Lenovo

Lenovo XClarity Orchestrator

計画およびインストール・ガイド

バージョン 2.1

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 Orchestrator 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 2 版 (2024 年 7月)

目次

変更の要約

Lenovo XClarity Orchestrator 管理ソフトウェアの以下のリリースでは、新しいソフトウェアの機能拡張および修正のサポートを提供しています。

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。

このバージョンでは、計画およびインストールに関して以下の機能拡張がサポートされています。以前のリリースの変更については、最新情報 XClarity Orchestrator オンライン・ドキュメント を参照してください。

機能	説明
計画およびインストール	XClarity Orchestrator では、最低 8 つの仮想プロセッサー・コアが必要です (サポートされるハードウェアおよびソフトウェアを参照).

第 1 章　XClarity Orchestrator の計画

ライセンス

Lenovo XClarity Orchestrator は、無料アプリケーションです。無料試用版ライセンスで最大 90 日間 XClarity Orchestrator を無料で使用できますが、無料試用期間の経過後、引き続き該当する XClarity Orchestrator 機能を使用し、XClarity Orchestrator サービスおよびサポートを取得するには、適切なライセンスを購入してインストールする必要があります。

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

- **XClarity Orchestrator**。Orchestrator およびベース管理機能サーバー、シャーシ、スイッチ、およびストレージ・デバイスおよび XClarity Orchestrator のサービスとサポートのための資格について確認します。Orchestrator 機能を使用するには、サーバー構成と OS デプロイメントをサポートしているすべてのデバイスに対して、XClarity Orchestrator でのライセンスが必要です。XClarity Orchestrator のサービスおよびサポートには、*すべての管理対象デバイス*にライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Orchestrator 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 Orchestrator のライセンスの数が必要な数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。必要な数のライセンスがインストールされる前に、ライセンスの猶予期間 (無料試用期間を含む) が終了した場合、すべての XClarity Orchestrator機能 (監視、基本管理、および分析を含む) は無効になります。ログインすると、追加のライセンスを適用できる「ライセンス情報」ページにリダイレクトされます。

  たとえば、追加の ThinkSystem サーバー 100 台とラック・スイッチ 20 個を管理を既存の XClarity Orchestrator で既存の XClarity Administrator インスタンスを使用して行う場合、ユーザー・インターフェースですべての機能が無効になるまでの 90 日間で、追加の XClarity Orchestrator 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。XClarity Orchestrator 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、XClarity Orchestrator でサービスおよびサポートを利用する場合は、これらが必要です。XClarity Orchestrator 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、機能が再び有効になります。

  重要：XClarity Orchestrator のベース・ライセンスは XClarity Pro および XClarity Orchestrator Analytics ライセンスの前提条件です。XClarity Pro または XClarity Orchestrator のライセンスの数が適合して*いる*が、アクティブなベース・ライセンスの数が適合して*いない*場合は、すべてのデバイスですべての XClarity Orchestrator 機能 (分析機能が無効を含む) が無効になります。

- **Lenovo XClarity Pro**。拡張管理機能 (サーバー構成および OS デプロイメント) を有効にします。拡張機能をサポートする管理対象デバイスごとに XClarity Orchestrator のライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Pro 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 Pro ライセンスの数が適合しない場合、適切なライセンスをインストールするための 90 日間の猶予期間があります。必要な数のライセンスがインストールされる前に猶予期間 (無料試用期間を含む) が終了した場合、サーバー構成および OS デプロイメントは*すべてのデバイス*で無効になります。

  XClarity Pro ライセンスのインストールについて詳しくは、ライセンスおよび 90 日間の無料トライアル XClarity Administrator オンライン・ドキュメントを参照してください。

- **XClarity Orchestrator 分析**。分析機能を有効にします。拡張機能をサポートする管理対象デバイスごとに XClarity Orchestrator のライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Orchestrator Analytics 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 Orchestrator Analytics ライセンスの数が必要な数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。必要な数のライセンスがインストールされる前に猶予期間 (無料試用期間を含む) が終了した場合、「**監視 ➡ 分析**」メニューがすべてのデバイスで無効になり、分析の表示、カスタム・アラート・ルールの作成、および*すべてのデバイス*への照会ができなくなります。

重要：XClarity Orchestrator Analytics ライセンスをインストールしたら、ユーザー・インターフェースを最新表示する必要があります。

注：期限が切れた (90 日の猶予期間を超えて有効期限を過ぎた) XClarity Orchestrator Analytics ライセンスをインストールして、ユーザー・インターフェースを最新表示すると、分析機能が無効になります。つまり、アクティブな試用期間または猶予期間が中断され、分析サービスが停止し、分析機能が淡色表示されます。(これには数分間かかる場合があります。)新しい有効なライセンスをインポートすることで、分析機能を再度有効にすることができます。

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*。

ライセンスが引き換えられると、アクティベーション期間が始まります。

ライセンス・*アクティベーション・キー*を使用してライセンスをインストールします。ライセンスを引き換えた後、使用可能なライセンスのすべてまたはサブセットのアクティベーション・キーを作成し、アクティベーション・キーをダウンロードして XClarity Orchestrator にインストールすることができます。

XClarity Orchestrator 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。

ライセンスが既にインストールされている場合、XClarity Orchestrator 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*。

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 Orchestrator 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。

XClarity Orchestrator をアップグレードする場合、またはアクティベーション・キーの復元を必要とするエラー状態が発生した場合は、Features on Demand Web ポータル からエクスポートされたキーを使用するか、すべてのアクティベーション・キー (顧客 ID ごとに) をダウンロードし、そのアクティベーション・キーを (個々のアクティベーション・キーとして、またはキー ZIP ファイルとしてまとめて) XClarity Orchestrator にインポートします。

ライセンス購入について詳しくは、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。

サポートされるハードウェアおよびソフトウェア

ご使用の環境が、Lenovo XClarity Orchestrator のハードウェア要件とソフトウェア要件を満たしていることを確認します。

ホスト・システム

XClarity Orchestrator は、ホスト・システム上の仮想アプライアンス内で実行されます。

ハイパーバイザー要件

XClarity Orchestrator のインストールでは、以下のハイパーバイザーがサポートされています。

- 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 2022
- VMware ESXi 7.0
- VMware ESXi 6.7、U1、U2 および U3
- VMware ESXi 6.5、U1 および U2

Hyper-V の場合、仮想アプライアンスは仮想ディスク・イメージ (VHD) です。VMware ESXi の場合、仮想アプライアンスは OVF テンプレートです。

ハードウェア要件

仮想アプライアンスで以下の*最小要件*が満たされている必要があります。ご使用環境の規模およびプロビジョニング機能の使用 (オペレーティング・システムのデプロイメント、ファームウェア更新、サーバーの構成など) 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。

- 8 仮想プロセッサー・コア
- 16 GB のメモリー
- 2 つの接続されたディスクにまたがる 551 GB ストレージ。
  - 仮想アプライアンス用に最小 251 GB (ディスク 0)
  - 更新リポジトリー用100 GB (ディスク 1)
  - OS イメージ・リポジトリー用200 GB (ディスク 2)

重要：更新リポジトリーと OS イメージ・リポジトリーに使用されているディスクのサイズを増減することはできません。

ソフトウェア要件

以下のソフトウェアが XClarity Orchestrator で必要になります。

- **認証サーバー。**XClarity Orchestrator はデフォルトで内部のライトウェイト・ディレクトリー・アクセス・プロトコル (LDAP) サーバーを使用して認証します。外部認証サーバーを使用する場合、以下の LDAP サーバーがサポートされています。
  - Windows Server 2008 以降で実行する Microsoft Active Directory
- **NTP サーバー。**リソース・マネージャーおよび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 Orchestrator 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)。XClarity Orchestrator をインストールするローカル・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、そのローカル・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

XClarity Orchestrator は、最大 10,000 のデバイス総数をまとめて管理できるリソース・マネージャーを無制限数サポートできます。

XClarity Orchestrator は以下のリソース・マネージャーをサポートしています。

- **Lenovo XClarity Management Hub 2.0**XClarity Orchestrator は、XClarity Management Hub 2.0 によって管理されているデバイスを管理および監視します。各 XClarity Management Hub 2.0 インスタンスは、最大 5,000 のデバイスを管理できます。

  重要：高度な機能 (構成パターンを使用したオペレーティング・システムのデプロイメントやサーバー構成など) は、この管理ハブではサポートされません

  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 Management Hub 2.0 サーバーで確認できます。

  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。

- **Lenovo XClarity Management Hub**XClarity Orchestrator は、XClarity Management Hub によって管理されているデバイスを管理、監視、およびプロビジョニングします。各 XClarity Management Hub インスタンスは、最大 10,000 の ThinkEdge クライアント・デバイスを管理できます。

サポートされる ThinkEdge クライアント・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 Management Hub サーバーで確認できます。

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。

- **Lenovo XClarity Administrator** v2.6 以降 XClarity Orchestrator は、XClarity Administrator によって管理されている物理デバイスを管理、監視、およびプロビジョニングします。各 XClarity Administrator インスタンスは、最大 1,000 のデバイス (サーバー、シャーシ、スイッチ、およびストレージ) を管理できます。

  XClarity Orchestrator は、特に明記されている場合を除き、XClarity Administrator および XClarity Management Hub でサポートされるすべてのデバイスをサポートします。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、次の Lenovo XClarity サポート Web ページで確認できます。
  - ThinkAgile、ThinkEdge、ThinkSystem、System x、 Converged HX、および NeXtScale サーバー
  - シャーシの Flex System および ThinkSystem デバイス
  - ThinkServer サーバー
  - スイッチ
  - ストレージ・デバイス

  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。

  注：OS デプロイメント機能を使用するには、XClarity Administrator v4.0 以降が必要です。
- **Schneider Electric EcoStruxure IT Expert**XClarity Orchestrator は、EcoStruxure IT エキスパート によって管理されるインフラストラクチャー・リソース (PDU や UPS など) を管理および監視します。
- **VMware vRealize オペレーション・マネージャー**XClarity Orchestrator は、仮想ワークロード・メトリックを vRealize Operations Manager から監視します。

  注：vRealize Operations Manager は、XClarity Orchestrator でデバイスを管理しないため、リソース・マネージャーのリストには含まれません。

Web ブラウザー

XClarity Orchestrator 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 80.0 以降
- Firefox ESR 68.6.0 以降
- Microsoft Edge 40.0 以降
- Safari 13.0.4 以降 (macOS 10.13 以降で実行されている場合)

サードパーティー・ソフトウェア

XClarity Orchestrator は、以下のソフトウェアと統合されています。

- Splunk v7.0.3 以降 (Splunk 用の XClarity Orchestrator アプリのユーザーズ・ガイドを参照)

ファイアウォールおよびプロキシー・サーバー

コール・ホームおよび保証状況を含む、一部のサービスおよびサポート機能では、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 Orchestrator およびリソース・マネージャ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。Lenovo XClarity Orchestrator およびリソース・マネージャーがインターネットに直接アクセスできない場合は、それらがプロキシ・サーバーを使用するように構成します。

ファイアウォール

必要に応じて、XClarity Orchestrator および該当するリソース・マネージャー (Lenovo XClarity Management Hub 2.0、Lenovo XClarity Management Hub、および Lenovo XClarity Administrator) 用にファイアウォール

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。各 DNS は、動的 IP アドレスを持つ地理的に分散したシステムを表します。

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。

DNS 名	ポート	プロトコル
更新のダウンロード (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)、リポジトリー・パック)		
download.lenovo.com	443	https
support.lenovo.com	443 および 80	https および http
Lenovo サポート (コール・ホーム) へのサービス・データの送信 – XClarity Orchestrator のみ		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 以降) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 以前)	443	https
Lenovo への定期的なデータの送信 – XClarity Orchestrator のみ		
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 以降) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 以前)	443	https
保証情報の取得		
supportapi.lenovo.com	443	https および http

プロキシー・サーバー

XClarity Orchestrator またはリソース・マネージャーがインターネットに直接アクセスできない場合は、それらが 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 (ネットワークの構成 XClarity Orchestrator オンライン・ドキュメントを参照)。

- 必ず、プロキシー・サーバーが基本認証を使用するようにセットアップされている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ー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ー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。

注意：XClarity Management Hub は、インターネットに直接アクセスできる必要があります。HTTP プロキシー・サーバーは、現在のところサポートされていません。

利用可能なポート

Lenovo XClarity Orchestrator およびリソース・マネージャーでは、通信を容易にするために、特定のポートが開いている必要があります。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、一部の機能が正しく動作しないことがあります。

XClarity Orchestrator、Lenovo XClarity Management Hub 2.0、Lenovo XClarity Management Hub、および Lenovo 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 Orchestrator

XClarity Orchestrator 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。XClarity Orchestrator とすべての管理対象リソー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リソースにアクセスするには、必要なポートが開いていることを確認します。

注：XClarity Orchestrator 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。

サービス	アウトバウンド (外部システムで開いたポート)	インバウンド (XClarity Orchestrator アプライアンスで開いたポート)
XClarity Orchestrator アプライアンス	• DNS – ポート **53** の TCP/UDP	• HTTPS – ポート **443** の TCP
外部認証サーバー	• LDAP – ポート **389**[1] の TCP	適用外
イベント転送サービス	• メール・サーバー (SMTP) – ポート **25**[1] の UDP • REST Web サービス (HTTP) – ポート **80**[1] の UPD • Splunk – ポート **8088**[11]、**8089**[1] の UDP • Syslog – ポート **514**[1] の UDP	適用外
Lenovo サービス (コール・ホームを含む)	• HTTPS (コール・ホーム) – ポート **443** の TCP	適用外

