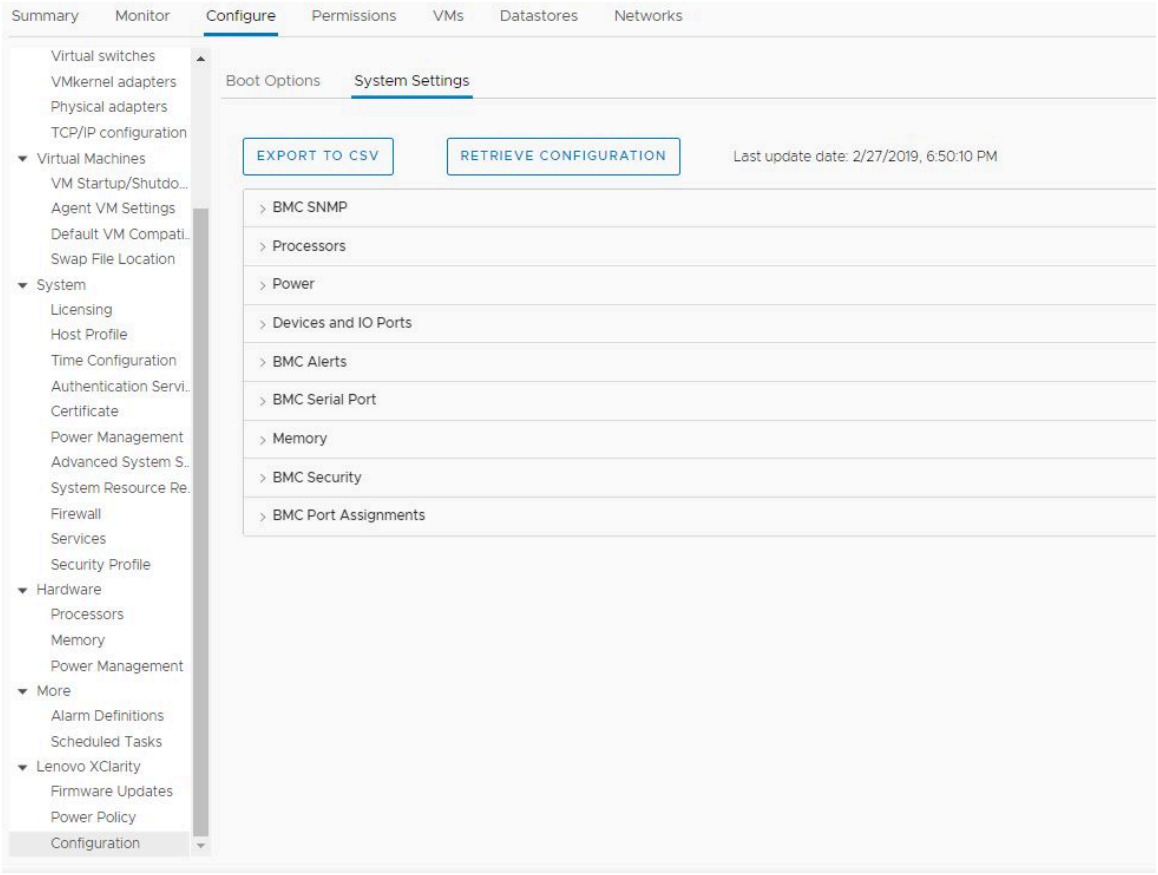


図 12. 「System Settings (システム設定)」ペイン

ステップ 2. 次のいずれかを実行します。

- 最新の設定値を取得するには、「**RETRIEVE CONFIGURATION** (構成の取得)」をクリックします。
- システム設定を CSV ファイルにエクスポートするには、「**EXPORT TO CSV** (CSV へのエクスポート)」をクリックします。

第 6 章　クラスターの管理

このセクションのトピックでは、Lenovo XClarity Integrator を使用したクラスターの管理方法について説明します。

手順

Lenovo XClarity Integrator クラスター管理機能を表示するには、以下の手順を実行します。

ステップ 1. vCenter インベントリー・ツリーからクラスターを選択します。

ステップ 2. 「**Configure** (構成)」タブをクリックします。
左側のナビゲーション・ペインで、必要に応じて「**Lenovo XClarity**」から以下のいずれかの機能を選択します。
- **Rolling Update** (ローリング更新)
- **Rolling Reboot** (ローリング・リブート)

vSphere Lifecycle Manager 機能の使用

ユーザーが単一イメージを使用してクラスターを管理する場合は、vSphere Lifecycle Manager 機能を使用することが推奨されます。

始める前に

LXCI が、vLCM のハードウェア・サポート・マネージャーとして有効になっていることを確認します。vLCM の有効化についての詳細は、10 ページの 「vSphere Lifecycle Manager の有効化/無効化」を参照してください。

ベース ESXi および Lenovo のアドオンのインポート

ESXi バージョンと Lenovo のアドオンを vLCM にインポートできます。

手順

ステップ 1. 「**Menu** (メニュー)」ドロップダウン・リストから「**Lifecycle Manager**」を選択します。
「**Lifecycle Manager**」ページが表示されます。

ステップ 2. 「**Lifecycle Manager**」ページで、「**ACTIONS (アクション)**」ドロップダウン・リストから次のいずれかを選択します。
- 「**Sync Updates** (更新を同期する)」を選択すると、オンライン vSphere Lifecycle Manager デポから標準の ESXi および Lenovo のカスタマイズ・アドオンが自動的にダウンロードされます。
- Lenovoカスタム ESXi イメージをデポに手動でインポートする場合は、「**Import Update** (更新のインポート)」を選択します。Lenovo カスタム ESXi イメージは、https://vmware.lenovo.com/content/custom_iso からダウンロードできます。

注：「**Image Depot (イメージ・デポ)**」領域では、ESXi バージョン/ベンダー・アドオン/コンポーネントを選択しても、右側のペインで詳細情報を表示できます。

ファームウェア・パッケージの管理

vSphere Client でファームウェア・パッケージを管理できます。

手順

ステップ 1. 「**Menu (メニュー)**」ドロップダウン・リストから「**Lenovo XClarity Integrator**」を選択し、左ペインで「**Manage Firmware Packages (ファームウェア・パッケージの管理)**」をクリックします。

ステップ 2. 右側のペインで、以下の 1 つ以上の操作を実行します。

- ファームウェアをダウングレードするには、「**Permit Downgrade (ダウングレードの許可)**」を有効にします。
- ホストにインストールされているバージョンが vLCM イメージで定義されたバージョンより新しいファームウェアのダウングレードを停止するには、「**Permit Downgrade (ダウングレードの許可)**」を無効にします。
- ファームウェアをステージにしたり、vLCM 操作でファームウェアをステージにスキップしたりするには、「**Stage Firmware (ファームウェアのステージング)**」を有効または無効にします。

  注：この機能は、ThinkSystem V3 および ThinkAgile V3 サーバーのみでサポートされています。
- 手動でファームウェア・パッケージをインポートするには、「**IMPORT (インポート)**」をクリックします。「Import Firmware Package (ファームウェア・パッケージのインポート)」ウィンドウが表示されます。
  1. 「**Remote repository (リモート・リポジトリー)**」ページで、URL、ユーザー名、およびパスワードを入力し、「**NEXT (次へ)**」をクリックします。
  2. 「**Firmware package (ファームウェア・パッケージ)**」ページで、ファームウェア・パッケージを選択し、「**FINISH (終了)**」をクリックします。
- 必要なファームウェア・パッケージをダウンロードするには、リストからターゲット・ファームウェア・パッケージを選択し、「**DOWNLOAD (ダウンロード)**」をクリックします。
- ファームウェア・パッケージをコピーするには、必要なファームウェア・パッケージを選択して、「**COPY (コピー)**」をクリックします。
- ファームウェア・パッケージをカスタマイズするには、必要なファームウェア・パッケージを選択して、「**EDIT (編集)**」をクリックします。「Edit Firmware Packages (ファームウェア・パッケージを編集)」ウィンドウが表示されます。

  注：
  – コピーされたファームウェア・パッケージのみ編集できます。
  – 交換したファームウェア・パッケージが Lenovo によって検証されない場合があります。その結果、更新が失敗する可能性があります。そのため、ファームウェア・パッケージの編集は推奨されません。
  1. ターゲット・ファームウェア・パッケージを選択し、「**REPLACE (交換)**」をクリックします。「Replace Firmware (ファームウェアの交換)」ウィンドウが表示されます。
  2. 「**Remote repository (リモート・リポジトリー)**」ページで、URL、ユーザー名、およびパスワードを入力し、「**NEXT (次へ)**」をクリックします。

     注：URL は、インポートする CHG/TXT/UXZ/XML ファームウェア・ファイルが含まれている共有フォルダの URL である必要があります。
  3. 「**Firmware (ファームウェア)**」ページで、インポートするファームウェア・パッケージを選択し、「**FINISH (終了)**」をクリックします。「**Edit Firmware Packages (ファームウェア・パッケージを編集)**」ページが表示されます。
  4. 「**Edit Firmware Packages (ファームウェア・パッケージを編集)**」ページで、次の 1 つ以上の操作を実行します。
     – 交換プロセスを終了するには、「**APPLY (適用)**」 ➡ 「**CONFIRM (確認)**」の順に選択します。
     – ファームウェア・パッケージを削除するには、「**REMOVE (削除)**」 ➡ 「**APPLY (適用)**」 ➡ 「**CONFIRM (確認)**」の順に選択します。
- ファームウェア・パッケージを削除するには、ターゲット・ファームウェア・パッケージを選択して、「**DELETE (削除)**」をクリックします。

- ファームウェア・パッケージ・リストをインポートするには、「**IMPORT LIST (リストをインポート)**」をクリックし、URL をクリックして、Lenovo Web サイトからダウンロードし、「**Choose File (ファイルの選択)**」をクリックして、ファイルをインポートし、「**IMPORT (インポート)**」をクリックします。

  注：LXCI がインターネットから切断されている場合は、このオプションを使用します。
- ファームウェア・パッケージ・リストを最新表示するには、「**REFRESH LIST (リストを最新表示)**」をクリックします。

  注：LXCI がインターネットにアクセスする場合は、このオプションを使用します。

イメージを使用したクラスターの管理

ユーザーは、イメージを使用してクラスターを管理できます。

手順

ステップ 1. 「**Menu (メニュー)**」ドロップダウン・リストから「**Hosts and Clusters (ホストおよびクラスター)**」を選択します。

ステップ 2. 左ペインで必要なクラスターを選択し、vLCM ページで「**Updates (更新)**」 → 「**Image (イメージ)**」をクリックします。

クラスター・イメージの作成

サーバーのクラスター・イメージを作成できます。

手順

ステップ 1. 「**Image (イメージ)**」領域で、「**EDIT (編集)**」をクリックし、次のいずれかの操作を行います。
- 「**ESXi Version (ESXi バージョン)**」フィールドで、ドロップダウン・リストから ESXi バージョンを選択します。
- 「**Vendor Addon (ベンダーのアドオン)**」フィールドで、「**SELECT (選択)**」をクリックして ESXi の Lenovo アドオンを選択します。
- 「**Firmware and Drivers Addon (ファームウェアおよびドライバーのアドオン)**」フィールドで、 をクリックして「**Select the hardware support manager (ハードウェア・サポート・マネージャーの選択)**」ドロップダウン・リストから「**Lenovo XClarity Integrator**」を選択し、「**Select a firmware and driver addon (ファームウェアとドライバーの選択)**」テーブルでファームウェアおよびドライバーのアドオンを選択します。

  注：vCenter でプロキシーを設定する場合、ユーザーはプロキシーを無効にするか、プロキシー構成で vCenter から Lenovo XClarity Integrator (プロトコル HTTPS、ポート 443) への接続を許可する必要があります。そうしないと、ファームウェアおよびドライバー・アドオンのリストが表示されません。
- 「**Components (コンポーネント)**」フィールドで、「**Show details (詳細を表示)**」をクリックしてコンポーネントを追加します。

ステップ 2. イメージの編集後以下のいずれかを実行します。
- 「**SAVE (保存)**」をクリックして、変更内容を保存します。
- 「**VALIDATE (検証)**」をクリックして、ESXi およびファームウェア・アドオンの Lenovo アドオンのコンプライアンスを確認します。
- 「**CANCEL (キャンセル)**」をクリックして、変更内容を破棄します。

ハードウェア互換性のチェック

ファームウェアを修復する前に、vSAN クラスターのハードウェア互換性を確認します。この関数は、イメージに表示されたファームウェアとドライバーを、vSAN ハードウェア互換性リスト (HCL) に記載されている Lenovo ハードウェアおよびサポートされているドライバーと比較します。

手順

ステップ 1. 「**Image** (イメージ)」領域で、 ... をクリックし、「**Check hardware compatibility** (ハードウェアの互換性のチェック)」を選択して、クラスターイメージ内のファームウェアおよびドライバーを vSAN ハードウェア互換性リスト (HCL) と比較します。

ステップ 2. 「**See details** (詳細の確認)」をクリックして、「**Compatibility check results** (互換性チェックの結果)」領域に比較結果を表示し、ハードウェア互換性の潜在的な問題を解決します。

クラスター・コンプライアンスの確認

クラスター内の既存のサーバーと構成されたイメージのコンプライアンスを確認できます。

手順

ステップ 1. 「**Image Compliance** (イメージ・コンプライアンス)」領域で、「**CHECK COMPLIANCE** (コンプライアンスの確認)」をクリックして、クラスター内の既存のサーバーと構成されたイメージの ESXi バージョン、ファームウェア、およびドライバーのコンプライアンスを確認します。

