Lenovo

Lenovo XClarity Administrator

問題判別ガイド

バージョン 4.3

注

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

第 4 版 (2025 4 月)

© Copyright Lenovo 2015, 2025.
制限付き権利に関する通知: データまたはソフトウェアが米国一般調達局 (GSA: General Services Administration) 契約に準じて提供される場合、使用、複製、または開示は契約番号 GS-35F-05925 に規定された制限に従うものとします。

目次

目次 i

変更の要約 v

第 1 章 . ヘルプおよび技術サポートの入手 1

第 2 章 . アラート、イベント、ジョブの表示 3

デバイスを保守モードにする 3
アラートの使用 4
アクティブなアラートの表示 4
アラートの除外 8
アラートの解決 9
アラートの確認 10
イベントの使用 10
イベント・ログでのイベントの監視 10
監視ログでのイベントの監視 12
イベントの解決 14
イベントの除外 14
イベントの転送 16
ジョブの操作 49
ジョブの監視 49
ジョブのスケジューリング 52
ジョブに対する解決策とコメントの追加 . . 55

第 3 章 . サービスおよびサポートの操作 57

Lenovo からの Bulletin の受け取り 57
保証情報の表示 58
自動問題通知のセットアップ 59
Lenovo サポートへの自動問題通知 (コール・ホーム) のセットアップ 60
Lenovo アップロード・ファシリティーへの自動問題通知のセットアップ 65
優先サービス・プロバイダーへの自動問題通知のセットアップ 69
サービス・リカバリー・パスワードの変更 . . . 72
サービス・ファイルの検査 72
特定のデバイスのサポート連絡先の定義 73
デバイスのサービス・データの収集とダウンロード 73
Lenovo XClarity Administrator サービス・ファイルの収集とダウンロード 75
応答しない Lenovo XClarity Administrator のサービス・ファイルの収集とダウンロード 77
ハードウェアの問題に関するサービス要求を Lenovo サポート・センターに送信します 78
XClarity Administrator の問題の報告 80
オープン・サービス・チケットへのサービス・ファイルの付加 82
サービス・チケットとステータスの表示 83
Lenovo サポートへのサービス・ファイルの転送 . 84
管理サーバー・ログ設定の構成 85
すべての管理対象デバイスでのコール・ホームの再有効化 86
Lenovo への定期的なデータの送信 86
サンプル使用データ 88
サンプル・ハードウェア・データ 91

第 4 章 . ディスク・スペースの管理 . 107

第 5 章 . 検出および管理に関する問題 111

デバイスを検出できない 111
デバイスを管理できない 112
SSL/TSL 証明書が無効なため、ストレージ・デバイスを管理できない 114
SSL/TSL 証明書が無効なため、スイッチを管理できない 115
背面 LED カードまたはミッドプレーン・アセンブリーを交換した後、管理対象 Flex System シャーシの接続をリカバリーできない 115
システム・ボードを交換した後、管理対象サーバーの接続性をリカバリーできない 116
サーバーを管理解除した後、encapsulation が無効にならない 116
計算ノードを管理した後に、ユーザー・インターフェースに表示されない 117
サーバーの電源状態が正しくない 117

第 6 章 . インストール、削除、更新、およびデータ移行に関する問題 . . . 119

XClarity Administrator を Red Hat KVM にインストールする場合、ビデオ出力が表示されない . . 119
アダプターの変更が認識されない 119
初期セットアップ中に Web ブラウザーで初期セットアップ・ウィザードを開くことができない . . 119
Lenovo XClarity Administrator デプロイメントが予期せず失敗する 119
Lenovo XClarity Administrator の更新に失敗する . 120

第 7 章 . 接続の問題 121

Lenovo XClarity Administrator にアクセスできない 121
Safari ブラウザーを使用して Lenovo XClarity Administrator に接続できない 121
ログインできない 121

© Copyright Lenovo 2015, 2025

Lenovo XClarity Administrator にログインできない 121
ローカル・リカバリーまたはスーパーバイザー・ユーザーのパスワードを忘れた . . . 122
管理対象 CMM に直接ログインできない . . 125
管理コントローラーに直接ログインできない 125
管理対象 Flex Power System サーバーにログインできない 125
デバイスへの接続が突然失われる. 126

第 8 章 . Lenovo XClarity Administrator 構成の問題. 127
外部 LDAP のセットアップの問題. 127
ユーザーにサーバーを構成するための十分な許可がない 127
Features on Demand アクティベーションの問題 . . 127
VMware による警告、VMXNET 3 ドライバーはサポートされていません 127

第 9 章 . パフォーマンスの問題 . . . 129
Lenovo XClarity Administrator パフォーマンスの問題. 129
ネットワーク・パフォーマンスに関する問題 . . 129

第 10 章 . セキュリティーの問題 . . 131
SSL 証明書を信頼できない 131
サーバー証明書の検証に失敗する. 131
Samba および Apache の脆弱性 132

第 11 章 . バックアップと復元の問題に関するトラブルシューティング . . . 135
バックアップ・プロセスが管理サーバーの再起動中にハングしているように見える. 135
XClarity Administrator ウィンドウは、バックアップ時に更新後に空白になります。. 135

第 12 章 . イベントの監視および転送の問題 137
イベントが転送されない 137

第 13 章 . デバイス管理に関する問題 139
フリーズしたドライブのドライブ・データを安全に消去できない 139
SATA SDD ボリュームが Marvel RAID に接続されている場合、安全に消去できない. 139
カードの追加または交換後にインベントリー・データが最新でない 139

第 14 章 . サーバー構成の問題. . . . 141
既存のサーバーからパターンを作成するときにエラーが発生する 141
パターンをデバイスにデプロイするときに、アクティベーション・エラーが発生する. 141
無効な構成がスイッチにデプロイされる 142

第 15 章 . ファームウェア更新とリポジトリーの問題 143
Lenovo リポジトリーに接続できませんでした . . 143
ファームウェア更新は成功したが、「適用/アクティブ化」ページに更新後のファームウェア・バージョンが表示されない 143
デバイスのファームウェアを更新できません . . 143
CMM ファームウェア更新がハングアップする . 143
ファームウェアは最新だが、コンプライアンス・チェックが失敗する 144
Flex System スイッチに対するファームウェア更新が予期せず失敗する 144
Flex スイッチに対するファームウェア更新が失敗し、「ファームウェアのダウンロード操作に失敗しました」というエラー・メッセージが表示されました。 144
Flex スイッチに対するファームウェア更新が失敗し、「DCSS_RC_CDT_FAIL」を示すエラー・メッセージが表示される. 145
Flex スイッチに対するファームウェア更新が失敗し、「タイムアウト」を示すエラー・メッセージが表示される。. 145
Flex スイッチに対するファームウェア更新が失敗し、「同じファームウェア・バージョンをダウンロードすることはできません。別のファームウェアをダウンロードしてください」というエラー・メッセージが表示される。」. 145
Flex スイッチに対するファームウェア更新が失敗し、ホストへのアクセスが失敗したことを示すエラー・メッセージが表示される . . 146
Flex スイッチに対するファームウェア更新が失敗し、「ファイルが存在しない」というエラー・メッセージが表示される. 146
Flex スイッチに対するファームウェア更新が失敗し、「フラッシュがエラーで終了」というエラー・メッセージが表示される 146
EN6131 40 Gb イーサネット・スイッチまたは IB6131 InfiniBand スイッチに対するファームウェア更新が予期せず失敗する. 146
Lenovo EN4091 パススルー・モジュールに対するファームウェア更新が失敗する 147
Flex System スイッチに対するファームウェア更新が失敗し、「ホスト鍵認証に失敗」したことを示すエラー・メッセージが表示される。. 147
更新の実行時にシステムが保守モードに入らない. 147
オペレーティング・システムからサーバーを再起動すると、保守モードがアクティブ化されない. 148
Red Hat Enterprise Linux (RHEL) を実行するサーバーが再起動しない 148

第 16 章 . OS デバイス・ドライバー更新とリポジトリーの問題 149

Lenovo サポート Web サイトに接続してデバイス・ドライバーの更新をダウンロードできない 149
サーバーでデバイス・ドライバーを更新できない 149

第 17 章 . オペレーティング・システム・デプロイメントに関する問題 . . 151
OS デプロイメント時に問題を報告しているステータス 151
オペレーティング・システムをデプロイできない 151
ファイルを OS イメージ・リポジトリーにインポートできない 152
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 153
OS インストーラーで ThinkServer サーバーをブートできない 154
VMware ESXi デプロイメントの問題 154
VMware デプロイメントによりシステムのハングまたは再起動が発生する 154
VMware デプロイメントがディスク・エラーで失敗する 154
オペレーティング・システムがブートせず ThinkServer サーバーへの ESXi のデプロイメントが完了しない 155
Red Hat および SUSE Linux のデプロイメントに関する問題 156
静的 IP を使用して Redhat 6.x をラックベース・サーバーにデプロイできない 156
ドライバーが欠落しているために OS デプロイメントが失敗する 156
Microsoft Windows のデプロイメントの問題 . . . 156
接続されたディスク・ドライブに既存のシステム・パーティションがあるため、OS デプロイメントが失敗する 156

第 18 章 . リモート制御に関する問題 159
リモート制御セッションが開始されない 159
リモート制御セッションがログイン後にハングアップする 159
サーバーに接続できない 160
リモート制御セッションの開始後に Flex System スイッチと通信できない 160
シングルユーザー・モードでサーバーに接続できない 160
リモート制御でサーバーに接続できるがビデオを使用できない 161
新しいセッションを追加するためのリストにサーバーが表示されない 161
サーバーの状態がリモート制御セッションと Lenovo XClarity Administrator とで一致しない . . 161
ドライブまたはイメージをサーバーにマウントできない 162
マウント可能なリモート・メディア・デバイスのリストにストレージ・メディアのオプションが表示されない 162
電源操作を実行できない 162
Flex System x280 X6、x480 X6、x880 X6 サーバーへの接続時にビデオが使用できない 162

第 19 章 . ユーザー・インターフェースの問題 165
メニュー項目、ツールバー・アイコン、およびボタンが無効になっています (淡色表示) 165
複数のタブが開いていると Web ブラウザーが応答しなくなる 165
JSON 応答の失敗、解析エラー、他の予期しないエラー 165
ユーザー・インターフェースで、希望の言語が使用されない 165
読み込みが低速または応答していないように見える、更新に長い時間がかかる、描画が適切でない 166
予期しないデータ損失 166
ラック・ビューでデバイスの場所の変更が反映されない 166

© Copyright Lenovo 2015, 2025

変更の要約

Lenovo XClarity Administrator 管理ソフトウェアの以下のリリースでは、新しいハードウェア、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。

このバージョンの、問題の判別および解決のための機能拡張はありません。

このバージョンでは、問題の判別および解決に以下の機能拡張がサポートされています。

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

機能	説明
サービスおよびサポート	tcpdump API のサポートは、カスタマー・エンゲージメント中の Lenovo サポートを支援するために追加されました。

© Copyright Lenovo 2015, 2025

第 1 章　ヘルプおよび技術サポートの入手

Lenovo XClarity Administrator に関するヘルプ、サービス、技術支援が必要な場合は、Lenovo がさまざまな形で提供している支援をご利用いただけます。

始める前に

必要に応じて、最適なサポートを得るための連絡先の電話番号、リソース、ガイダンスの一般的な情報については、Lenovo サポート計画 – ソフトウェア Web ページを参照してください。

手順

- 質問し、回答を検索するには、XClarity Administrator タイトル・バーで、ユーザー・アクション・メニュー (

) をクリックして、「**フォーラムにアクセス**」をクリックするか、Lenovo XClarity Community フォーラム Web サイト に直接移動します。
- XClarity Administrator に関するアイデアを送信するには、XClarity Administrator タイトル・バーで、ユーザー・アクション・メニュー (

) をクリックして、「**アイデアを送信**」をクリックするか、Lenovo XClarity アイディエーション Web サイト に直接移動します。
- イベント・ログを確認し、推奨処置に従ってイベント・コードを解決します (イベントの使用を参照)。
- 識別可能な症状がある問題の解決策を見つけ、推奨アクションに従ってすべての問題を解決します。最新のトラブルシューティング手順については、XClarity Administrator オンライン・ドキュメントのトラブルシューティングを参照してください。
- XClarity Administrator で問題が起こったときにお客様が問題解決に使用できるヒントや手法を、Lenovo データセンターサポート Web サイト で確認してください。これらの*技術ヒント*では、XClarity Administrator の動作に関する問題を回避する手順について説明しています。

  ご使用のサーバーで利用可能な技術ヒントを検索するには:

  1. Lenovo データセンターサポート Web サイト にアクセスします。
  2. 「**検索**」フィールドで、「XClarity Administrator」を入力します。
  3. 「**Top Articles (トップ記事)**」セクションで「**View All (すべて表示)**」をクリックしてすべてのヒントを表示するか、または「**Search (検索)**」フィールドにキーワードを入力して特定のヒントを検索します。

     ヒント: 「**Relevance (関連性)**」、「**Popularity (人気)**」、または「**Newest (最新)**」の順にリストをソートできます。
- 問題が管理対象デバイスにおけるハードウェアまたはベースボード管理コントローラーの問題の場合、問題と推奨アクションについてはそのデバイスに付属しているドキュメントを参照してください。
  - ThinkAgile アプライアンスの場合は、ThinkAgile オンライン・ドキュメントを参照してください。
  - サーバーやネットワーク・デバイスを含む ThinkSystem 製品の場合は、ThinkSystem オンライン・ドキュメントを参照してください。
  - コンバージド、System x、および RackSwitch 製品 (サーバー、ラック装着スイッチなど) の場合、System x オンライン・ドキュメントを参照してください。
  - NeXtScale 製品の場合は、NeXtScale オンライン・ドキュメントを参照してください。
  - Flex System 製品 (シャーシ、スイッチ、ストレージ・デバイス、計算ノードなど) の場合、Lenovo Flex System オンライン・ドキュメントを参照してください。
- 問題がある場合、XClarity Administrator管理サーバーでは、サービス・チケットを手動で送信できます (XClarity Administrator の問題の報告 を参照)。

© Copyright Lenovo 2015, 2025

- 問題が解決しない場合で、サポートライン契約、保守契約をお持ちであるか、保証対象である方は、オンラインサービス要求を送信してください。

  注：Lenovo XClarity Pro は、サービスおよびサポートに資格を提供し、XClarity Administrator の全機能有効化ライセンスも提供します。Lenovo XClarity Pro の購入について詳しくは、Lenovo 担当員または認定ビジネス・パートナーに連絡してください。

  サービス要求を送信すると、Lenovo サポートが迅速に、そして効果的に関連情報を使用できるようになることで、お客様の問題の解決策を判別するプロセスが開始されます。Lenovo サービス技術員は、お客様が要求を完了および送信するとすぐに、解決策の作業を開始します。

  注：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発生すると、問題を解決できるように XClarity Administrator 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 にサービス・ファイルが転送されます。コール・ホームの有効化については、Lenovo サポートへの自動問題通知 (コール・ホーム) のセットアップを参照してください。

  コール・ホームが有効になっていない場合、サービス要求とサービス・ファイルを手動で送信できます (ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照)。

  注：IBM は、XClarity Administrator に対する Lenovo の優先サービス・プロバイダーです。一部のデバイスのサービス・リクエストは、援助のために IBM に転送されます。

- Lenovo サポート・ラインを使用すると、ご使用の Lenovo 製品の使用法、構成、およびソフトウェアの問題について、技術的な援助を有料で受けることができます。

  各地域およびフリー・ダイヤルのサポート電話番号については、サポート電話番号リスト Web サイトを参照してください。地域で見つかった番号にダイヤルするか、または Web ページの「**連絡先**」をクリックして、サポートを受けることができます。

  重大度 1 の問題については、いつでも (1 日 24 時間、週 7 日) サポートを利用できます。その他のすべての重大度について、それぞれの地域の作業時間と言語が Web ページに示されます。

  中国での製品サポートへのお問い合わせについては、Lenovo サービス - 中国 Web サイトを参照してください。または、400-106-8888 に電話して製品サポートを依頼してください。電話によるサポートは、月曜から金曜までの午前 9 時から午後 6 時までご利用いただけます。

第 2 章　アラート、イベント、ジョブの表示

Lenovo XClarity Administrator には、管理対象デバイスのステータスの監視に使用できる方法がいくつかあります。

- アラート・リストには、XClarity Administratorまたは管理対象デバイスで見つかった問題がリアルタイムで表示されます。
- イベント・ログと監査ログには、XClarity Administrator によって識別されたユーザー操作とイベント・アクションの履歴が表示されます。
- ジョブ・ログには、1 台以上の管理対象デバイスに対して実行された長期間の実行タスクのリストが含まれます。

デバイスを保守モードにする

デバイスを保守モードにすると、Lenovo XClarity Administrator 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からそのデバイスのすべてのイベントとアラートを除外します。除外したアラートはログに記録されますが、ビューには表示されません。

このタスクについて

デバイスが保守の間にそのデバイスに対して生成されたイベントとアラートのみ除外されます。デバイスが保守モードになる前に生成されたイベントとアラートが表示されます。

管理対象デバイスを保守状態にした後でサービス状態に戻ると、そのデバイスのインベントリーが古くなる可能性があります。異常がある場合は、デバイスを選択し、「**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**」の順にクリックしてデバイスページからインベントリーを手動で更新します。

手順

デバイスを保守モードにするには、以下のいずれかの手順を実行してください。

ステップ 1. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**エンドポイント・アクション**」をクリックして、「エンドポイント・アクション」ページを表示します。

ステップ 3. 保守モードにするデバイスを 1 台以上選択します。

ステップ 4. 「**操作**」 ➡ 「**保守**」をクリックして、「保守モード」ダイアログを表示します。

ステップ 5. デバイスの保守モードを解除して、サービスを再開する日付と時刻を選択します。

デバイスを元の状態に戻す必要がない場合は、「**無制限**」を選択します。

ステップ 6. 「**確認**」をクリックします。そのデバイスのテーブルの「保守」列が「はい」に変わります。

終了後

デバイスの保守が終了したら、デバイスを選択し、「**操作**」 ➡ 「**保守**」の順にクリックしてから、ダイアログの「**保守をオフにする**」をクリックしてデバイスを再び稼働させることができます。デバイスを手動でサービス・モードに戻さなかった場合は、指定した終了日と時間が経過した後で、自動的にサービス・モードになります。

© Copyright Lenovo 2015, 2025

アラートの使用

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管理の状態です。Lenovo XClarity Administrator は、管理対象デバイスを非同期的にポーリングし、それらのデバイス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

詳細: XClarity Administrator: 監視

通常、アラートが受信されると、対応するイベントがイベント・ログに保存されます。アラートが受信されるだけで、対応するイベントがイベント・ログに (ログの先頭から上書きされる場合でも) 保存されない場合があります。たとえば、シャーシが管理対象になる前に発生したイベントはイベント・ログに表示されません。ただし、シャーシが管理対象になった後は Lenovo XClarity Administrator が CMM をポーリングするため、シャーシに関するアラートはアラート・ログに表示されます。

アクティブなアラートの表示

ハードウェアと管理に関するすべてのアクティブなアラートのリストを表示できます。

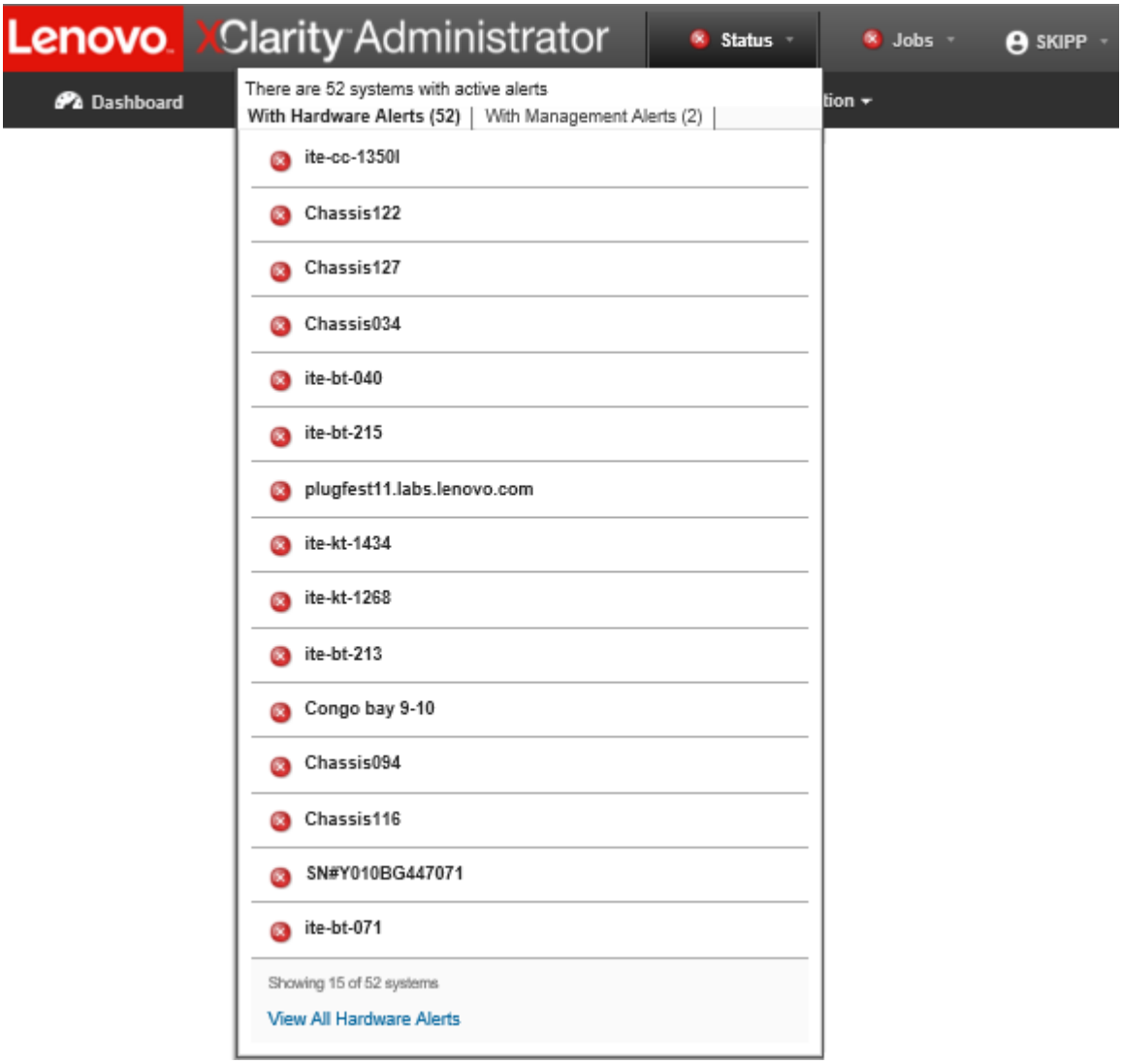
このタスクについて

注：Lenovo XClarity Administrator のロケールが別の言語に設定されている場合でも、Lenovo Storage デバイスのアラートは英語でのみ表示されます。必要に応じて、外部翻訳システムを使用してメッセージを翻訳してください。

手順

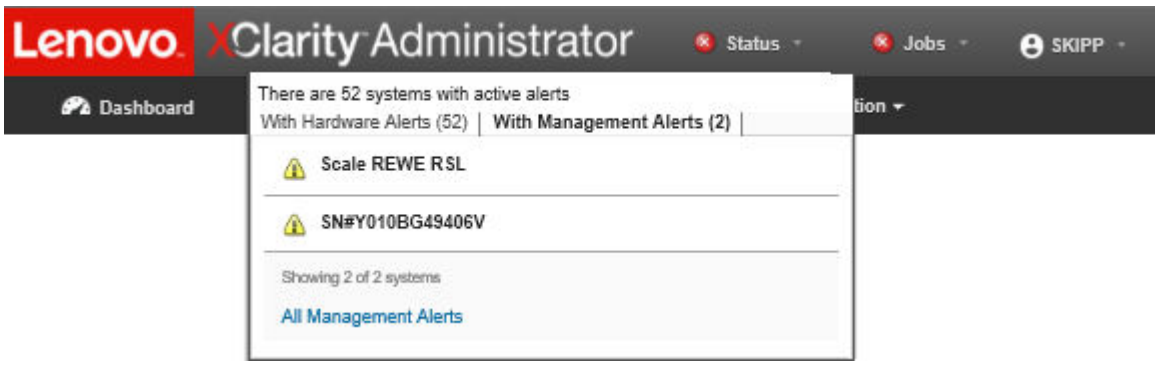
アクティブなアラートを表示するには、以下のいずれかの手順を実行します。

- 管理対象デバイスに関するアラート (*ハードウェア・アラート*と呼ばれる) のみを表示するには:
  1. XClarity Administrator タイトル・バーで、「**ステータス**」プルダウンをクリックして、ハードウェアと管理に関するアラートの要約を表示します。
  2. 「**ハードウェア・アラートあり**」タブをクリックして、各管理対象デバイスに関するアラートの要約を表示します。



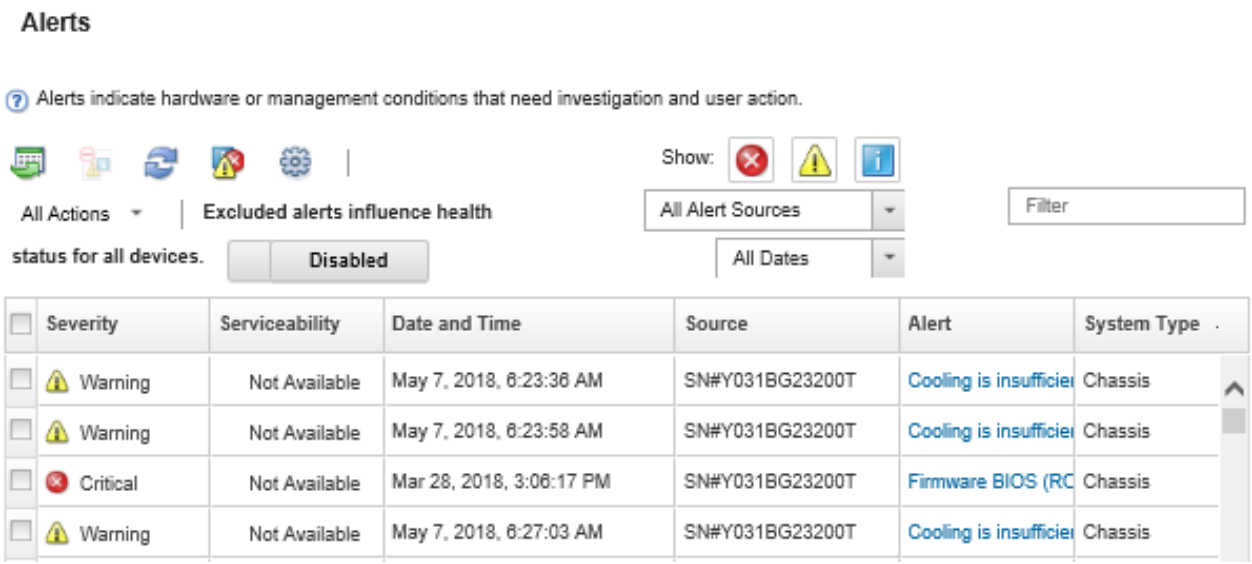
3. タブに表示されているデバイスの上にカーソルを置いて、そのデバイスのアラートのリストを表示します。
4. 「**すべてのハードウェア・アラート**」リンクをクリックすると、「アラート」ページが開いて、すべてのハードウェア・アラートのフィルタリングされたリストが表示されます。

- XClarity Administrator からのアラート (*管理アラート*と呼ばれる) のみを表示するには:
  1. XClarity Administrator タイトル・バーで、「**ステータス**」プルダウンをクリックして、ハードウェアと管理に関するアラートの要約を表示します。
  2. 「**管理アラートあり**」タブをクリックして、すべての CMM と XClarity Administrator のアラートの要約を表示します。



3. タブに表示されているデバイスの上にカーソルを置いて、そのデバイスのアラートのリストを表示します。
4. 「**すべての管理アラート**」リンクをクリックすると、「アラート」ページが開いて、CMM と XClarity Administrator からのすべてのアラートのフィルタリングされたリストが表示されます。

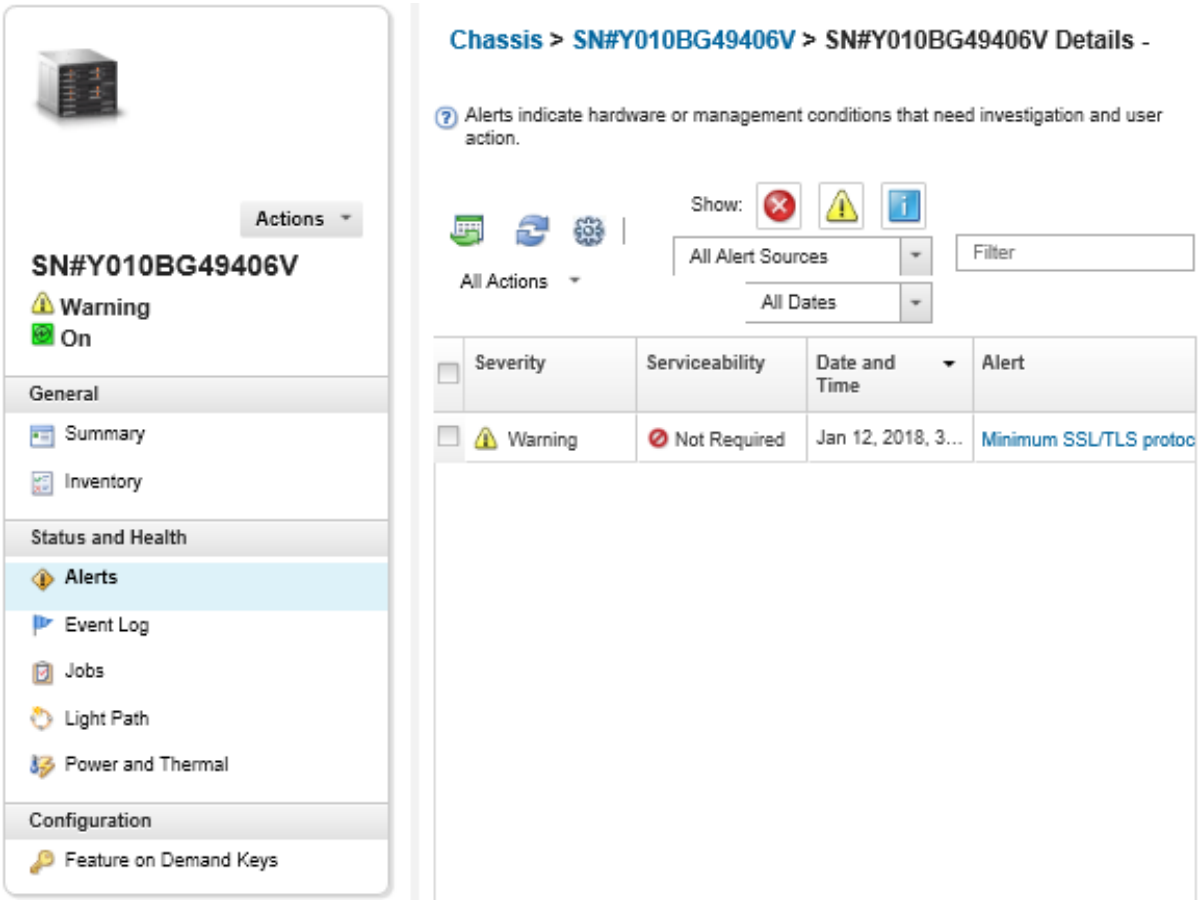
- XClarity Administrator ですべてのアラートを表示するには、XClarity Administrator メニュー・バーで「**監視**」 → 「**アラート**」をクリックします。「アラート」ページが開いて、すべてのアクティブなアラートのリストが表示されます。



- 特定のデバイスに関するアラートを表示するには:
  1. XClarity Administrator メニュー・バーで、「**ハードウェア**」をクリックして、デバイスのタイプをクリックします。ページが開いて、そのタイプのすべての管理対象デバイスがテーブル・ビューで表示されます。たとえば、「**ハードウェア**」 → 「**サーバー**」をクリックすると、「サーバー」ページが表示されます。
  2. 特定のデバイスをクリックして、そのデバイスの「要約」ページを表示します。
  3. 「ステータスと正常性」で、「**アラート**」をクリックすると、そのデバイスに関するすべてのアラートのリストが表示されます。

     注：次の場合は、保守容易性列に「使用不可」と表示されることがあります。

     – デバイスのアラートが、XClarity Administrator によって管理される前に発生した
     – イベント・ログが最大数に達したため、そのアラートに関連付けられたイベントがこれ以上イベント・ログに存在しない



結果

「アラート」ページでは、以下の操作を実行できます。

- アラートのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。

  ヒント: 新しいアラートが検出された場合、アラート・ログは 30 秒ごとに自動的に更新されます。
- 特定のアラートに関する情報 (説明、ユーザー操作など)、アラートの発生元であるデバイスに関する情報 (世界固有識別子) を表示する。「**アラート**」列のリンクをクリックします。ダイアログにアラート・プロパティと詳細に関する情報が表示されます。

  注：「**詳細**」タブの下にアラートの説明やリカバリー操作が表示されない場合は、Lenovo Flex System オンライン・ドキュメント に移動し、アラート ID (`FQXHMSE0004G` など) を検索します。この Web サイトでは常に最新の情報が提供されます。
- デフォルトでは、除外アラートは、管理対象デバイスのヘルス状況に影響を及ぼしません。「アラート」ページから、トグルをクリックし、「**除外アラートによりすべてのデバイスのヘルス状況に影響を与える**」を有効にすることで、除外アラートにより管理対象デバイスのヘルス状況に影響を与えることを許可できます。
- しきい値設定をセットして、ThinkSystem や ThinkServer サーバーの寿命などの特定の値が警告レベルまたはクリティカル・レベルを超過したときにアラートとイベントを発生させることができます (XClarity Administrator オンライン・ドキュメントのアラートおよびイベント生成のしきい値設定の 設定を参照)。
- アラート・ログをエクスポートする。「**CSV としてエクスポート**」アイコン ( ) をクリックします。

  注：エクスポートしたログ内のタイムスタンプには、Web ブラウザーに指定された現地時間が使用されます。

- 特定のアラートを、アラートが表示されているすべてのページから除外する (アラートの除外を参照)。
- 現在のページに表示されているアラートのリストを絞り込む。
  - 特定の重大度のアラートを表示/非表示にする。以下のいずれかのアイコンをクリックします。
    - 「**クリティカル・アラート**」アイコン ( )
    - 「**警告アラート**」アイコン ( )
    - 「**通知アラート**」アイコン ( )
  - 特定の発生元からのアラートのみを表示する。ドロップダウン・リストから、以下のいずれかのオプションを選択できます。
    - すべてのアラート・ソース
    - ハードウェア・イベント
    - 管理イベント
    - サービス・センター・イベント
    - 顧客による保守が可能なイベント
    - 保守できないイベント
  - 特定の日付と時刻のアラートのみを表示する。ドロップダウン・リストから、以下のいずれかのオプションを選択できます。
    - すべての日付
    - 直前の 2 時間
    - 直前の 24 時間
    - 過去 1 週間
    - 過去 1 カ月
  - 「**フィルター**」フィールドにテキストを入力して、特定のテキストを含むアラートのみを表示する。
  - 列の見出しをクリックして、アラートを列でソートする。

アラートの除外

不要なアラートがある場合、そのアラートは、アラートが表示されているすべてのページから除外できます。除外したアラートはログには残りますが、ログ・ビュー、デバイス・ステータスなど、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。

デバイスを保守モードにして、そのデバイスに関するすべてのイベントとアラートを除外することができます (デバイスを保守モードにするを参照)。

制限: 管理権限を持つユーザーのみがアラートを除外および復元できます。

重要：ステータス・アラートを除外した場合、デバイス・サマリーおよび詳細ページのデバイス・ステータスは変わりません。

手順アラート・ログからアラートを除外するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**監視**」 → 「**アラート**」をクリックします。「アラート」ページが表示されます。

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

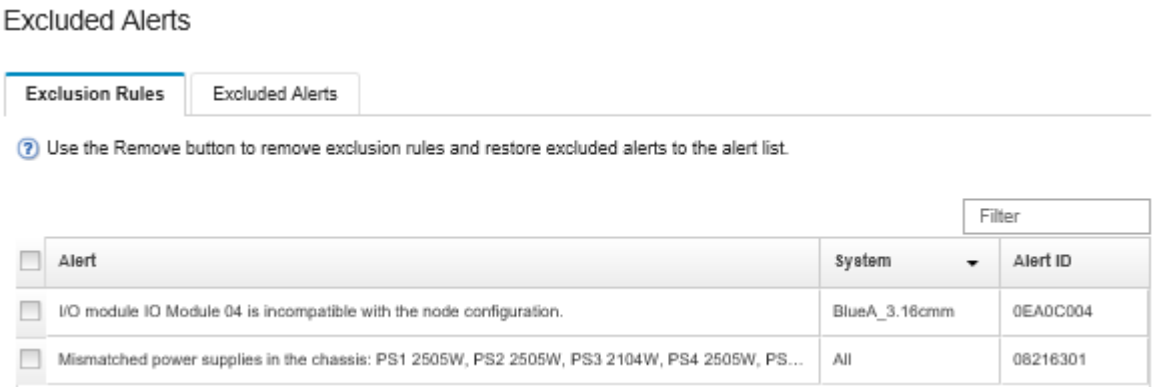
ステップ 3. 以下のどちらかを選択します。
- 「**選択したアラートをすべてのシステムから除外する**」。選択したアラートをすべての管理対象デバイスから除外します。

- 「**選択済みインスタンスの範囲に含まれるシステムのアラートのみを除外する**」。選択したアラートが該当する管理対象デバイスから、選択したアラートを除外します。

ステップ 4. 「**保存**」をクリックします。

終了後

アラートを除外すると、Lenovo XClarity Administrator 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。アラート・ページで除外ルールと除外アラートのリストを表示するには、「**除外済み/確認済みアラートの表示**」アイコン ( ) をクリックします。「除外済み/確認済みアラート」ダイアログで、「**除外ルール**」タブをクリックすると、除外ルールが表示されます。「**除外アラート**」タブをクリックすると、除外されたアラートの一覧が表示されます。



デフォルトでは、除外アラートは、管理対象デバイスのヘルス状況に影響を及ぼしません。「アラート」ページから、トグルをクリックし、「**除外済み/確認済みアラートの表示**」を有効にすることで、除外済みアラートは管理対象デバイスのヘルス状況に影響を変更することができます。

除外されたアラートをアラート・ログに復元するには、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、「**除外アラートの表示**」アイコン ( ) をクリックして「除外アラート」ダイアログを表示し、復元する除外ルールまたは除外アラートを選択して、「**削除**」をクリックします。

アラートの解決

Lenovo XClarity Administrator は、アラートを解決するために実行する適切なアクションに関する情報を提供します。

手順以下の手順を実行して、アラートを解決します。

ステップ 1. Lenovo XClarity Administrator メニュー・バーで、「**監視**」 → **アラート**をクリックして、「アラート」ページを表示します。

ステップ 2. アラート・ログでアラートを見つけます。

ステップ 3. 「**アラート**」列のリンクをクリックして、アラートに関する情報 (説明やリカバリー操作など) や、アラート発生元のデバイスに関するプロパティ (世界固有識別子など) を表示します。

ステップ 4. 「**詳細**」タブの下に示されているリカバリー操作を実行して、アラートを解決します。次の例は、イベントのリカバリー操作を説明したものです。

参照されている管理対象シャーシのセキュリティー・ポリシー設定を管理サーバーの現在のセキュリティー・ポリシーに合わせて変更してください。

シャーシのセキュリティー・ポリシーを変更するには、Chassis Management Module (CMM) でコマンド・ライン・インターフェース・セッションを開き、以下のいずれかのコマンドを実行します。

- セキュリティー・ポリシー・レベルを「Secure」に変更するには:
  `security -p secure -T mm[p]`
- セキュリティー・ポリシー・レベルを「Legacy」に変更するには:
  `security -p legacy -T mm[p]`

注：「**詳細**」タブの下にアラートの説明やリカバリー操作が表示されない場合は、Lenovo Flex System オンライン・ドキュメント に移動し、アラート ID (FQXHMSE0004G など) を検索します。この Web サイトでは常に最新の情報が提供されます。

推奨処置に従っても問題が解決しない場合は、Lenovo サポートに連絡してください。

アラートの確認

アクティブ・アラートが確認されると、アラートが表示されるページに一覧されますが、該当するデバイスの重大度ステータスには影響しません。

手順

以下の手順を実行して、アラートを確認します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**監視**」 → 「**アラート**」をクリックします。「アラート」ページが表示されます。

ステップ 2. 確認するアラートを選択します。

ステップ 3. 「**アラートの確認**」アイコン ( ) をクリックし ます。

終了後

- 「**除外済み/確認済みアラートの表示**」アイコン ( ) をクリックして「除外済み/確認済みアラート」ダイアログを表示し、「**確認済みアラート**」タブをクリックすると、「アラート」ページで確認済みアラートのリストを表示できます。
- 「**除外済み/確認済みアラートの表示**」アイコン ( ) をクリックして「除外済み/確認済みアラート」ダイアログを表示し、「**確認済みアラート**」タブをクリックし、アラートを選択し、「**確認の取り消し**」アイコン( )をクリックすると、有効なアラートの確認を取り消すことができます。

イベントの使用

Lenovo XClarity Administrator からイベント・ログと監査ログにアクセスできます。

このタスクについて

詳細: XClarity Administrator: 監視

*イベント・ログ*には、すべてのハードウェア/管理イベントの履歴が記録されています。

*監査ログ*には、Lenovo XClarity Administrator へのログオン、新しいユーザーの作成、ユーザー・パスワードの変更など、ユーザー操作の履歴が記録されています。監査ログを使用すると、IT システムでの認証や制御を追跡および文書化できます。

イベント・ログでのイベントの監視

*イベント・ログ*には、すべてのハードウェア/管理イベントの履歴が記録されています。

このタスクについて

イベント・ログには、通知イベントと通知以外のイベントが含まれています。それぞれのイベントの数は、イベント・ログ内の上限である 50,000 件に達するまでは変化します。この時点で、最大 25,000 件の通

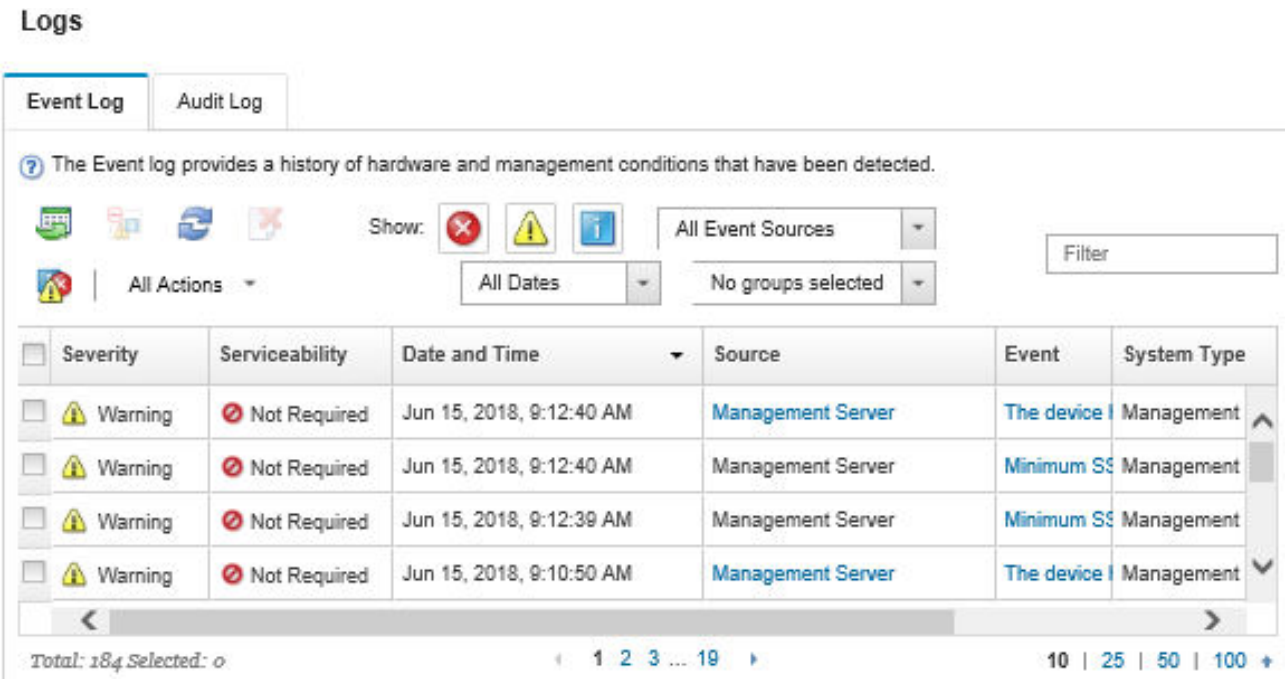
知イベントおよび最大 25,000 件の通知以外のイベントがあります。たとえば、イベント・ログにイベントが含まれていない状態で、20,000 件の通知イベントと 30,000 件の通知以外のイベントを受信したとします。次のイベントを受信すると、通知以外のイベントの方が古くても、最も古い通知イベントが破棄されます。最終的には、ログは、それぞれのイベント・タイプが 25,000 件ずつになるように相殺されます。

Lenovo XClarity Administrator は、イベント・ログが最小サイズの 80% に達するとイベントを送出し、イベントと監査ログの合計が最大サイズの 100% に達するとまた別のイベントを送出します。

ヒント: すべてのハードウェア/管理イベントの完全な記録を保持するには、イベント・ログをエクスポートしてください。イベント・ログをエクスポートするには、「**CSV としてエクスポート**」アイコン ( ) をクリックします。

手順

イベント・ログを表示するには、Lenovo XClarity Administrator メニュー・バーで「**監視**」 → 「**イベント・ログ**」をクリックし、「**イベント・ログ**」タブをクリックします。「イベント・ログ」ページが表示されます。



「**保守容易性**」列は、デバイスにサービスが必要かどうかを特定します。この列には次のいずれか 1 つの値が含まれる可能性があります。

- **必要なし**。サービスを必要としない通知イベントです。
- **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。

  特定のイベントの詳細を表示するには、「**イベント**」列のリンクをクリックします。イベント、イベントの詳細、およびリカバリー操作を送信したデバイスのプロパティに関する情報が示されたダイアログが表示されます。
- **サポート**。コール・ホーム が Lenovo XClarity Administrator で有効になっている場合、通常、イベントは Lenovo サポート・センター に送信されます。ただし、デバイスに対して同じイベント ID のオープン・サービス・チケットが既に存在する場合は除きます。

  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 XClarity Administrator オンライン・ドキュメントのサービス・チケットのオープンを参照)。

結果

「イベント・ログ」ページでは、以下の操作を実行できます。

- イベントのソースを表示するには、「**ソース**」列のリンクをクリックします。
- イベントのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。

  ヒント: 新しいイベントが検出された場合、イベント・ログは 30 秒ごとに自動的に更新されます。
- イベント・ログのすべてのイベントをクリアするには、「**すべての操作**」 → 「**イベント・ログをクリア**」を選択します。
- 特定のイベントの詳細を表示する。「**イベント**」列のリンクをクリックし、「**詳細**」タブをクリックします。
- イベント・ログをエクスポートする。「**CSV としてエクスポート**」アイコン ( ) をクリックします。

  注：エクスポートしたログ内のタイムスタンプには、Web ブラウザーに指定された現地時間が使用されます。
- 特定のイベントを、イベントが表示されているすべてのページから除外する (イベントの除外を参照)。
- 現在のページに表示されているハードウェアおよび管理イベントのリストを絞り込む。
  - 特定の重大度のイベントを表示/非表示にする。ドロップダウン・リストで以下のいずれかのアイコンをクリックします。
    - **クリティカル・イベント**・アイコン ( )
    - **警告イベント**・アイコン ( )
    - **通知イベント**・アイコン ( )
  - 特定の発生元からのイベントのみを表示する。ドロップダウン・リストから、以下のいずれかのオプションを選択できます。
    - すべてのアラート・ソース
    - ハードウェア・イベント
    - 管理イベント
    - 保守が可能なイベント
    - 顧客による保守が可能なイベント
    - 保守できないイベント
  - 特定の日付と時刻のイベントのみを表示する。以下のいずれかに対応するオプションを選択します。
    - すべての日付
    - 直前の 2 時間
    - 直前の 24 時間
    - 過去 1 週間
    - 過去 1 カ月
    - Custom

