



Lenovo XClarity Administrator

Docker 環境向けの

計画およびインストール・ガイド



バージョン 4.0.0

## 注

本書および本書で紹介する製品をご使用になる前に、[XClarity Administrator オンライン・ドキュメント](#)の一般事項および特記事項をお読みください。

第1版 (2023年2月)

© Copyright Lenovo 2022.

制限付き権利に関する通知: データまたはソフトウェアが米国一般調達局 (GSA: General Services Administration) 契約に準じて提供される場合、使用、複製、または開示は契約番号 GS-35F-05925 に規定された制限に従うものとします。

# 目次

|   |     |
|---|-----|
| 目次  | i   |
| 図   | iii |
| 表   | v   |
| 変更の要約   | vii |
| 第1章 . Lenovo XClarity Administrator 概要  | 1   |
| 第2章 . XClarity Administrator の計画  | 7   |
| ライセンスおよび90日間の無料トライアル  | 7   |
| ハードウェアおよびソフトウェアの必須条件  | 8   |
| ファイアウォールおよびプロキシ・サーバー  | 10  |
| 利用可能なポート  | 12  |
| 管理に関する考慮事項  | 16  |
| ネットワークに関する考慮事項  | 17  |
| IP構成の制限   | 17  |
| ネットワーク・タイプ  | 18  |
| ネットワーク構成  | 18  |
| セキュリティに関する考慮事項  | 29  |
| Encapsulationの管理  | 29  |
| 暗号管理  | 30  |
| セキュリティ証明書   | 32  |
| 認証  | 33  |
| ユーザー・アカウントと役割グループ   | 35  |
| ユーザー・アカウント・セキュリティ   | 36  |
| 高可用性に関する考慮事項  | 36  |
| Features on Demand  | 37  |
| 第3章 . Docker、CentOS、Citrix、Red Hat KVM、Rocky、Ubuntu、VMware ESXi、またはWindows Hyper-V環境でのLenovo XClarity Administrator | 39  |
| 単一データ/管理ネットワーク  | 39  |
| 手順1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線   | 41  |
| 手順2: ラック装着スイッチの構成   | 42  |
| 手順3: Chassis Management Module (CMM) の構成  | 42  |
| 手順4: Flex スイッチの構成   | 44  |
| 手順5: ホストのインストールと構成  | 45  |
| 手順6: XClarity Administrator のインストールと構成  | 46  |
| 物理的に分離したデータ/管理ネットワーク  | 49  |
| 手順1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線   | 51  |
| 手順2: ラック装着スイッチの構成   | 52  |
| 手順3: Chassis Management Module (CMM) の構成  | 52  |
| 手順4: Flex スイッチの構成   | 54  |
| 手順5: ホストのインストールと構成  | 55  |
| 手順6: XClarity Administratorのインストールと構成   | 56  |
| 仮想的に分離したデータ/管理ネットワーク・トポロジ   | 59  |
| 手順1: シャーシとラック・サーバーからラック装着スイッチへの配線   | 62  |
| 手順2: ラック装着スイッチの構成   | 63  |
| 手順3: Chassis Management Module (CMM) の構成  | 63  |
| 手順4: Flex スイッチの構成   | 65  |
| 手順5: ホストのインストールと構成  | 67  |
| 手順6: XClarity Administratorのインストールと構成   | 67  |
| 管理専用ネットワーク・トポロジ   | 71  |
| 手順1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線   | 73  |
| 手順2: ラック装着スイッチの構成   | 73  |
| 手順3: Chassis Management Module (CMM) の構成  | 74  |
| 手順4: Flex スイッチの構成   | 76  |
| 手順5: ホストのインストールと構成  | 76  |
| 手順6: XClarity Administratorのインストールと構成   | 77  |
| 高可用性の実装   | 80  |
| 第4章 . Lenovo XClarity Administrator の構成   | 81  |
| Lenovo XClarity Administrator Web インターフェースへの最初のアクセス   | 81  |
| ユーザー・アカウントの作成   | 84  |
| ネットワーク・アクセスの構成  | 85  |
| 日付と時刻の構成  | 91  |
| サービスおよびサポートの構成  | 93  |
| セキュリティの構成   | 96  |
| デバイスの管理   | 97  |
| 第5章 . XClarity Administrator の登録  | 109 |
| 第6章 . 全機能有効化ライセンスのインストール  | 111 |

XClarity Administrator Web インターフェースを  
使用した全機能有効化ライセンスのインストー  
ル . . . . . 113

Features on Demand Web ポータルを使用した全機  
能有効化ライセンスのインストー . . . . . 116

**第 7 章 . XClarity Administrator として  
の更新 . . . . . 119**

**第 8 章 . XClarity Administrator のアン  
インストール . . . . . 123**



|   |    |  |    |
|---|----|--|----|
| 1. 管理、データ、オペレーティング・システムのデプロイメントのための単一のネットワークの実装例 . . . . .                      | 22 | 11. シャーシにおける Flex スイッチの場所 . . . . .  | 45 |
| 2. 物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部) . . . . .      | 23 | 12. 仮想アプライアンスの物理的に分離したデータ/管理ネットワーク・トポロジーの例 . . . . .   | 50 |
| 3. 物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部). . . . .         | 24 | 13. コンテナの物理的に分離したデータ/管理ネットワーク・トポロジーの例 . . . . .  | 51 |
| 4. 仮想的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部) . . . . .      | 26 | 14. 物理的に分離したデータ/管理ネットワークの配線の例 . . . . .  | 52 |
| 5. 仮想的に分離した管理ネットワークとデータ・ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部) . . . . . | 27 | 15. シャーシにおける Flex スイッチの場所 . . . . .  | 55 |
| 6. オペレーティング・システム・デプロイメントをサポートしない管理専用ネットワークの実装例 . . . . .                        | 28 | 16. 仮想アプライアンスの仮想的に分離したデータ/管理ネットワーク・トポロジーの例 . . . . .   | 60 |
| 7. オペレーティング・システム・デプロイメントをサポートする管理専用ネットワークの実装例 . . . . .                         | 29 | 17. コンテナの仮想的に分離したデータ/管理ネットワーク・トポロジーの例 . . . . .  | 61 |
| 8. 仮想アプライアンスの単一データ/管理ネットワーク・トポロジーの例 . . . . .                                   | 40 | 18. 仮想的に分離したデータ/管理ネットワークの配線の例 . . . . .  | 62 |
| 9. コンテナの単一データ/管理ネットワーク・トポロジーの例 . . . . .  | 41 | 19. 管理ネットワークで VLAN タグ付けが有効になっている仮想的に分離したデータ/管理ネットワーク (VMware ESXi) での Flex スイッチの構成の例 . . . . . | 63 |
| 10. 単一データ/管理ネットワークの配線の例 . . . . .   | 42 | 20. 管理ネットワークで VLAN タグ付けが有効になっている仮想的に分離したデータ/管理ネットワーク (VMware ESXi) での Flex スイッチの構成の例 . . . . . | 66 |
|   |    | 21. 仮想アプライアンスの管理専用ネットワーク・トポロジーの例 . . . . .   | 72 |
|   |    | 22. コンテナの管理専用ネットワーク・トポロジーの例 . . . . .  | 72 |
|   |    | 23. 管理専用ネットワークの配線の例 . . . . .  | 73 |
|   |    | 24. シャーシにおける Flex スイッチの場所 . . . . .  | 76 |



---

## 表

|  |    |  |    |
|--|----|--|----|
| 1. 必要なインターネット接続 . . . . .                        | 10 | 3. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割 . . . . . | 86 |
| 2. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割 . . . . . | 20 |  |    |





---

## 変更の要約

Lenovo XClarity Administrator 管理ソフトウェアの以下のリリースでは、新しいハードウェアのサポート、ソフトウェアの機能拡張、および修正が行われています。

修正に関する情報については、更新パッケージ内に提供される変更履歴ファイル (\*.chg) を参照してください。

サポートされるすべてのハードウェア (サーバー、シャーシ、Flex スイッチなど) について詳しくは、[ハードウェアおよびソフトウェアの必須条件](#)を参照してください。

以前のリリースの変更については、XClarity Administrator オンライン・ドキュメントの [最新情報](#) を参照してください。

このリリースでサポートされているハードウェアは、次のとおりです。

### • サーバーとアプライアンス

- ThinkAgile HX630 V3 (7D6M)
- ThinkAgile HX645 V3 (7D9M)
- ThinkAgile HX650 V3 (7D6N)
- ThinkAgile HX665 V3 (7D9N)
- ThinkAgile MX630 V3 (7D6U)
- ThinkAgile MX650 V3 (7D6S)
- ThinkAgile VX630 V3 (7D6X、7Z63)
- ThinkAgile VX635 V3 (7D9V)
- ThinkAgile VX645 V3 (7D9K)
- ThinkAgile VX650 V2-DPU (7Z63)
- ThinkAgile VX650 V3 (7D6W)
- ThinkAgile VX650 V3-DPU (7D6W)
- ThinkAgile VX655 V3 (7D9W)
- ThinkAgile VX665 V3 (7D9L)
- ThinkAgile VX850 V3 (7DDK)
- ThinkEdge SE350 V2 (7DA9)
- ThinkEdge SE455 V3 (7DBY)
- ThinkEdge SE360 V2 (7DAM)
- ThinkSystem SD555 V3 (7DDP、7DDQ)
- ThinkSystem SD650 V3 (7D7M)
- ThinkSystem SD650-I V3 (7D7L)
- ThinkSystem SD650-N V3 (7D7L)
- ThinkSystem SD665 V3 (7D9P)
- ThinkSystem SD665-N V3 (7DAZ)
- ThinkSystem SR630 V3 (7D72、7D73、7D74)
- ThinkSystem SR635 V3 (7D9G、7D9H)
- ThinkSystem SR645 V3 (7D9C、7D9D)
- ThinkSystem SR650 V3 (7D75、7D76、7D77)
- ThinkSystem SR655 V3 (7D9E、7D9F)
- ThinkSystem SR665 V3 (7D9B、7D9A)
- ThinkSystem SR675 V3 (7D9Q、7D9R)
- ThinkSystem SR850 V3 (7D96、7D97、7D98)
- ThinkSystem SR860 V3 (7D93、7D94、7D95)
- ThinkSystem SR950 V3 (7DC4、7DC5、7DC6)
- ThinkSystem ST650 V3 (7D7A、7D7B)

### • ストレージ・デバイス

- ThinkSystem DE6400F オール・フラッシュ・アレイ (7DB6)
  - ThinkSystem DE6400H ハイブリッド・フラッシュ・アレイ (7DB6)
  - ThinkSystem DE6600F オール・フラッシュ・アレイ (7DB7)
  - ThinkSystem DE6600H ハイブリッド・フラッシュ・アレイ (7DB7)
- **スイッチ**
    - ThinkSystem DB730S FC SAN スイッチ (7D9J)
    - ThinkSystem DB400D FC SAN ダイレクター (6684)
    - ThinkSystem DB800D FC SAN ダイレクター (6682)



このバージョンでは、管理ソフトウェアに対する以下の計画やインストールの強化がサポートされています。

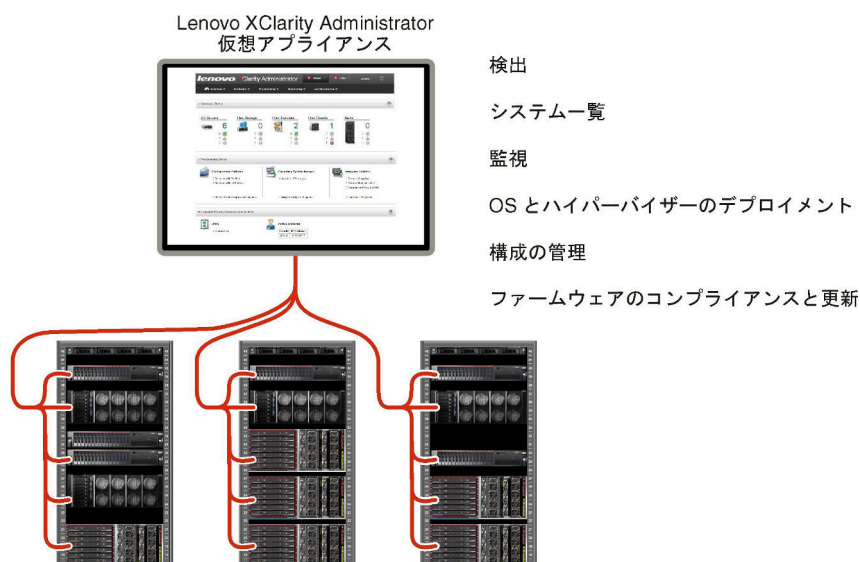
| 機能          | 説明   |
|-------------|--|
| 計画およびインストール | サポートされるホスト鍵アルゴリズムのリストから ssh-rsa を削除し、ssh-ed25519、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384、ecdsa-sha2-nistp521 を追加しました(「 <a href="#">暗号管理</a> 」を参照)。 |

# 第 1 章 Lenovo XClarity Administrator 概要

Lenovo XClarity Administrator は、Lenovo®サーバー・システムおよびソリューションのインフラストラクチャ管理を単純化し、応答性と可用性を高めることを目的としてリソースを一元的に管理するソリューションです。安全な環境でサーバー、ネットワーク、ストレージ・ハードウェアにおけるディスカバリー、インベントリ、追跡、監視、プロビジョニングを自動化する仮想アプライアンスとして機能します。

詳細:

-  [XClarity Administrator: ソフトウェアと同様にハードウェアを管理する](#)
-  [XClarity Administrator: 概要](#)



XClarity Administrator には一元管理インターフェースが用意されており、すべての管理対象デバイスに対して以下の機能を実行します。

## ハードウェア管理

XClarity Administrator はエージェントなしでハードウェアを管理します。サーバー、ネットワークおよびストレージ・ハードウェアを含む管理可能デバイスを自動的に検出できます。管理対象デバイスのインベントリ・データが収集され、管理対象ハードウェア・インベントリとそのステータスをひと目で把握できます。

ステータスとプロパティの表示、システムとネットワーク設定の構成、管理インターフェースの起動、電源のオンとオフ、リモート制御などのさまざまな管理タスクが、サポートされているデバイスごとに用意されています。デバイスの管理について詳しくは、XClarity Administrator オンライン・ドキュメントの [シャーシの管理](#)、[サーバーの管理](#)、および [スイッチの管理](#) を参照してください。

**ヒント:** XClarity Administrator で管理されるサーバー、ネットワーク、およびストレージ・ハードウェアは、[デバイス](#)と呼ばれます。XClarity Administrator の管理下に置かれるハードウェアは、[管理対象デバイス](#)と呼ばれます。

XClarity Administrator でラック・ビューを使用すると、データセンターのラックの物理的構成を反映して管理対象デバイスをグループ化できます。ラックについて詳しくは、XClarity Administrator オンライン・ドキュメントの [ラックの管理](#) を参照してください。

詳細:

-  [XClarity Administrator: 検出](#)
-  [XClarity Administrator: インベントリー](#)
-  [XClarity Administrator: リモート制御](#)

## ハードウェアの監視

XClarity Administrator では、管理対象デバイスから生成されるすべてのイベントとアラートの一元管理ビューを利用できます。イベントやアラートが XClarity Administrator に渡され、イベント・ログまたはアラート・ログに表示されます。すべてのイベントやアラートの要約は、ダッシュボードおよびステータス・バーから確認できます。特定のデバイスに関するイベントとアラートは、そのデバイスのアラートとイベントの詳細ページから確認できます。

ハードウェアの監視について詳しくは、XClarity Administrator オンライン・ドキュメントの[イベントの使用](#)および[アラートの使用](#)を参照してください。

詳細:  [XClarity Administrator: 監視](#)



## 構成の管理

一貫した構成を使用して、すべてのサーバーを簡単にプロビジョニングおよび事前プロビジョニングできます。構成設定 (ローカル・ストレージ、I/O アダプター、ブート設定、ファームウェア、ポート、管理コントローラーや UEFI の設定など) はサーバー・パターンとして保管され、1 つ以上の管理対象サーバーに適用できます。サーバー・パターンが更新されると、その変更は適用対象サーバーに自動的にデプロイされます。

また、サーバー・パターンは I/O アドレスの仮想化のサポートも統合しているため、Flex System ファブリック接続を仮想化したり、ファブリック接続を中断せずにサーバーの再利用を実行したりできます。

サーバーの構成について詳しくは、XClarity Administrator オンライン・ドキュメントの[XClarity Administrator を使用したサーバーの構成](#)を参照してください。

詳細:

-  [XClarity Administrator: ベア・メタルからクラスターへ](#)
-  [XClarity Administrator: 構成パターン](#)

## ファームウェアのコンプライアンスと更新




ファームウェア管理は管理対象デバイスに対してファームウェア・コンプライアンス・ポリシーを割り当てることによって簡略化されます。コンプライアンス・ポリシーを作成して管理対象デバイスに割り当てると、XClarity Administrator はこれらのデバイスに対するインベントリーの変更を監視し、コンプライアンス違反のデバイスにフラグを付けます。

デバイスにコンプライアンス違反がある場合、XClarity Administrator を使用してそのデバイスのすべてのデバイスに対して、管理するファームウェア更新のリポジトリからファームウェア更新を適用してアクティブ化できます。

注: リポジトリを更新したり、ファームウェア更新をダウンロードしたりするには、インターネットへの接続が必要です。XClarity Administrator がインターネットに接続されていない場合は、手動でファームウェア更新をリポジトリにインポートできます。

ファームウェアの更新について詳しくは、XClarity Administrator オンライン・ドキュメントの[管理対象デバイスでのファームウェアの更新](#)を参照してください。

詳細:



-  [XClarity Administrator: ベア・メタルからクラスターへ](#)
-  [XClarity Administrator: ファームウェア更新](#)
-  [XClarity Administrator: ファームウェア・セキュリティー更新のプロビジョニング](#)

## オペレーティング・システム・デプロイメント

XClarity Administrator を使用してオペレーティング・システム・イメージのリポジトリを管理し、最大 28 台の管理対象サーバーにオペレーティング・システム・イメージを同時にデプロイできます。

オペレーティング・システムのデプロイメントについて詳しくは、XClarity Administrator オンライン・ドキュメントの [オペレーティング・システム・イメージのデプロイ](#) を参照してください。

### 詳細:

-  [XClarity Administrator: ベア・メタルからクラスターへ](#)
-  [XClarity Administrator: オペレーティング・システムのデプロイメント](#)

## ユーザーの管理

XClarity Administrator には集中型認証サーバーが用意されており、ユーザー・アカウントを作成して管理します。また、ユーザー資格情報を管理して認証します。認証サーバーは、管理サーバーを初めて起動する際に自動的に作成されます。XClarity Administrator 用に作成したユーザー・アカウントは、管理対象認証モードで管理対象シャシやサーバーにログインするときにも使用できます。ユーザーについて詳しくは、XClarity Administrator オンライン・ドキュメントの [ユーザー・アカウントの管理](#) を参照してください。

XClarity Administrator は 3 タイプの認証サーバーをサポートしています。

- **ローカル認証サーバー。** デフォルトでは、XClarity Administrator は管理ノードのローカル認証サーバーを使用するように構成されています。
- **外部 LDAP サーバー。** 現在、Microsoft Active Directory のみサポートされます。このサーバーは、管理ネットワークに接続している外部の Microsoft Windows サーバーに存在している必要があります。外部 LDAP サーバーが使用されている場合、ローカル認証サーバーは無効になります。
- **外部 SAML 2.0 ID プロバイダー。** 現在、Microsoft Active Directory Federation Services (AD FS) のみサポートされます。ユーザー名とパスワードを入力するほか、PIN コードの要求やスマート・カードやクライアント証明書の読み込みによる追加セキュリティを有効にするマルチファクター認証をセットアップできます。

認証タイプについて詳しくは、XClarity Administrator オンライン・ドキュメントの [認証サーバーの管理](#) を参照してください。

ユーザー・アカウントを作成する際に、そのユーザー・アカウントに事前定義またはカスタマイズされた役割グループを割り当て、そのユーザーのアクセス・レベルを制御します。役割グループについて詳しくは、XClarity Administrator オンライン・ドキュメントの [役割グループの作成](#) を参照してください。

XClarity Administrator には、ログオン、新しいユーザーの作成、ユーザー・パスワードの変更など、ユーザー操作の履歴が記録された監査ログが含まれています。監査ログについて詳しくは、XClarity Administrator オンライン・ドキュメントの [イベントの使用](#) を参照してください。

## デバイス認証

XClarity Administrator は以下の方式を使用して管理対象シャシおよびサーバーで認証します。

- **管理対象認証。** 管理対象認証が有効の場合は、XClarity Administrator 用に作成したユーザー・アカウントは、管理対象シャシやサーバーに認証するときにも使用されます。

ユーザーについて詳しくは、XClarity Administrator オンライン・ドキュメントの [ユーザー・アカウントの管理](#) を参照してください。

- **ローカル認証。** 管理対象認証が無効の場合は、XClarity Administrator で定義されている保存された資格情報を使用して管理対象サーバーを認証します。保存された資格情報は、デバイスまたは Active Directory のアクティブなユーザー・アカウントに対応している必要があります。

保存された資格情報について詳しくは、XClarity Administrator オンライン・ドキュメントの [保存された資格情報の管理](#) を参照してください。

## セキュリティ

お使いの環境が NIST SP 800-131A 標準に従う必要がある場合、それらに完全に準拠した環境を作成するのに XClarity Administrator が役立ちます。

XClarity Administrator は、自己署名 SSL 証明書 (内部証明機関によって発行されたもの) および外部 SSL 証明書 (プライベートまたは商用 CA によって発行されたもの) をサポートします。

シャーマシおよびサーバーのファイアウォールを、XClarity Administrator からの受信要求のみを受け入れるように構成できます。

セキュリティについて詳しくは、XClarity Administrator オンライン・ドキュメントの[セキュアな環境の実装](#)を参照してください。

## サービスおよびサポート

一定の保守可能イベントが XClarity Administrator および管理対象デバイスで発生した場合に、診断ファイルを自動的に収集し優先サービス・プロバイダーに送信するように XClarity Administrator をセットアップできます。コール・ホーム を使用して診断ファイルを Lenovo サポート に送信するか、SFTP を使用して別のサービス・プロバイダーに送信するかを選択できます。また、手動で診断ファイルを収集したり、問題レコードを開いたり、診断ファイルを Lenovo サポート・センター に送信したりもできます。

詳細:  [XClarity Administrator: サービスおよびサポート](#)

## スクリプトによるタスクの自動化

XClarity Administrator は、オープンな REST アプリケーション・プログラミング・インターフェース (API) を使用して、外部のより高レベルな管理プラットフォームや自動化プラットフォームに組み込むことができます。REST API を使用して、XClarity Administrator は既存の管理インフラストラクチャーに容易に統合できます。

PowerShell ツールキットは、Microsoft PowerShell セッションからのプロビジョニングとリソース管理を自動化するコマンドレット・ライブラリーを提供します。Python ツールキットは、Ansible や Puppet などの OpenStack 環境からのプロビジョニングとリソース管理を自動化する、Python ベースのコマンドおよび API のライブラリーを提供します。これらのツールキットはどちらも、XClarity Administrator REST API にインターフェースを提供して、以下の機能を自動化します。

- XClarity Administrator へのログイン
- シャーマシ、サーバー、ストレージ・デバイス、およびラック装着スイッチ (デバイス) の管理と管理解除
- デバイスおよびコンポーネントのインベントリ・データの収集および表示
- オペレーティング・システム・イメージの 1 つ以上のサーバーへのデプロイ
- 構成パターンを使用したサーバーの構成
- デバイスに対するファームウェア更新の適用

## 他の管理対象ソフトウェアとの統合

XClarity Administrator モジュールは、XClarity Administrator をサードパーティー製管理ソフトウェアと統合して、検出、監視、構成、および管理機能を提供し、サポートされているデバイスのルーチン・システム管理のコストや複雑さを軽減します。



XClarity Administrator について詳しくは、次のドキュメントを参照してください。

- [Microsoft System Center 向け Lenovo XClarity Integrator](#)
- [VMware vCenter 向け Lenovo XClarity Integrator](#)

追加の考慮事項については、XClarity Administrator オンライン・ドキュメントの[管理に関する考慮事項](#)を参照してください。



### 詳細:

-  [Microsoft System Center 向け Lenovo XClarity Integrator 概要](#)
-  [VMware vCenter 向け Lenovo XClarity Integrator](#)

### 資料

XClarity Administrator 資料は、英語版がオンラインで常時更新されています。最新情報と手順は、[XClarity Administrator オンライン・ドキュメント](#) を参照してください。

オンライン・ドキュメントは、次の言語で入手できます。

- ドイツ語 (de)
- 英語 (en)
- スペイン語 (es)
- フランス語 (fr)
- イタリア語 (it)
- 日本語 (ja)
- 韓国語 (ko)
- ブラジル・ポルトガル語 (pt\_BR)
- ロシア語 (ru)
- タイ語 (th)
- 簡体字中国語 (zh\_CN)
- 繁体字中国語 (zh\_TW)

次の方法でオンライン・ドキュメントの言語を変更できます。

- ご使用の Web ブラウザーの言語設定を変更する
- URL の末尾に `?lang=<language_code>` を付け加える。たとえば、オンライン・ドキュメントを簡体字中国語で表示するには、次のようにします。

`http://sysmgmt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html?lang=zh_CN`





---


## 第 2 章 XClarity Administrator の計画

Lenovo XClarity Administrator をインストールする前に、インストールと日常管理の計画に役立つ以下の考慮事項について検討してください。

---

### ライセンスおよび 90 日間の無料トライアル

Lenovo XClarity Administrator には 90 日間の試用ライセンスがあり、限定された期間、すべての機能を完全に使用できます。

XClarity Administrator タイトル・バーからユーザー操作メニュー (  ) をクリックして、「バージョン情報」をクリックすることで、試用版の残り期間などのライセンスの状況を確認できます。

XClarity Administrator は、以下のライセンスをサポートします。

- **Lenovo XClarity Pro**. 各ライセンスは、1 台のデバイスに対して次の資格を提供します。
  - Lenovo XClarity Integrator のサービスおよびサポート
  - XClarity Administrator のサービスおよびサポート
  - XClarity Administrator 内の高度な機能:
    - 構成パターンを使用したサーバーの構成
    - オペレーティング・システムのデプロイ
    - コール・ホームを使用して XClarity Administrator の問題を報告する (ハードウェア・アラート向けのコール・ホームは影響されません。)

拡張機能をサポートする管理対象デバイスごとにライセンスを購入する必要があります。ライセンスは特定のデバイスに関連付けられていません。

ライセンス・コンプライアンスは、拡張機能をサポートする管理対象デバイスの数に基づいて決定されます。管理対象デバイスの数は、すべてのアクティブなライセンス・キーに含まれるライセンスの合計数を超えてはなりません。XClarity Administrator がインストール済みのライセンスに準拠していない場合 (たとえば、ライセンスの有効期限が切れた場合や、追加のデバイスを管理するとアクティブなライセンスの合計数を超える場合)、適切なライセンスをインストールする猶予期間は 90 日になります。XClarity Administrator が非準拠になるたびに、猶予期間が 90 日にリセットされます。ライセンスに準拠する前に猶予期間 (無料試用期間を含む) が終了した場合、拡張機能はすべてのデバイスで無効になります。

注 :

- 猶予期間が過ぎると、サーバー構成およびオペレーティング・システム・デプロイメント機能は無効になります。
- XClarity Administrator の問題のためのコール・ホーム (ソフトウェア・コール・ホーム機能) は、ライセンスが準拠していない場合、無効になります。この機能には、猶予期間はありません。ただし、ハードウェア・アラートのコール・ホームは影響を受けません。

ライセンスが既にインストールされている場合、XClarity Administrator の新規リリースにアップグレードする場合に新規のライセンスは必要ありません。

Lenovo XClarity Pro のライセンス購入については詳しくは、Lenovo 担当員または認定ビジネス・パートナーに連絡してください。

ライセンスのインストールについては、XClarity Administrator オンライン・ドキュメントの [全機能有効化ライセンスのインストール](#) を参照してください。

---

## ハードウェアおよびソフトウェアの必須条件

Lenovo XClarity Administrator 管理アプライアンスは、ホスト・システム上の仮想マシンで実行されます。

### ハイパーバイザー要件

#### コンテナ環境

XClarity Administrator をコンテナとして実行するには、以下のコンテナ環境がサポートされています。

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

#### ハイパーバイザー

XClarity Administrator を仮想アプライアンスとして実行するために、以下のハイパーバイザーがサポートされています。

- Citrix ハイパーバイザー v8.2
- Citrix XenServer v7.6
- CentOS 7 および 8<sup>1</sup>
- Hyper-V がインストールされている Microsoft Windows Server 2022
- Hyper-V がインストールされている Microsoft Windows Server 2019
- Hyper-V がインストールされている Microsoft Windows Server 2016
- Hyper-V がインストールされている Microsoft Windows Server 2012 R2
- Hyper-V がインストールされている Microsoft Windows Server 2012
- Nutanix Acropolis Hypervisor (AHV)
- カーネル・ベースの仮想マシン (KVM) v2.12.0 がインストールされている Red Hat v8.x
- KVM v1.2.17 がインストールされている Red Hat v7.x
- KVM v4.2.3 がインストールされた Ubuntu 20.04.2 LTS
- VMware ESXi 7.0、U1、U2 および U3
- VMware ESXi 6.7、U1、U2<sup>2</sup>、および U3

#### 注：

1. CentOS Linux は Red Hat によって更新されなくなりました。代わりに Red Hat Enterprise Linux への移行を検討してください ([Red Hat: CentOS または Oracle Linux から RHEL の Web ページに変換する方法](#)を参照)。
2. VMware ESXi 6.7 U2 の場合、ISO イメージ VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso 以降を使用する必要があります。

VMware および Citrix の場合、仮想マシンは OVF テンプレートとして入手できます。Hyper-V および Nutanix AHV の場合、仮想マシンは仮想ディスク・イメージ (VHD) です。CentOS および KVM の場合、仮想マシンは qcow2 形式として入手できます。

**重要：**2.6 カーネル・ベースの Linux ゲスト上で稼働し、仮想アプライアンス用に大量のメモリーを使用する Hyper-V 環境では、Hyper-V マネージャーの Hyper-V 設定パネルで不均一なメモリー・アクセス (NUMA) の使用を無効にする必要があります。この設定を変更するには、Hyper-V サービスを再起動する必要があります。Hyper-V を再起動すると、実行中のすべての仮想マシンも再起動されます。この設定を無効にしない場合は、XClarity Administrator 仮想アプライアンスで初回起動時に問題が発生する可能性があります。

### ハードウェア要件

XClarity Administrator では、以下の**最小要件**が満たされている必要があります。環境の規模と構成パターンの使用に応じて、最適なパフォーマンスを実現するために追加リソースが必要になることがあります。

- 仮想マイクロプロセッサが 2 個の場合
- 8 GB のメモリーを搭載している

- 192 GB のストレージを XClarity Administrator 仮想アプライアンスで使用できる
- 最小解像度が幅 1024 ピクセル (XGA) のディスプレイ

次の表は、特定の数のデバイスで推奨される最小構成を示しています。最小構成で実行している場合、管理タスクの完了までにかかる時間が予想以上に長くなる点に注意してください。オペレーティング・システムのデプロイ、ファームウェアの更新、サーバーの構成などのプロビジョニング・タスクでは、一時的にリソースを増やすことが必要になる場合があります。

| 管理対象デバイスの台数      | 仮想 CPU / メモリー構成   |
|------------------|-------------------|
| 0 ~ 100 デバイス     | 2 vCPU、8 GB RAM   |
| 100 ~ 200 デバイス   | 4 vCPU、10 GB RAM  |
| 200 ~ 400 デバイス   | 6 vCPU、12 GB RAM  |
| 400 ~ 600 デバイス   | 8 vCPU、16 GB RAM  |
| 600 ~ 800 デバイス   | 10 vCPU、20 GB RAM |
| 800 ~ 1,000 デバイス | 12 vCPU、24 GB RAM |

注：

- 1 つの XClarity Administrator インスタンスで最大 1,000 個のデバイスをサポートできます。
- 最新の推奨事項およびその他のパフォーマンスに関する考慮事項については、[XClarity Administrator: パフォーマンス・ガイド \(ホワイトペーパー\)](#) を参照してください。
- ご使用の管理対象環境のサイズとインストールでの使用パターンに応じて、許容可能なパフォーマンスを維持するためにリソースを追加することが必要になる場合があります。システム・リソースのダッシュボードのプロセッサ使用率で頻繁に高い値または非常に高い値が表示される場合、1 ~ 2 個の仮想プロセッサ・コアを追加することを検討してください。メモリー使用量がアイドル状態で 80 % を常時上回る場合は、1 ~ 2 GB の RAM を追加することを検討してください。ご使用のシステムが表で定義されているように構成時に応答する場合は、実行中のシステム・パフォーマンスの評価のためにより長時間 VM を実行することを検討してください。
- 不要になった XClarity Administrator リソースを削除してディスク・スペースを解放する方法については、XClarity Administrator オンライン・ドキュメントの[ディスク・スペースの管理](#)を参照してください。

## ソフトウェア要件

### • Orchestrator サーバー

複数の XClarity Administrator インスタンスを使用して多数のデバイスを管理する場合、Lenovo XClarity Orchestrator を使用した監視、管理、プロビジョニング、分析を一元管理できます。XClarity Orchestrator は、ThinkEdge ではないクライアント・デバイスを最大 10,000 台まとめて管理できる XClarity Administrator インスタンスを無制限数サポートできます。

Lenovo XClarity Orchestrator を使用して XClarity Administrator v4.0 以降のインスタンスを管理するには、XClarity Orchestrator v2.0 以降が必要です。

### • 認証サーバー

外部認証サーバーの使用を選択した場合、Windows Server 2008 以降で実行中の Microsoft Active Directory のみがサポートされます。

SAML 識別プロバイダーの使用を選択した場合、Windows Server 2012 で実行中の Microsoft Active Directory Federation Services (AD FS) バージョン 2.0 以降のみがサポートされます。

### • NTP サーバー

管理対象デバイスから受信したすべてのイベントおよびアラームのタイムスタンプが XClarity Administrator と同期されるようにするために、Network Time Protocol (NTP) サーバーが必要です。

NTP サーバーに管理ネットワークを介してアクセスできることを確認します (通常は Eth0 インターフェース)。

**ヒント:** XClarity Administrator をインストールするホスト・システムを NTP サーバーとして使用することを検討してください。この場合は、そのホスト・システムに管理ネットワークを介してアクセスできることを確認します。

## 管理可能なリソース

1 つの XClarity Administrator インスタンスで、最大 1,000 台の物理デバイスを管理、監視、プロビジョニングできます。

サポートされるデバイスとオプション (I/O、DIMM、およびストレージ・アダプターなど) の完全なリスト、ファームウェア・レベルの最小要件、制限に関する考慮事項は、[XClarity Administrator のサポート - 互換性に関する Web ページ](#) で「互換性」タブをクリックしてから、該当するデバイス・タイプのリンクをクリックすることで確認できます。

特定のデバイスのハードウェアの構成とオプションに関する一般情報については、[Lenovo Server Proven Web サイト](#) を参照してください。

**制限:** XClarity Administrator をインストールしたホスト・システムが管理対象ラックサーバーである場合、XClarity Administrator を使用して、そのホスト・システムまたはシャーシ全体にファームウェア更新を一度に適用することはできません。ホスト・システムにファームウェア更新が適用されたら、ホスト・システムを再起動する必要があります。ホスト・システムを再起動すると、XClarity Administrator も再起動され、XClarity Administrator を使用してホスト・システムで更新を完了できなくなります。

## サポートされている Web ブラウザー

XClarity Administrator Web インターフェースは次の Web ブラウザーで機能します。

- Chrome™ 48.0 以降 (リモート・コンソールには 55.0 以上)
- Firefox® ESR 38.6.0 以降
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 以降 (IOS7 以降および OS X)

---

## ファイアウォールおよびプロキシ・サーバー

管理サーバー更新、ファームウェア更新、サービスおよびサポートを含む Lenovo XClarity Administrator の一部の機能には、インターネットへのアクセスが必要です。ご使用のネットワークにファイアウォールがある場合、XClarity Administrator 管理サーバーを有効にするようにファイアウォールを構成し、これらの操作を実行します。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、XClarity Administrator を構成してプロキシ・サーバーを使用します。

### ファイアウォール

ファイアウォールで次の DNS 名およびポートが開いていることを確認します。

注：IP アドレスは、変更の対象です。可能な限り DNS 名を使用します。

表 1. 必要なインターネット接続

| DNS 名                     | IPv4 アドレス | IPv6 アドレス | ポート | プロトコル |
|---------------------------|-----------|-----------|-----|-------|
| ライセンス・アクティベーション・キーのダウンロード |           |           |     |       |
| fod.lenovo.com            | N/A       | N/A       | 443 | https |
| Service Bulletin のダウンロード  |           |           |     |       |

表 1. 必要なインターネット接続 (続き)

| DNS 名  | IPv4 アドレス  | IPv6 アドレス | ポート        | プロトコル          |
|--|--|-----------|------------|----------------|
| download.lenovo.com/servers/LXCA_Bulletin_Service.json   | N/A  | N/A       | 443 および 80 | https          |
| 更新 (管理サーバーの更新、ファームウェア更新、UpdateXpress System Packs (OS デバイス・ドライバー)、リポジトリ・パック) のダウンロード                     |  |           |            |                |
| datacentersupport.lenovo.com   | N/A  | N/A       | 443 および 80 | https          |
| download.lenovo.com  | N/A  | N/A       | 443 および 80 | https          |
| filedownload.lenovo.com  | N/A  | N/A       | 443 および 80 | https          |
| support.lenovo.com   | N/A  | N/A       | 443 および 80 | https および http |
| supportapi.lenovo.com  | N/A  | N/A       | 443 および 80 | https          |
| ファームウェアのダウンロード (Flex System x220、x222、x240、x280 x6、x440、x480 x6、x880 X 6、Flex スイッチの一部、および第 1 世代の CMM のみ) |  |           |            |                |
| www.ibm.com  | 129.42.56.216,<br>129.42.58.216,<br>129.42.60.216,<br>129.42.160.51,<br>207.25.252.197 | N/A       | 443 および 80 | https および http |
| www-03.ibm.com   | 204.146.30.17  | N/A       | 443 および 80 | https および http |
| download3.boulder.ibm.com  | 170.225.126.24   | N/A       | 443        | https          |
| download4.boulder.ibm.com  | 170.225.126.43   | N/A       | 443 および 80 | https および http |
| delivery04-bld.dhe.ibm.com   | 170.225.126.45   | N/A       | 443 および 80 | https および http |
| delivery04-mul.dhe.ibm.com   | 170.225.126.46   | N/A       | 443 および 80 | https および http |
| delivery04.dhe.ibm.com   | 170.225.126.44   | N/A       | 443 および 80 | https および http |
| サービス・データを Lenovo サポート (コール・ホーム) にアップロード  |  |           |            |                |
| soaus.lenovo.com   | 3.222.8.29,<br>52.6.14.20  | N/A       | 443        | https          |
| logupload.lenovo.com/BLL/Logupload.ashx  | N/A  | N/A       | 443 および 80 | https          |
| サービス・データを Lenovo 更新ファシリティにアップロード   |  |           |            |                |
| logupload.lenovo.com/BLL/Logupload.ashx  | N/A  | N/A       | 443 および 80 | https          |
| 保証情報のダウンロード  |  |           |            |                |

表 1. 必要なインターネット接続 (続き)

| DNS 名                        | IPv4 アドレス              | IPv6 アドレス | ポート        | プロトコル          |
|------------------------------|------------------------|-----------|------------|----------------|
| ibase.lenovo.com (ワールドワイド)   | N/A                    | N/A       | 443 および 80 | https および http |
| service.lenovo.com.cn (中国のみ) | 114.247.140.212 (中国のみ) | N/A       | 83         | http           |
| supportapi.lenovo.com        | N/A                    | N/A       | 443 および 80 | https および http |

注意：中国のユーザーは、XClarity Administratorを使用して管理対象デバイスに保証情報を取得するには、XClarity Administrator v.1.3.1 以降に更新する必要があります。

### プロキシ・サーバー

管理サーバーがインターネットに直接接続できない場合、管理サーバーが HTTP プロキシ・サーバーを使用するように構成されていることを確認します (ネットワーク・アクセスの構成を参照)。

