Lenovo

Lenovo XClarity Administrator

ユーザーズ・ガイド

バージョン 4.0.0

第 1 版 (2023 年 2 月)

目次

目次 i

表 v

変更の要約 vii

第 1 章 . Lenovo XClarity Administrator 概要 1

XClarity Administrator へのログイン 5

ユーザー・インターフェースのヒントと手法 . . . 9

Lenovo XClarity Mobile アプリの使用 10

第 2 章 . Lenovo XClarity Administrator の管理 17

認証と許可の管理 17

- 認証サーバーの管理 17
- ユーザー・アカウントの管理 34
- 保存された資格情報の管理 40
- 役割と役割グループの管理 41
- デバイスに対するアクセスの管理 57

セキュアな環境の実装 60

- ユーザー・アカウントのセキュリティー設定の変更 62
- 管理サーバーでの暗号化設定の構成 64
- 管理対象サーバーのセキュリティー設定の構成 66
- セキュリティー証明書の使用 68
- Encapsulation の有効化 79
- NIST SP 800-131A コンプライアンスの実装 . 80

VMware ツールの使用 81

ネットワーク・アクセスの構成 81

日付と時刻の設定 88

インベントリー設定の設定 90

アラートおよびイベント生成のしきい値設定の設定 91

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 91

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 97

XClarity Administrator を TruScale ポータルへのハブとして接続 100

システム・データと設定のバックアップ、復元、移行 100

- Lenovo XClarity Administrator のバックアップ 100
- Lenovo XClarity Administrator の復元 102
- 別の XClarity Administrator インスタンスへのシステム・データと設定の移行 104

ディスク・スペースの管理 106

リモート共有の管理 109

ユーザー・インターフェースの言語の変更 . . . 110

XClarity Administrator のシャットダウン 110

XClarity Administratorの再起動 111

第 3 章 . デバイスおよびアクティビティの監視 115

環境の概要の表示 115

- ハードウェア・ステータスの概要の表示 . . 116
- プロビジョニング・ステータスの要約の表示 117
- Lenovo XClarity Administrator 活動の要約の表示 118

監視システム・リソース 118

プロビジョニング・ステータスの傾向の監視 . . 120

履歴メトリックの監視 122

デバイスを保守モードにする 123

アラートの使用 124

- アクティブなアラートの表示 124
- アラートの除外 128
- アラートの解決 129
- アラートの確認 130

イベントの使用 130

- イベント・ログでのイベントの監視 130
- 監視ログでのイベントの監視 133
- イベントの解決 134
- イベントの除外 134
- イベントの転送 136

ジョブの操作 169

- ジョブの監視 170
- ジョブのスケジューリング 172
- ジョブに対する解決策とコメントの追加 . . 175

ジョブおよびイベントの間の関係の表示 175

第 4 章 . 管理に関する考慮事項 . . . 179

第 5 章 . リソース・グループの管理 . 181

リソース・グループのデバイスのステータスの表示 181

リソース・グループのメンバーの表示 183

動的リソース・グループの作成 186

静的リソース・グループの作成 188

リソース・グループの削除 189

リソース・グループのプロパティの変更 190

第 6 章 . ラックの管理 191

ラックのデバイスのステータスの表示 195

ラックの取り外し 197

第 7 章 . シャーシの管理 199
管理対象シャーシのステータスの表示 208
管理対象シャーシの詳細の表示 209
CMM 構成データのバックアップと復元 212
シャーシの CMM Web インターフェースの起動 . 212
シャーシのシステム・プロパティの変更 213
シャーシの管理 IP 設定の変更 213
CMM フェイルオーバーの構成 214
CMM の再始動 215
CMM の仮想再取り付け 216
シャーシの有効期限切れまたは無効の保存された資格情報の解決 217
管理サーバーの障害発生後の CMM による管理のリカバリー 218
シャーシの管理解除 219
正しく管理解除されなかったシャーシのリカバリー 220

第 8 章 . サーバーの管理 223
管理対象サーバーのステータスの表示 233
管理対象サーバーの詳細の表示 236
サーバー構成データのバックアップと復元 . . . 241
システム・ガードを有効にする 242
ドライブのデータの安全な消去 243
リモート制御の使用 244
リモート制御を使用した ThinkSystem または ThinkAgile サーバーの管理 244
リモート制御を使用した ThinkServer および NeXtScale sd350 M5 サーバーの管理 245
リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理 246
管理対象サーバーのオペレーティング・システムへのアクセスの管理 258
Features on Demand キーの表示 259
エネルギーおよび温度の管理 260
サーバーの電源のオン/オフ 261
Flex System シャーシのサーバーの仮想再取り付け 262
サーバーの管理コントローラー・インターフェースの起動 263
サーバーのシステム・プロパティの変更 264
サーバーの有効期限切れまたは無効の保存された資格情報の解決 265
サーバー・パターン・デプロイ後の障害の発生したサーバーのリカバリー 266
サーバー・パターンのデプロイ後のブート設定のリカバリー 267
管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー 268
管理の強制を使用した管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー 268
管理コントローラーを使用した、正しく管理解除されなかった System x または NeXtScale M4 サーバーのリカバリー 268
管理サーバーの障害後の管理コントローラー・リセットによる ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理のリカバリー 269
管理サーバーの障害後の cimcli を使用した ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理のリカバリー 270
管理サーバーの障害後の管理コントローラー・インターフェースを使用した ThinkServer サーバー管理のリカバリー . . . 272
ラック・サーバーまたはタワー・サーバーの管理解除 272
正しく管理解除されなかったラックまたはタワー・サーバーのリカバリー 274

第 9 章 . ストレージ・デバイスの管理 279
ストレージの管理に関する考慮事項 282
ストレージ・デバイスのステータスの表示 . . . 283
ストレージ・デバイスの詳細の表示 285
ストレージ構成データのバックアップと復元 . . 288
ストレージ・デバイスの電源のオン/オフ . . . 288
Flex System ストレージ・デバイスへのストレージ・コントローラーの仮想再取り付け 289
ストレージ・デバイスの管理コントローラー・インターフェースの起動 290
ストレージ・デバイスのシステム・プロパティの変更 290
管理サーバーの障害発生後のラック・ストレージ・デバイスによる管理のリカバリー 291
管理サーバーの障害発生後の Lenovo ThinkSystem DE Series ストレージ・デバイスによる管理のリカバリー 292
ストレージ・デバイスの管理解除 292
正しく管理解除されなかったラック・ストレージ・デバイスのリカバリー 293

第 10 章 . スイッチの管理 295
スイッチの管理に関する考慮事項 301
スイッチのステータスの表示 302
スイッチの詳細の表示 305
スイッチの電源のオン/オフ 308
スイッチ・ポートの有効化および無効化 308
スイッチ構成データのバックアップと復元 . . . 310
スイッチ構成データのバックアップ 310
スイッチ構成データの復元 311
スイッチ構成ファイルのエクスポートとインポート 313
スイッチの管理コントローラー・インターフェースの起動 315
スイッチのリモート SSH セッションの起動 . . . 316

スイッチのシステム・プロパティの変更 316
スイッチの有効期限切れまたは無効の保存された資格情報の解決 317
管理サーバーの障害発生後のスイッチによる管理のリカバリー 318
のスイッチの管理解除 318
管理対象から正しく除外されなかったスイッチのリカバリー 319

第 11 章 . 構成パターンを使用したサーバーの構成. 321
構成に関する考慮事項 323
アドレス・プールの定義 324
IP アドレス・プールの作成 326
イーサネット・アドレス・プールの作成 . . 327
Fibre Channel アドレス・プールの作成 . . . 329
サーバー・パターンの使用 333
サーバー・パターンの作成. 335
サーバーへのサーバー・パターンのデプロイ 358
サーバー・パターンの変更. 360
サーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート 362
サーバー・プロファイルの使用 362
サーバー・プロファイルのアクティブ化 . . 364
サーバー・プロファイルの非アクティブ化 . 365
サーバー・プロファイルの削除. 366
プレースホルダー・シャーシの使用. 367
プレースホルダー・シャーシの作成 367
プレースホルダー・シャーシへのサーバー・パターンのデプロイ 368
プレースホルダー・シャーシのデプロイ . . 369
ストレージ・アダプターのデフォルト値へのリセット. 370
メモリーの構成 372

第 12 章 . 構成テンプレートを使用したスイッチの構成 373
デフォルトのサーバー構成設定の設定 374
スイッチ構成テンプレートの作成. 375
VLAN ポート・メンバーシップ設定の定義 . 377
VLAN プロパティーの定義. 378
VLAN 設定の削除 379
VLAN の削除 380
ポート・チャネル基本設定の定義 380
ポート・チャネル詳細設定の定義 381
ポート・チャネルの削除 382
全般スイッチの設定の定義. 382
共通 L2 インターフェース設定の定義 . . . 383
ピア VLAG 設定の定義 384
VLAG インスタンス設定の定義 384
VLAG 詳細設定の定義 385
VLAG インスタンスの削除. 386
スパイン・リーフ・トポロジーの定義 . . . 386
ターゲット・スイッチへのスイッチ構成テンプレートのデプロイ 387
スイッチ構成デプロイメント履歴の表示 387

第 13 章 . 管理対象デバイスでのファームウェアの更新 389
ファームウェアの更新に関する考慮事項 396
ファームウェア更新リポジトリーの管理 403
ファームウェア更新のリモート・リポジトリーの使用 407
製品カタログの更新 408
ファームウェア更新のダウンロード 409
ファームウェア更新のエクスポートとインポート 417
ファームウェア更新の削除. 418
ファームウェア・コンプライアンス・ポリシーの作成と割り当て 419
準拠していないデバイスの特定 424
ファームウェア更新の共通設定の構成 425
ファームウェア更新の適用とアクティブ化 . . . 426
コンプライアンス・ポリシーを使用するバンドルされたファームウェア更新の適用 . . . 427
コンプライアンス・ポリシーを使用する選択済みファームウェア更新の適用 431
コンプライアンス・ポリシーを使用しない選択済みファームウェア更新の適用 438

第 14 章 . 管理対象サーバーの Windows デバイス・ドライバーの更新 445
OS デバイス・ドライバー更新の考慮事項 . . . 448
OS デバイス・ドライバー・リポジトリーの管理. 449
OS のデバイス・ドライバー・カタログの更新 451
Windows デバイス・ドライバーのダウンロード 452
OS デバイス・ドライバー更新用の Windows Server の構成 455
OS デバイス・ドライバー更新用のドメイン・アカウントの構成 456
共通 Windows デバイス・ドライバー更新設定の構成. 457
Windows デバイス・ドライバーの適用 458

第 15 章 . ベア・メタル・サーバーへのオペレーティング・システムのインストール 463
オペレーティング・システム・デプロイメントの考慮事項 466
サポートされているオペレーティング・システム. 471

オペレーティング・システム・イメージ・プロファイル 475
デプロイされたオペレーティング・システムで利用可能なポート 479
リモート・ファイル・サーバーの構成 481
オペレーティング・システム・イメージのインポート 483
OS イメージ・プロファイルのカスタマイズ . . 486
カスタマイズされた OS イメージ・プロファイルのインポート 493
ブート・ファイルのインポート 495
デバイス・ドライバーのインポート 500
カスタム構成設定のインポート 504
カスタム無人ファイルのインポート 522
無人ファイルを構成設定ファイルに関連付ける 527
カスタム・インストール・スクリプトのインポート 528
カスタム・ソフトウェアのインポート . . . 533
カスタム OS イメージ・プロファイルの作成 535
グローバル OS デプロイメント設定の構成 . . . 538
管理対象サーバーのネットワーク設定の構成 . . 540
管理対象サーバーの保管場所の選択 542
オペレーティング・システム・イメージのデプロイ 545
Windows Active Directory との統合 549
OS デプロイメントのシナリオ 553
カスタム・デバイス・ドライバーを伴う RHEL のデプロイ 553
カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ 555
カスタム・ソフトウェアおよびポスト・インストール・スクリプトを使用した RHEL および、Hello World PHP アプリケーションのデプロイ 559
カスタム・パッケージとタイム・ゾーンを使用した SLES 12 SP3 のデプロイ 562
カスタム・ソフトウェアを伴う SLES 12 SP3 のデプロイ 569
構成可能なロケールと NTP サーバーを使用する SLES 12 SP3 のデプロイ 572
静的 IP アドレスを使用したローカル・ディスクへの Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ 577
構成可能なロケールとセカンド・ユーザー資格情報を使用する Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ 580
カスタム機能を伴う Windows 2016 のデプロイ 585
カスタム・ソフトウェアを伴う Windows 2016 のデプロイ 588
日本語の Windows 2016 のデプロイ 592

第 16 章 . 新しいデバイスをセットアップするためのエンド・ツー・エンドのシナリオ 601

ローカル・ハードディスク・ドライブへの ESXi のデプロイ 601
事前定義済み仮想化パターンのデプロイ . . 601
Flex System x240 計算ノード への VMware ESXi のデプロイ 603
SAN ストレージへの ESXi のデプロイ 608
SAN ブートをサポートするためのサーバー・パターンのデプロイ 608
SAN ストレージへの VMware ESXi のデプロイ 611
注記 . . . . . dcxix
商標 . . . . . dcxix

表

1. アカウント・セキュリティー設定 62
2. ネットワーク・トポロジーに基づく各ネットワーク・インターフェースの役割 83
3. Lenovo MAC アドレス・プール 329
4. Brocade WWN アドレス・プール 330
5. Emulex WWN アドレス・プール 331
6. Lenovo WWN アドレス・プール 332
7. QLogic WWN アドレス・プール 333

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。

このバージョンは、管理ソフトウェアに対する以下の機能拡張をサポートします。

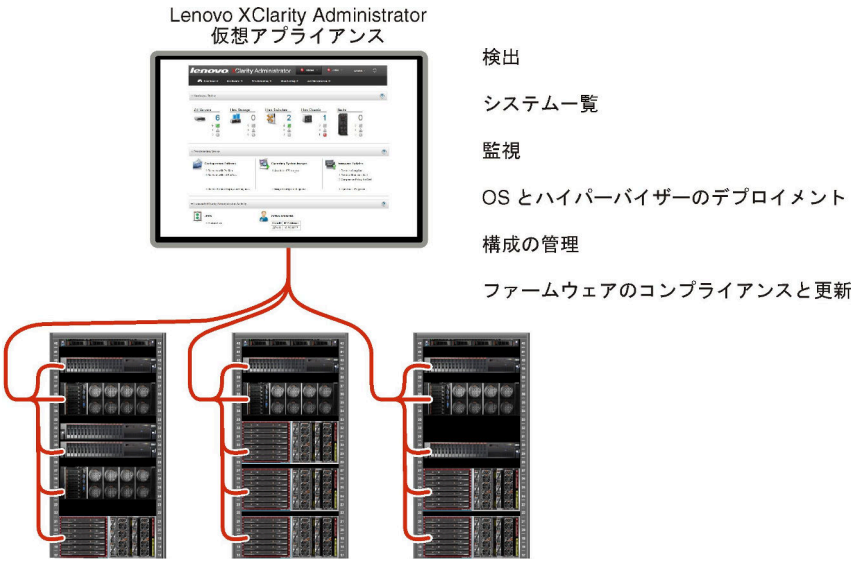
以前のリリースの変更については、XClarity Administrator オンライン・ドキュメントの 最新情報 を参照してください。

機能	説明
管理	XClarity Administrator 管理サーバーの完全修飾ドメイン名 (FQDN) と DNS 情報を、IMM2、XCC、および XCC2 の管理対象サーバーにプッシュすると、管理対象サーバーでこの情報を使用して管理サーバーを検索できます (「ネットワーク・アクセスの構成」を参照)。
監視	永続メモリー (PMEM) コンポーネントの追加のインベントリー・データを表示できます (「管理対象サーバーの詳細の表示」を参照)。 ストレージ・デバイスの追加のインベントリー・データを表示できます (「管理対象サーバーの詳細の表示」を参照)。
デバイス管理	XClarity Administrator とは別に特定のサーバーのセキュリティー・モードを表示および構成できます (「管理対象サーバーのセキュリティー設定の構成」および「管理サーバーでの暗号化設定の構成」)。 セカンダリー IP アドレスは、該当する ThinkSystem サーバーでベースボード管理コントローラーにサポートされています (管理対象サーバーの詳細の表示 参照)。
ファームウェア更新	IBM TS4300 テープライブラリのファームウェアを更新できます (「管理対象デバイスでのファームウェアの更新」を参照)。
オペレーティング・システムのデプロイメント	次のオペレーティング・システムを管理対象サーバーにデプロイできます (サポートされているオペレーティング・システムを参照)。 • Microsoft Windows Client 10 21H2、10 22H2、11 22H2 • RedHat Enterprise Linux 9.x • Ubuntu Server 22.04.x

第 1 章　Lenovo XClarity Administrator 概要

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

詳細:
- XClarity Administrator: ソフトウェアと同様に ハードウェアを管理する
- XClarity Administrator: 概要



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

ハードウェア管理

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

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

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

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

詳細:

- XClarity Administrator: 検出
- XClarity Administrator: インベントリー
- XClarity Administrator: リモート制御

ハードウェアの監視

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

ハードウェアの監視について詳しくは、イベントの使用およびアラートの使用を参照してください。

詳細: XClarity Administrator: 監視

構成の管理

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

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

サーバーの構成について詳しくは、構成パターンを使用したサーバーの構成を参照してください。

詳細:
- XClarity Administrator: ベア・メタルからクラスターへ
- XClarity Administrator: 構成パターン

ファームウェアのコンプライアンスと更新

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

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

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

ファームウェアの更新について詳しくは、管理対象デバイスでのファームウェアの更新を参照してください。

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

オペレーティング・システム・デプロイメント

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

オペレーティング・システムのデプロイメントについて詳しくは、ベア・メタル・サーバーへのオペレーティング・システムのインストールを参照してください。

詳細:

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

ユーザーの管理

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

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

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

認証タイプについて詳しくは、認証サーバーの管理を参照してください。

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

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

デバイス認証

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

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

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

  保存された資格情報について詳しくは、保存された資格情報の管理を参照してください。

セキュリティー

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

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

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

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

サービスおよびサポート

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

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

スクリプトによるタスクの自動化

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

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

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

他の管理対象ソフトウェアとの統合

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

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

- Microsoft System Center 向け Lenovo XClarity Integrator
- VMware vCenter 向け Lenovo XClarity Integrator

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

詳細:

-  Microsoft System Center 向け Lenovo XClarity Integrator 概要
-  VMware vCenter 向け Lenovo XClarity Integrator

資料

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

オンライン・ドキュメントは、次の言語で入手できます。
- ドイツ語 (de)
- 英語 (en)
- スペイン語 (es)
- フランス語 (fr)
- イタリア語 (it)
- 日本語 (ja)
- 韓国語 (ko)
- ブラジル・ポルトガル語 (pt_BR)
- ロシア語 (ru)
- タイ語 (th)
- 簡体字中国語 (zh_CN)
- 繁体字中国語 (zh_TW)

次の方法でオンライン・ドキュメントの言語を変更できます。

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

XClarity Administrator へのログイン

サポートされている Web ブラウザーを使用して Lenovo XClarity Administrator Web インターフェースにログインします。

始める前に

以下のサポートされる Web ブラウザーのいずれかを使用していることを確認してください。
- Chrome™ 48.0 以降 (リモート・コンソールには 55.0 以上)
- Firefox® ESR 38.6.0 以降
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 以降 (IOS7 以降および OS X)

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

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

手順

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

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

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

- **コンテナーの場合**: ${ADDRESS} 変数で指定した IPv4 アドレスと次の URL を使用して XClarity Administrator にアクセスします。
  `https://<IPv4_address>/ui/login.html`

  例:
  `https://192.0.2.10/ui/login.html`
- **仮想アプライアンスの場合**:使用する IP アドレスは、環境をどのようにセットアップしているかによって異なります。

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

静的な IPv4 アドレスの使用

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

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

例:

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

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

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

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

例:

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

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

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

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

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

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

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

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

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

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

– **Firefox**:

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

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

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

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

– **Internet Explorer**:

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

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

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

  ```
  PS C:> ipconfig
  Windows IP Configuration

  Ethernet adapter vEthernet (teamVirtualSwitch):

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

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

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

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

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

ステップ 2. 「**言語**」ドロップダウン・リストから、目的の言語を選択します。

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

ステップ 3. 有効なユーザー ID とパスワードを入力し、「**ログイン**」をクリックします。

ユーザー・アカウントで初めてログインしたときは、パスワードの変更を求められます。パスワードは以下の条件を満たす必要があります。

- (1) 1 つ以上の英字が含まれ、英字、数字、および QWERTY キーボードの連続を含めて、2 文字以上の連続が含まれない (「abc」、「123」、「asd」など)。
- (2) 少なくとも 1 つの数字 (0 - 9) が含まれていること。
- (3) 次の文字のうち、少なくとも *2* つが含まれる。
  - 大文字の英字 (A – Z)。
  - 子文字の英字 (a – z)。
  - 特殊文字 ; @ _ ! ' $ & +
- (4) ユーザー名の繰り返しや反転がないこと。
- (5) 2 つの同じ文字が連続していない (「aaa」、「111」、「...」など) こと。

終了後

XClarity Administrator ダッシュボード・ページが表示されます。

注：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、XClarity Administrator にログインを試みると認証エラーが表示されることがあります。この問題を解決するには、最後のバックアップから XClarity Administrator を復元して管理サーバーにアクセスします (Lenovo XClarity Administrator のバックアップを参照)。

XClarity Administrator タイトル・バーのユーザー操作メニュー (

) から、ユーザー・インターフェースの次の操作を実行できます。

- XClarity Administrator の使用方法に関する情報は、「**ヘルプ**」をクリックして組み込みのヘルプ・システムで参照できます。

  XClarity Administrator 資料は、英語版がオンラインで常時更新されています。最新情報と手順は、XClarity Administrator オンライン・ドキュメント を参照してください。
- 「**ライセンス**」をクリックして、XClarity Administrator ライセンスを表示できます。
- 「**バージョン情報**」をクリックして、XClarity Administrator のリリースに関する情報を表示できます。
- 「**言語の変更**」をクリックして、ユーザー・インターフェースの言語を変更できます。
- 「**ログアウト**」をクリックして、現行セッションからログアウトできます。
- 「**アイデアを送信**」または「**フィードバックを送信**」をクリックして、XClarity Administrator についてのアイデアやフィードバックを送信できます。
- 「**フォーラムにアクセス**」をクリックして、Lenovo XClarity Community フォーラム Web サイト で質問をしたり回答を検索したりできます。

ユーザー・インターフェースのヒントと手法

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

ページごとに表示するデータの量の増減

1 ページに表示される行数は、テーブルの右下にあるリンクを使用して変更できます。**10** 行、**25**行、**50** 行、または**すべて**の行を表示できます。

大きなリストのデータの検索

ほとんどのフィールドには最大 128 文字まで入力できます。

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

- 列見出しをクリックすると、テーブルの行をソートできます。

  テーブル列のソート順序を変更した場合、ユーザー・セッションが変わっても維持されます。
- 一部のページにある「**フィルター条件**」アイコンと「**表示**」ドロップダウン・リストを使用し、選択した基準に基づいてデータのサブセットを表示できます。
- このサブセットをさらに絞り込むには、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、使用可能な任意の列にあるデータを検索します。

  過去 10 件の検索から選択するには、「**フィルター**」フィールドにあるドロップダウン・メニューから検索を選択します。ページで最後にアクティブになっている検索は、ユーザー・セッションが変わっても維持されます。

列データの表示

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

テーブルの列の構成

テーブルを構成して、重要な情報を表示することができます。

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

ユーザー・インターフェースの言語の変更

初回ログイン時にユーザー・インターフェースの言語を設定できます。

ログイン後にユーザー・インターフェースの言語を変更する場合は、ユーザー-操作メニュー (

) をクリックし、「**言語の変更**」をクリックします。表示する言語を選択します。

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

ヘルプの入手

XClarity Orchestrator では、複数の方法でユーザー・インターフェースに関するヘルプを取得できます。

- 一部のページでは、「**ヘルプ**」アイコン () を使用して、特定のフィールドまたはステータスに関する追加情報にアクセスできます。アイコンの上にカーソルを置くと、役に立つ情報がポップアップで表示されます。
- ユーザー・インターフェースから特定の操作を実行する方法に関するヘルプを表示するには、ユーザー操作メニュー (

) をクリックし、「**ヘルプ**」をクリックします。

Lenovo XClarity Mobile アプリの使用

Lenovo XClarity Administrator では、Android および iOS デバイス向けのモバイル・アプリが提供されています。Lenovo XClarity Mobile アプリを使用して、物理システムの確実な監視、リアルタイム・ス

テータス・アラートと通知の取得、一般的なシステム・レベルのタスクに対するアクションを行うことができます。このアプリは、有効な USB ポート経由で ThinkSystem サーバーに直接接続し、仮想 LCD 機能を提供できます。

詳細: Lenovo XClarity Mobile アプリ概要

XClarity Mobile アプリを使用して、以下のアクティビティを実行できます。
- ネットワーク設定およびプロパティの構成
- 接続中の各 XClarity Administrator のステータス要約の表示。
- すべての管理対象デバイスのステータス要約の表示。
- シャーシ、ラック・サーバー、およびストレージ・デバイスをグラフィカル・ビュー (マップ) で表示。
- XClarity Administrator で定義されているリソースグループを表示します。
- ラック・スイッチ・ポート情報を表示し、構成されたポート・ステータスを変更します。
- インベントリーおよび各管理対象デバイスの詳細ステータスの監視。
- 監査イベント、ハードウェアおよび管理イベント、アラート、ジョブの監視。
- 管理対象デバイスのロケーション LED のオンまたはオフ。
- 管理対象デバイスの電源オン、電源オフ、再起動、再取り付け。
- 診断データの収集の起動。
- デバイスの保証情報およびステータスを表示します。
- コール・ホーム を使用した自動問題通知のセットアップ
- 開いているサービス・チケットの要約の表示とサービス・チケットの削除
- モバイル・デバイスへのイベントのプッシュ通知 (モバイル・デバイスへのイベントの転送参照)。
- アクティブなユーザーとシステム・リソース使用状況の要約の表示
- このモバイル・アプリについてのフィードバックを Lenovo サポートに送信します。
- モバイル・デバイスを直接 ThinkSystem サーバーに接続して、XClarity Mobile アプリを使用してサーバーを管理します (USB テザリングをサポートするデバイスの場合)。
- モバイル・デバイスが ThinkSystem サーバーに接続したら Lenovo XClarity Controller サービス・データをダウンロードします。

モバイル・デバイスを ThinkSystem サーバーに直接接続して XClarity Mobile アプリを起動し、同じ Web および CLI 資格情報を使用してサーバーのダッシュボード管理コントローラーにログインすることもできます。以下を含む追加情報と操作のメニューを使用できます。

- サービス
  - モバイル・デバイスで使用できるメールなどの手段を使用した要約情報の共有
  - イベントおよび監査ログの消去
  - イベントおよび監査ログのモバイル・デバイスのローカル・ストレージへのダウンロード、またはモバイル・デバイスで使用できる手段を使用したログの送信
  - BMC FFDC サービス・ファイルのモバイル・デバイスのローカル・ストレージへのダウンロード、またはモバイル・デバイスで使用できる手段を使用したファイルの送信
  - 電源、温度、およびシステム使用量の履歴グラフデータを表示します
  - アクティブなアラートおよび重要なデバイス情報の即時の要約を提示する「ワンタッチ」サービス・モードの有効化
- 構成および初期セットアップ
  - 選択した XClarity Administrator を使用した新しいデバイスの管理
  - 初期セットアップでのロケーションや連絡先情報などのサーバー・プロパティの構成
  - IPv4 および IPv6 BMC ネットワーク・インターフェース設定の表示および変更
  - ブート順序および 1 回限りのブート設定の指定
  - フロント・パネル USB ポートの割り当ての変更
  - サーバーのリブート回数と電源オン合計時間の表示
- 電源操作
  - サーバーの電源オンまたはオフ、NMI のトリガー
  - BMC のリセット

ヒント: アプリを開いた後で、更新されたステータス、インベントリー、イベント、ジョブを確認するには、アプリを最新の情報に更新する必要があります。

前提条件

- iOS タブレットは、iPhone の画面解像度でのみサポートされています。Android タブレットは、現在サポートされていません。
- 以下のオペレーティング・システムがサポートされています。
  - Android 7 ～ 11
  - iOS 10 以降

    注：

    - Android 5 は、XClarity Mobile 2.3.0 以前でのみサポートされます。
    - iPhone X/XR/XS デバイスで使用されている顔認識は、サポートされていません。
- ご使用のモバイル・デバイスから XClarity Administrator インスタンスへのネットワーク接続が使用可能であることを確認している。VPN ソリューションを使用する必要がある場合があります。ネットワーク管理者に相談してください。
- 各 XClarity Administrator の CA 証明書をインポートしている。

  重要：XClarity Administrator へのすべての接続が HTTPS を使用している。ただし、接続が信頼できるとみなされデータがモバイル・デバイスに受け渡されるには、まず有効な証明書チェーンが必要です。トラステッド証明書チェーンを作成するには、モバイル・デバイスに XClarity Administrator 自己署名証明機関 (CA) をインポートする必要があります。

  モバイル・デバイスに*各 XClarity Administrator インスタンス*の自己署名 CA 証明書をインポートするには、以下の手順を実行します。

  1. CA 証明書をローカル・システムにダウンロードします。
     a. ローカル・システムの Web ブラウザーを使用して XClarity Administrator インスタンスに接続します。
     b. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。
     c. 「証明書の管理」セクションで「**証明機関**」をクリックします。「証明機関」ページが表示されます。
     d. 「**証明機関ルート証明書のダウンロード**」をクリックします。

        注意：通常、このプロセスを完了するには、「**証明機関ルート証明書の再生成**」をクリックする必要はありません。これを行った場合、正しい手順に従わないと、管理対象デバイスとの通信が中断する場合があります。詳しくは、セキュリティー証明書の使用を参照してください。
     e. 「**der として保存**」または「**pem として保存**」をクリックして、サーバー証明書を DER または PEM ファイルとしてローカル・システムに保存します。PEM 形式はほとんどの場合に使用できます。
  2. アクセス可能なストレージ・リポジトリー (Dropbox™ など)、メール、接続ケーブルを使用したファイル転送などを利用して、CA 証明書ファイルをモバイル・デバイスに転送します。
  3. トラステッド CA 証明書をインポートします。
     - (Android) 通常は、電話のストレージから「**設定**」 ➡ 「**セキュリティー**」 ➡ 「**インストール**」を選択し、ダウンロードした証明書ファイルを選択して実行します。

       重要：正常にインストールした CA 証明書が第三者によって署名されたものではない場合、Android デバイスに「**ネットワークが不明な第三者によって監視される場合があります**」というメッセージが表示されます。CA 証明書はお客様の信頼できる環境で生成されたものであるた

め、このメッセージは安全に無視できます。メッセージを無視する前に、メッセージが XClarity Administrator CA 証明書についてのものであることを確認してください。

– (iOS) モバイル・デバイスでメールを開き、トラステッド CA 証明書をインポートするためにメールのドキュメント・リンクをクリックします。

注意：iOS 10.3 以降の場合は、インポートされた証明書は、デフォルトでは非トラステッドです。証明書を信頼するには、「**設定**」 ➞ 「**全般**」 ➞ 「**情報**」 ➞ 「**証明書信頼設定**」 の順に選択し、証明書の信頼を有効にします。

インストールとセットアップ

1. iTunes App Store (iOS) または Google Play ストア (Android) から XClarity Mobile アプリをダウンロードします。
2. アプリをインストールするには、モバイル・デバイスの指示に従ってください。

   重要：XClarity Mobile アプリを使用するには、画面アクセスをロック解除するモバイル OS レベルのセキュリティー・コードが必要です。まだセットアップしていない場合は、インストール中に設定するように指示されます。
3. 「**設定**」をクリックして自動検出を使用するか IP アドレスとユーザー資格情報を入力することで、複数の XClarity Administrator インスタンスへの接続を追加または編集できます。アプリの PIN コードの設定、イベント・ログおよび監査ログの変更、使用言語の選択もできます。

ThinkSystem サーバーへの直接接続

Lenovo Think System サーバーには、モバイル・デバイスを接続できる前面パネル USB ポートがあります。これは、他の Lenovo サーバーの LCD システム情報表示パネルにあったものと同様の機能を提供します。

サーバーに直接接続して ThinkSystem サーバーを管理するには、以下の手順を実行します。

1. 以下の手順のいずれかを実行して、サーバーの前面パネル USB をホストから BMC に切り替えます。
   a. 管理コントローラー CLI から、`usbfp` コマンドを実行します。
   b. 管理コントローラー Web インターフェースから、「**BMC 構成**」 ➞ 「**ネットワーク**」 ➞ 「**前面パネル USB ポート管理**」の順にクリックします。
   c. 前面パネルの青色の ID ロケーション LED を、ライトが 2 秒に 1 回点滅するまで、3 秒以上押し続けます。
2. 電話の USB ケーブルを ThinkSystem サーバーの前面パネル USB ポートに接続します。
3. モバイル・デバイスで、USB テザリングを有効にします。
   a. iOS の場合は、「**設定**」 ➞ 「**モバイルデータ通信**」 ➞ 「**インターネット共有**」の順にクリックします。
   b. Android の場合は、「**設定**」 ➞ 「**モバイルホットスポットとテザリング**」 ➞ 「**テザリング**」の順にクリックします。
4. モバイル・デバイスで、XClarity Mobile アプリを起動します。
5. 自動検出が無効になっている場合は USB 検出ページで「**検出**」をクリックし、サーバーの管理コントローラーに接続してインベントリー、ヘルス、ファームウェア、ネットワーク構成、最新のアクティブ・イベントのリストなどの情報を収集します。

ヒント:

- データおよび電力をサポートする高品質の USB ケーブルを使用してください。モバイル・デバイスに付属している一部のケーブルは、充電のみを目的としていることに注意してください。

  注：ThinkSystem SD530 に接続するには、高品質マイクロ USB - USB ケーブルまたはアダプターを使用する必要があります。
- サマリー・ステータス・カードの電圧、温度、使用統計の完全セットをレポートするには、USB で接続されたサーバーの電源がオンになっている必要があります。

- USB で接続されたサーバーの前面パネルに外部「青色の識別」LED/ボタンがない場合は、管理コントローラー Web インターフェースまたは CLI を使用して、必要に応じて前面パネル USB ポート管理の選択を変更する必要があります。
- XClarity Mobile アプリから管理コントローラーのネットワーク・インターフェースに対して行われた変更は、管理コントローラーを再起動する必要なく即時有効になります。たとえば、IPv4 インターフェースが静的アドレスから DHCP に変更された場合、インターフェースはただちに DHCP によって割り当てられたアドレスを取得します。
- NewsFeed タブで、「最新のアクティブ・イベント」カードには、最初は管理コントローラーのアクティブ・イベント・タブにリストされているアクティブ・イベントが最大 3 件表示されます。モバイル・アプリでこのカードをタップすると、すべてのアクティブ・イベントが表示されます。これはアクティブおよび解決済みイベントのリストであり、すべてのイベントの完全リストではないことに注意してください。

デモ・モードの使用

設定ページで「**デモ・モード**」を有効にして、ラックおよびシャーシを含む 2 つの XClarity Administrator インスタンスで XClarity Mobile アプリにデモ・データを入力できます。このモードでは、XClarity Administrator インスタンスのステータス要約の表示、デバイスの詳細ステータスおよびインベントリーの表示、イベントおよびアラートの監視を行うことができます。ただし、電源のオンやオフなどの管理操作はサポートされていません。

注：

- デモ・モードは、実際の XClarity Administrator インスタンスに接続していない場合にのみ、有効にできます。
- デモ・モードが有効になっている間は、実際の XClarity Administrator インスタンスへの接続を追加することはできません。

検索

「**検索**」フィールドを使用して、特定の名前またはステータス (重大、警告、正常) を指定して管理対象デバイスを表示できます。たとえば「crit」で検索すると、クリティカル状況の管理対象デバイスおよび名前に「crit」を含む管理対象エンドポイントのみが表示されます。

問題の解決

インストールに関する問題:

- Android モバイル・アプリでは、セキュリティーの強化のために安全鍵により「署名」されています。安全鍵のサイズは、新しいリリースでは増加しました。署名済みのアプリが以前のアプリ署名と一致しないため、Android のインストール セキュリ ティー・プロセスにより自動更新は中止されます。

  モバイル・アプリを更新するには、モバイル・アプリの現在のバージョンをアンインストールし、アプリ ストアから Android アプリの最新バージョンをダウンロードして、アプリを再インストールします。ほとんどの Android デバイスでは、メニュー項目「**設定**」 ➔ 「**プログラム**」 ➔ 「**アプリケーション・マネージャー**」でアプリをアンインストールできます。

接続の問題:

- iOS 14、14.0.1、および 14.0.2 の USB テザリング機能が正常に動作していないため、これらの iOS バージョンでは Lenovo XClarity Mobile アプリ・テザリング機能を使用することはできません。これは、データセンターの USB で接続されたハンドヘルド管理にのみ影響します。携帯電話および Wi-Fi 通信をサポートするモバイル・デバイスを使用したリモート管理は影響を受けず、管理対象デバイスでの XClarity Administrator データの接続と収集、および管理操作の実行に使用できます。

  USB 接続されたハンドヘルド管理機能が必要な場合は、iOS 14 にアップグレードしないでください。

  この通知は、Apple が iOS 14 の問題を解決したときに更新されます。

- XClarity Mobile には、モバイル・デバイスから XClarity Administrator インスタンスへのネットワーク接続が必要です。VPN ソリューションを使用する必要がある場合があります。ネットワーク管理者に相談してください。
- モバイル・デバイスから各 XClarity Administrator インスタンスへの接続にトラステッド証明書チェーンを要求される。モバイル・デバイスに信頼できる CA 証明書をダウンロードしてインストールする方法については、オンライン・ドキュメントを参照してください。

  正常にインストールした CA 証明書が第三者によって署名されたものではない場合、**ネットワークが不明な第三者によって監視される場合があります**というメッセージが表示されます。CA 証明書はお客様の信頼できる環境で生成されたものであるため、このメッセージは安全に無視できます。メッセージを無視する前に、メッセージが XClarity Administrator CA 証明書についてのものであることを確認してください。
- モバイル・デバイスを仮想プライベート・ネットワーク (VPN) からローカル・ネットワークに切り替えたり、その逆を行った場合、**セキュア・ゲートウェイによって接続が拒否されました。同じセキュア・ゲートウェイまたは別のセキュア・ゲートウェイに新しく接続する必要がある場合は、再認証が必要です。**というメッセージが表示される場合があります。アプリの使用を続ける場合は、Lenovo XClarity Mobile にログインしてください。

セキュリティーの問題:

- PIN コードを忘れた場合は、XClarity Mobile アプリをアンインストールしてから、再インストールします。その後、すべての接続を再確立します。
- Android デバイスで資格情報をクリアすると、暗号鍵が消去されます。すべての接続を再確立する必要があります。

イベントの問題:

- デフォルトでは、イベント・ログには 24 時間以内に受信したハードウェアと管理イベントが表示され、監査ログには直近 2 時間以内に受信した監査イベントが表示されます。選択した期間内に受信したイベントがない場合は、イベント・ログと監査ログは XClarity Mobile の「監視」ページに表示されません。
- イベントをメール・アカウントに送信するように XClarity Administrator でイベント転送をセットアップしている場合、Android デバイスではメール内のリンクが機能しない場合があります。ご使用の Android のバージョンおよびメール・アプリがハイパーリンクをサポートしていることを確認してください。ハイパーリンクがサポートされていない場合は、別のメール・アプリを使用してください。

ヘルプ・システムに関する問題:

- 一部のデバイスで、ヘルプ・システムが画面のサイズに合わせて正しくスケールされないヘルプ・システムのコントロールを使用してページを最大化してから最小化します。

第 2 章 Lenovo XClarity Administrator の管理

ユーザーの追加やジョブの表示など、いくつかの管理タスクは Lenovo XClarity Administrator から実行できます。

認証と許可の管理

Lenovo XClarity Administrator には、ユーザーの資格情報を確認し、リソースとタスクへのアクセスを制御するためのセキュリティー・メカニズムが用意されています。

認証サーバーの管理

デフォルトでは、Lenovo XClarity Administrator はローカルのライトウェイト・ディレクトリー・アクセス・プロトコル (LDAP) サーバーを使用してユーザー資格情報を認証します。

このタスクについて

サポートされる認証サーバー

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

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

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

  ThinkSystem または ThinkAgile サーバーのユーザー・アカウントが CyberArk にオンボードされている場合、サーバーを管理用に最初に設定しているときに XClarity Administrator CyberArk からサーバーにログインするための資格情報を取得するように選択できます。CyberArk から資格情報を取得する前に、XClarity Administrator で CyberArk パスを定義し、クライアント証明書を介して TLS 相互認証を使用して、CyberArk と XClarity Administrator の間で相互信頼を確立する必要があります。
- **外部 SAML ID プロバイダー**現在、 Microsoft Active Directory Federation Services (AD FS) のみサポートされます。ユーザー名とパスワードを入力するほか、PIN コードの要求やスマート・カードやクライアント証明書の読み込みによる追加セキュリティーを有効にするマルチファクター認証をセットアップできます。SAML ID プロバイダー が使用されている場合、ローカル認証サーバーは無効になりません。外部認証が使用できない場合に、PowerShell および REST API 認証、およびリカバリーのために管理対象シャーシまたはサーバーに直接ログインするには (そのデバイスで Encapsulation が有効になっている場合を除く)、ローカル・ユーザー・アカウントが必要です。

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

デバイス認証

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

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

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

  注：

  – RackSwitch デバイスは、認証用にのみ保存される資格情報をサポートします。XClarity Administrator ユーザー資格情報はサポートされていません。

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

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

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

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

  – XClarity Administrator 認証サーバーとしてローカルまたは外部 LDAP サーバーを使用している場合は、その認証サーバーで定義されているユーザー・アカウントが XClarity Administrator ドメイン内の XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されます。ローカルの CMM および管理コントローラー・ユーザー・アカウントは無効になります。

  – XClarity Administrator 認証サーバーとして SAML 2.0 ID プロバイダーを使用する場合、SAML アカウントは、管理対象デバイスにアクセスできなくなります。ただし、SAML ID プロバイダーと LDAP サーバーを同時に使用する場合で、ID プロバイダーが LDAP サーバーにあるアカウントを使用する場合、LDAP ユーザー・アカウントを使用して管理対象デバイスにログインできます。また、SAML 2.0 が提供するより高度な認証方法 (マルチファクター認証およびシングル・サインオンなど) を使用して XClarity Administrator にログインすることもできます。

  – シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます (XClarity Administratorオンライン・ドキュメントの「を参照)

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

  – ThinkSystem SR635 および SR655 サーバーで管理対象認証が有効になっている場合:

  - ベースボード管理コントローラー・ファームウェアは、最大 5 つの LDAP ユーザー・ロールをサポートします。XClarity Administrator は、管理中に次の LDAP ユーザー・ロールをサーバーに追加します: **lxc-supervisor**、**lxc-sysmgr**、 **lxc-admin**、**lxc-fw-admin** および **lxc-os-admin**。

    ThinkSystem SR635 および SR655 サーバーと通信するには、指定された少なくとも 1 つの LDAP ユーザー・ロールにユーザーが割り当てられている必要があります。
  - 管理コントローラーのファームウェアは、サーバーのローカル・ユーザーと同じユーザー名の LDAP ユーザーをサポートしていません。
- ThinkServer サーバーおよび System x M4 サーバーの場合は、XClarity Administrator 認証サーバーは使用しません。その代わり、デバイスで接頭辞「LXCA_」の後にランダムな文字列が続く IPMI アカウントが作成されます。(既存の IPMI ローカル・ユーザー・アカウントは無効になります。)ThinkServer サーバーを管理解除する場合は、「LXCA_」ユーザー・アカウントが無効になり接頭辞「LXCA_」が接頭辞「DISABLED_」に置き換えられます。ThinkServer サーバーが別のインスタンスによって管理されているかどうかを判別するために、XClarity Administrator は接頭辞「LXCA_」がついた IPMI アカウントを確認します。管理対象 ThinkServer サーバーの管理を強制することを選択した場合、そのデバイスで「LXCA_」がついたすべての IPMI アカウントが無効になり名前を変更されます。不要になった IPMI アカウントを手動で消去することを検討してください。

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

  注：デバイスに対して管理対象認証が有効になっている場合、XClarity Administrator を使用してそのデバイスの保管された資格情報を編集することはできません。
  - 手動で入力した認証情報を使用してデバイスを管理するたびに、以前の管理プロセス中にそのデバイス用に別の保存済み認証情報が作成されていても、そのデバイス用に新しい保存済み認証情報が作成されます。
  - デバイスを管理解除しても、XClarity Administrator は、管理プロセス中にそのデバイス用に自動的に作成され保管されている資格情報を削除しません。

リカバリー・アカウント

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

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

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

デバイス管理のリカバリーについては、218 ページの 「管理サーバーの障害発生後の CMM による管理のリカバリー」および 268 ページの 「管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー」を参照してください。

外部 LDAP 認証サーバーのセットアップ

管理ノードのローカル Lenovo XClarity Administrator 認証サーバーの代わりに外部 LDAP 認証サーバーを使用することができます。

始める前に

外部認証サーバーをセットアップする前に XClarity Administrator の初期セットアップを完了する必要があります。

次の外部認証サーバーがサポートされています:

- OpenLDAP
- Microsoft Active Directory。管理ネットワーク、データ・ネットワーク、またはその両方に接続している外部の Microsoft Windows サーバーに存在している必要があります。

外部認証サーバーに必要なすべてのポートがネットワークおよびファイアウォールで開いていることを確認します。ポート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。

外部認証サーバーで定義されているグループに合わせて、ローカル認証サーバーで役割グループを作成または名前変更する必要があります。

ローカル認証サーバーに **lxc-recovery** 権限を持つユーザーがいることを確認してください。このローカル・ユーザー・アカウントを使用して、外部 LDAP サーバーに通信エラーが発生した場合に XClarity Administrator に直接認証できます。

注：XClarity Administrator で外部認証サーバーを使用するように構成している場合、XClarity Administrator Web インターフェースの「ユーザー管理」ページは無効になります。

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

XClarity Administrator は、接続性チェックを 5 分おきに実行し、構成された外部 LDAP サーバーへの接続を維持します。多くの LDAP サーバーが存在する環境では、この接続チェック時に CPU の使用率が高くなる可能性があります。パフォーマンスを最大限に高めるには、ドメイン内のほとんどまたはすべての LDAP サーバーが到達可能であることを確認するか、認証サーバー選択方法を「**事前構成済みのサーバーを使用する**」に設定して到達可能な既知の LDAP サーバーのみ指定します。

手順

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

ステップ 1. Microsoft Active Directory または OpenLDAP のユーザー認証方式を設定します。

非セキュア認証を使用する場合は、追加の構成は必要ありません。Windows Active Directory または OpenLDAP ドメイン・コントローラーは、デフォルトで非セキュア LDAP 認証を使用します。

セキュア LDAP 認証を使用する場合は、セキュア LDAP 認証を許可するようにドメイン・コントローラーを設定する必要があります。Active Directory でセキュア LDAP 認証を構成する設定について詳細は、Microsoft TechNet Web サイトの 「LDAP over SSL (LDAPS) 証明書」の記事を参照してください。

Active Directory ドメイン・コントローラーがセキュア LDAP 認証を使用するように構成されていることを確認するには、以下の手順を実行します。

- ドメイン・コントローラーの「イベント ビューアー」ウィンドウで、「**現在、Secure Sockets Layer (SSL) で LDAP が利用できます**」イベントを探します。
- Windows の `ldp.exe` ツールを使用して、ドメイン・コントローラーとのセキュア LDAP 接続をテストします。

ステップ 2. Active Directory または OpenLDAP サーバー証明書に署名した証明機関の Active Directory サーバー証明書またはルート証明書をインポートします。

a. 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。

b. 「証明書の管理」セクションで「**トラステッド証明書**」をクリックします。

c. 「**作成**」アイコン ( ) をクリックして、証明書を追加します。

d. ファイルを参照するか、PEM 形式の証明書のテキストを貼り付けます。

e. 「**作成**」をクリックします。

ステップ 3. XClarity Administrator LDAP クライアントを構成します。

a. XClarity Administrator メニュー・バーで、**管理** ➡ 「**セキュリティー**」をクリックします。

b. 「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。

c. 以下の基準に基づいてダイアログで設定を行います。

1. 次のいずれかのユーザー認証方式を選択してください。

- **ローカル・ユーザーのログオンを許可**。認証はローカル認証を使用して実行されます。このオプションを選択すると、すべてのユーザー・アカウントが管理ノードのローカル認証サーバーに存在します。
- **LDAP ユーザーのログオンを許可**。認証は外部 LDAP サーバーで実行されます。この方式では、ユーザー・アカウントのリモート管理が有効になります。このオプションが選択されている場合、すべてのユーザー・アカウントがリモートの外部 LDAP サーバーに存在します。
- **ローカル・ユーザーを許可した後、LDAP ユーザーを許可**。最初にローカル認証サーバーで認証を実行します。失敗した場合は、外部 LDAP サーバーで認証を実行します。
- **LDAP ユーザーを許可した後、ローカル・ユーザーを許可**。最初に外部 LDAP サーバーで認証を実行します。失敗した場合、ローカル認証サーバーで認証を実行します。

2. セキュア LDAP を有効にするか無効にするかを選択します。
   - **セキュア LDAP を有効にする**。XClarity Administrator は、LDAPS プロトコルを使用して、外部認証サーバーに安全に接続します。このオプションを選択する場合は、セキュア LDAP のサポートを有効にするために、トラステッド証明書を構成する必要もあります。
   - **セキュア LDAP を無効にする**。XClarity Administrator は、セキュアでないプロトコルを使用して外部認証サーバーに接続します。この設定を選択した場合、ハードウェアがセキュリティーに対する攻撃を受けやすくなることがあります。
3. 次のいずれかのサーバー選択方法を選択します。
   - **事前構成済みのサーバーを使用する**。XClarity Administrator は、指定された IP アドレスとポートを使用して外部認証サーバーを検出します。

     このオプションを選択する場合は、最大 4 つの事前構成済みサーバーの IP アドレスとポートを指定します。LDAP クライアントは、最初のサーバー・アドレスを使用して認証を試行します。認証に失敗した場合、LDAP クライアントは次のサーバー IP アドレスを使用して認証を試行します。

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

     ポート番号が 3268 または 3269 に設定されている項目は、グローバル・カタログの項目と見なされます。LDAP クライアントは、構成されている最初のサーバー IP アドレスのドメイン・コントローラーを使用して認証を試みます。これに失敗した場合、LDAP クライアントは、次のサーバー IP アドレスのドメイン・コントローラーを使用して認証を試みます。

     重要：グローバル・カタログが指定されている場合でも、ドメイン・コントローラーを少なくとも 1 つ指定する必要があります。グローバル・カタログだけを指定した場合、正常に指定されたように見えますが、有効な構成ではありません。

     暗号化モードを NIST-800-131A に設定すると、XClarity Administrator で LDAP サーバーにより LDAP クライアントとのトランスポート層セキュリティー (TLS) バージョン 1.2 接続を確立できない場合、XClarity Administratorでセキュア・ポートを使用して (たとえば、デフォルト・ポートの 636 で LDAPS を使用して) 外部 LDAP サーバーに接続できないことがあります。
   - **LDAP サーバーの検索に DNS を使用する**。XClarity Administrator は、指定されたドメイン名またはフォレスト名を使用して動的に外部認証サーバーを検出します。ドメイン名とフォレスト名を使用してドメイン・コントローラーのリストが取得され、フォレスト名を使用してグローバル・カタログ・サーバーのリストが取得されます。

注意：DNS を使用して LDAP サーバーを検索するときは、外部認証サーバーでの認証で使用されるユーザー・アカウントが指定されたドメイン・コントローラーでホストされていることを確認します。ユーザー・アカウントが子ドメイン・コントローラーでホストされている場合は、子ドメイン・コントローラーをサーバー要求リストを含めます。

4. 以下のいずれかのバインディング方式を選択してください。

   - **構成済み資格情報**。このバインディング方式を使用すると、クライアント名とパスワードを使用して XClarity Administrator を外部認証サーバーにバインドします。このバインドに失敗すると認証プロセスも失敗します

     クライアント名は、LDAP サーバーでサポートされている、識別名、AMAccountName、NetBIOS 名、UserPrincipalName を含む任意の名前にできます。クライアント名は、少なくとも読み取り専用特権を持つ、ドメイン内のユーザー・アカウントである必要があります。例:

     ```
     cn=username,cn=users,dc=example,dc=com
     domain\username
     username@domain.com
     username
     ```

     注意：外部認証サーバーのクライアント・パスワードを変更した場合は、必ず XClarity Administrator の新規パスワードも更新してください。詳しくは、XClarity Administrator オンライン・ドキュメントのXClarity Administrator にログインできないを参照してください。

   - **ログイン資格情報**。このバインディング方式を使用すると、Active Directory または OpenLDAP のユーザー名とパスワードを使用して XClarity Administrator を外部認証サーバーにバインドします。

     指定されたユーザー ID とパスワードは、認証サーバーへの接続テストにのみ使用されます。成功すると、LDAP クライアントの設定は保存されますが、指定されたテスト・ログイン資格情報は保存されません。その後のバインドは XClarity Administrator にログインするために使用したユーザー名とパスワードを使用します。

     注：

     – 完全修飾ユーザー ID (たとえば、`administrator@domain.com` や `DOMAIN\admin`) を使用して XClarity Administrator にログインする必要があります。
     – バインディング方式では、完全修飾テスト・クライアント名を使用する必要があります。

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

5. 「**ルート DN**」フィールドにはルート識別名を指定しないことをお勧めします。これは複数のドメインがある環境で特にお勧めします。このフィールドを空白にすると、XClarity Administrator が外部認証サーバーで名前付けコンテキストを照会します。DNS を使用して外部認証サーバーを検出する場合、または複数のサーバーを指定する場合 (例: `dc=example,dc=com`) は、必要に応じて LDAP ディレクトリー・ツリーの最上位項目を指定できます。この場合、指定したルート識別名を検索ベースとして使用して検索が開始されます。
6. ユーザー名の検索に使用する属性を指定します。

   バインディング方式が「**構成済み資格情報**」に設定されている場合、LDAP サーバーへの初回バインドの直後に、ユーザーの DN、ログイン許可、およびグループ・メンバーシップなど、ユーザーに関する固有の情報を取得する検索要求が行われます。こ

の検索要求では、そのサーバー上でユーザー ID を表す属性名を指定する必要があります。この属性名は、このフィールドで構成されます。このフィールドをブランクのまま残した場合、デフォルトは「**cn**」です。

7. ユーザーが属するグループの識別に使用される属性名を指定します。このフィールドがブランクのまま残されると、フィルターの属性名はデフォルトの **memberOf** になります。
8. LDAP サーバーにより構成されるグループ名の識別に使用される属性名を指定します。このフィールドをブランクのまま残した場合、デフォルトは「**uid**」です。

d. 「**適用**」をクリックします。

XClarity Administrator は、構成をテストして、共通のエラーを検出しようとします。テストが失敗すると、エラー・メッセージが表示されます。このメッセージにはエラーのソースが示されています。テストに成功し指定されたサーバーへの接続が正常に完了しても、以下の場合ユーザー認証に失敗することがあります。

- **lxc-recovery** 権限を持つローカル・ユーザーが存在しない。
- ルート識別名が正しくない。
- ユーザーが、外部認証サーバー内で XClarity Administrator 認証サーバーの役割グループの名前と一致する少なくとも 1 つのグループに属していない。XClarity Administrator は、ルート DN が適切かどうかを検出できません。ただし、ユーザーが少なくとも 1 つのグループのメンバーであるかどうかを検出することはできます。少なくとも 1 つのグループに属していないユーザーが XClarity Administrator にログインしようとすると、エラー・メッセージが表示されます。外部認証サーバーに関する問題のトラブルシューティングについて詳しくは、XClarity Administrator オンライン・ドキュメントの接続の問題を参照してください。

ステップ 4. XClarity Administrator にアクセスできる外部ユーザー・アカウントを作成します。

a. 外部認証サーバーで、ユーザー・アカウントを作成します。この手順については、Active Directory または OpenLDAPのドキュメントを参照してください。
b. 定義済みの許可されている役割グループの名前を使用して、Active Directory または OpenLDAP のグローバル・グループを作成します。このグループは、LDAP クライアントで定義されているルート識別名のコンテキストに存在する必要があります。
c. 以前に作成したセキュリティー・グループのメンバーとして先ほどの Active Directory または OpenLDAP ユーザーを追加します。
d. Active Directory または OpenLDAP ユーザー名を使用して XClarity Administrator にログオンします。
e. **オプション**: 追加のグループを定義および作成します。「ユーザーとグループ」ページでそれらのグループを許可し、役割を割り当てることができます。
f. セキュア LDAP が有効になっている場合は、信頼できる証明書を外部 LDAP サーバーにインポートします (カスタマイズされた外部署名済みサーバー証明書のインストールを参照)。

結果

XClarity Administrator によって LDAP サーバー接続が検証されます。検証に成功した場合は、XClarity Administrator、CMM、および管理コントローラーにログインするときに、ユーザー認証が外部認証サーバーで行われます。

検証に失敗した場合は、認証モードが自動的に「**ローカル・ユーザーのログオンを許可**」に戻されて、失敗の原因を説明するメッセージが表示されます。

注：XClarity Administrator で正しい役割グループが構成されていて、Active Directory 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必要があります。そうでないと、ユーザー認証は失敗します。

外部 SAML ID プロバイダー のセットアップ

Lenovo XClarity Administratorの認証および許可の実行に、セキュリティー表明の言語マークアップ (SAML) 2.0 ID プロバイダー を使用するように選択できます。

始める前に

ID プロバイダー をセットアップする前に XClarity Administrator の初期セットアップを完了する必要があります。

ID プロバイダー は、管理ネットワーク、データネットワークのいずれかまたは両方に接続可能な Microsoft Active Directory Federated Service (AD FS) でなければなりません。Web ブラウザーを通じて認証が行われるため、Web ブラウザーから XClarity Administrator および SAML サーバーにアクセスできる必要があります。

次の URL を使用して IDP メタデータをダウンロードできます: URL: `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`。
ここで、*<ADFS_IP_Address>* は、AD FS の IP アドレスです (例: https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml)。

外部認証サーバーで定義されているグループに合わせて、ロケーション認証サーバーで役割グループを作成または名前変更する必要があります。

SAML ID プロバイダー をセットアップするには、**lxc_admin** または **lxc_supervisor** 役割グループのメンバーであるユーザーとしてログインする必要があります。

このタスクについて

XClarity Administrator はセキュリティー表明の言語マークアップ 2.0 ID プロバイダー を使用したユーザー認証および許可をサポートしています。ユーザー名とパスワードの入力に加えて、ID プロバイダー をセットアップして、PIN コードの入力、スマート・カードの読み込みおよびクライアント証明書を使用した認証など、ユーザーの身元を検証する追加条件を要求できます。

XClarity Administrator が ID プロバイダー を使用するようにセットアップされている場合、XClarity Administrator Web インターフェースからの対話式ログイン要求は認証のために ID プロバイダー にリダイレクトされます。ユーザーが認証されると、Web ブラウザーは XClarity Administrator にリダイレクトされて戻ります。

注：ID プロバイダー が有効にされている場合、ID プロバイダー をバイパスして、Web ブラウザーで XClarity Administrator ログイン・ページ (たとえば、`https://<ip_address>/ui/login.htm`) を開き、ローカルまたは外部 LDAP 認証サーバーを使用して XClarity Administrator にログインできます。

XClarity Administrator で ID プロバイダー プロファイルを使用するように構成している場合、XClarity Administrator Web インターフェースの「ユーザー管理」ページは無効になりません。管理対象シャーシまたはサーバーへの直接ログイン (そのデバイスで Encapsulation が有効になっている場合を除く)、および PowerShell および REST API 認証には、ローカル・ユーザー・アカウントが必要です。

手順

外部 SAML ID プロバイダー (AD FS) をセットアップするには、以下の手順を実行します。

ステップ 1. ID プロバイダー が利用できなくなった場合に XClarity Administrator へのログインに使用できるリカバリー・ユーザー・アカウントを作成します (ユーザー・アカウントの管理参照)。

ステップ 2. ID プロバイダー (IDP) メタデータを ID プロバイダー から取得し、XClarity Administrator ホストにファイルを保存します。

ステップ 3. XClarity Administrator SAML クライアントを構成します。

a. XClarity Administrator メニュー・バーで、**管理 → 「セキュリティー」**をクリックします。

b. 「ユーザーとグループ」セクションの「**SAML 設定**」をクリックして、「SAML 設定」ダイアログを表示します。

c. 「SAML 設定」ページのフィールドに入力します。

   1. エンティティーの ID が XClarity Administrator 管理サーバーの IP アドレスと一致していることを確認します。

2. 生成したメタデータにデジタル署名する必要があるかどうかを選択します。
3. 認証要求に署名する必要があるかどうかを選択します。
4. 認証レスポンスに署名する必要があるかどうかを選択します。
5. リモート ID プロバイダー に送信される Artifact Resolution 要求に署名する必要があるかどうかを選択します。
6. ID プロバイダー によって生成され 27 ページの ステップ 23 の手順で取得された SAML ID プロバイダー (IDP) メタデータを「**IDP メタデータ**」フィールドに貼り付けます。

d. 「**適用**」をクリックして変更を適評し、「SP メタデータ」フィールドのテキストを更新します。

注意：この時点では、「**SAML を有効にする**」を選択*しないでください*。SAML は後の手順で XClarity Administrator を再起動するために有効にします。

e. 「**SP メタデータ**」フィールドのデータをファイルにコピー・アンド・ペーストし、ファイルを拡張子 .XML (たとえば、sp_metadata.xml) で保存します。このファイルを AD FS ホストにコピーします。

ステップ 4. AD FS を構成します。

a. AD FS 管理ツールを開きます。
b. 「**ADFS**」 ➡ 「**証明書利用者の信頼**」をクリックします。
c. 「**証明書利用者の信頼**」を右クリックして、「**証明書利用者の信頼を追加**」をクリックしウィザードを表示します。
d. 「**スタート**」をクリックします。
e. 「データ・ソースの選択」ページで、「**証明書利用者のデータをファイルから追加**」を選択し、次に手順 3e で保存した SP メタデータ・ファイルを選択します。
f. ディスプレイ名を入力します。
g. すべてのページで「**次へ**」をクリックしてデフォルト値を選択します。
h. 「**完了**」をクリックして「要求規則」ページを表示します。
i. 「**LDAP の属性を要求として送信**」はデフォルトのままにして、「**次へ**」をクリックします。
j. 要求規則の名前を入力します。
k. 属性ストアに「**Active Directory**」を選択します。
l. マッピングを追加します。左側で「**SAM-Account-Name**」を選択し、右側で出力要求タイプに「**名前 ID**」を選択します。
m. 別のマッピングを追加します。左側で「**Token-Groups-Unqualified Names**」を選択し、右側で出力要求タイプに「**グループ**」を選択します。
n. 「**OK**」をクリックします。
o. 作成した信頼を「**証明書利用者の信頼**」リストで見つけます。
p. 信頼を右クリックして、「**プロパティの選択**」をクリックします。信頼の「プロパティ」ダイアログが表示されます。
q. 「**詳細**」タブをクリックして、セキュア・ハッシュ・アルゴリズムとして `SHA-1` を選択します。

ステップ 5. AD FS からのサーバー証明書を保存します。

a. 「**AD FS コンソール**」 ➡ 「**サービス**」 ➡ 「**証明書**」をクリックします。
b. トークン署名で「**証明書**」を選択します。
c. 証明書を右クリックし、「**証明書の表示**」をクリックします。
d. 「**詳細**」タブをクリックします。

e. 「**ファイルにコピー**」をクリックし、証明書を DER encoded binary X.509 (.CER) ファイルとして保存します。

f. サーバー証明書 .CER ファイルを XClarity Administrator ホストにコピーします。

ステップ 6. AD FS トラステッド証明書を XClarity Administrator Web インターフェースにインポートします。

a. 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。

b. 「証明書の管理」セクションで「**トラステッド証明書**」をクリックします。

c. 「**作成**」アイコン ( ) をクリックして、証明書を追加します。

d. 前の手順で保存したサーバー証明書 .CER ファイルを選択します。

e. 「**作成**」をクリックします。

ステップ 7. 「ユーザーとグループ」セクションの「**SAML 設定**」をクリックして、「SAML 設定」ダイアログを表示します。

ステップ 8. 外部 ID プロバイダー を使用したユーザー・アカウントの管理を有効にするには、「**SAML を有効にする**」を選択します。このオプションが選択されている場合、すべてのユーザー・アカウントがリモートで外部 ID プロバイダー に存在します。

ステップ 9. 「**適用**」をクリックして変更を適用し、管理サーバーを再起動してください。

ステップ 10. XClarity Administrator の再起動には数分間お待ち下さい。

注意：このプロセス中に仮想アプライアンスを手動で再起動しないでください。

ステップ 11. Web ブラウザーを閉じて開き直します。

ステップ 12. ID プロバイダー から XClarity Administrator Web インターフェースにログインします。

結果

XClarity Administrator は、構成をテストして、共通のエラーを検出しようとします。テストが失敗すると、エラー・メッセージが表示されます。このメッセージにはエラーのソースが示されています。

XClarity Administrator によって ID プロバイダー の接続が検証されます。検証に成功した場合は、XClarity Administrator にログインするときに、ユーザー認証が ID プロバイダー サーバーで行われます。

外部 ID 管理システムの設定

*ID 管理システム*は、オプションでXClarity Administratorと XClarity Controller の資格情報を格納するためにLenovo XClarity Administratorで使用できる、外部パスワード保管庫です。ID 管理システムがXClarity Administratorに追加されると、XClarity Administratorは認証サーバーではなく、ID 管理システムからパスワードを取得します。

このタスクについて

XClarity Administratorは、次の ID 管理システムをサポートしています。

- CyberArk

CyberArk ID 管理システムの設定

CyberArk は、オプションで XClarity Administrator および Lenovo XClarity Controller の資格情報を格納するために Lenovo XClarity Administrator で使用できる、外部パスワード保管庫です。アカウントのパスワードが CyberArk に保存されると、パスワードは CyberArk によって管理されます。

このタスクについて

XClarity Administrator を使用すると、サード・パーティーのサービスである CyberArk によって提供される ID 管理システムで XCC パスワードを保管できます。Lenovo は、CyberArk サービスに対して一切責任を負わないものとします。また、CyberArk との直接的関係についてはお客様の責任となります。

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

手順

CyberArk を使用するためにXClarity Administratorを構成するには、以下の手順を完了してください。

ステップ 1. CyberArk を設定します。

1. 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。
2. 「ID 管理」セクションの下にある「**CyberArk**」をクリックします。
3. ツールバーの「**CyberArk サーバーの詳細を編集**」をクリックします。
4. CyberArk のホスト名または IP アドレスとポート番号を指定します。
5. 「**適用**」をクリックします。

ステップ 2. XClarity Administrator相互認証証明書を CyberArk にインポートします。

1. 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。
2. 「証明書の管理」セクションにある「**サーバー証明書**」をクリックします。
3. 「**クライアント証明書**」タブをクリックします。
4. サーバー・タイプとして「**CyberArk**」を選択します。
5. 「**証明書の再生成**」をクリックして、CyberArk の新しい TLS 相互認証証明書を生成します。

   注意：XClarity Administrator と CyberArk との間で接続が確立された後に、CyberArk の TLS 相互認証証明書を再生成する場合、新しい証明書を CyberArk にインポートするまで接続は失われます。
6. 「**証明書のダウンロード**」をクリックし、「**der として保存**」または「**pem として保存**」をクリックして、証明書をファイルとしてローカル・システムに保存します。
7. ダウンロードした証明書を CyberArk にインポートします。

ステップ 3. CyberArk ルート CA 証明書をXClarity Administratorにインポートします。

1. CyberArk からルート CA 証明書をダウンロードします。
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. 「証明書の管理」セクションで「**トラステッド証明書**」をクリックします。
4. 「**作成**」アイコン ( ) をクリックして、証明書を追加します。
5. ファイルを参照するか、PEM 形式の証明書のテキストを貼り付けます。
6. 「**作成**」をクリックします。

ステップ 4. CyberArk でオンボードのユーザー・アカウントの場所を識別するパスを追加します。

1. 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。
2. 「ID 管理」セクションの下にある「**CyberArk**」をクリックします。

3. 「**パス**」タブをクリックします。
4. 「**作成**」アイコン ( ) をクリックして、「CyberArk パスの作成」ダイアログを表示します。

5. オプションで、CyberArk でのユーザー・アカウントの保存場所である、アプリケーション ID、セーフ、およびフォルダーを指定します。

   アプリケーション ID とセーフ、オプションでフォルダーを指定する場合、XClarity Administrator は、指定した場所でユーザー アカウントの検索を試行します。

   アプリケーション ID とセーフ以外のフィールドの組み合わせを指定する場合 (例: アプリケーション ID のみ、セーフとフォルダーのみ、またはアプリケーション ID とフォルダーのみを指定する場合)、XClarity Administrator は指定された値を使用してパスをフィルタリングします。
6. 「**適用**」をクリックします。

終了後

- 「**編集**」アイコン ( ) をクリックして、選択した CyberArk パスを変更します。
- 「**削除**」アイコン ( ) をクリックして、選択した CyberArk パスを削除します。

Lenovo XClarity Administrator によって使用される認証方式の種類の確認

現在使用されている認証方式のタイプを、「セキュリティー」ページの「**LDAP クライアント**」および「**SAML 設定**」タブから確認できます。

このタスクについて

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

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

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

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

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

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

手順

管理ソフトウェアによって使用されている認証サーバーの種類を確認するには、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 → 「セキュリティー」**をクリックします。

ステップ 2. 「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。

選択されているユーザー認証方式を確認します。

- **ローカル・ユーザーのログオンを許可**。認証はローカル認証を使用して実行されます。このオプションを選択すると、すべてのユーザー・アカウントが管理ノードのローカル認証サーバーに存在します。
- **LDAP ユーザーのログオンを許可**。認証は外部 LDAP サーバーで実行されます。この方式では、ユーザー・アカウントのリモート管理が有効になります。このオプションが選択されている場合、すべてのユーザー・アカウントがリモートの外部 LDAP サーバーに存在します。
- **ローカル・ユーザーを許可した後、LDAP ユーザーを許可**。最初にローカル認証サーバーで認証を実行します。失敗した場合は、外部 LDAP サーバーで認証を実行します。
- **LDAP ユーザーを許可した後、ローカル・ユーザーを許可**。最初に外部 LDAP サーバーで認証を実行します。失敗した場合、ローカル認証サーバーで認証を実行します。

ステップ 3. 「ユーザーとグループ」セクションの「**SAML 設定**」をクリックして、「SAML 設定」ページを表示します。

「**SAML を有効にする**」が選択されている場合は、ID プロバイダー が使用されています。

外部 LDAP サーバーの障害後の Lenovo XClarity Administrator へのアクセス

外部 LDAP 認証サーバーを使用しているときに、そのサーバーで障害が発生したかサーバーを利用できない場合は、以下の手順に従って、管理ノードのローカル認証サーバーを使用して Lenovo XClarity Administrator Web インターフェースへのアクセスを回復します。

手順

LDAP クライアントの設定を変更するには、以下の手順を実行します。

ステップ 1. **lxc-recovery** 権限を持つユーザー・アカウントを使用して XClarity Administrator Web インターフェースにログインします。クライアント・ドメイン名について詳しくは、外部 LDAP 認証サーバーのセットアップを参照してください。

ステップ 2. XClarity Administrator メニュー・バーで、**管理 → 「セキュリティー」**をクリックします。

ステップ 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」ダイアログを表示します。

ステップ 4. ユーザー認証方式として「**ローカル・ユーザーのログオンを許可**」を選択して、ユーザー・アカウントのローカル管理を有効にします。このオプションを選択するときは、すべてのユーザー・アカウントが管理サーバーにおいてローカルに存在します。

ステップ 5. 「**適用**」をクリックします。

結果

これで、ローカル認証サーバーのユーザー・アカウントを使用して XClarity Administrator 管理サーバーにアクセスできます。外部認証サーバーが復旧して、管理サーバーから使用できるようになったら、LDAP クライアント設定を外部認証サーバーに戻します。

外部 SAML ID プロバイダー サーバーの障害後の Lenovo XClarity Administrator へのアクセス

外部 SAML ID プロバイダーを使用しているときに、そのサーバーで障害が発生したかサーバーを利用できない場合は、以下の手順に従って、XClarity Administrator のローカル認証サーバーを使用して Lenovo XClarity Administrator Web インターフェースへのアクセスを回復します。

手順

SAML クライアントの設定を変更するには、以下の手順を実行します。

ステップ 1. Web ブラウザーで XClarity Administrator ログイン・ページ (たとえば、`https://<ip_address>/ui/login.html`) を開きます。

ステップ 2. ID プロバイダー をセットアップしたときに作成したローカル・リカバリー・ユーザー・アカウントを使用して XClarity Administrator Web インターフェースにログインします。

ステップ 3. XClarity Administrator メニュー・バーで、**管理 ➡ 「セキュリティー」**をクリックします。

ステップ 4. 「ユーザーとグループ」セクションの「**SAML 設定**」をクリックして、「SAML 設定」ダイアログを表示します。

ステップ 5. SAML ID プロバイダー を無効にするには、「**SAML を有効にする**」をクリアします。このオプションをクリアすると、ローカル認証サーバーまたは外部 LDAP サーバー (構成されている場合) が認証に使用されます。

ステップ 6. 「**適用**」をクリックします。

結果

これで、ローカル認証サーバーのユーザー・アカウントを使用して XClarity Administrator 管理サーバーにアクセスできます。外部 ID プロバイダー が復旧して、管理サーバーから使用できるようになったら、認証方法を ID プロバイダーに変更できます。

ユーザー・アカウントの管理

*ユーザー・アカウント*は、Lenovo XClarity Administrator と、XClarity Administrator によって管理されているすべてのシャーシとサーバーにログインしたり、それらを管理したりするために使用されます。XClarity Administrator のユーザー・アカウントには、認証と許可という、互いに依存する 2 つのプロセスが適用されます。

このタスクについて

*認証*は、ユーザーの資格情報の確認に使用されるセキュリティー・メカニズムです。認証プロセスでは、構成された認証サーバーに保存されているユーザー資格情報が使用されます。これにより、許可されていない管理サーバーや、管理対象システムの不正なアプリケーションによるリソースへのアクセスも防止さ

れます。認証が完了すると、ユーザーは XClarity Administrator にアクセスできるようになります。ただし、特定のリソースにアクセスしたり、特定のタスクを実行したりするには、適切な許可も必要です。

*許可*では、認証されたユーザーの権限を確認して、役割グループのメンバーシップに基づいてリソースへのアクセスを制御します。*役割グループ*は、認証サーバーで定義および管理されているユーザー・アカウントのセットに特定の役割を割り当てるために使用されます。たとえば、スーパーバイザー権限を持つ役割グループのメンバーになっているユーザーは、XClarity Administrator でユーザー・アカウントの作成、編集、削除を行うことができます。オペレーター権限を持っているユーザーは、ユーザー・アカウント情報の表示のみを行うことができます。

注：SYSMGR_* および SYSRDR_* ユーザー・アカウント (* は、文字 A ～ Z および 0 ～ 9 から作成され、ランダムに選択されたサフィックスです) は XClarity Administrator によって生成され、サービス・ユーザー・アカウントとして使用されるほか、管理対象認証、OS デプロイメント、ファームウェア更新などの機能で使用されます。SYSMGR_* および SYSRDR_* パスワードは、XClarity Administrator がブートされるたびに、またパスワードの有効期限が切れる直前にローテーションされます。

ユーザーの作成

ユーザー・アカウントは、リソースに対する許可やアクセスを管理するために使用されます。

このタスクについて

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

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

手順

XClarity Administrator にユーザーを追加するには、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 → 「セキュリティー」**をクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**ローカル・ユーザー**」をクリックして、「ユーザー管理」ページを表示します。

ステップ 3. 「**作成**」アイコン () をクリックして、ユーザーを作成します。「新しいユーザーの作成」ダイアログが表示されます。

ステップ 4. ダイアログで以下の情報を入力します。

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

ステップ 5. 「**作成**」をクリックします。

終了後

「ユーザー管理」テーブルにユーザー・アカウントが表示されます。このテーブルには、各ユーザー・アカウントに関連付けられている役割グループとアカウント・ステータスが表示されます。

ユーザー・アカウントを作成した後、選択したユーザー・アカウントに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、ユーザー・アカウントのユーザー名、説明、および役割を変更する。
- 「**削除**」アイコン ( ) をクリックして、ユーザー・アカウントを削除する。
- ユーザー・アカウントのパスワードをリセットする (ユーザーのパスワードのリセットを参照)。
- アカウントをロック解除する (ユーザーのロック解除を参照)。
- ユーザー・アカウントを有効または無効にする (ユーザーの有効化または無効化を参照)。

ユーザーの有効化または無効化

認証サーバーのローカル・ユーザー・アカウントを有効または無効に変更できます。

手順

ユーザー・アカウントを有効または無効にするには、以下の手順を実行します。

- ローカル認証サーバーを使用している場合:
  1. Lenovo XClarity Administrator のタイトル・バーで、「**管理**」 ➡ 「**セキュリティー**」の順にクリックします。
  2. 「ユーザーとグループ」セクションの「**ローカル・ユーザー**」をクリックして、「ユーザー管理」ページを表示します。
  3. ユーザー・アカウントを選択します。
  4. 有効になっているユーザー・アカウントを無効にするには、「**すべての操作**」 ➡ 「**選択済みアカウントを無効化する**」の順にクリックします。テーブルのアカウント・ステータスが `Disabled` に変わります。
  5. 無効になっているユーザー・アカウントを有効にするには、「**すべての操作**」 ➡ 「**選択済みアカウントを有効化する**」の順にクリックします。テーブルのアカウント・ステータスが `Enabled` に変わります。
- 外部 LDAP サーバーを使用している場合は、Microsoft Active Directory でユーザー・アカウントを有効または無効にします。
- 外部 SAML ID プロバイダー を使用している場合は、ID プロバイダー でユーザー・アカウントを有効または無効にします。

アクティブ・ユーザーのログオフ

Lenovo XClarity Administrator からアクティブ・ユーザーをログオフ (終了) させることができます。

lxc-supervisor または **lxc-security-admin** 権限を持つユーザー・アカウントで XClarity Administrator にログインする必要があります。

手順

アクティブ・ユーザーをログオフするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のタイトル・バーで、「**管理**」 → 「**セキュリティー**」の順にクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**アクティブ・セッション**」をクリックして、「アクティブ・セッションの管理」ページを表示します。

ステップ 3. 1 つ以上のユーザー・アカウントを選択します。

ステップ 4. 「**ユーザーをログオフする**」をクリックします。

ユーザー・アカウントのパスワードの変更

ユーザー・アカウントのパスワードを変更できます。

手順

パスワードを変更するには、以下の手順を実行します。

- ローカル認証サーバーを使用している場合:
  1. Lenovo XClarity Administrator のタイトル・バーで、ユーザー操作メニュー (ADMIN_USER) をクリックした後、「**パスワードの変更**」をクリックします。「パスワードの変更」ダイアログが表示されます。

  2. 現在のパスワードを入力します。
  3. 新しいパスワードを入力し、確認のためにもう一度入力します。現在のアカウント・セキュリティー設定に基づくパスワード規則が適用されます。
  4. 「**変更**」をクリックします。
- 外部認証サーバーを使用している場合は、Microsoft Active Directory でパスワードを変更します。

注意：Microsoft Active Directory を、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・アカウントの新規パスワードで更新した場合は、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 (外部 LDAP 認証サーバーのセットアップ参照)。

- 外部 SAML ID プロバイダー を使用している場合は、ID プロバイダー でパスワードを変更します。

ユーザーのパスワードのリセット

任意のユーザー・アカウントのパスワードをリセットできます。

手順

パスワードをリセットするには、以下の手順を実行します。

- ローカル認証サーバーを使用している場合、Lenovo XClarity Administrator Web インターフェースからパスワードをリセットします。
  1. XClarity Administrator メニュー・バーで、**管理 ➡ 「セキュリティー」**をクリックします。
  2. 「ユーザーとグループ」セクションの「**ローカル・ユーザー**」をクリックして、「ユーザー管理」ページを表示します。
  3. テーブルからユーザー・アカウントを選択します。
  4. ユーザー・アカウントが有効になっている場合は、**「すべての操作」 ➡ 「選択済みユーザーのパスワードをリセット」**の順にクリックします。「パスワードのリセット」ダイアログが表示されます。
     a. 新しいパスワードを入力し、確認のためにもう一度入力します。現在のアカウント・セキュリティー設定に基づくパスワード規則が適用されます。
     b. XClarity Administrator への初回ログイン時にパスワードの変更をユーザーに強制する場合は、「**最初のアクセス時に変更**」を「`Yes`」に設定します。
     c. 「**リセット**」をクリックします。
- 外部 LDAP サーバーを使用している場合は、Microsoft Active Directory でパスワードをリセットします。
- 外部 SAML ID プロバイダー を使用している場合は、ID プロバイダー でパスワードをリセットします。
- 別スーパーバイザー・アカウントを使用しても XClarity Administrator にログインできない場合、または別スーパーバイザー・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、リカバリーまたはスーパーバイザー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。詳しくは、 XClarity Administrator オンライン・ドキュメントのローカル・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を参照してください。

ユーザーのロック解除

Lenovo XClarity Administrator からロックアウトされたユーザー・アカウントをロック解除できます。ログインの試行回数が制限を超えるとユーザー・アカウントが一時的にロックされる場合があります。

このタスクについて

ロックアウトされたユーザーが再びログインを試行できるようになるまでの時間は、ユーザー・アカウントのセキュリティー設定によって制御されています。「**ログイン失敗が最大回数に達した後のロックアウト期間**」が `0` に設定されている場合は、管理者が明示的にロックを解除するまでユーザー・アカウントはロックされたままになります。「ログイン失敗が最大回数に達した後のロックアウト期間」について詳しくは、ユーザー・アカウントのセキュリティー設定の変更を参照してください。

ユーザー・アカウントを永続的に無効または有効にすることもできます。詳しくは、ユーザーの有効化または無効化を参照してください。

注：ユーザー・アカウントをロック解除するにはスーパーバイザー権限が必要です。

ヒント: XClarity Administrator でロック解除できるのは、ローカル認証サーバーを使用して管理されているユーザー・アカウントです。外部認証サーバーのユーザー・アカウントを XClarity Administrator でロック解除することはできません。

手順

ユーザー・アカウントをロック解除するには、以下の手順を実行します。

- ローカル認証サーバーを使用している場合:
  1. XClarity Administrator メニュー・バーで、**管理 ➡ 「セキュリティー」**をクリックします。
  2. 「ユーザーとグループ」セクションの「**ローカル・ユーザー**」をクリックして、「ユーザー管理」ページを表示します。
  3. テーブルからユーザー・アカウントを選択します。
  4. **「すべての操作」 ➡ 「選択済みユーザーのアカウントをアンロック」**の順にクリックします。
- 外部 LDAP サーバーを使用している場合は、Microsoft Active Directory でユーザー・アカウントをロック解除します。
- 外部 SAML ID プロバイダー を使用している場合は、ID プロバイダー でユーザー・アカウントをロック解除します。

アクティブなユーザーの監視

Lenovo XClarity Administrator Web インターフェースにログインしているユーザーは、ダッシュボード・ページで調べることができます。

手順

- XClarity Administrator メニュー・バーから「**ダッシュボード**」をクリックすると、アクティブ・ユーザーとその IP アドレスのリストがあります。

  アクティブなユーザー・セッションが「活動」セクションに表示されます。

- XClarity Administrator メニュー・バーから「**管理**」 ➡ 「**セキュリティー**」をクリックし、「**アクティブ・セッション**」をクリックすると、すべてのアクティブ・ユーザー (現在のユーザー以外) とその IP アドレスのリストがあります。

  注：特定時間を超えて非アクティブなユーザー・セッションは、自動的にログアウトします。XClarity Administrator メニュー・バーから「**管理**」 ➡ 「**セキュリティー**」をクリックし、「アカウント・セキュリティー設定」をクリックして、「**Web 非アクティブ・セッションのタイムアウト**」の値を調整することで、非アクティブな期間を設定します。この変更により、アクティブ・ユーザー・セッションに影響しないことに注意してください。設定の変更後に開始するユーザー・セッションにのみ影響します。

保存された資格情報の管理

*保存された資格情報*は、ローカル認証を使用して Lenovo XClarity Administrator によって管理されているシャーシとサーバーに対する承認やアクセスを管理するために使用されます。

始める前に

保存された資格情報を作成、変更、削除するには、**lxc-supervisor** または **lxc-security-admin** 権限が必要です。

このタスクについて

保存された資格情報は、デバイスのローカル・ユーザー・アカウントまたは Active Directory サーバーのユーザー・アカウントである必要があります。

XClarity Administrator 管理対象認証ではなく、ローカル認証を使用してデバイスを管理する場合、管理プロセス中に保管されている資格情報アカウントを選択する必要があります。

重要：XClarity Administrator は保存された資格情報に対して指定されるユーザー名とパスワードを検証しません。指定された情報がローカル・デバイスまたは Active Directory (管理対象デバイスが認証に Active Directory を使用するように構成されている場合) のアクティブなユーザー・アカウントに対応していることをお客様の責任で確認する必要があります。

注意：保存された資格情報には、スーパーバイザーのアクセス権、またはデバイスの構成を変更するための十分な権限が必要です。保存された資格情報に十分な権限がないデバイスでサーバーを管理しようとすると、管理プロセスが成功しても、アクセス拒否エラーのためにデバイスで追加管理インベントリー操作が失敗し、既知のデバイスとの接続の問題が発生する可能性があります。

手順

XClarity Administrator に保存された資格情報を追加するには、以下の手順を実行します。

ステップ 1. 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。「セキュリティー」ページが表示されます。

ステップ 2. 管理対象認証セクションの「**保存された資格情報**」をクリックして、保存された資格情報ページを表示します。

ステップ 3. 「**作成**」アイコン ( ) をクリックして、保存された資格情報を作成します。「新しい保存された資格情報を作成」ダイアログが表示されます。

ステップ 4. ダイアログで以下の情報を入力します。
- 保存された資格情報のユーザー名とオプションの説明を入力します。
- 保存された資格情報のパスワードを入力して確認します。
- 必要に応じて、RECOVERY_ID の保存されたリカバリー資格情報のパスワードを入力して確認します。

ステップ 5. 「**保存された資格情報を作成**」をクリックします。

終了後

保存された資格情報のアカウントは、保存された資格情報の表に表示されます。表には、保存された資格情報アカウントそれぞれに関連付けられている ID および説明が表示されます。

「保存された資格情報」ページでは、選択した保存された資格情報アカウントに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、保存された資格情報アカウントのユーザー名、パスワード説明を変更する。

  注：保存された資格情報を使用してデバイスを管理し、管理対象の認証を有効にする場合、保存された資格情報を編集することはできません。
- 「**削除**」アイコン ( ) をクリックして、保存された資格情報アカウントを削除する。

有効期限が切れたまたは無効になった保存された資格情報を解決するには、サーバーの有効期限切れまたは無効の保存された資格情報の解決を参照してください。

役割と役割グループの管理

*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。

カスタム役割の作成

*役割*は、特定の操作を実行するための*権限*セットまたは許可です。Lenovo XClarity Administratorには、いくつかの事前定義済みの (デフォルト) の役割が含まれています。また、ユーザーが実行できる固有の権限セットを強制するカスタムの役割を作成できます。

始める前に

このタスクを実行するには、**lxc-supervisor** 権限または **lxc-security-admin** 権限が必要です。

このタスクについて

カスタム・ロールを作成するには、作成する役割に最も近い事前定義済みロールを 1 つ以上選択し、制限する個々の権限をクリアします。これにより、意図した権限がすべて取得され、役割が依存権限を使用して正しく構築されるようになります。

一部の XClarity Administrator の権限は、管理対象デバイスでアクションを実行するために対応する管理モジュール権限に依存します (管理モジュール v1 の権限 および 管理モジュール v2 の権限 参照)。XClarity Administrator 権限は、管理対象デバイスでアクションを要求できる場合がありますが、CMM、IMM、または XCC に対する対応する権限を持っていない場合、デバイスは要求を拒否します。たとえば、管理対象デバイスで電源操作を実行するためのカスタム役割を作成した場合は、**lxc-inventory-modify device-power state** 権限を次のように追加します。

- ラック内の ThinkSystem サーバーについては、**mm-power-and-restart-access-v1** の権限を追加します。
- Flex System シャーシ全体 (シャーシ内のデバイスを含む) については、**mm-power-and-restart-access-v1** の権限を追加します。
- シャーシ内の ThinkSystem サーバーの場合は、**mm-power-and-restart-access-v1**、**mm-blade-operator-v2**、およびターゲット・サーバーと一致する **mm-blade-#-scope-v2** 権限を追加します。

すべての役割に読み取り専用権限が含まれています。どのカスタム役割も、**lxc-operator** 役割よりも制限を厳しくすることはできません。

ユーザーが特定の操作を実行する権限を持っていない場合、メニュー項目、ツールバー・アイコン、およびそれらの操作を実行するボタンは無効になります (淡色表示されます)。

XClarity Administrator は、役割と同じ名前を使用して、定義済みの各役割に役割グループを提供します。作成する新しい役割の役割グループを作成することを検討してください。役割グループの詳細については、カスタム役割グループの作成を参照してください。

- **lxc-supervisor**。この役割が割り当てられたユーザーは、管理サーバーとすべての管理対象デバイスで、利用可能なすべての操作にアクセスして構成および実行できます。この役割が割り当てられたユーザーは、常にすべての管理対象デバイスにアクセスできます。この役割でデバイスへのアクセスを制限することはできません。
- **lxc-admin**。この役割が割り当てられたユーザーは、管理サーバーで、セキュリティー関連以外の設定の変更やセキュリティー関連以外のすべての操作を実行できます。たとえば、管理サーバーの更新や再起動が可能です。また、この役割では、管理サーバーと管理対象デバイスに関するすべての構成とステータス情報を表示できる権限も付与されます。
- **lxc-security-admin**。この役割が割り当てられたユーザーは、管理サーバーと管理対象デバイスで、セキュリティー設定の変更やセキュリティー関連の操作を実行できます。また、この役割では、管理サーバーと管理対象デバイスに関するすべての構成とステータス情報を表示できる権限も付与されます。

  この役割が割り当てられたユーザーは、常にすべての管理対象デバイスにアクセスできます。この役割でデバイスへのアクセスを制限することはできません。
- **lxc-hw-admin**。この役割が割り当てられたユーザーは、管理対象デバイスで、セキュリティー以外の設定の変更やセキュリティー関連以外の操作を実行できます。たとえば、管理対象デバイスの更新や再起動が可能です。また、この役割では、管理サーバーとすべての管理対象デバイスに関するすべての構成とステータス情報を表示できる権限も付与されます。
- **lxc-fw-admin**.この役割が割り当てられたユーザーは、ファームウェア・ポリシーを作成し、管理対象デバイスにそのポリシーをデプロイできます。この役割を割り当てられていないユーザーは、ポリシー情報の表示のみができます。
- **lxc-os-admin**.この役割が割り当てられたユーザーは、オペレーティング・システムおよびデバイス・ドライバーの更新を管理対象サーバーにダウンロードし、デプロイできます。この役割が割り当てられていないユーザーは、オペレーティング・システムおよびデバイス・ドライバーの情報の表示のみを行うことができます。

- **lxc-service-admin**。この役割が割り当てられたユーザーは XClarity Administrator および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できます。この役割が割り当てられていないユーザーは、サービス・データを収集できますが、ダウンロードできません。
- **lxc-hw-manager**。この役割が割り当てられたユーザーは、新しいデバイスを検出し、それらのデバイスを XClarity Administrator の管理制御下に置くことができます。この役割を持つユーザーは、管理サーバーと管理対象デバイスで、新しいデバイスの検出と管理に必要な操作を超えた操作を実行したり、構成設定を変更したりすることができません。
- **lxc-operator**。この役割が割り当てられたユーザーは、管理サーバーと管理対象デバイスに関するすべての構成とステータス情報を表示できます。この役割のユーザーは、管理サーバーと管理対象デバイスで、操作を実行したり構成設定を変更したりできません。
- **lxc-recovery**。この役割が割り当てられたユーザーは、管理サーバーで、セキュリティー設定の変更やセキュリティー関連の操作を実行できます。認証方式が外部 LDAP サーバーに設定されている場合でも、XClarity Administrator に直接認証することもできます。この役割は、「ログイン資格情報」構成を使用する外部 LDAP サーバーとの通信で何らかのエラーが発生した場合、リカバリー機能を提供します。

  この役割が割り当てられたユーザーは、常にすべての管理対象デバイスにアクセスできます。この役割でデバイスへのアクセスを制限することはできません。

次の事前定義済みの役割は *予約済み* であり、新しい役割グループの作成に使用したり新規ユーザーに割り当てることはできません。
- **lxc sysrdr**
- **lxc-sysmgr**

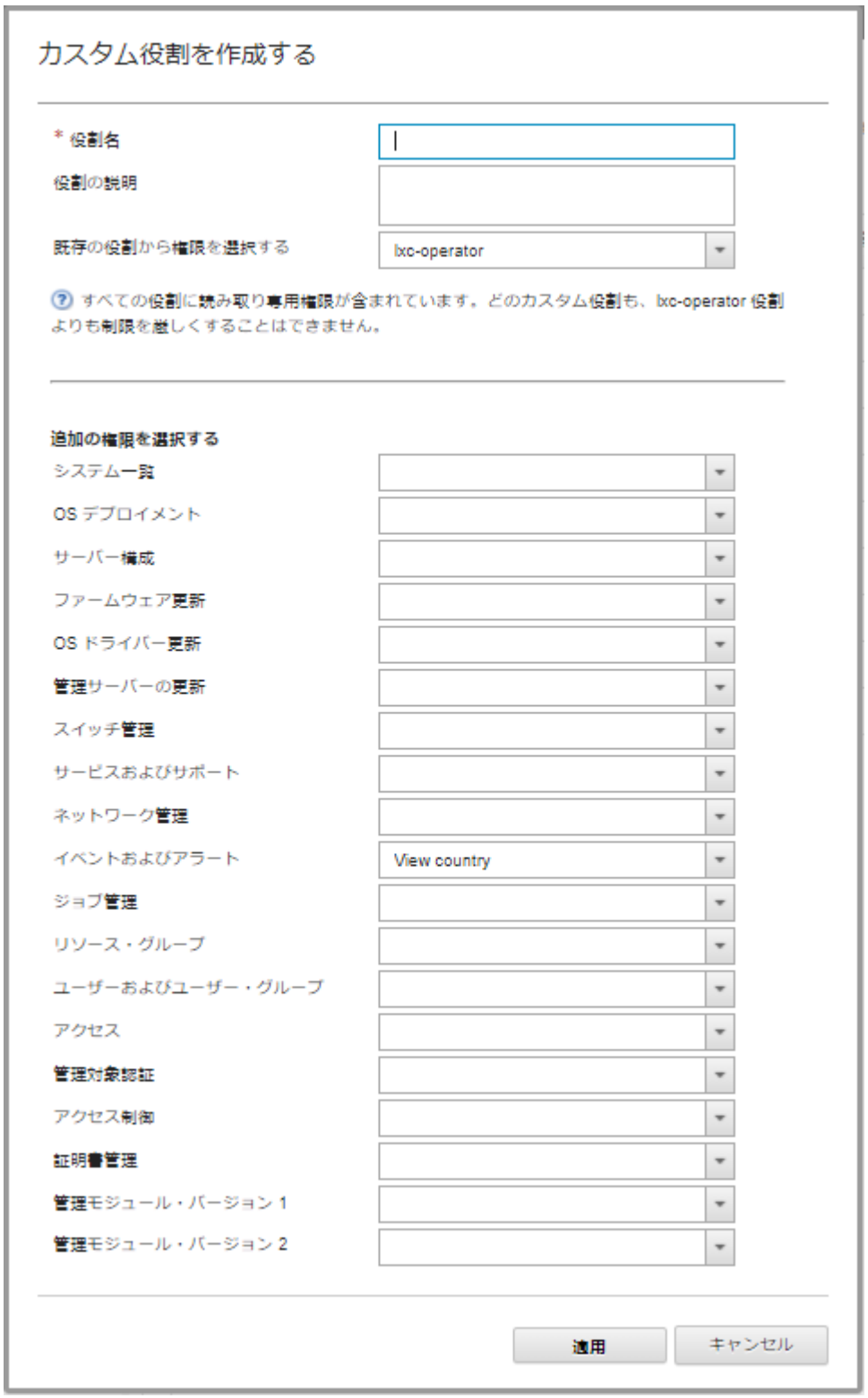
手順

カスタム役割を作成するには、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、**管理 → 「セキュリティー」**をクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**役割**」をクリックして、「役割管理」ページを表示します。

ステップ 3. 「**作成**」アイコン ( ) をクリックして、役割を作成します。「カスタム役割の作成」ダイアログが表示されます。



ステップ 4. 役割の名前と説明を入力します。

ステップ 5. このカスタム役割の開始点として使用する事前定義済みの役割を選択します。

既存の役割を選択すると、その役割に関連付けられている権限がダイアログで選択されます。

ステップ 6. 「**追加権限の選択**」ドロップダウン・メニューから権限を選択するか、選択を解除することによって、この新しい役割の権限を変更します。

注：特定のカテゴリーのすべての権限を選択した場合で、XClarity Administrator を更新またはアップグレードしたときにそのカテゴリーに権限が追加された場合、新しい権限がカスタム役割に自動的に追加されます。

ステップ 7. 「**作成**」をクリックします。「役割の管理」ページのテーブルに新しい役割が追加されます。

結果

また、以下の操作を実行できます。

- 役割を選択して、「**表示**」アイコン () をクリックすると、特定の役割に関連する権限が表示されます。
- 「**編集**」アイコン () をクリックすると、カスタム役割の名前の変更または編集を行うことができます。カスタム役割を編集する場合、その役割に関連付けられている選択した権限、説明、およびユーザーのリストを変更できます。

  注：事前定義済みの役割を変更することはできません
- 「**削除**」アイコン () をクリックすると、事前定義済みの役割またはカスタム役割を削除できます。
- 役割グループから役割を追加または削除します (複数のユーザーの役割グループからの追加および削除 を参照してください)。
- 「**すべての操作**」 ➞ 「**デフォルトの役割の復元**」をクリックすると、削除されたすべての事前定義済みの役割を復元できます。

事前定義済みの権限

Lenovo XClarity Administrator では、特定の操作の実行をユーザーに許可する*権限* (許可) セットを提供しています。この権限は、操作のタイプに基づくカテゴリに分類されています。

アクセス権限

これらの権限は、暗号化および SSL/TLS モードを変更するためのアクセス権限を提供します。

権限名	権限の説明	デフォルトの役割
lxc-sec-apply-crypto-settings	暗号化設定の適用	lxc-recovery、lxc-security-admin、lxc-supervisor

アクセス制御権限

これらの権限は、リソースへのアクセスを制御するアクセス権限を付与します。

権限名	権限の説明	デフォルトの役割
lxc-sec-modify-resource-access-control	リソース・アクセス制御設定の編集	lxc-recovery、lxc-security-admin、lxc-supervisor

証明書管理権限

これらの権限は、Lenovo XClarity Administrator のセキュリティー証明書を管理するアクセス権限を付与します。

権限名	権限の説明	デフォルトの役割
lxc-sec-add-external-certificates	外部証明書の追加	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-add-trusted-certificates	信頼できる証明書の追加	lxc-recovery、lxc-security-admin、lxc-supervisor

権限名	権限の説明	デフォルトの役割
lxc-sec-certificate-signing	証明書署名要求の生成	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-delete-external-certificates	既存の外部証明書の削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-delete-trusted-certificates	既存の証明書の削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-download-ca	証明機関ルート証明書のダウンロード	lxc-admin、lxc-hw-admin、lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-download-server-certificate	サーバー証明書のダウンロード	lxc-admin、lxc-hw-admin、lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-certificate-revocation-list	証明書取り消しリストの変更または置き換え	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-regenerate-ca	証明機関ルート証明書の再作成	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-regenerate-download-ca	証明機関ルート証明書の再作成	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-regenerate-server-certificate	サーバー証明書の再作成	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-resolve-untrusted-certificates	信頼できない証明書を解決	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-upload-server-certificate	サーバー証明書のアップロード	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc_sec_view_certpol_settings	証明書ポリシーの設定の表示	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
lxc_sec_apply_certpol_settings	証明書ポリシーの設定の適用	lxc-security-admin、lxc-supervisor

監視とイベントの権限

これらの権限は、イベントとアラートを管理する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-event-audit	イベントと監査ログの管理	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	イベント・フォワーダーの作成および変更	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-monitoring-create-edit-push-services	プッシュ・サービスの作成および変更	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-monitoring-remove-event-forwarders	イベント・フォワーダーの削除	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-monitoring-remove-push-services	プッシュ・サービスの削除	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-monitoring-set-event-thresholds	イベントしきい値の設定	lxc-admin、lxc-hw-admin、lxc-supervisor

ファームウェア更新の権限

これらの権限は、ファームウェア更新および UpdateXpress System Packs を管理、適用する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-fwUpdates-apply-assign-policy	ファームウェア・コンプライアンス・ポリシーのデバイスへの割り当て	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-apply-perform-updates	ファームウェアの更新の実行	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-policies-create-policies	ファームウェア・コンプライアンス・ポリシーの作成、コピー、編集、およびインポート	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-policies-delete-policies	コンプライアンス・ポリシーの削除	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-repository-delete-packages	ファームウェア更新パッケージの削除	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-repository-download-packages	ファームウェア更新パッケージをダウンロードおよびインポートして、ファームウェア更新パッケージのカタログを最新の情報への更新	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor
lxc-fwUpdates-repository-export-packages	ファームウェア更新パッケージのエクスポート	lxc-admin、lxc-fw-admin、lxc-hw-admin、lxc-supervisor

リソース・グループの権限

これらの権限は、リソース・グループを使用する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-resource-create-edit-group	リソース・グループの作成および変更	lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-resource-delete-group	リソース・グループの削除	lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor

インベントリーの権限

この権限は、デバイスの検出と管理、およびデバイス・インベントリーを表示する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-dm-manage-device	シャーシ、サーバー、ストレージ、およびスイッチの管理	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-dm-modify-ip-settings	同じサブネット内の IP アドレスの重複のチェックの有効化または無効化	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-inventory-modify-device-power-state	キャニスター、CMM、ノード、ストレージ、およびスイッチの電源状態の変更	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-inventory-modify-device-properties	キャビネット、キャニスター、シャーシ、CMM、ノード、ストレージ、およびスイッチのプロパティの変更	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	予知された障害アラート (PFA) の構成設定の変更	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor

ジョブ管理の権限
これらの権限は、ジョブ (タスク) を管理する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-tasks-remove-jobs	ジョブの削除	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-tasks-schedule-jobs	ジョブのスケジュール	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor

管理対象認証権限
これらの権限は、保管された資格情報を含む認証を管理するためのアクセス権限を提供します。

権限名	権限の説明	デフォルトの役割
lxc-sec-delete-stored-credentials	保存された資格情報の削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-stored-credentials	既存の保存された資格情報の編集	lxc-recovery、lxc-security-admin、lxc-supervisor

管理モジュール v1 の権限
これらの権限は、ラック・サーバーおよび Flex System シャーシ全体 (そのシャーシ内のすべてのデバイスを含む) の管理モジュールによって適用される LDAP アクセス権限ビット (bitstrings) に関連付けられています。

Lenovo XClarity Administrator では、これらの許可は適用されません。これらの許可は、XClarity Administrator ユーザー・アカウントを使用する管理対象デバイスによって適用されます。

デバイスが*管理対象認証*を使用して (ローカル認証サーバーを使用して) 管理されている場合、ローカル認証サーバーでは、管理対象デバイスに対してデバイスへのログイン時にユーザーに付与する権限を示すためにこれらの権限を使用します。

外部 LDAP サーバーで、同じこれらの許可を構成します。XClarity Administrator で外部 LDAP サーバーを使用する場合は、XClarity Administrator の役割グループ名と一致する名前を持つグループを外部 LDAP サーバーに追加し、外部 LDAP サーバーがそのグループのうちの 1 つ以上に追加されていることを確認します。外部 LDAP ユーザーは、管理モジュールのビット・ストリングに関連付けられている役割を含む XClarity Administrator 役割グループに一致する名前を持つ LDAP グループの一部である必要があります。XClarity Administrator はこれらのグループを使用して外部 LDAP ユーザーを XClarity Administrator の役割グループに関連付け、管理モジュールによって適用されるビット・ストリングに関連付けます。その後、ユーザーが外部 LDAP ユーザー・アカウントを使用して管理対象デバイスにログインすると、管理モジュールではユーザー・スーパーバイザー権限またはオペレーター権限のどちらを付与するかを認識します。

注：有効化されたセキュア IOM、RackSwitch スイッチ、ストレージ・デバイス、および ThinkServer サーバーを備えていない FlexSystem スイッチでは、管理モジュール v1 権限はサポートされません。

各管理モジュールの LDAP 許可ビットについては、オンライン・ドキュメントを参照してください。
- CMM および CMM2 のオンライン・ドキュメントの LDAP の構成
- IMM および IMM2 のオンライン・ドキュメントの LDAP の構成
- XCC オンライン・ドキュメントの LDAP の構成

権限名	権限の説明	デフォルトの役割
mm-advanced-adaptor-configuration-v1	アダプターの拡張構成	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-basic-configuration-v1	基本構成	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-clear-event-logs-v1	イベント・ログのクリア	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-deny-always-v1	常に拒否	lxc-admin、lxc-hw-admin、lxc-supervisor
mm-networking-and-security-v1	ネットワーキングおよびセキュリティー	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-power-and-restart-access-v1	サーバーおよび Flex スイッチの電源/再起動アクセス	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-remote-console-access-v1	サーバーのリモート制御アクセス	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	サーバーのリモート・コンソールおよび仮想メディア・アクセス	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-supervisor-v1	スーパーバイザー・アクセス権	lxc-admin、lxc-hw-admin、lxc-supervisor
mm-user-account-management-v1	ユーザーの管理	lxc-admin、lxc-hw-admin、lxc-recovery、lxc-security-admin、lxc-supervisor

管理モジュール v2 の権限

これらの権限は、シャーシ (有効化されたセキュア IOM を持つシャーシ、サーバー、およびスイッチ) 内の個々の FlexSystem および ThinkSystem デバイスの管理モジュールによって適用される LDAP アクセス権限ビット (bitstrings) に関連付けられています。

Lenovo XClarity Administrator では、これらの許可は適用されません。これらの許可は、XClarity Administrator ユーザー・アカウントを使用する管理対象デバイスによって適用されます。

デバイスが*管理対象認証*を使用して (ローカル認証サーバーを使用して) 管理されている場合、ローカル認証サーバーでは、管理対象デバイスに対してデバイスへのログイン時にユーザーに付与する権限を示すためにこれらの権限を使用します。

外部 LDAP サーバーで、同じこれらの許可を構成します。XClarity Administrator で外部 LDAP サーバーを使用する場合は、XClarity Administrator の役割グループ名と一致する名前を持つグループを外部 LDAP サーバーに追加し、外部 LDAP サーバーがそのグループのうちの 1 つ以上に追加されていることを確認します。外部 LDAP ユーザーは、管理モジュールのビット・ストリングに関連付けられている役割を含む XClarity Administrator 役割グループに一致する名前を持つ LDAP グループの一部である必要があります。XClarity Administrator はこれらのグループを使用して外部 LDAP ユーザーを XClarity Administrator の役割グループに関連付け、管理モジュールによって適用されるビット・ストリングに関連付けます。その後、ユーザーが外部 LDAP ユーザー・アカウントを使用して管理対象デバイスにログインすると、管理モジュールではユーザー・スーパーバイザー権限またはオペレーター権限のどちらを付与するかを認識します。

注：

- シャーシ全体の管理モジュール v1 権限も指定する必要があります (管理モジュール v1 の権限 を参照)。
- セキュア IOM が有効になっていない FlexSystem スイッチでは、管理モジュール v2 権限はサポートされません。

- Lenovo ThinkSystem シャーシの場合は、カスタム役割に「ノード管理」を許可するように IMM2 が設定されていることを確認します。カスタム役割が Lenovo ThinkSystem シャーシ内のすべてのデバイスを制御できるようにする場合は、カスタム役割が「ノード X の範囲」も持つように IMM2 が設定されていることを確認します。

各管理モジュールの LDAP 許可ビットについては、オンライン・ドキュメントを参照してください。
- CMM および CMM2 のオンライン・ドキュメントの LDAP の構成
- IMM および IMM2 のオンライン・ドキュメントの LDAP の構成
- XCC オンライン・ドキュメントの LDAP の構成

権限名	権限の説明	デフォルトの役割
mm-blade-1-scope-v2	ノード 1 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-2-scope-v2	ノード 2 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-3-scope-v2	ノード 3 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-4-scope-v2	ノード 4 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-5-scope-v2	ノード 5 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-6-scope-v2	ノード 6 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-7-scope-v2	ノード 7 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-8-scope-v2	ノード 8 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-9-scope-v2	ノード 9 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-10-scope-v2	ノード 10 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-11-scope-v2	ノード 11 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-12-scope-v2	ノード 12 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-13-scope-v2	ノード 13 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-14-scope-v2	ノード 14 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-administration-v2	ノード管理	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-configuration-v2	ノード構成	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-operator-v2	ブレード・オペレーター	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-blade-remote-presence-v2	ノード・リモート・プレゼンス	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-chassis-administration-v2	シャーシ管理	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor

権限名	権限の説明	デフォルトの役割
mm-chassis-configuration-v2	シャーシ構成	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-chassis-log-management-v2	シャーシ・ログ・アカウント管理	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-chassis-operator-v2	シャーシ・オペレーター	lxc-admin、lxc-hw-admin、lxc-supervisor
mm-chassis-scope-v2	シャーシの範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-chassis-user-account-management-v2	ユーザーの管理	lxc-admin、lxc-hw-admin、lxc-recovery、lxc-security-admin、lxc-supervisor
mm-deny-always-v2	常に拒否	lxc-admin、lxc-hw-admin、lxc-supervisor
mm-io-module-1-scope-v2	I/O モジュール 1 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-io-module-2-scope-v2	I/O モジュール 2 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-io-module-3-scope-v2	I/O モジュール 3 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-io-module-4-scope-v2	I/O モジュール 4 の範囲	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-switch-administration-v2	スイッチの管理	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-switch-configuration-v2	スイッチの構成	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
mm-switch-operator-v2	スイッチ・オペレーター	lxc-admin、lxc-hw-admin、lxc-supervisor
mm-supervisor-v2	スーパーバイザー・アクセス権	lxc-admin、lxc-hw-admin、lxc-supervisor

管理サーバーの権限

これらの権限は、管理サーバーを更新する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-mgmtserverupdates-delete-updates	管理サーバーの更新の削除	lxc-admin、lxc-fw-admin、lxc-supervisor
lxc-mgmtserverupdates-download-updates	管理サーバーの更新をダウンロードおよびインポートして、管理サーバーのカタログを最新の情報に更新	lxc-admin、lxc-fw-admin、lxc-supervisor
lxc-mgmtserverupdates-perform-updates	管理サーバーの更新の実行	lxc-admin、lxc-fw-admin、lxc-supervisor

ネットワーク管理の権限

これらの権限は、ネットワーク設定を構成する許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-network-edit	ネットワーク・アクセスの変更	lxc-admin、lxc-supervisor

OS デプロイメントの権限

これらの権限は、オペレーティング・システムの管理とデプロイを行う許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-osdeploy-create-edit-remote-file-server	リモート・ファイル・サーバー・エントリーの作成と編集	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	OS イメージおよびカスタム・ファイルの作成、インポート、エクスポート、および編集	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osdeploy-delete-os-files	OS イメージおよびカスタム・ファイルの削除	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osdeploy-delete-remote-file-server	リモート・ファイル・サーバー・エントリーの削除	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osdeploy-edit-global-settings	「共通設定」ダイアログの情報の編集 **注：**グローバル IP 割り当て設定の変更は、ネットワーク設定に影響を及ぼします。したがって、グローバルな IP 割り当て設定を変更するには、**lxc-osdeploy-edit-settings-and-deploy-os-images** の権限も必要です。	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	デプロイメント設定を変更し、1 つ以上のサーバーに OS イメージをデプロイ	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor

OS ドライバーの更新権限

これらの権限は、OS デバイス・ドライバー更新の管理および適用を行う許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-osDriverUpdates-apply-assign-uxsp	デバイスへの OS デバイス・ドライバー UXSP の割り当て	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	OS 認証の確認	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	OS デバイス・ドライバーのコンプライアンスの確認	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	OS デバイス・ドライバーの更新の実行	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	OS デバイス・ドライバー更新パッケージの削除	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	OS デバイス・ドライバーの更新パッケージをダウンロードおよびインポートして、OS デバイス・ドライバーの UXSP カタログを最新の情報に更新	lxc-admin、lxc-hw-admin、lxc-os-admin、lxc-supervisor

ユーザーとグループの権限

これらの権限は、ユーザー・アカウントとグループを管理するアクセス権限を付与します。

権限名	権限の説明	デフォルトの役割
lxc-sec-apply-saml-settings	SAML 設定の適用	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-delete-role-groups	役割グループの削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-delete-roles	役割の削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-delete-users	ユーザーの削除	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-edit-account-settings	アカウント・セキュリティー設定の変更	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-ldap-settings	LDAP 設定の適用	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-role-groups	役割グループの変更	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-roles	役割の変更	lxc-recovery、lxc-security-admin、lxc-supervisor
lxc-sec-modify-users	ユーザーの変更	lxc-recovery、lxc-security-admin、lxc-supervisor

サーバー構成の権限

これらの権限では、構成パターンを使用して、サーバーのプロビジョニングまたは事前プロビジョニングを行う許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-cp-edit-management-ip	シャーシの管理 IP アドレスを変更	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-edit-preferences	構成パターンの設定	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-manage-address-pools	アドレス・プールの管理	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-manage-patterns	パターンの管理	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-manage-placeholders	プレースホルダーの管理	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-manage-profiles	パターンのデプロイ、シャーシへのプレース ホルダーのデプロイ、プロファイルの管理	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-cp-other-server-config	ローカル・ストレージをリセットし、Intel Optane DCPMM セキュリティー操作を適用	lxc-admin、lxc-hw-admin、lxc-supervisor

サービス権限

これらの権限では、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・ステータスと保証情報の表示、およびサービス・データの収集と転送を行う許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-ss-alter-backup-credentials	バックアップ FFDC 資格情報の変更	lxc-admin、lxc-hw-admin、lxc-service-admin、lxc-supervisor
lxc-ss-call-home	コール・ホームの実行	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-ss-change-service-recovery-password	サービス・リカバリー・パスワードの変更	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-ss-change-service-tickets	サービス・チケットの変更	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-ss-remove-service-tickets	サービス・チケットの削除	lxc-admin、lxc-hw-admin、lxc-supervisor
lxc-ss-run-service-forwarders	サービス・フォワーダーの実行	lxc-admin、lxc-hw-admin、lxc-supervisor

スイッチ構成の権限

これらの権限は、スイッチを構成し、スイッチ構成データのバックアップと復元を行う許可を付与します。

権限名	権限の説明	デフォルトの役割
lxc-netcfg-template-management	スイッチ構成テンプレートの作成、変更、削除、およびデプロイ、スイッチ構成デプロイメントの削除	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-swirm-config-management	スイッチ構成データ・ファイルのバックアップ、復元、削除、エクスポート、およびインポート	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor
lxc-swirm-port-management	スイッチ・ポート・ステータスの変更	lxc-admin、lxc-hw-admin、lxc-hw-manager、lxc-supervisor

カスタム役割グループの作成

*役割グループ*は、役割セット、および同じ役割セットのメンバーであるユーザー・セットです。役割グループ内の各ユーザーに付与されるアクセス・レベルは、その役割グループに割り当てられている役割に基づきます。XClarity Administrator では、それぞれの事前定義済みの役割に対応する以下の定義済み役割グループが提供されています。カスタム役割ビューを作成することもできます。

このタスクについて

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。

XClarity Administrator の定義済みの役割グループを以下に示します。

- LXC-SUPERVISOR。lxc-supervisor の役割を含みます。
- LXC-ADMIN。lxca-admin の役割を含みます。
- LXC-SECURITY-ADMIN.lxc-security-admin の役割を含みます。
- LXC-HW-ADMIN。lxc-hw-admin の役割を含みます。
- LXC-FW-ADMIN。lxc-fw-admin の役割を含みます。
- LXC-OS-ADMIN。lxc-os-admin の役割を含みます。
- LXC-SERVICE-ADMIN。lxc-service-admin の役割を含みます。
- LXC-HW-MANAGER。lxc-hw-manager の役割を含みます。
- LXC-OPERATOR。lxc-operator の役割を含みます。

- **LXC-RECOVERY。lxc-recovery** の役割を含みます。

次の事前定義済みの役割は *予約済み* であり、新しい役割グループの作成に使用したり新規ユーザーに割り当てることはできません。
- **lxc sysrdr**
- **lxc-sysmgr**

手順

役割グループを作成するには、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、**管理 → 「セキュリティー」** をクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**役割グループ**」をクリックして、「グループ管理」ページを表示します。

ステップ 3. 「**作成**」アイコン ( ) をクリックして、役割グループを作成します。「新規役割グループの作成」ダイアログが表示されます。

ステップ 4. グループの名前と説明を入力します。

注：ヒント: グループ名には、文字、数字、スペース、アンダスコア、ダッシュ、ピリオドを使用することができます。

ステップ 5. この役割グループに割り当てる役割を 1 つ以上選択します。

ステップ 6. この役割グループのメンバーとして 1 人以上のユーザーを選択します。

ステップ 7. 「**作成**」をクリックします。「グループの管理」ページのテーブルに新しい役割グループが追加されます。

結果

「役割グループ」テーブルに役割グループが表示されます。このテーブルには、各役割グループに関連付けられている許可役割とグループのメンバーが表示されます。

役割グループを作成したら、選択した役割グループに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、この役割グループに割り当てられている役割を追加または削除します。
- 役割グループのメンバーであるユーザーを追加または削除する (56 ページの 「複数のユーザーの役割グループからの追加および削除」参照)。
- 「**すべての操作**」 → 「**CSV としてエクスポート**」をクリックして、アクセス権限を含む役割グループに関する情報をエクスポートする。
- 「**削除**」アイコン ( ) をクリックして、役割グループを削除する。事前定義済み役割グループは削除できません。

役割グループを作成、編集、または削除すると、その変更が直ちに管理対象のデバイスにプロビジョニングされます。

複数のユーザーの役割グループからの追加および削除

複数のユーザーを追加または削除して、役割グループのメンバーシップを変更できます。

手順

ユーザーを役割グループに追加または削除するには、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** → 「**セキュリティー**」をクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**役割グループ**」をクリックして、「グループ管理」ページを表示します。

ステップ 3. 「**編集**」アイコン () をクリックして、役割グループを編集します。「役割グループの編集」ダイアログが表示されます。

ステップ 4. 「**ユーザー・リスト**」ドロップダウン・リストをクリックして、この役割グループに含めるユーザー、または役割グループから除外するユーザーを選択します。

ステップ 5. 「**保存**」をクリックします。「**ユーザー・リスト**」列に役割グループの現在のユーザー・メンバーシップが表示されます。

デバイスに対するアクセスの管理

デバイスへのアクセス制御はデフォルトでは無効になっており、お客様が有効にするまで反映されません

デバイスが最初に Lenovo XClarity Administrator によって管理される際、役割グループの事前定義済みセットにはデフォルトでデバイスにアクセスするアクセス権限があります。この事前定義済みセットは、構成されるまでデフォルトでは空です。

特定の管理対象デバイスにアクセスできる役割グループを変更できます。特定の役割グループにアクセス権限が付与されると、その役割グループのメンバーになっているユーザーのみがそれらの特定のデバイスを表示および操作できます。

特定のデバイスへのアクセス制御

デバイスが最初に Lenovo XClarity Administrator によって管理される際、役割グループの事前定義済みセットにはデフォルトでデバイスにアクセスするアクセス権限があります。特定の管理対象デバイスにアクセスできる役割グループを変更できます。特定の役割グループにアクセス権限が付与されると、その役割グループのメンバーになっているユーザーのみがそれらの特定のデバイスを表示および操作できます。

始める前に

lxc-supervisor、**lxc-security-admin**、または **lxc-recovery** の権限を持つユーザーのみが、この操作を実行できます。

このタスクについて

アクセス制御は、個々のデバイスで設定されています。ラックおよびリソース・グループなどのコンテナには設定されません。

シャーシまたはエンクロージャー内のコンポーネントでは、シャーシまたはエンクロージャー内のコンポーネントを表示するユーザーは、少なくともそのシャーシまたはエンクロージャーに対する読み取り専用アクセスが必要です。シャーシまたはエンクロージャに対する読み取り専用アクセス以上の権限がないユーザーでも、一部のビューではシャーシ・コンポーネントが表示されますが、すべてのビューで表示されるとは限りません。

lxc-supervisor 権限を持つユーザーは、そのリソースへのアクセス権限が特に付与されている役割グループに属しているかどうかにかかわらず、すべてのリソースを表示および操作できます。**lxc-supervisor** 役割グループの任意のリソースへのアクセスを削除することはできません。

ユーザーが、特定の管理対象デバイスへのアクセス権限を持つ役割グループのメンバーでない場合は、そのユーザーはその特定のデバイスを表示または操作できません。これには、Lenovo XClarity Administrator 経由の管理コントローラー Web インターフェースの起動も含まれます。Flex および System x デバイスの場合、アクセス権限がない CMM または管理コントローラーに直接ログインすることもできません。

デフォルトのアクセス制御設定は、デバイスが最初に XClarity Administrator に管理される際に、そのデバイスのアクセス権限を設定するために使用されます。また、特定のデバイスのアクセス権限をデフォルト設定にリセットする場合にも使用されます。デフォルトのアクセス制御設定を変更しても、すでに管理対象になっているデバイスのアクセス権限は自動的に変更されません。

重要：

- ユーザーが 1 つ以上の役割グループのメンバーであり、その役割グループが異なるデバイスに割り当てられている場合は、ユーザーに許可されている操作が各デバイスで異なる場合があります。たとえば、ユーザーがデフォルトの役割グループ LXC-FW-ADMIN および LXC-OS-ADMIN のメンバーであり、LXC-FW-ADMIN にはサーバー A へのアクセス権限が付与されているが LXC-OS-ADMIN にはサーバー A へのアクセス権限が付与されていない場合、そのユーザーはサーバー A のファームウェアを更新することはできますが、サーバー A にオペレーティング・システムをデプロイすることはできません。LXC-OS-ADMIN にサーバー B へのアクセス権限が付与されているが LXC-FW-ADMIN にはサーバー B へのアクセス権限が付与されていない場合、同じユーザーはサーバー B にオペレーティング・システムをデプロイすることはできますが、サーバー B のファームウェアを更新することはできません。
- (Flex シャーシ内のサーバーやスイッチ) など、親リソースを持つデバイスへのアクセスに制限がある場合、ユーザーには、デバイスと完全に対話するために、親リソースに対する少なくとも読み取り専用のアクセス許可が必要です。ユーザーが親ではなくデバイスに対して少なくとも読み取り専用アクセスを持つ場合、ユーザーには装置インベントリーは表示されませんが、ジョブ、イベントなど、一部のビューでデバイスについて表示できる場合があります。

  たとえば、親の役割グループを作成し、その役割グループに **lxc-operator** の役割を割り当てることができます。該当する役割グループ内のいずれかの子 (Flex シャーシ内のサーバー、スイッチなど) にアクセスできるすべてのユーザーが含まれます。次に、親にアクセスできるいずれかのグループとしてその役割グループを含めます。

手順

特定のデバイスに役割グループを関連付けてそのデバイスへのアクセスを制御するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメイン・メニューで、「**管理**」 → 「**セキュリティー**」の順にクリックします。

ステップ 2. 左ナビゲーション・ペインで、「**リソース・ビュー**」をクリックします。「リソース・ビュー」ページが表示されます。

テーブルの列をソートすると特定のデバイスを見つけやすくなります。さらに、「**リソース・タイプ**」ドロップダウン・リストでデバイス・タイプを選択したり、「**役割グループ**」ドロップダウン・メニューで役割グループを選択したり、「**リソース・グループ**」ドロップダウン・メニューでリソース・グループを選択したり、「**フィルター**」フィールドにテキスト (リソース名やタイプなど) を入力したりして、選択された条件に一致するデバイスのみをリストできます。

ステップ 3. アクセスを制御するデバイスを 1 つ以上選択します。

ステップ 4. 「**編集**」アイコン ( ) をクリックします。「**リソース名**」フィールドにターゲット・デバイスがリストされた「リソースの編集」ダイアログが表示されます。

ステップ 5. 「**役割グループ**」ドロップダウン・リストで、ターゲット・デバイスにアクセスを許可する役割グループを選択します。

注：デバイスに親リソース (たとえば、Flex シャーシ内のサーバーまたはスイッチ) がある場合、デバイス (右の列) と親リソース (左の列) の両方に対するアクセスを指定できます。

ステップ 6. 「**公開アクセス**」を「No」に設定します。これにより、選択した役割グループのメンバーであるユーザーのみが、ターゲット・デバイスにアクセスできます。

ステップ 7. 「**保存**」をクリックします。

ステップ 8. アクセス権限の割り当てが完了したら、「**無効**」トグルをクリックして「**リソース・アクセス制御**」を有効に変更します。

リソース・アクセス制御は、特定のデバイスへのアクセスを構成する前でも構成した後でも、いつでも有効にできます。この設定が有効な場合、表に表示された構成が有効になりま

す。これには、そのデバイスへのアクセスが構成されているグループを持たないデバイスへのスーパーバイザー以外のユーザーのアクセスの拒否も含まれます。

終了後

また、以下の操作を実行して、デバイスへのアクセスを制御することもできます。

- デフォルトの役割グループおよび公開アクセスの設定のアクセス権限を変更するには、「**編集**」アイコン () をクリックしてから、「**デフォルトにリセット**」をクリックします。
- デフォルトの役割グループおよび公開アクセスの設定を変更します (デフォルトのアクセス権限の変更を参照)。
- リソース・アクセス制御を無効にするには、「**有効**」トグルをクリックして「**リソース・アクセス制御**」を無効に変更します。これにより、すべての役割グループがすべての管理対象デバイスにアクセスできます。

リソース・アクセス制御の無効化

すべてのデバイスまたは特定のデバイスのアクセス制御を無効にして、すべてのユーザーがそれらのデバイスを表示および操作できるようにします。

このタスクについて

lxc-supervisor、**lxc-security-admin**、または **lxc-recovery** の権限を持つユーザーのみが、この操作を実行できます。

手順

リソース・アクセス制御を無効にするには、以下の手順を実行します。

- すべての管理対象デバイスの場合
  1. Lenovo XClarity Administrator のメイン・メニューで、「**管理**」 → 「**セキュリティー**」の順にクリックします。
  2. 左ナビゲーション・ペインで、「**リソース・ビュー**」をクリックします。「リソース・ビュー」ページが表示されます。
  3. 「**有効**」トグルをクリックして「**リソース・アクセス制御**」を無効に変更します。
- 特定の管理対象デバイスの場合
  1. XClarity Administrator のメイン・メニューで、「**管理**」 → 「**セキュリティー**」の順にクリックします。
  2. 左ナビゲーション・ペインで、「**リソース・ビュー**」をクリックします。「リソース・ビュー」ページが表示されます。

     テーブルの列をソートすると特定のデバイスを見つけやすくなります。さらに、「**リソース・タイプ**」ドロップダウン・リストでデバイス・タイプを選択したり、「**役割グループ**」ドロップダウン・メニューで役割グループを選択したり、「**リソース・グループ**」ドロップダウン・メニューでリソース・グループを選択したり、「**フィルター**」フィールドにテキスト (リソース名やタイプなど) を入力したりして、選択された条件に一致するデバイスのみをリストできます。
  3. アクセスを変更するデバイスを 1 つ以上選択します。
  4. 「**編集**」アイコン () をクリックします。「**リソース名**」フィールドに選択したデバイスがリストされた「リソースの編集」ダイアログが表示されます。
  5. 「**公開アクセス**」を「Yes」に設定します。これにより、「**役割グループ**」ドロップダウン・リストにリストされている役割グループにかかわらず、すべての役割グループがそのターゲット・デバイスにアクセスできます。
  6. 「**保存**」をクリックします。

デフォルトのアクセス権限の変更

デバイスが最初に Lenovo XClarity Administrator に管理された際、役割グループがそのデバイスにアクセスできるかどうかを決定する設定は、公開アクセスと役割グループの 2 つがあります。公開アクセス設定はすべての役割グループ、または特定の役割グループのセットのみが、ターゲット・デバイスにアクセスできるかどうかを決定します。デフォルトでは、この設定は `Yes` に設定されており、すべての役割グループがターゲット・デバイスにアクセスできます。デフォルトの動作を変更するには、公開アクセスの設定を `No` に変更してから、ターゲット・デバイスにアクセスできる一連の役割グループを選択します。

このタスクについて

lxc-supervisor、**lxc-security-admin**、または **lxc-recovery** の権限を持つユーザーのみが、この操作を実行できます。

lxc-supervisor、**lxc-security-admin**、または **lxc-recovery** の権限を持つユーザーは、すべての管理対象デバイスにアクセスできます。これらの役割グループのデバイスへのアクセス権を削除することはできません。

デフォルトのアクセス制御設定は、デバイスが最初に XClarity Administrator に管理される際に、そのデバイスのアクセス権限を設定するために使用されます。また、特定のデバイスのアクセス権限をデフォルト設定にリセットする場合にも使用されます。デフォルトのアクセス制御設定を変更しても、すでに管理対象になっているデバイスのアクセス権限は自動的に変更されません。

手順

デフォルトアクセス制御を変更するには、以下の手順に従ってください。

ステップ 1. XClarity Administrator のメイン・メニューで、「**管理**」 ➡ 「**セキュリティー**」の順にクリックします。

ステップ 2. 左ナビゲーション・ペインで、「**リソース・ビュー**」をクリックします。「リソース・ビュー」ページが表示されます。

テーブルの列をソートすると特定のデバイスを見つけやすくなります。さらに、「**リソース・タイプ**」ドロップダウン・リストでデバイス・タイプを選択したり、「**役割グループ**」ドロップダウン・メニューで役割グループを選択したり、「**リソース・グループ**」ドロップダウン・メニューでリソース・グループを選択したり、「**フィルター**」フィールドにテキスト (リソース名やタイプなど) を入力したりして、選択された条件に一致するデバイスのみをリストできます。

ステップ 3. 「**すべての操作**」 ➡ 「**デフォルト・リソースの編集**」をクリックします。「デフォルト・リソースの編集」ダイアログが表示されます。

ステップ 4. 「**役割グループ**」ドロップダウン・リストで、デフォルト・セットとして定義する役割グループを選択します。

ステップ 5. デフォルトの「**公開アクセス**」設定を選択します。

- **はい**。デバイスが最初に管理される際は、「**役割グループ**」ドロップダウン・リストにリストされている役割グループにかかわらず、すべての役割グループがそのデバイスにアクセスできます。
- **いいえ**。デバイスが最初に管理される際、「**役割グループ**」ドロップダウン・リストにリストされている役割グループのみがそのデバイスにデフォルトでアクセスできます。

ステップ 6. 「**保存**」をクリックします。

セキュアな環境の実装

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

このタスクについて

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

環境のセキュリティー要件を評価する際、以下の情報を考慮してください。

- 環境の物理的セキュリティーは重要です。システム管理ハードウェアが置かれている部屋およびラックの利用を制限してください。
- ウィルスや無許可アクセスなどの既知および新しいセキュリティー脅威からネットワーク・ハードウェアおよびデータを保護するために、ソフトウェア・ベースのファイアウォールを使用してください。
- ネットワーク・スイッチとパススルー・モジュールのデフォルトのセキュリティー設定は変更しないでください。これらのコンポーネントの工場出荷時のデフォルト設定により、非セキュア・プロトコルが使用不可になり、署名付きファームウェア更新の要件が有効になります。
- CMM、ベースボード管理コントローラー、FSP、およびスイッチの管理アプリケーションは、これらのコンポーネントの署名付きファームウェア更新パッケージのみを許可して、確実に信頼できるファームウェアのみがインストールされるようにします。
- ファームウェア・コンポーネントの更新を許可されているユーザーのみがファームウェア更新権限を持つようにしてください。
- 少なくとも、重要なファームウェア更新が必ずインストールされるようにしてください。変更を行った後は必ず構成をバックアップしてください。
- DNS サーバーのセキュリティー関連の更新がすべて速やかにインストールされ、最新状態に維持されるようにしてください。
- ユーザーに、非トラステッド証明書を受け入れないように指示してください。詳しくは、セキュリティー証明書の使用を参照してください。
- Flex System ハードウェアで改ざん防止オプションを使用できます。ハードウェアが鍵の掛かっていないラックに取り付けられている場合、または開放されている場所に設置されている場合、侵入を防止して、識別するために、改ざん防止オプションを取り付けてください。改ざん防止オプションについての詳細は、Flex System 製品に付属の資料を参照してください。
- 実施可能であれば、システム管理ハードウェアを別のサブネット内に配置してください。一般的に、管理者のみがシステム管理ハードウェアにアクセスできるようにして、基本ユーザーにはアクセスを許可しないでください。
- パスワードを選択する際、簡単に推測できる語句 (たとえば、「password」または貴社名) は使用しないでください。パスワードを安全な場所で保管し、パスワードへのアクセスが制限されるようにしてください。貴社のパスワード・ポリシーを実装してください。

  重要：必ず、デフォルトのユーザー名とパスワードを変更してください。すべてのユーザーにストロング・パスワード規則の順守を要求する必要があります。
- サーバー上のデータおよびセットアップ・プログラムにアクセスできるユーザーを制御する方法として、ユーザーのパワーオン・パスワードを設定してください。始動パスワードについての詳細は、サーバーに付属の資料を参照してください。
- 環境内のさまざまなユーザーに対して使用できる多様な許可レベルを使用してください。すべてのユーザーに同じスーパーバイザー・ユーザー ID での処理を許可しないでください。
- セキュアな通信をサポートするために、環境で以下の NIST 800-131A の基準が満たされていることを確認してください。
  - TLS v1.2 プロトコルを介した Secure Sockets Layer (SSL) を使用する。
  - デジタル署名には SHA-256 以上の強度のハッシュ関数を使用し、その他の用途には SHA-1 以上の強度のハッシュ関数を使用する。

- RSA-2048、またはより強力な暗号を使用しているか、NIST が承認した 224 ビット以上の楕円曲線暗号を使用している。
- NIST が承認した対称鍵暗号で、鍵の長さが少なくとも 128 ビット以上のものを使用している。
- NIST が承認した乱数発生ルーチンを使用している。
- (可能な場合) Diffie-Hellman 鍵交換メカニズムまたは Elliptic Curve Diffie-Hellman 鍵交換メカニズム (あるいはこの両方) をサポートしている。

暗号化設定について詳しくは、管理サーバーでの暗号化設定の構成を参照してください。NIST 設定について詳しくは、NIST SP 800-131A コンプライアンスの実装を参照してください。

ユーザー・アカウントのセキュリティー設定の変更

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

手順

現在のユーザー・アカウントのセキュリティー設定を上書きするには、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 → 「セキュリティー」**をクリックします。

ステップ 2. 「ユーザーとグループ」セクションの「**アカウント・セキュリティー設定**」をクリックして、「ユーザー管理」ページを表示します。

ステップ 3. 以下の設定で必要に応じて新しい値を選択します。

表 1. アカウント・セキュリティー設定

セキュリティー設定	説明	使用できる値	デフォルト値
パスワードの有効期限	ユーザーが変更を求められることなくパスワードを使用できる期間 (日単位)。値を小さくすると、攻撃者がパスワードを推測する時間が少なくなります。 **0** に設定すると、パスワードは無期限になります。 **注：**この設定は、ユーザー・アカウントがローカル認証サーバーを使用して管理されている場合にのみ適用されます。外部認証サーバーが使用されている場合には使用されません。	0 - 365	90
パスワード失効の警告期間	ユーザー・パスワードの有効期間が満了する前に、期限が近づいていることを警告する通知をユーザーが最初に受け取るまでの期間 (日単位)。 **0** に設定すると、この警告はユーザーに通知されません。 **注：**この設定は、ユーザー・アカウントがローカル認証サーバーを使用して管理されている場合にのみ適用されます。外部認証サーバーが使用されている場合には使用されません。	0 ～ ***パスワード有効期間の最大値***	5
最短パスワード再利用サイクル	パスワードを変更する際、ユーザーが旧パスワードを再利用できるようになる前に、固有のパスワードを入力しなければならない最小回数 **0** に設定すると、パスワードをすぐに再利用できます。	0 - 10	5

表 1. アカウント・セキュリティー設定 (続き)

セキュリティー設定	説明	使用できる値	デフォルト値
最短パスワード変更期間	ユーザーがパスワードを変更した後、再度そのパスワードを変更できるようになるまでの最短時間 (時間単位)。この設定に、パスワードの有効期限の指定値を超える値を指定することはできません。 **0** に設定すると、すぐにパスワードを変更できます。	0 - 1440	24
最大ログイン失敗数	ユーザー・アカウントがロックアウトされる前に、ユーザーが正しくないパスワードでログインを試行できる最大回数。ログイン失敗が最大回数に達した後のロックアウト期間として指定する値は、ユーザー・アカウントがロックアウトされる期間を決定します。ロックされているアカウントは、有効なパスワードを入力しても、システムへのアクセスに使用できません。 **0** に設定すると、アカウントはロックされません。ログイン失敗のカウンターは、ログイン成功後、ゼロ (0) にリセットされます。	0 - 100	20
ログイン失敗が最大回数に達した後のロックアウト期間	ロックアウトされたユーザーが再びログインを試行できるようになるまでの最短時間 (分単位) **0** に設定すると、管理者が明示的にロックを解除するまで、アカウントはロックされたままになります。0 を設定した場合、故意にログイン試行を失敗してアカウントを永続的にロックさせることが可能になるため、システムは重大なサービス妨害攻撃の被害を受けやすくなります。 **ヒント**: スーパーバイザーの役割を持つユーザーなら誰でもユーザー・アカウントをロック解除できます。詳しくは、ユーザーのロック解除を参照してください。 **注：**この設定は、ユーザー・アカウントがローカル認証サーバーを使用して管理されている場合にのみ適用されます。外部認証サーバーが使用されている場合には使用されません。	0 - 2880	60
Web 非アクティブ・セッションのタイムアウト	XClarity Administrator との間で確立されたユーザー・セッションで操作が行われなくなってからユーザーがログアウトされるまでの時間 (分単位) **0** に設定すると、Web セッションは無期限になります。 **注：**この値を変更すると、設定の変更後に開始するユーザー・セッションのみが影響を受けます。	0 - 1440	1440
最小パスワード長	有効なパスワードの指定に使用できる最小文字数。	8 - 20	8

表 1. アカウント・セキュリティー設定 (続き)

セキュリティー設定	説明	使用できる値	デフォルト値
新しいパスワードの作成時に従う必要がある複雑性規則の数	新しいパスワードの作成時に従う必要がある複雑性規則の数 規則の適用は、規則 1 から、指定した規則数に至るまで行われます。たとえば、パスワードの複雑性が 4 に設定されている場合は、規則 1、2、3、および 4 に従う必要があります。パスワードの複雑性が 2 に設定されている場合は、規則 1 および 2 に従う必要があります。 XClarity Administrator では、以下のパスワード複雑性規則がサポートされています。 • (1) 1 つ以上の英字が含まれ、英字、数字、および QWERTY キーボードの連続を含めて、2 文字以上の連続が含まれない (「abc」、「123」、「asd」など)。 • (2) 少なくとも 1 つの数字 (0 - 9) が含まれていること。 • (3) 次の文字のうち、少なくとも *2* つが含まれる。 – 大文字の英字 (A – Z)。 – 子文字の英字 (a – z)。 – 特殊文字 ; @ _ ! ' $ & + • (4) ユーザー名の繰り返しや反転がないこと。 • (5) 2 つの同じ文字が連続していない (「aaa」、「111」、「...」など) こと。 0 に設定すると、パスワードは複雑性の規則に準拠する必要がなくなります。	0 – 5	4
特定ユーザーに対する最大アクティブ・セッション数	任意の時点で許可される特定ユーザーのアクティブ・セッションの最大数 0 に設定した場合、特定ユーザーに対して許可されるアクティブ・セッション数は無制限になります。	1 – 20	3
初回アクセス時にパスワードの変更をユーザーに強制する	ユーザーが XClarity Administrator へ初めてログインする場合、パスワードの変更をユーザーに求めるかどうかを指定します。	**はい**または**いいえ**	**はい**

ステップ 4. 「**適用**」をクリックします。

終了後

正常に保存された場合、新しい設定はすぐに有効になります。「Web 非アクティブ・セッションのタイムアウト」の設定を変更した場合は、アクティブ・セッションにも影響します。

パスワード・ポリシーを変更した場合は、ユーザーの次回のログインまたはパスワード変更から適用されます。

管理サーバーでの暗号化設定の構成

管理サーバーの SSL/TLS バージョンと暗号設定を構成できます。

始める前に

管理サーバーの設定修正前に暗号化の懸念事項を見直してください (XClarity Administratorオンライン・ドキュメントの「暗号管理」を参照)。

このタスクについて

*暗号モード*では、XClarity Administrator とすべての管理対象システムとの間でセキュアな通信をどのように処理するかが決定されます。セキュアな通信が実装されている場合、使用する暗号鍵の長さが設定されます。

注：選択した暗号モードに関係なく、NIST 認定のデジタル乱数生成器 (Digital Random Bit Generator) が常に使用され、128 ビット以上の鍵のみが対称暗号化に使用されます。

管理対象デバイスのセキュリティー設定を変更するには、管理対象サーバーのセキュリティー設定の構成 を参照してください。

手順

管理サーバーの暗号化設定を変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、**管理 → 「セキュリティー」**をクリックします。

ステップ 2. セキュアな通信に使用する暗号モードとして以下のいずれかを選択します。

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

  このモードを選択した場合:

  – ポート 8443 以外のすべてのポートでは、すべての TLS CBC 暗号および PFS (Perfect Forward Secrecy) をサポートしないすべての暗号が無効になります。

  – 一部のモバイル・デバイス・サブスクリプションでは、イベント通知が正常にプッシュされない可能性があります (モバイル・デバイスへのイベントの転送を参照)。Android や iOS などの外部デバイスは、SHA-1 (NIST SP 800-131A モードのより厳しい要件に従わないアルゴリズム) で署名された証明書を提示します。その結果、これらのサービスに対して行われる接続が、証明書例外またはハンドシェーク・エラーで失敗する可能性があります。

  NIST SP 800-131A への準拠について詳しくは、NIST SP 800-131A コンプライアンスの実装を参照してください。

ステップ 3. クライアントを他のサーバー (LDAP サーバーなど) に接続するために使用する TLS プロトコルの最小バージョンを選択します。以下のオプションを選択できます。

- **TLS1.2**。TLS v1.2 暗号化プロトコルを強制適用します。
- **TLS1.3**。TLS v1.3 暗号化プロトコルを強制適用します。

ステップ 4. サーバー接続 (Web サーバーなど) に使用する TLS プロトコルの最小バージョンを選択します。以下のオプションを選択できます。

- **TLS1.2**。TLS v1.2 暗号化プロトコルを強制適用します。
- **TLS1.3**。TLS v1.3 暗号化プロトコルを強制適用します。

ステップ 5. XClarity Administrator オペレーティング・システムのデプロイメントおよび OS デバイス・ドライバーの更新に使用される TLS プロトコルの最小バージョンを選択します。以下のオプションを選択できます。

- **TLS1.2**。TLS v1.2 暗号化プロトコルを強制適用します。
- **TLS1.3**。TLS v1.3 暗号化プロトコルを強制適用します。

注：XClarity Administrator でデプロイおよび更新できるのは、選択済みの、または強い暗号化アルゴリズムをサポートしているオペレーティング・システムのみです。

ステップ 6. 証明書のすべての部分 (ルート CA 証明書、サーバー証明書、外部署名済み証明書の CSR など) に使用する暗号鍵の長さとハッシュ・アルゴリズムを選択します。

- **RSA 2048 ビット / SHA-256** (デフォルト)

  このモードは、管理対象デバイスが「互換性」、「NIST SP 800-131A」、または「標準セキュリティ」モードの場合に使用できます。1 つ以上の管理対象デバイスが「**エンタープライズ・ストリクト・セキュリティー**」モードになっている場合、このモードを使用することは *できません*。

- **RSA 3072 ビット/SHA-384**

  このモードは、「**エンタープライズ・ストリクト・セキュリティー**」モードの管理対象デバイスの場合に必要です。

  重要：RSA-3072/SHA-384 証明書署名は、XCC2 を持つサーバーでのみサポートされています。RSA-3072/SHA-384 ベースの証明書を使用して XClarity Administrator を構成すると、非 XCC2 デバイスは管理を解除されます。非 XCC2 デバイスを管理するには、別の XClarity Administrator インスタンスが必要です。

ステップ 7. 「**適用**」をクリックします。

ステップ 8. XClarity Administrator を再起動します (XClarity Administratorの再起動を参照)。

ステップ 9. 暗号鍵の長さを変更した場合は、正しい鍵の長さとハッシュ・アルゴリズムを使用して証明機関ルート証明書を再生成します (「Lenovo XClarity Administrator の自己署名サーバー証明書の再生成または復元」または「カスタマイズされたサーバー証明書の Lenovo XClarity Administrator へのデプロイ」を参照)。

終了後

管理対象デバイスでサーバー証明書が非トラステッドであるとアラートを受信した場合は、非トラステッド・サーバー証明書の解決を参照してください。

管理対象サーバーのセキュリティー設定の構成

管理対象サーバーの SSL/TLS バージョンおよび暗号設定を構成できます。

このタスクについて

暗号モードを変更する際の考慮事項を以下に示します。

- 「**互換性セキュリティー**」モードまたは「**標準セキュリティー**」モードから「**エンタープライズ・ストリクト・セキュリティー**」モードへの変更はサポートされていません。
- 「**互換性セキュリティー**」モードから「**標準セキュリティー**」モードにアップグレードする場合、インポートされた証明書または SSH 公開鍵が適合しない場合に警告が表示されますが、「**標準セキュリティー**」モードにアップグレードすることはできます。
- 「**エンタープライズ・ストリクト・セキュリティー**」モードから「**互換性セキュリティー**」モードまたは「**標準セキュリティー**」モードにダウングレードする場合:
  - セキュリティー・モードを有効にするために、サーバーが自動的に再起動されます。

– Strict モードの FoD キーが XCC2 で欠落しているか有効期限が切れている場合、および XCC2 が自己署名 TLS 証明書を使用する場合、XCC2 は Standard Strict に準拠するアルゴリズムに基づいて自己署名証明書を再生成します。XClarity Administrator は、証明書エラーによる接続障害を表示します。信頼できない証明書のエラーを解決するには、XClarity Administrator オンライン・ドキュメントの「非トラステッド・サーバー証明書の解決」を参照してください。XCC2 がカスタム TLS 証明書を使用する場合、XCC2 はダウングレードを許可し、「**標準セキュリティー**」モードの暗号化に基づいてサーバー証明書をインポートする必要があるという警告が表示されます。

- 「NIST SP 800-131A」モードは、XCC2 を持つサーバーではサポートされていません。
- XClarity Administrator の暗号モードが TLS v1.2 に設定され、管理対象認証を使用する管理対象サーバーのセキュリティー・モードが TLS v1.2 に設定されている場合、XClarity Administrator または XCC のいずれかを使用してサーバーのセキュリティー・モードを TLS v1.3 に変更すると、サーバーは永続的にオフラインになります。
- XClarity Administratorの暗号モードが TLS v1.2 に設定され、セキュリティー・モードが TLS v1.3 に設定されている XCC を使用してサーバーを管理しようとしても、管理対象認証を使用してサーバーを管理することはできません。

次のデバイスのセキュリティー設定は変更できます。
- インテルまたは AMD プロセッサーを搭載した Lenovo ThinkSystem サーバー (SR635 / SR655 を除く)
- Lenovo ThinkSystem V2 サーバー
- インテルまたは AMD プロセッサーを搭載した Lenovo ThinkSystem V3 サーバー
- Lenovo ThinkEdge SE350 / SE450 サーバー
- Lenovo System x サーバー

手順

固有の管理対象サーバーのセキュリティー設定を変更するには、以下の手順を完了します。

ステップ 1. XClarity Administrator のメニューで、「**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がテーブル・ビューで表示されます。

ステップ 2. 1 つ以上のサーバーを選択します。

ステップ 3. セキュリティー・モードを構成する。

1. 「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**システム・セキュリティー・モードの設定**」をクリックして、「システム・セキュリティー・モードの設定」ダイアログを表示します。

   ダイアログには、各モードに設定できるサーバーの数がリストされています。各番号の上にカーソルを置き、該当するサーバー名のリストをポップアップで表示します。

2. セキュリティ・モードを選択します。これは以下のいずれかの値です。

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

     このモードは、XCC2 を持つサーバーではサポートされて*いません*。
   - **標準セキュリティー**。(XCC2 を持つサーバーのみ) これは、XCC2 を含むサーバーのデフォルトのセキュリティー・モードです。FIPS 140-3 基準に確実に準拠するには、このモードを選択してください。XCC を FIPS 140-3 検証モードで動作させるには、FIPS 140-3 レベルの暗号化をサポートするサービスのみが有効にできます。FIPS

140-2/140-3 レベル暗号化をサポートしないサービスは、デフォルトでは無効になっていますが、必要な場合は有効にできます。FIPS 140-3 レベル以外の暗号化を使用するサービスが有効になっている場合、XCC は FIPS 140-3 検証モードでは動作できません。このモードでは、FIP レベルの証明書が必要です。

- **エンタープライズ・ストリクト・セキュリティー**。(XCC2 を含むサーバー のみ) これは、最もセキュアなモードです。CNSA 基準に確実に準拠するには、このモードを選択してください。CNSA レベルの暗号化をサポートするサービスのみ使用できます。非セキュア・サービスは、デフォルトでは無効になっており、有効にすることはできません。このモードでは、CNSA レベルの証明書が必要です。

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

  重要：

  – このモードを使用するには、選択したそれぞれの XCC2 を含むサーバー に XCC2 Feature On Demand キーがインストールされていなければなりません。

  – このモードで XClarity Administrator が自己署名証明書を使用する場合は、XClarity Administrator は RSA3072/SHA384 ベースのルート証明書とサーバー証明書を使用する必要があります。XClarity Administrator が外部署名済み証明書を使用する場合は、XClarity Administrator は RSA3072/SHA384 ベースの CSR を生成し、外部 CA に問い合わせ、RSA3072/SHA384 に基づく新しいサーバー証明書に署名する必要があります。

  – XClarity Administrator が RSA3072/SHA384 ベースの証明書を使用する場合、XClarity Administrator は Flex System シャーシ (CMMS) サーバーおよびサーバー、ThinkSystem サーバー、ThinkServer サーバー、System x M4 および M5 サーバー、Lenovo ThinkSystem DB シリーズ・スイッチ、Lenovo RackSwitch、Flex System スイッチ、Mellanox スイッチ、ThinkSystem DE/DM ストレージ・デバイス、IBM テープ・ライブラリー・ストレージ、および 22C 以前のファームウェアがフラッシュされた ThinkSystem SR635/SR655 サーバー以外のデバイスを切断する可能性があります。切断されたデバイスの管理を続行するには、RSA2048/SHA384 ベースの証明書を使用して別の XClarity Administrator インスタンスをセットアップしてください。

3. 「**適用**」をクリックします。

ステップ 4. TLS の最小バージョンを構成します。

1. 「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**システム TLS バージョンの設定**」をクリックして、「システム TLS バージョンの設定」ダイアログを表示します。
2. クライアントを他のサーバーに接続するために使用する TLS プロトコルの最小バージョンを選択します (LDAP クライアントから LDAP サーバーへの接続など)。この値は、この設定をサポートする選択済みのデバイスで構成されます。以下のオプションを選択できます。

   - TLS1.2。TLS v1.2 暗号化プロトコルを強制適用します。
   - TLS1.3。TLS v1.3 暗号化プロトコルを強制適用します。

   注：System x および CMM デバイスがサポートするのは TLS v1.2 のみです。

3. 「**適用**」をクリックします。

セキュリティー証明書の使用

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

始める前に

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

このタスクについて

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

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

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

XClarity Administrator は、管理対象デバイスおよび外部サービスと通信する場合はクライアントとして機能します。XClarity Administrator がデバイスや外部サービスに接続する場合、デバイスや外部サービスはそのサーバー証明書を XClarity Administrator に提示して識別させます。XClarity Administrator は信頼できる証明書のリストを保持します。管理対象デバイスまたは外部サービスが提供する *トラステッド証明書*がリストに含まれていない場合、機密性の高い情報を信頼できないソースとやりとりすることを避けるために、XClarity Administrator は管理対象デバイスまたは外部サービスから切断されます。

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

- **サーバー証明書**。初期ブート時に、固有のキーと自己署名証明書が生成されます。これらはデフォルトのルート証明機関として使用され、XClarity Administrator のセキュリティー設定の「証明機関」ページで管理できます。キーが漏えいした場合や、組織にすべての証明書を定期的に交換しなければならないというポリシーがある場合を除いて、このルート証明書を再生成する必要はありません (Lenovo XClarity Administrator の自己署名サーバー証明書の再生成または復元 を参照)。

  また、初期セットアップ中に別のキーが生成され、内部の証明機関によって署名された別のサーバー証明書が作成されます。この証明書は、デフォルトのXClarity Administrator サーバー証明書として使用されます。これは、XClarity Administrator でネットワーク・アドレス (IP または DNS アドレス) の変更が検出されるたびに再生成され、証明書にサーバーの正しいアドレスが含まれるようになります。この証明書はカスタマイズでき、オンデマンドで生成できます (Lenovo XClarity Administrator の自己署名サーバー証明書の再生成または復元参照)。

  デフォルトの自己署名サーバー証明書の代わりに外部署名済みサーバー証明書を使用することもできます。これには、証明書署名要求 (CSR) を生成し、プライベートまたは商用の証明書のルート証明機関によって CSR に署名して、すべての証明書チェーンを XClarity Administrator にインポートします (カスタマイズされたサーバー証明書の Lenovo XClarity Administrator へのデプロイ を参照)。

デフォルトの自己署名サーバー証明書を使用する場合は、Web ブラウザーに証明書のエラー・メッセージが表示されないようにするために、信頼できるルート証明機関としてサーバー証明書を Web ブラウザーにインポートすることをお勧めします (Web ブラウザーへの証明機関証明書のインポート を参照)。

- **OS デプロイ証明書**。オペレーティング・システム・デプロイメント・サービスでは、別の証明書が使用されます。これは、オペレーティング・システムのインストーラーがオペレーティング・システムのインストール・プロセス中にデプロイメント・サービスに確実に接続するためのものです。キーが暗号漏えいした場合は、管理サーバーを再起動することで再生成できます。

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

- **トラステッド証明書**。

  この信頼ストアは、XClarity Administrator がクライアントとして機能する場合に、ローカルのリソースへの安全な接続を確立するために使用する証明書を管理します。ローカルのリソースの例には、管理対象デバイス、イベント転送時のローカルのソフトウェア、外部 LDAP サーバーなどがあります。

- **外部サービス証明書**。この信頼ストアは、XClarity Administrator がクライアントとして機能する場合に、外部サービスへの安全な接続を確立するために使用する証明書を管理します。外部サービスの例には、保証情報の取得やサービス・チケットの作成に使用するオンラインの Lenovo サポートのサービス、イベントを転送できる外部ソフトウェア (Splunk など)、iOS デバイスや Android デバイスで Lenovo XClarity Mobile のプッシュ通知を有効にしている場合の Apple や Google のプッシュ通知サーバーなどがあります。これには、一般によく知られている信頼できる特定の証明機関プロバイダー (Digicert や Globalsign など) のルート証明機関の事前に設定されたトラステッド証明書が含まれます。

  別の外部サービスへの接続を必要とする機能を使用するように XClarity Administrator を設定する場合は、資料を参照して、この信頼ストアに手動で証明書を追加する必要があるかどうかを確認してください。

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

XClarity Administrator は、RSA-3072/SHA-384、RSA-2048/SHA-256、ECDSA p256/SHA-256 証明書の署名をサポートします。SHA-1 ストロングや SHA ハッシュなどのアルゴリズムは、構成によってはサポートされる場合もあります。XClarity Administrator で選択されている暗号モード (「管理サーバーでの暗号化設定の構成」を参照)、管理対象サーバーで選択されているセキュリティ設定 (管理対象サーバーのセキュリティー設定の構成)、および環境内のその他のソフトウェアとデバイスの機能を検討してください。すべての楕円曲線ではなく一部の楕円曲線 (p256 含む) に基づいた ECDSA 証明書は、「トラステッド証明書」ページおよび XClarity Administrator 証明書の署名チェーンでサポートされていますが、XClarity Administrator サーバー証明書での使用は現在サポート *されていません*。

注：XClarity Administrator は、Strict モードでは、XCC2 を含むサーバー に RSA- 3072/SHA-384 証明書の署名を使用します。

カスタマイズされた外部署名済みサーバー証明書のインストール

プライベートまたは商用証明機関 (CA) によって署名されたサーバー証明書を使用できます。

始める前に

ルート証明機関が、所属する組織によって作成されていて組織内の証明書に署名するために使用されているか、一般によく知られている信頼できる証明機関であることを確認します (信頼できる証明機関のリスト Web ページ を参照)。

ルート証明機関の証明書のキーと署名のアルゴリズムがサポートされていることを確認します。RSA-3072/SHA-384 および RSA-2048/SHA-256 署名のみがサポートされています。現時点では、RSA-PSS 署名はサポートされていません。

管理対象デバイス間の接続に影響する可能性があるタスクを開始する前に、すべての管理対象デバイスに、最新の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。管理対象デバイスでファームウェアをアップグレードするには、管理対象デバイスでのファームウェアの更新を参照してください。

「**ハードウェア**」をクリックしデバイス・タイプ (シャーシまたはサーバー) をクリックして、XClarity Administrator がすべての管理対象デバイスと正常に通信していることを確認します。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。ステータスが「オフライン」なっているデバイスがある場合は、管理サーバーとそのデバイス間のネットワーク接続性が機能していることを確認し、必要な場合は非トラステッド証明書を解決します (非トラステッド・サーバー証明書の解決参照)。

このタスクについて

カスタマイズされた外部署名済みサーバー証明書を XClarity Administrator またはベースボード管理コントローラーや CMM にインストールする場合は、CA 署名チェーン全体が含まれる証明書バンドルを指定する必要があります。

カスタマイズされたサーバー証明書を、XClarity Administrator で管理されていないシャーシまたはサーバーにインストールする場合は、CMM で証明書バンドルをインストールしてから、その CMM のすべての管理コントローラーで証明書をインストールします。

カスタマイズされたサーバー証明書を管理対象シャーシにインストールする場合は、まず、CA 署名チェーンを XClarity Administrator 信頼ストアに追加し、サーバー証明書をすべての管理コントローラーと CMM にインストールしてから、サーバー証明書を XClarity Administrator にアップロードします。これは、すべての管理対象デバイスのすべての証明書チェーンの代わりに、すべてのルート証明機関の証明書を信頼/追加することで簡単に迅速化できます。インポートする証明書の数は、ルート証明機関の証明書の数 (ルート証明機関の証明書 + すべての中間証明機関の証明書) と同じである必要があります。詳しくは、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してください。

CA ルート証明書とすべての中間証明書を、XClarity Administrator 信頼ストアに 1 つずつ追加する必要があります。順番は重要ではありません。各証明書のインストールは 1 回のみです。したがって、すべてのデバイスが同じ CA および中間証明書を使用する場合は、その CA および中間証明書を一度に XClarity Administrator の信頼ストアにインストールする必要があります。複数の CA または中間 CA を使用する場合、管理対象デバイスの署名チェーンで使用される各固有 CA ルート証明書または中間証明書が、以下の手順でインポートされていることを確認します。

ヒント: 新しいサーバー証明書がトラステッド・サード・パーティーによって署名されていない場合は、次に XClarity Administrator に接続したときにブラウザーにセキュリティー・メッセージが表示されて、新しい証明書を承認するかどうかをたずねられます。このセキュリティー・メッセージが表示されないようにするには、サーバー証明書をダウンロードして、Web ブラウザーのトラステッド証明書のリストにインポートします。サーバー証明書のインポートについて詳しくは、Web ブラウザーへの証明機関証明書のインポートを参照してください。

カスタマイズされたサーバー証明書の Lenovo XClarity Administrator へのデプロイ

所属組織の証明機関またはサード・パーティーの証明機関に署名を要求する証明書署名要求 (CSR) を生成するように選択できます。CSR は、完全な証明書チェーンを作成します。これをインポートし、固有のデフォルトの内部署名済み証明書の代わりに使用できます。

始める前に

証明書の詳細に以下の要件が含まれていることを確認します。

- キー使用法には以下が含まれている必要があります。
  - キーの承諾
  - デジタル署名
  - キーの暗号化

- 拡張キー使用法には、以下の情報が含まれている必要があります。
  - サーバー認証 (1.3.6.1.5.5.7.3.1)
  - クライアント認証 (1.3.6.1.5.5.7.3.2)

このタスクについて

注意：NIST SP 800-131Aが有効になっている場合 (NIST SP 800-131A コンプライアンスの実装を参照)、NIST でカスタム証明書または外部署名証明書を使用しているか、または使用する予定の場合、チェーン内のすべての証明書は SHA-256 ハッシュ関数に基づいている必要があります。

サーバー証明書がアップロードされると、XClarity Administrator によってすべての管理対象デバイスに新しい CA 証明書がプロビジョニングされます。プロビジョニング・プロセスが成功した場合、XClarity Administrator は新しいサーバー証明書をすぐに使用し始めます。プロセスが失敗した場合、新しくインポートしたサーバー証明書を適用する前に問題を手動で修正するため、エラー・メッセージが直接お客様に送信されます。エラーが修正されてから、以前にアップロードされた証明書のインストールを実行してください。

注：XClarity Administrator がすでに同じルート証明機関が署名する証明書を使用している場合、CA をデバイスに送信する必要はなく、XClarity Administrator はすぐに証明書を使用し始めます。

XClarity Administrator v1.1.0 以前にサーバー証明書のアップロードされると、Web サーバーが再起動し、すべてのブラウザー・セッションは自動的に終了します。XClarity Administrator v1.1.1 以降では、既存のセッションを終了せずに新しい証明書を使用し始めます。新規セッションはすべて新しい証明書を使用して確立されます。使用中の新しい証明書を表示するには、Web ブラウザーを再起動します。

手順

Lenovo 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およびデプロイするには、以下のステップを実行します。

ステップ 1. XClarity Administrator の証明書署名要求 (CSR) を生成およびダウンロードします。

a. XClarity Administrator メニュー・バーで、「**管理**」 → 「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。

b. 「サーバー証明書」ページを表示するには、「証明書の管理」セクションで「**サーバー証明書**」をクリックします。

c. 「**証明書署名要求 (CSR) の生成**」タブをクリックします。

d. 要求の各フィールドに入力します。
   - 国または地域
   - 都道府県
   - 市区町村または地域
   - 組織
   - 組織単位 (オプション)
   - 共通名

   注意： XClarity Administrator が管理対象デバイスに接続するときに使用する IP アドレスまたはホスト名と一致する共通名を選択します。正しい値を選択しないと、信頼できない接続が発生する可能性があります。

e. CSR の生成時に X.509「subjectAltName」拡張に追加されるサブジェクト代替名 (SAN) をカスタマイズします。

   デフォルトでは、XClarity Administrator のゲスト・オペレーティング・システムのネットワーク・インターフェースによって検出された IP アドレスおよびホスト名に基づいて、XClarity Administrator が CSR のサブジェクト代替名 (SAN) を自動的を定義します。この SAN 値のカスタマイズ、削除、または SAN 値への追加を行うことができます。

指定する名前は、選択したタイプで有効であることが必要です。
- **directoryName** (例: `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (例: `lxca-example.dcg.company.com`)
- **ipAddress** (例: `192.0.2.0`)
- **registeredID** (例: `1.2.3.4.55.6.5.99`)
- **rfc822Name** (例: `example@company.com`)
- **uniformResourceIdentifier** (例: `https://lxca-dev.dcg.company.com/example`)

注：表に示されているすべての SAN は、次の手順で CSR を生成した後でのみ、検証、保存され、CSR に追加されます。

f. 「**CSR ファイルの生成**」をクリックします。サーバー証明書が「証明書署名要求」ダイアログに表示されます。

g. 「**ファイルに保存**」をクリックして、サーバー証明書をホスト・サーバーに保存します。

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

ステップ 3. 外部署名済みサーバー証明書を XClarity Administrator にアップロードします。証明書は CA のルート証明書、中間証明書およびサーバー証明書を含むバンドルでなければなりません。

a. XClarity Administrator メニュー・バーで、**管理 ➡ 「セキュリティー」**をクリックして、「セキュリティー」ページを表示します。

b. 「証明書の管理」セクションで「**サーバー証明書**」をクリックします。

c. 「**証明書のアップロード**」タブをクリックします。

d. 「**証明書のアップロード**」をクリックして、「証明書のアップロード」ダイアログを表示します。

e. PEM、DER または PKCS7 形式の証明書バンドル・ファイルを指定するか、PEM 形式の証明書バンドルを貼り付けます。

f. 「**アップロード**」をクリックしてサーバー証明書をアップロードし、証明書を XClarity Administrator 信頼ストアに保管します。

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

カスタマイズされたサーバー証明書を管理対象デバイスにデプロイするには、そのデバイスの CMM と管理コントローラーを使用して、外部署名された証明書バンドルをアップロードおよびインストールします。

始める前に

すべての管理対象デバイスに最新の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 (管理対象デバイスでのファームウェアの更新を参照)。

カスタム証明書の証明書署名要求 (CSR) を生成するときに、デバイスを特定する際に使用される IP アドレスまたはホスト名と一致する共通名を選択してください。正しい値を選択しないと、信頼できない接続が発生する可能性があります。

トラステッド CA のエンド・サーバー証明書からルート (ベース) 証明書まで、署名チェーン全体が含まれる証明書バンドルを取得してください。これは、信頼できる完全な証明書チェーンを確認するときに使用できます。

管理対象デバイスが「オフライン」中は、Lenovo XClarity Administrator サーバー証明書を変更しないでください。Lenovo XClarity Administrator を変更する前に接続を修復してください。そうしないと、接続の問題を修復するために追加手順が必要になる場合があります (非トラステッド・サーバー証明書の解決参照)。

このタスクについて

このセクションには、Lenovo XClarity Administrator と管理対象デバイス間の正常な通信を継続して確保するための推奨事項が含まれています。CSR の生成方法および署名済み証明書のインポート方法の詳細な手順については、デバイスの資料を参照してください。

Lenovo XClarity Administrator で 1 つ以上のシャーシ、ラック・サーバー、タワー・サーバーが管理され、デフォルトの Lenovo XClarity Administrator 内部署名済み証明書が Lenovo XClarity Administrator と管理対象デバイスにインストールされている場合は、カスタマイズされたサーバー証明書をデプロイできます。

Lenovo XClarity Administrator でデバイスを管理する *前に* 外部署名済みサーバー証明書がデバイスにインストールされている場合は、追加手順は必要ありません。Lenovo XClarity Administrator 管理下の管理対象デバイスにカスタム・サーバー証明書をデプロイするには、以下のいずれかの手順を実行して管理サーバーと管理対象デバイス間の接続を継続して維持する必要があります。

手順

カスタマイズされた外部署名済みサーバー証明書を、管理対象シャーシまたはサーバーにインポートするには、以下のいずれかのオプションを実行します。

- Lenovo XClarity Administrator で使用する証明書の署名が管理対象デバイスの証明機関と同じである場合は、管理対象デバイスに証明書をインストールする *前に*、カスタマイズされたサーバー証明書の Lenovo XClarity Administrator へのデプロイ で以下の手順を実行します。同じ CA からの Lenovo XClarity Administrator 証明書チェーンをインストールする場合は、最初に Lenovo XClarity Administrator 信頼ストアに証明書チェーンがあり、デバイスに外部署名済み証明書がインストールされた後に Lenovo XClarity Administrator でそのデバイスが信頼できるようにします。
- CA 署名チェーンの外部署名済み証明書を Lenovo XClarity Administrator 信頼ストアに追加します。

  CA ルート証明書とすべての中間証明書を、Lenovo XClarity Administrator 信頼ストアに 1 つずつ追加する必要があります。順番は重要ではありません。各証明書のインストールは 1 回のみです。したがって、すべてのデバイスが同じ CA および中間証明書を使用する場合は、その CA および中間証明書を一度に Lenovo XClarity Administrator の信頼ストアにインストールする必要があります。複数の CA または中間 CA を使用する場合、管理対象デバイスの署名チェーンで使用される各固有 CA ルート証明書または中間証明書が、以下の手順でインポートされていることを確認します。

  注： この手順では、エンド証明書となる非 CA サーバー証明書は追加しないでください。

  バンドルの証明書ごとに、以下の手順を実行します。

  1. Lenovo XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。
  2. 左側のナビゲーションで、「証明書の管理」の「**トラステッド証明書**」をクリックします。
  3. 「**作成**」アイコン () をクリックして、「証明書の追加」ダイアログを表示します。
  4. PEM または DER 形式の証明書ファイルを指定するか、PEM 形式の証明書を貼り付けます。
  5. 「**作成**」をクリックして、証明書を作成します。

  CA 署名チェーンがインストールされると、Lenovo XClarity Administrator は、外部署名されたサーバー証明書がインストールされている、CMM および管理コントローラー上の CIM サーバーへの接続を信頼します。
- 外部署名済み証明書を管理対象デバイスにインポートします。

  注： 必要な証明書が Lenovo XClarity Administrator 信頼ストア内にない場合、Lenovo XClarity Administrator と管理対象デバイス間の接続が失われます。非トラステッド・サーバー証明書の解決の手順を実行して接続を修復してください。

  重要： このオプションでは、一時的に接続が失われます。そのため、前記のいずれかのオプションが推奨されます。

Lenovo XClarity Administrator の自己署名サーバー証明書の再生成または復元

新しい証明機関またはサーバー証明書を生成して、現在の自己署名証明書を置き換えるか、現在 XClarity Administrator でカスタマイズされた外部署名済みサーバー証明書を使用している場合は Lenovo XClarity Administrator で生成された証明書を復元できます。新しい自己署名サーバー証明書は、XClarity Administrator で認証サーバー、HTTPS サーバー、CIM サーバーによって使用されます。また、すべての管理対象デバイスに自動的にプロビジョニングされます。

始める前に

XClarity Administrator 証明書を再生成またはアップロードすると、XClarity Administrator が再起動します。

新しい CA 証明書が生成されると、自動的にすべての管理対象シャーシ、ラック・サーバー、およびタワー・サーバーの各 CMM およびベースボード管理コントローラーにある信頼ストアにデプロイされ、トラステッド認証サーバーの接続は維持されます。CA ルート証明書のデプロイ中にエラーが発生した場合は、新しいサーバー証明書を生成する前に、証明機関ページから証明書をダウンロードして、正常にプロビジョニングされなかったすべての管理対象デバイスの信頼ストアに手動でインポートします。

CA 証明書を再生成する場合は、CA を再生成する時間を予約してプロビジョニングのエラーを解決し、すぐにサーバー証明書を再生成します。

新しい CA ルート証明書を生成すると、サーバー証明書が再生成されて署名されるまで、通信エラーが発生したり、デバイスにログインできなくなったりする場合があります。

重要：XClarity Administrator v1.1.1 以降の場合は、CA ルート証明書を各 CMM および管理コントローラーの信頼ストアにインポートする必要があります。CA ルート証明書のインポートの詳細については、CMM および管理コントローラーのドキュメントを参照してください。

手順

自己署名サーバー証明書を XClarity Administrator で復元するには、以下の手順を実行します。

注：XClarity Administrator で現在使用されているサーバー証明書は、自己署名であるか外部署名であるかにかかわらず、新しいサーバー証明書が再生成されて署名されるまで使用されます。

ステップ 1. **オプション**: 新しい CA ルート証明書を生成します。

a. XClarity Administrator メニュー・バーで、**管理 → 「セキュリティー」**をクリックして、「セキュリティー」ページを表示します。

b. 「証明書の管理」セクションで「**証明機関**」をクリックします。

c. 「**証明機関ルート証明書の再生成**」をクリックします。

CA の鍵および証明書が正常に生成されると、その証明書を LDAP トラステッド証明書としてすべての CMM および管理コントローラー (コンバージド、NeXtScale、および System x サーバー) にプロビジョニングするジョブのステータスを示すダイアログが表示されます。このダイアログおよびジョブ監視ページに、これらのプロビジョニング・ジョブそれぞれの成功または失敗が表示されます。

プロビジョニング・ジョブが失敗した場合は、以下の手順を実行して CA ルート証明書をダウンロードし、ジョブが失敗したデバイスにトラステッド LDAP 証明書として手動でインポートします。

ステップ 2. **オプション**: ホスト・システムに CA ルート証明書をダウンロードして Web ブラウザーにインポートします。

a. XClarity Administrator メニュー・バーで、**管理 → 「セキュリティー」**をクリックして、「セキュリティー」ページを表示します。

b. 「証明書の管理」セクションで「**証明機関**」をクリックします。

c. 「**証明機関ルート証明書のダウンロード**」をクリックします。現在の CA ルート証明書が「証明機関ルート証明書」ダイアログに表示されます。

d. 「**ファイルに保存**」をクリックして、CA ルート証明書をホスト・システムに保存します。

e. ご使用の Web ブラウザーまたは XClarity Administrator にアクセスする他のユーザーの Web ブラウザーの指示に従って、証明書をトラステッド・ルート証明機関としてインポートします。

ステップ 3. 新しいサーバー証明書を再生成し、新しい CA ルート証明書を使用してその証明書に署名します。

a. 「セキュリティー」ページの「証明書の管理」セクションで、「**サーバー証明書**」をクリックします。

b. 「**サーバー証明書の再生成**」タブをクリックします。

c. 「サーバー証明書の再生成」ページの各フィールドに入力します。
- 国または地域
- 都道府県
- 市区町村または地域
- 組織
- 組織編成
- 共通名
- 有効期間の開始日
- 有効期間の開始時刻
- 有効期間の終了日
- 有効期間の終了時刻

d. 「**証明書の再生成**」をクリックします。

e. 管理対象 CMM および管理コントローラー (コンバージド、NeXtScale、ThinkSystem、および System x サーバーの場合) で自己署名証明書を再生成する場合、各デバイスで証明書を再生成した後、新しいデバイス証明書を XClarity Administrator 信頼ストアにインポートします (非トラステッド・サーバー証明書の解決を参照)。または、デバイスから手動で証明書をダウンロードし、「トラステッド証明書」ページで XClarity Administrator にインポートできます。

XClarity Administrator v1.1.0 以前の場合は、証明書を再生成した後、Web サーバーが再起動し、すべてのブラウザー・セッションが自動的に終了します。XClarity Administrator v1.1.1 以降の場合は、既存のセッションを終了することなく、XClarity Administrator で新しい証明書の使用が始まります。新規セッションは新しい証明書を使用して確立されます。使用中の新しい証明書を表示するには、Web ブラウザーを再起動します。

ステップ 4. 管理対象 CMM および管理コントローラー (コンバージド、NeXtScale、ThinkSystem、および System x サーバーの場合) で自己署名証明書を再生成する場合、各デバイスで証明書を再生成した後、新しいデバイス証明書を XClarity Administrator 信頼ストアにインポートします (非トラステッド・サーバー証明書の解決を参照)。または、デバイスから手動で証明書をダウンロードし、「トラステッド証明書」ページで XClarity Administrator にインポートできます。

非トラステッド・サーバー証明書の解決

管理対象デバイスへのセキュアな接続を確立するために使用されるサーバー証明書は、信頼できなくなる場合があります。Lenovo XClarity Administrator 信頼ストアのデバイス CA ルート証明書またはデバイス自己証明証明書が下位レベル・バージョンであることが問題の原因の場合、XClarity Administrator は、非トラステッド・サーバー証明書を解決できます。

このタスクについて

管理対象デバイスが信頼できなくなると、XClarity Administrator では、そのデバイスと通信できなくなり、そのデバイスでは、管理またはインベントリー操作を行うことができません。

手順

管理対象デバイスの非トラステッド・サーバー証明書を解決するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで「**ハードウェア**」をクリックし、デバイス・タイプ (「**シャーシ**」、「**サーバー**」、「**ストレージ**」、または「**スイッチ**」) 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。

ステップ 2. 「オフライン」状態の特定のデバイスを選択します。

ステップ 3. 「**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。

ステップ 4. 「**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・デバイスから取得します。その証明書と、XClarity Administrator の信頼ストアにあるそのデバイスのトラステッド証明書が異なると、新しい証明書は XClarity Administrator 信頼ストアに配置され、そのデバイスの前の証明書をオーバーライドします。

この問題が解決しない場合は、ネットワーク接続が XClarity Administrator とデバイス間で動作していることを確認します。

サーバー証明書のダウンロード

ローカル・システムに現在のサーバーの証明書のコピーを、PEM/DER形式でダウンロードできます。Web ブラウザーまたは別のアプリケーションに証明書をインポートできます (Lenovo XClarity Mobile や Lenovo XClarity Integratorなど)。

手順

サーバー証明書を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. Lenovo XClarity Administrator メニュー・バーで、**管理** → 「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。

ステップ 2. 「証明書の管理」セクションで「**サーバー証明書**」をクリックします。「サーバー証明書」ページが表示されます。

ステップ 3. 「**証明書のダウンロード**」タブをクリックします。

ステップ 4. 「**証明書のダウンロード**」をクリックします。

ステップ 5. 「**der として保存**」または「**pem として保存**」をクリックして、サーバー証明書を DER または PEM ファイルとしてローカル・システムに保存します。

Web ブラウザーへの証明機関証明書のインポート

Lenovo XClarity Administrator にアクセスするときに、Web ブラウザーにセキュリティーの警告が表示されないようにするために、現在の証明機関 (CA) 証明書のコピーを PEM 形式または DER 形式でローカル・システムにダウンロードして、そのサーバー証明書を Web ブラウザーのトラステッド証明書のリストにインポートできます。

このタスクについて

XClarity Administrator は、RSA-3072/SHA-384、RSA-2048/SHA-256、ECDSA p256/SHA-256 証明書の署名をサポートします。SHA-1 ストロングや SHA ハッシュなどのアルゴリズムは、構成によってはサポートされる場合もあります。XClarity Administrator で選択されている暗号モード (「管理サーバーでの暗号化設定の構成」を参照)、管理対象サーバーで選択されているセキュリティ設定 (管理対象サーバーのセキュリティー設定の構成)、および環境内のその他のソフトウェアとデバイスの機能を検討してください。すべての楕円曲線ではなく一部の楕円曲線 (p256 含む) に基づいた ECDSA 証明書は、「トラステッド証明書」ページおよび XClarity Administrator 証明書の署名チェーンでサポートされていますが、XClarity Administrator サーバー証明書での使用は現在サポート*されていません*。

注：XClarity Administrator は、Strict モードでは、XCC2 を含むサーバー に RSA- 3072/SHA-384 証明書の署名を使用します。

手順

サーバー証明書を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 → 「セキュリティー」**をクリックして、「セキュリティー」ページを表示します。

ステップ 2. 「証明書の管理」セクションで「**証明機関**」をクリックします。「証明機関」ページが表示されます。

ステップ 3. 「**証明機関ルート証明書のダウンロード**」をクリックします。

ステップ 4. 「**der として保存**」または「**pem として保存**」をクリックして、サーバー証明書を DER または PEM ファイルとしてローカル・システムに保存します。

ステップ 5. ダウンロードした証明書をブラウザーのトラステッド・ルート証明機関証明書のリストにインポートします。

- Firefox:
  1. ブラウザーを開き、「**ツール**」 → 「**オプション**」 → 「**詳細**」の順にクリックします。
  2. 「**証明書**」タブをクリックします。
  3. 「**証明書の表示**」をクリックします。
  4. 「**インポート**」をクリックし、証明書をダウンロードした場所を参照します。
  5. 証明書を選択し、「**開く**」をクリックします。
- Internet Explorer:
  1. ブラウザーを開き、「**ツール**」 → 「**インターネット オプション**」 → 「**コンテンツ**」の順にクリックします。
  2. 「**証明書**」をクリックして、現在信頼されているすべての証明書のリストを表示します。
  3. 「**インポート**」をクリックして、「証明書のインポート ウィザード」を表示します。
  4. ウィザードに従って証明書をインポートします。

証明書取り消しリストの追加と置き換え

*証明書取り消しリスト*は、取り消された証明書と信頼されなくなった証明書のリストです。証明書が取り消されることがあるのは、その証明書が CA から間違って発行された場合や、証明書のキーの暗号漏えい、紛失、盗難が起こった場合です。

手順

新しい証明書取り消しリストを追加する場合や、既存の証明書取り消しリストを置き換える場合は、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 → 「セキュリティー」**をクリックして、「セキュリティー」ページを表示します。

ステップ 2. 左側のナビゲーションで、「証明書の管理」の「**証明書取り消しリスト**」をクリックします。「証明書取り消しリスト」ページが開いて、すべての証明書取り消しリストの一覧が表示されます。

ステップ 3. 「**CLR の追加/置換**」をクリックすることで証明書取り消しリストを追加するか、証明書取り消しリストを選択して「**CLR の追加/置換**」をクリックすることで CRL を置き換えます。

ステップ 4. PEM または DER 形式の証明書取り消しリスト・ファイルを指定するか、PEM 形式の証明書を貼り付けます。

ステップ 5. 「**作成**」をクリックして、証明書取り消しリストを作成します。

Encapsulation の有効化

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

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

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

「新しいデバイスの検出と管理」ページの「**今後すべての管理対象デバイスで Encapsulation を有効にする**」チェックボックスを選択して、管理プロセス中にすべてのデバイスに共通して encapsulation を有効化または無効化できます。encapsulation はデフォルトでは無効になっています。

また、デバイス要約ページでデバイスを選択し、「**操作**」 ➡ 「**Encapsulation を有効にする**」または「**操作**」 ➡ 「**Encapsulation を無効にする**」をクリックして、特定の管理対象デバイスの encapsulation をいつでも個別に有効化または無効化できます。

注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。

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

NIST SP 800-131A コンプライアンスの実装

NIST SP 800-131A に準拠する必要がある場合は、Lenovo XClarity Administrator を使用した完全に準拠する環境への取り組みを開始します。

このタスクについて

米国立標準技術研究所 (NIST) の Special Publication 800-131A (NIST SP 800-131A) では、セキュアな通信の処理方法が指定されています。この標準によってアルゴリズムが強化され、鍵の長さが増すことで、セキュリティーが向上します。NIST SP 800-131A 標準では、標準が厳密に適用されるようにユーザーを構成することが要求されています。

注：現在、以下の Flex System コンポーネントは NIST SP 800-131A をサポートしていません。XClarity Administrator または CMM とこれらのコンポーネントの間の通信は適合していません。

- Flex System EN4023 10 Gb スケーラブル・スイッチ
- Flex System EN6131 40 Gb イーサネット・スイッチ
- Flex System FC3171 8 Gb SAN スイッチ
- Flex System FC5022 16 Gb SAN スケーラブル・スイッチ
- Flex System IB6131 Infiniband スイッチ

注：SAML ID プロバイダーを認証に使用する場合、XClarity Administrator は SHA-1 を使用してメタデータに署名します。SHA-1 アルゴリズムを使用したデジタル署名は NIST SP 800-131A に準拠していません。

手順

NIST SP 800-131A コンプライアンスを実装するには、以下の手順を実行します。

ステップ 1. ご使用のデバイスが、以下の標準を満たしていることを確認してください。

- TLS v1.2 プロトコルを介した Secure Sockets Layer (SSL) を使用する。
- デジタル署名には SHA-256 以上の強度のハッシュ関数を使用し、その他の用途には SHA-1 以上の強度のハッシュ関数を使用する。
- RSA-2048、またはより強力な暗号を使用しているか、NIST が承認した 224 ビット以上の楕円曲線暗号を使用している。
- NIST が承認した対称鍵暗号で、鍵の長さが少なくとも 128 ビット以上のものを使用している。
- NIST が承認した乱数発生ルーチンを使用している。
- (可能な場合) Diffie-Hellman 鍵交換メカニズムまたは Elliptic Curve Diffie-Hellman 鍵交換メカニズム (あるいはこの両方) をサポートしている。

ステップ 2. Lenovo XClarity Administrator で暗号化設定を構成します。NIST SP 800-131A コンプライアンスに関連する設定は 2 つあります。

- *SSL/TLS モード*では、セキュアな通信に使用するプロトコルを指定します。XClarity Administrator では、XClarity Administrator とすべての管理対象デバイスで暗号化プロトコ

ルを TLS 1.2 に制限するための「**TLS 1.2 サーバーおよびクライアント**」という設定がサポートされています。

- セキュアな通信が実装されている場合には、*暗号モード*で使用される暗号鍵の長さが設定されます。暗号モードを「**NIST SP 800-131A**」と設定できます。ただし、一部のオペレーティング・システム・インストーラーでは制限付き設定がサポートされていないため、XClarity Administrator を使用してオペレーティング・システムをデプロイできない場合があります。オペレーティング・システム・デプロイメントをサポートするために、オペレーティング・システム・デプロイメントの例外を許可することを選択できます。

暗号設定を変更した場合は、XClarity Administrator によってすべての管理対象デバイスに新しい設定がプロビジョニングされ、それらのデバイスで新しい証明書を解決しようと試みられます。

注：暗号設定を変更した後、手動で XClarity Administrator を再起動して、変更を有効にし、失われたサービスを復元する必要があります (XClarity Administratorの再起動 を参照)。

これらの設定の詳細については、管理サーバーでの暗号化設定の構成を参照してください。

ステップ 3. TLS1.2 プロトコルと SHA-256 ハッシュ関数がサポートされている Web ブラウザーを使用し、Web ブラウザーでその設定を有効にします。

注：カスタム証明書または外部署名証明書を使用しているか、または使用する予定の場合、チェーン内のすべての証明書は SHA-256 ハッシュ関数に基づいている必要があります。

ステップ 4. すべての通信で暗号化されたプロトコルを使用します。XClarity Administrator 管理対象デバイスとのリモート通信に対して、Telnet、FTP、VNC などの暗号化されていないプロトコルを有効にしないでください。

VMware ツールの使用

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

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

ネットワーク・アクセスの構成

Lenovo XClarity Administrator の初期セットアップ時に、最大 2 つのネットワーク・インターフェースを構成します。また、これらのインターフェースのうちどちらをオペレーティング・システムのデプロイメントに使用するかを指定する必要があります。これらの設定は初期セットアップ後に変更できます。

始める前に

注意：

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

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

- XClarity Administrator を仮想アプライアンスとして実行する場合、管理ネットワークのネットワーク・インターフェースが DHCP (Dynamic Host Configuration Protocol) を使用するように設定されている場合は、DHCP のリースの有効期限が切れると管理インターフェースの IP アドレスが変更される可能性があります。IP アドレスが変更された場合は、シャーシ、ラック・サーバー、タワー・サーバーを管理解除してから、再度管理対象にする必要があります。この問題を避けるには、管理インターフェースを静的 IP アドレスに変更するか、DHCP アドレスが MAC アドレスに基づくように、または DHCP リースの有効期限が切れないように DHCP サーバー構成が設定されていることを確認します。
- オペレーティング・システムのデプロイや OS デバイス・ドライバーの更新に XClarity Administrator を使用*しない*場合は、ネットワーク・インターフェースを「**ハードウェアの検出と管理のみ**」オプションを使用するように変更することで、Samba および Apache サーバーを無効にできます。ネットワーク・インターフェースを変更すると管理サーバーは再起動されます。
- XClarity Administrator をコンテナーとして実行する場合は、以下の点に注意してください。
  - 行うことができるのは、重複 IP アドレスのチェックの有効化または無効化、ネットワーク・インターフェースの役割の変更、プロキシ設定の変更のみです。その他のネットワーク設定 (IP アドレス、ゲートウェイ、DNS など) は、コンテナーのセットアップ時に定義します。
  - macvlan ネットワークがホスト・システムでセットアップされている必要があります。

このタスクについて

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

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

    注：OS デプロイメントおよび OS デバイス・ドライバーの更新のために個別のネットワークを実装した場合は、データ・ネットワークではなくそのネットワークに接続するようにセカンド・ネットワーク・インターフェースを構成できます。ただし、各サーバーのオペレーティング・システムがデータ・ネットワークにアクセスできない場合は、必要に応じて、サーバーで追加インターフェースを構成して、OS デプロイメントおよび OS デバイス・ドライバーの更新のためにホスト・オペレーティング・システムからデータ・ネットワークへの接続を確立します。
- 2 つのネットワーク・インターフェース (eth0 と eth1) が存在する場合:
  - 最初のネットワーク・インターフェース (通常は Eth0 インターフェース) は、管理ネットワークに接続し、デバイスの検出と管理 (サーバーの構成およびファームウェアの更新を含む) をサポートするように構成する必要があります。各管理対象シャーシの CMM および Flex スイッチ、各管理対象サーバーの管理コントローラー、各 RackSwitch スイッチと通信できる必要があります。

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

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

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

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

ネットワーク・トポロジー	インターフェース 1 (eth0) の役割	インターフェース 2 (eth1) の役割
コンバージド・ネットワーク (OS デプロイメントと OS デバイス・ドライバーの更新をサポートする管理およびデータ・ネットワーク)	管理ネットワーク • 検出および管理 • サーバー構成 • ファームウェア更新 • サービス・データ収集 • 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど) • 保証データの取得 • OS デプロイメント • OS デバイス・ドライバーの更新	なし
OS デプロイメントと OS デバイス・ドライバーの更新をサポートする個別の管理ネットワークとデータ・ネットワーク	管理ネットワーク • 検出および管理 • サーバー構成 • ファームウェア更新 • サービス・データ収集 • 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど) • 保証データの取得 • OS デプロイメント • OS デバイス・ドライバーの更新	データ・ネットワーク • なし

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

ネットワーク・トポロジー	インターフェース 1 (eth0) の役割	インターフェース 2 (eth1) の役割
OS デプロイメントと OS デバイス・ドライバーの更新をサポートする個別の管理ネットワークとデータ・ネットワーク	管理ネットワーク • 検出および管理 • サーバー構成 • ファームウェア更新 • サービス・データ収集 • 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど) • 保証データの取得	データ・ネットワーク • OS デプロイメント • OS デバイス・ドライバーの更新
OS デプロイメントと OS デバイス・ドライバーの更新をサポートしない個別の管理ネットワークとデータ・ネットワーク	管理ネットワーク • 検出および管理 • サーバー構成 • ファームウェア更新 • サービス・データ収集 • 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど) • 保証データの取得	データ・ネットワーク • なし
管理ネットワークのみ (OS デプロイメントおよび OS デバイス・ドライバーの更新はサポートされません)	管理ネットワーク • 検出および管理 • サーバー構成 • ファームウェア更新 • サービス・データ収集 • 自動問題通知 (コール・ホーム、Lenovo 更新ファシリティーなど) • 保証データの取得	なし

IPv6 アドレスの制限を含む XClarity Administrator ネットワーク・インターフェースについて詳しくは、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。

手順

ネットワーク・アクセスを構成するには、以下の手順を完了します。

ステップ 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。現在のネットワーク設定が表示されます。

ステップ 2. 必要に応じて、「**重複 IP アドレスのチェック**」トグルをクリックして、同じサブネットの IP アドレスの重複のチェックを有効にします。

有効にすると、XClarity Administrator の IP アドレスを変更しようとした場合、または管理対象の他のデバイスや同じサブネットにある他のデバイスと同じ IP アドレスを持つデバイスを管理しようとした場合、XClarity Administrator によってアラートが出されます。

ステップ 3. 「**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。

ステップ 4. XClarity Administrator を使用してオペレーティング・システムをデプロイし、OS デバイス・ドライバーを更新する場合は、オペレーティング・システムの管理に使用するネットワーク・インターフェースを選択します。

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

ステップ 5. (仮想アプライアンスの XClarity Administrator のみ) IP 設定を変更します。

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

- 「**IPv4**」。インターフェースに IPv4 アドレスを割り当てる必要があります。静的に割り当てられた IP アドレスを使用するか、DHCP サーバーから IP アドレスを取得するかを選択できます。
- 「**IPv6**」。必要に応じて、以下のいずれかの割り当て方法を使用して、インターフェースに IPv6 アドレスを割り当てることができます。
  - 静的に割り当てられた IP アドレスを使用する
  - ステートフル・アドレス構成 (DHCPv6) を使用する
  - ステートレス・アドレス自動構成を使用する

  注：IPv6 アドレスについては、XClarity Administrator オンライン・ドキュメントの IPv6 構成の制限を参照してください。

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

  注：このインターフェースに割り当てる IP アドレスは、第 1 インターフェースに割り当てる IP アドレスとは異なるサブネットに属する必要があります。DHCP を使用して両方のインターフェース (Eth0 と Eth1) に IP アドレスが割り当てられるように選択した場

合、DHCP サーバーによって 2 つのインターフェースの IP アドレスに同じサブネットが割り当てられないようにしてください。

- 「**IPv4**」。静的に割り当てられた IP アドレスを使用するか、DHCP サーバーから IP アドレスを取得するかを選択できます。
- 「**IPv6**」。必要に応じて、以下のいずれかの割り当て方法を使用して、インターフェースに IPv6 アドレスを割り当てることができます。
  - 静的に割り当てられた IP アドレスを使用する
  - ステートフル・アドレス構成 (DHCPv6) を使用する
  - ステートレス・アドレス自動構成を使用する

c. デフォルト・ゲートウェイを指定します。

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

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

ヒント:

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

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

d. 「**IP 設定の保存**」をクリックします。

ステップ 6. (仮想アプライアンスの XClarity Administrator のみ) 任意で詳細設定を変更します。

a. 「**詳細ルーティング**」タブをクリックします。

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

1 つ以上の経路エントリを定義するには、以下の手順を実行します。
1. インターフェースを選択します。

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

c. 「**詳細ルーティングの保存**」をクリックします。

ステップ 7. 必要に応じて、DNS およびプロキシー設定を変更します。

XClarity Administrator をコンテナーとしてセットアップしている場合、Web インターフェースから変更できるのはプロキシ設定のみです。DNS 設定はコンテナーで定義します。

a. 「**DNS およびプロキシー**」タブをクリックします。

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

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

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

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

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

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

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

- 必ず、プロキシー・サーバーが基本認証を使用するようにセットアップされているようにしてください。
- プロキシ・サーバーが終了しないプロキシーとしてセットアップされていることを確認します。
- プロキシ・サーバーが転送プロキシーとしてセットアップされていることを確認します。

- ロード・バランサーがセッションを 1 つのプロキシ・サーバーで保持し、他のサーバーに切り替えないように構成されていることを確認します。

HTTP プロキシを使用するように選択した場合は、必須フィールドに入力します。
1. プロキシ・サーバーのホスト名およびポートを指定します。
2. 認証を使用するかどうかを選択し、必要に応じてユーザー名およびパスワードを指定します。
3. プロキシ・テストの URL を指定します。
4. 「**プロキシーのテスト**」をクリックして、プロキシ設定が正しく構成され機能することを確認します。

f. 「**DNS およびプロキシーの保存**」をクリックします。

g. XClarity Administrator 管理サーバーの完全修飾ドメイン名 (FQDN) と DNS 情報を、IMM2、XCC、および XCC2 の管理対象サーバーにプッシュし、管理対象サーバーでこの情報を使用して管理サーバーを検索できるようにします。
   1. 「**FQDN / DNS を BMC にプッシュ**」をクリックします。
   2. ベースボード管理コントローラーの既存の DNS エントリーの処理方法を選択します。
      - 既存の DNS エントリーを保持し、次に使用可能なスロットに管理サーバーの DNS エントリーを追加します。
      - すべての既存の DNS エントリーを管理サーバーの DNS エントリーに置き換えます。
   3. 編集フィールドに「**YES**」と入力します。
   4. 「**適用**」をクリックします。

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

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

ステップ 8. 「**再起動**」をクリックして管理サーバーを再起動します。

ステップ 9. ネットワーク設定を確認するには、「**接続のテスト**」をクリックします。

日付と時刻の設定

Lenovo XClarity Administrator に使用される日付と時刻を設定できます。

始める前に

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

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

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

注意：XClarity Administrator 仮想アプライアンスおよびそのホストは、XClarity Administrator とそのホスト間で誤った同期を防止するために、同じ時刻送信元と同期するように設定する必要があります。通常は、仮想アプライアンスがホストと時刻同期するようにホストが構成されます。If XClarity Administrator がホスト以外のソースと同期するように設定されている場合、XClarity Administrator 仮想アプライアンスとそのホスト間のホスト時刻同期を無効にする必要があります。

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

手順

XClarity Administrator の日付と時刻を設定するには、以下の手順を実行します。

ステップ 1. XClarity Administrator メニュー・バーで、**管理 ➡ 「日付と時刻」**をクリックします。「日付と時刻」ページが表示されます。このページには、XClarity Administrator の現在の日付と時刻が表示されます。

ステップ 2. 「**日付と時刻の編集**」をクリックして、「日付と時刻の編集」ページを表示します。

ステップ 3. 「日付と時刻」ダイアログに入力します。

1. XClarity Administrator のホストがあるタイム・ゾーンを選択します。

   選択されたタイム・ゾーンが夏時間 (DST) だった場合、時刻は自動的に DST に合わせて調整されます。

2. 12 時間または 24 時間の時計を選択します。

3. 運用ネットワーク内の各 NTP サーバーのホスト名または IP アドレスを指定します。NTP サーバーは最大 4 つまで定義できます。
4. ネットワーク内で「NTP v3 認証」を有効にする場合は「**必須**」を選択し、XClarity Administrator と NTP サーバー間で NTP v1 認証を使用する場合は「**なし**」を選択します。

   管理対象の Flex System の CMM およびベースボード管理コントローラーのファームウェアで v3 認証を必要とし、XClarity Administrator とネットワーク内の 1 つ以上の NTP サーバーの間で NTP v3 認証が必要な場合に、v3 認証を使用できます。
5. NTP v3 認証を有効にした場合、該当する各 NTP サーバーで、認証キーとインデックスを設定する必要があります。M-MD5 鍵、SHA1 鍵、またはその両方を指定できます。M-MD5 鍵または SHA1 鍵をともに指定した場合、XClarity Administrator により、管理対象の Flex System の CMM およびそれをサポートする管理コントローラーに、M-MD5 鍵または SHA1 鍵がプッシュされます。XClarity Administrator では、NTP サーバーを認証するためにこの鍵が使用されます。
   - M-MD5 鍵の場合は、大小英字 (a ～ z、A ～ Z)、数字 (0 ～ 9)、および特殊文字 @# のみが含まれる ASCII 文字列を指定します。
   - SHA1 鍵の場合は、40 文字の ASCII 文字列を指定します (0 ～ 9 および a ～ f のみ使用)。
   - 指定する鍵インデックスと認証鍵は、NTP サーバーで設定されている鍵 ID とパスワード値に一致する必要があります。たとえば、NTP サーバーで入力された SHA1 鍵のインデックスが 5 である場合、XClarity AdministratorSHA1 鍵の指定した鍵インデックスも 5 になります。鍵 ID とパスワードの設定の詳細については、NTP サーバーのドキュメントを参照してください。
   - 2 つ以上の NTP サーバーで同じ鍵を使用している場合でも、v3 認証を使用する各 NTP サーバーに鍵をを指定する必要があります。
   - V3 認証を有効にし、NTP サーバーの認証鍵とインデックスを指定しない場合は、デフォルトで v1 認証が使用されます。
   - 複数の NTP サーバーを指定した場合、NTP サーバーには、すべて v3 認証またはすべて v1 認証を適用する必要があります。NTP サーバーに対する V3 認証と v1 認証の混在はサポートされていません。
   - V3 認証を使用する複数の NTP サーバーを指定する場合は、鍵が同じでない場合には鍵インデックスが固有であることが必要です。たとえば、NTP サーバー 1 および 2 で SHA1 鍵が異なる場合に、NTP サーバー 1 と 2 で SHA1 鍵インデックス 1 を持つことはできません。他方の NTP サーバーとは異なる鍵インデックスの鍵を受け入れるように、いずれかの NTP サーバーを再構成する必要があります。そうしない場合、鍵インデックスに関連付けられている最後の定義済み鍵が、同じ鍵インデックスを持つすべての NTP サーバーに対して構成されます。

ステップ 4. 「**保存**」をクリックします。

インベントリー設定の設定

デバイス名を表示するために使用するプロパティを含む管理対象デバイスのインベントリー設定を設定できます。

手順

管理対象デバイスのインベントリー設定を設定するには、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**」 → 「**インベントリー設定**」をクリックします。「インベントリー設定」ページが表示されます。

ステップ 2. Lenovo XClarity Administrator ユーザー・インターフェースでデバイス名を表示するために使用するプロパティを選択します。以下のいずれかのプロパティを選択できます。
- **事前定義済みシーケンス (デフォルト)**
- **ユーザー定義名**

- **DNS ホスト名**
- **ホスト名**
- **IPv4 アドレス**
- **シリアル番号**

「**事前定義済みシーケンス**」を選択すると、表示されるデバイス名は前のリストのプロパティの並びに基づいて選択されます。たとえば、デバイスにユーザー定義名がある場合、その名前が表示されます。デバイスいユーザー定義名がない場合、DNS ホスト名が表示されます。デバイスいユーザー定義名または DNS ホスト名がない場合、ホスト名が表示されます。

注：デフォルト以外の値を選択すると、すべてのデバイスで Lenovo XClarity Administrator ユーザー・インターフェースに表示される名前が選択されたプロパティに変更されます。デバイスに割り当てられたユーザー定義の名前は変更されません。

ステップ 3. オプションで、「**有効**」をクリックすると、デバイス名に選択されている値を使用して、グリッド (テーブル) をソートできます。

ステップ 4. ラック番号順の設定として、上から下 (1 から 52 など) と下から上 (52 から 1 など) のいずれかを選択します。

注：番号順の設定を変更しても、ラック内のデバイスの位置は変更されません。

ステップ 5. 「**適用**」をクリックします。

終了後

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 (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)。

アラートおよびイベント生成のしきい値設定の設定

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。

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、「**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. 「**しきい値設定**」アイコン ( ) をクリックして、「しきい値設定」ダイアログを表示します。

ステップ 3. ThinkSystem および ThinkServer サーバーの SSD の寿命に関する警告およびクリティカルのしきい値を変更します。

SSD の寿命は、ベンダーのスマート・カウンタを使用して計算されます。デフォルト値は警告しきい値が 30%、クリティカルしきい値が 20% です。

ステップ 4. 「**有効**」トグルを選択して、各しきい値に到達した場合にアラートとイベントを生成します。

ステップ 5. 「**適用**」をクリックします。

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

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Lenovo サポート・センター は、管理対象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、自動的に Lenovo に連絡してサービス・チケットを開き、そのデバイスから収集されたサービス・データを送信します。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 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。

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・サーバーが基本認証を使用するように構成され、終了しないプロキシーとしてセットアップされていることを確認します。プロキシーのセットアップについて詳しくは、ネットワーク・アクセスの構成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。デバイスを指定しない場合、コール・ホーム は、Lenovo Support に問題通知を送信*しません*。

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、XClarity Administrator 診断ファイルの ダウンロードおよびデバイスの診断ファイルの収集とダウンロード 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、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て有効になっている場合**、サービス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・データが*自動*で収集され、サービス・チケットが開かれ、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。

  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・ホームの再有効化について XClarity Administrator オンライン・ドキュメントを参照してください。XCC2 を持つサーバーの場合、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 サポート・センター 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 Support 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 Support 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 サポート・センター に送信されます。

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。

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 (たとえば、`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を参照してください。

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. 連絡先と場所の情報を入力します。
5. Lenovo サポートによる連絡方法を選択します。
6. (オプション) システム情報を入力します。
7. 「**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。
8. 「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、XClarity Administrator オンライン・ドキュメントのLenovo サポートへの診断ファイルの転送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、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。
- 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、XClarity Administrator オンライン・ドキュメントのサービス・チケットとステータスの表示を参照してください。
- 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、XClarity Administrator オンライン・ドキュメントのデバイスの診断ファイル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、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。

  詳しくは、XClarity Administrator オンライン・ドキュメントの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。

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を管理対象デバイス (リカバリー不能なメモリー・エラーなど) を受信した場合に問題を解決できるように、特定の管理対象デバイスのセットに対する診断ファイルを優先サービス・プロバイダー (コール・ホームを使用した Lenovo サポートを含む) に自動的に送信するように Lenovo XClarity Administrator 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、ネットワーク・アクセスの構成XClarity Administrator オンライン・ドキュメントのネットワーク・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 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 および 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。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を参照してください。

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。

XCC2 を持つサーバーの場合、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 Support 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 Support 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、XClarity Administrator オンライン・ドキュメントの診断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、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。
- 「**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、XClarity Administrator オンライン・ドキュメントのデバイスの診断ファイル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、XClarity Administrator オンライン・ドキュメントのサービスおよびサポートの操作を参照してください。

XClarity Administrator を TruScale ポータルへのハブとして接続

Lenovo XClarity Administrator を管理ハブとして Lenovo TruScale ポータルに接続できます。

始める前に

注意：以下の構成手順は、Lenovo サービス担当員のみを対象とします。

手順

XClarity Administrator を TruScale ポータルに接続するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで「**管理**」 ➡ 「**ハブ構成**」の順にクリックし、「ハブ構成」ページを表示します。

ステップ 2. 「**登録要求の生成**」をクリックして、登録キーを作成します。登録要求の生成ダイアログが表示されます。

ステップ 3. 「**クリップボードにコピー**」をクリックして登録キーをコピーしてから、ダイアログを閉じます。

ステップ 4. 「**登録キーのインストール**」をクリックして、「登録キーのインストール」ダイアログを表示します。

ステップ 5. **登録キー**・フィールドに登録キーを貼り付けます。

ステップ 6. 「**送信**」をクリックします。

終了後

構成のリセットをクリックすると、登録キーをアンインストールできます。

システム・データと設定のバックアップ、復元、移行

Lenovo XClarity Administrator を使用して、システム・データと設定、およびオペレーティング・システム・イメージやファームウェア更新、OS デバイス・ドライバーなどのインポートされたファイルを、バックアップおよび復元できます。

Lenovo XClarity Administrator のバックアップ

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

始める前に

注意：バックアップ手順を開始する前に、必ずすべてのアクティブなユーザーに通知してください。データの変更を防止するため、XClarity Administrator は手順中は休止します。そのため、バックアップ手順の実行中は XClarity Administrator にアクセスできません。

XClarity Administrator 仮想アプライアンスから証明機関証明書をダウンロードし、Web ブラウザーにインポートしてあ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「Web ブラウザーへの証明機関証明書のインポート」を参照)。

実行中のすべてのジョブが完了し、保留中のジョブがないことを確認してください。ジョブが実行中の場合、実行中のジョブを停止してバックアップの作成を続行できます。

DNS サーバーの設定が正しいことを確認してください。正しくない場合、バックアップの復元後に SMTP および NTP が正しく動作しないことがあります。

管理サーバーに、バックアップで使用可能な十分なディスク・スペースがあることを確認します。十分なディスク・スペースがない場合は、以前のバックアップなど、不要になった XClarity Administrator リソースを削除してディスク・スペースを解放するか (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)、またはオペレーティング・システム・イメージ、ファームウェア更新、および OS デバイス・ドライバーをバックアップに含めないでください。

OS イメージをバックアップする場合は、適切なネットワーク・インターフェース (eth1 または eth0) で OS デプロイメントが構成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「ネットワーク・アクセスの構成」を参照)。

このタスクについて

初期セットアップおよび以下のような重要な構成の変更を行った後は必ず XClarity Administrator をバックアップしてください。

- XClarity Administrator をアップデートする前
- 新しいシャーシまたはラック・サーバーを管理するとき
- XClarity Administrator にユーザーを追加するとき
- 新しい構成パターンを作成およびデプロイするとき

XClarity Administrator を定期的にバックアップします。

バックアップは、ローカル・システムにダウンロードすることをお勧めします。ホスト・オペレーティング・システムが予期せずにシャットダウンした場合は、ホスト・オペレーティング・システムを再起動した後に XClarity Administrator を認証できない場合があります。この問題を解決するには、ローカル・システムの最後のバックアップから XClarity Administrator を復元します (Lenovo XClarity Administrator の復元を参照)。

手順

XClarity Administrator をバックアップするには、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**」 ➡ 「**データのバックアップと復元**」をクリックします。「データのバックアップと復元」ページが表示されます。

ステップ 2. 「**バックアップ**」アイコン () をクリックします。「データと設定のバックアップ」ダイアログが表示されます。

ステップ 3. このバックアップの説明を入力します。

ステップ 4. バックアップを作成する場所を選択します。ローカル・リポジトリーまたはリモート共有を使用できます。

デフォルトでは、バックアップはローカル・リポジトリーに作成されます。「**バックアップのコピー**」アイコン () をクリックして、バックアップをローカル・リポジトリーからリモート共有にコピーできます。

リモート共有を選択する場合は、バックアップは最初にローカル・リポジトリーに作成されます。その後、選択したリモート共有にバックアップがコピーされ、ローカルのコピーは削除されます。詳しくは、リモート共有の管理を参照してください。

ステップ 5. 必要に応じて、オペレーティング・システム・イメージ、ファームウェア更新、およびOSデバイス・ドライバーを含めることもできます。

ステップ 6. バックアップの暗号化パスフレーズを指定します。

注意：暗号化パスフレーズを記録します。パスフレーズは、バックアップをこの XClarity Administrator インスタンスまたは他のインスタンスに復元するために必要です。パスフレーズを忘れた場合、リカバリーする方法はありません。

ステップ 7. 「**バックアップ**」をクリックしてデータと設定を今すぐバックアップするか、「**スケジュール**」をクリックしてこのバックアップを後で実行するようにスケジュールします。

注意：今すぐバックアップするように選択した場合、プロセスが完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりしないでください。バックアップが生成されない可能性があります。

バックアップの生成に時間がかかる可能性があります。進行状況バーによってジョブの状況が示されます。

リモート共有にバックアップを作成する場合は、「ジョブ」ページで進行を監視できます (ジョブの監視を参照)。

バックアップをスケジュールする場合、バックアップ・プロセス中は管理サーバーが一時的にシャットダウンします。管理サーバーがオンラインに戻った後、「ジョブ」ページから、バックアップ・プロセスのステータスを監視できます。

ステップ 8. XClarity Administrator にログインして、ご使用のデバイスの管理を続行します。

終了後

「データのバックアップと復元」ページから、以下の操作を実行できます。

- XClarity Administrator バックアップをリモート共有から、またはにコピーするには、「**バックアップのコピー**」アイコン () をクリックします。
- 不要になったバックアップを選択してローカル・リポジトリーまたは リモート共有 から削除するには、「**バックアップの削除**」アイコン () をクリックします。
- システム・データと設定をこの管理サーバーに復元する (Lenovo XClarity Administrator の復元を参照)。
- バックアップをローカル・システムにインポートまたはシステムからエクスポートする。「**バックアップのインポート**」アイコン () または「**バックアップのエクスポート**」アイコン () をそれぞれクリックします。
- 選択したバックアップを新しい XClarity Administrator インスタンスにプッシュする (別の XClarity Administrator インスタンスへのシステム・データと設定の移行を参照)。

Lenovo XClarity Administrator の復元

バックアップしたデータと設定を使用して、Lenovo XClarity Administrator を前の状態に復元できます。

始める前に

注意：バックアップ手順を開始する前に、必ずすべてのアクティブなユーザーに通知してください。データの変更を防止するため、XClarity Administrator は手順中は休止します。そのため、バックアップ手順の実行中は XClarity Administrator にアクセスできません。

XClarity Administrator 仮想アプライアンスから証明機関証明書をダウンロードし、証明書を Web ブラウザーにインポートします (Web ブラウザーへの証明機関証明書のインポートを参照)。

実行中のすべてのジョブが完了し、保留中のジョブがないことを確認してください。

バックアップの作成に使用された XClarity Administrator バージョンと同じバージョンでのみ、バックアップを復元できます。

このタスクについて

注意：

- バックアップの作成後に加えられたすべての変更は失われます。
- データを復元するには、仮想アプライアンスは元のクリーンな状態にリセットされます。現在の設定、デバイス・インベントリーおよびファイル (オペレーティング・システム・イメージ、ファームウェア更新、および OS デバイス・ドライバー) は、バックアップのデータが復元される前に削除されます。バックアップのデータと設定は、仮想アプライアンスの現在のデータと設定とは混用できません。デバイス・インベントリー、オペレーティング・システム・イメージ、ファームウェア更新、および OS デバイス・ドライバーを復元しない選択をした場合、復元操作の完了後はデフォルトの XClarity Administrator データのみが存在します。

バックアップの復元によって XClarity Administrator インスタンスのバックアップは削除されません。

バックアップの復元によって管理対象デバイスのデータまたは設定は変更されません。たとえば、デバイスを管理解除してから、XClarity Administrator でデバイスが管理されていた時のバックアップを復元すると、復元操作の完了後にそのデバイスとの接続に問題が発生する場合があります。同様に、デバイスを管理しており、デバイスがまだ管理されていないときのバックアップを復元する必要がある場合は、手動でデバイスの構成を変更して管理対象になっているステータスを元に戻すか、XClarity Administrator で再度管理する際に「**強制**」オプションを使用する必要がある場合があります。

手順

XClarity Administratorを復元するには、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**」 ➡ 「**データのバックアップと復元**」をクリックします。「データのバックアップと復元」ページが表示されます。

ステップ 2. バックアップ・パッケージをローカル・システムにエクスポートして XClarity Administrator から削除した場合は、次の手順を実行します。

a. 「データのバックアップと復元」ページで、「**バックアップのインポート**」アイコン () をクリックして、「バックアップのインポート」ダイアログを表示します。

b. 「**参照**」をクリックして、ソース XClarity Administrator インスタンスからエクスポートしたバックアップを見つけます。

c. 「**インポート**」をクリックして、バックアップを XClarity Administrator にアップロードします。

バックアップのインポートに時間がかかる可能性があります。進行状況バーによってジョブの状況が示されます。

注意：アップロードが完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりすると、処理が失敗する可能性があります。

d. インポートが完了したら、バックアップの暗号化パスフレーズを指定します。

注：暗号化パスフレーズがない場合は、XClarity Administrator に新しいバックアップを作成する必要があります (Lenovo XClarity Administrator のバックアップを参照)。

ステップ 3. 復元するバックアップを選択し、「**バックアップの復元**」アイコン () をクリックします。「データの復元」ダイアログが表示されます。

ステップ 4. バックアップの暗号化パスフレーズを指定します。

ステップ 5. 「**確認**」をクリックします。

ステップ 6. 「データの復元の確認」ダイアログで、ダイアログの情報が正しいことを確認します。

ステップ 7. 「復元オプション」ダイアログで、オペレーティング・システム・イメージのインポート、ファームウェア更新、OS デバイス・ドライバー、ネットワーク設定、デバイス・インベントリーを必要に応じて選択します。

注意：このダイアログに表示されたすべての警告を注意深く読んでください。

ステップ 8. 「**確認**」をクリックしてデータの復元を開始します。

データと設定の復元には、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。

復元プロセスが完了したら、ログイン・ページにリダイレクトされます。

注意：処理が完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりすると、処理が失敗する可能性があります。

ステップ 9. XClarity Administrator にログインして、ご使用のデバイスの管理を続行します。

別の XClarity Administrator インスタンスへのシステム・データと設定の移行

バックアップしたシステム・データと設定を同じまたは別のネットワークにある新しい Lenovo XClarity Administrator に移行できます。

始める前に

ターゲットの管理サーバーは、バックアップを作成するために使用した管理サーバーと同じバージョンの*新しい* XClarity Administrator インスタンスであること、また初期セットアップ・ウィザードにあり、どのステップも完了していないことが必要です。詳しくは、XClarity Administrator オンライン・ドキュメントの XClarity Administrator のインストールとセットアップを参照してください。

バックアップ手順を開始する前に、必ずすべてのアクティブなユーザーに通知してください。データの変更を防止するため、XClarity Administrator は手順中は休止します。そのため、バックアップ手順の実行中は XClarity Administrator にアクセスできません。

XClarity Administrator から証明機関の証明書をダウンロードし、証明書を Web ブラウザーにインポートします (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)。

ソースの管理サーバーのバックアップ・リポジトリー内のバックアップは、ターゲットの管理サーバーに移行されません。データと設定を移行する前に、ローカル・システムに必要なすべてのバックアップをエクスポートしてください。

このタスクについて

バックアップの作成後にソース管理サーバーに加えた変更は、ターゲット管理サーバーに移行されません。

バックアップの復元によって管理対象デバイスのデータまたは設定は変更されません。たとえば、デバイスを管理解除してから、XClarity Administrator でデバイスが管理されていた時のバックアップを復元すると、復元操作の完了後にそのデバイスとの接続に問題が発生する場合があります。同様に、デバイスを管理しており、デバイスがまだ管理されていないときのバックアップを復元する必要がある場合は、手動でデバイスの構成を変更して管理対象になっているステータスを元に戻すか、XClarity Administrator で再度管理する際に「**強制**」オプションを使用する必要がある場合があります。

注：XClarity Administrator をコンテナーとして実行する場合は、一方のコンテナーのホストで作成されたボリュームを別のコンテナーでボリュームとして使用できます。ボリュームが新しい (ターゲットの) コンテナーにバインドされると、そのボリュームは最初 (ソース) のコンテナーで使用できなくなります。

1. ターゲットのコンテナーの `docker-compose.yml` ファイルを設定して、ソースのコンテナーと同じ IP アドレスとコンテナー名を使用します。

2. 次のコマンドを使用して、ソースのコンテナーを停止します。
   `docker-compose -p ${CONTAINER_NAME} down`
3. 次のコマンドを使用して、ターゲットのコンテナーを開始します。*<env_filename>*は環境変数ファイルの名前です。ターゲットのコンテナーが開始されると、ボリュームはターゲットの XClarity Administrator コンテナーにバインドされ、XClarity Administrator はそれらのボリュームのシステム・データと設定を使用します。
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

手順

XClarity Administratorを復元するには、以下の手順を実行します。

ステップ 1. ソースとターゲットの XClarity Administrator が同じネットワークにある場合は、以下の手順を実行します。

a. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**データのバックアップと復元**」をクリックします。「データのバックアップと復元」ページが表示されます。

b. 「**バックアップのプッシュ**」アイコン () をクリックして、「データのプッシュ」ダイアログを表示します。

c. ターゲット XClarity Administrator の現在の IP アドレスを指定します。

d. 「**続行**」をクリックして、バックアップをターゲット XClarity Administrator にアップロードします。

バックアップのアップロードに時間がかかる可能性があります。進行状況バーによってジョブの状況が示されます。

注意：アップロードが完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりすると、パッケージがアップロードされない可能性があります。

ステップ 2. ソースとターゲットの XClarity Administrator が同じネットワークにない場合は、以下の手順を実行します。

a. ソース側の XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**データのバックアップと復元**」をクリックします。「データのバックアップと復元」ページで「**バックアップのエクスポート**」アイコン () をクリクして、バックアップをローカル・システムにエクスポートします。

バックアップのエクスポートに時間がかかる可能性があります。

b. エクスポートしたバックアップを、ソース管理サーバーから同じネットワークのシステムに、ターゲット管理サーバーとしてコピーします。

c. ターゲットの XClarity Administrator のウィザード・ページで、「**バックアップのインポート**」アイコン () をクリックして、「データ・パッケージのインポート」ダイアログを表示します。

d. 「**参照**」をクリックして、ソース XClarity Administrator からエクスポートしたバックアップを見つけます。

e. 「**アップロード**」をクリックして、バックアップをターゲット XClarity Administrator にインポートします。

バックアップのインポートに時間がかかる可能性があります。進行状況バーによってジョブの状況が示されます。

注意：アップロードが完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりすると、処理が失敗する可能性があります。

ステップ 3. インポートが完了したら、バックアップの暗号化パスフレーズを指定します。

注：暗号化パスフレーズがない場合は、ソース XClarity Administrator に新しいバックアップを作成する必要があります (Lenovo XClarity Administrator のバックアップを参照)。

ステップ 4. 「データの復元の確認」ダイアログで、すべての情報が正しいことを確認します。

ステップ 5. 「**確認**」をクリックして、システム・データと設定のロードを開始します。

ステップ 6. 「復元オプション」ダイアログで、オペレーティング・システム・イメージのインポート、ファームウェア更新、OS デバイス・ドライバー、ネットワーク設定、デバイス・インベントリーを必要に応じて選択します。

注意：このダイアログに表示されたすべての警告を注意深く読んでください。

ステップ 7. ネットワーク設定またはデバイス・インベントリーのインポートを選択した場合は、そース XClarity Administrator で **「管理」 ➡ 「管理サーバーのシャットダウン」 ➡ 「シャットダウン」** の順にクリックして管理サーバーをシャットダウンします。

続行する前に、ソース仮想アプライアンスがシャットダウンされていることを確認します。

ステップ 8. ターゲットの XClarity Administrator で、「**確認**」をクリックしてパッケージからのデータと設定のロードを開始します。

ネットワーク設定のインポートを選択した場合は、移行が完了したら、ソース XClarity Administrator の IP アドレスがターゲット XClarity Administrator に再割り当てされます。

注意：送信元 XClarity Administrator が DHCP を使用している場合、ターゲット XClarity Administrator の MAC アドレスを、DHCP サーバーの対応する送信元 XClarity Administrator の IP アドレスにバインドする必要があります。DHCP サーバーを変更した後は、続行する前に少なくとも 15 分間待ちます。

ステップ 9. 「パッケージからのデータと設定のロード」進行状況バーが完了するまで待ちます。

データ移行プロセスが完了したら、ログイン・ページにリダイレクトされます。

注意：アップロードが完了する前に Web ブラウザーのタブまたはウィンドウを閉じたり更新したりすると、処理が失敗する可能性があります。

ステップ 10. ターゲット XClarity Administrator にログインして、ご使用のデバイスの管理を続行します。

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。

- **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、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 (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 のメニュー・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、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。

リモート共有の管理

リモート共有をマウントし、Lenovo XClarity Administrator のバックアップやファームウェア更新などの大きなデータ・ファイルをローカル・リポジトリーからリモート共有に移動して、管理サーバーで使用できるディスク・スペースを管理できます。

始める前に

XClarity Administrator をコンテナーとして実行する際は、インストール時に yml ファイルを使用してリモート共有をコンテナーに取り付けます (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)。

XClarity Administrator を仮想アプライアンスとして実行する際に、リモート共有 を取り付け・取り外すには、**lxc-supervisor** 権限が必要です・

ファイル・サーバーと XClarity Administrator 間のネットワークが高速で安定していることを確認します。

コンテナーとして XClarity Administrator を実行する際、リモート共有はサポートされません。

このタスクについて

XClarity Administrator のバックアップとファームウェア更新を保存するには、それぞれ別のリモート共有を使用する必要があります。

XClarity Administrator のバックアップ・ファイルは、リモート共有から直接使用することはできません。バックアップ・ファイルを使用するには、ローカル・リポジトリーに戻す必要があります。

現在、SSHFS のみサポートされます。

手順

仮想アプライアンスとして XClarity Administrator を実行する際に、リモート共有 を追加するには、次の手順を実行します。

1. XClarity Administrator のメニュー・バーで、「**管理**」 → 「**リモート共有**」の順にクリックします。「リモート共有」ページが表示されます。
2. 「**作成**」アイコン () をクリックして、リモート共有を作成します。「リモート共有作成」ダイアログが表示されます。
3. リモート共有をホストするファイル・サーバーの IP アドレス指定します。
4. リモート共有へのアクセスに使用する保存された資格情報を指定します。

   ヒント: 保存された資格情報を作成するには、保存された資格情報の管理 を参照してください。
5. リモート共有のマウントに使用する管理サーバーのマウント・ポイント (ローカル・ディレクトリー) を指定します。

   重要：パスは「/mnt」で開始する必要があります。

6. 管理サーバーで、リモート共有としてマウントする共有ディレクトリー (リモート・サーバーのパス) を指定します。
7. 「**作成**」をクリックします。

終了後

- リモート共有を選択して「**削除**」( ) アイコンをクリックし、リモート共有をマウント解除します。
- XClarity Administrator のバックアップ・ファイルをリモート共有との間で移動します (ディスク・スペースの管理 を参照)。
- XClarity Administrator を構成して、ファームウェア更新リポジトリとしてリモート共有を使用します (「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)。

ユーザー・インターフェースの言語の変更

ログイン後、ユーザー・インターフェースの言語を変更できます。

手順

Lenovo XClarity Administrator のタイトル・バーで、ユーザー操作メニュー (ADMIN_USER) 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。

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

XClarity Administrator のシャットダウン

Lenovo XClarity Administrator がシャットダウンすると、Lenovo XClarity Administrator への接続が失われます。

始める前に

XClarity Administrator 仮想アプライアンスをシャットダウンするには、**lxc-supervisor** または **lxc-admin** 権限が必要です。

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

手順

Lenovo XClarity Administrator をシャットダウンするには、以下の手順を実行します。

- **コンテナー**

  コンテナーを停止するには、次のコマンドを実行します。
  ```
  docker-compose -p ${CONTAINER_NAME} down
  ```
- **仮想アプライアンス**
  1. Lenovo XClarity Administrator のメニュー・バーで、**管理 → 「管理サーバーのシャットダウン」** をクリックします。

     確認ダイアログが開いて、現在実行されているジョブのリストが表示されます。XClarity Administrator をシャットダウンすると、ジョブはキャンセルされます。
  2. 「**シャットダウン**」をクリックします。

終了後

shutdown後に XClarity Administrator を再起動するには、 XClarity Administratorの再起動を参照してください。

XClarity Administratorの再起動

シャットダウン後に Web インターフェースまたはハイパーバイザーから Lenovo XClarity Administrator を再起動できます。

始める前に

XClarity Administrator を再起動するには、**lxc-supervisor** または **lxc-admin** 権限が必要です。

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

このタスクについて

以下のような場合に Lenovo XClarity Administrator を再起動する必要があります。
- サーバー証明書を再生成する場合
- 新しいサーバー証明書をアップロードする場合

手順

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

- **コンテナー**

  次のコマンドを実行して、コンテナーを停止して開始します。*<env_filename>* は環境変数ファイルの名前です。

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

- **仮想アプライアンス**
  - Web インターフェースからの Lenovo XClarity Administrator の再起動:
    1. Lenovo XClarity Administrator のメニュー・バーで、「**管理**」 ➡ 「**管理サーバーのシャットダウン**」の順にクリックします。

       確認ダイアログが開いて、現在実行されているジョブのリストが表示されます。Lenovo XClarity Administrator を再起動すると、ジョブはキャンセルされます。
    2. 「**再起動**」をクリックします。

       Lenovo XClarity Administrator がシャットダウンすると、Lenovo XClarity Administrator への接続が失われます。
    3. Lenovo XClarity Administrator が再起動するまで数分待ってから再度ログオンしてください。
  - シャットダウン後にハイパーバイザーから Lenovo XClarity Administrator を再起動します。
    - Microsoft Hyper-V
      1. サーバー マネージャーのダッシュボードで、「Hyper-V」クリックします。
      2. サーバーを右クリックし、「**Hyper-V マネージャー**」をクリックします。
      3. 仮想マシンを右クリックし、「**起動**」をクリックします。仮想マシンが始動すると、次の例に示すように、各インターフェースの IPv4 および IPv6 アドレスがリストに表示されます。

         XClarity Administrator eth0 管理ポートは、デフォルトで DHCP IP アドレスを使用します。XClarity Administrator のブート・プロセスの最後に、eth0 管理ポート用の静的 IP アドレスを選択できます。次の例のように、プロンプトが表示されたら 1 を入力します。プロンプトは 150 秒間表示され、その後ログイン・プロンプトが表示されます。待たずにログイン・プロンプトに進むには、プロンプトで x を入力します。

         重要：

- 静的 IP アドレスの設定を変更する場合、最大 60 秒以内に新しい設定を入力します。必要な IP 情報があることを確認してから続行します。
  - IPv4 設定では、IP アドレス、サブネット・マスク、およびゲートウェイ IP アドレスが必要です
  - IPv6 設定では、IP アドレスおよびプレフィックスの長さが必要です
- DHCP サーバーを使用していない場合は、構成ファイルを使用して、XClarity Administrator にアクセスするために使用する XClarity Administrator eth0 管理ポートの IP 設定を指定できます。詳細については、以下の「次に行うこと」セクションを参照してください。
- コンソールから IP アドレスの設定を変更した場合、XClarity Administrator が再起動され、新しい設定が適用されます。
- ログインするためにアクションは不要です。コンソールのログイン・メッセージは無視してください。コンソール・インターフェースはお客様用ではありません。
- コンソールに「**TCP: eth0: ドライバーに GRO が実装されている可能性があります。TCP のパフォーマンスが低下する可能性があります**」というメッセージが表示されることがあります。仮想マシンのパフォーマンスには影響しないため、この警告は無視して構いません。

注意：デバイスの管理後に XClarity Administrator 管理ポートの IP アドレスを変更すると、XClarity Administrator でデバイスがオフライン状態になる場合があります。XClarity Administrator の電源がオンになり稼働した後に IP アドレスを変更する場合は、IP アドレスを変更する前に、すべてのデバイスが管理対象から除外されていることを確認してください。

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

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

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

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

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

4. Lenovo XClarity Administrator にログインします (XClarity Administrator へのログインを参照してください)。

– VMware ESXi

1. VMware vSphere Client を介してホストに接続します。
2. 仮想マシンを右クリックし、「**電源**」 ➡ 「**電源オン**」をクリックします。
3. 「**コンソール**」タブをクリックします。仮想マシンが始動すると、次の例に示すように、各インターフェースの IPv4 および IPv6 アドレスがリストに表示されます。

   XClarity Administrator eth0 管理ポートは、デフォルトで DHCP IP アドレスを使用します。XClarity Administrator のブート・プロセスの最後に、eth0 管理ポート用の静的 IP アドレスを選択できます。次の例のように、プロンプトが表示されたら 1 を入力します。プロンプトは 150 秒間表示され、その後ログイン・プロンプトが表示されます。待たずにログイン・プロンプトに進むには、プロンプトで x を入力します。

重要：

- 静的 IP アドレスの設定を変更する場合、最大 60 秒以内に新しい設定を入力します。必要な IP 情報があることを確認してから続行します。
  - IPv4 設定では、IP アドレス、サブネット・マスク、およびゲートウェイ IP アドレスが必要です
  - IPv6 設定では、IP アドレスおよびプレフィックスの長さが必要です
- DHCP サーバーを使用していない場合は、構成ファイルを使用して、XClarity Administrator にアクセスするために使用する XClarity Administrator eth0 管理ポートの IP 設定を指定できます。詳細については、以下の「次に行うこと」セクションを参照してください。
- コンソールから IP アドレスの設定を変更した場合、XClarity Administrator が再起動され、新しい設定が適用されます。
- ログインするためにアクションは不要です。コンソールのログイン・メッセージは無視してください。コンソール・インターフェースはお客様用ではありません。
- コンソールに「**TCP: eth0: ドライバーに GRO が実装されている可能性があります。TCP のパフォーマンスが低下する可能性があります**」というメッセージが表示されることがあります。仮想マシンのパフォーマンスには影響しないため、この警告は無視して構いません。

注意：デバイスの管理後に XClarity Administrator 管理ポートの IP アドレスを変更すると、XClarity Administrator でデバイスがオフライン状態になる場合があります。XClarity Administrator の電源がオンになり稼働した後に IP アドレスを変更する場合は、IP アドレスを変更する前に、すべてのデバイスが管理対象から除外されていることを確認してください。

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

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

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

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

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

4. Lenovo XClarity Administrator にログインします (XClarity Administrator へのログインを参照してください)。

終了後

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

第 3 章　デバイスおよびアクティビティの監視

デバイスおよびアクティビティは、ダッシュ ボード、アラート、監査ログ、およびジョブ ログで監視できます。

環境の概要の表示

ダッシュボードには、すべての管理対象デバイスの現在の状況、すべてのプロビジョニング関連タスクの概要、Lenovo XClarity Administrator リソースおよびアクティビティに関する情報が表示されます。

詳細: XClarity Administrator: 監視

手順

ステップ 1. XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。

ステップ 2. ハードウェア・ステータス、プロビジョニング・ステータス、または管理者活動セクションを展開して、各領域に関する詳細を取得します。

ハードウェア・ステータスの概要の表示

ハードウェア・ステータス領域には、すべての管理対象デバイスのステータスが表示されます。

手順

そのタイプのすべてのデバイスに関する詳細を取得するには、デバイス・タイプに示されている番号をクリックします。

そのタイプおよびステータスのデバイスに関する情報のみを表示するには、アイコンまたは各ステータス・アイコンの横にある数字をクリックします。

- **サーバー**。XClarity Administratorによって管理されているサーバー (計算ノード、ラック・サーバー、およびタワー・サーバー) の総数、および通常、警告、およびクリティカル状況のサーバーの数が表示されます。詳しくは、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。
- **ストレージ**。XClarity Administrator によって管理されているストレージ・デバイスの総数、および通常状況、警告状況、およびクリティカル状況のストレージ・デバイスの数が表示されます。詳しくは、ストレージ・デバイスのステータスの表示を参照してください。
- **スイッチ**。XClarity Administrator によって管理されている RackSwitch および Flex System スイッチの総数、および通常、警告、およびクリティカル状況のスイッチの数が表示されます。詳しくは、スイッチのステータスの表示 を参照してください。
- **Chassis**.XClarity Administrator によって管理されている Flex シャーシの総数、および通常、警告、および重大な状況の Flex シャーシの数が表示されます。詳しくは、管理対象シャーシのステータスの表示を参照してください。
- **ラック**。XClarity Administrator で作成されたラックの数、およびもっとも重大度が高い状況として通常、警告、クリティカル状況にあるデバイスが存在するラックの数が表示されます。詳しくは、ラックのデバイスのステータスの表示を参照してください。
- **リソース・グループ**。XClarity Administrator が管理するリソース・グループの数と、正常、警告、クリティカル (もっとも重大度が高い状況) 状況にあるデバイスが存在するリソース・グループの数が表示されます。詳しくは、リソース・グループのデバイスのステータスの表示を参照してください。

ダッシュボードに表示されるハードウェア・リソースをカスタマイズするには、「**カスタマイズ**」アイコンをクリックします ( )。表示または非表示にするデバイス・タイプを選択できます。単一の要約にサーバーを集約し、サーバーのタイプ (ラックおよびタワー、Flex System、ThinkServer、および NeXtScale サーバー) ごとに別個に要約を表示するか、または特定のタイプのサーバーを省略できます。

プロビジョニング・ステータスの要約の表示

プロビジョニング・ステータス領域には、プロビジョニング・デバイスに関連付けられているすべてのタスクの要約が示されます。

手順

- **構成パターン**。プロファイルがあるサーバーの数について、次の統計データを含む詳細が表示されます。

  注：管理サーバーがライセンス準拠ではない場合、すべての値は 0 です (XClarity Administrator オンライン・ドキュメントの 全機能有効化ライセンスのインストール を参照)。

  - サーバー・プロファイルが適合しているサーバーの数。数字をクリックして、「構成パターン: サーバー・プロファイル」ページと適合しているサーバーのリストを表示できます。
  - サーバー・プロファイルが非適合のサーバーの数。数字をクリックして、「構成パターン: サーバー・プロファイル」ページで非準拠サーバーのリストのリストを表示できます。
  - コンプライアンスの状態が不明なデバイスの数。数字をクリックして、「構成パターン: サーバー・プロファイル」ページと不明なコンプライアンスがあるサーバーのリストを表示できます。

    注：Lenovo XClarity Administrator がサーバーから構成情報を収集しなかった場合、部分的なプロファイルのデプロイメントの後、コンプライアンスの状態が不明になります。サーバー・インベントリーを更新するか、サーバー・プロファイルの詳細ページに再び移動して、強制的にサーバーから構成情報を収集してください。
  - サーバー・プロファイルが割り当てられているサーバーの数。数字をクリックして、「構成パターン: サーバー・プロファイル」ページとプロファイルがあるサーバーのリストを表示できます。
  - サーバー・プロファイルが割り当てられていないサーバーの数。数字をクリックして、「構成パターン: サーバー・パターン」ページと、プロファイルを使用しないでサーバーにデプロイできるサーバー・パターンのリストを表示できます。
  - 現在デプロイされているサーバー・パターンの数。

  構成パターンのトレンド・データを表示するには、「**トレンド・データの表示**」をクリックします (プロビジョニング・ステータスの傾向の監視を参照)。

  構成パターンとサーバー・プロファイルについて詳しくは、構成パターンを使用したサーバーの構成を参照してください。
- 「**オペレーティング・システム・イメージ**」。次の統計データを含むオペレーティング・システム・デプロイメントに関する詳細が表示されます。

注：管理サーバーがライセンス準拠ではない場合、すべての値は 0 です (XClarity Administrator オンライン・ドキュメントの 全機能有効化ライセンスのインストール を参照)。

  - リポジトリ内の OS イメージの数。番号をクリックすると、オペレーティング・システムの一覧が記載された「オペレーティング・システムのデプロイ: OS イメージの管理」ページが表示されます。
  - 進行中の現在の OS デプロイの数。番号をクリックすると、オペレーティング・システムがインストールされたデバイスの一覧が記載された「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページが表示されます。

- 「**ファームウェア更新**」。以下の統計データを含むファームウェア更新に関する詳細が表示されます。
  - 準拠しているデバイス数。数字をクリックして、「ファームウェア更新: 適用/アクティブ化」ページと準拠しているデバイスのリストを表示できます。
  - 準拠していないデバイス数。数字をクリックして、「ファームウェア更新: 適用/アクティブ化」ページと準拠していないデバイスのリストを表示できます。
  - ファームウェア・コンプライアンス・ポリシーが割り当てられていないデバイス数。数字をクリックして、「ファームウェア更新: 適用/アクティブ化」ページとコンプライアンス・ポリシーがないデバイスのリストを表示できます。

    このページで「**割り当て済みポリシー**」列からポリシーを選択して、各デバイスにファームウェア・コンプライアンス・ポリシーを割り当てることができます。
  - 更新がサポートされていないデバイスの数。数字をクリックして、「ファームウェア更新: 適用/アクティブ化」ページと更新がサポートされていないデバイスのリストを表示できます。
  - 進行中の更新の数。
  - ファームウェアが保留状態のデバイスの数。数字をクリックして、「ファームウェア更新: 適用/アクティブ化」ページと更新のアクティベーションが保留中のデバイスのリストを表示できます。

  ファームウェア更新のトレンド・データを表示するには、「**トレンド・データの表示**」をクリックします (プロビジョニング・ステータスの傾向の監視を参照)。

  ファームウェア更新とコンプライアンス・ポリシーについて詳しくは、管理対象デバイスでのファームウェアの更新を参照してください。

Lenovo XClarity Administrator 活動の要約の表示

「XClarity Administrator の活動」領域には、XClarity Administrator のアクティブ・ジョブ、アクティブ・セッション、およびシステム・リソースについての情報が表示されます。

手順

- **ジョブ**。現在進行中のアクティブ・ジョブの数が表示されます。ジョブについて詳しくは、ジョブの監視を参照してください。
- **アクティブ・セッション**。アクティブな XClarity Administrator セッションそれぞれのユーザー ID および IP アドレスが表示されます。ユーザーについて詳しくは、ユーザー・アカウントの管理を参照してください。
- **リソース使用状況**。ホスト・システムおよびリモートファイル共有のプロセッサー使用率、メモリー使用量、およびディスク容量を表示します。システム・リソースについての詳細は、監視システム・リソース を参照してください。

監視システム・リソース

「ダッシュボード」ページから、ホスト・システムのプロセッサー使用率、メモリー使用量、およびディスク容量を確認できます。

始める前に

XClarity Administrator では、以下の*最小要件*が満たされている必要があります。環境の規模と 構成パターン の使用に応じて、最適なパフォーマンスを実現するために追加リソースが必要になることがあります。
- 仮想マイクロプロセッサーが 2 個の場合
- 8 GB のメモリーを搭載している
- 192 GB のストレージを XClarity Administrator 仮想アプライアンスで使用できる
- 最小解像度が幅 1024 ピクセル (XGA) のディスプレイ

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

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

注：

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

手順

Lenovo XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。

ホスト・システムのリソース使用状況が「XClarity Administrator の活動」セクションに表示されます。

プロセッサー
使用率の測定は、ホストのプロセッサーに同時にアクセスしている XClarity Administrator プロセスの数を示します。

ヒント: 使用率の測定値が「高い」または「非常に高い」まで急激に上がる場合があります。使用率が 30 分以上このレベルにある場合は、ジョブ・ログをチェックして長期実行中のジョブが進行中かどうかを確認します (ジョブの監視参照)。

合計容量の測定は、ホストで使用できるプロセッサーの数を示します。

メモリー
使用量の測定は、XClarity Administrator で現在使用されているメモリーの量を示します。

合計容量の測定は、ホストで使用できるメモリーの合計容量を示します。

ユーザー・データ
使用量の測定は、ホスト・システムの XClarity Administrator で現在使用されているディスク容量の量を示します。

合計容量の測定は、オペレーティング・システムやファームウェア更新などのユーザー・データに割りてられたスペースの合計容量 (使用中および未使用) を示します。

ディスク・スペースの管理についての詳細は、ディスク・スペースの管理を参照してください。

注意：割り当てられたリソースが良好なパフォーマンスで現在数の管理対象デバイスを処理するために不十分である場合は、リソースの割り当てを増やすことを検討してください。ご使用の環境の管理対象デバイスの数に基づく推奨ハードウェア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。

プロビジョニング・ステータスの傾向の監視

Lenovo XClarity Administrator は定期的に、すべての管理対象デバイスのファームウェア更新や構成パターンのコンプライアンスおよびアクティブなジョブを含むプロビジョニング・ステータスを収集するため、一定期間の傾向を監視することができます。

このタスクについて

トレンド・データを表示するには、**lxc_admin** または **lxc-supervisor** 権限が必要です。

次のデータが収集されます。

- **ファームウェア更新**
  - **適合デバイス**。割り当てられているファームウェア・コンプライアンス・ポリシーに適合しているデバイス数
  - **非適合デバイス**。割り当てられているファームウェア・コンプライアンス・ポリシーに適合していないデバイス数
  - **ポリシーのないデバイス**。ファームウェア・コンプライアンス・ポリシーが割り当てられていないデバイス数
  - **更新がサポートされていないデバイス**。ファームウェア更新がサポートされていないデバイス数
  - **進行中の更新**。ファームウェア更新が進行中のデバイス数
- **構成パターン**
  - **プロファイルを持つサーバー**。サーバー・プロファイルが割り当てられているデバイスの数
  - **プロファイルを持たないサーバー**。サーバー・プロファイルが割り当てられていないデバイスの数
  - **適合サーバー**。割り当てられたサーバー・プロファイルに適合しているデバイスの数
  - **非適合サーバー**。割り当てられたサーバー・プロファイルに適合していないデバイスの数
  - **パターンが進行中のサーバー**。構成パターン更新が進行中のデバイス数

手順

プロビジョニング・ステータスの傾向を表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックして、「ダッシュボード」ページを表示します。

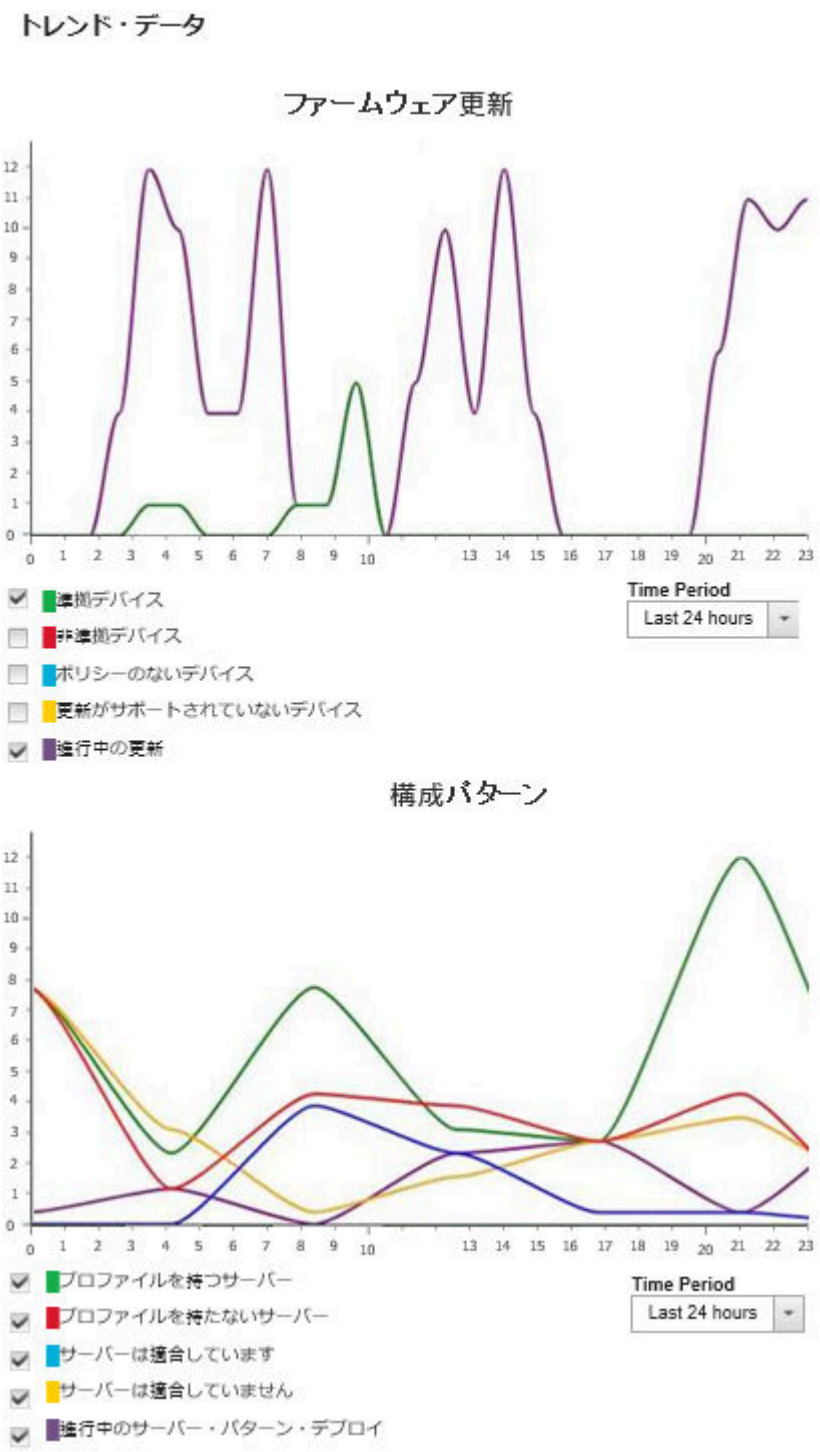
ステップ 2. 「**トレンド・データ**」リンクをクリックして「しきい値設定」ダイアログを表示します。

ステップ 3. 表示するデータを選択または選択解除します。

ステップ 4. 表示する期間を選択します。

- **24 時間**。直近 24 時間のデータを表示します。各データ・ポイントは、1 時間の平均です。
- **1 カ月**。直近 30 日のデータを表示します。各データ・ポイントは、24 時間の平均です。

トレンド・データは、選択された期間のグラフで表示されます。



履歴メトリックの監視

Lenovo XClarity Administrator では、管理対象の ThinkSystem および ThinkAgile デバイスのメトリック・データを定期的に収集するため、ご使用の環境の現在の状態を分析することができます。

始める前に

履歴メトリックは ThinkSystem サーバーでのみサポートされています (SR635、SR645、SR655、および SR665 を除く)。

2019 年 4 月以降にリリースされた XCC ファームウェアを実行する ThinkAgile サーバーおよび ThinkSystem サーバー (SR635 および SR655 を除く) の SSD のみがサポートされます。

オンボード SATA ドライバーはサポートされません。

NVMe ドライブは、NVMe 管理インターフェース (NVMe-MI) 仕様をサポートしている必要があります。

このタスクについて

以下のメトリックが収集されます。

- **SSD 監視**このレポート・カードには、次の統計情報とグラフが含まれています。
  - 管理対象デバイス内の SSD の総数 (スコープに基づく)。
  - 分析された SSD の数
  - 分析の対象ではない SSD の数
  - 残り寿命が特定の範囲にある SSD を持つデバイスの数を示す円形グラフ。
    - 残り寿命 <= 10%。残り寿命が 10% 以下の SSD の数
    - 残り寿命 11 ～ 50%。残り寿命が 11 ～ 50% の SSD の数
    - 残り寿命 51 ～ 100%。残り寿命が 50% を超える SSD の数
- **システム使用率**このレポート・カードには、次の統計情報とグラフが含まれています。
  - 現在のプロセッサー使用率 (パーセント)
  - 現在のメモリー使用率 (パーセント)
  - プロセッサーとメモリーの時間経過に伴う使用率を示す折れ線グラフ
- **電力消費量**このレポート・カードには、次の統計情報とグラフが含まれています。
  - すべての電源の現在の合計電源入力 (ワット)
  - 合計電源入力を時系列で示す折れ線グラフ
- **デバイスの温度**このレポート・カードには、次の統計情報とグラフが含まれています。
  - 吸気口の現在の最大温度 (摂氏)
  - 最大温度を時系列で示す折れ線グラフ

円グラフの色分けされた各線、折れ線グラフの各点、各メトリックの横の数字にカーソルを合わせると、メトリックの詳しい情報が表示されます。凡例の色アイコンをクリックすると、グラフのメトリックを表示または非表示にできます。また、リンクの数字またはカードの右上にある「**設定**」アイコン () のオプションをクリックすると、選択した条件に一致するメトリックを持つすべてのデバイスのリストを表示することもできます。

手順

特定のアクティビティーのフロー・ダイアグラムを表示するには、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、「**監視**」 → 「**履歴メトリック**」をクリックして、各メトリック・タイプのレポート・カードが表示された「履歴メトリック」ページを表示します。

ステップ 2. スコープをデバイスのすべてまたは特定のグループに設定します。

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。

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。

詳細: XClarity Administrator: 監視

このタスクについて

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

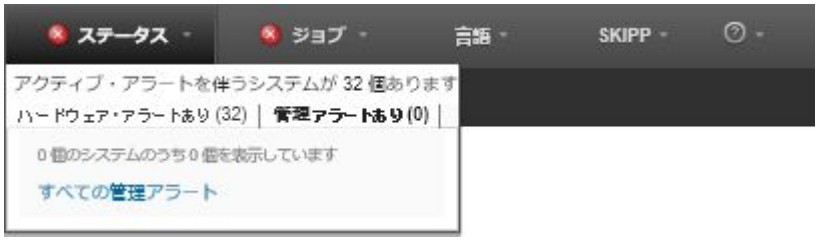
注：Lenovo XClarity Administrator のロケールが別の言語に設定されている場合でも、Lenovo Storage デバイスのアラートは英語でのみ表示されます。必要に応じて、外部翻訳システムを使用してメッセージを翻訳してください。

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 (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。

詳細: XClarity Administrator: 監視

このタスクについて

*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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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 Gmail SMTP サービスにイベント転送をセットアップする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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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

パラメーター	値
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

パラメーター	値
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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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**」トグルをクリックして、除外イベントの転送を許可または禁止します。

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・カテゴリーの一致。**
  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 (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 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。

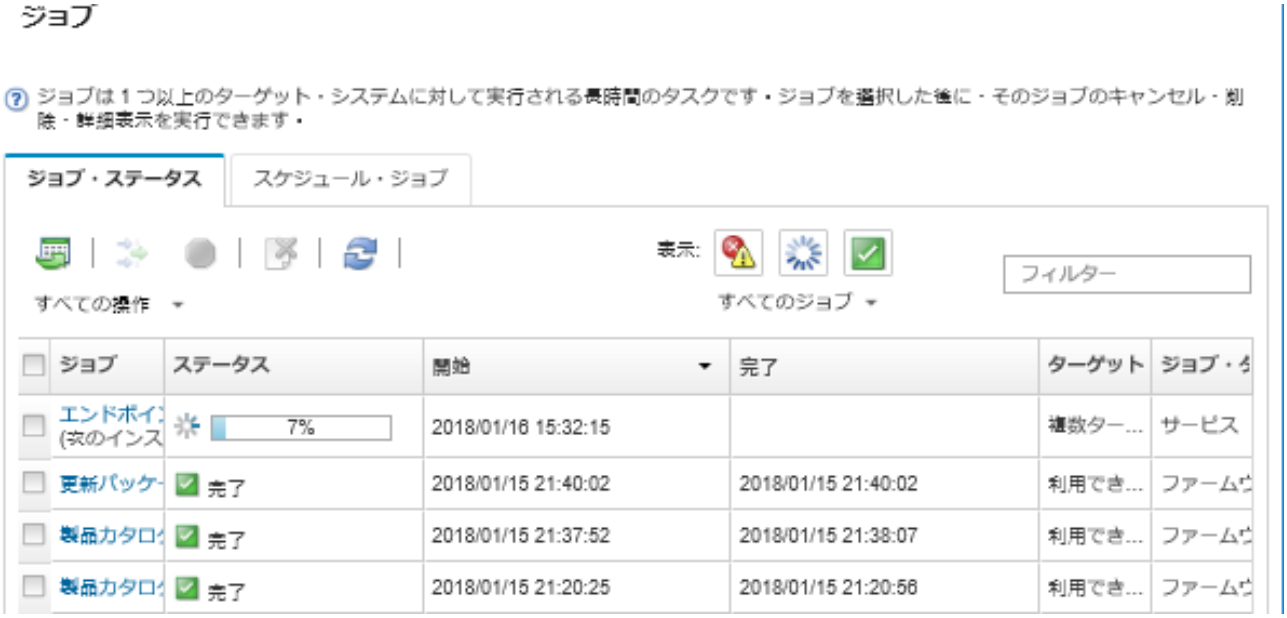
このプルダウンで以下のタブをクリックできます。
- **エラー**。エラーが関連付けられているすべてのジョブのリストが表示されます。
- **警告**。警告が関連付けられているすべてのジョブのリストが表示されます。
- 「**実行中**」。現在進行中のすべてのジョブのリストが表示されます。
- 「**完了**」。完了したすべてのジョブのリストが表示されます。

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。

ジョブおよびイベントの間の関係の表示

*フロー・ダイアグラム*は、アクティビティ (ジョブやイベントなど) 間の関係を示すグラフィカル・ビューです。ユーザーが手動で開始することも、Lenovo XClarity Administrator によって自動的に開始することも

できます。フロー・ダイアグラムで、開始されたアクションのシーケンスと生成されたイベント、それが生成された時間、それが生成された原因を図示化することで、問題を識別しやすくなります。

始める前に

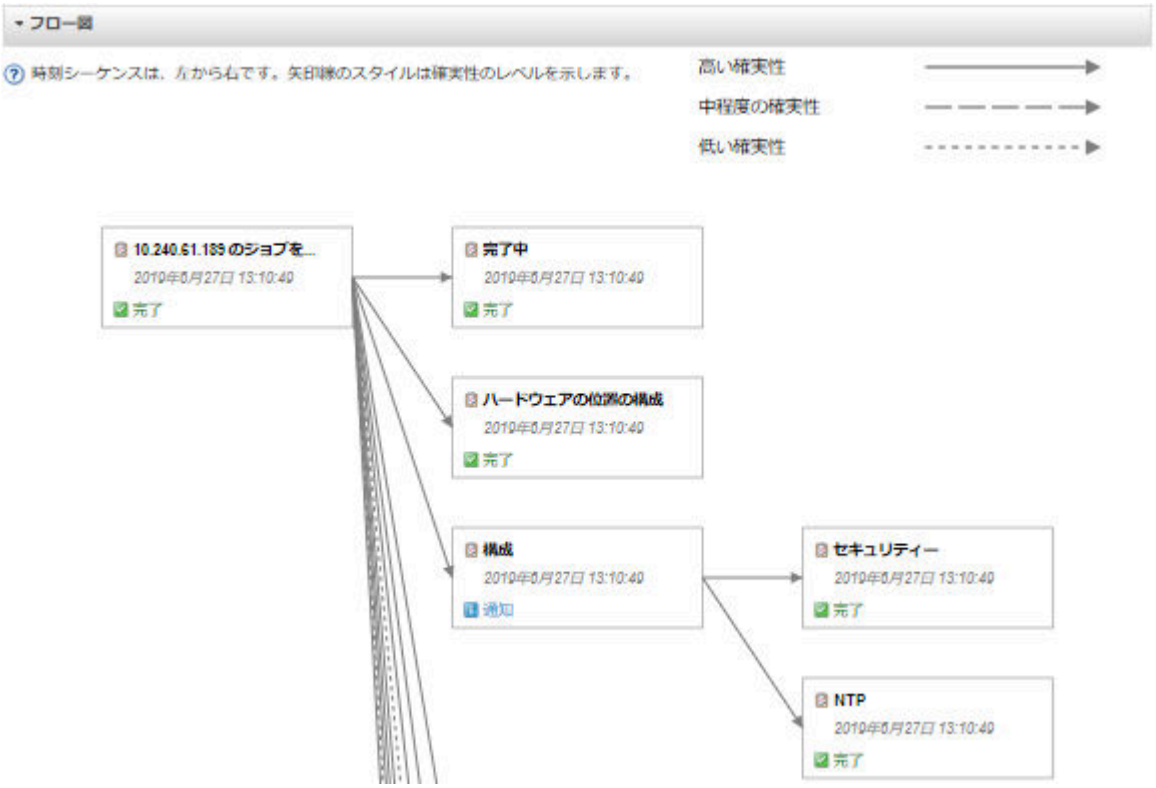
アクティビティー・フローはデフォルトでは無効になっています。アクティビティーについてフローを生成する前に、アクティビティー・フローを有効にする必要があります。アクティビティ・フローが有効になっている場合に発生するアクティビティのみフローを表示できます。

注意：アクティビティー・フローを有効にすると、XClarity Administrator によるメモリー使用量が増加します。既に XClarity Administrator によるメモリー使用量が高い場合は、アクティビティー・フローを有効にしないことをお勧めします。

このタスクについて

以下にフロー・ダイアグラムの例を示します。イベントのシーケンスは左から右に流れます。フロー内の各ノードは単一のアクティビティーを表し、アクティビティーの説明、日付、ステータスが含まれます。ノードのタイトルの上にカーソルを置くと、アクティビティのに関する追加情報が表示されます。

ノード間の線の種類は、ノード間の関係の確実性を表しています。
- 実線は確実性が高いことを表します。
- 長い破線は確実性が中程度であることを表します。
- 短い破線は確実性が低いことを表します。



手順

特定のアクティビティーのフロー・ダイアグラムを表示するには、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、「**監視**」 → 「**アクティビティー・フロー**」をクリックして、「アクティビティー・フロー」ページを表示します。

ステップ 2. 「**アクティビティー・フローの有効化**」を選択してアクティビティー・フローを有効にします。

ステップ 3. 「**アクティビティ**」セクションで、ジョブまたはイベントを選択します。

テーブルの列をソートすると特定のアクティビティーを見つけやすくなります。また、ステータス・タイプ、アクティビティー・タイプ、日付を選択したり、カスタム・フィルターを入力したり、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、選択した条件に一致するアクティビティーのみをリストできます。

ステップ 4. 「**フロー・ダイアグラムの生成**」をクリックして、「**フロー・ダイアグラム**」セクションにフロー・ダイアグラムを表示します。

終了後

このページでは、以下の操作を実行できます。

- フロー・ダイアグラム内の各アクティビティーに関する追加情報を表示する。アクティビティーの上にカーソルを合わせます。
- 選択したアクティビティーの関連フローを CSV ファイルにエクスポートする。「**操作**」 → 「**CSV へのエクスポート**」をクリックします。

第 4 章　管理に関する考慮事項

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

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

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

ThinkSystem、ThinkServer、および System x デバイス

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

Flex System デバイス

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

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

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

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

第 5 章　リソース・グループの管理

リソース・グループを Lenovo XClarity Administrator で使用して、管理対象デバイスをまとめて表示し操作できる論理セットを作成できます。

詳細: XClarity Administrator: リソース・グループ

このタスクについて

リソース・グループには、3 つのタイプがあります。

- **Static**。特定のデバイスのカスタマイズされたグループ。
- **動的**。ルールに基づいたデバイスのグループ (たとえば、特定のタイプのすべてのサーバー)。このグループには、インベントリーのプロパティ・セットに基づいたデバイスの動的リストが含まれています。

リソース・グループを操作することはできません。ただし、グループ内のすべてのデバイスを選択して、すべての選択したデバイスでまとめて操作を実行することはできます。

リソース・グループのデバイスのステータスの表示

リソース・グループのすべての管理対象デバイスのステータスを表示できます。

このタスクについて

以下のステータス・アイコンは、リソース・グループ内のすべてのデバイスの全体的な正常性を示します。グループの全体的な正常性は、グループ内で重大度が最も高いデバイスを示しています。

- 「**クリティカル**」アイコン ( )
- 「**警告**」アイコン ( )
- 「**正常**」アイコン ( )

手順

リソース・グループのデバイスのステータスを表示するには、次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、「**ダッシュボード**」をクリックします。ダッシュボード・ページが開いて、すべての管理対象デバイスとリソース・グループを含むその他のリソースの概要とステータスが表示されます。

ステップ 2. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**リソース・グループ**」の順にクリックします。「すべてのリソース・グループ」ページが表示されます。

「すべてのリソース・グループ」ページには、各リソース・グループが、グループの名前、グループに存在する管理対象デバイスの数、およびグループ内で最も重大度が高いデバイスのステータスとともに表示されます。

このページでは、以下の操作を実行できます。

- 新しいリソース・グループの作成 (動的リソース・グループの作成および 静的リソース・グループの作成を参照)
- グループ・メンバーシップを編集する。グループを選択し、「**編集**」アイコン ( ) をクリックします。
- グループのプロパティを編集する。グループを選択し、「**すべての操作**」 → 「**プロパティの編集**」をクリックします。
- リソース・グループを削除する。グループを選択し、「**削除**」アイコン ( ) をクリックします。

注：グループを削除すると、グループ定義のみが削除されます。グループ内のデバイスには影響しません。

- 1 つ以上のリソース・グループのすべてのデバイスに関する詳細情報を CSV ファイルにエクスポートする。「**エクスポート**」アイコン ( ) をクリックします。

ステップ 3. 「すべてのリソース・グループ」ページで「**グループ**」列の名前をクリックすると、そのグループのデバイス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。

- 静的リソース・グループのデバイスを追加または削除する。「**編集**」アイコン ( ) をクリックします。
- リソース・グループの特定のデバイスに関する詳細情報を表示する。「**デバイス名**」列のデバイス名をクリックします。
- 1 つ以上のリソース・グループのすべてのデバイスに関する詳細情報を CSV ファイルにエクスポートする。「**エクスポート**」アイコン ( ) をクリックします。

リソース・グループのメンバーの表示

グループ・メンバーを含むリソース・グループに関する詳細情報を表示できます。

手順

グループ・メンバーシップを表示するには、以下の手順を実行します。

- デバイスがメンバーとして属するすべてのグループを表示するには
  1. Lenovo XClarity Administrator のメニュー・バーで「**ハードウェア**」をクリックし、すべてのデバイスのページで表示するデバイス・タイプをクリックします。

     「**グループ**」列のグループのリストにカーソルを合わせると、デバイスがメンバーとして属するグループの一覧が表示されます。

2. 最初の列のデバイス名のリンクをクリックします。そのデバイスの要約ページが表示され、デバイスがメンバーとして属するリソース・グループのリストが表示されます。

- グループのメンバーを表示するには
  1. XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。ダッシュボード・ページが開いて、すべての管理対象デバイスとラックを含むその他のリソースの概要とステータスが表示されます。
  2. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**グループ**」の順にクリックします。「リソース・グループ」ページが表示されます。

     このページでは、グループ内のメンバーの合計数と、デバイス・タイプごとのメンバー数が一覧表示されます。

3. 「すべてのリソース・グループ」ページで「**グループ**」列の名前をクリックすると、リソース・グループの詳細が表示されます。

   このページには、そのリソース・グループのメンバーである各デバイスが表示されます。

動的リソース・グループの作成

一連の条件に基づいて、管理対象デバイスを動的にセットにするリソース・グループを作成できます。

このタスクについて

各デバイス・タイプについて、次の 1 つ以上の条件を使用して動的リソース・グループを作成できます。

条件	シャーシ	高密度シャーシ	サーバー	Flex System スイッチ	RackSwitch スイッチ	ストレージ・デバイス
アドイン・カード名			✓ (ThinkServer を除く)			
連絡先	✓		✓		✓	✓
説明	✓	✓	✓		✓	✓
完全修飾ドメイン名	✓		✓			

条件	シャーシ	高密度シャーシ	サーバー	Flex System スイッチ	RackSwitch スイッチ	ストレージ・デバイス
ホスト名	✓		✓	✓	✓	
IPv4 アドレス*	✓		✓	✓	✓	✓
IPv6 アドレス	✓		✓	✓	✓	
ロケーション	✓	✓	✓		✓	✓
マシン・タイプ	✓		✓	✓	✓	✓
モデル番号	✓		✓	✓	✓	✓
全体のヘルス状態	✓		✓	✓	✓	✓
プロセッサー・コア			✓			
製品名	✓		✓	✓	✓	✓
ラック	✓	✓	✓		✓	✓
部屋	✓	✓	✓		✓	✓
ユーザー定義名	✓	✓	✓	✓	✓	✓

注：IPv4 アドレスの場合、単一のアドレスを指定したり、アドレス範囲をダッシュで区切るかアスタリスクをワイルドカードとして使用して指定 (たとえば、1.1.1.* や 1.1.1.1-1.1.1.255 (スペースなし)) したりできます。

手順

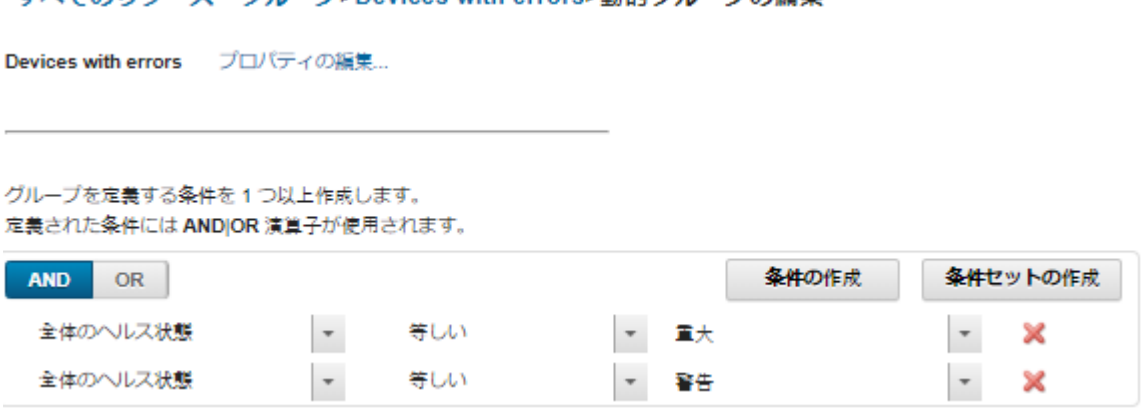
動的リソース・グループを作成して設定するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**リソース・グループ**」の順にクリックします。「すべてのリソース・グループ」ページが表示されます。

ステップ 2. 「**作成**」アイコン ( ) をクリックして、空のグループを作成します。「空のグループの作成」ダイアログが表示されます。

ステップ 3. 「**動的グループ**」を選択して、一連の条件に基づいてデバイスをグループにします。

ステップ 4. 「**作成**」をクリックします。「動的グループの編集」ダイアログが表示されます。



ステップ 5. この動的グループの条件を追加します。

- グループのセットで使用するオペレーターを選択します。これは以下のいずれかの値です。
  - AND。メンバーは、指定された値をすべて満たす必要があります。
  - OR。メンバーは、指定された値を 1 つ以上満たす必要があります。

- 「**条件の作成**」をクリックして、新しい条件をセットに追加します。
- 「**条件セットの作成**」をクリックして条件ルールのサブセットを追加します。

注：新しい条件と条件セットは、常にリストの最後に追加されます。

ステップ 6. 「**適用**」をクリックしてグループ条件を保存しグループを作成するか、「**プレビュー**」をクリックして、グループを作成することなく現在の条件を使用するグループに含まれデバイスを確認します。

終了後

- すべてのデバイスのページおよびデバイス要約ページの「**グループ**」列から、デバイスが属するリソース・グループを確認できます。
- 動的グループの条件を変更するには、リソース・グループを選択して、「**編集**」アイコン ( ) をクリックします。
- 「**すべての操作**」 → 「**プロパティの編集**」の順にクリックして、リソース・グループのプロパティを変更できます。

静的リソース・グループの作成

管理対象デバイスのカスタマイズされたセットを含むリソース・グループを作成できます。

手順

静的リソース・グループを作成して設定するには、以下の手順を実行します。

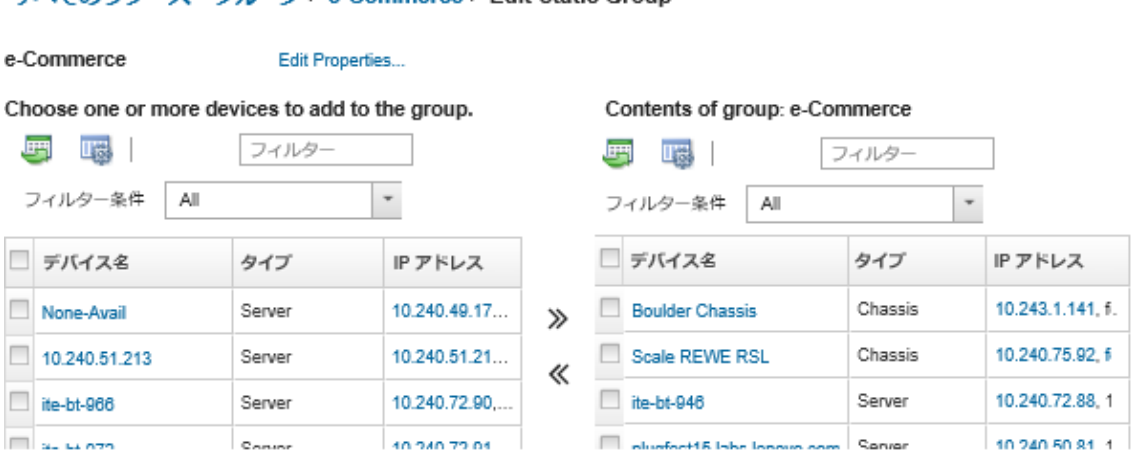
ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**リソース・グループ**」の順にクリックします。「リソース・グループ」ページが表示されます。

ステップ 2. 「**作成**」アイコン ( ) をクリックして、空のグループを作成します。「空のグループの作成」ダイアログが表示されます。

ステップ 3. グループ名と任意の説明を指定します。

ステップ 4. 「**静的グループ**」を選択して明示的に定義されたデバイスのグループを作成します。

ステップ 5. 「**作成**」をクリックします。「静的グループの編集」ページが表示されます。



ステップ 6. 「**グループに属していない選択可能デバイス**」リストからグループに追加するデバイスを選択して「**追加**」アイコン ( ) をクリックし、選択したデバイスを「**グループの内容**」リストに移動します。

注：

- 列ヘッダーをクリックしてリストをソートすると特定のストレージ・デバイスを見つけやすくなります。「**フィルター条件**」ドロップダウン・リストでデバイス・タイプを選択し、ドロップダウン・リストからシャーシを選択するか、または「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、ステータス・アイコンをクリックすると、選択された条件に一致するデバイスのみをリストすることもできます。
- シャーシをグループに移動する場合、シャーシ内のデバイスは自動的にグループに追加されません。すべてのシャーシ・コンポーネントをグループに追加するには、「**表示**」で「**シャーシ**」 → *<chassis_name>*を選択します。これによって指定したシャーシ内のすべてのコンポーネントがリストされます。次に、「デバイス名」列ヘッダーの隣にあるチェック・ボックスを選択してすべてのデバイスを選択し、「**追加**」アイコン (≫) をクリックして、選択したデバイスを「**グループの内容**」リストに移動します。

終了後

- すべてのデバイスのページおよびデバイス要約ページの「**グループ**」列から、デバイスが属するリソース・グループを確認できます。
- デバイスを静的リソース・グループに追加またはグループから削除するには、すべてのデバイスのページおよびデバイスの詳細ページから、「**すべての操作**」 → 「**グループ**」 → 「**グループに追加**」 または「**すべての操作**」 → 「**グループ**」 → 「**グループから削除**」をクリックします。

  注：デバイスを追加および削除できるのは静的リソース・グループのみです。動的グループから削除することはできません。
- 「**すべての操作**」 → 「**プロパティの編集**」の順にクリックして、リソース・グループのプロパティを変更できます。

リソース・グループの削除

Lenovo XClarity Administrator からリソース・グループを削除できます。

このタスクについて

グループを削除すると、グループ定義のみが削除されます。そのグループ内のデバイスには影響しません。

手順

リソース・グループを削除するには、次の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**リソース・グループ**」の順にクリックします。「すべてのリソース・グループ」ページが表示されます。

「すべてのリソース・グループ」ページには、各リソース・グループが、グループの名前、グループに存在する管理対象デバイスの数、およびグループ内で最も重大度が高いデバイスのステータスとともに表示されます。

ステップ 2. 削除するリソース・グループを選択します。

ステップ 3. 「**削除**」アイコン (✖) をクリックします。

ステップ 4. 「**削除**」をクリックします。

リソース・グループのプロパティの変更

特定のリソース・グループのプロパティを変更できます。

手順

リソース・グループのプロパティを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**リソース・グループ**」の順にクリックして、「すべてのリソース・グループ」ページを表示します。

ステップ 2. 更新するリソース・グループを選択します。

ステップ 3. 「**すべての操作**」 → 「**プロパティの編集**」をクリックし、「グループ・プロパティの編集」ダイアログを表示します。

ステップ 4. 以下の情報を必要に応じて変更します。
- グループ名
- 説明

ステップ 5. 「**保存**」をクリックします。

注：変更されたプロパティが XClarity Administrator Web インターフェースに表示されるまで少し時間がかかる場合があります。

第 6 章　ラックの管理

Lenovo XClarity Administrator でラックを使用すると、データセンターのラックの物理的構成を反映して管理対象デバイスをグループ化できます。

始める前に

シャーシ間でノードを移動した後、シャーシが含まれている XClarity Administrator でラックを編集する前に、5 ～ 10 分待ちます。

ラックからデバイスを移動すると、デバイス・インベントリーで、ラック名と最小ラック・ユニット値がクリアされます。部屋と場所の値はクリアされません。

このタスクについて

この手順では、管理対象デバイスとフィラーを含む 1 つのラックを手動で作成および設定する方法を説明します。

ラックに多数のデバイスを追加する必要がある場合や、多数のラックを編集する必要がある場合は、スプレッドシートを使用して一括インポートを実行するか、PowerShell スクリプトを実装してタスクを自動化することを検討してください。一括インポートの使用について詳しくは、シャーシの管理およびサーバーの管理を参照してください。PowerShell スクリプトに関する詳細は、XClarity Administrator オンライン・ドキュメントの PowerShell (LXCAPSTool) ツールキット を参照してください。

XClarity Administrator は管理可能なデバイス内で定義されたラックのプロパティを認識します。そのデバイスを管理する場合、XClarity Administrator はそのデバイスにシステム・プロパティを設定し、ラック・ビューを更新します。ラックが XClarity Administratorに存在していない場合、新規ラックが作成され、その新規ラックにデバイスが追加されます。

注：

- System x3500 M5 サーバー、NeXtScale nx360 M5 サーバー、ThinkServer SD350 サーバーおよびタワー・サーバーはラック・ビューではサポートされていません。
- System x3850 X5 スケーラブル複合システム、それぞれのラックに、各ノード (サーバー) を追加する必要があります。
- XClarity Administrator が再起動した時のデモのハードウェアは、ラック ビューで永続的ではありません。

手順

ラックを作成して設定するには、以下の手順を実行します。

- 管理対象デバイスを含む 1 つのラックを作成および設定します。
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**ラック**」の順にクリックします。「すべてのラック」ページが表示されます。

     「すべてのラック」ページには、各ラックのサムネール・イメージが、ラックの名前、ラックに存在する管理対象デバイスの数、および最も重大度が高いデバイスのステータスとともに表示されます。

     注：ツールバーの以下のアイコンをクリックすると、ラックを重大度別にフィルタリングできます。また、「**フィルター**」フィールドにラック名を入力して、表示されるラックを絞り込むこともできます。
     – 「**クリティカル・アラート**」アイコン ()

– 「**警告アラート**」アイコン ( )
– 「**正常アラート**」アイコン ( )

2. 「**作成**」アイコン ( ) をクリックして、空のラックを作成します。「空のラックの作成」ダイアログが表示されます。
3. ラックの名前、高さ、場所、部屋を入力します。

   注：

   – ラック名は、固有である必要はありません。場所または部屋、あるいは両方が異なる限り、同じ名前のラックを作成できます。
   – ラック名には、大文字、小文字、数字、および特殊文字 (ピリオド (.)、ダッシュ (-)、アンダスコア (_)) のみ使用できます。
   – ロケーションには最大 23 文字使用できます。
4. 「**作成**」をクリックします。「すべてのラック」ページに新しいラックのサムネール・イメージが追加されます。
5. そのラックのサムネール・イメージをダブルクリックします。ラック・ビュー・ページに空のラックのイメージとそのラックのプロパティが表示されます。

6. 「**ラックの編集**」をクリックして、「ラックの編集」ページを表示します。

7. 該当する管理対象のデバイスとフィラーをすべてグラフィカル・ビューに追加します。

   注：オンライン状態の管理対象デバイスのみラックに追加できます。

   - ラックに追加されていない管理対象シャーシのリストを表示するには、「**シャーシ**」タブをクリックします。管理対象シャーシをラックの目的の場所にドラッグ・アンド・ドロップして、シャーシをラックに追加します。
   - ラックに追加されていない管理対象ラック・サーバーおよびマルチノード・サーバー格納装置のリストを表示するには、「**サーバー・エンクロージャー**」タブをクリックします。ラック・サーバーまたはサーバー格納装置をラックの目的の場所にドラッグ・アンド・ドロップして、ラック・サーバーをラックに追加します。
   - ラックに追加されていない管理対象 RackSwitch スイッチのリストを表示するには、「**RackSwitch**」タブをクリックします。RackSwitch スイッチをラックの目的の場所にドラッグ・アンド・ドロップして、スイッチをラックに追加します。
   - 各種ストレージ・デバイスのリストを表示するには、「**ストレージ**」タブをクリックします。目的のストレージ・デバイスをラックの目的の場所にドラッグ・アンド・ドロップして、ストレージ・デバイスをラックに追加します。
   - 各種フィラーのリストを表示するには、「**フィラー**」タブをクリックします。目的のフィラーをラックの目的の場所にドラッグ・アンド・ドロップして、フィラーをラックに追加します。

     フィラーは、XClarity Administrator で管理されていないラック内にあるデバイスです。使用可能なフィラーは次のとおりです。
     - 汎用フィラー
     - 汎用ラック装着スイッチ
     - ストレージ・コントローラーとエンクロージャー
     - パートナー・ストレージ・コントローラーとエンクロージャー (IBM、NetApp、EMC など)

   - ラックからデバイスを追加または削除する場合は、そのデバイスのロケーション、設置部屋、ラック、最下段ラック・ユニットのプロパティが更新されます。
   - 「**表示順**」ドロップダウン・リストを使用して各タブのデバイスのリストをソートできます。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるデバイスを絞り込むこともできます。
   - ラックから管理対象のデバイスやフィラーを削除するには、それらのオブジェクトをラックの外にドラッグ・アンド・ドロップします。

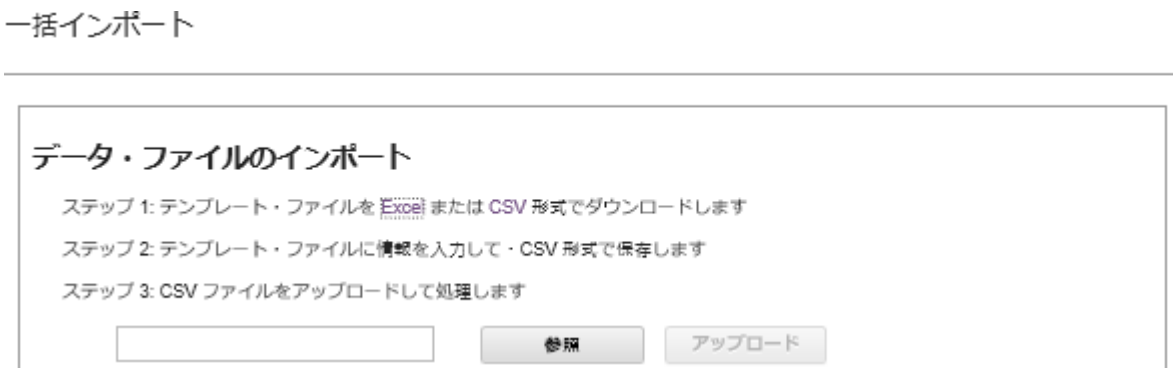
8. 「**保存**」をクリックして、ラック構成を保存します。

   構成プロセスが完了するまでに数分かかることがあります。構成の間に、ラックと場所の情報が管理対象デバイスの CMM やベースボード管理コントローラーにプッシュされます。

9. フィラーをクリックしてから「**プロパティの編集**」をクリックし、ラックに追加したフィラーをカスタマイズします。「プロパティの編集」ダイアログで、そのデバイスの管理ユーザー・インターフェースを起動するために使用される名前、最下段ラック・ユニット (LRU)、および URL を指定できます。

   ヒント: ラック構成を保存した後、ラック内のフィラーをクリックし、「**URL の起動**」リンクをクリックして、フィラーの管理ユーザー・インターフェースを起動できます。

- 一括インポート・ファイルを使用してラックを作成および設定します。
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。
  2. 「**一括インポート**」をクリックします。「一括インポート」ウィザードが表示されます。

  3. 「データ・ファイルのインポート」ページで「**Excel**」リンクまたは「**CSV**」リンクをクリックして、Excel 形式または CSV 形式でテンプレート一括インポート・ファイルをダウンロードします。

     重要：テンプレート・ファイルは、リリースごとに異なる可能性があります。常に最新のテンプレートを使用するように注意してください。

  4. テンプレート・ファイル内のデータ・ワークシートに入力し、そのファイルを CSV 形式で保存します。

     ヒント: Excel テンプレートには、**Data** ワークシートと **Readme** ワークシートが含まれています。**Data** データ・ワークシートを使用して、デバイス・データに入力します。**Readme** ワークシートからは、必須のフィールドなど、**Data** ワークシートの各フィールドへの入力方法に関する情報やサンプル・データを得られます。

     重要：

     – デバイスは、一括インポート・ファイルに記載されている順序で管理されます。
     – XClarity Administratorでは、デバイスが管理されている場合に、デバイスの構成で定義されているラックの割り当て情報を使用します。XClarity Administrator でラックの割り当てを変更した場合、XClarity Administrator によりデバイス構成が更新されます。デバイスの管理後にデバイスの構成を更新した場合、その変更内容が XClarity Administrator に反映されます。
     – ラックをデバイスに割り当てる前に、スプレッドシートでラックを明示的に作成することは、必須ではありませんが、推奨されます。ラックが明示的に定義されていない場合で、XClarity Administrator にラックがまだ存在していないときは、デフォルトの 52U の高さのラックを作成するために、デバイスに指定されたラックの割り当て情報が使用されます。

       ラックで別の高さを使用する場合は、デバイスに割り当てる前に、スプレッドシートでラックを明示的に定義する必要があります。

一括インポート・ファイルでラックを定義するには、次の必須列に入力します。
– (列 A) デバイス・タイプの「ラック」を指定します。
– (列 V) ラック名を指定します。
– (列 X) ラックの高さを指定します。サポートされているラックの高さは、6U、12U、18U、25U、37U、42U、45U、46U、48U、50U、および 52U です。

以下の図は、ラックが定義された一括インポート・ファイルの例を示しています。

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

注：同じ一括インポート・ファイルを使用して、デバイスを管理し、デバイスをラックに追加できます (Lenovo XClarity Administratorオンライン・ドキュメントのシステムの管理 を参照)。

5. 「一括インポート」ウィザードで、CSV ファイルの名前を入力して処理するファイルをアップロードします。このファイルを見つけるには、「**参照**」をクリックします。
6. 「**アップロード**」をクリックしてアップロードし、ファイルを検証します。
7. 管理するラックおよび管理対象のその他のデバイスの概要を確認する場合は、「**次へ**」をクリックすると、「入力要約」ページにラックおよびその他のデバイスのリストが表示されます。
8. 「**次へ**」をクリックして、「デバイスの資格情報」ページを表示します。各タブをクリックし、必要に応じて、特定タイプのすべてのデバイスで使用するグローバルな設定と資格情報を指定します。グローバルな設定と資格情報を使用するデバイスは、各タブの右側に表示されます。
9. 「**管理**」をクリックします。「結果の監視」ページには、一括インポート・ファイル内の各デバイスの管理ステータスに関する情報が表示されます。

   管理プロセスのジョブが作成されます。一括インポート・ウィザードを終了する場合はバックグラウンドで実行されている管理プロセスが続行します。ジョブ・ログから管理プロセスのステータスを監視できます。ジョブ・ログについて詳しくは、170 ページの 「ジョブの監視」を参照してください。

終了後

ラック番号順の設定を変更できます (インベントリー設定の設定を参照)。

ラックのデバイスのステータスの表示

ラックごとに、そのラックのすべての管理対象デバイスのステータスを表示できます。

手順

ラックのすべてのデバイスのステータスを表示するには、次の 1 つ以上の操作を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。
ダッシュボード・ページが開いて、すべての管理対象デバイスとラックを含むその他のリソースの概要とステータスが表示されます。

ステップ 2. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**ラック**」の順にクリックします。「ラック」ページが表示されます。

「ラック」ページには、各ラックのサムネール・イメージが、ラックの名前、ラックに存在する管理対象デバイスの数、および最も重大度が高いデバイスのステータスとともに表示されます。

注：特定のラックを見つけやすくするために、ラック名、ラックのデバイス数、または重大度別に、ラックのリストをソートできます。ソートでは、左から右、上から下の順になります。ツールバーの以下のアイコンをクリックすることで、ラックを重大度別にフィルターできます。さらに、「**フィルター**」フィールドにラック名を入力して、表示されるラックをフィルタリングできます。

- 「**クリティカル・アラート**」アイコン ( )
- 「**警告アラート**」アイコン ( )
- 「**正常アラート**」アイコン ( )

ステップ 3. 「すべてのラック」ページで、ラック名をクリックするか、ラックのサムネールをダブルクリックして、そのラックのグラフィカル・ビューとプロパティを表示します。

前面ラックのグラフィカル・ビューである *ラック・ビュー*には、シャーシ、ラック・サーバー、ラック装着スイッチ、フィラーなど、ラックの各デバイスが表示されます。各デバイスのステータス・アイコンは、そのデバイスの現在のステータスを示します。

このページでは、以下の操作を実行できます。

- 「**ラックの編集**」をクリックして、ラックのデバイスを追加または削除する。

  注：ラックのコンポーネントを変更した場合、変更された情報が XClarity Administrator インターフェースに表示されるまで少し時間がかかる場合があります。
- デバイスおよびフィルターのプロパティ (名前、ロケーション、および管理 Web インターフェースを起動する URL を含む) を変更するには、デバイスまたはフィラーをクリックし、デバイスの要約ペインで「**プロパティの編集**」をクリックします。
- デバイスまたはフィラーの管理コントローラー Web インターフェースを表示するには、デバイスまたはフィラーをクリックし、デバイス要約ペインで「**URL の起動**」リンクをクリックします。

ステップ 4. デバイスまたはコンポーネントの要約または詳細なステータスを表示します。

a. ラックのデバイスまたはコンポーネントをクリックすると、ステータスの要約およびプロパティ、およびそのデバイスまたはコンポーネントのステータスが表示されます。

b. デバイスをダブルクリックすると、デバイスの詳細ページが表示されます。

手順

ラック番号順の設定を変更できます (インベントリー設定の設定を参照)。

ラックの取り外し

Lenovo XClarity Administrator からラックを取り外すことができます。

手順

ラックを取り外すには、次の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**ラック**」の順にクリックします。「すべてのラック」ページが表示されます。

「すべてのラック」ページには、各ラックのサムネール・イメージが、ラックの名前、ラックに存在する管理対象デバイスの数、および最も重大度が高いデバイスのステータスとともに表示されます。

注：特定のラックを見つけやすくするために、ラック名、ラックのデバイス数、または重大度別に、ラックのリストをソートできます。ソートでは、左から右、上から下の順になります。ツールバーの以下のアイコンをクリックすることで、ラックを重大度別にフィルターできます。さらに、「**フィルター**」フィールドにラック名を入力して、表示されるラックをフィルタリングできます。

- 「**クリティカル・アラート**」アイコン ( )
- 「**警告アラート**」アイコン ( )
- 「**正常アラート**」アイコン ( )

ステップ 2. 取り外すラックのサムネールを選択します。

ステップ 3. 「**削除**」アイコン ( ) をクリックします。

ステップ 4. 「**削除**」をクリックします。

結果

ラックのサムネールが「すべてのラック」ページから削除され、そのラックにあったすべてのデバイスが「ラックの編集」ページで他のラックに取り付け可能になります。

第 7 章　シャーシの管理

Lenovo XClarity Administrator では、Flex System シャーシなど、複数のタイプのシステムを管理できます。

詳細: XClarity Administrator: 検出

始める前に

注：シャーシ・コンポーネント (CMM、Flex 計算ノード、Flex スイッチなど) は、それらを含むシャーシを管理する際に自動的に検出され管理されます。シャーシとは別にシャーシ・コンポーネントを検出、管理することはできません。

シャーシを管理する前に、以下の条件が満たされていることを確認してください。

- デバイスを管理する前に、管理に関する考慮事項を検討してください。詳しくは、XClarity Administrator オンライン・ドキュメントの 管理に関する考慮事項 を参照してください。
- 特定のポートが管理対象シャーシの CMM との通信に使用できることが必要です。シャーシを管理する前に、これらのポートが使用可能になっていることを確認します。ポートについて詳しくは、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。
- XClarity Administrator を使用して管理する各シャーシに、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。
- シャーシで、CMM の「**LDAP ユーザーについての同時アクティブ・セッションの数**」設定が 0 (ゼロ) に設定されていることを確認します。この設定は、CMM Web インターフェースで「**管理モジュールの管理**」 ➡ 「**ユーザー・アカウント**」 をクリックし、「**グローバル・ログイン設定**」をクリックして「**全般**」タブをクリックすることにより確認できます。
- CMM とのアウト・オブ・バンド通信に使用する TCP コマンド・モード・セッションが少なくとも 3 つ設定されていることを確認します。セッション数の設定については、CMM オンライン・ドキュメントの tcpcmdmode コマンドを参照してください。
- XClarity Administrator から*別の*サブネットにあるシャーシを検出するには、以下のいずれかの条件を満たしていることを確認してください。
  - マルチキャスト SLP 転送が環境内のルーターと同様にラック装着スイッチで有効になっていることを確認します。マルチキャスト SLP 転送が有効になっているかどうかを調べる方法や、無効になっている場合に有効にする方法については、そのスイッチやルーターに付属のドキュメントを参照してください。
  - SLP がエンドポイントまたはネットワークで無効の場合、DNS 検出メソッドを代わりに使用できます。これを行うには、手動でサービス・レコード (SRV レコード) をドメイン・ネーム・サーバー (DNS) に追加します。たとえば XClarity Administrator の場合は次のようになります。
    ```
    _lxca._tcp.labs.lenovo.com    service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```
    次に、管理 Web インターフェースから CMM の DNS 検出を有効にします。これを行うには、「**管理モジュールの管理**」 ➡ 「**ネットワーク・プロトコル**」の順にクリックし、「DNS」タブをクリックして「**Lenovo XClarity Administrator の検出に DNS を使用する**」を選択します。

    注：
    - DNS を使用した自動検出をサポートするには、CMM が 2017 年 5 月以降のファームウェア・レベルを実行している必要があります。

– ご使用の環境に複数の XClarity Administrator インスタンスがある場合、検索要求に最初に応答したインスタンスによってのみ、シャーシが検出されます。シャーシはすべてのインスタンスによっては検出されません。

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

注意：Flex スタック・リリース 1.3.2.1 2PET12K から 2PET12Q までのファームウェア・レベルを実行している、3 週間以上実行中でデュアル CMM 構成の CMM を管理する場合は、ファームウェアを更新する前に、XClarity Administrator を使用して CMM の仮想再取り付けを行う必要があります。

重要：Lenovo XClarity Administrator の他に別の管理ソフトウェアを使用してシャーシを監視する場合、その管理ソフトウェアで SNMPv3 通信が使用されているときは、まず、適切な SNMPv3 情報で構成されたローカル CMM ユーザー ID を作成し、そのユーザー ID で CMM にログインして、パスワードを変更する必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントの管理に関する考慮事項を参照してください。

このタスクについて

XClarity Administrator を使用すると、XClarity Administrator と同じ IP サブネットにある管理可能システムのプローブによって、環境内のシャーシを自動的に検出できます。他のサブネットにあるシャーシを検出するには、IP アドレスまたは IP アドレス範囲を指定するか、スプレッドシートから情報をインポートします。

シャーシが XClarity Administrator の管理対象になると、XClarity Administrator は各管理対象シャーシを定期的にポーリングして、インベントリー、重要な製品データ、ステータスなどの情報を収集します。各管理シャーシを表示および監視して、管理操作 (システム情報、ネットワーク設定、フェイルオーバーなど) を実行できます。保護モードのシャーシについては、管理操作は無効になっています。

シャーシは*XClarity Administrator 管理対象認証*を使用して管理されます。

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

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

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

  注：

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

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

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

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

– XClarity Administrator 認証サーバーとしてローカルまたは外部 LDAP サーバーを使用している場合は、その認証サーバーで定義されているユーザー・アカウントが XClarity Administrator ドメイン内の XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されます。ローカルの CMM および管理コントローラー・ユーザー・アカウントは無効になります。

– XClarity Administrator 認証サーバーとして SAML 2.0 ID プロバイダーを使用する場合、SAML アカウントは、管理対象デバイスにアクセスできなくなります。ただし、SAML ID プロバイダーと LDAP サーバーを同時に使用する場合で、ID プロバイダーが LDAP サーバーにあるアカウントを使用する場合、LDAP ユーザー・アカウントを使用して管理対象デバイスにログインできます。また、SAML 2.0 が提供するより高度な認証方法 (マルチファクター認証およびシングル・サインオンなど) を使用して XClarity Administrator にログインすることもできます。

– シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます (XClarity Administratorオンライン・ドキュメントの「を参照)

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

– ThinkSystem SR635 および SR655 サーバーで管理対象認証が有効になっている場合:

  – ベースボード管理コントローラー・ファームウェアは、最大 5 つの LDAP ユーザー・ロールをサポートします。XClarity Administrator は、管理中に次の LDAP ユーザー・ロールをサーバーに追加します: **lxc-supervisor**、**lxc-sysmgr**、 **lxc-admin**、**lxc-fw-admin** および **lxc-os-admin**。

    ThinkSystem SR635 および SR655 サーバーと通信するには、指定された少なくとも 1 つの LDAP ユーザー・ロールにユーザーが割り当てられている必要があります。

  – 管理コントローラーのファームウェアは、サーバーのローカル・ユーザーと同じユーザー名の LDAP ユーザーをサポートしていません。

– ThinkServer サーバーおよび System x M4 サーバーの場合は、XClarity Administrator 認証サーバーは使用しません。その代わり、デバイスで接頭辞「LXCA_」の後にランダムな文字列が続く IPMI アカウントが作成されます。(既存の IPMI ローカル・ユーザー・アカウントは無効になります。)ThinkServer サーバーを管理解除する場合は、「LXCA_」ユーザー・アカウントが無効になり接頭辞「LXCA_」が接頭辞「DISABLED_」に置き換えられます。ThinkServer サーバーが別のインスタンスによって管理されているかどうかを判別するために、XClarity Administrator は接頭辞「LXCA_」がついた IPMI アカウントを確認します。管理対象 ThinkServer サーバーの管理を強制することを選択した場合、そのデバイスで「LXCA_」がついたすべての IPMI アカウントが無効になり名前を変更されます。不要になった IPMI アカウントを手動で消去することを検討してください。

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

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

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

1 台のデバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず最初の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。管理対象除外プロセス中にエラーが発生した場合、新規の XClarity Administrator で管理する際に「**管理の強制**」オプションを選択できます。

注：管理可能デバイスのネットワークをスキャンする場合、XClarity Administrator は、デバイスがすでに別のマネージャーで管理されているかどうかは、まずデバイスを管理しようとしなければ分かりません。

管理プロセスでは、XClarity Administrator によって以下の処理が実行されます。

- 指定された資格情報を使用してシャーシにログインする。
- 各シャーシ内のすべてのコンポーネント (CMM、計算ノード、ストレージ・デバイス、Flex スイッチなど) についてインベントリーを収集する。

  注：管理プロセスが完了した後、インベントリー・データが一部収集されます。すべてのインベントリー・データが収集されるまで、シャーシの状態は「保留中」になります。管理対象デバイスでは、そのデバイスのすべてのインベントリー・データが収集されてシャーシの状態が「保留中」でなくなるまで、サーバー・パターンのデプロイなどの特定のタスクを実行できません。
- すべての管理対象デバイスが XClarity Administrator の NTP サーバーを使用するように、NTP サーバーの設定を構成する。
- 最後に編集したファームウェア・コンプライアンス・ポリシーをシャーシに割り当てます。
- Lenovo Flex デバイスの場合は、オプションでデバイスのファイアウォール規則を構成し、XClarity Administrator からの受信要求のみを受け入れるようにします。
- CMM とのセキュリティー証明書の交換時に、CMM のセキュリティー証明書を XClarity Administrator 信頼ストアにコピーし、XClarity Administrator の CA セキュリティー証明書を CMM に送信する。CMM は CMM 信頼ストアに証明書を読み込んで、計算ノード・サービス・プロセッサーに配布し、その信頼ストアに含めます。
- 管理対象認証を構成します。CMM LDAP クライアント設定は認証サーバーとして XClarity Administrator を使用するように変更され、CMM のグローバル・ログイン設定は「**外部認証サーバーのみ**」に変更されます。管理対象認証について詳しくは、認証サーバーの管理を参照してください。
- リカバリー・ユーザー・アカウント (`RECOVERY_ID`) を作成します。`RECOVERY_ID` アカウントについて詳しくは、認証サーバーの管理を参照してください。

注意：シャーシを管理する場合、XClarity Administrator は、セキュア TCP コマンド・モードでの同時接続の最大数を 15 に変更し、レガシー TCP コマンド・モードでの同時接続の最大数を 0 に設定します。これにより、CMM で既に行った設定が上書きされます。

注：XClarity Administrator の管理プロセスでは、セキュリティー設定または暗号化設定 (暗号モードとセキュアな通信に使用されるモード) は変更されません。暗号化設定は、シャーシを管理対象にした後に変更できます (管理サーバーでの暗号化設定の構成)。

手順

XClarity Administrator を使用してシャーシを検出し、管理するには、以下のいずれかの手順を実行します。

- 一括インポート・ファイルを使用して多数のシャーシとその他のデバイスを検出および管理します (Lenovo XClarity Administratorオンライン・ドキュメントのシステムの管理を参照してください)。
- XClarity Administrator と同じ IP サブネットにあるシャーシを検出して管理する。
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「新しいデバイスの検出と管理」ページが表示されます。

     テーブルの列をソートすると、管理するシャーシを見つけやすくなります。「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるシャーシを絞り込むこともできます。「**列のカスタマイズ**」アイコン ( ) をクリックして、表示する列とデフォルトのソート順序を変更できます。
  2. 「**更新**」アイコン ( ) をクリックして、XClarity Administratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
  3. 管理プロセス中にすべてのデバイスのファイアウォール規則を変更して XClarity Administrator からの受信要求のみを受け入れるようにするには、「**今後すべての管理対象デバイスで Encapsulation を有効にする**」チェックボックスをクリックします。

     Encapsulation は、特定のデバイスが管理対象になった後で有効または無効にできます。

     注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。

4. 管理するシャーシを 1 台以上選択します。
5. 「**選択を管理**」をクリックします。
6. このデバイスで XClarity Administrator 管理対象認証またはローカル認証を使用するように選択します。管理対象認証はデフォルトで選択されています。ローカル認証を使用するには、「**管理対象認証**」をオフにします。

   注：管理対象認証およびローカル認証は、ThinkServer および System x M4 サーバーではサポートされていません。
7. デバイスで使用する資格情報を選択して適切な資格情報を指定します。
   - **手動で入力した資格情報を使用**
     - CMM への認証に使用される、**lxc-supervisor** 権限を持つローカル・ユーザー ID とパスワードを指定します。
     - (オプション) パスワードが現在、デバイスで有効期限が切れている場合は、指定された CMM ユーザー・アカウントの新しいパスワードを指定します。
   - **保存された資格情報を使用**

     この管理対象デバイスで使用する **lxc-supervisor** 権限を持つ、保存された資格情報を選択します。「**保存された資格情報の管理**」をクリックして、保存された資格情報を追加できます。

     注：ローカル認証を使用するように選択する場合、デバイスの管理に保存された資格情報を選択する必要があります。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

   通常および保存された資格情報について詳しくは、ユーザー・アカウントの管理および保存された資格情報の管理を参照してください。
8. 管理対象認証が選択されている場合、リカバリー・パスワードを指定します。

   リカバリー・アカウント (`RECOVERY_ID`) が CMM で作成され、すべてのローカル・ユーザー・アカウントは無効になります。XClarity Administrator に問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用しても CMM にログイン *できません*。ただし、`RECOVERY_ID` アカウントを使用してログインできます。

   注:
   - 管理対象認証を使用するように選択した場合は、リカバリー・パスワードは必須です。ローカル認証を使用するように選択した場合は利用できません。
   - ローカル・リカバリー・アカウントまたは保存されているリカバリー資格情報を使用するように選択できます。いずれの場合も、ユーザー名は常に `RECOVERY_ID` です。
   - パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。
   - リカバリー・パスワードは後で使用できるように記録しておいてください。

   リカバリー ID について詳しくは、認証サーバーの管理を参照してください。
9. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：
   - 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   - 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。
10. 「**管理**」をクリックします。

ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、この進行状況を監視します。

プロセスが完了すると、ダイアログにシャーシ内のデバイスの数とシャーシのステータスが表示されます。

注：管理プロセスが完了した後、インベントリー・データが一部収集されます。すべてのインベントリー・データが収集されるまで、シャーシの状態は「保留中」になります。管理対象デバイスでは、そのデバイスのすべてのインベントリー・データが収集されてシャーシの状態が「保留中」でなくなるまで、サーバー・パターンのデプロイなどの特定のタスクを実行できません。

11. プロセスが完了したら、「**OK**」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    - 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

      注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
    - デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
    - デバイスが正しく管理対象から除外されなかった場合。

    注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

12. 新しいシャーシの場合は、「**シャーシの構成に進む**」をクリックして、シャーシ全体 (計算ノードと Flex スイッチを含む) の管理ネットワーク設定を検証して変更します。また、サーバー・パターンを作成してデプロイすることで、計算ノードの情報、ローカル・ストレージ、I/O アダプター、ブート・ターゲット、ファームウェア設定を構成します。詳しくは、シャーシの管理 IP 設定の変更と構成パターンを使用したサーバーの構成を参照してください。

- IP アドレスを手動で指定して、XClarity Administrator と同じ IP サブネットにないシャーシを検出して管理する。

  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。
  2. 管理プロセス中にすべてのデバイスのファイアウォール規則を変更して XClarity Administrator からの受信要求のみを受け入れるようにするには、「**今後すべての管理対象デバイスで Encapsulation を有効にする**」チェックボックスをクリックします。

     Encapsulation は、特定のデバイスが管理対象になった後で有効または無効にできます。

     注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。
  3. 「**手動で入力**」を選択します。
  4. 管理するシャーシのネットワーク・アドレスを指定します。

     - 「**単一システム**」をクリックし、単一の IP アドレス、ドメイン名、または完全修飾ドメイン名 (FQDN) を入力します。

注：FQDN を指定するには、「ネットワーク・アクセス」ページで有効なドメイン名が指定されていることを確認します (ネットワーク・アクセスの構成を参照)。

- 「**複数システム**」をクリックし、IP アドレスの範囲を入力します。別の範囲を追加するには、「**追加**」アイコン () をクリックします。範囲を削除するには、「**削除**」アイコン () をクリックします。

5. 「**OK**」をクリックします。
6. このデバイスで XClarity Administrator 管理対象認証またはローカル認証を使用するように選択します。管理対象認証はデフォルトで選択されています。ローカル認証を使用するには、「**管理対象認証**」をオフにします。

   注：管理対象認証およびローカル認証は、ThinkServer および System x M4 サーバーではサポートされていません。
7. デバイスで使用する資格情報を選択して適切な資格情報を指定します。
   - **手動で入力した資格情報を使用**
     - CMM への認証に使用される、**lxc-supervisor** 権限を持つローカル・ユーザー ID とパスワードを指定します。
     - (オプション) パスワードが現在、デバイスで有効期限が切れている場合は、指定された CMM ユーザー・アカウントの新しいパスワードを指定します。
   - **保存された資格情報を使用**

     この管理対象デバイスで使用する **lxc-supervisor** 権限を持つ、保存された資格情報を選択します。「**保存された資格情報の管理**」をクリックして、保存された資格情報を追加できます。

     注：ローカル認証を使用するように選択する場合、デバイスの管理に保存された資格情報を選択する必要があります。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

   通常および保存された資格情報について詳しくは、ユーザー・アカウントの管理および保存された資格情報の管理を参照してください。
8. 管理対象認証が選択されている場合、リカバリー・パスワードを指定します。

   リカバリー・アカウント (`RECOVERY_ID`) が CMM で作成され、すべてのローカル・ユーザー・アカウントは無効になります。XClarity Administrator に問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用しても CMM にログイン *できません*。ただし、`RECOVERY_ID` アカウントを使用してログインできます。

   注:

   - 管理対象認証を使用するように選択した場合は、リカバリー・パスワードは必須です。ローカル認証を使用するように選択した場合は利用できません。
   - ローカル・リカバリー・アカウントまたは保存されているリカバリー資格情報を使用するように選択できます。いずれの場合も、ユーザー名は常に `RECOVERY_ID` です。
   - パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。
   - リカバリー・パスワードは後で使用できるように記録しておいてください。

   リカバリー ID について詳しくは、認証サーバーの管理を参照してください。
9. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

- 現在のユーザーに割り当てられている役割グループのリストから選択できます。
- 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

10. 「**管理**」をクリックします。

    ダイアログが開き、この管理プロセスの進行状況が表示されます。進行状況を監視して、プロセスが正常に完了することを確認します。

    プロセスが完了すると、ダイアログにシャーシ内のデバイスの数とシャーシのステータスが表示されます。

    注：管理プロセスが完了した後、インベントリー・データが一部収集されます。すべてのインベントリー・データが収集されるまで、シャーシの状態は「保留中」になります。管理対象デバイスでは、そのデバイスのすべてのインベントリー・データが収集されてシャーシの状態が「保留中」でなくなるまで、サーバー・パターンのデプロイなどの特定のタスクを実行できません。

11. プロセスが完了したら、「**OK**」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    - 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

      注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
    - デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
    - デバイスが正しく管理対象から除外されなかった場合。

    注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

12. 新しいシャーシの場合は、「**シャーシの構成に進む**」をクリックして、シャーシ全体 (計算ノードと Flex スイッチを含む) の管理ネットワーク設定を検証して変更します。また、サーバー・パターンを作成してデプロイすることで、計算ノードの情報、ローカル・ストレージ、I/O アダプター、ブート・ターゲット、ファームウェア設定を構成します。詳しくは、シャーシの管理 IP 設定の変更と構成パターンを使用したサーバーの構成を参照してください。

終了後

- 追加のデバイスを検出して管理します。
- オペレーティング・システムがまだインストールされていないサーバーにオペレーティング・システム・イメージをデプロイします。詳しくは、ベア・メタル・サーバーへのオペレーティング・システムのインストールを参照してください。
- 現行ポリシーに従っていないデバイスのファームウェアを更新します (管理対象デバイスでのファームウェアの更新を参照)。
- 新たに管理するデバイスを適切なラックに追加して物理的環境を反映します (ラックの管理を参照)。
- ハードウェアのステータスと詳細を監視します (管理対象サーバーのステータスの表示を参照)。
- イベントとアラートを監視します (イベントの使用とアラートの使用を参照)。

管理対象シャーシのステータスの表示

Lenovo XClarity Administrator から、管理対象シャーシおよびこれらに取り付けられたコンポーネントの概要と詳細なステータスを表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

以下のステータス・アイコンは、デバイスの全体的な正常性を示します。証明書が一致しない場合、該当する各デバイスのステータスに「(非トラステッド)」と付加されます。たとえば、「警告 (非トラステッド)」となります。接続に問題がある場合やデバイスへの接続が信頼されない場合、該当する各デバイスのステータスに「(接続)」と付加されます。たとえば、「警告 (接続)」となります。

- () クリティカル
- () 警告
- () 保留中
- () 通知
- () 正常
- () オフライン
- () 不明

手順

管理対象シャーシのステータスを表示するには、以下の手順を実行します。

- シャーシに関する詳細情報を表示するには、「**詳細**」リンクをクリックするか、「**操作**」 → 「**ビュー**」 → 「**詳細**」をクリックします。
- シャーシの CMM Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (シャーシの CMM Web インターフェースの起動を参照)。
- サポートの連絡先、シャーシの場所、説明などの情報を変更するには、「**操作**」 → 「**インベントリー**」 → 「**プロパティの編集**」をクリックします。
- 計算ノード、Flex スイッチなど、シャーシ全体の管理 IP 設定を変更するには、「**操作**」 → 「**インベントリー**」 → 「**管理 IP アドレスを編集**」をクリックします。
- 1 つ以上のシャーシに関する詳細情報を単一 CSV ファイルにエクスポートするには、シャーシを選択し、「**操作**」 → 「**インベントリー**」 → 「**インベントリーのエクスポート**」をクリックします。

  注：最大 60 個のデバイスのインベントリー・データを一度にエクスポートできます。

  ヒント: CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- Lenovo XClarity Administrator のセキュリティー証明書とシャーシ内の CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、シャーシを選択し、「**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。

管理対象シャーシの詳細の表示

Lenovo XClarity Administrator から管理対象シャーシに関する詳細情報 (ファームウェア・レベル、IP アドレス、世界固有識別子 (UUID) など) を表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

システム・レベルの室温は、サーバーの前面にある物理センサーによって測定されます。この温度は、サーバーの吸気口の温度を表します。温度が異なる時点で取得された場合、XClarity Administrator および CMM によって報告される温度が異なる可能性があることに注意してください。

手順

管理対象シャーシの詳細を表示するには、以下の手順を実行します。

ステップ 1. XClarity 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。「シャーシ」ページが開いて、すべての管理対象シャーシがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するシャーシを見つけやすくなります。「**フィルター**」フィールドにテキスト (シャーシ名や IP アドレスなど) を入力して、表示されるシャーシを絞り込むこともできます。

ステップ 2. 「**シャーシ**」列のシャーシ名をクリックします。そのシャーシのステータス要約ページが開いて、シャーシのプロパティと、シャーシに取り付けられたコンポーネントが表示されます。

ステップ 3. 必要に応じて、以下の操作を実行します。

- システム情報や取り付けられたコンポーネントなどシャーシの要約を表示するには、「**要約**」をクリックします (管理対象シャーシのステータスの表示を参照)。
- 以下のようなシャーシ・コンポーネントの詳細を表示するには、「**インベントリー詳細**」をクリックします。
  - シャーシ内のすべてのコンポーネントのファームウェア・レベル
  - CMM の詳細 (ホスト名、IPv4 アドレス、IPv6 アドレス、MAC アドレスなど)
  - シャーシとそのシャーシに取り付けられた CMM のアセットの詳細 (名前、世界固有識別子 (UUID)、場所など)
- このシャーシの現在のアラートのリストを表示するには、「**アラート**」をクリックします (アラートの使用を参照)。

- このシャーシのイベントのリストを表示するには、「**イベント・ログ**」をクリックします (イベント・ログでのイベントの監視を参照)。
- シャーシに関連付けられているジョブのリストを表示するには、「**ジョブ**」をクリックします (ジョブの監視を参照)。
- ロケーション、障害、情報など、シャーシの LED の現在のステータスを表示するには、「**Light Path**」をクリックします。これは、シャーシの前面パネルを確認することに相当します。
- 電源とエア・フローの詳細を表示するには、「**電源および熱**」をクリックします。

  ヒント: 電源および熱の最新データを収集するには、Web ブラウザーの最新表示ボタンを使用します。データの収集には数分かかる場合があります。
- Feature on Demand キーの注文に必要な情報およびその他のエージェントレス情報にアクセスするには「**Feature on Demand キー**」をクリックします (Features on Demand キーの表示を参照)。

終了後

シャーシに対しては、要約と詳細情報の表示に加えて、以下の操作を実行できます。

- グラフィカルなラック・ビューまたはシャーシ・ビューでシャーシを表示するには、「**操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューで表示**」 または「**操作**」 ➡ 「**ビュー**」 ➡ 「**シャーシ・ビューで表示**」をクリックします。
- CMM Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (シャーシの CMM Web インターフェースの起動を参照)。
- サポートの連絡先、シャーシの場所、説明などの情報を変更するには、「**プロパティの編集**」をクリックします (シャーシのシステム・プロパティの変更を参照)。
- 計算ノード、Flex スイッチなど、シャーシ全体の管理 IP 設定を変更するには、「**すべての操作**」 ➡ 「**イベントリー**」 ➡ 「**管理 IP アドレスを編集**」をクリックします (シャーシの管理 IP 設定の変更を参照)。
- シャーシに関する詳細情報を CSV ファイルにエクスポートするには、「**操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーのエクスポート**」をクリックします。

  注：

  – CSV ファイルのインベントリー・データについて詳しくは、GET /chassis/*<UUID_list>* について XClarity Administrator オンライン・ドキュメントを参照してください。

  – CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- シャーシを管理解除します (シャーシの管理解除を参照)。
- シャーシでファイアウォール規則の変更を有効または無効にして受信要求を XClarity Administrator からのみに制限するには、シャーシを選択して「**操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を有効にする**」 または「**操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を無効にする**」をクリックします。

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

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

  共通 encapsulation の設定が有効にされ、デバイスが encapsulation をサポートする場合、XClarity Administrator は管理プロセス中にデバイスと通信し、デバイスの encapsulation モードを「encapsulationLite」に変更し、受信要求を XClarity Administratorからのみに制限するためデバイスのファイアウォール規則を変更します。

注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。

- XClarity Administrator のセキュリティー証明書とシャーシ内の CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、シャーシを選択し、「**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 (非トラステッド・サーバー証明書の解決を参照)。

CMM 構成データのバックアップと復元

Lenovo XClarity Administrator には、CMM 構成データの組み込みバックアップ機能はありません。代わりに、ご使用の管理対象 CMM で使用可能なバックアップ機能を使用します。

管理 Web インターフェースまたはコマンド・ライン・インターフェース (CLI) を使用して CMM をバックアップおよび復元します。

- CMM 構成データのバックアップ
  - 管理 Web インターフェースから、「**管理モジュールの管理**」 ➡ 「**構成**」 ➡ 「**バックアップ構成**」をクリックします。詳しくは、Flex Systems オンライン・ドキュメントの Web インターフェース を使用した CMM 構成の保存を参照してください。
  - CLI から、`write` コマンドを使用します。詳しくは、Flex Systems オンライン・ドキュメントの CMM write コマンド を参照してください。
- CMM 構成データの復元
  - 管理 Web インターフェースから、「**管理モジュールの管理**」 ➡ 「**構成**」 ➡ 「**ファイルから構成を復元する**」をクリックします。詳しくは、Flex Systems オンライン・ドキュメントの Web インターフェースを使用した CMM 構成の復元を参照してください。
  - CLI から、`read` コマンドを使用します。詳しくは、Flex Systems オンライン・ドキュメントの CMM read コマンドを参照してください。

注：ヒント: シャーシ・コンポーネントのバックアップおよび復元について詳しくは、PureFlex および Flex System のバックアップと復元に関する ベスト・プラクティス・ガイドを参照してください。

シャーシの CMM Web インターフェースの起動

Lenovo XClarity Administrator から特定のシャーシの CMM Web インターフェースを起動できます。

手順

CMM Web インターフェースを起動するには、以下の手順を実行します。

注：Safari Web ブラウザーでは、XClarity Administrator からこの CMM Web インターフェースを起動することはできません。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**シャーシ**」をクリックして、「シャーシ」ページを表示します。

テーブルの列をソートすると、管理するシャーシを見つけやすくなります。「**フィルター**」フィールドにテキスト (シャーシ名や IP アドレスなど) を入力して、表示されるシャーシを絞り込むこともできます。

ステップ 2. 「**シャーシ**」列のシャーシのリンクをクリックします。そのシャーシのステータスの要約ページが表示されます。

ステップ 3. 「**すべての操作**」 ➡ 「**起動**」 ➡ 「**管理 Web インターフェース**」をクリックします。CMM Web インターフェースが起動されます。

ヒント: IP アドレスをクリックして、CMM を起動することもできます。

ステップ 4. XClarity Administrator ユーザー資格情報を使用して CMM Web インターフェースにログオンします。

シャーシのシステム・プロパティの変更

特定のシャーシのシステム・プロパティを変更できます。

手順

以下の手順を実行して、システム・プロパティを変更します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**シャーシ**」をクリックして、「シャーシ」ページを表示します。

ステップ 2. 更新するシャーシを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックし、「編集」ダイアログを表示します。

ステップ 4. 以下の情報を必要に応じて変更します。

- サーバー名
- サポート連絡先
- 説明

注：Web インターフェースのラックからデバイスを追加または削除する場合は、ロケーション、設置部屋、ラック、最下段ラック・ユニットのプロパティが XClarity Administrator によって更新されます (ラックの管理を参照)。

ステップ 5. 「**保存**」をクリックします。

注：変更されたプロパティが XClarity Administrator Web インターフェースに表示されるまで少し時間がかかる場合があります。

シャーシの管理 IP 設定の変更

計算ノード、ストレージ・デバイス、Flex スイッチなど、シャーシ全体の管理 IP 設定を変更できます。

手順

以下の手順を実行して、管理 IP 設定を変更します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**シャーシ**」をクリックして、「シャーシ」ページを表示します。

ステップ 2. シャーシを選択します。

ステップ 3. 「**すべての操作**」 → 「**インベントリー**」 → 「**管理 IP アドレスを編集**」をクリックし、「シャーシとコンポーネントの IP 設定」ページを表示します。

ステップ 4. 以下の共通設定を必要に応じて変更します。

- IPv4 アドレスを有効にするか無効にするかを選択します。

  IPv4 アドレスを有効にする場合、以下の設定を指定します。IPv4 グローバル設定は、IPv4 アドレスが更新されたときにコンポーネントに適用されます。
  - (オプション) 静的に割り当てられた IP アドレスを使用して IP アドレスを取得することを選択します。
  - サブネット・マスクおよびゲートウェイ・アドレスを指定します。
- IPv6 アドレスに以下の設定を指定します。IPv6 グローバル設定は、IPv6 アドレスが更新されたときにコンポーネントに適用されます。
  - (オプション) 静的に割り当てられた IP アドレスを使用して IP アドレスを取得することを選択します。

    静的 IP アドレスが使用されている場合は、ステートレス IP アドレス自動構成およびステートフル IP アドレス構成の使用を選択できます。
  - プレフィックスの長さおよびゲートウェイ・アドレスを指定します。
- DNS サーバーを有効にするか無効にするかを選択します。

  DNS サーバーを有効にする場合:
  - DNS サーバーの検索設定を選択します。
  - DNS 検索順序に使用する IP アドレスを入力します。
  - ドメイン名を入力します。

ステップ 5. CMM の以下の IP 設定を変更します。

- CMM のホスト名と IP アドレスを入力します。
- 「**IP アドレスの自動生成**」をクリックして、CMM の IP アドレスから計算ノード、ストレージ・デバイス、Flex スイッチの IP アドレスが生成されるようにします。

ステップ 6. シャーシ内の各計算ノードのホスト名と IP アドレスを入力します。

ステップ 7. シャーシ内の各ストレージ・デバイスのホスト名と IP アドレスを入力します。

ステップ 8. シャーシ内の各 Flex スイッチの IP アドレスを入力します。

ステップ 9. 「**保存**」をクリックします。ダイアログ・ボックスが開き、ネットワーク設定の要約が表示されます。

ステップ 10. 「**適用**」をクリックします。

シャーシ内のすべての既存のコンポーネントが、指定した共通設定に更新されます。更新が完了すると、変更された設定がダイアログに表示されます。

注：変更された情報が Lenovo XClarity Administrator インターフェースに表示されるまで少し時間がかかる場合があります。

ステップ 11. 「**閉じる**」をクリックします。

CMM フェイルオーバーの構成

シャーシに 2 台目の CMM を取り付けると、デフォルトで 2 台目の CMM がスタンバイ CMM として自動的に設定されます。プライマリー CMM で障害が発生すると、スタンバイ CMM の IP アドレスがプライマリー CMM で使用されていた IP アドレスに代わり、スタンバイ CMM がシャーシの管理を引き

継ぎます。ただし、シャーシの管理コントローラー Web インターフェースからより詳細なフェイルオーバーの構成を実行できます。

このタスクについて

たとえば、以下のオプションがあります。

- スタンバイ CMM のネットワーク・インターフェースを無効にします。フェイルオーバーされません。
- スタンバイ CMM のネットワーク・インターフェースを使用可能にし、フェイルオーバー中に 2 つの CMM 間での IP アドレスのスワップを許可します。
- スタンバイ CMM のネットワーク・インターフェースを使用可能にし、フェイルオーバー中に 2 つの CMM 間での IP アドレスのスワップを行いません。

CMM の拡張フェイルオーバー機能について詳しくは、CMM オンライン・ドキュメントの advfailover コマンドを参照してください。

手順

プライマリー CMM とスタンバイ CMM のスワップ可能な IP アドレスを有効にするには、以下の手順を実行します。

ステップ 1. シャーシの管理コントローラー Web インターフェースで、「**管理モジュールの管理**」 ➡ 「**ネットワーク**」 ➡ 「**イーサネット**」をクリックして、「イーサネット構成」ページを表示します。

ステップ 2. システムに応じて「**IPv4**」と「**IPv6**」のいずれかを選択します。

ステップ 3. 「**IP アドレスの構成**」で、静的 IP アドレスを使用するオプションを選択します。他のプロトコルについてもこの手順を繰り返します。

ステップ 4. 「**管理モジュールの管理**」 ➡ 「**プロパティ**」 ➡ 「**拡張フェイルオーバー**」をクリックし、拡張フェイルオーバー・オプションを有効にします。

ステップ 5. 「**管理モジュール IP アドレスのスワップ**」を選択します。

ステップ 6. テスト・シナリオを実行して、フェイルオーバーが正しく動作し、Lenovo XClarity Administrator がプライマリーおよびバックアップ CMM に接続できることを確認します。

CMM の再始動

Lenovo XClarity Administrator から Chassis Management Module (CMM) を再起動できます。

手順

シャーシを再起動するには、次の手順で行います。

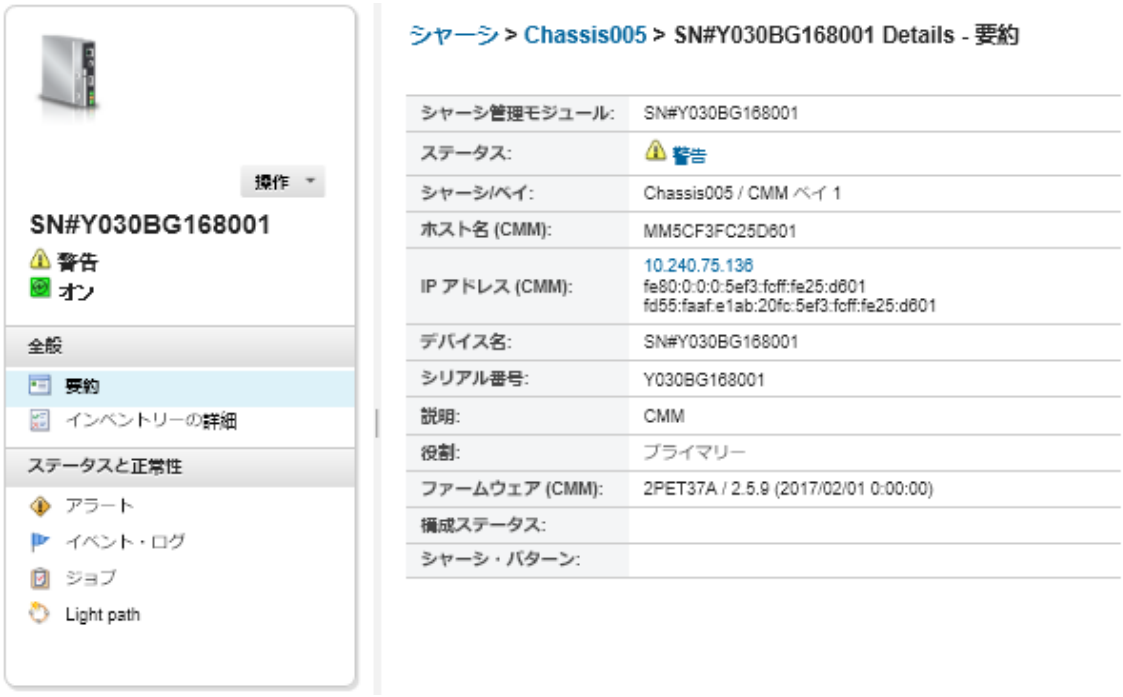
注：CMM の再起動時に、CMM に対する既存のすべてのネットワーク接続が一時的に失われます。

ステップ 1. XClarity Administrator メニューで、「**ハードウェア**」 ➡ 「**シャーシ**」をクリックします。「シャーシ」ページが開いて、すべての管理対象シャーシがテーブル・ビューで表示されます。

ステップ 2. 「**シャーシ**」列のシャーシ名をクリックして、シャーシをグラフィカル・ビューで表示します。

ステップ 3. CMM のグラフィックをクリックすると、CMM の要約ページが表示されます。

ヒント: または、「**テーブル・ビュー**」をクリックし、次に「**名前**」列で CMM 名をクリックしても、「CMM の要約」ページを表示できます。



ステップ 4. 「**アクション**」 ➔ 「**電源操作**」 ➔ 「**再起動**」をクリックします。

ステップ 5. 「**今すぐ再起動**」をクリックします。

この操作には数分かかる場合があります。ページを最新の情報に更新するまで、結果が表示されないこともあります。

CMM の仮想再取り付け

シャーシでの Chassis Management Module (CMM) の取り外しと再挿入をシミュレートできます。

このタスクについて

仮想再取り付けの間に、CMM に対する既存のネットワーク接続がすべて失われ、CMM の電源状態が変更されます。

注意：仮想再取り付けを実行する前に、CMM 上のすべてのユーザー・データが保存されていることを確認してください。

手順

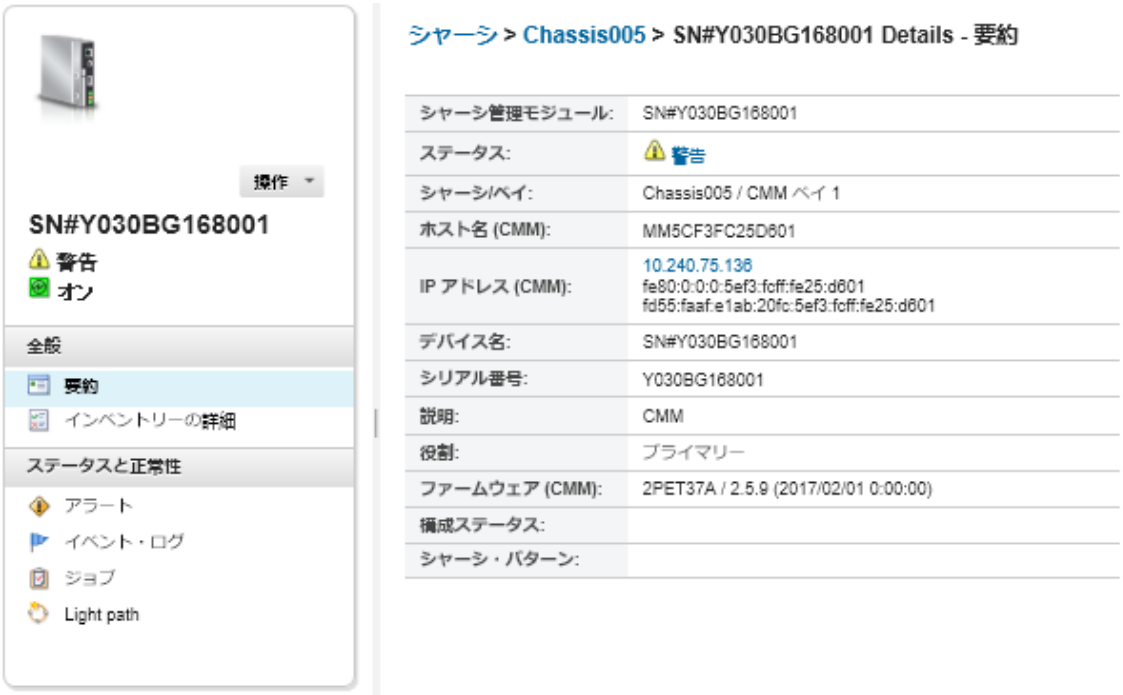
CMM の仮想再取り付けを行うには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator メニューで、「**ハードウェア**」 ➔ 「**シャーシ**」をクリックします。「シャーシ」ページが開いて、すべての管理対象シャーシがテーブル・ビューで表示されます。

ステップ 2. 「**シャーシ**」列のシャーシ名をクリックして、シャーシをグラフィカル・ビューで表示します。

ステップ 3. CMM のグラフィックをクリックすると、CMM の要約ページが表示されます。

ヒント: または、「**テーブル・ビュー**」をクリックし、次に「**名前**」列で CMM 名をクリックしても、「CMM の要約」ページを表示できます。



ステップ 4. 「**操作**」 → 「**サービス**」 → 「**仮想再取り付け**」をクリックします。

ステップ 5. 「**仮想再取り付け**」をクリックします。

シャーシの有効期限切れまたは無効の保存された資格情報の解決

保存された資格情報が期限切れまたはデバイスで動作しない場合、そのデバイスのステータスは「オフライン」と表示されます。

手順

シャーシの有効期限切れまたは無効の保存された資格情報を解決するには

ステップ 1. Lenovo 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。「シャーシ」ページが開いて、すべての管理対象シャーシがテーブル・ビューで表示されます。

ステップ 2. テーブル上部で「**電源**」列の見出しをクリックして、すべてのオフライン・シャーシをグループにします。

テーブルの列をソートすると、管理するシャーシを見つけやすくなります。「**フィルター**」フィールドにテキスト (シャーシ名や IP アドレスなど) を入力して、表示されるシャーシを絞り込むこともできます。

ステップ 3. 解決するシャーシを選択します。

ステップ 4. 「**すべての操作**」 ➔ 「**セキュリティー**」 ➔ 「**保存された資格情報を編集**」をクリックします。

ステップ 5. 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。

注：同じ保存された資格情報を使用して複数のデバイスを管理しており、その保存された資格情報のパスワードを変更する場合、パスワードの変更は現在その保存された資格情報を使用しているすべてのデバイスに影響します。

管理サーバーの障害発生後の CMM による管理のリカバリー

シャーシが Lenovo XClarity Administrator の管理対象になっているときに、XClarity Administrator に障害が発生した場合は、管理ノードの復元または交換を待たずに、CMM の管理機能とローカル・ユーザー・アカウントを復元できます。

手順

CMM で管理を復元するには、以下のいずれかの手順を実行します。

- 交換 XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード、および「**管理の強制**」オプションを使用してデバイスを再度管理します (シャーシの管理参照)。
- ペーパー・クリップを使用して CMM のピンホール・ボタンを少なくとも 10 秒間押し、CMM を出荷時のデフォルト値にリセットします。CMM のリセットについての重要事項を含む詳細については、Flex Systems オンライン・ドキュメントの CMM のリセットを参照してください。
- 以下の手順を使用して CMM 構成をリセットします。
  1. SSH セッションから、シャーシの管理コマンド・ライン・インターフェースを開き、RECOVERY_ID アカウントでログインします。

     注：RECOVERY_ID アカウントのパスワードは、「管理ドメイン」ページで管理対象シャーシを選択したときに設定されています。アカウントの集中管理について詳しくは、シャーシの管理を参照してください。

     CMM に RECOVERY_ID アカウントでログインするのが初めてであれば、パスワードの変更を求められます。
  2. プロンプトが表示されたら、RECOVERY_ID アカウントの新しいパスワードを入力します。
  3. CMM 構成を復元するには、以下のいずれかの手順を実行します。
     - 2015 年 6 月リリース以降の CMM ファームウェアを実行している場合は、次のコマンドを実行します:
       `read -f unmanage -T mm[p]`
       詳しくは、CMM オンライン・ドキュメントの read コマンド を参照してください。
     - 2015 年 6 月リリースより前の CMM ファームウェアを実行している場合は、次のコマンドを順番に実行します。
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

`fsmcm` コマンドにより XClarity Administrator ユーザー・アカウント管理が無効になり、ローカルの CMM ユーザー・アカウントを使用して、シャーシに取り付けられた CMM と管理プロセッサーすべてに対して認証できるようになります。

`fsmcm -off` コマンドを実行した後、`RECOVERY_ID` アカウントが CMM ユーザー・レジストリーから削除されます。`fsmcm -off` コマンドを実行すると、CMM CLI セッションが終了します。これで、XClarity Administrator によるユーザー管理の復元を待たずに、ローカルの CMM 資格情報で CMM と他のシャーシ・コンポーネントに対して認証し、ローカルの CMM 資格情報を使用してシャーシの CMM Web インターフェースまたは CLI にアクセスすることができます。

詳しくは、CMM オンライン・ドキュメントの fsmcm コマンド を参照してください。

XClarity Administrator が復元または交換されると、シャーシをもう一度管理できるようになります (シャーシの管理を参照)。シャーシに関するすべての情報 (ネットワーク設定など) は保持されます。

シャーシの管理解除

シャーシを Lenovo XClarity Administrator の管理対象から除外できます。このプロセスは*管理解除*と呼ばれます。シャーシの管理解除後は、ローカル CMM ユーザー・アカウントを使用してシャーシの CMM にログインできます。

始める前に

XClarity Administrator を有効にすると、一定期間オフラインになっているデバイスを管理対象から自動的に解除できます。これはデフォルトで無効になっています。オフライン・デバイスの自動管理解除を有効にするには、XClarity Administrator メニューから「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックし、「**管理除外オフライン・デバイスが無効**」の横の「**編集**」をクリックします。次に、「**管理除外オフライン・デバイスの有効化**」を選択し、時間間隔を設定します。デフォルトでは、デバイスは 24 時間オフラインになった後、管理解除されます。

シャーシを管理解除する前に、シャーシに取り付けられたいずれのデバイスに対しても実行中のアクティブ・ジョブがないことを確認します。

XClarity Administratorでコール・ホームが有効になっている場合、重複する問題レコードが作成されないようにするため、すべての管理対象シャーシとサーバーでコール・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、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 (XClarity Administrator オンライン・ドキュメントの 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)。

このタスクについて

シャーシを管理解除すると、XClarity Administrator では以下の処理が実行されます。

- 集中型ユーザー管理に使用されている構成をクリアする。
- XClarity Administrator 信頼ストアから CMM セキュリティー証明書を削除する。
- デバイスで Encapsulation が有効である場合は、デバイスが管理される前に、設定にデバイスのファイアウォール規則を構成する。
- CMM から NTP サーバーへのアクセス権限を削除する。
- XClarity Administrator 構成から CMM への CIM サブスクリプションを削除する。これにより、XClarity Administrator はそのシャーシからイベントを受信しなくなります。

シャーシを管理解除しても、XClarity Administrator にはシャーシに関する特定の情報が保持されます。この情報は、そのシャーシの管理を再開したときに再適用されます。

シャーシを管理解除すると、シャーシ・コンポーネントから送信されたイベントは破棄されます。イベントを保持するには、syslog などの外部リポジトリーにイベントを転送します (イベントの転送を参照)。

ヒント: 初期セットアップ中にオプションで追加されたすべてのデモ・デバイスは、シャーシ内のノードです。デモ・デバイスを管理対象から除外するには、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」オプションを使用してシャーシを管理対象から除外します。

手順

シャーシを管理解除するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**シャーシ**」をクリックして、「シャーシ」ページを表示します。

ステップ 2. 管理対象シャーシのリストから 1 つ以上のシャーシを選択します。

ステップ 3. 「**シャーシを管理対象から除外**」をクリックします。「管理対象から除外」ダイアログが表示されます。

ステップ 4. **オプション**: 「**デバイスに到達できない場合であっても、管理対象からの除外を強制します**」を選択します。

重要：デモ・ハードウェアを管理解除する場合は、このオプションを選択してください。

ステップ 5. 「**非管理**」をクリックします。
「管理対象から除外」ダイアログには、管理解除プロセスの各ステップの進行状況が表示されます。

ステップ 6. 管理解除プロセスが完了したら、「OK」をクリックします。

終了後

管理解除プロセスの完了後、ローカル CMM ユーザー・アカウントを使用して CMM にログインできます。いずれのローカル CMM ユーザー・アカウントのユーザー名またはパスワードも覚えていない場合は、CMM を出荷時の状態にリセットして、CMM にログインします。出荷時の状態への CMM のリセットについては、CMM の製品ドキュメントのFlex Systems オンライン・ドキュメントの CMM のリセットを参照してください。

正しく管理解除されなかったシャーシのリカバリー

シャーシが正しく管理解除されなかった場合、管理するには前にシャーシをリカバリーする必要があります。

手順

CMM で管理を復元するには、以下のいずれかの手順を実行します。

- 交換 XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード、および「**管理の強制**」オプションを使用してデバイスを再度管理します (シャーシの管理参照)。
- ペーパー・クリップを使用して CMM のピンホール・ボタンを少なくとも 10 秒間押し、CMM を出荷時のデフォルト値にリセットします。CMM のリセットについての重要事項を含む詳細については、Flex Systems オンライン・ドキュメントの CMM のリセットを参照してください。
- 以下の手順を使用して CMM 構成をリセットします。
  1. SSH セッションから、シャーシの管理コマンド・ライン・インターフェースを開き、`RECOVERY_ID` アカウントでログインします。

     注：`RECOVERY_ID` アカウントのパスワードは、「管理ドメイン」ページで管理対象シャーシを選択したときに設定されています。アカウントの集中管理について詳しくは、シャーシの管理を参照してください。

CMM に RECOVERY_ID アカウントでログインするのが初めてであれば、パスワードの変更を求められます。

2. プロンプトが表示されたら、RECOVERY_ID アカウントの新しいパスワードを入力します。
3. CMM 構成を復元するには、以下のいずれかの手順を実行します。
   - 2015 年 6 月リリース以降の CMM ファームウェアを実行している場合は、次のコマンドを実行します:
     `read -f unmanage -T mm[p]`
     詳しくは、CMM オンライン・ドキュメントの read コマンド を参照してください。
   - 2015 年 6 月リリースより前の CMM ファームウェアを実行している場合は、次のコマンドを順番に実行します。
     a. `env -T mm[p]`
     b. `sslcfg -client disabled -tc1 remove`
     c. `accseccfg -am local`
     d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
     e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
     f. `cimsub -clear all`
     g. `fsmcm -off`

        `fsmcm` コマンドにより XClarity Administrator ユーザー・アカウント管理が無効になり、ローカルの CMM ユーザー・アカウントを使用して、シャーシに取り付けられた CMM と管理プロセッサーすべてに対して認証できるようになります。

        `fsmcm -off` コマンドを実行した後、RECOVERY_ID アカウントが CMM ユーザー・レジストリーから削除されます。`fsmcm -off` コマンドを実行すると、CMM CLI セッションが終了します。これで、XClarity Administrator によるユーザー管理の復元を待たずに、ローカルの CMM 資格情報で CMM と他のシャーシ・コンポーネントに対して認証し、ローカルの CMM 資格情報を使用してシャーシの CMM Web インターフェースまたは CLI にアクセスすることができます。

        詳しくは、CMM オンライン・ドキュメントの fsmcm コマンド を参照してください。

XClarity Administrator が復元または交換されると、シャーシをもう一度管理できるようになります (シャーシの管理を参照)。シャーシに関するすべての情報 (ネットワーク設定など) は保持されます。

第 8 章　サーバーの管理

Lenovo XClarity Administrator では、ThinkAgile、ThinkSystem、コンバージド、Flex System、NeXtScale、System x®、および ThinkServer® サーバーなど、複数のタイプのシステムを管理できます。

詳細:  XClarity Administrator: 検出

始める前に

注：Flex 計算ノードは、それらを含むシャーシを管理する際に自動的に検出され管理されます。シャーシとは別に Flex 計算ノードを検出、管理することはできません。

サーバーを管理する前に、以下の条件が満たされていることを確認してください。

- デバイスを管理する前に、管理に関する考慮事項を検討してください。詳しくは、XClarity Administrator オンライン・ドキュメントの 管理に関する考慮事項 を参照してください。
- 特定のポートがデバイスとの通信に使用できる必要があります。サーバーを管理する前に、必要なポートがすべて使用可能になっていることを確認します。ポートについては、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。
- 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。
- 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。
  1. `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。
  2. 「**IMM 管理**」 ➡ 「**セキュリティー**」をクリックします。
  3. 「**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。
- 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。
- 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 (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)。
- XClarity Administrator から*別の*サブネットにあるサーバーを検出するには、以下のいずれかの条件を満たしていることを確認してください。
  - マルチキャスト SLP 転送が環境内のルーターと同様にラック装着スイッチで有効になっていることを確認します。マルチキャスト SLP 転送が有効になっているかどうかを調べる方法や、無効になっている場合に有効にする方法については、そのスイッチやルーターに付属のドキュメントを参照してください。

– SLP がエンドポイントまたはネットワークで無効の場合、DNS 検出メソッドを代わりに使用できます。これを行うには、手動でサービス・レコード (SRV レコード) をドメイン・ネーム・サーバー (DNS) に追加します。たとえば XClarity Administrator の場合は次のようになります。
`_lxca._tcp.labs.lenovo.com service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

次に、管理 Web インターフェースからベースボード管理コンソールの DNS 検出を有効にします。これを行うには、「**IMM 管理**」 ➡ 「**ネットワーク・プロトコル**」の順にクリックし、「DNS」タブをクリックして「**Lenovo XClarity Administrator の検出に DNS を使用する**」を選択します。

注：

– DNS を使用した自動検出をサポートするには、管理コントローラーが 2017 年 5 月以降のファームウェア・レベルを実行している必要があります。

– ご使用の環境に複数の XClarity Administrator インスタンスがある場合、検索要求に最初に応答したインスタンスによってのみ、サーバーが検出されます。サーバーはすべてのインスタンスによっては検出されません。

- ThinkServer サーバーを検出および管理するには、以下の要件を満たしていることを確認してください。詳しくは、XClarity Administrator オンライン・ドキュメントの デバイスを検出できない、デバイスを管理できない を参照してください。

  – XClarity Administrator が自動的にサーバーを検出するようにするには、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必要があります。

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

  – ユニキャスト SLP が必要です。

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

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

- ThinkAgile、ThinkSystem、コンバージド、Flex System の場合。サーバー内のアダプターの取り外し、交換、または構成を行った場合、NeXtScale と System x サーバーはサーバーを少なくとも 1 回再起動して、ベースボード管理コントローラーおよび XClarity Administrator レポート (サーバーの電源のオン/オフ) の新しいアダプター情報を更新します。

- サーバーの管理操作を実行する際は、サーバーの電源がオフになっているのか、BIOS/UEFI セットアップを起動しているのか、またはオペレーティング・システムを実行しているのかを確認します。(XClarity Administrator の「サーバー」ページで 「**すべての操作**」 ➡ 「**電源操作**」 ➡ 「**再起動して UEFI/BIOS セットアップ**」をクリックして、BIOS/UEFI セットアップを起動できます。)サーバーの電源がオンになっているがオペレーティング・システムがない場合、オペレーティング・システムを検出するために管理コントローラーによってサーバーのリセットが繰り返されます。

- `UEFI_Ethernet_*` と `UEFI_Slot_*` の設定がすべてサーバーの UEFI 設定で有効になっていることを確認します。設定を確認するには、サーバーを再起動し、プロンプト `<F1> Setup` が表示されたら、`F1` を押して Setup Utility を起動します。「**System Settings**」 ➡ 「**Devices and I/O Ports**」 ➡ 「**Enable / Disable Adapter Option ROM Support**」に移動し、「**Enable / Disable UEFI Option ROM(s)**」セクションを見つけて設定が有効であることを確認します。

  注：サポートされている場合、ベースボード管理インターフェースでリモート・コンソール機能を使用して設定をリモートで確認および変更することもできます。

- System x3950 X6 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。

このタスクについて

XClarity Administrator を使用すると、XClarity Administrator と同じ IP サブネットにある管理可能デバイスのプローブによって、環境内のラックおよびタワー・サーバーを自動的に検出できます。他のサブネットにあるラックおよびタワー・サーバーを検出するには、IP アドレスまたは IP アドレス範囲を指定するか、スプレッドシートから情報をインポートします。

重要：System x3850 および x3950 X6 サーバーについては、拡張可能なラック環境で各サーバーを管理する必要があります。

サーバーが XClarity Administrator の管理対象になった後、Lenovo XClarity Administrator は各管理対象サーバーを定期的にポーリングして、インベントリー、重要な製品データ、ステータスなどの情報を収集します。各管理対象サーバーを表示および監視して、管理操作 (システム設定、オペレーティング・システム・イメージのデプロイ、電源オン/オフなど) を実行できます。

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

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

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

  注：

  – RackSwitch デバイスは、認証用にのみ保存される資格情報をサポートします。XClarity Administrator ユーザー資格情報はサポートされていません。

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

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

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

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

  – XClarity Administrator 認証サーバーとしてローカルまたは外部 LDAP サーバーを使用している場合は、その認証サーバーで定義されているユーザー・アカウントが XClarity Administrator ドメイン内の XClarity Administrator、CMM、ベースボード管理コントローラーへのログインに使用されます。ローカルの CMM および管理コントローラー・ユーザー・アカウントは無効になります。

  – XClarity Administrator 認証サーバーとして SAML 2.0 ID プロバイダーを使用する場合、SAML アカウントは、管理対象デバイスにアクセスできなくなります。ただし、SAML ID プロバイダーと LDAP サーバーを同時に使用する場合で、ID プロバイダーが LDAP サーバーにあるアカウントを使用する場合、LDAP ユーザー・アカウントを使用して管理対象デバイスにログインできます。また、SAML 2.0 が提供するより高度な認証方法 (マルチファクター認証およびシングル・サインオンなど) を使用して XClarity Administrator にログインすることもできます。

– シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます (XClarity Administratorオンライン・ドキュメントの「を参照)

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

– ThinkSystem SR635 および SR655 サーバーで管理対象認証が有効になっている場合:

  – ベースボード管理コントローラー・ファームウェアは、最大 5 つの LDAP ユーザー・ロールをサポートします。XClarity Administrator は、管理中に次の LDAP ユーザー・ロールをサーバーに追加します: **lxc-supervisor**、**lxc-sysmgr**、 **lxc-admin**、**lxc-fw-admin** および **lxc-os-admin**。

    ThinkSystem SR635 および SR655 サーバーと通信するには、指定された少なくとも 1 つの LDAP ユーザー・ロールにユーザーが割り当てられている必要があります。

  – 管理コントローラーのファームウェアは、サーバーのローカル・ユーザーと同じユーザー名の LDAP ユーザーをサポートしていません。

– ThinkServer サーバーおよび System x M4 サーバーの場合は、XClarity Administrator 認証サーバーは使用しません。その代わり、デバイスで接頭辞「LXCA_」の後にランダムな文字列が続く IPMI アカウントが作成されます。(既存の IPMI ローカル・ユーザー・アカウントは無効になります。)ThinkServer サーバーを管理解除する場合は、「LXCA_」ユーザー・アカウントが無効になり接頭辞「LXCA_」が接頭辞「DISABLED_」に置き換えられます。ThinkServer サーバーが別のインスタンスによって管理されているかどうかを判別するために、XClarity Administrator は接頭辞「LXCA_」がついた IPMI アカウントを確認します。管理対象 ThinkServer サーバーの管理を強制することを選択した場合、そのデバイスで「LXCA_」がついたすべての IPMI アカウントが無効になり名前を変更されます。不要になった IPMI アカウントを手動で消去することを検討してください。

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

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

  – 手動で入力した認証情報を使用してデバイスを管理するたびに、以前の管理プロセス中にそのデバイス用に別の保存済み認証情報が作成されていても、そのデバイス用に新しい保存済み認証情報が作成されます。

  – デバイスを管理解除しても、XClarity Administrator は、管理プロセス中にそのデバイス用に自動的に作成され保管されている資格情報を削除しません。

1 台のデバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず最初の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。管理対象除外プロセス中にエラーが発生した場合、新規の XClarity Administrator で管理する際に「**管理の強制**」オプションを選択できます。

注：管理可能デバイスのネットワークをスキャンする場合、XClarity Administrator は、デバイスがすでに別のマネージャーで管理されているかどうかは、まずデバイスを管理しようとしなければ分かりません。

注：ネットワークで管理可能デバイスをスキャンするとき、XClarity Administrator は ThinkServer デバイスがすでに管理されているかどうかを認識しません。したがって、管理対象 ThinkServer デバイスが管理可能デバイスのリストに表示されることがあります。

管理プロセスでは、XClarity Administrator によって以下の処理が実行されます。

- 指定された資格情報を使用してサーバーにログインする。
- 各サーバーのインベントリーを収集する。

  注：管理プロセスが完了した後、インベントリー・データが一部収集されます。管理対象サーバーでは、そのサーバーのすべてのインベントリー・データが収集されてサーバーが保留状態でなくなるまで、サーバー・パターンのデプロイなどの特定のタスクをサーバーで実行できません。
- すべての管理対象デバイスが XClarity Administrator で構成されているものと同じ NTP サーバー構成を使用するように、NTP サーバーの設定を構成する。
- (System x および NeXtScale サーバーのみ) 最後に編集したファームウェア・コンプライアンス・ポリシーをサーバーに割り当てる。
- (Lenovo System x および NeXtScale サーバーのみ) オプションでデバイスのファイアウォール規則を構成し、XClarity Administrator からの受信要求のみを受け入れる。
- (System x および NeXtScale サーバーのみ) 管理コントローラーとのセキュリティー証明書の交換時に、CIM サーバー証明書と LDAP クライアント証明書を管理コントローラーから XClarity Administrator の信頼ストアにコピーし、XClarity Administrator の CA セキュリティー証明書と LDAP 信頼証明書を管理コントローラーに送信する。管理コントローラーは管理コントローラーの信頼ストアに証明書を読み込みます。それにより、管理コントローラーが XClarity Administrator の LDAP および CIM サーバーへの接続を信頼できるようになります。

  注：CIM サーバー証明書や LDAP クライアント証明書が存在しない場合、管理プロセス中に作成されます。
- 該当する場合は、管理対象認証を構成します。管理対象認証についての詳細は、認証サーバーの管理を参照してください。
- 該当する場合、リカバリー・ユーザー・アカウント (`RECOVERY_ID`) を作成します。`RECOVERY_ID` アカウントについて詳しくは、認証サーバーの管理を参照してください。

注：XClarity Administrator の管理プロセスでは、セキュリティー設定または暗号化設定 (暗号モードとセキュアな通信に使用されるモード) は変更されません。暗号化設定は、サーバーを管理対象にした後に変更できます (管理サーバーでの暗号化設定の構成を参照)。

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

手順

XClarity Administrator を使用してラックおよびタワー・サーバーを管理するには、以下のいずれかの手順を実行します。

- 一括インポート・ファイルを使用して多数のタワー / ラック・サーバーとその他のデバイスを検出および管理します (XClarity Administratorオンライン・ドキュメントのシステムの管理を参照してください)。
- XClarity Administrator と同じ IP サブネットにあるラックおよびタワー・サーバーを検出して管理します。

  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックします。「新しいデバイスの検出と管理」ページが表示されます。

テーブルの列をソートすると、管理するサーバーを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。「**列のカスタマイズ**」アイコン ( ) をクリックして、表示する列とデフォルトのソート順序を変更できます。

2. 「**更新**」アイコン ( ) をクリックして、XClarity Administrator ドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
3. 管理プロセス中にすべてのデバイスのファイアウォール規則を変更して XClarity Administrator からの受信要求のみを受け入れるようにするには、「**今後すべての管理対象デバイスで Encapsulation を有効にする**」チェックボックスをクリックします。

   Encapsulation は、特定のデバイスが管理対象になった後で有効または無効にできます。

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

   注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。
4. 管理するサーバーを 1 台以上選択します。
5. 「**選択を管理**」をクリックします。「管理」ダイアログが表示されます。

6. このデバイスで XClarity Administrator 管理対象認証またはローカル認証を使用するように選択します。管理対象認証はデフォルトで選択されています。ローカル認証を使用するには、「**管理対象認証**」をオフにします。
7. デバイスの認証に使用する資格情報のタイプを選択して適切な資格情報を指定します。
   - **手動で入力した資格情報を使用**
     - サーバーへの認証に使用されるユーザー ID とパスワードを指定します。
     - (オプション) パスワードが現在、デバイスで有効期限が切れている場合は、指定されたユーザー名の新しいパスワードを設定します。

     注：手動で入力した資格情報を使用するには、XClarity Administrator 管理対象認証を選択する必要があります 。
   - **保存された資格情報を使用**

     この管理対象デバイスで使用する保存された資格情報を選択します。「**新しいユーザーの作成**」をクリックして、新しい保存された資格情報を追加できます。
   - **ID 管理システムの使用**

     この管理対象デバイスに使用する ID 管理システムを選択します。次に、残りのフィールド (管理対象サーバーの IP アドレスまたはホスト名、ユーザー名、オプションでアプリケーション ID、セーフ、およびフォルダーなど) に入力します。

     アプリケーション ID を指定する場合は、必要に応じて、セーフとフォルダーも指定する必要があります。

     アプリケーション ID を指定しない場合は、XClarity Administrator CyberArk でオンボード・アカウントを識別するために CyberArk を設定したときに定義したパスを使用してください。

     注：ThinkSystem サーバーまたは ThinkAgile サーバーのみがサポートされます。ID 管理システムはXClarity Administratorで構成する必要があります。また、管理対象の ThinkSystem サーバーまたは ThinkAgile サーバーのLenovo XClarity Controllerは CyberArk と統合する必要があります。

   デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで他の XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

   通常および保存された資格情報について詳しくは、ユーザー・アカウントの管理および保存された資格情報の管理を参照してください。
8. 管理対象認証が選択されている場合、リカバリー・パスワードを指定します。

   パスワードを指定すると、このリカバリー・アカウント (`RECOVERY_ID`) がサーバーに作成され、すべてローカル・ユーザー・アカウントが無効になります。XClarity Administrator に問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用しても管理コントローラーにログイン *できません*。ただし、リカバリー・アカウントを使用してログインできます。

   注：
   - 管理対象認証を使用するように選択した場合は、リカバリー・パスワードはオプションです。ローカル認証を使用するように選択した場合は利用できません。
   - ローカル・リカバリー・アカウントまたは保存されているリカバリー資格情報を使用するように選択できます。いずれの場合も、ユーザー名は常に `RECOVERY_ID` です。
   - パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。
   - リカバリー・パスワードは後で使用できるように記録しておいてください。
   - リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。

リカバリー ID について詳しくは、認証サーバーの管理を参照してください。

9. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

   – 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   – 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

10. 「**管理**」をクリックします。

    ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、この進行状況を監視します。

11. プロセスが完了したら、「OK」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    – 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

      注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

    – デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
    – デバイスが正しく管理対象から除外されなかった場合。

    注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

- IP アドレスを手動で指定して、XClarity Administrator と同じ IP サブネットにないラックおよびタワー・サーバーを検出して管理する。

  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➔ 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。
  2. 管理プロセス中にすべてのデバイスのファイアウォール規則を変更して XClarity Administrator からの受信要求のみを受け入れるようにするには、「**今後すべての管理対象デバイスで Encapsulation を有効にする**」チェックボックスをクリックします。

     Encapsulation は、特定のデバイスが管理対象になった後で有効または無効にできます。

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

     注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。

  3. 「**手動で入力**」を選択します。
  4. 管理するサーバーのネットワーク・アドレスを指定します。

     – 「**単一システム**」をクリックし、単一の IP アドレス、ドメイン名、または完全修飾ドメイン名 (FQDN) を入力します。

注：FQDN を指定するには、「ネットワーク・アクセス」ページで有効なドメイン名が指定されていることを確認します (ネットワーク・アクセスの構成を参照)。

- 「**複数システム**」をクリックし、IP アドレスの範囲を入力します。別の範囲を追加するには、「**追加**」アイコン (➕) をクリックします。範囲を削除するには、「**削除**」アイコン (❌) をクリックします。

5. 「OK」をクリックします。「管理」ダイアログが表示されます
6. このデバイスで XClarity Administrator 管理対象認証またはローカル認証を使用するように選択します。管理対象認証はデフォルトで選択されています。ローカル認証を使用するには、「**管理対象認証**」をオフにします。
7. デバイスの認証に使用する資格情報のタイプを選択して適切な資格情報を指定します。
   - **手動で入力した資格情報を使用**
     - サーバーへの認証に使用されるユーザー ID とパスワードを指定します。
     - (オプション) パスワードが現在、デバイスで有効期限が切れている場合は、指定されたユーザー名の新しいパスワードを設定します。

     注：手動で入力した資格情報を使用するには、XClarity Administrator 管理対象認証を選択する必要があります 。
   - **保存された資格情報を使用**

     この管理対象デバイスで使用する保存された資格情報を選択します。「**新しいユーザーの作成**」をクリックして、新しい保存された資格情報を追加できます。
   - **ID 管理システムの使用**

     この管理対象デバイスに使用する ID 管理システムを選択します。次に、残りのフィールド (管理対象サーバーの IP アドレスまたはホスト名、ユーザー名、オプションでアプリケーション ID、セーフ、およびフォルダーなど) に入力します。

     アプリケーション ID を指定する場合は、必要に応じて、セーフとフォルダーも指定する必要があります。

     アプリケーション ID を指定しない場合は、XClarity Administrator CyberArk でオンボード・アカウントを識別するために CyberArk を設定したときに定義したパスを使用してください。

     注：ThinkSystem サーバーまたは ThinkAgile サーバーのみがサポートされます。ID 管理システムはXClarity Administratorで構成する必要があります。また、管理対象の ThinkSystem サーバーまたは ThinkAgile サーバーのLenovo XClarity Controllerは CyberArk と統合する必要があります。

   デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで他の XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

   通常および保存された資格情報について詳しくは、ユーザー・アカウントの管理および保存された資格情報の管理を参照してください。
8. 管理対象認証が選択されている場合、リカバリー・パスワードを指定します。

   パスワードを指定すると、このリカバリー・アカウント (`RECOVERY_ID`) がサーバーに作成され、すべてローカル・ユーザー・アカウントが無効になります。XClarity Administrator に問題が発生して、何らかの理由で機能しなくなった場合、通常のユーザー・アカウントを使用しても管理コントローラーにログイン *できません*。ただし、リカバリー・アカウントを使用してログインできます。

   注：

   - 管理対象認証を使用するように選択した場合は、リカバリー・パスワードはオプションです。ローカル認証を使用するように選択した場合は利用できません。

- ローカル・リカバリー・アカウントまたは保存されているリカバリー資格情報を使用するように選択できます。いずれの場合も、ユーザー名は常に RECOVERY_ID です。
- パスワードがデバイスのセキュリティー・ポリシーおよびパスワード・ポリシーに従っていることを確認します。セキュリティー・ポリシーとパスワード・ポリシーが異なる場合があります。
- リカバリー・パスワードは後で使用できるように記録しておいてください。
- リカバリー・アカウントは ThinkServer および System x M4 サーバーではサポートされていません。

リカバリー ID について詳しくは、認証サーバーの管理を参照してください。

9. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

   - 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   - 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

10. 「**管理**」をクリックします。

    ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、この進行状況を監視します。

11. プロセスが完了したら、「OK」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    - 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

      注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

    - デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
    - デバイスが正しく管理対象から除外されなかった場合。

    注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

終了後

- 追加のデバイスを検出して管理します。
- サーバー・パターンを作成してデプロイすることで、システム情報、ローカル・ストレージ、I/O アダプター、ブート・ターゲット、ファームウェア設定を構成します (構成パターンを使用したサーバーの構成を参照)。
- オペレーティング・システムがまだインストールされていないサーバーにオペレーティング・システム・イメージをデプロイします (ベア・メタル・サーバーへのオペレーティング・システムのインストール参照)。
- 現行ポリシー (管理対象デバイスでのファームウェアの更新を参照) に従っていないデバイスのファームウェアを更新します。
- デバイスを適切なラックに追加して物理的環境を反映します (ラックの管理を参照)。
- ハードウェアのステータスと詳細を監視します (管理対象サーバーのステータスの表示を参照)。

- イベントとアラートを監視します (イベントの使用とアラートの使用を参照)。
- XClarity Administrator のメニュー・バーで「**ハードウェア**」 ➡ 「**サーバー**」をクリックしてサーバーを選択し、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**SEL ログをクリア**」をクリックしてサーバーの SEL ログをクリアします。この操作は ThinkSystem および ThinkAgile サーバーでのみサポートされています。
- 有効期限が切れたまたは無効になった保存された資格情報を解決します (保存された資格情報の管理を参照)。
- すべての管理対象の ThinkSystem および ThinkAgile サーバーのシングル・サインオンを有効または無効にするには、XClarity Administrator のメニュー・バーで「**管理**」 ➡ 「**セキュリティー**」をクリックし、「**アクティブ・セッション**」をクリックして、「**シングル・サインオン**」を有効または無効にします。
- 管理対象の ThinkSystem および ThinkAgile サーバーのシングル・サインオンを有効または無効にします。
  - すべての管理対象の ThinkSystem および ThinkAgile サーバー (グローバル) については、XClarity Administrator のメニュー・バーで「**管理**」 ➡ 「**セキュリティー**」をクリックし、「**アクティブ・セッション**」をクリックして、「**シングル・サインオン**」を有効または無効にします。
  - 特定の ThinkSystem および ThinkAgile サーバーについては、XClarity Administrator のメニュー・バーで「**ハードウェア**」 ➡ 「**サーバー**」をクリックし、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**シングル・サインオンを使用可能にする**」または 「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**シングル・サインオンを使用不可にする**」をクリックします。

  注：シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます 。

管理対象サーバーのステータスの表示

Lenovo XClarity Administrator から、管理対象サーバーおよびこれらに取り付けられたコンポーネントの概要と詳細なステータスを表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

以下のステータス・アイコンは、デバイスの全体的な正常性を示します。証明書が一致しない場合、該当する各デバイスのステータスに「(非トラステッド)」と付加されます。たとえば、「警告 (非トラステッド)」となります。接続に問題がある場合やデバイスへの接続が信頼されない場合、該当する各デバイスのステータスに「(接続)」と付加されます。たとえば、「警告 (接続)」となります。

- ( ) クリティカル
- ( ) 警告
- ( ) 保留中
- ( ) 通知
- ( ) 正常
- ( ) オフライン

- ( ) 不明

デバイスは、以下のいずれかの電源状態になります。
- オン
- オフ
- のシャットダウン
- スタンバイ
- 休止
- 不明

手順

管理対象サーバーのステータスを表示するには、次の 1 つ以上の操作を実行します。

- XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。ダッシュボード・ページが開いて、すべての管理対象デバイスとその他のリソースの概要とステータスが表示されます。

- 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・サーバーおよびタワー・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。

  テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、ステータス・アイコンをクリックすると、選択された条件に一致するサーバーのみをリストすることもできます。

このページでは、以下の操作を実行できます。

- サーバーとそのコンポーネントに関する詳細情報を表示します (管理対象サーバーの詳細の表示を参照)。
- グラフィカルなラック・ビューまたはシャーシ・ビューでサーバーを表示するには、「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューで表示**」または「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**シャーシ・ビューで表示**」をクリックします。
- サーバーの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (サーバーの管理コントローラー・インターフェースの起動を参照)。
- サーバーをリモート管理します (リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理を参照)。
- サーバーの電源オン/電源オフを実行します (サーバーの電源のオン/オフを参照)。
- システム情報を変更するには、サーバーを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックします。
- インベントリーを最新の情報に更新するには、サーバーを選択して「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーを最新の情報に更新**」をクリックしてください。
- サーバーを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーのエクスポート**」をクリックして、1 つ以上のサーバーに関する詳細情報を単一 CSV ファイルにエクスポートします。

  注：最大 60 個のデバイスのインベントリー・データを一度にエクスポートできます。

  ヒント: CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- サーバーを管理解除します (ラック・サーバーまたはタワー・サーバーの管理解除を参照)。
- ローカル・ストレージ・アダプターを出荷時のデフォルト設定にリセットするには、「**すべての操作**」 ➡ 「**サービス**」 ➡ 「**ローカル・ストレージをデフォルトにリセット**」をクリックします。
- サーバーのロケーション LED の状態をオン/オフまたは点滅するには、サーバーを選択して、「**すべての操作**」 ➡ 「**サービス**」 ➡ 「**ロケーション LED 状態の切り替え**」をクリックして選択し、「**適用**」をクリックして変更します。
  - ThinkSystem SR635 および SR655 サーバーのロケーション LED の切り替えはサポートされていません。
  - ThinkServer サーバーのロケーション LED をオンまたはオフにすることができます。点滅はサポートされていません。

- サーバーの仮想再取り付けを実行します (Flex System シャーシのサーバーの仮想再取り付けを参照)。
- 不要なイベントは、「**イベントの除外**」アイコン ( ) をクリックして、イベントが表示されているすべてのページから除外します (イベントの除外を参照)。
- マスク不可割り込み (NMI) を使用してサーバーを再起動するには、「**すべての操作**」 ➡ 「**サービス**」 ➡ 「**NMI を発生させる**」をクリックします。
- サーバーでファイアウォール規則の変更を有効または無効にして受信要求を XClarity Administrator からのみに制限するには、サーバーを選択して 「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を有効化する**」または「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を無効化する**」をクリックします。共通 encapsulation 設定はデフォルトでは無効になっています。無効にされた場合、デバイスの encapsulation モードは「通常」に設定され、ファイアウォール規則は管理プロセスの一部として変更されません。

  共通 encapsulation の設定が有効にされ、デバイスが encapsulation をサポートする場合、XClarity Administrator は管理プロセス中にデバイスと通信し、デバイスの encapsulation モードを「encapsulationLite」に変更し、受信要求を XClarity Administratorからのみに制限するためデバイスのファイアウォール規則を変更します。

  注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。
- (コンバージド、Flex System、NeXtScale、System x、ThinkSystem サーバーのみ) XClarity Administrator のセキュリティー証明書とサーバー内のベースボード管理コントローラーのセキュリティー証明書との間で発生する可能性がある問題を解決する。サーバーを選択し、「**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 (非トラステッド・サーバー証明書の解決を参照)。
- グループ内のデバイスの有効期限が切れたまたは無効な保存された資格情報を解決します (サーバーの有効期限切れまたは無効の保存された資格情報の解決を参照)。
- サーバーを静的リソース・グループに追加またはグループから削除する。「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループに追加**」 または 「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループから削除**」 をクリックします。

管理対象サーバーの詳細の表示

Lenovo XClarity Administrator から管理対象サーバーに関する詳細情報 (ファームウェア・レベル、サーバー名、世界固有識別子 (UUID) など) を表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

CPU 使用率は、集約された C 状態の存在の測定値です。1 秒間の、使用済みおよび最大の C0 存在のパーセンテージとして測定されます。

メモリー使用量は、すべてのメモリー・チャネルの集約された読み取り/書き込みボリュームの測定値です。これは、1 秒あたりの、使用された帯域幅と使用可能な最大メモリー帯域幅のパーセンテージとして計算されます。

システム・レベルの室温は、サーバーの前面にある物理センサーによって測定されます。この温度は、サーバーの吸気口の温度を表します。温度が異なる時点で取得された場合、XClarity Administrator および CMM によって報告される温度が異なる可能性があることに注意してください。

手順

管理対象サーバーの詳細を表示するには、以下の手順を実行します。

ステップ 1. XClarity 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。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. 「**サーバー**」列のサーバーのリンクをクリックします。そのサーバーのステータス要約ページが開いて、サーバーのプロパティと、そのサーバーに取り付けられたコンポーネントのリストが表示されます。

注：System x および NeXtScale サーバーの場合、このページには LAN over USB アドレスがリストされますが、そのアドレスを XClarity Administrator から変更することはできません。その代わりに、サーバーでベースボード管理コントローラー・インターフェースを使用する必要があります。詳しくは、サーバーの資料で「LAN over USB インターフェースを使用した IMM2 へのアクセス」を参照してください。BladeCenter オンライン・ドキュメントで、ご使用のサーバーの製品ドキュメントが見つかります。

ステップ 3. 必要に応じて、以下の操作を実行します。

- システム情報や取り付けられたコンポーネントなどサーバーの要約を表示するには、「**要約**」をクリックします (管理対象サーバーのステータスの表示を参照)。
- 以下のようなサーバー・コンポーネントの詳細を表示するには、「**インベントリー詳細**」をクリックします。
  - サーバーと管理コントローラーのファームウェア・レベル。
  - 管理モジュール・ネットワークの詳細 (ホスト名、IPv4 アドレス、IPv6 アドレス、MAC アドレスなど)。
  - アセットの詳細 (サーバー名、世界固有識別子 (UUID)、場所など)
  - コンポーネントの詳細 (CPU、メモリー、ドライブ、拡張カードなど)

  注：

  - サーバーのすべての IP アドレスがリストされます。管理コントローラー・ポートの IP アドレスが最初にリストされます。管理コントローラーの IP アドレスが使用可能な場合、サーバーへの接続に使用されます。
  - データが特定のアダプターで使用できない場合、アダプターのいくつかのフィールド (製品名など) が空である場合があります。
  - 新しいアダプターがサーバーにインストールされた場合、アダプターがインベントリーに現れるにはサーバーをリブートする必要があります。
  - 一部のアドイン・カードの場合、デバイス名の下に Feature on Demand (FoD) 情報が表示されます。
  - 「タイプ」列のリンクをポイントすると、Intel Optain DCPMM メモリーなど、特定のコンポーネントに関する詳細情報が表示されます。
- このサーバーの現在のアラートのリストを表示するには、「**アラート**」をクリックします (アラートの使用を参照)。

  注：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 (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)。
- このサーバーのイベントのリストを表示するには、「**イベント・ログ**」をクリックします (イベント・ログでのイベントの監視を参照)。
- サーバーに関連付けられているジョブのリストを表示するには、「**ジョブ**」をクリックします (ジョブの監視を参照)。
- ロケーション、障害、情報など、サーバーの LED の現在のステータスを表示するには、「**Light Path**」をクリックします。これは、サーバーの前面パネルを確認することに相当します。
- 電力使用と室温の詳細を表示するには、「**電源および熱**」をクリックします。

  ヒント: 電源および熱の最新データを収集するには、Web ブラウザーの最新表示ボタンを使用します。データの収集には数分かかる場合があります。
- 「**構成**」をクリックして、サーバーの現在の構成情報 (ローカル・ストレージ、I/O アダプター、SAN ブート設定、ファームウェア設定など) および割り当てられた構成パターンへの準拠を表示します (構成パターンを使用したサーバーの構成 を参照)。
- 現在管理対象サーバーにインストールされている Feature on Demand キーのリストを表示するには、「**Feature on Demand キー**」をクリックします (Features on Demand キーの表示を参照)。

終了後

サーバーに対しては、要約と詳細情報の表示に加えて、以下の操作を実行できます。

- 「要約」ページからラックまたはシャーシ名をクリックすると、サーバーに関連付けられているラックまたはシャーシが表示されます。
- グラフィカルなラック・ビューまたはシャーシ・ビューで選択済みサーバーを表示するには、「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューで表示**」または「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**シャーシ・ビューで表示**」をクリックします。
- 選択済みサーバーの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (サーバーの管理コントローラー・インターフェースの起動を参照)。
- サーバーにリモート・アクセスします (リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理を参照)。
- 選択済みサーバーの電源オン/電源オフを実行します (サーバーの電源のオン/オフを参照)。
- 選択済みサーバーのシステム情報を変更するには、「**プロパティの編集**」をクリックします。
- 選択済み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、「**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。
- サーバーに関する詳細情報を CSV ファイルにエクスポートするには、「**操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーのエクスポート**」をクリックします。

  注：

  – CSV ファイルのインベントリー・データについて詳しくは、XClarity Administrator オンライン・ドキュメントの GET /nodes/*<UUID_list>* REST API を参照してください。

  – CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- 不要なイベントは、「**操作**」 ➡ 「**サービスのリセット**」 ➡ 「**イベントの除外**」をクリックして、イベントが表示されているすべてのページから除外します (イベントの除外を参照)。
- マスク不可割り込み (NMI) を使用して選択済みサーバーを再起動するには、「**操作**」 ➡ 「**サービス**」 ➡ 「**NMI を発生させる**」をクリックします。
- 選択済みサーバーのロケーション LED の状態をオン/オフまたは点滅するには、「**操作**」 ➡ 「**サービス**」 ➡ 「**ロケーション LED 状態の切り替え**」をクリックして状態を選択し、「**適用**」をクリックします。

  注：
  – ThinkSystem SR635 および SR655 サーバーのロケーション LED の切り替えはサポートされていません。
  – ThinkServer サーバーのロケーション LED をオンまたはオフにすることができます。点滅はサポートされていません。
- 選択した ThinkSystem および ThinkAgile サーバーのシングル・サインオンを有効または無効にするには、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**シングル・サインオンを使用可能にする**」または「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**シングル・サインオンを使用不可にする**」をクリックします。

  シングル・サインオンを使用すると、既に XClarity Administrator にログインしているユーザーが自動的にベースボード管理コントロールにログインすることができます。シングル・サインオンは、ThinkSystem または ThinkAgile サーバーが XClarity Administrator によって管理対象になるとデフォルトで有効になります (サーバーが CyberArk パスワードで管理されている場合を除く)。すべての管理対象の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効または無効にするように、グローバル設定を構成できます。特定の ThinkSystem サーバーおよび ThinkAgile サーバーのシングル・サインオンを有効にすると、すべての ThinkSystem サーバーおよび ThinkAgile サーバーのグローバル設定が上書きされます 。

  注：認証に CyberArk ID 管理システムを使用すると、シングル・サインオンは自動的に無効になります。
- 選択済みサーバーでファイアウォール規則の変更を有効または無効にして受信要求を XClarity Administrator からのみに制限するには、「**操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を有効にする**」または「**操作**」 ➡ 「**セキュリティー**」 ➡ 「**Encapsulation を無効にする**」をクリックします。共通

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

共通 encapsulation の設定が有効にされ、デバイスが encapsulation をサポートする場合、XClarity Administrator は管理プロセス中にデバイスと通信し、デバイスの encapsulation モードを「encapsulationLite」に変更し、受信要求を XClarity Administratorからのみに制限するためデバイスのファイアウォール規則を変更します。

注意：encapsulation が有効にされ、エンドポイントが管理解除になるまでに XClarity Administrator が使用できなくなった場合、encapsulation を無効にしてデバイスの通信を確立するのに必要な段階を踏む必要があります。リカバリー手順については、lenovoMgrAlert.mib ファイルと管理サーバー障害後の CMM による管理の回復。

- (ThinkServer 以外のサーバーのみ) Lenovo XClarity Administrator のセキュリティー証明書と選択済みサーバー内の管理コントローラーのセキュリティー証明書との間で発生する可能性がある問題を解決するには、「**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 (非トラステッド・サーバー証明書の解決を参照)。

サーバー構成データのバックアップと復元

Lenovo XClarity Administrator には、サーバー構成データの組み込みバックアップ機能はありません。代わりに、ご使用の管理対象サーバーで使用可能なバックアップ機能を使用します。

- **コンバージド、Flex System、System x、ThinkSystem、および NeXtScale サーバー**
  - サーバー構成データのバックアップ

    管理 Web インターフェースまたは CLI を使用して、ファームウェアをバックアップします。

    - IMM Web インターフェースから、「**IMM 管理**」 ➡ 「**IMM 構成**」をクリックします。
    - CLI から、`backup` コマンドを使用します。

    IMM によるサーバーのバックアップについて詳しくは、Integrated Management Module II オンライン・ドキュメントを参照してください。

    サーバー上で稼働しているアプリケーションをバックアップするには、オペレーティング・システムによって提供されているツールを使用します。詳しくは、お使いのオペレーティング・システムに付属の資料を参照してください。

    Flex System 計算デバイスの場合、計算ノードにインストールされているオプションの設定を必ずバックアップします。Advanced Setup Utility (ASU) を使用すると、オプション設定を含めて、計算ノードのすべての設定をバックアップできます。ASU に関する情報については、Advanced Settings Utility (ASU) Web サイトを参照してください。
  - サーバー構成データの復元

    管理 Web インターフェースまたは CLI を使用して、ファームウェアを復元します。BMC によるサーバーの復元について詳しくは、Integrated Management Module II オンライン・ドキュメントを参照してください。

    サーバーにインストールされているソフトウェアを復元するには、サーバーで実行されているオペレーティング・システムとすべてのアプリケーションに付属のドキュメントを使用します。

    - IMM Web インターフェースから、「**IMM 管理**」 ➡ 「**IMM 構成**」をクリックします。
    - CLI から、`restore` コマンドを使用します。

  注：ヒント: シャーシ・コンポーネントのバックアップおよび復元について詳しくは、PureFlex および Flex System のバックアップと復元に関する ベスト・プラクティス・ガイドを参照してください。
- **ThinkServer サーバー**復元手順は ThinkServer サーバーのタイプごとに異なります。デバイスの復元については、サーバーに付属の製品ドキュメントを参照してください。

システム・ガードを有効にする

システム・ガードは、XCC2 を持つ ThinkSystem サーバーのハードウェア・インベントリーの逸脱を監視します。

このタスクについて

監視対象インベントリーには、プロセッサー、メモリー、PCI アダプター、ドライブ、システム・ボード、およびライザーが含まれます。ファームウェア・レベルおよび構成設定の変更は検出されません。

システム・ガードが有効になっている場合、ハードウェア・インベントリーのスナップショットは、選択した各デバイスのトラステッド・リファレンスとして取得されます。デバイスがリブートすると、デバイス内のベースボード管理コントローラーが現在のシステム構成を収集し、スナップショットと比較します。1 つ以上のコンポーネントで相違が検出されると、システム・ガードがイベントを発動します。プロセッサーまたはメモリーの相違が検出された場合、システム・ガードはイベントを発動し、サーバーはオプションで OS からブートできなくなります。

手順

もう 1 つの XCC2 を含むサーバー のシステム・ガードを有効にするには、 以下の手順を完了します。

ステップ 1. XClarity Administrator のメニューで、「**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がテーブル・ビューで表示されます。

ステップ 2. 1 つ以上の XCC2 を含むサーバー を選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**システム・ガードの有効化**」をクリックして、「システム・ガードの有効化」ダイアログを表示します。

ステップ 4. システム・ガードが有効になっている状態で、インベントリーの変更が検出され、サーバーが不適合になったときに実行する操作を選択します。

- **有効化、システムのデフォルト動作を保持**。現在の動作が使用されています。。デフォルトの動作では、イベントを生成します。
- **有効化、非適合の場合に OS ブートを防止**。1 つのイベントが発行されています。OS からブートしようとすると、システム・ガードがプロセッサーまたはメモリーへの構成の変更を検出するという警告が表示されます。この場合、変更が予期しないものであれば、ベースボード管理コントローラーにログインするように求めるプロンプトが表示されます。そうでない場合は、ブートまたはシャットダウンのプロセスを続行できます。5 分以内に応答しない場合は、サーバーがデフォルトでシャットダウンされます。
- **有効化、非適合の場合にイベントを生成**。イベントが発行されましたが、その他の操作は実行されません。

ステップ 5. 「**適用**」をクリックします。

ジョブが作成され、選択したサーバーのインベントリー・スナップショットが作成されます。ジョブ・ログからジョブのプロセスを監視できます。XClarity Administrator のメニューで、「**監視**」 ➡ 「**ジョブ**」の順にクリックします。ジョブ・ログについて詳しくは、「ジョブの監視」を参照してください。

終了後

選択したサーバーでシステム・ガードを無効にするには、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**システム・ガードの無効化**」をクリックして、「**適用**」をクリックします。

ドライブのデータの安全な消去

Lenovo XClarity Administrator は、バージョン 22B 以降を実行している選択済みの ThinkSystem サーバーと ThinkAgile サーバーのすべてのドライブのデータを安全に消去できます。この操作では、ドライブ全体に 2 進数の 0 と 1 (ランダムなデータ) を入力することで各ドライブを永久的に上書きするため、ドライブに何が保存されていたかがわかりにくくなります。

注意：

- この操作は、ドライブのすべてのデータを*永久的*および*不可逆的*に消去します。
- ジョブが送信された後にこの操作を取り消す方法はありません。

始める前に

ドライブのデータを消去するには、**lxc-supervisor** 権限が必要です。

消去する管理対象サーバーに UEFI 管理パスワードが設定されていないことを確認します。UEFI 管理パスワードがサーバーに設定されている場合、それらのサーバーのドライブは消去されません。

デフォルトでは、一度に最大 3 つのサーバーのドライブのデータを安全に消去できます。一度に消去できるサーバーの数を設定するには、「**管理**」 ➡ 「**インベントリー設定**」をクリックし、「**一度に消去できるサーバーの最大数**」を目的の値に設定します。選択できるサーバー数は `3 - 100` です。

一度に許可される安全な消去のジョブは 1 つのみです。安全な消去の別のジョブを開始する前に、現在のジョブが完了するまで待つ必要があります。

非常に大きなドライブを消去するには、数時間かかる場合があります。

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。

このタスクについて

以下のドライブのデータを消去できます。

- NVMe
- SAS
- SAS HBA
- SAS RAID
- SATA
- 外部接続ストレージ・デバイス
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

安全な消去の操作を行うと、監査ログにエントリーが作成されます。イベント転送機能を使用して、このイベントを転送することができます (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 を参照)。

安全な消去での問題のトラブルシューティングについては、XClarity Administratorオンライン・ドキュメントの「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」および「Marvel RAID に 接続した際に、SATA SDD ボリュームを安全に消去できない」を参照してください。

手順

特定の管理対象サーバーのすべてのドライブを安全に消去するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニューで、「**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がテーブル・ビューで表示されます。

ステップ 2. サーバーを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**サービス**」 ➡ 「**ドライブの安全な消去 (HDD/SDD)**」をクリックします。

ステップ 4. スーパーバイザー・パスワードを入力して、選択済みサーバーのすべてのドライブを消去することを確認します。

ステップ 5. 「**消去**」をクリックします。

一度に 3 つより多いサーバーのドライブの消去を実行するように選択した場合、ユーザー ID とパスワードの入力を求められます。XClarity Administrator へのログインに使用したユーザー資格情報と同じユーザー資格情報を入力してください。

この操作を実行するためのジョブが作成されます。XClarity Administrator のメニューで「**監視**」 ➡ 「**ジョブ**」をクリックすると、「ジョブ」ページで更新の進行状況を確認できます。ジョブが正常に完了しなかった場合は、ジョブのリンクをクリックしてジョブの詳細を表示します (ジョブの監視 を参照)。

リモート制御の使用

Lenovo XClarity Administrator Web インターフェースで、リモート制御セッションを開いてローカル・コンソールで作業しているかのように管理対象サーバーを管理できます。リモート制御セッションを使用して、サーバーの電源のオン/オフや、ローカルまたはリモート・ドライブの論理マウントなどの操作を実行できます。

任意のデバイスに対してリモート制御セッションを起動するには、**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** 権限が必要です。

リモート制御を使用した ThinkSystem または ThinkAgile サーバーの管理

Lenovo XClarity Administrator Web インターフェースで、リモート制御セッションを開いてローカル・コンソールで作業しているかのように管理対象 ThinkSystem サーバーまたは ThinkAgile サーバーを管理できます。リモート制御セッションを使用して、電源操作と、ローカルまたはネットワーク・ドライブの論理マウント操作を実行できます。

始める前に

サーバーでは、encapsulation を無効にする必要があります。

サーバーへのリモート制御セッションを開くには、サーバーが「オンライン」または「正常」状態になっている必要があります。他のアクセス状態のサーバーの場合、そのサーバーにリモート制御セッションは接続できません。サーバー・ステータスの表示について詳しくは、管理対象サーバーの詳細の表示を参照してください。

ThinkSystem SR635 および SR655 サーバーの場合は、以下の考慮事項を確認してください。

- ベースボード管理コントローラー・ファームウェア v2.94 以降が必要です。
- マルチユーザー・モードのみがサポートされています。シングルユーザー・モードはサポートされていません。
- Internet Explorer 11 はサポートされていません。

- リモート制御セッションからサーバーの電源をオンまたはオフにすることはできません。

このタスクについて

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

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

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

手順

特定のサーバーへのリモート制御セッションを開くには、以下の手順を実行します。

ステップ 1. XClarity 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。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. リモート制御セッションを開くサーバーを選択します。

ステップ 3. 「**リモート制御**」アイコン () をクリックします。

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

終了後

リモート制御セッションが正しく開かない場合、XClarity Administrator オンライン・ドキュメントのリモート制御に関する問題を参照してください。

リモート制御を使用した ThinkServer および NeXtScale sd350 M5 サーバーの管理

Lenovo XClarity Administrator Web インターフェースで、管理対象 ThinkServer サーバーおよび NeXtScale sd350 M5 サーバーに対してリモート制御セッションを開き、ローカル・コンソールから管理しているかのようにサーバーを管理できます。リモート制御セッションを使用して、電源操作やリセット操作、ローカルまたはネットワーク・ドライブのサーバーへの論理マウント、スクリーンショットのキャプチャやビデオの録画を実行できます。

始める前に

- これらのサーバーに対してリモート制御を行うには、Java WebStart サポートを使用した Java Runtime Environment (JRE) がクライアント・サイドにインストールされている必要があります。オープンソースの JDK を強くお勧めします。ベンダーの JRE または JDK を使用する場合は、商用に適切にライセンスされていることを確認してください。以下の JRE がサポートされています。
  - Oracle JRE 7 (Oracle Java ダウンロード Web サイト 参照)

    注意：
    - Java 7 では、TLSv1.2 以降のサポートが必要です (管理サーバーでの暗号化設定の構成 を参照)。
    - Java 7 のサポートは、今後廃止される予定です。
  - Oracle JRE 8 (有料ライセンスが必要) (Oracle Java ダウンロード Web サイト 参照)
  - Adoptium OpenJDK 8 と IcedTea-Web v1.8 プラグイン (Adoptium OpenJDK Web サイト を参照)
  - Amazon Corretto 8 (Amazon Corretto 8 ダウンロード Web サイト を参照)

Java WebStart は OpenJDK または Coretto のインストール・パッケージには含まれていないため、別途インストールする必要があります。IcedTea-Web または OpenWebStart は GNU GPLV2 ライセンスで使用できます (IcedTea-OpenJDK ダウンロード Web サイト および OpenWebStart Web サイト を参照)。

- 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Features on Demand キーの表示

このタスクについて

XClarity Administrator から 1 つの ThinkServer サーバーに対して、リモート制御セッションを起動できます。

サーバーへのリモート制御セッションを開くには、サーバーが「オンライン」または「正常」状態になっている必要があります。他のアクセス状態のサーバーの場合、そのサーバーにリモート制御セッションは接続できません。サーバー・ステータスの表示について詳しくは、管理対象サーバーの詳細の表示を参照してください。

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

手順

特定のサーバーへのリモート制御セッションを開くには、以下の手順を実行します。

ステップ 1. XClarity 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。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. リモート制御セッションを開くサーバーを選択します。

ステップ 3. 「**リモート制御**」アイコン () をクリックします。

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

終了後

リモート制御セッションが正しく開かない場合、XClarity Administrator オンライン・ドキュメントのリモート制御に関する問題を参照してください。

リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理

Lenovo XClarity Administrator Web インターフェースでリモート制御セッションを開き、ローカル・コンソールから管理しているかのように、コンバージド、Flex System、NeXtScale、および System x サーバーを管理できます。

始める前に

詳細:  XClarity Administrator: リモート制御

- これらのサーバーに対してリモート制御を行うには、Java WebStart サポートを使用した Java Runtime Environment (JRE) がクライアント・サイドにインストールされている必要があります。オープンソースの JDK を強くお勧めします。ベンダーの JRE または JDK を使用する場合は、商用に適切にライセンスされていることを確認してください。以下の JRE がサポートされています。

  - Oracle JRE 7 (Oracle Java ダウンロード Web サイト 参照)

    注意：
    - Java 7 では、TLSv1.2 以降のサポートが必要です (管理サーバーでの暗号化設定の構成 を参照)。
    - Java 7 のサポートは、今後廃止される予定です。
  - Oracle JRE 8 (有料ライセンスが必要) (Oracle Java ダウンロード Web サイト 参照)
  - Adoptium OpenJDK 8 と IcedTea-Web v1.8 プラグイン (Adoptium OpenJDK Web サイト を参照)
  - Amazon Corretto 8 (Amazon Corretto 8 ダウンロード Web サイト を参照)

  Java WebStart は OpenJDK または Coretto のインストール・パッケージには含まれていないため、別途インストールする必要があります。IcedTea-Web または OpenWebStart は GNU GPLV2 ライセンスで使用できます (IcedTea-OpenJDK ダウンロード Web サイト および OpenWebStart Web サイト を参照)。
- リモート制御セッションは、以下のオペレーティング・システム (32 ビットまたは 64 ビット) を実行しているサーバーで開始できます。
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- リモート制御を使用するには、コンバージド、NeXtScale、および System x サーバーにリモート・プレゼンスの Features on Demand キーがインストールされている必要があります。FoD キーがサーバーで検出されない場合、使用可能なサーバーのリストを表示すると、リモート制御セッションに「**アクティベーション・キーが見つかりません**」というメッセージが表示されます。「サーバー」ページから、リモート・プレゼンスの有効化または無効化を行うか、あるいはサーバーにインストールしないことを選択できます (管理対象サーバーのステータスの表示を参照)。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、Features 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の開始に使用するユーザー・アカウントは、XClarity Administrator 認証サーバーに定義されている有効なユーザー・アカウントであることが必要です。ユーザー・アカウントには、サーバーにアクセスして管理するための十分なユーザー権限が必要です。
- リモート制御セッションを開く前に、セキュリティー、パフォーマンス、キーボードに関する考慮事項を確認してください。これらの考慮事項について詳しくは、リモート制御に関する考慮事項を参照してください。
- 「リモート制御」ダイアログでは、ローカル・システムのオペレーティング・システムで定義されたロケールと表示言語設定が使用されます。ローカル・システムが Windows で実行されている場合、ロケール設定を変更する方法については Java Web サイトを参照してください。表示言語を変更するには、Windows のローカライズ版をインストールするか、Windows Web サイトから言語パックをインストールします。

このタスクについて

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

サーバーへのリモート制御セッションを開くには、サーバーが「オンライン」または「正常」状態になっている必要があります。他のアクセス状態のサーバーの場合、そのサーバーにリモート制御セッションは接続できません。サーバー・ステータスの表示について詳しくは、管理対象サーバーの詳細の表示を参照してください。

Lenovo XClarity Administrator のメニュー・バーから「**プロビジョニング**」 ➡ 「**リモート制御**」の順にクリックして、非ターゲットのリモート制御セッションを開くことができます。その後、Web ブラウザーによるセキュリティ警告をすべて受け入れます。

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

手順

以下の手順を実行して、特定のコンバージド、Flex System、NeXtScale、および System x サーバーへのリモート制御セッションを開きます。

ステップ 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。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. リモート制御セッションを開くサーバーを選択します。

ステップ 3. 「**リモート制御**」アイコン () をクリックします。

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

ステップ 5. オプションで、デスクトップに Remote Control アイコンを保存することを選択します。このアイコンを使用して、XClarity Administrator Web インターフェースにログインしないでリモート制御セッションが起動できます。

ステップ 6. プロンプトが表示されたら、次のいずれかの接続モードを選択します。

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

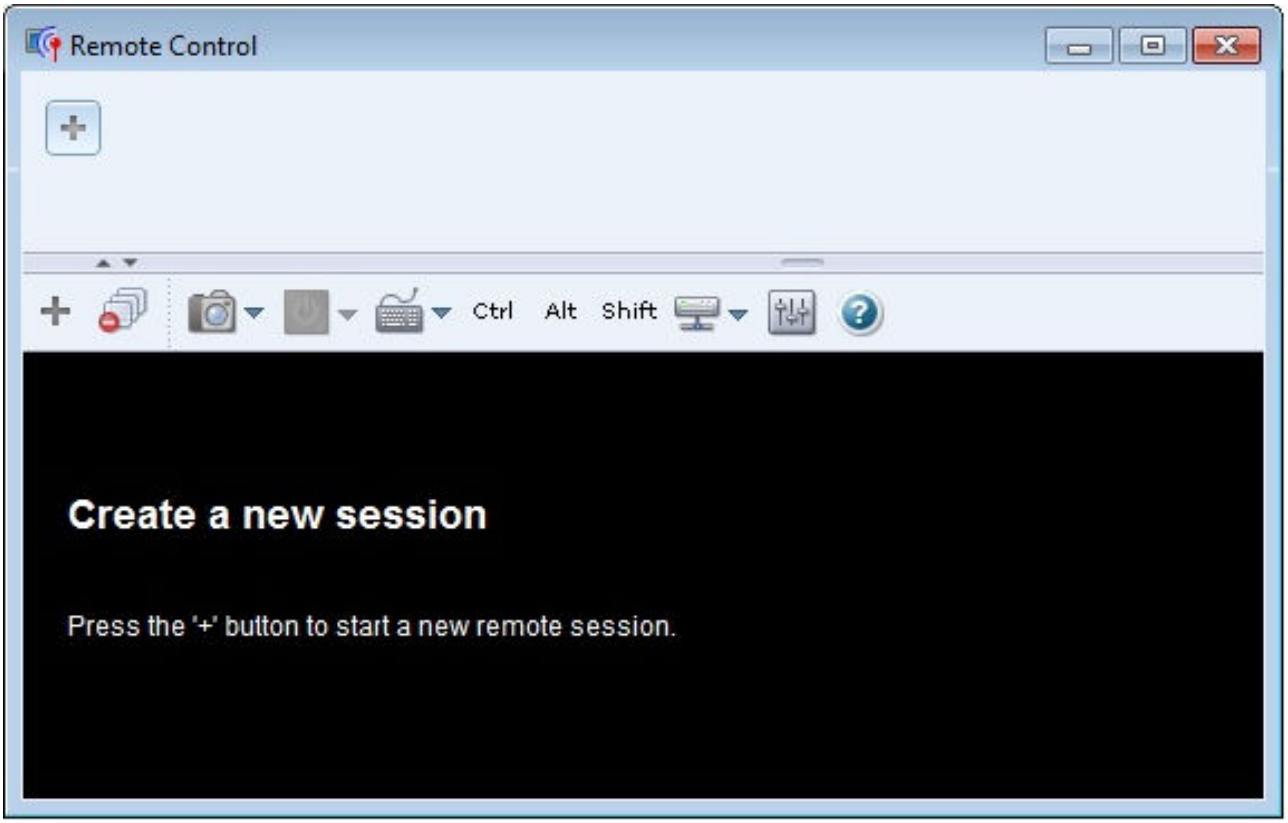
ステップ 7. プロンプトが表示されたら、ローカル・システムのリモート制御セッションにショートカットを保存するかどうかを選択します。

ショートカットを保存すると、指定したサーバーに対するリモート制御セッションをそのショートカットから開けるようになります。XClarity Administrator の Web インターフェースからリモート制御セッションを開始する必要はありません。ただし、XClarity Administrator 認証サーバーを使用してユーザー・アカウントが検証されるため、ローカル・システムが XClarity Administrator にアクセスできる必要はあります。

このショートカットには、手動でサーバーを追加できる空のリモート制御セッションを開くリンクが含まれています。

結果

「リモート制御」ウィンドウが表示されます。



サムネール領域には、現在リモート制御セッションによって管理されているすべてのサーバー・セッションのサムネールが表示されます。

複数のサーバー・セッションを表示し、サムネールをクリックしてサーバー・セッション間を移動できます。サムネールをクリックすると、そのサーバーのコンソールがビデオ・セッション領域に表示されます。アクセスしているサーバーが多すぎてサムネール領域に表示しきれない場合は、「**右にスクロール**」アイコン () と「**左にスクロール**」アイコン () をクリックすると、画面がスクロールしてその他のサーバーのサムネールが表示されます。**すべてのセッション**アイコン () をクリックすると、開いているすべてのサーバー・セッションのリストが表示されます。

サムネール領域で、**サーバーの追加**アイコン () をクリックすると、管理しているサーバーのリストに新しいサーバーを追加できます。セッションの追加について詳しくは、リモート制御セッションへのサーバー・コンソールの追加を参照してください。「サムネール」ページでは、サムネール領域の表示/非表示やサムネールの更新間隔を制御できます。サムネール設定について詳しくは、リモート制御の設定を参照してください。

終了後

リモート制御セッションが正しく開かない場合、XClarity Administrator オンライン・ドキュメントのリモート制御に関する問題を参照してください。

「リモート制御」ダイアログでは、以下の操作を実行できます。

- 他のサーバーへのセッションを現在のリモート制御セッションに追加できます (リモート制御セッションへのサーバー・コンソールの追加を参照)。

- サムネール領域の表示/非表示を切り替えるには、「**サムネール切り替え**」アイコン () をクリックします。
- リモート制御セッションをウィンドウまたはフルスクリーンとして表示するには、「**画面**」アイコン () をクリックし、「**フルスクリーンをオンに切り替え**」または「**フルスクリーンをオフに切り替え**」をクリックします。
- リモート制御セッションで Ctrl、Alt、Shift キーを使用します (Ctrl、Alt、Shift キーの使用を参照)。
- ソフトキーと呼ばれるカスタム・キー・シーケンスを定義します (ソフトキーの定義を参照)。
- 現在選択されているサーバー・セッションのスクリーン・キャプチャーを取得してさまざまな形式で保存するには、「**画面**」アイコン () をクリックし、「**スクリーンショット**」をクリックします。
- リモート・メディア (CD、DVD、USB の各デバイスや、ディスク・イメージ、CD (ISO イメージ) など) を選択したサーバーにマウントするか、マウントされたデバイスを別のサーバーに移動します (リモート・メディアのマウントまたは移動を参照)。
- イメージをリモート・メディアからサーバーにアップロードします (サーバーへのイメージのアップロードを参照)。
- リモート・コンソールからサーバーの電源をオンまたはオフにします (リモート制御セッションからのサーバーの電源のオン/オフを参照)。
- リモート制御の設定を変更します (リモート制御の設定を参照)。

リモート制御に関する考慮事項

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

セキュリティーに関する考慮事項

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

デフォルトでは、複数のリモート制御セッションをサーバーに対して確立できます。ただし、リモート制御セッションを開始するとき、シングルユーザー・モードでセッションを開始してサーバーに対して排他的なセッションを確立するオプションがあります。サーバーから切断するまで、そのサーバーに対する他のすべてのリモート制御セッションはブロックされます。

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

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

1. ローカル・システムにインストールされた FIPS 140 認定の暗号プロバイダーのプロバイダー名を見つけます。

   ヒント: FIPS 140 コンプライアンスについて詳しくは、SunJSSE 向け FIPS 140 Compliant Mode Web サイトを参照してください。
2. ファイル `$(java.home)/lib/security/java.security` を編集します。
3. `com.sun.net.ssl.internal.ssl.Provider` を含む行に FIPS 140 認定の暗号プロバイダーの名前を追加します。例えば、以下のように変更します。
   ```
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider
   ```
   次のように変更できるようにします:
   ```
   security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS
   ```

パフォーマンスに関する考慮事項

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

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

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

キーボードに関する考慮事項

リモート制御セッションでは以下のキーボード・タイプがサポートされています。

- ベルギー語 105 キー
- ブラジル語
- 中国語
- フランス語 105 キー
- ドイツ語 105 キー
- イタリア語 105 キー
- 日本語 109 キー
- 韓国語
- ポルトガル語
- ロシア語
- スペイン語 105 キー
- スイス語 105 キー
- 英語 (英国) 105 キー
- 英語 (米国) 104 キー

キーボード設定については、リモート制御の設定を参照してください。

リモート制御セッションへのサーバー・コンソールの追加

1 つ以上のサーバー・コンソールを現在のリモート制御セッションに追加できます。

手順

1 つ以上のサーバー・コンソールを現在のリモート制御セッションに追加するには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウから、「**新しいセッション**」アイコン () をクリックします。

Lenovo XClarity Administrator によって管理されており、ユーザー・アカウントで管理できるシャーシとラック・サーバーのリストがダイアログに表示されます。

ヒント: リストにサーバーが表示されない場合は、XClarity Administrator オンライン・ドキュメントのリモート制御に関する問題で問題を解決できる可能性のある手順を参照してください。

ステップ 2. 接続するサーバーを 1 台以上選択します。

「**タイプ**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (システム名やエンクロージャー名など) を入力することで、表示されるサーバーを絞り込むことができます。

「**すべて選択**」を選択すると、リスト内のすべてのサーバーを選択できます。

ステップ 3. **オプション**: 選択した各サーバーに対して排他的なセッションを開くには、「**シングルユーザー・モード**」を選択します。

このオプションを選択した場合、選択したサーバーから切断するまで、選択したサーバーに対する他のすべてのリモート制御ッションはブロックされます。このオプションを使用できるのは、選択したサーバーに対して他のリモート制御ッションが確立されていない場合のみです。

このオプションを選択しない場合は、デフォルトでマルチユーザー・モードが使用されます。

ステップ 4. 「**接続**」をクリックします。

リモート制御セッションからのサーバーの電源のオン/オフ

リモート制御セッションからサーバーの電源をオンまたはオフにすることができます。

手順

サーバーの電源のオン/オフを実行するには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウで、電源のオン/オフを行うサーバーのサムネールをクリックします。

ステップ 2. 「**電源**」アイコン () をクリックし、次のいずれかの電源操作をクリックします。

- **電源オン**
- **通常の電源オフ**
- **今すぐ電源オフ**
- **通常の再起動**
- **今すぐ再起動**
- **NMI を発生させる**
- **システム・セットアップから再起動** (Lenovo コンバージド、Flex System、NeXtScale、System x サーバーのみ)

ヒント: 「**電源**」アイコンは、サーバーの電源がオンになっている場合に緑色になります。

ソフトキーの定義

現在のリモート制御セッションに対して、*ソフトキー*と呼ばれる独自のカスタム・キー・シーケンスを定義することができます。

始める前に

ソフトキー定義の最新のリストを表示するには、「**キーボード**」アイコン () をクリックします。

ソフト・キー定義は、リモート制御セッションを開始したシステムに保管されます。そのため、別のシステムからリモート制御セッションを開始する場合は、ソフトキーを定義し直す必要があります。

ユーザー設定 (ソフトキーを含む) を「設定」ダイアログの「**ユーザー設定**」タブでエクスポートすることもできます。詳しくは、ユーザー設定のインポートとエクスポートを参照してください。

注：国際キーボードを使用する場合に、オルタネート・グラフィック・キー (AltGr) を必要とするソフトキーを定義するには、リモート制御アプリケーションの起動に使用するワークステーションのオペレーティング・システムと、リモート・アクセスするサーバーのオペレーティング・システムが、同じタイプである必要があります。たとえば、サーバーで Linux が実行されている場合は、Linux を実行しているワークステーションでリモート制御セッションを呼び出す必要があります。

手順

ソフトキーを追加するには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウから、「**キーボード**」アイコン () をクリックし、「**ソフトキーの追加**」をクリックします。「設定」ダイアログに「**ソフトキー・プログラマー**」タブが表示されます。

ステップ 2. 「**新規**」をクリックします。

ステップ 3. 定義するキー・シーケンスを入力します。

ステップ 4. 「**OK**」をクリックします。新しいソフトキーがソフトキーのリストに追加されます。

Ctrl、Alt、Shift キーの使用

一部のオペレーティング・システムには、リモート・サーバーに渡されずにインターセプトされるキーがあります。スティッキー・キー・ボタンを使用すると、管理しているサーバーに直接キー・ストロークを送信できます。

手順

Ctrl キーまたは Alt キーの組み合わせを送信するには、ツールバーの「**Ctrl**」または「**Alt**」をクリックし、カーソルをビデオ・セッション領域に置いて、キーボードのキーを押します。

たとえば、Ctrl+Alt+Del のキーの組み合わせを送信するには、以下の手順を実行します。

1. ツールバーの「**Ctrl**」をクリックします。
2. ツールバーの「**Alt**」をクリックします。
3. ビデオ・セッション領域の任意の場所を左クリックします。
4. キーボードの Delete キーを押します。

注：マウス・キャプチャー・モードが有効になっている場合は、カーソルをビデオ・セッション領域の外に移動するには左 Alt キーを押す必要があります。マウス・キャプチャー・モードはデフォルトで無効になっていますが、「ツールバー」ページで有効にすることができます (リモート制御の設定を参照)。

ツールバーの「**Ctrl**」、「**Alt**」、「**Shift**」は、クリックしてキーをアクティブにすると、キーボードのキーを押すか、そのボタンをもう一度クリックするまで、アクティブなままになります。

リモート・メディアのマウントまたは移動

リモート・メディア機能を使用すると、ローカル・システムのリモート・メディア (CD、DVD、USB の各デバイスや、ディスク・イメージ、CD (ISO イメージ) など) を選択したサーバーにマウントすることができます。ベースボード管理コントローラー (BMC) で使用できるローカル・ストレージにイメージをアップロードすることもできます。

始める前に

管理コントローラーのローカル・ストレージをマウントしてデータをアップロードできるのは一度に 1 人のユーザーのみです。管理コントローラーのローカル・ストレージがマウントされている間や、データがローカル・ストレージにアップロードされている間は、他のユーザーはローカル・ストレージにアクセスできません。

Linux オペレーティング・システムを実行しているサーバーでは、複数の ISO イメージのマウントはサポートされていません。

手順

リモート・メディアをマウントまたは移動するには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウから、「**リモート・メディア**」アイコン () をクリックします。

ステップ 2. 次のいずれかの操作をクリックします。

- **リモート・メディアのマウント**

  この操作を実行すると、現在選択されているサーバーでローカル・メディア・リソースを使用できるようになります。1 つのリモート制御ッションで特定のメディア・リソースをマウントできるのは一度に 1 つのサーバーのみです。

  「**リモート・メディアのマウント**」をクリックすると、以下のオプションを選択できるようになります。

  – **マウントするイメージを選択します。**そのイメージは、デバイスをアンマウントするか、リモート制御セッションを閉じるまで、現在選択されているサーバーで使用できます。1 つのサーバーに複数のイメージをマウントすることができ、各イメージを複数のサーバーにマウントすることもできます。

  – **マウントするドライブ (CD、DVD、または USB デバイスなど) を選択します。**そのデバイスは、ドライブをアンマウントするか、リモート制御セッションを閉じるまで、現在選択されているサーバーで使用できます。1 つのサーバーに複数のデバイスをマウントできますが、それぞれのデバイスをマウントできるのは一度に 1 つのサーバーのみです。

    注：ドライブを選択する場合は、ドライブからメディアを取り出す前にドライブをアンマウントしてください。

  – **イメージを IMM にアップロードします。**選択したサーバーの管理コントローラーのローカル・ストレージにイメージを保存するには、このオプションを使用します。そのイメージは、リモート制御セッションを終了したり、サーバーを再起動したりしても、管理コントローラーに残ります。

    管理コントローラーには約 50 MB のデータを保存できます。

    総容量が 50 MB 未満であれば、複数のイメージを管理コントローラーにアップロードできます。

    管理コントローラーにアップロードしたイメージは、自動的にサーバーにマウントされます。管理コントローラーにアップロードしたイメージを別のサーバーの管理コントローラーに移動することもできます。イメージを移動すると、以前にアップロードしたイメージが現在のサーバーから削除されて、選択したサーバーにアップロードされます。

- **リモート・メディアの移動**

  以前にマウントしたメディア・リソースをサーバー間で移動できます。

  リソースをサーバーで使用できるようにするには、以下の手順を実行します。

  1. リソースを 1 つ以上選択します。
  2. 「**追加**」をクリックして、リソースを「**選択済みリソース**」リストに移動します。
  3. 「**マウント**」をクリックして、リソースをサーバーで使用できるようにマウントします。リモート制御セッションによってリソースのデバイスが定義され、現在選択されているサーバーのマウント・ポイントにマップされます。マウントされたメディアを書き込み保護することもできます。

サーバーへのイメージのアップロード

選択したサーバーのベースボード管理コントローラー (BMC) で使用できるローカル・ストレージにイメージをアップロードすることもできます。

このタスクについて

そのイメージは、リモート制御セッションを終了したり、サーバーを再起動したりしても、管理コントローラーに残ります。

管理コントローラーには約 50 MB のデータを保存できます。

総容量が 50 MB 未満であれば、複数のイメージを管理コントローラーにアップロードできます。

管理コントローラーにアップロードしたイメージは、自動的にサーバーにマウントされます。管理コントローラーにアップロードしたイメージを別のサーバーの管理コントローラーに移動することもできます。イメージを移動すると、以前にアップロードしたイメージが現在のサーバーから削除されて、選択したサーバーにアップロードされます。

手順

イメージをサーバーにアップロードするには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウから、「**リモート・メディア**」アイコン () をクリックします。

ステップ 2. 「**リモート・メディアのマウント**」をクリックします。

ステップ 3. 「**IMM にイメージをアップロードする**」をクリックします。

ユーザー設定のインポートとエクスポート

現在のリモート制御セッションのユーザー設定をインポートまたはエクスポートできます。

このタスクについて

ユーザー設定をエクスポートすると、現在のリモート制御セッションすべてのユーザー設定がローカル・システムのプロパティ・ファイルに保存されます。このプロパティ・ファイルを別のシステムにコピーして、これらの設定をリモート制御アプリケーションにインポートし、設定を使用することができます。

手順

現在のリモート制御セッションのユーザー設定をインポートまたはエクスポートするには、以下の手順を実行します。

ステップ 1. 「リモート制御」ウィンドウから、「**設定**」アイコン () をクリックします。

ステップ 2. 「**ユーザー設定**」タブをクリックします。

ステップ 3. 「**インポート**」をクリックしてエクスポートされたファイルから設定をインポートするか、「**エクスポート**」をクリックして現在のユーザー設定をすべてローカル・システムのプロパティ・ファイルに保存します。

リモート制御の設定

現在のリモート制御セッションの設定を変更できます。

手順

リモート制御設定を変更するには、以下の手順を実行します。

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

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

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

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

  注：このページのすべての設定をデフォルト設定に復元するには、「**デフォルトの復元**」をクリックします。
  - 「**ツールバーをウィンドウにピン留め**」。デフォルトでは、ツールバーはリモート制御セッション・ウィンドウの上に隠れていて、その上にマウス・ポインターを置いたときにのみ表示されます。このオプションを選択すると、ツールバーがウィンドウに固定され、サムネール・パネルとリモート制御セッション・ウィンドウとの間に常に表示されます。
  - 「**キーボード・ボタンを表示する**」。ツールバーにキーボード・ボタンのアイコン (CapsLock、NumLock、ScrollLock) を表示するかどうかを指定します。
  - 「**電源制御を表示する**」。ツールバーに電源制御オプションを表示するかどうかを指定します。
  - 「**スティッキー・キー・ボタンを表示する**」。ツールバーにスティッキー・キー・ボタンのアイコン (Ctrl、Alt、Delete) を表示するかどうかを指定します。

- 「**ローカル・マウス・ポインターを非表示にする**」。現在ビデオ・セッション領域に表示されているサーバー・セッションにカーソルを置いたときにローカル・マウス・ポインターを表示するかどうかを指定します。
- 「**マウス・キャプチャー・モードの有効化**」。デフォルトでは、マウス・キャプチャー・モードは無効になっています。そのため、カーソルをビデオ・セッション領域の内外に自由に移動できます。マウス・キャプチャー・モードを有効にすると、左 Alt キーを押さないとカーソルをビデオ・セッション領域の外に移動できなくなります。マウス・キャプチャー・モードが有効になっている場合は、Ctrl+Alt キーを使用してマウス・キャプチャー・モードを終了するかどうかを指定できます。デフォルトでは左 Alt キーを使用します。
- 「**ツールバーの背景の不透明度を指定**」。不透明度を下げると、ツールバーの背景越しにビデオ・セッション領域が表示されるようになります。

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

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

リモート制御ログとトレースの表示

リモート制御セッションを開始すると、ログ・ファイルが作成されます。これらのファイルに記録されるイベントのタイプは、デバッグ・モードによって決まります。デバッグ・モードは、「設定」ダイアログの「**全般**」タブで設定します。これらのログ・ファイルを使用して問題を解決できます。

手順

リモート制御ログ・ファイルは以下の場所に保存されます。

オペレーティング・システム	ログ・ディレクトリ

Windows 7 および 8	`%USERPROFILE%\lenovo\remoteaccess`
	たとえば、次のような場合です。
	`C:\Users\win_user\lenovo\remoteaccess`

診断ファイルを収集し、ファイルを Lenovo サポート に送信する方法については、Lenovo XClarity Administrator オンライン・ドキュメントのサービスおよびサポートの操作を参照してください。

管理対象サーバーのオペレーティング・システムへのアクセスの管理

管理対象サーバーのオペレーティング・システムへのアクセスを管理できます。

始める前に

デバイス・ドライバーの管理とデプロイ、および「Windows ドライバー更新」ページからの管理対象サーバーの電源操作の実行には、**lxc-os-admin**、**lxc-supervisor**、**lxc-admin** または **lxc-hw-admin** 権限が必要です。

このタスクについて

Lenovo XClarity Administrator が管理対象システムの OS デバイス・ドライバーを更新するには、OS IP アドレスや保存された管理者の資格情報など、ホスト・オペレーティング・システムにアクセスするための情報を指定する必要があります。OS デバイス・ドライバーの更新について詳しくは、管理対象サーバーの Windows デバイス・ドライバーの更新を参照してください。

XClarity Administrator は保存された資格情報を使用してホスト・オペレーティング・システムに対して認証します。XClarity Administrator での保存された資格情報の作成について詳しくは、保存された資格情報の管理を参照してください。

ヒント: XClarity Administrator はこのページで指定された情報を自動的に検証しません。

手順

以下の手順を実行して、オペレーティング・システム・プロパティを変更します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS アクセスの管理**」をクリックして、「OS アクセスの管理」ページを表示します。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. 更新するサーバーを選択します。

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

ステップ 4. ターゲット・サーバーごとに、以下の情報を指定します。
- ホスト・オペレーティング・システムの IP アドレスまたはホスト名
- (オプション) ホスト・オペレーティング・システムにアクセスするための保存された資格情報
- (オプション) ホスト・オペレーティング・システムの説明

ステップ 5. 「**保存**」をクリックします。

終了後

オペレーティング・システムのアクセス管理では次のアクションを実行できます。

- オペレーティング・システム情報 (IP アドレス、資格情報および説明) をクリアする。サーバーを選択して、「**OS 情報を削除する**」アイコン ( ) をクリックします。
- Windows サーバーで認証をテストする。「**プロビジョニング**」 → 「**Windows ドライバー更新: 適用**」をクリックし、ターゲット・サーバーを選択して、「**認証の確認**」をクリックします。
- サーバー名の上にカーソルを合わせることによって、特定のサーバーのオペレーティング・システムのデプロイメント情報を表示します。

  注：デプロイメント情報は、XClarity Administratorインスタンスによって正常にデプロイされたオペレーティング・システムでのみ使用できます。デプロイメント情報は、失敗したデプロイメントおよび他の方法 (別の XClarity Administrator のインスタンスを含む) によって実行されたデプロイメントには使用できません。

Features on Demand キーの表示

現在管理対象サーバーにインストールされている Features on Demand キーのリストを表示できます。

このタスクについて

Lenovo XClarity Administrator Web インターフェースで Features on Demand キーを購入、インストール、管理することはできません。Features on Demand キーの入手とインストールについては、XClarity Administrator オンライン・ドキュメントのFeatures on Demandを参照してください。

手順

特定の管理対象サーバーにインストールされている FoD キーのリストを表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニューで、「**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・サーバーおよびタワー・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。

ステップ 2. 「**サーバー**」列でサーバー名をクリックします。そのサーバーのステータス要約ページが開いて、サーバーのプロパティと、そのサーバーに取り付けられたコンポーネントのリストが表示されます。

ステップ 3. 左側のナビゲーションで、「全般」の「**インベントリー詳細**」をクリックし、各ハードウェア・コンポーネント・セクションを展開して、それらのコンポーネントの FoD 固有 ID を表示します。

ステップ 4. 左側のナビゲーションで、「構成」の「**Features on Demand キー**」をクリックして、そのサーバーにインストールされているすべての FoD キーに関する情報を表示します。

エネルギーおよび温度の管理

コンバージド、NeXtScale、System x、および ThinkServer サーバーの電力使用量と温度をモニターおよび管理して、Lenovo XClarity Energy Manager を使用するとエネルギー効率が向上します。

詳細: Lenovo XClarity Energy Manager

このタスクについて

XClarity Administrator は、サポートするサーバーの電力消費量と温度をモニターおよび管理できるスタンドアロン ユーザー・インターフェースで、以下を含みます:

- エネルギー使用量の監視、電源の要求の見積もり、および必要に応じてサーバーに電源を再割り振りすること。
- サーバーの温度、および冷却能力の監視。
- 特定のイベントが発生、またはしきい値を超えた時に通知を送信。
- ポリシーを使用してデバイスが消費する電力の量の制限。

- リアルタイムの吸気温度の監視、アウト・オブ・バンド電源データに基づく低使用サーバーの識別、異なるサーバー・モデルの電源レーンジャーの測定、リソースの可用性に基づいて新規ワークロードに適合する方法を評価し、エネルギー効率を最適化。
- 電源イベントの緊急時 (データ・センターの電源障害など) に、電力使用量を最小レベルにしサービス時間を拡張。

XClarity Administrator をダウンロードして使用する方法については、Lenovo XClarity Energy Manager Web サイト を参照してください。

サーバーの電源のオン/オフ

Lenovo XClarity Administrator からサーバーの電源オン/電源オフを実行できます。

始める前に

- 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。XClarity Administrator から「**通常の再起動**」または「**今すぐ再起動**」操作を実行する前に、オペレーティング・システムを手動で構成して電源ボタンの動作を電源オフに変更する必要があります。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。
- SUSE Linux Enterprise Server (SLES) の場合、オペレーティング・システムの電源遮断は、SLES セッションで root パスワードを入力する必要があります。XClarity Administrator で「**通常の電源オフ**」または「**今すぐ電源オフ**」操作を実行する前に、ローカル SLES インターフェースを使用して手動でサーバーの電源をオフにする必要があり、パスワードを入力する時に「**ユーザー認証を忘れないでください**」オプションを選択する必要があります。または、必要な認証を無効にすることができるどうかセキュリティー・ポリシーを確認します。
- 有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。
- 電源操作「**システム・セットアップから再起動**」は、サーバーを再起動して、通常のオペレーティング・システム・ブートではなく、リモート制御セッションの BIOS/UEFI スタートアップ・ユーティリティを開きます。
- 電源操作「**通常の電源オフ**」および「**今すぐ電源オフ**」は、デバイスにインストールされているオペレーティング・システムの構成によって異なり、オペレーティング・システムがサポートするよう構成されている場合にのみ作動します。
- 「**すべての操作**」 → 「**サービス**」 → 「**NMI を発生させる**」をクリックすることで、マスク不可割り込み (NMI) を使用してデバイスを再起動できます。

手順

サーバーの電源をオンまたはオフにするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニューで、「**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。

ステップ 2. サーバーを選択します。

ステップ 3. 「**すべての操作**」 → 「**電源操作**」をクリックし、次のいずれかの電源操作をクリックします。
- **電源オン**は、デバイスの電源をオンにします。
- **通常の電源オフ**は、オペレーティング・システムをシャットダウンしてデバイスの電源をオフにします。
- **今すぐ電源オフ**は、デバイスの電源をオフにします。
- **通常の再起動**は、オペレーティング・システムをシャットダウンしてデバイスを再起動します。
- **今すぐ再起動**は、デバイスを再起動します。

- **システム・セットアップから再起動**は、デバイスを BIOS/UEFI (F1) セットアップに再起動します。ThinkServer 以外の制限なしでサポートされているサーバーでサポートされています。
- **管理コントローラー**は、BMC を再起動します。
- 「**今すぐ再起動して PXE ブートを実行**」は、サーバーを即時に再起動して Preboot Execution Environment (PXE) ネットワークにブートします。Lenovo Flex System、System x、および ThinkSystem サーバーでサポートされています。

  注：PXE ブートに関連する UEFI 設定がサーバーで構成されている必要があります。

Flex System シャーシのサーバーの仮想再取り付け

マスク不可割り込み (NMI) を使用してサーバーを再起動して、Flex System シャーシでのサーバーの取り外しと再挿入をシミュレートできます。

このタスクについて

仮想再取り付けの間に、サーバーに対する既存のネットワーク接続がすべて失われ、サーバーの電源状態が変更されます。仮想再取り付けを実行する前に、すべてのユーザー・データが保存されていることを確認してください。

注意：

- Lenovo サポート からの指示がない限り、仮想再取り付けを実行しないでください。
- 仮想再取り付けを実行すると、データが失われる可能性があります。サーバーの再取り付けを実行する前に、必要な操作を実行してユーザー・データを保護してください。
- 仮想再取り付けを実行する代わりにサーバーの電源をオフにすることを検討してください。電源操作については、サーバーの電源のオン/オフを参照してください。

手順

Flex System シャーシのサーバーの仮想再取り付けを行うには、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、「**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がテーブル・ビューで表示されます。

テーブルの列をソートすると、再取り付けするサーバーを見つけやすくなります。「**すべてのデバイス**」ドロップダウン・リストでデバイス・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. テーブルでサーバーを選択します。

ステップ 3. 「**すべての操作**」 → 「**サービス**」 → 「**仮想再取り付け**」の順にクリックします。

ステップ 4. 「**仮想再取り付け**」をクリックします。

サーバーの管理コントローラー・インターフェースの起動

Lenovo XClarity Administrator から特定のサーバーの管理コントローラー Web インターフェースを起動できます。

始める前に

XClarity Administratorを介して ThinkSystem SR635 SR655 サーバーにアクセスするには、ユーザーに **lxc-supervisor**、**lxc-sysmgr**、**lxc-admin**、**lxc-fw-admin** または **lxc-os-admin** の権限を付与してください (認証サーバーの管理 を参照)。

シングル・サインオンを使用する場合は、ログインせずに XClarity Administrator から管理対象サーバーの管理インターフェースを起動することができます。シングル・サインオンは ThinkSystem および ThinkAgile サーバー (SR635 および SR655 を除く) でサポートされています。ThinkSystem SR645 および SR665 サーバーでは、XCC ファームウェア 21A 以降が必要です。

XClarity Administrator にログインせずに、ローカルまたは外部の LDAP ユーザー・アカウントを使用して管理コントローラーに直接ログインする場合は、 URL `https://{XCC_IP_adderss}/#/login` を使用してください。

手順

サーバーの管理コントローラー・インターフェースを起動するには、以下の手順を実行します。

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

ステップ 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」ページを表示します。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. 「**サーバー**」列のサーバーのリンクをクリックします。そのサーバーのステータスの要約ページが表示されます。

ステップ 3. 「**すべての操作**」 ➡ 「**起動**」 ➡ 「**管理 Web インターフェース**」をクリックします。サーバーの管理コントローラー Web インターフェースが起動します。

ヒント: 「**IP アドレス**」列の IP アドレスをクリックして、管理コントローラー・インターフェースを起動することもできます。

ステップ 4. XClarity Administrator ユーザー資格情報を使用して管理コントローラー・インターフェースにログインします。

終了後

サーバーの管理コントローラー・インターフェースの使用について詳しくは、Integrated Management Module II オンライン・ドキュメントおよびXClarity Controller オンライン・ドキュメントを参照してください。

サーバーのシステム・プロパティの変更

特定のサーバーのシステム・プロパティを変更できます。

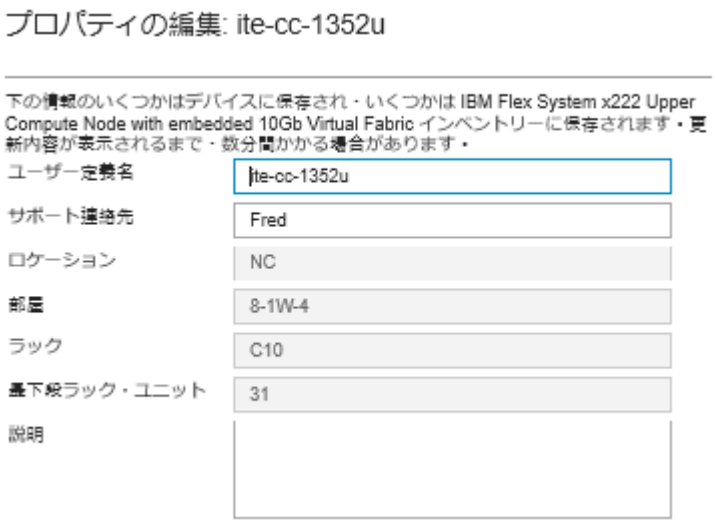
手順

以下の手順を実行して、システム・プロパティを変更します。

ステップ 1. Lenovo 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」ページを表示します。

ステップ 2. 更新するサーバーを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックし、「編集」ダイアログを表示します。



ステップ 4. 以下の情報を必要に応じて変更します。
- サーバーのユーザー定義名
- サポート連絡先
- 説明

注：Web インターフェースのラックからデバイスを追加または削除する場合は、ロケーション、設置部屋、ラック、最下段ラック・ユニットのプロパティが XClarity Administrator によって更新されます (ラックの管理を参照)。

ステップ 5. 「**保存**」をクリックします。

注：変更されたプロパティが XClarity Administrator Web インターフェースに表示されるまで少し時間がかかる場合があります。

サーバーの有効期限切れまたは無効の保存された資格情報の解決

保存された資格情報が期限切れまたはデバイスで動作しない場合、そのデバイスのステータスは「オフライン」と表示されます。

手順

サーバーの有効期限切れまたは無効の保存された資格情報を解決するには

ステップ 1. Lenovo 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。

ステップ 2. テーブル上部で「**電源**」テーブル列の見出しをクリックして、すべてのオフライン・サーバーをグループにします。

「すべてのシステム」ドロップダウン・リストでシステム・タイプを選択し、「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 3. 解決するサーバーを選択します。

ステップ 4. 「**すべての操作**」 ➔ 「**セキュリティー**」 ➔ 「**保存された資格情報を編集**」をクリックします。

ステップ 5. 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。

注：同じ保存された資格情報を使用して複数のデバイスを管理しており、その保存された資格情報のパスワードを変更する場合、パスワードの変更は現在その保存された資格情報を使用しているすべてのデバイスに影響します。

サーバー・パターン・デプロイ後の障害の発生したサーバーのリカバリー

サーバー・パターンをデプロイした後でサーバーで障害が発生した場合にサーバーをリカバリーするには、そのサーバーからプロファイルの割り当てを解除して、そのプロファイルをスタンバイ・サーバーに再割り当てします。

手順

Lenovo XClarity Administrator 管理対象認証を使用する障害の発生したサーバーをリカバリーするには、サーバーの管理をリカバリーするのには、以下の手順を実行します。

ステップ 1. 障害の発生したサーバーを特定します。

ステップ 2. 障害の発生したサーバーからサーバー・プロファイルの割り当てを解除します (サーバー・プロファイルの非アクティブ化を参照してください)。

注意：プロファイルを再割り当てする*前に*、障害の発生したサーバーの電源をオフにして、割り当てられた仮想アドレスを非アクティブ化する必要があります。サーバー・プロファイルの割り当てを解除する際に、「サーバー・プロファイルの割り当て解除」ダイアログで「**サーバーの電源オフ**」を選択して、障害の発生したサーバーの電源をオフにします (サーバーの電源のオン/オフを参照してください)。

ステップ 3. そのサーバー・プロファイルをスタンバイ・サーバーに割り当てます (サーバー・プロファイルのアクティブ化を参照してください)。

ステップ 4. プロファイルをアクティブにします。現在スタンバイ・サーバーの電源がオフの場合は電源をオンにし、オンの場合は再起動します (サーバーの電源のオン/オフを参照)。

ステップ 5. 接続されているスイッチの VLAN 設定をスタンバイ・サーバーに移行します。

ステップ 6. 障害の発生したサーバーの電源がオフになっていることを確認します。

ステップ 7. 障害の発生したサーバーを交換するか修理します。修理する場合は、以下の手順を実行して、新たに修理したサーバーをデフォルト設定にリセットします。

a. サーバーの管理 Web インターフェースを使用して、BMC を工場出荷時の状態にリセットします。BMC のリセットについては、管理サーバーの障害後の管理コントローラー・リセットによる ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理のリカバリーを参照してください。

b. Unified Extensible Firmware Interface (UEFI) のメニューを使用して、I/O アダプター仮想アドレスを含む UEFI の情報をクリアします。詳しくは、UEFI のマニュアルを参照してください。

サーバー・パターンのデプロイ後のブート設定のリカバリー

新しいサーバー・パターンをデプロイした後に起動しなくなったサーバーがある場合は、ブート設定がサーバー・パターンのデフォルトのブート設定で上書きされたことが原因と考えられます。UEFI モードでインストールされたオペレーティング・システムの場合、デフォルト設定を復元すると、追加の構成手順を実行してブート構成を復元する必要が生じることがあります。

手順

元のブート設定を復元するには、影響を受けた各サーバーで以下の手動リカバリーの手順を実行します。

- Red Hat Enterprise Linux がインストールされているサーバーの場合:
  1. サーバーにリモート・アクセスしている場合はリモート制御セッションを確立します (リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理を参照)。
  2. 「**ツール**」 → 「**電源**」 → 「**オン**」の順にクリックして、サーバーを再起動します。リモート制御セッションにサーバーの UEFI スプラッシュ画面が表示されたら、F1 キーを押します。Setup Utility が表示されます。
  3. 「**Boot Manager**」を選択します。
  4. 「**Add Boot Option**」を選択します。
  5. 「**UEFI Full Path Option**」を選択します。
  6. 表示されるリストで、`SAS` を含む項目を選択します。
  7. 「**EFI**」を選択します。
  8. 「**redhat**」を選択します。
  9. 「**grub.efi**」を選択します。
  10. 「**Input the Description**」フィールドを選択します。
  11. 「`Red Hat Enterprise Linux`」と入力します。
  12. 「**Commit Changes**」を選択します。
  13. `Red Hat Enterprise Linux` を Boot Order 内の最初のオプションにし、Boot Order 内の他のオプションをすべて削除します。
  14. Esc キーを押し、「**変更を保存してこのメニューを終了します**」を選択します。
  15. Esc キーを押し、「**Exit the Configuration Utility and Reboot**」を選択します。計算ノードが再起動します。

- Microsoft Windows Server 2008 がインストールされているサーバーの場合:
  1. サーバーの電源をオンにして、プロンプトが表示されたら F1 キーを押してセットアップに入ります。
  2. 「**Boot Manager**」を選択します。
  3. 「**Boot from File**」を選択します。
  4. Microsoft Windows Server 2008 をインストールした GUID パーティション・テーブル (GPT) システム・パーティションを選択します。
  5. 「**EFI**」を選択します。
  6. 「**Microsoft**」を選択します。
  7. 「**Boot**」を選択します。
  8. 「**bootmgfw.EFI**」を選択します。

  注：詳しくは、RETAIN tip 5079636を参照してください。

管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー

ラックまたはタワー・サーバーが Lenovo XClarity Administrator の管理対象になっているときに、XClarity Administrator に障害が発生した場合は、XClarity Administrator の復元または交換を待たずに、管理機能を復元できます。

このタスクについて

Flex System サーバーの管理をリカバリーするには、管理サーバーの障害発生後の CMM による管理のリカバリー を参照してください。

管理の強制を使用した管理サーバーの障害後のラックまたはタワー・サーバー管理のリカバリー

管理の強制オプションを使用してサーバーを再度管理することで、サーバー管理をリカバリーできます。

手順

交換する Lenovo XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、`RECOVERY_ID` アカウントとパスワード、および「**管理の強制**」オプションを使用してデバイスを再度管理できます (サーバーの管理を参照)。

管理コントローラーを使用した、正しく管理解除されなかった System x または NeXtScale M4 サーバーのリカバリー

ベースボード管理コントローラー (BMC) を使用することにより、System x または NeXtScale M4 サーバーの管理をリカバリーできます。

手順

サーバー管理 (Lenovo XClarity Administrator 管理対象認証を使用するサーバーの) をリカバリーするには、以下の手順を実行します。

ステップ 1. サーバーが XClarity Administrator の管理対象となる前に作成したユーザー・アカウントとパスワードを使用して、管理コントローラー Web インターフェースにログインします。

ステップ 2. すべての SNMP トラップ設定
   a. 「**IMM 管理**」 → 「**ネットワーク**」をクリックします。
   b. 「**SNMP**」タブをクリックします。

c. 「**コミュニティー (Communities)**」タブをクリックします。

d. たとえば、前の XClarity Administrator のコミュニティー・エントリーを見つけます。
   - **LXCA IP アドレス**: 10.240.198.84
   - **LXCA ホスト**: LXCA_maqCBIt86d
   - **コミュニティー 2**:
   - **コミュニティー名**: LXCA_maqCBIt86d
   - **アクセス・タイプ**: トラップ
   - **特定のホストにこのコミュニティーでのトラップの受信を許可**: 10.240.198.84

e. コミュニティー・エントリーのフィールドで値を削除します。

f. 「**適用**」をクリックします。

ステップ 3. ユーザー・アカウントをクリアします。

a. 「**IMM 管理**」 → 「**ユーザー**」をクリックします。

b. 「**ユーザー・アカウント**」タブをクリックします。

c. XClarity Administrator であるすべてのユーザー・アカウント (以下の接頭部を持つユーザー・アカウントを含む) を削除します。
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

終了後

XClarity Administrator が復元または交換されると、System x または NeXtScale サーバーをもう一度管理できるようになります (サーバーの管理を参照)。ネットワーク設定、サーバー・ポリシー、ファームウェア・コンプライアンス・ポリシーなど、サーバーに関するすべての情報が保持されます。

管理サーバーの障害後の管理コントローラー・リセットによる ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理のリカバリー

サーバーのベースボード管理コントローラーを出荷時のデフォルト値にリセットすることにより、ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバーの管理をリカバリーできます。

手順

サーバー管理 (Lenovo XClarity Administrator 管理対象認証を使用するサーバーの) をリカバリーするには、以下の手順を実行します。

ステップ 1. デバイスで Encapsulation が有効である場合は、障害が発生した 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管理コントローラーに接続します。

ステップ 2. 障害の発生したサーバーの管理コントローラーを工場出荷時の状態にリセットします。

a. サーバーが XClarity Administrator の管理対象となる前に作成したリカバリー・ユーザー・アカウントとパスワードを使用して、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します。

b. 「**IMM 管理**」タブをクリックします。

c. 「**IMM を工場出荷時の状態にリセットする**」をクリックします。

d. 「**OK**」をクリックしてリセット操作を確認します。

重要：BMC 構成が完了した後、BMC は再起動されます。これがローカル・サーバーである場合は、TCP/IP 接続が破壊されるので、接続をリストアするためにネットワーク・インターフェースを再構成する必要があります。

ステップ 3. サーバーの管理コントローラー Web インターフェースに再度ログオンします。

- BMC は、DHCP サーバーから IP アドレスの取得を試みるように初期構成されます。取得できない場合、IMM は静的 IPv4 アドレス `192.168.70.125` 使用します。
- IMMBMC の初期設定では、ユーザー名は `USERID`、パスワードは `PASSWORD` (文字の O ではなくゼロ) になっています。このデフォルトのユーザー・アカウント・では、Supervisor アクセス権があります。拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。

ステップ 4. 接続をリストアするために、ネットワーク・インターフェースを再構成します。詳しくは、Integrated Management Module II オンライン・ドキュメント を参照してください。

終了後

XClarity Administrator が復元または交換されると、サーバーをもう一度管理できるようになります (サーバーの管理を参照)。ネットワーク設定、サーバー・ポリシー、ファームウェア・コンプライアンス・ポリシーなど、サーバーに関するすべての情報が保持されます。

サーバーが 構成パターン を使用して構成されている場合、サーバーに割り当てられているサーバー・プロファイルを非アクティブ化してから再アクティブ化することにより、構成を適用できます (サーバー・プロファイルの使用を参照)。

管理サーバーの障害後の cimcli を使用した ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理のリカバリー

`cimcli` ユーティリティーを使用して CIM サブスクリプションをクリアすることにより、ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理をリカバリーできます。

始める前に

ターゲット・サーバーにネットワーク・アクセスできるシステムに OpenPegasus が cimcli ユーティリティーを使用してインストールされている必要があります。OpenPegasus のダウンロード、構成、およびコンパイルについては、Linux 用 OpenPegasus Release RPM Web サイトを参照してください。

注：Red Hat Enterprise Linux (RHEL) Server 7 以降では、OpenPegasus のソースおよびバイナリー RPM が、Red Hat ディストリビューションの一部として含まれています。`top-pegasus-test.x86_64` パッケージに cimcli ユーティリティーが含まれています。

このタスクについて

サーバーが復元されると、サーバーをもう一度管理できるようになります。ネットワーク設定、サーバー・ポリシー、ファームウェア・コンプライアンス・ポリシーなど、サーバーに関するすべての情報が保持されます。

手順

サーバー管理をリカバリーするには、Lenovo XClarity Administrator 管理対象認証を使用し、OpenPegasus がインストールされているサーバーから以下の手順を実行します。

ステップ 1. Encapsulation がデバイス上で有効である場合:

a. 障害が発生した 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。

b. 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
```