    「**カスタム**」を選択した場合、カスタマイズした開始日と現在の日付の間に発生したハードウェアおよび管理イベントをフィルターすることできます。
  - 「**フィルター**」フィールドにテキストを入力して、特定のテキストを含むイベントのみを表示する。
  - 列見出しをクリックして、イベントを列でソートする。

監視ログでのイベントの監視

*監査ログ*には、Lenovo XClarity Administrator へのログオン、新しいユーザーの作成、ユーザー・パスワードの変更など、ユーザー操作の履歴が記録されています。監査ログを使用すると、IT システムでの認証や制御を追跡および文書化できます。

このタスクについて

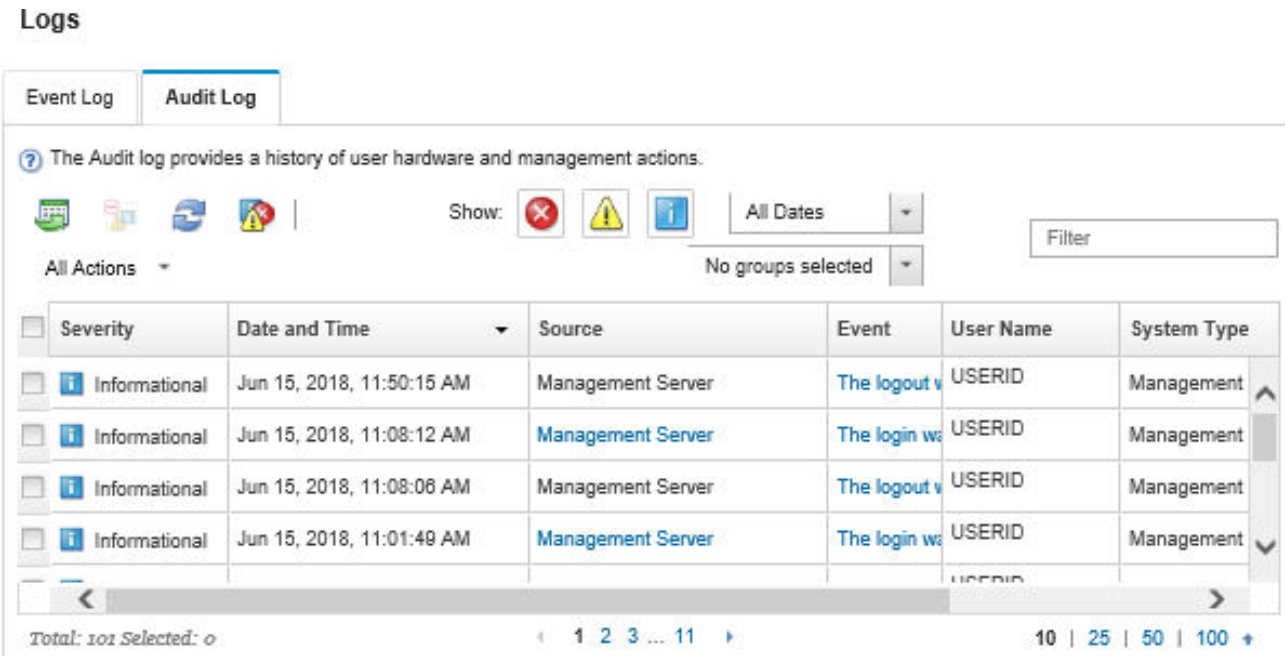
監査ログには、最大で 50,000 のイベントを含めることができます。最大サイズに達すると、そのログで最も古いイベントが廃棄され、新規イベントがログに追加されます。

XClarity Administrator は、監査ログが最大サイズの 80% に達するとイベントを送出し、イベントと監査ログの合計が最大サイズの 100% に達するとまた別のイベントを送出します。

ヒント: すべての監査イベントの完全な記録を保持するには、監査ログをエクスポートしてください。監査ログをエクスポートするには、「**CSV としてエクスポート**」アイコン ( ) をクリックします。

手順

監査ログを表示するには、XClarity Administrator メニュー・バーで「**監視**」 → 「**イベント・ログ**」を選択し、「**監査ログ**」タブをクリックします。「監査ログ」ページが表示されます。



特定の監査イベントの詳細を表示するには、「**イベント**」列のリンクをクリックします。イベント、イベントの詳細、およびリカバリー操作を送信したデバイスのプロパティに関する情報が示されたダイアログが表示されます。

結果

このページでは、以下の操作を実行できます。

- 監査イベントのソースを表示するには、「**ソース**」列のリンクをクリックします。
- 監査イベントのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。

  ヒント: 新しいイベントが検出された場合、イベント・ログは 30 秒ごとに自動的に更新されます。
- 特定の監査イベントの詳細を表示する。「**イベント**」列のリンクをクリックし、「**詳細**」タブをクリックします。
- 監査ログをエクスポートする。「**CSV としてエクスポート**」アイコン ( ) をクリックします。

  注：エクスポートしたログ内のタイムスタンプには、Web ブラウザーに指定された現地時間が使用されます。

- 特定の監査イベントを、イベントが表示されているすべてのページから除外する (イベントの除外を参照)。
- 現在のページに表示されている監査イベントのリストを絞り込む。
  - 特定の重大度のイベントを表示/非表示にする。以下のいずれかのアイコンをクリックします。
    - **クリティカル・イベント**・アイコン ( )
    - **警告イベント**・アイコン ( )
    - **通知イベント**・アイコン ( )
  - 特定の日付と時刻のイベントのみを表示する。ドロップダウン・リストから、以下のいずれかのオプションを選択できます。
    - すべての日付
    - 直前の 2 時間
    - 直前の 24 時間
    - 過去 1 週間
    - 過去 1 カ月
    - Custom

    「**カスタム**」を選択した場合、カスタマイズした開始日と現在の日付の間に発生したハードウェアおよび管理イベントをフィルターすることできます。
  - 「**フィルター**」フィールドにテキストを入力して、特定のテキストを含むイベントのみを表示する。
  - 列見出しをクリックして、イベントを列でソートする。

イベントの解決

Lenovo XClarity Administrator は、イベントを解決するために実行する適切なアクションに関する情報を提供します。

手順

以下の手順を実行して、イベントを解決します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**監視**」 → 「**イベント・ログ**」をクリックして「ログ」ページを表示します。

ステップ 2. 「**イベント・ログ**」タブをクリックします。

ステップ 3. イベント・ログでイベントを見つけます。

ステップ 4. 「**イベント**」列のリンクをクリックして、そのイベントに関する情報 (説明やリカバリー操作など) や、イベント発生元のデバイスに関する情報を表示します。

ステップ 5. 「**詳細**」タブをクリックします。

ステップ 6. 「**詳細**」タブに示されている回復手順を実行して、イベントを解決します。

注：イベントの説明や回復操作が表示されない場合は、Lenovo Flex System オンライン・ドキュメント に移動し、イベント・タイトルを検索します。この Web サイトでは常に最新の情報が提供されます。

推奨処置に従っても問題が解決しない場合は、Lenovo サポートに連絡してください。

イベントの除外

不要なイベントがある場合、そのイベントは、イベントが表示されているすべてのページから除外できます。除外したイベントはログには残りますが、イベン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。

デバイスを保守モードにすると、そのデバイスに関するすべてのイベントとアラートを除外することができます (デバイスを保守モードにするを参照)。

制限: 管理権限を持つユーザーのみがイベントを除外および復元できます。

手順

イベント・ログから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. Lenovo XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント・ログ**」をクリックして、「**イベント・ログ**」タブをクリックします。イベント・ログが表示されます。

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

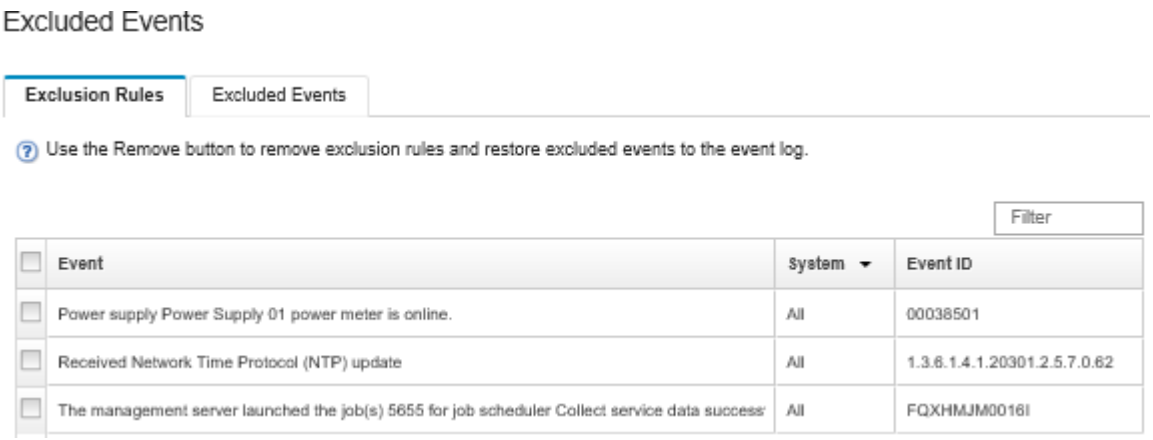
ステップ 3. 以下のどちらかを選択します。
- 「**選択したイベントをすべてのシステムから除外する**」。選択したイベントをすべての管理対象デバイスから除外します。
- 「**選択済みインスタンスの範囲に含まれるシステムのイベントのみを除外する**」。選択したイベントを、その適用先の管理対象デバイスから除外します。

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、Lenovo XClarity Administrator 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。

- 「ログ」ページから除外ルールと除外イベントのリストを表示するには、「**除外イベントの表示**」アイコン ( ) をクリックします。「除外イベント」ダイアログで、「**除外ルール**」タブをクリックすると、除外ルールが表示されます。「**除外イベント**」タブをクリックすると、除外イベントが表示されます。

- イベント・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、「**除外イベントの表示**」アイコン ( ) をクリックして「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、「**除外を削除**」をクリックします。
- 除外イベントのリストに含まれるサービス可能イベントが自動的に問題レポートを開かないようにするには、Lenovo XClarity Administrator メニュー・バーで 「**管理**」 → 「**サービスおよびサポート**」 をクリックして、「**サービス・フォワーダー**」タブをクリックし、「**除外イベント時に問題レポートを開きますか?**」という質問の隣にある「**いいえ**」を選択します。

イベントの転送

ハードウェア環境についてハードウェアのステータスと実行時の問題を集約して監視するために、モバイル・デバイスおよび運用環境内で接続されているアプリケーションにイベントが転送されるように、Lenovo XClarity Administrator を構成できます。

詳細: XClarity Administrator: 監視

Syslog、リモート SNMP マネージャー、メールまたは他のイベント・サービスへのイベント転送

ハードウェア環境についてハードウェアのステータスと実行時の問題を集約して監視するために、運用環境内で接続されているアプリケーションにイベントが転送されるように、Lenovo XClarity Administrator を構成できます。転送するイベントの範囲は、デバイス、イベント・クラス、イベントの重大度、コンポーネントに基づいて定義できます。

このタスクについて

Lenovo XClarity Administrator は、1 つ以上のデバイスに関するイベントを転送できます。監査イベントについては、すべての監査イベントを転送するか、いずれのイベントも転送しないかを選択できます。特定の監査イベントを転送することはできません。ハードウェア/管理イベントについては、1 つ以上の重大度 (重大、警告、情報) と 1 つ以上のコンポーネント (ディスク・ドライブ、プロセッサー、アダプターなど) に関するイベントを転送するように選択できます。

Lenovo XClarity Administrator は、イベント・フォワーダーを使用してイベントを転送します。*イベント・フォワーダー*の定義には、使用するプロトコル、受信者、監視するデバイス、転送するイベントに関する情報が含まれています。イベント・フォワーダーを作成して有効にした後、Lenovo XClarity Administrator によってフィルター基準に基づいた受信イベントの監視が開始されます。フィルター基準に一致するイベントが見つかると、関連付けられたプロトコルを使用してそのイベントが転送されます。

以下のプロトコルがサポートされています。

- **Azure Log Analytics**。Lenovo XClarity Administrator は、ネットワークを介して監視対象イベントを Microsoft Azure Log Analytics に転送します。
- **メール**。Lenovo XClarity Administrator は、SMTP を使用して監視対象イベントを 1 つ以上のメール・アドレスに転送します。メールには、イベントに関する情報、発生元デバイスのホスト名、Lenovo XClarity Administrator Web インターフェースおよび Lenovo XClarity Mobile アプリへのリンクが含まれています。
- **FTP**。ネットワークを介して監視対象イベントを FTP サーバーに転送します。
- **REST**。Lenovo XClarity Administrator は、ネットワークを介して監視対象イベントを REST Web サービスに転送します。
- **SNMP**。Lenovo XClarity Administrator は、ネットワークを介して監視対象イベントをリモート SNMP マネージャーに転送します。SNMPv1 および SNMPv3 トラップがサポートされています。

  Lenovo XClarity Administrator によって生成される SNMP トラップを記述した管理情報ベース (MIB) ファイルについては、Lenovo XClarity Administrator オンライン・ドキュメントの lenovoMgrAlert.mib ファイル を参照してください。
- **Syslog**。Lenovo XClarity Administrator は、ネットワークを介して監視対象イベントを一元管理ログ・サーバーに転送します。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。

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

注：たとえば、Lenovo XClarity Administrator とイベント・フォワーダーの間の接続がダウンしている場合、またはポートがブロックされている場合、イベントは配信されません。

Azure Log Analytics へのイベント転送のセットアップ

特定のイベントを Azure Log Analytics に転送するように Lenovo XClarity Administrator を構成できます。

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

手順

Azure Log Analytics 用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**Azure Log Analytics**」を選択し、プロトコル固有の情報を入力します。

- イベント・フォワーダーの名前、および必要に応じて説明を入力します。
- Azure Log Analytics インターフェースのプライマリ・キーを入力します。
- 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 30 秒です。
- **オプション**: 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。
  - **なし**。認証は使用しません。

ステップ 5. 「**出力フォーマット**」をクリックして、転送するイベント・データの出力形式を選択します。情報は、イベント・フォワーダーのタイプごとに異なります。

次の例の出力形式は、Azure Log Analytics 受信者のデフォルトの形式です。二重角かっこ内のすべての単語は変数であり、イベント転送時に実際の値に置き換えられます。Azure Log Analytics 受信者が使用できる変数は、「出力フォーマット」ダイアログにリストされています。

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
```

```
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

「**デフォルトにリセット**」をクリックすると、出力形式をデフォルトのフィールドに戻すことができます。

ステップ 6. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 7. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 8. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 9. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 10. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 11. このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。
  4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
  5. 転送するイベント・クラスと保守容易性レベルを選択します。
  6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。
- **イベント・コードの一致**。転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外**。
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。

3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
5. 除外するイベント・クラスと保守容易性レベルを選択します。
6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。

- **イベント・コードで除外**。除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 12. 特定のタイプのイベントを含めるかどうかを選択します。
- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。
- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 13. 通知するイベントのタイプと重大度を選択します。

ステップ 14. イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 15. 「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 16. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

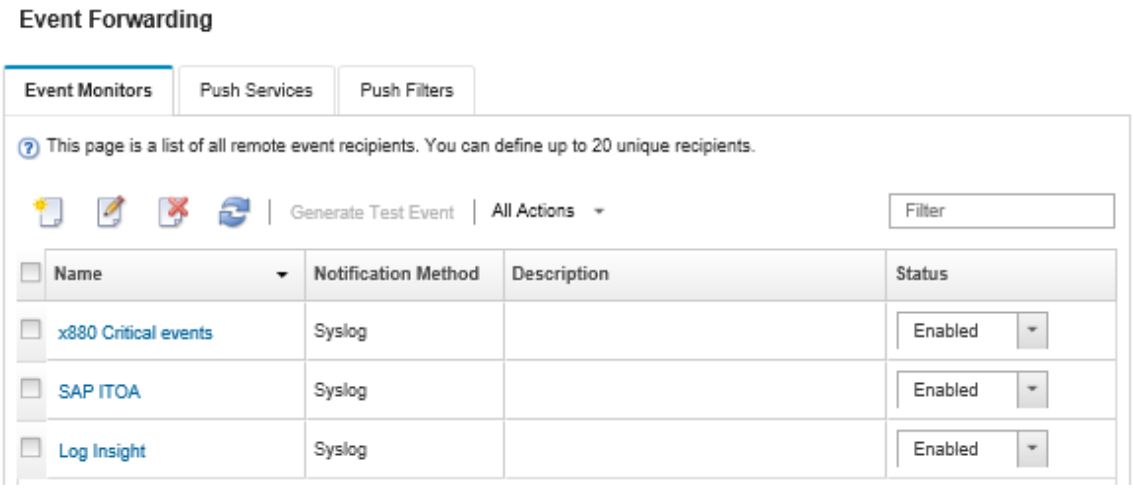
イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:
- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。
- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 17. 「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 18.新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切な Azure Log Analytics サーバーに正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。

SMTP を使用するメール・サービスへのイベント転送のセットアップ

SMTP を使用するメール・サービスに特定のイベントを転送するように Lenovo XClarity Administrator を構成できます。

始める前に

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転送を設定する前に、Lenovo XClarity Administrator オンライン・ドキュメントの Syslog、リモート SNMP マネージャー、またはメールへの イベント転送のセットアップ の情報を確認してください。

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを

適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

手順

SMTP を使用するメール用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**メール**」を選択し、プロトコル固有の情報を入力します。

- イベント・フォワーダーの名前、宛先ホスト、必要に応じて説明を入力します。
- 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。

  デバイスに割り当てられたサポート連絡先にメールを送信するには、「**サポート連絡宛てにメールを使用**」を選択します (XClarity Administrator オンライン・ドキュメントのデバイスのサポート連絡先の定義を参照してください)。
- **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) 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 LXCA.*<source_identifier>*@*<smtp_host>* です。

  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、*<LXCA_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 Administrator 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 Administrator 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 (LXCA.*<source_identifier>*@*<smtp_host>*) は拒否されます。この場合、「**送信元アドレス**」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。
- **オプション**: SMTP サーバーへのセキュアな接続を確立するには、以下の接続タイプを選択します。
  – SSL。通信中は SSL プロトコルを使用します。
  – STARTTLS。TLS 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、LXCA は信頼ストアに 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。この証明書を信頼ストアに追加することを承諾するように要求されます。
- **オプション**: 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。
- **NTLM**。指定されたユーザー ID、パスワード、およびドメイン名を使用して、指定された SMTP サーバーへの認証に NT LAN Manager (NTLM) プロトコルを使用します。
- **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 5. 「**出力フォーマット**」をクリックして、転送するイベント・データのメール本文の出力形式と、メールの件名の形式を選択します。情報は、イベント・フォワーダーのタイプごとに異なります。

次の例の出力形式は、メール受信者のデフォルトの形式です。二重角かっこ内のすべての単語は変数であり、イベント転送時に実際の値に置き換えられます。メール受信者が使用できる変数は、「出力フォーマット 」ダイアログにリストされています。

メールの件名

```
[[DeviceName]]-[[EventMessage]]
```

メールの本文

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint  : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name      : [[DeviceName]]\n
Product name     : [[DeviceProductName]]\n
Host name        : [[DeviceHostName]]\n
Machine Type     : [[DeviceMachineType]]\n
Machine Model    : [[DeviceMachineModel]]\n
Serial Number    : [[DeviceSerialNumber]]\n
DeviceHealthStatus : [[DeviceHealthStatus]]\n
IPv4 addresses   : [[DeviceIPV4Addresses]]\n
IPv6 addresses   : [[DeviceIPV6Addresses]]\n
Chassis         : [[DeviceChassisName]]\n
DeviceBays       : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
 Event ID     : [[EventID]]\n
 Common Event ID : [[CommonEventID]]\n
 EventSeverity  : [[EventSeverity]]\n
 Event Class   : [[EventClass]]\n
 Sequence ID   : [[EventSequenceID]]\n
 Event Source ID : [[EventSourceUUID]]\n
 Component ID  : [[EventComponentUUID]]\n
 Serial Num    : [[EventSerialNumber]]\n
 MTM         : [[EventMachineTypeModel]]\n
 EventService  : [[EventService]]\n
 Console link  : [[ConsoleLink]]\n
 iOS link      : [[iOSLink]]\n
 Android link  : [[AndroidLink]]\n
 System Name   : [[DeviceFullPathName]]\n
```

「**デフォルトにリセット**」をクリックすると、出力形式をデフォルトのフィールドに戻すことができます。

ステップ 6. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 7. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 8. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 9. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 10. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 11. このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。
  4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
  5. 転送するイベント・クラスと保守容易性レベルを選択します。
  6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。
- **イベント・コードの一致**。転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外**。
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。
  3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
  4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
  5. 除外するイベント・クラスと保守容易性レベルを選択します。
  6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。
- **イベント・コードで除外**。除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 12. 特定のタイプのイベントを含めるかどうかを選択します。

- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。

- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 13. 通知するイベントのタイプと重大度を選択します。

ステップ 14. イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 15. 「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 16. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

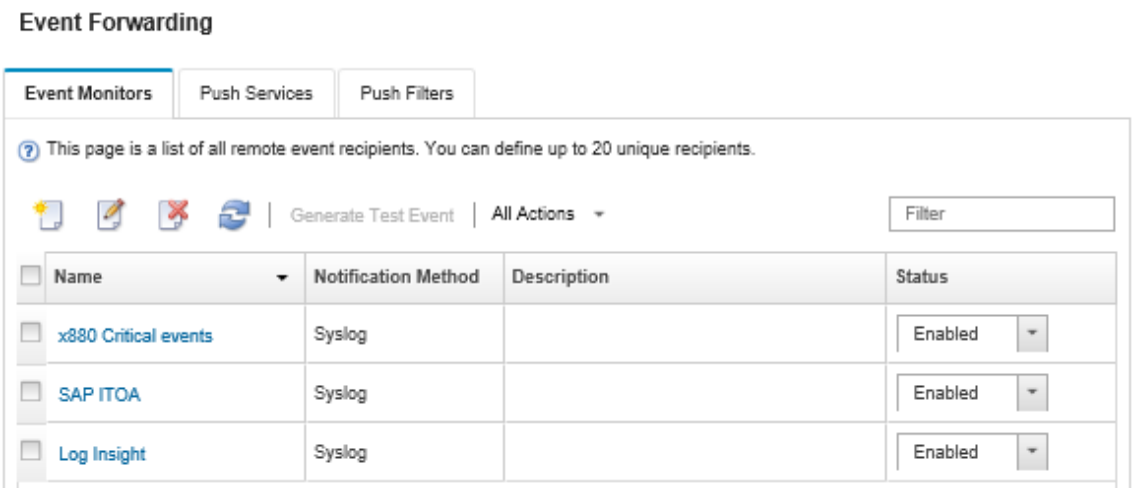
イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:
- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。
- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 17. 「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 18.新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切なメール・サービスに正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。

Gmail SMTP サービスへのイベント転送のセットアップ

Lenovo XClarity Administrator をセットアップして、監視対象イベントを、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。
   e. 検索結果の「**GMAIL API**」をクリックします。
   f. 「**有効**」をクリックします。
   g. 「**資格情報**」タブをクリックします。
   h. 「**OAuth 同意画面**」をクリックします。
   i. 「**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。
   j. 「**視覚情報の作成**」 → 「**OAuth クライアント ID**」 をクリックします。
   k. 「**その他**」を選択して名前を入力します。
   l. 「**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。
   m. 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。
   n. 「**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 Administrator 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 Administrator 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)

FTP サーバーへのイベント転送のセットアップ

特定のイベントを FTP サーバーに転送するように Lenovo XClarity Administrator を構成できます。

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

手順

FTP サーバー用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**FTP**」を選択し、プロトコル固有の情報を入力します。

- イベント・フォワーダーの名前、宛先ホスト、必要に応じて説明を入力します。
- 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 21 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。
- **オプション**: ファイル・コンテンツから削除する文字のシーケンスを指定します。
- 転送されたイベントを含むファイルに使用するファイル名の形式を入力します。デフォルトの形式は `event_[[EventSequenceID]].txt` です。

  注：それぞれのファイルには、1 つのイベントの情報が含まれています。
- ファイルをアップロードするリモート FTP サーバーのパスを入力します。
- 文字エンコーディング **UTF-8** または **Big5** のいずれかを選択します。デフォルトでは UTF-8 です。
- 認証タイプを選択します。これは以下のいずれかの値です。
  - **匿名**。(デフォルト) 認証は使用しません
  - **基本**。指定されたユーザー ID とパスワードを使用して FTP サーバーへの認証を行います。

ステップ 5. 「**出力フォーマット**」をクリックして、転送するイベント・データの出力形式を選択します。情報は、イベント・フォワーダーのタイプごとに異なります。

次の例の出力形式は、FTP 受信者のデフォルトの形式です。二重角かっこ内のすべての単語は変数であり、イベント転送時に実際の値に置き換えられます。FTP 受信者が使用できる変数は、「出力フォーマット」ダイアログにリストされています。

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint   : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name      : [[DeviceName]]\n
Product name     : [[DeviceProductName]]\n
Host name        : [[DeviceHostName]]\n
Machine Type     : [[DeviceMachineType]]\n
```

```
Machine Model     : [[DeviceMachineModel]]\n
Serial Number     : [[DeviceSerialNumber]]\n
DeviceHealthStatus : [[DeviceHealthStatus]]\n
IPv4 addresses    : [[DeviceIPV4Addresses]]\n
IPv6 addresses    : [[DeviceIPV6Addresses]]\n
Chassis         : [[DeviceChassisName]]\n
DeviceBays       : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
 Event ID      : [[EventID]]\n
 Common Event ID : [[CommonEventID]]\n
 EventSeverity  : [[EventSeverity]]\n
 Event Class    : [[EventClass]]\n
 Sequence ID    : [[EventSequenceID]]\n
 Event Source ID : [[EventSourceUUID]]\n
 Component ID   : [[EventComponentUUID]]\n
 Serial Num     : [[EventSerialNumber]]\n
 MTM         : [[EventMachineTypeModel]]\n
 EventService   : [[EventService]]\n
 Console link   : [[ConsoleLink]]\n
 iOS link       : [[iOSLink]]\n
 Android link   : [[AndroidLink]]\n
 System Name    : [[DeviceFullPathName]]\n"
```

「**デフォルトにリセット**」をクリックすると、出力形式をデフォルトのフィールドに戻すことができます。

ステップ 6. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 7. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 8. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 9. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 10. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 11. このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。

4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
5. 転送するイベント・クラスと保守容易性レベルを選択します。
6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。

- **イベント・コードの一致**。転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外**。
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。
  3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
  4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
  5. 除外するイベント・クラスと保守容易性レベルを選択します。
  6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。
- **イベント・コードで除外**。除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 12. 特定のタイプのイベントを含めるかどうかを選択します。
- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。
- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 13. 通知するイベントのタイプと重大度を選択します。

ステップ 14. イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 15. 「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 16. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

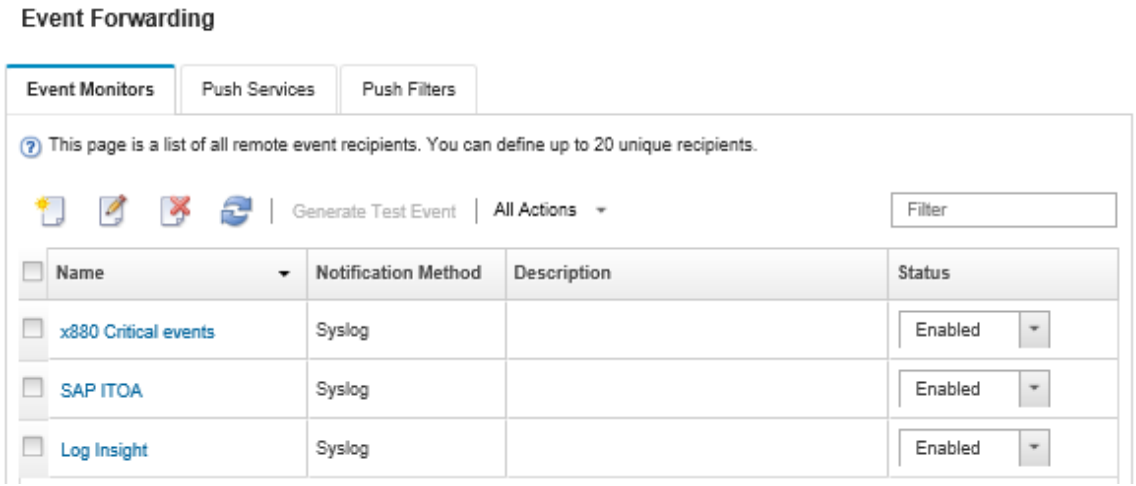
1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:
- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。

- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 17.「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 18.新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切な FTP サーバーに正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。

REST Web サービスへのイベント転送のセットアップ

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

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを

適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

手順

REST Web サービス用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**REST**」を選択し、プロトコル固有の情報を入力します。

- 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)。
- 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**
- 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**
- 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**: 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。
  - **なし**。認証は使用しません。

ステップ 5. 「**出力フォーマット**」をクリックして、転送するイベント・データの出力形式を選択します。情報は、イベント・フォワーダーのタイプごとに異なります。

次の例の出力形式は、REST Web サービス受信者のデフォルトの形式です。二重角かっこ内のすべての単語は変数であり、イベント転送時に実際の値に置き換えられます。REST Web サービス受信者が使用できる変数は、「出力フォーマット」ダイアログにリストされています。

```
{\"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]]\"}"
```

「**デフォルトにリセット**」をクリックすると、出力形式をデフォルトのフィールドに戻すことができます。

ステップ 6. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 7. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 8. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 9. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 10.「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 11.このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。
  4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
  5. 転送するイベント・クラスと保守容易性レベルを選択します。
  6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。
- **イベント・コードの一致**。転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外**。
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。
  3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
  4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
  5. 除外するイベント・クラスと保守容易性レベルを選択します。
  6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。
- **イベント・コードで除外**。除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 12.特定のタイプのイベントを含めるかどうかを選択します。

- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。
- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 13.通知するイベントのタイプと重大度を選択します。

ステップ 14.イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 15.「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 16. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

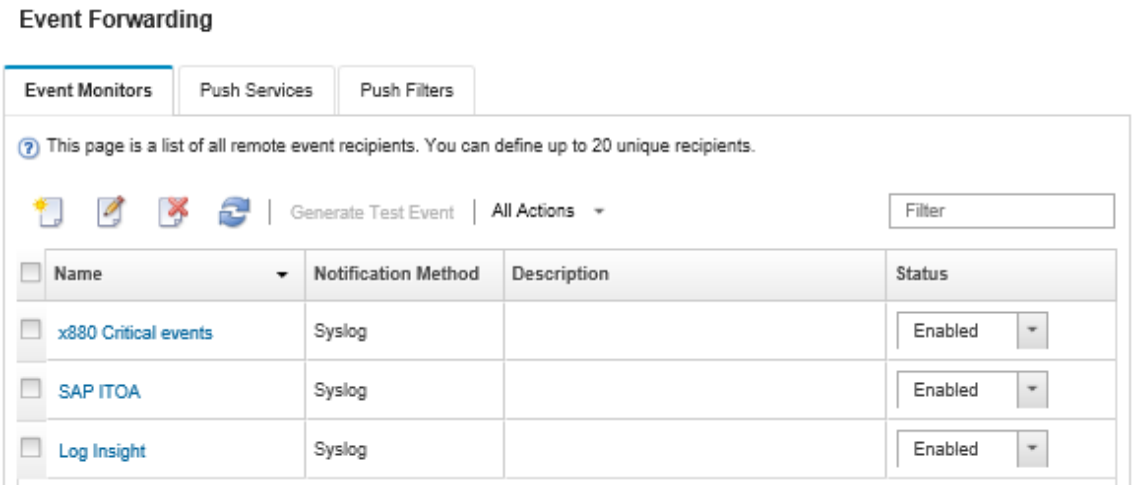
イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:
- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。
- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 17. 「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 18. 新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切な REST Web サービスに正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。

リモート SNMPv1 または SNMPv3 マネージャーへのイベント転送のセットアップ

特定のイベントをリモート SNMPv1 または SNMPv3 マネージャーに転送するように Lenovo XClarity Administrator を構成できます。

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

XClarity Administrator MIB について詳しくは、lenovoMgrAlert.mib ファイル を参照してください。

手順

リモート SNMPv1 または SNMPv3 マネージャー用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**SNMPv1**」または「**SNMPv3**」を選択し、プロトコル固有の情報を入力します。

- イベント・フォワーダーの名前および宛先ホストを入力します。
- 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 162 です。
- **オプション**: 説明、連絡先の名前、ロケーションなどの追加情報を入力します。
- SNMP のバージョンを選択します。これは以下のいずれかの値です。
  - **SNMPv1**。このバージョンを選択する場合、デバイスへの SNMP 要求と一緒に送信されるコミュニティー・パスワードを指定します。
  - **SNMPv3**。これはデフォルトのバージョンです。セキュリティーを強化するために推奨されています。SNMPv3 を選択する場合、オプションでユーザー ID、認証タイプとパスワード、およびプライバシー・タイプとパスワードを指定します。

    SNMPv3 トラップ・レシーバーに XClarity Administrator インスタンスのエンジン ID が必要な場合は、以下の手順を実行してエンジン ID を確認できます。

1. 接続パラメーター (ユーザー名、authProtocol、authPassword、privProtocol、privPassword) が XClarity Administrator に設定されたものと一致することを確認します。
2. 任意のソフトウェア (snmpwalk など) を使用して、XClarity Administrator サーバーで以下の OID のいずれかを使用して SNMP GET 要求を実行します。
   - EngineID: 1.3.6.1.6.3.10.2.1.1.0
   - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

   `snmpget` コマンドには、次の構文を使用します。-a フォワーダー認証タイプは SHA またはブランク (認証なし) であることに注意してください。
   ```
   snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A
   <FORWARDER_AUTH_PW> -x <FORWARDER_PRIVACY_TYPE> -X <FORWARDER_PRIVACY_
   PW> <LXCA_IP> 1.3.6.1.6.3.10.2.1.1.0
   ```
   たとえば、XClarity Administrator の IP アドレスが 192.0.1.0、認証タイプが SHA で、プライバシー・タイプが AES の場合、次のコマンドで engineID を示します。
   ```
   snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1 192.0.1.0
   ```
   次のような応答例が返されます。この例では、engineID は 0x80001370017F00000134C27E12 です。
   ```
   iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
   ```

- 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**: トラップの認証が必要な場合は、ユーザー ID と認証パスワードを入力します。トラップを転送するリモート SNMP マネージャーにも同じユーザー ID とパスワードを入力する必要があります。
- リモート SNMP マネージャーがトラップ送信者の確認に使用する認証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
  - **SHA**。指定されたユーザー ID、パスワード、およびドメイン名を使用して、指定された SNMP サーバーへの認証に SHA プロトコルを使用します。
  - **None**。認証は使用しません
- トラップの暗号化が必要な場合は、プライバシー・タイプ (暗号化プロトコル) とパスワードを入力します。これは以下のいずれかの値です。トラップを転送するリモート SNMP マネージャーにも同じプロトコルとパスワードを入力する必要があります。
  - **AES**
  - **DES**
  - **なし**

ステップ 5. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 6. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 7. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 8. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 9. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 10. このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。
  4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
  5. 転送するイベント・クラスと保守容易性レベルを選択します。
  6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。
- **イベント・コードの一致**。転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外**。
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。
  3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
  4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
  5. 除外するイベント・クラスと保守容易性レベルを選択します。
  6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。
- **イベント・コードで除外**。除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 11. 特定のタイプのイベントを含めるかどうかを選択します。
- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。
- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 12. 通知するイベントのタイプと重大度を選択します。

ステップ 13. イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 14. 「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 15. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

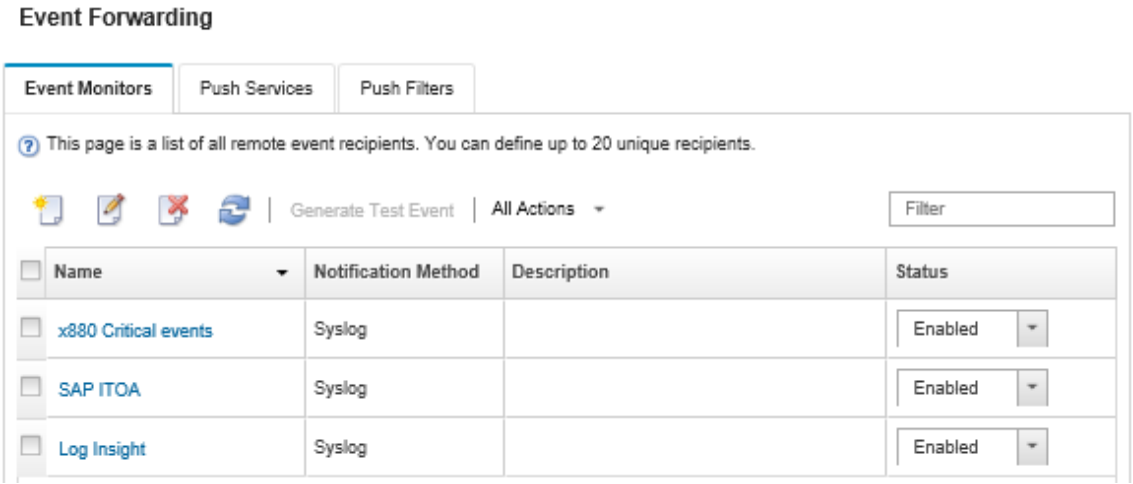
1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:

- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。
- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 16.「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 17.新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切なリモート SNMP マネージャーに正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。
- SNMP トラップに関する情報が含まれている MIB ファイルをダウンロードします。これを行うには、「**作成**」アイコン ( ) をクリックしてから、「新しいイベント転送」ダイアログの「全般」タブで「**MIB ファイルのダウンロード**」をクリックします。

lenovoMgrAlert.mib ファイル

この管理情報ベース (MIB) ファイルには、XClarity Administrator と管理対象デバイスによって発生したアラートを含む、Lenovo XClarity Administratorが生成する SNMP トラップが記述されています。この MIB ファイルは、任意の SNMP トラップ・マネージャーでコンパイルできます。これにより、XClarity Administrator から送信された SNMP トラップを、意味のある方法でレンダリングできます。

MIB ファイルを Web インターフェースからダウンロードするには、メニュー・バーから**監視 → イベント転送**をクリックし、**作成**アイコン( ) をクリックします。イベント・フォワーダーのタイプで SNMP を選択した後、ダイアログの下部で **MIB ファイルのダウンロード**をクリックします。

すべての発信 SNMP トラップに以下のオブジェクトが含まれています。一部の SNMP トラップには追加のオブジェクトが含まれる場合があります。すべてのオブジェクトが MIB ファイルに記述されています。トラップにはリカバリー情報が含まれないことに注意してください。

注：このリストは、XClarity Administrator のリリースごとに異なる場合があります。
- **mgrTrapAppId**。これは「Lenovo イベント・マネージャー」です。
- **mgrTrapCommonEvtID**。共通イベント ID
- **mgrTrapDateTime**。イベントが発生した現地での日付と時刻
- **mgrTrapEventClass**。イベントのソース。これには、監査、冷却、電源、ディスク、メモリー、プロセッサー、システム、テスト、アダプター、拡張、I/O モジュール、またはブレードがあります。
- **mgrTrapEvtID**。イベントの固有 ID
- **mgrTrapFailFRUs**。障害が発生している FRU UUID のコンマ区切りリスト (該当する場合)
- **mgrTrapFailSNs**。障害が発生している FRU のシリアル番号のコンマ区切りリスト (該当する場合)。
- **mgrTrapFullyQualifiedDomainName**。完全修飾ドメイン名: ホスト名とドメイン名
- **mgrTrapID**。トラップ ID
- **mgrTrapMsgText**。メッセージ・テキスト (英語のみ)
- **mgrTrapMsgID**。メッセージ ID
- **mgrTrapMtm**。イベントが発生したデバイスのモデル・タイプ・モデル
- **mgrTrapService**。保守容易性のインジケーターです。これは、000 (不明)、100 (なし)、200 (サービス・センター)、または 300 (お客様) です。
- **mgrTrapSeverity**。重大度のインジケーターです。これは、通知、警告、マイナー、メジャー、またはクリティカルで表示されます。
- **mgrTrapSN**。イベントが発生したデバイスのシリアル番号
- **mgrTrapSrcIP**。発生したイベントを受信したデバイスの IP アドレス
- **mgrTrapSrcLoc**。イベントが発生したデバイスのロケーション (英語のみ、Slot#xx など)
- **mgrTrapSrcName**。イベントが発生したデバイスのホスト名または表示名
- **mgrTrapSysContact**。ユーザーが構成した連絡先 ID
- **mgrTrapSysLocation**。ユーザーが構成したデバイスのロケーション情報
- **mgrTrapSystemName**。デバイス名、コンポーネント名、およびスロットのロケーション
- **mgrTrapTxtId**。トラップを発生させた Lenovo イベント・マネージャーのサーバーのホスト名または IP アドレス
- **mgrTrapUserid**。イベントに関連付けられたユーザー ID (イベントが内部であり、イベント・クラスが監査の場合)
- **mgrTrapUuid**。イベントが発生したデバイスの UUID

syslog へのイベント転送のセットアップ

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

このタスクについて

特定の受信者にイベントを送信するために、最大 20 のイベント・フォワーダーを作成して有効にすることができます。

イベント・フォワーダーの構成後に XClarity Administrator がリブートされた場合、イベントが正しく転送されるためには、管理サーバーによって内部データが再生成されるのを待つ必要があります。

注：XClarity Administrator v1.2.0 以降の場合、「**スイッチ**」は「新しいイベント・フォワーダー」ダイアログと「イベント・フォワーダーの変更」ダイアログの「**イベント**」タブにあります。以前のリリースから 1.2.0 以降にアップグレードした場合は、必ずイベント・フォワーダーを更新して RackSwitch イベントを適切に追加または除外してください。これは、「**すべてのシステム**」チェックボックスにチェックを入れてすべてのデバイスを選択した場合も必要です。

手順

syslog 用のイベント・フォワーダーを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**イベント・フォワーダー**」タブをクリックします。

ステップ 3. 「**作成**」アイコン ( ) をクリックします。「新しいイベント・フォワーダー」ダイアログの「**全般**」タブが表示されます。

ステップ 4. イベント・フォワーダーのタイプとして「**Syslog**」を選択し、プロトコル固有の情報を入力します。

- イベント・フォワーダーの名前、宛先ホスト、必要に応じて説明を入力します。
- 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。
- 任意で 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 5. 「**出力フォーマット**」をクリックして、転送するイベント・データの出力形式を選択します。情報は、イベント・フォワーダーのタイプごとに異なります。

次の例では、出力形式は sylog 受信者のデフォルトの形式です。二重角かっこ内のすべての単語は変数であり、イベント転送時に実際の値に置き換えられます。sylog 受信者が使用できる変数は、「出力フォーマット」ダイアログにリストされています。

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

「**デフォルトにリセット**」をクリックすると、出力形式をデフォルトのフィールドに戻すことができます。

ステップ 6. 「**除外イベントを許可する**」を選択して除外イベントが転送されないようにするか、「**除外イベントを許可する**」をクリアして除外イベントを転送します。詳しくは、イベントの除外を参照してください。

ステップ 7. 「**このフォワーダーを有効化する**」を選択して、このイベント・フォワーダーのイベント転送をアクティブ化します。

ステップ 8. 「**次へ**」をクリックして、「**デバイス**」タブを表示します。

ステップ 9. このイベント・フォワーダーで監視するデバイスおよびグループを選択します。

ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。

ステップ 10. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

ステップ 11. このイベント・フォワーダーで使用するフィルターを選択します。

- **イベント・カテゴリーによって一致**
  1. レベルのステータスにかかわらずすべての監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
  2. すべての保証イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  3. すべてのヘルスの状態変更イベントを転送するには、「**ステータス変更イベントを含める**」を選択します。
  4. すべてのヘルスの状態更新イベントを転送するには、「**ステータス更新イベントを含める**」を選択します。
  5. 転送するイベント・クラスと保守容易性レベルを選択します。
  6. 転送から除外する 1 つ以上のイベントの ID を入力します。コンマを使用して ID で区切ります (例: `FQXHMEM0214I,FQXHMEM0214I`)。
- **イベント・コードの一致。**転送する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。
- **イベント・カテゴリーで除外。**
  1. ステータスのレベルに関わらず、すべての監査イベントを除外するには、「**すべての監査イベントを除外する**」を選択します。
  2. すべての保証イベントを除外するには、「**保証イベントを除外する**」を選択します。
  3. すべてのヘルスの状態変更イベントを除外するには、「**ステータス変更イベントを除外する**」を選択します。
  4. すべてのヘルスの状態更新イベントを除外するには、「**ステータス更新イベントを除外する**」を選択します。
  5. 除外するイベント・クラスと保守容易性レベルを選択します。
  6. 転送する 1 つ以上のイベントの ID を入力します。ID はコンマで区切ります。
- **イベント・コードで除外。**除外する 1 つ以上のイベントの ID を入力します。複数の ID はコンマで区切ります。

ステップ 12. 特定のタイプのイベントを含めるかどうかを選択します。

- 「**すべての監査イベントを含む**」。選択したイベントのクラスや重大度に基づいて、監査イベントに関する通知を送信します。
- 「**保証イベントを含める**」。保証に関する通知を送信します。
- 「**ステータス変更イベントを含める**」。ステータスの変更に関する通知を送信します。
- 「**ステータス更新イベントを含める**」。新しいアラートに関する通知を送信しました
- 「**Bulletin イベントを含める**」。新しい Bulletin に関する通知を送信します。

ステップ 13. 通知するイベントのタイプと重大度を選択します。

ステップ 14. イベントを保守容易性でフィルタリングするかどうかを選択します。

ステップ 15. 「**次へ**」をクリックして、「**スケジューラー**」タブを表示します。

ステップ 16. **オプション**: このイベント・フォワーダーに、指定したイベントを転送する時間と日数を定義します。指定された期間中に発生するイベントのみが転送されます。

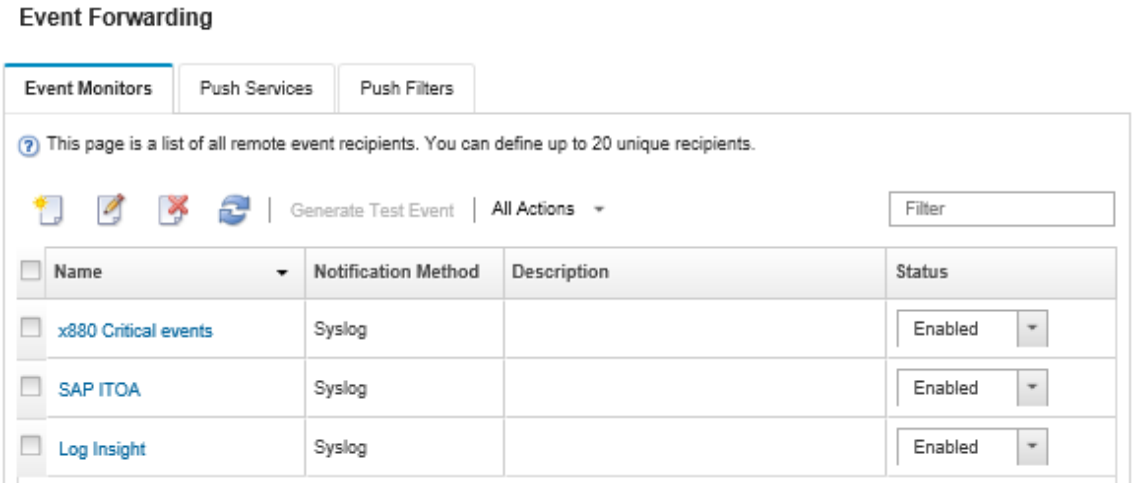
イベント・フォワーダーのスケジュールを作成しない場合、イベントは 24 時間 365 日転送されます。

1. 「**左にスクロール**」アイコン (◀) と「**右にスクロール**」アイコン (▶)、および「**日**」、「**週**」、「**月**」ボタンを使用して、スケジュールを開始する日付および時刻を見つけます。
2. タイム・スロットをダブルクリックして、「新しい期間」ダイアログを開きます。
3. 日付、開始時間および終了時間、スケジュールを再発生させるかどうかなどの必要情報を入力します。
4. 「**作成**」をクリックしてスケジュールを保存し、ダイアログを閉じます。新しいスケジュールがカレンダーに追加されます。

