Lenovo

Lenovo XClarity Orchestrator

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

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をサポートしています。

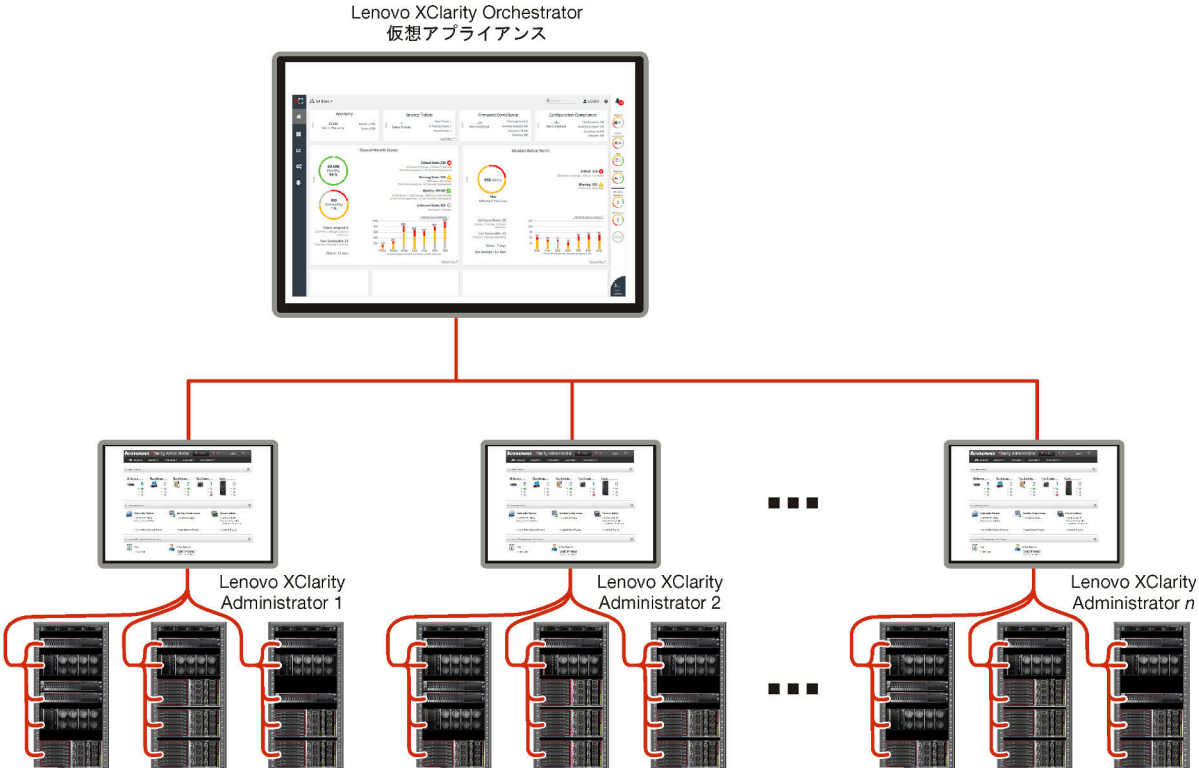
修正に関する情報については、更新パッケージ内に提供される変更履歴ファイル (*.chg) を参照してください。

このバージョンは、管理ソフトウェアに対する以下の機能拡張をサポートします。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
管理	ユーザー・インターフェースから Orchestrator サーバーを再起動できます (XClarity Orchestratorの再起動を参照)。
リソースの管理	Lenovo XClarity Management Hub 2.0 は、Lenovo ThinkSystem および ThinkEdge サーバーの管理に使用できる新しいライトウェイト・デバイス・マネージャーです (リソース・マネージャーの接続を参照)。 一括管理オプションを使用して、多数のサーバーを管理できます (サーバーの管理を参照)。 完全修飾ドメイン名を使用してサーバーを管理できます (サーバーの管理を参照)。
リソースおよびアクティビティの監視	メモリー・インベントリー・データが表形式で表示されます (デバイスの詳細の表示を参照)。 すべてのスケジュール・ジョブのリストを表示できます (ジョブの監視を参照)。
リソースのプロビジョニング	特定の日時に実行するファームウェア更新をスケジュールできます (管理対象サーバーへの更新の適用とアクティブ化を参照)。

第 1 章　Lenovo XClarity Orchestrator 概要

Lenovo XClarity Orchestrator は、多数のデバイスが含まれる環境の監視、管理、プロビジョニング、および分析を一元化します。また、既存の リソース・マネージャー (Lenovo XClarity Administrator、Schneider Electric EcoStruxure IT Expert など) を複数のサイトで活用して、全体のヘルスを表示したり、デバイス・インベントリーとヘルス・サマリーを収集したり、デバイスの詳細にドリル・ダウンしたり、イベント・ログと監査ログを表示したり、管理対象リソースに更新を適用したりできます。



詳細:

- XClarity Orchestrator の概要
- 管理機能

リソースの監視と管理の一元化

XClarity Orchestrator は、リソース・マネージャーと、それらのリソース・マネージャーで管理されるデバイスを監視および管理するための 1 つのインターフェースを提供します。

- リソース・マネージャー、デバイス、インフラストラクチャー・リソース (PDU や UPS など) を含む管理対象リソースの正常性に関する要約ビュー
- 複数のサイトにわたるコンポーネントの正常性、資産インベントリー、保証状況、およびデバイスに関するアドバイザリーの要約と詳細ビュー
- クリティカルなアラートとイベントの集約、カスタム・アラートの作成、および外部アプリケーションへのイベントの転送
- 管理対象デバイスのライフサイクル制御 (電源操作を含む)
- デバイス・サマリー・ページからの、リソース・マネージャーおよび管理対象デバイス用ユーザー・インターフェースのコンテキスト起動

更新のプロビジョニング

XClarity Orchestrator を使用して、管理対象リソースの現在のソフトウェア・レベルを維持することができます。更新カタログを使用して、使用可能なソフトウェア・レベルを確認し、更新コンプライアンス・ポリシーを使用して、カスタム条件に基づいて更新する必要のあるリソースを特定し、それらのリソースに必要な更新をデプロイすることができます。XClarity Orchestrator は、ターゲット・リソースが正しい順序で更新されていることを確認します。

XClarity Orchestrator は、以下のプロビジョニング操作をサポートしています。

- Lenovo XClarity Administrator リソース・マネージャーへの更新のデプロイ。
- XClarity Administrator によって管理されているデバイスへのファームウェア更新のデプロイ。

更新のプロビジョニングについて詳しくは、管理対象リソースへの更新のプロビジョニングを参照してください。

サーバー構成のプロビジョニング

一貫した構成を使用して、管理対象サーバーをすばやくプロビジョニングできます。構成設定 (ベースボード管理コントローラーや UEFI の設定など) は、複数のサーバーに適用できるパターンとして保存されます。

XClarity Orchestrator では、管理対象サーバーに構成パターンは直接デプロイされません。代わりに、適切なリソース・マネージャーに要求を送信して、デプロイメントを実行するジョブを開始してから、要求の進行状況を追跡します。

サーバー構成のプロビジョニングについて詳しくは、サーバー構成のプロビジョニングを参照してください。

オペレーティング・システムのプロビジョニング

XClarity Orchestrator を使用して、オペレーティング・システム・イメージ を複数のサーバーにデプロイできます。

XClarity Orchestrator では、管理対象サーバーにオペレーティング・システムは直接デプロイされません。代わりに、適切な XClarity Administrator リソース・マネージャーに要求を送信して、更新を実行するジョブを開始してから、要求の進行状況を追跡します。

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。

サーバー構成のプロビジョニングについて詳しくは、オペレーティング・システムのプロビジョニングを参照してください。

ビジネス・インテリジェンスの機械学習と予測分析

XClarity Orchestrator は、ビジネス・インテリジェンスの機械学習および予測分析を行うサード・パーティーのサービス (Splunk など) に接続して、以下のことを実行できます。

- トレンド・データ (プロセッサーとメモリーの使用状況、電力の消費量、温度、不正アクセス、繰り返しイベントと紛失イベント、およびファームウェア更新やシステム再起動などのプロセス間の平均時間など) を収集および表示する。
- メトリック・データを使用して、障害を予測します (イベントの繰り返しや正常性レポートなど)
- アラート、イベント、デバイス・インベントリー、およびデバイス・メトリックなどの既存のデータに基づいて、カスタム分析レポートを作成します。
- 環境に特定の条件が存在し、それが有効な場合にアラートを生成する、カスタム・アラート・ルールを定義します。

詳細: 分析および予測機能

予測分析について詳しくは、傾向の分析と問題の予測 参照してください。

サービスおよびサポート

一定の保守可能イベントが管理対象デバイスで発生した場合に、コール・ホームを使用して診断ファイルを自動的に収集し、Lenovo サポートに送信するように XClarity Orchestrator を設定できます。また、手動で診断ファイルを収集したり、問題レコードを開いたり、診断ファイルを Lenovo サポート・センターに送信したりすることもできます。

サービスおよびサポートについて詳しくは、サービスおよびサポートの操作 を参照してください。

資料

オンライン・ドキュメントは定期的に英語で更新されます。最新の情報と手順については、XClarity Orchestrator のオンライン・ドキュメント を参照してください。

オンライン・ドキュメントは、次の言語で入手できます。
- 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)

次の方法でオンライン・ドキュメントの言語を変更できます。

- たとえば、オンライン・ドキュメントを簡体字中国語で表示するには、*<language_code>* を `https://pubs.lenovo.com/lxco/` の後に追加します。
  `https://pubs.lenovo.com/lxco/zh-CN/`

XClarity Orchestrator へのログイン

XClarity Orchestrator 仮想アプライアンスにネットワーク接続されているシステムから、Lenovo XClarity Orchestrator Web インターフェースにログインします。

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 XClarity Orchestrator オンライン・ドキュメント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。

LDAP ユーザー・アカウントを使用する場合は、ユーザー名または username@domain を使用してログインできます (たとえば、`user1@company.com`)。

XClarity Orchestrator では、活動に関係なく、一定時間にわたり非アクティブなユーザー・セッション、および一定時間にわたり開いているユーザー・セッションを自動的にログアウトします。以下のデフォルト値は、XClarity Orchestrator によって設定されます。

- *30 分間*ユーザー・インターフェースでクリックまたは入力を行っていない場合、ユーザー・セッションは読み取り専用操作に制限されます。データを変更しようとすると、ユーザー・セッションは自動的にログアウトされます。
- *1440 分間* (24 時間) データをアクティブに表示していない場合、ユーザー・セッションは自動的にログアウトされます。
- *24 時間*後、ユーザー・セッションは、ユーザー・アクティビティーに関係なく自動的にログアウトされます。

手順

XClarity Orchestrator Web インターフェースにログインするには、以下の手順を実行してください。

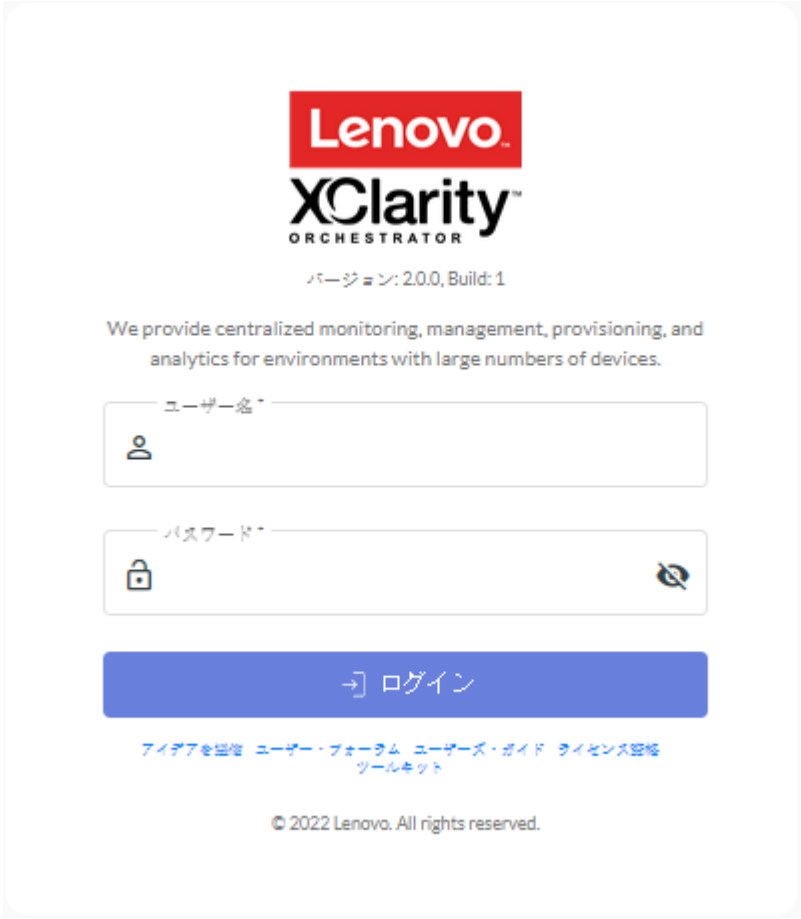
1. ブラウザーで XClarity Orchestrator 仮想アプライアンスの IP アドレスを指定します。

   - **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. 有効なユーザー ID とパスワードを入力し、「**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

XClarity Orchestrator のダッシュボードが開いて、ご使用の環境でのリソースのヘルスとアクティビティの要約が表示されます。

XClarity Orchestrator 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。

- 現在のユーザーのパスワードを変更するには、「**パスワードの変更**」をクリックします。
- 「**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 Orchestrator ログイン・ページが表示されます。

  ログイン・ページから、「**ライセンス資格**」リンクをクリックしてFeatures on Demand Web ポータルを開くことができます。ここでは、ご使用の Lenovo 製品のライセンスをすべて検索して管理することができます。
- 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。
- 「**ツールキット**」をクリックして、XClarity Orchestrator PowerShell (LXCOPSTool) ツールキットをダウンロードします。LXCOPSTool ツールキットは、Microsoft PowerShell セッションからのプロビジョニングとリソース管理を自動化するコマンドレット・ライブラリーを提供します。
- XClarity Orchestrator の使用方法に関する情報は、「**ヘルプ**」をクリックして組み込みのヘルプ・システムで参照できます。

  オンライン・ドキュメントは定期的に英語で更新されます。最新の情報と手順については、XClarity Orchestrator のオンライン・ドキュメント を参照してください。
- 「**バージョン情報**」をクリックして、XClarity Orchestrator のリリースに関する情報を表示できます。

  「バージョン情報」ダイアログには、「**使用許諾契約書**」、「**オープン・ソース・ライセンス**」、および「**Lenovo のプライバシーに関する声明**」を表示するリンクがあります。
- 「**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)

ユーザー・インターフェースのヒントと手法

Lenovo XClarity Orchestrator および Lenovo XClarity Management Hub のユーザー・インターフェースを使用する場合は、以下のヒントと手法を参照してください。

ファイルのインポート中

ファイルをインポートするには、「インポート」ダイアログにファイルをドラッグ・アンド・ドロップします。

ファイルをインポートすると、各インポート・プロセスの進行状況とステータスに関する情報が、ユーザー・インターフェースの右下隅に展開可能なポップアップで表示されます。ポップアップ上のアイコンにより、各インポートのプロセス・ステータスをすばやく識別できます。インポートが正常に完了すると、ファイルを検証するジョブが開始されます。インポート・プロセス中にエラーが発生した場合は、問題を迅速に解決するのに役立つエラー・メッセージがポップアップ・ダイアログにリストされます。

ポップアップが折りたたまれているときは、「**ドラッグ**」アイコン ( ) をクリックしたままポップアップを別の位置に移動できます。

完了したインポート・プロセスのリストをクリアするには、「**すべてをクリア**」をクリックします。すべてのインポート・プロセスが完了すると、ポップアップは非表示になります。

テキスト・フィールドへのテキストの入力

一部のテキスト・フィールドに入力できる文字が制限されています。次のリストは、許可される文字を示しています。

- **名前**。サポートされている言語のすべての文字と数字、および特殊文字 @ - _ + / [ ] . , : およびスペースが含まれます。
- **説明**。サポートされている言語のすべての文字と数字、および特殊文字 @ - _ % & * + = / ( ) { } [ ] . , : およびスペースが含まれます。
- **パスワード**。ローカル・ユーザー・アカウントの場合、パスワードはデフォルトで **8 ～ 256** 文字にすることができますが、16 文字以上が推奨されます。パスワードに文字の制限はありません。ただし、パスワードには特定のタイプの文字が必要であり、セキュリティーのためにいくつかのシーケンスを制限します。
  - 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)。

ナビゲーション・ペインの展開と折りたたみ

ナビゲーション・ペインはデフォルトでは折りたたまれ、特定のメニュー項目を表すアイコンのみ表示されています。アイコンをクリックすると、そのアイコンのナビゲーション・ペインとメニューが一時的に展開表示されます。ナビゲーション・ペインからカーソルを移動すると、ペインは折りたたまれ、アイコンのみが表示されます。

ナビゲーション・ペインを永続的に展開しておくには、「**展開**」アイコン (⊕) をクリックします。ナビゲーション・ペインを折りたたむには、「**折りたたみ**」アイコン (⊗) をクリックします。

ユーザー・インターフェースのスコープ決定

デフォルトでは、XClarity Orchestrator は*すべてのリソース*のデータを表示します。ページの上部にある「**現在のスコープ**」ドロップダウン・メニューで、現在のユーザー・セッションで表示されるデータのスコープを特定のリソース・マネージャーとグループにあるリソースのみに絞り込むことができます。ドロップダウン・メニューから、現在のスコープに含まれるリソース・マネージャーとグループのリストを「**マイ・スコープ・リスト**」に表示したり、「**スコープの変更**」をクリックして、複数のリソース・マネージャーとグループを含むカスタムのスコープを作成するダイアログを表示したり、「**すべてのリソース**」を選択して、すべてのリソースを表示するようにスコープを変更したりすることができます。

選択したスコープは、現在のユーザー・セッション内でのみ維持されます。複数のユーザー・セッションを開き、それぞれ異なるビューのダッシュボードやリソース、イベント、アラート・データを開くことができます。

注：VMware vRealize オペレーション・マネージャー リソース・マネージャーは、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。

ページごとに表示するデータの量の増減

1 ページのテーブルに表示される行数は、各テーブルの下部にある「**ページに表示される行数**」ドロップダウン・リストで変更できます。10、15、25、または 50 の行数で表示できます。

大きなリストのデータの検索

特定の基準に基づいて大きなリストのサブセットを表示するには、いくつかの方法があります。

- 列見出しをクリックすると、テーブルの行をソートできます。
- ページの上部にある「**現在のスコープ**」ドロップダウン・メニューで、現在のユーザー・セッションで表示されるデータのスコープを特定のリソース・マネージャーまたはグループにあるリソースのみに絞り込めます (上記の「ユーザー・インターフェースのスコープ決定」を参照)。
- 「**フィルター**」入力フィールドを使用することで、特定の列で検出されたデータに基づいてリストのサブセットを動的に作成することができます。表示されている列と非表示の列に対してフィルタリングできます。定期的に使用するフィルター・クエリを保存することもできます。
- このサブセットをさらに絞り込むには、「**検索**」フィールドにテキスト (名前や IP アドレスなど) を入力して、使用可能な任意の列にあるデータを検索します。

  ヒント: 複数の検索はコンマで区切ります。たとえば、「180,190」と入力すると、表示可能なすべての列のうち 180 または 190 を含むすべての行が表示されます。
- テーブルにリストされているすべての項目を選択またはクリアするには、テーブル・ヘッダーのチェックボックスを選択します。

テーブル・データの表示

「**最新表示**」アイコン (⟳) をクリックすると、データ・テーブルが更新されます。

各行を展開または縮小して、展開可能な行 (ジョブやリポジトリー管理カードなど) を含むテーブルのサブ詳細を表示または非表示にします。「**すべて縮小表示**」アイコン (≡) をクリックしてすべての行のサブ詳細を非表示にすることもできます。

列のサイズによって、一部の情報がテーブル・セルに表示されない (省略記号で示される) 場合は、セル内にマウス・ポインターを置くと、完全な情報がポップアップで表示されます。

テーブル・データのエクスポート

現在のテーブルのデータをローカル・システムにエクスポートするには、「**データをエクスポート**」アイコン (⊟) をクリックします。すべてのページ、現在のページ、または選択した行をエクスポートすることにして、ファイル形式 (XLSX、CSV、または JSON) を選択し、すべての列を含めるか、または表示可能な列のみを含めるかを選択できます。CSV 形式の場合は、データを区切る方法 (セミコロン、タブ、またはパイプ文字) を選択することもできます。

ヒント: JSON 形式の場合、エクスポートされたデータのタイムスタンプは、ローカル・システムではなく、XClarity Orchestrator に設定されているタイム・ゾーンを反映します。CSV 形式と XLSX 形式の場合、タイムスタンプはユーザーのタイム・ゾーンに変換され、Web インターフェースに表示されます。

データをエクスポートすると、進行状況とステータスに関する情報が、ユーザー・インターフェースの右下隅に展開可能なポップアップで表示されます。ポップアップ上のアイコンにより、各エクスポートのプロセスのステータスをすばやく識別できます。エクスポート・プロセス中にエラーが発生した場合は、問題を迅速に解決するのに役立つエラー・メッセージがポップアップ・ダイアログにリストされます。

ポップアップが折りたたまれているときは、「**ドラッグ**」アイコン (⋮⋮) をクリックしたままポップアップを別の位置に移動できます。

完了したエクスポート・プロセスのリストをクリアするには、「**すべてをクリア**」をクリックします。すべてのエクスポート・プロセスが完了すると、ポップアップは非表示になります。

テーブルの列の構成

テーブルを構成して、最も重要な情報を表示することができます。

- 「**すべての操作**」 ➔ 「**列の切り替え**」の順にクリックして、表示または非表示にする列を選択できます。
- 列の順序を変更するには、列見出しを希望の場所にドラッグします。

ユーザー・インターフェースの言語の変更

ログイン後、ユーザー・インターフェースの言語を変更できます。

ログイン後にユーザー・インターフェースの言語を変更する場合は、「**ユーザー・アカウント**」メニュー (⚙) をクリックし、「**言語の変更**」をクリックします。

注：ヘルプ・システムは、ユーザー・インターフェースに選択されているのと同じ言語で表示されます。

ヘルプの入手

複数の方法でユーザー・インターフェースに関するヘルプを取得できます。

- 一部のページでは、「**ヘルプ**」アイコン(?) にカーソルを合わせると、特定のフィールドに関する詳細がポップアップに表示されます。
- 一部のページで「**詳細**」をクリックすると、ヘルプ・システムが開き、コンテキストに関するより詳細な情報が表示されます。
- ユーザー・インターフェースから特定の操作を実行する方法に関するヘルプを表示するには、「**ユーザー・アカウント**」メニュー (⚙) をクリックし、「**ヘルプ**」をクリックします。オンライン・ドキュメントは定期的に英語で更新されます。最新の情報と手順については、XClarity Orchestrator のオンライン・ドキュメント を参照してください。

第 2 章　XClarity Orchestrator の管理

「日付と時刻」および「ネットワーク・アクセス」、「リソース・マネージャーの接続」、「認証サーバーとユーザー・アクセスの管理」、「セキュリティー証明書の管理」など、各種の管理操作を実行できます。

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

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 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、XClarity Management Hub 2.0 の XClarity Orchestrator への接続 XClarity Orchestrator オンライン・ドキュメント を参照してください。
- **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、XClarity Management Hub の XClarity Orchestrator への接続 XClarity Orchestrator オンライン・ドキュメント を参照してください。
- **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。

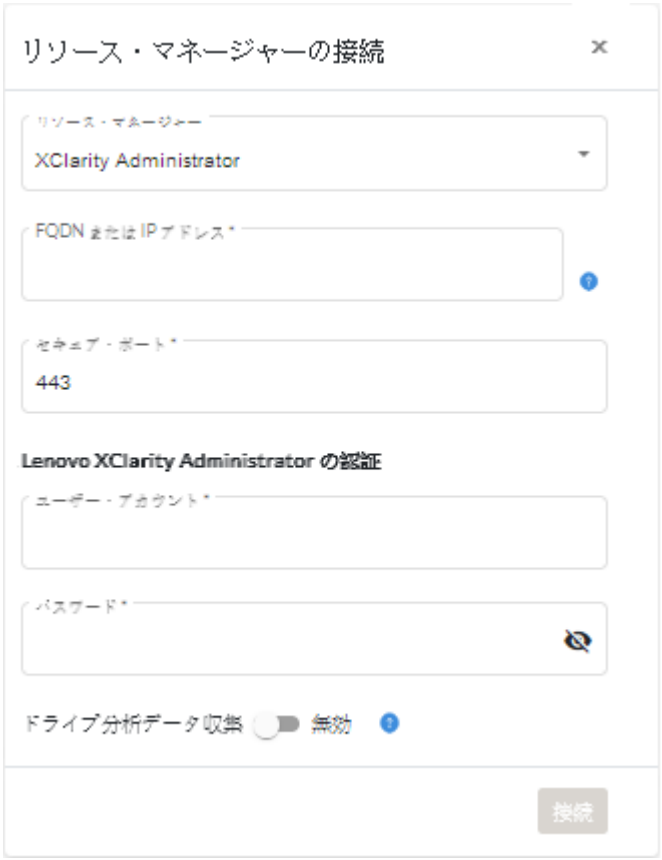
指定したネットワーク・アドレス (IP アドレスまたはホスト名) はマネージャー名として使用されます。

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

「リソース・マネージャー」カードから、以下の操作を実行できます。

- 「**ヘルス状況**」列からリソース・マネージャーの接続ステータスを確認する。
- 選択済みリソース・マネージャーの資格情報とプロパティを変更するには、「**編集**」アイコン ( ) 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)。
- 「**編集**」アイコン ( ) をクリックして、選択した XClarity Administrator リソース・マネージャーのドライブ分析データ収集を有効または無効にします。

  注：「**ドライブ分析データ収集**」のトグルは、XClarity Administrator の接続または資格情報に問題がある場合、無効になります (リソース・マネージャーへの接続が突然失われる XClarity Orchestrator オンライン・ドキュメント を参照)。
- 選択済みリソース・マネージャーを切断して削除するには、「**削除**」アイコン ( ) をクリックします。

  注：XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**強制切断**」を選択します。

  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・マネージャーを削除すると、そのリソース・マネージャーが管理しているデバイスもすべて削除されます。これには、デバイス・インベントリー、ログ、メトリック・データ、および分析レポートが含まれます。
- リソース・マネージャーを接続するときに発生する問題をトラブルシューティングします (リソース・マネージャーに接続できない XClarity Orchestrator オンライン・ドキュメント を参照)。

デバイスの検出と管理

Lenovo XClarity Orchestrator を使用してデバイスを検出および管理し、それらのデバイスの管理を特定のリソース・マネージャーに割り当てることができます。

始める前に

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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、リソース・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。リソース・マネージャーを接続する場合は、XClarity Orchestrator ではそのリソース・マネージャーによって管理されるすべてのデバイスを管理します。

XClarity Orchestrator を使用してデバイスを管理下に置くこともできます。XClarity Orchestrator では、リソース・マネージャーによってすでに検出された (が管理されていない) デバイスの一覧が作成されます。XClarity Orchestrator から検出されたデバイスを管理する場合、そのデバイスは検出したリソース・マネージャーによって管理されます。IP アドレス、ホスト名、またはサブネットを使用してデバイスの手動での検出と管理を行う場合、デバイスの管理に使用するリソース・マネージャーを選択します。XClarity Management Hub を使用して ThinkEdge クライアント・デバイスを管理できます。XClarity Management Hub 2.0 を使用して ThinkServer デバイスを管理できます。Lenovo XClarity Administrator を使用してサーバー、ストレージ、スイッチ、およびシャーシを管理できます。

注：

- XClarity Management Hub 2.0 を通じてデバイスを管理しようとして、そのデバイスが既に別の XClarity Management Hub 2.0 で管理されている場合、XClarity Orchestrator は、以前の管理の確認を行わずに管理ユーザー・アカウントとサブスクリプションをデバイスから削除し、新しい管理ハブを通じてデバイスを再度管理します。このプロセスの完了後、デバイスは以前の管理ハブによる管理対象のままオフライン状態ですが、デバイスはその管理ハブにデータを送信しなくなりました。接続されているポータルを通じて最初の管理ハブからデバイスを手動で管理解除する必要があることに注意してください。
- XClarity Management Hub 2.0 を通じてデバイスを管理しようとして、そのデバイスが既に別の XClarity Administrator で管理されている場合、XClarity Orchestrator は、XClarity Administrator の確認を行わずに XClarity Administrator によって XCC に登録されている管理ユーザー・アカウント、サブスクリプション、LDAP および SSO 情報をデバイスから削除し、新しい XClarity Management Hub 2.0 を通じてデバイスを再度管理します。このプロセスの完了後、デバイスは XClarity Administrator ハブによる管理対象のままオフライン状態ですが、デバイスはその管理ハブにデータを送信しなくなりました。接続されているポータルを通じて XClarity Administrator からデバイスを手動で管理解除する必要があることに注意してください。

以下のデバイスは、リソース・マネージャーによってサービス検出プロトコルを使用して自動的に検出できます。
- ThinkSystem サーバー、ThinkAgile サーバー、およびアプライアンス
- ThinkEdge SE サーバー
- Flex System シャーシ、Flex System シャーシ内の ThinkSystem デバイスおよび Flex System デバイス
- ThinkServer ラック・サーバーとタワー・サーバー
- System x、Converged HX、NeXtScale サーバー、およびアプライアンス
- ストレージ・デバイス

以下のデバイスは、リソース・マネージャーによってサービス検出プロトコルを使用して自動的に検出することが *できません*。これらのデバイスがセキュアに検出および管理される前に、UDC エージェントをインストールする必要があります。
- ThinkCentre クライアント
- ThinkEdge クライアント

現在のところ、XClarity Orchestrator からスイッチを管理対象にすることはできません。XClarity Orchestrator から Flex System スイッチを管理対象から除外することもできません。

デバイスの管理に関する考慮事項

XClarity Orchestrator を使用してデバイスの検索と管理を行う前に、以下の考慮事項を確認してください。
- 一般的な考慮事項
- サーバーに関する考慮事項
- ストレージに関する考慮事項

- スイッチに関する考慮事項
- シャーシに関する考慮事項
- 複数の管理ツールに関する考慮事項

一般的な考慮事項

管理するデバイスが XClarity Orchestrator でサポートされていることを確認します。

管理する各システムに、最小限必要なファームウェアがインストールされていることを確認します。

特定のポートがデバイスとの通信に使用できる必要があります。サーバーを管理する前に、必要なポートがすべて使用可能になっていることを確認します。

サービス検出プロトコルを使用して、XClarity Orchestrator では、XClarity Orchestrator と同じ IP サブネットにある管理可能デバイスのプローブによって、環境内のデバイスを自動的に検出できます。他のサブネットにあるデバイスを検出するには、IP アドレス、ホスト名、IP アドレス範囲、またはサブネットを手動で指定できます。

デバイスが XClarity Orchestrator の管理対象になった後、XClarity Orchestrator は各管理対象ストレージ・デバイスを定期的にポーリングして、インベントリー、重要プロダクト・データ、ステータスなどの情報を収集します。

XClarity Orchestrator で、管理プロセスのインベントリーの収集時にデバイスとの通信が失われた場合 (例: 電源の喪失、ネットワーク障害の発生、スイッチがオフラインなどの理由により)、管理は正常に完了します。ただし、一部のインベントリー情報の収集が完了していない可能性があります。デバイスがオンラインになり XClarity Orchestrator によってインベントリーについてデバイスがポーリングされるのを待つか、またはデバイスを選択して、「**すべての操作 ➞ インベントリー ➞ インベントリーを最新の情報に更新**」を選択することでデバイス・マネージャー Web インターフェースから手動でデバイスのインベントリーを収集します。

デバイスを管理できるリソース・マネージャー (XClarity Orchestrator、XClarity Management Hub 2.0、XClarity Management Hub、または XClarity Administrator) は一度に 1 つのみです。デバイスが 1 つのリソース・マネージャーの管理対象になっており、そのデバイスを別のリソース・マネージャーを使用して管理にする場合は、まず元のリソース・マネージャーで管理対象から除外する必要があります。

デバイスが XClarity Orchestrator によって管理された後にデバイスの IP アドレスを変更する場合、は新しい IP アドレスを認識し、デバイスの管理を続けます。ただし、XClarity Orchestrator は一部のサーバーの IP アドレスの変更を認識しません。IP アドレスを変更した後、XClarity Orchestrator でサーバーがオフラインであると表示される場合は、「**管理の強制**」オプションを使用してサーバーを再度管理します。

デバイス内のアダプターの取り外し、交換、または構成を行った場合は、デバイスを少なくとも 1 回再起動してインベントリー情報を更新します。

リソース・マネージャーから*別の*サブネットにあるデバイスを検出するには、以下のいずれかの条件を満たしていることを確認してください。

- マルチキャスト SLP 転送が環境内のラック・スイッチとルーターで有効になっていることを確認します。マルチキャスト SLP 転送が有効になっているかどうかを調べる方法や、無効になっている場合に有効にする方法については、そのスイッチやルーターに付属のドキュメントを参照してください。
- SLP がデバイスまたはネットワークで無効の場合、DNS 検出メソッドを代わりに使用できます。これを行うには、手動でサービス・レコード (SRV レコード) をドメイン・ネーム・サーバー (DNS) に追加します。例:
  ```
  lxco.company.com  service = 0 0 443 server1.company.com
  ```
  次に、「**BMC 構成 ➞ ネットワーク**」をクリックし、「DNS」タブをクリックして、管理 Web インターフェースからベースボード管理コンソールで DNS 検出を有効にします。

Encapsulation の考慮事項

デバイス管理プロセス中、シャーシおよびサーバーで encapsulation の有効化を選択できます。共通 encapsulation の設定が有効にされ、デバイスが encapsulation をサポートする場合、リソース・マネージャーは管理プロセス中にデバイスと通信し、デバイスの encapsulation モードを **encapsulationLite** に変更し、受信要求をリソース・マネージャーからのみに制限するためデバイスのファイアウォール規則を変更します。

注：動的ホスト構成プロトコル (DHCP) を使用するように管理ネットワーク・インターフェースを構成し、encapsulation を有効にしてデバイスを管理すると時間がかかることがあります。

共通 encapsulation 設定はデフォルトでは無効になっています。無効にされた場合、デバイスの encapsulation モードは**通常**に設定され、デバイス管理プロセス中にファイアウォール規則が変更されません。

注意：管理対象デバイスで encapsulation モードが **encapsulationLite** である場合、以下の状況により、リソース・マネージャーおよび管理対象デバイス間の通信と認証に問題が発生し、管理対象デバイスに到達できなくなる可能性があります。デバイスは、他の送信元からの TCP 要求を無視するよう構成されているため、ネットワーク・インターフェースを介してそれらのデバイスにアクセスすることができません。ほとんどの場合、それらのデバイスは ping、SSH、または TELNET 要求に応答しません。

- リソース・マネージャーが実行されているハイパーバイザーにおけるネットワークの変更
- 仮想ローカル・エリア・ネットワーク (VLAN) または VLAN タグの変更
- encapsulation が有効になっているときのデバイス IP アドレスの永続的な変更
- encapsulation が有効になっているときのデバイスの管理対象から強制的な除外
- リソース・マネージャーの仮想マシンの喪失
- 仮想マシンと管理対象デバイス間の TCP 通信の喪失
- encapsulation が有効になっているときの、リソース・マネージャーが管理対象デバイスと直接通信できなくなる他のネットワークの問題

永続的な問題が発生した場合、以下のいずれかの操作を実行し、以前管理対象であったデバイスへのアクセスを回復します。詳しくは、XClarity Administrator オンライン・ドキュメント「Encapsulation の管理」、「管理サーバーの障害発生後の CMM による管理のリカバリー」、「管理サーバーの障害発生後の CMM による管理のリカバリー」を参照してください。

- encapsulation モードが有効な管理対象 IMM へのアクセスを回復するには、UEFI グラフィカル・ユーザー・インターフェースを通じてローカル・コンソールからデフォルト設定をロードする必要があります。
- USB - Ethernet ブリッジを使用して管理コントローラーへのインバンド・アクセスを取得し、コマンド
  `encaps lite -off`
  を実行します。
- encapsulation モードが有効な管理対象 CMM へのアクセスを回復するには、背面のリセット・ボタンを使用するか、コマンド
  `accesscontrol -off -T mm[p]`
  を実行して (コンソールにまだアクセスできる場合) デフォルト設定をロードする必要があります。

サーバーに関する考慮事項

デバイスで CIM over HTTPS が有効になっていることを確認します。`RECOVERY_ID` ユーザー・アカウントを使用して、サーバーの管理 Web インターフェースにログインします。「**BMC 構成**」 → 「**セキュリティー**」をクリックしてから、「**CIM Over HTTPS**」タブをクリックし、「**CIM Over HTTPS を有効に設定**」が選択されていることを確認します。

サーバーの管理操作を実行する際は、サーバーの電源がオフになっているのか、BIOS/UEFI セットアップを起動しているのか、またはオペレーティング・システムを実行しているのかを確認します (管理対象サーバーでの電源操作の実行 を参照)。サーバーの電源がオンになっているがオペレーティング・システムがない場合、オペレーティング・システムを検出するために管理コントローラーによってサーバーのリセットが繰り返されます。

UEFI_Ethernet_* と UEFI_Slot_* の設定がすべてサーバーの UEFI 設定で有効になっていることを確認します。設定を確認するには、サーバーを再起動し、プロンプト <F1> Setup が表示されたら、**F1** を押して

Setup Utility を起動します。「**システム設定 → デバイスおよび I/O ポート → アダプター・オプション ROM のサポートの有効/無効**」に移動し、「**UEFI オプション ROM の有効化/無効化**」セクションを見つけて設定が有効であることを確認します。サポートされている場合、ベースボード管理インターフェースでリモート・コンソール機能を使用して設定をリモートで確認および変更することもできます。

デバイスのサーバー証明書が外部証明機関によって署名されている場合は、証明機関証明書および任意の中間証明書が XClarity Orchestrator 信頼ストアにインポートされていることを確認します (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 を参照)。

ThinkEdge クライアント・デバイス
ThinkEdge クライアント・デバイスには、ベースボード管理コントローラーを搭載していないため、サービス検出プロトコルを使用した検出ができません。割り当てられた Lenovo XClarity Management Hub リソース・マネージャーによってデバイスが安全に検出および管理される前に、ThinkEdge クライアント・デバイスに UDC エージェントをインストールする必要があります。詳しくは、ThinkEdge クライアント・デバイスの管理を参照してください。

ThinkSystem SR635 および SR655 サーバー
オペレーティング・システムがインストールされていること、およびサーバーが OS、マウントされたブート可能メディア、または efishell に少なくとも 1 回はブートされていることを確認して、XClarity Orchestrator がそれらのサーバーのインベントリーを収集できるようにします。

IPMI over LAN が使用可能であることを確認します。「IPMI over LAN」は、これらのサーバーではデフォルトで無効であり、サーバーを管理するには手動で有効にする必要があります。ThinkSystem System Manager Web インターフェースから IPMI over LAN を有効にするには、「**設定**」 → 「**IPMI 構成**」をクリックします。変更をアクティブにするには、サーバーの再起動が必要になることがあります。

ThinkServer サーバー
サーバーのホスト名は、有効なホスト名または IP アドレスを使用してこれらのサーバーを自動的に検出するように構成される必要があります。

ネットワーク構成では、XClarity Orchestrator とサーバー間の SLP トラフィックを許可する必要があります。

ユニキャスト SLP が必要です。

自動的に ThinkServer サーバーを検出するには、マルチキャスト SLP が必要です。さらに、ThinkServer System Manager (TSM) で SLP を有効にする必要があります。

ThinkServer サーバーが、XClarity Orchestrator と別のネットワーク上に存在する場合、XClarity Orchestrator がそのデバイスのイベントを受信できるように、ポート 162 を介してインバウンド UDP を許可するようにそのネットワークを構成する必要があります。

System x3950 X6 サーバー
これらのサーバーは、それぞれ独自のベースボード管理コントローラーを持つ 2 つの 4U エンクロージャーとして管理する必要があります。

サーバーの管理について詳しくは、サーバーの管理 および ThinkEdge クライアント・デバイスの管理 を参照してください。

ストレージに関する考慮事項

ラック・ストレージ・デバイスを検出および管理する前に、以下の要件を満たしていることを確認してください (ThinkSystem DE シリーズ以外)。

- ネットワーク構成では、リソース・マネージャーとラック・ストレージ・デバイス間の SLP トラフィックを許可する必要があります。

- ユニキャスト SLP が必要です。
- XClarity Orchestrator が自動的に Lenovo Storage デバイスを検出するには、マルチキャスト SLP が必要です。さらに、ラック・ストレージ・デバイスで SLP を有効にする必要があります。

ストレージ・デバイスの管理について詳しくは、ストレージ・デバイスの管理 を参照してください。

スイッチに関する考慮事項

XClarity Orchestrator を使用したスイッチの管理は、現在サポートされていません。

シャーシに関する考慮事項

シャーシの管理を実行すると、そのシャーシのすべてのドライブも管理されます。シャーシとは別にシャシー内のコンポーネントの検索と管理を行うことはできません。

シャーシで、CMM の「LDAP ユーザーについての同時アクティブ・セッションの数」設定が 0 (ゼロ) に設定されていることを確認します。この設定は、CMM Web インターフェースで「**BMC 構成**」➡「**ユーザー・アカウント**」をクリックし、「**グローバル・ログイン設定**」をクリックして「**全般**」タブをクリックすることにより確認できます。

CMM とのアウト・オブ・バンド通信に使用する TCP コマンド・モード・セッションが少なくとも 3 つ設定されていることを確認します。セッション数の設定については、CMM オンライン・ドキュメントの tcpcmdmode コマンドを参照してください。

XClarity Orchestrator によって管理されているすべての CMM と Flex System に対して、IPv4 *または* IPv6 アドレスのいずれかを実装することを検討してください。一部の CMM と Flex スイッチに IPv4 を実装し、その他の CMM と Flex スイッチに IPv6 を実装すると、一部のイベントが監査ログで (または監査トラップとして) 取得されない可能性があります。

リソース・マネージャーから*別の*サブネットにあるシャーシを検出するには、以下のいずれかの条件を満たしていることを確認してください。

- マルチキャスト SLP 転送が環境内のラック・スイッチとルーターで有効になっていることを確認します。マルチキャスト SLP 転送が有効になっているかどうかを調べる方法や、無効になっている場合に有効にする方法については、そのスイッチやルーターに付属のドキュメントを参照してください。
- SLP がデバイスまたはネットワークで無効の場合、DNS 検出メソッドを代わりに使用できます。これを行うには、手動でサービス・レコード (SRV レコード) をドメイン・ネーム・サーバー (DNS) に追加します。例:
  ```
  lxco.company.com  service = 0 0 443 cmm1.company.com
  ```
  次に、「**BMC 構成 ➡ ネットワーク**」をクリックし、「**DNS**」タブをクリックして、管理 Web インターフェースからベースボード管理コンソールで DNS 検出を有効にします。

シャーシの管理について詳しくは、シャーシの管理 を参照してください。

複数の管理ツールに関する考慮事項

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

ThinkSystem、ThinkServer、および System x デバイス
別の管理ソフトウェアを使用して管理対象デバイスを監視する場合、ベースボード管理コントローラー・インターフェースから適切な SNMP または IPMI を使用して新しいローカル・ユーザーを作成します。必要に応じて、必ず SNMP または IPMI 権限を付与してください。

Flex System デバイス

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

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

共通検出設定の構成

デバイスを検出する際に使用する優先設定を選択します。

手順

ステップ 1. XClarity Orchestrator のメニュー・バーで、「**リソース (⎈) ➡ 新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。

ステップ 2. 「⎈**構成**」をクリックして、「検出設定」ダイアログを表示します。

ステップ 3. 優先検出設定を選択します。

- 「**SLP 検出**」サービス・ロケーション・プロトコル (SLP) を使用してデバイスを自動的に検出するかどうかを示します。

  有効の場合、XClarity Orchestrator は、15 分ごとに、およびユーザーがログインするごとに新しいデバイスの検索を試行します。

  注：XClarity Orchestrator で選択した SLP 検出設定は、XClarity Orchestrator によって管理される Lenovo XClarity Administrator インスタンスに対して選択された SLP 検出設定によってオーバーライドされます。Lenovo XClarity Administrator で SLP 検出設定が変更される場合は、XClarity Orchestrator を使用して同期されます。

- 「**今後管理されるすべてのデバイスの encapsulation**」デバイス管理時に encapsulation が有効化されるかどうかを示します。

  encapsulation はデフォルトでは無効になっています。無効にされた場合、デバイスの encapsulation モードは **通常** に設定され、ファイアウォール規則は管理プロセスの一部として変更されません。

  encapsulation 有効で、デバイスが encapsulation をサポートする場合、XClarity Orchestrator では管理プロセス時にデバイスと通信し (リソース・マネージャーを介して) デバイスの encapsulation モードを **encapsulationLite** に変更し、受信する要求をデバイスの管理のために選択されたリソース・マネージャーからのみに変更するよう、デバイスのファイアウォール規則を変更します。

  注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでにデバイスの管理のために選択されたリソース・マネージャーが使用できなくなった場合、encapsulation を無効にしてデバイスとの通信を確立するのに必要な段階を踏む必要があります。

- 「**登録要求が有効化されています**」管理コントローラーが DNS を使用してリソース・マネージャー・インスタンスを検索する際に、リソース・マネージャー (Lenovo XClarity Administrator および Lenovo XClarity Management Hub) がベースボード管理コントローラーからの検出要求を受け入れるかどうかを示します。有効にすると、管理コントローラーはリソース・マネージャーを検出されたデバイスとして登録できます。
- 「**オフラインのデバイスのクリーンアップ**」。オフラインのデバイスを、「**オフラインのデバイスのタイムアウト**」によって指定された時間内に、自動的に管理解除するかどうかを示します。有効にすると、XClarity Orchestrator が 1 時間ごとに、およびユーザーがポータルにログインするごとに、オフライン・デバイスを確認します。
- 「**オフラインのデバイスのタイムアウト**」オフラインになっているデバイスが自動的に管理解除されるまでの時間は 1 時間単位です。この値は 1 ～ 24 時間です。デフォルトは 24 時間です。

ステップ 4. 「**保存**」をクリックします。

サーバーの管理

Lenovo XClarity Orchestrator を使用して、複数のタイプの サーバーを管理できます。

始める前に

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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。

デバイスを管理する前に、管理に関する考慮事項を検討してください (デバイスの管理に関する考慮事項 を参照)。

デバイスを管理する前に、グローバル検出設定を確認します (共通検出設定の構成を参照)。

サービス検出プロトコルに応答しない Edge デバイスの検索と管理を行うには、ThinkEdge クライアント・デバイスの管理 を参照してください。

一括管理オプションは、サーバーでのみ使用できます。他のデバイス・タイプはサポートされていません。

このタスクについて

XClarity Orchestrator は、リソース・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。リソース・マネージャーを接続する場合は、XClarity Orchestrator ではそのリソース・マネージャーによって管理されるすべてのデバイスを管理します。

XClarity Orchestrator を使用してデバイスを管理下に置くこともできます。XClarity Orchestrator では、リソース・マネージャーによってすでに検出された (が管理されていない) デバイスの一覧が作成されます。XClarity Orchestrator から検出されたデバイスを管理する場合、そのデバイスは検出したリソース・マネージャーによって管理されます。IP アドレス、ホスト名、またはサブネットを使用してデバイスの手動での検出と管理を行う場合、デバイスの管理に使用するリソース・マネージャーを選択します。XClarity Management Hub を使用して ThinkEdge クライアント・デバイスを管理できます。XClarity Management Hub 2.0 を使用して ThinkServer デバイスを管理できます。Lenovo XClarity Administrator を使用してサーバー、ストレージ、スイッチ、およびシャーシを管理できます。

注：

- XClarity Management Hub 2.0 を通じてデバイスを管理しようとして、そのデバイスが既に別の XClarity Management Hub 2.0 で管理されている場合、XClarity Orchestrator は、以前の管理の確認を行わずに管理ユーザー・アカウントとサブスクリプションをデバイスから削除し、新しい管理ハブを通じてデバイスを再度管理します。このプロセスの完了後、デバイスは以前の管理ハブによる管理対象のままオフライ

ン状態ですが、デバイスはその管理ハブにデータを送信しなくなりました。接続されているポータルを通じて最初の管理ハブからデバイスを手動で管理解除する必要があることに注意してください。

- XClarity Management Hub 2.0 を通じてデバイスを管理しようとして、そのデバイスが既に別の XClarity Administrator で管理されている場合、XClarity Orchestrator は、XClarity Administrator の確認を行わずに XClarity Administrator によって XCC に登録されている管理ユーザー・アカウント、サブスクリプション、LDAP および SSO 情報をデバイスから削除し、新しい XClarity Management Hub 2.0 を通じてデバイスを再度管理します。このプロセスの完了後、デバイスは XClarity Administrator ハブによる管理対象のままオフライン状態ですが、デバイスはその管理ハブにデータを送信しなくなりました。接続されているポータルを通じて XClarity Administrator からデバイスを手動で管理解除する必要があることに注意してください。

以下のデバイスは、リソース・マネージャーによってサービス検出プロトコルを使用して自動的に検出できます。

- ThinkSystem サーバー、ThinkAgile サーバー、およびアプライアンス
- ThinkEdge SE サーバー
- Flex System シャーシ、Flex System シャーシ内の ThinkSystem デバイスおよび Flex System デバイス
- ThinkServer ラック・サーバーとタワー・サーバー
- System x、Converged HX、NeXtScale サーバー、およびアプライアンス
- ストレージ・デバイス

手順

サーバーを管理するには、以下のいずれかの手順を実行します。

- 手動でのサーバーの検出
- 検出されたサーバーの管理
- *多数のサーバーの管理*

手動でのサーバーの検出

Orchestrator サーバーと同じサブネットにない特定のシャーシを手動で検出して管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) ➡ **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。
2. 「**手動で入力**」をクリックして、「新しいデバイスの検索」ダイアログを表示します。
3. 「**サービス検出プロトコルに応答するデバイス**」を選択してから、「**次へ**」をクリックします。
4. 「**手動**」を選択してから、「**次へ**」をクリックします。
5. デバイスを検出する方法を選択し、適切な値を指定します。
   - 「**IP アドレス/ホスト名**」。管理する各デバイスの IPV4 または IPv6 IP アドレスまたは完全修飾ドメイン名 (例: 192.0.2.0 または d1.acme.com) を入力します。
   - 「**IP 範囲**」。管理する一連のデバイスの開始および終了 IP アドレスを入力します。
   - 「**サブネット**」。サブネットの IP アドレスとマスクを入力します。XClarity Orchestrator は、管理可能デバイスのサブネットをスキャンします。
6. デバイスの管理に使用するリソース・マネージャーを選択します。
7. 「**デバイスの検出**」をクリックします。検出プロセスが完了すると、検出されたデバイスが「新しいデバイス」テーブルにリストされます。

検出されたサーバーの管理

既に検出されたデバイスを管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) ➡ **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。

2. 「**すべての操作**」 ➡ 「**更新**」をクリックして、XClarity Orchestratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
3. 管理するサーバーを 1 台以上選択します。
4. 「**選択したデバイスの管理**」アイコン (⊕) をクリックして、「検出されたデバイスの管理」ダイアログを表示します。
5. 管理する選択したデバイスのリストを確認し、「**次へ**」をクリックします。
6. サーバーへの認証に使用されるユーザー名とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することを検討してください。下位レベルの権限を持つアカウントを使用すると、管理に失敗することや、管理は成功するものの、一部の機能が失敗することがあります。
7. **オプション**: 「**リカバリー・アカウントを作成して、すべてのローカル・ユーザーを無効にする**」を選択してから、リカバリー・パスワードを指定します。無効にした場合、ローカル・ユーザー・アカウントが認証に使用されます。

   有効にした場合、割り当てられたリソース・マネージャーによって管理対象認証ユーザー・アカウントとリカバリー・アカウント (RECOVERY_ID) がサーバーに作成され、その他すべてのローカル・ユーザー・アカウントは無効になります。管理対象認証ユーザー・アカウントは、XClarity Orchestrator およびリソース・マネージャーによって認証に使用されます。XClarity Orchestrator またはリソース・マネージャーに問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用してもベースボード管理コントローラーにログイン *できません*。ただし、RECOVERY_ID アカウントを使用してログインできます。

   重要：リカバリー・パスワードは後で使用できるように記録しておいてください。

   注：リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。
8. **オプション**: 「**資格情報の有効期限が切れた場合は新しいパスワードを設定する**」を有効にしてから、新しいサーバー・パスワードを指定します。現在のサーバー・パスワードの有効期限が切れ

ている場合、パスワードが変更されるまで検出は失敗します。新しいパスワードを指定すると、資格情報が変更され、管理プロセスを続行できます。パスワードは、現行パスワードが期限切れである場合にのみ使用されます。

9. 「**管理**」を選択します。ジョブは、バックグラウンドで管理プロセスを完了するために作成されます。ログまたはジョブ・ログから管理プロセスのステータスを監視するには、「**監視** (📈) ➡ **ジョブ**」をクリックします (ジョブの監視 を参照)。

   以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。

   - リソース・マネージャーで障害が発生したため、復元できません。

     注：交換リソース・マネージャー・インスタンスで、障害が発生したリソース・マネージャーと同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
   - デバイスが管理対象から除外される前に、リソース・マネージャーが停止した場合。
   - デバイスは正常に管理解除されませんでした。
   - XClarity Orchestrator は、デバイスの IP アドレスが変更された後、管理対象デバイスをオフラインとして表示します。

多数のサーバーの管理

多数のサーバーを管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) ➡ **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。
2. 「**一括管理**」ボタンをクリックして、「一括管理」ダイアログを表示します。
3. デバイスの管理に使用するリソース・マネージャーを選択します。
4. 管理する各サーバーの IP アドレスまたは完全修飾ドメイン名をコンマで区切って入力します (例: 192.0.2.0, d1.acme.com)。

   重要：

   - これらの指定されたサーバーはすべて、同じ資格情報を使用する必要があります。
   - FQDN には、英数字、ピリオド、およびダッシュのみを含めることができます。
5. 「**次へ**」をクリックします。
6. サーバーへの認証に使用されるユーザー名とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することを検討してください。下位レベルの権限を持つアカウントを使用すると、管理に失敗することや、管理は成功するものの、一部の機能が失敗することがあります。
7. **オプション**: 「**リカバリー・アカウントを作成して、すべてのローカル・ユーザーを無効にする**」を選択してから、リカバリー・パスワードを指定します。無効にした場合、ローカル・ユーザー・アカウントが認証に使用されます。

   有効にした場合、割り当てられたリソース・マネージャーによって管理対象認証ユーザー・アカウントとリカバリー・アカウント (RECOVERY_ID) がサーバーに作成され、その他すべてのローカル・ユーザー・アカウントは無効になります。管理対象認証ユーザー・アカウントは、XClarity Orchestrator およびリソース・マネージャーによって認証に使用されます。XClarity Orchestrator またはリソース・マネージャーに問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用してもベースボード管理コントローラーにログイン *できません*。ただし、RECOVERY_ID アカウントを使用してログインできます。

   重要：リカバリー・パスワードは後で使用できるように記録しておいてください。

注：リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。

8. **オプション**:「**資格情報の有効期限が切れた場合は新しいパスワードを設定する**」を有効にしてから、新しいサーバー・パスワードを指定します。現在のサーバー・パスワードの有効期限が切れている場合、パスワードが変更されるまで検出は失敗します。新しいパスワードを指定すると、資格情報が変更され、管理プロセスを続行できます。パスワードは、現行パスワードが期限切れである場合にのみ使用されます。
9. 「**管理**」を選択します。ジョブは、バックグラウンドで管理プロセスを完了するために作成されます。ログまたはジョブ・ログから管理プロセスのステータスを監視するには、「**監視** () ➡ **ジョブ**」をクリックします (ジョブの監視 を参照)。

   以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。

   - リソース・マネージャーで障害が発生したため、復元できません。

     注：交換リソース・マネージャー・インスタンスで、障害が発生したリソース・マネージャーと同じ IP アドレスを使用している場合は、`RECOVERY_ID` アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
   - デバイスが管理対象から除外される前に、リソース・マネージャーが停止した場合。
   - デバイスは正常に管理解除されませんでした。
   - XClarity Orchestrator は、デバイスの IP アドレスが変更された後、管理対象デバイスをオフラインとして表示します。

終了後

管理対象デバイスに対して、以下の操作を実行できます。

- デバイスのステータスと詳細を監視します (デバイスの状態の表示 および デバイスの詳細の表示 を参照)。
- 「**リソース**」 () をクリックして選択したデバイスを管理解除して削除します。次に左側のナビゲーションでデバイス・タイプをクリックして、そのタイプのすべての管理対象デバイスのテーブル・ビューを含むカードを表示します。そして、管理解除するデバイスを選択してから、「**管理解除**」アイコン () を選択します。