ステップ 2. 次のコマンドを実行して、CIM_ListenerDestinationCIMXML、CIM_Indicationfilter、および CIM_IndicationSubscription に対する CIM インスタンスを特定します。

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_IndicationSubscription
```

<IP_address>、*<user_ID>*、および *<password>* は、管理コントローラーの IP アドレス、ユーザー ID、パスワードです。例:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

ステップ 3. 次のコマンドを実行して、CIM_ListenerDestinationCIMXML、CIM_Indicationfilter、および CIM_IndicationSubscription の CIM インスタンスを、一度に 1 つずつ削除します。

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s di '<cim_instance>'
```

<IP_address>、*<user_ID>*、および *<password>* は管理コントローラーの IP アドレス、ユーザー ID、パスワードであり、*<cim_instance>* は前のステップで各 CIM インスタンスに返された情報を単一引用符で囲んだものです。例:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
```

```
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

終了後

Lenovo XClarity Administrator が復元または交換されると、System x または NeXtScale サーバーをもう一度管理できるようになります (サーバーの管理を参照)。ネットワーク設定、サーバー・ポリシー、ファームウェア・コンプライアンス・ポリシーなど、サーバーに関するすべての情報が保持されます。

管理サーバーの障害後の管理コントローラー・インターフェースを使用した ThinkServer サーバー管理のリカバリー

管理コントローラー・インターフェースから ThinkServer サーバーの管理をリカバリーできます。

手順

サーバーの管理をリカバリーするには、以下の手順を実行します。

ステップ 1. サーバーの管理コントローラー Web インターフェースに管理者としてログオンします (サーバーの管理コントローラー・インターフェースの起動を参照)。

ステップ 2. メイン・メニューでユーザーを選択して Lenovo XClarity Administrator が作成した IPMI アカウントを削除し、プレフィックス「LXCA_」がつくすべてのユーザー・アカウントを削除します。

また、アカウント・ユーザー名を名前変更してプレフィックス「LXCA_」を削除することもできます。

ステップ 3. メイン・メニューで「**PEF 管理**」を選択して SNMP トラップ宛先を削除し、「**LAN 宛先**」タブをクリックして、XClarity Administrator の IP アドレスをポイントする項目を削除します。

ステップ 4. メイン・メニューで「**NTP 設定**」を選択して有効な NTP 設定があることを確認し、手動で日付と時刻を構成するか、有効な NTP サーバー・アドレスを指定してください。

ラック・サーバーまたはタワー・サーバーの管理解除

ラック・サーバーまたはタワー・サーバーを Lenovo XClarity Administrator の管理対象から除外できます。このプロセスは*管理解除*と呼ばれます。

始める前に

XClarity Administrator を有効にすると、一定期間オフラインになっているデバイスを管理対象から自動的に解除できます。これはデフォルトで無効になっています。オフライン・デバイスの自動管理解除を有効にするには、XClarity Administrator メニューから「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックし、「**管理除外オフライン・デバイスが無効**」の横の「**編集**」をクリックします。次に、「**管理除外オフライン・デバイスの有効化**」を選択し、時間間隔を設定します。デフォルトでは、デバイスは 24 時間オフラインになった後、管理解除されます。

ラック・サーバーまたはタワー・サーバーを管理解除する前に、そのサーバーに対して実行されているアクティブなジョブがないことを確認します。

サーバー・パターンとラック・サーバーまたはタワー・サーバー上の任意の仮想アドレスを削除する場合、サーバーを管理解除する前にサーバー・プロファイルを非アクティブ化します (サーバー・プロファイルの非アクティブ化を参照)。

XClarity Administratorでコール・ホームが有効になっている場合、重複する問題レコードが作成されないようにするため、すべての管理対象シャーシとサーバーでコール・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、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 (XClarity Administrator オンライン・ドキュメントの 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)。

このタスクについて

ラック・サーバーまたはタワー・サーバーを管理解除すると、Lenovo XClarity Administrator では以下の処理が実行されます。

- 集中型ユーザー管理に使用されている構成をクリアする。
- XClarity Administrator 信頼ストアからベースボード管理コントローラー・セキュリティー証明書を削除する。
- デバイスで Encapsulation が有効である場合は、デバイスが管理される前に、設定にデバイスのファイアウォール規則を構成する。
- XClarity Administrator 構成への CIM サブスクリプションを削除する。これにより、XClarity Administrator はそのラック・サーバーまたはタワー・サーバーからイベントを受信しなくなります。
- コール・ホーム が現在 XClarity Administrator で有効になっている場合、コール・ホーム がラック・サーバーまたはタワー・サーバーで無効になります。
- ラック・サーバーまたはタワー・サーバーから送信されたイベントは破棄されます。イベントを保持するには、syslog などの外部リポジトリーにイベントを転送します (イベントの転送を参照)。