1. デフォルトのポートです。このポートは、XClarity Orchestratorユーザー・インターフェースから構成できます。

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 では、通信を容易にするために、特定のポートが開いている必要があります。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、一部の管理ハブ機能が正しく動作しないことがあります。

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管理ハブからこれらのデバイスを管理するには、管理ハブと各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。

サービスまたはコンポーネント	アウトバウンド (外部システムで開いたポート)	インバウンド (ターゲット・デバイスで開いたポート)
XClarity Management Hub 2.0	• DNS - ポート **53** の UDP • NTP - ポート **123** の UDP • HTTPS - ポート **443** の TCP • SSDP - ポート **1900** の UDP • DHCP - ポート **67** の UDP	• HTTPS - ポート **443** の TCP • SSDP - ポート **32768** ～ **65535** の UDP
ThinkSystem および ThinkAgile サーバー	• HTTPS – ポート **443** の TCP • SSDP 検出 – ポート **1900** の UDP	• HTTPS – ポート **443** の TCP

XClarity Management Hub

XClarity Management Hub 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。

サービスまたはコンポーネント	アウトバウンド (外部システムで開いたポート)	インバウンド (XClarity Management Hub アプライアンスで開いたポート)
XClarity Management Hub アプライアンス[1]	• DNS – ポート 53[2] の TCP/UDP	• HTTPS – ポート 443 の TCP • MQTT – ポート 8883 の TCP
ThinkEdge クライアント・デバイス[3]	適用外	• MQTT – ポート 8883 の TCP

1. XClarity Management Hub を使用して XClarity Orchestrator を介してデバイスを管理する場合、通信を容易にするために特定のポートを開く必要があります。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 XClarity Orchestrator 機能が正しく動作しないことがあります。
2. XClarity Management Hub はオプションで、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。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。
3. 管理可能な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 Management Hub からこれらのデバイスを管理するには、XClarity Management Hub と Edge デバイス間の通信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

Lenovo XClarity Administrator を使用して Lenovo XClarity Orchestrator を介してデバイスを管理する場合、通信を容易にするために特定のポートを開く必要があります。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 XClarity Orchestrator 機能が正しく動作しないことがあります。

XClarity Administrator 用に開く必要があるポートについては、利用可能なポート XClarity Administrator オンライン・ドキュメント を参照してください。

ネットワークに関する考慮事項

XClarity Orchestrator は、管理およびデータ通信に単一のサブネット (eth0) を使用します。ネットワークを構成する前に、以下の考慮事項を確認してください。

- ネットワーク・インターフェースは検出と管理に使用されます。ネットワーク・インターフェースは、管理するすべてのデバイスと通信できる必要があります。
- 収集されたサービス・データを Lenovo サポートに手動で送信したり、自動問題通知 (コール・ホーム) を使用する場合は、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。
- リソース・マネージャーの接続後に XClarity Orchestrator 仮想アプライアンスの IP アドレスを変更すると、XClarity Orchestrator とマネージャーとの通信が失われ、マネージャーはオフラインと表示されます。XClarity Orchestrator の電源がオンになり稼働した後に仮想アプライアンスの IP アドレスを変更する必要がある場合は、IP アドレスを変更する前に、すべてのリソース・マネージャーが切断 (削除) されていることを確認してください。
- 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 を使用する場合は、DHCP アドレスを MAC アドレスに基づくものにしたり、リースの有効期限が切れないように DHCP を設定するなど、IP アドレスの変更を最小限にします。IP アドレスが変更された場合は、管理対象デバイスを切断 (削除) してから、再度接続する必要があります。
- 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。

セキュリティーに関する考慮事項

Lenovo XClarity Orchestrator とすべての管理対象リソースのセキュリティー計画に役立つ以下の考慮事項を確認してください。

セキュアな環境に関する考慮事項

環境のセキュリティー要件を評価し、すべてのセキュリティー・リスクを理解して、それらのリスクを最小限に抑えることが重要です。Lenovo XClarity Orchestrator には、環境の保護に役立つ機能がいくつか含まれています。環境のセキュリティー計画の実施に役立つ情報を以下に示します。

重要：ご使用の環境のセキュリティー機能、構成手順、および適切な制御の評価、選択、実装は、お客様の責任で行っていただきます。ここで説明するセキュリティー機能を実装しても、環境が完全に保護されるわけではありません。

環境のセキュリティー要件を評価する際、以下の情報を考慮してください。

- 環境の物理的セキュリティーは重要です。システム管理ハードウェアが置かれている部屋およびラックの利用を制限してください。
- ウィルスや無許可アクセスなどの既知および新しいセキュリティー脅威からネットワーク・ハードウェアおよびデータを保護するために、ソフトウェア・ベースのファイアウォールを使用してください。
- ネットワーク・スイッチとパススルー・モジュールのデフォルトのセキュリティー設定は変更しないでください。これらのコンポーネントの工場出荷時のデフォルト設定により、非セキュア・プロトコルが使用不可になり、署名付きファームウェア更新の要件が有効になります。
- 少なくとも、重要なファームウェア更新が必ずインストールされるようにしてください。変更を行った後は必ず構成をバックアップしてください。
- DNS サーバーのセキュリティー関連の更新がすべて速やかにインストールされ、最新状態に維持されるようにしてください。
- ユーザーに、非トラステッド証明書を受け入れないように指示してください。詳しくは、セキュリティー証明書の使用 XClarity Orchestrator オンライン・ドキュメント を参照してください。
- 実施可能であれば、システム管理ハードウェアを別のサブネット内に配置してください。一般的に、スーパーバイザーのみがシステム管理ハードウェアにアクセスできるようにして、基本ユーザーにはアクセスを許可しないでください。
- パスワードを選択する際、簡単に推測できる語句 (たとえば、「password」または貴社名) は使用しないでください。パスワードを安全な場所で保管し、パスワードへのアクセスが制限されるようにしてください。貴社のパスワード・ポリシーを実装してください。

  重要：すべてのユーザーにストロング・パスワード規則の順守を要求する必要があります。
- サーバー上のデータおよびセットアップ・プログラムにアクセスできるユーザーを制御する方法として、ユーザーのパワーオン・パスワードを設定してください。始動パスワードについての詳細は、ハードウェアに付属の資料を参照してください。

暗号化に関する考慮事項

Lenovo XClarity Orchestrator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。

セキュリティーを強化するため、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。

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

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

セキュリティー証明書に関する考慮事項

Lenovo XClarity Orchestrator は SSL 証明書を使用して、XClarity Orchestrator と管理対象リソース・マネージャー (Lenovo XClarity Administrator または Schneider Electric EcoStruxure IT Expertなど) との間で信頼できるセキュアな通信を確立するだけでなく、XClarity Orchestrator ユーザーまたはさまざまなサービスとの通信も確立します。デフォルトでは、XClarity Orchestrator および Lenovo XClarity Administrator は、で発行された自己署名 XClarity Orchestrator 生成証明書を使用します。

XClarity Orchestrator の各インスタンス固有で生成されるデフォルトの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 Orchestrator 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 Orchestrator 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 Orchestrator 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、 を参照してください。

認証サーバーに関する考慮事項

認証サーバーとして、ローカル Lightweight Directory Access Protocol (LDAP) サーバーや別の外部 LDAP サーバーを使用できます。

*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 Orchestrator は 2 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 Orchestrator は、Orchestrator サーバーにあるローカル (組み込み) の LDAP 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**。サポートされている外部 LDAP サーバーは Microsoft Active Directory です。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 サーバーのセットアップについて詳しくは、 を参照してください。

アクセス制御に関する考慮事項

Lenovo XClarity Orchestrator は、*アクセス制御リスト* (ACL) を使用して、ユーザーがアクセスできるリソース (デバイス、リソース・マネージャー、および XClarity Orchestrator) を決定します。ユーザーが特定のリソース・セットにアクセスした場合、それらのリソースにのみ関連するデータ (インベントリー、イベント、アラート、分析など) を表示できます

このタスクについて

ACL は、ユーザー・グループとリソース・グループの組み合わせです。

- *ユーザー・グループ*は、この ACL によって影響を受けるユーザーを識別します。ACL には、1 つのユーザー・グループを含める必要があります。事前定義された**スーパーバイザー**役割が割り当てられているグループのメンバーであるユーザーは、常にすべてのリソースにアクセスできます。スーパーバイザー・ユーザーのリソース・アクセスを制限することはできません。

  リソース・ベース・アクセスが有効になっている場合、事前定義済みの*スーパーバイザー*役割が割り当てられているグループのメンバー**ではない**ユーザーは、デフォルトではどのリソース (デバイスおよびリソース・マネージャー) にもアクセスできません。これらのユーザーが特定のリソース・セットにアクセスできるようにするには、アクセス制御リストの一部であるユーザー・グループに、スーパーバイザー以外のユーザーを追加する必要があります。

  リソース・ベース・アクセスが無効になっている場合、すべてのユーザーがデフォルトですべてのリソース (デバイスおよびリソース・マネージャー) にアクセスできます。

- *リソース・グループ*は、アクセスできるリソース (デバイス、リソース・マネージャー、および XClarity Orchestrator) を識別します。ACL には少なくとも 1 つのリソース・グループを含める必要があります。

  注：管理グループにアクセスできるユーザーが、そのリソース・マネージャーによって管理されているすべてのデバイスに自動的にアクセスすることはありません。デバイス・グループを使用して明示的にデバイスにアクセスできるようにする必要があります。

アクセス制御リストについて詳しくは、リソースへのアクセス制御 XClarity Orchestrator オンライン・ドキュメント を参照してください。

高可用性に関する考慮事項

Lenovo XClarity Orchestrator の高可用性を実装するには、ホスト・オペレーティング・システムの高可用性機能を使用します。

Microsoft Hyper-V

Hyper-V 環境用に提供されている高可用性機能を使用します。

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す。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)。

第 2 章　XClarity Orchestrator のインストール

ローカル環境内のシステムに Lenovo XClarity Orchestrator 仮想アプライアンスをインストールして構成します。

始める前に

ハードウェアの要件および推奨を含めて、XClarity Orchestrator の前提条件を把握していることを確認します (サポートされるハードウェアおよびソフトウェアを参照)。

XClarity Orchestrator 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)。

管理する予定のリソース・マネージャーがサポートされていて、必要なバージョン・レベルになっていることを確認します (サポートされるハードウェアおよびソフトウェアを参照)。

インストール済みの XClarity Orchestrator 仮想アプライアンスの更新について詳しくは、XClarity Orchestrator の更新を参照してください。

高可用性環境のセットアップについては、高可用性の実装を参照してください。

Lenovo XClarity Orchestrator は、無料アプリケーションです。無料試用版ライセンスで最大 90 日間 XClarity Orchestrator を無料で使用できますが、無料試用期間の経過後、引き続き該当する XClarity Orchestrator 機能を使用し、XClarity Orchestrator サービスおよびサポートを取得するには、適切なライセンスを購入してインストールする必要があります。ライセンス購入について詳しくは、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詳しくは、XClarity Orchestrator ライセンスの適用を参照してください。

このタスクについて

構成中に eth0 ポートの静的 IP アドレスを使用して、仮想アプライアンスの IP アドレスを割り当てることができます。

構成中に IP アドレスを割り当てていない場合、IP 設定は、仮想アプライアンスを最初に起動したときにデフォルトで動的ホスト構成プロトコル (DHCP) を使用して割り当てられます。仮想アプライアンスを初めて起動するときに、XClarity Orchestrator の IP 設定を構成できます。起動する前に、必要な IP 情報がお手元にあることを確認してください。各プロンプトでは、60 秒以内に設定を入力する必要があります。

- 静的 IPv4 設定では、IP アドレス、サブネット・マスク、ゲートウェイの IP アドレス、および DNS 1 IP アドレス (オプション) と DNS 2 IP アドレス (オプション) を変更できます。
- 静的 IPv6 設定では、IP アドレス、プレフィックスの長さ、および DNS 1 IP アドレス (オプション) と DNS 2 IP アドレス (オプション) を変更できます。
- DHCP 設定では、プライマリーおよびループバック・インターフェースの設定 (自動 lo、iface lo inet loopback、自動 eth0、および iface eth0 inet DHCP) を変更できます。

注意：リソース・マネージャーの接続後に XClarity Orchestrator 仮想アプライアンスの IP アドレスを変更すると、XClarity Orchestrator とマネージャーとの通信が失われ、マネージャーはオフラインと表示されます。XClarity Orchestrator の電源がオンになり稼働した後に仮想アプライアンスの IP アドレスを変更する必要がある場合は、IP アドレスを変更する前に、すべてのリソース・マネージャーが切断 (削除) されていることを確認してください。IP アドレスの設定について詳しくは、ネットワークの構成を参照してください。

手順

XClarity Orchestrator 仮想アプライア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. XClarity Orchestrator ダウンロード Web ページ から XClarity Orchestrator イメージをローカル・システムにダウンロードします。Web サイトにログインし、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。

Hyper-V の場合、仮想アプライアンスは仮想ディスク・イメージ (VHD) です。VMware ESXi の場合、仮想アプライアンスは OVF テンプレートです。

