Lenovo

Lenovo XClarity Management Hub

インストールおよびユーザーズ・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

第 1 章　Lenovo XClarity Management Hub の計画

Lenovo XClarity Management Hub のインストールの計画に役立つ以下の考慮事項と前提を確認してください。

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 Management Hub 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

ハイパーバイザー要件

Lenovo XClarity Management Hub 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。

- VMware ESXi 7.0、U1、U2、および U3
- VMware ESXi 6.7、U1、U2[1]、および U3

VMware ESXi の場合、仮想アプライアンスは OVF テンプレートです。

重要：

- 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。

ハードウェア要件

次の表は、管理対象の Edge クライアント・デバイスの数に基づく XClarity Management Hub の*最小推奨*構成の一覧です。ご使用環境によっては、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。

管理対象の Edge クライアント・デバイスの数	プロセッサー	メモリー	ストレージ
0 ～ 100 デバイス	6	32 GB	340 GB
100 ～ 200 デバイス	8	34 GB	340 GB
200 ～ 400 デバイス	10	36 GB	340 GB
400 ～ 600 デバイス	12	40 GB	340 GB
600 ～ 800 デバイス	14	44 GB	340 GB
800 ～ 1,000 デバイス	16	48 GB	340 GB

1. これは、XClarity Management Hub 仮想アプライアンスで SSD データストアとして使用するストレージの最小量です。

ソフトウェア要件

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

- **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 Management Hub 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)。

管理可能なデバイス

XClarity Management Hub で、最大 10,000 台の ThinkEdge Client デバイス (ベースボード管理コントローラーなし) を管理、監視、プロビジョニングできます。

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。

Web ブラウザー

XClarity Management Hub 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)

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		

DNS 名	ポート	プロトコル
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

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)
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

Lenovo XClarity Management Hub を構成して、1 つのネットワーク・インターフェース (eth0) や 2 つのネットワーク・インターフェース (eth0 および eth1) を通信に使用できます。

Lenovo XClarity Management Hub は、以下のネットワーク上で通信します。

- *管理ネットワーク*は、Lenovo XClarity Management Hub と管理対象デバイスの間の通信に使用されます。
- *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。

1 つのインターフェース (eth0)

1 つのインターフェース (eth0) を使用する場合、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。

Lenovo XClarity Management Hub をセットアップする際に、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。

- デバイス検出および管理 (ファームウェア更新を含む) をサポートするようにネットワーク・インターフェースを構成する必要があります。Lenovo XClarity Management Hub は、管理ネットワークから管理すべてのデバイスと通信できる必要があります。Lenovo XClarity Management Hub は、ネットワークから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。
- OS イメージをデプロイするには、eth0 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。
- **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。

2 つのインターフェース (eth0 および eth1)

2 つのネットワーク・インターフェース (eth0 と eth1) を使用する場合、物理的に分離したネットワークまたは仮想的に分離したネットワークとしてネットワークをセットアップできます。

eth0 および eth1 ネットワーク・インターフェースを定義する際は、以下の考慮事項を確認します。

- eth0 ネットワーク・インターフェースは、管理ネットワークに接続され、デバイス検出および管理をサポートするように構成されている必要があります。Lenovo XClarity Management Hub は、管理ネットワークから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。

- eth1 ネットワーク・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。
- オペレーティング・システム・イメージをデプロイするには、eth1 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するサーバー・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。
- どちらのネットワークでも機能を実行できます。
- 仮想的に分離したネットワークでは、管理ネットワークからのパケットとデータ ネットワークからのパケットは、同じ物理接続を介して送信されます。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 タグ付けを使用します。

IP アドレスに関する考慮事項

ネットワークを構成する前に、以下の IP アドレスに関する考慮事項を確認してください。

- XClarity Management Hub が稼働した後で仮想アプライアンスの IP アドレスを変更すると、XClarity Orchestrator とすべての管理対象デバイスで接続の問題が発生します。IP アドレスを変更する必要がある場合は、XClarity Orchestrator から XClarity Management Hub を切断し、IP アドレスを変更する前にすべての管理対象デバイスを管理解除し、IP アドレスの変更が完了した後で XClarity Management Hub を XClarity Orchestrator に再接続します
- 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。管理対象デバイス (ThinkEdge クライアント・デバイス以外) の IP アドレスが変更された場合は、デバイスを管理解除してから、再度管理対象に戻す必要があります。
- 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。
- 以下のデバイスを管理するには、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。
  - 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。

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　エッジ・クライアント・デバイス用 XClarity Management Hub の構成

Lenovo XClarity Management Hub に初めてアクセスするときは、XClarity Management Hub の初期セットアップを行うために実行が必要な手順がいくつかあります。

手順

XClarity Management Hub の初期セットアップを行うには、以下の手順を実行します。

ステップ 1. XClarity Management Hub Web インターフェースにログインします。

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. 追加ユーザー・アカウントの作成。

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. Orchestrator サーバーで XClarity Management Hub に登録します。