  注：

  – 最大 50 台のデバイスを一度に管理解除できます。
  – デバイスで実行されているアクティブなジョブがないことを確認します。
  – XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」を選択します。
  – デフォルトでは、XClarity Administrator によって管理されているデバイス、および 24 時間以上オフラインのデバイスは自動的に管理解除されます (共通検出設定の構成を参照)。
  – ほとんどのデバイスでは、デバイスが管理解除された後もデバイスに関する特定の情報が保持されます。デバイスが管理解除されている場合は、以下のようになります。
    – 管理ユーザー・アカウント、イベントおよびメトリック・サブスクリプションがデバイスから削除されます。
    – XClarity Administrator によって管理されているデバイスでは、コール・ホームが現在 XClarity Administrator で有効になっている場合、コール・ホームはデバイスで無効になっています。
    – XClarity Administrator によって管理されているデバイスでは、デバイスで encapsulation が有効になっている場合、デバイスのファイアウォール規則は、デバイスが管理される前に設定に変更されます。
    – デバイスによって生成された機密情報、インベントリー、イベントおよびアラートは管理ハブで廃棄されます。

– デバイスの管理ハブによって生成されたイベントおよびアラートは、管理ハブで保持されます。

ThinkEdge クライアント・デバイスの管理

ThinkEdge クライアント・デバイスには、ベースボード管理コントローラーを搭載していないため、サービス検出プロトコルを使用した検出ができません。割り当てられた Lenovo XClarity Management Hub リソース・マネージャーによってデバイスが安全に検出および管理される前に、ThinkEdge クライアント・デバイスにユニバーサル・デバイス・クライアント (UDC) エージェントをインストールする必要があります。Lenovo XClarity Management Hub リソース・マネージャーのみがこれらのデバイスの検索と管理を行うことができます。

始める前に

デバイスを管理する前に、管理に関する考慮事項を検討してください (デバイスの管理に関する考慮事項 を参照)。

1 つ以上の Lenovo XClarity Management Hub リソース・マネージャーがオンラインで、XClarity Orchestrator に接続されていることを確認します (リソース・マネージャーの接続 を参照)。

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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。

UDS Portal 資格情報がクライアント ID およびシークレットで構成されていることを確認します。資格情報は、クライアント・プロビジョニング・パッケージで使用されるポリシーに署名するために使用されます。UDS ポータルは、UDC エージェントが正しく機能できるようこのポリシーに署名するための信頼できるソースです。資格情報を構成するには、メニュー・バーで「**リソース**」( ) → 「**新しいデバイス**」をクリックし、「**UDS Portal 資格情報**」をクリックしてから、クライアント ID とシークレットを入力します。クライアント ID およびシークレットを Lenovo にリクエストするには、メールの説明に「UDS Portal 資格情報」を使用し、会社名、お問い合わせ先情報 (メール・アドレスまたは電話番号)、および 10 桁の Lenovo お客様番号を記載して、uedmcredreq@lenovo.com にメールを送信します。

UDC エージェントが ThinkEdge クライアント・デバイスに現在インストールされて*いない*ことを確認します。UDC エージェントがインストールされている場合は、次のコマンドを実行してアンインストールする必要があります。UDC エージェントをインストールするには、権限が必要です。

- **Linux**
  ```
  sudo apt purge udc-release
  ```
- **Windows**
  ```
  PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall

  POPD
  ```

*{hub-domain}*が、ThinkEdge Client デバイスの管理に使用する XClarity Management Hub リソース・マネージャーの完全修飾ドメイン名である、次のドメインが含まれるように DNS サーバーが構成されていることを確認します。

- api.*{hub-domain}*
- api-mtls.*{hub-domain}*
- auth.*{hub-domain}*
- mqtt.*{hub-domain}*
- mqtt-mtls.*{hub-domain}*
- s3.*{hub-domain}*
- s3console.*{hub-domain}*

このタスクについて

XClarity Orchestrator は、リソース・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。リソース・マネージャーを接続する場合は、XClarity Orchestrator ではそのリソース・マネージャーによって管理されるすべてのデバイスを管理します。

XClarity Orchestrator を使用してデバイスを管理下に置くこともできます。XClarity Orchestrator では、リソース・マネージャーによってすでに検出された (が管理されていない) デバイスの一覧が作成されます。XClarity Orchestrator から検出されたデバイスを管理する場合、そのデバイスは検出したリソース・マネージャーによって管理されます。IP アドレス、ホスト名、またはサブネットを使用してデバイスの手動での検出と管理を行う場合、デバイスの管理に使用するリソース・マネージャーを選択します。XClarity Management Hub を使用して ThinkEdge クライアント・デバイスを管理できます。XClarity Management Hub 2.0 を使用して ThinkServer デバイスを管理できます。Lenovo XClarity Administrator を使用してサーバー、ストレージ、スイッチ、およびシャーシを管理できます。

Lenovo XClarity サポート Web サイト からサポートされる ThinkEdge Client デバイスの全リストを見つけるには、「**互換性**」タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

注：ThinkEdge サーバー (SE350、SE360、SE450 など) にはベースボード管理コントローラーが搭載されており、サービス検出プロトコルを使用して検出できます。これらのデバイスを管理するには、サーバーの管理 を参照してください。

手順

ThinkEdge クライアント・デバイスの検索と管理を行うには、以下の手順を実行します。

1. 各 ThinkEdge クライアント・デバイスに UDC エージェントをインストールします。
   a. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) → **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。
   b. 「**手動で入力**」をクリックして、「新しいデバイスの検索」ダイアログを表示します。
   c. 「**サービス検出プロトコルに応答しないデバイス**」を選択してから、「**次へ**」をクリックします。
   d. ThinkEdge Client デバイスの管理に使用する XClarity Management Hub リソース・マネージャーの IP アドレスを選択します。正常な状態の XClarity Management Hub リソース・マネージャーのみを選択できます。
   e. サーバーにインストールされているオペレーティング・システムのタイプを選択します。
      - 「**Linux ARM**」
      - 「**Linux x86**」
      - 「**Windows**」
   f. UDC エージェント・インストーラーがダウンロード後使用不可能な日数を選択します。デフォルトは 30 日です。
   g. UDC エージェントをサーバーにインストールする予定の回数を選択します。これは通常、UDC エージェントをインストールする必要があるデバイスの数です。最大 1000000 回を指定できます。デフォルトは 10 回です。
   h. 「**UDC エージェントのダウンロード**」をクリックして、UDC エージェント・インストーラーをローカル・システムにダウンロードします。ジョブは、バックグラウンドでダウンロード・プロセスを完了するために作成されます。ログまたはジョブ・ログからダウンロード・プロセスのステータスを監視するには、「**監視**」(📈) → 「**ジョブ**」をクリックします (ジョブの監視を参照)。
   i. 「**閉じる**」をクリックして、ダイアログを閉じます。
   j. 該当する ThinkEdge クライアント・デバイスに UDC エージェント・インストーラーをコピーし、パッケージを解凍/unzip してから、次のコマンドを使用してそれらのデバイスに UDC エージェントをインストールします。エージェントをインストールするには、**管理者**権限が必要です。
      - Linux `install.sh`
      - Windows `setup.cmd`

各 ThinkEdge クライアント・デバイスに UDC エージェントが正常にインストールされると、選択したXClarity Management Hub リソース・マネージャーによってデバイスを自動的に検出できます。

2. ThinkEdge クライアント・デバイスを管理します。
   a. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) → **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。

      注：テーブルに IP アドレスが表示されるのにしばらく時間がかかる場合があります。

   b. 「**すべての操作**」 → 「**更新**」をクリックして、XClarity Orchestratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
   c. ThinkEdge クライアント・デバイスを 1 台以上選択します。
   d. 「**管理**」アイコン (⚙) をクリックして、「デバイスの管理」ダイアログを表示します。
   e. 管理する選択したデバイスの一覧を確認します。
   f. 「**管理**」を選択します。ジョブは、バックグラウンドで管理プロセスを完了するために作成されます。ログまたはジョブ・ログから管理プロセスのステータスを監視するには、「**監視** (📈) → **ジョブ**」をクリックします (ジョブの監視 を参照)。

      以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。

      - リソース・マネージャーで障害が発生したため、復元できません。

        注：交換リソース・マネージャー・インスタンスで、障害が発生したリソース・マネージャーと同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
      - デバイスが管理対象から除外される前に、リソース・マネージャーが停止した場合。
      - デバイスは正常に管理解除されませんでした。

- XClarity Orchestrator は、デバイスの IP アドレスが変更された後、管理対象デバイスをオフラインとして表示します。

終了後

管理対象デバイスに対して、以下の操作を実行できます。

- デバイスのステータスと詳細を監視します (デバイスの状態の表示 および デバイスの詳細の表示 を参照)。
- 「**リソース**」 () をクリックして選択したデバイスを管理解除して削除します。次に左側のナビゲーションでデバイス・タイプをクリックして、そのタイプのすべての管理対象デバイスのテーブル・ビューを含むカードを表示します。そして、管理解除するデバイスを選択してから、「**管理解除**」アイコン () を選択します。

  注：

  - 最大 50 台のデバイスを一度に管理解除できます。
  - デバイスで実行されているアクティブなジョブがないことを確認します。
  - XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」を選択します。
  - デフォルトでは、XClarity Administrator によって管理されているデバイス、および 24 時間以上オフラインのデバイスは自動的に管理解除されます (共通検出設定の構成を参照)。
  - ほとんどのデバイスでは、デバイスが管理解除された後もデバイスに関する特定の情報が保持されます。デバイスが管理解除されている場合は、以下のようになります。
    - 管理ユーザー・アカウント、イベントおよびメトリック・サブスクリプションがデバイスから削除されます。
    - XClarity Administrator によって管理されているデバイスでは、コール・ホームが現在 XClarity Administrator で有効になっている場合、コール・ホームはデバイスで無効になっています。
    - XClarity Administrator によって管理されているデバイスでは、デバイスで encapsulation が有効になっている場合、デバイスのファイアウォール規則は、デバイスが管理される前に設定に変更されます。
    - デバイスによって生成された機密情報、インベントリー、イベントおよびアラートは管理ハブで廃棄されます。
    - デバイスの管理ハブによって生成されたイベントおよびアラートは、管理ハブで保持されます。

ストレージ・デバイスの管理

Lenovo XClarity Orchestratorでは、複数のタイプの Lenovo Storage アプライアンス、デバイス、およびテープ・ライブラリーを管理できます。

始める前に

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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。

デバイスを管理する前に、管理に関する考慮事項を検討してください (デバイスの管理に関する考慮事項 を参照)。

サービス検出プロトコルに応答しない Edge デバイスの検索と管理を行うには、ThinkEdge クライアント・デバイスの管理 を参照してください。

一括管理オプションは、サーバーでのみ使用できます。他のデバイス・タイプはサポートされていません。

このタスクについて

XClarity Orchestrator は、リソース・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。リソース・マネージャーを接続する場合は、XClarity Orchestrator ではそのリソース・マネージャーによって管理されるすべてのデバイスを管理します。

XClarity Orchestrator を使用してデバイスを管理下に置くこともできます。XClarity Orchestrator では、リソース・マネージャーによってすでに検出された (が管理されていない) デバイスの一覧が作成されます。XClarity Orchestrator から検出されたデバイスを管理する場合、そのデバイスは検出したリソース・マネージャーによって管理されます。IP アドレス、ホスト名、またはサブネットを使用してデバイスの手動での検出と管理を行う場合、デバイスの管理に使用するリソース・マネージャーを選択します。XClarity Management Hub を使用して ThinkEdge クライアント・デバイスを管理できます。XClarity Management Hub 2.0 を使用して ThinkServer デバイスを管理できます。Lenovo XClarity Administrator を使用してサーバー、ストレージ、スイッチ、およびシャーシを管理できます。

手順

ストレージ・デバイスを管理するには、以下のいずれかの手順を完了します。
- 手動でのストレージ・デバイスの検出
- 検出されたストレージ・デバイスの管理

手動でのストレージ・デバイスの検出

Orchestrator サーバーと同じサブネットにない特定のストレージ・デバイスを手動で検出して管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) ➡ **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。
2. 「**手動で入力**」をクリックして、「新しいデバイスの検索」ダイアログを表示します。
3. 「**サービス検出プロトコルに応答するデバイス**」を選択してから、「**次へ**」をクリックします。
4. 「**手動**」を選択してから、「**次へ**」をクリックします。
5. デバイスを検出する方法を選択し、適切な値を指定します。
   - 「**IP アドレス/ホスト名**」。管理する各デバイスの IPV4 または IPv6 IP アドレスまたは完全修飾ドメイン名 (例: 192.0.2.0 または d1.acme.com) を入力します。
   - 「**IP 範囲**」。管理する一連のデバイスの開始および終了 IP アドレスを入力します。
   - 「**サブネット**」。サブネットの IP アドレスとマスクを入力します。XClarity Orchestrator は、管理可能デバイスのサブネットをスキャンします。
6. デバイスの管理に使用するリソース・マネージャーを選択します。
7. 「**デバイスの検出**」をクリックします。検出プロセスが完了すると、検出されたデバイスが「新しいデバイス」テーブルにリストされます。

検出されたストレージ・デバイスの管理

既に検出されたデバイスを管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) ➡ **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。

2. 「**すべての操作**」 ➡ 「**更新**」をクリックして、XClarity Orchestratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
3. 管理するストレージ・デバイスを 1 台以上選択します。
4. 「**選択したデバイスの管理**」アイコン (⎄) をクリックして、「検出されたデバイスの管理」ダイアログを表示します。
5. 管理する選択したデバイスのリストを確認し、「**次へ**」をクリックします。
6. サーバーへの認証に使用されるユーザー名とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することを検討してください。下位レベルの権限を持つアカウントを使用すると、管理に失敗することや、管理は成功するものの、一部の機能が失敗することがあります。
7. 「**管理**」を選択します。ジョブは、バックグラウンドで管理プロセスを完了するために作成されます。ログまたはジョブ・ログから管理プロセスのステータスを監視するには、「**監視** (📈) ➡ **ジョブ**」をクリックします (ジョブの監視 を参照)。

   以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。

   - リソース・マネージャーで障害が発生したため、復元できません。

     注：交換リソース・マネージャー・インスタンスで、障害が発生したリソース・マネージャーと同じ IP アドレスを使用している場合は、`RECOVERY_ID` アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
   - デバイスが管理対象から除外される前に、リソース・マネージャーが停止した場合。
   - デバイスは正常に管理解除されませんでした。
   - XClarity Orchestrator は、デバイスの IP アドレスが変更された後、管理対象デバイスをオフラインとして表示します。

終了後

管理対象デバイスに対して、以下の操作を実行できます。

- デバイスのステータスと詳細を監視します (デバイスの状態の表示 および デバイスの詳細の表示 を参照)。
- 「**リソース**」 () をクリックして選択したデバイスを管理解除して削除します。次に左側のナビゲーションでデバイス・タイプをクリックして、そのタイプのすべての管理対象デバイスのテーブル・ビューを含むカードを表示します。そして、管理解除するデバイスを選択してから、「**管理解除**」アイコン () を選択します。

  注：

  – 最大 50 台のデバイスを一度に管理解除できます。
  – デバイスで実行されているアクティブなジョブがないことを確認します。
  – XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」を選択します。
  – デフォルトでは、XClarity Administrator によって管理されているデバイス、および 24 時間以上オフラインのデバイスは自動的に管理解除されます (共通検出設定の構成を参照)。
  – ほとんどのデバイスでは、デバイスが管理解除された後もデバイスに関する特定の情報が保持されます。デバイスが管理解除されている場合は、以下のようになります。
    – 管理ユーザー・アカウント、イベントおよびメトリック・サブスクリプションがデバイスから削除されます。
    – XClarity Administrator によって管理されているデバイスでは、コール・ホームが現在 XClarity Administrator で有効になっている場合、コール・ホームはデバイスで無効になっています。
    – XClarity Administrator によって管理されているデバイスでは、デバイスで encapsulation が有効になっている場合、デバイスのファイアウォール規則は、デバイスが管理される前に設定に変更されます。
    – デバイスによって生成された機密情報、インベントリー、イベントおよびアラートは管理ハブで廃棄されます。
    – デバイスの管理ハブによって生成されたイベントおよびアラートは、管理ハブで保持されます。

シャーシの管理

Lenovo XClarity Orchestrator では、複数のタイプのシャーシおよびシャーシ・コンポーネントを管理できます。

始める前に

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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。

デバイスを管理する前に、管理に関する考慮事項を検討してください (デバイスの管理に関する考慮事項 を参照)。

サービス検出プロトコルに応答しない Edge デバイスの検索と管理を行うには、ThinkEdge クライアント・デバイスの管理 を参照してください。

一括管理オプションは、サーバーでのみ使用できます。他のデバイス・タイプはサポートされていません。

このタスクについて

XClarity Orchestrator は、リソース・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。リソース・マネージャーを接続する場合は、XClarity Orchestrator ではそのリソース・マネージャーによって管理されるすべてのデバイスを管理します。

XClarity Orchestrator を使用してデバイスを管理下に置くこともできます。XClarity Orchestrator では、リソース・マネージャーによってすでに検出された (が管理されていない) デバイスの一覧が作成されます。XClarity Orchestrator から検出されたデバイスを管理する場合、そのデバイスは検出したリソース・マネージャーによって管理されます。IP アドレス、ホスト名、またはサブネットを使用してデバイスの手動での検出と管理を行う場合、デバイスの管理に使用するリソース・マネージャーを選択します。XClarity Management Hub を使用して ThinkEdge クライアント・デバイスを管理できます。XClarity Management Hub 2.0 を使用して ThinkServer デバイスを管理できます。Lenovo XClarity Administrator を使用してサーバー、ストレージ、スイッチ、およびシャーシを管理できます。

手順

シャーシを管理するには、以下のいずれかの手順を実行します。

手動でのシャーシの検出

Orchestrator サーバーと同じサブネットにない特定のシャーシを手動で検出して管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) → **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。
2. 「**手動で入力**」をクリックして、「新しいデバイスの検索」ダイアログを表示します。
3. 「**サービス検出プロトコルに応答するデバイス**」を選択してから、「**次へ**」をクリックします。
4. 「**手動**」を選択してから、「**次へ**」をクリックします。
5. デバイスを検出する方法を選択し、適切な値を指定します。
   - 「**IP アドレス/ホスト名**」。管理する各デバイスの IPV4 または IPv6 IP アドレスまたは完全修飾ドメイン名 (例: 192.0.2.0 または d1.acme.com) を入力します。
   - 「**IP 範囲**」。管理する一連のデバイスの開始および終了 IP アドレスを入力します。
   - 「**サブネット**」。サブネットの IP アドレスとマスクを入力します。XClarity Orchestrator は、管理可能デバイスのサブネットをスキャンします。
6. デバイスの管理に使用するリソース・マネージャーを選択します。
7. 「**デバイスの検出**」をクリックします。検出プロセスが完了すると、検出されたデバイスが「新しいデバイス」テーブルにリストされます。

検出されたシャーシの管理

既に検出されたデバイスを管理するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで、「**リソース** (⚙) → **新しいデバイス**」をクリックして「新しいデバイスの検出および管理カード」を表示します。

2. 「**すべての操作**」 → 「**更新**」をクリックして、XClarity Orchestrator ドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
3. 管理するシャーシを 1 台以上選択します。
4. 「**選択したデバイスの管理**」アイコン (⎄) をクリックして、「検出されたデバイスの管理」ダイアログを表示します。
5. 管理する選択したデバイスのリストを確認し、「**次へ**」をクリックします。
6. サーバーへの認証に使用されるユーザー名とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することを検討してください。下位レベルの権限を持つアカウントを使用すると、管理に失敗することや、管理は成功するものの、一部の機能が失敗することがあります。
7. **オプション**: 「**リカバリー・アカウントを作成して、すべてのローカル・ユーザーを無効にする**」を選択してから、リカバリー・パスワードを指定します。無効にした場合、ローカル・ユーザー・アカウントが認証に使用されます。

   有効にした場合、割り当てられたリソース・マネージャーによって管理対象認証ユーザー・アカウントとリカバリー・アカウント (RECOVERY_ID) がサーバーに作成され、その他すべてのローカル・ユーザー・アカウントは無効になります。管理対象認証ユーザー・アカウントは、XClarity Orchestrator およびリソース・マネージャーによって認証に使用されます。XClarity Orchestrator またはリソース・マネージャーに問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用してもベースボード管理コントローラーにログイン *できません*。ただし、RECOVERY_ID アカウントを使用してログインできます。

   重要：リカバリー・パスワードは後で使用できるように記録しておいてください。

   注：リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。
8. **オプション**: 「**資格情報の有効期限が切れた場合は新しいパスワードを設定する**」を有効にしてから、新しいサーバー・パスワードを指定します。現在のサーバー・パスワードの有効期限が切れ

ている場合、パスワードが変更されるまで検出は失敗します。新しいパスワードを指定すると、資格情報が変更され、管理プロセスを続行できます。パスワードは、現行パスワードが期限切れである場合にのみ使用されます。

9. 「**管理**」を選択します。ジョブは、バックグラウンドで管理プロセスを完了するために作成されます。ログまたはジョブ・ログから管理プロセスのステータスを監視するには、「**監視** () ➡ **ジョブ**」をクリックします (ジョブの監視 を参照)。

   以下のエラー条件のいずれかにより管理でエラーが発生した場合は、「管理の強制」オプションを使用してこの手順を繰り返します。

   - リソース・マネージャーで障害が発生したため、復元できません。

     注：交換リソース・マネージャー・インスタンスで、障害が発生したリソース・マネージャーと同じ IP アドレスを使用している場合は、`RECOVERY_ID` アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
   - デバイスが管理対象から除外される前に、リソース・マネージャーが停止した場合。
   - デバイスは正常に管理解除されませんでした。
   - XClarity Orchestrator は、デバイスの IP アドレスが変更された後、管理対象デバイスをオフラインとして表示します。

終了後

管理対象デバイスに対して、以下の操作を実行できます。

- デバイスのステータスと詳細を監視します (デバイスの状態の表示 および デバイスの詳細の表示 を参照)。
- 「**リソース**」 () をクリックして選択したデバイスを管理解除して削除します。次に左側のナビゲーションでデバイス・タイプをクリックして、そのタイプのすべての管理対象デバイスのテーブル・ビューを含むカードを表示します。そして、管理解除するデバイスを選択してから、「**管理解除**」アイコン () を選択します。

  注：

  – 最大 50 台のデバイスを一度に管理解除できます。
  – デバイスで実行されているアクティブなジョブがないことを確認します。
  – XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」を選択します。
  – デフォルトでは、XClarity Administrator によって管理されているデバイス、および 24 時間以上オフラインのデバイスは自動的に管理解除されます (共通検出設定の構成を参照)。
  – ほとんどのデバイスでは、デバイスが管理解除された後もデバイスに関する特定の情報が保持されます。デバイスが管理解除されている場合は、以下のようになります。
    – 管理ユーザー・アカウント、イベントおよびメトリック・サブスクリプションがデバイスから削除されます。
    – XClarity Administrator によって管理されているデバイスでは、コール・ホームが現在 XClarity Administrator で有効になっている場合、コール・ホームはデバイスで無効になっています。
    – XClarity Administrator によって管理されているデバイスでは、デバイスで encapsulation が有効になっている場合、デバイスのファイアウォール規則は、デバイスが管理される前に設定に変更されます。
    – デバイスによって生成された機密情報、インベントリー、イベントおよびアラートは管理ハブで廃棄されます。
    – デバイスの管理ハブによって生成されたイベントおよびアラートは、管理ハブで保持されます。

デバイスの管理解除

Lenovo XClarity Orchestrator を使用して、それぞれのリソース・マネージャーの管理からデバイスを削除できます。このプロセスは*管理解除*と呼ばれます。

始める前に

このタスクを実行するには、事前定義された**スーパーバイザー**または**セキュリティー管理者**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。

デバイスで実行されているアクティブなジョブがないことを確認します。

このタスクについて

XClarity Orchestrator では、デフォルトで 24 時間以上オフラインのデバイスを自動的に管理解除します (共通検出設定の構成 を参照)。

ほとんどのデバイス、XClarity Orchestrator およびリソース・マネージャーでは、管理解除後もデバイスに関する特定の情報が保持されます。この情報は、同じデバイスの管理を再開したときに再適用されます。

手順

デバイスを管理解除するには、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** ()」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。

ステップ 2. 管理解除するデバイスを 1 つ以上選択します。

ステップ 3. 「**管理解除**」アイコン () をクリックすると、管理解除ダイアログが表示されます。

ステップ 4. 「**デバイスに到達できない場合でも管理対象からの除外を強制する**」を選択します。

ステップ 5. 「**非管理**」をクリックします。

「管理対象から除外」ダイアログには、管理解除プロセスの各ステップの進行状況が表示されます。

VMware Tools の使用

VMware Tools パッケージは、Lenovo XClarity Orchestrator を VMware ESXi ベース環境にインストールする場合に、仮想マシンのゲスト・オペレーティング・システムにインストールされます。このパッケージは、アプリケーションの状態と継続性を保持しながら、最適化された仮想アプライアンスのバックアップと移行をサポートする VMware ツールのサブセットを提供します。

VMware ツールの使用について詳しくは、VMware vSphere ドキュメント センター Web サイト内 「VMware Tools 構成ユーティリティーの使用」を参照してください。

ネットワーク設定の構成

1 つのネットワーク・インターフェース (IPv4 および IPv6 設定を使用)、インターネットのルーティング設定、およびプロキシ設定を構成できます。

始める前に

詳細: ネットワークの構成方法および NTP サーバーのセットアップ方法

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。

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。

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

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。

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。

セキュリティー証明書の使用

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。

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

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。

XClarity Orchestrator 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、XClarity Orchestrator 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。XClarity Orchestrator 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 XClarity Orchestrator から切断されます。

XClarity Orchestrator は、リソース・マネージャー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、リソース・マネージャーまたは外部サービスは、XClarity Orchestrator が検証するサーバー証明書を提供します。XClarity Orchestrator によってトラステッド証明書のリストが維持されます。リソース・マネージャー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、XClarity Orchestrator 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、XClarity Orchestrator 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、XClarity Orchestrator 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 (XClarity

Orchestrator 内部署名済み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 XClarity Orchestrator サーバー証明書として使用されます。これは、XClarity Orchestrator 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 (XClarity Orchestrator 内部署名済み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 XClarity Orchestrator にインポートします (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 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 (Web ブラウザーへのサーバー証明書のインポート を参照)。

以下のカテゴリー (信頼ストア) の証明書は、XClarity Orchestrator クライアントによって使用されます。

- **信頼できる証明書**この信頼ストアは、XClarity Orchestrator がクライアントとして機能する場合に、ローカルのリソースへの安全な接続を確立するために使用する証明書を管理します。ローカルのリソースの例には、管理対象リソース・マネージャー、イベント転送時のローカルのソフトウェアなどがあります。
- **外部サービス証明書**。この信頼ストアは、XClarity Orchestrator がクライアントとして機能する場合に、外部サービスへの安全な接続を確立するために使用する証明書を管理します。外部サービスの例として、保証情報の取得またはサービス・チケットの作成に使用されるオンライン Lenovo Support サービス、イベントの転送先の外部ソフトウェア (Splunk など) があります。これには、一般によく知られている信頼できる特定の証明機関プロバイダー (Digicert や Globalsign など) のルート証明機関の事前に設定されたトラステッド証明書が含まれます。別の外部サービスへの接続を必要とする機能を使用するように XClarity Orchestrator を設定する場合は、資料を参照して、この信頼ストアに手動で証明書を追加する必要があるかどうかを確認してください。

  なお、この信頼ストアの証明書は、メインのトラステッド証明書信頼ストアにも追加しない限り、他のサービス (LDAP など) との接続を確立する場合に信頼されません。この信頼ストアから証明書を削除すると、これらのサービスが正常に機能しなくなります。

外部サービス用トラステッド証明書の追加

これらの証明書は、外部サービスとの信頼関係を確立するために使用されます。たとえば、この信頼ストア内の証明書は、Lenovo から保証情報の取得、チケットの作成、外部アプリケーション (Splunk など) へのイベントの転送、および外部 LDAP サーバーの使用などを行う場合に使用されます。

始める前に

この信頼ストア内の証明書は、メインのトラステッド証明書信頼ストアにも追加されない限り、他のサービスとの接続を確立する場合は信頼されません。この信頼ストアから証明書を削除すると、これらのサービスが正常に機能しなくなります。

手順

トラステッド証明書を追加するには、次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「**外部サービス証明書**」をクリックして、「外部サービスのトラステッド証明書」カードを表示します。

ステップ 2. 「**追加**」アイコン (⊙) をクリックして、証明書を追加します。「証明書の追加」ダイアログが表示されます。

ステップ 3. PEM 形式の証明書データをコピーして貼り付けます。

ステップ 4. 「**追加**」をクリックします。

終了後

「外部サービスのトラステッド証明書」カードからは、以下の操作を実行できます。

- 選択したトラステッド証明書の詳細を表示するには、「**表示**」アイコン (⊙) をクリックします。
- 選択したトラステッド証明書をローカル・システムに保存するには、「**表示**」アイコン (⊙) をクリックした後、「**pem として保存**」をクリックします。
- 「**削除**」アイコン (🗑) をクリックして、選択したトラステッド証明書を削除します。

内部サービス用トラステッド証明書の追加

この証明書は、リソース・マネージャー、ローカル・ソフトウェアへのイベント転送、組み込み LDAP サーバーなどのリソースに対するクライアントとして Lenovo XClarity Orchestrator が機能する場合に、ローカル・リソースとの信頼関係を確立するために使用されます。さらに、 内部 CA 証明書やカスタマイズされた外部署名済みサーバー証明書の CA 証明書 (インストールされている場合) もこの信頼ストアに存在し、 内部の XClarity Orchestrator 通信をサポートします。

手順

トラステッド証明書を追加するには、次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「**トラステッド証明書**」をクリックして、「トラステッド証明書」カードを表示します。

ステップ 2. 「**追加**」アイコン (⊙) をクリックして、証明書を追加します。「証明書の追加」ダイアログが表示されます。

ステップ 3. PEM 形式の証明書データをコピーして貼り付けます。

ステップ 4. 「**追加**」をクリックします。

終了後

「トラステッド証明書」カードから、以下の操作を実行できます。

- 選択したトラステッド証明書の詳細を表示するには、「**表示**」アイコン (⊙) をクリックします。
- 選択したトラステッド証明書をローカル・システムに保存するには、「**表示**」アイコン (⊙) をクリックした後、「**pem として保存**」をクリックします。
- 「**削除**」アイコン (🗑) をクリックして、選択したトラステッド証明書を削除します。

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

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。

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 XClarity Orchestrator 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 (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 Orchestrator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。

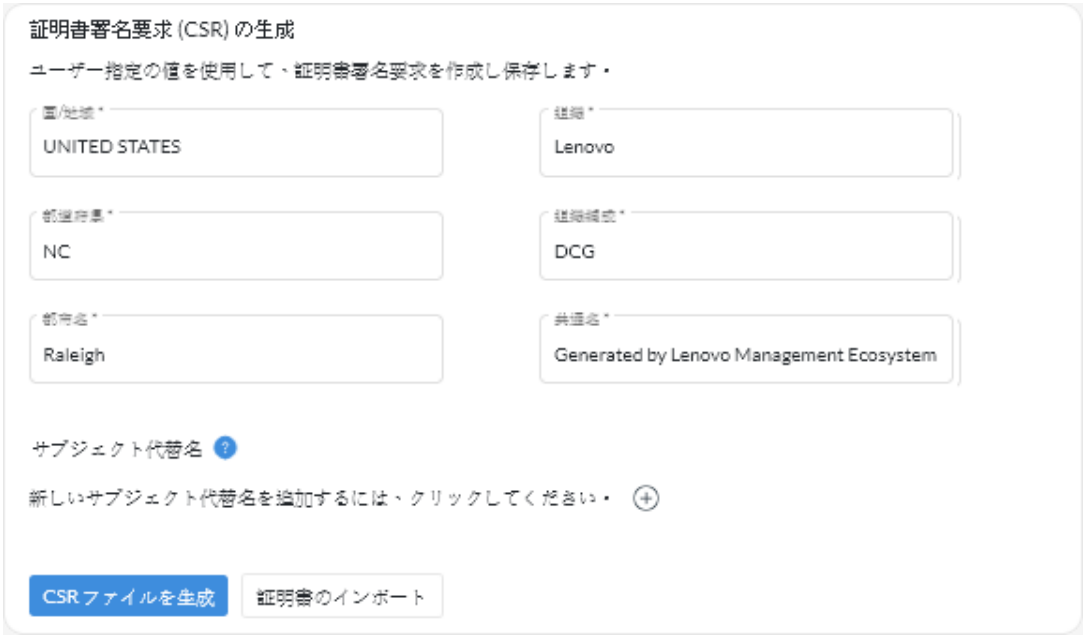
重要：サーバー証明書を変更した場合、すべての確立されたユーザー・セッションで Ctrl＋F5 をクリックして Web ブラウザーの情報を最新に更新し、XClarity Orchestrator に対する接続を再確立することによって、新しい証明書を受け入れる必要があります。

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 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「**サーバー証明書**」をクリックして、「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。
   - オプション: CSR の生成時に X.509 「subjectAltName」拡張に追加されるサブジェクト代替名。デフォルトでは、XClarity Orchestrator 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 Orchestrator が CSR のサブジェクト代替名を自動的を定義します。このサブジェクト代替名値のカスタマイズ、削除、またはサブジェクト代替名値への追加を行うことができます。ただし、サブジェクト代替名はサーバーの完全修飾ドメイン名 (FQDN) または IP アドレスを持っている必要があり、サブジェクト名を FQDN に設定する必要があります。

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)

注：表に示されているすべてのサブジェクト代替名は、次の手順で CSR を生成した後でのみ、検証、保存され、CSR に追加されます。

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 Orchestrator 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 Orchestrator 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。

XClarity Orchestrator 内部署名済み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、現在の内部署名済み Lenovo XClarity Orchestrator サーバー証明書を置き換えるか、現在 XClarity Orchestrator 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 Orchestrator が生成した証明書を復元できます。この新しい内部署名されたサーバー証明書は、XClarity Orchestrator によって HTTPS アクセスに使用されます。

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、内部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再生成されて署名されるまでは使用されます。

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 Orchestrator 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

内部署名済み XClarity Orchestrator 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 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「**サーバー証明書**」をクリックして、「サーバー証明書の再作成」カードを表示します。

ステップ 2. 「サーバー証明書の再作成」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。
- サーバー証明書が無効になった日付と時刻。

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. 「**証明書の再生成**」をクリックし、内部署名済み証明書を再生成して、「**証明書の再生成**」をクリックして確認します。

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。

終了後

「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。

Web ブラウザーへのサーバー証明書のインポート

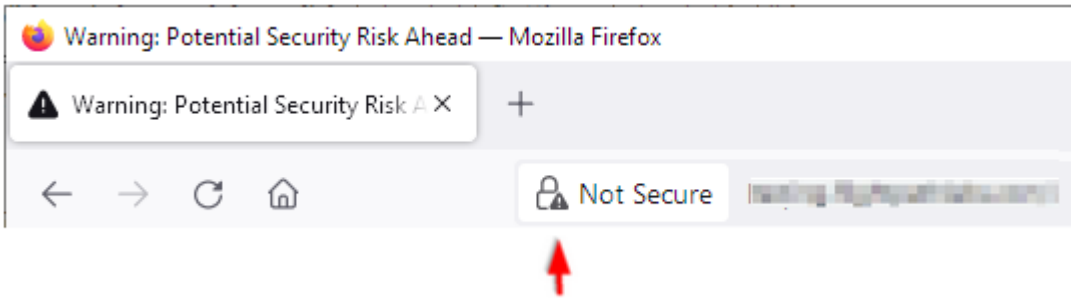
ローカル・システムに現在のサーバーの証明書のコピーを、PEM 形式で保存できます。次に、Lenovo XClarity Orchestrator にアクセスしたときに Web ブラウザーにセキュリティー警告メッセージが表示されないようにするために、Web ブラウザーのトラステッド証明書のリストまたは他のアプリケーション (Lenovo XClarity Mobile や Lenovo XClarity Integrator など) に証明書をインポートできます。

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. XClarity Orchestrator 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. 「**証明書の (無効)**」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. 「**ファイルにコピー**」をクリックして、「証明書のエクスポート ウィザード」を表示します。
     e. 「**暗号メッセージ構文標準**」を選択して、「**次へ**」をクリックします。
     f. 証明書ファイルの名前と場所を指定し、「**終了**」を選択して証明書をエクスポートします。
     g. 「**OK**」をクリックして「証明書」ダイアログを閉じます。
  2. XClarity Orchestrator 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**」をクリックします。
     b. 「**プライバシーとセキュリティー**」セクションまでスクロールし、「**証明書の管理**」をクリックして「証明書」ダイアログを表示します。
     c. 「**インポート**」をクリックし、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。
     d. 「**証明書ストア**」の横にある「**参照**」をクリックし、「**信頼されたルート証明機関**」を選択します。次に「**OK**」をクリックします。
     e. 「**完了**」をクリックします。
     f. Chrome ブラウザーを閉じてから開き直し、XClarity Orchestrator を開きます。
- Firefox
  1. XClarity Orchestrator 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. 「安全ではない接続」を展開し、「詳細を表示」をクリックしてダイアログを表示します。
c. 「**証明書の表示**」をクリックします。
d. 「ダウンロード」セクションまで下にスクロールして、「**PEM (cert)**」リンクをクリックします。
e. 「**ファイルを保存する**」を選択して「**OK**」をクリックします。

2. XClarity Orchestrator 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. ブラウザーを開き、「**ツール**」 → 「**オプション**」 → 「**詳細**」の順にクリックします。
   b. 「**証明書**」タブをクリックします。
   c. 「**証明書の表示**」をクリックします。
   d. 「**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。
   e. 証明書を選択し、「**開く**」をクリックします。

認証の管理

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 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 XClarity Orchestrator オンライン・ドキュメント を参照してください。

サポートされている外部 LDAP サーバーは Microsoft Active Directory のみです。

XClarity Orchestratorでは、外部 LDAP サーバーで定義されているユーザー・グループのクローンを自動的には作成しません。ただし、LDAP ユーザー・グループのクローンを手動で作成できます (ユーザー・グループの作成を参照)。

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。

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。

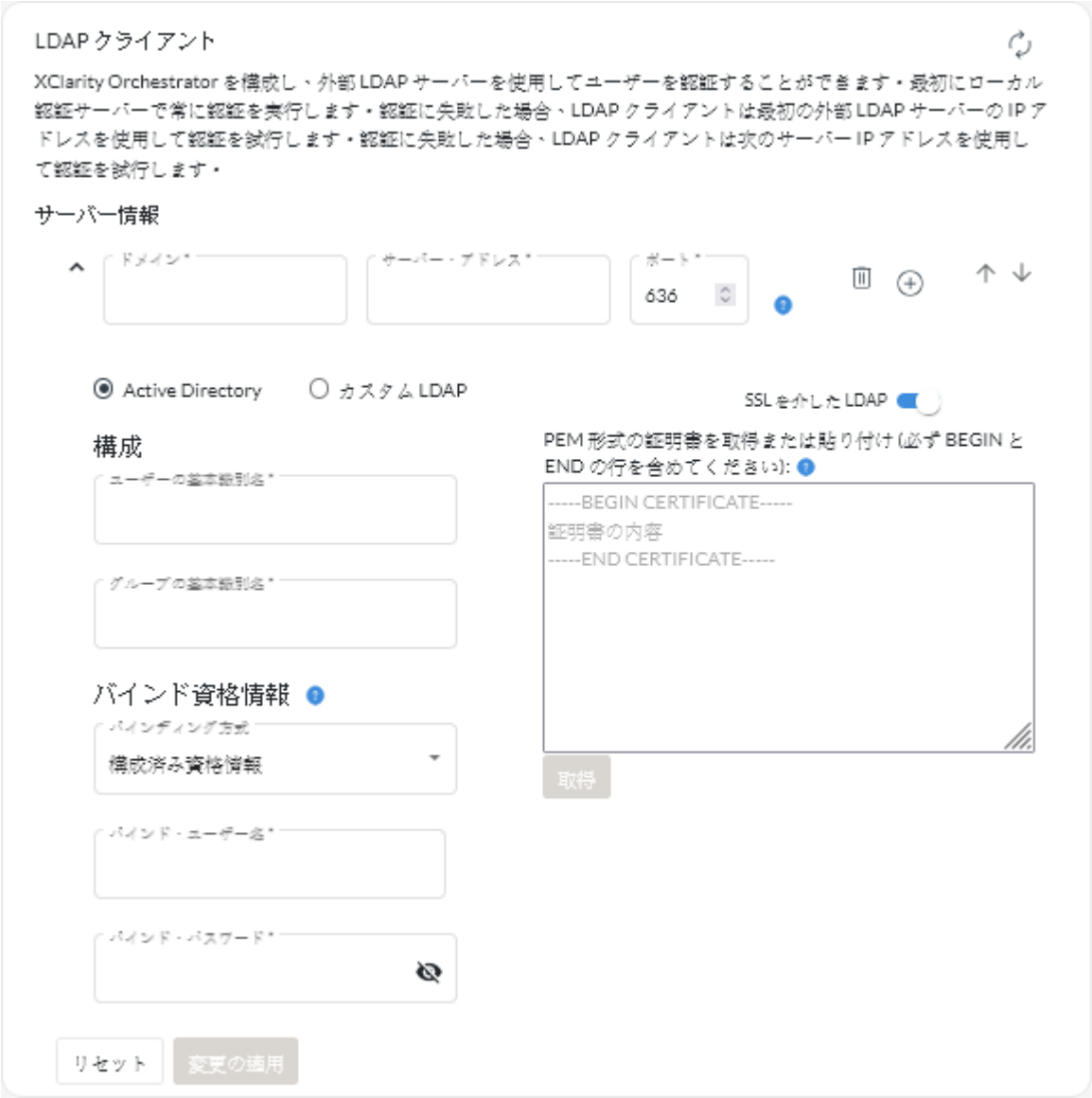
外部 LDAP サーバーが構成されている場合は、XClarity Orchestrator はまず、ローカル認証サーバーを使用してユーザーを認証しようとします。認証に失敗した場合、XClarity Orchestrator は最初の LDAP サーバーの IP アドレスを使用して認証を試行します。認証に失敗した場合、LDAP クライアントは次の LDAP サーバーの IP アドレスを使用して認証を試行します。

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

LDAP サーバー構成を削除するには、構成の横にある「**削除**」アイコン (🗑) をクリックします。LDAP サーバー構成を削除して、同じドメイン内に他の LDAP サーバー構成がない場合、そのドメイン内のクローン・ユーザーとクローン・ユーザー・グループも削除されます。

ユーザーおよびユーザー・セッションの管理

*ユーザー・アカウント*は、Lenovo XClarity Orchestrator のログインおよび管理に使用されます。

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

外部 LDAP サーバーのユーザーは、初めてログインしたときに *{username}@{domain}* という名前でローカル認証サーバーに自動的にクローンが作成されます。このクローン作成されたユーザー・アカウントはリソースへのアクセス許可にだけ使用できます。認証は、これらのユーザーに対して LDAP 認証サーバーで実行されますが、ユーザー・アカウントへの変更 (説明および役割以外) は、LDAP で行う必要があります。

XClarity Orchestrator は、役割を使用する機能 (アクション) へのアクセスを制御します。ローカル・ユーザーとクローン作成されたユーザーに別の役割を割り当てるには、それらのユーザーを、目的の役割に関連付けられている 1 つ以上のユーザー・グループに追加します。デフォルトでは、すべてのユーザーがユーザー・グループの**オペレーター・グループ**のメンバーです (ユーザー・グループの作成を参照)。

少なくとも 1 人のユーザーは、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*ローカル・ユーザー・グループ*のメンバーである必要があります (機能へのアクセス制御を参照).

注意：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。

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

「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。

- テーブルの行をクリックしてユーザーのプロパティを表示し、「ユーザーの詳細」ダイアログを表示します。

- 選択したユーザーのプロパティ (パスワードおよびユーザー・グループなど) を変更するには、「**編集**」アイコン () をクリックします。
- 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。LDAP ユーザーから既存の LDAP ユーザー・グループを削除することはできません
- 「**エクスポート**」アイコン () をクリックして、ユーザー名、名、姓などのユーザーの詳細をエクスポートします。

ユーザー・グループの作成

ユーザー・グループは、リソースへのアクセスを許可するために使用されます。

始める前に

詳細: ユーザー・グループの作成方法

ローカル・リポジトリーで手動でユーザー・グループを作成できます。ローカル・ユーザー・グループには、ローカル・ユーザーおよびクローン作成されたユーザーが含まれます。

外部 LDAP サーバーで定義されているユーザー・グループのクローンを作成できます。クローン作成された LDAP ユーザー・グループの名前は、ローカル・リポジトリー内で *{domain}\{groupName}* となります。このクローン作成されたユーザー・グループは、リソースへのアクセスを許可するためだけに使用できます。グループ名、説明、およびメンバーシップの変更は、LDAP を通じて行う必要があります。

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。

LDAP サーバー構成がログイン資格情報を使用するようにセットアップされている場合で、ローカルの XClarity Orchestrator ユーザー ID を使用してXClarity Orchestratorにログインした場合 、LDAP ユーザー・グループのクローンを作成するときに LDAP ユーザー資格情報を指定するように求められます。それ以外の場合、ユーザーの資格情報は不要です。

このタスクについて

XClarity Orchestrator には、以下の事前定義されたユーザー・グループがあります (事前定義された役割ごとに 1 つ)。役割について詳しくは、機能へのアクセス制御を参照してください。

- **スーパーバイザー・グループ**。このユーザー・グループのユーザーには、**スーパーバイザー**役割が割り当てられます。
- **ハードウェア管理者グループ**。このユーザー・グループのユーザーには、**ハードウェア管理者**役割が割り当てられます。
- **セキュリティー管理者グループ**。このユーザー・グループのユーザーには、**セキュリティー管理者**役割が割り当てられます。
- **レポーター・グループ**。このユーザー・グループのユーザーには、**レポーター**の役割が割り当てられます。
- **更新管理者グループ**。このユーザー・グループのユーザーには、**更新管理者**役割が割り当てられます。
- **オペレーター・グループ**。このユーザー・グループのユーザーには、**オペレーター**役割が割り当てられます。
- **オペレーター・レガシー・グループ**。このユーザー・グループのユーザーには、**オペレーター・レガシー**役割が割り当てられます。このユーザー・グループは今後のリリースで廃止されることに注意してください。

少なくとも 1 人のユーザーは、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 *ローカル・ユーザー・グループ*のメンバーである必要があります (機能へのアクセス制御を参照).

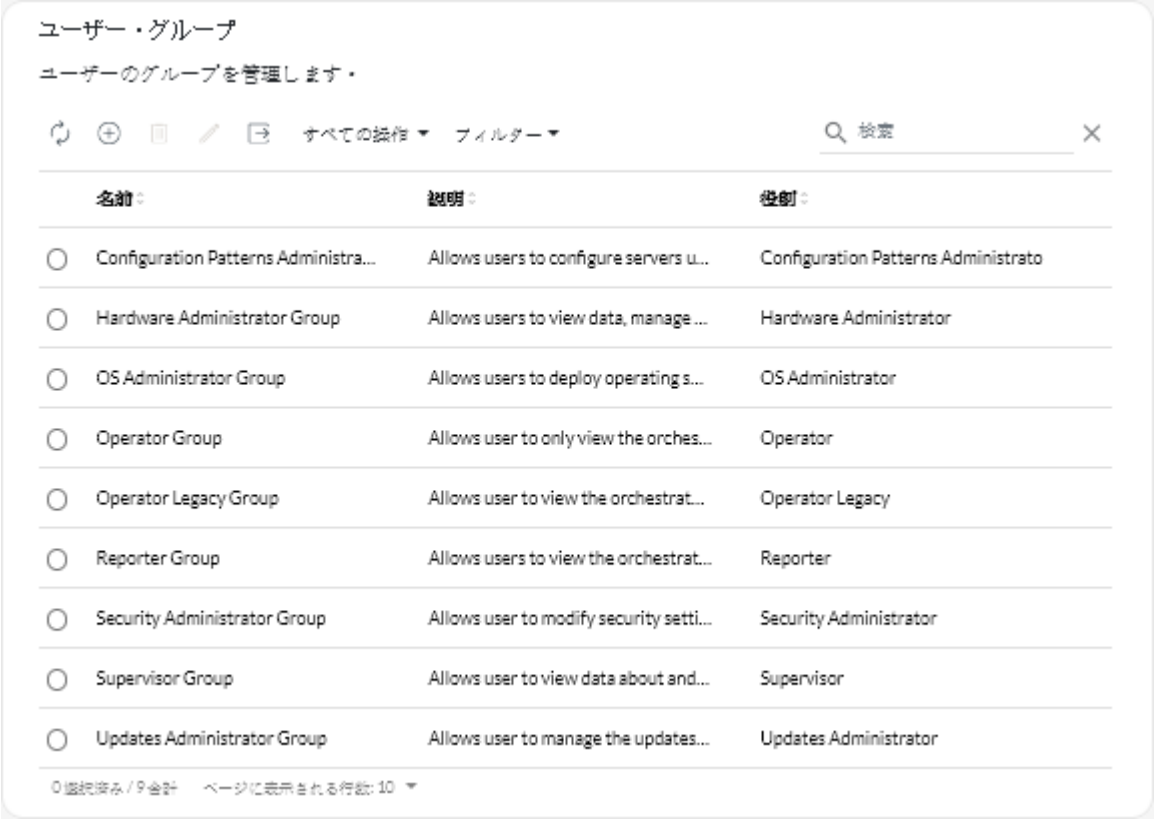
外部 LDAP ユーザーが XClarity Orchestrator にログインするには、XClarity Orchestrator でクローン作成された LDAP ユーザー・グループの直接のメンバーである必要があります。XClarity Orchestrator では、外

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。

手順

ユーザー・グループを作成するには、以下の手順を実行します。

- **ローカル・ユーザー・グループを作成します**
  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「**ユーザー・グループ**」をクリックして、「ユーザー・グループ」カードを表示します。



  2. 「**作成**」アイコン (⊕) をクリックして、「グループの作成」ダイアログを表示します。
  3. グループ・タイプとして「**ローカル・ユーザー・グループ**」を選択します。
  4. このユーザー・グループの名前および説明 (任意) を指定します。
  5. 「**利用可能なユーザー**」タブをクリックし、このユーザー・グループに追加するユーザーを選択します。
  6. 「**役割**」タブをクリックし、このユーザー・グループで割り当てる役割を選択します。役割が選択されていない場合は、デフォルトで**オペレーター**役割が割り当てられます。
  7. 「**作成**」をクリックします。
- **外部 LDAP サーバーからユーザー・グループをクローン作成します**
  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「**ユーザー・グループ**」をクリックして、「ユーザー・グループ」カードを表示します。
  2. 「**作成**」アイコン (⊕) をクリックして、「グループの作成」ダイアログを表示します。
  3. グループ・タイプとして「**LDAP ユーザー・グループ**」を選択します。

4. オプションで、グループの説明を指定します。
5. 追加するユーザー・グループが含まれている外部 LDAP サーバーの LDAP 構成を選択します。

   ヒント: 入力を開始すると、指定したキーワードを含むすべてのグループ名が見つかります。
6. ログイン資格情報を使用して外部 LDAP サーバーを構成している場合は、外部 LDAP サーバーにログインするためのユーザー名とパスワードを指定します。
7. 「**グループの検索**」フィールドで検索文字列 (最低 3 文字) を指定し、「**検索**」をクリックして検索文字列に一致する外部 LDAP サーバー内のユーザー・グループを見つけます。次に、追加するグループを選択します。
8. 「**役割**」タブをクリックし、このユーザー・グループで割り当てる役割を選択します。役割が選択されていない場合は、デフォルトで**オペレーター**役割が割り当てられます。
9. 「**作成**」をクリックします。

終了後

「ユーザー・グループ」カードから、以下の操作を実行できます。

- 選択したユーザー・グループのプロパティ、ローカル・メンバーシップ、および役割を変更するには、**編集**アイコン (✎) をクリックします。
  - グループからユーザーを追加または削除したときに、その新たなグループ割り当てによって役割 (権限) が変更された場合は、そのユーザーは自動的にログアウトされます。そのユーザーが再びログインすると、割り当てられたユーザー・グループの集約された役割に基づくアクションを実行できます。
  - ユーザーは、それぞれ少なくとも 1 つのユーザー・グループのメンバーである必要があります。この属性を空の配列または null に設定した場合は、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。
  - 事前定義されたユーザー・グループの場合は、グループ・メンバーシップのみ変更できます。
  - LDAP ユーザー・グループの場合は、説明と役割のみを変更できます。その他のプロパティやメンバーシップを変更するには、外部 LDAP サーバーを使用します。
- 選択したユーザー・グループを削除するには、「**削除**」アイコン (🗑) をクリックします。

  注：事前定義済みのユーザー・グループは削除できません。
- ユーザー・グループのメンバーを表示するには、グループ名をクリックし、「グループの表示」ダイアログを表示して、「**メンバーの概要**」タブをクリックします。

ユーザー・アカウントの詳細の変更

ユーザー・アカウントのパスワード、フルネーム、メール・アドレス、および電話番号を変更できます。

このタスクについて

デフォルトでは、ユーザーのパスワードは 0 日後に有効期限が切れます。

手順

パスワードおよびその他の属性を変更するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のタイトル・バーで、右上隅の「**ユーザー操作**」メニュー (⚙) をクリックし、「**パスワードの変更**」をクリックします。「パスワードの変更」ダイアログが表示されます。

ステップ 2. 現在のパスワードを入力します。

ステップ 3. 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。

- 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)。

ステップ 4. 必要に応じて、フルネーム、メール・アドレス、および電話番号を変更します。

ステップ 5. 「**変更**」をクリックします。

他のユーザーの詳細の変更

スーパーバイザー・ユーザーは、パスワードなど、別のユーザーの詳細を変更できます。

このタスクについて

デフォルトでは、ユーザーのパスワードは 0 日後に有効期限が切れます。

パスワードの有効期限とパスワードの複雑性の規則を構成できます (ユーザー・セキュリティー設定の構成 を参照)。

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. ユーザー・アカウントを選択します。

ステップ 3. 「**編集**」アイコン (✎) をクリックしてユーザーのプロパティを変更します。「ユーザーの編集」ダイアログが表示されます。

ステップ 4. 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。

- 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)。

ステップ 5. 「**編集**」をクリックします。

ユーザー・セキュリティー設定の構成

ユーザー・アカウント・セキュリティー設定により、ローカル・ユーザーのパスワード、ログイン、およびユーザー・セッションの設定が構成されます。

詳細:  ユーザー・セキュリティー設定の構成方法

手順

ローカル・ユーザーのセキュリティー設定を構成するには、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「**アカウント・セキュリティー設定**」をクリックして、「アカウント・セキュリティー設定」カードを表示します。

ステップ 2. 以下のセキュリティー設定を構成します。

セキュリティー設定	説明	使用できる値	デフォルト値
パスワードの有効期限	ユーザーが変更を求められることなくパスワードを使用できる期間 (日単位)。 値を小さくすると、攻撃者にパスワードを推測される危険が少なくなります。 0 を設定すると、パスワードは無期限になります。	0 – 365	0
パスワード失効の警告期間	ユーザー・パスワードの有効期間満了日から、期限が近づいていることを警告する通知をユーザーが最初に受け取るまでの期間 (日単位)。 0 に設定すると、この警告はユーザーに通知されません。	0 – 30	0
最短パスワード再利用サイクル	パスワードを変更する際、ユーザーが旧パスワードを再利用できるようになる前に、固有のパスワードを指定しなければならない最小回数 0 に設定すると、パスワードをすぐに再利用できます。	0 – 10	5
最短パスワード変更期間	ユーザーがパスワードを変更した後、再度そのパスワードを変更できるようになるまでの最短時間 (時間単位)。 この設定に、「**パスワードの有効期限**」で指定した値を超える値を指定することはできません。 0 を設定すると、パスワードはすぐに変更できます。	0 – 240	1