ステップ 2. 「**Software compliance** (ソフトウェア・コンプライアンス)」テーブルおよび「**Firmware compliance** (ファームウェア・コンプライアンス)」テーブルでコンプライアンスの結果を確認します。

非適合サーバーの修復

クラスター内の非適合サーバーの ESXi バージョン、ESXi の Lenovo のアドオン、ファームウェア、およびドライバーの修復が可能です。

手順

ステップ 1. 「**RUN PRE-CHECK (事前チェックを実行)**」をクリックして、既存のサーバーのステータスを確認します。

注：始動パスワードまたはシステム・ガードにより、サーバーの再起動が停止します。始動パスワードまたはシステム・ガードが有効になっていて、更新中にターゲット・サーバーの再起動が必要な場合、ユーザーはプロンプト・メッセージに従ってアクションを実行する必要があります。

ステップ 2. 「Pre-check completed (事前確認完了)」ウィンドウの結果を確認し、問題を解決します。

ステップ 3. 1 つまたはすべての非適合サーバーのESXi バージョン、ESXi の Lenovo のアドオン、ファームウェア、およびドライバーを修復するには、いかのいずれかを実行します。

- すべてのサーバーを修復するには、「**REMEDIATE ALL (すべて修復)**」をクリックします。
- 1 つのサーバーを修復するには、ターゲット・サーバーを選択して、「Server (サーバー)」ページで「**Actions (操作)**」 ➡ 「**Remediate (修復)**」の順に選択します。

ダウングレードの許可

ホストにインストールされているファームウェアのバージョンが vLCM イメージで定義されているバージョンより新しい場合、ユーザーはクラスター内のファームウェアをダウングレードできます。

手順

ステップ 1. 「Manage Firmware Packages (ファームウェア・パッケージの管理)」ページで、「**Permit Downgrade (ダウングレードの許可)**」を有効にします。「37 ページの 「ファームウェア・パッケージの管理」」を参照してください。

ステップ 2. vLCM 操作を実行します。

ステージング・ファームウェア

ユーザーは、クラスター下の非適合サーバーのファームウェアをステージ出来ます。

注：この機能は、ESXi バージョンが v8.0 以降の ThinkSystem V3 および ThinkAgile V3 サーバーでのみサポートされます。

手順

ステップ 1. 「Manage Firmware Packages (ファームウェア・パッケージの管理)」ページで、「**Stage Firmware (ファームウェアのステージング)**」を有効にします。「37 ページの「ファームウェア・パッケージの管理」」を参照してください。

ステップ 2. 「**STAGE ALL (すべてステージ)**」または「**ACTIONS (操作)**」 ➡ 「**Stage (ステージ)**」の順に選択し、ファームウェアをステージします。

ステップ 3. (オプション) 非適合サーバーを修復します。40 ページの「非適合サーバーの修復」を参照してください。

事前対応ハードウェア管理機能の使用

vSphere 8.0u3 で導入された事前対応ハードウェア管理 (PHM) は、vSAN で読み取り/書き込みの問題が発生する前に、障害が発生したディスク・ドライブで通知する機能です。そのため、ディスク正常性の問題が発生した場合に VMware および Lenovo からの推奨事項をユーザーが把握できます。

始める前に

- LXCI が、PHM のハードウェア・サポート・マネージャーとして有効になっていることを確認します。PHM の有効化について詳しくは、11 ページの「事前対応ハードウェア管理の有効化/無効化」を参照してください。
- ディスクが vSAN ディスク・グループに追加されていることを確認します。PHM は vSAN ディスク・グループのディスクでのみ機能します。

正常性情報の表示

LXCI が XCC からサポートされている PHM イベントを受信すると、vCenter に通知されます。

ターゲット・クラスターの正常性情報を表示するには、以下を実行します。

手順

ステップ 1. vSAN クラスターを選択し、**Monitor (監視)** ➡ **vSAN** ➡ **Skyline Health (スカイライン・ヘルス)** をクリックします。「Skyline Health (スカイライン・ヘルス)」ページが表示されます。

ステップ 2. 「Skyline Health (スカイライン・ヘルス)」ページで、スクロールダウンして「**Storage Vendor Reported Drive Health (ストレージ・ベンダーが報告したドライブの正常性)**」領域を見つけ、「**TROUBLESHOOT (トラブルシューティング)**」をクリックして、以下の 1 つ以上を実行します。

- イベントの詳細と推奨事項を確認するには、「**TROUBLESHOOT (トラブルシューティング)**」タブを選択します。
- イベントの履歴を確認するには、「**HISTORY DETAILS (履歴の詳細)**」タブを選択します。

ローリング・システム更新機能の操作

ローリング・システム更新 (RSU) は、ファームウェア更新の無停止アプローチを提供します。RSU は定義された VMware クラスター内で動的仮想マシン移動を利用する「ローリング」更新を調整し、更新プロセス全体 (ホストで実行されているアプリケーション・サービスの中断なしの ESXi ホストの自動再起動を含む) を完了することで、ファームウェアを完全に管理します。

vSphere Lifecycle Manager を一部のシナリオで使用できない場合は、「Rolling System Update (ローリング・システム更新)」機能を使用してファームウェアを更新します。たとえば、クラスターが単一イメージで管理されていないか、またはユーザーは、vLCM のファームウェア・パッケージにない、一部のファームウェアをアップグレードすることを意図しています。

vLCM を使用したファームウェア更新については、「37 ページの 「vSphere Lifecycle Manager 機能の使用」」を参照してください。

始める前に

- サポートされるサーバーには以下のものがあります。
  - ThinkServer サーバー
  - ThinkAgile HX シリーズ・サーバー
- VMware vCenter DRS が有効で、完全自動化モードで実行されていることを確認します。
- ポート 6990 が使用可能であることを確認します。

ローリング・システム更新設定の構成

「Preferences (設定)」ペインで、ファームウェア更新の更新リポジトリーおよびダウンロード設定を構成できます。

更新リポジトリーの場所の指定

「**Update without Policy (ポリシーのない更新)**」タイプのタスクを作成するときに、「ローリング・システム更新」機能がファームウェア更新を確認する更新リポジトリーを構成できます。

手順

ステップ 1. 左側のナビゲーション・ペインで、「**Lenovo XClarity Integrator**」の「**Rolling Update (ローリング更新)**」をクリックします。次に、右ペインの「**Preferences** (設定)」をクリックします。

ステップ 2. 「Preferences (設定)」ペインで、次のいずれかの方法でファームウェア・リポジトリーの場所を指定します。

- デフォルトでは、Lenovo XClarity Integrator アプライアンス・サーバーの内部ディレクトリはファームウェア・リポジトリーとして使用され、「**Download metadata from Lenovo website** (Lenovo Web サイトからメタデータをダウンロード)」は有効になっています。
- 外部フォルダーをファームウェア・ーとして使用する場合は、「**Repository folder (リポジトリー・フォルダー)**」セクションで「**EDIT (編集)**」をクリックします。
  1. 「**リポジトリー設定 (Repository Settings)**」ページで、「**リモート・リポジトリーを使用 (Use Remote Repository)**」を選択します。
  2. リポジトリーの URL を *\\<IP_address>\<repository_path>* 形式で入力し、必要に応じてユーザー名とパスワードを入力します。
  3. 「**OK**」をクリックして、変更内容を保存します

  注：
  - IPv6 アドレスを使用するホストでのリポジトリーをセットアップする場合は、完全修飾ドメイン・ネーム (FQDN) を使用してネットワーク・アドレスを指定する必要があります。
  - 共有フォルダーの書き込み権限が付与されている必要があります。
  - LXCI は、ネットワーク上の以下のタイプの外部フォルダーをサポートしています。
    - Windows サーバー上の共有フォルダー
    - Linux Samba ファイル・サーバー上の共有フォルダー (NTLM セキュリティー・モード)

ステップ 3. 「**Download metadata from the Lenovo website (メタデータを Lenovo Web サイトからダウンロード)**」の右にある「**EDIT (編集)**」をクリックして、更新パッケージのダウンロード設定を構成します。

a. LXCI サーバーからインターネットに直接アクセスできない場合は、「Lenovo XClarity Integrator」のアプライアンス管理ページでインターネット設定を構成します。Web ページにログインした後、左側のペインで「**Network Settings** (ネットワーク設定)」をクリックし、右側のペインで「**Internet settings** (インターネット設定)」をクリックします。次に、プロキシ設定を構成します。

b. 「**Download from website (Web サイトからダウンロード)**」と「**Periodically download (定期的にダウンロード)**」を選択し、更新パッケージを定期的に自動でダウンロードする頻度を設定します。

c. 「**OK**」をクリックします。

ステップ 4. (オプション) ペインの右下にある「**CHECK NOW (今すぐ確認)**」をクリックして、最新の更新パッケージを Lenovo Web サイトからダウンロードします。

注：
- 「CHECK NOW (今すぐ確認)」は、前の手順で「**Download from website** (Web サイトからダウンロード)」が選択されている場合にのみ表示されます。
- 最新のダウンロード時刻が、ペインの右下に表示されます。

ローリング・システム更新タスクの管理

ローリング・システム更新 (RSU)」機能を使用すると、ユーザーはローリング・システム更新タスクを作成および管理できます。RSU タスクには、ローリング・システム更新に必要なすべての情報とオプションが含まれています。

手順

ステップ 1. インベントリー・ツリーから対象のクラスターを選択して「**Configure (構成する)**」タブをクリックします。

ステップ 2. 左側のナビゲーション・ペインで、「**Lenovo XClarity Integrator**」の「**Rolling Update (ローリング更新)**」をクリックします。「**Rolling Update (ローリング更新)**」ページは、右側のペインに表示されます。

タスク表には、RSU タスクに関する次の詳細情報が記載されます。
- タスク名
- タイプ
- 状態
- 作成時刻
- 開始時刻
- 終了時刻

表 11. ローリング・システム更新タスク・ステータス

ターゲット	ステータス	説明
ローリング更新タスク	未スタート	タスクは開始されていません。
	実行中	タスクは実行中です。
	キャンセル済み	タスクはキャンセルされました。
	失敗	ファームウェア・パッケージのダウンロードに失敗した。
	終了	タスクは完了しました。

表 11. ローリング・システム更新タスク・ステータス (続き)

ターゲット	ステータス	説明
ホスト	未スタート	ホストの更新は開始されていません。
	移行中	ホストは保守モードに入りました。
	保守	ホストは保守モードです。
	更新	ホストのファームウェアは更新中です。
	リブート	ホストは更新され、再起動中です。
	保守の終了	ホストの保守モードが終了しました。
	成功	ファームウェア更新が正常に完了しました。
	失敗	ホスト障害の原因: • 更新パッケージを取得できない。 • 保守モードを開始できない。 • ファームウェアを更新できない。 • ホストを再起動できない。 • 保守モードを終了できない。
ファームウェア	未スタート	ファームウェア更新は開始されていません。
	実行中	ファームウェア更新は実行中です。
	成功	ファームウェア更新が正常に完了しました。
	失敗	ファームウェア更新は失敗しました。

ステップ 3. 以下のいずれかのステップを実行します。

表 12. ローリング・システム更新タスク機能

タスク機能	説明
作成	新しい RSU タスクを作成します。
コピー	既存の RSU タスクから新しい RSU タスクを作成します。
編集	開始されていない RSU タスクを編集します。
削除	タスク・リストから RSU タスクを削除します。
キャンセル	実行中の RSU タスクを停止します。
最新表示	RSU リストを最新表示します。

RSU タスクの作成

「**CREATE (作成)**」オプションを使用すると、新しいローリング・システム更新 (RSU) タスクを作成でき、ホストファームウェア更新をスケジュールした期間にスケジュールできます。

手順

ステップ 1. 「**Configure (構成する)**」 → 「**Lenovo XClarity Integrator**」 → 「**Rolling Update (ローリング更新)**」の順に選択し、上部の「**Rolling Update (ローリング更新)**」タブをクリックします。

ステップ 2. 「**Rolling Update (ローリング更新)**」ページで、「**CREATE (作成)**」をクリックすると「Create Task (タスクの作成)」ウィザードが起動します。

ステップ 3. 「**Create Task (タスクの作成)**」ページで、タスク名を入力し、以下のタスク・タイプを 1 つ選択したら、「**Next (次へ)**」をクリックします。

- **XClarity Administrator のポリシーで更新**: このオプションを選択すると、サーバーのファームウェアが適合しているかを確認できます。更新の前に、次のことを確認します。
  - ESXi を実行するサーバーが追加されており、Lenovo XClarity Administrator により管理されている。
  - ファームウェア・コンプライアンス・ポリシーが Lenovo XClarity Administrator で作成されている。
  - ファームウェアが Lenovo XClarity Administrator にダウンロードされている。
  - Lenovo XClarity Administrator が Lenovo XClarity Integrator に登録されている。
  - 1 つのサーバーのファームウェアが Lenovo XClarity Administrator の代わりに他の方法で更新される場合は、vCenter で (ポリシーのある) ローリング更新タスクを作成する前に、Lenovo XClarity Administrator のこのサーバーのインベントリー情報を更新することをお勧めします。
- **ポリシーのない更新**: Lenovo XClarity Administrator が利用できない場合は、個別のファームウェア更新または、各サーバーの UXSP を選択します。更新の前に、次のことを確認します。
  - BMC アクセスが許可されます。
  - 更新リポジトリーが構成され、ファームウェアがダウンロードされます (42 ページの「ローリング・システム更新設定の構成」 を参照)。