ステップ 2. ローカル・システムで仮想アプライアンスをインストール、構成します。

- **VMware vSphere を使用した ESXi の場合**
  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て、**仮想マシン** ➡ 「**VM の作成/登録**」 ➡ 「**OVF または OVA ファイルから仮想マシンをデプロイ**」の順に選択します。
  3. 仮想アプライアンスのデプロイメント・ウィザードで各手順を完了します。ウィザードの手順を進める際には以下の点に留意してください。
     - **アプライアンス名**。このホストに一意の名前を選択します。
     - **Storage**。551 GB 以上の空き容量のあるデータストアを選択します。
     - **ディスク・フォーマット**。組織の要件を満たしているディスク・フォーマットを選択します。選択するフォーマットがわからない場合は、「**シン・プロビジョニング**」を選択します。
     - **追加設定**。オプションで、仮想アプライアンスのネットワーク構成を更新して、eth0 インターフェースの静的 IP アドレスを設定します。
- **VMware vCenter を使用した ESXi の場合**
  1. VMware vCenter を介してホストに接続します。
  2. 「ホストおよびクラスター」または「VM とテンプレート」でホストを右クリックし、「**ファイル**」 ➡ 「**OVF テンプレートのデプロイ**」をクリックします。
  3. 仮想アプライアンスのデプロイメント・ウィザードで各手順を完了します。ウィザードの手順を進める際には以下の点に留意してください。
     - **アプライアンス名**。このホストに一意の名前を選択します。
     - **ストレージ**。551 GB 以上の空き容量のあるデータストアを選択します。
     - **ディスク・フォーマット**。組織の要件を満たしているディスク・フォーマットを選択します。選択するフォーマットがわからない場合は、「**シン・プロビジョニング**」を選択します。
     - **テンプレートのカスタマイズ**。オプションで、仮想アプライアンスのネットワーク構成を更新して、eth0 インターフェースの静的 IP アドレスを設定します。
  4. 仮想アプライアンスの静的 IP アドレスを設定する場合は、以下のステップを実行します。
     a. インベントリーで VM を選択します。
     b. 「**構成**」 ➡ 「**vApp**」とクリックして、「**vApp オプションの有効化**」を選択します。
     c. 有効にした後、IP 割り当てスキームの「**OVF 環境**」を選択します。
     d. 「**OVF の詳細**」タブで、「**OVF 環境トランスポート**」の「VMware ツール」を選択します。
- **Microsoft Hyper-V の場合**
  1. 「Server Manager 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. 「**操作**」で、「**新規**」 ➡ 「**仮想マシン**」をクリックし、仮想マシンの新規作成ウィザードを開始して、「**次へ**」をクリックします。
4. 「名前およびロケーションの指定」ページで、新しい仮想マシンの名前 (LXCO-*{version}* など) を入力します。
5. 「世代を指定」ページで、「**世代 1**」を選択します。
6. 「メモリーの割り当て」ページで、この仮想マシンに使用する 16 GB 以上のメモリーを選択します (サポートされるハードウェアおよびソフトウェア を参照)。
7. 「ネットワークの構成」ページで、ホストをインストールして構成したときに作成した仮想スイッチを選択します。
8. 「仮想ハードディスクの接続」ページで、「**既存の仮想ハードディスクを使用する**」をクリックし、XClarity Orchestrator VHD イメージをコピーした場所を参照して、***disk001*.vhd** イメージを選択します。
9. 「**完了**」をクリックします。
10. 先ほど作成した仮想マシンを右クリックし、「**設定**」をクリックします。
11. 仮想マシンに割り当てるプロセッサー数を構成します。
    a. 「**プロセッサー**」を選択し、この仮想マシンに使用する 8 個以上の仮想プロセッサーを指定します (サポートされるハードウェアおよびソフトウェア を参照)。
    b. 「**適用**」をクリックし、「OK」をクリックします。
12. 仮想アプライアンスに 2 つ目のハードディスク・ドライブを追加します。
    a. 「IDE Controller 0」を展開し、「**ハードディスク・ドライブ**」を選択します。
    b. 「**仮想ハードディスク**」フィールドで、XClarity Orchestrator VHD イメージをコピーした場所を参照し、***disk002*.vhd** イメージを選択します。
    c. 「**適用**」をクリックし、「OK」をクリックします。
13. 仮想アプライアンスに 3 つ目のハードディスク・ドライブを追加します。
    a. 「IDE Controller 1」を展開し、「**ハードディスク・ドライブ**」を選択します。
    b. 「**仮想ハードディスク**」フィールドで、XClarity Orchestrator VHD イメージをコピーした場所を参照し、***disk003*.vhd** イメージを選択します。
    c. 「**適用**」をクリックし、「OK」をクリックします。
14. (オプション) オプションで、各ネットワーク・アダプターの静的 MAC アドレスを設定できます。これを行うには、仮想スイッチの「**ネットワーク・アダプター**」を展開して、「**高度な機能**」をクリックし、「**MAC アドレス**」の下の「**静的**」をクリックしてから MAC アドレスを指定します。

ステップ 3. 仮想アプライアンスの電源を入れます。

仮想アプライアンスが起動すると、次の例に示すように、DHCP によって割り当てられた IPv4 アドレスおよび IPv6 アドレスが、インターフェースごとにリスト表示されます。

```
Lenovo XClarity Orchestrator  Version x.x.x
---------------

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

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

You have 118 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
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 x. To continue without changing IP settings
```

... ...

ステップ 4. オプションで、コンソールから仮想アプライアンス IP 設定を構成できます。指定された時間内に選択を行わない場合、または x を入力した場合は、デフォルトで割り当てられた IP 設定を使用して、最初の起動が続行されます。

- **eth0 ポートの静的 IP アドレスを割り当てる。**1 を入力し、指示に従って設定を変更します。
- **DHCP を使用して eth0 ポートに新しい IP アドレスを割り当てる。**2 を入力し、指示に従って設定を変更します。
- **仮想アプライアンスの内部ネットワークのサブネットを選択します。**3 を入力し、指示に従って設定を変更します。デフォルトでは、XClarity Orchestrator は、内部ネットワーク用にサブネット 192.168.252.0/24 を使用します。このサブネットがホスト・ネットワークと重複する場合は、ネットワークの問題を回避するために、サブネットを他の使用可能な選択肢の 1 つに変更します。
  - 192.168.252.0/24
  - 172.31.252.0/24
  - 10.255.252.0/24

重要：無効な値を指定した場合は、エラーが返されます。最大 4 回まで、有効な値の入力を試行できます。

終了後

ログインして XClarity Orchestrator を構成します。

第 3 章　高可用性の実装

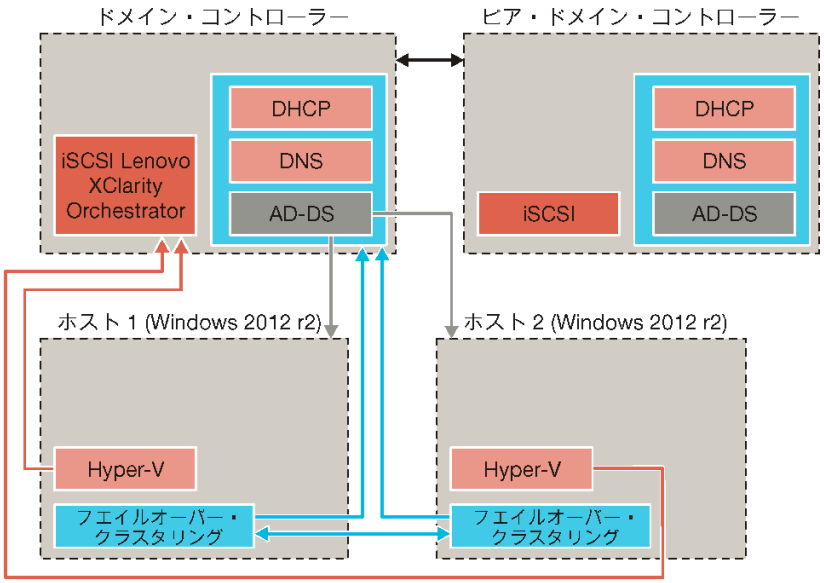
Lenovo XClarity Orchestrator の高可用性を実装するには、ホスト環境で用意されている高可用性機能を使用します。

高可用性の実装 (Hyper-V)

Microsoft Hyper-V 環境で Lenovo XClarity Orchestrator の高可用性を実装するには、Microsoft Hyper-V に用意されている高可用性機能を使用します。

このタスクについて

次の図では、Hyper-V 環境で XClarity Orchestrator の高可用性を実装する 1 つの方法の概要を示します。この例では、XClarity Orchestrator イメージが共有ストレージにインストールされており、クラスターによってアクセスされます。



手順

高可用性環境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. ドメイン・コントローラーをセットアップします。

a. 初期 DHCP セットアップを実行します。

b. DNS をセットアップします。

c. Active Directory ドメイン サービス (AD-DS) をセットアップします。

d. DHCP セットアップを完了します。

ステップ 2. 最初のホストをセットアップします。

a. Microsoft Windows 2012 R2 をインストールします。

b. AD-DS ドメインに参加します。

c. 以下の機能を追加します。
- Hyper-V
- フェイルオーバー・クラスタリング

ステップ 3. 2 番目のホストをセットアップします。

a. Microsoft Windows 2012 R2 をインストールします。
b. AD-DS ドメインに参加します。
c. 以下の機能を追加します。
   - Hyper-V
   - フェイルオーバー・クラスタリング

ステップ 4. ドメイン・コントローラーと両方のホストで共有ストレージ (iSCSI など) を構成します。

ステップ 5. フェイルオーバー・クラスタリングを構成します。

ステップ 6. XClarity Orchestrator イメージを追加します。

高可用性の実装 (ESXi)

VMware ESXi 環境で Lenovo XClarity Orchestrator の高可用性を実装するには、ESXi に用意されている高可用性機能を使用します。

このタスクについて

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す。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。

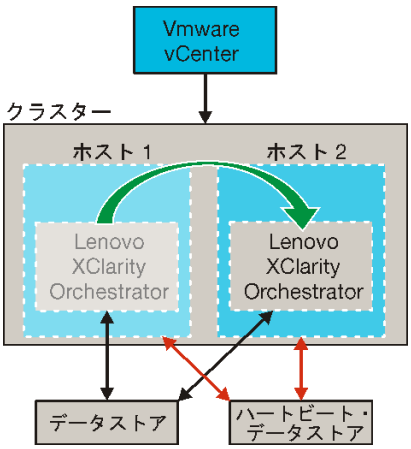
VMware High Availability には以下のコンポーネントが必要です。

- 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)。

次の図は、ESXi 環境で XClarity Orchestrator の高可用性を実装する 1 つの方法を示しています。このシナリオでは、XClarity Orchestrator 仮想アプライアンスが共有ストレージにインストールされており、クラスターによってアクセスされます。



VMware High Availability クラスター (VMware 5.0) のセットアップについて詳しくは、VMware に対する HA の設定に関する Web ページを参照してください。

手順

高可用性環境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. クラスター内のすべてのホストからアクセス可能になる共有ストレージをセットアップします。

ステップ 2. 2 台のサーバーに ESXi をインストールし、それぞれに静的 IP アドレスを割り当てます。VMware vCenter が別のサーバーで構成されていることを確認します。

ステップ 3. VMware vCenter を起動します。

ステップ 4. VMware vCenter と連携するように他の 2 台のホストを構成します。

a. クラスターを作成します。

b. クラスターにホストを追加します。

c. クラスター内のホストに両方のデータストアを追加します。

注：2 番目のデータストアはハートビート用に必要です。

ステップ 5. クラスターに XClarity Orchestrator をデプロイします。

第 4 章　初めての XClarity Orchestrator の構成

Lenovo XClarity Orchestrator に初めてアクセスするときには、いくつかの手順を実行して初期セットアップを完了する必要があります。

手順

XClarity Orchestrator を最初に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. XClarity Orchestrator Web インターフェースにアクセスします。

ステップ 2. 初期パスワードを変更します。

ステップ 3. 使用許諾契約書を読み、同意します。

ステップ 4. 追加ユーザー・アカウントの作成。

ステップ 5. 日付と時刻を構成します。

ステップ 6. 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 7. デフォルトの認証サーバーを使用するか、外部 LDAP クライアントを構成するか選択します。

ステップ 8. 追加のセキュリティー設定を構成します (内外のサービスのトラステッド証明書のインポートを含みます)。

ステップ 9. 可能であれば、自動問題通知の構成と有効化を行います。

ステップ 10. 特定のサービスおよびアプリケーションにイベントを転送するように XClarity Orchestrator を構成します (該当する場合)。

ステップ 11. リソース・マネージャーを接続します。

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

Lenovo XClarity Orchestrator Web インターフェースは、XClarity Orchestrator 仮想マシンへのネットワーク接続が可能な任意のシステムから起動できます。

始める前に

サポートされる以下の 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。詳しくは、サポートされるハードウェアおよびソフトウェアを参照してください。

- Chrome 80.0 以降
- Firefox ESR 68.6.0 以降
- Microsoft Edge 40.0 以降
- Safari 13.0.4 以降 (macOS 10.13 以降で実行されている場合)

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。

XClarity Orchestrator は単一のサブネット (通常は eth0) を使用します。

XClarity Orchestrator 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 Orchestrator に接続できる別の VM から XClarity Orchestrator にアクセスすることを検討してください。たとえば、XClarity Orchestrator がインストールされているホストの別の VM から XClarity Orchestrator にアクセスできます。

