H3Cサーバー
UniSystemユーザーガイド

New h3c Technologies Co.,Ltd.
http://www.h3c.com

ソフトウェアバージョン:UniSystem-2.72以上ドキュメントバージョン:6W111-20250107

Copyright(C)2020-2025, New H3C Technologies Co.,Ltd. and its licensors

無断複写転載を禁じます。

このマニュアルのいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または送信することはできません。

商標

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者に帰属します。

お知らせ

このドキュメントの情報は、予告なしに変更されることがあります。記述、情報、および推奨事項を含むこのドキュメントのすべての内容は正確であると考えられますが、それらは明示的または黙示的を問わず、いかなる種類の保証もなしに提示されています。H3Cは、ここに含まれる技術的または編集上の誤りまたは省略に対して責任を負わないものとします。

はじめに

ここでは、マニュアルに関する次のトピックについて説明します。

- 対象読者
- 表記規則。
- ドキュメントに関するフィードバック。

対象読者

このマニュアルは、次の読者を対象としています。

- ネットワークプランナー。
- フィールドテクニカルサポートおよびサービスエンジニア。
- G3、G5、およびG6サーバーで作業するサーバー管理者。

表記規則

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法

条約	説明
太字	太字のテキストは、文字通り入力したコマンドとキーワードを表します。
斜体	斜体のテキストは、実際の値に置き換える引数を表します。
[ ]	角カッコは、オプションの構文選択肢(キーワードまたは引数)を囲みます。
{ x | y | ... }	中カッコは、必要な構文の選択肢を縦棒で区切って囲み、その中から1つを選択します。
[x | y | ...]	角カッコは、縦棒で区切られたオプションの構文選択肢のセットを囲み、その中から1つを選択するか、何も選択しないかを選択します。
{ x | y | ... } *	アスタリスクの付いた中括弧は、縦棒で区切られた必要な構文の選択肢のセットを囲み、その中から少なくとも1つを選択します。
[x | y | ...] *	アスタリスクの付いた角カッコは、縦棒で区切られたオプションの構文選択肢を囲み、そこから1つの選択肢を選択するか、複数の選択肢を選択するか、または何も選択しないかを選択します。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	ポンド記号(#)で始まる行はコメントです。

GUIの規則

条約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。たとえば、**New user**ウィンドウが開いたら、**OK**をクリックします。
>	複数レベルのメニューは、山カッコで区切ります。例: **File>Create＞フォルダ**。

記号

条約	説明
⚠警告!	理解または従わないと人身傷害を引き起こす可能性のある重要な情報に注意を喚起する警告。
△注意:	理解または従わないと、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある重要な情報に注意を喚起するアラート。
ⓘ重要:	重要な情報に注意を喚起するアラート。
メモ:	追加または補足情報を含むアラート。
ヒント:	有用な情報を提供するアラート。

ネットワークトポロジアイコン

条約	説明
	ルータ、スイッチ、ファイアウォールなどの一般的なネットワークデバイスを表します。
	ルータまたはレイヤ3スイッチなどのルーティング対応デバイスを表します。
	レイヤ2またはレイヤ3スイッチなどの汎用スイッチ、またはレイヤ2フォワーディングおよびその他のレイヤ2機能をサポートするルータを表します。
	アクセスコントローラ、ユニファイド有線WLANモジュール、またはユニファイド有線WLANスイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向性信号を表します。
	方向信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。
	ファイアウォール、ロードバランシング、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

本書で提供される例

このドキュメントの例では、ハードウェアモデル、設定、またはソフトウェアバージョンがお使いのデバイスとは異なるデバイスが使用されている場合があります。ポート番号、サンプル出力、スクリーンショット、および例に含まれるその他の情報が、お使いのデバイスの情報と異なるのは正常です。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお送りください。

ご意見をお待ちしております。

内容

はじめに 1
アーキテクチャ 1
特長 1
アプリケーションシナリオ 2
対象製品 2
ガイドライン 4
UniSystemにログインする 5
UniSystem(非統合O&Mバージョン)へのログイン 5
UniSystemログインの準備 5
UniSystem Webインターフェイスにログインする 7
UniSystem(統合O&Mバージョン)へのログイン 7
ハードウェア環境をセットアップする 7
UniSystem Webインターフェイスにログインする 8
UniSystem Webインターフェイスのレイアウト 10
ショートカットでアクセス 11
UniSystemのバージョン情報の確認 12
ユーザーの管理 12
ユーザーの管理 12
ローカルユーザーの管理 12
LDAPユーザーグループの管理 17
ロール管理 20
オンラインユーザー情報の表示 23
デバイスの管理 25
エンクロージャーの管理 25
一般的な制限事項とガイドライン 25
エンクロージャーの管理 25
OMモジュールの管理 32
AEモジュールの管理 33
ブレードサーバーの管理 34
インターコネクトモジュールの表示 39
電源システム情報の表示 39
ファンシステム情報の表示 40
電源情報を表示する 43
電源履歴の表示 44
VCの事前設定 45
システムログを表示する 45
エンクロージャートポロジの表示 46
サーバーの管理 48
サーバーの管理 48
サーバー情報の表示 64
UniSystemによるサーバーのリモート管理 71
スイッチの管理 76
スイッチ管理機能を使用する 76
スイッチの詳細の表示 81
スイッチラベルの管理 83
インフラストラクチャ 85
インフラストラクチャの管理 85
インフラストラクチャの詳細を表示 86
インフラストラクチャデバイスのより多くのオプション 88
カスタム監視テンプレートの管理 92
データセンター管理 99
データセンター情報の表示 99
データセンターの管理 99

機器室情報を表示する 100
機器室の管理 101
キャビネット情報の表示 103
キャビネットの管理 103
デバイスの管理 106
テンプレートの管理 108
エンクロージャーテンプレートの管理 108
エンクロージャーテンプレート情報の表示 108
エンクロージャーテンプレートを追加する 109
エンクロージャーテンプレートの削除 110
エンクロージャーテンプレートをコピーする 110
エンクロージャーテンプレートを編集する 111
サーバーテンプレートの管理 111
サーバーテンプレートの管理について 111
サーバーテンプレートを追加する 111
HDM/BIOSテンプレートの設定 112
HDMをオンラインで構成 113
BIOSをオンラインで設定します。 121
接続設定の構成 122
RAID構成テンプレートの構成 124
OSの設定 127
HDM/BIOSテンプレートの設定 136
このタスクについて 136
HDM/BIOS設定のエクスポート 136
テンプレートの管理 137
リポジトリの設定 137
このタスクについて 137
ネットワークダイアグラム 138
リポジトリを追加する 138
リポジトリのインベントリを作成する 140
(オプション)カスタムリポジトリまたはISOファイルを作成します。 141
リポジトリを編集する 142
LastestREPO更新を有効にする 143
スイッチテンプレートの管理 144
スイッチテンプレートリストページにアクセスする 144
スイッチテンプレートの削除 145
アドレスプールの管理 145
IPv4アドレスプールを管理する 145
IPv6アドレスプールを管理する 147
ホスト名プールの管理 148
ネットワークテンプレートを管理する 150
ネットワークの管理 150
インターコネクトモジュールテンプレートの管理 152
イメージの管理 154
制約事項とガイドライン 154
手順 154
クローンイメージ 155
このタスクについて 155
制約事項とガイドライン 156
手順 157
ディスクレスブートを構成する 158
はじめに 158
サポートされるオペレーティングシステム 159
ボリュームを作成する 159
ボリュームをコピーする 160
ボリュームを削除する 161

認証の設定 ... 161
サーバーの導入 ... 162
エンクロージャーテンプレートの適用 ... 162
エンクロージャーテンプレートをエンクロージャーに適用する ... 162
エンクロージャー設定ファイル ... 164
このタスクについて ... 164
手順 ... 164
エンクロージャースロットコンフィギュレーションファイル ... 165
このタスクについて ... 165
手順 ... 166
サーバーテンプレートの適用 ... 167
サーバーテンプレートをサーバーに適用する ... 167
サーバー構成ファイル ... 170
サーバー構成ファイルを表示する ... 171
サーバー構成ファイルを編集する ... 171
サーバー構成ファイルの適用 ... 172
サーバー構成ファイルの削除 ... 173
コンポーネントを更新する ... 173
タスクを追加する ... 173
タスクのインベントリと展開 ... 175
タスクの詳細を表示する ... 177
タスクを編集する ... 178
問題のトラブルシューティング ... 178
ファームウェアのアップデート ... 180
ファームウェアをオフラインで更新します。 ... 180
HDM帯域外管理を使用してファームウェアを更新する ... 181
安全な消去 ... 182
サーバーソフトウェアライセンス管理 ... 185
サーバーの診断 ... 188
診断タスクリストを表示する ... 188
診断タスクを構成する ... 188
タスクの詳細を表示する ... 190
監視の構成 ... 192
操作ログの表示 ... 192
このタスクについて ... 192
手順 ... 192
アラーム転送の設定 ... 192
リスニング設定の構成 ... 193
電子メール通知を構成する ... 195
SNMP設定の構成 ... 198
WeCom通知の設定 ... 199
webhook通知を構成する ... 201
SMS通知を構成する ... 202
音声通知を設定する ... 203
WhatsApp通知を設定する ... 204
ノイズ低減ポリシーを設定する ... 206
アクティビティログの表示 ... 208
故障予知 ... 208
ドライブ予測 ... 208
電力効率と予測の管理(G6以降のサーバー) ... 210
エネルギー効率統計 ... 210
効率統計について ... 210
手順 ... 211
エネルギー効率分析 ... 211
入口温度解析の設定 ... 211

サーバー使用率分析の構成 ... 213
ラックスペースの分析 ... 214
電源解析 ... 214
詳細設定を構成する ... 215
ワンキー消費電力制限を行う ... 215
このタスクについて ... 215
制約事項とガイドライン ... 215
手順 ... 216
キャビネットのインテリジェントな電源管理 ... 217
キャビネットのインテリジェント電源管理について ... 217
制約事項とガイドライン ... 217
手順 ... 218
資産管理 ... 219
資産の概要 ... 219
資産インベントリ ... 220
資産の変更 ... 228
資産検査 ... 229
このタスクについて ... 229
前提条件 ... 230
特定のタスクの表示 ... 230
検査タスクを追加する ... 231
検査タスクに関する詳細情報の表示 ... 233
検査タスクの編集 ... 233
検査タスクの削除 ... 234
保守管理 ... 234
DHCPサーバーを設定する ... 236
DHCPクライアント情報を表示する ... 237
静的IP割り当ての設定 ... 238
IP割り当て一覧をエクスポートする ... 239
PXEデプロイメントの設定 ... 239
このタスクについて ... 239
サポートされるOS ... 240
制約事項とガイドライン ... 240
手順 ... 240
PXE OSインストールパラメーターの設定 ... 241
カスタムKSファイルを編集する ... 242
既定のKSファイルを表示する ... 243
KSファイルを適用する ... 244
ソフトウェアのプッシュとインストール ... 244
このタスクについて ... 244
制約事項とガイドライン ... 244
前提条件 ... 245
手順 ... 248
リモートコマンド ... 250
pingコマンド ... 250
IPMIコマンド ... 250
Redfishコマンド ... 251
UniSystemをUniSystemプラグインとしてvCenter Serverに組み込む ... 252
この機能について ... 252
前提条件 ... 252
制約事項とガイドライン ... 252
UniSystemプラグインのインストール ... 252
UniSystemプラグインのアンインストール ... 253
システム設定を構成する ... 254
ネットワーク設定を構成する ... 254
Ethernetアダプターの基本情報を表示する ... 255

UniSystemのホスト名を設定する ... 256
ネットワークポートのIPアドレス取得方法とDNSサーバードレスを設定します。 ... 256
DNS情報を表示する ... 257
ネットワーク接続のテスト ... 257
プロキシ設定の構成 ... 258
このタスクについて ... 258
手順 ... 258
システム時刻の設定 ... 259
このタスクについて ... 259
NTPサーバーとのシステム時刻の同期 ... 260
システム時刻を手動で設定する ... 260
クラスタを構成する ... 261
このタスクについて ... 261
前提条件 ... 261
制約事項とガイドライン ... 261
手順 ... 261
保守とアップグレード ... 263
UniSystemデータのバックアップと復元 ... 263
UniSystemソフトウェアのアップグレード ... 264
ログイン時のセキュリティヒントを設定する ... 267
このタスクについて ... 267
手順 ... 267
リモートコントロール ... 267
修復設定を有効にする ... 268
修復ステータスの表示 ... 270
カスタムメニュー ... 271
現在のメニューとすべてのメニュー項目を表示する ... 271
カスタムメニューを作成する ... 271
カスタムメニューを編集する ... 272
カスタムメニューを削除する ... 273
SMTP設定 ... 274
iService構成 ... 274
スコープマネジメント ... 276
スコープを表示する ... 276
スコープを追加する ... 277
スコープを編集する ... 278
範囲を削除する ... 279
LDAPの管理 ... 279
LDAPサーバー情報の表示とサーバーへの接続のテスト ... 279
LDAPサーバーを追加する ... 280
LDAPサーバーの編集 ... 280
LDAPサーバーを削除する ... 281
SSL証明書の管理 ... 281
略語 ... 286
付録Aディスクレスブート互換OSのインストール ... 287
概要 ... 287
制約事項とガイドライン ... 287
手順 ... 287
UniSystemのインストール ... 287
OSイメージファイルを準備する ... 287
ストレージボリュームを作成する ... 287
AEモジュールのIPアドレスを設定します。 ... 288
BIOSを使用してサーバーのEthernetアダプターを設定します。 ... 289
OSのインストール ... 295
付録B:UniSystem VGAを使用 ... 304

Webインターフェイスのレイアウト 304
関数 305
ブレードサーバーのKVMコンソールへのアクセス(AEモジュールの場合のみ) 305
UniSystemサーバーのIPアドレスの構成 305

はじめに

UniSystemは、インテリジェントで拡張可能なサーバー管理ソフトウェアであり、統一された直感的なグラフィカルユーザーインターフェイスからリモートでサーバーを管理できます。

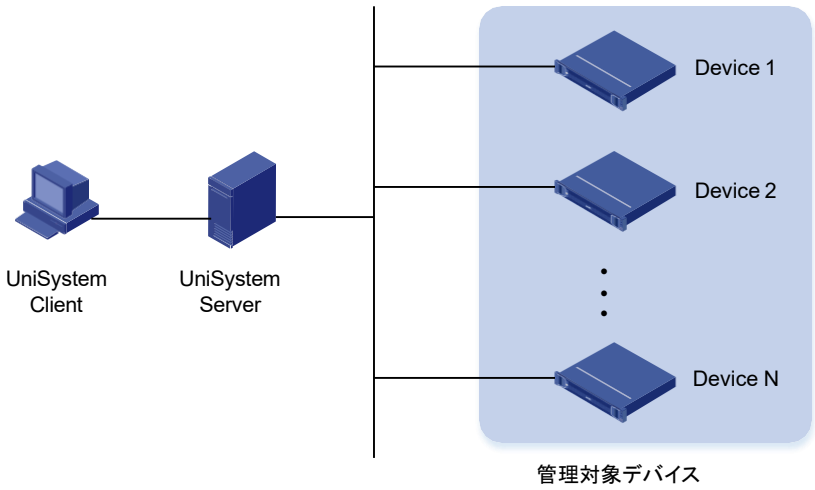
アーキテクチャ

図1に示すように、UniSystemアーキテクチャには次の要素が含まれています。

- **UniSystemクライアント**: Webブラウザを介してUniSystemにアクセスするために使用されるエンドポイントデバイス(PCなど)。
- **UniSystemサーバー**: UniSystemサーバーソフトウェアをホストするPC、物理サーバー、AEモジュールまたはVM。AEモジュールにはUniSystemが事前にインストールされています。
- **Managed devices**: UniSystemによって管理されるデバイス。

UniSystemクライアントとUniSystemサーバーは同じデバイス上に存在できます。つまり、UniSystemサーバーが存在するホストのブラウザからUniSystemにアクセスできます。

図1 UniSystemアーキテクチャ



特長

UniSystemは次の機能を提供します。

- **Devices**: UniSystemのエンクロージャー、サーバー、およびスイッチを一元管理できます。UniSystemにデバイスを追加したり、UniSystemが管理するデバイスに関する情報を表示したり、デバイスを管理したりできます。
- **Templates**: BIOS、HDM、RAID、およびオペレーティングシステムの設定をサーバーにデプロイするためのテンプレートを定義できます。
- **Deployment**: サーバーとエンクロージャーのテンプレートを適用してデバイスを一括構成し、ファームウェアやドライバーの更新などのコンポーネントの更新をサーバーにデプロイできます。
- **Monitor**:次の機能を提供します。
  - レポートと操作ログを使用して、管理対象サーバーのステータスを確認できます。
  - ユーザー定義のアラーム電子メール通知設定に基づいて、指定された電子メール受信者

へのアラームの転送をサポートします。

モニター機能は、問題のトラブルシューティングに役立ち、運用とメンテナンスの効率を向上させます。

- **Asset management**: 資産を包括的に監視および管理し、資産のステータスをリアルタイムで把握し、リソース使用率を最適化するために、資産の概要、資産インベントリ、資産検査などの機能を提供します。
- **Tools**: DHCPサーバー、PXE、FIST SMSなどの管理ツールを設定できます。
- **System**: UniSystemのシステム構成および管理オプションを提供します。たとえば、UniSystemのシステム時刻、ネットワーク、バックアップおよびリストアの設定を構成できます。また、UniSystemのユーザーカウントを管理し、UniSystemノードをセカンダリノードとチーム化することでUniSystemクラスタを設定できます。

アプリケーションシナリオ

UniSystemは、企業がリソースをより効果的に管理、監視、更新、クエリーしてデバイス管理を簡素化するのに役立つバルクサーバー管理ツールです。

H3C UniServer B16000 AEモジュールには、UniSystemがプリインストールされています。AEモジュール内に組み込まれたUniSystemは、ローカルエンクロージャーだけでなく、エンクロージャー内のブレードサーバー、ラックサーバー、およびスイッチも管理できます。AEモジュール内のUniSystemは、ハイブリッドITアーキテクチャとクラスターモード管理をサポートします。

対象製品

このマニュアルは、次の製品に適用されます。

- AEモジュール
- H3C UniServer B16000
- H3C UniServer R5500 G7
- H3C UniServer R4330 G7
- H3C UniServer R4930 G7
- H3C UniServer R4970 G7
- H3C UniServer B5700 G6
- H3C UniServer E3300 G6
- H3C UniServer R3950 G6
- H3C UniServer R4300 G6
- H3C UniServer R4500 G6
- H3C UniServer R4700 G6
- H3C UniServer R4700LE G6
- H3C UniServer R4900 G6
- H3C UniServer R4900LE G6 Ultra
- H3C UniServer R4900 G6 Ultra
- H3C UniServer R4950 G6
- H3C UniServer R5350 G6
- H3C UniServer R5300 G6
- H3C UniServer R5500 G6 AMD

- H3C UniServer R5500 G6インテル
- H3C UniServer R6700 G6
- H3C UniServer R6900 G6
- H3C UniServer B5700 G5
- H3C UniServer R4300 G5
- H3C UniServer R4330 G5
- H3C UniServer R4330 G5 H3
- H3C UniServer R4700 G5
- H3C UniServer R4700LC G5
- H3C UniServer R4900 G5
- H3C UniServer R4900LC G5
- H3C UniServer R4930 G5
- H3C UniServer R4930 G5 H3
- H3C UniServer R4930 G5 H3 PKG
- H3C UniServer R4930LC G5 H3
- H3C UniServer R4950 G5
- H3C UniServer R5300 G5
- H3C UniServer R5500 G5
- H3C UniServer R5500LC G5
- H3C UniServer R6900 G5
- H3C UniServer B5700 G3
- H3C UniServer B5800 G3
- H3C UniServer B7800 G3
- H3C UniServer E3200 G3
- H3C UniServer R2700 G3
- H3C UniServer R2900 G3
- H3C UniServer R4300 G3
- H3C UniServer R4360 G3
- H3C UniServer R4500 G3
- H3C UniServer R4700 G3
- H3C UniServer R4900 G3
- H3C UniServer R4950 G3
- H3C UniServer R4960 G3
- H3C UniServer R5300 G3
- H3C UniServer R6700 G3
- H3C UniServer R6900 G3
- H3C UniServer R8900 G3
- H3CユニスターX10828 G5
- H3CユニスターX10516 G6
- H3CユニスターX10529 G6
- H3CユニスターX10536 G6
- H3CユニスターX18000 G6

ガイドライン

カスタム設定オプションまたは機能が含まれている場合、このドキュメントの情報は製品と異なる場合があります。

このドキュメントに記載されているハードウェアオプションのモデル名は、モデル名ラベルと多少異なる場合があります。モデル名ラベルは、一致するサーバーブランドや該当する地域を識別するなどの目的で、ハードウェアコードモデル名に接頭辞または接尾辞を追加する場合があります。たとえば、ストレージコントローラーモデルHBA-1000-M2-1は、接頭辞UN-を持つストレージコントローラーモデルラベルUN-HBA-1000-M2-1を表します。

このドキュメントで使用されているウェブページのスクリーンショットは説明のみを目的としており、お使いの製品とは異なる場合があります。

UniSystemにログインする

UniSystem(非統合O&Mバージョン)へのログイン

UniSystemログインの準備

UniSystemサーバーをネットワークに接続します。

PCまたはサーバー上で実行されているUniSystemにログインするには、UniSystemクライアントとUniSystemサーバーが同じネットワークセグメント上にあることを確認してください。

AEモジュールで実行されているUniSystemにログインするには、最初に次のタスクを実行します。

1. エンクロージャーに少なくとも1つのAEモジュールが取り付けられていることを確認します。

   図2に示すように、エンクロージャーは最大2つのAEモジュールをサポートします。

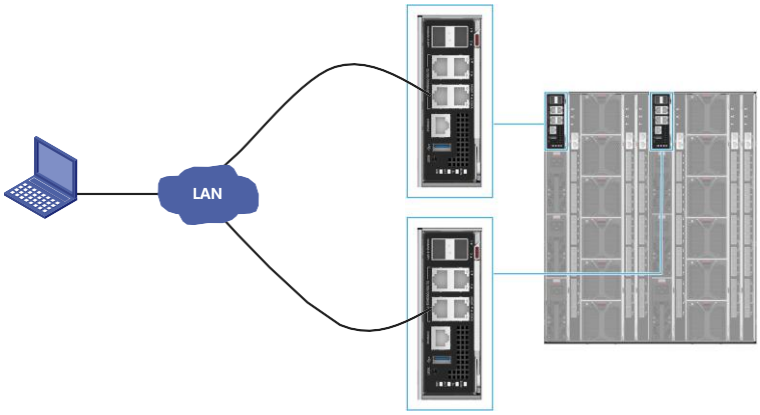
   図2 AEモジュールスロット



スロットE1×1	(2)スロットE2

2. 図3に示すように、UniSystemクライアントホストのイーサネットポートを、LAN経由でプライマリまたはスタンバイOMモジュールのMGMTポートに接続します。

図3 OMモジュールへの接続



3. UniSystemクライアントで、UniSystemサーバーと同じネットワークセグメントに存在するIPアドレスを指定します。UniSystemサーバーのデフォルトIPアドレスについては、図2を参照してください。

UniSystemサーバーIPアドレスを取得する

重要:

デフォルトのIPアドレスを使用してAEモジュールで実行されているUniSystemにログインした後、将来のIPアドレスの競合を回避するためにUniSystem IPアドレスを変更します。UniSystem IPアドレスの変更方法については、「ネットワークポートおよびDNSサーバードレスのIPアドレス取得方法の設定」を参照してください。

表1は、AEモジュールで実行されるUniSystemのデフォルト設定を示しています。

表1 デフォルトのUniSystem設定

パラメータ	UniSystemサーバーの場所	パラメータ値
Username	該当なし	admin
Password		Password@_
UniSystem ログインIPアドレス	AEモジュールスロットE1	192.168.0.100/24
	AEモジュールスロットE2	192.168.0.101/24
	非AE環境	UniSystemが常駐するデバイスのシステムIPアドレス。

UniSystemクライアントの要件

ユーザーは、Webブラウザから直接UniSystemにアクセスできます。サポートされているWebブラウザと推奨される解像度については、表2を参照してください。

表2 クライアントの要件

ブラウザ	解像度
• Google Chrome 80.0以降 • Mozilla Firefox 90.0以降	1600×900以上

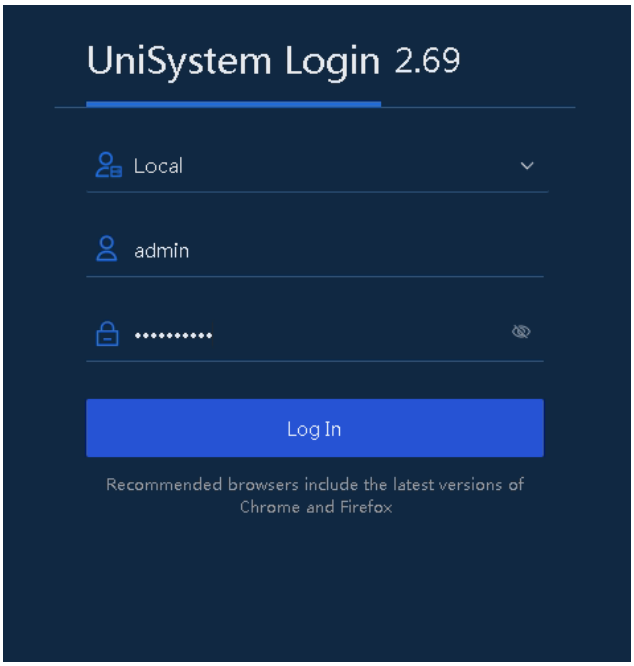
UniSystem Webインターフェイスにログインする

1. ブラウザのアドレスバーに、次のいずれかのURLを入力します。
   - **http**://*UniSystem ip address*:*port*。ここで、portはUniSystemが使用するHTTPポート番号を表します。
   - **https**://*UniSystem ip address*:*port*。ここで、portは、UniSystemが使用するHTTPSポート番号です。

   UniSystemサービスの起動設定で、UniSystemのHTTPポートおよびHTTPSポートを構成できます。詳細は、H3C Servers UniSystem Installation Guideを参照してください。

   または、UniSystemがインストールされているサーバーからUniSystemにローカルにアクセスすることもできます。これを行うには、Webブラウザのアドレスバーに**http://localhost**:*port*または**http://127.0.0.0.1**と入力します。
2. UniSystemログインページで、UniSystemユーザーのユーザー名とパスワードを入力します。