エッジ・クライアント・デバイス用 XClarity Management Hub へのログイン

XClarity Management Hub Web インターフェースは、XClarity Management Hub 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

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

XClarity Management Hub では、アクティビティに関係なく、60 分後にユーザー・セッションから自動的にログアウトされます。

手順

以下の手順を実行して、XClarity Management Hub Web インターフェースにログインします。

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

```
https://<IPv4_address>
```

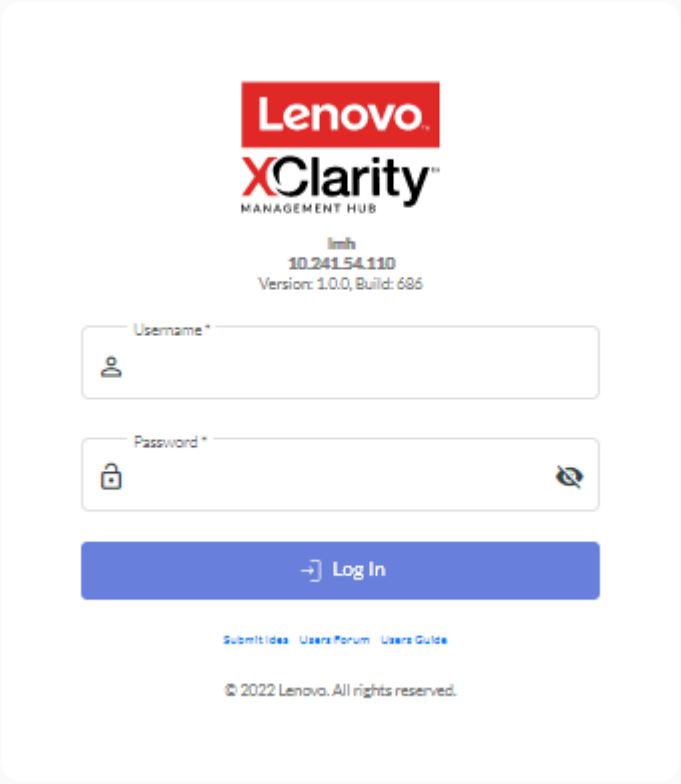
例:

```
https://192.0.2.10
```

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。

- 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 Management Hub にアクセスします。
- XClarity Management Hub 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 Management Hub 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 Management Hub にアクセスします。
- 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 Management Hub 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 Management Hub 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。

XClarity Management Hub 初期ログイン・ページが表示されます。



ステップ 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：構成設定および管理対象デバイスが提供する値は英語のみである場合があります。

ステップ 3. 資格情報を入力し、「**ログイン**」をクリックします。

初めて XClarity Management Hub ログインする場合、デフォルトの資格情報 USERID および PASSW0RD (0 はゼロ) を入力します。

ステップ 4. 使用許諾契約書を読み、同意します。

ステップ 5. デフォルトの資格情報を使用して初めてログインした場合、パスワードの変更を求めるプロンプトが表示されます。デフォルトでは、パスワードには 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) 少なくとも 1 つの大文字の英字が含まれている

- (2) 少なくとも 1 つの小文字の英字が含まれている
- (3) 少なくとも 1 つの数字が含まれている
- (4) 少なくとも 1 つの特殊文字が含まれている
- (5) ユーザー名と同じではない

ステップ 6. 初めてログインした場合、現在の自己署名証明書を使用するか、外部 CA 署名済み証明書を使用するかを選択するよう求めるプロンプトが表示されます。外部署名済み証明書を使用する場合、「サーバー証明書」ページが表示されます。

注意：自己署名証明書はセキュアではありません。独自の外部署名済み証明書を生成し、インストールすることをお勧めします。

外部署名済み証明書の使用については、エッジ・クライアント・デバイス用 XClarity Management Hub の信頼できる外部署名済みサーバー証明書のインストールを参照してください。

終了後

XClarity Management Hub Web インターフェースの右上隅の「**ユーザー・アカウント**」メニュー (⚙) から、以下の操作を実行できます。

- 「**ログアウト**」をクリックして、現行セッションからログアウトできます。XClarity Management Hub ログイン・ページが表示されます。
- Lenovo XClarity Community フォーラム Web サイトを使用して質問し、回答を確認します。
- XClarity Management Hub に関するアイデアを送信するには、Web インターフェースの右上隅の「**ユーザー・アカウント**」メニュー (⚙) で「**アイデアを送信**」をクリックし、Lenovo XClarity アイディエーション Web サイト に直接移動します。
- 「**ユーザーズ・ガイド**」をクリックしてオンライン・ドキュメントを表示します。
- 「**バージョン情報**」をクリックして、XClarity Management Hub のリリースに関する情報を表示できます。
- 「**言語の変更**」をクリックして、ユーザー・インターフェースの言語を変更できます。以下の言語がサポートされています。
  - 英語 (en)
  - 簡体字中国語 (zh-CN)
  - 繁体字中国語 (zh-TW)
  - フランス語 (fr)
  - ドイツ語 (de)
  - 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)
  - スペイン語 (es)
  - タイ語 (th)