ラック・サーバーまたはタワー・サーバーを管理解除しても、XClarity Administrator にはサーバーに関する特定の情報が保持されます。この情報は、そのラック・サーバーまたはタワー・サーバーの管理を再開したときに再適用されます。

重要：ThinkServer サーバーを管理解除した後、そのサーバーを別の XClarity Administrator インスタンスを使用して管理する場合、そのサーバーに関する情報は失われます。

ヒント: 初期セットアップ中にオプションで追加されたすべてのデモ・デバイスは、シャーシ内のノードです。デモ・デバイスを管理対象から除外するには、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」オプションを使用してシャーシを管理対象から除外します。

手順

ラック・サーバーまたはタワー・サーバーを管理解除するには、以下の手順を実行します。

ステップ 1. XClarity 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」ページを表示します。

ステップ 2. 管理解除するラック・サーバーまたはタワー・サーバーを 1 つ以上選択します。

ステップ 3. 「**非管理**」をクリックします。「管理対象から除外」ダイアログが表示されます。

ステップ 4. **オプション**: 「**デバイスに到達できない場合であっても、管理対象からの除外を強制します**」を選択します。

重要：デモ・ハードウェアを管理解除する場合は、このオプションを選択してください。

ステップ 5. 「**非管理**」をクリックします。
「管理対象から除外」ダイアログには、管理解除プロセスの各ステップの進行状況が表示されます。

ステップ 6. 管理解除プロセスが完了したら、「OK」をクリックします。

正しく管理解除されなかったラックまたはタワー・サーバーのリカバリー

コンバージド、NeXtScale、System x、または ThinkServer サーバーが正しく管理解除されなかった場合、再管理する前にサーバーをリカバリーする必要があります。

管理の強制を使用した正しく管理解除されなかったラックまたはタワー・サーバーのリカバリー

管理の強制オプションを使用してサーバーを再度管理することで、サーバー管理をリカバリーできます。

手順

交換する Lenovo XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、`RECOVERY_ID` アカウントとパスワード、および「**管理の強制**」オプションを使用してデバイスを再度管理できます (サーバーの管理を参照)。

管理コントローラーを使用した、正しく管理解除されなかった System x または NeXtScale M4 サーバーのリカバリー

管理コントローラーを使用することにより、System x または NeXtScale M4 サーバー管理をリカバリーできます。

手順

サーバーの管理をリカバリーするには、以下の手順を実行します。

ステップ 1. サーバーが XClarity Administrator の管理対象となる前に作成したユーザー・アカウントとパスワードを使用して、管理コントローラー Web インターフェースにログインします。

ステップ 2. すべての SNMP トラップ設定

a. 「**IMM 管理**」 → 「**ネットワーク**」をクリックします。

b. 「SNMP」タブをクリックします。

c. 「**コミュニティー (Communities)**」タブをクリックします。

d. たとえば、前の XClarity Administrator のコミュニティー・エントリーを見つけます。
- **LXCA IP アドレス**: 10.240.198.84
- **LXCA ホスト**: LXCA_maqCBIt86d
- **コミュニティー 2**:
- **コミュニティー名**: LXCA_maqCBIt86d
- **アクセス・タイプ**: トラップ
- **特定のホストにこのコミュニティーでのトラップの受信を許可**: 10.240.198.84

e. コミュニティー・エントリーのフィールドで値を削除します。

f. 「**適用**」をクリックします。

ステップ 3. ユーザー・アカウントをクリアします。

a. 「**IMM 管理**」 → 「**ユーザー**」をクリックします。

b. 「**ユーザー・アカウント**」タブをクリックします。

c. XClarity Administrator であるすべてのユーザー・アカウント (以下の接頭部を持つユーザー・アカウントを含む) を削除します。
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

ステップ 4. Lenovo XClarity Administrator を使用してサーバーを管理します。

a. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。

b. 「**手動で入力**」を選択します。

c. 「**単一システム**」をクリックし、管理するサーバーの IP アドレスを入力して、「OK」クリックします。

d. サーバーへの認証に使用されるユーザー ID とパスワードを指定します。

e. 「**管理**」をクリックします。

ダイアログが開き、この管理プロセスの進行状況が表示されます。進行状況を監視して、プロセスが正常に完了することを確認します。

f. プロセスが完了したら、「OK」をクリックします。

管理コントローラーを工場出荷時の状態にリセットすることによる、正しく管理解除されなかった ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバーのリカバリー

サーバーのベースボード管理コントローラー (BMC) を出荷時のデフォルト値にリセットすることにより、ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバー管理をリカバリーできます。

手順

サーバーの管理をリカバリーするには、以下の手順を実行します。

ステップ 1. デバイスで Encapsulation が有効である場合は、障害が発生した 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管理コントローラーに接続します。

ステップ 2. 障害の発生したサーバーの管理コントローラーを工場出荷時の状態にリセットします。

a. サーバーが XClarity Administrator の管理対象となる前に作成したリカバリー・ユーザー・アカウントとパスワードを使用して、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します。

b. 「**IMM 管理**」タブをクリックします。

c. 「**IMM を工場出荷時の状態にリセットする**」をクリックします。

d. 「OK」をクリックしてリセット操作を確認します。

重要：BMC 構成が完了した後、BMC は再起動されます。これがローカル・サーバーである場合は、TCP/IP 接続が破壊されるので、接続をリストアするためにネットワーク・インターフェースを再構成する必要があります。

ステップ 3. サーバーの管理コントローラー Web インターフェースに再度ログオンします。

- BMC は、DHCP サーバーから IP アドレスの取得を試みるように初期構成されます。取得できない場合、IMM は静的 IPv4 アドレス `192.168.70.125` 使用します。
- IMMBMC の初期設定では、ユーザー名は `USERID`、パスワードは `PASSWORD` (文字の O ではなくゼロ) になっています。このデフォルトのユーザー・アカウント・では、Supervisor アクセス権があります。拡張セキュリティーを使用するには、初期構成時にこのユーザー名とパスワードを変更してください。

ステップ 4. 接続をリストアするために、ネットワーク・インターフェースを再構成します。詳しくは、Integrated Management Module II オンライン・ドキュメント を参照してください。

ステップ 5. Lenovo XClarity Administrator を使用してサーバーを管理します。

a. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。

b. 「**手動で入力**」を選択します。

c. 「**単一システム**」をクリックし、管理するサーバーの IP アドレスを入力して、「OK」クリックします。

d. サーバーへの認証に使用されるユーザー ID とパスワードを指定します。
e. 「**管理**」をクリックします。

   ダイアログが開き、この管理プロセスの進行状況が表示されます。進行状況を監視して、プロセスが正常に完了することを確認します。
f. プロセスが完了したら、「**OK**」をクリックします。

ステップ 6. サーバーが構成パターンを使用して構成されていた場合は、サーバーに割り当てられていたサーバー・プロファイルを再アクティブ化します。

a. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**サーバー・プロファイル**」の順にクリックします。「構成パターン: サーバー・プロファイル」ページが表示されます。
b. サーバー・プロファイルを選択し、「**サーバー・プロファイルの非アクティブ化**」アイコン () をクリックします。
c. 「**ITE の電源をオフ**」をクリックして、サーバーの電源をオフにします。サーバーの電源が再びオンになったときに、仮想アドレスの割り当てが出荷時のデフォルト設定に戻されます。
d. 「**非アクティブ化**」をクリックします。「プロファイルのステータス」列でプロファイルの状態が「非アクティブ」に変わります。注: プロファイルを非アクティブ化してもサーバーの識別情報 (ホスト名、IP アドレス、仮想 MAC アドレスなど) は維持されます。
e. サーバー・プロファイルを再び選択し、「**サーバー・プロファイルのアクティブ化**」アイコン () をクリックします。
f. 「**アクティブにする**」をクリックして、サーバーのサーバー・プロファイルをアクティブにします。「プロファイルのステータス」列でプロファイルの状態が「アクティブ」に変わります。

ステップ 7. コンプライアンス・ポリシーがサーバーに割り当てられていた場合は、コンプライアンス・ポリシーを割り当て直します。

a. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページに管理対象デバイスのリストが表示されます。
b. 「**割り当て済みポリシー**」列のドロップダウン・メニューから、サーバーの適切なポリシーを選択します。

cimcli を使用した、正しく管理解除されなかった ThinkSystem、コンバージド、NeXtScale、または System x M5/M6 サーバーのリカバリー

`cimcli` を使用して CIM サブスクリプションをクリアすることにより、ThinkSystem、コンバージド、NeXtScale、または System x サーバー管理をリカバリーできます。

始める前に

ターゲット・サーバーにネットワーク・アクセスできるシステムに OpenPegasus が cimcli ユーティリティーを使用してインストールされている必要があります。OpenPegasus のダウンロード、構成、およびコンパイルについては、Linux 用 OpenPegasus Release RPM Web サイトを参照してください。

注：Red Hat Enterprise Linux (RHEL) Server 7 以降では、OpenPegasus のソースおよびバイナリー RPM が、Red Hat ディストリビューションの一部として含まれています。`top-pegasus-test.x86_64` パッケージに cimcli ユーティリティーが含まれています。

このタスクについて

サーバーが復元されると、サーバーをもう一度管理できるようになります。ネットワーク設定、サーバー・ポリシー、ファームウェア・コンプライアンス・ポリシーなど、サーバーに関するすべての情報が保持されます。

手順

サーバー管理をリカバリーするには、Lenovo XClarity Administrator 管理対象認証を使用し、OpenPegasus がインストールされているサーバーから以下の手順を実行します。

ステップ 1. Encapsulation がデバイス上で有効である場合:

a. 障害が発生した 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。

b. 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
```

ステップ 2. 次のコマンドを実行して、CIM_ListenerDestinationCIMXML、CIM_Indicationfilter、および CIM_IndicationSubscription に対する CIM インスタンスを特定します。
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s ni CIM_IndicationSubscription
```

<IP_address>、*<user_ID>*、および *<password>* は、管理コントローラーの IP アドレス、ユーザー ID、パスワードです。例:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

ステップ 3. 次のコマンドを実行して、CIM_ListenerDestinationCIMXML、CIM_Indicationfilter、および CIM_IndicationSubscription の CIM インスタンスを、一度に 1 つずつ削除します。
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
    -s di '<cim_instance>'
```

<IP_address>、*<user_ID>*、および *<password>* は管理コントローラーの IP アドレス、ユーザー ID、パスワードであり、*<cim_instance>* は前のステップで各 CIM インスタンスに返された情報を単一引用符で囲んだものです。例:

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

ステップ 4. Lenovo XClarity Administrator を使用してサーバーを管理します。

a. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。

b. 「**手動で入力**」を選択します。

c. 「**単一システム**」をクリックし、管理するサーバーの IP アドレスを入力して、「OK」クリックします。

d. サーバーへの認証に使用されるユーザー ID とパスワードを指定します。

e. 「**管理**」をクリックします。

ダイアログが開き、この管理プロセスの進行状況が表示されます。進行状況を監視して、プロセスが正常に完了することを確認します。

f. プロセスが完了したら、「OK」をクリックします。

管理コントローラー・インターフェースを使用した、正しく管理解除されなかった ThinkServerサーバー管理のリカバリー

管理コントローラー Web インターフェースを使用して ThinkServer サーバーの管理をリカバリーできます。

手順

サーバーの管理をリカバリーするには、以下の手順を実行します。

ステップ 1. サーバーの管理コントローラー Web インターフェースに管理者としてログオンします (サーバーの管理コントローラー・インターフェースの起動を参照)。

ステップ 2. メイン・メニューでユーザーを選択して Lenovo XClarity Administrator が作成した IPMI アカウントを削除し、プレフィックス「LXCA_」がつくすべてのユーザー・アカウントを削除します。

また、アカウント・ユーザー名を名前変更してプレフィックス「LXCA_」を削除することもできます。

ステップ 3. メイン・メニューで「**PEF 管理**」を選択して SNMP トラップ宛先を削除し、「**LAN 宛先**」タブをクリックして、XClarity Administrator の IP アドレスをポイントする項目を削除します。

ステップ 4. メイン・メニューで「**NTP 設定**」を選択して有効な NTP 設定があることを確認し、手動で日付と時刻を構成するか、有効な NTP サーバー・アドレスを指定してください。

第 9 章　ストレージ・デバイスの管理

Lenovo XClarity Administrator では、Lenovo Storage、Flex System ストレージ・システム、テープ・ライブラリーなど、複数のタイプのストレージ・デバイスを管理できます。

詳細:  XClarity Administrator: 検出

始める前に

注意：ストレージ・デバイスを管理する前には、ストレージの管理に関する考慮事項を確認してください。

注：Flex System ストレージ・デバイスは、それらを含むシャーシを管理する際に自動的に検出され管理されます。シャーシとは別に Flex System ストレージ・デバイスを検出、管理することはできません。

特定のポートがデバイスとの通信に使用できる必要があります。ストレージ・デバイスを管理する前に、必要なポートがすべて使用可能になっていることを確認します。ポートについては、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。

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

重要：ラック・ストレージ・デバイスを検出および管理する前に、以下の要件を満たしていることを確認してください (ThinkSystem DE シリーズ以外)。詳しくは、XClarity Administrator オンライン・ドキュメントの デバイスを検出できない、デバイスを管理できない を参照してください。

- ネットワーク構成では、XClarity Administrator とラック・ストレージ・デバイス間の SLP トラフィックを許可する必要があります。
- ユニキャスト SLP が必要です。
- XClarity Administrator が自動的に Lenovo Storage デバイスを検出するには、マルチキャスト SLP が必要です。さらに、ラック・ストレージ・デバイスで SLP を有効にする必要があります。

このタスクについて

XClarity Administrator を使用すると、XClarity Administrator と同じ IP サブネットにある管理可能デバイスのプローブによって、環境内のストレージ・デバイスを自動的に検出できます。他のサブネットにあるストレージ・デバイスを検出するには、IP アドレスまたは IP アドレス範囲を指定するか、スプレッドシートから情報をインポートします。

ストレージ・デバイスが XClarity Administrator の管理対象になった後、XClarity Administrator は各管理対象ストレージ・デバイスを定期的にポーリングして、インベントリー、重要プロダクト・データ、ステータスなどの情報を収集します。各管理対象ストレージ・デバイスを表示および監視して、管理操作 (システム設定、ファームウェアの更新、電源オン/オフなど) を実行できます。

1 台のデバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず最初の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。管理対象除外プロセス中にエラーが発生した場合、新規の XClarity Administrator で管理する際に「**管理の強制**」オプションを選択できます。

注：管理可能デバイスのネットワークをスキャンする場合、XClarity Administrator は、デバイスがすでに別のマネージャーで管理されているかどうかは、まずデバイスを管理しようとしなければ分かりません。

手順

XClarity Administrator を使用してストレージ・デバイスを管理するには、以下のいずれかの手順を実行します。

- 一括インポート・ファイルを使用して多数のストレージ・デバイスとその他のタイプのデバイスを検出および管理します (XClarity Administratorオンライン・ドキュメントのシステムの管理を参照してください)。
- XClarity Administrator と同じ IP サブネットにあるストレージ・デバイスを検出して管理する。
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「新しいデバイスの検出と管理」ページが表示されます。

     テーブルの列をソートすると、管理するストレージ・デバイスを見つけやすくなります。「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるストレージ・システムを絞り込むこともできます。「**列のカスタマイズ**」アイコン ( ) をクリックして、表示する列とデフォルトのソート順序を変更できます。
  2. 「**更新**」アイコン ( ) をクリックして、XClarity Administratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
  3. 管理するストレージ・デバイスを 1 台以上選択します。

4. 「**選択を管理**」をクリックします。「管理」ダイアログが表示されます。
5. ストレージ・デバイスへの認証に使用されるユーザー ID とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator の操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。
6. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

   – 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   – 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。
7. 「**管理**」をクリックします。

   ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、この進行状況を監視します。
8. プロセスが完了したら、「OK」をクリックします。

   これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

   – 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

     注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。
   – デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
   – デバイスが正しく管理対象から除外されなかった場合。

   注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

- XClarity Administrator と同じ IP サブネットにないストレージ・デバイスを、IP アドレスを手動で指定して検出し管理する場合。

  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。
  2. 「**手動で入力**」を選択します。
  3. 管理するストレージ・デバイスのネットワーク・アドレスを指定します。

     – 「**単一システム**」をクリックし、単一の IP アドレス、ドメイン名、または完全修飾ドメイン名 (FQDN) を入力します。

       注：FQDN を指定するには、「ネットワーク・アクセス」ページで有効なドメイン名が指定されていることを確認します (ネットワーク・アクセスの構成を参照)。
     – 「**複数システム**」をクリックし、IP アドレスの範囲を入力します。別の範囲を追加するには、「**追加**」アイコン () をクリックします。範囲を削除するには、「**削除**」アイコン () をクリックします。
  4. 「OK」をクリックします。

5. ストレージ・デバイスへの認証に使用されるユーザー ID とパスワードを指定します。

   ヒント: デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator の操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

6. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

   – 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   – 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

7. 「**管理**」をクリックします。

   ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、この進行状況を監視します。

8. プロセスが完了したら、「OK」をクリックします。

   これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

   – 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

     注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

   – デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
   – デバイスが正しく管理対象から除外されなかった場合。

   注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

終了後

- 追加のデバイスを検出して管理します。
- 現行ポリシー (管理対象デバイスでのファームウェアの更新を参照) に従っていないデバイスのファームウェアを更新します。
- 新しいデバイスを適切なラックに追加して物理的環境を反映します (ラックの管理参照)。
- ハードウェアのステータスと詳細を監視します (ストレージ・デバイスのステータスの表示を参照)。
- イベントとアラートを監視します (イベントの使用とアラートの使用を参照)。

ストレージの管理に関する考慮事項

ストレージ・デバイスを管理する前に、以下の重要な考慮事項を確認してください。

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。

重要：ラック・ストレージ・デバイスを検出および管理する前に、以下の要件を満たしていることを確認してください (ThinkSystem DE シリーズ以外)。詳しくは、XClarity Administrator オンライン・ドキュメントの デバイスを検出できない、デバイスを管理できない を参照してください。

- ネットワーク構成では、XClarity Administrator とラック・ストレージ・デバイス間の SLP トラフィックを許可する必要があります。
- ユニキャスト SLP が必要です。
- XClarity Administrator が自動的に Lenovo Storage デバイスを検出するには、マルチキャスト SLP が必要です。さらに、ラック・ストレージ・デバイスで SLP を有効にする必要があります。

Lenovo Storage デバイスの場合、システム・レベルの温度は、システムのミッドプレーンに最も近い温度センサーで計測され、通気がドライブを通った後の周囲温度を反映します。温度が異なる時点で取得された場合、XClarity Administrator および管理コントローラーによって報告される温度が異なる可能性があることに注意してください。

Lenovo DE シリーズ・ストレージ・デバイスの場合、初期管理中に両方の管理コントローラーがネットワーク経由で到達可能である必要があります。

ストレージ・デバイスでは、SNMP トラップは英語のみです。

ストレージ・デバイスのステータスの表示

Lenovo XClarity Administrator から管理対象ストレージ・デバイスの概要と詳細なステータスを表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

以下のステータス・アイコンは、デバイスの全体的な正常性を示します。証明書が一致しない場合、該当する各デバイスのステータスに「(非トラステッド)」と付加されます。たとえば、「警告 (非トラステッド)」となります。接続に問題がある場合やデバイスへの接続が信頼されない場合、該当する各デバイスのステータスに「(接続)」と付加されます。たとえば、「警告 (接続)」となります。

- ( ) クリティカル
- ( ) 警告
- ( ) 保留中
- ( ) 通知
- ( ) 正常
- ( ) オフライン
- ( ) 不明

手順

管理対象ストレージ・デバイスのステータスを表示するには、次の 1 つ以上の操作を実行します。

- Lenovo XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。ダッシュボード・ページが開いて、すべての管理対象ストレージ・デバイスとその他のリソースの概要とステータスが表示されます。

- Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックします。「ストレージ」ページが開いて、管理対象シャーシに取り付けられているすべてのストレージ・デバイスがテーブル・ビューで表示されます。

  テーブルの列をソートすると、管理するストレージ・デバイスを見つけやすくなります。また、「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力してステータス・アイコンをクリックすると、指定された条件に一致するストレージ・デバイスのみがリストされます。

  このページでは、以下の操作を実行できます。

  - ストレージ・デバイスとそのコンポーネントに関する詳細情報を表示します (ストレージ・デバイスの詳細の表示を参照)。
  - グラフィカルなラック・ビューまたはシャーシ・ビューでストレージ・デバイスを表示するには、「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューで表示**」 または 「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**シャーシ・ビューで表示**」をクリックします。
  - ストレージ・デバイスの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (ストレージ・デバイスの管理コントローラー・インターフェースの起動を参照)。
  - ストレージ・デバイス内のストレージ・コントローラーの電源をオンおよびオフにします (ストレージ・デバイスの電源のオン/オフを参照)。

- システム情報を変更するには、ストレージ・デバイスを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックします。
- インベントリーを最新の情報に更新するには、ストレージ・デバイスを選択して「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーを最新の情報に更新**」をクリックします。
- ストレージ・デバイスを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーのエクスポート**」をクリックして、1 つ以上のストレージ・デバイスに関する詳細情報を単一 CSV ファイルにエクスポートします。

  注：最大 60 個のデバイスのインベントリー・データを一度にエクスポートできます。

  ヒント: CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- ストレージ・デバイスを管理対象から除外 (ストレージ・デバイスの管理解除を参照)。
- (Flex System Storage デバイスのみ) ストレージ・デバイスのストレージ・コントローラーの仮想再取り付けを実行します (Flex System ストレージ・デバイスへのストレージ・コントローラーの仮想再取り付けを参照)。
- 不要なイベントは、「**イベントの除外**」アイコン ( ) をクリックして、イベントが表示されているすべてのページから除外します。(イベントの除外 を参照)。
- Lenovo XClarity Administrator のセキュリティー証明書と、ストレージ・デバイスが取り付けられているシャーシ内の CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、ストレージ・デバイスを選択し、「**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 (非トラステッド・サーバー証明書の解決を参照)。
- ストレージ・デバイスを静的リソース・グループに追加またはグループから削除するには、「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループに追加**」 または 「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループから削除**」 をクリックします。

ストレージ・デバイスの詳細の表示

Lenovo XClarity Administrator から管理対象ストレージ・デバイスに関する詳細情報 (IP アドレス、製品名、シリアル番号、各キャニスターの詳細など) を表示できます。

このタスクについて

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

Lenovo Storage デバイスの場合、システム・レベルの温度は、システムのミッドプレーンに最も近い温度センサーで計測され、通気がドライブを通った後の周囲温度を反映します。温度が異なる時点で取得された場合、XClarity Administrator および管理コントローラーによって報告される温度が異なる可能性があることに注意してください。

手順

特定の管理対象ストレージ・デバイスの詳細を表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックします。「ストレージ」ページが開いて、管理対象シャーシに取り付けられているすべてのストレージ・デバイスがテーブル・ビューで表示されます。

テーブルの列をソートすると特定のストレージ・デバイスを見つけやすくなります。「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるストレージ・デバイスを絞り込むこともできます。

ステップ 2. 「**ストレージ**」列でストレージ・デバイス名をクリックします。「要約」ページが開いて、プロパティと、そのストレージ・デバイスに取り付けられたコンポーネントのリストが表示されます。

ステップ 3. ストレージの詳細を表示するには、以下の操作を 1 つまたは複数実行します。表示されるデータは、ストレージ・デバイスのタイプによって異なる場合があります。

- システム情報や取り付けられたデバイスなど、サーバーとそこに取り付けられているコンポーネントの要約を表示するには、「**要約**」をクリックします (ストレージ・デバイスのステータスの表示を参照)。
- 以下のようなストレージ・デバイス・コンポーネントの詳細を表示するには、「**インベントリー詳細**」をクリックします。
  - ストレージ・デバイスのファームウェア・レベル
  - 管理コントローラー・ネットワークの詳細 (ホスト名、IPv4 アドレス、IPv6 アドレス、MAC アドレスなど)。
  - ストレージ・デバイスのアセットの詳細
  - ストレージ・デバイスの各キャニスターの詳細

  ヒント: Flex System ストレージ拡張ノードや Flex System PCIe Expansion Node などの拡張ノードがシャーシに取り付けられてストレージ・デバイスに接続されている場合は、その拡張ノードのインベントリーの詳細も表示されます。
- ストレージ・デバイスに関連するアラートをアラート・リストに表示するには、「**アラート**」をクリックします (アラートの使用 を参照)。
- ストレージ・デバイスストレージ・デバイスに関連するイベントをイベント・ログに表示するには、「**イベント・ログ**」をクリックします (イベントの使用 を参照)。
- ストレージ・デバイスに関連付けられているジョブのリストを表示するには、「**ジョブ**」をクリックします (ジョブの監視 を参照)。
- ストレージ・デバイスの各 LED の現在の状態を表示するには、「**Light Path**」をクリックします。
- ストレージ・デバイスの電源および熱の特性を表示するには、「**電源および熱**」をクリックします。

  ヒント: 電源および熱の最新データを収集するには、Web ブラウザーの最新表示ボタンを使用します。データの収集には数分かかる場合があります。

終了後

ストレージ・デバイスに対しては、要約と詳細情報の表示に加えて、以下の操作を実行できます。

- グラフィカルなラック・ビューまたはシャーシ・ビューでストレージ・デバイスを表示するには、「**操作**」 → 「**ビュー**」 → 「**ラック・ビューで表示**」または「**操作**」 → 「**ビュー**」 → 「**シャーシ・ビューで表示**」をクリックします。
- ストレージ・デバイスに関する詳細情報を CSV ファイルにエクスポートするには、「**操作**」 → 「**インベントリー**」 → 「**インベントリーのエクスポート**」をクリックします。

  注：

  - CSV ファイルのインベントリー・データについて詳しくは、Lenovo XClarity Administrator オンライン・ドキュメントの GET /storage/*<UUID_list>* REST API を参照してください。
  - CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- ストレージ・デバイスの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (ストレージ・デバイスの管理コントローラー・インターフェースの起動を参照)。
- ストレージ・デバイス内のストレージ・コントローラーの電源をオンおよびオフにします (ストレージ・デバイスの電源のオン/オフを参照)。
- ストレージ・デバイスにストレージ・コントローラーを仮想再取り付けします (Flex System シャーシのサーバーの仮想再取り付けを参照)。

- システム情報を変更するには、ストレージ・デバイスを選択し、「**プロパティの編集**」をクリックします。
- インベントリーを最新の情報に更新するには、ストレージ・デバイスを選択して「**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。
- 不要なイベントは、「**操作**」 ➡ 「**サービスのリセット**」 ➡ 「**イベントの除外**」をクリックして、イベントが表示されているすべてのページから除外します (イベントの除外を参照)。
- XClarity Administrator のセキュリティー証明書と、ストレージ・デバイスが取り付けられているシャーシ内の CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、ストレージ・デバイスを選択し、「**操作**」 ➡ 「**サービス**」 ➡ 「**非トラステッド証明書の解決**」をクリックします (非トラステッド・サーバー証明書の解決を参照)。

ストレージ構成データのバックアップと復元

Lenovo XClarity Administrator には、ストレージ構成データの組み込みバックアップ機能はありません。代わりに、ご使用の管理対象ストレージ・デバイスで使用可能なバックアップ機能を使用します。

デバイスの回復方法については、ストレージ・デバイスに付属の製品ドキュメントを参照してください。
- Lenovo Storage デバイスの場合は、Lenovo Storage S2200/S3200 製品ドキュメントを参照してください。
- Lenovo ThinkSystem ストレージ・デバイスの場合は、ThinkSystem ストレージの製品ドキュメントを参照してください。

ストレージ・デバイスの電源のオン/オフ

Lenovo XClarity Administrator からストレージ・デバイスの電源オン/電源オフを実行できます。

このタスクについて

Flex System ストレージ・デバイスでは、ストレージ・コントローラーの電源をオフにすると、ストレージ・デバイスはデータを内蔵ドライブに保存してからスタンバイ状態に入ります。ストレージ・デバイスがスタンバイ状態に入ると、ストレージ・デバイスによって提供されているボリュームにアクセスできなくなります。

ThinkSystem DM シリーズのストレージ・デバイスの電源をオンにするには、管理に使用するストレージ・コントローラーがオンラインであり、その IP アドレスから外部ネットワークを通じて電源オフのストレージ・コントローラーのサービス・プロセッサーに直接通信できることを確認してください。

手順

管理対象ストレージ・デバイスの電源をオンまたはオフにするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックします。「ストレージ」ページが開いて、管理対象シャーシに取り付けられているすべてのストレージ・デバイスがテーブル・ビューで表示されます。

テーブルの列をソートすると特定のストレージ・デバイスを見つけやすくなります。また、「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるストレージ・デバイス を絞り込むこともできます。

ステップ 2. 電源をオンまたはオフにするストレージ・デバイスを選択します。

ステップ 3. 「**すべての操作**」をクリックし、次のいずれかの電源操作をクリックします。

- **電源オン・コントローラー A**
- **電源オン・コントローラー B**
- **電源オフ・コントローラー A**
- **電源オフ・コントローラー B**
- **再起動コントローラー A**
- **再起動コントローラー B**

Flex System ストレージ・デバイスへのストレージ・コントローラーの仮想再取り付け

ストレージ・コントローラー (キャニスター) をストレージ・デバイス・ベイから取り外して再び挿入する操作をシミュレートする仮想再取り付けを実行できます。

このタスクについて

仮想再取り付けの間に、ストレージ・デバイスに対する既存のネットワーク接続がすべて失われ、ストレージ・デバイスの電源状態が変更されます。仮想再取り付けを実行する前に、すべてのユーザー・データが保存されていることを確認してください。

手順

ストレージ・コントローラーを仮想再取り付けするには、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、「**ハードウェア**」 ➔ 「**ストレージ**」の順にクリックします。「ストレージ」ページが開いて、すべてのストレージ・デバイスがテーブル・ビューで表示されます。

テーブルの列をソートすると特定のストレージ・デバイスを見つけやすくなります。「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるストレージ・デバイスを絞り込むこともできます。

ステップ 2. Flex System ストレージ・デバイスを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**サービス**」の順にクリックして、「**コントローラー A の仮想再取り付け**」または「**コントローラー B の仮想再取り付け**」をクリックします。

ステップ 4. 「**仮想再取り付け**」をクリックします。

ストレージ・デバイスの管理コントローラー・インターフェースの起動

ストレージ・デバイスが取り付けられているシャーシの管理コントローラー Web インターフェースを Lenovo XClarity Administrator から起動できます。

手順

管理コントローラー Web インターフェースを起動するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックします。「ストレージ」ページが開いて、すべての管理対象ストレージ・デバイスがテーブル・ビューで表示されます。

テーブルの列をソートすると特定のストレージ・デバイスを見つけやすくなります。「**フィルター**」フィールドにテキスト (デバイス名や IP アドレスなど) を入力して、表示されるストレージ・デバイスを絞り込むこともできます。

ステップ 2. ストレージ・デバイスを選択します。

ステップ 3. 「**操作**」 ➡ 「**起動**」 ➡ 「**管理 Web インターフェース**」をクリックします。管理コントローラー Web インターフェースが起動します。

ステップ 4. 管理コントローラー・インターフェースにログオンします。

注：Flex System ストレージ・デバイスの場合は、XClarity Administrator ユーザー資格情報を使用します。

ストレージ・デバイスのシステム・プロパティの変更

特定のストレージ・デバイスのシステム・プロパティを変更できます。

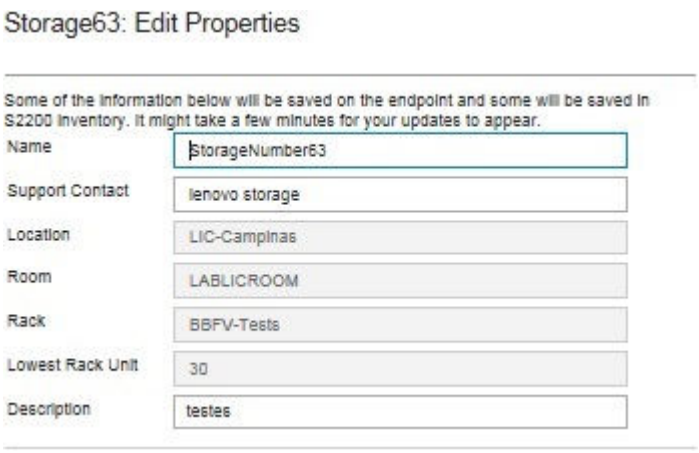
手順

システム・プロパティを変更するには、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、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックして、「ストレージ」ページを表示します。

ステップ 2. 更新するストレージ・デバイスを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックし、「編集」ダイアログを表示します。



ステップ 4. 以下の情報を必要に応じて変更します。
- 名前
- サポート連絡先
- 説明

注：Web インターフェースのラックからデバイスを追加または削除する場合は、ロケーション、設置部屋、ラック、最下段ラック・ユニットのプロパティが XClarity Administrator によって更新されます (ラックの管理を参照)。

ステップ 5. 「**保存**」をクリックします。

注：変更されたプロパティが XClarity Administrator Web インターフェースに表示されるまで少し時間がかかる場合があります。

管理サーバーの障害発生後のラック・ストレージ・デバイスによる管理のリカバリー

ラック・ストレージ・デバイスが正しく管理解除されなかった場合、再管理する前にストレージ・デバイスをリカバリーする必要があります。Lenovo XClarity Administrator によって以前に設定されたストレージ・デバイス構成の特定の部分をクリアすることによってシステム管理をリカバリーできます。

手順

ラック・ストレージ・デバイスをリカバリーするには、以下の手順のいずれかを実行します。

- 交換 XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、「**管理の強制**」オプションを使用してデバイスを再度管理できます (ストレージ・デバイスの管理参照)。
- ストレージ・デバイスから、接頭部「LXCA_」を持つすべてのユーザー・アカウントを削除し、接頭部「SYSMGR_」を持ちタイプが「SNMPv3」のユーザー・アカウントも任意で削除します。

終了後

XClarity Administrator が復元または交換されると、ストレージ・デバイスをもう一度管理できるようになります (ストレージ・デバイスの管理を参照)。ストレージ・デバイスに関するすべての情報 (システム・プロパティなど) は保持されます。

管理サーバーの障害発生後の Lenovo ThinkSystem DE Series ストレージ・デバイスによる管理のリカバリー

Lenovo ThinkSystem DE シリーズ・ストレージ・デバイスが正しく管理解除されなかった場合、再管理する前にストレージ・デバイスをリカバリーする必要があります。Lenovo XClarity Administrator によって以前に設定されたストレージ・デバイス構成の特定の部分をクリアすることによってシステム管理をリカバリーできます。

手順

Lenovo ThinkSystem DE シリーズ・ストレージ・デバイスをリカバリーするには、以下の手順のいずれかを実行します。

- 交換 XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、「**管理の強制**」オプションを使用してデバイスを再度管理できます (ストレージ・デバイスの管理参照)。
- ストレージ・デバイスの鍵ペア API から「LXCA_REMOTE_MANAGMENT_VERIFICATION」鍵ペアの登録を削除します。

終了後

XClarity Administrator が復元または交換されると、ストレージ・デバイスをもう一度管理できるようになります (ストレージ・デバイスの管理を参照)。ストレージ・デバイスに関するすべての情報 (システム・プロパティなど) は保持されます。

ストレージ・デバイスの管理解除

ストレージ・デバイスを Lenovo XClarity Administrator の管理対象から除外できます。このプロセスは*管理解除*と呼ばれます。

始める前に

ストレージ・デバイスを管理解除する前に、そのスイッチに対して実行中のアクティブ・ジョブがないことを確認します。

このタスクについて

ストレージ・デバイスを管理解除しても、XClarity Administrator にはストレージ・デバイスに関する特定の情報が保持されます。この情報は、そのストレージ・デバイスの管理を再開したときに再適用されます。

ヒント: 初期セットアップ中にオプションで追加されたすべてのデモ・デバイスは、シャーシ内のノードです。デモ・デバイスを管理対象から除外するには、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」オプションを使用してシャーシを管理対象から除外します。

手順

ストレージ・デバイスを管理解除するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**ストレージ**」の順にクリックして、「ストレージ」ページを表示します。

ステップ 2. 管理対象スイッチのリストから 1 つ以上のストレージ・デバイスを選択します。

ステップ 3. 「**非管理**」をクリックします。「管理対象から除外」ダイアログが表示されます。

ステップ 4. **オプション**: 「**デバイスに到達できない場合であっても、管理対象からの除外を強制します**」を選択します。

重要：デモ・ハードウェアを管理解除する場合は、このオプションを選択してください。

ステップ 5. 「**非管理**」をクリックします。
「管理対象から除外」ダイアログには、管理解除プロセスの各ステップの進行状況が表示されます。

ステップ 6. 管理解除プロセスが完了したら、「OK」をクリックします。

正しく管理解除されなかったラック・ストレージ・デバイスのリカバリー

Lenovo XClarity Administrator がラック・ストレージ・デバイスを管理しているときに、XClarity Administrator に障害が発生した場合は、管理サーバーの復元または交換を待たずに、管理機能を回復できます。XClarity Administrator によって以前に設定されたストレージ・デバイス構成の特定の部分をクリアすることによってシステム管理をリカバリーできます。

手順

ラック・ストレージ・デバイスをリカバリーするには、以下の手順のいずれかを実行します。

- 交換 XClarity Administrator インスタンスが、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、「**管理の強制**」オプションを使用してデバイスを再度管理できます (ストレージ・デバイスの管理参照)。
- ストレージ・デバイスから、接頭部「LXCA_」を持つすべてのユーザー・アカウントを削除し、接頭部「SYSMGR_」を持ちタイプが「SNMPv3」のユーザー・アカウントも任意で削除します。

終了後

XClarity Administrator が復元または交換されると、ストレージ・デバイスをもう一度管理できるようになります (ストレージ・デバイスの管理を参照)。ストレージ・デバイスに関するすべての情報 (システム・プロパティなど) は保持されます。

第 10 章　スイッチの管理

Lenovo XClarity Administratorでネットワーク・スイッチを管理できます。

詳細:

- XClarity Administrator: 検出
- XClarity Administrator: スイッチの管理

始める前に

注意：スイッチを管理する前に、スイッチ管理に関する考慮事項を検討してください。詳しくは、スイッチの管理に関する考慮事項を参照してください。

注：Flex スイッチは、それらを含むシャーシを管理する際に自動的に検出され管理されます。シャーシとは別に Flex スイッチを検出、管理することはできません。

特定のポートがスイッチとの通信に使用できることが必要です。スイッチを管理する前に、必要なポートがすべて使用可能になっていることを確認します。ポートについては、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。

XClarity Administrator を使用して管理する各スイッチに、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。

ラック・スイッチを管理する前に、XClarity Administrator に保存された資格情報を作成してください。XClarity Administrator はラック・スイッチの認証に保存された資格情報のみを使用します。保存された資格情報は、デバイス上のアクティブなユーザー・アカウントと一致する必要があります。管理ダイアログまたは「保存された資格情報」ページから、保存された資格情報を作成できます。詳しくは、保存された資格情報の管理を参照してください。

すべての RackSwitch デバイスで、ループバック・インターフェースを使用した管理がサポートされます。静的経路を追加するか、ルーティング・プロトコルを介してアドレスをアドバタイズすることで、XClarity Administrator がループバック・インターフェースに接続していることを確認します。管理ポートと*任意*のデータ・ポート (ループバックを含む) 間でルーティングを実行できないことに注意してください。

Lenovo ThinkSystem DB シリーズ・スイッチの場合

- FOS 8.2.3 以降が必要です。
- スイッチを管理する*前*に、スイッチで `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw` コマンドを実行して、SNMPv3 ユーザーをインデックス 1 で設定する必要があります。
- スイッチで REST が有効になっていることを確認します。REST を有効にするには、`mgmtapp --enable rest` コマンドを実行します。
- 許可する REST セッション数を 10 にする必要があります。この REST セッション数を設定するには、`mgmtapp --config -maxrestsession 10` コマンドを実行します。
- Lenovo ThinkSystem DB シリーズ・スイッチは、サービス検出プロトコルを使用して検出できません。これらのスイッチを管理するには、「**手動入力**」オプションを使用して「**サービス検出プロトコルを使用してデバイス・タイプを識別する**」をオフにし、「**デバイス・タイプ**」リストから「「Lenovo ThinkSystem DB シリーズ・スイッチ」」を選択します。詳しくは、XClarity Administrator として同じ IP サブネットにないスイッチを検出および管理する以下の手順を参照してください。

NVIDIA スイッチの場合

- Cumulus 4.3 以降が必要です
- NVIDIA スイッチは、サービス検出プロトコルを使用して検出できません。これらのスイッチを管理するには、**手動で入力**オプションを使用して「サービス検出プロトコルを使用してデバイス・タイプを識別する」をオフにした後、**デバイス・タイプ**のリストから「NVIDIA スイッチ」を選択します。詳細については、XClarity Administrator と同じ IP サブネット上にないスイッチの検出と管理に関する以下の手順を参照してください。

このタスクについて

XClarity Administrator を使用すると、XClarity Administrator と同じ IP サブネットにある管理可能デバイスのプローブによって、環境内の RackSwitch スイッチを自動的に検出できます。他のサブネットにあるスイッチを検出するには、IP アドレスまたは IP アドレス範囲を指定するか、スプレッドシートから情報をインポートします。

注：XClarity Administrator では、手動の資格情報はラック・スイッチではサポートされていません。

スイッチが XClarity Administrator の管理対象になった後、XClarity Administrator は各管理対象スイッチを定期的にポーリングして、インベントリー、重要な製品データ、ステータスなどの情報を収集します。各管理対象スイッチを表示および監視して、管理コンソールの起動や電源オン/オフなどの管理タスクを実行できます。

XClarity Administrator で、管理プロセス中のインベントリーの収集時に、(たとえば、電源喪失、ネットワーク障害の発生、またはスイッチがオフラインであるなどの理由により) スイッチとの通信が喪失した場合、管理は正常に完了します。ただし、一部のインベントリー情報の収集が完了していない可能性があります。スイッチがオンラインになり XClarity Administrator によってインベントリーについてスイッチがポーリングされるのを待つか、または手動でスイッチのインベントリーを収集するために「スイッチ」ページからスイッチを選択して「**すべての操作**」 ➔ 「**インベントリー**」 ➔ 「**インベントリーを最新の情報に更新**」をクリックします。

注：スイッチはスタックできます。*スタック・スイッチ*とは、1 つのネットワーク・スイッチとして動作するスイッチのグループです。スタックには、1 つの *マスター・スイッチ*と 1 つ以上の *メンバー・スイッチ*が含まれます。Flex スイッチの場合、スタック内の各スイッチを表示および監視し、診断データを収集できます。ただし、管理タスク (ファームウェア更新、サーバー構成など) はスタック・スイッチでは実行できません。これらの XClarity Administrator 管理タスクは、マスター・スイッチを含むすべてのスタック・スイッチで無効になっています。マスター・スイッチ CLI から直接スタック・スイッチのファームウェアを更新できます。RackSwitch スイッチの場合、マスター・スイッチ情報のみ表示およびモニターできます。メンバー・スイッチは XClarity Administrator によって検出されません。

管理タスクは、保護モードの Flex スイッチでも無効になっています。

1 台のデバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず最初の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。管理対象除外プロセス中にエラーが発生した場合、新規の XClarity Administrator で管理する際に「**管理の強制**」オプションを選択できます。

注：管理可能デバイスのネットワークをスキャンする場合、XClarity Administrator は、デバイスがすでに別のマネージャーで管理されているかどうかは、まずデバイスを管理しようとしなければ分かりません。

スイッチが SSH を使用して直接管理されている場合または CMM を経由して間接的に管理されている場合、スイッチは XClarity Administrator の管理対象として識別され、やり取りに必要な構成が実行され、インベントリーが収集されます。

手順

XClarity Administrator を使用して RackSwitch スイッチを管理するには、以下のいずれかの手順を実行します。

- 一括インポート・ファイルを使用して多数のスイッチとその他のデバイスを検出および管理します (Lenovo XClarity Administratorオンライン・ドキュメントのシステムの管理を参照してください)。
- XClarity Administrator と同じ IP サブネットにある RackSwitch スイッチを検出して管理する。
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**新しいデバイスの検出と管理**」をクリックします。「新しいデバイスの検出と管理」ページが表示されます。

     テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。「**列のカスタマイズ**」アイコン ( ) をクリックして、表示する列とデフォルトのソート順序を変更できます。
  2. 「**更新**」アイコン ( ) をクリックして、XClarity Administratorドメイン内のすべての管理可能なデバイスを検出します。検出には数分間かかる場合があります。
  3. 管理するスイッチを 1 台以上選択します。
  4. 「**選択を管理**」をクリックします。
  5. スイッチへの認証に使用される保存された資格情報を指定します。

ヒント:

- 「**保存された資格情報の管理**」をクリックして、保存された資格情報を作成し XClarity Administrator で管理します (保存された資格情報の管理を参照)。
- デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。

6. (ENOS を実行しているスイッチのみ) 設定されている場合は、スイッチの特権実行モードに入るために使用する「有効」パスワードも指定します。

   ENOS を実行する RackSwitch スイッチを管理するときは、スイッチでの「特権実行モード」へのアクセスが必要です。これは、スイッチに「enable」コマンドを発行するときに XClarity Administrator で使用されます。デフォルトでは、スイッチでこのコマンドにパスワードは設定されていません。ただし、スイッチ管理者がセキュリティを高めるためにこのコマンドにパスワードを構成した場合、XClarity Administrator がスイッチを正常に管理するにはパスワードを入力する必要があります。

7. オプション: (ENOS を実行するスイッチのみ) スイッチで HTTPS を有効にするかどうかを選択する。「**詳細**」をクリックし、「**HTTPS を有効にする**」を選択します。これはデフォルトで有効になっています。

   注：

   - CNOS を実行するスイッチの場合、スイッチで HTTPS を有効にしてから管理する必要があります (スイッチの管理に関する考慮事項を参照)。
   - HTTPS を有効にしない場合は、スイッチの現在の設定が使用されます。
   - スイッチが管理対象から除外された場合、XClarity Administrator は HTTPS を元の設定に復元します。

8. オプション: スイッチの NTP 構成を Lenovo XClarity Administrator 用に定義された NTP 構成とタイム・ゾーン設定に置き換える。「**詳細**」をクリックして、「**管理サーバーから NTP 設定を使用するよう、NTP クライアントを構成**」を選択します。これはデフォルトで有効になっています。

   注：

   - NTP 構成とタイム・ゾーンを置き換えない場合、ログ項目およびイベントのタイム・スタンプが管理対象スイッチおよび管理サーバーと同期されない場合があります。
   - スイッチが管理対象から除外された場合、XClarity Administrator は NTP 構成とタイム・ゾーンを元の設定に復元します。

9. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

   注：

   - 現在のユーザーに割り当てられている役割グループのリストから選択できます。
   - 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

10. 「**管理**」をクリックします。

    ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、進行状況を監視します。

11. プロセスが完了したら、「**OK**」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    - 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

- デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
- デバイスが正しく管理対象から除外されなかった場合。

注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

- IP アドレスを手動で指定して、XClarity Administrator と同じ IP サブネットにない RackSwitch スイッチを検出して管理する。

1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックします。「検索と管理」ページが表示されます。
2. 「**手動で入力**」を選択します。
3. 管理するスイッチのネットワーク・アドレスを指定します。
   - 「**単一システム**」をクリックし、単一の IP アドレス、ドメイン名、または完全修飾ドメイン名 (FQDN) を入力します。

     注：FQDN を指定するには、「ネットワーク・アクセス」ページで有効なドメイン名が指定されていることを確認します (ネットワーク・アクセスの構成を参照)。
   - 「**複数システム**」をクリックし、IP アドレスの範囲を入力します。別の範囲を追加するには、「**追加**」アイコン (➕) をクリックします。範囲を削除するには、「**削除**」アイコン (❌) をクリックします。
4. サービス検出プロトコルを使用してデバイス・タイプを検出できない場合は、「サービス検出プロトコルを使用してデバイス・タイプを識別する」をオフにして、管理するデバイスのタイプをドロップダウン・リストから選択します。

   SLP や SSDP などのサービス検出プロトコルを使用すると、XClarity Administrator で、管理するデバイスのタイプを自動的に検出して、適切なメカニズムを使用してデバイスを管理することができます。一部のデバイス・タイプではサービス検出プロトコルがサポートされません。また、一部の環境では、サービス検出プロトコルが意図的に無効になっています。いずれの場合も、適切なデバイス・タイプを選択して管理プロセスを完了する必要があります。以下のデバイス・タイプは、明示的に識別する必要があります。
   - Lenovo ThinkSystem DB シリーズ・スイッチ
   - NVIDIA Mellanox スイッチ
5. 「**OK**」をクリックします。
6. スイッチへの認証に使用される保存された資格情報を指定します。

   ヒント:
   - 「**保存された資格情報の管理**」をクリックして、保存された資格情報を作成し XClarity Administrator で管理します (保存された資格情報の管理を参照)。
   - デバイスの管理にはスーパーバイザー / 管理者アカウントを使用することをお勧めします。それより低いレベルの権限を持つアカウントを使用した場合、管理が失敗するか、管理に成功してもデバイスで今後行う XClarity Administrator 操作が失敗する可能性があります (特にデバイスが管理対象認証を使わないで管理されている場合)。
7. (ENOS を実行しているスイッチのみ) 設定されている場合は、スイッチの特権実行モードに入るために使用する「有効」パスワードも指定します。

   ENOS を実行する RackSwitch スイッチを管理するときは、スイッチでの「特権実行モード」へのアクセスが必要です。これは、スイッチに「enable」コマンドを発行するときに XClarity Administrator

で使用されます。デフォルトでは、スイッチでこのコマンドにパスワードは設定されていません。ただし、スイッチ管理者がセキュリティを高めるためにこのコマンドにパスワードを構成した場合、XClarity Administrator がスイッチを正常に管理するにはパスワードを入力する必要があります。

8. オプション: (ENOS を実行するスイッチのみ) スイッチで HTTPS を有効にするかどうかを選択する。「**詳細**」をクリックし、「**HTTPS を有効にする**」を選択します。これはデフォルトで有効になっています。

   注：

   – CNOS を実行するスイッチの場合、スイッチで HTTPS を有効にしてから管理する必要があります (スイッチの管理に関する考慮事項を参照)。
   – HTTPS を有効にしない場合は、スイッチの現在の設定が使用されます。
   – スイッチが管理対象から除外された場合、XClarity Administrator は HTTPS を元の設定に復元します。

9. オプション: スイッチの NTP 構成を Lenovo XClarity Administrator 用に定義された NTP 構成とタイム・ゾーン設定に置き換える。「**詳細**」をクリックして、「**管理サーバーから NTP 設定を使用するよう、NTP クライアントを構成**」を選択します。これはデフォルトで有効になっています。

   注：

   – NTP 構成とタイム・ゾーンを置き換えない場合、ログ項目およびイベントのタイム・スタンプが管理対象スイッチおよび管理サーバーと同期されない場合があります。
   – スイッチが管理対象から除外された場合、XClarity Administrator は NTP 構成とタイム・ゾーンを元の設定に復元します。

10. 「**変更**」をクリックして、デバイスに割り当てられる役割グループを変更します。

    注：

    – 現在のユーザーに割り当てられている役割グループのリストから選択できます。
    – 役割グループを変更しない場合は、デフォルトの役割グループが使用されます。デフォルトの役割グループの詳細については、デフォルトのアクセス権限の変更を参照してください。

11. 「**管理**」をクリックします。

    ダイアログが開き、この管理プロセスの進行状況が表示されます。プロセスが正常に完了することを確認するには、進行状況を監視します。

12. プロセスが完了したら、「**OK**」をクリックします。

    これで、デバイスは XClarity Administrator の管理対象になり、自動的にポーリングされて、インベントリーなどの最新の情報が定期的に収集されます。

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

    – 管理元の XClarity Administrator で障害が発生したため、復元できない場合。

      注：交換 XClarity Administrator インスタンスで、障害が発生した XClarity Administrator と同じ IP アドレスを使用している場合は、RECOVERY_ID アカウントとパスワード (該当する場合)、および「**管理の強制**」オプションを使用してデバイスを再度管理できます。

    – デバイスが管理対象から除外される前に、管理元の XClarity Administrator が停止した場合。
    – デバイスが正しく管理対象から除外されなかった場合。

    注意：デバイスを同時に管理できるのは 1 つの XClarity Administrator インスタンスのみです。複数の XClarity Administrator インスタンスによる管理はサポートされていません。デバイスが 1 つの XClarity Administrator の管理対象になっており、そのデバイスを別の XClarity Administrator の管理対象にする場合は、まず元の XClarity Administrator で管理対象から除外してから新しい XClarity Administrator で管理する必要があります。

終了後

- 追加のデバイスを検出して管理します。
- 新たに管理するデバイスを適切なラックに追加して物理的環境を反映します (ラックの管理を参照)。
- ハードウェアのステータスと詳細を監視します (スイッチのステータスの表示を参照)。
- イベントを監視します (イベントの使用を参照)。

スイッチの管理に関する考慮事項

スイッチを管理する前に、以下の重要な考慮事項を確認してください。

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。

RackSwitch デバイスは管理ポートまたはデータ・ポートのいずれかを使用して管理できます。「管理」VRF または「デフォルト」VRF のいずれかに所属するインターフェースでのみ、CNOS を実行する Rackswitch デバイスを管理できます。

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

XClarity イベントと SNMP トラップの構成

ENOS (任意のバージョン) を実行する RackSwitch デバイスを管理する場合は、SNMP トラップ・ソースが管理に使用する IP アドレスを持つインターフェースに設定されます。

CNOS v10.8.1 以降を実行している RackSwitch デバイスが管理されている場合、SNMP トラップ・ソース VRF がチェックされ、管理に使用するポートに一致するように変更されます。

v10.8.1 より前の CNOS を実行する RackSwitch デバイスの場合は、XClarity Administrator で SNMP トラップ・ソースを管理に使用するポートに接続されている VRF にする必要があります。デフォルト値「すべて」は、管理ポートまたはデータ・ポートを使用できます。スイッチ構成がデフォルト値を使用しない場合は、管理に使用するポートに一致するように変更する必要があります。

- 管理に管理ポートを使用する場合、SNMP トラップ・ソース VRF を「すべて」または「管理」に設定します。
- 管理にデータ・ポートのいずれかを使用する場合、SNMP トラップ・ソース VRF を「すべて」または「デフォルト」に設定します。

CNOS を実行している RackSwitch スイッチ

管理では HTTPS を有効にする必要があります。検出では SLP を有効にする必要があります。

注：HTTPS は CNOS ではデフォルトで有効です。restApi のデフォルト構成を変更した場合 (`feature restApi http` コマンドを使用して)、`feature restApi` コマンドを使用して HTTPS に戻すことができます。現在の状況を確認するには、`display restApi server` コマンドを使用します。出力には現在の状況が反映されます。ポート番号に「(HTTP)」が続く場合、HTTPS が *無効* であることを意味します。その他の場合、ポートは 443 です。

RackSwitch デバイスが管理対象外である場合、XClarity Administrator は、CNOS ファームウェアのバージョンに応じて、デバイスの管理前の値に「優先」オプションを復元しないことがあります。

ENOS を実行している RackSwitch スイッチ

- RackSwitch スイッチが、XClarity Administratorと別のネットワーク上に存在する場合、XClarity Administrator がイベントを受信してそのデバイスを管理できるように、ポート 161 および 162 を介してインバウンド UDP を許可するようにそのネットワークを構成する必要があります。

- 管理では SSH を有効にする必要があります。検出では SLP を有効にする必要があります。HTTPS はオプションです。ただし、スイッチの Web インターフェースを起動する場合は有効でなければなりません
- RackSwitch スイッチのファームウェア・バージョンによっては、スイッチが XClarity Administrator によって検出・管理できるように、以下のコマンドを使用して各 RackSwitch スイッチでマルチキャスト SLP 転送および SSH を手動で有効にする必要がある場合があります。詳しくは、System x オンライン・ドキュメントのラック装着スイッチ参照してください。
  - `ip slp enable`
  - `ssh enable`
- RackSwitch スイッチが管理されている場合、XClarity Administrator が以下の構成設定を変更します。管理対象のスイッチの設定を変更すると、接続が中断し、管理操作が正しく実行されない可能性があります。RackSwitch スイッチが管理対象外である場合、構成設定は(管理前の)元の値に復元されます。
  - snmpサーバー・アクセス 32
  - snmpサーバー・グループ 16
  - snmpサーバーは、16 に通知します。
  - snmpサーバー ターゲット・パラメーター16
  - snmpサーバーのターゲット・アドレス 16
  - snmp-server trap-source *<IP interface>*
  - snmpサーバー ユーザー 16
  - snmp-server vesrion *<v3only or v1v2v3>*
  - ntpの有効化
  - ntp primary-server *<hostname or IP address>* MGT
  - ntp secondary-server *<hostname or IP address>* MGT
  - ntp 間隔 1500
  - ntpオフセット 500
  - http アクセスの有効化

  XClarity Administrator を使用し、スイッチのサポートのお問い合わせ先情報、名称またはロケーション・プロパティを変更することによって、以下の構成設定を変更できます。スイッチをラックに追加すると、ロケーションが変更されます。
  - hostname "*<device_name>*"
  - snmpサーバー・ロケーション「ロケーション:*<location>*、部屋:*<room>*、ラック:*<rack>*、LRU:*<lru>*」
  - snmpサーバー接続「*<contact_name>*」

スイッチのステータスの表示

Lenovo XClarity Administrator によって管理されているすべてのスイッチのステータスを表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

このタスクについて

以下のステータス・アイコンは、デバイスの全体的な正常性を示します。証明書が一致しない場合、該当する各デバイスのステータスに「(非トラステッド)」と付加されます。たとえば、「警告 (非トラステッド)」となります。接続に問題がある場合やデバイスへの接続が信頼されない場合、該当する各デバイスのステータスに「(接続)」と付加されます。たとえば、「警告 (接続)」となります。

- ( ) クリティカル
  - 1 つ以上の温度センサーが障害の範囲にあります。
  - 以下のように、ファン・モジュールまたはファンが正しく作動していません:
    - RackSwitch G8124-E: 1 つ以上のファンが100 RPM以下で稼働しています。

  - RackSwitch G8052: 正常な状態のファン・モジュールは 3 個未満です。ファン・モジュールは、そのモジュール内のファンが 500 RPM 超で稼働している場合、正常と見なされます。
  - RackSwitch G8264、G8264CS、G8332、G8272: 正常な状態のファン・モジュールは 4 個未満です。ファン・モジュールは、そのモジュール内のファンが 500 RPM 超で稼働している場合、正常と見なされます。
  - RackSwitch G8296: 正常な状態のファン・モジュールは 3 個未満です。ファン・モジュールは、そのモジュール内のファンが 480 RPM 超で稼働している場合、正常と見なされます。
  - RackSwitch G7028、G7052: 正常な状態のファン・モジュールは 3 個未満です。ファン・モジュールは、そのモジュール内のファンが 500 RPM 超で稼働している場合、正常と見なされます。
  - 1 つのパワー・サプライがオフです。
- () 警告
  - 1 つ以上の温度センサーが警告範囲にあります。
  - パニックダンプが点滅しています。
- () 保留中
- () 通知
- () 正常
  - すべての温度センサーが正常の範囲にあります。
  - すべてのファン・モジュールまたはファンが正しく作動しています。
  - パワー・サプライはどちらもオンです。
  - パニックダンプは点滅していません。
- () オフライン
- () 不明

デバイスは、以下のいずれかの電源状態になります。
- オン
- オフ
- のシャットダウン
- スタンバイ
- 休止
- 不明

手順

管理対象スイッチのステータスを表示するには、次の 1 つ以上の操作を実行します。

- XClarity Administrator のメニュー・バーで、「**ダッシュボード**」をクリックします。ダッシュボード・ページが開いて、すべての管理対象スイッチとその他のリソースの概要とステータスが表示されます。

- XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、すべての管理対象スイッチがテーブル・ビューで表示されます。

  テーブルの列をソートすると、管理するスイッチを見つけやすくなります。また、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力してステータス・アイコンをクリックすると、指定された条件に一致するスイッチのみがリストされます。

  このページでは、以下の操作を実行できます。

  - スイッチに関する詳細情報を表示します (スイッチの詳細の表示参照)。
  - グラフィカルなラック・ビューまたはシャーシ・ビューで Flex スイッチを表示するには、「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューで表示**」または「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**シャーシ・ビューで表示**」をクリックします。
  - グラフィカルなラック・ビューで RackSwitch スイッチを表示するには、「**すべての操作**」 ➡ 「**ビュー**」 ➡ 「**ラック・ビューに表示**」をクリックします。
  - スイッチの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (スイッチの管理コントローラー・インターフェースの起動を参照)。
  - スイッチの SSH コンソールを起動します (スイッチのリモート SSH セッションの起動参照)。

- スイッチの電源オン/電源オフを実行します (スイッチの電源のオン/オフを参照)。
- (RackSwitch スイッチのみ) システム情報を変更するには、スイッチを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックします。
- インベントリーを最新の情報に更新するには、サーバーを選択して「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーを最新の情報に更新**」をクリックしてください。
- 1 つ以上のスイッチに関する詳細情報を単一 CSV ファイルにエクスポートするには、スイッチを選択し、「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**インベントリーのエクスポート**」をクリックします (イベントの除外を参照)。

  注：最大 60 個のデバイスのインベントリー・データを一度にエクスポートできます。

  ヒント: CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。
- 不要なイベントは、「**イベントの除外**」アイコン () をクリックして、イベントが表示されているすべてのページから除外します (イベントの除外を参照)。
- (Flex スイッチのみ) XClarity Administrator のセキュリティー証明書と、スイッチが取り付けられているシャーシ内の CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、スイッチを選択し、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**非トラステッド証明書の解決**」をクリックします (非トラステッド・サーバー証明書の解決を参照)。
- スイッチを静的リソース・グループに追加またはグループから削除するには、「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループに追加**」 または 「**すべての操作**」 ➡ 「**グループ**」 ➡ 「**グループから削除**」 をクリックします。

スイッチの詳細の表示

Lenovo XClarity Administrator から管理対象スイッチに関する詳細情報 (ファームウェア・レベルや IP アドレスなど) を表示できます。

詳細:

- XClarity Administrator: インベントリー
- XClarity Administrator: 監視

手順

XClarity Administrator によって管理されている特定のスイッチの詳細を表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。

ステップ 3. インベントリーの詳細情報を表示するには、以下の手順を実行します。

注：一部のスイッチでは一部の詳細が表示されない場合があります。

- システム情報やファームウェアなどスイッチの要約を表示するには、「**要約**」をクリックします (ストレージ・デバイスのステータスの表示を参照)。
- 以下のようなスイッチ・コンポーネントの詳細を表示するには、「**インベントリー詳細**」をクリックします。
  - スイッチのファームウェア・レベル
  - 管理コントローラー・ネットワークの詳細 (ホスト名、IPv4 アドレス、IPv6 アドレス、MAC アドレスなど)。

  - スイッチのアセットの詳細
- 「**I/O 接続**」をクリックし、選択済みスイッチと、そのスイッチに取り付けられたネットワーク・アダプターの接続について、詳細を表示します。
- スイッチに関連するアラートをアラート・リストに表示するには、「**アラート**」をクリックします (アラートの使用参照)。
- スイッチに関連するイベントをイベント・ログに表示するには、「**イベント・ログ**」をクリックします (イベントの使用参照)。
- 「**構成ファイル**」をクリックして、スイッチ構成をバックアップして復元します (スイッチ構成データのバックアップと復元 を参照)。
- 「**デプロイメント履歴**」をクリックして、スイッチにデプロイされたスイッチ構成テンプレートに関する情報を表示します (スイッチ構成デプロイメント履歴の表示 を参照)。
- 「**ジョブ**」をクリックして、スイッチの構成データ・ファイルを表示します (ジョブの監視を参照)。
- 管理対象スイッチのすべてのポートのステータスおよび構成を表示し、スイッチ・ポートを有効または無効にするには、「**ポート**」をクリックします。

  注：Flex スイッチの場合は、「**最新表示**」アイコン () をクリックして現行のポート・データを収集します。データの収集には数分かかる場合があります。
- スイッチの各 LED の現在の状態を表示するには、「**Light Path**」をクリックします。
- 温度、電源機構、ファンに関する情報を表示するには、「**電源および熱**」をクリックします。

  ヒント: 電源および熱の最新データを収集するには、Web ブラウザーの最新表示ボタンを使用します。データの収集には数分かかる場合があります。

終了後

スイッチに対しては、要約と詳細情報の表示に加えて、以下の操作を実行できます。

- グラフィカルなラック・ビューまたはシャーシ・ビューで Flex スイッチを表示するには、「**操作**」 → 「**ビュー**」 → 「**ラック・ビューで表示**」または「**操作**」 → 「**ビュー**」 → 「**シャーシ・ビューで表示**」をクリックします。
- グラフィカルなラック・ビューで RackSwitch スイッチを表示するには、「**操作**」 → 「**ビュー**」 → 「**ラック・ビューに表示**」をクリックします。
- スイッチの管理コントローラー Web インターフェースを起動するには、「**IP アドレス**」リンクをクリックします (スイッチの管理コントローラー・インターフェースの起動を参照)。
- スイッチの SSH コンソールを起動します (スイッチのリモート SSH セッションの起動参照)。
- スイッチの電源オン/電源オフを実行します (スイッチの電源のオン/オフを参照)。
- (RackSwitch のみ) システム情報を変更するには、スイッチを選択し、「**プロパティの編集**」をクリックします。
- スイッチに関する詳細情報を CSV ファイルにエクスポートするには、「**操作**」 → 「**インベントリー**」 → 「**インベントリーのエクスポート**」をクリックします。

  注：
  - CSV ファイルのインベントリー・データについて詳しくは、XClarity Administrator オンライン・ドキュメントの GET /switches/*<UUID_list>* REST API を参照してください。
  - CSV ファイルを Microsoft Excel にインポートする場合、Excel は数字のみを含むテキスト値を数値として扱います (例えば、UUID の値)。このエラーを修正するには、各セルの形式をテキストにします。

- 不要なイベントは、「**操作**」 ➞ 「**サービスのリセット**」 ➞ 「**除外イベント**」をクリックして、イベントが表示されているすべてのページから除外します (イベントの除外を参照)。
- XClarity Administrator のセキュリティー証明書と、Flex System スイッチが取り付けられているシャーシ内の RackSwitch または CMM のセキュリティー証明書との間で発生する可能性がある問題を解決するには、スイッチを選択し、「**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 (非トラステッド・サーバー証明書の解決を参照)。

スイッチの電源のオン/オフ

Lenovo XClarity Administrator から Flex System または RackSwitch スイッチの電源オン/電源オフを実行できます。

手順

管理対象のスイッチの電源をオンまたはオフにするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➞ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. 電源をオンまたはオフ、または再起動するスイッチを選択します。

ステップ 3. 「**すべての操作**」をクリックし、次のいずれかの電源操作をクリックします。
- **電源オン** (Flex System スイッチのみ)
- **電源オフ** (Flex System スイッチのみ)
- **再起動**。現在実行中のすべての操作を完了した後、スイッチは再起動されます。スイッチの再起動中の操作は拒否されます。

スイッチ・ポートの有効化および無効化

RackSwitch または Flex System スイッチの特定のポートを有効または無効にします。

手順

スイッチ・ポートを有効または無効にするには、以下の手順を実行します。

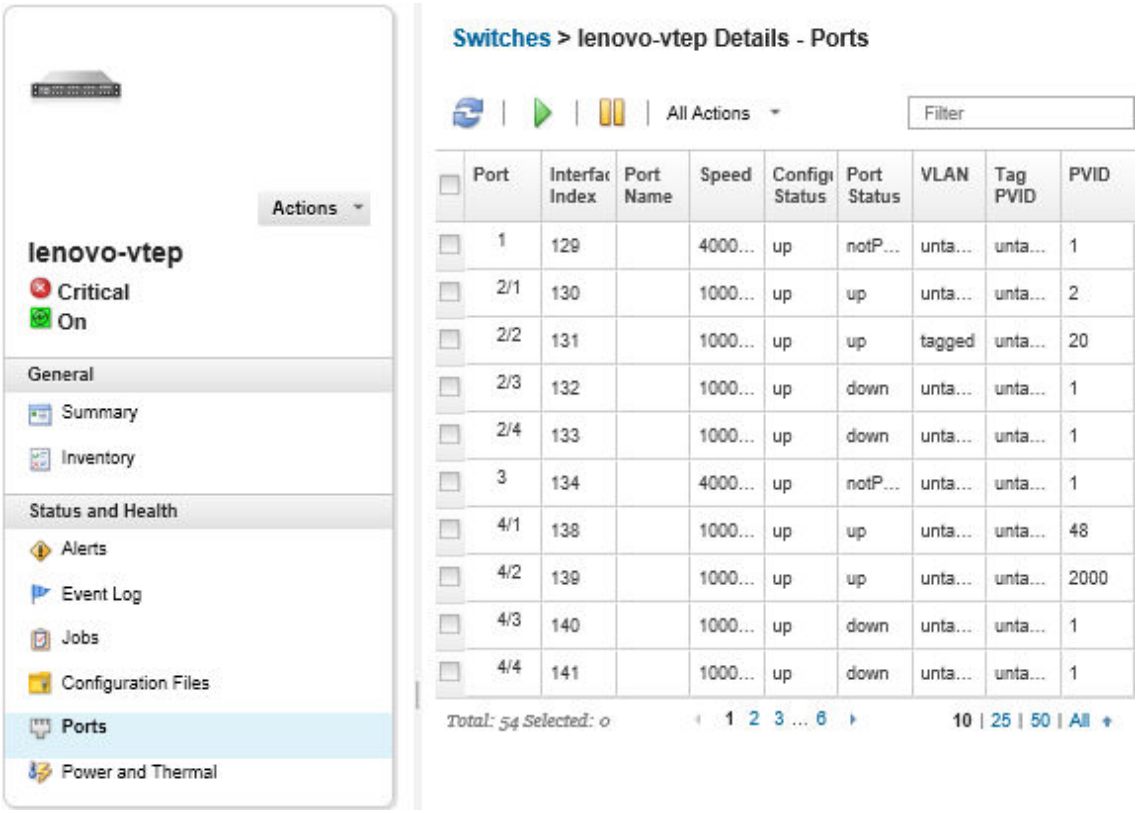
ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➞ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。

ステップ 3. スイッチのすべてのポートのステータスおよび構成を表示するには、左ナビゲーションの「**ポート**」をクリックします。

注：Flex スイッチの場合は、「**最新表示**」アイコン ( ) をクリックして現行のポート・データを収集します。データの収集には数分かかる場合があります。



ステップ 4. ポートを選択し、「**有効**」アイコン ( ) または「**無効**」アイコン ( ) をクリックします。

スイッチ構成データのバックアップと復元

Lenovo XClarity Administrator を使用して、RackSwitch および Flex System スイッチの構成データをバックアップおよび復元できます。スイッチ構成ファイルをローカル・システムにエクスポートしたり、スイッチ構成ファイルを XClarity Administrator にインポートすることもできます。

スイッチ構成データのバックアップ

Flex System または RackSwitch スイッチの構成データをバックアップできます。スイッチをバックアップする場合、構成データがターゲット・スイッチから Lenovo XClarity Administrator にスイッチ構成ファイルとしてインポートされます。

手順

管理対象スイッチの構成データをバックアップするには、以下の手順を実行します。

- 単一スイッチの場合:
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

     テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

  2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。
  3. 「**構成**」をクリックして、スイッチの構成ファイルを表示します。
  4. 「**構成データをバックアップ**」アイコン ( ) をクリックして、スイッチ構成をバックアップします。
  5. (オプション) スイッチ構成ファイルの名前を指定します。

     CNOS デバイスの場合、ファイル名に英数字と次の特殊文字を含めることができます: 下線 (_)、ハイフン (-)、ピリオド (.)。ENOS スイッチの場合、ファイル名に英数字と任意の特殊文字を含めることができます。

     ファイル名を指定しない場合、次のデフォルト名が使用されます。「*<switch_name>_<IP_address>_<timestamp>*.cfg.」
  6. (オプション) バックアップについて説明するコメントを追加します。
  7. 「**バックアップ**」をクリックしてスイッチ構成データを今すぐバックアップするか、「**スケジュール**」をクリックしてこのバックアップを後で実行するようにスケジュールします。

バックアップのスケジュールを選択した場合、「**上書き**」を選択すると、各ジョブの実行で同じファイルにスイッチ構成データをバックアップし、内容を上書きできます。ファイルを上書きしない場合は、以降のバックアップのファイル名に固有の番号が付加されます (たとえば、MyBackup_33.cfg など)。

注：バックアップのスケジュールでは、各スケジュール・ジョブに動的なファイル名またはコメントを選択することはできません。

- 複数のスイッチの場合:
  1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。
  2. スイッチを 1 つ以上選択します。
  3. 「**すべての操作**」 ➡ 「**構成**」 ➡ 「**構成ファイルのバックアップ**」 をクリックします。
  4. (オプション) スイッチ構成ファイルの名前を指定します。

     CNOS デバイスの場合、ファイル名に英数字と次の特殊文字を含めることができます: 下線 (_)、ハイフン (-)、ピリオド (.)。ENOS スイッチの場合、ファイル名に英数字と任意の特殊文字を含めることができます。

     ファイル名を指定しない場合、次のデフォルト名が使用されます。「*<switch_name>*_*<IP_address>*_*<timestamp>*.cfg.」
  5. (オプション) バックアップについて説明するコメントを追加します。
  6. 「**バックアップ**」をクリックしてスイッチ構成データを今すぐバックアップするか、「**スケジュール**」をクリックしてこのバックアップを後で実行するようにスケジュールします。

     バックアップのスケジュールを選択した場合、「**上書き**」を選択すると、各ジョブの実行で同じファイルにスイッチ構成データをバックアップし、内容を上書きできます。ファイルを上書きしない場合は、以降のバックアップのファイル名に固有の番号が付加されます (たとえば、MyBackup_33.cfg など)。

     注：バックアップのスケジュールでは、各スケジュール・ジョブに動的なファイル名またはコメントを選択することはできません。

終了後

バックアップ・プロセスが完了すると、スイッチ詳細ページの「**構成ファイル**」タブにスイッチ構成ファイルが追加されます。

このページでは、選択したスイッチ構成ファイルに対して以下の操作を実行できます。

- スイッチ構成ファイルを選択して「**構成データを復元**」アイコン () をクリックし、スイッチ構成を復元します。
- 「**削除**」アイコン () をクリックして、スイッチ構成ファイルを XClarity Administrator から削除します。
- ファイルを選択して「**構成ファイルをエクスポート**」アイコン () をクリックし、スイッチ構成ファイルをローカル・システムにエクスポートします。
- 「**構成ファイルをインポート**」アイコン () をクリックし、XClarity Administrator にスイッチ構成ファイルをインポートします。

スイッチ構成データの復元

Lenovo XClarity Administrator にバックアップまたはインポートされた Flex System または RackSwitch スイッチの構成データを復元できます。スイッチ構成ファイルが XClarity Administrator からターゲット・スイッチにダウンロードされ、構成が自動的に有効になります。

構成ファイルは、特定のスイッチに関連付けられます。構成ファイルは関連するスイッチでのみ復元できます。あるスイッチ用にバックアップされた構成ファイルを、別のスイッチの構成を復元するために使用することはできません。

手順

管理対象スイッチで構成データを復元するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。

ステップ 3. 「**構成ファイル**」をクリックして、スイッチの構成ファイルを表示します。

ステップ 4. スイッチで復元したいスイッチ構成ファイルを選択し、「**構成データを復元**」アイコン ( ) をクリックします。「復元」ダイアログが表示されます。

ステップ 5. (CNOS を実行するスイッチのみ)復元操作が完了したら、スイッチを再起動するかどうかを選択します。

スイッチを自動的に再起動しない場合は、復元された構成データをアクティブにするために CNOS スイッチを手動で再起動する必要があります。待機時間が長すぎ、保存処理が実行された場合 (たとえば、ポートが有効化または無効化されている場合)、復元処理は中断し、実行中の構成データが使用されます。

ステップ 6. 「**復元**」をクリックしてスイッチで構成データを今すぐ復元するか、「**スケジュール**」をクリックしてこの復元ジョブを後で実行するようにスケジュールします。

注：定期的な復元ジョブをスケジュールするときには注意してください。ご使用のスイッチが以前の構成にリセットする場合は、「スケジュール・ジョブ」ページでスケジュールされた復元ジョブを確認します。

スイッチ構成ファイルのエクスポートとインポート

スイッチ構成ファイルをローカル・システムにエクスポートしたり、スイッチ構成ファイルを Lenovo XClarity Administrator にインポートできます。

手順

管理対象スイッチの構成データをバックアップするには、以下の手順を実行します。

- スイッチ構成ファイルのエクスポート

1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

   テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。
3. 「**構成**」をクリックして、スイッチの構成ファイルを表示します。
4. エクスポートするスイッチ構成ファイルを選択します。
5. 「**構成ファイルをエクスポート**」アイコン ( ) をクリックして、スイッチ構成をバックアップします。

- スイッチ構成ファイルのインポート

1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

   テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

2. 「**スイッチ**」列でスイッチをクリックします。「要約」ページが開いて、プロパティと、そのスイッチに取り付けられたコンポーネントのリストが表示されます。
3. 「**構成**」をクリックして、スイッチの構成ファイルを表示します。

4. 「**構成ファイルをインポート**」アイコン ( ) をクリックして、スイッチ構成をバックアップします。
5. スイッチ構成ファイル名を入力するか、「**参照**」をクリックしてインポートするブート・ファイルを見つけます。
6. **オプション**: スイッチ構成ファイルの説明を入力します。
7. 「**インポート**」をクリックします。

   ファイルのアップロード中にアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

スイッチの管理コントローラー・インターフェースの起動

ENOS を実行している RackSwitch または Flex System スイッチの管理コントローラー Web インターフェースは、Lenovo XClarity Administrator から起動できます。

手順

スイッチの管理コントローラー・インターフェースを起動するには、以下の手順を実行します。

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

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. スイッチを選択し、「**すべての操作**」 ➡ 「**起動**」 ➡ 「**管理 Web インターフェースの起動**」の順にクリックします。スイッチの管理コントローラー Web インターフェースが表示されます。

ヒント: 「**IP アドレス**」列、およびスイッチ要約ページとスイッチ詳細ページの IP アドレス・リンクをクリックして管理コントローラー・インターフェースを起動することもできます。

ステップ 3. 管理コントローラー・インターフェースにログオンします。

ヒント: Flex スイッチの場合は、XClarity Administrator ユーザー資格情報を使用します。XClarity Administratorスイッチの場合は、スイッチ資格情報を使用します。

スイッチのリモート SSH セッションの起動

管理対象 RackSwitch または Flex スイッチのリモート SSH セッションを、Lenovo XClarity Administrator から起動できます。リモート SSH セッションから、コマンド・ライン・インターフェースを使用して XClarity Administrator では提供されていない管理タスクを実行できます。

始める前に

スイッチの構成で SSH が有効になっていることを確認します。RackSwitch スイッチの場合、スイッチが XClarity Administrator により管理されている場合は SSH は有効です。Flex スイッチの場合、SSH は通常デフォルトで有効です。有効になっていない場合は、XClarity Administrator によってスイッチが管理される前に有効にする必要があります。

手順

管理対象スイッチのリモート SSH セッションを起動するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、管理対象シャーシに取り付けられているすべてのスイッチがテーブル・ビューで表示されます。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 2. SSH セッションを起動するスイッチを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**起動**」 ➡ 「**SSH コンソール**」をクリックします。

ステップ 4. 必要に応じて、ユーザー ID とパスワードを使用してスイッチにログインします。

スイッチのシステム・プロパティの変更

特定の Flex System または RackSwitch スイッチのシステム・プロパティを変更できます。

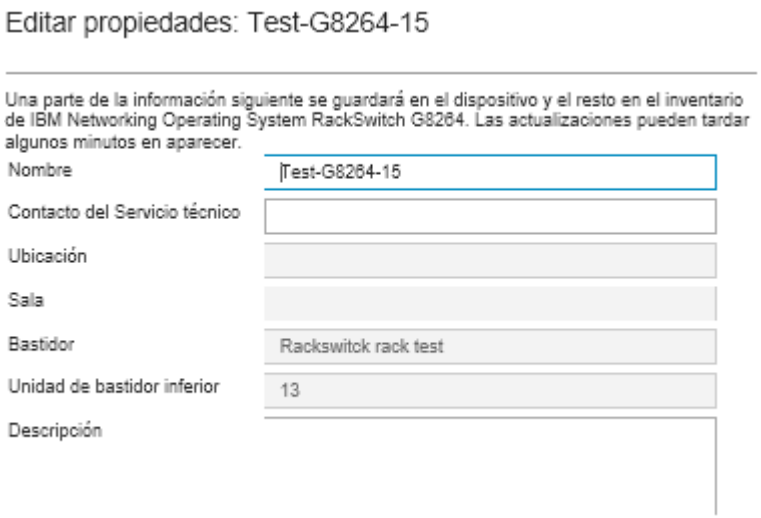
手順

以下の手順を実行して、システム・プロパティを変更します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**ハードウェア**」 ➡ 「**スイッチ**」の順にクリックして、「スイッチ」ページを表示します。

ステップ 2. 更新するスイッチを選択します。

ステップ 3. 「**すべての操作**」 ➡ 「**インベントリー**」 ➡ 「**プロパティの編集**」をクリックし、「編集」ダイアログを表示します。



ステップ 4. 以下の情報を必要に応じて変更します。
- スイッチ名
- サポート連絡先
- 説明

注：Web インターフェースのラックからデバイスを追加または削除する場合は、ロケーション、設置部屋、ラック、最下段ラック・ユニットのプロパティが XClarity Administrator によって更新されます (ラックの管理を参照)。

ステップ 5. 「**保存**」をクリックします。

注：変更されたプロパティが XClarity Administrator Web インターフェースに表示されるまで少し時間がかかる場合があります。

スイッチの有効期限切れまたは無効の保存された資格情報の解決

保存された資格情報が期限切れまたはデバイスで動作しない場合、そのデバイスのステータスは「オフライン」と表示されます。

手順

スイッチの有効期限切れまたは無効の保存された資格情報を解決するには、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、「**ハードウェア**」 → 「**スイッチ**」の順にクリックします。「スイッチ」ページが開いて、すべての管理対象スイッチがテーブル・ビューで表示されます。

ステップ 2. テーブル上部で「**電源**」列の見出しをクリックして、すべてのオフライン・スイッチをグループにします。

テーブルの列をソートすると、管理するスイッチを見つけやすくなります。「**フィルター**」フィールドにテキスト (システム名や IP アドレスなど) を入力して、表示されるスイッチを絞り込むこともできます。

ステップ 3. 解決するスイッチを選択します。

ステップ 4. 「**すべての操作**」 ➔ 「**セキュリティー**」 ➔ 「**保存された資格情報を編集**」をクリックします。

ステップ 5. 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。

注：同じ保存された資格情報を使用して複数のデバイスを管理しており、その保存された資格情報のパスワードを変更する場合、パスワードの変更は現在その保存された資格情報を使用しているすべてのデバイスに影響します。

管理サーバーの障害発生後のスイッチによる管理のリカバリー

管理対象から完全に除外されなかった (管理対象から除外している際に接続の問題が発生したり、管理元の Lenovo XClarity Administrator で障害が発生したりしたことなどにより) スイッチの管理をリカバリーできます。

手順

- 「**管理の強制**」オプションを使用して再度スイッチを管理します (スイッチの管理を参照)。
- 管理対象から完全に除外されず、再度管理対象となることがないスイッチで XClarity Administrator 固有の構成を永続的に削除するには、以下の手順を実行します。
  - 「**管理の強制**」オプションを使用して再度スイッチを管理し (スイッチの管理を参照)、次にスイッチを管理対象から除外して構成をクリーンアップします (のスイッチの管理解除を参照)。
  - (ENOS) スイッチ・コンソール・ポートや SSH または telnet セッションを使用してスイッチにログインし、指定された順序で以下の構成コマンドを実行してスイッチ構成をクリアします。

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

のスイッチの管理解除

Lenovo XClarity Administrator によってスイッチを管理対象から除外できます。このプロセスは*管理解除*と呼ばれます。

始める前に

XClarity Administrator を有効にすると、一定期間オフラインになっているデバイスを管理対象から自動的に解除できます。これはデフォルトで無効になっています。オフライン・デバイスの自動管理解除を有効にするには、XClarity Administrator メニューから「**ハードウェア**」 → 「**新しいデバイスの検出と管理**」をクリックし、「**管理除外オフライン・デバイスが無効**」の横の「**編集**」をクリックします。次に、「**管理除外オフライン・デバイスの有効化**」を選択し、時間間隔を設定します。デフォルトでは、デバイスは 24 時間オフラインになった後、管理解除されます。

スイッチを管理対象から除外する前に、そのスイッチに対して実行中のアクティブ・ジョブがないことを確認します。

このタスクについて

スイッチを管理対象から除外しても、XClarity Administrator にはそのスイッチに関する特定の情報が保持されます。この情報は、そのスイッチの管理を再開したときに再適用されます。

ヒント: 初期セットアップ中にオプションで追加されたすべてのデモ・デバイスは、シャーシ内のノードです。デモ・デバイスを管理対象から除外するには、「**デバイスに到達できない場合でも管理対象からの除外を強制する**」オプションを使用してシャーシを管理対象から除外します。

手順

スイッチを管理解除するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**ハードウェア**」 → 「**スイッチ**」の順にクリックして、「スイッチ」ページを表示します。

ステップ 2. 管理対象スイッチのリストから 1 つまたは複数のスイッチを選択します。

ステップ 3. 「**スイッチを管理対象から除外**」をクリックします。「管理対象から除外」ダイアログが表示されます。

ステップ 4. **オプション**: 「**デバイスに到達できない場合であっても、管理対象からの除外を強制します**」を選択します。

重要：デモ・ハードウェアを管理解除する場合は、このオプションを選択してください。

ステップ 5. 「**非管理**」をクリックします。
「管理対象から除外」ダイアログには、管理解除プロセスの各ステップの進行状況が表示されます。

ステップ 6. 管理解除プロセスが完了したら、「OK」をクリックします。

管理対象から正しく除外されなかったスイッチのリカバリー

スイッチが Lenovo XClarity Administrator の管理対象になっていて、XClarity Administrator に障害が発生した場合、管理サーバーの復元または交換を待たずに、管理機能を回復できます。

手順

- 「**管理の強制**」オプションを使用して再度スイッチを管理します (スイッチの管理を参照)。
- 管理対象から完全に除外されず、再度管理対象となることがないスイッチで XClarity Administrator 固有の構成を永続的に削除するには、以下の手順を実行します。
  - 「**管理の強制**」オプションを使用して再度スイッチを管理し (スイッチの管理を参照)、次にスイッチを管理対象から除外して構成をクリーンアップします (のスイッチの管理解除を参照)。
  - (ENOS) スイッチ・コンソール・ポートや SSH または telnet セッションを使用してスイッチにログインし、指定された順序で以下の構成コマンドを実行してスイッチ構成をクリアします。

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
```

```
no snmp-server target-address 16
no snmp-server user 16
```

第 11 章　構成パターンを使用したサーバーの構成

サーバー・パターンを使用すると、定義済み構成設定の単一のセットから複数のサーバー (ラックおよびタワー・サーバーと計算ノード) を迅速にプロビジョニングまたは事前プロビジョニングできます。

詳細:
- XClarity Administrator: ベア・メタルからクラスターへ
- XClarity Administrator: 構成パターン

始める前に

90 日間の無料トライアル期間の経過後も、引き続きハードウェアの管理や監視に XClarity Administrator を無料で使用できます。ただし、サーバー構成機能の使用を継続するには、XClarity Administrator の高度な機能をサポートする各管理サーバー向けの全機能有効化ライセンスを購入する必要があります。Lenovo XClarity Pro は、サービスおよびサポートに資格を提供し、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。詳しくは、XClarity Administrator オンライン・ドキュメントの全機能有効化ライセンスのインストールを参照してください。

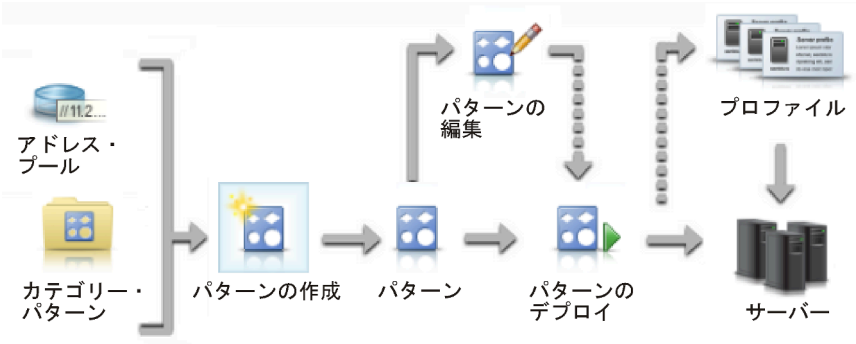
特定のサーバーの構成サポートに関する重要な情報について、構成に関する考慮事項を確認してください。

このタスクについて

XClarity Administrator のサーバー・パターンを使用すると、管理対象サーバーのローカル・ストレージ、I/O アダプター、ブート順序、およびその他のベースボード管理コントローラーと Unified Extensible Firmware Interface (UEFI) の設定を構成できます。また、サーバー・パターンは I/O アドレスの仮想化のサポートも統合しているため、サーバー・ファブリック接続を仮想化したり、ファブリック接続を中断せずにサーバーの再利用を実行したりできます。Fibre Channel アドレスを仮想化 (事前構成) して新しいハードウェアを受け取る前に、SAN ゾーニング変更要求を開始することもできます。

手順

次の図は、管理対象サーバーの構成のワークフローを示しています。実線の矢印はユーザーが実行する操作を、破線の矢印は XClarity Administrator によって自動的に実行される操作を示しています。



ステップ 1. **アドレス・プールを作成する。**
*アドレス・プール*とは、一連の定義済みアドレス範囲です。サーバー・パターンをサーバーにデプロイすると、Lenovo XClarity Administrator がアドレス・プールを使用して IP アドレスと I/O アドレスを個々のサーバーに割り当てます。

アドレス・プールの作成について詳しくは、アドレス・プールの定義を参照してください。

ステップ 2. **カテゴリー・パターンを作成する。**

*カテゴリー・パターン*は、関連するファームウェア設定をまとめてグループ化したもので、複数のサーバー・パターンで再利用できます。以下のファームウェア・カテゴリーのパターンを作成できます。

- システム情報
- 管理インターフェース
- デバイスおよび I/O ポート
- FC ブート・ターゲット
- I/O アダプター・ポート

カテゴリー・パターンについて詳しくは、サーバー・パターンの使用を参照してください。

ステップ 3. **サーバー・パターンを作成する。**

*サーバー・パターン*は、事前 OS サーバー構成を表します。これには、ローカル・ストレージ構成、I/O アダプター構成、ブート設定、その他のベースボード管理コントローラーおよび UEFI ファームウェア設定が含まれます。サーバー・パターンは、複数のサーバーを一度にすばやく構成する全体的なパターンとして使用されます。

データ・センターで使用するためのさまざまな構成を表す、複数のサーバー・パターンを定義できます。

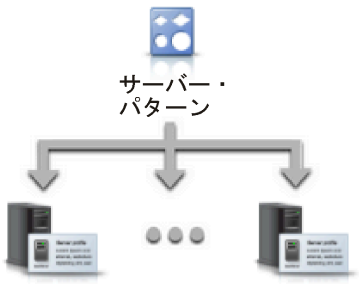
サーバー・パターンを定義するときに、必要に応じてカテゴリー・パターンおよびアドレス・プールを選択し、特定のサーバー・グループの希望する構成を構築できます。カテゴリー・パターンは、複数のサーバー・パターンで再利用できる関連構成設定をまとめてグループ化します。

コンバージド、Flex System、NeXtScale、および System x サーバーのサーバー・パターンを最初から作成して、ハードウェアが到着する前に希望する構成を定義できます。既存の管理対象サーバーからサーバー・パターンを作成することもできます。既存のサーバーからサーバー・パターンを作成すると、選択したサーバーのカテゴリー・パターンが XClarity Administrator によって学習されます。

サーバー・パターンの作成について詳しくは、サーバー・パターンの作成を参照してください。

ステップ 4. **サーバー・パターンをデプロイする。**

サーバー・パターンは、1 つ以上の個別のサーバーまたはサーバーのグループにデプロイできます。たとえば、サーバー・パターンをシャーシにデプロイすることで、そのシャーシ内のすべての計算ノードに同じ構成を適用できます。デプロイ中に、サーバー・パターンがデプロイされた各サーバーのサーバー・プロファイルが XClarity Administrator によって作成されます。各 *サーバー・プロファイル*は、1 つのサーバーの固有の構成を表し、サーバー・パターンから継承された設定と、サーバー固有の情報 (割り当てられた IP アドレスや MAC アドレスなど) を含んでいます。サーバー・プロファイルはサーバー・パターンの設定を継承するため、サーバー・パターンに変更を加えると、自動的にサーバー・プロファイルが更新されます。これにより、共通の構成を 1 か所で管理できます。



注：構成パターンを使用せず設定が変更された場合、またはデプロイメント中にファームウェアの問題または無効な設定が発生した場合、サーバーの設定がそのサーバー・プロファイルのコンプライアンス違反になります。「構成パターン: サーバー・プロファイル」ページから、各サーバーのコンプライアンス状況を調べることができます。

サーバー・パターンは以下の対象にデプロイできます。

- **既存のサーバー**。各サーバーのサーバー・プロファイルが作成されます。サーバー・プロファイルは、関連サーバーのリブート後にアクティブになります。
- **既存のシャーシの空のベイ**。空の各ベイのサーバー・プロファイルが作成されます。その後、空のベイに関連付けられたサーバー・プロファイルを、計算ノードが取り付けられた後にアクティブにできます。
- **まだ手元にないシャーシのプレースホルダー**。ハードウェアが到着する前に、サーバー・パターンのターゲットとして動作する*プレースホルダー・シャーシ*を定義することにより、まだ手元にないシャーシの計算ノードを事前プロビジョニングできます。プレースホルダー・シャーシを使用すると、空の計算ノード・ベイに対して作成されたすべてのサーバー・プロファイルを 1 つにまとめることができるため、ハードウェアが到着したら、その新しいシャーシにプレースホルダー・シャーシをデプロイすることで、その新しいシャーシのすべての計算ノードにサーバー・プロファイルを割り当てることができます。各サーバー・プロファイルは、関連付けられている計算ノードのリブート後にアクティブになります。

注：1 つのサーバー・パターンを複数のサーバーにデプロイできますが、複数のパターンを 1 つのサーバーにデプロイすることはできません。

サーバー・パターンのデプロイについて詳しくは、サーバーへのサーバー・パターンのデプロイおよびプレースホルダー・シャーシのデプロイを参照してください。

ステップ 5. **サーバー・パターンを編集する。**

サーバー・パターンを使用すると、共通の構成を 1 か所で制御できます。サーバーで直接設定を更新する必要はありません。代わりに、カテゴリー・パターンとサーバー・パターンを更新します。変更は、すべての関連プロファイルおよびそのサーバーに自動的にデプロイされます。

サーバー・パターンの編集について詳しくは、サーバー・パターンの変更を参照してください。

構成に関する考慮事項

Lenovo XClarity Administrator を使用してサーバーの構成を開始する前に、以下の重要な考慮事項を確認してください。

- サーバー・プロファイルに以前のファームウェア・レベルが含まれる場合に、ファームウェアをより新しいレベルに更新すると、XClarity Administrator は、保存されたプロファイル設定とサーバー設

定を比較し、「非適合」と報告します。「非適合」のステータスの上にカーソルを置くと、非準拠の理由を確認することができます。

デバイスを選択して「**すべての操作**」➔「**適合化**」をクリックすると、プロファイルを再デプロイせずに「非適合」デバイスのステータスを手動で「適合」に変更できます。

- サーバー上のファームウェア (UEFI、BMC、I/O コントローラーなど) をアップグレードした後、一部の構成が変更される可能性があります (たとえば、新しい項目の追加、既存の項目の削除、項目の値の範囲や動作の変更を行った場合など)。その結果、サーバー・プロファイルが非準拠になるか、以前のファームウェア・レベルを使用して作成した場合にサーバー・パターンを適用できない場合があります。この場合は、更新されたファームウェアに基づいて新しいパターンを学習するか、失敗したパターンを編集して特定の項目の構成を除外してから、そのパターンをサーバーに適用することをお勧めします。
- QLogic 8200 2-Port 10GbE SFP+ VFA アダプターには、iSCSIFirstTargetParameters_iSCSIName、iSCSISecondTargetParameters_iSCSIName および IPv6LinkLocalAddress の設定に対して無効な値があります。サーバーから構成パターンを学習する前、または学習した構成パターンの値を修正する前に、システム・セットアップでこれらの値を手動で訂正する必要があります。
- RAID アダプターが組み込まれている Flex System x240 および x440 計算ノードの場合、RAID 構成を定義するサーバー・パターンは、既存の RAID 構成がないサーバーだけにデプロイできます。既存の RAID 構成があるサーバーにサーバー・パターンをデプロイしても、既存のアレイとボリュームは上書きされません。サーバー・パターンで定義されている RAID 構成を適用するには、最初にサーバーの既存の RAID 構成をクリアした後 (ストレージ・アダプターのデフォルト値へのリセットを参照)、サーバーを選択して「**詳細**」➔「**サーバー・プロファイルのデプロイ**」をクリックし、サーバー・プロファイルを再デプロイする必要があります。
- Flex System x220、Flex System x222 および ThinkSystem サーバーのオンボード・ストレージ・コントローラーは、ソフトウェア・ベースの RAID をサポートします。ただし、構成パターンを使用したソフトウェア RAID の構成はサポートされません。
- 構成パターン を使用して RAID を構成する場合、サーバーの電源がオフであれば、サーバーは自動的にブートしてサーバー・プロファイルがアクティブ化される前に BIOS/UEFI Setup に入ります。
- ThinkServer サーバーで、構成パターン はサポートされていません。
- 特定の I/O デバイスは、サーバー・パターンを使用して構成することはできません。詳しくは、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。
- Flex スイッチ EN4093R、CN4093、SI4093、SI4091 で高度な機能 (SPAR、簡単な接続、スタックなど) が有効になっている場合、ネットワーク構成が内部ポートに正しく適用されないことがあります。
- デフォルトでは、Flex スイッチ SI4093 は SPAR が有効な状態で出荷されます。これらのスイッチの内部ポートにポート・パターンを使用してネットワーク設定をデプロイする場合は、スイッチの内部ポートを SPAR から、または SPAR 構成をスイッチから手動で削除する必要があります。
- 構成パターンを使用してコンバージドおよび ThinkAgile アプライアンスに構成するために、XClarity Administrator を使用 *しない* ことをお勧めします。
- すべての使用可能なポートと設定がパターンに含まれるように、構成パターンを作成する前に取り付けられたアダプターのすべての使用可能なポートが有効になっていることを確認します。必要な場合は、パターンで定義された適切な設定を使用してポートを無効にできます。パターンの作成時にポートが無効な場合、パターンが正しく作成されず、正常にデプロイされない可能性があります。

アドレス・プールの定義

*アドレス・プール*とは、一連の定義済みアドレス範囲です。サーバー・パターンをサーバーにデプロイすると、Lenovo XClarity Administrator がアドレス・プールを使用して IP アドレスと I/O アドレスを個々のサーバーに割り当てます。

このタスクについて

XClarity Administrator は、IP アドレス・プールと I/O アドレス・プールをサポートしています。

IP アドレス・プール

*IP アドレス・プール*は、サーバーのベースボード管理コントローラー・ネットワーク・インターフェースを構成するときに使用するための IP アドレスの範囲を定義します。事前定義済みのアドレス・プールを使用したりカスタマイズしたりできるほか、必要に応じて新しいプールを作成することもできます。サーバー・パターンを作成するときに、デプロイ時に使用する IP アドレス・プールを選択できます。サーバー・パターンがデプロイされると、選択したプールから IP アドレスが割り振られて、個々の管理コントローラーに割り当てられます。

注：現在の管理コントローラー・ネットワーク構成に満足している場合はこのオプションを使用しないでください。

注意：

- データ・センターの既存の I/O アドレスと競合しない IP アドレス副範囲を選択するようにしてください。
- 指定した範囲内の IP アドレスが同じサブ・ネットワークの一部であること、XClarity Administrator から到達可能であることを確認してください。
- アドレスの競合を回避するために、指定した範囲内の IP アドレスが各 XClarity Administrator ドメインおよび既存の IP 管理ツールに対して一意であることを確認してください。

アドレス・プール範囲全体は、指定されたルーティング・プレフィックスの長さに加え、ゲートウェイまたは開始範囲から取得されます。固有のルーティング・プレフィックスの長さに基づいて異なるサイズのプールを作成できますが、プール範囲全体は XClarity Administrator ドメイン内で一意である必要があります。次に、プール範囲全体から範囲を作成します。

アドレス範囲を使用することによって、オペレーティング・システムのタイプ、ワークロードのタイプ、ビジネスのタイプなどでホストを分離することができます。アドレス範囲を組織のネットワーク・ルールに結合することもできます。

イーサネット・アドレス・プール

*イーサネット・アドレス・プール*とは、サーバーを構成するときにネットワーク・アダプターに割り当てることのできる固有の MAC アドレスのコレクションです。定義済みのアドレス・プールを使用したり、必要に応じてカスタマイズしたりできるほか、新しいプールを作成することもできます。サーバー・パターンを作成するときに、デプロイ時に使用するイーサネット・アドレス・プールを選択できます。サーバー・パターンがデプロイされると、選択したプールからアドレスが割り振られて、個々のアダプター・ポートに割り当てられます。

以下の事前定義済み MAC アドレス・プールを使用できます。

- Lenovo MAC アドレス・プール

このプールの MAC アドレス範囲のリストについては、イーサネット・アドレス (MAC) プールを参照してください。

Fibre Channel アドレス・プール

*Fibre Channel アドレス・プール*とは、サーバーを構成するときに Fibre Channel アダプターに割り当てることのできる固有の WWNN/WWPN アドレスのコレクションです。定義済みのアドレス・プールを使用したり、必要に応じてカスタマイズしたりできるほか、新しいプールを作成することもできます。サーバー・パターンを作成するときに、デプロイ時に使用する Fibre Channel アドレス・プールを選択できます。サーバー・パターンがデプロイされると、選択したプールからアドレスが割り振られて、個々のアダプター・ポートに割り当てられます。

以下の事前定義済み Fibre Channel アドレス・プールを使用できます。

- LenovoWWN アドレス
- BrocadeWWN アドレス
- EmulexWWN アドレス
- QLogicWWN アドレス

これらのプールの WWN アドレス範囲のリストについては、Fibre Channel アドレス (WWN) プールを参照してください。

アドレス・プール内のアドレス範囲は XClarity Administrator ドメイン内で一意である必要があります。定義された範囲や割り当てられたアドレスが管理ドメイン内で一意であることを XClarity Administrator が確認します。

重要：複数の XClarity Administrator インスタンスを含む大規模な環境では、アドレスの重複を回避するために、各 XClarity Administrator が固有のアドレス範囲を使用するようにしてください。

イーサネット・アドレス・プールと Fibre Channel アドレス・プールは、組織で固有の I/O アドレスを割り当てるために I/O アダプターの仮想アドレス指定で使用されます。仮想アドレス指定は、計算ノードのサーバー・パターンを作成するときに、デバイスおよび I/O アダプターの構成の一部として有効にすることができます。仮想アドレス指定を有効にすると、アドレスの競合を回避するために、イーサネット・アドレス・プールと Fibre Channel アドレス・プールからアドレスが割り当てられます。

制限: 仮想アドレス指定は Flex System 計算ノードでのみサポートされています。スタンドアロン・ラック・サーバーおよびタワー・サーバーはサポートされていません。

サーバー・パターンの作成については、サーバー・パターンの作成を参照してください。

IP アドレス・プールの作成

*IP アドレス・プール*は、サーバーのベースボード管理コントローラーのネットワーク・インターフェースを構成するときに使用するための IP アドレスの範囲を定義します。関連付けられているサーバー・パターンがデプロイされると、指定したプールから IP アドレスが割り振られて、個々のサーバーに割り当てられます。

このタスクについて

「新しい IP アドレス・プール」ダイアログの「ネットワーク情報全体」テーブルのデータは、指定されたサブネット・マスクに加え、ゲートウェイまたは開始範囲から取得されます。特定のサブネット・マスクに基づいて異なるサイズのプールを作成できますが、プール範囲全体は管理ドメイン内で一意である必要があります。次に、プール範囲全体から範囲を作成します。すべての範囲は、同じサブ・ネットワークの一部である必要があります。また、「ネットワーク情報全体」テーブルに表示される限界によって制限されます。

プールと範囲は Lenovo XClarity Administrator スコープを持ちます。複数の XClarity Administrator インスタンスが存在する大規模な環境では、XClarity Administrator ごとに一意のプールと範囲を作成することによって、アドレスの競合を回避できるとともに、既存の IP 管理ツールとのアドレスの競合も回避できます。範囲を使用することによって、ホストを分離し (オペレーティング・システムのタイプ、ワークロードのタイプ、ビジネス機能などにより)、組織のネットワーク・ルールに結合することもできます。

手順

IP アドレス・プールを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**アドレス・プール**」の順にクリックします。「構成パターン: アドレス・プール」ページが表示されます。

ステップ 2. 「**IP アドレス・プール**」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 IP アドレス・プール・ウィザード」ダイアログが表示されます。

ステップ 4. 以下の情報を入力します。

- アドレス・プールの名前と説明を入力します。
- IPv4 アドレスを使用するか IPv6 アドレスを使用するかを選択します。

- サブネット・マスク (IPv4 の場合) またはルーティング・プレフィックスの長さ (IPv6 の場合) を選択します。
- ゲートウェイ・アドレスを指定します。指定したサブネット・マスクとゲートウェイまたは初期範囲に基づくネットワーク情報の値がテーブルに設定されます。
- 1 つ以上のアドレス範囲を追加します。
  1. 「**範囲の追加**」をクリックして、アドレス範囲を追加します。「IP アドレス範囲の新規追加」ダイアログが表示されます。
  2. 範囲の名前、最初のアドレス、および範囲のサイズを入力します。最後のアドレスは自動的に計算されます。
  3. 「**OK**」をクリックします。「**IP プールのアドレス範囲の定義**」テーブルに範囲が追加され、要約セクションのフィールドが自動的に更新されます。

  「**編集**」アイコン ( ) をクリックして範囲を編集したり、「**削除**」アイコン ( ) をクリックして範囲を削除したりできます。

ステップ 5. 「**作成**」をクリックします。

終了後

「IP アドレス・プール」ページのテーブルに新しい IP アドレス・プールが表示されます。

このページでは、選択したアドレス・プールに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、アドレス・プールを変更する。
- 「**名前変更**」アイコンをクリックして、アドレス・プールの名前を変更する。
- 「**削除**」アイコン ( ) をクリックして、アドレス・プールを削除する。
- 「**プール名**」列でプール名をクリックすることにより、仮想アドレスとインストールされたアダプターのポートおよび予約済み仮想アドレスの間のマッピングなど、アドレス・プールに関する詳細を表示します。

イーサネット・アドレス・プールの作成

*イーサネット・アドレス・プール*とは、ネットワーク・アダプターに割り当てることのできる固有のメディア・アクセス制御 (MAC) アドレスのコレクションです。定義済みのアドレス・プールを使用したり、必要に応じてカスタマイズしたりできるほか、新しいアドレス・プールを作成することもできます。サーバー・パターンを作成するときにイーサネット・アダプターの仮想アドレス指定を有効にすると、パターンのデプロイ時に使用するイーサネット・アドレス・プールを選択できます。関連付けられているサーバー・パターンがデプロイされると、選択したアドレス・プールから MAC アドレスが割り振られて、サーバーの個々のネットワーク・アダプターに割り当てられます。

手順

イーサネット・アドレス・プールを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**アドレス・プール**」の順にクリックします。「構成パターン: アドレス・プール」ページが表示されます。

ステップ 2. 「**イーサネット・アドレス・プール**」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。「新しいイーサネット (MAC) アドレス・プール」ダイアログが表示されます。

ステップ 4. アドレス・プールの名前と説明を入力します。

ステップ 5. 1 つ以上のアドレス範囲を追加します。

a. 「**範囲の追加**」をクリックして、アドレス範囲を追加します。「Ethernet (MAC) Address Range (イーサネット MAC アドレス範囲)」ダイアログが表示されます。

b. 範囲の名前、最初の MAC アドレス、および範囲のサイズを入力します。

最後の MAC アドレスは自動的に計算されます。

c. 「**追加**」をクリックします。

「**イーサネット (MAC) プール・アドレス範囲の定義**」テーブルに範囲が追加され、要約セクションのフィールドが自動的に更新されます。

「**編集**」アイコン ( ) をクリックして範囲を編集したり、「**削除**」アイコン ( ) をクリックして範囲を削除したりできます。

ステップ 6. 「**保存**」をクリックします。

終了後

「イーサネット・アドレス・プール」ページに新しいイーサネット・アドレス・プールが表示されます。

このページでは、選択したアドレス・プールに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、アドレス・プールを変更する。
- 「**名前変更**」アイコンをクリックして、アドレス・プールの名前を変更する。
- 「**削除**」アイコン ( ) をクリックして、アドレス・プールを削除する。
- 「**プール名**」列でプール名をクリックすることにより、仮想アドレスとインストールされたアダプターのポートおよび予約済み仮想アドレスの間のマッピングなど、アドレス・プールに関する詳細を表示します。

イーサネット・アドレス (MAC) プール

イーサネット・アドレス・プールとは、ネットワーク・アダプターに割り当てることのできる固有のメディア・アクセス制御 (MAC) アドレスのコレクションです。以下の事前定義済みのアドレス・プールをサーバー・パターンで使用できます。

表 3. Lenovo MAC アドレス・プール

事前定義済み範囲	開始アドレス	終了アドレス
範囲 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
範囲 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
範囲 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
範囲 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
範囲 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
範囲 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
範囲 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
範囲 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
範囲 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Fibre Channel アドレス・プールの作成

*Fibre Channel アドレス・プール*とは、Fibre Channel アダプターに割り当てることのできる固有のワールド・ワイド・ノード名 (WWNN) およびワールド・ワイド・ポート名 (WWPN) アドレスのコレクションです。定義済みのアドレス・プールを使用したり、必要に応じてカスタマイズしたりできるほか、新しいプールを作成することもできます。サーバー・パターンを作成するときにイーサネット・アダプターの仮想アドレス指定を有効にすると、パターンのデプロイ時に使用する Fibre Channel アドレス・プールを選択できます。関連付けられているサーバー・パターンがデプロイされると、そのプールから WWNN/WWPN アドレスが割り振られて、個々のサーバーに割り当てられます。

手順

Fibre Channel アドレス・プールを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**アドレス・プール**」の順にクリックします。「構成パターン: アドレス・プール」ページが表示されます。

ステップ 2. 「**Fibre Channel アドレス・プール**」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。「Fibre Channel アドレス・プール」ダイアログが表示されます。

ステップ 4. アドレス・プールの名前と説明を入力します。

ステップ 5. 1 つ以上のアドレス範囲を追加します。

a. 「**範囲の追加**」をクリックして、アドレス範囲を追加します。「Fibre Channel (WWN) アドレス範囲」ダイアログが表示されます。

b. 範囲の名前、範囲のサイズ、および各ファブリックの最初のアドレスを入力します。

最後のアドレスは自動的に計算されます。

c. 「**追加**」をクリックします。

「**Fibre Channel (WWN) プール・アドレス範囲の定義**」テーブルに範囲が追加され、要約セクションのフィールドが自動的に更新されます。

「**編集**」アイコン ( ) をクリックして範囲を編集したり、「**削除**」アイコン ( ) をクリックして範囲を削除したりできます。

ステップ 6. 「**保存**」をクリックします。

終了後

「Fibre Channel アドレス・プール」テーブルに新しい Fibre Channel アドレス・プールが表示されます。

このページでは、選択したアドレス・プールに対して以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、アドレス・プールを変更する。
- 「**削除**」アイコン ( ) をクリックして、アドレス・プールを削除する。
- 「**プール名**」列でプール名をクリックすることにより、仮想アドレスとインストールされたアダプターのポートおよび予約済み仮想アドレスの間のマッピングなど、アドレス・プールに関する詳細を表示します。

Fibre Channel アドレス (WWN) プール

Fibre Channel アドレス・プールとは、Fibre Channel アダプターに割り当てることのできる固有のワールド・ワイド・ノード名 (WWNN) およびワールド・ワイド・ポート名 (WWPN) アドレスのコレクションです。以下の事前定義済みのアドレス・プールをサーバー・パターンで使用できます。

330 ページの 表 4「Brocade WWN アドレス・プール」 は、Brocade ワールド・ワイド・ネーム (WWN) アドレス・プールの一覧です。各 Brocade 範囲に 1,864,135 個のアドレスが含まれています。

331 ページの 表 5「Emulex WWN アドレス・プール」 は、Emulex WWN アドレス・プールの一覧です。各 Emulex 範囲に 1,864,135 個のアドレスが含まれています。

332 ページの 表 6「Lenovo WWN アドレス・プール」 は、Lenovo WWN アドレス・プールの一覧です。各 Lenovo WWN 範囲に 116,508 個のアドレスが含まれています。

333 ページの 表 7「QLogic WWN アドレス・プール」 は、QLogic WWN アドレス・プールの一覧です。各 QLogic WWN 範囲に 116,508 個のアドレスが含まれています。

表 4. Brocade WWN アドレス・プール

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 開始アドレス	WWPN 終了アドレス
ファブリック A				
範囲 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6

表 4. Brocade WWN アドレス・プール (続き)

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 開始アドレス	WWPN 終了アドレス
範囲 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
範囲 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
範囲 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
範囲 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
範囲 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
範囲 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
範囲 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
範囲 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
ファブリック B				
範囲 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
範囲 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
範囲 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54
範囲 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
範囲 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
範囲 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
範囲 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
範囲 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
範囲 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

表 5. Emulex WWN アドレス・プール

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 開始アドレス	WWPN 終了アドレス
ファブリック A				
範囲 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
範囲 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
範囲 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
範囲 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
範囲 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
範囲 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
範囲 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
範囲 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
範囲 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
ファブリック B				
範囲 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
範囲 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D

表 5. Emulex WWN アドレス・プール (続き)

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 開始アドレス	WWPN 終了アドレス
範囲 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
範囲 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B
範囲 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
範囲 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
範囲 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
範囲 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
範囲 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

表 6. Lenovo WWN アドレス・プール

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 開始アドレス	WWPN 終了アドレス
ファブリック A				
範囲 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
範囲 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
範囲 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
範囲 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
範囲 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
範囲 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
範囲 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
範囲 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
範囲 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
ファブリック B				
範囲 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
範囲 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
範囲 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
範囲 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
範囲 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B
範囲 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
範囲 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
範囲 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
範囲 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

表 7. QLogic WWN アドレス・プール

事前定義済み範囲	WWNN 開始アドレス	WWNN 終了アドレス	WWPN 終了アドレス	WWPN 終了アドレス
ファブリック A				
範囲 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
範囲 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
範囲 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
範囲 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
範囲 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
範囲 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
範囲 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
範囲 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
範囲 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
ファブリック B				
範囲 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
範囲 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
範囲 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
範囲 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
範囲 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
範囲 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A:AA:A7
範囲 7	20:81:00:E0:8B:2A:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A:AA:A8	21:81:00:E0:8B:2C:71:C3
範囲 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
範囲 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F:FF:FB

サーバー・パターンの使用

*サーバー・パターン*は、事前 OS サーバー構成を表します。これには、ローカル・ストレージ、I/O アダプター、SAN ブート、その他のベースボード管理コントローラーおよび UEFI ファームウェア設定が含まれます。また、サーバー・パターンは I/O アドレスの仮想化のサポートも統合しているため、サーバー・ファブリック接続を仮想化したり、中断なしでサーバーの再利用を実行したりできます。サーバー・パターンは、複数のサーバーを一度にすばやく構成する全体的なパターンとして使用されます。

このタスクについて

データ・センターで使用するためのさまざまな構成を表す、複数のサーバー・パターンを定義できます。

サーバー・パターンを定義するときに、必要に応じてカテゴリー・パターンおよびアドレス・プールを選択または作成し、特定のサーバー・グループの希望する構成を構築できます。*カテゴリー・パターン*は、複数のサーバー・パターンで再利用できる特定のファームウェア設定を定義します。アドレス・プールを使用すると、サーバー・パターンのデプロイ時に各サーバーへのアドレスの割り当てに使用するアドレス範囲を定義できます。これらは、IP アドレス・プール、イーサネット・アドレス (MAC) プール、および Fibre Channel アドレス (WWN) プールです。

サーバー・パターンを複数のサーバーにデプロイすると、複数のサーバー・プロファイルが自動的に生成されます (各サーバーに 1 つのプロファイル)。各プロファイルは、親サーバー・パターンから設定を継承します。これにより、共通の構成を 1 か所で制御できます。

サーバー・パターンを最初から作成して、ハードウェアが到着する前に希望する構成を定義することも、既存のサーバーからサーバー・パターンを作成し、そのパターンを使用して残りのサーバーをプロビジョニングすることもできます。既存のサーバーからサーバー・パターンを作成すると、そのサーバーの現在の設定が学習されて、拡張カテゴリー・パターンが動的に作成されます。カテゴリーの設定を変更する場合は、直接サーバー・パターンで編集できます。

注意：新しいサーバー・パターンを最初から作成する際には、サーバーのブート設定を定義する必要があります。そのサーバー・パターンをサーバーにデプロイすると、サーバーの既存のブート順序がサーバー・パターンのデフォルトのブート順序設定で上書きされます。サーバー・パターンをデプロイした後にサーバーが起動しなくなった場合は、元のブート設定が新しいサーバー・パターンのデフォルトのブート順序設定で上書きされたことが原因と考えられます。サーバーの元のブート設定を復元するには、サーバー・パターンのデプロイ後のブート設定のリカバリーを参照してください。

重要：サーバー・パターンを作成する際には、サーバー・タイプごとに作成するようにしてください。たとえば、すべての Flex System x240 計算ノード用のサーバー・パターンと、すべての Flex System x440 計算ノード用のサーバー・パターンを作成します。別のサーバー・タイプ用のサーバー・パターンをデプロイしないようにしてください。

重要：管理ノードで障害が発生すると、サーバー・パターンが失われる可能性があります。サーバー・パターンを作成または変更した後は、必ず管理ソフトウェアをバックアップしてください (Lenovo XClarity Administrator のバックアップを参照)。

ネットワーク・デバイスの設定

一部の Flex System ネットワーク・デバイスには、サーバー・パターンに他のネットワーク・デバイスより多くの構成オプションが用意されています。

サーバー・パターンは任意のネットワーク・デバイスに適用できますが、特定のネットワーク・アダプターに限定されている機能もあります。また、イーサネット・ネットワーク・アダプターの詳細設定の中には、現在サポートされていないものもあります (アダプターおよびポートの互換性の設定など)。

サーバー・パターンを使用すると、サポートされているネットワーク・アダプターの既存の構成データと構成設定を学習したり、パターン・デプロイメントを通して構成設定を変更したりできます。

カテゴリー・パターン

ファームウェア設定は、関連する設定をまとめるカテゴリーに分類されています。各カテゴリーについて、共通のファームウェア設定を含む*カテゴリー・パターン*を作成して、複数のサーバー・パターンで再利用できます。ベースボード管理コントローラーや UEFI で直接構成できるファームウェア設定のほとんどは、カテゴリー・パターンでも構成できます。使用できるファームウェア設定は、サーバー・タイプ、現在の Flex System 環境、およびサーバー・パターンのスコープによって異なります。

カテゴリー・パターンは、サーバー・パターンとは別に作成できます。

カテゴリー・パターンには、事前定義済みカテゴリー・パターン、既存のサーバーから学習されるカテゴリー・パターン、およびユーザー定義カテゴリー・パターンがあります。

- **拡張カテゴリー・パターン**

  *拡張カテゴリー・パターン*とは、特定の管理対象サーバーから学習されて動的に作成される、I/O アダプター・ポート、拡張 Unified Extensible Firmware Interface (UEFI)、およびベースボード管理コントローラー (BMC) の一部の設定のパターンです。これらのパターンは、既存のサーバーからサーバー・パ

ターンを作成すると Lenovo XClarity Administrator によって作成されます。拡張カテゴリー・パターンを手動で作成することはできませんが、作成後にパターンを編集することはできます。

次の拡張 UEFI パターンは、特定の環境に合わせてサーバーが最適化されるように XClarity Administrator により事前定義されます。

- **ESXi のインストール・オプション**
- **効率 - パフォーマンス優先**
- **効率 -電力優先**
- **最大パフォーマンス**
- **最小電力**

- **ユーザー定義カテゴリー・パターン**

  *ユーザー定義カテゴリー・パターン*とは、ユーザーが作成できるパターンで、システム情報、管理インターフェース、デバイスおよび I/O ポート、Fibre Channel ブート・ターゲット、I/O アダプター・ポートなどがあります。作成できるカテゴリー・パターンを以下に示します。

  - 「**システム情報**」。システム名の自動生成、場所、連絡先などの設定が含まれています。
  - **管理インターフェース**。管理インターフェースのホスト名の自動生成、IP アドレス、ドメイン・ネーム・スペース (DNS)、インターフェース速度、ポートの割り当てなどの設定が含まれています。デュプレックス設定はサーバー・パターンでサポートされていません。
  - 「**デバイスおよび I/O ポート**」。コンソール・リダイレクトおよび COM ポートなどの設定が含まれています。サーバー・パターンを使用すると、「コンソール・リダイレクト」領域で Serial over LAN を有効にすることができますが、Serial over LAN を有効にすると、サーバー・パターンでサポートされるシリアル・ポート・アクセス・モードの設定が「**専用**」のみになり、「**共用**」および「**プリブート**」の IPMI 設定は使用できなくなります。

    重要：既存のサーバーからサーバー・パターンを作成した場合、そのサーバーのシリアル・ポート・アクセス・モードが「**共用**」または「**プリブート**」に設定されていても、そのサーバーから学習されたデバイスおよび I/O ポート・パターンのシリアル・ポート・アクセス・モードは「**専用**」に設定されます。
  - **Fibre Channel ブート・ターゲット**。プライマリーとセカンダリーの Fibre Channel WWN ブート・ターゲットなどの設定が含まれています。
  - **ポート**。ファブリック・インターコネクトを構成するための I/O アダプターおよびポートなどの設定が含まれています。

サーバー・パターンの作成

サーバー・パターンを作成する際には、特定のサーバー・タイプの構成の特性を定義します。サーバー・パターンは、デフォルト設定を使用して最初から作成することも、既存のサーバーの設定を使用して作成することもできます。

このタスクについて

サーバー・パターンを作成する前に、以下のアドバイスについて検討してください。

- サーバー・パターンを初めて作成するときには、既存のサーバーから作成することを検討してください。既存のサーバーからサーバー・パターンを作成すると、I/O アダプター・ポート、UEFI、およびベースボード管理コントローラーの一部の設定の拡張カテゴリー・パターンが Lenovo XClarity Administrator によって学習および作成されます。これらのカテゴリー・パターンは、後で作成するサーバー・パターンで使用できるようになります。カテゴリー・パターンについて詳しくは、ファームウェア設定の定義を参照してください。
- 同じハードウェア・オプションを持ち、同じように構成する必要があるサーバーのグループを特定します。サーバー・パターンを使用すると、複数のサーバーに同じ構成設定を適用できるため、共通の構成を 1 か所から制御できます。

- サーバー・パターンでカスタマイズする必要がある構成を特定します (ローカル・ストレージ、ネットワーク・アダプター、ブート設定、管理コントローラー設定、UEFI 設定など)。
- ローカル・ユーザー・アカウントを管理したり、構成パターンを使用して LDAP サーバーを構成することはできません。

重要：管理ノードで障害が発生すると、サーバー・パターンが失われる可能性があります。サーバー・パターンを作成または変更した後は、必ず管理ソフトウェアをバックアップしてください (XClarity Administrator オンライン・ドキュメントのLenovo XClarity Administrator のバックアップ)。

手順

サーバー・パターンを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」 ページが表示されます。

ステップ 2. 「**サーバー・パターン**」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。「新しいサーバー・パターン・ウィザード」が表示されます。

ステップ 4. サーバー・パターンを作成するには、次のいずれかの操作を実行します。

- 既存のサーバーの設定を使用するには、「**既存のサーバーからの新しいパターンの作成**」をクリックします。その後、表示されるリストで、新しいパターンのベースとして使用する管理対象サーバーを選択します。

  既存のサーバーからサーバー・パターンを作成すると、XClarity Administrator が指定された管理対象サーバーの設定 (拡張ポート、UEFI、ベースボード管理コントローラーの設定など) を学習し、それらの設定のカテゴリー・パターンを動的に作成します。新しいサーバーの場合、Lenovo XClarity Administrator は出荷時の設定を学習します。XClarity Administrator でサーバーが管理されている場合、XClarity Administrator はカスタマイズされた設定を使用します。その後、このパターンをデプロイするサーバーに合わせてそれらの設定をカスタマイズできます。
- デフォルト設定を使用するには、「**新しいパターンを最初から作成**」をクリックします。その後、「**フォーム・ファクター**」フィールドでサーバー・タイプを選択します。

注：パターンを作成するサーバーのタイプに応じて、残りのタブに表示されるオプションが異なる場合があります。

ステップ 5. パターンの名前と説明を入力します。

ステップ 6. 「**カスタム**」トグルを選択してから、名前付けスキームに含める 1 つ以上の要素 (カスタム・テキスト、サーバー名、増分番号など) および順序を選択して、サーバー・プロファイル名をカスタマイズします。

ステップ 7. 「**次へ**」をクリックします。

ステップ 8. このパターンをサーバーにデプロイするときに適用するローカル・ストレージの構成を選択し、「**次へ**」をクリックします。

ローカル・ストレージの設定については、ローカル・ストレージの定義を参照してください。

ステップ 9. **オプション**: I/O アダプター・アドレス指定を変更し、このパターンで構成するハードウェアに合わせて追加の I/O アダプターを定義して、「**次へ**」をクリックします。

I/O アダプターの設定については、I/O アダプターの定義を参照してください。

ステップ 10. このパターンをサーバーにデプロイするときに適用するブート順序を定義して、「**次へ**」をクリックします。

SAN ブート・ターゲットの設定については、ブート・オプションの定義を参照してください。

ステップ 11.既存のカテゴリー・パターンのリストからファームウェア設定を選択します。

新しいカテゴリー・パターンを作成するには、「**作成**」アイコン ( ) をクリックします。

ファームウェア設定については、ファームウェア設定の定義を参照してください。

ステップ 12.「**保存**」をクリックしてパターンを保存します。パターンを保存してすぐに 1 つ以上のサーバーにデプロイする場合は、「**保存してデプロイ**」をクリックします。

サーバー・パターンのデプロイについて詳しくは、サーバーへのサーバー・パターンのデプロイを参照してください。

終了後

「**保存してデプロイ**」をクリックした場合は、「サーバー・パターンのデプロイ」ページが表示されます。このページでは、サーバー・パターンを特定のサーバーにデプロイできます。

「**保存**」をクリックした場合は、サーバー・パターンとすべてのカテゴリー・パターンが「サーバー・パターン」ページに保存されます。

構成パターン: パターン

このページでは、選択したサーバー・パターンに対して以下の操作を実行できます。

- 「**名前**」列でパターン名をクリックして、パターンの詳細を表示する。
- パターンをデプロイする (サーバーへのサーバー・パターンのデプロイを参照してください)。
- 「**コピー**」アイコン ( ) をクリックしてパターンをコピーする。
- パターンを編集する (XClarity Administrator オンライン・ドキュメントのサーバー・パターンの変更を参照)。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- サーバー・パターンをエクスポートおよびインポートする (サーバー・パターンおよびカテゴリー・パターンのエクスポートとインポートを参照)。

ローカル・ストレージの定義

このパターンをデプロイしたときにターゲット・サーバーに適用されるローカル・ストレージ構成を定義できます。

このタスクについて

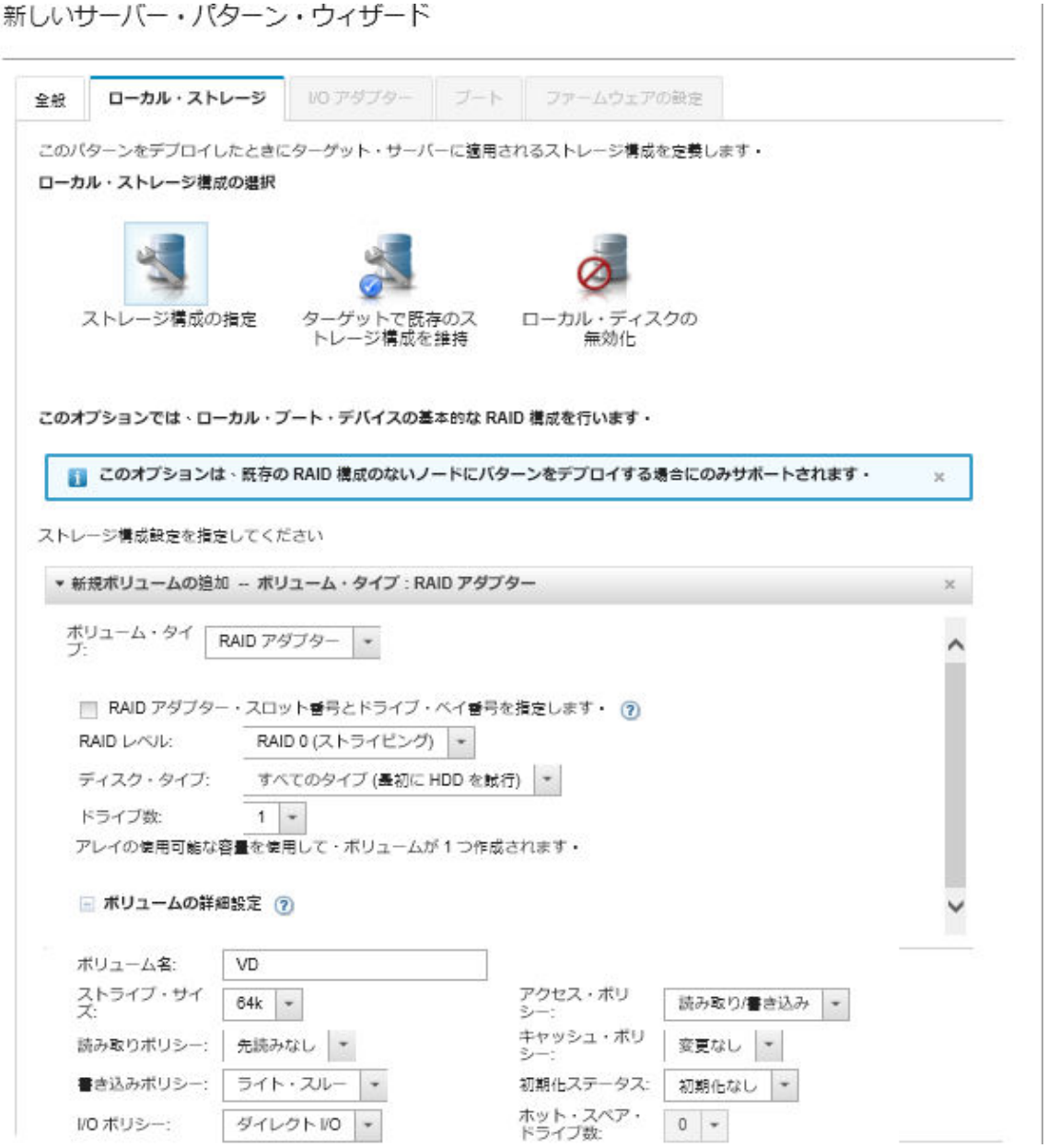
注：

- Flex System x220、Flex System x222 および ThinkSystem サーバーのオンボード・ストレージ・コントローラーは、ソフトウェア・ベースの RAID をサポートします。ただし、構成パターンを使用したソフトウェア RAID の構成はサポートされません。
- 構成パターン を使用して RAID を構成する場合、サーバーの電源がオフであれば、サーバーは自動的にブートしてサーバー・プロファイルがアクティブ化される前に BIOS/UEFI Setup に入ります。

手順

ローカル・ストレージの構成を定義するには、以下の手順を実行します。

ステップ 1. 新しいサーバー・パターン・ウィザードで、「**ローカル・ストレージ**」タブをクリックします。



ステップ 2. ローカル・ストレージの設定を定義するには、次のいずれかのオプションを選択します。

- **ストレージ構成の指定**。(既存の RAID 構成を含まないデバイスのみ) 基本的な RAID 設定は、デプロイメント中にローカル・ブート・デバイスで構成されます。

  ストレージ・オプションに基づいてストレージ構成を指定します。「**追加**」をクリックして追加のストレージ・オプションを追加できます (➕) アイコンをクリックして他のボリューム・タイプを追加できます。

  - **RAID アダプター**。サーバーに取り付けられているドライブの RAID レベル、特性、および数を選択します。RAID 0、1、5 がサポートされます。さらに、ストライプ・サイズ、ポリシー、ホット・スペア・ドライブ数など、詳細なボリュームの設定を選択できます。

    XCC バージョン 2.1 以降を含む ThinkSystem サーバーでは (ThinkSystem SR950 では XCC バージョン 1.4 以降が必要)、RAID アダプター・スロット番号とドライブ・ベイ番号を指定することでアレイ容量を使用して 1 つのボリュームを作成することもできます。この場合、RAID レベル 0、1、5、6、10、50、60、および 00 がサポートされます。さらに、ストライプ・サイズ、ポリシー、ホット・スペア・ドライブなど、詳細なボリュームの設定を選択できます。

    注：ターゲット・サーバーで、指定されたタイプの使用可能なドライブが十分にあることを確認し、ドライブの RAID の状態がサーバーの「インベントリー詳細」ページの「**ドライブ**」セクションで未構成で良好と報告されていることを確認します (Lenovo XClarity Administrator オンライン・ドキュメントの管理対象サーバーの詳細の表示を参照)。
  - **Lenovo SD メディア・アダプター**。ボリューム・サイズとボリュームを作成する場所を選択します。メディア・タイプ、アクセス・ポリシーなど、詳細なボリューム設定を指定できます。
  - **ThinkSystem M.2 (ミラーリングあり)**。PCI スロット、RAID レベル、ボリューム名、ストライプ・サイズを選択して、使用可能なアレイ容量に基づいて 1 つのボリュームを作成します。

    - それぞれ異なる PCI スロットに装着されているミラーリング・ストレージ・アダプターを使用して複数の ThinkSystem M.2 を定義できます。
    - ThinkSystem Edge サーバーの場合、特定の PCI スロット番号を指定する必要があります。M.2 RAID アダプターが 1 つしか取り付けられていないその他の ThinkSystem サーバーでは、「最初に一致」(デフォルト値) を選択するか、特定の PCI スロット番号を指定することができます。
  - **Intel Optane DC 永続メモリー**。永続メモリーのタイプ、残容量のパーセンテージの警告しきい値、およびメモリーとして使用する合計容量のパーセンテージを選択します(残りのメモリーは、永続ストレージとして使用されます)。

    注意：
    - Intel Optane DC永続メモリー DIMM を構成するには、セキュリティーを無効にする必要があります。また、名前空間を作成することはできません。
    - セキュリティーの有効化は、サーバー内のすべての Intel Optane DC 永続メモリー DIMM に対してセキュリティー状態が「無効」の場合にのみサポートされます。
    - セキュリティー状態が「ロック済み」で、サーバー内のすべての Intel Optane DC 永続メモリー DIMM に対して「パスフレーズ」が同じ場合にのみ、セキュリティーの無効化およびセキュアな消去がサポートされます。
    - Intel Optane DC PMEM セキュリティーの状態は、XClarity Administrator インベントリーには含まれません。UEFI のセキュリティーの状態は、手動で確認できます。
- 「**ターゲットで既存のストレージ構成を維持**」。デプロイメント中には、既存のストレージの構成は変更されません。ターゲット・サーバーの既存のストレージ構成を使用するには、このオプションを選択します。
- 「**Disable local disk**」。(Flex System x240 計算ノード のみ) デプロイメント中にオンボード・ストレージ・コントローラーとストレージ・オプション ROM (UEFI と Legacy の両方)

を無効にします。ローカル・ディスク・ドライブを無効にすると、SAN からブートするときにブート時間全体を短縮できます。

I/O アダプターの定義

このパターンをデプロイしたときにターゲット・サーバーに適用される I/O ポート設定とアドレス指定モードを定義できます。

このタスクについて

I/O アダプター・アドレスを仮想化または再割り当てする場合は、仮想 I/O アダプター・アドレス指定を使用するようにこのパターンを構成できます。

既存のサーバーからパターンを作成すると、一部のアダプター情報を自動的に学習します。このパターンをデプロイするサーバーのハードウェアと一致するように、追加の I/O アダプター・パターンを定義できます。I/O アダプター・パターンを定義することにより、サポートされるアダプターのアダプター・ポートの設定を構成できます。仮想 I/O アダプター・アドレス指定を使用する場合は、追加する Fibre Channel アダプターの SAN ブート・ターゲットを定義することもできます (ブート・オプションの定義を参照)。

手順

I/O アダプターの設定を定義するには、以下の手順を実行します。

ステップ 1. 新しいサーバー・パターン・ウィザードで、「**I/O アダプター**」タブをクリックします。

注：「**詳細設定**」をクリックして、I/O アダプターに関する追加情報を表示できます。

ステップ 2. Flex System シャーシ内のサーバーのサーバー・パターンを作成する場合、I/O アダプター・アドレス指定モードのタイプを選択します。

- 「**出荷時書き込み**」。製造時にアダプターに付与されたワールド・ワイド・ネーム (WWN) およびメディア・アクセス制御 (MAC) の既存のアドレスを使用します。
- 「**仮想**」。仮想 I/O アダプター・アドレス指定を使用して、LAN の接続および SAN の接続の管理を簡素化します。I/O アドレスを仮想化すると、出荷時書き込みハードウェア・アドレスが仮想化されたファイバー WWN およびイーサネット MAC アドレスで再割り当てされます。これにより、SAN のゾーン・メンバーシップを事前構成することでデプロイメントの時間を短縮でき、ハードウェアの交換時に SAN のゾーニングと LUN のマスキングの割り当ての再構成を不要にすることによってフェイルオーバーを容易にできます。

  仮想アドレス指定を有効にすると、デフォルトでは、定義されているアダプターに関係なく、イーサネットと Fibre Channel の両方のアドレスが割り当てられます。イーサネット・アドレスと Fibre Channel アドレスの割り当て元のプールを選択できます。

アドレス指定モードの横にある「**編集**」アイコン () をクリックして、仮想アドレスの設定を編集することもできます。

制限: 仮想アドレス指定は、Flex System シャーシ内のサーバーでのみサポートされています。ラック・サーバーとタワー・サーバーはサポートされていません。

ステップ 3. Flex System シャーシ内のサーバーのサーバー・パターンを作成する場合、以下のスケーラビリティ・オプションのいずれかを選択します。テーブル内の行は、選択内容に基づいて変化します。
- 非スケーラブル Flex System
- 2 ノード非スケーラブル Flex System
- 4 ノード非スケーラブル Flex System

ステップ 4. このパターンをデプロイするサーバーに取り付けられていると予想される I/O アダプターを選択します。アダプターを追加するには、以下の手順を実行します。

a. テーブルの「**I/O アダプターの追加**」リンクをクリックして、「I/O アダプター 1 または LOM の追加」ダイアログを表示します。

b. アダプターの PCI スロットを選択します。

c. テーブルからアダプター・タイプを選択します。

注：デフォルトでは、テーブルには管理対象サーバーに現在取り付けられている I/O アダプターのみがリストされています。すべてのサポート対象 I/O アダプターをリストするには、「**サポートされているすべてのアダプター**」をクリックします。

d. パターンのデプロイ時にポート・グループのすべてのポートに割り当てる開始ポート・パターンを選択します。

*ポート・パターン*は、サーバーから学習したポート設定を変更するために使用されます。最初にアダプターを追加する場合には、これらの開始ポート・パターンが割り当てられます。アダプターが追加されたら、個々のポートに対し、「I/O アダプター」ページから異なるパターンを割り当てることができます。

ポート・パターンを作成するには、「**作成**」アイコン () をクリックします。既存のパターンに基づいてポート・パターンを作成するには、「**編集**」アイコン () をクリックします。

ポート・パターンについて詳しくは、ポート設定の定義を参照してください。

e. 「**追加**」をクリックして、ポート・パターンを「I/O アダプター」ページのテーブルに追加します。

ブート・オプションの定義

このパターンをデプロイするときにターゲット・サーバーに適用するブート順序を定義できます。

手順

ブート・オプション・パターンを作成するには、以下の手順を実行します。

ステップ 1. 新しいサーバー・パターン・ウィザードで、「**Boot**」タブをクリックします。

ステップ 2. 以下のシステム・ブート・モードから、いずれかを選択します。

- 「**UEFI Only ブート**」。Unified Extensible Firmware Interface (UEFI) をサポートしているサーバーを構成するには、このオプションを選択します。UEFI 対応オペレーティング・システムをブートする場合は、このオプションを選択すると、Legacy オプション ROM が無効になり、ブート時間を短縮できます。

  パターンが Thinksystem サーバーから学習された場合、「**プライマリー・ブート順序**」タブをクリックしてブート順序を指定できます。パターンをデプロイするサーバーで指定されているブート順序を保持するか、ブート順序を構成してブート・オプションを適用する順序を指定することができます。ただし、デバイス・グループ (ブート・オプション) に含まれているブート・デバイスのブート優先順位はサポートされていません。

- 「**最初に UEFI、次に Legacy**」。最初に UEFI を使用してブートするようにサーバーを構成するには、このオプションを選択します。問題があった場合は Legacy モードでブートします。

  パターンが Thinksystem サーバーから学習された場合、「**プライマリー・ブート順序**」タブをクリックしてブート順序を指定できます。パターンをデプロイするサーバーで指定されているブート順序を保持するか、ブート順序を構成してブート・オプションを適用する順序を指定することができます。ただし、デバイス・グループ (ブート・オプション) に含まれているブート・デバイスのブート優先順位はサポートされていません。

- **Legacy Only ブート**。レガシー (BIOS) ファームウェアを必要とするオペレーティング・システムをブートするようにサーバーを構成する場合は、このオプションを選択します。このオプションを選択するのは、UEFI 未対応オペレーティング・システムを起動する場合だけです。

  ヒント: Legacy Only ブート・モード (ブート時間が大幅に短縮されます) を選択する場合は、Features on Demand (FoD) キーをアクティブにすることはできません。

  このオプションを選択した場合、次のオプションを指定できます。

  - 「**プライマリー・ブート順序**」。パターンをデプロイするサーバーで指定されているブート順序を保持するように選択します。Legacy Only ブート順序を構成するように選択して、ブート・オプションを適用する順序を指定することもできます。
  - 「**Wake on LAN (WOL) ブート順序**」。パターンをデプロイするサーバーで指定されている現在の WOL ブート順序を保持するように選択します。Legacy Only ブート順序を構成するように選択して、WOL ブート・オプションを適用する順序を指定することもできます。

- 「**既存のブート・モードを維持**」。ターゲット・サーバーの既存の設定を保持するには、このオプションを選択します。パターンをデプロイするときにブート順序は変更されません。

ステップ 3. 「**SAN ブート**」タブを選択し、ブート・ターゲット・パターンを選択して、ブート・デバイス・ターゲットを指定します。

注：I/O アダプターを定義したときに、Fibre Channel アダプターを定義して仮想アドレス指定を有効にした場合は、Fibre Channel アダプターのプライマリーとセカンダリーの SAN ブート・ターゲットを設定できます。ストレージ・ターゲットのワールド・ワイド・ポート名 (WWPN) と論理装置番号 (LUN) 識別子は複数指定できます。

ファームウェア設定の定義

このパターンをデプロイしたときにターゲット・サーバーに適用するベースボード管理コントローラーおよび UEFI ファームウェア設定を指定できます。

このタスクについて

ファームウェア設定は、関連する設定をまとめるカテゴリーに分類されています。各カテゴリーについて、共通のファームウェア設定を含む*カテゴリー・パターン*を作成して、複数のサーバー・パターンで再利用できます。ベースボード管理コントローラーや UEFI で直接構成できるファームウェア設定のほとんどは、カテゴリー・パターンでも構成できます。使用できるファームウェア設定は、サーバー・タイプ、現在の Flex System 環境、およびサーバー・パターンのスコープによって異なります。

カテゴリー・パターンには、事前定義済みカテゴリー・パターン、ユーザー定義カテゴリー・パターン、および既存のサーバーから学習されるカテゴリー・パターンがあります。

- *拡張カテゴリー・パターン*とは、特定の管理対象サーバーから学習されて動的に作成される、I/O アダプター・ポート、拡張 Unified Extensible Firmware Interface (UEFI)、およびベースボード管理コントローラー (BMC) の一部の設定のパターンです。これらのパターンは、既存のサーバーからサーバー・パターンを作成すると Lenovo XClarity Administrator によって作成されます。拡張カテゴリー・パターンを手動で作成することはできませんが、作成後にパターンを編集することはできます。
- *ユーザー定義カテゴリー・パターン*とは、ユーザーが作成できるパターンで、システム情報、管理インターフェース、デバイスおよび I/O ポート、Fibre Channel ブート・ターゲット、I/O アダプター・ポートなどがあります。

手順

ファームウェアの設定を定義するには、以下の手順を実行します。

ステップ 1. 新しいサーバー・パターン・ウィザードで、「**ファームウェアの設定**」タブをクリックします。

ステップ 2. 定義する設定を含むカテゴリー・パターン・タイプを選択します。

- 「**システム情報**」。システム名の自動生成、連絡先の名前、および場所を定義するには、このカテゴリー・パターンを使用します。システム情報パターンについて詳しくは、システム情報設定の定義を参照してください。
- 「**管理インターフェース**」。ホスト名の自動生成、管理 IP アドレス割り当て、ドメイン・ネーム・システム (DNS) 設定、およびインターネット速度設定を定義するには、このカテゴリー・パターンを使用します。管理インターフェース・パターンについて詳しくは、管理インターフェース設定の定義を参照してください。
- 「**デバイスおよび I/O ポート**」。コンソール・リダイレクトおよび COM ポート、PCIe 速度、オンボード・デバイス、アダプター・オプション ROM、およびオプション ROM 実行順序を定義するには、このカテゴリー・パターンを使用します。デバイスおよび I/O ポート・パターンについて詳しくは、デバイスおよび I/O ポート設定の定義を参照してください。
- 「**拡張 BMC**」。その他のベースボード管理コントローラーの設定を定義するには、このカテゴリー・パターンを使用します。既存のサーバーからサーバー・パターンを作成すると、拡張管理コントローラー・パターンが自動的に作成されます。拡張管理コントローラー・パターンを手動で作成することはできません。管理インターフェース・パターンについて詳しくは、拡張管理コントローラー設定の定義を参照してください。
- 「**拡張 UEFI**」。その他の Unified Extensible Firmware Interface (UEFI) の設定を定義するには、このカテゴリー・パターンを使用します。既存のサーバーからサーバー・パターンを作成すると、拡張 UEFI パターンが自動的に作成されます。拡張 UEFI パターンを手動で作成することはできません。管理インターフェース・パターンについて詳しくは、拡張 UEFI 設定の定義を参照してください。

ステップ 3. そのカテゴリー・パターン・タイプの横にある「**作成**」アイコン ( ) をクリックして、新しいカテゴリー・パターンを作成します。

または、特定のパターンをドロップダウン・リストから選択し、そのカテゴリー・パターン・タイプの横にある「**編集**」アイコン ( ) をクリックすることによって、既存のカテゴリー・パターンを編集することもできます。また、パターンを編集し、「**名前を付けて保存**」をクリックして新しい名前で保存することにより、既存のカテゴリー・パターンをにコピーすることもできます。