注：
- 更新の前に、ターゲット・タスク・タイプが要件を満たしていることを確認します。
- 非 ASCII 文字はタスク名に使用できません。

ステップ 4. 「**Select Version (バージョンの選択)**」ページで、マシン・タイプ、ホスト、およびポリシーを選択し、「**Next (次へ)**」をクリックします。

ステップ 5. 「**Task Options (タスク・オプション)**」ページで、次のオプションを 1 つ以上選択するか、切り替え、「**Next (次へ)**」をクリックします。
- 「**Reboot after Update (更新後に再起動)**」: ファームウェアを更新後に OS を再起動するかどうかを指定します。「**Update without a policy (ポリシーのない更新)**」を選択した場合、このオプションは必須です。
- **並列で更新するノード数**: 同時に更新するホスト数を指定します。LXCA メソッドからポリシーを使用して更新する場合、最大数は 16 です。ポリシー方式を使用しない更新の場合、最大数は 8 です。1 つの LXCI インスタンスは、最大で 32 台のホストに対してファームウェアを並列更新します。
- **現在のバージョンより古いファームウェア・バージョンに更新することを許可**: 現在のバージョンより低いファームウェア・バージョンを許可するかどうかを指定します。
- **メモリー・テストの実行**: サーバーの再起動後にファームウェアを更新したら、メモリー・テストを実行します。このオプションは、ThinkSystem SR635、SR645、SR655 および SR665 以外の、サポートされているすべての ThinkSystem サーバーでサポートされます。ユーザーは、LXCI のイベント・ビューでメモリー・テスト結果を確認するか、LXCA のジョブ・ステータスを確認することができます。
- 「**Perform VM Evacuation** (VM 移行の実行)」: ホストを更新する前に仮想マシンを移行するかどうかを指定します。
- **いずれかのノードで障害が発生した場合にタスク全体を停止する**: クラスター内の 1 つのホストの更新ができなかった場合、更新タスク全体を停止するかどうかを指定します。
- **更新を実行する**: 更新の実行時間を選択します。「**Now (今すぐ)**」を選択すると、即時に更新が実行されます。または、スケジュール時刻に更新する場合は、「**Schedule Time (スケジュール時刻)**」に値を設定します。

注：始動パスワードまたはシステム・ガードにより、サーバーの再起動が停止します。始動パスワードまたはシステム・ガードが有効になっていて、更新中にターゲット・サーバーの再起動が必要な場合、ユーザーはプロンプト・メッセージに従ってアクションを実行する必要があります。

ステップ 6. 「**Confirm (確認)**」ページで、情報を確認して、「**FINISH (終了)**」をクリックします。

完了した RSU タスクの複製

「COPY (コピー)」オプションを使用して、「finished (終了)」、「failed (失敗)」、「canceled (キャンセル)」状態のタスクを使用した新しいローリング・システム・更新タスク (RSU) のクローンを作成します。

手順

ステップ 1. 「Configure (構成する)」 ➡ 「Lenovo XClarity Integrator」 ➡ 「Rolling Update (ローリング更新)」の順に選択し、上部の「Rolling Update (ローリング更新)」タブをクリックします。

ステップ 2. 「Rolling Update (ローリング更新)」ページのリストで、終了した RSU タスク、失敗した RSU タスク、キャンセルした RSU タスクを選択します。

ステップ 3. 「COPY (コピー)」をクリックして、「copy task (コピー・タスク)」ウィザードを起動します。

ステップ 4. 元の選択肢を編集して、「FINISH (終了)」をクリックして、新しいタスクを保存します。

開始されていない RSU タスクの編集

「EDIT (編集)」オプションを使用して、開始されていないローリング・システム更新 (RSU) タスクを編集します。

手順

ステップ 1. 「Configure (構成する)」 ➡ 「Lenovo XClarity Integrator」 ➡ 「Rolling Update (ローリング更新)」の順に選択します。

ステップ 2. 開始されていない RSU タスクをリストから選択し、「EDIT (編集)」をクリックして「Create Task (タスクの作成)」ウィザードを起動します。

ステップ 3. タスクを編集し、「FINISH (終了)」をクリックして変更を保存します。

RSU タスクの削除

ローリング・システム更新 (RSU) タスクが現在実行中ではない場合は、「REMOVE (削除)」オプションを使用して、これをタスク・リストから削除します。現在実行中ではないすべての RSU タスクを削除できます。

手順

ステップ 1. 「Configure (構成する)」 ➡ 「Lenovo XClarity Integrator」 ➡ 「Rolling Update (ローリング更新)」の順に選択します。

ステップ 2. リストで、現在実行中ではない RSU タスクを 1 つ以上選択します。

ステップ 3. 「REMOVE (削除)」をクリックします。選択したタスクがタスク・リストから削除されます。

実行中の RSU タスクのキャンセル

「CANCEL (キャンセル)」オプションを使用すると、実行中のローリング・システム更新 (RSU) タスクをキャンセルできます。タスクがキャンセルされると、タスクのステータスが「Canceling (キャンセル中)」に変更されます。

手順

ステップ 1. 「Configure (構成する)」 ➡ 「Lenovo XClarity Integrator」 ➡ 「Rolling Update (ローリング更新)」の順に選択します。

ステップ 2. リストから実行中の RSU タスクを選択します。

ステップ 3. 「CANCEL (キャンセル)」をクリックします。RSU は既に開始されたホストの更新を完了させ、その他のみをキャンセルします。このタスクは、完了までに数分かかります。

RSU タスク・リストの更新

「REFRESH (最新表示)」オプションを使用すると、ローリング・システム更新 (RSU) タスク・リストが最新表示されます。

手順

ステップ 1. 「**Configure (構成する)**」 → 「**Lenovo XClarity Integrator**」 → 「**Rolling Update (ローリング更新)**」の順に選択します。

ステップ 2. 「**REFRESH (最新表示)**」をクリックすると RSU タスク・リストが最新表示されます。

ローリング・システム・リブート機能の操作

ローリング・システム・リブート (RSR) 機能は、システムを実行し続けながら、サーバーを再起動します。その際、動的 VM 移動により実行中のアプリケーション・サービスの中断は発生しません。

始める前に

ローリング・システム・リブート機能を使用するための前提条件を以下に示します。

- サポートされるサーバーには以下のものがあります。
  - ThinkAgile HX シリーズ・サーバー
- VMware vCenter Enterprise または Enterprise Plus Edition と DRS が必要です。
- DRS が有効で、完全自動化モードで実行されている。

ローリング・システム・リブート・タスクの管理

「Rolling System Reboot (RSR) (ローリング・システム・リブート (RSR))」機能は、ローリング再起動タスクを作成および管理をサポートします。RSR タスクには、ローリング再起動に必要なすべての情報とオプションが含まれます。

手順

ステップ 1. インベントリー・ツリーから対象のクラスターを選択して「**Configure (構成する)**」タブをクリックします。

ステップ 2. 左側のナビゲーション・ペインで、「**Lenovo XClarity Integrator**」の「**Rolling Reboot (ローリング・リブート)**」をクリックします。「**Rolling Reboot (ローリング・リブート)**」ページは、右側のペインに表示されます。

タスクの表には、RSR タスクに関する以下の詳細情報があります。

- タスク名
- ステータス
- 進行状況
- 開始時刻
- 終了時刻

ステップ 3. 以下のいずれかのステップを実行します。

表 13. ローリング・システム・リブート・タスク機能

タスク機能	説明
作成	新しい RSR タスクを作成します。
編集	開始されていない RSR タスクを編集します。
コピー	既存の RSR タスクから新しい RSR タスクを作成します。
削除	タスク・リストから RSR タスクを削除します。
キャンセル	実行中の RSR タスクを停止します。

RSR タスクの作成

「**CREATE (作成)**」オプションを使用して、新しいローリング・システム・リブート (RSR) タスクを作成します。クラスターごとに 1 つのアクティブな RSR タスクのみが許可されています。

手順

ステップ 1. 「**Configure (構成する)**」 ➞ 「**Lenovo XClarity Integrator**」 ➞ 「**Rolling Reboot (ローリング・リブート)**」の順に選択します。

ステップ 2. 「**CREATE (作成)**」をクリックして、タスク「CREATE (作成)」ウィザードを起動します。

注：「**CREATE (作成)**」 ボタンは、タスクが、タスク・リストで、「**Finished (終了)**」、「**Canceled (キャンセル)**」、「**Failed (失敗)**」の状態になっているときのみ使用できます。

ステップ 3. 「**Select hosts (ホストの選択)**」ページで、タスク名を入力し、1 つ以上のターゲット・ホストを選択したら、「**Next (次へ)**」をクリックします

ステップ 4. 「**Reboot options (ブート・オプション)**」で、1 つ以上の次のオプションを選択するか、切り替え、「**Next (次へ)**」をクリックします。

- **並列処理**: 同時に再起動できるホスト数を指定します。複数のホストを同時にリブートするには、より多くのシステム・リソースが必要です。この値は、vCenter Server 上の CPU やメモリーなど、クラスターで現在利用可能なシステム・リソースに応じて設定することをお勧めします。デフォルト値は、1 で、最大値は、4 です。
- **エラーで停止**: 1 つのホストに障害が発生した場合に更新を続行するかどうかを指定します。
- **再稼働モード**: このオプションは vSAN クラスターでのみ表示されます。ユーザーは、仮想マシンを移行するときに、廃止モードを指定できます。
- **スケジュール**: タスクを開始する時間を指定します。

注：始動パスワードまたはシステム・ガードにより、サーバーの再起動が停止します。始動パスワードまたはシステム・ガードが有効になっていて、更新中にターゲット・サーバーの再起動が必要な場合、ユーザーはプロンプト・メッセージに従ってアクションを実行する必要があります。

ステップ 5. 「**Summary (要約)**」ページで、情報を確認して、「**FINISH (終了)**」をクリックします。RSR がスケジュールに従ってタスクを開始します。

開始されていない RSR タスクの編集

「**EDIT (編集)**」オプションを使用して、開始されていないローリング・システム・リブート (RSR) タスクを編集します。

手順

ステップ 1. 「**Configure (構成する)**」 ➞ 「**Lenovo XClarity Integrator**」 ➞ 「**Rolling Reboot (ローリング・リブート)**」の順に選択します。

ステップ 2. 開始されていない RSR タスクをリストから選択し、「**EDIT (編集)**」をクリックしてタスクの「CREATE (作成)」ウィザードを起動します。

ステップ 3. タスクを編集し、「**FINISH (終了)**」をクリックして変更を保存します。

完了した RSR タスクの複製

「**COPY (コピー)**」オプションを使用して、「finished (終了)」、「failed (失敗)」、「canceled (キャンセル)」状態のタスクを使用した新しいローリング・システム・リブート・タスク (RSR) のクローンを作成します。

手順

ステップ 1. 「**Configure (構成する)**」 ➞ 「**Lenovo XClarity Integrator**」 ➞ 「**Rolling Reboot (ローリング・リブート)**」の順に選択します。

ステップ 2. リストから完了、失敗、またはキャンセルした RSR タスクを選択します。

ステップ 3. 「**COPY (コピー)**」をクリックして、「copy task (コピー・タスク)」ウィザードを起動します。

ステップ 4. 元の選択肢を編集して、「**FINISH (終了)**」をクリックして、新しいタスクを保存します。

RSR タスクの削除

ローリング・システム・リブート (RSR) タスクが現在実行中ではない場合は、「**DELETE (削除)**」オプションを使用して、これをタスク・リストから削除します。現在実行中ではないすべての RSR タスクを削除できます。

手順

ステップ 1. 「**Configure (構成する)**」 → 「**Lenovo XClarity Integrator**」 → 「**Rolling Reboot (ローリング・リブート)**」の順に選択します。

ステップ 2. リストで、現在実行中でない RSR タスクを 1 つ以上選択します。

ステップ 3. 「**DELETE (削除)**」をクリックします。選択したタスクがタスク・リストから削除されます。

実行中の RSR タスクのキャンセル

「**CANCEL (キャンセル)**」オプションを使用すると、ローリング・システム・リブート (RSR) タスクを実行中にキャンセルできます。タスクがキャンセルされると、タスクのステータスが「Canceling (キャンセル中)」に変更されます。

手順

ステップ 1. 「**Configure (構成する)**」 → 「**Lenovo XClarity Integrator**」 → 「**Rolling Reboot (ローリング・リブート)**」の順に選択します。

ステップ 2. リストから実行中の RSR タスクを選択します。

ステップ 3. 「**CANCEL (キャンセル)**」をクリックします。RSR は既に開始されたホストの更新を完了させ、その他のみをキャンセルします。このタスクは、完了までに数分かかります。

RSR タスク・レポートの表示

ローリング・システム・リブート・レポート・ビューには、タスク・ステータスの詳細情報が表示されます。

手順

「**Configure (構成)**」 → 「**Lenovo XClarity**」 → 「**Rolling Reboot (ローリング・リブート)**」を選択し、「**Status** (ステータス)」列のステータス・リンクをクリックしてローリング・システム・リブート・レポート・ビューを開きます。以下の表に、タスクおよびホストのステータスを示します。ローリング・システム・リブート・タスクについて詳しくは、47 ページの 「ローリング・システム・リブート機能の操作」 を参照してください。

表 14. ローリング・システム・リブート・タスクのステータス

ターゲット	ステータス	説明
ローリング・リブート・タスク	未スタート	タスクは開始されていません。
	実行中	タスクは実行中です。
	キャンセル済み	タスクはキャンセルされました。
	失敗	タスクの失敗の原因: • ファームウェア・パッケージのダウンロードに失敗した。 • ESXi ホストの再起動に失敗した。 • VM の移行に失敗した。 • ファームウェア更新に失敗した
	終了	タスクは完了しました。