   図4 UniSystemログインページ



3. **Log In**をクリックします。

   ユーザー名またはパスワードが正しくない場合は、その後の試行時にCAPTCHAコードを入力する必要があります。

UniSystem(統合O&Mバージョン)へのログイン

メモ:

この章は、U-CenterプラットフォームにインストールされたUniSystemにのみ適用されます。

ハードウェア環境をセットアップする

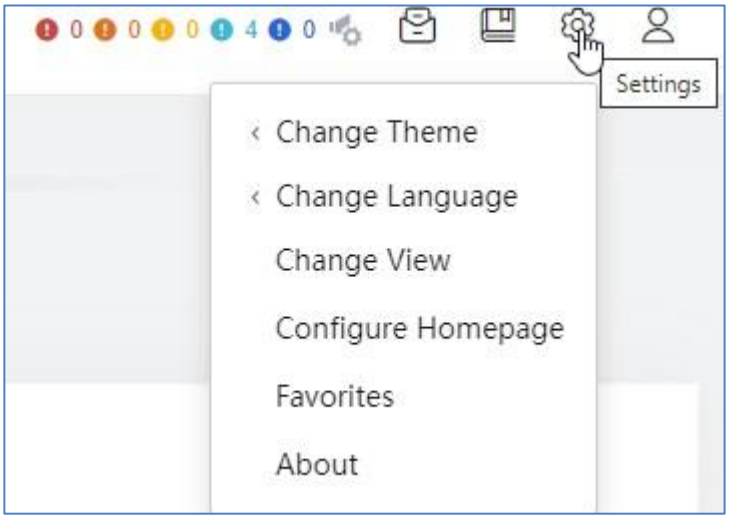
U-Centerプラットフォームには、統一されたO&MバージョンのUniSystemがインストールされています。

詳細については、『H3C U-Center 2.0 Deployment Guide』を参照してください。

UniSystem Webインターフェイスにログインする

1. U-Center 2.0ログインアドレスを**http**://ip_address:portの形式で入力します。ここで、*ip_address*はノースバウンドサービス仮想IPアドレスを表し、portはポータルアプリケーションの展開で設定されたサービスポート番号を表します。
2. ログインページで、ユーザー名とパスワードを入力します。デフォルトのユーザー名は**admin**、デフォルトのパスワードは**Pwd@12345**です。オペレーティングシステムのインストール時にパスワードを設定した場合は、設定したパスワードを使用します。
3. **Log in**をクリックします。
4. 右上隅にあるアイコンをクリックします。ドロップダウンリストで、**Change View**をクリックします。

   図5 ドロップダウンメニュー

5. UniSystemのアイコンをクリックして、UniSystemビューに切り替えます。

図6 ビューの切り替え

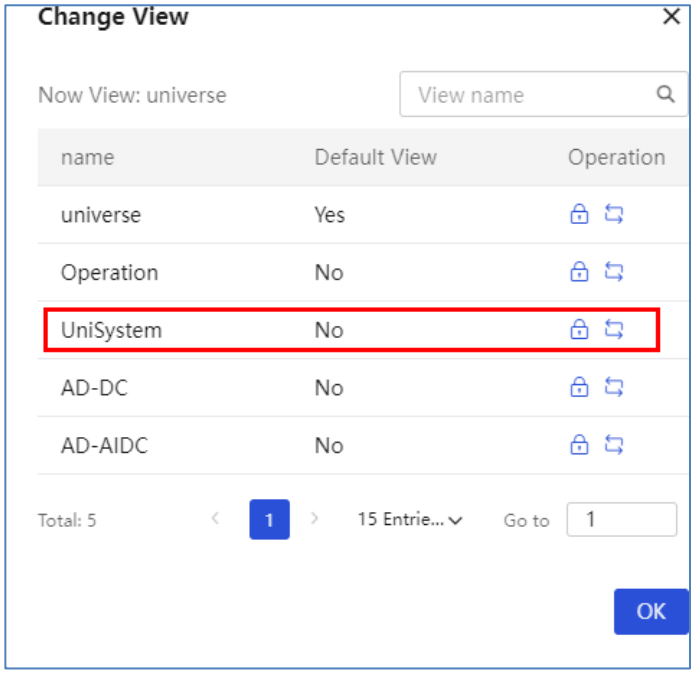
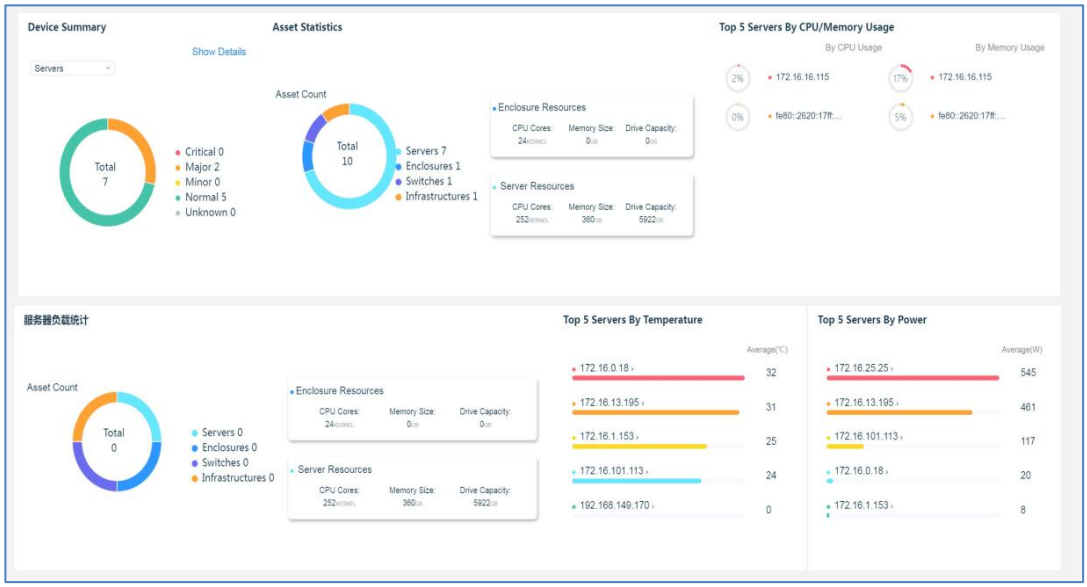


図7に示すように、UniSystemホームページが開きます。

図7 UniSystemホームページ



UniSystem Webインターフェイスのレイアウト

図8に示すように、UniSystem Webインターフェースが開きます。UniSystem Webインターフェースは、表3に示すように、2つの領域に分けることができます。

図8 UniSystemホームページ(非統合O&Mバージョン)

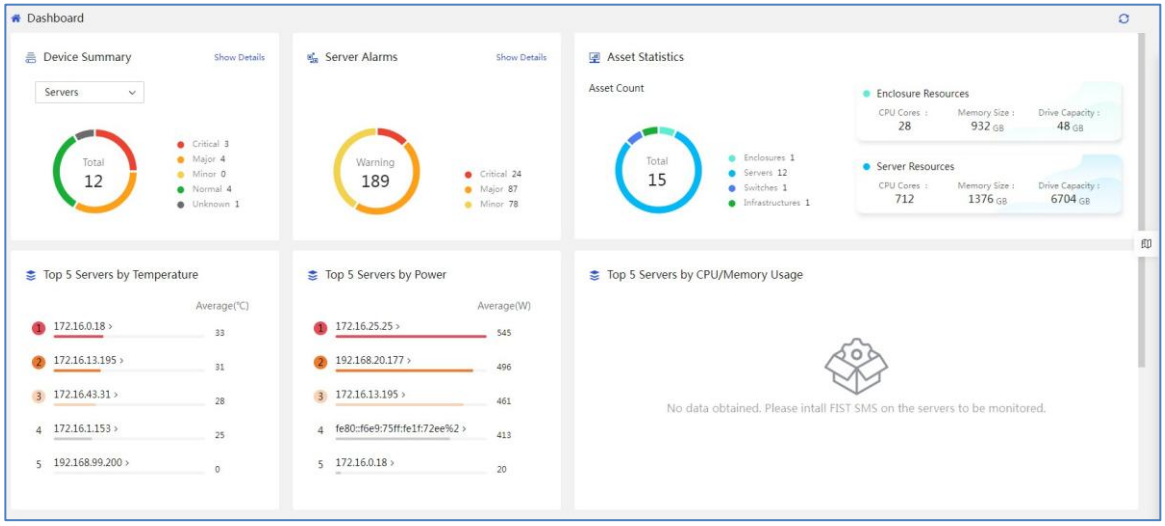


図9 UniSystemホームページ(統合O&Mバージョン)

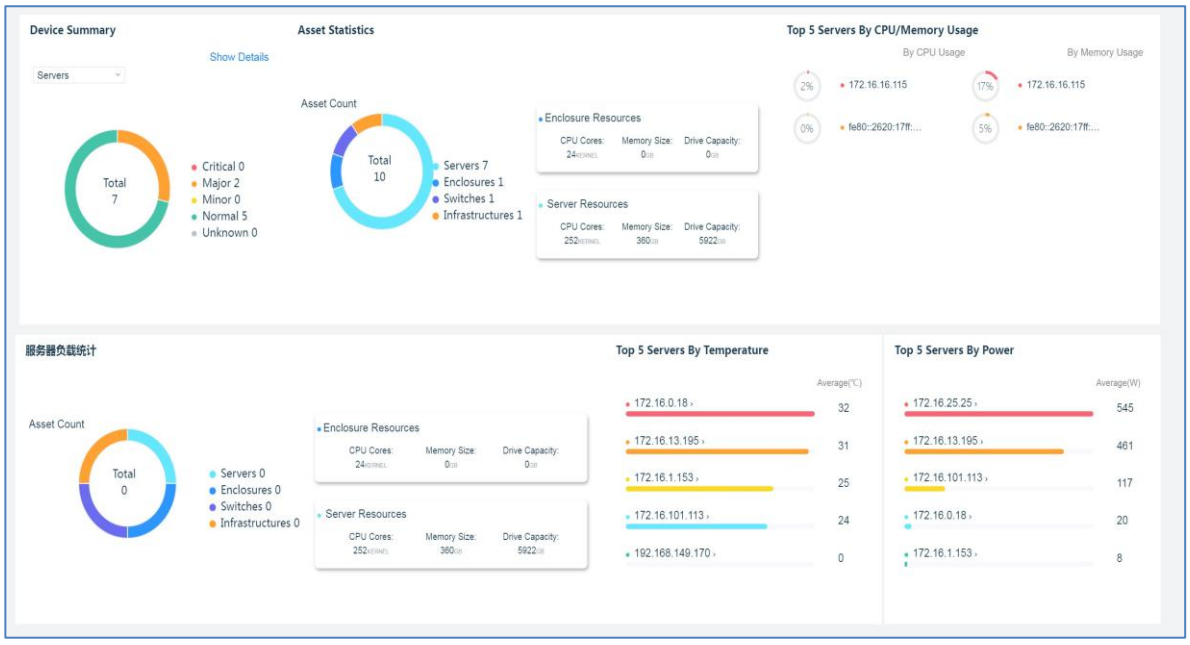


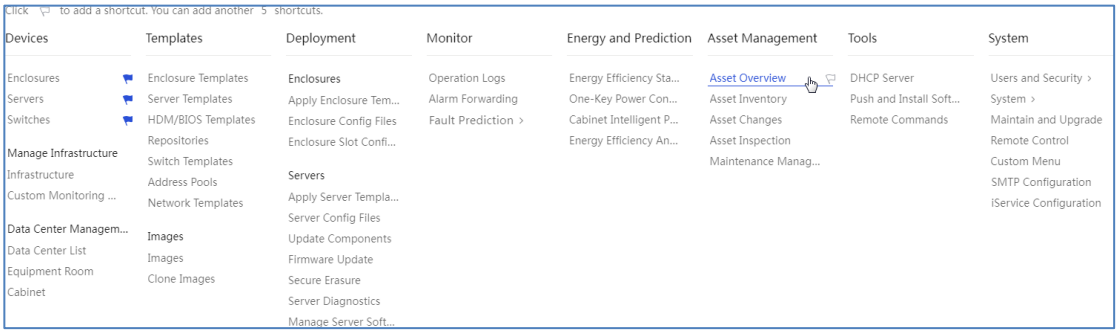
表3 UniSystem Webインターフェイスの設計

エリア	説明
ヘッダーセクション	• -ユーザー名、ユーザーロール、ログイン時間およびIPアドレスを表示します。ローカルユーザーの場合は、パスワードを編集できます。管理者ロールのローカルユーザーの場合は、**View Details**をクリックしてローカルユーザーページにアクセスし、ローカルユーザーを管理できます。 • Search for menu or page -使用可能なオプションを検索してアクセスするには、UniSystemのメニューまたはページの名前を入力します。UniSystemには、ユーザーがすばやくアクセスできるように、よく使用される推奨機能メニューが表示されます。検索ボックスをクリックすると、検索履歴が表示されます。検索履歴をクリアするには、**Clear**をクリックします。 • -クイックアクセスに追加されたメニュー項目を表示します。メニュー項目をクリックして、対応する機能ページにナビゲートします。 • または-CDU5204テンプレートのアラームを除く、サーバーおよびインフラストラクチャデバイスの最新の10個のアラームメッセージを表示します。は、アラーム音声機能が有効であることを示し、は、アラーム音声機能が無効であることを示します。左上隅のアイコンを使用して、リスニングIP、リスニングポート、アラーム音声有効化ステータス、およびアラーム音声トリガーレベルを設定できます。すべてのアラームメッセージを表示するには、**More**をクリックします。 • -オンラインヘルプを表示します。 • -UniSystemのバージョン情報を表示します。 • -表示言語を変更します。 • -テーマを切り替えます。UniSystemは**Light**テーマと**Dark**テーマをサポートしています。デフォルトでは、**Light**テーマが使用されます。 • -フィードバックページにアクセスします。
作業ペイン	操作情報と機能リンクを表示します。
操作ガイド(非統一O&Mバージョン)	主な機能とサービスの構成ガイドを提供します。アイコンをクリックして操作ガイドを開くことができます。デフォルトでは、アイコンはタブにも表示されます。 • **Wizard**: 特定の操作を段階的に説明します。ユーザーが製品の主な機能やサービスを理解して利用するのに役立ち、操作の効率と精度が向上します。 • **Shortcuts**: 特定のページにアクセスするためのショートカットが表示されます。 検索ボックスにキーワードを入力して、ガイド情報をフィルタリングできます。

ショートカットでアクセス

トップナビゲーションバーの**Shortcuts**を使用して、指定したメニューに直接アクセスできます。メニューを**Shortcuts**に追加するには、**Menu**をクリックし、をクリックします。メニューを**Shortcuts**から削除するには、Menuをクリックし、をクリックします。最大15個のメニューを**Shortcuts**に追加できます。

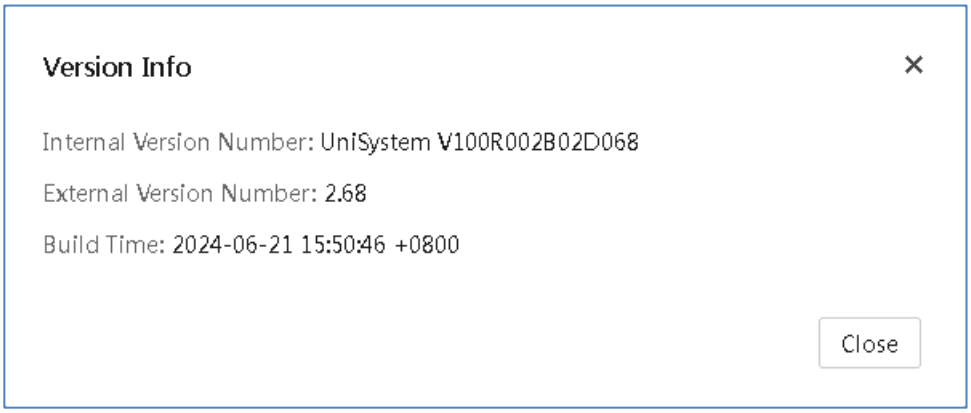
図10 ショートカットへのメニューの追加



UniSystemのバージョン情報の確認

図11に示すように、右上隅にあるバージョン情報ボタンをクリックして、UniSystemのバージョン情報を確認します。

図11 UniSystemのバージョン情報



ユーザーの管理

統合O&Mバージョンの UniSystemでは、ユーザーの管理はサポートされていません。

ユーザーの管理

ローカルユーザーとLDAPユーザーの両方がUniSystemにログインできます。

ローカルユーザーの管理

ユーザーの追加

このタスクについて

新規ユーザーを追加し、ユーザーロールおよびスコープを構成するには、次のタスクを実行します。ユーザーロールおよびドメインの詳細は、「ロール管理」および「スコープマネジメント」を参照してください。

UniSystemには、管理者ロールの**admin**という名前のデフォルトのadminユーザーカウントが用意されています。作成する新規ユーザーの名前は、システムで使用される**System**にはできません。

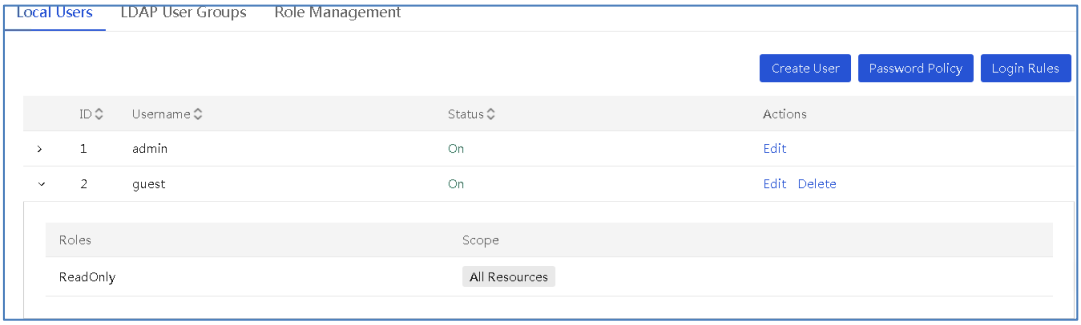
同じadminユーザーカウントでの同時ログインがサポートされ、各ログインは個別のユーザーとしてカウントされます。UniSystemは、最大30人の同時オンラインユーザーをサポートします。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **User List**.を選択します。

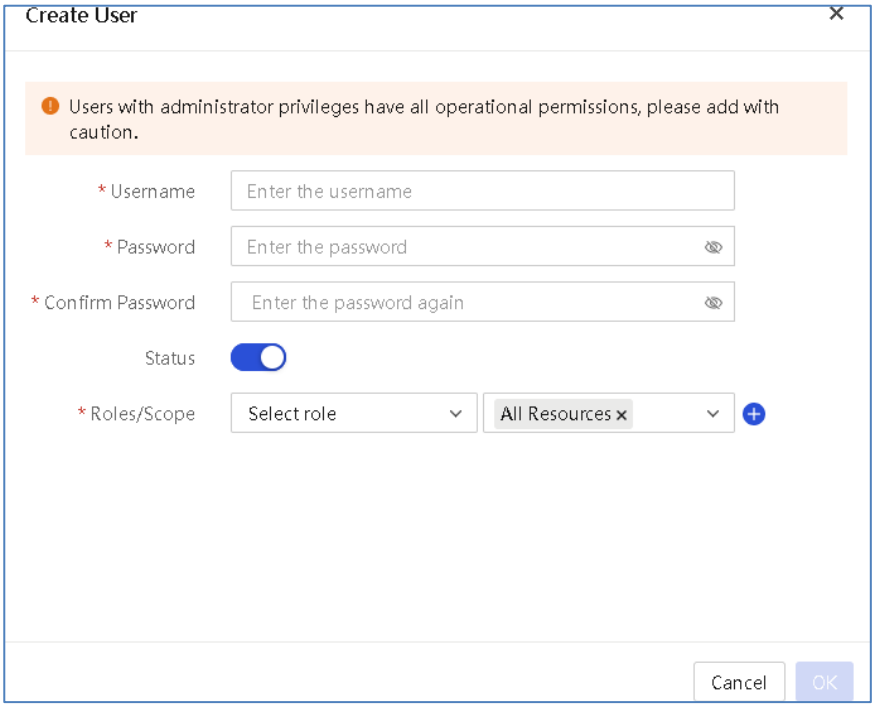
   Usersページにすべてのユーザーが表示されます。

   図12 Usersページ



2. **Local Users**タブで、**Create User**vをクリックします。**Create User**ダイアログボックスで、次の手順を実行します。
   - ユーザー名を入力します。
   - パスワードを入力して確認します。
   - ロールとスコープを選択します。**All Resources**の値は、システム内のすべてのリソースを表します。これは、ユーザーがすべてのリソースを管理でき、スコープによる制限を受けないことを示します。
   - ロールと範囲セットを追加するには、⊕をクリックします。1人のユーザーに最大15個のロールを追加し、各ロールに最大20個の範囲をバインドできます。

図13 ユーザーの作成



3. **OK**をクリックします。

ユーザーの編集

このタスクについて

編集可能なユーザー情報は、ユーザーロールによって異なります。

- 管理者ロールを持つユーザーの場合:
  - ユーザーがすべてのリソースに対する権限を持っている場合は、次の操作を実行できます。
    - デフォルトユーザー**admin**のパスワードを変更します。
    - パスワード、イネーブルステータス、ロール、スコープなどのユーザーパラメータを変更します。
  - ユーザーがすべてのリソースに対するアクセス許可を持っていない場合、ユーザーは自分のパスワードのみを編集できます。
- 管理者以外の役割を持つユーザーは、自分のパスワードのみを変更できます。

制約事項とガイドライン

- ユーザーのパスワードは、パスワードポリシーのすべての要件を満たす必要があります。
- オンラインユーザーを編集すると、そのユーザーは強制的にログアウトされます。新しい設定は、ユーザーが次にログインしたときに有効になります。

手順

デフォルトユーザーのパスワードを変更するには、次のようにします。

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、デフォルトユーザー**admin**のActionsカラムにある**Edit**をクリックします。
3. 表示されたダイアログボックスで、現在のパスワードを入力し、新しいパスワードを入力して確認します。
4. **OK**をクリックします。

デフォルト以外のユーザーを編集するには、次の手順に従います。

5. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
6. **Local Users**タブで、既定以外のユーザーの**Actions**列の**Edit**をクリックします。
7. 表示されるダイアログボックスで、次の操作を実行します。
   - パスワードを変更します。**Change Password**を選択します。次に、現在のパスワードを入力し、新しいパスワードとパスワードの確認を入力します。
   - ユーザーのステータスを変更します。
   - 対応するフィールドから新しいロールまたはスコープを選択します。ロールおよびスコープセットを追加するには、をクリックします。ロールおよびスコープセットを削除するには、をクリックします。1人のユーザーに最大15個のロールを設定し、1つのロールに最大20個のスコープをバインドできます。
8. **OK**をクリックします。

ユーザーを削除する

このタスクについて

デフォルト以外のユーザーを削除するには、次の作業を実行します。

制約事項とガイドライン

- 管理者ユーザーのみがユーザーを削除できます。
- デフォルトのユーザー**admin**は削除できません。
- オンラインユーザーを削除すると、そのユーザー(削除操作を実行している現在のユーザーを含む)は強制的にログアウトされます。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、削除するユーザーの**Actions**列の**Delete**をクリックします。
3. 表示されるダイアログボックスで、現在のログインユーザーのパスワードを入力します。
4. **OK**をクリックします。

パスワードポリシーの構成

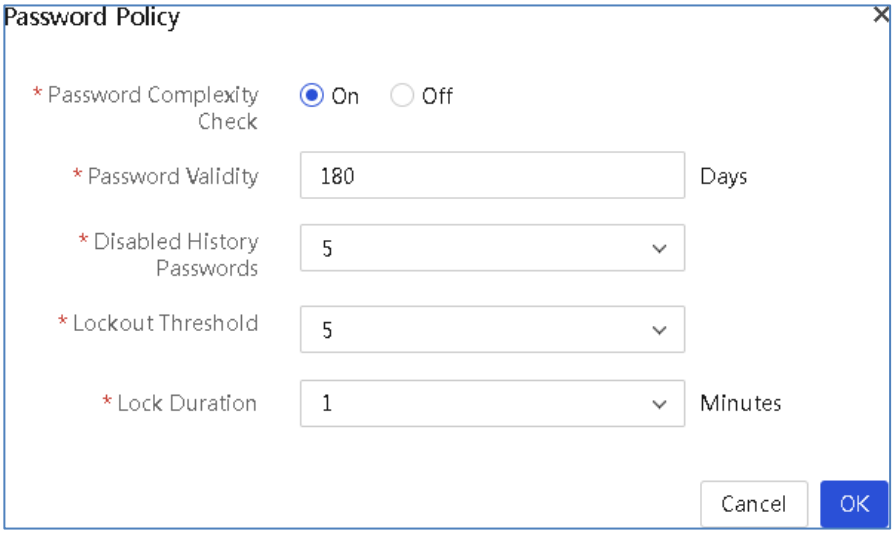
このタスクについて

このタスクを実行して、ユーザーカウント(デフォルトユーザーadminを含む)のパスワードが従う必要があるルールを設定することにより、UniSystemアクセスセキュリティーを強化します。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、**Password Policy**をクリックします。
3. **Password Policy**ダイアログボックスで、次の手順を実行します。
   - パスワードの複雑度チェックを有効または無効にします。
   - パスワードの有効性を設定します。
   - 無効にする履歴パスワードの数を選択します。
   - パスワードロックアウトのしきい値を選択します。
   - パスワードロックアウトの期間を選択します。

図14 パスワードポリシーダイアログボックス



4. OKをクリックします。

パラメータ

- **Password Complexity Check**: パスワードの複雑度チェックをディセーブルまたはイネーブルにします。
  - この機能が有効になっている場合、パスワードは次の高度な複雑さの要件を満たす必要があります。
    - 長さは8～20文字です。
    - 大文字と小文字を区別します。有効な文字は、文字、数字、スペース、および次の特殊文字です:`~!@#$%^&*()_+-=\{};':",./<>?
    - 大文字、小文字、数字の少なくとも2つのカテゴリの文字が含まれている必要があります。
    - 少なくとも1つのスペースまたは特殊文字が含まれている必要があります。
    - ユーザー名と同一であったり、ユーザー名を逆にしたりしないでください。
  - この機能が無効になっている場合、パスワードは次の基本的な複雑さの要件を満たす必要があります。
    - 1～20文字の長さ。
    - 大文字と小文字を区別します。有効な文字は、文字、数字、スペース、および次の特殊文字です:`~!@#$%^&*()_+-=\{};':",./<>?
- **Password Validity**:パスワードの有効期間。パスワードの有効期限が近づくと、UniSystemはユーザーにパスワードの変更を求めます。
- **Disabled History Passwords**:履歴パスワードを再利用する前にユーザーが作成する必要がある一意のパスワードの数。たとえば、この値を2に設定した場合、ユーザーは履歴パスワードを使用する前に2つの一意のパスワードを作成する必要があります。
- **Lockout Threshold**: ユーザーカウントがロックされるまでの連続ログイン失敗回数。
- **Lock Duration**: ロックされたアカウントが再度使用できるようになるまでの時間。