システム情報設定の定義

システム情報パターンを作成することで、システム名、連絡先、場所の情報を定義することができます。

手順

システム情報パターンを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**システム情報パターン**」垂直タブをクリックし、「**作成**」アイコン ( ) をクリックします。

ヒント: 新しいシステム情報パターンは、「新しいサーバー・パターン」ウィザードの「ファームウェアの設定」ページで、「**システム情報**」の選択ボックスの横にある「**作成**」アイコンをクリックして作成することもできます。

ステップ 4. 「新しいシステム情報パターン」ダイアログで、以下の情報を指定します。

- パターンの名前と説明を入力します。
- システム名を自動的に生成するかどうかを選択します。「**カスタム**」をクリックすると、パターンのデプロイ時に名前を生成する方法を指定できます。「**無効**」をクリックすると、パターンのデプロイ時に各サーバーのシステム名は変更されません。ほとんどのデバイスで、名前の長さは英字 256 文字にベースボード管理コントローラーによって制限されています。自動的に生成された名前は、256 文字までで切り捨てられます。

- このサーバーの連絡先担当者とサーバーの場所を指定します。

  注：SNMP が有効になっている場合は、連絡先とシステムの場所を指定する必要があります。

ステップ 5. 「**作成**」をクリックします。

結果

「構成パターン: カテゴリー・パターン」ページの「**システム情報パターン**」タブに新しいパターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**編集**」アイコン ( ) をクリックして現在のパターン設定を変更する。
- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

管理インターフェース設定の定義

管理インターフェース・パターンを作成することで、管理インターフェースのホスト名、IP アドレス、ドメイン・ネーム・システム (DNS)、インターフェース速度、およびポートの割り当てを定義できます。

手順

管理インターフェース・パターンを作成するには、以下の手順を実行します。

注：デュプレックス設定はサーバー・パターンでサポートされていません。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**管理インターフェース・パターン**」垂直タブをクリックし、「**作成**」アイコン ( ) をクリックします。

ヒント: 新しい管理インターフェース・パターンは、「新しいサーバー・パターン」ウィザードの「ファームウェアの設定」ページで、「**管理インターフェース**」の選択ボックスの横にある「**作成**」アイコン ( ) をクリックして作成することもできます。

ステップ 4. 「新しい管理インターフェース・パターン」ダイアログで、以下の情報を指定します。

- パターンの名前と説明を入力します。
- 「**ホスト名**」タブをクリックし、ホスト名を自動的に生成するかどうかを選択します。「**カスタム**」をクリックすると、パターンのデプロイ時に名前を生成する方法を指定できます。「**無効**」をクリックすると、パターンのデプロイ時に各サーバーのホスト名は変更されません。

  ホスト名の長さは、ベースボード管理コントローラーによって英数字 63 文字に制限されています。自動的に生成された名前は、63 文字までで切り捨てられます。
- 「**管理 IP アドレス**」タブをクリックし、IPv4 アドレスと IPv6 アドレスの設定を構成します。

  IPv4 アドレスに対しては、次のいずれかのオプションを選択できます。
  - 「**DHCP サーバーから動的 IP アドレスを取得する**」。
  - **最初は DHCP から取得します。**DHCP を試して、成功しない場合はアドレス・プールから静的 IP アドレスを取得する。
  - 「**アドレス・プールから静的 IP アドレスを取得する。**」

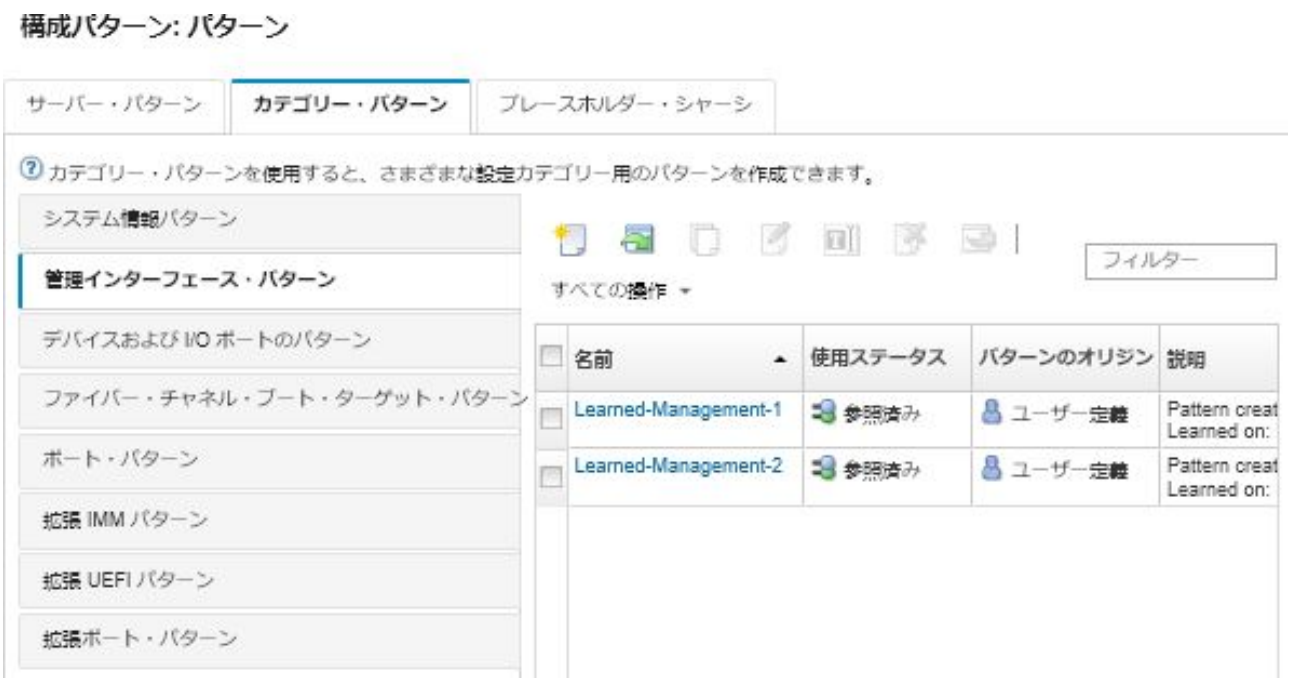
  IPv6 アドレスに対しては、次のいずれかのオプションを選択できます。
  - 「**ステートレス・アドレス自動構成を使用する**」。
  - 「**DHCP サーバーから動的 IP アドレスを取得する**」。
  - 「**アドレス・プールから静的 IP アドレスを取得する**」。

  「**ドメイン・ネーム・システム (DNS)**」タブで、ダイナミック・ドメイン・ネーム・サービス (DDNS) を有効にするか無効にするかを選択します。DDNS を有効にする場合は、次のいずれかのオプションを選択できます。
  - DHCP サーバーからドメイン名を取得します。
  - ドメイン名を指定してください。
- 「**インターフェース設定**」タブをクリックし、最大伝送単位 (MTU) を指定します。デフォルトは 1500 です。
- 「**ポートの割り当て**」タブをクリックし、以下のポートに使用する番号を指定します。
  - HTTP
  - HTTPS
  - Telnet CLI
  - SSH CLI
  - SNMP エージェント
  - SNMP トラップ
  - リモート制御コンソール
  - CIM over HTTP
  - CIM over HTTPS

ステップ 5. 「**作成**」をクリックします。

結果

「構成パターン: カテゴリー・パターン」ページの「**管理インターフェース・パターン**」タブに新しいパターンが表示されます。



このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**編集**」アイコン ( ) をクリックして現在のパターン設定を変更する。
- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

デバイスおよび I/O ポート設定の定義

デバイスおよび I/O ポート・パターンを作成することで、コンソール・リダイレクトを有効にしたり、COM 1 ポートの特性を有効にして定義したりできます。

手順

デバイスおよび I/O ポート・パターンを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**デバイスおよび I/O ポートのパターン**」垂直タブをクリックし、「**作成**」アイコン ( ) をクリックします。

ヒント: 新しいデバイスおよび I/O ポートのパターンは、「新しいサーバー・パターン」ウィザードの「ファームウェアの設定」ページで、「**デバイスおよび I/O ポート**」の選択ボックスの横にある「**作成**」アイコン ( ) をクリックして作成することもできます。

ステップ 4. 「新しいデバイスおよび I/O ポート・パターン」ダイアログで、以下の情報を指定します。

- パターンの名前と説明を入力します。
- コンソール・リダイレクトを有効にするか無効にするかを選択します。コンソール・リダイレクトを有効にする場合は、以下のオプションを有効にするか無効にするかを選択できます。
  - 「Serial over LAN」。

  - 「**サービス・プロセッサーのリダイレクト**」。サービス・プロセッサーのリダイレクトを有効にした場合、レガシー・オプション・シリアル・データ・ポートで COM ポート 1 または 2 を使用することを選択できます。無効な場合、常に COM ポート 1 が使用されることに注意してください。以下のいずれかの CLI モードを選択することもできます。
    - 無効にする
    - ユーザー定義キー・ストローク・シーケンスを有効化する
    - EMS 互換キー・ストローク・シーケンスを有効化する
- COM ポート 1 と 2 を有効にするか無効にするかを選択します。COM ポートを有効にする場合は、以下の設定を指定します。
  - ボー・レート
  - データ・ビット
  - パリティ
  - ストップ・ビット
  - テキスト・エミュレーション
  - ブート後アクティブ
  - フロー制御

ステップ 5. 「**作成**」をクリックします。

結果

「構成パターン: カテゴリー・パターン」ページの「**デバイスおよび I/O ポート・パターン**」タブに新しいパターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**編集**」アイコン ( ) をクリックして現在のパターン設定を変更する。
- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

Fibre Channel ブート・ターゲット設定の定義

Fibre Channel ブート・ターゲット・パターンを作成することで、ローカル・ディスク・ドライブではなくストレージ・エリア・ネットワーク (SAN) デバイスからブートするようにサーバーを構成できます。

手順

Fibre Channel ブート・ターゲット・パターンを作成するには、以下の手順を実行します。

制限: Fibre Channel ブート・ターゲットは Flex 計算ノードでのみサポートされています。スタンドアロン・ラック・サーバーおよびタワー・サーバーはサポートされていません。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**Fibre Channel ブート・ターゲット・パターン**」垂直タブをクリックし、「**作成**」アイコン ( ) をクリックします。

ステップ 4. 「新しい Fibre Channel ブート・ターゲット・パターン」ダイアログで、以下の情報を指定します。

- パターンの名前と説明を入力します。
- プライマリー・ブート・ターゲットとして使用する WWPN アドレスと LUN 識別子を 1 つ以上指定します。必要に応じて、セカンダリー・ブート・ターゲットとして使用する WWPN アドレスと LUN 識別子を指定することもできます。

  たとえば、ストレージのプライマリー・パスをプライマリー・ターゲットとして追加し、ストレージのセカンダリー・パスをセカンダリー・ターゲットとして追加することができます。サーバー・パターンごとに異なるターゲット・グループを使用すると、複数のホストから同時にブート要求が送られてきた場合にストレージの負荷を分散することができます。

  ヒント: WWPN に「00:00:00:00:00:00:00:00」を指定すると、XClarity Administrator は、最初に見つかったターゲットからブートします。

ステップ 5. 「**作成**」をクリックします。

結果

「構成パターン: カテゴリー・パターン」ページの「**Fibre Channel ブート・ターゲット・パターン**」タブに新しいパターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**編集**」アイコン ( ) をクリックして現在のパターン設定を変更する。
- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

ポート設定の定義

ポート・パターンを作成することで、特定のタイプの I/O アダプターの標準的なポート設定を定義できます。

このタスクについて

ポート・パターンのネットワーク設定を使用してスイッチの内部ポートを構成します。ただし、ポート・パターンを使用してスイッチの共通設定 (VLAN ID、グローバル UFP モード、グローバル CEE モード、グローバル FIP など) を構成することはできません。ポート・パターンをデプロイする前に、デプロイする内部ポート・パターンと互換性のある共通設定を、以下のルールを使用して手動で構成する必要があります。ポート・パターンを使用して PVID のタグ付けを構成することもできます。共通設定と内部ポート設定の互換性を確認する方法と、ご使用のスイッチに対してこれらの設定を構成する方法については、そのスイッチに付属のドキュメントを参照してください。

- PFC を構成する場合、「**globalCEEState**」が「オン」であることを確認します。
- vport が「FCoE」モードに設定されている場合、「**globalCEEState**」が「オン」であることを確認します。
- FIP を構成する場合、「**globalCEEState**」が「オン」であり、「**globalFIPsState**」が「オン」であることを確認します。
- スイッチの内部ポート・モードが「UFP」モードに設定されている場合、「**globalUFPMode**」が「有効」であることを確認します。

- ポートを特定の VLAN に追加する前に、VLAN ID が作成されていることを確認します。

手順

I/O アダプター・ポート・パターンを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**ポート・パターン**」垂直タブをクリックし、「**作成**」アイコン () をクリックします。

ヒント: 新しいポート・パターンは、「I/O アダプターの追加」ページで、「**開始ポート・パターン**」の選択ボックスの横にある「**作成**」アイコン () をクリックして作成することもできます。

ステップ 4. 「新しいポート・パターン」ダイアログで、以下の情報を指定します。

- パターンの名前と説明を入力します。
- アダプターとポートの互換性に関する以下の設定を指定します。アダプターとポートにパターンを割り当てる際に、ターゲットとなるアダプターやポートとの互換性に基づいてパターン設定がフィルタリングされます。
  - ターゲット・アダプター・タイプ
  - 以下のターゲット・ポートの動作モード
    - pNIC モード
    - vNIC 仮想ファブリック・モード
    - vNIC スイッチ独立モード
    - vNIC 統合ファブリック・プロトコル・モード

    これらの設定は、NIC の仮想化を有効にします。詳しくは、Flex System Fabric Solutions での NIC の仮想化を参照してください。
  - 以下を含むターゲット・ポートのプロトコル:
    - イーサネットのみ
    - イーサネットおよび FCoE
    - イーサネットおよび iSCSI
  - ポート拡張設定パターン。サーバーから学習された追加のポート設定を構成するために使用されます。
- ターゲット・ポートの動作モードを「**pNIC モード**」に設定した場合、該当すれば、対応する設定を Flex スイッチの内部ポートに適用するように選択します。選択する場合は、以下の追加の VLAN 設定と詳細設定を構成できます。
  - ターゲット・ポートのプロトコルを指定します。
  - ターゲット・ポートのプロトコルを「**イーサネットおよび FCoE**」に設定した場合、オプションで優先度 2 の ID を選択して指定します。
- ターゲット・ポートの動作モードを「**vNIC 仮想ファブリック・モード**」に設定した場合、各機能のタイプや VLAN タグなど、物理機能設定を構成します。
- ターゲット・ポートの動作モードを「**vNIC スイッチ独立モード**」に設定した場合、有効な各機能についてタイプ、最小帯域幅、および VLAN タグを構成します。該当する場合には、対応する設定を Flex スイッチの内蔵ポートに適用することもできます。選択した場合は、以下の追加スイッチ内部ポートおよび詳細設定を構成できます。
  - オペレーティング・システムがタグの付いていないパケットを送信するときにのみ使用されるデフォルトの LAN を指定する。
  - VLAN のコンマ区切りのリストを指定する。
  - 手動制御を構成するように選択してトリガーを指定する。

  - 以下のフロー制御タイプを選択します。
    - 既存のフロー制御の保持
    - 優先度ベースのフロー制御
    - リンク・レベル・フロー制御

    これらのフロー制御タイプの詳細については、Flex スイッチに付属するドキュメントを参照してください。
- ターゲット・ポートの動作モードを「**vNIC 統合ファブリック・プロトコル・モード**」に設定した場合、該当すれば、対応する設定を Flex スイッチの内部ポートに適用するように選択します。選択する場合は、以下の追加の UFP 機能と詳細設定を構成できます。
  - QoS モードを指定します (帯域幅または優先順位)。
  - デフォルトの VLAN ID タグ付けを有効にし、有効な各機能についてモード、最小帯域幅、VLAN タグを指定します。
  - レイヤー 2 の障害について構成し、各機能のトリガーの数を指定します。
  - 帯域幅 QoS モードで、フロー制御タイプを指定します (優先順位ベース、リンク・レベル、または既存のフロー制御)。
  - 帯域幅 QoS モードで、iSCSI が選択されているときに優先順位 4 を有効にするかどうかを選択します。

  注：フェイルオーバー のトリガーを定義した場合、グローバル・フェイルオーバーが「On」であることを確認します。

ステップ 5. 「**作成**」をクリックします。

結果

「構成パターン: カテゴリー・パターン」ページの「**ポート・パターン**」タブに新しいパターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**編集**」アイコン ( ) をクリックして現在のパターン設定を変更する。
- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。

- 「**名前変更**」アイコン () をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

拡張管理コントローラー設定の定義

拡張ベースボード管理コントローラーの設定は、特定の管理対象サーバーから学習されて動的に作成されます。これらのパターンは、既存のサーバーからサーバー・パターンを作成すると Lenovo XClarity Administrator によって作成されます。拡張管理コントローラー・パターンを手動で作成することはできませんが、既に作成されているパターンをコピーして変更することはできます。

始める前に

注：IMM の温度設定は、UEFI の動作モードの設定と競合する可能性があります。競合した場合は、デバイスの再起動時に UEFI 設定によって IMM 設定が上書きされ、拡張ベースボード管理コントローラー・パターンで定義した温度設定はコンプライアンス対象外になります。非準拠の問題を解決するには、拡張ベースボード管理コントローラー・パターンから設定を削除するか、現在の UEFI の動作モード設定と競合しない設定を選択します。

手順

拡張管理コントローラー・パターンを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**拡張 BMC パターン**」垂直タブをクリックします。

ステップ 4. 変更するパターンを選択し、「**編集**」アイコン () をクリックします。

ステップ 5. 適切なフィールドを変更します。

「**設定の包含/除外**」をクリックして、カテゴリー・パターンに含める設定を選択します。

- DNS 設定を構成するには、「**ネットワーク設定インターフェイス**」 → 「**DNS 構成**」の順にクリックします。DNS を有効にして、IP プロトコルを選択し、最大 3 つの IPv4 または IPv6 アドレスを指定すると、XClarity Administrator IP アドレスの検出を有効にすることができます。

  注：Flex System デバイスの場合、XClarity Administrator サーバーの検出に使用する IP アドレスのみを構成できます。

- NTP 設定を構成するには、「**ネットワーク設定インターフェイス**」 → 「**統合済みモジュール NTP 設定**」の順にクリックします。最大 4 個の NTP サーバーのホスト名と頻度を指定できます。

  注：Flex System デバイスの場合、NTP 設定を構成することはできません。

- (ラック・サーバーのみ) データおよび時刻の設定については、「**全般設定**」 → 「**統合済みモジュールのクロック設定**」をクリックします。タイム・ゾーン (UTC オフセット) を指定するか、夏時間 (DST) を有効または無効にするか、ホストで UTC を使用するか、現地時間を使用するかを選択できます。
- ユーザー・アカウントのセキュリティー設定を変更するには、「**アカウントのセキュリティー構成**」をクリックします。

ステップ 6. 「**保存**」をクリックして変更を現在のカテゴリー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいカテゴリー・パターンに保存します。

結果

「構成パターン: カテゴリー・パターン」ページの「**拡張 BMC パターン**」タブに変更されたカテゴリー・パターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

拡張 UEFI 設定の定義

拡張 Unified Extensible Firmware Interface (UEFI) の設定は、特定の管理対象サーバーから学習されて動的に作成されます。これらのパターンは、既存のサーバーからサーバー・パターンを作成すると Lenovo XClarity Administrator によって作成されます。拡張 UEFI パターンを手動で作成することはできませんが、既に作成されているパターンをコピーして変更することはできます。

このタスクについて

次の拡張 UEFI パターンは、特定の環境に合わせてサーバーが最適化されるように Lenovo XClarity Administrator により事前定義されます。

- **ESXi のインストール・オプション**
- **効率 - パフォーマンス優先**
- **効率 -電力優先**
- **最大パフォーマンス**
- **最小電力**

注：

- 拡張 UEFI パターンを使用すると、UEFI セキュリティー設定の変更 (セキュア・ブート、Trusted Platform Module (TPM)、物理プレゼンス・ポリシー構成) はサポートされません。
- 「サーバー」ページで選択した ThinkSystem サーバーと ThinkAgile サーバーの UEFI 管理者パスワードを変更するには、「**すべての操作**」 ➡ 「**セキュリティー**」 ➡ 「**UEFI 管理者パスワード**」をクリックします。Lenovo XClarity Controllerファームウェア・レベル 20A が必要です。

手順

拡張 UEFI パターンを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**拡張 UEFI パターン**」垂直タブをクリックします。

ステップ 4. 変更するパターンを選択し、「**編集**」アイコン ( ) をクリックします。

ステップ 5. 適切なフィールドを変更します。

「**設定の包含/除外**」をクリックして、カテゴリー・パターンに含める設定を選択します。

ステップ 6. 「**保存**」をクリックして変更を現在のカテゴリー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいカテゴリー・パターンに保存します。

結果

「構成パターン: カテゴリー・パターン」ページの「**拡張 UEFI パターン**」タブに変更されたカテゴリー・パターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

拡張ポート設定の定義

拡張ポート設定は、特定の管理対象サーバーから学習されて動的に作成されます。これらのパターンは、既存のサーバーからサーバー・パターンを作成すると Lenovo XClarity Administrator によって作成されます。拡張ポート・パターンを手動で作成することはできませんが、既に作成されているパターンをコピーして変更することはできます。

このタスクについて

XClarity Administrator は、以下の定義済みの拡張ポート・パターンを備えています。

- **仮想ファブリックのバランスが取れたイーサネット**。仮想ファブリック・モード vNIC モード (イーサネットのみ) の、Lenovo により提供されるポート・パターン。

Mellanox および Broadcom の I/O アダプターでは、一部のデバイス・レベルの設定を、すべてのポートで同じ値に設定する必要があります。別のポートの設定が異なる値に設定されている場合、1 つのポートの設定が使用され、他のポートの設定はコンプライアンスから除外されます。不適合の問題を解決するには、それらのデバイス・レベル設定で同じ値を選択します。

Mellanox I/O アダプターの場合、以下の設定は、すべてのポートで同じ値に設定する必要があります。
- 詳細な電源設定
- アドバタイズされた PCI 仮想関数
- スロット電源リミッター
- 仮想化モード

Broadcom I/O アダプターの場合、以下の設定は、すべてのポートで同じ値に設定する必要があります。
- バナー・メッセージ・タイムアウト
- BW の限度
- BW 制限有効
- BW 予約
- BW 予約有効
- PME 機能を有効にします
- PF MSI X ベクターの最大数
- 多機能モード
- VF あたりの MSI X ベクターの数
- PF あたりの VF の数
- オプションの ROM
- SR-IOV
- RDMA のサポート

手順

拡張ポート・パターンを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**拡張ポート・パターン**」垂直タブをクリックします。

ステップ 4. 変更するパターンを選択し、「**編集**」アイコン ( ) をクリックします。

ステップ 5. 適切なフィールドを変更します。

「**設定の包含/除外**」をクリックして、カテゴリー・パターンに含める設定を選択します。

ステップ 6. 「**保存**」をクリックして変更を現在のカテゴリー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいカテゴリー・パターンに保存します。

結果

「構成パターン: カテゴリー・パターン」ページの「**拡張ポート・パターン**」タブに変更されたカテゴリー・パターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

拡張済み SR635/SR655 BIOS 設定の定義

拡張済み SR635/SR655 BIOS 設定は、特定の管理対象サーバーから学習して動的に作成されます。既存の ThinkSystem SR635 または SR655 サーバーからサーバー・パターンを作成すると、Lenovo XClarity Administrator がこれらのパターンを作成します。拡張済み SR635/SR655 BIOS パターンを手動で作成することはできませんが、既に作成されているパターンをコピーして変更することはできます。

手順

拡張済み SR635/SR655 BIOS パターンを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**拡張済み SR635/SR655 BIOS パターン**」垂直タブをクリックします。

ステップ 4. 変更するパターンを選択し、「**編集**」アイコン ( ) をクリックします。

ステップ 5. 適切なフィールドを変更します。

「**設定の包含/除外**」をクリックして、カテゴリー・パターンに含める設定を選択します。

ステップ 6. 「**保存**」をクリックして変更を現在のカテゴリー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいカテゴリー・パターンに保存します。

結果

「構成パターン: カテゴリー・パターン」ページの「**拡張済み SR635/SR655 BIOS パターン**」タブに変更されたカテゴリー・パターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

拡張 ThinkServer CPlus BIOS 設定の定義

拡張 ThinkServer CPlus BIOS 設定は、特定の管理対象サーバーから学習して動的に作成されます。既存の ThinkServer CPlus サーバーからサーバー・パターンを作成すると、Lenovo XClarity Administrator がこれらのパターンを作成します。拡張 ThinkServer CPlus BIOS パターンを手動で作成することはできませんが、既に作成されているパターンをコピーして変更することはできます。

手順

拡張 ThinkServer CPlus BIOS パターンを変更するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**カテゴリー・パターン**」タブをクリックします。

ステップ 3. 「**拡張 ThinkServer CPlus BIOS パターン**」垂直タブをクリックします。

ステップ 4. 変更するパターンを選択し、「**編集**」アイコン ( ) をクリックします。

ステップ 5. 適切なフィールドを変更します。

「**設定の包含/除外**」をクリックして、カテゴリー・パターンに含める設定を選択します。

ステップ 6. 「**保存**」をクリックして変更を現在のカテゴリー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいカテゴリー・パターンに保存します。

結果

「構成パターン: カテゴリー・パターン」ページの「**拡張 ThinkServer CPlus BIOS パターン**」タブに変更されたカテゴリー・パターンが表示されます。

このページでは、選択したカテゴリー・パターンに対して以下の操作を実行することもできます。

- 「**コピー**」アイコン ( ) をクリックして既存のパターンをコピーする。
- 「**削除**」アイコン ( ) をクリックして、パターンを削除する。
- 「**名前変更**」アイコン ( ) をクリックして、パターンの名前を変更する。
- パターンをインポートまたはエクスポートする (XClarity Administrator オンライン・ドキュメントのサーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート)。

サーバーへのサーバー・パターンのデプロイ

サーバー・パターンは、1 つ以上の管理対象サーバーにデプロイできます。また、Lenovo XClarity Administrator によって管理されているシャーシまたはプレースホルダー・シャーシの 1 つ以上の空のベイにサーバー・パターンをデプロイすることもできます。サーバーが取り付けられる前にサーバー・パター

ンをデプロイすると、管理 IP アドレスが予約されて、仮想イーサネット/Fibre Channel アドレスが予約され、ネットワーク設定が関連するスイッチの内部ポートにプッシュされます。

始める前に

管理対象デバイスにサーバー・パターンを適用する前に、サーバー構成に関する考慮事項を確認してください (サーバーへのサーバー・パターンのデプロイを参照)。

手順

サーバー・パターンを管理対象サーバーにデプロイするには、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、「**プロビジョニング**」 → 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。

ステップ 2. 「**サーバー・パターン**」タブをクリックします。

ステップ 3. デプロイするサーバー・パターンを選択し、「**デプロイ**」アイコン () をクリックします。

選択したサーバー・パターンが、「サーバー・パターンのデプロイ」ダイアログの「**デプロイするパターン**」リストに表示されます。

ステップ 4. 構成をいつアクティブにするかを選択します。

- 「**全文**」。直ちにサーバーの電源をオンにするかサーバーを再起動して、サーバー、ベースボード管理コントローラー、および Unified Extensible Firmware Interface (UEFI) の構成をアクティブにします。
- 「**一部**」。(デフォルト) 直ちに管理コントローラーの構成はアクティブになりますが、サーバーおよび UEFI の構成のアクティブ化は、サーバーが次に再起動するまで据え置かれます。プロファイルを完全にアクティブにするには、手動でサーバーの電源をオンにするかサーバーを再起動する必要があります。

  注：IMM 設定 (システム情報、管理インターフェース、拡張 BMC カテゴリー・パターンなど) のみ含まれるサーバー・パターンをデプロイする場合、サーバーを再起動する必要はありません。
- 「**据え置き**」。サーバー、管理コントローラー、および UEFI 設定のプロファイルが生成されます。ただし、その構成設定はサーバー上でアクティブ化されません。プロファイルを完全にアクティブにする前に、サーバーを再起動することによって手動でサーバー・プロファイルをアクティブにする必要があります。

注：アクティベーション構成に関係なく、デプロイされるとすぐに関連するスイッチの内部ポートのネットワーク設定がそのスイッチにプッシュされます。

ステップ 5. このサーバー・パターンをデプロイするサーバーまたは空のシャーシ・ベイを 1 つ以上選択します。

注：空のシャーシ・ベイのリストを表示するには、「**空のベイの表示**」を選択します。

ステップ 6. 「**デプロイ**」をクリックします。ダイアログが開き、選択した各ベイのデプロイメント・ステータスが表示されます。

ステップ 7. もう一度「**デプロイ**」をクリックして、デプロイメント・プロセスを開始します。

注：デプロイが完了するまでに数分かかることがあります。デプロイ中に、サーバー・プロファイルが作成されて、選択した各サーバーまたはシャーシ・ベイに割り当てられます。

ステップ 8. 「**閉じる**」をクリックします。

終了後

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、デプロイの進行を監視できます。「**プロビジョニング**」 → 「**サーバー・プロファイル**」の順にクリックすると、サーバー・プロファイルの作成を監視することもできます。デプロイが完了したら、生成されたサーバー・プロファイルを確認し、管理 IP アドレスと仮想イーサネット/Fibre Channel アドレスを記録します。

既存のサーバーにサーバー・パターンをデプロイした場合は次のようになります。

- アクティブ化のオプションで「**全文**」を選択した場合は、各サーバーのサーバー・プロファイルが作成され、各サーバーに構成が伝播されて、構成の変更をアクティブにするために各サーバーがリブートします。
- アクティブ化のオプションで「**一部**」を選択した場合は、各サーバーのサーバー・プロファイルが作成され、各サーバーに構成が伝播されます。構成の変更を完全にアクティブにするには、手動で各サーバーの電源をオンにするか各サーバーを再起動する必要があります (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)。
- アクティブ化のオプションで「**据え置き**」を選択した場合は、各サーバーのサーバー・プロファイルが作成されます。サーバーのサーバー・プロファイルを手動でアクティブ化する必要があります (サーバー・プロファイルのアクティブ化を参照)。

管理対象シャーシまたはプレースホルダー・シャーシの空のベイにサーバー・パターンをデプロイした場合は、計算ノードが適切なシャーシ・ベイに物理的に取り付けられ、Lenovo XClarity Administrator によって検出されて管理対象になった後、その新たに取り付けられた計算ノードにサーバー・プロファイルをデプロイして、プロファイルをアクティブにする必要があります (サーバー・プロファイルのアクティブ化を参照)。

新しいサーバー・パターンをデプロイした後に起動しなくなったサーバーがある場合は、ブート設定がサーバー・パターンのデフォルトのブート設定で上書きされたことが原因と考えられます。UEFI モードでインストールされたオペレーティング・システムの場合、デフォルト設定を復元すると、追加の構成手順を実行してブート構成を復元する必要が生じることがあります。Windows または Linux で実行しているサーバーでのブート設定のリカバリーの例については、サーバー・パターンのデプロイ後のブート設定のリカバリーを参照してください。

サーバー・パターンの変更

既存の任意のサーバー・パターンの構成を後から変更することができます。元のサーバー・パターンがサーバーにデプロイされている場合 (使用中の場合)、そうしたすべてのサーバーまたはそうしたサーバーのサブ・セットに、変更したサーバー・パターンを再デプロイできます。

このタスクについて

注：変更したサーバー・パターンをサーバー・セットに再デプロイしない場合、そうしたサーバーは引き続き、元の変更されていないサーバー・パターンに関連付けられます。

サーバー・パターンを編集して、共通の構成を 1 か所から管理し、仮想アドレスの元の割り当てセットを維持できます。

手順

サーバー・パターンを変更するには、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、「**プロビジョニング**」 → 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。

ステップ 2. 「**サーバー・パターン**」タブをクリックします。

ステップ 3. 編集するサーバー・パターンを選択し、「**編集**」アイコン () をクリックします。「サーバー・パターン・ウィザードの編集」が表示されます。

ステップ 4. パターンの名前と説明を入力します。

ステップ 5. このパターンをサーバーにデプロイするときに適用するローカル・ストレージの構成を選択し、「**次へ**」をクリックします。

ローカル・ストレージの設定については、ローカル・ストレージの定義を参照してください。

ステップ 6. **オプション**: I/O アダプター・アドレス指定を変更し、このパターンで構成するハードウェアに合わせて追加の I/O アダプターを定義して、「**次へ**」をクリックします。

I/O アダプターの設定については、I/O アダプターの定義を参照してください。

ステップ 7. このパターンをサーバーにデプロイするときに適用するブート順序を定義して、「**次へ**」をクリックします。

SAN ブート・ターゲットの設定については、ブート・オプションの定義を参照してください。

ステップ 8. 既存のカテゴリー・パターンのリストからファームウェア設定を選択します。

新しいカテゴリー・パターンを作成するには、「**作成**」アイコン () をクリックします。

ファームウェア設定については、ファームウェア設定の定義を参照してください。

ステップ 9. 「**保存**」をクリックして構成の変更を現在のサーバー・パターンに保存するか、「**名前を付けて保存**」をクリックして新しいサーバー・パターンに保存します。

ステップ 10. 現在のサーバー・パターンまたは新しいサーバー・パターンのいずれに変更内容を保存するかを選択します。

- 「**保存**」をクリックすると、現在のサーバー・パターンに変更内容が保存されます。「パターンの保存と再デプロイ」ダイアログで、以下の手順を実行します。
  1. 構成をいつアクティブにするかを選択します。
     - 「**全文**」。直ちにサーバーの電源をオンにするかサーバーを再起動して、サーバー、ベースボード管理コントローラー、および Unified Extensible Firmware Interface (UEFI) の構成をアクティブにします。
     - 「**一部**」。(デフォルト) 直ちに管理コントローラーの構成はアクティブになりますが、サーバーおよび UEFI の構成のアクティブ化は、サーバーが次に再起動するまで据え置かれます。プロファイルを完全にアクティブにするには、手動でサーバーの電源をオンにするかサーバーを再起動する必要があります。

       注： IMM 設定 (システム情報、管理インターフェース、拡張 BMC カテゴリー・パターンなど) のみ含まれるサーバー・パターンをデプロイする場合、サーバーを再起動する必要はありません。

     注： アクティベーション構成に関係なく、デプロイされるとすぐに関連するスイッチの内部ポートのネットワーク設定がそのスイッチにプッシュされます。
  2. 構成の変更を再デプロイするターゲット・サーバーを選択します。元のサーバー・パターンがデプロイされたすべてのサーバー、またはそうしたサーバーのサブセットを選択できます。
  3. 「**再デプロイ**」をクリックします。
- 「**名前を付けて保存**」をクリックすると、新しいサーバー・パターンに変更内容が保存されます。新しいパターンのデプロイについては、サーバーへのサーバー・パターンのデプロイ を参照してください。

サーバー・パターンおよびカテゴリー・パターンのエクスポートとインポート

複数の Lenovo XClarity Administrator インスタンスがある場合は、いずれかの XClarity Administrator インスタンスからサーバー・パターンおよびカテゴリー・パターンをエクスポートして、別の XClarity Administrator インスタンスにインポートすることができます。

このタスクについて

エクスポートできるのはサーバー・パターンとカテゴリー・パターンだけです。ポリシー、アドレス・プール、およびプロファイルはエクスポートできません。パターンをエクスポートすると、アドレス・プールの参照が解除されます。インポートしたパターンでアドレス・プールを活用するには、パターンを編集して、インポート先の XClarity Administrator のプールに関連付けし直します。

注：サーバー・パターンをエクスポートする場合、関連のカテゴリー・パターンもエクスポートされます。

手順

- 1 つ以上のパターンをエクスポートする場合:
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。
  2. 「**サーバー・パターン**」タブまたは「**カテゴリー・パターン**」タブをクリックします。
  3. エクスポートするパターンを 1 つ以上選択します。
  4. 「**エクスポート**」アイコン ( ) をクリックします。
  5. 「**エクスポート**」をクリックしてパターンをエクスポートします。
  6. パターン・データ・ファイルをローカル・システムに保存します。

     注：エクスポートされたパターンがアドレス・プールを参照している場合、そのパターンが別の XClarity Administrator インスタンスにインポートされた際の競合を避けるために、それらの参照はエクスポートされたパターンから削除されます。パターンが再インポートされると、インポートされたパターンを編集して、目的のアドレス・プールを割り当てることができます。
- 1 つ以上のパターンをインポートする場合:
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。
  2. 「**インポート**」アイコン ( ) をクリックしてパターンをインポートします。「パターンのインポート」ダイアログが表示されます。
  3. 「**ファイルの選択**」をクリックし、インポートするパターン・データ・ファイルを選択します。追加のパターン・データ・ファイルについてもこの手順を繰り返します。
  4. 「**インポート**」をクリックして選択されたファイルをインポートします。

     要約レポートと、インポートされたパターン、名前競合で名前を変更されたパターン、既に存在するためにスキップされたパターンのリストが表示されます。

サーバー・プロファイルの使用

*サーバー・プロファイル*とは、特定のサーバーに適用されるサーバー・パターンのインスタンスです。サーバー・プロファイルは、サーバー・パターンを 1 つ以上のサーバーにデプロイすると自動的に生成されて割り当てられます。個々のターゲット・サーバーに 1 つのサーバー・プロファイルが作成されます。各サーバー・プロファイルは、1 つのサーバーの固有の構成を含み、そのサーバーに固有の情報 (割り当てられた名前、IP アドレス、MAC アドレスなど) を含んでいます。

このタスクについて

サーバー・プロファイルは、ベースボード管理コントローラーの起動プロセスでアクティブ化されます。次の選択を行えます。
- パターンがデプロイされたらサーバーをリブートして、サーバー・プロファイルを直ちにアクティブにする。
- 次回のリブートまでアクティブ化を据え置く。
- 手動でサーバー・プロファイルをアクティブにするまでアクティブ化を据え置く。

複数のサーバー・プロファイルは、1 つのサーバー・パターンから継承できます。サーバー・パターンを 1 つ以上のサーバーにデプロイした後、親のサーバー・パターンとカテゴリー・パターンを編集することにより、構成の変更を複数のサーバーにすばやくデプロイできます。依存サーバー・プロファイルは、自動的に更新されて関連サーバーに再デプロイされます。サーバー・パターンを編集することにより、共通の構成を 1 か所で制御できます。

既存のサーバーを交換した場合や、事前プロビジョニングしたサーバーをシャーシの空のベイに取り付けた場合は、その新しいサーバーのサーバー・プロファイルをアクティブにして、構成の変更をプロビジョニングする必要があります。

注：1 つのサーバー・パターンを複数のサーバーにデプロイできますが、複数のパターンを 1 つのサーバーにデプロイすることはできません。

サーバーに関連付けられているサーバー・プロファイルを変更するにはいくつかの方法があります。どの方法を使用するかは変更の理由によって決まります。

- サーバーを移動または再利用する場合:
  1. 現在のサーバーで現在のサーバー・プロファイルを非アクティブ化します (サーバー・プロファイルの非アクティブ化を参照してください)。
  2. 新しいサーバーに新しいサーバー・パターンをデプロイします (サーバーへのサーバー・パターンのデプロイを参照してください)。
- サーバーで障害が発生したために予備のサーバーを使用する場合:
  1. 障害の発生したサーバーで現在のサーバー・プロファイルを非アクティブ化します (サーバー・プロファイルの非アクティブ化を参照してください)。
  2. 予備のサーバーで同じサーバー・プロファイルをアクティブにします (サーバー・プロファイルのアクティブ化を参照してください)。
  3. 障害の発生したサーバーの修理が完了したら、上の手順を繰り返してプロファイルを元に戻します。
- サーバーで障害が発生したためにハードウェアを交換する場合:
  1. 障害の発生したサーバーで現在のサーバー・プロファイルを非アクティブ化します (サーバー・プロファイルの非アクティブ化を参照してください)。
  2. 障害の発生したサーバーを交換します。
  3. 新しいサーバーで同じサーバー・プロファイルをアクティブにします (サーバー・プロファイルのアクティブ化を参照してください)。

重要：

- アドレス仮想化を使用すると、サーバーは電源がオンにされるまで割り振られた仮想 MAC アドレスまたは WWN アドレスを保持します。アドレス仮想化が有効になっているプロファイルを非アクティブ化すると、「**サーバーの電源をオフにします**」チェックボックスがデフォルトで選択されます。アドレスの競合を回避するために、非アクティブ化したプロファイルを別のサーバーでアクティブにする前に元のサーバーの電源をオフにしてください。
- もっとも最近作成されたものではないプロファイルを削除すると、仮想 MAC および WWN アドレスはアドレス・プールから解放されません。詳しくは、サーバー・プロファイルの削除を参照してください。

- 構成パターンを使用せず設定が変更された場合、またはデプロイメント中にファームウェアの問題または無効な設定が発生した場合、サーバーの設定がそのサーバー・プロファイルのコンプライアンス違反になります。「構成パターン: サーバー・プロファイル」ページから、各サーバーのコンプライアンス状況を調べることができます。

サーバー・プロファイルのアクティブ化

サーバーを交換した場合、再割り当てした場合、または新たにインストールして管理する場合に、そのサーバーでサーバー・プロファイルをアクティブにすることができます。

このタスクについて

既存のサーバーを交換した場合や、事前プロビジョニングしたサーバーをシャーシの空のベイに取り付けた場合は、その新しいサーバーのサーバー・プロファイルをアクティブにして、構成の変更をプロビジョニングする必要があります。

重要：

- アドレス仮想化を使用すると、サーバーは電源がオンにされるまで割り振られた仮想 MAC アドレスまたは WWN アドレスを保持します。アドレス仮想化が有効になっているプロファイルを非アクティブ化すると、「**サーバーの電源をオフにします**」チェックボックスがデフォルトで選択されます。アドレスの競合を回避するために、非アクティブ化したプロファイルを別のサーバーでアクティブにする前に元のサーバーの電源をオフにしてください。
- もっとも最近作成されたものではないプロファイルを削除すると、仮想 MAC および WWN アドレスはアドレス・プールから解放され*ません*。詳しくは、サーバー・プロファイルの削除を参照してください。
- 構成パターンを使用せず設定が変更された場合、またはデプロイメント中にファームウェアの問題または無効な設定が発生した場合、サーバーの設定がそのサーバー・プロファイルのコンプライアンス違反になります。「構成パターン: サーバー・プロファイル」ページから、各サーバーのコンプライアンス状況を調べることができます。

手順

サーバー・プロファイルをアクティブにするには、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、「**プロビジョニング**」 ➡ 「**サーバー・プロファイル**」の順にクリックします。「構成パターン: サーバー・プロファイル」ページが表示されます。

ステップ 2. アクティブにするサーバー・プロファイルを選択します。

ヒント: サーバー・プロファイルの現在の状態が「**プロファイルのステータス**」列に表示されます。アクティブ化の状態が「非アクティブ」または「保留中」のサーバー・プロファイルをアクティブにできます。

ステップ 3. 「**サーバー・プロファイルのアクティブ化**」アイコン () をクリックします。

ステップ 4. 「**アクティブにする**」をクリックします。

プロファイルが「保留中」、「アクティブ」、または「アクティブの障害」状態の場合、デプロイをアクティブ化するタイミングを選択できます。

- 「**全文**」。直ちにサーバーの電源をオンにするかサーバーを再起動して、サーバー、ベースボード管理コントローラー、および Unified Extensible Firmware Interface (UEFI) の構成をアクティブにします。
- 「**一部**」。(デフォルト) 直ちに管理コントローラーの構成はアクティブになりますが、サーバーおよび UEFI の構成のアクティブ化は、サーバーが次に再起動するまで据え置かれます。プロファイルを完全にアクティブにするには、手動でサーバーの電源をオンにするかサーバーを再起動する必要があります。

注：IMM 設定 (システム情報、管理インターフェース、拡張 BMC カテゴリー・パターンなど) のみ含まれるサーバー・パターンをデプロイする場合、サーバーを再起動する必要はありません。

サーバー・プロファイルが初めてアクティブ化されると、プロファイルのステータスが「アクティブ」に変わります。コンプライアンスが検証された後、ステータスは「コンプライアンス」または「非準拠」に変わります。

結果

「構成パターン: サーバー・プロファイル」ページのサーバー・プロファイルの状態が「アクティブ」に変わります。

サーバー・プロファイルの非アクティブ化

サーバーまたはシャーシからサーバー・プロファイルの割り当てを解除するには、プロファイルを非アクティブ化します。

手順

サーバー・プロファイルを非アクティブ化するには、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、「**プロビジョニング**」 → 「**サーバー・プロファイル**」の順にクリックします。「構成パターン: サーバー・プロファイル」ページが表示されます。

ステップ 2. 非アクティブ化するサーバー・プロファイルを選択します。

ヒント: サーバー・プロファイルの現在の状態が「**プロファイルのステータス**」列に表示されます。

ステップ 3. 「**サーバー・プロファイルの非アクティブ化**」アイコン ( ) をクリックします。

ステップ 4. 以下のいずれかの非アクティブ化オプションを選択します。

- **IMM の ID 設定をリセットする。**プロファイルに構成された識別情報 (ベースボード管理コントローラーのホスト名、デバイス名、または管理インターフェースに割り当てられた静的 IP アドレスを含む) をリセットします。関連付けられているサーバー・パターンを使用して構成された設定のみがリセットされます。

注：静的に割り当てられた IP アドレスを持つサーバーの場合は、このオプションは DHCP モードを有効にします。ネットワーク上で有効になっている DHCP サーバーがない場合、有効な静的 IP アドレスを使用してサーバーを手動で再構成する必要があります。コンバージド、NeXtScale、System x ラック・サーバーおよびタワー・サーバーは、XClarity Administratorを使用して管理対象に戻す必要があります。

- **サーバーの電源をオフにします。**サーバーの電源をオフにします。サーバーの電源が再びオンになったときに、仮想アドレスの割り当てが出荷時のデフォルト設定に戻されます。
- **非アクティブ化を強制する。**サーバーが削除されたか到達不能な場合でもサーバー・プロファイルを非アクティブ化します。
- **スイッチの内蔵ポート設定のリセット。**UFP モードの無効化および関連付けられているメンバー vport の VLAN 定義から削除を含めて、プロファイルにより構成されたスイッチの内部ポート設定をデフォルト値にリセットします。関連付けられているサーバー・パターンを使用して構成された設定のみがリセットされます。

  このオプションは、デフォルトで無効になっています。

  このオプションを選択すると、以前のスイッチ・ポート構成と競合する設定を含めずに、サーバー・プロファイルを別のサーバーにデプロイできる状態で、スイッチ・ポートを維持します。

ステップ 5. 「**非アクティブ化**」をクリックします。

結果

「構成パターン: サーバー・プロファイル」ページのサーバー・プロファイルの状態が「非アクティブ」に変わります。

注：XClarity Administrator が管理コントローラーと通信できない場合 (たとえば管理コントローラーがエラー状態にある、再起動中の場合)、サーバー・プロファイルの非アクティブ化は失敗し、サーバー・プロファイルは非アクティブ化されません。この場合は、非アクティブ化を再試行して非アクティブ化の強制オプションを選択し、プロファイルを非アクティブ化します。先に割り当てられたサーバーは、プロファイルに割り当てられている ID およびアドレス割り当てを使用して構成されたままです。アドレスの競合を防ぐため、サーバーの電源を手動で落としインフラストラクチャーから外してください。

サーバー・プロファイルの削除

非アクティブ化されているサーバー・プロファイルのみ削除できます。

始める前に

削除するサーバー・プロファイルが非アクティブ化されていることを確認します (サーバー・プロファイルの非アクティブ化を参照)。

手順

サーバー・プロファイルを削除するには、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、「**プロビジョニング**」 ➡ 「**サーバー・プロファイル**」の順にクリックします。「構成パターン: サーバー・プロファイル」ページが表示されます。

ステップ 2. 「非アクティブ化」状態のサーバー・プロファイルを選択します。

ヒント: サーバー・プロファイルの現在の状態が「**プロファイルのステータス**」列に表示されます。

ステップ 3. 「**削除**」アイコン ( ) をクリックします。

注：もっとも最近作成されたプロファイルを削除すると、仮想 MAC または WWN アドレスがアドレス・プールから解放されます。もっとも最近作成されたものではないプロファイルを削除すると、仮想 MAC および WWN アドレスはアドレス・プールから解放され*ません*。

プレースホルダー・シャーシの使用

物理ハードウェアが到着するまでサーバー・パターンのターゲットとして動作する *プレースホルダー・シャーシ*を定義することにより、後で Flex System シャーシに取り付けられるサーバーを事前プロビジョニングできます。

このタスクについて

プレースホルダー・シャーシにサーバー・パターンをデプロイすると、Lenovo XClarity Administrator でその Flex System シャーシのすべてのサーバー・ベイ (14 台) のサーバー・プロファイルが作成され、それらのサーバーの管理 IP アドレスと、仮想イーサネットまたは Fibre Channel アドレスが予約されます。

プレースホルダー・シャーシでは、すべてのサーバー・プロファイルが 1 つにまとめられているため、ハードウェアが到着したら、プレースホルダー・シャーシをデプロイすることで、14 個のサーバー・プロファイルを個別にすべてデプロイしなくても、物理サーバーでサーバー・プロファイルをアクティブにすることができます。サーバー・プロファイルを完全にアクティブにするには、各サーバーをリブートする必要があります。

プレースホルダー・シャーシの作成

ハードウェアを取り付ける前に事前にプロビジョニングできるプレースホルダー・シャーシを作成することができます。そのシャーシで計算ノードをプロビジョニングすると、管理 IP アドレスと仮想イーサネット/Fibre Channel アドレスが予約されます。

手順

プレースホルダー・シャーシを作成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**プレースホルダー・シャーシ**」タブをクリックします。

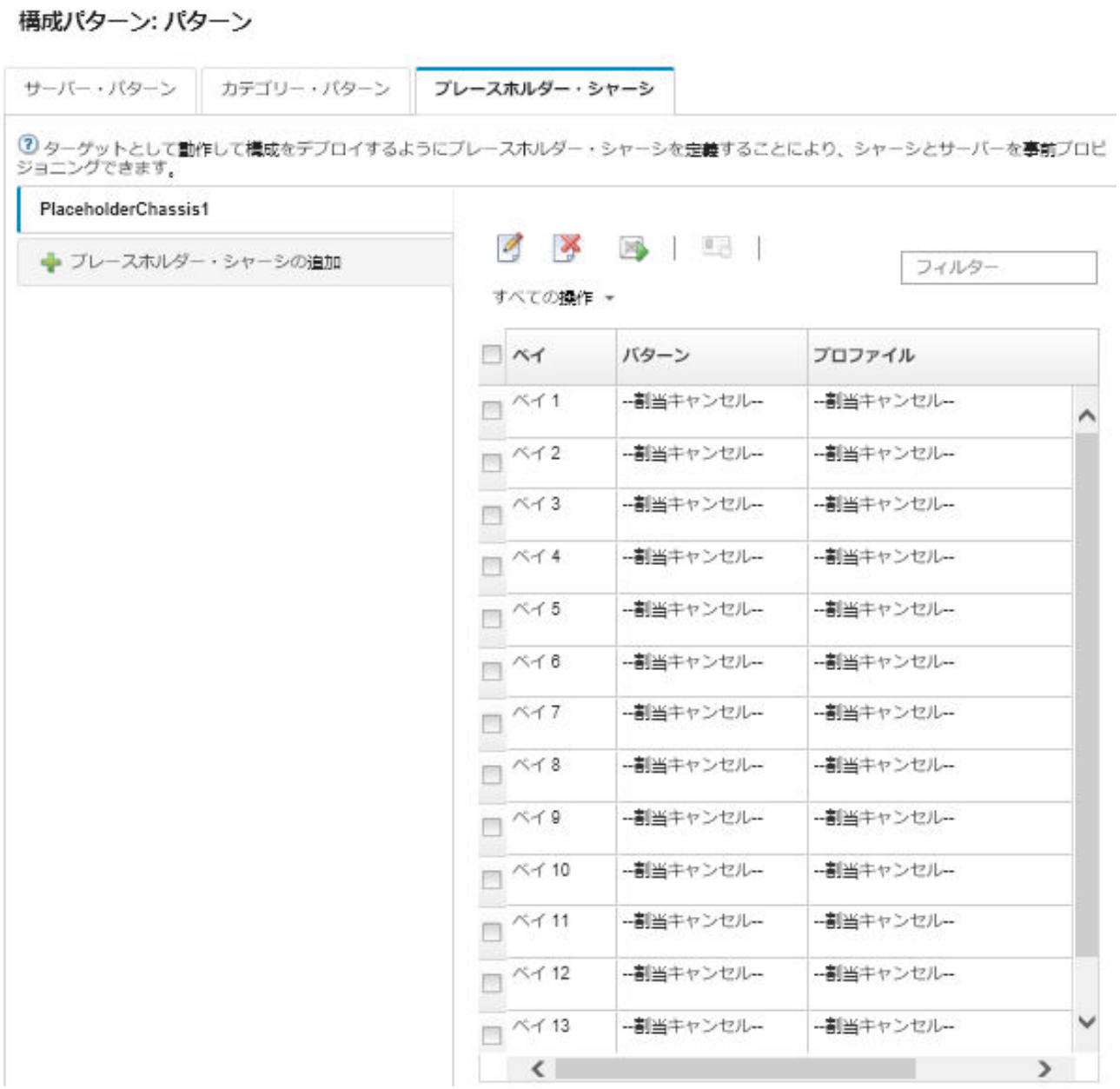
ステップ 3. 「**プレースホルダー・シャーシの追加**」垂直タブをクリックします。

ステップ 4. プレースホルダー・シャーシの名前と説明を入力します。

ステップ 5. 「**追加**」をクリックします。

終了後

「構成パターン: プレースホルダー・シャーシ」ページに、新しいプレースホルダー・シャーシの垂直タブが追加されます。



このページでは、選択したプレースホルダー・シャーシに対して以下の操作を実行できます。

- 「**デプロイ**」アイコン ( ) をクリックして、プレースホルダー・シャーシをデプロイする。
- 「**編集**」アイコン ( ) をクリックして、プレースホルダー・シャーシの名前と説明を変更する。
- プレースホルダー・シャーシにサーバー・パターンをデプロイする (プレースホルダー・シャーシへのサーバー・パターンのデプロイを参照してください)。
- プレースホルダー・シャーシのサーバー・プロファイルを非アクティブ化する (サーバー・プロファイルの非アクティブ化を参照してください)。
- 「**削除**」アイコン ( ) をクリックして、プレースホルダー・シャーシを削除する。

プレースホルダー・シャーシへのサーバー・パターンのデプロイ

プレースホルダー・シャーシの各ベイにサーバー・パターンをデプロイできます。サーバーが Flex System シャーシに取り付けられる前にサーバー・パターンをデプロイすると、シャーシ内の各サーバー・ベイのサーバー・プロファイルが作成され、管理 IP アドレスと仮想イーサネット/Fibre Channel アドレスが予約されます。

手順

サーバー・パターンをプレースホルダー・シャーシにデプロイするには、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、「**プロビジョニング**」 ➡ 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。

ステップ 2. 「**サーバー・パターン**」タブをクリックします。

ステップ 3. プレースホルダー・シャーシにデプロイするサーバー・パターンを選択します。

ステップ 4. 「**デプロイ**」アイコン ( ) をクリックします。「サーバー・パターンのデプロイ」ダイアログが開き、使用可能なシャーシとプレースホルダー・シャーシのリストが表示されます。

ステップ 5. 「**アクティベーション**」リストで「**据え置き**」を選択します。

ステップ 6. 「**空のベイの表示**」をクリックします。

ステップ 7. このサーバー・パターンをデプロイするプレースホルダー・シャーシ・ベイを 1 つ以上選択します。

ステップ 8. 「**デプロイ**」をクリックします。ダイアログが開き、選択した各ベイのデプロイメント・ステータスが表示されます。

ステップ 9. もう一度「**デプロイ**」をクリックして、デプロイメント・プロセスを開始します。

選択した各プレースホルダー・シャーシ・ベイのサーバー・プロファイルが作成されて割り当てられます。

注：デプロイが完了するまでに数分かかることがあります。

ステップ 10. 「**閉じる**」をクリックします。

終了後

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、デプロイの進行を監視できます。「**プロビジョニング**」 ➡ 「**サーバー・プロファイル**」の順にクリックすると、サーバー・プロファイルの作成を監視することもできます。デプロイが完了したら、生成されたサーバー・プロファイルを確認し、管理 IP アドレスと仮想イーサネット/Fibre Channel アドレスを記録します。

Flex System シャーシが物理的にラックに取り付けられ、XClarity Administrator によって検出されて管理対象になったら、プレースホルダー・シャーシをデプロイして、シャーシ内のすべてのサーバーをプロビジョニングできます (プレースホルダー・シャーシへのサーバー・パターンのデプロイ を参照)。

プレースホルダー・シャーシのデプロイ

サーバー・パターンをデプロイしてプレースホルダー・シャーシを事前構成した後に、実際のシャーシが検出されて管理対象になったら、そのプレースホルダー・シャーシをデプロイして実際の計算ノードを構成できます。

手順

プレースホルダー・シャーシをデプロイするには、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、「**プロビジョニング**」 ➡ 「**サーバー構成パターン**」の順にクリックします。「サーバー構成パターン」ページが表示されます。

ステップ 2. 「**プレースホルダー・シャーシ**」タブをクリックします。

ステップ 3. デプロイするプレースホルダー・シャーシの垂直タブを選択します。

ステップ 4. 「**プレースホルダー・シャーシのデプロイ**」アイコン ( ) をクリックして「プレースホルダー・シャーシのデプロイ」ダイアログを表示します。

ステップ 5. 構成をいつアクティブにするかを選択します。

注：アクティベーション構成に関係なく、デプロイされるとすぐに関連するスイッチの内部ポートのネットワーク設定がそのスイッチにプッシュされます。

- 「**全文**」。直ちにサーバーの電源をオンにするかサーバーを再起動して、サーバー、ベースボード管理コントローラー、および Unified Extensible Firmware Interface (UEFI) の構成をアクティブにします。
- 「**一部**」。(デフォルト) 直ちに管理コントローラーの構成はアクティブになりますが、サーバーおよび UEFI の構成のアクティブ化は、サーバーが次に再起動するまで据え置かれます。プロファイルを完全にアクティブにするには、手動でサーバーの電源をオンにするかサーバーを再起動する必要があります。

  注：IMM 設定 (システム情報、管理インターフェース、拡張 BMC カテゴリー・パターンなど) のみ含まれるサーバー・パターンをデプロイする場合、サーバーを再起動する必要はありません。

ステップ 6. 「**アクティブにする**」をクリックします。

ストレージ・アダプターのデフォルト値へのリセット

1 つ以上のサーバーでローカル・ストレージ・アダプターを出荷時のデフォルト設定にリセットできます。

このタスクについて

注意：この操作は、ローカル・ストレージ・アダプターのすべてのデータのクリアします。

サーバーの電源がオフであり RAID リンクがサポートされている場合、サーバーはブートしてシステム・セットアップに入り、ローカル HDD および SSD アダプターをリセットします。

手順

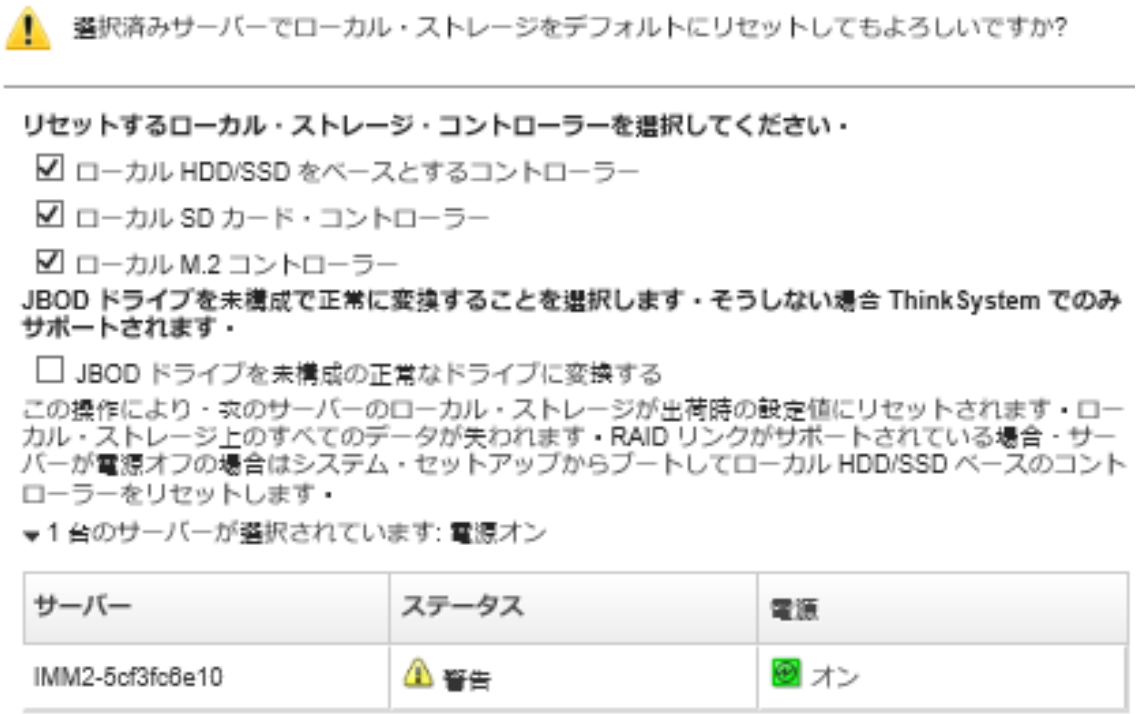
1 つ以上のサーバーの RAID 構成をクリアするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**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。

テーブルの列をソートすると、管理するサーバーを見つけやすくなります。「**すべてのシステム**」ドロップダウン・リストでサーバー・タイプを選択し、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーを絞り込むこともできます。

ステップ 2. 1 つ以上のサーバーを選択します。

ステップ 3. 「**すべての操作**」 → 「**サービス**」 → 「**ローカル・ストレージをデフォルトにリセット**」の順に選択します。追加情報の入力を求めるダイアログが表示されます。



ステップ 4. リセットするローカル・ストレージ・アダプターを選択します。

ステップ 5. : (ThinkSystem サーバーのみ) JBOD を未構成で正常に変換するために選択します。

ステップ 6. 「**ストレージのリセット**」をクリックします。

メモリーの構成

Intel® Optane™ DC 永続メモリー DIMM の永続メモリーの暗号化および復号化を行うことができます。

手順

以下の手順を実行して、永続メモリーの暗号化および復号化を行います。

ステップ 1. XClarity Administrator のメニューで、「**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。

ステップ 2. 構成するサーバーを 1 台以上選択します。

ステップ 3. 「**すべての操作**」 → 「**セキュリティー**」 → 「**Intel Optane PMEM Operation**」をクリックし、「Intel Optane PMEM Operation」ダイアログを表示します。

ステップ 4. 次のように、実行するセキュリティー操作を選択します。

- **セキュリティーの有効化**。永続メモリー領域に書き込まれるデータは、指定したパスフレーズを使用して暗号化されます。

  重要：暗号化パスフレーズを記録します。このパスフレーズは、セキュリティーの無効化または暗号化パスフレーズの消去を許可するために必要です。

- **セキュリティーの無効化**永続メモリー領域に書き込まれるデータは、暗号化されません。

  永続メモリー領域に既に保存されているデータは引き続き暗号化され、依然としてアクセスできます。

  注：この操作は、セキュリティーが有効であり、パスフレーズが設定されている場合にのみ使用できます。この操作は、現在のパスフレーズを使用して許可する必要があります。すべての DIMM で同じパスフレーズを共有する場合にのみ、デバイス内の複数の DIMM でセキュリティーを無効にすることができます。

- **セキュアな消去**データを確実にリカバリー不能な状態にするために、永続メモリー領域に格納されているデータの暗号化に使用される暗号化パスフレーズを消去します。

  注：この操作は、セキュリティーが有効であり、パスフレーズが設定されている場合にのみ使用できます。この操作は、現在のパスフレーズを使用して許可する必要があります。

- **パスフレーズなしのセキュアな消去**。デバイスの指定された DIMM の永続メモリーに格納されているすべてのデータを安全に消去します。セキュアな消去を実行すると、すべてのデータが復元できなくなります。

  注：この操作は、セキュリティーが無効であり、パスフレーズが不要の場合にのみ使用できます。

ステップ 5. 必要に応じて、パスフレーズを指定して確認します。

ステップ 6. 「OK」をクリックします。

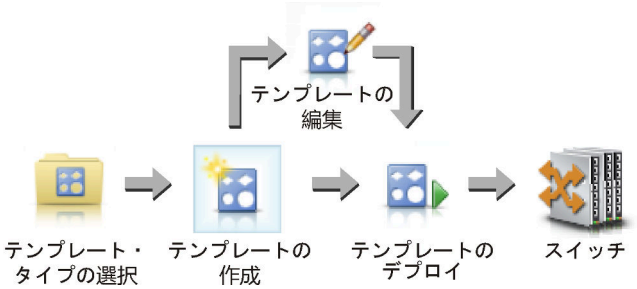
第 12 章　構成テンプレートを使用したスイッチの構成

テンプレートを使用すると、単一の定義済み構成設定セットから複数の CNOS ラック・スイッチをすばやくプロビジョニングできます。

このタスクについて

XClarity Administrator でスイッチ構成テンプレートを使用して、管理対象スイッチの共通設定、ポート・チャネル、仮想 LAN、仮想リンク集約グループ、およびスパイン・リーフ・トポロジーを構成できます。現在、CNOS を実行するラック・スイッチのみがサポートされています。

次の図は、管理対象ラック・スイッチの構成のワークフローを示しています。



1. **テンプレート・タイプの選択。**

   *スイッチ構成テンプレート*は、関連するスイッチ設定をグループ化します。以下のタイプのスイッチ構成テンプレートを作成できます。
   - **グローバル**。システム・プロパティ、ネイティブ VLAN タグ、L2 インターフェースなどの共通設定を構成します。
   - **ポート・チャネル**。基本および拡張ポート・チャネル設定の構成、ポートおよびポート・チャネルの削除を行います。
   - **スパイン・リーフ**。既存のトポロジーにスパイン・リーフ構成をデプロイします。
   - **仮想 LAN (VLAN)**。VLAN 設定およびプロパティを構成し、VLAN を削除します。
   - **仮想リンク集約グループ (VLAG)**。基本、詳細、およびピア VLAG 設定を構成し、VLAG 設定を削除します。また VLAG インスタンスを作成し、削除します。

2. **テンプレートの作成。**

   データ・センターで使用するためのさまざまな構成を表す、複数のスイッチ構成テンプレートを作成できます。スイッチ構成テンプレートを使用して、共通のスイッチ構成を 1 か所で管理できます。

   スイッチ構成テンプレートの作成について詳しくは、スイッチ構成テンプレートの作成を参照してください。

3. **テンプレートを 1 台以上のスイッチにデプロイします。**

   サーバー・パターンは、CNOS を実行する 1 つ以上の個々のラック・スイッチにデプロイできます。

   スイッチ構成のデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

4. **テンプレートを編集します。**

   スイッチ構成テンプレートを編集しても、初期テンプレートがデプロイされたすべてのスイッチに、更新された設定が自動的にデプロイされるわけではありません。変更されたテンプレートを手動で再デプロイする必要があります。履歴ページでは、デプロイメントごとの設定が追跡されます。

デフォルトのサーバー構成設定の設定

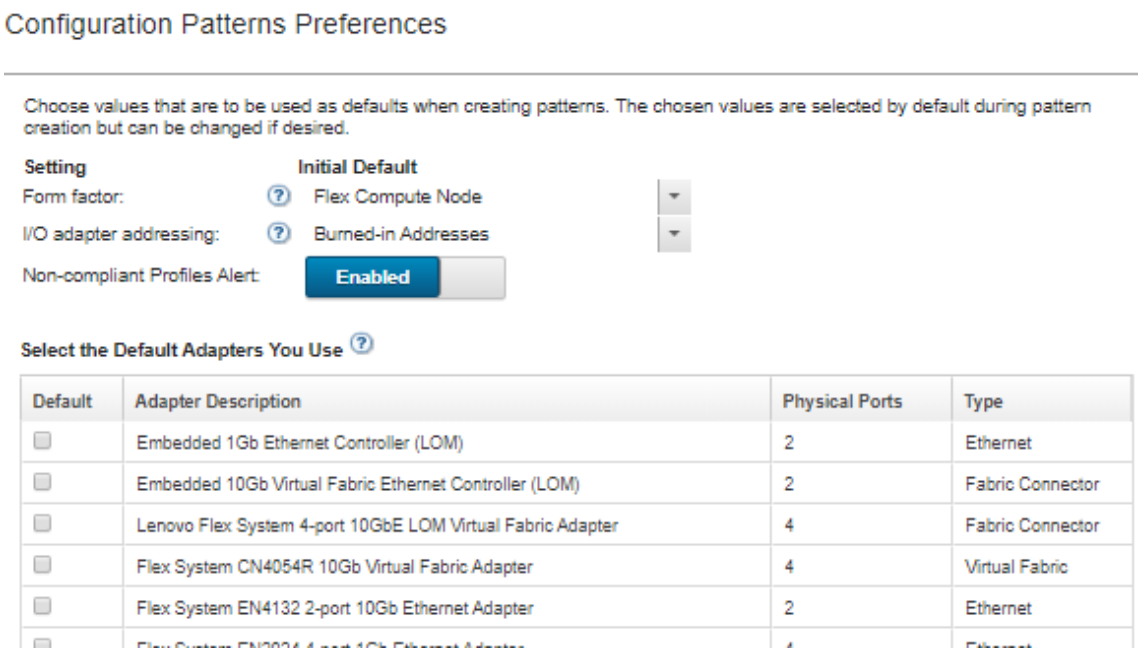
サーバー構成パターンを作成するときにデフォルトで選択される値を定義できます。それらの値は、サーバー・パターンの作成時に変更できます。

手順

デフォルトのサーバー構成設定を設定するには、以下のステップを実行してください。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで「**プロビジョニング**」をクリックし、「**構成パターン**」の後ろにあるヘルプ・アイコン ( ) をクリックして「構成パターン: はじめに」ページを表示します。

ステップ 2. 「**構成パターン設定の設定**」をクリックして、「構成パターン設定」ダイアログを表示します。



ステップ 3. デフォルト・サーバー・フォーム・ファクターを選択します。

ステップ 4. デフォルトの I/O アダプター・アドレス指定モードを選択します。

- 「**出荷時書き込み**」。製造時にアダプターに付与されたワールド・ワイド・ネーム (WWN) およびメディア・アクセス制御 (MAC) の既存のアドレスを使用します。
- 「**仮想**」。仮想 I/O アダプター・アドレス指定を使用して、LAN の接続および SAN の接続の管理を簡素化します。I/O アドレスを仮想化すると、出荷時書き込みハードウェア・アドレスが仮想化されたファイバー WWN およびイーサネット MAC アドレスで再割り当てされます。これにより、SAN のゾーン・メンバーシップを事前構成することでデプロイメントの時間を短縮でき、ハードウェアの交換時に SAN のゾーニングと LUN のマスキングの割り当ての再構成を不要にすることによってフェイルオーバーを容易にできます。

  仮想アドレス指定を有効にすると、デフォルトでは、定義されているアダプターに関係なく、イーサネットと Fibre Channel の両方のアドレスが割り当てられます。イーサネット・アドレスと Fibre Channel アドレスの割り当て元のプールを選択できます。

  アドレス指定モードの横にある「**編集**」アイコン ( ) をクリックして、仮想アドレスの設定を編集することもできます。

  制限: 仮想アドレス指定は、Flex System シャーシ内のサーバーでのみサポートされています。ラック・サーバーとタワー・サーバーはサポートされていません。

ステップ 5. サーバーの構成設定が、割り当てられたサーバー構成プロファイルと一致しない場合、アラートの生成を有効にするか無効にするかを選択します。

アラートは、アクティブ・プロファイル (ASSIGNED または ERROR_ACTIVATING 状態) に非準拠の場合のみ発生します。

サーバーの構成が準拠になった場合、またはサーバー・プロファイルが割り当て解除された場合、非準拠プロファイル・アラートが削除されます。

ステップ 6. 選択リストで、設定アダプターとして使用するデフォルトの I/O アダプターを 1 つ以上選択します。

ステップ 7. 「**保存**」をクリックします。

スイッチ構成テンプレートの作成

スイッチ構成テンプレートを作成する際には、特定の構成タイプの設定を定義します。

始める前に

スイッチ構成テンプレートを作成する前に、以下のアドバイスについて検討してください。

- 同じハードウェア・オプションを持ち、同じように構成する必要があるスイッチのグループを特定します。スイッチ構成テンプレートを使用すると、複数のスイッチに同じ構成設定を適用できるため、共通の構成を 1 か所から制御できます。
- カスタマイズする必要のある構成設定を特定します (たとえば、共通、ポート・チャネル、または VLAN 設定)。

手順

スイッチ構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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から、作成するテンプレートのタイプを選択します。

ステップ 3. 「**作成**」アイコン ( ) をクリックして、「新しいテンプレートの作成」ダイアログを表示します。

このダイアログに表示されているフィールドは、テンプレートのタイプに応じて異なります。

ステップ 4. 「**保存**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**保存してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

終了後

「**保存してデプロイ**」をクリックした場合は、「スイッチ・テンプレートのデプロイ」ページが表示されます。このページでは、スイッチ構成テンプレートを特定のスイッチにデプロイできます。

「**保存**」をクリックした場合、スイッチ構成テンプレートが「スイッチ構成テンプレート」ページに保存されます。このページでは、選択したサーバー・パターンに対して以下の操作を実行できます。

- 「名前」列でテンプレート名をクリックして、テンプレートの詳細を表示する。
- すべてのテンプレートの集約リストを表示し、「**その他**」 → 「**すべてのテンプレート**」をクリックします。
- テンプレートをデプロイする (ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照)。
- 「**コピー**」アイコン ( ) をクリックし、テンプレートをコピーして変更する。
- 「**編集**」アイコン ( ) をクリックして、テンプレートを編集する。

注：テンプレートに対する変更は、元のテンプレートがデプロイされていたスイッチに*自動的に再デプロイされません。*

- 「**名前変更**」アイコン () をクリックして、パターンの名前を変更する。
- 「**削除**」アイコン () をクリックして、パターンを削除する。

VLAN ポート・メンバーシップ設定の定義

VLAN ポート・メンバーシップ構成テンプレートを使用して、1 つ以上の (トランク用) VLAN に物理ポートおよびポート・チャネルを追加できます。

手順

ポート・メンバーシップ構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAN**」 → 「**ポート・メンバーシップ構成**」をクリックし、「**作成**」アイコンをクリックします ()。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

重要：1 つ以上の物理 L2 インターフェースまたはポート・チャネル ID を指定する必要があります。

- テンプレートの名前と説明を入力します。
- 1 つ以上の有効な物理 L2 インターフェースを指定します。たとえば、コンマで区切ったインターフェース、ダッシュで区切った ID の範囲、またはその両方の組み合わせにより、インターフェースのリストを指定できます。
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- 有効なポート・チャネル ID (ポート・アグリゲーター・インターフェース) を 1 つ以上指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- ポートがタグ付きトラフィックまたはタグなしのトラフィックを受け入れるかどうかを選択します。これは以下のいずれかの値です。
  - **アクセス**。このポートは、単一の VLAN のトラフィックを実行します。
  - **トランク**。(デフォルト) このポートは、スイッチでアクセス可能なすべての VLAN トラフィックを実行します。
- ポートの VLAN メンバーシップのリストに追加する 1 つ以上の VLAN ID を指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

注：

- ポート・モードが「アクセス」に設定されている場合、最初の VLAN ID のみが使用されます。たとえば、範囲 2-4,5,10-20 では、2 のみが使用されます。
- CNOS はデフォルトで VLAN ID 4000 ～ 4095 を予約します。予約済み VLAN ID (CNOS またはその他のユーザー) を使用すると、スイッチ構成のデプロイメントが失敗する可能性があります。

- タグなしトラフィックをタグ付けするネイティブ VLAN ID を指定します。1 ～ 4096 の数字を入力できます。

  注：
  - このフィールドは、ポート・モードが「トランク」である場合にのみ無効です
  - 指定されていない場合、または ID がポートのエンド・ステート VLAN の外部にある場合、ポートは事実上、タグが付いていないトラフィックを許可しません。

- 「**VLAN の作成**」を選択すると、ターゲット・スイッチで現在欠落している VLAN ID が作成されます。

  作成されていない VLAN にポートが属している場合、そのポートは引き続きその VLAN のメンバーであるにもかかわらず、その VLAN ID でタグ付けされてポートに到達するトラフィックは合格できません。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAN プロパティーの定義

VLAN プロパティ構成テンプレートを使用して、VLAN の詳細プロパティを定義できます。

手順

VLAN プロパティ構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAN**」 ➡ 「**VLAN プロパティ構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- 変更を適用する VLAN ID を指定します。1 ～ 4095 の数字を入力できます。

  注：CNOS はデフォルトで VLAN ID 4000 ～ 4095 を予約します。予約済み VLAN ID (CNOS またはその他のユーザー) を使用すると、スイッチ構成のデプロイメントが失敗する可能性があります。

- VLAN のカスタム名を指定します。
- VLAN がアクティブ (有効) 状態または中断 (無効) 状態であるかを選択します。
- IPv4 または IPv6 インターフェースで、ターゲット VLAN 上の IP マルチキャスト (IPMC) フラッドを管理 (有効) するかどうかを選択します。これは以下のいずれかの値です。
  - **無効**。IPv4 および IPv6 は無効です。
  - **有効**。IPv4 および IPv6 は有効です。
  - **IPv4 の無効化**。
  - **IPv4 の有効化**

- **IPv6 の無効化**
- **IPv6 の有効化**

このアクションは加法的で、「無効」の上にデプロイされる「IPv4 の無効化」は「IPv4 の有効化」となりますが、「IPv6 の有効化」の上へのデプロイは「有効」になります。無効化のオプションではこの逆のことがあてはまります。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAN 設定の削除

VLAN の削除テンプレートを使用して VLAN からインターフェースを削除できます。

手順

VLAN の削除テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAN**」 ➡ 「**VLAN の削除**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

重要：1 つ以上の物理 L2 インターフェースまたはポート・チャネル ID を指定する必要があります。

- テンプレートの名前と説明を入力します。
- 1 つ以上の有効な物理 L2 インターフェースを指定します。たとえば、コンマで区切ったインターフェース、ダッシュで区切った ID の範囲、またはその両方の組み合わせにより、インターフェースのリストを指定できます。
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- 有効なポート・チャネル ID (ポート・アグリゲーター・インターフェース) を 1 つ以上指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- ポートの VLAN メンバーシップのリストから削除する 1 つ以上の VLAN ID を指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13

注：ポート・モードが「アクセス」に設定されている場合、VLAN を取り外すとポートが VLAN 1 に移行します。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAN の削除

VLAN の削除テンプレートを使用してスイッチから VLAN 構成を削除できます。

手順

VLAN の削除テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAN**」 ➡ 「**VLAN の削除**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- ポートの VLAN メンバーシップのリストから削除する 1 つ以上の VLAN ID を指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

注：リザーブされている VLAN ID を削除することはできません。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

ポート・チャネル基本設定の定義

ポート・チャネル基本構成テンプレートを使用して、ポート・アグリゲーターを作成し、ポートをアグリゲーターに追加できます。

ポート・チャネルにポートが存在し、それらのポートの一部がテンプレートに含まれている場合、そのプロパティ (ポートの優先順位、モード、タイムアウト) はテンプレートのデプロイ時にテンプレートの設定で更新されます。

手順

ポート・チャネル基本構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**ポート・チャネル**」 ➡ 「**基本構成**」をクリックし、「**作成**」アイコン ( ) をクリックします。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- 1 つ以上の有効な物理 L2 インターフェースを指定します。たとえば、コンマで区切ったインターフェース、ダッシュで区切った ID の範囲、またはその両方の組み合わせにより、インターフェースのリストを指定できます。
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- 作成または更新するポート・チャネル ID (ポート・アグリゲーター・インターフェース) を指定します。1 ～ 4095 の数字を入力できます。
- リンク集約制御プロトコル (LACP) ポート・モードを指定します。これは以下のいずれかの値です。
  - **アクティブ**。(デフォルト) LACP を無条件で有効にします
  - **パッシブ**。LCAP デバイスが検出された場合にのみ LACP を有効にします。
  - **Static**。LCAP を無効にします

  注：アクティブおよびパッシブは同じアグリゲーター内で混在させることができますが、静的は混在できません。
- LACP ポートの優先順位を指定します。1 ～ 65535 の数字を入力できます。

  注：LACP ポートの優先順位は、LACP ポート ID からのポート番号に使用されます。
- LACP タイムアウト・モードは、LCAP が個々のモードに入る前に指定します。これは以下のいずれかの値です。
  - **長い**。(デフォルト) 90 秒
  - **短い**。3 秒

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

ポート・チャネル詳細設定の定義

ポート・チャネル拡張構成テンプレートを使用して、ポート・チャネルの詳細プロパティを定義できます。

手順

ポート・チャネル詳細構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**ポート・チャネル**」 ➡ 「**拡張構成**」をクリックし、「**作成**」アイコン ( ) をクリックします。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- 更新するポート・チャネル ID (ポート・アグリゲーター・インターフェース) を指定します。1 ～ 4095 の数字を入力できます。

- LACP に障害が発生した場合に個々のポートをアクティブのままにするかどうかを選択します。これは以下のいずれかの値です。
  - **アクティブ**。(デフォルト) LACP を無条件で有効にします。
  - **中断**。LACP を無効にします。
- ポート・チャネルがアップとみなされるためにアップである必要があるリンクの最小数を指定します。1 ～ 32 の数字を入力できます。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

ポート・チャネルの削除

ポート・チャネルの削除テンプレートを使用して、スイッチからポート・チャネルを削除できます。

手順

ポート・チャネルの削除テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**ポート・チャネル**」 ➡ 「**ポート・チャネルの削除**」をクリックし、「**作成**」アイコン ( ) をクリックします。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- 削除するポート・チャネル ID (ポート・アグリゲーター・インターフェース) を 1 つ以上指定します。コンマで区切った数字、ダッシュで区切った数字の範囲、またはその両方の組み合わせにより数字のリストを指定できます。値および範囲は、たとえば次のように、1 ～ 4096 の数値にすることができます。
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

全般スイッチの設定の定義

全般スイッチのプロパティは、共通汎用構成テンプレートを使用して構成できます。

手順

スイッチの共通汎用構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**グローバル**」 ➡ 「**汎用構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- LACP システム ID の生成に使用される LACP システムの優先順位を指定します。1 ～ 65535 の数字を入力できます。
- ネイティブ VLAN タグ付けを有効にする場所を選択します。これは以下のいずれかの値です。
  - **入力および出力**
  - **出力のみ**

  注：このプロパティは CNOS 10.10.1 以降でサポートされています。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

共通 L2 インターフェース設定の定義

L2 インターフェース構成テンプレートを使用して、L2 インターフェースの VLAN タグ付けプロパティを構成することができます。

手順

L2 インターフェース構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**共通**」 ➡ 「**L2 インターフェース構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- 1 つ以上の有効な物理 L2 インターフェースを指定します。たとえば、コンマで区切ったインターフェース、ダッシュで区切った ID の範囲、またはその両方の組み合わせにより、インターフェースのリストを指定できます。
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- ネイティブ VLAN タグ付けを有効にする場所を選択します。これは以下のいずれかの値です。
  - **入力および出力**
  - **出力のみ**

  注：このプロパティは CNOS 10.10.1 以降でサポートされています。
- トンネリング (QinQ) サポートを有効にするか無効にするかを選択します。

  注：このプロパティは CNOS 10.10.1 以降でサポートされています。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

ピア VLAG 設定の定義

VLAG ピアを構成するには、VLAG ピア構成テンプレートを使用します。

手順

VLAG ピア構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAG**」 → 「**ピア構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- VLAG を有効にするか無効にするかを選択します。
- ピア 1 とピア 2 では、以下のフィールドに入力します。両方のピアのフィールドに値を入力する必要があります。
  - ヘルス・チェックに使用する VLAG ピアの IIPv4 または IPv6 アドレスを指定します。
  - 2 つのピア間で使用するポート・チャネルの ID を指定します。1 ～ 4095 の数字を入力できます。
  - ヘルス・チェックに使用する VRF を指定します (たとえば、管理、デフォルト、customVRF)。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAG インスタンス設定の定義

VLAG インスタンス構成テンプレートを使用して、VLAG インスタンスを作成または更新できます。VLAG インスタンスは、VLAG が 1 つのデバイスとして表示される両方のスイッチ (通常はポート集約によって) に接続されているデバイスです。

手順

VLAG インスタンス構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAG**」 → 「**インスタンス構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- VLAG ID を指定します。1 ～ 64 の数字を入力できます。
- ピア 1 とピア 2 に接続されているポート・チャネルの ID を指定します。この値は 1 ～ 4095 の数値にすることができます。
- VLAG インスタンスを有効にするか無効にするかを選択します。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAG 詳細設定の定義

VLAG 詳細構成テンプレートを使用して、VLAG の詳細プロパティを定義できます。

手順

VLAG 詳細構成テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAG**」 ➡ 「**拡張構成**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- どのピアが 1 次であるかを制御するために使用される優先順位を指定します。1 ～ 65535 の数字を入力できます。

  指定しない場合、スイッチのデフォルトの優先順位が使用されます。CNOS では、デフォルトは 0 です。
- 同時リブート後に VLAG がオンラインになるまでの猶予期間を秒単位で指定します。240 ～ 3600 の数字を入力できます。

  指定しない場合、スイッチのデフォルトが使用されます。CNOS では、デフォルトは 300 です。
- 同じネットワーク内の VLAG セットアップを区別するために使用される階層 ID を指定します。1 ～ 512 の数字を入力できます。
- ピアの再ロード後にポートを起動するまでの時間を遅らせるために使用される vLAG 起動遅延間隔を秒単位で指定します。0 ～ 3600 の数字を入力できます。

  指定しない場合、スイッチのデフォルトが使用されます。CNOS では、デフォルトは 120 です。
- VLAG が失敗するまでの VLAG キープ・アライブ試行 (未応答の hello メッセージ) の数を指定します。1 ～ 24 の数字を入力できます。

  指定しない場合、スイッチのデフォルトが使用されます。CNOS では、デフォルトは 3 です。
- VLAG キープ・アライブ試行の間隔を秒単位で指定します。2 ～ 300 の数字を入力できます。

  指定しない場合、スイッチのデフォルトが使用されます。CNOS では、デフォルトは 5 です。
- VLAG キープ・アライブ再試行の間隔を秒単位で指定します。1 ～ 300 の数字を入力できます。

  指定しない場合、スイッチのデフォルトが使用されます。CNOS では、デフォルトは 30 です。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

VLAG インスタンスの削除

VLAG インスタンスの削除テンプレートを使用して、VLAG インスタンスを削除できます。

手順

VLAG インスタンスの削除テンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**VLAG**」 → 「**インスタンスの削除**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- VLAG インスタンスの固有 ID を指定します。1 ～ 64 の数字を入力できます。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

スパイン・リーフ・トポロジーの定義

物理的なトポロジーを確認し、スパイン・リーフ・トポロジー・ウィザードのテンプレートを使用して、管理対象スイッチに SpineLeaf (L3 ファブリック) セットアップをデプロイできます。

手順

スパイン・リーフ・トポロジー・ウィザードのテンプレートを作成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」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、「**スパイン・リーフ**」 → 「**トポロジー・ウィザード**」をクリックし、「**作成**」アイコンをクリックします ( )。

ステップ 3. 「新しいテンプレートの作成」ダイアログで、以下の情報を指定します。

- テンプレートの名前と説明を入力します。
- スイッチで実行されているボーダー・ゲートウェイ・プロトコル (BGP) プロトコルの自律システム (AS) の数を指定します。1 ～ 4294967295 の数字を入力できます。

  注：このプロパティは CNOS 10.9.3 以降でサポートされています。
- スイッチ間の単一のリンクを許可するかどうかを選択します。

  通常、スパイン・スイッチとリーフ・スイッチ間に少なくとも 2 つのリンクがない場合、デプロイメントは失敗します。

ステップ 4. 「**作成**」をクリックしてテンプレートを保存するか、パターンを保存してすぐに 1 つ以上の管理対象ラック・スイッチにテンプレートをデプロイする場合は、「**作成してデプロイ**」をクリックします。

テンプレートのデプロイについて詳しくは、ターゲット・スイッチへのスイッチ構成テンプレートのデプロイを参照してください。

ターゲット・スイッチへのスイッチ構成テンプレートのデプロイ

VLAN ポート構成テンプレートを作成することで、VLAN ポート設定を定義できます。

このタスクについて

デプロイメントには、次の 3 つのタイプがあります。

- **正常**。基本レイヤー・アーキテクチャー内の 1 つ以上のラック・スイッチにスイッチ構成設定をデプロイします。
- **VLAG**。仮想リンク集約グループ (VLAG) アーキテクチャをサポートする指定の 2 つのスイッチにスイッチ構成設定をデプロイします。このスイッチのモデルおよびソフトウェア・バージョンは同じであることが必要です。
- **スパイン・リーフ**。1 つ以上のスパイン・スイッチとリーフ・スイッチにテンプレートを展開します。

手順

スイッチ構成テンプレートを 1 台以上の管理対象スイッチにデプロイするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」ページが表示されます。

ステップ 2. デプロイするスイッチ構成テンプレートを 1 つ以上選択します。

ステップ 3. 「**デプロイ**」アイコン () をクリックして、「テンプレートのデプロイ」ダイアログを表示します。

ステップ 4. テンプレートをデプロイするスイッチを 1 台以上選択します。

選択したテンプレートと互換性のあるスイッチのみが表示されます。

ステップ 5. 「**デプロイ**」をクリックします。ダイアログが開き、選択した各スイッチのデプロイメント・ステータスが表示されます。

ステップ 6. もう一度「**デプロイ**」をクリックして、デプロイメント・プロセスを開始します。

注：デプロイが完了するまでに数分かかることがあります。

終了後

デプロイメントの履歴を表示できます (スイッチ構成デプロイメント履歴の表示 を参照)。

スイッチ構成デプロイメント履歴の表示

テンプレートの名前、テンプレートのタイプ、タイムスタンプ、デプロイ先のスイッチを含めて、管理対象スイッチにデプロイ済みであるスイッチ構成テンプレートに関する情報を表示できます。各デプロイメントには、デプロイ時のスナップショット・テンプレートが含まれています。

手順

スイッチ構成デプロイメント履歴を表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**構成テンプレートの切り替え**」の順にクリックします。「スイッチ構成テンプレート」ページが表示されます。

ステップ 2. 左ナビゲーションの「**デプロイメント**」を展開し、「**履歴**」をクリックすると、デプロイ済みテンプレートのテーブルが表示されます。

「**ステータス**」列に、構成デプロイメントが正常に完了したかどうかが示されます。状態は以下のいずれかです。

- 「**成功**」。すべてのターゲット・スイッチへの構成のデプロイメントが正常に完了しました。
- 「**警告**」。1 つ以上のターゲット・スイッチへの構成のデプロイメントが完了しましたが、警告があります。
- 「**失敗**」。1 つ以上のターゲット・スイッチへの構成のデプロイメントが失敗しました。

終了後

- テーブルのテンプレート名をクリックして、デプロイされたテンプレートや成功したか失敗したかなど、デプロイされた各テンプレートに関する情報を表示できます。
- デプロイメントを選択し、「**削除**」アイコン ( ) をクリックすると、デプロイメント履歴がクリアされます。

第 13 章　管理対象デバイスでのファームウェアの更新

Lenovo XClarity Administrator Web インターフェースから、シャーシ、サーバー、ストレージ・システム、およびスイッチなどの管理対象デバイスのファームウェア更新について、ダウンロード、インストール、管理を実行できます。ファームウェア・コンプライアンス・ポリシーを管理対象デバイスに割り当て、それらのデバイスのファームウェアの適合状態が保たれるようにすることができます。検証されたファームウェア・レベルが推奨される事前定義ポリシーと一致しない場合、ファームウェア・コンプライアンス・ポリシーを作成および編集することもできます。

詳細:
- XClarity Administrator: ファームウェア更新時の 効率の向上
- Lenovo ThinkSystem ファームウェアおよび ドライバー更新のベスト・プラクティス
- XClarity Administrator: ベア・メタルからクラスターへ
- XClarity Administrator: ファームウェア更新
- XClarity Administrator: ファームウェア・ セキュリティー更新のプロビジョニング

始める前に

XClarity Administrator では、ファームウェアの更新とデバイス・ドライバーの更新は別の処理であり、これらの処理に関連はありません。XClarity Administrator では、デバイス・ドライバーをファームウェアと同時に更新することをお勧めしますが、管理対象デバイスのファームウェアとデバイス・ドライバーの間のコンプライアンスは維持されません。

このタスクについて

注：オペレーティング・システムはファームウェアを更新する必要がありません。ベア・メタル・サーバーの場合は、ファームウェアを更新する前に、サーバーの電源がオフになっていることを確認してください。

以下の管理対象デバイスのファームウェア更新を管理および適用できます。
- **Chassis**。CMM 更新
- **ThinkAgile、ThinkSystem、System x、コンバージド、Flex System および NeXtScale サーバー**。ベースボード管理コントローラー、UEFI、DSA、メザニン、およびアダプターの更新
- **RackSwitch および Flex System スイッチ**
- **Lenovo Storage および ThinkSystem DM ストレージ・デバイス**
- **IBM TS4300 テープ・ライブラリー・デバイス**

以下のデバイスのファームウェアは、XClarity Administrator から更新できません。

- **ThinkServer サーバー**。ファームウェアの更新方法に関する情報ついては、サーバーに付属の資料を参照してください。
- **Flex Power Systems 計算ノード**。Flex Power Systems 計算ノードのファームウェアを更新するにはいくつかの方法があります。詳しくは、IBM Flex System p260/p460 計算ノード オンライン・ドキュメントを参照してください。その他の Flex Power Systems 計算ノードのプロセスも同様です。
- **スタック・モードまたは保護モードの Flex スイッチ**。スタック・スイッチのファームウェアは*更新できません*。スタックされているすべてのスイッチでは、ファームウェアの更新が無効になります。
- **Flex スイッチ**。以下のスイッチを使用している場合は、ファームウェアの更新方法に関する情報については、そのスイッチに付属のドキュメントを参照してください。
  - Cisco Nexus B22 Fabric Extender

手順

次の図は、管理対象デバイスのファームウェア更新のワークフローを示しています。

ステップ 1. **ファームウェア更新リポジトリーの管理**

*ファームウェア更新リポジトリー*には、管理対象デバイスに適用できる使用可能な更新および更新パッケージのカタログが含まれます。

*カタログ*には、 XClarity Administrator でサポートされているすべてのデバイスに対して、現在使用できるファームウェア更新に関する情報が含まれます。このカタログでは、ファームウェア更新がデバイス・タイプごとに分類されています。カタログを最新の情報に更新すると、XClarity Administrator は Lenovo の Web サイト (メタデータ .xml または .json および readme .txt ファイルを含む) から利用可能な最新のファームウェア更新に関する情報を取得し、その情報をファームウェア更新リポジトリーに保存します。ペイロード・ファイル (.exe) がダウンロードされていません。カタログの更新について詳しくは、製品カタログの更新を参照してください。

新しいファームウェア更新が使用可能になったとき、管理対象デバイスでそのファームウェアを更新するには、最初に更新パッケージをダウンロードする必要があります。カタログを更新しても、更新パッケージが自動的にダウンロードされるわけではありません。ファームウェア更新リポジトリーページにある**製品カタログ**表では、どの更新パッケージがダウンロード済みで、どれがダウンロード可能かを識別できます。

ファームウェア更新をダウンロードするには、いくつかの方法があります。

- **ファームウェア更新リポジトリー・パック**

  ファームウェア更新リポジトリー・パックとは、最もサポートされているすべてのデバイスに対する XClarity Administrator のリリースと同時に使用できる、最新のファームウェアのコレクションであり、更新済みのデフォルトのファームウェア・コンプライアンス・ポリシーです。これらのリポジトリー・パックは、インポートされた後管理サーバーの更新ページで適用されます。ファームウェア更新リポジトリー・パックを適用すると、パック内の各更新パッケージがファームウェア更新リポジトリーに追加され、すべての管理可能デバイスでデフォルトのファームウェア・コンプライアンス・ポリシーが自動的に作成されます。この事前定義済みポリシーはコピーすることはできますが、変更することはできません。

  以下のリポジトリー・パックを使用できます。

  - **lnvgy_sw_lxca_cmmswitchrepo*x-x.x.x*_anyos_noarch**。すべての CMM および Flex System スイッチのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_storagerackswitchrepo*x-x.x.x*_anyos_noarch**。すべての RackSwitch スイッチと Lenovo Storage デバイスのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_systemxrepo*x-x.x.x*_anyos_noarch**。すべての Converged HX シリーズ、Flex System、NeXtScale、および System x サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_thinksystemrepo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_thinksystemv2repo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem V2 サーバーのファームウェア更新が含まれます。
  - **lnvgy_sw_lxca_thinksystemv3repo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem V3 サーバーのファームウェア更新が含まれます。

「管理サーバーの更新」ページの「**ダウンロード・ステータス**」列で、ファームウェア更新リポジトリー・パックがリポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

- **ダウンロード済み**。ファームウェア更新リポジトリー・パックはリポジトリーに保存されています。
- **未ダウンロード**。ファームウェア更新リポジトリー・パックは使用できますが、リポジトリーに保存されていません。

- UpdateXpress System Packs (UXSPs)

  注：XCC2 を持つサーバーの場合、これらのパックはファームウェア・バンドルと呼ばれます。*バンドル*は、パッケージ名および事前定義されたポリシー名で使用されます。

  UXSP には、オペレーティング・システムごとに分類された利用可能な最新のファームウェアおよびデバイス・ドライバーの更新が含まれています。UXSP をダウンロードすると、カタログに示されたバージョンに基づいて UXSP が XClarity Administrator によりダウンロードされ、ファームウェア更新リポジトリーに更新パッケージが保存されます。UXSP をダウンロードすると、UXSP 内の各ファームウェア更新がファームウェア更新リポジトリーに追加され、「**個別更新**」タブにリストされ、以下の名前を使用してすべての管理可能デバイスにデフォルトのファームウェア・コンプライアンス・ポリシーが自動的に作成されます。この事前定義済みポリシーはコピーすることはできますが、変更することはできません。
  - *{uxsp-version}-{date}-{server-short-name}*-UXSP (例: `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{buildnumber}-{server-short-name}*-bundle (例、`22a.0-kaj92va-SR650V3-bundle`)

  注：「ファームウェア更新: リポジトリー」ページから UXSP をダウンロードまたはインポートした場合、ファームウェア更新のみがダウンロードされ、リポジトリーに保存されます。デバイス・ドライバーの更新は破棄されます。UXSP を使用した Windows デバイス・ドライバー更新のダウンロードまたはイン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 OS デバイス・ドライバー・リポジトリーの管理。

  「ファームウェア更新: リポジトリー」ページの「**個別更新**」タブにある「**ダウンロード状況**」の列で、UXSP がファームウェア更新リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

  - **ダウンロード済み**。更新パッケージ全体または個々のファームウェア更新がリポジトリーに保存されています。
  - ***x*/*y* ダウンロード済み**。更新パッケージ内の一部のファームウェア更新がリポジトリーに保存されています。括弧内の番号は、利用可能な更新数と、保存された更新数、または特定のデバイス・タイプの更新がないことを示します。
  - **未ダウンロード**。更新パッケージ全体または個々のファームウェア更新を使用できますが、リポジトリーに保存されていません。

- **個別のファームウェア更新**

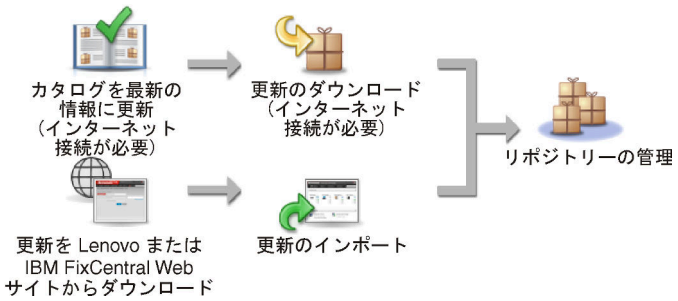
  ファームウェア更新パッケージを個別にダウンロードすることもできます。ファームウェア更新パッケージをダウンロードすると、カタログに示されたバージョンに基づいて更新が XClarity Administrator によりダウンロードされ、ファームウェア更新リポジトリーに更新パッケージが保存されます。その後、これらの更新パッケージを使用して、各管理対象デバイスのファームウェア・コンプライアンス・ポリシーを作成できます。

  注：コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。管理対象サーバーにどのファームウェア更新パッケージを使用するかについて詳しくは、ファームウェア更新のダウンロードを参照してください。

「ファームウェア更新: リポジトリー」ページの「**個別更新**」タブの「**ダウンロード・ステータス**」列で、*ファームウェア更新*がファームウェア更新リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

- **ダウンロード済み**。更新パッケージ全体または個々のファームウェア更新がリポジトリーに保存されています。
- ***x*/*y* ダウンロード済み**。更新パッケージ内の一部のファームウェア更新がリポジトリーに保存されています。括弧内の番号は、利用可能な更新数と、保存された更新数、または特定のデバイス・タイプの更新がないことを示します。
- **未ダウンロード**。更新パッケージ全体または個々のファームウェア更新を使用できますが、リポジトリーに保存されていません。

カタログを更新してファームウェア更新をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていない場合、Web ブラウザーを使用して XClarity Administrator ホストへのネットワーク・アクセスを持つワークステーションにファイルを手動でダウンロードし、ファームウェア更新リポジトリにファイルをインポートします。



XClarity Administrator に手動でファームウェア更新をインポートする際は、ペイロード (イメージと MIB)、メタデータ、変更履歴、README の各ファイルを含める必要があります。例:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

注意：

- これらの必要なファイルのみをインポートします。ファームウェアのダウンロード Web サイトに記載されている他のファイルはインポートしないでください。
- 更新パッケージに XML ファイルが含まれていない場合、更新はインポートされません。
- 更新に関連する必要なすべてのファイルを含めなかった場合、リポジトリーで更新が未ダウンロードと表示されます。これは、一部インポート済みであることを意味します。その後、不足しているファイルを選択してインポートできます。
- コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。管理対象サーバーにどのファームウェア更新パッケージを使用するかについて詳しくは、ファームウェア更新のダウンロードを参照してください。

ファームウェア更新について詳しくは、ファームウェア更新リポジトリーの管理を参照してください。

ステップ 2. **(オプション) ファームウェア・コンプライアンス・ポリシーの作成と割り当て**

*ファームウェア・コンプライアンス・ポリシー*を使用すると、注意が必要なデバイスにフラグを付けることで、特定の管理対象デバイス上のファームウェアを現在のレベルまたは指定されたレベルに維持することができます。各ファームウェア・コンプライアンス・ポリシーは、デバイスのコンプライアンスを保つために、監視対象のデバイスと、インストールする必要のあるファームウェア・レベルを指定します。コンプライアンスは、デバイスまたはファームウェア・コンポーネントのレベルで設定できます。その後、XClarity Administrator はこれらのポリシーを使用して、管理対象デバイスのステータスを確認し、コンプライアンスに違反しているデバイスを特定します。

ファームウェア・コンプライアンス・ポリシーを作成するときは、以下のような場合に XClarity Administrator がデバイスにフラグを立てるように選択できます。

- デバイスのファームウェアが下位レベル
- デバイスのファームウェアがコンプライアンス・ターゲット・バージョンと完全に一致していない

XClarity Administrator には、**リポジトリの最新ファームウェア**と呼ばれる事前定義されたファームウェア・コンプライアンス・ポリシーが用意されています。新しいファームウェアがリポジトリーにダウンロードまたはインポートされると、このポリシーが更新されて、リポジトリー内で使用可能なファームウェアの最新バージョンが含まれるようになります。

ファームウェア・コンプライアンス・ポリシーをデバイスに割り当てた後、XClarity Administrator はデバイス・インベントリーの変更またはファームウェア更新リポジトリーの変更があると、各デバイスのコンプライアンス状況を確認します。デバイスのファームウェアが割り当てられたポリシーに準拠していない場合、XClarity Administrator はファームウェア・コンプライアンス・ポリシーで指定したルールに基づいて、「ファームウェア更新: 適用/アクティブ化」ページでデバイスを非準拠として識別します

たとえば、すべての ThinkSystem SR850 デバイスにインストールされたファームウェアの基準レベルを定義するファームウェア・コンプライアンス・ポリシーを作成し、そのファームウェア・コンプライアンス・ポリシーをすべての管理対象 ThinkSystem SR850 デバイスに割り当てることができます。ファームウェア更新リポジトリ—が最新の情報に更新され、新しいファームウェア更新が追加されると、それらの計算ノードがコンプライアンス違反となる可能性があります。その場合、XClarity Administrator は「ファームウェア更新: 適用/アクティブ化」ページを更新し、そのデバイスが非適合であることを表示して、アラートを生成します。

注：割り当てられたファームウェア・コンプライアンス・ポリシーの要件を満たしていないデバイスのアラートの表示または非表示を選択できます (ファームウェア更新の共通設定の構成を参照)。デフォルトではアラートは非表示です。

ファームウェア・コンプライアンス・ポリシーについて詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。

ステップ 3. **更新の取得とアクティブ化**

XClarity Administrator では、管理対象デバイスにファームウェア更新が自動的に適用されません。ファームウェアを更新するには、選択されたデバイスで更新を手動で適用してアクティブ化する必要があります。ファームウェアは以下のいずれかの方法で適用できます。

- **コンプライアンス・ポリシーを使用するバンドルされたファームウェア更新の適用**

適用可能なファームウェア更新パッケージを含むバンドル・イメージを使用して、割り当てられたファームウェア・コンプライアンス・ポリシーに従って、選択済みデバイスのすべてのコンポーネントにファームウェア更新を適用できます。

バンドル更新プロセスは、まず、ベースボード管理コントローラーと UEFI アウト・オブ・バンドを更新します。これらの更新が完了すると、プロセスは、マシン・タイプに基づいて、コンプライアンス ポリシー内の残りのファームウェアのバンドル・イメージを作成します。次に、プロセスは選択したデバイスにイメージをマウントし、デバイスを再起動してイメージをブートします。イメージは自動的に実行され、残りの更新が実行されます。

注意：選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 ➔ 「**ジョブ**」をクリックします。

注：

- バンドルされたファームウェアの更新の適用は、ThinkSystem SR635 および SR655 サーバーでのみサポートされています。
- バンドルされたファームウェア更新の適用は、IPv4 アドレスでのみサポートされています。IPv6 アドレスはサポートされていません。
- インベントリー情報全体を取得するために、各ターゲット・デバイスが少なくとも 1 回 OS にブートされたことを確認してください。
- バンドル更新機能を使用するには、ベースボード管理コントローラー・ファームウェア v2.94 以降が必要です。
- リポジトリー・パックからのファームウェア更新または個々のファームウェア更新のみが使用されます。UpdateXpress System Packs (UXSPs) はサポートされていません。
- ダウンロードしたファームウェア更新のみが適用されます。製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロード)。

  注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。
- コンプライアンス確認は、ThinkSystem SR635 および SR655 サーバーのベースボード管理コントローラーと UEFI でのみサポートされます。ただし、XClarity Administrator は、利用可能なすべてのハードウェア・コンポーネントにファームウェア更新を適用しようとします。
- 更新は、割り当てられたファームウェア・コンプライアンス・ポリシーに従って適用されます。コンポーネントのサブセットを更新することはできません。
- Lenovo XClarity Provisioning Manager (LXPM)、LXPM のウィンドウ・ドライバー、または LXPM Linux ドライバーのファームウェア更新を ThinkSystem SR635 および SR655 サーバーに適用するには、XClarity Administrator v3.2 以降が必要です。
- 現在インストールされているバージョンが、割り当てられたコンプライアンス・ポリシーよりも新しい場合、ベースボード管理コントローラーと UEFI の更新はスキップされます。
- ファームウェア・コンプライアンス・ポリシーが作成済みであり、ファームウェア更新を適用するデバイスに割り当て済みである必要があります。詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。
- 選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。

- コンプライアンス・ポリシーを使用する、または使用しない**選択済みファームウェア更新の適用**

  適用可能なファームウェア更新パッケージを使用する割り当てられたファームウェア・コンプライアンス・ポリシーに従って、選択済みコンポーネントとデバイスにファームウェア更新を適用できます。また、コンプライアンス・ポリシーを使用せずに、選択済みコンポーネントとデバイスに現在インストールされているファームウェアよりも新しいファームウェア更新を適用することもできます。

  特定のデバイスのすべてのコンポーネントに更新を適用することを選択できます。また、ベースボード管理コントローラーや UEFI など、選択済みデバイスでコンポーネントのサブセットのみを更新することもできます。

  ファームウェア更新をアクティブ化するには、デバイスを再起動する必要があります。(デバイスの再起動には中断が伴うことに注意してください。)更新プロセスの一部としてデバイスを再起動するか (*即時アクティベーション*と呼ばれます)、保守期間でデバイスを再起動できるようになるまで待機するか (*据え置きアクティベーション*と呼ばれます) を選択できます。この場合、更新を有効にするためにデバイスを手動で再起動する必要があります。

  管理対象デバイスのファームウェアを更新する場合は、以下の手順を実行します。

  1. XClarity Administrator がファームウェア更新 (たとえば、管理コントローラーの場合は UEFI や DSA など) をデバイスを送信します。
  2. デバイスが再起動すると、デバイスでファームウェアの更新がアクティブになります。
  3. サーバーの場合、XClarity Administrator がオプション・デバイスの更新 (ネットワーク・アダプターやハードディスク・ドライブの更新など) を送信します。XClarity Administrator によりこれらの更新が適用され、サーバーが再起動します。
  4. デバイスを再起動するか、即時アクティベーションを選択すると、オプション・デバイスの更新がアクティブになります。

  注：

  – コンプライアンス・ポリシーを使用して更新を適用する場合は、ファームウェア・コンプライアンス・ポリシーを作成し、各ターゲット・デバイスに割り当てる必要があります。詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。
  – 複数のコンポーネントに対する更新を含むファームウェア更新パッケージをインストールするように選択した場合、更新パッケージが適用されるすべてのコンポーネントが更新されます。
  – CMM および Flex スイッチに対する更新は、遅延アクティベーションを選択した場合でも、常に即座にアクティブ化されます。

デバイス一式で更新の実行をする場合、XClarity Administrator は、次の順番で更新を実行します。

- シャーシの CMM
- RackSwitch および Flex System スイッチ
- Flex 計算ノード、およびラックとタワー・サーバー
- Lenovo Storage デバイス

注意：管理対象デバイスでファームウェア更新を適用しようとする前に、以下の操作を完了していることを確認してください。

- 管理対象デバイスでファームウェアを更新する前に、ファームウェア更新の考慮事項を読んでください (ファームウェアの更新に関する考慮事項 を参照)。
- 最初は、更新がサポートされていないデバイスはビューに表示されません。サポートされていないデバイスを更新するように選択することはできません。

- デフォルトでは、検出されたすべてのコンポーネントが更新を適用できるコンポーネントとしてリストされますが、下位レベルのファームウェアが原因で、コンポーネントがインベントリーに表示されない可能性や、バージョン情報が詳細に報告されない可能性があります。更新を適用できる、すべてのポリシー・ベースのパッケージをリストに表示するには、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**下位レベルのデバイスの拡張サポート**」を選択します。このオプションを選択すると、未検出のデバイスの「インストール済みバージョン」列に「その他の利用可能なソフトウェア」がリストされます。詳しくは、ファームウェア更新の共通設定の構成を参照してください。

  注：

  – 管理対象デバイスに対する更新が進行中の場合、グローバル設定を変更することはできません。

  – 追加のオプションを生成するには数分かかります。しばらくしてから、テーブルを更新するために「**最新表示**」アイコン ( ) をクリックする必要がある場合があります。

- ターゲット・サーバーで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 ➡ 「**ジョブ**」をクリックします。

- デプロイするファームウェア・パッケージがファームウェア更新リポジトリーに含まれていることを確認します。含まれていない場合は、製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロードを参照)。

  注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。

  前提条件ファームウェアをインストールする場合は、前提条件ファームウェアもリポジトリーにダウンロードしていることを確認してください。

  場合によっては、ファームウェアを更新するために複数のバージョンが必要になることがあり、その場合はすべてのバージョンをリポジトリーにダウンロードする必要があります。たとえば、IBM FC5022 SAN スケーラブル・スイッチを v7.4.0a から v8.2.0a にアップグレードするには、まず v8.0.1-pha、次に v8.1.1、そして v8.2.0a をインストールします。スイッチを v8.2.0a に更新するには、この 3 つのバージョンすべてがリポジトリーに含まれる必要があります。

- 通常、ファームウェア更新をアクティブ化するにはデバイスを再起動する必要があります。更新プロセス中にデバイスの再起動を選択した場合 (*即時アクティベーション*)、必ず実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。

更新のインストールについて詳しくは、ファームウェア更新の適用とアクティブ化を参照してください。

ファームウェアの更新に関する考慮事項

Lenovo XClarity Administrator を使用して管理対象デバイスのファームウェアを更新する前に、以下の重要な考慮事項を確認してください。

- 一般的な考慮事項
- CMM の考慮事項
- ベースボード管理コントローラーに関する考慮事項
- ThinkSystem デバイスに関する考慮事項
- Flex System デバイスに関する考慮事項

- ストレージに関する考慮事項

一般的な考慮事項

- **ファームウェア・レベルの最小要件。**

  XClarity Administrator を使用してそれらのデバイスでファームウェアを更新する前に、各管理対象デバイスにインストールされたファームウェアが最小限必要なレベルにあ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。

  注：I/O デバイスのサポートと既知の制限について詳しくは、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。

- **すべてのコンポーネントをファームウェア更新リポジトリーに含まれているレベルに更新する。**

  Flex System コンポーネントのファームウェア更新がまとめてテストおよびリリースされているため、Flex System シャーシ内のすべてのコンポーネントでファームウェア・レベルを同じに保つことをお勧めします。そのため、シャーシ内のすべてのコンポーネントのファームウェアを同じ保守期間に更新することが重要です。選択した更新は、XClarity Administrator により自動的に適切な順序で適用されます。

- **LXPM Linux ドライバーおよび LXPM Windows ドライバーは、UXSP のダウンロード時には含まれていません**

  Lenovo XClarity Provisioning Manager (LXPM) Linux および Windows ドライバーは、UpdateXpress System Packs (UXSPs)に含まれていません。これらの更新パッケージをデバイスに適用するには、最新のファームウェア更新リポジトリー・パックをダウンロードするか、個別のパッケージを手動でダウンロードして、それらのパッケージを含めるファームウェア・コンプライアンス・ポリシーを作成します。

- **一部のファームウェア更新と最小レベルのデバイス・ドライバーとの相互依存関係。**

  サーバーでアダプターと I/O のファームウェア更新を適用する前に、デバイス・ドライバーを最小レベルに更新する必要がある場合があります。通常は、ファームウェア更新は特定のレベルのデバイス・ドライバーに依存しません。ファームウェア更新の README ファイルでこれらの相互依存関係について確認し、ファームウェアを更新する前にオペレーティング・システムのデバイス・ドライバーを更新してください。XClarity Administrator では、オペレーティング・システムのデバイス・ドライバーは更新されません。

- **ファームウェアを更新する前に XClarity Administrator をリブートする**

  以前にファームウェアの更新に失敗した場合は、XClarity Administrator を再起動してからファームウェアを更新してください。管理サーバーをリブートすると、ファームウェアの更新に使用されているシステム予約済みアカウントが、管理対象デバイスで同期されるようになります。

- **ファームウェアの更新には中断が伴うため、デバイスでワークロードを休止させる必要があります。**

  更新をすぐにアクティブ化することを選択した場合、管理対象デバイスのファームウェア更新には中断が伴います。即時アクティベーションを使用してファームウェアを更新する前に、デバイスを休止する必要があります。

  サーバーでファームウェアを更新すると、アダプター、ディスク・ドライブ、およびソリッド・ステート・ドライブのデバイス・ドライバーを更新するために、サーバーがシャットダウンされてメンテナンス・オペレーティング・システムに置かれます。

  ファームウェアの更新プロセスでは、特定のシャーシ内の Flex スイッチが順番に更新されて再起動されます。冗長データ・パスを実装すると中断を軽減できますが、それでも、ファームウェアの更新中にネットワーク接続の短い中断が発生する可能性があります。

- **XClarity Administrator が実行されているサーバーのファームウェアの更新に XClarity Administrator を使用しない。**

  XClarity Administrator が、管理側のサーバーで実行されているハイパーバイザー・ホストで実行されている場合、XClarity Administrator を使用してそのサーバーでファームウェアを更新しないでください。ファームウェア更新が即時アクティベーションで適用されると、ターゲット・サーバーが XClarity Administrator によって強制的に再起動されます。これにより、ハイパーバイザー・ホストと XClarity

Administrator も再起動されます。据え置きアクティベーションによって適用された場合は、ターゲット・システムが再起動されるまで、一部のファームウェアのみが適用されます。

CMM の考慮事項

- **ファームウェアを更新する前に CMM の仮想再取り付けを実行します。**

  3 週間以上稼働しているデュアル CMM 構成の CMM で、ファームウェア・レベルのスタック・リリースが 1.3.2.1 の 2PET12K から 2PET12Q までを実行している CMM を更新する場合は、ファームウェアを更新する前にプライマリー CMM とスタンバイ CMM の両方を仮想的に再取り付けする必要があります (CMM の仮想再取り付け を参照)。

ベースボード管理コントローラーに関する考慮事項

- **アクティベーション保留中ステータスで必要な最小 BMC レベル**

  アクティベーション保留中ステータスを確認するには、以下のファームウェア・バージョンが、サーバー内のプライマリー・ベースボード管理コントローラーにインストールされている必要があります。
  - IMM2: TCOO46F、TCOO46E またはそれ以降 (プラットフォームによって異なります)
  - XCC: CDI328M、PSI316N、TEI334I またはそれ以降 (プラットフォームによって異なります)

- **更新はプライマリー管理コントローラーおよび UEFI ファームウェア・パーティションに適用される。**

  ベースボード管理コントローラー (BMC) と UEFI の更新は、管理コントローラーと UEFI のプライマリー・ファームウェア・パーティションとバックアップ・ファームウェア・パーティションに個別に適用できます。

  管理コントローラーと UEFI の更新を、サーバーのプライマリー・ファームウェア・パーティションにのみ適用することもできます。デフォルトでは、管理コントローラーは、プライマリー管理コントローラーが満足できる状態で実行されていて新しいレベルがバックアップにプロモートできるようになった後、バックアップ管理コントローラー・パーティションをプライマリー管理コントローラー・パーティションと同期するように構成されています。ただし、管理コントローラーは UEFI バックアップ・パーティションをデフォルトで同期するようには構成されていません。そのため、管理コントローラーでは次のいずれかの選択肢を検討する必要があります。

  - UEFI バックアップ・パーティションの自動同期を有効にする。

    これにより、プライマリーとバックアップの両方のパーティションで同じレベルのファームウェアが実行されるようになります (バックアップ UEFI ファームウェアと管理コントローラー・ファームウェアの互換性も確保されます)。
  - 管理コントローラー・バックアップ・パーティションの自動同期を無効にする。

    推奨されませんが、これにより、管理コントローラーと UEFI のファームウェア・レベルを完全に制御できるようになります。ただし、両方のパーティションの管理コントローラー・ファームウェアと UEFI ファームウェアを手動で更新する必要があります。

  各デバイスに適用された更新を調べるには、ファームウェア・コンプライアンス・ポリシーを使用します。ファームウェア・コンプライアンス・ポリシーについて詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。

  注：管理コントローラーと UEFI が、プライマリーからバックアップ・ファームウェアを自動的に同期するように構成されている場合、XClarity Administrator がバックアップ・バンクを更新する必要はありません。その場合は、サーバーに更新を適用するときにバックアップ・バンクの更新を消去できます。または、ファームウェア・コンプライアンス・ポリシーからバックアップ・バンクを削除できます。

- **管理コントローラーがリセットされると VMware vSphere ESXi でシステム障害が発生する (ホストで紫色の診断画面が表示される) 可能性がある。**

  サーバーで VMware vSphere ESXi を実行している場合は、そのサーバーのファームウェアを更新する前に、インストールされている VMware ESXi のレベルが以下の最小要件を満たしていることを確認してください。

  - VMware vSphere ESXi 5.0 を実行している場合の最小レベルは 5.0u2 (update 2) です。

– VMware vSphere ESXi 5.1 を実行している場合の最小レベルは 5.1u1 (update 1) です。

これらの最小レベルが満たされていないと、管理コントローラーがリセットされるたびに (管理コントローラー・ファームウェアが適用されてアクティブ化された場合を含む) VMware vSphere ESXi でシステム障害が発生する (ホストで紫色の診断画面が表示される) 可能性があります。

注：この問題は、ESXi v5.5 には影響しません。

ThinkSystem デバイスに関する考慮事項

- **20A より前の XCC ファームウェア・バージョンを実行している ThinkSystem SE350 サーバーの場合、管理コントローラーが XClarity Administrator と通信できるように、ベースボード管理コントローラーで IPMI over KCS アクセスを手動で有効にする必要があります。**

  ThinkSystem SE350 サーバーでは、IPMI over KCS はデフォルトで無効になっています。XCC ファームウェア・バージョン 20A 以降を実行している ThinkSystem SE350 サーバーの場合、XClarity Administrator はファームウェアの更新中に IPMI over KCS を自動的に有効にし、ファームウェアの更新が完了した後で無効にします。ただし、20A より前の XCC ファームウェア・バージョンを実行する ThinkSystem SE350 サーバーでは、Lenovo XClarity Controller ユーザー・インターフェースから、「**BMC 構成**」 → 「**セキュリティー**」 → 「**IPMI over KCS アクセス**」をクリックして、このオプションを手動で有効にする必要があります。

- ThinkSystem SR635 および SR655 サーバーの場合は、以下の制限が適用されます。
  – 即時アクティベーションのみサポートされます。遅延アクティベーションと優先度付きアクティベーションはサポートされていません。
  – XClarity Administratorv3.1.1 以降では、バンドルされた更新機能を使用して、ベースボード管理コントローラー、UEFI、ディスク・ドライブ、IO オプションを含む ThinkSystem SR635 および SR655 サーバー上のすべてのコンポーネントを更新できます。

    注意：選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 → 「**ジョブ**」をクリックします。

    注：

    – バンドルされたファームウェアの更新の適用は、ThinkSystem SR635 および SR655 サーバーでのみサポートされています。
    – バンドルされたファームウェア更新の適用は、IPv4 アドレスでのみサポートされています。IPv6 アドレスはサポートされていません。
    – インベントリー情報全体を取得するために、各ターゲット・デバイスが少なくとも 1 回 OS にブートされたことを確認してください。
    – バンドル更新機能を使用するには、ベースボード管理コントローラー・ファームウェア v2.94 以降が必要です。
    – リポジトリー・パックからのファームウェア更新または個々のファームウェア更新のみが使用されます。UpdateXpress System Packs (UXSPs) はサポートされていません。
    – ダウンロードしたファームウェア更新のみが適用されます。製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロード)。

      注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。
    – コンプライアンス確認は、ThinkSystem SR635 および SR655 サーバーのベースボード管理コントローラーと UEFI でのみサポートされます。ただし、XClarity Administrator は、利用可能なすべてのハードウェア・コンポーネントにファームウェア更新を適用しようとします。

  - 更新は、割り当てられたファームウェア・コンプライアンス・ポリシーに従って適用されます。コンポーネントのサブセットを更新することはできません。
  - Lenovo XClarity Provisioning Manager (LXPM)、LXPM のウィンドウ・ドライバー、または LXPM Linux ドライバーのファームウェア更新を ThinkSystem SR635 および SR655 サーバーに適用するには、XClarity Administrator v3.2 以降が必要です。
  - 現在インストールされているバージョンが、割り当てられたコンプライアンス・ポリシーよりも新しい場合、ベースボード管理コントローラーと UEFI の更新はスキップされます。
  - ファームウェア・コンプライアンス・ポリシーが作成済みであり、ファームウェア更新を適用するデバイスに割り当て済みである必要があります。詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。
  - 選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。

  ファームウェア更新をベースボード管理コントローラーと UEFI のみに適用するには、従来の更新機能も使用できます。
- XClarity Administratorv3.0 の場合:
  - 20A から 20B または 20C にファームウェアを更新する場合、管理データは正常に更新されません。この問題を回避するには、管理解除とデバイスを再管理するか、XClarity Administrator を再起動します。
  - ファームウェア更新のダウングレードはサポートされていません。

- **ThinkSystem サーバーでは、DHCPv6 または静的に割り当てられた IPv6 アドレスを使用しているファームウェア更新はサポートされていません。**

  ThinkSystem サーバーで IPv6 アドレスを使用する場合、ファームウェア更新は、IPv6 Link-Local Address(LLA) およびステートレス・アドレスのみでサポートされます。
- **ファームウェアをバージョン 20D に更新するときは、UEFI と XCC の両方を同時に更新する必要があります。**

  バージョン 20D では、UEFI および Lenovo XClarity Controller (XCC) を一緒に更新する必要があります。XCC を更新して UEFI は更新しない、および UEFI を更新して XCC は更新しない場合は、問題が発生する場合があります。

Flex System デバイスに関する考慮事項

- **更新する Flex スイッチの電源がオンであることを確認します。**
- **Flex System 1.3.2 より下位の管理コントローラー・ファームウェア・レベルにある計算ノードを更新する場合は、即時アクティベーションを選択する。**

  Flex System 1.3.2, 2nd Quarter lifecycle release を計算ノードに適用するとき、*即時アクティベーション*を選択して計算ノードを更新する必要があります。即時アクティベーションでは、更新プロセス中に計算ノードの再起動が強制されます。
- **Flex スイッチが XClarity Administrator から到達可能な IP アドレスで構成されている必要がある。**

  XClarity Administrator がファームウェア更新をダウンロードして適用できるように、XClarity Administrator と通信できる IP アドレスがターゲット Flex スイッチに割り当てられている必要があります。
- **x480 X6 や x880 X6 ノードなどのスケーラブル・マルチノード・システムの更新のサポート。**

  Flex System x480 X6 計算ノードや x880 X6 計算ノードなどのスケーラブル・ノードの更新のサポートは、マルチノード複合システムの一部であるすべての計算ノードを含む*単一パーティション*の構成に制限されます。複数のパーティションで構成される複合システムを XClarity Administrator で更新することはできません。

  スケーラブル・マルチノード・システム (Flex System x480 X6 や x880 X6 計算ノードなど) に複数のサーバーを含むパーティションにファームウェア・コンプライアンス・ポリシーを割り当てる場合、XClarity Administrator はデフォルトでパーティション内の各サーバーのすべての管理コントロー

ラーおよび UEFI ファームウェアを更新します。ただし、パーティション内のコンポーネントのサブセットを選択した場合、XClarity Administrator はパーティション内の選択したコンポーネントのみのファームウェアを更新します。

- **CMM2 を v1.30 (1AON06C) 以降に更新する前に、Flex スイッチが Enhanced Configuration and Management (EHCM L3) レベル 3 バージョンを実行している必要があります**

  CMM2 および Flex スイッチは EHCM プロトコルを使用して通信します。このプロトコルは、XClarity Administrator が Flex スイッチを更新するために必要です。CMM2 を v1.30 (1AON06C) 以降に更新するときに、XClarity Administrator は Flex スイッチで EHCM L3 が実行されていることを確認します。実行されていない場合は、Flex スイッチを先に EHCM-L3 をサポートするバージョンに更新する必要があることを示す警告が表示され、CMM 更新がキャンセルされます。CMM ファームウェアの更新時に、「**既に適合しているコンポーネントの更新を試行します**」を選択してこの検査をオーバーライドできます。

  注意：現在、EHCM L3 をサポートする Flex System EN6131 イーサネット・スイッチおよび IB6131 InfiniBand スイッチのファームウェア・バージョンはありません。つまり、CMM2 をファームウェア v1.30 (1AON06C) 更新すると、これらのスイッチの更新に XClarity Administrator を使用できなくなります。回避策は、シャーシの管理コントローラー Web インターフェースまたはコマンド・ライン・インターフェースを使用してスイッチを更新することです。

Flex System スイッチ	バージョン	リリース日付
CN4093	7.8.4.0	2014 年 6 月
EN4023	6.0.0	2015 年 4 月
EN4093	7.8.4.0	2014 年 6 月
EN4093R	7.8.4.0	2014 年 6 月
EN6132	使用不可	使用不可
FC3171	9.1.3.02.00	2014 年 6 月
FC5022	7.4.0b1	2016 年 3 月
IB6132	使用不可	使用不可
SI4091	7.8.4.0	2014 年 6 月
SI4093	7.8.4.0	2014 年 6 月

注：EN2092 1-Gb イーサネット・スケーラブル・スイッチには EHCM L3 が必要なため、この制限はありません。

ストレージに関する考慮事項

- **ThinkSystem DM ストレージ・デバイスに関する考慮事項**

  ThinkSystem DM ストレージ・デバイスのファームウェアを更新するには、デバイスで v9.7 以降を実行している必要があります。

  ダウングレードはマイナー・バージョンでのみサポートされます。たとえば、9.7P11 を 9.7P9 にダウングレードできます。ただし、9.8 を 9.7 にダウングレードすることはできません。

  ThinkSystem DM シリーズのストレージ・デバイスのファームウェアをダウンロードするには:

  – 1 つ以上の ThinkSystem DM シリーズのストレージ・デバイスを XClarity Administrator で管理する必要があります。

  – 各 ThinkSystem DM シリーズのストレージ・デバイスは、ハードウェアのサービスとサポートの対象である必要があります。

  – 「ファームウェアの更新: リポジトリー」ページで ThinkSystem DM シリーズのストレージ・デバイスが配置されている国を指定する必要があります。アルメニア、ベラルーシ、中国、キュー

バ、イラン、カザフスタン、キルギスタン、北朝鮮、ロシア、スーダン、シリアの国のデバイスの暗号化されたファームウェアのみダウンロードできます。

- **ディスク・ドライブは、JBOD、オンライン、動作可能、または未構成 (良好) な状態である必要があります。**

  ディスク・ドライブのファームウェアを更新するには、RAID の状態が JBOD、オンライン、動作可能、または未構成 (良好) である必要があります。その他の状態はサポートされていません。ディスク・ドライブの RAID 状態を判別するには、デバイスの「インベントリー」ページに移動し、「**ドライブ**」セクションを展開し、そのドライブの「**RAID 状態**」を確認します (XClarity Administrator オンライン・ドキュメントの管理対象サーバーの詳細の表示)。

- **ディスク・ドライブとソリッド・ステート・ドライブのファームウェア・バージョンは検出されません。**

  XClarity Administrator では、インストール済みのファームウェア・バージョンが検出され、MegaRAID または NVME アダプターに接続されているディスク・ドライブおよびソリッド・ステート・ドライブ (SSD) のコンプライアンス・チェックのみが実行されます。その他の接続ドライブでは、ファームウェアがサポートされていないレベルであるか、ファームウェア・バージョンの報告がサポートされていない可能性があります。ただし、これらのドライブが選択された場合、ファームウェア更新は適用されます。

- **NVMe ファームウェアは、ターゲット・コンポーネントで識別されていなくても適用されます。**

  「適用/アクティブ化」ページに、ソリッド・ステート・ドライブ (SSD) の NVMe ファームウェア・バージョンがリストされます。検出された NVMe デバイスのターゲット・ファームウェア更新が識別されていないため、ターゲット・システムを更新しようとすると警告メッセージが表示されます。ただし、HDD/SSD の更新は、ターゲット・コンポーネントで識別されなくても適用されるため、この場合も NVMe ファームウェアは更新されます。

- **ServeRAID M5115 PSoC3 更新パッケージを XClarity Administrator から適用するには、レベル 68 以上がインストールされている必要があります。**

  バージョン 68 より下位のバージョンからの ServeRAID M5115 PSoC3 (Programmable System-on-Chip) の更新は、制御された方法で行う必要があります。

  ヒント: ServeRAID M5115 PSoC3 のコード・バージョンを表示するには、CMM Web インターフェースにログインし、ターゲット計算ノードの「**ファームウェア**」タブを選択します。その後、ServeRAID M5115 アダプターの拡張カードを選択します。PSoc3 コードのバージョンは汎用ファームウェア・タイプです。

  68 より下位のインストール済みバージョンについては、XClarity Administrator を使用して更新することはできません。その代わりに、Chassis Management Module (CMM) Web インターフェースまたはコマンド・ライン・インターフェース (CLI) のいずれかから、以下の手順を実行する必要があります。

  - **CMM Web インターフェースを使用して、以下の手順を実行します。**
    1. Chassis Management Module (CMM) の Web インターフェースにログインします。
    2. メイン・メニューから「**サービスおよびサポート**」 ➡ 「**詳細**」をクリックします。
    3. 「**サービスのリセット**」タブを選択します。
    4. 適切な計算ノードを、ラジオ・ボタンをクリックして選択します。
    5. 「**リセット**」プルダウン・ボタンから、「**仮想再取り付け**」をクリックします。
    6. 「OK」をクリックして確認します。
  - **CMM CLI を使用する**:
    - CMM の Secure Shell (SSH) インターフェースにログインします。
    - 仮想再取り付けを実行するには、次のコマンドを入力します。
      `'service -vr -T blade[x]`

      x は、仮想再取り付けを行う計算ノードのベイ番号です。

システムが再び起動したら、オペレーティング・システムにブートし、展開された組み込み更新パッケージを使用して、ServeRAID M5115 PSoC3 を更新します。次の手順を実行して、組み込みパッケージを展開してください。

– **Microsoft Windows を使用する場合**:

  更新パッケージ (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) を開き、「ハードディスク・ドライブへの抽出」を選択します。次に、組み込みパッケージの抽出先となるパスを選択します。

– **Linux を使用する場合**:

  以下のコマンドを実行します。

  ```
  lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x
  ```

  ここで、*x* は組み込みパッケージの抽出場所です。

ファームウェア更新リポジトリーの管理

*ファームウェア更新リポジトリー*には、管理対象デバイスに適用できる使用可能な更新および更新パッケージのカタログが含まれます。

このタスクについて

*カタログ*には、 XClarity Administrator でサポートされているすべてのデバイスに対して、現在使用できるファームウェア更新に関する情報が含まれます。このカタログでは、ファームウェア更新がデバイス・タイプごとに分類されています。カタログを最新の情報に更新すると、XClarity Administrator は Lenovo の Web サイト (メタデータ .xml または .json および readme .txt ファイルを含む) から利用可能な最新のファームウェア更新に関する情報を取得し、その情報をファームウェア更新リポジトリーに保存します。ペイロード・ファイル (.exe) がダウンロードされていません。カタログの更新について詳しくは、製品カタログの更新を参照してください。

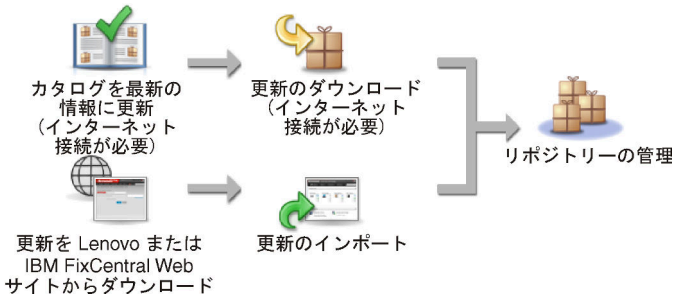
新しいファームウェア更新が使用可能になったとき、管理対象デバイスでそのファームウェアを更新するには、最初に更新パッケージをダウンロードする必要があります。カタログを更新しても、更新パッケージが自動的にダウンロードされるわけではありません。ファームウェア更新リポジトリーページにある**製品カタログ**表では、どの更新パッケージがダウンロード済みで、どれがダウンロード可能かを識別できます。

ファームウェア更新をダウンロードするには、いくつかの方法があります。

- **ファームウェア更新リポジトリー・パック**。すべてのサポート済みデバイスで利用可能な最新のファームウェア更新と更新済みのデフォルトのファームウェア・コンプライアンス・ポリシーを含むリポジトリー・パック。これらのリポジトリー・パックは、インポートされた後管理サーバーの更新ページで適用されます。
- **UpdateXpress System Packs (UXSPs)**。UXSP には、オペレーティング・システムごとに分類された利用可能な最新のファームウェアおよびデバイス・ドライバーの更新が含まれています。「ファームウェア更新: リポジトリー」ページから UXSP をダウンロードした場合、ファームウェア更新のみがダウンロードされ、リポジトリーに保存されます。デバイス・ドライバーの更新は除外されます。

  注：XCC2 を持つサーバーの場合、これらのパックはファームウェア・*バンドル*と呼ばれます。
- **個別のファームウェア更新**。カタログに記載されたバージョンに基づいて、個別のファームウェア更新パッケージを一度に 1 つずつダウンロードできます。

カタログを更新してファームウェア更新をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていない場合、Web ブラウザーを使用して XClarity Administrator ホストへのネットワーク・アクセスを持つワークステーションにファイルを手動でダウンロードし、ファームウェア更新リポジトリにファイルをインポートします。



XClarity Administrator に手動でファームウェア更新をインポートする際は、ペイロード (イメージと MIB)、メタデータ、変更履歴、README の各ファイルを含める必要があります。例:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

注意：

- これらの必要なファイルのみをインポートします。ファームウェアのダウンロード Web サイトに記載されている他のファイルはインポートしないでください。
- 更新パッケージに XML ファイルが含まれていない場合、更新はインポートされません。
- 更新に関連する必要なすべてのファイルを含めなかった場合、リポジトリーで更新が未ダウンロードと表示されます。これは、一部インポート済みであることを意味します。その後、不足しているファイルを選択してインポートできます。
- コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。管理対象サーバーにどのファームウェア更新パッケージを使用するかについて詳しくは、ファームウェア更新のダウンロードを参照してください。

ファームウェア更新をリポジトリーにダウンロードすると、リリース日、サイズ、ポリシーの使用状況、および重大度を含む各更新についての情報が表示されます。重大度は、更新適用の影響と必要性を示すので、運用環境への影響を評価するのに役立ちます。

- 「**初回リリース**」。これは、ファームウェアの初回リリースです。
- 「**重大**」。このファームウェア・リリースにはデータ破損、セキュリティー、または安定性の問題の緊急な修正が含まれています。
- 「**推奨**」。このファームウェア・リリースは、発生する可能性がある問題に対する重要な修正が含まれています。
- 「**非クリティカル**」。このファームウェア・リリースには、マイナーな修正、パフォーマンス強化、およびテキストの変更が含まれています。

注：

- 重大度は、以前にリリースされた更新のバージョンに関連しています。例えば、インストール済みのファームウェアが v1.01 で、更新 v1.02 が「クリティカル」であり、更新 v1.03 が「推奨」である場合、更新は累積的である (v1.03 は v1.02 のクリティカルな問題を含む) ので、1.02 から 1.03 の更新は推奨されるのに対し、v1.01 から v1.03 への更新はクリティカルであることを意味します。
- 特定のマシン・タイプあるいはオペレーティング・システムに対してだけ更新がクリティカル/推奨されている特別な場合もあります。追加情報については、リリース情報を参照してください。

手順

使用可能なファームウェア更新を製品カタログに表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**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」ページに、使用可能なファームウェア更新パッケージのリストが、デバイス・タイプごとに整理されて表示されます。

ステップ 2. 「**個別更新**」タブをクリックして使用可能なファームウェア更新パッケージに関する情報を表示するか、「**UpdateXpress System Packs (UXSPs)**」タブをクリックして使用可能な UXSP に関する情報を表示します。

ステップ 3. デバイスとデバイス・コンポーネントを展開し、そのデバイスの更新パッケージとファームウェア更新の一覧を表示します。

テーブル列をソートし、「**すべて展開表示**」アイコン ( ) と「**すべて縮小表示**」アイコン ( ) をクリックして、特定のファームウェア更新を見つけやすくします。さらに、「**表示**」メニューでオプションを選択して、特定の時間を経過したファームウェア更新、すべてのサーバー・タイプまたは管理対象サーバー・タイプのみのファームウェア更新を表示したり、「**フィルター**」フィールドにテキストを入力して、表示されたデバイスおよびファームウェア更新のリストをフィルタリングすることもできます。特定のデバイスを検索する場合は、デバイスのみがリストされ、デバイス名の下にファームウェア更新はリストされないことに注意してください。

注：サーバーの場合、サーバーのタイプに応じて特定の更新パッケージが使用可能です。たとえば、サーバーを展開した場合 (Flex System x240 計算ノード など)、その計算ノードに使用可能な更新パッケージが明確に表示されます。

結果

このページでは、以下の操作を実行できます。

- このページをカタログ内の現在のファームウェア更新情報で更新するには、「**最新表示**」アイコン ( ) をクリックします。
- 使用可能な更新に関する最新情報を取得するには、「**カタログを最新の情報に更新**」をクリックします。この情報の取得には数分かかることがあります。詳しくは、製品カタログの更新を参照してください。
- ファームウェア更新をリポジトリーに追加するには、製品カタログで 1 つ以上の更新パッケージまたは更新を選択し、「**ダウンロード**」アイコン ( ) をクリックします。ファームウェア更新がダウンロードされてリポジトリーに追加されると、ステータスが「ダウンロード済み」に変わります。

  注：XClarity Administrator ユーザー・インターフェースを使用して更新を取得するには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていなくても、既にダウンロードされている更新をインポートすることができます。

  更新のダウンロードについて詳しくは、ファームウェア更新のダウンロードを参照してください。

- XClarity Administrator にネットワーク・アクセスできるワークステーションに手動でダウンロードしたファームウェア更新をインポートするには、1 つ以上の更新を選択し、「**インポート**」アイコン () をクリックします。更新のインポートについて詳しくは、ファームウェア更新のダウンロードを参照してください。
- 現在進行中のファームウェアのダウンロードを停止するには、1 つ以上の更新を選択し、「**ダウンロードのキャンセル**」アイコン () をクリックします。ダウンロードをキャンセルすると、進行中の すべてのファームウェア・ダウンロードがキャンセルされます。ジョブ・ログから特定のファームウェア・ダウンロードの詳細な進行状況を監視したり、停止したりすることができます (ジョブの監視を参照)。
- リポジトリ—から更新パッケージまたは個々の更新を削除します (ファームウェア更新の削除参照)。
- ファームウェア更新リポジトリーにあるファームウェア更新をローカル・システムにエクスポートできます (ファームウェア更新のエクスポートとインポートを参照)。

ファームウェア更新のリモート・リポジトリーの使用

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。

始める前に

ファームウェア更新のみをリモート共有に保存できます。Windows のデバイス・ドライバーや XClarity Administrator の更新は、ローカルの更新リポジトリーにのみ保存できます。

リモート共有サーバーでポート 22 の SFTP サービスが開いていることを確認します。ベースボード管理コントローラーは、このポートにアクセスできる必要があります。

リモート共有は、ファームウェア・リポジトリーとして使用する場合、SFTP サーバーとして使用されます。SSHD 構成の更新時に SFTP を無効にしていないことを確認します。

このタスクについて

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*。

XClarity Administrator にリモート・リポジトリーの読み取り/書き込み権限がある場合の動作は、ローカル・リポジトリーを使用する場合と同じです。ただし、XClarity Administrator に読み取り専用権限がある場合は、カタログを最新の情報に更新したり、更新をリポジトリーにダウンロード/インポートしたりすることはできません。

複数の XClarity Administrator インスタンスで同じリモート・リポジトリーを共有できます。ただし、1 つの XClarity Administrator インスタンスがリポジトリーを変更しても、他の XClarity Administrator インスタンスには自動的に通知されません。リポジトリーを最新の情報に更新して、最新の詳細を取得する必要があります。リポジトリーを最新の情報に更新するには、「ファームウェア更新: リポジトリー」ページで「**すべての操作**」 ➞ 「**リポジトリーを最新の情報に更新**」をクリックします。

注：ファームウェア更新リポジトリーが複数の XClarity Administrator インスタンスで使用されているリモート共有にある場合、ファームウェア更新と UXSP の削除には注意が必要です。

手順

リモートのファームウェア更新リポジトリーを使用するには、以下の手順を実行します。

ステップ 1. XClarity Administrator にリモート共有を追加します (リモート共有の管理 を参照)。

ステップ 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。

ステップ 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。

ステップ 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。

ステップ 5. 必要に応じて、「**現在のリポジトリーのクリーンアップ**」を選択して、ファームウェア更新ファイルを現在のリポジトリーの場所から削除します。

ステップ 6. 必要に応じて、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。

デフォルトでは、新しい場所にあるファームウェア更新ファイルはコピーされません (スキップされます)。必要に応じて、「**上書きルール**」ドロップダウン・リストで、すべての既存のファイルを上書きするか、サイズや変更日が異なる既存のファイルのみを上書きするかを選択できます。

ステップ 7. 「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 のメニュー・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。

製品カタログの更新

製品カタログには、Lenovo XClarity Administrator でサポートされているすべてのデバイス (シャーシ、サーバー、Flex スイッチ など) に対して、使用できるすべてのファームウェア更新に関する情報が含まれます。

始める前に

製品カタログを更新するには、インターネット接続が必要です。

カタログを最新の情報に更新するには数分かかることがあります。

このタスクについて

カタログを最新の情報に更新すると、Lenovo XClarity サポート Web サイトから提供中の最新のファームウェア更新に関する情報が XClarity Administrator により取得され、情報がファームウェア更新リポジトリーに保存されます。

カタログを更新すると、使用可能なファームウェア更新に関する情報だけがリポジトリーに追加されます。更新パッケージはダウンロードされません。更新をインストールできるようにするには、ファームウェア更新をダウンロードする必要があります。更新のダウンロードについて詳しくは、ファームウェア更新のダウンロードを参照してください。

手順

製品カタログを最新表示にするには、以下の手順を実行します。

ステップ 1. 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。

ステップ 2. 「**個別更新**」タブをクリックし、個別のファームウェア更新パッケージに関する情報を取得するか、「**UpdateXpress System Pack (UXSP)**」タブをクリックして UXSP に関する情報を取得します。

ステップ 3. 「**カタログを最新の情報に更新**」をクリックし、次のいずれかのオプションをクリックして、使用可能な最新のファームウェア更新に関する情報を取得します。

- 「**選択した情報の更新 - 最新のみ**」。選択したデバイスでのみ使用可能なファームウェア更新の最新のバージョンの情報を取得します。
- 「**すべて更新 - 最新のみ**」。サポートされているすべてのデバイスのすべてのファームウェア更新の最新バージョンの情報を取得します。
- 「**選択した情報の更新**」。選択したデバイスでのみ使用可能なファームウェア更新のすべてのバージョンの情報を取得します。
- 「**すべて更新**」。サポートされているすべてのデバイスのすべてのファームウェア更新のすべてのバージョンの情報を取得します。

ヒント:**「すべての操作」 ➡ 「更新」の順にクリックして、すべての管理対象デバイスをダウンロードするか、または「すべての操作」 ➡ 「更新」の順にクリックして、選択したデバイスの最新版をダウンロードします。**

ファームウェア更新のダウンロード

インターネットへのアクセス状況に応じて、ファームウェア更新をファームウェア更新リポジトリーにダウンロードするかインポートできます。管理対象デバイスでファームウェア更新を実行する前に、更新パッケージをファームウェア更新リポジトリーで使用できるようにする必要があります。

始める前に

ファームウェアをダウンロードする前に、Lenovo XClarity Administrator 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。

デバイス・タイプがファームウェア更新リポジトリーにリストされていない場合は、最初にそのタイプのデバイスを管理対象にしてから、そのデバイス・タイプの個々のファームウェア更新をダウンロードまたはインポートする必要があります。