手順

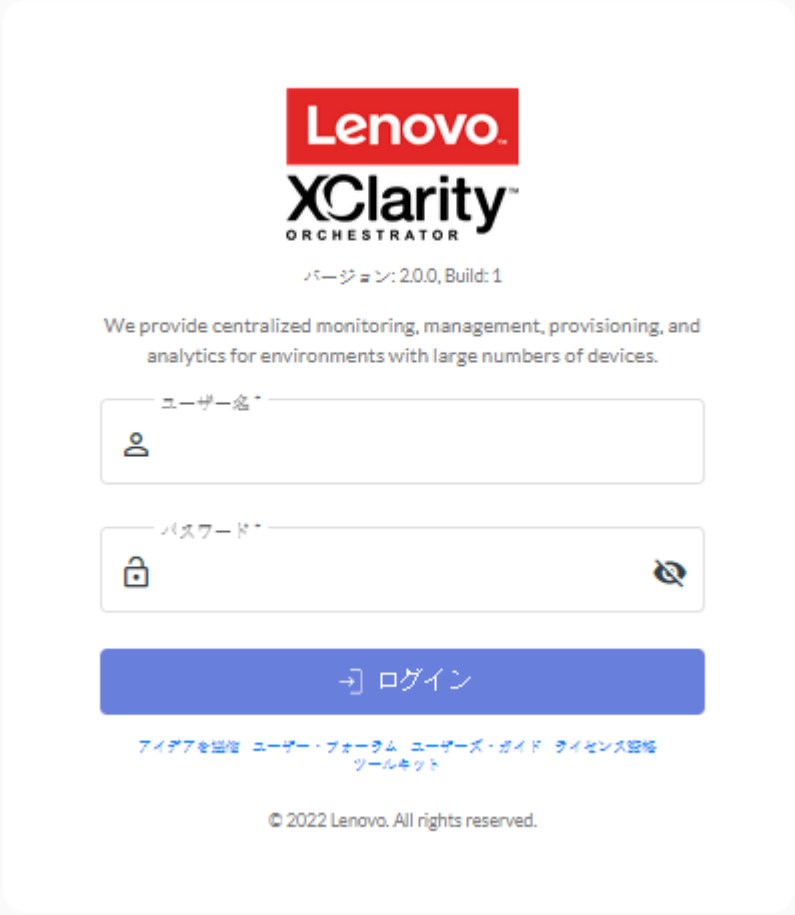
初めて XClarity Orchestrator Web インターフェースにアクセスするには、以下の手順を実行します。

1. ブラウザーで XClarity Orchestrator 仮想アプライアンスの IP アドレスを指定します。
   - **静的な IPv4 アドレスの使用**インストール時に IPv4 アドレスを指定した場合は、その IPv4 アドレスで Web インターフェースにアクセスします。URL は次のとおりです。
     `https://{IPv4_address}/#/login.html`

     例:
     `https://192.0.2.10/#/login.html`
   - **XClarity Orchestrator** 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DHCP サーバーが XClarity Orchestrator と同じブロードキャスト・ドメインにセットアップされている場合は、XClarity Orchestrator 仮想アプライアンスのコンソールに表示されている IPv4 アドレスを使用して Web インターフェースにアクセスします。URL は次のとおりです。
     `https://{IPv4_address}/#/login.html`

     例:
     `https://192.0.2.10/#/login.html`

   初期ログイン・ページが表示されます。



「ログイン」ページでは、以下の操作を実行できます。

- Lenovo XClarity アイディエーション Web サイトから、または「**アイデアを送信**」をクリックして、XClarity Orchestrator に関するアイデアを送信します。
- 「**ユーザー・フォーラム**」をクリックして、Lenovo XClarity Community フォーラム Web サイト で質問をしたり回答を検索したりできます。
- 「**ユーザーズ・ガイド**」をクリックして、XClarity Orchestrator の使用方法に関する情報を見つけます。

- 「**ライセンス資格**」をクリックして、Features on Demand Web ポータル で Lenovo のすべてのライセンスを検索および管理します。
- 「**ツールキット**」をクリックして、使用可能な API に関する情報を見つけます。

2. 「言語」ドロップダウン・リストから、目的の言語を選択します。

   注：リソース・マネージャーおよび管理対象デバイスが提供する構成設定およびデータは英語のみである場合があります。

3. デフォルトの資格情報「USERID」および「PASSWORD」(0 はゼロ) を入力し、「**ログイン**」をクリックします。特定のユーザー・アカウントで XClarity Orchestrator に初めてログインしたときに、パスワードの変更を求められます。デフォルトでは、パスワードは**8 - 256**文字が含まれ、以下の条件を満たしている必要があります。

   重要：16 文字以上の強力なパスワードを使用をお勧めします。

   - 1 つ以上の英字が含まれ、英字、数字、および QWERTY キーボードの連続を含めて、2 文字以上の連続が含まれない (「abc」、「123」、「asd」など)。
   - 少なくとも 1 つの数字が含まれていなければなりません
   - 次の文字のうち、少なくとも 2 つが含まれる。
     – 大文字の英字 (A – Z)。
     – 子文字の英字 (a – z)。
     – 特殊文字 ; @ _ ! ' $ & +
     空白文字は使用できません。
   - ユーザー名の繰り返しや反転がない。
   - 2 つの同じ文字が連続していない (「aaa」、「111」、「...」など)。

終了後

重要：初めて XClarity Orchestrator 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。

ローカル・ユーザーの作成に進んで、初期セットアップを続行してください。

ローカル・ユーザーの作成

ローカル (組み込み) 認証サーバーでは、手動でユーザー・アカウントを作成できます。*ローカル・ユーザー・アカウント*は、Lenovo XClarity Orchestrator へのログインおよびリソースへのアクセス許可に使用されます。

このタスクについて

追加のセキュリティー対策として、ユーザー・アカウントを少なくとも 2 つ作成します。

手順

ローカル・ユーザーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーから「**管理 (⚙)**」 ➔ 「**セキュリティー**」の順にクリックし、左側のナビゲーションで「**ローカル・ユーザー**」をクリックして、「ローカル・ユーザー」カードを表示します。

ステップ 2. 「**作成**」アイコン (⊕) をクリックして、ユーザーを作成します。「新しいユーザーの作成」ダイアログが表示されます。

ステップ 3. ダイアログで以下の情報を入力します。

- 固有のユーザー名を入力します。英数字、ピリオド (.)、ダッシュ (-)、下線 (_) 文字を含む、最大 32 文字を指定できます。

  注：ユーザー名は大/小文字が区別されません。

- 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。デフォルトでは、パスワードは**8 - 256**文字が含まれ、以下の条件を満たしている必要があります。

  重要：16 文字以上の強力なパスワードを使用をお勧めします。

  – 1 つ以上の英字が含まれ、英字、数字、および QWERTY キーボードの連続を含めて、2 文字以上の連続が含まれない (「abc」、「123」、「asd」など)。
  – 少なくとも 1 つの数字が含まれていなければなりません
  – 次の文字のうち、少なくとも 2 つが含まれる。
    – 大文字の英字 (A – Z)。
    – 子文字の英字 (a – z)。
    – 特殊文字 ; @ _ ! ' $ & +
    空白文字は使用できません。
  – ユーザー名の繰り返しや反転がない。
  – 2 つの同じ文字が連続していない (「aaa」、「111」、「...」など)。

- (オプション) フルネーム、メール・アドレス、電話番号など、ユーザー・アカウントのお問い合わせ先情報を指定します。

  ヒント: フルネームには、文字、数字、スペース、ピリオド、ハイフン、アポストロフィ、およびコンマを含めて最大 128 文字を指定できます。

ステップ 4. 「**ユーザー・グループ**」タブをクリックし、このユーザーをメンバーにするユーザー・グループを選択します。

ヒント: ユーザー・グループが選択されていない場合は、デフォルトで**オペレーター・グループ**が割り当てられます

ステップ 5. 「**作成**」をクリックします。

ユーザー・アカウントが表に追加されます。

終了後

ネットワークの構成に進んで、初期セットアップを続行してください。

ネットワークの構成

Lenovo XClarity Orchestrator の初期セットアップ時に、1 つのネットワーク・インターフェース (IPv4 および IPv6 の設定を使用) を構成する必要があります。インターネットのルーティング設定も構成できます。

始める前に

インターフェースを選択する際は、以下の考慮事項を確認してください。

- このインターフェースは、検出と管理をサポートするように構成する必要があります。管理対象のリソース・マネージャーとデバイスと通信できる必要があります。
- 収集されたサービス・データを Lenovo サポートに手動で送信したり、自動問題通知 (コール・ホーム) を使用する場合は、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。

注意：

- リソース・マネージャーの接続後に XClarity Orchestrator 仮想アプライアンスの IP アドレスを変更すると、XClarity Orchestrator とマネージャーとの通信が失われ、マネージャーはオフラインと表示されます。XClarity Orchestrator の電源がオンになり稼働した後に仮想アプライアンスの IP アドレスを変更する必要がある場合は、IP アドレスを変更する前に、すべてのリソース・マネージャーが切断 (削除) されていることを確認してください。
- ネットワーク・インターフェースが動的ホスト構成プロトコル (DHCP) を使用するように構成されている場合は、DHCP リースの有効期限が切れると 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、リソース・マネージャーを切断 (削除) してから、再度接続する必要があります。この問題を避けるには、ネットワーク・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。
- 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。

手順

ネットワーク設定を構成するには、XClarity Orchestrator メニュー・バーから「**管理** (⚙)」 ➡ 「**ネットワーク**」をクリックし、以下の 1 つ以上の手順を実行します。

- **IP 設定の構成**「Ipv4 構成」カードおよび「IPv6 構成」カードから、IPv4 および IPv6 ネットワーク設定を使用する選択が可能です。適用可能な IP 構成設定を有効にして変更し、「**適用**」をクリックします。
  - **IPv4 設定**。IP の割り当て方法、IPv4 アドレス、ネットワーク・マスク、およびデフォルト・ゲートウェイを構成することができます。IP 割り当て方法については、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。静的 IP アドレスを使用する場合は、IP アドレス、ネットワーク・マスク、およびデフォルト・ゲートウェイを指定する必要があります。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で有効な IP アドレスを指定する必要があります。

    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。
  - **IPv6 設定**。IP の割り当て方法、IPv6 アドレス、プレフィックスの長さ、およびデフォルト・ゲートウェイを構成することができます。IP 割り当て方法については、静的に割り当てられた IP アドレス、ステートフル・アドレス構成 (DHCPv6)、ステートレス・アドレス自動構成を使用することを選択可能です。静的 IP アドレスを使用する場合は、IPv6 アドレス、プレフィックスの長さ、およびゲートウェイを指定する必要があります。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で有効な IP アドレスを指定する必要があります。

- **インターネットのルーティング設定も構成します**オプションで、「DNS 構成」カードからドメイン・ネーム・システム (DNS) の設定を構成します。次に、「**適用**」をクリックします。

  現在、IPv4 アドレスのみがサポートされています。

  DHCP を使用して IP アドレスを取得するか、「DHCP DNS」を有効または無効にして静的 IP アドレスを指定するかを選択します。静的 IP アドレスの使用を選択した場合は、1 つまたは 2 つの DNS サーバーの IP アドレスを指定します。

  DNS ホスト名とドメイン名を指定します。DHCP サーバーからドメイン名を取得するか、カスタム・ドメイン名を指定するかを選択できます。

  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 Orchestrator の DHCP リースの次回更新時に上書きされます。
  – DNS 設定を変更する場合は、仮想マシンを手動で再起動して変更を適用する必要があります。
  – DNS 設定を DHCP から静的 IP アドレスに変更した場合は、必ず DNS サーバー自体の IP アドレスも変更してください。

- **HTTP プロキシ設定を構成します。**オプションで、「プロキシ構成」カードからプロキシ・サーバーのホスト名、ポート、およびオプション資格情報を有効にして指定します。次に、「**適用**」をクリックします。

  注：
  - 必ず、プロキシー・サーバーが基本認証を使用するようにセットアップされている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ー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ー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。

終了後

日付と時刻の構成に進んで、初期セットアップを続行してください。

日付と時刻の構成

リソース・マネージャーから受信したイベントと、Lenovo XClarity Orchestrator のタイムスタンプを同期するために、少なくとも 1 つの (最大 4 つの) Network Time Protocol (NTP) サーバーをセットアップする必要があります。

始める前に

各 NTP サーバーは、ネットワークを介してアクセスできる必要があります。XClarity Orchestrator が実行されているローカル・システムでの 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 Orchestrator 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 Orchestrator 仮想アプライアンスおよびそのホストは、XClarity Orchestrator 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 Orchestrator 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 Orchestrator 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**VMware – 時刻同期の無効化 Web ページ の手順に従います。
- **Hyper-V**Hyper-V マネージャーから、XClarity Orchestrator 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 Orchestrator の日付と時刻を設定するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーで、「**管理** (⚙)」 ➞ 「**日付と時刻**」の順にクリックして、「日付と時刻」カードを表示します。

ステップ 2. XClarity Orchestrator 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。

ステップ 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。

ステップ 4. 「**適用**」をクリックします。

終了後

認証サーバーのセットアップに進んで、初期セットアップを続行してください。

認証サーバーのセットアップ

Lenovo XClarity Orchestrator には、ローカル (埋め込み) 認証サーバーが含まれます。また、独自の外部の Active Directory LDAP サーバーを使用することもできます。

始める前に

外部 LDAP ユーザーが XClarity Orchestrator にログインするには、XClarity Orchestrator でクローン作成された LDAP ユーザー・グループの直接のメンバーである必要があります。XClarity Orchestrator では、外部 LDAP サーバーで定義され、クローン作成された LDAP ユーザー・グループ内にネストされているユーザー・グループのメンバーであるユーザーを認識しません。

外部認証サーバーに必要なすべてのポートがネットワークおよびファイアウォールで開いていることを確認します。ポート要件については、利用可能なポート を参照してください。