- 必ず、プロキシ・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ようにしてください。
- プロキシ・サーバーが終了しないプロキシとしてセットアップされていることを確認します。
- プロキシ・サーバーが転送プロキシとしてセットアップされていることを確認します。
- ロード・バランサーがセッションを1つのプロキシ・サーバーで保持し、他のサーバーに切り替えないように構成されていることを確認します。

## 利用可能なポート

ご使用の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する必要があります。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 Administrator 機能が動作しないことがあります。

ご使用の環境に基づいて、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表には、各ポートの XClarity Administrator での使用方法、影響を受け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記載されています。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 Administrator へのフローを識別するため、XClarity Administrator アプライアンスでポートを開く必要があります。アウトバウンドは XClarity Administrator から管理対象デバイスへのトラフィック・フローです。

- [XClarity Administrator サーバーへのアクセス](#)
- [XClarity Administrator と管理対象デバイス間のアクセス](#)
- [OS デプロイメントとデバイス・ドライバーの更新のための XClarity Administrator とデータ・ネットワーク間のアクセス](#)

### XClarity Administrator サーバーへのアクセス

XClarity Administrator 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る場合、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するには、XClarity Administrator ポートが開いていることを確認する必要があります。また、SNMP および SMTP を使用してイベントを管理する場合は、XClarity Administrator サーバーによって使用されているポートが、イベント転送のために開いていることを確認しなければならないこともあります。

XClarity Administrator サーバーは、次の表に示すポートで listen し、そのポートを介して応答します。

注：



- XClarity Administrator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。
- XClarity Administrator はオプションで、LDAP、SMTP、または syslog などの外部サービスにアウトバウンド接続を確立するように構成できます。これらの接続には、一般的にユーザーが構成可能でこのリストに含まれていない追加のポートが必要になる場合があります。また、これらの接続では、TCP または UDP ポート 53 でドメイン名サービス (DNS) サーバーにアクセスして外部サーバー名を解決する必要がある場合もあります。

| 通信   | XClarity Administrator アプライアンス   | 外部認証サーバー   | イベント転送サービス  | Lenovo サービス (コール・ホームを含む)   |
|--|--|--|---|--|
| アウトバウンド (外部システムでオープンされるポート)                    | <ul style="list-style-type: none"> <li>• DNS – ポート 53 の TCP/UDP</li> </ul> | <ul style="list-style-type: none"> <li>• LDAP – ポート 389<sup>1</sup> の TCP</li> <li>• LDAPS – ポート 636 の TCP</li> <li>• SAML 認証 – ポート 3268、3269 の TCP</li> </ul> | <ul style="list-style-type: none"> <li>• FTP サーバー – ポート 21<sup>1</sup> の TCP</li> <li>• メール・サーバー (SMTP) – ポート 25<sup>1</sup> の UDP</li> <li>• REST Web サービス (HTTP) – ポート 80<sup>1</sup> の UDP</li> <li>• SNMP マネージャー – ポート 161<sup>2</sup>、162<sup>1</sup> の UDP</li> <li>• MS Azure – ポート 443<sup>1</sup> の UDP</li> <li>• Syslog – ポート 514<sup>1</sup> の UDP</li> <li>• Apple プッシュ<sup>3</sup> – ポート 443、2195、5223 の TCP</li> <li>• Google プッシュ<sup>4</sup> – ポート 443、5288、5299、5230 の TCP</li> </ul> | <ul style="list-style-type: none"> <li>• Warranty (保証) (中国のみ) – ポート 83<sup>5</sup> の TCP</li> <li>• HTTPS (コール・ホーム) – ポート 443 の TCP</li> </ul> |
| インバウンド (XClarity Administrator アプライアンスで開いたポート) | <ul style="list-style-type: none"> <li>• HTTPS – ポート 443 の TCP</li> </ul>  | 適用外  | <ul style="list-style-type: none"> <li>• SNMP – ポート 161 の UDP</li> </ul>  | 適用外  |

1. デフォルトのポートです。このポートは、ユーザー・インターフェースから構成できます。
2. このポートは、ユーザー認証での SNMP イベント転送の構成時に使用されます。
3. Wi-Fi がファイアウォールまたは携帯端末データ用のプライベート・アクセス・ポイント名 (APN) を介した先にある場合は、このポートを開きます。このポートでは、プロキシを介さず直接 APN サーバーに接続する必要があります。このポートは、デバイスがポート 5223 で Apple プッシュ通知サービスに接続できない場合の Wi-Fi のフェイルバックとしてのみ使用されます。IP アドレス範囲は 17.0.0.0/8 です。
4. IP アドレス範囲については、Google ASN 15169 を参照してください。ドメインは android.googleapis.com です。
5. 中国以外では必須ではありませんが、XClarity Administrator が他の国でこのサービスに接続を試みる可能性があります。

## XClarity Administrator 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いる場合、そのファイアウォールの外側にある XClarity Administrator サーバーからこれらのデバイスを管理するには、XClarity Administrator と各管理対象デバイス上のベースボード管理コントローラーに関連するすべてのポートが開いていることを確認する必要があります。

XClarity Administrator を使用してオペレーティング・システムを管理対象デバイスにインストールする場合は、[OS デプロイメントとデバイス・ドライバの更新のための XClarity Administrator とデータ・ネットワーク間のアクセス](#)のポートのリストを必ず確認してください。

### • Flex シャーシ CMM

| 通信   | Flex シャーシ CMM   |
|--|---|
| アウトバウンド (外部システムでオープンされるポート)                    | <ul style="list-style-type: none"> <li>- SLP - ポート 427 の UDP/TCP</li> <li>- CIM HTTP - ポート 5988<sup>2</sup> の TCP</li> <li>- CIM HTTPS - ポート 5989 の TCP</li> <li>- TCP コマンド - ポート 6090<sup>2</sup> の TCP</li> <li>- セキュア TCP コマンド - ポート 6091 の TCP</li> </ul> |
| インバウンド (XClarity Administrator アプライアンスで開いたポート) | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>1</sup> の TCP</li> <li>- CIM 表示 HTTPS - TCP 9090</li> <li>- LDAPS - ポート 50637 の TCP</li> </ul>   |

1. このポートは、SFTP を使用してファームウェア更新プログラムを転送するために使用されます。
2. 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。

### • サーバーと計算ノード

| 通信                                   | ThinkSystem および ThinkAgile   | System x  | Flex System   | ThinkServer   |
|--------------------------------------|--|---|---|---|
| アウトバウンド (外部システムでオープンされるポート)          | <ul style="list-style-type: none"> <li>- SFTP - ポート 115 の TCP</li> <li>- SLP - ポート 427 の UDP/TCP</li> <li>- HTTPS - ポート 443 の TCP</li> <li>- SSDP 検出 - ポート 1900 の UDP</li> <li>- リモート制御 - ポート 3888<sup>4</sup> の TCP</li> <li>- リモート KVM - ポート 3889<sup>4</sup> の TCP</li> <li>- CIM HTTPS - ポート 5989 の TCP</li> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- SLP - ポート 427 の UDP/TCP</li> <li>- HTTPS - ポート 443 の TCP</li> <li>- IPMI - ポート 623 の TCP</li> <li>- リモート制御 - ポート 3888<sup>4</sup> の TCP</li> <li>- リモート KVM - ポート 3889<sup>4</sup> の TCP</li> <li>- CIM HTTP - ポート 5988<sup>3</sup> の TCP</li> <li>- CIM HTTPS - ポート 5989<sup>3</sup> の TCP</li> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- SLP - ポート 427 の UDP/TCP</li> <li>- リモート制御 - ポート 3888<sup>4</sup> の TCP</li> <li>- リモート KVM - ポート 3889<sup>1, 4</sup> の TCP</li> <li>- CIM HTTP - ポート 5988<sup>3</sup> の TCP</li> <li>- CIM HTTPS - ポート 5989<sup>3</sup> の TCP</li> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- SNMP トラップ - ポート 162 の UDP</li> <li>- IPMI - ポート 623 の UDP</li> </ul> |
| インバウンド (XClarity Administrator アプライ) | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>2</sup> の TCP</li> <li>- HTTPS - ポート 443 の TCP</li> </ul>   | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>2</sup> の TCP</li> <li>- HTTPS - ポート 443 の TCP</li> </ul>  | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>2</sup> の TCP</li> <li>- HTTPS - ポート 443 の TCP</li> </ul>  | <ul style="list-style-type: none"> <li>- SNMP トラップ - ポート 162 の UDP</li> </ul>                                 |



| 通信          | ThinkSystem および ThinkAgile   | System x   | Flex System  | ThinkServer |
|-------------|--|--|--|-------------|
| アンスで開いたポート) | <ul style="list-style-type: none"> <li>- SSDP 検出 - ポート 1900 の UDP</li> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> <li>- CIM 表示 HTTPS - TCP 9090</li> <li>- LDAPS - ポート 50636<sup>6</sup>、50637 の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> <li>- CIM 表示 HTTPS - TCP 9090</li> <li>- LDAPS - ポート 50636<sup>6</sup>、50637 の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- ファームウェア更新 - ポート 6990<sup>5</sup> の TCP</li> <li>- CIM 表示 HTTPS - TCP 9090</li> <li>- LDAPS - ポート 50636<sup>6</sup>、50637 の TCP</li> </ul> |             |

1. このポートは、IMM2 を使用するサーバーでのみ開く必要があります。
2. このポートは、SFTP を使用してファームウェア更新プログラムを転送するために使用されます。
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. リモート制御およびリモート KVM は、XClarity Administratorサーバーではなく、Web ブラウザーから起動されます。
5. 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。
6. このポートは、構成パターンを使用してサーバーを構成するために必要です。

● ラック・スイッチおよび Flex スイッチ

| 通信  | ラック・スイッチ  | Flex スイッチ  |
|---|---|--|
| アウトバウンド(外部システムでオープンされるポート)                    | <ul style="list-style-type: none"> <li>- SSH - ポート 22<sup>1, 3</sup> の TCP</li> <li>- SNMP - ポート 161<sup>2</sup> の UDP</li> <li>- SLP - ポート 427<sup>6</sup> の UDP/TCP</li> <li>- HTTPS - ポート 443<sup>7</sup> の TCP</li> </ul> | <ul style="list-style-type: none"> <li>- SSH - ポート 22<sup>3</sup> の TCP</li> <li>- SNMP - ポート 161<sup>5</sup> の UDP</li> </ul>       |
| インバウンド(XClarity Administrator アプライアンスで開いたポート) | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>4</sup> の TCP</li> <li>- SNMP トラップ - ポート 162<sup>2</sup> の TCP</li> </ul>  | <ul style="list-style-type: none"> <li>- SFTP - ポート 22<sup>4</sup> の TCP</li> <li>- SNMP トラップ - ポート 162<sup>2</sup> の TCP</li> </ul> |

1. ENOS ラック・スイッチでは、CMM および Flex スイッチ間で使用されるヘッド・スタック (HoS) 資格情報の構成、ファームウェア・スロットのアクティブ化、および SFTP ファイル転送操作前の SSH ホスト・キーのクリアに、このポートを使用します。
2. スイッチが XClarity Administrator と別のネットワーク上に存在する場合、XClarity Administrator がそのデバイスのイベントを受信できるように、XClarity Administrator アプライアンス (インバウンド) でこのポートを開く必要があります。
3. このポートは管理 (SSH) に使用されます。
4. このポートは、SFTP を使用してファームウェア更新プログラムを転送するために使用されます。
5. ENOS ラック・スイッチの場合、このポートはインベントリ・データの転送に使用されます。
6. このポートは検出に使用されます。
7. このポートは、ファームウェア更新プログラムを適用するために使用されます。

● ストレージ・デバイス

| 通信   | ストレージ・デバイス  |
|--|---|
| アウトバウンド (外部システムでオープンされるポート)                    | <ul style="list-style-type: none"> <li>- FTP - ポート 21 の TCP</li> <li>- SFTP - ポート 22<sup>2</sup> の TCP</li> <li>- SLP - ポート 427 の UDP/TCP</li> <li>- HTTPS - ポート 443<sup>1</sup> の TCP</li> </ul> |
| インバウンド (XClarity Administrator アプライアンスで開いたポート) | <ul style="list-style-type: none"> <li>- HTTPS - ポート 443<sup>2</sup> の TCP</li> <li>- SNMP トラップ - ポート 115 の UDP</li> </ul>  |

1. このポートは、ファームウェア更新プログラムを転送するために使用されます。
2. このポートは、ファームウェア更新プログラムを転送して適用するために使用されます。

## OS デプロイメントとデバイス・ドライバーの更新のための XClarity Administrator とデータ・ネットワーク間のアクセス

| 通信   | OS デプロイメント <sup>1, 2, 3</sup>  | OS デバイス・ドライバーの更新 <sup>2</sup>   |
|--|--|---|
| アウトバウンド (外部システムでオープンされるポート)                    |  | <ul style="list-style-type: none"> <li>• HTTP 経由の WinRM - ポート 5985<sup>5</sup> の TCP</li> <li>• HTTPS 経由の WinRM - ポート 5986<sup>6</sup> の TCP</li> </ul> |
| インバウンド (XClarity Administrator アプライアンスで開いたポート) | <ul style="list-style-type: none"> <li>• SMB 通信 - ポート 445<sup>4</sup> の TCP</li> <li>• HTTPS (ThinkServer を除く) - ポート 8443<sup>6</sup> の TCP</li> </ul> | <ul style="list-style-type: none"> <li>• SMB 通信 - ポート 445<sup>4</sup> の TCP</li> </ul>  |

1. オペレーティング・システム・デプロイメント・ネットワークを使用するように XClarity Administrator を構成している場合は、そのネットワークでポートが開いている必要があります。
2. オペレーティング・システムのデプロイに利用する必要があるポートの一覧については、XClarity Administrator オンライン・ドキュメントの「[デプロイされたオペレーティング・システムで利用可能なポート](#)」を参照してください。たとえば、データ・ネットワーク (eth1) を使用するようにオペレーティング・システム・デプロイメントを構成している場合は、そのネットワークでこれらのポートが開いている必要があります。
3. 各 XClarity Administrator インスタンスには、OS デプロイメントでのみ使用される固有証明機関 (CA) があります。その CA がポート 8443 のターゲット・サーバーに使用する証明書に署名します。OS デプロイメントが開始されると、CA 証明書は、ターゲット・サーバーにプッシュされた OS イメージに含まれます。デプロイメント・プロセスの一部として、サーバーは、ポート 8443 に接続しなおされ、CA 証明書があるため、ハンドシェイク中にポート 8443 が提供した証明書が検証されます。
4. このポートは、Windows ドライバー・ファイルの転送に使用されます。
5. このポートは、ターゲット・サーバー WinRM に接続するために使用されます。
6. このポートは、ターゲット OS と XClarity Administrator の間でデータ (OS イメージとステータスを含む) を交換するために使用されます。

## 管理に関する考慮事項

デバイスを管理する場合は、選択肢がいくつかあります。管理されているデバイスによっては、複数の管理ソリューションを同時に実行する必要がある場合もあります。

デバイスの管理に使用できる Lenovo XClarity Administrator のインスタンスは 1 つだけです。ただし、他の管理ソフトウェア (VMware vRealize Operations Manager など) を Lenovo XClarity Administrator と一緒に使用して、XClarity Administrator が管理するデバイスを監視できます。

**注意：**複数の管理ツールを使用してデバイスを管理する場合は、予期できない競合を防ぐため十分に注意してください。たとえば、別のツールを使用して電源状態の変更を送信すると、XClarity Administrator で実行されている構成ジョブや更新ジョブと競合する可能性があります。

## ThinkSystem、ThinkServer、および System x デバイス

別の管理ソフトウェアを使用して管理対象デバイスを監視する場合、IMM インターフェースから適切な SNMP または IPMI を使用して新しいローカル・ユーザーを作成します。必要に応じて、必ず SNMP または IPMI 特権を付与してください。

## Flex System デバイス

別の管理ソフトウェアを使用して管理対象デバイスを監視する場合、およびその管理ソフトウェアで SNMPv3 または IPMI 通信が使用されている場合は、各管理対象 CMM で以下の手順を実行して環境を準備する必要があります。

1. RECOVERY\_ID のユーザー名とパスワードを使用して、シャーシの管理コントローラー Web インターフェースにログインします。
2. セキュリティー・ポリシーが「**保護**」に設定されている場合は、ユーザー認証方式を変更します。
  - a. 「**管理モジュールの管理**」 → 「**ユーザー・アカウント**」をクリックします。
  - b. 「**アカウント**」タブをクリックします。
  - c. 「**グローバル・ログイン設定**」をクリックします。
  - d. 「**General**」タブをクリックします。
  - e. ユーザー認証方式で「**最初に外部認証、次にローカル認証**」を選択します。
  - f. 「**OK**」をクリックします。
3. 管理コントローラー Web インターフェースから正しい SNMP または IPMI 設定で新規のローカル・ユーザーを作成します。
4. セキュリティー・ポリシーが「**保護**」に設定されている場合は、管理コントローラー Web インターフェースからログアウトし、新規ユーザー名とパスワードを使用してログインします。プロンプトが表示されたら、新規ユーザーのパスワードを変更します。

これで、新規ユーザーをアクティブな SNMP または IPMI ユーザーとして使用できます。

**注：**シャーシを管理対象から除外して再度管理対象にした場合、この新規ユーザー・アカウントはロックされ無効になります。この場合、手順を繰り返して新規ユーザー・アカウントを作成してください。

---

## ネットワークに関する考慮事項

Lenovo XClarity Administrator のインストールを計画するときは、環境に実装されているするネットワーク・トポロジーと、XClarity Administrator をそのトポロジー内にどのように収めるかを考慮してください。

**重要：**デバイスとコンポーネントは、IP アドレスの変更が最小限で済むように構成します。動的ホスト構成プロトコル (DHCP) ではなく、静的 IP アドレスを使用することを検討してください。DHCP が使用されている場合は、IP アドレスの変更が最小限に抑えられていることを確認します。

## IP 構成の制限

以下の機能および管理対象デバイスについては、ネットワーク・インターフェースは、IPv4 アドレスを使用して構成する必要があります。IPv6 アドレスはサポートされていません。

- Lenovo Storage デバイスのファームウェア更新
- ThinkServer サーバー
- Lenovo Storage デバイス

データ・ポートまたは管理ポート経由の IPv6 リンク・ローカルを使用した RackSwitch デバイスの管理はサポートされていません。

1つのIPアドレス・スペースを別のIPアドレス・スペースに再マップするネットワーク・アドレス変換(NAT)はサポートされていません。

## ネットワーク・タイプ

通常は、ほとんどの環境で以下のネットワーク・タイプが実装されています。要件に応じて、これらのネットワークのいずれか1つのみを実装する場合もあれば、3つすべてを実装する場合もあります。

### • 管理ネットワーク

管理ネットワークは、通常、Lenovo XClarity Administrator と管理対象デバイスの管理プロセッサの間の通信用に予約されています。たとえば、管理ネットワークは、XClarity Administrator、各管理対象シャーシのCMM、およびXClarity Administratorが管理する各サーバーのベースボード管理コントローラーが含まれるように構成されている場合があります。

### • データ・ネットワーク

データ・ネットワークは、通常、サーバーにインストールされているオペレーティング・システムと会社のイントラネットまたはインターネット(あるいはその両方)の間の通信に使用されます。

### • オペレーティング・システム・デプロイメント・ネットワーク

場合によっては、オペレーティング・システム・デプロイメント・ネットワークが、サーバーへのオペレーティング・システムのデプロイに必要な通信を分離するように実装されていることがあります。実装されている場合、このネットワークには、通常、XClarity Administrator とすべてのサーバー・ホストが含まれます。

オペレーティング・システム・デプロイメント・ネットワークを別途実装する代わりに、この機能を管理ネットワークまたはデータ・ネットワークに組み込むこともできます。

## ネットワーク構成

1つまたは2つのネットワーク・インターフェースを使用するようにLenovo XClarity Administratorを構成できます。

### 注意：

- デバイスの管理後にXClarity Administrator IPアドレスを変更すると、XClarity Administratorでデバイスがオフライン状態になります。IPアドレスを変更する前に、すべてのデバイスを管理対象から除外してください。
- 「重複するIPアドレスをチェック」トグルをクリックして、同じサブネット内のIPアドレスの重複のチェックを有効または無効にできます。これは、デフォルトでは無効になっています。有効にすると、XClarity AdministratorのIPアドレスを変更しようとした場合、または管理対象の他のデバイスや同じサブネットにある他のデバイスと同じIPアドレスを持つデバイスを管理しようとした場合、XClarity Administratorによってアラートが出されます。

注：有効にすると、XClarity AdministratorはARPスキャンを実行して同じサブネット上のアクティブなIPv4デバイスを検索します。ARPスキャンを防ぐには、**重複IPアドレスのチェック**を無効にします。

- XClarity Administratorを仮想アプライアンスとして実行する場合、管理ネットワークのネットワーク・インターフェースがDHCP(Dynamic Host Configuration Protocol)を使用するように設定されている場合は、DHCPのリースの有効期限が切れると管理インターフェースのIPアドレスが変更される可能性があります。IPアドレスが変更された場合は、シャーシ、ラック・サーバー、タワー・サーバーを管理解除してから、再度管理対象にする必要があります。この問題を避けるには、管理インターフェースを静的IPアドレスに変更するか、DHCPアドレスがMACアドレスに基づくように、またはDHCPリースの有効期限が切れないようにDHCPサーバー構成が設定されていることを確認します。
- オペレーティング・システムのデプロイやOSデバイス・ドライバの更新にXClarity Administratorを使用しない場合は、ネットワーク・インターフェースを「ハードウェアの検出と管理のみ」オプションを使用するように変更することで、SambaおよびApacheサーバーを無効にできます。ネットワーク・インターフェースを変更すると管理サーバーは再起動されます。

- XClarity Administrator をコンテナとして実行する場合は、以下の点に注意してください。
  - 行うことができるのは、重複 IP アドレスのチェックの有効化または無効化、ネットワーク・インターフェースの役割の変更、プロキシ設定の変更のみです。その他のネットワーク設定 (IP アドレス、ゲートウェイ、DNS など) は、コンテナのセットアップ時に定義します。
  - macvlan ネットワークがホスト・システムでセットアップされている必要があります。

XClarity Administrator では、実装するネットワーク・トポロジーに応じて、環境で2つのネットワーク・インターフェースを定義することができます。仮想アプライアンスの場合、これらのネットワーク・インターフェース名は eth0 と eth1 です。コンテナの場合は、カスタム名を選択できます。

- 1つのネットワーク・インターフェース (eth0) のみが存在する場合:
  - (サーバーの構成、ファームウェアの更新など) デバイスの検出と管理をサポートするようにインターフェースを構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーのベースボード管理コントローラー、各 RackSwitch スイッチと通信する必要があります。
  - XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
  - サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティーを含む) 自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。
  - オペレーティング・システム・イメージをデプロイし、OS デバイス・ドライバーを更新する場合は、このネットワーク・インターフェースに、ホスト・オペレーティング・システムへのアクセスに使用されるサーバーのネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

- 2つのネットワーク・インターフェース (eth0 と eth1) が存在する場合:
  - 最初のネットワーク・インターフェース (通常は Eth0 インターフェース) は、管理ネットワークに接続し、デバイスの検出と管理 (サーバーの構成およびファームウェアの更新を含む) をサポートするように構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーの管理コントローラー、各 RackSwitch スイッチと通信する必要があります。
  - セカンド・ネットワーク・インターフェース (通常は eth1 インターフェース) は、内部データ・ネットワークまたはパブリック・データ・ネットワーク、あるいはその両方と通信するように構成できます。
  - XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
  - サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティーを含む) 自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。
  - オペレーティング・システム・イメージをデプロイして、デバイス・ドライバーを更新する場合は、eth1 または eth0 のいずれかのインターフェースを使用することもできます。ただし、使用するインターフェースでは、ホスト・オペレーティング・システムへのアクセスに使用されるサーバー・ネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

次の表に、環境に実装されているネットワーク・トポロジーのタイプに基づく、XClarity Administrator ネットワーク・インターフェースの考えられる構成を示します。この表を使用して、各ネットワーク・インターフェースの定義方法を確認してください。

表 2. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割

| ネットワーク・トポロジー   | インターフェース 1 (eth0) の役割   | インターフェース 2 (eth1) の役割   |
|--|---|---|
| コンバージド・ネットワーク (OS デプロイメントと OS デバイス・ドライバーの更新をサポートする管理およびデータ・ネットワーク) | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティなど)</li> <li>保証データの取得</li> <li>OS デプロイメント</li> <li>OS デバイス・ドライバーの更新</li> </ul> | なし  |
| OS デプロイメントと OS デバイス・ドライバーの更新をサポートする個別の管理ネットワークとデータ・ネットワーク          | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティなど)</li> <li>保証データの取得</li> <li>OS デプロイメント</li> <li>OS デバイス・ドライバーの更新</li> </ul> | データ・ネットワーク <ul style="list-style-type: none"> <li>なし</li> </ul>                                   |
| OS デプロイメントと OS デバイス・ドライバーの更新をサポートする個別の管理ネットワークとデータ・ネットワーク          | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティなど)</li> <li>保証データの取得</li> </ul>   | データ・ネットワーク <ul style="list-style-type: none"> <li>OS デプロイメント</li> <li>OS デバイス・ドライバーの更新</li> </ul> |
| OS デプロイメントと OS デバイス・ドライバーの更新をサポートしない個別の管理ネットワークとデータ・ネットワーク         | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティなど)</li> <li>保証データの取得</li> </ul>   | データ・ネットワーク <ul style="list-style-type: none"> <li>なし</li> </ul>                                   |
| 管理ネットワークのみ (OS デプロイメントおよび OS デバイス・ドライバーの更新はサポートされません)              | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティなど)</li> <li>保証データの取得</li> </ul>   | なし  |

## 単一データ/管理ネットワーク

このネットワーク・トポロジーでは、管理およびデータの通信とオペレーティング・システム・デプロイメントが同じネットワークで行われます。このトポロジーは、**統合ネットワーク**と呼ばれます。

**重要：**共用データ/管理ネットワークを実装すると、ネットワーク構成(サーバーからのトラフィックの優先順位が高く、管理コントローラーからのトラフィックの優先順位が低い場合など)によっては、トラフィックが中断し、パケットのドロップや管理ネットワークの接続の問題などが発生することがあります。管理ネットワークは、TCP だけでなく UDP トラフィックを使用します。ネットワーク・トラフィックの優先順位が高い場合は、UDP トラフィックの優先順位が低くなります。

Lenovo XClarity Administrator をインストールする際に、以下の考慮事項を念頭に置いて eth0 ネットワーク・インターフェースを定義してください。

- (サーバーの構成、ファームウェアの更新など) デバイスの検出と管理をサポートするようにインターフェースを構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーのベースボード管理コントローラー、各 RackSwitch スイッチと通信する必要があります。
- XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも 1 つのネットワーク・インターフェースが(できればファイアウォールを介して)インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
- サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティを含む)自動問題通知を使用する場合は、少なくとも 1 つのネットワーク・インターフェースが(できればファイアウォールを介して)インターネットに接続している必要があります。
- オペレーティング・システム・イメージをデプロイし、OS デバイス・ドライバーを更新する場合は、このネットワーク・インターフェースに、ホスト・オペレーティング・システムへのアクセスに使用されるサーバーのネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

- XClarity Administrator は、単一データ/管理ネットワーク・トポロジーまたは仮想的に分離したデータ/管理ネットワーク・トポロジーを実装している場合にのみ、XClarity Administrator の要件を満たす管理対象サーバーなどのシステムにセットアップできます。ただし、XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。その場合も、一部のファームウェアのみが即時アクティベーションで適用され、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。

XClarity Administrator から同じネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成して、冗長性をサポートすることもできます。

次の図は、統合ネットワーク・トポロジーの実装例を示しています。

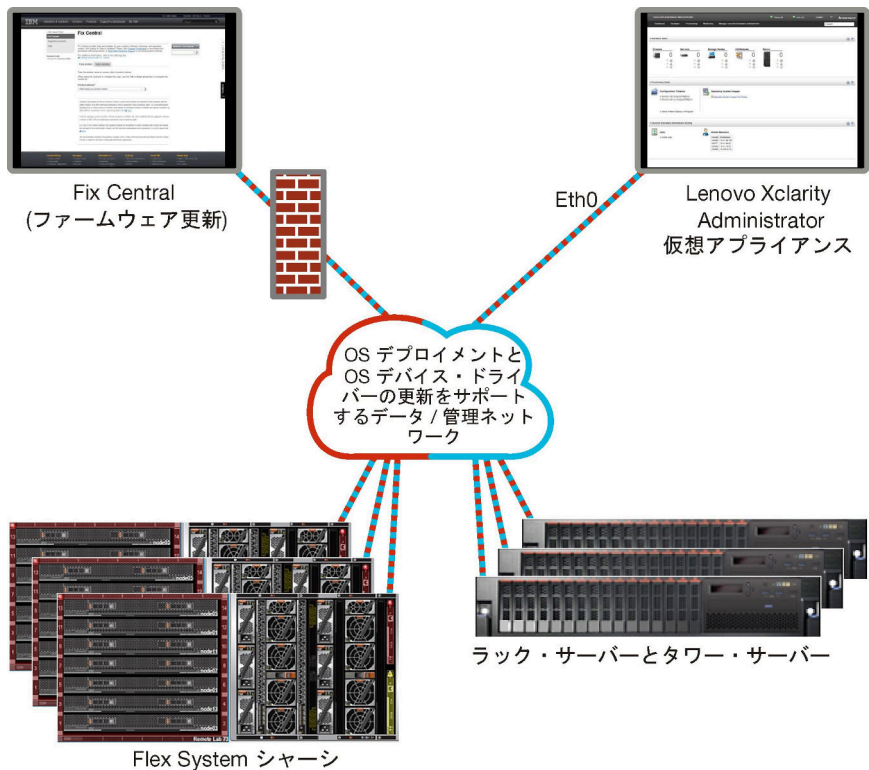


図1. 管理、データ、オペレーティング・システムのデプロイメントのための単一のネットワークの実装例

## 物理的に分離したデータ/管理ネットワーク

このネットワーク・トポロジでは、管理ネットワークとデータ・ネットワークは物理的に分離したネットワークで、オペレーティング・システム・デプロイメント・ネットワークは管理ネットワークまたはデータ・ネットワークの一部として構成されています。

Lenovo XClarity Administrator をインストールする際に、以下の考慮事項を念頭に置いてネットワーク設定を定義してください。

- 最初のネットワーク・インターフェース (通常は Eth0 インターフェース) は、管理ネットワークに接続し、デバイスの検出と管理 (サーバーの構成およびファームウェアの更新を含む) をサポートするように構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーの管理コントローラー、各 RackSwitch スイッチと通信できる必要があります。
- セカンド・ネットワーク・インターフェース (通常は eth1 インターフェース) は、内部データ・ネットワークまたはパブリック・データ・ネットワーク、あるいはその両方と通信するように構成できます。
- XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
- サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティを含む) 自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。
- オペレーティング・システム・イメージをデプロイして、デバイス・ドライバーを更新する場合は、eth1 または eth0 のいずれかのインターフェースを使用することもできます。ただし、使用するインターフェースでは、ホスト・オペレーティング・システムへのアクセスに使用されるサーバー・ネットワーク・インターフェースへの IP ネットワーク接続が必要です。



注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

23 ページの 図 2「物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部)」は、分離した管理ネットワークとデータ・ネットワークの実装例です。この例では、オペレーティング・システム・デプロイメント・ネットワークが、データ・ネットワークの一部として構成されています。

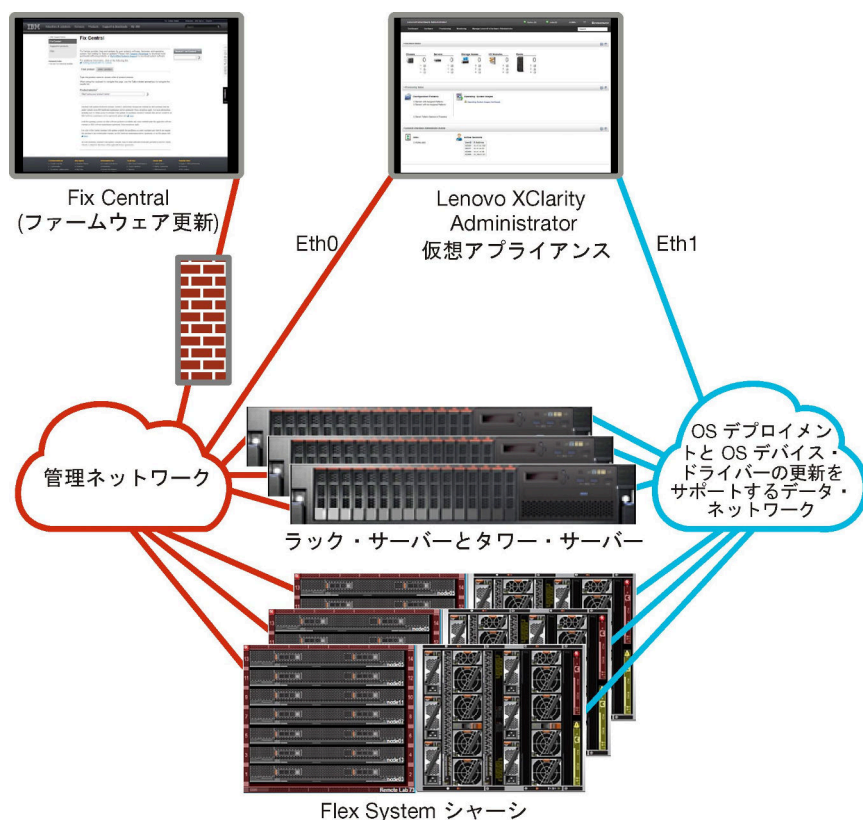


図 2. 物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部)

24 ページの 図 3「物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部)」も、分離した管理ネットワークとデータ・ネットワークの実装例です。この例では、オペレーティング・システム・デプロイメント・ネットワークが、管理ネットワークの一部として構成されています。この実装では、XClarity Administrator にデータ・ネットワークへの接続は必要ありません。

注：オペレーティング・システム・デプロイメント・ネットワークがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加のインターフェースを構成して、サーバーのホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

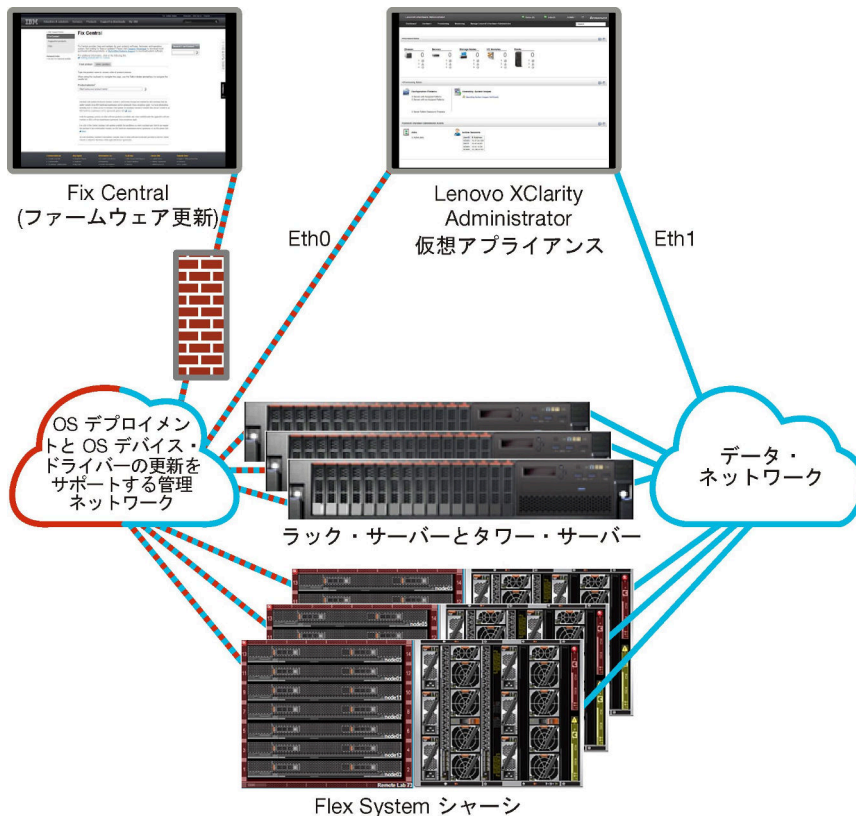


図3. 物理的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部)

### 仮想的に分離したデータ/管理ネットワーク

このトポロジーでは、データ・ネットワークと管理ネットワークが仮想的に分離しています。データ・ネットワークの packets と管理ネットワークの packets は、同じ物理接続を介して送信されるため、2つのネットワーク間でトラフィックを区別するために、すべての管理ネットワーク・データ・packet で VLAN タグ付けが使用されます。

注：Lenovo XClarity Administrator が、シャーシ内の管理対象サーバーで実行されているホストにインストールされている場合、XClarity Administrator を使用して、そのシャーシ全体にファームウェア更新を一度に適用することはできません。ファームウェア更新が適用されたら、ホスト・システムを再起動する必要があります。

XClarity Administrator をインストールする際に、以下の考慮事項を念頭に置いてネットワーク設定を定義してください。

- 最初のネットワーク・インターフェース (通常は Eth0 インターフェース) は、管理ネットワークに接続し、デバイスの検出と管理 (サーバーの構成およびファームウェアの更新を含む) をサポートするように構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーの管理コントローラー、各 RackSwitch スイッチと通信できる必要があります。
- セカンド・ネットワーク・インターフェース (通常は eth1 インターフェース) は、内部データ・ネットワークまたはパブリック・データ・ネットワーク、あるいはその両方と通信するように構成できます。
- XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。

- サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティーを含む) 自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが(できればファイアウォールを介して) インターネットに接続している必要があります。
- オペレーティング・システム・イメージをデプロイして、デバイス・ドライバーを更新する場合は、eth1 または eth0 のいずれかのインターフェースを使用することもできます。ただし、使用するインターフェースでは、ホスト・オペレーティング・システムへのアクセスに使用されるサーバー・ネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

- XClarity Administrator は、単一データ/管理ネットワーク・トポロジーまたは仮想的に分離したデータ/管理ネットワーク・トポロジーを実装している場合にのみ、XClarity Administrator の要件を満たす管理対象サーバーなどのシステムにセットアップできます。ただし、XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。その場合も、一部のファームウェアのみが即時アクティベーションで適用され、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。

26 ページの 図 4 「仮想的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部)」 は、仮想的に分離した管理ネットワークとデータ・ネットワークの実装例です。この例では、オペレーティング・システム・デプロイメント・ネットワークが、データ・ネットワークの一部として構成されています。また、XClarity Administrator は、シャーシ内の管理対象サーバーにインストールされています。

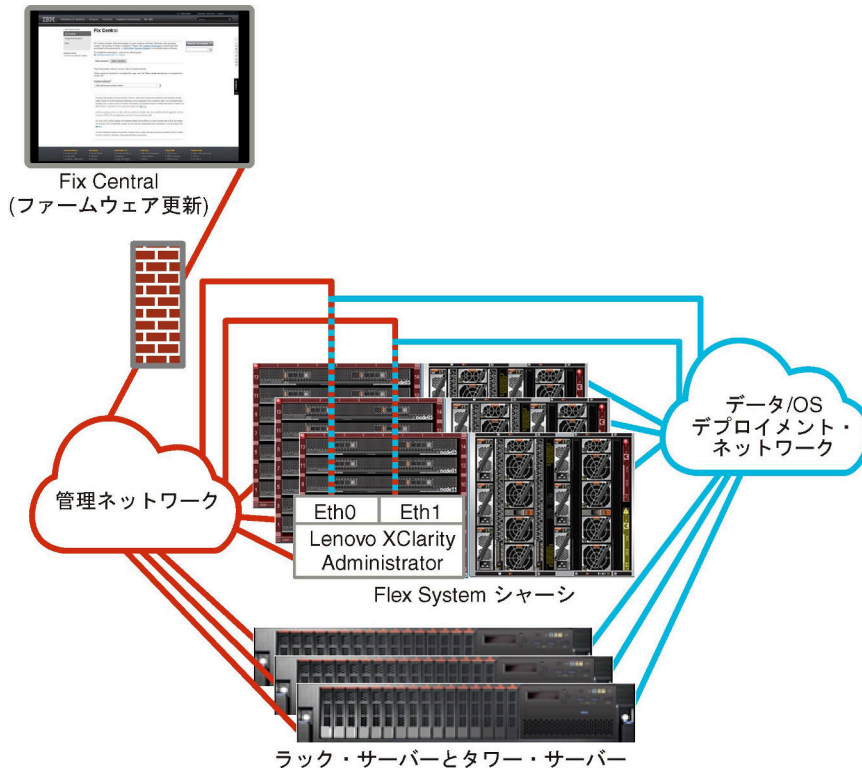


図4. 仮想的に分離したデータ/管理ネットワークの実装例 (オペレーティング・システム・ネットワークはデータ・ネットワークの一部)