エッジ・クライアント・デバイス用 Lenovo XClarity Management Hub のユーザー・アカウントの作成

Lenovo XClarity Management Hub のユーザー・アカウントを 10 まで作成できます。

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. Lenovo XClarity Management Hub メニュー・バーで、「**セキュリティー**」(⚙) → 「**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、パスワードには **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) 少なくとも 1 つの大文字の英字が含まれている
  - (2) 少なくとも 1 つの小文字の英字が含まれている
  - (3) 少なくとも 1 つの数字が含まれている
  - (4) 少なくとも 1 つの特殊文字が含まれている
  - (5) ユーザー名と同じではない

ステップ 4. 「**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

「ローカル・ユーザー」カードから、以下の操作を実行できます。

- 「**編集**」アイコン (✎) をクリックしてユーザー・アカウントのパスワードとプロパティを変更する。パスワードに有効期限はない点に注意してください。
- 選択したユーザーを削除するには、「**削除**」アイコン (🗑) をクリックします。

エッジ・クライアント・デバイス用 XClarity Management Hub のネットワーク設定の構成

1 つの IPv4 ネットワーク・インターフェースとインターネットのルーティング設定を構成できます。

始める前に

ネットワークを構成する前に、ネットワークに関する考慮事項を確認してください (ネットワークに関する考慮事項 を参照)。

手順

ネットワーク設定を構成するには、XClarity Management Hub 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**eth0 インターフェースの場合、「**Eth0 インターフェース**」タブをクリックし、該当する IPv4 アドレス設定を構成してから、「**適用**」をクリックします。

  注意：

  – XClarity Management Hub が稼働した後で仮想アプライアンスの IP アドレスを変更すると、XClarity Orchestrator とすべての管理対象デバイスで接続の問題が発生します。IP アドレスを変更する必要がある場合は、XClarity Orchestrator から XClarity Management Hub を切断し、IP アドレスを変更する前にすべての管理対象デバイスを管理解除し、IP アドレスの変更が完了した後で XClarity Management Hub を XClarity Orchestrator に再接続します

  現在、IPv4 アドレスのみがサポートされています。

  – **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・ゲートウェイには、有効な IP アドレスを入力し、有効なインターフェース (eth0) 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。

    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。

- **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。

  DNS サーバーの IP アドレスを変更できます。

DNS サーバーの完全修飾ドメイン名 (FQDN) とホスト名は XClarity Management Hub サーバーと同じのため、変更できません。

エッジ・クライアント・デバイス用 XClarity Management Hub の日付と時刻の構成

タイム・スタンプを XClarity Management Hub とすべての管理対象デバイスの間で同期するために、少なくとも 1 つの (最大 4 つの) Network Time Protocol (NTP) サーバーを設定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 Management Hub 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 Management Hub 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 Management Hub 仮想アプライアンスおよびそのホストは、XClarity Management Hub 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。XClarity Management Hub 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 Management Hub 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。

手順

XClarity Management Hub 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 Management Hub 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 Management Hub 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。

エッジ・クライアント・デバイス用 Lenovo XClarity Management Hub のセキュリティー証明書の管理

Lenovo XClarity Management Hub は SSL 証明書を使用して、Lenovo XClarity Management Hub と管理対象デバイス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、ユーザーまたはさまざまなサービスによる Lenovo XClarity Management Hub との通信も確立します。デフォルトでは、Lenovo XClarity Management Hub および XClarity Orchestrator は、自己署名され、内部証明機関によって発行されたXClarity Orchestrator による生成証明書を使用します。

始める前に

このセクションは、SSL 標準と SSL 証明書の基本的な知識を持つ管理者を対象としており、その説明と管理方法が含まれています。公開鍵と証明書に関する一般情報については、Wikipedia の X.509 の Web ページと Internet X.509 Public Key Infrastructure Certificate および Certificate Revocation List (CRL) Profile (RFC5280) Web ページ を参照してください。

このタスクについて

Lenovo XClarity Management Hub 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、Lenovo XClarity Management Hub 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。Lenovo

XClarity Management Hub 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 Lenovo XClarity Management Hub 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。

Lenovo XClarity Management Hub は、送信されてくる SSL/TLS 接続を受け入れるいくつかのサービスを提供します。Web ブラウザーなどのクライアントがこれらのサービスのいずれかに接続する場合、Lenovo XClarity Management Hub はその *サーバー証明書*を接続してきたクライアントに提示して識別させます。クライアントは、トラステッド証明書のリストを維持する必要があります。Lenovo XClarity Management Hub のサーバー証明書がクライアントのリストに含まれていない場合、機密性の高い情報を信頼できないソースとやりとりすることを避けるために、クライアントは Lenovo XClarity Management Hub から切断されます。

Lenovo XClarity Management Hub は、管理対象デバイスおよび外部サービスと通信する場合はクライアントとして機能します。これが発生すると、管理対象デバイスまたは外部サービスは、Lenovo XClarity Management Hub が検証するサーバー証明書を提供します。Lenovo XClarity Management Hub によってトラステッド証明書のリストが維持されます。管理対象デバイスまたは外部サービスが提供する *トラステッド証明書*がリストに含まれていない場合、機密性の高い情報を信頼できないソースとやりとりすることを避けるために、Lenovo XClarity Management Hub は管理対象デバイスまたは外部サービスから切断されます。