ヒント:
- タイム・スロットを変更するには、カレンダーの別のタイム・スロットにスケジュール項目をドラッグします。
- 期間を変更するには、スケジュール項目の上部または下部を選択してカレンダーの新しい時間にドラッグします。
- 終了時間を変更するには、スケジュール項目の下部を選択してカレンダーの新しい時間にドラッグします。
- スケジュールを変更するには、カレンダーのスケジュール項目をダブルクリックして「**項目の編集**」をクリックします。
- すべてのスケジュール項目の要約を表示するには、「**スケジューラーの要約を表示**」を選択します。要約には、各項目のタイム・スロットおよび反復可能な項目が含まれます。
- カレンダーまたはスケジューラーの要約からスケジュール項目を削除するには、項目を選択して「**項目の削除**」を選択します。

ステップ 17.「**作成**」をクリックします。

イベント・フォワーダーが「イベント転送」テーブルに示されます。



ステップ 18.新しいイベント・フォワーダーを選択して「**テスト・イベントの生成**」をクリックします。イベントが適切な syslog に正しく転送されることを確認します。

終了後

「イベント転送」ページでは、選択したイベント・フォワーダーに対して以下の操作を実行できます。

- イベント・フォワーダーのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フォワーダーの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フォワーダーのプロパティとフィルター基準を変更する。「**名前**」列でイベント・フォワーダー名をクリックします。
- イベント・フォワーダーを削除する。「**削除**」アイコン ( ) をクリックします。
- イベント転送を一時停止する (イベント転送の一時停止を参照)。

イベント転送の一時停止

イベント・フォワーダー無効にすることで、イベント転送を一時停止できます。イベント転送を一時停止すると、受信イベントの監視が停止します。監視が一時停止している間に受信されたイベントは転送されません。

このタスクについて

無効になっている状況は永続的ではありません。管理ノードが再起動された場合、すべてのイベント・フォワーダーが有効になります。

手順

イベント転送を無効にするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベントの転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 一時停止する各イベント・フォワーダーの「**ステータス**」列で「**無効**」を選択します。

モバイル・デバイスへのイベントの転送

Lenovo XClarity Administrator を構成してイベントをモバイル・デバイスにプッシュ通知できます。

始める前に

モバイル・デバイスにイベントを転送するには、以下の要件を満たす必要があります。

- Lenovo XClarity Administrator が Apple または Google のプッシュ・サーバーに接続できるように、有効な DNS サーバーが構成されていることを確認します。「**管理**」 → 「**ネットワーク・アクセス**」 → 「**ネットワーク・アクセスの編集**」 の順にクリックし、「**インターネット設定**」タブをクリックして構成できます (Lenovo XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成参照)。
- イベント管理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。ポートの要件について詳しくは、 Lenovo XClarity Administrator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。

このタスクについて

Lenovo XClarity Mobile アプリケーションがモバイル・デバイスにインストールされている場合、接続している各 Lenovo XClarity Administrator インスタンスでモバイル・デバイスへのイベントのプッシュ通知を有効にできます。プッシュ通知が特定のインスタンスで有効になっている場合、そのモバイル・デバイス用のサブスクリプションが Lenovo XClarity Administrator に作成されます。

モバイル・デバイスにプッシュ通知するイベントは、各 Lenovo XClarity Administrator インスタンスに事前定義済みまたはカスタマイズ済みグローバル・イベント・フィルターを割り当てることで定義できます。事前定義済みグローバル・イベント・フィルターは、デフォルトで有効になっています。Lenovo XClarity Administrator によってフィルター基準に基づいた受信イベントの監視が開始されます。フィルター基準に一致するイベントが見つかると、そのイベントがモバイル・デバイスに転送されます。

Lenovo XClarity Mobile およびサポートされるモバイル・デバイスの詳細については、 Lenovo XClarity Administrator オンライン・ドキュメントのLenovo XClarity Mobile アプリの使用を参照してください。

手順

そのモバイル・デバイスへのプッシュ通知をセットアップするには、モバイル・デバイスの Lenovo XClarity Mobile アプリから以下の手順を実行します。

ステップ 1. プッシュ通知の有効化:

- Lenovo XClarity Administrator インスタンスへの接続を作成すると、プッシュ通知を有効にできます。プッシュ通知は、デフォルトで有効です。
- 1 つ以上のイベント・フィルターを有効にすることで、既存の接続でのプッシュ通知を有効にできます

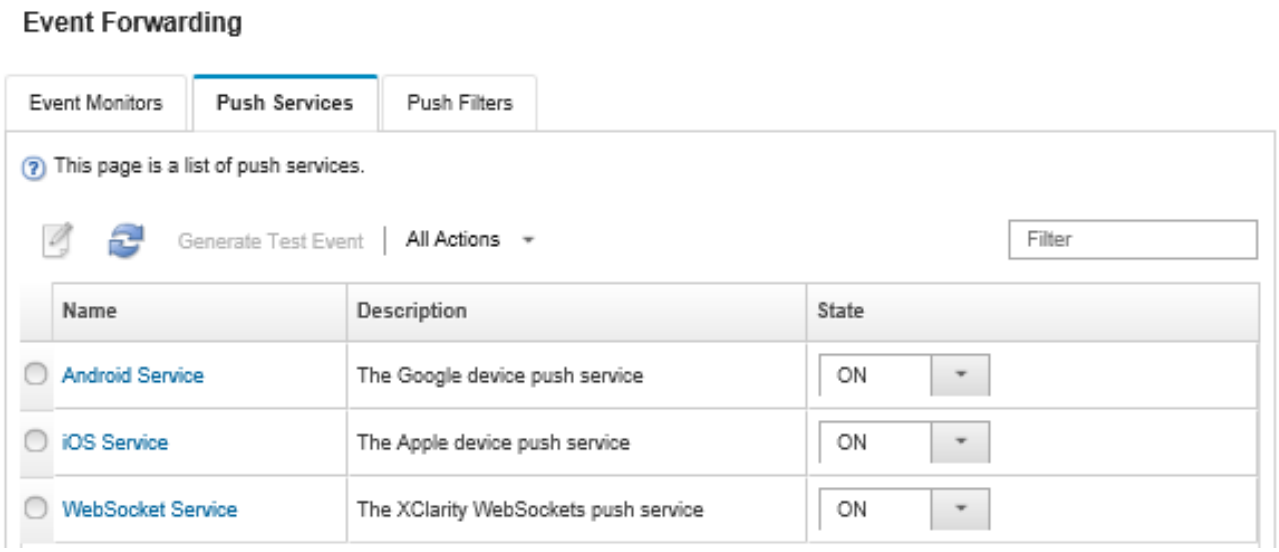
ステップ 2. モバイル・デバイスに転送するイベントを指定するには、グローバル・イベント・フィルターを割り当てます。

注：グローバル・フィルターの追加やサブスクリプションからの削除は、Lenovo XClarity Mobile アプリからのみ行うことができます。Lenovo XClarity Administrator Web インターフェースからのみグローバル・フィルターを作成できます。カスタマイズ済みグローバル・イベント・フィルターの作成については、モバイル・デバイスおよび WebSockets 用のイベント・フィルターの作成を参照してください。

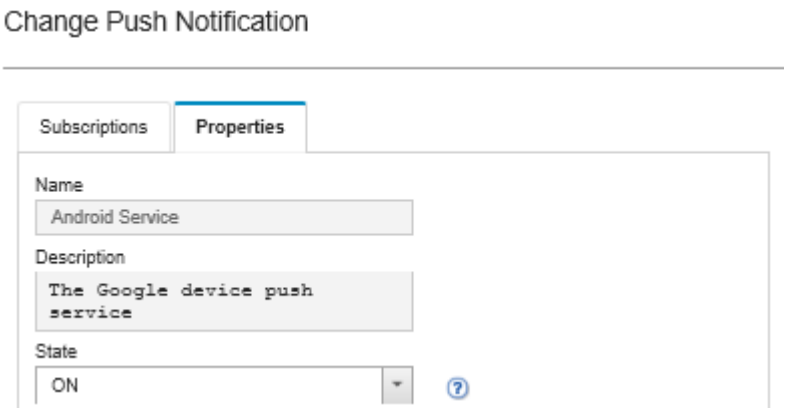
1. 「**設定**」 ➡ 「**プッシュ通知**」 をタップします。Lenovo XClarity Administrator 接続のリストが表示されます。
2. Lenovo XClarity Administrator インスタンスをタップしてプッシュ・フィルターのリストを表示します。
3. Lenovo XClarity Administrator インスタンスで、モバイル・デバイスにプッシュ通知するイベントのイベント・フィルターを有効にします。
4. 「**タッチしてテスト・プッシュ通知を生成**」をタップして、イベント通知が正しくプッシュ通知されることを確認します。

結果

Lenovo XClarity Administrator Web インターフェースの「イベント転送」ページからサブスクリプションを管理できます。「**監視**」 ➡ 「**イベント転送**」 をクリックして「イベント転送」ページを表示します。

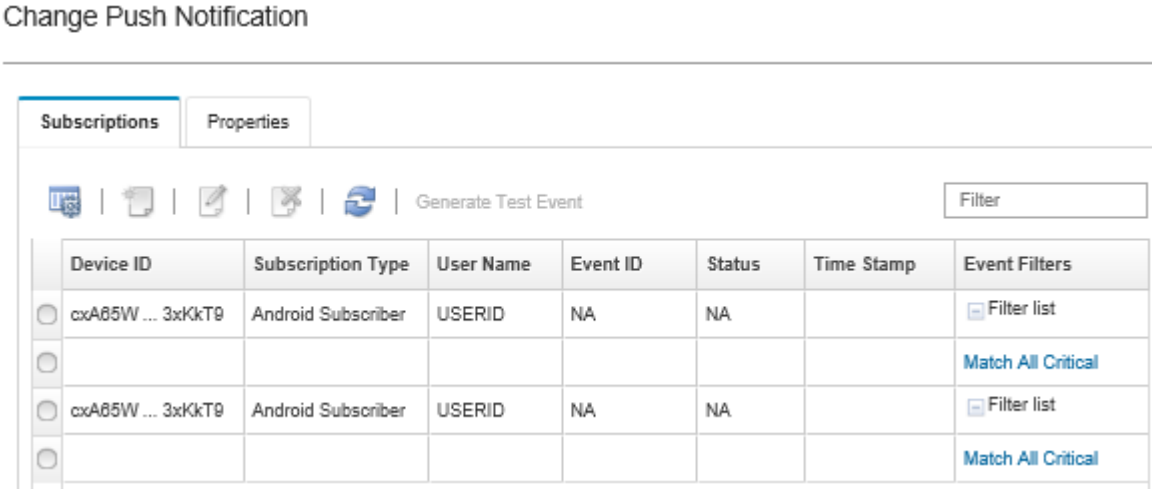


- デバイス通知サービスのプロパティは、「イベント転送」ページの「**プッシュ・サービス**」タブから変更できます。「**名前**」列のプッシュ通知サービス (Google または Apple) へのリンクをクリックして、「プッシュ通知の変更」ダイアログを表示し、「**プロパティ**」タブをクリックします。



- サブスクリプションを有効および無効にできます。
  - 「イベント転送」ページの「**プッシュ・サービス**」タブから特定のデバイスでの通知サービスのすべてのサブスクリプションを有効または無効にするには、デバイス通知サービスのテーブルで「**ON**」または「**OFF**」を選択します。
  - Lenovo XClarity Mobile アプリから特定のデバイスのすべてのサブスクリプションを有効または無効にするには、「**設定**」 ➡ 「**プッシュ通知**」 をタップして、プッシュ通知を有効にするか有効になっているプッシュ通知を無効にします。
  - Lenovo XClarity Mobile アプリから特定のサブスクリプションを有効または無効にするには、「**設定**」 ➡ 「**プッシュ通知**」 をタップして、Lenovo XClarity Administrator 接続をタップし、少なくとも 1 つのイベント・フィルターを有効にするか、すべてのイベント・フィルターを無効にします。
- 「イベント転送」ページの「**プッシュ・サービス**」タブで、特定のモバイル・デバイスのすべてのサブスクリプションのテスト・イベントを生成できます。モバイル・サービスを選択して「**テスト・イベントの生成**」をクリックします。
- 現行サブスクリプションのリストを確認できます。「イベント転送」ページの「**プッシュ・サービス**」タブから、「**名前**」列の該当するデバイス通知サービス (Android または iOS) へのリンクをクリックして、「プッシュ通知の変更」ダイアログを表示し、「**サブスクリプション**」タブをクリックします。デバイス ID は各サブスクリプションを識別します。

  ヒント:
  - デバイス ID はプッシュ登録 ID の最初と最後の 6 桁の数値です。Lenovo XClarity Mobile アプリで 「**設定**」 ➡ 「**バージョン情報**」 ➡ 「**プッシュ登録 ID**」 をタップしてプッシュ登録 ID を確認できます。
  - 以下の役割を持つユーザーとしてログインしている場合は、すべてのサブスクリプションが表示されます。それ以外の場合は、ログインしているユーザーのサブスクリプションのみが表示されます。
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- 「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブでサブスクリプションに割り当てられたイベント・フィルターのリストを確認できます。そのサブスクリプションの「**イベント・フィルター**」列の「**フィルター・リスト**」を展開します。



- 「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブから特定のサブスクリプションのイベント・フィルターを作成できます。サブスクリプションを選択して、「**作成**」アイコン ( ) をクリックします。

注：これらのイベント・フィルターは特定のサブスクリプションのみに適用され、他サブスクリプションに使用することはできません。

また、イベント・フィルターを選択して「**編集**」アイコン ( ) または「**削除**」アイコン () をクリックして、イベント・フィルターの編集または削除ができます。

- 「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブから、特定のサブスクリプションで最後に試みられたプッシュの状況を確認できます。「**タイム・スタンプ**」列は、最後のプッシュ通知の日付と時刻を示しています。「**ステータス**」は、プッシュ通知が正常にプッシュ・サービスに配信されたかどうかを示します。サービスからデバイスにプッシュ通知が正常に配信されたかどうかに関するステータスはありません。プッシュ・サービス対する配信が失敗した場合は、「ステータス」列に失敗に関する追加情報が表示されます。
- 「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブから特定のサブスクリプションのテスト・イベントを生成できます。サブスクリプションを選択して、「**テスト・イベントの生成**」をクリックします。
- 「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブからサブスクリプションを削除できます。サブスクリプションを選択して、「**削除**」アイコン () をクリックします。

WebSocket サービスへのイベントの転送

Lenovo XClarity Administrator を構成してイベントを WebSocket サービスにプッシュ通知できます。

このタスクについて

WebSocket サブスクリプションは Lenovo XClarity Administrator に永続的に保存されません。Lenovo XClarity Administrator のリブート時に、WebSocket サブスクライバーを再びサブスクライブする必要があります。

手順

WebSocket サービスにイベント通知をプッシュするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。

ステップ 2. 「**プッシュ・サービス**」タブをクリックします。

ステップ 3. 「**名前**」列の「**WebSocket サービス**」のリンクをクリックします。「プッシュ通知の変更」ダイアログが表示されます。

ステップ 4. 「**サブスクリプション**」タブをクリックします。

ステップ 5. 「**作成**」アイコン ( ) をクリックします。

ステップ 6. 宛先ホストの IP アドレスを入力します。

ステップ 7. 「**作成**」をクリックします。

ステップ 8. 新しいサブスクリプションを選択し、「**テスト・イベントの生成**」をクリックします。イベントが WebSocket サービスに正常に転送されたことを確認します。

結果

「プッシュ通知の変更」ダイアログの「**サブスクリプション**」タブで、選択した WebSocket サブスクリプションに対して以下の操作を実行できます。

- WebSocket サービスのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- サブスクリプションを削除する。サブスクリプションを選択して、「**削除**」アイコン () をクリックします。
- 特定のサブスクリプションで最後に試みられたプッシュのステータスを確認する。「**ステータス**」列の内容を確認します。試行が失敗した場合は、この列にエラーを示すメッセージが含まれています。

「プッシュ通知の変更」ダイアログの「**プロパティ**」タブで、以下の操作を実行できます。

- 接続のアイドル時間、最大バッファ・サイズ、最大サブスクライバー数、登録タイムアウト期間などの WebSocket サービスのプロパティを変更します。
- WebSocket サービスをデフォルト設定にリセットする。「**デフォルトの復元**」をクリックします。
- WebSocket サービスのすべてのサブスクリプションへのイベント通知のプッシュを中断する。「**状態**」を「オフ」に設定します。

「イベント転送」ページの「**プッシュ・サービス**」タブで、すべての WebSocket サブスクリプションのテスト・イベントを生成できます。WebSocket サービスを選択して「**テスト・イベントの生成**」をクリックします。

モバイル・デバイスおよび WebSockets 用のイベント・フィルターの作成

モバイル・デバイスおよび WebSockets のサブスクリプションに使用できるグローバル・イベント・フィルターを作成できます。また、サブスクリプションに固有のイベント・フィルターを作成できます。

始める前に

イベント・フィルターを作成するにはスーパーバイザー権限が必要です。

最大 20 個のグローバル・イベント・フィルターを作成できます。

このタスクについて

以下のグローバル・イベント・フィルターが事前定義されています。

- **すべてのクリティカルに一致**。このフィルターは、管理対象デバイスまたは XClarity Administrator によって生成されるすべてのクリティカル・イベントに一致します。
- **すべての警告に一致**。このフィルターは、管理対象デバイスまたは XClarity Administrator によって生成されるすべての警告イベントに一致します。

手順

グローバル・イベント・フィルターを作成するには、以下の手順を実行します。

- すべてのサブスクリプションに使用できるグローバル・イベント・フィルターを作成します。
  1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「イベント転送」ページが表示されます。
  2. 「**プッシュ・フィルター**」タブをクリックします。
  3. 「**作成**」アイコン ( ) をクリックします。「新しいプッシュ・フィルター」ダイアログの「**全般**」タブが表示されます。
  4. このイベント・フィルターの名前および説明 (オプション) を指定します。
  5. 「**次へ**」をクリックして、「**システム**」タブを表示します。
  6. 監視するデバイスを選択します。

     ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。
  7. 「**次へ**」をクリックして、「**イベント**」タブを表示します。

8. イベント転送の対象となるコンポーネントとイベントが転送する重大度を選択します。

   ヒント:
   – すべてのハードウェア・イベントが転送されるようにするには、「**すべてのイベントに一致**」を選択します。
   – 監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
   – 保障イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
9. 「**作成**」をクリックします。

- 特定のサブスクリプションのイベント・フィルターを作成します。
  1. XClarity Administrator メニュー・バーで、「**監視**」 → 「**イベント転送**」をクリックします。「新しいイベント転送」ページが表示されます。
  2. 「**プッシュ・フィルター**」タブをクリックします。
  3. テーブルの「名前」列にあるモバイル・デバイスのタイプ (Android または iOS) のリンクを選択します。「プッシュ通知の変更」ダイアログが表示されます。
  4. アクティブなサブスクリプションのリストを表示するには、「**サブスクリプション**」をクリックします。
  5. サブスクリプションを選択して、「**作成**」アイコン ( ) をクリックします。「新しいイベント・フィルター」ダイアログの「**全般**」タブが表示されます。
  6. このイベント・フィルターの名前および説明 (オプション) を指定します。
  7. 「**次へ**」をクリックして、「**システム**」タブを表示します。
  8. 監視するデバイスを選択します。

     ヒント すべての管理対象デバイスのイベント (現行および将来) を転送するには、「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れます。「**すべてのシステムと突き合わせ**」チェックボックスにチェックを入れなかった場合、選択したデバイスの UUID 列にダミー UUID がないことを確認します。ダミー UUID は、再起動後にリカバリーしていない、または管理サーバーによってすべては検出されていないデバイスに割り当てられます。ダミー UUID のあるデバイスを選択した場合、デバイスがすべて検出され、あるいはリカバリーされてダミー UUID がリアル UUID に変わるまで、イベント転送はこのデバイスに実行されません。
  9. 「**次へ**」をクリックして、「**イベント**」タブを表示します。
  10. イベント転送の対象となるコンポーネントとイベントが転送する重大度を選択します。

      ヒント:
      – すべてのハードウェア・イベントが転送されるようにするには、「**すべてのイベントに一致**」を選択します。
      – 監査イベントが転送されるようにするには、「**すべての監査イベントを含む**」を選択します。
      – 保障イベントが転送されるようにするには、「**保証イベントを含める**」を選択します。
  11. 「**作成**」をクリックします。

終了後

「イベント転送」ページの「プッシュ・フィルター」タブでは、選択したイベント・フィルターに対して以下の操作を実行できます。

- イベント・フィルターのリストを更新する。「**最新表示**」アイコン ( ) をクリックします。
- 特定のイベント・フィルターの詳細を表示する。「**名前**」列のリンクをクリックします。
- イベント・フィルターのプロパティとフィルター基準を変更する。「**編集**」アイコン ( ) をクリックします。

イベント・フィルターを削除する。「**削除**」アイコン ( ) をクリックします。

ジョブの操作

*ジョブ*とは、1 つ以上のデバイスに対して実行される、比較的実行時間の長いタスクです。特定のジョブを 1 回だけ (即時にまたは後で) 実行するようにスケジュールすることも、反復ベースでも、または特定のイベントが発生した際に実行するようにスケジュールすることもできます。

ジョブはバックグラウンドで実行されます。ジョブ・ログで各ジョブのステータスを確認できます。

ジョブの監視

Lenovo XClarity Administrator 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。ジョブ・ログには、実行中、完了、エラーありの各ジョブが含まれています。

このタスクについて

*ジョブ*とは、1 つ以上のデバイスに対して実行される、比較的実行時間の長いタスクです。たとえば、オペレーティング・システムを複数のサーバーにデプロイする場合、各サーバーのデプロイが個別のジョブとして表示されます。

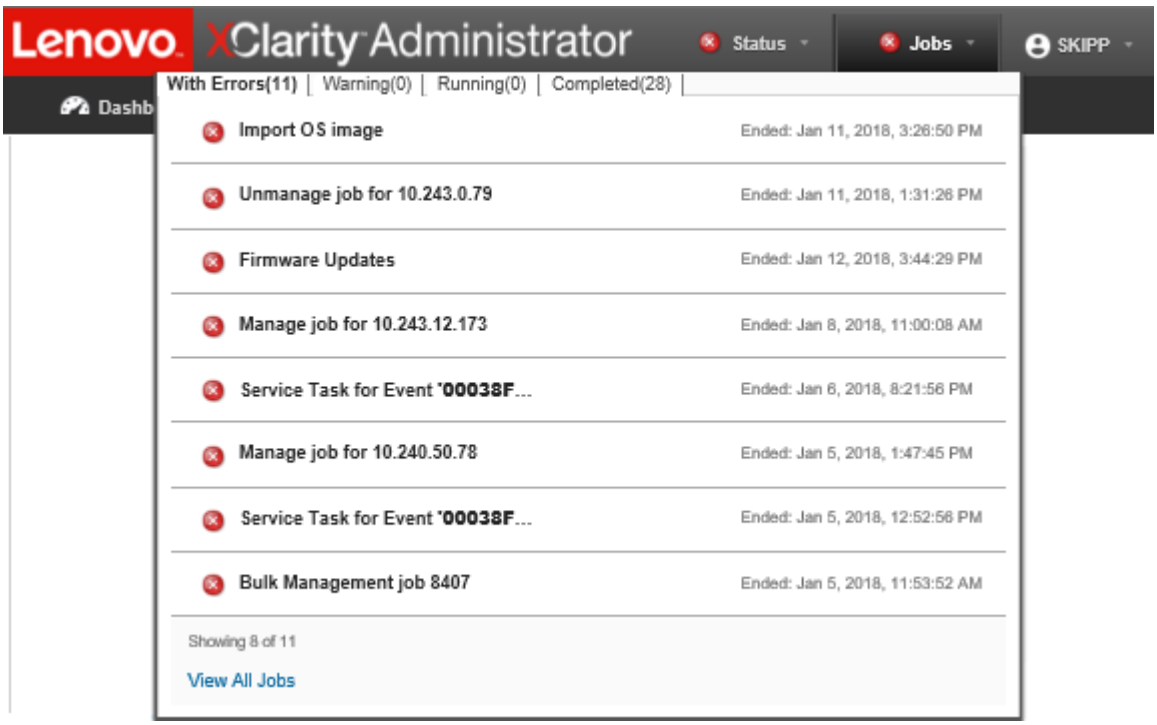
ジョブはバックグラウンドで実行されます。ジョブ・ログで各ジョブのステータスを確認できます。

ジョブ・ログには各ジョブに関する情報が含まれています。ログには、最大で 1,000 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。

手順

ジョブ・ログを表示するには、以下のいずれかの手順を実行します。

- XClarity Administrator のタイトル・バーで「**ジョブ**」をクリックします。実行中、完了、エラーありの各ジョブの概要が表示されます。



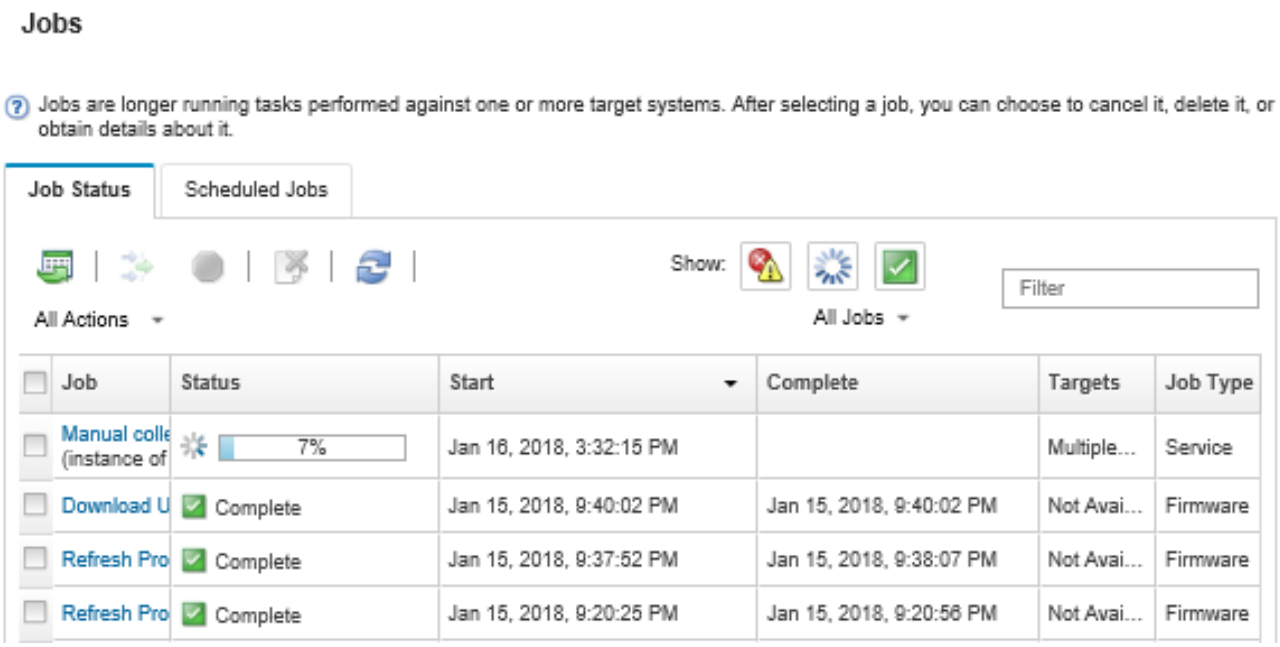
このプルダウンで以下のタブをクリックできます。
- **エラー**。エラーが関連付けられているすべてのジョブのリストが表示されます。
- **警告**。警告が関連付けられているすべてのジョブのリストが表示されます。
- 「**実行中**」。現在進行中のすべてのジョブのリストが表示されます。
- 「**完了**」。完了したすべてのジョブのリストが表示されます。

ジョブの詳細を確認するには、プルダウン内のジョブ項目の上にマウスを移動します。ジョブの詳細には、ジョブの状況、進行状況、およびそのジョブを作成したユーザーが含まれます。

- XClarity Administrator のタイトル・バーで、「**ジョブ**」をクリックし、「**すべてのジョブの表示**」リンクをクリックして、「ジョブ・ステータス」ページを表示します。
- XClarity Administrator のメニュー・バーで、「**モニター**」 → 「**ジョブ**」をクリックし、「**ジョブ・ステータス**」タブをクリックして「ジョブ・ステータス」ページを表示します。

終了後

「ジョブ」ページには、XClarity Administrator のすべてのジョブのリストが表示されます。



このページでは、以下の操作を実行できます。

- ジョブ・スケジュールを作成する。「**スケジュール・ジョブ**」タブをクリックします (ジョブのスケジューリングを参照)。
- 特定のジョブに関する詳細情報を表示する。「**ジョブ**」列のジョブの説明をクリックします。サブタスク (サブジョブ) のリストとその対象、必要な操作を含むサブタスクの概要、各メッセージの重大度とタイムスタンプを含むログの詳細を表示するダイアログが表示されます。。子タスクのログは表示または非表示にできます。
- ジョブのスケジュールに関する情報を表示する。スケジュールされたジョブについては、「**ジョブ**」列のジョブの説明の下にある「この」リンクをクリックします。
- 1 ページに表示するジョブの数を変更する。デフォルトは 10 ジョブです。25、50、またはすべてのジョブを表示できます。
- 表示されているジョブのリストを絞り込む。
  - 特定のソースのジョブのみを表示する。「**ジョブ・タイプ**」をクリックして、以下のいずれかのオプションを選択します。
    - **すべてのジョブ・タイプ**
    - Service
    - Management
    - Configuration
    - **ファームウェア**
    - **状況**
    - Power
    - **リモート・アクセス**
    - **システム ID**
    - **OS イメージ**
    - **OS デプロイメント**
    - **OS プロファイルのエクスポート**
    - Custom
    - Inventory
    - Unknown
  - 特定のスケジュール・タイプに関連付けられたスケジュール済みジョブのみを表示する。「**スケジュール・タイプ**」をクリックし、以下のいずれかのオプションを選択します。

  - **すべてのスケジュール・タイプ**
  - **一回限り**
  - **反復**
  - **トリガー**
- 「**エラーまたは警告があるジョブを非表示にする**」アイコン ( ) をクリックして、エラーまたは警告があるジョブの表示/非表示を切り替える。
- 「**実行中のジョブを非表示にする**」アイコン ( ) をクリックして、現在実行されているジョブの表示/非表示を切り替える。
- 「**完了したジョブを非表示にする**」アイコン ( ) をクリックして、完了したジョブの表示/非表示を切り替える。
- 「**フィルター**」フィールドにテキストを入力して、特定のテキストを含むジョブのみを表示する。
- ページにフィルタリングが適用されている場合、「**すべてのジョブを表示**」アイコン ( ) をクリックしてフィルターを削除します。
- 列見出しをクリックして、ジョブを列でソートする。

- ジョブ・リストを CSV ファイルとしてエクスポートする。「**CSV としてエクスポート**」アイコン ( ) をクリックします。

  注：エクスポートしたログ内のタイムスタンプには、Web ブラウザーに指定された現地時間が使用されます。
- 実行中のジョブまたはサブタスクを 1 つ以上選択し、「**停止**」アイコン ( ) をクリックして、実行中のジョブまたはサブタスクをキャンセルする。

  注：ジョブのキャンセルは数分かかることがあります。
- 完了したジョブまたはサブタスクを 1 つ以上選択し、「**削除**」アイコン ( ) をクリックして、完了したジョブまたはサブタスクをジョブ・ログから削除する。
- 特定のジョブに関する情報をエクスポートする。ジョブを選択して、「**CSV としてエクスポート**」アイコンをクリックします ( )。
- 「**最新表示**」アイコン ( ) をクリックして、ジョブ・ログを最新の情報に更新する。

ジョブのスケジューリング

Lenovo XClarity Administrator でスケジュールを作成して特定のタスクを特定の時間に実行できます。

このタスクについて

以下のタイプのジョブをスケジュールできます。
- 電源オフやリブートなどのシンプルなタスク
- 特定のデバイスのサービス・データの収集
- Lenovo Web サイトからファームウェア更新および OS デバイス・ドライバー・カタログを更新する
- Lenovo Web サイトからの XClarity Administrator 更新カタログの更新
- Lenovo Web サイトからのファームウェアのダウンロード
- 管理対象デバイスでファームウェアおよび OS デバイス・ドライバーを更新する
- XClarity Administrator データと設定をバックアップ
- スイッチ構成データのバックアップと復元

次の条件でジョブの実行をスケジュールできます。
- 一回限り (直ちにまたは後で)
- 反復ベースで
- 特定のイベントが発生した時

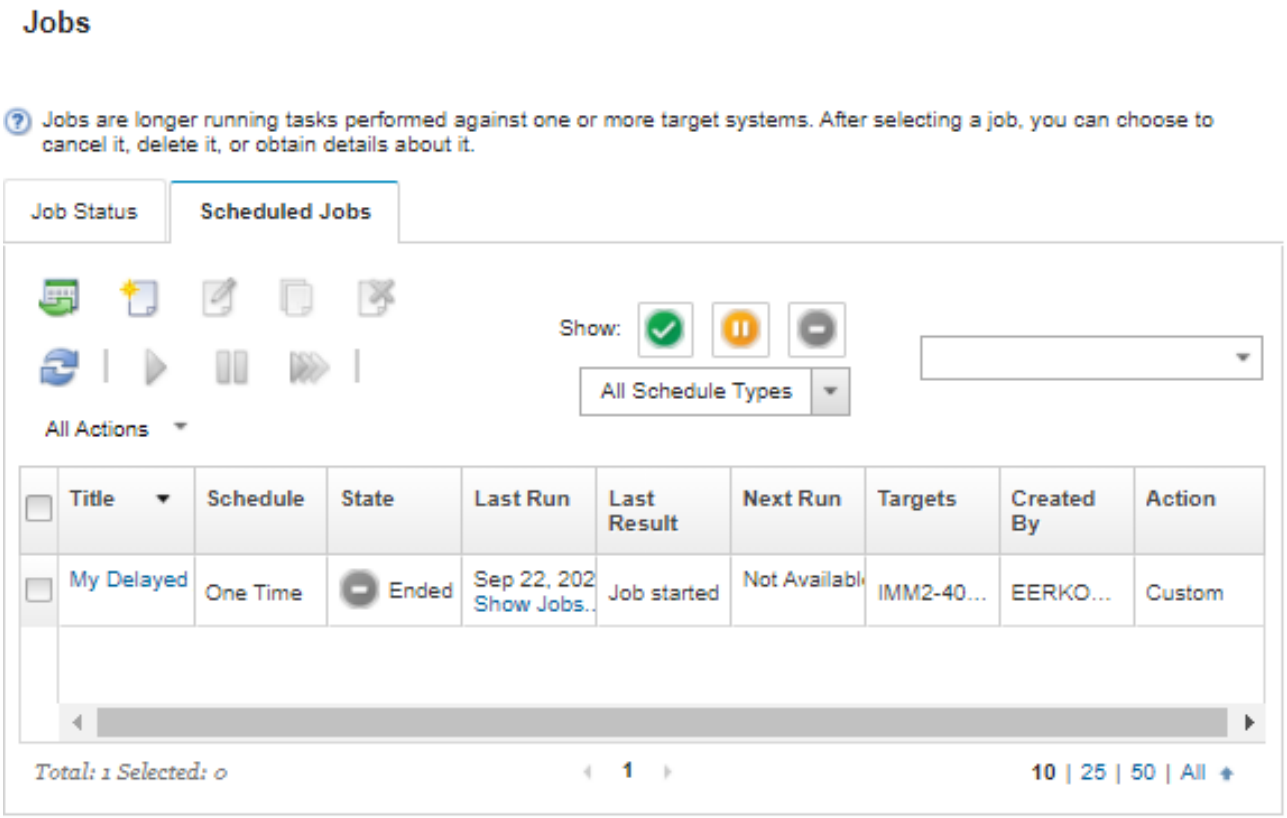
手順

ジョブを作成してスケジュールするには、以下の手順を実行します。

- ファームウェアの更新やサービス・データの収集などの複雑なタスクの場合は、現在のタスク・ページまたはダイアログでジョブを作成します。
  1. 「**スケジュール**」をクリックしてこのタスクを実行するスケジュールを作成します。「新しいジョブのスケジュール」ダイアログが表示されます。
  2. ジョブの名前を入力します。
  3. ジョブを実行する時を指定します。使用可能なオプションは、ジョブのタイプによって異なります。一部のジョブは反復またはイベントによってトリガーすることはできません。
     - **一回限り**。これらのジョブは、1 回のみ実行されます。このジョブを実行する日付と時刻を指定します。
     - **反復**。これらのジョブは、1 回以上実行されます。このジョブを実行する時と頻度を指定します。
     - **イベントでトリガー**。これらのジョブは特定のイベントが発生すると実行されます。
       a. このジョブを実行する日付と時刻を指定して、「**次へ**」をクリックします。
       b. ジョブをトリガーするイベントを選択します。
  4. 「**ジョブの作成**」をクリックします。
- 電源オンやリブートなどのシンプルなタスクの場合は、「ジョブ」ページからジョブ・スケジュールを作成します。
  1. XClarity Administrator 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」ページを表示します。
  2. 「**作成**」アイコン ( ) をクリックして「新しいジョブのスケジュール」ダイアログを表示します。
  3. ジョブの名前を入力します。
  4. ジョブを実行する時を指定します。
     - **一回限り**。これらのジョブは、1 回のみ実行されます。
       a. このジョブを実行する日付と時刻を指定して、「**次へ**」をクリックします。
       b. ジョブを実行する管理対象デバイスを選択します。
     - **反復**。これらのジョブは、1 回以上実行されます。
       a. このジョブを実行する時と頻度を指定します。
       b. ジョブを実行する管理対象デバイスを選択します。
     - **イベントでトリガー**。これらのジョブは特定のイベントが発生すると実行されます。
       a. このジョブを実行する日付と時刻を指定して、「**次へ**」をクリックします。
       b. ジョブを実行する管理対象デバイスを選択して、「**次へ**」をクリックします。
       c. ジョブをトリガーするイベントを選択します。
  5. 「**作成**」をクリックします。

終了後

「スケジュールされたジョブ」タブが表示され、XClarity Administrator のすべてのジョブ・スケジュールの一覧が表示されます。



このページでは、以下の操作を実行できます。

- 特定のジョブ・スケジュールのすべてのアクティブなジョブと完了済みジョブに関する情報を表示する。「**ジョブ**」列のリンクをクリックします。
  - 特定のスケジュール・タイプで表示されるジョブ・スケジュールのリストを絞り込む。「**スケジュール・タイプ**」をクリックし、以下のいずれかのオプションを選択します。
    - **すべてのスケジュール・タイプ**
    - **一回限り**
    - **反復**
    - **トリガー**
  - 特定の状態のジョブ・スケジュールのみを表示または非表示にする。次のいずれかのアイコンをクリックします。
    - アクティブなすべてのスケジュール済みジョブは、「**アクティブ**」アイコン ( ) をクリックします。
    - アクティブではないすべてのスケジュール済みジョブは、「**一時停止**」アイコン ( ) をクリックします。
    - 既に実行済みで再度実行するようにスケジュールされていないすべてのスケジュール済みジョブは、「**終了**」アイコン ( ) をクリックします。
  - 特定のテキストを含むスケジュール済みジョブのみを表示には、「**フィルター**」フィールドにテキストを入力します。
  - スケジュール済みジョブを列でソートには、列見出しをクリックします。
- ジョブが最後に実行された時を確認するには、「**前回の実行**」列を確認します。この列の「ジョブ・ステータス」リンクをクリックすると、最後に実行されたジョブのステータスが表示されます。
- ジョブが次回実行されるスケジュールを確認するには、「**次回の実行**」列を確認します。その列の「詳細」リンクをクリックすると、今後のすべての日付と時刻のリストが表示されます。

- スケジュールに関連付けられたジョブを今すぐ実行するには、「**実行**」アイコンをクリックします ( ) をクリックします。
- ジョブ・スケジュールを無効または有効にするには、「**一時停止**」アイコン ( ) または「**アクティブにする**」アイコン ( ) をそれぞれクリックします。
- ジョブ・スケジュールをコピーして変更するには、「**コピー**」アイコン ( ) をクリックします。
- ジョブ・スケジュールを編集するには、「**編集**」アイコン ( ) をクリックします。
- 選択したジョブ・スケジュールを 1 つ以上削除するには、「**削除**」アイコン ( ) をクリックします。
- 特定のジョブ・スケジュールに関する情報をエクスポートする。ジョブ・スケジュールを選択して、「**CSV としてエクスポート**」アイコンをクリックします ( )。
- ジョブ・スケジュールのリストを最新表示にするには、「**すべての操作**」 → 「**最新表示**」をクリックします。

ジョブに対する解決策とコメントの追加

解決方法とコメントは、成功またはエラーの状態にかかわらず、完了したジョブに追加できます。親ジョブおよびそのジョブのサブタスクでこれを行うことができます。

手順

ジョブに解決策およびコメントを追加するには、以下のいずれかの手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**モニター**」 → 「**ジョブ**」をクリックし、「**ジョブ・ステータス**」タブをクリックして「ジョブ・ステータス」ページを表示します。

ステップ 2. 「**ジョブ**」列で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。

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

このダイアログから、このジョブに追加されたすべての備考の履歴と解決策を確認できます。「**すべての記録のクリア**」をクリックすると履歴をクリアできます。

ステップ 4. 以下のいずれかの解決策を選択します。
- **変更なし**
- **調査中**
- **解決済み**
- **異常終了**

ステップ 5. 「**備考**」フィールドに再マークを追加します。

ステップ 6. 「**適用**」をクリックします。

「ジョブ・ステータス」ページで、そのジョブの「**ステータス**」列に解決が表示されます。

第 3 章　サービスおよびサポートの操作

Lenovo XClarity Administrator Web インターフェースには、各管理対象デバイスのサポート連絡先の定義、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。

詳細: XClarity Administrator: サービスおよびサポート

Lenovo からの Bulletin の受け取り

Lenovo は、サポート Web サイトでセキュリティーに関する注意やオンライン・サービスへの影響などの情報を継続的に更新しています。Lenovo XClarity Administrator Web インターフェースでは、Lenovo からこれらの情報を Bulletin として受け取るようにすることができます。

始める前に

Lenovo から通知を受信するには、XClarity Administrator がインターネットにアクセスできる必要があります。

Bulletin に必要なインターネット・アドレスへの接続があることを確認します。

このタスクについて

Bulletin の受け取りは、デフォルトで有効になっています。

有効にすると、Lenovo から以下のような Bulletin が届きます。
- 新しいリリースの XClarity Administrator またはファームウェアが利用可能
- ファームウェアまたは管理サーバーに影響する脆弱性などのセキュリティー・アラートが検出された
- Lenovo XClarity オンライン・サービスに影響する計画された停止

Bulletin は複数の方法で表示できます。

- 新しい Bulletin は、XClarity Administrator Web インターフェースのポップアップ・メッセージに表示されます。
- 「ログイン」ページでユーザー操作メニュー (ADMIN_USER) をクリックして、「**Lenovo Bulletins サービス**」をクリックすると、過去 30 日間の Bulletin のリストを表示できます。
- メール・フォワーダーを設定して「**Bulletin イベントを含める**」オプションを有効にすると、Bulletin をメールで受け取ることができます (XClarity Administrator のオンライン・ドキュメントの SMTP を使用するメール・サービスへのイベント転送の セットアップ を参照)。

手順

Bulletin の受け取りを有効にするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator 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「**Lenovo Bulletins サービス**」をクリックして、「Lenovo Bulletin サービス」ページを表示します。

ステップ 2. 「**Lenovo から Bulletin を受け取ることに同意します**」を選択します。

ステップ 3. 「**適用**」をクリックします。

© Copyright Lenovo 2015, 2025

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 Administrator 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、XClarity Administrator 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。

- Lenovo Warranty データベース (ワールドワイド) - https://ibase.lenovo.com/POIRequest.aspx
- Lenovo Warranty データベース (中国のみ) - http://service.lenovo.com.cn:83/webservice/NewProductQueryService.asmx
- Lenovo Warranty Web サービス - http://supportapi.lenovo.com/warranty/ または https://supportapi.lenovo.com/warranty/

「すべての操作」 ➡ 「保証リンクの構成」をクリックして、XClarity Administrator で保証 URL を有効または無効にできます。

注：RackSwitch の場合、**「シリアル番号」**列に該当するシリアル番号が表示されます。

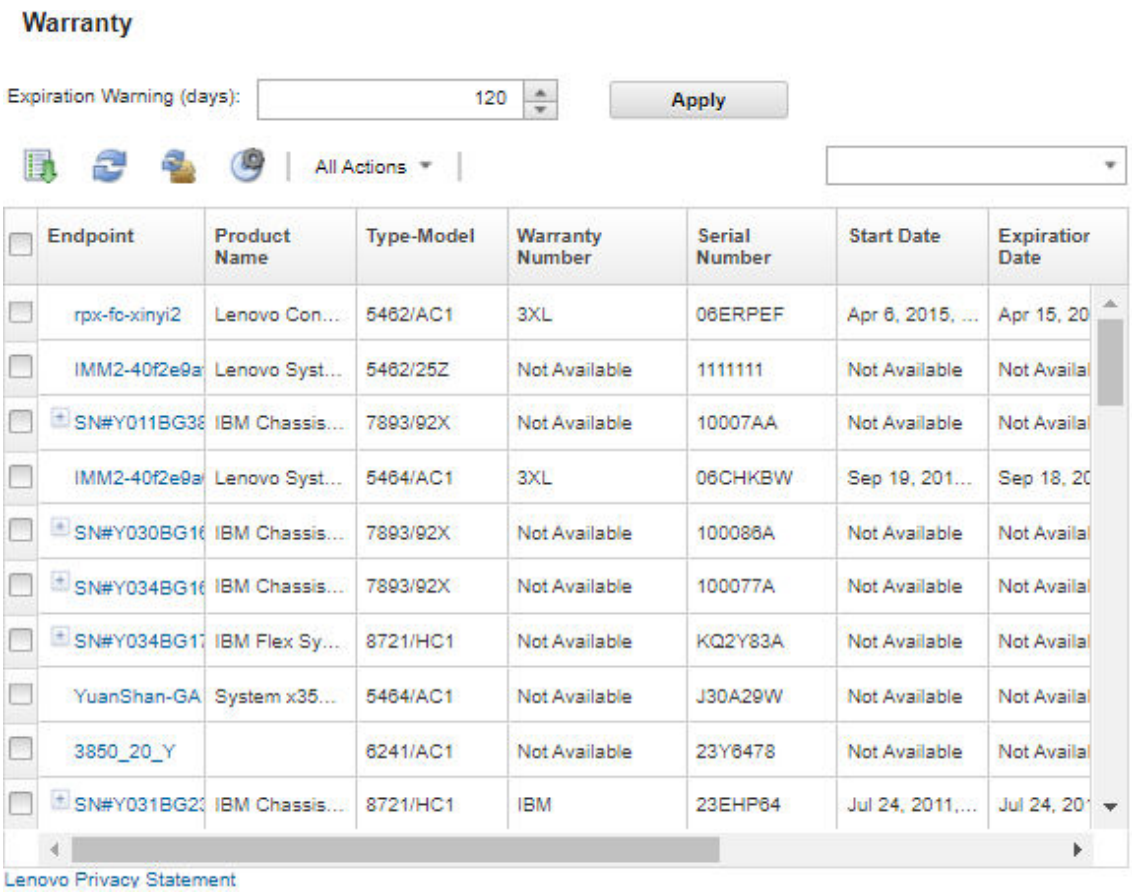
手順

管理対象デバイスの保証ステータスを表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、**「管理」 ➡ 「サービスおよびサポート」**をクリックします。

ステップ 2. 左ナビゲーションの**「保証」**をクリックして、「保証」ページを表示します。

このページには、各管理対象デバイスの保証情報 (開始日、停止日、ステータス) をリストした表が表示されます。



終了後

「保証」ページで、以下の操作を実行できます。

- 「**失効の警告**」フィールドを使用して、管理対象デバイスの保証の有効期限に関する警告を受けたい場合に設定します。デフォルトは、保証の有効期限が切れる 30 日前です。
- 「**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。
- すべての管理対象デバイスにおける保証状況を CSV ファイルにエクスポートする。「**CSV としてダウンロード**」アイコン ( ) をクリックします。
- 「**サーバー・リストを最新の情報に更新**」 アイコン ( ) をクリックして、すべての管理対象デバイスの保証情報を最新表示にする。

自動問題通知のセットアップ

特定の管理対象デバイスでサービス可能イベントが発生した場合にサービス・データを優先サービス・プロバイダーに自動的に送信するサービス・フォワーダーを作成できます。デバイスのサービス・データを Lenovo サポート に送信 (コール・ホーム) するか、Lenovo アップロード・ファシリティーを使用して Lenovo サービス技術員に送信するか、SFTP を使用して別のサービス・プロバイダーに送信できます。