表 14. ローリング・システム・リブート・タスクのステータス (続き)

ターゲット	ステータス	説明
ホスト	未スタート	ホストの更新は開始されていません。
	移行中	ホストは保守モードに入りました。
	保守	ホストは保守モードです。
	リブート	ホストは更新され、再起動中です。
	保守の終了	ホストの保守モードが終了しました。
	成功	ファームウェア更新が正常に完了しました。
	失敗	ホスト障害の原因: • 保守モードを開始できない。 • ホストを再起動できない。 • 保守モードを終了できない。

プロアクティブ HA の操作

VMware vSphere v6.5 には新しい Proactive HA 機能が追加されています。これは、元の高可用性 (HA) 機能を拡張したものです。VMware vCenter 対応 Lenovo XClarity Integrator は、Lenovo Proactive HA Provider を VMware vCenter に登録することで Proactive HA 機能をサポートします。

始める前に

- VMware vSphere v6.5 以降がインストールされていることを確認してください。
- Lenovo XClarity Integrator が VMware vCenter に正常に登録されていることを確認してください。

クラスタ用の Lenovo Proactive HA Provider を使用した VMware vCenter Proactive HA の有効化

始める前に

クラスターが空のクラスターでない場合は、クラスター内の各ホストに対して BMC アクセスを要求していることを確認してください。要求しないと、Lenovo Proactive HA Provider が正しく表示されない場合があります。

BMC アクセス権を持つ同じホストを削除して追加し直した場合は、ユーザー・インターフェースでホストが BMC にアクセスできることを示している場合でも、BMC アクセスを再度要求する必要があります。要求しないと、Lenovo Proactive HA Provider が正しく表示されない場合があります。

手順

ステップ 1. vSphere Client で、構成するクラスターをクリックします。

ステップ 2. 「**Configure (構成)**」 ➡ 「**vSphere Availability (vSphere の可用性)**」を選択してから、ページ右側の「**Edit (編集)**」をクリックします。構成ダイアログが表示されます。

ステップ 3. 「**vSphere DRS**」で「**Turn ON vSphere DRS**」を選択します。

ステップ 4. 「**vSphere Availability** (vSphere の可用性)」で「**Turn ON Proactive HA** (Proactive HA をオンにする)」を選択します。

ステップ 5. 「**Proactive HA Failures and Responses**」で、「**Automation Level**」を「`Automated`」に設定し、「**Remediation** (修復)」を「`Mixed Mode`」または「`Maintenance Mode`」に設定します。

ステップ 6. Proactive HA Provider のリストで、「**com.lenovo.HealthUpdateProvider_ver100**」プロバイダーを選択します。

ステップ 7. オプション: ダイアログの右側にある「**Edit (編集)**」をクリックして、特定のホストまたはクラスター全体の特定の障害状態を無視するように選択します。障害条件を無視するためのイベントとホストを選択できる別のダイアログが表示されます。詳しくは、「VMware vSphere ユーザーズ・ガイド」を参照してください。

注：VMware によると、他の自動化レベルと修復設定を使用できますが、いくつかの制限があります。たとえば、「手動」および「検疫」モードを使用する場合、ホストには、少なくとも 1 つの VM が必要です。そうでない場合、インバウンドの正常性イベントを受信しません。

事前対応型 HA 対応（Lenovo Provider を使用）クラスタへのホストの追加

手順

ステップ 1. ホストを DataCenter またはその他の Proactive HA 非対応クラスターに追加します。

ステップ 2. ホストの BMC アクセスを要求します (15 ページの 「BMC の検出と管理」 を参照)。

ステップ 3. ホストを Proactive HA 対応クラスターに移動します。

注：BMC アクセス権を持つ同じホストを削除して追加し直した場合は、ユーザー・インターフェースでホストが BMC にアクセスできることを示している場合でも、BMC アクセスを再度要求する必要があります。要求しないと、ホストが、Proactive HA 対応クラスターを削除できない場合があります。

Lenovo Proactive HA Provider の再利用

ウィザードまたは「Administration (管理)」ページで Lenovo XClarity Integrator を VMware vCenter に登録すると、Lenovo Proactive HA Provider が VMware vCenter に自動登録されます。VMware vCenter から Lenovo XClarity Integrator の登録解除をすると、Proactive HA Provider の登録を解除するかどうかを確認するウィンドウが表示されます。通常は、プロバイダーを VMware vCenter に保持すると、次回 Lenovo XClarity Integrator を VMware vCenter に登録する際に再利用するように設定できるように、プロバイダー設定を VMware vCenter で保持します。

事前対応型 HA ハートビート

事前対応型 HAが正しく機能するように、Lenovo XClarity Integrator は VMware vCenter でハートビートを必要とします。「Provider com.lenovo.HealthUpdateProvider_ver101 has not posted an update in 300 seconds (300 秒間、Provider com.lenovo.HealthUpdateProvider_ver101 更新をポストしていません)」というメッセージが Proactive HA 対応クラスターのイベント・リストで表示されない場合、いくつかの理由により、ハートビートが機能していない場合があります。ネットワークをチェックして、Lenovo XClarity Integrator が VMware vCenter と正しく通信しているかどうか、および Lenovo XClarity Integrator アプライアンスが使用可能かどうかを確認してください。問題が解決しない場合は、Lenovo XClarity Integrator を再起動します。

ハードウェア・イベントの管理

ハードウェア・イベントおよびアラームは、vCenter に統合されます。VMware vCenter 対応 Lenovo XClarity Integrator は、アウト・オブ・バンド (OOB) BMC ノードから vCenter サーバーにイベントをロードし、管理者は、それらを vSphere Client から表示および管理できます。これにより、管理者は管理対象環境内のすべてのホスト・システム・イベントを異機種混合で一元表示できます。

次に行うこと

vSphere Client の「**Events (イベント)**」タブを選択して、Lenovo ハードウェア・イベントを表示します。

アラーム

Lenovo イベントが VMware vCenter Server に送信されると、ホスト全体のステータスが対応するイベント重大度を基にして変更されます。ホスト・ステータスの変更が管理者によって割り当てられた条件を満たすと、アラームが起動されます。

アラームが発生すると、vSphere Client タブの上にあるバー沿いの vSphere Client ウィンドウの右側、またはインベントリー・ツリーのホスト・アイコンの上にアイコンが表示されます。

「Alarms (アラーム)」タブに格納されているすべてのアラームのリストを表示するには、アラーム・アイコンをクリックします。

第 7 章 Lenovo XClarity Integrator の管理

この章では、VMware vCenter 対応 Lenovo XClarity Integrator 管理者 Web ページを使用してサービス・データの収集、プラグインの登録、アプライアンス構成のバックアップと修復を行う方法について説明します。

vCenter 接続の構成

VMware vCenter 対応 Lenovo XClarity Integrator が最初にデプロイされるとき、Lenovo XClarity Integrator が vCenter サーバーに登録されます。VMware vCenter の Lenovo XClarity Integrator は、追加の vCenter サーバーから登録できます。VMware vCenter の Lenovo XClarity Integrator は、vCenter サーバーから登録抹消することもできます。

Lenovo XClarity Integrator の vCenter サーバーへの登録

Lenovo XClarity Integrator をリンク・モードの 1 台の vCenter サーバーまたは複数の vCenter サーバーに登録できます。

始める前に

vCenter サーバーに Lenovo XClarity Integrator を登録するための vCenter ユーザー名とパスワードを準備します。vCenter ユーザーは、セキュリティ権限の低い vCenter 管理者または専用のサービス・ユーザーになることができます。専用のサービス・ユーザーを使用する場合は、以下の権限が必要です。

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

注：これらの権限は、登録時に vCenter ユーザーに手動または自動で付与することができます。

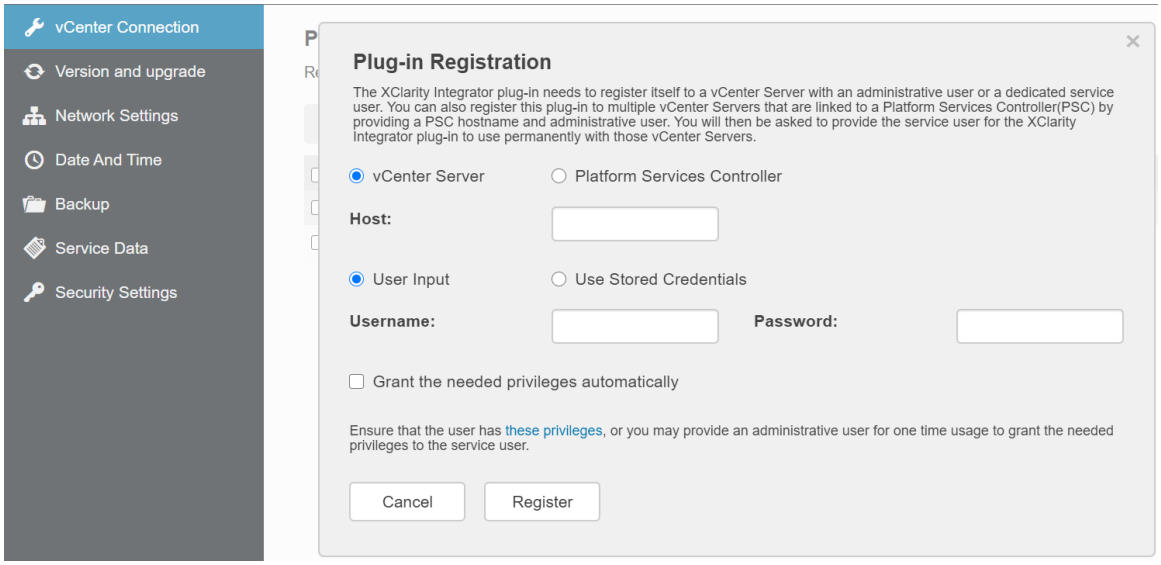
1 台の vCenter サーバーへの LXCI の登録

Lenovo XClarity Integrator は vCenter サーバーまたは複数の vCenter サーバーに個別に登録できます。

手順

Lenovo XClarity Integrator を vCenter サーバーに登録するには、次の手順を実行します。

ステップ 1. 「**vCenter 接続**」ページで、「**Register** (登録)」をクリックします。「**Plug-in Registration (プラグイン登録)**」ページが表示されます。



ステップ 2. 「**vCenter Server** (vCenter サーバー)」を選択します。「**Host** (ホスト)」フィールドで、vCenter サーバーの完全修飾ドメイン名 (FQDN) または IP アドレスを入力します。

注：vCenter が FQDN で構成されている場合、IP アドレスの代わりに vCenter FQDN を入力することをお勧めします。同時に、「**Network Settings** (ネットワーク設定)」ペインで DNS が構成されていることを確認してください。

ステップ 3. 次のいずれかを行います。

- 手動で登録する場合は、「**User Input**(ユーザー入力)」を選択し、「**Username**(ユーザー名)」フィールドに vCenter のユーザー名、「**Password**(パスワード)」フィールドにパスワードをそれぞれ入力します。
- 資格情報を使用して登録するには、「**Use Stored Credentials (保存された資格情報の管理)**」 ➡ 「**Manage (管理)**」 ➡ 「**Create (作成)**」を選択します。「新しい保存された資格情報を作成」ウィンドウで、vCenter のユーザー名を「**User name (ユーザー名)**」フィールドに、パソワードを「**Password (パスワード)**」フィールドおよび「**Confirm Password (パスワードの確認)**」フィールドに入力し、「**Save (保存)**」 ➡ 「**Close (閉じる)**」をクリックして、資格情報をドロップダウン・リストから選択します。

注：vCenter ユーザーに Lenovo XClarity Integrator で必要な権限がない場合は、「**Grant the needed privileges automatically (必要な権限を自動的に付与)**」チェック・ボックスを選択して、「**Administrative user (管理ユーザー)**」フィールドに管理ユーザー・アカウントを入力し、「**Password (パスワード)**」フィールドにパスワードを入力します。Lenovo XClarity Integrator は、管理ユーザー・アカウントを使用して自動的に vCenter ユーザーに権限を付与します。ただし、Lenovo XClarity Integrator は管理者アカウント情報を保存しません。

ステップ 4. 「**Register** (登録)」をクリックします。

リンク・モードの複数の vCenter サーバーへの LXCI の登録

PSC ホスト名を使用して、リンク・モードで Platform Services Controller (PSC) に接続されている複数の vCenter サーバーに Lenovo XClarity Integrator を登録できます。

注：1 つの LXCI プラグイン・インスタンスで管理できる vCenter サーバーの最大数は 1,000 です。リンク・モードの vCenter サーバーの総数が 1,000 を超える場合、ユーザーは複数の LXCI プラグイン・インスタンスをデプロイし、各インスタンスを 1 つの vCenter に登録する必要があります。