以下のカテゴリーの証明書は、Lenovo XClarity Management Hub のサービスによって使用され、接続しているクライアントによって信頼されるものです。

- **サーバー証明書**。初期ブート時に、固有のキーと自己署名証明書が生成されます。これらはデフォルトのルート証明機関として使用され、Lenovo XClarity Management Hub のセキュリティー設定の「証明機関」ページで管理できます。キーが漏えいした場合や、組織にすべての証明書を定期的に交換しなければならないというポリシーがある場合を除いて、このルート証明書を再生成する必要はありません (エッジ・クライアント・デバイス用 XClarity Management Hub の自己署名サーバー証明書の再生成 を参照)。また、初期セットアップ中に別の鍵が生成され、内部証明機関によって署名されたサーバー証明書が作成されます。この証明書は、デフォルトのLenovo XClarity Management Hub サーバー証明書として使用されます。これは、Lenovo XClarity Management Hub でネットワーク・アドレス (IP または DNS アドレス) の変更が検出されるたびに再生成され、証明書にサーバーの正しいアドレスが含まれるようになります。この証明書はカスタマイズでき、オンデマンドで生成できます (エッジ・クライアント・デバイス用 XClarity Management Hub の自己署名サーバー証明書の再生成参照)。

  デフォルトの自己署名サーバー証明書の代わりに外部署名済みサーバー証明書を使用することもできます。これには、証明書署名要求 (CSR) を生成し、プライベートまたは商用の証明書のルート証明機関によって CSR に署名して、すべての証明書チェーンを Lenovo XClarity Management Hub にインポートします (エッジ・クライアント・デバイス用 XClarity Management Hub の信頼できる外部署名済みサーバー証明書のインストール を参照)。

  デフォルトの自己署名サーバー証明書を使用する場合は、Web ブラウザーに証明書のエラー・メッセージが表示されないようにするために、信頼できるルート証明機関としてサーバー証明書を Web ブラウザーにインポートすることをお勧めします (エッジ・クライアント・デバイス用 Lenovo XClarity Management Hub の Web ブラウザーへのサーバー証明書のインポート を参照)。
- **OS デプロイ証明書**。オペレーティング・システム・デプロイメント・サービスでは、別の証明書が使用されます。これは、オペレーティング・システムのインストーラーがデプロイ・プロセス中にデプロイメント・サービスに確実に接続するためのものです。キーが暗号漏えいした場合は、Lenovo XClarity Management Hub を再起動することで再生成できます。

エッジ・クライアント・デバイス用 XClarity Management Hub の自己署名サーバー証明書の再生成

新しい証明機関またはサーバー証明書を生成して、現在の自己署名 Lenovo XClarity Management Hub サーバー証明書を置き換えるか、現在 XClarity Management Hub がカスタマイズされた外部署名済みサーバー証明書を使用している場合は、XClarity Management Hub が生成した証明書を復元できます。この新しい自己署名サーバー証明書は、XClarity Management Hub によって HTTPS アクセスに使用されます。

始める前に

注意：新しいルート CA を使用して XClarity Management Hub サーバー証明書を再生成した場合、XClarity Management Hub から管理対象デバイスへの接続が失われるため、デバイスを再度管理対象にする必要があります。ルート CA を変更せずに XClarity Management Hub サーバー証明書を再生成する場合 (証明書の有効期限が切れた場合など)、デバイスを再管理する必要はありません。

このタスクについて

現在使用されているサーバー証明書は、自己署名であるか外部署名であるかにかかわらず、新しいサーバー証明書が生成、署名、インストールされるまでは使用されます。

重要：サーバー証明書が変更された場合、管理ハブが再起動し、すべてのユーザー・セッションが終了します。ユーザーが Web インターフェースでの作業を続ける場合はログインしなおす必要があります。

手順

自己署名 XClarity Management Hub サーバー証明書を生成するには、以下の手順を実行します。

ステップ 1. XClarity Management Hub メニュー・バーで、「**セキュリティー**」(⚙) → 「**サーバー証明書**」をクリックし、「**自己署名サーバー証明書の再生成**」カードを表示します。

ステップ 2. 「**自己署名サーバー証明書の再生成**」カードから、要求のためのフィールドに入力します。

- 証明機関に関連付けられた発行国または発行地域の 2 文字の ISO 3166 コード (米国の場合は US)。
- 証明書に関連付けられた州または都道府県のフルネーム (California、New Brunswick など)。