27 ページの 図5「仮想的に分離した管理ネットワークとデータ・ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部)」は、仮想的に分離した管理ネットワークとデータ・ネットワークの実装例です。この例では、オペレーティング・システム・デプロイメント・ネットワークが、管理ネットワークの一部として構成されています。また、XClarity Administrator は、シャーシ内の管理対象サーバーにインストールされています。この実装では、XClarity Administrator にデータ・ネットワークへの接続は必要ありません。

注：オペレーティング・システム・デプロイメント・ネットワークがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加のインターフェースを構成して、サーバーのホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。



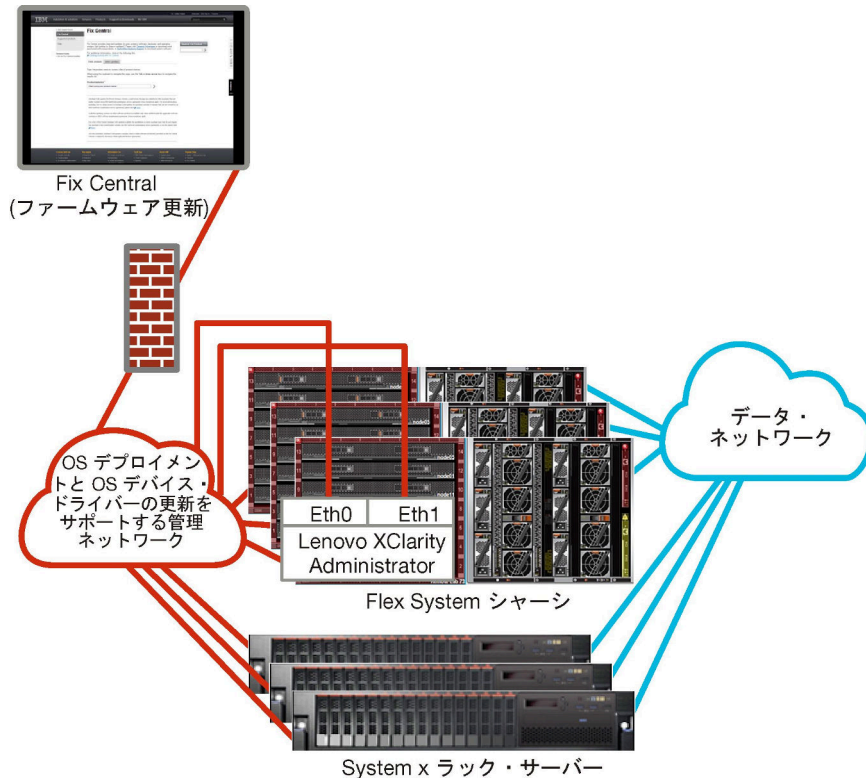


図 5. 仮想的に分離した管理ネットワークとデータ・ネットワークの実装例 (オペレーティング・システム・ネットワークは管理ネットワークの一部)

## 管理専用ネットワーク

このトポロジーでは、Lenovo XClarity Administrator は管理ネットワークにのみアクセスできます。このトポロジーでは、データ・ネットワークにアクセスすることはできません。ただし、XClarity Administrator から管理対象サーバーにオペレーティング・システム・イメージをデプロイする場合、XClarity Administrator はオペレーティング・システム・デプロイメント・ネットワークにアクセスする必要があります。

XClarity Administrator をインストールしてネットワーク設定を定義する際に、Eth0 ネットワーク・インターフェースを次のように構成する必要があります。

- (サーバーの構成、ファームウェアの更新など) デバイスの検出と管理をサポートするようにインターフェースを構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーのベースボード管理コントローラー、各 RackSwitch スイッチと通信する必要があります。
- XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバの更新を取得する場合は、少なくとも 1 つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
- サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティを含む) 自動問題通知を使用する場合は、少なくとも 1 つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。
- オペレーティング・システム・イメージをデプロイし、OS デバイス・ドライバを更新する場合は、このネットワーク・インターフェースに、ホスト・オペレーティング・システムへのアクセスに使用されるサーバーのネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワー

ク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

XClarity Administrator から同じネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成して、冗長性をサポートすることもできます。

28 ページの 図 6 「オペレーティング・システム・デプロイメントをサポートしない管理専用ネットワークの実装例」は管理専用ネットワークの実装例です。このネットワークでは、XClarity Administrator からのオペレーティング・システム・デプロイメントはサポートされていません。

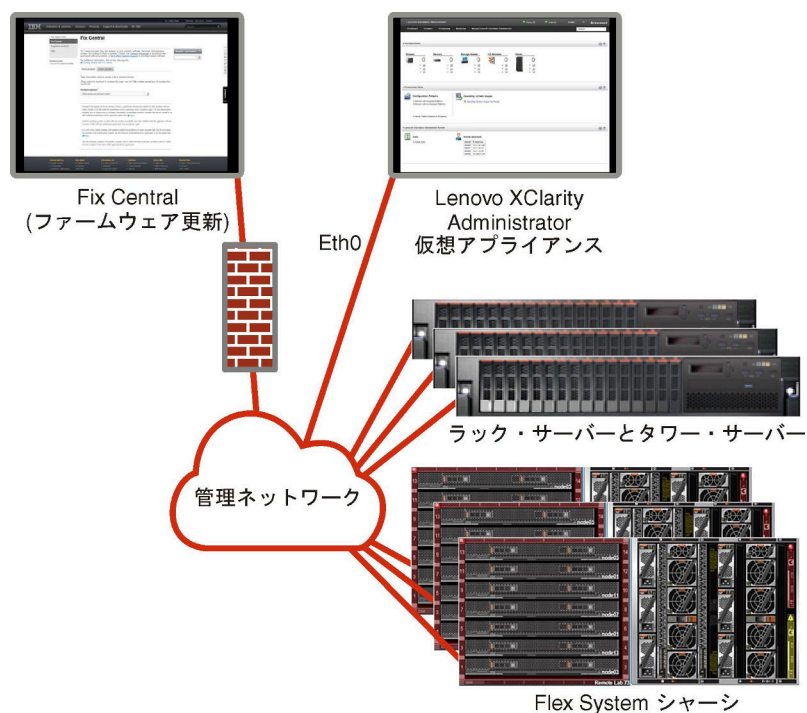


図 6. オペレーティング・システム・デプロイメントをサポートしない管理専用ネットワークの実装例

28 ページの 図 6 「オペレーティング・システム・デプロイメントをサポートしない管理専用ネットワークの実装例」は管理専用ネットワークの実装例です。このネットワークでは、XClarity Administrator からのオペレーティング・システム・デプロイメントがサポートされています。

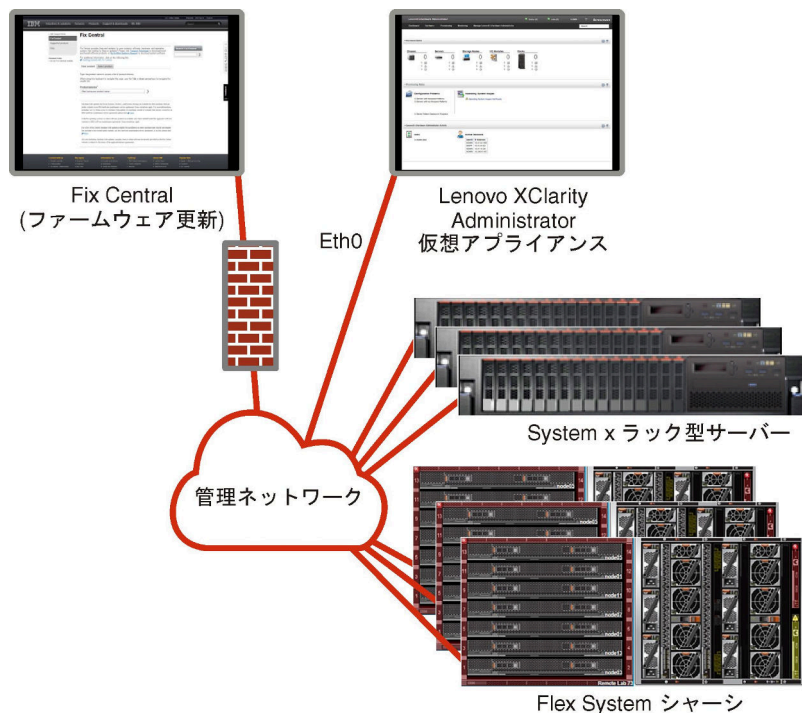


図7. オペレーティング・システム・デプロイメントをサポートする管理専用ネットワークの実装例

## セキュリティに関する考慮事項

Lenovo XClarity Administrator とすべての管理対象デバイスのセキュリティの計画を立てます。

### Encapsulation の管理

Lenovo XClarity Administrator 内の Lenovo シャーシおよびサーバーを管理する場合、Lenovo XClarity Administrator のデバイスのファイアウォール規則を変更して、Lenovo XClarity Administrator からの受信要求のみを受け入れるように構成できます。これは、「*encapsulation*」と呼ばれます。また、既に Lenovo XClarity Administrator によって管理されているシャーシおよびサーバーでの *encapsulation* を有効または無効にできます。

*encapsulation* をサポートするデバイスで *encapsulation* が有効になっている場合、Lenovo XClarity Administrator はデバイスの *encapsulation* モードを「*encapsulationLite*」に変更し、この Lenovo XClarity Administrator からの受信要求のみに制限するためデバイスのファイアウォール規則を変更します。

無効にされた場合、*encapsulation* モードは「通常」に設定されます。*encapsulation* がデバイスに以前に使用可能にされていた場合は、*encapsulation* のファイアウォール規則が削除されます。

**注意：** *encapsulation* が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、*encapsulation* を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、[管理サーバーの障害発生後の CMM による シャーシ管理のリカバリー](#) および [XClarity Administrator オンライン・ドキュメントの管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー](#) を参照してください。

**注：**

- Encapsulation は、スイッチ、ストレージ・デバイスおよび Lenovo 以外のシャーシおよびサーバーではサポートされていません。

- 動的ホスト構成プロトコル (DHCP) を使用するように管理ネットワーク・インターフェースを構成し、encapsulation を有効にすると、ラック・サーバーの管理に長時間かかります。

encapsulation について詳しくは、XClarity Administrator オンライン・ドキュメントの[Encapsulation の有効化](#)を参照してください。

## 暗号管理

暗号化管理は、Lenovo XClarity Administrator と管理対象デバイス (シャーシ、サーバー、Flex スイッチなど) の間のセキュアな通信の処理方法を制御する通信モードとプロトコルで構成されています。

### 暗号化アルゴリズム

XClarity Administrator では、セキュアなネットワーク接続用に TLS 1.2 およびより強力な暗号アルゴリズムをサポートしています。

セキュリティを強化するため、強度の高い暗号のみがサポートされています。クライアント・オペレーティング・システムと Web ブラウザーが、以下のいずれかの暗号スイートをサポートしていなければなりません。

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

### 管理サーバーの暗号モード

この設定は、管理サーバーからのセキュアな通信に使用されるモードを判断します。

- 「**互換性**」。デフォルトのモードです。このモードは、NIST SP 800-131A への準拠のために必要とされる厳格なセキュリティ規格を満たしていない旧バージョンのファームウェア、ブラウザ、およびその他のネットワーク・クライアントと互換性があります。
- **NIST SP 800-131A**。このモードは、NIST SP 800-131A 規格への準拠を目的としています。XClarity Administrator は、必ず強力な暗号化を内部的に使用するように、また、可能な場合は、強力な暗号化ネットワーク接続を使用するように設計されています。ただし、このモードでは、NIST SP 800-131A で承認されていない暗号化を使用したネットワーク接続は許可されていません。これには、SHA-1 または弱いハッシュで署名されたトランスポート層セキュリティ (TLS) 証明書の拒否が含まれます。

このモードを選択した場合:

- ポート 8443 以外のすべてのポートでは、すべての TLS CBC 暗号および PFS (Perfect Forward Secrecy) をサポートしないすべての暗号が無効になります。
- 一部のモバイル・デバイス・サブスクリプションでは、イベント通知が正常にプッシュされない可能性があります (XClarity Administrator オンライン・ドキュメントの[モバイル・デバイスへのイベントの転送](#)を参照)。Android や iOS などの外部デバイスは、SHA-1 (NIST SP 800-131A モードのより厳しい要件に従わないアルゴリズム) で署名された証明書を提示します。その結果、これらのサービスに対して行われる接続が、証明書例外またはハンドシェイク・エラーで失敗する可能性があります。

NIST SP 800-131A への準拠について詳しくは、XClarity Administrator オンライン・ドキュメントの[NIST 800-131A コンプライアンスの実装](#)を参照してください。



管理サーバーのセキュリティ設定について詳しくは、XClarity Administrator オンライン・ドキュメントの「[暗号モードと通信プロトコルの設定](#)」を参照してください。

### 管理対象サーバーのセキュリティ・モード

この設定は、管理対象サーバーからのセキュアな通信に使用されるモードを判断します。

- **互換性セキュリティ**。サービスおよびクライアントで CNSA/FIPS 準拠ではない暗号化が必要な場合に、このモードを選択します。このモードでは、広範な暗号化アルゴリズムがサポートされており、すべてのサービスを有効にできます。
- 「NIST SP 800-131A」。NIST SP 800-131A 基準に確実に準拠するには、このモードを選択してください。これには、RSA 鍵が 2048 ビット以上であること、デジタル署名に用いるハッシュ値は SHA-256 で得られる値以上の長さであること、NIST が承認している対称暗号アルゴリズムのみを使用することなどの制限が課されます。このモードは、SSL/TLS モードを「**TLS 1.2 サーバーおよびクライアント**」に設定する必要があります。

このモードは、XCC2 を持つサーバーではサポートされていません。

- **標準セキュリティ**。(XCC2 を持つサーバーのみ) これは、XCC2 を含むサーバーのデフォルトのセキュリティ・モードです。FIPS 140-3 基準に確実に準拠するには、このモードを選択してください。XCC を FIPS 140-3 検証モードで動作させるには、FIPS 140-3 レベルの暗号化をサポートするサービスのみが有効にできます。FIPS 140-2/140-3 レベル暗号化をサポートしないサービスは、デフォルトでは無効になっていますが、必要な場合は有効にできます。FIPS 140-3 レベル以外の暗号化を使用するサービスが有効になっている場合、XCC は FIPS 140-3 検証モードでは動作できません。このモードでは、FIP レベルの証明書が必要です。
- **エンタープライズ・ストリクト・セキュリティ**。(XCC2 を含むサーバーのみ) これは、最もセキュアなモードです。CNSA 基準に確実に準拠するには、このモードを選択してください。CNSA レベルの暗号化をサポートするサービスのみ使用できます。非セキュア・サービスは、デフォルトでは無効になっており、有効にすることはできません。このモードでは、CNSA レベルの証明書が必要です。

XClarity Administrator は「**エンタープライズ・ストリクト・セキュリティ**」モードのサーバーに RSA-3072/SHA-384 証明書の署名を使用します。

#### 重要：

- このモードを使用するには、選択したそれぞれの XCC2 を含むサーバーに XCC2 Feature On Demand キーがインストールされていなければなりません。
- このモードで XClarity Administrator が自己署名証明書を使用する場合は、XClarity Administrator は RSA3072/SHA384 ベースのルート証明書とサーバー証明書を使用する必要があります。XClarity Administrator が外部署名済み証明書を使用する場合は、XClarity Administrator は RSA3072/SHA384 ベースの CSR を生成し、外部 CA に問い合わせ、RSA3072/SHA384 に基づく新しいサーバー証明書に署名する必要があります。
- XClarity Administrator が RSA3072/SHA384 ベースの証明書を使用する場合、XClarity Administrator は Flex System シャーシ (CMMS) サーバーおよびサーバー、ThinkSystem サーバー、ThinkServer サーバー、System x M4 および M5 サーバー、Lenovo ThinkSystem DB シリーズ・スイッチ、Lenovo RackSwitch、Flex System スイッチ、Mellanox スイッチ、ThinkSystem DE/DM ストレージ・デバイス、IBM テープ・ライブラリー・ストレージ、および 22C 以前のファームウェアがフラッシュされた ThinkSystem SR635/SR655 サーバー以外のデバイスを切断する可能性があります。切断されたデバイスの管理を続行するには、RSA2048/SHA384 ベースの証明書を使用して別の XClarity Administrator インスタンスをセットアップしてください。

暗号モードを変更する際の考慮事項を以下に示します。

- 「互換性セキュリティ」モードまたは「標準セキュリティ」モードから「エンタープライズ・ストリクト・セキュリティ」モードへの変更はサポートされていません。

- 「互換性セキュリティー」モードから「標準セキュリティー」モードにアップグレードする場合、インポートされた証明書または SSH 公開鍵が適合しない場合に警告が表示されますが、「標準セキュリティー」モードにアップグレードすることはできます。
- 「エンタープライズ・ストリクト・セキュリティー」モードから「互換性セキュリティー」モードまたは「標準セキュリティー」モードにダウングレードする場合:
  - セキュリティー・モードを有効にするために、サーバーが自動的に再起動されます。
  - Strict モードの FoD キーが XCC2 で欠落しているか有効期限が切れている場合、および XCC2 が自己署名 TLS 証明書を使用する場合、XCC2 は Standard Strict に準拠するアルゴリズムに基づいて自己署名証明書を再生成します。XClarity Administrator は、証明書エラーによる接続障害を表示します。信頼できない証明書のエラーを解決するには、XClarity Administrator オンライン・ドキュメントの「[非トラステッド・サーバー証明書の解決](#)」を参照してください。XCC2 がカスタム TLS 証明書を使用する場合、XCC2 はダウングレードを許可し、「標準セキュリティー」モードの暗号化に基づいてサーバー証明書をインポートする必要があるという警告が表示されます。
- 「NIST SP 800-131A」モードは、XCC2 を持つサーバーではサポートされていません。
- XClarity Administrator の暗号モードが TLS v1.2 に設定され、管理対象認証を使用する管理対象サーバーのセキュリティー・モードが TLS v1.2 に設定されている場合、XClarity Administrator または XCC のいずれかを使用してサーバーのセキュリティー・モードを TLS v1.3 に変更すると、サーバーは永続的にオフラインになります。
- XClarity Administrator の暗号モードが TLS v1.2 に設定され、セキュリティー・モードが TLS v1.3 に設定されている XCC を使用してサーバーを管理しようとしても、管理対象認証を使用してサーバーを管理することはできません。

次のデバイスのセキュリティー設定は変更できます。

- インテルまたは AMD プロセッサーを搭載した Lenovo ThinkSystem サーバー (SR635 / SR655 を除く)
- Lenovo ThinkSystem V2 サーバー
- インテルまたは AMD プロセッサーを搭載した Lenovo ThinkSystem V3 サーバー
- Lenovo ThinkEdge SE350 / SE450 サーバー
- Lenovo System x サーバー

管理サーバーのセキュリティー設定について詳しくは、XClarity Administrator オンライン・ドキュメントの「[サーバーのセキュリティー設定の構成](#)」を参照してください。

## セキュリティー証明書

Lenovo XClarity Administrator は SSL 証明書を使用して、XClarity Administrator とその管理対象デバイス (System x サーバーのシャーシやサービス・プロセッサーなど) との間で信頼できる安全な通信を確立するだけでなく、ユーザーや他のサービスと XClarity Administrator の通信も同様に確立します。デフォルトでは、XClarity Administrator、CMM、およびベースボード管理コントローラーは、内部証明機関で発行された自己署名 XClarity Administrator 生成証明書を使用します。

XClarity Administrator の各インスタンスに固有で生成されるデフォルトの自己署名サーバー証明書によって、多くの環境で十分なセキュリティーが提供されます。また、XClarity Administrator で証明書を管理できるほか、サーバー証明書をカスタマイズしたり置き換えたりすることもできます。XClarity Administrator には、環境に合わせて証明書をカスタマイズするオプションが用意されています。たとえば、以下のオプションがあります。

- 組織に固有の値を使用する内部証明機関やエンド・サーバーの証明書を再生成して、新しいキーのペアを生成できます。
- 選択した証明機関に送信できる証明書署名要求 (CSR) を生成してカスタムの証明書に署名し、それを XClarity Administrator にアップロードしてホストしているすべてのサービスでエンド・サーバー証明書として使用できます。
- サーバー証明書をローカル・システムにダウンロードして、その証明書を Web ブラウザーの信頼できる証明書のリストにインポートできます。

証明書について詳しくは、XClarity Administrator オンライン・ドキュメントの[セキュリティー証明書の使用](#)を参照してください。

## 認証

### サポートされる認証サーバー

認証サーバーとは、ユーザー資格情報の認証に使用されるユーザー・レジストリーです。Lenovo XClarity Administrator は以下のタイプの認証サーバーをサポートしています。

- **ローカル認証サーバー**デフォルトでは、XClarity Administrator は、管理サーバーにある組み込みの LDAP (Lightweight Directory Access Protocol) サーバーを使用するように構成されています。
- **外部 LDAP サーバー**。現在、Microsoft Active Directory および OpenLDAP トラップのみがサポートされています。このサーバーは、管理ネットワークに接続している外部の Microsoft Windows サーバーに存在している必要があります。外部 LDAP サーバーが使用されている場合、ローカル認証サーバーは無効になります。

注意：ログイン資格情報を使用するように Active Directory のバインディング方式を構成するには、各管理対象サーバーのベースド管理コントローラーで 2016 年 9 月以降のファームウェアが実行されている必要があります。

- **外部 ID 管理システム**。現在、CyberArk のみサポートされます。

ThinkSystem または ThinkAgile サーバーのユーザー・アカウントが CyberArk にオンボードされている場合、サーバーを管理用に最初に設定しているときに XClarity Administrator CyberArk からサーバーにログインするための資格情報を取得するように選択できます。CyberArk から資格情報を取得する前に、XClarity Administrator で CyberArk パスを定義し、クライアント証明書を介して TLS 相互認証を使用して、CyberArk と XClarity Administrator の間で相互信頼を確立する必要があります。

- **外部 SAML ID プロバイダー**現在、Microsoft Active Directory Federation Services (AD FS) のみサポートされます。ユーザー名とパスワードを入力するほか、PIN コードの要求やスマート・カードやクライアント証明書の読み込みによる追加セキュリティーを有効にするマルチファクター認証をセットアップできます。SAML ID プロバイダーが使用されている場合、ローカル認証サーバーは無効になりません。外部認証が使用できない場合に、PowerShell および REST API 認証、およびリカバリーのために管理対象シャーシまたはサーバーに直接ログインするには (そのデバイスで Encapsulation が有効になっている場合を除く)、ローカル・ユーザー・アカウントが必要です。

外部 LDAP サーバーおよび外部 ID プロバイダーの両方を使用するように選択できます。両方とも有効である場合は、外部 LDAP サーバーが管理対象デバイスへの直接ログインに使用され、ID プロバイダーは管理サーバーへのログインに使用されます。

認証サーバーについて詳しくは、XClarity Administrator オンライン・ドキュメントの[認証サーバーの管理](#)を参照してください。

### デバイス認証

デフォルトでは、デバイスは XClarity Administrator 管理対象認証を使用したデバイスへのログインを使用して管理されます。ラック・サーバーおよび Lenovo シャーシを管理する場合、デバイスへのログインにローカル認証を使用するか管理対象認証を使用するかを選択できます。

- **ラック・サーバー、Lenovo シャーシ、および Lenovo ラック・スイッチにローカル認証が使用されている場合**、XClarity Administrator はデバイスに対する認証に保存された資格情報を使用します。保存された資格情報は、デバイスのアクティブなユーザー・アカウントまたは Active Directory サーバーのユーザー・アカウントにできます。

ローカル認証を使用してデバイスを管理する前に、デバイスのアクティブ・ユーザー・アカウントまたは Active Directory サーバーのユーザー・アカウントに一致する、XClarity Administrator に保存される資格情報を作成する必要があります (XClarity Administrator オンライン・ドキュメントの[保存された資格情報の管理](#)を参照)。

注：

- RackSwitch デバイスは、認証用にのみ保存される資格情報をサポートします。XClarity Administrator ユーザー資格情報はサポートされていません。
- **管理対象認証**を使用することで、ローカル認証資格情報の代わりに、XClarity Administrator 認証サーバーの資格情報により、複数のデバイスを管理および監視できます。デバイス (ThinkServer サーバー、System x M4 サーバー、およびスイッチを除く) で管理対象認証が使用されている場合、XClarity Administrator は、そのデバイスとそこに取り付けられているコンポーネントを、集中型管理用の XClarity Administrator 認証サーバーを使用するように構成します。

- 管理対象認証が有効な場合、手動で入力した資格情報か、保存された資格情報のいずれかを使用してデバイスを管理できます (XClarity Administrator オンライン・ドキュメントの [ユーザー・アカウントの管理](#) および [保存された資格情報の管理](#) を参照)。

保存された資格情報は、XClarity Administrator が、デバイスの LDAP 設定を構成するまでの間のみ使用されます。その後は、保存された資格情報を変更しても、デバイスの管理または監視に影響しません。

注：デバイスに対して管理対象認証が有効になっている場合、XClarity Administrator を使用してそのデバイスの保管された資格情報を編集することはできません。

- XClarity Administrator 認証サーバーとしてローカルまたは外部 LDAP サーバーを使用している場合は、その認証サーバーで定義されているユーザー・アカウントが XClarity Administrator ドメイン内の XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されます。ローカルの CMM および管理コントローラー・ユーザー・アカウントは無効になります。
- XClarity Administrator 認証サーバーとして SAML 2.0 ID プロバイダーを使用する場合、SAML アカウントは、管理対象デバイスにアクセスできなくなります。ただし、SAML ID プロバイダーと LDAP サーバーを同時に使用する場合で、ID プロバイダーが LDAP サーバーにあるアカウントを使用する場合、LDAP ユーザー・アカウントを使用して管理対象デバイスにログインできます。また、SAML 2.0 が提供するより高度な認証方法 (マルチファクター認証およびシングル・サインオンなど) を使用して XClarity Administrator にログインすることもできます。
- シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます (XClarity Administrator オンライン・ドキュメントの「[サーバーの管理](#)」を参照)

注：認証に CyberArk ID 管理システムを使用すると、シングル・サインオンは自動的に無効になります。

- ThinkSystem SR635 および SR655 サーバーで管理対象認証が有効になっている場合:
  - ベースボード管理コントローラー・ファームウェアは、最大 5 つの LDAP ユーザー・ロールをサポートします。XClarity Administrator は、管理中に次の LDAP ユーザー・ロールをサーバーに追加します: `lxc-supervisor`、`lxc-sysmgr`、`lxc-admin`、`lxc-fw-admin` および `lxc-os-admin`。  
ThinkSystem SR635 および SR655 サーバーと通信するには、指定された少なくとも 1 つの LDAP ユーザー・ロールにユーザーが割り当てられている必要があります。
  - 管理コントローラーのファームウェアは、サーバーのローカル・ユーザーと同じユーザー名の LDAP ユーザーをサポートしていません。
- ThinkServer サーバーおよび System x M4 サーバーの場合は、XClarity Administrator 認証サーバーは使用しません。その代わりに、デバイスで接頭辞「LXCA\_」の後にランダムな文字列が続く IPMI アカウントが作成されます。(既存の IPMI ローカル・ユーザー・アカウントは無効になります。)ThinkServer サーバーを管理解除する場合は、「LXCA\_」ユーザー・アカウントが無効になり接



頭辞「LXCA\_」が接頭辞「DISABLED\_」に置き換えられます。ThinkServer サーバーが別のインスタンスによって管理されているかどうかを判別するために、XClarity Administrator は接頭辞「LXCA\_」がついた IPMI アカウントを確認します。管理対象 ThinkServer サーバーの管理を強制することを選択した場合、そのデバイスで「LXCA\_」がついたすべての IPMI アカウントが無効になり名前を変更されます。不要になった IPMI アカウントを手動で消去することを検討してください。

手動で入力した資格情報を使用する場合、XClarity Administrator は自動的に保存された資格情報を作成し、その保存された資格情報を使用してデバイスを管理します。

注：デバイスに対して管理対象認証が有効になっている場合、XClarity Administrator を使用してそのデバイスの保管された資格情報を編集することはできません。

- 手動で入力した認証情報を使用してデバイスを管理するたびに、以前の管理プロセス中にそのデバイス用に別の保存済み認証情報が作成されていても、そのデバイス用に新しい保存済み認証情報が作成されます。
- デバイスを管理解除しても、XClarity Administrator は、管理プロセス中にそのデバイス用に自動的に作成され保管されている資格情報を削除しません。

## リカバリー・ユーザー・アカウント

リカバリー・パスワードを指定すると、XClarity Administrator ではローカル CMM または管理コントローラー・ユーザー・アカウントが無効になり、デバイスで新しいリカバリー・ユーザー・アカウント (RECOVERY\_ID) が作成され以降の認証に使用されます。管理サーバーで障害が発生した場合は、この RECOVERY\_ID アカウントを使用してデバイスにログインし、リカバリー操作を実行して、管理ノードが復旧または交換されるまでデバイスのアカウント管理機能を復元できます。

RECOVERY\_ID ユーザー・アカウントを持つデバイスを管理解除すると、すべてのローカル・ユーザー・アカウントが有効になり、RECOVERY\_ID アカウントが削除されます。

- 無効になっているローカル・ユーザー・アカウントに変更を加えても (パスワードを変更するなど)、RECOVERY\_ID アカウントには影響しません。管理対象認証モードで使用できるアクティブなユーザー・アカウントは、RECOVERY\_ID アカウントだけです。
- RECOVERY\_ID アカウントは緊急時にのみ使用します (管理サーバーで障害が発生した場合、ネットワークの問題によってデバイスがユーザー認証のために XClarity Administrator に接続できない場合など)。
- デバイスを検出したときに RECOVERY\_ID パスワードが指定されます。後で使用できるように記録しておいてください。

デバイス管理のリカバリーについては、XClarity Administrator オンライン・ドキュメントの[管理サーバーの障害発生後の CMM による シャーシ管理のリカバリー](#)および[管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー](#)を参照してください。

## ユーザー・アカウントと役割グループ

ユーザー・アカウントは、Lenovo XClarity Administrator とすべての管理対象シャーシおよびサーバーにログインしたり、それらを管理したりするために使用されます。XClarity Administrator のユーザー・アカウントには、認証と許可という、互いに依存する 2 つのプロセスが適用されます。

**認証**は、ユーザーの資格情報の確認に使用されるセキュリティ・メカニズムです。認証プロセスでは、構成された認証サーバーに保存されているユーザー資格情報を使用されます。これにより、許可されていない管理サーバーや、管理対象システムの不正なアプリケーションによるリソースへのアクセスも防止されます。認証が完了すると、ユーザーは XClarity Administrator にアクセスできるようになります。ただし、特定のリソースにアクセスしたり、特定のタスクを実行したりするには、適切な許可も必要です。

**許可**では、認証されたユーザーの権限を確認して、役割グループのメンバーシップに基づいてリソースへのアクセスを制御します。**役割グループ**は、認証サーバーで定義および管理されているユーザー・アカウントのセットに特定の役割を割り当てるために使用されます。たとえば、スーパーバイザー権限を持つ

役割グループのメンバーになっているユーザーは、XClarity Administrator でユーザー・アカウントの作成、編集、削除を行うことができます。オペレーター権限を持っているユーザーは、ユーザー・アカウント情報の表示のみを行うことができます。

ユーザー・アカウントと役割グループについては、XClarity Administrator オンライン・ドキュメントの[ユーザー・アカウントの管理](#)を参照してください。

## ユーザー・アカウント・セキュリティー

ユーザー・アカウントの設定は、パスワードの複雑さ、アカウントのロックアウト、Web 非アクティブ・セッションのタイムアウトを制御します。アカウント・セキュリティー設定の値は変更できます。

アカウント・セキュリティー設定については、Lenovo XClarity Administrator オンライン・ドキュメントの[ユーザー・アカウントのセキュリティー設定の変更](#)を参照してください。

---

## 高可用性に関する考慮事項

Lenovo XClarity Administrator の高可用性を実装するには、ホスト・オペレーティング・システムまたはコンテナ環境の高可用性機能を使用します。

### Docker

Docker Datacenter を使用して、Docker Engine で実行される XClarity Administrator コンテナの高可用性環境を実装できます。Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー](#) および[アプリ Web ページ](#)を参照してください。

### Citrix

Citrix 環境用に提供されている高可用性機能を使用します。詳しくは、XClarity Administrator オンライン・ドキュメントの[高可用性の実装 \(Citrix\)](#)を参照してください。

### KVM (CentOS、RedHat、Ubuntu)

OpenStack を使用できます。また、既に高可用性環境がある場合は、引き続き内部プロセスを使用できます。OpenStack の高可用性について詳しくは、XClarity Administrator オンライン・ドキュメントの[高可用性の実装 \(KVM\)](#)を参照してください。

### Microsoft Hyper-V

ESXi 環境用に提供されている高可用性機能を使用します。詳しくは、XClarity Administrator オンライン・ドキュメントの[高可用性の実装 \(Microsoft Hyper-V\)](#)を参照してください。

### Nutanix AHV

Nutanix AHV 環境用に提供されている仮想マシン高可用性機能を使用します。詳しくは、XClarity Administrator オンライン・ドキュメントの[高可用性の実装 \(Nutanix\)](#)を参照してください。

### VMware ESXi

VMware High Availability 環境では、複数のホストがクラスターとして構成されます。クラスター内のホストに仮想マシン (VM) のディスク・イメージを利用できるように、共有ストレージが使用されません。VM は一度に 1 台のホストでのみ実行されます。VM に問題があると、その VM の別のインスタンスがバックアップ・ホストで起動されます。

VMware High Availability には以下のコンポーネントが必要です。

- ESXi がインストールされている最低 2 台のホスト。これらのホストは VMware クラスターの一部になります。
- VMware vCenter がインストールされている 3 台目のホスト。

**ヒント:** このホストには必ず、クラスター内で使用するホストにインストールされている ESXi のバージョンと互換性のある、VMware vCenter のバージョンをインストールしてください。

VMware vCenter は、クラスター内で使用するいずれかのホストにインストールしてもかまいません。ただし、そのホストが電源オフまたは使用不可になると、VMware vCenter インターフェースへのアクセスも失うことになります。

- クラスター内のすべてのホストからアクセスできる共有ストレージ(データストア)。VMware によってサポートされているいずれのタイプの共有ストレージも使用できます。VMware はデータストアを使用して、VM が別のホストにフェイルオーバーする必要があるかどうかを調べます(ハートビート)。

VMware High Availability クラスターのセットアップについては、XClarity Administrator オンライン・ドキュメントの [高可用性の実装 \(VMware ESXi\)](#) を参照してください。

---

## Features on Demand

Features on Demand では、ハードウェアを取り付けたり新しい装置を購入する必要なく、機能をアクティブ化します。このアクティベーションは、対応する Features on Demand キーを取得してインストールすることで実行されます。

Lenovo XClarity Administrator でリモート制御およびオペレーティング・システム・デプロイメント操作を使用するには、サーバーの XClarity Controller Enterprise レベルおよび MM 拡張アップグレードを有効にする必要があります。これは、デフォルトでアクティブ化されている機能には付属していません。これらの操作では、リモート・プレゼンスの Features on Demand キーが ThinkSystem サーバー、コンバージド・サーバーおよび System x サーバーにインストールされている必要もあります。「サーバー」ページから、リモート・プレゼンスの有効化または無効化を行うか、あるいはサーバーにインストールしないことを選択できます(XClarity Administrator オンライン・ドキュメントの [管理対象サーバーのステータスの表示](#) を参照)。

一部の拡張サーバーの機能は Features on Demand キーを使用してアクティブ化されます。機能に UEFI セットアップ中に提示される構成可能な設定が存在する場合、構成パターンを使用して設定を構成できます。ただし、設定した構成は対応する Features on Demand キーがインストールされるまでアクティブ化されません。

**注:** XClarity Administrator からは Features on Demand キーをインストールまたは管理できません。ただし、管理対象サーバーに現在インストールされている Features on Demand キーのリストを表示することはできます。インストールされている Features on Demand キーの表示について詳しくは、XClarity Administrator オンライン・ドキュメントの [Feature on Demand キーの表示](#) を参照してください。

Features on Demand キーを取得およびインストールするには:

1. 適切な部品番号を使用して、Features on Demand アップグレードを購入します。  
キーは [Features on Demand Web ポータル](#) から購入できます。購入が完了すると、認証コードがメールで送信されます。
2. [Features on Demand Web ポータル](#) で、受け取った認証コードと、アップグレードするサーバーの一意的システム ID を入力します。
3. アクティベーション・キー(.KEY ファイル)をダウンロードします。
4. アクティベーション・キーを、サーバーの管理コントローラーにアップロードします。
5. サーバーを再起動します。再起動が完了すると、機能がアクティブになります。

Features on Demand キーについて詳しくは、[Lenovo Features on Demand の使用](#) を参照してください。





---





## 第 3 章 Docker、CentOS、Citrix、Red Hat KVM、Rocky、Ubuntu、VMware ESXi、または Windows Hyper-V 環境での Lenovo XClarity Administrator

管理可能なデバイスをネットワークに接続し、それらのデバイスを管理するように Lenovo XClarity Administrator 仮想アプライアンスを設定するには、いくつかの方法があります。このセクションの情報を参考にして、Docker、CentOS、Citrix、Red Hat KVM、Ubuntu、VMware ESXi、または Windows Hyper-V 環境に管理可能なデバイスを設定し、XClarity Administrator

このセクションでは、いくつかの一般的なトポロジーのセットアップ方法について説明します。このセクションは、使用できるすべてのネットワーク・トポロジーに対応しているわけではありません。

**注意：**デバイスを管理するには、XClarity Administrator から管理ネットワークにアクセスできる必要があります。

詳細:

-  [VMware vCenter への Lenovo XClarity Administrator のインストール](#)
-  [VMware vSphere への Lenovo XClarity Administrator のインストール](#)
-  [Windows Hyper-V への Lenovo XClarity Administrator のインストール](#)
-  [Red Hat KVM への Lenovo XClarity Administrator のインストール](#)

---

### 単一データ/管理ネットワーク

このネットワーク・トポロジーでは、データ・ネットワークと管理ネットワークは同じネットワークです。

#### 始める前に

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します (XClarity Administrator オンライン・ドキュメントの[利用可能なポート](#))。

XClarity Administrator を使用して管理する各デバイスに、最小限必要なファームウェアがインストールされていることを確認します。[XClarity Administrator のサポート - 互換性に関する Web ページ](#)から最小限必要なレベルのファームウェアを見つけるには、「互換性」タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

**重要：**デバイスとコンポーネントは、IP アドレスの変更が最小限で済むように構成します。動的ホスト構成プロトコル (DHCP) ではなく、静的 IP アドレスを使用することを検討してください。DHCP が使用されている場合は、IP アドレスの変更が最小限に抑えられていることを確認します。

#### このタスクについて

仮想アプライアンスの場合、XClarity Administrator とネットワークとの間のすべての通信は、ホストの eth0 ネットワーク・インターフェースを介して行われます。コンテナの場合は、カスタム名を使用できます。この例では、eth0 を使用します。

**重要：**共用データ/管理ネットワークを実装すると、ネットワーク構成 (サーバーからのトラフィックの優先順位が高く、管理コントローラーからのトラフィックの優先順位が低い場合など) によっては、トラフィックが中断し、パケットのドロップや管理ネットワークの接続の問題などが発生することがあります。管理ネットワークは、TCP だけでなく UDP トラフィックを使用します。ネットワーク・トラフィックの優先順位が高い場合は、UDP トラフィックの優先順位が低くなります。

次の図では、データ・ネットワークと管理ネットワークが同じネットワークである場合に、運用環境をセットアップする方法の1つを示しています。図の番号は、以下のセクションにある番号付きの手順に対応しています。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、ラック・サーバー、ラック・スイッチ、Flex スイッチ、CMM の配線オプション要件のうち、単一データ/管理ネットワークのセットアップに関連するものだけを示しています。