重要：

- XClarity Administrator v1.1.1 以前では、Lenovo データセンターサポート Web サイトから Lenovo ハードウェア用のファームウェア更新を手動でダウンロードしてインストールする必要があります。
- XClarity Administrator では、RackSwitch スイッチおよび Lenovo DE、DX、および SS シリーズのストレージ・デバイスの更新を Lenovo Web サイトからファームウェア更新リポジトリーにダウンロードできません。これらの更新を Lenovo Web サイトから XClarity Administrator ホストにネットワークで接続しているワークステーションに手動でダウンロードしてインポートするか、すべての利用可能なファームウェア更新が含まれている *ファームウェア更新リポジトリー・パック*をダウンロードして適用する必要があります。
- 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、。
- ThinkSystem DM シリーズのストレージ・デバイスのファームウェアをダウンロードするには:
  - 1 つ以上の ThinkSystem DM シリーズのストレージ・デバイスを XClarity Administrator で管理する必要があります。
  - 各 ThinkSystem DM シリーズのストレージ・デバイスは、ハードウェアのサービスとサポートの対象である必要があります。

– 「ファームウェアの更新: リポジトリー」ページで ThinkSystem DM シリーズのストレージ・デバイスが配置されている国を指定する必要があります。アルメニア、ベラルーシ、中国、キューバ、イラン、カザフスタン、キルギスタン、北朝鮮、ロシア、スーダン、シリアの国のデバイスの暗号化されたファームウェアのみダウンロードできます。

このタスクについて

ファームウェア更新をダウンロードするには、いくつかの方法があります。

- **ファームウェア更新リポジトリー・パック**

  ファームウェア更新リポジトリー・パックとは、最もサポートされているすべてのデバイスに対する XClarity Administrator のリリースと同時に使用できる、最新のファームウェアのコレクションであり、更新済みのデフォルトのファームウェア・コンプライアンス・ポリシーです。これらのリポジトリー・パックは、インポートされた後管理サーバーの更新ページで適用されます。ファームウェア更新リポジトリー・パックを適用すると、パック内の各更新パッケージがファームウェア更新リポジトリーに追加され、すべての管理可能デバイスでデフォルトのファームウェア・コンプライアンス・ポリシーが自動的に作成されます。この事前定義済みポリシーはコピーすることはできますが、変更することはできません。

  以下のリポジトリー・パックを使用できます。

  – **lnvgy_sw_lxca_cmmswitchrepo*x-x.x.x*_anyos_noarch**。すべての CMM および Flex System スイッチのファームウェア更新が含まれます。
  – **lnvgy_sw_lxca_storagerackswitchrepo*x-x.x.x*_anyos_noarch**。すべての RackSwitch スイッチと Lenovo Storage デバイスのファームウェア更新が含まれます。
  – **lnvgy_sw_lxca_systemxrepo*x-x.x.x*_anyos_noarch**。すべての Converged HX シリーズ、Flex System、NeXtScale、および System x サーバーのファームウェア更新が含まれます。
  – **lnvgy_sw_thinksystemrepo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem サーバーのファームウェア更新が含まれます。
  – **lnvgy_sw_lxca_thinksystemv2repo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem V2 サーバーのファームウェア更新が含まれます。
  – **lnvgy_sw_lxca_thinksystemv3repo*x-x.x.x*_anyos_noarch**。すべての ThinkAgile および ThinkSystem V3 サーバーのファームウェア更新が含まれます。

  「管理サーバーの更新」ページの「**ダウンロード・ステータス**」列で、ファームウェア更新リポジトリー・パックがリポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

  – **ダウンロード済み**。ファームウェア更新リポジトリー・パックはリポジトリーに保存されています。
  – **未ダウンロード**。ファームウェア更新リポジトリー・パックは使用できますが、リポジトリーに保存されていません。

- **UpdateXpress System Packs (UXSPs)**

  注：XCC2 を持つサーバーの場合、これらのパックはファームウェア・バンドルと呼ばれます。*バンドル*は、パッケージ名および事前定義されたポリシー名で使用されます。

  UXSP には、オペレーティング・システムごとに分類された利用可能な最新のファームウェアおよびデバイス・ドライバーの更新が含まれています。UXSP をダウンロードすると、カタログに示されたバージョンに基づいて UXSP が XClarity Administrator によりダウンロードされ、ファームウェア更新リポジトリーに更新パッケージが保存されます。UXSP をダウンロードすると、UXSP 内の各ファームウェア更新がファームウェア更新リポジトリーに追加され、「**個別更新**」タブにリストされ、以下の名前を使用してすべての管理可能デバイスにデフォルトのファームウェア・コンプライアンス・ポリシーが自動的に作成されます。この事前定義済みポリシーはコピーすることはできますが、変更することはできません。
  – ***{uxsp-version}-{date}-{server-short-name}*-UXSP** (例: `v1.50-2017-11-22- SD530-UXSP`)

– *{uxsp-version}-{buildnumber}-{server-short-name}*-bundle (例、 `22a.0-kaj92va-SR650V3-bundle`)

注：「ファームウェア更新: リポジトリー」ページから UXSP をダウンロードまたはインポートした場合、ファームウェア更新のみがダウンロードされ、リポジトリーに保存されます。デバイス・ドライバーの更新は破棄されます。UXSP を使用した Windows デバイス・ドライバー更新のダウンロードまたはイン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 OS デバイス・ドライバー・リポジトリーの管理。

「ファームウェア更新: リポジトリー」ページの「**個別更新**」タブにある「**ダウンロード状況**」の列で、UXSP がファームウェア更新リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

– **ダウンロード済み**。更新パッケージ全体または個々のファームウェア更新がリポジトリーに保存されています。
– ***x*/*y* ダウンロード済み**。更新パッケージ内の一部のファームウェア更新がリポジトリーに保存されています。括弧内の番号は、利用可能な更新数と、保存された更新数、または特定のデバイス・タイプの更新がないことを示します。
– **未ダウンロード**。更新パッケージ全体または個々のファームウェア更新を使用できますが、リポジトリーに保存されていません。

- **個別のファームウェア更新**

  ファームウェア更新パッケージを個別にダウンロードすることもできます。ファームウェア更新パッケージをダウンロードすると、カタログに示されたバージョンに基づいて更新が XClarity Administrator によりダウンロードされ、ファームウェア更新リポジトリーに更新パッケージが保存されます。その後、これらの更新パッケージを使用して、各管理対象デバイスのファームウェア・コンプライアンス・ポリシーを作成できます。

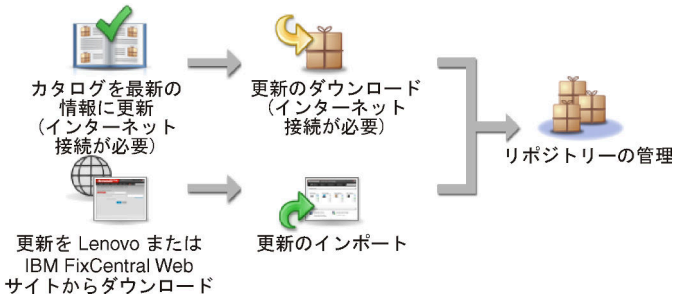
  注：コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。管理対象サーバーにどのファームウェア更新パッケージを使用するかについて詳しくは、ファームウェア更新のダウンロードを参照してください。

  「ファームウェア更新: リポジトリー」ページの「**個別更新**」タブの「**ダウンロード・ステータス**」列で、*ファームウェア更新*がファームウェア更新リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

  – **ダウンロード済み**。更新パッケージ全体または個々のファームウェア更新がリポジトリーに保存されています。
  – ***x*/*y* ダウンロード済み**。更新パッケージ内の一部のファームウェア更新がリポジトリーに保存されています。括弧内の番号は、利用可能な更新数と、保存された更新数、または特定のデバイス・タイプの更新がないことを示します。
  – **未ダウンロード**。更新パッケージ全体または個々のファームウェア更新を使用できますが、リポジトリーに保存されていません。

新しいリリースに XClarity Administrator をインストールまたは更新するときには、最新のリポジトリー・パックをダウンロードして最新のファームウェア更新を使用できるようにすることをお勧めします。次に、定期的なジョブをスケジュールしてカタログを更新し、最後のリポジトリー・パック以降に Web に投稿された個別の更新を検索して、それらの更新を一度に電子的にダウンロードすることができます。

カタログを更新してファームウェア更新をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていない場合、Web ブラウザーを使用して XClarity Administrator ホストへのネットワーク・アクセスを持つワークステーションにファイルを手動でダウンロードし、ファームウェア更新リポジトリにファイルをインポートします。



XClarity Administrator に手動でファームウェア更新をインポートする際は、ペイロード (イメージと MIB)、メタデータ、変更履歴、README の各ファイルを含める必要があります。例:

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

注：コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。

リポジトリーが 50% 以上埋まると、メッセージがページに表示されます。リポジトリーが 85% 以上埋まると、別のメッセージがページに表示されます。リポジトリーで使用されているスペースを減らすには、未使用のイメージ・ファイルとポリシーを削除します。未使用のファームウェア・コンプライアンス・ポリシーと関連するファームウェア・パッケージは、「**プロビジョニング**」 ➞ 「**コンプライアンス・ポリシー**」をクリックし、削除する 1 つ以上のポリシーを選択して、「**操作**」 ➞ 「**ポリシーおよびファームウェア・パッケージの削除**」をクリックすることにより削除できます。

次の表に、ファームウェア更新リポジトリー・パック、UXSPs、および個々のファームウェア更新パッケージの取得の違いを要約します。

更新パッケージ	ファイルをダウンロードおよびインポートするための UI ページ	ファイルを手動でダウンロードするための Web ページ	ファームウェア更新リポジトリーが更新されていますか?	ファームウェア・コンプライアンス・ポリシーは自動的に更新されていますか?
ファームウェア更新リポジトリー・パック	「管理サーバーの更新」ページ **注：**リポジトリー・パックをインポートし、適用します。	XClarity Administrator ダウンロード Web ページ	はい	はい
UpdateXpress System Packs	「ファームウェア更新: リポジトリー」ページ、「**UpdateXpress System Packs (UXSP)**」タブ	Lenovo XClarity Essentials UpdateXpress Web ページ	はい	はい
ファームウェア更新	「ファームウェアの更新: リポジトリー」ページで、「**個別更新**」タブを選択します	Lenovo データセンターサポート Web サイト **注：**以下のデバイスについては、Fix Central Web サイトを使用します。 • Flex System x220 タイプ 2585、7906 • Flex System x222 計算ノード・タイプ 2589、7916	はい	いいえ

更新パッケージ	ファイルをダウンロードおよびインポートするための UI ページ	ファイルを手動でダウンロードするための Web ページ	ファームウェア更新リポジトリーが更新されていますか?	ファームウェア・コンプライアンス・ポリシーは自動的に更新されていますか?
		• Flex System x240 タイプ 7863、8737、8738、8956 • Flex System x280 / x480 / x880 X6 タイプ 4259、7903 • Flex System x440 タイプ 2584、7917		

手順

1 つ以上のファームウェア更新をダウンロードするには、以下の手順を実行します。

- 1 つ以上の *ファームウェア更新リポジトリー・パック*をインポートするには:
  1. XClarity Administrator のメニュー・バーで、「**管理**」 ➡ 「**管理サーバーの更新**」の順にクリックして、「管理サーバーの更新」ページを表示します。
  2. 最新のリポジトリー・パックをダウンロードします。
     - XClarity Administrator がインターネットに接続されている場合:
       a. 「**カタログを最新の情報に更新**」 ➡ 「**管理対象をすべて更新 - 最新のみ**」をクリックして、最新の更新に関する情報を取得します。新しい管理サーバーの更新とファームウェア更新リポジトリー・パックが「管理サーバーの更新」ページの表に表示されます。

          リポジトリーの更新には数分かかることがあります。

          注: リポジトリーを更新しても、ペイロード・ファイルが自動的にダウンロードされるわけではありません。メタデータおよび readme ファイルのみをダウンロードします。
       b. ダウンロードするファームウェア更新リポジトリー・パックを選択します。

          ヒント: 「**タイプ**」列に「補足パック」と表示されているパッケージを選択してください。
       c. 「**選択をダウンロード**」アイコン () をクリックします。ダウンロードが完了すると、そのソフトウェア更新の「**ダウンロード・ステータス**」が「ダウンロード済み」に変わります。
     - XClarity Administrator がインターネットに接続されていない場合:
       a. XClarity Administrator ホストにネットワーク接続できるワークステーションに、XClarity Administrator ダウンロード Web ページからファームウェア更新リポジトリー・パックをダウンロードします。
       b. 「管理サーバーの更新」ページで、「**インポート**」アイコンをクリックします ()。
       c. 「**ファイルの選択**」をクリックし、ワークステーション上のファームウェア更新リポジトリー・パックの場所を参照します。
       d. すべてのパッケージ・ファイルを選択し、「**開く**」をクリックします。

          メタデータ・ファイル (.xml または .json) とイメージまたはペイロード・ファイル (.zip、.bin、.uxz、または .tgz) をインポートし、履歴ファイル (.chg) と readme ファイル (.txt) を変更して更新します。選択されているがメタデータ・ファイルに指定されていないファイルはすべて破棄されます。メタデータ・ファイルを含めなかった場合、更新はインポートされません。
       e. 「**インポート**」をクリックします。

インポートが完了すると、「管理サーバーの更新」ページのテーブルにファームウェア更新リポジトリー・パックが表示され、各更新の「**ダウンロード・ステータス**」が「ダウンロード済み」になります。

3. ファームウェア更新リポジトリーにインストールするファームウェア更新リポジトリー・パックを選択します。

   注：「**ダウンロード・ステータス**」が「ダウンロード済み」であり、「**タイプ**」が「パッチ」であることを確認します。

4. 「**更新の実行**」アイコン () をクリックして、ファームウェア更新パッケージをリポジトリーに追加します。
5. 更新が完了するまで数分間待った後、XClarity Administrator を再起動します。
6. Web ブラウザーを最新表示にして、更新が完了したかどうかを確認します。

   完了した場合は「管理サーバーの更新」ページが表示され、「**適用済みステータス**」列が「適用済み」に変わります。

7. Web ブラウザーのキャッシュをクリアします。

- 1 つ以上の *UXSPs* をダウンロードするには。
  1. 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**」をクリックして、「ファームウェア更新リポジトリー」ページを表示します。
  2. 「**UpdateXpress System Packs (UXSPs)**」 タブをクリックします。
  3. 最新の UXSPs をダウンロードします。
     - XClarity Administrator がインターネットに接続されている場合:

       カタログを更新して、すべての管理対象デバイスの最新の UXSP をダウンロードするには、**「すべての操作」 ➡ 「リフレッシュ」の順にクリックし、すべての管理対象デバイスの最新版をダウンロードします。**

       カタログを更新して、選択したデバイスのみの最新の UXSP をダウンロードする:

       a. 使用可能な UXSPs のリストを表示するには、デバイスを展開します。
       b. ダウンロードする UXSPを 1 つ以上選択します。
       c. **「すべての操作」 ➡ 「リフレッシュ」の順にクリックし、選択したデバイスの最新版をダウンロードします。**

          ダウンロードが完了すると、選択した UXSP の**ダウンロード・ステータス**が「ダウンロード済み」に変わります。

     - XClarity Administrator がインターネットに接続されていない場合:

       a. XClarity Administrator ホストにネットワーク接続できるワークステーションに、Lenovo XClarity Essentials UpdateXpress Web ページから UXSPs をダウンロードします。
       b. XClarity Administrator から、「**インポート**」アイコン () をクリックします。
       c. 「**ファイルの選択**」をクリックし、ワークステーション上の UXSPs の場所を参照します。
       d. すべてのパッケージ・ファイルを選択し、「**開く**」をクリックします。

          メタデータ・ファイル (.xml または .json) とイメージまたはペイロード・ファイル (.zip、.bin、.uxz、または .tgz) をインポートし、履歴ファイル (.chg) と readme ファイル (.txt) を変更して更新します。選択されているがメタデータ・ファイルに指定されていないファイルはすべて破棄されます。メタデータ・ファイルを含めなかった場合、更新はインポートされません。

       e. 「**インポート**」をクリックします。

          インポートが完了すると、「管理サーバーの更新」ページのテーブルにファームウェア更新リポジトリー・パックが表示され、各更新の「ダウンロード・ステータス」が「ダウンロード済み」になります。

- 1 つ以上の個別の *ファームウェア更新パッケージ*をダウンロードするには。
  1. 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**」をクリックして、「ファームウェア更新リポジトリー」ページを表示します。
  2. ThinkSystem DM シリーズのストレージ・デバイスのファームウェアをダウンロードする場合は、ストレージ デバイスが配置されている国を選択します。
  3. 「**個別更新**」タブをクリックします。
  4. 最新の個別のファームウェア更新をダウンロードします。
     - XClarity Administrator がインターネットに接続されている場合:

       カタログを更新して、すべての管理対象デバイスの最新ファームウェアをダウンロードするには、**「すべての操作」 ➡ 「リフレッシュ」 の順にクリックし、すべての管理対象デバイスの最新版をダウンロードします。**

       カタログを更新して、選択したデバイスのみの最新ファームウェアをダウンロードする:
       a. 使用可能なファームウェア更新のリストを表示するには、デバイスを展開します。
       b. ダウンロードするファームウェア更新を 1 つ以上選択します。

          ヒント: 更新パッケージは、複数のファームウェア更新で構成される場合があります。ファームウェア更新をダウンロードするとき、更新パッケージ全体をダウンロードするか特定の更新のみをダウンロードするかを選択できます。複数のパッケージを一度にダウンロードすることを選択することもできます。
       c. **「すべての操作」 ➡ 「リフレッシュ」の順にクリックし、選択したデバイスの最新版をダウンロードします。**

          ダウンロードが完了すると、そのファームウェア更新の**ダウンロード・ステータス**が「ダウンロード済み」に変わります。
     - XClarity Administrator がインターネットに接続されていない場合:
       a. XClarity Administrator ホストにネットワーク接続できるワークステーションに、Lenovo データセンターサポート Web サイト からファームウェア更新パッケージをダウンロードします。

          以下のサーバーについては、SLES 11 オペレーティング・システム用のファームウェア更新を Fix Central Web サイト からダウンロードします。
          - Flex System x220 タイプ 2585、7906
          - Flex System x222 計算ノード・タイプ 2589、7916
          - Flex System x240 タイプ 7863、8737、8738、8956
          - Flex System x280 / x480 / x880 X6 タイプ 4259、7903
          - Flex System x440 タイプ 2584、7917

          他のすべてのサーバーについては、RHEL 6 オペレーティング・システム用のファームウェア更新を Lenovo XClarity サポート Web サイト からダウンロードします。
       b. XClarity Administrator から、「**インポート**」アイコン () をクリックします。
       c. 「**ファイルの選択**」をクリックし、ワークステーション上のファームウェア更新の場所を参照します。
       d. すべてのパッケージ・ファイルを選択し、「**開く**」をクリックします。

          メタデータ・ファイル (.xml または .json) とイメージまたはペイロード・ファイル (.zip、.bin、.uxz、または .tgz) をインポートし、履歴ファイル (.chg) と readme ファイル (.txt) を変更して更新します。選択されているがメタデータ・ファイルに指定されていないファイルはすべて破棄されます。

          注意：

- これらの必要なファイルのみをインポートします。ファームウェアのダウンロード Web サイトに記載されている他のファイルはインポートしないでください。
- 更新パッケージに XML ファイルが含まれていない場合、更新はインポートされません。
- 更新に関連する必要なすべてのファイルを含めなかった場合、リポジトリーで更新が未ダウンロードと表示されます。これは、一部インポート済みであることを意味します。その後、不足しているファイルを選択してインポートできます。
- コア ファームウェア更新 (管理コントローラー、UEFI、pDSA など) は、オペレーティング・システムに依存しません。RHEL 6 または SLES 11 オペレーティング・システム用のファームウェア更新パッケージは、計算ノードとラック・サーバーの更新に使用されます。管理対象サーバーにどのファームウェア更新パッケージを使用するかについて詳しくは、ファームウェア更新のダウンロードを参照してください。

e. 「**インポート**」をクリックします。

カタログの更新やファームウェア更新のダウンロードには、数分かかる場合があります。更新がダウンロードされてリポジトリーに保存されると、製品カタログの行が強調表示され、「**ダウンロード・ステータス**」列が「ダウンロード済み」に変わります。

注：一部のスイッチのマシン・タイプは、16 進数として表示される場合があります。

終了後

「ファームウェア・リポジトリー」ページで、「**すべての操作**」 ➡ 「**共通設定**」をクリックして、更新リポジトリー (ファームウェア、OS デバイス・ドライバー、管理サーバー更新など) の最大サイズを構成できます。最小サイズは 50 GB です。最大サイズは、ローカル・システム上のディスク・スペースの量によって異なります。

ファームウェア更新のエクスポートとインポート

リポジトリー内に存在する個々のファームウェア更新および UpdateXpress System Packs (UXSPs) をローカル・システムにエクスポートできます。

このタスクについて

リポジトリー内に存在するファームウェア更新のみがエクスポートされます。選択したファームウェア更新のダウンロード・ステータスが「ダウンロード済み」であることを確認します。

更新イメージまたはペイロード・ファイル (.zip、.bin、.uxz、または .tgz)、メタデータ・ファイル (.xml または .json)、変更履歴ファイル (.chg)、および readme ファイル (.txt) を含めて、ファームウェア更新に関連付けられているすべてのファイルがエクスポートされます。

注意：ファームウェア更新ファイルの名前を変更しないでください。

手順

- ファームウェア更新をエクスポートするには:
  1. 「**個別更新**」タブまたは「**UpdateXpress System Packs (UXSP)**」タブをクリックします。
  2. ファームウェア更新を 1 つ以上選択します。
  3. 「**エクスポート**」アイコン () をクリックします。
- ファームウェア更新をインポートするには:

  Lenovo XClarity Administrator から手動でエクスポートしたファイル、および Web から手動でダウンロードしたファイルをインポートできます。詳しくは、ファームウェア更新のダウンロードを参照してください。

ファームウェア更新の削除

ファームウェア更新と UpdateXpress System Packs (UXSPs) は、ファームウェア更新リポジトリーから削除できます。

始める前に

削除するファームウェア更新が含まれるファームウェア・コンプライアンス・ポリシーを使用する実行中のジョブとスケジュールされたジョブがすべて完了しているか、キャンセルされていることを確認します (ジョブの監視参照)。

更新を削除する前に、その更新がファームウェア・コンプライアンス・ポリシーで使用されていないことを確認してください。1 つ以上のファームウェア・コンプライアンス・ポリシーで現在使用中のファームウェア更新パッケージを削除することはできません。

UXSP を削除すると、該当する UXSP に対して自動的に作成されたファームウェア・コンプライアンス・ポリシーも削除されます。

注：ファームウェア更新リポジトリーが複数の XClarity Administrator インスタンスで使用されているリモート共有である場合、ファームウェア更新と UXSP の削除には注意が必要です。

手順

リポジトリーから 1 つ以上のファームウェア更新を削除するには、以下の手順を実行してください。

ステップ 1. 削除するファームウェア更新が含まれるすべてのファームウェア・コンプライアンス・ポリシーを、すべての管理対象デバイスから割り当て解除します。

   a. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページが表示されます。

   b. ファームウェア・コンプライアンス・ポリシーを使用する管理対象デバイスの「**割り当て済みポリシー**」列で、「割り当てがありません」を選択するか、別のファームウェア・コンプライアンス・ポリシーを選択します。

ステップ 2. 削除するファームウェア更新が含まれるユーザー定義のファームウェア・コンプライアンス・ポリシーをすべて削除するか、ファームウェア・コンプライアンス・ポリシーを編集して、削除するファームウェア更新を削除します。

a. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**コンプライアンス・ポリシー**」の順にクリックします。「ファームウェア更新コンプライアンス・ポリシー」ページが表示されます。

b. ファームウェア・コンプライアンス・ポリシーを選択し、「**削除**」アイコン ( ) を選択してポリシーを削除するか、「**編集**」アイコン ( ) をクリックしてポリシーからファームウェア更新を削除します。

ステップ 3. ファームウェア更新を削除します。

- **個別のファームウェア更新**
  1. 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。
  2. 「**個別更新**」タブをクリックします。
  3. 削除するファームウェア更新を 1 つ以上選択します。
  4. イメージまたはペイロード・ファイル (.zip、.bin、.uxz、または .tgz) のみを削除するには、「**イメージのみ削除**」アイコン ( ) をクリックします。更新に関する情報は残るので、更新を簡単に再度ダウンロードできます。または、**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、ペイロード・ファイル、変更履歴ファイル (.chg)、readme ファイル (.txt)、メタデータ・ファイル (.xml または .json) を含む、すべての更新パッケージ・ファイルを削除します。

  ファームウェア更新を削除すると、ペイロード・ファイルは削除されます。ただし、更新に関する情報を含むメタデータ・ファイルは残るので、必要に応じて更新を簡単に再度ダウンロードできます。また、「**ダウンロード状況**」が「未ダウンロード」に変化します。
- **UXSPs**
  1. 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。
  2. 「**UpdateXpress System Pack (UXSP)**」 タブをクリックします。
  3. 削除する UXSP を 1 つ以上選択します。
  4. **UXSP および関連ポリシーの削除**アイコン ( ) をクリックして、ペイロード・ファイル、変更履歴ファイル (.chg)、readme ファイル (.txt)、メタデータ・ファイル (.xml または .json)、および関連するファームウェア・コンプライアンス・ポリシーを含む、すべての UXSP ファイルを削除します。

  選択した UXSP が、(デバイスに割り当てられた) 使用中のポリシーに関連付けられている場合は、「UXSP、ポリシー、および更新パッケージの削除」ダイアログが表示されます。UXSP および未使用のポリシーに加えて、割り当て済みポリシーを削除するかどうかを選択し、「**OK**」をクリックします。

ファームウェア・コンプライアンス・ポリシーの作成と割り当て

*ファームウェア・コンプライアンス・ポリシー*を使用すると、注意が必要なデバイスにフラグを付けることで、特定の管理対象デバイス上のファームウェアを現在のレベルまたは指定されたレベルに維持することができます。各ファームウェア・コンプライアンス・ポリシーは、デバイスのコンプライアンスを保つために、監視対象のデバイスと、インストールする必要のあるファームウェア・レベルを指定します。コンプライアンスは、デバイスまたはファームウェア・コンポーネントのレベルで設定できます。その後、XClarity Administrator はこれらのポリシーを使用して、管理対象デバイスのステータスを確認し、コンプライアンスに違反しているデバイスを特定します。

始める前に

ファームウェア・コンプライアンス・ポリシーを作成するときは、ポリシーに割り当てられるデバイスに適用するターゲット更新バージョンを選択します。ポリシーを作成する前に、ターゲット・バージョンのファームウェア更新が更新リポジトリーにあることを確認してください (ファームウェア更新のダウンロードを参照)。

デバイス・タイプがファームウェア更新リポジトリーにリストされていない場合は、最初にそのタイプのデバイスを管理対象にしてから、ファームウェア更新の全セットをダウンロードまたはインポートする必要があります。その後、そのタイプのデバイスに対するコンプライアンス・ポリシーを作成します。

このタスクについて

ファームウェア・コンプライアンス・ポリシーを作成するときは、以下のような場合に XClarity Administrator がデバイスにフラグを立てるように選択できます。

- デバイスのファームウェアが下位レベル
- デバイスのファームウェアがコンプライアンス・ターゲット・バージョンと完全に一致していない

XClarity Administrator には、**リポジトリの最新ファームウェア**と呼ばれる事前定義されたファームウェア・コンプライアンス・ポリシーが用意されています。新しいファームウェアがリポジトリーにダウンロードまたはインポートされると、このポリシーが更新されて、リポジトリー内で使用可能なファームウェアの最新バージョンが含まれるようになります。

ファームウェア・コンプライアンス・ポリシーをデバイスに割り当てた後、XClarity Administrator はデバイス・インベントリーの変更またはファームウェア更新リポジトリーの変更があると、各デバイスのコンプライアンス状況を確認します。デバイスのファームウェアが割り当てられたポリシーに準拠していない場合、XClarity Administrator はファームウェア・コンプライアンス・ポリシーで指定したルールに基づいて、「ファームウェア更新: 適用/アクティブ化」ページでデバイスを非準拠として識別します

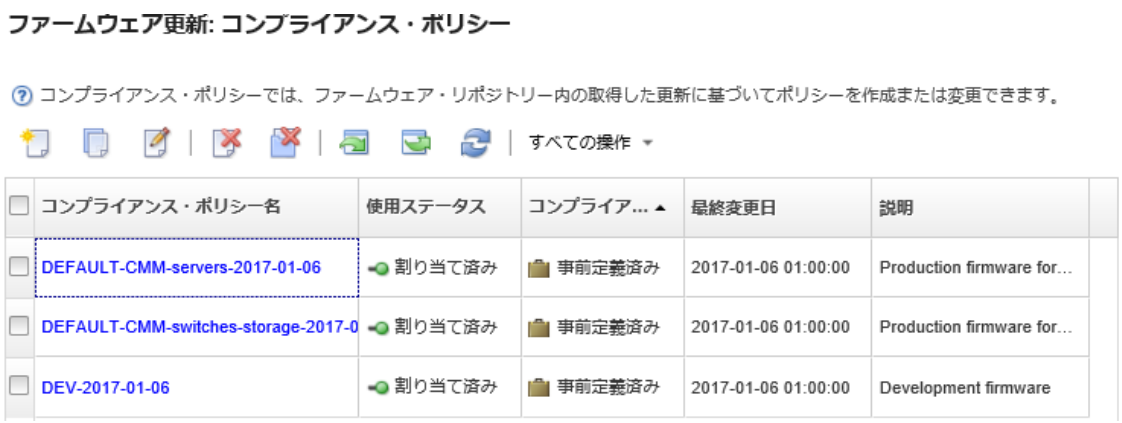
たとえば、すべての ThinkSystem SR850 デバイスにインストールされたファームウェアの基準レベルを定義するファームウェア・コンプライアンス・ポリシーを作成し、そのファームウェア・コンプライアンス・ポリシーをすべての管理対象 ThinkSystem SR850 デバイスに割り当てることができます。ファームウェア更新リポジトリーが最新の情報に更新され、新しいファームウェア更新が追加されると、それらの計算ノードがコンプライアンス違反となる可能性があります。その場合、XClarity Administrator は「ファームウェア更新: 適用/アクティブ化」ページを更新し、そのデバイスが非適合であることを表示して、アラートを生成します。

注：割り当てられたファームウェア・コンプライアンス・ポリシーの要件を満たしていないデバイスのアラートの表示または非表示を選択できます (ファームウェア更新の共通設定の構成を参照)。デフォルトではアラートは非表示です。

手順

ファームウェア・コンプライアンス・ポリシーを作成して割り当てるには、以下の手順を実行します。

ステップ 1. 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: コンプライアンス・ポリシー**」の順にクリックします。「コンプライアンス・ポリシー」ページにすべての既存のファームウェア・コンプライアンス・ポリシーのリストが表示されます。



ステップ 2. ファームウェア・コンプライアンス・ポリシーを作成します。

1. 「**作成**」アイコン ( ) をクリックして、「新しいポリシーの作成」ダイアログを表示します。

2. ファームウェア・コンプライアンス・ポリシーの名前と説明を入力します。
3. 各デバイスについて、以下の基準に基づいてテーブルに入力します。
   - **デバイス・タイプ**。このポリシーが適用されるデバイスまたはコンポーネントのタイプを選択します。

     ヒント: サーバーを選択した場合、コンプライアンス・レベルは UXSP レベルで指定されます。ただし、サーバーを展開して、各コンポーネント (ベースボード管理コントローラーや UEFI など) に特定のファームウェア・レベルを指定することもできます。
   - 「**コンプライアンス・ターゲット**」。該当するデバイスとのサブコンポーネントのコンプライアンス・ターゲットを指定します。

     サーバーの場合、以下の値のいずれかを選択できます。

     – **デフォルト**。各サブコンポーネントのコンプライアンス・ターゲットをデフォルト値に変更します (そのデバイスのリポジトリーにあるファームウェアの最新セットなど)。

– **更新しない**。各サブコンポーネントのコンプライアンス・ターゲットを「更新しない」に変更します。

サブコンポーネントがないデバイス (CMM、スイッチ、ストレージ・デバイスなど) の場合、またはサーバー内のサブコンポーネントの場合、以下のいずれかの値を選択できます。

– *<firmware_level>*。基準のファームウェア・レベルを指定します。
– **更新しない**。ファームウェアを更新しないことを指定します。バックアップ管理コントローラーのファームウェアはデフォルト更新されないことに注意してください。

注：サーバー内の任意のサブコンポーネントのデフォルト値を変更すると、そのサーバーのコンプライアンス・ターゲットが「**カスタム**」に変わります。

- 「**コンプライアンス・ルール**」。「ファームウェア更新: 適用/アクティブ化」の「**インストール済みバージョン**」列でデバイスに不適合のフラグが付けられる条件を指定します。

  – **下位レベルの場合はフラグを設定**。デバイスにインストールされているファームウェア・レベルがファームウェア・コンプライアンス・ポリシーで指定したレベルより下位である場合、デバイスには不適合のフラグが付けられます。たとえば、計算ノードのネットワーク・アダプターを交換した場合で、そのネットワーク・アダプターのファームウェアがファームウェア・コンプライアンス・ポリシーで指定されているレベルより前のレベルである場合、その計算ノードには不適合のフラグが付けられます。
  – **完全一致でなければフラグを設定**。デバイスにインストールされているファームウェア・レベルがファームウェア・コンプライアンス・ポリシーで指定したレベルと完全に一致しない場合、デバイスには不適合のフラグが付けられます。たとえば、デバイス (計算ノードのネットワーク・アダプターなど) を交換した場合で、そのネットワーク・アダプターのファームウェアがファームウェア・コンプライアンス・ポリシーで指定されているレベルと異なる場合、その計算ノードには不適合のフラグが付けられます。
  – **フラグなし**コンプライアンス違反デバイスにフラグが付けられません。

4. **オプション**: システム・タイプを展開してパッケージ内の各更新を表示し、コンプライアンス・ターゲットとして使用するファームウェア・レベルを選択するか、「更新しない」を選択してそのデバイスでファームウェアが更新されないようにします。
5. 「**作成**」をクリックします。

   ファームウェア・コンプライアンス・ポリシーが「ファームウェア更新: コンプライアンス・ポリシー」ページのテーブルに示されます。テーブルには、使用ステータス、ポリシーの作成元 (ユーザー定義か事前定義済みか)、前回の変更日が表示されます。

ステップ 3. 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: 適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページに管理対象デバイスのリストが表示されます。

ステップ 4. ファームウェア・コンプライアンス・ポリシーをデバイスに割り当てます。

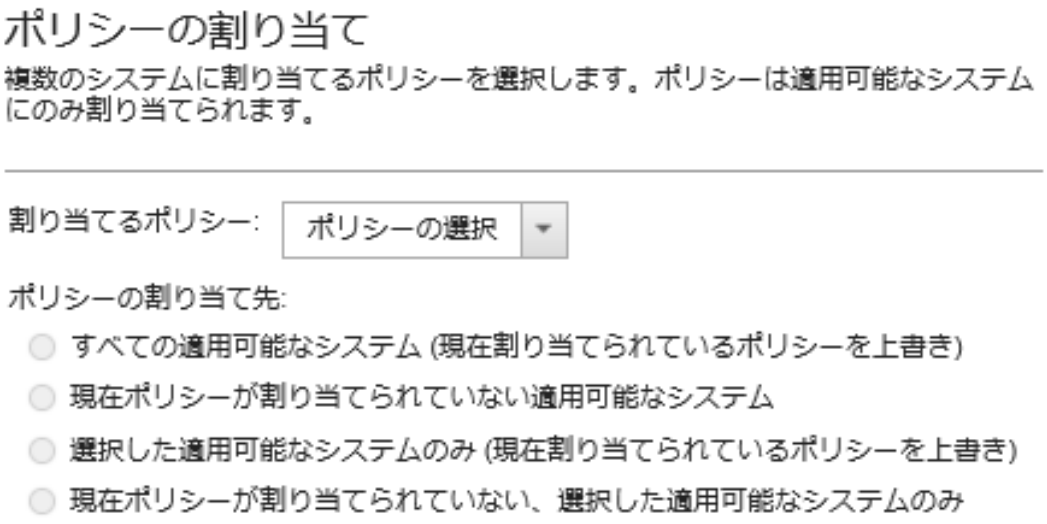
- **単一デバイスの場合**

  各デバイスについて、「**割り当て済みコンプライアンス・ポリシー**」列でドロップダウン・メニューからポリシーを選択します。

  各デバイスに適用可能なファームウェア・コンプライアンス・ポリシーのリストから選択できます。デバイスに現在ポリシーが割り当てられていない場合、割り当て済みポリシーは「**割り当てがありません**」に設定されます。デバイスに適用可能なポリシーがない場合、割り当て済みポリシーは**適用できるポリシーがありません**に設定されます。

- **複数のデバイスの場合**

1. **オプション**: ファームウェア・コンプライアンス・ポリシーを割り当てるデバイスを 1 つ以上選択します。
2. **ポリシーの割り当て**アイコン ( ) をクリックして、ポリシーの割り当てダイアログを表示します。



3. 「**割り当てるポリシー**」ドロップダウン・メニューからファームウェア・コンプライアンス・ポリシーを選択します。

   選択済みのすべてのデバイスに適用可能なファームウェア・コンプライアンス・ポリシーのリストから選択できます。ダイアログを開く前にデバイスを選択しなかった場合は、すべてのポリシーが一覧表示されます。

   ポリシーの割り当てを解除するには、**割り当てがありません**を選択します。
4. 以下のいずれかのポリシー割り当て範囲を選択します。
   - **以下の内容を満たす、適用可能なすべてのデバイス**
   - **以下の内容を満たす、選択済みの適用可能なデバイスのみ**
5. デバイスに関する 1 つまたは複数の基準を選択します。
   - **割り当て済みポリシーがない**
   - **非適合 (現在割り当てられているポリシーを上書き)**
   - **適合 (現在割り当てられているポリシーを上書き)**
   - **監視されていない (現在割り当てられているポリシーを上書き)**
   - **その他 (現在割り当てられているポリシーを上書き)**。これは、保留中の状態など、データが欠落している、または更新がサポートされていないなど、他の状態のデバイスに適用されます。ヘルプ・アイコン ( ) をポイントすると、該当するデバイスのリストが表示されます。

   注：監視されていないおよび**その他**の基準は、それらの状態にあるデバイスがある場合にのみ一覧表示されます。
6. 「**OK**」をクリックします。

   「ファームウェア更新: リポジトリー」ページの「**割り当て済みポリシー**」列に表示されたポリシーが、選択したファームウェア・コンプライアンス・ポリシーの名前に変わります。

終了後

ファームウェア・コンプライアンス・ポリシーを作成したら、選択したファームウェア・コンプライアンス・ポリシーに対して以下の操作を実行できます。

- 割り当てられたデバイスの一覧を含むポリシーの詳細を、テーブルのポリシー名をクリックして表示します。
- 「**コピー**」アイコン () をクリックして、選択済みポリシーの複製を作成します。
- 「**編集**」アイコン () をクリックして、選択済みポリシーを名前変更または変更します。事前定義済みのファームウェア・コンプライアンス・ポリシーまたは管理対象デバイスに割り当てられているポリシーは編集できません。

  割り当てられたポリシーを変更して、割り当てられた特定のデバイスに適用されなくなるようにすると、そのポリシーは自動的にそれらのデバイスから割り当て解除されます。

  事前定義済みの**最新ファームウェア**・ポリシーを名前変更したり、変更したりすることはできません。
- 「**ポリシーの削除**」アイコン () をクリックして、選択済みファームウェア・コンプライアンス・ポリシーを削除するか、または「**ポリシーおよびファームウェア・パッケージの削除**」アイコン () をクリックして、選択済みファームウェア・コンプライアンス・ポリシーおよびそのポリシーのみで使用されている関連するすべてのファームウェア更新を削除します。デバイスに割り当てられている場合でも、ポリシーを削除できます。

  デバイスに割り当てられているポリシーを削除する場合、ポリシーが割り当て解除されてから削除されます。

  事前定義済みの**最新ファームウェア**・ポリシーを削除することはできませんが、「**共通設定**」アイコン () をクリックし、「**最新ファームウェア・ポリシーを無効にする**」を選択することによって、ポリシーを無効にすることができます。このオプションを選択すると、最新のファームウェア・ポリシーが管理対象デバイスから割り当て解除され、そのポリシーは、リポジトリー内で使用可能な最新バージョンのファームウェアを含むように更新されなくなります。
- 選択済みポリシーをローカル・システムにエクスポートするには、ポリシーを選択し、「**エクスポート**」アイコン () をクリックします。その後、「**インポート**」アイコン () をクリックして、ポリシーを別の XClarity Administrator インスタンスにインポートできます。

ファームウェア・コンプライアンス・ポリシーを作成したら、ポリシーを特定のデバイスに割り当て (ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照)、そのデバイスの更新を適用およびアクティブ化できます (ファームウェア更新の適用とアクティブ化参照)。

準拠していないデバイスの特定

ファームウェア・コンプライアンス・ポリシーが管理対象デバイスに割り当てられている場合、そのデバイスのファームウェアがそのポリシーに適合しているかどうかを調べることができます。

手順

デバイスのファームウェアが割り当てられたファームウェア・コンプライアンス・ポリシーに適合しているかどうかを調べるには、Lenovo XClarity Administrator メニュー・バーから「**プロビジョニング**」 → 「**ファームウェア更新: 適用/アクティブ化**」をクリックして「ファームウェア更新: コンプライアンス・ポリシー」ページを表示し、そのデバイスの「**インストール済みバージョン**」列を確認します。

「**インストール済みバージョン**」列には、次のいずれかの値が含まれています。

- **ファームウェア・バージョン**。デバイスにインストールされたファームウェア・バージョンが、割り当てられたポリシーに適合しています。
- **適合**。デバイスにインストールされたファームウェアが、割り当てられたポリシーに適合しています。
- **非適合**。デバイスにインストールされたファームウェアが、割り当てられたポリシーに適合していません。

- **コンプライアンス・ポリシー未設定。**ファームウェア・コンプライアンス・ポリシーがデバイスに割り当てられていません。

「**最新表示**」アイコン ( ) をクリックすると、「**インストール済みバージョン**」列の内容を更新できます。

ファームウェア更新の共通設定の構成

共通設定は、オファームウェア更新が適用されるときに、デフォルト設定として使用されます。

このタスクについて

「共通設定」ページでは、以下の設定を構成できます。
- 下位レベルのデバイスの拡張サポート
- 割り当てられたポリシーに適合していないデバイスに関するアラート
- ポリシーが割り当てられていないデバイスに対するファームウェア・コンプライアンス・ポリシーの自動割り当て
- ファームウェア・コンプライアンス・ポリシーでターゲットが関連付けられていないファームウェア・コンポーネントを持つデバイスの非コンプライアンス・ステータス

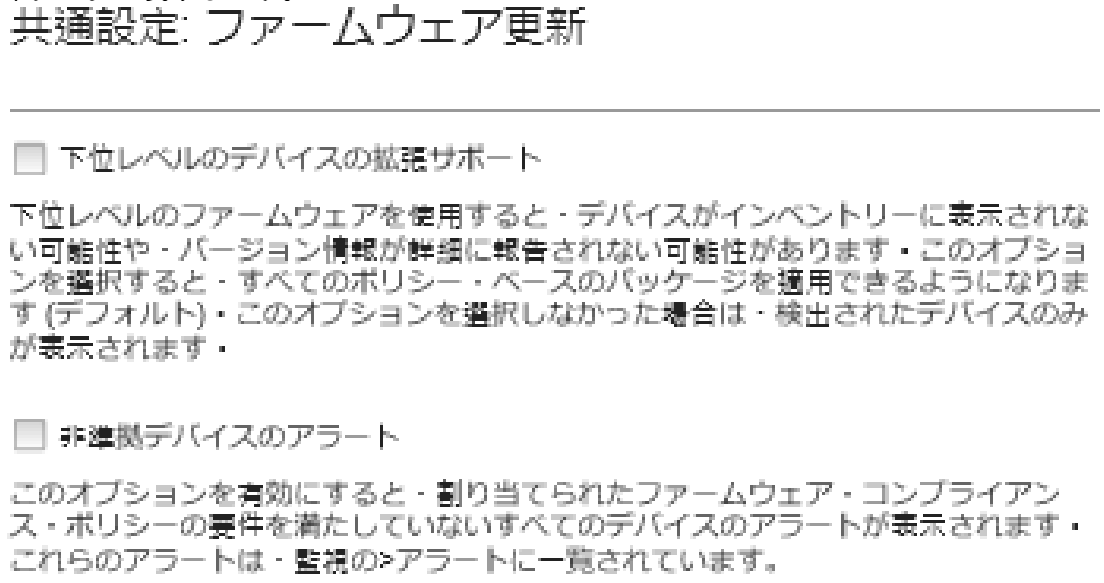
手順

すべてのサーバーに使用される共通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 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: 適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページが表示されます。

ステップ 2. 「**ポリシーのある更新**」タブまたは「**ポリシーのない更新**」タブをクリックします。

ステップ 3. 「**すべての操作**」 ➡ 「**共通設定**」をクリックして、「共通設定: ファームウェア更新」ダイアログを表示します。



ステップ 4. 任意で以下のオプションを選択します。

- ファームウェアが下位レベルの場合またはデバイスがインベントリーにない場合でもすべてのデバイスのインベントリーと全バージョン情報を表示するには、「**下位レベルのデバイスの拡張サポート**」を選択します。

- 割り当てられたファームウェア・コンプライアンス・ポリシーの要件を満たしていないデバイスのアラートを「アラート」ページに表示するには、「**非適合デバイスのアラート**」を選択します。デフォルトでは、アラートは「アラート」ページで非表示になっています。詳しくは、アクティブなアラートの表示を参照してください。
- 「**自動ポリシー割り当てを無効にする**」を選択し、ポリシーが割り当てられていないデバイスに対するファームウェア・コンプライアンス・ポリシーの自動割り当てを無効にします。このオプションが選択されていない場合、XClarity Administrator を再起動したり、新しいデバイスを管理したりするときに、ポリシーを使用せずにファームウェア・コンプライアンス・ポリシーがデバイスに割り当てられます。
- ファームウェア・コンポーネントがファームウェア・コンプライアンス・ポリシーのターゲットに関連付けられていない場合に、**Report Non-Compliance for Firmware Without Target** を選択すると、非コンプライアンスとしてデバイスをフラグできます。このオプションが選択されていない場合、ターゲットのないデバイスには準拠しているとしてフラグが付けられます。

ステップ 5. 「OK」をクリックして、ダイアログを閉じます。

ファームウェア更新の適用とアクティブ化

Lenovo XClarity Administrator では、管理対象デバイスにファームウェア更新が自動的に適用されません。コンプライアンス・ポリシーの有無を問わずファームウェア更新を適用できます。

始める前に

コンプライアンス・ポリシーを使用した場合、複数のデバイスの更新を同時にスケジュールできます。XClarity Administrator によってデバイスは自動的に正しい順序で更新されます。まず CMM、次にスイッチ、サーバーおよびストレージ・デバイスと続いて更新されます。

ダウンロードしたファームウェア更新のみが適用できます。

ファームウェア更新を実行すると、XClarity Administrator により 1 つ以上のジョブが開始されて更新が実行されます。

ファームウェア更新の進行中は、ターゲット・デバイスはロックされています。更新プロセスが完了するまでは、ターゲット・デバイス上にある他の管理タスクを開始できません。

ファームウェア更新がデバイスに適用された後、ファームウェア更新を完全にアクティブ化するため再起動が 1 回以上必要になる可能性があります。デバイスをすぐに再起動するか、後でアクティブ化するか、またはアクティブ化に優先順位を付けることを選択できます。すぐに再起動することを選択した場合、XClarity Administrator により必要な再起動回数が最小限に抑えられます。後でアクティブ化することを選択した場合、次回デバイスが再起動されたときに更新がアクティブ化されます。アクティブ化に優先順位を付ける場合は、ベースボード管理コントローラーの更新が即座にアクティブ化され、その他のすべてのファームウェア更新は次回のデバイスの再起動時に有効になることに注意してください。

一度に最大 50 台のデバイスで選択したファームウェアを更新できます。50 台以上のデバイスで選択したファームウェアを更新する場合、残りのデバイスはキューに置かれます。更新対象デバイスでアクティベーションが完了するか、更新対象デバイスが保留中の保守モード状態になると (そのデバイスで再起動が必要な場合)、キューに入っているデバイスは、「選択したファームウェアの更新」キューから取り出されます。保留中の保守モード状態のデバイスが再起動されると、デバイスは保守モードでブートし、ファームウェア更新の最大数が既に進行中であっても更新プロセスを続行します。

一度に最大 10 台のデバイスで、バンドルしたファームウェアを更新できます。10 台以上のデバイスで、バンドルしたファームウェアを更新する場合、残りのデバイスはキューに置かれます。バンドルしたファームウェアの更新が実行されたデバイスでアクティベーションが完了すると、キューに入っているデバイスは「バンドルしたファームウェアの更新」キューから取り出されます。

注意：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。XClarity Administrator から「**通常の再起動**」または「**今すぐ再起動**」操作を実行する前に、オペレーティング・システムを手動で構成して電源ボタンの動作を電源オフに変更する必要があります。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。

注：XClarity Administrator により LAN-over-USB インターフェースが自動的に有効になります。

コンプライアンス・ポリシーを使用するバンドルされたファームウェア更新の適用

Lenovo XClarity Administratorが管理対象デバイスを不適合として示したら、適応可能なファームウェア更新パッケージを含むバンドル・イメージを使用して、割り当てられたファームウェア・コンプライアンス・ポリシーに適合していない、選択済み ThinkSystem SR635 および SR655 サーバーの *すべて*のコンポーネントにファームウェア更新を手動で適用できます。*バンドル・イメージ*は、コンプライアンス・ポリシーからすべてのファームウェア更新プログラム・パッケージを収集することで、更新プロセス中に作成されます。

始める前に

- 管理対象デバイスでファームウェアを更新する前に、ファームウェア更新の考慮事項を読んでください (ファームウェアの更新に関する考慮事項 を参照)。
- 最初は、更新がサポートされていないデバイスはビューに表示されません。サポートされていないデバイスを更新するように選択することはできません。
- デフォルトでは、検出されたすべてのコンポーネントが更新を適用できるコンポーネントとしてリストされますが、下位レベルのファームウェアが原因で、コンポーネントがインベントリーに表示されない可能性や、バージョン情報が詳細に報告されない可能性があります。更新を適用できる、すべてのポリシー・ベースのパッケージをリストに表示するには、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**下位レベルのデバイスの拡張サポート**」を選択します。このオプションを選択すると、未検出のデバイスの「インストール済みバージョン」列に「その他の利用可能なソフトウェア」がリストされます。詳しくは、ファームウェア更新の共通設定の構成を参照してください。

  注：

  – 管理対象デバイスに対する更新が進行中の場合、グローバル設定を変更することはできません。

  – 追加のオプションを生成するには数分かかります。しばらくしてから、テーブルを更新するために「**最新表示**」アイコン ( ) をクリックする必要がある場合があります。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 ➡ 「**ジョブ**」をクリックします。
- バンドルされたファームウェアの更新の適用は、ThinkSystem SR635 および SR655 サーバーでのみサポートされています。
- バンドルされたファームウェア更新の適用は、IPv4 アドレスでのみサポートされています。IPv6 アドレスはサポートされていません。
- インベントリー情報全体を取得するために、各ターゲット・デバイスが少なくとも 1 回 OS にブートされたことを確認してください。
- バンドル更新機能を使用するには、ベースボード管理コントローラー・ファームウェア v2.94 以降が必要です。
- リポジトリー・パックからのファームウェア更新または個々のファームウェア更新のみが使用されます。UpdateXpress System Packs (UXSPs) はサポートされていません。
- ダウンロードしたファームウェア更新のみが適用されます。製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロード)。

注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。

- コンプライアンス確認は、ThinkSystem SR635 および SR655 サーバーのベースボード管理コントローラーと UEFI でのみサポートされます。ただし、XClarity Administrator は、利用可能なすべてのハードウェア・コンポーネントにファームウェア更新を適用しようとします。
- 更新は、割り当てられたファームウェア・コンプライアンス・ポリシーに従って適用されます。コンポーネントのサブセットを更新することはできません。
- Lenovo XClarity Provisioning Manager (LXPM)、LXPM のウィンドウ・ドライバー、または LXPM Linux ドライバーのファームウェア更新を ThinkSystem SR635 および SR655 サーバーに適用するには、XClarity Administrator v3.2 以降が必要です。
- 現在インストールされているバージョンが、割り当てられたコンプライアンス・ポリシーよりも新しい場合、ベースボード管理コントローラーと UEFI の更新はスキップされます。
- ファームウェア・コンプライアンス・ポリシーが作成済みであり、ファームウェア更新を適用するデバイスに割り当て済みである必要があります。詳しくは、ファームウェア・コンプライアンス・ポリシーの作成と割り当てを参照してください。
- 選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。

注意：選択したデバイスは、更新プロセスを開始する前に電源がオフになります。必ず、実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 → 「**ジョブ**」をクリックします。

このタスクについて

バンドル更新プロセスは、まず、ベースボード管理コントローラーと UEFI アウト・オブ・バンドを更新します。これらの更新が完了すると、プロセスは、マシン・タイプに基づいて、コンプライアンス ポリシー内の残りのファームウェアのバンドル・イメージを作成します。次に、プロセスは選択したデバイスにイメージをマウントし、デバイスを再起動してイメージをブートします。イメージは自動的に実行され、残りの更新が実行されます。

一度に最大 10 台のデバイスで、バンドルしたファームウェアを更新できます。10 台以上のデバイスで、バンドルしたファームウェアを更新する場合、残りのデバイスはキューに置かれます。バンドルしたファームウェアの更新が実行されたデバイスでアクティベーションが完了すると、キューに入っているデバイスは「バンドルしたファームウェアの更新」キューから取り出されます。

デバイス内のコンポーネントの更新中にエラーが発生した場合、その特定のコンポーネントのファームウェアはファームウェアの更新プロセスにより更新されません。ただし、ファームウェアの更新プロセスは、デバイス内の他のコンポーネントの更新を続行し、現在のファームウェア更新ジョブに含まれる他のすべてのデバイスの更新を続行します。

手順

管理対象デバイスにバンドル・イメージの形式でファームウェアの更新を適用するには、次の手順を実行します。

ステップ 1. 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: 適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページが表示されます。

ステップ 2. 「**ポリシーのある更新**」タブをクリックします。

ステップ 3. ファームウェア更新を適用するデバイスとコンポーネントを 1 台以上選択します。

テーブルの列をソートすると特定のデバイスを見つけやすくなります。また、「**表示**」メニューのオプションを選択して特定のシャーシ、ラック、グループのデバイスのみをリストし、表示されたデバイスのリストをフィルタリングすることもできます。これを行うには、

「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力するか、次のアイコンをクリックして特定のステータスのデバイスのみをリストします。

- **準拠デバイスを非表示** アイコン ()
- 「**非準拠デバイスのステータスを非表示**」アイコン ()
- **割り当て済みコンプライアンス・ポリシーのないデバイスを非表示** アイコン ()
- 「**監視されていないデバイスを非表示**」アイコン ()
- 「**アクティベーション保留中のファームウェアがあるデバイスを非表示**」アイコン ()
- 「**コンプライアンス・エラーが発生したデバイスを非表示**」アイコン ()
- 「**更新がサポートされていないデバイスを非表示**」アイコン ()
- 「**ファームウェア更新を実行中のデバイスを非表示**」アイコン ()
- 「**ステージング不可能なファームウェアがあるデバイスを非表示**」アイコン ()

「**グループ**」列には、各デバイスがメンバーとなっているグループが表示されます。「**グループ**」列にカーソルを合わせると、グループ・タイプ別のグループの完全リストが取得できます。

「**インストール済みバージョン**」列には、インストール済みファームウェア・バージョン、コンプライアンスの状態、デバイスの状態が表示されます。

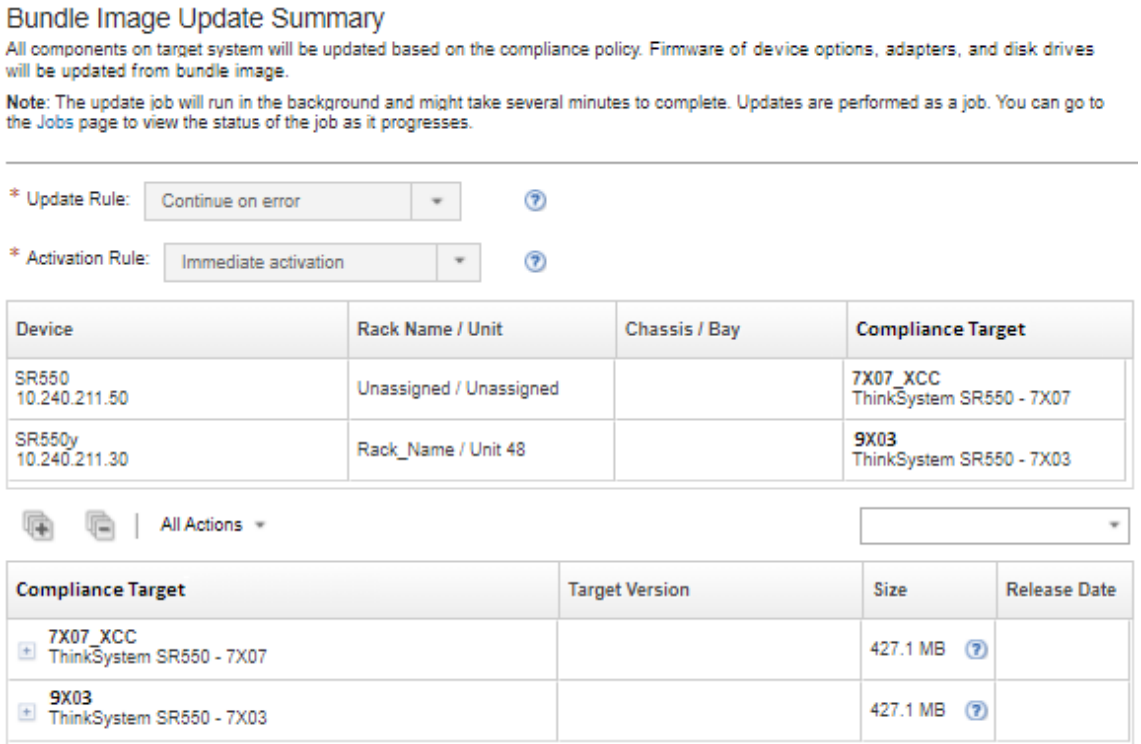
コンプライアンスの状態は以下のいずれかです。

-  **適合**
-  **コンプライアンス・エラー**
-  **非適合**
-  **コンプライアンス・ポリシー未設定**
-  **監視されていません**

デバイスの状態は以下のいずれかです。

-  **更新がサポートされていません**
-  **更新が進行中です**

ステップ 4. 「**バンドル・イメージからの更新の実行**」アイコンをクリックします ( )。「バンドル・イメージの更新の要約」ダイアログが表示されます。このダイアログには、バンドル・イメージに含まれる選択済みデバイスとファームウェアの更新が一覧表示されます。



ステップ 5. 「**バンドル・イメージからの更新の実行**」をクリックして今すぐ更新するか、「**スケジュール**」をクリックして、後で実行するようにスケジュールします。

終了後

ファームウェア更新を適用する際、サーバーが保守モードに切り替わらない場合は、更新をもう一度適用してみてください。

更新が正常に終了しなかった場合、トラブルシューティングと修正処置については、XClarity Administrator オンライン・ドキュメントのファームウェア更新とリポジトリーの問題を参照してください。

「ファームウェア更新: 適用/アクティブ化」ページからは、以下の操作を実行できます。

- 「**すべての操作**」 → 「**表示を CSV としてエクスポート**」をクリックして、各管理対象デバイスのファームウェアとコンプライアンス情報をエクスポートする。

  注：CSV ファイルには、現在のビューでフィルタリングされている情報のみが含められます。ビューから除外された情報と非表示列の情報は含められません。
- デバイスを選択して「**更新のキャンセル**」アイコン ( ) をクリックすることで、デバイスに適用する更新をキャンセルする。

  注：キューにあって開始を待つファームウェア更新をキャンセルできます。更新プロセスの開始後は、保守モードへの変更やデバイスの再起動など、実際に更新を適用するタスク以外のタスクを更新プロセスが実行している途中に、ファームウェア更新をキャンセルできます。
- 「適用/アクティブ化」ページの「**ステータス**」列でファームウェア更新のステータスを直接確認する。
- ジョブ・ログから更新プロセスのステータスを監視する。Lenovo XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。

  ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

ファームウェア更新ジョブが完了したら、「**プロビジョニング**」 → 「**ファームウェア更新: 適用/アクティブ化**」をクリックして「ファームウェア更新: 適用/アクティブ化」ページに戻り、「**最新表示**」アイコン ( ) をクリックすることで、デバイスが適合していることを確認できます。各デバイスでアクティブな現在のファームウェア・バージョンが、「**インストール済みバージョン**」列に表示されます。

コンプライアンス・ポリシーを使用する選択済みファームウェア更新の適用

Lenovo XClarity Administrator がデバイスを不適合であることを示したら、Web インターフェースを使用して管理対象デバイスのファームウェア更新を手動で適用してアクティブ化できます。ファームウェア・コンプライアンス・ポリシーに該当するすべてのファームウェア更新を適用してアクティブ化するか、ポリシー内の特定のファームウェア更新のみを適用してアクティブ化するように選択できます。ダウンロードしたファームウェア更新のみが適用されます。

詳細:

- XClarity Administrator: ファームウェア更新時の 効率の向上
- Lenovo ThinkSystem ファームウェアおよび ドライバー更新のベスト・プラクティス
- XClarity Administrator: ベア・メタルからクラスターへ
- XClarity Administrator: ファームウェア更新
- XClarity Administrator: ファームウェア・ セキュリティー更新のプロビジョニング

始める前に

- 管理対象デバイスでファームウェアを更新する前に、ファームウェア更新の考慮事項を読んでください (ファームウェアの更新に関する考慮事項 を参照)。
- 最初は、更新がサポートされていないデバイスはビューに表示されません。サポートされていないデバイスを更新するように選択することはできません。
- デフォルトでは、検出されたすべてのコンポーネントが更新を適用できるコンポーネントとしてリストされますが、下位レベルのファームウェアが原因で、コンポーネントがインベントリーに表示されない可能性や、バージョン情報が詳細に報告されない可能性があります。更新を適用できる、すべてのポリシー・ベースのパッケージをリストに表示するには、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**下位レベルのデバイスの拡張サポート**」を選択します。このオプションを選択すると、未検出のデバイスの「インストール済みバージョン」列に「その他の利用可能なソフトウェア」がリストされます。詳しくは、ファームウェア更新の共通設定の構成を参照してください。

  注：

  – 管理対象デバイスに対する更新が進行中の場合、グローバル設定を変更することはできません。

  – 追加のオプションを生成するには数分かかります。しばらくしてから、テーブルを更新するために「**最新表示**」アイコン ( ) をクリックする必要がある場合があります。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 ➡ 「**ジョブ**」をクリックします。
- デプロイするファームウェア・パッケージがファームウェア更新リポジトリーに含まれていることを確認します。含まれていない場合は、製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロードを参照)。

  注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。

  前提条件ファームウェアをインストールする場合は、前提条件ファームウェアもリポジトリーにダウンロードしていることを確認してください。

  場合によっては、ファームウェアを更新するために複数のバージョンが必要になることがあり、その場合はすべてのバージョンをリポジトリーにダウンロードする必要があります。たとえば、IBM FC5022 SAN スケーラブル・スイッチを v7.4.0a から v8.2.0a にアップグレードするには、まず v8.0.1-pha、次に v8.1.1、そして v8.2.0a をインストールします。スイッチを v8.2.0a に更新するには、この 3 つのバージョンすべてがリポジトリーに含まれる必要があります。
- 通常、ファームウェア更新をアクティブ化するにはデバイスを再起動する必要があります。更新プロセス中にデバイスの再起動を選択した場合 (*即時アクティベーション*)、必ず実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。
- ThinkSystem SR635 および SR655 サーバーの場合、この従来の更新機能を使用して、ベースボード管理コントローラーと UEFI ファームウェア更新のみを適用できます。管理コントローラー・ファームウェア・バージョン AMBT10M 以降が必要であり、UEFI ファームウェア・バージョン CFE114L 以降が必要です。すべてのコンポーネント (管理コントローラー、UEFI、ディスク・ドライブ、および IO オプションを含む) を更新するには、バンドル更新機能を使用します (コンプライアンス・ポリシーを使用するバンドルされたファームウェア更新の適用を参照)。

このタスクについて

- 一度に最大 50 台のデバイスで選択したファームウェアを更新できます。50 台以上のデバイスで選択したファームウェアを更新する場合、残りのデバイスはキューに置かれます。更新対象デバイスでアクティベーションが完了するか、更新対象デバイスが保留中の保守モード状態になると (そのデバイスで再起動が必要な場合)、キューに入っているデバイスは、「選択したファームウェアの更新」キューから取り出されます。保留中の保守モード状態のデバイスが再起動されると、デバイスは保守モードでブートし、ファームウェア更新の最大数が既に進行中であっても更新プロセスを続行します。
- 現在インストールされているファームウェアよりも新しいファームウェアを適用してアクティブ化できます。
- 特定のデバイスのすべての更新を適用することを選択できます。ただし、デバイスを展開して、特定のコンポーネント (ベースボード管理コントローラーや UEFI など) の更新を指定することもできます。
- 複数のコンポーネントに対する更新を含むファームウェア更新パッケージをインストールするように選択した場合、更新パッケージが適用されるすべてのコンポーネントが更新されます。

手順

管理対象デバイスに更新を適用してアクティブにするには、以下の手順を実行します。

ステップ 1. 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: 適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページが表示されます。

ステップ 2. 「**ポリシーのある更新**」タブをクリックします。

ステップ 3. ファームウェア更新を適用するデバイスとデバイスを 1 台以上選択します。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。また、「**表示**」メニューのオプションを選択して特定のシャーシ、ラック、グループのデバイスのみをリストし、表示されたデバイスのリストをフィルタリングすることもできます。これを行うには、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力するか、次のアイコンをクリックして特定のステータスのデバイスのみをリストします。

- **準拠デバイスを非表示** アイコン ()
- 「**非準拠デバイスのステータスを非表示**」アイコン ()
- **割り当て済みコンプライアンス・ポリシーのないデバイスを非表示** アイコン ()
- 「**監視されていないデバイスを非表示**」アイコン ()
- 「**アクティベーション保留中のファームウェアがあるデバイスを非表示**」アイコン ()
- 「**コンプライアンス・エラーが発生したデバイスを非表示**」アイコン ()
- 「**更新がサポートされていないデバイスを非表示**」アイコン ()
- 「**ファームウェア更新を実行中のデバイスを非表示**」アイコン ()
- 「**ステージング不可能なファームウェアがあるデバイスを非表示**」アイコン ()

「**グループ**」列には、各デバイスがメンバーとなっているグループが表示されます。「**グループ**」列にカーソルを合わせると、グループ・タイプ別のグループの完全リストが取得できます。

「**インストール済みバージョン**」列には、インストール済みファームウェア・バージョン、コンプライアンスの状態、デバイスの状態が表示されます。

コンプライアンスの状態は以下のいずれかです。

-  **適合**
-  **コンプライアンス・エラー**

- **非適合**
- **コンプライアンス・ポリシー未設定**
- **監視されていません**

デバイスの状態は以下のいずれかです。
- **更新がサポートされていません**
- **更新が進行中です**

注：インストール済みファームウェアのバージョンがアクティベーション保留中である場合、該当する各デバイスのインストール済みファームウェアのバージョンまたはコンプライアンスの状態に「(アクティベーション保留中)」が追加されます。例: 「2.20 / A9E12EUS (アクティベーション保留中)」。アクティベーション保留中ステータスを確認するには、以下のファームウェア・バージョンが、サーバー内のプライマリー・ベースボード管理コントローラーにインストールされている必要があります。
- **IMM2**: TCOO46F、TCOO46E またはそれ以降 (プラットフォームによって異なります)
- **XCC**: CDI328M、PSI316N、TEI334I またはそれ以降 (プラットフォームによって異なります)

ファームウェア更新: 適用/有効化

ステップ 4. 「**更新の実行**」アイコン ( ) をクリックします。「更新の要約」ダイアログが表示されます。

ステップ 5. 以下の更新ルールのいずれかを選択します。

- **エラーですべての更新を停止**。ターゲット・デバイスのいずれかのコンポーネント (アダプターや管理コントローラーなど) の更新中にエラーが発生した場合、現在のファームウェア更新ジョブに含まれるすべての選択したデバイスに対して、ファームウェアの更新プロセスが停止します。この場合、デバイスの更新パッケージに含まれるどの更新も適用されません。すべての選択したシステムにインストールされている現在のファームウェアが引き続き有効になります。
- **エラーで続行**。デバイス内のいずれかのデバイスの更新中にエラーが発生した場合、その特定のデバイスのファームウェアはファームウェアの更新プロセスにより更新されません。ただし、ファームウェアの更新プロセスは、デバイス内の他のデバイスの更新を続行し、現在のファームウェア更新ジョブに含まれる他のすべてのデバイスの更新を続行します。
- **エラーで次のシステムに進む**。デバイス内のいずれかのデバイスの更新中にエラーが発生した場合、ファームウェアの更新プロセスがその特定のデバイスのファームウェアの更新試行をすべて停止するため、そのデバイスにインストールされた現在のファームウェアが有効なままになります。ファームウェアの更新プロセスは、現在のファームウェア更新ジョブに含まれる他のすべてのデバイスの更新を続行します。

ステップ 6. 以下のアクティブベーション・ルールのいずれかを選択します。

- **即時アクティベーション**。更新プロセス中に、更新プロセス全体が完了するまでの間、デバイスが複数回自動的に再起動される可能性があります。続行する前に、デバイスのすべてのアプリケーションを休止させてください。
- **遅延アクティベーション**。全部ではなく一部の更新操作が実行されます。更新プロセスを続行するには、デバイスを再起動する必要があります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。

  ステータスが「**ファームウェア保守モードを保留中**」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

  何らかの理由でデバイスが再起動すると、遅延更新プロセスが完了します。

  このアクティベーション・ルールは、サーバーおよびラック・スイッチでのみサポートされています。CMM と Flex スイッチは、この設定に関係なく即座にアクティブ化されます。

  ステータスが「**ファームウェア保守モードを保留中**」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

遅延更新プロセスは、何らかの理由でデバイスが再起動すると (手動再起動を含む) 完了します。サーバーを再起動する必要がある場合は、時間制限はありません。

XClarity Administrator では、遅延アクティベーションを使用して、最大 50 台のデバイスに更新を一度に適用できます。遅延アクティベーションを使用して 50 台を超えるデバイスに更新を適用しようとすると、残りのデバイスはキューに入れられます。更新するデバイスが「**ファームウェア保守モードを保留中**」状態になると、デバイスがキューから出ます。

重要：

- 更新ジョブ中に XClarity Administrator が再起動すると、更新ジョブがエラーになり、停止します。
- XClarity Administrator が停止または到達不能なときに、「**ファームウェア保守モードを保留中**」状態のサーバーが再起動された場合、サーバーは BMU にブートしますが、XClarity Administrator は 60 秒後に BMU に接続できないため、システムの電源ステータスはベースボード管理コントローラーによって復元されます (電源がオフの場合はオフで、電源がオンの場合は再起動します)。

- **優先順位を設定したアクティベーション**。ベースボード管理コントローラーのファームウェア更新は即座にアクティブ化されます。その他のすべてのファームウェア更新は、次回にデバイスが再起動したときに有効になります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。このルールは、サーバーでのみサポートされています。

  ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

注：有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。

ステップ 7. **オプション**: ファームウェア・レベルが最新の場合でも選択したコンポーネントのファームウェアを更新するか、現在選択されたコンポーネントにインストールされているものより前のファームウェア更新を適用するには、「**強制更新**」を選択します。

注：以前のバージョンのファームウェアをデバイス・オプション、アダプター、下位レベルをサポートするドライブに適用することができます。下位レベルがサポートされているかどうかを判別するには、ハードウェアの資料を参照してください。

ステップ 8. **オプション**:前提条件となるファームウェアをインストールしたくない場合は、「**前提条件となるファームウェアをインストール**」をオフにします。デフォルトでは、前提条件となるファームウェアがインストールされます。

注：前提条件となるファームウェア更新に**遅延アクティベーション**または**優先順位を付けたアクティベーション**を使用すると、前提条件となるファームウェアをアクティブ化するためにサーバーを再起動する必要があります。最初の再起動後に**即時アクティベーション**を使用して残るファームウェアの更新がインストールされます。

ステップ 9. **オプション**: **即時アクティベーション** を選択した場合、**[メモリー・テスト]** を選択して、更新中にサーバーがリブートした場合に、ファームウェア更新の完了後にメモリー・テストを実行します。

このオプションは ThinkSystem v1 および v2 サーバー (ThinkSystem SR635、SR645、SR655、SR665 サーバーを除く) でサポートされます。

ステップ 10.「**更新の実行**」をクリックして今すぐ更新するか、「**スケジュール**」を更新してこの更新を後で実行するようにスケジュールします。

必要な場合、管理対象デバイスで電源操作を実行できます。電源操作は、「**遅延アクティベーション**」が選択されていて、デバイスが「保守を保留中」状態で待機しているときに更新を続行したい場合に役立ちます。このページから管理対象デバイスで電源操作を実行するには、「**すべての操作**」 ➡ 「**電源操作**」をクリックし、以下のいずれかの電源操作をクリックします。

- **電源オン**
- **OS のシャットダウンと電源オフ**
- **電源オフ**
- **OS のシャットダウンと再起動**
- **再起動**

終了後

ファームウェア更新を適用する際、サーバーが保守モードに切り替わらない場合は、更新をもう一度適用してみてください。

更新が正常に終了しなかった場合、トラブルシューティングと修正処置については、XClarity Administrator オンライン・ドキュメントのファームウェア更新とリポジトリーの問題を参照してください。

「ファームウェア更新: 適用/アクティブ化」ページからは、以下の操作を実行できます。

- 「**すべての操作**」 ➡ 「**表示を CSV としてエクスポート**」をクリックして、各管理対象デバイスのファームウェアとコンプライアンス情報をエクスポートする。

  注：CSV ファイルには、現在のビューでフィルタリングされている情報のみが含められます。ビューから除外された情報と非表示列の情報は含められません。
- デバイスを選択して「**更新のキャンセル**」アイコン () をクリックすることで、デバイスに適用する更新をキャンセルする。

  注：キューにあって開始を待つファームウェア更新をキャンセルできます。更新プロセスの開始後は、保守モードへの変更やデバイスの再起動など、実際に更新を適用するタスク以外のタスクを更新プロセスが実行している途中に、ファームウェア更新をキャンセルできます。
- 「適用/アクティブ化」ページの「**ステータス**」列でファームウェア更新のステータスを直接確認する。
- ジョブ・ログから更新プロセスのステータスを監視する。Lenovo XClarity Administrator のメニューで、「**監視**」 ➡ 「**ジョブ**」の順にクリックします。

  ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

ファームウェア更新ジョブが完了したら、「**プロビジョニング**」 ➡ 「**ファームウェア更新: 適用/アクティブ化**」をクリックして「ファームウェア更新: 適用/アクティブ化」ページに戻り、「**最新表示**」アイコン ( ) をクリックすることで、デバイスが適合していることを確認できます。各デバイスでアクティブな現在のファームウェア・バージョンが、「**インストール済みバージョン**」列に表示されます。

コンプライアンス・ポリシーを使用しない選択済みファームウェア更新の適用

コンプライアンス・ポリシーを使用せずに、単一の管理対象デバイスまたはデバイス・グループに現在インストールされているファームウェアよりも新しいファームウェアをすばやく適用してアクティブ化できます。

詳細:

- XClarity Administrator: ファームウェア更新時の 効率の向上
- Lenovo ThinkSystem ファームウェアおよび ドライバー更新のベスト・プラクティス
- XClarity Administrator: ベア・メタルからクラスターへ
- XClarity Administrator: ファームウェア更新
- XClarity Administrator: ファームウェア・ セキュリティー更新のプロビジョニング

始める前に

- 管理対象デバイスでファームウェアを更新する前に、ファームウェア更新の考慮事項を読んでください (ファームウェアの更新に関する考慮事項 を参照)。
- 最初は、更新がサポートされていないデバイスはビューに表示されません。サポートされていないデバイスを更新するように選択することはできません。
- デフォルトでは、検出されたすべてのコンポーネントが更新を適用できるコンポーネントとしてリストされますが、下位レベルのファームウェアが原因で、コンポーネントがインベントリーに表示されない可能性や、バージョン情報が詳細に報告されない可能性があります。更新を適用できる、すべてのポリシー・ベースのパッケージをリストに表示するには、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**下位レベルのデバイスの拡張サポート**」を選択します。このオプションを選択すると、未検出のデバイスの「インストール済みバージョン」列に「その他の利用可能なソフトウェア」がリストされます。詳しくは、ファームウェア更新の共通設定の構成を参照してください。

  注：

  - 管理対象デバイスに対する更新が進行中の場合、グローバル設定を変更することはできません。
  - 追加のオプションを生成するには数分かかります。しばらくしてから、テーブルを更新するために「**最新表示**」アイコン () をクリックする必要がある場合があります。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。ジョブを実行中の場合、更新ジョブは他のジョブがすべて完了するまでキューに入れられます。アクティブ・ジョブのリストを表示するには、「**監視**」 → 「**ジョブ**」をクリックします。
- デプロイするファームウェア・パッケージがファームウェア更新リポジトリーに含まれていることを確認します。含まれていない場合は、製品カタログを更新し、適切なファームウェア更新をダウンロードします (製品カタログの更新とファームウェア更新のダウンロードを参照)。

  注：XClarity Administrator を最初にインストールしたときは、製品カタログとリポジトリーは空です。

  前提条件ファームウェアをインストールする場合は、前提条件ファームウェアもリポジトリーにダウンロードしていることを確認してください。

  場合によっては、ファームウェアを更新するために複数のバージョンが必要になることがあり、その場合はすべてのバージョンをリポジトリーにダウンロードする必要があります。たとえば、IBM FC5022 SAN スケーラブル・スイッチを v7.4.0a から v8.2.0a にアップグレードするには、まず v8.0.1-pha、次に v8.1.1、そして v8.2.0a をインストールします。スイッチを v8.2.0a に更新するには、この 3 つのバージョンすべてがリポジトリーに含まれる必要があります。
- 通常、ファームウェア更新をアクティブ化するにはデバイスを再起動する必要があります。更新プロセス中にデバイスの再起動を選択した場合 (*即時アクティベーション*)、必ず実行中のワークロードを停止してください。仮想化環境で作業している場合は、別のサーバーに移動してください。

このタスクについて

- 一度に最大 50 台のデバイスで選択したファームウェアを更新できます。50 台以上のデバイスで選択したファームウェアを更新する場合、残りのデバイスはキューに置かれます。更新対象デバイスでアクティベーションが完了するか、更新対象デバイスが保留中の保守モード状態になると (そのデバイスで再起動が必要な場合)、キューに入っているデバイスは、「選択したファームウェアの更新」キューから取り出されます。保留中の保守モード状態のデバイスが再起動されると、デバイスは保守モードでブートし、ファームウェア更新の最大数が既に進行中であっても更新プロセスを続行します。
- 現在インストールされているファームウェアよりも新しいファームウェアを適用してアクティブ化できます。
- 特定のデバイスのすべての更新を適用することを選択できます。ただし、デバイスを展開して、特定のコンポーネント (ベースボード管理コントローラーや UEFI など) の更新を指定することもできます。
- 複数のコンポーネントに対する更新を含むファームウェア更新パッケージをインストールするように選択した場合、更新パッケージが適用されるすべてのコンポーネントが更新されます。

手順

管理対象デバイスに更新を適用してアクティブにするには、以下の手順を実行します。

ステップ 1. 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: 適用/アクティブ化**」の順にクリックします。「ファームウェア更新: 適用/アクティブ化」ページが表示されます。

ステップ 2. 「**ポリシーのない更新**」タブをクリックします。

ステップ 3. 更新するデバイスごとに「**ダウンロード済みの新しいバージョン**」列でファームウェア・レベルを選択します。

ステップ 4. 更新するデバイスを 1 つ以上選択します。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。また、「**表示**」メニューのオプションを選択して特定のシャーシ、ラック、グループのデバイスのみをリストし、表示されたデバイスのリストをフィルタリングすることもできます。これを行うには、

「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力するか、次のアイコンをクリックして特定のステータスのデバイスのみをリストします。

- 「**新しいバージョンがあるコンポーネントを非表示**」アイコン ()
- 「**新しいバージョンがないコンポーネントを非表示**」アイコン ()
- 「**更新がサポートされていないデバイスを非表示**」アイコン ()
- 「**ファームウェア更新を実行中のデバイスを非表示**」アイコン ()
- 「**ステージング不可能なファームウェアがあるデバイスを非表示**」アイコン ()

「**グループ**」列には、各デバイスがメンバーとなっているグループが表示されます。「**グループ**」列にカーソルを合わせると、グループ・タイプ別のグループの完全リストが取得できます。

「**インストール済みバージョン**」列には、インストール済みファームウェア・バージョン、コンプライアンスの状態、デバイスの状態が表示されます。

コンプライアンスの状態は以下のいずれかです。

-  **適合**
-  **コンプライアンス・エラー**
-  **非適合**
-  **コンプライアンス・ポリシー未設定**
-  **監視されていません**

デバイスの状態は以下のいずれかです。

-  **更新がサポートされていません**
-  **更新が進行中です**

注：インストール済みファームウェアのバージョンがアクティベーション保留中である場合、該当する各デバイスのインストール済みファームウェアのバージョンまたはコンプライアンスの状態に「(アクティベーション保留中)」が追加されます。例: 「2.20 / A9E12EUS (アクティベーション保留中)」。アクティベーション保留中ステータスを確認するには、以下のファームウェア・バージョンが、サーバー内のプライマリー・ベースボード管理コントローラーにインストールされている必要があります。

- IMM2: TCOO46F、TCOO46E またはそれ以降 (プラットフォームによって異なります)
- XCC: CDI328M、PSI316N、TEI334I またはそれ以降 (プラットフォームによって異なります)

ステップ 5. 「**更新の実行**」アイコン ( ) をクリックします。「更新の要約」ダイアログが表示されます。

ステップ 6. 以下の更新ルールのいずれかを選択します。

- **エラーですべての更新を停止**。ターゲット・デバイスのいずれかのコンポーネント (アダプターや管理コントローラーなど) の更新中にエラーが発生した場合、現在のファームウェア更新ジョブに含まれるすべての選択したデバイスに対して、ファームウェアの更新プロセスが停止します。この場合、デバイスの更新パッケージに含まれるどの更新も適用されません。すべての選択したシステムにインストールされている現在のファームウェアが引き続き有効になります。
- **エラーで続行**。デバイス内のいずれかのデバイスの更新中にエラーが発生した場合、その特定のデバイスのファームウェアはファームウェアの更新プロセスにより更新されません。ただし、ファームウェアの更新プロセスは、デバイス内の他のデバイスの更新を続行し、現在のファームウェア更新ジョブに含まれる他のすべてのデバイスの更新を続行します。

- **エラーで次のシステムに進む**。デバイス内のいずれかのデバイスの更新中にエラーが発生した場合、ファームウェアの更新プロセスがその特定のデバイスのファームウェアの更新試行をすべて停止するため、そのデバイスにインストールされた現在のファームウェアが有効なままになります。ファームウェアの更新プロセスは、現在のファームウェア更新ジョブに含まれる他のすべてのデバイスの更新を続行します。

注：有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。

ステップ 7. 以下のアクティブベーション・ルールのいずれかを選択します。

- **即時アクティベーション**。更新プロセス中に、更新プロセス全体が完了するまでの間、デバイスが複数回自動的に再起動される可能性があります。続行する前に、デバイスのすべてのアプリケーションを休止させてください。
- **遅延アクティベーション**。全部ではなく一部の更新操作が実行されます。更新プロセスを続行するには、デバイスを再起動する必要があります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。

  ステータスが「**ファームウェア保守モードを保留中**」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

  何らかの理由でデバイスが再起動すると、遅延更新プロセスが完了します。

  このアクティベーション・ルールは、サーバーおよびラック・スイッチでのみサポートされています。CMM と Flex スイッチは、この設定に関係なく即座にアクティブ化されます。

  ステータスが「**ファームウェア保守モードを保留中**」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

  遅延更新プロセスは、何らかの理由でデバイスが再起動すると (手動再起動を含む) 完了します。サーバーを再起動する必要がある場合は、時間制限はありません。

  XClarity Administrator では、遅延アクティベーションを使用して、最大 50 台のデバイスに更新を一度に適用できます。遅延アクティベーションを使用して 50 台を超えるデバイスに更新を適用しようとすると、残りのデバイスはキューに入れられます。更新するデバイスが「**ファームウェア保守モードを保留中**」状態になると、デバイスがキューから出ます。

  重要：

  – 更新ジョブ中に XClarity Administrator が再起動すると、更新ジョブがエラーになり、停止します。

  – XClarity Administrator が停止または到達不能なときに、「**ファームウェア保守モードを保留中**」状態のサーバーが再起動された場合、サーバーは BMU にブートしますが、XClarity Administrator は 60 秒後に BMU に接続できないため、システムの電源ステータスはベースボード管理コントローラーによって復元されます (電源がオフの場合はオフで、電源がオンの場合は再起動します)。
- **優先順位を設定したアクティベーション**。ベースボード管理コントローラーのファームウェア更新は即座にアクティブ化されます。その他のすべてのファームウェア更新は、次回にデバイスが再起動したときに有効になります。その後、更新操作が完了するまでの間、さらに何回か再起動が必要となります。このルールは、サーバーでのみサポートされています。

  ステータスが「ファームウェア保守モードを保留中」に変わるとイベントが発生し、サーバーの再起動が必要なときに通知されます。

注：有効にすると、Wake-on-LAN ブート・オプションが、サーバーの電源をオフにする XClarity Administrator の操作 (ネットワーク内に「Wake on Magic Packet」コマンドを発行する Wake-on-LAN クライアントがある場合はファームウェア更新など) によって中断されることがあります。

ステップ 8. **オプション**: ファームウェア・レベルが最新の場合でも選択したコンポーネントのファームウェアを更新するか、現在選択されたコンポーネントにインストールされているものより前のファームウェア更新を適用するには、「**強制更新**」を選択します。

注：以前のバージョンのファームウェアをデバイス・オプション、アダプター、下位レベルをサポートするドライブに適用することができます。下位レベルがサポートされているかどうかを判別するには、ハードウェアの資料を参照してください。

ステップ 9. **オプション**:前提条件となるファームウェアをインストールしたくない場合は、「**前提条件となるファームウェアをインストール**」をオフにします。デフォルトでは、前提条件となるファームウェアがインストールされます。

注：前提条件となるファームウェア更新に**遅延アクティベーション**または**優先順位を付けたアクティベーション**を使用すると、前提条件となるファームウェアをアクティブ化するためにサーバーを再起動する必要があります。最初の再起動後に**即時アクティベーション**を使用して残るファームウェアの更新がインストールされます。

ステップ 10. **オプション**: **即時アクティベーション** を選択した場合、**[メモリー・テスト]** を選択して、更新中にサーバーがリブートした場合に、ファームウェア更新の完了後にメモリー・テストを実行します。

このオプションは ThinkSystem v1 および v2 サーバー (ThinkSystem SR635、SR645、SR655、SR665 サーバーを除く) でサポートされます。

ステップ 11. 「**更新の実行**」をクリックして今すぐ更新するか、「**スケジュール**」を更新してこの更新を後で実行するようにスケジュールします。

必要な場合、管理対象デバイスで電源操作を実行できます。電源操作は、「**遅延アクティベーション**」が選択されていて、デバイスが「保守を保留中」状態で待機しているときに更新を続行したい場合に役立ちます。このページから管理対象デバイスで電源操作を実行するには、「**すべての操作**」 ➡ 「**電源操作**」をクリックし、以下のいずれかの電源操作をクリックします。

- **電源オン**
- **OS のシャットダウンと電源オフ**
- **電源オフ**
- **OS のシャットダウンと再起動**
- **再起動**

終了後

ファームウェア更新を適用する際、サーバーが保守モードに切り替わらない場合は、更新をもう一度適用してみてください。

更新が正常に終了しなかった場合、トラブルシューティングと修正処置については、XClarity Administrator オンライン・ドキュメントのファームウェア更新とリポジトリーの問題を参照してください。

「ファームウェア更新: 適用/アクティブ化」ページからは、以下の操作を実行できます。

- 「**すべての操作**」 ➡ 「**表示を CSV としてエクスポート**」をクリックして、各管理対象デバイスのファームウェアとコンプライアンス情報をエクスポートする。

  注：CSV ファイルには、現在のビューでフィルタリングされている情報のみが含められます。ビューから除外された情報と非表示列の情報は含められません。

- デバイスを選択して「**更新のキャンセル**」アイコン ( ) をクリックすることで、デバイスに適用する更新をキャンセルする。

注：キューにあって開始を待つファームウェア更新をキャンセルできます。更新プロセスの開始後は、保守モードへの変更やデバイスの再起動など、実際に更新を適用するタスク以外のタスクを更新プロセスが実行している途中に、ファームウェア更新をキャンセルできます。

- 「適用/アクティブ化」ページの「**ステータス**」列でファームウェア更新のステータスを直接確認する。
- ジョブ・ログから更新プロセスのステータスを監視する。Lenovo XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。

  ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

ファームウェア更新ジョブが完了したら、「**プロビジョニング**」 → 「**ファームウェア更新: 適用/アクティブ化**」をクリックして「ファームウェア更新: 適用/アクティブ化」ページに戻り、「**最新表示**」アイコン ( ) をクリックすることで、デバイスが適合していることを確認できます。各デバイスでアクティブな現在のファームウェア・バージョンが、「**インストール済みバージョン**」列に表示されます。

第 14 章　管理対象サーバーの Windows デバイス・ドライバーの更新

Windows の UpdateXpress System Packs (UXSPs) を使用して、デプロイ済み Windows オペレーティング・システムで OS デバイス・ドライバーを更新できます。

始める前に

OS デバイス・ドライバーの管理とデプロイ、および「Windows ドライバー更新」ページからの管理対象サーバーの電源操作の実行には、**lxc-os-admin**、**lxc-supervisor**、**lxc-admin** または **lxc-hw-admin** 権限が必要です。

XClarity Administrator では、ファームウェアの更新とデバイス・ドライバーの更新は別の処理であり、これらの処理に関連はありません。XClarity Administrator では、デバイス・ドライバーをファームウェアと同時に更新することをお勧めしますが、管理対象デバイスのファームウェアとデバイス・ドライバーの間のコンプライアンスは維持されません。

このタスクについて

Windows UpdateXpress System Packs (UXSPs) には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。

Windows Server 2012 R2 以降のデバイス・ドライバーのみサポートされます。XClarity Administrator では、Linux または VMware デバイス・ドライバーの更新はサポートされていません。

オペレーティング・システムのデプロイ時のデバイス・ドライバーのインストールについては、XClarity Administrator オンライン・ドキュメントのベア・メタル・サーバーへのオペレーティング・システムのインストールを参照してください。

手順

ステップ 1. **OS デバイス・ドライバー更新用の Windows Server の構成**

Lenovo XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行します。OS デバイス・ドライバーを更新する前に、WinRM サービスがターゲット・サーバーで正しく構成されている必要があります。 (OS デバイス・ドライバー更新用の Windows Server の構成を参照)。

ステップ 2. **OS デバイス・ドライバー・リポジトリーの管理**

*OS デバイス・ドライバー・リポジトリー*には、管理対象デバイスに適用できる使用可能な Windows デバイス・ドライバーとデバイス・ドライバー・パッケージのカタログが含まれます。

この*カタログ*には、Windows をサポートするすべての Lenovo サーバーで利用可能なすべての Windows UpdateXpress System Packs (UXSPs) とデバイス・ドライバーの更新に関する情報が含まれています。このカタログでは、デバイス・ドライバーの更新をデバイス・タイプ別に分類しています。カタログを最新の情報に更新すると、XClarity Administrator により提供中の UXSPs が Lenovo データセンターサポート Web サイト から取得され (メタデータ .xml および readme .txt ファイルを含む)、ファームウェア更新リポジトリーに保存されます。ペイロード・ファイル (.exe) がダウンロードされていません。カタログの更新について詳しくは、OS のデバイス・ドライバー・カタログの更新を参照してください。

リポジトリーで Windows UXSP をダウンロードまたはインポートできます。Windows UXSP には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。管理対象サーバーで Windows デバイス・ドライバーを更新するには、リポジトリーで UXSP が使用可能である必要があります。デバイス・ドライバーのダウンロードについて詳しくは、Windows デバイス・ドライバーのダウンロードを参照してください。

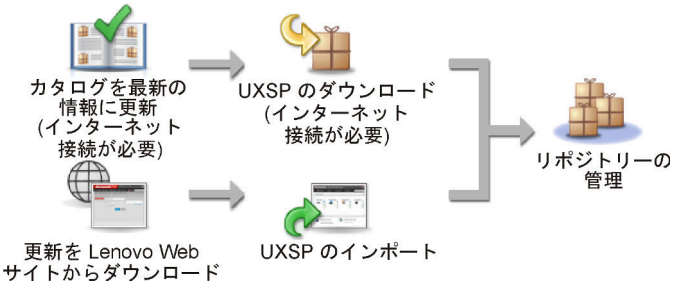
「Windows ドライバー更新のリポジトリー」ページの「個別更新」タブにある「ダウンロード状況」の列で、UXSP が OS デバイス・ドライバー・リポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

- **ダウンロード済み**。パッケージ全体または個々の更新がリポジトリーに保存されています。
- ***x*/*y* ダウンロード済み**。パッケージ内の一部の更新がリポジトリーに保存されています。括弧内の番号は、利用可能な更新数と、保存された更新数、または特定のデバイス・タイプの更新がないことを示します。
- **未ダウンロード**。パッケージ全体または個々の更新を使用できますが、リポジトリーに保存されていません。

注：「Windows ドライバー更新リポジトリー」ページから UXSP をダウンロードまたはインポートした場合、デバイス・ドライバーのみがダウンロードされ、リポジトリーに保存されます。ファームウェア更新は破棄されます。ファームウェア更新のダウンロードまたはインポートについて詳しくは、ファームウェア更新リポジトリーの管理 を参照してください。

カタログを更新して UXSPs をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていない場合、Web ブラウザーを使用して、XClarity Administrator ホストにネットワークでアクセス可能なワークステーションに UXSPs を手動でダウンロードできます。この UXSPs のダウンロードは、zip 形式のファイルで、ペイロード (.exe)、メタデータ (.xml)、変更履歴ファイル (.chg)、readme ファイル (.txt) を含めて、UXSP に対して必要なすべてのデバイス・ドライバー・ファイルが含まれます。

注：ファームウェア (fw) ファイルは不要であり、削除された旨のメッセージが表示されます。このプロセスを使用して更新されるのは Windows デバイス・ドライバーだけなので、これは正常です。



注意：

- インポートする前に UXSP の unzip を行わないでください。
- Windows UXSPs には、デバイス・ドライバーとファームウェア更新が含まれています。Windows UXSPs のファームウェア更新は、UXSPs がリポジトリーにインポートされるときに破棄され、警告メッセージが表示されます。デバイス・ドライバーのみがインポートされます。

ステップ 3. **OS デバイス・ドライバーの適用**

XClarity Administrator では、管理対象サーバーでデバイス・ドライバーが自動的に更新されません。デバイス・ドライバーを更新するには、選択されたサーバーでデバイス・ドライバーを手動で適用する必要があります。

注意：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、必ず以下の考慮事項を確認し、該当する前提条件となる操作を実行してください。

- サポートされていないデバイスを更新するように選択することはできません。
- 管理対象サーバーでデバイス・ドライバーを更新しようとする前に、デバイス・ドライバー更新の考慮事項を読んでください (OS デバイス・ドライバー更新の考慮事項を参照)。
- デプロイする UXSPs およびデバイス・ドライバーがリポジトリーに含まれていることを確認します (Windows デバイス・ドライバーのダウンロードを参照)。

  注：XClarity Administrator を最初にインストールしたときは、カタログとリポジトリーは空です。
- XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行できます。HTTPS がデフォルトです。HTTP を使用するには、「Windows ドライバーの更新: 適用」ページで、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**Windows ドライバーの更新に HTTPS を使用**」をオフにします。

  注意：HTTP を使用した場合、Windows ユーザー資格情報は、暗号化を*使用せずに*ネットワークで送信され、一般的なネットワーク・トラブルシューティング・ツールを使用して簡単に確認できます。

  重要：

  – ターゲット・サーバーの Windows リモート管理 (WinRM) が、XClarity Administrator で定義されている同じ設定 (HTTPS または HTTP) を使用するように構成されていることを確認します (OS デバイス・ドライバー更新用の Windows Server の構成を参照してください)。
  – ターゲット・サーバーの WinRM が基本認証で構成されていることを確認します。
  – HTTPS を使用している場合、ターゲット・サーバー上の WinRM が **allowUnencrypted=false** で構成されていることを確認します。
- ターゲット・サーバーで PowerShell がサポートされていることを確認します。
- デバイス・ドライバーを更新する前に、ターゲット・サーバーの電源がオンになっていることを確認します。サーバーの電源がオンになっていない場合は、ターゲット・サーバーを選択して、「**すべての操作**」 ➡ 「**電源操作**」 ➡ 「**電源オン**」 の順にクリックします。
- XClarity Administrator に、ホスト・オペレーティング・システムにアクセスするために必要な情報があることを確認します (XClarity Administrator オンライン・ドキュメントの管理対象サーバーのオペレーティング・システムへのアクセスの管理を参照)。
- OS デバイス・ドライバーを更新するときにドメイン・アカウントを使用する場合は、必要な構成ファイルを作成したことを確認してください (OS デバイス・ドライバー更新用のドメイン・アカウントの構成を参照)。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。実行中のジョブによってロックされている管理対象サーバーのデバイス・ドライバーは更新できません。別の更新ジョブがターゲット・サーバーで実行中の場合、この更新ジョブは、現在の更新ジョブが完了するまでキューにあります。アクティブ・ジョブのリストを表示するには、「**監視**」 ➡ 「**ジョブ**」をクリックします。

デバイス・ドライバーの更新について詳しくは、Windows デバイス・ドライバーの適用を参照してください。

OS デバイス・ドライバー更新の考慮事項

Lenovo XClarity Administrator を使用して管理対象デバイスの OS デバイス・ドライバーを更新する前に、以下の重要な考慮事項を確認してください。

注：デバイス・ドライバーの管理とデプロイ、および「Windows ドライバー更新」ページからの管理対象サーバーの電源操作の実行には、**lxc-os-admin**、**lxc-supervisor**、**lxc-admin** または **lxc-hw-admin** 権限が必要です。

ネットワークに関する考慮事項

- UpdateXpress System Packs (UXSPs) をダウンロードする前に、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必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントの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。
- XClarity Administrator から管理ネットワークおよびデータ・ネットワークにアクセスしてオペレーティング・システムにアクセスできる必要があります。
- XClarity Administrator が、XClarity Administrator のネットワーク・アクセスを構成したときに選択したネットワーク・インターフェース (Eth0 または Eth1) 経由でターゲット・サーバー (ベースボード管理コントローラーおよびサーバーのデータ・ネットワークの両方) と通信できる必要があります。また、インターフェースは IPv4 アドレスまたは IPv6 自動 ULA アドレスを使用して構成されている必要があります。

  オペレーティング・システム・デプロイメントに使用するインターフェースを指定するには、ネットワーク・アクセスの構成を参照)。

  オペレーティング・システム・デプロイメント・ネットワークおよびインターフェースについて詳しくは、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。
- IP アドレスはホスト・オペレーティング・システムに固有である必要があります。
- XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行できます。HTTPS がデフォルトです。HTTP を使用するには、「Windows ドライバーの更新: 適用」ページで、「**すべての操作**」 ➡ 「**共通設定**」をクリックし、「**Windows ドライバーの更新に HTTPS を使用**」をオフにします。

  注意：HTTP を使用した場合、Windows ユーザー資格情報は、暗号化を*使用せずに*ネットワークで送信され、一般的なネットワーク・トラブルシューティング・ツールを使用して簡単に確認できます。

管理対象デバイスに関する考慮事項

- ThinkAgile、ThinkSystem SR635、および ThinkSystemSR655 サーバーの場合、Windows デバイス・ドライバーの更新はサポートされていません。
- ThinkSystem、Lenovo System x および Lenovo Flex System サーバーのみがサポートされます。
- XClarity Administrator は管理コントローラーとオペレーティング・システムの間の関係を検証しません。サーバーの電源のオンオフにはベースボード管理コントローラーが使用されます。
- LAN-over-USB インターフェースが有効であることを確認します。LAN over USB は、OS デバイス・ドライバーを更新する場合に使用されます。

オペレーティング・システムおよびデバイス・ドライバーに関する考慮事項

- 以下のオペレーティング・システムでは、デバイス・ドライバーを更新できます。
  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

注：XClarity Administrator は、XClarity Administrator バージョンのリリース時に、Microsoft によってサポートされている Windows バージョンのみを使用してテストされています。

- ターゲット・サーバーで HTTPS 用に Windows Remote Management (WinRM) が構成されている必要があります (OS デバイス・ドライバー更新用の Windows Server の構成を参照)。
- ターゲット・サーバーで PowerShell がサポートされている必要があります。
- OS IP アドレスおよび資格情報を含む、ターゲット・サーバーでホスト・オペレーティング・システムにアクセスするために必要な情報を指定する必要があります (XClarity Administrator オンライン・ドキュメントの管理対象サーバーのオペレーティング・システムへのアクセスの管理を参照)。管理者権限を持つユーザー・アカウントの資格情報を指定する必要があります。
- XClarity Administrator はコンプライアンスに違反しているデバイス・ドライバーのみを更新します。デバイス・ドライバーは、サーバー上のバージョンが選択された UXSP のバージョンより古い場合にコンプライアンス違反になります。選択された UXSP のバージョンと同じかそれ以降のデバイス・ドライバーはスキップされます。
- デバイス・ドライバーのコンプライアンスはハードウェアが存在する場合のみ正確です。ハードウェアが存在しない場合でもデバイス・ドライバーはサーバーに適用されます。不足しているハードウェアがサーバーに追加されると、Windows は最新バージョンをロードします。
- System x サーバーでは、XClarity Administrator に用意されている事前定義済みデバイス・ドライバーの一部がサポートされていません。これらのサーバーにデバイス・ドライバーをデプロイするには、必要なデバイス・ドライバーのみを含むカスタム・プロファイルを作成します。

OS デバイス・ドライバー・リポジトリーの管理

*OS デバイス・ドライバー・リポジトリー*には、カタログおよびダウンロード済み Windows デバイス・ドライバーが含まれています。

このタスクについて

この*カタログ*には、Windows をサポートするすべての Lenovo サーバーで利用可能なすべての Windows UpdateXpress System Packs (UXSPs) とデバイス・ドライバーの更新に関する情報が含まれています。このカタログでは、デバイス・ドライバーの更新をデバイス・タイプ別に分類しています。カタログを最新の情報に更新すると、XClarity Administrator により提供中の UXSPs が Lenovo データセンターサポート Web サイトから取得され (メタデータ .xml および readme .txt ファイルを含む)、ファームウェア更新リポジトリーに保存されます。ペイロード・ファイル (.exe) がダウンロードされていません。カタログの更新について詳しくは、OS のデバイス・ドライバー・カタログの更新を参照してください。

Windows UpdateXpress System Packs (UXSPs) には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。 リポジトリーで Windows UXSP をダウンロードまたはインポートできます。Windows UXSP には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。管理対象サーバーで Windows デバイス・ドライバーを更新するには、リポジトリーで UXSP が使用可能である必要があります。デバイス・ドライバーのダウンロードについて詳しくは、Windows デバイス・ドライバーのダウンロードを参照してください。

カタログを更新して UXSPs をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。インターネットに接続されていない場合、Web ブラウザーを使用して、XClarity Administrator ホストにネットワークでアクセス可能なワークステーションに UXSPs を手動でダウンロードできます。この UXSPs のダウンロードは、zip 形式のファイルで、ペイロード (.exe)、メタデータ (.xml)、変更履歴ファイル (.chg)、readme ファイル (.txt) を含めて、UXSP に対して必要なすべてのデバイス・ドライバー・ファイルが含まれます。

UXSP がリポジトリーにダウンロードされた後は、パックの各デバイス・ドライバーに関する情報が「Windows ドライバーの更新リポジトリー」ページに追加されます。これには、リリース日、サイズ、

および重大度が含まれます。重大度は、更新適用の影響と必要性を示すので、運用環境への影響を評価するのに役立ちます。

- 「**初回リリース**」。これは、デバイス・ドライバーの初回リリースです。
- 「**重大**」。このデバイス・ドライバーにはデータ破損、セキュリティー、または安定性の問題の緊急な修正が含まれています。
- 「**推奨**」。このデバイス・ドライバーは、発生する可能性がある問題に対する重要な修正が含まれています。
- 「**非クリティカル**」。このデバイス・ドライバーには、マイナーな修正、パフォーマンス強化、およびテキストの変更が含まれています。

注：

- 重大度は、以前にリリースされたデバイス・ドライバーのバージョンに関連しています。例えば、インストール済みのデバイス・ドライバーが v1.01 で、更新 v1.02 が「クリティカル」であり、更新 v1.03 が「推奨」である場合、更新は累積的である (v1.03 は v1.02 のクリティカルな問題を含む) ので、1.02 から 1.03 の更新は推奨されるのに対し、v1.01 から v1.03 への更新はクリティカルであることを意味します。
- 特定のマシン・タイプに対してだけ更新がクリティカル/推奨されている特別な場合もあります。追加情報については、リリース情報を参照してください。

手順

リポジトリー内で使用可能な UXSPs およびデバイス・ドライバーを表示するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**Windows ドライバー更新: リポジトリー**」の順にクリックします。「Windows ドライバー更新リポジトリー」ページに、使用可能な UXSPs のリストが、デバイス・タイプごとに整理されて表示されます。

ステップ 2. サーバー・タイプを展開し、そのサーバー・タイプで使用可能な UXSPs を展開して、そのサーバー・タイプで使用できるデバイス・ドライバーを一覧表示します。

テーブル列をソートしたり、「**すべて展開表示**」アイコン () および「**すべて縮小表示**」アイコン () をクリックして、特定のデバイス・ドライバーを見つけやすくします。さらに、「**表示**」メニューでオプションを選択して、特定の時間を経過したデバイス・ドライバー、すべてのサーバー・タイプまたは管理対象サーバー・タイプのみのデバイス・ドライバーを表示したり、「**フィルター**」フィールドにテキストを入力して、表示されたサーバー・タイプおよびデバイス・ドライバーのリストをフィルタリングすることもできます。

このページでは、以下の操作を実行できます。

- 使用可能な UXSPs に関する最新情報を取得する。「**カタログを最新の情報に更新**」をクリックします。

  この情報の取得には数分かかることがあります。詳しくは、OS のデバイス・ドライバー・カタログの更新を参照してください。
- XClarity Administrator を使用して UXSPs およびデバイス・ドライバーをダウンロードする。カタログを最新表示にして「**ダウンロード**」アイコン ( ) をクリックします。UXSPs およびデバイス・ドライバーがダウンロードされてリポジトリーに追加されると、ステータスが「ダウンロード済み」に変わります。

  UXSPs およびデバイス・ドライバーのダウンロードについて詳しくは、Windows デバイス・ドライバーのダウンロードを参照してください。
- Web からワークステーションに手動でダウンロードした UXSPs、または XClarity Administrator からエクスポートしたデバイス・ドライバーをインポートします (Windows デバイス・ドライバーのダウンロードを参照)。
- 現在進行中の選択したダウンロードを停止する。「**ダウンロードのキャンセル**」アイコン ( ) をクリックします。
- 選択した UXSPs または個別のデバイス・ドライバーをリポジトリーから削除する。「**削除**」アイコン ( ) をクリックします。

OS のデバイス・ドライバー・カタログの更新

OS デバイス・ドライバー・カタログには、Windows デバイス・ドライバーの更新をサポートするすべての Lenovo サーバーで利用できるすべての Windows UpdateXpress System Packs (UXSPs) およびデバイス・ドライバーの更新に関する情報が含まれています。

始める前に

Lenovo XClarity Administrator がインターネットに接続されていることを確認します。

このタスクについて

カタログを最新の情報に更新すると、XClarity Administrator により提供中の UXSPs が Lenovo データセンターサポート Web サイト から取得され (メタデータ .xml および readme .txt ファイルを含む)、ファームウェア更新リポジトリーに保存されます。ペイロード・ファイル (.exe) がダウンロードされていません。 管理対象サーバーのデバイス・ドライバーを更新する前に、必要な UXSP および OS デバイス・ドライバー・ペイロードをダウンロードする必要があります。デバイス・ドライバーのダウンロードについて詳しくは、Windows デバイス・ドライバーのダウンロードを参照してください。

注：カタログを最新の情報に更新するには数分かかることがあります。

手順

カタログを最新表示にするには、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、「**プロビジョニング**」 ➡ 「**Windows ドライバー更新: リポジトリー**」 をクリックして、「Windows ドライバー更新: リポジトリー」ページを表示します。

ステップ 2. 「**カタログを最新の情報に更新**」をクリックし、次のいずれかのオプションをクリックして、使用可能な最新の UXSPs に関する情報を取得します。

- 「**選択した情報の更新 - 最新のみ**」。選択したサーバーでのみ使用可能な最新の UXSP バージョンの情報を取得します。
- 「**すべて更新 - 最新のみ**」。サポートされているすべてのサーバーの最新バージョンの UXSP の情報を取得します。
- 「**選択した情報の更新**」。選択したサーバーでのみ使用可能なすべての UXSP バージョンの情報を取得します。
- 「**すべて更新**」。すべてのサポートされているサーバーで使用可能なすべての UXSP バージョンの情報を取得します。

ステップ 3. 「**カタログを最新の情報に更新**」をクリックして今すぐ更新するか、「**スケジュール**」をクリックしてこの更新を後で実行するようにスケジュールします。

Windows デバイス・ドライバーのダウンロード

Windows UpdateXpress System Packs (UXSPs) には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。 リポジトリーで Windows UXSP をダウンロードまたはインポートできます。Windows UXSP には、サポートされている Windows バージョンおよび Windows をサポートする Lenovo サーバーの Windows デバイス・ドライバーが含まれています。管理対象サーバーで Windows デバイス・ドライバーを更新するには、リポジトリーで UXSP が使用可能である必要があります。

始める前に

UpdateXpress System Packs (UXSPs) をダウンロードする前に、必要なポートとインターネット・アドレスがすべて使用可能になっていることを確認します。詳しくは、XClarity Administrator オンライン・ドキュメントの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。

XClarity Administrator を使用して UXSPs をダウンロードするには、XClarity Administrator がインターネットに接続されていることを確認します。

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、。

このタスクについて

カタログを更新して UXSPs をダウンロードするには、XClarity Administrator がインターネットに接続されている必要があります。XClarity Administrator がインターネットに接続されていない場合は、XClarity

Administrator ホストにネットワーク・アクセスできるワークステーションで Web ブラウザーを使用してファイルを手動でダウンロードした後、更新をファームウェア更新リポジトリーにインポートできます。

「Windows ドライバー更新リポジトリー」ページの「**ダウンロード・ステータス**」列で、UXSPs がリポジトリーに保存されているかどうかを調べることができます。この列には、以下の値が含まれます。

- **ダウンロード済み**。UXSP のすべてのデバイス・ドライバー、または個々のデバイス・ドライバーは、リポジトリーにダウンロードされます。
- ***x*/*y* ダウンロード済み**。リポジトリーにダウンロードされる UXSP のデバイス・ドライバーは一部でありすべてではありません。括弧内の数字は、使用可能なデバイス・ドライバーの数とダウンロードされたデバイス・ドライバーの数を示しています。
- **未ダウンロード**。UXSP または個々のデバイス・ドライバーは Lenovo サポート・サイトに掲載されていますが、リポジトリーにダウンロードされません。

UXSPs およびデバイス・ドライバーに使用できる空き容量が全容量の 50% 以上の場合は、「Windows ドライバー更新リポジトリー」ページにメッセージが表示されます。リポジトリーが 85% 以上埋まると、別のメッセージがページに表示されます。リポジトリー内の使用する容量を削減するには、ターゲット・ファイルを選択して「**削除**」アイコン ( ) をクリックすることで不要なファイルを削除できます。詳しくは、ディスク・スペースの管理を参照してください。

注意：Windows UXSPs には、デバイス・ドライバーとファームウェア更新が含まれています。Windows UXSPs のファームウェア更新は、UXSPs がリポジトリーにインポートされるときに破棄され、警告メッセージが表示されます。デバイス・ドライバーのみがインポートされます。

手順

UXSPs および特定のデバイス・ドライバーをダウンロードするには、以下のいずれかの手順を実行します。

- XClarity Administrator がインターネットに接続されている場合:
  1. XClarity Administrator メニュー・バーで、「**プロビジョニング**」 → 「**Windows ドライバー更新: リポジトリー**」 をクリックして、「Windows ドライバー更新: リポジトリー」ページを表示します。
  2. 「**カタログを最新の情報に更新**」をクリックし、次のいずれかのオプションをクリックして、使用可能な最新の UXSPs に関する情報を取得します。
     - 「**選択した情報の更新 - 最新のみ**」。選択したサーバーでのみ使用可能な最新の UXSP バージョンの情報を取得します。
     - 「**すべて更新 - 最新のみ**」。サポートされているすべてのサーバーの最新バージョンの UXSP の情報を取得します。
     - 「**選択した情報の更新**」。選択したサーバーでのみ使用可能なすべての UXSP バージョンの情報を取得します。
     - 「**すべて更新**」。すべてのサポートされているサーバーで使用可能なすべての UXSP バージョンの情報を取得します。

     注：カタログを最新の情報に更新するには数分かかることがあります。
  3. 使用可能な UXSPs のリストを表示するには、サーバー・タイプを展開します。UXSP を展開し、使用可能なデバイス・ドライバーのリストを表示します。

4. ダウンロードするターゲット UXSPs とデバイス・ドライバーを 1 つ以上選択します。
5. 「**選択をダウンロード**」アイコン ( ) をクリックします。
6. 「**ダウンロード**」をクリックして今すぐダウンロードするか、「**スケジュール**」をクリックしてこのダウンロードを後で実行するようにスケジュールします。

   UXSPs のダウンロードには数分かかる場合があります。UXSPs およびデバイス・ドライバーがダウンロードされてリポジトリーに保存されると、カタログの行が強調表示され、「**ダウンロード・ステータス**」列が「ダウンロード済み」に変わります。

   ジョブ・ログからダウンロード・プロセスのステータスを監視できます。XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

- XClarity Administrator がインターネットに接続されて*いない*場合:
  1. XClarity Administrator ホストにネットワーク接続できるワークステーションに、Lenovo データセンターサポート Web サイトから UXSPs をダウンロードします。
  2. XClarity Administrator メニュー・バーで、「**プロビジョニング**」 → 「**Windows ドライバー更新: リポジトリー**」 をクリックして、「Windows ドライバー更新: リポジトリー」ページを表示します。
  3. 「**インポート**」アイコン ( ) をクリックします。
  4. 「**ファイルの選択**」をクリックし、ワークステーション上の UXSP の場所を参照します。
  5. UXSP .zip ファイルを選択し (インポートの前に zip ファイルの unzip は行わないでください)、「**開く**」をクリックします。

     UXSP.zip ファイルには、メタデータ・ファイル (.xml)、ペイロード (.exe)、変更履歴ファイル (.chg)、および readme ファイル (.txt) が含まれています。
  6. 「**インポート**」をクリックします。

     ジョブ・ログからインポート・プロセスのステータスを監視できます。XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

終了後

このページでは、選択した UXSPs に対して以下の操作を実行できます。

- 現在進行中のダウンロードをキャンセルする。「**ダウンロードのキャンセル**」アイコン () をクリックします。
- UXSP に関連付けられたすべてのファイルを削除する。「**削除**」アイコン () をクリックします。

OS デバイス・ドライバー更新用の Windows Server の構成

Lenovo XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行します。OS デバイス・ドライバーを更新する前に、WinRM サービスがターゲット・サーバーで正しく構成されている必要があります。

始める前に

必要なポートが使用できる必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントの 利用可能なポートを参照してください。

OS デバイス・ドライバーを更新する前に Windows Server を構成する方法の詳細については、XClarity Administrator: OS デバイス・ドライバーの更新の準備 (ホワイト・ペーパー)を参照してください。

手順

OS デバイス・ドライバーの更新をサポートするために Windows サーバーを構成するには、以下のステップを実行します。

- **HTTPS の場合**
  1. ターゲット Windows システムそれぞれで、サーバー証明書に署名してインストールします。

     重要：証明書には、以下の情報を含める必要があります。

     – サブジェクトで、ドメイン・コンポーネントが設定されていることを確認します (たとえば、DC = labs、DC = com、DC = company など)。

     – サブジェクト代替名では、DNS 名とホスト IP アドレスが設定されていることを確認します (たとえば、DNS Name=node1325C554A6F.labs.company.com、IP Address=10.245.43.149 など)。
  2. 管理コマンド・プロンプトから次のコマンドのいずれかを実行し、推奨される構成の変更を確認して、リモート管理コマンドおよびデータを HTTPS 接続経由で構成します。

     –
     ```
     winrm quickconfig -transport:https
     ```

     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     WinRM のドキュメントに従って WinRM HTTPS リスナーを手動で設定する場合については、HTTPS Web ページ WinRM を構成する方法 を参照してください。
  3. ローカル Windows ユーザーの基本認証を有効にするには、管理コマンド・プロンプトから次のコマンドを実行します。
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  4. コンプライアンス検査およびドライバー更新の実行時に、タイムアウトや WinRM 要求エラーの送信を回避するには、管理コマンド・プロンプトから次のコマンドを実行して、WinRM 応答タイムアウトのデフォルト値を大きくします。値 280000 が推奨されます。詳しくは、Windows Remote Management Web ページのインストールおよび構成 を参照してください。
     ```
     winrm set winrm/config @{MaxTimeoutms="280000"}
     ```