このタスクについて

外部 LDAP サーバーが構成されていない場合は、XClarity Orchestrator は常にローカル認証サーバーを使用してユーザーを認証します。

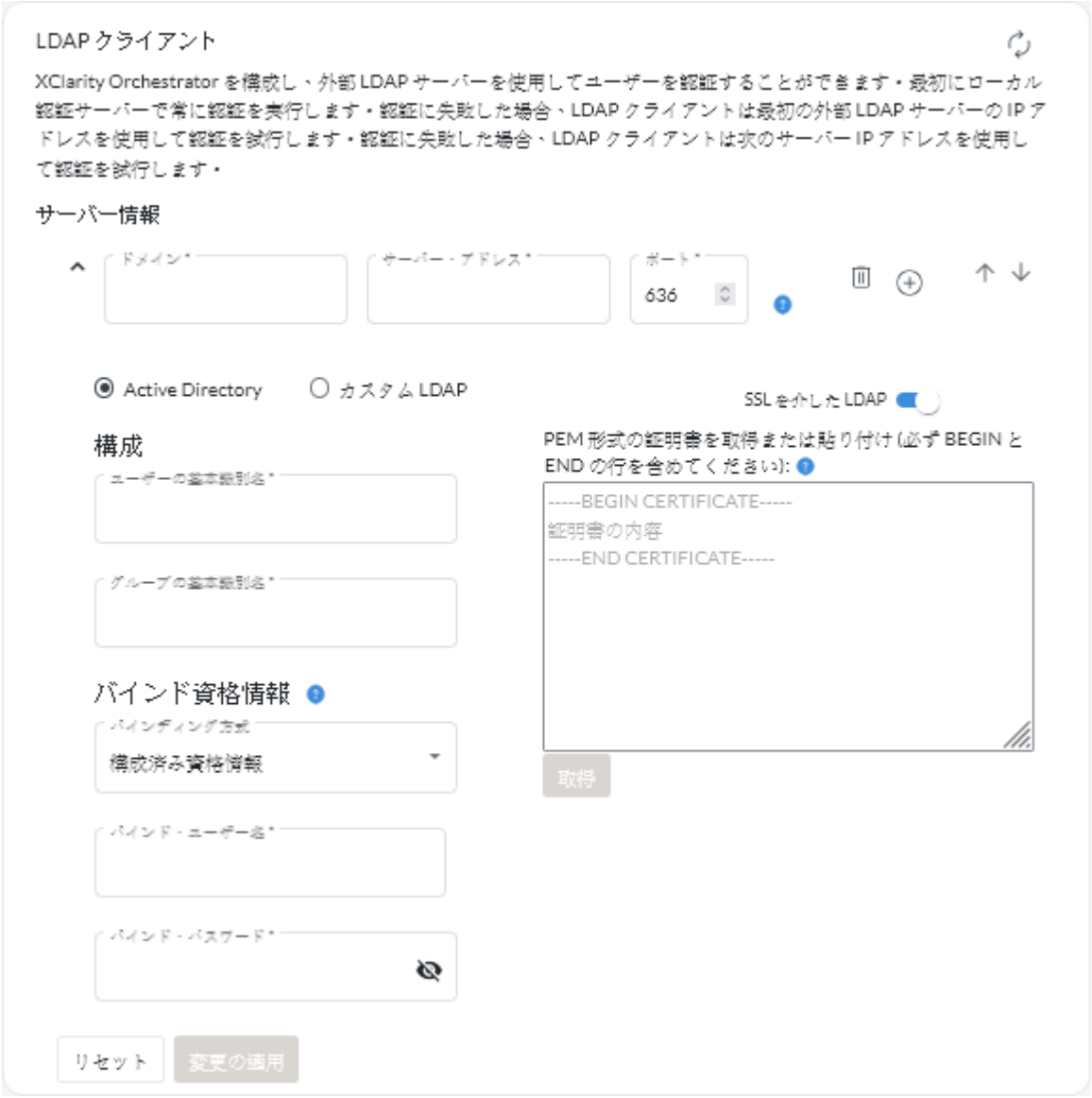
外部 LDAP サーバーが構成されている場合は、XClarity Orchestrator はまず、ローカル認証サーバーを使用してユーザーを認証しようとします。認証に失敗した場合、XClarity Orchestrator は最初の LDAP サーバーの IP アドレスを使用して認証を試行します。認証に失敗した場合、LDAP クライアントは次の LDAP サーバーの IP アドレスを使用して認証を試行します。

外部 LDAP ユーザーが XClarity Orchestrator に初めてログインすると、<ユーザー名>@<ドメイン> のユーザー・アカウントのクローンが XClarity Orchestrator で自動的に作成されます。クローン作成された外部 LDAP ユーザーをユーザー・グループに追加したり、アクセス制御の LDAP グループを使用したりできます。外部 LDAP ユーザーにスーパーバイザー権限を追加することもできます。

手順

外部 LDAP 認証サーバーを使用するように XClarity Orchestrator を構成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーで、「**管理** (⚙)」 → 「**セキュリティー**」の順にクリックし、左側のナビゲーションで「**LDAP クライアント**」をクリックして、「LDAP クライアント」カードを表示します。



ステップ 2. 次の手順を使用して、各外部 LDAP サーバーを構成します。

1. 「**追加**」アイコン (⊕) をクリックして、LDAP サーバーを追加します。
2. 外部 LDAP サーバーのドメイン名、IP アドレス、およびポートを指定します。

   ポート番号が 3268 または 3269 に明示的に設定*されていない*項目は、 ドメイン・コントローラーの項目と見なされます。

   ポート番号が 3268 または 3269 に設定されている項目は、グローバル・カタログの項目と見なされます。LDAP クライアントは、構成されている最初のサーバー IP アドレスのドメイン・コントローラーを使用して認証を試みます。これに失敗した場合、LDAP クライアントは、次のサーバー IP アドレスのドメイン・コントローラーを使用して認証を試みます。
3. 必要に応じて、詳細構成設定のカスタマイズを有効にします。カスタム構成を使用する場合は、ユーザー検索フィルターを指定できます。ユーザー検索フィルターを指定しない場合、`(&(objectClass=user)(|(userPrincipalName={0})(sAMAccountName={0})))` がデフォルトで使用されます。

   詳細構成が無効になっている場合は、既定の Active Directory 構成が使用されます。

4. 完全修飾 LDAP ベースの識別名を指定します。LDAP クライアントはそこからユーザー認証の検索を開始します。
5. 完全修飾 LDAP ベースの識別名を指定します。LDAP クライアントはそこからユーザー・グループの検索を開始します (たとえば、`dc=company,dc=com`)。
6. オプションで、XClarity Orchestratorを外部認証サーバーにバインドするための資格情報を指定します。2 つのバインディング方式のいずれかを使用できます。
   - **構成済み資格情報。**このバインディング方式を使用すると、特定のクライアント名とパスワードを使用してXClarity Orchestratorを外部認証サーバーにバインドします。このバインドに失敗すると認証プロセスも失敗します。ユーザー・アカウントの完全修飾 LDAP 識別名 (例:`cn=somebody,dc=company,dc=com`)、またはメール・アドレス (`somebody@company.com`) と LDAP 認証に使用するパスワードを指定して、 XClarity Orchestratorを LDAP サーバーにバインドします。このバインドに失敗すると認証プロセスも失敗します。

     識別名は、少なくとも読み取り専用特権を持つ、ドメイン内のユーザー・アカウントである必要があります。

     LDAP サーバーにサブドメインがない場合、そのドメインを指定せずにユーザー名を指定できます (例: `user1`)。ただし、LDAP サーバーにサブドメイン (例: `company.com` ドメイン内の `new.company.com` サブドメインなど) がある場合は、ユーザー名とドメイン (例: `user1@company.com`) を指定する必要があります。

     注意：外部 LDAP サーバーのクライアント・パスワードを変更した場合は、必ず XClarity Orchestrator の新規パスワードも更新してください (XClarity Orchestrator にログインできない XClarity Orchestrator オンライン・ドキュメント を参照)。
   - **ログイン資格情報。**このバインディング方式を使用すると、LDAP のXClarity Orchestrator ユーザー名とパスワードを使用して XClarity Orchestrator を外部認証サーバーにバインドします。認証サーバーへの接続を検証するために、*テスト・ユーザー・アカウント*の完全修飾 LDAP 識別名と、LDAP 認証に使用するパスワードを指定します。

     これらのユーザー資格情報は保存されません。成功すると、以降のすべてのバインドでは XClarity Orchestrator にログインするのに使用したユーザー名とパスワードを使用します。このバインドに失敗すると認証プロセスも失敗します。

     注：完全修飾ユーザー ID (例: administrator@domain.com) を使用してXClarity Orchestrator にログインする必要があります。
7. オプションで、セキュア LDAP を使用するには、「**LDAP over SSL**」トグルを選択して「**取得**」をクリックし、信頼できる SSL 証明書を取得してインポートします。「サーバー証明書の取得」ダイアログが表示された後、「**同意する**」をクリックして証明書を使用します。LDAP over SSL を使用すると、XClarity Orchestrator は LDAPS プロトコルを使用して、外部認証サーバーに安全に接続します。このオプションを選択すると、セキュア LDAP サポートを有効にするために、トラステッド証明書が使用されます。

   注意：LDAP over SSL を無効にすると、XClarity Orchestrator は安全ではないプロトコルを使用して、外部認証サーバーに接続します。この設定を選択した場合、ハードウェアがセキュリティーに対する攻撃を受けやすくなることがあります。
8. オプションで、「**上へ移動**」アイコン (↑) と「**下へ移動**」アイコン (↓) を使用して、LDAP サーバーの順序を変更できます。LDAP クライアントは、最初のサーバーの IP アドレスを使用して認証を試行します。認証に失敗した場合、LDAP クライアントは次のサーバー IP アドレスを使用して認証を試行します。

   重要：安全な LDAP 認証のためには、LDAP サーバーのルート認証局 (CA) の証明書、またはサーバーの中間証明書の 1 つを使用します。次のコマンドを実行することにより、コマンド・プロンプトでルート CA 証明書または中間 CA 証明書を取得できます。

そこでは、*{FullyQualifiedHostNameOrIpAddress}*は外部 LDAP サーバーの完全修飾名です。ルート CA 証明書または中間 CA 証明書は通常、出力の最後の証明書です (最後の `BEGIN-END`セクション)。

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

9. 「**変更の適用**」をクリックします。XClarity Orchestrator は IP アドレス、ポート、SSL 証明書、およびバインディング資格情報をテストし、LDAP サーバー接続を検証して、共通のエラーを検出しようとします。検証に成功した場合は、ユーザーが XClarity Orchestrator にログインするときに、ユーザー認証が外部認証サーバーで行われます。検証が失敗すると、エラー・メッセージが表示されます。このメッセージにはエラーのソースが示されています。

   注：検証に成功し LDAP サーバーへの接続が正常に完了しても、ルート識別名が正しくない場合、ユーザー認証に失敗することがあります。

終了後

追加のセキュリティー設定の構成に進んで、初期セットアップを続行してください。

追加のセキュリティー設定の構成

証明書、ユーザー・アカウントのセキュリティー設定など、追加のセキュリティー設定を構成できます。

手順

追加のセキュリティーを構成するには、以下の手順を 1 つ以上実行します。

- Lenovo XClarity Orchestrator は SSL 証明書を使用して、XClarity Orchestrator とリソース・マネージャー (Lenovo XClarity Administrator など) との間で信頼できるセキュアな通信を確立するだけでなく、ユーザーからXClarity Orchestrator への通信も確立します。デフォルトでは、XClarity Orchestrator およびリソース・マネージャーは、XClarity Orchestrator が生成する証明書を使用します。これは、内部証明機関 (CA) で発行された自己署名証明書です。外部の証明機関 (所属組織の証明機関、サード・パーティーの証明機関など) に署名を要求する証明書署名要求 (CSR) を生成するように選択できます (信頼できる外部署名済み XClarity Orchestrator サーバー証明書のインストール XClarity Orchestrator オンライン・ドキュメント を参照)。
- 外部サービス用のトラステッド証明書を XClarity Orchestrator 信頼ストアにインポートして、リソース・マネージャーおよびイベント・インテグレーター (Splunk など) とのセキュアな接続を確立できます (外部サービス用トラステッド証明書の追加 XClarity Orchestrator オンライン・ドキュメント を参照)。
- 内部サービス用のトラステッド証明書を XClarity Orchestrator 信頼ストアにインポートして、リソース・マネージャーおよび信頼できる LDAP サーバーとのセキュアな接続を確立できます (内部サービス用トラステッド証明書の追加 XClarity Orchestrator オンライン・ドキュメント を参照)。
- パスワードの複雑さ、アカウントのロックアウト、非アクティブな Web セッションのタイムアウトについて、セキュリティー設定を構成してください。これらの設定の詳細については、ユーザー・セキュリティー設定の構成 XClarity Orchestrator オンライン・ドキュメント を参照してください。

終了後

自動問題通知の構成および有効化 (コール・ホーム)に進んで、初期セットアップを続行してください。

自動問題通知の構成および有効化 (コール・ホーム)

特定の保守可能なイベント (リカバリー不能なメモリー・エラーなど) が特定のデバイスで生成された場合に問題を解決できるように、コール・ホーム機能を使用してサービス・チケットを自動的に開いてサービス・データを Lenovo サポートに送信するように Lenovo XClarity Orchestrator をセットアップできます。

始める前に

コール・ホーム機能を有効にする前に、XClarity Orchestrator およびコール・ホーム機能に必要なすべてのポートが使用可能であ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 XClarity Orchestrator オンライン・ドキュメント を参照してください。

コール・ホームによって要求されたインターネット・アドレスに対する接続が存在することを確認します。ファイアウォールについては、ファイアウォールおよびプロキシー・サーバー XClarity Orchestrator オンライン・ドキュメント を参照してください。