セキュリティー設定	説明	使用できる値	デフォルト値
最大ログイン失敗数	ユーザー・アカウントがロックアウトされる前に、ユーザーが正しくないパスワードでログインを試行できる最大回数。 **注：**同じユーザー名とパスワードを使用して連続してログインを試行した場合は、ログインに 1 回失敗したとカウントされます。 0 を設定すると、アカウントはロックされません。	0 – 10	5
ログイン失敗のカウンターのリセット	「**最大ログイン失敗数**」のカウンターが 0 にリセットされるまでの、最後のログイン試行からの経過時間。 0 を設定すると、カウンターがリセットされることはありません。たとえば、最大ログイン失敗数が 2 で、ログインに 1 回失敗してから 24 時間でもう一度に失敗すると、ログインに 2 回失敗したことがシステムに登録され、アカウントがロックアウトされます。 **注：**この設定は、「**最大ログイン失敗数**」が 1 以上に設定されている場合にのみ適用されます。	0 – 60	15
ログイン失敗が最大回数に達した後のロックアウト期間	ロックされたユーザーが再びログインを試行できるようになるまでの最短時間 (分単位)。 ロックされているユーザー・アカウントは、有効なパスワードを入力しても、XClarity Orchestrator にアクセスできません。 0 を設定すると、ユーザー・アカウントはロックされません。 **注：**この設定は、「**最大ログイン失敗数**」が 1 以上に設定されている場合にのみ適用されます。	0 – 2880	60
Web 非アクティブ・セッションのタイムアウト	orchestrator サーバーとの間で確立されたユーザー・セッションが、ユーザー・セッションおよびユーザーが自動的にログアウトされる前に非アクティブになるまでの時間 (分単位)。このタイムアウトは、すべての操作 (ページを開く、現在のページを更新する、データを変更するなど) に適用されます。 これは、ユーザー・セッションのプライマリ・タイムアウトです。 セッションがアクティブな場合、このタイマーは、ユーザーが操作を実行するたびにリセットされます。タイムアウト値を超えると、次回ユーザーがアクションを実行しようとしたときにログイン・ページが表示されます。 0 に設定すると、このタイムアウトは無効になります。	0, 60 - 1440	1440

セキュリティー設定	説明	使用できる値	デフォルト値
	注：この設定を変更すると、認証タイプに関係なく、すべてのユーザー・セッションにすぐに影響を及ぼします。新しいタイムアウト値よりも長く非アクティブだった既存のセッションは期限切れになります。		
全操作に対する非アクティブな Web タイムアウト	データを変更した操作 (リソースの作成、更新、削除など) が無効になるまでに、Orchestrator サーバーで確立されたユーザー・セッションを非アクティブにすることができる時間 (分単位) これはオプションのセカンダリ・タイムアウトであり、プライマリの **非アクティブな Web セッションのタイムアウト**の値より短くなります。 セッションがアクティブな場合、このタイマーは、ユーザーが操作を実行するたびにリセットされます。このタイムアウト値を超過しても、プライマリの **非アクティブな Web セッションのタイムアウト**の値を*超えないように*すると、ユーザーはプライマリの **非アクティブな Web セッションのタイムアウト**の値を超過するまで読み取り専用操作 (ページを開く、ページを更新するなど) に制限されます。ただし、ユーザーがデータを変更する操作を実行しようとすると、ユーザー・セッションの期限が切れてログイン・ページが表示されます。 0 に設定すると、このタイムアウトは無効になります。 **注：**この設定を変更すると、認証タイプに関係なく、すべてのユーザー・セッションにすぐに影響を及ぼします。新しいタイムアウト値よりも長く非アクティブだった既存のセッションは期限切れになります。	0, 15 – 60	30
Web ベースのセッションの有効期限 (必須)	ユーザーのアクティビティに関係なく、Orchestrator サーバーとの間で確立されたユーザー・セッションが、ユーザーが自動的にログアウトされる前にオープンになるまでの時間 (時間単位) **注：**この設定を変更すると、認証タイプに関係なく、すべてのユーザー・セッションにすぐに影響を及ぼします。新しいタイムアウト値よりも長く非アクティブだった既存のセッションは期限切れになります。	24 – 240	24
最小パスワード長	有効なパスワードの指定に使用できる最小文字数。	8 – 256	256

セキュリティー設定	説明	使用できる値	デフォルト値
最大パスワード長	有効なパスワードの指定に使用できる最大文字数。	8 – 128	128
特定ユーザーに対する最大アクティブ・セッション数	任意の時点で許可される特定ユーザーのアクティブ・セッションの最大数。最大数に達すると、(作成タイムスタンプに基づいて) そのユーザーの最も古いアクティブ・セッションが削除されてから、そのユーザーに対して新しいセッションが作成されます。 0 に設定した場合、特定ユーザーに対して許可されるアクティブ・セッション数は無制限になります。 **注：**設定の変更後に開始されるユーザー・セッションにのみ影響します。	0 – 20	20
新しいパスワードの作成時に従う必要がある複雑性規則の数	新しいパスワードの作成時に従う必要がある複雑性規則の数 規則の適用は、規則 1 から、指定した規則数に至るまで行われます。たとえば、パスワードの複雑性が 4 に設定されている場合は、規則 1、2、3、および 4 に従う必要があります。パスワードの複雑性が 2 に設定されている場合は、規則 1 および 2 に従う必要があります。 XClarity Orchestrator では、以下のパスワード複雑性規則がサポートされています。 • 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)。 0 を設定すると、パスワードは複雑性の規則に準拠する必要がなくなります。	0 – 5	4
初回アクセス時にパスワードの変更をユーザーに強制する	XClarity Orchestrator への初回ログイン時に、パスワードの変更をユーザーに求めるかどうかを指定します。	**はい**または**いいえ**	**はい**

ステップ 3. 「**適用**」をクリックします。

変更が適用されると、新しい設定は即時に有効になります。パスワード・ポリシーを変更した場合は、ユーザーの次回のログインまたはパスワード変更から適用されます。

終了後

「アカウント・セキュリティー設定」カードから、以下の操作を実行できます。

- この設定をデフォルト値にリセットするには、「**デフォルトの復元**」をクリックします。

アクティブなユーザー・セッションの監視

XClarity Orchestrator Web インターフェースにログインしているユーザーを調べることができます。

始める前に

デフォルトで、24 時間を超えて非アクティブなユーザー・セッションは自動的にログアウトされます。非アクティブな Web セッションのタイムアウトを構成できます (ユーザー・セキュリティー設定の構成 を参照)。

手順

XClarity Orchestrator のメニュー・バーから「**管理** (⚙)」 ➔ 「**セキュリティー**」をクリックし、左側のナビゲーションで「**アクティブ・セッション**」をクリックすると、「アクティブ・セッション」カードが表示されます。

終了後

「アクティブ・セッション」カードから、以下の操作を実行できます。

- 選択したユーザー・セッションを切断するには、「**削除**」アイコン (🗑) をクリックします。

  注：現在のセッションを切断することはできません。

機能へのアクセス制御

Lenovo XClarity Orchestrator は、*役割*と*ユーザー・グループ*を使用してユーザーが実行を許可されている機能 (アクション) を特定します。

このタスクについて

*役割*とは、一連の機能です。役割がユーザー・グループに割り当てられると、そのグループのすべてのユーザーはその役割に含まれる機能を実行できます。

XClarity Orchestrator には以下の定義済みの役割があります。

- **スーパーバイザー**。ユーザーが Orchestrator サーバーとすべての管理対象リソース (リソース・マネージャーおよびデバイス) に関するデータを表示し、使用可能なすべての操作を実行できるようにします。この役割が割り当てられたユーザーは、常にすべてのリソース (デバイスおよびリソース・

マネージャー) およびすべての機能にアクセスできます。この役割に対して、リソースまたは機能へのアクセスを制限することはできません。

次の操作を実行するには、スーパーバイザー権限が必要です。
- Orchestrator サーバーの再起動
- 保守タスクの実行 (ライセンスのインストールや新しいバージョンへの更新など)
- リソース・マネージャーの接続および切断
- システム設定の変更 (ネットワーク設定、日時など)
- Lenovo への定期的なデータの送信に対する同意

スーパーバイザー権限を持つユーザーは少なくとも 1 人は必要です。

重要：XClarity Orchestrator v1.0 からそれ以降のリリースにアップグレードする場合、XClarity Orchestrator v1.0 で作成されたすべてのユーザーにデフォルトでスーパーバイザー権限が与えられます。スーパーバイザー・ユーザーは、権限を必要としないユーザーのスーパーバイザー権限を削除できます。

- **ハードウェア管理者**。ユーザーはデータの表示、構成パターンの管理とデプロイ、OS プロファイルを使用したオペレーティング・システムの管理とデプロイ、分析の表示とカスタマイズ、およびアクセス可能なリソースに対するアクションの実行を行うことができます。この役割のユーザーは、管理対象リソース上のソフトウェアまたはファームウェアの更新、およびリソース・グループの管理を行うことはできません。
- **サーバー構成管理者**。ユーザーはデータの表示、構成パターンを使用したサーバーの構成、事前定義済み分析の表示、アクセス可能なリソースの表示を行うことができます。この役割では、ユーザーがデバイスへのリモート・アクセスおよびデバイスの電源オン/オフを行うことはできません。
- **OS 管理者**。ユーザーは、OS プロファイル使用したオペレーティング・システムのデプロイ、事前定義済み分析の表示、アクセス可能なリソースの表示を行うことができます。この役割では、ユーザーがデバイスへのリモート・アクセスおよびデバイスの電源オン/オフを行うことはできません。
- **更新管理者**。ユーザーは、リソース・マネージャーのデバイスおよびソフトウェアでのファームウェアの更新し、アクセス可能なリソースのデータの表示、事前定義された分析の表示を行うことができます。
- **セキュリティー管理者**。ユーザーは、Orchestrator サーバーでのセキュリティー設定の変更やセキュリティー関連のアクションの実行、すべての管理対象リソースのデータの表示、リソース・グループの管理、および事前定義された分析の表示を行うことができます。この役割が割り当てられたユーザーは、常にすべてのリソース (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。この役割でリソースへのアクセスを制限することはできません。
- **レポーター**。ユーザーは、Orchestrator サーバー構成の表示、アクセス可能なリソースに関するデータの表示、カスタム・レポートを生成するためのクエリの作成、およびレポートをスケジュールおよびメールで送信するためのデータ・フォワーダーの作成を行うことができます。この役割では、ユーザーがリソースのプロビジョニングおよびデバイスの電源オン/オフを行うことはできません。
- **オペレーター**。ユーザーは Orchestrator サーバーの構成のみの表示、およびアクセス可能なリソースのデータを表示を行うことができます。この役割のユーザーは、Orchestrator サーバーと管理対象リソースでアクションの実行および構成設定の変更、分析レポートの作成および表示、およびカスタム・アラートの作成はできません。
- **オペレーター・レガシー**。ユーザーは、アクセス可能なリソースのでデータの表示、および特定の操作 (インベントリー、アラート、サービス・チケットの管理など) の実行を行うことができます。この役割のユーザーは、管理対象リソースのソフトウェアまたはファームウェアの更新、リソース・グループの作成、分析レポートの作成および表示、およびカスタム・アラートの作成はできません。

  注意：XClarity Orchestrator v1.2 からそれ以降のリリースにアップグレードする場合、**オペレーター**役割が割り当てられたユーザーは、自動的に**オペレーター・レガシー**役割に変更され、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。**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。

ユーザーが特定のアクションを実行できない場合、それらのアクションを実行するために使用するメニュー項目、ツールバー・アイコン、およびボタンは無効になります (淡色表示されます)。

注：リソース関連データは、役割に基づく制限なく表示できます。すべてのユーザーは、アクセスできるリソースのリソース関連データ (インベントリー、アラート、ジョブ、およびサービス・チケットなど) を表示できます。

手順

事前定義済みの役割の詳細を表示するには、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「**役割**」をクリックします。

役割の行をクリックすると「役割」ダイアログが表示され、役割のプロパティに関する情報、役割の機能のリスト、その役割が割り当てられているユーザー・グループのリストが確認できます。

ユーザーへの役割の割り当て

Lenovo XClarity Orchestrator は、*役割*と*ユーザー・グループ*を使用してユーザーが実行を許可されている機能 (アクション) を特定します。

始める前に

アクティブ・セッションに現在ログインしているユーザーの役割が変更された場合、そのユーザーのセッションは自動的に終了し、ユーザー・インターフェースからログアウトされます。そのユーザーが再びログインすると、新しく割り当てられた役割に基づく機能を実行できるようになります。

このタスクについて

ユーザー・グループに複数の役割を割り当てると、各役割での機能は集約されます。

ユーザー・グループのメンバーであるすべてのユーザーは、そのユーザー・グループに割り当てられた役割に含まれる機能を実行できます。

ユーザーの役割は、次の方法で変更できます。
- ユーザー・グループからそのユーザーを追加または削除する
- そのユーザーがメンバーであるユーザー・グループから役割を追加または削除する
- そのユーザーがメンバーであるユーザー・グループを削除する

注：

- LDAP ユーザーが LDAP サーバーの LDAP ユーザー・グループに追加または削除されると、その LDAP ユーザーと LDAP ユーザー・グループ間の関連付けの変更は、既存のクローン作成された LDAP ユーザー・グループに基づく XClarity Orchestrator で自動的に更新されます。
- ユーザー・グループに割り当てられた役割が変更された場合、役割の変更を有効にするためにユーザーは再度ログインする必要があります。

リソースへのアクセス制御

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。

手順

リソースへのアクセスを制御するには、以下の手順を実行します。

ステップ 1. リソースにアクセスできるユーザーのグループを作成します。

ステップ 2. アクセスを制限するリソースのグループを 1 つ以上作成します。

ステップ 3. ユーザー・グループと 1 つ以上のリソース・グループを含むアクセス制御リストを作成します。

ステップ 4. リソース・ベース・アクセス制御を有効にします。

リソース・ベース・アクセスの有効化

ユーザーがアクセスできるリソースを制限する場合、リソース・ベース・アクセスを有効にします。

このタスクについて

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。

手順

リソース・ベース・アクセス制御を有効にするには、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「**アクセス制御**」をクリックして、「アクセス制御」カードを表示します。

ステップ 2. 「**リソース・ベース・アクセス**」トグルをクリックし、アクセス制御リストを使用してリソース・アクセス制御を有効にします。

アクセス制御リストの作成

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

始める前に

詳細: アクセス制御リストの作成方法

ACL に関連付けるユーザー・グループが定義されていることを確認します (ユーザー・グループの作成 を参照)。

この ACL に関連付けるすべてのリソース・グループが定義されていることを確認します (リソース・グループの作成 を参照)。

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。

手順

アクセス制御リストを作成するには、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「**アクセス制御**」をクリックして、「アクセス制御」カードを表示します。

ステップ 2. 「**追加**」アイコン (⊕) をクリックして、ACL を追加します。「アクセス制御の作成」ダイアログが表示されます

ステップ 3. ACL の名前および説明 (任意) を指定します。

ステップ 4. 「**ユーザー・グループ**」をクリックし、この ACL に追加するユーザー・グループを選択します。

ステップ 5. 「**リソース・グループ**」をクリックし、この ACL に追加するリソース・グループを選択します。

ステップ 6. 「**作成**」をクリックします。

アクセス制御リストが表に追加されます

終了後

このページでは、以下の操作を実行できます。

- 特定の ACL 内のユーザー・グループとリソース・グループを表示するには、その ACL の行の任意の場所をクリックします。
- 選択した ACL のプロパティおよびメンバーシップを変更するには、「**編集**」アイコン (✎) をクリックします。
- 選択した ACL を削除するには、「**削除**」アイコン (🗑) をクリックします。
- ユーザーが特定のリソースのデータにアクセスできない場合、またはアクセスすべきではない特定のリソースのデータにアクセスできる場合は、そのユーザーに関連付けられているアクセス制御リストを特定し、それらのアクセス制御リストにも関連付けられている各リソース・グループのメンバーシップを表示します。問題のリソースがそれらのリソース・グループに含まれているかどうかを確認します。

ディスク・スペースの管理

不要になったファイルを削除することで、Lenovo XClarity Orchestrator が使用するディスク・スペースの大きさを管理できます。

このタスクについて

手順

不要なファイルを削除するには、以下の手順を 1 つ以上実行します。

デバイス・サービス・データ・ファイル

1. Lenovo 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、「**サービス・データ**」タブをクリックして「デバイス・サービス・データ」カードを表示します。
2. 削除するサービス・データ・ファイルを 1 つ以上選択し、「**削除**」アイコンをクリックします。

オペレーティング・システム・イメージ

1. Lenovo XClarity Orchestrator のメニュー・バーで、「**管理**」 → 「**OS デプロイメント**」をクリックしてから、「**OS 管理**」タブをクリックして「OS イメージ」カードを表示します。
2. OS イメージを 1 つ以上選択し、「**削除**」アイコンをクリックします。

ペイロード・ファイルの更新

削除した更新が更新コンプライアンス・ポリシーで使用されていないことを確認します。「適用して有効化」カードでポリシーから更新を削除できます (更新コンプライアンス・ポリシーの作成と割り当て を参照)。

1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング**」 → 「**更新**」をクリックしてから、「**リポジトリー管理**」タブをクリックして、「リポジトリー管理」カードを表示します。
2. 削除する更新パッケージまたは更新ファイルを 1 つ以上選択します。
3. 「**ペイロード・ファイルのみを削除**」アイコンをクリックして、選択済みの各更新のイメージ (ペイロード) ファイルのみを削除します。更新に関する情報 (XML メタデータ・ファイル) はリポジトリーに残り、ダウンロード・ステータスは「未ダウンロード」に変わります。

XClarity Orchestrator 更新

「ダウンロード済み」状態の Orchestrator サーバーの更新を削除できます。テーブルの「**適用済みステータス**」列は、その更新のステータスを示します。

1. XClarity Orchestrator メニュー・バーで、「**保守**」をクリックし、「**Orchestrator サーバーの更新**」タブをクリックすると、「Orchestrator サーバーの更新」カードが表示されます。
2. 削除する更新を 1 つ以上選択し、「**削除**」アイコンをクリックします。削除された更新の「**取得されたステータス**」列が「未ダウンロード」に変わります。

XClarity Orchestratorの再起動

サーバー証明書の再生成時やアップロード時など、特定の状況では、Lenovo XClarity Orchestrator を再起動する必要があります。Web インターフェースから Lenovo XClarity Orchestrator を再起動できます。

始める前に

XClarity Orchestrator を再起動するには、**スーパーバイザー**権限が必要です。

再起動する前に、Orchestrator サーバーのバックアップを検討してください (Orchestrator サーバーのデータのバックアップと復元を参照)。

現在実行されているジョブがないことを確認します。現在実行中のジョブは、再起動プロセス中にキャンセルされます。ジョブ・ログを表示するには、ジョブの監視を参照してください。

再起動プロセス中にジョブが停止され、すべてのユーザーがログオフされて、Orchestrator サーバーへの接続が失われます。Orchestrator サーバーが再起動するまで 15 分以上待ってから (管理対象デバイスの数によって異なります) 再度ログインしてください (XClarity Orchestrator へのログイン)。

XClarity Orchestrator は、再起動すると、各管理対象デバイスのインベントリーを再収集します。ファームウェア更新、構成パターン・デプロイメント、またはオペレーティング・システム・デプロイメントを行う前に、管理対象デバイスの数に応じて 30 ～ 45 分ほど待ちます。

手順

XClarity Orchestrator を再起動するには、以下のいずれかの手順を実行します。

ユーザー・インターフェースから

1. XClarity Orchestrator のメニュー・バーで、「**保守**」 ➡ 「**アプライアンスの再起動**」をクリックします。
2. 「**再起動**」をクリックします。
3. 「**はい**」をクリックします。
4. ブラウザーを更新します。

ハイパーバイザーから

Microsoft Hyper-V

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. 仮想マシンを右クリックし、「**リセット**」をクリックします。

VMware 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**」 ➡ 「**リセット**」をクリックします。
3. 「**コンソール**」タブをクリックします。

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
```

... ...

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。

Orchestrator サーバーのデータのバックアップと復元

Lenovo XClarity Orchestrator には、組み込みのバックアップ機能や復元機能がありません。代わりに、XClarity Orchestrator がインストールされている仮想ホスト・オペレーティング・システムに用意されているバックアップ機能を使用します。

このタスクについて

初期セットアップおよび以下のような重要な構成の変更を行った後は必ず XClarity Orchestrator をバックアップしてください。
- XClarity Orchestrator を更新する前
- ネットワークの変更を行った後
- XClarity Orchestrator のローカル認証サーバーにユーザーを追加した後
- 新しいリソース・マネージャーを管理した後

仮想ホスト用に所定のバックアップおよび復元手順がある場合は、その手順に必ず XClarity Orchestrator が含まれるようにします。

重要：

- バックアップの作成前に、必ず実行中のすべてのジョブを完了し、XClarity Orchestrator をシャットダウンします。
- XClarity Orchestrator を定期的にバックアップします。ホスト・オペレーティング・システムが予期せずにシャットダウンした場合は、ホスト・オペレーティング・システムを再起動した後に XClarity Orchestrator を認証できない場合があります。この問題を解決するには、最後のバックアップから XClarity Orchestrator を復元します。

VMware ESXi ホストでの Orchestrator サーバー・データのバックアップと復元

s Orchestrator サーバーのデータをバックアップから復元する必要が生じる場合があります。VMware ESXi ホストで実行されている XClarity Orchestrator 仮想アプライアンスをバックアップおよび復元する方法は複数あります。通常は、バックアップの作成に使用した方法によって、どの方法で復元するかが決まります。このトピックでは、VMware vSphere Client を使用したバックアップと復元の方法について説明します。

このタスクについて

VMware vCenter Server がインストールされている場合は、VMware vCenter に用意されているバックアップ機能を使用して、XClarity Orchestrator をバックアップすることができます。

VMware vCenter Server がインストールされていない場合は、VMware vSphere Client を使用して XClarity Orchestrator フォルダーから同じデータストア内の別のフォルダーにファイルをコピーすることで、仮想マシンのバックアップを作成できます。また、追加のバックアップ保護用に、別のデータストアや別のホストにファイルをコピーすることもできます。

注：VMware vCenter Server は、この手順を使用したバックアップの実行には必要ありません。

手順

- **XClarity Orchestrator のバックアップ**VMware vSphere Client を使用して XClarity Orchestrator のバックアップを作成するには、以下の手順を実行します。
  1. XClarity Orchestrator をシャットダウンします。
  2. VMware vSphere Client を起動し、XClarity Orchestrator がある ESXi ホストに接続します。
  3. XClarity Orchestrator 用の同じデータストアに新しいフォルダーを作成します。
     a. ナビゲーション・ツリーで ESXi ホストを選択し、右側のウィンドウで「**構成**」タブをクリックします。
     b. 「**ハードウェア**」 ➡ 「**ストレージ**」をクリックします。
     c. XClarity Orchestrator 用のデータストアを右クリックし、「**データストアの参照**」をクリックします。
     d. ルート・フォルダーを選択し、XClarity Orchestrator ファイルのコピーを保存する新しいフォルダーを作成します。
  4. XClarity Orchestrator フォルダーをクリックします。
  5. フォルダー内のファイルをすべて選択し、先ほど作成したバックアップ・フォルダーにコピーします。
  6. XClarity Orchestrator を再起動します。
- **XClarity Orchestrator の復元**前の手順で作成したバックアップを使用して XClarity Orchestrator を復元するには、以下の手順を実行します。
  1. VMware vSphere Client を起動し、XClarity Orchestrator がインストールされている ESXi ホストに接続します。
  2. 左側のナビゲーション・ツリーで XClarity Orchestrator を右クリックし、「**電源**」 ➡ 「**電源オフ**」の順にクリックします。
  3. 再度、左側のナビゲーション・ツリーで XClarity Orchestrator を右クリックし、「**インベントリーから削除**」をクリックします。
  4. XClarity Orchestrator によって使用されるデータストアの XClarity Orchestrator フォルダーのファイルを削除します。
     a. ナビゲーション・ツリーで ESXi ホストを選択し、右側のウィンドウで「**構成**」タブをクリックします。
     b. 「**ハードウェア**」 ➡ 「**ストレージ**」をクリックします。
     c. XClarity Orchestrator 用のデータストアを右クリックし、「**データストアの参照**」をクリックします。
     d. XClarity Orchestrator フォルダーを選択します。
     e. フォルダー内のすべてのファイルを選択し、ファイルを右クリックして、「**選択した項目の削除**」をクリックします。
  5. バックアップ・ファイルが保存されているフォルダーを選択します。
  6. フォルダー内のファイルをすべて選択し、XClarity Orchestrator フォルダーにコピーします。

7. XClarity Orchestrator フォルダーで VMX ファイルを右クリックし、「**インベントリーへの追加**」をクリックします。
8. ウィザードに従って XClarity Orchestrator のデータを追加します。
9. VMware vSphere Client から XClarity Orchestrator を再起動します。
10. VM を移動したかコピーしたかを選択するプロンプトが表示された場合は、「**移動**」を選択します。

    重要：「**コピー**」を選択した場合、VM には元の VM とは異なる UUID が割り当てられます。これにより、VM は新しいインスタンスと同様に動作し、以前に管理対象であったデバイスを表示することはできません。

Microsoft Hyper-V ホストでの Orchestrator サーバー・データのバックアップと復元

Lenovo XClarity Orchestrator Orchestrator サーバーのデータをバックアップから復元する必要が生じる場合があります。Microsoft Hyper-V ホストで実行されている XClarity Orchestrator 仮想アプライアンスをバックアップおよび復元する方法は複数あります。通常は、バックアップの作成に使用した方法によって、どの方法で復元するかが決まります。このトピックでは、Windows Server Backup を使用したバックアップと復元の方法について説明します。

始める前に

以下の手順を実行して、Windows Server Backup が正しくセットアップされていることを確認します。

1. Windows サーバー・マネージャーを起動します。
2. 「**管理**」 ➔ 「**役割と機能の追加**」をクリックします。
3. 「**機能の選択**」ページが表示されるまでウィザードの手順をスキップします。
4. 「**Windows Server Backup**」チェック・ボックスを選択します。
5. ウィザードの手順を完了します。

手順

- **XClarity Orchestrator のバックアップ**Windows Server Backup を使用して XClarity Orchestrator のバックアップを作成するには、以下の手順を実行します。
  1. Windows Server Backup を起動し、「**ローカル バックアップ**」を参照します。
  2. 「操作」ペインで、「**バックアップ (1 回限り)**」をクリックして、バックアップ (1 回限り) ウィザードを起動します。
  3. 「バックアップ オプション」ページで、「**別のオプション**」をクリックし、「**次へ**」をクリックします。
  4. 「バックアップ構成の選択」ページで、「**カスタム**」をクリックし、「**次へ**」をクリックします。
  5. 「バックアップする項目を選択」ページで、「**項目の追加**」をクリックして、「項目の選択」ウィンドウを表示します。
  6. Hyper-V の項目を展開し、XClarity Orchestrator 仮想マシンをクリックして、「**OK**」をクリックします。
  7. 「**次へ**」をクリックして先に進みます。
  8. 「作成先の種類の指定」ページで、バックアップ用のストレージのタイプ (「ローカル ドライブ」または「リモート共有フォルダー」) を選択し、「**次へ**」をクリックします。
  9. 「バックアップ先の選択」または「リモート フォルダーの指定」ページで、バックアップを保存する場所を指定し、「**次へ**」をクリックします。
  10. 「**バックアップ**」をクリックして、バックアップ・プロセスを開始します。
- **XClarity Orchestrator の復元**前の手順で作成したバックアップを使用して XClarity Orchestrator を復元するには、以下の手順を実行します。
  1. Windows Server Backup を起動し、「**ローカル バックアップ**」を参照します。

2. 「操作」ペインで、「**回復**」をクリックして、回復ウィザードを起動します。
3. 「はじめに」ページで、バックアップが保存されている場所を指定し、「**次へ**」をクリックします。
4. 「バックアップの日付の選択」ページで、復元するバックアップを選択し、「**次へ**」をクリックします。
5. 「回復の種類の選択」ページで、「**Hyper-V**」オプションを選択し、「**次へ**」をクリックします。
6. 「回復する項目の選択」ページで、「Hyper-V」を展開し、「XClarity Orchestrator仮想マシン」を選択します。その後、「**次へ**」をクリックします。
7. 「回復オプションの指定」ページで、VM を元の場所に回復するように選択し、「**次へ**」をクリックします。
8. 「確認」ページで、「**回復**」をクリックします。仮想マシンが復元され、Hyper-V に登録されます。
9. Hyper-V マネージャーから XClarity Orchestrator を再起動します。

第 3 章　リソースおよびアクティビティの監視

Lenovo XClarity Orchestrator を使用して、管理対象デバイスの資産のインベントリー、ファームウェアと構成の適合性、ヘルス・ステータス、およびイベント履歴を監視できます。

環境の概要の表示

ダッシュボードは Lenovo XClarity Orchestrator のハブであり、ここからユーザーにとって重要な情報にアクセスできます。ここに表示されるレポート・カードから、ご使用の環境におけるリソースとアクティビティのステータス (デバイスのヘルス、適合性、アラートなど) の要約を確認できます。

ダッシュボードにアクセスするには、XClarity Orchestrator のメニュー・バーで、「**ダッシュボード** ()」をクリックします。

「**マネージャーを選択**」ドロップダウン・メニューで、要約の範囲を特定のリソース・マネージャーや特定のリソース・グループで管理されているデバイスのみに変更できます。

ダッシュボードのリンクされている統計のいずれかをクリックすると、その条件に適合するデータのフィルタリング・リストを表示できます。

保証

「保証」カードには、以下のデータを含めて、管理対象デバイスの保証期間が要約されています。
- 保証が切れているデバイスの数
- 保証が有効なデバイスの数
- 保証データが利用できないデバイスの数

サービス・チケット

「サービス・チケット」カードには、以下のデータを含む、管理対象の要約が表示されます。
- アクティブなサービス・チケットの合計数
- 開いているサービス・チケットの数
- 進行中のサービス・チケットの数
- 保留中のサービス・チケットの数
- クローズされたサービス・チケットの数
- 他の状態のサービス・チケットの数

ファームウェアのコンプライアンス

「ファームウェアのコンプライアンス」カードには、以下のデータを含む、XClarity Orchestrator の管理対象デバイスに割り当てられたファームウェア・コンプライアンス・ポリシーに従った適合性の要約が表示されます。
- ポリシーに*適合していない*デバイスの数
- ポリシーに適合しているデバイスの数
- ファームウェア・コンプライアンス・ポリシーが*割り当てられていない*デバイスの数
- 適合性の対象になっていないデバイスの数
- 割り当てられたポリシーに対するコンプライアンスが確認されているデバイスの数

注：このデータは、XClarity Orchestrator によって割り当てられたポリシーに基づいて、ファームウェア・コンプライアンスを表します。Lenovo XClarity Administrator リソース・マネージャーによって割り当てられたポリシーを表すものではありません。

構成の適合性

「構成のコンプライアンス」カードには、以下のデータを含む、管理対象デバイスのサーバー構成パターンのコンプライアンスに関する情報が要約で表示されます。

- 割り当てられたパターンに適合して*いない*デバイスの数
- 割り当てられたパターンに適合しているデバイスの数
- パターンが割り当てられて*いない*デバイスの数
- 構成コンプライアンスの確認が進行中のデバイスの数
- パターン・デプロイメントを完了するために手動で再起動する必要があるデバイス数 (再起動を保留中)
- 最後のパターン・デプロイメントが失敗したデバイスの数

注：このデータは、XClarity Orchestratorによって割り当てられたパターンに基づくすべてのデバイスのサーバー構成のコンプライアンスを表します。管理対象の XClarity Administrator リソース・マネージャーによって割り当てられたパターンを表すものではありません。

セキュリティー修正

セキュリティー修正カードには、利用可能な共通脆弱性識別子 (CVE) を持つ管理対象デバイスの数を、最も高い CVE 重大度別にまとめた要約が表示されます。

- 少なくとも重大な脆弱性があるデバイスの数
- 高、中、または低の脆弱性が最低 1 つ以上存在するが、重大な脆弱性が存在しないデバイスの数
- 既知の脆弱性がなく、保護されているデバイスの数

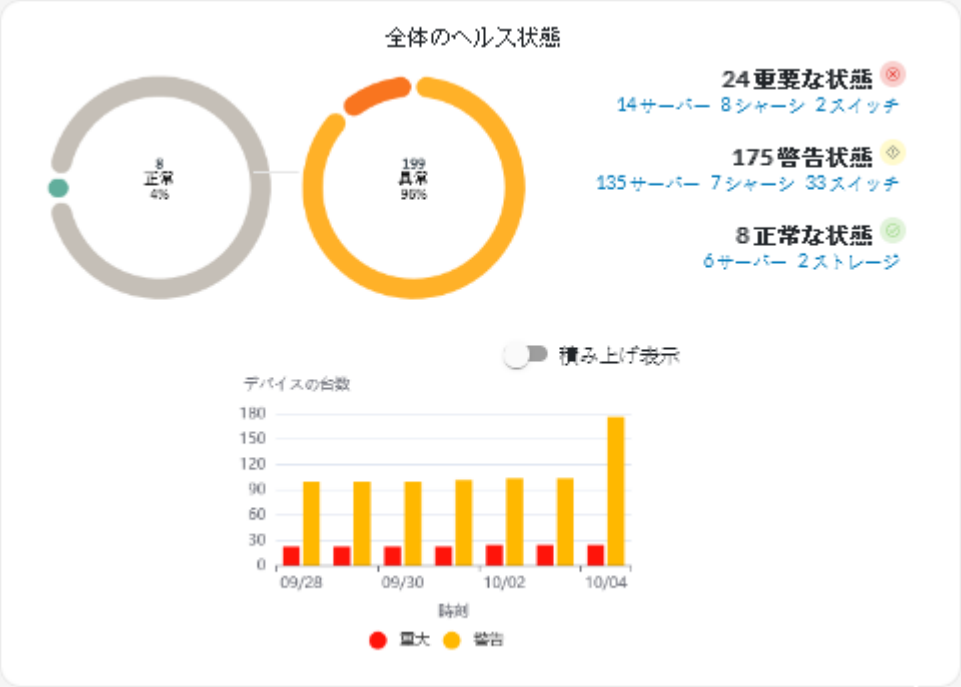
ファームウェアの年数

「ファームウェアの年数」カードには、コンポーネントの種類ごとのファームウェアの経過時間の要約が表示されます。

- 各コンポーネントタイプに対して 2 年以上前のファームウェア数
- 各コンポーネント・タイプに対して 1 ～ 2 年前のファームウェア数
- 各コンポーネント・タイプに対して 6 か月～ 1 年前のファームウェア数
- 各コンポーネントタイプに対して 6 か月未満のファームウェア数

全体のヘルス状況

「全体のヘルス・ステータス」カードには、ご使用環境内の管理対象デバイスが現時点で正常か異常かが要約表示されます。



このカードには、以下のデータが含まれています。

- 正常な状態 (正常) のデバイスと、異常な状態 (クリティカル、警告、不明) のデバイスの比率を表す円形グラフ

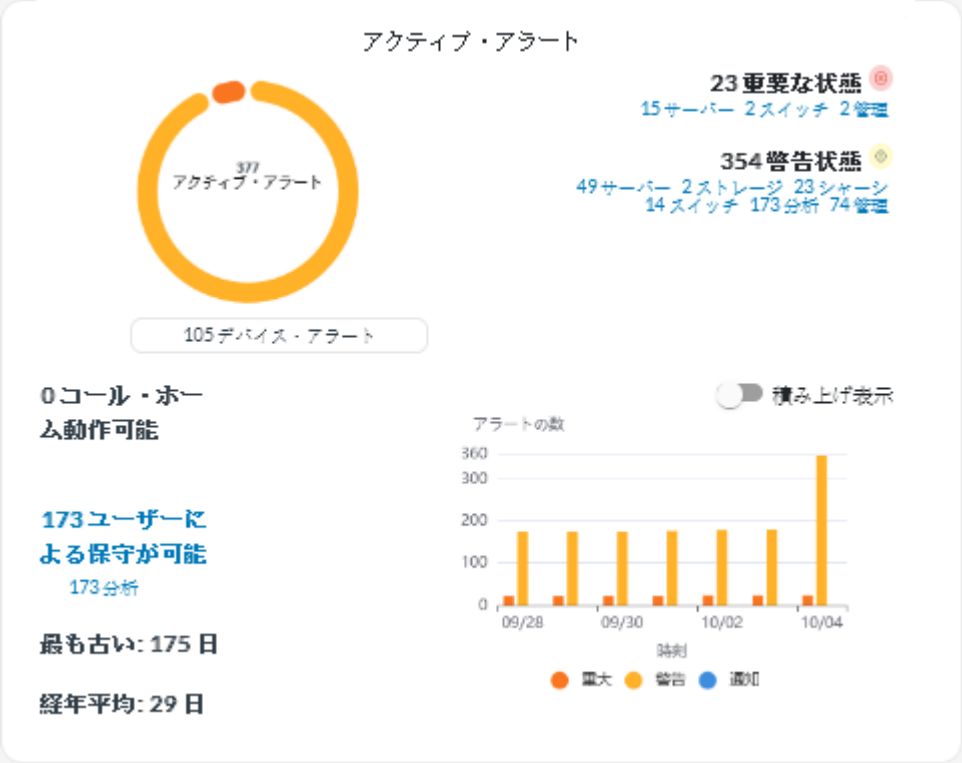
  ヒント: 円グラフの各カラー・バーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。
- 正常なデバイスと異常なデバイスの合計数とパーセント
- 現在クリティカル、警告、正常、不明それぞれの状態にある各タイプのデバイスの数

  ヒント: 特定の状態にあるデバイスの数をクリックすると、基準に一致するデバイスのフィルタリングされたリストが表示されたページが開きます。
- 異常な状態のデバイスの数を時系列で表す折れ線グラフ

  ヒント: 棒グラフの各色のバーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。

アクティブ・アラート

「デバイスのアクティブ・アラート」カードには、管理対象デバイスによって生成されたアクティブなアラートが要約表示されます。



このカードには、以下のデータが含まれています。

- 各重大度 (クリティカル、警告、通知、不明) のアクティブなアラートの比率を表す円グラフ

  ヒント: 円グラフの各色のバーは、特定の重大度に設定されているアラートの数を示しています。各カラー・バーをマウスでポイントすると、重大度に関する詳細情報がわかります。
- アクティブなアラートの合計数
- アクティブなアラートがあるデバイスの数
- 各重大度のアクティブ・アラートの合計数、および各重大度のアクティブ・アラートが生じている各タイプのデバイス数

  ヒント: 特定の状態にあるデバイスの数をクリックすると、基準に一致するデバイスのフィルタリングされたリストが表示されたページが開きます。
- 異常な状態のデバイスの数を時系列で表す折れ線グラフ

  ヒント: 棒グラフの各カラー・バーは、特定の重大度に設定されているアラートの数を示しています。各カラー・バーをマウスでポイントすると、重大度に関する詳細情報がわかります。
- Lenovo サポート・センター (コール・ホーム) を使用してサービス・チケットを開いたアクティブ・アラートの数
- ユーザー操作を必要とする (ユーザーが保守できる) アクティブ・アラートの合計数、およびアクティブでユーザー保守可能なアラートを持つ各タイプのデバイスの数
- 最も古いアクティブ・アラートの経過日数
- すべてのアクティブ・アラートの平均経過時間

リソース・マネージャーの状態と詳細の表示

各リソース・マネージャーのタイプ、バージョン、ステータス、および接続を表示できます。

このタスクについて

「**ヘルス・ステータス**」列には、リソース・マネージャーの全体的なヘルスが表示されます。ヘルスの状態は以下のとおりです。

- (○) 正常
- (○) 警告
- (⊗) クリティカル

手順

リソース・マネージャーの詳細を表示するには、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、「リソース・マネージャー」カードを表示します。

終了後

「リソース・マネージャー」カードから、以下の操作を実行できます。

- リソース・マネージャーを接続するには、「**接続**」アイコン (○) をクリックします (リソース・マネージャーの接続 を参照)。
- 選択済みリソース・マネージャーを切断して削除するには、「**削除**」アイコン (🗑) をクリックします。

  注：XClarity Orchestrator がリソース・マネージャーに接続できない場合 (たとえば、資格情報が期限切れの場合や、ネットワークに問題がある場合) は、「**強制切断**」を選択します。

  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・マネージャーを削除すると、そのリソース・マネージャーが管理しているデバイスもすべて削除されます。これには、デバイス・インベントリー、ログ、メトリック・データ、および分析レポートが含まれます。
- すべてのリソース・マネージャーまたは選択したリソース・マネージャーのステータスの要約を表示するには、XClarity Orchestrator のメニュー・バーで「**ダッシュボード** (⊞)」をクリックします。「**マネージャーを選択**」ドロップダウン・メニューで、1 つのリソース・マネージャーまたはリソース・グループに範囲を絞り込むことができます。

デバイスの状態の表示

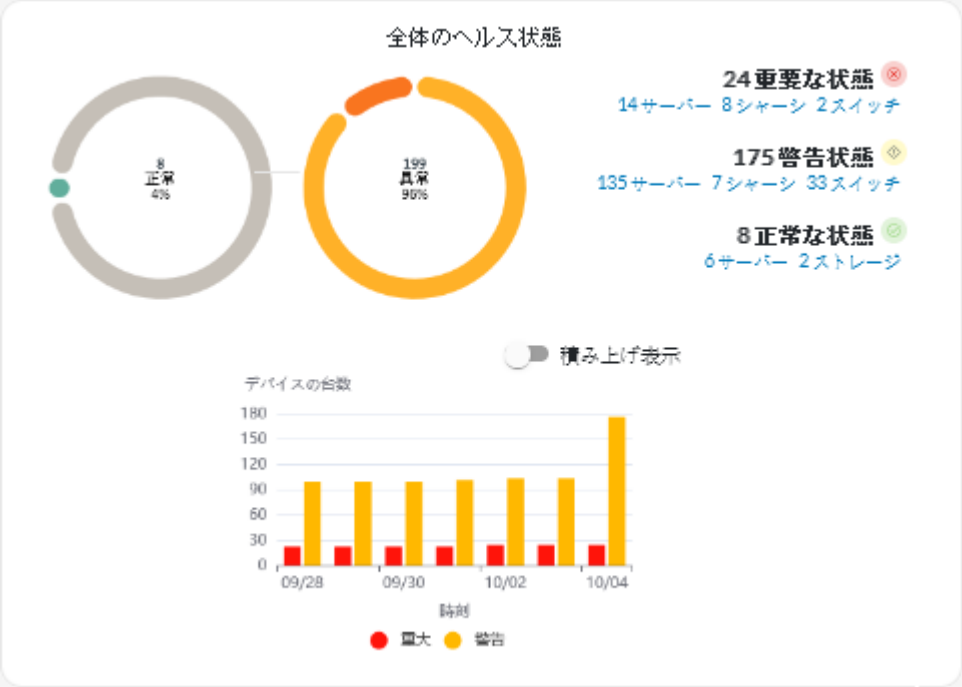
すべてのリソース・マネージャーで管理されているすべてのデバイスのステータスを表示できます。

手順

管理対象デバイスのステータスを表示するには、以下の手順を実行します。

- **すべてのデバイスのステータス要約**の XClarity Orchestrator のメニュー・バーから、「**ダッシュボード**()」をクリックすると、「ダッシュボード」カードに、すべての管理対象デバイスとその他のリソースの概要とステータスが表示されます (環境の概要の表示 を参照)。

  「**マネージャーを選択**」ドロップダウン・メニューで、要約の範囲を特定のリソース・マネージャーや特定のリソース・グループで管理されているデバイスのみに変更できます。



  円グラフおよび棒グラフの各カラー・バーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。各状態のデバイスの数をクリックして、その条件に一致するすべてのデバイスのリストを表示することもできます。

- **特定のタイプのデバイスすべてのステータス**アクティブ・アラート全体の要約を表示するには、XClarity Orchestrator のメニュー・バーで「**リソース**」() をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。たとえば「**サーバー**」を選択すると、すべてのラック、タワー、および高密度サーバーと、シャーシ内のすべての Flex System および ThinkSystem サーバーのリストが表示されます。

  「**分析の基準**」ドロップダウン・リストからデバイスのプロパティーに基づく要約の範囲を変更できます。
  - **マシン・タイプ/モデル**。(デフォルト) このレポートでは、マシン・タイプ・モデル (MTM) ごとにデバイス・ヘルスが要約されます。
  - **マシン・タイプ**このレポートでは、マシン・タイプごとにデバイス・ヘルスが要約されます。
  - **製品名**。このレポートでは、製品ごとにデバイス・ヘルスが要約されます。

XClarity Orchestrator は、特定の基準に基づいてデバイス・ヘルスを要約します。各要約には、以下の情報が含まれます。

- 異常なデバイスの合計数、および各異常状態のデバイスのパーセンテージ (クリティカル、警告、および不明) を示す円グラフ。

  円グラフの各カラー・バーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。
- 指定された日数における、各ヘルス状態の 1 日あたりのデバイス数を示す折れ線グラフ。

  折れ線グラフの各色のバーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。
- 特定の日の、異常がある各タイプのデバイス数。デフォルトでは現在の日が表示されています。日を変更するには、折れ線グラフでそれぞれの日をポイントします。

- **特定のデバイスのステータス**XClarity Orchestrator のメニュー・バーで「**リソース**」 () をクリックし、デバイス・タイプをクリックすると、該当するタイプのすべてのデバイスのテーブル・ビューを含むカードが表示されます。たとえば「**サーバー**」を選択すると、すべてのラック、タワー、および高密度サーバーと、シャーシ内のすべての Flex System および ThinkSystem サーバーのリストが表示されます。

「**ステータス**」列には、デバイス全体のヘルスが表示されます。ヘルスの状態は以下のとおりです。デバイスが異常な状態にある場合は、アラート・ログを使用して問題を特定し、解決します (アクティブなアラートの監視を参照)。

– (◦) 正常
– (◦) 警告
– (◦) クリティカル

「**接続**」列には、デバイスと XClarity Orchestrator の間の接続ステータスが表示されます。接続の状態は以下のとおりです。

– ( ) オフライン
– ( ) オフライン管理対象
– (◦) オンライン
– ( ) 一部
– ( ) 保留中

「**電源**」列には、電源のステータスが表示されます。電源状態は以下のとおりです。

– (◦) オン
– ( ) オフ

「**相談**」列には、各サーバーに関連するオンライン顧客相談 (技術的なヒント) の数が表示されます。番号をクリックすると、デバイスの詳細ページに「相談」カードが表示され、各相談の概要やリンクなど、オンライン顧客相談の一覧が表示されます。リンクをクリックすると、その相談の詳細が記載された Web ページが開きます。

終了後

「デバイス」カードでは、以下の操作を実行できます。

- 選択したデバイスをグループに追加するには、「**すべての操作**」 ➞ 「**グループにアイテムを追加**」の順にクリックします。
- 「**レポート・フォワーダーの作成**」アイコン ( ) をクリックして、特定のデバイス・タイプに関するレポートを 1 つ以上のメールアドレスに転送します。レポートは、現在テーブルに適用されているデータ・フィルターを使用して送信されます。表示および非表示されたテーブルのすべての列がレポートに含まれます。詳しくは、レポートの転送を参照してください。
- 「**レポート・フォワーダーに追加**」アイコン ( ) をクリックして、テーブルに現在適用されているデータ・フィルターを使用して、特定のレポート・フォワーダーに特定のデバイス・タイプに関するレポートを追加します。レポート・フォワーダーにそのデバイス・タイプに関するレポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。

デバイスの詳細の表示

各デバイスに関する詳細情報 (デバイスのヘルスとステータス、インベントリー、アラートとイベント、システム・メトリックス、およびファームウェアの全体的な要約など) を表示できます。

手順

デバイスの詳細を表示するには、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** ( )」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。

ステップ 2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。

ステップ 3. 以下の 1 つ以上の操作を実行してください。

各カードの詳細は、デバイス・タイプによって異なる場合があります。

- 「**要約**」をクリックして、デバイス情報、ステータス、インベントリーのヘルス、OS 情報、システム・メトリック、サービス・チケット、保証など、デバイス全体の要約を表示します。このページには、デバイスで実行できる操作 (電源操作の実行、サービス・データの収集、リモート制御セッションの起動など) を一覧で表示する「**クイック操作**」カードも含まれています。このページでは、前面オペレーター・パネルの各 LED の状態が表示されます。
  - **電源 LED**
    - **オン** (●)。装置の電源が入っています。
    - **オフ** ( )。装置の電源が入っていません。
  - **ロケーション LED**
    - **オン** (■)。コントロール パネルのロケーション LED が点灯します。

  - **点滅** (◉)。コントロール パネルのロケーション LED が点灯または点滅します。
  - **オフ** ( )。コントロール パネルのロケーション LED は点灯しません。
- **障害 LED**
  - **オン** (◉)。コントロール パネルの障害 LED が点灯します。
  - **オフ** ( )。コントロール パネルの障害 LED は点灯しません。

- 「**インベントリー**」をクリックして、デバイスのハードウェア・コンポーネント (プロセッサー、メモリー・モジュール、ドライブ、パワー・サプライ、ファン、PCI デバイス、システム・ボードなど) の詳細を表示します。

  注：

  - インベントリーは、ThinkSystem DS2200、Lenovo Storage S2200 と S3200、および Flex System V7000 ストレージ・ノードのストレージ・デバイスではサポート*されていません*。
  - ファームウェア詳細は、ThinkSystem DS4200 と DS6200、および Lenovo Storage DX8200C、DX8200D、DX8200N のストレージ・デバイスでは*使用できません*。
- 「**アラート・ログ**」をクリックすると、そのデバイスのアクティブ・アラートのリストとアラート分析が表示されます (アクティブなアラートの監視を参照)。
- 「**イベント・ログ**」をクリックすると、デバイスのイベント・リストが表示されます (イベントの監視を参照)。
- 「**ファームウェア**」をクリックすると、そのデバイスとデバイス・コンポーネントの現在のファームウェア・レベルのリストが表示されます。
- 「**サービス**」をクリックすると、デバイスのサービス・データ・アーカイブおよびサービス・チケットに関する情報が表示されます。
- 「**使用率**」をクリックして、ThinkAgile および ThinkSystem デバイスの時間経過に伴うシステム使用率、温度、および電力のメトリックを表示します。
- 「**相談**」をクリックして、各相談の概要とリンクを含むオンライン顧客相談の一覧を表示します。リンクをクリックすると、その相談の詳細が記載された Web ページが開きます。

終了後

このページでは、デバイスに対して、要約と詳細情報の表示に加えて以下の操作も実行できます。

- 「**要約**」タブからベースボード管理コントローラーの Web インターフェースを起動するには、デバイスのメイン IP アドレスをクリックします。
- 「**要約**」タブからデバイスの Web インターフェースを起動するには、「IP アドレス」をクリックします。
- 「**要約**」タブからデバイスを管理しているリソース・マネージャーの Web インターフェースを起動するには、リソース・マネージャー名または IP アドレスをクリックします。

インフラストラクチャー・リソースの状態と詳細の表示

Schneider Electric EcoStruxure IT Expert リソース・マネージャーで管理される、データ・センターのインフラストラクチャー・リソース (PDU および UPS など) に関する状態と詳細情報を表示できます。

始める前に

「**ステータス**」列には、インフラストラクチャー・リソース全体の正常性が表示されます。ヘルスの状態は以下のとおりです。インフラストラクチャー・リソースが異常な状態にある場合は、アラート・ログを使用して問題を特定し、解決します (アクティブなアラートの監視を参照)。

- (◉) 正常

- (⟐) 警告
- (⊗) クリティカル

手順

- **特定のインフラストラクチャー・リソースの状態**インフラストラクチャー・リソースの状態を表示するには、XClarity Orchestrator のメニュー・バーで、「**リソース**」(⊗) ➡ 「**インフラストラクチャー**」の順にクリックし、「インフラストラクチャー」カードを表示します。インフラストラクチャー・リソースが異常な状態にある場合は、アラート・ログを使用して問題を特定し、解決します (アクティブなアラートの監視を参照)。

- **特定のインフラストラクチャー・リソースの詳細**
  1. XClarity Orchestrator のメニュー・バーで、「**リソース**」(⊗) ➡ 「**インフラストラクチャー**」の順にクリックして、「インフラストラクチャー」カードを表示します。
  2. インフラストラクチャー・リソースの行をクリックすると、そのリソースの要約カードが表示されます。
  3. 以下の 1 つ以上の操作を実行してください。
     - 「**要約**」をクリックして、デバイス情報、状態など、リソース全体の要約を表示します。
     - 「**アラート・ログ**」をクリックすると、リソースのアクティブ・アラートとアラート分析の一覧が表示されます (アクティブなアラートの監視を参照)。
     - 「**イベント・ログ**」をクリックすると、リソースのイベント・リストが表示されます (イベントの監視を参照)。
     - リソース 内のセンサーのリストを表示するには、「**センサー**」をクリックします。センサー・カードからセンサーの最新の測定値を確認できます。または、1 つ以上のセンサーを選択してか

ら「**グラフ**」アイコン ( ) をクリックすると、選択した各センサーの経時的な折れ線グラフを表示できます。同じ単位 (ワットやアンペアなど) のセンサーは同じグラフに表示されます。

注：Schneider Electric EcoStruxure IT Expertでは、センサーのデータを 5 分ごとに収集し、XClarity Orchestrator でこのデータを 1 時間ごとに同期します。現在、XClarity Orchestrator は、直近 60 分間のデータのみ保存します。

終了後

このページでは、インフラストラクチャー・リソースに関する要約と詳細情報の表示に加えて、以下の操作も実行できます。

- 「**要約**」タブから特定のインフラストラクチャー・リソースの Web インターフェースを起動するには、リソースの IP アドレスをクリックします。

ジョブの監視

*ジョブ*は、バックグラウンドで実行される長時間実行タスクです。Lenovo XClarity Orchestrator によって開始されているすべてのジョブのログを表示することができます。

このタスクについて

長時間実行されるタスクが複数のリソースをターゲットとする場合は、リソースごとに個別のジョブが作成されます。

ジョブ・ログで各ジョブのステータスと詳細を確認できます。ジョブ・ログには、最大で 500 件のイベントまたは 1 GB まで含めることができます。最大サイズに達すると、最も古い正常に完了したジョブが削除されます。ログに正常に完了したジョブがない場合、最も古い警告ありで完了したジョブが削除されます。ログに正常に完了したまたは警告ありで完了したジョブがない場合、最も古いエラーありで完了したジョブが削除されます。

注：24 時間以上実行されているジョブは停止され、期限切れ状態になります。

手順

ジョブを表示するには、以下の 1 つ以上の手順を実行します。

- **スケジュール・ジョブの表示**XClarity Orchestrator のメニュー・バーで、「**モニター**」( ) → 「**ジョブ**」をクリックし、「**スケジュール・ジョブ**」タブをクリックして「スケジュール・ジョブ」カードを表示します。このカードには、各スケジュール・ジョブに関する情報 (ステータス、ジョブが実行されるようにスケジュールされたタイムスタンプ、ジョブが開始されたタイムスタンプなど) がリストされます。
- **ジョブの表示**XClarity Orchestrator のメニュー・バーで、「**監視** ( )」 → 「**ジョブ**」をクリックして、「ジョブ」カードを表示します。このカードには、状況、進行状況、開始タイムスタンプと終了タイムスタンプ、およびターゲット・リソースなど、各ジョブに関する情報が一覧表示されています。

ジョブに関する詳細情報を表示するには、テーブルでそのジョブの行をクリックします。ジョブ内の各サブタスクに関する情報 (ステータス、進行状況、開始タイムスタンプと終了タイムスタンプ、ターゲット・デバイス、およびジョブ・ログなど)が一覧表示されたカードが表示されます。

終了後

「ジョブ」カードから、以下の操作を実行できます。

- *完了した*または*有効期限が切れた*ジョブまたはサブタスクを選択し、「**削除**」(🗑) アイコンをクリックして、完了したまたは有効期限が切れたジョブまたはサブタスクをジョブ・ログから削除する。

アクティブなアラートの監視

アラートは、調査とユーザー操作を必要とするハードウェアまたは Orchestrator イベントの状態です。Lenovo XClarity Orchestrator は、リソース・マネージャーを非同期的にポーリングし、それらのマネージャーから受信したアラートを表示します。

このタスクについて

ローカル・リポジトリーに保存されるアクティブなアラートの数に制限はありません。

アラート・カードで、すべてのアクティブ・アラートのリストを表示できます。

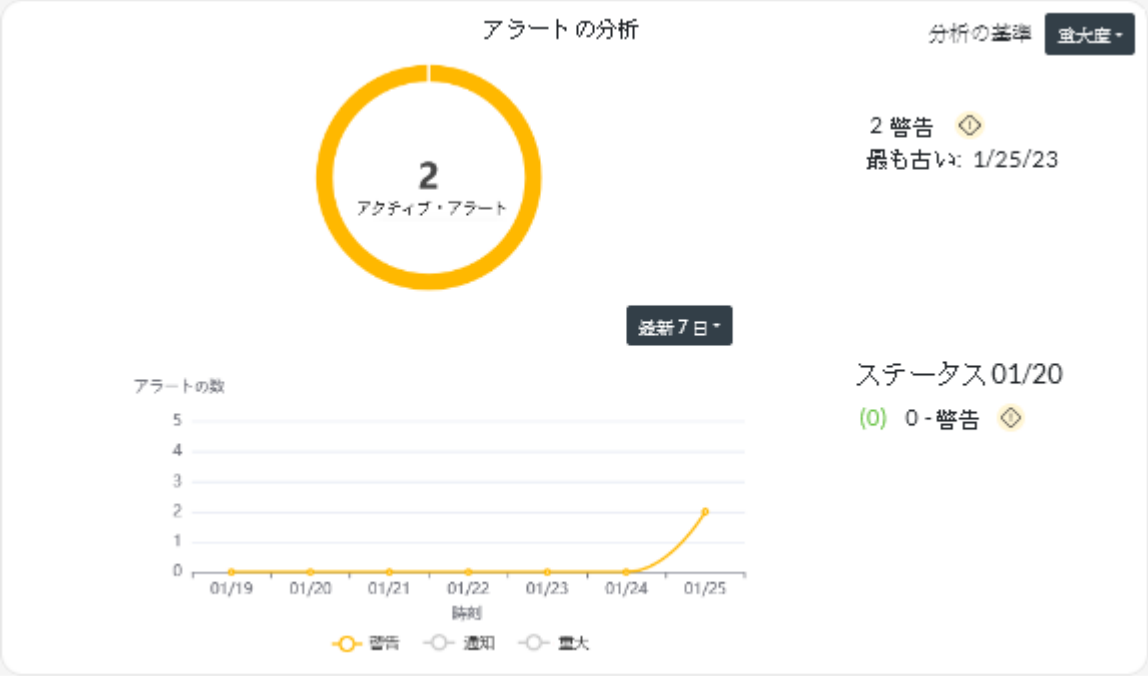
「**重大度**」列には、アラートの重大度が示されます。以下の重大度が使用されます。

- (🛈) **通知**。操作は不要です。
- (⚠) **警告**。操作を遅延させることができます。または操作は不要です。
- (⊗) **クリティカル**。即時操作が必要です。

「**保守容易性**」列には、デバイスにサービスが必要かどうかと、そのサービスを通常だれが実行するかが表示されます。保守容易性には以下のタイプがあります。

- **なし**。保守を必要としない通知アラートです。
- (👤) **ユーザー**。問題を解決するための回復アクションを実行します。
- (🏢) **サポート**。コール・ホームが関連するデバイスを管理するXClarity Orchestratorまたはリソース・マネージャーで有効になっている場合、通常、アラートは Lenovo サポート・センターに送信されます。ただし、そのデバイスに対して同じアラート ID のオープン・サービス・チケットがすでに存在する場合は除きます (コール・ホームを使用してサービス・チケットを自動的に開く XClarity Orchestrator オンライン・ドキュメント を参照)。コール・ホームが有効になっていない場合は、サービス・チケットを手動で開いて問題を解決することをお勧めします (Lenovo サポート・センターでサービス・チケットを手動で開く XClarity Orchestrator オンライン・ドキュメント を参照)。

アクティブなアラートが存在する場合、アラートの統計が「アラートの分析」カードに表示されます。現在の日付および指定された期間を通じた重大度、発信元、リソース、および保守容易性について、アラート統計を確認できます (アクティブなアラートの分析 を参照)。



手順

アクティブなアラートを表示するには、以下の 1 つ以上の手順を実行します。

- **すべてのアクティブ・アラートの表示**XClarity Orchestrator のメニュー・バーで、「**監視**」(📈) → 「**アラート**」をクリックして、「アラート」カードを表示します。

  特定のアラートの詳細を表示するには、「**アラート**」列の説明をクリックします。アラート、説明、およびリカバリー操作のソースに関する情報がポップアップで表示されます。
- **特定のデバイスに関するアクティブ・アラートの表示**
  1. XClarity Orchestrator のメニュー・バーで「**リソース** (⚙)」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。
  2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。

3. 「**アラート・ログ**」をクリックすると、そのデバイスのアクティブ・アラートのリストと「アラート分析」カードが表示されます。特定のアラートの詳細を表示するには、「**アラート**」列の説明をクリックします。アラート、説明、およびリカバリー操作のソースに関する情報がポップアップで表示されます。

イベントの監視

Lenovo XClarity Orchestrator から、すべてのリソース・イベントと監査イベントの履歴リストにアクセスできます。

詳細: 特定のデバイス・イベントを監視する方法

このタスクについて

*リソース・イベント*は、管理対象デバイス、リソース・マネージャー、または XClarity Orchestrator で発生したハードウェアまたは Orchestrator の状態を識別します。これらの監査イベントを使用して、ハードウェアおよび Orchestrator サーバーに関連する問題の追跡と分析を行うことができます。

*監査イベント*は、リソース・マネージャーまたは XClarity Orchestrator から実行されたユーザー・アクティビティの記録です。これらの監査イベントを使用して、認証関連の問題の追跡と分析を行うことができます。

イベント・ログには、リソース・イベントと監査イベントの両方が含まれています。また、すべてのソースから最大 10 万イベントを含めることができます。1 つのリソース・マネージャーとその管理対象デバイスからは、最大 5 万のイベントを記録できます。1 つの管理対象デバイスからは、最大 1,000 のイベントを記録できます。イベント数が最大に達すると、次のイベントを受信したときに最も古いイベントが破棄されます。

「**重大度**」列には、イベントの重大度が示されます。以下の重大度が使用されます。

- (◦) **通知**。操作は不要です。
- (◦) **警告**。操作を遅延させることができます。または操作は不要です。
- (◦) **クリティカル**。即時操作が必要です。

「**保守容易性**」列には、デバイスにサービスが必要かどうかと、そのサービスを通常だれが実行するかが表示されます。保守容易性には以下のタイプがあります。

- **なし**。保守を必要としない通知アラートです。
- (◦) **ユーザー**。問題を解決するための回復アクションを実行します。
- (◦) **サポート**。コール・ホームが関連するデバイスを管理する XClarity Orchestrator またはリソース・マネージャーで有効になっている場合、通常、アラートは Lenovo サポート・センターに送信されます。ただし、そのデバイスに対して同じアラート ID のオープン・サービス・チケットがすでに存在する場合は除きます (コール・ホームを使用してサービス・チケットを自動的に開く XClarity Orchestrator オンライン・ドキュメント を参照)。コール・ホームが有効になっていない場合は、サービス・チケットを手動で開いて問題を解決することをお勧めします (Lenovo サポート・センターでサービス・チケットを手動で開く XClarity Orchestrator オンライン・ドキュメント を参照)。

手順

イベントを表示するには、以下の 1 つ以上の手順を実行します。

- **すべてのリソースまたは監査イベントの表示**XClarity Orchestrator のメニュー・バーで、「**監視** (◦)」 ➡ 「**イベント**」をクリックして、「イベント」カードを表示します。次に、「**リソース・イベント**」タブまたは「**監査イベント**」タブをクリックして、ログ項目を表示します。

- **特定のデバイスに関するリソースまたは監査イベントの表示**
  1. XClarity Orchestrator のメニュー・バーで「**リソース** ()」をクリックし、デバイス・タイプ(「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。
  2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。
  3. 「**イベント・ログ**」タブをクリックして、そのデバイスの「イベント」ページを表示します。

アラートとイベントの除外

特定のイベントおよび関心のないアクティブなアラートがある場合、そのイベントとアクティブなアラートは、イベントとアラートが表示されているすべてのページおよび要約から除外できます。除外イベントとアラートはログに残りますが、ログ・ビューやリソースの状態など、イベントとアラートが表示されているすべてのページで非表示になります。

このタスクについて

除外されたアラートは、構成を設定したユーザーだけでなく、すべてのユーザーに対して非表示になります。

関連するアラートがあるイベントを除外すると、そのアラートも除外されます。

手順

アラートおよびイベントを除外するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator メニュー・バーで、「**監視** (📈)」 → 「**アラート**」 または 「**監視** (📈)」 → 「**イベント**」をクリックして、「アラート」または「イベント」のカードを表示します。

ステップ 2. 除外するアラートまたはイベントを選択し、「**除外**」アイコン (⊘) をクリックします。「アラートの除外」またはた「イベントの除外」ダイアログが表示されます。

ステップ 3. 以下のいずれかのオプションを選択します。

- 「**選択したイベントをすべてのデバイスから除外する**」。選択したイベントをすべての管理対象デバイスから除外します。
- 「**選択済みインスタンスの範囲に含まれるデバイスのイベントのみを除外する**」。選択したイベントを、その適用先の管理対象デバイスから除外します。

ステップ 4. 「**保存**」をクリックします。

終了後

イベントを除外すると、XClarity Orchestrator では、指定した情報に基づいて除外ルールが作成されます。

- 除外ルールおよび除外イベントや除外アラートのリストを表示するには、「**除外を表示**」アイコン (⊘) をクリックして、「除外アラート」ダイアログまたは「除外イベント」ダイアログを表示します。「**除外ルール**」タブをクリックして除外ルールを表示するか、「**除外アラート**」タブまたは「**除外イベント**」タブをクリックして除外アラートや除外イベントを表示します。

- ログから除外されたイベントを復元するには、該当する除外ルールを削除します。除外ルールを削除するには、「**除外を表示**」アイコン (⊘) をクリックして「除外アラート」ダイアログまたは「除外イベント」ダイアログを表示し、復元する除外ルールを選択して、「**削除**」アイコン (🗑) をクリックします。

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

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

手順

データを転送するには、以下の手順を実行します。

ステップ 1. **フォワーダーの宛先を作成します。**

*フォワーダーの宛先*は、複数のデータ・フォワーダーで使用できる共通の構成です。フォワーダーの宛先は、特定のタイプのフォワーダーにおいてデータを送信する宛先を識別します。

ステップ 2. **イベント・フィルターとリソース・フィルターを作成します (イベント・フォワーダーのみ)。**

必要に応じて、共通の*データ転送フィルター*を複数のデータ・フォワーダーに割り当てることができます。これらのフィルターは、特定の基準を定義し、どのリソースのイベントが転送されるかを決定するために使用されます。

データ・フォワーダーにフィルターを割り当てない場合、すべてのリソースのすべてのイベントが、選択したフォワーダーの宛先に転送されます。

ステップ 3. **データ・フォワーダーを作成して有効にします。**

データ・フォワーダーを作成して有効にし、特定の外部アプリケーションにイベント・データを転送できます。作成するフォワーダーのタイプに適用されるフォワーダーの宛先を選択する必要があります。

データ転送フィルターの作成

複数のフォワーダーで使用できる共通の*データ転送フィルター*を定義して、特定の条件に一致する転送データをトリガーできます。

このタスクについて

以下のタイプのフィルターを作成できます。

- *イベント・フィルター*では、特定のイベント・コードまたはプロパティ (イベント・クラス、イベント重大度、サービス・タイプなど) に一致するイベントのみが転送されます。
  - すべてのコードおよびプロパティがすべてのイベント・ソースに適用されます。
  - クラス・プロパティが選択されていない場合は、すべてのクラス・プロパティが一致します。
  - 保守可能なプロパティが選択されていない場合は、すべての保守可能なプロパティが一致します。
  - 重大度プロパティが選択されていない場合は、すべての重大度プロパティが一致します。
  - イベント・コードが指定されていない場合は、すべてのイベント・コードが一致します。
- *リソース・フィルター*は、特定のリソース (XClarity Orchestrator、リソース・マネージャー、およびデバイス) によって生成されたデータを転送します。1 つ以上のリソース・グループを選択して、リソースのサブセットを選択することができます。
  - リソース・タイプが無効である場合、該当するリソース・タイプからのデータは転送されません。
  - リソース・タイプが有効である場合で、グループが選択されていないときは、該当するリソース・タイプからのすべてのデータが転送されます。
  - リソース・タイプが有効である場合で、1 つ以上のグループが選択されているときは、選択したグループ内のリソースによって生成されたデータのみが転送されます。

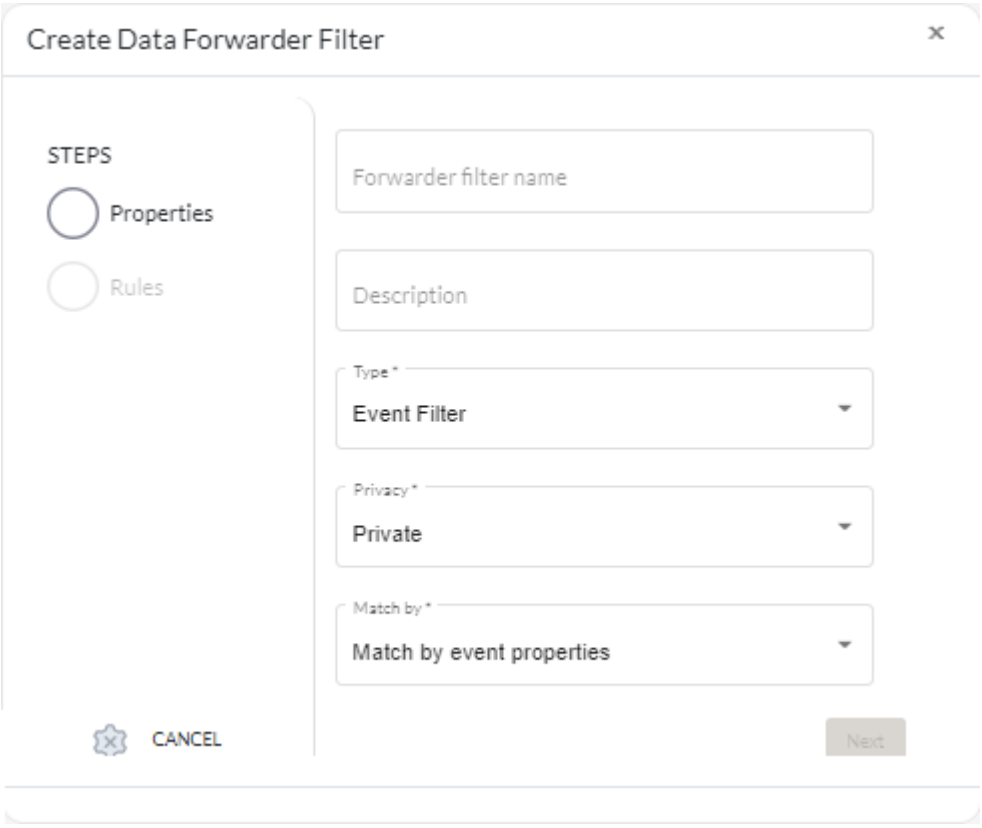
複数のフォワーダーでイベントとリソース・フィルターを再利用できます。ただし、各フォワーダーに、最大 1 つのイベント・フィルターと 1 つのリソース・フィルターを追加することができます。

手順

データ転送フィルターを作成するには、作成するフィルターのタイプに応じて、以下のいずれかの手順を実行します。

- **イベント・フィルター**
  1. XClarity Orchestrator のメニュー・バーで、「**監視**」( ) → 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー・フィルター**」をクリックして、「データ・フォワーダー・フィルター」カードを表示します。

2. 「**作成**」アイコン (⊕) をクリックして、「データ・フォワーダー・フィルターの作成」ダイアログを表示します。



3. フィルター名と任意の説明を指定します。
4. フィルター・タイプとして「**イベント・フィルター**」を選択します。
5. プライバシー・タイプを選択します。
   - 「**プライベート**」。フィルターを作成したユーザーのみがフィルターを使用できます。
   - 「**パブリック**」。すべてのユーザーがフィルターを使用できます。
6. このフィルターの条件として、「イベント・プロパティ」または「イベント・コード」を選択します。

7. 「**規則**」をクリックし、前のステップで選択した条件のタイプに基づいて、このフィルターの基準を選択します。

   – **プロパティによってイベントに一致**。1 つ以上の重大度、保守容易性、およびクラスのプロパティを選択します。選択したプロパティに一致するイベントのみが転送されます。たとえば、「警告」および「クリティカル」の重大度、そしてアダプターとメモリーのクラスを選択した場合、イベントの保守性にかかわらず、警告メモリー・イベント、クリティカル・メモリー・イベント、警告アダプター・イベント、およびクリティカル・アダプター・イベントについてのみイベント・データが転送されます。ユーザーの保守容易性のみを選択した場合、重大度またはクラスにかかわらず、ユーザーによる保守が可能なイベントについてのみイベント・データが転送されます。

     注：
     – クラス・プロパティが選択されていない場合は、すべてのクラス・プロパティが一致します。
     – 保守可能プロパティが選択されていない場合は、すべての保守可能プロパティが一致します。
     – 重大度プロパティが選択されていない場合は、すべての重大度プロパティが一致します。

   – **コードによってイベントに一致**。フィルタリングするイベント・コードを入力し、「**追加**」アイコン (⊕) をクリックして、イベント・コードをリストに追加します。追加するイベント・コードごとにこの手順を繰り返します。イベント・コードを削除するには、該当する個別のコードの横にある「**削除**」アイコン (🗑) をクリックします。リストされているいずれかのイベント・コードに一致するイベントのみが転送されます。

     イベント・コードの全体または一部を指定できます。たとえば、FQXXOCO0001I は特定のイベントに一致し、FQXXOSE はすべての XClarity Orchestrator セキュリティー・イベントに一致し、CO001 はこれらの文字が含まれるすべてのイベントに一致します。

     イベント・コードを指定しない場合は、すべてのイベント・コードが一致します。

     使用可能なイベント・コードのリストについては、イベントとアラートのメッセージ XClarity Orchestrator オンライン・ドキュメント を参照してください。

8. 「**作成**」をクリックして、フィルターを作成します。フィルターがテーブルに追加されます。

- **リソース・フィルター**

1. XClarity Orchestrator のメニュー・バーで、「**監視**」(📈) ➡ 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー・フィルター**」をクリックして、「データ・フォワーダー・フィルター」カードを表示します。
2. 「**作成**」アイコン (⊕) をクリックして、「データ・フォワーダー・フィルターの作成」ダイアログを表示します。
3. フィルター名と任意の説明を指定します。
4. フィルター・タイプとして「**リソース・フィルター**」を選択します。
5. プライバシー・タイプを選択します。
   – 「**プライベート**」。フィルターを作成したユーザーのみがフィルターを使用できます。
   – 「**パブリック**」。すべてのユーザーがフィルターを使用できます。
6. 「**リソース**」をクリックし、このフィルターのイベントのソースを選択します。

   – **すべての XClarity Orchestrator イベントに一致**。この XClarity Orchestrator によって生成されたイベントを転送します。このオプションは、デフォルトで無効になっています。

   – **すべてのリソース・マネージャーのイベントと一致します**。リソース・マネージャーによって生成されたイベントを転送します。このオプションは、デフォルトで無効になっています。
     – このオプションを無効にすると、どのリソース・マネージャーからのイベントも転送されません。
     – このオプションを有効にしても、マネージャー・グループを選択しない場合、すべてのリソース・マネージャーによって生成されたイベントが転送されます。
     – このオプションを有効にした場合で、1 つ以上のマネージャー・グループを選択したときは、選択したグループ内のリソース・マネージャーによって生成されたイベントのみが転送されます。

ヒント: このカードからマネージャー・グループを作成するには、「**作成**」アイコン (⊙) をクリックします。

- **すべてのデバイス・イベントに一致。**このデバイスによって生成されたイベントを転送します。このオプションはデフォルトで有効になっています。
  - このオプションを無効にすると、どのデバイスからのイベントも転送されません。
  - このオプションを有効にしても、デバイス・グループを選択しない場合、すべてのデバイスによって生成されたイベントが転送されます。
  - このオプションを有効にした場合で、1 つ以上のデバイス・グループを選択したときは、選択したグループ内のデバイスによって生成されたイベントのみが転送されます。

ヒント: このカードからデバイス・グループを作成するには、「**作成**」アイコン (⊙) をクリックします。

7. 「**作成**」をクリックして、フィルターを作成します。フィルターがテーブルに追加されます。

終了後

「データ・フォワーダー・フィルター」カードから、以下の操作を実行できます。

- 「**削除**」アイコン (🗑) をクリックして、選択されたフィルターを削除します。フォワーダーに割り当てられているフィルターを削除することはできません。

SAP Data Intelligence へのイベントの転送

SAP Data Intelligence (Intelligent Insights) にイベントを転送するように Lenovo XClarity Orchestrator を構成できます。

始める前に

注意：XClarity Orchestrator および SAP Data Intelligence 間の接続では、暗号化されたトランスポートが使用されますが、リモート・システムの TLS 証明書は検証されません。

このタスクについて

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

SAP Data Intelligence に転送されるデータはフィルターできません。

次の例は、SAP Data Intelligence に転送されるデータのデフォルトの形式を示しています。二重角かっこ内の単語は属性であり、データの転送時に実際の値に置き換えられます。

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
```

```
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

手順

SAP Data Intelligence にイベント・データを転送するには、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、「**監視** ()」 ➔ 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」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、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 3. フォワーダー名と任意の説明を指定します。

ステップ 4. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 5. フォワーダーのタイプとして「**Intelligent Insights**」を選択します。

ステップ 6. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- SAP Data Intelligence のホスト名または IP アドレスを入力します。
- イベント転送に使用するポートを入力します。デフォルトは 443 です。
- フォワーダーがイベントを転送するリソース・パスを入力します (たとえば、/rest/test)。
- REST メソッドを選択します。これは以下のいずれかの値です。
  - PUT
  - POST
- イベント転送に使用するプロトコルを選択します。これは以下のいずれかの値です。
  - HTTP
  - HTTPS
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは 30 秒です。
- 認証が必要な場合は、以下の認証タイプのいずれかを選択します。
  - **基本**。指定されたテナント、ユーザー ID、およびパスワードを使用して指定されたサーバーへの認証を行います。
  - **トークン**。指定されたトークンのヘッダー名と値を使用して指定されたサーバーへの認証を行います。

ステップ 7. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 8. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン () をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン () をクリックして、選択したフォワーダーを削除します。

REST Web サービスへのイベントの転送

特定のイベントを REST Web サービスに転送するように Lenovo XClarity Orchestrator を構成できます。

始める前に

注意：データをこのサービスに転送するとき、セキュアな接続は確立されません。データは、平文プロトコルを使用して送信されます。

このタスクについて

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

共通の*データ転送フィルター*は、イベント・コード、イベント・クラス、イベント重大度、サービス・タイプ、およびイベントを生成したリソースに基づいて、転送するイベントの範囲を定義するために使用されます。このフォワーダーに使用するイベント・フィルターおよびリソース・フィルターが既に作成されていることを確認します (データ転送フィルターの作成を参照)。

次の例は、REST Web サービスに転送されるデータのデフォルトの形式を示しています。二重角かっこ内の単語は属性であり、データの転送時に実際の値に置き換えられます。

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

手順

REST Web サービスにデータを転送するには、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、「**監視** ( )」 ➔ 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」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、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 3. フォワーダー名と任意の説明を指定します。

ステップ 4. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 5. フォワーダーのタイプとして「**REST**」を選択します。

ステップ 6. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- REST サーバーのホスト名または IP アドレスを入力します。
- イベント転送に使用するポートを入力します。デフォルトは `80` です。

- フォワーダーがイベントを転送するリソース・パスを入力します (たとえば、/rest/test)。
- REST メソッドを選択します。これは以下のいずれかの値です。
  - PUT
  - POST
- イベント転送に使用するプロトコルを選択します。これは以下のいずれかの値です。
  - HTTP
  - HTTPS
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは 30 秒です。
- 認証が必要な場合は、以下の認証タイプのいずれかを選択します。
  - **基本**。指定されたユーザー ID とパスワードを使用して指定されたサーバーへの認証を行います。
  - **トークン**。指定されたトークンのヘッダー名と値を使用して指定されたサーバーへの認証を行います。

ステップ 7. 「**フィルター**」をクリックし、オプションでこのフォワーダーに使用するフィルターを選択します。

最大で 1 つのイベント・フィルターと 1 つのリソース・フィルターを選択できます。

フィルターを選択しない場合は、すべてのリソース (デバイス、リソース・マネージャー、および XClarity Orchestrator) で生成されたすべてのイベントに対してデータが転送されます。

このタブから、「**除外イベント**」トグルを「**はい**」に設定することで、除外イベントを転送することもできます。

ステップ 8. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 9. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン (✎) をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン (🗑) をクリックして、選択したフォワーダーを削除します。

SMTP を使用するメール・サービスへのイベントの転送

SMTP を使用して特定のイベントを 1 つ以上のメール・アドレスに転送するように、Lenovo XClarity Orchestrator を構成できます。

始める前に

注意：データをこのサービスに転送するとき、セキュアな接続は確立されません。データは、平文プロトコルを使用して送信されます。

Web ベースのメール・サービス (Gmail、Hotmail、または Yahoo など) にメールを転送するには、SMTP サーバーが転送 Web メールをサポートしている必要があります。

Gmail Web サービスへのイベント・フォワーダーを設定する前に、Gmail SMTP サービスへのイベントの転送の情報を確認してください。

このタスクについて

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

共通の*データ転送フィルター*は、イベント・コード、イベント・クラス、イベント重大度、サービス・タイプ、およびイベントを生成したリソースに基づいて、転送するイベントの範囲を定義するために使用されます。このフォワーダーに使用するイベント・フィルターおよびリソース・フィルターが既に作成されていることを確認します (データ転送フィルターの作成を参照)。

次の例は、メール・サービスに転送されるデータのデフォルトの形式を示しています。二重角かっこ内の単語は属性であり、データの転送時に実際の値に置き換えられます。

メールの件名