5. WinRM HTTPS リスナーに対して構成されているポートをご使用のファイアウォールで開きます。デフォルトの HTTPS ポートは 5986 です。以下に例を示します。
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow protocol=TCP localport=5986
   ```
6. HTTPS リスナーを使用している場合は、次の手順を実行して、証明書を XClarity Administrator 信頼ストアに追加します。信頼ストアに証明書を追加することにより、XClarity Administrator が接続先の WinRM HTTPS リスナーを信頼します。Windows Remote Management サービスで信頼する必要がある追加の証明書パスがあれば、以下のステップを繰り返します。
   a. ターゲット Windows システムに対してサーバー証明書の署名に使用する証明機関ルート証明書を識別して収集します。CA ルート証明書にアクセスできない場合は、サーバー証明書自体または証明書パス内の別の証明書を収集します。
   b. XClarity Administrator メニュー・バーで、「**管理**」 ➡ 「**セキュリティー**」をクリックして、「セキュリティー」ページを表示します。
   c. 「証明書の管理」セクションで「**トラステッド証明書**」をクリックします。
   d. 「**作成**」アイコン ( ) をクリックして、「証明書の追加」ダイアログを表示します。
   e. ステップ 1 で収集した証明書ファイルを参照するか、テキスト・ボックスに証明書ファイルの内容をコピーして貼り付けます。
   f. 「**作成**」をクリックします。
7. WinRM リスナーがターゲット Windows システムで実行中になると、XClarity Administrator がこれらのシステムに接続し、デバイス・ドライバー更新を実行できます。

- **HTTP 用**
  1. 管理コマンド・プロンプトから次のコマンドを実行し、推奨される構成の変更を確認して、リモート管理コマンドおよびデータを HTTP 接続経由で構成します。
     ```
     winrm quickconfig
     ```
  2. ローカル Windows ユーザーの基本認証を有効にするには、管理コマンド・プロンプトから次のコマンドを実行します。
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. 管理コマンド・プロンプトから、次のコマンドを実行して、このシステムで更新コマンドに十分なメモリーを割り当てます。
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. 管理コマンド・プロンプトから、次のコマンドを実行して、暗号化されていないデータを許可します。
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. WinRM HTTP リスナーに対して構成されているポートをご使用のファイアウォールで開きます。デフォルトの HTTPS ポートは 5985 です。以下に例を示します。
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow protocol=TCP localport=5985
     ```

  WinRM リスナーがターゲット Windows システムで実行中になると、XClarity Administrator がこれらのシステムに接続し、デバイス・ドライバー更新を実行できます。

OS デバイス・ドライバー更新用のドメイン・アカウントの構成

ドメイン・アカウントを使用して、ドメイン・コントローラーで権限を簡単に管理できます。OS デバイス・ドライバーを更新するときにドメイン・アカウントを使用するには、ドメイン・アカウントを構成する必要があります。

始める前に

ドメイン・アカウントを構成する前に、管理対象の Windows サーバーがドメイン・ネットワーク内にあることを確認します。

Lenovo XClarity Administrator で Windows ユーザー・アカウントを追加する場合は、USER@DOMAIN 形式を使用します。DOMAIN/USER 形式はサポートされていません。

手順

ドメイン・アカウントを構成するには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**Windows ドライバー更新: 適用**」の順にクリックします。「Windows ドライバー更新: 適用」ページが表示されます。

ステップ 2. 「**すべての操作**」 → 「**ドメイン・アカウントの管理**」をクリックします。「ドメイン・アカウント」ページが表示されます。

ステップ 3. ドメイン・アカウントのレルムを追加するには、「**作成**」アイコン ( ) をクリックします。「レルムの作成」ダイアログが表示されます。

ステップ 4. レルムの名前と 1 つ以上の鍵配布センターのホスト名を指定します。別のホスト名を追加するには「**追加**」アイコン ( ) を使用し、ホスト名を削除するには「**削除**」アイコン ( ) を使用します。

ステップ 5. 「**OK**」をクリックして、レルムを保存します。

ステップ 6. 「ドメイン・アカウント」ページで、デフォルトで使用するレルムをオプションで選択します。

ステップ 7. 「**保存**」をクリックして、構成を保存します。

終了後

「ドメイン・アカウントの構成」ページから、以下の操作を実行できます。

- 「**編集**」アイコン ( ) をクリックして、選択したレルムを変更します。
- 選択したレルムを削除するには、「**削除**」アイコン ( ) をクリックします。

共通 Windows デバイス・ドライバー更新設定の構成

共通設定は、Windows デバイス・ドライバー更新が適用される際はデフォルト設定となります。

このタスクについて

「共通設定」ページでは、以下の設定を構成できます。

- Windows ドライバー更新に HTTPS を使用する
- 取り付け済みのハードウェアのデバイス・ドライバーを表示

手順

すべてのサーバーに使用される共通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 のメニュー・バーで、「**プロビジョニング**」 → 「**Windows ドライバー更新: 適用**」の順にクリックします。「Windows ドライバー更新: 適用」ページが表示されます。

ステップ 2. 「**すべての操作**」 → 「**共通設定**」の順にクリックして、「共通設定: Windows ドライバー更新の適用」ダイアログを表示します。

ステップ 3. 任意で以下のオプションを選択します。

- 「**Windows ドライバー更新に HTTPS を使用する**」を選択して、HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用すると、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行できます。HTTPS がデフォルトです。

  HTTP を使用するには、これをクリアします。

  注意：HTTP を使用した場合、Windows ユーザー資格情報は、暗号化を*使用せずに*ネットワークで送信され、一般的なネットワーク・トラブルシューティング・ツールを使用して簡単に確認できます。
- 「**取り付けられたハードウェアのデバイス・ドライバーの表示**」を選択すると、管理対象ハードウェアのデバイス・ドライバーのみを表示します。

  この設定をクリアすると、すべてのインポートされた UpdateXpress System Packs (UXSPs) のすべてのデバイス・ドライバーがリストされます。

  重要：このオプションを選択した後、「Windows ドライバーの更新: 適用」ページから「**コンプライアンスの確認**」アイコン ( ) をクリックしてコンプライアンス・チェックを実行する必要があります。

ステップ 4. 「OK」をクリックして、ダイアログを閉じます。

Windows デバイス・ドライバーの適用

Windows を実行する管理対象サーバーにデバイス・ドライバーを適用できます。

始める前に

- Lenovo XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行します。OS デバイス・ドライバーを更新する前に、WinRM サービスがターゲット・サーバーで正しく構成されている必要があります。 (OS デバイス・ドライバー更新用の Windows Server の構成を参照)。
- サポートされていないデバイスを更新するように選択することはできません。
- 管理対象サーバーでデバイス・ドライバーを更新しようとする前に、デバイス・ドライバー更新の考慮事項を読んでください (OS デバイス・ドライバー更新の考慮事項を参照)。
- デプロイする UXSPs およびデバイス・ドライバーがリポジトリーに含まれていることを確認します (Windows デバイス・ドライバーのダウンロードを参照)。

  注：XClarity Administrator を最初にインストールしたときは、カタログとリポジトリーは空です。
- XClarity Administrator は HTTPS または HTTP 経由でリッスンする Windows Remote Management サービス (WinRM) を使用して、ターゲットの Windows システムでデバイス・ドライバー更新のコマンドを実行できます。HTTPS がデフォルトです。HTTP を使用するには、「Windows ドライバーの更新:

適用」ページで、「**すべての操作**」 ➞ 「**共通設定**」をクリックし、「**Windows ドライバーの更新に HTTPS を使用**」をオフにします。

注意：HTTP を使用した場合、Windows ユーザー資格情報は、暗号化を*使用せずに*ネットワークで送信され、一般的なネットワーク・トラブルシューティング・ツールを使用して簡単に確認できます。

重要：

- ターゲット・サーバーの Windows リモート管理 (WinRM) が、XClarity Administrator で定義されている同じ設定 (HTTPS または HTTP) を使用するように構成されていることを確認します (OS デバイス・ドライバー更新用の Windows Server の構成を参照してください)。
- ターゲット・サーバーの WinRM が基本認証で構成されていることを確認します。
- HTTPS を使用している場合、ターゲット・サーバー上の WinRM が **allowUnencrypted=false** で構成されていることを確認します。

- ターゲット・サーバーで PowerShell がサポートされていることを確認します。
- デバイス・ドライバーを更新する前に、ターゲット・サーバーの電源がオンになっていることを確認します。サーバーの電源がオンになっていない場合は、ターゲット・サーバーを選択して、「**すべての操作**」 ➞ 「**電源操作**」 ➞ 「**電源オン**」 の順にクリックします。
- XClarity Administrator に、ホスト・オペレーティング・システムにアクセスするために必要な情報があることを確認します (XClarity Administrator オンライン・ドキュメントの管理対象サーバーのオペレーティング・システムへのアクセスの管理を参照)。
- OS デバイス・ドライバーを更新するときにドメイン・アカウントを使用する場合は、必要な構成ファイルを作成したことを確認してください (OS デバイス・ドライバー更新用のドメイン・アカウントの構成を参照)。
- ターゲット・サーバーで現在実行されているジョブがないことを確認します。実行中のジョブによってロックされている管理対象サーバーのデバイス・ドライバーは更新できません。別の更新ジョブがターゲット・サーバーで実行中の場合、この更新ジョブは、現在の更新ジョブが完了するまでキューにあります。アクティブ・ジョブのリストを表示するには、「**監視**」 ➞ 「**ジョブ**」をクリックします。

このタスクについて

XClarity Administrator はコンプライアンスに違反しているデバイス・ドライバーのみを更新します。デバイス・ドライバーは、サーバー上のバージョンが選択された UXSP のバージョンより古い場合にコンプライアンス違反になります。選択された UXSP のバージョンと同じかそれ以降のデバイス・ドライバーはスキップされます。

手順

管理対象サーバーに Windows デバイス・ドライバーを適用するには、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、「**プロビジョニング**」 ➞ 「**Windows ドライバー更新: 適用**」をクリックして、「Windows ドライバー更新: 適用」ページを表示します。

重要：

- ターゲット・サーバーでデバイス・ドライバーを検出してコンプライアンスを判別するには、ターゲット・サーバーを選択し、コンプライアンス・チェックを実行する必要があります。初めてコンプライアンス・チェックを実行すると、行を展開してターゲット・サーバー上のデバイス・ドライバーのリストを表示できます。
- 「**Windows システム**」列は、ホスト名またはホスト・オペレーティング・システムの IP アドレスを識別します。
- 「**サーバー**」列は、管理対象サーバーの名前と IP アドレスを識別します。

ステップ 2. 1 つ以上のターゲット・サーバーとデバイス・ドライバーを選択します。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されるサーバーのリストを絞り込むこともできます。

ヒント:

- 特定のオペレーティング・システムのすべてのデバイス・ドライバーを更新することも、オペレーティング・システムを展開して特定のデバイスのみを更新することもできます。
- 「**更新ステータス**」列には、各サーバーの認証ステータスと各デバイス・ドライバーの更新ステータスが表示されます。
- 「**OS 資格情報**」列には、オペレーティング・システムへの認証に使用される、保存された資格情報が表示されます (例:「901 – company\USER1」)。

  ターゲット・サーバー上のホスト・オペレーティング・システムに OS 資格情報が定義されていない場合は、「OS 資格情報の編集」ダイアログが表示されます。単一のターゲット・サーバーの場合は、この操作に使用するユーザー名とパスワードを指定します。複数のターゲット・サーバーの場合は、各サーバーに使用する保管された資格情報を選択します。その後、「**保存**」をクリックします。

  注:「OS 資格情報の編集」ダイアログで選択する OS 資格情報がホスト・オペレーティング・システムに保存されていません。OS 資格情報を保存するには、管理対象サーバーのオペレーティング・システムへのアクセスの管理を参照してください。

ステップ 3. 「**認証の確認**」アイコン () をクリックして、認証と前提条件の確認を実行します。

XClarity Administrator は「**OS 資格情報**」列に記載されている保存された資格情報を使用してホスト・オペレーティング・システムに接続し、OS バージョンを判別して WinRM が有効になっていることを確認し、その他の前提条件の確認を実行してから、ホスト OS から切断します。

ホスト・オペレーティング・システム用に保存された資格情報の変更については、XClarity Administrator オンライン・ドキュメントの管理対象サーバーのオペレーティング・システムへのアクセスの管理を参照してください。

ステップ 4. ターゲット・サーバーごとに、「**コンプライアンス・ターゲット**」列から、デバイス・ドライバーの更新に使用する UXSP を選択します。

ステップ 5. ターゲット・サーバーをもう一度を選択し、「**コンプライアンスの確認**」アイコン () をクリックして、各デバイス・ドライバーのコンプライアンスを検証します。

コンプライアンス・チェックによって、「**インストール済みドライバー・バージョン**」列のコンプライアンス・ステータスが更新されます。この列には、サーバーとインストール済みバージョン全体のコンプライアンス・ステータスと、割り当てられた UXSP に対する各デバイス・ドライバーのコンプライアンス・ステータスが表示されます。

- **適合**。インストール済みデバイス・ドライバーは、割り当てられた UXSP と等しいかそれ以降のバージョンです。
- **非適合**。インストール済みデバイス・ドライバーは、割り当てられた UXSP より前のバージョンです。リンクをクリックすると非適合に関する詳細情報を取得できます。

注：デバイス・ドライバーのコンプライアンスはハードウェアが存在する場合のみ正確です。ハードウェアが存在しない場合でもデバイス・ドライバーはサーバーに適用されます。不足しているハードウェアがサーバーに追加されると、Windows は最新バージョンをロードします。

ステップ 6. 「**更新の実行**」アイコン () をクリックします。

ステップ 7. 以下の更新ルールのいずれかを選択します。

- **エラーですべての更新を停止**。ターゲット・デバイスのデバイス・ドライバーのいずれかの更新中にエラーが発生した場合、現在のデバイス・ドライバーの更新ジョブのすべてのターゲット・デバイスで更新プロセスが停止します。この場合、ターゲット・デバイスの UXSP のデバイス・ドライバーの更新はいずれも適用されません。すべてのターゲット・デバイスにインストールされている現在のデバイス・ドライバーが引き続き有効になります。
- **エラーで続行**。ターゲット・デバイス内のいずれかのデバイス・ドライバーの更新中にエラーが発生した場合、その特定のデバイスのデバイス・ドライバーは更新プロセスにより更新されません。ただし、更新プロセスはデバイス内の他のデバイス・ドライバーの更新を続行し、現在のデバイス・ドライバー更新ジョブに含まれる他のすべてのターゲット・デバイスの更新を続行します。
- **エラーで次のシステムに進む**。デバイス内のいずれかのデバイス・ドライバーの更新中にエラーが発生した場合、更新プロセスがその特定のデバイスのデバイス・ドライバーの更新試行をすべて停止するため、そのデバイスにインストールされた現在のデバイス・ドライバーが有効なままになります。更新プロセスは、現在のデバイス・ドライバー更新ジョブに含まれる他のすべてのデバイスの更新を続行します。

ステップ 8. 「**更新の実行**」をクリックして今すぐ更新するか、「**スケジュール**」を更新してこの更新を後で実行するようにスケジュールします。

終了後

更新を適用する際、ターゲット・サーバーが保守モードに切り替わらない場合は、更新をもう一度適用してみてください。

更新が正常に終了しなかった場合、トラブルシューティングと修正処置については、OS デバイス・ドライバー更新の考慮事項を参照してください。

「Windows ドライバー更新: 適用」ページからは、以下の操作を実行できます。

- 「適用」ページの「**更新ステータス**」列でデバイス・ドライバー更新のステータスを直接確認する。
- ジョブ・ログからデバイス・ドライバー更新のステータスを監視する。XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。

  ジョブ・ログについて詳しくは、XClarity Administrator オンライン・ドキュメントのジョブの監視。

更新ジョブが完了すると、「Windows ドライバー更新: 適用」ページでデバイスが適合していることを確認できます。各デバイスでアクティブな現在のドライバー・バージョンが、「**インストール済みドライバー・バージョン**」列に表示されます。

第 15 章　ベア・メタル・サーバーへのオペレーティング・システムのインストール

Lenovo XClarity Administrator を使用すると、OS イメージ・リポジトリー を管理し、最大 28 台のベア・メタル・サーバーにオペレーティング・システム・イメージを同時にデプロイできます。

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

始める前に

90 日間の無料試用期間の経過後も、引き続きハードウェアの管理や監視に XClarity Administrator を無料で使用できます。ただし、OS デプロイメント機能の使用を継続するには、XClarity Administrator の高度な機能をサポートする各管理対象サーバー向けの全機能有効化ライセンスを購入する必要があります。Lenovo XClarity Pro は、サービスおよびサポートに資格を提供し、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。詳しくは、XClarity Administrator オンライン・ドキュメントの全機能有効化ライセンスのインストールを参照してください。

このタスクについて

XClarity Administrator には、オペレーティング・システム・イメージを *ベア・メタル*・サーバーにデプロイする簡単な方法が用意されています。このベア・メタル・サーバーには、通常、オペレーティング・システムがインストールされていません。

注意：オペレーティング・システムがインストールされているサーバーにオペレーティング・システムをデプロイすると、XClarity Administrator によってフレッシュ・インストールが実行されターゲット・ディスク上のパーティションが上書きされます。

オペレーティング・システムをサーバーにデプロイする際の所要時間は、以下のいくつかの要因によって決まります。

- サーバーに搭載された RAM の容量。サーバーの起動時間に影響します。
- サーバーに取り付けられた I/O アダプターのタイプと数。XClarity Administrator サーバーのインベントリーの実行時間に影響します。また、サーバー起動時の UEFI ファームウェアの起動にかかる時間にも影響します。オペレーティング・システムのデプロイメント中、サーバーは複数回、再起動されます。
- ネットワーク・トラフィック。XClarity Administrator は、データ・ネットワークまたはオペレーティング・システム・デプロイメント・ネットワークを介してオペレーティング・システム・イメージをダウンロードします。
- Lenovo XClarity Administrator 仮想アプライアンスがインストールされているホストのハードウェア構成。RAM、プロセッサー、ハードディスク・ドライブ・ストレージの容量はダウンロードにかかる時間に影響を与えることがあります。

重要：XClarity Administrator からオペレーティング・システム・イメージをデプロイするには、少なくとも 1 つの XClarity Administrator インターフェース (Eth0 または Eth1) に、ホスト・オペレーティング・システムへのアクセスに使用するサーバー・ネットワーク・インターフェースへの IP ネットワーク接続が必要です。オペレーティング・システム・デプロイメントでは、「ネットワーク・アクセス」ページで定義されているインターフェースが使用されます。ネットワーク設定について詳しくは、ネットワーク・アクセスの構成を参照してください。

サーバーでベアメタル・オペレーティング・システム・デプロイメントを実行する前に、そのサーバーを準備してください。サーバーを準備するには、ファームウェアを最新レベルに更新し、構成パターン を使用してサーバーを構成します。詳しくは、管理対象デバイスでのファームウェアの更新および構成パターンを使用したサーバーの構成を参照してください。

注意：Converged と ThinkAgile アプライアンスでのベアメタル・オペレーティング・システム・デプロイメントを実行するために、XClarity Administrator を使用*しない*ことをお勧めします。

手順

次の図は、サーバーへの OS イメージのデプロイのワークフローを示しています。

ステップ 1. **OS イメージをインポートします。**

OS イメージをサーバーにデプロイする前に、まず、オペレーティング・システムをリポジトリーにインポートする必要があります。OS イメージをインポートするとき、XClarity Administrator。

- オペレーティング・システムのインポートの前に、OS イメージ・リポジトリー に十分なスペースがあるかどうかを確認する。十分なスペースがない場合は、既存のイメージを削除してからやり直します。
- そのイメージのプロファイルが 1 つ以上作成され、そのプロファイルを OS イメージ・リポジトリー に保存する。各*プロファイル*には、OS イメージとインストール・オプションが含まれています。事前定義された OS イメージ・プロファイルについて詳しくは、オペレーティング・システム・イメージ・プロファイルを参照してください。

*ベース・オペレーティング・システム*は、OS イメージ・リポジトリーにインポートされたフル OS イメージです。インポートされたベース・イメージには、そのイメージのインストールの構成を記述する事前定義済みプロファイルが含まれています。特定の構成用にカスタム・プロファイルをベース OS イメージ内に作成してデプロイできます。

また、サポートされている*カスタム・オペレーティング・システム*をインポートすることもできます。このカスタム・イメージには、事前定義済みプレースホルダー・プロファイルが含まれていますが、デプロイすることはできません。デプロイできるカスタム・プロファイルをインポートするか、プレースホルダー・プロファイルに基づいて独自のカスタム・プロファイルを作成する必要があります。カスタム・プロファイルが追加された後、プレースホルダー・プロファイルは自動的に削除されます。

Microsoft Windows Server 2016 および 2019 では、各リリースのカスタム・オペレーティング・システム・イメージをインポートできます。インポートされたベース・イメージには、そのイメージのインストールの構成を記述する事前定義済みプロファイルが含まれています。カスタム OS イメージでカスタム・プロファイルを作成することはできません。

サポートされるオペレーティング・システムのリストについては、Lenovo XClarity Administrator オンライン・ドキュメントの 対応オペレーティング・システムサポートされているオペレーティング・システム を参照してください。

ステップ 2. **(オプション) OS イメージをカスタマイズします。**

デバイス・ドライバー、ブート・ファイル (Windows のみ)、構成設定、無人ファイル、ポスト・インストール・スクリプト、およびソフトウェアを追加して OS イメージをカスタマイ

ズできます。ベース OS イメージをカスタマイズすると、カスタム・ファイルおよびインストール・オプションを含むカスタマイズされた OS イメージが XClarity Administrator により作成されます。

OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

ステップ 3. **共通設定を構成します。**

共通設定は、オペレーティング・システムのデプロイメント用にデフォルトとして使用される構成オプションです。以下のグローバル設定を構成できます。

- オペレーティング・システムをデプロイするときに使用する管理者ユーザー・アカウントのパスワード
- サーバーに IP アドレスを割り当てる方法
- インストールされたオペレーティング・システムをアクティブ化するときに使用するライセンス・キー
- Windows オペレーティング・システムのデプロイメントの一環として Active Directory ドメインに参加 (オプション)

ステップ 4. **ネットワーク設定を構成します。**

オペレーティング・システムがデプロイされる各サーバーのネットワーク設定を指定できます。

DHCP を使用して動的に IP アドレスを割り当てる場合は、MAC アドレスを構成する必要があります。

静的 IP アドレスを使用する場合は、オペレーティング・システムを特定のサーバーにデプロイする前に、そのサーバーに対して以下のネットワーク設定を構成する必要があります。これらの設定が構成されると、サーバーのデプロイメント・ステータスは「動作可能」に変更されます。(一部のフィールドは固定 IPv6 アドレスでは使用できない点に注意してください。)

- ホスト名

  ホスト名は、以下の規則に従っている必要があります。
  - 各管理対象サーバーのホスト名は固有でなければなりません。
  - ホスト名にはピリオド (.) で区切られた複数の文字列 (ラベル) を含めることができます。
  - 各ラベルには ASCII 文字、数字、ダッシュ (-) を使用できます。ただし、文字列をダッシュで開始または終了することはできません。すべて数字にすることもできません。
  - 最初のラベルの長さは 2 ～ 15 文字にすることができます。後続のラベルの長さは 2 ～ 63 文字にすることができます。
  - ホスト名の合計の長さが、255 文字を超えないようにしてください。
- オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレス。

  MAC アドレスはデフォルトで「自動」に設定されています。この設定は、デプロイメント用に構成して使用できるイーサネット・ポートを自動的に検出します。検出された最初の MAC アドレス (ポート) が、デフォルトで使用されます。別の MAC アドレスとの接続が検出された場合は、XClarity Administrator ホストが自動的に再起動され、新しく検出された MAC アドレスをデプロイメントに使用します。

  「ネットワーク設定」ダイアログの「**MAC アドレス**」ドロップダウン・メニューから OS デプロイメントに使用されている MAC アドレス・ポートのステータスを確認できます。複数のポートが稼働している場合、またはすべてのポートがダウンしている場合、デフォルトでは AUTO が使用されます。

  注：

- 仮想ネットワーク・ポートはサポートされていません。1 つの物理ネットワーク・ポートを使用して複数の仮想ネットワーク・ポートをシミュレートしないでください。
- サーバーのネットワーク設定が AUTO に設定されている場合、XClarity Administrator はスロット 1 ～ 16 のネットワーク・ポートを自動的に検出できます。スロット 1 ～ 16 にあるポートのうち少なくとも 1 つは、XClarity Administrator に接続する必要があります。
- スロット 17 以上のネットワーク・ポートを MAC アドレスに使用する場合、AUTO を使用できません。代わりに、サーバーのネットワーク設定を、使用する特定のポートの MAC アドレスに設定する必要があります。
- ThinkServer サーバーでは、すべてのホスト MAC アドレスが表示されるわけではありません。多くの場合、AnyFabric Ethernet アダプターの MAC アドレスは「ネットワーク設定の編集」ダイアログにリストされます。他のイーサネット・アダプターの MAC アドレス (LAN-on-Motherboard など) はリストされません。アダプターの MAC アドレスが使用できない場合、非 VLAN デプロイメント用の自動方式を使用してください。

- IP アドレスとサブネット・マスク
- IP ゲートウェイ
- ドメイン・ネーム・システム (DNS) サーバー (2 つまで)
- 最大転送単位 (MTU) 速度
- VLAN IP モードが有効な場合は VLAN ID

VLAN を使用するように選択する場合は、構成しているホスト・ネットワーク・アダプターに VLAN ID を割り当てることができます。

ステップ 5. **ストレージ・オプションの選択**

各デプロイメントについて、オペレーティング・システムがデプロイされる優先格納場所を選択できます。オペレーティング・システムによっては、ローカル・ディスク・ドライブ、組み込みハイパーバイザー・キー、または SAN にデプロイすることもできます。

ステップ 6. **追加のオプションとカスタム構成設定を選択して OS イメージをデプロイします。**

OS デプロイメント用のライセンス・キーなどの追加のデプロイメント・オプションやカスタムの構成設定を構成できます。Microsoft Windows をインストールする場合には、参加する Active Directory ドメインも構成できます。

注：

- 特定のカスタム OS プロファイルのカスタム構成設定を定義した場合は、プロファイルをサーバーにデプロイする前に、必要なカスタム構成設定の値を定義する必要があります。
- カスタム設定を含むカスタム OS プロファイルをデプロイする場合は、すべてのターゲット・サーバーが同じカスタム OS プロファイルを使用する必要があり、カスタム設定の値はすべてのターゲット・サーバーに適用されます。

次に、デプロイメントのターゲット・サーバーとデプロイする OS イメージを選択します。オペレーティング・システムをデプロイするには、サーバーのデプロイメント・ステータスが「動作可能」になっている必要があることに注意してください。

最大 28 台のサーバーに、オペレーティング・システム・イメージを同時にデプロイできます。

オペレーティング・システム・イメージをデプロイする前に、オペレーティング・システム・デプロイメントの考慮事項を確認してください。

オペレーティング・システム・デプロイメントの考慮事項

オペレーティング・システム・イメージをデプロイする前に、以下の考慮事項を確認してください。

Lenovo XClarity Administrator 考慮事項

- ターゲット・サーバーで現在実行されているジョブがないことを確認します。アクティブ・ジョブのリストを表示するには、「**監視**」 ➡ 「**ジョブ**」をクリックします。
- 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。管理対象サーバーでサーバー・パターンのアクティブ化が据え置きされているか、またはサーバー・パターンが部分的にアクティブ化されている場合は、サーバーを再起動してすべての構成設定を適用する必要があります。部分的にアクティブ化されたサーバー・パターンを使用してオペレーティング・システムをサーバーにデプロイしないでください。サーバーの構成ステータスを判断するには、管理対象サーバーの「要約」ページで「**構成ステータス**」フィールドを確認します (管理対象サーバーの詳細の表示を参照してください)。
- オペレーティング・システムのデプロイに使用される管理者アカウントのパスワードが、「共通設定: オペレーティング・システムのデプロイ」ダイアログに指定されていることを確認します。パスワードの設定について詳しくは、グローバル OS デプロイメント設定の構成を参照してください。
- 共通のデフォルト設定がこのオペレーティング・システム・デプロイメントに適していることを確認します (グローバル OS デプロイメント設定の構成を参照)。

オペレーティング・システムの考慮事項

- 該当するすべてのオペレーティング・システムのライセンスがあり、インストールされているオペレーティング・システムをアクティブ化できることを確認します。ライセンスは、オペレーティング・システムのメーカーから直接取得する必要があります。
- デプロイするオペレーティング・システム・イメージが既に OS イメージ・リポジトリーに読み込まれていることを確認します。イメージのインポートについては、オペレーティング・システム・イメージのインポートを参照してください。
- XClarity Administrator のリポジトリーのオペレーティング・システム・イメージは、特定のハードウェア・プラットフォームに限定され、サポートされていない場合があります。「OS イメージのデプロイ」ページには、選択したサーバーでサポートされている OS イメージ・プロファイルのみが表示されます。Lenovo OS 相互運用性ガイド Web サイト から、オペレーティング・システムが特定のサーバーと互換性があるかどうかを判別できます。
- Windows の場合、Windows プロファイルをデプロイする前に、OS イメージ・リポジトリーにブート・ファイルをインポートする必要があります。Lenovo は事前定義済み WinPE_64.wim ブート・ファイルとデバイス・ドライバーのセットを 1 つのパッケージにバンドルします。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれているので、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・ファイル**」タブからインポートできます。
- SLES 15 および 15 SP1 では、インストーラー・イメージおよび関連するパッケージ・イメージの両方を サーバーの OS サポート・センターの Web ページ からインポートする必要があります。SLES 15 SP2 以降の場合、SUSE Linux Enterprise Server 15 および 15 SP1 から統一されたインストーラーおよびパッケージ DVD を作成することは推奨されないため、完全なインストールメディア・イメージのみをインポートする必要があります。
- ThinkSystem サーバーの場合、XClarity Administrator には、オペレーティング・システムのインストール、および最終オペレーティング・システム用の基本ネットワークとストレージを構成できるデバイス・ドライバーが同梱されています。その他のサーバーの場合は、デプロイするオペレーティング・システム・イメージに、ハードウェア環境に合ったイーサネット、Fibre Channel およびストレージ・アダプターのデバイス・ドライバーが含まれていることを確認します。I/O アダプター・デバイス・ドライバーがオペレーティング・システムに含まれていない場合、アダプターは OS デプロイメントではサポートされません。必要な inbox I/O アダプター・デバイス・ドライバーおよびブート・ファイルが最新であるように、常に最新のオペレーティング・システムをインストールしてください。また、XClarity Administrator にインポートされたオペレーティング・システムにアウト・オブ・ボックス・デバイス・ドライバーとブート・ファイルを追加できます (XClarity Administrator オンライン・ドキュメントの OS イメージ・プロファイルのカスタマイズを参照)。

VMware の場合、最新のアダプター・サポートを含む、最新の ESXi の Lenovo Custom Image を使用してください。そのイメージの入手方法については、VMware サポート - ダウンロード Web サイトを参照してください。

- ThinkSystem サーバーの場合、SLES 12 SP2 をデプロイするには、kISO プロファイルを使用する必要があります。kISO プロファイルを取得するには、ベース SLES オペレーティング・システムをインポートした後に、適切な SLES kISO イメージをインポートする必要があります。Linux サポート - ダウンロード Web サイトから SLES kISO イメージをダウンロードすることができます。

  注：

  – SLES kISO イメージはインポート済みの OS イメージを最大数までカウントします。

    サポートされるオペレーティング・システムのリストについては、Lenovo XClarity Administrator オンライン・ドキュメントの 対応オペレーティング・システム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。

  – すべての kISO プロファイルを削除する場合、SLES 12 SP2 を ThinkSystem サーバーでデプロイするには、ベース SLES オペレーティング・システムを削除してから、再度基本オペレーティング・システムおよび kISO イメージをインポートしする必要があります。

  – kISO プロファイルに基づいてカスタム OS プロファイルを作成する場合、ベース・オペレーティング・システムの事前定義済みデバイス・ドライバーは含まれません。kISO に含まれるデバイス・ドライバーが代わりに使用されます。カスタム OS プロファイルにデバイス・ドライバーを追加することもできます (カスタム OS イメージ・プロファイルの作成を参照)。

特定のオペレーティング・システムの制限について詳しくは、サポートされているオペレーティング・システムを参照してください。

ネットワークに関する考慮事項

- 必要なすべてのポートが開いていることを確認します (デプロイされたオペレーティング・システムで利用可能なポートを参照)。
- XClarity Administrator が、XClarity Administrator ネットワーク・アクセスを構成したときに選択したインターフェース (Eth0 または Eth1) 経由でターゲット・サーバー (ベースボード管理コントローラーおよびサーバーのデータ・ネットワークの両方) と通信できることを確認します。

  オペレーティング・システム・デプロイメントに使用するインターフェースを指定するには、ネットワーク・アクセスの構成を参照)。

  オペレーティング・システム・デプロイメントのネットワークおよびインターフェースについて詳しくは、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。
- IP アドレスがホスト・オペレーティング・システムに対して一意であることを確認してください。XClarity Administrator はデプロイメント・プロセス中に、ネットワーク・アドレスとして指定された IP アドレスの重複をチェックします。
- ネットワークが低速またはが不安定な場合は、オペレーティング・システムのデプロイが予期しない結果になる可能性があります。
- XClarity Administrator管理に使用されるネットワーク・インターフェースは、「共通設定: オペレーティング・システムのデプロイメント」ダイアログで選択した IP アドレス方式と同じものを使用して、ベースボード管理コントローラーに接続されるよう構成する必要があります。たとえば、XClarity Administratorが管理用に eth0 を使用するよう設定され、デプロイ済み OS を構成するときに手動で割り当てられた静的 IPv6 アドレスの使用を選択した場合、eth0 はベースボード管理コントローラーと接続された IPv6 アドレスと一緒に構成されている必要があります。
- OS デプロイメントの共通設定で IPv6 アドレスを使用するように選択した場合、XClarity Administrator の IPv6 アドレスがベースボード管理コントローラーとサーバーのデータ・ネットワークにルーティング可能である必要があります。

- ThinkServer では IPv6 モードはサポートされていません (XClarity Administrator オンライン・ドキュメントの IPv6 構成の制限を参照)。
- DHCP を使用して動的に IP アドレスを割り当てる場合は、MAC アドレスを構成する必要があります。
- 静的 IP アドレスを使用する場合は、オペレーティング・システムを特定のサーバーにデプロイする前に、そのサーバーに対して以下のネットワーク設定を構成する必要があります。これらの設定が構成されると、サーバーのデプロイメント・ステータスは「動作可能」に変更されます。(一部のフィールドは固定 IPv6 アドレスでは使用できない点に注意してください。)
  - ホスト名

    ホスト名は、以下の規則に従っている必要があります。
    - 各管理対象サーバーのホスト名は固有でなければなりません。
    - ホスト名にはピリオド (.) で区切られた複数の文字列 (ラベル) を含めることができます。
    - 各ラベルには ASCII 文字、数字、ダッシュ (-) を使用できます。ただし、文字列をダッシュで開始または終了することはできません。すべて数字にすることもできません。
    - 最初のラベルの長さは 2 ～ 15 文字にすることができます。後続のラベルの長さは 2 ～ 63 文字にすることができます。
    - ホスト名の合計の長さが、255 文字を超えないようにしてください。
  - オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレス。

    MAC アドレスはデフォルトで「自動」に設定されています。この設定は、デプロイメント用に構成して使用できるイーサネット・ポートを自動的に検出します。検出された最初の MAC アドレス (ポート) が、デフォルトで使用されます。別の MAC アドレスとの接続が検出された場合は、XClarity Administrator ホストが自動的に再起動され、新しく検出された MAC アドレスをデプロイメントに使用します。

    「ネットワーク設定」ダイアログの「**MAC アドレス**」ドロップダウン・メニューから OS デプロイメントに使用されている MAC アドレス・ポートのステータスを確認できます。複数のポートが稼働している場合、またはすべてのポートがダウンしている場合、デフォルトでは AUTO が使用されます。

    注：

    - 仮想ネットワーク・ポートはサポートされていません。1 つの物理ネットワーク・ポートを使用して複数の仮想ネットワーク・ポートをシミュレートしないでください。
    - サーバーのネットワーク設定が AUTO に設定されている場合、XClarity Administrator はスロット 1 ～ 16 のネットワーク・ポートを自動的に検出できます。スロット 1 ～ 16 にあるポートのうち少なくとも 1 つは、XClarity Administrator に接続する必要があります。
    - スロット 17 以上のネットワーク・ポートを MAC アドレスに使用する場合、AUTO を使用できません。代わりに、サーバーのネットワーク設定を、使用する特定のポートの MAC アドレスに設定する必要があります。
    - ThinkServer サーバーでは、すべてのホスト MAC アドレスが表示されるわけではありません。多くの場合、AnyFabric Ethernet アダプターの MAC アドレスは「ネットワーク設定の編集」ダイアログにリストされます。他のイーサネット・アダプターの MAC アドレス (LAN-on-Motherboard など) はリストされません。アダプターの MAC アドレスが使用できない場合、非 VLAN デプロイメント用の自動方式を使用してください。
  - IP アドレスとサブネット・マスク
  - IP ゲートウェイ
  - ドメイン・ネーム・システム (DNS) サーバー (2 つまで)
  - 最大転送単位 (MTU) 速度
  - VLAN IP モードが有効な場合は VLAN ID
- VLAN を使用するように選択する場合は、構成しているホスト・ネットワーク・アダプターに VLAN ID を割り当てることができます。

オペレーティング・システム・デプロイメント・ネットワークおよびインターフェースについて詳しくは、管理対象サーバーのネットワーク設定の構成および 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および ネットワークに関する考慮事項を参照してください。

ストレージおよびブート・オプションの考慮事項

- オペレーティング・システムをデプロイする前に、ターゲット・サーバーの UEFI ブート・オプションが「UEFI ブートのみ」に設定されていることを確認します。「Legacy Only」および「最初に UEFI、次に Legacy」ブート・オプションは、オペレーティング・システム・デプロイメントに対してサポートされません。
- 各サーバーにハードウェア RAID アダプターが取り付けられ構成されている。

  注意：

  – ハードウェア RAID を使用してセットアップされているストレージのみがサポートされています。

  – 通常はオンボード Intel SATA ストレージ・アダプターにあるソフトウェア RAID または JBOD としてセットアップされているストレージは、サポートされません。ただし、ハードウェア RAID アダプターが存在せず、SATA アダプターがオペレーティング・システム・デプロイメントで「**AHCI SATA モード**」対応の場合、または JBOD に未構成の正常ディスクが設定されている場合は、機能する場合があります。詳しくは、XClarity Administrator オンライン・ドキュメントのOS インストーラーで XClarity Administrator にインストールするディスクが見つからないを参照してください。

    この例外は M.2 ドライブには適用されません。

  – 管理対象デバイスに、ハードウェア RAID 用に構成されていないローカル・ドライブ (SATA、SAS、または SSD) および M.2 ドライブの両方がある場合、M.2 ドライブを使用する場合はローカル・ドライブを無効に、ローカル・ドライブを使用する場合は M.2 ドライブを無効にする必要があります。ウィザードのローカル・ストレージ・タブで「ローカル・ディスクの無効化」を選択するか、既存のサーバーから構成パターンを作成してから、拡張 UEFI パターンの M.2 デバイスを無効にすることで、構成パターンを使用して、オンボード・ストレージ・コントローラー・デバイス、およびレガシーと UEFI ストレージ・オプション ROM を無効にできます。

  – SATA アダプターが有効な場合、SATA モードを「IDE」に設定*しないでください*。
- サーバー・マザーボードまたは HBA コントローラーに接続された NVMe ストレージはサポートされていないため、デバイスにインストールしないでください。インストールすると、非 NVMe ストレージに OS をデプロイすることはできません。
- RHEL をデプロイするとき、ターゲット・ストレージ上の同じ LUN に接続されているマルチ・ポートはサポートされていません。
- セキュア・ブート・モードがサーバーに対して無効であることを確認します。セキュア・ブート・モードが有効なオペレーティング・システム (Windows など) をデプロイする場合は、セキュア・ブート・モードを無効にして、オペレーティング・システムをデプロイし、その後セキュア・ブート・モードを再度有効にします。
- Microsoft Windows をサーバーにデプロイする場合は、アタッチされた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 (XClarity Administrator オンライン・ドキュメントの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を参照)。
- ThinkServer サーバーの場合は、以下の要件を満たしていることを確認してください。

  – サーバーのブート設定で、ストレージ OpROM ポリシーが `UEFI Only` に設定されている必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントのOS インストーラーが ThinkServer サーバーを起動できない - XClarity Administratorを参照してください。

  – ESXi をデプロイする場合で PXE ブート可能なネットワーク・アダプターがある場合は、オペレーティング・システムをデプロイする前に、ネットワーク・アダプターの PXE サポートを無効にします。デプロイメントの完了後、必要に応じて PXE サポートを再度有効にできます。

  – ESXi をデプロイする場合で、オペレーティング・システムがインストールされているドライブ以外の起動可能デバイスがブート順序リストにある場合は、オペレーティング・システムをデプロイする前にその起動可能デバイスをブート順序リストから削除してください。デプロイの完了

後、起動可能デバイスをリストに戻すことができます。インストールされているドライブがリストの先頭にあることを確認します。

ストレージ・ロケーションの設定の詳細については、管理対象サーバーの保管場所の選択を参照してください。

管理対象デバイスに関する考慮事項

- 特定のデバイスのオペレーティング・システム・デプロイメント制限について詳しくは、XClarity Administrator のサポート – 互換性に 関する Web ページ で「**互換性**」タブをクリックしてから、該当するデバイス・タイプのリンクをクリックしてください。
- ターゲット・サーバーにマウントされたメディア (ISO イメージなど) がないことを確認します。さらに、管理コントローラーに対してアクティブなリモート・メディア・セッションが開いていないことを確認します。
- BIOS のタイム・スタンプが現在の日時に設定されていることを確認します。
- システム・ガードが有効になっている XCC2 を持つサーバーで、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。
- ThinkSystem および System x サーバーの場合は、レガシー BIOS オプションが無効になっていることを確認します。BIOS/UEFI (F1) Setup utility で、「**UEFI セットアップ**」 ➡ 「**システム設定**」の順にクリックし、レガシー BIOS が無効に設定されていることを確認します。
- Flex System サーバーの場合、シャーシの電源がオンになっていることを確認します。
- コンバージド、NeXtScale、および System x サーバーの場合、リモート・プレゼンスの Feature on Demand (FoD) キーがインストールされていることを確認します。「サーバー」 ページから、リモート・プレゼンスの有効化または無効化を行うか、あるいはサーバーにインストールしないことを選択できます (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)。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、Features on Demand キーの表示を参照してください。
- ThinkSystem サーバーおよび ThinkAgile アプライアンスの場合、オペレーティング・システム・デプロイメントに XClarity Controller Enterprise 機能が必要です。詳しくは、Features on Demand キーの表示を参照してください。
- Converged と ThinkAgile アプライアンスについて、ベアメタル・オペレーティング・システム・デプロイメントを実行するために、XClarity Administrator を使用*しない*ことをお勧めします。

サポートされているオペレーティング・システム

Lenovo XClarity Administrator は、複数のオペレーティング・システムのデプロイメントをサポートします。サポートされるバージョンのオペレーティング・システムのみ、XClarity Administrator OS イメージ・リポジトリーにロードできます。

重要：

- 特定のデバイスのオペレーティング・システム・デプロイメント制限について詳しくは、XClarity Administrator のサポート – 互換性に 関する Web ページ で「**互換性**」タブをクリックしてから、該当するデバイス・タイプのリンクをクリックしてください。
- XClarity Administrator の暗号管理機能を使用すると、特定の最小 SSL/TLS モードへの通信を制限できます。たとえば、TLS 1.2 を選択する場合は、XClarity Administrator でデプロイできるのは、インストール・プロセスが TLS 1.2 と強い暗号化アルゴリズムをサポートしているオペレーティング・システムのみであることに注意してください。
- XClarity Administrator のリポジトリーのオペレーティング・システム・イメージは、特定のハードウェア・プラットフォームに限定され、サポートされていない場合があります。「OS イメージのデプロ

イ」ページには、選択したサーバーでサポートされている OS イメージ・プロファイルのみが表示されます。Lenovo OS 相互運用性ガイド Web サイト から、オペレーティング・システムが特定のサーバーと互換性があるかどうかを判別できます。

- OS とハイパーバイザーに関連する互換性、および Lenovo サーバーおよびソリューションに対するサポート情報とリソースについては、サーバーの OS サポート・センターの Web ページ を参照してください。

次の表に、XClarity Administrator でデプロイできる 64 ビット・オペレーティング・システムを示します。

オペレーティング・システム	バージョン	注
CentOS Linux	7.2 and later 8.0 8.1 8.2	注： • 特に断りがない限り、すべての既存および将来のマイナーバージョンがサポートされます。 • DHCP、静的 IPv4、および静的 IPv6 アドレスがサポートされています。 • VLAN タグ付けがサポートされていません。 • アウト・オブ・ボックス・ドライバーはサポートされていません。 • OS プロファイルのカスタマイズはサポートされていません。 • CentOS 8.3 はサポートされていません。
Microsoft® Windows® Azure Stack HCI	20H2 21H2	OS プロファイルのカスタマイズはサポートされていません。
Microsoft Windows Client	10 21H2 10 22H2 11 22H2	
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	リテール版とボリューム・ライセンス版がサポートされています。 注：XClarity Administrator は、XClarity Administrator バージョンのリリース時に、Microsoft によってサポートされている Windows バージョンのみを使用してテストされています。 以下は *サポートされていません*。 • Windows リセラー・オプション・キット (ROK) • Windows Server Semi-Annual Channel (SAC) v1709、v1803 および v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Windows Server 2012 評価版 • 組み込みハイパーバイザー・キーを持つ管理対象サーバーへの Windows Server イメージ Intel CLX プロセッサーが含まれているサーバー上の Windows Server 2012 R2 Windows イメージをデプロイする前に、ターゲット・サーバーから組み込みハイパーバイザー・キーを物理的に取り外す必要があります。これには、いずれかの仮想化プロファイルによる Hyper-V が含まれます。 – Datacenter – Datacenter コア – Datacenter 仮想化 (Hyper-V) – Datacenter 仮想化コア (コア付属 Hyper-V) – 標準 – 標準コア – 標準の仮想化 (Hyper-V) – 標準の仮想化コア (コア付属 Hyper-V)

オペレーティング・システム	バージョン	注
Red Hat® Enterprise Linux (RHEL) サーバー	6.8 and later 7.2 and later 8.x 9.x	KVM が含まれます。 注： • 特に断りがない限り、すべての既存および将来のマイナーバージョンがサポートされます。 • DVD 版の OS イメージをインポートする場合は、DVD1 のみがサポートされます。 • RHEL を ThinkSystem サーバーにインストールする場合は、RHEL v7.4 以降が推奨です。 • RHEL 7.2 をデプロイするには、IPv4 アドレスを使用するようにグローバル IP 割り当てを設定する必要があります。グローバル設定については、グローバル OS デプロイメント設定の構成を参照してください。 • OS インストーラーのタイムアウトにより、低帯域幅 IPv6 ネットワークで OS デプロイメント障害が確認されました。 • VLAN タグ付けがサポートされていません。
Rocky Linux	8.x 9.x	注： • 特に断りがない限り、すべての既存および将来のマイナーバージョンがサポートされます。 • DHCP、静的 IPv4、および静的 IPv6 アドレスがサポートされています。 • VLAN タグ付けがサポートされていません。 • アウト・オブ・ボックス・ドライバーはサポートされていません。
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	KVM および Xen ハイパーバイザーが含まれます 注： • 特に断りがない限り、すべての既存および将来のサービス・パックがサポートされます。 • DVD 版の OS イメージをインポートする場合は、DVD1 のみがサポートされます。 • OS インストーラーのタイムアウトにより、帯域幅の狭い IPv6 ネットワークで OS のデプロイの失敗が確認されています。 • ThinkSystem サーバーに、SLES 12 SP2 をデプロイするには、kISO プロファイルを使用する必要があります。kISO プロファイルを取得するには、適切な SLES kISO イメージをインポートする必要があります。詳しくは、オペレーティング・システム・デプロイメントの考慮事項を参照してください。 • SLES 15 および 15 SP1 では、インストーラー・イメージおよび関連するパッケージ・イメージの両方を サーバーの OS サポート・センターの Web ページ からインポートする必要があります。SLES 15 SP2 以降の場合、SUSE Linux Enterprise Server 15 および 15 SP1 から統一されたインストーラーおよびパッケージ DVD を作成することは推奨されないため、完全なインストールメディア・イメージのみをインポートする必要があります。 • VLAN タグ付けがサポートされていません。

オペレーティング・システム	バージョン	注
Ubuntu サーバー	20.04.x 22.04.x	**注：** • 選択したストレージ・オプション (ローカル・ディスク・ドライブ、M.2 ドライブ、または FC SAN ボリューム) にイメージをインストールすることができます。 • 特に断りがない限り、すべての既存および将来のマイナーバージョンがサポートされます。 • DHCP のみサポートされます。静的 IPv4 および静的 IPv6 アドレスはサポート*されていません*。 • VLAN タグ付けがサポート*されていません*。 • アウト・オブ・ボックス・ドライバーはサポート*されていません*。 • OS プロファイルのカスタマイズはサポート*されていません*。
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	基本 VMware vSphere Hypervisor (ESXi) イメージおよび Lenovo VMware ESXi カスタム・イメージがサポートされます。 Lenovo VMware ESXi カスタム・イメージは、ファームウェアの更新や構成、プラットフォーム診断、拡張ハードウェア・アラートなどのオンライン・プラットフォーム管理を実行できるように特定のハードウェア向けにカスタマイズされています。また、Lenovo 管理ツールでも、特定の System x サーバーにおける ESXi の簡易管理がサポートされています。このイメージは、VMware サポート - ダウンロード Web サイト からダウンロードできます。イメージに付与されるライセンスは 60 日間の無料試用版です。使用するには、VMware ライセンスのすべての要件を満たす必要があります。 **重要：** • 特筆されない限り、すべての既存の更新パックと今後の更新パックは、6.0、6.5、6.7、7.0、8.0 でサポートされます。 • (Lenovo カスタマイズを含まない) 基本 ESXi イメージには、ネットワークおよびストレージ向けの基本インボックス・デバイス・ドライバーが含まれます。この基本イメージには、(Lenovo VMware ESXi カスタム・イメージに含まれない) アウト・オブ・ボックス・デバイス・ドライバーは含まれません。独自のカスタム OS0image プロファイルを作成することで、アウト・オブ・ボックス・デバイス・ドライバーを追加できます (XClarity Administratorオンライン・ドキュメントのOS イメージ・プロファイルのカスタマイズを参照)。 • Lenovo VMware ESXi Custom イメージの一部のバージョンでは、System x、ThinkSystem および ThinkServer で個別のイメージが用意されている場合があります。OS イメージ・リポジトリーに同時に存在できる固有のリリースのイメージは 1 つのみです。 • 特定の古いサーバーでは ESXi のデプロイメントがサポートされません。サポートされるサーバーについては、Lenovo OS 相互運用性ガイド Web サイトを参照してください。 • ThinkServer デバイスでは次のバージョンがサポートされます: ESXi 6.0u3、6.5 以降。 • ESXi 5.5 (任意の更新)、または 6.0 の Flex System シャーシ内のサーバーへのインストール中に、 `Loading image.pld` というメッセージが表示された直後は、サーバーが応答しなくなったり再起動したりする場合があります。 • ESXi 5.5 では、システムの最初の 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、システムで 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、XClarity Administrator オンライン・ドキュメントの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を参照してください。

オペレーティング・システム	バージョン	注
		• ESXi を静的 IPv6 モードを使用してデプロイする場合、XClarity Administrator のネットワーク設定ページで定義されたホスト名は、デプロイされた ESXi インスタンスでは構成されません。代わりに、デフォルトのホスト名 `localhost` が使用されます。XClarity Administrator で定義されたホスト名と一致するように、デプロイされた ESXi のホスト名を手動で設定する必要があります。 • 管理対象サーバーで 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。オペレーティング・システムをデプロイする前に、PXE ブートのサポートを無効にするか、インストールするドライブ以外の起動可能デバイスを取り外す必要があります。詳しくは、XClarity Administrator オンライン・ドキュメントのThinkServer サーバーに ESXi をデプロイした後、 オペレーティング・システムがブートしないを参照してください。 **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、拡張 UEFI 設定の定義を参照してください。

オペレーティング・システム・イメージ・プロファイル

OS イメージを OS イメージ・リポジトリー にインポートすると、Lenovo XClarity Administrator がそのイメージのプロファイルを 1 つ以上作成し、そのプロファイルを OS イメージ・リポジトリー に保存します。事前定義された各 *プロファイル*には、OS イメージとそのイメージのインストール・オプションが含まれます。

OS イメージ・プロファイル属性

OS イメージ・プロファイルの属性は、OS イメージ・プロファイルに関する情報を提供します。以下の属性が表示されます。

- **kISO**。SLES 12 SP2 を ThinkSystem サーバーにデプロイするには、kISO プロファイルを使用する必要があります。Linux サポート - ダウンロード Web サイトから SLES kISO イメージをダウンロードすることができます。

事前定義された OS イメージ・プロファイル

次の表は、オペレーティング・システム・イメージのインポート時に XClarity Administrator によって定義されたプロファイルのリストです。各プロファイルに含まれるパッケージもリストしています。

ベース・オペレーティング・システムのカスタマイズされた OS イメージ・プロファイルを作成できます。詳しくは、OS イメージ・プロファイルのカスタマイズを参照してください。

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ	
CentOS Linux	基本	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	最小	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	仮想化	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Microsoft® Windows® Azure Stack HCI	Azure	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="Containers" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Client	Enterprise		
	Enterprise N		
	Workstations Pro		
	Workstations_Pro N		

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ	
Microsoft Windows Hyper-V Server 2016	Hyper_V	<selection name="Microsoft-Hyper-V" state="true" /> <selection name="MultipathIo" state="true" /> <selection name="FailoverCluster-PowerShell" state="true" /> <selection name="FailoverCluster-FullServer" state="true" /> <selection name="FailoverCluster-CmdInterface" state="true" /> <selection name="FailoverCluster-AutomationServer" state="true" /> <selection name="FailoverCluster-AdminPak" state="true" /> <selection name="MicrosoftWindowsPowerShellRoot" state="true" /> <selection name="MicrosoftWindowsPowerShell" state="true" /> <selection name="ServerManager-Core-RSAT" state="true" /> <selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />	
Microsoft Windows Server **注：***仮想化プロファイル*で Hyper-V が含まれます。	Datacenter	GUI	
	Datacenter 仮想化	GUI Hyper-V role	
	Datacenter 仮想化コア	Hyper-V role	
	Datacenter コア		
	標準	GUI	
	標準の仮想化	GUI Hyper-V role	
	標準の仮想化コア	Hyper-V role	
	標準コア		
カスタマイズされた Microsoft Windows Server	Datacenter_customized		
	Standard_customized		
Red Hat Enterprise Linux (RHEL) **注：**KVM が含まれます。	基本	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	最小	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	仮想化	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ	
		@kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Rocky Linux	基本	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	最小	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	仮想化	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 15	基本、基本	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	

オペレーティング・システム	プロファイル	プロファイルに含まれるパッケージ
	最小、最小	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	仮想化 - KVM および仮想化 - KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
	仮想化 - Xen および仮想化 - Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	最小	OpenSSH サーバー
	仮想化	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	仮想化	基本 VMware vSphere Hypervisor (ESXi) イメージおよび Lenovo VMware ESXi カスタム・イメージがサポートされます。

デプロイされたオペレーティング・システムで利用可能なポート

ポートの中には、特定のオペレーティング・システム・プロファイルではブロックされているものがあります。次の表は、開いている (ブロックされていない) ポートのリストを示しています。

通信	RHEL、Centos、および Rocky 仮想化プロファイル[1]	RHEL、Centos、および Rocky の基本プロファイルと最小プロファイル[1]	SLES の仮想化、基本プロファイルと最小プロファイル[2]	Ubuntu の仮想化、基本プロファイルと最小プロファイル[3]	VMware ESXi の仮想化プロファイル[4]	Windows プロファイル
アウトバウンド (外部システムでオープンされるポート)	• RHEL KVM ネットワーク・デバイスとの通信 – ポート 53 および 67 の TCP および UDP • SNMP エージェントとの通信 – ポート 161 の UDP • SLP サービス・エージェント、SLP ディレクトリー・エージェントとの通信 – ポート 427 の TCP および UDP • CIM-XML over HTTP 通信 – ポート 15988 および 15989 の TCP • KVM 仮想サーバー通信 – ポート 49152 ～ 49215 の TCP					• SMB 通信 – ポート 445 の TCP
インバウンド (XClarity Administrator アプライアンスで開いたポート)	• SSH – ポート 22 の TCP • RHEL KVM ネットワーク・デバイス – ポート 53 および 67 の TCP および UDP • SNMP エージェント – ポート 162 の UDP • OS デプロイメント – ポート 445、3900、および 8443 の	• SSH – ポート 22 の TCP • OS デプロイメント – ポート 445、3900、および 8443 の TCP および UDP	• OS デプロイメント – ポート 445、3900、および 8443 の TCP および UDP	• OS デプロイメント – ポート 445、3900、および 8443 の TCP および UDP	• OS デプロイメント – ポート 445、3900、および 8443 の TCP および UDP	• OS デプロイメント – ポート 445、3900、および 8443 の TCP および UDP

通信	RHEL、Centos、および Rocky 仮想化プロファイル[1]	RHEL、Centos、および Rocky の基本プロファイルと最小プロファイル[1]	SLES の仮想化、基本プロファイルと最小プロファイル[2]	Ubuntu の仮想化、基本プロファイルと最小プロファイル[3]	VMware ESXi の仮想化プロファイル[4]	Windows プロファイル
	TCP および UDP • SLP サービス・エージェント、SLP ディレクトリー・エージェント ー ポート 427 の TCP および UDP • KVM 仮想サーバー – ポート 49152 ～ 49215 の TCP					

1. デフォルトでは、Red Hat Enterprise Linux (RHEL) プロファイルによって、次の表で一覧されているポート以外のすべてのポートがブロックされます。
2. SUSE Linux Enterprise Server (SLES) の場合、オープン・ポートがオペレーティング・システムのバージョンおよびプロファイルに基づいて、動的に割り当てられます。オープン・ポートのリストについては、SUSE Linux Enterprise Server ドキュメントを参照してください。
3. Ubuntu Linux サーバーの場合、一部のオープン・ポートがオペレーティング・システムのバージョンおよびプロファイルに基づいて、動的に割り当てられます。オープン・ポートの一覧については、「Ubuntu サーバー」ドキュメントを参照してください。
4. Lenovo カスタマイズ版の VMware vSphere Hypervisor (ESXi) のオープン・ポートの一覧については、VMware 知識ベース Web サイト の「ESXi」を参照してください。

リモート・ファイル・サーバーの構成

OS イメージ、デバイス・ドライバー、ブート・ファイルをローカル・システムまたはリモート・ファイル・サーバーから OS イメージ・リポジトリーにインポートできます。リモート・ファイル・サーバーからファイルをインポートするには、まずそのリモート・ファイル・サーバーへの接続の認証に使用されるプロファイルを作成する必要があります。

このタスクについて

次の暗号化アルゴリズムがサポートされています。
- RSA–2048 ビット
- RSA–4096 ビット
- ECDSA–521 ビット (secp521r1 曲線)

以下のプロトコルがサポートされています。
- 認証を使用しない HTTP。
- 基本認証を使用する HTTP。
- 基本認証を使用する HTTPS (証明書の検証)。
- 認証を使用しない HTTPS (証明書の検証)。
- パスワード認証を使用する FTP。

- パスワード認証を使用する SFTP (クライアントの検証)。
- 公開鍵認証を使用する SFTP (クライアントの検証)。

SFTP の公開鍵認証と HTTPS の証明書の検証では、Lenovo XClarity Administrator によりリモート・ファイル・サーバーの証明書が検証されます。サーバー証明書が信頼ストアに存在しない場合、サーバー証明書を受け入れて、信頼ストアに追加するように求められます。検証の問題のトラブルシューティングについて詳しくは、XClarity Administrator オンライン・ドキュメントのサーバー証明書の検証に失敗するを参照してください。

手順

リモート・ファイル・サーバーを構成するには、以下のステップを実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**ファイル・サーバーの構成**」アイコン ( ) をクリックして「リモート・ファイル・サーバーの構成 」ダイアログを表示します。

ステップ 3. 「**リモート・ファイル・サーバーのプロトコル**」リストからリモート・ファイル・サーバーのプロトコルを選択します。

ステップ 4. 「**作成**」をクリックします。「リモート・ファイル・サーバーの構成」ダイアログが表示されます。

注：このダイアログは、選択したプロトコルによって異なります。

ステップ 5. サーバー名、アドレス、ポートを入力します。

ステップ 6. 基本認証を使用する HTTP、HTTPS、FTP、SFTP の場合、サーバーへのアクセスに認証が必要な場合はユーザー名とパスワードを入力します。

ステップ 7. 基本認証を使用する SFTP の場合、「**サーバー証明書の検証**」をクリックして公開鍵署名を取得します。

注：OS デプロイメント・プロセスが SFTP ファイル・サーバーの公開鍵を信頼しないことを示すダイアログが表示される場合があります。「OK」をクリックして、OS デプロイメントのトラステッド鍵ストアの SFTP 公開鍵を保存して信頼します。成功すると、公開鍵署名が「**SFTP サーバーの公開鍵署名**」フィールドに表示されます。

ステップ 8. 公開鍵認証を使用する SFTP の場合

a. サーバーへのアクセスに認証が必要な場合、鍵パスフレーズおよびパスワードを入力して、鍵タイプを選択します。

b. 「**管理サーバー鍵の生成**」をクリックして公開鍵署名を取得します。

c. 生成された鍵を SFTP リモート・ファイル・サーバーの authorized_keys ファイルにコピーします。

d. XClarity Administrator の「**管理鍵がサーバーにコピーされました**」チェックボックスを選択します。

e. 「**サーバー証明書の検証**」をクリックして公開鍵署名を検証します。

注：OS デプロイメント・プロセスが SFTP ファイル・サーバーの公開鍵を信頼しないことを示すダイアログが表示される場合があります。「OK」をクリックして、OS デプロイメントのトラステッド鍵ストアの SFTP 公開鍵を保存して信頼します。成功すると、公開鍵署名が「**SFTP サーバーの公開鍵署名**」フィールドに表示されます。

f. 「**保存**」をクリックします。

ステップ 9. 「**サーバーの保存**」をクリックします。

終了後

「リモート・ファイル・サーバーの構成」ダイアログでは、以下の操作を実行できます。

- リモート・ファイル・サーバーのリストを最新表示にする。「**更新**」アイコン ( ) をクリックします。
- 「**編集**」アイコン ( ) をクリックして、選択されたリモート・ファイル・サーバーを変更します。
- 「**削除**」アイコン ( ) をクリックして、選択されたリモート・ファイル・サーバーを削除します。

オペレーティング・システム・イメージのインポート

XClarity Administrator OS イメージ・リポジトリー でオペレーティング・システムを表示して、ライセンス交付を受けたオペレーティング・システムを管理対象サーバーにデプロイするには、まず、 にイメージをインポートする必要があります。

このタスクについて

インポートおよびデプロイ可能なオペレーティング・システム・イメージについては、サポートされているオペレーティング・システムを参照してください。

サポートされるオペレーティング・システムのリストについては、Lenovo XClarity Administrator オンライン・ドキュメントの 対応オペレーティング・システム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。

一度にインポートできるイメージは 1 つだけです。OS イメージ・リポジトリーにイメージが表示されてから、次のイメージをインポートしてください。オペレーティング・システムのインポートには時間がかかることがあります。

ESXi の場合のみ、同じメジャー/マイナー・バージョンの複数の ESXi イメージを OS イメージ・リポジトリーにインポートできます。

ESXi の場合のみ、メジャー/マイナー・バージョンと build 番号が同じでカスタマイズされた複数の ESXi イメージを OS イメージ・リポジトリーにインポートできます。

オペレーティング・システム・イメージをインポートするとき、XClarity Administrator では、次の処理が実行されます。

- オペレーティング・システムのインポートの前に、OS イメージ・リポジトリー に十分なスペースがあるかどうかを確認する。十分なスペースがない場合は、既存のイメージを削除してからやり直します。

- そのイメージのプロファイルが 1 つ以上作成され、そのプロファイルを OS イメージ・リポジトリーに保存する。各 *プロファイル*には、OS イメージとインストール・オプションが含まれています。事前定義された OS イメージ・プロファイルについて詳しくは、オペレーティング・システム・イメージ・プロファイルを参照してください。

注：Internet Explorer および Microsoft Edge Web ブラウザーには、4 GB のアップロード制限があります。インポートするファイルが 4 GB を超える場合、Chrome や Firefox など、別の Web ブラウザーを使用するか、またはリモート・ファイル・サーバーにファイルをコピーし、「**リモート・インポート**」オプションを使用してインポートすることを検討してください。

手順

OS イメージ・リポジトリーにオペレーティング・システム・イメージをインポートするには、以下の手順を実行します。

ステップ 1. ライセンス交付を受けたオペレーティング・システムの ISO イメージを入手します。

注：該当するオペレーティング・システムのライセンスを取得するのはお客様の責任となります。

ステップ 2. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 3. 「**イメージのインポート**」アイコン () をクリックして、「OS イメージとファイルのインポート」ダイアログを表示します。

ステップ 4. 「**ローカル**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン () をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. パスとイメージ・ファイル名を入力し、「**参照**」をクリックしてインポートする ISO イメージを見つけます。

*ローカル・ファイル・サーバー*を使用する場合、ISO イメージ・ファイルの絶対パスを入力する必要があります。*リモート・ファイル・サーバー*を使用する場合、ISO イメージ・ファイルの絶対パス (例: `/home/user/isos.osimage.iso`) または相対パス (例: `/isos.osimage.iso`) を入力する必要があります (リモート・ファイル・サーバーの構成による)。ファイルが見つからない場合、ファイルのパスが正しいことを確認し、再試行します。

ステップ 7. **オプション**: OS イメージの説明を入力します。

ステップ 8. **オプション**: チェックサム・タイプを選択して、XClarity Administrator にインポートする ISO イメージが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされた OS イメージの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたイメージがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、イメージを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。

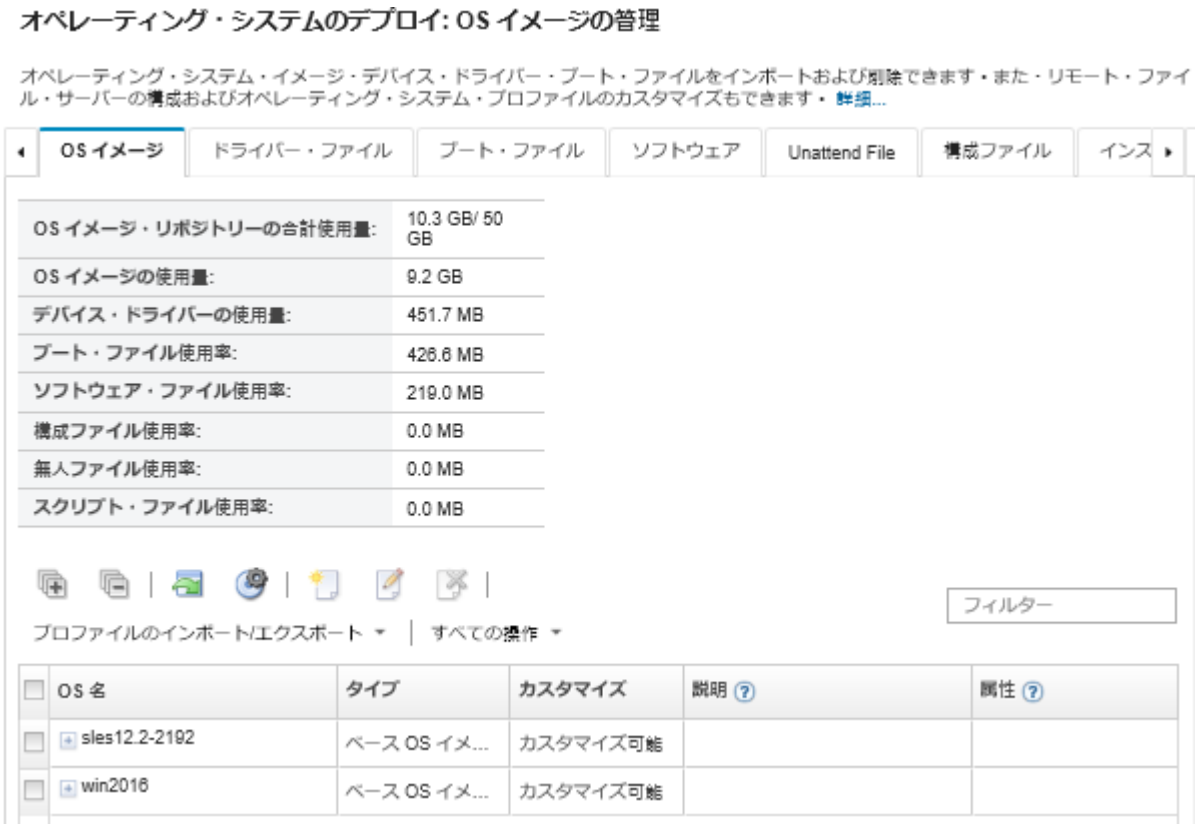
- MD5
- SHA1
- SHA256

ステップ 9. 「**インポート**」をクリックします。

> **ヒント**: ISO イメージのアップロードは、安全なネットワーク接続を介して行われます。このため、イメージのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。オペレーティング・システム・イメージのアップロード中にアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

結果

XClarity Administrator によって、OS イメージがアップロードされ、イメージ・プロファイルが OS イメージ・リポジトリーに作成されます。



このページでは、以下の操作を実行できます。

- 「**ファイル・サーバーの構成**」アイコン ( ) をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。
- 「**カスタマイズされたプロファイルの作成**」アイコン ( ) をクリックして、OS イメージをカスタマイズする。
- 「**編集**」アイコン ( ) をクリックして、OS イメージを変更する。
- 「**プロファイルのインポート/エクスポート**」 → 「**カスタマイズされたプロファイル・イメージのインポート**」をクリックして、カスタマイズされた OS イメージ・プロファイルをインポートし、ベース OS イメージに適用する (カスタマイズされた OS イメージ・プロファイルのインポートを参照)。
- 選択された OS イメージまたはカスタム OS イメージ・プロファイルを削除する。「**削除**」アイコン ( ) をクリックします。

- 選択されたカスタム OS イメージ・プロファイルをエクスポートする。「**プロファイルのインポート/エクスポート**」 ➡ 「**カスタマイズされたプロファイル・イメージのエクスポート**」をクリックします。

注：Windows Server イメージをインポートする際は、関連バンドル・ファイルもインポートする必要があります。Lenovo は事前定義済み WinPE_64.wim ブート・ファイルとデバイス・ドライバーのセットを 1 つのパッケージにバンドルします。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれているので、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・ファイル**」タブからインポートできます。。詳しくは、ブート・ファイルのインポートおよびデバイス・ドライバーのインポートを参照してください。

OS イメージ・プロファイルのカスタマイズ

*ベース・オペレーティング・システム*は、OS イメージ・リポジトリーにインポートされたフル OS イメージです。インポートされたベース・イメージには、そのイメージのインストールの構成を記述する事前定義済みプロファイルが含まれています。また、特定の構成用にカスタム・プロファイルをベース OS イメージ内に作成してデプロイできます。カスタム・プロファイルには、カスタム・ファイルとインストール・オプションが含まれています。

注：カスタム Microsoft Windows サーバー・イメージのカスタム OS イメージ・プロファイルを作成することはできません。

Windows および SLES を含む OS イメージのカスタマイズとデプロイに関するシナリオの複数のサンプルを、英語でのみご用意しています。詳しくは、新しいデバイスをセットアップするためのエンド・ツー・エンドのシナリオを参照してください。

以下のタイプのファイルをカスタム OS イメージ・プロファイルを追加できます。

- **ブート・ファイル**

  ブート・ファイルは、ブートストラップ・インストール環境として機能します。Windows の場合、これは Windows プレインストール (WinPE) ファイルです。WinPE ブート・ファイルは Windows のデプロイに必須です。

  Lenovo XClarity Administrator は事前定義済みブート・ファイルおよびカスタム・ブート・ファイルをサポートします。

  – **事前定義済みブート・ファイル**。Lenovo は、事前定義済み OS イメージ・プロファイルのデプロイに使用できる WinPE_64.wim ブート・ファイルを提供します。

    Lenovo は事前定義済み WinPE_64.wim ブート・ファイルとデバイス・ドライバーのセットを 1 つのパッケージにバンドルします。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれているので、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・ファイル**」タブからインポートできます。

    注：

    – 事前定義済みブート・ファイルは XClarity Administrator にプリロードされていません。Windows プロファイルをデプロイする前に、OS イメージ・リポジトリーにブート・ファイルをインポートする必要があります。
    – XClarity Administrator をインストールした際にロードした事前定義済みブート・ファイルを削除することはできません。ただし、Lenovo バンドルからインポートされた事前定義済みブート・ファイルは削除できます。
    – XClarity Administrator では、インポートされたバンドル・ファイルが Lenovo によって署名されている必要があります。バンドル・ファイルをインポートする際に、.asc 署名ファイルもインポートする必要があります。

– **カスタム・ブート・ファイル**。Windows のデプロイメントのブート・オプションをカスタマイズする WinPE ブート・ファイルを作成できます。その後、カスタム Windows プロファイルにそのブート・ファイルを追加できます。

  XClarity Administrator にはブート・ファイルを正しい形式で作成するためのスクリプトが用意されています。カスタム・ブート・ファイルの作成について詳しくは、ブート (WinPE) ファイルの作成および Window PE (WinPE) の概要 Web サイトを参照してください。

  カスタム・ブート・ファイルのインポートでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているブート・ファイル・タイプ	サポートされているバンドル・ファイル・タイプ
CentOS Linux	サポートされていない	サポートされていない
Microsoft® Windows® Azure Stack HCI	サポートされていない	サポートされていない
Microsoft Windows Hyper-V Server	**genimage.cmd** スクリプトを使用して作成された WinPE ファイルを含む .zip ファイル	デバイス・ドライバーおよびブート・ファイルを含む .zip ファイル
Microsoft Windows Server	**genimage.cmd** スクリプトを使用して作成された WinPE ファイルを含む .zip ファイル	デバイス・ドライバーおよびブート・ファイルを含む .zip ファイル
Red Hat® Enterprise Linux (RHEL) サーバー	サポートされていない	サポートされていない
Rocky Linux	サポートされていない	サポートされていない
SUSE® Linux Enterprise Server (SLES)	サポートされていない	サポートされていない
Ubuntu	サポートされていない	サポートされていない
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	サポートされていない	サポートされていない

- **デバイス・ドライバー**

  デプロイするオペレーティング・システム・イメージに、ハードウェア環境に合ったイーサネット、Fibre Channel およびストレージ・アダプターのデバイス・ドライバーが含まれていることを確認する必要があります。I/O アダプター・デバイス・ドライバーがオペレーティング・システムのイメージまたはプロファイルに含まれていない場合、アダプターは OS デプロイメントではサポートされません。必要なアウト・オブ・ボックス・デバイス・ドライバーが含まれているカスタム OS イメージ・プロファイルを作成できます。

  Lenovo XClarity Administrator は、事前定義済みまたはカスタムのアウト・オブ・ボックスデバイス・ドライバーと同様に、インボックス・デバイス・ドライバーもサポートします。

  – **インボックス・デバイス・ドライバー**。XClarity Administrator はインボックス・デバイス・ドライバーを管理しません。必要な最新のインボックス・デバイス・ドライバーを使用できるよう、必ず、最新のオペレーティング・システムをインストールしてください。

    注：カスタム WinPE ブート・ファイルを作成して、デバイス・ドライバー・ファイルを `C:\drivers` ディレクトリー内のホスト・システムにコピーすることで、インボックス・デバイス・ドライバーをカスタマイズされた Windows プロファイルに追加できます。カスタム・ブート・ファイルを使用するカスタム OS イメージ・プロファイルを作成すると、C:\drivers ディレクトリーにあるデバイス・ドライバーが WinPE および最終的な OS の両方に含まれます。これらはインボックスとして扱われます。そのため、カスタム OS イメージ・プロファイルの作成に使用するデバイス・ドライバーを指定する際に、これらのインボックス・デバイス・ドライバーを XClarity Administrator にインポートする必要はありません。

- **事前定義済みデバイス・ドライバー**。ThinkSystem サーバーの場合、XClarity Administrator には、オペレーティング・システムのインストール、および最終オペレーティング・システム用の基本ネットワークとストレージを構成できる、Linux 用のアウト・オブ・ボックス・デバイス・ドライバーのセットがプリロードされています。これらの事前定義済みデバイス・ドライバーをカスタム OS イメージ・プロファイルに追加して、ご使用の管理対象サーバーにプロファイルをデプロイできます。

  Lenovo はまた、事前定義済みデバイス・ドライバーのセットを 1 つのパッケージにバンドルしています。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。現在、バンドル・ファイルは Windows でのみ使用できます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれている場合、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・イメージ**」タブからインポートできます。

  注：

  - デフォルトでは、事前定義された OS イメージ・プロファイルには、事前定義済みデバイス・ドライバーが含まれます。
  - XClarity Administrator をインストールした際にロードした事前定義済みデバイス・ドライバーを削除することはできません。ただし、Lenovo バンドルからインポートされた事前定義済みデバイス・ドライバーは削除できます。
  - XClarity Administrator では、インポートされたバンドル・ファイルが Lenovo によって署名されている必要があります。バンドル・ファイルをインポートする際に、.asc 署名ファイルもインポートする必要があります。
- **カスタム・デバイス・ドライバー**。アウト・オブ・ボックス・デバイス・ドライバーを OS イメージ・リポジトリーにインポートし、カスタム OS イメージ・プロファイルにそれらのデバイス・ドライバーを追加できます。

  デバイス・ドライバーは Lenovo YUM リポジトリー Web ページ やベンダー (Red Hat など) から入手するか、独自に生成したカスタム・デバイス・ドライバーを使用して入手できます。一部の Windows デバイス・ドライバーの場合、デバイス・ドライバーをインストール実行ファイルからローカル・システムに抽出して .zip アーカイブ・ファイルを作成することにより、カスタム・デバイス・ドライバーを生成できます。

  カスタム・デバイス・ドライバーのインポートでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているデバイス・ドライバー・ファイルのタイプ
CentOS Linux	サポートされていない
Microsoft® Windows® Azure Stack HCI	サポートされていない
Microsoft Windows Hyper-V Server	ロー・デバイス・ドライバー・ファイル (通常、.Inf、.cat、および .dll ファイルのグループ化) を含む .zip ファイルです。
Microsoft Windows Server	ロー・デバイス・ドライバー・ファイル (通常、.Inf、.cat、および .dll ファイルのグループ化) を含む .zip ファイルです。
Red Hat® Enterprise Linux (RHEL) サーバー	.rpm または .iso イメージ形式のドライバー更新ディスク (DUD) **注：**DUD .rpm をカスタム・プロファイルを適用する場合は、最終的なオペレーティング・システムにのみ .rpm がインストールされます。インストール環境 (initrd) にはインストールされません。Initrd にカスタム・デバイス・ドライバーをインストールするには、DUD .iso をインポートし、カスタム・プロファイルに .iso を適用します。
Rocky Linux	サポートされていない

オペレーティング・システム	サポートされているデバイス・ドライバー・ファイルのタイプ
SUSE® Linux Enterprise Server (SLES)	.rpm または .iso イメージ形式のドライバー更新ディスク (DUD) **注：**DUD .rpm をカスタム・プロファイルを適用する場合は、最終的なオペレーティング・システムにのみ .rpm がインストールされます。インストール環境 (initrd) にはインストールされません。Initrd にカスタム・デバイス・ドライバーをインストールするには、DUD .iso をインポートし、カスタム・プロファイルに .iso を適用します。
Ubuntu	サポートされていない
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	.vib イメージ形式のデバイス・ドライバー

注：OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

- **カスタム構成設定**

  構成設定には、OS デプロイメント中に動的に収集する必要があるデータについて記述されています。Lenovo XClarity Administrator は、共通、ネットワーク、および格納場所などの設定を含む一連の事前定義済み構成設定を使用します。これらの事前定義済み構成設定を使用して、XClarity Administrator

  カスタム構成設定は JSON スキーマの形式で定義されます。スキーマは JSON 仕様に準拠する必要があります。

  カスタム構成設定を XClarity Administrator にインポートすると、XClarity Administrator によって JSON スキーマが検証されます。検証に合格した場合、XClarity Administrator は設定ごとにカスタム・マクロを生成します。

  無人ファイルおよびポスト・インストール・スクリプトでは、カスタム・マクロでを使用できます。

  無人ファイル

  カスタム構成ファイルを無人ファイルに関連付けて、これらのカスタム・マクロ (および事前定義済みマクロ) をその無人ファイルに含めることができます。

  カスタム・プロファイルには、1 つ以上のカスタム構成設定ファイルを追加できます。一連のターゲット・サーバーに OS プロファイルをデプロイする場合、使用する構成設定ファイルを選択できます。XClarity Administrator は、構成設定ファイルの JSON スキーマに基づいて「OS イメージのデプロイ」タブに「**カスタム設定**」タブを生成します。これによって、ファイル内に定義された各設定 (JSON オブジェクト) の値を指定できます。

  注：必須のカスタム構成設定のいずれかに指定が入力されていない場合、OS デプロイメントは進行されません。

  ポスト・インストール・スクリプト

  OS デプロイメント中にデータが収集された後、XClarity Administrator によって、ポスト・インストール・スクリプトが使用するホスト・システムに構成設定ファイル (選択されたファイルのカスタム設定および事前定義済み設定のサブセットを含む) のインスタンスが作成されます。

  注：

  – 構成設定ファイルはカスタム OS イメージ・プロファイルに固有です。
  – 事前定義済み OS イメージ・プロファイルの構成設定は変更できません。
  – 構成設定では、以下のオペレーティング・システムのみがサポートされています。
    – Microsoft® Windows® Server
    – Red Hat® Enterprise Linux (RHEL) サーバー
    – Rocky Linux
    – SUSE® Linux Enterprise Server (SLES)

– Lenovo Customization 6.0u3 以降の更新および 6.5 以降を実行する VMware vSphere® Hypervisor (ESXi)

OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

- **カスタム無人ファイル**

  OS イメージ・プロファイルをカスタマイズして、無人ファイルを使用してオペレーティング・システムのデプロイメントを自動化できます。

  カスタム無人ファイルでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft Windows Server	Unattend (.xml)	無人ファイルについて詳しくは、無人 Windows セットアップのリファレンス Web ページを参照してください。
Red Hat® Enterprise Linux (RHEL) サーバー	Kickstart (.cfg)	無人ファイルについて詳しくは、Red Hat: Kickstart を使用したインストールの自動化 Web ページを参照してください。ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 – 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 – 推奨される **#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 – 推奨される **#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。
Rocky Linux	Kickstart (.cfg)	無人ファイルについて詳しくは、Red Hat: Kickstart を使用したインストールの自動化 Web ページを参照してください。ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 – 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 – 推奨される **#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 – 推奨される **#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	無人ファイルについて詳しくは、SUSE: AutoYaST Web ページを参照してください。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	Kickstart (.cfg)	ESXi 6.0u3 およびそれ以降の更新と、6.5 以降でのみサポートされています。 無人ファイルについて詳しくは、VMware: スクリプトを使用したホストの インストールまたはアップグレード Web ページを参照してください。 ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 – 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 – 推奨される **#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 – 推奨される **#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。

注意：

– オブジェクトの固有名を使用して、無人ファイルに事前定義済みおよびカスタム・マクロ (構成設定) を挿入できます。事前定義済みの値は XClarity Administrator インスタンスに基づいて動的に変化します。カスタム・マクロは、OS のデプロイ時に指定されたユーザー入力に基づいて動的に変化します。

注：

– マクロ名は、ハッシュ記号 (#) で囲みます。
– ネストされたオブジェクトの場合は、各オブジェクト名をピリオドで区切ります (例: **#server_settings.server0.locale#**)。
– カスタム・オブジェクト名の場合、最上部のオブジェクト名は含めません。事前定義済みのマクロには、マクロ名にプレフィックス「predefined」を付けます。
– テンプレートからオブジェクトが作成されると、0 から固有番号名が付加されます (例: **server0**、**server1**)。
– 各カスタム設定の隣にある「ヘルプ」アイコン ( ) にマウスを合わせることで、「OS イメージのデプロイ」ダイアログの「カスタム設定」タブから、各マクロの名前を確認できます。
– 事前定義済みマクロのリストについては、事前定義済みマクロを参照してください。カスタム構成設定およびマクロについては、カスタム・マクロを参照してください。

– XClarity Administrator は、OS インストーラーからのステータスの通信、およびその他の重要なインストール手順で使用される以下の事前定義済みマクロを提供します。これらのマクロを無人ファイルに含めることを強くお勧めします (事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照)。
  – #predefined.unattendSettings.preinstallConfig#
  – #predefined.unattendSettings postinstallConfig#

- **カスタム・インストール・スクリプト**

  OS イメージ・プロファイルをカスタマイズして、OS デプロイメントの完了後にインストール・スクリプトを実行できます。

現時点では、ポスト・インストール・スクリプトのみがサポートされています。

次の表は、Lenovo XClarity Administrator が各オペレーティング・システムでサポートしているインストール・スクリプトのファイルタイプのリストです。特定のオペレーション・システムのバージョンでは、XClarity Administrator でサポートされているすべてのファイル・タイプを必ずしもサポートしないことに注意してください (たとえば、一部の RHEL バージョンでは、最小プロファイルに Perl が含まれず、したがって、Perl スクリプトが実行されません)。デプロイするオペレーティング・システムのバージョンに合ったファイル・タイプを使用していることを確認してください。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft® Windows® Server	コマンド・ファイル (.cmd)、PowerShell (.ps1)	デフォルトのカスタム・データとファイルのパスは `C:\lxca` です。 インストール・スクリプトについて詳しくは、Windows セットアップへのカスタム・スクリプトの追加 Web ページを参照してください。
Red Hat® Enterprise Linux (RHEL) サーバー	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。 インストール・スクリプトについて詳しくは、RHEL: ポスト・インストール・スクリプト Web ページを参照してください。
Rocky Linux	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。 インストール・スクリプトについて詳しくは、RHEL: ポスト・インストール・スクリプト Web ページを参照してください。
SUSE® Linux Enterprise Server (SLES)	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。 インストール・スクリプトについて詳しくは、SUSE: カスタム・ユーザー・スクリプト Web ページを参照してください。
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	Bash (.sh)、Python (.py)	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。 インストール・スクリプトについて詳しくは、VMware: インストールとアップグレード・スクリプト Web ページを参照してください。

- **カスタム・ソフトウェア**

  OS イメージ・プロファイルをカスタマイズして、OS デプロイメントおよびポスト・インストール・スクリプトの完了後にカスタム・ソフトウェア・ペイロードをインストールできます。

カスタム・ソフトウェアでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft Windows® Server	ソフトウェア・ペイロードを含む .zip ファイル。	デフォルトのカスタム・データとファイルのパスは `C:\lxca` です。
Red Hat® Enterprise Linux (RHEL) サーバー	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
SUSE® Linux Enterprise Server (SLES)	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
Rocky Linux	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。

カスタマイズされた OS イメージ・プロファイルのインポート

カスタマイズされた OS イメージ・プロファイルをインポートし、既存の互換ベース OS イメージに追加できます。

このタスクについて

カスタム・プロファイルをインポートする前に、ベース OS イメージをインポートする必要があります。

カスタム OS イメージ・プロファイルは、同じタイプのベース OS イメージにのみ追加できます。たとえば、エクスポートされたプロファイルが Windows 2016 イメージ用の場合、そのプロファイルは OS イメージ・リポジトリー内の既存の Windows 2016 イメージにのみインポートおよび追加できます。

OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限にカスタム・プロファイルを保存できます。

手順

カスタマイズされた OS イメージ・プロファイルをインポートするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**OS イメージ**」タブで、カスタマイズされた OS イメージ・プロファイルを追加するベース OS イメージを選択します。

ステップ 3. 「**プロファイルのインポート/エクスポート**」 → 「**カスタマイズされたプロファイル・イメージのインポート**」をクリックします。「カスタマイズされた OS イメージ・プロファイルのインポート」ダイアログが表示されます。

ステップ 4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン () をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. プロファイル名を入力し、「**参照**」をクリックしてインポートするプロファイルを見つけます。

ステップ 7. **オプション**: ローカル・インポートの場合、チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。
- MD5
- SHA1
- SHA256

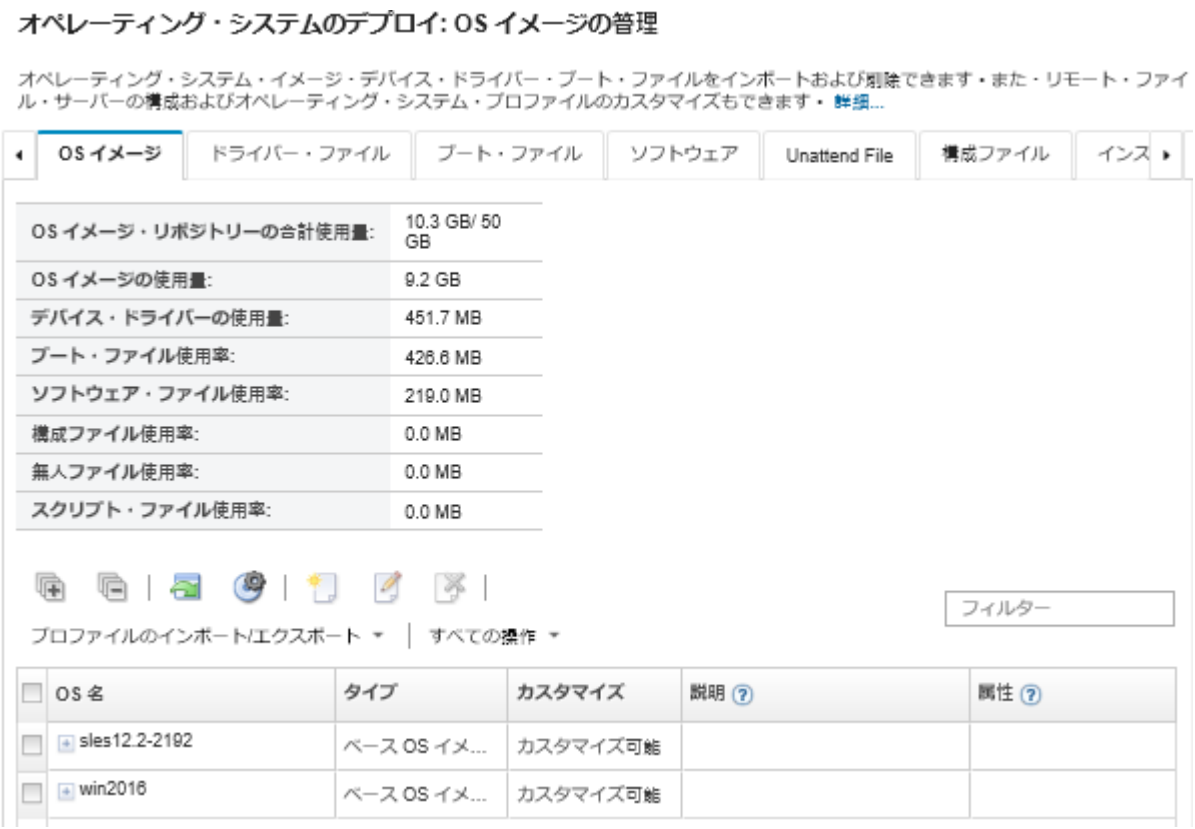
ステップ 8. 「**インポート**」をクリックします。

ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

カスタマイズされた OS イメージは、「OS イメージの管理」ページのベース・オペレーティング・システムの下にリストされます。



このページでは、以下の操作を実行できます。

- カスタマイズされた OS イメージ・プロファイルを作成する (カスタム OS イメージ・プロファイルの作成を参照)。
- 選択されたカスタム OS イメージ・プロファイルをエクスポートする。「**プロファイルのインポート/エクスポート**」 ➡ 「**カスタマイズされたプロファイル・イメージのエクスポート**」をクリックします。

  重要：FTP または SFTP プロトコルを使用するようにセットアップされているリモート・ファイル・サーバーに、カスタマイズされた OS イメージ・プロファイルをエクスポートできます。HTTP または HTTPS を使用するようにセットアップされているリモート・ファイル・サーバーには、エクスポートできません。
- 「**編集**」アイコン ( ) をクリックして、選択済みのカスタマイズされた OS イメージ・プロファイルを変更します。
- 「**削除**」アイコン ( ) をクリックして、選択済みのカスタマイズされた OS イメージ・プロファイルを削除します。

ブート・ファイルのインポート

ブート・ファイルは、OS イメージ・リポジトリーにインポートできます。その後、これらのファイルを使用して Windows イメージをカスタマイズおよびデプロイできます。

このタスクについて

ブート・ファイルは、ブートストラップ・インストール環境として機能します。Windows の場合、これは Windows プレインストール (WinPE) ファイルです。WinPE ブート・ファイルは Windows のデプロイに必須です。

Lenovo XClarity Administrator は事前定義済みブート・ファイルおよびカスタム・ブート・ファイルをサポートします。

- **事前定義済みブート・ファイル**。Lenovo は、事前定義済み OS イメージ・プロファイルのデプロイに使用できる WinPE_64.wim ブート・ファイルを提供します。

  Lenovo は事前定義済み WinPE_64.wim ブート・ファイルとデバイス・ドライバーのセットを 1 つのパッケージにバンドルします。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページからダウンロードして OS イメージ・リポジトリーにインポートできます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれているので、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・ファイル**」タブからインポートできます。

  注：

  – 事前定義済みブート・ファイルは XClarity Administrator にプリロードされていません。Windows プロファイルをデプロイする前に、OS イメージ・リポジトリーにブート・ファイルをインポートする必要があります。

  – XClarity Administrator をインストールした際にロードした事前定義済みブート・ファイルを削除することはできません。ただし、Lenovo バンドルからインポートされた事前定義済みブート・ファイルは削除できます。

  – XClarity Administrator では、インポートされたバンドル・ファイルが Lenovo によって署名されている必要があります。バンドル・ファイルをインポートする際に、.asc 署名ファイルもインポートする必要があります。

- **カスタム・ブート・ファイル**。Windows のデプロイメントのブート・オプションをカスタマイズする WinPE ブート・ファイルを作成できます。その後、カスタム Windows プロファイルにそのブート・ファイルを追加できます。

  XClarity Administrator にはブート・ファイルを正しい形式で作成するためのスクリプトが用意されています。カスタム・ブート・ファイルの作成について詳しくは、ブート (WinPE) ファイルの作成および Window PE (WinPE) の概要 Web サイトを参照してください。

  カスタム・ブート・ファイルのインポートでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているブート・ファイル・タイプ	サポートされているバンドル・ファイル・タイプ
CentOS Linux	サポートされていない	サポートされていない
Microsoft® Windows® Azure Stack HCI	サポートされていない	サポートされていない
Microsoft Windows Hyper-V Server	**genimage.cmd** スクリプトを使用して作成された WinPE ファイルを含む .zip ファイル	デバイス・ドライバーおよびブート・ファイルを含む .zip ファイル
Microsoft Windows Server	**genimage.cmd** スクリプトを使用して作成された WinPE ファイルを含む .zip ファイル	デバイス・ドライバーおよびブート・ファイルを含む .zip ファイル
Red Hat® Enterprise Linux (RHEL) サーバー	サポートされていない	サポートされていない
Rocky Linux	サポートされていない	サポートされていない
SUSE® Linux Enterprise Server (SLES)	サポートされていない	サポートされていない
Ubuntu	サポートされていない	サポートされていない
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	サポートされていない	サポートされていない

注：OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

手順

- OS イメージ・リポジトリーにブート・ファイルを含む Windows バンドル・ファイルをインポートするには、以下の手順を実行します。
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
  2. 「**ブート・ファイル**」タブをクリックします。

  3. 「**ダウンロード**」 ➡ 「**Windows バンドル・ファイル**」をクリックして Lenovo サポート Web ページに移動し、OS イメージに合わせたバンドル・ファイルと関連署名ファイルをローカル・システムにダウンロードします。
  4. 「**バンドル・ファイルのインポート**」アイコン ( ) をクリックします。「バンドル・ファイルのインポート」ダイアログが表示されます。
  5. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

     注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。
  6. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。
  7. リリースするオペレーティング・システム・タイプを選択します。
  8. バンドル・ファイルおよび関連署名ファイルのファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。
  9. **オプション**: バンドル・ファイルの説明を入力します。
  10. 「**インポート**」をクリックします。

      ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

      ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。
- OS イメージ・リポジトリーにブート・ファイルを個別でインポートするには、以下の手順を実行します。
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
  2. 「**ブート・ファイル**」タブをクリックします。

3. 「**ファイルのインポート**」アイコン () をクリックします。「ファイルのインポート」ダイアログが表示されます。
4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

   注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン () をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。
5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。
6. リリースするオペレーティング・システム・タイプを選択します。
7. ファイル名を入力するか、「**参照**」をクリックしてインポートするブート・ファイルを見つけます。
8. **オプション**: ブート・ファイルの説明を入力します。
9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

   チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

   次の 3 つのチェックサム・タイプがサポートされます。
   - MD5
   - SHA1
   - SHA256
10. 「**インポート**」をクリックします。

    ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

    ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

ブート・ファイルは、「OS イメージの管理」ページの「**ブート・ファイル**」タブにリストされます。

このページでは、以下の操作を実行できます。

- 「**ファイル・サーバーの構成**」アイコン () をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。
- 「**削除**」アイコン () をクリックして、選択されたブート・ファイルを削除します。
- カスタマイズされた OS イメージ・プロファイルにブート・ファイルを追加します (カスタム OS イメージ・プロファイルの作成を参照)。

ブート (WinPE) ファイルの作成

Windows イメージのカスタマイズに使用できるブート・ファイルを作成できます。

始める前に

- プロビジョニングするオペレーティング・システムが、ホストにインストールされていることを確認します。たとえば、WinPE ファイルを使用して Windows 2016 をプロビジョニングする場合、ホストに Windows 2016 をインストールします。
- インストールされているオペレーティング・システムと互換性がある Microsoft ADK もホストにインストールされていることを確認します。たとえば、Windows 2012R2 では、ADK バージョン 8.1 の更新が必要です。
- ブート・ファイルに追加するデバイス・ドライバーを .inf 形式で取得します。

  デバイス・ドライバーは Lenovo YUM リポジトリー Web ページ やベンダー (Red Hat など) から入手するか、独自に生成したカスタム・デバイス・ドライバーを使用して入手できます。一部の Windows デバイス・ドライバーの場合、デバイス・ドライバーをインストール実行ファイルからローカル・システムに抽出して .zip アーカイブ・ファイルを作成することにより、カスタム・デバイス・ドライバーを生成できます。

  Lenovo はまた、事前定義済みデバイス・ドライバーのセットを 1 つのパッケージにバンドルしています。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。現在、バンドル・ファイルは Windows でのみ使用できます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれている場合、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・イメージ**」タブからインポートできます。
- `genimage.cmd`、および `startnet.cmd` ファイルを一時ディレクトリのホスト (例: `C:\customwim`) にダウンロードします。

  `genimage.cmd` コマンドは .wim ファイルを含む WinPE ブート・ファイルの生成に使用されます。`startnet.cmd` コマンドは、Windows インストーラーのブートストラップを行うために XClarity Administrator により使用されます。
- ブート・ファイルにデバイス・ドライバーを組み込む方法を決定します。これは、以下のいずれかの方法で行うことができます。
  - デバイス・ドライバー・ファイルを C:\drivers ディレクトリー内のホスト・システムにコピーして、インボックス・デバイス・ドライバーをカスタマイズされた Windows プロファイルに追加します。これらは、後で genimage.cmd が実行される際のブート・ファイルに含まれます。

    注：カスタム・ブート・ファイルを使用するカスタム OS イメージ・プロファイルを作成すると、C:\drivers ディレクトリーにあるデバイス・ドライバーが WinPE および最終的な OS の両方に含まれます。これらはインボックスとして扱われます。そのため、カスタム OS イメージ・プロファイルの作成に使用するデバイス・ドライバーを指定する際に、これらのインボックス・デバイス・ドライバーを XClarity Administrator にインポートする必要はありません。
  - アウト・オブ・ボックス・デバイス・ドライバーをブート・ファイルに直接追加します。

    注：この方法を使用する場合、デバイス・ドライバーはブート・ファイルにのみ適用されるため、WinPE インストール環境に適用されます。デバイス・ドライバーは、最終的なインストール済みの OS には適用されません。デバイス・ドライバーを OS イメージのデバイス・ドライバー・リポジトリーに手動でインポートし、OS イメージプロファイルのカスタマイズの一部として選択する必要があります。
- ブート・ファイルについて詳しくは、Window PE (WinPE) の概要 Web サイトを参照してください。

手順

ブート・ファイルを作成するには、以下の手順を実行します。

ステップ 1. 管理者権限を持つ ID を使用して、Windows ADK コマンド「Deployment and Imaging Tools Environment」を実行します。コマンド・セッションが表示されます。

ステップ 2. コマンド・セッションから、`genimage.cmd` ファイルと `starnet.cmd` ファイルがダウンロードされたディレクトリー (`C:\customwim` など) に移動します。

ステップ 3. 次のコマンドを実行して、以前にマウントされたイメージがホストにないことを確認します。

```
dism /get-mountedwiminfo
```

マウントされたイメージがある場合、以下のコマンドを実行して廃棄します。

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

ステップ 4. インボックス・デバイス・ドライバーをカスタマイズされた Windows プロファイルに追加する場合、ロー・デバイス・ドライバー・ファイル (.inf format 形式) を C:\drivers ディレクトリー内のホスト・システムにコピーします。

ステップ 5. 次のコマンドを実行してブート・ファイル (.wim 形式) を生成し、コマンドが完了するまで数分間待ちます。
```
genimage.cmd amd64 <ADK_Version>
```

ここの *<ADK_Version>* は以下のいずれかの値です。

- **8.1**.Windows 2012 R2 の場合
- **10**.Windows 2016 の場合

このコマンドにより、ブート・ファイル C:\WinPE_64\media\Boot\WinPE_64.wim が作成されます。

ステップ 6. 次のコマンドを実行してブート・ファイルをマウントします。
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

ステップ 7. アウト・オブ・ボックス・デバイス・ドライバーをブート・ファイルに追加する場合、次の手順を実行します。

1. 以下のディレクトリー構造を作成します。*<os_release>* は 2012、2012R2、または 2016 です。
   ```
   drivers\<os_release>\
   ```
2. デバイス・ドライバー (.inf 形式) をパス内のディレクトリーにコピーします。たとえば、次のとおりです。
   ```
   drivers\<os_release>\<driver1>\<driver1_files>
   ```
3. drivers ディレクトリーをマウント・ディレクトリーにコピーします。たとえば、次のとおりです。
   ```
   C:\WinPE_64\mount\drivers
   ```

ステップ 8. フォルダー、ファイル、起動スクリプト、言語パック、アプリの追加など、ブート・ファイルに追加のカスタマイズを行います。ブート・ファイルのカスタマイズについて詳しくは、WinPE: マウントとカスタマイズの Web サイトを参照してください。

ステップ 9. 次のコマンドを実行してイメージをアンマウトします。
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

ステップ 10.C:\WinPE_64\media ディレクトリーの内容を WinPE_64.zip という zip ファイルに圧縮します。

ステップ 11..zip ファイルを XClarity Administrator にインポートします (ブート・ファイルのインポートを参照)。

デバイス・ドライバーのインポート

OS イメージ・リポジトリーには個別のデバイス・ドライバーおよびバンドル・ファイルをインポートできます。その後、これらのファイルを使用して Linux および Windows イメージをカスタマイズできます。

このタスクについて

デプロイするオペレーティング・システム・イメージに、ハードウェア環境に合ったイーサネット、Fibre Channel およびストレージ・アダプターのデバイス・ドライバーが含まれていることを確認する必要があります。I/O アダプター・デバイス・ドライバーがオペレーティング・システムのイメージまたはプロファイルに含まれていない場合、アダプターは OS デプロイメントではサポートされません。

必要なアウト・オブ・ボックス・デバイス・ドライバーが含まれているカスタム OS イメージ・プロファイルを作成できます。

Lenovo XClarity Administrator は、事前定義済みまたはカスタムのアウト・オブ・ボックスデバイス・ドライバーと同様に、インボックス・デバイス・ドライバーもサポートします。

- **インボックス・デバイス・ドライバー**。XClarity Administrator はインボックス・デバイス・ドライバーを管理しません。必要な最新のインボックス・デバイス・ドライバーを使用できるよう、必ず、最新のオペレーティング・システムをインストールしてください。

  注：カスタム WinPE ブート・ファイルを作成して、デバイス・ドライバー・ファイルを `C:\drivers` ディレクトリー内のホスト・システムにコピーすることで、インボックス・デバイス・ドライバーをカスタマイズされた Windows プロファイルに追加できます。カスタム・ブート・ファイルを使用するカスタム OS イメージ・プロファイルを作成すると、C:\drivers ディレクトリーにあるデバイス・ドライバーが WinPE および最終的な OS の両方に含まれます。これらはインボックスとして扱われます。そのため、カスタム OS イメージ・プロファイルの作成に使用するデバイス・ドライバーを指定する際に、これらのインボックス・デバイス・ドライバーを XClarity Administrator にインポートする必要はありません。

- **事前定義済みデバイス・ドライバー**。ThinkSystem サーバーの場合、XClarity Administrator には、オペレーティング・システムのインストール、および最終オペレーティング・システム用の基本ネットワークとストレージを構成できる、Linux 用のアウト・オブ・ボックス・デバイス・ドライバーのセットがプリロードされています。これらの事前定義済みデバイス・ドライバーをカスタム OS イメージ・プロファイルに追加して、ご使用の管理対象サーバーにプロファイルをデプロイできます。

  Lenovo はまた、事前定義済みデバイス・ドライバーのセットを 1 つのパッケージにバンドルしています。これは Lenovo Windows ドライバーおよび WinPE イメージ・リポジトリー Web ページ からダウンロードして OS イメージ・リポジトリーにインポートできます。現在、バンドル・ファイルは Windows でのみ使用できます。バンドル・ファイルにデバイス・ドライバーとブート・ファイルの両方が含まれている場合、バンドル・ファイルを「**デバイス・ドライバー**」タブまたは「**ブート・イメージ**」タブからインポートできます。

  注：

  - デフォルトでは、事前定義された OS イメージ・プロファイルには、事前定義済みデバイス・ドライバーが含まれます。
  - XClarity Administrator をインストールした際にロードした事前定義済みデバイス・ドライバーを削除することはできません。ただし、Lenovo バンドルからインポートされた事前定義済みデバイス・ドライバーは削除できます。
  - XClarity Administrator では、インポートされたバンドル・ファイルが Lenovo によって署名されている必要があります。バンドル・ファイルをインポートする際に、.asc 署名ファイルもインポートする必要があります。

- **カスタム・デバイス・ドライバー**。アウト・オブ・ボックス・デバイス・ドライバーを OS イメージ・リポジトリーにインポートし、カスタム OS イメージ・プロファイルにそれらのデバイス・ドライバーを追加できます。

  デバイス・ドライバーは Lenovo YUM リポジトリー Web ページ やベンダー (Red Hat など) から入手するか、独自に生成したカスタム・デバイス・ドライバーを使用して入手できます。一部の Windows デバイス・ドライバーの場合、デバイス・ドライバーをインストール実行ファイルからローカル・システムに抽出して .zip アーカイブ・ファイルを作成することにより、カスタム・デバイス・ドライバーを生成できます。

  カスタム・デバイス・ドライバーのインポートでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているデバイス・ドライバー・ファイルのタイプ
CentOS Linux	サポートされていない
Microsoft® Windows® Azure Stack HCI	サポートされていない

オペレーティング・システム	サポートされているデバイス・ドライバー・ファイルのタイプ
Microsoft Windows Hyper-V Server	ロー・デバイス・ドライバー・ファイル (通常、.Inf、.cat、および .dll ファイルのグループ化) を含む .zip ファイルです。
Microsoft Windows Server	ロー・デバイス・ドライバー・ファイル (通常、.Inf、.cat、および .dll ファイルのグループ化) を含む .zip ファイルです。
Red Hat® Enterprise Linux (RHEL) サーバー	.rpm または .iso イメージ形式のドライバー更新ディスク (DUD) **注：**DUD .rpm をカスタム・プロファイルを適用する場合は、最終的なオペレーティング・システムにのみ .rpm がインストールされます。インストール環境 (initrd) にはインストールされません。Initrd にカスタム・デバイス・ドライバーをインストールするには、DUD .iso をインポートし、カスタム・プロファイルに .iso を適用します。
Rocky Linux	サポートされていない
SUSE® Linux Enterprise Server (SLES)	.rpm または .iso イメージ形式のドライバー更新ディスク (DUD) **注：**DUD .rpm をカスタム・プロファイルを適用する場合は、最終的なオペレーティング・システムにのみ .rpm がインストールされます。インストール環境 (initrd) にはインストールされません。Initrd にカスタム・デバイス・ドライバーをインストールするには、DUD .iso をインポートし、カスタム・プロファイルに .iso を適用します。
Ubuntu	サポートされていない
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	.vib イメージ形式のデバイス・ドライバー

注：OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

手順

- OS イメージ・リポジトリーにデバイス・ドライバーを含む Windows バンドル・ファイルをインポートするには、以下の手順を実行します。
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
  2. 「**ドライバー・ファイル**」タブをクリックします。

3. 「**ダウンロード**」 → 「**Windows バンドル・ファイル**」をクリックして Lenovo サポート Web ページに移動し、OS イメージに合わせたバンドル・ファイルと関連署名ファイルをローカル・システムにダウンロードします。
4. 「**バンドル・ファイルのインポート**」アイコン ( ) をクリックします。「バンドル・ファイルのインポート」ダイアログが表示されます。
5. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

   注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。
6. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。
7. リリースするオペレーティング・システム・タイプを選択します。
8. バンドル・ファイルおよび関連署名ファイルのファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。
9. **オプション**: バンドル・ファイルの説明を入力します。
10. 「**インポート**」をクリックします。

    ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

    ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

- OS イメージ・リポジトリーにデバイス・ドライバーを個別でインポートするには、以下の手順を実行します。
  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
  2. 「**ドライバー・ファイル**」タブをクリックします。

3. 「**ファイルのインポート**」アイコン () をクリックします。「ファイルのインポート」ダイアログが表示されます。
4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

   注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン () をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。
5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。
6. リリースするオペレーティング・システム・タイプを選択します。
7. ファイル名を入力するか、「**参照**」をクリックしてインポートするデバイス・ドライバーを見つけます。
8. **オプション**: デバイス・ドライバーの説明を入力します。
9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

   チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

   次の 3 つのチェックサム・タイプがサポートされます。
   - MD5
   - SHA1
   - SHA256
10. 「**インポート**」をクリックします。

    ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

    ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

デバイス・ドライブ・イメージは、「OS イメージの管理」ページの「**ドライバー・ファイル**」タブにリストされます。

このページでは、以下の操作を実行できます。

- 「**ファイル・サーバーの構成**」アイコン () をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。
- 「**削除**」アイコン () をクリックして、選択されたデバイス・ドライバーを削除します。
- カスタマイズされた OS イメージ・プロファイルにデバイス・ドライバーを追加します (カスタム OS イメージ・プロファイルの作成を参照)。

カスタム構成設定のインポート

構成設定には、OS デプロイメント中に動的に収集する必要があるデータについて記述されています。Lenovo XClarity Administrator は、共通、ネットワーク、および格納場所などの設定を含む一連の事前定義

済み構成設定を使用します。これらの事前定義済み構成設定を使用して、XClarity Administrator 経由では使用できないカスタム構成設定を追加できます。

このタスクについて

カスタム構成設定は JSON スキーマの形式で定義されます。スキーマは JSON 仕様に準拠する必要があります。

カスタム構成設定を XClarity Administrator にインポートすると、XClarity Administrator によって JSON スキーマが検証されます。検証に合格した場合、XClarity Administrator は設定ごとにカスタム・マクロを生成します。

無人ファイルおよびポスト・インストール・スクリプトでは、カスタム・マクロでを使用できます。

無人ファイル

カスタム構成ファイルを無人ファイルに関連付けて、これらのカスタム・マクロ (および事前定義済みマクロ) をその無人ファイルに含めることができます。

カスタム・プロファイルには、1 つ以上のカスタム構成設定ファイルを追加できます。一連のターゲット・サーバーに OS プロファイルをデプロイする場合、使用する構成設定ファイルを選択できます。XClarity Administrator は、構成設定ファイルの JSON スキーマに基づいて「OS イメージのデプロイ」タブに「**カスタム設定**」タブを生成します。これによって、ファイル内に定義された各設定 (JSON オブジェクト) の値を指定できます。

注：必須のカスタム構成設定のいずれかに指定が入力されていない場合、OS デプロイメントは進行されません。

ポスト・インストール・スクリプト

OS デプロイメント中にデータが収集された後、XClarity Administrator によって、ポスト・インストール・スクリプトが使用するホスト・システムに構成設定ファイル (選択されたファイルのカスタム設定および事前定義済み設定のサブセットを含む) のインスタンスが作成されます。

注：

- 構成設定ファイルはカスタム OS イメージ・プロファイルに固有です。
- 事前定義済み OS イメージ・プロファイルの構成設定は変更できません。
- 構成設定では、以下のオペレーティング・システムのみがサポートされています。
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) サーバー
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - Lenovo Customization 6.0u3 以降の更新および 6.5 以降を実行する VMware vSphere® Hypervisor (ESXi)

OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

手順

OS イメージ・リポジトリーに構成設定ファイルをインポートするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**構成設定**」タブをクリックします。

ステップ 3. 「**ファイルのインポート**」アイコン ( ) をクリックします。「構成設定のインポート」ダイアログが表示されます。

ステップ 4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. オペレーティング・システム・タイプを選択します。

ステップ 7. 構成設定ファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。

ステップ 8. **オプション**: 構成設定の説明を入力します。

ヒント:「**説明**」フィールドを使用して、同じ名前のカスタム・ファイルを区別できます。

ステップ 9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。
- MD5
- SHA1
- SHA256

ステップ 10.「**インポート**」をクリックします。ファイルをインポートすると、JSON 形式が検証されます。エラーが検出された場合は、エラー・メッセージとロケーションを示すダイアログが表示されます。

ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

注意：ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

構成設定ファイルは、「OS イメージの管理」ページの「**構成設定**」タブにリストされます。

このページでは、以下の操作も実行できます。

- 構成設定ファイルを作成する。「**作成**」アイコン () をクリックして、ファイル名、説明、OS タイプ、および構成設定と値を指定します。「**検証**」をクリックしてスキーマを検証してから、ファイルを保存します。

  エディターは、ファイル内で検出されたすべてのエラーの位置を識別します。一部のメッセージは英語のみであることに注意してください。
- 構成設定ファイルを表示および変更する。「**編集**」アイコン () をクリックします。

  無人ファイルに関連付けられている構成設定ファイルは編集できません。

  エディターは、ファイル内で検出されたすべてのエラーの位置を識別します。一部のメッセージは英語のみであることに注意してください。
- 構成設定ファイルをコピーする。「**コピー**」アイコン () をクリックします。

  無人ファイルに関連付けられている構成設定ファイルをコピーすると、関連する無人ファイルもコピーされ、コピーした両方のファイルの間で関連付けが自動的に作成されます。
- 選択された構成設定ファイルを削除する。「**削除**」アイコン () をクリックします。
- 「**ファイル・サーバーの構成**」アイコン () をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。

カスタマイズされた OS イメージ・プロファイルへの構成設定の追加については、カスタム OS イメージ・プロファイルの作成を参照してください。

カスタム・マクロ

*マクロ*により、無人ファイルまたはポスト・インストール・スクリプトに、変数データ (構成設定) を追加できます。Lenovo XClarity Administrator では、JSON 形式を使用してカスタム構成設定ファイルを作成することで、独自のカスタム設定を定義できます。

各カスタム構成設定値は、OS デプロイメント中に指定されたユーザー入力に応じて異なります。

カスタム構成設定を XClarity Administrator にインポートすると、XClarity Administrator によって JSON スキーマが検証されます。検証に合格した場合、XClarity Administrator は設定ごとにカスタム・マクロを生成します。

無人ファイルまたはポスト・インストール・スクリプトにカスタム・マクロを挿入するには、オブジェクトの一意名を使用し、ピリオドでネストされたオブジェクトを分割して、ハッシュ記号 (#) でマクロ名を囲みます。例: **#server_settings.server0.locale#**。

注：

- 一番上のオブジェクト名を含めないでください。
- テンプレートからオブジェクトが作成されると、0 から固有番号名が付加されます (例: server0、server1)。
- 各カスタム設定の隣にある「**ヘルプ**」アイコン () にマウスを合わせることで、「OS イメージのデプロイ」ダイアログの「カスタム設定」タブから、各マクロの名前を確認できます。

構成設定

以下のカスタム構成設定を定義できます。

- すべてのターゲット・サーバーに共通の設定または特定のターゲット・サーバーに固有の設定。
- 静的 (構成不能) 値、またはOS イメージ・プロファイルのデプロイ時に入力される動的 (構成可能) 値。
- テンプレートに応じて異なる要素数。たとえば、デプロイメント時に 0 ～ 3 台 NTP サーバーを指定する構成設定を定義できます。

共通設定

OS デプロイメント中に、**content** オブジェクトに示されたオブジェクトに基づいて、「OS イメージのデプロイ」ダイアログに「**共通設定**」タブの UI 要素が生成されます。オブジェクトは、すべてのターゲット・サーバーが OS デプロイメントに必要とする設定と値を説明します。

全てのサーバーに共通の設定を示すには、JSON ファイルに親オブジェクトと `"common":true` 名前/値のペアを含むネストされたオブジェクトが含まれる必要があります。

次の例では、すべてのサーバーに同じ構成可能な (動的) NTP サーバーを使用します。

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
      "autoCreateInstance": true,
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string"
    }],
    "type": "array"
  },
  ...,
}
```

次の例では、同じ非構成 (静的) ポスト・インストール・スクリプトのログ・ディレクトリーを使用します。

```
{
  "category": "dynamic",
  "content": [{
    "category": "static",
    "common": true,
    "description": "Directory location for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
  },
```

```
  ...,
}
```

サーバー固有設定

OS デプロイメント中に、テンプレートの **content** オブジェクトに示されたオブジェクトに基づいて、「OS イメージのデプロイ」ダイアログに「**サーバー固有設定**」タブの UI 要素が生成されます。オブジェクトは、固有のターゲット・サーバーが OS デプロイメントに必要とする設定と値を説明します。

サーバー固有の値が UI に収集された後、**template** オブジェクトに基づいて、各ターゲット・サーバーの **content** オブジェクトが JSON で作成されます。各 **content** オブジェクトには、固有の **name** および **targetServer** フィールド、およびそのサーバー用に入力された値が含まれています。

サーバー固有の設定を示すには、JSON ファイルに次の内容を含む親オブジェクトが含まれる必要があります。

- `"category":"dynamic"` 名/値のペア。
- `"common":false` 名/値のペアを含むネストされたオブジェクト。1 つの `"common": false` オブジェクトのみが親オブジェクトのコンテンツでサポートされています。
- 組み込みコンテンツ・オブジェクトを使用するテンプレート・オブジェクト。このテンプレートアレイには、1 つのオブジェクトのみを含めることができます。

たとえば、各ターゲット・サーバーに固有の OS ロケールを定義する場合

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      }],
      "name": "server",
      "optional": false,
      "type": "assoc_array"
    }],
    "type": "assoc_array"
  },
  ...,
}
```

JSON 仕様

次の表では、JSON 仕様で許可されているフィールドについて説明します。

パラメーター	必須/オプション	タイプ	説明
autoCreateInstance	オプションの	ブール	デプロイメント時にテンプレート・オブジェクトのインスタンスが自動的に JSON ファイルで作成されるかどうかを示します。これは以下のいずれかの値です。 • **true**。デプロイメント時にテンプレート・オブジェクトのインスタンスが自動的に JSON ファイルで作成されます。 • **false**。(デフォルト) デプロイメント時にテンプレート・オブジェクトのインスタンスは自動的に JSON ファイルで作成*されません*。 **注：**このフィールドは、テンプレート・オブジェクトにのみ含めることができます。
category	必須	ストリング	各設定の値の入力方法を示します。これは以下のいずれかの値です。 • **dynamic**。値はユーザーによって実行時に入力されます。Lenovo XClarity Administrator によって OS デプロイメント中にこの値の入力を求められます。 • **predefined**。値は Lenovo XClarity Administrator によって事前設定されます。 • **static**。値はスキーマで指定され、実行時に変更されません。 ネストされたオブジェクトは、このフィールドの値を親オブジェクトから継承します。 親オブジェクトで **category** が `static` に設定されている場合、すべてのネストされたオブジェクトでも `static` に設定される必要があります。親オブジェクトで **category** が `dynamic` に設定されている場合、ネストされたオブジェクトでは `static` または `dynamic` のいずれかに設定できます。
choices	オプションの	**type** プロパティに一致する値の配列	ユーザーが OS デプロイメント中に選択できる構成設定の固定値の配列 (文字列または整数など) (例: `["enabled","disabled"]`)。
common	オプションの	ブール	すべてのターゲット・サーバーにこの構成スキーマが適用されるかどうかを示します。 • **true**。オブジェクトはすべてのターゲット・サーバーに適用されます。 • **false**。(デフォルト) オブジェクトは特定のターゲット・サーバーに適用されます。 ネストされたオブジェクトは、このフィールドの値を親オブジェクトから継承します。 親オブジェクトで **common** が `true` に設定されている場合、すべてのネストされたオブジェクトでも `true` に設定される必要があります。親オブジェクトで **common** が `false` に設定されている場合、すべてのネストされたオブジェクトで `false` に設定される必要があります。
content	オプションの	オブジェクトのアレイ	スキーマのネストされたオブジェクトを表すパターン。OS デプロイメント中にユーザー入力データが収集された後、このフィールドは、デプロイメント用に作成された構成設定ファイルのインスタンスの指定されたテンプレートの最終値を示すために使用されます。

パラメーター	必須/オプション	タイプ	説明
default	オプションの	値は **type** によって異なります。	デフォルト値。
description	オプションの	ストリング	オブジェクトの説明
label	オプションの	ストリング	OS デプロイメント中に表示されているユーザー・インターフェースの設定のラベル
max	オプションの	整数	**type** が整数に設定されている場合の最大値。 デフォルト値は無制限です。
maxElements	オプションの	整数	このオブジェクトのアレイ内のエントリーの最大数。
min	オプションの	整数	**type** が整数に設定されている場合の最小値。 デフォルト値は 0 です。
minElements	オプションの	整数	このオブジェクトのアレイ内のエントリーの最小数。
name	必須	ストリング	オブジェクトの個有名。 この名前は、次の文字のみを含めることができます。英数字 (a ～ z、A ～ Z、および 0 ～ 9)、下線 (_)、ダッシュ (-)。 **name** は無人ファイルでカスタム・マクロとして参照できます。ネストされた **name** オブジェクトを参照する場合は、各オブジェクトをピリオドで区切ります (例: `mydeploy.node.locale`)。
optional	必須	ブール	オブジェクトがオプションであるかどうかを示します。これは以下のいずれかの値です。 • **true**。このフィールドはオプションです • **false**。このフィールドは必須です。
regex	オプションの	ストリング	値を検証する正規表現 (例: `"[\\w\\.]{1,64}$"`)
script	オプションの	ストリングのアレイ	このオブジェクトのデータに依存している、コンマで区切ったスクリプトのリスト (例: `["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]`)。 **注：** スクリプトは、インストール・スクリプトまたはカスタム・ソフトウェアとして OS イメージ・プロファイルで使用できる必要があります。
targetServer	オプションの	ストリング	OS デプロイメントのターゲットであるサーバーの UUID。 common が true のばあい、このフィールドは空白または null にして、ターゲット・サーバーを OS デプロイメント中に指定できます。

パラメーター	必須/オプション	タイプ	説明

template	オプションの	オブジェクトのアレイ	再利用可能なオブジェクトを表すパターン。
			OS デプロイメント中に、このテンプレートはオブジェクトの複数のインスタンスを表すことができます。**minElements** および **maxElements** フィールドを使用してインスタンス数を制限できます。
			
			次の例では、テンプレートを使用して、1 ～ 3 台の NTP サーバーの配列を表します。
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"template": [{
			"autoCreateInstance": true,
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			},
			
			OS デプロイメント中にユーザー入力値が収集された後、OS がデプロイされる各デバイスに固有の内容をもつ構成設定ファイルのインスタンスが作成されます。
			{
			"category": "dynamic",
			"common": true,
			"description": "NTP Servers",
			"label": "NTP Servers",
			"maxElements": 3,
			"minElements": 0,
			"name": "common-ntpservers",
			"optional": true,
			"content": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver0",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string",
			"value": "192.0.2.1"
			}],
			"template": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",

パラメーター	必須/オプション	タイプ	説明
			"label": "NTP Server", "name": "ntpserver", "optional": true, "regex": "[\\w\\.]{1,64}$", "type": "string" }], "type": "array" } **注：** • サーバー固有のオブジェクトの最上部ではテンプレートは*必須*です (common=false)。 • **category** が `static` の場合、template フィールドは無視されます。
type	必須	ストリング	オブジェクトのデータ・タイプ。これは以下のいずれかの値です。 • **アレイ** (array) • **assoc_array** • **boolean** • **integer** • **パスワード** • **string** • **user_data**
value	オプションの	ストリング	構成設定の単一の固定値。 **注：** • **default** が設定されている場合、このフィールドは空または null にできます。その他の場合は、**type** に一致する値を指定します。 • **type** が `password` の場合、暗号化されていないストリングを指定します。 • **type** が `assoc_array` または `array` の場合、空の **content** フィールド主指定する必要があります。 • **type** が `user_data` の場合、有効な JSON 形式の **value** を指定します。 • **regex** が設定されている場合、この値は指定された正規表現を使用して検証されます。

次の構成設定の例では、カスタム・プロファイルに追加できる SLES デプロイメントのロケール設定を定義します。

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "template": [{
      "autoCreateInstance": true,
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
```

```
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                        English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server",
      "optional": false,
      "type": "assoc_array"
    }],
    "type": "assoc_array"
  },
  {
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string"
    }],
    "type": "array"
  },
  {
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
  }],
  "description": "Custom configuration file for deployment of custom locale, NTP server,
                  and directory for post-installation script logs.",
  "label": "My Custom Deployment",
  "name": "myCustomDeploy",
```

```
  "optional": false,
  "type": "array"
}
```

以下は、デプロイメント中にユーザー入力値が定義された後、ホスト・システムで作成された構成設定ファイルのインスタンスの例です。

```
{
  "category": "dynamic",
  "content": [{
    "category": "dynamic",
    "common": false,
    "name": "server-settings",
    "optional": false,
    "content": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server0",
      "optional": false,
      "type": "assoc_array",
      "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
    },
    {
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
```

```
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server1",
      "optional": false,
      "type": "assoc_array",
      "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
      "category": "dynamic",
      "common": false,
      "content": [{
        "category": "dynamic",
        "choices": ["en_US", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the OS language locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "OS Locale",
        "name": "locale",
        "optional": false,
        "type": "string",
        "value": "en_US"
      },
      {
        "category": "dynamic",
        "choices": ["english-us", "pt_BR", "ja_JP"],
        "common": false,
        "description": "This parameter defines the keyboard locale to use with this deployment.
                English, Brazilian Portuguese, and Japanese are supported.",
        "label": "Keyboard Locale",
        "name": "keyboardLocale",
        "optional": false,
        "type": "string",
        "value": "english-us"
      }],
      "name": "server",
      "optional": false,
      "type": "assoc_array"
    }],
    "type": "assoc_array"
  },
  {
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "content": [{
      "category": "dynamic",
      "common": true,
```

```
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver0,
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string",
      "value": "192.0.2.1"
    },
    {
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver1",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string",
      "value": "192.0.2.2"
    }],
    "template": [{
      "category": "dynamic",
      "common": true,
      "description": "A NTP Server",
      "label": "NTP Server",
      "name": "ntpserver",
      "optional": true,
      "regex": "[\\w\\.]{1,64}$",
      "type": "string"
    }],
    "type": "array"
  },
  {
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logs.",
    "name": "logpath",
    "optional": false,
    "type": "string",
    "value": "/tmp/mylogger.log"
  }],
  "description": "Custom configuration file for deployment of custom locale, NTP server,
                  and directory for post-installation script logs.",
  "label": "My Custom Deployment",
  "name": "myCustomDeploy",
  "optional": false,
  "type": "array"
}
```

事前定義済みマクロ

*マクロ*によって、無人ファイルまたはポスト・インストール・スクリプトに、変数データ (構成設定) を追加できます。Lenovo XClarity Administrator では、一連の事前定義済み構成設定が用意されており、使用できます。

事前定義済みマクロ、無人ファイルまたはポスト・インストール・スクリプト・ファイルに挿入するには、事前定義済みマクロに「predefined」のプレフィックスを付け、ネストされたオブジェクトをピリオドで区切り、ハッシュ (#) 記号でマクロ名を囲みます (例: **#predefined.globalSettings.ipAssignment#**)。

事前定義された各マクロの値は、XClarity Administrator インスタンスに応じて異なります。たとえば、**「OS イメージのデプロイ」 ➡ 「共通設定」 ➡ 「IP の割り当て」**フィールドで、IP モードを指定できます。OS デプロイメント中にユーザー入力された値が収集された後、その値が事前定義済みマクロの

#predefined.globalSettings.ipAssignment# によって事前定義済み構成設定に表示されます。また、および構成設定 JSON ファイルのインスタンスの ipAssignment オブジェクト名の下にも表示されます。

次の表は、XClarity Administrator で使用できる事前定義済みマクロ (構成設定) のリストです。

マクロ名	タイプ	説明
事前定義	オブジェクト	すべての事前定義 OS デプロイメント設定に関する情報
globalSettings	オブジェクト	グローバル OS デプロイメント設定に関する情報
credentials	オブジェクトのアレイ	ユーザー資格情報に関する情報
name	ストリング	
type	ストリング	オペレーティング・システムのタイプ。これは以下のいずれかの値です。 • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	ストリング	オペレーティング・システムをデプロイするためのホスト・ネットワーク設定オプション。これは以下のいずれかの値です。 • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	ストリング	VLAN モードが使用されているかどうかを示します。これは以下のいずれかの値です。 • **true**。VLAN モードが使用されます。 • **false**。VLAN モードは使用されていません。
hostPlatforms	オブジェクト	ホスト・プラットフォームからのデプロイメント設定
licenseKey	ストリング	Microsoft Windows または VMware ESXi で使用されるライセンス・キー。ライセンス・キーがない場合は、このフィールドを null に設定できます。
networkSettings	アレイ	ネットワーク設定に関する情報
dns1	ストリング	オペレーティング・システムがデプロイされた後に使用されるホスト・サーバーの優先 DNS サーバー
dns2	ストリング	オペレーティング・システムがデプロイされた後に使用されるホスト・サーバーの代替 DNS サーバー
gateway	ストリング	オペレーティング・システムがデプロイされた後に使用されるホスト・サーバーのゲートウェイ。グローバル OS デプロイメント設定でネットワーク設定が静的に設定されている場合に使用されます。 **ヒント**: IP モードを判別するには、GET /osdeployment/globalSettings を使用します。
hostname	ストリング	ホスト・サーバーのホスト名。ホスト名を指定しない場合は、デフォルトのホスト名が割り当てられます。
ipAddress	ストリング	オペレーティング・システムがデプロイされた後に使用されるホスト・サーバーの IP アドレス。グローバル OS デプロイメント設定でネットワーク設定が静的に設定されている場合に使用されます。

マクロ名	タイプ	説明
mtu	Long	オペレーティング・システムがデプロイされた後に使用されるホストの最大転送単位。
prefixLength	ストリング	オペレーティング・システムがデプロイされた後に使用されるホスト IP アドレスのプレフィックスの長さ。グローバル OS デプロイメント設定でネットワーク設定が静的 IPv6 に設定されている場合に使用されます。
selectedMAC	ストリング	IP アドレスがバインドされるホスト・サーバーの MAC アドレス。MAC アドレスはデフォルトで「自動」に設定されています。この設定は、デプロイメント用に構成して使用できるイーサネット・ポートを自動的に検出します。検出された最初の MAC アドレス (ポート) が、デフォルトで使用されます。別の MAC アドレスとの接続が検出された場合は、XClarity Administrator ホストが自動的に再起動され、新しく検出された MAC アドレスをデプロイメントに使用します、および selectedMAC は新たに検出された MAC アドレスに設定されます。 VLAN モードは、インベントリー内に MAC アドレスがあるサーバーでのみサポートされます。AUTO がそのサーバーで唯一の MAC アドレスである場合、そのサーバーへのオペレーティング・システムのデプロイに VLAN を使用することはできません。 **ヒント**: MAC アドレスを取得するには、GET /hostPlatforms の **macaddress** 応答プロパティを使用します。
subnetCIDRNumber	整数	オペレーティング・システムのデプロイ後に使用されるホスト・サーバーのサブネット・マスク (Classless Inter-Domain Routing (CIDR) 形式)。グローバル OS デプロイメント設定でネットワーク設定が静的に設定されている場合に使用されます。 CIDR 番号は、通常はスラッシュ (/) で始まり、IP アドレスに従っています。たとえば、サブネット・マスク (8 つのネットワーク・ビットを持つ) の 255.0.0.0 の 131.10.55.70 の IP アドレスは、131.10.55.70 /8 となります。詳しくは、CIDR 表記のチュートリアル Web ページ を参照してください。 **ヒント**: IP モードを判別するには、GET /osdeployment/globalSettings を使用します。
subnetMask	ストリング	ドット数値記法でのオペレーティング・システムのデプロイ後に使用されるホスト・サーバーのサブネット・マスク (例: 255.0.0.0)。グローバル OS デプロイメント設定でネットワーク設定が静的に設定されている場合に使用されます。 **ヒント**: IP モードを判別するには、GET /osdeployment/globalSettings を使用します。
vlanId	ストリング	オペレーティング・システム VLAN タグ付けの VLAN ID。 このパラメーターは VLAN モードが有効の場合にのみ有効です。VLAN モードが有効になっているかどうかを確認するには、XClarity Administrator オンライン・ドキュメントの GET /osdeployment/globalSettings を使用します)。 **重要：**VLAN タグがネットワーク上で機能するために必要な場合のみ VLAN ID を指定します。VLAN タグを使用すると、ホスト・オペレーティング・システムと XClarity Administrator の間のネットワーク・ルーティング可能性に影響を与えることがあります。
selectedImage	ストリング	デプロイするオペレーティング・システム・イメージのプロファイル ID。 **ヒント**: オペレーティング・システム・イメージのプロファイル ID を取得するには、GET /hostPlatforms の **availableImages** 応答プロパティを使用します。

マクロ名	タイプ	説明
storageSettings	アレイ	オペレーティング・システム・イメージをデプロイする優先格納場所
targetDevice	ストリング	ターゲット・デバイス。これは以下のいずれかの値です。 • **ローカル・ディスク**。ローカル・ディスク・ドライブ。管理対象サーバーで最初に列挙されたローカル・ディスク・ドライブが使用されます。 • **M.2 ドライブ**。M.2 ドライブ。管理対象サーバーで最初に列挙された M.2 ドライブが使用されます。 • **USB ディスク**。埋め込み USB ハイパーバイザー。この場所は、VMware ESXi イメージが管理対象サーバーにデプロイされている場合にのみ適用できます。2 つのハイパーバイザー・キーが管理対象サーバーにインストールされている場合、VMware インストーラーは、最初に列挙されているキーをデプロイ時に選択します。 • **lunpluswwn=*LUN*@*WWN***。FC SAN ストレージ (例: `lunpluswwn=2@50:05:07:68:05:0c:09:bb`)。 • **lunplusiqn=*LUN*@*IQN***。iSCSI SAN ストレージ (例: `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`)。iSCSI ターゲットが 1 つしか構成されていない場合は、*IQN* の指定はオプションです。*IQN* が指定されていない場合、最初に検出された iSCSI ターゲットが OSDN に対して選択されます。指定されている場合、完全一致が作成されます。 **注：**ThinkServer サーバーの場合、この値は常に「localdisk」です。
unattendFileId	ストリング	このデプロイメントで使用する無人ファイルの ID
UUID	ストリング	オペレーティング・システムのデプロイ先となるホスト・サーバーの UUID
imageSettings	オブジェクト	各 OS イメージとイメージ・プロファイルに関する情報
name	ストリング	オペレーティング・システム・イメージ名
profile	ストリング	イメージ・プロファイル名
otherSettings	オブジェクト	現在実行中の OS デプロイメント・ジョブに関連する追加設定
deployDataAndSoftwareLocation	ストリング	展開されたソフトウェア・ペイロード、カスタム・ファイル、およびデプロイメント・データ (証明書やログなど) へのパス

installRepoUrl	ストリング	(SLES 15 以降のみ) インポート済みパッケージ イメージの URL アドオン・セクションの media_url のカスタム無人で、この事前定義済みマクロを使用できます。例:
		`<add-on>`
		`  <add_on_products config:type="list">`
		`  <listentry>`
		`  <media_url>`**#predefined.otherSettings.installRepoUrl#**
		`  </media_url>`
		`  <product>sle-module-basesystem</product>`
		`  <product_dir>/Module-Basesystem</product_dir>`
		`  </listentry>`
		`  </add_on_products>`
		`</add-on>`

lxcaIp	ストリング	XClarity Administrator インスタンスの IP アドレス

マクロ名	タイプ	説明
lxcaRelease	ストリング	XClarity Administrator リリース (例:2.0.0)
jobId	ストリング	現在実行中の OS デプロイメント・ジョブの ID
ntpServer	ストリング	XClarity Administrator に関連する NTP サーバー
statusSettings	オブジェクト	OS デプロイメント・ステータスの設定
urlStatus	ストリング	XClarity Administrator がステータスを報告する HTTPS URL (ポートを含む)
certLocation	ストリング	初回ブートでホスト OS から **urlStatus** Web サービスにアクセスするために必要な証明書が含まれるフォルダー
sdkLocation	ストリング	XClarity Administrator が提供するヘルパー・スクリプトおよび XClarity Administrator にアクセスするインターフェースの場所
timezone	ストリング	XClarity Administrator に対して設定されたタイム・ゾーン (たとえば、America/New_York など)
unattendSettings	オブジェクト	無人ファイルを作成するために使用する設定。これらの値は、XClarity Administrator のバージョンに固有です
networkConfig	ストリング	(ESXi および RHEL のみ) 無人インストール時間に使用される XClarity Administrator の事前定義済みのコンテンツ。これにより、オペレーティング・システムのネットワーク設定が構成されます。
preinstallConfig	ストリング	プレインストール無人時間に使用される XClarity Administrator によって事前定義済みのコンテンツ。これには、プレインストールのステータスが含まれます。 • ESXi および RHEL の場合は、%pre 初期インストール・スクリプト・フックが使用されます。 • SLES の場合は、<scripts> 初期インストール・スクリプト・フックが使用されます。 **注意：**このマクロをカスタム無人ファイルに含めることを強くお勧めします。無人ファイルの行 1 の後ろ (<xml> タグの後ろ) の任意の場所にマクロを配置できます。
postinstallConfig	ストリング	サーバーが構成され初めてブートされた後に使用する XClarity Administrator の事前定義済みコンテンツ。これには、ポスト・インストールのステータスが含まれます。 • ESXi および RHEL の場合は、%post ポスト・インストール・スクリプト・フックが使用されます。 • SLES の場合は、<scripts> ポスト・インストール・スクリプト・フックが使用されます。 • Windows の場合、「専門設定」セクションが使用されます。 **注意：**このマクロをカスタム無人ファイルに含めることを強くお勧めします。無人ファイルの行 1 の後ろ (<xml> タグの後ろ) の任意の場所にマクロを配置できます。
reportWorkloadNotComplete	ストリング	このマクロが存在している場合、postinstallConfig マクロは「OS インストールが完了しました (17)」ステータスを報告しません。カスタム・プロファイルでは完了を報告する必要があります。
storageConfig	ストリング	(ESXi および RHEL のみ) 無人インストール時間に使用される XClarity Administrator の事前定義済みのコンテンツ。これにより、オペレーティング・システムのストレージ設定が構成されます。

カスタム無人ファイルのインポート

カスタム無人ファイルは、OS イメージ・リポジトリーにインポートできます。その後、これらのファイルを使用して Linux および Windows OS イメージ・プロファイルをカスタマイズできます。

このタスクについて

カスタム無人ファイルでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft Windows Server	Unattend (.xml)	無人ファイルについて詳しくは、無人 Windows セットアップのリファレンス Web ページを参照してください。
Red Hat® Enterprise Linux (RHEL) サーバー	Kickstart (.cfg)	無人ファイルについて詳しくは、Red Hat: Kickstart を使用したインストールの自動化 Web ページを参照してください。 ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 • 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 • 推奨される**#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 • 推奨される**#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。
Rocky Linux	Kickstart (.cfg)	無人ファイルについて詳しくは、Red Hat: Kickstart を使用したインストールの自動化 Web ページを参照してください。 ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 • 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 • 推奨される**#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 • 推奨される**#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	無人ファイルについて詳しくは、SUSE: AutoYaST Web ページを参照してください。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	Kickstart (.cfg)	ESXi 6.0u3 およびそれ以降の更新と、6.5 以降でのみサポートされています。 無人ファイルについて詳しくは、VMware: スクリプトを使用したホストの インストールまたはアップグレード Web ページを参照してください。 ファイルに %pre、%post、%firstboot セクションを追加する場合は、以下を検討してください。 • 無人ファイルには複数の %pre、%post、%firstboot セクションを追加できますが、セクションの順序に注意してください。 • 推奨される**#predefined.unattendSettings.preinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %pre セクションをファイル内の他のすべての %pre セクションの前に追加します。 • 推奨される**#predefined.unattendSettings.postinstallConfig#** マクロが無人ファイルにある場合、XClarity Administrator は %post および %firstboot セクションをファイル内の他のすべての %post および %firstboot セクションの前に追加します。

注意：

- オブジェクトの固有名を使用して、無人ファイルに事前定義済みおよびカスタム・マクロ (構成設定) を挿入できます。事前定義済みの値は XClarity Administrator インスタンスに基づいて動的に変化します。カスタム・マクロは、OS のデプロイ時に指定されたユーザー入力に基づいて動的に変化します。

  注：

  – マクロ名は、ハッシュ記号 (#) で囲みます。
  – ネストされたオブジェクトの場合は、各オブジェクト名をピリオドで区切ります (例: **#server_settings.server0.locale#**)。
  – カスタム・オブジェクト名の場合、最上部のオブジェクト名は含めません。事前定義済みのマクロには、マクロ名にプレフィックス「predefined」を付けます。
  – テンプレートからオブジェクトが作成されると、0 から固有番号名が付加されます (例: **server0**、**server1**)。
  – 各カスタム設定の隣にある「ヘルプ」アイコン ( ) にマウスを合わせることで、「OS イメージのデプロイ」ダイアログの「カスタム設定」タブから、各マクロの名前を確認できます。
  – 事前定義済みマクロのリストについては、事前定義済みマクロを参照してください。カスタム構成設定およびマクロについては、カスタム・マクロを参照してください。

- XClarity Administrator は、OS インストーラーからのステータスの通信、およびその他の重要なインストール手順で使用される以下の事前定義済みマクロを提供します。これらのマクロを無人ファイルに含めることを強くお勧めします (事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照)。
  – #predefined.unattendSettings.preinstallConfig#
  – #predefined.unattendSettings postinstallConfig#

OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

手順

OS イメージ・リポジトリーに無人ファイルをインポートするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**無人ファイル**」タブをクリックします。

ステップ 3. 「**ファイルのインポート**」アイコン ( ) をクリックします。「ファイルのインポート」ダイアログが表示されます。

ステップ 4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. オペレーティング・システム・タイプを選択します。

ステップ 7. 無人ファイルのファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。

ステップ 8. **オプション**: 無人ファイルの説明を入力します。

ヒント:「**説明**」フィールドを使用して、同じ名前のカスタム・ファイルを区別できます。

ステップ 9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。

- MD5
- SHA1

- SHA256

ステップ 10.「**インポート**」をクリックします。

ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

無人ファイル・イメージは、「OS イメージの管理」ページの「**無人ファイル**」タブにリストされます。

このページでは、以下の操作を実行できます。

- 無人ファイルを作成する。「**作成**」アイコン ( ) をクリックします。
  エディターは、ファイル内で検出されたすべてのエラーの位置を識別します。一部のメッセージは英語のみであることに注意してください。
- 無人ファイルを構成設定ファイルに関連付ける (無人ファイルを構成設定ファイルに関連付けるを参照)。
- 無人ファイルを表示および変更する。「**編集**」アイコン ( ) をクリックします。
  エディターは、ファイル内で検出されたすべてのエラーの位置を識別します。一部のメッセージは英語のみであることに注意してください。
- 無人ファイルをコピーする。「**コピー**」アイコン ( ) をクリックします。
  構成設定ファイルに関連付けられている無人ファイルをコピーすると、関連する構成設定ファイルもコピーされ、コピーした両方のファイルの間で関連付けが自動的に作成されます。
- 選択された無人ファイルを削除する。「**削除**」アイコン ( ) をクリックします。
- 「**ファイル・サーバーの構成**」アイコン ( ) をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。

カスタマイズされた OS イメージ・プロファイルへの無人ファイルの追加については、カスタム OS イメージ・プロファイルの作成を参照してください。

事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入

事前定義済みマクロおよびカスタム・マクロを無人ファイルに挿入できます。

このタスクについて

*マクロ*を使用すると、任意の動的データ (構成設定) を無人ファイルに追加できます。OS イメージ・プロファイルをデプロイするときに、データの値を指定します。

Lenovo XClarity Administrator では*事前定義済み*マクロのセットを提供します。これは、カスタム構成設定ファイルを関連付けずに無人ファイルに追加できます。事前定義済みマクロのリストについては、事前定義済みマクロを参照してください。

次の事前定義済みマクロをカスタム無人ファイルに含めることを強くお勧めします。

- #predefined.unattendSettings.preinstallConfig# および #predefined.unattendSettings postinstallConfig#OS インストーラーからのステータスの通信、およびその他の重要なインストール手順で使用されます。

インストール構成マクロを含める方法について詳しくは、次の OS デプロイメント・シナリオの例を参照してください。
  - カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ
  - 構成可能なロケールと NTP サーバーを使用する SLES 12 SP3 のデプロイ
  - 静的 IP アドレスを使用したローカル・ディスクへの Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ
  - カスタム機能を伴う Windows 2016 のデプロイ

- **#predefined.unattendSettings.networkConfig#**。(ESXi および RHEL のみ) XClarity Administrator を有効にしてネットワークを構成します。このマクロでは、「OS イメージのデプロイ」ページで指定されているネットワーク設定を使用します。無人ファイルにこのマクロが含まれていない場合、またはネットワーク設定が XClarity Administrator で定義されていない場合は、XClarity Administrator に戻るネットワーク経路がホストに含まれるように、無人ファイルの一部として IP インターフェースを構成する必要があります。

  ネットワーク構成マクロを含める方法について詳しくは、次の OS デプロイメント・シナリオの例を参照してください。
  - カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ
  - 静的 IP アドレスを使用したローカル・ディスクへの Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ

- **#predefined.unattendSettings.storageConfig#**。(ESXi および RHEL のみ) XClarity Administrator を有効にしてホスト上のストレージを構成します。このマクロでは、「OS イメージのデプロイ」ページで指定されているストレージ設定を使用します。無人ファイルでこのマクロが含まれていない場合、または XClarity Administrator でストレージ設定が定義されていない場合、無人ファイルでストレージ構成を指定する必要があります。

  ストレージ構成マクロを含める方法について詳しくは、次の OS デプロイメント・シナリオの例を参照してください。
  - カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ
  - 静的 IP アドレスを使用したローカル・ディスクへの Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ

構成設定ファイルを作成し、無人ファイルをカスタム構成設定ファイルに関連付けることで、*カスタム・マクロ*を作成できます。カスタム構成設定ファイルをインポートする場合、XClarity Administrator によってファイル内の各構成設定にマクロが作成されます。

手順

以下の手順を実行してマクロを無人ファイルに追加します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**無人ファイル**」タブをクリックします。

ステップ 3. 編集する無人ファイルを選択します。

ステップ 4. 「**編集**」アイコン () をクリックして、「無人ファイルの編集」ダイアログを表示します。

ステップ 5. 次の例のような事前定義済みの推奨マクロを追加します:

1. 無人ファイルの行 1 の後ろ (<xml> タグの後ろ) の任意の場所にカーソルを置きます。
2. 使用可能なマクロのリスト内の 「**predefine**」 ➔ 「**unattendSettings**」 リストを展開します。
3. 「**preinstallConfig**」および「**postinstallConfig**」をクリックして、必要な事前定義済みマクロを無人ファイルに追加します。

   以下のコードがファイルに追加されます。

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

ステップ 6. 無人ファイルの正しい場所にカーソルを置いてリストのマクロをクリックすることで、さらに事前定義済みマクロまたはカスタム・マクロを追加します。

ステップ 7. 「**保存**」をクリックします。

無人ファイルを構成設定ファイルに関連付ける

構成設定を無人ファイルに関連付け (バインド) し、関連付けられたカスタム・マクロを無人ファイルに追加できます。

このタスクについて

カスタム構成設定ファイルを関連付けずに、事前定義済みマクロを無人ファイルに関連づけることができます。

無人ファイルに関連付けられている構成設定ファイルは編集できません。ただし、関連付けられたファイルをコピーし、そのコピーを編集できます。

手順

以下の手順を実行して、無人ファイルを構成設定ファイルに関連付けます。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**無人ファイル**」タブをクリックします。

ステップ 3. カスタム無人ファイルを選択します。

ステップ 4. 「**構成ファイルの関連付け**」アイコン ( ) をクリックして、「無人ファイルの関連付け」ダイアログを表示します。

ステップ 5. 無人ファイルに関連付ける構成設定ファイルを選択します。

ステップ 6. 事前定義済みマクロおよびカスタム・マクロを無人ファイルに追加します。エディタ内のマクロを追加する場所にカーソルを置き、利用可能なリストからマクロをクリックします (事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照)。

オブジェクトの固有名を使用して無人ファイルにマクロを挿入できます。ネストされた名前のオブジェクトの場合は、各オブジェクトをピリオドで区切ります (例: `server_specific_settings.server.locale`)。一番上の名前は含めないことに注意してください。

ステップ 7. 「**関連付ける**」をクリックしてフォルダをひとつにバインドします。

カスタム・インストール・スクリプトのインポート

インストール・スクリプトは、OS イメージ・リポジトリーにインポートできます。その後、これらのファイルを使用して Linux および Windows イメージをカスタマイズできます。

このタスクについて

現時点では、ポスト・インストール・スクリプトのみがサポートされています。

次の表は、Lenovo XClarity Administrator が各オペレーティング・システムでサポートしているインストール・スクリプトのファイルタイプのリストです。特定のオペレーション・システムのバージョンでは、XClarity Administrator でサポートされているすべてのファイル・タイプを必ずしもサポートしないことに注意してください (たとえば、一部の RHEL バージョンでは、最小プロファイルに Perl が含まれず、したがって、Perl スクリプトが実行されません)。デプロイするオペレーティング・システムのバージョンに合ったファイル・タイプを使用していることを確認してください。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft® Windows® Server	コマンド・ファイル (.cmd)、PowerShell (.ps1)	デフォルトのカスタム・データとファイルのパスは `C:\lxca` です。インストール・スクリプトについて詳しくは、Windows セットアップへのカスタム・スクリプトの追加 Web ページを参照してください。
Red Hat® Enterprise Linux (RHEL) サーバー	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。インストール・スクリプトについて詳しくは、RHEL: ポスト・インストール・スクリプト Web ページを参照してください。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
Rocky Linux	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは /home/lxca です。インストール・スクリプトについて詳しくは、RHEL: ポスト・インストール・スクリプト Web ページを参照してください。
SUSE® Linux Enterprise Server (SLES)	Bash (.sh)、Perl (.pm または .pl)、Python (.py)	デフォルトのカスタム・データとファイルのパスは /home/lxca です。インストール・スクリプトについて詳しくは、SUSE: カスタム・ユーザー・スクリプト Web ページを参照してください。
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	Bash (.sh)、Python (.py)	デフォルトのカスタム・データとファイルのパスは /home/lxca です。インストール・スクリプトについて詳しくは、VMware: インストールとアップグレード・スクリプト Web ページを参照してください。

注：OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

OS デプロイメント中にデータが収集された後、XClarity Administrator によって、ポスト・インストール・スクリプトが使用するホスト・システムに構成設定ファイル (選択されたファイルのカスタム設定および事前定義済み設定のサブセットを含む) のインスタンスが作成されます。

オブジェクトの固有名を使用して、ポスト・インストール・スクリプトに事前定義済みおよびカスタム・マクロ (構成設定) を挿入できます。事前定義済みの値は XClarity Administrator インスタンスに基づいて動的に変化します。カスタム・マクロは、OS のデプロイ時に指定されたユーザー入力に基づいて動的に変化します。

注：

- マクロ名は、ハッシュ記号 (#) で囲みます。
- ネストされたオブジェクトの場合は、各オブジェクト名をピリオドで区切ります (例: **#server_settings.server0.locale#**)。
- カスタム・オブジェクト名の場合、最上部のオブジェクト名は含めません。事前定義済みのマクロには、マクロ名にプレフィックス「predefined」を付けます。
- テンプレートからオブジェクトが作成されると、0 から固有番号名が付加されます (例: **server0**、**server1**)。
- 各カスタム設定の隣にある「ヘルプ」アイコン () にマウスを合わせることで、「OS イメージのデプロイ」ダイアログの「カスタム設定」タブから、各マクロの名前を確認できます。
- 事前定義済みマクロのリストについては、事前定義済みマクロを参照してください。カスタム構成設定およびマクロについては、カスタム・マクロを参照してください。

ポスト・インストール・スクリプトがダウンロードおよび実行されると、無人ファイル内の推奨される事前定義済みマクロによって、オペレーティング・システムのデプロイメントの最終的なステータスが報告されます。ポスト・インストール・スクリプトを変更して、ターゲット・オペレーティング・システムに応じたカスタム・ステータス報告を含めることができます。詳しくは、インストール・スクリプトに報告するカスタム・ステータスの追加を参照してください。

手順

OS イメージ・リポジトリーにインストール・スクリプトをインポートするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**インストール・スクリプト**」タブをクリックします。

ステップ 3. 「**ファイルのインポート**」アイコン ( ) をクリックします。「インストール・スクリプトのインポート」ダイアログが表示されます。

ステップ 4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. オペレーティング・システム・タイプを選択します。

ステップ 7. インストール・スクリプトのファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。

ステップ 8. **オプション**: インストール・スクリプトの説明を入力します。

ヒント:「**説明**」フィールドを使用して、同じ名前のカスタム・ファイルを区別できます。

ステップ 9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。

- MD5
- SHA1
- SHA256

ステップ 10.「**インポート**」をクリックします。

> **ヒント**: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。
>
> ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

インストール・スクリプトは、「OS イメージの管理」ページの「**インストール・スクリプト**」タブにリストされます。

このページでは、以下の操作を実行できます。

- 「**ファイル・サーバーの構成**」アイコン () をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。
- 選択されたインストール・スクリプトを削除する。「**削除**」アイコン () をクリックします。

カスタマイズされた OS イメージ・プロファイルへのインストール・スクリプトの追加については、カスタム OS イメージ・プロファイルの作成を参照してください。

インストール・スクリプトに報告するカスタム・ステータスの追加

ポスト・インストール・スクリプトがダウンロードおよび実行されると、無人ファイル内の推奨される事前定義済みマクロによって、オペレーティング・システムのデプロイメントの最終的なステータスが報告されます。ポスト・インストール・スクリプトに追加のステータス報告を含めることができます。

Linux

Linux の場合、以下の `curl` コマンドを使用してステータスを報告します。

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

<status_ID> は以下のいずれかの値です。

- **44**.ワークロードのデプロイメントが成功しました
- **45**.ワークロードのデプロイメントが警告ありで実行中です。
- **46**.ワークロードのデプロイメントが失敗しました
- **47**.ワークロード・デプロイメント・メッセージ
- **48**.カスタム・ポスト・インストール・スクリプト・エラー

`curl` コマンドは、Lenovo XClarity Administrator がステータスをレポートするために使用する HTTPS URL (**predefined.otherSettings.statusSettings.urlStatus**)、および最初のブート時にホスト OS から urlStatus Web サービスにアクセスするために必要な証明書を含むフォルダー (**predefined.otherSettings.statusSettings.certLocation**) に、事前定義済みマクロを使用します。次の例では、ポスト・インストール・スクリプトで発生したエラーを報告します。

次の例では、ポスト・インストール・スクリプトで発生したエラーを報告します。

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Wiindows の場合、`LXCA.psm1` スクリプトをインポートして次のコマンドを呼び出し、ステータスを報告できます。

- **initializeRestClient**

  REST クライアントを初期化します。このコマンドを実行するには、次の構文を使用します。このコマンドは、レポーティング・コマンドを実行する前に必要です。

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  XClarity Administrator がホスト・サーバーに接続できることを検証します。このコマンドを実行するには、次の構文を使用します。このコマンドはオプションですが、レポーティング・コマンドを実行する前にインストール・スクリプト内で推奨されます。

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  正常完了メッセージが XClarity Administrator ジョブ・ログに記録されたことを報告します。このコマンドを実行するには、次の構文を使用します。

  ヒント: #predefined.unattendSettings.reportWorkloadNotComplete# マクロがカスタム無人ファイルまたはポスト・インストール・スクリプトに含まれている場合、**reportWorkloadDeploymentSucceeded** コマンドをポスト・インストール・スクリプトに含めて正常に完了した信号を送信します。その他の場合は、XClarity Administrator によってポスト・インストール・スクリプトの実行後に自動的に完了ステータスが報告されます。

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  警告メッセージが XClarity Administrator ジョブ・ログに記録されたことを報告します。このコマンドを実行するには、次の構文を使用します。

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  失敗メッセージが XClarity Administrator ジョブ・ログに記録されたことを報告します。このコマンドを実行するには、次の構文を使用します。