- 証明書に関連付けられた都市のフルネーム (San Jose など)。この値は、50 文字を超えてはなりません。
- 証明書を所有する組織 (会社)。通常、これは正式な会社名です。Ltd.、Inc.、Corp など、サフィックスを含める必要があります (ACME International Ltd. など)。この値は、60 文字を超えてはなりません。
- (オプション) 証明書を所有する組織単位 (ABC Division など)。この値は、60 文字を超えてはなりません。
- 証明書の所有者の共通名。これは通常、証明書を使用するサーバーの完全修飾ドメイン名 (FQDN) または IP アドレスです (`www.domainname.com`、`192.0.2.0` など)。この値は、63 文字を超えてはなりません。

  注：現在のところ、この属性は証明書に影響を与えません。
- サーバー証明書が無効になった日付と時刻。

  注：現在のところ、これらの属性は証明書に影響を与えません。

注：サーバー証明書の再生成時に、サブジェクト代替名を変更できません。

ステップ 3. 「**自己署名サーバー証明書の再生成**」をクリックして、自己署名証明書を再生成し、「**証明書の再作成**」をクリックして確認します。
管理ハブが再起動され、確立されたユーザー・セッションがすべて終了します。

ステップ 4. Web ブラウザーでログインしなおします。

終了後

「自己署名サーバー証明書の再作成」カードから、以下の操作を実行できます。
- 「**証明書の保存**」をクリックして、現在のサーバー証明書を PEM 形式でローカル・システムに保存します。
- 「**証明書のリセット**」をクリックして、デフォルト設定を使用してサーバー証明書を再生成します。プロンプトが表示されたら、Ctrl + F5 を押してブラウザーの情報を更新し、Web インターフェースへの接続を再確立します。

エッジ・クライアント・デバイス用 XClarity Management Hub の信頼できる外部署名済みサーバー証明書のインストール

プライベートまたは商用証明機関 (CA) によって署名された信頼できるサーバー証明書を使用できます。外部署名済みサーバー証明書を使用するには、証明書署名要求 (CSR) を生成し、そのサーバー証明書をインポートして、既存のサーバー証明書と置き換えます。

始める前に

注意：

- 新しいルート CA を使用して外部署名済み Lenovo XClarity Management Hub サーバー証明書をインストールした場合、XClarity Management Hub から管理対象デバイスへの接続が失われるため、デバイスを再度管理対象にする必要があります。ルート CA を変更せずに外部署名済み Lenovo XClarity Management Hub サーバー証明書をインストールする場合 (証明書の有効期限が切れた場合など)、デバイスを再管理する必要はありません。
- CSR が生成された後、署名済みサーバー証明書がインポートされる前に新しいデバイスが追加された場合、新しいサーバー証明書を受け取るにはそれらのデバイスを再起動する必要があります。

このタスクについて

ベスト・プラクティスとして、常に v3 署名済み証明書を使用してください。

外部署名済みサーバー証明書は、「**CSR ファイルの生成**」ボタンを使用して最後に生成された証明書署名要求から作成する必要があります。

外部署名済みサーバー証明書コンテンツは、CA のルート証明書、中間証明書、およびサーバー証明書を含む CA 署名チェーン全体を含む証明書バンドルであることが必要です。

新しいサーバー証明書が信頼できる第三者によって署名されていない場合は、次に Lenovo XClarity Management Hub に接続したときに Web ブラウザーにセキュリティー・メッセージが表示されて、新しい証明書を承認するかどうかをたずねられます。このセキュリティー・メッセージが表示されないようにするには、サーバー証明書をダウンロードして、Web ブラウザーのトラステッド証明書のリストにインポートします (エッジ・クライアント・デバイス用 Lenovo XClarity Management Hub の Web ブラウザーへのサーバー証明書のインポート を参照)。

XClarity Management Hubは、現行セッションを終了することなく、新しいサーバー証明書の使用を開始します。新規セッションは新しい証明書を使用して確立されます。使用中の新しい証明書を使用するには、Web ブラウザーを再起動します。

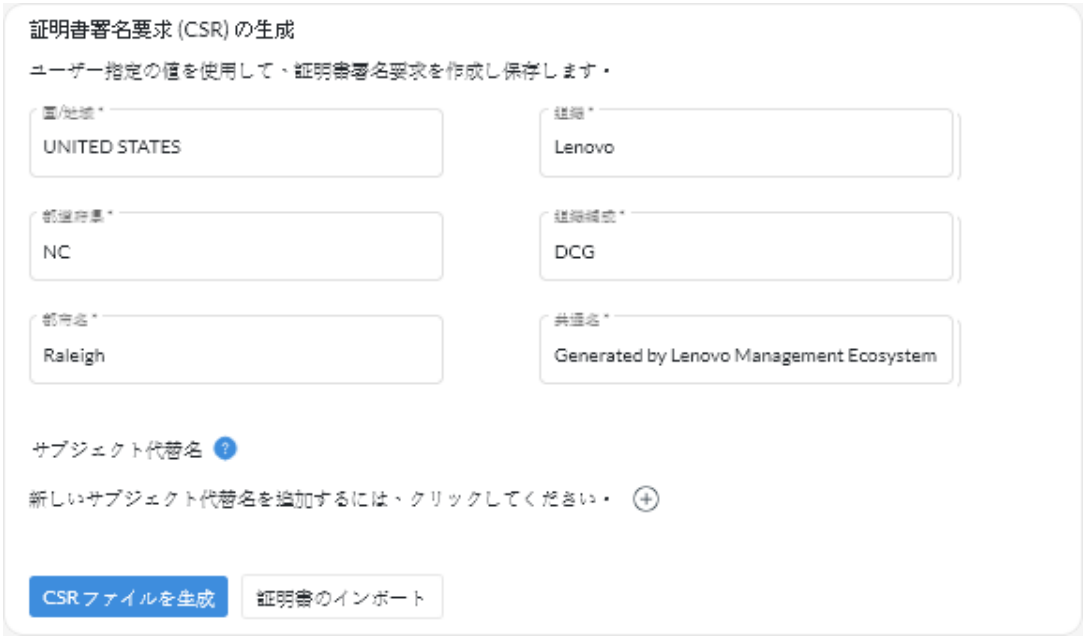
重要：サーバー証明書を変更した場合、すべての確立されたユーザー・セッションで Ctrl + F5 をクリックして Web ブラウザーの情報を最新に更新し、XClarity Management Hub に対する接続を再確立することによって、新しい証明書を受け入れる必要があります。