```
Event Forwarding
```

メールの本文

```
{
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
      forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
          being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
          based on the eventID. At the moment the orchestrator server can not offer more
          information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB649109748919 3447A655C",
  "managerID": "23C87F0A2CB649109748919 3447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXHMEM0216I",
```

```
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
  },
  "resourceType": "XClarity Administrator",
  "componentType": "XClarity Administrator",
  "sourceType": "Management",
  "resourceName": "xhmc194.labs.lenovo.com",
  "fruType": "other",
  "ipAddress": "10.243.2.107",
  "_id": 252349
}
```


手順

SMTP を使用してメール・サービスにデータを転送するには、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、「**監視** ()」 ➡ 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」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、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 3. フォワーダー名と任意の説明を指定します。

ステップ 4. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 5. フォワーダーのタイプとして「**メール**」を選択します。

ステップ 6. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- SMTP サーバーのホスト名または IP アドレスを入力します。
- イベント転送に使用するポートを入力します。デフォルトは 25 です。
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは 30 秒です。
- 各受信者のメール・アドレスを入力します。複数のメール・アドレスはコンマで区切ります。
- **オプション**: メール送信側のメール・アドレス (たとえば、john@company.com) と送信側ドメインを入力します。メール・アドレスを指定しない場合、送信側アドレスはデフォルトで LXCO.*<source_identifier>*@*<smtp_host>* です。

  送信側ドメインのみを指定する場合は、送信側アドレスの形式は、*<LXCO_host_name>*@*<sender_domain>* (たとえば、XClarity1@company.com) です。

  注：

  – メールの転送にホスト名を要求するように SMTP サーバーをセットアップした場合、XClarity Orchestrator のホスト名をセットアップしないと、SMTP サーバーが転送されたイベントを拒否する可能性があります。XClarity Orchestrator にホスト名がない場合、イベントは IP アドレスを使用して転送されます。IP アドレスが取得できない場合は、代わりに「localhost」が送信され、SMTP サーバーでイベントが拒否されることになります。

  – 送信側ドメインを指定する場合は、ソースでは送信側アドレスを識別しません。代わりに、メールの本文に、システム名、IP アドレス、タイプ/モデル、およびシリアル番号を含むイベントの原因に関する情報が含まれています。

  – SMTP サーバーが登録ユーザーから送信されたメールのみを受け入れる場合、デフォルトの送信側アドレス (LXCO.*<source_identifier>*@*{smtp_host>*) は拒否されます。この場合、「**送信元ユーザー**」フィールドに少なくとも 1 つのドメイン名を指定する必要があります。

- SMTP サーバーへのセキュアな接続を確立するには、以下のいずれかの接続タイプを選択します。
  - **SSL**。SSL プロトコルを使用して、セキュアな通信を確立します。
  - **STARTTLS**。TLS プロトコルを使用してセキュアではないチャネルを経由するセキュアな通信を形成します。

  これらの接続タイプのいずれかを選択すると、XClarity Orchestrator は XClarity Orchestrator 信頼ストアに SMTP サーバーの証明書をダウンロードしてインポートします。この証明書を受け入れるように求めるプロパティが表示されます。
- 認証が必要な場合は、以下の認証タイプのいずれかを選択します。
  - **Regular**。指定されたユーザー ID とパスワードを使用して指定された SMTP サーバーへの認証を行います。
  - **OAUTH2**。指定されたユーザー名およびセキュリティー・トークンを使用して、指定された SMTP サーバーへの認証に Simple Authentication and Security Layer (SASL) プロトコルを使用します。通常、ユーザー名はメール・アドレスです。

    注意：セキュリティー・トークンは、短時間で有効期限が切れます。セキュリティー・トークンの更新はお客様の責任で行っていただきます。
  - **なし**。認証は使用しません。

ステップ 7. 「**フィルター**」をクリックし、オプションでこのフォワーダーに使用するフィルターを選択します。

最大で 1 つのイベント・フィルターと 1 つのリソース・フィルターを選択できます。

フィルターを選択しない場合は、すべてのリソース (デバイス、リソース・マネージャー、および XClarity Orchestrator) で生成されたすべてのイベントに対してデータが転送されます。

このタブから、「**除外イベント**」トグルを「**はい**」に設定することで、除外イベントを転送することもできます。

ステップ 8. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 9. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン (✎) をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン (🗑) をクリックして、選択したフォワーダーを削除します。

Gmail SMTP サービスへのイベントの転送

Lenovo XClarity Orchestrator をセットアップして、イベントを、Gmail などの Web ベースのメール・サービスに転送できます。

Gmail SMTP サービスを使用するようにイベント・フォワーダーをセットアップするには、以下の構成例を使用します。

注：Gmail では、もっとも安全な通信手段として OAUTH2 認証方式を使用することをお勧めします。通常の認証を選択した場合、アプリケーションが最新セキュリティー基準を使用しないでアカウントの使用を試みたことを知らせるメールを受信します。メールには、このようなタイプのアプリケーションを受け入れるようにお客様のメール・アカウントを構成する手順が記載されています。

Gmail SMTP サーバーの構成について詳しくは、https://support.google.com/a/answer/176600?hl=enを参照してください。

ポート 465 の SSL を使用した通常の認証

この例では、ポート 465 経由の SSL プロトコルを使用して Gmail SMTP サーバーと通信し、有効な Gmail ユーザー・アカウントおよびパスワードを使用して認証します。

パラメーター	値
Host	smtp.gmail.com
ポート	465
SSL	選択
STARTTLS	クリア
認証	通常
ユーザー	有効な Gmail メール・アドレス
パスワード	Gmail 認証パスワード
送信元アドレス	(オプション)

ポート 587 の TLS を使用した通常の認証

この例では、ポート 587 経由の TLS プロトコルを使用して Gmail SMTP サーバーと通信し、有効な Gmail ユーザー・アカウントおよびパスワードを使用して認証します。

パラメーター	値
Host	smtp.gmail.com
ポート	587
SSL	クリア
STARTTLS	選択
認証	通常
ユーザー	有効な Gmail メール・アドレス
パスワード	Gmail 認証パスワード
送信元アドレス	(オプション)

ポート 587 の TLS を使用した OAUTH2 認証

この例では、ポート 587 経由の TLS プロトコルを使用して Gmail SMTP サーバーと通信し、有効な Gmail ユーザー・アカウントおよびセキュリティー・トークンを使用して認証します。

以下の手順の例を使用してセキュリティー・トークンを取得します。

1. Google Developers Console にプロジェクトを作成して、クライアント ID およびクライアント・シークレットを取得します。詳しくは、Web サイト用 Google サインインの Web ページ Web サイトを参照してください。
   a. Web ブラウザーで、Google API Web ページ を開きます。
   b. Web ページのメニューから「**プロジェクトの選択**」 → 「**プロジェクトの作成**」 をクリックします。「新規プロジェクト」ダイアログが表示されます。
   c. 名前を入力し、「**はい**」を選択してご使用条件に同意して、「**作成**」をクリックします。
   d. 「**概要**」タブで、検索フィールドを使用して「gmail」を検索します。検索結果の「**GMAIL API**」をクリックします。
   e. 「**有効**」をクリックします。
   f. 「**資格情報**」タブをクリックします。
   g. 「**OAuth 同意画面**」をクリックします。
   h. 「**ユーザーに表示される製品名**」フィールドに名前を入力して、「**保存**」をクリックします。
   i. 「**視覚情報の作成**」 → 「**OAuth クライアント ID**」 をクリックします。
   j. 「**その他**」を選択して名前を入力します。
   k. 「**作成**」をクリックします。「OAuth クライアント」ダイアログにクライアント ID およびクライアント・シークレットが表示されます。
   l. 後で使用するためにクライアント ID およびクライアント・シークレットを記録します。
   m. 「OK」をクリックして、ダイアログを閉じます。
2. oauth2.py Python スクリプトを使用して、セキュリティー・トークンを生成して認証します。プロジェクト作成時に生成されたクライアント ID およびクライアント・シークレットを入力します。

   注：次のステップを実行するには、Python 2.7 が必要です。Python 2.7 は Python Web サイト からダウンロードしてインストールできます。
   a. Web ブラウザーで、gmail-oauth2-tools Web ページ を開きます。
   b. 「Raw」をクリックし、ファイル名を `oauth2.py` としてコンテンツをローカル・システムに保存します。
   c. 次のコマンドを端末 (Linux) またはコマンド・ライン (Windows) で実行します。
      ```
      py oauth2.py --user=<your_email> --client_id=<client_id>
        --client_secret=<client_secret> --generate_oauth2_token
      ```
      例:
      ```
      py oauth2.py --user=jon@gmail.com
        --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
        --client_secret=3tnyXgEiBIbT2mOOzqnlTszk --generate_oauth2_token
      ```

      このコマンドは、トークンの認証と Google Web サイトからの検証コードの取得に必要な URL を返します。以下に例を示します。
      ```
      To authorize token, visit this url and follow the directions:

      https://accounts.google.com/o/oauth2/auth?client_id=884243132302
      -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
      urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
      google.com%2F

      Enter verification code:
      ```
   d. Web ブラウザーで、前のステップで返された URL を開きます。
   e. 「**許可**」をクリックしてこのサービスに同意します。検証コードが返されます。

f. 検証コードを `oauth2.py` コマンドに入力します。コマンドが、セキュリティー・トークンを返しトークンを更新します。以下に例を示します。

```
Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600
```

重要：セキュリティー・トークンは、一定時間で有効期限が切れます。oauth2.py Python スクリプトを使用して、トークンを更新し新しいセキュリティー・トークンを生成できます。新しいセキュリティー・トークンを生成し、その新しいトークンで Lenovo XClarity Orchestrator のイベント・フォワーダーを更新する作業は、お客様の責任で行っていただきます。

3. Lenovo XClarity Orchestrator Web インターフェースから、次の属性を使用してメールのイベント・フォワーダーをセットアップします。

パラメーター	値
Host	smtp.gmail.com
ポート	587
SSL	クリア
STARTTLS	選択
認証	OAUTH2
ユーザー	有効な Gmail メール・アドレス
トークン	セキュリティー・トークン
送信元アドレス	(オプション)

Splunk へのインベントリーおよびイベントの転送

事前定義された形式の特定のインベントリーおよびイベントを Splunk アプリケーションに転送するように Lenovo XClarity Orchestrator を構成できます。ユーザーは、そのデータに基づいて Splunk でグラフや図表を作成し、環境内の状態の分析や問題の予測に役立てることができます。

始める前に

注意：データをこのサービスに転送するとき、セキュアな接続は確立されません。データは、平文プロトコルを使用して送信されます。

このタスクについて

Splunk は、イベント・ログやその他のデータを追跡して分析するためのデータ・センター・オペレーター用のツールです。Lenovo は、XClarity Orchestrator によって転送されるイベントを分析し、一連のダッシュボードに分析を表示する Splunk 用の XClarity Orchestrator アプリを提供します。環境内の潜在的な問題を見つけるために、このアプリのダッシュボードを監視して、重大な問題が発生する前に対処することができます。詳しくは、Splunk 用の XClarity Orchestrator アプリのユーザーズ・ガイド XClarity Orchestrator オンライン・ドキュメント を参照してください。

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 Splunk インスタンスは 1 つだけです。そのため、Splunk の構成は一度に 1 つしか有効にできません。

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

Splunk アプリケーションに転送されるデータはフィルターできません。

手順

Splunk アプリケーションにインベントリーおよびイベント・データを転送するには、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、「**監視** ()」 → 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」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、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 3. フォワーダー名と任意の説明を指定します。

ステップ 4. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 5. フォワーダーのタイプとして「**Splunk**」を選択します。

ステップ 6. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- Splunk アプリケーションのホスト名または IP アドレスを入力します。
- Splunk サービス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。
- Splunk サービスへの接続に使用する REST API とデータ・ポート番号を指定します。
- HTTP イベント・コレクターのインデックスを 1つ以上指定します。デフォルトのインデックスは **lxco** です。
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは 30 秒です。

ステップ 7. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 8. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン (✎) をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン (🗑) をクリックして、選択したフォワーダーを削除します。

syslog へのイベントの転送

特定のイベントを syslog に転送するように Lenovo XClarity Orchestrator を構成できます。

始める前に

注意：データをこのサービスに転送するとき、セキュアな接続は確立されません。データは、平文プロトコルを使用して送信されます。

このタスクについて

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

共通の*データ転送フィルター*は、イベント・コード、イベント・クラス、イベント重大度、サービス・タイプ、およびイベントを生成したリソースに基づいて、転送するイベントの範囲を定義するために使用されます。このフォワーダーに使用するイベント・フィルターおよびリソース・フィルターが既に作成されていることを確認します (データ転送フィルターの作成を参照)。

次の例は、syslog に転送されるデータのデフォルトの形式を示しています。二重角かっこ内の単語は属性であり、データの転送時に実際の値に置き換えられます。

```
{
  "appl": "LXCO",
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
      forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
           being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
          based on the eventID. At the moment the orchestrator server can not offer more
          information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
  "managerID": "23C87F0A2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXHMEM0216I",
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
    "serialNumber": null
  },
  "resourceType": "XClarity Administrator",
  "componentType": "XClarity Administrator",
  "sourceType": "Management",
```