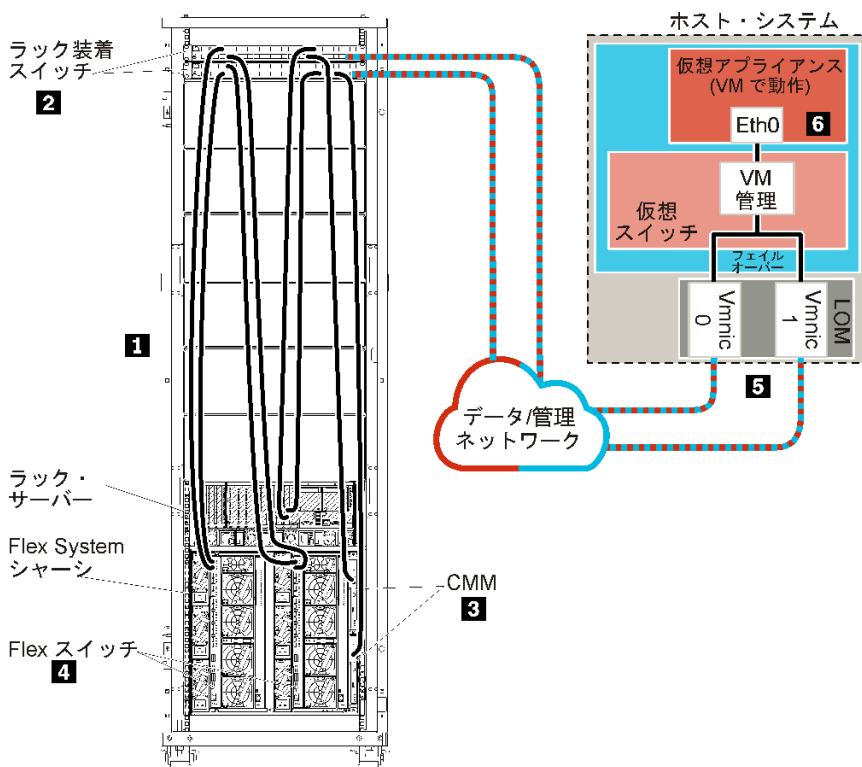


図8. 仮想アプライアンスの単一データ/管理ネットワーク・トポロジーの例

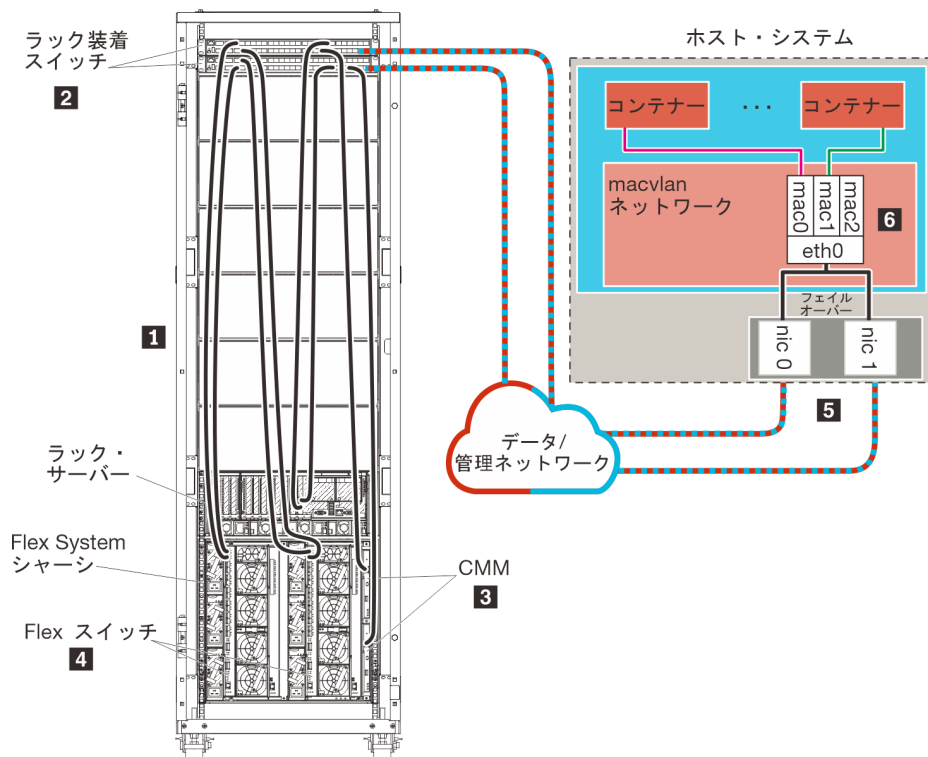


図9. コンテナの単一データ/管理ネットワーク・トポロジーの例

**重要：**管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジーまたは単一データ/管理ネットワーク・トポロジーのいずれかを実装できます。
- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用されるときであっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」→「計算ノード」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

XClarity Administrator をインストールして、既に構成済みのシャーシとラック・サーバーを管理する場合は、[手順 5: ホストのインストールと構成](#)に進みます。

ネットワーク設定や Eth1 と Eth0 の構成に関する情報など、このトポロジーの計画の追加情報については、[単一データ/管理ネットワーク](#)を参照してください。

## 手順 1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線

シャーシ、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチに配線して、デバイスとネットワークとが通信できるようにします。

## 手順

各シャーシ内の各 Flex スイッチと CMM、各ラック・サーバー、XClarity Administrator ホスト内から両方のラック装着スイッチに配線します。ラック装着スイッチの任意のポートを選択できます。

次の図は、シャーシ (Flex スイッチと CMM)、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチへの配線を示す例です。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、ラック・サーバー、ラック・スイッチ、Flex スイッチ、CMM の配線オプション要件のうち、単一データ/管理ネットワークのセットアップに関連するものだけを示しています。

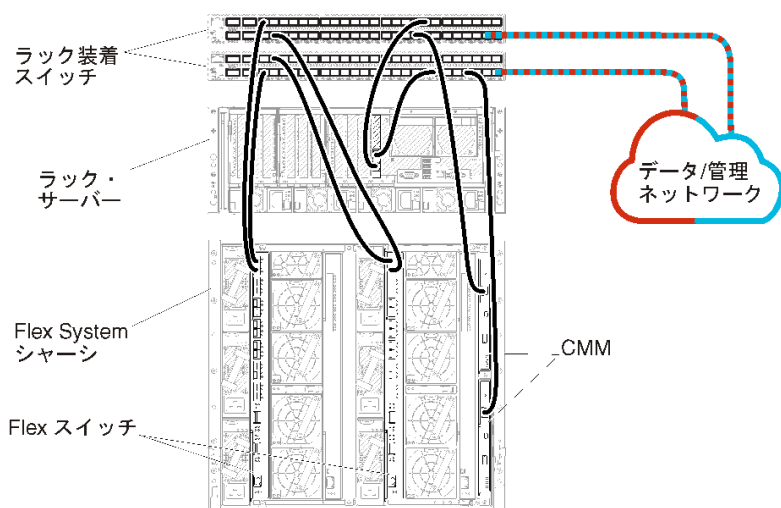


図 10. 単一データ/管理ネットワークの配線の例

## 手順 2: ラック装着スイッチの構成

ラック装着スイッチを構成します。

### 始める前に

ラック装着スイッチの一般的な構成要件を満たしていることに加えて、Flex スイッチ、ラック・サーバー、ネットワークへの外部ポートと、CMM、ラック・サーバー、ネットワークへの内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

## 手順

構成手順は、取り付けられたラック・スイッチの種類によって異なることがあります。

Lenovo ラック装着スイッチの構成については、[System x オンライン・ドキュメントのラック装着スイッチ](#)を参照してください。その他のラック装着スイッチが取り付けられている場合は、そのスイッチに付属のドキュメントを参照してください。

## 手順 3: Chassis Management Module (CMM) の構成

シャーシ内のすべてのデバイスを管理するように、シャーシ内のプライマリー Chassis Management Module (CMM) を構成します。

### このタスクについて

CMM の構成について詳しくは、[Flex System のシャーシ・コンポーネントの構成 オンライン・ドキュメント](#)を参照してください。

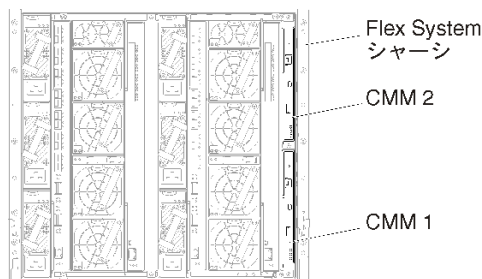
さらに、シャーシに付属の操作指示ポスターで手順 4.1 ~ 4.5 も参照してください。

## 手順

CMM を構成するには、以下の手順を実行します。

2 台の CMM を取り付けている場合、プライマリー CMM のみを構成してください。プライマリー CMM からスタンバイ CMM に構成は自動的に同期されます。

ステップ 1. ベイ 1 内の CMM からクライアント・ワークステーションにイーサネット・ケーブルを直接接続します。



初めて CMM に接続するには、クライアント・ワークステーションでインターネット・プロトコルのプロパティの変更が必要になる場合があります。

**重要：**クライアント・ワークステーション・サブネットが CMM サブネットと同じであることを確認してください(デフォルトの CMM サブネットは 255.255.255.0 です)。クライアント・ワークステーション用に選択する IP アドレスは CMM と同じネットワークに属する必要があります (192.168.70.0 ~ 192.168.70.24 など)。

ステップ 2. CMM 管理インターフェースを起動するには、クライアント・ワークステーションで Web ブラウザーを開き、CMM の IP アドレスを参照します。

注：

- セキュアな接続を使用し、URL に **https** を含めていることを確認します (https://192.168.70.100 など)。https を含めていない場合、ページが見つからないことを示すエラーが表示されます。
- デフォルトの IP アドレスである 192.168.70.100 を使用している場合、CMM 管理インターフェースが利用可能になるまでに数分かかることがあります。この遅延が発生するのは、CMM がデフォルトの静的アドレスにフォールバックするまでの 2 分間、DHCP アドレスを取得しようとするためです。

ステップ 3. デフォルトのユーザー ID (USERID) とパスワード (PASSWORD) を使用して CMM 管理インターフェースにログインします。ログイン後、デフォルトのパスワードを変更する必要があります。

ステップ 4. CMM 初期セットアップ・ウィザードの残りの手順を実行して、運用環境の詳細を指定します。初期セットアップ・ウィザードでは、必要に応じて以下の操作を実行することができます。

- シャーシのインベントリーと正常性を表示する。
- 既存の構成ファイルから構成をインポートする。
- CMM の全般設定を構成する。
- CMM の日付と時刻を構成する。

ヒント: XClarity Administratorのインストール時には、XClarity Administrator だけでなく XClarity Administrator のすべての管理対象シャーシでも NTP サーバーが使用されるように構成します。

- CMM の IP 情報を構成する。
- CMM のセキュリティー・ポリシーを構成する。
- ドメイン・ネーム・システム (DNS) を構成する。
- イベント・フォワーダーを構成する。

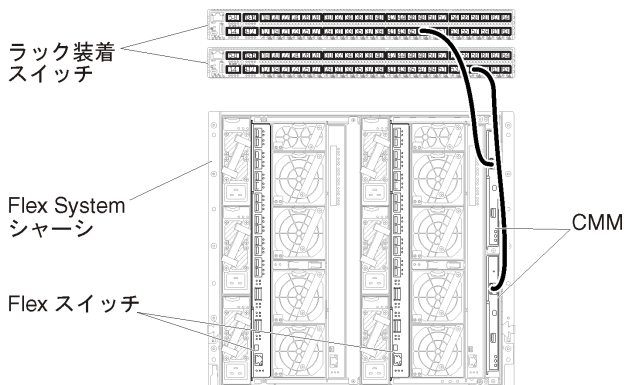
ステップ 5. セットアップ・ウィザードの設定を保存し、変更を適用した後、シャーシ内のすべてのコンポーネントの IP アドレスを構成します。

シャーシに付属の操作指示ポスターで手順 4.6 を参照してください。

注: 新しい IP アドレスを表示するには、各計算ノードのシステム管理プロセッサをリセットし、Flex スイッチを再起動する必要があります。

ステップ 6. CMM 管理インターフェースを使用して CMM を再起動します。

ステップ 7. CMM が再起動されたら、CMM のイーサネット・ポートから運用ネットワークにケーブルを接続します。



ステップ 8. 新しい IP アドレスを使用して CMM 管理インターフェースにログインします。

## 終了後

冗長性がサポートされるように CMM を構成することもできます。以下の各ページで使用できるフィールドについて詳しくは、CMM のヘルプ・システムを使用してください。

- プライマリー CMM にハードウェア障害が発生した場合の CMM のフェイルオーバーを構成します。CMM 管理インターフェースで、「管理モジュールの管理」 → 「プロパティ」 → 「拡張フェイルオーバー」をクリックします。
- ネットワークに問題が発生した場合のフェイルオーバー (アップリンク) を構成します。CMM 管理インターフェースで、「管理モジュールの管理」 → 「ネットワーク」をクリックし、「イーサネット」タブをクリックして、「拡張イーサネット」をクリックします。少なくとも、必ず「物理ネットワーク・リンクの消失した場合のフェイルオーバー」を選択します。

## 手順 4: Flex スイッチの構成

各シャーシで Flex スイッチ (I/O モジュール) を構成します。

### 始める前に

Flex スイッチからラック装着スイッチへの外部ポート、CMM への内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。



Flex スイッチが動的ネットワーク設定 (IP アドレス、ネットマスク、ゲートウェイ、DNS アドレス) を取得するようにセットアップする場合、Flex スイッチが一貫した設定になるようにする必要があります (たとえば、IP アドレスは CMM と同じサブネット内にある必要があります)

**重要：** Flex System シャーシごとに、シャーシ内の各サーバーの拡張カードのファブリック・タイプが、同じシャーシ内のすべての Flex スイッチのファブリック・タイプと互換性があることを確認します。たとえば、イーサネット・スイッチをシャーシに取り付ける場合、そのシャーシ内のすべてのサーバーは、LAN-on-motherboard コネクタまたはイーサネット拡張カードを介してイーサネットに接続できる必要があります。Flex スイッチの構成について詳しくは、[Flex Systems オンライン・ドキュメントの I/O モジュールの構成](#)を参照してください。

## 手順

構成手順は、取り付けられた Flex スイッチの種類によって異なることがあります。サポートされる各 Flex スイッチについて詳しくは、[Flex Systems オンライン・ドキュメントの Flex System ネットワーク・スイッチ](#)を参照してください。

通常、Flex スイッチ・ベイ 1 と 2 の Flex スイッチを構成する必要があります。

**ヒント:** シャーシの背面から見ると、Flex スイッチ・ベイ 2 は 3 番目のモジュール・ベイです。

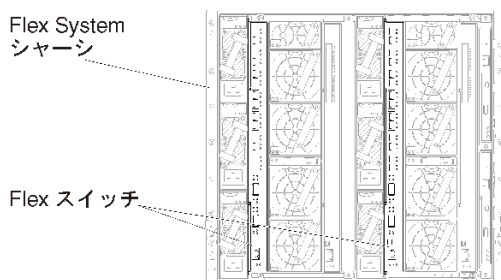


図 11. シャーシにおける Flex スイッチの場所

## 手順 5: ホストのインストールと構成

Lenovo XClarity Administrator の要件を満たす任意のサーバーに Docker をインストールできます。

### 始める前に

Docker Datacenter を使用して、Docker Engine で実行される XClarity Administrator コンテナの高可用性環境を実装できます。Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー およびアプリ Web ページ](#)を参照してください。

[ハードウェアおよびソフトウェアの必須条件](#)で定義されている前提条件をホストが満たしていることを確認します。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

**重要：** 管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジーまたは単一データ/管理ネットワーク・トポロジーのいずれかを実装できます。

- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用されるときであっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」 → 「計算ノード」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

## 手順

お使いの Docker ディストリビューションにより提供されている手順を使用して、ホストに Docker をインストールして構成します。

## 手順 6: XClarity Administrator のインストールと構成

Lenovo XClarity Administrator コンテナを、前の手順でインストールした Docker ホストにインストールして構成します。

### 始める前に

ホスト・システムがハードウェアとソフトウェアの最小要件を満たしていることを確認します ([ハードウェアおよびソフトウェアの必須条件](#) を参照)。

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します ([利用可能なポート](#) を参照)。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

ホスト OS と XClarity Administrator は、同じ NTP サーバーを使用する必要があります。

XClarity Administrator では、データの管理、ハードウェアの管理、OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 を使用します。

macvlan ネットワークがホスト・システムのカーネルにロードされている必要があります。ロードされているかどうかを確認するには、`lsmod | grep macvlan` コマンドを使用します。macvlan をカーネルにロードするには、`modprobe macvlan` コマンドを実行します。

同じホストで複数の XClarity Administrator コンテナを実行する場合は、それぞれのコンテナに固有の名前と IP アドレスを使用します。

ThinkServer および他のレガシー・デバイスを管理する場合は、IPv6 が有効化されている必要があります。

1. `/etc/docker/daemon.json` ファイルを編集し、`ipv6` 鍵を `true` に設定して、`fixed-cidr-v6` 鍵を IPv6 サブネットに設定します。以下に `daemon` ファイルの例を示します。

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. 次のコマンドを実行して Docker 構成ファイルをリロードします。  
`systemctl reload docker`

注：XClarity Administrator は特権コンテナとして実行されません。



## 手順

Docker Compose を使用して XClarity Administrator コンテナをインストールするには、以下の手順を実行します。

ステップ 1. [XClarity Administrator ダウンロード Web ページ](#) から、XClarity Administrator 仮想アプライアンス・イメージ、環境ファイル、および YAML ファイルをクライアント・ワークステーションにダウンロードします。Web サイトにログオンし、付与されたアクセス・キーを使用してイメージをダウンロードします。

ステップ 2. 次のコマンドを実行して、XClarity Administrator コンテナ・イメージを Docker ホストにインポートします。

```
docker load -i lnvgu_sw_lxca_<ver>_anyos_noarch.tar.gz
```

ステップ 3. `docker_compose.env` ファイルを編集し、以下の環境変数を更新します。

- **CONTAINER\_NAME**。各 XClarity Administrator インスタンスに Docker ボリュームを作成するために使用する固有のコンテナ名 (例: `CONTAINER_NAME=LXCA-203`)。
- **ADDRESS**。コンテナの静的 IPv4 アドレス (例: `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**。(任意) XClarity Administrator のバックアップの保存に使用するリモート共有のパス。これは、`/mnt/backup_share` である必要があります。
- **FIRMWARE\_MOUNT**。(オプション) ファームウェア更新のリモート・リポジトリとして使用するリモート共有のパス。これは、`/mnt/fw_share` である必要があります。

以下に環境ファイルの例を示します。

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

ステップ 4. `docker_compose.yml` を編集し、以下のプロパティを更新します。

- **image** プロパティに、手順 2 で使用したインストール・イメージ・ファイルの名前を設定します。

注：イメージ・ファイル名は、`docker tag` コマンドを使用して変更できます (例: 「latest」)。

- リモート共有をリモート・ファームウェア・リポジトリとして使用し、XClarity Administrator のバックアップを保存する場合は、**volumes** プロパティで各リモート共有のホストのマウント・ポイントを設定します。
- **dns** プロパティを DNS サーバーの IP アドレスに設定します。
- コンテナは、ホストで使用できるプロセッサとメモリー・リソースのプールを共有します。必要に応じて、**cpus** および **メモリー** のプロパティを設定することにより、リソース使用量の制限を定義します。
- **parent** プロパティに、コンテナの `macvlan` インターフェースの親のインターフェースとして使用するホスト・システムのネットワーク・インターフェース名を設定します。このインターフェースは、コンテナに割り当てるサブネットに直接アクセスできる必要があります。
- ネットワーク・トポロジーに応じて **サブネット** と **ゲートウェイ** を設定します。通常、`subnet` と `gateway` は、`${ADDRESS}` が属する管理ネットワークのものです。
- IPv6 をサポートする場合は、**enable\_ipv6** プロパティを `true` に設定し、**ipv6\_address** プロパティを IPv6 アドレスに設定して、ネットワーク・トポロジーに応じて別の **subnet** および **gateway** プロパティのセットを追加します (通常、IPv6 アドレスが属する管理ネットワークに)。

注：XClarity Administrator は、macvlan を使用してコンテナ・ネットワークを構成します。詳しくは、「[macvlan ネットワークの使用 Web ページ](#)」を参照してください。

IPv6 が有効な YAML ファイルの例を次に示します。

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

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

ステップ 5. 次のコマンドを実行して、Docker にイメージをデプロイします。<ENV\_FILENAME>は、手順 2 で作成した環境変数ファイルの名前です。

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

## 終了後

XClarity Administrator にログインして構成します ([Lenovo XClarity Administrator Web インターフェースへの最初のアクセス](#)および[Lenovo XClarity Administratorの構成](#)を参照)。

---

## 物理的に分離したデータ/管理ネットワーク

このトポロジーでは、データ・ネットワークと管理ネットワークは物理的に分離した、別々のネットワークです。Lenovo XClarity Administrator とネットワークとの間の管理通信は、ホストの Eth0 ネットワーク・インターフェースを介して行われます。データ通信は Eth1 ネットワーク・インターフェースを介して行われます。

### 始める前に

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します (XClarity Administrator オンライン・ドキュメントの[利用可能なポート](#))。

XClarity Administrator を使用して管理する各デバイスに、最小限必要なファームウェアがインストールされていることを確認します。XClarity Administrator の[サポート - 互換性に関する Web ページ](#)から最小限必要なレベルのファームウェアを見つけるには、「**互換性**」タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

**重要** : デバイスとコンポーネントは、IP アドレスの変更が最小限で済むように構成します。動的ホスト構成プロトコル (DHCP) ではなく、静的 IP アドレスを使用することを検討してください。DHCP が使用されている場合は、IP アドレスの変更が最小限に抑えられていることを確認します。

### このタスクについて

次の図では、データ・ネットワークと管理ネットワークが物理的に異なるネットワークである場合に、運用環境をセットアップする方法の 1 つを示しています。図の番号は、以下のセクションにある番号付きの手順に対応しています。

**注** : 次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、物理的に分離したデータ/管理ネットワークのセットアップに関連するものだけを示しています。

**ヒント** : 冗長性を確保するために、2 台の物理スイッチを各ネットワークに接続してセットアップする (合計 4 台のスイッチ) 代わりに、1 台の物理スイッチを各ネットワークに接続してセットアップできます (合計 2 台のスイッチ)。その場合は、各スイッチを両方のネットワークに接続し、2 つの VLAN

を実装します。1つはデータ・ネットワークに使用し、もう1つは管理ネットワークに使用することで、データ・トラフィックを管理ネットワークから分離します。

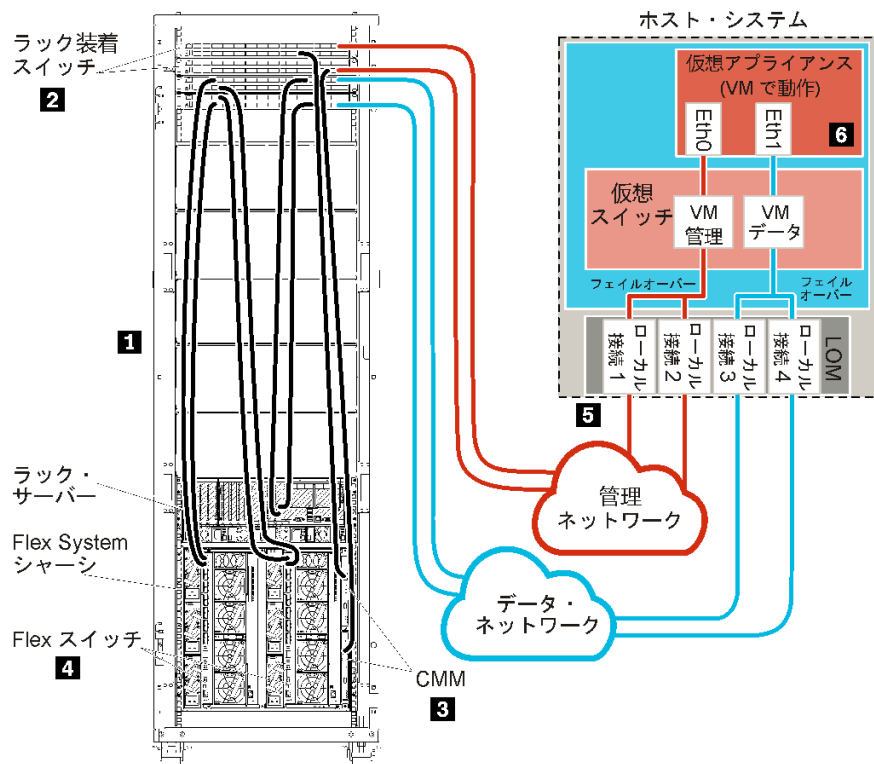


図 12. 仮想アプライアンスの物理的に分離したデータ/管理ネットワーク・トポロジーの例

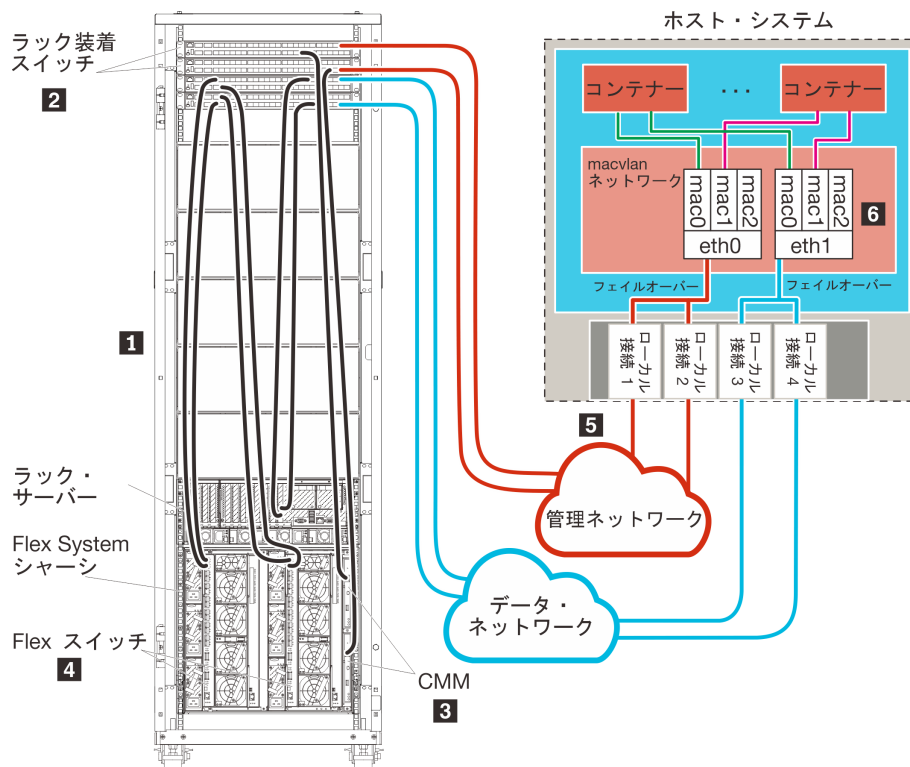


図 13. コンテナの物理的に分離したデータ/管理ネットワーク・トポロジーの例

XClarity Administrator をインストールして、既に構成済みのシャーシとラック・サーバーを管理する場合は、[手順 5: ホストのインストールと構成](#)に進みます。

ネットワーク設定や Eth1 と Eth0 の構成に関する情報など、このトポロジーの計画の追加情報については、[物理的に分離したデータ/管理ネットワーク](#)を参照してください。

## 手順 1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線

シャーシ、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチに配線して、デバイスとネットワークとが通信できるようにします。

### 手順

各シャーシ内の各 Flex スイッチと CMM、各ラック・サーバー、XClarity Administrator ホスト内から両方のラック装着スイッチに配線します。ラック装着スイッチの任意のポートを選択できます。

次の図は、シャーシ (Flex スイッチと CMM)、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチへの配線を示す例です。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、物理的に分離したデータ/管理ネットワークのセットアップに関連するものだけを示しています。

ヒント: 冗長性を確保するために、2 台の物理スイッチを各ネットワークに接続してセットアップする (合計 4 台のスイッチ) 代わりに、1 台の物理スイッチを各ネットワークに接続してセットアップできます (合計 2 台のスイッチ)。その場合は、各スイッチを両方のネットワークに接続し、2 つの VLAN

を実装します。1つはデータ・ネットワークに使用し、もう1つは管理ネットワークに使用することで、データ・トラフィックを管理ネットワークから分離します。

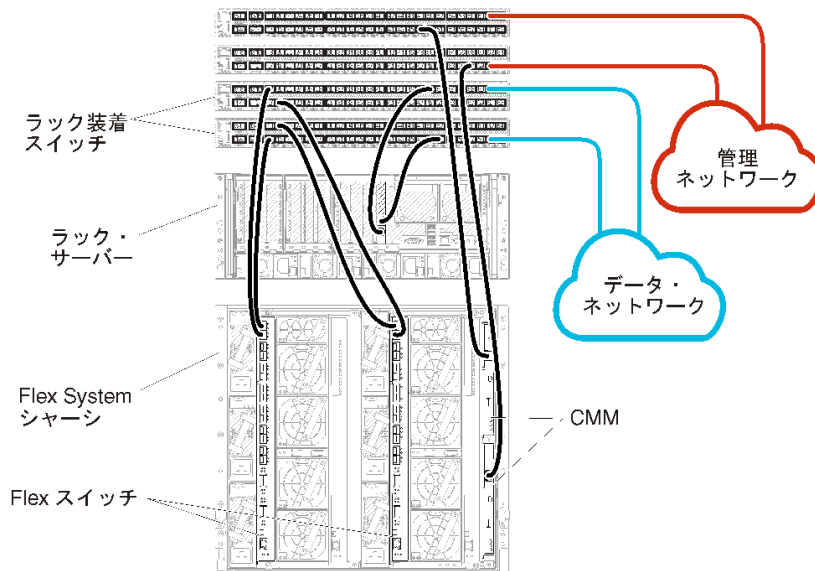


図 14. 物理的に分離したデータ/管理ネットワークの配線の例

## 手順 2: ラック装着スイッチの構成

ラック装着スイッチを構成します。

### 始める前に

ラック装着スイッチの一般的な構成要件を満たしていることに加えて、Flex スイッチ、ラック・サーバー、ネットワークへの外部ポートと、CMM、ラック・サーバー、ネットワークへの内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

### 手順

構成手順は、取り付けられたラック・スイッチの種類によって異なることがあります。

Lenovo ラック装着スイッチの構成について詳しくは、[System x オンライン・ドキュメントのラック装着スイッチ](#)を参照してください。その他のラック装着スイッチが取り付けられている場合は、そのスイッチに付属のドキュメントを参照してください。

## 手順 3: Chassis Management Module (CMM) の構成

シャーシ内のすべてのデバイスを管理するように、シャーシ内のプライマリー Chassis Management Module (CMM) を構成します。

### このタスクについて

CMM の構成について詳しくは、[Flex System のシャーシ・コンポーネントの構成 オンライン・ドキュメント](#)を参照してください。

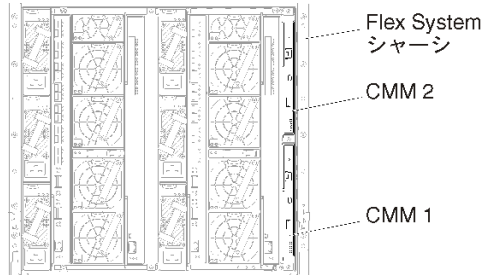
さらに、シャーシに付属の操作指示ポスターで手順 4.1 ~ 4.5 も参照してください。

### 手順

CMM を構成するには、以下の手順を実行します。

2 台の CMM を取り付けている場合、プライマリー CMM のみを構成してください。プライマリー CMM からスタンバイ CMM に構成は自動的に同期されます。

ステップ 1. ベイ 1 内の CMM からクライアント・ワークステーションにイーサネット・ケーブルを直接接続します。



初めて CMM に接続するには、クライアント・ワークステーションでインターネット・プロトコルのプロパティの変更が必要になる場合があります。

**重要：**クライアント・ワークステーション・サブネットが CMM サブネットと同じであることを確認してください(デフォルトの CMM サブネットは 255.255.255.0 です)。クライアント・ワークステーション用に選択する IP アドレスは CMM と同じネットワークに属する必要があります (192.168.70.0 ~ 192.168.70.24 など)。

ステップ 2. CMM 管理インターフェースを起動するには、クライアント・ワークステーションで Web ブラウザーを開き、CMM の IP アドレスを参照します。

注：

- セキュアな接続を使用し、URL に **https** を含めていることを確認します (<https://192.168.70.100> など)。https を含めていない場合、ページが見つからないことを示すエラーが表示されます。
- デフォルトの IP アドレスである 192.168.70.100 を使用している場合、CMM 管理インターフェースが利用可能になるまでに数分かかることがあります。この遅延が発生するのは、CMM がデフォルトの静的アドレスにフォールバックするまでの 2 分間、DHCP アドレスを取得しようとするためです。

ステップ 3. デフォルトのユーザー ID (USERID) とパスワード (PASSWORD) を使用して CMM 管理インターフェースにログインします。ログイン後、デフォルトのパスワードを変更する必要があります。

ステップ 4. CMM 初期セットアップ・ウィザードの残りの手順を実行して、運用環境の詳細を指定します。初期セットアップ・ウィザードでは、必要に応じて以下の操作を実行することができます。

- シャーシのインベントリーと正常性を表示する。
- 既存の構成ファイルから構成をインポートする。
- CMM の全般設定を構成する。
- CMM の日付と時刻を構成する。

**ヒント:** XClarity Administrator のインストール時には、XClarity Administrator だけでなく XClarity Administrator のすべての管理対象シャーシでも NTP サーバーが使用されるように構成します。

- CMM の IP 情報を構成する。
- CMM のセキュリティー・ポリシーを構成する。
- ドメイン・ネーム・システム (DNS) を構成する。



- イベント・フォワーダーを構成する。

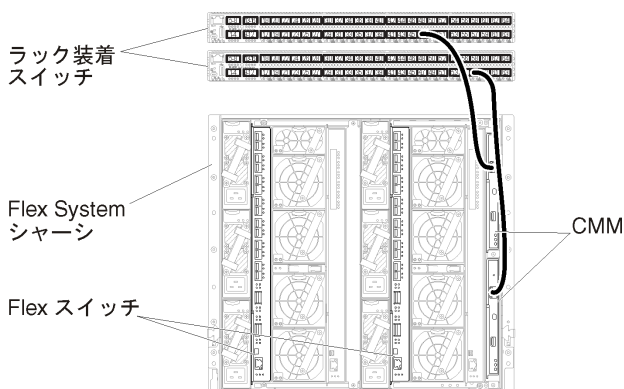
ステップ5. セットアップ・ウィザードの設定を保存し、変更を適用した後、シャーシ内のすべてのコンポーネントの IP アドレスを構成します。

シャーシに付属の操作指示ポスターで手順 4.6 を参照してください。

注：新しい IP アドレスを表示するには、各計算ノードのシステム管理プロセッサをリセットし、Flex スイッチを再起動する必要があります。

ステップ6. CMM 管理インターフェースを使用して CMM を再起動します。

ステップ7. CMM が再起動されたら、CMM のイーサネット・ポートから運用ネットワークにケーブルを接続します。



ステップ8. 新しい IP アドレスを使用して CMM 管理インターフェースにログインします。

## 終了後

冗長性がサポートされるように CMM を構成することもできます。以下の各ページで使用できるフィールドについて詳しくは、CMM のヘルプ・システムを使用してください。

- プライマリー CMM にハードウェア障害が発生した場合の CMM のフェイルオーバーを構成します。CMM 管理インターフェースで、「管理モジュールの管理」→「プロパティ」→「拡張フェイルオーバー」をクリックします。
- ネットワークに問題が発生した場合のフェイルオーバー（アップリンク）を構成します。CMM 管理インターフェースで、「管理モジュールの管理」→「ネットワーク」をクリックし、「イーサネット」タブをクリックして、「拡張イーサネット」をクリックします。少なくとも、必ず「物理ネットワーク・リンクの消失した場合のフェイルオーバー」を選択します。

## 手順 4: Flex スイッチの構成

各シャーシ内の Flex スイッチを構成します。

### 始める前に

Flex スイッチからラック装着スイッチへの外部ポート、CMM への内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

Flex スイッチが動的ネットワーク設定 (IP アドレス、ネットマスク、ゲートウェイ、DNS アドレス) を取得するようにセットアップする場合、Flex スイッチが一貫した設定になるようにする必要があります (たとえば、IP アドレスは CMM と同じサブネット内にある必要があります)

**重要：** Flex System シャーシごとに、シャーシ内の各サーバーの拡張カードのファブリック・タイプが、同じシャーシ内のすべての Flex スイッチのファブリック・タイプと互換性があることを確認します。



たとえば、イーサネット・スイッチをシャーシに取り付ける場合、そのシャーシ内のすべてのサーバーは、LAN-on-motherboard コネクタまたはイーサネット拡張カードを介してイーサネットに接続できる必要があります。Flex スイッチの構成については、[Flex Systems オンライン・ドキュメントの I/O モジュールの構成](#)を参照してください。

## 手順

構成手順は、取り付けられた Flex スイッチの種類によって異なることがあります。サポートされる各 Flex スイッチについては詳しくは、[Flex Systems オンライン・ドキュメントの Flex System ネットワーク・スイッチ](#)を参照してください。

通常、Flex スイッチ・ベイ 1 と 2 の Flex スイッチを構成する必要があります。

ヒント: シャーシの背面から見ると、Flex スイッチ・ベイ 2 は 3 番目のモジュール・ベイです。

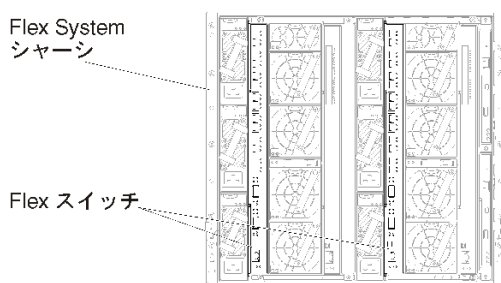


図 15. シャーシにおける Flex スイッチの場所

## 手順 5: ホストのインストールと構成

Lenovo XClarity Administrator の要件を満たす任意のサーバーに Docker をインストールできます。

### 始める前に

Docker Datacenter を使用して、Docker Engine で実行される XClarity Administrator コンテナの高可用性環境を実装できます。Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー およびアプリ Web ページ](#)を参照してください。

[ハードウェアおよびソフトウェアの必須条件](#)で定義されている前提条件をホストが満たしていることを確認します。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

**重要:** 管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジまたは単一データ/管理ネットワーク・トポロジのいずれかを実装できます。
- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用されるときであっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」→「計算ノード」

ド」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

## 手順

お使いの Docker ディストリビューションにより提供されている手順を使用して、ホストに Docker をインストールして構成します。

## 手順 6: XClarity Administratorのインストールと構成

Lenovo XClarity Administrator コンテナを、前の手順でインストールした Docker ホストにインストールして構成します。

### 始める前に

ホスト・システムがハードウェアとソフトウェアの最小要件を満たしていることを確認します ([ハードウェアおよびソフトウェアの必須条件](#) を参照)。

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します ([利用可能なポート](#) を参照)。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

ホスト OS と XClarity Administrator は、同じ NTP サーバーを使用する必要があります。

XClarity Administrator では、データの管理、ハードウェアの管理、OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 を使用します。

XClarity Administrator では、データやハードウェアの管理や OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 と eth1 をそれぞれ使用します。

macvlan ネットワークがホスト・システムのカーネルにロードされている必要があります。ロードされているかどうかを確認するには、`lsmod | grep macvlan` コマンドを使用します。macvlan をカーネルにロードするには、`modprobe macvlan` コマンドを実行します。

同じホストで複数の XClarity Administrator コンテナを実行する場合は、それぞれのコンテナに固有の名前と IP アドレスを使用します。

ThinkServer および他のレガシー・デバイスを管理する場合は、IPv6 が有効化されている必要があります。

1. `/etc/docker/daemon.json` ファイルを編集し、`ipv6` 鍵を `true` に設定して、`fixed-cidr-v6` 鍵を IPv6 サブネットに設定します。以下に `daemon` ファイルの例を示します。

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. 次のコマンドを実行して Docker 構成ファイルをリロードします。  
`systemctl reload docker`