コール・ホーム、Lenovo アップロード・ファシリティー、または SFTP のサービス・フォワーダー向けのサービス・フォワーダーは、最大 50 個まで作成し有効化することができます。

Lenovo サポートへの自動問題通知 (コール・ホーム) のセットアップ

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) を特定の管理対象デバイスから受信した場合に問題を解決できるように、コール・ホーム を使用してすべての管理対象デバイスのサービス・データを Lenovo サポート に自動的に送信するようにサービス・フォワーダーを構成できます。このサービス・フォワーダーは、「デフォルト・コール・ホームと呼ばれます。」

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。有効の場合、コール・ホームは、デバイスからのハードウェア障害の報告時、またはユーザーが手動コール・ホームを開始するように選択したときに、サービス・データを Lenovo アップロード・ファシリティーに送信します。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 アップロード・ファシリティ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 アップロード・ファシリティーでのサービス・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。

始める前に

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。

コール・ホーム を有効にする前に、Lenovo XClarity Administrator 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 Administrator 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 Administrator 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 Administrator 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、プロキシー・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、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。

コール・ホームを構成後、**デフォルトの Lenovo コール・ホーム**・サービス・フォワーダーが、「サービス・フォワーダー」ページに追加されます。このフォワーダーを編集すると追加設定を構成できます。これには、このフォワーダーに関連付けられているデバイスが含まれます。すべてのデバイスはデフォルトでマッチされます。

注意：「**すべてのデバイスと突き合わせ**」が無効になっている場合、有効なコール・ホーム・フォワーダーで個別に、またはリソース・グループを通じて明示的に選択されていないデバイスは、保守可能なイベントのために Lenovo サポートにコール・ホームを開始*しません*。

現在、特定のデバイスの除外コール・ホーム・オプションはありません。保守可能なイベントに対してコール・ホームではないデバイスのサブセットを取得する可能性が低い状況では、目的のデバイスを回避する静的リソース・グループと動的リソース・グループの混在を作成し、それらのリソース・グループをコール・ホーム・フォワーダーに追加できます。

注意：コール・ホーム・フォワーダーで「**すべてのデバイスと突き合わせ**」が有効になっていない場合、コール・ホームはデバイスで開始されません。そのため、最終手段のフォワーダーとして「**すべてのデバイスと突き合わせ**」が有効なデフォルトのコール・ホーム・フォワーダーを 1 つ以上使用することをお勧めします。

重要：

- Lenovo XClarity Administrator で コール・ホーム サービス・フォワーダーを有効にしている場合、重複する問題レコードが作成されないようにするために、各管理対象デバイスで コール・ホーム が無効になります。XClarity Administrator を使用したデバイスの管理をやめる場合、または XClarity

Administrator での コール・ホーム を無効にする場合は、後で各デバイスで コール・ホーム を再度有効にする代わりに、XClarity Administrator からすべての管理対象デバイスで コール・ホーム を再度有効にできます。 コール・ホームのサービス・フォワーダーが無効な場合にすべての管理対象デバイスでコール・ホームを再度有効化する方法については、すべての管理対象デバイスでのコール・ホーム の再有効化を参照してください。

- XClarity Administrator では ThinkAgile および ThinkSystem デバイスでのコール・ホームはサポートされていますが、一部の ThinkAgile および ThinkSystem デバイスのベースボード管理コントローラーにコール・ホームのサポートは含まれていません。そのため、これらのデバイス自体でコール・ホームを有効にしたり無効にしたりすることはできません。コール・ホームは、その XClarity Administrator レベルのデバイスに対してのみ有効にすることができます。

このタスクについて

*サービス・フォワーダー*は、保守可能イベントが発生した際にサービス・データ・ファイルを送信する宛先に関する情報を定義します。サービス・フォワーダーは最大 50 件まで定義できます。

- **コール・ホームサービス・フォワーダーが構成されていない場合**、新しいサービス要求 Web ページ 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・ファイルの収集とダウンロードについては、Lenovo XClarity Administrator サービス・ファイルの収集とダウンロードおよびXClarity Administrator オンライン・ドキュメントのデバイスのサービス・データの収集とダウンロード。
- **コール・ホームサービス・フォワーダーが構成されているが有効になっていない場合**、いつでも コール・ホーム 機能を使用してサービス・チケットを*手動*で開き、サービス・ファイルを収集して Lenovo サポート・センター に転送できます。詳しくは、ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照してください。
- **コール・ホーム・サービス・フォワーダーが構成され、有効になると**、XClarity Administrator は、*自動的に*サービス・チケットを開いて、サービス・データを収集し、アーカイブ・ファイルとして保存します。また、サービス可能なイベントが発生すると、サービス・アーカイブ・ファイルを Lenovo アップロード・ファシリティーに転送するので、問題に対処できます。アーカイブ・サービス・ファイルには、デバイスおよび XClarity Administrator のサービス・データが含まれます。

  注：ThinkSystem V3 および V4 サーバー (XCC2 または XCC3 を使用)の場合、XClarity Administrator はリポジトリーの 2 つのファイルにサービス・データを保存します。

  – **サービス・ファイル**。(.zip) このファイルには、デバイス・サービス情報とインベントリーが簡単に読み取り可能な形式で含まれています。このファイルは、サービス可能イベントが発生すると、Lenovo アップロード・ファシリティーに自動的に送信されます。
  – **デバッグ・ファイル**。(.tzz) このファイルには、Lenovo アップロード・ファシリティーで使用するためのすべてのデバイス・サービス情報、インベントリー、およびデバッグ・ログが含まれています。問題を解決するために追加情報が必要な場合は、このファイルを Lenovo サポートに手動で送信できます。

  他のデバイスの場合、XClarity Administrator はリポジトリーの単一のサービス・ファイルにサービス・データファイル (XClarity Administrator およびデバイス・サービス情報、インベントリー、デバッグ・ログなど) を保存します。このファイルは、サービス可能イベントが発生すると、Lenovo サポート・センター に送信されます。

  デバイスの繰り返しイベントに対してサービス・チケットが開かれている場合、そのデバイスに対するそのイベントに対してコール・ホームは抑止されます。ThinkAgile および ThinkSystem デバイスのイベントに対してサービス・チケットが開かれている場合、そのデバイスに対する同様のイベントに対してもコール・ホームは抑止されます。ThinkAgile および ThinkSystem イベントは、***xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx*** の形式の 16 文字の文字列です (例: `806F010D0401FFFF`)。イベントは、読み取りタイプ、センサー・タイプ、およびエンティティー ID が同じである場合に似ています。たとえば、特定の ThinkAgile または ThinkSystem デバイスでイベント 806f010d0401ffff のサービス・チケットが開かれている場合、そのデバイスで発

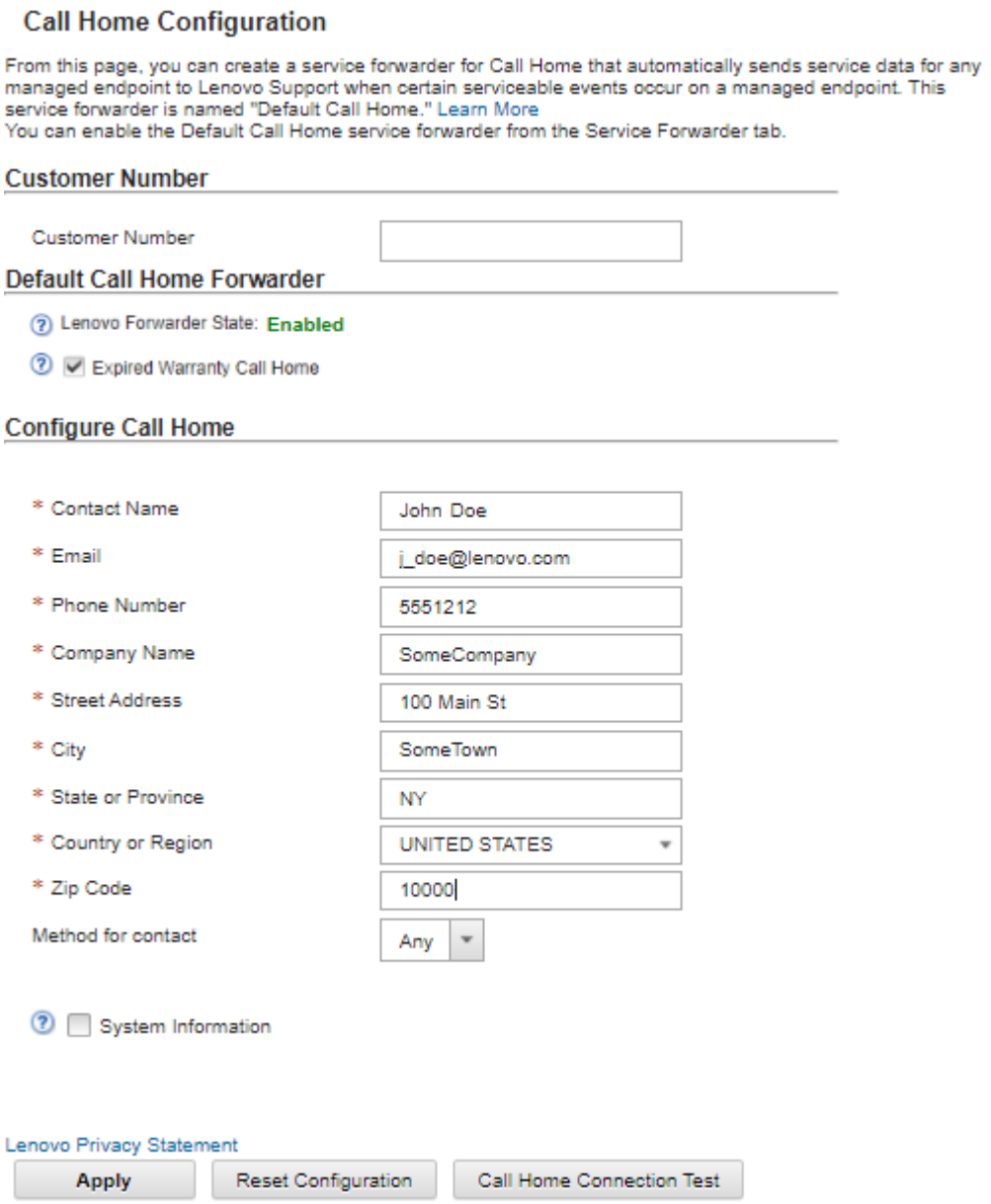
生した *xx*6F01*xx*04*xxxxxx* (ここで、*x* は任意の英数字) などのイベント ID を持つイベントはすべて抑止されます。

コール・ホームサービス・フォワーダーによって自動的に開かれたサービス・チケットの表示の詳細については、XClarity Administratorのオンライン・ドキュメントのサービス・チケットとステータスの表示。

手順

コール・ホーム のサービス・フォワーダーをセットアップするには、以下の手順を実行します。

- すべての管理対象デバイスで コール・ホーム をセットアップします (現行および将来)。
  1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。
  2. 左ナビゲーションの「**コール・ホーム構成**」をクリックして「コール・ホーム構成」ページを表示します。



3. (オプション) XClarity Administrator による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。

   ヒント: お客様番号は、Lenovo XClarity Pro 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。

4. (オプション)「**有効期限が切れた保証のコール・ホーム**」をクリアし、保証の有効期限が切れたデバイスについては、コール・ホームによってサービス・チケットが自動的に開かないようにします。

   注：このオプションは、保証の有効期限が切れたデバイスのサービス・チケットを手動で開くことを妨げるものではありません

5. 連絡先と場所の情報を入力します。
6. Lenovo サポートによる連絡方法を選択します。
7. (オプション) システム情報を入力します。
8. 「**適用**」をクリックします。

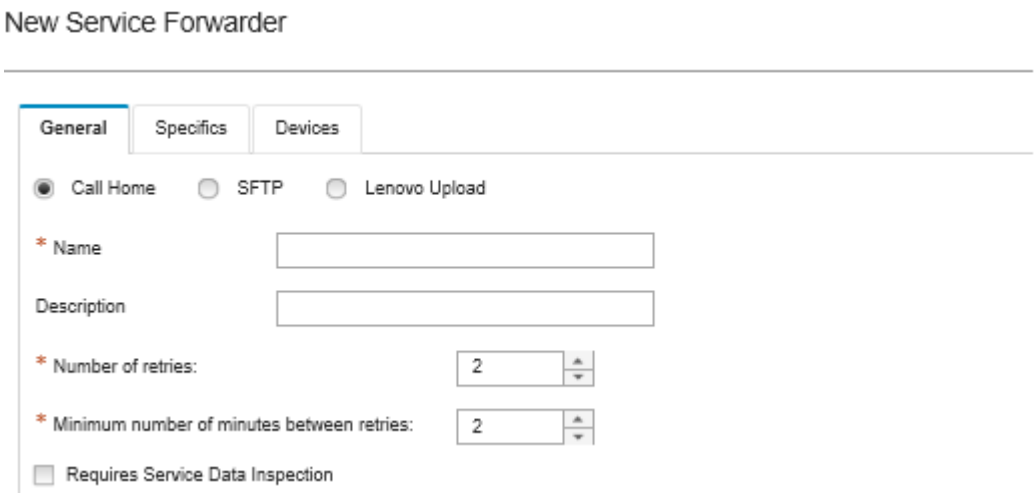
   指定されたお問い合わせ先情報を使用して、「デフォルトのコール・ホーム」という名前の コール・ホーム サービス・フォワーダーがすべての管理対象デバイスに対して作成されます。

9. 「デフォルトのコール・ホーム」サービス・フォワーダーを有効にしてテストします。
   a. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。
   b. 「デフォルトのコール・ホーム」サービス・フォワーダーの「**ステータス**」列で「**有効**」を選択します。
   c. 「デフォルトのコール・ホーム」サービス・フォワーダーを選択し、「**サービス・フォワーダーのテスト**」をクリックして、サービス・フォワーダー用のテスト・イベントを生成して XClarity Administrator が Lenovo サポート・センターと通信できることを確認します。

      XClarity Administrator のメニュー・バーで「**監視**」 → 「**ジョブ**」の順にクリックすると、テストの進行を監視できます。

      注：テストの前にサービス・フォワーダーを有効にする必要があります。

- 特定の管理対象デバイスの コール・ホーム をセットアップします。
  1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。
  2. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。
  3. 「**サービス・フォワーダーの作成**」アイコン ( ) をクリックして、「新規サービス・フォワーダー」ダイアログを表示します。
  4. 「**全般**」タブをクリックします。



a. 「**コール・ホーム**」をサービス・フォワーダーとして選択します。
b. サービス・フォワーダーの名前と説明を入力します。
c. 自動通知の再試行回数を指定します。デフォルトは 2 です。
d. 再試行の最小間隔を分で指定します。デフォルトは 2 です。
e. (オプション) サービス・データ・ファイルを転送する前に検査する場合は、「**サービス・データの検査を要求する**」をクリックし、サービス・ファイルの検査が必要な場合に通知を送信する連絡先のメール・アドレスをオプションで指定します。

5. 「**固有**」タブで、連絡先とシステムの情報を入力します。

   ヒント: 「コール・ホーム構成」ページで構成したものと同じ連絡先と場所の情報を使用するには、「**構成**」ドロップダウン・メニューで「**全般構成**」を選択します。

6. 「**デバイス**」タブをクリックし、このサービス・フォワーダーによってサービス・ファイルを転送する管理対象デバイスおよびリソース・グループを選択します。

   ヒント: すべての管理対象デバイスのサービス・ファイル (現行および将来) を転送するには、「**すべてのデバイスと突き合わせ**」チェックボックスにチェックを入れます。

7. 「**作成**」をクリックします。サービス・フォワーダーが「サービスおよびサポート」ページに追加されます。
8. 「サービス・フォワーダー」ページの「**ステータス**」列で「**有効**」を選択してサービス・フォワーダーを有効にします。
9. サービス・フォワーダーを選択し、「**サービス・フォワーダーのテスト**」をクリックして、サービス・フォワーダー用のテスト・イベントを生成して XClarity Administrator が Lenovo サポート・センターと通信できることを確認します。

   XClarity Administrator のメニュー・バーで「**監視**」 → 「**ジョブ**」の順にクリックすると、テストの進行を監視できます。

   注：テストの前にサービス・フォワーダーを有効にする必要があります。

終了後

「サービスおよびサポート」ページからは、以下の操作も実行できます。

- 「**サービス・データの検査を要求する**」が選択されていて、サービス・フォワーダーに関連付けられている管理対象デバイスから保守可能なイベントを受信した場合、サービス・プロバイダーにファイルを転送する前にサービス・ファイルを検査する必要があります。詳しくは、を参照してください。

- 管理対象デバイスでコール・ホームが有効か無効かを確認するには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックし、「**コール・ホーム・ステータス**」列で状態を確認します。

  ヒント:「**コール・ホームステータス**」列に「不明な状態」が表示されている場合は、正しいステータスを表示するために Web ブラウザーを最新の情報に更新します。
- 特定の管理対象デバイスのサポートの連絡先と場所の情報を定義するには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**連絡先プロファイルの作成**」アイコン ( ) または「**連絡先プロファイルの編集**」アイコン ( ) をクリックします。管理対象デバイスの連絡先と場所の情報は、コール・ホームがLenovo サポート・センターに送信するサービス・チケットに含まれます。固有の連絡先と場所の情報が管理対象デバイスに指定されている場合は、その情報がサービス・チケットに含まれます。それ以外の場合は、「**コール・ホーム 構成**」ページまたは「**サービス・フォワーダー**」ページで指定されている XClarity Administrator コール・ホーム 構成の一般情報が使用されます。詳しくは、Lenovo サポート・センターを参照してください。詳しくは、特定のデバイスのサポート連絡先の定義を参照してください。
- Lenovo サポート・センター に送信されたサービス・チケットを表示するには、左ナビゲーションの「**サービス・チケットのステータス**」をクリックします。このページには、コール・ホーム・サービス・フォワーダーによって自動または手動で開かれたサービス・チケット、ステータス、Lenovo サポート・センターに送信されたサービス・ファイルが一覧表示されます。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。
- 特定のデバイスのサービス・データを収集するには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**サービス・データの収集**」アイコン ( ) をクリックします。詳しくは、デバイスのサービス・データの収集とダウンロードを参照してください。
- 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・データを収集して、それらのファイルを Lenovo サポート・センターに送信するには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**すべての操作**」 ➞ 「**手動コール・ホームの実行**」をクリックします。Lenovo サポート・センター が追加の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。

  詳しくは、ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照してください。
- すべての管理対象デバイスでコール・ホームを再度有効にするには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックし、「**すべての操作**」 ➞ 「**すべてのデバイスでコール・ホームを有効化する**」をクリックします。

  Lenovo XClarity Administrator で コール・ホーム サービス・フォワーダーを有効にしている場合、重複する問題レコードが作成されないようにするために、各管理対象デバイスで コール・ホーム が無効になります。XClarity Administrator を使用したデバイスの管理をやめる場合、または XClarity Administrator での コール・ホーム を無効にする場合は、後で各デバイスで コール・ホーム を再度有効にする代わりに、XClarity Administrator からすべての管理対象デバイスで コール・ホーム を再度有効にできます。

Lenovo アップロード・ファシリティーへの自動問題通知のセットアップ

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) を特定の管理対象デバイスから受信した場合に問題を解決できるように、Lenovo アップロード・ファシリティーを使用してすべての管理対象デバイスのサービス・データを Lenovo サービス技術員に自動的に送信するサービス・フォワーダーを作成できます。このサービス・フォワーダーの名前は「デフォルトの Lenovo アップロード・ファシリティー」です。

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。ビジネス・データが送信されることはありません。Lenovo アップロード・ファシリティーでのサービス・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。

始める前に

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。

サービス・フォワーダーをセットアップする前に、Lenovo XClarity Administrator 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。ポートについて詳しくは、XClarity Administrator 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。

Lenovo アップロード・ファシリティーによって要求された必要なインターネット・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 Administrator 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 Administrator 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、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。

注：複数のサービス・フォワーダーが同じデバイスでセットアップされている場合、いずれかのサービス・フォワーダーのみサービス・データを転送します。使用するメールとアップロード URL は、どのサービス・フォワーダーが最初にトリガーされたかによって異なります。

このタスクについて

*サービス・フォワーダー*は、保守可能イベントが発生した際にサービス・データ・ファイルを送信する宛先に関する情報を定義します。サービス・フォワーダーは最大 50 件まで定義できます。

- **Lenovo アップロード・ファシリティー・サービス・フォワーダーが構成されているが有効になっていない場合**、収集されたサービス・ファイルをいつでも*手動で*Lenovo アップロード・ファシリティーに転送できます。詳しくは、ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照してください。
- **Lenovo アップロード・ファシリティー・サービス・フォワーダーが構成され、有効になると、** XClarity Administrator は、*自動で*サービス・データを収集し、サービス可能なイベントが発生すると、サービス・ファイルを Lenovo アップロード・ファシリティーに転送するので、問題に対処できます。

  ThinkSystem V3 および V4 サーバー (XCC2 または XCC3 を使用)の場合、XClarity Administrator はリポジトリーの 2 つのファイルにサービス・データを保存します。

  - **サービス・ファイル**。(.zip) このファイルには、サービス情報とインベントリーが簡単に読み取り可能な形式で含まれています。このファイルは、サービス可能イベントが発生すると、Lenovo アップロード・ファシリティーに自動的に送信されます。
  - **デバッグ・ファイル**。(.tzz) このファイルには、Lenovo サポートで使用するためのすべてのサービス情報、インベントリー、およびデバッグ・ログが含まれています。問題を解決するために追加情報が必要な場合は、このファイルを Lenovo サポートに手動で送信できます。

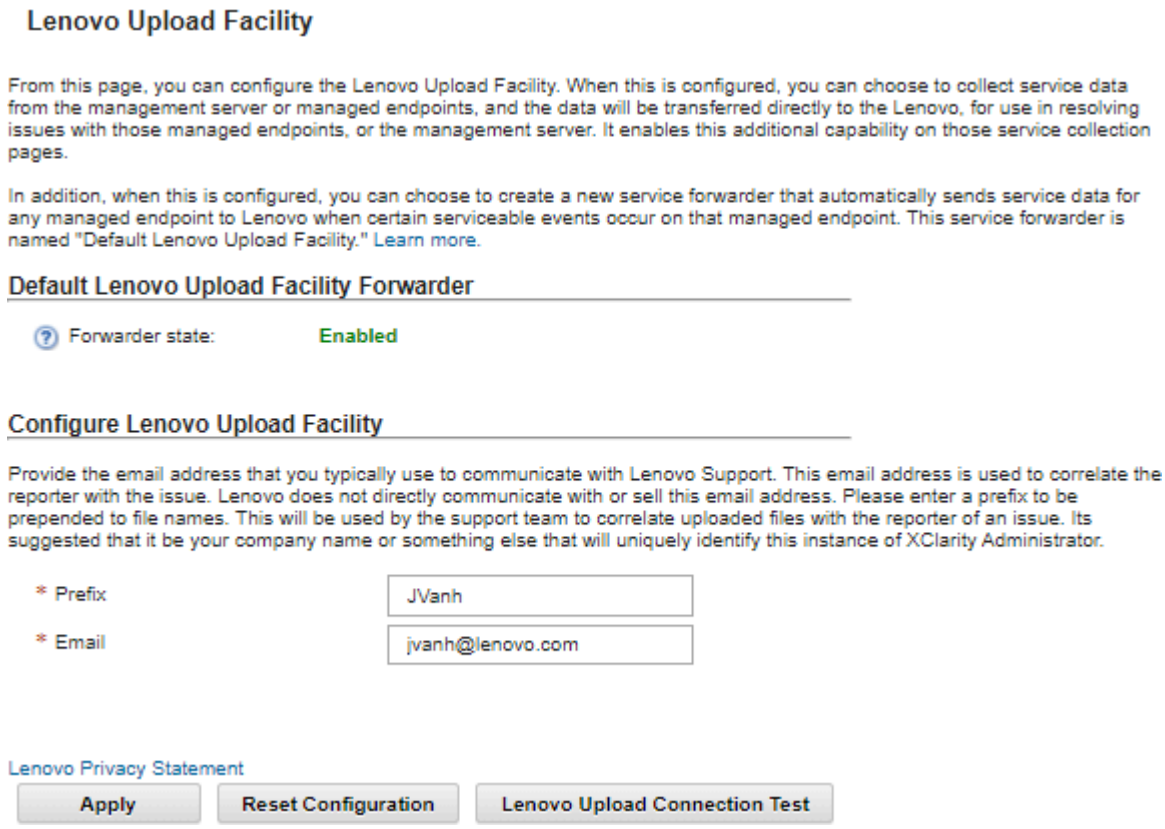
  他のデバイスの場合、XClarity Administrator はリポジトリーの単一のサービス・ファイルにサービス・データファイル (サービス情報、インベントリー、デバッグ・ログなど) を保存します。このファイルは、サービス可能イベントが発生すると、Lenovo アップロード・ファシリティーに送信されます。

手順

Lenovo アップロード・ファシリティーのサービス・フォワーダーをセットアップする以下の手順を実行します。

- すべての管理対象デバイスの Lenovo アップロード・ファシリティーにサービス・フォワーダーをセットアップします。
  1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。

2. 左ナビゲーションの「**Lenovo アップロード・ファシリティー**」をクリックして、「Lenovo アップロード・ファシリティー」ページを表示します。



3. Lenovo サポートにより提供されたメール・アドレスと URL を入力します。
4. 「**適用**」をクリックします。

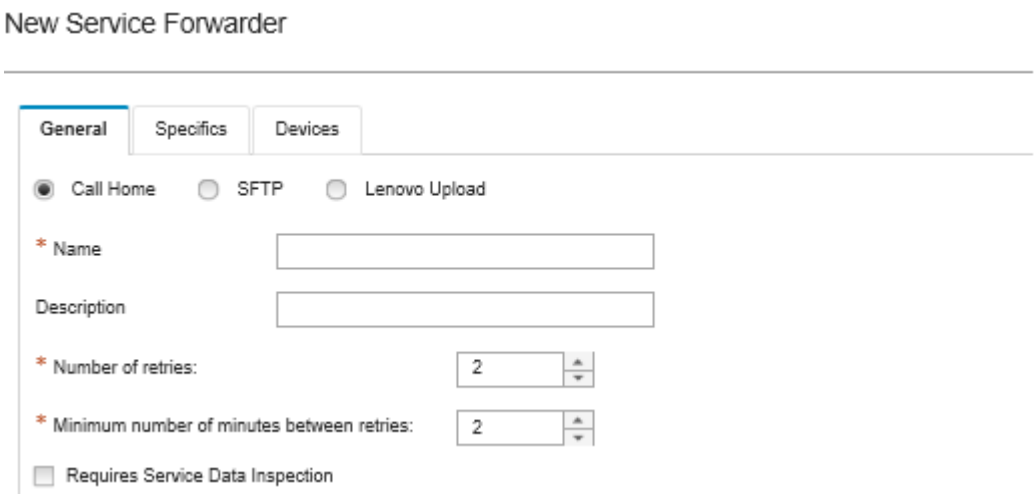
   指定されたお問い合わせ先情報を使用して、「Default Lenovo Upload Facility」という名前のサービス・フォワーダーがすべての管理対象デバイスに対して作成されます。
5. 「Default Lenovo Upload Facility」サービス・フォワーダーを有効にしてテストします。
   a. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。
   b. 「Default Lenovo Upload Facility」サービス・フォワーダーの「**ステータス**」列で「**有効**」を選択します。
   c. 「Default Lenovo Upload Facility」サービス・フォワーダーを選択し、「**サービス・フォワーダーのテスト**」をクリックして、サービス・フォワーダー用のテスト・イベントを生成して XClarity Administrator が Lenovo アップロード・ファシリティーと通信できることを確認します。

      XClarity Administrator のメニュー・バーで「**監視**」 → 「**ジョブ**」の順にクリックすると、テストの進行を監視できます。

      注：テストの前にサービス・フォワーダーを有効にする必要があります。

- 特定の管理対象デバイスの Lenovo アップロード・ファシリティーにサービス・フォワーダーをセットアップします。
  1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。
  2. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。

3. 「**サービス・フォワーダーの作成**」アイコン ( ) をクリックして、「新規サービス・フォワーダー」ダイアログを表示します。
4. 「**General**」タブをクリックします。



   a. サービス・フォワーダーの「**Lenovo アップロード**」を選択します。
   b. サービス・フォワーダーの名前と説明を入力します。
   c. 自動通知の再試行回数を指定します。デフォルトは 2 です。
   d. 再試行の最小間隔を分で指定します。デフォルトは 2 です。
   e. (オプション) サービス・ファイルを転送する前に検査する場合は、「**サービス・データの検査を要求する**」をクリックし、サービス・ファイルの検査が必要な場合に通知を送信する連絡先のメール・アドレスをオプションで指定します。
5. 「**固有**」タブをクリックし、Lenovo サポートにより提供されたメール・アドレスとアップロード URL を入力します。
6. 「**デバイス**」タブをクリックし、このサービス・フォワーダーによってサービス・データを転送する管理対象デバイスおよびリソース・グループを選択します。

   ヒント: すべての管理対象デバイスのサービス・データ (現行および将来) を転送するには、「**すべてのデバイスと突き合わせ**」チェックボックスにチェックを入れます。
7. 「**作成**」をクリックします。サービス・フォワーダーが「サービスおよびサポート」ページに追加されます。
8. 「サービスおよびサポート」ページの「**ステータス**」列で「**有効**」を選択してサービス・フォワーダーを有効にします。
9. サービス・フォワーダーを選択し、「**サービス・フォワーダーのテスト**」をクリックして、各サービス・フォワーダー用のテスト・イベントを生成して XClarity Administrator が Lenovo アップロード・ファシリティーに転送できることを確認します。

   注：テストの前にサービス・フォワーダーを有効にする必要があります。

終了後

「サービスおよびサポート」ページからは、以下の操作も実行できます。

- 「**サービス・データの検査を要求する**」が選択されていて、サービス・フォワーダーに関連付けられている管理対象デバイスから保守可能なイベントを受信した場合、サービス・プロバイダーにファイルを転送する前にサービス・ファイルを検査する必要があります。詳しくは、サービス・ファイルの検査を参照してください。

- サービス・フォワーダー情報を変更する。左ナビゲーションの「**サービス・フォワーダー**」をクリックして「**サービス・フォワーダーの編集**」アイコン ( ) をクリックします。
- サービス・プロバイダーを有効または無効にする。「**サービス・フォワーダー**」をクリックし、「**ステータス**」列の「**有効**」または「**無効**」をクリックします。
- サービス・プロバイダーを削除する。「**サービス・フォワーダー**」をクリックして「**サービス・フォワーダーの削除**」アイコン ( ) をクリックします。
- 左側のナビゲーションで「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**サービス・データの収集**」アイコン ( ) をクリックして、特定の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・データの収集とダウンロードを参照してください。

優先サービス・プロバイダーへの自動問題通知のセットアップ

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) を特定の管理対象デバイスから受信した場合に問題を解決できるように、SFTP を使用してサービス・データを優先サービス・プロバイダーに自動的に送信するようにサービス・フォワーダーを構成できます。

始める前に

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。

サービス・フォワーダーをセットアップにする前に、XClarity Administrator 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 Administrator 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。

サービス・プロバイダー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。

Lenovo サポート を使用することを選択した場合、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 Administrator 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 Administrator 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、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。

このタスクについて

*サービス・フォワーダー*は、保守可能イベントが発生した際にサービス・データ・ファイルを送信する宛先に関する情報を定義します。サービス・フォワーダーは最大 50 件まで定義できます。

サービス・フォワーダーごとに、サービス・データを Lenovo サポート (*コール・ホーム* と呼ばれます)、Lenovo アップロード・ファシリティ、または SFTP を使用して別のサービス・プロバイダーに自動的に転送することを選択できます。コール・ホーム のサービス・フォワーダーのセットアップについては、XClarity Administrator オンライン・ドキュメントの 自動問題通知のセットアップ。Lenovo アップロード・ファシリティーのサービス・フォワーダーのセットアップについては、XClarity Administrator オンライン・ドキュメントのLenovo アップロード・ファシリティーへの自動問題通知のセットアップ。

サービス・フォワーダーが構成され SFTP が有効になっている場合、XClarity Administrator は*自動的に*サービス・データを収集してサービス・ファイルを優先サービス・プロバイダーの指定された SFTP サイトに転送します。

ThinkSystem V3 および V4 サーバー (XCC2 または XCC3 を使用)の場合、XClarity Administrator はリポジトリーの 2 つのファイルにサービス・データを保存します。

- **サービス・ファイル**。(.zip) このファイルには、サービス情報とインベントリーが簡単に読み取り可能な形式で含まれています。このファイルは、サービス可能イベントが発生すると、優先サービス・プロバイダーに自動的に送信でされます。
- **デバッグ・ファイル**。(.tzz) このファイルには、Lenovo サポートで使用するためのすべてのサービス情報、インベントリー、およびデバッグ・ログが含まれています。問題を解決するために追加情報が必要な場合は、このファイルを Lenovo サポートに手動で送信できます。

他のデバイスの場合、XClarity Administrator はリポジトリーの単一のサービス・ファイルにサービス・データファイル (サービス情報、インベントリー、デバッグ・ログなど) を保存します。このファイルは、サービス可能イベントが発生すると、優先サービス・プロバイダーに送信でされます。

注：複数の SFTP サービス・フォワーダーが同じデバイスでセットアップされている場合、いずれかのサービス・フォワーダーのみサービス・データを転送します。使用するアドレスとポートは、どのサービス・フォワーダーが最初にトリガーされたかによって異なります。

手順

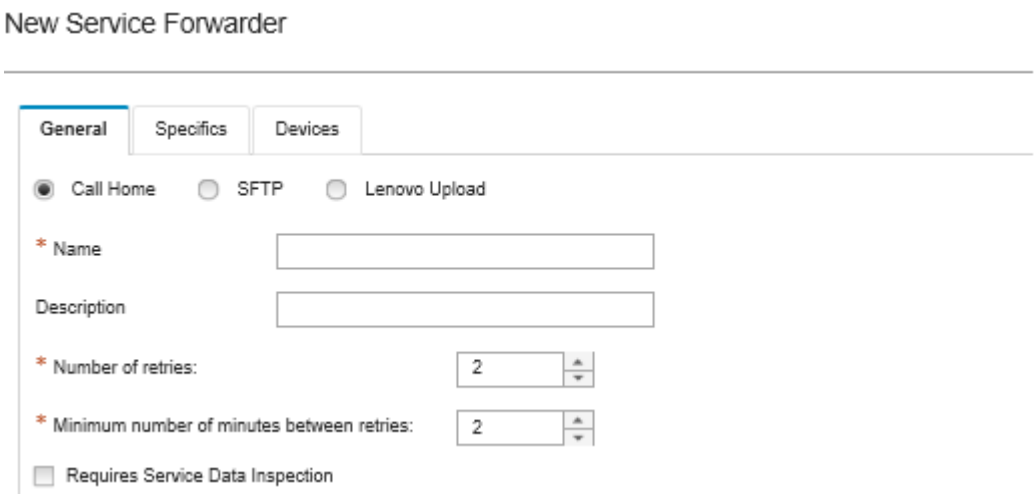
サービス・フォワーダーを定義して有効にするには、以下のステップを実行します。

ステップ 1. XClarity Administrator メニュー・バーで、**管理 → 「サービスおよびサポート」**をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。

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

ステップ 4. 「**General**」タブをクリックします。



1. サービス・フォワーダーの「**SFTP**」を選択します。
2. サービス・フォワーダーの名前と説明を入力します。
3. 自動通知の再試行回数を指定します。デフォルトは 2 です。
4. 再試行の最小間隔を分で指定します。デフォルトは 2 です。
5. (オプション) サービス・ファイルを転送する前に検査する場合は、「**サービス・データの検査を要求する**」をクリックし、サービス・ファイルの検査が必要な場合に通知を送信する連絡先のメール・アドレスをオプションで指定します。

ステップ 5. 「**固有**」タブで、以下の情報を入力します。

- SFTP サーバーの IP アドレスとポート番号
- SFTP サーバーへの認証に使用されるユーザー ID とパスワード

ステップ 6. 「**デバイス**」タブをクリックし、このサービス・フォワーダーによってサービス・データを転送する管理対象デバイスおよびリソース・グループを選択します。

ヒント: すべての管理対象デバイスのサービス・データ (現行および将来) を転送するには、「**すべてのデバイスと突き合わせ**」チェックボックスにチェックを入れます。

ステップ 7. 「**作成**」をクリックします。サービス・フォワーダーが「サービスおよびサポート」ページに追加されます。

ステップ 8. 「サービスおよびサポート」ページの「**ステータス**」列で「**有効** 」を選択してサービス・フォワーダーを有効にします。

ステップ 9. 除外イベントのリストに含まれるサービス可能イベントが自動的に問題レポートを開かないようにするには、「**除外イベント時に問題レポートを開きますか?**」という質問の隣にある「**いいえ**」を選択します。

ステップ 10. サービス・フォワーダーを選択し、「**サービス・フォワーダーのテスト**」をクリックしてテスト・イベントを作成します。それぞれサービス・フォワーダーについて、XClarity Administrator が各サービス・プロバイダーと通信できることを確認します。

注：テストの前にサービス・フォワーダーを有効にする必要があります。

終了後

「サービスおよびサポート」ページからは、以下の操作も実行できます。

- 「**サービス・データの検査を要求する**」が選択されていて、サービス・フォワーダーに関連付けられている管理対象デバイスから保守可能なイベントを受信した場合、サービス・プロバイダーにファイルを転送する前にサービス・ファイルを検査する必要があります。詳しくは、サービス・ファイルの検査を参照してください。
- サービス・フォワーダー情報を変更する。左ナビゲーションの「**サービス・フォワーダー**」をクリックして「**サービス・フォワーダーの編集**」アイコン ( ) をクリックします。
- サービス・プロバイダーを有効または無効にする。「**サービス・フォワーダー**」をクリックし、「**ステータス**」列の「**有効**」または「**無効**」をクリックします。
- サービス・プロバイダーを削除する。「**サービス・フォワーダー**」をクリックして「**サービス・フォワーダーの削除**」アイコン ( ) をクリックします。
- 特定の管理対象デバイスのサポートの連絡先と場所の情報を定義するには、左側のナビゲーションで「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**連絡先プロファイルの作成**」アイコン ( ) または「**連絡先プロファイルの編集**」アイコン ( ) をクリックします。管理対象デバイスの連絡先と場所の情報は、コール・ホームが Lenovo サポート・センター に作成する問題レコードに含まれます。固有の連絡先と場所の情報が管理対象デバイスに指定されている場合は、その情報が問題レコードに含まれます。それ以外の場合は、XClarity Administrator コール・ホーム構成 (「**コール・ホーム構成**」ページまたは「**サービス・フォワーダー**」ページ) で指定されている一般情報が使用されます。詳しくは、特定のデバイスのサポート連絡先の定義を参照してください。
- 「**エンドポイント・アクション**」をクリックしてデバイスを選択し、「**サービス・データの収集**」アイコン ( ) をクリックして、特定の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・データの収集とダウンロードを参照してください。

これらのサービスおよびサポート・タスクについて詳しくは、サービスおよびサポートの操作を参照してください。

サービス・リカバリー・パスワードの変更

Lenovo XClarity Administrator が応答しなくなりリカバリーできない場合、その XClarity Administrator インスタンスのサービス・データとログを収集してダウンロードできます。サービスにアクセスしてデータを収集およびダウンロードするには、サービス・リカバリー・パスワードが必要です。

始める前に

パスワードを変更するには、**lxc-service-admin** または **lxc-supervisor** 権限が必要です。

注：後で使用できるように記録しておいてください。このパスワードを使用しないで、応答しない管理ハブをリカバリーすることはできません。

サービス・リカバリー・パスワードの使用について詳しくは、応答しない Lenovo XClarity Administrator のサービス・ファイルの収集とダウンロードを参照してください。

手順

サービス・リカバリー・パスワードを変更するには、以下の手順に従ってください。

ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**サービス・リカバリー・パスワード**」をクリックして、「サービス・リカバリー・パスワード」ページを表示します。

ステップ 3. 新しいパスワードの入力

パスワードには、**16 ～ 256** 文字 (1 つ以上の大文字と小文字の英字、数字、特殊文字を含む) が含まれている必要があります。

ステップ 4. 「**適用**」をクリックします。

サービス・ファイルの検査

サービス・ファイルを送信する前にファイルの検査と同意を必須にするようにサービス・フォワーダーをセットアップできます。

このタスクについて

サービス・フォワーダー・テーブルの「**注意が必要**」列は、サービス・プロバイダーに転送する前に検査を必要とするサービス・ファイルがあるかどうかを示しています。検査が必要なサービス・ファイルが 1 つ以上ある場合は、列に「**はい**」が表示されます。その他の場合は、「**いいえ**」が表示されます。

手順

特定のサービス・ファイルをサービス・プロバイダーに転送するには、以下のステップを実行します。

ステップ 1. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、サービス・フォワーダーのテーブルを表示します。

ステップ 3. 「**注意が必要**」列の「**はい**」リンクをクリックして、検査が必要なサービス・ファイルのリストを表示する「注意が必要」ダイアログを表示します。

ステップ 4. サービス・ファイルを 1 つ以上選択し、「**ダウンロード**」をクリックしてサービス・ファイルをダウンロードし、検査します。

ステップ 5. 再度サービス・ファイルを 1 つ以上選択し、「同意する」をクリックして構成されたサービス・プロバイダーに対するファイル転送を開始します。

注：代わりに「**同意しない**」を選択すると、サービス・ファイルは「注意が必要」ダイアログからは消えますが、リポジトリーには削除されるまで残ります。

特定のデバイスのサポート連絡先の定義

デバイスが複数のユーザーによって管理されている場合、1 つ以上の特定のデバイスのサポートお問い合わせ先情報を一意にすると役立ちます。

このタスクについて

デバイスにサポートのお問い合わせ先情報が定義されている場合、そのデバイスのコール・ホーム によって自動的に開かれる問題レコードにデバイス固有の情報が含められます。デバイス固有の情報が定義されていない場合、「**サービス・フォワーダー**」ページまたは「**コール・ホーム 構成**」ページで定義された Lenovo XClarity Administrator の一般的なお問い合わせ先情報が代わりに含められます。

手順

特定のデバイスのサポート連絡先と場所の情報を定義するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左側のナビゲーションで「**エンドポイント・アクション**」をクリックして、「エンドポイント・アクション」ページを表示します。

ステップ 3. 1 つ以上のデバイスを選択し、「**連絡先プロファイルの作成**」アイコン ( ) ををクリックして、「連絡先プロファイルの作成」ダイアログを表示します。

ステップ 4. 要求されたフィールドを入力し、「**保存**」をクリックします。

終了後

デバイスのお問い合わせ先情報を定義した後、デバイスを選択して「**連絡先プロファイルの編集**」アイコン ( ) または「**連絡先プロファイルの削除**」アイコン ( ) をクリックすることで、お問い合わせ先情報を変更または削除できます。

注：選択したデバイスの連絡先プロファイルが存在しない場合、連絡先プロファイルの編集を試みると、「連絡先プロファイルの作成」ダイアログが表示されます。

デバイスのサービス・データの収集とダウンロード

管理対象デバイスに問題が発生し、解決にサービス・プロバイダーのサポートが必要な場合、Lenovo XClarity Administrator Web インターフェースを使用し、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、デバッグログなど) を手動で収集し、問題の原因の特定に役立てることができます。サービス・データは、tar.gz 形式のサービス・ファイルとして保存されます。サービス・ファイルをダウンロードしたり、優先サービス・プロバイダーに送信したりすることができます。

このタスクについて

一度に最大 20 個のサービス・データ収集プロセスを実行できます。

ThinkSystem V3 および V4 サーバー (XCC2 または XCC3 を使用)の場合、XClarity Administrator はリポジトリーの 2 つのファイルにサービス・データを保存します。

- **サービス・ファイル**。(.zip) このファイルには、サービス情報とインベントリーが簡単に読み取り可能な形式で含まれています。

- **デバッグ・ファイル**。(.tzz) このファイルには、Lenovo サポートで使用するためのすべてのサービス情報、インベントリー、およびデバッグ・ログが含まれています。

他のデバイスの場合、XClarity Administrator はリポジトリーの単一のサービス・ファイルにサービス・データファイル (サービス情報、インベントリー、デバッグ・ログなど) を保存します。

管理対象デバイスが、コール・ホーム をトリガーするサービス可能なイベントを生成すると (XClarity Administratorオンライン・ドキュメントの 自動的にサポートに通知されるハードウェア・イベント を参照)、XClarity Administrator はそのデバイスのサービス・データを自動的に収集します。サービス・フォワーダーが構成され有効になっている場合、XClarity Administrator によってサービス・ファイルが指定されたサービス・プロバイダー (たとえば、コール・ホーム を使用する Lenovo サポート・センター または SFTP サイト) にも送信されます。サービス・プロバイダーが追加のデータを必要とする場合、以下で説明する手順を使用して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依頼されることがあります。

サービス・データ・リポジトリーが最大容量に到達すると、新しいファイルの領域を空けるため、最も古いファイル・セットが削除されます。

注：

- スタック・スイッチの場合、*マスター・スイッチ*と、XClarity Administrator がアクセス可能な IP アドレスを持つ*スタンバイ・スイッチ*のサービス・データを収集してダウンロードできます。*メンバー・スイッチ*や保護モードのスイッチのサービス・データは収集できません。
- スタック・モードをサポートするがスタンドアロン・モードになっているスイッチのサービス・データは収集できません。

XClarity Administrator のサービス・データのダウンロードについては、Lenovo XClarity Administrator サービス・ファイルの収集とダウンロードを参照してください。

サービス・データを Lenovo サポート・センター に手動で送信する方法については、ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照してください。

自動サービス・フォワーダーのセットアップについては、自動問題通知のセットアップを参照してください。

手順

特定の管理対象デバイスのサービス・データを収集してダウンロードするには、以下の手順を実行します。

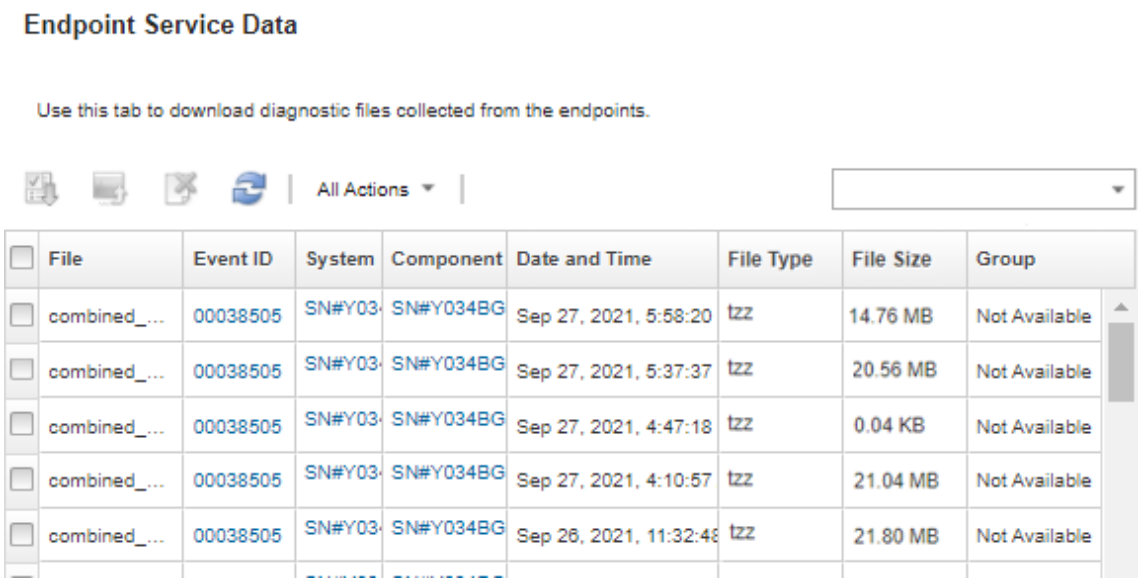
ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。

ステップ 2. 左ナビゲーションの「**エンドポイント・アクション**」をクリックして、「エンドポイント・アクション」ページを表示します。

ステップ 3. 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。

ステップ 4. オプションで、サービス・ファイルをローカル・システムに保存します。

ステップ 5. 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、「デバイス・サービス・データ」ページを表示します。サービス・データ・アーカイブがテーブルに表示されます。