手順

外部署名済みサーバー証明書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. 証明書署名要求を作成し、該当ファイルをローカル・システムに保存します。

1. XClarity Management Hub のメニュー・バーで、「**セキュリティー**」() → 「**サーバー証明書**」をクリックし、新しい「証明書署名要求の生成」カードを表示します。



2. 「証明書署名要求 (CSR) の生成」カードから、要求のためのフィールドに入力します。
   - 証明機関に関連付けられた発行国または発行地域の 2 文字の ISO 3166 コード (米国の場合は US)。
   - 証明書に関連付けられた州または都道府県のフルネーム (California、New Brunswick など)。

- 証明書に関連付けられた都市のフルネーム (San Jose など)。この値は、50 文字を超えてはなりません。
- 証明書を所有する組織 (会社)。通常、これは正式な会社名です。Ltd.、Inc.、Corp など、サフィックスを含める必要があります (ACME International Ltd. など)。この値は、60 文字を超えてはなりません。
- (オプション) 証明書を所有する組織単位 (ABC Division など)。この値は、60 文字を超えてはなりません。
- 証明書の所有者の共通名。これは、証明書を使用しているサーバーのホスト名である必要があります。この値は、63 文字を超えてはなりません。

  注：現在のところ、この属性は証明書に影響を与えません。
- (オプション) CSR の生成時にカスタマイズ、削除され、X.509「subjectAltName」拡張に追加されるサブジェクト代替名。指定されたサブジェクト代替名は検証 (指定されたタイプに基づいて) され、CSR が生成された後にのみ CSR に追加されます。デフォルトでは、XClarity Management Hub のゲスト・オペレーティング・システムのネットワーク・インターフェースによって検出された IP アドレスおよびホスト名に基づいて、XClarity Management Hub が CSR のサブジェクト代替名を自動的を定義します。

  注意：サブジェクト代替名は、管理ハブの完全修飾ドメイン名 (FQDN) または IP アドレスを含んでいる必要があり、サブジェクト名を管理ハブの FQDN に設定する必要があります。CSR プロセスを開始する前に、これらの必須フィールドが存在し、正しいことを確認し、作成された証明書が完了していることを確認します。証明書データが欠落していると、管理ハブを Lenovo XClarity Orchestrator に接続しようとするときに、信頼できない接続が発生する可能性があります。

  指定する名前は、選択したタイプに対して有効である必要があります。
  - **DNS** (FQDN を使用します (例: hostname.labs.company.com))
  - **IP アドレス** (例: 192.0.2.0)
  - **メール** (例: example@company.com)

ステップ 2. トラステッド証明機関 (CA) に CSR を送信します。CA は CSR に署名して、サーバー証明書を返送します。

ステップ 3. 外部署名済みサーバー証明書と CA 証明書を XClarity Management Hub にインポートし、現在のサーバー証明書を置き換えます。

1. 「証明書署名要求 (CSR) の生成」カードから、「**証明書のインポート**」をクリックして、「証明書のインポート」ダイアログを表示します。
2. サーバー証明書と CA 証明書を PEM 形式でコピーして貼り付けます。サーバー証明書から始めて、ルート CA 証明書の証明書チェーン全体を指定する必要があります。
3. 「**インポート**」をクリックして、サーバー証明書を XClarity Management Hub 信頼ストアに保存します。

ステップ 4. Ctrl + F5 を押してブラウザーの情報を更新し、Web インターフェースへの接続を再確立して、新しい証明書を受け入れます。これは、すべての確立済みユーザー・セッションで実行する必要があります。