ログイン規則の管理

このタスクについて

UniSystemログインを制御するログインルールを構成するには、次のタスクを実行します。ユーザーログインの情報がログインルールと一致する場合、ログインは許可されます。ユーザーログインの情報がどのログインルールとも一致しない場合、ログインは拒否されます。デフォルトでは、ログインルールは

構成されず、すべてのログインが許可されます。

制約事項とガイドライン

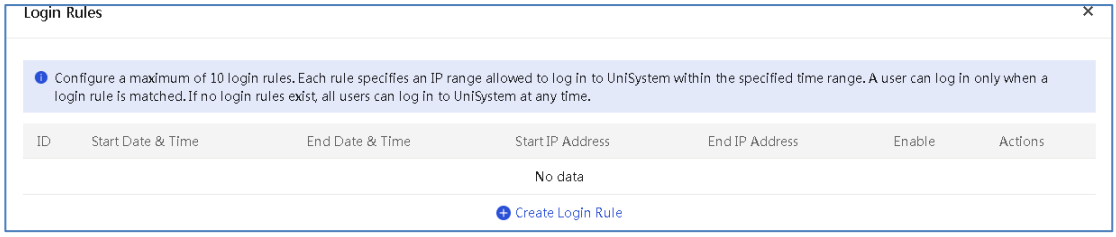
ユーザーがUniSystemにログインできるのは、一致するログイン規則が見つかった場合だけであるため、ログイン規則の設定には注意が必要です。

手順

ログイン規則を作成するには、次の手順に従います。

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、**Login Rules**をクリックします。
3. 表示された**Login Rules**ダイアログボックスで、**Create Login Rule**をクリックし、次の手順を実行します。
   - ユーザーがUniSystemにログインできる時間範囲の開始日時と終了日時を入力します。
   - 開始IPアドレスと終了IPアドレスを入力します。
   - **Enable**カラムのチェックボックスをオンにして、ルールをアクティブにします。

   図15 Login Rulesダイアログボックス



4. OKをクリックします。

ログイン規則を編集するには、次の手順に従います

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、**Login Rules**をクリックします。
3. 表示された**Login Rules**ダイアログボックスで、ログイン規則の設定を編集します。
4. **OK**をクリックします。

ログイン規則を削除するには、次の手順に従います。

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Local Users**タブで、**Login Rules**をクリックします。
3. 表示された**Login Rules**ダイアログボックスで、削除するログイン規則の**Actions**列にある**Delete**をクリックします。
4. **OK**をクリックします。

LDAPユーザーグループの管理

UniSystemに追加されたLDAPユーザーグループのユーザーは、UniSystemに直接ログインできます。LDAPアカウントは、Windows 2000より前のログオン名ではUniSystemにログインできません。

スコープマネジメントユーザーグループを構成する前に、まずスコープを構成します。スコープの詳細は、「LDAPサーバー」を参照してください。

LDAPユーザーグループの追加

このタスクについて

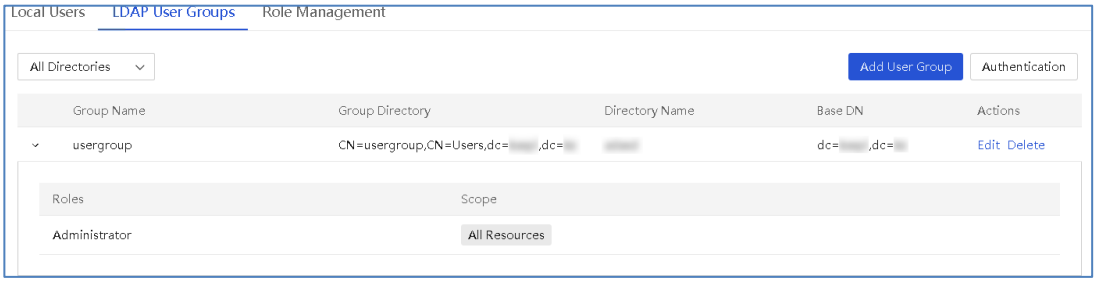
LDAPサーバー上のLDAPユーザーグループをUniSystemに追加するには、次の作業を実行します。UniSystemは、LDAPサーバーごとに最大100のユーザーグループをサポートします。

LDAPユーザーグループをUniSystemに追加する前に、まず、LDAPユーザーグループをホストするLDAPサーバーをUniSystemに追加します。詳細は、「LDAPの管理」を参照してください。

手順

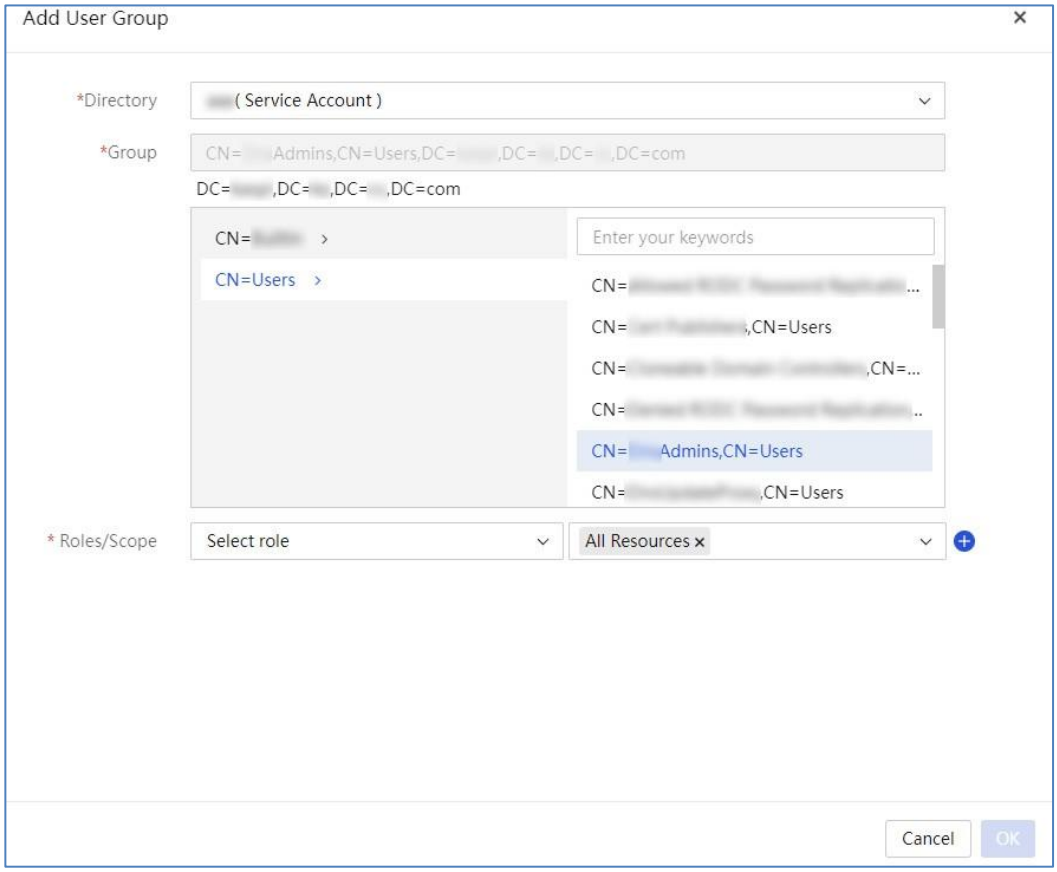
1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **LDAP User Groups**タブをクリックします。

   図16 LDAP user groupsタブ



3. **Add User Group**をクリックします。表示される**Add User Group**ダイアログボックスで、次のパラメータを設定します。
   a. **Directory List**からLDAPサーバーを選択します。
   b. **Group**テキストボックスで、追加するLDAPユーザーグループのディレクトリを選択します。
   c. 対応するフィールドからロールとスコープを選択します。ロールとスコープセットを追加するには、をクリックします。ロールとスコープセットを削除するには、をクリックします。1人のユーザーに最大15個のロールを設定し、1つのロールに最大20個のスコープをバインドできます。

図17 Add user groupダイアログボックス



4. **OK**をクリックします。

LDAPユーザーグループの編集

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **LDAP User Groups**タブをクリックします。
3. ターゲットLDAPユーザーグループの**Actions**カラムで**Edit**アイコンをクリックします。
4. 表示された**Edit User Group**ダイアログボックスで、ユーザーグループ設定を編集し、**OK**をクリックします。

LDAPユーザーグループの削除

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **LDAP User Groups**タブをクリックします。
3. ターゲットLDAPユーザーグループの**Actions**列でDeleteアイコンをクリックします。
4. 表示された確認ダイアログボックスで、**OK**をクリックします。

ユーザー認証の構成

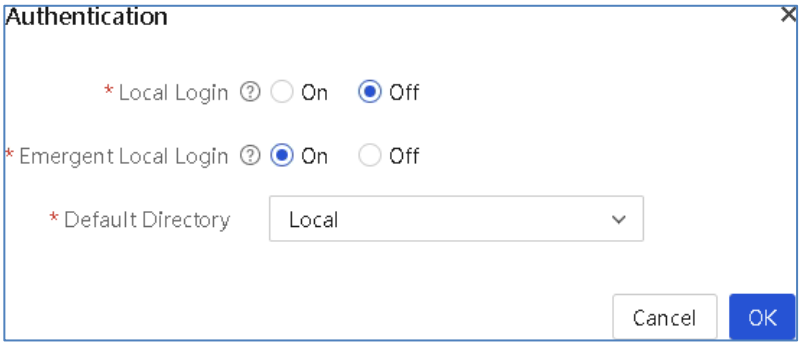
認証機能を使用すると、管理者はローカルユーザーのシステムリソースへのアクセスを制御できます。これにより、許可されたユーザーのみがログインしてリソースにアクセスできるようになり、システムセキュリティが効果的に保護されます。さらに、緊急ローカルログイン機能を使用すると、緊急操作やトラブルシューティングのために緊急の状況で特別なアクセスが提供されます。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。

2. **LDAP User Groups**タブをクリックします。
3. **Authentication**をクリックします。表示されたダイアログボックスで、次のようにユーザー認証を構成します。
   - ローカルログインを有効または無効にします。
   - 緊急ローカルログインを有効または無効にします。このフィールドは、ローカルログインが無効になっている場合に使用できます。
   - デフォルトのディレクトリを設定します。
4. **OK**をクリックします。

図18 ユーザー認証



パラメータ

- **Local Login**: ローカルログインを有効または無効にします。
- **Emergency Local Login**: 緊急ローカルログインを有効または無効にします。このフィールドは、ローカルログインが無効な場合に使用できます。この機能を有効にすると、システムのデフォルトユーザーadminのみがローカルログインを実行できます。この機能を無効にすると、すべてのローカルユーザーログインが禁止されます。
- **Default Directory**: デフォルトのログインディレクトリを選択します。デフォルトでは、ローカルディレクトリが使用されます。
  ローカルログインと緊急ローカルログインの両方が無効になっている場合は、ローカルディレクトリを選択できません。システムに追加されたLDAPサーバーをデフォルトディレクトリとして選択できます。LDAPサーバー構成の詳細は、「LDAPの管理」を参照してください。

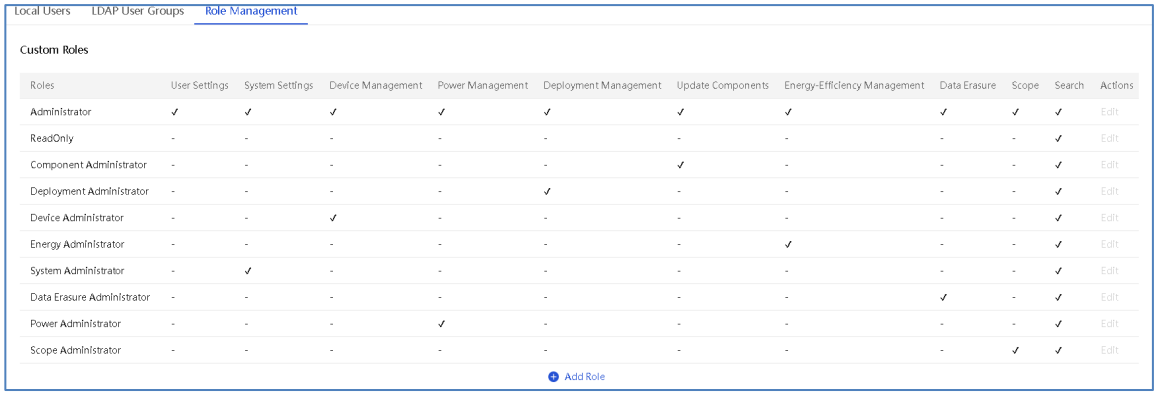
制約事項とガイドライン

ローカルログインを無効にした後、adminアカウントを使用して緊急ログインを実行できます。緊急ローカルログインを無効にすると、ディレクトリサービスにアクセスできない場合に、すべてのユーザーがデバイスにアクセスできなくなる可能性があります。この操作は、不要なアクセス制限やセキュリティリスクを回避するために注意して実行してください。

ロール管理

UniSystemには、Administrator、ReadOnly、Component Administrator、Deployment Administrator、Device Administrator、Energy Administrator、System Administrator、Data Erasure Administrator、Power Administrator、およびScope Administratorのデフォルトロールが用意されています。

図19 ロール管理



さらに、UniSystemは、ロール名や権限モジュールなどのカスタムロールをサポートしています。各権限モジュールの説明を次の表に示します。

メモ:

- UniSystemでサポートされる機能は、環境によって異なる場合があります。具体的な違いについては、実際のインターフェイスの表示を参照してください。
- UniSystem Webインタフェースに表示されるメニューは、ユーザーの役割と権限によって異なります。

表4許可モジュールの説明

Permissionモジュール	権限の詳細
ユーザー構成	ユーザー管理、LDAP管理、およびオンラインユーザー
システム設定	ネットワーク設定、プロキシ設定、時間設定、メンテナンスと更新、ログインセキュリティ、リモートサポート、クラスタ管理、カスタムメニュー、SMTP、およびiService
デバイス管理	シャーシ、シャーシトポロジ、サーバー、スイッチ、インフラストラクチャ、カスタム監視テンプレート、データセンター、機器室、キャビネット、資産概要、資産インベントリ、資産変更、資産検査、保守管理、およびアラーム転送
電源操作の実行	組み込まれているすべてのデバイスの電源管理操作
導入管理	シャーシ構成テンプレート、シャーシ構成テンプレートアプリケーション、サーバー構成テンプレート、サーバー構成テンプレートアプリケーション、HDM/BIOS構成テンプレート、スイッチ構成テンプレート、シャーシ構成ファイル、シャーシスロット構成ファイル、サーバー構成ファイル、アドレスプール、ネットワークテンプレート、イメージクローニング、ディスクレスブート、DHCPサーバー、ソフトウェアプッシュインストール、PXE、イメージ管理(リポジトリへの同期を除く)、サーバーソフトウェアライセンス管理
コンポーネントの更新	REPO、コンポーネントの更新、ファームウェアの更新、およびイメージ管理
エネルギー効率管理	エネルギー効率の統計、ワンクリックでの緊急消費電力、キャビネットのインテリジェントな電源管理、およびエネルギー効率の分析
データ消去	安全なデータ消去
範囲	範囲
検索	すべてのシステムページの表示権限、操作ログ(表示、リセット、およびエクスポート)、自分のパスワードの変更、およびメニュー(ショートカットの追加)

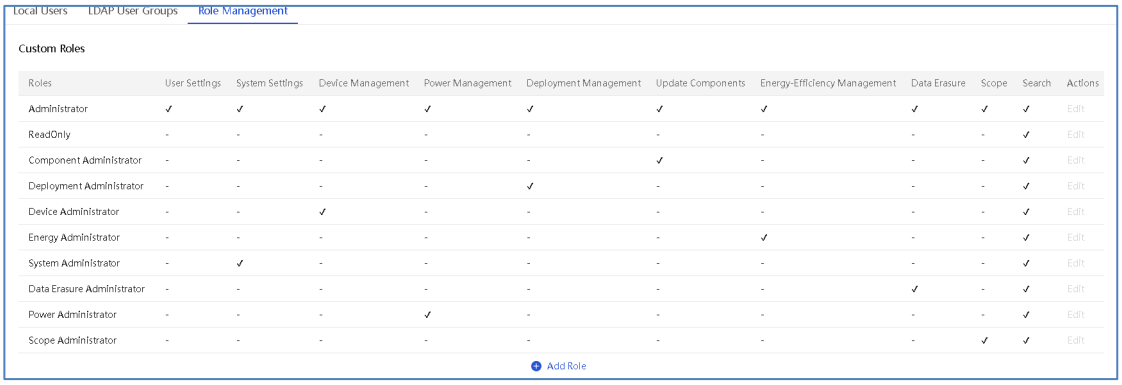
ロールの追加

UniSystemでは、デフォルトのロールを含めて最大15個のロールの追加がサポートされています。管理者ロールを持つユーザーのみがロールを構成できます。

手順

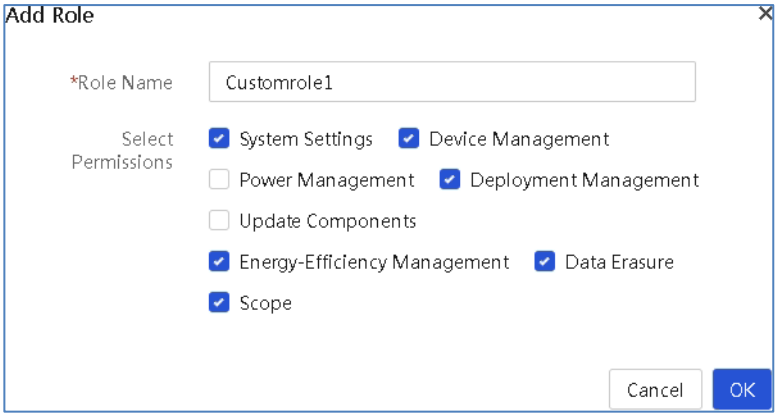
1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Role Management**タブをクリックします。

図20 ロール管理



3. **Add Role**をクリックします。開いたダイアログボックスで、ロールの名前を入力し、権限を選択します。

図21 ロールの追加



4. **OK**をクリックします。パラメータ

- **Role Name**:作成するロールの名前。大文字と小文字を区別し、1から32文字の文字列で指定します。
  文字、数字、ドット(.)、ハイフン(-)、アンダースコア(_)およびアットマーク(@)がサポートされています。文字列の先頭または末尾にスペースを使用することはできません。また、文字列をNULLにすることもできません。
- **Select Permissions**: システム設定、デバイス管理、電源管理、導入管理、コンポーネントの更新、エネルギー効率管理、データ消去、範囲などの権限モジュールを選択します。

ロールの編集

作成したロールを編集するには、次のタスクを実行します。ロールを編集できるのは、管理者ロールを持つユーザーのみです。

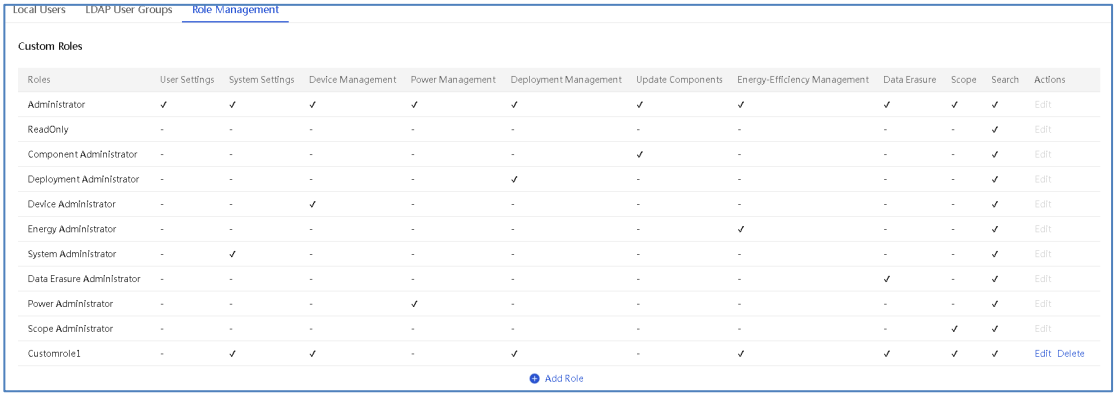
制約事項とガイドライン

- デフォルトのロールは編集できません。
- ロールにバインドされたユーザーが存在し、そのユーザーがセッション中である場合、編集操作が失敗したことを示すメッセージが表示されます。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Role Management**タブをクリックします。

図22 ロール管理



3. ターゲットロールの**Actions**列で**Edit**をクリックします。表示されるダイアログボックスで、ロールの名前を入力し、権限を選択します。
4. **OK**をクリックします。

ロールを削除する

作成したロールを削除するには、次のタスクを実行します。ロールを削除できるのは、管理者ロールを持つユーザーのみです。

制約事項とガイドライン

デフォルトのロール、またはユーザーにバインドされているロールは削除できません。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>User List**の順に選択します。
2. **Role Management**タブをクリックします。
3. ターゲットロールの**Actions**列で**Delete**をクリックします。表示された確認ダイアログボックスで、**OK**をクリックします。

オンラインユーザー情報の表示

このタスクについて

すべてのオンラインユーザーに関する情報を表示するには、次の作業を実行します。

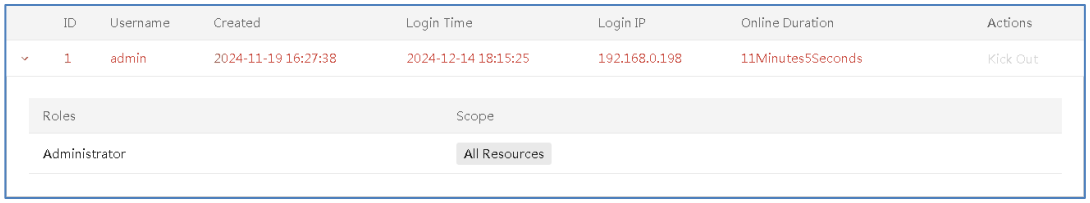
制約事項とガイドライン

ユーザーがUniSystem Webインターフェイスで**Log Out**をクリックせずにUniSystemを終了した場合、タイムアウトタイマーが期限切れになるまで、そのユーザーはオンラインユーザーリストから削除されません。

手順

1. ナビゲーションペインで、**Menu>System>Users and Security>Online Users**を選択します。オンラインユーザーリストには、UniSystemのすべてのオンラインユーザーが表示されます。
2. オンラインユーザーに関する情報を表示します。
3. オンラインユーザーをキックアウトするには、そのユーザーの**Actions**列にある**Kick Out**リンクをクリックします。オンラインユーザーをキックアウトできるのは、管理者ロールを持つユーザーのみです。
4. >ターゲットユーザーのアイコンを選択すると、そのユーザーのロールとスコープに関する情報が表示されます。

図23 Online Usersページ



パラメータ

- **Username**:オンラインユーザーの名前。
- **Created**:ユーザーが作成された時刻。
- **Login Time**:ユーザーが最後にUniSystemにログインした時刻。
- **Login IP**:ユーザーがUniSystemにログインするために使用するIPアドレス。
- **Online Duration**:ユーザーがUniSystemにログインしてから経過した時間。
- **Roles**:ユーザーのロール。
- **Scop**:ユーザーの管理有効範囲。

デバイスの管理

UniSystemは、エンクロージャー、サーバー、スイッチからインフラストラクチャおよびデータセンター全体までの統合管理をカバーする、包括的で柔軟なデバイス管理機能を提供します。これにより、さまざまな種類の機器の効率的な調整と管理が可能になります。

- 一元管理

  統一されたプラットフォームを通じてさまざまなデバイスを一元管理することで、運用プロセスが簡素化され、全体的な管理効率が向上します。

- 洗練されたスコープマネジメント

  部門または地域に基づく多次元の範囲分割をサポートし、デバイスをそれらの範囲内のリソースとして分類します。ユーザーは、割り当てられた役割と範囲に従って、承認されたリソースのみにアクセスして管理できるため、セキュリティとリソース制御が強化されます。

メモ:

- スコープに基づいてデバイスを管理するには、最初にスコープを構成する必要があります。詳細については、「スコープマネジメント」を参照してください。
- すべてのリソースの値は、システム内のすべてのリソースを表します。これは、ユーザーがすべてのリソースを管理でき、範囲による制限を受けないことを示します。現在のユーザーがすべてのリソースを管理できる場合、共有構成はオプションです。

エンクロージャーの管理

エンクロージャーリストメニューから、エンクロージャーとエンクロージャー内のブレードサーバーおよびその他のモジュールを管理できます。

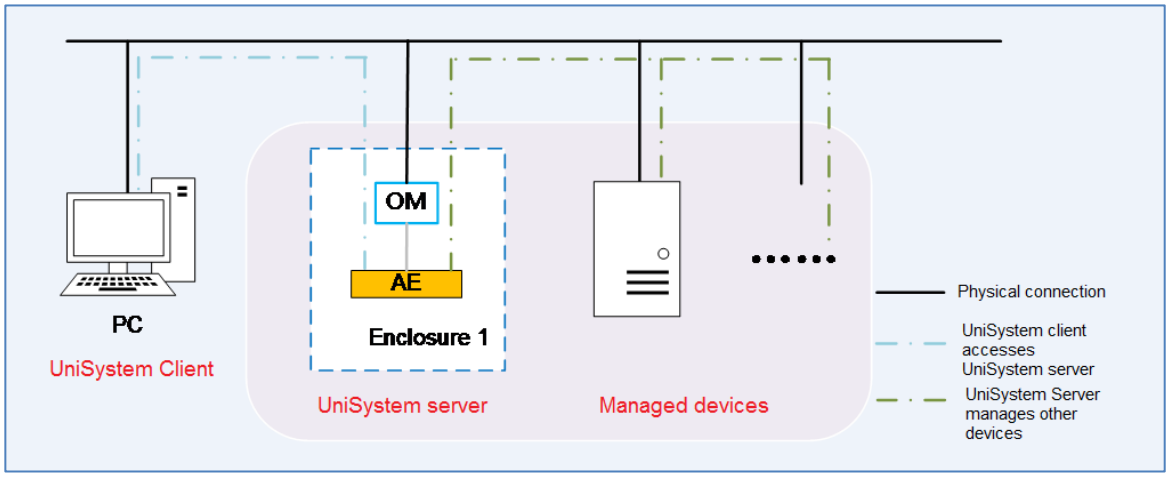
一般的な制限事項とガイドライン

UniSystemは、HTTPを介してエンクロージャーのOMモジュールと通信し、エンクロージャーを管理します。UniSystemがエンクロージャーを正しく管理するには、OM Webインターフェイスで HTTPサービスを無効にしないでください。