終了後

「デバイス・サービス・データ」ページからは、これらのタスクも実行できます。

- サービス・ファイルを Lenovo サービス技術員に直接手動で送信します (XClarity Administrator オンライン・ドキュメントのLenovo サポートへのサービス・ファイルの転送)。
- サービス・ファイルを Lenovo サポートに手動で送信し、サービス・チケットを開きます (XClarity Administrator オンライン・ドキュメントのハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信しますを参照)。
- ファイルを選択して「**サービス・チケットに添付**」をクリックすることで、サービス・ファイルを既存のサービス・チケットに付加し、Lenovo サポート・センターに送信します。次に、サービス・チケットを選択し、「**関連付ける**」をクリックします。
- 1 つ以上のファイルを選択して「**選択済みサービス・ファイルのダウンロード**」アイコン ( ) をクリックすることで、サービス・ファイルをダウンロードします。複数のファイルが選択されている場合、ファイルはダウンロード前に 1 つの .tar.gz ファイルに圧縮されます。
- 不要になったサービス・ファイルは、ファイルを 1 つ以上選択して「**選択済みサービス・ファイルの削除**」アイコン ( ) をクリックすることで削除します。

Lenovo XClarity Administrator サービス・ファイルの収集とダウンロード

Lenovo XClarity Administrator および特定の管理対象デバイスのサービス・データを手動で収集して、その情報を tar.gz 形式のサービス・ファイルとして保存し、そのサービス・ファイルをダウンロードまたは優先サービス・プロバイダーに送信して、発生した問題の解決に支援を受けることができます。

このタスクについて

注：すべてのサービス・ファイルをダウンロードする場合、既に進行中のジョブがないことを確認してください (ジョブの監視を参照)。ユーザーが開始したジョブがまだ進行中の場合、その同じユーザーがすべてのサービス・ファイルを再度ダウンロードするには、ジョブの完了まで待機する必要があります。そうしないと、2 回目のダウンロード試行は失敗します。

すべてのサービス・ファイル、特定のサービス・ファイル、またはログをダウンロードするかは、Lenovo サポートに問い合わせて決定してください。

XClarity Administrator では、最大 100 個のサービス・ファイルがリポジトリーに保存されます。

XClarity Administrator サービス・データおよびログをダウンロードする際に、特定のデバイスのサービス・データをダウンロード・ファイルに含めるかどうか選択できます。既に存在するサービス・ファイルを使用するか、ダウンロード・プロセスの一部として現在サービス・データを収集するかを選択できます。

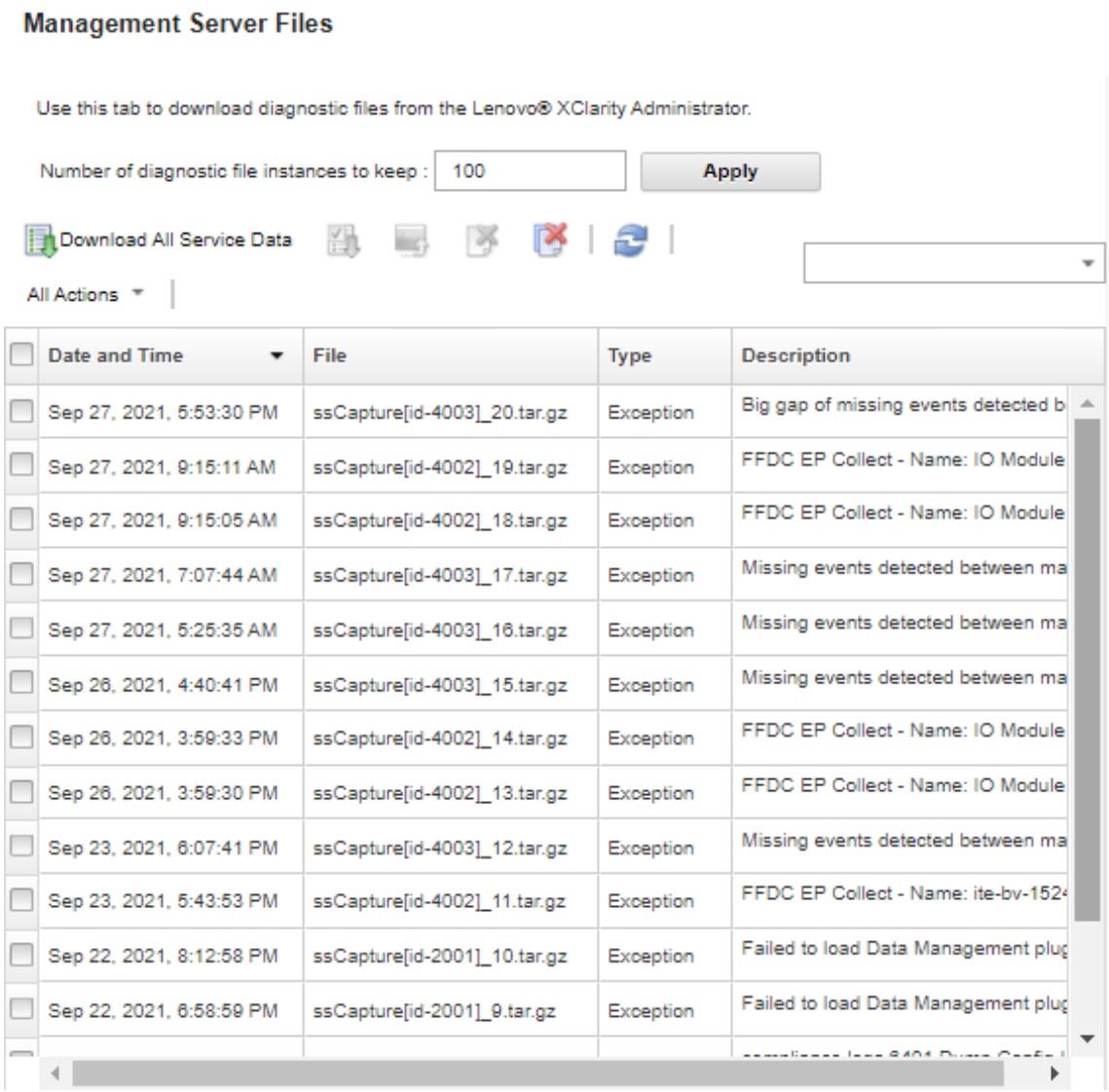
注意：サービス・プロバイダーからの指示がない限り、保持するサービス・ファイルの数を変更しないでください。

手順

XClarity Administrator のサービス・データまたはログを収集およびダウンロードするには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。

ステップ 2. 左ナビゲーションの「**管理サーバー・ファイル**」をクリックして、「管理サーバー・ファイル」ページを表示します。



ステップ 3. すべてのサービス・データまたはすべてのサービス・ログをダウンロードするように選択します。

- 「**すべてのサービス・データのダウンロード**」をクリックして、すべてのサービス・ファイル、管理サーバー・ログ、および特定のデバイスのサービス・ファイルをダウンロードします。
- 「**すべての操作**」 ➡ 「**すべてのサービス・ログのダウンロード**」をクリックして、すべての管理サーバー・ログおよび特定のデバイスのサービス・ファイルをダウンロードします。

ダウンロードするデータの推定量を示すメッセージが表示されます。サービス・ファイルをダウンロードすると、ファイルの数とサイズによっては、ダウンロードに長時間かかることがあります。

ステップ 4. 「**管理対象デバイス用に収集済みのサービス・データを含める**」を選択し、含めるサービス・データ・ファイルを選択して、「**適用**」をクリックします。

ステップ 5. 「**新しいサービス・データを収集する管理対象デバイスを選択**」を選択し、ターゲット・デバイスを選択して、「**適用**」をクリックします。

ステップ 6. サービス・ファイルを Lenovo サポートに送信するか、ファイルをローカル・システムまたはネットワーク・ストレージに保存することを選択します。サービス・データまたはログ・ファイルは送信前に 1 つの .tar.gz ファイルに圧縮されます。

- 「**Lenovo アップロード**」をクリックする場合は、オプションでケース番号を入力して「**OK**」をクリックし、サービス・ファイルを収集して Lenovo アップロード・ファシリティーに転送します。

  注：Lenovo サポートでファイルの場所を見つけやすくするために、ケース番号を指定することをお勧めします。
- 「**ローカルに保存**」をクリックする場合は、Web ブラウザーの機能を使用してファイルをローカル・システムに保存します。
- 「**ネットワーク・ストレージに保存**」をクリックする場合は、IP アドレス、資格情報、ディレクトリーおよびポートを指定して、「保存」をクリックしサービス・ファイルをリモート・サーバーに転送します。

終了後

「管理サーバー・ファイル」ページからは、以下のタスクを実行することもできます。

- ファイルを 1 つ以上を選択して、「**すべての操作**」 ➡ 「**選択済みサービス・ファイルのダウンロード**」をクリックし、既存のファイルをダウンロードします。

  サービス・ファイルを Lenovo サポートに送信するか、ファイルをローカル・システムまたはネットワーク・ストレージに保存するかを選択できます。複数のファイルを選択した場合、ファイルは送信前に 1 つの .tar.gz ファイルに圧縮されます。
- 「**選択済みサービス・ファイルの削除**」アイコン ( ) をクリックして、1 つ以上の選択済みサービス・ファイルを削除します。
- 「**サービス・ファイルをすべてクリア**」アイコン ( ) をクリックして、すべてのサービス・ファイルを削除します。
- 「**すべての操作**」 ➡ 「**すべてのサービス・ログのクリア**」をクリックして、すべての管理サーバー・ログを削除します。

応答しない Lenovo XClarity Administrator のサービス・ファイルの収集とダウンロード

Lenovo XClarity Administrator が応答しなくなりリカバリーできない場合、その XClarity Administrator インスタンスのサービス・データとログを収集してダウンロードできます。サービス・データとログは tar.gz 形式のサービス・ファイルとしてローカル・システムにダウンロードされます

始める前に

XClarity Administrator Web インターフェースは次の Web ブラウザーで機能します。
- Chrome™ 48.0 以降 (リモート・コンソールには 55.0 以上)
- Firefox® ESR 38.6.0 以降
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 以降 (IOS7 以降および OS X)

XClarity Administrator がインストールされているシステムにネットワークで接続できるシステムから、Web インターフェースにログインしていることを確認します。

手順

応答しない XClarity Administrator インスタンスのサービス・データまたはログを収集およびダウンロードするには、以下の手順を実行します。

ステップ 1. 次の URL を使用して、XClarity Administrator 仮想マシンの IP アドレスをブラウザーで指定します。

```
https://<IP_address>:58081
```

例:

```
https://192.0.2.0:58081
```

ステップ 2. 「**passKey**」フィールドにサービス・リカバリー・パスワードを指定します。

これは、XClarity Administrator の初期セットアップで指定したパスワード、または「サービスおよびサポート」ページの「**サービス・リカバリー・パスワード**」タブで変更したパスワードです (72 ページの 「サービス・リカバリー・パスワードの変更」を参照)。

ステップ 3. 収集するファイルのタイプを選択します。
- 「**すべてのサービス・データ**」。すべてのサービス・ファイルと管理サーバー・ログを収集します。
- 「**すべてのサービス・ログ**」。すべての管理サーバー・ログを収集します。

ステップ 4. 「**収集**」をクリックし、Web ブラウザーの機能を使用してファイルをローカル・システムに保存します。サービス・データまたはログ・ファイルは送信前に 1 つの .tar.gz ファイルに圧縮されます。

ハードウェアの問題に関するサービス要求をLenovo サポート・センターに送信します

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 Administrator は自動的にサービス・チケットを開き、サービス・データを収集してアーカイブ・ファイルとして保存し、Lenovo アップロード・ファシリティーにサービス・アーカイブ・ファイルを転送します。アーカイブ・サービス・ファイルには、デバイスおよび XClarity Administrator のサービス・データが含まれます。また、手動で管理対象デバイスのサービス・ファイルを収集およびダウンロードし、XClarity Administrator を使用していつでも 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・チケットを開くと、Lenovo サポートが迅速に、そして効果的に関連情報を使用できるようになることで、お客様のハードウェアの問題の解決策を判別するプロセスが開始されます。Lenovo サービス技術員は、お客様がサービス・チケットを完了および送信するとすぐに、解決策の作業を開始します。

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 アップロード・ファシリティ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 アップロード・ファシリティーでのサービス・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。

始める前に

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。

コール・ホームのお問い合わせ先情報が構成されていることを確認します。

1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。
2. 左ナビゲーションの「**コール・ホーム構成**」をクリックして「コール・ホーム構成」ページを表示します。
3. 連絡先と場所の情報を入力します。
4. オプション: システム情報を入力します。
5. 「**適用**」をクリックします。

コール・ホーム を有効にする前に、XClarity Administrator 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 Administrator 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 Administrator 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 Administrator 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、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。

このタスクについて

「エンドポイント・アクション」ページの「**コール・ホーム・ステータス**」列に、コール・ホームがベースボード管理コントローラーで有効になっているかどうかが示されます。「適用外」の値は、管理コントローラーによってコール・ホームがサポートされていないことを示します。XClarity Administrator は、管理コントローラーがコール・ホームをサポートしているかどうかに関係なく、デバイスのコール・ホームを実行できます。特定のデバイスでコール・ホームがサポートされているかどうかを判別するには、XClarity Administrator のサポート – 互換性に 関する Web ページを参照してください。

サービス・データを Lenovo サポート・センターに自動的に送信するようにコール・ホームを構成して有効にする方法について詳しくは、Lenovo サポートへの自動問題通知 (コール・ホーム) のセットアップを参照してください。

サービス・データを手動で収集およびダウンロードする方法については、デバイスのサービス・データの収集とダウンロードとLenovo XClarity Administrator サービス・ファイルの収集とダウンロードを参照してください。

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 が構成されているが有効になっていない場合、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・データを収集およびダウンロードして、ファイルを Lenovo サポート・センター に送信します。
    1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

2. 左ナビゲーションの「**エンドポイント・アクション**」をクリックして、「エンドポイント・アクション」ページを表示します。
3. デバイスを選択し、「**すべての操作**」 ➡ 「**手動 コール・ホーム の実行**」をクリックします。

   ヒント:「**すべての操作**」 ➡ 「**コール・ホームテストの実行**」をクリックして、実際にLenovo サポート にデータを送信することなく、Lenovo サポート・センターとの通信をテストし、コール・ホームが正しくセットアップされていることを確認できます。
4. 報告する問題の説明を入力してます (関連するイベント ID など)。
5. 「**OK**」をクリックします。

- コール・ホーム が構成または有効化されていない場合、Lenovo サポート・ラインにお問い合わせすることでサービス要求を送信できます。詳しくは、ヘルプおよび技術サポートの入手を参照してください。

終了後

「**サービス・チケットのステータス**」ページから開いているサービス・チケットを監視できます (サービス・チケットとステータスの表示を参照)。

XClarity Administrator の問題の報告

ソフトウェア (管理サーバー) に関する問題の報告のためにサービス要求を送信すると、Lenovo XClarity Administrator によりサービス・チケットが開き、管理サーバーからサービス・データが収集され、コール・ホームを使用してファイルが Lenovo サポート・センターに送信されます。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、ソフト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。

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。

始める前に

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。

- XClarity Administrator に関する問題の要求を送信する前に、次のリソースでヘルプを参照してください。
  - XClarity Administrator に関するアイデアを送信するには、XClarity Administrator タイトル・バーで、ユーザー・アクション・メニュー (

) をクリックして、「**アイデアを送信**」をクリックするか、Lenovo XClarity アイディエーション Web サイト に直接移動します。
  - 質問し、回答を検索するには、XClarity Administrator タイトル・バーで、ユーザー・アクション・メニュー (

) をクリックして、「**フォーラムにアクセス**」をクリックするか、Lenovo XClarity Community フォーラム Web サイト に直接移動します。
  - XClarity Administrator で問題が起こったときにお客様が問題解決に使用できるヒントや手法を、Lenovo データセンターサポート Web サイト で確認してください。これらの*技術ヒント*では、XClarity Administrator の動作に関する問題を回避する手順について説明しています。

    ご使用のサーバーで利用可能な技術ヒントを検索するには:

    1. Lenovo データセンターサポート Web サイト にアクセスします。
    2. 「**検索**」フィールドで、「XClarity Administrator」を入力します。

3. 「**Top Articles (トップ記事)**」セクションで「**View All (すべて表示)**」をクリックしてすべてのヒントを表示するか、または「**Search (検索)**」フィールドにキーワードを入力して特定のヒントを検索します。

   ヒント: 「**Relevance (関連性)**」、「**Popularity (人気)**」、または「**Newest (最新)**」の順にリストをソートできます。

- XClarity Administrator 問題に関して Lenovo サポートでサービス要求を送信するには、Lenovo XClarity Pro が必要です。Lenovo XClarity Pro では、サービスとサポートへの資格および全機能有効化ライセンスが提供されます。Lenovo XClarity Pro の購入について詳しくは、Lenovo 担当員または認定ビジネス・パートナーに連絡してください。
- **デフォルトの Lenovo コール・ホーム**・フォワーダーが構成されて有効になっていることを確認します (Lenovo サポートへの自動問題通知 (コール・ホーム) のセットアップ を参照)。
- コール・ホームを有効にする前に、XClarity Administrator 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 Administrator 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 Administrator 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 Administrator 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、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。

このタスクについて

別のコール・ホームの開始時にコール・ホームが既に進行中である場合、2 回目のコール・ホームについてデータが収集、送信される前に、最初のコール・ホームで Lenovo サポートにデータが収集、送信されます。そのため、2 回目のコール・ホームのデータ送信で遅延が発生する可能性があります。

手順

XClarity Administrator で問題を報告するには、以下の手順を実行してください。

- コール・ホームが構成されている場合、以下の手順を実行してサービス・チケットを開いた後、管理サーバーのサービス・データを収集およびダウンロードして、ファイルを Lenovo サポート・センターに送信します。
  1. XClarity Administrator タイトル・バーから、「**問題を報告**」をクリックします。管理サーバーは、Lenovo サポートへの接続をテストします。
  2. 「**続行**」をクリックして、「ソフトウェア問題に関する情報」ダイアログを表示します。
  3. Lenovo XClarity Pro の購入時に受け取った Lenovo お客様番号をご提示ください。
  4. 関連するイベント ID と、問題に関連付けられているデバイスなど、問題に関する情報を提供します。

     注：

     – 管理サーバーのサービス・ログとデータが自動的に収集、送信されます。
     – 問題に関連するデバイスを選択した場合、そのデバイスのサービス・データも収集され、自動的に送信されます。
     – 「**ファイルのアップロード**」をクリックして、問題のトラブルシューティングで Lenovo サポートに役立つように、追加ファイル (スクリーン・キャプチャーやビデオなど) を添付することもできます。
  5. 問題を再現する手順を説明します。

6. 問題が発生した機能領域を選択します。
7. 「**次へ**」をクリックします。
8. 問題についての主な連絡先となる担当者の情報を指定します。追加の連絡先を指定するには、「**別の連絡先を追加**」をクリックします。
9. 「**Lenovo に送信**」をクリックし、Lenovo サポートにサービス・チケットを作成します。

- コール・ホームが構成、または構成されているが有効化されていない場合、Lenovo サポート・ラインにお問い合わせすることでサービス・リクエストを送信できます。詳しくは、ヘルプおよび技術サポートの入手を参照してください。

終了後

「**サービス・チケットのステータス**」ページから開いているサービス・チケットを監視できます (サービス・チケットとステータスの表示を参照)。

問題が送信された後、オープン・サービス・チケットに追加ファイルを付加できます。

1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。
2. 左ナビゲーションの「**サービス・チケットのステータス**」をクリックして、「サービス・チケットのステータス」ページを表示します。
3. サービス・チケットを選択します。
4. 「**サービス・ファイルを付加**」をクリックした後、サービス・チケットに付加するサービス・データ・アーカイブまたは別のファイルを選択し、Lenovo サポートに送信します。

オープン・サービス・チケットへのサービス・ファイルの付加

特定のデバイスのサービス・データ・ファイルを Lenovo サポート・センター の開いているサービス・チケットに付加できます。

始める前に

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

現在のサービス・データ・アーカイブ、スクリーン・キャプチャー、ビデオなど、追加ファイルをオープン・サービス・チケットに添付できます。

手順

開いているサービス・チケットにサービス・ファイルを追加するには、以下のステップを実行します。

- 「**デバイス・サービス・データ**」ページで、以下の操作を実行します。
  1. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。
  2. 左ナビゲーションの「**エンドポイント・サービス・データ**」をクリックして、「エンドポイント・サービス・データ」ページを表示します。
  3. サービス・チケットに付加するサービス・ファイルを選択します。
  4. 「**操作**」 → 「**サービス・チケットに付加**」の順にクリックした後、サービス・ファイルを付加するサービス・チケットを選択します。

5. 「**関連付ける**」をクリックして、サービス・チケットに添付し、Lenovo サポートに送信するサービス・ファイルを選択します。

- 「**サービス・チケットのステータス**」タブで、以下の操作を実行します。
  1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。
  2. 左ナビゲーションの「**サービス・チケットのステータス**」をクリックして、「サービス・チケットのステータス」ページを表示します。
  3. サービス・チケットを選択します。
  4. 「**サービス・ファイルを付加**」をクリックした後、サービス・チケットに付加するサービス・ファイルを選択し、Lenovo サポートに送信します。

サービス・チケットとステータスの表示

コール・ホームを使用して手動または自動で Lenovo サポート・センター に送信されたサービス・チケットに関する情報を表示できます。これには、Lenovo サポート・センター に転送された現在のステータスおよび関連サービス・ファイル、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ービス・チケットが含まれます。

手順

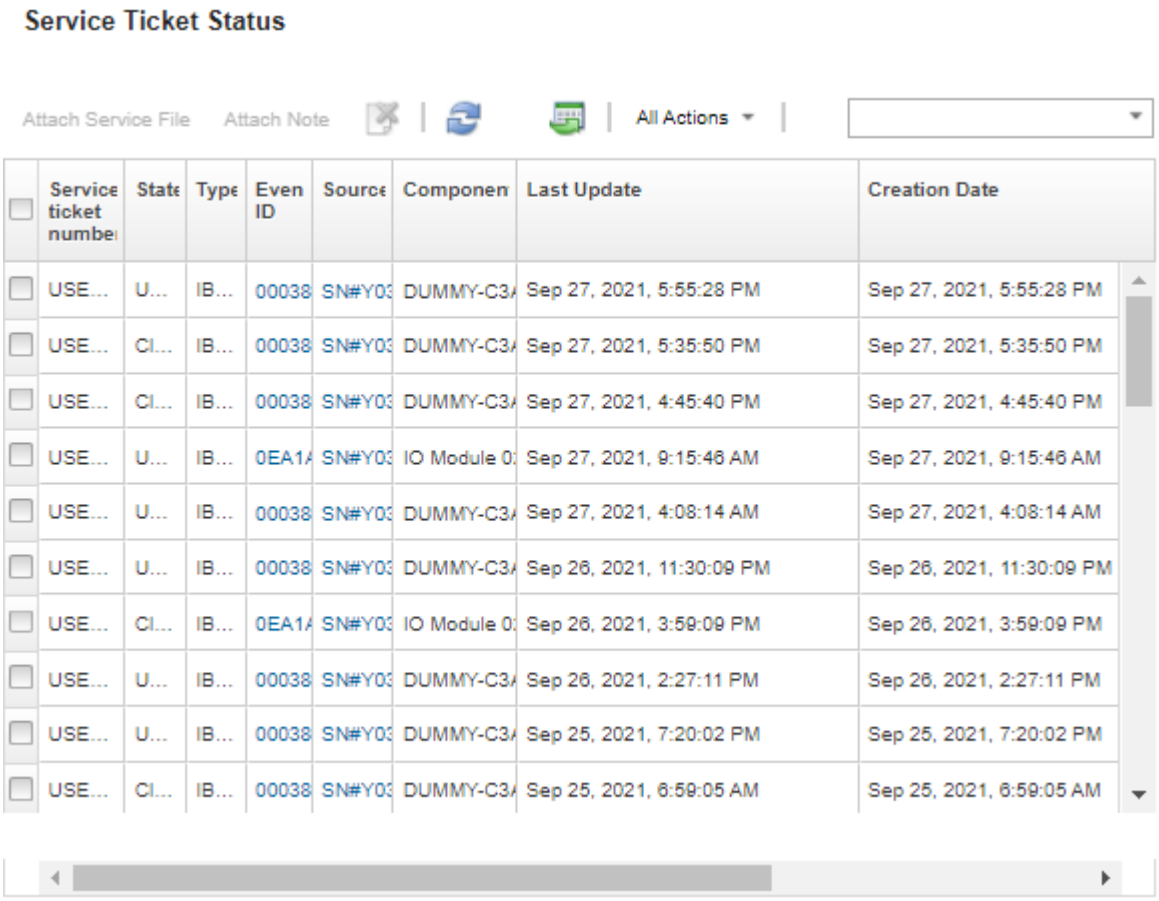
XClarity Administrator のサービス・チケットを表示するには、「**管理**」 → 「**サービスおよびサポート**」をクリックし、左ナビゲーション・ペインの「**サービス・チケット・ステータス**」をクリックして「サービス・チケット・ステータス」ページを表示します。

「**サービス・チケット番号**」列には、イベントに対して開かれたサービス・チケットの ID が表示されます。同じイベントに対して複数のサービス・チケットが開かれた場合 (たとえば、Lenovo サポート・センターで 1 つ、ServiceNow インテグレーターでもう 1 つ開かれた場合など)、サービス・チケットごとに別個の行がテーブルに表示されます。対応するサービス・チケットは、「**相互参照 ID**」列で見つけることができます。たとえば、「**サービス・チケット番号**」に Lenovo サポート・サービス・チケット ID が表示されている場合、「**相互参照 ID**」には ServiceNow サービス・チケット ID が表示されます。その逆も同様です。

「**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。
- **IBM コール・ホーム**
- **IBM コール・ホーム・テスト**
- **Lenovo コール・ホーム**
- **Lenovo コール・ホーム・テスト**
- **Lenovo ソフトウェア・コール・ホーム**
- **Lenovo ソフトウェア・コール・ホーム・テスト**
- Cherwill
- ServiceNow

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**
- **キャンセル**
- **解決済み**
- **不明**

「**相互参照 ID**」列には、Lenovo サービス・チケットに関連する外部サポート・サービス (ServiceNow など) によるサービス・チケット ID が含まれています。



終了後

「サービス・チケットのステータス」ページからは、選択したサービス・チケットに対して以下の手順を実行できます。

- Lenovo サポート・センター で、「**サービス・ファイルを付加**」をクリックして、開いているサービス・チケットに特定のデバイスのサービス・ファイルを付加します (オープン・サービス・チケットへのサービス・ファイルの付加を参照)
- 「**注を添付**」をクリックして Lenovo サポート・センター の開いているサービス・チケットに注を添付します。
- 「**サービス・チケットの削除**」アイコン ( ) をクリックして、サービス・チケットを削除します。アクティブ状態でないサービス・チケットのみを削除できます。
- 「**サービス・チケット・ステータス状態を更新**」アイコン ( ) をクリックして、Lenovo サポート・センター から開いているすべてのサービス・チケットについての最新情報を取得します。
- 「**すべてを CSV としてエクスポート**」アイコン ( ) をクリックして、すべてのサービス・チケットのステータスを CSV ファイルにエクスポートします。

Lenovo サポートへのサービス・ファイルの転送

問題を解決するために Lenovo サポートと連携している場合、Lenovo アップロード・ファシリティーを使用して Lenovo サポート担当者に直接手動でサービス・ファイルを転送することができます。

始める前に

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。

手順

Lenovo サポートに直接サービス・ファイルを転送するには、以下の手順を実行します。

ステップ 1. Lenovo アップロード・ファシリティーを構成します。

a. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

b. 左ナビゲーションの「**Lenovo アップロード・ファシリティー**」をクリックします。

c. メール・アドレスを入力してください。

d. 「**適用**」をクリックします。

ステップ 2. 送信する必要があるログに応じて、左ナビゲーションの「**管理サーバー・ファイル**」または「**エンドポイント・サービス・データ**」をクリックします。

ステップ 3. Lenovo サポートに送信するサービス・ファイルを 1 つ以上選択し、「**選択済みファイルの Lenovo アップロード**」アイコン ( ) をクリックします。「Lenovo アップロード情報」ダイアログが表示されます。

ステップ 4. オプションで、ケース番号を入力します。

ステップ 5. 「**OK**」をクリックしてサービス・ファイルを転送します。

管理サーバー・ログ設定の構成

ログの設定は、必要なときのみロギングの詳細レベルを調整するために Lenovo サポートが使用します。

このタスクについて

注意：Lenovo サポートからの指示がない限り、このページの設定を変更しないでください。

手順

ログ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. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**サーバー・ロギング設定**」をクリックして、「サーバー・ロギング設定」ページを表示します。

ステップ 3. Lenovo サポートから指示されたとおりに各設定を調整し、「**適用**」クリックします。

終了後

「サーバー・ロギング設定」ページからは、以下の手順も実行できます。

- 「**LogBack のダウンロード**」をクリックして、管理サーバーログ構成設定をローカル・システムにダウンロードします。設定は、logback.xml という名前のファイルとして、デフォルトのダウンロード・ディレクトリーにダウンロードされます。
- 「**デフォルトの復元**」をクリックして、デフォルト設定を復元します。
- 「**構成ファイルのアップロード**」をクリックし、XClarity Administrator にインポートするファイルを選択して、構成ファイルをインポートします。ファイルの名前は logback.xml でなければなりません。

  重要：Lenovo サービス技術員によって提供された構成ファイルのみを、サービス技術員の指示があった場合のみ、インポートしてください。

すべての管理対象デバイスでのコール・ホーム の再有効化

Lenovo XClarity Administrator で コール・ホーム サービス・フォワーダーを有効にしている場合、重複する問題レコードが作成されないようにするために、各管理対象デバイスで コール・ホーム が無効になります。XClarity Administrator を使用したデバイスの管理をやめる場合、または XClarity Administrator での コール・ホーム を無効にする場合は、後で各デバイスで コール・ホーム を再度有効にする代わりに、XClarity Administrator からすべての管理対象デバイスで コール・ホーム を再度有効にできます。

このタスクについて

注意：すべてのデバイスで コール・ホーム を再び有効にしても、一部のデバイスでは コール・ホーム が動作しない可能性があります。以前に各デバイスを構成していない場合には、各デバイスで独自に構成が必要な可能性があります。

XClarity Administrator では ThinkAgile および ThinkSystem デバイスでのコール・ホームはサポートされていますが、一部の ThinkAgile および ThinkSystem デバイスのベースボード管理コントローラーにコール・ホームのサポートは含まれていません。そのため、これらのデバイス自体でコール・ホームを有効にしたり無効にしたりすることはできません。コール・ホームは、その XClarity Administrator レベルのデバイスに対してのみ有効にすることができます。

手順

すべての管理対象デバイスで コール・ホーム を再度有効にするには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 → 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**サービス・フォワーダー**」をクリックして、「サービス・フォワーダー」ページを表示します。

ステップ 3. すべてのコール・ホーム・サービス・フォワーダーのステータスを変更します (「デフォルトのコール・ホーム」を**無効**に変更するなど)。

ステップ 4. 左ナビゲーションの「**エンドポイント・アクション**」をクリックして、「エンドポイント・アクション」ページを表示します。

ステップ 5. 各管理対象デバイスで コール・ホーム を有効化するには、「**すべての操作**」 → 「**すべてのデバイスで コール・ホーム を有効にする**」をクリックします。

Lenovo への定期的なデータの送信

オプションで、製品の使用方法や環境の変更に関するデータを収集し、そのデータを定期的に Lenovo に送信することを XClarity Administrator 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

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

以下のタイプのデータを収集して Lenovo に送信することができます。

- **使用データ**

  複数のユーザーの使用データを分析することにより、Lenovo は XClarity Administrator がどのように使用されているかを把握できます。これにより、Lenovo は、頻繁に使用されている機能を調べたり、XClarity Administrator インスタンスで発生している問題を特定したりすることができます。その後、お

客様のニーズを満たす製品の機能拡張に関する将来の投資の決定を下したり、将来のリリースで問題を修正したり、製品の品質を向上したりするためにこのデータが利用されます。

使用データを Lenovo に送信することに同意した場合、以下のデータが収集され、毎週送信されます。このデータは*匿名*です。プライベート・データ (シリアル番号、UUID、ホスト名、IP アドレス、ユーザー名など) が収集されることも、Lenovo に送信されることもありません。
- 実行された操作のログ
- 発生したイベントのリスト、および発生時のタイムスタンプ
- 発生した監査イベントのリスト、および発生時のタイムスタンプ
- 実行されたジョブのリスト、および各ジョブの成功または失敗の情報
- メモリー使用量、プロセッサー使用量、ディスク・スペースを含む、XClarity Administrator のメトリック
- すべての管理対象デバイスに関する限定的なインベントリー・データ

- **ハードウェア・データ**

  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。このデータは*匿名ではありません*。ハードウェア・データには、UUID やシリアル番号などの属性が含まれています。IP アドレスやホスト名は含まれません。

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

データが Lenovo に送信されると、HTTPS を使用して XClarity Administrator 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 Administrator に事前にロードされた証明書が認証に使用されます。XClarity Administrator 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 Administrator 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。

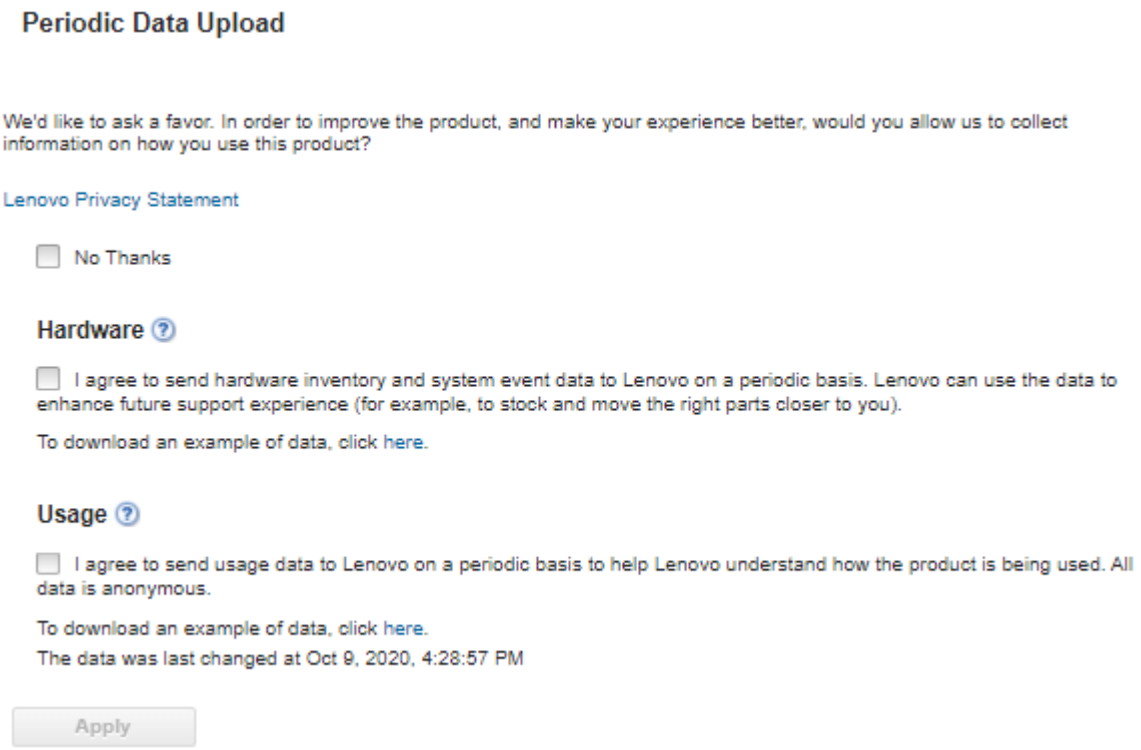
その後、データは Lenovo カスタマー・ケア・リポジトリーに移動され、最大 5 年間保管されます。このリポジトリーは安全な場所であり、問題のトラブルシューティングのためにデバッグ・データを Lenovo に送信する際にも使用されます。ほとんどの Lenovo サーバー、ストレージ、およびスイッチ製品で使用されます。

Lenovo カスタマー・ケア・リポジトリーからは、すべてのハードウェアおよび使用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 Administrator に許可するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**サービスおよびサポート**」をクリックします。「サービスおよびサポート」ページが表示されます。



ステップ 2. 左ナビゲーションの「**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」ページを表示します。

ステップ 3. オプションで、ハードウェアおよび使用データを Lenovo に送信することに同意します。

ステップ 4. 「**適用**」をクリックします。

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。

- 該当するチェック・ボックスの下にある日付を参照して、データが最後に送信された時刻を確認する。
- 該当するチェック・ボックスの下にあるリンクをクリックして、最後に送信されたデータ・アーカイブをダウンロードする。

サンプル使用データ

使用データを Lenovo に送信することに同意した場合、次の例が収集され、定期的に Lenovo に送信されます。

XClarity Administrator メトリック・データ

```
Timestamp  cpuLoad usedSpace usedRam usedJavaCpu usedJavaRam
1497861662 0.99   12.6225   13.3644 71.9     9.4
1497861668 1.23   12.6343   18.5676 0       14.4
1497861674 1.89   12.6371   19.6182 77.9     15.3
1497861679 1.98   12.6442   23.0782 37.9     18.6
1497861685 2.06   12.647    23.2412 77.9     18.6
1497861690 2.14   12.6654   25.3697 10       19
1497861696 2.37   7.75276   25.8952 2       19.4
1497861701 2.34   7.76077   26.0184 24       19.5
1497861056 2.55   7.77003   26.4222 85.9     19.7
1497861061 2.82   7.77877   26.5485 159.9    19.7
1497861067 3     7.7954    27.0066 131.9    20
```

操作データ

```
/updates/images/userdefined.png={"GET"\:1}
/config/profile={"GET"\:865}
/node/AD9547AB3C8011E79DCC000E1E7D4EE0={"GET"\:1}
/usage/data={"GET"\:12}
/compliancePolicies/persistedResult={"GET"\:3}
/jobs/88={"PUT"\:31}
/osdeployment/rest/internal/event/aicc={"POST"\:186}
/aicc={"GET"\:56}
/updates/images/powerStates.png={"GET"\:2}
/jobs/84={"PUT"\:3}
/updates/images/ActionSprite.png={"GET"\:1}
/nodes/AD9547AB3C8011E79DCC000E1E7D4EE0/lock={"GET"\:1,"PUT"\:2}
/updates/customUI/gridxExtensions/Mark.js={"GET"\:2}
/updates/images/ac22_deleteall_inactive_24.png={"GET"\:1}
/service/forwarders={"GET"\:12}
/nodes/7C64A0A8413811E7A6C6000E1EB35A90/lock={"GET"\:1,"PUT"\:2}
/config/deploy/status={"GET"\:865}
/node/235435543C7D11E7AA13000E1E7D54A0={"GET"\:1}
/updates/ApplyActivateUpdates.js={"GET"\:2}
/discovery={"GET"\:3}
/userAccountSettings={"GET"\:1}
/discoverRequest/jobs/610={"GET"\:9}
/compliancePolicies/events={"POST"\:25}
/events/audit={"GET"\:5}
/updates/images/st22_filterRunning_24.png={"GET"\:2}
/updates/images/st16_running_24.gif={"GET"\:1}
/updates/images/complianceStatus.png={"GET"\:2}
/usage={"GET"\:4}
/updates/json/firmwareRepository/exportPayloads.json={"GET"\:1}
/updates/images/ac22_collapseall_OneUI_24.png={"GET"\:3}
/chassis/0AC502DEFCD6419FB20FB5A9A49D0293={"GET"\:17}
/updates/images/ac22_copy_inactive_24.png={"GET"\:1}
/service/endPoint/collectedArchives={"GET"\:4}
/jobs/lock/88={"DELETE"\:1}
/updates/customUI/gridxModules/IndirectSelect.js={"GET"\:2}
/stgupdates/inventory/events={"POST"\:70}
/electronicDownload={"GET"\:1}
/updates/images/st16_firm_normal_24.png={"GET"\:3}
/updates/images/st16_Empty_24.png={"GET"\:1}
/updates/json/compliancePolicy/getCompByUxsp.json={"GET"\:1}
```

イベント・データ

```
{
  "action":100,
  "commonEventID":"FQXHMSE0203I",
  "cn":"1",
  "eventClass":200,
  "eventID":"FQXHMSE0203I",
  "flags":"",
  "mtm":"",
  "msgID":"",
  "service":100,
  "severity":200},
  "timeStamp":"2017-06-16T15:56:06Z"
}
```

監査データ

```
{
```

```
  "action":100,
  "commonEventID":"FQXHMSE0200I",
  "cn":"1",
  "eventClass":200,
  "eventID":"FQXHMSE0200I",
  "flags":"",
  "msgID":"",
  "mtm":"",
  "service":100,
  "severity":200,
  "timeStamp":"2017-06-16T15:56:06Z"
}
```


インベントリー・データ


```
-377665639={
  "firmwareList"\:[{
    "build"\:"2PET41C",
    "date"\:"2017-12-19T05\:00\:00Z",
    "name"\:"CMM firmware",
    "type"\:"CMM firmware",
    "version"\:""
  }],
  "mtm"\:"/",
  "productName"\:"",
  "stillManaged"\:"true",
  "uuid"\:"-377665639"
}
-177044123={
  "firmwareList"\:[{
    "build"\:"A3E117D",
    "date"\:"2018-01-26T00\:00\:00Z",
    "name"\:"UEFI Firmware/BIOS",
    "type"\:"UEFI",
    "version"\:"A3E117D-1.80"
  },{
    "build"\:"A3E113C",
    "date"\:"2016-12-16T00\:00\:00Z",
    "name"\:"UEFI Backup Firmware/BIOS",
    "type"\:"UEFI-Backup",
    "version"\:"A3E113C-1.60"
  },{
    "build"\:"DSALB1Q",
    "date"\:"2018-05-15T00\:00\:00Z",
    "name"\:"DSA Diagnostic Software",
    "type"\:"DSA",
    "version"\:"DSALB1Q-10.3"
  },{
    "build"\:"TCOO39A",
    "date"\:"2018-01-19T00\:00\:00Z",
    "name"\:"IMM2 Firmware",
    "type"\:"IMM2",
    "version"\:"TCOO39A-4.70"
  },{
    "build"\:"TCOO39A",
    "date"\:"2018-01-19T00\:00\:00Z",
    "name"\:"IMM2 Backup Firmware",
    "type"\:"IMM2-Backup",
    "version"\:"TCOO39A-4.70"
  }],
  "mtm"\:"7162/CC1",
```

```
  "productName"\:"Lenovo Flex System x240 Compute Node",
  "stillManaged"\:"true",
  "uuid"\:"-177044123"
}
-734000615={
  "firmwareList"\:[],
  "mtm"\:"8721/HC1",
  "productName"\:"IBM Flex System Enterprise Chassis Midplane Card"},
  "stillManaged"\:"true",
  "uuid"\:"-734000615"
1150304995={
  "firmwareList"\:[{
    "date"\:"06/12/2014",
    "build"\:"",
    "name"\:"Boot ROM",
    "type"\:"Boot ROM",
    "version"\:"7.8.5.0"
  },{
    "date"\:"06/12/2014",
    "build"\:"",
    "name"\:"Main Application 1",
    "type"\:"Main Application 1",
    "version"\:"7.8.5.0"
  },{
    "date"\:"03/29/2013",
    "build"\:"",
    "name"\:"Main Application 2",
    "type"\:"Main Application 2",
    "version"\:"7.5.3.0"
  }],
  "mtm"\:"/",
  "productName"\:"IBM Flex System Fabric EN4093 10Gb Scalable Switch",
  "stillManaged"\:"true",
  "uuid"\:"1150304995"
}
-1050714125={
  "firmwareList"\:[{
    "date"\:"04/19/2016",
    "build"\:"",
    "name"\:"Main Application",
    "type"\:"Main Application",
    "version"\:"7.4.1c"
  }],
  "mtm"\:"/",
  "productName"\:"IBM Flex System FC5022 12-port 16Gb ESB SAN Scalable Switch",
  "stillManaged"\:"true",
  "uuid"\:"-1050714125"
}
```


サンプル・ハードウェア・データ

ハードウェア・データを Lenovo に送信することに同意した場合、次の例が収集され、定期的に Lenovo に送信されます。

データは毎日および毎週収集されます。

- 92 ページの「毎日のハードウェア・データ」。インベントリー変更イベント (FQXHMDM0001I)、および各インベントリー変更のハードウェア・インベントリーに対する変更が含まれます。
- 96 ページの「毎週のハードウェア・データ」。すべてのデバイスのインベントリーが含まれます。

毎日のハードウェア・データ


```
[{
  "2020-03-23T12:32:24.765": {
    "event": {
      "severity": 200,
      "timeStamp": "2020-03-23T16:32:21Z",
      "eventID": "FQXHMDM0001I",
      "eventClass": 800,
      "service": 100,
      "mtm": "",
      "flags": ["Hidden"],
      "action": 100,
      "msgID": "",
      "commonEventID": "FQXHMDM0001I",
      "cn": ""
    },
    "deviceInventoryChanges": [{
      "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36": [{
        "MODIFIED": [
          { "nodes": [] },
          { "accessState": "Pending" },
          { "powerSupplies": [{
            "cmmDisplayName": "Power Supply 06",
            "cmmHealthState": "Non-Critical",
            "dataHandle": 0,
            "description": "Power Supply",
            "excludedHealthState": "Normal",
            "firmware": [{
              "build": "",
              "classifications": [],
              "date": "",
              "name": "Power Supply Firmware",
              "revision": "0",
              "role": "",
              "softwareID": "",
              "status": "",
              "type": "Power Supply Firmware",
              "version": ""
            }],
            "FRU": "69Y5817",
            "fruSerialNumber": "ZK125115V0VS",
            "hardwareRevision": "5.0",
            "healthState": "NA",
            "inputVoltageMax": -1,
            "inputVoltageIsAC": true,
            "inputVoltageMin": -1,
            "leds": [{
              "color": "Green",
              "location": "Planar",
              "name": "OUT",
              "state": "Off"
            },
            {
              "color": "Amber",
              "location": "Planar",
              "name": "FAULT",
              "state": "Off"
            },
            {
              "color": "Green",
              "location": "Planar",
```

```
    "name": "IN",
    "state": "Off"
  }],
  "machineType": "",
  "manufactureDate": "2211",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
  "name": "Power Supply 06",
  "overallHealthState": "Normal",
  "parent": {
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "partNumber": "69Y5801",
  "productName": "IBM 2500 W Power Supply",
  "posID": "60",
  "powerAllocation": {
    "totalInputPower": 0,
    "totalOutputPower": 343
  },
  "powerState": "Unknown",
  "productId": "303",
  "serialNumber": "",
  "slots": [6],
  "type": "PowerSupply",
  "userDescription": "",
  "uri": "powerSupply/04382F96885411E00095009500950095",
  "uuid": "04382F96885411E00095009500950095",
  "vpdID": "128"
},
{
  "cmmDisplayName": "Power Supply 04",
  "cmmHealthState": "Normal",
  "dataHandle": 0,
  "description": "Power Supply",
  "excludedHealthState": "Normal",
  "firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Power Supply Firmware",
    "revision": "5",
    "role": "",
    "softwareID": "",
    "status": "",
    "type": "Power Supply Firmware",
    "version": ""
  }],
  "FRU": "69Y5806",
  "fruSerialNumber": "ZK128116T03B",
  "hardwareRevision": "75.54",
  "healthState": "NA",
  "inputVoltageIsAC": true,
  "inputVoltageMax": 240,
  "inputVoltageMin": 220,
  "leds": [{
    "color": "Green",
    "location": "Planar",
    "name": "OUT",
    "state": "On"
```

```
  },
  {
    "color": "Amber",
    "location": "Planar",
    "name": "FAULT",
    "state": "Off"
  },
  {
    "color": "Green",
    "location": "Planar",
    "name": "IN",
    "state": "On"
  }],
  "machineType": "",
  "manufactureDate": "2511",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
  "name": "Power Supply 04",
  "overallHealthState": "Normal",
  "parent": {
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "partNumber": "69Y5802",
  "productId": "304",
  "productName": "IBM 2500 W Power Supply",
  "powerAllocation": {
    "totalInputPower": 2505,
    "totalOutputPower": 343
  },
  "powerState": "Unknown",
  "posID": "61",
  "serialNumber": "",
  "slots": [4],
  "type": "PowerSupply",
  "userDescription": "",
  "uri": "powerSupply/FF2D840D7A644BCE91ADC16C78978A03",
  "uuid": "FF2D840D7A644BCE91ADC16C78978A03",
  "vpdID": "128"
}]},
{ "fanMuxes": [{
  "cmmDisplayName": "Fan Logic 01",
  "cmmHealthState": "Non-Critical",
  "dataHandle": 0,
  "description": "Fan Logic Module",
  "excludedHealthState": "Normal",
  "FRU": "81Y2912",
  "fruSerialNumber": "Y031BG16D00S",
  "hardwareRevision": "4.0",
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "On"
  }],
  "machineType": "",
  "manufacturer": "IBM",
  "manufactureDate": "2511",
  "manufacturerId": "20301",
  "model": "",
```

```
        "name": "Fan Logic 01",
        "overallHealthState": "Normal",
        "parent": {
          "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
          "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
        },
        "partNumber": "81Y2990",
        "productId": "338",
        "productName": "IBM Fan Pack Multiplexor Card",
        "status": "Non-Critical",
        "serialNumber": "",
        "slots": [1],
        "type": "FanMux",
        "uri": "fanMux/4247F859984711E08372E99E4175BAB0",
        "uuid": "4247F859984711E08372E99E4175BAB0"
      },
      {
        "cmmDisplayName": "Fan Logic 02",
        "cmmHealthState": "Non-Critical",
        "dataHandle": 0,
        "description": "Fan Logic Module",
        "excludedHealthState": "Normal",
        "FRU": "81Y2912",
        "fruSerialNumber": "Y031BG16D0CE",
        "hardwareRevision": "4.0",
        "leds": [{
          "color": "Amber",
          "location": "FrontPanel",
          "name": "FAULT",
          "state": "On"
        }],
        "machineType": "",
        "manufactureDate": "2511",
        "manufacturer": "IBM",
        "manufacturerId": "20301",
        "model": "",
        "name": "Fan Logic 02",
        "overallHealthState": "Normal",
        "parent": {
          "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
          "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
        },
        "productId": "338",
        "productName": "IBM Fan Pack Multiplexor Card",
        "partNumber": "81Y2990",
        "serialNumber": "",
        "slots": [2],
        "status": "Non-Critical",
        "type": "FanMux",
        "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
        "uuid": "71F72BE3985011E0B5A8E216694D6175"
      }]},
      { "switches": [] },
      { "excludedHealthState": "Normal" },
      { "overallHealthState": "Normal" },
      { "inventoryState": null }
    ]}
  ]
 }
}]
```