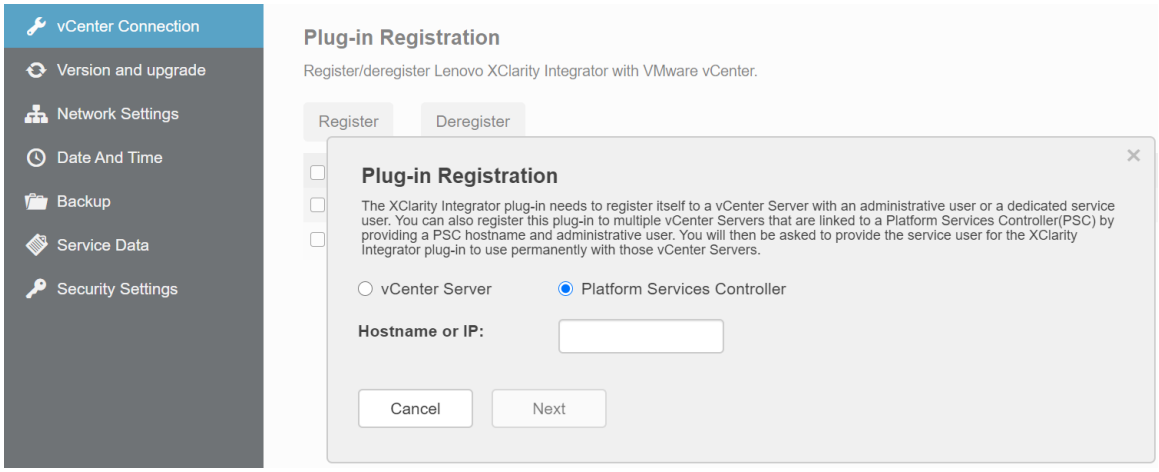
手順

以下の手順を実行して、Lenovo XClarity Integrator をリンク・モードの複数の vCenter サーバーに登録します。

ステップ 1. 「**vCenter 接続**」ページで、「**Register** (登録)」をクリックします。「**Plug-in Registration (プラグイン登録)**」ページが表示されます。

ステップ 2. 「**Platform Services Controller**」を選択して、「**ホスト名または IP**」フィールドに PSC の完全修飾ドメイン名 (FQDN) または IP アドレスを入力し、「**Next** (次へ)」をクリックします。

注：FQDN を入力した場合、DNS は、「Network Settings (ネットワーク設定)」ページで構成されます。



ステップ 3. 「**Host (ホスト)**」リストで、ターゲット vCenter サーバーを選択し、「**Next (次へ)**」をクリックします。

ステップ 4. 次のいずれかを行います。

- 手動で登録する場合は、「**User Input**(ユーザー入力)」を選択し、「**Username**(ユーザー名)」フィールドに vCenter のユーザー名、「**Password**(パスワード)」フィールドにパスワードをそれぞれ入力します。
- 資格情報を使用して登録するには、「**Use Stored Credentials (保存された資格情報の管理)**」 ➔ 「**Manage (管理)**」 ➔ 「**Create (作成)**」を選択します。「**Create new stored credentials (新しい保存された資格情報を作成)**」ウィンドウで、「**User name (ユーザー名)**」フィールドに vCenter のユーザー名、「**Password (パスワード)**」フィールドおよび「**Confirm Password (パスワードの確認)**」フィールドにパスワードを入力し、「**Save (保存)**」 ➔ 「**Close (閉じる)**」をクリックして、資格情報をドロップダウン・リストから選択します。

注：

- vCenter ユーザーは、すべてのターゲット vCenter サーバーにアクセスできる必要があります。
- vCenter ユーザーに Lenovo XClarity Integrator で必要な権限がない場合は、「**Grant the needed privileges automatically (必要な権限を自動的に付与)**」チェック・ボックスを選択して、「**Administrative user (管理ユーザー)**」フィールドに管理ユーザー・アカウントを入力し、「**Password (パスワード)**」フィールドにパスワードを入力します。Lenovo XClarity Integrator は、管理ユーザー・アカウントを使用して自動的に vCenter ユーザーに権限を付与します。ただし、Lenovo XClarity Integrator は管理者アカウント情報を保存しません。

ステップ 5. 「**Register** (登録)」をクリックします。

Lenovo XClarity Integrator の vCenter サーバーからの登録抹消

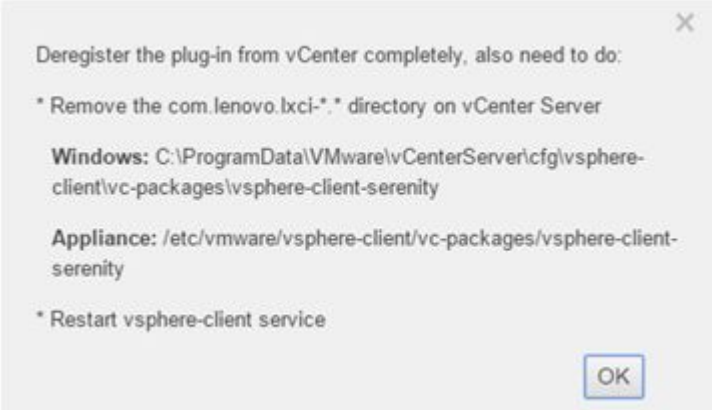
ユーザーは、Lenovo XClarity Integrator を vCenter サーバーから登録解除できます。

手順

ステップ 1. 1 つまたは複数の vCenter サーバーを選択し、「**Deregister** (登録解除)」をクリックします。確認ダイアログが表示されます。

ステップ 2. 「**Yes (はい)**」をクリックし、 Lenovo XClarity Integrator の登録解除を確認します。
ステップ 3. 「**Yes** (はい)」を再度クリックし、登録解除プロセスを完了します。

成功すると、次の図に示されているようなダイアログが表示されます。



ステップ 4. vCenter サーバーで、com.lenovo.lxci-*.* ディレクトリーを削除します。
ステップ 5. 「vsphere-client」サービスを再起動します。

サーバー資格情報の編集

ユーザーは、サーバー資格情報を編集できます。

手順

ステップ 1. ターゲット vCenter サーバーを選択し、「**Edit Credential (資格情報の編集)**」をクリックします。
ステップ 2. 「Edit selected credential (選択済みの資格情報を編集)」ウィンドウで、ユーザー名とパスワードを入力したら、「**Save (保存)**」をクリックします。

管理サーバー・ソフトウェアの更新

この「Setting (設定)」ページでは、LXCI Web サイトから最新の更新パッケージをダウンロードし、管理サーバー・ソフトウェアを最新バージョンに更新することができます。

手順

ステップ 1. 左のナビゲーション・ペインで、「**Version and upgrade**(バージョンとアップグレード)」をクリックします。「**Update Management Server** (管理サーバーの更新)」ページが表示されます。
ステップ 2. 「**Update Management Server (管理サーバーの更新)**」ページで、「**Check for Updates (更新プログラムの確認)**」をクリックして、現在の LXCI サーバーに適用可能な新しい更新パッケージを確認します。

注：LXCI インスタンスがインターネットに接続されている場合は、自動的に更新を確認し、ユーザーに週 1 回通知します。

ステップ 3. リストから必要なパッケージを選択し、「**Download (ダウンロード)**」をクリックします。
ステップ 4. リストから必要なパッケージを選択し、「**Perform Update** (更新の実行)」をクリックします。

ネットワーク・アクセスの構成

この「Setting (設定)」ページでは、Eth0 および Eth1 インターフェースのホスト名、ドメイン・ネーム、DNS、IP 設定を構成できます。

始める前に

Lenovo XClarity Integrator が最初にデプロイされるとき、VMWare vCenter およびベースボード管理コントローラー (BMC) ネットワークの両方を接続するために Eth0 インターフェースが有効になります。BMC ネットワーク接続では、オプションで Eth1 インターフェースを有効にできます。Eth1 インターフェースが有効になると、Eth0 インターフェースを BMC 接続に使用できなくなります。

ウィザードで設定したネットワーク設定の変更は推奨されません。ネットワーク設定を変更する場合は、以下の手順を実行して、仮想アプライアンスを再構成します。

注意：設定を間違って変更した場合は、仮想アプライアンスが切断される場合があります。

1. サーバー証明書を再生成します (64 ページの「セキュリティー証明書の使用」 を参照)。
2. vCenter の登録を解除し、再登録します (53 ページの「vCenter 接続の構成」 を参照)。
3. vCenter サーバーで Lenovo XClarity Integrator をクリーンアップします (13 ページの「VMware vCenter 対応 Lenovo XClarity Integrator のアンインストール」を参照)。
4. 以下の場合、Lenovo XClarity Integrator により管理されているすべてのホストで管理を無効にし、ホストを再度管理します。
   - Eth0 が変更され、Eth1 が無効になっている。
   - Eth1 が変更された。

ホスト名、ドメイン名、DNS の構成

ホスト名、ドメイン・ネーム、DNS は、「Network Settings (ネットワーク設定)」ページで構成できます。

手順

ステップ 1. 左側のナビゲーション・ペインの「**Network Settings (ネットワーク設定)**」をクリックし、右ペインの「**IP and DNS Settings (IP と DNS の設定)**」タブをクリックします。

ステップ 2. **仮想アプライアンスのホスト名、ドメイン・ネーム、DNS**領域では、ホスト名、DNS およびドメイン・ネームを変更できます。

注：
- ドメイン名はオプションです。ホスト名とドメイン・ネームの両方を構成する場合、完全修飾ドメイン・ネーム (FQDN) が定義されます。この場合、この FQDN は vCenter の登録とサーバー証明書の生成に使用されます。DNS が vCenter で正しく設定されていることを確認します。
- ホストを使用して、vCenter および vCenter 管理 EXSi ホストを接続するには、Lenovo XClarity Integrator に対して DNS を構成し、ホスト名を介して vCenter と ESXi ホスト に Lenovo XClarity Integrator がアクセスできるようにします。

ステップ 3. 「**Save (保存)**」をクリックします。

Eth0 IP 設定の構成

Eth0 IP アドレスとゲートウェイ設定は、「Network Settings (ネットワーク設定)」ページで変更できます。

このタスクについて

Eth0 インターフェースの IP 設定を変更すると、Lenovo XClarity Integrator Web インターフェースへの接続が失われます。VM コンソールで新しい Eth0 IP アドレスを確認し、Lenovo XClarity Integrator Web インターフェースを再度開いてセットアップを続行します。

手順

ステップ 1. 左側のナビゲーション・ペインの「**Network Settings (ネットワーク設定)**」をクリックし、右ペインの「**IP and DNS Settings (IP と DNS の設定)**」タブをクリックします。

ステップ 2. 「IP Settings (IP 設定)」領域で、Eth0 インターフェース の IPv4 アドレスと IPv6 アドレスまたは両方を指定します。

IPv4 の場合、静的に割り当てられた IP アドレスを使用するか、DHCP サーバーから IP アドレスを取得するか、IPv4 を無効にするかを選択できます。

IPv6 の場合、以下のいずれかの割り当て方法を使用して、インターフェースに IPv6 アドレスを割り当てることができます。
- 静的に割り当てられた IP アドレスを使用する
- ステートフル・アドレス構成 (DHCPv6) を使用する
- ステートレス・アドレス自動構成を使用する

ステップ 3. デフォルト・ゲートウェイを指定します。

注：
- Eth1 は、Eth1 サブネット内の BMC ネットワークにへの接続に意図的に使用されているため、ユーザーは、Eth0 に対してのみしか、デフォルト・ゲートウェイを構成できません。
- デフォルト・ゲートウェイを使用する場合、有効な IP アドレスを入力し、同じネットワーク・マスク (同じサブネット) を Eth0 のIP アドレスとして使用する必要があります。
- Eth0 が DHCP を使用して IP アドレスを取得する場合、デフォルト・ゲートウェイも、DHCP を使用する必要があるので変更できません。

ステップ 4. 「Save (保存)」をクリックします。

Eth1 IP 設定の構成

「Network Settings (ネットワーク設定)」ページで、ベースボード管理コントローラー (BMC) ネットワークに対して Eth1 インターフェースを有効にし、Eth1 IP アドレスとゲートウェイ設定を変更することができます。

このタスクについて

デフォルトでは、Eth0 と Eth1 の両方が「VM Network」というラベルを持つ同じ VM ネットワークに接続されます。以下の手順を実行して、Eth1 が別のネットワークに接続するように構成できます。
1. Lenovo XClarity Integrator の VM 設定を編集します。
2. 「Network adapter 2 (ネットワーク・アダプター 2)」を選択し、ターゲット VM ネットワークを選択します。
3. 設定を保存します。

手順

ステップ 1. 左側のナビゲーション・ペインの「Network Settings (ネットワーク設定)」をクリックし、右ペインの「IP and DNS Settings (IP と DNS の設定)」タブをクリックします。

ステップ 2. 「IP Settings (IP 設定)」領域で、「Enable Eth1 (Eth1 の有効化)」」を選択 して Eth1 を有効にします。IP 設定フィールドが表示されます。

ステップ 3. Eth1 インターフェースの IPv4 アドレス、IPv6 アドレス、またはその両方を指定します。

注：Eth1 インターフェースに割り当てる IP アドレスは、Eth0 インターフェースに割り当てる IP アドレスとは異なるサブネットに属する必要があります。DHCP を使用して両方のインターフェース (Eth0 と Eth1) に IP アドレスが割り当てられるように選択した場合、DHCP サーバーによって 2 つのインターフェースの IP アドレスに同じサブネットが割り当てられないようにしてください。

IPv4 の場合、静的に割り当てられた IP アドレスを使用するか、DHCP サーバーから IP アドレスを取得するか、IPv4 を無効にするかを選択できます

IPv6 の場合、以下のいずれかの割り当て方法を使用して、インターフェースに IPv6 アドレスを割り当てることができます。
- 静的に割り当てられた IP アドレスを使用する
- ステートフル・アドレス構成 (DHCPv6) を使用する
- ステートレス・アドレス自動構成を使用する