エンクロージャーの管理

図24に示すように、AEモジュールはUniSystemがプリインストールされた状態で出荷されます。UniSystemは、AEモジュールが存在するローカルエンクロージャー、リモートエンクロージャー、ラックサーバー、スイッチなどのデータセンターデバイスの一元管理を提供します。OMモジュールの管理ポートに接続するだけで、AEモジュール上のUniSystemにアクセスできます。OMモジュールは、デフォルトではエンクロージャー内のAEモジュールに接続されています。

図24 UniSystem管理エンクロージャーのネットワーク図



エンクロージャーの追加

このタスクについて

UniSystemにエンクロージャーを追加するには、次のタスクを実行します。追加するエンクロージャーにカスケード接続されたエンクロージャーがある場合、UniSystemは自動的にカスケード接続されたエンクロージャーを追加します。

UniSystemがAEモジュールで実行されている場合、AEモジュールが存在するエンクロージャーはUniSystemに自動的に追加され、削除できません。

エンクロージャーをUniSystemに追加すると、エンクロージャーに取り付けられているすべてのブレードサーバーが自動的にUniSystemに追加されます。ブレードサーバーは、**Menu** > **Devices** > **Servers**で表示できます。

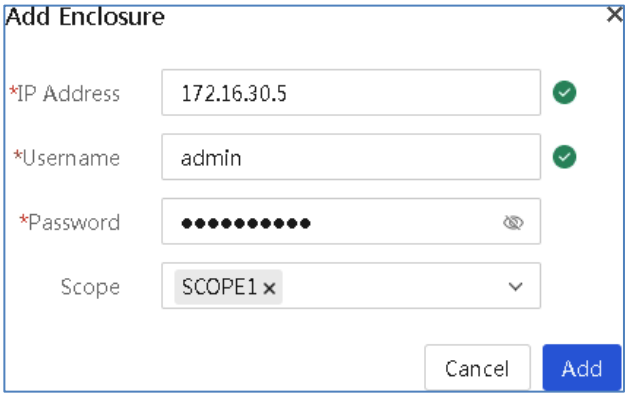
制約事項とガイドライン

追加するエンクロージャーのOM管理アドレスがUniSystemとは異なるサブネット上にある場合は、UniSystemがエンクロージャーと通信できるようにネットワーク設定を構成する必要があります。詳しくは、「ネットワークポートおよびDNSサーバードレスのIPアドレス取得方法の設定」を参照してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. **Add Enclosure**をクリックします。
3. 表示されるダイアログボックスで、次のタスクを実行してエンクロージャーを追加します。
   a. エンクロージャーのマネジメントポートのIPアドレスを入力します。
   b. エンクロージャーのOMモジュールへのログインに使用するユーザー名を入力します。指定したユーザーが管理者ロールを持っていることを確認してください。
   c. エンクロージャーのOMモジュールへのログインに使用するパスワードを入力します。
   d. エンクロージャーのスコープを選択します。
4. **OK**をクリックします。

図25 エンクロージャーの追加



エンクロージャーを削除する

このタスクについて

エンクロージャーを削除するには、次の作業を実行します。

制約事項とガイドライン

UniSystemがAEモジュールで実行されている場合、AEモジュールが存在するエンクロージャーは削除できません。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. 削除するエンクロージャーの**Actions**列で**Delete**をクリックします。
3. 表示された確認ダイアログボックスで、OKをクリックします。

エンクロージャー情報の表示

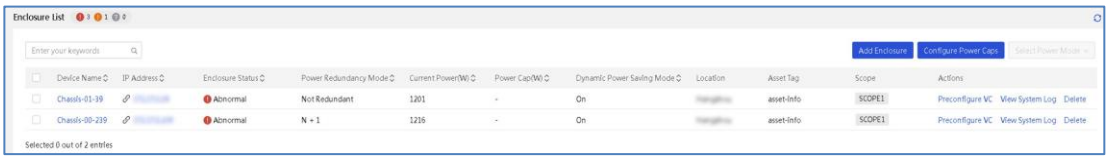
このタスクについて

エンクロージャーリストページにアクセスして、UniSystemが管理するエンクロージャーに関する情報を表示するには、次のタスクを実行します。このページから、ドリルダウンして個々のエンクロージャーの詳細情報を表示することもできます。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。**Enclosures**ページには、すべてのエンクロージャーに関する情報が表示されます。

図26 Enclosuresページ



2. エンクロージャーの名前をクリックして、エンクロージャーの詳細ページを開きます。

図27 エンクロージャーの詳細



エンクロージャーの消費電力上限を設定する

このタスクについて

選択した構成方法に応じて、静的または動的にエンクロージャーの消費電力上限を設定するには、次の作業を実行します。エンクロージャーに設定されている消費電力上限によって、エンクロージャーおよびエンクロージャーに取り付けられているすべてのデバイスが消費できる最大電力量が決まります。

サポートされている消費電力上限の設定方法は次のとおりです。

- **Auto**: 選択したエンクロージャーに消費電力上限を一括して動的に割り当てるように、UniSystemを自動構成します。このモードでは、ターゲットエンクロージャーを選択し、これらのエンクロージャーに割り当てることができる消費電力上限の合計値を設定して、**OK**をクリックします。次に、UniSystemは、選択したすべてのエンクロージャーによって消費される総電力に対するエンクロージャーの割合に応じて、各エンクロージャーに消費電力上限を自動的に割り当てます。つまり、エンクロージャーの現在の電力が高いほど、割り当てられる消費電力上限も高くなります。エンクロージャーに対して計算された消費電力上限が制限(18000 W)を超える場合、エンクロージャーの消費電力上限は18000 Wに設定されます。
- **Manual** - のエンクロージャーの消費電力上限を手動で指定します。

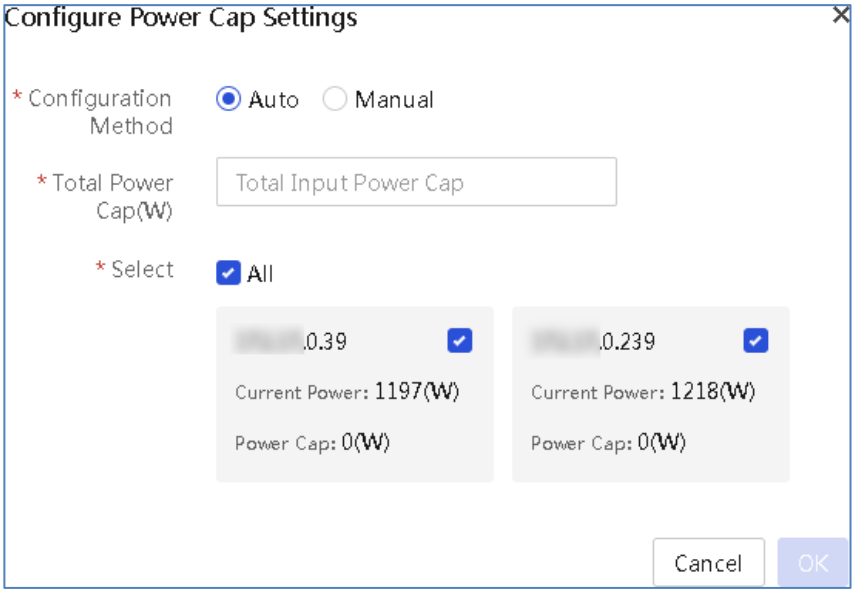
制約事項とガイドライン

- エンクロージャーの消費電力上限は、2500 W～18000 Wの範囲です。
- 使用可能な消費電力上限の合計からN台のエンクロージャーの消費電力上限を動的に設定するには、総消費電力上限を2500 W*N～18000W*Nの範囲で指定します。

手順

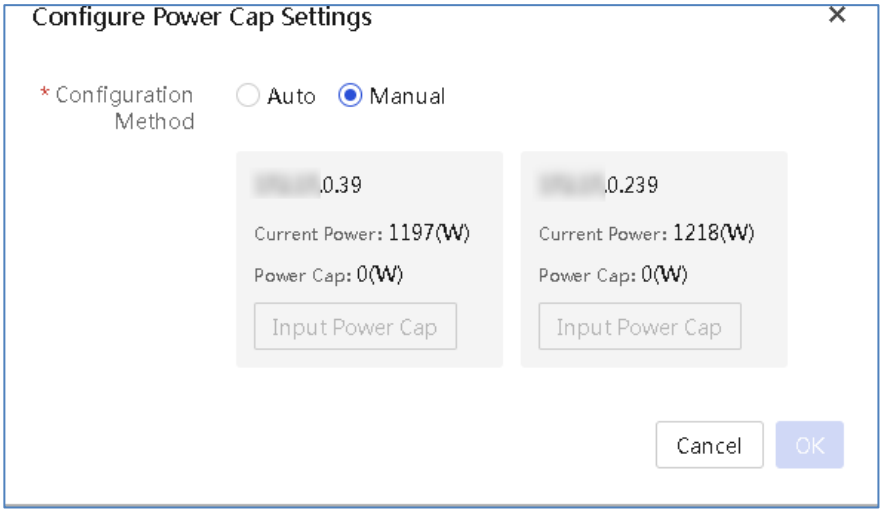
1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. **Configure Power Caps**をクリックします。
3. 構成方法として**Manual**または**Auto**を選択します。
4. UniSystemでエンクロージャーに消費電力上限を動的に割り当てるには、以下の手順に従ってください。
   a. **Configuration Method**で**Auto**を選択します。
   b. ターゲットエンクロージャーを選択します。デフォルトでは、すべてのエンクロージャーが選択されています。
   c. **Total Power Cap (W)**フィールドで、選択したエンクロージャーに割り当てることができる合計消費電力上限の値を指定します。

図28 選択したエンクロージャーに消費電力上限を動的に割り当てるためのUniSystemの設定



5. 個々のエンクロージャーの消費電力上限を手動で設定するには、以下の手順に従ってください。
   a. **Configuration Method**で**Manual**を選択します。
   b. 各エンクロージャーの消費電力上限値を設定します。

図29 エンクロージャーの消費電力上限の手動設定



6. **OK**をクリックします。

エンクロージャーの電源モードを設定する

このタスクについて

エンクロージャーの電源設定を構成するには、次の作業を実行します。

エンクロージャーのパワーサプライシステムには、最大6台のホットスワップ可能なパワーサプライを搭載できます。パワーサプライを取り付け、エンクロージャーの電力要件。エンクロージャーに取り付けられているデバイスの数とタイプによって異なります。

UniSystemは、次の電源管理機能をサポートしています。

- **Power redundancy mode**: パワーサプライの障害からエンクロージャーを保護します。

  UniSystemは、N+1とN+Nの両方の冗長モードをサポートしています。1つ以上の電源に障害が発生した場合、冗長電源が負荷を引き継ぎ、システムの電源が切断されないようにします。システムの電源が切断されるのは、残っている電源にシステムの電源要件を満たすだけの十分な電力がない場合のみです。冗長電源が使用できない場合(No Redundancyモードの場合など)、1つの電源に障害が発生するとシステムの電源が切断されることがあります。

- **Dynamic power saving mode**: 未使用の電源装置を自動的にスタンバイモードにして、エンクロージャーの電源装置の効率を向上させます。これにより、電力需要が少ないときのエンクロージャーの消費電力を最小限に抑えることができます。電力需要が増加すると、スタンバイ電源装置は自動的にフルパフォーマンスに戻ります。

  たとえば、エンクロージャーに6台のパワーサプライが取り付けられ、N+1電源リダンダンシモードで動作するように設定されており、現在の電力を供給するために2台のアクティブなパワーサプライが必要であるとします。

  - ダイナミック省電力モードが有効になっている場合は、3台のパワーサプライのみがエンクロージャーの電力負荷の供給を共有します。1台はリダンダントパワーサプライです。残りの3台のパワーサプライはスタンバイモードになります。
  - ダイナミック省電力モードがディセーブルの場合、6つの電源装置すべてが電力負荷を共有します。

制約事項とガイドライン

- エンクロージャーに取り付けられているすべてのパワーサプライが同じモデルであることを確認してください。表5に、サポートされているパワーサプライに関する情報を示します。

  表5サポートされている電源

タイプ	モデル	定格入力電圧範囲	最大定格出力
3000 W AC電源装置	PSR3000-12A	AC 100 V~AC 240 V	3000 W

- エンクロージャーの電源リダンダンシモードを設定する場合は、エンクロージャーの適切な位置に適切な数のパワーサプライが取り付けられていることを確認してください。

  表6は、3000 W AC電源装置を搭載したエンクロージャーの推奨電源設定を示しています。電源装置の数が推奨数を超える場合は、動的省電力モードを有効にして消費電力を削減します。

  表6 3000 W AC電源装置を搭載したエンクロージャーの推奨電源設定

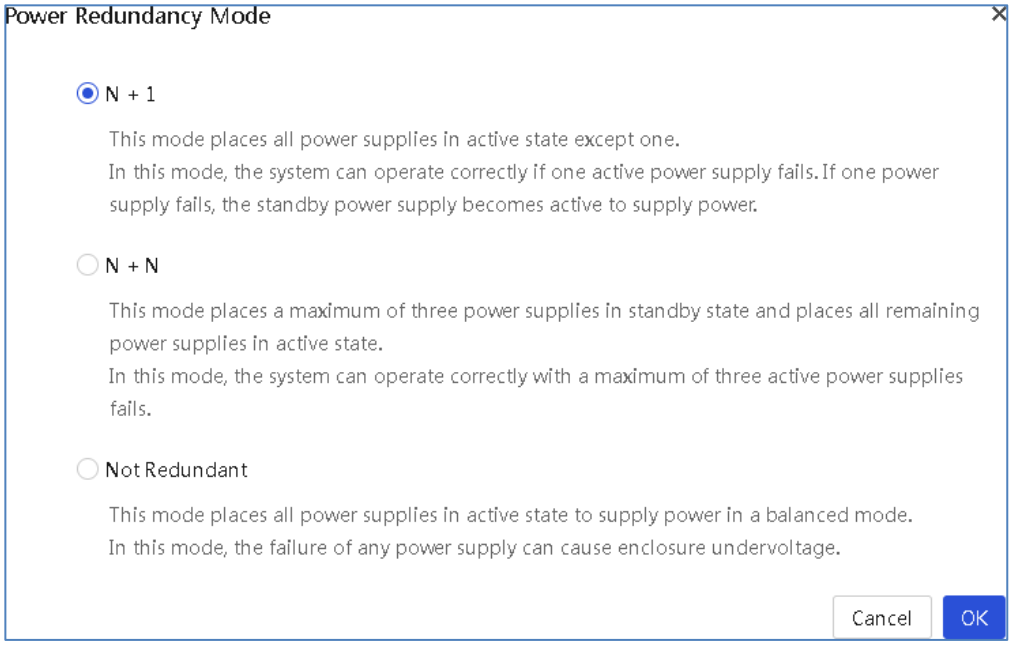
供給可能な最大電力	電源冗長モード	搭載されている電源装置の数	推奨されるパワーサプライベイ
3000 W	冗長性なし	1	PSU_1
6000 W	冗長性なし	2	PSU_1、PSU_2
9000 W	冗長性なし	3	PSU_1、PSU_2、PSU_3
12000 W	冗長性なし	4	PSU_1、PSU_2、PSU_3、PSU_4
15000 W	冗長性なし	5	PSU_1、PSU_2、PSU_3、PSU_4、PSU_5

供給可能な最大電力	電源冗長モード	パワーサプライの数 インストール済み	推奨されるパワーサプライベイ
18000 W	冗長性なし	6	PSU_1、PSU_2、PSU_3、PSU_4、PSU_5、PSU_6
3000 W	1+1冗長性	2	PSU_1、PSU_2
6000 W	2+1冗長性	3	PSU_1、PSU_2、PSU_3
9000 W	3+1冗長性	4	PSU_1、PSU_2、PSU_3、PSU_4
12000 W	4+1冗長性	5	PSU_1、PSU_2、PSU_3、PSU_4、PSU_5
15000 W	5+1冗長性	6	PSU_1、PSU_2、PSU_3、PSU_4、PSU_5、PSU_6
6000 W	2+2冗長性	4	PSU_1、PSU_2、PSU_3、PSU_4
9000 W	3+3冗長性	6	PSU_1、PSU_2、PSU_3、PSU_4、PSU_5、PSU_6

手順

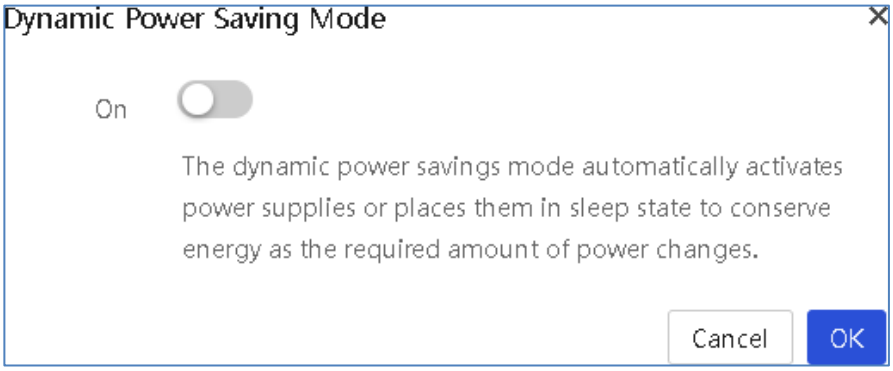
1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの電源**redundancy**モードを設定するには、エンクロージャーを選択して**Select Power Mode**をクリックし、メニューから電源リダンダンシモードを選択します。表示されるダイアログボックスで、必要に応じて**Power Redundancy Mode**を選択し、OKをクリックします。

   図30 電源冗長モードの設定



3. エンクロージャーの動的省電力モードを有効または無効にするには、エンクロージャーを選択して**Select Power Mode**をクリックし、メニューから**Dynamic Power Saving Mode**を選択します。表示されるダイアログボックスで、必要に応じて動的省電力モードを有効または無効にし、**OK**をクリックします。

図31 動的省電力モードの有効化または無効化



OMモジュールの管理

このタスクについて

エンクロージャーの管理コアとして、OMモジュールは、エンクロージャーのバックプレーンを介してエンクロージャー内の他のすべてのモジュールと相互接続され、一元的な管理と監視を提供します。

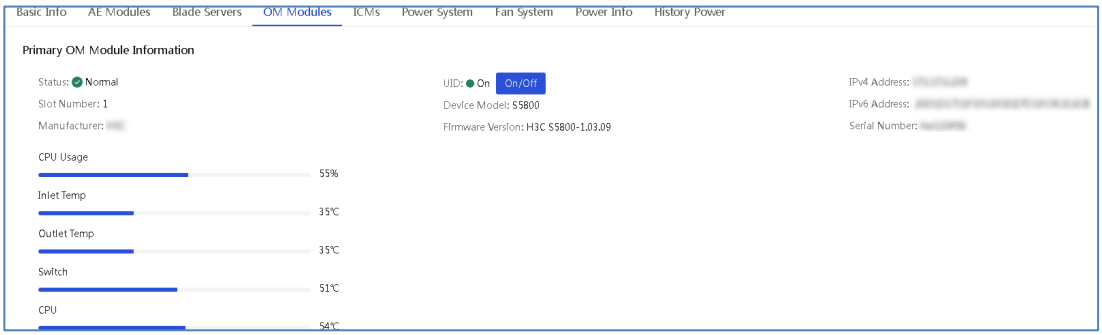
エンクロージャーの詳細ページの**OM Modules**タブには、エンクロージャー内のプライマリおよびセカンダリOMモジュールに関する情報が表示されます。このタブでは、OMモジュールのUID LEDをオンまたはオフにすることができます。UID LEDをオンにすると、エンクロージャーの位置を特定するのに役立ちます。特に、高密度の機器室では有効です。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. **enclosure**の名前をクリックします。
3. **OM Modules**タブをクリックします。

   このタブには、エンクロージャー内のプライマリおよびセカンダリOMモジュールに関する情報が表示されます。
4. (オプション)必要に応じて、UID LEDをオンまたはオフにします。

図32 エンクロージャーのOMモジュール情報の表示



AEモジュールの管理

エンクロージャーの詳細ページの**AE Modules**タブでは、次のタスクを実行できます。

- エンクロージャー内の各AEモジュールに関する基本情報と詳細情報を表示します。
- AEモジュールのUID LEDをオンまたはオフにします。
- AEモジュールの仮想電源を管理します。たとえば、選択した1つ以上のAEモジュールの電源を入れることができます。
- AEモジュールに対してリモートコンソールを起動します。

UniSystemが常駐するAEモジュールでは、基本情報の表示のみが可能です。その他の機能はサポートされていません。

AEモジュール一覧ページにアクセスする

このタスクについて

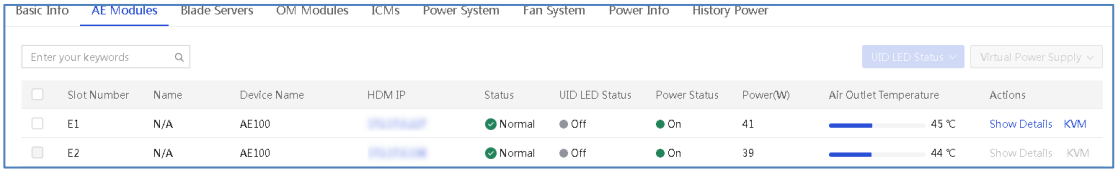
エンクロージャーのAEモジュールリストページにアクセスするには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **AE Modules**タブをクリックします。

   このタブには、エンクロージャー内のすべてのAEモジュールが表示されます。

   図33 エンクロージャーのAEモジュールリストページ



4. 1つまたは複数のAEモジュールのUID LEDの状態を変更するには、AEモジュールを選択し、右上隅にある**UID LED Status**リストから**On**または**Off**を選択します。
5. 1つ以上のAEモジュールの仮想電源の状態を変更するには、AEモジュールを選択し、右上隅にある**Virtual Power Supply**リストから電源オプションを選択します。次に、表示されたダイアログボックスで**OK**をクリックします。

AEモジュールに関する詳細情報の表示

このタスクについて

AEモジュールの詳細ページにアクセスするには、次のタスクを実行します。このページでは、**Basic Info**、**CPU**および**Memory**などの個別のタブにAEモジュールに関する情報が表示されます。

制約事項とガイドライン

UniSystemが常駐するローカルAEモジュールに関する詳細情報は表示できません。

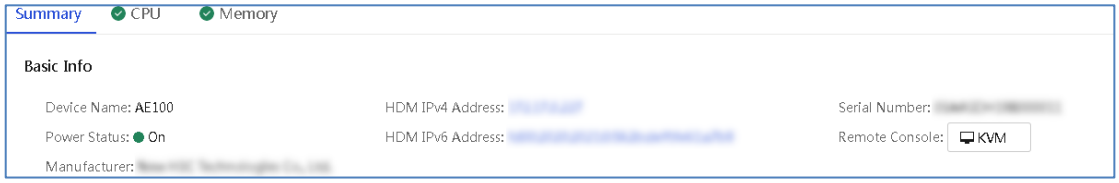
手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **AE Modules**タブをクリックします。

   AEモジュール一覧画面が表示されます。

4. 詳細情報を表示するAEモジュールの**Actions column**で**Show Details**をクリックします。
   AE module detailsページが開き、デフォルトで**Summary**タブが表示されます。
5. AEモジュールのCPU情報を表示するには、**CPU**タブをクリックします。
6. AEモジュールのメモリー**information**を表示するには、**Memory**タブをクリックします。

図34 AEモジュールの詳細ページ



リモートコンソールを起動する

このタスクについて

KVMリモートコンソールからAEモジュールを管理するには、次の作業を実行します。

前提条件

UniSystemからAEモジュールのKVMリモートコンソールを起動する前に、AEモジュールでKVMサービスが有効になっていることを確認します。KVMサービスが有効になっていない場合は、AEモジュールのHDM Webインターフェイスの**Security>Access services**ページでKVMサービスを有効にします。

制約事項とガイドライン

この関数は、UniSystemが常駐するローカルAEモジュールでは使用できません。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. **enclosure**の名前をクリックします。
3. **AE Modules**タブをクリックします。
4. ターゲットAEモジュールの**Actions**列にある**KVM**リンクをクリックします。
5. プロンプトが表示されたら.jnlpファイルを**Download**し、そのファイルを実行してリモートコンソールウィンドウを起動します。

ブレードサーバーの管理

エンクロージャー内のブレードサーバーは、コンピューティングサービスとストレージサービスを提供します。

エンクロージャーの詳細ページの**Blade Servers**タブでは、以下のタスクを実行できます。

- エンクロージャー内のブレードサーバーに関する基本情報と詳細情報を表示します。
- ブレードサーバーのUID LEDを点灯または消灯します。
- ブレードサーバーの仮想電源を管理します。たとえば、ブレードサーバーの電源をオンまたはオフにできます。
- ブレードサーバーのワンタイムブートオプションを設定する
- ブレードサーバーへのリモートコンソールを起動します。

エンクロージャーのブレードサーバーリストページにアクセスする

このタスクについて

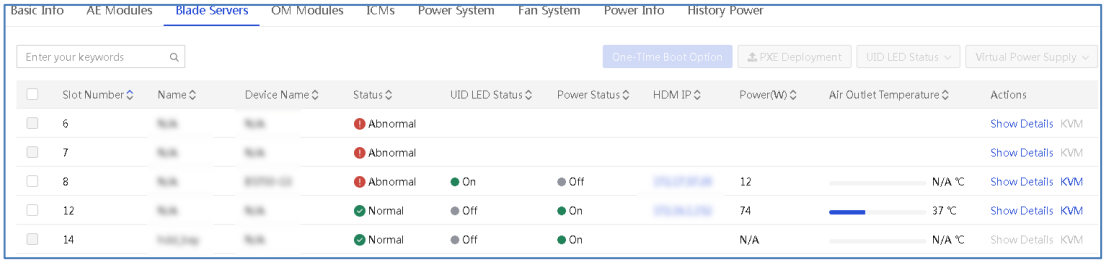
エンクロージャーのブレードサーバーリストページを開くには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **Blade Servers**タブをクリックします。