注：XClarity Administrator は特権コンテナとして実行されません。

## 手順

Docker Compose を使用して XClarity Administrator コンテナをインストールするには、以下の手順を実行します。

ステップ 1. [XClarity Administrator ダウンロード Web ページ](#) から、XClarity Administrator 仮想アプライアンス・イメージ、環境ファイル、および YAML ファイルをクライアント・ワークステーションにダウンロードします。Web サイトにログオンし、付与されたアクセス・キーを使用してイメージをダウンロードします。

ステップ 2. 次のコマンドを実行して、XClarity Administrator コンテナ・イメージを Docker ホストにインポートします。

```
docker load -i lnvgy_sw_lxca_<ver>_angos_noarch.tar.gz
```

ステップ 3. `docker_compose.env` ファイルを編集し、以下の環境変数を更新します。

- **CONTAINER\_NAME**。各 XClarity Administrator インスタンスに Docker ボリュームを作成するために使用する固有のコンテナ名 (例: `CONTAINER_NAME=LXCA-203`)。
- **ADDRESS**。コンテナの静的 IPv4 アドレス (例: `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**。(任意) XClarity Administrator のバックアップの保存に使用するリモート共有のパス。これは、`/mnt/backup_share` である必要があります。
- **FIRMWARE\_MOUNT**。(オプション) ファームウェア更新のリモート・リポジトリとして使用するリモート共有のパス。これは、`/mnt/fw_share` である必要があります。

以下に環境ファイルの例を示します。

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

ステップ 4. `docker_compose.yml` を編集し、以下のプロパティを更新します。

- **image** プロパティに、手順 2 で使用したインストール・イメージ・ファイルの名前を設定します。

注：イメージ・ファイル名は、`docker tag` コマンドを使用して変更できます (例: 「latest」)。

- リモート共有をリモート・ファームウェア・リポジトリとして使用し、XClarity Administrator のバックアップを保存する場合は、**volumes** プロパティで各リモート共有のホストのマウント・ポイントを設定します。
- **dns** プロパティを DNS サーバーの IP アドレスに設定します。
- コンテナは、ホストで使用できるプロセッサとメモリー・リソースのプールを共有します。必要に応じて、**cpus** および **メモリー** のプロパティを設定することにより、リソース使用量の制限を定義します。
- **parent** プロパティに、コンテナの `macvlan` インターフェースの親のインターフェースとして使用するホスト・システムのネットワーク・インターフェース名を設定します。このインターフェースは、コンテナに割り当てるサブネットに直接アクセスできる必要があります。
- ネットワーク・トポロジーに応じて **サブネット** と **ゲートウェイ** を設定します。通常、`subnet` と `gateway` は、`ADDRESS` が属する管理ネットワークのものです。
- IPv6 をサポートする場合は、**enable\_ipv6** プロパティを `true` に設定し、**ipv6\_address** プロパティを IPv6 アドレスに設定して、ネットワーク・トポロジーに応じて別の `subnet` および `gateway` プロパティのセットを追加します (通常、IPv6 アドレス が属する管理ネットワークに)。

IPv6 が有効な YML ファイルの例を次に示します。

```

version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

networks:
  lan1:

```

```

name: lan1
driver: macvlan
enable_ipv6: true
driver_opts:
  parent: eno1
ipam:
  config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
lan2:
name: lan2
driver: macvlan
enable_ipv6: true
driver_opts:
  parent: virbr0
ipam:
  config:
    - subnet: 192.0.122.0/24
    - subnet: "2001:8003:7d51:2005::/80"

```

ステップ 5. 次のコマンドを実行して、Docker にイメージをデプロイします。<ENV\_FILENAME> は、手順 2 で作成した環境変数ファイルの名前です。

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

## 終了後

XClarity Administrator にログインして構成します ([Lenovo XClarity Administrator Web インターフェースへの最初のアクセス](#) および [Lenovo XClarity Administrator の構成](#) を参照)。

---

## 仮想的に分離したデータ/管理ネットワーク・トポロジー

このトポロジーでは、データ・ネットワークと管理ネットワークが仮想的に分離しています。データ・ネットワークのパケットと管理ネットワークのパケットは、同じ物理接続を介して送信されるため、2つのネットワーク間でトラフィックを区別するために、すべての管理ネットワーク・データ・パケットで VLAN タグ付けが使用されます。

### 始める前に

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します (XClarity Administrator オンライン・ドキュメントの [利用可能なポート](#))。

XClarity Administrator を使用して管理する各デバイスに、最小限必要なファームウェアがインストールされていることを確認します。XClarity Administrator の [サポート - 互換性に関する Web ページ](#) から最小限必要なレベルのファームウェアを見つけるには、「互換性」タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

VLAN ID がデータ・ネットワークと管理ネットワーク用にセットアップされていることを確認します。必要に応じて、Flex スイッチからタグ付けを実装するかラック装着スイッチから有効にする場合や、ラック装着スイッチからタグ付けを実装する場合は、Flex スイッチから VLAN タグ付けを有効にします。

CMM が接続されているポートを管理 VLAN に属するポートとして定義していることを確認します。

**重要：** デバイスとコンポーネントは、IP アドレスの変更が最小限で済むように構成します。動的ホスト構成プロトコル (DHCP) ではなく、静的 IP アドレスを使用することを検討してください。DHCP が使用されている場合は、IP アドレスの変更が最小限に抑えられていることを確認します。

## このタスクについて

次の図は、管理ネットワークが仮想ネットワークから分離されるように運用環境をセットアップする方法の1つを示しています。図の番号は、以下のセクションにある番号付きの手順に対応しています。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、仮想的に分離したデータ/管理ネットワークのセットアップに関連するものだけを示しています。

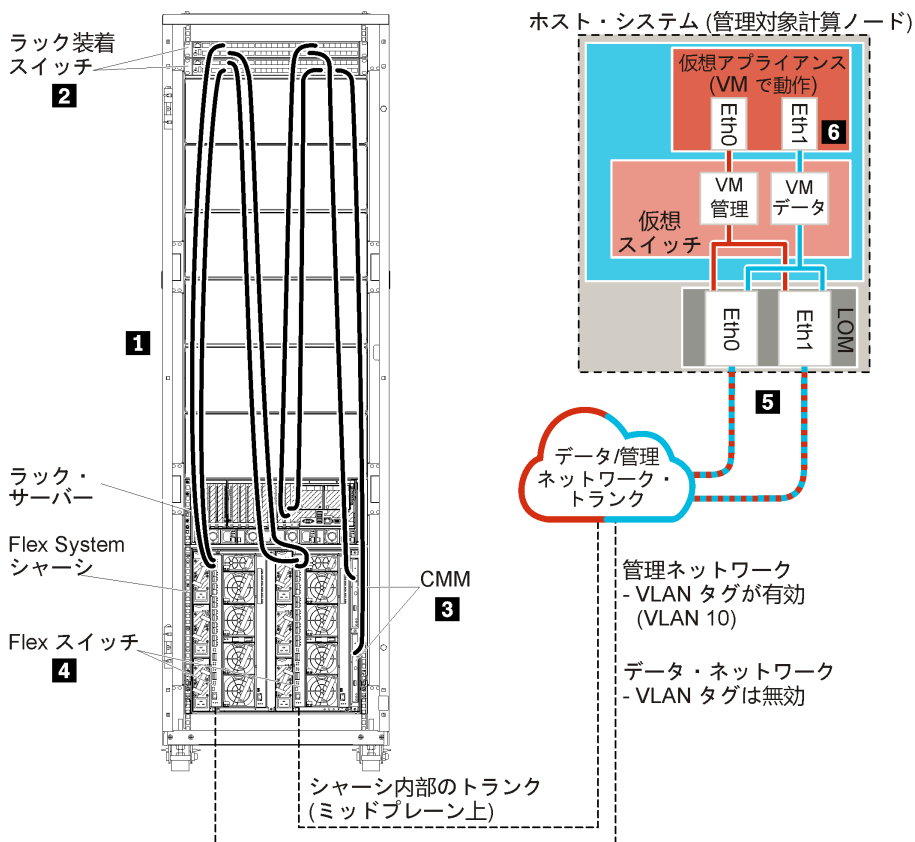


図 16. 仮想アプライアンスの仮想的に分離したデータ/管理ネットワーク・トポロジーの例

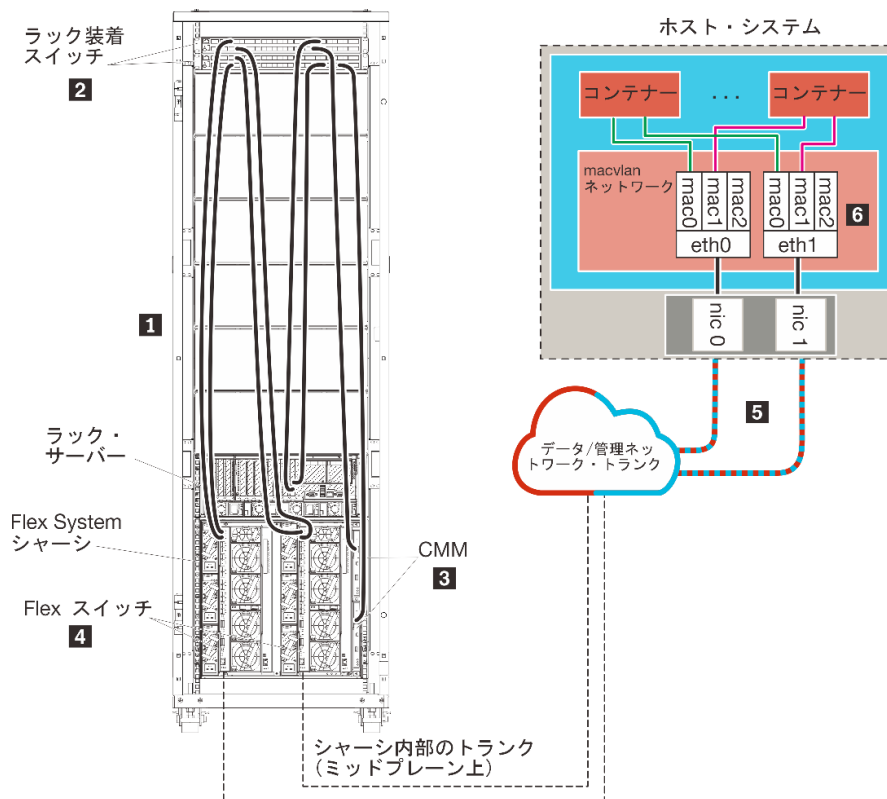


図 17. コンテナの仮想的に分離したデータ/管理ネットワーク・トポロジーの例

このシナリオでは、XClarity Administrator が、XClarity Administrator により管理されている Flex System シャーシ内のサーバーにインストールされています。

**重要：**管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジーまたは単一データ/管理ネットワーク・トポロジーのいずれかを実装できます。
- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用される場合であっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」→「計算ノード」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

さらに、このシナリオでは、すべてのデータが同じ物理接続を介して送信されます。管理ネットワークをデータ・ネットワークから分離するために VLAN タグ付けが使用されます。この方法では、管理ネットワークに対応する特定のタグが受信データ・パケットに付加されて、それらのパケットが適切なインターフェースに振り分けられます。VLAN タグは送信データ・パケットからは削除されます。

VLAN タグ付けは以下のいずれかのデバイスに対して有効にすることができます。



- **ラック装着スイッチ**。パケットがラック装着スイッチに入るときに、管理ネットワークに対応する VLAN タグがパケットに付加されます。その後、パケットは Flex スイッチ を通って Flex System シャーシ内のサーバーに渡されます。復路で、パケットがラック装着スイッチから管理コントローラーに送信されるときに、VLAN タグが削除されます。
- **Flex スイッチ**。パケットが Flex スイッチ に入るときに、管理ネットワークに対応する VLAN タグがパケットに付加されます。その後、パケットは Flex System シャーシ内のサーバーに渡されます。復路で、VLAN タグがサーバーによってパケットに付加され、それらのパケットは Flex スイッチ に渡されます。その後、管理コントローラーに転送されるときに、VLAN タグが削除されます。

VLAN タグ付けを実装するかどうかは、運用環境の要件と複雑さに基づいて選択します。

XClarity Administrator をインストールして、既に構成済みのシャーシとラック・サーバーを管理する場合は、[手順 5: ホストのインストールと構成](#)に進みます。

ネットワーク設定や Eth1 と Eth0 の構成に関する情報など、このトポロジーの計画の追加情報については、[仮想的に分離したデータ/管理ネットワーク](#)を参照してください。

## 手順 1: シャーシとラック・サーバーからラック装着スイッチへの配線

シャーシとラック・サーバーから同じラック装着スイッチに配線して、デバイス間で通信できるようにします。

### 手順

各シャーシ内の各 Flex スイッチと CMM、および各ラック・サーバーから両方のラック装着スイッチに配線します。ラック装着スイッチの任意のポートを選択できます。

次の図は、Lenovo XClarity Administrator が XClarity Administrator により管理されるシャーシ内のサーバーにインストールされている場合のシャーシ (Flex スイッチと CMM) とラック・サーバーからラック装着スイッチへの配線を示す例です。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、仮想的に分離したデータ/管理ネットワークのセットアップに関連するものだけを示しています。

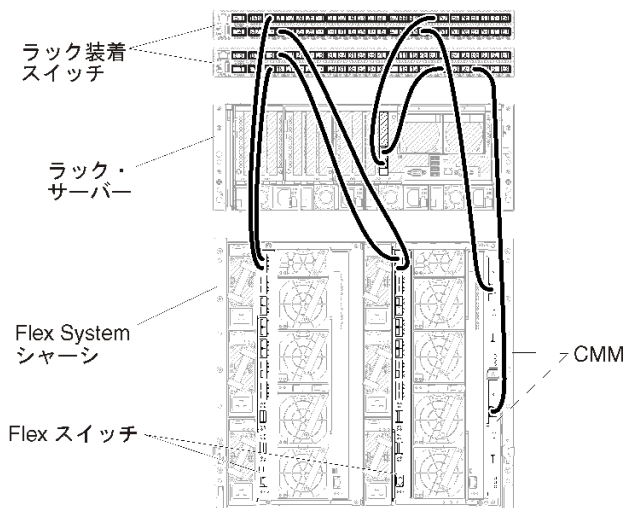


図 18. 仮想的に分離したデータ/管理ネットワークの配線の例

## 手順 2: ラック装着スイッチの構成

ラック装着スイッチを構成します。

### 始める前に

ラック装着スイッチの一般的な構成要件を満たしていることに加えて、Flex スイッチ、ラック・サーバー、ネットワークへの外部ポートと、CMM、ラック・サーバー、ネットワークへの内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

運用環境の要件と複雑さによっては、VLAN タグ付けを Flex スイッチまたはラック装着スイッチで実装することができます。タグ付けをラック装着スイッチから実装する場合、VLAN タグ付けをラック装着スイッチから有効にします。

VLAN ID が管理ネットワークとデータ・ネットワーク用にセットアップされていることを確認します。

### 手順

構成手順は、取り付けられたラック・スイッチの種類によって異なることがあります。

次の図は、ラック装着スイッチに実装され、管理ネットワークでのみ有効になった VLAN タグ付けを示すシナリオの例です。管理 VLAN は VLAN 10 としてセットアップされている。

このシナリオでは、CMM が接続されているポートを管理 VLAN に属するポートとして定義する必要があります。

注：データ・ネットワークで VLAN タグ付けを有効にして、データ VLAN を構成することもできます。

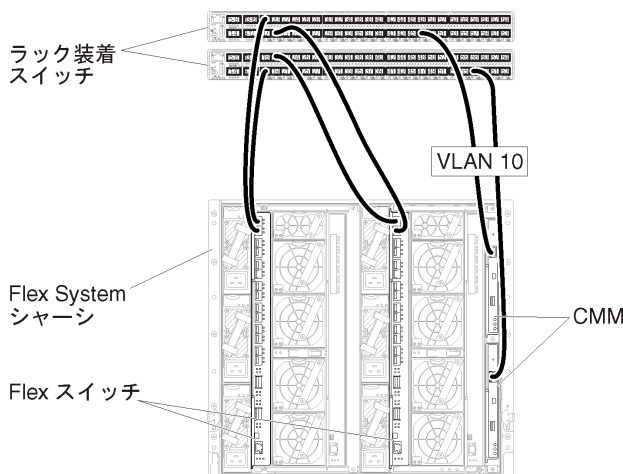


図 19. 管理ネットワークで VLAN タグ付けが有効になっている仮想的に分離したデータ/管理ネットワーク (VMware ESXi) での Flex スイッチの構成の例

Lenovo ラック装着スイッチの構成については、[System x オンライン・ドキュメントのラック装着スイッチ](#)を参照してください。その他のラック装着スイッチが取り付けられている場合は、そのスイッチに付属のドキュメントを参照してください。

## 手順 3: Chassis Management Module (CMM) の構成

シャーシ内のすべてのデバイスを管理するように、シャーシ内のプライマリー Chassis Management Module (CMM) を構成します。

## このタスクについて

CMM の構成について詳しくは、[Flex System のシャーシ・コンポーネントの構成 オンライン・ドキュメント](#)を参照してください。

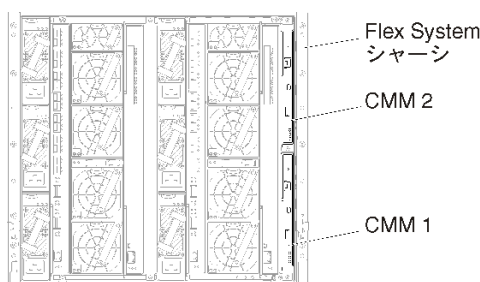
さらに、シャーシに付属の操作指示ポスターで手順 4.1 ~ 4.5 も参照してください。

### 手順

CMM を構成するには、以下の手順を実行します。

2 台の CMM を取り付けている場合、プライマリー CMM のみを構成してください。プライマリー CMM からスタンバイ CMM に構成は自動的に同期されます。

ステップ 1. ベイ 1 内の CMM からクライアント・ワークステーションにイーサネット・ケーブルを直接接続します。



初めて CMM に接続するには、クライアント・ワークステーションでインターネット・プロトコルのプロパティの変更が必要になる場合があります。

**重要：**クライアント・ワークステーション・サブネットが CMM サブネットと同じであることを確認してください(デフォルトの CMM サブネットは 255.255.255.0 です)。クライアント・ワークステーション用に選択する IP アドレスは CMM と同じネットワークに属する必要があります (192.168.70.0 ~ 192.168.70.24 など)。

ステップ 2. CMM 管理インターフェースを起動するには、クライアント・ワークステーションで Web ブラウザーを開き、CMM の IP アドレスを参照します。

注：

- セキュアな接続を使用し、URL に **https** を含めていることを確認します (<https://192.168.70.100> など)。https を含めていない場合、ページが見つからないことを示すエラーが表示されます。
- デフォルトの IP アドレスである 192.168.70.100 を使用している場合、CMM 管理インターフェースが利用可能になるまでに数分かかることがあります。この遅延が発生するのは、CMM がデフォルトの静的アドレスにフォールバックするまでの 2 分間、DHCP アドレスを取得しようとするためです。

ステップ 3. デフォルトのユーザー ID (USERID) とパスワード (PASSWORD) を使用して CMM 管理インターフェースにログインします。ログイン後、デフォルトのパスワードを変更する必要があります。

ステップ 4. CMM 初期セットアップ・ウィザードの残りの手順を実行して、運用環境の詳細を指定します。初期セットアップ・ウィザードでは、必要に応じて以下の操作を実行することができます。

- シャーシのインベントリーと正常性を表示する。
- 既存の構成ファイルから構成をインポートする。
- CMM の全般設定を構成する。

- CMM の日付と時刻を構成する。

ヒント: XClarity Administratorのインストール時には、XClarity AdministratorだけでなくXClarity Administratorのすべての管理対象シャーシでもNTPサーバーが使用されるように構成します。

- CMM のIP情報を構成する。
- CMM のセキュリティー・ポリシーを構成する。
- ドメイン・ネーム・システム (DNS) を構成する。
- イベント・フォワーダーを構成する。

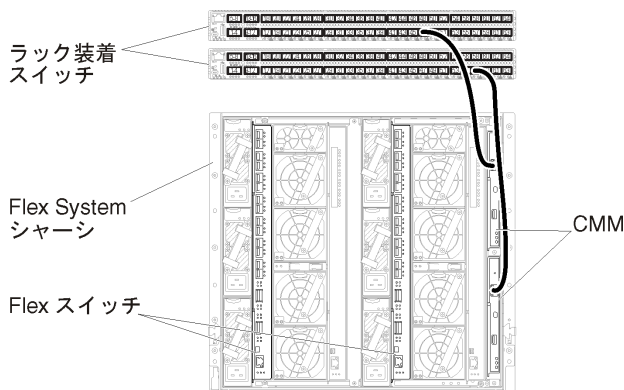
ステップ5. セットアップ・ウィザードの設定を保存し、変更を適用した後、シャーシ内のすべてのコンポーネントのIPアドレスを構成します。

シャーシに付属の操作指示ポスターで手順4.6を参照してください。

注: 新しいIPアドレスを表示するには、各計算ノードのシステム管理プロセッサをリセットし、Flexスイッチを再起動する必要があります。

ステップ6. CMM管理インターフェースを使用してCMMを再起動します。

ステップ7. CMMが再起動されたら、CMMのイーサネット・ポートから運用ネットワークにケーブルを接続します。



ステップ8. 新しいIPアドレスを使用してCMM管理インターフェースにログインします。

## 終了後

冗長性がサポートされるようにCMMを構成することもできます。以下の各ページで使用できるフィールドについて詳しくは、CMMのヘルプ・システムを使用してください。

- プライマリーCMMにハードウェア障害が発生した場合のCMMのフェイルオーバーを構成します。CMM管理インターフェースで、「管理モジュールの管理」→「プロパティ」→「拡張フェイルオーバー」をクリックします。
- ネットワークに問題が発生した場合のフェイルオーバー(アップリンク)を構成します。CMM管理インターフェースで、「管理モジュールの管理」→「ネットワーク」をクリックし、「イーサネット」タブをクリックして、「拡張イーサネット」をクリックします。少なくとも、必ず「物理ネットワーク・リンクの消失した場合のフェイルオーバー」を選択します。

## 手順4: Flexスイッチの構成

各シャーシ内のFlexスイッチを構成します。

### 始める前に

Flex スイッチからラック装着スイッチへの外部ポート、CMM への内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

運用環境の要件と複雑さによっては、VLAN タグ付けを Flex スイッチまたはラック装着スイッチで実装することができます。タグ付けを Flex スイッチから実装する場合、VLAN タグ付けを Flex スイッチから有効にします。

VLAN ID が管理ネットワークとデータ・ネットワーク用にセットアップされていることを確認します。

**重要：** Flex System シャーシごとに、シャーシ内の各サーバーの拡張カードのファブリック・タイプが、同じシャーシ内のすべての Flex スイッチのファブリック・タイプと互換性があることを確認します。たとえば、イーサネット・スイッチをシャーシに取り付ける場合、そのシャーシ内のすべてのサーバーは、LAN-on-motherboard コネクタまたはイーサネット拡張カードを介してイーサネットに接続できる必要があります。Flex スイッチの構成については、[Flex Systems オンライン・ドキュメントの I/O モジュールの構成](#)を参照してください。

## 手順

構成手順は、取り付けられた Flex スイッチの種類によって異なることがあります。サポートされる各 Flex スイッチについては、[Flex Systems オンライン・ドキュメントの Flex System ネットワーク・スイッチ](#)を参照してください。

次の図は、Flex スイッチに実装され、管理ネットワークでのみ有効になった VLAN タグ付けを示すシナリオの例です。管理 VLAN は VLAN 10 としてセットアップされている。

注：データ・ネットワークで VLAN タグ付けを有効にして、データ VLAN を構成できます。

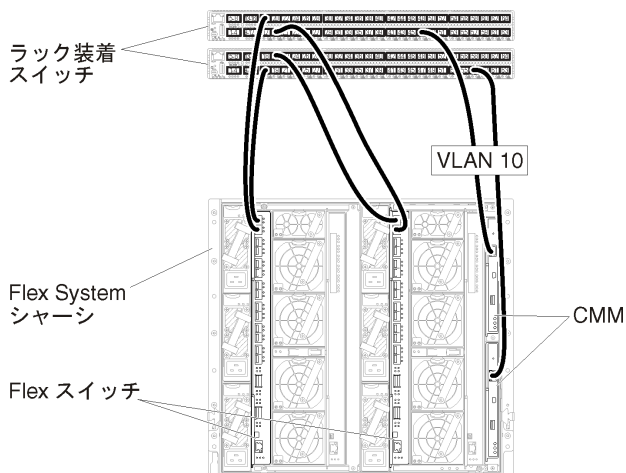


図 20. 管理ネットワークで VLAN タグ付けが有効になっている仮想的に分離したデータ/管理ネットワーク (VMware ESXi) での Flex スイッチの構成の例

このシナリオの Flex スイッチを構成するには、以下の手順を実行します。

ステップ 1. Flex スイッチ・ベイ 1 で Flex スイッチを構成します。

- a. ラック装着管理スイッチに配線されている外部ポートを含む管理 VLAN (この例では VLAN 10 (Ext1) を選択) を定義します。
- b. VLAN 10 (管理 VLAN) に属する内部ポートを定義します。そのポートで VLAN トランッキングが有効になっていることを確認します。

ステップ 2. Flex スイッチ・ベイ 2 で Flex スイッチを構成します。



**ヒント:** シャーシの背面から見ると、Flex スイッチ・ベイ 2 は実際には 3 番目のモジュール・ベイです。

- a. ラック装着管理スイッチに配線されている外部ポートを含む管理 VLAN (この例では VLAN 10 を選択) を定義します。
- b. VLAN 10 (管理 VLAN) に属する内部ポートを定義します。そのポートで VLAN トランキングが有効になっていることを確認します。

## 手順 5: ホストのインストールと構成

Lenovo XClarity Administrator の要件を満たす任意のシステムに Docker をインストールできます。

### 始める前に

Docker Datacenter を使用して、Docker Engine で実行される XClarity Administrator コンテナの高可用性環境を実装できます。Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー およびアプリ Web ページ](#) を参照してください。

[ハードウェアおよびソフトウェアの必須条件](#) で定義されている前提条件をホストが満たしていることを確認します。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

**重要:** 管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジーマたは単一データ/管理ネットワーク・トポロジのいずれかを実装できます。
- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用されるときであっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」→「計算ノード」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

### 手順

お使いの Docker ディストリビューションにより提供されている手順を使用して、ホストに Docker をインストールして構成します。

## 手順 6: XClarity Administrator のインストールと構成

Lenovo XClarity Administrator コンテナを、前の手順でインストールした Docker ホストにインストールして構成します。

### 始める前に

ホスト・システムがハードウェアとソフトウェアの最小要件を満たしていることを確認します ([ハードウェアおよびソフトウェアの必須条件](#) を参照)。

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します ([利用可能なポート](#) を参照)。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

ホスト OS と XClarity Administrator は、同じ NTP サーバーを使用する必要があります。

XClarity Administrator では、データの管理、ハードウェアの管理、OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 を使用します。

XClarity Administrator では、データやハードウェアの管理や OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 と eth1 をそれぞれ使用します。

macvlan ネットワークがホスト・システムのカーネルにロードされている必要があります。ロードされているかどうかを確認するには、`lsmod | grep macvlan` コマンドを使用します。macvlan をカーネルにロードするには、`modprobe macvlan` コマンドを実行します。

同じホストで複数の XClarity Administrator コンテナを実行する場合は、それぞれのコンテナに固有の名前と IP アドレスを使用します。

ThinkServer および他のレガシー・デバイスを管理する場合は、IPv6 が有効化されている必要があります。

1. `/etc/docker/daemon.json` ファイルを編集し、`ipv6` 鍵を `true` に設定して、`fixed-cidr-v6` 鍵を IPv6 サブネットに設定します。以下に `daemon` ファイルの例を示します。

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. 次のコマンドを実行して Docker 構成ファイルをリロードします。  
`systemctl reload docker`

注：XClarity Administrator は特権コンテナとして実行されません。

## 手順

Docker Compose を使用して XClarity Administrator コンテナをインストールするには、以下の手順を実行します。

ステップ 1. [XClarity Administrator ダウンロード Web ページ](#) から、XClarity Administrator 仮想アプライアンス・イメージ、環境ファイル、および YAML ファイルをクライアント・ワークステーションにダウンロードします。Web サイトにログオンし、付与されたアクセス・キーを使用してイメージをダウンロードします。

ステップ 2. 次のコマンドを実行して、XClarity Administrator コンテナ・イメージを Docker ホストにインポートします。

```
docker load -i lnvgy_sw_lxca_<ver>_angos_noarch.tar.gz
```

ステップ 3. `docker_compose.env` ファイルを編集し、以下の環境変数を更新します。

- **CONTAINER\_NAME**。各 XClarity Administrator インスタンスに Docker ボリュームを作成するために使用する固有のコンテナ名 (例: `CONTAINER_NAME=LXCA-203`)。
- **ADDRESS**。コンテナの静的 IPv4 アドレス (例: `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**。(任意) XClarity Administrator のバックアップの保存に使用するリモート共有のパス。これは、`/mnt/backup_share` である必要があります。
- **FIRMWARE\_MOUNT**。(オプション) ファームウェア更新のリモート・リポジトリとして使用するリモート共有のパス。これは、`/mnt/fw_share` である必要があります。

以下に環境ファイルの例を示します。



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

ステップ 4. `docker_compose.yml` を編集し、以下のプロパティを更新します。

- **image** プロパティに、手順 2 で使用したインストール・イメージ・ファイルの名前を設定します。  
  
注：イメージ・ファイル名は、`docker tag` コマンドを使用して変更できます (例: 「latest」)。
- リモート共有をリモート・ファームウェア・リポジトリとして使用し、XClarity Administrator のバックアップを保存する場合は、**volumes** プロパティで各リモート共有のホストのマウント・ポイントを設定します。
- **dns** プロパティを DNS サーバーの IP アドレスに設定します。
- コンテナは、ホストで使用できるプロセッサとメモリー・リソースのプールを共有します。必要に応じて、**cpus** および**メモリー**のプロパティを設定することにより、リソース使用量の制限を定義します。
- **parent** プロパティに、コンテナの `macvlan` インターフェースの親のインターフェースとして使用するホスト・システムのネットワーク・インターフェース名を設定します。このインターフェースは、コンテナに割り当てるサブネットに直接アクセスできる必要があります。
- ネットワーク・トポロジーに応じて**サブネット**と**ゲートウェイ**を設定します。通常、`subnet` と `gateway` は、`ADDRESS` が属する管理ネットワークのものです。
- IPv6 をサポートする場合は、**enable\_ipv6** プロパティを `true` に設定し、**ipv6\_address** プロパティを IPv6 アドレスに設定して、ネットワーク・トポロジーに応じて別の `subnet` および `gateway` プロパティのセットを追加します (通常、IPv6 アドレス が属する管理ネットワークに)。

IPv6 が有効な YML ファイルの例を次に示します。

```
version: '3.8'  
  
services:  
  
  lxca:  
    image: lenovo/lxca:4.1.0-124  
    container_name: ${CONTAINER_NAME}  
    tty: true  
    stop_grace_period: 60s  
    volumes:  
      #bind mount example  
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}  
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}  
      #docker volume mount  
      - data:/opt/lenovo/lxca/data  
      - postgresql:/var/lib/postgresql  
      - log:/var/log  
      - confluent-etc:/etc/confluent  
      - confluent-log:/var/log/confluent  
      - confluent:/var/lib/confluent  
      - propconf:/opt/lenovo/lxca/bin/conf  
      - ssh:/etc/ssh  
      - xcat:/etc/xcat  
    networks:
```

```

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

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

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"

```

ステップ 5. 次のコマンドを実行して、Docker にイメージをデプロイします。<ENV\_FILENAME>は、手順 2 で作成した環境変数ファイルの名前です。

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

## 終了後

XClarity Administrator にログインして構成します ([Lenovo XClarity Administrator Web インターフェースへの最初のアクセス](#)および[Lenovo XClarity Administratorの構成](#)を参照)。

---

## 管理専用ネットワーク・トポロジー

このトポロジーでは、Lenovo XClarity Administrator には管理ネットワークのみがあります。データ・ネットワークはありません。

### 始める前に

以下の該当するポートがすべて有効になっていることを確認します。

- XClarity Administrator に必要なポート (XClarity Administrator オンライン・ドキュメントの[利用可能なポート](#))
- ネットワークへの外部ポート
- CMM への内部ポート

XClarity Administrator を使用して管理する各デバイスに、最小限必要なファームウェアがインストールされていることを確認します。[XClarity Administrator のサポート - 互換性に関する Web ページ](#)から最小限必要なレベルのファームウェアを見つけるには、「[互換性](#)」タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

**重要：**デバイスとコンポーネントは、IP アドレスの変更が最小限で済むように構成します。動的ホスト構成プロトコル (DHCP) ではなく、静的 IP アドレスを使用することを検討してください。DHCP が使用されている場合は、IP アドレスの変更が最小限に抑えられていることを確認します。

### このタスクについて

次の図は、Lenovo XClarity Administrator に管理ネットワークのみがある (データ・ネットワークがない) 場合に、運用環境をセットアップする方法の 1 つを示しています。図の番号は、以下のセクションにある番号付きの手順に対応しています。

**注：**次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、管理専用ネットワークのセットアップに関連するものだけを示しています。

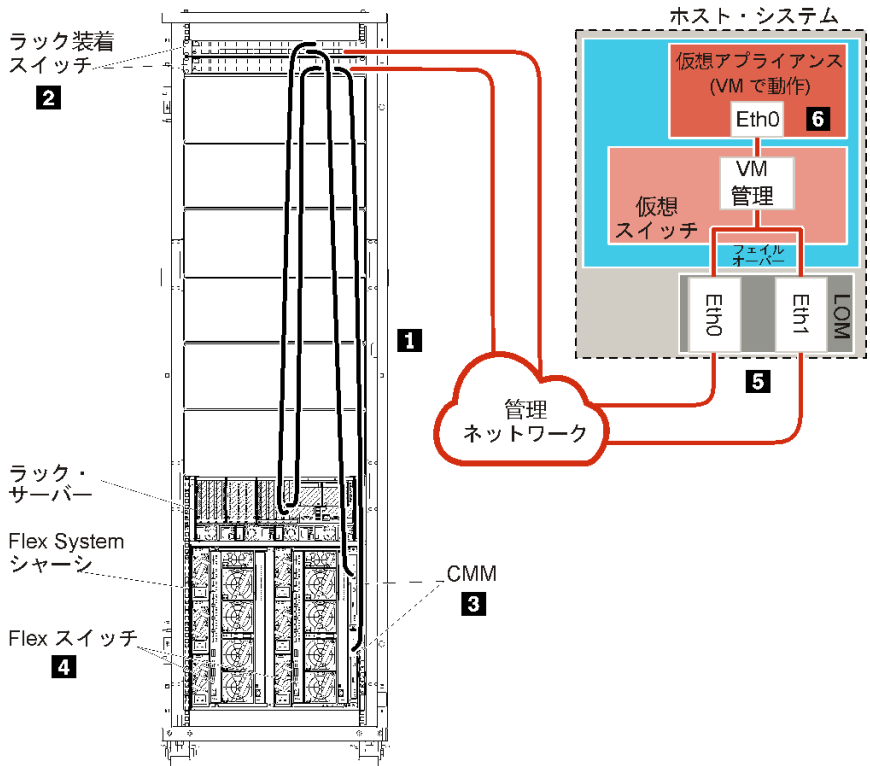


図 21. 仮想アプライアンスの管理専用ネットワーク・トポロジーの例

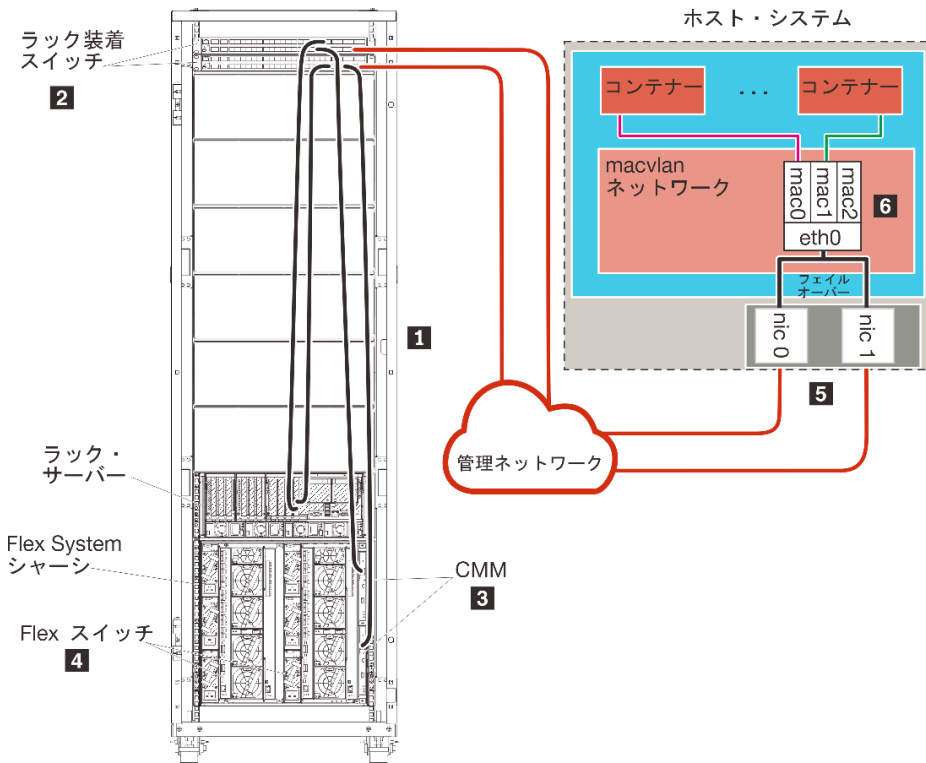


図 22. コンテナの管理専用ネットワーク・トポロジーの例

XClarity Administrator をインストールして、既に構成済みのシャーシとラック・サーバーを管理する場合は、[手順 5: ホストのインストールと構成](#)に進みます。

ネットワーク設定や Eth1 と Eth0 の構成に関する情報など、このトポロジーの計画の追加情報については、[管理専用ネットワーク](#)を参照してください。

## 手順 1: シャーシ、ラック・サーバー、Lenovo XClarity Administrator ホストからラック装着スイッチへの配線

シャーシ、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチに配線して、デバイスとネットワークとが通信できるようにします。

### 手順

各シャーシ内の各 Flex スイッチと CMM、各ラック・サーバー、XClarity Administrator ホスト内から両方のラック装着スイッチに配線します。ラック装着スイッチの任意のポートを選択できます。

次の図は、シャーシ (Flex スイッチと CMM)、ラック・サーバー、XClarity Administrator ホストからラック装着スイッチへの配線を示す例です。

注：次の図は、環境に必要なすべての配線オプションを表しているわけではありません。ここでは、Flex スイッチ、CMM、ラック・サーバーの配線オプション要件のうち、管理専用ネットワークのセットアップに関連するものだけを示しています。

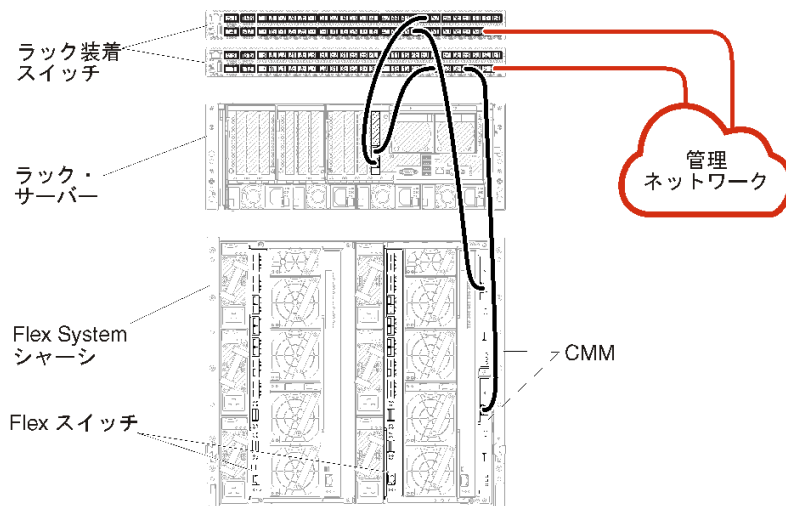


図 23. 管理専用ネットワークの配線の例

## 手順 2: ラック装着スイッチの構成

ラック装着スイッチを構成します。

### 始める前に

ラック装着スイッチの一般的な構成要件を満たしていることに加えて、Flex スイッチ、ラック・サーバー、ネットワークへの外部ポートと、CMM、ラック・サーバー、ネットワークへの内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