ステップ 4. 「Save (保存)」をクリックします。

プロキシーの構成

ユーザーは、「Network Settings (ネットワーク設定)」ページで、LXCI のプロキシーを設定してインターネットに接続します。

注：HTTP プロトコルのみがサポートされています。

手順

ステップ 1. 左側のナビゲーション・ペインの「Network Settings (ネットワーク設定)」をクリックし、右ペインの「Internet Settings (インターネット設定)」タブをクリックします。

ステップ 2. 「Proxy settings (プロキシー設定)」領域で、「Use HTTP proxy (HTTP プロキシーの使用)」を選択し、プロキシー、ポート、ユーザー名およびパスワードを入力します。

注：
- プロキシーは、IPv4/IPv6 アドレスまたは FQDN である必要があります。
- プロキシー・ポートは、0 ～ 65535 の間の整数でなければなりません。

ステップ 3. 「Save (保存)」をクリックします。

詳細ルーティングの構成

ユーザーは、「Network Settings (ネットワーク設定)」ページで、ルートを追加、編集および削除できます。

手順

ステップ 1. 左側のナビゲーション・ペインの「Network Settings (ネットワーク設定)」をクリックし、右ペインの「Advanced Routing (詳細ルーティング)」タブをクリックします。

ステップ 2. 次のいずれかを行います。
- 経路の追加:
  1. 「Add (追加)」をクリックします。「Advanced Route Settings (詳細な経路設定)」ウィンドウが表示されます。
  2. 「Advanced Route Settings (詳細な経路設定)」ウィンドウのドロップダウン・リストからインターフェースと経路タイプを選択し、接続先、ネットマスクおよびゲートウェイを入力します。
  3. 「Save (保存)」をクリックします。
- 経路の編集:
  1. ターゲット経路を選択し、「Edit (編集)」をクリックします。「Advanced Route Settings (詳細な経路設定)」ウィンドウが表示されます。
  2. 「Advanced Route Settings (詳細な経路設定)」ウィンドウのドロップダウン・リストからインターフェースと経路タイプを選択し、接続先、ネットマスクおよびゲートウェイを編集します。
  3. 「Save (保存)」をクリックします。
- 経路を削除するには、ターゲット経路を選択して「Remove (削除)」をクリックします。

ネットワーク接続テスト

「Network Settings (ネットワーク設定)」ページで、ネットワーク接続をテストできます。

手順

ステップ 1. 左側のナビゲーション・ペインの「**Network Settings (ネットワーク設定)**」をクリックし、右ペインの「**Test Connection (接続のテスト)**」タブをクリックします。

ステップ 2. ドロップダウン・リストで、テスト方法を選択し、ホスト名、ポート番号、カウント、プローブ、およびタイムアウトを入力します。

ステップ 3. 「**Test Connection (接続のテスト)**」をクリックします。テスト結果が、「**Result (結果)**」領域に表示されます。

日付と時刻の設定

「**Date And Time (日付と時刻)**」ページでは、日付と時刻を変更できます。

手順

ステップ 1. 左のナビゲーション・ペインで、「**Date And Time (日付と時刻)**」をクリックします。

ステップ 2. 地域とタイム・ゾーンを指定します。

ステップ 3. 日付と時刻を指定します。日付やと時刻を手動で設定するか、Lenovo XClarity Integrator が NTP サーバーと同期できるようにします。

注：
- Lenovo XClarity Integrator は NTP バージョン 4 のみをサポートします。
- 複数の NTP サーバー・アドレスが追加されている場合は、コンマ (,) を使用して区切ります。

ステップ 4. 「**Save (保存)**」をクリックします。

ディスク容量の管理

ユーザーは、「**System Monitor (システム・モニター)**」ページからディスク容量を管理できます。

手順

ステップ 1. 左側のナビゲーション・ペインで「**System Monitor (システム・モニター)**」をクリックします。

ステップ 2. 以下の操作を 1 つ以上実行します。
- 右ペインの「Disk Usage (ディスク使用量)」ページで各項目のディスク使用量を確認します。
- vLCM リポジトリーをクリーンアップするには、「**Clean Up (クリーンアップ)**」をクリックし、「**Notice (通知)**」ウィンドウの手順に従ってリポジトリーを削除します。
- ファームウェア更新リポジトリーをクリーンアップするには、「**Clean Up (クリーンアップ)**」 → 「**Yes (はい)**」をクリックします。

サービス・データの収集

サポートを受ける場合、ユーザーは、Lenovo XClarity Integrator ログを収集して、Lenovo Service に送信します。

手順

ステップ 1. 左側のナビゲーション・ペインで「**Service Data (サービス・データ)**」をクリックします。

ステップ 2. (オプション) 「**Send LXCI audit logs to vCenter (LXCI 監査ログを vCenter に送信する)**」を有効にします。

ステップ 3. 「**Collect Log (ログを収集)**」ページで、ドロップダウン・リストからログ・レベルを選択します。

注：必要に応じて、「**Debug (デバッグ)**」を選択します。問題が解決されたら、必ずログ・レベルを情報に復元してください。

ステップ 4. 「**Collect Log** (ログの収集)」をクリックします。「**Download Log** (ログのダウンロード)」リンクが表示されます。

ステップ 5. 「**Download Log** (ログのダウンロード)」リンクをクリックしてログをダウンロードします。

認証と許可の管理

VMware vCenter 対応 Lenovo XClarity Integrator は、ユーザー資格情報を確認し、リソースとタスクへのアクセスを制御するためのセキュリティー・メカニズムを提供します。

外部 LDAP 認証サーバーのセットアップ

ローカルの VMware vCenter 用 LXCI管理ノードにある認証サーバーの代わりに、外部 LDAP 認証サーバーを使用できます。

始める前に

- VMware vCenter 用 LXCI の初期セットアップは、外部認証サーバーの設定前に完了する必要があります。
- 次の外部認証サーバーがサポートされています。
  - Microsoft Active Directory。VMware vCenter 用 LXCI アプライアンスと通信可能な外部 Microsoft Windows サーバーに存在している必要があります。
- VMware vCenter 用 LXCI は、構成された外部 LDAP サーバーへの接続を維持するために、10 分ごとに接続を確認します。多くの LDAP サーバーが存在する環境では、この接続チェック時に CPU の使用率が高くなる可能性があります。最良のパフォーマンスを実現するには、LDAP クライアントの構成時に到達可能な既知の LDAP サーバーのみ指定してください。
- この XClarity Integrator Web インターフェースにログインできる LDAP ユーザーは、LDAP サーバーの LDAP グループのメンバーである必要があります。

  この LDAP クライアントを構成する前に、グループを作成して LDAP サーバーのそのグループにユーザーを追加します。
  1. 外部認証サーバーで、ユーザー・アカウントを作成します。手順については、LDAP サーバーの資料を参照してください。
  2. LDAP サーバーでグループを作成します。LDAP グループ名には、デフォルト名 **LXCI-SUPERVISOR** または他のユーザー定義の名前を使用できます。このグループは、LDAP クライアントで定義されているルート識別名のコンテキストに存在する必要があります。
  3. 前に作成したグループのメンバーとしてユーザーを追加します。

手順

外部認証サーバーを使用するように VMware vCenter 用 LXCI を構成するには、次の手順を実行します。

ステップ 1. Microsoft Active Directory のユーザー認証方式を設定するには、以下のいずれかの手順を実行します。
- 非セキュア認証を使用する場合は、追加の構成は必要ありません。Windows Active Directory ドメイン・コントローラーは、デフォルトで非セキュア LDAP 認証を使用します。
- セキュア LDAP 認証を使用する:
  1. セキュア LDAP 認証を許可するようにドメイン・コントローラーをセットアップします。Active Directory で、セキュアな LDAP 認証を構成するには、https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx を参照してください。
  2. Active Directory ドメイン・コントローラーがセキュアな LDAP 認証を使用するように構成されていることを確認します。
     - ドメイン・コントローラーの「Event Viewer (イベント ビューアー)」ウィンドウで、「LDAP over Secure Sockets layer (SSL) is now available (現在、Secure Sockets Layer (SSL) で LDAP が利用できます)」イベントを探します。

– Windows の ldp.exe ツールを使用して、ドメイン・コントローラーとのセキュア LDAP 接続をテストします。

3. サーバー証明書に署名している証明機関の LDAP サーバー証明書、中間証明書 (ある場合)、ルート証明書をインポートします。
   a. VMware vCenter 用 LXCI メニューの左側のナビゲーション・ペインで、「**Security Settings (セキュリティー設定)**」をクリックします。
   b. 「Certificate Management (証明書管理)」セクションで、「**Trusted Certificates (トラステッド証明書)**」をクリックします。
   c. 「**Add** (追加)」をクリックします。
   d. 「Add (追加)」ウィンドウで、「**Choose File (ファイルの選択)**」をクリックして、ターゲット証明書をアップロードします。
   e. 「**Upload Certificate (証明書のアップロード)**」をクリックします。

ステップ 2. VMware vCenter 用 LXCI LDAP クライアントを構成します。

a. VMware vCenter 用 LXCI のみだり側のナビゲーション・ペインで、「**Security Settings (セキュリティー設定)**」 ➡ 「**LDAP Client (LDAP クライアント)**」の順に選択します。

b. 次のいずれかのユーザー認証方式を選択します。

- **ローカル・ユーザーからのログオンを許可**。認証はローカル認証を使用して実行されます。このオプションを選択すると、ユーザーはローカル・アカウントを使用して LXCI にしかログインできません。

- **最初に LDAP ユーザーを許可し、次にローカル ユーザーを許可**。最初に外部 LDAP サーバーで認証を実行します。失敗した場合、ローカル認証サーバーで認証を実行します。この方式を選択する場合は、以下を実行します。
  1. 1 つ以上のサーバー・アドレスとポートを入力します。
  2. 入力 LDAP グループ名。

     注：
     – デフォルトでは、LDAP グループ名は **LXCI-SUPERVISOR** です。ユーザーは他の名前を入力することもできます。
     – 「**Use nested group search (入れ子になったグループ検索を使用)**」 ➡ 「**OK**」を選択すると、LXCI はターゲット・ユーザーのグループとその親グループを検索できます。この機能は、Active Directory にのみ適用されます。
  3. 以下のいずれかのバインディング方式を選択します。
     – **構成済み資格情報**。クライアント名とパスワードを使用して、VMware vCenter 用 LXCI を外部認証サーバーにバインドするには、のバインディング方式を使用します。このバインドに失敗すると認証プロセスも失敗します

       クライアント名には、識別名、sAMAccountName、NetBIOS 名または UserPrincipalName などの LDAP サーバーでサポートされている名前を使用できます。クライアント・ユーザー名は、少なくとも読み取り専用特権を持つ、ドメイン内のユーザー・アカウントである必要があります。たとえば、
       `cn=administrator,cn=users,dc=example,dc=com`
       `example\administrator`
       `administrator@example.com`
       です。

       注意：外部認証サーバーでクライアント・パスワードを変更するには、VMware vCenter 用 LXCI の新規パスワードが更新されているか確認してください。外部 LDAP サーバーでクライアント・パスワードが変更されている場合、ユーザーは、ローカル・アカウントを使用して、Integrator にログインし、新規パスワードを更新します。
     – **ログイン資格情報**。このバインディング方式を使用すると、LDAP の ユーザー名とパスワードを使用して VMware vCenter 用 LXCI を外部認証サーバーにバインドします。

指定されたユーザー ID とパスワードは、認証サーバーへの接続テストにのみ使用します。成功すると、LDAP クライアントの設定は保存されますが、指定されたテスト・ログイン資格情報は保存されません。その後のバインドは VMware vCenter 用 LXCI にログインするために使用したユーザー名とパスワードを使用します。

注：
- ユーザーは、完全修飾ユーザー ID (たとえば、`administrator@domain.com` や `DOMAIN\admin`) を使用して、VMware vCenter 用 LXCI にログインする必要があります。
- バインディング方式では、完全修飾テスト・クライアント名を使用する必要があります。

4. 「**Root DN (ルート DN)**」フィールドで、LDAP ディレクトリー・ツリーの一番上のエントリーを指定します。この場合、指定したルート識別名を検索ベースとして使用して検索が開始されます。
5. 「**User Search Attribute (ユーザー検索属性)**」フィールドで、ユーザー名の検索に使用する属性を指定します。

   バインディング方式が「**Configured Credentials (構成済み資格情報)**」に設定されている場合、LDAP サーバーへの最初のバインディングのあとに、ユーザー DN、グループ・メンバーシップなどのユーザーに関する特定情報を検索する検索リクエストが実行されます。この検索リクエストでは、そのサーバー上でユーザー ID を表す属性名前を指定する必要があります。この属性名前は、このフィールドで構成されます。
6. 「**Group Search Attribute (グループ検索属性)**」フィールドで、ユーザーが属するグループの特定に使用する属性名前を指定します。
7. 「**Group Name Attribute (グループ名属性)**」フィールドで、LDAP サーバーが構成したグループ名の特定に使用する属性名前を指定します。

c. 「**Save** (保存)」をクリックします。

VMware vCenter 用 LXCI は、構成をテストして、共通のエラーを検出しようとします。テストが失敗すると、エラー・メッセージが表示されます。このメッセージにはエラーのソースが示されています。**構成済み資格情報**バインディングの場合、テストが成功し、指定されたサーバーへの接続が正常に完了した場合、以下の条件で、ユーザー認証が失敗します。
- LDAP サーバーで誤った構成や変更が行われた場合、ユーザーはローカル・アカウントを使用してログインできる。ローカル・アカウントとパスワードは記録しておくことをお勧めします。
- ルート識別名が正しくない。
- ユーザーが LDAP サーバーの LDAP グループのメンバーではない。

d. 「**OK**」をクリックします。

結果

VMware vCenter 用 LXCI によって LDAP サーバー接続が検証されます。検証に成功した場合は、VMware vCenter 用 LXCI にログインするときに、ユーザー認証が外部認証サーバーで行われます。