   このタブには、エンクロージャー内のすべてのブレードサーバーが表示されます。

   図35 エンクロージャーのブレードサーバータブ



4. 1台または複数のブレードサーバーのUID LEDの状態を変更するには、ブレードサーバーを選択し、**UID LED Status**リストから**On**または**Off**を選択します。
5. 1つまたは複数のブレードサーバーの仮想パワーサプライの状態を変更するには、ブレードサーバーを選択し、**Virtual Power Supply**リストから電源オプションを選択します。次に、表示されたダイアログボックスで**OK**をクリックします。
6. ブレードサーバーの詳細情報を表示するには、サーバーの**Actions**列にある**Details**リンクをクリックします。

   このページには、デフォルトでブレードサーバーのサマリー情報が表示されます。必要に応じて、**Summary**、**CPU**、**Memory**および**Node Interconnect**タブをクリックして、サーバーのCPU、メモリーおよびメザニンカード情報を表示します。

   図36 ブレードサーバーの詳細ページ



ブレードサーバーの消費電力上限を設定する

このタスクについて

ブレードサーバーの消費電力上限または消費電力上限割り当ての重みを設定するには、次の作業を実行します。

ブレードサーバーの消費電力上限を設定するには、まずサーバーが搭載されているエンクロージャーの消費電力上限機能を無効にする必要があります。詳しくは、「電力情報の表示」を参照してください。

エンクロージャーの消費電力上限が有効になっている場合は、エンクロージャーに取り付けられている個々のブレードサーバーの消費電力上限割り当ての重みを設定できます。重みが大きいほど、ブレードサーバーは高い消費電力上限値を取得できます。デフォルトの消費電力上限割り当ての重みは、ブレードサーバーのタイプによって異なります。

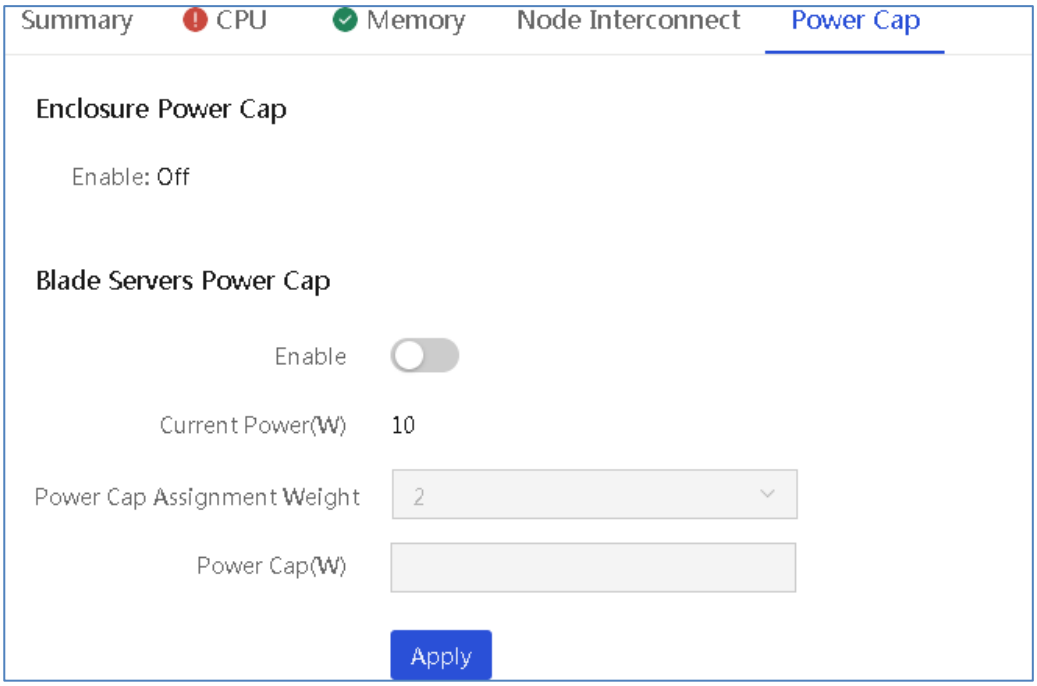
- 2プロセッサーコンピュートブレードサーバーの場合、デフォルト値は2です。

- 2プロセッサーストレージブレードサーバーの場合、デフォルト値は3です。
- 4プロセッサーのコンピュートブレードサーバーの場合、デフォルト値は4です。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックし、**Blade Servers**タブをクリックします。
3. 消費電力上限を設定するブレードサーバーの**Actions**列で、**Show Details**をクリックします。
4. **Power Cap**タブをクリックします。
5. ブレードサーバーの消費電力上限割り当ての重みまたは消費電力上限値を設定します。
   - エンクロージャーの消費電力上限が有効になっている場合は、ブレードサーバーの消費電力上限割り当ての重みを設定します。
   - エンクロージャーの消費電力上限が無効になっている場合は、ブレードサーバーの消費電力上限を有効にして、ブレードサーバーの消費電力上限値を設定します。
6. **Apply**をクリックします。

図37 エンクロージャーの消費電力上限の設定



次回の再起動時のブートオプションを構成する

このタスクについて

次回のリブート時にサーバーが使用するワンタイムブートモードおよびブートデバイスを指定するには、次の作業を実行します。

手順

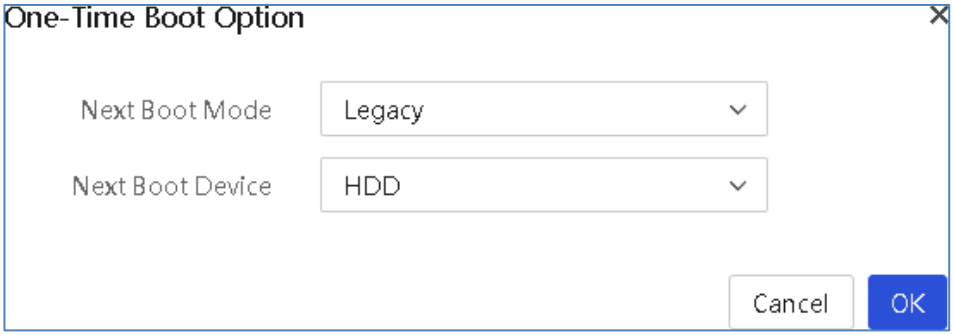
1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **Blade Servers**タブをクリックします。
4. ターゲットサーバーを選択して、**One-Time Boot Option**をクリックします。
5. 必要に応じて、次のパラメータを設定します。
   - **Next Boot Mode**: 次回の再起動時の起動モードを選択します。オプションには、

Legacyと**UEFI**(デフォルト)があります。次回の再起動時にBIOSで設定された起動モードを使用するには、このフィールドを空のままにします。

- **Next Boot Devic**: 次回の再起動時の起動デバイスを選択します。オプションには、**HDD**、**PXE**、**BIOS**、および**CD/DVD**があります。次回の再起動時にBIOS設定を使用するには、このフィールドを空のままにします。

6. **OK**をクリックします。

図38 ワンタイムブートオプションの設定



PXEを使用してオペレーティングシステムをインストールする

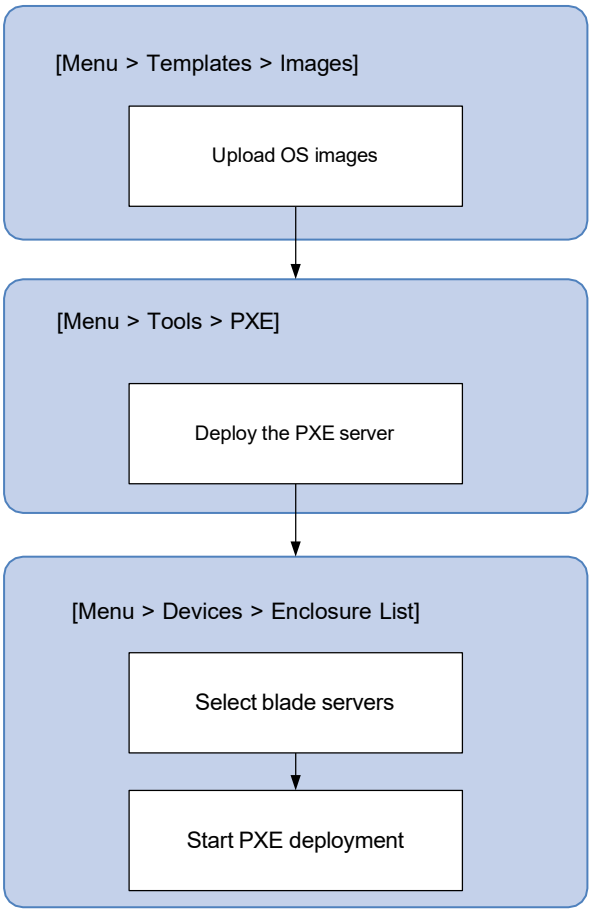
このタスクについて

PXEを使用してブレードサーバーにオペレーティングシステムを一括インストールするには、次の作業を実行します。

PXEを展開する前に、OSイメージをメニュー>テンプレート>イメージの**Menu** > **Templates** > **Images** 一覧にアップロードし、PXEサーバーを有効にします。詳細については、「イメージを管理する」および「PXE展開を構成する」を参照してください。

図39に、PXEデプロイメントプロシージャーを示します。

図39 PXEデプロイメントプロシージャー



制約事項とガイドライン

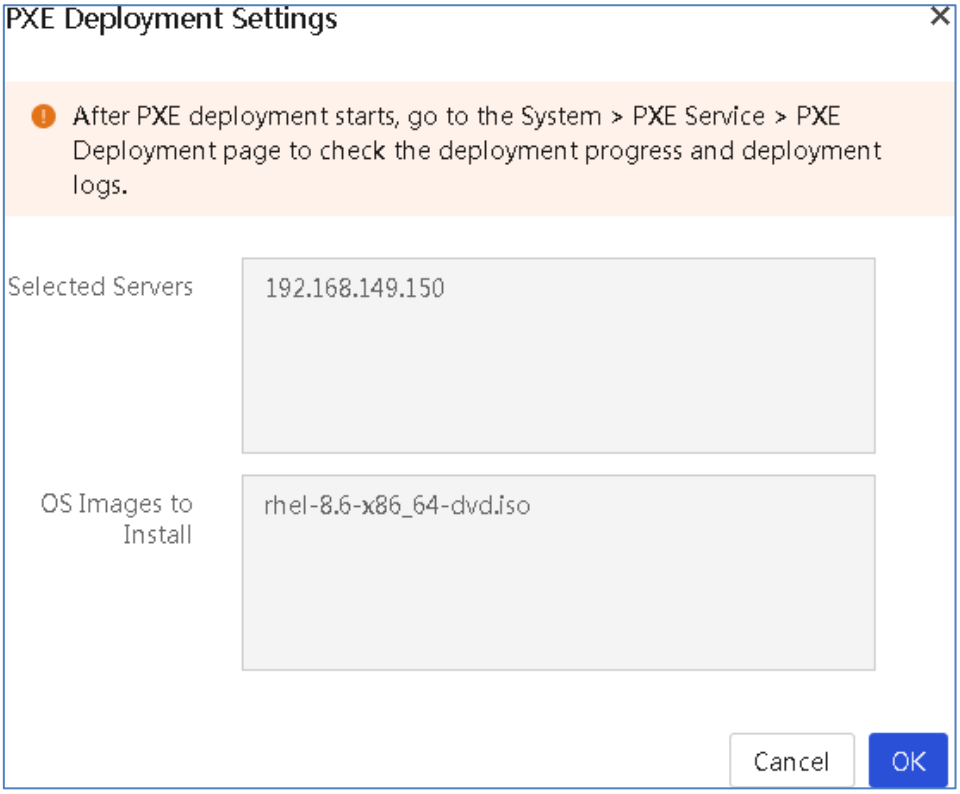
DHCP IPプール内のIPアドレスが、ネットワーク上の既存のIPアドレスと競合していないことを確認します。

オペレーティングシステムのPXEインストール中に使用されるBIOSブートモードが、その後のオペレーティングシステムへのアクセスに使用されるBIOSブートモードと同じであることを確認してください。同じでない場合、その後のオペレーティングシステムへのアクセスが失敗する可能性があります。

この機能によってインストールされたLinux OSのデフォルトのrootパスワードは**123456**です。

2. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
3. エンクロージャーの名前をクリックします。
4. **Blade Servers**タブをクリックします。
5. ターゲットサーバーを選択し、**PXE Deployment**をクリックします。
6. PXEインストールパラメーターを設定し、選択したサーバーでOSのインストールを完了します。

図40 PXEを使用したオペレーティングシステムのインストール



インターコネクトモジュールの表示

このタスクについて

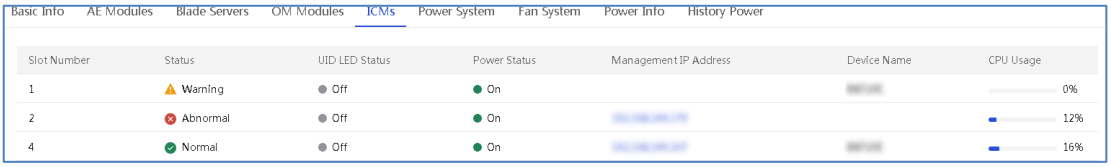
エンクロージャー内のインターコネクトモジュールを表示するには、次の作業を実行します。

インターコネクトモジュールは、エンクロージャー内のデバイスを相互に通信できるように接続します。また、外部デバイスに接続するための外部データインターフェイスも提供します。

手順

1. ナビゲーションペインで、**Menu** > **Devices** > **Enclosures**を選択します。
2. **enclosure**の名前をクリックします。
3. **ICMs**タブをクリックします。

図41 ICMsタブ



電源システム情報の表示

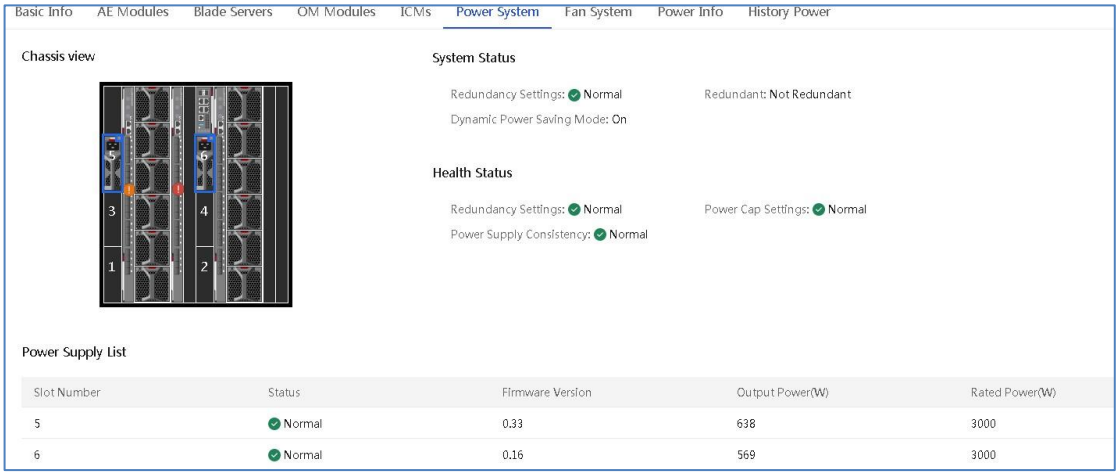
このタスクについて

電源システム情報、ヘルスステータス、電源リストなど、エンクロージャーの電源情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **Power System**タブをクリックします。
   このタブには、エンクロージャー内のパワーサプライに関する情報が表示されます。

   図42 電源システムタブ



ファンシステム情報の表示

このタスクについて

ファンシステム情報、ヘルスステータス、ファンモジュールリストなど、ファンに関する基本情報を表示するには、次の作業を実行します。

ファンシステムは、1台のエンクロージャーで最大12個のファンをサポートし、N+1の冗長性を提供します。1個のファンに障害が発生した場合、残りのファンはフルスピードで動作し続けて放熱を確保し、ファンシステムは通常の状態を維持します。

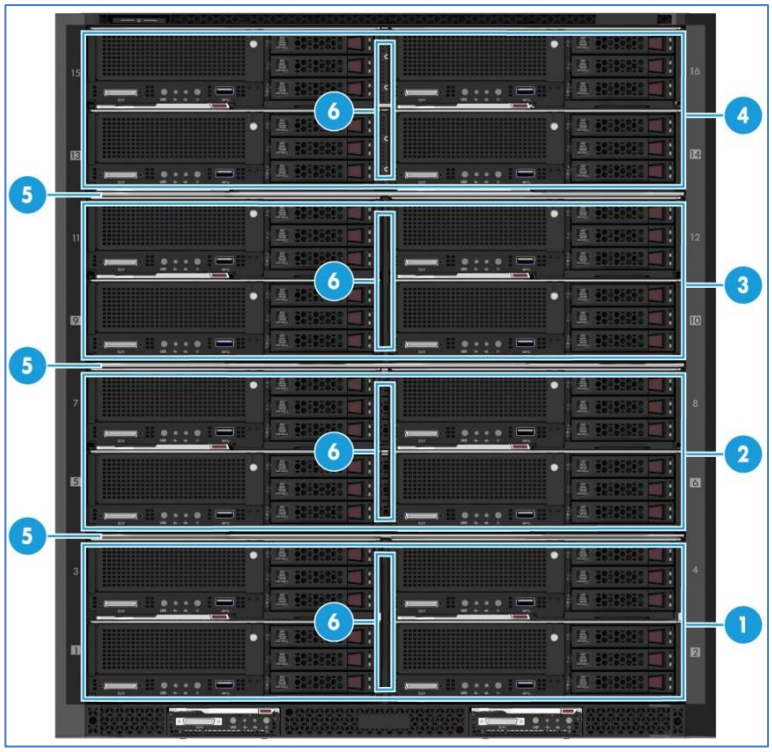
ファン構成の要件は、エンクロージャーへのブレードサーバーの取り付け状況によって異なります。エンクロージャーにブレードサーバーを取り付ける場合は、次の制約事項およびガイドラインに従ってください。

- エンクロージャーにブレードサーバーを左から右に、下から上に取り付けます。
- ハーフ幅ブレードサーバーとフル幅ブレードサーバーの両方を取り付ける場合は、最初にハーフ幅ブレードサーバーを取り付けます。

エンクロージャー内のブレードサーバーの取り付け状況に応じて、次のいずれかのファン構成を使用します。

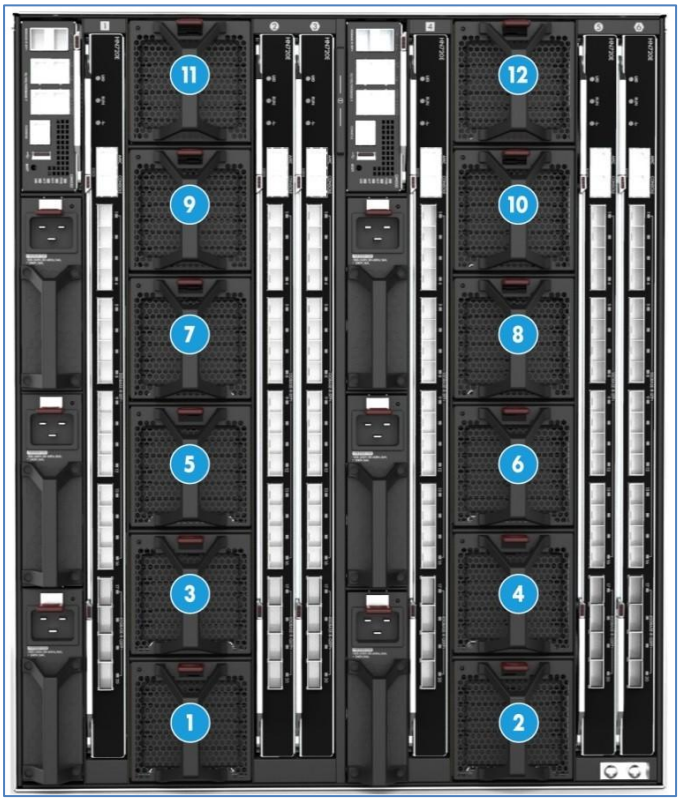
- **8ファン構成**: エンクロージャーのエリア3にブレードサーバーが取り付けられていない場合は、エンクロージャーに8個以上のファンを取り付ける必要があります。ファンベイ1～8にファンが取り付けられていることを確認してください。
- **12-ファン構成**: エンクロージャーのエリア3にブレードサーバーが取り付けられている場合は、エンクロージャーに12個のファンを取り付ける必要があります。

図43 ブレードサーバーの設置場所



(1)~(4)ブレードサーバーの設置場所
(5)固定デバイスベイシェルフ
(6)リムーバブルデバイスベイディバイダー

図44 ファンベイ

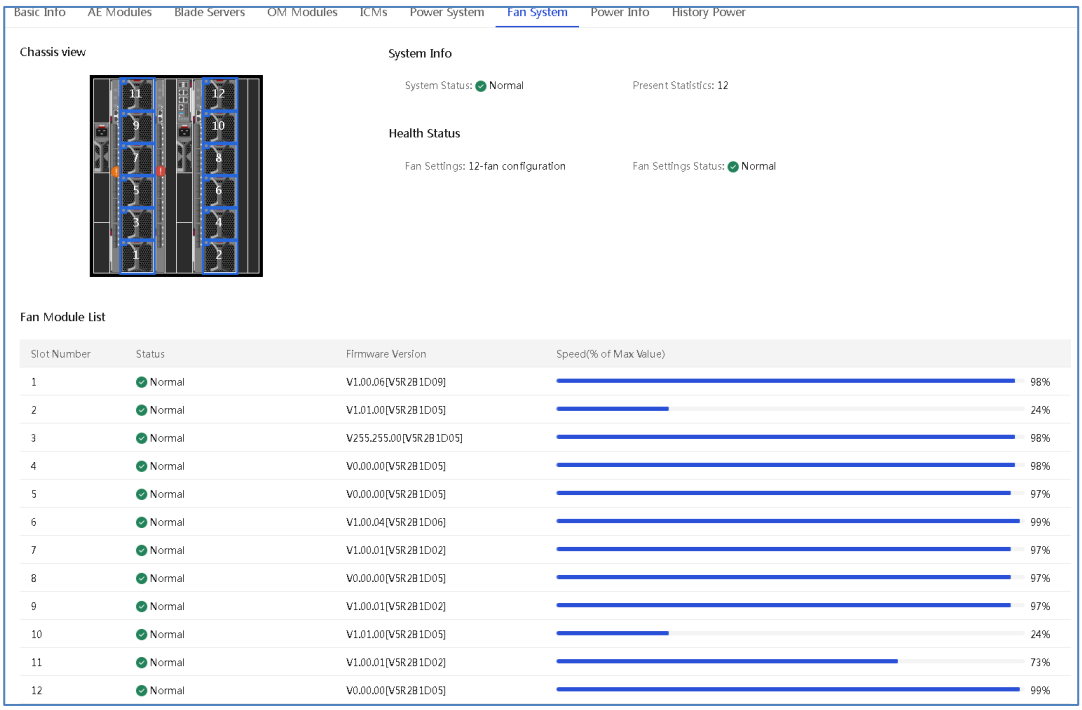


ファンベイ×1～12

手順

1. ナビゲーションペインで、Menu>Devices>Enclosuresを選択します。
2. エンクロージャーの名前をクリックします。
3. **Fan System**タブをクリックします。
   このタブには、エンクロージャー内のファンに関する情報が表示されます。

図45 Fan Systemタブ



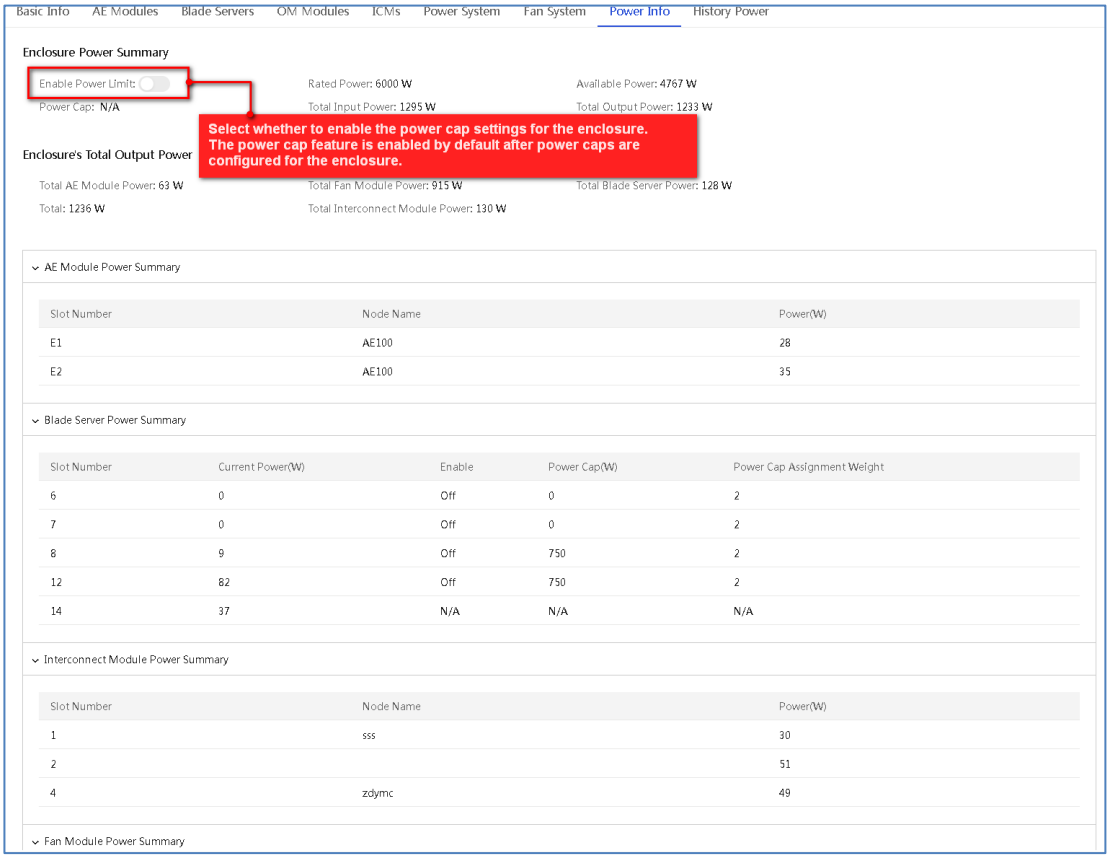
電源情報を表示する

エンクロージャーの電力概要情報、エンクロージャーの総出力電力情報、およびAEモジュール、ブレードサーバー、インターコネクトモジュール、およびファンの電力概要情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. **Power Info**タブをクリックします。
   このタブには、エンクロージャーの電源情報に関する情報が表示されます。