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
  ```

- **reportCustomPostInstallScriptError**

  ポスト・インストール・スクリプト・エラー・メッセージが XClarity Administrator ジョブ・ログに記録されたことを報告します。このコマンドを実行するには、次の構文を使用します。

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  一般メッセージが XClarity Administrator ジョブ・ログに記録されたことを報告します。デプロイメントの状態には影響しません。このコマンドを実行するには、次の構文を使用します。

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

ここで *<message_text>* は各ステータス状況で XClarity Administrator に返すメッセージです。

これらのコマンドは XClarity Administrator インスタンスの IP アドレス (#predefined.otherSettings.lxcaIp#) およびオペレーティング・システムがデプロイされるホスト・サーバーの UUID (#predefined.hostPlatforms.uuid#) に事前定義済みマクロを使用することに注意してください。

次の例は、Java をインストールし、インストールが失敗した場合はエラーを報告する、PowerShell インストール スクリプトです。

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
  Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
  [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
    -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

カスタム・ソフトウェアのインポート

ソフトウェアは、OS イメージ・リポジトリーにインポートできます。その後、これらのファイルを使用して Linux および Windows イメージをカスタマイズできます。

このタスクについて

カスタム・ソフトウェア・ファイルは、オペレーティング・システム・デプロイメントおよびポスト・インストール・スクリプトの完了後にインストールします。

カスタム・ソフトウェアでは、以下のファイル・タイプがサポートされます。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
CentOS Linux	サポートされていない	
Microsoft® Windows® Azure Stack HCI	サポートされていない	
Microsoft Windows Hyper-V Server	サポートされていない	
Microsoft Windows® Server	ソフトウェア・ペイロードを含む .zip ファイル。	デフォルトのカスタム・データとファイルのパスは `C:\lxca` です。
Red Hat® Enterprise Linux (RHEL) サーバー	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
SUSE® Linux Enterprise Server (SLES)	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
Rocky Linux	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。

オペレーティング・システム	サポートされているファイル・タイプ	その他の情報
Ubuntu	サポートされていない	
VMware vSphere® Hypervisor (ESXi) (Lenovo カスタマイズ対応)	ソフトウェア・ペイロードを含む .tar.gz ファイル。	デフォルトのカスタム・データとファイルのパスは /home/lxca です。

注：OS イメージ・リポジトリーには、ファイルの保存に十分なスペースがあれば、無制限に事前定義済みファイルおよびカスタム・ファイルを保存できます。

手順

OS イメージ・リポジトリーにソフトウェアをインポートするには、以下の手順を実行します。

ステップ 1. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**ソフトウェア**」タブをクリックします。

ステップ 3. 「**ファイルのインポート**」アイコン ( ) をクリックします。「インストール・スクリプトのインポート」ダイアログが表示されます。

ステップ 4. 「**ローカル・インポート**」タブをクリックしてローカル・システムからファイルをアップロードするか、「**リモート・インポート**」タブをクリックしてリモート・ファイル・サーバーからファイルをアップロードします。

注：リモート・ファイル・サーバーからファイルをアップロードするには、まず「**ファイル・サーバーの構成**」アイコン ( ) をクリックしてリモート・ファイル・サーバー・プロファイルを作成する必要があります。詳しくは、リモート・ファイル・サーバーの構成を参照してください。

ステップ 5. リモート・ファイル・サーバーを使用することを選択した場合、「**リモート・ファイル・サーバー**」リストから使用するサーバーを選択します。

ステップ 6. オペレーティング・システム・タイプを選択します。

ステップ 7. ソフトウェア・ファイルのファイル名を入力し、「**参照**」をクリックしてインポートするファイルを見つけます。

ステップ 8. **オプション**: ソフトウェア・ファイルの説明を入力します。

ヒント: 「**説明**」フィールドを使用して、同じ名前のカスタム・ファイルを区別できます。

ステップ 9. **オプション**: チェックサム・タイプを選択して、アップロードするファイルが破損していないことを確認し、チェックサム値をコピーして、指定されたテキスト・フィールドに貼り付けます。

チェックサム・タイプを選択した場合は、アップロードされたファイルの整合性とセキュリティーをチェックするために、チェックサム値を指定する必要があります。この値は、信頼できる機関の安全なソースから取得する必要があります。アップロードされたファイルがチェックサム値と一致したら、デプロイメントを安全に続行できます。そうでない場合は、ファイルを再度アップロードするか、チェックサム値を確認する必要があります。

次の 3 つのチェックサム・タイプがサポートされます。
- MD5
- SHA1
- SHA256

ステップ 10.「**インポート**」をクリックします。

ヒント: ファイルのアップロードは、安全なネットワーク接続を介して行われます。このため、ファイルのインポートにかかる時間はネットワークの信頼性とパフォーマンスに左右されます。

ファイルのアップロード中にローカルのアップロード先の Web ブラウザーのタブまたはウィンドウを閉じると、インポートは失敗します。

終了後

インストール・スクリプトは、「OS イメージの管理」ページの「**ソフトウェア**」タブにリストされます。

このページでは、以下の操作を実行できます。

- 「**ファイル・サーバーの構成**」アイコン () をクリックして、リモート・ファイル・サーバー・プロファイルを作成する。
- 選択されたソフトウェア・ファイルを削除する。「**削除**」アイコン () をクリックします。

カスタマイズされた OS イメージ・プロファイルへのソフトウェア・ファイルの追加については、カスタム OS イメージ・プロファイルの作成を参照してください。

カスタム OS イメージ・プロファイルの作成

OS イメージ・リポジトリーにある事前定義された OS イメージ・プロファイルに、カスタム・デバイス・ドライバー、ブート・ファイル (Windows のみ)、構成設定、無人ファイル、インストール・スクリプト、およびソフトウェアを追加できます。OS イメージにファイルを追加する際、Lenovo XClarity Administrator によりその OS イメージ用のカスタム・プロファイルが作成されます。カスタム・プロファイルには、カスタム・ファイルとインストール・オプションが含まれています。

始める前に

追加するカスタム・ファイルは、OS イメージ・リポジトリーに存在している必要があります (ブート・ファイルのインポート、デバイス・ドライバーのインポート、カスタム構成設定のインポート、カスタム無人ファイルのインポート、カスタム・インストール・スクリプトのインポート、および カスタム・ソフトウェアのインポートを参照)。

手順

OS イメージをカスタマイズするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

ステップ 2. 「**OS イメージ**」タブをクリックします。

ステップ 3. カスタマイズする事前定義済みの OS イメージ・プロファイルを選択します。

「**カスタマイズ**」列は、カスタマイズ可能な OS イメージを識別します。特定の OS イメージのカスタマイズについて詳しくは、「**ヘルプ**」アイコン ( ) をクリックしてください。

- 「**カスタマイズ可能**」。OS イメージはカスタマイズをサポートしていますが、カスタマイズされていません。
- 「**カスタマイズ不可**」。OS イメージはカスタマイズをサポートしていません。

注：「**ファイルのインポート**」アイコン ( ) をクリックして、ローカルまたはリモート・システムから追加のベース OS イメージ (.iso 形式) をインポートできます。

ステップ 4. 「**カスタマイズされたプロファイルの作成**」アイコン ( )。「新規カスタム OS イメージ」ダイアログが表示されます。

ステップ 5. 「**全般**」タブで、新しいカスタマイズされた OS イメージ・プロファイルの名前、説明、デプロイメント・ホスト上のカスタム・ファイルおよびデプロイメント・データのパス、およびカスタマイズ・タイプを指定します。

カスタマイズ・タイプは以下のいずれかです。

- **無人ファイルのみ**
- **構成ファイルのみ**
- **関連付けられていない無人ファイルおよび構成ファイル**
- **関連付けられた無人ファイルと構成ファイル**
- **なし**

ステップ 6. 「**次へ**」をクリックします。

ステップ 7. 「**デバイス・ドライバー**」タブで、Linux OS イメージ・プロファイルに追加するデバイス・ドライブを選択します。

サポートされるフォーマットのリストについては、デバイス・ドライバーのインポートを参照してください。

選択されたファイルは、構成ウィザードの完了後に適用されます。

注：「**ファイルのインポート**」アイコン ( ) をクリックして、ローカルまたはリモート・システムから追加のデバイス・ドライバーをインポートできます。

ステップ 8. 「**次へ**」をクリックします。

ステップ 9. (Windows のみ)「**ブート・オプション**」タブで、Windows OS イメージ・プロファイルに追加するブート・ファイルを選択します。

サポートされるフォーマットのリストについては、ブート・ファイルのインポートを参照してください。

選択されたファイルは、構成ウィザードの完了後に適用されます。

ステップ 10.「**次へ**」をクリックします。

ステップ 11.「**構成設定**」タブ (該当する場合) で、OS イメージ・プロファイルに追加するカスタム構成ファイルを 1 つ以上選択します。ファイルは最大 1 つを選択できます

ステップ 12.「**次へ**」をクリックします。

ステップ 13.「**無人ファイル**」タブで、以下の操作を行います。

a. OS イメージ・プロファイルに追加する無人ファイルを選択します。

サポートされるフォーマットのリストについては、カスタム無人ファイルのインポートを参照してください。

選択されたファイルは、構成ウィザードの完了後に適用されます。

b. 「**関連付けられた構成ファイル**」列から、無人ファイルに関連付ける構成ファイルを選択します。

c. オプションで、選択した構成ファイルで使用できるカスタム・マクロを選択するか、.xml 形式でカスタム・マクロを追加します。

ステップ 14.「**次へ**」をクリックします。

ステップ 15.「**インストール・スクリプト**」タブ (該当する場合) で、Windows OS イメージ・プロファイルに追加するインストール・スクリプトを選択します。ポスト・インストール・スクリプトは最大 1 つを選択できます。

サポートされるフォーマットのリストについては、カスタム・インストール・スクリプトのインポートを参照してください。

選択されたファイルは、構成ウィザードの完了後に適用されます。

注：「**ファイルのインポート**」アイコン () をクリックして、ローカルまたはリモート・システムから追加のインストール・スクリプトをインポートできます。

ステップ 16.「**次へ**」をクリックします。

ステップ 17.「**ソフトウェア**」タブで、Linux OS イメージ・プロファイルに追加するソフトウェアを選択します。

サポートされるフォーマットのリストについては、カスタム・ソフトウェアのインポートを参照してください。

選択されたファイルは、構成ウィザードの完了後に適用されます。

注：「**ファイルのインポート**」アイコン () をクリックして、ローカルまたはリモート・システムから追加のソフトウェアをインポートできます。

ステップ 18.「**次へ**」をクリックします。

ステップ 19.「**要約**」タブで設定を確認し、「**カスタマイズ**」をクリックしてカスタマイズされた OS イメージ・プロファイルを作成します。

終了後

カスタマイズされた OS イメージ・プロファイルは、「OS イメージの管理」ページの「**OS イメージ**」タブにあるベース・オペレーティング・システムの下にリストされます。

このページでは、以下の操作を実行できます。

- 「**プロファイルのインポート/エクスポート**」 ➡ 「**カスタマイズされたプロファイル・イメージのエクスポート**」をクリックして、カスタマイズされた OS イメージ・プロファイルをインポートし、ベース OS イメージに適用する (カスタマイズされた OS イメージ・プロファイルのインポートを参照)。
- 選択されたカスタム OS イメージ・プロファイルをエクスポートする。「**プロファイルのインポート/エクスポート**」 ➡ 「**カスタマイズされたプロファイル・イメージのエクスポート**」をクリックします。
- 「**編集**」アイコン ( ) をクリックして、選択済みのカスタマイズされた OS イメージ・プロファイルを変更します。
- 「**削除**」アイコン ( ) をクリックして、選択済みのカスタマイズされた OS イメージ・プロファイルを削除します。

グローバル OS デプロイメント設定の構成

共通設定は、オペレーティング・システムがデプロイされるときに、デフォルト設定として使用されます。

このタスクについて

「共通設定」ページでは、以下の設定を構成できます。

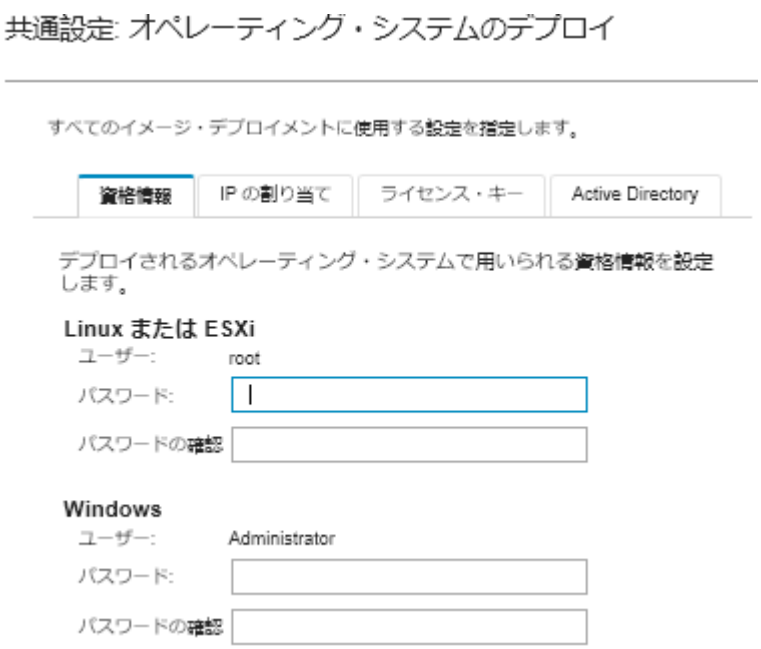
- オペレーティング・システムをデプロイするときに使用する管理者ユーザー・アカウントのパスワード
- サーバーに IP アドレスを割り当てる方法
- インストールされたオペレーティング・システムをアクティブ化するときに使用するライセンス・キー
- Windows オペレーティング・システムのデプロイメントの一環として Active Directory ドメインに参加 (オプション)

手順

すべてのサーバーに使用される共通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 のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「OS イメージのデプロイ」ページを表示します。

ステップ 2. 「**共通設定**」アイコン ( ) をクリックして、「共通設定: オペレーティング・システムのデプロイ」ダイアログを表示します。



ステップ 3. 「**資格情報**」タブで、オペレーティング・システムにログインするために使用する管理者アカウントのパスワードを入力します。

ステップ 4. 「**IP の割り当て**」タブで、以下のオプションを選択します。

a. **オプション**: 「**VLAN を使用する**」を選択して「ネットワーク設定」ダイアログで VLAN 設定を構成できるようにします (管理対象サーバーのネットワーク設定の構成を参照)。

注：注:

- Linux オペレーティング・システム・デプロイメントで VLAN タグ付けがサポートされていません。
- ThinkServer デバイスでのオペレーティング・システムのデプロイメントでは、VLAN タグ付けはサポートされていません。
- VLAN モードは、インベントリー内に MAC アドレスがあるサーバーでのみサポートされます。AUTO がそのサーバーで唯一の MAC アドレスである場合、そのサーバーへのオペレーティング・システムのデプロイに VLAN を使用することはできません。

b. デプロイされたオペレーティング・システムの構成時に、IP アドレスの割り当て方法を選択します。

注：XClarity Administrator管理に使用されるネットワーク・インターフェースは、「共通設定: オペレーティング・システムのデプロイメント」ダイアログで選択した IP アドレス方式と同じものを使用して、ベースボード管理コントローラーに接続されるよう構成する必要があります。たとえば、XClarity Administratorが管理用に eth0 を使用するよう設定され、デプロイ済み OS を構成するときに手動で割り当てられた静的 IPv6 アドレスの使用を選択した場合、eth0 はベースボード管理コントローラーと接続された IPv6 アドレスと一緒に構成されている必要があります。

- **静的 IPv4 アドレスを手動で割り当てる。**静的 IPv4 アドレスを割り当てる場合は、オペレーティング・システムをデプロイする前に、サーバーの静的 IPv4 アドレス、ゲートウェイ・アドレス、およびサブネット・マスクを構成してください (管理対象サーバーのネットワーク設定の構成を参照)。
- **動的ホスト構成プロトコル (DHCP) を使用して、アドレスを割り当てる。**ネットワークに DHCPv4 インフラストラクチャーが既に存在している場合は、そのインフラストラクチャーを使用してサーバーに IP アドレスを割り当てることができます。

注：DHCP IPv6 はオペレーティング・システムのデプロイメントでサポートされていません。

- **静的 IPv6 アドレスを手動で割り当てる。**静的 IPv6 アドレスを割り当てる場合は、オペレーティング・システムをデプロイする前に、サーバーの静的 IPv6 アドレス、ゲートウェイ・アドレス、およびサブネット・マスクを構成してください (管理対象サーバーのネットワーク設定の構成を参照)。

ステップ 5. **オプション**:「**ライセンス・キー**」タブで、インストールされた Windows オペレーティング・システムをアクティブ化するときに使用するグローバル・ボリューム・ライセンス・キーを指定します。

このタブでグローバル・ボリューム・ライセンス・キーを指定すると、「OS イメージのデプロイ」ページから、指定したライセンス・キーを任意の Windows OS イメージ・プロファイルに対して選択できます。

ヒント: XClarity Administrator では、グローバル・ボリューム・ライセンス・キー (Windows) と個別のリテール・ライセンス・キー (Windows と VMware ESXi の両方) を使用できます。デプロイ処理の一環として個別のリテール・ライセンス・キーを指定できます (オペレーティング・システム・イメージのデプロイを参照)。

ステップ 6. **オプション**:「**Active Directory**」タブで、Windows オペレーティング・システム・デプロイメントを行うための Active Directory 設定を構成します。Active Directory との統合については、Windows Active Directory との統合を参照してください。

ステップ 7. 「**OK**」をクリックして、ダイアログを閉じます。

管理対象サーバーのネットワーク設定の構成

ネットワーク設定は、各サーバーに固有の構成オプションです。管理対象サーバーにオペレーティング・システムをデプロイする前に、そのサーバーのネットワーク設定を構成する必要があります。

このタスクについて

DHCP を使用して動的に IP アドレスを割り当てる場合は、MAC アドレスを構成する必要があります。

静的 IP アドレスを使用する場合は、オペレーティング・システムを特定のサーバーにデプロイする前に、そのサーバーに対して以下のネットワーク設定を構成する必要があります。これらの設定が構成されると、サーバーのデプロイメント・ステータスは「動作可能」に変更されます。(一部のフィールドは固定 IPv6 アドレスでは使用できない点に注意してください。)

- ホスト名

  ホスト名は、以下の規則に従っている必要があります。
  - 各管理対象サーバーのホスト名は固有でなければなりません。
  - ホスト名にはピリオド (.) で区切られた複数の文字列 (ラベル) を含めることができます。
  - 各ラベルには ASCII 文字、数字、ダッシュ (-) を使用できます。ただし、文字列をダッシュで開始または終了することはできません。すべて数字にすることもできません。
  - 最初のラベルの長さは 2 ～ 15 文字にすることができます。後続のラベルの長さは 2 ～ 63 文字にすることができます。
  - ホスト名の合計の長さが、255 文字を超えないようにしてください。
- オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレス。

  MAC アドレスはデフォルトで「自動」に設定されています。この設定は、デプロイメント用に構成して使用できるイーサネット・ポートを自動的に検出します。検出された最初の MAC アドレス (ポート) が、デフォルトで使用されます。別の MAC アドレスとの接続が検出された場合は、XClarity Administrator ホストが自動的に再起動され、新しく検出された MAC アドレスをデプロイメントに使用します。

「ネットワーク設定」ダイアログの「**MAC アドレス**」ドロップダウン・メニューから OS デプロイメントに使用されている MAC アドレス・ポートのステータスを確認できます。複数のポートが稼働している場合、またはすべてのポートがダウンしている場合、デフォルトでは AUTO が使用されます。

注：

- 仮想ネットワーク・ポートはサポートされていません。1 つの物理ネットワーク・ポートを使用して複数の仮想ネットワーク・ポートをシミュレートしないでください。
- サーバーのネットワーク設定が AUTO に設定されている場合、XClarity Administrator はスロット 1 ～ 16 のネットワーク・ポートを自動的に検出できます。スロット 1 ～ 16 にあるポートのうち少なくとも 1 つは、XClarity Administrator に接続する必要があります。
- スロット 17 以上のネットワーク・ポートを MAC アドレスに使用する場合、AUTO を使用できません。代わりに、サーバーのネットワーク設定を、使用する特定のポートの MAC アドレスに設定する必要があります。
- ThinkServer サーバーでは、すべてのホスト MAC アドレスが表示されるわけではありません。多くの場合、AnyFabric Ethernet アダプターの MAC アドレスは「ネットワーク設定の編集」ダイアログにリストされます。他のイーサネット・アダプターの MAC アドレス (LAN-on-Motherboard など) はリストされません。アダプターの MAC アドレスが使用できない場合、非 VLAN デプロイメント用の自動方式を使用してください。

- IP アドレスとサブネット・マスク
- IP ゲートウェイ
- ドメイン・ネーム・システム (DNS) サーバー (2 つまで)
- 最大転送単位 (MTU) 速度
- VLAN IP モードが有効な場合は VLAN ID

VLAN を使用するように選択する場合は、構成しているホスト・ネットワーク・アダプターに VLAN ID を割り当てることができます。

手順

1 つ以上のサーバーのネットワーク設定を構成するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。

ステップ 2. 構成するサーバーを 1 つ以上選択します。最大 28 台のサーバーを選択して一度に構成できます。

ステップ 3. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックして「ネットワーク設定の編集」ページを表示します。

ステップ 4. 各サーバーのテーブルのフィールドに入力します。

ヒント: 一部のフィールドについては、各行に値を入力する代わりにテーブルのすべての行を更新することもできます。

a. 「**すべての行の変更**」 ➡ 「**ホスト名**」の順にクリックして、すべてのサーバーのホスト名を設定します。事前定義済みの名前付けスキームを使用することも、カスタム名前付けスキームを使用することもできます。

b. IP アドレスの範囲、サブネット・マスク、ゲートウェイを割り当てるには、「**すべての行の変更**」 ➡ 「**IP アドレス**」をクリックします。各サーバーに対して IP アドレスが割り当てられます。この割り当ては、表示されている最初の IP アドレスから始まり、最後の IP アドレスで終わります。サブネット・マスクとゲートウェイ IP アドレスが各サーバーに適用されます。

c. 「**すべての行の変更**」 ➞ 「**ドメイン・ネーム・システム (DNS)**」の順にクリックして、オペレーティング・システムが DNS ルックアップに使用する DNS サーバーを設定します。DNS サーバーがネットワークによって自動的に定義される場合、または DNS サーバーを定義しない場合は、「**なし**」を選択します。

d. 「**すべての行の変更**」 ➞ 「**最大転送単位 (MTU)**」をクリックし、デプロイされたオペレーティング・システムで構成されたイーサネット・アダプターに適用される MTU を設定します。

e. **すべての行の変更** ➞ **VLAN ID** の順にクリックして、オペレーティング・システムの VLAN タグ付け用に特定の VLAN ID を設定します。

   1 ～ 4095 の値を指定できます。デフォルト値は 1 で、VLAN モードが使用されないことを意味しています。

   このオプションは、「共通設定」で「VLAN を使用」が有効になっている場合のみ使用できます (グローバル OS デプロイメント設定の構成参照)。

   重要：

   - VLAN タグがネットワーク上で機能するために必要な場合のみ VLAN ID を指定します。**VLAN タグを使用**すると、ホスト・オペレーティング・システムと XClarity Administrator の間のネットワーク・ルーティング可能性に影響を与えることがあります。
   - シャーシまたはラック装着スイッチは VLAN タグ付けされたパケットを扱うために個別に構成する必要があります。これらのパケットを正しく取り扱うために XClarity Administrator とデータ・ネットワークが構成されていることを確認します。
   - VLAN モードは、インベントリー内に MAC アドレスがあるサーバーでのみサポートされます。AUTO がそのサーバーで唯一の MAC アドレスである場合、そのサーバーへのオペレーティング・システムのデプロイに VLAN を使用することはできません。
   - VLAN タグ付けは Linux オペレーティング・システム・デプロイメントではサポートされていません。ただし、一部のサーバーに VLAN を使用してデプロイし、同時に VLAN を使用しない他のサーバーにもデプロイする場合は、VLAN ID を 1 に設定して、VLAN モードで強制的にデプロイできます。

ステップ 5. 「OK」をクリックして、設定を保存します。設定は Web ブラウザーのローカル・ストレージ・キャッシュにのみ保存され、永続的に適用されます。

結果

「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページで、構成された各サーバーのデプロイメント・ステータスが「**動作可能**」となります。

管理対象サーバーの保管場所の選択

1 台以上のサーバーについて、オペレーティング・システム・イメージをデプロイする格納場所を選択します。

始める前に

格納場所を選択する前に、ストレージおよびブート・オプションの考慮事項を確認してください (オペレーティング・システム・デプロイメントの考慮事項を参照)。

オペレーティング・システムを次のタイプのストレージにデプロイできます。

- **論理ディスク・ドライブ**

  RAID コントローラーまたは SAS/SATA HBA に接続されているディスクのみがサポートされます。

Lenovo XClarity Administrator は、オペレーティング・システム・イメージを、管理対象サーバーに列挙された最初のローカル RAID ディスクにインストールします。

サーバー上で RAID 構成が正しく構成されていないか、非アクティブな場合、ローカル・ディスクは Lenovo XClarity Administrator に表示されない可能性があります。この問題を解決するには、構成パターン (ローカル・ストレージの定義を参照) またはサーバー上の RAID 管理ソフトウェアを使用して RAID 構成を有効にします。

注：

- M.2 ドライブも存在している場合は、ローカル・ディスク・ドライブをハードウェア RAID 用に構成する必要があります。
- SATA アダプターが有効な場合、SATA モードを「IDE」に設定*しないでください*。
- ThinkServer サーバーの場合、ローカル・ディスクにのみオペレーティング・システムをデプロイできます。SAN ストレージおよび組み込みハイパーバイザーはサポートされません。
- ThinkServer サーバーでは、サーバーで RAID 管理ソフトウェアを使用してのみ構成を行うことができます。

ローカルに取り付けられたディスク・ドライブに VMware ESXi 5.5 をデプロイするサンプル・シナリオについては、ローカル・ハードディスク・ドライブへの ESXi のデプロイを参照してください。

- **(ESXi のみ) Embedded hypervisor (USB または SD メディア・アダプター)**

  この場所は、VMware ESXi イメージが管理対象サーバーにデプロイされている場合にのみ適用できます。

  組み込みハイパーバイザーは以下のいずれかのデバイスです。

  - 以下のいずれかのサーバーにある特定の使用ポートにマウントされた IBM ライセンス USB キー (PN 41Y8298) または Lenovo ライセンス USB キー:
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - 次のサーバーにインストールされた SD メディア・アダプター:
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    また、ドライブを次のように構成する必要があります。
    - メディア・アダプターで適切なドライブが定義されている必要があります。
    - SD メディア・アダプターのモードは「**作動可能**」に設定する必要があります。
    - 所有者は「システム」または「システムのみ」である必要があります。
    - アクセスは「読み取り/書き込み」に設定されている必要があります。
    - ドライブに LUN 番号として 0 が割り当てられている必要があります。

    重要：SD メディア・アダプターが正しく構成されていないと、Lenovo XClarity Administrator から SD メディア・アダプターへのオペレーティング・システム・デプロイメントは正常に完了できません。

    SD メディア・アダプターのモードを「**構成**」に変更し、管理コントローラー CLI から `sdraid` コマンドを使用してメディア・アダプターを構成できます。SD メディア・アダプターのモードの設定と、CLI からのアダプターの構成について詳しくは、Integrated Management Module II オンライン・ドキュメントを参照してください。

2 つのハイパーバイザー・キーが管理対象サーバーにインストールされている場合、VMware インストーラーは、最初に列挙されているキーをデプロイ時に選択します。

注：Microsoft Windows を、ハイパーバイザー・キーがインストールされている管理対象サーバーにデプロイしようとすると、組み込みハイパーバイザー・キーを選択しなくても、問題が発生する場合があります。Microsoft デプロイメント・エラーが発生した場合は、組み込みハイパーバイザー・キーを管理対象サーバーから削除し、Microsoft Windows をそのサーバーに再度デプロイしてみてください。

- **M.2 ドライブ**

  Lenovo XClarity Administrator は、オペレーティング・システム・イメージを、管理対象サーバーで構成された最初の M.2 ドライブにインストールします。

  M.2 ストレージは、ThinkSystem サーバーでのみサポートされます。

  注意：管理対象デバイスに、ハードウェア RAID 用に構成されていないローカル・ドライブ (SATA、SAS、または SSD) および M.2 ドライブの両方がある場合、M.2 ドライブを使用する場合はローカル・ドライブを無効に、ローカル・ドライブを使用する場合は M.2 ドライブを無効にする必要があります。ウィザードのローカル・ストレージ・タブで「ローカル・ディスクの無効化」を選択するか、既存のサーバーから構成パターンを作成してから、拡張 UEFI パターンの M.2 デバイスを無効にすることで、構成パターンを使用して、オンボード・ストレージ・コントローラー・デバイス、およびレガシーと UEFI ストレージ・オプション ROM を無効にできます。

- **SAN ストレージ**

  Lenovo XClarity Administrator は、オペレーティング・システム・イメージを、管理対象サーバーで構成された SAN ブート・ターゲットにインストールします。

  以下のプロトコルがサポートされています。
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (Emulex VFA5.2 2x10 GbE SFP+ Adapter および FCoE/iSCSI SW または Emulex VFA5.2 ML2 2x10 GbE SFP+ Adapter および FCoE/iSCSI SW アダプターのみを使用)

  管理対象ラック・サーバーでは、Windows または RHEL は SAN ストレージにのみデプロイできます。管理対象サーバーで SAN ブート・ターゲットが構成されていることを確認します。FC SAN ブート・ターゲットも構成するには、サーバー・パターンを使用します (ブート・オプションの定義を参照)。

  VMware ESXi をデプロイする場合:

  - ローカル・ハードディスクが無効になっているか、サーバーから削除されている必要があります。ローカル・ハードディスクを無効にするには、サーバー・パターンを使用します (ローカル・ストレージの定義を参照)。
  - 複数の SAN ボリュームを使用できる場合は、最初のボリュームのみがデプロイで使用されます。

  インストール先の OS ボリュームが、オペレーション・システムに表示されている唯一のボリュームであることを確認します。

  サーバーに接続された SAN ボリュームに VMware ESXi 5.5 をデプロイするサンプル・シナリオについては、SAN ストレージへの ESXi のデプロイを参照してください。

注：各サーバーにハードウェア RAID アダプターまたは SAS/SATA HBA が取り付けられ構成されている。通常はオンボード Intel SATA ストレージ・アダプターにあるソフトウェア RAID または JBOD としてセットアップされているストレージは、サポートされません。ただし、ハードウェア RAID アダプターが存在せず、SATA アダプターがオペレーティング・システム・デプロイメントで「**AHCI SATA モード**」対応の場合、または JBOD に未構成の正常ディスクが設定されている場合は、機能する場合があります。詳しくは、XClarity Administrator オンライン・ドキュメントの OS インストーラーで XClarity Administrator にインストールするディスクが見つからないを参照してください。

手順

1 台以上の管理対象サーバーの格納場所を選択するには、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、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」をクリックして、「OS イメージのデプロイ」ページを表示します。

ステップ 2. ストレージ設定を変更するサーバーを選択します。

ステップ 3. **「選択の変更」 ➡ 「格納場所」**をクリックして、すべての選択したサーバーの格納場所の優先順位を変更します。最初の格納場所が適合しない場合は、次の格納場所を試します。

次の格納場所の優先順位を設定できます。
- **ローカル・ディスク・ドライブ・ストレージを使用**
- **ESXi が選択されている場合は、組み込みハイパーバイザー (USB または SD メディア・アダプター) を使用**
- **M.2 ドライブを使用**
- **SAN ストレージを使用**

ステップ 4. サーバーごとに、オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。以下の値から選択できます。この値は、前の手順の値に対応します。
- **ローカル・ディスク・ドライブ**
- **埋め込みハイパーバイザー**
- **M.2 ドライブ**
- **SAN ストレージ**

「**SAN ストレージ**」を選択した場合は、ダイアログが表示され、SAN ボリュームを構成することができます。デプロイメント中にターゲット SAN ボリュームに到達可能であることを確認します。

選択した格納場所がサーバーに対応していない場合、Lenovo XClarity Administrator は、オペレーティング・システムを、前の手順で定義した優先順位に従って次の格納場所にデプロイしようとします。

オペレーティング・システム・イメージのデプロイ

Lenovo XClarity Administrator を使用して、最大 28 台のサーバーに、オペレーティング・システム・イメージを同時にデプロイできます。

始める前に

ご使用の管理対象サーバーにオペレーティング・システムをデプロイする前に、オペレーティング・システム・デプロイメントの考慮事項をお読みください (オペレーティング・システム・デプロイメントの考慮事項を参照)。

「**OS イメージ**」タブで、デプロイするオペレーティング・システムの「**デプロイ・ステータス**」が「「動作可能」」に設定されていることを確認します。Windows オペレーティング・システムをデプ

ロイするには、WinPE ブート・ファイルが必要です。一致する WinPE ファイルが使用できない場合、「**デプロイ・ステータス**」は「「作動不能」」に設定され、オペレーティング・システムをデプロイできません。WinPE ファイルを手動でダウンロードおよびインポートする必要があります (ブート・ファイルのインポートを参照)。

「**OS イメージの管理**」タブで、「**すべて表示**」 ➡ 「**デプロイ・ステータス**」 をクリックして、OS イメージのリストをフィルターできます。「動作可能」、「作動不能」、および「警告」ステータスのサーバーのみをリストでフィルタリングできます。オペレーティング・システム・イメージのデプロイ・ステータスが「作動不能」の場合、そのオペレーティング・システムはデプロイ可能なオペレーティング・システムのリストに含まれないので注意してください。

英語のロケールはデフォルトでサポートされています。言語固有のロケールを指定する場合、カスタム構成ファイルおよび無人ファイルを使用する必要があります。詳しくは、構成可能なロケールと NTP サーバーを使用する SLES 12 SP3 のデプロイおよび日本語の Windows 2016 のデプロイを参照してください。

非 RAID で取り付けられたストレージへのオペレーティング・システム・デプロイメントはサポートされていません。

注意：サーバーに現在インストールされているオペレーティング・システムがある場合、OS イメージ・プロファイルをデプロイすると現在のオペレーティング・システムが上書きされます。

システム・ガードが有効になっている XCC2 を持つサーバーで、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。

手順

オペレーティング・システム・イメージを 1 台以上の管理対象サーバーにデプロイするには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。

ヒント: スケーラブル・マルチノード・システムでは、オペレーティング・システムがプライマリー・パーティションにデプロイされるため、プライマリー・パーティションのみがサーバー・リストに含まれます。

ステップ 2. オペレーティング・システムがデプロイされるサーバーを 1 台以上選択します。最大 28 台のサーバーに、オペレーティング・システム・イメージを一度にデプロイできます。

テーブルの列をソートすると特定のサーバーを見つけやすくなります。さらに、「**表示**」メニューのオプションを選択して特定のシャーシ、ラック、またはグループのデバイスのみをリストしたり、「**フィルター**」フィールドにテキスト (名前や IP アドレスなど) を入力して、表示されたデバイスのリストをフィルタリングできます。

ヒント: すべての計算ノードに同じオペレーティング・システムをデプロイする場合は、複数のシャーシから複数の計算ノードを選択できます。

ステップ 3. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックして、ネットワーク設定を構成します。

詳しくは、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。

ステップ 4. サーバーごとに、「**デプロイするイメージ**」列のドロップダウン・リストから、デプロイする OS イメージ・プロファイルを選択します。

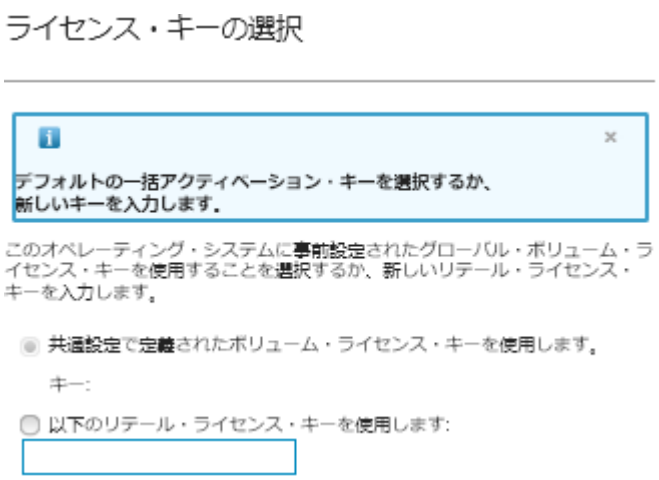
選択したサーバーと互換性がある OS イメージ・プロファイルを選択してください。「OS イメージの管理」ページの「**属性**」列にリストされたプロファイル属性から、互換性を確認できます。プロファイル属性について詳しくは、オペレーティング・システム・イメージ・プロファイルを参照してください。

ステップ 5. サーバーごとに、「**ライセンス・キー**」アイコン ( ) をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。

XClarity Administrator では、デフォルト・ボリューム・ライセンス・キー (Windows) と個別の販売キー (Windows と VMware ESXi) を使用できます。

「共通設定」ダイアログで指定したグローバル・ボリューム・ライセンス・キーを使用するには、「**共通設定で定義されたボリューム・ライセンス・キーを使用します**」を選択します。グローバル・ボリューム・ライセンスについて詳しくは、グローバル OS デプロイメント設定の構成を参照してください。

個別のリテール・ライセンス・キーを使用するには、「**以下のリテール・ライセンス・キーを使用します**」を選択し、続くフィールドにキーを入力します。



ステップ 6. **オプション**: 任意のサーバーに対して Windows オペレーティング・システムを選択した場合、オペレーティング・システム・デプロイメントの一環として Windows オペレーティング・システムを Active Directory ドメインに参加させるには、オペレーティング・システム・イメージの横に表示される「**フォルダー**」アイコン ( ) をクリックし、Active Directory 名を選択します。

「共通設定」ダイアログで指定したデフォルト Active Directory を使用するには、「**共通設定で定義された Active Directory を使用します**」を選択します。Active Directory ドメインへの参加について詳しくは、Windows Active Directory との統合を参照してください。

個々の Active Directory を使用するには、「**次の Active Directory を使用します**」を選択して Active Directory ドメインを選択します。

ステップ 7. サーバーごとに、オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。
- **ローカル・ディスク・ドライブ**
- **埋め込みハイパーバイザー**
- **M.2 ドライブ**
- **SAN ストレージ**

選択した格納場所がサーバーに対応していない場合、XClarity Administrator は、オペレーティング・システムを優先順位に従って次の格納場所にデプロイしようとします。

注：ThinkServer サーバーの場合は、「**ローカル・ディスク**」のみ使用できます。

格納場所を構成する方法について詳しくは、管理対象サーバーの保管場所の選択を参照してください。

注：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、管理対象サーバーから切り離します。

ステップ 8. 選択したサーバーすべてのデプロイメント・ステータスが「動作可能」になっていることを確認します。

重要：選択したサーバーすべてのデプロイ・ステータスが「動作可能」になっていることを確認します。サーバーのステータスが「作動不能」の場合、そのサーバーにオペレーティング・システム・イメージをデプロイすることはできません。「**作動不能**」リンクをクリックして、問題解決に役立つ情報を取得します。ネットワーク設定が無効の場合、「**選択の変更**」 ➔ 「**ネットワーク設定**」をクリックして、ネットワーク設定を構成します。

ステップ 9. 「**イメージのデプロイ**」アイコン ( ) をクリックして、オペレーティング・システム・デプロイメントを開始します。

カスタム構成設定が OS イメージ・プロファイルに追加されている場合、「OS イメージのデプロイ」ダイアログに「**カスタム設定**」タブが表示されます。カスタム設定、サーバーの共通設定、および特定のサーバーの設定を指定し、「**次へ**」をクリックして OS デプロイメントを続行します。必須のカスタム構成設定のいずれかに指定が入力されていない場合、OS デプロイメントは進行されないことに注意してください。

終了後

ジョブ・ログからデプロイメント・プロセスのステータスを監視できます。XClarity Administrator のメニューで、「**監視**」 ➡ 「**ジョブ**」の順にクリックします。ジョブ・ログについて詳しくは、ジョブの監視を参照してください。

サーバーがインストールの進行状況を監視するように、ベースボード管理コントローラーを使用してリモート制御セッションをセットアップすることもできます。リモート制御について詳しくは、リモート制御を使用したコンバージド、Flex System、NeXtScale および System x サーバーの管理を参照してください。

オペレーティング・システムのデプロイメント情報が保存されています。デプロイメント情報を表示するには、「**プロビジョニング**」 ➡ 「**OS アクセスの管理**」をクリックし、サーバー名の上にマウス・ポインターを移動します。

Windows Active Directory との統合

Lenovo XClarity Administrator を使用して Windows イメージをデプロイするときに、オペレーティング・システム・デプロイメントの一環として Active Directory ドメインに参加できます。

始める前に

Windows イメージ・デプロイメントの一環として Active Directory ドメインに参加するには、管理サーバーと、影響を受ける Active Directory ドメイン・コントローラーを実行している Windows Server の両方を構成する必要があります。この構成を実行するには以下のアクセス権が必要です。

- Active Directory サーバーのドメインに対する認証および参加の権限を持つ管理者アカウント。このアカウントには、デフォルトの Domain Administrators グループと同等の権限が必要です。このグループのアカウントを使用してこの構成を行うこともできます。
- ドメイン・コントローラーを実行している Active Directory サーバーに解決されるドメイン・ネーム・システム (DNS) へのアクセス。この DNS は、オペレーティング・システムをデプロイするサーバーの「**ネットワーク設定**」 ➡ 「DNS」オプションで指定されている必要があります。
- オペレーティング・システムをデプロイするには、事前に Active Directory サーバーの管理者がドメイン・サーバーで必要なコンピューター名を作成している必要があります。参加試行の際にコンピューター名は作成されません。名前が指定されていないと参加できません。
- Active Directory サーバーの管理者は、「**ネットワーク設定**」 ➡ 「**ホスト名**」フィールドをクリックして、イメージをデプロイするサーバーのホスト名を、目的の組織単位のコンピューター名として指定する必要があります。

  指定するホスト名 (コンピューター名) は固有でなければなりません。別の Windows インストールによって既に使用されている名前を指定すると参加に失敗します。

以下のいずれかの方法を使用して Active Directory ドメインに参加できます。

- **Active Directory ドメインを使用**

  事前定義されたドメインのリストから特定の Active Directory ドメインを選択できます。以下の手順に従って、XClarity Administrator で Active Directory ドメインを定義します。複数のドメインを使用する場合は、ドメイン名ごとにこの手順を繰り返します。

  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「OS イメージのデプロイ」ページを表示します。

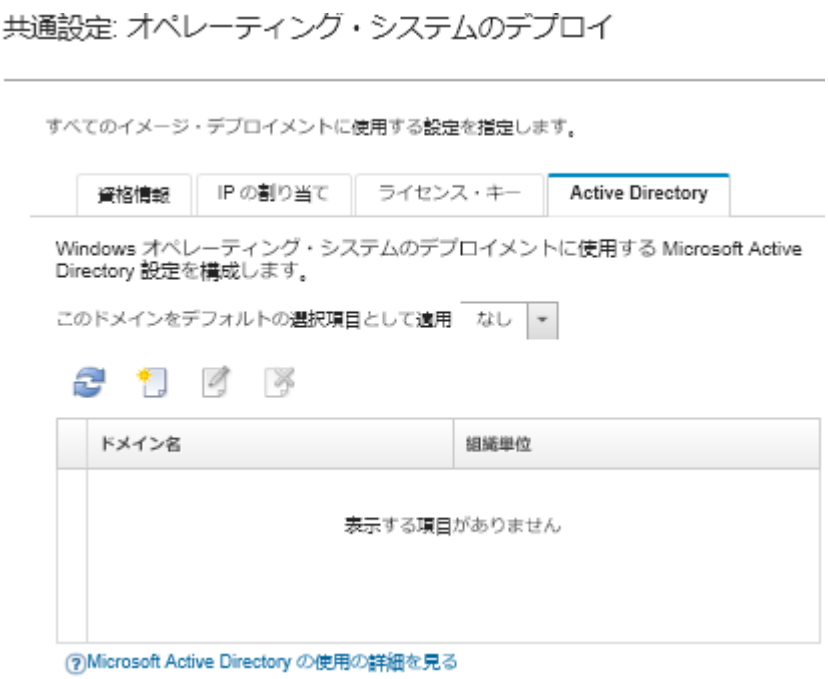
2. 「**共通設定**」アイコン ( ) をクリックして、「共通設定: オペレーティング・システムのデプロイ」ダイアログを表示します。
3. 「**Active Directory**」タブをクリックします。
4. 「**作成**」アイコン ( ) をクリックして、「新しい Active Directory ドメインの追加」ダイアログを表示します。
5. ドメイン・ネームと組織装置を指定します。

   オペレーティング・システム・デプロイメントでは、ドメインへの参加とドメイン内の組織単位の作成がサポートされています。組織単位を指定する場合は、参加の際に OU を明示的に指定する必要はありません。Active Directory では、ドメイン名とコンピューター名を使用して自動的に適切な OU が生成されます。
6. 「**OK**」をクリックします。

- **デフォルト Active Directory ドメインの使用**

  共通設定で定義されたデフォルトの Active Directory ドメインの使用を選択できます。以下の手順に従って、XClarity Administrator でデフォルト Active Directory ドメインを設定します。

  1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「OS イメージのデプロイ」ページを表示します。
  2. 「**共通設定**」アイコン ( ) をクリックして、「共通設定: オペレーティング・システムのデプロイ」ダイアログを表示します。
  3. 「**Active Directory**」タブをクリックします。



  4. 「**このドメインをデフォルトの選択項目として適用**」ドロップダウン・メニューから、Windows のすべてのデプロイにデフォルトで使用する Active Directory ドメインを選択します。
  5. 「**OK**」をクリックします。

- **メタデータ BLOB データの使用**

  Active Directory コンピューター・アカウント・メタデータ (Base-64 でエンコードされた BLOB 形式) を使用すると、任意のサーバーの Active Directory ドメインに参加できます。メタデータ BLOB データを生成するには、以下の手順を実行します。

1. 管理者アカウントを使用してコンピューターにログインします。コンピューターは、参加する Active Directory ドメインの一部でなければなりません。
2. 「**スタート**」 ➡ 「**プログラム**」 ➡ 「**アクセサリ**」をクリックします。「**コマンド・プロンプト**」を右クリックし、「**管理者として実行**」をクリックします。
3. C:\windows\system32 ディレクトリーに移動します。
4. 次の形式を使用して `djoin` コマンドを実行し、オフラインでのドメイン参加を実行します。
   `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

   ここで、それぞれ以下の意味があります。

   – *<AD_domain_name>* は、Active Directory ドメインの名前です。
   – *<hostname>* は、イメージをデプロイするサーバーのホスト名です。「**ネットワーク設定**」 ➡ 「**ホスト名**」フィールドをクリックして、目的の組織単位のコンピューター名として指定します。

   このコマンドは、メタデータ BLOB データを含む `blob` というファイルを作成します。このファイルの内容は、Active Directory 参加の詳細を指定するためにオペレーティング・システムのデプロイメント・プロセスにより使用されるため、このデータは近くに取っておいてください。

   メタデータ BLOB データは機密データです。

オペレーティング・システム・イメージのデプロイについて詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

手順

Active Directory ドメインに参加するには、以下の手順を実行します。

ステップ 1. Windows オペレーティング・システム・イメージを OS イメージ・リポジトリーにインポートします (オペレーティング・システム・イメージのインポートを参照)。

ステップ 2. オペレーティング・システムがデプロイされるサーバーを 1 台以上選択します。最大 28 台のサーバーに、オペレーティング・システム・イメージを一度にデプロイできます。

ヒント: すべての計算ノードに同じオペレーティング・システムをデプロイする場合は、複数のシャーシから複数の計算ノードを選択できます。

ステップ 3. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックして、ネットワーク設定を構成します。

a. 「**すべての行の変更**」 ➡ 「**ドメイン・ネーム・システム (DNS)**」をクリックし、少なくとも Active Directory ドメインに解決される DNS を指定します。

b. サーバーごとに、参加するドメインと組織単位内の既存のコンピューター名と一致するホスト名を指定します。

ネットワーク設定について詳しくは、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。

ステップ 4. サーバーごとに、「**Image to Deploy**」列でデプロイする Windows オペレーティング・システム・イメージを選択します。フォルダー・アイコンとライセンス・キー・アイコンが、イメージ名の横に表示されます。

ステップ 5. サーバーごとに、「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。

ステップ 6. サーバーごとに、「**フォルダー**」アイコン () をクリックして、Active Directory ドメインを指定します。以下のいずれかの値を選択できます。

- デフォルト・ドメインを使用する場合は、**共通設定で定義された Active Directory を使用します。**
- 特定のドメインを選択する場合は、**次の Active Directory を使用します。**
- BLOB ファイルの内容を指定するには、**メタデータ・ブロック・データを使用します。**

  メタデータ BLOB データには機密情報が含まれており、フィールドに表示されません。この情報は、デプロイメント操作が完了するまでのみ使用可能です。永続的ではありません。

ステップ 7. サーバーごとに、オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

- **ローカル・ディスク・ドライブ**
- **埋め込みハイパーバイザー**
- **M.2 ドライブ**
- **SAN ストレージ**

選択した格納場所がサーバーに対応していない場合、XClarity Administrator は、オペレーティング・システムを優先順位に従って次の格納場所にデプロイしようとします。

格納場所を構成する方法について詳しくは、管理対象サーバーの保管場所の選択を参照してください。

注：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、管理対象サーバーから切り離します。

ステップ 8. 選択したサーバーすべてのデプロイメント・ステータスが「動作可能」になっていることを確認します。

サーバーのステータスが「作動不能」の場合、そのサーバーにオペレーティング・システム・イメージをデプロイすることはできません。「**作動不能**」リンクをクリックして、問題解決に役立つ情報を取得します。ネットワーク設定が無効の場合、「**選択の変更**」 ➞ 「**ネットワーク設定**」をクリックして、ネットワーク設定を構成します。

ステップ 9. 「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。

「デプロイの確認」ダイアログが表示され、Active Directory サーバーに対する認証とドメインへの参加に使用する資格情報の入力を求められます。セキュリティー上の理由で、これらの資格情報は XClarity Administrator に保管されていません。ドメインに参加するすべての Windows のデプロイに対して資格情報を指定する必要があります。

ジョブ・ログからデプロイメント・プロセスのステータスを監視できます。XClarity Administrator のメニューで、「**監視**」 → 「**ジョブ**」の順にクリックします。ジョブ・ログについて詳しくは、ジョブの監視を参照してください。

結果

オペレーティング・システム・デプロイメントが完了したら、Web ブラウザーを開いて、「ネットワーク設定の編集」ページで指定した IP アドレスにアクセスしてログオンし、構成プロセスに進みます。

OS デプロイメントのシナリオ

このシナリオを使用してオペレーティング・システムをカスタマイズし管理対象サーバーにデプロイします。

カスタム・デバイス・ドライバーを伴う RHEL のデプロイ

このシナリオでは、Red Hat Enterprise Linux (RHEL) オペレーティング・システムおよびベース・オペレーティング・システムにはない追加のデバイス・ドライバーをインストールします。追加のデバイス・ドライバーが含まれているカスタム・プロファイルが使用されます。カスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。

始める前に

Lenovo XClarity Administrator を使用してオペレーティング・システムをデプロイする場合、オペレーティング・システムには、ハードウェア環境に合ったイーサネット、Fibre Channel およびストレージ・アダプターのデバイス・ドライバーが含まれている必要があります。デバイス・ドライバーがオペレーティング・システムに含まれていない場合、そのアダプターは OS デプロイメントではサポートされません。XClarity Administrator v1.2.0 以降では、デバイス・ドライバーを追加してオペレーティング・システムをカスタマイズできます。

デバイス・ドライバーは Lenovo YUM リポジトリー Web ページ やベンダー (Red Hat など) から入手するか、独自に生成したカスタム・デバイス・ドライバーを使用して入手できます。一部の Windows デバイス・ドライバーの場合、デバイス・ドライバーをインストール実行ファイルからローカル・システムに抽出して .zip アーカイブ・ファイルを作成することにより、カスタム・デバイス・ドライバーを生成できます。

注：RHEL デバイス・ドライバーは .rpm または .iso イメージ形式の である必要があります。

手順

カスタム・デバイス・ドライバーを使用して RHEL をデプロイするには、以下の手順を実行します。

ステップ 1. Red Hat Web サイトからローカル・システムに基本 RHEL オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン ( ) をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする RHEL イメージを探して選択します (例: `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。

7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに、カスタム・デバイス・ドライバーをダウンロードして、ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、XClarity Administrator オンライン・ドキュメントの デバイス・ドライバーのインポート を参照してください。

1. 「**デバイス・ドライバー**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに RHEL を選択します。
5. オペレーティング・システム・バージョンを選択します。
6. デバイス・タイプを選択します。
7. 「**参照**」をクリックし、インポートするデバイス・ドライバーを見つけて選択します (例: kmod-i40e-2.0.12-1.el7.x86_64.rpm)。
8. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 3. カスタムデバイス・ドライバーを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: Virtualization)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: Custom RHEL with device drivers) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプとして「**なし**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、プロファイルに含めるカスタム・デバイス・ドライバーを選択し、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
7. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 4. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom RHEL with device drivers) を選択します。

注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

d. (オプション)「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。

e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

注：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、管理対象サーバーから切り離します。

f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**要約**」タブで設定を確認します。
5. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ

このシナリオでは、カスタム・ソフトウェア (Apache HTTP、PHP、および hello world PHP アプリケーション) を含む RHEL オペレーティング・システムをインストールします。カスタム無人が含まれるカスタム OS イメージ・プロファイルが使用されます。これにより、yum リポジトリを使用できるように内部 Lenovo RHEL サブスクリプション サービスにオペレーティング・システムを登録し、Apache パッケージおよび PHP パッケージをインストールして、Apache 接続を許可するようにファイアウォールを構成し、Hello World PHP アプリケーションを作成して、Apache Web サーバー・ディレクトリーにコピーし、PHP をサポートするように Apache 構成ファイルを構成します。

始める前に

カスタム・ソフトウェアを含む RHEL をデプロイするには、いくつか方法があります。この例では、カスタム OS イメージ・プロファイルに含めるカスタム無人ファイルを使用します。また、リポジトリーにインポートし、カスタム OS イメージ・プロファイルに含めるカスタム・ソフトウェアをインストールするポスト・インストール・スクリプトを使用することもできます。ポスト・インストール・スクリプトを使用したソフトウェアのインストールについては、カスタム・ソフトウェアおよびポスト・インストール・スクリプトを使用した RHEL および、Hello World PHP アプリケーションのデプロイ を参照してください。

このシナリオでは、以下のサンプル・ファイルを使用します。

- RHEL_installSoftware_customUnattend.cfg このカスタム無人ファイルは、構事前定義済みのカスタム・マクロの値を使用し、カスタム・ソフトウェアをインストール、構成します。

手順

カスタム無人ファイルを使用して、カスタム・ソフトウェアを含む RHEL をデプロイするには、以下の手順を実行します。

ステップ 1. Red Hat Web サイトからローカル・システムに基本 RHEL オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。

2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする RHEL イメージを探して選択します (例: RHEL-*<ver>*-*<date>*-Server-x86_64-dvd1.iso)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. RHEL 無人 (kickstart) ファイルを変更して、オペレーティング・システムを RHEL サテライト登録サービスに登録し、HTTP (Apache) および PHP パッケージをインストールし、シンプルな Hello World PHP アプリケーションを作成し、必須の事前定義済みマクロと、必要に応じて IP アドレス、ゲートウェイ、DNS とホスト名の設定などその他の事前定義済みマクロを追加し、OS イメージ・リポジトリーにそのカスタム・ファイルをインポートします。詳しくは、カスタム無人ファイルのインポートを参照してください。

RHEL 衛星にホストを登録するためのコマンドを追加します。例:

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

重要：無人ファイルの例では、サブスクリプション・サービスの構成に基づいて、サテライト・サーバーおよび組織の IP アドレスを指定します。

ホストを更新し、apache および php パッケージをインストールして構成するコマンドを追加します。例:

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
```

```
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

注：この無人ファイルの例では、kickstart ファイルとともにインストールされるデフォルトのパッケージを変更します。%packages セクションの一環として、Apache パッケージと PHO パッケージを指定します。

ESXi と RHEL の場合にのみ、XClarity Administrator では、UI で定義されたすべてのネットワーク設定を無人ファイルに追加する **#predefined.unattendSettings.networkConfig#** マクロ、および UI で定義されているすべてのストレージ設定を無人ファイルに追加する **#predefined.unattendSettings.storageConfig#** マクロが提供されます。この無人ファイルの例には、こうしたマクロが既に含まれています。

XClarity Administrator はまた、OOB ドライバー挿入、ステータスのレポート、ポスト・インストール・スクリプト、カスタム・ソフトウェアなど、一部の基本的な便宜マクロを提供しています。ただし、これらの事前定義マクロを利用するには、次のマクロをカスタム無人ファイルで指定する必要があります。ファイルの例には、必要なマクロが既に含まれています。

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

サンプルのファイルには、必須マクロおよびターゲット・サーバーおよびタイムゾーンのネットワーク設定を動的に指定する追加の事前定義済みマクロが既に含まれています。マクロの無人ファイルへの追加について詳しくは、事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

また、XClarity Administrator のジョブ・ログにカスタム・メッセージを送信するコマンドを追加することもできます。詳しくは、インストール・スクリプトに報告するカスタム・ステータスの追加を参照してください。

カスタム・インストール・スクリプトをインポートするには、以下の手順を実行します。詳しくは、カスタム・インストール・スクリプトのインポートを参照してください。

カスタム無人ファイルをインポートするには、以下の手順を実行します。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに RHEL を選択します。
5. 「**参照**」をクリックし、インポートするソフトウェア・ファイルを検索して選択します (例: RHEL_installSoftware_customUnattend.cfg)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 3. カスタム・ソフトウェアおよびポスト・インストール・スクリプトを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。

2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Basic`)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: `Custom RHEL with software using custom unattend`) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**無人ファイルのみ**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
7. 「**無人ファイル**」タブで、カスタム無人ファイルを選択し、(例: `RHEL_installSoftware_customUnattend.cfg`) 「**次へ**」をクリックします。
8. 「**インストール・スクリプト**」タブで、「**次へ**」をクリックします。
9. 「**要約**」タブで設定を確認します。
10. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 4. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント:

      - VLAN 設定は、VLAN モードが 「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」 で設定されている場合のみ使用できます。
      - 「ネットワーク設定」ダイアログで指定したネットワーク設定が、無人ファイルの実行時に #predefined.hostPlatforms.networkSettings.*<setting>*# マクロを使用して無人ファイルに追加されます。

   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_`Custom RHEL with software using custom unattend`) を選択します。

      注: すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

   d. (オプション) 「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。
   e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

      注: 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、管理対象サーバーから切り離します。

f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン ( ) をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「カスタム設定」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム無人ファイル (例: `RHEL_installSoftware_customUnattend.cfg`) を選択します。

5. 「**要約**」タブで設定を確認します。
6. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム・ソフトウェアおよびポスト・インストール・スクリプトを使用した RHEL および、Hello World PHP アプリケーションのデプロイ

このシナリオでは、カスタム・ソフトウェア (Apache HTTP、PHP、および hello world PHP アプリケーション) を含む RHEL オペレーティング・システムをインストールします。カスタム・ソフトウェアとポスト・インストール・スクリプトが含まれるカスタム OS イメージ・プロファイルが使用されます。このポスト・インストール・スクリプトは、yum リポジトリを使用できるように内部 Lenovo RHEL サブスクリプション サービスにオペレーティング・システムを登録し、Apache パッケージおよび PHP パッケージをインストールして、Apache 接続を許可するようにファイアウォールを構成し、Hello World PHP アプリケーションを作成して、Apache Web サーバー・ディレクトリーにコピーし、PHP をサポートするように Apache 構成ファイルを構成します。カスタム・ソフトウェア・パッケージは、デプロイ中にホストにエクスポートされ、カスタム・ポスト・インストール・スクリプトで使用可能になります。

始める前に

RHEL および Hello World PHP アプリケーションは、いくつかの方法でデプロイできます。この例では、リポジトリーにインポートし、カスタム OS イメージ・プロファイルに含めるカスタム・ソフトウェアをインストールするポスト・インストール・スクリプトを使用します。カスタム OS イメージ・プロファイルに含めるカスタム無人ファイルを使用することもできます。カスタム無人ファイルを使用したソフトウェアのインストールについては、カスタム無人ファイルを使用した RHEL および Hello World PHP アプリケーションのデプロイ を参照してください

このシナリオでは、以下のサンプル・ファイルを使用します。

- httpd.conf。Apache HTTP 対応のインストール・ファイルです。

- hello_world.php Hello World PHP アプリケーションです。
- RHEL_installSoftware_customScript.sh このポスト・インストール・スクリプトは、カスタム・ソフトウェアをインストール、構成します。

注：

- RHEL インストール・スクリプトは以下のいずれかの形式です。Bash (.sh)、Perl (.pm または .pl)、Python (.py)
- ソフトウェア・ファイルおよびインストール・スクリプトは、デプロイメント時に指定されたカスタム・データとファイル・パスからインストールされます。デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。

手順

ポスト・インストール・スクリプトを使用して、カスタム・ソフトウェアを含む RHEL をデプロイするには、以下の手順を実行します。

ステップ 1. Red Hat Web サイトからローカル・システムに基本 RHEL オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン ( ) をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする RHEL イメージを探して選択します (例: `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに、カスタム・ソフトウェアをダウンロードして、ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム・ソフトウェアのインポートを参照してください。

ヒント: カスタム・ソフトウェアを XClarity Administrator にインポートするには、そのファイルを .tar.gz ファイルに含める必要があります。この例では、続行する前に、`httpd.conf` と `index.php` のソフトウェア・ファイルを `RHEL_installSoftware_customsw.tar.gz` というファイル名の tar.gz に圧縮しています。

1. 「**ソフトウェア**」タブをクリックします。
2. 「**インポート**」アイコン ( ) をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに `RHEL` を選択します。
5. 「**参照**」をクリックし、インポートするソフトウェア・ファイルを検索して選択します (例: `RHEL_installSoftware_customsw.tar.gz`)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 3. カスタム・ポスト・インストール・スクリプトを作成して、OS イメージ・リポジトリーにファイルをインポートします。

RHEL 衛星にホストを登録するためのコマンドを追加します。例:

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

ホストを更新し、apache および php パッケージをインストール、構成するコマンドを追加します。例:

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

たとえば、Web serversatellite PHP アプリケーションを追加するためのコマンドを追加します。

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Apache HTTP を構成するためのコマンドを追加します。例:

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

これらのコマンドは、抽出されたデータおよびソフトウェア・ファイルへのパスに事前定義済みマクロを使用することに注意してください (**predefined.otherSettings.deployDataAndSoftwareLocation**)。

また、XClarity Administrator のジョブ・ログにカスタム・メッセージを送信するコマンドを追加することもできます。詳しくは、インストール・スクリプトに報告するカスタム・ステータスの追加を参照してください。

カスタム・インストール・スクリプトをインポートするには、以下の手順を実行します。詳しくは、カスタム・インストール・スクリプトのインポートを参照してください。

1. 「**インストール・スクリプト**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに RHEL を選択します。
5. 「**参照**」をクリックして、インポートするポスト・インストール・スクリプト (例: RHEL_installSoftware_customScript.sh) を検索して選択します。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. カスタム・ソフトウェアおよびポスト・インストール・スクリプトを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: Basic)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前を入力します (例: Custom RHEL with software using post-installation script)。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。

c. カスタマイズ・タイプとして「**なし**」を選択します。
d. 「**次へ**」をクリックします。

5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、ソフトウェア・インストール・ファイル (例: `httpd.conf` および `index.php`) を選択し、「**次へ**」をクリックします。
7. 「**インストール・スクリプト**」タブで、インストール・スクリプト (例: `RHEL_installSoftware_customScript.sh`) を選択し、「**次へ**」をクリックします。
8. 「**要約**」タブで設定を確認します。
9. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 5. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom RHEL with software using post-installation script) を選択します。

      注: すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。
   d. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

      注: 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、管理対象サーバーから切り離します。
   e. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。
3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**要約**」タブで設定を確認します。
5. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム・パッケージとタイム・ゾーンを使用した SLES 12 SP3 のデプロイ

このシナリオでは、SLES 12 SP3 オペレーティング・システム (英語版) と、いくつかのオプション SLES パッケージをインストールします。また、タイム・ゾーンの設定も必要です。カスタム構成ファイルおよびカスタム無人ファイルを含むカスタム OS イメージ・プロファイルが使用されます。このカスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。デプロイする SLE パッケージの選択とタイム・ゾーンの指定は「**カスタム設定**」タブで行います。選択された値は、カスタム無人ファイルのカスタム・マクロに置き換えられ、SLES autoyast インストーラー無人ファイルはこれらの値を使用してオペレーティング・システムを構成します。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- SLES_installPackages_customConfig.json。この構成ファイルでは、タイム・ゾーンの入力およびオプションの SLES パッケージ (Linux、Apache、MySQL、PHP ソフトウェア・パッケージ、SLES メール・サーバー・パッケージ、および SLES ファイル・サーバー・パッケージ) のインストールを求められます。
- SLES_installPackages_customUnattend.xml この無人ファイルは、構成ファイルで定義されている事前定義済みマクロおよびカスタム・マクロの値を使用します。

手順

カスタム OS イメージ・プロファイルを使用して SLES 12 SP3 をサーバーにデプロイするには、以下の手順を実行します。

ステップ 1. SUSE Web サイトからローカル・システムに基本 SLES オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン ( ) をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする SLES 12 SP3 イメージを探して選択します (例: `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. カスタム構成設定ファイルを作成して、OS イメージ・リポジトリーにファイルをインポートします。

構成設定ファイルは、OS デプロイメント・プロセス中に動的に収集する必要があるデータを記述する JSON ファイルです。このシナリオでは、インストールできるオプション SLES パッケージ (SLES Linux、Apache、MySQL、PHP ソフトウェア・パッケージ、SLES メール・サーバー・パッケージ、および SLES ファイル・サーバー・パッケージ) と、各 OS デプロイメントで使用するタイム・ゾーンを指定してみます。構成設定ファイルの作成について詳しくは、カスタム・マクロを参照してください。

構成設定ファイルをインポートするには、以下の手順を実行します。詳しくは、カスタム構成設定のインポートを参照してください。

1. 「**構成ファイル**」タブをクリックします。
2. 「**インポート**」アイコン ( ) をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに `SLES` を選択します。
5. 「**参照**」をクリックし、インポートする構成設定ファイルを検索して選択します (例: `SLES_installPackages_customConfig.json`)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

注：カスタム構成設定をファイルをインポートすると、XClarity Administrator によって、ファイル内の各設定についてカスタム・マクロが生成されます。これらのマクロは無人ファイルに追加できます。OS デプロイメント中、マクロは実際の値に置き換えられます。

ステップ 3. SLES 無人ファイルを変更して、オプションの SLES パッケージおよびタイム・ゾーンの動的な値を指定してから、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム無人ファイルのインポートを参照してください。

<general> セクションで、タイム・ゾーン情報を追加します。例:

```
<timezone>
  <hwclock></hwclock>
  <timezone></timezone>
</timezone>
```

<patterns> セクションで、3 つのパターン・タグを追加します。これらのタグはオプションの SLES パッケージ設定のカスタム・マクロで使用されます。例:

```
<patterns config:type="list">
  <pattern>32bit</pattern>
  <pattern>Basis-Devel</pattern>
  <pattern>Minimal</pattern>
  <pattern>WBEM</pattern>
  <pattern>apparmor</pattern>
  <pattern>base</pattern>
  <pattern>documentation</pattern>
  <pattern>fips</pattern>
  <pattern>gateway_server</pattern>
  <pattern>ofed</pattern>
  <pattern>printing</pattern>
  <pattern>sap_server</pattern>
  <pattern>x11</pattern>
  <pattern></pattern>
  <pattern></pattern>
  <pattern></pattern>
</patterns>
```

注：

- これらのタグはサンプル無人ファイルにあります。
- カスタム無人ファイルを使用すると、事前定義済み無人ファイルを使用した場合に得られる多くの正常な便宜機能が XClarity Administrator では提供されません。たとえば、<DiskConfiguration>、<ImageInstall>、<ProductKey> といったターゲット、管理者用 <UserAccounts>、ネットワーキング用 <Interfaces>、およびインストール機能の <package> リストが、アップロードするカスタム無人ファイルで指定されている必要があります。

カスタム無人ファイルをインポートするには、以下の手順を実行します。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに SLES を選択します。
5. 「**参照**」をクリックし、インポートする無人ファイルを検索して選択します (例: SLES_installPackages_customUnattend.xml)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

   注：無人ファイルに事前定義マクロが欠落しているという警告が表示されます。今のところ警告は無視しても構いません。事前定義済みマクロは次のステップで追加します

7. 警告ダイアログの「**閉じる**」をクリックして「無人ファイルの編集」ダイアログを開きます。

ステップ 4. カスタム無人ファイルをカスタム構成設定ファイルに関連付け、構成設定ファイルから無人ファイルに必要な事前定義済みマクロおよびカスタム・マクロ (設定) を追加します。詳しくは、無人ファイルを構成設定ファイルに関連付けるおよび事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

ヒント: 必要に応じて、カスタム構成設定ファイルにカスタム無人ファイルを関連付けて、無人ファイルのインポート時にマクロを追加できます。

1. 「無人ファイルの編集」ダイアログで、「**構成ファイルの関連付け**」ドロップダウン・リストから無人ファイルに関連付ける構成設定ファイルを選択します (例: SLES_installPackages_customConfig)。
2. 必要な事前定義済みマクロを無人ファイルに追加します。
   a. 「**使用できるマクロ**」ドロップダウン・リストから、「**事前定義済み**」を選択します。
   b. 無人ファイルの行 1 の後ろ (<xml> タグの後ろ) の任意の場所にカーソルを置きます。
   c. 使用可能な事前定義済みマクロのリスト内の 「predefined」 → 「unattendSettings」 リストを展開します。
   d. 「preinstallConfig」および「postinstallConfig」マクロをクリックして、マクロを無人ファイルに追加します。

   例:

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

3. タイム・ゾーンを指定するためのカスタム・マクロを追加します。
   a. 「**使用できるマクロ**」ドロップダウン・リストから、「**カスタム**」を選択します。
   b. <hwclock> タグの後ろにカーソルを置き、「timezone」をクリックしてタイム・ゾーン・マクロを追加します。
   c. <timezone> タグの後ろにカーソルを置き、「timezone」をクリックしてタイム・ゾーン・マクロを追加します。

   例:

```
<timezone>
  <hwclock>#timezone#</hwclock>
  <timezone>#timezone#</timezone>
</timezone>
```

4. オプションの SLES パッケージを指定するためのカスタム・マクロを追加します。
   a. 使用可能なカスタム・マクロのリスト内の 「server-settings」 → 「node」 リストを展開します。
   b. 空の <pattern> タグのいずれかにカーソルを置き、「fileserver」をクリックします。
   c. 空の <pattern> タグのいずれかにカーソルを置き、「lampserver」をクリックします。
   d. 空の <pattern> タグのいずれかにカーソルを置き、「mailserver」をクリックします。

   例:

```
<patterns config:type="list">
  <pattern>32bit</pattern>
  <pattern>Basis-Devel</pattern>
  <pattern>Minimal</pattern>
  <pattern>WBEM</pattern>
  <pattern>apparmor</pattern>
  <pattern>base</pattern>
  <pattern>documentation</pattern>
```

```
    <pattern>fips</pattern>
    <pattern>gateway_server</pattern>
    <pattern>ofed</pattern>
    <pattern>printing</pattern>
    <pattern>sap_server</pattern>
    <pattern>x11</pattern>
    <pattern>#server-settings.node.fileserver#</pattern>
    <pattern>#server-settings.node.lampserver#</pattern>
    <pattern>#server-settings.node.mailserver#</pattern>
  </patterns>
```

5. 「**保存**」をクリックしてファイルをグループ化し、変更を無人ファイルに保存します。

ステップ 5. カスタム構成設定ファイルおよび無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Basic`)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: `Custom SLES with optional packages`) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**関連付けられた無人ファイルと構成設定ファイル**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
7. 「**無人ファイル**」タブで、無人ファイルを選択し、(例: `SLES_installPackages_customUnattend.xml`) 「**次へ**」をクリックします。

   関連する構成設定ファイルが自動的に選択されます。
8. 「**インストール・スクリプト**」タブで、「**次へ**」をクリックします。
9. 「**要約**」タブで設定を確認します。
10. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 6. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_`Custom SLES with optional packages`) を選択します。

注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

d. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

注：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、管理対象サーバーから切り離します。

e. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン ( ) をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム構成設定ファイル (例: `SLES_installPackages_customConfig`) を選択します。

注：関連するカスタム無人ファイルが自動的に選択されます。

5. 「**サーバー固有設定**」サブタブで、ターゲット・サーバーおよびデプロイするオプション SLES パッケージを選択します。

6. 「**共通設定**」サブタブで、すべてのターゲット・サーバーに設定するタイム・ゾーンを選択します。

7. 「**要約**」タブで設定を確認します。
8. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム・ソフトウェアを伴う SLES 12 SP3 のデプロイ

このシナリオでは、カスタム・ソフトウェア (Java および Eclipse IDE) とともに、SLES 12 SP3 オペレーティング・システムをインストールします。カスタム・ソフトウェアのインストールと構成は、カスタム・ソフトウェアおよびポスト・インストール・スクリプトを含むカスタム・プロファイルが使用されます。カスタム・ソフトウェア・パッケージは、デプロイ中にホストにコピーされ、カスタム・ポスト・インストール・スクリプトで使用可能になります。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- jre-8u151-linux-x64.tar.gz。これは、Eclipse 対応 Java のインストール・ファイルです。
- eclipse-4.6.3-3.1.x86_64.tar.gz これは、Eclipse IDE のインストール・ファイルです。
- SLES_installSoftware_customScript.sh このポスト・インストール・スクリプトは、ユーザーを作成して Eclipse を起動し、Eclipse IDE および Java をインストールします。

注：

- SLES インストール・スクリプトは以下のいずれかの形式です。Bash (.sh)、Perl (.pm または .pl)、Python (.py)
- ソフトウェア・ファイルおよびインストール・スクリプトは、デプロイメント時に指定されたカスタム・データとファイル・パスからインストールされます。デフォルトのカスタム・データとファイルのパスは `/home/lxca` です。
- SLES 12 SP3 の場合は、Eclipse IDE に GCC コンパイラが必要です。これは事前定義済み基本プロファイルに含まれています。このシナリオでは、事前定義済みの基本プロファイルをベースとして使用して、カスタム OS イメージ・プロファイルを作成します。別のプロファイルを使用する場合は、GCC コンパイラがプロファイルに含まれていることを確認する必要があります。

手順

カスタム・ソフトウェアとともに SLES 12 SP3 をデプロイするには、以下の手順を実行します。

ステップ 1. SUSE Web サイトからローカル・システムに基本 SLES 12 SP3 オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする SLES 12 SP3 イメージを探して選択します (例: `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに、カスタム・ソフトウェアをダウンロードして、ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム・ソフトウェアのインポートを参照してください。

1. 「**ソフトウェア**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。

3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに SLES を選択します。
5. 「**参照**」をクリックし、インポートするソフトウェア・ファイルを検索して選択します (例: jre-8u151-linux-x64.tar.gz)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。
7. 「**インポート**」アイコン () をもう一度クリックします。
8. 「**ローカル・インポート**」をクリックします。
9. オペレーティング・システムに SLES を選択します。
10. 「**参照**」をクリックし、インポートするソフトウェア・ファイルを検索して選択します (例: eclipse-4.6.3-3.1.x86_64.tar.gz)。
11. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 3. カスタム・ポスト・インストール・スクリプトを作成して、OS イメージ・リポジトリーにファイルをインポートします。

Eclipse をこのファイルで起動するためのユーザーを作成するコマンドを追加します。例:

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "Passw0rd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

ソフトウェアをインストールするためのコマンドを追加します。例:

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

これらのコマンドは、XClarity Administrator がステータスをレポートするために使用する HTTPS URL (**predefined.otherSettings.statusSettings.urlStatus**)、最初のブート時にホスト OS から urlStatus Web サービスにアクセスするために必要な証明書を含むフォルダー (**predefined.otherSettings.statusSettings.certLocation**)、および展開したデータおよびソフトウェア・ファイルへのパス (**predefined.otherSettings.deployDataAndSoftwareLocation**) に、事前定義済みマクロを使用します。

また、サンプル・ファイルに示されているように、XClarity Administrator のジョブ・ログにカスタム・メッセージを送信するコマンドを追加することもできます。詳しくは、インストール・スクリプトに報告するカスタム・ステータスの追加を参照してください。

カスタム・インストール・スクリプトをインポートするには、以下の手順を実行します。詳しくは、カスタム・インストール・スクリプトのインポートを参照してください。

1. 「**インストール・スクリプト**」タブをクリックします。

2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに SLES を選択します。
5. 「**参照**」をクリックして、インポートするポスト・インストール・スクリプト (例: SLES_installSoftware_customScript.sh) を検索して選択します。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. カスタム・ソフトウェアおよびポスト・インストール・スクリプトを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: Basic)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: Custom SLES with software) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプとして「**なし**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、ソフトウェアのインストール・ファイルを選択します (例: jre-8u151-linux-x64.tar.gz や eclipse-4.6.3-3.1.x86_64.tar.gz) を選択して「**次へ**」をクリックします。
7. 「**インストール・スクリプト**」タブで、インストール・スクリプト (例: SLES_installSoftware_customScript.sh) を選択し、「**次へ**」をクリックします。
8. 「**要約**」タブで設定を確認します。
9. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 5. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 → 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 → 「**IP の割り当て**」 → 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom SLES with software) を選択します。

      注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

d. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

   注：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、管理対象サーバーから切り離します。

e. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**要約**」タブで設定を確認します。
5. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

構成可能なロケールと NTP サーバーを使用する SLES 12 SP3 のデプロイ

このシナリオでは、キーボードおよびオペレーティング・システムのロケールが英語、ブラジル語、日本語に対応した SLES 12 SP3 オペレーティング・システムをインストールします。また、最大 3 つの NTP サーバーの IP アドレスを構成します。ロケールと NTP サーバーの設定の選択には、無人ファイル (事前定義済みおよびカスタムのマクロを含む) および構成設定ファイルを含むカスタム OS イメージ・プロファイルが使用されます。このカスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。また、ロケールおよび NTP サーバー設定は「**カスタム設定**」タブで選択できます。指定された値は、カスタム無人ファイルに含まれるカスタム・マクロに置き換えられ、SLES autoyast インストーラー無人ファイルはこれらの値を使用してオペレーティング・システムを構成します。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- SLES_locale_customConfig.json。このカスタム構成ファイルは、SLES および NTP サーバーの OS ロケールおよびキーボードようにインストールする言語の入力を求めます。
- SLES_locale_customUnattend.xml。このカスタム無人ファイルは、構成ファイルで定義されているカスタム・マクロの値を使用します。

手順

カスタム OS イメージ・プロファイルを使用して SLES 12 SP3 をデプロイするには、以下の手順を実行します。

ステップ 1. SUSE Web サイトからローカル・システムに基本 SLES オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする SLES 12 SP3 イメージを探して選択します (例: `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。

ステップ 2. カスタム構成設定ファイルを作成して、OS イメージ・リポジトリーにファイルをインポートします。

構成設定ファイルは、OS デプロイメント・プロセス中に動的に収集する必要があるデータを記述する JSON ファイルです。このシナリオでは、オペレーティング・システムのロケール (en_US、ja_JP、pt_BR)、キーボードのロケール (米国英語、日本語、ブラジル・ポルトガル語)、および各 OS デプロイメントで使用する最大 3 つの NTP サーバーの IP アドレスを指定します。構成設定ファイルの作成について詳しくは、カスタム・マクロを参照してください。

構成設定ファイルをインポートするには、以下の手順を実行します。詳しくは、カスタム構成設定のインポートを参照してください。

1. 「**構成ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに SLES を選択します。
5. 「**参照**」をクリックし、インポートする構成設定ファイルを検索して選択します (例: SLES_locale_customConfig.json)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

   注：カスタム構成設定をファイルをインポートすると、XClarity Administrator によって、ファイル内の各設定についてカスタム・マクロが生成されます。これらのマクロは無人ファイルに追加できます。OS デプロイメント中、マクロは実際の値に置き換えられます。

ステップ 3. SLES 無人ファイルを変更して、オペレーティング・システムのロケール、キーボードのロケール、および NTP サーバーの IP アドレスの動的な値を指定してから、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム無人ファイルのインポートを参照してください。

<profile> タグの直後に、NTP サーバーおよびネットワーク情報を追加します。次の例には、2 つの NTP サーバーのタグが含まれています。IP アドレスは後の手順でマクロとして追加されます。

```
<ntp-client>
  <configure_dhcp config:type="boolean">false</configure_dhcp>
  <peers config:type="list">
    <peer>
      <address></address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address></address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
  <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

次の例に示すように、<general> セクションで、OS およびキーボード・ロケール情報を追加します。キーボードおよびオペレーティング・システムのロケール設定は後の手順でマクロとして追加されます。

```
<keyboard>
  <keymap></keymap>
</keyboard>
<language></language>
```

注：カスタム無人ファイルを使用すると、事前定義済み無人ファイルを使用した場合に得られる多くの正常な便宜機能が XClarity Administrator では提供されません。たとえば、<DiskConfiguration>、<ImageInstall>、<ProductKey> といったターゲット、管理者用 <UserAccounts>、ネットワーキング用 <Interfaces>、およびインストール機能の <package> リストが、アップロードするカスタム無人ファイルで指定されている必要があります。

カスタム無人ファイルをインポートするには、以下の手順を実行します。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに SLES を選択します。
5. 「**参照**」をクリックし、インポートする無人ファイルを検索して選択します (例: SLES_locale_customUnattend.xml)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. カスタム無人ファイルをカスタム構成設定ファイルに関連付け、構成設定ファイルから無人ファイルに必要な事前定義済みマクロおよびカスタム・マクロ (設定) を追加します。詳しくは、無人ファイルを構成設定ファイルに関連付けるおよび事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

ヒント: 必要に応じて、カスタム構成設定ファイルを使用して無人ファイルをカスタマイズし、無人ファイルのインポート時にマクロを追加できます。

1. 「**無人ファイル**」タブで、カスタム・アテンド・ファイル (例: SLES_locale_customUnattend.xml) を選択します。
2. 「**構成ファイルの関連付け**」アイコン () をクリックして、「無人ファイルの関連付け」ダイアログを表示します。
3. 無人ファイルに関連付ける構成設定ファイルを選択します (例: SLES_locale_customConfig)。
4. 必要な事前定義済みマクロを無人ファイルに追加します。
   a. 「**使用できるマクロ**」ドロップダウン・リストから、「**事前定義済み**」を選択します。
   b. 無人ファイルの行 1 の後ろ (<xml> タグの後ろ) の任意の場所にカーソルを置きます。
   c. 使用可能な事前定義済みマクロのリスト内の「predefined」 ➞ 「unattendSettings」リストを展開します。
   d. 「preinstallConfig」および「postinstallConfig」マクロをクリックして、マクロを追加します。

   例:

   ```
   <?xml version="1.0"?>
   <!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
     #predefined.unattendSettings.preinstallConfig#
     #predefined.unattendSettings.postinstallConfig#
   <profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
   ```
5. オペレーティング・システムのロケールを指定するためのカスタム・マクロを追加します。
   a. 「**使用できるマクロ**」ドロップダウン・リストから、「**カスタム**」を選択します。
   b. <language> タグの後ろにカーソルを置きます。

c. 使用できるカスタム・マクロのリストで「**server-settings**」 ➞ 「**node**」 を展開し、「**locale**」をクリックして OS ロケール・マクロを追加します。

例:

```
<language>#server-settings.node.locale#</language>
```

6. キーボードのロケールを指定するためのカスタム・マクロを追加します。
   a. **<keymap>** タグの後ろにカーソルを置きます。
   b. 使用できるカスタム・マクロのリストで「**server-settings**」 ➞ 「**node**」 を展開し、「**keyboardLocale**」をクリックしてキーボード・ロケール・マクロを追加します。

   例:

```
<keyboard>
  <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. NTP サーバーの IP アドレスを指定するためのカスタム・マクロを追加します。

   このシナリオでは、カスタム構成設定のファイルはテンプレートを使用して、3 つの NTP サーバーに 0 を指定します。構成設定ファイルでテンプレートを使用すると、テンプレートに関連付けられているマクロは「無人ファイルの関連付け」ダイアログに表示されません。代わりに、手動で無人ファイルを編集してマクロおよび適切なタグを追加する必要があります。

   たとえば、3 つの NTP サーバーを含めるには、以下のタグおよびマクロを無人ファイルに追加します。このシナリオの無人ファイルの例では、これらのタグおよびマクロが既に存在します。

```
<ntp-client>
  <configure_dhcp config:type="boolean">false</configure_dhcp>
  <peers config:type="list">
    <peer>
      <address>#server-settings.ntpserver1#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver2#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
    <peer>
      <address>#server-settings.ntpserver3#</address>
      <initial_sync config:type="boolean">true</initial_sync>
      <options></options>
      <type>server</type>
    </peer>
  </peers>
  <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. 「**関連付ける**」をクリックしてファイルをグループ化し、変更を無人ファイルに保存します。

ステップ 5. カスタム構成設定ファイルおよび無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Basic`)。

3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前を入力します (例: `Custom SLES for OS and keyboard locale and NTP server`)。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**関連付けられた無人ファイルと構成設定ファイル**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
7. 「**無人ファイル**」タブで、カスタム無人ファイルを選択し、(例: `SLES_locale_customUnattend.xml`) 「**次へ**」をクリックします。

   関連する構成設定ファイルが自動的に選択されます。
8. 「**インストール・スクリプト**」タブで、「**次へ**」をクリックします。
9. 「**要約**」タブで設定を確認します。
10. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 6. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 → 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 → 「**IP の割り当て**」 → 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_`Custom SLES for OS と keyboard locale および NTP server`) を選択します。

      注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。
   d. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

      注：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、管理対象サーバーから切り離します。
   e. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。
3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム構成設定ファイル (例: `SLES_locale_customConfig`) を選択します。

注：関連するカスタム無人ファイルが自動的に選択されます。

5. 「**サーバー固有設定**」サブタブで、ターゲット・サーバー、OS のロケール、キーボードのロケールを選択します。
6. 「**共通設定**」サブタブで、「**追加**」をクリックして最大 3 個の NTP サーバーの IP アドレスを指定します。
7. 「**要約**」タブで設定を確認します。
8. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

静的 IP アドレスを使用したローカル・ディスクへの Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ

このシナリオでは、Lenovo Customization オペレーティング・システム対応 VMware ESXi v6.7 を、ホスト・サーバーの静的 IP アドレスを使用してローカル・ディスクにインストールします。無人ファイル (事前定義済みマクロ含む) を含むカスタム OS イメージ・プロファイルが使用されます。このカスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。既知の値は、カスタム無人ファイルに含まれる事前定義済みマクロに置き換えられ、VMware ESXi kickstart インストーラーは無人ファイルのこれらの値を使用してオペレーティング・システムを構成します。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- ESXi_staticIP_customUnattend.cfg。このカスタム無人ファイルは、事前定義済みマクロの値を使用します。

手順

カスタム OS イメージ・プロファイルを使用して VMware ESXi v6.7 をデプロイするには、以下の手順を実行します。

ステップ 1. VMware サポート - ダウンロード Web サイト Web サイトからローカル・システムに Lenovo Customization オペレーティング・システム対応 VMware vSphere® Hypervisor (ESXi) をダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする ESXi イメージを探して選択します (例: `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。

ステップ 2. ESXi 無人 (kickstart) ファイルを変更して、必要なマクロおよび必要に応じてその他の事前定義済みマクロ (IP アドレス、ゲートウェイ、DNS およびホスト名設定など) を追加し、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム無人ファイルのインポートを参照してください。

ESXi および RHEL 専用に、XClarity Administrator に **#predefined.unattendSettings.networkConfig#** マクロが用意されています。これは UI で定義されているすべてのネットワーク設定を無人ファイルに追加します。この例では、UI で定義されていない設定 (**--addvmportgroup**) を指定するため、サンプルの無人ファイルの **#predefinedunattendSettings.storageConfig#** マクロは使用しません。代わりに、ネットワーク設定は個別にファイルに追加され、**#predefined.hostPlatforms.networkSettings.*<setting>*#** マクロが使用されます。

ESXi および RHEL 専用に、XClarity Administrator に **#predefined.unattendSettings.storageConfig#** マクロも用意されています。これは UI で定義されているすべてのストレージ設定を無人ファイルに追加します。この例では、UI で定義されていない設定 (**--novmfsondisk** および **–ignoressd**) を指定するため、サンプルの無人ファイルの **#predefinedunattendSettings.storageConfig#** マクロは使用しません。代わりに、ストレージの設定は個別に追加され **--firstdisk=local** がファイルにハードコーディングされます。

注：XClarity Administrator は、OOB ドライバー挿入、ステータスのレポート、ポスト・インストール・スクリプト、カスタム・ソフトウェアなど、一部の基本的な便宜マクロを提供します。ただし、これらの事前定義マクロを利用するには、次のマクロをカスタム無人ファイルで指定する必要があります。ファイルの例には、必要なマクロが既に含まれています。%firstboot セクションが含まれるため、これらの事前定義済みマクロの順序付けに注意してください。詳しくは、カスタム無人ファイルのインポートを参照してください。
`#predefined.unattendSettings.preinstallConfig#`
`#predefined.unattendSettings.postinstallConfig#`
サンプルのファイルには、必須マクロおよびターゲット・サーバーのネットワーク設定を動的に指定する追加の事前定義済みマクロが既に含まれています。マクロの無人ファイルへの追加について詳しくは、事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

使用可能な事前定義済みマクロについて詳しくは、事前定義済みマクロを参照してください。

カスタム無人ファイルをインポートするには、以下の手順を実行します。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに `ESXi` を選択します。

5. 「**参照**」をクリックし、インポートする無人ファイルを検索して選択します (例: `ESXi_staticIP_customUnattend.cfg`)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 3. カスタム無人を含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Virtualization`)。
3. 「**作成**」アイコン ( ) をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: `Custom ESXi using static IP`) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**無人ファイルのみ**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**無人ファイル**」タブで、無人ファイルを選択し、(例: `ESXi_staticIP_customUnattend.cfg`) 「**次へ**」をクリックします。
6. 「**要約**」タブで設定を確認します。
7. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 4. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント:

      - VLAN 設定は、VLAN モードが 「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」 で設定されている場合のみ使用できます。
      - 「ネットワーク設定」ダイアログで指定したネットワーク設定が、無人ファイルの実行時に #predefined.hostPlatforms.networkSettings.*<setting>*# マクロを使用して無人ファイルに追加されます。

   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_`Custom ESXi using static IP`) を選択します。

      注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

   d. (オプション) 「**ライセンス・キー**」アイコン ( ) をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。
   e. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

注：--**firstdisk=local** が無人ファイルで指定されているため、「**ストレージ**」列で優先する格納場所を指定する必要はありません。UI の設定は無視されます。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン ( ) をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム無人ファイル (例: `ESXi_staticIP_customUnattend.cfg`) を選択します。

5. 「**要約**」タブで設定を確認します。
6. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

構成可能なロケールとセカンド・ユーザー資格情報を使用する Lenovo Customization 対応 VMware ESXi v6.7 のデプロイ

このシナリオでは、キーボードの言語が構成可能でセカンド ESXi ユーザーの資格情報を使用する Lenovo Customization オペレーティング・システム対応 VMware ESXi v6.7 をインストールします。この例では、UI で定義されているネットワークおよびストレージの基本的な設定を使用します。パスワードの選択には、無人ファイル (事前定義済みおよびカスタムのマクロを含む) および構成設定ファイルを含むカスタム OS イメージ・プロファイルが使用されます。このカスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。次に、「**カスタム設定**」タブでパスワードを指定できます。指定された値は、カスタム無人ファイルのカスタム・マクロに置き換えられ、ESXi インストーラーは無人ファイルのこれらの値を使用してオペレーティング・システムを構成します。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- ESXi_locale_customConfig.json。このカスタム構成ファイルはキーボードのロケールとセカンド ESXi ユーザーの資格情報の入力を求めます。
- ESXi_locale_customUnattend.cfg。このカスタム無人ファイルは、構成ファイルで定義されている事前定義済みマクロおよびカスタム・マクロの値を使用します。

手順

カスタム OS イメージ・プロファイルを使用して VMware ESXi v6.7 をデプロイするには、以下の手順を実行します。

ステップ 1. VMware サポート - ダウンロード Web サイト Web サイトからローカル・システムに Lenovo Customization オペレーティング・システム対応 VMware vSphere® Hypervisor (ESXi) をダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックし、インポートする ESXi イメージを探して選択します (例: `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`)。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。

ステップ 2. カスタム構成設定ファイルを作成して、OS イメージ・リポジトリーにファイルをインポートします。

構成設定ファイルは、OS デプロイメント・プロセス中に動的に収集する必要があるデータを記述する JSON ファイルです。このシナリオでは、セカンド ESXi ユーザーが各 OS デプロイメントで使用するキーボードのロケールとユーザー ID およびパスワードを選択します。構成設定ファイルの作成について詳しくは、カスタム・マクロを参照してください。

構成設定ファイルをインポートするには、以下の手順を実行します。詳しくは、カスタム構成設定のインポートを参照してください。

1. 「**構成ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに `ESXi` を選択します。
5. 「**参照**」をクリックし、インポートする構成設定ファイルを検索して選択します (例: `ESXi_locale_customConfig.json`)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

   注：カスタム構成設定をファイルをインポートすると、XClarity Administrator によって、ファイル内の各設定についてカスタム・マクロが生成されます。これらのマクロは無人ファイルに追加できます。OS デプロイメント中、マクロは実際の値に置き換えられます。

ステップ 3. ESXi 無人 (kickstart) ファイルを変更して、オペレーティング・システムのロケールおよびキーボードのロケール、セカンド ESXi ユーザーのユーザー資格情報を指定してから、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム無人ファイルのインポートを参照してください。

キーボード・ロケールを設定するコマンドを追加します。例:

```
# Set the keyboard locale
keyboard ''
```

セカンド ESXi ユーザーを作成するコマンドを追加します。次の例では、*<user_id>* および *<password>* は、次のステップのカスタム・マクロで置き換えられます。

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
```

```
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

カスタム無人ファイルをインポートするには、以下の手順を実行します。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに ESXi を選択します。
5. 「**参照**」をクリックし、インポートする無人ファイルを検索して選択します (例: ESXi_locale_customUnattend.cfg)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. カスタム無人ファイルをカスタム構成設定ファイルに関連付け、構成設定ファイルから無人ファイルに必要な事前定義済みマクロおよびカスタム・マクロ (設定) を追加します。詳しくは、無人ファイルを構成設定ファイルに関連付けるおよび事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

ヒント:

- 必要に応じて、カスタム構成設定ファイルにカスタム無人ファイルを関連付けて、無人ファイルのインポート時にマクロを追加できます。
- XClarity Administrator は、OOB ドライバー挿入、ステータスのレポート、ポスト・インストール・スクリプト、カスタム・ソフトウェアなど、一部の基本的な便宜マクロを提供します。ただし、これらの事前定義マクロを利用するには、次のマクロをカスタム無人ファイルで指定する必要があります。ファイルの例には、必要なマクロが既に含まれています。%firstboot セクションが含まれるため、これらの事前定義済みマクロの順序付けに注意してください。詳しくは、カスタム無人ファイルのインポートを参照してください。
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator では、UI で定義されているすべてのネットワークおよびストレージ・ロケーションの設定を挿入するマクロも提供されています。これらのマクロは、デプロイメントで基本的な設定のみが必要な場合に便利です。ファイルの例には、必要なマクロが既に含まれています。
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

マクロの無人ファイルへの追加について詳しくは、事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。使用可能な事前定義済みマクロについて詳しくは、事前定義済みマクロを参照してください。

カスタム無人ファイルをカスタム構成設定ファイルに関連付けるには、次の手順を実行します。

1. 「**無人ファイル**」タブで、カスタム・アテンド・ファイル (例: ESXi_locale_customUnattend.cfg) を選択します。
2. 「**構成ファイルの関連付け**」アイコン () をクリックして、「無人ファイルの関連付け」ダイアログを表示します。
3. 無人ファイルに関連付ける構成設定ファイルを選択します (例: ESXi_locale_customConfig)。
4. 「**使用できるマクロ**」ドロップダウン・リストから、「**カスタム**」を選択します。
5. キーボードの後ろの一重引用符の間にカーソルを置いて「**keyboard_locale**」をクリックし、キーボードのロケールを指定するカスタム・マクロを追加します。

例:

```
# Set the keyboard locale
keyboard '#keyboard_locale#'
```

6. ユーザー ID を追加するそれぞれの場所にカーソルを置いて「**second_user_id**」をクリックし、セカンド・ユーザーの ID を指定するカスタム・マクロを追加します。例のファイルでは、それぞれの *<user_id>* がカスタム・マクロで置き換えられます。

   例:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. パスワードを追加する場所にカーソルを置いて「**second_user_password**」をクリックし、セカンド・ユーザーのパスワードを指定するカスタム・マクロを追加します。例のファイルでは、*<password>* がカスタム・マクロで置き換えられます。

   例:

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. 「**関連付ける**」をクリックしてファイルをグループ化し、変更を無人ファイルに保存します。

ステップ 5. カスタム構成設定ファイルおよび無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Virtualization`)。
3. 「**作成**」アイコン ( ) をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前を入力します (例: `Custom ESXi using custom locale and second user credentials`)。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**関連付けられた無人ファイルと構成設定ファイル**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**無人ファイル**」タブで、無人ファイルを選択し、(例: `ESXi_locale_customUnattend.cfg`) 「**次へ**」をクリックします。

   関連する構成設定ファイルが自動的に選択されます。
6. 「**要約**」タブで設定を確認します。
7. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 6. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。

a. サーバーを選択します。
b. 「**選択の変更**」 ➙ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

   ヒント:

   - VLAN 設定は、VLAN モードが 「**共通設定**」 ➙ 「**IP の割り当て**」 ➙ 「**VLAN を使用する**」 で設定されている場合のみ使用できます。
   - 「ネットワーク設定」ダイアログで指定したネットワーク設定が、無人ファイルの実行時に #predefined.hostPlatforms.networkConfig#マクロを使用して無人ファイルに追加されます。

c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom ESXi using custom locale and second user credentials) を選択します。

   注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。

d. (オプション) 「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。
e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

   注：

   - 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、管理対象サーバーから切り離します。
   - 「ストレージ設定」ダイアログで指定したストレージ設定が、無人ファイルの実行時に #predefined.hostPlatforms.storageConfig#マクロを使用して無人ファイルに追加されます。

f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム構成設定ファイル (例: ESXi_locale_customConfig) を選択します。

   注：関連するカスタム無人ファイルが自動的に選択されます。

5. 「**サーバー固有設定**」サブタブで、キーボードのロケールおよびセカンド ESXi ユーザーの資格情報を選択します。
6. 「**要約**」タブで設定を確認します。
7. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム機能を伴う Windows 2016 のデプロイ

このシナリオでは、Windows 2016 オペレーティング・システムと、複数の追加機能をインストールします。カスタム無人ファイルを含むカスタム・プロファイルが使用されます。カスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- Windows_installFeatures_customUnattend.xml。このカスタム無人ファイルは、WindowsMediaPlayer および BitLocker 機能をインストールし、動的な値に使用定義済みマクロを使用します。

手順

カスタム・機能とともに Windows 2016 をデプロイするには、以下の手順を実行します。

ステップ 1. ローカル・システムに日本語版 Windows 2016 オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン ( ) をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `ja_windows_server_2016_x64_dvd_9720230.iso`) を見つけて選択します。

6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに Windows 2016 のバンドル・ファイルをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、デバイス・ドライバーのインポートを参照してください。

バンドル・ファイルには最新のデバイス・ドライバーおよび WinPE ブート・ファイルが含まれており、カスタム OS イメージ・プロファイルに追加できます。このシナリオではカスタム・ブート・ファイルを使用するため、バンドル内のブート・ファイルは使用しません。

1. 「**ドライバー・ファイル**」タブをクリックします。
2. 「**ダウンロード**」 ➡ 「**Windows バンドル・ファイル**」をクリックして Lenovo サポート Web ページに移動し、Windows 2016 のバンドル・ファイルをローカル・システムにダウンロードします。
3. 「**インポート**」アイコン ( ) をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `bundle_win2016_20180126130051.zip`) を見つけて選択します。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 3. Windows 無人ファイルを変更して追加機能 (WindowsMediaPlayer や BitLocker など) をインストールし、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。

Windows 無人ファイルの「servicing」セクションに、インストールする Windows 機能を追加します。例:

```
<servicing>
  <package action="configure">
    <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
              processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
              language=""></assemblyIdentity>
    <selection name="Microsoft-Hyper-V" state="true"></selection>
    <selection name="MultipathIo" state="true"></selection>
    <selection name="FailoverCluster-PowerShell" state="true"></selection>
    <selection name="FailoverCluster-FullServer" state="true"></selection>
    <selection name="FailoverCluster-CmdInterface" state="true"></selection>
    <selection name="FailoverCluster-AutomationServer" state="true"></selection>
    <selection name="FailoverCluster-AdminPak" state="true"></selection>
    <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
    <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
    <selection name="ServerManager-Core-RSAT" state="true"></selection>
    <selection name="WindowsMediaPlayer" state="true"></selection>
    <selection name="BitLocker" state="true"></selection>
  </package>
</servicing>
```

注：

- これらのタグはサンプル無人ファイルにあります。
- カスタム無人ファイルを使用すると、事前定義済み無人ファイルを使用した場合に得られる多くの正常な便宜機能が XClarity Administrator では提供されません。たとえば、`<DiskConfiguration>`、`<ImageInstall>`、`<ProductKey>` といったターゲット、管理者用

<UserAccounts>、ネットワーキング用 <Interfaces>、およびインストール機能の <package> リストが、アップロードするカスタム無人ファイルで指定されている必要があります。

カスタム無人ファイルをインポートするには、以下の手順を実行します。詳しくは、カスタム無人ファイルのインポートを参照してください。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに Windows を選択します。
5. 「**参照**」をクリックし、カスタム無人ファイルを検索して選択します (例: Windows_installFeatures_customUnattend.xml)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

XClarity Administrator は、OOB ドライバー挿入、ステータスのレポート、ポスト・インストール・スクリプト、カスタム・ソフトウェアなど、一部の基本的な便宜マクロを提供します。ただし、これらの事前定義マクロを利用するには、次のマクロをカスタム無人ファイルで指定する必要があります。

- #predefined.unattendSettings.preinstallConfig#
- #predefined.unattendSettings.postinstallConfig#

サンプルのファイルには、既に追加機能をインストールするコード、必須マクロ、および動的入力のために必要なその他のマクロが既に含まれています。マクロの無人ファイルへの追加について詳しくは、事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。

使用可能な事前定義済みマクロについて詳しくは、事前定義済みマクロを参照してください。

ステップ 4. 無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズするプロファイルを選択します (例: win2016-x86_64-install-Datacenter_Virtualization)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: Custom Windows with features) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**無人ファイルのみ**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ブート・オプション**」タブで、「**次へ**」をクリックします。デフォルトでは、事前定義済み WinPE ブート・ファイルが選択されます。
7. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
8. 「**無人ファイル**」タブで、カスタム無人ファイルを選択し、(例: Windows_installFeatures_customUnattend.xml) 「**次へ**」をクリックします。
9. 「**インストール・スクリプト**」タブで、「**次へ**」をクリックします。
10. 「**要約**」タブで設定を確認します。

11. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 5. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、サブネット・マスク、ゲートウェイ、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom Windows with features) を選択します。

      注: すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。
   d. (オプション)「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。
   e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

      注: 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、管理対象サーバーから切り離します。
   f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。
3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム無人ファイル (例: `Windows_installFeatures_customUnattend.xml`) を選択します。
5. (オプション)「**Active Directory ドメイン**」タブで、Active Directory ドメインを Windows イメージ・デプロイメントの一部として結合するための情報を指定します (Windows Active Directory との統合を参照)。
6. 「**要約**」タブで設定を確認します。
7. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

カスタム・ソフトウェアを伴う Windows 2016 のデプロイ

このシナリオでは、カスタム・ソフトウェア (Java および Eclipse IDE) とともに、Windows 2016 オペレーティング・システムをインストールします。カスタム・ソフトウェアのインストールと構成は、カスタム・ソフトウェアおよびポスト・インストール・スクリプトを含むカスタム・プロファイルが使用されます。カスタム・ソフトウェア・パッケージは、デプロイ中にホストにコピーされ、カスタム・ポスト・インストール・スクリプトで使用可能になります。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- jre-8u151-windows-x64-with-configfile.zip。これは、Eclipse 対応 Java のインストール・ファイルです。
- eclipse-java-oxygen-1a-win32-x86_64.zip これは Eclipse IDE のインストール・ファイルです。
- Windows_installSoftware_customScript.ps1 このポスト・インストール・スクリプトは、ユーザーを作成して、Eclipse を起動し、Eclipse IDE および Java をインストールします。

注：

- Windows インストール・スクリプトは以下のいずれかの形式です。コマンド・ファイル (.cmd)、PowerShell (.ps1)
- ソフトウェア・ファイルおよびインストール・スクリプトは、デプロイメント時に指定されたカスタム・データとファイル・パスからインストールされます。デフォルトのカスタム・データとファイルのパスは `C:\lxca` です。

手順

カスタム・ソフトウェアとともに Windows 2016 をデプロイするには、以下の手順を実行します。

ステップ 1. ローカル・システムに日本語版 Windows 2016 オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `ja_windows_server_2016_x64_dvd_9720230.iso`) を見つけて選択します。
6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに Windows 2016 のバンドル・ファイルをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、デバイス・ドライバーのインポートを参照してください。

バンドル・ファイルには最新のデバイス・ドライバーおよび WinPE ブート・ファイルが含まれており、カスタム OS イメージ・プロファイルに追加できます。このシナリオではカスタム・ブート・ファイルを使用するため、バンドル内のブート・ファイルは使用しません。

1. 「**ドライバー・ファイル**」タブをクリックします。
2. 「**ダウンロード**」 → 「**Windows バンドル・ファイル**」をクリックして Lenovo サポート Web ページに移動し、Windows 2016 のバンドル・ファイルをローカル・システムにダウンロードします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `bundle_win2016_20180126130051.zip`) を見つけて選択します。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 3. ローカル・システムに、カスタム・ソフトウェアをダウンロードして、ファイルを OS イメージ・リポジトリーにインポートします。詳しくは、カスタム・ソフトウェアのインポートを参照してください。

1. 「**ソフトウェア**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに Windows を選択します。
5. 「**参照**」をクリックし、インポートする構成設定ファイルを検索して選択します (例: jre-8u151-windows-x64-with-configfile.zip)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。
7. 「**インポート**」アイコン () をもう一度クリックします。
8. 「**ローカル・インポート**」をクリックします。
9. オペレーティング・システムに Windows を選択します。
10. 「**参照**」をクリックし、インポートする構成設定ファイルを検索して選択します (例: eclipse-java-oxygen-1a-win32-x86_64.zip)。
11. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. カスタム・ポスト・インストール・スクリプトを作成して、OS イメージ・リポジトリーにファイルをインポートします。

ソフトウェアをインストールするためのコマンドを追加します。例:

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
    {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
    [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
    /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
    "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
    -DestinationPath $eclipseDir
```

これらのコマンドは、抽出されたデータおよびソフトウェア・ファイルへのパスに事前定義済みマクロを使用することに注意してください (predefined.otherSettings.deployDataAndSoftwareLocation)。

また、サンプル・ファイルに示されているように、XClarity Administrator のジョブ・ログにカスタム・メッセージを送信するコマンドを追加することもできます。詳しくは、インストール・スクリプトに報告するカスタム・ステータスの追加を参照してください。

カスタム・インストール・スクリプトをインポートするには、以下の手順を実行します。詳しくは、カスタム・インストール・スクリプトのインポートを参照してください。

1. 「**インストール・スクリプト**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに Windows を選択します。

5. 「**参照**」をクリックし、インポートする無人ファイルを検索して選択します (例: `Windows_installSoftware_customScript.ps1`)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 5. カスタム無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズする OS イメージ・プロファイルを選択します (例: `Datacenter virtualization`)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: `Custom Windows with software`) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプとして「**なし**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ブート・オプション**」タブで、「**次へ**」をクリックします。デフォルトでは、事前定義済み WinPE ブート・ファイルが選択されます。
7. 「**ソフトウェア**」タブで、ソフトウェアのインストール・ファイル (例: `jre-8u151-windows-x64-with-configfile.zip` や `eclipse-java-oxygen-1a-win32-x86_64.zip`) を選択し、「**次へ**」をクリックします。
8. 「**インストール・スクリプト**」タブで、インストール・スクリプト (例: `Windows_installSoftware_customScript.ps1`) を選択し、「**次へ**」をクリックします。
9. 「**要約**」タブで設定を確認します。
10. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 6. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 ➡ 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 ➡ 「**IP の割り当て**」 ➡ 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom Windows with software) を選択します。

      注: すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。
   d. (オプション) 「**ライセンス・キー**」アイコン () をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。

e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

注：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、管理対象サーバーから切り離します。

f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン () をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**要約**」タブで設定を確認します。
5. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

日本語の Windows 2016 のデプロイ

このシナリオでは、キーボードおよびオペレーティング・システムのロケールが日本語に対応した Windows 2016 オペレーティング・システムを複数のサーバーにインストールします。カスタム WinPE ブート・ファイルおよび無人ファイルを含むカスタム・プロファイルが使用されます。カスタム・プロファイルは「OS イメージのデプロイ」ページで選択できます。

始める前に

このシナリオでは、以下のサンプル・ファイルを使用します。

- `WinPE_64_ja.zip`.このカスタム Windows ブート (WinPE) ファイルは、日本語のロケールをインストールします。
- Windows_locale_customUnattend.xml.このカスタム無人ファイルは、WinPE ファイルを使用して日本語をインストールします。

注：サンプルのカスタム無人ファイルは以下を前提とします。

- サーバーには見えるディスクは 1 つのみ (ディスク 0) であり、そこにはシステム・パーティションはまだありません。
- 静的 IPv4 モードが使用され、静的 IP を設定します (カスタム無人ファイルで事前定義済みマクロとして使用されます)。

手順

カスタム OS イメージ・プロファイルを使用して日本語版 Windows 2016 をターゲット・サーバーにデプロイするには、以下の手順を実行します。

ステップ 1. ローカル・システムに日本語版 Windows 2016 オペレーティング・システムをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、オペレーティング・システム・イメージのインポートを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➔ 「**OS イメージの管理**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージの管理」ページを表示します。
2. 「**OS イメージ**」タブをクリックします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `ja_windows_server_2016_x64_dvd_9720230.iso`) を見つけて選択します。

6. 「**インポート**」をクリックして、イメージを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 2. ローカル・システムに Windows 2016 のバンドル・ファイルをダウンロードして、OS イメージ・リポジトリーにイメージをインポートします。詳しくは、デバイス・ドライバーのインポートを参照してください。

バンドル・ファイルには最新のデバイス・ドライバーおよび WinPE ブート・ファイルが含まれており、カスタム OS イメージ・プロファイルに追加できます。このシナリオではカスタム・ブート・ファイルを使用するため、バンドル内のブート・ファイルは使用しません。

1. 「**ドライバー・ファイル**」タブをクリックします。
2. 「**ダウンロード**」 ➡ 「**Windows バンドル・ファイル**」をクリックして Lenovo サポート Web ページに移動し、Windows 2016 のバンドル・ファイルをローカル・システムにダウンロードします。
3. 「**インポート**」アイコン () をクリックします。
4. 「**ローカル・インポート**」をクリックします。
5. 「**参照**」をクリックして、インポートする OS イメージ (例: `bundle_win2016_20180126130051.zip`) を見つけて選択します。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。
7. インポートが完了するのを待ちます。しばらく時間がかかる場合があります。

ステップ 3. WinPE のインストール中に日本語ロケールを使用するカスタム WinPE ブート・ファイルを作成し、ファイルを OS イメージ・リポジトリーにインポートします。

XClarity Administrator は事前定義済みプレインストール (WinPE) ブート・ファイルを使用して Windows オペレーティング・システムをインストールします。この事前定義済みブート・ファイルで使用されているロケールは、英語 (en-US) です。Windows のセットアップ中に使用するロケールを変更する場合は、目的のロケールを使用してカスタム WinPE ブート・ファイルを作成して、カスタム・プロファイルにそのカスタム・ブート・ファイルを割り当てます。

WinPE にロケールを挿入する方法については、Windows WinPE: パッケージの追加 Web ページを参照してください。

重要：WinPE ブート・ファイルで英語以外のロケールを指定しても、デプロイされる最終的な OS のロケールは変更されません。Windows のインストールとセットアップ中に表示されるロケールのみ変更されます。

日本語のロケールが含まれているカスタム WinPE ブート・ファイルを作成するには、以下の手順を実行します。詳しくは、ブート (WinPE) ファイルの作成を参照してください。

1. 管理者権限を持つ ID を使用して、Windows ADK コマンド「Deployment and Imaging Tools Environment」を実行します。コマンド・セッションが表示されます。
2. コマンド・セッションから、`genimage.cmd` ファイルと `starnet.cmd` ファイルがダウンロードされたディレクトリー (`C:\customwim` など) に移動します。
3. 次のコマンドを実行して、以前にマウントされたイメージがホストにないことを確認します。
   ```
   dism /get-mountedwiminfo
   ```
   マウントされたイメージがある場合、以下のコマンドを実行して廃棄します。
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```

4. インボックス・デバイス・ドライバーをカスタマイズされた Windows プロファイルに追加する場合、ロー・デバイス・ドライバー・ファイル (.inf format 形式) を `C:\drivers` ディレクトリー内のホスト・システムにコピーします。
5. 次のコマンドを実行してブート・ファイル (.wim 形式) を生成し、コマンドが完了するまで数分間待ちます。
   ```
   genimage.cmd amd64 <ADK_Version>
   ```
   ここの *<ADK_Version>* は以下のいずれかの値です。
   - **8.1**.Windows 2012 R2 の場合
   - **10**.Windows 2016 の場合

   このコマンドにより、ブート・ファイル `C:\WinPE_64\media\Boot\WinPE_64.wim` が作成されます。
6. 次のコマンドを実行してブート・ファイルをマウントします。
   ```
   DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
   ```
7. アウト・オブ・ボックス・デバイス・ドライバーをブート・ファイルに追加する場合、次の手順を実行します。
   a. 次のディレクトリー構造を作成します。*<os_release>* は、`2012R2` または `2016` です。
      ```
      drivers\<os_release>\
      ```
   b. デバイス・ドライバー (.inf 形式) をパス内のディレクトリーにコピーします。たとえば、次のとおりです。
      ```
      drivers\<os_release>\<driver1>\<driver1_files>
      ```
   c. `drivers` ディレクトリーをマウント・ディレクトリーにコピーします。たとえば、次のとおりです。
      ```
      C:\WinPE_64\mount\drivers
      ```
8. **オプション**: フォルダー、ファイル、起動スクリプト、言語パック、アプリの追加など、ブート・オプション・ファイルに追加のカスタマイズを行います。ブート・ファイルのカスタマイズについて詳しくは、WinPE: マウントとカスタマイズの Web サイトを参照してください。
9. たとえば、日本語のパッケージを追加します。
10. インストールされたパッケージを表示して、日本語専用パッケージがインストールされていることを確認します。
    ```
    Dism /Add-Package /Image:"C:\WinPE_64\mount"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
    and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
    /PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
    Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
    ```
11. イメージの国際設定を確認します。
    ```
    Dism /Get-Packages /Image:"C:\WinPE_64\mount"
    ```

12. 次のコマンドを実行してイメージをアンマウトします。
    `DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit`
13. `C:\WinPE_64\media` ディレクトリーの内容を `WinPE_64_ja.zip` という zip ファイルに圧縮します。
14. .zip ファイルを XClarity Administrator にインポートします (ブート・ファイルのインポートを参照)。
    a. 「**ブート・ファイル**」タブをクリックします。
    b. 「**インポート**」アイコン () をクリックします。
    c. 「**ローカル・インポート**」をクリックします。
    d. オペレーティング・システムに `Windows` を選択します。
    e. 「**参照**」をクリックし、カスタム・ブート・ファイルを検索して選択します (例: `WinPE_64_ja.zip`)。
    f. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 4. Windows 無人ファイルを変更して日本語を OS イメージに含めるように指定し、カスタム・ファイルを OS イメージ・リポジトリーにインポートします。

Windows インストールの「windowsPE」パスに、オペレーティング・システム言語およびロケールとして日本語を追加します。例:

```
<settings pass="windowsPE">
  <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
        publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
        xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <SetupUILanguage>
      <UILanguage>ja-JP</UILanguage>
    </SetupUILanguage>
    <SystemLocale>ja-JP</SystemLocale>
    <UILanguage>ja-JP</UILanguage>
    <UserLocale>ja-JP</UserLocale>
    <InputLocale>0411:00000411</InputLocale>
  </component>
</settings>
```

注：カスタム無人ファイルを使用すると、事前定義済み無人ファイルを使用した場合に得られる多くの正常な便宜機能が XClarity Administrator では提供されません。たとえば、`<DiskConfiguration>`、`<ImageInstall>`、`<ProductKey>` といったターゲット、管理者用 `<UserAccounts>`、ネットワーキング用 `<Interfaces>`、およびインストール機能の `<package>` リストが、アップロードするカスタム無人ファイルで指定されている必要があります。

XClarity Administrator は、OOB ドライバー挿入、ステータスのレポート、ポスト・インストール・スクリプト、カスタム・ソフトウェアなど、一部の基本的な便宜マクロを提供します。ただし、これらの事前定義マクロを利用するには、次のマクロをカスタム無人ファイルで指定する必要があります。

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

ファイルの例には、必要なマクロが既に含まれています。マクロの無人ファイルへの追加について詳しくは、事前定義済みマクロおよびカスタム・マクロの無人ファイルへの挿入を参照してください。使用可能な事前定義済みマクロについて詳しくは、事前定義済みマクロを参照してください。

カスタム無人ファイルをインポートするには、以下の手順を実行します。詳しくは、カスタム無人ファイルのインポートを参照してください。

1. 「**無人ファイル**」タブをクリックします。
2. 「**インポート**」アイコン () をクリックします。
3. 「**ローカル・インポート**」をクリックします。
4. オペレーティング・システムに Windows を選択します。
5. 「**参照**」をクリックし、カスタム無人ファイルを検索して選択します (例: Windows_locale_customUnattend.xml)。
6. 「**インポート**」をクリックして、ファイルを OS イメージ・リポジトリーにアップロードします。

ステップ 5. カスタム・ブート (WinPE) ファイルおよび無人ファイルを含むカスタム OS イメージ・プロファイルを作成します。詳しくは、カスタム OS イメージ・プロファイルの作成を参照してください。

1. 「**OS イメージ**」タブをクリックします。
2. カスタマイズするプロファイルを選択します (例: win2016-x86_64-install-Datacenter_Virtualization)。
3. 「**作成**」アイコン () をクリックして、「カスタマイズされたプロファイルの作成」ダイアログを表示します。
4. 「**全般**」タブで、以下の操作を行います。
   a. プロファイルの名前 (例: Custom Windows for Japanese profile) を入力します。
   b. 「**カスタム・データおよびファイル・パス**」フィールドにはデフォルト値を使用します。
   c. カスタマイズ・タイプに「**無人ファイルのみ**」を選択します。
   d. 「**次へ**」をクリックします。
5. 「**ドライバー・オプション**」タブで、「**次へ**」をクリックします。同梱のデバイス・ドライバーはデフォルトで含まれています。
6. 「**ブート・ファイル**」タブで、カスタム・ブート・ファイル (WinPE_64_ja など) を選択し、「**次へ**」をクリックします。
7. 「**ソフトウェア**」タブで、「**次へ**」をクリックします。
8. 「**無人ファイル**」タブで、カスタム無人ファイルを検索して選択し、(例: Windows_locale_customUnattend.xml) 「**次へ**」をクリックします。
9. 「**インストール・スクリプト**」タブで、「**次へ**」をクリックします。
10. 「**要約**」タブで設定を確認します。

11. 「**カスタマイズ**」をクリックして、カスタム OS イメージ・プロファイルを作成します。

ステップ 6. カスタム OS イメージ・プロファイルをターゲット・サーバーにデプロイします。詳しくは、オペレーティング・システム・イメージのデプロイを参照してください。

1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」をクリックして、「オペレーティング・システムのデプロイ: OS イメージのデプロイ」ページを表示します。
2. 各ターゲット・サーバーで、以下の操作を実行します。
   a. サーバーを選択します。
   b. 「**選択の変更**」 → 「**ネットワーク設定**」をクリックし、サーバーのホスト名、IP アドレス、サブネット・マスク、ゲートウェイ、DNS、MTU および VLAN 設定を指定します。

      ヒント: VLAN 設定は、VLAN モードが「**共通設定**」 → 「**IP の割り当て**」 → 「**VLAN を使用する**」で設定されている場合のみ使用できます。
   c. 「**デプロイするイメージ**」列のドロップダウン・リストから、カスタム OS イメージ・プロファイル (例: *<base_OS>*|*<timestamp>*_Custom Windows for Japanese profile) を選択します。

      注：すべてのターゲット・サーバーが同じカスタム・プロファイルを使用していることを確認します。
   d. (オプション) 「**ライセンス・キー**」アイコン ( ) をクリックして、インストールしたオペレーティング・システムをアクティブにするときに使用するライセンス・キーを指定します。
   e. オペレーティング・システム・イメージをデプロイする格納場所を「**ストレージ**」列から選択します。

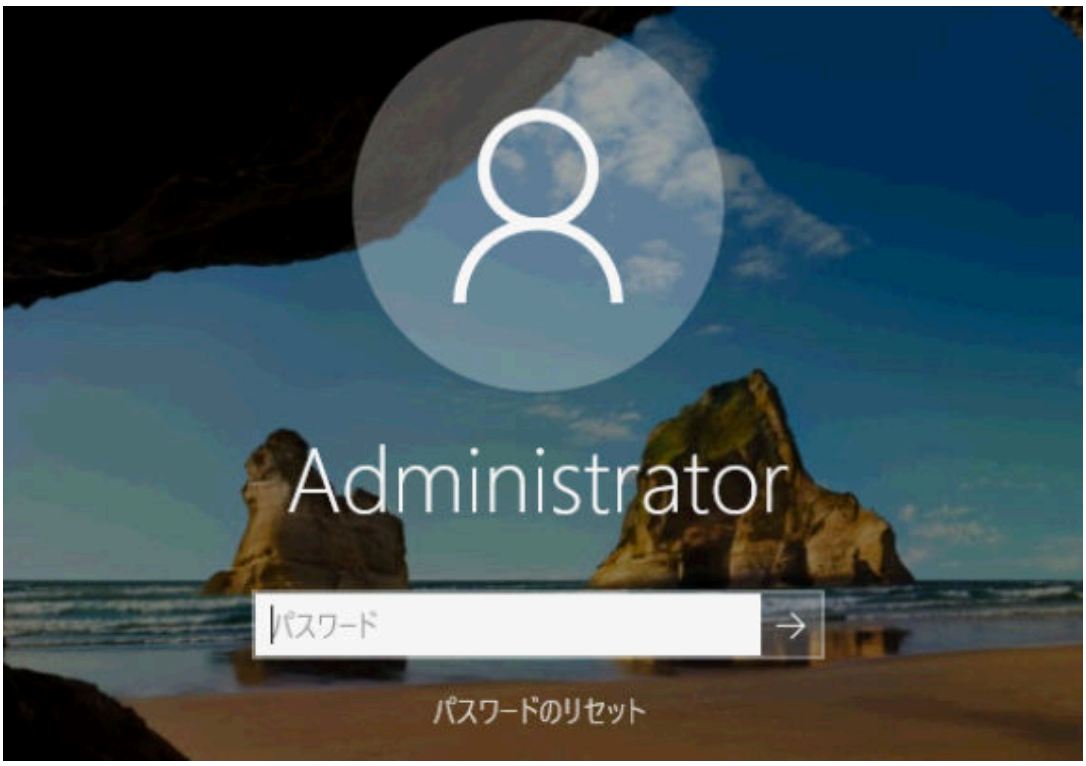
      注：オペレーティング・システム・デプロイメントが成功したことを確認するには、オペレーティング・システム・デプロイメント用に選択されたストレージ以外のすべてのストレージを、管理対象サーバーから切り離します。
   f. 選択したサーバーのデプロイメント・ステータスが「**動作可能**」になっていることを確認します。

3. ターゲット・サーバーをすべて選択し、「**イメージのデプロイ**」アイコン ( ) をクリックして、オペレーティング・システム・デプロイメントを開始します。
4. 「**カスタム設定**」タブで、「**無人および構成設定**」サブタブをクリックし、カスタム無人ファイル (例: `Windows_locale_customUnattend.xml`) を選択します。

5. (オプション) 「**Active Directory ドメイン**」タブで、Active Directory ドメインを Windows イメージ・デプロイメントの一部として結合するための情報を指定します (Windows Active Directory との統合を参照)。
6. 「**要約**」タブで設定を確認します。
7. 「**デプロイ**」をクリックしてオペレーティング・システムをデプロイします。

   「Windows のインストール」ダイアログが日本語で表示されます。

   インストールの完了後は、Windows ログイン・ページも日本語で表示されます。


Administrator
パスワード
パスワードのリセット

第 16 章　新しいデバイスをセットアップするためのエンド・ツー・エンドのシナリオ

このエンド・ツー・エンドのシナリオを使用して、Lenovo XClarity Administrator を使用して一貫性があり簡単に反復可能な方法で新しいデバイスをセットアップする方法を説明します。

ローカル・ハードディスク・ドライブへの ESXi のデプロイ

この手順を使用して、Flex System x240 計算ノード 上でローカルに取り付けられたハードディスク・ドライブに VMware ESXi 5.5 をデプロイします。この手順では、既存のサーバーからサーバー・パターンを学習し、そのサーバー・パターンの拡張 UEFI 設定カテゴリー・パターンを変更する方法、および VMware ESXi をインストールする方法を示します。

VMware ESXi 5.5 では、システムの最初の 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、システムで 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、VMware ESXi 5.5 がインストールされる各サーバーの Setup ユーティリティーを使用して、MM Config オプションの値を 3 GB に増やします。

また、仮想化に関連する事前定義済み拡張 UEFI カテゴリー・パターンのいずれかが含まれるサーバー・パターンをデプロイすることもできます。これにより、MM Config オプションが設定され、PCI 64 ビットのリソース割り振りが無効になります。

事前定義済み仮想化パターンのデプロイ

カテゴリー・パターンは、複数のサーバー・パターンで再利用できる特定のファームウェア設定を定義します。事前定義済み仮想化パターンをデプロイするには、サーバー・パターンを作成し、事前定義済み拡張 UEFI パターンをそのサーバー・パターンに適用します。その後、そのサーバー・パターンは、Flex System x240 計算ノード、Flex System x880 X6 計算ノード など、同じタイプの複数のサーバーに適用できます。

このタスクについて

サーバー・パターンを作成する場合、自身で構成を作成するか、既にセットアップされている既存のサーバーからパターン属性を学習するかを選択できます。既存のサーバーから新しいパターンを学習すると、パターン属性のほとんどが既に定義されています。

サーバー・パターンとカテゴリー・パターンについて詳しくは、サーバー・パターンの使用を参照してください。

手順

既存のサーバーから新しいパターンを学習するには、以下の手順を実行します。

ステップ 1. XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. 「**サーバー・パターン**」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。「新しいサーバー・パターン・ウィザード」が表示されます。

ステップ 4. 「**既存のサーバーからの新しいパターンの作成**」をクリックします。パターンを最初から作成することもできますが、通常は、希望する構成が含まれる既存のサーバーからパターンを作成する方が効率的です。

既存のサーバーからサーバー・パターンを作成すると、XClarity Administrator が管理対象サーバーの設定 (拡張ポート、UEFI、ベースボード管理コントローラーの設定など) を学習し、それらの設定のカテゴリー・パターンを動的に作成します。新しいサーバーの場合、XClarity Administrator は出荷時の設定を学習します。既に使用されているサーバーの場合、XClarity Administrator はカスタマイズされた設定を学習します。その後、このパターンをデプロイするサーバーに合わせてそれらの設定を変更できます。

ステップ 5. パターンを作成するときに基本構成として使用するサーバーを選択します。

注：選択するサーバーは、サーバー・パターンのデプロイ先サーバーと同じモデルである必要があります。このシナリオは、Flex System x240 計算ノード の選択に基づいています。

ステップ 6. 新しいパターンの名前と説明を入力します。

例:

- 名前: **x240_ESXi_deployment**
- 説明: **VMware ESXi のデプロイメントに適した拡張 UEFI 設定のパターン**

ステップ 7. 「**次へ**」をクリックして、選択したサーバーから情報をロードします。

ステップ 8. 「**ローカル・ストレージ**」タブで、「**ストレージ構成の指定**」を選択し、ストレージ・タイプのいずれかを選択します。その後「**次へ**」をクリックします。

ローカル・ストレージの設定について詳しくは、ローカル・ストレージの定義を参照してください。

ステップ 9. 「**I/O アダプター**」タブで、VMware ESXi をインストールするサーバーで使用されているアダプターの情報を入力します。

ベースとして使用されているサーバーに存在していたすべてのアダプターが表示されます。

インストール内のすべての Flex System x240 計算ノード が同じアダプターを使用している場合、このタブの設定を変更する必要はありません。

I/O アダプターの設定について詳しくは、I/O アダプターの定義を参照してください。

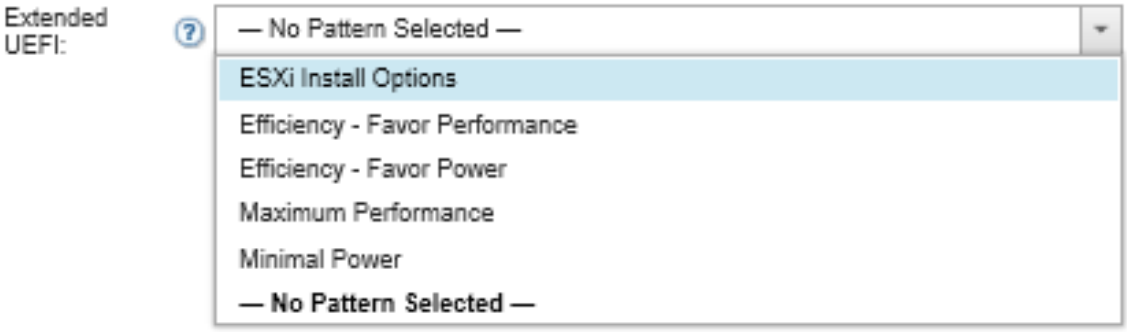
ステップ 10. 「**次へ**」をクリックして先に進みます。

ステップ 11.「**Boot**」タブで、Legacy Only ブート環境と SAN ブート環境の設定を構成します。どちらの環境も使用していない場合は、デフォルトの「**UEFI Only ブート**」を受け入れて、「**次へ**」をクリックします。

ブート設定について詳しくは、ブート・オプションの定義を参照してください。

ステップ 12.「**ファームウェアの設定**」タブで、このパターンをデプロイしたときにターゲット・サーバーに対して使用される管理コントローラーおよび UEFI ファームウェア設定を指定します (たとえば、「**x240 仮想化**」を選択します)。

このタブでは、事前定義済み拡張 UEFI パターンのいずれかを選択できます。



ファームウェア設定について詳しくは、ファームウェア設定の定義を参照してください。

ステップ 13.「**保存してデプロイ**」をクリックして、パターンを XClarity Administrator に保存し、VMware ESXi をインストールするサーバーにデプロイします。

終了後

サーバー・パターンがすべてのサーバーにデプロイされたら、オペレーティング・システムをそのサーバーにインストールできます。

Flex System x240 計算ノード への VMware ESXi のデプロイ

以下の手順をサンプル・フローとして使用することで、Flex System x240 計算ノード に ESXi オペレーティング・システムをデプロイするプロセスを示します。

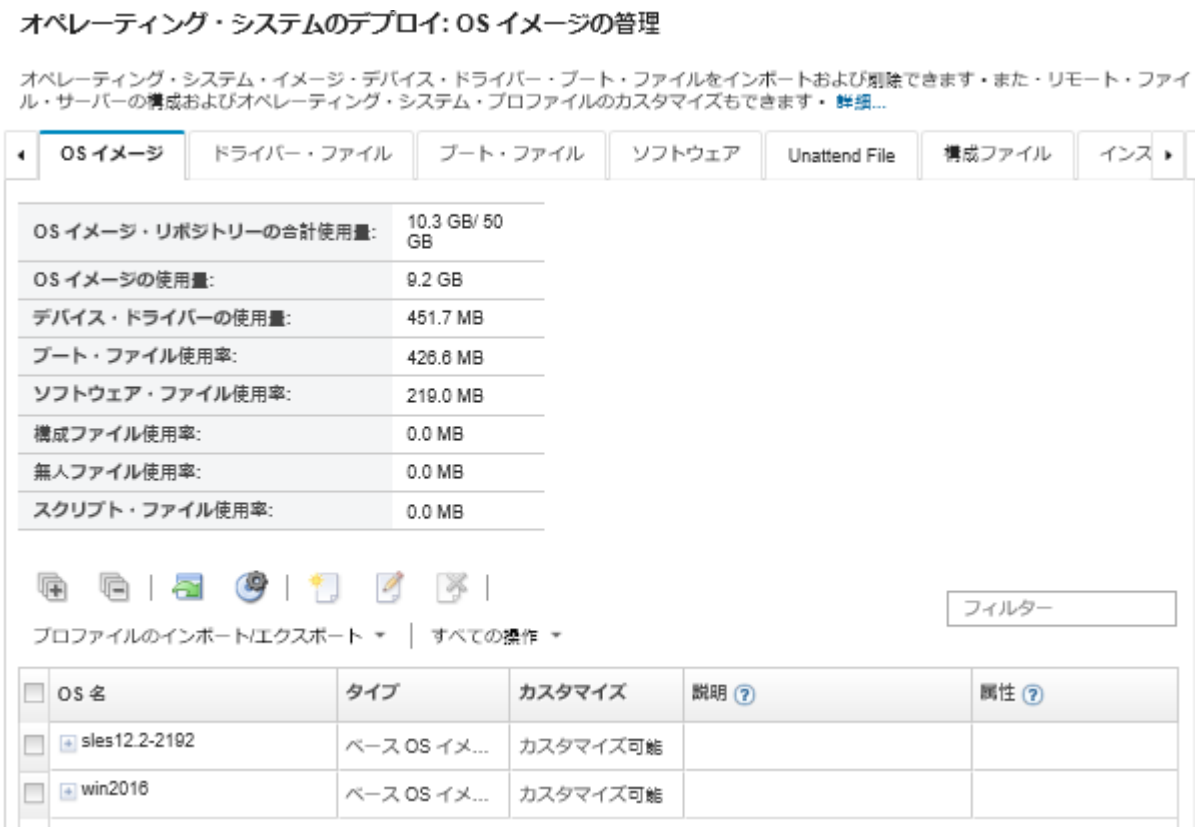
始める前に

この手順を開始する前に、Flex System x240 計算ノード が取り付けられたシャーシが Lenovo XClarity Administrator の管理対象になっていることを確認してください。

手順

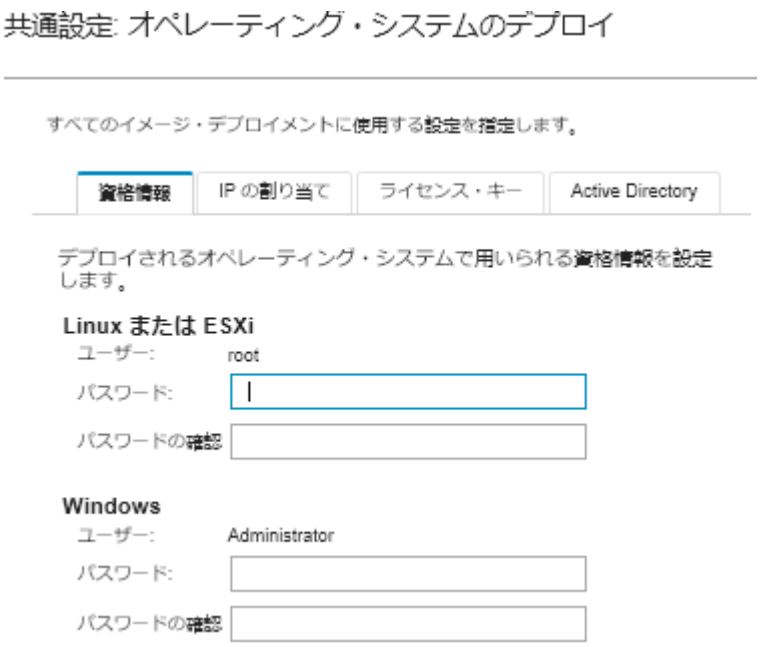
Flex System x240 計算ノード に ESXi オペレーティング・システムをデプロイするには、以下の手順を実行します。

ステップ 1. 「**すべての操作**」 → 「**OS イメージの管理**」の順にクリックして使用可能なすべてのイメージのリストを表示し、デプロイするイメージが既にOS イメージ・リポジトリーに読み込まれていることを確認します。



ステップ 2. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**OS イメージのデプロイ**」の順にクリックします。「OS イメージのデプロイ」ページが表示されます。

ステップ 3. 「**すべての操作**」 → 「**共通設定**」の順にクリックして「共通設定」ダイアログを表示し、すべてのイメージ・デプロイメントでデフォルトとして使用される共通設定を設定します。



a. 「**資格情報**」タブで、管理者アカウントによってオペレーティング・システムへのログインに使用されるパスワードを入力します。

b. 「**IP の割り当て**」タブで、オペレーティング・システムの IP アドレスをサーバーに割り当てる方法を指定します。

「**IP アドレスの割り当てに動的ホスト構成プロトコル (DHCP) を使用する**」を選択して IP アドレスを割り当てると、IP アドレス情報は、「ネットワーク設定の編集」ダイアログに表示されません (手順 605 ページの ステップ 89 を参照)。「**静的 IP アドレスの割り当て (IPv4)**」を選択すると、デプロイメントごとに IP アドレス、サブネット、およびゲートウェイを指定できます。

c. 必要に応じて、「**ライセンス・キー**」タブで、一括アクティベーション・キーを入力します。

d. 「OK」をクリックして、ダイアログを閉じます。

ステップ 4. オペレーティング・システムがデプロイされるサーバーを選択して、サーバーでオペレーティング・システム・デプロイメントの準備ができていることを確認します。最初は、デプロイ・ステータスが「作動不能」になっている場合があります。サーバーにオペレーティング・システムをデプロイするには、デプロイ・ステータスが「動作可能」になっている必要があります。

ヒント: すべてのサーバーに同じオペレーティング・システムをデプロイする場合は、複数の Flex System シャーシから複数のサーバーを選択できます。最大 28 個のサーバーを選択できます。

ステップ 5. 「**デプロイするイメージ**」列をクリックし、VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**) を選択します。

ステップ 6. 同じ列で「**ライセンス・キー**」アイコン ( ) をクリックして、このデプロイメントのライセンス・キーを入力します。

ヒント: 「共通設定」ダイアログに入力した一括アクティベーション・キーを使用することもできます。

ステップ 7. 「ストレージ」列で「**ローカル・ディスク**」が選択されていることを確認します。

ステップ 8. サーバーの行の「**ネットワーク設定**」列で「**編集**」をクリックして、このデプロイに使用されるネットワーク設定を構成します。「ネットワーク設定の編集」ページが表示されます。

以下のフィールドに入力します。

- ホスト名

- オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレス
- ドメイン・ネーム・システム (DNS) サーバー (必要な場合)
- 最大転送単位 (MTU) 速度

注：「共通設定」ダイアログから「**静的 IP アドレスの割り当て (IPv4)**」を選択した場合は (手順 604 ページの ステップ 34 を参照)、次の情報も入力します。

- IPv4 アドレス
- サブネット・マスク
- ゲートウェイ

ステップ 9. 「**OK**」をクリックして、ダイアログを閉じます。

「OS イメージのデプロイ」ページで、サーバーのデプロイ・ステータスが「動作可能」と表示されていることを確認します。

ステップ 10. 「**すべての操作**」 ➡ 「**イメージのデプロイ**」をクリックしてオペレーティング・システムをデプロイします。

ステップ 11. 構成ページで、「**デプロイ**」をクリックしてイメージをデプロイします。

サーバーに現在インストールされているオペレーティング・システムがある場合、イメージをデプロイすると現在のオペレーティング・システムが上書きされることが警告されます。

ヒント: インストールの進行状況を監視するように、リモート制御セッションをセットアップできます。「**すべての操作**」 ➡ 「**リモート制御**」をクリックして、サーバーでリモート制御セッションを開始します。

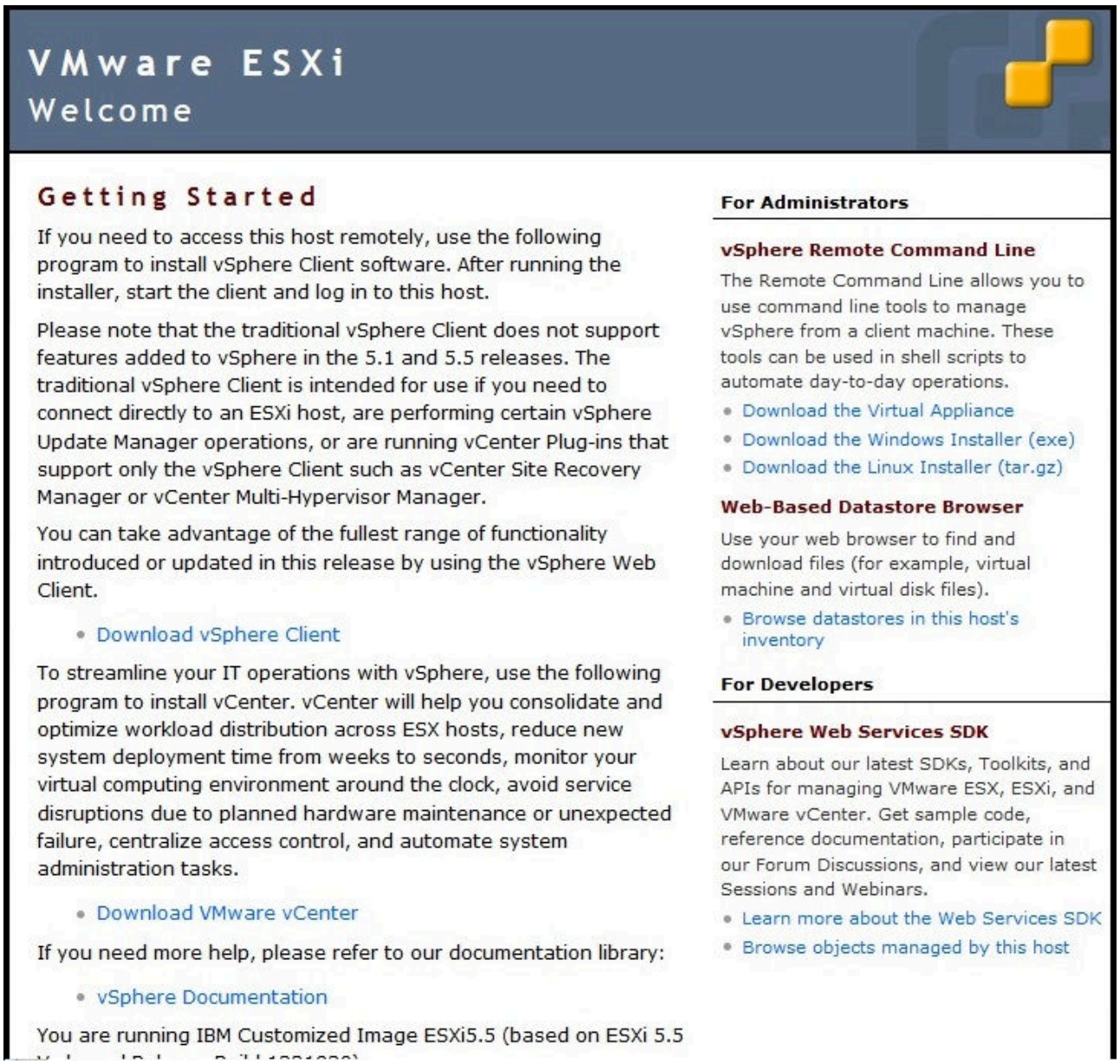
オペレーティング・システムをデプロイする際には、Lenovo XClarity Administrator によってデプロイを追跡するジョブが開始されます。デプロイメント・ジョブのステータスを表示するには、Lenovo XClarity Administrator のメニュー・バーで「**ジョブ**」をクリックします。その後、「**実行中**」タブをクリックします。

実行中のジョブをポイントすると、ジョブの完了率などの詳細が表示されます。

結果

オペレーティング・システムのデプロイメントが完了したら、「ネットワーク設定の編集」ページで指定した IP アドレスにログインして、構成プロセスに進みます。

注：イメージに付与されるライセンスは 60 日間の無料試用版です。使用するには、VMware ライセンスのすべての要件を満たす必要があります。



SAN ストレージへの ESXi のデプロイ

この手順を使用して、サーバーに接続されている SAN ボリュームに VMware ESXi 5.5 をデプロイします。

オペレーティング・システムを SAN にデプロイすると、そのオペレーティング・システムは、サーバー・パターンを使用して構成された最初の SAN ブート・ターゲットにデプロイされます。また、SAN からブートされるサーバーで、ローカル・ハードディスク・ドライブを有効にすることはできません。ハードディスク・ドライブが存在する場合は、無効にするか削除する必要があります。

SAN ブートをサポートするためのサーバー・パターンのデプロイ

サーバー・パターンを作成およびデプロイして、SAN からのシステムのブートをサポートする場合は、サーバーの一部である SAN ブート・ターゲットとアダプターを確実に特定してください。

手順

SAN ストレージへのオペレーティング・システムのデプロイメントをサポートするサーバー・パターンを作成およびデプロイするには、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、「**プロビジョニング**」 → 「**パターン**」の順にクリックします。「構成パターン: パターン」ページが表示されます。

ステップ 2. オペレーティング・システムがデプロイされるストレージ・ボリュームの WWPN および LUN ID を特定するには、カテゴリー・パターンを作成します。

a. 「**カテゴリー・パターン**」タブをクリックします。

b. 「**Fibre Channel ブート・ターゲット・パターン**」をクリックし、「**作成**」アイコン ( ) をクリックします。

c. ストレージ・ターゲットの WWPN を入力します。

注：「**複数の LUN 識別子を許可する**」をクリックし、複数のターゲット LUN 識別子を同じストレージ・ボリュームに割り当てます。

d. 「**作成**」をクリックして、パターンを作成します。ターゲットは、Fibre Channel ブート・ターゲット・パターンのリストに表示されます。

ステップ 3. 「**サーバー・パターン**」タブをクリックして、パターンを作成します。

ステップ 4. 「**作成**」アイコン ( ) をクリックします。「新しいサーバー・パターン・ウィザード」が表示されます。

ステップ 5. 「**新しいパターンを最初から作成**」をクリックします。

ステップ 6. 「**全般**」タブで、以下の操作を行います。

- フォーム・ファクターの「**Flex 計算ノード**」を選択します。
- パターンの名前 (**x240_san_boot**) と説明を指定します。
- 「**次へ**」をクリックします。

ステップ 7. ローカル・ドライブのスキャンに関連するブート時間を改善するためにディスクレス・システムを使用している場合は、「**ローカル・ストレージ**」タブで、ローカル・ストレージ・アダプターを無効にすることを検討してください。その後、「**次へ**」をクリックします。

ステップ 8. 「**I/O アダプター**」タブで、イーサネット・カードと Fibre Channel カードを追加します。アダプターが適切な PCI スロットにあることを確認します。

a. カードごとに、「**I/O アダプターの追加**」をクリックし、カードがある PCI スロットを選択して、カードを選択します。

注：必ずイーサネット・カードと Fibre Channel カードを指定してください。

b. I/O アダプター・アドレス指定が「**仮想**」に設定されていることを確認します。次に、「**編集**」アイコン ( ) をクリックして、イーサネット (MAC) 仮想アドレス指定と Fibre Channel (WWN) 仮想アドレス指定に使用する構成を指定します。

注：「仮想アドレス指定の編集」ページで、イーサネット・カードの出荷時書き込み MAC アドレスを使用するように選択するには、仮想アドレス指定を無効にします。ただし、Fibre Channel ブート・ターゲット・パターンを選択して利用するには、Fibre Channel アダプターの仮想アドレス指定を使用する必要があります。

c. 「**次へ**」をクリックします。

ステップ 9. 「**Boot**」タブで、前に作成した SAN ブート・ターゲット・パターンを追加します。

a. 「**SAN ブート**」タブで、定義したブート・ターゲット・パターンを選択します。

b. 「**次へ**」をクリックします。

ステップ 10.「**ファームウェアの設定**」タブで、このサーバー・パターンに含める追加のカテゴリー・パターンを定義します。定義できるカテゴリー・パターンを以下に示します。

- **システム情報** (Lenovo XClarity Administratorオンライン・ドキュメントのシステム情報設定の定義)
- **管理インターフェース** (Lenovo XClarity Administratorオンライン・ドキュメントの管理インターフェース設定の定義)
- **デバイスおよび I/O ポート** (Lenovo XClarity Administratorオンライン・ドキュメントのデバイスおよび I/O ポート設定の定義)
- 「**拡張 BMC**」。以前に学習したベースボード管理コントローラー設定から選択できます (拡張管理コントローラー設定の定義を参照)。
- 「**拡張 UEFI**」。事前定義済み設定または以前に学習した UEFI 設定から選択できます (拡張 UEFI 設定の定義を参照)。

ステップ 11.「**保存してデプロイ**」をクリックして、パターンを Lenovo XClarity Administrator に保存し、VMware ESXi をインストールするサーバーにデプロイします。

終了後

サーバー・パターンがすべてのサーバーにデプロイされたら、以下の手順を考慮してください。

1. 作成された仮想化 WWPN アドレスをストレージ・ゾーンに追加します。これにより、サーバーは定義済みストレージ LUN にアクセスできます。

   ヒント: サーバー・プロファイルのデプロイ後、仮想化 WWPN アドレスを見つけるには、サーバー・プロファイルを確認します。

   a. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 → 「**サーバー・プロファイル**」の順にクリックします。

   b. デプロイされたサーバー・プロファイル (たとえば **x240_SAN_boot**) をクリックします。「**仮想アドレス・マッピング**」タブにアドレスのリストが表示されます。

2. オペレーティング・システムをサーバーにデプロイします。

SAN ストレージへの VMware ESXi のデプロイ

以下の手順をサンプル・フローとして使用することで、サーバーに接続されている SAN ストレージに ESXi オペレーティング・システムをデプロイするプロセスを示します。

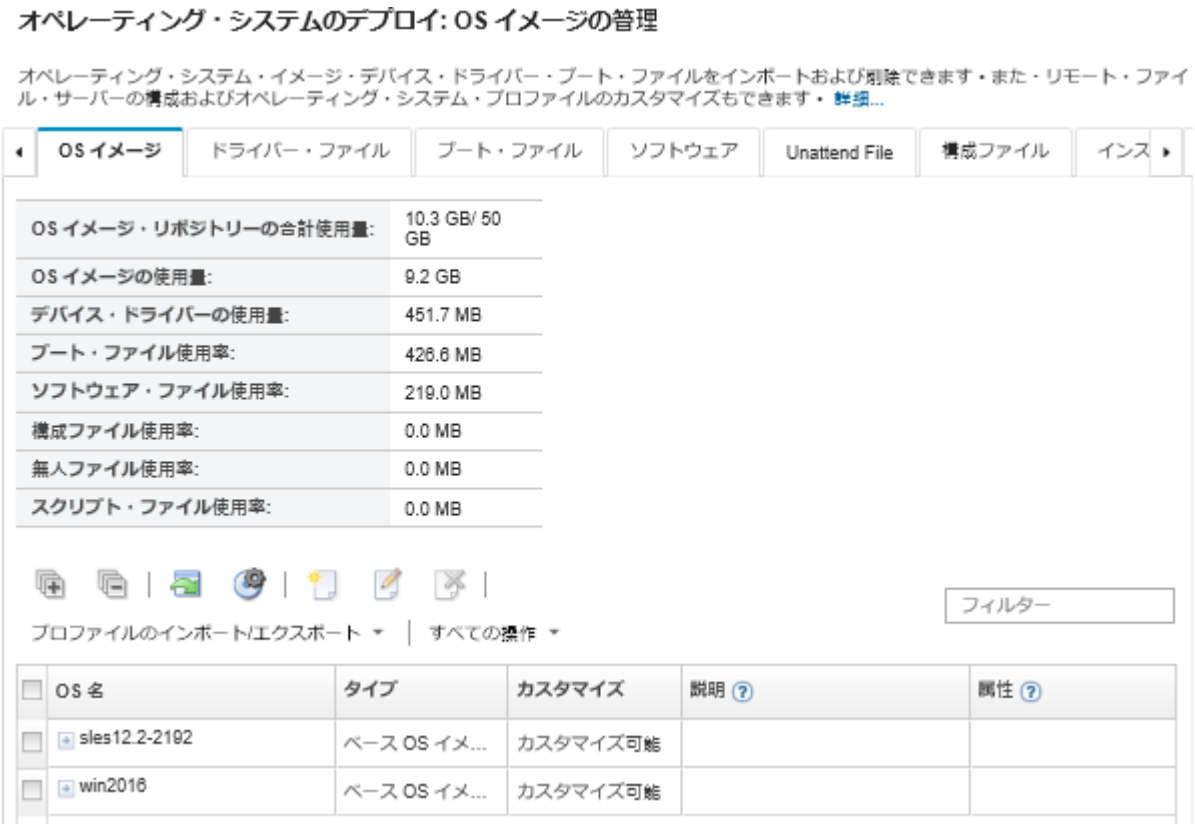
始める前に

この手順を開始する前に、Flex System x220 計算ノード が取り付けられたシャーシが Lenovo XClarity Administrator の管理対象になっていることを確認してください。

手順

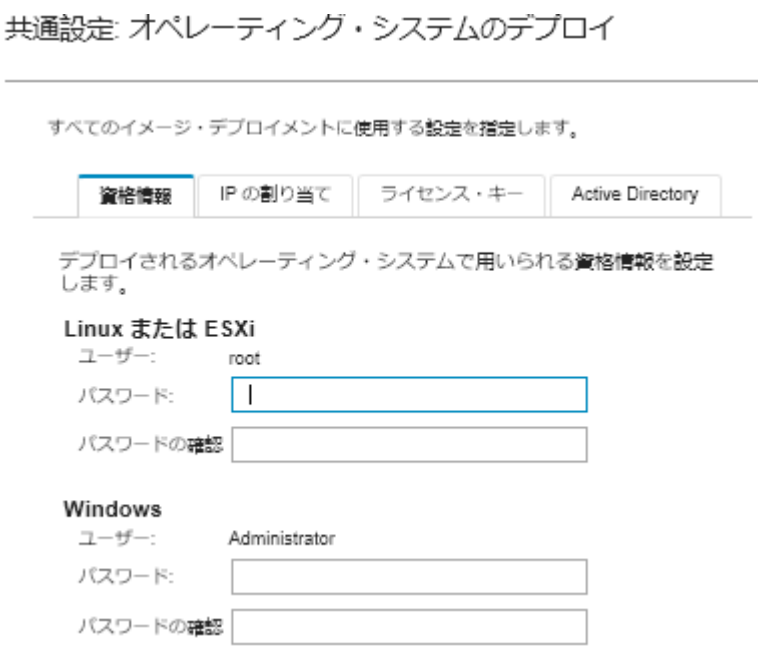
Flex System x222 計算ノード に ESXi オペレーティング・システムをデプロイするには、以下の手順を実行します。

ステップ 1. 「**すべての操作**」 ➡ 「**OS イメージの管理**」の順にクリックして、デプロイするイメージが既にOS イメージ・リポジトリーに読み込まれていることを確認します。



ステップ 2. Lenovo XClarity Administrator のメニュー・バーで、「**プロビジョニング**」 ➡ 「**OS イメージのデプロイ**」の順にクリックします。

ステップ 3. 「**すべての操作**」 ➡ 「**共通設定**」の順にクリックして「共通設定: オペレーティング・システムのデプロイ」ダイアログを表示し、すべてのイメージ・デプロイメントでデフォルトとして使用される共通設定を設定します。



a. 「**資格情報**」タブで、管理者アカウントによってオペレーティング・システムへのログインに使用されるパスワードを入力します。

b. 「**IP の割り当て**」タブで、オペレーティング・システムの IP アドレスをサーバーに割り当てる方法を指定します。

「**IP アドレスの割り当てに動的ホスト構成プロトコル (DHCP) を使用する**」を選択して IP アドレスを割り当てると、IP アドレス情報は、「ネットワーク設定の編集」ダイアログに表示されません (手順 614 ページの ステップ 89 を参照)。「**静的 IP アドレスの割り当て (IPv4)**」を選択すると、デプロイメントごとに IP アドレス、サブネット、およびゲートウェイを指定できます。

c. 必要に応じて、「**ライセンス・キー**」タブで、一括アクティベーション・キーを入力します。

d. 「**OK**」をクリックして、ダイアログを閉じます。

ステップ 4. オペレーティング・システムがデプロイされるサーバーを選択して、サーバーでオペレーティング・システム・デプロイメントの準備ができていることを確認します。最初は、デプロイ・ステータスが「作動不能」になっている場合があります。サーバーにオペレーティング・システムをデプロイするには、デプロイ・ステータスが「動作可能」になっている必要があります。

ヒント: すべてのサーバーに同じオペレーティング・システムをデプロイする場合は、複数の Flex System シャーシから複数のサーバーを選択できます。最大 28 個のサーバーを選択できます。

ステップ 5. 「**デプロイするイメージ**」列をクリックし、VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**) を選択します。

ステップ 6. 同じ列で「**ライセンス・キー**」アイコン ( ) をクリックして、このデプロイメントのライセンス・キーを入力します。

ヒント: 「共通設定: オペレーティング・システムのデプロイ」ダイアログに入力した一括アクティベーション・キーを使用することもできます。

ステップ 7. 「**ストレージ**」列で、オペレーティング・システムのデプロイメント先となる SAN ストレージを選択します。

ストレージが以下のように表示されます。
LUN: *<LUN VALUE>* WWPN: *<WWPN_VALUE>*

ステップ 8. サーバーの「**ネットワーク設定**」列の「**編集**」をクリックして、このデプロイに使用されるネットワーク設定を構成します。「ネットワーク設定の編集」ページが表示されます。

以下のフィールドに入力します。
- ホスト名
- オペレーティング・システムがインストールされるホスト上にあるポートの MAC アドレス
- ドメイン・ネーム・システム (DNS) サーバー (必要な場合)
- 最大転送単位 (MTU) 速度

注：「共通設定: オペレーティング・システムのデプロイ」ダイアログから「**静的 IP アドレスの割り当て (IPv4)**」を選択した場合は (手順 612 ページの ステップ 34)、次の情報も入力します。
- IPv4 アドレス
- サブネット・マスク
- ゲートウェイ

ステップ 9. 「OK」をクリックして、ダイアログを閉じます。

「OS イメージのデプロイ」ページで、サーバーのデプロイメント・ステータスが現在「動作可能」と表示されています。

ステップ 10. 「**すべての操作**」 ➡ 「**イメージのデプロイ**」をクリックしてオペレーティング・システムをデプロイします。

ステップ 11. 構成ページで、「**デプロイ**」をクリックしてイメージをデプロイします。

サーバーに現在インストールされているオペレーティング・システムがある場合、イメージをデプロイすると現在のオペレーティング・システムが上書きされることが警告されます。

ヒント: インストールの進行状況を監視するように、リモート制御セッションをセットアップできます。「**すべての操作**」 ➡ 「**リモート制御**」をクリックして、サーバーでリモート制御セッションを開始します。

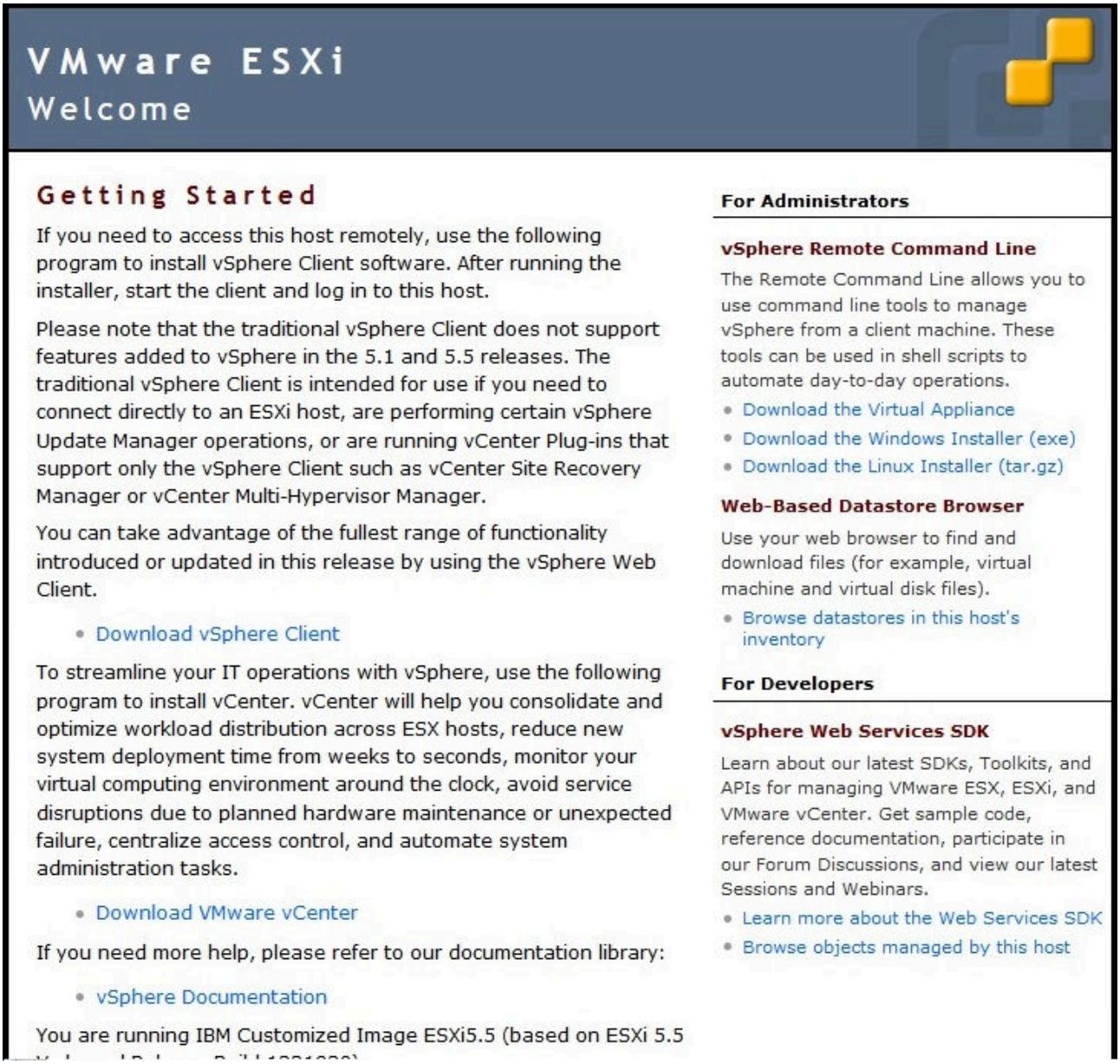
オペレーティング・システムをデプロイする際には、Lenovo XClarity Administrator によってデプロイを追跡するジョブが開始されます。デプロイメント・ジョブのステータスを表示するには、Lenovo XClarity Administrator のメニュー・バーで「**ジョブ**」をクリックします。その後、「**実行中**」タブをクリックします。

実行中のジョブをポイントすると、ジョブの完了率などの詳細が表示されます。

結果

オペレーティング・システム・デプロイメントが完了したら、「ネットワーク設定の編集」ページで指定した IP アドレスにログインして、構成プロセスに進みます。

注：イメージに付与されるライセンスは 60 日間の無料試用版です。使用するには、VMware ライセンスのすべての要件を満たす必要があります。


VMware ESXi
Welcome
Getting Started
If you need to access this host remotely, use the following program to install vSphere Client software. After running the installer, start the client and log in to this host.
Please note that the traditional vSphere Client does not support features added to vSphere in the 5.1 and 5.5 releases. The traditional vSphere Client is intended for use if you need to connect directly to an ESXi host, are performing certain vSphere Update Manager operations, or are running vCenter Plug-ins that support only the vSphere Client such as vCenter Site Recovery Manager or vCenter Multi-Hypervisor Manager.
You can take advantage of the fullest range of functionality introduced or updated in this release by using the vSphere Web Client.
Download vSphere Client
To streamline your IT operations with vSphere, use the following program to install vCenter. vCenter will help you consolidate and optimize workload distribution across ESX hosts, reduce new system deployment time from weeks to seconds, monitor your virtual computing environment around the clock, avoid service disruptions due to planned hardware maintenance or unexpected failure, centralize access control, and automate system administration tasks.
Download VMware vCenter
If you need more help, please refer to our documentation library:
vSphere Documentation
You are running IBM Customized Image ESXi5.5 (based on ESXi 5.5
For Administrators
vSphere Remote Command Line
The Remote Command Line allows you to use command line tools to manage vSphere from a client machine. These tools can be used in shell scripts to automate day-to-day operations.
Download the Virtual Appliance
Download the Windows Installer (exe)
Download the Linux Installer (tar.gz)
Web-Based Datastore Browser
Use your web browser to find and download files (for example, virtual machine and virtual disk files).
Browse datastores in this host's inventory
For Developers
vSphere Web Services SDK
Learn about our latest SDKs, Toolkits, and APIs for managing VMware ESX, ESXi, and VMware vCenter. Get sample code, reference documentation, participate in our Forum Discussions, and view our latest Sessions and Webinars.
Learn more about the Web Services SDK
Browse objects managed by this host

注記

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、Lenovo の営業担当員にお尋ねください。

本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、他の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、いかなる特許出願においても実施権を許諾することを意味するものではありません。お問い合わせは、書面にて下記宛先にお送りください。

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO は、本書を特定物として「現存するままの状態で」提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書の内容は、Lenovo またはサード・パーティーの知的所有権のもとで明示または黙示のライセンスまたは損害補償として機能するものではありません。本書に記載されている情報はすべて特定の環境で得られたものであり、例として提示されるものです。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

LENOVO、SYSTEM、NEXTSCALE、SYSTEM X、THINKSERVER、THINKSYSTEM および XCLARITY は Lenovo の商標です。