### 手順

構成手順は、取り付けられたラック・スイッチの種類によって異なることがあります。

Lenovo ラック装着スイッチの構成について詳しくは、[System x オンライン・ドキュメントのラック装着スイッチ](#)を参照してください。その他のラック装着スイッチが取り付けられている場合は、そのスイッチに付属のドキュメントを参照してください。

### 手順 3: Chassis Management Module (CMM) の構成

シャーシ内のすべてのデバイスを管理するように、シャーシ内のプライマリー Chassis Management Module (CMM) を構成します。

#### このタスクについて

CMM の構成について詳しくは、[Flex System のシャーシ・コンポーネントの構成 オンライン・ドキュメント](#)を参照してください。

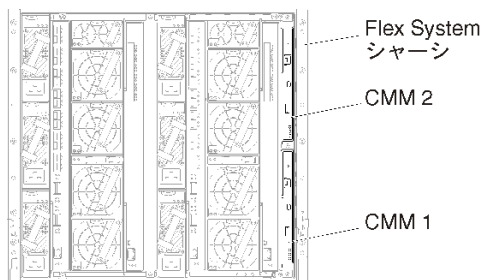
さらに、シャーシに付属の操作指示ポスターで手順 4.1 ~ 4.5 も参照してください。

#### 手順

CMM を構成するには、以下の手順を実行します。

2 台の CMM を取り付けている場合、プライマリー CMM のみを構成してください。プライマリー CMM からスタンバイ CMM に構成は自動的に同期されます。

ステップ 1. ベイ 1 内の CMM からクライアント・ワークステーションにイーサネット・ケーブルを直接接続します。



初めて CMM に接続するには、クライアント・ワークステーションでインターネット・プロトコルのプロパティの変更が必要になる場合があります。

**重要：**クライアント・ワークステーション・サブネットが CMM サブネットと同じであることを確認してください(デフォルトの CMM サブネットは 255.255.255.0 です)。クライアント・ワークステーション用に選択する IP アドレスは CMM と同じネットワークに属する必要があります (192.168.70.0 ~ 192.168.70.24 など)。

ステップ 2. CMM 管理インターフェースを起動するには、クライアント・ワークステーションで Web ブラウザーを開き、CMM の IP アドレスを参照します。

#### 注：

- セキュアな接続を使用し、URL に **https** を含めていることを確認します (https://192.168.70.100 など)。https を含めていない場合、ページが見つからないことを示すエラーが表示されます。
- デフォルトの IP アドレスである 192.168.70.100 を使用している場合、CMM 管理インターフェースが利用可能になるまでに数分かかることがあります。この遅延が発生するのは、CMM がデフォルトの静的アドレスにフォールバックするまでの 2 分間、DHCP アドレスを取得しようとするためです。

ステップ3. デフォルトのユーザー ID (USERID) とパスワード (PASSWORD) を使用して CMM 管理インターフェースにログインします。ログイン後、デフォルトのパスワードを変更する必要があります。

ステップ4. CMM 初期セットアップ・ウィザードの残りの手順を実行して、運用環境の詳細を指定します。初期セットアップ・ウィザードでは、必要に応じて以下の操作を実行することができます。

- シャーシのインベントリと正常性を表示する。
- 既存の構成ファイルから構成をインポートする。
- CMM の全般設定を構成する。
- CMM の日付と時刻を構成する。

ヒント: XClarity Administrator のインストール時には、XClarity Administrator だけでなく XClarity Administrator のすべての管理対象シャーシでも NTP サーバーが使用されるように構成します。

- CMM の IP 情報を構成する。
- CMM のセキュリティー・ポリシーを構成する。
- ドメイン・ネーム・システム (DNS) を構成する。
- イベント・フォワーダーを構成する。

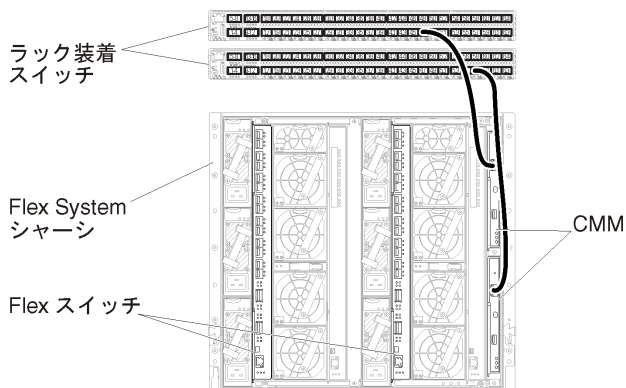
ステップ5. セットアップ・ウィザードの設定を保存し、変更を適用した後、シャーシ内のすべてのコンポーネントの IP アドレスを構成します。

シャーシに付属の操作指示ポスターで手順 4.6 を参照してください。

注: 新しい IP アドレスを表示するには、各計算ノードのシステム管理プロセッサをリセットし、Flex スイッチを再起動する必要があります。

ステップ6. CMM 管理インターフェースを使用して CMM を再起動します。

ステップ7. CMM が再起動されたら、CMM のイーサネット・ポートから運用ネットワークにケーブルを接続します。



ステップ8. 新しい IP アドレスを使用して CMM 管理インターフェースにログインします。

## 終了後

冗長性がサポートされるように CMM を構成することもできます。以下の各ページで使用できるフィールドについて詳しくは、CMM のヘルプ・システムを使用してください。

- プライマリー CMM にハードウェア障害が発生した場合の CMM のフェイルオーバーを構成します。CMM 管理インターフェースで、「管理モジュールの管理」 → 「プロパティ」 → 「拡張フェイルオーバー」をクリックします。



- ネットワークに問題が発生した場合のフェイルオーバー(アップリンク)を構成します。CMM 管理インターフェースで、「管理モジュールの管理」→「ネットワーク」をクリックし、「イーサネット」タブをクリックして、「拡張イーサネット」をクリックします。少なくとも、必ず「物理ネットワーク・リンクの消失した場合のフェイルオーバー」を選択します。

## 手順 4: Flex スイッチの構成

各シャーシ内の Flex スイッチを構成します。

### 始める前に

Flex スイッチからラック装着スイッチへの外部ポート、CMM への内部ポートを含め、該当するすべてのポートが有効になっていることを確認します。

Flex スイッチが動的ネットワーク設定 (IP アドレス、ネットマスク、ゲートウェイ、DNS アドレス) を取得するようにセットアップする場合、Flex スイッチが一貫した設定になるようにする必要があります (たとえば、IP アドレスは CMM と同じサブネット内にある必要があります)

**重要:** Flex System シャーシごとに、シャーシ内の各サーバーの拡張カードのファブリック・タイプが、同じシャーシ内のすべての Flex スイッチのファブリック・タイプと互換性があることを確認します。たとえば、イーサネット・スイッチをシャーシに取り付ける場合、そのシャーシ内のすべてのサーバーは、LAN-on-motherboard コネクタまたはイーサネット拡張カードを介してイーサネットに接続できる必要があります。Flex スイッチの構成について詳しくは、[Flex Systems オンライン・ドキュメントの I/O モジュールの構成](#)を参照してください。

### 手順

構成手順は、取り付けられた Flex スイッチの種類によって異なることがあります。サポートされる各 Flex スイッチについて詳しくは、[Flex Systems オンライン・ドキュメントの Flex System ネットワーク・スイッチ](#)を参照してください。

通常、Flex スイッチ・ベイ 1 と 2 の Flex スイッチを構成する必要があります。

**ヒント:** シャーシの背面から見ると、Flex スイッチ・ベイ 2 は 3 番目のモジュール・ベイです。

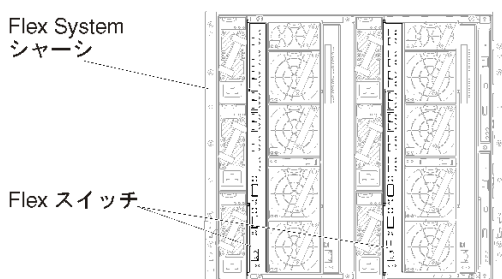


図 24. シャーシにおける Flex スイッチの場所

## 手順 5: ホストのインストールと構成

Lenovo XClarity Administrator の要件を満たす任意のシステムに Docker をインストールできます。

### 始める前に

Docker Datacenter を使用して、Docker Engine で実行される XClarity Administrator コンテナの高可用性環境を実装できます。Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー およびアプリ Web ページ](#) を参照してください。

[ハードウェアおよびソフトウェアの必須条件](#) で定義されている前提条件をホストが満たしていることを確認します。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

**重要：**管理対象サーバーを含め、XClarity Administrator の要件を満たす任意のシステムに XClarity Administrator をセットアップできます。XClarity Administrator ホストに管理対象サーバーを使用する場合、次のようになります。

- 仮想的に分離したデータ/管理ネットワーク・トポロジまたは単一データ/管理ネットワーク・トポロジのいずれかを実装できます。
- XClarity Administrator を使用して、その管理対象サーバーにファームウェア更新を適用することはできません。一部のファームウェアのみが即時アクティベーションで適用されるときであっても、ターゲット・サーバーは、XClarity Administrator によって強制的に再起動されます。これにより、XClarity Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、XClarity Administrator ホストが再起動されたときに、一部のファームウェアのみが適用されます。
- Flex System シャーシのサーバーを使用する場合、サーバーの電源が自動的にオンになるように設定されていることを確認してください。CMM Web インターフェースで「シャーシ管理」→「計算ノード」をクリックしてサーバーを選択し、「自動電源オン・モード」として「自動電源」を選択することにより、このオプションを設定できます。

## 手順

お使いの Docker ディストリビューションにより提供されている手順を使用して、ホストに Docker をインストールして構成します。

## 手順 6: XClarity Administrator のインストールと構成

Lenovo XClarity Administrator コンテナを、前の手順でインストールした Docker ホストにインストールして構成します。

### 始める前に

ホスト・システムがハードウェアとソフトウェアの最小要件を満たしていることを確認します ([ハードウェアおよびソフトウェアの必須条件](#) を参照)。

XClarity Administrator に必要なポートを含む、該当するポートがすべて有効になっていることを確認します ([利用可能なポート](#) を参照)。

ホスト・システムが、管理するデバイスと同じネットワークに存在していることを確認します。

ホスト OS と XClarity Administrator は、同じ NTP サーバーを使用する必要があります。

XClarity Administrator では、データの管理、ハードウェアの管理、OS のデプロイに使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 を使用します。

XClarity Administrator では、データやハードウェアの管理に使用するネットワークにカスタム名を使用できます ([ネットワーク構成](#) を参照)。以下の手順の例では、eth0 を使用します。

macvlan ネットワークがホスト・システムのカーネルにロードされている必要があります。ロードされているかどうかを確認するには、`lsmod | grep macvlan` コマンドを使用します。macvlan をカーネルにロードするには、`modprobe macvlan` コマンドを実行します。

同じホストで複数の XClarity Administrator コンテナを実行する場合は、それぞれのコンテナに固有の名前と IP アドレスを使用します。

ThinkServer および他のレガシー・デバイスを管理する場合は、IPv6 が有効化されている必要があります。

1. /etc/docker/daemon.json ファイルを編集し、`ipv6` 鍵を `true` に設定して、`fixed-cidr-v6` 鍵を IPv6 サブネットに設定します。以下に daemon ファイルの例を示します。

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. 次のコマンドを実行して Docker 構成ファイルをリロードします。  
`systemctl reload docker`

注：XClarity Administrator は特権コンテナとして実行されません。

## 手順

Docker Compose を使用して XClarity Administrator コンテナをインストールするには、以下の手順を実行します。

ステップ 1. [XClarity Administrator ダウンロード Web ページ](#) から、XClarity Administrator 仮想アプライアンス・イメージ、環境ファイル、および YAML ファイルをクライアント・ワークステーションにダウンロードします。Web サイトにログオンし、付与されたアクセス・キーを使用してイメージをダウンロードします。

ステップ 2. 次のコマンドを実行して、XClarity Administrator コンテナ・イメージを Docker ホストにインポートします。

```
docker load -i lnvgy_sw_lxca_<ver>_angos_noarch.tar.gz
```

ステップ 3. `docker_compose.env` ファイルを編集し、以下の環境変数を更新します。

- **CONTAINER\_NAME**。各 XClarity Administrator インスタンスに Docker ボリュームを作成するために使用する固有のコンテナ名 (例: `CONTAINER_NAME=LXCA-203`)。
- **ADDRESS**。コンテナの静的 IPv4 アドレス (例: `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**。(任意) XClarity Administrator のバックアップの保存に使用するリモート共有のパス。これは、`/mnt/backup_share` である必要があります。
- **FIRMWARE\_MOUNT**。(オプション) ファームウェア更新のリモート・リポジトリとして使用するリモート共有のパス。これは、`/mnt/fw_share` である必要があります。

以下に環境ファイルの例を示します。

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

ステップ 4. `docker_compose.yml` を編集し、以下のプロパティを更新します。

- **image** プロパティに、手順 2 で使用したインストール・イメージ・ファイルの名前を設定します。

注：イメージ・ファイル名は、`docker tag` コマンドを使用して変更できます (例: 「latest」)。

- リモート共有をリモート・ファームウェア・リポジトリとして使用し、XClarity Administrator のバックアップを保存する場合は、**volumes** プロパティで各リモート共有のホストのマウント・ポイントを設定します。
- **dns** プロパティを DNS サーバーの IP アドレスに設定します。
- コンテナは、ホストで利用できるプロセッサとメモリー・リソースのプールを共有します。必要に応じて、**cpus** および**メモリー**のプロパティを設定することにより、リソース使用量の制限を定義します。
- **parent** プロパティに、コンテナの **macvlan** インターフェースの親のインターフェースとして使用するホスト・システムのネットワーク・インターフェース名を設定します。このインターフェースは、コンテナに割り当てるサブネットに直接アクセスできる必要があります。
- ネットワーク・トポロジーに応じて**サブネット**と**ゲートウェイ**を設定します。通常、**subnet** と **gateway** は、**ADDRESS** が属する管理ネットワークのものです。
- IPv6 をサポートする場合は、**enable\_ipv6** プロパティを **true** に設定し、**ipv6\_address** プロパティを IPv6 アドレスに設定して、ネットワーク・トポロジーに応じて別の **subnet** および **gateway** プロパティのセットを追加します (通常、IPv6 アドレス が属する管理ネットワークに)。

IPv6 が有効な YML ファイルの例を次に示します。

```
version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
```

```

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

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

```

ステップ 5. 次のコマンドを実行して、Docker にイメージをデプロイします。<ENV\_FILENAME> は、手順 2 で作成した環境変数ファイルの名前です。

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

## 終了後

XClarity Administrator にログインして構成します ([Lenovo XClarity Administrator Web インターフェースへの最初のアクセス](#) および [Lenovo XClarity Administrator の構成](#) を参照)。

---

## 高可用性の実装

Docker Datacenter を使用して、Docker Engine で実行される Lenovo XClarity Administrator コンテナの高可用性環境を実装できます。

Docker Datacenter の高可用性について詳しくは、[Docker Datacenter を使用した高可用性アーキテクチャー](#) および [アプリ Web ページ](#) を参照してください。

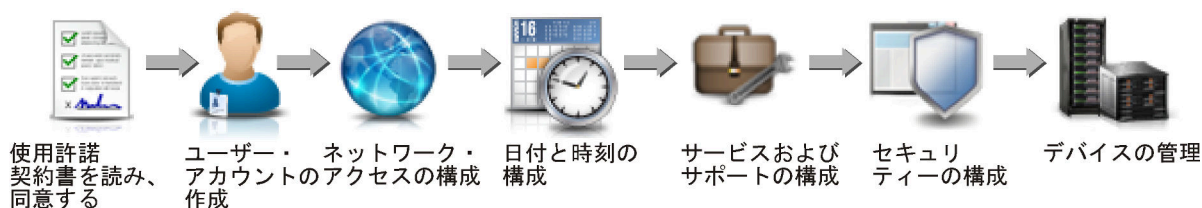
## 第 4 章 Lenovo XClarity Administratorの構成

Lenovo XClarity Administrator に初めてアクセスするときは、XClarity Administrator の初期セットアップを行うために実行する必要がある手順がいくつかあります。

詳細:  [XClarity Administrator: 初めての構成](#)

### 手順

XClarity Administrator の初期セットアップを実行するには、以下の手順を実行します。



ステップ 1. XClarity Administrator Web インターフェースにアクセスします。

ステップ 2. 使用許諾契約書を読み、同意します。

ステップ 3. スーパーバイザー権限を持つユーザー・アカウントを作成します。

**ヒント:** バックアップを必要に応じて利用できるよう、スーパーバイザー権限を持つユーザー・アカウントを2つ以上作成することを検討してください。

ステップ 4. データ・ネットワークと管理ネットワークの IP アドレスを含め、ネットワーク・アクセスを構成します。

ステップ 5. 日付と時刻を構成します。

ステップ 6. サービスおよびサポート設定を構成します。これには、プライバシーに関する声明、使用およびハードウェア・データ、Lenovo サポート (コール・ホーム)、Lenovo アップロード・ファシリティ、製品保証などが含まれます。

ステップ 7. 認証サーバー、ユーザー・グループ、サーバー証明書、暗号モードなど、セキュリティ設定を構成します。

ステップ 8. ご使用のシャーシ、サーバー、スイッチ、およびストレージ・デバイスを管理します。

### Lenovo XClarity Administrator Web インターフェースへの最初のアクセス

XClarity Administrator Web インターフェースは、XClarity Administrator 仮想マシンへのネットワーク接続を持つ任意のコンピューターから起動できます。

#### 始める前に

以下のサポートされる Web ブラウザーのいずれかを使用していることを確認してください。

- Chrome™ 48.0 以降 (リモート・コンソールには 55.0 以上)
- Firefox® ESR 38.6.0 以降
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 以降 (IOS7 以降および OS X)

注: Safari Web ブラウザーでは、XClarity Administrator から管理コントローラー・インターフェースを起動することはできません。

XClarity Administrator Web インターフェースへのログイン元となるシステムが XClarity Administrator 管理ノードにネットワーク接続されていることを確認します。

## 手順

初めて XClarity Administrator Web インターフェースにアクセスするには、以下の手順を実行します。

ステップ 1. ブラウザーで XClarity Administrator の IP アドレスを参照します。

**ヒント:** Web インターフェースにはセキュアな接続を介してアクセスする必要があります。  
**https** を使用していることを確認してください。

- **コンテナの場合:** `{ADDRESS}` 変数で指定した IPv4 アドレスと次の URL を使用して XClarity Administrator にアクセスします。

`https://<IPv4_address>/ui/login.html`

例:

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

- **仮想アプライアンスの場合:** 使用する IP アドレスは、環境をどのようにセットアップしているかによって異なります。

別のサブネットに Eth0 と Eth1 のネットワークがあり、DHCP が両方のサブネットで使用される場合、初期セットアップのために Web インターフェースにアクセスする際には *Eth1* の IP アドレスを使用します。XClarity Administrator を初めて起動する場合、Eth0 と Eth1 の両方が DHCP 割り当て IP アドレスを取得し、XClarity Administrator のデフォルト・ゲートウェイに *Eth1* の DHCP 割り当てゲートウェイが設定されます。

### 静的な IPv4 アドレスの使用

`eth0_config` で IPv4 アドレスを指定した場合は、その IPv4 アドレスを使用して XClarity Administrator にアクセスします。URL は次のとおりです。

`https://<IPv4_address>/ui/login.html`

例:

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

### XClarity Administrator と同じブロードキャスト・ドメインでの DHCP サーバーの使用

XClarity Administrator と同じブロードキャスト・ドメインに DHCP サーバーがセットアップされている場合は、XClarity Administrator 仮想マシンのコンソールに表示されている IPv4 アドレスを使用して、XClarity Administrator にアクセスします。使用する URL は次のとおりです。

`https://<IPv4_address>/ui/login.html`

例:

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

### XClarity Administrator とは異なるブロードキャスト・ドメインでの DHCP サーバーの使用

同じブロードキャスト・ドメインに DHCP サーバーがセットアップされていない場合は、XClarity Administrator 仮想マシンのコンソールに `eEth0` (管理ネットワーク) に対して表示されている IPv6 リンク・ローカル・アドレス (LLA) を使用して、XClarity Administrator にアクセスします。例:

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

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

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



=====  
=====

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

**ヒント:** IPv6 リンク・ローカル・アドレス (LLA) は、インターフェースの MAC アドレスから導き出されます。

**注意:** XClarity Administrator をリモートから構成する場合は、同じレイヤー 2 ネットワークへの接続が必要です。初期セットアップが完了するまでは、ルーティングされないアドレスからアクセスする必要があります。そのため、XClarity Administrator に接続できる別の VM から XClarity Administrator にアクセスすることを検討してください。たとえば、XClarity Administrator がインストールされているホストの別の VM から XClarity Administrator にアクセスできます。

– **Firefox:**

Firefox ブラウザーから XClarity Administrator Web インターフェースにアクセスするには、次の URL を使用してログインします。IPv6 アドレスを入力するときには角かっこが必要なことに注意してください。

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

たとえば、前の Eth0 の例に基づいて、Web ブラウザーに次の URL を入力します。

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

– **Internet Explorer:**

Internet Explorer ブラウザーから XClarity Administrator Web インターフェースにアクセスするには、次の URL を使用してログインします。IPv6 アドレスを入力するときには角かっこが必要なことに注意してください。

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

ここで、<zone\_index> は、Web ブラウザーを起動したコンピューターから管理ネットワークへの接続に使用されるイーサネット・アダプターの識別子です。Windows でブラウザーを使用する場合は、ipconfig コマンドを使用してゾーン・インデックスを見つけます。ゾーン・インデックスはアダプターのリンク・ローカル IPv6 アドレス内でパーセント記号 (%) の後に表示されます。次の例では、ゾーン・インデックスは「30」です。

```
PS C:> ipconfig
Windows IP Configuration
```

```
Ethernet adapter vEthernet (teamVirtualSwitch):
```

```
Connection-specific DNS Suffix . . :
Link-local IPv6 Address . . . . . : 2001:db8:56ff:fe80:bea3%30
Autoconfiguration IPv4 Address. . . : 192.0.2.30
Default Gateway . . . . . :
```

Linux でブラウザーを使用する場合は、ifconfig コマンドを使用してゾーン・インデックスを見つけます。アダプターの名前 (通常は Eth0) をゾーン・インデックスとして使用することもできます。

たとえば、Eth0 とゾーン・インデックスの例に基づいて、Web ブラウザーに次の URL を入力します。

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

ステップ 2. 初めて Lenovo XClarity Administrator にアクセスしたときにセキュリティーまたは証明書の警告が表示されることがありますが、警告は無視しても構いません。

## 結果

「初期セットアップ」ページが表示されます。

### 初期セットアップ

言語:   [さらに詳しい説明を見る](#)

|   |   |   |
|---|---|---|
|    | • Lenovo® XClarity Administrator 使用許諾契約書を読み、同意してください                          | > |
|    | • ユーザー・アカウントの作成   | > |
|    | • ネットワーク・アクセスの構成<br>管理とデータ・ネットワーク・アクセス用の IP 設定を構成します。                         | > |
|    | • 日付と時刻の設定の構成<br>ローカルの日付と時刻を設定するか、外部の Network Time Protocol (NTP) サーバーを使用します。 | > |
|   | • サービスおよびサポート設定の構成<br>「サービスおよびサポート」ページに移動して設定を構成します。                          | > |
|  | 追加のセキュリティー設定の構成<br>「セキュリティー」ページに移動して、証明書・ユーザー・グループ・LDAP クライアントのデフォルト設定を変更します。 | > |
|  | システム管理の開始<br>「新しいデバイスの検出と管理」ページに移動して、管理するシステムを選択します。                          | > |

## 終了後

初期セットアップの手順を実行して XClarity Administrator を構成します ([Lenovo XClarity Administrator の構成](#)を参照)。

---

## ユーザー・アカウントの作成

ユーザー・アカウントは、管理している認証の対象である Lenovo XClarity Administrator およびデバイスの承認とアクセスを管理します。

### このタスクについて

最初に作成するユーザー・アカウントは、スーパーバイザーの役割を持つアクティブ (有効) なアカウントである必要があります。

追加のセキュリティ対策として、**スーパーバイザー**の役割を持つユーザー・アカウントを少なくとも2つ作成します。Lenovo XClarity Administrator を復元しなければならなくなったときのために、それらのユーザー・アカウントのパスワードを記録して安全な場所に保管してください。


## 手順

ユーザー・アカウントを作成するには、以下の手順を実行します。

ステップ 1. 「新しいスーパーバイザー・ユーザーの作成」ダイアログで以下の情報を入力します。

- ユーザーのユーザー名と説明を入力します。
- 新しいパスワードを入力し、確認のためにもう一度入力します。現在のアカウント・セキュリティ設定に基づくパスワード規則が適用されます。
- ユーザーに適切なタスクの実行を許可するために1つ以上の役割グループを選択します。  
役割グループの詳細とカスタム役割グループの作成方法については、XClarity Administrator オンライン・ドキュメントの[役割グループの作成](#)を参照してください。
- (オプション) XClarity Administrator への初回ログイン時にパスワードの変更をユーザーに強制する場合は、「**最初のアクセス時にパスワードを変更**」を「Yes」に設定します。

ステップ 2. 「作成」をクリックします。

ステップ 3. 「作成」アイコン()をクリックして前の手順を繰り返し、追加のユーザーを作成します。

ステップ 4. 「初期セットアップに戻る」をクリックします。

---

## ネットワーク・アクセスの構成

ネットワーク・アクセスの構成にするには、最大2個のネットワーク・インターフェース、Lenovo XClarity Administrator のホスト名、および使用する DNS サーバーを構成できます。

### このタスクについて

XClarity Administrator では、実装するネットワーク・トポロジーに応じて、環境で2つのネットワーク・インターフェースを定義することができます。仮想アプライアンスの場合、これらのネットワーク・インターフェース名は eth0 と eth1 です。コンテナの場合は、カスタム名を選択できます。

- 1つのネットワーク・インターフェース (eth0) のみが存在する場合:
  - (サーバーの構成、ファームウェアの更新など) デバイスの検出と管理をサポートするようにインターフェースを構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーのベースボード管理コントローラー、各 RackSwitch スイッチと通信できる必要があります。
  - XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが(できればファイアウォールを介して)インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
  - サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティーを含む)自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが(できればファイアウォールを介して)インターネットに接続している必要があります。
  - オペレーティング・システム・イメージをデプロイし、OS デバイス・ドライバを更新する場合は、このネットワーク・インターフェースに、ホスト・オペレーティング・システムへのアクセスに使用されるサーバーのネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェー

スを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

● 2つのネットワーク・インターフェース (eth0 と eth1) が存在する場合:

- 最初のネットワーク・インターフェース (通常は Eth0 インターフェース) は、管理ネットワークに接続し、デバイスの検出と管理 (サーバーの構成およびファームウェアの更新を含む) をサポートするように構成する必要があります。各管理対象サーバーの CMM および Flex スイッチ、各管理対象サーバーの管理コントローラー、各 RackSwitch スイッチと通信する必要があります。
- セカンド・ネットワーク・インターフェース (通常は eth1 インターフェース) は、内部データ・ネットワークまたはパブリック・データ・ネットワーク、あるいはその両方と通信するように構成できます。
- XClarity Administrator を使用してファームウェアおよび OS デバイス・ドライバーの更新を取得する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。この方法を使用しない場合は、更新をリポジトリにインポートする必要があります。
- サービス・データを収集したり、(コール・ホーム機能、Lenovo アップロード・ファシリティーを含む) 自動問題通知を使用する場合は、少なくとも1つのネットワーク・インターフェースが (できればファイアウォールを介して) インターネットに接続している必要があります。
- オペレーティング・システム・イメージをデプロイして、デバイス・ドライバーを更新する場合は、eth1 または eth0 のいずれかのインターフェースを使用することもできます。ただし、使用するインターフェースでは、ホスト・オペレーティング・システムへのアクセスに使用されるサーバー・ネットワーク・インターフェースへの IP ネットワーク接続が必要です。

注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。

次の表に、環境に実装されているネットワーク・トポロジーのタイプに基づく、XClarity Administrator ネットワーク・インターフェースの考えられる構成を示します。この表を使用して、各ネットワーク・インターフェースの定義方法を確認してください。

表 3. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割

| ネットワーク・トポロジー   | インターフェース 1 (eth0) の役割  | インターフェース 2 (eth1) の役割   |
|--|--|---|
| コンバージド・ネットワーク (OS デプロイメントと OS デバイス・ドライバーの更新をサポートする管理およびデータ・ネットワーク) | 管理ネットワーク <ul style="list-style-type: none"> <li>● 検出および管理</li> <li>● サーバー構成</li> <li>● ファームウェア更新</li> <li>● サービス・データ収集</li> <li>● 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど)</li> <li>● 保証データの取得</li> <li>● OS デプロイメント</li> <li>● OS デバイス・ドライバーの更新</li> </ul> | なし  |
| OS デプロイメントと OS デバイス・ドライバーの更新をサポートする個別の管理ネットワークとデータ・ネットワーク          | 管理ネットワーク <ul style="list-style-type: none"> <li>● 検出および管理</li> <li>● サーバー構成</li> <li>● ファームウェア更新</li> <li>● サービス・データ収集</li> <li>● 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど)</li> <li>● 保証データの取得</li> </ul>   | データ・ネットワーク <ul style="list-style-type: none"> <li>● なし</li> </ul> |

表 3. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割 (続き)

| ネットワーク・トポロジー  | インターフェース 1 (eth0) の役割  | インターフェース 2 (eth1) の役割  |
|---|--|--|
|   | <ul style="list-style-type: none"> <li>OS デプロイメント</li> <li>OS デバイス・ドライバの更新</li> </ul>  |  |
| OS デプロイメントと OS デバイス・ドライバの更新をサポートする個別の管理ネットワークとデータ・ネットワーク  | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど)</li> <li>保証データの取得</li> </ul> | データ・ネットワーク <ul style="list-style-type: none"> <li>OS デプロイメント</li> <li>OS デバイス・ドライバの更新</li> </ul> |
| OS デプロイメントと OS デバイス・ドライバの更新をサポートしない個別の管理ネットワークとデータ・ネットワーク | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど)</li> <li>保証データの取得</li> </ul> | データ・ネットワーク <ul style="list-style-type: none"> <li>なし</li> </ul>                                  |
| 管理ネットワークのみ (OS デプロイメントおよび OS デバイス・ドライバの更新はサポートされません)      | 管理ネットワーク <ul style="list-style-type: none"> <li>検出および管理</li> <li>サーバー構成</li> <li>ファームウェア更新</li> <li>サービス・データ収集</li> <li>自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど)</li> <li>保証データの取得</li> </ul> | なし   |

XClarity Administrator ネットワーク・インターフェースについて詳しくは、[ネットワークに関する考慮事項](#)を参照してください。

## 手順

ネットワーク・アクセスを構成するには、以下の手順を実行します。

- ステップ 1. 「初期セットアップ」ページで、「**ネットワーク・アクセスの構成**」をクリックします。  
「ネットワーク・アクセスの編集」ページが表示されます。

## ネットワーク・アクセスの編集

|       |      |           |
|-------|------|-----------|
| IP 設定 | 拡張設定 | インターネット設定 |
|-------|------|-----------|

IP 設定

DHCP と外部セキュリティ証明書を使用する場合は、管理サーバー IP アドレスの変更時にマネージ・リソースとの通信に障害が発生する事態を回避するために、DHCP サーバーによる管理サーバーへのアドレス・リースを永続的に実行してください。

1つのネットワーク・インターフェースが検出されました:

Eth0:  有効 - 使用対象  ハードウェアの検索と管理、オペレーティング・システム・イメージの管理とデブ... ?

|               | IPv4   | IPv6   |
|---------------|--|--|
| Eth0:         | <input type="checkbox"/> 静的に割り当てられた IP アドレスを使用する<br>* IP アドレス: <input type="text" value="10.240.61.98"/><br>ネットワーク・マスク: <input type="text" value="255.255.252.0"/> | <input type="checkbox"/> ステートフル・アドレス構成 (DHCPv6) を...<br>IP アドレス: <input type="text"/><br>プレフィックスの長さ: <input type="text" value="64"/> |
| デフォルト・ゲートウェイ: | ゲートウェイ: <input type="text" value="10.240.60.1"/>   | ゲートウェイ: <input type="text" value="DHCP"/>  |

ステップ 2. XClarity Administrator を使用してオペレーティング・システムをデプロイし、OS デバイス・ドライバーを更新する場合は、オペレーティング・システムの管理に使用するネットワーク・インターフェースを選択します。

- 1つのインターフェースのみが XClarity Administrator に定義されている場合は、そのインターフェースをハードウェアの検出と管理にのみ使用するか、オペレーティング・システムの管理にも使用するかを選択します。
- 2つのインターフェース (Eth0 と Eth1) が XClarity Administrator に定義されている場合は、オペレーティング・システムの管理に使用するインターフェースを決定します。「なし」を選択した場合、XClarity Administrator から管理対象サーバーにオペレーティング・システム・イメージのデプロイまたは OS デバイス・ドライバーの更新を行うことはできません。

ステップ 3. IP 設定を指定します。

- a. 第 1 インターフェースの場合は、IPv4 アドレス、IPv6 アドレス、またはその両方を指定します。

- 「IPv4」。インターフェースに IPv4 アドレスを割り当てる必要があります。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を選択できます。
- 「IPv6」。必要に応じて、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

注：IPv6 アドレスについては、XClarity Administrator オンライン・ドキュメントの [IP 構成の制限](#)。

- b. 第 2 インターフェースを使用できる場合は、IPv4 アドレス、IPv6 アドレス、またはその両方を指定します。

注：このインターフェースに割り当てる IP アドレスは、第 1 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」。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を選択できます。
  - 「IPv6」。必要に応じて、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
- c. デフォルト・ゲートウェイを指定します。

デフォルト・ゲートウェイを指定する場合は、有効な IP アドレスを入力し、いずれかのネットワーク・インターフェース (Eth0 または Eth1) の IP アドレスと同じネットワーク・マスク (同じサブネット) を使用する必要があります。1つのインターフェースを使用する場合は、デフォルト・ゲートウェイはネットワーク・インターフェースと同じサブネット内にあることが必要です。

いずれかのインターフェースが DHCP を使用して IP アドレスを取得する場合は、デフォルト・ゲートウェイも DHCP を使用します。DHCP サーバーから受信したゲートウェイをオーバーライドするデフォルト・ゲートウェイ・アドレスを手動で入力するには、「ゲートウェイのオーバーライド」チェックボックスにチェックを入れます。

#### ヒント:

- ゲートウェイがネットワーク・インターフェースのサブネットのいずれかと一致することを確認します。デフォルト・ゲートウェイは、そのネットワーク・インターフェースを介して自動的に設定されます。
- DHCP が提供するゲートウェイに戻る場合は、「ゲートウェイのオーバーライド」チェックボックスのチェックを外します。

#### 警告:

ゲートウェイをオーバーライドする場合は、注意して正しいゲートウェイ・アドレスを入力してください。そうしないと、この管理サーバーに到達できなくなり、これを修正するためにリモートでログインする方法はありません。

- d. 「IP 設定の保存」をクリックします。

ステップ 4. オプション: 必要に応じて、詳細設定を構成します。

- a. 「詳細ルーティング」タブをクリックします。

#### ネットワーク・アクセスの編集

| IP 設定    | 拡張設定  | インターネット設定 |                 |             |   |
|----------|-------|-----------|-----------------|-------------|---|
| 詳細な経路設定  |       |           |                 |             |   |
| インターフェース | 経路の種類 | 宛先        | マスク/プレフィックスの長さ  | ゲートウェイ・アドレス |   |
| Eth0     | ホスト   | IPv4      | 255.255.255.255 |             |   |

- b. 「詳細な経路設定」テーブルでこのインターフェースによって使用される経路エントリを1つ以上指定します。

1つ以上の経路エントリを定義するには、以下の手順を実行します。

1. インターフェースを選択します。

2. 別のホストまたはネットワークへの経路として使用できる経路のタイプを指定します。
3. 経路上の宛先となるホストまたはネットワーク・アドレスを指定します。
4. 宛先アドレスのサブネット・マスクを指定します。
5. パケットが送信されるゲートウェイ・アドレスを指定します。

c. 「詳細ルーティングの保存」をクリックします。

ステップ 5. 必要に応じて、DNS およびプロキシ設定を変更します。

a. 「DNS およびプロキシ」タブをクリックします。

#### ネットワーク・アクセスの編集



インターネット設定

仮想アプライアンスのホスト名とドメイン名

ホスト名: idxhwmgr

ドメイン名: labs.lenovo.com

DNS サーバー

DNS 動作モード: 静的

| 順序 | サーバー・アドレス   |
|----|-------------|
| 1  | 10.240.0.10 |
| 2  | 10.240.0.11 |

インターネット設定

インターネット・アクセス: 直接接続 HTTP プロキシ

b. XClarity Administrator に使用されるホスト名とドメイン名を指定します。

c. DNS 動作モードを選択します。これは、「静的」または「DHCP」です。

注意：DNS 動作モードを変更する場合は、管理サーバーを再起動する必要があります。

注：DHCP サーバーを使用して IP アドレスを取得するように選択した場合、「DNS サーバー」フィールドで行った変更は、XClarity Administrator の DHCP リースの次回更新時に上書きされます。

d. 使用する 1 つ以上のドメイン・ネーム・システム (DNS) サーバーの IP アドレスと、それぞれの優先順位を指定します。

e. インターネットへのアクセスが直接接続であるか HTTP プロキシ経由であるかを指定します (XClarity Administrator がインターネットにアクセスできる場合)。

注：HTTP プロキシを使用している場合は、以下の要件を満たしていることを確認してください。

- 必ず、プロキシ・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ようにしてください。
- プロキシ・サーバーが終了しないプロキシとしてセットアップされていることを確認します。
- プロキシ・サーバーが転送プロキシとしてセットアップされていることを確認します。
- ロード・バランサーがセッションを 1 つのプロキシ・サーバーで保持し、他のサーバーに切り替えないように構成されていることを確認します。

HTTP プロキシを使用するように選択した場合は、必須フィールドに入力します。

1. プロキシ・サーバーのホスト名およびポートを指定します。
  2. 認証を使用するかどうかを選択し、必要に応じてユーザー名およびパスワードを指定します。
  3. プロキシ・テストの URL を指定します。
  4. 「**プロキシのテスト**」をクリックして、プロキシ設定が正しく構成され機能することを確認します。
- f. 「**DNS およびプロキシの保存**」をクリックします。
- g. XClarity Administrator 管理サーバーの完全修飾ドメイン名 (FQDN) と DNS 情報を、IMM2、XCC、および XCC2 の管理対象サーバーにプッシュし、管理対象サーバーでこの情報を使用して管理サーバーを検索できるようにします。
1. 「**FQDN / DNS を BMC にプッシュ**」をクリックします。
  2. ベースボード管理コントローラーの既存の DNS エントリーの処理方法を選択します。
    - 既存の DNS エントリーを保持し、次に使用可能なスロットに管理サーバーの DNS エントリーを追加します。
    - すべての既存の DNS エントリーを管理サーバーの DNS エントリーに置き換えます。
  3. 編集フィールドに「**YES**」と入力します。
  4. 「**適用**」をクリックします。

この操作を実行するためのジョブが作成されます。「**監視**」 → 「**ジョブ**」カードから、ジョブの進行状況を監視できます。ジョブが正常に完了しなかった場合、ジョブ・リンクをクリックし、ジョブに関する詳細を表示します (XClarity Administrator オンライン・ドキュメントの「[ジョブの操作](#)」を参照)。

「**FQDN / DNS を BMC から削除**」をクリックして、IMM2、XCC、および XCC2 の管理対象サーバーから管理サーバーの FQDN および DNS 情報を削除することもできます。他の既存の DNS エントリーを保持するか、すべての DNS エントリーを削除するか、または管理サーバー情報と一致するエントリーのみを削除するかを選択できます。