図46 電源情報タブ



電源履歴の表示

このタスクについて

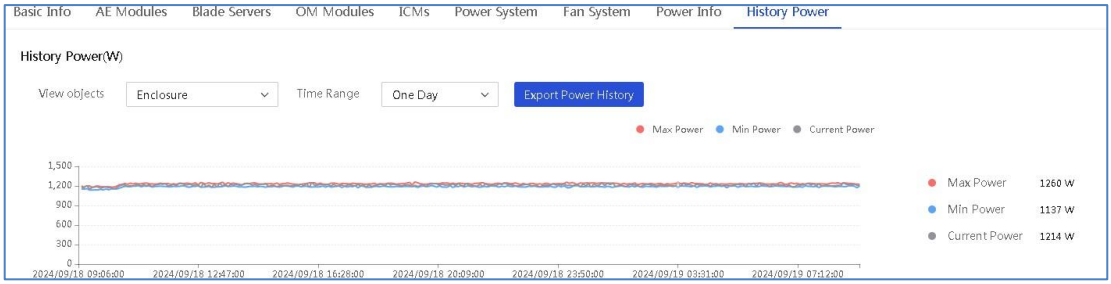
エンクロージャーまたはエンクロージャー内のブレードサーバーの電力履歴データを表示してエクスポートするには、次の作業を実行します。1時間間隔で集計された先週のデータ、または5分間隔で集計された最終日のデータを表示できます。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの名前をクリックします。
3. 電力履歴**History Power**タブをクリックします。

   このタブページには、エンクロージャーの電力履歴グラフと電力履歴統計情報が表示されます。
4. 時間範囲内のオブジェクトの電力履歴統計を表示するには、**View Objects**リストからオブジェクトを選択し、**Time Range**リストから時間範囲を選択します。電力履歴グラフのポイントにカーソルを合わせると、対応する時間の電力統計が表示されます。
5. 電力履歴の統計情報をエクスポートするには、**Export Power History**をクリックします。

図47 電力履歴タブ



VCの事前設定

このタスクについて

Virtual Connectの事前設定機能を使用すると、OMを使用してインターコネクトモジュールを自動的に設定し、インターコネクトモジュール上のVC設定用にリソースを予約できます。

制約事項とガイドライン

この機能は、インターコネクトモジュールがIRFで設定されている場合は使用できなくなります。

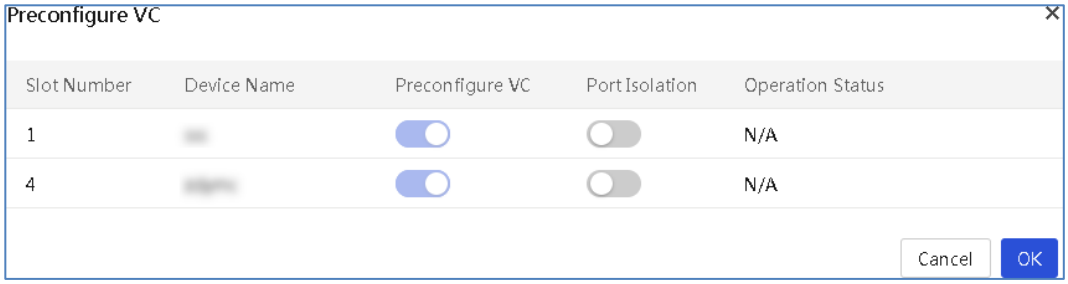
VC事前設定機能を使用するには、OMモジュールのファームウェアバージョンがUN_BLADE-OM-1.02.08～1.02.12であることを確認します。

VCを事前設定する前に、OMモジュールとインターコネクトモジュールの残りのストレージ容量が、設定の失敗を回避するのに十分であることを確認してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. **Actions**列の**Preconfigure VC**をクリックします。
3. 図48に示すように開いたダイアログボックスで、VCを事前設定し、**OK**をクリックします。

図48 VCの事前設定



システムログを表示する

このタスクについて

エンクロージャーのシステムログを表示およびエクスポートするには、次のタスクを実行します。システムログには、エンクロージャーで発生したすべてのイベントが記録されます。

制約事項とガイドライン

OMモジュールまたはエンクロージャーを再起動すると、OMモジュールまたはエンクロージャーのすべて

のシステムログがクリアされます。

システムは最大100個のシステムログを保存できます。この制限に達すると、最も古いシステムログが削除されます。

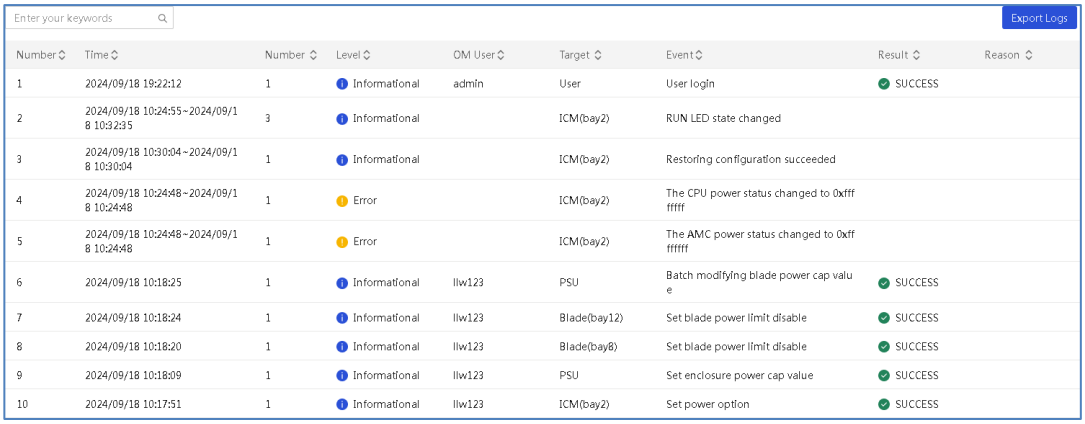
31日以内のシステムログをローカルファイルにエクスポートできます。エクスポートされたシステムログは、**System Logs**ページから削除されます。

過去1年間のシステムログを表示およびエクスポートするには、OM Webインターフェースにログインする必要があります。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures**を選択します。
2. エンクロージャーの**Actions**列で**View System Log**をクリックします。システムログページが開きます。
3. システムログをエクスポートするには、**Export Logs**タブをクリックします。
4. システムは、過去31日間のシステムログを**sys_log**という名前のローカルファイルにエクスポートします。

図49 エンクロージャーのシステムログの表示



Number	Time	Number	Level	OM User	Target	Event	Result	Reason
1	2024/09/18 19:22:12	1	Informational	admin	User	User login	SUCCESS	
2	2024/09/18 10:24:55~2024/09/18 10:32:35	3	Informational		ICM(bay2)	RUN LED state changed		
3	2024/09/18 10:30:04~2024/09/18 10:30:04	1	Informational		ICM(bay2)	Restoring configuration succeeded		
4	2024/09/18 10:24:48~2024/09/18 10:24:48	1	Error		ICM(bay2)	The CPU power status changed to 0xffffffff		
5	2024/09/18 10:24:48~2024/09/18 10:24:48	1	Error		ICM(bay2)	The AMC power status changed to 0xffffffff		
6	2024/09/18 10:18:25	1	Informational	llw123	PSU	Batch modifying blade power cap value	SUCCESS	
7	2024/09/18 10:18:24	1	Informational	llw123	Blade(bay12)	Set blade power limit disable	SUCCESS	
8	2024/09/18 10:18:20	1	Informational	llw123	Blade(bay8)	Set blade power limit disable	SUCCESS	
9	2024/09/18 10:18:09	1	Informational	llw123	PSU	Set enclosure power cap value	SUCCESS	
10	2024/09/18 10:17:51	1	Informational	llw123	ICM(bay2)	Set power option	SUCCESS	

エンクロージャートポロジの表示

このタスクについて

エンクロージャーの内部トポロジーおよびカスケードトポロジ(存在する場合)を表示するには、次の作業を実行します。

- **nternal topology**: ブレードサーバー、OMモジュール、メザニンカード、インターコネクトモジュール、およびAEモジュールと、エンクロージャー内のそれらのインターコネクトを表示します。エンクロージャー トポロジーページから、ドリルダウンしてブレードサーバーに関する詳細情報を表示できます。
- **Cascade topology**: エンクロージャーにカスケードされたエンクロージャーを表示します。

制約事項とガイドライン

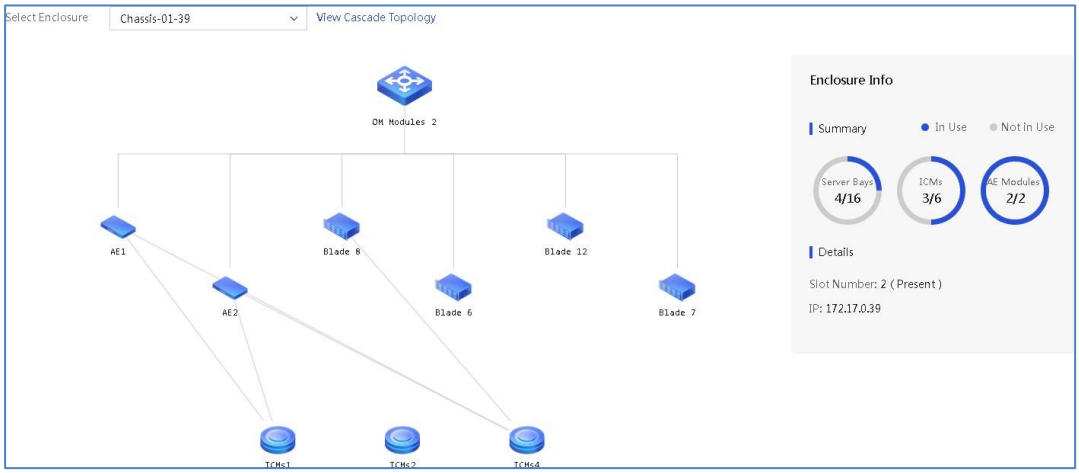
UniSystemは、オンラインエンクロージャーのトポロジーのみを表示できます。エンクロージャーがオフラインであるか、何らかの理由で接続できない場合は、エンクロージャー名にオフラインタグが追加され、エンクロージャーのトポロジーを表示できません。

手順

1. ナビゲーションペインで、**Menu>Devices>Enclosures>Enclosure Topology**を選択します。

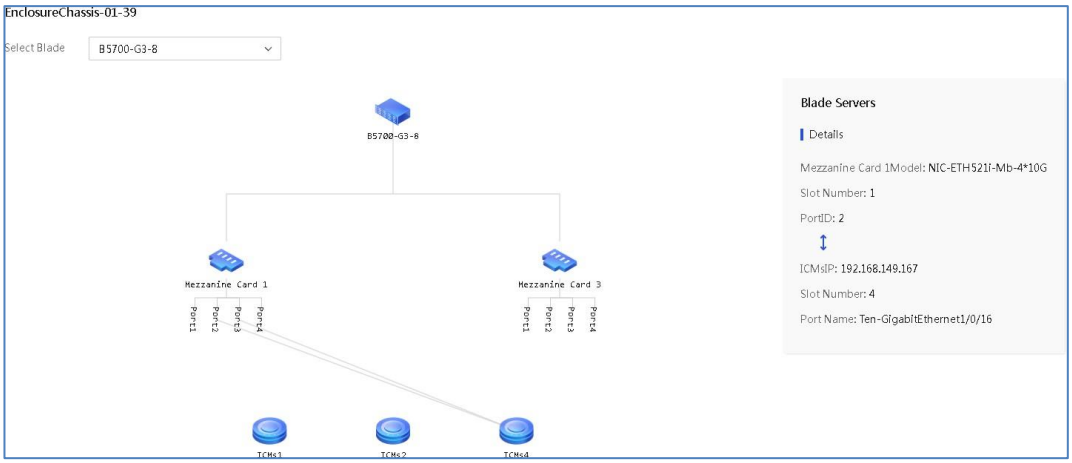
2. **Select Enclosure**から、トポロジーを開くエンクロージャーの名前を選択します。

図50 エンクロージャーのトポロジー



3. トポロジー内のブレードサーバーをクリックして、そのサーバーの**Enclosure Network Topology Blade Server Details**ページを開きます。このページには、サーバー上のインターコネクトモジュールとメザニンカード間の接続が表示されます。

図51 エンクロージャーのネットワークトポロジー-ブレードサーバーの詳細ページ



4. エンクロージャー内の別のブレードサーバーに関する情報を表示するには**Blade list**を選択します。
5. エンクロージャーのカスケードトポロジを表示するには、**Back**をクリックします。表示された**Enclosure Topology**ページで、エンクロージャー名の横にある**View Cascade Topology**をクリックします。カスケードトポロジの表示がグレー表示されている場合は、エンクロージャーにカスケードされているエンクロージャーがないことを示します。

   Enclosure Cascade Topologyページには、エンクロージャーにカスケードされているエンクロージャーが表示されます。このページでエンクロージャーをクリックすると、エンクロージャー名、カスケード番号、エンクロージャーIPアドレス、エンクロージャーステータスなどの詳細を表示できます。

図52 エンクロージャーのEnclosure Cascade Topologyページ



6. このページで選択したエンクロージャーの内部トポロジーに戻るには、**View Enclosure Topology**をクリックします。選択したエンクロージャーがUniSystemによって管理されていない場合、またはオフラインの場合、このリンクは使用できません。
7. **Select Enclosure**リストから選択したエンクロージャーの内部トポロジーに戻るには**Back**をクリックします。

サーバーの管理

サーバーの管理

UniSystemは、サーバーにインストールされているHDMまたはFIST SMSを通じてサーバーを管理できます。UniSystemを使用すると、次のサーバー管理タスクを実行できます。

- UniSystemへのサーバーの追加、UniSystemでのサーバー管理設定の編集、およびUniSystemからサーバーの削除。
- 管理対象サーバーに対してリモートコンソールを起動します。
- UniSystemが管理するサーバーに関する情報を表示します。
- UniSystemからリモートでサーバーを管理します。たとえば、サーバーの電源をオンまたはオフにしたり、サーバーのUID LEDをオンまたはオフにしたりできます。

一般的な制限事項とガイドライン

- デバイスがUniSystemによって管理されている場合は、デバイスのポート番号を変更しないでください。ポート番号が変更された場合は、デバイスを再度追加するか、デバイスがポート番号を自動的に復元するまで最大30分待つ必要があります。
- FIST SMSサーバーノードをUniSystemに追加する場合は、次の要件が満たされていることを確認してください。
  - サーバーでファイアウォールが無効になっているか、ポート12580がファイアウォールのホワイトリストに追加されています。
  - SELinuxは無効になっています。
  - サーバーにはHDMがインストールされており、進行中のアップグレードプロセスはありません。
  - サーバーノードは、オペレーティングシステムのIPアドレスを使用してUniSystemサーバーに接続できます。
- HDMサーバーノードをUniSystemに追加する場合は、次の要件が満たされていることを確認してください。
  - UniSystemサーバーは、HDMサーバーノード上のHDM専用ネットワークポートまたは共有ネットワークポートに接続できます。

- UniSystemとの通信に使用されるアクセスサービスポートは、HDMサーバーノードで使用できます。表7に、アクセスサービスで使用されるデフォルトのポート番号を示します。

  IPMI通信障害を回避するには、IPMIサービスが使用するデフォルトポートを変更しないでください。

  表7 アクセスサービスが使用するデフォルトのポート番号

サービス	デフォルトのセキュアでないポート	デフォルトのセキュアポート
CD-Media	5120	5124
IPMI	623	623
KVM	7578	7582
SNMP Trap	162	なし
Web	80	443

サーバーを手動でUniSystemに追加する

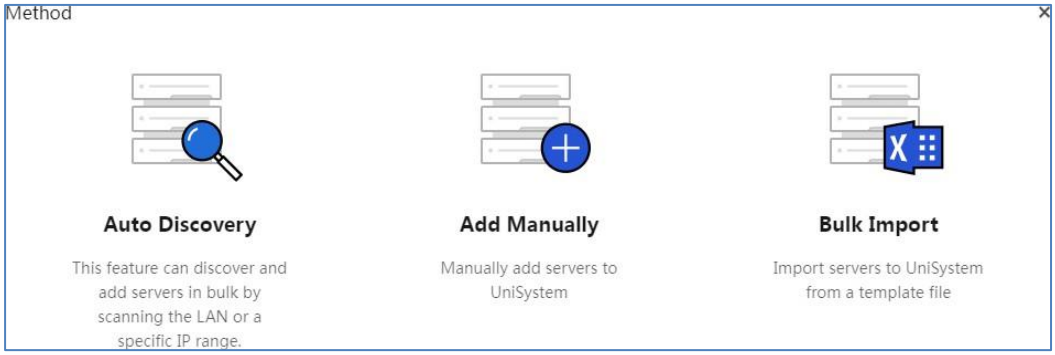
このタスクについて

HDMまたはFIST SMSサーバーノードをUniSystemに手動で追加するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. **Add**をクリックします。
3. **Add Manually**ダイアログボックスで、**Add Manually**を選択します。

図53 メソッドの選択

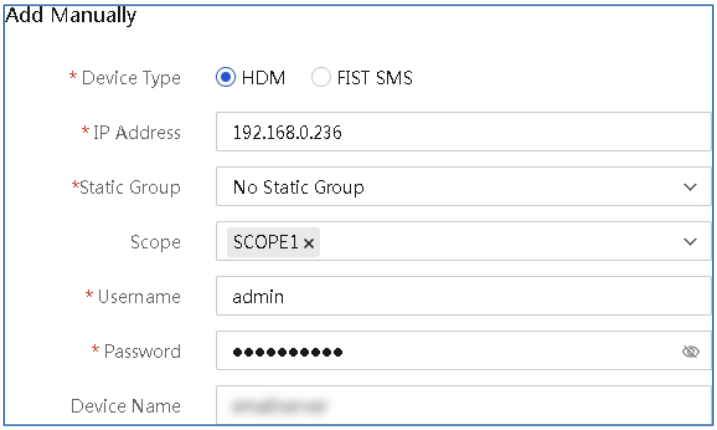


4. デバイス情報を入力し、スタティックグループを選択して、スコープを選択します。
   - HDMサーバーノードを追加するには、**Device Type**として**HDM** を選択します。HDM IPアドレスとデバイス名を指定します。

     Usernameおよび**Password**フィールドで、UniSystemのHDM管理者アカウントのユーザー名とパスワードを指定します。管理者以外のアカウントを指定すると、UniSystemが提供するサーバー管理機能の一部がHDMサーバーノードで使用できなくなります。

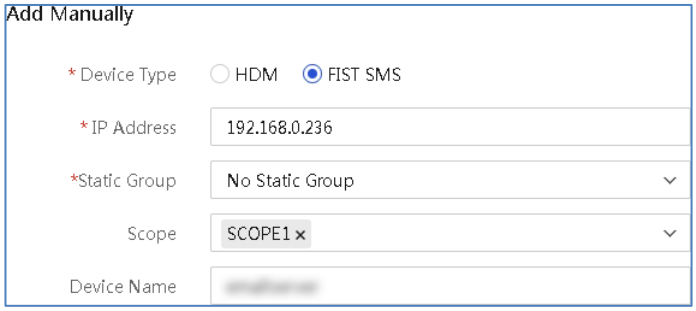
     HDMサーバーノードは、複数のUniSystemサーバーで管理できます。

図54 HDMサーバーノードの追加



- FIST SMSサーバーノードを追加するには、**Device Type**で**FIST SMS**を選択します。サーバーのFIST SMS IPアドレスおよび名前を指定します。

図55 FIST SMSサーバーノードの追加



5. **OK**をクリックします。

サーバーのインポート

このタスクについて

ファイルからUniSystemにサーバーをインポートするには、次のタスクを実行します。

前提条件

サーバーをUniSystemにインポートする前に、まずインポートするサーバーを含む有効なインポートファイルを準備します。Import Devicesページでインポートファイルテンプレートをダウンロードし、必要に応じてデバイス情報を入力できます。

表8に、サポートされているテンプレートをリストします。

表8 サポートされているテンプレート

テンプレート	説明
template-1.txt	各行は、「IPアドレス、ユーザー名、パスワード、デバイス名」の形式でデバイスを表します。HDMデバイスの場合は、IPアドレス、ユーザー名およびパスワードを入力します。FIST SMSデバイスの場合は、IPアドレスのみが必須です。デバイス名はオプションのフィールドです。
template-2.xlsx	各行は、「最初の列がデバイスタイプ、2番目の列がIPアドレス、3番目の列がユーザー名、4番目の列がパスワード」という形式でデバイスを表します。 5番目の列のデバイス名」。HDMデバイスの場合は、デバイスタイプ、IPアドレス、ユーザー名、およびパスワードを入力します。FIST SMSデバイスの場合は、デバイスタイプとIPアドレスのみを入力します。デバイス名はオプションフィールドです。

template-3.xls	各行は、「1列目がデバイスタイプ、2列目がIPアドレス、3列目がユーザー名、4列目がパスワード、5列目がデバイス名」の形式でデバイスを表します。HDMデバイスの場合は、デバイスタイプ、IPアドレス、ユーザー名およびパスワードを入力します。FIST SMSデバイスの場合は、デバイスタイプとIPアドレスのみが必須です。デバイス名はオプションのフィールドです。

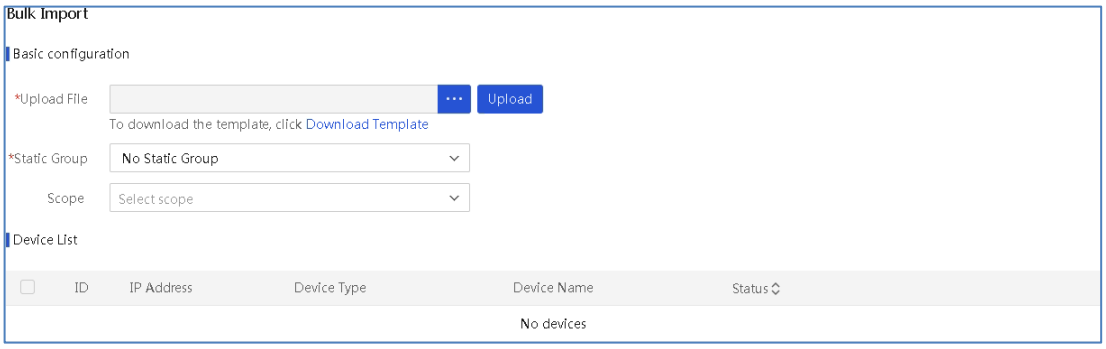
手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. **Add**をクリックし、**Bulk Import**を選択します。
3. **Upload File**フィールドで、…をクリックしてインポートファイルを選択し、**Upload**をクリックしてファイルをアップロードします。

   UniSystemは、ファイル内のすべてのデバイスをデバイスリストに表示します。
4. スタティックグループを選択します。
5. スコープを選択します。
6. UniSystemにインポートするサーバーを選択し、**OK**をクリックします。

   インポート処理には時間がかかる場合があります。

図56 UniSystemへのサーバーの一括インポート



自動検出によるサーバーの追加

このタスクについて

自動検出では、Simple Service Discovery Protocol(SSDP)またはIPサブネットスキャンを使用してネットワークでサーバーを検索し、検出されたサーバーをUniSystemに追加できます。自動検出では、HDMサーバーノードとFIST SMSサーバーノードの両方を追加できます。

制約事項とガイドライン

SSDP方式は、G6サーバーおよびそれ以降の世代のサーバーでのみ使用できます。

- サーバーのUniSystem管理は、レイヤ2ネットワークでのみ実装できます。
- UniSystemとHDMはIPv6で有効にする必要があります。HDMはSSDPでも有効にする必要があり、リスニングにポート1900を使用します。

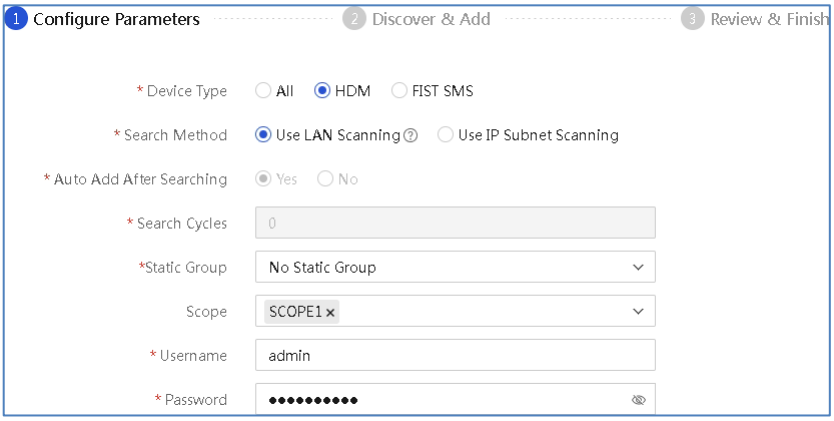
手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. **Add**をクリックし、**Auto Discovery**を選択します。
3. デバイスタイプと検索方法を選択します。
   - HDMサーバーノードのみを検索する場合、またはFIST SMSとHDMサーバーノードの両方を検索する場合は**HDM**または全てのDevice Typeを選択します。
     - **Use IP Subnet Scanning**を選択した場合は、IPアドレス範囲の開始IPアドレスと