エッジ・クライアント・デバイス用 Lenovo XClarity Management Hub の Web ブラウザーへのサーバー証明書のインポート

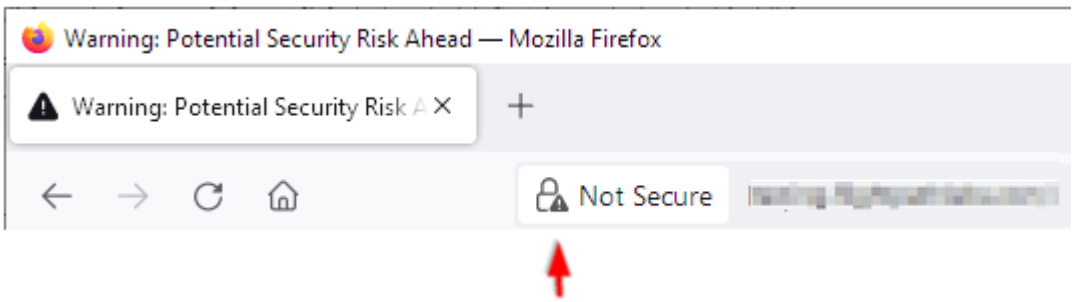
ローカル・システムに現在のサーバーの証明書のコピーを、PEM 形式で保存できます。次に、Lenovo XClarity Management Hub にアクセスしたときに Web ブラウザーにセキュリティー警告メッセージが表示されないようにするために、Web ブラウザーのトラステッド証明書のリストまたは他のアプリケーションに証明書をインポートできます。

手順

ご使用の Web ブラウザーにサーバー証明書をインポートするには、以下の手順を実行します。

- Chrome
  1. Lenovo XClarity Management Hub サーバー証明書をエクスポートします。
     a. 上部アドレス・バーにある「保護されていない通信」の警告アイコンをクリックします。例:

     b. 「**証明書が無効です**」をクリックして、「証明書」ダイアログを表示します。
     c. 「**詳細**」タブをクリックします。
     d. 「**エクスポート**」をクリックします。
     e. 証明書ファイルの名前と場所を指定し、「**保存**」を選択して証明書をエクスポートします。
     f. 「証明書ビューアー」ダイアログを閉じます。
  2. Lenovo XClarity Management Hub サーバー証明書をブラウザーのトラステッド・ルート証明機関証明書のリストにインポートします。
     a. Chrome ブラウザーで、ウィンドウの右上隅にある 3 つのドットをクリックし、「**設定**」をクリックして、「設定」ページを開きます。
     b. 「**プライバシーとセキュリティー**」をクリックし「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。
     c. 「**詳細**」セクションまでスクロールし、「**デバイス証明書の管理**」をクリックします。
     d. 「**インポート**」をクリックし、「**次へ**」をクリックします。
     e. 前にエクスポートした証明書ファイルを選択して、「**次へ**」をクリックします。
     f. 証明書を保存する場所を選択し、「**次へ**」をクリックします。
     g. 「**完了**」をクリックします。
     h. Chrome ブラウザーを閉じてから開き直し、Lenovo XClarity Management Hub を開きます。
- Firefox
  1. Lenovo XClarity Management Hub サーバー証明書をエクスポートします。
     a. 上部アドレス・バーにある「保護されていない通信」の警告アイコンをクリックします。例:



     b. 「**接続が安全ではありません**」をクリックし、「**詳細情報**」をクリックします。
     c. 「**証明書の表示**」をクリックします。
     d. 「**その他**」セクションまでスクロールダウンし、「**PEM (cert)**」リンクをクリックして、ファイルをローカル・システムに保存します。

2. Lenovo XClarity Management Hub サーバー証明書をブラウザーのトラステッド・ルート証明機関証明書のリストにインポートします。
   a. ブラウザーを開いて、**ツール → 設定**をクリックし、「**プライバシーとセキュリティー**」をクリックします。
   b. 「**セキュリティー**」セクションまでスクロールダウンします。
   c. 「**証明書の表示**」をクリックして、「証明書マネージャー」ダイアログを表示します。
   d. 「**証明書**」タブをクリックします。
   e. 「**インポート**」をクリックし、証明書をダウンロードした場所を参照します。
   f. 証明書を選択し、「**開く**」をクリックします。
   g. 「証明書マネージャー」ダイアログを閉じます。

XClarity Orchestrator への エッジ・クライアント・デバイス用 XClarity Management Hub の接続

Lenovo XClarity Management Hub を Lenovo XClarity Orchestratorに登録 (接続) すると、デバイスの管理と監視を開始できます。