ステップ 6. 「**戻る**」をクリックします。

ステップ 7. ネットワーク設定を確認するには、「**接続のテスト**」をクリックします。

---

## 日付と時刻の構成

Lenovo XClarity Administrator の日付と時刻を手動で設定することもできますが、Network Time Protocol (NTP) サーバーをセットアップして、XClarity Administrator とすべての管理対象デバイスの間でタイムスタンプを同期することをお勧めします。

### 始める前に

管理対象デバイスから受信したすべてのイベントのタイム・スタンプを XClarity Administrator と同期するために、少なくとも 1 つの (最大 4 つの) Network Time Protocol (NTP) サーバーを使用する必要があります。

**ヒント:** NTP サーバーには、管理ネットワークを介してアクセスできる必要があります (通常は Eth0 インターフェース)。XClarity Administrator が実行されているホストでの NTP サーバーのセットアップを検討してください。

NTP サーバーの時刻を変更した場合、XClarity Administrator が新しい時刻と同期するまでにしばらく時間がかかることがあります。

**注意:** XClarity Administrator 仮想アプライアンスおよびそのホストは、XClarity Administrator とそのホスト間で誤った同期を防止するために、同じ時刻送信元と同期するように設定する必要があります。通常は、

仮想アプライアンスがホストと時刻同期するようにホストが構成されます。If XClarity Administrator がホスト以外のソースと同期するように設定されている場合、XClarity Administrator 仮想アプライアンスとそのホスト間のホスト時刻同期を無効にする必要があります。

- ESXi については、[VMware – 時刻同期の無効化 Web ページ](#)の手順に従います。
- Hyper-V の場合は、Hyper-V マネージャーから、XClarity Administrator 仮想マシンを右クリックして、「設定」をクリックします。ダイアログで、ナビゲーション・ペインの「管理」>「統合サービス」をクリックして、「時刻同期」を選択解除します。

## 手順

XClarity Administrator 用の NTP サーバーをセットアップするには、以下の手順を実行します。

ステップ 1. 初期セットアップ・ページで、「日付と時刻の設定の構成」をクリックします。「日付と時刻の編集」ページが表示されます。

### 日付と時刻の編集

日付と時刻は NTP サーバーと自動的に同期します。

タイム・ゾーン

UTC -05:00, 東部標準時 アメリカ/ニュー・ヨーク

夏時間 (DST) を自動調整します。

クロック設定を編集 (12 時間または 24 時間形式):

24 12

NTP サーバー・ホスト名または IP アドレス:

us.pool.ntp.org

0.0.0.0

0.0.0.0

0.0.0.0

NTP v3 認証:

必須

なし

\*

NTP 認証キー (少なくとも 1 つ入力する必要があります)

M-MD5 キーを使用:

M-MD5 鍵インデックス:

M-MD5 キー:

SHA1 キーを使用:

SHA1 鍵インデックス:

SHA1 キー:

ステップ 2. 「日付と時刻」ダイアログに入力します。

1. XClarity Administrator のホストがあるタイム・ゾーンを選択します。  
選択されたタイム・ゾーンが夏時間 (DST) だった場合、時刻は自動的に DST に合わせて調整されます。
2. 12 時間または 24 時間の時計を選択します。
3. 運用ネットワーク内の各 NTP サーバーのホスト名または IP アドレスを指定します。NTP サーバーは最大 4 つまで定義できます。
4. ネットワーク内で「NTP v3 認証」を有効にする場合は「必須」を選択し、XClarity Administrator と NTP サーバー間で NTP v1 認証を使用する場合は「なし」を選択します。

管理対象の Flex System の CMM およびベースボード管理コントローラーのファームウェアで v3 認証を必要とし、XClarity Administrator とネットワーク内の 1 つ以上の NTP サーバーの間で NTP v3 認証が必要な場合に、v3 認証を使用できます。

5. NTP v3 認証を有効にした場合、該当する各 NTP サーバーで、認証キーとインデックスを設定する必要があります。M-MD5 鍵、SHA1 鍵、またはその両方を指定できます。M-MD5 鍵または SHA1 鍵をともに指定した場合、XClarity Administrator により、管理対象の Flex System の CMM およびそれをサポートする管理コントローラーに、M-MD5 鍵または SHA1 鍵がプッシュされます。XClarity Administrator では、NTP サーバーを認証するためにこの鍵が使用されます。
  - M-MD5 鍵の場合は、大小英字 (a ~ z、A ~ Z)、数字 (0 ~ 9)、および特殊文字 @# のみが含まれる ASCII 文字列を指定します。
  - SHA1 鍵の場合は、40 文字の ASCII 文字列を指定します (0 ~ 9 および a ~ f のみ使用)。
  - 指定する鍵インデックスと認証鍵は、NTP サーバーで設定されている鍵 ID とパスワード値に一致する必要があります。たとえば、NTP サーバーで入力された SHA1 鍵のインデックスが 5 である場合、XClarity Administrator SHA1 鍵の指定した鍵インデックスも 5 になります。鍵 ID とパスワードの設定の詳細については、NTP サーバーのドキュメントを参照してください。
  - 2 つ以上の NTP サーバーで同じ鍵を使用している場合でも、v3 認証を使用する各 NTP サーバーに鍵を指定する必要があります。
  - V3 認証を有効にし、NTP サーバーの認証鍵とインデックスを指定しない場合は、デフォルトで v1 認証が使用されます。
  - 複数の NTP サーバーを指定した場合、NTP サーバーには、すべて v3 認証またはすべて v1 認証を適用する必要があります。NTP サーバーに対する V3 認証と v1 認証の混在はサポートされていません。
  - V3 認証を使用する複数の NTP サーバーを指定する場合は、鍵が同じでない場合には鍵インデックスが固有であることが必要です。たとえば、NTP サーバー 1 および 2 で SHA1 鍵が異なる場合に、NTP サーバー 1 と 2 で SHA1 鍵インデックス 1 を持つことはできません。他方の NTP サーバーとは異なる鍵インデックスの鍵を受け入れるように、いずれかの NTP サーバーを再構成する必要があります。そうしない場合、鍵インデックスに関連付けられている最後の定義済み鍵が、同じ鍵インデックスを持つすべての NTP サーバーに対して構成されます。

ステップ 3. 「保存」をクリックします。

---

## サービスおよびサポートの構成

使用データ、Lenovo サポート (コール・ホーム)、Lenovo アップロード・ファシリティ、製品保証など、サービスおよびサポートの設定を構成できます。

### 手順

セキュリティーを構成するには、以下の手順を実行してください。

- ステップ 1. 初期セットアップ・ページで、「サービスおよびサポート設定の構成」をクリックします。「サービスおよびサポート」ページが表示されます。

## 定期的なデータ・アップロード

**i 重要** ×

---

初期セットアップ・プロセスを完了するには、このパネルのすべてのステップを実行し、最後に「初期セットアップに戻る」をクリックする必要があります。

お願い製品のご利用方法に関する情報の収集を許可していただくことにより、製品の強化や操作性の向上にご協力ください。

### Lenovo のプライバシーに関する声明

いいえ

#### ハードウェア ?

ハードウェア・インベントリおよびシステム・イベント・データを定期的に Lenovo に送信することに同意します。Lenovo では、このデータを使用して将来のサポート・エクスペリエンスを向上させることができます (たとえば、適切な部品を在庫に含め、お客様に近い場所で用意しておくことができます)。

データの例をダウンロードするには、ここをクリックしてください。

#### 使用量 ?

製品がどのように使用されているかについて Lenovo の理解に役立てるために、使用データを定期的に Lenovo に送信することに同意します。すべてのデータは匿名です。

データの例をダウンロードするには、ここをクリックしてください。

この設定は、「サービスおよびサポート」ページからいつでも変更できます。

適用

ステップ 2. [Lenovo のプライバシーに関する声明](#) を読み、同意します。

注：データを収集して Lenovo に送信する前に、[Lenovo のプライバシーに関する声明](#) に同意する必要があります。プライバシーに関する声明に同意しないことを選択した場合、後で「サービスおよびサポート」→「コール・ホーム構成」ページからプライバシーに関する声明を確認して同意することができます。

ステップ 3. オプションで、使用状況およびハードウェアの情報の収集を Lenovo XClarity Administrator に許可するように選択し、「適用」をクリックします。

以下のタイプのデータを収集して Lenovo に送信することができます。

#### ● 使用データ

使用データを Lenovo に送信することに同意した場合、以下のデータが収集され、毎週送信されます。このデータは匿名です。プライベート・データ (シリアル番号、UUID、ホスト名、IP アドレス、ユーザー名など) が収集されることも、Lenovo に送信されることもありません。

- 実行された操作のログ
- 発生したイベントのリスト、および発生時のタイムスタンプ
- 発生した監査イベントのリスト、および発生時のタイムスタンプ
- 実行されたジョブのリスト、および各ジョブの成功または失敗の情報
- メモリー使用量、プロセッサ使用量、ディスク・スペースを含む、XClarity Administrator のメトリック
- すべての管理対象デバイスに関する限定的なインベントリ・データ

#### ● ハードウェア・データ



ハードウェア・データを Lenovo に送信することに同意した場合、以下のデータが収集され、定期的に送信されます。このデータは匿名ではありません。ハードウェア・データには、UUID やシリアル番号などの属性が含まれています。IP アドレスやホスト名は含まれません。

- **毎日のハードウェア・データ。** 各インベントリー変更には、次のデータが含まれています。
  - インベントリー変更イベント (FQXHMDM0001I)
  - そのイベントに関連付けられているデバイスのインベントリー・データに対する変更
- **毎週のハードウェア・データ。** すべての管理対象デバイスのインベントリー・データが含まれています。

使用データとハードウェア・データが Lenovo に送信されると、イベントが監査ログに記録されます。

この設定はいつでも変更することができ、収集されて Lenovo に送信された最新のアーカイブは、「管理」 → 「サービスおよびサポート」をクリックして「定期的なデータ・アップロード」をクリックすると表示されるリンクを使用してダウンロードできます。

- ステップ 4. オプションで、「**コール・ホーム構成**」をクリックして Lenovo サポートへの自動問題通知(コール・ホーム)をセットアップします。次に、「**適用して有効化**」をクリックしてデフォルトのコール・ホーム・サービス・フォワーダーを作成するか、「**適用のみ**」をクリックして問い合わせ先情報を保存します。

Lenovo サポートへの自動問題通知のセットアップについては、XClarity Administrator オンライン・ドキュメントの**コール・ホームのセットアップ**を参照してください。

- ステップ 5. オプションで、「**Lenovo アップロード・ファシリティ**」をクリックして Lenovo アップロード・ファシリティへの自動問題通知をセットアップします。次に、「**適用して有効化**」をクリックしてデフォルトの Lenovo アップロード・ファシリティ・サービス・フォワーダーを作成するか、「**適用のみ**」をクリックして設定情報を保存します。

Lenovo アップロード・ファシリティへの自動問題通知のセットアップについては、XClarity Administrator オンライン・ドキュメントの**Lenovo アップロード・ファシリティへの自動問題通知のセットアップ**を参照してください。

- ステップ 6. オプションで、「**保証**」をクリックして管理対象デバイスの保証情報を収集するために必要な外部接続を有効にします。

管理対象デバイスの保証状況(延長保証を含む)の表示については、XClarity Administrator オンライン・ドキュメントの**保証情報の表示**を参照してください。

- ステップ 7. 任意で Lenovo が XClarity Administrator に Service Bulletin を送信するのを許可するには、「**Lenovo Bulletin サービス**」をクリックして、「**適用**」をクリックします

Lenovo が送信する Service Bulletin のタイプについての詳細は、XClarity Administrator オンライン・ドキュメントの「**Lenovo からの Bulletin の受け取り**」を参照してください。

- ステップ 8. XClarity Administrator が応答しなくなりリカバリーできない場合にサービス・データとログを収集してダウンロードするために使用できるサービス・リカバリー・パスワードを指定します。

サービス・リカバリー・パスワードについては、XClarity Administrator オンライン・ドキュメントの**サービス・リカバリー・パスワードの変更**を参照してください。

- ステップ 9. 「**初期セットアップに戻る**」をクリックします。



---

## セキュリティの構成

役割グループ、認証サーバー、ユーザー・アカウントのセキュリティ設定、暗号化、証明書などのセキュリティを構成できます。

### 手順

セキュリティを構成するには、以下の手順を実行してください。

- ステップ 1. 初期セットアップ・ページで、「[追加のセキュリティ設定の構成](#)」をクリックします。「セキュリティ」ページが表示されます。
- ステップ 2. カスタマイズされた役割グループを作成して、リソースに対する許可やアクセスを管理します (XClarity Administrator オンライン・ドキュメントの[役割グループの作成](#)を参照)。

役割グループは、1 つ以上の役割のコレクションであり、それらの役割を複数のユーザーに割り当てるために使用されます。役割グループに対して構成する役割により、その役割グループのメンバーであるユーザーに付与されるアクセス・レベルが決まります。XClarity Administrator ユーザーは、それぞれ少なくとも 1 つの役割グループのメンバーになっている必要があります。

- ステップ 3. 認証サーバーを構成します (XClarity Administrator オンライン・ドキュメントの[認証サーバーの管理](#)を参照)。

認証サーバーは、ユーザー資格情報の認証に使用される Microsoft Active Directory (LDAP) サーバーです。XClarity Administrator では、1 台の認証サーバーを使用してすべての管理対象デバイスのユーザーを一元管理します (Flex スイッチを除く)。デバイスが XClarity Administrator によって管理されている場合、管理対象デバイスと、そのデバイスに取り付けられているコンポーネント (Flex スイッチを除く) を、XClarity Administrator の認証サーバーを使用するように構成します。これにより、認証サーバーで定義されているユーザー・アカウントが XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されるようになります。

管理ノードのローカル認証サーバーの代わりに外部認証サーバーを使用できます。

- ステップ 4. パスワードの複雑さ、アカウントのロックアウト、Web 非アクティブ・セッションのタイムアウトを制御するユーザー・アカウントのセキュリティ設定を構成します (XClarity Administrator オンライン・ドキュメントの[ユーザー・アカウントのセキュリティ設定の変更](#)を参照)。
- ステップ 5. XClarity Administrator と管理対象デバイス間のセキュアな通信の処理方法を制御する通信モードとプロトコルを定義する暗号化設定を構成します (XClarity Administrator オンライン・ドキュメントの[暗号モードと通信プロトコルの設定](#)を参照)。
- ステップ 6. XClarity Administrator 管理対象認証ではなくローカル認証を使用してラック・サーバーを管理する場合は、管理プロセス中にサーバーへのログインに使用するデバイスまたは Active Directory で、アクティブなユーザー・アカウントに対応する保存された資格情報を 1 つ以上作成します。保存された資格情報について詳しくは、XClarity Administrator オンライン・ドキュメントの[保存された資格情報の管理](#)を参照してください。
- ステップ 7. 自分の情報が含まれているカスタマイズされたサーバー証明書や、外部署名された証明書を使用する場合は、システムの管理を開始する前に新しい証明書をデプロイする必要があります。独自のセキュリティ証明書の生成については、XClarity Administrator オンライン・ドキュメントの[セキュリティ証明書の使用](#)を参照してください。
- ステップ 8. 「セキュリティ」ページの縦方向のメニューで、「[初期セットアップに戻る](#)」をクリックします。

---

## デバイスの管理

Lenovo XClarity Administrator では、Flex System シャーシ、ラック/タワー・サーバー、RackSwitch スイッチ、ストレージ・デバイスなど、複数のタイプのシステムを管理できます。一括インポート・ファイルを使用してデバイスに関する情報をインポートすることによって、環境内の多数のデバイスを簡単に検出および管理できます。

### 始める前に

#### 重要：

- 最大 300 台のデバイスを一度に管理できます。一括インポート・ファイルには 300 台を超えるデバイスを含めないでください。
- デバイス管理操作を開始した後、管理ジョブ全体が完了するまで待ってから、別のデバイス管理操作を開始します。

シャーシ・コンポーネント (CMM、計算ノード、スイッチ、およびストレージ・デバイスなど) は、それらを含むシャーシを管理する際に自動的に検出され管理されます。シャーシとは別にシャーシ・コンポーネントを検出、管理することはできません。

特定のポートがシャーシ内の CMM およびサーバー内のベースボード管理コントローラーとの通信に使用できる必要があります。システムを管理する前に、これらのポートが使用可能になっていることを確認します。ポートについて詳しくは、[利用可能なポート](#)を参照してください。

XClarity Administrator を使用して管理する各システムに、最小限必要なファームウェアがインストールされていることを確認します。[XClarity Administrator のサポート - 互換性に関する Web ページ](#)から最小限必要なレベルのファームウェアを見つけるには、[互換性](#)タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

CMM とのアウト・オブ・バンド通信に使用する TCP コマンド・モード・セッションが少なくとも 3 つ設定されていることを確認します。セッション数の設定については、[CMM オンライン・ドキュメント](#)の `tcpcmdmode` コマンドを参照してください。

XClarity Administrator によって管理されているすべての CMM と Flex スイッチに対して、IPv4 または IPv6 アドレスのいずれかを実装することを検討してください。一部の CMM と Flex スイッチに IPv4 を実装し、その他の CMM と Flex スイッチに IPv6 を実装すると、一部のイベントが監査ログで (または監査トラップとして) 取得されない可能性があります。

マルチキャスト SLP 転送が環境内のルーターと同様にラック装着スイッチで有効になっていることを確認します。マルチキャスト SLP 転送が有効になっているかどうかを調べる方法や、無効になっている場合に有効にする方法については、そのスイッチやルーターに付属のドキュメントを参照してください。

#### 重要：

- RackSwitch スイッチのファームウェア・バージョンによっては、スイッチが XClarity Administrator によって検出・管理できるように、以下のコマンドを使用して各 RackSwitch スイッチでマルチキャスト SLP 転送および SSH を手動で有効にする必要がある場合があります。詳しくは、[System x オンライン・ドキュメントのラック装着スイッチ](#)参照してください。
- XClarity Administrator によって各ストレージ・デバイスを検出するには、マルチキャスト SLP 転送を各システムで有効にする必要があります。
- 自分の情報が含まれているカスタマイズされたサーバー証明書や、外部署名された証明書を使用する場合は、システムの管理を開始する前に新しい証明書をデプロイする必要があります。独自のセキュリティー証明書の生成については、XClarity Administrator オンライン・ドキュメントの[セキュリティー証明書の使用](#)を参照してください。

- Lenovo XClarity Administrator の他に別の管理ソフトウェアを使用してシャーシを監視する場合、その管理ソフトウェアで SNMPv3 通信が使用されているときは、まず、適切な SNMPv3 情報で構成されたローカル CMM ユーザー ID を作成し、そのユーザー ID で CMM にログインして、パスワードを変更する必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントの[管理に関する考慮事項](#)を参照してください。
- SLP や SSDP などのサービス検出プロトコルを使用すると、XClarity Administrator で、管理するデバイスのタイプを自動的に検出して、適切なメカニズムを使用してデバイスを管理することができます。一部のデバイス・タイプではサービス検出プロトコルがサポートされません。また、一部の環境では、サービス検出プロトコルが意図的に無効になっています。いずれの場合も、適切なデバイス・タイプを選択して管理プロセスを完了する必要があります。以下のデバイス・タイプは、明示的に識別する必要があります。
  - Lenovo ThinkSystem DB シリーズ・スイッチ
  - NVIDIA Mellanox スイッチ

## このタスクについて

XClarity Administrator では、XClarity Administrator と同じ IP サブネットにある管理可能デバイスのプローブ、指定した IP アドレスまたは IP アドレス範囲の使用、またはスプレッドシートからの情報のインポートによって、環境内のシステムを検出できます。

デフォルトでは、デバイスは XClarity Administrator 管理対象認証を使用したデバイスへのログインを使用して管理されます。ラック・サーバーおよび Lenovo シャーシを管理する場合、デバイスへのログインにローカル認証を使用するか管理対象認証を使用するかを選択できます。

- ラック・サーバー、Lenovo シャーシ、および Lenovo ラック・スイッチにローカル認証が使用されている場合、XClarity Administrator はデバイスに対する認証に保存された資格情報を使用します。保存された資格情報は、デバイスのアクティブなユーザー・アカウントまたは Active Directory サーバーのユーザー・アカウントにできます。

ローカル認証を使用してデバイスを管理する前に、デバイスのアクティブ・ユーザー・アカウントまたは Active Directory サーバーのユーザー・アカウントに一致する、XClarity Administrator に保存される資格情報を作成する必要があります (XClarity Administrator オンライン・ドキュメントの[保存された資格情報の管理](#)を参照)。

注：

- RackSwitch デバイスは、認証用にのみ保存される資格情報をサポートします。XClarity Administrator ユーザー資格情報はサポートされていません。
- **管理対象認証**を使用することで、ローカル認証資格情報の代わりに、XClarity Administrator 認証サーバーの資格情報により、複数のデバイスを管理および監視できます。デバイス (ThinkServer サーバー、System x M4 サーバー、およびスイッチを除く) で管理対象認証が使用されている場合、XClarity Administrator は、そのデバイスとそこに取り付けられているコンポーネントを、集中型管理用の XClarity Administrator 認証サーバーを使用するように構成します。
  - 管理対象認証が有効な場合、手動で入力した資格情報か、保存された資格情報のいずれかを使用してデバイスを管理できます (XClarity Administrator オンライン・ドキュメントの[ユーザー・アカウントの管理](#) および [保存された資格情報の管理](#)を参照)。
 保存された資格情報は、XClarity Administrator が、デバイスの LDAP 設定を構成するまでの間のみ使用されます。その後は、保存された資格情報を変更しても、デバイスの管理または監視に影響しません。

注：デバイスに対して管理対象認証が有効になっている場合、XClarity Administrator を使用してそのデバイスの保管された資格情報を編集することはできません。

- XClarity Administrator 認証サーバーとしてローカルまたは外部 LDAP サーバーを使用している場合は、その認証サーバーで定義されているユーザー・アカウントが XClarity Administrator ドメイン内の

XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されます。ローカルの CMM および管理コントローラー・ユーザー・アカウントは無効になります。

- XClarity Administrator 認証サーバーとして SAML 2.0 ID プロバイダーを使用する場合、SAML アカウントは、管理対象デバイスにアクセスできなくなります。ただし、SAML ID プロバイダーと LDAP サーバーを同時に使用する場合で、ID プロバイダーが LDAP サーバーにあるアカウントを使用する場合、LDAP ユーザー・アカウントを使用して管理対象デバイスにログインできます。また、SAML 2.0 が提供するより高度な認証方法 (マルチファクター認証およびシングル・サインオンなど) を使用して XClarity Administrator にログインすることもできます。
- シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます (XClarity Administrator オンライン・ドキュメントの「[サーバーの管理](#)」を参照)

注：認証に CyberArk ID 管理システムを使用すると、シングル・サインオンは自動的に無効になります。

- ThinkSystem SR635 および SR655 サーバーで管理対象認証が有効になっている場合:
  - ベースボード管理コントローラー・ファームウェアは、最大 5 つの LDAP ユーザー・ロールをサポートします。XClarity Administrator は、管理中に次の LDAP ユーザー・ロールをサーバーに追加します: `lxc-supervisor`、`lxc-sysmgr`、`lxc-admin`、`lxc-fw-admin` および `lxc-os-admin`。  
ThinkSystem SR635 および SR655 サーバーと通信するには、指定された少なくとも 1 つの LDAP ユーザー・ロールにユーザーが割り当てられている必要があります。
  - 管理コントローラーのファームウェアは、サーバーのローカル・ユーザーと同じユーザー名の LDAP ユーザーをサポートしていません。
- ThinkServer サーバーおよび System x M4 サーバーの場合は、XClarity Administrator 認証サーバーは使用しません。その代わりに、デバイスで接頭辞「LXCA\_」の後にランダムな文字列が続く IPMI アカウントが作成されます。(既存の IPMI ローカル・ユーザー・アカウントは無効になります。)ThinkServer サーバーを管理解除する場合は、「LXCA\_」ユーザー・アカウントが無効になり接頭辞「LXCA\_」が接頭辞「DISABLED\_」に置き換えられます。ThinkServer サーバーが別のインスタンスによって管理されているかどうかを判別するために、XClarity Administrator は接頭辞「LXCA\_」がついた IPMI アカウントを確認します。管理対象 ThinkServer サーバーの管理を強制することを選択した場合、そのデバイスで「LXCA\_」がついたすべての IPMI アカウントが無効になり名前を変更されます。不要になった IPMI アカウントを手動で消去することを検討してください。

手動で入力した資格情報を使用する場合、XClarity Administrator は自動的に保存された資格情報を作成し、その保存された資格情報を使用してデバイスを管理します。

注：デバイスに対して管理対象認証が有効になっている場合、XClarity Administrator を使用してそのデバイスの保管された資格情報を編集することはできません。

- 手動で入力した認証情報を使用してデバイスを管理するたびに、以前の管理プロセス中にそのデバイス用に別の保存済み認証情報が作成されていても、そのデバイス用に新しい保存済み認証情報が作成されます。
- デバイスを管理解除しても、XClarity Administrator は、管理プロセス中にそのデバイス用に自動的に作成され保管されている資格情報を削除しません。

システムが XClarity Administrator の管理対象になった後、XClarity Administrator は各管理対象システムを定期的にポーリングして、インベントリ、重要な製品データ、ステータスなどの情報を収集しま



す。各管理対象システムを表示および監視して、管理操作(システム設定、オペレーティング・システム・イメージのデプロイ、電源オン/オフなど)を実行できます。

1台のシステムを同時に管理できるのは1つのXClarity Administratorのみです。複数のマネージャーによる管理はサポートされていません。システムが1つのXClarity Administratorの管理対象になっており、そのシステムを別のXClarity Administratorの管理対象にする場合は、まず、現在のXClarity Administratorの管理対象から除外する必要があります。この後、そのシステムを別のXClarity Administratorの管理対象にすることができます。システムの管理解除については、XClarity Administrator オンライン・ドキュメントの [シャーシの管理解除](#)、[サーバーの管理解除](#)、[RackSwitch スイッチの管理解除](#) および [Lenovo Storage ストレージ・システムの管理解除](#) を参照してください。

注：XClarity Administrator の管理プロセスでは、セキュリティ設定または暗号化設定(暗号モードとセキュアな通信に使用されるモード)は変更されません。暗号化設定は、システムを管理対象にした後に変更できます(XClarity Administrator オンライン・ドキュメントの [暗号モードと通信プロトコルの設定](#) を参照)。

注：XClarity Administrator に、デモ・シャーシ(CMM、計算ノード、スイッチなど)と、実際のハードウェアをシミュレートするデモ・ラックまたはタワー・サーバーのハードウェア・インベントリを事前に取り込むことができます。デモ・デバイスが Web インターフェース・ページで装備されており、これを使用して管理操作を試すことができます。ただし、管理操作は失敗します。たとえば、構成パターンを作成し、デモ・サーバーにパターンをデプロイすることができますが、デプロイメントは失敗します。デモ・デバイスは、それらを管理解除することで削除できます([シャーシの管理解除](#) および XClarity Administrator オンライン・ドキュメントの [サーバーの管理解除](#) を参照)。デモ・デバイスが削除されると、再度管理することはできません。

## 手順

XClarity Administrator で一括インポート・ファイルを使用してシステムを検出、管理するには、以下のステップを実行します。

注：一括インポートを使用してスイッチを管理する場合、HTTPS はスイッチで有効になり、スイッチの NTP クライアントは管理サーバーの NTP 設定を使用するように構成されます。これらの設定を変更するには、手動でスイッチを管理する必要があります。

1. XClarity Administrator のメニュー・バーで、「ハードウェア」→「新しいデバイスの検出と管理」をクリックします。「検索と管理」ページが表示されます。
2. 管理プロセス中にすべてのデバイスのファイアウォール規則を変更して XClarity Administrator からの受信要求のみを受け入れるようにするには、「今後すべての管理対象デバイスで Encapsulation を有効にする」チェックボックスをクリックします。

注：

- Encapsulation は、スイッチ、ストレージ・デバイスおよび Lenovo 以外のシャーシおよびサーバーではサポートされていません。
- 動的ホスト構成プロトコル(DHCP)を使用するように管理ネットワーク・インターフェースを構成し、encapsulation を有効にすると、ラック・サーバーの管理に長時間かかります。

Encapsulation は、特定のデバイスが管理対象になった後で有効または無効にできます。

注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、[管理サーバーの障害発生後の CMM による シャーシ管理のリカバリー](#) および XClarity Administrator オンライン・ドキュメントの [管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー](#) を参照してください。

3. 「一括インポート」をクリックします。「一括インポート」ウィザードが表示されます。

## 一括インポート

### データ・ファイルのインポート

ステップ 1: テンプレート・ファイルを **Excel** または **CSV** 形式でダウンロードします

ステップ 2: テンプレート・ファイルに情報を入力して、CSV 形式で保存します

ステップ 3: CSV ファイルをアップロードして処理します

- 「データ・ファイルのインポート」ページで「Excel」リンクまたは「CSV」リンクをクリックして、Excel 形式または CSV 形式でテンプレート一括インポート・ファイルをダウンロードします。

**重要:** テンプレート・ファイルは、リリースごとに異なる可能性があります。常に最新のテンプレートを使用するよう注意してください。

- テンプレート・ファイル内のデータ・ワークシートに入力し、そのファイルをコンマ区切りの CSV 形式で保存します。

**ヒント:** Excel テンプレートには、**Data** ワークシートと **Readme** ワークシートが含まれています。**Data** データ・ワークシートを使用して、デバイス・データに入力します。**Readme** ワークシートからは、必須のフィールドなど、**Data** ワークシートの各フィールドへの入力方法に関する情報やサンプル・データを得られます。

### 重要:

- デバイスは、一括インポート・ファイルに記載されている順序で管理されます。
- XClarity Administrator では、デバイスが管理されている場合に、デバイスの構成で定義されているラックの割り当て情報を使用します。XClarity Administrator でラックの割り当てを変更した場合、XClarity Administrator によりデバイス構成が更新されます。デバイスの管理後にデバイスの構成を更新した場合、その変更内容が XClarity Administrator に反映されます。
- ラックをデバイスに割り当てる前に、スプレッドシートでラックを明示的に作成することは、必須ではありませんが、推奨されます。ラックが明示的に定義されていない場合で、XClarity Administrator にラックがまだ存在していないときは、デフォルトの 52U の高さのラックを作成するために、デバイスに指定されたラックの割り当て情報が使用されます。  
ラックで別の高さを使用する場合は、デバイスに割り当てる前に、スプレッドシートでラックを明示的に定義する必要があります。

一括インポート・ファイルでデバイスを定義するには、次の列に入力します。

- (列 A ~ C) 基本検出を行うには、デバイス・タイプと、デバイスの現在の IP アドレスまたはシリアル番号のいずれかを指定する必要があります。サポートされているタイプは以下のとおりです。
  - filler**。管理対象外デバイスのプレースホルダー。ラック・ビューでは、このデバイスは汎用フィルター・グラフィックとして表示されます。他のフィルター・タイプについては、Excel テンプレートの **Readme** ワークシートを参照してください。
  - flexchassis**。10U Flex System Chassis
  - server**。XClarity Administrator によりサポートされているラック・サーバーおよびタワー・サーバー
  - rack**。6U、12U、18U、25U、37U、42U、45U、46U、48U、50U、および 52U のラック。その他のラックの高さはサポートされていません。デフォルトでは 52U が使用されます。
  - storage**。ストレージ・デバイス
  - switch**。RackSwitch スイッチ

注：Flex System 計算ノード、スイッチ、およびストレージ・デバイスはシャーシ検出および管理プロセスの一部と見なされます。

- (列 D ~ H) 保存された資格情報 (列 Z) または ID (列 AF ~ AJ) の代わりに手動で入力された資格情報を使用する場合は、現在のユーザ名とパスワードを指定します。一部のデバイスの資格情報が異なる場合は、手動で入力された資格情報が便利です。ファイルの一括インポートに 1 つ以上のデバイスの資格情報を指定しない場合、「一括インポート」ダイアログで指定したグローバル資格情報が代わりに使用されます。手動で入力されたユーザーおよび管理対象資格情報について詳しくは、XClarity Administrator オンライン・ドキュメントの [ユーザー・アカウントの管理](#) を参照してください。

注：

- 手動で入力した資格情報を使用するには、XClarity Administrator 管理対象認証を選択する必要があります。
- 一部のデバイスに適用されないフィールドもあります。
- (シャーシの場合) 管理対象認証を選択 (列 AA または一括インポート・ダイアログで) する場合、一括インポート・ファイルの列 G または一括インポート・ダイアログで RECOVERY\_ID パスワードを指定できます。ローカル認証を選択した場合、リカバリー・パスワードは使用できません。一括インポート・ファイルの G 列または一括インポート・ダイアログで、リカバリー・パスワードを指定しないでください。
- (ラック・サーバーの場合) 管理対象認証を選択 (列 AA または一括インポート・ダイアログで) する場合、オプションで一括インポート・ファイルの列 G または一括インポート・ダイアログでリカバリー・パスワードを指定できます。ローカル認証を選択した場合、リカバリー・パスワードは使用できません。一括インポート・ファイルの G 列または一括インポート・ダイアログで、リカバリー・パスワードを指定しないでください。
- (ラックスイッチの場合) RackSwitch デバイスでは、スイッチ認証用に (列 Z に) 保存された資格情報のみがサポートされます。手動のユーザー資格情報はサポートされません。
- (列 I ~ U) 管理が成功したときにデバイスに変更を適用する場合は、必要に応じて追加情報を提供できます。

注：一部のデバイスに適用されないフィールドもあります。これらのフィールドは RackSwitch スイッチには適用されません。

- (列 V ~ Z) 必要に応じて、ラックの名前、場所、部屋、最小ラック・ユニット、高さなど、ラックの作成と割り当てのための情報を提供できます。

注：

- ラックを作成する際、ラックの名前、ラックの高さを指定する必要があります。サポートされているラックの高さは、6U、12U、18U、25U、37U、42U、45U、46U、48U、50U、および 52U です。その他のラックの高さはサポートされていません。
- 汎用フィルターを作成する際、ラックの名前、フィルターの高さを指定する必要があります。サポートされているフィルターの高さは、1U、2U、および 4U です。
- 特定のフィルターを作成する場合、フィルターの高さは無視されます。XClarity Administrator では、特定の各フィルターの高さが認識されます。フィルターのタイプと高さについては、テンプレートのスプレッドシートを参照してください。
- ラックにデバイスを割り当てる場合、デバイスの高さは無視されます。デバイスの高さは、デバイスのインベントリから取得されます。
- (列 AA) 以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。
  - 管理元の XClarity Administrator で障害が発生したため、復元できない場合。



注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY\_ID アカウントとパスワード (該当する場合)、および「管理の強制」オプションを使用してデバイスを再度管理できます。

- デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
- デバイスが正しく管理対象から除外されなかった場合。

デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

**重要：**サーバーが XClarity Administrator によって管理された後、サーバーの IP アドレスを変更する場合、XClarity Administrator は新しい IP アドレスを認識し、サーバーの管理を続けます。ただし、XClarity Administrator は一部のサーバーの IP アドレスの変更を認識しません。IP アドレスを変更した後、XClarity Administrator でサーバーがオフラインであると表示される場合は、「管理の強制」オプションを使用してサーバーを再度管理します。

- (列 AB) 手動で入力された資格情報 (列 D ~ H) または ID (列 AF ~ AJ) の代わりに、保存された資格情報を使用する場合は、保存された資格情報 ID を指定します。保存された資格情報ページで保存された資格情報の ID を見つけるには、XClarity Administrator メニューから「管理」→「セキュリティ」をクリックして、左ナビゲーションで「保存された資格情報」をクリックします。保存された資格情報およびローカル認証について詳しくは、および XClarity Administrator オンライン・ドキュメントの[保存された資格情報の管理](#)を参照してください。

注：

- RackSwitch デバイスは、認証用に保存された資格情報のみをサポートします。手動のユーザー資格情報 (列 D) はサポートされません。
- 保存された資格情報を使用してデバイスを管理し、管理対象の認証を有効にする場合、保存された資格情報を編集することはできません。
- (列 AC) シャーシとラック・サーバーで、管理対象認証を選択した場合、一括インポート・ファイルの列 G または一括インポート・ダイアログで RECOVERY\_ID パスワードを指定できます。ローカル認証を選択した場合、リカバリー・パスワードは使用できません。一括インポート・ファイルの G 列または一括インポート・ダイアログで、リカバリー・パスワードを指定しないでください。
- (列 AD) ラック・サーバーの場合、この列に FALSE を指定することによって、オプションで XClarity Administrator 管理対象認証の代わりに、ローカル認証を使用するように選択できます。管理対象認証およびローカル認証について詳しくは、XClarity Administrator オンライン・ドキュメントの[認証サーバーの管理](#)を参照してください。
- (列 AE) オプションでデバイスを表示および管理できる役割グループの一覧を指定できます。現在のユーザーが属する役割グループのみを指定できます。

注：管理対象シャーシにデバイスを追加した場合、新しいデバイスはシャーシと同じ役割グループに属します。

- (列 AF ~ AJ) 手動で入力された資格情報 (列 D ~ H) または保存された資格情報 (列 AB) の代わりに ID 管理システムを使用する場合は、管理対象サーバーの IP アドレスまたはホスト名、ユーザー名、およびオプションでアプリケーション ID、セーフ、およびフォルダーを指定します。アプリケーション ID を指定する場合は、必要に応じて、セーフとフォルダーも指定する必要があります。

アプリケーション ID を指定しない場合、XClarity Administrator は、CyberArk セットアップ時に定義したパスを使用して、CyberArk のオンボード・アカウントを識別します。

注：ThinkSystem サーバーまたは ThinkAgile サーバーのみがサポートされます。ID 管理システムは XClarity Administrator で構成する必要があります。また、管理対象の ThinkSystem サーバーまたは ThinkAgile サーバーの Lenovo XClarity Controller は CyberArk と統合する必要があります。

以下の図は、一括インポート・ファイルの例を示しています。

| Required fields (Type + SN or IP) |               |            | Optional fields  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
|-----------------------------------|---------------|------------|------------------|------------------|--------------|-------------------|------------------------|------------|------------------|----------------------|------------|------------|----------|-------------|--------------|-----------|-----------|--------|----------------|----------------|
| Type                              | Serial Number | Current IP | Current username | Current password | New password | Recovery password | Switch enable password | New IPv4   | IPv4 subnet mask | IPv4 default gateway | IPv4 DNS1  | IPv4 DNS2  | New IPv6 | IPv6 prefix | IPv6 gateway | IPv6 DNS1 | IPv6 DNS2 | Domain |                |                |
| server                            |               | 10.1.0.198 |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| server                            | P67X30EL      |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| flexchassis                       |               | 10.1.0.213 | USERID           | passw0rdx        | Pa55word@    | abcd1234          |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| flexchassis                       | Z3499DD       |            |                  |                  | Pa55word@    | abcd1234          |                        | 9.27.20.51 | 255.255.255.0    | 9.27.20.1            | 9.0.148.50 | 9.0.146.50 |          |             |              |           |           |        | ebg.lenovo.com |                |
| server                            | 35T88XP       |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             | 2002:939     | 2002:9    | 2002:939  | 2002:9 | 2002:9         | ebg.lenovo.com |
| server                            |               | 10.1.0.214 |                  |                  |              |                   |                        | 10.1.2.213 | 255.255.255.0    | 10.1.2.1             | 9.0.148.50 | 9.0.146.50 |          |             |              |           |           |        | ebg.lenovo.com |                |
| rack                              |               |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| filler                            |               |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| filler                            |               |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |
| filler                            |               |            |                  |                  |              |                   |                        |            |                  |                      |            |            |          |             |              |           |           |        |                |                |

| IPv6 DNS2 | Domain         | Host name | User-defined name | Rack name | Location | Room | Lowest rack unit | Height | Force | Stored credentials ID | Stored credentials ID for RECOVERY_ID | Managed authentication | Role Groups | Identity/Managements systemEnabled | IMS type | IMS AppID | Folder | Safe |
|-----------|----------------|-----------|-------------------|-----------|----------|------|------------------|--------|-------|-----------------------|---------------------------------------|------------------------|-------------|------------------------------------|----------|-----------|--------|------|
|           |                |           |                   |           |          |      |                  |        |       |                       |                                       |                        |             | TRUE                               | CyberArk | LXCA      |        | Test |
|           | ebg.lenovo.com | chassis01 | chassis01         | SH3G05A34 |          |      |                  | 25     | TRUE  |                       |                                       |                        |             |                                    |          |           |        |      |
| 2002:9    | ebg.lenovo.com | host4     | c02node01         | SH3G05B12 |          |      |                  | 38     |       |                       | 2                                     | 3                      | FALSE       |                                    |          |           |        |      |
|           | ebg.lenovo.com | host5     | web02             | SH3G05B12 |          |      |                  | 10     |       |                       |                                       |                        |             |                                    |          |           |        |      |
|           |                |           | SG2R01A01         |           |          |      |                  | 37     |       |                       |                                       |                        |             |                                    |          |           |        |      |
|           |                |           | SH3G05A34         |           |          |      |                  | 46     |       |                       |                                       |                        |             |                                    |          |           |        |      |
|           |                |           | APC UPS           | SH3G05A34 |          |      |                  | 1      | 4     |                       |                                       |                        |             |                                    |          |           |        |      |
|           |                |           | FC switch         | SH3G05A34 |          |      |                  | 40     | 2     |                       |                                       |                        |             |                                    |          |           |        |      |
|           |                |           | KVM switch        | SH3G05B12 |          |      |                  | 22     | 1     |                       |                                       |                        |             |                                    |          |           |        |      |