検証に失敗した場合は、認証モードが自動的に「**Allow logons from local users (ローカル・ユーザーからのログオンを許可)**」設定に戻り、失敗の原因が表示されたメッセージが表示されます。

注：正確な役割グループを VMware vCenter 用 LXCI で構成し、ユーザー・アカウントは、LDAP サーバーの LDAP グループのメンバーとして定義される必要があります。そうでないと、ユーザー認証は失敗します。

セキュリティー証明書の使用

Lenovo XClarity Integrator およびそれをサポートするソフトウェア (Lenovo XClarity Administrator と VMWare vCenter) は、SSL 証明書を使用して互いにセキュアな接続を確立します。デフォルトでは、Lenovo XClarity Integrator は、内部証明機関 (CA) で発行された自己署名 Lenovo XClarity Integrator 生成証明書を使用します。

カスタマイズされた外部署名済みサーバー証明書の生成

カスタマイズされたサーバー証明書を Lenovo XClarity Integrator にインストールする場合は、CA 署名チェーン全体が含まれる証明書バンドルを指定する必要があります。

このタスクについて

新しいサーバー証明書が信頼できる国際サード・パーティ (VeriSign など) によって署名されていない場合は、次に Lenovo XClarity Integrator に接続したときに、ブラウザー内の例外として、新しい証明書を承認するようにセキュリティー・メッセージが表示されます。このセキュリティー・メッセージが表示されないようにするには、サーバー証明書の CA 署名チェーンを、トラステッド証明書の Webブラウザー・リストにインポートします。

証明書のインポートの詳細については、「19 ページの 「Lenovo XClarity Integrator 証明書を Web ブラウザーにインポート」」を参照してください。

手順

カスタマイズされたサーバー証明書を生成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Integrator に対する証明書署名要求 (CSR) を生成します。

a. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

b. 「**Server Certificate** (サーバー証明書)」をクリックして「**Server Certificate** (サーバー証明書)」ページを表示します。

c. 「**Generate Certificate Signing Request (CSR)** (証明書署名要求 (CSR) の生成)」タブをクリックします。

d. 「証明書署名要求 (CSR)の生成」ページの各フィールドに入力します。
- 国
- 都道府県
- 市区町村または地域
- 組織
- 組織単位 (オプション)
- 共通名
- 別名

注意：Lenovo XClarity Integrator 仮想アプライアンスの IP アドレスまたはホスト名と一致する共通名を選択します。正しい値を選択しないと、信頼できない接続が発生する可能性があります。Lenovo XClarity Integrator を許可して、「LXCI により生成」を指定すると、共通名を自動生成できます。

注：サブジェクト代替名の証明書をサポートする CA で署名する CSR を作成するために、ユーザーは別名を追加することができます。「**Alternative Names (別名)**」フィールドの ＋ をクリックします。「Add Alternative Names (別名の追加)」ウィンドウで、デフォルト・アドレスの後の ＋ をクリックして代替 IP/DNS アドレスを追加し、「**Submit (送信)**」をクリックします。

e. 「**Generate CSR File** (CSR ファイルの生成)」をクリックし、生成されたファイルをダウンロードします。

ステップ 2. 署名のために、すべての CSR をトラステッド CA に送信します。トラステッド CA が CSR ごとに証明書バンドルを返します。証明書バンドルには、署名された証明書と信頼できる完全な証明機関 (CA) チェーンが含まれています。

ステップ 3. 外部署名済みサーバー証明書を Lenovo XClarity Integrator にアップロードします。

注：アップロードする証明書は、「**Generate CSR File** (CSR ファイルの生成)」ボタンを使用して作成された最新の証明書署名要求から作成されたものであることが必要です。アップロードするファイルには、ルート証明書およびすべての中間証明書を含むすべての証明書チェーンが含まれている必要があります。ファイル内の証明書の順序は、サーバー証明書、中間証明書、ルート証明書にする必要があります。

1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。
2. 設定ページで「**Server Certificate** (サーバー証明書)」をクリックします。
3. 「**Upload Certificate** (証明書のアップロード)」タブをクリックします。
4. 「**Choose File** (ファイルの選択)」ボタンをクリックして、証明書ファイル (.der、.pem、または .cer) を選択します。
5. 「**Upload Certificate** (証明書のアップロード)」ボタンをクリックします。証明書ファイルがアップロードされます。

サーバー証明書がアップロードされると、Lenovo XClarity Integrator が再起動され、Lenovo XClarity Integrator Web インターフェースへのブラウザー接続が終了します。タスクを続行するには、Lenovo XClarity Integrator Web インターフェースに再度ログインします。

注：新しいサーバー証明書がアップロードされた後、VMware vCenter の登録を更新します。

Lenovo XClarity Integrator 生成サーバー証明書の復元

カスタマイズされたサーバー証明書が Lenovo XClarity Integrator で使用されている場合は、新しいサーバー証明書を生成して、Lenovo XClarity Integrator 生成サーバー証明書を復元できます。その後、カスタマイズされたサーバー証明書が交換され、新しい自己署名サーバー証明書が Lenovo XClarity Integrator で使用されます。

手順

新しいサーバー証明書を生成し、現在生成されている CA ルート証明書を使用してその証明書に署名するには、以下の手順を実行します。

ステップ 1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

ステップ 2. 設定ページで「**Server Certificate** (サーバー証明書)」をクリックします。

ステップ 3. 「**Regenerate Server Certificate** (サーバー証明書の再生成)」タブをクリックします。

ステップ 4. 「**Regenerate Server Certificate** (サーバー証明書の再生成)」ページの各フィールドに入力します。

- 国
- 都道府県
- 市区町村または地域
- 組織
- 組織編成
- 共通名

注：Lenovo XClarity Integrator 仮想アプライアンスの IP アドレスまたはホスト名と一致する共通名を選択します。正しい値を選択しないと、信頼できない接続が発生する可能性があります。「LXCI により生成」を指定すると、Lenovo XClarity Integrator は共通名を自動生成します。

ステップ 5. 「**Regenerate Certificate** (証明書の再生成)」をクリックします。

新しいサーバー証明書を生成する際は、Lenovo XClarity Integrator が再起動され、Lenovo XClarity Integrator Web インターフェースへのブラウザー接続が終了します。作業を続行するには、Lenovo XClarity Integrator Web インターフェースに再度ログインします。

注：サーバー証明書が登録された後、VMWare vCenter の登録を更新します。

証明機関 (CA) ルートの再生成

証明機関 (CA) ルートは再作成できます。

手順

ステップ 1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

ステップ 2. 設定ページで「**Certificate Authority** (証明機関)」をクリックします。

ステップ 3. 「**Regenerate Certificate Authority Root Certificate** (証明機関ルート証明書の再生成)」をクリックします。

注：

1. ユーザーは、CA ルートを再生成した後、サーバー証明書を再生成します。65 ページの「Lenovo XClarity Integrator 生成サーバー証明書の復元」を参照してください。
2. CA ルートを再生成した後は、すべてのクライアント PC で CA を再度信頼する必要があります。19 ページの 「Lenovo XClarity Integrator 証明書を Web ブラウザーにインポート」 を参照してください。

証明機関 (CA) ルート証明書のダウンロードとインストール

証明機関 (CA) ルートをダウンロードしてインストールできます。

手順

ステップ 1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

ステップ 2. 設定ページで「**Certificate Authority** (証明機関)」をクリックします。

ステップ 3. 「**Download Certificate Authority Root Certificate** (証明機関ルート証明書のダウンロード)」をクリックします。

ステップ 4. ca.der ファイルをダブルクリックします。

ステップ 5. 「**General** (全般)」タブをクリックして、「**Install Certificate** (証明書のインストール)」をクリックします。

ステップ 6. 「**Next** (次へ)」をクリックします。

ステップ 7. 「Certificate Store (証明書ストア)」ページで、「**Place all certificates in the following store** (すべての証明書を次のストアに配置する)」を選択し、「**Browse** (参照)」をクリックします。

ステップ 8. 「**Trusted Root Certificate Authorities** (信頼されたルート証明機関)」を選択し、「**OK**」をクリックします。

ステップ 9. 「**Finish** (終了)」をクリックします。

注：ユーザーのブラウザーが Firefox の場合、手順 3 でダイアログが表示されます。このダイアログでは、証明書を信頼するかどうかについて質問されます。「**Trust this CA to identify websites** (この CA を信頼して Web サイトを識別する)」をオンにして、「**OK**」をクリックし、ステップ 4 ～ 9 をスキップします。

サーバー証明書のダウンロード

サーバー証明書をダウンロードできます。

手順

ステップ 1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

ステップ 2. 設定ページで「**Server Certificate** (サーバー証明書)」をクリックします。

ステップ 3. 「**Download Certificate** (証明書のダウンロード)」タブをクリックします。

ステップ 4. 「**Download Certificate** (証明書のダウンロード)」をクリックします。

トラステッド証明書の管理

トラステッド証明書を追加、ダウンロード、または削除することができます。

手順

ステップ 1. 左ナビゲーション・ペインで、「**Security Settings** (セキュリティー設定)」をクリックします。

ステップ 2. 「setting (設定)」ページで、「**Trusted Certificates (トラステッド証明書)**」をクリックします。

ステップ 3. 次のいずれかを行います。

- トラステッド証明書の追加:
  1. 「**Add** (追加)」をクリックします。
  2. 「Add (追加)」ウィンドウで、「**Choose File (ファイルの選択)**」をクリックして、ターゲット証明書をアップロードします。
  3. 「**Upload Certificate (証明書のアップロード)**」をクリックします。
- トラステッド証明書のダウンロード:
  1. ターゲット証明書を選択します。
  2. 「**Save** (保存)」をクリックします。証明書はロカールに保存されます。
- トラステッド証明書の削除:
  1. ターゲット証明書を選択します。
  2. 「**Remove** (削除)」をクリックします。証明書を削除するかどうかを確認するポップアップ・ダイアログが表示されます。
  3. 「**Yes** (はい)」をクリックします。

Lenovo XClarity Integrator のシャットダウンまたは再起動

Lenovo XClarity Integrator をシャットダウンまたは再起動できます。ただし、Lenovo XClarity Integrator はシャットダウンまたは再起動後に切断されるため、このプロセスの後に再接続してください。

始める前に

ジョブが実行されていないことを確認します。Lenovo XClarity Integrator をシャットダウンまたは再起動すると、実行中のジョブがすべてキャンセルされます。

手順

Lenovo XClarity Integrator をシャットダウンまたは再起動するには、以下の手順を実行します。

ステップ 1. 「**Lenovo XClarity Integrator for VMware vCenter** (VMware vCenter 対応 Lenovo XClarity Integrator)」ページで、右上隅にある「**Power Control** (電源制御)」をクリックします。確認ダイアログに実行されているジョブのリストが表示されます。

ステップ 2. 「**Shut down** (シャットダウン)」または「**Restart** (再起動)」をクリックします。Lenovo XClarity Integrator がシャットダウンまたは再起動され、実行中のジョブがすべてキャンセルされます。

付録 A　サポートされる事前対応ハードウェア管理イベント

LE-FQXSPSD0002G [StorageVolumeElementName] でアレイ [ComputerSystemElementName] の障害が予知されました。

[StorageVolumeElementName] でアレイ [ComputerSystemElementName] の障害が予知されました。

このメッセージは、アレイ障害が予測されることが実装環境で検出された場合に使用されます。

Internal Event

No

重大度

警告

アラート・カテゴリー

システム - 障害予知

ユーザー操作

問題が解決するまで、以下のステップを実行します。

1. ドライブに障害があるかどうかを確認します。
2. 障害がある場合は、障害のあるドライブを交換します。
3. 問題が解決しない場合は、XCC WebGUI からサービス・データ・ログを収集し、Lenovo サポートに連絡してください。

Reviewed

LE-FQXSPSD0003G: エンクロージャー/シャーシ (MTM-SN: [arg2]) 内のドライブ [arg1] の障害が予知されました。

エンクロージャー/シャーシ (MTM-SN: [arg2]) 内のドライブ [arg1] の障害が予知されました。

このメッセージは、アレイ障害が予測されることが実装環境で検出された場合に使用されます。

Internal Event

No

重大度

警告

アラート・カテゴリー

システム - 障害予知

ユーザー操作

問題が解決するまで、以下のステップを実行します。

1. ドライブに障害があるかどうかを確認します。
2. 障害がある場合は、障害のあるドライブを交換します。
3. 問題が解決しない場合は、XCC WebGUI からサービス・データ・ログを収集し、Lenovo サポートに連絡してください。

Reviewed

付録 B　トラブルシューティング

このセクションを使用して、VMware vCenter 対応 Lenovo XClarity Integrator の問題をトラブルシューティングし、解決します。

LXCA が LXCI に追加されると、サーバーは自動的に管理できない

LXCA を LXCI に追加するときに、ユーザーが「**Create a new account by connecting with this administrative account (この管理者アカウントに接続して新しいアカウントを作成する)**」を選択する場合、新しいアカウントに割り当てられるデフォルトの役割グループは **lxc-operator**、**lxc-fw-admin**、**lxc-hw-admin**、および **lxc-os-admin** である必要があります。ただし、「**Resource Access Control (リソース・アクセス制御)**」が有効になっている場合、サーバーのデフォルトの役割グループは **lxc-supervisor** です。