終了IPアドレスを入力します。

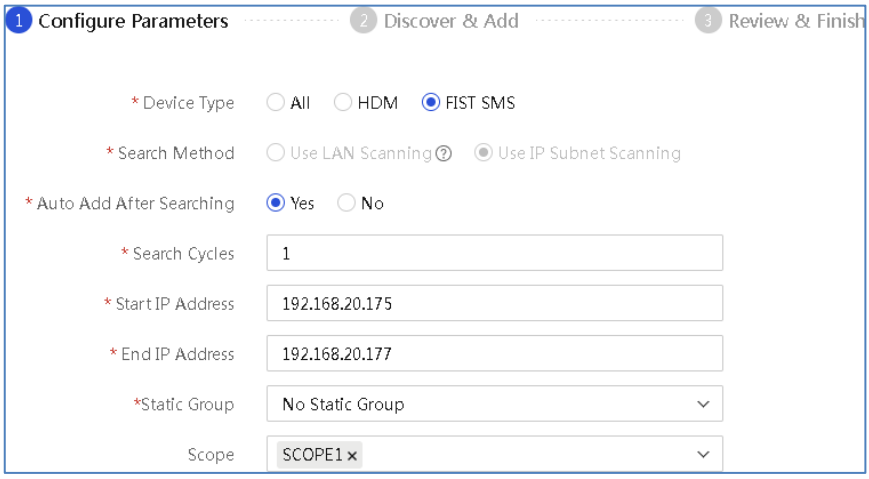
– **Use LAN Scanning**を選択した場合は、サーバーのHDMログインユーザー名とパスワードを入力します。

図57 HDMノードとFIST SMSノードの両方、またはHDMノードのみの検索



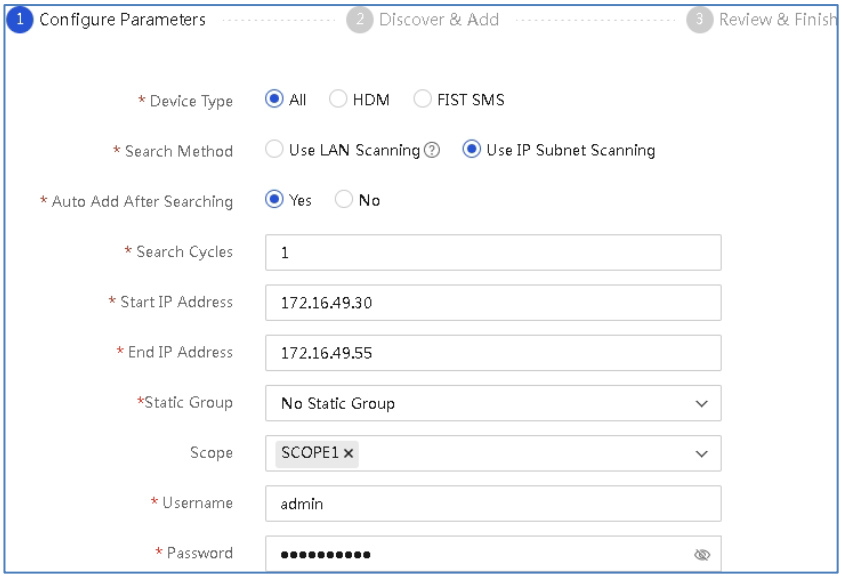
- FIST SMSサーバーノードのみを検索するには、**Device Type**で**FIST SMS**を選択します。このデバイスタイプでは、IPサブネットスキャン方式のみがサポートされます。IPアドレス範囲の開始IPアドレスと終了IPアドレスを入力します。

図58 FIST SMSサーバーノードのみの検索



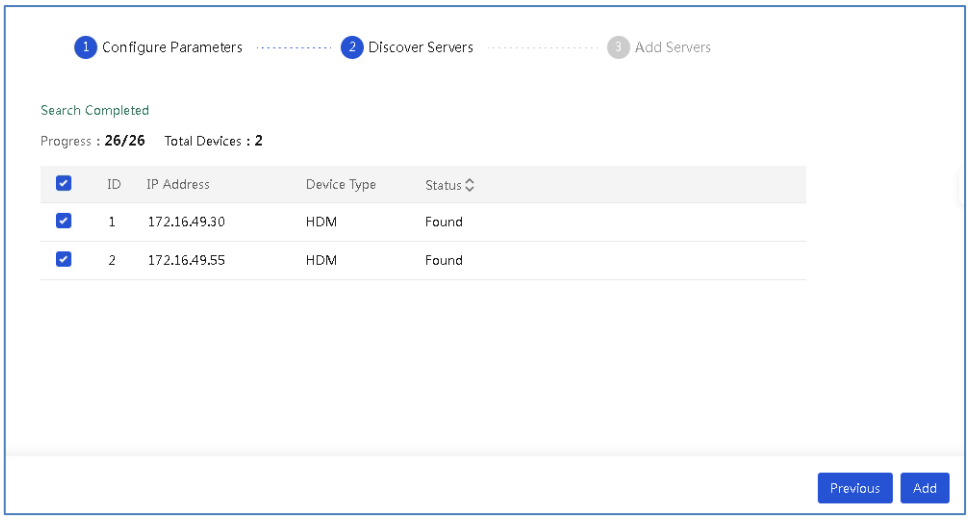
4. 検出されたサーバーを自動的に追加するかどうかを選択します。
   - **Search Method**で**Use LAN Scanning**を選択した場合、検出されたサーバーはデフォルトで自動的に追加されます。
   - **Search Method**で**Use IP Subnet Scanning**を選択し、**Auto Add After Searching**で**Yes**を選択した場合は、**Search Cycles**フィールドに検索サイクル数を入力します。

図59 検出されたサーバーの自動追加



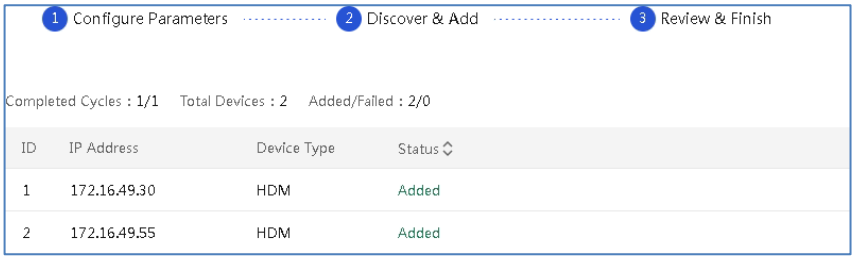
5. スタティックグループを選択します。
6. スコープを選択します。
7. **Search**をクリックします。
    - **Auto Add After Searching**で**No**を選択した場合は、検出されたサーバーの一覧から追加するサーバーを選択し、**Add**をクリックします。

図60 選択したサーバーのUniSystemへの追加



    - **Auto Add After Searching**で**YES**を選択した場合、UniSystemはサーバーを検出すると自動的にサーバーを追加します。プロセスを中止するには、検出されたサーバーのリストの右上隅にある**Abort**をクリックします。

図61 検出されたサーバーのUniSystemへの自動追加



8. **Server**ページに戻って新しく追加されたサーバーを表示するには、ページの左上隅にある**Back**をクリックします。

IP設定を一括設定する

はじめに

IP構成テンプレートファイルを使用して、複数のサーバーのHDM管理IPアドレスを一括編集するには、次のタスクを実行します。サーバーは、UniSystemで管理されているサーバーまたは管理されていないサーバーのいずれかです。この機能は、HDM-3.10以降のバージョンを使用しているサーバーでのみ使用できます。

メモ:

HDM専用ネットワークポートと共有ネットワークポートのIPアドレスを同時に変更する場合は、異なるネットワークセグメントにIPアドレスを設定します。
同じサブネットでは、サーバーネットワーク障害が発生する可能性があります。

UniSystemは、次の方法でIPアドレスのバッチ設定をサポートします。

- **IP Address**: サーバーのデフォルトのHDM管理IPアドレスが変更された場合に適用されます。
  - UniSystem管理IPアドレスとサーバーの現在のHDM管理IPアドレスが同じネットワークセグメント上にあることを確認します。
  - テンプレートに入力するときは、サーバーの現在のHDM管理IPアドレスが必要です。
- **Port MAC**: サーバーのデフォルトHDM管理IPアドレスが変更されていないシナリオに適用されます。
  - UniSystem管理IPアドレスとサーバーの現在のHDM管理IPアドレスが同じレイヤ2ネットワーク内にあり、レイヤ2で相互に通信できることを確認します。
  - UniSystem管理インタフェースとサーバーの現在のHDM管理インタフェースに対してIPv6機能が有効になっていること、および両方のインタフェースのローカルリンクアドレスが**fe80**で始まっていることを確認します。
  - テンプレートに入力するときは、サーバーの現在のHDM管理インターフェイスのMACアドレスが必要です。
- **Serial Number**: サーバーのデフォルトのHDM管理IPアドレスが変更されていない場合に適用されます。
  - SSDP方式と非SSDP方式の両方がサポートされています。
  - SSDP(G6以降のサーバーでのみサポート)を使用してIPアドレスを変更するには、以下の手順に従ってください。
    - サーバーHDMのSSDP機能が有効になっており、ポート番号が1900であることを確認します。
    - UniSystem管理IPアドレスとサーバーの現在のHDM管理IPアドレスが同じレイヤ2ネット

ワーク内にあり、レイヤ2で相互に通信できることを確認します。

- UniSystem管理インタフェースとサーバーの現在のHDM管理インタフェースに対してIPv6機能が有効になっていること、および両方のインタフェースのローカルリンクアドレスが**fe80**で始まっていることを確認します。
- テンプレートに入力するときは、サーバーのシリアル番号が必要です。

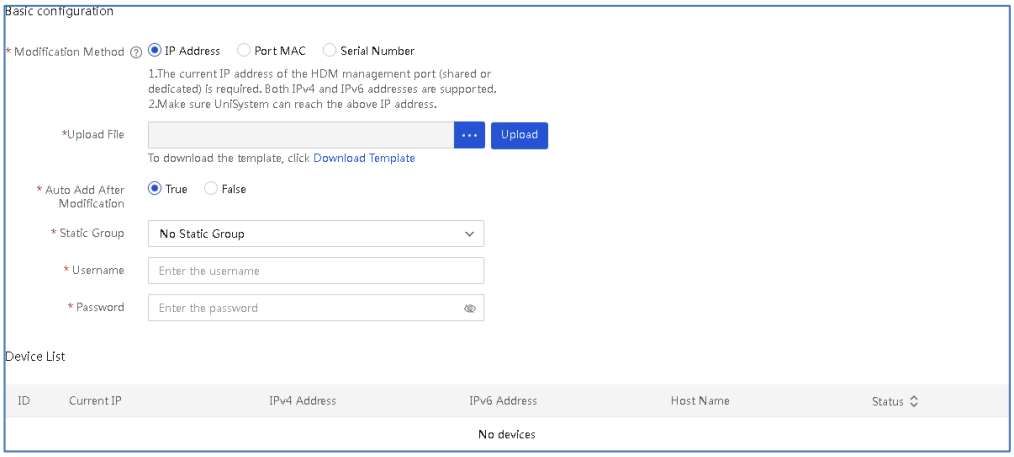
○ 非SSDP方式でIPアドレスを変更するには、次の手順を実行します。

- UniSystem管理IPアドレスとサーバーの現在のHDM管理IPアドレスが同じネットワークセグメント上にあることを確認します。
- テンプレートに入力するときは、サーバーのシリアル番号が必要です。

手順

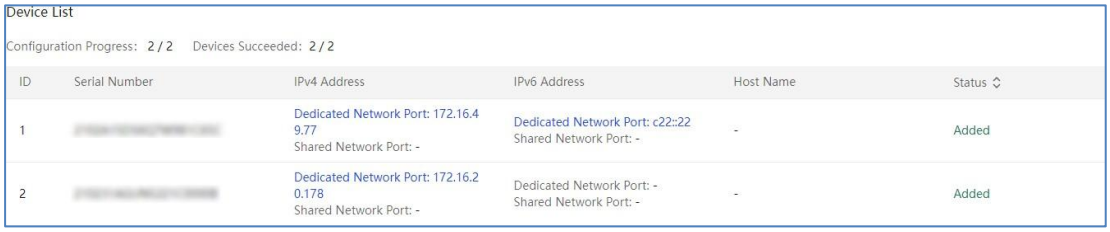
1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. **Bulk IP Settings**をクリックします。図62に示す**Bulk IP Settings**ページが開きます。

図62 IP設定の一括構成



3. **Modification Method**フィールドで、IP設定を一括構成する方法を選択します。オプションには、**IP Address**、**Port MAC**および**Serial Number**があります。
4. デバイスファイルテンプレートを取得するには、**Download Template**をクリックします。
5. 選択した変更方法に従って、ターゲットサーバーのIPアドレス、ネットワークポートMACアドレスまたはシリアル番号を入力します。HDM専用ネットワークポートまたは共有ネットワークポート(IPv4およびIPv6アドレスを含む)の変更されたIPアドレス情報を指定します。テンプレートの入力要件の詳細は、テンプレートとともにダウンロードされるREADMEファイルを参照してください。
6. **Upload File**フィールドで、アイコンをクリックします。表示されるダイアログボックスで、デバイスIPコンフィギュレーションファイルを選択します。
7. **Upload**をクリックします。アップロード後、デバイスリストからアップロードされたデバイス情報を表示できます。
8. **Auto Add After Modification**フィールドを構成します。変更後にサーバーをUniSystemで管理する必要がない場合は、**False**を選択できます。変更後にサーバーをUniSystemで管理する必要がある場合は、**True**を選択します。
9. (任意)スタティックグループを選択します。
10. **Username**フィールドと**Password**フィールドに、ターゲットサーバーのHDMユーザー名とパスワードをそれぞれ入力します。
11. **OK**をクリックして、サーバーのHDM管理IPアドレスの一括編集を開始します。**Auto Add After Modification**で**True**を選択すると、IPアドレスの編集後にサーバーがサーバーリストに追加されます。

図63 バルクIP設定のデバイスリスト



12. **Back**をクリックして、**Server**ページに戻ります。

サーバーの削除

このタスクについて

UniSystemからサーバーを削除するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 削除するサーバーを選択し、左上隅にある**More**をクリックして、**Delete**を選択します。
3. 表示された確認ダイアログボックスでOKをクリックします。

サーバーの編集

このタスクについて

UniSystemによって管理されるサーバーの名前とHDMログインクレデンシャルを一括編集するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーを選択し、**More**、**Edit**の順にクリックします。
3. **Edit HDM Username & Password**オプションを選択し、サーバーの新しいHDMログインユーザー名とパスワードを指定します。
4. **Edit Server Name**オプションを選択し、選択したサーバーの名前を次のように変更します。
   - 自動的に生成されたシーケンス番号を含む一意の名前を各サーバーに割り当てるには、文字列%*iを使用してデバイス名を入力し、開始シーケンス番号を指定します。文字列%*iのアスタリスク(*)を、シーケンス番号に含める桁数に置き換えます。この桁数は、1～4の整数である必要があります。1桁のシーケンス番号を使用するには、%*iを%1iまたは%iとして指定します。

     たとえば、デバイス名が**UniSystem%4i**に設定され、開始番号が6に設定されている場合、UniSystemは最初のサーバーの名前をUniSystem0006に変更し、後続のサーバーの名前をUniSystem0007、UniSystem0008などに変更します。

     選択したすべてのサーバーに統一された名前を割り当てるには、サーバー名を入力し、**Start Number** フィールドを空のままにします。
5. **OK**をクリックします。

図64 サーバー設定の編集



サーバーをグループ別に管理する

この機能を使用すると、サーバーの静的グループと動的グループを作成して、サーバーの識別とフィルタリングを容易に行うことができます。

nullキーワードを使用すると、**-**、**N/A**、および**Unknown**の情報を除外できます。

制約事項とガイドライン

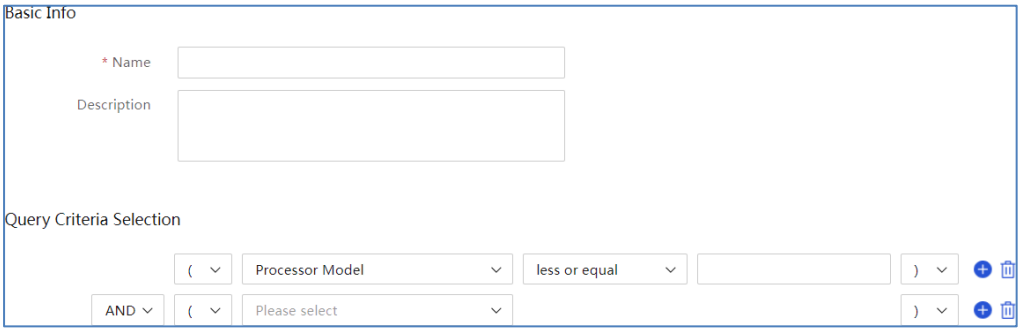
- 動的グループの名前および説明は、大文字と小文字が区別され、255文字を超えることはできません。中国語の文字、数字、文字、スペースおよび特殊文字のみ`~!@#$%^&*()_+-=\{};':",./<>?は使用できますが、文字列の先頭または末尾にスペースを使用することはできません。
- 動的グループ名は一意である必要があります。
- 動的グループごとに最大6つの問合せ基準を指定でき、問合せ基準は重複できます。動的グループには、少なくとも1つの問合せ基準が必要です。
- 条件タイプの値を入力する場合、最大64文字まで入力できます。テキストタイプの条件タイプの場合は、文字、数字、スペースおよび特殊文字のみ入力できます。`~!@#$%^&*()_+-=\{};':",./<>?は使用できますが、文字列の先頭または末尾にスペースを使用することはできません。整数タイプの条件タイプでは、整数のみが使用でき、その数は2147483647を超えることはできません。
- 条件タイプとサブタイプは英語であり、ソフトウェア言語の切り替えによって変更されることはありません。
- システムは、コピーされたグループのグループ名に**-copy**文字列を追加します。グループ名の長さが上限を超えていないことを確認してください。
- 静的グループの名前および説明は、大文字と小文字が区別され、255文字を超えることはできません。中国語の文字、数字、文字、スペースおよび特殊文字のみ`~!@#$%^&*()_+-=\{};':",./<>?は使用できますが、文字列の先頭または末尾にスペースを使用することはできません。
- 静的グループ名は一意である必要があります。

動的グループを作成する

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。

2. **Dynamic Group**の右にあるアイコン をクリックし、**Create Dynamic Group**を選択します。

図65 動的グループの作成



3. 開いたページで、基本情報を入力し、クエリー条件を指定します。
4. **OK**をクリックします。

基準タイプと算術演算子タイプ

問合せ基準を指定する場合は、基準タイプと算術演算子の両方を指定する必要があります。異なる基準タイプと算術演算子によって多数の組合せが形成されるため、算術演算子と基準タイプは次のように分類されます。

表9 算術演算子の種類

タイプ	演算子	アプリケーションシナリオ
タイプ1	• not equal to • less than • less or equal • equals • greater than • greater or equal • is not null • is null	整数を照会
タイプ2	• not equal to • less than • less or equal • equals • greater than • greater or equal • is not null • does not contain • is null • contains • begins with • ends with	クエリー文字列
タイプ3	• not equal to • equals • is not null • is null	ステータスなどの列挙情報を照会します。

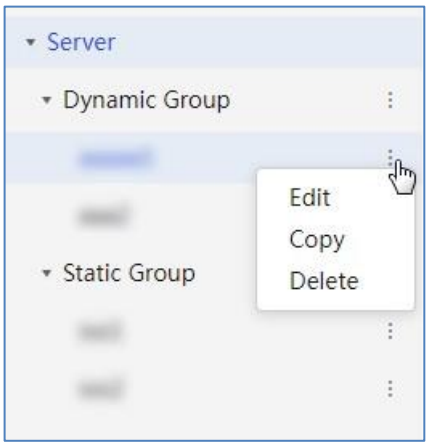
表10 基準の種類

基準タイプ	サブタイプ	演算子の種類	値のタイプ
プロセッサー	プロセッサーモデル	タイプ2	文字列。
	基本周波数	タイプ1	整数。
	コア数	タイプ1	整数。
	スレッド数	タイプ1	整数。
	プロセッサーステータス	タイプ3	列挙。
ハードディスク	ハードディスクベンダー	タイプ2	文字列。
	ハードディスクモデル	タイプ2	文字列。
	ファームウェアバージョン	タイプ2	文字列。
	ハードディスクの状態	タイプ2	文字列。
	ハードディスクの種類	タイプ3	列挙。
	伝送速度	タイプ2	1.5 Gbpsなどの文字列。
	容量	タイプ2	1.81 TiBや285 GBなどの文字列。
デバイス	製品名	タイプ2	R4900 G6などの文字列。
	IPv4アドレス	タイプ2	文字列。このオプションは、HDMおよびSMS IPv4アドレスもフィルタリングします。
	ホスト名	タイプ2	文字列。
ファームウェア	プライマリパーティション HDMバージョン	タイプ2	文字列。
	セカンダリパーティションの HDMバージョン	タイプ2	文字列。
	BIOSバージョン	タイプ2	文字列。
	CPLDバージョン	タイプ2	文字列。
	iFISTバージョン	タイプ2	文字列。

動的グループを編集する

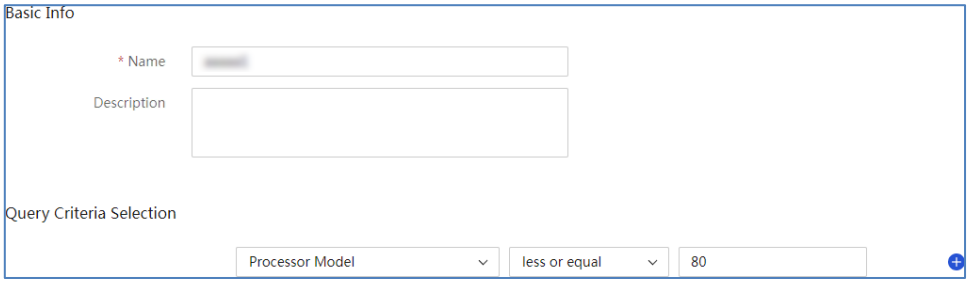
1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 作成した動的グループの右側にあるアイコン をクリックし、**Edit**を選択します

図66 動的グループの編集



3. 開いたページで、基本情報を入力し、クエリー条件を指定します。

図67 編集情報の指定



4. **OK**をクリックします。

動的グループをコピーする

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 作成した動的グループの右側にあるアイコン をクリックし、**Copy**を選択します。

図68 動的グループのコピー

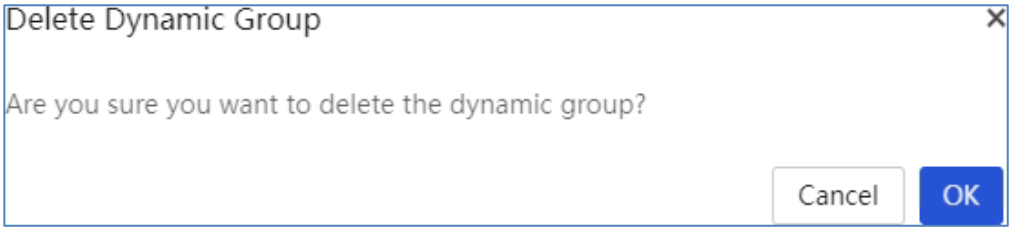


3. **OK**をクリックします。

動的グループを削除する

4. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
5. 作成した動的グループの右側にあるアイコン をクリックし、**Delete**を選択します。

図69 動的グループの削除

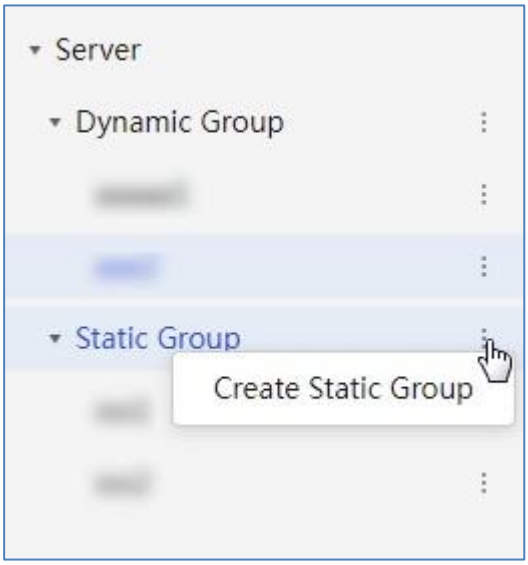


6. 表示されたダイアログボックスで、**OK**をクリックします。

静的グループを作成する

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. **Static Group**の右側にあるアイコン⋮をクリックし、**Create Static Group**を選択します。

図70 静的グループの作成



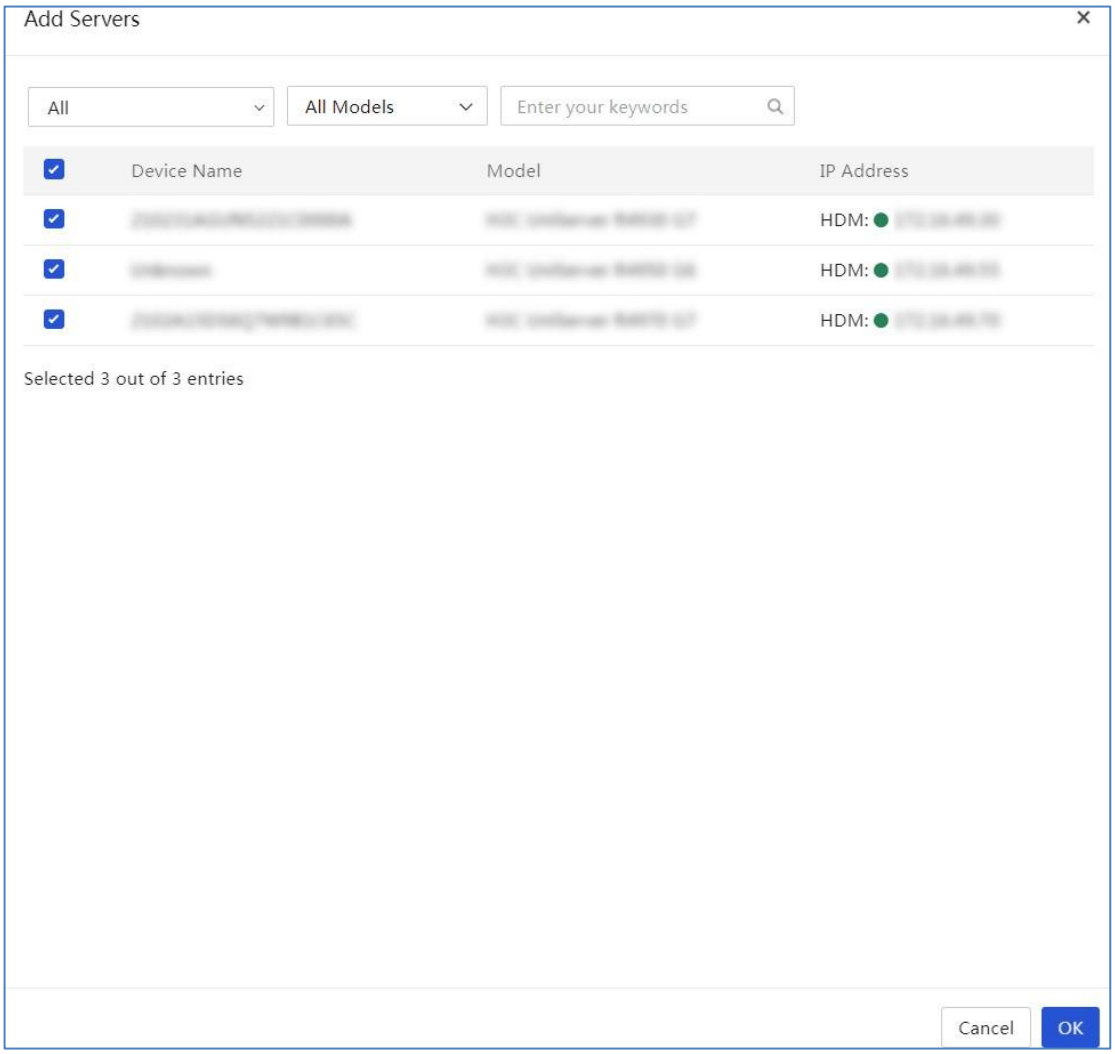
3. 表示されたページで、基本情報を入力します。
4. スタティックグループの基本情報を入力します。