XClarity Orchestrator が HTTP プロキシーを介してインターネットにアクセスしている場合は、プロキシ・サーバーが基本認証を使用するように構成され、終了しないプロキシーとしてセットアップされていることを確認します。プロキシの設定について詳しくは、ネットワーク設定の構成 XClarity Orchestrator オンライン・ドキュメント を参照してください。

重要：コール・ホームが XClarity Orchestrator および Lenovo XClarity Administrator の両方で有効になっている場合、サービス・チケットの重複を避けるために、Lenovo XClarity Administrator v2.7 以降が使用されていることを確認します。コール・ホームが XClarity Orchestrator で有効になっており、Lenovo XClarity Administrator で無効になっている場合は、Lenovo XClarity Administrator v2.6 以降がサポートされます。

このタスクについて

コール・ホームが構成されて有効になっている場合、保守可能なイベントが特定のデバイスで発生すると、XClarity Orchestrator によりサービス・チケットが*自動的に*開かれ、Lenovo サポート・センターにそのデバイスのサービス・データが転送されます。

重要：Lenovo は、セキュリティーを確保することをお約束しています。Lenovo サポートに通常であれば手動でアップロードするサービス・データは、TLS 1.2 以降を使用して HTTPS 経由で Lenovo サポート・センターに自動的に送信されます。ビジネス・データが送信されることはありません。Lenovo サポート・センターでのサービス・データへのアクセスは、権限を持つサービス担当員に制限されています。

コール・ホームが有効でない場合、サポート・チケットの Web ページを開く方法の手順に従ってサービス・チケットを手動で開き、サービス・ファイルを Lenovo サポート・センターに送信できます。サービス・ファイルを収集する方法について詳しくは、XClarity Orchestrator オンライン・ドキュメントのLenovo サポート・センターでサービス・チケットを手動で開くを参照してください。

コール・ホームによって自動的に開かれたサービス・チケットの表示については、XClarity Orchestrator オンライン・ドキュメントのサービス・チケットとステータスの表示を参照してください。

手順

コール・ホームの自動問題通知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. XClarity Orchestrator のメニュー・バーで、「**管理** (⚙)」 ➡ 「**サービスおよびサポート**」をクリックし、左側のナビゲーションで「**コール・ホーム構成**」をクリックして「コール・ホーム構成」カードを表示します。

ステップ 2. Lenovo のプライバシーに関する声明 を確認して、「**Lenovo のプライバシーに関する声明に同意する**」をクリックします。

ステップ 3. 問題の報告時に使用するデフォルトの Lenovo お客様番号を指定します。

お客様番号は、XClarity Orchestrator ライセンスの購入時に受信した有効化証明のメールに記載されています。

ステップ 4. コール・ホーム・ステータスを「**有効**」に変更します。

ステップ 5. 複数のグループ割り当てから使用する主要連絡先を選択します。

デバイスのグループに主要サポート連絡先を割り当てることができます。デバイスが複数のグループのメンバーである場合、各グループに異なる主要連絡先が割り当てられている可能性があります。最初のグループに対して、またはデバイスが割り当てられた最後のグループに対して、主要連絡先の割り当てを選択できます。

ステップ 6. 連絡先情報と Lenovo サポートによるお問い合わせ方法を記入してください。

デバイスが、割り当てられた主要連絡先を持つグループのメンバーでない場合、デフォルトの連絡先はコール・ホームに使用されます。

ステップ 7. システム・ロケーション情報を入力します。

ステップ 8. 「**コール・ホームの接続テスト**」をクリックして、XClarity Orchestrator が Lenovo サポート・センターと通信できることを検証します。

ステップ 9. 「**適用**」をクリックします。

終了後

イベント・データ転送のセットアップに進んで、初期セットアップを続行してください。

イベント・データ転送のセットアップ

イベント、インベントリー、およびメトリックス・データを Lenovo XClarity Orchestrator から外部アプリケーションに転送して、データの監視と分析に使用できます。

このタスクについて

イベント・データ

XClarity Orchestrator は、指定した条件 (フィルター) に基づいて、ご使用の環境で発生したイベントを外部ツールに転送できます。すべての生成済みイベントが監視され、条件に一致するかどうかが確認されます。一致した場合、指定されたプロトコルを使用して指定された場所にイベントが転送されます。

XClarity Orchestrator は、以下の外部ツールへのイベント・データの転送をサポートしています。

- **メール**。イベント・データが、SMTP を使用して 1 つ以上のメール・アドレスに転送されます。
- **Intelligent Insights**。イベント・データは、事前定義された形式で、SAP Data Intelligence に転送されます。その後、SAP Data Intelligence を使用して、イベント・データを管理および監視できます。
- **REST**。イベント・データが、ネットワークを介して REST Web サービスに転送されます。
- **Syslog**。イベント・データが、ネットワークを介して一元管理ログ・サーバーに転送されます。そのサーバーでネイティブ・ツールを使用した syslog の監視が可能です。

XClarity Orchestrator は、*グローバル・フィルター*を使用して、転送するイベント・データの範囲を定義します。イベント・フィルターを作成して、イベント・コード、イベント・クラス、イベント重大度、およびサービス・タイプなど、特定のプロパティを持つイベントのみを転送できます。デバイス・フィルターを作成して、特定のデバイスによって生成されたイベントのみを転送することもできます。

インベントリーとイベント・データ

XClarity Orchestrator では、すべてのデバイスのすべてのインベントリーとイベント・データを外部アプリケーションに転送して、データの監視と分析に使用できます。

- **Splunk**。イベント・データは、事前定義された形式で、Splunk アプリケーションに転送されます。Splunk を使用して、イベント・データに基づくグラフや図表を作成できます。Splunk では複数の構

成を定義できます。ただし、XClarity Orchestrator がイベントを転送できるのは、1つの Splunk 構成対してのみです。そのため、Splunk の構成は一度に 1 つしか有効にできません。

メトリック・データ
XClarity Orchestrator は、管理対象デバイスに関して収集したメトリック・データを次の外部ツールに転送できます。

- **TruScale Infrastructure Services**。メトリック・データは、事前定義された形式で、Lenovo TruScale Infrastructure Services に転送されます。その後、TruScale Infrastructure Services を使用して、メトリック・データを管理および監視できます。

  注意：TruScale Infrastructure Services フォワーダーに関する情報は、Lenovo サービス担当員のみを対象とします。

  複数の TruScale Infrastructure Services フォワーダーを定義できます。ただし、XClarity Orchestrator がメトリック・データを転送できる TruScale Infrastructure Services フォワーダーは 1 つだけです。そのため、TruScale Infrastructure Services フォワーダーは一度に 1 つしか有効にできません。

  詳細: Lenovo TruScale Infrastructure Services について理解する

イベント・データ転送の詳細については、イベント、インベントリー、およびメトリック・データの転送 XClarity Orchestrator オンライン・ドキュメント を参照してください。

終了後

リソース・マネージャーの接続に進んで、初期セットアップを続行してください。

リソース・マネージャーの接続

Lenovo XClarity Orchestrator では、リソース・マネージャーおよびアプリケーション・マネージャーを使用してデバイスを監視および管理します。

始める前に

XClarity Orchestrator は、最大 10,000 のデバイス総数をまとめて管理できるリソース・マネージャーを無制限数サポートできます。

リソース・マネージャーがサポートされていることを確認します (サポートされるハードウェアおよびソフトウェア XClarity Orchestrator オンライン・ドキュメント を参照)。

リソース・マネージャーがオンラインであり、XClarity Orchestrator からネットワーク経由で到達可能であることを確認します。

リソース・マネージャーの認証に使用するユーザー・アカウントに正しい権限があることを確認します。XClarity Administrator の場合、ユーザー・アカウントが **lxc-supervisor**、**lxc-admin**、**lxc-security-admin**、**lxc-hw-admin** および **lxc-recovery** の役割のいずれかに割り当てられている必要があります。

リソース・マネージャーが、サポートされるイベント・フォワーダーの最大数に達していないことを確認します。XClarity Orchestrator は、リソース・マネージャーへの接続が作成されるとイベント・フォワーダーを作成します。

外部署名済み証明書があるリソース・マネージャーに接続する場合:

- X.509 v3 証明書である必要があります。XClarity Orchestrator は、外部署名された v1 証明書があるリソース・マネージャーに接続できません。
- 証明書の詳細に以下の要件が含まれていることを確認します。

- キー使用法には以下が含まれている必要があります。
  - キーの承諾
  - デジタル署名
  - キーの暗号化
- 拡張キー使用法には、以下の情報が含まれている必要があります。
  - サーバー認証 (1.3.6.1.5.5.7.3.1)
  - クライアント認証 (1.3.6.1.5.5.7.3.2)

このタスクについて

XClarity Orchestrator は以下のリソース・マネージャーおよびアプリケーション・マネージャーをサポートしています。

- **Lenovo XClarity Management Hub 2.0**。ThinkSystem および ThinkAgile デバイスを管理、監視、プロビジョニングします。デバイスと XClarity Orchestrator の間の通信を可能にするには、各 ThinkEdge クライアント・デバイスに UDC エージェントがインストールされている必要があります。

  重要：登録プロセス XClarity Management Hub 2.0 は、他のリソース・マネージャーとは異なります。詳細な手順については、。
- **Lenovo XClarity Management Hub**。ThinkEdge クライアント・デバイスを管理、監視、プロビジョニングします。デバイスと XClarity Orchestrator の間の通信を可能にするには、各 ThinkEdge クライアント・デバイスに UDC エージェントがインストールされている必要があります。

  重要：登録プロセス XClarity Management Hub は、他のリソース・マネージャーとは異なります。詳細な手順については、。
- **Lenovo XClarity Administrator**。ベースボード管理コントローラーを使用して Lenovo デバイスを管理、監視、プロビジョニングします。
- **Schneider Electric EcoStruxure IT Expert**。インフラストラクチャー・リソースの管理および監視。
- **VMware vRealize オペレーション・マネージャー**。

XClarity Management Hub または XClarity Administrator リソース・マネージャー、XClarity Orchestrator に接続する場合:

- リソース・マネージャーで管理されているすべてのデバイスに関する情報を取得します。
- 管理サーバーでイベント・フォワーダー (REST Web サービス用) が作成されて有効になるため、イベントを監視して XClarity Orchestrator に転送できるようになります。

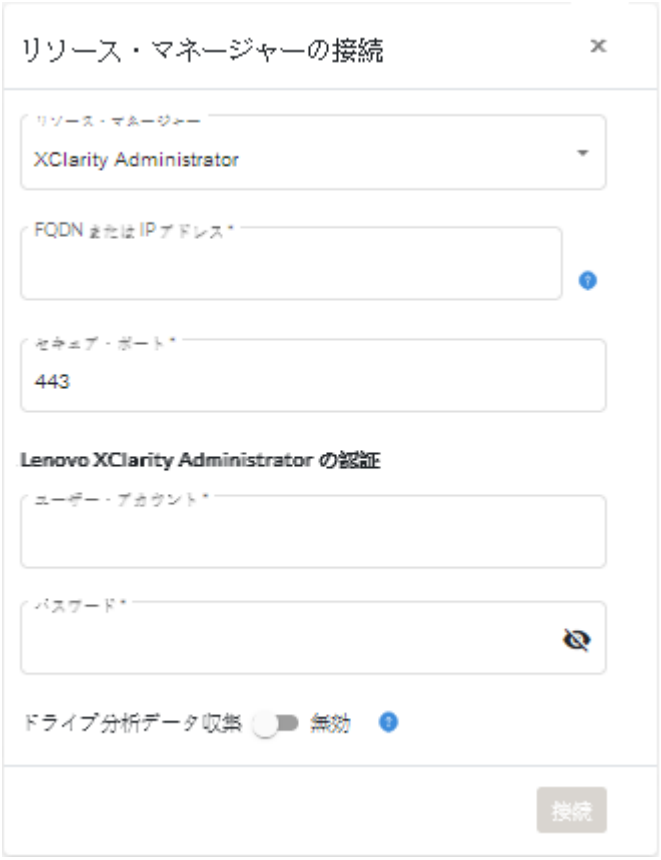
指定したネットワーク・アドレス (IP アドレスまたはホスト名) はマネージャー名として使用されます。

手順

リソースまたはアプリケーション・マネージャーに接続するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⎈)」 ➡ 「**リソース・マネージャー**」の順にクリックして、「リソース・マネージャー」カードを表示します。

ステップ 2. 「**接続**」アイコン (⊙) をクリックして、リソース・マネージャー を表示します。「リソース・マネージャーの接続」ダイアログ。



ステップ 3. リソース・マネージャーのタイプを選択し、必要な情報を入力します。

- XClarity Management Hub 2.0 または **XClarity Management Hub**
  1. 管理ハブ・インスタンスによって生成された登録キーを入力し、「**接続**」をクリックします。登録要求トークンを取得するには、管理ハブ・ポータルにログインし、「**登録**」をクリックしてから、「**登録キーの作成**」をクリックします。
  2. 生成された XClarity Orchestrator 登録鍵をコピーします。
  3. 管理ハブ・ポータルで、「**登録**」をクリックして「**登録キーのインストール**」をクリックし、XClarity Orchestrator 登録トークンを貼り付け、「**接続**」をクリックします。
- **XClarity Administrator**