手順

問題を解決するには、以下のステップを実行してください。

ステップ 1. LXCA Web ページにログインします。

ステップ 2. 「**Administration (管理)**」 → 「**Security (セキュリティ)**」 → 「**Access Control (アクセス制御)**」 → 「**Resource View (リソース・ビュー)**」をクリックします。

ステップ 3. 次のいずれかを行います。
- 「**Resource Access Control (リソース・アクセス制御)**」を無効にします。
- 次の 1 つ以上のグループをサーバーに追加します: **lxc-operator**、**lxc-fw-admin**、**lxc-hw-admin**、および **lxc-os-admin**。

vCenter の LXCI ページに「No healthy upstream (正常なアップストリームなし)」と表示される

vCenter 8.0u3 以降のバージョンでは、LXCI ページに「**No healthy upstream (正常なアップストリームなし)**」と表示されることがあります。これは、LXCI 証明書の有効期限が切れていることが原因である可能性があります。この場合、vCenter から LXCI に接続できないため、ユーザーは新しい証明書を再生成するか、新しい証明書を LXCI にアップロードし、LXCI を vCenter に再登録する必要があります。

手順

問題を解決するには、以下のステップを実行してください。

ステップ 1. LXCI 管理ページにログインします。
```
https://<LXCI IP>/admin
```

ステップ 2. 「**Security Settings (セキュリティー設定)**」 → 「**Server Certificate (サーバー証明書)**」 → 「**Download Certificate (証明書のダウンロード)**」 → 「**Download (ダウンロード)**」をクリックします。

ステップ 3. ダウンロードした証明書を開き、有効期限が切れていないかどうかを確認します。

ステップ 4. 証明書の有効期限が切れている場合は、新しい証明書を再生成またはアップロードします。

ステップ 5. vCenter への LXCI の登録を解除し、vCenter に再登録します。

ファームウェアおよびドライバー・アドオンのリストが表示されない

vSphere Lifecycle Manager を使用して、クラスターのイメージを作成する際に、**Lenovo XClarity Integrator** が、ハードウェア・サポート・マネージャーとして選択されていて、プロキシーが vCenter で有効になっているが、vCenter から LXCI (プロトコル HTTPS、ポート 443) への接続を許可しないように構成されている場合、ファームウェアとドライバー・アドオン・リストが表示されない場合があります。

手順

問題を解決するには、以下のステップを実行してください。

ステップ 1. この問題を再現してください。

ステップ 2. vCenter シェル・コンソールにログインします。

ステップ 3. シェルで、次のコマンドを実行します。
```
vi /storage/log/vmware/vmware-updatemgr/vum-server/hsm-service.log
```

ステップ 4. 次のエラー・メッセージ以上が表示された場合、vCenter から XClarity Integrator への HTTPS リクエストがプロキシーによって禁止されます。ユーザーは、プロキシーを無効にするか、vCenter から Lenovo XClarity Integrator (プロトコル HTTPS、ポート 443) への接続をプロキシー構成で許可する必要があります。
```
HTTPSConnectionPool(host='<XClarity Integrator IP or FQDN', port=443): Max retries exceeded with url:
/hsm/vsphere-lcm/hw-support/v1/packages (Caused by ProxyError('Cannot connect to proxy.', OSError
('XXX failed or timeout: '))).
```

BMC ディスカバリー失敗

BMC 検出リストが正しく表示されない場合は、BMC 検出プロセスが失敗しています。

このタスクについて

「**Discovery** (検出)」をクリックした後、検出リストの表示に失敗した場合は、以下の手順を実行します。

手順

ステップ 1. vCenter とホストの間のネットワーク接続が機能していることを確認します。

ステップ 2. 「**Discovery** (検出)」をクリックして、検出プロセスを再試行します。

シャーシ・マップ、ファームウェア更新、または構成パターン・ページが表示されない

シャーシ・マップ、ファームウェア更新、または構成パターン・ページが表示されないことがあります。

手順

問題を解決するには、以下のステップを実行してください。

ステップ 1. 19 ページの 「Lenovo XClarity Integrator 証明書を Web ブラウザーにインポート」 の手順に従って、Lenovo XClarity Integrator 証明書をインストールしたことを確認します。

ステップ 2. vCenter FQDN を使用して Lenovo XClarity Integrator を vCenter Client に登録した場合、vCenter FQDN を使用して vSphere Client を開きます。

インストール後に、vSphere Client に Lenovo XClarity Integrator が表示されない

Lenovo XClarity Integrator をインストールし、vCenter に正常に登録されたら、vSphere Client は、Lenovo XClarity Integrator プラグインのダウンロードとデプロイに失敗することがあります。この場合は、Lenovo XClarity Integrator が vSphere Client に表示されません。

手順

次のエラー・メッセージがないか `vsphere_client_virgo.log` ファイルをチェックします。
```
Error downloading https://[********LXCI IP********]:443/IVPUI.zip. Make sure that the URL is reachable;
then logout/login to force another download. java.net.ConnectionException: Network is unreachable.
```

注：vCenter のバージョンによって、ログ・ファイルは
`C:\ProgramData\VMware\vCenterServer\logs\vsphere-client\logs` または
`/storage/log/vmware/vsphere-client/logs` ディレクトリーにあります。

エラー・メッセージがログ・ファイル内に存在する場合は、次のいずれかのステップを実行します。
- Windows vCenter の場合は、VMware vCenter Server で Web ブラウザーを開いてエラー・メッセージに表示された URL (例の場合は `https://[********LXCI IP********]:443/IVPUI.zip`) にアクセスします。機能しない場合は、Lenovo XClarity Integrator サーバーが稼働していることを確認してください。
- vCenter 仮想アプライアンスの場合は、VMware vCenter Server でコマンド `curl` *<URL>* を実行します。ここでの *<URL>* は、エラー・メッセージに表示された URL (例の場合は `https://[********LXCI IP********]:443/IVPUI.zip`) です。

エラー・メッセージが「SSL certificate problem, verify that the CA cert is OK (SSL 証明書に問題があります。CA 証明書が正しいことを確認してください)」や「Certificate verify failed (証明書を検証できません)」に類似したものである場合は、次の手順を実行して Lenovo XClarity Integrator 証明書を VMware vCenter Server アプライアンスにインポートしてください。
1. Lenovo XClarity Integrator アプライアンス管理 Web ページを開いて、その Web ページにログインします。
2. 左ペインの「**Security Settings (セキュリティー設定)**」、「**Certificate Authority (証明機関)**」の順に選択します。
3. 「**Download Certificate Authority Root Certificate** (証明機関ルート証明書のダウンロード)」をクリックします。
4. Lenovo XClarity Integrator 証明書に、VMware vCenter Server を信頼されたルート証明書としてインポートします。

Lenovo XClarity Integrator を Internet Explorer 11 以降のバージョンで開くと、Lenovo XClarity Integrator に表示されるデータが最新ではない

Internet Explorer のキャッシュ・メカニズムが Lenovo XClarity Integrator の使用に影響を与えている可能性があります。Internet Explorer 11 以降のバージョンを使用して Lenovo XClarity Integrator Web ページにアクセスしたら、インターネット・オプションを設定する必要があります。

手順

ステップ 1. Internet Explorer ブラウザーを開き、「**Tools (ツール)**」 → 「**Internet options (インターネット オプション)**」をクリックします。「Internet Options (インターネット オプション)」ウィンドウが表示されます。

ステップ 2. 「**General** (全般)」タブをクリックして、「**Settings** (設定)」をクリックします。「Website Data Settings (Web サイト データの設定)」ウィンドウが表示されます。

ステップ 3. 「**Every time I visit the webpage** (Web サイトを表示するたびに確認する)」を選択し、「**OK**」をクリックします。

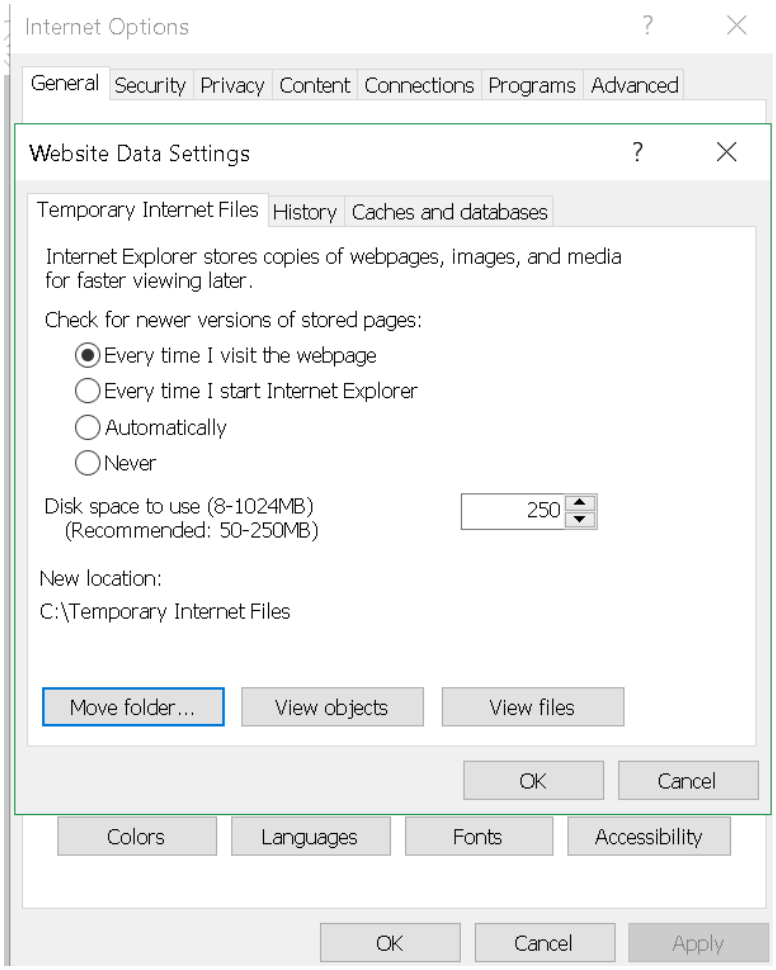


図 13. Internet Explorer の設定

ステップ 4. 「Internet Options (インターネット オプション)」ウィンドウで「**OK**」をクリックします。

このホストが 2 つの vCenter クライアントにより管理されている場合にホストのハードウェア・イベントが失われる

1 つのホストを管理できるのは 1 つの vCenter クライアントだけです。ホストを元の vCenter から削除せずに新しい vCenter クライアントに追加した場合、元の vCenter クライアントの LXCI はこのホストのハードウェア・イベントを受け取りません。

元の vCenter からホストを削除する必要があります。

付録 C　アクセシビリティー機能

アクセシビリティー機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術製品を快適に使用できるようにサポートします。

Lenovo は、年齢あるいは身体の能力に関係なく、あらゆるユーザーがアクセスできる製品を提供するよう努力しています。

「*VMware vCenter 対応 Lenovo XClarity Integrator インストールおよびユーザー・ガイド*」は、システム管理ソフトウェアに組み込まれているアクセシビリティー機能をサポートします。アクセシビリティー機能およびキーボード・ナビゲーションに関する具体的な情報については、システム管理ソフトウェアの資料を参照してください。

VMware vCenter のトピック集およびその関連資料は、スクリーン・リーダー技術を使用したアクセシビリティー機能が有効になっています。マウスの代わりに、すべての機能をキーボードを使用して操作することができます。

VMware vCenter 対応 Lenovo XClarity Integrator の資料は、Adobe Acrobat Reader を使用して Adobe PDF 形式で表示することができます。資料は、VMware 対応 Lenovo XClarity Integrator Web サイトで入手可能です。

Lenovo とアクセシビリティー

アクセシビリティーに対する Lenovo の取り組みについて詳しくは、Lenovo アクセシビリティ Web サイトを参照してください。

付録 D　特記事項

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 Lenovo の営業担当員にお尋ねください。

本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、他の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

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

LENOVO は、本書を特定物として「現存するまま」の状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書の内容は、Lenovo またはサード・パーティーの知的所有権のもとで明示または黙示のライセンスまたは損害補償として機能するものではありません。本書に記載されている情報はすべて特定の環境で得られたものであり、例として提示されるものです。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

LENOVO、FLEX SYSTEM、SYSTEM X、NEXTSCALE SYSTEM は Lenovo の商標です。インテルおよび Xeon は、Intel Corporation または子会社の米国およびその他の国における商標または登録商標です。Internet Explorer、Microsoft、および Windows は、Microsoft グループの商標です。Linux は、Linus Torvalds の米国およびその他の国における商標です。他の商標はすべて、個々の所有者の財産です。

重要事項

プロセッサーの速度とは、マイクロプロセッサーの内蔵クロックの速度を意味しますが、他の要因もアプリケーション・パフォーマンスに影響します。

主記憶装置、実記憶域と仮想記憶域、またはチャネル転送量を表す場合、KB は 1,024 バイト、MB は 1,048,576 バイト、GB は 1,073,741,824 バイトを意味します。

ハードディスク・ドライブの容量、または通信ボリュームを表すとき、MB は 1,000,000 バイトを意味し、GB は 1,000,000,000 バイトを意味します。ユーザーがアクセス可能な総容量は、オペレーティング環境によって異なります。

Lenovo は、他社製品に関して一切の保証責任を負いません。他社製品のサポートがある場合は、Lenovo ではなく第三者によって提供されます。

いくつかのソフトウェアは、その小売り版 (利用可能である場合) とは異なる場合があり、ユーザー・マニュアルまたはすべてのプログラム機能が含まれていない場合があります。