始める前に

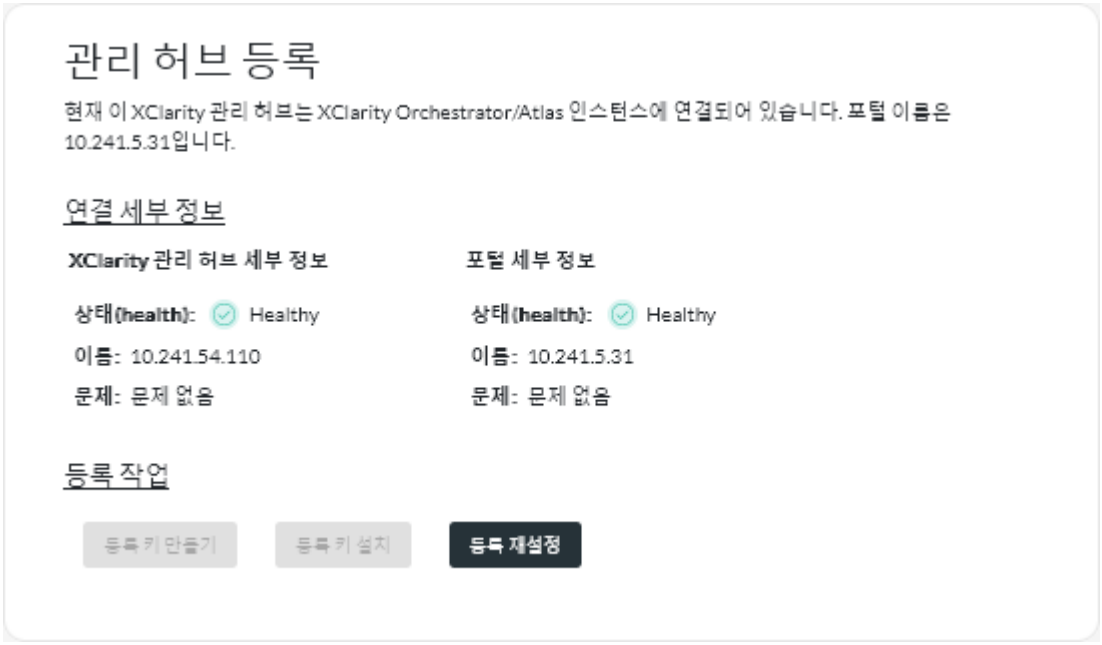
XClarity Management Hubに XClarity Orchestrator から到達できることと、ネットワーク上の XClarity Orchestrator に XClarity Management Hub から到達できることを確認します。

手順

XClarity Management Hub を登録するには、次の手順を実行します。

ステップ 1. 管理ハブの登録キーを作成します。

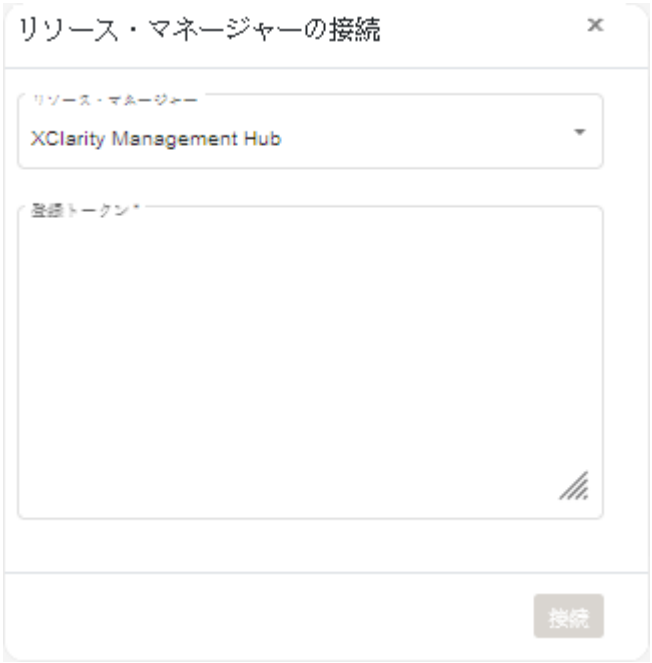
1. Management Hub メニュー・バーで、「**登録**」をクリックして、「登録」ページを表示します。



2. 「**登録キーの作成**」をクリックします。
3. 「**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てから、ダイアログを閉じます。

ステップ 2. 管理ハブの登録キーを XClarity Orchestrator に追加します。

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。
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。



3. **XClarity Management Hub** をリソース・マネージャーとして選択します。
4. 「**登録トークン**」フィールドに登録キーをコピーします。
5. 「**接続**」をクリックして、XClarity Orchestrator 登録キーを含む「リソース・マネージャーの接続」ダイアログを表示します。
6. 「**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てから、ダイアログを閉じます。

ステップ 3. XClarity Orchestrator 登録キーを管理ハブに追加します。

1. Management Hub メニュー・バーで、「**登録**」をクリックして、「登録」ページを表示します。
2. 「**登録キーのインストール**」クリックします。
3. 「**登録トークン**」フィールドに登録キーをコピーします。
4. 「**接続**」をクリックします。

終了後

- 管理ハブを使用してデバイスを管理します (ThinkEdge クライアント・デバイスの管理 XClarity Orchestrator オンライン・ドキュメントを参照)。
- 「**登録のリセット**」をクリックして、現在の管理ハブの登録キーを削除します。

第 3 章　エッジ・クライアント・デバイス用 XClarity Management Hub のアンインストール

XClarity Management Hub 仮想アプライアンスまたはコンテナー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 Management Hub 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. XClarity Management Hub によって現在管理されているすべてのデバイスを管理解除します。

ステップ 2. オペレーティング・システムによっては、XClarity Management Hub をアンインストールします。

- 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。