- 完全修飾ドメイン名または IP アドレス (IPv4 または IPv6) を指定します。ドメイン名なしでホスト名を使用することはサポートされていません。
- オプションで、リソース・マネージャーのポートを変更します。デフォルトは 443 です。
- リソース・マネージャーへのログインに使用するユーザー・アカウントとパスワードを指定します。
- オプションで、**ドライブ分析データ収集**を有効にします。有効にすると、ThinkSystem および ThinkAgile デバイスでドライブ分析データが毎日収集され、予測分析に使用されます。ドライブ分析データ収集は、XClarity Administrator v3.3.0 以降のリソース・マネージャーでのみサポートされています。

  注意：データの収集時にシステムのパフォーマンスに影響する場合があります。

- **EcoStruxure IT エキスパート**。接続に使用する名前、トークン・キー、および URL を指定します。
- **vRealize Operations Manager**
  - 完全修飾ドメイン名または IP アドレス (IPv4 または IPv6) を指定します。ドメイン名なしでホスト名を使用することはサポートされていません。
  - オプションで、リソース・マネージャーのポートを変更します。デフォルトは 443 です。
  - オプションで、ユーザーとグループの認証ソースを選択します。
  - vRealize Operations Manager へのログインに使用するユーザー・アカウントとパスワードを指定します。

ステップ 4. 「**接続**」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は、ジョブのリンクをクリックしてジョブの詳細を表示します (を参照)。

リソース・マネージャーとの接続が確立されると、マネージャーがテーブルに追加されます。

ステップ 5. XClarity Management Hub に接続することを選択した場合 、登録キーを含むダイアログが表示されます。

接続されたら、「**クリップボードにコピー**」をクリックして登録キーをコピーします。次に、XClarity Management Hubにログインして「**管理**」 → 「**ハブ構成**」をクリックし、「**登録キーのインストール**」をクリックします。次に、登録キーを貼り付け、「**送信**」をクリック します。

終了後

初期セットアップが完了しました。

第 5 章　XClarity Orchestrator ライセンスの適用

Lenovo XClarity Orchestrator は、無料アプリケーションです。無料試用版ライセンスで最大 90 日間 XClarity Orchestrator を無料で使用できますが、無料試用期間の経過後、引き続き該当する XClarity Orchestrator 機能を使用し、XClarity Orchestrator サービスおよびサポートを取得するには、適切なライセンスを購入してインストールする必要があります。

始める前に

ライセンス購入について詳しくは、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。

高度な機能 (サーバー構成と OS デプロイメント) をサポートする各管理対象デバイスにライセンスが必要です。

- 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*。だたし、これらデバイスに対して XClarity Orchestrator 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

事前定義された**スーパーバイザー**の役割が割り当てられているユーザー・グループのメンバーである必要があります。

このタスクについて

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

- **XClarity Orchestrator**。Orchestrator およびベース管理機能サーバー、シャーシ、スイッチ、およびストレージ・デバイスおよび XClarity Orchestrator のサービスとサポートのための資格について確認します。Orchestrator 機能を使用するには、サーバー構成と OS デプロイメントをサポートしているすべてのデバイスに対して、XClarity Orchestrator でのライセンスが必要です。XClarity Orchestrator のサービスおよびサポートには、*すべての管理対象デバイス*にライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Orchestrator 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 Orchestrator のライセンスの数が必要な数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。必要な数のライセンスがインストールされる前に、ライセンスの猶予期間 (無料試用期間を含む) が終了した場合、すべての XClarity Orchestrator機能 (監視、基本管理、および分析を含む) は無効になります。ログインすると、追加のライセンスを適用できる「ライセンス情報」ページにリダイレクトされます。

  たとえば、追加の ThinkSystem サーバー 100 台とラック・スイッチ 20 個を管理を既存の XClarity Orchestrator で既存の XClarity Administrator インスタンスを使用して行う場合、ユーザー・インター

フェースですべての機能が無効になるまでの 90 日間で、追加の XClarity Orchestrator 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。XClarity Orchestrator 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、XClarity Orchestrator でサービスおよびサポートを利用する場合は、これらが必要です。XClarity Orchestrator 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、機能が再び有効になります。

重要：XClarity Orchestrator のベース・ライセンスは XClarity Pro および XClarity Orchestrator Analytics ライセンスの前提条件です。XClarity Pro または XClarity Orchestrator のライセンスの数が適合*している*が、アクティブなベース・ライセンスの数が適合して*いない*場合は、すべてのデバイスですべての XClarity Orchestrator 機能 (分析機能が無効を含む) が無効になります。

- **Lenovo XClarity Pro**。拡張管理機能 (サーバー構成および OS デプロイメント) を有効にします。拡張機能をサポートする管理対象デバイスごとに XClarity Orchestrator のライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Pro 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 Pro ライセンスの数が適合しない場合、適切なライセンスをインストールするための 90 日間の猶予期間があります。必要な数のライセンスがインストールされる前に猶予期間 (無料試用期間を含む) が終了した場合、サーバー構成および OS デプロイメントは*すべてのデバイス*で無効になります。

  XClarity Pro ライセンスのインストールについて詳しくは、ライセンスおよび 90 日間の無料トライアル XClarity Administrator オンライン・ドキュメントを参照してください。

- **XClarity Orchestrator 分析**。分析機能を有効にします。拡張機能をサポートする管理対象デバイスごとに XClarity Orchestrator のライセンスが必要です。

  ライセンスの準拠は、管理される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 XClarity Orchestrator Analytics 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 Orchestrator Analytics ライセンスの数が必要な数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。必要な数のライセンスがインストールされる前に猶予期間 (無料試用期間を含む) が終了した場合、「**監視 → 分析**」メニューがすべてのデバイスで無効になり、分析の表示、カスタム・アラート・ルールの作成、および*すべてのデバイス*への照会ができなくなります。

  重要：XClarity Orchestrator Analytics ライセンスをインストールしたら、ユーザー・インターフェースを最新表示する必要があります。

  注：期限が切れた (90 日の猶予期間を超えて有効期限を過ぎた) XClarity Orchestrator Analytics ライセンスをインストールして、ユーザー・インターフェースを最新表示すると、分析機能が無効になります。つまり、アクティブな試用期間または猶予期間が中断され、分析サービスが停止し、分析機能が淡色表示されます。(これには数分間かかる場合があります。)新しい有効なライセンスをインポートすることで、分析機能を再度有効にすることができます。

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*。

ライセンスが引き換えられると、アクティベーション期間が始まります。

ライセンス・*アクティベーション・キー*を使用してライセンスをインストールします。ライセンスを引き換えた後、使用可能なライセンスのすべてまたはサブセットのアクティベーション・キーを作成し、アクティベーション・キーをダウンロードして XClarity Orchestrator にインストールすることができます。

XClarity Orchestrator 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。

ライセンスが既にインストールされている場合、XClarity Orchestrator 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*。

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 Orchestrator 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。

XClarity Orchestrator をアップグレードする場合、またはアクティベーション・キーの復元を必要とするエラー状態が発生した場合は、Features on Demand Web ポータル からエクスポートされたキーを使用するか、すべてのアクティベーション・キー (顧客 ID ごとに) をダウンロードし、そのアクティベーション・キーを (個々のアクティベーション・キーとして、またはキー ZIP ファイルとしてまとめて) XClarity Orchestrator にインポートします。

Features on Demand Web ポータル から現在のソフトウェア・ライセンスのリストを表示できます。

手順

XClarity Orchestrator ライセンスをインストールするには、次の手順で行います。

ステップ 1. 管理したいデバイス数に基づいてライセンスをご購入される場合については、Lenovo 担当員または認定ビジネス・パートナーにお問い合わせください。

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。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。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。

認証コードは 22 文字の英数字文字列です。次の手順を完了するには、認証コードが必要です。

ステップ 2. ライセンスのアクティベーション・キーを取得します。

- **認証コードからのアクティベーション・キーの作成**
  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。このキー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**」フィールドと一致させます。

     使用可能なライセンスのサブセットを引き換えると、同じ認証コードを使用して、別のアクティベーション・キーに残っているライセンスを引き換えることができます。
  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**」をクリックしてアクティベーション・キーを生成します。
  8. 必要に応じて、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、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は、アクティベーション・キーを含むメールを受信します。アクティベーション・キーは、.KEY 形式のファイルです。

     注：「**ダウンロード・リンク**」をクリックして、Features on Demand Web ポータル からアクティベーション・キーをダウンロードすることもできます (別個または一括で)。
- **既存のアクティベーション・キーのダウンロード**
  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. 「**履歴の取得**」をクリックします。

3. 「**検索タイプ**」として「Lenovo お客様番号で履歴を検索する」を選択します。
4. 「**検索値**」フィールドに Lenovo お客様番号を入力します。お客様番号の形式は 121XXXXXXX です。
5. 「**すべて選択**」をクリックしてすべてのアクティベーション・キーをダウンロードするか、リストから個々のアクティベーション・キーを選択します。
6. 「**メール**」をクリックしてキーをメールで送信するか、「**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. XClarity Orchestrator でライセンスを適用します。

1. XClarity Orchestrator のメニュー・バーで、「**保守** ()」をクリックし、「**ライセンス**」タブをクリックすると「ライセンス情報」カードが表示されます。

2. 「**インポートして適用**」アイコン () をクリックし、ライセンスを適用します。
3. 適用するライセンスのアクティベーション・キー・ファイルを「インポート」ダイアログにドラッグ・アンド・ドロップするか、「**参照**」をクリックしてファイルを見つけます。

   複数のアクティベーション・キーをインポートするには、.ZIP ファイルにキーを押し、インポートする ZIP ファイルを選択します。
4. 「**インポート**」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、アクティベーション (ライセンス) キーが、インストール済みライセンス数およびアクティベーション期間 (開始日と有効期限) とともに表に示されます。

ステップ 4. 機能を無効にした後で有効なライセンスを適用した場合は、ログアウトしてから再度ログインして、該当する機能を有効にします。

終了後

「ライセンス情報」カードから、以下の操作を実行できます。

- 「**保存**」アイコン () をクリックして、ローカル・システムに選択した 1 つ以上のアクティベーション・キーを保存します。

  複数の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。

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 (北アメリカ)
  - ESDAP@lenovo.com (アジア太平洋)

  - ESDEMEA@lenovo.com (欧州、中東、アジア)
  - ESDLA@lenovo.com (中南米)
  - 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) 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) までお問い合わせください。

第 6 章　XClarity Orchestrator の更新

Lenovo XClarity Orchestrator を更新して最新の Orchestrator ソフトウェアを使用することができます。

始める前に

詳細: XClarity Orchestrator の更新方法

事前定義された**スーパーバイザー**の役割が割り当てられているユーザー・グループのメンバーである必要があります。

XClarity Orchestrator修正バンドル (v1.4.2 など) は、同じリリースのバージョン (v1.4.0 や v1.4.1 など) にのみ適用できます。修正バンドルには以前のすべての修正が含まれています (たとえば、v1.4.2 には、v1.4.1 と同様の修正と追加の修正が含まれています)。ただし、修正バンドルにはコード・ベースの全体が含まれているわけではありません。

注意：XClarity Orchestrator を更新する前に以下の考慮事項を確認してください。

- **XClarity Orchestrator v2.0 へ**仮想アプライアンスに必要な最小ストレージは、3 つの接続されたディスクで**合計** 551 GB です。また、200 GB 以上の 3 番目のディスク (ディスク 2) を接続する必要があります。

  新しいハードディスクを追加する前に、XClarity Orchestrator 仮想アプライアンスの電源をオフにする必要があります。

  仮想アプライアンスに新しいハードディスクを追加するには、以下の手順を実行します。

  - **VMware vSphere を使用した ESXi の場合**
    1. VMware vSphere Client を介してホストに接続します。
    2. XClarity Orchestrator 仮想マシンの電源をオフにします。
    3. 仮想マシンを右クリックし、「**設定の編集**」をクリックします。
    4. 「**新しいデバイスの追加**」 ➔ 「**ハードディスク**」を選択します。
    5. サイズを 200 GB に変更します。
    6. 「OK」をクリックします。
    7. XClarity Orchestrator 仮想マシンの電源を入れます。
  - **VMware vCenter を使用した ESXi の場合**
    1. VMware vCenter を介してホストに接続します。
    2. 仮想マシンの電源をオフにします。
    3. 仮想マシンの設定を開き、「**追加**」をクリックします。
    4. 「**ハードディスク**」 ➔ 「**新しい仮想ディスクの作成**」をクリックします。
    5. ディスク・フォーマットとして「SCSI」を選択します。
    6. HDD の容量を 200 GB に構成します。
    7. 「OK」をクリックします。
    8. 仮想マシンの電源を入れます。
  - **Microsoft Hyper-V の場合**
    1. 「サーバー・マネージャー」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. XClarity Orchestrator 仮想マシンを選択し、「アクション」ペインで「**シャットダウン**」をクリックします。
    4. 「**設定**」をクリックして「設定」ダイアログを表示します。
    5. 「IDE Controller 1」を選択します。
    6. 右側のペインで、「**ハードディスク・ドライブ**」を選択し、「**追加**」をクリックして新しいハードディスクを追加します。

7. 右側のペインで、「**仮想ハードディスク (.vhd) ファイル**」を選択し、「**新規**」をクリックして「新規仮想ハードディスク・ウィザード」を表示します。
8. 指示に従ってウィザードを完了します。.vhd 形式 (例: `LXCO-disk3.vhd`) を使用してディスク・ドライブ名を指定し、サイズを 200 GB に設定します。
9. XClarity Orchestrator 仮想マシンを選択し、「操作」ペインで「**スタート**」をクリックします。