毎週のハードウェア・データ


```
{
  "2020-03-23T12:41:28.045": {
    "cabinetList": [{
      "cabinetName": "STANDALONE_OBJECT_NAME",
      "chassisList": [{
        "itemName": "SN#Y010BG57Y01G",
        "itemUUID": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "itemParentUUID": "",
        "itemLocationRoom": "",
        "itemLocationRack": "",
        "itemLocation": "No Location ConfiguredL",
        "itemLowerUnit": 0,
        "itemType": "CHASSIS",
        "itemHeight": 10,
        "itemSubType": "unknown_type",
        "itemInventory": {
          "accessState": "Online",
          "activationKeys": [],
          "backedBy": "real",
          "bladeSlots": 14,
          "cmmDisplayName": "SN#Y010BG57Y01G",
          "cmmHealthState": "Non-Critical",
          "cmms": [{
            "accessState": "Online",
            "backedBy": "real",
            "cmmDisplayName": "Standby CMM",
            "dataHandle": 1584981183026,
            "cmmHealthState": "Normal",
            "description": "CMM",
            "firmware": [{
              "build": "1AON58O",
              "classifications": [],
              "date": "2020-03-20T04:00:00Z",
              "name": "CMM firmware",
              "revision": "58",
              "role": "",
              "status": "",
              "type": "CMM firmware",
              "version": "2.5.0"
            }],
            "FRU": "68Y7032",
            "fruSerialNumber": "Y030BG168020",
            "hostConfig": [],
            "ipInterfaces": [{
              "IPv4DHCPmode": "UNKNOWN",
              "IPv4enabled": false,
              "IPv6DHCPenabled": false,
              "IPv6enabled": false,
              "IPv6statelessEnabled": false,
              "IPv6staticEnabled": false,
              "label": "External",
              "name": "eth0"
            }],
            "errorFields": [],
            "excludedHealthState": "Normal",
            "leds": [{
              "color": "Amber",
              "location": "FrontPanel",
              "name": "FAULT",
              "state": "Off"
```

```
  }],
  "machineType": "",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
  "name": "Standby CMM",
  "overallHealthState": "Normal",
  "partNumber": "68Y7054",
  "parent": {
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "powerAllocation": {
    "maximumAllocatedPower": 20,
    "minimumAllocatedPower": 20
  },
  "productId": "65",
  "role": "backup",
  "serialNumber": "",
  "slots": [2],
  "type": "CMM",
  "uri": "cmm/F1F06BE6946511E089AEB9871E6892B2",
  "userDefinedName": "",
  "userDescription": "",
  "uuid": "F1F06BE6946511E089AEB9871E6892B2"
}],
"complex": [],
"contact": "No Contact Configured",
"dataHandle": 1584981227532,
"description": "Lenovo Flex System Chassis",
"displayName": "SN#Y010BG57Y01G",
"encapsulation": {
  "encapsulationMode": "normal"
},
"energyPolicies": {
  "acousticAttenuationMode": "Off",
  "hotAirRecirculation": {
    "chassisBay": [],
    "isEnabled": false,
    "maxVariation": 9.0
  },
  "powerCappingPolicy": {
    "cappingPolicy": "OFF",
    "currentPowerCap": 0,
    "maxPowerCap": 5010,
    "minPowerCap": 1504,
    "powerCappingAllocUnit": "watts"
  },
  "powerRedundancyMode": 4
},
"errorFields": [],
"excludedHealthState": "Warning",
"fanSlots": 10,
"fanMuxes": [{
  "cmmDisplayName": "Fan Logic 02",
  "cmmHealthState": "Non-Critical",
  "dataHandle": 0,
  "description": "Fan Logic Module",
  "excludedHealthState": "Warning",
  "FRU": "81Y2912",
  "fruSerialNumber": "Y031BG16D0CE",
```

```
  "hardwareRevision": "4.0",
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "On"
  }],
  "machineType": "",
  "manufactureDate": "2511",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
  "name": "Fan Logic 02",
  "overallHealthState": "Warning",
  "parent": {
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "partNumber": "81Y2990",
  "productId": "338",
  "productName": "IBM Fan Pack Multiplexor Card",
  "serialNumber": "",
  "slots": [2],
  "status": "Non-Critical",
  "type": "FanMux",
  "uri": "fanMux/71F72BE3985011E0B5A8E216694D6175",
  "uuid": "71F72BE3985011E0B5A8E216694D6175"
}],
"fanMuxSlots": 2,
"fans": [{
  "cmmDisplayName": "Fan 06",
  "cmmHealthState": "Normal",
  "dataHandle": 0,
  "description": "IBM Fan Pack",
  "errorFields": [],
  "excludedHealthState": "Normal",
  "firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Fan Controller",
    "revision": "226",
    "role": "",
    "status": "",
    "type": "Fan Controller",
    "version": "226"
  }],
  "FRU": "88Y6685",
  "fruSerialNumber": "YK10JPB69582",
  "hardwareRevision": "4.0",
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FAULT",
    "state": "Off"
  }],
  "machineType": "",
  "manufactureDate": "2411",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
```

```
  "name": "Fan 06",
  "overallHealthState": "Normal",
  "parent": {
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "partNumber": "88Y6691",
  "posID": "11",
  "powerAllocation": {
    "maximumAllocatedPower": 75,
    "minimumAllocatedPower": 75
  },
  "powerState": "Unknown",
  "productId": "342",
  "productName": "80mm Fan Pack for ITE Cooling",
  "serialNumber": "",
  "slots": [6],
  "type": "Fan",
  "userDescription": "",
  "uri": "fan/7293CA21938011E0BC13CB5D330B7C19",
  "uuid": "7293CA21938011E0BC13CB5D330B7C19",
  "vpdID": "373"
}],
"height": 10,
"isConnectionTrusted": "true",
"lastOfflineTimestamp": -1,
"ledCardSlots": 1,
"leds": [{
  "color": "Blue",
  "location": "FrontPanel",
  "name": "Location",
"state": "Off"
}],
"location": {
  "location": "No Location ConfiguredL",
  "lowestRackUnit": 0,
  "rack": "",
  "room": ""
},
"machineType": "8721",
"managerName": "UNKNOWN",
"managerUuid": "UNKNOWN",
"manufacturer": "IBM",
"manufacturerId": "20301",
"mmSlots": 2,
"model": "HC1",
"name": "SN#Y010BG57Y01G",
"nist": {
  "currentValue": "Compatibility",
  "possibleValues": ["Nist_800_131A_Strict","unsupported","Nist_800_131A_Custom","Compatibility"]
},
"nodes": [{
  "accessState": "Online",
  "activationKeys": [],
  "addinCards": [],
  "addinCardSlots": 0,
  "arch": "Unknown",
  "backedBy": "real",
  "bladeState": 0,
  "bladeState_health": "CRITICAL",
  "bladeState_string": "Init failed",
```

```
"bootMode": {
  "currentValue": "",
  "possibleValues": []
},
"bootOrder": {
  "bootOrderList": [],
  "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)/bootOrder"
},
"cmmDisplayName": "Node 07",
"cmmHealthState": "Critical",
"complexID": -1,
"contact": "",
"dataHandle": 1584981175839,
"description": "",
"driveBays": 0,
"drives": [],
"embeddedHypervisorPresence": false,
"encapsulation": {
  "encapsulationMode": "notSupported"
},
"errorFields": [
  { "HostAndDomain": "NO_CONNECTOR" },
  { "PhysicalAndLocation": "NO_CONNECTOR" },
  { "Encapsulation": "NO_CONNECTOR" },
  { "Memory": "NO_CONNECTOR" },
  { "ServerFirmwareData": "NO_CONNECTOR" },
  { "RackCPU": "NO_CONNECTOR" },
  { "ServerOnboardPciDevices": "NO_CONNECTOR" },
  { "BootMode": "NO_CONNECTOR" },
  { "SecureBootMode": "NO_CONNECTOR" },
  { "BootOrder": "NO_CONNECTOR" },
  { "FlashDimm": "NO_CONNECTOR" },
  { "HostMacAddress": "NO_CONNECTOR" },
  { "VnicMode": "NO_CONNECTOR" },
  { "RemotePresenceEnabled": "NO_CONNECTOR" },
  { "ActivationKey": "NO_CONNECTOR" },
  { "LanOverUsbMode": "NO_CONNECTOR" },
  { "ServerStaticMetrics": "NO_CONNECTOR" },
  { "ScalableComplexPartitionUUIDData": "NO_CONNECTOR" },
  { "ActiveAlerts": "NO_CONNECTOR" },
  { "PFAConfiguration": "NO_CONNECTOR" },
  { "ServerIPaddresses": "NO_CONNECTOR" },
  { "FaceplateInfo": "NO_CONNECTOR" },
  { "IOCompatibilityData": "NO_CONNECTOR" },
  { "LanOverUsbPortForwardingModes": "NO_CONNECTOR" },
  { "ServerConfigFiles": "NO_CONNECTOR" }
],
"excludedHealthState": "Normal",
"expansionCards": [],
"expansionCardSlots": 0,
"expansionProducts": [],
"expansionProductType": "",
"faceplateIDs": [],
"firmware": [],
"flashStorage": [],
"FRU": "",
"fruSerialNumber": "",
"hasOS": false,
"hostMacAddresses": "",
"ipInterfaces": [],
"isConnectionTrusted": "true",
```

```
"isITME": false
"isRemotePresenceEnabled": false,
"isScalable": false,
"lanOverUsb": "disabled",
"lanOverUsbPortForwardingModes": [],
"leds": [],
"location": {
  "location": "",
  "lowestRackUnit": 0,
  "rack": "",
  "room": ""
},
"logicalID": -1,
"m2Presence": false,
"machineType": "",
"manufacturer": "",
"manufacturerId": "",
"memoryModules": [],
"memorySlots": 0,
"mgmtProcType": "UNKNOWN",
"model": "",
"name": "Node 07",
"nist": {
  "currentValue": "Unknown",
  "possibleValues": ["Nist_800_131A_Strict","unsupported","Compatibility"]
},
"onboardPciDevices": [],
"osInfo": {
  "description": "",
  "storedCredential": ""
},
"overallHealthState": "Normal",
"parent": {
  "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
  "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
},
"partitionID": -1,
"partNumber": "",
"pciCapabilities": [],
"pciDevices": [],
"ports": [],
"posID": "",
"powerAllocation": {
  "maximumAllocatedPower": 0,
  "minimumAllocatedPower": 0
},
"powerStatus": 0,
"powerSupplies": [],
"primary": false,
"processors": [],
"processorSlots": 0,
"productId": "",
"productName": "",
"raidSettings": [],
"secureBootMode": {
  "currentValue": "",
  "possibleValues": []
},
"securityDescriptor": {
  "managedAuthEnabled": false,
  "managedAuthSupported": true,
```

```
    "publicAccess": false,
    "roleGroups": ["lxc-supervisor"],
    "storedCredentials": {
      "description": "Credentials for null",
      "id": "1703",
      "userName": "USERID"
    },
    "uri": "nodes/dummy-671d5d9ebb4440a4-chassis(1)-blade(7)"
  },
  "serialNumber": "",
  "slots": [7],
  "status": {
    "message": "managed",
    "name": "MANAGED"
  },
  "subSlots": [],
  "subType": "",
  "tlsVersion": {
    "currentValue": "Unknown",
    "possibleValues": ["unsupported","TLS_12","TLS_11","TLS_10"]
  },
  "type": "ITE",
  "uri": "nodes/DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
  "userDefinedName": "",
  "userDescription": "",
  "uuid": "DUMMY-671D5D9EBB4440A4-CHASSIS(1)-BLADE(7)",
  "vnicMode": "disabled",
  "vpdID": ""
}],
"overallHealthState": "Warning",
"parent": {
  "uri": "cabinet/",
  "uuid": ""
},
"partNumber": "88Y6660",
"passThroughModules": [],
"posID": "14",
"powerAllocation": {
  "allocatedOutputPower": 1504,
  "midPlaneCardMaximumAllocatedPower": 38,
  "midPlaneCardMinimumAllocatedPower": 38,
  "remainingOutputPower": 3506,
  "totalInputPower": 5445,
  "totalOutputPower": 5010
},
"powerSupplies": [{
  "dataHandle": 0,
  "cmmDisplayName": "Power Supply 06",
  "cmmHealthState": "Non-Critical",
  "description": "Power Supply",
  "excludedHealthState": "Warning",
  "firmware": [{
    "build": "",
    "classifications": [],
    "date": "",
    "name": "Power Supply Firmware",
    "revision": "0",
    "role": "",
    "softwareID": "",
    "status": "",
    "type": "Power Supply Firmware",
```

```
    "version": ""
  }               ],
  "FRU": "69Y5817",
  "fruSerialNumber": "ZK125115V0VS",
  "hardwareRevision": "5.0",
  "healthState": "NA",
  "inputVoltageIsAC": true,
  "inputVoltageMax": -1,
  "inputVoltageMin": -1,
  "leds": [{
    "color": "Green",
    "location": "Planar",
    "name": "OUT",
    "state": "Off"
  }],
  "machineType": "",
  "manufactureDate": "2211",
  "manufacturer": "IBM",
  "manufacturerId": "20301",
  "model": "",
  "name": "Power Supply 06",
  "overallHealthState": "Warning",
  "parent": {
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36"
  },
  "partNumber": "69Y5801",
  "posID": "60",
  "powerAllocation": {
    "totalInputPower": 0,
    "totalOutputPower": 343
  },
  "powerState": "Unknown",
  "productId": "303",
  "productName": "IBM 2500 W Power Supply",
  "serialNumber": "",
  "slots": [6],
  "type": "PowerSupply",
  "uri": "powerSupply/04382F96885411E00095009500950095",
  "userDescription": "",
  "uuid": "04382F96885411E00095009500950095",
  "vpdID": "128"
}],
"powerSupplySlots": 6,
"productId": "336",
"productName": "IBM Chassis Midplane",
"securityDescriptor": {
  "managedAuthEnabled": false,
  "managedAuthSupported": true,
  "publicAccess": false,
  "roleGroups": ["lxc-supervisor"],
  "storedCredentials": {
    "description": "Credentials for null",
    "id": "1703",
    "userName": "USERID"
  },
  "uri": "chassis/671d5d9ebb4440a49d9daf08a9edfb36"
},
"SecurityPolicy": {
  "cmmPolicyState": "ACTIVE",
  "cmmPolicyLevel": "SECURE"
```

```
},
"serialNumber": "23DVG73",
"status": {
  "message": "MANAGED",
  "name": "MANAGED"
},
"switches": [{
  "accessState": "Online",
  "accessStateRecords": [{
    "health": "OFFLINE",
    "ipAddress": "10.241.53.20",
    "messageBundle": "com.lenovo.lxca.inventory.base.bundle.connections.messages",
    "messageDisplay": "Authentication failed occurred due to HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\").",
    "messageID": "0510",
    "messageParameter": "HTTP 401 - Unauthorized (OpenPegasus Error: \"User Unauthorized\")",
    "protocol": "CIM",
    "username": "USERID",
    "timestamp": 1584709239559,
    "trusted": true
  }],
  "attachedNodes": [],
  "backedBy": "real",
  "cmmDisplayName": "IO Module 04",
  "cmmHealthState": "Normal",
  "dataHandle": 1584981209777,
  "description": "FC5022 16Gb SAN Scalable Switch",
  "deviceName": "FC5022",
  "errorFields": [{
    "IOCompatibilityData": "FETCH_FAILED"
  }],
  "excludedHealthState": "Normal",
  "firmware": [{
    "classifications": [],
    "build": "",
    "date": "2016-04-19T04:00:00Z",
    "name": "Main Application",
    "status": "Active",
    "type": "Main Application",
    "version": "7.4.1c"
  }],
  "FRU": "00Y3329",
  "fruSerialNumber": "Y050UZ67D009",
  "ipInterfaces": [{
    "IPv4DHCPmode": "DHCP_THEN_STATIC",
    "IPv4enabled": true,
    "IPv6enabled": true,
    "IPv6DHCPenabled": true,
    "IPv6statelessEnabled": true,
    "IPv6staticEnabled": false,
    "label": "",
    "name": "ioe0"
  }],
  "leds": [{
    "color": "Amber",
    "location": "FrontPanel",
    "name": "FRU Fault",
    "state": "Off"
  }],
  "machineType": "",
  "manufacturer": "LNV",
  "manufacturerId": "20301",
```

```
      "model": "",
      "name": "IO Module 04",
      "ntpPushEnabled": false,
      "ntpPushFrequency": 17,
      "overallHealthState": "Normal",
      "parent": {
        "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
        "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36"
      },
      "partNumber": "00MM452",
      "ports": [],
      "posID": "17",
      "powerAllocation": {
        "maximumAllocatedPower": -1,
        "minimumAllocatedPower": -1
      },
      "powerState": "On",
      "productId": "329",
      "productName": "Flex System FC5022 24-port 16Gb SAN Scalable Switch",
      "protectedMode": "Not supported",
      "securityDescriptor": {
        "managedAuthEnabled": false,
        "managedAuthSupported": true,
        "publicAccess": false,
        "roleGroups": [],
        "storedCredentials": {
          "description": "Credentials for null",
          "id": "1702",
          "userName": "USERID"
        },
        "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6"
      },
      "serialNumber": "",
      "slots": [4],
      "stackMode": "N/A",
      "type": "Switch",
      "uri": "switches/AE986BEC1DD1B201684FC4F57C3B16B6",
      "userDefinedName": "",
      "userDescription": "",
      "uuid": "AE986BEC1DD1B201684FC4F57C3B16B6",
      "vpdID": "309"
    }],
    "switchSlots": 4,
    "tlsVersion": {
      "currentValue": "TLS_12_Server",
      "possibleValues": ["TLS_12_Server","unsupported","TLS_12_Server_Client","SSL_30"]
    },
    "type": "Chassis",
    "uri": "chassis/671D5D9EBB4440A49D9DAF08A9EDFB36",
    "userDefinedName": "SN#Y010BG57Y01G",
    "userDescription": "",
    "uuid": "671D5D9EBB4440A49D9DAF08A9EDFB36",
    "vpdID": "336"
  }
}],
"complexList": [],
"height": 52,
"nodeList": [],
"location": "",
"placeholderList": [],
"room": "",
```

```
    "storageList": [],
    "switchList": [],
    "UUID": "STANDALONE_OBJECT_UUID"
   }]
  }
}
```

第 4 章 ディスク・スペースの管理

Lenovo XClarity Administrator によって使用されているディスク・スペースの大きさを管理できます。すぐには必要のない大きなデータ・ファイルを リモート共有 に移動するか、不要になったリソースを削除します。

このタスクについて

現在使用されているディスク・スペースの大きさを判別するには、XClarity Administrator メニュー・バーの「**ダッシュボード**」をクリックします。リポジトリーおよび リモート共有 のディスク・スペースの使用率が「XClarity Administrator の活動」セクションに表示されます。

手順

以下の手順の 1 つ以上を実行し、ファイルをリモート共有に移動して不要なリソースを削除することにより、ディスク・スペースを解放します。

- **不要なリソースの削除**

  以下のステップを実行することで、不要になったファイルをローカル・リポジトリーから簡単に削除できます。

  1. XClarity Administrator のメニュー・バーで、「**管理**」 → 「**ディスク・クリーンアップ**」をクリックして、「ディスク・クリーンアップ」ページを表示します。
  2. 削除するファイルを選択します。セクション・ヘッダーに、ファイルを削除したときに解放される容量が表示されます。
     - **オペレーティング・システム関連ファイル**

       OS イメージ、ブート・オプション・ファイル、およびソフトウェア・ファイルを削除できます。
     - **ファームウェア更新**

       UpdateXpress System Packs (UXSPs) に関連付けられたすべての OS デバイス・ドライバー、およびダウンロード済み状態の個々のデバイス・ドライバーのペイロード・ファイルを削除できます。

       ダウンロード済み状態になっていて、ファームウェア・コンプライアンス・ポリシーで使用しない個々のファームウェア更新のペイロード・ファイルを削除できます。

       ダウンロード済み状態の管理サーバーの更新のペイロード・ファイルを削除できます。

       注：ファームウェア更新リポジトリーがリモート共有にある場合は、ディスク・クリーンアップ機能を使用して個々のファームウェア更新や UXSP を削除することはできません。
     - **サービス・データ・ファイル**

       デバイスでサービス・イベントが発生すると、そのデバイスのサービス・データが自動的に収集されます。管理サーバーのサービス・データは、XClarity Administrator で例外が発生するたびに自動的に収集されます。XClarity Administrator と管理対象デバイスが問題なく実行されている場合、これらのアーカイブは定期的に削除することをお勧めします。

       管理サーバーの更新が正常に適用されると、更新ファイルがリポジトリーから自動的に削除されます。
  3. 「**選択を削除**」をクリックします。
  4. 選択したファイルのリストを確認し、「**削除**」をクリックします。
- **未使用のファームウェア更新パッケージのクリーンアップ**

© Copyright Lenovo 2015, 2025

更新リポジトリー内の未使用のすべてのファームウェア・パッケージを削除するには、XClarity Administrator メニュー・バーで、「**プロビジョニング**」 ➡ 「**ファームウェア更新: リポジトリー**」をクリックし、「**すべての操作**」 ➡ 「**クリーンアップ・リポジトリー**」をクリックします。

最新バージョンを保持するか削除するかは、使用されていない場合に選択できます。

この要求を実行するためのジョブが作成されます。XClarity Administrator メニュー・バーで「**監視**」 ➡ 「**ジョブ**」をクリックすると、ジョブの進行状況を確認できます。

- **ファームウェア更新パッケージのリモート・リポジトリーへの移動**

  デフォルトでは、Lenovo XClarity Administrator はファームウェア更新を保存するためにローカル (内部) リポジトリーを使用します。SSHFS (SSH File System) を使用してマウントされたリモート共有をリモート・リポジトリーとして使用することで、XClarity Administrator のローカル・リポジトリーで使用できるディスク・スペースを解放できます。そのうえで、リモート・リポジトリーから直接ファームウェア更新ファイルを使用して、デバイスのファームウェアのコンプライアンスを維持できます。 詳しくは、XClarity Administrator オンライン・ドキュメントのファームウェア更新のリモート・リポジトリーの使用を参照してください。

  ファームウェア更新リポジトリーの場所を変更する場合、元のリポジトリーから新しいリポジトリーにすべてのファームウェア更新をコピーできます。

  場所を変更しても、元のリポジトリーのファームウェア更新ファイルは自動的にクリーンアップ*されません*。

  ヒント: リモート更新リポジトリーは、複数の XClarity Administrator 管理サーバーで共有できます。

  ファームウェア更新をリモートのファームウェア更新リポジトリーに移動するには、以下の手順を実行します。

  1. リモート共有を XClarity Administrator に追加します (XClarity Administrator オンライン・ドキュメントのリモート共有の管理を参照)。
  2. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**ファームウェア更新: リポジトリー**」の順にクリックします。「ファームウェア更新リポジトリー」ページが表示されます。
  3. 「**すべての操作**」 ➡ 「**リポジトリーの場所の切り替え**」をクリックして、「リポジトリーの場所の切り替え」ダイアログを表示します。
  4. 「**リポジトリーの場所**」ドロップダウン・リストで、先ほど作成したリモート共有を選択します。
  5. リポジトリーの場所を切り替える前に、「**現在のリポジトリーから新しいリポジトリーに更新パッケージをコピー**」を選択して、ファームウェア更新ファイルを新しいリポジトリーの場所にコピーします。
  6. 「**OK**」をクリックします。

     ファームウェア更新パッケージを新しいリポジトリーにコピーするジョブが作成されます。XClarity Administrator メニュー・バーで「**監視**」 ➡ 「**ジョブ**」をクリックすると、ジョブの進行状況を確認できます。
  7. ローカル・リポジトリーのファームウェア更新ファイルをクリーンアップします。
     a. 「**すべての操作**」 ➡ 「**リポジトリーの場所の切り替え**」をクリックしてローカル・リポジトリーに場所を切り替え、リポジトリーの場所に「**ローカル・リポジトリー**」を選択して「**OK**」をクリックします。
     b. 「**個別更新**」タブをクリックし、表の「すべて選択」チェックボックスをクリックしてすべてのファームウェア更新を選択して、「**更新パッケージ・ファイルを完全に削除**」アイコン ( ) をクリックします。
     c. 「**UpdateXpress System Pack (UXSP)**」タブをクリックし、表の「すべて選択」チェックボックスをクリックしてすべての UXSP を選択して、「**UXSP および関連ポリシーの削除**」アイコン ( ) をクリックします。

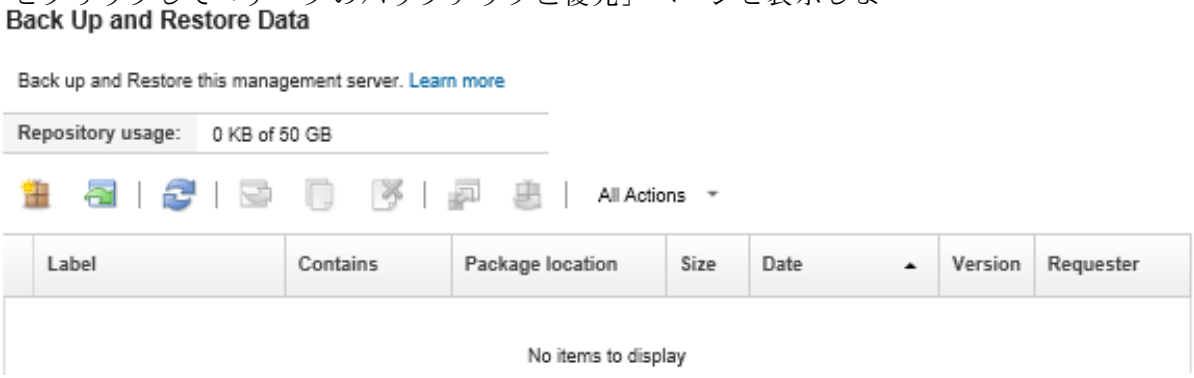
d. 「**すべての操作**」 ➡ 「**リポジトリーの場所の切り替え**」をクリックしてリモート・リポジトリーに場所を切り替え、リポジトリーの場所に新しいリモート・リポジトリーを選択して「**OK**」をクリックします。

- **リモート共有への XClarity Administrator バックアップの移動**

  XClarity Administrator バックアップを リモート共有 に移動させることで、XClarity Administrator リポジトリーが使用できるディスク・スペースを解放できます。ただし、リモート共有 にあるファイルを直接使用することはできません。ファイルを使用するには、XClarity Administrator ローカル・リポジトリーに戻す必要があります。リモート共有について詳しくは、XClarity Administrator オンライン・ドキュメントの リモート共有の管理を参照してください。

  重要：XClarity Administrator のバックアップを削除する前に、ローカル・システムにバックアップをダウンロードするか、リモート共有にバックアップをコピーすることをお勧めします。

  1. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**データのバックアップと復元**」 をクリックして「データのバックアップと復元」ページを表示します。

     「**パッケージの場所**」列は、XClarity Administrator ローカル・リポジトリーにローカルで保存されているか、リモート共有にあるバックアップが保存されている場所を識別します。
  2. バックアップを選択し、「**バックアップのコピー**」アイコン ( ) をクリックして「バックアップのコピー」ダイアログを表示します。
  3. リモート共有を選択してバックアップを保存します。
  4. 「**コピー**」をクリックします。
  5. 「ジョブ」ページでコピーの進行状況を監視します。コピーが完了したら、もう一度バックアップを選択し、「**バックアップの削除**」アイコン ( ) をクリックして、「バックアップの削除」ダイアログを表示します。
  6. 場所では「ローカル」を選択します。
  7. 「**削除**」をクリックします。

第 5 章　検出および管理に関する問題

この情報を使用して、デバイスの検出および管理に関する問題をトラブルシューティングしてください。

デバイスを検出できない

この情報を使用して、管理可能なデバイスを探索するときの問題をトラブルシューティングしてください。

1. Lenovo XClarity Administrator でそのデバイスがサポートされていることを確認します。サポートされるデバイスのリストについては、「XClarity Administrator のサポート – 互換性に 関する Web ページ」を参照してください。「**互換性**」タブをクリックして、該当するデバイス・タイプのリンクをクリックします。
2. ネットワーク上のデバイスに XClarity Administrator から到達できることと、ネットワーク上の XClarity Administrator にデバイスから到達できることを確認します。
3. ファイアウォールで正しいポートが開いていることを確認します。ポートの要件について詳しくは、XClarity Administrator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。
4. ユニキャストおよびマルチキャスト SLP がネットワーク上で有効になっていることを確認します。
5. ThinkServer サーバーの場合
   a. サーバーの管理 Web インターフェースを使用して、サーバーのホスト名が有効なホスト名または IP アドレスを使用して構成されていることを確認します。
   b. ThinkServer System Manager (TSM) 上で SLP が有効になっており、ホスト名が有効になっていることを確認します。
      - SLP がどのThinkServer サーバーで有効にされているかを判別するには、優先 SLP ツールを使用して、WBEM サービスに SLP 要求照会を送信します。
        ```
        $ slptool findsrvs service:wbem
        service:wbem:http://<TSM_IP>:5988,65535
        service:wbem:https://<TSM_IP>:5989,65535
        ```
      - SLP が特定の ThinkServer で有効にされているかを判別するには、優先 SLP ツールを使用して、WBEM サービスに SLP 要求照会を送信します。
        ```
        $ slptool unicastfindattrs <TSM_IP> service:wbem
        (template-type=wbem),(template-version=2.0),(template-url-syntax=service:URL),
        (service-hi-name=qom),(service-hi-description=Quasi Object Manager 1.0.0),
        (CommunicationMechanism=cim-xml),(CommunicationMechanismsVersion=1.0),
        (MultipleOperationsSupported=false),(AuthenticationMechanismsSupported=Basic),
        (InteropSchemaNamespace=root/interop),(service-id=Lenovo G5 WBEM Service)
        ```
      - デバイスが SLP 要求に応答しない場合は、以下のパラメーターを使用して TSM に IPMI コマンドを送信し、TSM ファームウェアを再起動します。TSM が再起動するまでに数分かかる場合があります。
        ```
        NetFn = 0x06
        Command = 0x03
        Data = ()
        ```
        次の例では、 `ipmitool` オープン・ソース・ツールを使用して SLP を有効にします。
        ```
        $ ipmitool -H <TSM_IP> -U <ipmi_user> -P <ipmipassword> raw 0x06 0x03
        ```
6. RackSwitch スイッチの場合は、SLPが有効になっており、ホスト名が構成スイッチで設定されていることを確認します。
   - ThinkSystem DB シリーズ・スイッチは検出できません。これらのスイッチを管理するには、「新しいデバイスの検出と管理」ページで「**手動入力**」をクリックして、スイッチの IP アドレスを手動で入力します。

© Copyright Lenovo 2015, 2025

- NVIDIA Mellanox スイッチを検出できません。これらのスイッチを管理するには、「新しいデバイスの検出と管理」ページで「**手動入力**」をクリックして、スイッチの IP アドレスを手動で入力します。
- その他のスイッチの場合は、SLP が有効になっており、ホスト名がスイッチ構成で設定されていることを確認します。
  - SLP がどのスイッチで有効にされているかを判別するには、優先SLPツールを使用して、次のSLPマルチキャスト要求を送信します。

    注：この要求は、SLP ツールが実行中のサーバーと同じサブネット上にあるスイッチだけを検索します。

    ```
    $ slptool findsrvs service:io-device.Lenovo:management-module
    service:io-device.Lenovo:management-module://<RackSwitch IP>,64225
    ```
  - SLP が特定のスイッチで有効にされているかを判別するには、優先 SLP ツールを使用して、次のユニキャスト SLP 要求を送信します。
    ```
    $ slptool findattrs service:io-device.Lenovo:management-module://<RackSwitch IP>
    (level=1.0),(Type=switch),(data-protocols=ethernet),(serial-number=US7116000D),
    (sysoid=1.3.6.1.4.1.26543.1.7.6),(ipv4-enabled=TRUE),(ipv4-address=<RackSwitch IP>),
    (ipv6-enabled=FALSE),ipv6-addresses,(ipv4-mgmt-protocols=http:80:true,https:443:true,
    telnet:23:true,ssh:22:true,snmpv1v2v3:161:true,snmpv3only:161:false),
    (snmp-engineid=80:00:67:af:03:08:17:f4:33:d3),
    (ssh-fingerprint=8a:43:cb:be:47:d9:31:37:7a:3b:80:f6:dd:00:61:a6),
    (deviceName=<RackSwitch hostname>)
    ```

7. (ThinkSystem DE シリーズ以外の) Lenovo Storage デバイスの場合、SLP が有効になっており、ネットワークが XClarity Administrator とストレージ・デバイス間の SLP 通信をブロックしていないことを確認します。
   - SLP がどのストレージ・デバイスで有効にされているかを判別するには、優先 SLP ツールを使用して、API サービスに SLP 要求照会を送信します。
     ```
     $ slptool findsrvs service:api
     service:api:https://<CONTROLLER_IP>:443/api,65535
     service:api:https://<CONTROLLER_IP>:443/api,65535
     ```
   - SLP が特定のストレージ・デバイスで有効にされているかを判別するには、優先 SLP ツールを使用して、API サービスに SLP 要求照会を送信します。
     ```
     $ slptool unicastfindattrs <CONTROLLER_IP> service:api
     (x-system-name=S3200_5.65),(x-system-location=rack\2Crack\2Crack),(x-system-contact=Support contact),
     (x-system-information=S3200_65),(x-vendor-name=Lenovo),(x-product-id=S3200),(x-product-brand=Storage),
     (x-midplane-serial-number=00C0FF2682A8),(x-platform-type=Gallium),(x-bundle-version=""),
     (x-build-date=""),(x-health=OK),(x-wwnn=208000c0ff2682a8),(x-mac-address=00:00:00:00:00:EB)
     ```

   ストレージ・デバイスが SLP 要求に応答しない場合:
   - ネットワークでデバイス間の SLP 通信が許可されていることを確認します。
   - ストレージ・デバイスに「Storage Management Initiative Specification (SMI-S)」が有効になっていることを確認し、管理 Web インターフェースまたは CLI を使用してストレージ・デバイスを再起動します。

デバイスを管理できない

この情報を使用して、デバイスを管理するときの問題をトラブルシューティングしてください。

1. デバイスが Lenovo XClarity Administrator によってサポートされていることを確認してください。デバイスのサポートについての詳細は、「XClarity Administrator のサポート – 互換性に 関する Web ページ」を参照してください。「**互換性**」タブをクリックして、該当するデバイス・タイプのリンクをクリックします。

2. ネットワーク上のデバイスに XClarity Administrator から到達できることと、ネットワーク上の XClarity Administrator にデバイスから到達できることを確認します。
3. 管理に使用される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。ポートの要件について詳しくは、 XClarity Administrator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。
4. XClarity Administrator を使用して管理する各サーバーに、最小限必要なファームウェアがインストールされていることを確認します。XClarity Administrator のサポート – 互換性に 関する Web ページ から最小限必要なレベルのファームウェアを見つけるには、 **互換性**タブをクリックし、該当するデバイス・タイプのリンクをクリックします。
5. XClarity Administratorサーバー証明書に問題がないかどうかを確認します。
   a. XClarity Administrator サーバー証明書の有効期限が切れていないことを確認します。
   b. XClarity Administrator サーバー証明書の SubjectAltName に有効な IP アドレスが含まれていることを確認します (XClarity Administrator オンライン・ドキュメントのXClarity Administrator へのカスタマイズされたサーバー 証明書のデプロイを参照)。
6. サーバーの日付が LDAP 証明書と競合していないことを確認します。たとえば、LDAP 証明書が 2022/8/3 から 2024/11/3 まで有効で、XCC の日付が 2000-04-15 である場合、サーバーは TLS チェックに合格しません。
7. 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。
   a. `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。
   b. 「**IMM 管理**」 ➡ 「**セキュリティー**」をクリックします。
   c. 「**CIM Over HTTPS**」タブをクリックして、「**CIM Over HTTPS を有効にする**」を選択していることを確認します。
8. ThinkSystem SR635 および SR655 サーバーの場合:
   - 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 Administrator 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。TSM を使用して IPMI over LAN を有効にするには、「**設定**」 ➡ 「**IPMI の構成**」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。
9. 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 Administrator 信頼ストアにインポートされていることを確認します (XClarity Administrator オンライン・ドキュメントの 管理対象デバイスへのカスタマイズされたサーバー証明書の デプロイ を参照。
10. デバイスの資格情報が正しいことを確認します。

    注：パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。

    デバイスが XClarity Administrator により管理されているとき、管理コントローラーのユーザーは集中型で管理されます。つまり、XClarity Administrator 内部または外部認証サーバーで定義されているユーザー・アカウントが管理コントローラーへのログインにも使用されます。管理コントローラーで他の全てのローカル・アカウントが無効になっている間、RECOVERY_ID という新しいローカル・ユーザー・アカウントが作成されます。

    集中型ユーザー管理の構成中に管理プロセスに失敗した場合、管理コントローラーのローカル・ユーザー・アカウントが無効になることがあります。以下の手順を実行して、ローカル・ユーザー・アカウントをリカバリーします。

    - コンバージド、NeXtScale、および System x サーバー

a. 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。
b. 「**IMM 管理**」 ➔ 「**ユーザー**」をクリックします。
c. 管理コントローラーのユーザー認証方式を「**最初にローカル認証、次に LDAP**」に設定します。
   1) 「**グローバル・ログイン設定**」をクリックします。「グローバル・ログイン設定」ダイアログが表示されます。
   2) 「**General**」タブをクリックします。
   3) ユーザー認証方式で「**最初にローカル認証、次に LDAP**」を選択し、「**OK**」をクリックします。
d. ローカル・ユーザー・アカウント (RECOVERY_ID ユーザー・アカウント以外) を削除して再作成します。
e. 「**管理の強制**」オプションを使用してシャーシの管理を再度試み、前の管理試行から残りの CIM サブスクリプションをクリーンアップします。

- シャーシ
  a. RECOVERY_ID ユーザー・アカウントを使用して、SSH セッションからシャーシの管理 CLI インターフェースにログインします。
  b. 次のコマンドを実行してユーザーの集中管理を無効にし、ローカル・ユーザー・アカウントを使用して管理コントローラーと他のシャーシ・コンポーネントを認証できるようにします。

     注：このコマンドを実行すると、RECOVERY_ID ユーザー・アカウントがユーザー・レジストリーから削除され、CLI セッションが終了します。ローカル・ユーザー・アカウントを使用して管理コントローラーと他のシャーシ・コンポーネントを認証できるようになります。

     ```
     fsmcm -off -T mm[p]
     ```

  c. 「**管理の強制**」オプションを使用してシャーシの管理を再度試み、前の管理試行から残りの CIM サブスクリプションをクリーンアップします。

11. RackSwitch スイッチの場合
    - スイッチで SSH が有効になっていることを確認します。
    - 設定されている場合は、スイッチの特権実行モードに入るために使用する「有効」パスワードが正しいことを確認します。
12. System x3950 X6 サーバーの場合、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 4U エンクロージャーとして管理する必要があります。
13. デバイスのシステム・ボードが交換された場合、デバイスには新しいシリアル番号と UUID が割り当てられます。XClarity Administrator が交換前と同じデバイスとしてデバイスを認識するようにする場合、以前のシリアル番号および UUID と一致するようにシリアル番号および UUIDを更新する必要があります。手順については、ご使用のデバイスの資料を参照してください。
14. デバイスが XClarity Administrator によって管理されていたが正しく管理除外されなかった場合、リカバリー手順については以下の情報を参照してください。
    - XClarity Administratorオンライン・ドキュメントの 管理サーバーの障害発生後の CMM による シャーシ管理のリカバリー
    - XClarity Administratorオンライン・ドキュメントの 管理サーバーの障害後のサーバー管理のリカバリー
    - XClarity Administratorオンライン・ドキュメントの 正しく管理解除されなかった RackSwitch スイッチの リカバリー
    - XClarity Administratorオンライン・ドキュメントの 管理サーバーの障害発生後の Lenovo Storage デバイスによる 管理のリカバリー

SSL/TSL 証明書が無効なため、ストレージ・デバイスを管理できない

この情報を使用して、ストレージ・アレイを管理するときの問題をトラブルシューティングしてください。

各デバイスには、Lenovo XClarity Administrator が HTTPS を介してデバイスと通信するために使用する自己署名 SSL 証明書があります。この証明書には、証明書に関連付けられたホスト名 (IP アドレス) を識別する共通名 (CN) があります。共通名は SSL 証明書で保護されている名前を表し、証明書は要求のホスト名が証明書の共通名と一致する場合にのみ有効です。したがって、ストレージ・アレイの IP アドレスが変更された場合、既存の証明書は無効になり、SSL/TSL 証明書が無効であるため、XClarity Administrator はそのアドレスを管理できません。

この問題を解決するには、以下の手順を実行します。

- DE ストレージ・デバイスから送信された証明書の CN 値の IP アドレスが IPv4 形式でがあることを確認します。
- 既存の SSL/TSL 認証が有効であることを確認します
  - Lenovo ThinkSystem DE ストレージ・アレイでは、ストレージ・アレイの管理証明書を出荷時の自己署名証明書にリセットします。詳しくは、ThinkSystem Storage DE シリーズ・オンライン・ドキュメントの 管理証明書のリセット を参照してください。
  - Lenovo ThinkSystem DS ストレージ・アレイでは、管理 Web インターフェースまたは CLI を使用して、新しい IP アドレスまたはホスト名で正しい CN により証明書を再生成するために、ストレージ・デバイスの管理コントローラーを再起動します。

SSL/TSL 証明書が無効なため、スイッチを管理できない

この情報を使用して、CNOS を実行中のスイッチを管理する際の証明書の問題をトラブルシューティングしてください。

各デバイスには、Lenovo XClarity Administrator が HTTPS を介してデバイスと通信するために使用する自己署名 SSL 証明書があります。スイッチの証明書を削除または再生成すると、スイッチと XClarity Administrator の間の通信が失敗し、スイッチはオフラインと表示されます。

この問題を修正するには、「すべてのスイッチ」ページでスイッチを選択し、**「すべての操作」 ➡ 「セキュリティー」 ➡ 「信頼できない証明書を解決」** をクリックします。

背面 LED カードまたはミッドプレーン・アセンブリーを交換した後、管理対象 Flex System シャーシの接続をリカバリーできない

Lenovo XClarity Administrator は、世界固有識別子 (UUID) および UUID ベースのトラステッド証明書を使用してデバイスを管理します。Flex System シャーシの場合、UUID は、ミッドプレーン・アセンブリーにある背面 LED カードに重要プロダクト・データ (VPD) の一部として保存されます。背面 LED カード・アセンブリーまたはミッドプレーン・アセンブリーを交換する場合は、交換する背面 LED カードにある UUID を新しい背面 LED カードに転送する必要があります。

1. シャーシの UUID を取得します。シャーシが動作していない場合は、サポートに連絡してシャーシ・ラベルの 1 つにあるマシン・タイプおよびシリアル番号を提供することで、UUID を入手できます。
2. シャーシの UUID を変更します。ミッドプレーン/背面 LED カードの交換と UUID の変更の手順については、Lenovo Flex System オンライン・ドキュメント でご使用のデバイスを参照してください。
3. シャーシの非トラステッド証明書を解決します。
   a. XClarity Administrator メニュー・バーで、**「ハードウェア」 ➡ 「シャーシ」** をクリックします。「すべてのシャーシ」ページが表示されます。
   b. 交換した部品があるシャーシを選択します。
   c. **「すべての操作」 ➡ 「セキュリティー」 ➡ 「信頼できない証明書を解決」** の順にクリックします。
   d. **「証明書をインストールする」** をクリックします。

XClarity Administrator は現在の証明書をターゲット・シャーシから取得し、XClarity Administrator 信頼ストア内に配置して、そのシャーシの前の証明書をオーバーライドします。

4. シャーシのインベントリーを最新の情報に更新するには、「**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**」をクリックします。

システム・ボードを交換した後、管理対象サーバーの接続性をリカバリーできない

Lenovo XClarity Administrator は、世界固有識別子 (UUID) および UUID ベースのトラステッド証明書を使用してデバイスを管理します。サーバーの場合、UUID はシステム・ボードに重要プロダクト・データ (VPD) の一部として保存されます。システム・ボードを交換する場合、新しいシステム・ボードに交換されたシステム・ボードの UUID を転送する必要があります。

重要：システム・ボードを交換する前に、サーバーの管理を解除することをお勧めします。システム・ボードの交換後に、サーバーはもう一度管理できるようになります。

新しいシステム・ボードに交換されたシステム・ボードの UUID を転送するには、以下の操作を実行します。

1. サーバーの UUID を取得します。サポートが動作していない場合は、サポートに連絡してサポート・ラベルの 1 つにあるマシン・タイプおよびシリアル番号を提供することで、UUID を入手できます。
2. サーバーの UUID を変更します。コンポーネントの交換と UUID の変更の手順については、ご使用のデバイスのハードウェア・マニュアルを参照してください。
3. サーバーの非トラステッド証明書を解決します。
   a. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**サーバー**」の順にクリックします。「すべてのシャーシ」ページが表示されます。
   b. 交換した部品があるサーバーを選択します。
   c. 「**すべての操作**」 → 「**セキュリティー**」 → 「**信頼できない証明書を解決**」の順にクリックします。
   d. 「**証明書をインストールする**」をクリックします。

   XClarity Administrator は現在の証明書をターゲット・サーバーから取得し、XClarity Administrator 信頼ストア内に配置して、そのサーバーの前の証明書をオーバーライドします。
4. サーバーのインベントリーを最新の情報に更新するには、「**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**」をクリックします。

サーバーを管理解除した後、encapsulation が無効にならない

共通 encapsulation が有効になっている場合、encapsulation モードはサーバーの管理時に「encapsulation lite」に変更されます。通常、サーバーを管理対象から除外すると、encapsulation モードは「normal」(無効) に戻ります。

encapsulation モードが「normal」に変更されない場合は、以下の手順を実行して encapsulation を無効にします。

1. ベースボード管理コントローラーをリブートします。
2. 障害が発生した Lenovo XClarity Administrator 仮想アプライアンスの IP アドレスを使用するように構成されたシステムからターゲット・サーバーに接続します。デバイスに対して SSH セッションを開き、次のコマンドを実行することで、encapsulation を無効にします。
   ```
   encaps lite off
   ```