```
  "resourceName": "xhmc194.labs.lenovo.com",
  "fruType": "other",
  "ipAddress": "10.243.2.107",
  "_id": 252349
}
```


手順

データを syslog に転送するには、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、「**監視** ( )」 → 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」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、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 3. フォワーダー名と任意の説明を指定します。

ステップ 4. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 5. フォワーダーのタイプとして「**Syslog**」を選択します。

ステップ 6. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- syslog のホスト名または IP アドレスを入力します。
- イベント転送に使用するポートを入力します。デフォルトは 514 です。
- イベント転送に使用するプロトコルを選択します。これは以下のいずれかの値です。
  - UDP
  - TCP
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは 30 秒です。
- **オプション**: syslog のタイムスタンプの形式を選択します。これは以下のいずれかの値です。
  - **現地時刻**。デフォルトの形式。例: Fri Mar 31 05:57:18 EDT 2017。
  - **GMT 時刻**。日時の国際標準 (ISO8601) 。例: 2017-03-31T05:58:20-04:00。

ステップ 7. 「**フィルター**」をクリックし、オプションでこのフォワーダーに使用するフィルターを選択します。

最大で 1 つのイベント・フィルターと 1 つのリソース・フィルターを選択できます。

フィルターを選択しない場合は、すべてのリソース (デバイス、リソース・マネージャー、および XClarity Orchestrator) で生成されたすべてのイベントに対してデータが転送されます。

このタブから、「**除外イベント**」トグルを「**はい**」に設定することで、除外イベントを転送することもできます。

ステップ 8. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 9. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン (✎) をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン (🗑) をクリックして、選択したフォワーダーを削除します。

Lenovo TruScale Infrastructure Services へのメトリックス・データの転送

Lenovo XClarity Orchestrator を構成して、Lenovo TruScale Infrastructure Services にメトリックス (テレメトリー) データを転送できます。

始める前に

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

注意：以下の構成手順は、Lenovo サービス担当員のみを対象とします。

データを TruScale Infrastructure Services に転送するとき、セキュアな接続が確立されます。

XClarity Orchestrator v1.2.0 以降が実行されていることを確認します。

メトリック・データの転送先となる、デバイスを管理する Lenovo XClarity Administrator リソース・マネージャーで、v3.0.0 以上のフィックスパックが実行されていることを確認します。

適切な XClarity Administrator リソース・マネージャーが XClarity Orchestrator に接続されていることを確認します (リソース・マネージャーの接続を参照)。

メトリック・データを転送するデバイスで最新の Lenovo XClarity Controller ファームウェアが実行されていることを確認します (リソース・マネージャーへの更新の適用とアクティブ化 を参照)。

次のリソースでデータと時刻の設定が正しく構成されていることを確認します。
- XClarity Orchestrator (日付と時刻の構成 を参照)
- XClarity Administrator リソース・マネージャー (XClarity Administrator オンライン・ドキュメントの日付と時刻の設定を参照)
- 各デバイスのベースボード管理コントローラー (Lenovo XClarity Controller オンライン・ドキュメントのXClarity Controller の日付と時刻の設定を参照)

XClarity Orchestrator のネットワーク設定が正しく構成されていることを確認します。

デバイス要約ページで使用率グラフを表示して、管理対象デバイスのメトリック・データが収集されていることを確認します (デバイスの詳細の表示を参照)。メトリック・データが表示されない場合は、データ転送に関する問題のトラブルシューティング を参照してください。

Lenovo TruScale Infrastructure Services の詳細については、TruScale Infrastructure Services Web サイトを参照してください。

このタスクについて

複数の Lenovo TruScale Infrastructure Services 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 Lenovo TruScale Infrastructure Services インスタンスは 1 つだけです。そのため、Lenovo TruScale Infrastructure Services の構成は一度に 1 つしか有効にできません。

リソース・ベース・アクセス制御が有効になっている場合、データはアクセス制御リストを使用してアクセスできるリソースのみ転送されます。事前定義の**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場合、作成するフォワーダーに 1 つ以上のアクセス制御リストを割り当てる必要

があります。アクセスできるすべてのリソースのデータを送信する場合は、関連付けられている使用可能なアクセス制御リストをすべて選択します。事前定義の**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ある場合は、すべてのリソースのデータを送信するか、またはアクセス制御リストを割り当ててリソースを制限することを選択できます。

Lenovo TruScale Infrastructure Services に転送されるデータはフィルターできません。

次の例は、Lenovo TruScale Infrastructure Services に転送されるデータのデフォルトの形式を示しています。二重角かっこ内の単語は属性であり、データの転送時に実際の値に置き換えられます。

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

手順

データを Lenovo TruScale Infrastructure Services に転送するには、以下の手順を実行します。

ステップ 1. Lenovo TruScale Infrastructure Services によって提供される信頼できる SSL 証明書を追加します。

1. XClarity Orchestrator のメニュー・バーから、XClarity Orchestrator のメニュー・バーをクリックし、「**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「**トラステッド証明書**」をクリックして、「トラステッド証明書」カードを表示します。
2. 「**追加**」アイコン (⊕) をクリックして、証明書を追加します。「証明書の追加」ダイアログが表示されます。
3. PEM 形式の証明書データをコピーして貼り付けます。
4. 「**追加**」をクリックします。

ステップ 2. XClarity Orchestrator のメニュー・バーで、「**監視** (📈)」 ➡ 「**転送**」をクリックし、左側のナビゲーションで「**データ・フォワーダー**」をクリックして、「データ・フォワーダー」カードを表示します。

ステップ 3. 「**作成**」アイコン (⊕) をクリックして、「データ・フォワーダーの作成」ダイアログを表示します。

ステップ 4. フォワーダー名と任意の説明を指定します。

ステップ 5. 「**状態**」をクリックして切り替え、フォワーダーを有効または無効にします。

ステップ 6. フォワーダーのタイプとして「**TruScale Infrastructure Services**」を選択します。

ステップ 7. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- TruScale Infrastructure Service のホスト名または IP アドレスを入力します。
- イベント転送に使用するポートを入力します。デフォルトは `9092` です。
- オプションで、データをプッシュする頻度 (分単位) で入力します。デフォルトは `60` 分です。
- トピック名を入力します。
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは `300` 秒です。

ステップ 8. 「**接続を検証**」をクリックして、構成に基づいて接続を確立できることを確認します。

注意：接続の検証が完了するまでに数分かかることがあります。ポップアップ・メッセージを閉じて、検証プロセスを中断せずにフォワーダーの作成を続行できます。検証が完了すると、接続が成功したかどうかを通知する別のポップアップ・メッセージが表示されます。

ステップ 9. 「**アクセス制御リスト**」をクリックし、このフォワーダーに関連付けるアクセス制御リストを 1 つ以上選択します。

リソース・ベース・アクセスが有効になっている場合、少なくとも 1 つのアクセス制御リストを選択する必要があります。

ヒント: 事前定義の**スーパーバイザー**役割が割り当てられたグループのメンバーであるユーザーは、オプションとしてアクセス制御リストを選択せずに「**すべてを一致させる**」を選択すると、転送されるデータが制限されません。

ステップ 10.「**作成**」をクリックして、フォワーダーを作成します。

終了後

「データ・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したフォワーダーを有効または無効にします。
- 「**編集**」アイコン ( ) をクリックして、選択したフォワーダーを変更します。
- 「**削除**」アイコン ( ) をクリックして、選択したフォワーダーを削除します。

レポートの転送

SMTP Web サービスを使用して、反復ベースのレポートを 1 つ以上のメール・アドレスに転送できます。

このタスクについて

*レポート*は、ユーザー・インターフェースで表形式で表示されるデータです。現在、以下のレポートがサポートされています。

- アクティブ・アラート
- リソースと監査イベント
- 管理対象デバイス (サーバー、ストレージ、スイッチ、およびシャーシ)
- デバイス・ファームウェア・コンプライアンス
- サーバー構成のコンプライアンス
- サーバーの保証状況
- アクティブなサービス・チケット

フォワーダーの宛先構成の作成

複数のレポート・フォワーダーで使用できる共通の宛先構成を定義できます。宛先は、レポートが送信される場所を識別します。

手順

レポート・フォワーダーの宛先構成を作成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーで、「**監視** ( )」 ➡ 「**転送**」をクリックし、左側のナビゲーションで「**フォワーダーの宛先**」をクリックして、「フォワーダー宛先」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、「フォワーダーの宛先の作成」ダイアログを表示します。

ステップ 3. レポート・フォワーダー名と任意の説明を指定します

ステップ 4. 宛先のタイプとして「**SMTP**」を選択します。

ステップ 5. 「**構成**」をクリックし、プロトコル固有の情報を入力します。

- SMTP (メール) サーバーのホスト名または IP アドレスを入力します。
- 宛先に使用するポートを入力します。デフォルトは `25` です。
- 要求のタイムアウト時間 (秒単位) を入力します。デフォルトは `30` 秒です。
- 各受信者のメール・アドレスを入力します。複数のメール・アドレスはコンマで区切ります。
- **オプション**: メール送信側のメール・アドレス (たとえば、john@company.com) と送信側ドメインを入力します。メール・アドレスを指定しない場合、送信側アドレスはデフォルトで LXCO.*{source_identifier}*@*{smtp_host}* になります。

  送信側のみドメインを指定する場合は、送信側アドレスの形式は *{LXCO_host_name}*@*{sender_domain}* (たとえば、`XClarity1@company.com`) です。

  注：

  – メールの転送にホスト名を要求するように SMTP サーバーをセットアップした場合、XClarity Orchestrator のホスト名をセットアップしないと、SMTP サーバーがメールを拒否する可能性があります。XClarity Orchestrator にホスト名がない場合、メールは IP アドレスを使用して転送されます。IP アドレスが取得できない場合は、代わりに「localhost」が送信され、SMTP サーバーでメールが拒否されることになります。

  – 送信側ドメインを指定する場合は、ソースでは送信側アドレスを識別しません。代わりに、メールの本文に、システム名、IP アドレス、マシン・タイプ/モデル、およびシリアル番号を含むデータ・ソースに関する情報が含まれています。

  – SMTP サーバーが登録ユーザーから送信されるメールのみを受け入れる場合、デフォルトの送信側アドレス (`LXCO.<source_identifier>@<smtp_host>`) は拒否されます。この場合、「**送信元ユーザー**」フィールドに少なくとも 1 つのドメイン名を指定する必要があります。

- SMTP サーバーへのセキュアな接続を確立するには、以下のいずれかの接続タイプを選択します。
  – **SSL**。SSL プロトコルを使用して、セキュアな通信を確立します。
  – **STARTTLS**。TLS プロトコルを使用してセキュアではないチャネルを経由するセキュアな通信を形成します。

  これらの接続タイプのいずれかを選択すると、XClarity Orchestrator は XClarity Orchestrator 信頼ストアに SMTP サーバーの証明書をダウンロードしてインポートします。この証明書を受け入れるように求めるプロパティが表示されます。
- 認証が必要な場合は、以下の認証タイプのいずれかを選択します。
  – **Regular**。指定されたユーザー ID とパスワードを使用して指定された SMTP サーバーへの認証を行います。
  – **OAUTH2**。指定されたユーザー名およびセキュリティー・トークンを使用して、指定された SMTP サーバーへの認証に Simple Authentication and Security Layer (SASL) プロトコルを使用します。通常、ユーザー名はメール・アドレスです。

    注意：セキュリティー・トークンは、短時間で有効期限が切れます。セキュリティー・トークンの更新はお客様の責任で行っていただきます。
  – **なし**。認証は使用しません。

ステップ 6. 「**作成**」をクリックして宛先構成を作成します。

終了後

「フォワーダーの宛先」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、選択した宛先を変更します。

- 「**削除**」アイコン ( ) をクリックして、選択した宛先を削除します。フォワーダーに割り当てられている宛先を削除することはできません

メールを使用したレポートの転送

SMTP Web サービスを使用して、反復ベースのレポートを 1 つ以上のメール・アドレスに転送できます。

このタスクについて

*レポート*は、ユーザー・インターフェースで表形式で表示されるデータです。現在、以下のレポートがサポートされています。
- アクティブ・アラート
- リソースと監査イベント
- 管理対象デバイス (サーバー、ストレージ、スイッチ、およびシャーシ)
- デバイス・ファームウェア・コンプライアンス
- サーバー構成のコンプライアンス
- サーバーの保証状況
- アクティブなサービス・チケット

各レポート・フォワーダーには、各タイプのレポートを 1 つのみ含めることができます。

レポートはアーカイブ・ファイルとして作成され、Orchestrator サーバー・ホストに保存されます。ファイルが 10 MB 以下の場合、ファイルはメールの添付ファイルとして転送されます。ファイルのサイズが 10MB を超える場合、メールにはファイルの場所が含まれます。また、レポートの行で「**レポートの履歴**」をクリックし、「**ダウンロード**」をクリックしてアーカイブ・ファイルをダウンロードできます。

Lenovo XClarity Orchestrator では、最大 100 のレポートが保存されます。レポートの最大数に達した場合は、新しいレポートを生成する前に XClarity Orchestrator によって最も古いレポートが削除されます。

手順

メール形式でレポートを転送するには、以下のいずれかの手順を実行します。

- **フィルタリングされていないデータの送信**
  1. XClarity Orchestrator のメニュー・バーで、「**監視** ( )」 ➡ 「**転送**」をクリックし、左側のナビゲーションで「**レポート・フォワーダー**」をクリックして、「レポート」カードを表示します。
  2. 「**作成**」アイコン ( ) をクリックして「レポートの作成」ダイアログを作成します。
  3. レポート・フォワーダー名と任意の説明を指定します。
  4. 「**状態**」をクリックして切り替え、レポート・フォワーダーを有効または無効にします。
  5. 「**コンテンツ・リスト**」をクリックし、転送するレポートを 1 つ以上選択します。
  6. 「**フォワーダーの宛先**」をクリックして、宛先を選択します (フォワーダーの宛先構成の作成を参照)。
  7. 「**スケジュール**」をクリックし、レポートを送信する週の日、時刻、期間 (開始日と終了日) を指定します。レポートは、指定された期間中の毎週同じ日と時刻に送信されます。
  8. 「**作成**」をクリックして、フォワーダーを作成します。
- **フィルタリングされたデータの送信**
  1. XClarity Orchestratorメニュー・バーで、送信するレポートが含まれるカードを開きます。以下のレポートがサポートされています。
     - デバイス・データ (**リソース** ( ) ➡ *{device_type}*をクリック)
     - アクティブ・アラート・データ (「**監視** ( )」 ➡ 「**アラート**」をクリックします)
     - リソースおよび監査イベント・データ (「**監視** ( )」 ➡ 「**イベント**」をクリックします)

- ファームウェア・コンプライアンス (「**プロビジョニング**」 ➔ 「**更新**」 ➔ 「**適用して有効化**」 ➔ 「**デバイス**」をクリックします)
- サーバー構成コンプライアンス (「**プロビジョニング**」 ➔ 「**サーバー構成**」 ➔ 「**割り当てとデプロイ**」をクリックします)
- デバイス保証データ (「**管理**」 ➔ 「**サービスおよびサポート**」 ➔ 「**保証**」をクリックします)
- アクティブ・サービス・チケット (「**管理**」 ➔ 「**サービスおよびサポート**」 ➔ 「**サービス・チケット**」をクリックします)

2. 必要に応じて、特定のリソース・マネージャーとグループにあるリソースにのみデータの範囲を絞り込み、フィルターと検索を使用して特定の基準に一致するデータを含め、目的の情報にのみデータ・セットを絞り込みます (ユーザー・インターフェースのヒントと手法を参照)。
3. 「**すべての操作**」 ➔ 「**レポート・フォワーダーの作成**」をクリックして、「レポート・フォワーダーの作成」ダイアログを表示します。
4. レポート・フォワーダー名と任意の説明を指定します。
5. 「**状態**」をクリックして切り替え、レポート・フォワーダーを有効または無効にします。
6. 「**フォワーダーの宛先**」をクリックして、宛先を選択します (フォワーダーの宛先構成の作成を参照)。
7. 「**スケジュール**」をクリックし、レポートを送信する週の日、時刻、期間 (開始日と終了日) を指定します。レポートは、指定された期間中の毎週同じ日と時刻に送信されます。
8. 「**作成**」をクリックして、フォワーダーを作成します。

終了後

「レポート・フォワーダー」カードから、以下の操作を実行できます。

- 「**状態**」列を選択して切り替え、選択したレポート・フォワーダーを有効または無効にします。
- 「**編集**」アイコン () をクリックして、選択したレポート・フォワーダーを変更します。
- 「**削除**」アイコン () をクリックして、選択したレポート・フォワーダーを削除します。
- 「**レポートの履歴**」タブをクリックし、各レポートで「**ダウンロード**」をクリックして、ローカル・システムにレポートを保存します。

サポートされているいずれかのレポート・カードから既存のレポート・フォワーダーにレポートを追加するには、そのカードから「**すべての操作**」 ➔ 「**既存のレポート・フォワーダーにコンテンツを追加**」をクリックして、テーブルに現在適用されているデータ・フィルターを使用します。レポート・フォワーダーにそのタイプのレポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。

第 4 章　リソースの管理

Lenovo XClarity Orchestrator を使用して、オフライン・デバイスの詳細を表示するなど、リソースを管理できます。

リソース・グループの作成

*リソース・グループ*はリソースのセットで、Lenovo XClarity Orchestrator でまとめて表示および操作することができます。複数のタイプのリソース・グループがサポートされています。

詳細: リソース・グループの作成方法

このタスクについて

複数のタイプのリソース・グループがサポートされています。

- *動的デバイス・グループ*には、特定の条件に基づいたデバイスの動的なセットが含まれます。
- *デバイス・グループ*には、特定のデバイスの静的なセットが含まれます。
- *マネージャー・グループ*には、特定のリソース・マネージャーの静的なセットおよびXClarity Orchestrator自体が含まれます。
- *インフラストラクチャー・グループ*には、ネットワーク・デバイスのセットが含まれます。Schneider Electric EcoStruxure IT Expertリソース・マネージャーを管理する場合は、管理対象のEcoStruxure IT エキスパートで定義されている「グループ」コレクションのクローンがXClarity Orchestratorで自動的に作成されます。クローン作成されたグループの名前は、ローカル・リポジトリー内で *{domain}\{groupName}* となります。場所の種類に関するコレクション (サイト、建物、部屋、並び、およびラック) はクローン作成されませんので注意してください。

注：デバイス、リソース・マネージャー、およびインフラストラクチャー・リソースが混在するリソース・グループを作成することはできません。

手順

リソース・グループを作成してメンバーシップを管理するには、以下の手順を実行します。

- **動的デバイス・グループを作成し、デバイスを追加します。**
  1. XClarity Orchestrator のメニュー・バーで、「**リソース**」() → 「**グループ**」の順にクリックして、「グループ」カードを表示します。

  2. 「**作成**」アイコン () をクリックして、「グループの作成」ダイアログを表示します。
  3. グループ・タイプとして「**ダイナミック・デバイス・グループ**」を選択します。
  4. グループの名前および説明 (任意) を指定します。

5. 「**グループ条件**」をクリックし、グループ・メンバーシップに使用するルールを選択します。

   - 「**条件**」一致ドロップダウンから、デバイスは、「**いずれか**」 (1 つ以上) または「**すべて**」のルールに一致する必要があるかどうかを選択します。
   - 各ルールの属性、オペレーター、および値を指定します。**条件の追加**をクリックして、別のルールを追加します。
6. **連絡先情報**をクリックし、必要に応じて、一次サポート連絡先 (**主要連絡先**列) と 1 つ以上の二次的連絡先 (**二次的連絡先**列) を選択して、グループ内のすべてのデバイスに割り当てます。
7. 「**作成**」をクリックします。グループが表に追加されます。

- **静的リソース・グループを作成し、リソースを追加します。**
  1. XClarity Orchestrator のメニュー・バーで、「**リソース** ()」 → 「**グループ**」の順にクリックして、「グループ」カードを表示します。
  2. 「**作成**」アイコン () をクリックして、「グループの作成」ダイアログを表示します。
  3. グループ・タイプとして「**デバイス・グループ**」または「**マネージャー・グループ**」を選択します。
  4. グループの名前および説明 (任意) を指定します。
  5. グループ・タイプに応じて「**使用可能なデバイス**」または「**使用可能なリソース・マネージャー**」をクリックし、グループに含めるリソースを選択します。
  6. **連絡先情報**をクリックし、必要に応じて、一次サポート連絡先 (**主要連絡先**列) と 1 つ以上の二次的連絡先 (**二次的連絡先**列) を選択して、グループ内のすべてのデバイスに割り当てます。
  7. 「**作成**」をクリックします。グループが表に追加されます。
- **静的デバイス・グループにデバイスを追加します。**
  1. XClarity Orchestrator のメニュー・バーで「**リソース** ()」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべてのデバイスが表示されます。

2. グループに追加するデバイスを 1 つ以上選択します。
3. 「**グループにアイテムを追加**」アイコン (⊕) をクリックして、グループを追加します。
4. 既存のグループを選択するか、名前とオプションの説明を指定して新しいグループを作成し、「**適用**」をクリックします。

- **静的マネージャー・グループにリソース・マネージャーを追加します。**
  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. グループに追加するリソース・マネージャーを 1 つ以上選択します。
  3. 「**グループにアイテムを追加**」アイコン (⊕) をクリックして、グループを追加します。
  4. 既存のグループを選択するか、名前とオプションの説明を指定して新しいグループを作成し、「**適用**」をクリックします。

終了後

「グループ」カードから、以下の操作を実行できます。

- 選択したグループのプロパティおよびメンバーシップを変更するには、「**編集**」アイコン (✎) をクリックします。

  注：Schneider Electric EcoStruxure IT Expert からクローン作成されたインフラストラクチャー・グループの場合、グループ名、説明、およびメンバーシップを変更するには Schneider Electric EcoStruxure IT Expert を使用します。
- 選択したグループを削除するには、「**削除**」アイコン (🗑) をクリックします。
- リソース・グループのメンバーを表示するには、グループ名をクリックし、「グループの表示」ダイアログを表示して、「**メンバーの概要**」タブをクリックします。

オフラインでのデバイスの管理

デバイスが現在リソース・マネージャーで管理されていない場合、Lenovo XClarity Orchestrator を使用して、そのデバイスに関連付けられているサービス・データ・アーカイブをインポートすることで、そのデバイスを*オフライン・モード*で管理できます。

このタスクについて

IMM2 または XCC ベースボード管理コントローラーを備えたサーバーのみをオフラインで管理できます。これらのデバイスは、「オフライン管理対象」接続ステータスを使用して Web インターフェースで認識されます。

オフラインで管理されるデバイスに対して、以下の操作を実行できます。その他のすべての操作は無効です。

- デバイスのインベントリーを表示する
- アラートおよびイベントを除外する
- サービス・データを管理する
- コール・ホームを使用して Lenovo サポート・センターでサービス・チケットを開き、それらのサービス・チケットを管理する
- 保証情報の取得
- これらのデバイスの問題を予測および分析する分析機能

重要：XClarity Orchestrator は、オフライン・デバイスと通信して最新データを取得することはありません。

手順

オフライン・デバイスを管理するには、以下の手順に従ってください。

ステップ 1. Lenovo XClarity Orchestrator のメニュー・バーで、「**リソース**」( ) → 「**サーバー**」の順にクリックします。「サーバー」ページが表示されます。

ステップ 2. 「**インポート**」アイコン ( ) をクリックし、サービス・データ・アーカイブをインポートします。

ステップ 3. 1 つ以上のサービス・データ・アーカイブ (.gz、.tzz または .tgz 形式) 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**」をクリックしてアーカイブを見つけます。

ステップ 4. オプションとして、「**サービス・データのサーバーを表示専用でインベントリーに追加**」を有効にして、オフライン管理モードにある該当するサーバーを管理します (オフラインでのデバイスの管理 を参照)。

ステップ 5. 「**インポート**」をクリックし、アーカイブをインポートして解析します。解析が完了すると、インポートされたアーカイブの解析ステータスが「**解析済み**」に変わります。

ジョブ・ログから、インポートおよび解析プロセスのステータスを監視できます (ジョブの監視)。

終了後

「**管理対象から除外**」アイコン ( ) をクリックすると、オフラインで管理されている選択したデバイスを管理対象から除外できます。

管理対象サーバーでの電源操作の実行

Lenovo XClarity Orchestratorを使用すると、管理対象サーバーの電源オン、電源オフ、再起動を実行できます。

始める前に

事前定義された**スーパーバイザー**または**ハードウェア管理者**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。

ThinkSystem サーバーでは、電源操作を実行するオペレーティング・システムが必要です。

サーバーのオペレーティング・システムが拡張構成と電力インターフェース (ACPI) に準拠しており、シャットダウン操作を許可するように構成されていることを確認します。

このタスクについて

XClarity Orchestratorは、以下の電源操作をサポートしています。
- **電源オン**。現在電源がオフになっている選択済みサーバーの電源をオンにします。
- **通常の電源オフ**。オペレーティング・システムをシャットダウンし、現在電源がオンになっている選択済みサーバーの電源をオフにします。
- **今すぐ電源オフ**。現在電源がオンになっている選択済みサーバーの電源をオフにします。
- **通常の再起動**。オペレーティング・システムをシャットダウンし、現在電源がオンになっている選択済みサーバーを再起動します。
- **今すぐ再起動**。現在電源がオンになっている選択済みサーバーを再起動します。
- **システム・セットアップから再起動**。選択済みサーバーの BIOS/UEFI (F1) セットアップに再起動します。
- **管理コントローラーを再起動**。選択済みサーバーの管理コントローラーを再起動します。

注：

- ThinkEdge クライアント・デバイスの場合、「**通常の再起動**」のみがサポートされます。
- サーバーの接続ステータスがオンラインである必要があります。オフラインのデバイス (オフライン管理対象デバイスなど) では、電源操作を実行できません。

一度に最大 25 台のデバイスに対して電源操作を実行できます。

- **手順**

  サーバーの電源オン、電源オフ、または再起動を行うには、以下の手順を実行します。

単一サーバーの場合

a. XClarity Orchestrator のメニューで、「**リソース**」() → 「**サーバー**」の順にクリックします。すべての管理対象サーバーがテーブル・ビューで「サーバー」カードに表示されます。
b. サーバーの行をクリックすると、該当サーバーのサーバー要約カードが表示されます。
c. クイック操作カードで「**電源操作**」をクリックし、目的の電源操作をクリックします。
d. 「**確認**」をクリックします。

複数のサーバーの場合

a. XClarity Orchestrator のメニューで、「**リソース**」() → 「**サーバー**」の順にクリックします。すべての管理対象サーバーがテーブル・ビューで「サーバー」カードに表示されます。
b. 1 つ以上のサーバーを選択します。最大 25 台のサーバーを選択できます。
c. 「**電源操作**」をクリックし、目的の電源操作をクリックします。

   選択済みデバイスのリストがダイアログに表示されます。該当しない (電源操作をサポートしない) デバイスは、淡色表示されることに注意してください。
d. 「**確認**」をクリックします。

グループ内のすべてのサーバーの場合

a. XClarity Orchestrator のメニューで、「**リソース**」 → 「**グループ**」の順にクリックします。すべてのグループがテーブル・ビューで「グループ」カードに表示されます。
b. サーバーのグループを選択します。
c. クイック操作カードで「**電源操作**」をクリックし、目的の電源操作をクリックします。

   選択済みデバイスのリストがダイアログに表示されます。該当しない (電源操作をサポートしない) デバイスは、淡色表示されることに注意してください。
d. グループ内の特定のサーバーを選択して操作します。最大 25 台のサーバーを選択できます。
e. 「**確認**」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)。

管理対象サーバーのリモート制御セッションの開き方

管理対象サーバーへのリモート制御セッションを、ローカル・コンソールにいるかのように開くことができます。その後、リモート制御セッションを使用して、サーバーの電源のオン/オフや、ローカルまたはリモート・ドライブの論理マウントなどの操作を実行できます。

ThinkSystem または ThinkAgile サーバーのリモート制御セッションの開き方

管理対象 ThinkSystem または ThinkAgile サーバーに対して、ローカル・コンソールにいるかのようにリモート制御セッションを開くことができます。その後、リモート制御セッションを使用して管理操作を実行できます。

始める前に

事前定義された**スーパーバイザー**または**ハードウェア管理者**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。

管理対象サーバーの正常性状態が正常で、接続状態がオンラインである必要があります。サーバー・ステータスの表示について詳しくは、デバイスの詳細の表示を参照してください。

ThinkSystem SR635 および SR655 サーバーの場合は、以下の考慮事項を確認してください。
- ベースボード管理コントローラー・ファームウェア v2.94 以降が必要です。
- マルチユーザー・モードのみがサポートされています。シングルユーザー・モードはサポートされていません。
- Internet Explorer 11 はサポートされていません。
- リモート制御セッションからサーバーの電源をオンまたはオフにすることはできません。

このタスクについて

1 つの ThinkSystem サーバーまたは ThinkAgile サーバーに対して、リモート制御セッションを起動できます。

リモート・コンソールおよびメディア機能の使用の詳細については、ThinkSystem サーバーまたは ThinkAgile サーバーのドキュメントを参照してください。

注：ThinkSystem および ThinkAgile サーバーでは、Java WebStart サポートを使用した Java Runtime Environment (JRE) は必要ありません。

手順

ThinkSystem または ThinkAgile サーバーのリモート制御セッションを開くには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニューで、「**リソース** (⚙)」 ➔ 「**サーバー**」の順にクリックします。すべての管理対象サーバーがテーブル・ビューで「サーバー」カードに表示されます。

ステップ 2. リモート制御するサーバーを選択します。

ステップ 3. 「**リモート制御の起動**」アイコン (🖵) をクリックします。

ステップ 4. Web ブラウザーによるセキュリティ警告をすべて受け入れます。

終了後

リモート制御セッションが正常に開かない場合は、リモート制御に関する問題 XClarity Orchestrator オンライン・ドキュメントを参照してください。

ThinkServer サーバーのリモート制御セッションの開き方

管理対象 ThinkServer サーバーへのリモート制御セッションを、ローカル・コンソールにいるかのように開くことができます。そして、リモート制御セッションを使用して、電源操作やリセット操作、ローカルまたはネットワーク・ドライブのサーバーへの論理マウント、スクリーンショットのキャプチャーやビデオの録画を実行できます。

始める前に

事前定義された**スーパーバイザー**または**ハードウェア管理者**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。

管理対象サーバーの正常性状態が正常で、接続状態がオンラインである必要があります。サーバー・ステータスの表示について詳しくは、デバイスの詳細の表示を参照してください。

ThinkServer System Manager Premium Upgrade の Features on Demand キーを管理対象サーバーにインストールする必要があります。サーバーにインストールされている FoD キーについて詳しくは、Lenovo XClarity Administratorオンライン・ドキュメントのFeatures on Demand キーの表示を参照してください。

Java WebStart サポートのある Java Runtime Environment (JRE) (IcedTea-Web v1.8 プラグインを使用した Adopt OpenJDK 8 など) をローカル・サーバーにインストールしておく必要があります。

このタスクについて

リモート制御セッションは、1 つの ThinkServer サーバーに対してのみ開くことができます。

ThinkServer のリモート・コンソールおよびメディア機能の使用の詳細については、ThinkServer サーバーのドキュメントを参照してください。

手順

ThinkSystem または ThinkAgile サーバーのリモート制御セッションを開くには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニューで、「**リソース** (⚙)」 ➔ 「**サーバー**」の順にクリックします。すべての管理対象サーバーがテーブル・ビューで「サーバー」カードに表示されます。

ステップ 2. リモート制御するサーバーを選択します。

ステップ 3. 「**リモート制御の起動**」アイコン (🖵) をクリックします。

ステップ 4. Web ブラウザーによるセキュリティ警告をすべて受け入れます。

終了後

リモート制御セッションが正常に開かない場合は、リモート制御に関する問題 XClarity Orchestrator オンライン・ドキュメントを参照してください。

System x サーバーのリモート制御セッションの開き方

管理対象 System x サーバーへのリモート制御セッションを、ローカル・コンソールにいるかのように開くことができます。そして、リモート制御セッションを使用して、電源操作やリセット操作、ローカルまたはネットワーク・ドライブのサーバーへの論理マウント、スクリーンショットのキャプチャーやビデオの録画を実行できます。

始める前に

リモート制御セッションを開く前に、セキュリティー、パフォーマンス、キーボードに関する考慮事項を確認してください。これらの考慮事項について詳しくは、リモート制御に関する考慮事項を参照してください。

事前定義された**スーパーバイザー**または**ハードウェア管理者**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。

管理対象サーバーの正常性状態が正常で、接続状態がオンラインである必要があります。サーバー・ステータスの表示について詳しくは、デバイスの詳細の表示を参照してください。

Lenovo XClarity Orchestratorのユーザー・アカウントを使用して、リモート制御セッションにログインします。ユーザー・アカウントは、サーバーにアクセスして管理するのに十分なユーザー権限を持っている必要があります。

Java WebStart サポートのある Java Runtime Environment (JRE) (IcedTea-Web v1.8 プラグインを使用した Adopt OpenJDK 8 など) をローカル・サーバーにインストールしておく必要があります。

リモート・プレゼンスの Features on Demand キーが管理対象サーバーにインストールされ、有効になっている必要があります。リモート・プレゼンスが有効または無効かは、「サーバー」ページで「**フィルター**」 ➔ 「**リモート・プレゼンス**」の順にクリックして確認できます。無効の場合:

- サーバーの正常性状態が正常で、接続状態がオンラインであることを確認します。
- XClarity Controller Enterprise レベルまたは MM 拡張アップグレードが有効になっていることを確認します (これらの機能がデフォルトで有効になっていないサーバーの場合)。

リモート制御セッションでは、ローカル・システムのオペレーティング・システムに定義されているロケールと表示言語の設定が使用されます。

このタスクについて

複数のリモート制御セッションを開始することができます。各セッションで複数のサーバーを管理できます。

注：Flex System x280、x480、x880 サーバーの場合、プライマリー・ノードとのリモート制御セッションのみを開始できます。プライマリー以外のノードへのリモート制御セッションを開始しようとすると、リモート制御ダイアログが開きますが、ビデオは表示されません。

手順

System x サーバーのリモート制御セッションを開くには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニューで、「**リソース** ()」 ➔ 「**サーバー**」の順にクリックします。すべての管理対象サーバーがテーブル・ビューで「サーバー」カードに表示されます。

ステップ 2. リモート制御するサーバーを選択します。

サーバーを選択しない場合、非ターゲットのリモート制御セッションが開きます。

ステップ 3. 「**リモート制御の起動**」アイコン () をクリックします。

ステップ 4. Web ブラウザーによるセキュリティ警告をすべて受け入れます。

ステップ 5. プロンプトが表示されたら、次のいずれかの接続モードを選択します。

- **シングルユーザー・モード**。サーバーとの排他リモート制御セッションを確立します。サーバーから切断するまで、そのサーバーに対する他のすべてのリモート制御セッションはブロックされます。このオプションは、サーバーに対して他のリモート制御セッションが確立されていない場合にのみ使用できます。
- **マルチユーザー・モード**。同じサーバーに対して複数のリモート制御セッションを確立できます。XClarity Orchestrator では、1 つのサーバーに対して最大 6 つの同時リモート制御セッションがサポートされます。

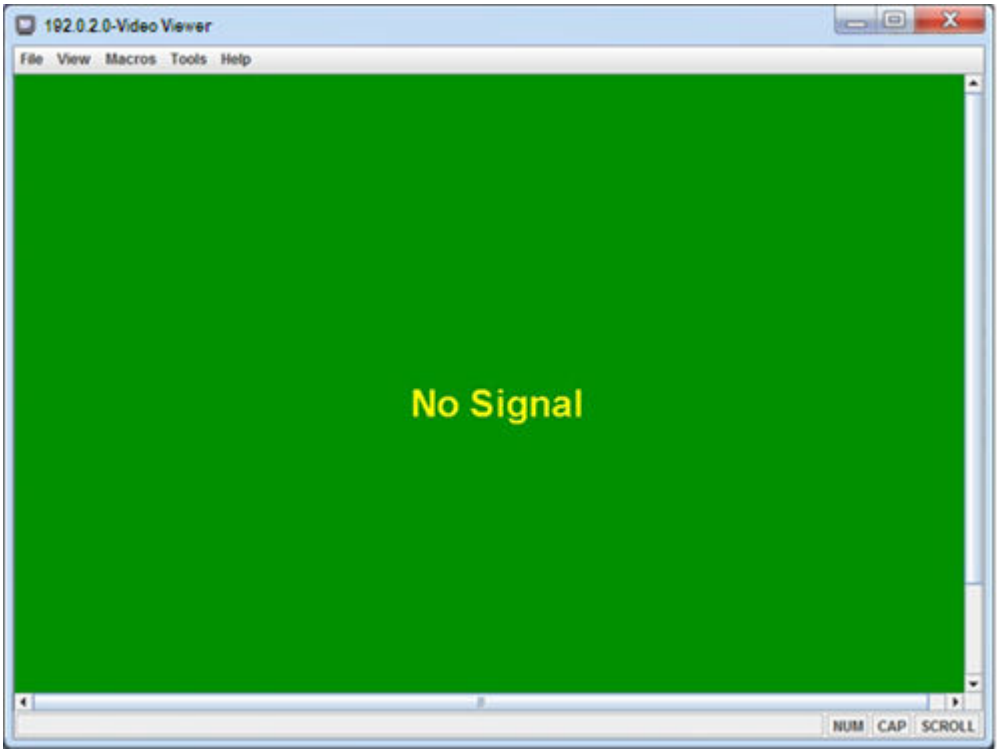
ステップ 6. **リモート制御の起動**をクリックします。

ステップ 7. プロンプトが表示されたら、ローカル・システムのリモート制御セッションにショートカットを保存するかどうかを選択します。このショートカットを使用して、XClarity Orchestrator Web インターフェースにログインしないでリモート制御セッションが起動できます。このショートカットには、手動でサーバーを追加できる空のリモート制御セッションを開くリンクが含まれています。

注：XClarity Orchestrator認証サーバーでユーザー・アカウントを検証するには、ローカル・システムがXClarity Orchestratorにアクセスできる必要があります。

終了後

リモート制御セッションには、セッションを通じて現在管理されている各サーバのサムネール (アイコン) があります。



リモート制御セッションが正常に開かない場合は、リモート制御に関する問題 XClarity Orchestrator オンライン・ドキュメントを参照してください。

リモート制御セッションでは、以下の操作を実行できます。

- 複数のサーバー・コンソールを表示し、サムネールをクリックしてサーバー・コンソール間を移動する。サーバー・コンソールがビデオ・セッション領域に表示されます。アクセスしているサーバーが多

すぎてアイコン領域に表示しきれない場合は、「**右にスクロール**」アイコン () と「**左にスクロール**」アイコン () をクリックすると、画面がスクロールしてその他のサーバーのサムネールが表示されます。「**すべてのセッション**」アイコン () をクリックすると、開いているすべてのサーバー・セッションのリストが表示されます。

- 「**サーバーの追加**」アイコン () をクリックして、サーバー・コンソールを現在のリモート制御セッションに追加します。
- サムネール領域の表示/非表示を切り替えるには、「**サムネール切り替え**」アイコン () をクリックします。
- リモート制御セッションをウィンドウまたはフルスクリーンとして表示するには、「**画面**」アイコン () をクリックし、「**フルスクリーンをオンに切り替え**」または「**フルスクリーンをオフに切り替え**」をクリックします。
- スティッキー・キー・ボタンの Ctrl、Alt、および Shift を使用して、サーバーに直接キー・ストロークを送信します。スティッキー・キーをクリックすると、キーボード・キーを押したり、ボタンをもう一度クリックしたりするまで、キーはアクティブなままです。Ctrl キーまたは Alt キーの組み合わせを送信するには、ツールバーの「Ctrl」または「Alt」をクリックし、カーソルをビデオ・セッション領域に置いて、キーボードのキーを押します。

  注：マウス・キャプチャー・モードが有効になっている場合は、カーソルをビデオ・セッション領域の外に移動するには左 Alt キーを押す必要があります。マウス・キャプチャー・モードはデフォルトで無効になっていますが、「ツールバー」ページで有効にすることができます (リモート制御の設定を参照)。
- 「**キーボード**」アイコン () をクリックして、ソフトキーと呼ばれるカスタム・キー・シーケンスを定義します。ソフト・キー定義は、リモート制御セッションを開始したシステムに保管されます。そのため、別のシステムからリモート制御セッションを開始する場合は、ソフトキーを定義し直す必要があります。ソフトキーを含むユーザー設定をエクスポートするには、「**設定**」アイコン () をクリックし、「**ユーザー設定**」タブをクリックして、「**インポート**」をクリックします。
- 現在選択されているサーバー・セッションのスクリーン・キャプチャーを取得してさまざまな形式で保存するには、「**画面**」アイコン () をクリックし、「**スクリーンショット**」をクリックします。
- リモート・メディア (CD、DVD、USB の各デバイスや、ディスク・イメージ、CD (ISO イメージ) など) を選択したサーバーにマウントするか、「**リモート・メディア**」アイコン () をクリックして、マウントされたデバイスを別のサーバーに移動します。
- 「**リモート・メディア**」アイコン () をクリックし、「**リモート・メディアのマウント**」をクリックして「**イメージを IMM にアップロードする**」をクリックして、リモート・メディアからサーバーにイメージをアップロードします。
- 「**電源**」アイコン () をクリックして、リモート・コンソールからサーバーの電源をオンまたはオフにします。
- サーバー・アイコンの更新頻度など、リモート制御設定を変更します (リモート制御の設定を参照)。

リモート制御に関する考慮事項

リモート制御セッションを使用した管理対象サーバーへのアクセスについてセキュリティー、パフォーマンス、キーボードに関する考慮事項を把握しておく必要があります。

セキュリティーに関する考慮事項

リモート制御セッションの開始に使用するユーザー・アカウントは、Lenovo XClarity Orchestrator 認証サーバーに定義されている有効なユーザー・アカウントであることが必要です。ユーザー・アカウントには、サーバーにアクセスして管理するための十分なユーザー権限が必要です。

デフォルトでは、複数のリモート制御セッションをサーバーに対して確立できます。ただし、リモート制御セッションを開始するとき、シングルユーザー・モードでセッションを開始してサーバーに対して排

他的なセッションを確立するオプションがあります。サーバーから切断するまで、そのサーバーに対する他のすべてのリモート制御セッションはブロックされます。

注：このオプションは、サーバーに対して他のリモート制御セッションが現在確立されていない場合にのみ使用できます。

連邦情報処理規格 (FIPS) 140 を使用するには、ローカル・システムで以下の手順を実行して FIPS 140 を手動で有効にする必要があります。

1. ローカル・システムにインストールされた FIPS 140 認定の暗号プロバイダーのプロバイダー名を見つけます。
2. ファイル `$(java.home)/lib/security/java.security` を編集します。
3. `com.sun.net.ssl.internal.ssl.Provider` を含む行に FIPS 140 認定の暗号プロバイダーの名前を追加します。例えば、以下のように変更します。
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   次のように変更できるようにします:
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

パフォーマンスに関する考慮事項

リモート制御セッションが低速になるか応答しなくなった場合は、選択したサーバーに対して確立しているすべてのビデオおよびリモート・メディア・セッションを終了し、サーバーに対して開いている接続の数を減らします。また、以下の設定を変更することで、パフォーマンスが向上することがあります。詳しくは、リモート制御の設定を参照してください。

- KVM
  - アプリケーションによって使用されるビデオ帯域幅のパーセンテージを減らす。リモート制御セッションのイメージ品質が下がります。
  - アプリケーションによって更新されるフレームのパーセンテージを減らす。これにより、リモート制御セッションの更新頻度が低下します。
- **サムネール**
  - サムネールの更新間隔を長くする。これにより、アプリケーションによるサムネールの更新速度が遅くなります。
  - サムネールを非表示にする。

リモート制御セッション・ウィンドウのサイズとアクティブなセッションの数は、ワークステーションのリソース (メモリーやネットワーク帯域幅など) に影響を与える場合があり、その結果、パフォーマンスに影響することがあります。リモート制御セッションではソフト・リミットとして、開くセッションは 32 個までに制限されます。32 個を超えるセッションを開いた場合、パフォーマンスが大幅に低下し、リモート制御セッションが応答しなくなることがあります。ネットワーク帯域幅やローカル・メモリーなどのリソースが十分でない場合は、開いたセッションが 32 個未満であっても、パフォーマンスが低下することがあります。

キーボードに関する考慮事項

リモート制御セッションでは以下のキーボード・タイプがサポートされています。

- ベルギー語 105 キー
- ブラジル語
- 中国語
- フランス語 105 キー
- ドイツ語 105 キー
- イタリア語 105 キー
- 日本語 109 キー
- 韓国語
- ポルトガル語

- ロシア語
- スペイン語 105 キー
- スイス語 105 キー
- 英語 (英国) 105 キー
- 英語 (米国) 104 キー

キーボード設定については、リモート制御の設定を参照してください。

リモート制御の設定

現在のリモート制御セッションの設定を変更できます。

手順

リモート制御設定を変更するには、以下の手順を実行します。

ステップ 1. リモート制御の設定を変更するには、「**設定**」アイコン () をクリックします。変更はすべて即時に有効になります。

- KVM
  - 「**ビデオ帯域幅の比率**」。帯域幅を増やすと、リモート制御セッションの外観の品質は改善されますが、リモート制御セッションのパフォーマンスに影響を与える可能性があります。
  - 「**フレームの更新率**」。フレーム・リフレッシュのパーセントを高くすると、リモート制御セッションの更新頻度は高くなりますが、リモート制御セッションのパフォーマンスに影響を与える可能性があります。
  - 「**キーボードの種類**」。リモート制御セッションで使用しているキーボードのタイプを選択します。選択するキーボードタイプは、ローカル・システムのキーボード設定、およびリモート・ホストのキーボード設定と一致している必要があります。

    注：国際キーボードを選択する場合に、オルタネート・グラフィック・キー (AltGr) を必要とするキーの組み合わせを入力するには、リモート制御セッションの呼び出しに使用するワークステーションのオペレーティング・システムと、リモート・アクセスするサーバーのオペレーティング・システムが、同じタイプである必要があります。たとえば、サーバーで Linux が実行されている場合は、Linux を実行しているワークステーションでリモート制御アプリケーションを呼び出す必要があります。
  - 「**イメージをウィンドウに合わせる**」。サーバーから受け取るビデオ・イメージをビデオ・セッション領域のサイズに合わせるには、このオプションを選択します。
- **セキュリティー**
  - 「**シングルユーザー・モード接続を使用**」。サーバーに接続するときにデフォルトでシングルユーザー・モード接続を使用するかどうかを指定します。シングルユーザー・モードで接続すると、サーバーに接続できるのは一度に 1 人のユーザーのみになります。このボックスが選択されていない場合のデフォルトの機能では、マルチユーザー・モードでサーバーに接続します。
  - 「**(安全な) トンネリング接続を要求する**」。管理ノードを介してサーバーにアクセスするには、このオプションを選択します。このオプションを使用すると、サーバーと同じネットワーク上にないクライアントからサーバーにアクセスできます。

    注：リモート制御アプリケーションは常に、リモート制御が開始されたローカル・システムからサーバーに直接接続しようとします。このオプションを選択すると、クライアント・ワークステーションから直接サーバーにアクセスできない場合には、リモート制御アプリケーションは Lenovo XClarity Orchestrator を介してサーバーにアクセスします。
- **ツールバー**

注：このページのすべての設定をデフォルト設定に復元するには、「**デフォルトの復元**」をクリックします。

- 「**ツールバーをウィンドウにピン留め**」。デフォルトでは、ツールバーはリモート制御セッション・ウィンドウの上に隠れていて、その上にマウス・ポインターを置いたときにのみ表示されます。このオプションを選択すると、ツールバーがウィンドウに固定され、サムネール・パネルとリモート制御セッション・ウィンドウとの間に常に表示されます。
- 「**キーボード・ボタンを表示する**」。ツールバーにキーボード・ボタンのアイコン (CapsLock、NumLock、ScrollLock) を表示するかどうかを指定します。
- 「**電源制御を表示する**」。ツールバーに電源制御オプションを表示するかどうかを指定します。
- 「**スティッキー・キー・ボタンを表示する**」。ツールバーにスティッキー・キー・ボタンのアイコン (Ctrl、Alt、Delete) を表示するかどうかを指定します。
- 「**ローカル・マウス・ポインターを非表示にする**」。現在ビデオ・セッション領域に表示されているサーバー・セッションにカーソルを置いたときにローカル・マウス・ポインターを表示するかどうかを指定します。
- 「**マウス・キャプチャー・モードの有効化**」。デフォルトでは、マウス・キャプチャー・モードは無効になっています。そのため、カーソルをビデオ・セッション領域の内外に自由に移動できます。マウス・キャプチャー・モードを有効にすると、左 Alt キーを押さないとカーソルをビデオ・セッション領域の外に移動できなくなります。マウス・キャプチャー・モードが有効になっている場合は、Ctrl+Alt キーを使用してマウス・キャプチャー・モードを終了するかどうかを指定できます。デフォルトでは左 Alt キーを使用します。
- 「**ツールバーの背景の不透明度を指定**」。不透明度を下げると、ツールバーの背景越しにビデオ・セッション領域が表示されるようになります。

  注：このオプションは、ツールバーがウィンドウに固定されていないときにのみ使用可能です。

- **サムネール**
  - 「**サムネールを表示する**」。リモート制御セッションでサムネール域を表示するには、このオプションを選択します。
  - 「**サムネールの更新間隔を指定**」。サムネールの更新間隔を短くすると、サーバーのサムネールが更新される頻度が高くなります。
- **全般**
  - 「**デバッグ・モード**」。リモート制御アプリケーションにデバッグ・モードを設定するかどうかを指定します。この設定により、ログ・ファイルに記録されるイベントの詳細レベルが決まります。デフォルトでは、重大なイベントのみが記録されます。
  - 「**システムの外観設定の継承**」。この設定では、ローカル・サーバー (Windows を実行しているサーバー) に対して構成されている配色に合わせて外観が変更されます。これらの設定を有効にするには、リモート制御アプリケーションを再起動する必要があります。
  - 「**デスクトップ・アイコンの作成**」。この設定では、リモート制御アプリケーションをシステムから直接起動できるようにローカル・システムにデスクトップ・アイコンが作成されます。この場合も、管理ソフトウェアへのアクセスは必要です。
  - 「**管理サーバーと同期**」。この設定を使用すると、リモート制御アプリケーションに表示されるサーバー・データが、管理ソフトウェアから表示されるサーバー・データと一致するようになります。

第 5 章　リソースのプロビジョニング

Lenovo XClarity Orchestrator を使用して、Lenovo XClarity Administrator リソース・マネージャーと管理対象サーバーへの更新のデプロイおよび管理対象サーバーの構成など、管理対象リソースをプロビジョニングできます。

サーバー構成のプロビジョニング

サーバー構成パターンを使用すると、定義済み構成設定の単一のセットから複数のサーバーを迅速に構成できます。各パターンでは、特定のサーバー・タイプの構成の特性を定義します。既存のサーバーから設定を学習して、サーバー・パターンを作成できます。

始める前に

構成するサーバーが最新のファームウェアで最新の情報に更新されている必要があります。

このタスクについて

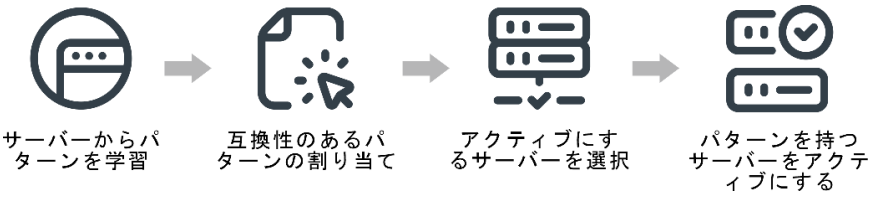
パターンを使用したサーバーの構成は ThinkSystem サーバーでのみサポートされています (SR635 および SR655 を除く)。

サーバー構成パターンを使用して、管理対象サーバーのベースボード管理コントローラーと Unified Extensible Firmware Interface (UEFI) の設定および定義を構成することができます。パターンは I/O アドレスの仮想化のサポートを統合しているため、サーバー・ファブリック接続を仮想化したり、ファブリック接続を中断せずにサーバーの再利用を実行したりできます。

以下の設定を構成することはできません。
- ブート順序
- ローカル・ストレージと SAN ゾーニング
- I/O アダプター
- ローカル・ユーザー・アカウント
- LDAP サーバー

手順

次の図は、管理対象サーバーの構成のワークフローを示しています。



ステップ 1. **サーバー・パターンを作成する**

既存のサーバーの構成設定と定義を学習することで、データ・センターで使用されるさまざまな構成を表すパターンを作成できます。

重要：データ・センター内のサーバーのタイプごとに新しいサーバー・パターンを作成する方法を検討してください。たとえば、すべての ThinkSystem SR650 サーバー用のサーバー・パターンと、すべての ThinkSystem SR850 サーバー用のサーバー・パターンを作成します。別のサーバー・タイプ用のサーバー構成パターンをデプロイしないようにしてください。

サーバー・パターンの作成について詳しくは、既存のサーバーからのサーバー構成パターンの学習を参照してください。

ステップ 2. **パターンを 1 台以上の管理対象サーバーに割り当てる**

パターンを複数のサーバーに割り当てることができます。ただし、各サーバーに割り当てられるパターンは 1 つのみ (XClarity Orchestrator) です。

データ・センター内のサーバーのタイプごとに新しいサーバー・パターンを作成する方法を検討してください。たとえば、すべての ThinkSystem SR650 サーバー用のサーバー・パターンと、すべての ThinkSystem SR850 サーバー用のサーバー・パターンを作成します。

別のサーバー・タイプ用のサーバー・パターンを割り当てたり、デプロイしたりしないようにしてください。

適用可能なパターンを 1 つ以上のターゲット・サーバーに割り当てると、サーバーでXClarity Orchestratorがコンプライアンス・チェックを実行し、サーバー構成がパターンと一致するかどうかを判断します。割り当てられたパターンに適合していないサーバーにフラグが付けられます。

サーバー・パターンの作成について詳しくは、リソース・マネージャーへの更新の適用とアクティブ化を参照してください。

ステップ 3. **割り当てられたパターンをターゲット・サーバーにデプロイする**

1 つ以上の特定のサーバーまたはサーバーのグループに割り当てられたパターンをデプロイできます。パターンをデプロイすると、そのパターンの構成設定と定義が共有メモリーに書き込まれ、その後アクティブになります。一部の設定では、アクティブになる前にシステムのリブートが必要です。

ベースボード管理コントローラーや Unified Extensible Firmware Interface (UEFI) 構成設定など、特定の構成の変更をアクティブにするには、サーバーを再起動する必要があります。変更をいつアクティブにするかを選択できます。

- **据え置きアクティベーション**は、次回のサーバーの再起動後に構成の変更をすべてアクティブにします。デプロイメント・プロセスを続行するには、ターゲット・サーバーを手動で再起動する必要があります。

  重要：「**通常の再起動**」を使用してサーバーを再起動し、更新プロセスを続行します。「**今すぐ再起動**」を使用 *しないでください*。

注：割り当てられたパターンではなくサーバーで直接設定が変更された場合、または割り当てられたパターンのデプロイ時に問題が発生した場合 (ファームウェアの問題や無効な設定など)、サーバーでの設定がパターンに適合しなくなる可能性があります。「**割り当てとデプロイ**」タブから、各サーバーのコンプライアンス・ステータスを調べることができます。

注意：XClarity Orchestrator は、サーバー・パターンをデプロイする際に、IP アドレスと I/O アドレスを個々のサーバーに割り当てません。

更新コンプライアンス・ポリシーの作成について詳しくは、サーバー構成パターンの割り当てとデプロイ を参照してください。

ステップ 4. **パターンを変更して再デプロイする**

既存のパターンの構成を後から変更することができます。パターンを保存すると、そのパターンが割り当てられているサーバーでXClarity Orchestratorがコンプライアンス・チェックを実行し、サーバーの構成がパターンと一致するかどうかを判断します。その後、変更したパターンを、そのパターンが割り当てられているサーバーのすべてまたはサブセットに再デプロイできます。

サーバー構成に関する考慮事項

Lenovo XClarity Orchestrator を使用してサーバーの構成を開始する前に、以下の重要な考慮事項を確認してください。

サーバーに関する考慮事項

- パターンを使用したサーバーの構成は ThinkSystem サーバーでのみサポートされています (SR635 および SR655 を除く)。
- 構成するサーバーが最新のファームウェアで最新の情報に更新されている必要があります。

構成パターンに関する考慮事項

- パターンを複数のサーバーに割り当てることができます。ただし、各サーバーに割り当てられるパターンは 1 つのみ (XClarity Orchestrator) です。

  注：XClarity Orchestratorは、Lenovo XClarity Administratorで割り当てられたパターンまたはサーバー・プロファイルがあるサーバーにサーバー構成パターンを割り当てたりデプロイしたりすることを妨げるものではありません。XClarity Orchestratorを使用してパターンをデプロイすると 、XClarity Administratorのパターンのコンプライアンスに影響を及ぼす場合があります。

- サーバー構成パターンを使用して、管理対象サーバーのベースボード管理コントローラーと Unified Extensible Firmware Interface (UEFI) の設定および定義を構成することができます。パターンは I/O アドレスの仮想化のサポートを統合しているため、サーバー・ファブリック接続を仮想化したり、ファブリック接続を中断せずにサーバーの再利用を実行したりできます。

  以下の設定を構成することはできません。
  - ブート順序
  - ローカル・ストレージと SAN ゾーニング
  - I/O アダプター
  - ローカル・ユーザー・アカウント