- **XClarity Orchestrator v1.6 へ**。XClarity Orchestrator v1.6 にアップデートするには、XClarity Orchestrator v1.5 が必要です。XClarity Orchestrator v1.5 を実行していない場合は、XClarity Orchestrator v1.6 にアップデートする前に、XClarity Orchestrator v1.5 にアップデートする必要があります。
- **XClarity Orchestrator v1.5 へ**。XClarity Orchestrator v1.5 にアップデートするには、XClarity Orchestrator v1.4 が必要です。XClarity Orchestrator v1.4 を実行していない場合は、XClarity Orchestrator v1.5 にアップデートする前に、XClarity Orchestrator v1.4 にアップデートする必要があります。
- **XClarity Orchestrator v1.4 へ**。XClarity Orchestrator v1.4 にアップデートするには、XClarity Orchestrator v1.3 が必要です。XClarity Orchestrator v1.3 を実行していない場合は、XClarity Orchestrator v1.4 にアップデートする前に、XClarity Orchestrator v1.3 にアップデートする必要があります 。
- **XClarity Orchestrator v1.3 へ**
  - XClarity Orchestrator v1.3 への更新は、完了までに 2 時間以上かかる場合があります。更新が完了したかどうかを確認するには、「**メンテナンス**」 ➞ 「**Orchestrator サーバーの更新**」をクリックし、新しいリリースが一覧に表示され、「適用済みステータス」が「適用中」ではないことを確認します。
  - **重要**: XClarity Orchestrator を v1.3 にアップデートする前に、XClarity Orchestrator 仮想アプライアンスのホスト名が **lxco** であり、「**管理 (⎈)**」 ➞ 「**ネットワーク**」ページの「DNS 構成」カードにドメイン名が設定されていないことを確認してください。
  - **スーパーバイザー**役割が割り当てられたユーザーは、更新中にユーザー・グループの**スーパーバイザー・グループ**に追加されます。
  - **オペレーター**役割が割り当てられたユーザーは、更新中にユーザー・グループの**オペレーター・レガシー・グループ**に追加されます。ユーザー・グループの**オペレーター・レガシー・グループ**は、**オペレーター・レガシー**役割に関連付けられ、ユーザーには以前のリリースの**オペレーター**役割と同じ権限が与えられます。**オペレーター・レガシー**役割およびユーザー・グループの**オペレーター・レガシー・グループ**は、今後のリリースで廃止される予定です。既存のユーザー・グループには、更新中に**オペレーター**役割が割り当てられます。
  - カスタム分析アラートを生成するルールの作成がXClarity Orchestrator v1.3 で簡略化されます。既存のカスタム・アラート・ルールは新しい形式に移行されず、更新完了後に失われます。
- **XClarity Orchestrator v1.1 から**
  - **スーパーバイザー**役割が割り当てられたユーザーは、更新中にユーザー・グループの**スーパーバイザー・グループ**に追加されます。
  - **オペレーター**役割が割り当てられたユーザーは、更新中にユーザー・グループの**オペレーター・レガシー・グループ**に追加されます。ユーザー・グループの**オペレーター・レガシー・グループ**は、**オペレーター・レガシー**役割に関連付けられ、ユーザーには以前のリリースの**オペレーター**役割と同じ権限が与えられます。**オペレーター・レガシー**役割およびユーザー・グループの**オペレーター・レガシー・グループ**は、今後のリリースで廃止される予定です。既存のユーザー・グループには、更新中に**オペレーター**役割が割り当てられます。
  - カスタム分析アラートを生成するルールの作成がXClarity Orchestrator v1.3 で簡略化されます。既存のカスタム・アラート・ルールは新しい形式に移行されず、更新完了後に失われます。
  - 仮想アプライアンスに必要な最小ストレージは、2 つの接続されたディスクで**合計 301 GB** です。ディスク 0 のストレージを 251 GB 以上に増やす必要があります。また、100 GB 以上の 2 番目のディスク (ディスク 1) を接続する必要があります。新しいハードディスクを追加する前に、XClarity Orchestrator 仮想アプライアンスの電源をオフにする必要があります。

    仮想アプライアンスに新しいハードディスクを追加するには、以下の手順を実行します。

    - **VMware vSphere を使用した ESXi の場合**
      1. VMware vSphere Client を介してホストに接続します。

2. XClarity Orchestrator 仮想マシンの電源をオフにします。
3. 仮想マシンを右クリックし、「**設定の編集**」をクリックします。
4. 「**新しいデバイスの追加**」 ➔ 「**ハードディスク**」を選択します。
5. サイズを 100 GB に変更します。
6. 「**OK**」をクリックします。
7. XClarity Orchestrator 仮想マシンの電源を入れます。

– **VMware vCenter を使用した ESXi の場合**
1. VMware vCenter を介してホストに接続します。
2. 仮想マシンの電源をオフにします。
3. 仮想マシンの設定を開き、「**追加**」をクリックします。
4. 「**ハードディスク**」 ➔ 「**新しい仮想ディスクの作成**」をクリックします。
5. ディスク・フォーマットとして「**SCSI**」を選択します。
6. HDD の容量を 100 GB に構成します。
7. 「**OK**」をクリックします。
8. 仮想マシンの電源を入れます。

– **Microsoft Hyper-V の場合**
1. 「サーバー・マネージャー」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. XClarity Orchestrator 仮想マシンを選択し、「アクション」ペインで「**シャットダウン**」をクリックします。
4. 「**設定**」をクリックして「設定」ダイアログを表示します。
5. 「**IDE Controller 0**」を選択します。
6. 右側のペインで、「**ハードディスク・ドライブ**」を選択し、「**追加**」をクリックして新しいハードディスクを追加します。
7. 右側のペインで、「**仮想ハードディスク (.vhd) ファイル**」を選択し、「**新規**」をクリックして「新規仮想ハードディスク・ウィザード」を表示します。
8. 指示に従ってウィザードを完了します。.vhd 形式 (例: `LXCO-disk2.vhd`) を使用してディスク・ドライブ名を指定し、サイズを 100 GB に設定します。
9. XClarity Orchestrator 仮想マシンを選択し、「操作」ペインで「**スタート**」をクリックします。

- **XClarity Orchestrator v1.1 へ**
  – すべてのユーザーが自動的に**SupervisorGroup** ユーザー・グループに追加されます。すべてのユーザは更新完了後、デフォルトでスーパーバイザー特権を持ちます。スーパーバイザー・ユーザーは、権限を必要としないその他のユーザーのスーパーバイザー権限を削除できます。
  – 既存の外部 LDAP 構成は削除されています。更新が完了した後で、外部 LDAP 認証サーバーを再構成する必要があります。

更新プロセス中に Orchestrator サーバーが再起動すると、すべてのユーザーがログオフします。再起動が完了するまで数分待つ必要があります。更新が完了して再起動した後、Web ブラウザーのキャッシュをクリアし、Web ブラウザーを更新してから再びログインしてください。

更新をインストールする前に、XClarity Orchestrator 仮想アプライアンスをバックアップしてください (管理サーバー・データのバックアップと復元 XClarity Orchestrator オンライン・ドキュメント を参照)。

XClarity Orchestrator を更新する前に、必要なポートとインターネット・アドレスがすべて使用可能になっていることを確認します。詳しくは、利用可能なポートとファイアウォールおよびプロキシー・サーバーを参照してください。

手順

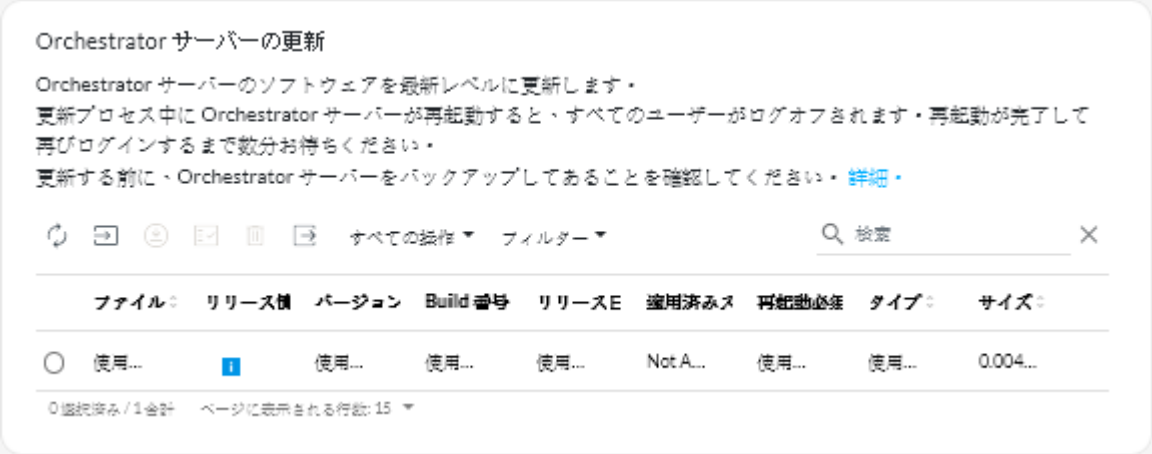
XClarity Orchestrator を更新するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator ホストにネットワーク接続できるワークステーションに、XClarity Orchestrator ダウンロード Web ページ から Orchestrator サーバーの更新パッケージ・ファイル (.tgz) をダウンロードします。

更新パッケージ・ファイルには、ペイロード・ファイル (.tar.gz)、メタデータ (.xml)、変更履歴 (.chg)、readme (.txt) の必要なファイルがすべて含まれています。

ステップ 2. XClarity Orchestrator のメイン・メニューから、「**保守**」() をクリックし、さらに「**Orchestrator サーバーの更新**」をクリックすると、「Orchestrator サーバーの更新」カードが表示されます。

現在インストールされているバージョンより前の Orchestrator サーバーの更新は、「適用できない」というステータスが適用されたテーブルにリストされ、Orchestrator サーバーに適用することはできません。



ステップ 3. 「**インポート**」アイコン () をクリックして、「インポート」ダイアログを表示します。

ステップ 4. 更新パッケージ・ファイル (.tgz) 全体を「インポート」ダイアログにドラッグ・アンド・ドロップするか、または「**参照**」をクリックしてファイルを特定します。

ステップ 5. 「**インポート**」をクリックします。

注意：更新ファイルのインポートに時間がかかる可能性があります。インポート処理が完了するまで、「Orchestrator サーバーの更新」カードから移動しないでください。「Orchestrator サーバーの更新」カードから移動すると、インポート・プロセスは中止されます。

インポートが完了すると、「Orchestrator サーバー・ファイル」カードのテーブルに Orchestrator サーバーの更新が表示されます。

XClarity Orchestrator のメニュー・バーで「**監視**」() → 「**ジョブ**」の順にクリックすると、インポートの進行を監視できます。

ステップ 6. 「Orchestrator サーバー・ファイル」カードから、インストールする更新パッケージを選択します。

ステップ 7. 「**更新の適用**」アイコン () をクリックします。

XClarity Orchestrator のメニュー・バーで「**監視**」() → 「**ジョブ**」の順にクリックすると、更新の進行を監視できます。

ステップ 8. 更新が完了し、XClarity Orchestrator が再起動するまで待ちます。更新プロセスに時間がかかる可能性があります。

仮想アプライアンス・ホストにアクセスできる場合は、仮想アプライアンス・コンソールから進行状況を監視できます。以下に例を示します。

```
Lenovo XClarity Orchestrator  Version x.x.x
---------------

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

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

You have 118 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
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 x. To continue without changing IP settings
  ... ...
```

ステップ 9. Web ブラウザーのキャッシュをクリアして、Web ブラウザーの表示情報を更新します。

完了すると、「**適用済みステータス**」列が「適用済み」に変わります。

終了後

「Orchestrator サーバー・ファイル」カードから、以下の操作を実行できます。

- XClarity Orchestrator のインスタンスの現在のバージョンおよびビルド番号を表示するには、XClarity Orchestrator タイトル・バーの「**ユーザー・アカウント**」メニュー (⚙) をクリックし、「**バージョン情報**」をクリックします。
- XClarity Orchestrator に適用された特定の更新の更新履歴を表示するには、「**適用済みステータス**」列の更新ステータスのリンクをクリックします。
- 「**名前を付けて保存**」アイコン (↓) をクリックして、選択した Orchestrator サーバーの更新をローカル・システムに保存します。
- 「**削除**」アイコン (🗑) をクリックして、選択された Orchestrator サーバーの更新を削除します。

第 7 章　XClarity Orchestrator のアンインストール

仮想マシン管理ツールを使用して、Lenovo XClarity Orchestrator の仮想アプライアンスをアンインストールできます。

手順

XClarity Orchestrator 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. すべての リソース・マネージャー を切断して削除します。

a. XClarity Orchestrator のメニュー・バーで、「**リソース** ()」 → 「**リソース・マネージャー**」の順にクリックして、「リソース・マネージャー」カードを表示します。

b. リソース・マネージャーをすべて選択します。

c. 「**削除**」アイコン () をクリックします。

ステップ 2. 仮想マシン管理ツールを使用して XClarity Orchestrator をアンインストールします。

- **VMware vCenter を使用した ESXi の場合**
  1. VMware vCenter を介してホストに接続します。
  2. 「**VMware ホスト**」クライアント・インベントリでXClarity Orchestrator 仮想マシンを右クリックし、ポップアップ・メニューから「**ゲスト OS**」を選択します。
  3. 「**シャットダウン**」をクリックします。
  4. 「**VMware ホスト**」クライアント・インベントリで仮想マシンを右クリックし、ポップアップ・メニューから「**ゲスト OS**」を選択します。
  5. 「**削除**」をクリックします。
- **VMware vSphere を使用した ESXi**
  1. VMware vSphere Client を介してホストに接続します。
  2. XClarity Orchestrator 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. 「Server Manager」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. XClarity Orchestrator 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。