- 「一括インポート」ウィザードで、CSV ファイルの名前を入力して処理するファイルをアップロードします。このファイルを見つけるには、「参照」をクリックします。
- 「アップロード」をクリックしてアップロードし、ファイルを検証します。
- 「次へ」をクリックすると、「入力要約」ページに管理対象デバイスの一覧が表示されます。

### 一括インポート

4 管理される合計デバイス数: シャーシ x 1・スイッチ x 1・サーバー x 2・ストレージ x 0

| CSV Row | Name      | Current IP | Credentials | Type        |
|---------|-----------|------------|-------------|-------------|
| 2       | Server_1  | 192.0.2.0  | 入力が必要       | server      |
| 3       | Chassis_1 |            | 入力が必要       | flexchassis |
| 4       | Rack_2    |            | 入力が必要       | rack        |
| 5       | Filler    |            | 入力が必要       | filler      |

- 管理するデバイスの要約を確認します。  
「潜在的な問題を含む行のみを表示」を選択すると、不完全なデータを含む行が一覧表示されます。一括インポート・ファイルで問題を修正した後、「戻る」をクリックして修正された CSV ファイルをアップロードします。

### 注：

- 必要なデータが一括インポート・ファイルで指定されていない場合、関連するデバイスは管理されていません。
- 「入力要約」ページで、資格情報を含まない行にフラグが付けられます。ファイルの一括インポートに資格情報を指定しない場合、「一括インポート」ウィザードで指定したグローバル資格情報が代わりに使用されます。

10. 「次へ」をクリックして、「デバイスの資格情報」ページを表示します。

## 一括インポート

### デバイスの資格情報

これらのデバイスの管理を続行するには、1つ以上の資格情報セットが必要です。これらの資格情報は、デバイス・タイプごとにここに入力してください。完了したら、「管理」を押して管理プロセスを開始します。

シャーシ (1)    サーバー (2)    スイッチ (1)    ストレージ    リカバリー (3)

#### Chassis

管理対象認証を使用するかどうかを選択

管理対象認証

資格情報のタイプを選択

手動で入力した資格情報を使用  
 保存された資格情報を使用

Chassis Management Module

現在の資格情報 (共通)

ユーザー名  
パスワード

新しい資格情報 (共通)  
(注: 現在の資格情報の有効期限が切れた場合にのみ使用されます)

新しいパスワード  
パスワードの確認

システムが Lenovo® XClarity Administrator の別のインスタンスまたは別のインスタンスによって管理されている場合の管理の強制  
管理を強制する場合は、リカバリー ID 管理を使用する必要があります。

#### これらの資格情報を使用するデバイス

Chassis\_1

11. **オプション:** 各タブをクリックし、必要に応じて、特定タイプのすべてのデバイスで使用するグローバルな設定と資格情報を指定します。グローバルな設定と資格情報を使用するデバイスは、各タブの右側に表示されます。

グローバル資格情報を使用する場合は、特定のデバイス・タイプの資格情報は、一括インポート・ファイルに資格情報が入力されていない同タイプのすべてのデバイスで同じである必要があります。たとえば、CMMの資格情報はすべてのシャーシで同じである必要があります。また、ストレージ管理の資格情報はすべてのストレージ・デバイスで同じである必要があります。資格情報が同じでない場合は、一括インポート・ファイルに資格情報を入力する必要があります。

- **Chassis.** 認証モードおよび資格情報のタイプを指定します。一括インポート・ファイルで定義されている、すべてのシャーシへのログインに使用する現在の資格情報を指定します。現在のCMM資格情報の有効期限が切れている場合は、新しいパスワードを指定します。

シャーシの管理を強制した場合、デバイスの資格情報の RECOVERY\_ID アカウントとパスワードを指定します。

- **サーバー.** 認証モードおよび資格情報のタイプを指定します。一括インポート・ファイルで定義されている、すべてのラックおよびタワー・サーバーへのログインに使用する現在の資格情報を指定します。現在のベースボード管理コントローラー資格情報の有効期限が切れている場合は、新しいパスワードを指定します。

サーバーの管理を強制した場合、デバイスの資格情報の RECOVERY\_ID アカウントとパスワードを指定します。

- **スイッチ**。一括インポート・ファイルで定義されている、すべての RackSwitch スイッチへのログインに使用する保存された資格情報を指定します。設定されている場合は、スイッチの特権実行モードに入るために使用する「有効」パスワードも指定します。
- **ストレージ**。一括インポート・ファイルで定義されている、すべてのストレージ・デバイスへのログインに使用する現在の資格情報を指定します。
- **リカバリー**。一括インポート・ファイルで定義されている、すべてのサーバーおよびシャーシへのログインに使用するリカバリー・パスワードを指定します。

ローカル・ユーザー・アカウントまたは保存されているリカバリー資格情報を使用するように選択できます。いずれの場合も、ユーザー名は常に RECOVERY\_ID です。

パスワードを指定すると、この RECOVERY\_ID がデバイスで作成され、すべてローカル・ユーザー・アカウントが無効になります。

- シャーシの場合、リカバリー・パスワードが必要です。
- サーバーの場合、管理対象認証を使用するように選択した場合は、リカバリー・パスワードはオプションです。ローカル認証を使用するように選択した場合は利用できません。
- パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。
- リカバリー・パスワードは後で使用できるように記録しておいてください。
- リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。

一括インポート・ファイルで指定した情報により、「デバイスの資格情報」ページで指定した類似する情報がオーバーライドされます。

以下の場合に、オプションで、各タイプのデバイスの強制管理を選択できます：

- デバイスが現在、別の XClarity Administrator インスタンスや IBM Flex System Manager など別の管理システムによって管理されている
- XClarity Administrator が停止したが、停止前にデバイスが管理対象から除外されなかった
- デバイスが正常に管理対象から除外されず、CIM サブスクリプションがクリアされなかった場合

注：デバイスが別の XClarity Administrator インスタンスによって管理されている場合、管理の強制が発生してから一定期間は、デバイスが元のインスタンスにより管理されているように見えます。デバイスを管理対象から除外して、元の XClarity Administrator インスタンスから除外できます。

12. 「管理」をクリックします。「結果の監視」ページには、一括インポート・ファイル内の各デバイスの管理ステータスに関する情報が表示されます。

管理プロセスのジョブが作成されます。一括インポート・ウィザードを終了する場合はバックグラウンドで実行されている管理プロセスが続行します。ジョブ・ログから管理プロセスのステータスを監視できます。ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントの [ジョブの監視](#) を参照してください。

XClarity Administrator が、一括インポート・ファイルに指定された資格情報またはダイアログで指定されたグローバル資格情報を使用してデバイスにログインできない場合、そのデバイスの管理は失敗し、XClarity Administrator は一括インポート・ファイル内の次のデバイスに進みます。

注：以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「**管理の強制**」オプションを使用してこの手順を繰り返します。

- 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY\_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

- デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。



- デバイスが正しく管理対象から除外されなかった場合。

注意：デバイスを同時に管理できるのは1つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが1つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

13. ファイルの一括インポートに新しいシャーシが含まれている場合、シャーシ全体 (計算ノードと Flex スイッチを含む) の管理ネットワーク設定を検証して変更します。また、サーバー・パターンを作成してデプロイすることで、計算ノードの情報、ローカル・ストレージ、I/O アダプター、ブート・ターゲット、ファームウェア設定を構成します。詳しくは、XClarity Administrator オンライン・ドキュメントの [シャーシの管理 IP 設定の変更](#) および [XClarity Administrator を使用したサーバーの構成](#) を参照してください。

## 終了後

システムを管理した後、次のアクションを実行できます。

- 追加システムを検出および管理します ([シャーシの管理](#)、[ラックの管理](#)、[サーバーの管理](#)、[ストレージ・デバイスの管理](#)、および [スイッチの管理](#) を参照)。
- サーバー・パターンを作成してデプロイすることで、システム情報、ローカル・ストレージ、I/O アダプター、ブート設定、ファームウェア設定を構成します (Lenovo XClarity Administrator オンライン・ドキュメントの [XClarity Administrator を使用したサーバーの構成](#) を参照)。
- オペレーティング・システムがまだインストールされていないサーバーにオペレーティング・システム・イメージをデプロイします (XClarity Administrator オンライン・ドキュメントの [オペレーティング・システム・イメージのデプロイ](#) を参照)。
- 現行ポリシー (XClarity Administrator オンライン・ドキュメントの [管理対象デバイスでのファームウェアの更新](#) を参照) に従っていないデバイスのファームウェアを更新します。
- 新たに管理するシステムを適切なラックに追加して物理的環境を反映します (XClarity Administrator オンライン・ドキュメントの [ラックの管理](#) を参照)。
- ハードウェアのステータスと詳細を監視します (XClarity Administrator オンライン・ドキュメントの [管理対象サーバーのステータスの表示](#) を参照)。
- イベントとアラートを監視します (XClarity Administrator オンライン・ドキュメントの [イベントの使用](#) および [アラートの使用](#) を参照)。
- 管理対象の ThinkSystem および ThinkAgile サーバーのシングル・サインオンを有効または無効にします。
  - すべての管理対象の ThinkSystem および ThinkAgile サーバー (グローバル) については、XClarity Administrator のメニュー・バーで「管理」 → 「セキュリティ」をクリックし、「アクティブ・セッション」をクリックして、「シングル・サインオン」を有効または無効にします。
  - 特定の ThinkSystem および ThinkAgile サーバーについては、XClarity Administrator のメニュー・バーで「ハードウェア」 → 「サーバー」をクリックし、「すべての操作」 → 「セキュリティ」 → 「シングル・サインオンを使用可能にする」または「すべての操作」 → 「セキュリティ」 → 「シングル・サインオンを使用不可にする」をクリックします。

注：シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます。



---

## 第 5 章 XClarity Administrator の登録

Lenovo XClarity Administrator のインスタンスを登録することで、トライアルの有効期限や非準拠ライセンスに関する、繰り返し表示される警告を受け取らずに基本機能を使用できます。登録すると、非準拠ライセンスに関する警告は表示されなくなります。ただし、ライセンスが必要なすべての機能は、管理対象デバイスの数に基づいてライセンスを購入してインストールするまで無効のままになります。

### このタスクについて

XClarity Administrator インスタンスの登録で、お問い合わせ先情報を共有する必要はありません。Lenovo は、提供された情報を他の外部のエンティティと共有することはありません。

拡張機能のライセンスをインストールしている場合は、XClarity Administrator インスタンスを登録する必要はありません。ライセンスおよび拡張機能については、[全機能有効化ライセンスのインストール](#)を参照してください。

### 手順

XClarity Administrator を登録するには、次の手順を実行します。

- XClarity Administrator がインターネットに接続されている場合
  1. Lenovo XClarity Administrator メニュー・バーで、「管理」 → 「登録」をクリックして、「登録」ページを表示します。
  2. 「登録」をクリックして、XClarity Administrator の新しいインスタンスを登録します。
  3. 会社名、XClarity Administrator で管理されるデバイスの数、および XClarity Administrator が配置されている国を入力します。
  4. 「送信」をクリックします。
- XClarity Administrator がインターネットに接続されていない場合
  1. XClarity Administrator を登録します。
    - a. Web ブラウザーで、[Lenovo XClarity 登録 Web ポータル](#)を開きます。
    - b. 会社名、XClarity Administrator で管理されるデバイスの数、および XClarity Administrator が配置されている国を入力します。
    - c. 「送信」をクリックして登録トークンを受け取ります。
  2. Lenovo XClarity Administrator メニュー・バーで、「管理」 → 「登録」をクリックして、「登録」ページを表示します。
  3. 「インポート」をクリックし、登録トークンをインポートします。
  4. ステップ 1 で受信した登録トークンを入力します。
  5. 「送信」をクリックします。





## 第 6 章 全機能有効化ライセンスのインストール

90 日の無料試用期間の経過後、引き続き Lenovo XClarity Administrator のオペレーティング・システムのデプロイ機能およびデバイス構成機能を使用するには、拡張機能をサポートするすべての管理対象デバイスの Lenovo XClarity Pro ライセンスの購入とインストールを行う必要があります。XClarity Administrator サービスおよびサポートを取得するには、すべての管理対象デバイスに対する Lenovo XClarity Pro ライセンスが必要です。

詳細:  [XClarity Administrator: ライセンスのインストール](#)

### 始める前に

以下のライセンスに関する考慮事項を確認してください。

- ライセンスは特定のデバイスに関連付けられていません。
- シャーシ・ライセンスは 14 台のデバイスのライセンスを提供します。
- System x3850 X6 (6241) の拡張可能な複合サーバーの場合、パーティションに関係なく、各サーバーに、個別のライセンスが必要です。
- System x3950 X6 (6241) の拡張可能な複合サーバーの場合、パーティションが存在しない場合は、各サーバーに個別のライセンスが必要です。パーティション分割されている場合は、各パーティションに別個のライセンスが必要です。
- 以下のデバイスでは、高度な機能はサポートされていないため、これら機能に対してライセンスは必要としません。ただし、これらデバイスに対して XClarity Administrator サービスやサポートを取得する場合は、ライセンスをご購入ください。
  - ThinkServer サーバー
  - System x M4 サーバー
  - System x X5 サーバー
  - System x3850 X6 および x3950 X6 (3837) サーバー
  - ストレージ・デバイス
  - スイッチ

ライセンスをインストールするには、`lxc-supervisor` 権限または `lxc-security-admin` 権限が必要です。

### このタスクについて

XClarity Administrator は、以下のライセンスをサポートします。

- **Lenovo XClarity Pro**. 各ライセンスは、1 台のデバイスに対して次の資格を提供します。
  - Lenovo XClarity Integrator のサービスおよびサポート
  - XClarity Administrator のサービスおよびサポート
  - XClarity Administrator 内の高度な機能:
    - 構成パターンを使用したサーバーの構成
    - オペレーティング・システムのデプロイ
    - コール・ホームを使用して XClarity Administrator の問題を報告する (ハードウェア・アラート向けのコール・ホームは影響されません。)

ライセンスのアクティベーション期間は、ライセンスを購入して認証コードが作成されると開始されます。

ライセンス・コンプライアンスは、拡張機能をサポートする管理対象デバイスの数に基づいて決定されます。管理対象デバイスの数は、すべてのアクティブなライセンス・キーに含まれるライセンスの合計数を超えてはなりません。XClarity Administrator がインストール済みのライセンスに準拠していない場合 (たと

えば、ライセンスの有効期限が切れた場合や、追加のデバイスを管理するとアクティブなライセンスの合計数を超える場合)、適切なライセンスをインストールする猶予期間は90日になります。XClarity Administratorが非準拠になるたびに、猶予期間が90日にリセットされます。ライセンスに準拠する前に猶予期間(無料試用期間を含む)が終了した場合、拡張機能はすべてのデバイスで無効になります。


たとえば、既存のXClarity Administratorインスタンス内の追加のThinkSystemサーバー100台とラック・スイッチ20個を管理する場合、ユーザー・インターフェース(すべてのデバイス)で拡張機能が無効になるまでの90日間で、追加のライセンスを100個購入してインストールする必要があります。拡張機能を使用するために20個のラック・スイッチのライセンスは必要ありません。ただし、サービスおよびサポートが必要な場合は、これらを使用する必要があります。拡張機能が無効になっている場合は、十分なライセンスをインストールしてコンプライアンスを回復すると、拡張機能が再び有効になります。

無料試用ライセンスを使用している場合や、猶予期間が準拠するようになった場合に、XClarity Administratorの新しいバージョンにアップグレードした場合、試用ライセンスまたは猶予期間が90日にリセットされます。

注：

- 猶予期間が過ぎると、サーバー構成およびオペレーティング・システム・デプロイメント機能は無効になります。
- XClarity Administratorの問題のためのコール・ホーム(ソフトウェア・コール・ホーム機能)は、ライセンスが準拠していない場合、無効になります。この機能には、猶予期間はありません。ただし、ハードウェア・アラートのコール・ホームは影響を受けません。

ライセンスが既にインストールされている場合、XClarity Administratorの新規リリースにアップグレードする場合に新規のライセンスは必要ありません。

XClarity Administrator タイトル・バーからユーザー操作メニュー (  ) をクリックして、「バージョン情報」をクリックすることで、試用版の残り期間などのライセンスの状況を確認できます。

## ヘルプの入手

- ビジネス・パートナー経由でのご利用で問題が発生した場合は、トランザクションおよび有効化の確認のためにビジネス・パートナーにお問い合わせください。
- 電子有効化証明、許可コードまたはアクティベーション・キーを受信していない、または宛先が正しくないときは、それぞれの地域のいずれかの地域担当者にご連絡ください。
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (北アメリカ)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (アジア太平洋)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (欧州、中東、アジア)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (中南米)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (中国)
- 自身の有効化に関する情報が正しくない場合は、Lenovo サポート([SW\\_override@lenovo.com](mailto:SW_override@lenovo.com))宛てに以下の情報を含むメールでお知らせください。
  - オーダー番号
  - メール・アドレスを含む問い合わせ先情報。
  - ご使用の物理アドレス
  - 必要な変更
- ライセンスのダウンロードに関する問題やご質問は、Lenovo サポート ([-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com)) までお問い合わせください。

# XClarity Administrator Web インターフェースを使用した全機能有効化ライセンスのインストール

XClarity Administrator がインターネットにアクセスできる場合は、XClarity Administrator Web インターフェースを使用して既存の認証のライセンスを引き換えおよび取得して、引き換えたライセンスをインポートしてインストールできます。

## 始める前に

有効にする機能と管理するデバイスの数に基づいて Lenovo XClarity Pro ライセンスを購入するには、Lenovo の担当者または認定ビジネス・パートナーにご連絡ください。ライセンスを購入すると、認証コードが電子有効化証明メールで送られます。認証コードは 22 文字の英数字の文字列で、これをライセンスと引き換えてインストールする必要があります。このメールは受信しない場合で、ビジネス・パートナーからライセンスを購入された場合は、認証コードをビジネス・パートナーにご依頼ください。

Features on Demand Web ポータルで「認証コードの取得」をクリックして、認証コードを取得することもできます。

## 手順

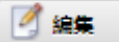
管理サーバーに Lenovo XClarity Pro ライセンスをインストールするには、以下のいずれかの手順を実行します。

### • 単一の認証コードの残りのライセンスのすべてまたは一部の引き換えとインストール


単一の認証コードの使用可能なライセンスのすべてまたは一部を引き換えて、ライセンス・アクティベーション・キー (引き換えたライセンスに関する各情報を含むファイル) を作成できます。そのライセンス・アクティベーション・キー・ファイルを使用して、引き換えたライセンスをインストールできます。

1. XClarity Administrator メニュー・バーで、「管理」 → 「ライセンス」をクリックして、「ライセンス管理」ページを表示します。


### ライセンス管理

警告期間: 90 日 

アクティブキー: 1401 のアクティブな資格のうち 213 を使用 (75 はまもなく有効期限が切れます)

 | すべての操作 ▾ |

| <input type="checkbox"/> | ライセンス・キーの説明  | ライセンスの数 | 開始日        | 有効期限       | ステータス               |
|--------------------------|--------------|---------|------------|------------|---------------------|
| <input type="checkbox"/> | XClarity Pro | 100     | 01/05/2022 | 12/31/2022 | ✔ 有効                |
| <input type="checkbox"/> | XClarity Pro | 126     | 01/05/2022 | 12/30/2023 | ✔ 有効                |
| <input type="checkbox"/> | XClarity Pro | 75      | 01/05/2022 | 01/31/2022 | ⚠ もうすぐ期限切れ、残り日数: 23 |
| <input type="checkbox"/> | XClarity Pro | 1100    | 01/05/2022 | 12/31/2022 | ✔ 有効                |

2. 「アクティベーション・キーの要求」アイコン () をクリックして、「アクティベーション・キーの要求」ダイアログを表示します。
3. 「単一の認証コード」をクリックします。

- 22 文字の認証コードを入力し、「検索」をクリックして、指定した認証コードの購入したライセンスに関する情報を Features on Demand Web サイトから取得します。

受け取った認証コードが受け入れられない場合は、Lenovo サポートにお問い合わせください。

- 「Lenovo お客様番号」フィールドに 10 桁の Lenovo お客様番号を入力します。
- 引き換えるライセンスの数を「引き換え数量」フィールドに入力し、「続行」をクリックします。この認証コードで使用可能なすべてのライセンスを引き換えるには、「使用可能なライセンス数」フィールドと数を一致させます。

使用可能なライセンスの一部を引き換える場合は、後で同じ認証コードを使用して、残りのライセンスを引き換えることができます。

**ヒント:** XClarity Administrator ごとに、最大 1,000 の管理対象デバイスがサポートされます。そのため、XClarity Administrator インスタンスにインストールできる単一のライセンス・アクティベーション・キーのライセンス数が 1,000 を超えることはできません。

- 連絡先情報が正しいことを確認し、必要に応じて変更を行います。
- 「要求の送信」をクリックして、ライセンスを引き換えてライセンス・アクティベーション・キーを作成します。
- インストールするライセンスが含まれているライセンス・アクティベーション・キーを選択します。
- 「インストール」をクリックして、ライセンスを管理サーバーにインストールします。
- 「閉じる」をクリックします。


#### ● 複数の認証コードの残りのすべてのライセンスの引き換えとインストール

複数の認証コードの残りのすべてのライセンスを引き換えることができます。ライセンス・アクティベーション・キーは、それぞれの認証コードに対して作成されます。そのライセンス・アクティベーション・キーを使用して、引き換えたライセンスをインストールできます。認証コードは、指定されたテンプレートを使用して、CSV 形式ファイルで提供する必要があります。

- XClarity Administrator メニュー・バーで、「管理」→「ライセンス」をクリックして、「ライセンス管理」ページを表示します。
- 「アクティベーション・キーの要求」アイコン (🔑) をクリックして、「アクティベーション・キーの要求」ダイアログを表示します。
- 「複数の認証コード」をクリックします。
- 「テンプレートのダウンロード」リンクをクリックして、Excel ファイルを開きます。各認証コードをファイルに追加し、そのファイルを CSV 形式でローカル・システムに保存します。
- 「参照」をクリックして認証コードの CSV ファイルを見つけて選択し、「検索」をクリックして認証コードに関する情報を Lenovo サポート Web サイトから取得します。
- 各認証コードに関連付けられている購入したライセンスと使用可能なライセンス・アクティベーション・キーに関する情報を確認します。
- 「Lenovo お客様番号」フィールドに 10 桁の Lenovo お客様番号を入力します。
- 連絡先情報が正しいことを確認し、必要に応じて変更を行います。次に、「続行」をクリックします。
- 「はい、すべての有効な認証コードを引き換えます」を選択し、「要求の送信」をクリックしてライセンス・アクティベーション・キーを生成します。
- インストールするライセンス・アクティベーション・キーを選択します。
- 「インストール」をクリックして、ライセンス・アクティベーション・キーを管理サーバーにインストールします。
- 「閉じる」をクリックします。



#### ● 引き換えたライセンスの取得とインストール

Features on Demand Web ポータルにアクセスできる XClarity Administrator インスタンスからローカル・システムにライセンス・アクティベーション・キーをダウンロードし、そのライセンス・アクティベーション・キーを別の XClarity Administrator インスタンスにインポートしてインストールできます。これは、インターネットにアクセスできない XClarity Administrator インスタンスにライセンスをインストールする場合や、XClarity Administrator を再インストールしてインストールされていたライセンスを復元する場合に役立ちます。

1. XClarity Administrator メニュー・バーで、「管理」 → 「ライセンス」をクリックして、「ライセンス管理」ページを表示します。
2. 「履歴の取得」アイコン () をクリックして、「履歴を取得」ダイアログを表示します。
3. Lenovo お客様番号または 22 文字の認証コードを入力します。
4. 「検索」をクリックして、使用可能なライセンスと引き換えたライセンスに関する情報を取得します。  
受け取った認証コードが受け入れられない場合は、Lenovo サポートにお問い合わせください。
5. インストールするライセンス・キー・ファイルを選択します。
6. 「インストール」をクリックして、XClarity Administrator にライセンス・アクティベーション・キーをインストールします。
7. 「閉じる」をクリックします。

#### ● 引き換えたライセンスの別の XClarity Administrator インスタンスへのインポートとインストール

XClarity Administrator インスタンスを使用してライセンスを引き換えてそのライセンスを別の XClarity Administrator インスタンスにインストールする場合や、インストールしたライセンスの復元が必要なエラー状況が発生した場合は、ローカル・システムから他の XClarity Administrator インスタンスにライセンス・キー・ファイルをインポートできます。


1. Features on Demand Web ポータルにアクセスできる XClarity Administrator インスタンスから Features on Demand Web ポータルのライセンス・アクティベーション・キーを取得し、そのライセンス・アクティベーション・キーをファイルとしてローカル・システムに保存します。
  - a. XClarity Administrator メニュー・バーで、「管理」 → 「ライセンス」をクリックして、「ライセンス管理」ページを表示します。
  - b. 「履歴の取得」アイコン () をクリックして、「履歴を取得」ダイアログを表示します。
  - c. 22 文字の認証コードを入力します。
  - d. 「検索」をクリックして、その認証コードの使用可能なライセンスと引き換えたライセンスに関する情報を取得します。  
受け取った認証コードが受け入れられない場合は、Lenovo サポートにお問い合わせください。
  - e. インストールするライセンス・アクティベーション・キー・ファイルを選択します。
  - f. 「ダウンロード」をクリックして、ライセンス・キー・ファイルをローカル・システムに保存します。
2. ライセンス・アクティベーション・キーをインストールする XClarity Administrator インスタンスで、以下の操作を実行します。
  - a. XClarity Administrator メニュー・バーで、「管理」 → 「ライセンス」をクリックして、「ライセンス管理」ページを表示します。
  - b. 「インポートして適用」アイコン () をクリックして、ライセンスをインポートしてインストールします。
  - c. 「参照」をクリックして、インストールするライセンスのライセンス・アクティベーション・キーを選択します。  
複数のライセンス・アクティベーション・キーをインポートするには、.KEY ファイルを .ZIP ファイルに圧縮して、その ZIP ファイルを選択してインポートします。
  - d. 「ライセンスに同意する」をクリックし、ライセンスをインポートして適用します。




インストールが完了すると、ライセンス・アクティベーション・キーが、インストール済みのライセンス数やアクティベーション期間 (開始日と有効期限) と一緒に表に表示されます。

## 終了後

「ライセンス」 ページで、以下の操作を実行できます。

- 「**エクスポート**」アイコン () をクリックして、1つ以上の特定のライセンス・アクティベーション・キーをローカル・システムにダウンロードします。

注：複数のライセンス・アクティベーション・キーをエクスポートすると、ファイルは単一の ZIP ファイルとしてダウンロードされます。

- 特定のライセンス・アクティベーション・キーを削除するには、「**削除**」アイコン () をクリックします。
- ページの上部にある「**編集**」ボタンをクリックして、ライセンス警告期間を構成します。ライセンス警告期間は、XClarity Administrator が警告をトリガーしたてからライセンスの有効期限が切れるまでの日数です。

## ヘルプの入手

- ビジネス・パートナー経由でのご利用で問題が発生した場合は、トランザクションおよび有効化の確認のためにビジネス・パートナーにお問い合わせください。
- 電子有効化証明、許可コードまたはアクティベーション・キーを受信していない、または宛先が正しくないときは、それぞれの地域のいずれかの地域担当者にご連絡ください。
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (北アメリカ)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (アジア太平洋)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (欧州、中東、アジア)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (中南米)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (中国)
- 自身の有効化に関する情報が正しくない場合は、Lenovo サポート([SW\\_override@lenovo.com](mailto:SW_override@lenovo.com))宛てに以下の情報を含むメールでお知らせください。
  - オーダー番号
  - メール・アドレスを含む問い合わせ先情報。
  - ご使用の物理アドレス
  - 必要な変更
- ライセンスのダウンロードに関する問題やご質問は、Lenovo サポート ([-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com)) までお問い合わせください。

---

## Features on Demand Web ポータルを使用した全機能有効化ライセンスのインストール

XClarity Administrator がインターネットにアクセスできない場合は、XClarity Administrator へのネットワーク・アクセスがある別のシステムから [Features on Demand Web ポータル](#) を使用して、既存の認証コードのライセンスを引き換えおよび取得できます。その後で、XClarity Administrator Web インターフェースを使用して、引き換えたライセンスをインポートしてインストールできます。

## 手順

管理サーバーに Lenovo XClarity Pro ライセンスをインストールするには、以下の手順を実行します。

ステップ 1. 各管理対象デバイスの Lenovo XClarity Pro ライセンスを購入します。

有効にする機能と管理するデバイスの数に基づいて Lenovo XClarity Pro ライセンスを購入するには、Lenovo の担当者または認定ビジネス・パートナーにご連絡ください。ライセンスを購入すると、認証コードが [電子有効化証明メール](#) で送られます。認証コードは 22 文字

の英数字の文字列で、これをライセンスと引き換えてインストールする必要があります。  
このメールは受信しない場合で、ビジネス・パートナーからライセンスを購入された場合は、認証コードをビジネス・パートナーにご依頼ください。

[Features on Demand Web ポータル](#)で「**認証コードの取得**」をクリックして、認証コードを取得することもできます。

ステップ2. 認証コードを使用して、ライセンスのすべてまたは一部を引き換えます。ライセンスを引き換えると、ライセンス・アクティベーション・キー・ファイルが生成されます。

1. Web ブラウザーから [Features on Demand Web ポータル](#) を開き、ユーザー ID のメール・アドレスを使用してポータルにログインします。
2. 「**アクティベーション・キーの要求**」をクリックします。
3. 「**単一許可コードの入力**」を選択します。
4. 22 文字の認証コードを入力し、「**続行**」をクリックします。
5. 「**Lenovo お客様番号**」フィールドに Lenovo お客様番号を入力します。
6. 引き換えるライセンスの数を「**引き換え数量**」フィールドに入力し、「**続行**」をクリックします。

この認証コードで使用可能なすべてのライセンスを引き換えるには、「**使用可能なライセンス数**」フィールドと数を一致させます。

使用可能なライセンスの一部を引き換える場合は、同じ認証コードを使用して、別のライセンス・アクティベーション・キーで残りのライセンスを引き換えることができます。


**ヒント:** XClarity Administrator ごとに、最大 1,000 の管理対象デバイスがサポートされません。そのため、XClarity Administrator インスタンスにインストールする単一のライセンス・アクティベーション・キーのライセンス数が 1,000 を超えることはできません。

7. プロンプトに従って製品の詳細と連絡先情報を入力し、「**続行**」をクリックしてライセンス・アクティベーション・キーを生成します。
8. 必要に応じて、ライセンス・アクティベーション・キーを受け取る追加の受信者を指定します。
9. 「**送信**」をクリックして、ライセンス・アクティベーション・キーを送信します。

発注書に割り当てられたユーザーと追加の受信者がライセンス・アクティベーション・キーを含むメールを受け取ります。キーは、.KEY 形式のファイルです。

**注:** ライセンス・アクティベーション・キーは、[Features on Demand Web ポータル](#)で「**履歴の取得**」をクリックし、Lenovo お客様番号を使用してライセンス・アクティベーション・キーを検索して、キーのすべてまたは一部を (個別または一括で) ダウンロードすることもできます。その後で、「**メール**」をクリックしてキーをメールで送るか、「**ダウンロード**」をクリックしてキーをローカル・システムにダウンロードします。

ステップ3. ライセンスを XClarity Administrator にインポートしてインストールします。

1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**ライセンス**」をクリックして、「**ライセンス管理**」ページを表示します。
2. 「**インポートして適用**」アイコン () をクリックし、ライセンスをインストールします。
3. 「**参照**」をクリックして、インストールするライセンスのライセンス・アクティベーション・キー・ファイルを選択します。


**ヒント:** 複数のライセンス・アクティベーション・キーをインポートするには、.KEY ファイルを .ZIP ファイルに圧縮して、その ZIP ファイルを選択してインポートします。

4. 「**ライセンスに同意する**」をクリックし、ライセンスをインポートして適用します。


インストールが完了すると、ライセンス・アクティベーション・キーが、インストール済みのライセンス数やアクティベーション期間(開始日と有効期限)と一緒に表に表示されます。

## 終了後

「ライセンス」ページで、以下の操作を実行できます。

- 「**エクスポート**」アイコン()をクリックして、1つ以上の特定のライセンス・アクティベーション・キーをローカル・システムにダウンロードします。

注：複数のライセンス・アクティベーション・キーをエクスポートすると、ファイルは単一のZIPファイルとしてダウンロードされます。

- 特定のライセンス・アクティベーション・キーを削除するには、「**削除**」アイコン()をクリックします。
- ページの上部にある「**編集**」ボタンをクリックして、ライセンス警告期間を構成します。ライセンス警告期間は、XClarity Administrator が警告をトリガーしたてからライセンスの有効期限が切れるまでの日数です。

## ヘルプの入手

- ビジネス・パートナー経由でのご利用で問題が発生した場合は、トランザクションおよび有効化の確認のためにビジネス・パートナーにお問い合わせください。
- 電子有効化証明、許可コードまたはアクティベーション・キーを受信していない、または宛先が正しくないときは、それぞれの地域のいずれかの地域担当者にご連絡ください。
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (北アメリカ)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (アジア太平洋)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (欧州、中東、アジア)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (中南米)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (中国)
- 自身の有効化に関する情報が正しくない場合は、Lenovo サポート([SW\\_override@lenovo.com](mailto:SW_override@lenovo.com))宛てに以下の情報を含むメールでお知らせください。
  - オーダー番号
  - メール・アドレスを含む問い合わせ先情報。
  - ご使用の物理アドレス
  - 必要な変更
- ライセンスのダウンロードに関する問題やご質問は、Lenovo サポート([-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com))までお問い合わせください。

---

## 第 7 章 XClarity Administrator としての更新

Lenovo XClarity Administrator をコンテナとして実行する場合は、この更新手順を使用して最新のソフトウェアを新しいコンテナとしてインストールし、元のコンテナのボリュームを新しいコンテナにバインドします。

### 始める前に

XClarity Administrator v4.0 以降は、XClarity Administrator v3.0 以降のインスタンスからのみ更新できます。v3.0 より前のバージョンの XClarity Administrator を使用している場合は、v4.0 にアップグレードする前に v3.0 以降にアップグレードする必要があります。

Lenovo XClarity Orchestrator を使用して XClarity Administrator v4.0 以降のインスタンスを管理するには、XClarity Orchestrator v2.0 以降が必要です。XClarity Administrator を v4.0 以降に更新する場合は、XClarity Orchestrator は既に v2.0 以降がインストール済みである必要があります。

### このタスクについて

`docker-compose.yml` ファイルは、元のコンテナのインストール時に設定した以下の環境変数を使用します。これらの環境変数は、新しいコンテナによっても使用されます。

- **CONTAINER\_NAME**。各 XClarity Administrator インスタンスに Docker ボリュームを作成するために使用する固有のコンテナ名 (例: `CONTAINER_NAME=LXCA-203`)。

XClarity Administrator は、コンテナ名を使用してコンテナのボリュームを作成します。新しいコンテナに同じコンテナ名を使用すると、新しい XClarity Administrator インスタンスは同じボリュームを使用するため、元の XClarity Administrator インスタンス (コンテナ) と同じシステム・データや設定にアクセスできます。

コンテナ名を変更すると、そのコンテナに新しいボリュームが作成され、新しい XClarity Administrator インスタンスは元の XClarity Administrator インスタンス (コンテナ) と同じシステム・データや設定にはアクセスできなくなります。コンテナの名前や IP アドレスを変更する必要がある場合は、新しいコンテナをインストールする前に元の XClarity Administrator インスタンスのシステム・データと設定をバックアップし、そのバックアップを使用して新しいコンテナにシステム・データと設定を復元します。

- **ADDRESS**。コンテナの静的 IPv4/IPv6 アドレス (例: `ADDRESS=192.0.2.0`)。

デバイスの管理後に XClarity Administrator IP アドレスを変更すると、XClarity Administrator でデバイスがオフライン状態になります。IP アドレスを変更する前に、すべてのデバイスを管理対象から除外してください。

- **BACKUP\_MOUNT** と **FIRMWARE\_MOUNT**。(任意) XClarity Administrator のバックアップを保存するために使用するリモート共有やファームウェア更新のリモート・リポジトリとして使用するリモート共有のパス。このパスは、それぞれ `/mnt/backup_share` と `/mnt/fw_share` である必要があります。

注：XClarity Administrator は特権コンテナとして実行されません。

### 手順

XClarity Administrator コンテナを更新するには、以下の手順を実行します。

ステップ 1. XClarity Administrator コンテナ・イメージを [XClarity Administrator ダウンロード Web ページ](#) からクライアント・ワークステーションにダウンロードします。Web サイトにログオンし、付与されたアクセス・キーを使用してイメージをダウンロードします。

ステップ 2. 次のコマンドを実行して、XClarity Administrator コンテナ・イメージを Docker ホストにインポートします。

```
docker load -i lnvggy_sw_lxca_110-3.5.0_anyos_noarch
```

ステップ3. 元のコンテナで使用していたのと同じ `docker-compose.yml` を編集します。ファイルの先頭にある `image` プロパティを更新して、手順2の新しい Docker イメージをポイントします。イメージのタグは、`docker tag` コマンドを使用して変更できます。

IPv6 が有効な `yml` ファイルの例を次に示します。

```
version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

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

```
xcat:
  name: ${CONTAINER_NAME}-xcat

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

ステップ 4. 次のコマンドを実行して、元のコンテナをシャットダウンします。

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

ステップ 5. 次のコマンドを実行して、Docker に新しいイメージをデプロイします。<ENV\_FILENAME> は、環境変数ファイルの名前です。

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





---

## 第 8 章 XClarity Administrator のアンインストール

Lenovo XClarity Administrator 仮想アプライアンスまたはコンテナをアンインストールするには、以下の手順を実行します。

### 手順

XClarity Administrator 仮想アプライアンスをアンインストールするには、以下の手順を実行します。

ステップ 1. 現在 XClarity Administrator の管理対象になっているすべてのデバイスを管理対象から除外します (XClarity Administrator オンライン・ドキュメントの[シャージの管理](#)、[サーバーの管理](#)、[スイッチの管理](#)を参照)。

ステップ 2. オペレーティング・システムによっては、XClarity Administrator をアンインストールします。

- **Docker-compose** 次のコマンドを実行してコンテナを停止し、ネットワークおよびボリュームを削除します。  
`docker-compose down -v`
- **CentOS、Red Hat、Rocky、および Ubuntu**
  1. 仮想マシン・マネージャーを使用してホストに接続します。
  2. 仮想マシンを右クリックし、**シャットダウン** → **強制的にオフ** をクリックします。
  3. 仮想マシンをもう一度右クリックし、「**削除**」をクリックします。「**削除の確認**」ダイアログ・ボックスが表示されます。
  4. すべてのチェック・ボックスをオフにし、「**削除**」をクリックします。
- **ESXi**
  1. VMware vSphere Client を介してホストに接続します。
  2. 仮想マシンを右クリックし、「**電源**」 → 「**電源オフ**」 をクリックします。
  3. 仮想マシンをもう一度右クリックし、「**ディスクから削除**」 をクリックします。
- **Hyper-V**
  1. サーバー マネージャーのダッシュボードで、「**Hyper-V**」 をクリックします。
  2. サーバーを右クリックし、「**Hyper-V マネージャー**」 をクリックします。
  3. 仮想マシンを右クリックし、「**シャットダウン**」 をクリックします。
  4. 仮想マシンをもう一度右クリックし、「**削除**」 をクリックします。