  - LDAP サーバー
- データ・センター内のサーバーのタイプごとに新しいサーバー・パターンを作成する方法を検討してください。たとえば、すべての ThinkSystem SR650 サーバー用のサーバー・パターンと、すべての ThinkSystem SR850 サーバー用のサーバー・パターンを作成します。
- 別のサーバー・タイプ用のサーバー・パターンを割り当てたり、デプロイしたりしないようにしてください。
- サーバーの設定は、以下のインスタンスで割り当てられたパターンに準拠しなくなる可能性があります。「**割り当てとデプロイ**」タブから、各サーバーのコンプライアンス・ステータスを調べることができます。
  - 構成設定は、割り当てられたパターンではなく、サーバーで直接変更されました。
  - パターンのデプロイ中に問題が発生しました。ファームウェアの問題、または無効な設定です。
  - ファームウェアが更新され、構成設定と定義が変更されました。

    注：割り当てられたパターンが以前のファームウェア・レベルに基づいている場合、デプロイメントが失敗することがあります。この場合は、インストールされている現在のファームウェアに基づいて新しいパターンを学習するか、既存のパターンを変更して特定の項目の構成を除外してから、そのパターンをデプロイすることをお勧めします。

構成プロセスに関する考慮事項

- 構成の進行中は、ターゲット・サーバーがロックされています。構成プロセスが完了するまでは、ターゲット・サーバー上にある他の管理タスクを開始できません。
- 構成パターンをサーバーにデプロイした後、変更を完全にアクティブ化するために再起動が 1 回以上必要になる場合があります。サーバーをすぐに再起動してすべての変更をアクティブにできます。サーバーをすぐに再起動する場合は、XClarity Orchestratorで必要な再起動回数を最小限に抑えま

す。据え置きアクティベーションにすることを選択した場合、次回サーバーが再起動されたときにすべての変更がアクティブ化されます。部分的なアクティベーションを選択した場合、サーバーの再起動を必要としない変更が即時にアクティブになり、次回サーバーが再起動されると、他のすべての変更がアクティブになります。

- ターゲット・サーバーで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、構成ジョブは他のジョブがすべて完了するまでキューに入れられます。
- 一部の拡張サーバーの機能は Features on Demand キーを使用してアクティブ化されます。UEFI セットアップ中に提示される構成可能な設定がある機能の場合、構成パターンを使用して設定を構成できます。ただし、設定した構成は対応する Features on Demand キーがインストールされるまでアクティブ化されません。

既存のサーバーからのサーバー構成パターンの学習

サーバー構成パターンでは、特定のサーバー・タイプの構成の特性を定義します。既存のサーバーから設定を学習して、サーバー・パターンを作成できます。

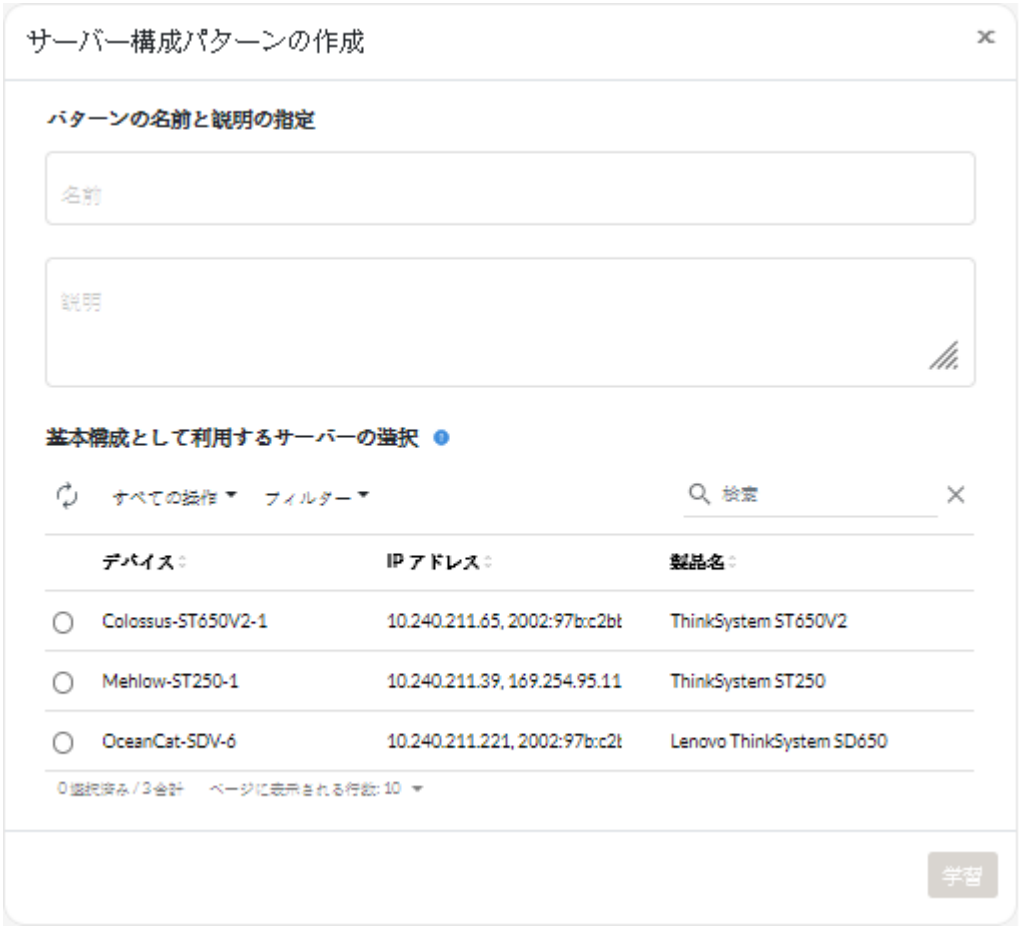
始める前に

- サーバー構成パターンを作成する前に、サーバー構成に関する考慮事項を確認してください (デプロイメントの考慮事項の更新を参照)。
- パターンの作成に使用するサーバーがオンラインであることを確認します。
- 同じハードウェア・オプションを持ち、同じように構成する必要があるサーバーのグループを特定します。サーバー・パターンを使用すると、複数のサーバーに同じ構成設定をデプロイできるため、共通の構成を 1 か所から制御できます。

既存のサーバーの構成を学習してパターンを作成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator のメニュー・バーで「**プロビジョニング**」( ) → 「**サーバー構成**」をクリックした後「**パターン**」タブをクリックし、「サーバー構成パターン」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、「サーバー構成パターンの作成」ダイアログを表示します。



ステップ 3. パターンの名前および説明 (任意) を指定します。

ステップ 4. このパターンのベースとして使用するサーバーを選択します。

注：サポートされていないデバイス・モデルはグレーのテキストで表示されており選択できません。

ステップ 5. 「**学習**」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)。

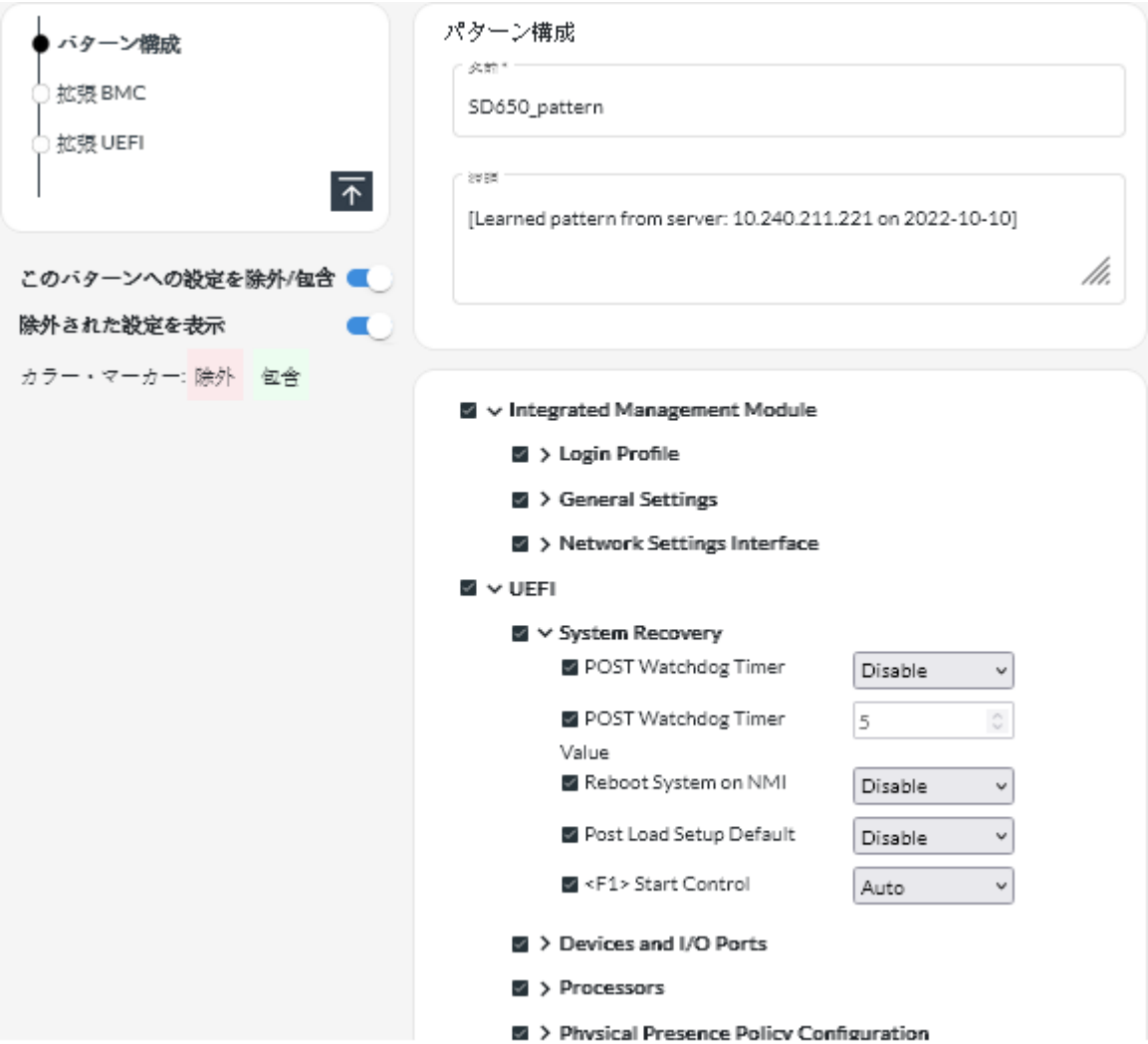
終了後

「パターン」カードから、以下の操作を実行できます。

- パターンの詳細を表示するには、パターンの行をクリックします。
- 「**コピー**」アイコン ( ) をクリックして、選択済みパターンをコピーします。
- パターンの詳細を表示するためにパターンの行をクリックし、必要な変更を加えた後「**保存**」をクリックして、パターンの構成設定を変更します。デフォルトでは、学習した設定はすべてパターンに含まれます。パターンから設定を除外するには、「**パターンへの設定を除外/包含**」を選択し、パターンに含めない設定をクリアします。クリアされた (除外マークが付いている) 設定は、黄色で強調表示されます。「**保存**」をクリックすると、パターンに含まれる設定だけが表示されます。除外した設定を再び含めるには、「**パターンへの設定を除外/包含**」をクリックし、「**除外された設定を表示**」をクリックしてから、パターンに含める設定を選択します。選択された (包含マークが付いている) 設定は、緑色で強調表示されます。

注：コンプライアンスの確認は、含まれる設定にのみ基づいて行います。除外した設定はチェックが行われません。

変更されたパターンを保存すると、そのパターンが割り当てられているサーバーでXClarity Orchestratorがコンプライアンス・チェックを実行し、サーバーの構成がパターンと一致するかどうかを判断します。その後、変更したパターンを非適合のサーバーにデプロイできます (サーバー構成パターンの割り当てとデプロイを参照)。



- パターンの詳細を表示するためにパターンの行をクリックし、構成パターンをコピーした後「**名前を付けて保存**」をクリックします。
- 選択済みパターンを削除するには、「**削除**」アイコン () をクリックします。パターンが 1 つ以上のサーバーに割り当てられている場合、適用可能なサーバーのリストがダイアログに表示されます。削除要求を確認すると、それらのサーバーからパターンの割り当てが解除されます。

  注：サーバーにアクティブにデプロイされているパターンは削除できません。
- パターンを 1 つ以上のターゲット・サーバーに割り当て、デプロイします (サーバー構成パターンの割り当てとデプロイを参照)。

サーバー構成パターンの割り当てとデプロイ

1 つ以上の管理対象サーバーに対してサーバー構成パターンを割り当て、デプロイできます。

始める前に

- サーバーにパターンを割り当てる、またはデプロイする前に、サーバー構成に関する考慮事項を確認してください (デプロイメントの考慮事項の更新を参照)。
- 構成するサーバーが最新のファームウェアで最新の情報に更新されている必要があります。
- 別のサーバー・タイプ用のサーバー・パターンを割り当てたり、デプロイしたりしないようにしてください。
- XClarity Orchestratorは、Lenovo XClarity Administratorで割り当てられたパターンまたはサーバー・プロファイルがあるサーバーにサーバー構成パターンを割り当てたりデプロイしたりすることを妨げるものではありません。XClarity Orchestratorを使用してパターンをデプロイすると 、XClarity Administratorのパターンのコンプライアンスに影響を及ぼす場合があります。
- XClarity Orchestrator は、サーバー・パターンをデプロイする際に、IP アドレスと I/O アドレスを個々のサーバーに割り当てません。

このタスクについて

パターンをサーバーに割り当てると、XClarity Orchestratorがコンプライアンス・チェックを実行してサーバー上の現在の構成設定と構成パターンの設定を比較し、その結果に基づいて「**コンプライアンス・ステータス**」列を更新します。コンプライアンス・ステータスは以下のいずれかの値です。

- **適合**。割り当てられたパターンのすべての構成設定が、サーバーの設定と一致しています。
- **非適合**。割り当てられたパターンの 1 つ以上の構成設定が、サーバーの設定と一致*しません*。テーブル・セルの上にマウスを合わせると、設定と値の不一致を一覧表示するポップアップが表示されます。
- **保留中**.パターン・デプロイメントまたはコンプライアンス・チェックが進行中です。
- **再起動を保留中**。パターン・デプロイメント後に構成の変更をアクティブにするには、サーバーを再起動する必要があります。
- **利用できない**。パターンがサーバーに割り当てられていません。

パターンをサーバーにデプロイすると、XClarity Orchestratorは割り当てられたサーバー構成パターンに合わせてサーバーの設定を変更します。デプロイが完了したら、XClarity Orchestratorでコンプライアンス・チェックを実行して割り当てられたパターンの設定がサーバーの設定と一致しているかを検証し、サーバーのコンプライアンス・ステータスを更新します。

手順

サーバー構成パターンを 1 台以上のサーバーに割り当ててデプロイするには、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「**プロビジョニング**」( ) → 「**サーバー構成**」をクリックし、「**割り当てとデプロイ**」タブをクリックして、「サーバー構成パターンの割り当てとデプロイ」カードを表示します。

ステップ 2. パターンを 1 つ以上のサーバーに割り当てます。

1. 1 つ以上のサーバーを選択します。
2. 「**割り当て**」アイコン ( ) をクリックして、「サーバー構成パターンの割り当て」ダイアログを表示します。

3. 割り当てるパターンを選択します。

注：

- このリストには、特定のサーバーのすべての適用可能なパターンが表示されます。リストは、Orchestrator サーバーが該当するパターンを計算している場合は、不完全である可能性があります。この場合は、ダイアログを閉じて、しばらく待ってから、ダイアログを再度開いてください。

- 「**割り当てなし**」パターンを選択して、選択したデバイスのリストからパターンの割り当てを解除します。

4. 割り当てルールを選択します。これは以下のいずれかの値です。
   - **適用可能なすべてのデバイス (割り当てられているパターンを上書き)**
   - **パターンが割り当てられていない適用可能なデバイス**
   - **選択した適用可能なデバイスのみ (割り当てられているパターンを上書き)**
   - **パターンが割り当てられていない、選択した適用可能なデバイスのみ**
5. 「**割り当て**」をクリックします。

ステップ 3. 割り当てられたパターンを特定のサーバーにデプロイします。

1. 1 つ以上のサーバーを選択します。

   注：サポートされていないデバイス・モデルはグレーのテキストで表示されており選択できません。
2. 「**デプロイ**」アイコン (⎙) をクリックして、「サーバー構成パターンのデプロイ」ダイアログを表示します。

3. 更新をいつアクティブにするかを選択します。
   - **据え置きアクティベーション**は、次回のサーバーの再起動後に構成の変更をすべてアクティブにします。デプロイメント・プロセスを続行するには、ターゲット・サーバーを手動で再起動する必要があります。

     重要：「**通常の再起動**」を使用してサーバーを再起動し、更新プロセスを続行します。「**今すぐ再起動**」を使用 *しないでください*。
4. 「**デプロイ**」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)。

終了後

「パターン」カードから、以下の操作を実行できます。

- 「**すべての操作**」 ➡ 「**コンプライアンスの確認**」をクリックして、選択したサーバーで構成コンプライアンスの確認を手動で実行します。

- 「**割り当てなし**」パターンを割り当て、1 つ以上のターゲット・サーバーからパターンの割り当てを解除します。
- 「**レポート・フォワーダーの作成**」アイコン (⊕) をクリックして、反復ベースの構成コンプライアンスに関するレポートを 1 つ以上のメールアドレスに転送します。レポートは、現在テーブルに適用されているデータ・フィルターを使用して送信されます。表示および非表示されたテーブルのすべての列がレポートに含まれます。詳しくは、レポートの転送を参照してください。
- 「**レポート・フォワーダーに追加**」アイコン (↱) をクリックして、テーブルに現在適用されているデータ・フィルターを使用して、特定のレポート・フォワーダーに構成コンプライアンス・レポートを追加します。レポート・フォワーダーに構成コンプライアンス・レポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。

サーバー構成のコンプライアンスの維持

構成パターンを使用せず設定が変更された場合、構成パターンの適用中に問題が発生した場合 (たとえば、サーバーにあるものよりも下位のファームウェア・レベルからパターンが作成された場合)、またはサーバー構成を変更したファームウェア更新の適用中に問題が発生した場合 (たとえば、設定が追加または削除されたり、設定の動作が変更されたり、新しい選択項目が追加されたり、値範囲が変更されたりした場合)、サーバーの設定がコンプライアンス違反になります。

このタスクについて

「サーバー構成: 割り当てとデプロイ」ページの「**コンプライアンス・ステータス**」列から、各サーバーのコンプライアンス・ステータスを調べることができます。サーバーが非適合の場合は、ステータスの上にカーソルを置き、理由を判別します。

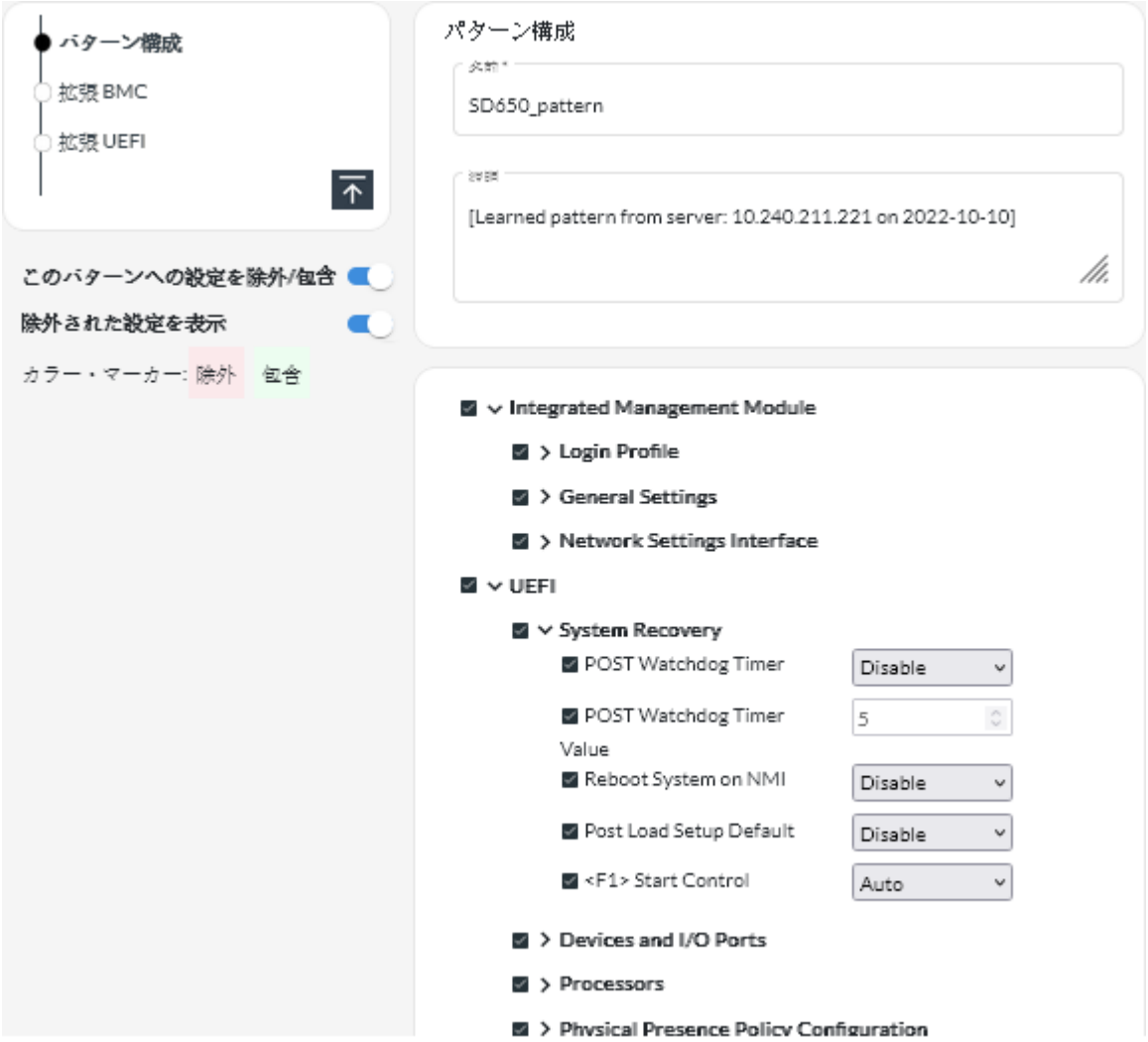
手順

構成のコンプライアンスの問題を修復するには、以下のいずれかの手順を実行します。

- 現在のファームウェア・レベルに基づいて新しい構成パターンを学習します (既存のサーバーからのサーバー構成パターンの学習を参照)。次に、そのパターンをサーバーに割り当て、適用します (サーバー構成パターンの割り当てとデプロイを参照)。
- パターンの詳細を表示するためにパターンの行をクリックし、必要な変更を加えた後「**保存**」をクリックして、該当する構成パターンを変更して非適合設定を修正します。デフォルトでは、学習した設定はすべてパターンに含まれます。パターンから設定を除外するには、「**パターンへの設定を除外/包含**」を選択し、パターンに含めない設定をクリアします。クリアされた (除外マークが付いている) 設定は、黄色で強調表示されます。「**保存**」をクリックすると、パターンに含まれる設定だけが表示されます。除外した設定を再び含めるには、「**パターンへの設定を除外/包含**」をクリックし、「**除外された設定を表示**」をクリックしてから、パターンに含める設定を選択します。選択された (包含マークが付いている) 設定は、緑色で強調表示されます。

  注：コンプライアンスの確認は、含まれる設定にのみ基づいて行います。除外した設定はチェックが行われません。

  変更されたパターンを保存すると、そのパターンが割り当てられているサーバーでXClarity Orchestratorがコンプライアンス・チェックを実行し、サーバーの構成がパターンと一致するかどうかを判断します。その後、変更したパターンを非適合のサーバーにデプロイできます (サーバー構成パターンの割り当てとデプロイを参照)。



- パターンの詳細を表示するためにパターンの行をクリックし、必要な変更を加えた後「**名前を付けて保存**」をクリックして、構成パターンの変更されたコピーを作成します。次に、そのパターンを非適合サーバーに割り当て、適用します (サーバー構成パターンの割り当てとデプロイを参照)。

オペレーティング・システムのプロビジョニング

Lenovo XClarity Orchestrator を使用して OS イメージ・リポジトリーを管理し、オペレーティング・システム・イメージをデプロイできます。

始める前に

XClarity Orchestrator では、オペレーティング・システムはデバイスに直接デプロイされません。代わりに、デプロイメントを実行するために適切なリソース・マネージャーに要求が送信されます。リソース・マネージャーに、OS デプロイメント機能を実行するために必要なライセンスがインストールされていることを確認します。

ご使用の管理対象デバイスにオペレーティング・システムをデプロイする前に、デプロイメントの考慮事項を確認してください (オペレーティング・システム・デプロイメントの考慮事項 を参照)。

管理対象サーバーのすべてのファームウェアが最新レベルであることを確認します (管理対象リソースへの更新のプロビジョニング を参照)。

管理対象サーバーの構成が最新の情報に更新されていることを確認します (サーバー構成のプロビジョニング を参照)。

注意：Converged と ThinkAgile アプライアンスでのベアメタル・オペレーティング・システム・デプロイメントを実行するために、XClarity Orchestrator を使用*しない*ことをお勧めします。

注：サーバーが XClarity Administrator v4.0 以降を使用して管理されていることを確認します。

このタスクについて

XClarity Orchestrator には、オペレーティング・システム・イメージを *ベア・メタル・サーバー*にデプロイする簡単な方法が用意されています。このベア・メタル・サーバーには、通常、オペレーティング・システムがインストールされていません。オペレーティング・システムがインストールされているサーバーにオペレーティング・システムをデプロイすると、XClarity Orchestrator によってフレッシュ・インストールが実行されターゲット・ディスク上のパーティションが上書きされます。

オペレーティング・システムをサーバーにデプロイする際の所要時間は、以下のいくつかの要因によって決まります。

- サーバーに搭載された RAM の容量。サーバーの起動時間に影響します。
- サーバーに取り付けられた I/O アダプターの数とタイプは、インベントリー・データの収集にかかる時間に影響します。また、サーバー起動時の UEFI ファームウェアの起動にかかる時間にも影響します。オペレーティング・システムのデプロイメント中、サーバーは複数回、再起動されます。
- ネットワーク・トラフィックの量。オペレーティング・システム・イメージは、データ・ネットワークまたはオペレーティング・システム・デプロイメント・ネットワークを介して、サーバーにダウンロードされます。
- Orchestrator サーバーおよびリソース・マネージャーで使用可能な RAM、プロセッサー、およびハードディスク・ドライブ・ストレージの容量。

手順

次の図は、サーバーへの OS イメージのデプロイのワークフローを示しています。

ステップ 1. **OS イメージをインポートします。**

オペレーティング・システムを管理対象サーバーにデプロイするを管理対象サーバーにデプロイする前に、まず、オペレーティング・システム・イメージを XClarity Orchestrator リソース・マネージャーの OS イメージ・リポジトリーにインポートする必要があります。OS イメージをインポートする場合:

- オペレーティング・システムのインポートの前に、OS イメージ・リポジトリーに十分なスペースがあるかどうかを確認します。十分なスペースがない場合は、既存のイメージを OS イメージ・リポジトリーから削除してから、新しいイメージの再インポートを試みます。
- そのイメージのプロファイルを 1 つ以上作成し、OS イメージ・リポジトリーに保存します。各 *プロファイル*には、OS イメージとインストール・オプションが含まれています。事前定義された OS イメージ・プロファイルについて詳しくは、オペレーティング・システム・イメージ・プロファイルを参照してください。

*ベース・オペレーティング・システム*は、OS イメージ・リポジトリーにインポートされたフル OS イメージです。インポートされたベース・イメージには、そのイメージのインストールの構成を記述する事前定義済みプロファイルが含まれています。特定の構成にデ

プロイ可能なベース OS イメージ内の事前定義済みプロファイルに基づいて、カスタム・プロファイルを作成できます。

サポートされるベースおよびカスタムのオペレーティング・システムについては、サポートされているオペレーティング・システムを参照してください。

ステップ 2. **OS プロファイルのカスタマイズと割り当て**

オペレーティング・システム・プロファイルは、オペレーティング・システムをインポートする際に自動的に作成されます。作成されるプロファイルは、オペレーティング・システムのタイプとバージョンに基づいて作成されます。OS 資格情報、ホスト名、ネットワークおよびストレージ設定、ライセンス・キー、格納場所などのプロファイルを変更できます。

ステップ 3. **OS プロファイルの割り当てとデプロイ**

OS プロファイルを 1 つ以上のターゲット・サーバーに割り当てた後、プロファイルをそれらのサーバーにデプロイできます。。オペレーティング・システムをデプロイするには、サーバーのデプロイメント・ステータスが「**動作可能**」になっている必要があることに注意してください。

XClarity Orchestrator では、オペレーティング・システムはデバイスに直接デプロイされません。その代わりに、該当するリソース・マネージャーに要求を送信してデプロイメントを実行し、要求の進行状況を追跡します。XClarity Orchestrator は適用可能なイメージをリソース・マネージャーに転送し、デプロイメントを実行するリソース・マネージャーでジョブを開始するための要求を作成します。

オペレーティング・システム・イメージをデプロイする前に、オペレーティング・システム・デプロイメントの考慮事項を確認してください。

OS プロファイルの割り当てとデプロイについて詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

オペレーティング・システム・デプロイメントの考慮事項

オペレーティング・システム・イメージをデプロイする前に、以下の考慮事項を確認してください。

リソース・マネージャーに関する考慮事項

- Lenovo XClarity Administrator を使用して管理されているデバイスの場合、XClarity Administrator インスタンスに OS デプロイメント機能を実行するために必要なライセンスまたは試用期間が設定されている必要があります。
- OS デプロイメントは、Lenovo XClarity Management Hub によって管理されているデバイスではサポートされません。

管理対象デバイスに関する考慮事項

- ターゲット・デバイスで OS デプロイメント機能がサポートされている必要があります。を参照してください。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。アクティブ・ジョブのリストを表示するには、「**監視**」 → 「**ジョブ**」をクリックします。
- 管理対象サーバーのすべてのファームウェアが最新レベルであることを確認します (管理対象リソースへの更新のプロビジョニング を参照)。
- 管理対象サーバーの構成が最新の情報に更新されていることを確認します (サーバー構成のプロビジョニング を参照)。また、ターゲット・デバイスにアクティブ化が据え置きされたサーバー・パターンまたは部分的にアクティブ化されたサーバー・パターンがないことを確認します。管理対象サーバーでサーバー・パターンのアクティブ化が据え置きされているか、またはサーバー・パターンが部

分的にアクティブ化されている場合は、サーバーを再起動してすべての構成設定を適用する必要があります。部分的にアクティブ化されたサーバー・パターンを使用してオペレーティング・システムをサーバーにデプロイしないでください。

サーバーの構成ステータスを判断するには、管理対象サーバーの「要約」ページで「**構成ステータス**」フィールドを確認します (デバイスの詳細の表示 を参照)。

- オペレーティング・システムのデプロイに使用するルート・アカウントのパスワードが定義されていることを確認します。パスワードの設定について詳しくは、オペレーティング・システム・プロファイルの構成を参照してください。
- ターゲット・サーバーにマウントされたメディア (ISO イメージなど) がないことを確認します。さらに、管理コントローラーに対してアクティブなリモート・メディア・セッションが開いていないことを確認します。
- BIOS のタイム・スタンプが現在の日時に設定されていることを確認します。
- ThinkSystem サーバー用
  - Legacy BIOS オプションが無効であることを確認します。BIOS/UEFI (F1) Setup utility で、「**UEFI セットアップ**」 ➞ 「**システム設定**」の順にクリックし、レガシー BIOS が無効に設定されていることを確認します。
  - XClarity Controller Enterprise 機能は、オペレーティング・システム・デプロイメントに必要です。
- System x サーバー用
  - Legacy BIOS オプションが無効であることを確認します。BIOS/UEFI (F1) Setup utility で、「**UEFI セットアップ**」 ➞ 「**システム設定**」の順にクリックし、レガシー BIOS が無効に設定されていることを確認します。
  - リモート・プレゼンス用の Feature on Demand (FoD) キーがインストールされていることを確認します。「サーバー」ページから、リモート・プレゼンスの有効化または無効化を行うか、あるいはサーバーにインストールしないことを選択できます (デバイスの詳細の表示を参照)。
- Flex System サーバーの場合、シャーシの電源がオンになっていることを確認します。
- NeXtScale サーバーにリモート・プレゼンスの Feature on Demand (FoD) キーがインストールされていることを確認します。「サーバー」ページから、リモート・プレゼンスの有効化または無効化を行うか、あるいはサーバーにインストールしないことを選択できます (デバイスの詳細の表示を参照)。
- Converged と ThinkAgile アプライアンスについて、ベアメタル・オペレーティング・システム・デプロイメントを実行するために、XClarity Orchestrator を使用 *しない* ことをお勧めします。

オペレーティング・システムの考慮事項

- 該当するすべてのオペレーティング・システムのライセンスがあり、インストールされているオペレーティング・システムをアクティブ化できることを確認します。ライセンスは、オペレーティング・システムのメーカーから直接取得する必要があります。
- デプロイするオペレーティング・システム・イメージが既に OS イメージ・リポジトリーに読み込まれていることを確認します。イメージのインポートについては、オペレーティング・システム・イメージのインポートを参照してください。
- OS イメージ リポジトリーのオペレーティング・システム・イメージは、特定のハードウェア・プラットフォームに限定され、サポートされていない場合があります。Lenovo OS 相互運用性ガイド Web サイト から、オペレーティング・システムが特定のサーバーと互換性があるかどうかを判別できます。
- I/O アダプターの最新のインボックス・デバイス・ドライバーを使用できるよう、必ず、最新のオペレーティング・システムをインストールしてください。VMware の場合、最新のアダプター・サポートを含む、最新の ESXi の Lenovo Custom Image を使用してください。そのイメージの入手方法については、VMware サポート - ダウンロード Web サイトを参照してください。

特定のオペレーティング・システムの制限について詳しくは、サポートされているオペレーティング・システムを参照してください。

ネットワークに関する考慮事項

- 必要なすべてのポートが開いていることを確認します (デプロイされたオペレーティング・システムで利用可能なポートを参照)。
- リソース・マネージャーが管理ネットワークとデータ・ネットワークの両方を使用するように構成されていることを確認します。
- リソース・マネージャーが、管理ネットワーク・インターフェースとデータ・ネットワーク・インターフェースの両方を介してターゲット・サーバー (ベースボード管理コントローラーとサーバーのデータ・ネットワークの両方) と通信できることを確認します。オペレーティング・システム・デプロイメントに使用するインターフェースを指定するには、ネットワーク・アクセスの構成XClarity Administrator オンライン・ドキュメント を参照してください。

  オペレーティング・システム・デプロイメントについて詳しくは、ネットワークに関する考慮事項 XClarity Administrator オンライン・ドキュメント を参照してください。
- ネットワークが低速またはが不安定な場合は、オペレーティング・システムのデプロイが予期しない結果になる可能性があります。
- DHCP を使用して動的に割り当てられた IP アドレスを使用する必要があります。静的 IP アドレスはサポートされていません。

オペレーティング・システム・デプロイメントについて詳しくは、ネットワーク・アクセスの構成 およびネットワークに関する考慮事項 XClarity Administrator オンライン・ドキュメント を参照してください。

ストレージおよびブート・オプションの考慮事項

- ローカル・ディスク・ドライブにのみオペレーティング・システムをインストールできます。埋め込みハイパーバイザー、M.2 ドライバー、および SAN ストレージはサポートされません。
- 各サーバーにハードウェア RAID アダプターまたは SAS/SATA HBA が取り付けられ構成されている。通常はオンボード Intel SATA ストレージ・アダプターにあるソフトウェア RAID または単なるディスクの集まりとしてセットアップされているストレージは、サポートされません。ただし、ハードウェア RAID アダプターが存在せず、SATA アダプターがオペレーティング・システム・デプロイメントで「AHCI SATA モード」対応の場合、または単なるディスクの集まりに未構成の正常ディスクが設定されている場合は、機能する場合があります。詳しくは、OS インストーラーで、インストールするディスク・ドライブが見つからない XClarity Orchestrator オンライン・ドキュメント を参照してください。
- オペレーティング・システムをデプロイする前に、ターゲット・サーバーの UEFI ブート・オプションが「UEFI ブートのみ」に設定されていることを確認します。「Legacy Only」および「最初に UEFI、次に Legacy」ブート・オプションは、オペレーティング・システム・デプロイメントに対してサポートされません。
- 各サーバーにハードウェア RAID アダプターが取り付けられ構成されている。

  注意：

  – ハードウェア RAID を使用してセットアップされているストレージのみがサポートされています。
  – 通常はオンボード Intel SATA ストレージ・アダプターにあるソフトウェア RAID または単なるディスクの集まりとしてセットアップされているストレージは、サポートされません。ただし、ハードウェア RAID アダプターが存在せず、SATA アダプターがオペレーティング・システム・デプロイメントで「**AHCI SATA モード**」対応の場合、または単なるディスクの集まりに未構成の正常ディスクが設定されている場合は、機能する場合があります。
  – SATA アダプターが有効な場合、SATA モードを「IDE」に設定*しないでください*。
- サーバー・マザーボードまたは HBA コントローラーに接続された NVMe ストレージはサポートされていないため、デバイスにインストールしないでください。インストールすると、非 NVMe ストレージに OS をデプロイすることはできません。
- セキュア・ブート・モードがサーバーに対して無効であることを確認します。セキュア・ブート・モードが有効なオペレーティング・システム (Windows など) をデプロイする場合は、セキュア・ブー

ト・モードを無効にして、オペレーティング・システムをデプロイし、その後セキュア・ブート・モードを再度有効にします。

- ThinkServer サーバーの場合は、以下の要件を満たしていることを確認してください。
  - サーバーのブート設定で、ストレージ OpROM ポリシーが `UEFI Only` に設定されている必要があります。
  - ESXi をデプロイする場合で PXE ブート可能なネットワーク・アダプターがある場合は、オペレーティング・システムをデプロイする前に、ネットワーク・アダプターの PXE サポートを無効にします。デプロイメントの完了後、必要に応じて PXE サポートを再度有効にできます。
  - ESXi をデプロイする場合で、オペレーティング・システムがインストールされているドライブ以外の起動可能デバイスがブート順序リストにある場合は、オペレーティング・システムをデプロイする前にその起動可能デバイスをブート順序リストから削除してください。デプロイの完了後、起動可能デバイスをリストに戻すことができます。インストールされているドライブがリストの先頭にあることを確認します。

ストレージ・ロケーションの設定の詳細については、オペレーティング・システム・プロファイルの構成を参照してください。

サポートされているオペレーティング・システム

Lenovo XClarity Orchestrator は、複数のオペレーティング・システムのデプロイメントをサポートします。サポートされるバージョンのオペレーティング・システムのみ XClarity Orchestrator OS のイメージ・リポジトリーにロードできます。

重要：

- 特定のオペレーティング・システムの制限について詳しくは、サポートされるハードウェアおよびソフトウェア XClarity Orchestrator オンライン・ドキュメント を参照してください。
- XClarity Orchestrator の暗号管理機能を使用すると、特定の最小 SSL/TLS モードへの通信を制限できます。たとえば、TLS 1.2 を選択する場合は、XClarity Orchestrator でデプロイできるのは、インストール・プロセスが TLS 1.2 と強い暗号化アルゴリズムをサポートしているオペレーティング・システムのみであることに注意してください。
- OS イメージ リポジトリーのオペレーティング・システム・イメージは、特定のハードウェア・プラットフォームに限定され、サポートされていない場合があります。Lenovo OS 相互運用性ガイド Web サイト から、オペレーティング・システムが特定のサーバーと互換性があるかどうかを判別できます。
- OS とハイパーバイザーに関連する互換性、および Lenovo サーバーおよびソリューションに対するサポート情報とリソースについては、サーバーの OS サポート・センターの Web ページ を参照してください。

次の表に、XClarity Orchestrator でデプロイできる 64 ビット・オペレーティング・システムを示します。

オペレーティング・システム	バージョン	注
Red Hat® Enterprise Linux (RHEL) サーバー	`7.2 and later 8.x`	KVM が含まれます **注：** • 特に断りがない限り、すべての既存および将来のマイナーバージョンがサポートされます。 • DVD 版の OS イメージをインポートする場合は、DVD1 のみがサポートされます。

オペレーティング・システム	バージョン	注
		• RHEL を ThinkSystem サーバーにインストールする場合は、RHEL v7.4 以降が推奨です。
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	KVM および Xen ハイパーバイザーが含まれます **注：** • 特に断りがない限り、すべての既存および将来のサービス・パックがサポートされます。 • DVD 版の OS イメージをインポートする場合は、DVD1 のみがサポートされます。
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.x	基本 VMware vSphere Hypervisor (ESXi) イメージおよび Lenovo VMware ESXi カスタム・イメージがサポートされます。 Lenovo VMware ESXi カスタム・イメージは、ファームウェアの更新や構成、プラットフォーム診断、拡張ハードウェア・アラートなどのオンライン・プラットフォーム管理を実行できるように特定のハードウェア向けにカスタマイズされています。また、Lenovo 管理ツールでも、特定の System x サーバーにおける ESXi の簡易管理がサポートされています。このイメージは、VMware サポート - ダウンロード Web サイト からダウンロードできます。イメージに付与されるライセンスは 60 日間の無料試用版です。使用するには、VMware ライセンスのすべての要件を満たす必要があります。 **重要：** • 特に断りがない限り、すべての既存および将来の更新パックがサポートされます。 • (Lenovo カスタマイズを含まない) 基本 ESXi イメージには、ネットワークおよびストレージ向けの基本インボックス・デバイス・ドライバーが含まれます。この基本イメージには、(Lenovo VMware ESXi カスタム・イメージに含まれない) アウト・オブ・ボックス・デバイス・ドライバーは含まれません。 • Lenovo VMware ESXi Custom イメージの一部のバージョンでは、ThinkSystem、System x、 および ThinkServer で個別のイメージが用意されている場合があります。OS イメージ・リポジトリーに同時に存在できる固有のリリースのイメージは 1 つのみです。 • 特定の古いサーバーでは ESXi のデプロイメントがサポートされません。サポートされるサーバーについては、Lenovo OS 相互運用性ガイド Web サイトを参照してください。

オペレーティング・システム・イメージ・プロファイル

OS イメージをインポートすると、事前定義された OS プロファイルが生成されます。事前定義された各プロファイルには、OS イメージとそのイメージのインストール・オプションが含まれます。

プロファイルを変更して、資格情報、ネットワーク、およびストレージの設定を構成できます。事前定義された OS ポリシーに基づいて新しいプロファイルを作成できます。詳しくは、オペレーティング・システム・プロファイルの構成を参照してください。

次の表は、オペレーティング・システム・イメージのインポート時に作成された、事前定義された OS イメージのリストです。各プロファイルに含まれるパッケージもリストしています。

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ	
Red Hat Enterprise Linux (RHEL) 注：KVM が含まれます	基本	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	最小	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	仮想化	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 12.3 以降	基本	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>	
	最小	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>	
	仮想化 - KVM	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern>	

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ
		<pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	仮想化 - Xen	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15.2 以降	基本	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	最小	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	仮想化 - KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	仮想化 - Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern>

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ
		<pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
VMware vSphere® Hypervisor (ESXi)	仮想化	基本 VMware vSphere Hypervisor (ESXi) イメージおよび Lenovo VMware ESXi カスタム・イメージがサポートされます。

デプロイされたオペレーティング・システムで利用可能なポート

ポートの中には、特定のオペレーティング・システム・プロファイルではブロックされているものがあります。次の表は、開いている (ブロックされていない) ポートのリストを示しています。

Lenovo XClarity Orchestrator アプライアンスを実行するハイパーバイザーが、ポート 139、445、3001、3900、8443 でのネットワーク・トラフィック (TCP/UDP) を許可していることを確認してください。これらは、オペレーティング・システム・デプロイメントに必要です。

RHEL の仮想化プロファイル

デフォルトでは、Red Hat Enterprise Linux (RHEL) の仮想化プロファイルによって、次の表に示すポートを除くすべてのポートがブロックされます。

表 1. RHEL の仮想化プロファイルで利用可能なポート

ポート	TCP または UDP	方向	通信の説明
22	TCP	着信	SSH 通信
53	TCP、UDP	発信/着信	RHEL KVM ネットワーキング・デバイスとの通信
67	TCP、UDP	発信/着信	RHEL KVM ネットワーキング・デバイスとの通信
161	UDP	発信	SNMP エージェントとの通信
162	UDP	着信	SNMP エージェントとの通信
427	TCP、UDP	発信/着信	SLP サービス・エージェント、SLP ディレクトリー・エージェントとの通信
3001	TCP	発信/着信	管理ソフトウェアのイメージ・デプロイ・サービスとの通信
15988	TCP	発信	CIM-XML over HTTP 通信
15989	TCP	発信	CIM-XML over HTTP 通信
49152 - 49215	TCP	発信/着信	KVM 仮想サーバー通信

RHEL の基本プロファイルと最小プロファイル

デフォルトでは、RHEL の基本プロファイルと最小プロファイルによって、次の表に示すポートを除くすべてのポートがブロックされます。

表 2. RHEL の基本プロファイルと最小プロファイルで利用可能なポート

ポート	TCP または UDP	方向	通信の説明
22	TCP	着信	SSH 通信
3001	TCP	発信/着信	管理ソフトウェアのイメージ・デプロイメント・サービスとの通信

SLES の仮想化、基本プロファイルと最小プロファイル

SUSE Linux Enterprise Server (SLES) の場合、オープン・ポートがオペレーティング・システムのバージョンおよびプロファイルに基づいて、動的に割り当てられます。オープン・ポートのリストについては、SUSE Linux Enterprise Server ドキュメントを参照してください。

VMware ESXi の仮想化プロファイル

VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応) で開いているポートの完全なリストについては、VMware 知識ベース Web サイト で ESXi 用の VMware ドキュメントを参照してください。

オペレーティング・システム・イメージのインポート

ライセンス交付を受けたオペレーティング・システムを管理対象サーバーにデプロイするには、OS イメージリポジトリーにイメージをインポートする必要があります。

このタスクについて

インポートおよびデプロイ可能なオペレーティング・システム・イメージ (サポートされるベース・オペレーティング・システムおよびカスタム・オペレーティング・システムなど) については、サポートされているオペレーティング・システム を参照してください。

ESXi の場合のみ、同じメジャー/マイナー・バージョンの複数の ESXi イメージを OS イメージ・リポジトリーにインポートできます。

ESXi の場合のみ、メジャー/マイナー・バージョンと build 番号が同じでカスタマイズされた複数の ESXi イメージを OS イメージ・リポジトリーにインポートできます。

オペレーティング・システム・イメージをインポートするとき、XClarity Orchestrator では、次の処理が実行されます。

- オペレーティング・システムのインポートの前に、OS イメージ・リポジトリーに十分なスペースがあるかどうかを確認します。十分なスペースがない場合は、既存のイメージを削除してからやり直します。
- そのイメージのプロファイルを 1 つ以上作成し、OS イメージ・リポジトリーに保存します。各 *プロファイル*には、OS イメージとインストール・オプションが含まれています。事前定義された OS イメージ・プロファイルについて詳しくは、オペレーティング・システム・イメージ・プロファイルを参照してください。

注：Internet Explorer および Microsoft Edge Web ブラウザーには、4 GB のアップロード制限があります。インポートするファイルが 4 GB を超える場合、別の Web ブラウザー (Chrome や Firefox など) を使用することを検討してください。

手順

OS イメージ・リポジトリーにオペレーティング・システム・イメージをインポートするには、以下の手順を実行します。

ステップ 1. ライセンス交付を受けたオペレーティング・システムの ISO イメージを入手します。

注：該当するオペレーティング・システムのライセンスを取得するのはお客様の責任となります。

ステップ 2. XClarity Orchestrator メニュー・バーで、「**プロビジョニング**」 ( ) → 「**OS デプロイメント**」をクリックして、「**OS 管理**」タブをクリックしてから、「OS 管理」ページを表示します。

ステップ 3. 左側のナビゲーションで「**OS イメージ**」をクリックして、「OS イメージ」カードを表示します。

ステップ 4. 「**ファイルのインポート**」アイコン ( ) をクリックして、「OS イメージのインポート」ダイアログを表示します。

ステップ 5. ISO イメージ・ファイル名をインポートする .iso イメージをドラッグ・アンド・ドロップするか、「**参照**」をクリックしてインポートする ISO イメージを見つけます。

ステップ 6. **オプション**: チェックサム・タイプを選択し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされた OS イメージの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたイメージがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、イメージを再度アップロードするか、チェックサム値を確認する必要があります。

次のチェックサム・タイプがサポートされます: MD5、SHA1、SHA256。

ステップ 7. 「**インポート**」をクリックします。

XClarity Orchestrator によって OS イメージ・リポジトリーに OS イメージがアップロードされ、事前定義された OS プロファイルが「**OS プロファイル**」タブに追加されます。

ヒント: ISO イメージのアップロードは、安全なネットワーク接続を介して行われます。このため、イメージのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

終了後

このページでは、以下の操作を実行できます。

- 選択済み OS イメージを削除するには、「**削除**」アイコン ( ) をクリックします。

- XClarity Orchestrator メニュー・バーをクリックして「**プロビジョニング**」 (🔒) ➔ 「**OS デプロイメント**」をクリックします。「**OS プロファイル**」タブをクリックしてプロファイルを選択し、「**編集**」アイコン (✎) をクリックします (「オペレーティング・システム・プロファイルの構成」を参照)。
- XClarity Orchestrator メニュー・バーをクリックし、「**プロビジョニング**」(🔒) ➔ 「**OS デプロイメント**」をクリックします。そして、「**OS プロファイル**」タブでプロファイルを選択し、「**削除**」アイコン (🗑) をクリックして、OS プロファイルを削除します。

  注：オペレーティング・システムの最後まで残った事前定義プロファイルを削除すると、オペレーティング・システムも削除されます。

オペレーティング・システム・プロファイルの構成

オペレーティング・システム・プロファイルは、オペレーティング・システムをインポートする際に自動的に作成されます。作成されるプロファイルは、オペレーティング・システムのタイプとバージョンに基づいて作成されます。OS 資格情報、ホスト名、ネットワークおよびストレージ設定、ライセンス・キー、格納場所などのプロファイルを変更できます。

始める前に

オペレーティング・システムを管理対象サーバー・デバイスにデプロイする前に、考慮事項を確認します。詳しくは、オペレーティング・システム・デプロイメントの考慮事項を参照してください。

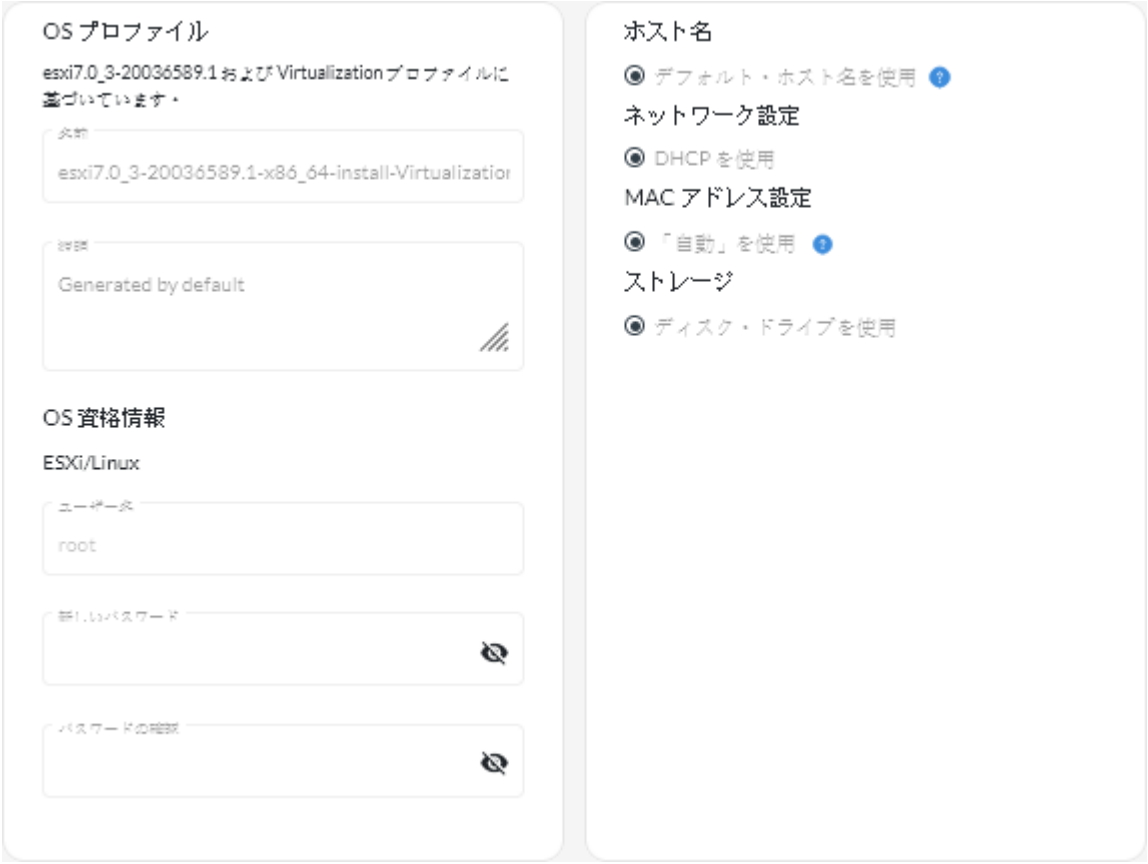
手順

デプロイメントのために OS イメージ・プロファイルを構成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング**」 (🔒) ➔ 「**OS デプロイメント**」をクリックして、「**OS プロファイル**」タブをクリックしてから、「OS プロファイル」ページを表示します。

ステップ 2. OS プロファイルを選択します。

ステップ 3. 「**編集**」アイコン (✎) をクリックして、「OS プロファイルの詳細カード」を表示します。



ステップ 4. プロファイル属性を構成します。

- **名前**。プロファイル名を変更すると、新しい OS プロファイルが作成されます。
- **説明**。この OS プロファイルの説明を変更します。
- **OS 資格情報**。オペレーティング・システムにログインするために使用する管理者アカウントの OS 資格情報を入力します。
- **ホスト名**。ホスト名に使用する情報を選択します。以下のいずれかの値を選択できます。
  - 「**デフォルト・ホスト名を使用**」。(デフォルト) ホスト名は「node」の後に、続いてデバイス ID の最初の 11 文字 が続きます (たとえば、`nodeABC31213310`)。
- **ネットワーク設定**。このプロファイルの IP 設定を選択します。以下のいずれかの値を選択できます。
  - 「**DHCP**」。(デフォルト) 既存の DHCP インフラストラクチャーを使用して、サーバーに IPv4 アドレスを割り当てます。
- 「**MAC アドレス設定**」。オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレスを選択します。以下のいずれかの値を選択できます。

  注：仮想ネットワーク・ポートはサポートされていません。1 つの物理ネットワーク・ポートを使用して複数の仮想ネットワーク・ポートをシミュレートしないでください。
  - 「**AUTO を使用**」。(デフォルト) デプロイメント用に構成して使用できるイーサネット・ポートを自動的に検出します。検出された最初の MAC アドレス (ポート) が、デフォルトで使用されます。別の MAC アドレスとの接続が検出された場合は、サーバーが自動的に再起動され、新しく検出された MAC アドレスをデプロイメントに使用します。XClarity Administrator リソース・マネージャーは、スロット 1 ～ 16 のネットワーク・ポートを自動的に検出できます。スロット 1 ～ 16 のポートの少なくとも 1 つが、該当するリソース・マネージャーに接続できる必要があります。

スロット 17 以上のネットワーク・ポートを MAC アドレスに使用する場合、AUTO を使用できません。

- Storage。オペレーティング・システム・イメージをデプロイする格納場所を選択します。
  - 「**ディスク・ドライブを使用**」。オペレーティング・システム・イメージを、管理対象サーバーに列挙された最初のローカル RAID ディスク・ドライブにインストールします。RAID コントローラーまたは SAS/SATA HBA に接続されているディスク・ドライブのみがサポートされます。

    サーバー上で RAID 構成が正しく構成されていないか、非アクティブな場合、ローカル・ディスクは Orchestrator サーバー に表示されない可能性があります。この問題を解決するには、構成パターン (既存のサーバーからのサーバー構成パターンの学習 を参照) またはサーバー上の RAID 管理ソフトウェアを使用して RAID 構成を有効にします。

    注：
    - M.2 ドライブも存在している場合は、ディスク・ドライブをハードウェア RAID 用に構成する必要があります。
    - SATA アダプターが有効な場合、SATA モードを「IDE」に設定*しない*でください。
    - ThinkServer サーバーでは、サーバーで RAID 管理ソフトウェアを使用してのみ構成を行うことができます。

ステップ 5. 「**保存**」をクリックします。

終了後

以下のアクションを実行できます。

- 選択するサーバー、「**割り当て**」アイコン (⇄) の順にクリックして選択するか、「**割り当て**」アイコン (⇄) をクリックしてからサーバーのグループを選択することで、「**割り当てとデプロイ**」タブで 1 つ以上の OS プロファイルを割り当てます。OS プロファイルを選択すると、OS プロファイルを以下に割り当てることを選択できます。
  - 「**適用可能なすべてのデバイス (割り当てられているプロファイルを上書き)**」
  - 「**プロファイルが割り当てられていない適用可能なデバイス**」
  - 「**選択した適用可能なデバイスのみ (割り当てられているプロファイルを上書き)**」
  - 「**プロファイルが割り当てられていない、選択した適用可能なデバイスのみ**」
- 選択済み OS プロファイルを削除するには、「**削除**」アイコン (🗑) をクリックします。

  注：オペレーティング・システムの最後まで残った事前定義プロファイルを削除すると、オペレーティング・システムも削除されます。

オペレーティング・システム・イメージのデプロイ

Lenovo XClarity Orchestrator を使用して、オペレーティング・システムを管理対象サーバーにデプロイできます。

始める前に

ご使用の管理対象サーバーにオペレーティング・システムをデプロイする前に、オペレーティング・システム・デプロイメントの考慮事項をお読みください (オペレーティング・システム・デプロイメントの考慮事項を参照)。

注意：サーバーに現在インストールされているオペレーティング・システムがある場合、OS イメージ・プロファイルをデプロイすると現在のオペレーティング・システムが上書きされます。

手順

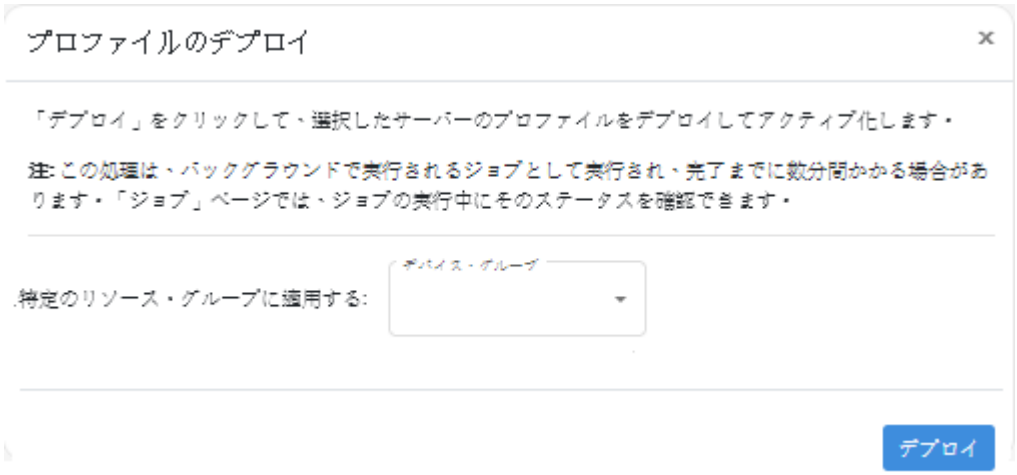
オペレーティング・システム・イメージを 1 台以上の管理対象サーバーにデプロイするには、以下のいずれかの手順を実行します。

- **特定のデバイスへ**
  1. XClarity Orchestrator のメニュー・バーで「**プロビジョニング**(🔒) → **OS デプロイメント**」をクリックし、「**割り当てとデプロイ**」タブをクリックして、「割り当てとデプロイ」カードを表示します。

  2. オペレーティング・システムがデプロイされるサーバーを 1 台以上選択します。
  3. ターゲット・サーバーごとに、「**OS プロファイル**」列のドロップダウン・リストから、デプロイする OS イメージ・プロファイルを選択します。ターゲット・サーバーと互換性がある OS イメージ・プロファイルを選択してください。
  4. 選択したサーバーすべての「**ステータス**」列が「動作可能」になっていることを確認します。
  5. 「**デプロイ**」アイコン (⎋) をクリックして、「プロファイルのデプロイ」ダイアログを表示します。
  6. 「**デプロイ**」をクリックして、オペレーティング・システム・デプロイメントを開始します。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)。
- **特定のグループのすべてのデバイスへ**
  1. XClarity Orchestrator のメニュー・バーで「**プロビジョニング**(🔒) → **OS デプロイメント**」をクリックし、「**割り当てとデプロイ**」タブをクリックして、「割り当てとデプロイ」カードを表示します。
  2. サーバーのグループに OS プロファイルを割り当てます。
     a. 「**割り当て**」アイコン (⎋) をクリックして、「プロファイルの割り当て」ダイアログを表示します。

b. 割り当てるプロファイルを選択します。
c. 割り当てるデバイスのグループを選択します。
d. グループ内で割り当てるデバイスを選択します。
   - 「**適用可能なすべてのデバイス (割り当てられているプロファイルを上書き)**」
   - 「**プロファイルが割り当てられていない適用可能なデバイス**」
   - 「**選択した適用可能なデバイスのみ (割り当てられているプロファイルを上書き)**」
   - 「**プロファイルが割り当てられていない、選択した適用可能なデバイスのみ**」
e. 「**デプロイ**」をクリックします。

3. 「**デプロイ**」アイコン (⊙) をクリックして、「プロファイルのデプロイ」ダイアログを表示します。



4. 割り当てられた OS プロファイルをデプロイするデバイスのグループを選択します。

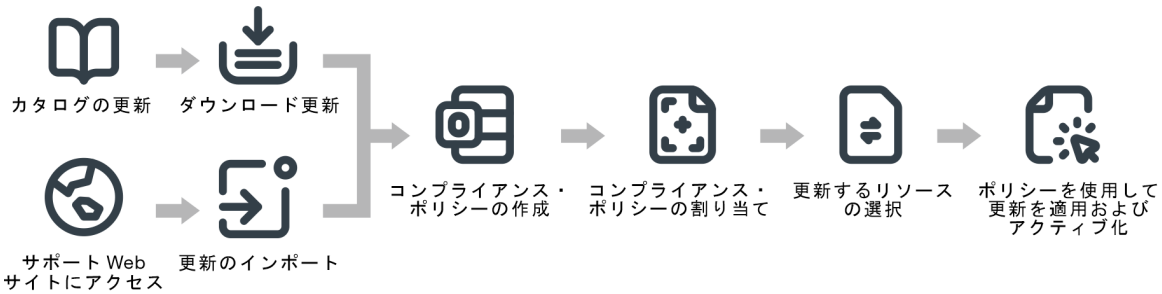
5. 「**デプロイ**」をクリックして、オペレーティング・システム・デプロイメントを開始します。この操作を実行するためのジョブが作成されます。「**監視**」( ) → 「**ジョブ**」カードから、ジョブの進行状況を監視できます。ジョブが正常に完了しなかった場合は、ジョブのリンクをクリックしてジョブの詳細を表示します (を参照)。

管理対象リソースへの更新のプロビジョニング

Lenovo XClarity Orchestrator を使用して、Lenovo XClarity Administratorリソース・マネージャーと管理対象サーバーの現在のソフトウェア・レベルを維持することができます。更新カタログを使用して、使用可能なソフトウェア・レベルを確認し、更新コンプライアンス・ポリシーを使用して、カスタム条件に基づいて更新する必要のあるリソースを特定し、それらのリソースに必要な更新をデプロイすることができます。

手順

次の図は、管理対象リソースの更新のワークフローを示しています。



ステップ 1. **カタログの更新**

*更新リポジトリー*には、管理対象リソースに適用できるカタログおよび更新パッケージが含まれます。

*カタログ*には、現在使用できる更新に関する情報が含まれています。このカタログでは、リソース・タイプ (プラットフォーム) およびコンポーネント別に更新が分類されています。カタログを更新すると、XClarity Orchestrator により提供中の最新の更新に関する情報が Lenovo サポート Web サイトから取得され、更新リポジトリーに保存されます。

重要：カタログを更新するには、XClarity Orchestrator がインターネットに接続されている必要があります。

新しい更新パッケージが使用可能になったら、更新を適用する前に該当する更新パッケージをインポートする必要があります。カタログを更新しても、更新パッケージが自動的にインポートされるわけではありません。

XClarity Orchestrator を最初にインストールしたときは、更新リポジトリーは空です。

ステップ 2. **リポジトリーへの更新パッケージのダウンロードまたはインポート**

XClarity Orchestrator がインターネットに接続されている場合は、更新カタログに記載されている更新パッケージを Lenovo サポート Web サイトから直接ダウンロードすることができます。XClarity Orchestrator がインターネットに接続されていない場合、XClarity Orchestrator ホストにネットワークでアクセス可能なワークステーションに Lenovo データセンターサポート Web サイト から既にダウンロードされている更新パッケージを手動でインポートできます。

マイナー・リリースをダウンロードすることを選択した場合は、前提条件となる更新パッケージもダウンロードされます。

リポジトリー・パックを手動でインポートする場合は、ペイロード (.tgz)、メタデータ (.xml)、変更ログ (.chg)、readme (.txt) をインポートする必要があります。

更新を手動でインポートする場合は、リソース・タイプに基づいて必要なファイルをインポートする必要があります。

- ThinkSystem V3 サーバーの場合は、単一の更新パッケージ (.zip) をインポートします。この .zip ファイルには、ペイロード、メタデータ・ファイル (複数の *.json ファイル)、変更ログ・ファイル (*.chg)、および readme ファイル (*.txt) が含まれています。
- ThinkEdge クライアント・デバイスの場合は、ペイロード (Windows .exe) をインポートします。readme (.txt) はオプションです。現在、**Windows 更新用の BIOS フラッシュ・ユーティリティー・パッケージ**のみがサポートされていることに注意してください。
- XClarity Management Hub、および XClarity Management Hub 2.0 の場合は、単一の更新パッケージ・ファイル (.tgz) をインポートします。このファイルには、ペイロード、メタデータ、変更履歴、readme ファイルが含まれています。
- その他すべてのリソース (XClarity Administrator、ThinkEdge サーバー、ThinkSystem V1 および V2、およびレガシー・デバイス) の場合は、ペイロード (.zip、.uxz、.tar.gz、.tar、.bin)、メタデータ (.xml)、変更ログ (.chg)、および readme (.txt) をインポートします。

更新のインポートについて詳しくは、更新のダウンロードとインポートを参照してください。

ステップ 3. **更新コンプライアンス・ポリシーの作成と割り当て**

*更新コンプライアンス・ポリシー*を使用すると、注意が必要なリソースにフラグを付けることで、特定の管理対象リソース上のソフトウェアまたはファームウェアを、現在のレベルまたは指定されたレベルに維持することができます。各更新コンプライアンス・ポリシーは、監視対象のリソースと、コンプライアンスでリソースを保つためにインストールする必要があるソフトウェアおよびファームウェア・レベルを識別します。XClarity Orchestrator はこれらのポリシーを使用して管理対象リソースのステータスを確認し、コンプライアンスに違反しているリソースを特定します。

更新コンプライアンス・ポリシーを作成する場合は、リソースのソフトウェアまたはファームウェアが下位レベルである場合に、XClarity Orchestrator がリソースにフラグを立てるように選択できます。

更新コンプライアンス・ポリシーがリソースに割り当てられると、XClarity Orchestrator は更新リポジトリーが変更されたときに、リソースのコンプライアンス状況を確認します。リソースのソフトウェアまたはファームウェアが割り当てられたポリシーに適合しない場合、XClarity Orchestrator は、更新コンプライアンス・ポリシーで指定したルールに基づいて、そのリソースが非適合であることを「適用/有効化」ページでフラグを付けて表示します。

たとえば、XClarity Administrator の基準となるソフトウエア・レベルを定義する更新コンプライアンス・ポリシーを作成し、そのポリシーをすべての XClarity Administrator リソース・マネージャーに割り当てることができます。更新カタログが更新され、新しい更新がダウンロードまたはインポートされると、それらの XClarity Administrator インスタンスがコンプライアンス違反となる可能性があります。その場合、XClarity Orchestrator は「適用/有効化」ページを更新し、非適合である XClarity Administrator インスタンスを表示して、アラートを生成します。

更新コンプライアンス・ポリシーの作成について詳しくは、更新コンプライアンス・ポリシーの作成と割り当て を参照してください。

ステップ 4. **更新の適用とアクティブ化**

XClarity Orchestrator では、更新は自動的に適用されません。ソフトウェア・リソースを更新するには、選択したリソースで、割り当てられた更新コンプライアンス・ポリシーに適合していないものに対して、更新を手動で適用してアクティブにする必要があります。

XClarity Orchestrator は、リソースを直接更新しません。その代わりに、該当するリソース・マネージャーに要求を送信して更新を実行し、要求の進行状況を追跡します。XClarity Orchestrator は更新を実行するために必要な依存関係を識別し、ターゲット・リソースを正しい順序で確実に更新し、適用可能な更新パッケージをリソース・マネージャーに転送し、リソース・マネージャーでジョブを開始して更新を実行する要求を作成します。

更新の適用について詳しくは、リソース・マネージャーへの更新の適用とアクティブ化および管理対象サーバーへの更新の適用とアクティブ化を参照してください。

デプロイメントの考慮事項の更新

Lenovo XClarity Orchestrator を使用して更新をデプロイする前に、以下の重要な考慮事項を確認してください。

- 最適なパフォーマンスを保つには、Lenovo XClarity Administrator リソース・マネージャーが v3.2.1 以降を実行していることを確認してください。
- 適用する更新パッケージが更新リポジトリ—に含まれていることを確認します。含まれていない場合は、製品カタログを更新し、適切な更新をダウンロードします (更新のダウンロードとインポートを参照)。
- ターゲット・リソースで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。
- リソースに割り当てられた更新コンプライアンス・ポリシーがあり、更新の結果がコンプライアンス違反になる場合、コンプライアンス・ポリシーを調整するか、別のポリシーを割り当てて違反を修正する必要があります。
- 複数のコンポーネントに対する更新を含む更新パッケージをインストールするように選択した場合、更新パッケージが適用されるすべてのコンポーネントが更新されます。

リソースに関する検討事項