計算ノードを管理した後に、ユーザー・インターフェースに表示されない

先に既存のサーバーを管理解除せずにシャーシ内の ThinkSystem SD530 を交換した場合、新しいサーバーがユーザー・インターフェースに表示されない場合があります。

この問題を解決するには、強制オプションを使用してシャーシを管理解除し、シャーシ内のすべての ThinkSystem SD530 を再度管理します。

サーバーの電源状態が正しくない

オペレーティング・システムがないサーバーの電源をオンにすると、Lenovo XClarity Administrator でそのサーバーの電源状態が正しく表示されない場合があります。

この問題を解決するには、以下の手順のいずれかを実行してください。

- ベア・メタル・サーバーの電源がオフであることを確認します。
- XClarity Administrator v1.2.2 以降では、サーバーを起動して BIOS/UEFI (F1) セットアップに入ります (XClarity Administrator オンライン・ドキュメントのサーバーの電源のオン/オフを参照)。

第 6 章 インストール、削除、更新、およびデータ移行に関する問題

この情報を使用して、インストール、削除、更新、およびデータ移行に関する問題をトラブルシューティングしてください。

XClarity Administrator を Red Hat KVM にインストールする場合、ビデオ出力が表示されない

Red Hat KVM ユーザー・インターフェースを使用した Lenovo XClarity Administrator 仮想アプライアンスのインストール時にコンソールにビデオ出力がなく、XClarity Administrator 仮想マシンの起動時に仮想マシンのバナーと XClarity Administrator IP 情報が表示されず、コンソール画面が暗転することがあります。

コンソールのビデオ出力を表示するには、XClarity Administrator 仮想ハードウェア詳細画面を開き、左側のナビゲーションで「**ビデオ**」をクリックして、ビデオ・デバイスが **Cirrus** に設定されていることを確認します。デフォルトでは、RedHat KVM ユーザー・インターフェースではビデオ・デバイスは QXL に設定されます。

アダプターの変更が認識されない

アダプターの取り外し、交換、または構成を行った後、Lenovo XClarity Administrator で変更が認識されません。

ベースボード管理コントローラー (BMC) が変更を認識できるように、デバイスを再起動します。詳しくは、System x オンライン・ドキュメントを参照してください。

初期セットアップ中に Web ブラウザーで初期セットアップ・ウィザードを開くことができない

この情報を使用して、Lenovo XClarity Administrator を初期セットアップするときの問題をトラブルシューティングしてください。

1. 物理ホスト・システムが最小システム要件を満たしていることを確認します (XClarity Administrator オンライン・ドキュメントのサポートされているホスト・システムを参照)。
2. 最小システム要件を満たしサポートされている仮想システムを使用していることを確認します (XClarity Administrator オンライン・ドキュメントのサポートされているホスト・システムを参照)。
3. Web ブラウザーのバージョンが XClarity Administrator と互換性があることを確認します。サポート対象の Web ブラウザーのリストについては、XClarity Administrator オンライン・ドキュメントのXClarity Administrator Web インターフェースへのアクセスを参照してください。
4. デフォルトでは、ネットワーク構成で DHCP が有効になっています。仮想マシンにローカルでログインし、`ifconfig` コマンドを実行して、有効な IP アドレスが割り当てられていることを確認します。静的構成を使用している場合は、必ず以下の手順に従ってインストールを正しく構成します。詳細については、XClarity Administratorオンライン・ドキュメントのVMware ESXi ベースの環境における XClarity Administrator のインストールを参照してください。

Lenovo XClarity Administrator デプロイメントが予期せず失敗する

この情報を使用して、Lenovo XClarity Administrator を初期セットアップするときの問題をトラブルシューティングしてください。

© Copyright Lenovo 2015, 2025

1. イベント・ログでデプロイメント関連のイベントがないか調べて、先にそれらを解決します。イベント・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのイベントの使用を参照してください。
2. 物理ホスト・システムが最小システム要件を満たしていることを確認します。
3. システムまたは仮想システムが最小システム要件を満たしていることを確認します。
4. サポートされている仮想マシン・マネージャーを使用していることを確認します。

要件について詳しくは、XClarity Administrator オンライン・ドキュメントのサポートされているホスト・システムを参照してください。

Lenovo XClarity Administrator の更新に失敗する

この情報を使用して、Lenovo XClarity Administrator の更新に関する問題をトラブルシューティングしてください。

1. 前提条件となる更新がインストールすべてされていることを確認します。
2. 更新をインストールするためのユーザー権限があることを確認します。

XClarity Administrator の更新について詳しくは、XClarity Administrator オンライン・ドキュメントのXClarity Administrator 管理サーバーの更新 を参照してください。

第 7 章　接続の問題

この情報を使用して、接続に関する問題をトラブルシューティングしてください。

Lenovo XClarity Administrator にアクセスできない

この情報を使用して、Lenovo XClarity Administrator に接続するときの問題をトラブルシューティングしてください。

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された場合は、最新のバックアップから XClarity Administrator を復元します。XClarity Administrator のバックアップと復元については、XClarity Administrator オンライン・ドキュメントのXClarity Administrator のバックアップと復元を参照してください。

Safari ブラウザーを使用して Lenovo XClarity Administrator に接続できない

この情報を使用して、Safari Web ブラウザーを使用して XClarity Administrator に接続するときの問題をトラブルシューティングしてください。

Safari Web ブラウザーを使用して XClarity Administrator Web インターフェースに接続しようとすると、ユーザー・アカウントに関連付けられたクライアント証明書のリストが表示されます。これらの証明書のいずれかを選択すると、「接続不可」エラーが発生する可能性があります。この問題は、Safari Web ブラウザーがクライアント証明書を XClarity Administrator に送信しようとしたが、そのクライアント証明書が XClarity Administrator サーバーで有効でない場合に発生する可能性があります。問題を解決するには、クライアント証明書を削除し、もう一度 XClarity Administrator Web インターフェースに接続してみてください。Safari ブラウザーを使用したときのこの問題について詳しくは、Safari クライアント証明書の問題に関する Web ページを参照してください。

ログインできない

この情報を使用して、Lenovo XClarity Administrator、CMM、ベースボード管理コントローラーにログインするときの問題をトラブルシューティングしてください。

Lenovo XClarity Administrator にログインできない

この情報を使用して、Lenovo XClarity Administrator にログインするときの問題をトラブルシューティングしてください。

1. パスワードが正しいこと、Caps Lock キーと Num Lock キーがオンになっていないことを確認します。
2. ユーザー・アカウントがロックされていないことを確認します。ロックされている場合は、スーパーバイザーにユーザー・アカウントのロックを解除してもらってください (XClarity Administrator オンライン・ドキュメントのユーザーのロック解除参照)。
3. ユーザー・アカウントが無効になっていないことを確認します。無効になっている場合は、スーパーバイザーにユーザー・アカウントを有効にしてもらってください (XClarity Administrator オンライン・ドキュメントのユーザーの有効化または無効化参照)。
4. 外部認証サーバーを使用している場合:
   a. XClarity Administrator で正しい役割グループが構成されていることを確認します。役割グループについては、Lenovo XClarity Administrator オンライン・ドキュメントの役割グループの作成を参照してください。
   b. 外部認証サーバーでユーザー・アカウントがそれらの役割グループのいずれかのメンバーとして定義されていることを確認します。

© Copyright Lenovo 2015, 2025

c. XClarity Administrator を外部認証サーバーにバインドするために使用するクライアント・アカウントのパスワードを変更した場合は、必ず XClarity Administrator Web インターフェースの新規パスワードも更新してください。

   1) 現在 XClarity Administrator で定義されているクライアント名とパスワードを使用して XClarity Administrator にログインします (XClarity Administrator オンライン・ドキュメントの外部認証サーバーのセットアップを参照)。
   2) XClarity Administrator のメニュー・バーで、「**管理**」 ➡ 「**セキュリティー**」の順にクリックします。
   3) 「ユーザーとグループ」セクションの「**LDAP クライアント**」をクリックして、「LDAP クライアント設定」ダイアログを表示します。
   4) 「**クライアント・パスワード**」フィールドのパスワードを更新し、「**適用**」をクリックします。

   外部認証サーバーでパスワードが変更された後、ログインの失敗が多すぎるためにクライアント・アカウントがロックされた場合は、外部認証サーバーで直接アカウントのロックを解除するか、ロックアウト期間が過ぎるまで待ってから XClarity Administrator でパスワードを変更してください。

d. XClarity Administrator を外部認証サーバーにバインドするために使用するクライアント・アカウントのパスワードが有効期限切れの場合は、以下の手順を実行してアカウントのロックを解除し、XClarity Administrator でパスワードを変更してください。

   1) クライアント・アカウントをロック解除し、外部認証サーバーのクライアント・パスワードを変更します。
   2) 現在 XClarity Administrator で定義されているクライアント名とパスワードを使用して XClarity Administrator にログインします (XClarity Administrator オンライン・ドキュメントの外部認証サーバーのセットアップを参照)。
   3) XClarity Administrator のメニュー・バーで、「**管理**」 ➡ 「**セキュリティー**」の順にクリックします。
   4) 「ユーザーとグループ」セクションの「**LDAP クライアント**」をクリックして、「LDAP クライアント設定」ダイアログを表示します。
   5) 「**クライアント・パスワード**」フィールドのパスワードを更新し、「**適用**」をクリックします。

5. 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されて、認証エラーが発生するようになった場合は、最新のバックアップから XClarity Administrator を復元します。XClarity Administrator のバックアップと復元については、XClarity Administrator オンライン・ドキュメントの XClarity Administrator のバックアップと復元を参照してください。

ローカル・リカバリーまたはスーパーバイザー・ユーザーのパスワードを忘れた

スーパーバイザー・アカウントまたは別のスーパーバイザー・アカウントが存在しない場合は、新規パスワードで構成ファイルを含む ISO イメージをマウントすることで、**lxc-recovery** または **lxc-supervisor** 権限を持つローカル・ユーザーのパスワードをリセットできます。

始める前に

注意：この手順は、XClarity Administrator v3.3.x および v3.4.x では機能しません。これらのバージョンのいずれかを使用している場合は、Lenovo サポートに連絡して XClarity Administrator へのアクセスのリカバリーを行ってください。

この方法を使用してパスワードをリセットするには、XClarity Administrator ホスト・システムのアクセス権限が必要です。

リセットされているユーザー名には **lxc-recovery** または **lxc-supervisor** 権限が必要です。

パスワードは、XClarity Administrator によって適用される検証規則と同じ規則に従う必要があります。

パスワードがリセットされた後、初回アクセスでパスワードを変更する必要はありません

手順

ISO イメージを作成してマウントするには、以下の手順を実行します。

1. 仮想マシンの電源をオフにします。
2. 以下のパラメーターを含む `passwordreset.properties` という名前のファイルを作成します。
   ```
   user=
   password=
   ```
   エコー・コマンドを使用して、ファイルを作成できます。例:
   ```
   ECHO user=admin > ./ passwordreset.properties
   ECHO password=New_PasswOrd >> ./ passwordreset.properties
   ```
3. passwordreset.properties ファイルが含まれる ISO イメージを作成します。

   Windows で ISO イメージを作成する場合、どの ISO ソフトウェアを使用してもかまいません。Linux では、たとえば `mkisofs` コマンドを使用します。

   ```
   mkisofs -V passreset -J -o ./passreset.iso ./passwordreset.properties
   ```

   -V はボリューム・ラベル、**-J** は Joliet 形式、**-o** は出力ファイル名、/ **passwordreset.properties** は ISO イメージに含めるファイルです
4. データストア・ブラウザーを使用して、適切な場所に ISO イメージをアップロードします。
5. ISO イメージを仮想マシンにマウントします。
   - **Citrix の場合**:
     a. 仮想マシンに物理 CD ドライブとして、構成の ISO イメージをマウントします。
     b. Citrix から、XClarity Administrator 仮想マシンを選択します。
     c. 「**コンソール**」タブをクリックします。
     d. ドライブ・リストから、物理 CD を選択します。
   - **Nutanix AHV ホストの場合**:
     a. 「**Settings**」メニュー (⚙) で、「**Image configuration**」をクリックして「Image Configuration」ダイアログを表示します。
     b. `eth0_config.iso` イメージをアップロードします。
        1) 「Image Configuration」ダイアログで、「**Upload Image**」クリックし、をもう一度「Create Image」ダイアログを表示します。
        2) ISO イメージの名前を指定します。
        3) イメージ・タイプとして ISO を選択します。
        4) 「**ファイルのアップロード**」を選択して「**ファイルの選択**」をクリックし、`eth0_config.iso` イメージを選択します。
        5) 「**保存**」をクリックして、ファイルをアップロードします。
        6) 「**Close**」をクリックして「Image Configuration」ダイアログを閉じます。
     c. セットアップの手順を続行する前に、アップロード・プロセスが完了するまで待ちます。プロセスが完了すると、メニューのステータスが丸になります。
     d. `eth0_config.iso` イメージのディスクを追加します。
        1) VM から下部のメニュー・バーで、「**Update**」をクリックします。
        2) CDROM ディスクの「**Edit**」アイコンをクリックし、「Edit Disk」ダイアログを表示します。

3) 操作として「**Clone from Image Service**」を選択します。
4) イメージ・リストから以前に作成した ISO イメージを選択します。
5) 「**Update**」をクリックします。
6) 「**保存**」をクリックします。

- **RedHat KVM ホストの場合**:
  a. Virtual Machine Manager から、仮想マシンを選択し、「**ハードウェアの追加**」をクリックすると、「新しい仮想ハードウェアの追加」ダイアログが表示されます。
  b. 「**ストレージ**」タブをクリックします。
  c. 「**管理対象ストレージまたは他の既存のストレージの選択**」を選択し、「**参照**」をクリックして、`eth0_config.iso` イメージを選択します。
  d. デバイス・タイプとして「**VirtIO**」を選択します。

     注：XClarity Administrator 1.4.0 以前の場合は、ディスク・バスに「**IDE**」を選択します。
  e. キャッシュ・モードとして「**なし**」を選択します。
  f. 「**完了**」をクリックします。
- **VMware ESXi ホストの場合**:

  XClarity Administrator 仮想マシンで CD/DVD ドライブとしてマウントできるように、ISO ファイルは ESXi ホストのデータストアに存在する必要があります。
  a. 仮想マシンを右クリックし、「**設定の編集**」をクリックします。
  b. 「**追加**」をクリックして、「ハードウェアの追加」ウィザードを表示します。
  c. 「**CD/DVD ドライブ**」をクリックし、「**次へ**」をクリックします。
  d. 「**ISO イメージを使用する**」を選択し、「**次へ**」をクリックします。
  e. ISO イメージを選択し、「**次へ**」をクリックします。
  f. 仮想デバイス・ノードを選択し、「**次へ**」クリックします。
  g. 「**完了**」をクリックします。
- **Windows Hyper-V ホストの場合**:

  重要：ISO イメージをマウントする前に、仮想マシンの電源をオフにする必要があります。
  a. 「Hyper-V マネージャー」ウィンドウで、仮想アプライアンスを右クリックし、「**接続**」をクリックして「仮想マシンの接続」ウィンドウを表示します。
  b. 「**メディア**」 ➞ 「**DVD ドライブ**」 ➞ 「**ディスクの挿入**」の順にクリックします。
  c. ISO イメージを選択し、「**開く**」をクリックします。

6. 仮想マシンの電源をオンにして、`passwordreset.properties` ファイルに指定されたユーザー名とパスワードを使用して XClarity Administrator Web インターフェースにログインします (XClarity Administrator オンライン・ドキュメントの XClarity Administrator Web インターフェースへのアクセスを参照)。
7. ドライブをアンマウントして ISO イメージを削除します。
   - Citrix の場合
     a. Citrix ハイパーバイザーから、XClarity Administrator 仮想マシンを選択します。
     b. 「**コンソール**」タブをクリックします。
     c. ドライバー・リストから、構成 ISO に関連付けられている物理 CD をクリアします。
   - **Nutanix AHV ホストの場合**:
     a. VM から下部のメニュー・バーで、「**Update**」をクリックします。
     b. CDROM ディスクの「**Edit**」アイコンをクリックし、「Edit Disk」ダイアログを表示します。
     c. 「**イジェクト**」アイコンをクリックします。
     d. 「**保存**」をクリックします。

- **VMware ESXi ホストの場合**:
  a. 仮想マシンを右クリックし、「**設定の編集**」をクリックします。
  b. ハードウェアのリストからマウントされたドライブを選択し、「**削除**」をクリックします。
  c. 「**OK**」をクリックします。これでドライブが切断されます。
  d. 仮想マシンを右クリックし、もう一度「**設定の編集**」をクリックします。
  e. ハードウェアのリストからドライブを選択し、「**電源オン時に接続**」チェックボックスのチェックを外します。
  f. 「**OK**」をクリックします。
  g. データストアから ISO イメージを削除します。
- **Windows Hyper-V ホストの場合**:
  a. 「Hyper-V マネージャー」ウィンドウで、仮想アプライアンスを右クリックし、「**接続**」をクリックして「仮想マシンの接続」ウィンドウを表示します。
  b. 「**メディア**」 ➔ 「**DVD ドライブ**」 ➔ 「***iso_image_name*.iso の取り出し**」をクリックします。
  c. データストアから ISO イメージを削除します。

管理対象 CMM に直接ログインできない

この情報を使用して、管理対象 CMM に直接ログインするときの問題をトラブルシューティングしてください。

1. パスワードが正しいこと、Caps Lock キーと Num Lock キーがオンになっていないことを確認します。
2. 資格情報が Lenovo XClarity Administrator に保存された資格情報と一致することを確認します。CMM が XClarity Administrator の管理対象である場合、ローカル CMM アカウントを使用してログインすることはできません。XClarity Administrator での非集中型ユーザー管理について詳しくは、XClarity Administrator オンライン・ドキュメントの認証サーバーの管理を参照してください。

管理コントローラーに直接ログインできない

この情報を使用して、管理コントローラーに直接ログインしたときの問題をトラブルシューティングしてください。

1. パスワードが正しいこと、Caps Lock キーと Num Lock キーがオンになっていないことを確認します。
2. 資格情報が Lenovo XClarity Administrator に保存された資格情報と一致することを確認します。
3. 管理コントローラーのバージョンが XClarity Administrator と互換性があることを確認します。
4. 管理コントローラーを管理している XClarity Administrator サーバーが 1 つだけであることを確認します。

管理対象 Flex Power System サーバーにログインできない

この情報を使用して、管理対象 Flex Power System サーバーに直接ログインするときの問題をトラブルシューティングしてください - Lenovo XClarity Administrator

Flex System サーバーと Flex Power System サーバーの両方が搭載された管理対象シャーシがある場合、認証の問題のため Flex Power System サーバーに直接ログインできないことがあります。

シャーシが XClarity Administrator により管理されている場合、CMM のユーザーは一元管理されます。つまり、内部または外部認証サーバーで定義されているユーザー・アカウントが Chassis Management Module (CMM) へのログインにも使用され、ローカル CMM ユーザー・アカウントは無効になります。

管理対象 Flex Power System サーバーの管理コントローラー Web インターフェースにログインするには、シャーシが XClarity Administrator により管理されていたときに作成された RECOVERY_ID アカウントを使

用します。このアカウントを使用して CMM にログインし、パスワードを変更します (パスワードは、最初のアクセス時に変更する必要があります)。パスワードが変更されたら、RECOVERY_ID アカウントを使用して Power System ノードの管理コントローラー Web インターフェースにログインすることができます。

HMC (ハードウェア管理コンソール) から Flex Power System ノードを管理する場合、以下の手順を実行します。

1. SSH を使用して管理 CLI インターフェースにログインします。
2. 以下のコマンドを実行して、CMM でのユーザー認証方式を「**最初にローカル認証ー、次に外部認証**」に構成し、USERID アカウントを削除して再作成します。
```
env -T mm[p]
accseccfg -am localldap
users -n USERID -clear
users -add -n USERID -p <password> -g Supervisor -ms 0
```

デバイスへの接続が突然失われる

この情報を使用して、単一のデバイスに接続するときの問題をトラブルシューティングしてください。

1. 保存された資格情報を使用するデバイスがオフラインになっている場合、保存された資格情報が、有効期限切れまたは無効になっていないことを確認します。有効期限切れまたは無効の場合は、以下の手順を実行します。
   a. 「すべてのデバイス」ページで、解決するデバイスを選択します。
   b. 「**すべての操作**」 → 「**セキュリティー**」 → 「**保存された資格情報の解決**」をクリックします。
   c. 保存された資格情報のパスワードを変更するか、管理対象デバイスで使用する別の保存された資格情報を選択します。
2. イベント・ログでそのデバイスのネットワーク・イベントがないか調べて、先にそれらを解決します。イベント・ログについて詳しくは、Lenovo XClarity Administrator オンライン・ドキュメントのイベントの使用を参照してください。
3. ネットワーク・ハードウェアが、デバイスへの接続パスで正しく動作していることを確認します。
4. デバイスでスイッチとファイアウォールの正しいポートが有効になっていることを確認します。必要なポートについて詳しくは、XClarity Administrator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。
5. デバイスにログインし、ネットワークの IP アドレスが有効であることを確認して、デバイスに有効なネットワーク構成があることを確認します。デバイスに ping 送信して、ネットワーク上で見えるかどうかをテストします。
6. デバイスへの直接ログインを試みます。

第 8 章　Lenovo XClarity Administrator 構成の問題

この情報を使用して、Lenovo XClarity Administrator 構成に関する問題をトラブルシューティングしてください。

外部 LDAP のセットアップの問題

この情報を使用して、外部認証サーバーをセットアップするときの問題をトラブルシューティングしてください。

1. ルート識別名が正しいことを確認します。
2. Lenovo XClarity Administrator ユーザー・アカウントが少なくとも 1 つの役割グループのメンバーになっていることを確認します。役割グループについては、XClarity Administrator オンライン・ドキュメントの役割グループの作成を参照してください。
3. XClarity Administrator 役割グループが、LDAP サーバーの少なくとも 1 つの役割グループと一致していることを確認します。
4. 事前に構成されたサーバー・アドレスを使用している場合、サーバーの IP アドレスとポート番号が正しいことを確認します。
5. DNS 構成設定が正しいことを確認します。
6. DNS を使用してサーバーを検出する場合、ドメイン名とフォレスト名が正しいことを確認します。
7. クライアント識別名とパスワードが正しいことを確認します。

外部認証サーバーのセットアップについては、XClarity Administrator オンライン・ドキュメントの外部認証サーバーのセットアップを参照してください。

ユーザーにサーバーを構成するための十分な許可がない

この情報を使用して、管理対象サーバーを構成するときの問題をトラブルシューティングしてください。

1. スーパーバイザーまたは管理者の役割グループに属するユーザー・アカウントにログインしていることを確認します。ユーザー役割については、Lenovo XClarity Administrator オンライン・ドキュメントの役割グループの作成を参照してください。
2. システム管理者に問い合わせて権限を更新してもらいます。

Features on Demand アクティベーションの問題

この情報を使用して、機能をアクティブ化するときの問題をトラブルシューティングしてください。

必ず Features on Demand (FoD) キーの適用に使用するツールの手順に従ってください。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Feature on Demand キーの表示を参照してください。

VMware による警告、VMXNET 3 ドライバーはサポートされていません

Lenovo XClarity Administrator のインストール時、XClarity Administrator アプライアンス仮想マシン設定の編集時、XClarity Administrator の vmotion の実行時、または VMware に関連付けられた管理または監視インフラストラクチャ内で、VMXNET 3 ドライバーがサポートされていないという警告が表示されることがあります。

© Copyright Lenovo 2015, 2025

XClarity Administrator アプライアンスには VMXNET 3 ドライバーが含まれています。ドライバーがサポートされていないという VMware エラーは安全に無視することができます。

第 9 章　パフォーマンスの問題

この情報を使用して、パフォーマンスに関する問題をトラブルシューティングしてください。

Lenovo XClarity Administrator パフォーマンスの問題

この情報を使用して、Lenovo XClarity Administrator のパフォーマンスに関する問題をトラブルシューティングしてください。

使用している環境に多数のデバイスと多数の並行ユーザー・セッションが存在し、システム・パフォーマンスの低下が発生している場合は、XClarity Administrator Web インターフェースに対する並行ユーザー・セッションの数を減らすか、仮想アプライアンスに割り当てられている仮想 CPU リソースを増やします。

仮想マシン (メモリ、ディスク・サイズ、プロセッサー) に利用可能なリソースが、管理対象となっているデバイスの数に適していることを確認します。仮想マシンの要件について詳しくは、XClarity Administrator オンライン・ドキュメントのサポートされているホスト・システムを参照してください。

その他のパフォーマンスに関する考慮事項およびヒントについては、XClarity Administrator: パフォーマンス・ガイド (ホワイト ペーパー) を参照してください。

ネットワーク・パフォーマンスに関する問題

この情報を使用して、ネットワーク・パフォーマンスの低下に関する問題をトラブルシューティングしてください。

1. システムの検出、オペレーティング・システム・デプロイメント、ファームウェア更新のロールアウト/ロールバックなど、大規模なネットワーク操作が実行中でないことを確認します。
2. 残りのネットワークが通常の使用率で動作していることを確認します。
3. サービス品質を実装している場合、Lenovo XClarity Administrator への最適な接続が許容されるように構成されていることを確認します。
4. ネットワーク・トポロジーが XClarity Administrator の接続とパフォーマンスに合わせて最適化されていることを確認します。

© Copyright Lenovo 2015, 2025

第 10 章　セキュリティーの問題

この情報を使用して、ユーザー管理および認証を含むセキュリティーの問題をトラブルシューティングしてください。

SSL 証明書を信頼できない

証明書チェーンに、自己署名や既知の証明機関からではない署名が含まれている場合があります。

ポート 443、3888、9090、50636、50637
各 Lenovo XClarity Administrator インスタンスには固有の内部生成された証明機関 (CA) があります。デフォルトでは、これらのポート (ユーザーと仮想アプライアンス間または管理対象デバイスと仮想アプライアンス間の通信に使用) は、その CA によって署名された証明書を使用します。SSL 証明書が信頼できない場合、XClarity Administrator にカスタマイズされた外部署名済みサーバー証明書を生成してデプロイします。詳しくは、XClarity Administrator オンライン・ドキュメントの XClarity Administrator へのカスタマイズされたサーバー 証明書のデプロイを参照してください。

ポート 8443
各 XClarity Administrator インスタンスには、OS デプロイメントでのみ使用される固有証明機関 (CA) があります。その CA がポート 8443 のターゲット・サーバーに使用する証明書に署名します。OS デプロイメントが開始されると、CA 証明書は、ターゲット・サーバーにプッシュされた OS イメージに含まれます。デプロイメント・プロセスの一部として、サーバーは、ポート 8443 に接続しなおされ、CA 証明書があるため、ハンドシェイク中にポート 8443 が提供した証明書が検証されます。

サーバー証明書の検証に失敗する

Lenovo XClarity Administrator にサーバー証明書をインストールしようとして、証明書の検証に失敗した場合は、この情報を使用します。

このタスクについて

XClarity Administrator が次の操作を行おうとすると、サーバー証明書の検証が失敗することがあります。

- HTTPS 経由で CIM-XML を使用して管理対象デバイスに接続する。
- セキュア LDAP を使用して外部認証サーバーに接続する (セキュア LDAP 接続を構成した場合)。
- セキュア接続を使用して外部 SAML ID プロバイダーに接続する (SAML を構成した場合)。
- OS イメージをインポートするためのリモート・ファイル・サーバーに接続する (HTTPS イメージ・サーバーを構成した場合)。
- Lenovo に接続して保証状況情報を取得する。
- Apple および Google のプッシュ通知サーバーに接続する (iOS または Android デバイスに対する Lenovo XClarity Mobile プッシュ通知が有効になっている場合)。

手順

この問題を解決するには、以下の手順を実行します。

- 証明書またはその署名証明書が、XClarity Administrator 内のトラステッド証明書信頼ストアまたは外部サービス証明書信頼ストアに存在することを確認します。トラステッド証明書と外部サービス証明書について詳しくは、XClarity Administrator オンライン・ドキュメントの セキュリティー証明書の使用を参照してください。
- 証明書が取り消されていないことを確認します (XClarity Administrator オンライン・ドキュメントの 証明書取り消しリストの追加と置き換え を参照)。

© Copyright Lenovo 2015, 2025

- サーバーの IP アドレスまたはホスト名が、サブジェクト代替名または証明書内の共通名 (SAN が存在しない場合) のいずれかと一致していることを確認します。
- 今日の日付が証明書の「有効期間の開始日」と「有効期間の終了日」の間に収まっていることを確認します。
- 証明書が、サポートされているアルゴリズム (レガシー・モードの場合は SHA1 以上、NIST Strict モードの場合は SHA256 以上) を使用して署名されていることを確認します (XClarity Administrator オンライン・ドキュメントの 暗号モードと通信プロトコルの設定 を参照)。

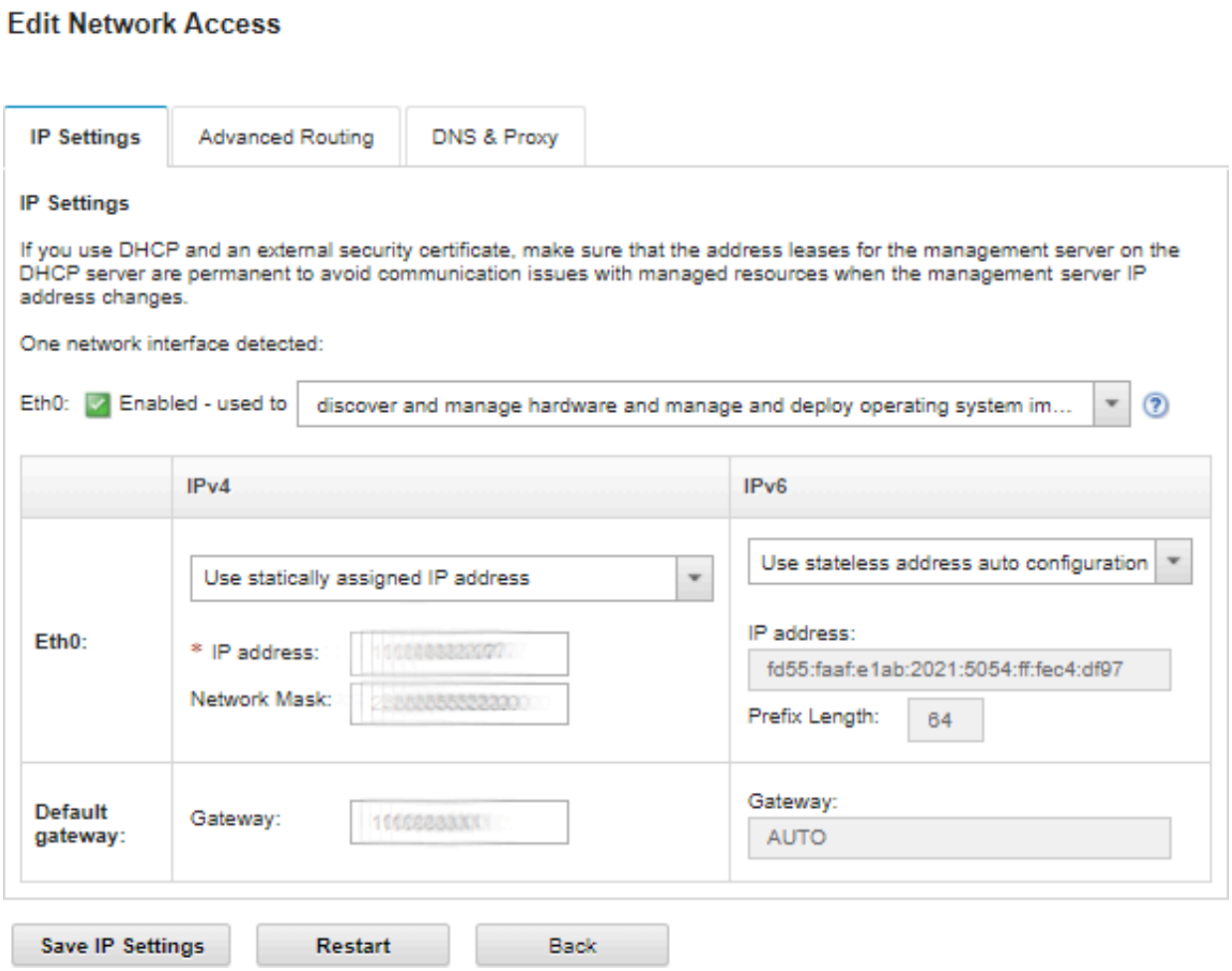
Samba および Apache の脆弱性

Lenovo XClarity Administrator はオペレーティング・システムのデプロイ時および OS デバイス・ドライバーの更新時に、Samba および Apache サーバーを読み取り専用リモート共有として使用します。XClarity Administrator を使用してオペレーティング・システムを管理しない場合は、XClarity Administrator ネットワーク役割をハードウェアの検索と管理のみに設定することで、Samba および Apache サーバーを無効化できます。

手順

Samba および Apache サーバーを無効にするは、以下の手順を実行します。

1. XClarity Administrator のメニュー・バーで、「**管理**」 ➡ 「**ネットワーク・アクセス**」をクリックします。現在定義されているネットワーク設定が表示されます。
2. 「**ネットワーク・アクセスの編集**」をクリックして「ネットワーク・アクセスの編集」ページを表示します。



3. ネットワーク・インターフェースに「**ハードウェアの検索と管理のみ**」オプションを選択します。
4. 「**IP 設定の保存**」をクリックします。
5. 「**再起動**」をクリックして管理サーバーを再起動します。

第 11 章 バックアップと復元の問題に関するトラブルシューティング

この情報を参考にして、バックアップおよび復元に関する問題をトラブルシューティングしてください。

バックアップ・プロセスが管理サーバーの再起動中にハングしているように見える

Lenovo XClarity Administrator バックアップの生成には時間がかかる場合があります。進行状況バーによってジョブの状況が示されます。

手順

バックアップ・プロセスがハングしたように見える場合は、以下の手順を実行します。

- 「**キャンセル**」ボタンが表示される場合は、バックアップ・プロセスをキャンセルできます。
- 「**キャンセル**」ボタンが表示されない場合は、新しいタブを開き、「**キャンセル**」ボタンが表示されるかどうかを確認します。
- これによって問題が解決しない場合は、仮想マシンをリブートします。

注：バックアップ・プロセスをキャンセルするか、または仮想マシンをリブートした場合、バックアップが作成されないことがあります。

XClarity Administrator ウィンドウは、バックアップ時に更新後に空白になります。

データの変更を防ぐため、この手順の間、Lenovo XClarity Administrator は休止します。バックアップ・プロセスが完了し、管理サーバーが再起動する前に、XClarity Administrator ウィンドウを更新するか閉じた場合、管理サーバーが依然として休止モードであるときは、XClarity Administratorウィンドウが空白で表示される可能性があります。

手順

この問題を解決するには、以下の手順を実行します。

1. ロードされたかどうかを確認するために、定期的にページを更新してください。
2. 相当な時間が経過してもウィンドウが空白なままの場合は、仮想マシンを再起動します。
3. 依然としてロードされない場合は、 `/opt/lenovo/lxca/bin/QUIESCE_MODE_FLAG` ファイルを手動で削除します。

   注：この手順では、ルート・アクセスが必要です。この手順を実行する前に、サポートに連絡してください。
4. XClarity Administrator仮想マシンを起動します。

© Copyright Lenovo 2015, 2025

第 12 章 イベントの監視および転送の問題

この情報を使用して、イベントの監視および転送の問題をトラブルシューティングしてください。

イベントが転送されない

この情報を使用して、イベントを転送するときの問題をトラブルシューティングしてください。

- スケジュールがイベント・フォワーダー用に作成された場合、スケジュールされた時刻スロット中に発生したイベントのみが転送されます。スケジュールした時刻が経過していないことを確認してください。
- メール・ベースの Web サービスの場合:
  - イベント・フォワーダーにセキュアな接続タイプが選択されている場合、Lenovo XClarity Administrator によって信頼ストアに SMTP サーバー証明書がダウンロードされインポートされます。この証明書を信頼ストアに追加することを承諾するように要求されます。これに失敗すると、SMTP サーバーに接続できません。

    この問題を解決するには、証明書を手動で XClarity Administrator 信頼ストアにインポートします。「**管理**」 ➡ 「**セキュリティー**」 ➡ 「**トラステッド証明書**」、「**作成**」アイコン ( ) の順にクリックします。
  - 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かどうか確認します。この場合、デフォルトの送信者アドレス (LXCA.*<source_identifier>*@*<smtp_host>*) は拒否されます。この問題を解決するには、イベント・フォワーダーの「**送信元アドレス**」フィールドに少なくとも 1 つのドメイン名を指定します。
  - OAUTH2 認証を使用している場合は、セキュリティー・トークンの期限が切れていないことを確認します。有効期限切れの場合は、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・トークンを生成します。その後、新しいセキュリティー・トークンを使用して XClarity Administrator のイベント・フォワーダーを更新します。詳しくは、Gmail SMTP サービスへのイベント転送のセットアップを参照してください。

© Copyright Lenovo 2015, 2025

第 13 章　デバイス管理に関する問題

この情報を使用して、デバイスの管理および操作に関する問題をトラブルシューティングしてください。

フリーズしたドライブのドライブ・データを安全に消去できない

この情報を使用して、SATA ハードディスク・ドライブで**ディスクがフリーズしていて消去できない**というエラーが発生したため、安全な消去が失敗した場合の問題をトラブルシューティングしてください。

オンボード SATA ハードディスク・ドライブは、デフォルトではフリーズ状態です。サーバーにフリーズしているドライブがある場合、Lenovo XClarity Administrator はフリーズしているドライブを一時的に解除し、ベア・メタル更新 (BMU) で起動してドライブを消去します。XClarity Administrator BMU が終了してサーバーがオペレーティング・システムを起動すると、ドライブは自動的に再びフリーズします。

XClarity Administrator で*管理対象認証*モードを使用してサーバーが管理されている場合、XClarity Administrator ではローカル資格情報ではなく、サーバーを管理および監視するための SYSMGR_xxx LDAP アカウントを作成します (XClarity Administrator オンライン・ドキュメントの認証サーバーの管理を参照)。その SYSMGR_xxx LDAP アカウントには IPMI 特権が付与されていないため、XClarity Administrator はディスクのフリーズを解除できず、そのサーバーでの安全な消去の操作が失敗します。

この問題を解決するには、*ローカル認証*モードを使用してサーバーを管理し、ドライブの安全な消去を試行します。

SATA SDD ボリュームが Marvel RAID に接続されている場合、安全に消去できない

この情報を使用して、ボリュームのある SATA SDD が、Marvell RAID コントローラーに接続されている場合に安全な消去に失敗する問題をトラブルシューティングしてください。

Marvell RAID コントローラーに接続されている SATA SDD ボリュームを安全に消去することはできません。代わりに、以下の推奨事項について検討してください。

- 7mm SATA SSD の場合、Broadcom RAID コントローラーに接続して安全な消去を実行します。
- M.2 SATA SSD の場合、Marvell の非 RAID コントローラー (ThinkSystem M.2 SATA/NVMe 2 ベイ・イネーブルメント・キットなど) に接続して安全な消去を実行します。

Marvell RAID ファームウェアには、内部タイムアウト (9 秒) があります。SSD がコマンドに対して時間内に応答しない (消去が完了しない) 場合、Marvell RAID ファームウェアは SDD をリセットし、SDD はロックされ、安全な消去が失敗します。SDD のロックを解除するには、次のコマンドを実行します。

```
hdparm -user-master u -security-unlock user123 %diskName%
```

カードの追加または交換後にインベントリー・データが最新でない

AMD1P および TSM ベースのデバイスの場合、新しく挿入した PCIe カードの正しいインベントリー・データ (FRU およびファームウェアなど) が Lenovo XClarity Administrator で表示されない場合があります。

PCIe カードを変更した後、管理対象デバイスを再起動し、ベースボード管理コントローラーがインベントリーを更新するまで数分間待つ必要があります。

XClarity Administrator は、24 時間ごとに管理対象デバイスからインベントリー・データを自動的に取得します。次回のインベントリー収集を待つか、「サーバー」ページでサーバーを選択し、**操作 → イ**

© Copyright Lenovo 2015, 2025

ンベントリー → インベントリーを最新の情報に更新の順にクリックしてインベントリー・データを手動で収集できます。

第 14 章　サーバー構成の問題

この情報を使用して、サーバー・パターンとプロファイルに関する問題をトラブルシューティングしてください。

既存のサーバーからパターンを作成するときにエラーが発生する

この情報を使用して、既存の管理対象サーバーからのサーバー・パターンの作成に関する問題をトラブルシューティングしてください。

1. サーバーのステータスが「オフライン」でないことを確認します。サーバー・パターンについて詳しくは、Lenovo XClarity Administrator オンライン・ドキュメントのサーバー・パターンの作成を参照してください。
2. 操作を再試行します。

パターンをデバイスにデプロイするときに、アクティベーション・エラーが発生する

アクティベーション・エラーは、サーバー・パターンを管理対象デバイスにデプロイするときに問題が発生したことを示します。アクティベーション・エラーは、さまざまな理由で発生します。この情報を使用して、このタイプの問題をトラブルシューティングしてください。

「ジョブ」ページでジョブの詳細を確認します。ステータスが「停止 (エラーあり)」になっているサーバー・プロファイル・アクティベーション・ジョブを見つけ、クリックします。問題を識別するには、エラー・メッセージを確認します。

- Lenovo XClarity Administrator と管理対象デバイス間の接続またはネットワーク・ルーティングの問題

  これらの問題が、ジョブ・メッセージで LDAP エラーとして表示される場合があります。これは、構成されたネットワーク・インターフェースの 1 つを経由して仮想アプライアンスに接続するデバイスに関連した問題があることを示します。

  XClarity Administrator 仮想アプライアンスとデバイス間のネットワーク接続が動作していることを確認します。異なるネットワーク・セグメントにある場合は、2 つのセグメント間がネットワークで接続可能であることを確認してください。
- サーバー・パターンの構成設定によって、選択した管理対象デバイスで有効ではない設定に変更される場合があります。次の例を考慮してください。
  - 選択した UEFI 拡張パターンが選択したデバイスと互換性がない。

    たとえば、X6 ベースの XClarity Administrator サーバー (System x3950 X6 など) で提供された UEFI パターンが選択され、System x3650 M4 サーバーにデプロイされた場合、2 つのサーバーのプロセッサー設定の違いによりプロファイルのアクティベーションに失敗することがあります。この問題を解決するには、選択された拡張 UEFI パターンが選択されたサーバーと互換性があることを確認してください。
  - イーサネット・アダプター・ポートのポート・パターンが、選択した設定をサポートしていないポートに割り当てられている。

    たとえば、Emulex ベースのアダプターには、特に詳細モードやポートを無効にするために使用されるポート設定で、アダプターの最初のポートのみに開示される設定があります。これらの設定がアダプターの 2 番目のポートに割り当てられている場合、アクティベーション・エラーが発生する可能性があります。これらの問題はジョブ・メッセージとして「**詳細モード設定ではありません**」または「**ポート 1 設定ではありません**」と表示される可能性があります。この問題を解決するには、このような詳細モードの拡張ポート・パターン設定またはポートの有効化を含むポート・パターンが、アダプターの最初のポートにのみ割り当てられていることを確認します。

© Copyright Lenovo 2015, 2025

– ファームウェア更新後、選択した管理対象デバイスで、いくつかの設定がサポートされない。

  たとえば、I/O アダプターのファームウェアを更新した後、新しいファームウェアによっていくつかの設定が削除されるか、名前が変更され、したがってサーバー・パターンの設定がターゲット・サーバーでは無効化されることがあります。この問題は、ジョブ・メッセージ「xxx 設定ではありません」として通知されることがあります。この問題を解決するために、新しいパターンに新しいファームウェアでサポートされているすべての設定が含まれるように、サーバーから新しいサーバー・パターンを学習できます。古いパターンを引き続き使用する必要がある場合は、サーバー・パターンを手動で編集して無効な設定を削除します。

- パターンまたはプロファイルのデプロイメントで完全なアクティブ化を選択すると、電源投入時またはサーバーの再起動時にエラーが発生する

  デバイスの電源状態が XClarity Administrator で正しく示されていることを確認します。正しくない場合は、インベントリーを最新表示にして電源状態を同期させます。

  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**サーバー**」の順にクリックします。「サーバー」ページが開いて、すべての管理対象サーバー (ラック・サーバーと計算ノード) がテーブル・ビューで表示されます。
  2. サーバーを選択し、「**すべての操作**」 → 「**インベントリーを最新の情報に更新**」の順にクリックします。

無効な構成がスイッチにデプロイされる

無効な構成がスイッチにデプロイされる場合は、この情報を使用して問題をトラブルシューティングしてください。

特定の VLAN にポートを追加する前に、VLAN ID を作成する必要があります。スイッチに事前構成されていない VLAN ID が設定されたスイッチ内部ポート VLAN 設定がポート・パターンに含まれている場合、プロファイルのアクティブ化には成功する可能性がありますが、スイッチ上の未適用の無効な構成を修復する必要があります。

この問題を解決するには、スイッチにログインして前提条件を手動で構成するか、有効な設定を含むパターンをデプロイすることによって変更を取り消します。

第 15 章　ファームウェア更新とリポジトリーの問題

この情報を使用して、ファームウェア更新に関する問題をトラブルシューティングしてください。

Lenovo リポジトリーに接続できませんでした

Lenovo XClarity Administrator バージョン2.8 以前では、Lenovo サポートに HTTP 接続を使用して、ファームウェア更新カタログを更新し、更新パッケージをダウンロードすることができます。ただし、Lenovo サポートには HTTPS 接続が必要になりました。

最新の GAFix をご使用の XClarity Administrator インスタンスにインストールするか、XClarity Administrator バージョン 3.0.0 以降にアップグレードしてください。

ファームウェア更新は成功したが、「適用/アクティブ化」ページに更新後のファームウェア・バージョンが表示されない

この情報を使用して、「ファームウェア更新: 適用/アクティブ化」ページのユーザー・インターフェースに関する問題をトラブルシューティングしてください。

「ファームウェア更新: 適用/アクティブ化」ページの「**最新表示**」アイコン ( ) をクリックして Lenovo XClarity Administrator アプライアンス・データとの同期を要求し、最新のインベントリーが比較されていることを確認してください。

デバイスのファームウェアを更新できません

この情報を使用して、管理対象デバイスでファームウェアを更新するときの問題をトラブルシューティングしてください。

- XClarity Administratorオンライン・ドキュメントのファームウェアの更新に関する考慮事項の推奨事項に従ってください。
- サーバー・ステータスが「オフライン」ではなく、Lenovo XClarity Administrator 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。
- ファームウェアの更新に問題が発生した場合、FOS v7.4.x 以前を実行する FC5022 スイッチで、コマンド・ライン・インターフェースから次のコマンドを実行します。詳しくは、技術ヒント HT507915を参照してください。
  ```
  Seccrypto -- default -type SSH -force
  ```

CMM ファームウェア更新がハングアップする

この情報を使用して、3 週間以上実行中であり、デュアル CMM 構成の一部である CMM ファームウェア、Flex スタック・リリース 1.3.2.1 2PET12K から 2PET12Q の更新に関する問題をトラブルシューティングしてください。

1. CMM の仮想再取り付けを行います。2 つの CMM が同じシャーシ内にある場合は、両方の CMM の仮想再取付けを同時に行います。XClarity Administrator のサポート – 互換性に 関する Web ページから最小限必要なレベルのファームウェアを見つけるには、 **互換性**タブをクリックし、該当するデバイス・タイプのリンクをクリックします。
2. XClarity Administrator から更新を再実行してください。

© Copyright Lenovo 2015, 2025

ファームウェアは最新だが、コンプライアンス・チェックが失敗する

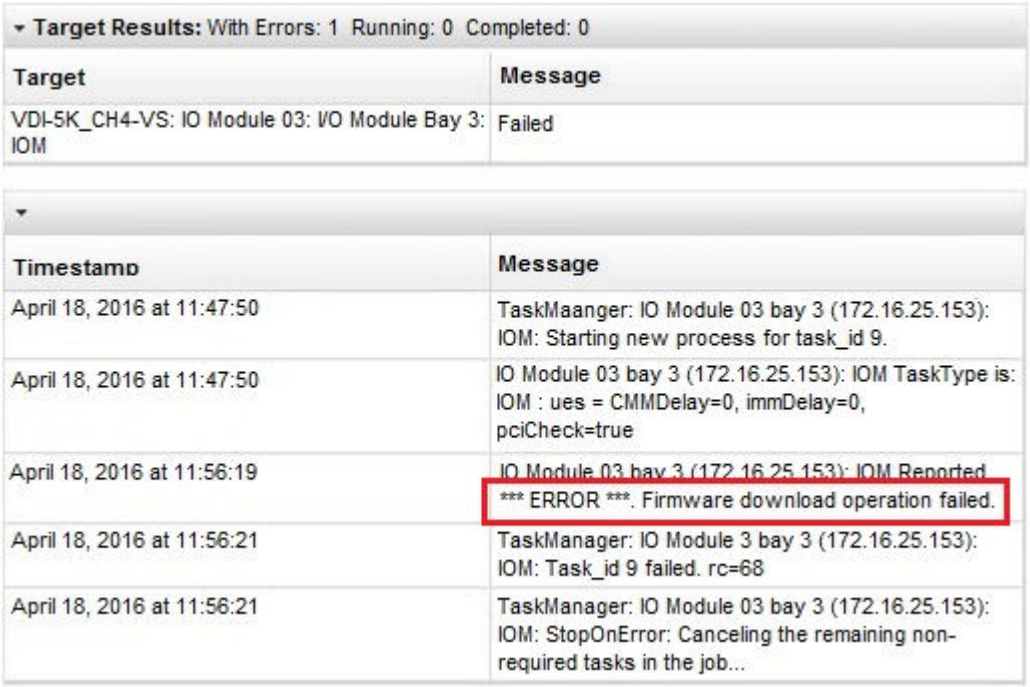
この情報を使用して、ファームウェア更新後のコンプライアンスに関する問題をトラブルシューティングしてください。

デバイスで仮想再取付けを実行するか、HDD 更新などの追加更新を実行します。

Flex System スイッチに対するファームウェア更新が予期せず失敗する

以下のトピックでは、ジョブ・ログに記録されるエラーについて説明します。

メッセージを検索するには、Lenovo XClarity Administrator メニューから「**監視**」 → 「**ジョブ**」をクリックします。エラー・メッセージは、「**ジョブ**」列のジョブのリンクをクリックしてジョブの要約と結果ダイアログを表示すると確認できます。ターゲット結果セクションの下の「**メッセージ**」列に、「***エラー***」で始まるメッセージがリストされています。



Target Results: With Errors: 1 Running: 0 Completed: 0

Target	Message
VDI-5K_CH4-VS: IO Module 03: I/O Module Bay 3: IOM	Failed

Timestamp	Message
April 18, 2016 at 11:47:50	TaskMaanger: IO Module 03 bay 3 (172.16.25.153): IOM: Starting new process for task_id 9.
April 18, 2016 at 11:47:50	IO Module 03 bay 3 (172.16.25.153): IOM TaskType is: IOM : ues = CMMDelay=0, immDelay=0, pciCheck=true
April 18, 2016 at 11:56:19	IO Module 03 bay 3 (172.16.25.153): IOM Reported *** ERROR ***. Firmware download operation failed.
April 18, 2016 at 11:56:21	TaskManager: IO Module 3 bay 3 (172.16.25.153): IOM: Task_id 9 failed. rc=68
April 18, 2016 at 11:56:21	TaskManager: IO Module 03 bay 3 (172.16.25.153): IOM: StopOnError: Canceling the remaining non-required tasks in the job...