- 更新機能では、サーバーとリソース・マネージャーの更新のみをサポートしています。ThinkSystem SR635 および SR655 では、BMC および UEFI ファームウェア更新のみサポートされています。

  ThinkSystem デバイスおよび ThinkAgile デバイスの場合、ベースボード管理コントローラーおよび UEFI バックアップ・バンクではファームウェア更新はサポートされていません。代わりに、プライマリ・バンクを更新し、自動プロモーションを有効にします。
- 管理対象デバイスを更新する前に、重要な更新に関する考慮事項を必ずお読みください (ファームウェア更新に関する考慮事項 XClarity Administrator オンライン・ドキュメント を参照)。
- XClarity Administrator リソース・マネージャーを更新する前に、XClarity Administrator の更新に関する考慮事項を読んでください (XClarity Administrator 管理サーバーの更新 XClarity Administrator オンライン・ドキュメント を参照)。
- XClarity Administrator リソース・マネージャーを更新する前に、クローンを作成して仮想アプライアンスをバックアップします (XClarity Administrator のバックアップ XClarity Administrator オンライン・ドキュメント を参照)。
- 更新するリソースに、更新コンプライアンス・ポリシーが割り当てられていることを確認します。
- XClarity Orchestrator は、更新プロセス中に、適用可能な更新をリソース・マネージャーに転送します。管理サーバーに、更新を含めるための十分なディスク・スペースがあることを確認します。
- ThinkEdge Client デバイスでは、Windows 10 バージョン 1809 以降の 64 ビット・オペレーティング・システムを実行するサーバーでの BIOS 更新のみがサポートされます。現在、特別版 (10 S や 10x など) はサポートされていません。
- Web インターフェースから次のサーバーのファームウェア更新をダウンロードすることはできません。代わりに、ibm.com から更新を手動でダウンロードして、更新をインポートします。
  - IBM System x iDataPlex dx360 M4
  - IBM System シリーズ M4

- IBM System x3100 M5 および x3250 M
- IBM System x3850 X5 および x3950 X5
- IBM System x3850 X6 および x3950 X6
- IBM Flex System

リポジトリーに関する考慮事項

- 適用する更新パッケージが更新リポジトリーに含まれていることを確認します。含まれていない場合は、製品カタログを更新し、適切な更新をダウンロードします (更新のダウンロードとインポート を参照)。ターゲット更新に加えて、前提条件となる更新をインストールすることもできます。前提条件となるすべての更新は、適用前にリポジトリーにダウンロードする必要があります。

  場合によっては、更新を適用するために複数のバージョンが必要になることがあり、その場合はすべてのバージョンをリポジトリーにダウンロードする必要があります。

更新プロセスに関する考慮事項

- 複数のコンポーネントに対する更新を含む更新パッケージをインストールするように選択した場合、更新パッケージが適用されるすべてのコンポーネントが更新されます。
- リソース・マネージャーおよびそのリソース・マネージャーによって管理されている 1 つ以上のデバイスに更新を適用する要求が行われると、最初に更新がリソース・マネージャーに適用されます。
- 更新の進行中は、ターゲット・リソースはロックされています。更新プロセスが完了するまでは、ターゲット・リソース上にある他の管理タスクを開始できません。
- 更新がリソースに適用された後、更新を完全にアクティブ化するため再起動が 1 回以上必要になる可能性があります。リソースをすぐに再起動するか、後でアクティブ化するか、またはアクティブ化に優先順位を付けることを選択できます。すぐに再起動することを選択した場合、XClarity Orchestrator により必要な再起動回数が最小限に抑えられます。後でアクティブ化することを選択した場合、次回リソースが再起動されたときに更新がアクティブ化されます。アクティブ化に優先順位を付ける場合は、ベースボード管理コントローラーの更新が即座にアクティブ化され、その他のすべての更新は次回のデバイスの再起動時に有効になることに注意してください。
- 更新プロセス中にリソースの再起動を選択した場合 (*即時アクティベーション*)、必ず実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のリソースに移動してください。
- 一部のファームウェア更新では、モニターがターゲット・デバイスに接続されている必要があります。モニターが接続されていない場合、更新プロセスが失敗する可能性があります。

更新のダウンロードとインポート

更新を管理対象リソースに適用するには、更新パッケージが更新リポジトリーにある必要があります。

始める前に

更新パッケージに関する最新情報を取得するには、リソース・タイプを選択し、**「更新プログラムの確認」 ➡ 「選択した更新」**をクリックして、すべての利用可能な更新パッケージに関する情報を取得するか、**「更新プログラムの確認」 ➡ 「選択した更新 - 最新のみ」**をクリックして、そのリソースの最新の更新パッケージに関する情報のみを取得します。次に、「**名前**」列を使用してテーブルをソートし、バージョンによって更新を順序付けします。

XClarity Orchestrator は、更新リポジトリーに個別のドライブを使用します。このドライブの最小サイズ要件は、100 GB です。

このタスクについて

1 つの XClarity Administrator リポジトリー・パックまたは 1 つ以上の更新パッケージを一度にダウンロードまたはインポートできます。

- **XClarity Administrator リポジトリー・パック**Lenovo XClarity Administrator リポジトリー・パックには、ほとんどのサポート済みデバイスに対して特定の時点での利用可能な最新のファームウェア更新と、更新済みのデフォルトのファームウェア・コンプライアンス・ポリシーが含まれます。XClarity Administrator ダウンロード Web ページ からリポジトリー・パックをダウンロードすると、リポジトリー・パック内の各更新パッケージが抽出されて、更新リポジトリーにインポートされ、リポジトリー・ペイロード・ファイルが削除されます。更新された既定のファームウェア・コンプライアンス・ポリシーも、定義済みポリシーとしてインポートされます。この事前定義済みのポリシーを変更することはできません。

  以下のリポジトリー・パックを使用できます。
  - **lnvgy_sw_lxca_cmmswitchrepo*x-x.x.x*_anyos_noarch**。すべての CMM および Flex System スイッチのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_storagerackswitchrepo*x-x.x.x*_anyos_noarch**。すべての RackSwitch スイッチと Lenovo Storage デバイスのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_systemxrepo*x-x.x.x*_anyos_noarch**。すべての Converged HX シリーズ、Flex System、および System x サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_thinksystemrepo*x-x.x.x*_anyos_noarch**。すべての ThinkSystem サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_thinksystemv2repo*x-x.x.x*_anyos_noarch**。すべての ThinkSystem V2 サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_thinksystemv3repo*x-x.x.x*_anyos_noarc**。すべての ThinkAgile および ThinkSystem V3 サーバーのファームウェア更新が含まれます。

  リポジトリー・パックを手動でインポートする場合は、ペイロード (.tgz)、メタデータ (.xml)、変更ログ (.chg)、readme (.txt) をインポートする必要があります。

  リポジトリー・パックの状態は、「リポジトリー管理」ページの「**状態**」列から判別できます。この列には、以下の値が含まれます。
  - **未ダウンロード**。リポジトリー・パックは Web から入手できますが、更新リポジトリーはダウンロードされず、抽出もされません。
  - **保留中のダウンロード**。リポジトリー・パックは、インターネットからのダウンロード用のキューに入っています。
  - **ダウンロード中**。リポジトリー・パックは、インターネットからダウンロードされています。
  - **保留中の適用**。リポジトリー・パックは、リポジトリー・パック内の更新パッケージを更新リポジトリーに抽出するためのキューに入っています。
  - **適用中**。リポジトリー・パック内の更新パッケージが更新リポジトリーに抽出されています。
  - ***x* / *y* ダウンロード済み**。すべてのリポジトリー・パックではなく、一部が更新リポジトリーにダウンロードされ、抽出されます。括弧内の数字は、ダウンロードされた更新の数と利用可能な更新の数を示しています。
  - **ダウンロード済み**。リポジトリー・パック内のすべての更新パッケージが更新リポジトリーに格納され、リポジトリー・パックのペイロード・ファイルが削除されます。
- **更新パッケージ**XClarity Orchestrator がインターネットに接続されている場合は、更新カタログに記載されている更新パッケージを Lenovo サポート Web サイトから直接ダウンロードすることができます。XClarity Orchestrator がインターネットに接続されていない場合、XClarity Orchestrator ホストにネットワークでアクセス可能なワークステーションに Lenovo データセンターサポート Web サイト から既にダウンロードされている更新パッケージを手動でインポートできます。

  マイナー・リリースをダウンロードすることを選択した場合は、前提条件となる更新パッケージもダウンロードされます。

  更新を手動でインポートする場合は、リソース・タイプに基づいて必要なファイルをインポートする必要があります。

  - ThinkSystem V3 サーバーの場合は、単一の更新パッケージ (.zip) をインポートします。この .zip ファイルには、ペイロード、メタデータ・ファイル (複数の *.json ファイル)、変更ログ・ファイル (*.chg)、および readme ファイル (*.txt) が含まれています。
  - ThinkEdge クライアント・デバイスの場合は、ペイロード (Windows .exe) をインポートします。readme (.txt) はオプションです。現在、**Windows 更新用の BIOS フラッシュ・ユーティリティー・パッケージ**のみがサポートされていることに注意してください。

– XClarity Management Hub、および XClarity Management Hub 2.0 の場合は、単一の更新パッケージ・ファイル (.tgz) をインポートします。このファイルには、ペイロード、メタデータ、変更履歴、readme ファイルが含まれています。
– その他すべてのリソース (XClarity Administrator、ThinkEdge サーバー、ThinkSystem V1 および V2、およびレガシー・デバイス) の場合は、ペイロード (.zip、.uxz、.tar.gz、.tar、.bin)、メタデータ (.xml)、変更ログ (.chg)、および readme (.txt) をインポートします。

重要：一度にインポートできるすべてのファイルの最大サイズは 8 GB です。

「リポジトリー管理」ページの「**状態**」列で、特定の更新ファイルが更新リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。
– **未ダウンロード**。更新パッケージ全体、または個々の更新は Web から入手できますが、現在、リポジトリーに保存されていません。
– **保留中のダウンロード**。更新パッケージは、インターネットからのダウンロード用のキューに入っています。
– **ダウンロード中**。更新パッケージは、インターネットからダウンロードされています。
– ***x*/*y* ダウンロード済み**。更新パッケージ内の一部の更新がリポジトリーに保存されています。括弧内の数字は、保存された更新の数と使用可能な更新の数を示しています。
– **ダウンロード済み**。更新パッケージ全体または個々の更新がリポジトリーに保存されています。

注：一部の更新パッケージは、複数のプラットフォームで使用されます。テーブルで更新パッケージを選択した場合、そのパッケージを使用するすべてのプラットフォームで選択されます。

手順

更新パッケージとリポジトリー・パッケージをダウンロードまたは手動でインポートするには、以下のいずれかの手順を実行します。

- XClarity Orchestrator がインターネットに接続されている場合は、カタログに示された更新パッケージをダウンロードします。
  1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** ( )」 ➔ 「**更新**」をクリックし、「**リポジトリー管理**」をクリックして、「リポジトリー管理」カードを表示します。「リポジトリー管理」カードには、更新パッケージに関する情報が、リソース・タイプ、コンポーネント、および更新パッケージごとにツリー構造で表示されます。デフォルトでは、*管理対象*リソースのリソース・タイプのみがテーブルに表示されます。「**使用可能なリソース・タイプの表示**」をクリックすると、カタログで*サポート可能な*すべてのリソース・タイプが一覧表示されます。

2. (オプション) テーブル内のリソース・タイプを 1 つ以上選択して、「**更新プログラムの確認**」をクリックし、次のいずれかのオプションをクリックして、特定のリソース・タイプについて利用可能な最新の更新に関する情報をダウンロードします。
   – 「**選択した更新**」。選択したリソースで使用可能なすべての更新のバージョンに関する情報を取得します。
   – 「**選択した更新 - 最新のみ**」。選択したリソースで使用可能な最新の更新のバージョンに関する情報を取得します。ThinkEdge クライアント・デバイスでは、「**選択した更新 - 最新のみ**」のみがサポートされています。

   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)。
3. ダウンロードするリポジトリー・パック、リソース、コンポーネント、更新バージョンを 1 つ以上選択します。リソース・タイプとコンポーネントを展開すると、各リソース・タイプおよびコンポーネントのカタログで使用可能な更新バージョンのリストを表示できます。
4. 「**ダウンロード更新**」アイコン ( ) をクリックして、選択した更新をダウンロードします。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)。

ダウンロードが完了すると、選択した更新の「**ダウンロード状況**」が「ダウンロード済み」に変わります。

- XClarity Orchestrator がインターネットに接続されていない場合は、更新パッケージとリポジトリー・パックを手動でインポートします。
  1. Web ブラウザーを使用して、XClarity Orchestrator ホストにネットワークでアクセス可能なワークステーションに各リポジトリー・パックと更新パッケージのファイルをダウンロードします。適用可能な更新をダウンロードするには、以下のリンクを使用します。
     - Lenovo XClarity Administrator の更新については、XClarity Administrator ダウンロード Web ページにアクセスしてください 。Lenovo XClarity Essentials OneCLI コマンドを使用して、XClarity Administrator の更新をダウンロードすることもできます。次の例では、最新の更新 (ペイロードを含む) を /lxca-updates ディレクトリーにダウンロードし、ログ・ファイルを /logs/lxca-updates ディレクトリーに保存します。OneCLI について詳しくは、Lenovo XClarity Essentials OneCLI オンライン・ドキュメントの acquire コマンドを 参照してください。
       ```
       Onecli.exe update acquire --lxca  --ostype none --mt lxca --scope latest --superseded --xml
       --dir ./lxca-updates --output ./logs/lxca-updates
       ```
     - ファームウェア更新リポジトリー・パックについては、XClarity Administrator ダウンロード Web ページにアクセスしてください。
     - ファームウェア更新については、Lenovo データセンターサポート Web サイトにアクセスしてください。
  2. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** ()」 ➡ 「**更新**」をクリックし、「**リポジトリー管理**」をクリックして、「リポジトリー管理」カードを表示します。
  3. 「**インポート**」アイコン () をクリックして、「更新のインポート」ダイアログを表示します。
  4. ダウンロードしたファイルを「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、または「**参照**」をクリックしてファイルを特定します。

     注意：

     - ThinkEdge クライアント・デバイスの場合、各更新パッケージのペイロード・ファイルをインポートする必要があります。readme ファイルはオプションです。
     - すべてのその他のデバイスでは、メタデータ・ファイルと画像ファイルまたはペイロード・ファイルをインポートし、履歴ファイルと、各リポジトリー・パックおよび更新パッケージの readme ファイルを変更する必要があります。選択されているがメタデータ・ファイルに指定されていないファイルはすべて破棄されます。メタデータ・ファイルを含めなかった場合、更新はインポートされません。
     - Lenovo ダウンロード Web サイトに記載されている他のファイルはインポートしないでください。
     - リポジトリー・パックまたは更新パッケージのメタデータ・ファイル (.xml または .json) を含めない場合、リポジトリー・パックまたは更新パッケージはインポートされません。
  5. 「**インポート**」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)。

     ファイルがインポートされてリポジトリーに保存されると、「**ダウンロード状況**」列が「ダウンロード済み」に変わります。

終了後

「リポジトリー管理」カードから、以下の操作を実行できます。

- 「**リリース・ノート**」列の情報 () アイコンをクリックして、特定の更新の readme ファイル、変更履歴ファイルと、修正された共通脆弱性識別子 (CVE) のリストを確認します。「**修正済み CVE**」列の上にカーソルを置くことでも、修正済み CVE のリストを表示できます。「CVE ID」をクリックすると、National Vulnerability Data の Web サイトから、その CVE に関する詳細情報が表示されます。

「**リリース・ノート**」列と「**修正済み CVE**」列は、デフォルトでは非表示になっています。これらの列をテーブルに表示するには、「**すべての操作**」 ➔ 「**列の切り替え**」の順にクリックします。

- 「**ペイロード・ファイルのみを削除**」アイコン ( ) をクリックして、選択済みの各更新のイメージ (ペイロード) ファイルのみを削除します。更新に関する情報 (XML メタデータ・ファイル) はリポジトリーに残り、ダウンロード・ステータスは「未ダウンロード」に変わります。

  重要：

  – ダウンロードまたはインポート処理中に更新パッケージが抽出された後、リポジトリー・パックのペイロードは自動的に削除されます。
  – 更新コンプライアンス・ポリシーで使用中の更新パッケージからペイロードを削除することはできません。まず更新パッケージをポリシーから削除する必要があります (更新コンプライアンス・ポリシーの作成と割り当てを参照)。
  – 一部の更新パッケージは、複数のプラットフォームおよびコンポーネントで共通です。共通更新パッケージを削除すると、それを使用しているすべてのプラットフォームおよびコンポーネントに影響します。

更新コンプライアンス・ポリシーの作成と割り当て

更新リポジトリーで取得した更新に基づいて、更新コンプライアンス・ポリシーを作成することができます。その後、ポリシーを 1 つ以上のリソース・マネージャーまたは管理対象サーバーに割り当てることができます。

始める前に

更新コンプライアンス・ポリシーを作成するときは、ポリシーに割り当てられるリソースに適用するターゲット更新バージョンを選択します。ポリシーを作成する前に、ターゲット・バージョンの更新ファイルが更新リポジトリーにあることを確認してください。

ファームウェア更新リポジトリー・パックをダウンロードまたはインポートすると、リポジトリー・パック内の定義済みのファームウェア・コンプライアンス・ポリシーが更新リポジトリーに追加されます。これは、*事前定義されたポリシーと見なされ*、変更または削除することはできません。

このタスクについて

*更新コンプライアンス・ポリシー*を使用すると、注意が必要なリソースにフラグを付けることで、特定の管理対象リソース上のソフトウェアまたはファームウェアを、現在のレベルまたは指定されたレベルに維持することができます。各更新コンプライアンス・ポリシーは、監視対象のリソースと、コンプライアンスでリソースを保つためにインストールする必要があるソフトウェアおよびファームウェア・レベルを識別します。XClarity Orchestrator はこれらのポリシーを使用して管理対象リソースのステータスを確認し、コンプライアンスに違反しているリソースを特定します。

更新コンプライアンス・ポリシーを作成する場合は、リソースのソフトウェアまたはファームウェアが下位レベルである場合に、XClarity Orchestrator がリソースにフラグを立てるように選択できます。

更新コンプライアンス・ポリシーがリソースに割り当てられると、XClarity Orchestrator は更新リポジトリーが変更されたときに、リソースのコンプライアンス状況を確認します。リソースのソフトウェアまたはファームウェアが割り当てられたポリシーに適合しない場合、XClarity Orchestrator は、更新コンプライアンス・ポリシーで指定したルールに基づいて、そのリソースが非適合であることを「適用/有効化」ページでフラグを付けて表示します。

たとえば、XClarity Administrator の基準となるソフトウエア・レベルを定義する更新コンプライアンス・ポリシーを作成し、そのポリシーをすべての XClarity Administrator リソース・マネージャーに割り当てることができます。更新カタログが更新され、新しい更新がダウンロードまたはインポートされると、それらの XClarity Administrator インスタンスがコンプライアンス違反となる可能性があります。その場

合、XClarity Orchestrator は「適用/有効化」ページを更新し、非適合である XClarity Administrator インスタンスを表示して、アラートを生成します。

手順

更新コンプライアンス・ポリシーを作成して割り当てるには、以下の手順を実行します。

ステップ 1. 更新コンプライアンス・ポリシーを作成する。

1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング**」( ) → 「**更新**」をクリックし、「**ポリシー管理**」をクリックして、「ポリシー管理」カードを表示します。

2. 「**作成**」アイコン ( ) をクリックして、「コンプライアンス・ポリシーの作成」ダイアログを表示します。
3. ポリシーの名前および説明 (任意) を指定します。
4. ポリシーのトリガーを指定します。これは以下のいずれかの値です。
   - **完全一致でなければフラグを設定**。リソースにインストールされているソフトウェアまたはファームウェア・バージョンが更新コンプライアンス・ポリシーのターゲット・ファームウェア・バージョン*以前またはそれ以降*である場合、リソースには「非適合」のフラグが付きます。たとえば、サーバーのネットワーク・アダプターを交換した場合で、そのネットワーク・アダプターのファームウェアが割り当てられた更新コンプライアンス・ポリシーのターゲット・ファームウェア・バージョンと異なる場合、そのサーバーには「不適合」のフラグが付けられます。
   - **フラグを設定しない**。コンプライアンス違反リソースにフラグが付けられません。
5. このポリシーにコンプライアンス・ルールを追加するには、「**規則**」タブをクリックします。
   a. このポリシーのリソース・タイプを選択します。

b. 該当するリソースとのコンポーネントのコンプライアンス・ターゲットを指定します。コンポーネントがあるリソースの場合、以下の値のいずれかを選択できます。

- **カスタム**。各リソース・コンポーネントのコンプライアンス・ターゲットは、デフォルトで、そのコンポーネントのリポジトリー内の現在の最新バージョンに設定されます。
- **更新しない**。各リソース・コンポーネントのコンプライアンス・ターゲットはデフォルトで「**更新しない**」に設定されます。コンポーネントのデフォルト値を変更すると、そのリソース全体のコンプライアンス・ターゲットが「**カスタム**」に変わります。コンポーネントがないリソースの場合、コンポーネントごとに以下の値のいずれかを選択できます。
  - *{firmware_level}*.コンポーネントのファームウェアが、選択したベースライン・ファームウェア・バージョンである必要があることを指定します。
  - **更新しない**。コンポーネント上のファームウェアを更新しないよう指定します。バックアップ (セカンダリ) 管理コントローラーのファームウェアはデフォルトで更新されないことに注意してください。

c. 追加の規則を追加するには、「**追加**」アイコン (⊕) をクリックし、「**削除**」アイコン (🗑) をクリックして規則を削除します。

6. 「**作成**」をクリックします。

ステップ 2. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** (🔧)」 → 「**更新**」をクリックし、「**適用して有効化**」をクリックして、「適用して有効化」カードを表示します。

ステップ 3. リソースに更新コンプライアンス・ポリシーを割り当てる。

- **単一のリソースの場合**各リソースで、「**割り当て済みコンプライアンス・ポリシー**」列のドロップダウン・リストからポリシーを選択します。

  リソースに適用可能なコンプライアンス・ポリシーのリストからのみ選択できます。リソースに現在ポリシーが割り当てられていない場合、割り当て済みポリシーは「**割り当てなし**」に設定されます。リソースに適用可能なポリシーがない場合、割り当て済みポリシーは「**適用できるポリシーがありません**」に設定されます。

- **複数のリソースの場合**

  1. ポリシーを割り当てるリソースを 1 つ以上選択します。
  2. 「**割り当て**」アイコン (📄) をクリックして、「ポリシーの割り当て」ダイアログを表示します。
  3. 割り当てるポリシーを選択します。すべての選択済みリソースに適用可能なコンプライアンス・ポリシーのリストから選択できます。リソースに現在ポリシーが割り当てられていない場合、割り当て済みポリシーは「**割り当てなし**」に設定されます。リソースに適用可能なポリシーがない場合、割り当て済みポリシーは「**適用できるポリシーがありません**」に設定されます。ダイアログを開く前にリソースを選択しなかった場合は、すべてのポリシーが一覧表示されます。

     注：「**割り当てなし**」を選択して、選択したリソースからポリシー割り当てを削除します。
  4. 以下のいずれかのポリシー割り当て範囲を選択します。
     - **以下の内容を満たす、適用可能なすべてのデバイス**
     - **以下の内容を満たす、選択済みの適用可能なデバイスのみ**
  5. ポリシーに関する 1 つまたは複数の基準を選択します。
     - **割り当て済みポリシーがない**
     - **非適合 (現在割り当てられているポリシーを上書き)**
     - **適合 (現在割り当てられているポリシーを上書き)**

6. 「**適用**」をクリックします。「ファームウェア更新: リポジトリー」ページの「割り当て済みポリシー」列に表示されたポリシーが、選択したファームウェア・コンプライアンス・ポリシーの名前に変わります。

- **リソースのグループへ**
  1. 「**割り当て**」アイコン () をクリックして、「ポリシーの割り当て」ダイアログを表示します。
  2. 割り当てるポリシーを選択します。グループ内のすべてのリソースに適用可能なファームウェア・コンプライアンス・ポリシーのリストから選択できます。リソースに現在ポリシーが割り当てられていない場合、割り当て済みポリシーは「**割り当てなし**」に設定されます。リソースに適用可能なポリシーがない場合、割り当て済みポリシーは「**適用できるポリシーがありません**」に設定されます。

     注：「**割り当てなし**」を選択して、グループ内のリソースからポリシー割り当てを削除します。
  3. ポリシーを割り当てるリソースのグループを 1 つ以上選択します。
  4. 以下のいずれかのポリシー割り当て範囲を選択します。
     - **以下の内容を満たす、適用可能なすべてのデバイス**
     - **以下の内容を満たす、選択済みの適用可能なデバイスのみ**
  5. ポリシーに関する 1 つまたは複数の基準を選択します。
     - **割り当て済みポリシーがない**
     - **非適合 (現在割り当てられているポリシーを上書き)**
     - **適合 (現在割り当てられているポリシーを上書き)**
  6. 「**適用**」をクリックします。「ファームウェア更新: リポジトリー」ページの「割り当て済みポリシー」列に表示されたポリシーが、選択したファームウェア・コンプライアンス・ポリシーの名前に変わります。

終了後

「ポリシー管理」カードから、以下の操作を実行できます。

- ポリシーの詳細を表示するには、テーブル内の行をクリックします。
- 「**編集**」アイコン () をクリックして、選択したポリシーを変更します。

  注：1 つ以上のリソースに割り当てられたポリシーを変更することはできません。最初にポリシーの割り当てを解除する必要があります。
- 「**コピー**」アイコン () をクリックして、選択したポリシーをコピーして変更します。
- 選択した*ユーザーが定義した*ポリシーを削除するには、「**削除**」アイコン () をクリックします。

  注：1 つ以上のリソースに割り当てられたポリシーを削除することはできません。最初にポリシーの割り当てを解除する必要があります。

「適用して有効化」カードで、「**割り当て**」アイコン () をクリックして、「**割り当てなし**」ポリシーを選択した後、ポリシーの割り当てが設定されたすべてのリソースに変更を適用するか、または選択済みリソースのみに変更を適用するかを選択して、選択済みリソースのポリシーの割り当てを解除できます。

リソース・マネージャーへの更新の適用とアクティブ化

XClarity Orchestrator では、更新は自動的に適用されません。ソフトウェアを更新するには、選択した Lenovo XClarity Administrator リソース・マネージャーで、割り当てられた更新コンプライアンス・ポリシーに適合していないものに対して、更新を手動で適用してアクティブ化する必要があります。

始める前に

リソースで更新を適用してアクティブ化しようとする前に、更新の考慮事項を必ず読んでください (デプロイメントの考慮事項の更新 を参照)。

更新コンプライアンス・ポリシーがターゲット・リソースに割り当てられていることを確認します (更新コンプライアンス・ポリシーの作成と割り当て を参照)。

現在インストールされているソフトウェア・レベルと同じかそれ以前のソフトウェアレベルの更新を適用することはできません。

このタスクについて

割り当てられた更新コンプライアンス・ポリシーのあるデバイスと、そのポリシーに適合していない XClarity Administrator リソース・マネージャーにファームウェア更新を適用することができます。ソフトウェアの更新は、以下の方法で実行することができます。

- 特定の非準拠マネージャーに
- 特定のグループ内のすべての非準拠マネージャーに
- 特定の更新コンプライアンス・ポリシーが割り当てられているすべての非準拠マネージャーに
- 特定の更新コンプライアンス・ポリシーが割り当てられている、特定のグループ内のすべての非準拠マネージャーに
- ポリシーに割り当てられ、そのポリシーに準拠していないすべての非準拠マネージャーに

XClarity Orchestrator は、リソースを直接更新しません。その代わりに、該当するリソース・マネージャーに要求を送信して更新を実行し、要求の進行状況を追跡します。XClarity Orchestrator は更新を実行するために必要な依存関係を識別し、ターゲット・リソースを正しい順序で確実に更新し、適用可能な更新パッケージをリソース・マネージャーに転送し、リソース・マネージャーでジョブを開始して更新を実行する要求を作成します。

更新プロセス中に、更新プロセスの全体が完了するまでの間、ターゲット・リソースが複数回自動的に再起動される可能性があります。続行する前に、ターゲット・リソースのすべてのアプリケーションを休止させてください。

ターゲット・リソース内のいずれかのコンポーネントの更新中にエラーが発生した場合、そのコンポーネントは更新プロセスにより更新されません。ただし、更新プロセスは、リソース内の他のコンポーネントの更新を続行し、現在の更新ジョブに含まれる他のすべてのターゲット・リソースの更新を続行します。

前提条件となる更新は、自動的には適用されません。

ヒント:

- この表には、更新可能なリソース・マネージャーのみ表示されています。
- 「**Build 番号**」および「**コンプライアンス・ターゲット・Build 番号**」の列は、デフォルトで非表示になっています。「**すべての操作**」 ➡ 「**列の切り替え**」の順にクリックすると、これらの列を表示できます。

手順

XClarity Orchestrator リソース・マネージャーに更新を適用するには、以下のいずれかの手順を実行します。

- **特定の非準拠リソース・マネージャーに**
  1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング**」( ) ➡ 「**更新**」をクリックし、「**適用して有効化**」をクリックして、「適用して有効化」カードを表示します。

2. 「**リソース・マネージャー**」タブをクリックします。
3. 更新を適用するリソース・マネージャーを 1 つ以上選択します。
4. 「**更新の適用**」アイコン () をクリックして、「更新の要約」ダイアログを表示します。
5. 「**更新の実行**」をクリックして更新を適用します。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)。

- **特定のグループ内の、または特定の更新コンプライアンス・ポリシーが割り当てられている、すべての非準拠リソース・マネージャーに**

1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** ()」 → 「**更新**」をクリックし、「**適用して有効化**」をクリックして、「適用して有効化」カードを表示します。
2. 「**リソース・マネージャー**」タブをクリックします。
3. 「**更新の適用**」アイコン () をクリックして、「更新の要約」ダイアログを表示します。
4. グループと更新コンプライアンス・ポリシーを選択します。
   - ポリシーまたはグループを選択しない場合、ポリシーが割り当てられており、そのポリシーに準拠していないすべてのマネージャーが更新されます。
   - ポリシーを選択したが、グループを選択していない場合、そのポリシーが割り当てられており、そのポリシーに準拠していないすべてのマネージャーが更新されます。
   - 1 つ以上のグループを選択したが、ポリシーを選択していない場合、割り当てられたポリシーに準拠していないグループ内の、すべてのマネージャーが更新されます。
   - ポリシーを選択して、1 つ以上のグループを選択した場合、そのポリシーに割り当てられ、そのポリシーに準拠していないグループ内の、すべてのマネージャーが更新されます。
5. 「**更新の実行**」をクリックして更新を適用します。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)。

管理対象サーバーへの更新の適用とアクティブ化

Lenovo XClarity Orchestrator では、更新は自動的に適用されません。ファームウェアを更新するには、選択したデバイスの中で、割り当てられた更新コンプライアンス・ポリシーに適合していないものに対して、更新を手動で適用してアクティブ化する必要があります。

始める前に

デバイスに更新を適用してアクティブ化する前に、更新の注意事項を必ず読んでください (デプロイメントの考慮事項の更新 を参照)。

更新コンプライアンス・ポリシーがターゲット・デバイスに割り当てられていることを確認します (更新コンプライアンス・ポリシーの作成と割り当て を参照)。

管理対象サーバーにのみファームウェア更新を適用できます。

一度に多くのデバイスでファームウェアを更新する場合は、パフォーマンスを向上させるために、XClarity Orchestrator v1.3.1 以降と Lenovo XClarity Administrator v3.2.1 以降を使用してください。

このタスクについて

割り当てられた更新コンプライアンス・ポリシーのあるデバイスと、そのポリシーに準拠していないデバイスにファームウェア更新を適用することができます。ファームウェアの更新は、以下の方法で実行することができます。

- 特定の非準拠デバイスに
- 特定のグループ内のすべての非準拠デバイスに
- 特定の更新コンプライアンス・ポリシーが割り当てられているすべての非準拠デバイスに
- 特定の更新コンプライアンス・ポリシーが割り当てられている、特定のグループ内のすべての非準拠デバイスに
- ポリシーに割り当てられ、そのポリシーに準拠していないすべての非準拠デバイスに

1 つ以上のコンポーネントのインストール済みファームウェア・バージョンが更新コンプライアンス・ポリシーのターゲット・ファームウェア・バージョン*以前またはそれ以降*である場合、サーバーには「非適合」のフラグが付きます。インストール済みのファームウェア・バージョンがターゲットのファームウェア・バージョンより*新しい*場合は、コンポーネント上のファームウェアのダウングレードに更新を適用する際に、「**強制更新**」オプションを選択する必要があります。「**強制更新**」オプションが選択されていない場合、インストール済みのバージョンより新しいターゲットのファームウェア・バージョンのみが適用されます。

注：特定のデバイス・オプション、アダプター、およびドライブのみがダウングレードをサポートします。ダウングレードがサポートされているかどうかを判別するには、ハードウェアの資料を参照してください。

XClarity Orchestrator は、リソースを直接更新しません。その代わりに、該当するリソース・マネージャーに要求を送信して更新を実行し、要求の進行状況を追跡します。XClarity Orchestrator は更新を実行するために必要な依存関係を識別し、ターゲット・リソースを正しい順序で確実に更新し、適用可能な更新パッケージをリソース・マネージャーに転送し、リソース・マネージャーでジョブを開始して更新を実行する要求を作成します。

更新プロセス中に、更新プロセス全体が完了するまでの間、ターゲット・デバイスが複数回自動的に再起動される可能性があります。続行する前に、ターゲット・デバイスのすべてのアプリケーションを休止させてください。

ターゲット・デバイス内のいずれかのコンポーネントの更新中にエラーが発生した場合、そのコンポーネントは更新プロセスにより更新されません。ただし、更新プロセスは、デバイス内の他のコンポーネントの更新を続行し、現在の更新ジョブに含まれる他のすべてのターゲット・デバイスの更新を続行します。

前提条件となる更新は、自動的には適用されません。

ヒント:

- この表には、更新可能なデバイスのみ表示されています。
- 「**Build 番号**」、「**コンプライアンス・ターゲット・Build 番号**」、「**製品名**」 の各列は、デフォルトで非表示になっています。「**すべての操作**」 ➡ 「**列の切り替え**」の順にクリックすると、これらの列を表示できます。

- ThinkSystem SR635、SR645、SR655、および SR665 サーバーの場合、インバンドおよびアウト・オブ・バンドの両方のファームウェアを適用するには、まずベースボード管理コントローラーに更新を適用してから、残りのオプションにファームウェア更新を適用します。

手順

管理対象デバイスに更新を適用するには、以下のいずれかの手順を実行します。

- **特定の非準拠デバイスに**
  1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** ( )」 ➔ 「**更新**」をクリックし、「**適用して有効化**」をクリックして、「適用して有効化」カードを表示します。
  2. 「**デバイス**」タブをクリックします。
  3. 更新を適用するデバイスを 1 つ以上選択します。
  4. 「**更新の適用**」アイコン ( ) をクリックして、「更新の要約」ダイアログを表示します。
  5. 更新をいつアクティブにするかを選択します。
     - **優先順位を設定したアクティベーション**。ベースボード管理コントローラーのファームウェア更新は即座にアクティブ化されます。その他のすべてのファームウェア更新は、次回にデバイスが再起動したときに有効になります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。
     - **遅延アクティベーション**。全部ではなく一部の更新操作が実行されます。更新プロセスを続行するには、ターゲット・デバイスを手動で再起動する必要があります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

       何らかの理由でターゲット・デバイスが再起動すると、遅延更新プロセスが完了します。

       重要：

       - 「**通常の再起動**」を使用してサーバーを再起動し、更新プロセスを続行します。「**今すぐ再起動**」を使用 *しないでください*。
       - 一度に 50 台を超えるデバイスに対して「遅延アクティベーション」を選択しないでください。XClarity Orchestrator は、遅延アクティベーションが設定されているデバイスを積極的に監視し、デバイスが再起動したときに遅延アクティベーションが処理されるようにします。遅延アクティベーションを使用して 50 台を超えるデバイスに更新を適用するには、更新をバッチに分けて一度に 50 台のデバイスを更新するように選択します。
     - **即時アクティベーション**。更新プロセス中に、更新プロセス全体が完了するまでの間、ターゲット・デバイスが複数回自動的に再起動される可能性があります。続行する前に、ターゲット・デバイスのすべてのアプリケーションを休止させてください。

     注：

     - XClarity Management Hub 2.0 によって管理されているサーバーおよび ThinkEdge クライアント・デバイスの場合、選択したアクティベーション・ルールに関係なく、「即時アクティベーション」のみがサポートされます。
     - 有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする Lenovo XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。
  6. **オプション**: ファームウェア・レベルが最新の場合でも、選択済みコンポーネントのファームウェアを更新するか、選択済みコンポーネントに現在インストールされているものよりも前のファームウェア更新を適用するには、「**強制更新**」を選択します。

7. **オプション**: ファームウェア更新を実行する日付と時刻を選択するには、「**更新のスケジュール**」を選択します。選択しない場合、ファームウェアはすぐに更新されます。
8. 「**更新の実行**」をクリックして更新を適用します。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)。

- **特定の更新コンプライアンス・ポリシーが割り当てられている、特定のグループ内のすべての非準拠デバイスに**
  1. XClarity Orchestrator メニュー・バーで、「**プロビジョニング** ( )」 → 「**更新**」をクリックし、「**適用して有効化**」をクリックして、「適用して有効化」カードを表示します。
  2. 「**デバイス**」タブをクリックします。
  3. 更新を適用するデバイス・グループを 1 つ以上選択します。
  4. 「**更新の適用**」アイコン ( ) をクリックして、「更新の要約」ダイアログを表示します。
  5. グループと更新コンプライアンス・ポリシーを選択します。
     – ポリシーまたはグループを選択しない場合、ポリシーが割り当てられており、そのポリシーに準拠していないすべてのデバイスが更新されます。
     – ポリシーを選択したが、グループを選択していない場合、そのポリシーが割り当てられており、そのポリシーに準拠していないすべてのデバイスが更新されます。
     – 1 つ以上のグループを選択したが、ポリシーを選択していない場合、割り当てられたポリシーに準拠していないグループ内の、すべてのデバイスが更新されます。
     – ポリシーを選択して、1 つ以上のグループを選択した場合、そのポリシーが割り当てられており、そのポリシーに準拠していないグループ内の、すべてのデバイスが更新されます。
  6. 更新をいつアクティブにするかを選択します。
     – **優先順位を設定したアクティベーション**。ベースボード管理コントローラーのファームウェア更新は即座にアクティブ化されます。その他のすべてのファームウェア更新は、次回にデバイスが再起動したときに有効になります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。
     – **遅延アクティベーション**。全部ではなく一部の更新操作が実行されます。更新プロセスを続行するには、ターゲット・デバイスを手動で再起動する必要があります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

       何らかの理由でターゲット・デバイスが再起動すると、遅延更新プロセスが完了します。

       重要：

       – 「**通常の再起動**」を使用してサーバーを再起動し、更新プロセスを続行します。「**今すぐ再起動**」を使用 *しないでください*。
       – 一度に 50 台を超えるデバイスに対して「遅延アクティベーション」を選択しないでください。XClarity Orchestrator は、遅延アクティベーションが設定されているデバイスを積極的に監視し、デバイスが再起動したときに遅延アクティベーションが処理されるようにします。遅延アクティベーションを使用して 50 台を超えるデバイスに更新を適用するには、更新をバッチに分けて一度に 50 台のデバイスを更新するように選択します。
     – **即時アクティベーション**。更新プロセス中に、更新プロセス全体が完了するまでの間、ターゲット・デバイスが複数回自動的に再起動される可能性があります。続行する前に、ターゲット・デバイスのすべてのアプリケーションを休止させてください。

       注：

       – XClarity Management Hub 2.0 によって管理されているサーバーおよび ThinkEdge クライアント・デバイスの場合、選択したアクティベーション・ルールに関係なく、「即時アクティベーション」のみがサポートされます。

– 有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする Lenovo XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。

7. **オプション**: ファームウェア・レベルが最新の場合でも、選択済みコンポーネントのファームウェアを更新するか、選択済みコンポーネントに現在インストールされているものよりも前のファームウェア更新を適用するには、「**強制更新**」を選択します。
8. **オプション**: ファームウェア更新を実行する日付と時刻を選択するには、「**更新のスケジュール**」を選択します。選択しない場合、ファームウェアはすぐに更新されます。
9. 「**更新の実行**」をクリックして更新を適用します。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)。

終了後

「パターン」カードから、以下の操作を実行できます。

- 「**レポート・フォワーダーの作成**」アイコン () をクリックして、反復ベースのファームウェア・コンプライアンスに関するレポートを 1 つ以上のメールアドレスに転送します。レポートは、現在テーブルに適用されているデータ・フィルターを使用して送信されます。表示および非表示されたテーブルのすべての列がレポートに含まれます。詳しくは、レポートの転送を参照してください。
- 「**レポート・フォワーダーに追加**」アイコン () をクリックして、テーブルに現在適用されているデータ・フィルターを使用して、特定のレポート・フォワーダーにファームウェア・コンプライアンス・レポートを追加します。レポート・フォワーダーにファームウェア・コンプライアンス・レポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。

まだ実行されていないスケジュールされたファームウェア更新ジョブをキャンセルするには、XClarity Orchestrator のメニュー・バーで、「**監視**」 → 「**ジョブ**」をクリックし、「**スケジュール**」タブをクリックして「スケジュール・ジョブ」カードを表示します。スケジュール・ジョブを選択し、「**キャンセル**」 () アイコンをクリックします。

第 6 章　傾向の分析と問題の予測

Lenovo XClarity Orchestrator は、既知のハードウェアおよびファームウェアの問題に基づいて分析アラートを生成し、傾向を監視して管理対象リソースの異常を検出し、ヒューリスティックを構築します。これによって、差し迫った問題や障害の可能性を計算することができます。この傾向は、照会、グラフ、図表として視覚化され、これによって適合状況、問題履歴、最も問題のあるリソースの内訳がわかります。これらの傾向を分析すれば、問題の原因を詳しく把握し、問題を迅速に解決することができます。

重要：

- XCC ファームウェア v1.4 以降を実行している ThinkAgile、ThinkSystem、ThinkEdge サーバーでは、分析機能がサポートされています。
- 分析機能を使用するには、分析機能をサポートする各対象デバイスに対して、Lenovo XClarity Orchestrator Analytics ライセンスが必要になります。ライセンスは特定のデバイスに関連付けられて*いません*。詳しくは、XClarity Orchestrator ライセンスの適用 XClarity Orchestrator オンライン・ドキュメント を参照してください。

カスタム分析レポートの作成

分析レポートはバックグラウンドで継続的に実行されるため、データ・センターがリアルタイムでどの程度適切に稼働しているかを把握することができます。

このタスクについて

Lenovo XClarity Orchestratorは、管理対象リソースから収集されたイベント、インベントリ、またはメトリック・データに基づいて、いくつかの事前定義済み 分析レポートを提供します。その後、統計 (表形式)、またはグラフを棒グラフまたは円グラフで表示します。これらのレポートの例については、「**分析** ()」 ➡ 「**事前定義済み分析**」ページを参照してください。

独自のカスタム・レポートを作成して、最も関心のあるデータを表示することもできます。

手順

カスタム分析レポートを作成するには、以下の手順を実行します。

ステップ 1. カスタム・アラートを作成します。

XClarity Orchestrator 既知のハードウェアとファームウェアの問題に基づいて分析アラートを生成します。カスタム・レポートで使用するカスタム・アラートを作成することもできます。

ステップ 2. カスタム・レポート (照会) を作成します。

最も関心のあるデータに基づいてクエリを定義することにより、カスタム・グラフィカル・レポートを XClarity Orchestrator に追加できます。

カスタム分析アラートのルールの作成

Lenovo XClarity Orchestrator は、既知のハードウェアおよびファームウェアの問題に基づいてアラートを生成します。カスタム・*アラート・ルール*を定義すると、特定のイベントが発生した場合、または特定のメトリックに違反した場合に分析アラートを生成します。その後、そのアラートを使用してカスタム分析レポート (照会) を生成できます。

このタスクについて

カスタム分析アラートを含むすべてのアラートに対して、イベントが発生します。アクティブ・アラートとイベントの両方に使用されるイベント・コードは FQXXOCA*xxxxc* という形式です。*xxxx* は固有 ID で、*c* は重大度です。

カスタム・アラートは、ヘルス状況に関するアクティブ・アラートのリストに含まれます。カスタム・アラートを含むすべてのアクティブ・アラートが、1 つの統合ビューに表示されます (アクティブなアラートの監視を参照)。

手順

カスタム・アラート・ルールを作成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator メニュー・バーで、「**分析** ( )」 → 「**カスタム・アラート**」をクリックして、「カスタム・アラート・ルール」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、「カスタム・アラート・ルールの作成」ダイアログを表示します。

ステップ 3. カスタム・アラートの固有名とオプションの説明を指定します。

ステップ 4. このルールのソース・タイプを選択します。
- **イベント**。ルールの基準に基づいて、特定のイベントが発生するとアラートを生成します。
- **メトリック**。ルールの基準に基づいて、特定のメトリックに違反するとアラートを生成します。

ステップ 5. 「**ルール・トリガーの詳細**」をクリックし、このルールの基準を指定します。基準はソース・タイプによって異なります。

- **イベント・ベースのアラート・ルール**
  - このアラートのターゲット・タイプを指定します。
    - **デバイス**。任意のデバイスでイベントが発生するとアラートを生成します。このアラートにはデバイス名が含まれています。
    - **デバイス・グループ**。任意のデバイス・グループのデバイスでイベントが発生するとアラートを生成します。このアラートにはグループ名が含まれています。
  - アラートをトリガーするイベントの ID を指定します。イベント IDのリストについては、イベントとアラートのメッセージ XClarity Orchestrator オンライン・ドキュメントを参照してください。
  - アラートが生成されるまでに、指定された間隔でそのイベントが発生しなければならない回数 (カウント) を指定します。
  - アラートが生成されるまでに、そのイベントが発生する期間 (間隔、分単位) を選択します。
- **メトリック・ベースのアラート・ルール**
  - 基準モードを選択します。
    - **平均**。メトリックの平均値が、特定の間隔の間にしきい値に達する (比較演算子に基づく) と、アラートを生成します。

たとえば、24 時間 (**interval**) の平均 CPU 温度 (**metric**) が 40°C (**threshold**) より大きい (**operator**) 場合にアラートを生成するルールを作成できます。

- **カウント**。メトリックが、特定の間隔の間に一定回数しきい値に達する (比較演算子に基づく) と、アラートを生成します。

  たとえば、24 時間 (**interval**) で 5 回 (**count**)、CPU 温度 (**metric**) が 40°C (**threshold**) より大きい (**operator**) 場合にアラートを生成するルールを作成できます。

- **簡易**。メトリックがしきい値に達する (比較演算子に基づく) とアラートを生成します。

  たとえば、CPU 温度 (**metric**) が 40°C (**threshold**) より大きい (**operator**) 場合にアラートを生成するルールを作成できます。

- 管理対象リソースでサポートされている測定のリストから、このアラートの測定 (メトリック) を選択します。
- 基準モードが「カウント」の場合、アラートが生成されるまでに、指定された間隔でその値に到達した回数を指定します。
- 比較関数を選択します。
  - >=。以上
  - <=。以下
  - >。よりも大きい
  - <。未満
  - =.等しい
  - !=.以外
- メトリック値と比較するしきい値を指定します。
- 基準モードが「平均」または「カウント」の場合は、メトリックが評価される期間 (間隔、分単位) を選択します。

ステップ 6. 「**アラートとイベントの詳細**」をクリックし、アラートとイベントについて表示する情報を指定します。

1. 関連するアラートおよびイベントについて表示するメッセージ、説明、およびユーザー操作を指定します。変数を含めるには、フィールド (変数) 名を二重角かっこで囲みます (例: [[DeviceName]])。入力フィールドの右側のテーブルに、使用可能なフィールドのリスト (選択した測定に基づく) が表示されます。
2. このアラート・ルールの重大度を選択します。
   - 「**警告**」。対処が必要かどうかをユーザーが決定できます。
   - 「**重大**」。広い範囲の対処が今すぐ必要です (重要なリソースの機能停止が間もなく発生する可能性があります)。
3. このアラートのイベント・コードとして使用する固有の 4 桁の番号を指定します。未使用の 0001 ～ 9999 の数字を指定できます。

ステップ 7. オプションで、ステータスを「**有効**」に変更して XClarity Orchestrator を有効にし、カスタム・アラートの基準を満たした場合に分析アラートを発生させます。

ステップ 8. 「**作成**」をクリックします。

終了後

「**監視** ()」 ➙ 「**アラート**」をクリックすると、有効になっているカスタム・アラート・ルールに基づいて発生した分析アラートのリストを表示できます。

「カスタム・アラート・ルール」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、選択済みカスタム・アラート・ルールのプロパティを変更します。
- 「**削除**」アイコン () をクリックして、選択済みカスタム・アラート・ルールを削除します。

- 1 つ以上の選択済みカスタム・アラート・ルールを有効または無効にするには、「**有効**」アイコン (○) または「**無効**」アイコン (⊗) をクリックします。

カスタム・レポート (クエリ) の作成

アラート、イベント、インベントリー、デバイス・メトリック、またはカスタム・メトリック (集約) などの収集されたデータに基づいてクエリを定義することにより、カスタムの表形式のレポートおよびグラフィカル・レポートを Lenovo XClarity Orchestrator に追加できます。

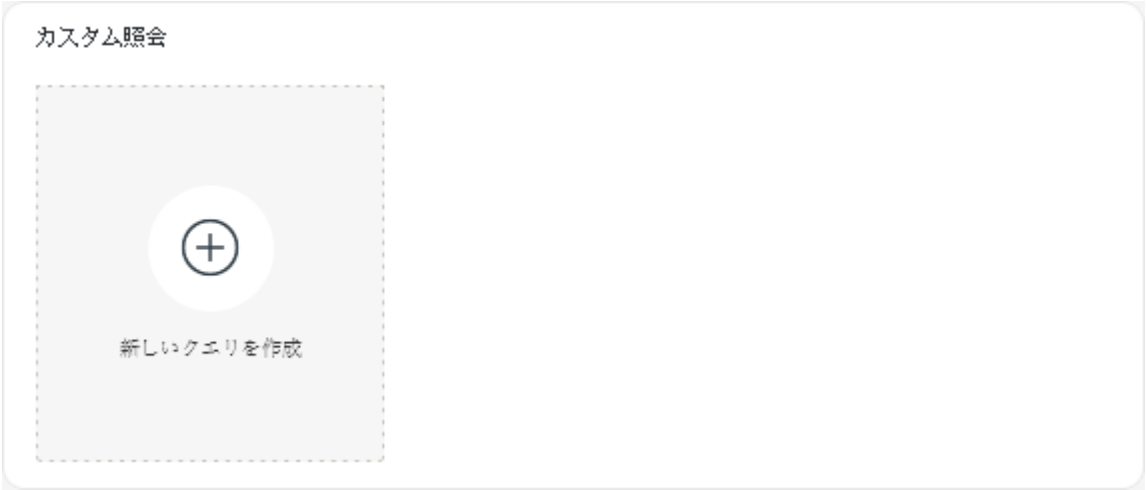
始める前に

重要：XClarity Orchestrator でのカスタム分析レポートの作成には、データベースおよびデータベース照会の基本的な理解が必要です。

このタスクについて

カスタム・レポートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Orchestrator メニュー・バーで、「**分析** (📊) → **分析**」をクリックして、「カスタマイズされたクエリ」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、「カスタム・クエリの作成」ダイアログを表示します。

ステップ 3. このカスタム・クエリの固有名を指定します。

ステップ 4. このクエリのソースとして使用するデータのタイプを選択します。

次のデータ・ソースのタイプのいずれかを選択できます。
- **アラート**。調査とユーザー操作が必要になるハードウェアまたは管理の状態
- **イベント**。リソースと監査イベント
- **イベント - リソース**。管理対象デバイス、リソース・マネージャー、または XClarity Orchestrator で発生したハードウェアまたは Orchestrator の状態。
- **イベント - 監査**。リソース・マネージャーまたは XClarity Orchestrator から実行されたユーザー・アクティビティ
- **インベントリー - マネージャー**。リソース・マネージャーのインベントリー・データ
- **インベントリー - デバイス**。すべてのタイプの管理対象デバイスのインベントリー・データ
- **インベントリー - デバイス - サーバー**。管理対象サーバーのインベントリー・データ
- **インベントリー - デバイス - スイッチ**。管理対象スイッチのインベントリー・データ
- **インベントリー - デバイス - ストレージ**。管理対象ストレージ・デバイスのインベントリー・データ
- **インベントリー - デバイス - シャーシ**。管理対象シャーシのインベントリー・データ

- **CPUTemp**。管理対象デバイスの各プロセッサーの温度 (摂氏) のメトリック・データ。メトリックは 1 分ごとに収集されます。
- **CPUUtilizationStats**。管理対象デバイスのプロセッサー使用率のメトリック・データ (パーセント)。メトリックは 1 分ごとに収集されます。
- **InletAirTemp**。管理対象デバイスの吸気口の温度 (摂氏) のメトリック・データ。温度は 1 分ごとに収集されます。
- **MemoryUtilizationStats**。管理対象デバイスのメモリー使用量のメトリック・データ (パーセント)。メトリックは 1 分ごとに収集されます。
- **PowerMetrics**。管理対象デバイスのすべてのプロセッサー、メモリー・モジュール、またはシステム全体の消費電力のメトリック・データ (ワット)。これらのメトリックは 30 秒ごとに収集されます。
- **PowerSupplyStats**。管理対象デバイスのパワー・サプライの入出力のメトリック・データ (ワット)。これらのメトリックは 30 秒ごとに収集されます。

リストされているデータ・ソースのタイプ (アラート、イベント、インベントリー、およびメトリック) は、XClarity Orchestrator で使用可能なデータによって異なります。たとえば、アラート・データが使用可能な場合は、**アラート**・タイプがリストされます。イベント・データが使用可能な場合は、すべての**イベント** - * タイプがリストされます。

選択済みデータ・ソースは、「**クエリ条件**」タブで使用可能なデータに影響を及ぼします。「**インベントリー - デバイス**」などの汎用タイプを選択した場合は、すべてのデバイスに共通の属性のみがリストされます。「**インベントリー - デバイス - サーバー**」を選択した場合は、すべてのサーバーに共通の属性がリストされます。

ステップ 5. 「**クエリ条件**」をクリックして、レポートのクエリ条件を定義します。

1. このクエリに使用するデータを絞り込みます。
   a. 「**フィルタリングされたフィールド**」ドロップダウン・リストから 1 つ以上のフィールドを選択します。手順 4 で選択したデータ・ソース・タイプに基づいてリストされているフィールド。
   b. 複数のフィルター・フィールドを選択した場合は、クエリの作成に使用する演算子を選択します。これは以下のいずれかの値です。
      - **AND**。すべての値が一致している必要があります。
      - **OR**。1 つ以上の値が一致している必要があります。
      - 「**AND (否定)**」。すべての値が一致していない必要があります。
      - 「**OR (否定)**」。1 つ以上の値が一致していない必要があります。
   c. 選択済みのフィルタリングされた各フィールドについて、「**比較**」ドロップダウン・リストから比較演算子を選択し、フィールドの値を選択します。使用可能な比較演算子は、属性のデータ・タイプによって異なります。
      - >=。*以上*の値を指定された値に一致させます
      - <=。*以下*の値を指定された値に一致させます
      - 「>」。*より大きい*値を指定された値に一致させます
      - 「<」。*未満*の値を指定された値に一致させます
      - =.*等しい*値を指定された値に一致させます
      - !=.*以外*の値を指定された値に一致させます
      - **Contains**。(インベントリーおよびイベント・クエリのみ) 配列で指定された一部の値を一致させます
      - **In**。(インベントリーおよびイベント・クエリのみ) 配列で指定されたすべての値を一致させます
      - **NotIn**。(インベントリーおよびイベント・クエリのみ) 配列で指定されたどの値も一致させません

      ヒント: いずれかのフィールドの現在の値を検索するには、同じデータ - ソース・タイプを使用して新しいクエリを作成し、「**グループ化されたフィールド**」ドロップダウ

ン・リストでフィールド名を選択し、「**限度**」に **0** を指定して、「**保存**」をクリックします。「**グラフ オプション**」タブには、現在のすべての値のリストが表示されます。

2. オプションで、「**結果の集約**」セクションで集約関数を選択して、フィルタリングされたデータに基づいて新しいフィールドを作成し、新しいフィールドの名前 (別名) を指定します。平均や最大などの一部の集約関数では、関数を適用するフィールドも指定する必要があります。

   イベントおよびインベントリー・クエリの場合は、以下のいずれかの関数を選択できます。
   - **Average**。すべての値の統計的な平均値
   - **Sum**。すべての値の合計
   - **Count**。値の数