重要：XClarity Administrator を使用した Flex スイッチのファームウェア更新が、断続的に失敗する場合があります。障害が発生した場合は、以下のトピックの提案に従ってください。XClarity Administrator を使用した Flex スイッチのファームウェア更新が失敗し続ける場合は、Flex スイッチ・インターフェースから直接 Flex スイッチを更新します。

注：スイッチで EHCM L3 が実行されていない場合、Flex System スイッチに対するファームウェア更新が予期せず失敗する可能性があります。詳しくは、 XClarity Administratorオンライン・ドキュメントのファームウェアの更新に関する考慮事項を参照してください。

Flex スイッチに対するファームウェア更新が失敗し、「ファームウェアのダウンロード操作に失敗しました」というエラー・メッセージが表示されました。

この情報を使用して、ジョブ・ログの「**IOM: 報告 ***エラー*** ファームウェアのダウンロード操作に失敗しました**」エラー・メッセージをトラブルシューティングしてください。これは、以前のファームウェ

ア更新バージョンをスキップして最新バージョンにジャンプする必要がある、中断を伴う更新を実行しようとした場合に、EN4023 および FC5022 スイッチで発生する可能性があります。

この問題を回避するには、Flex スイッチ CLI または Web インターフェースから Flex スイッチを直接更新します。

FC5022 の場合、FOS v7.3 から v8.0.1-pha への移行は中断を伴う更新です。FOS v7.4 から FOS v8.0.1-pha への移行は中断を伴わない更新です。

XClarity Administrator のサポート – 互換性に 関する Web ページから最小限必要なレベルのファームウェアを見つけるには、 **互換性**タブをクリックし、該当するデバイス・タイプのリンクをクリックします。

Flex スイッチに対するファームウェア更新が失敗し、「DCSS_RC_CDT_FAIL」を示すエラー・メッセージが表示される

この情報を使用して、ジョブ・ログの「IOM: 報告 ***エラー*** DCSS_RC_CDT_FAIL」エラー・メッセージをトラブルシューティングしてください。このメッセージは、Flex スイッチの電源がオフになっているか、何らかの通信上の問題が発生している可能性があることを示します。

以下の操作を以下の順序で実行します。各手順の実行後に、ファームウェアの更新を再試行してください。

1. Flex スイッチの電源がオンになっていることを確認します。
2. Flex スイッチの IP アドレスが有効であることを確認します。
3. Flex スイッチをリセットします。
4. CMM をリセット/リブートします。

Flex スイッチに対するファームウェア更新が失敗し、「タイムアウト」を示すエラー・メッセージが表示される。

この情報を使用して、ジョブ・ログの「IOM: 報告 ***エラー*** タイムアウト」エラー・メッセージをトラブルシューティングしてください。この問題は、スイッチの IP アドレスが Lenovo XClarity Administrator からネットワーク経由で到達可能でない場合に発生することがあります。

以下の操作を以下の順序で実行します。各手順の実行後に、ファームウェアの更新を再試行してください。

1. Flex スイッチの IP アドレスが有効であり、ネットワーク上で XClarity Administrator から到達可能であることを確認します。
2. Flex スイッチをリセットします。
3. CMM をリセット/リブートします。

Flex スイッチに対するファームウェア更新が失敗し、「同じファームウェア・バージョンをダウンロードすることはできません。別のファームウェアをダウンロードしてください」というエラー・メッセージが表示される。」

この情報を使用して、「IOM: 報告 ***エラー*** 同じファームウェア・バージョンをダウンロードすることはできません。別のファームウェアをダウンロードしてください」というジョブ・ログ内のエラー・メッセージをトラブルシューティングします。これは、EN4023 を同一レベルに更新しようとした場合に発生することがあります。

EN4023 では、既に実行されているレベルと同じレベルにファームウェアを更新することは許可されません。

Flex スイッチに対するファームウェア更新が失敗し、ホストへのアクセスが失敗したことを示すエラー・メッセージが表示される

この情報を使用して、ジョブ・ログの「IOM: 報告 ***エラー*** ホストへのアクセス失敗」エラー・メッセージをトラブルシューティングしてください。この問題は、スイッチの IP アドレスが Lenovo XClarity Administrator からネットワーク経由で到達可能でない場合に発生することがあります。

以下の操作を以下の順序で実行します。各手順の実行後に、ファームウェアの更新を再試行してください。

1. スイッチの IP アドレスが有効であり、ネットワーク上で XClarity Administrator から到達可能であることを確認します。
2. スイッチを再起動します。
3. CMM を再起動します。

Flex スイッチに対するファームウェア更新が失敗し、「ファイルが存在しない」というエラー・メッセージが表示される

この情報を使用して、ジョブ・ログの「IOM: 報告 ***エラー*** ファイルが存在しない」エラー・メッセージをトラブルシューティングしてください。この問題は、スイッチの IP アドレスが Lenovo XClarity Administrator からネットワーク経由で到達可能でない場合に発生することがあります。

以下の操作を以下の順序で実行します。各手順の実行後に、ファームウェアの更新を再試行してください。

1. スイッチの IP アドレスが有効であり、ネットワーク上で XClarity Administrator から到達可能であることを確認します。
2. スイッチをリセットします。
3. CMM をリセット/リブートします。

Flex スイッチに対するファームウェア更新が失敗し、「フラッシュがエラーで終了」というエラー・メッセージが表示される

この情報を使用して、ジョブ・ログの「IOM: 報告 ***エラー*** フラッシュがエラーで終了」エラー・メッセージをトラブルシューティングしてください。これは、スイッチの IP アドレスが有効でない場合に起こることがあります。

スイッチの IP アドレスが有効であり、ネットワーク上で Lenovo XClarity Administrator から到達可能であることを確認します。

EN6131 40 Gb イーサネット・スイッチまたは IB6131 InfiniBand スイッチに対するファームウェア更新が予期せず失敗する

この情報を使用して、EN6131 40 Gb Ethernet Switch または IB6131 InfiniBand Switch に対するファームウェア更新時の予期しない失敗に関する問題をトラブルシューティングしてください。

1. ジョブ・ログでスイッチからのエラー・メッセージを確認します (「**イメージのダウンロードに使用できる十分なディスク・スペースがありません**」など)。

   注：ジョブ・ログに追加情報が含まれていることがあります。多くの場合、この情報は「IOM: **エラー報告** ***ERROR*** *msg*」の書式で表示され、*msg* はモジュール固有のエラーです。
2. ご使用のネットワークの速度および安定性を確認します。30 分以内に更新が完了しなかった場合、ファームウェア更新が失敗することがあります。
3. スイッチ上で更新ファイル用の十分なディスク・スペースを解放します。ディスク・スペースは、更新ファイルをスイッチにコピーするときに使用されます。ディスク・スペースを管理する手順については、Flex Systems オンライン・ドキュメントの Lenovo Flex System EN6131 40Gb イーサネット・スイッチを参照してください。

4. Lenovo XClarity Administrator から更新を再実行してください。

Lenovo EN4091 パススルー・モジュールに対するファームウェア更新が失敗する

この情報を使用して、Lenovo EN4091 パススルー・モジュールに対するファームウェア更新時の予期しない失敗に関する問題をトラブルシューティングしてください。

1. ジョブ・ログで、パススルー・モジュールからのエラー・メッセージを確認します (「**ファームウェア・イメージのデータ保全性検査の失敗**」エラーや、「**ホストへのアクセス失敗**」など)。

   注：ジョブ・ログに追加情報が含まれていることがあります。多くの場合、メッセージは「**IOM: エラー報告** ***ERROR*** *msg*」の書式で表示され、*msg* はモジュール固有のエラーです。
2. Lenovo EN4091 の仮想再取り付けを行います。
3. Lenovo XClarity Administrator から更新を再実行してください。

Flex System スイッチに対するファームウェア更新が失敗し、「ホスト鍵認証に失敗」したことを示すエラー・メッセージが表示される。

ジョブ・ログのエラー・メッセージに、「IOM: 報告 ***エラー*** ホスト鍵認証に失敗」という書式のエラー・メッセージが表示されます。これは、先に Flex System スイッチの更新で使用した SFTP サーバーで SFTP キーが変更されている場合に発生します。影響を受けるスイッチは、CN4093、EN2092、EN4091、EN4093、EN4093R、SI4093 です。

Lenovo XClarity Administrator では、このエラーは Flex System スイッチで既にファームウェアを更新しているため、最新バージョンの XClarity Administrator を別にインストールしたり、XClarity Administrator を再起動した後スイッチを更新しようとした場合に発生する可能性があります。これは、XClarity Administrator の新規バージョンのインストール、または XClarity Administrator のリブートにより、新しい SFTP 鍵が生成される場合があるためです。

この問題を解決するには、Flex System スイッチまたは Lenovo Flex System スイッチの CLI から、次のコマンドを入力して SSH 鍵をクリアします。スイッチで ISCLI が使用されている場合、このコマンドを実行するには Configuration Terminal モードにする必要があります。`enable` コマンドを実行して `configure terminal` コマンドを実行することにより、Configuration Terminal モードに変更できます。

```
clear ssh-clienthostkey all
```

注：Flex System スイッチが IBMNOS CLI モードの場合、スイッチ CLI から以下のコマンドを入力し、SSH 鍵をクリアします。

```
maint
clssh
all
exit
```

更新の実行時にシステムが保守モードに入らない

この情報を使用して、ファームウェア更新と保守モードに関する問題をトラブルシューティングしてください。

ファームウェアの更新を再試行してください。

オペレーティング・システムからサーバーを再起動すると、保守モードがアクティブ化されない

以下のいずれかのサーバーで遅延アクティベーションを使用してファームウェアを更新した場合、サーバーをオペレーティング・システムから再起動した後でも、更新ステータスに「保守モードを保留中」と表示されます。

- Flex System x240 M5、タイプ 2591 および 9532
- NeXtScale nx360 M5、タイプ 5465
- System x3250 M6、タイプ 3633 および 3943
- System x3550 M5、タイプ 5463
- System x3500 M5、タイプ 5464
- System x3550 M5、タイプ 8869
- System x3650 M5、タイプ 5462
- System x3650 M5、タイプ 8871

この問題を解決するには、管理コントローラー Web インターフェースからサーバーを再起動します。サーバーがオンライン戻ると、更新アクティベーション・プロセスが再開されます。

Red Hat Enterprise Linux (RHEL) を実行するサーバーが再起動しない

Red Hat® Enterprise Linux (RHEL) v7 以降の場合は、オペレーティング・システムをグラフィカル・モードから再起動すると、デフォルトではサーバーが停止します。

RHEL を手動で構成して、電源ボタンの動作を電源オフに変更します。手順については、Red Hat データ移行および管理ガイド: グラフィカル・ターゲット・モードで電源ボタンを 押したときの動作を変更するを参照してください。

第 16 章　OS デバイス・ドライバー更新とリポジトリーの問題

この情報を使用して、OS デバイス・ドライバー更新に関する問題をトラブルシューティングしてください。

Lenovo サポート Web サイトに接続してデバイス・ドライバーの更新をダウンロードできない

Lenovo サポート Web サイトから UpdateXpress System Packs (UXSPs) およびデバイス・ドライバーをダウンロードする際に問題のトラブルシューティングを行うには、この情報を使用します。

- 管理用に構成された Lenovo XClarity Administrator アプライアンス・ポート (eth0 または eth1) がインターネットにアクセスできることを確認してください。ネットワークに関する考慮事項について詳しくは、XClarity Administrator オンライン・ドキュメントのネットワークに関する考慮事項を参照してください。
- 管理対象サーバーでデバイス・ドライバーを更新する前に、必要なポートとインターネット・アドレスがすべて使用可能になっていることを確認します。ポートについて詳しくは、利用可能なポートおよび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。

サーバーでデバイス・ドライバーを更新できない

この情報を使用して、管理対象サーバーでデバイス・ドライバーを更新するときの問題をトラブルシューティングしてください。

- サーバーがオンラインであり、Lenovo XClarity Administrator 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。
- デバイス・ドライバー更新の考慮事項を確認します (XClarity Administrator オンライン・ドキュメントの OS デバイス・ドライバー更新の考慮事項を参照)。

© Copyright Lenovo 2015, 2025

第 17 章 オペレーティング・システム・デプロイメントに関する問題

オペレーティング・システムを Lenovo XClarity Administrator から管理対象サーバーにデプロイしようとしたときに発生する問題をトラブルシューティングするには、この情報を使用します。

オペレーティング・システム・デプロイメントに関する一般的な問題については、オペレーティング・システムをデプロイできないを参照してください。

OS デプロイメント時に問題を報告しているステータス

オペレーティング・システム・デプロイメント時に Lenovo XClarity Administrator によって報告されたステータスとともに、この情報を使用して問題をトラブルシューティングします。

- XClarity Administrator 1.4.0 以前を使用して VMware 6.5 以降をデプロイした場合、ジョブ・ステータスによりオペレーティング・システムの準備が整う前にデプロイメントが完了したことが報告されることがあります。

  OS デプロイメントの完了を監視するためにスクリプトを使用している場合、OS デプロイメントが完了したことを示すデプロイメント・ジョブ・ステータスを受信した後、10 分間の遅延をスクリプトに追加します。
- VLAN タグを使用するネットワーク経由で Windows をデプロイする場合、デプロイメントの *専用構成パス*時にステータス エラーが報告されることがあります。

  このエラーは無視しても構いません。

オペレーティング・システムをデプロイできない

オペレーティング・システムを Lenovo XClarity Administrator から管理対象サーバーにデプロイしようとしたときに発生する一般的な問題をトラブルシューティングするには、このセクションの情報を使用します。

低速なネットワーク環境では、SLES 12 と 12.1 のオペレーティング・システム・デプロイメントを静的 IP モードで行うと、このモードではネットワーク遅延ブート・パラメーターが有効にならないため、失敗する可能性があります。この問題は SLES 12.2 で修正されています。

この問題を解決するには、以下の手順を実行します。

1. システム・ガードが有効になっている ThinkSystem V3 および V4 サーバー (XCC2 または XCC3 を使用) で、操作が「**OS ブートを防止**」に設定されている場合、システム・ガードがデバイスに準拠している必要があります。システム・ガードが適合しない場合、デバイスはブート・プロセスを完了できません。これが原因で OS デプロイメントは失敗します。これらのデバイスをプロビジョニングするには、システム・ガードのブート・プロンプトに手動で応答して、デバイスが正常にブートするようにします。
2. `https://<management_server_IP>/osdeployment/connection/...` **権限が拒否されました**というメッセージが表示される場合、サーバーの BIOS を更新し、日付と時刻の設定を現在の日付と時刻に変更します。
3. デプロイされているオペレーティング・システムのすべての要件を確認します。XClarity Administrator オンライン・ドキュメントの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。例:
   - Memory Mapped I/O (MMIO) 領域を 3 GB 以上に設定しないと、VMware ESXi のデプロイで問題が発生する場合があります。

© Copyright Lenovo 2015, 2025

- Microsoft Windows のデプロイと Active Directory ドメインへの参加を実行している場合は、XClarity Administrator オンライン・ドキュメントのWindows Active Directory との統合に記載されている考慮事項に従います。

4. 特定の I/O アダプターのオペレーション・システム・デプロイメント・サポート制限を確認します。I/O アダプターのサポートについては、XClarity Administrator のサポート – 互換性に 関する Web ページを参照してください。
5. XClarity Administrator とオペレーティング・システムがインストールされるデバイス (管理対象サーバー) の間のネットワーク接続が安定していることを確認します。

   注：SLES 11 SP4 をデプロイすると、ネットワーク接続が XClarity Administrator とデバイス間で失われた場合、デプロイメントが停止し、再開されない場合があります。これが発生した場合、ネットワーク環境を調べ、オペレーティング システムを再デプロイします。
6. XClarity Administrator で少なくとも 1 つのネットワーク・ポートがオペレーティング・システム・イメージを管理およびデプロイするように設定されていることを確認します。XClarity Administrator ネットワーク・トポロジーは、「ネットワーク・アクセス」ページで構成できます。「ネットワーク・アクセス」ページについて詳しくは、XClarity Administrator オンライン・ドキュメントのネットワーク・アクセスの構成を参照してください。
7. データ・ネットワークへの接続に用いられている XClarity Administrator ネットワーク・ポートが、管理対象サーバーのデータ・ネットワーク・ポートと同じネットワークに存在するよう構成されていることを確認します。サーバーのポートは MAC アドレスによって指定されており、「オペレーティング・システム」>「ネットワーク設定」ページで構成できます。ネットワーク設定の編集について詳しくは、XClarity Administrator オンライン・ドキュメントの管理対象サーバーのネットワーク設定の構成を参照してください。
8. ターゲット・サーバー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。ターゲット・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、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します。
9. 「OS イメージのデプロイ」ページからサーバーのステータスを表示して、デプロイメント・ステータスが「動作可能」であることを確認します。ステータスが「作動不能」の場合は、ステータス・リンクをクリックして、オペレーティング・システム・デプロイメントに対してサーバーの準備ができていない理由を確認します。オペレーティング・システム・デプロイメントについて詳しくは、XClarity Administrator オンライン・ドキュメントのオペレーティング・システム・イメージのデプロイを参照してください。
10. デバイスを、オペレーティング・システム・デプロイメントに対して選択された格納場所で確認できることを確かめます。

    ヒント: オペレーティング・システム・デプロイメントが成功したことを確認するには、オペレーティング・システム・デプロイメント用に選択されたストレージ以外のすべてのストレージをサーバーから切り離します。

ファイルを OS イメージ・リポジトリーにインポートできない

ファイルを Lenovo XClarity Administrator イメージ・リポジトリーにインポートしようとしているときに発生する問題をトラブルシューティングするには、このセクションの情報を使用します。

この問題を解決するには、以下の手順を実行します。

- インポート中のファイルがチェックサム・テストによって検証されていることを確認します。
- ベースとなるオペレーティング・システムが XClarity Administrator によってサポートされていることを確認します。XClarity Administrator オンライン・ドキュメントの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。
- ローカル・システムからインポートする場合:

  - 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、Chrome や Firefox など、別の Web ブラウザーを使用するか、
- リモート・ファイル・サーバーからインポートする場合:
  - ファイルへの絶対パスがリモート・ファイル・サーバー上の実際のパスと一致していることを確認します。
  - ファイルへの絶対パスに含まれるスラッシュまたはバック・スラッシュが、リモート・ファイル・サーバーをホストするオペレーティング・システムに応じて正しいことを確認します。
  - 必要なアクセス権限がリモート・ファイル・サーバーのディレクトリーに付与されていることを確認します。
  - OS イメージ・リポジトリーに、ファイルの保存に十分なディスク・スペースがあることを確認します (XClarity Administrator オンライン・ドキュメントの ディスク・スペースの管理を参照)。
  - 正しい資格情報を使用してリモート・ファイル・サーバーにログオンしていることを確認します。
  - XClarity Administrator とリモート・ファイル・サーバー間のネットワーク接続が安定していることを確認します。
  - 正しいトラステッド証明書がインポートされていること、その証明書が取り消されていないことを確認します (XClarity Administrator オンライン・ドキュメントの セキュリティー証明書の使用を参照)。
  - SSH が必要とするアルゴリズムの各タイプについて、XClarity Administrator でサポートされている転送アルゴリズムが少なくとも 1 つ、リモート・サーバーでサポートされていることを確認してください (XClarity Administrator オンライン・ドキュメントの セキュアな環境の実装を参照)。

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

ソフトウェア RAID アダプター (110i AnyRAID アダプター、ServeRAID C100 または C105 アダプター、および Intel RSTe SATA ソフトウェア RAID アダプターなど) を含むサーバーの場合、SATA アダプターが管理コントローラーで有効になっている場合は、SATA モードが「AHCI」に設定されている必要があります。その他のモード (「RAID」や「IDE」など) は、RHEL、SUSE、VMware または Windows オペレーティング・システムではソフトウェア RAID でサポートされていません。

注：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。通常オンボード Intel SATA ストレージ・アダプターに存在する RAID ソフトウェアはサポートされていません。ただし、ハードウェア RAID アダプターがない場合は、SATA アダプターを AHCI SATA モードに設定すると、オペレーティング・システム・デプロイメントが動作する場合があります。

ThinkServer で SATA モードを変更するには、以下の手順を実行します。
1. AMI Setup Utility から、「**Advanced Settings**」メニューを選択します。
2. 矢印キーを使用して「**SATA Mode**」を選択します。
3. `AHCI` に値を変更するには、「+」を押します。
4. 「**F10**」を押して変更を保存します。

その他のサーバーで SATA モードを変更するには、以下の手順を実行します。
1. F1 セットアップ・ユーティリティーで、「**System Settings**」 ➞ 「**Devices and I/O Ports**」 ➞ 「**Onboard SATA Mode**」 メニューを選択します。
2. `AHCI` に値を変更するには、「+」を押します。
3. 「**F10**」を押して変更を保存します。

OS インストーラーで ThinkServer サーバーをブートできない

ThinkServer サーバーでは、ThinkServer Management Module のストレージ OpROM ポリシーを「UEFI Only」設定しないと OS インストーラー・イメージが正しくブートできません。ポリシーが「Legacy Only」に設定されている場合、OS インストーラーはブートしません。

ストレージ OpROM ポリシーを変更するには、以下の手順を実行します。

1. AMI Setup Utility から、「**Boot Manager**」 ➡ 「**Miscellaneous Boot Settings**」メニューを選択します。
2. 矢印キーを使用して「**Storage OpROM Policy**」を選択します。
3. `UEFI Only` に値を変更するには、「+」を押します。
4. 「**F10**」を押して変更を保存します。

詳しくは、ご使用の ThinkServer の資料を参照してください。

VMware ESXi デプロイメントの問題

VMware ESXi オペレーティング・システムを Lenovo XClarity Administrator から管理対象サーバーにデプロイしようとしたときに発生する問題をトラブルシューティングするには、この情報を使用します。

VMware デプロイメントによりシステムのハングまたは再起動が発生する

VMware 5.1u1、5.1u2、5.1u3、または 5.5 (任意の update) の管理対象サーバーへのインストール中に、サーバーがハングアップしたり再起動したりする場合があります。

ハングアップまたは再起動は、次のメッセージの直後に発生する可能性があります。

```
Loading image.pld
```

VMware 5.5 では、サーバーの最初の 4 GB に Memory Mapped I/O (MMIO) 領域が構成されている必要があります。構成によっては、サーバーで 4 GB を超えるメモリーが使用されて、エラーが発生することがあります。

この問題を解決するには、以下の手順を実行します。

ヒント: 各サーバーの Setup Utility を通じて「**MM Config**」を設定する代わりに、仮想化に関連する事前定義済み拡張 UEFI パターンのいずれかを使用することを検討してください。これにより、MM Config オプションが 3 GB に設定され、PCI 64 ビットのリソース割り振りが無効になります。これらのパターンについて詳しくは、XClarity Administrator オンライン・ドキュメントの拡張 UEFI 設定の定義を参照してください。

1. システムを再起動します。「`Press <F1> Setup`」が表示されたら、F1 を押します。
2. 「**System Settings**」 ➡ 「**Devices and I/O Ports**」を選択します。
3. 「**MM Config**」の設定を 2 GB から 3 GB に変更します。
4. 「**PCI 64-Bit Resource**」の設定が「Disable」に設定されていることを確認します。
5. VMware イメージのインストールを再試行してください。

VMware デプロイメントがディスク・エラーで失敗する

VMware ESXi のインストール中、ディスク・ドライブに関連するエラーが返され、デプロイメントに失敗することがあります。

次の例のようなエラー・メッセージが表示されます。

```
error:/tmp/partitioning:line 2: install requires –disk
or –firstdisk
error:/tmp/partitioning:line 1: clearpart requires
```

```
one of the following arguments: -alldrives, -firstdisk,
-ignoredrives=, -drives=
```

このエラーは、フォーマットとインストールに使用可能な ESXi インストーラーが SAS 構成を検出しない場合に発生します。通常、これはサーバー上で RAID 構成が非アクティブであるか、正しく構成されていないことを意味します。または、サーバー・パターンが Lenovo XClarity Administrator を通じてデプロイされ、パターンに「**Disable local disk**」が選択された場合に発生することもあります。

この問題を解決するには、以下の手順を実行します。

- サーバー・パターンがこのサーバーにデプロイされていて、「**Disable local disk**」が選択されている場合、サーバー・パターンを更新してもう一度デプロイしてください。サーバー・パターンを使用したローカル・ストレージの構成について詳しくは、XClarity Administrator オンライン・ドキュメントの ローカル・ストレージの定義を参照してください。
- サーバーで RAID 構成が正しいことを確認してください。
  1. サーバーを再起動し、F12 キーを押して (HD0 などを選択) Legacy オプションでのブートを試みます。
  2. 起動中、LSI SAS アダプターに関する情報が表示されたら、Ctrl + C を押して構成を変更します。
  3. ユーザー・インターフェースが表示されたら、「**RAID properties**」、「**View Existing Configuration**」の順に選択します。
     - 「**View Existing Configuration**」が表示されない場合、RAID は構成されていません。
     - 既存の構成に「Inactive」ステータスが表示される場合、RAID が正しく構成されていることを確認します。

オペレーティング・システムがブートせず ThinkServer サーバーへの ESXi のデプロイメントが完了しない

この情報を使用して、インストール・ドライブ以外で、PXE が有効になっているネットワーク・カードまたは起動可能デバイスがブート順序リストに含まれている場合に、Lenovo XClarity Administrator から管理対象サーバーに VMware ESXi オペレーティング・システムをデプロイしようと試みたときに発生する可能性のある問題をトラブルシューティングしてください。

ThinkServer サーバーで ESXi をデプロイする際、オペレーティング・システムはオペレーティング・システムがインストールされているドライブをブート順序リストの最上位に明示的に移動させません。ブート可能 OS を含むブート・デバイスまたは PXE サーバーが ESXi を含むブート・デバイスよりも前に指定されている場合、ESXi はブートしません。ESXi デプロイメントでは、ほとんどのサーバーで XClarity Administrator がブート順序リストを更新して、ESXi ブート・デバイスがブート順序の最上位に来るようにします。ただし、ThinkServer サーバーでは XClarity Administrator 向けにブート順序リストを更新する手段がありません。

ThinkServer サーバーで PXE ブート可能なネットワーク・アダプターがある場合は、ネットワーク・アダプターで PXE のサポートを無効にし、オペレーティング・システムを再デプロイしてから、PXE サポートを再度有効にします。F12 を押してブートをインターセプトし、PXE 設定に入ります。PXE ブート設定の変更について詳しくは、ネットワーク・アダプターの資料を参照してください。

ThinkServer サーバーに、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、その起動可能デバイスをブート順序リストから削除し、オペレーティング・システムを再デプロイしてから、起動可能デバイスをブート順序リストに戻します。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。ブート順序リストの変更について詳しくは、ThinkServer の資料を参照してください。

Red Hat および SUSE Linux のデプロイメントに関する問題

Red Hat および SUSE Linux オペレーティング・システムを Lenovo XClarity Administrator から管理対象サーバーにデプロイしようとしたときに発生する問題をトラブルシューティングするには、この情報を使用します。

静的 IP を使用して Redhat 6.x をラックベース・サーバーにデプロイできない

管理対象サーバーがラック装着 (TOR) スイッチに接続されている場合、Redhat 6.x をそのサーバーにデプロイしようとすると問題が発生することがあります。TOR スイッチで**スパンニング・ツリー・プロトコル**が有効になっていて、**デフォルトでの転送**が無効になっている場合、Redhat イメージをサーバーにダウンロードすることができません。

この問題を解決するには、以下の手順を実行します。

- サーバーが DHCP を使用する (静的 IP アドレスを使用しない) ように構成されていることを確認します。その後、オペレーティング・システムのデプロイを再試行してください。
- ラック装着 (TOR) スイッチの構成を変更し、スパンニング・ツリー・プロトコルを無効にするか、デフォルトでのパケット転送を有効にします。

ドライバーが欠落しているために OS デプロイメントが失敗する

Red Hat® Enterprise Linux (RHEL) サーバーまたは SUSE® Linux Enterprise Server (SLES) をサーバーにデプロイする場合、デプロイを停止し、デプロイ・ジョブが最終的にタイムアウトになるエラー・メッセージが表示される場合があります。

この問題は、管理対象サーバーにインストールされているすべてのアダプターをサポートするドライバーがオペレーティング・システム・イメージに含まれていない場合に発生することがあります。

特定の Mellanox IB アダプター向けのすぐに利用可能なドライバーは、Lenovo XClarity Administrator では事前にロードされていません。したがって、これらの Mellanox アダプターを使用して RHEL または SLES をサーバーにデプロイすることはサポートされていません。Mellanox アダプターの制限事項に関する詳細は、Mellanox 向け Lenovo XClarity Administrator のサポート アダプター Web ページ を参照してください。

Microsoft Windows のデプロイメントの問題

Microsoft Windows を Lenovo XClarity Administrator から管理対象サーバーにデプロイしようとしたときに発生する問題をトラブルシューティングするには、この情報を使用します。

接続されたディスク・ドライブに既存のシステム・パーティションがあるため、OS デプロイメントが失敗する

Microsoft Windows をサーバーにデプロイする場合は、アタッチされたディスク・ドライブに既存のシステム・パーティションがあってはなりません。パーティションが検出されると、OS デプロイメントは失敗します。

この問題を解決するには、以下の手順のいずれかを実行してください。

- アタッチされたディスク・ドライブを切り離します。
- アタッチされたディスク・ドライブのシステム・パーティションを手動で削除します。

  注意：ディスク・ドライブのパーティションを削除すると、データが失われる可能性があります。パーティションを削除する前に、ディスク・ドライブのすべてのデータをバックアップしてください。

  1. Windows コマンド・プロンプトから、`diskpart` ユーティリティーを実行します (DiskPart コマンド Web サイトを参照)。

2. `select disk` ***<number>*** と入力してディスクを選択します。*<number>* は削除するパーティションを含むディスクのディスク番号です (ディスクの選択 Web サイトを参照)。
3. `select partition` ***<number>*** と入力して削除するパーティションを選択します。*<number>* は選択したディスクのパーティション番号です (パーティションの選択 Web サイトを参照)。
4. `delete partition override` と入力してパーティションを削除します。ディスク番号とパーティション番号は、システム・パーティションが検出されたときに表示される WinPE エラー・メッセージに含まれています。これはジョブ・ログにもあります。(パーティションの削除 Web サイトを参照)

第 18 章　リモート制御に関する問題

Lenovo XClarity Administrator でリモート制御アプリケーションの使用時に発生する可能性がある問題を解決するには、この情報を使用します。

リモート制御セッションが開始されない

Lenovo XClarity Administrator Web インターフェースまたはシステムのショートカットからリモート制御セッションを開始しようとしている場合は、この情報を使用します。

この問題を解決するには、以下の手順を実行します。

1. 接続先のサーバーが XClarity Administrator によって管理されていること、および「オンライン」または「正常」状態であることを確認します。サーバー状況について詳しくは、XClarity Administrator オンライン・ドキュメントの管理対象サーバーのステータスの表示を参照してください。
2. Web ブラウザーでセッションのポップアップ・ダイアログが無効になっていないことを確認します。
3. Web ブラウザーで XClarity Administrator ノードのセキュリティー証明書が受け入れられていることを確認します。通常は、ブラウザーから初めて XClarity Administrator にアクセスしたときに、証明書を承認するように求められます。
4. 「リモート制御」ウィンドウで、**「設定」 ➡ 「全般」 ➡ 「管理サーバーと同期」**をクリックし、1 分間待ちます。その後、リモート制御セッションをもう一度開きます。
5. サポートされている JRE を使用してアプリケーションを起動していることを確認します。
   - Internet Explorer で、**「ツール」 ➡ 「インターネット オプション」 ➡ 「詳細設定」**の順にクリックします。正しい JRE が選択されていることを確認します (JRE バージョン 7.0、Update 18 以降)。
   - Firefox で、**「ツール」 ➡ 「オプション」 ➡ 「プログラム」**の順にクリックします。JNLP というファイルの種類に Java Web Start Launcher が関連付けられていることを確認します。

   注：Java コントロール・パネルで「**Use SSL 2.0 compatible ClientHello format**」オプションが選択されて*いない*ことを確認します。

   デスクトップのショートカットからアプリケーションを起動している場合は、ローカル・システムが XClarity Administrator に接続できることを確認します。XClarity Administrator 認証サーバーを使用してユーザー ID が検証されます。
6. ローカル・システムの Java Web Start のキャッシュをクリアします。Windows オペレーティング・システムを実行しているシステムで Java Web Start のキャッシュをクリアするには、コマンド `javaws -uninstall` を実行します。これは、Windows コントロール パネルの JAVA メニューでも行うことができます。
7. リモート制御を使用するには、ThinkServer サーバーに ThinkServer System Manager Premium Upgrade の Features on Demand キーがインストールされている必要があります。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、XClarity Administratorオンライン・ドキュメントの Feature on Demand キーの表示を参照してください。

リモート制御セッションがログイン後にハングアップする

ここには、リモート制御セッションがログイン後にハングアップした場合の問題を解決するための情報が含まれています。

サポートされている JRE が使用されていないと、リモート制御セッションがログイン後にハングアップすることがあります。リモート制御セッションがログイン後にハングアップしているように見える場合は、サポートされている JRE を使用してアプリケーションを起動していることを確認してください。

© Copyright Lenovo 2015, 2025

- Oracle JRE バージョン 6.18 以降

サーバーに接続できない

ここには、サーバーとのリモート制御セッションを確立できない場合に問題を解決するための情報が含まれています。

この問題を解決するには、以下の手順を実行します。

- **lxc-supervisor**、**lxc-admin**、**lxc-security-admin**、**lxc-fw-admin**、**lxc-os-admin**、**lxc-hw-admin**、**lxc-service-admin** または **lxc-hw-manager** 権限があることを確認します。
- ローカル・システムがネットワークに接続されていて、Lenovo XClarity Administrator に接続できることを確認します。
- XClarity Administrator のメニュー・バーで「**ハードウェア**」 → 「**サーバー**」の順にクリックして、サーバーが XClarity Administrator により管理されていることを確認します。
- ローカル・システムにファイアウォールがインストールされている場合は、ファイアウォールでその管理対象サーバーの IP アドレスへの接続が許可されていることを確認します。
- その管理対象サーバーの IP アドレスに対して ping を実行して、ローカル・システムがその管理対象サーバーに接続できることを確認します。外部ネットワークの IP アドレスを持つローカル・システムから管理対象サーバーにアクセスしている場合は、その管理対象サーバーにも外部からアクセスできる IP アドレスが必要です。
- プライベート管理ネットワークでのみネットワーク・アドレス指定可能な管理対象サーバーに対するリモート制御要求を XClarity Administrator がトンネリングできるように、XClarity Administrator トンネリングが無効になっていないことを確認します。トンネリングはデフォルトで有効です。XClarity Administrator トンネリングは、「設定」ダイアログの「**セキュリティー**」タブで有効にすることができます。詳しくは、リモート制御の設定を参照してください。

リモート制御セッションの開始後に Flex System スイッチと通信できない

ここには、リモート制御セッションの開始後に Lenovo XClarity Administrator が Cisco Nexus B22 Fabric Extender ネットワーク・スイッチとの通信を停止した場合に問題を解決するための情報が含まれています。

CMM が自動検出を使用するように構成されている場合は、Cisco Nexus B22 Fabric Extender ネットワーク・スイッチのネットワーク・ポートが自動ネゴシエーション・モードを使用するように構成されていることを確認します。

シングルユーザー・モードでサーバーに接続できない

ここには、シングルユーザー・モードでサーバーに接続できない場合に問題を解決するための情報が含まれています。

シングルユーザー・モードでサーバーに接続する場合、そのサーバーに対して確立できるリモート制御セッションは一度に 1 つだけです。

この問題を解決するには、以下の手順を実行します。

1. マルチユーザー・モードで管理対象サーバーに接続します (セキュリティー要件で許可されている場合)。
2. 他のユーザーに問い合わせて、その管理対象サーバーで既にリモート制御セッションを確立しているユーザーがいるかどうかを確認します。確立している場合は、管理対象サーバーでのそのユーザーのリモート制御セッションが終了するまで待ちます。
3. 再びシングルユーザー・モードで管理対象サーバーに接続します。

リモート制御でサーバーに接続できるがビデオを使用できない

ここには、リモート制御セッションからサーバーに接続するとセッションに「No video available」というメッセージが表示される場合に、問題を解決するための情報が含まれています。

サーバーの電源がオンになっていることと、オペレーティング・システムで使用されている解像度とリフレッシュ・レートがサポートされていることを確認します。

サポートされている解像度とリフレッシュ・レートを次の表に示します。

表 1. サポートされる解像度およびリフレッシュ・レート

解像度	リフレッシュ・レート
640 x 480	60、72、75、および 85 Hz
800 x 600	60、72、75、および 85 Hz
1024 x 768	60、72、75、および 85 Hz
1440 x 900	60 Hz
1280 x 1024	60 および 75 Hz
1680 x 1050	60 Hz
1600 x 1200	60 および 75 Hz

新しいセッションを追加するためのリストにサーバーが表示されない

ここには、新しいセッションを追加するためのリストにサーバーが表示されない場合や、サーバーがサムネール領域に表示されなくなった場合に、問題を解決するための情報が含まれています。

この問題を解決するには、以下の手順を実行します。

1. XClarity Administrator のメニュー・バーで「**ハードウェア**」 → 「**サーバー**」の順にクリックして、管理対象サーバーが Lenovo XClarity Administrator により管理されていることを確認します。
2. リモート制御の設定メニューで「**全般**」タブをクリックし、「**管理サーバーと同期**」をクリックして、インベントリーを同期します。リモート制御設定について詳しくは、XClarity Administrator オンライン・ドキュメントのリモート制御の設定を参照してください。

サーバーの状態がリモート制御セッションと Lenovo XClarity Administrator とで一致しない

ここには、リモート制御セッションの管理対象サーバーの状態が Lenovo XClarity Administrator の管理対象サーバーの状態と一致しないときのトラブルシューティングのための情報が含まれています。

この問題を解決するには、以下の手順を実行します。

1. XClarity Administrator のメニュー・バーで「**ハードウェア**」 → 「**サーバー**」の順にクリックして、サーバーが XClarity Administrator により管理されていることを確認します。
2. リモート制御の設定メニューで「**全般**」タブをクリックし、「**管理サーバーと同期**」をクリックして、インベントリーを同期します。リモート制御設定について詳しくは、XClarity Administrator オンライン・ドキュメントのリモート制御の設定を参照してください。

ドライブまたはイメージをサーバーにマウントできない

ここには、リモート・メディアを使用してドライブまたはイメージをマウントしようとしてもマウントできない問題のトラブルシューティングのための情報が含まれています。

この問題を解決するには、以下の手順を実行します。

1. リモート制御セッションを停止して再起動します。
2. リモート制御セッションのデバッグ・モードを「全文」に設定します。デバッグ・モードは、「**全般**」ページの「設定」で設定できます。デバッグ・モードを「全文」に設定すると、リモート制御セッションによって診断ログ・ファイルが生成されます。デバッグ・モードについて詳しくは、リモート制御の設定を参照してください。
3. Lenovo サポートに連絡してログ・ファイルを提供します。診断データを Lenovo サポートに送信する方法について詳しくは、サービスおよびサポートの操作を参照してください。

マウント可能なリモート・メディア・デバイスのリストにストレージ・メディアのオプションが表示されない

ここには、マウント可能なリモート・メディア・デバイスのリストにストレージ・メディアのオプションが表示されないときのトラブルシューティングのための情報が含まれています。

管理対象サーバーにマウントできるリモート・メディア・デバイスのリストに CD、DVD、または USB デバイスが表示されない場合は、リモート・メディア・パネルで「**管理者アカウントを使用して再起動**」をクリックして他のローカル・デバイスにアクセスしてください。

電源操作を実行できない

管理対象サーバーでリモート制御セッションから電源操作を実行しようとしても実行できないときに発生する問題をトラブルシューティングするには、この情報を使用します。

管理対象サーバーでリモート制御セッションから電源操作を実行しようとしたときに、電源操作が失敗したこと、または管理対象サーバーの現在のステータスでは電源操作を適用できないことを示すメッセージが表示される場合があります。

この問題を解決するには、以下の手順を実行します。

1. サーバーが Lenovo XClarity Administrator により管理されていることを確認します。詳しくは、XClarity Administrator オンライン・ドキュメントの管理対象サーバーのステータスの表示を参照してください。
2. 「サーバー」ページから、サーバーのステータスが有効であることを確認してください。
3. サーバーの現在の状態に対して電源操作が有効であることを確認します。たとえば、サーバーの電源が現在オフになっている場合は、電源オフを実行しても無効です。
4. 電源操作が完了したかどうかをジョブ・ログで確認します。XClarity Administrator の現在の負荷によっては、操作が完了するのに多少時間がかかることもあります。ジョブ・ステータスの表示について詳しくは、ジョブの監視を参照してください。

Flex System x280 X6、x480 X6、x880 X6 サーバー への接続時にビデオが使用できない

Flex System x280 X6、x480 X6、x880 X6 サーバー マルチノード・システムとのリモート・コンソール・セッションを開始しようとしたときの問題、または新しいタブにビデオが表示されないときの問題をトラブルシューティングするには、この情報を使用します。

この問題を解決するには、以下の手順を実行します。

1. 開始した接続がまだアクティブな場合は、新しいタブを閉じて接続を終了します。
2. マルチノード構成では、*プライマリー・サーバー*とのリモート接続を開始する必要があります。

第 19 章 ユーザー・インターフェースの問題

この情報を使用して、ユーザー・インターフェースに関する問題をトラブルシューティングしてください。

メニュー項目、ツールバー・アイコン、およびボタンが無効になっています (淡色表示)

ユーザー・インターフェースで特定の操作が無効になっている場合は、この情報を使用して、問題をトラブルシューティングしてください。

*役割*は、リソースへのユーザー・アクセスを制御したり、ユーザーがそれらのリソースで実行できる操作を制限したりするために使用されます。*役割グループ*は、1 つ以上の役割のコレクションであり、それらの役割を複数のユーザーに割り当てるために使用されます。役割グループに対して構成する役割により、その役割グループのメンバーであるユーザーに付与されるアクセス・レベルが決まります。Lenovo XClarity Administrator ユーザーは、それぞれ少なくとも 1 つの役割グループのメンバーになっている必要があります。役割と権限については、XClarity Administrator オンライン・ドキュメントの 役割の管理 を参照してください。

操作を実行するために必要な権限を持つ役割グループにユーザー・アカウントが割り当てられていることを確認します。詳細については、システム管理者にお問い合わせください。

複数のタブが開いていると Web ブラウザーが応答しなくなる

Lenovo XClarity Administrator ページを含む複数のタブが開いていると、Web ブラウザーが異常終了またはが応答しなくなる場合がある

XClarity Administrator は管理サーバーと大量のデータを交換するクライアント側 JavaScript を使用します。複数のタブが開いていると、Web ブラウザーはより多くのメモリー、プロセッサー・サイクル、ネットワーク帯域幅を使用します。複数のタブを開くと、一部のブラウザーが異常終了したり応答しなくなることがあります。影響は Web ブラウザーのタイプとバージョンによって異なります。

この問題を解決するには、XClarity Administrator ページを開いている Web ブラウザーのタブの数を減らします。

詳しくは、Tip HT504133 を参照してください。

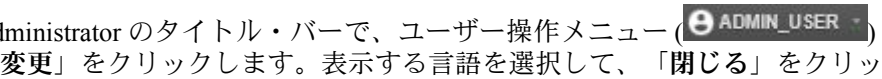
JSON 応答の失敗、解析エラー、他の予期しないエラー

この情報を使用して、JSON 応答に関する問題をトラブルシューティングしてください。

Lenovo XClarity Administrator からログアウトし、再度ログインしてみます。

ユーザー・インターフェースで、希望の言語が使用されない

この情報を使用して、言語設定に関する問題をトラブルシューティングしてください。

1. Web ブラウザーが希望の言語のロケールを使用していることを確認します。
2. Lenovo XClarity Administrator のタイトル・バーで、ユーザー操作メニュー (

) をクリックした後、「**言語の変更**」をクリックします。表示する言語を選択して、「**閉じる**」をクリックします。

© Copyright Lenovo 2015, 2025

読み込みが低速または応答していないように見える、更新に長い時間がかかる、描画が適切でない

この情報を使用して、ユーザー・インターフェースに関する問題をトラブルシューティングしてください。

1. Web ブラウザーで「**最新の情報に更新**」ボタンを使用してページを更新します。
2. Web ブラウザーのキャッシュをクリアして、ページを再ロードします。

予期しないデータ損失

この情報を使用して、Lenovo XClarity Administrator のデータ損失に関する問題をトラブルシューティングしてください。

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された場合は、最新のバックアップから XClarity Administrator を復元します (XClarity Administrator オンライン・ドキュメントのXClarity Administrator のバックアップと復元を参照)。

ラック・ビューでデバイスの場所の変更が反映されない

この情報を使用して、Lenovo XClarity Administrator のラック・ビューに関する問題をトラブルシューティングしてください。

デバイスが XClarity Administrator により管理された後、以下の REST API またはベースボード管理コントローラーのいずれかを使用してデバイスの場所を変更した場合は、XClarity Administrator ユーザー・インターフェースのラック・ビューには変更が反映されません。デバイスのプロパティまたはユーザー・インターフェースのラックを編集して、API または管理コントローラーでの変更を反映します (サーバーのシステム・プロパティの変更、管理対象シャーシの詳細の表示、およびラックの管理を参照)。

- PUT /canisters/*<UUID>*
- PUT /chassis/*<UUID>*
- PUT /nodes/*<UUID>*