   - **Maximum**。最大値
   - **Minimum**。最小値
   - **最初**。最も古いタイムスタンプの値
   - **最後**。最も新しいタイムスタンプの値

   メトリック・クエリの場合は、次のいずれかの関数を選択できます。
   - **Count**。null 以外の値の数
   - **Distinct**。固有値のリスト
   - **Integral**。平均フィールド値
   - **Mean**。値の算術平均 (平均)
   - **Median**。中央値
   - **Mode**。最も頻度の高い値
   - **Spread**。最小値と最大値の差
   - **Stddev**。標準偏差
   - **Sum**。すべての値の合計
3. オプションで、「**グループ化されたフィールド**」ドロップダウン・リストで、クエリ結果をグループ化するために使用するフィールドを選択します。グループ化されたフィールドを選択した場合、XClarity Orchestrator は選択したフィールドの各値にデータ・ポイントが存在するように、データをアンワインド (分解) します。
4. オプションで、「**フィールドで並び替え**」ドロップダウン・リストでフィールドを選択し、「**ソート順序**」ドロップダウン・リストでソート順序を選択して、クエリ結果を並べ替える方法を選択します。メトリック・クエリの場合、時間でのみ並べ替えることができます。
5. オプションで、クエリ結果に返すデータ・ポイントの数を「**限度**」フィールドに指定します。デフォルトの制限は 10 です。0 を指定するか、空のままにしておくと、すべてのデータ・ポイントが返されます。

   オプションで、「**オフセット**」フィールドのクエリ結果で、スキップするデータ・ポイントの数を指定することもできます。
6. (メトリック・クエリのみ) グループ化されたフィールドを選択した場合は、オプションでクエリ結果に返されるデータ・セットの数を「**系列の制限**」フィールドで指定します。デフォルトの制限は空 (0) です。0 を指定するか、空のままにしておくと、すべてのデータ・セットが返されます。

   オプションで、「**系列のオフセット**」フィールドのクエリ結果で、スキップするデータ・セットの数を指定することもできます。
7. 「**保存**」をクリックしてクエリを保存し、レポートを生成します。

ステップ 6. レポートのルック・アンド・フィールを選択するには、「**グラフ・オプション**」をリックします。次のタイプのグラフがあります。

- **テーブル**。データを表形式で表示します。
- 「**棒**」。データをグラフィカルな棒グラフで表示します。x 軸と y 軸に使用するフィールドを選択します。

- 「**円**」。データをグラフィカルな円グラフで表示します。x 軸と y 軸に使用するフィールドを選択します。データがグループ化されていない場合にのみ円グラフの使用を選択できます。

ステップ 7. 「**作成**」をクリックして、現在のクエリ結果に関するレポートを含む新しいカードを追加します。

終了後

「カスタマイズされたクエリ」カードから、以下の操作を実行できます。

- カスタム・レポート・カードの「**拡大**」アイコン ( ) をクリックして、カスタム・レポートを拡大します。表形式のレポートの場合、「カスタマイズされたクエリ」カードのレポート・アイコンには、テーブルの最初の 4 列のみが表示されます。レポートを拡大して、テーブル内のすべての列を表示できます。

  テーブル列の「**詳細の確認**」リンクは、列に複数のデータ・フィールドが含まれていることを示します。「**詳細の確認**」リンクをクリックすると、その他のデータを一覧表示するポップアップ・テーブルが表示されます。
- カードの「**編集**」アイコン ( ) をクリックして、カスタム・レポートのプロパティを変更します。
- カードの「**削除**」アイコン ( ) をクリックして、カスタム・レポートを削除します。

デバイスのブート時間の分析

「分析」パネルには、管理対象デバイスのブート時間を要約するレポート・カードが含まれています。*ブート時間*とは、オペレーティング・システムが立ち上がるまでの、システム・ブートの完了にかかった時間を秒単位で示したものです。

ブート時間レポートを表示するには、「**分析**」( ) → 「**事前定義済み分析**」をクリックし、「**ブート時間**」をクリックして、関連する分析カードを表示します。

注：ブート統計は、XCC ファームウェア v1.40 以降を実行している ThinkSystem デバイスおよび ThinkAgile デバイスでのみ使用可能です。

ブート時間

このレポート・カードには棒グラフが含まれており、最後のブート時間が最も長いデバイスについて、ブートの完了にかかった時間を示します。

接続に関する問題の分析

「分析」パネルには、接続の問題に関する統計を示すレポート・カードが含まれます。

接続が失われた場合は、次のイベントによりレポートされます。

- **FQXHMDM0163J**。デバイス内のリソース・マネージャーとベースボード管理コントローラーとの間の接続がオフラインになっています。

接続性喪失のレポートを表示するには、「**分析**」( ) → 「**事前定義済み分析**」をクリックし、「**接続の問題**」をクリックして、関連する分析カードを表示します。

時間別の接続の問題

このレポート・カードには棒グラフが含まれ、各リソースに関して現在の日付または月で発生した接続問題の数が示されます。

カードの右上隅にある「**設定**」アイコン ( ) を選択して、特定の時間範囲のデータを表示できます。

接続問題の数での上位 10 台のデバイス

このレポート・カードには棒グラフが含まれ、このグラフには最大合計数の接続に関する問題をレポートしている上位 10 台のデバイスが示されます。特定のリソースに関する詳細情報を表示するには、凡例の項目をクリックします。

セキュリティー修正の分析

「分析」パネルには、既知の共通脆弱性識別子 (CVE) のセキュリティー修正に関する分析を示すレポート・カードが含まれます。

CVE レポートを表示するには、「**分析**」( ) → 「**事前定義済み分析**」をクリックし、「**セキュリティー修正**」をクリックして、関連する分析カードを表示します。

セキュリティー修正

このレポート・カードには、次の統計情報とグラフが含まれています。

- セキュリティー修正が利用可能な共通脆弱性識別子 (CVE) を持つ管理対象デバイスの数を、最も高い CVE 重大度別に示す円グラフ
  - 「**重大**」。重大な CVE が少なくとも 1 つ存在するデバイスの数
  - 「**重大でない**」。高、中、または低の CVE が少なくとも 1 つ存在するが、重大な CVE が存在しないデバイスの数
  - **保護**。既知の CVE が存在せず、保護されているデバイスの数
- セキュリティー修正が利用可能な一意の CVE の数を、重大度 (重大、高、中、低) 別に示す円グラフ

円グラフに各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。各状態の隣にある数字をクリックして、その条件に一致するすべてのデバイスのリストを表示することもできます。

デバイス

デバイス・カードには、セキュリティー修正が利用可能な CVEs の総数、および各デバイスの CVE の最も高い重大度が一覧表示されます。デバイスを展開すると、そのデバイス内でセキュリティー修正が適用されているコンポーネントのリストと、更新リポジトリーにダウンロードされているファームウェア更新から利用できるセキュリティー修正の数を表示できます。

セキュリティー修正の数をクリックすると、そのコンポーネントに適用できる CVE のフィルタリングされたリストが表示されたダイアログが開きます。そのダイアログで CVE リンクをクリックすると、その CVE に関する詳細情報が Web 上で表示されます。

「**デバイスの表示 / 非表示**」トグルをクリックすると、「デバイス」カードを表示または非表示にできます。グラフ内の数字をクリックすると、トグルが自動的に「**デバイスを表示**」に変わります。

ドライブの正常性の分析

「分析」パネルには、管理対象の ThinkAgile サーバーおよび ThinkSystem サーバーの、ハードディスク・ドライブおよびソリッド・ステート・ドライブの状態および障害予知に関する分析を示すレポート・カードが含まれます。

ファームウェア・レポートを表示するには、「**分析**」( ) → 「**事前定義済み分析**」をクリックした後、「**予測分析を推進する**」をクリックして、関連する分析カードを表示します。

分析では、以下のドライブ・モデル・タイプがサポートされます。

ハード・ドライブ

- ST2000NX0253
- ST8000NM0055

- ST10000NM0086
- ST12000NM0008

ソリッド・ステート・ドライブ
- Intel SSDSC2BB800G4

重要：古いファームウェアを使用するドライブは分析対象として適格ではありません。ドライバーを最新のファームウェア・レベルに更新して予測分析を有効にしてください。

危険な状態のドライブ

このレポート・カードには、それぞれの正常性状態 (正常または危険) のドライブ数を示す円グラフが含まれます。

危険な状態のドライブの履歴

このレポート・カードには、前週または前年の間に障害が発生したドライブの数を示す棒グラフが含まれます。グラフ内の各棒の上にカーソルを置くと、その日に障害が発生したドライブのフィルタリング・リストがデバイスごとに表示されます。

障害予知のあるドライブ

レポート・カードには、障害が発生したドライブのある、デバイスの詳細をリストした表が含まれます。デバイスをクリックすると、そのデバイスの各危険なドライブの詳細を一覧表示できます。

ファームウェアの分析

「分析」パネルには、ファームウェアに関する分析を示すレポート・カードが含まれます。

ファームウェア・レポートを表示するには、「**分析**」( ) → 「**事前定義済み分析**」をクリックし、次に「**ファームウェア分析**」をクリックして、関連する分析カードを表示します。

ファームウェア分析

このレポート・カードには、ファームウェアのカテゴリーと経年数に基づいて、管理対象デバイスにインストール済みのファームウェア数を示す棒グラフが含まれます。

ファームウェアは、以下のカテゴリーにグループ化されます。
- 管理コントローラー
- システム・ツール
- UEFI

ファームウェアの経年数は、次の間隔にグループ化されます
- **6 か月以内**
- **6 ～ 12 か月**
- **1 ～ 2 年**
- **2 年以上**

「**フィルター**」入力フィールドを使用して、レポートに含むデバイスをフィルタリングできます。定期的に使用するフィルタリングされたクエリを保存することもできます。

「**デバイスの表示 / 非表示**」トグルをクリックすると、「デバイス」カードを表示または非表示にできます。デバイス・カードには、グラフに含まれるすべてのデバイスのファームウェア・タイプと経年数が一覧表示されます。

紛失イベントの分析

「分析パネル」には、紛失イベントに関する統計を示すレポート・カードが含まれます。紛失イベントは、シーケンス番号の差によって識別されます

イベントには、各イベントが特定のデバイスで発生した順序を示すシーケンス番号があります。特定のデバイスに関するイベント・シーケンス番号は連続している必要があります。連続していないシーケンス番号がある場合、差は 1 つ以上のイベントが失われたことを示している可能性があります。

紛失イベント・レポートを表示するには、「**分析 ()**」 → 「**事前定義済み分析**」をクリックし、「**紛失イベント**」をクリックして、関連する分析カードを表示します。

時間別の紛失イベント

このレポート・カードには棒グラフが含まれ、各リソースに関して現在の日付または月で紛失されたイベントの数が示されます。

カードの右上隅にある「**設定**」アイコン () を選択して、特定の時間範囲のデータを表示できます。

紛失イベントの数での上位 10 台のデバイス

このレポート・カードには棒グラフが含まれ、このグラフには最大合計数の紛失イベントをレポートしている上位 10 台のデバイスが示されます。

リソース・マネージャーの容量を分析および予測する

「分析」パネルには、リソース・マネージャーで管理対象デバイスの最大数を超えると予測されるレポート・カードが含まれます。Lenovo XClarity Administrator リソース・マネージャーの場合、最大 1000 台の管理対象デバイスがサポートされます。

リソース・マネージャー容量レポートを表示するには、「**高度な分析**」() → 「**事前定義済み分析**」をクリックし、「**マネージャーの容量予測**」をクリックして、関連する分析カードを表示します。

マネージャーの容量

このレポートには、管理対象デバイスの数や容量ステータス、容量を超過しているかなど、各リソース・マネージャーのデバイスの容量がリストされます。容量の状態は以下のとおりです。

- () **正常**。サポートされるデバイスの最大数を下回る管理対象デバイスの数。
- () **警告**。サポートされるデバイスの最大数に近い管理対象デバイスの数。
- () **重大**。サポートされるデバイスの最大数を超える管理対象デバイスの数。

容量トレンドの管理

このレポート・カードには、特定のリソース・マネージャーについて管理されているデバイスの数 (時間経過に伴う) と、その管理対象デバイスの数がそのリソース・マネージャーの最大サポート容量に到達する予測トレンドを示す線グラフが含まれています。

「マネージャーの容量」テーブルの行をクリックして、そのリソース・マネージャーの容量トレンドを表示します。

表示される期間を変更するには、ドロップダウン・メニューをクリックします。データは年別、四半期別、月別、または日別に表示できます。グラフの下にあるズーム・ボックスを使用して、グラフに表示する期間の数を変更することもできます。

使用率の傾向を分析および予測する

「分析」パネルには、デバイスおよび仮想リソース (ホスト、クラスター、仮想マシンなど) でのプロセッサー、ストレージ、メモリーの使用量の履歴および予測を表示するレポート・カードが含まれます。

重要：この機能を使用するには、VMware vRealize オペレーション・マネージャー リソース・マネージャーに接続する必要があります (リソース・マネージャーの接続を参照)。

使用率のトレンド・レポートを表示するには、「**高度な分析 ( )**」 ➡ 「**事前定義済み分析**」をクリックし、「**ワークロード使用率のトレンド**」をクリックして、関連する分析カードを表示します。

リソース選択

このレポートには、Orchestrator サーバーで管理されているデバイスと仮想リソースがリストされます。

テーブルの行をクリックして、そのリソースの使用率のトレンドを表示します。

CPU 使用率トレンド

このレポート・カードには、特定の仮想リソースについてプロセッサー使用率 (時間経過に伴う) と、そのプロセッサー使用率がその仮想リソースの最大サポート容量に到達する予測トレンドを示す線グラフが含まれています。

「**履歴**」ドロップダウン・メニューおよび「**投影**」ドロップダウン・メニューのそれぞれから履歴および予測データを表示する期間を変更できます。グラフの下にあるズーム・ボックスを使用して、グラフに表示する期間の数を変更することもできます。

メモリー使用率のトレンド

このレポート・カードには、特定の仮想リソースについてメモリー使用率 (時間経過に伴う) と、そのメモリー使用率がその仮想リソースの最大サポート容量に到達する予測トレンドを示す線グラフが含まれています。

「**履歴**」ドロップダウン・メニューおよび「**投影**」ドロップダウン・メニューのそれぞれから履歴および予測データを表示する期間を変更できます。グラフの下にあるズーム・ボックスを使用して、グラフに表示する期間の数を変更することもできます。

ストレージ使用率のトレンド

このレポート・カードには、特定の仮想リソースについてストレージ使用率 (時間経過に伴う) と、そのストレージ使用率がその仮想リソースの最大サポート容量に到達する予測トレンドを示す線グラフが含まれています。

「**履歴**」ドロップダウン・メニューおよび「**投影**」ドロップダウン・メニューのそれぞれから履歴および予測データを表示する期間を変更できます。グラフの下にあるズーム・ボックスを使用して、グラフに表示する期間の数を変更することもできます。

パフォーマンスおよび使用量メトリックの分析

「分析」パネルには、直近 24 時間の特定のメトリックおよびリソースに基づいてヒートマップを示すレポート・カードが含まれています。

パフォーマンス・ヒートマップを表示するには、「**高度な分析**」( ) ➡ 「**事前定義済み分析**」をクリックし、「**パフォーマンス・ヒートマップ**」をクリックして、関連する分析カードを表示します。

パフォーマンス・ヒートマップ

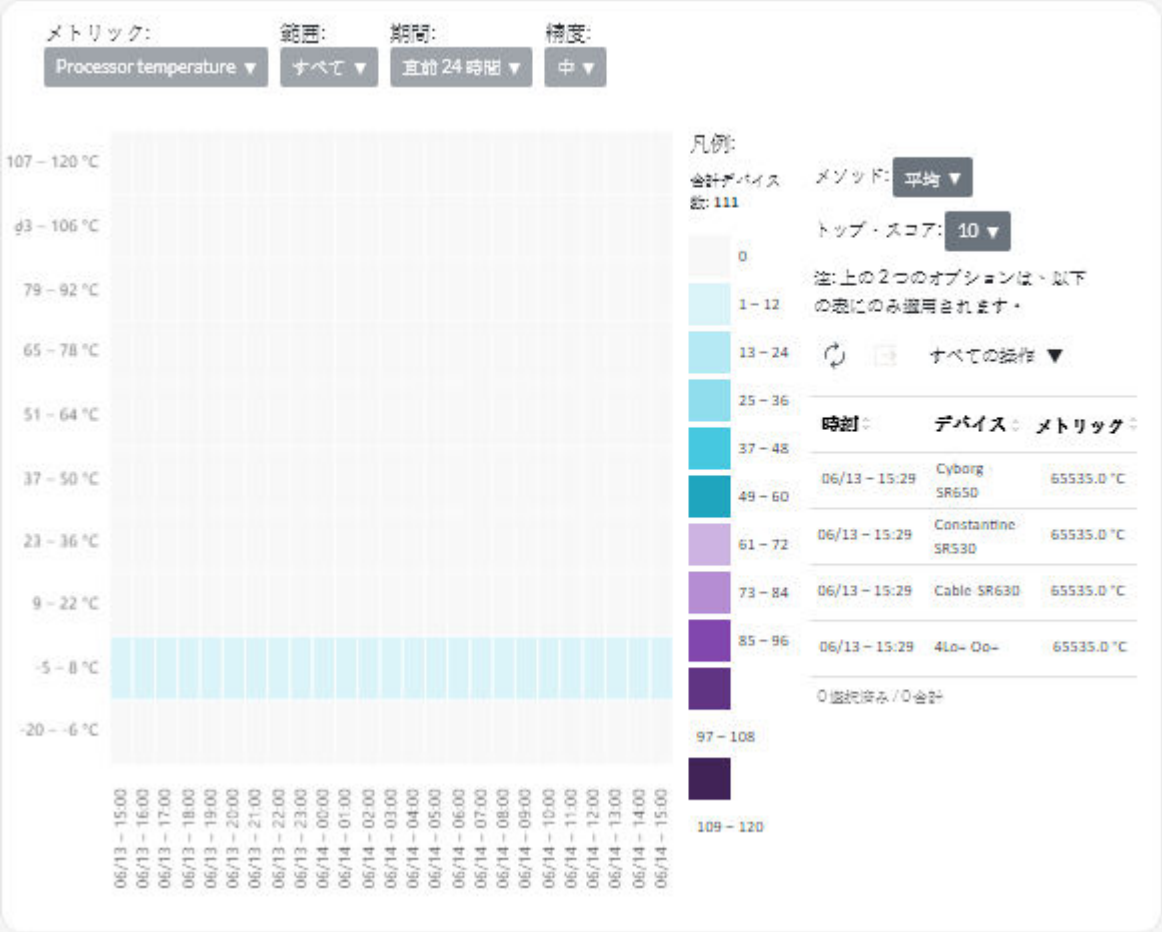
このレポート・カードには、特定の期間に特定の数の範囲内のメトリック値を持つデバイスの数を示すヒートマップが含まれています。

ヒートマップ内の任意のセルをクリックして、そのセルによって表されるデバイスのポップアップ・リストを表示し、メトリックが収集されたときの各デバイスおよびタイム・スタンプの実際のメトリック値と情報を表示できます。

関心のある情報のみを表示するようにヒートマップを構成できます。

- 表示するメトリックのデータを以下から 1 つ選択できます。
  - プロセッサー温度
  - プロセッサー使用率
  - メモリー使用率
- 平均値またはピーク (最高) 値に基づいてメトリック・データを集約することを選択できます。
- ヒートマップをフィルタリングして、特定のデバイス・グループのデバイスに関するメトリック・データのみを含めることができます。

  注：ユーザー・インターフェースを特定のリソース・マネージャーに適用すると、選択したグループ内にある、リソース・マネージャーでも管理されているデバイスのデータのみがヒートマップに含まれるようになります。
- ヒートマップの x 軸に表示する数値範囲を選択することもできます。最大値と最小値の間の値の数は、選択した数に基づいて等しい間隔で分割されます。10、15、または 20 を選択できます。
- メトリックを収集したときに、上位 10 台、15 台、または 20 台のデバイスを最大値とタイム・スタンプとともに一覧表示するように選択することもできます。



繰り返しイベントの分析

「分析」パネルには、各デバイスの繰り返しイベントを要約するレポート・カードが含まれています。

*繰り返しイベント*は、以下の条件が発生した場合に生成されます。

- **FQXXOIS0002J**。同じ ID を持つクリティカル・イベントまたは警告イベントが、連続した 5 分間に少なくとも 3 回、同じデバイスに対して 1 回以上生成された場合。
- **FQXXOIS0003J**。6 件以上のクリティカル・イベントまたは警告イベントが、連続した 2 時間以上の間、1 時間ごとに同じデバイスに対して生成された場合。

繰り返しイベント・レポートを表示するには、「**高度な分析**」( ) → 「**事前定義済み分析**」をクリックし、「**繰り返しイベント**」をクリックして、関連する分析カードを表示します。

繰り返しイベント

このレポート・カードには、各デバイスの繰り返しイベントの合計数を示す棒グラフが含まれています。

時間ごとの繰り返しイベント

このレポート・カードには、デバイスごとに、現在の日付に発生した繰り返しイベントの数を示す棒グラフが含まれています。

不正アクセスの試行の分析

「分析」パネルには、不正アクセスの試行 (ログイン試行の失敗) を要約するレポート・カードが含まれています。

不正アクセス・レポートを表示するには、「**分析**」() → 「**事前定義済み分析**」をクリックし、次に「**不正アクセスの試行**」をクリックして、不正アクセス分析カードを表示します。

ユーザーごとのログイン試行の失敗数

このレポート・カードには、不正アクセス試行の合計数をユーザー (ユーザー名) ごとに示すグラフが含まれています。データを棒グラフ () または円グラフ () として表示するには、カードの左上隅の該当するアイコンをクリックします。

グラフ内の各棒や区分をマウスでポイントすると、直前の発生などの詳細情報を得ることができます。

ユーザーごとのログイン試行の失敗数 (期間ごと)

このレポート・カードには、現在の日付に発生した不正アクセス試行の合計数をユーザー (ユーザー名) ごとに示す棒グラフが含まれています。

ユーザー IP アドレスごとのログイン試行の失敗数

このレポート・カードには、不正アクセス試行の合計数をユーザー (IP アドレス) 別に示す棒グラフが含まれています。データを棒グラフ () または円グラフ () として表示するには、カードの左上隅の該当するアイコンをクリックします。

グラフ内の各棒や区分をマウスでポイントすると、直前の発生などの詳細情報を得ることができます。

ユーザー IP アドレスごとのログイン試行の失敗数 (期間ごと)

このレポート・カードには、現在の日付に発生した不正アクセス試行の合計数をユーザー (IP アドレス) ごとに示す棒グラフが含まれています。

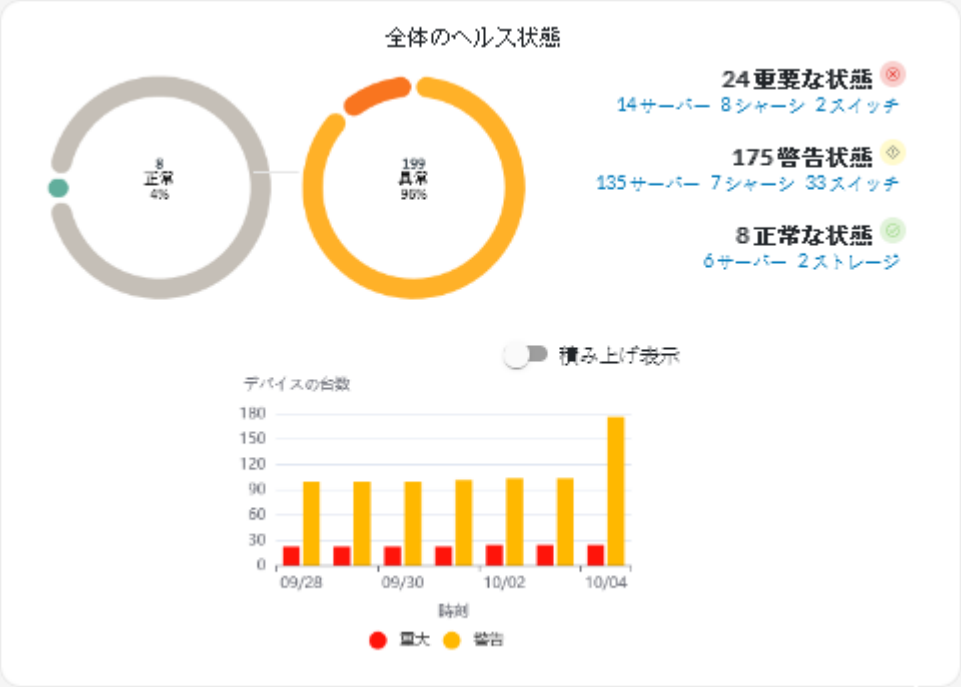
デバイスの正常性の分析

ダッシュボードの全体のヘルス・ステータス・カードと、各デバイスのデバイス分析カードには、管理対象デバイスの全体的なヘルス情報が要約されます。

すべてのデバイスのステータス要約

の XClarity Orchestrator のメニュー・バーから、「**ダッシュボード** ()」をクリックすると、「ダッシュボード」カードに、すべての管理対象デバイスとその他のリソースの概要とステータスが表示されます (環境の概要の表示 を参照)。

「**マネージャーを選択**」ドロップダウン・メニューで、要約の範囲を特定のリソース・マネージャーや特定のリソース・グループで管理されているデバイスのみに変更できます。



円グラフおよび棒グラフの各カラー・バーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。各状態のデバイスの数をクリックして、その条件に一致するすべてのデバイスのリストを表示することもできます。

特定タイプのデバイスすべてのステータスの要約

アクティブ・アラート全体の要約を表示するには、XClarity Orchestrator のメニュー・バーで「**リソース**」() をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。たとえば「**サーバー**」を選択すると、すべてのラック、タワー、および高密度サーバーと、シャーシ内のすべての Flex System および ThinkSystem サーバーのリストが表示されます。

「**分析の基準**」ドロップダウン・リストからデバイスのプロパティーに基づく要約の範囲を変更できます。

- **マシン・タイプ/モデル**。(デフォルト) このレポートでは、マシン・タイプ・モデル (MTM) ごとにデバイス・ヘルスが要約されます。
- **マシン・タイプ**このレポートでは、マシン・タイプごとにデバイス・ヘルスが要約されます。
- **製品名**。このレポートでは、製品ごとにデバイス・ヘルスが要約されます。

XClarity Orchestrator は、特定の基準に基づいてデバイス・ヘルスを要約します。各要約には、以下の情報が含まれます。

- 異常なデバイスの合計数、および各異常状態のデバイスのパーセンテージ (クリティカル、警告、および不明) を示す円グラフ。

  円グラフの各カラー・バーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。
- 指定された日数における、各ヘルス状態の 1 日あたりのデバイス数を示す折れ線グラフ。

  折れ線グラフの各色のバーは、特定の状態にあるデバイスの数を示しています。各カラー・バーをマウスでポイントすると、状態に関する詳細情報がわかります。
- 特定の日の、異常がある各タイプのデバイス数。デフォルトでは現在の日が表示されています。日を変更するには、折れ線グラフでそれぞれの日をポイントします。

インフラストラクチャー・リソースの正常性の分析

インフラストラクチャー・リソースの全体的な正常性とセンサーの傾向を判別できます。

インフラストラクチャー・リソースの正常性状態

Lenovo XClarity Orchestrator のメニュー・バーで、「**リソース**」(⎈) → 「**インフラストラクチャー**」の順にクリックして、「インフラストラクチャー」カードを表示します。「**ステータス**」列から各リソースの正常性状態を確認できます。

センサーの傾向

XClarity Orchestratorメニュー・バーで「**リソース**」(⎈) → 「**インフラストラクチャー**」をクリックして、インフラストラクチャー・カードを表示します。その後、テーブルでインフラストラクチャー・リソースをクリックすると、そのリソースのセンサーのリストと各センサーの最新の測定値が表示されます。

1 つ以上のセンサーを選択し、「**グラフ**」アイコン ( ) をクリックすると、選択した各センサーの経時的な測定値を示す折れ線グラフが表示されます。デフォルトでは、同じ単位 (ワットやアンペアなど) のセンサーは同じグラフに表示されます。

注：Schneider Electric EcoStruxure IT Expertでは、センサーのデータを 5 分ごとに収集し、XClarity Orchestrator でこのデータを 1 時間ごとに同期します。現在、XClarity Orchestrator は、直近 60 分間のデータのみ保存します。

アクティブなアラートの分析

アクティブなアラートは、アラート分析カードに要約されています。

Lenovo XClarity Orchestrator は、特定の基準に基づいてアクティブ・アラートを要約します。各要約には、以下の情報が含まれます。

- 各要約タイプに関連付けられたアクティブなアラートの合計数とアラートのパーセンテージを示す円グラフ
- 各要約タイプのアクティブなアラートの数
- 古いアクティブ・アラートの経過日数
- 指定された日数における、各要約タイプの 1 日あたりのアクティブ・アラートの数を示す折れ線グラフ
- 要約タイプごとに、特定の日にアクティブであったアラートの数。デフォルトでは現在の日が表示されています。日を変更するには、折れ線グラフでそれぞれの日をポイントします。

全体のアクティブ・アラート

アクティブ・アラート全体の要約を表示するには、以下の手順を実行します。

1. XClarity Orchestrator メニュー・バーで、「**監視**」( ) → 「**アラート**」をクリックして、「アラートの分析」カードを表示します。
2. 折れ線グラフの上にあるドロップダウン・リストから期間を選択します。デフォルトは、最近 7 日間です。
3. 「**分析の基準**」ドロップダウン・リストから、要約のタイプを選択します。
   - **重大度**。(デフォルト) このレポートには、クリティカル、警告、通知といった重大度別に、アクティブ・アラートが要約されています。
   - **ソース・タイプ**。このレポートには、ソース・タイプ別 (デバイス、管理、分析など) に生成されたアクティブなアラートが要約されています。
   - **リソース・タイプ**。このレポートには、デバイス、リソース・マネージャー、XClarity Orchestrator などリソース・タイプ別のアクティブ・アラートが要約されています。
   - **保守容易性**。このレポートには、各保守容易性に関連付けられたアクティブ・アラートが要約されています。**none** は「保守不要」、**user** は「ユーザーが保守を実行」、**serviceable** は「Lenovo が保守を実行」の意味です。

特定のデバイスに関するアクティブ・アラート

特定デバイスのアクティブ・アラートを表示するには、以下の手順を実行します。

1. XClarity Orchestrator のメニュー・バーで「**リソース** ( )」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。
2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。
3. 「**アラート・ログ**」をクリックすると、そのデバイスのアクティブ・アラートのリストとアラート分析カードが表示されます。

4. 「アラートの分析」カードで、折れ線グラフの上のドロップダウン・リストから期間を選択します。デフォルトは、最近 7 日間です。
5. 「**分析の基準**」ドロップダウン・リストから、要約のタイプを選択します。
   - **ソース・タイプ**。このレポートには、ソース・タイプ別 (デバイス、管理、分析など) に生成されたアクティブなアラートが要約されています。
   - **保守容易性のタイプ**。このレポートには、各保守容易性に関連付けられたアクティブ・アラートが要約されています。none は「保守不要」、user は「ユーザーが保守を実行」、serviceable は「Lenovo が保守を実行」の意味です。
   - **重大度**。このレポートには、クリティカル、警告、通知といった重大度別に、アクティブ・アラートが要約されています。

第 7 章　サービスおよびサポートの操作

Lenovo XClarity Orchestrator には、サービス・ファイルの収集とそのデータの Lenovo サポート への送信、特定のデバイスで特定の保守可能なイベントが発生したときのサービス・プロバイダーへの自動通知のセットアップ、サービス・チケット・ステータスの表示、保証情報に使用できる一連のツールが用意されています。問題が発生したときは、Lenovo サポートに問い合わせてヘルプおよび技術サポートを入手することができます。

Lenovo への定期的なデータの送信

オプションで、ハードウェア環境に関する情報を収集し、そのデータを定期的に Lenovo に送信することを Lenovo XClarity Orchestrator に許可することができます。Lenovo では、Lenovo 製品や Lenovo サポートの品質向上にこのデータを利用しています。

始める前に

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。

注意：Lenovo サポートにデータを転送するには、Lenovo のプライバシーに関する声明 に同意する必要があります。

このタスクについて

複数のユーザーのハードウェア・データを分析することにより、Lenovo は定期的に発生するハードウェアの変更について把握することができます。その後、予測分析を強化したり、適切な場所に部品の在庫を確保することでサービスおよびサポート・エクスペリエンスを向上したりするために、このデータが利用されます。

ハードウェア・データを Lenovo に送信することに同意した場合、以下のデータが収集され、定期的に送信されます。

- **毎日のハードウェア・データ**。各管理対象デバイスのインベントリー・データおよびドライブ分析データ (データ収集が有効な場合) の変更のみ
- **毎週のハードウェア・データ**。管理対象デバイスのすべてのインベントリー・データ、および接続されているリソース・マネージャーに関する情報

注意：このデータは*匿名ではありません*。

- 収集されるデータには、UUID、WWN、デバイス ID、およびシリアル番号が*含まれます*。XClarity Orchestrator は、SHA512 で UUID、WWN、およびデバイス ID をハッシュ計算することでインベントリーを変更します。
- 収集されるデータに、ネットワーク情報 (IP アドレス、ドメイン名、ホスト名) やユーザー情報は*含まれません*。

データが Lenovo に送信されると、HTTPS を使用して XClarity Orchestrator インスタンスから Lenovo アップロード・ファシリティーに転送されます。この HTTPS 接続経由で REST API が呼び出され、データが送信されます。XClarity Orchestrator に事前にロードされた証明書が認証に使用されます。XClarity Orchestrator インスタンスがインターネットに直接アクセスできず、XClarity Orchestrator でプロキシが構成されている場合、データはそのプロキシを介して送信されます。

その後、データは Lenovo カスタマー・ケア・リポジトリーに移動され、最大 5 年間保管されます。このリポジトリーは安全な場所であり、問題のトラブルシューティングのためにデバッグ・データを

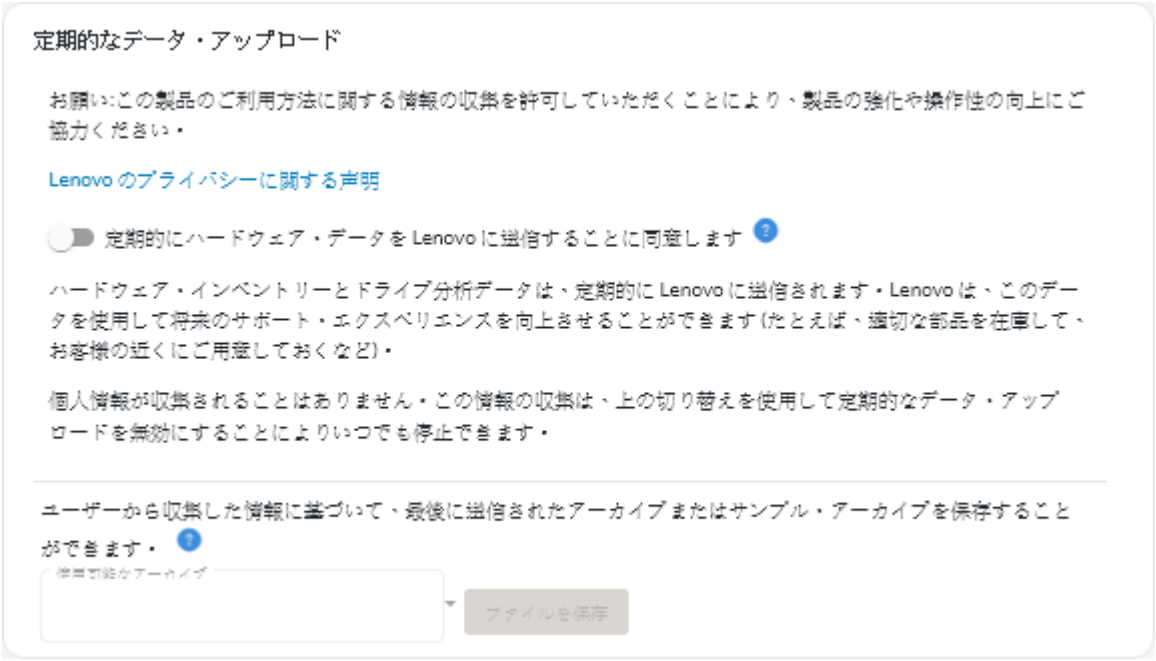
Lenovo に送信する際にも使用されます。ほとんどの Lenovo サーバー、ストレージ、およびスイッチ製品で使用されます。

Lenovo カスタマー・ケア・リポジトリーからは、提供されたデータについて照会が実行され、Lenovo 製品チームが分析に使用できるグラフが生成されます。

手順

お客様のデータを収集して Lenovo に送信することを XClarity Orchestrator に許可するには、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「**定期的なデータ・アップロード**」をクリックして「定期的なデータ・アップロード」カードを表示します。



ステップ 2. オプションで、ハードウェア・データを Lenovo に送信することに同意します。

ステップ 3. Lenovo のプライバシーに関する声明 に同意します。

終了後

データの送信に同意した場合、このページからは以下の操作を実行できます。

- ダウンロードするアーカイブを選択して「**ファイルの保存**」をクリックすることで、Lenovo に送信された最新の毎日/毎週のデータ・アーカイブをローカル・システムに保存できます。

サービス・データの収集 - XClarity Orchestrator

Lenovo XClarity Orchestrator 用にサービス・データを手動で収集し、その情報を tar.gz 形式のアーカイブとしてローカル・システムに保存することができます。次に、サービス・ファイルをダウンロードするか優先サービス・プロバイダーに送信し、発生した問題の解決に役立てることができます。

始める前に

詳細: サービス・データの収集方法

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。

サービス・データのダウンロード中に Web ブラウザーが XClarity Orchestrator Web サイトのポップアップをブロックしないことを確認します。

手順

XClarity Orchestrator のサービス・データを収集するには、以下の手順を実行します。

ステップ 1. 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「**サービス・データ**」をクリックして「サービス・データの管理」カードを表示します。

ステップ 2. 「**名前を付けて保存**」をクリックし、サービス・データを収集してアーカイブをローカル・システムに保存します。

サービス・データを収集するジョブを作成します。「**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)。

終了後

また、以下の操作を実行できます。

- 「**サービス・チケットを開く**」アイコン (📄) をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから特定のデバイスのサービス・チケットを手動で開きます (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)。
- 「**サービス・ファイルを付加**」アイコン (📎) をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから、選択したアクティブ・サービス・チケットにサービス・データ・アーカイブを付加します。XClarity Orchestrator またはローカル・システムからファイルを添付できます。

  注：

  – 2 GB 以下の単一アーカイブ・ファイルを接続できます。ファイル名の最大長は 200 文字です。サービス・データ・アーカイブの作成については、デバイスのサービス・データの収集を参照してください。
  – サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットにアーカイブをアタッチすることはできません。
  – リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットにアーカイブを付加することはできません。
- 「**保存**」アイコン (⬇) をクリックして、選択した 1 つ以上のサービス・データ・アーカイブを「管理サービス・データ」カードからローカル・システムに保存します。複数のファイルを選択した場合、ファイルはダウンロード前に 1 つの .tar.gz ファイルに圧縮されます。
- 「管理サービス・データ」カードから「**削除**」アイコン (🗑) をクリックして、必要なくなった 1 つ以上の選択済みのサービス・データ・アーカイブを削除するか、「**すべて削除**」アイコン (⊖) をクリックしてアーカイブをすべて削除します。

デバイスのサービス・データの収集

デバイスに問題が発生し、解決に Lenovo サポートなどサービス・プロバイダーのサポートが必要な場合、そのデバイスのサービス・データ (サービス情報、インベントリー、ログなど) を tar.gz 形式のアーカイブ・ファイルとして手動で収集し、問題の原因の特定に役立てることができます。このアーカイブ・ファイルはローカル・システムに保存してから、優先サービス・プロバイダーに送信することができます。

始める前に

サービス・データを収集する前に、Lenovo のプライバシーに関する声明 を受諾する必要があります。プライバシーに関する声明を受諾するには、「**管理 (⚙)**」 ➔ 「**サービスおよびサポート**」をクリックして、左側のナビゲーションで「**コール・ホーム構成**」をクリックしてから、「**Lenovo のプライバシーに関する声明に同意する**」を選択します。

XClarity Orchestrator 用サービス・データのローカル・システムへの 保存については、196 ページの 「サービス・データの収集 - XClarity Orchestrator」 を参照してください。

サービス・チケットを手動で開き、サービス・データを Lenovo サポートに送信する方法については、205 ページの 「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。

保守可能なイベントがデバイスで発生した際に、Lenovo サポート・センターでサービス・チケットを自動的に開いて、サービス・データ・アーカイブを送信するコール・ホームのセットアップについては、202 ページの 「コール・ホームを使用して自動的にサービス・チケットを開く」 を参照してください。

このタスクについて

Lenovo XClarity Orchestrator でサービス・データを収集する場合、Orchestrator サーバーがリソース・マネージャー (Lenovo XClarity Administrator など) に要求を送信します。リソース・マネージャーは、データを収集してアーカイブ・ファイルとしてローカル・リポジトリーに保存した後、アーカイブ・ファイルを XClarity Orchestrator に転送します。

最大 50 個のデバイスのサービス・データを一度に収集できます。

手順

特定のデバイスのサービス・データを収集するには、以下の手順を実行します。

ステップ 1. 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「**デバイス操作**」をクリックして「デバイス操作」カードを表示します。

ステップ 2. サービス・データを収集するデバイスを選択し、「**サービス・データの収集**」アイコン ( ) 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)。

ステップ 3. 左ナビゲーションの「**デバイス・サービス・データ**」をクリックして、「サービス・データ」カードを表示します。サービス・データ・アーカイブがテーブルに表示されます。

ステップ 4. オプションで、サービス・ファイルをローカル・システムに保存するには、「**保存**」アイコン ( ) をクリックします。

終了後

また、以下の操作を実行できます。

- 「**サービス・チケットを開く**」アイコン () をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから特定のデバイスのサービス・チケットを手動で開きます (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)。
- 「**サービス・ファイルを付加**」アイコン () をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから、選択したアクティブ・サービス・チケットにサービス・データ・アーカイブを付加します。XClarity Orchestrator またはローカル・システムからファイルを添付できます。

  注：

  – 2 GB 以下の単一アーカイブ・ファイルを接続できます。ファイル名の最大長は 200 文字です。サービス・データ・アーカイブの作成については、デバイスのサービス・データの収集を参照してください。

  – サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットにアーカイブをアタッチすることはできません。

  – リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットにアーカイブを付加することはできません。
- 「**保存**」アイコン () をクリックして、選択した 1 つ以上のサービス・データ・アーカイブを「サービス・データ」カードからローカル・システムに保存します。複数のファイルが選択されている場合、ファイルは 1 つの tar. gz ファイルとして保存されます。

  注：ローカル・システムには、一度に最大 50 個のサービス・データ・アーカイブを保存できます。
- 「サービス・データ」カードから「**削除**」アイコン () をクリックして、必要なくなった 1 つ以上の選択済みのサービス・データ・アーカイブを削除するか、「**すべて削除**」アイコン () をクリックしてアーカイブをすべて削除します。

  注：すべてのアーカイブを削除するには、SupervisorGroup グループのメンバーである必要があります。

デバイスのサービス・データをインポートする

特定のデバイスのサービス・データ・アーカイブをインポートできます。アーカイブは、Lenovo XClarity Administrator リソース・マネージャーから、またはベースボード管理コントローラーから直接取得できます。

このタスクについて

一度に最大 10 ファイル、合計 2GB までインポートできます。

保存デバイスのサービス・データを複数回インポートした場合、インベントリー・データは最後にインポートされたサービス・データによって上書きされます。

手順

サービス・データ・アーカイブをインポートするには、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「**サービス・データ**」をクリックして「デバイス・サービス・データ」カードを表示します。

ステップ 2. 「**インポート**」アイコン () をクリックし、サービス・データ・アーカイブをインポートします。

ステップ 3. 1 つ以上のサービス・データ・アーカイブ (.tar.gz、tzz、または tgz 形式) 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**」をクリックしてアーカイブを見つけることができます。

ステップ 4. アーカイブが現在 XClarity Orchestrator によって管理されていないデバイス用である場合のみ、「**確認目的でのみサービス・データのサーバーをインベントリーに追加**」を選択します。

ステップ 5. 「**インポート**」をクリックしてアーカイブをインポートおよび解析し、オプションとしてオフライン・デバイスを管理します。

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)。

サービスおよびサポートの連絡先の作成と割り当て

リソースが Lenovo サポートからの支援を必要とする場合、Lenovo は連絡先を知る必要があります。1 つの場所の連絡先情報を定義し、それらの連絡先を特定のリソースのデフォルトの主要連絡先および二次的連絡先として割り当てることができます。

始める前に

Lenovo のプライバシーに関する声明 が受け入れられていることを確認します。「**管理**」 → 「**サービスおよびサポート**」 → 「**コール・ホームの構成**」ページからプライバシーに関する声明を確認して同意することができます。

このタスクについて

リソース・グループに主要連絡先と二次的連絡先を割り当てることができます。連絡先をリソース・グループに割り当てると、連絡先はそのグループ内のすべてのリソースに割り当てられます。

主要連絡先と二次的連絡先の割り当てはオプションです。ただし、二次的連絡先を割り当てる場合は、主要連絡先も割り当てる必要があります。

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 (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)。

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、デフォルトではコール・ホーム連絡先が割り当てられます。コール・ホーム連絡先は、コール・ホームを使用してサービス・チケットを自動的に開くときに使用されます (コール・ホームを使用して自動的にサービス・チケットを開く を参照)。リソースおよびグループに割り当てられた連絡先は、デフォルトのコール・ホーム連絡先よりも優先されます。

サービス・チケットを手動で開くときに、問題のあるリソースに割り当てられている連絡先を使用するか、別の連絡先を選択するかを選択できます (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)。

手順

- **連絡先の定義**
  1. Lenovo 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「**連絡先情報**」をクリックして「連絡先情報」カードを表示します。
  2. 「**作成**」アイコン ( ) をクリックして、「連絡先を追加」ダイアログを表示します。
  3. 連絡先の名前、メール、電話番号、および場所を入力します。
  4. 希望の連絡方法を選択します。
  5. 「**保存**」をクリックして連絡先を作成します。
- **リソース・グループへの連絡先の割り当て**

1. Lenovo XClarity Orchestrator のメニュー・バーで、「**リソース**」() → 「**グループ**」の順にクリックして、「グループ」カードを表示します。
2. グループを選択して、「**編集**」アイコン () をクリックし、「グループを編集」ダイアログを表示します。
3. リソース・グループを選択します。
4. 「**連絡先情報**」タブをクリックします。
5. グループ内のすべてのデバイスに割り当てる主要サポート連絡先と 1 つ以上の二次的サポート連絡先を選択します。
6. 「**保存**」をクリックします。

終了後

「連絡先情報」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、選択済み連絡先を変更します。
- 「**削除**」アイコン () をクリックして、選択済み連絡先を削除します。

コール・ホームを使用して自動的にサービス・チケットを開く

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

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。

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。

連絡先が以下の国内にある場合、コール・ホームには Lenovo Premier Support 契約が必要です。詳細については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。
- カタール
- サウジアラビア
- アラブ首長国連邦

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、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、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

サービス・データに関連する以下の操作を実行できます。

- 「**構成のリセット**」をクリックして、コール・ホーム設定をデフォルト値にリセットします。
- 左側のナビゲーションで「**サービス・チケット**」をクリックし、コール・ホームを使用して自動または手動で、Lenovo サポート・センターに送信されたすべてのサービス・チケットに関する情報を表示できます。詳しくは、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。
- 「**サービス・データの収集**」アイコン ( ) をクリックして、「デバイス操作」カードから、選択したデバイスのサービス・データを収集します。詳しくは、デバイスのサービス・データの収集を参照してください。
- 「**サービス・ファイルを付加**」アイコン ( ) をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから、選択したアクティブ・サービス・チケットにサービス・データ・アーカイブを付加します。XClarity Orchestrator またはローカル・システムからファイルを添付できます。

  注：

  – 2 GB 以下の単一アーカイブ・ファイルを接続できます。ファイル名の最大長は 200 文字です。サービス・データ・アーカイブの作成については、デバイスのサービス・データの収集を参照してください。

  – サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットにアーカイブをアタッチすることはできません。

  – リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットにアーカイブを付加することはできません。
- デバイスを選択し、「**サービス・チケットを開く**」アイコン ( ) をクリックすることで、Lenovo サポート・センターでサービス・チケットを手動で開き、特定のデバイスのサービス・データを収集し、該当ファイルを「デバイス操作」カードから Lenovo サポート・センターに送信します。詳しくは、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。Lenovo サポート・センターで追加データを必要とする場合、そのデバイスまたは別のデバイスのサービス・データを再収集するように Lenovo サポートから依頼されることがあります。

Lenovo サポート・センターでサービス・チケットを手動で開く

サービス・フォワーダーを使用するコール・ホームが有効になっている場合、管理対象デバイスで保守可能なイベントが発生すると、Lenovo XClarity Orchestrator により自動的にサービス・チケットが開かれ、サービス・ファイルが収集およびダウンロードされて、Lenovo サポート・センターに送信されます。ま

た、手動で管理対象デバイスのサービス・ファイルをアーカイブとして収集し、アーカイブをローカル・システムに保存して、いつでも Lenovo サポート・センターに送信することもできます。サービス・チケットが開かれると、お客様の問題に関する情報が Lenovo サポートに迅速かつ効率的に届き、ハードウェアの問題に対する解決方法を決定するための処理が開始されます。Lenovo サービス技術員は、お客様がサービス・チケットを完了してオープンするとすぐに、解決策の作業を開始します。

始める前に

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・ホームのお問い合わせ先情報が構成されており、有効であることを確認します (コール・ホームを使用して自動的にサービス・チケットを開く)。
- XClarity Orchestrator 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」ページを表示し、XClarity Orchestrator で Lenovo サポート・センターと通信できることを確認します。次に、「**コール・ホーム構成テスト**」をクリックしてテスト・イベントを生成し、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。
- コール・ホームを有効にする前に、XClarity Orchestrator に必要なすべてのポート (コール・ホームに必要なポートを含む) 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、XClarity Orchestrator オンライン・ドキュメントの利用可能なポー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、XClarity Orchestrator オンライン・ドキュメントの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。
- 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。プロキシーのセットアップについて詳しくは、ネットワーク設定の構成を参照してください。

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。

このタスクについて

サービス・チケットを手動で開くときに、問題のあるリソースに割り当てられている連絡先を使用するか、別の連絡先を選択するかを選択できます。

主要連絡先と二次的連絡先がグループに割り当てられると、それらの連絡先はそのグループの各デバイスに割り当てられます。各デバイスには、1 つの主要連絡先と 1 つ以上の二次的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、デバイスがメンバーであるすべてのグループに割り当てられているすべての二次的連絡先がデバイスに割り当てられます。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 (コール・ホームを使用して自動的にサービス・チケットを開くを参照)。

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、デフォルトではコール・ホーム連絡先が割り当てられます。コール・ホーム連絡先は、コール・ホームを使用してサービス・チケットを自動的に開くときに使用されます (コール・ホームを使用して自動的にサービス・チケットを開くを参照)。リソースおよびグループに割り当てられた連絡先は、デフォルトのコール・ホーム連絡先よりも優先されます。

手順

サービス・チケットを手動で開くには、以下の手順を実行します。

- コール・ホームが構成されており、有効である場合、以下の手順を実行してサービス・チケットを開いた後、サービス・データを収集して、ファイルを Lenovo サポート・センターに送信します。
  1. XClarity Orchestrator のメニュー・バーで「**リソース** ( )」をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。
  2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。
  3. 左ナビゲーションの「**サービス**」をクリックして、「サービス・チケット」カードを表示します。
  4. 「**サービス・チケットを開く**」アイコン ( ) をクリックして、「新規チケットの追加」ダイアログを表示します。
  5. 報告する問題の説明を入力します (関連するイベント・コードなど)。
  6. 必要に応じて、問題の重大度を選択します。これは以下のいずれかの値です。
     - **緊急**
     - **高い**
     - **中** (デフォルト)
     - **低い**
  7. 「**送信**」をクリックします。
- 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。

終了後

デバイス固有の「サービス」ページから、以下の操作を実行できます。

- XClarity Orchestrator のメニュー・バーで、「**サービスおよびサポート**」 → 「**サービス・チケット**」をクリックして、開かされている*すべて*のサービス・チケットに関する情報を表示できます。
- 「**サービス・チケットの注を追加**」アイコン ( ) をクリックして、選択したサービス・チケットに注を追加します。

  注：

  - サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットに注を追加することはできません。
  - 注は、Lenovo のサービス・チケットにのみ追加できます。IBM、Service Now、または Cherwill のサービス・チケットに注を追加することはできません。
  - リソース・マネージャーに対して開かれた*ソフトウェア*のサービス・チケットに注を追加することはできません。
- 「**サービス・ファイルを付加**」アイコン ( ) をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから、選択したアクティブ・サービス・チケットにサービス・データ・アーカイブを付加します。XClarity Orchestrator またはローカル・システムからファイルを添付できます。

  注：

  - 2 GB 以下の単一アーカイブ・ファイルを接続できます。ファイル名の最大長は 200 文字です。サービス・データ・アーカイブの作成については、デバイスのサービス・データの収集を参照してください。
  - サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットにアーカイブをアタッチすることはできません。

– リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットにアーカイブを付加することはできません。

サービス・チケットとステータスの表示

コール・ホームを使って手動で作成された、または自動で Lenovo Support センターに送信されたサービス・チケット、およびコール・ホーム以外のサポート・サービスによって生成されたサポート・チケットの情報を表示できます。

このタスクについて

サービス・チケットのステータスは、24 時間ごとに Lenovo サポート・センターと同期して更新されます。

「**状態**」列は、サービス・チケットのステータスを示します。サービス・チケットは、以下のいずれかの状態になります。
- **アクティブ**
- **応答済み**
- **キャンセル**
- **キャンセル**
- **作成**
- **お客様がキャンセルしました**
- **終了**
- **拒否されたパーティ**
- **複製**
- **エラー**
- **エラー状態**
- **進行中**
- **初期化済み**
- **マージ済み**
- **監視 - ソリューションがデプロイされました**
- **新規**
- **保留中**
- **保留中**
- **問題の発生**
- **解決された問題**
- **処理中**
- **拒否**
- **再検索中**
- **解決済み**
- **提供されたソリューション**
- **送信済み**
- **不明**
- **待機中**
- **詳細を待機中**
- **Lenovo 内部サポートを待機する**
- **外部サポート・パーティを待機しています**
- **お客様からのフィードバックをソリューションで待機しています**
- **ソリューションのデプロイメントを待機しています**
- **管理対象サービスに転送されています**
- **ウォーム転送**
- **進行中**

「**タイプ**」列には、「サービス・チケット番号」列にリストされているサービス・チケットのタイプが示されます。サービス・チケット・タイプは以下のいずれかの値です。
- **Cherwill チケット**

- IBM コール・ホーム・チケット
- Lenovo コール・ホーム・チケット
- Lenovo パススルー・コール・ホーム・チケット
- Lenovo ソフトウェア・コール・ホーム・チケット
- ServiceNow

手順

- **すべてのサービス・チケットのステータスの表示**「サービス・チケット」カードを表示するには、「**管理**」 (⚙) ➔ 「**サービスおよびサポート**」の順にクリックして、左側のナビゲーションで「**サービス・チケット**」をクリックします。

  ヒント: イベント ID をクリックすると、サービス・チケットが生成されたイベント (発生した場合のユーザー操作など) の要約が表示されます。

- **特定のデバイスのサービス・チケットのステータスの表示**
  1. XClarity Orchestrator のメニュー・バーで「**リソース**」 (⚙) をクリックし、デバイス・タイプ (「サーバー」、「スイッチ」など) をクリックすると、カード・リストに、該当するタイプのすべての管理対象デバイスが表示されます。
  2. デバイスの行をクリックすると、該当デバイスのデバイス要約カードが表示されます。
  3. 左側のナビゲーションで「**サービス**」をクリックすると、「サービス・チケット」カードが開き、デバイスのサービス・チケットのリストが表示されます。

     ヒント: イベント ID をクリックすると、サービス・チケットが生成されたイベント (発生した場合のユーザー操作など) の要約が表示されます。

終了後

サービス・チケットに関連する以下の操作を実行できます。

- XClarity Orchestrator を構成して、保守可能なイベントが発生したときに自動的にサービス・チケットを開きます (202 ページの「コール・ホームを使用して自動的にサービス・チケットを開く」を参照)。
- 「**サービス・チケット・ステータスの更新**」アイコン () をクリックして、Lenovo サポート・センターとデータを同期し、すべてのアクティブ・サービス・チケットのステータスを更新します。
- 「**サービス・チケットを開く**」アイコン () をクリックして、デバイス固有の「サービス」ページのサービス・チケット・カードから特定のデバイスのサービス・チケットを手動で開きます。
- 「**サービス・チケットの注を追加**」アイコン () をクリックして、選択したサービス・チケットに注を追加します。

  注：

  – サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットに注を追加することはできません。

  – 注は、Lenovo のサービス・チケットにのみ追加できます。IBM、Service Now、または Cherwill のサービス・チケットに注を追加することはできません。

  – リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットに注を追加することはできません。
- 「**サービス・ファイルを付加**」アイコン () をクリックして、デバイス固有の「サービス」ページの「サービス・チケット」カードから、選択したアクティブ・サービス・チケットにサービス・データ・アーカイブを付加します。XClarity Orchestrator またはローカル・システムからファイルを添付できます。

  注：

  – 2 GB 以下の単一アーカイブ・ファイルを接続できます。ファイル名の最大長は 200 文字です。サービス・データ・アーカイブの作成については、デバイスのサービス・データの収集を参照してください。

  – サービス・チケットは、オープン、進行中、保留中のいずれかの状態であることが必要です。クローズ状態またはその他の状態のサービス・チケットにアーカイブをアタッチすることはできません。

  – リソース・マネージャーに対して開かれたソフトウェアのサービス・チケットにアーカイブを付加することはできません。
- 「**レポート・フォワーダーの作成**」アイコン () をクリックして、反復ベースのアクティブなサービス・チケットに関するレポートを 1 つ以上のメール・アドレスに転送します。レポートは、現在テーブルに適用されているデータ・フィルターを使用して送信されます。表示および非表示されたテーブルのすべての列がレポートに含まれます。詳しくは、 を参照してください。
- 「**レポート・フォワーダーに追加**」アイコン () をクリックして、テーブルに現在適用されているデータ・フィルターを使用して、特定のレポート・フォワーダーにアクティブなサービス・チケット・レポートを追加します。レポート・フォワーダーにアクティブなサービス・チケット・レポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。

保証情報の表示

管理対象デバイスの保証状況 (延長保証を含む) を確認できます。

始める前に

Lenovo XClarity Orchestrator で管理対象デバイスの保証情報を収集するには、以下の URL にアクセスできる必要があります。これらの URL へのアクセスをブロックしているファイアウォールがないことを確認します。詳しくは、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。

- Lenovo Warranty データベース (ワールドワイド) - https://ibase.lenovo.com/POIRequest.aspx

- Lenovo Warranty Web サービス - http://supportapi.lenovo.com/warranty/ または https://supportapi.lenovo.com/warranty/

注：

- 保証サポートは現在、中国のユーザー向けにはサポートされていません。
- 保証はシャーシに対してリストされていますが、対応する Chassis Management Module (CMM) ではありません。

このタスクについて

保証情報は、保証のあるデバイスについては毎週取得され、保証のないデバイスについては毎日取得されます。

手順

保証情報を表示するには、「**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「**保証**」をクリックして「保証」カードを表示します。

終了後

「保証」カードから、以下の操作を実行できます。

- 管理対象デバイスの保証の有効期限について通知を受け取るには、「**保証設定の構成**」アイコン ( ) をクリックして構成します。以下の設定を構成できます。
  - デバイス保証の有効期限が来る前にアラートを生成する機能を有効にします。
  - 保証の有効期限が来る何日前にアラートを生成するかを設定します。
- 「**ステータス**」列のリンクをクリックして、特定のデバイスの保証情報 (ある場合) を Lenovo サポート Web サイトで検索します。
- 「**すべての操作 ➔ レポート・フォワーダーの追加**」をクリックして、反復ベースの保証に関するレポートを 1 つ以上のメール・アドレスに転送します。レポートは、現在テーブルに適用されているデータ・フィルターを使用して送信されます。表示および非表示されたテーブルのすべての列がレポートに含まれます。
- 「**レポート・フォワーダーに追加**」アイコン ( ) をクリックして、テーブルに現在適用されているデータ・フィルターを使用して、特定のレポート・フォワーダーに保証レポートを追加します。レポート・フォワーダーに保証レポートが既に含まれている場合、現在のデータ・フィルターを使用するためにレポートが更新されます。