図71 基本情報の入力



5. **Add Servers**をクリックします。表示されたページで、追加するサーバーを選択し、**OK**をクリックします。

図72 静的グループへのサーバーの追加



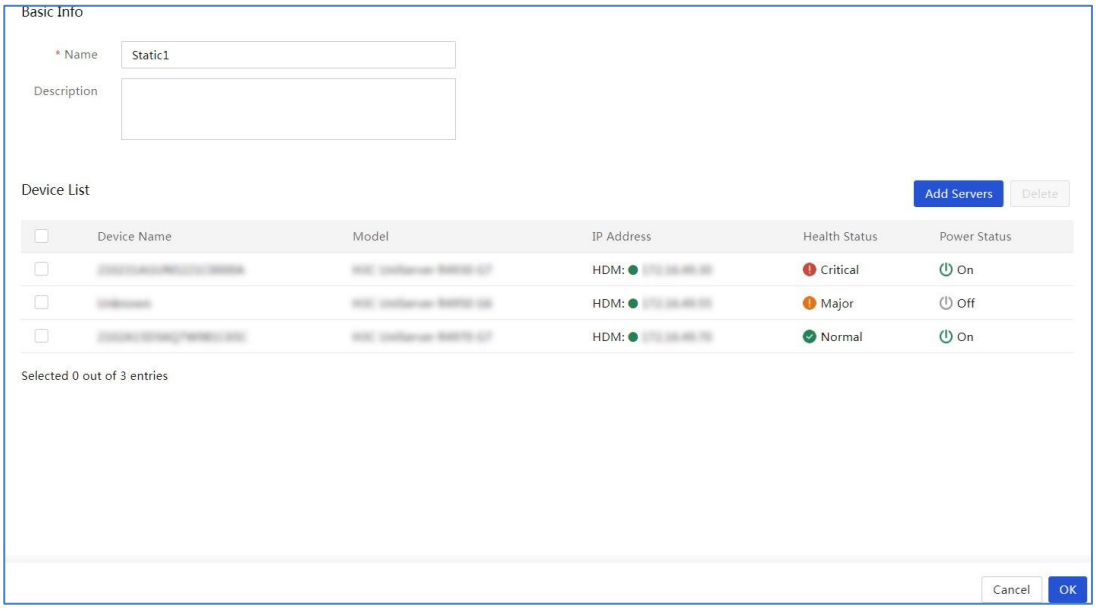
6. **OK**をクリックします。

スタティックグループを編集する

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 作成したスタティックグループの右側にあるアイコン をクリックし、**Edit**を選択します。
3. 開いたページで、基本情報を入力し、**Add Servers to add servers to the group**をクリック

します。

図73 静的グループの編集

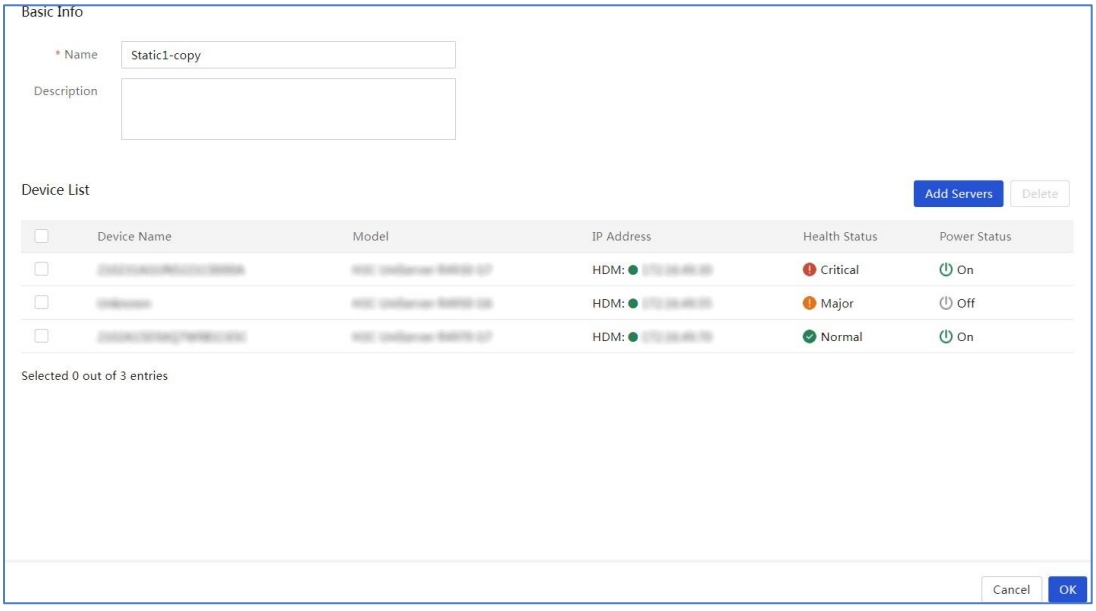


4. **OK**をクリックします。

静的グループをコピーする

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 作成した静的グループの右側にあるアイコン をクリックし、**Copy**を選択します。

図74 静的グループのコピー



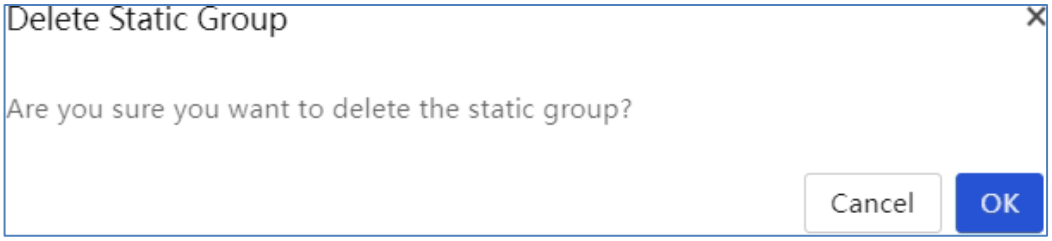
3. **OK**をクリックします。

静的グループの削除

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。

2. 作成したスタティックグループの右側にあるアイコン をクリックし、**Delete**を選択します。
3. 表示されたダイアログボックスで、**OK**をクリックします。

図75 静的グループの削除



リモートコンソールを起動する

このタスクについて

KVMまたはH5 KVMリモートコンソールを起動してサーバーを設定および管理するには、次の作業を実行します。

制約事項とガイドライン

- リモートコンソールを起動できるのは、KVMリモートコントロール権限を持つアカウントだけです。
- 最大4つの同時リモート制御セッションがサポートされます。
- UID LEDの点滅は、サーバー上のリモートコンソールがアクティブであることを示します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーの**Actions**列で**KVM**または**H5 KVM**をクリックします。

サーバー情報の表示

サーバーの詳細の表示

このタスクについて

Server Detailsページでは、概要、ハードウェアの詳細、温度情報、電源設定など、サーバーの詳細情報を表示できます。

制約事項とガイドライン

UniSystemは、ブレードサーバーのパワーサプライまたはファンに関する情報を提供しません。

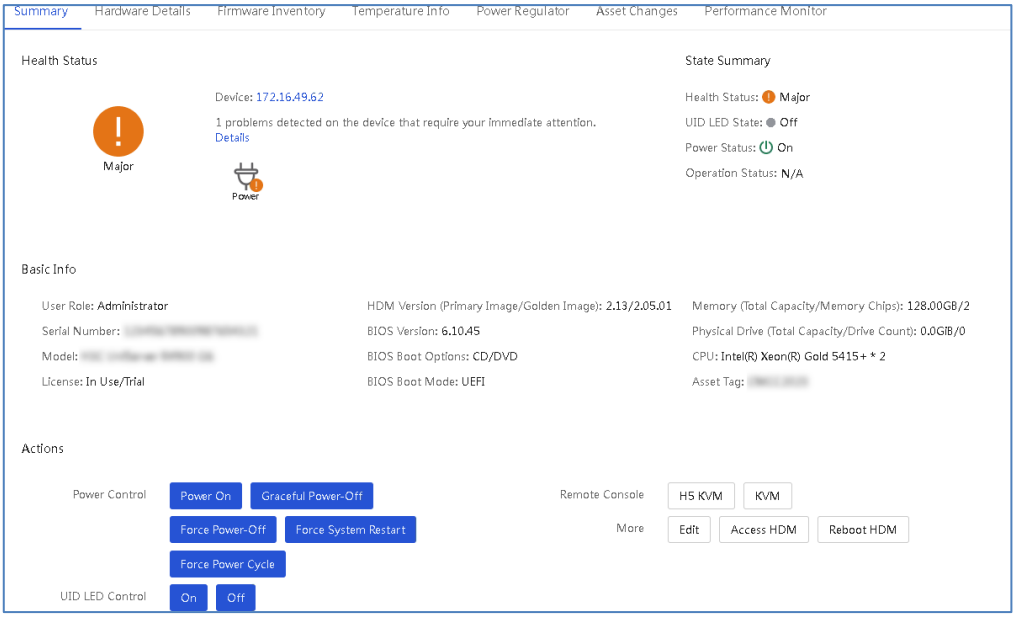
手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 詳細情報を表示するサーバーの名前をクリックします。
3. **Server Details**ページで、タブをクリックして、タブに表示される情報を表示します。

   使用可能なタブは次のとおりです。

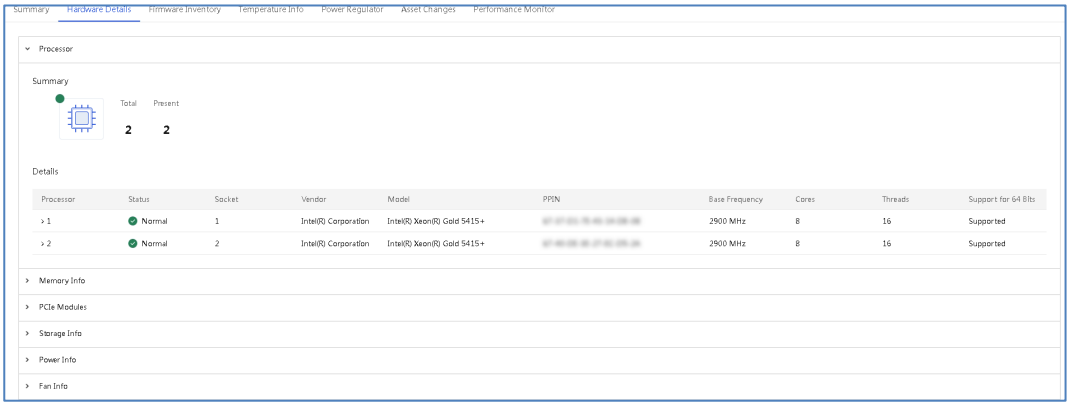
   - **Summary**: サーバーの全体的な健全性、ステータス、および基本情報を表示し、サーバーの管理オプションを提供します。

図76 Summaryタブ



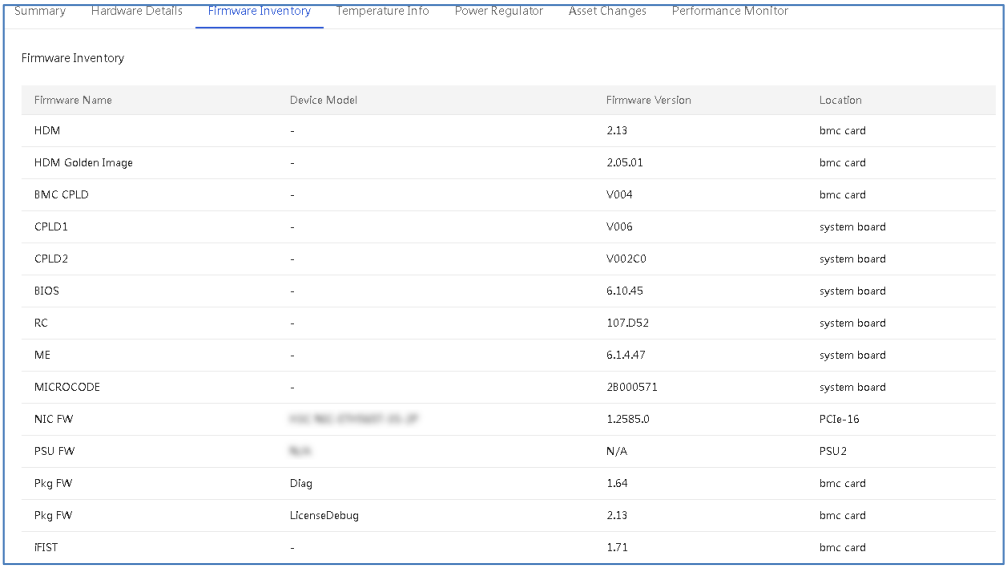
- **Hardware Details**: サーバー上のプロセッサー、メモリー、PCIeモジュール、ストレージコントローラー、論理ドライブ、物理ドライブ、パワーサプライ、ファン、および水冷モジュールに関する情報を表示します。

図77 Hardware Detailsタブ



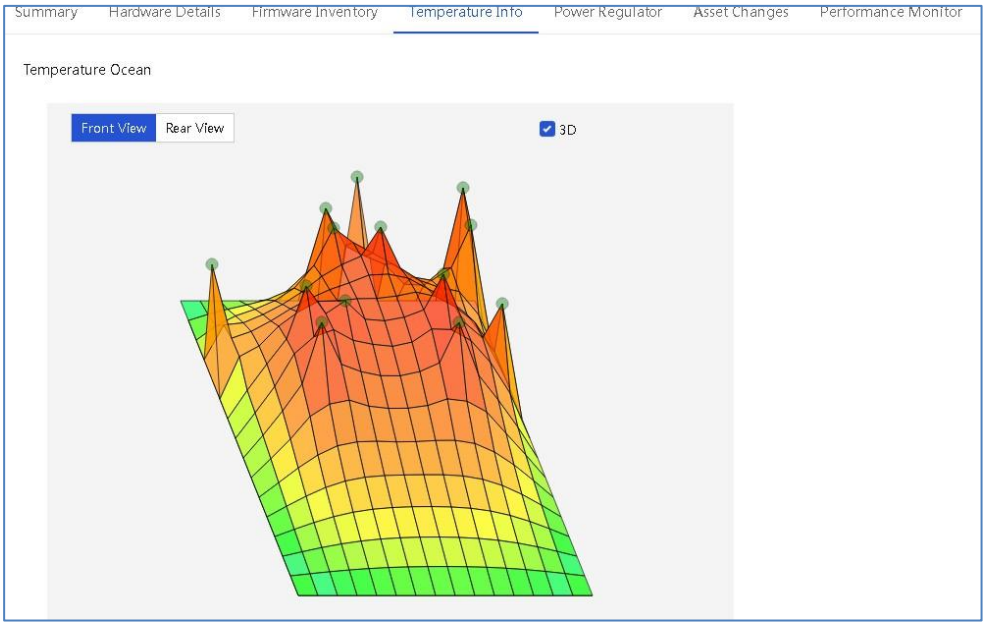
- **Firmware Inventory**: サーバーファームウェアのコンポーネントモデルとバージョン情報を表示します。

図78 Firmware Inventoryタブ



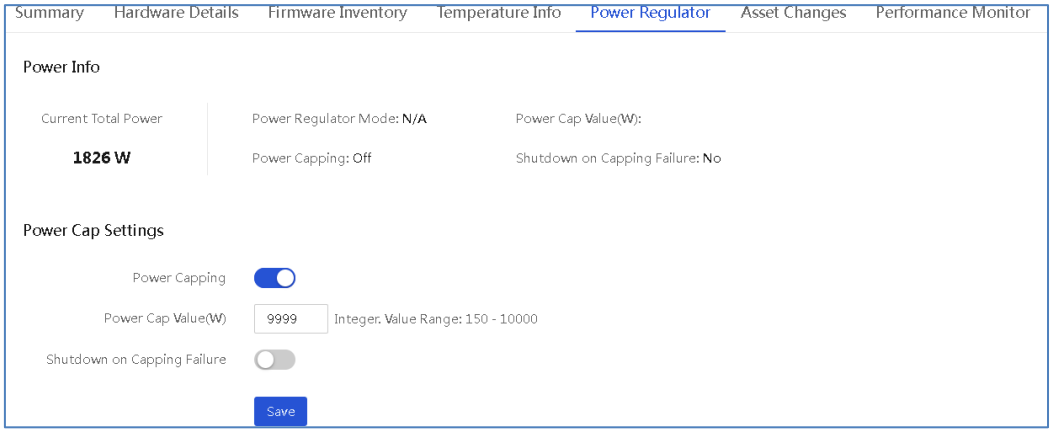
- **Temperature Info**: サーバーに関する温度情報を温度ヒートマップに表示します。マップの上にカーソルを置くと、温度センサーの名前、ステータス、および測定値が表示されます。

図79 温度情報タブ



- **Power Regulator**: サーバーの電源設定を表示および構成できます。サーバーの電源設定の設定方法については、「消費電力上限の設定」を参照してください。

図80 パワーレギュレータタブ



消費電力上限の設定

このタスクについて

Server Detailsページの**Power Regulator**タブから、サーバーの消費電力上限を設定できます。

消費電力上限機能を使用すると、サーバーの消費電力を、サーバーの最大定格電力以下の消費電力上限値に制限できます。

消費電力上限の値を超えると、サーバーは、プロセッサーなどのシステムコンポーネントの動作周波数を自動的に下げることによって消費電力を減らそうとします。消費電力上限は、消費電力が30秒以内に消費電力上限の値を下回ることができない場合、失敗します。

消費電力上限の障害が発生したときに、サーバーをシャットダウンするか、実行を継続するように構成できます。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. サーバーの名前をクリックして、サーバーの詳細ページに入ります。
3. **Power Regulator**タブをクリックします。
4. 消費電力上限を有効にするには、**Power Capping**で**Enable**を選択します。
5. 消費電力上限値を設定します。

   消費電力上限を設定すると、システムのパフォーマンスが低下します。特に、サーバーにGPUやSSDなどの電力を大量に消費するコンポーネントが搭載されている場合は、パフォーマンスの低下を避けるために、消費電力上限の値を慎重に選択してください。
6. (任意)必要に応じて、**Shutdown on Capping Failure**機能をイネーブルまたはディセーブルにします。
7. **Save**をクリックします。

サーバー資産の変更の表示

このタスクについて

サーバーの資産変更情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. デバイス名のリンクをクリックして、サーバーの詳細ページに入ります。
3. **Asset Changes**タブをクリックします。

4. プロセッサー、メモリー、ネットワークアダプター、PCIeデバイス、ファン、電源、ストレージコントローラー、FC HBA、ドライブ、GPUなど、現在のサーバーの資産変更情報を表示します。

図81 資産の変更

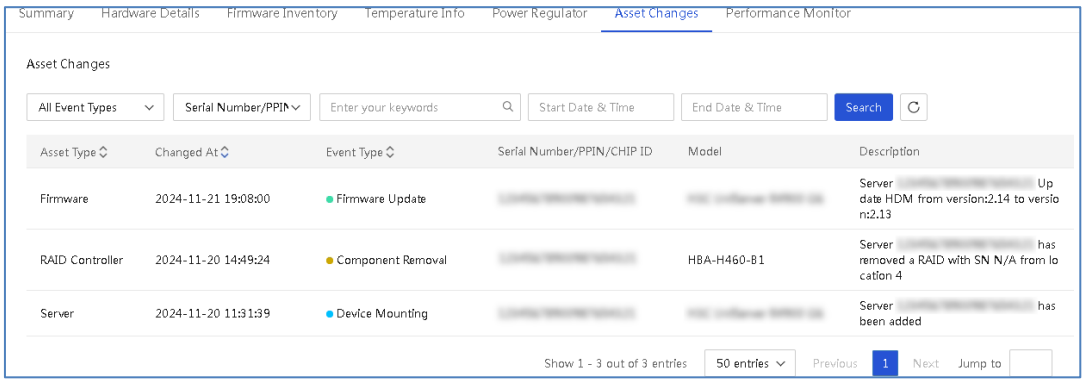


表11資産変更のパラメータの説明

パラメータ	説明
資産タイプ	サーバーの種類または特定のコンポーネント(プロセッサー、メモリー、ネットワークアダプター、PCIeデバイス、ファン、パワーサプライ、RAIDコントローラー、FC HBA、ドライブ、GPUなど)。
変更日時	資産変更が発生した時刻。
イベントの種類	資産変更のイベントタイプ。次のものが含まれます。 • **Device Mounting**: サーバーをUniSystem管理リストに追加します。 • **Component Adding**: コンポーネントをサーバーにインストールします。 • **Component Removal**: からコンポーネントを削除します。 • **Firmware Update**: HDM(プライマリおよびバックアップパーティション)、BIOS、ME、システムボードCPLD、またはiFISTファームウェアを更新します。
シリアル番号/PPIN	デバイスまたはコンポーネントのシリアル番号またはPPIN情報。
モデル	デバイスモデル情報。
説明	資産変更の説明情報。

FIST SMSサーバーノードのパフォーマンス監視データの表示

このタスクについて

FIST SMSサーバーノードの場合、**Server Performance Monitor**ページで物理リソース使用率情報を表示できます。UniSystemは、管理対象FIST SMSサーバーノードのCPU使用率、ドライブ領域使用量、メモリー使用量、ネットワークスループット、キャッシュメモリー、GPU使用量、ドライブI/O、ドライブスループット、ドライブ読取り/書込み比率、ドライブキューの深さ、I/O待機時間、NFSクライアント読取り/書込み速度、NFSサーバー読取り/書込み速度、システム負荷、入口温度および電力情報を30秒のモニター間隔で収集します。FIST SMSサーバーの過去30日間のリソース使用率データを表示できます。

NFSサーバーの読み取り/書き込み速度、NFSクライアントの読み取り/書き込み速度、およびシステム負荷は、Linuxオペレーティングシステムでのみ使用できます。

CLIベースの取得方法を必要とするNFSサーバーの読み取り/書き込み速度、GPU使用率、ディスク情報、および物理リソースデータを監視するには、最初に環境を構成する必要があります。リソース取得方法の詳細については、「H3C Servers FIST SMS User Guide」を参照してください。

- GPU使用情報:nvidia-smiをインストールして実行する必要があります。

- NFSクライアントの読み取り/書き込み速度とNFSサーバーの読み取り/書き込み速度:NFSクライアントをインストールし、サーバー環境をセットアップする必要があります。

システムに付属のiostatツールを使用してリソースを取得する場合、iostatで対応するフィールドが欠落していると値の取得に失敗します。この場合、手動インストールが必要です。iostatを手動でインストールするには、ソフトウェアパッケージマネージャまたはソースコードを使用します。ソースコードメソッドを使用するには、シンボリックリンクを使用してiostatファイルパスを置き換えます。iostatツールは/usr/bin/ディレクトリにあります。

サーバーのFIST SMSがUniSystemに追加されていない場合、サーバーのパフォーマンス監視ページには、サーバーの電力および温度トレンドの履歴グラフのみが表示されます。

制約事項とガイドライン

- UniSystemが監視期間のサーバー情報の取得に失敗した場合、監視期間に対応するデータは空として表示されます。FIST SMSノードへの接続に失敗したことを示すメッセージが表示されます。
- 特定の種類のリソースの使用量が対応するアラームしきい値を超えると、サーバーは対応するSNMPアラームを送信します。使用量がしきい値を下回ると、サーバーはSNMPアラームをクリアするためのメッセージを送信します。UniSystemを使用してSNMPアラームをリッスンするには、アラーム転送ページで関連機能を設定します。詳細については、「アラーム転送の設定」を参照してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 監視データを表示するFIST SMSサーバーのデバイス名をクリックします。
3. **Monitor**タブをクリックします。

   このタブには、FIST SMSサーバーノードの次の物理リソース使用情報が表示されます。

   - **CPU Usage**: サーバーで実行されているアプリケーションのCPU使用率を表示します。
   - **Drive Usage**:サーバーの使用可能なドライブ容量の合計に対する、使用済みドライブ容量の割合を表示します。
   - **Memory Usage**: 使用可能なメモリー領域の合計に対する、すべてのプロセスで使用されているメモリー領域の割合を表示します。
   - **Network Throughput**: 選択したネットワークアダプタの伝送速度および受信速度(Mbps単位)が表示されます。折れ線グラフの右上隅で、データを表示するネットワークアダプタのMACアドレスを選択します。
   - **History Temperature**:サーバーの吸気温度の変化傾向を表示します。
   - **History Power**:サーバーの電力変化の傾向をワット単位で表示します。
   - **CPU Usage Alarm Threshold**: アラームをトリガーするCPU使用率のしきい値。値0は、アラームを無効にすることを示します。
   - **Memory Usage Alarm Threshold**: アラームをトリガーするメモリー使用量のしきい値。値0は、アラームを使用不可にすることを示します。
   - **Drive Usage Alarm Threshold**: アラームをトリガーするドライブ使用のしきい値。値0は、アラームを無効にすることを示します。
   - **Cache Memory(MB)**: キャッシュメモリーのサイズ。
   - **GPU Usage**: 使用可能なGPUリソースの合計に対する、実行中のサービスで使用されているGPUリソースの割合。
   - **Drive I/O (operations/s)**: 特定の時間単位でのドライブの読み取り/書き込み。
   - **Read/Write Ratio**: 特定の単位時間内の読み取り/書き込み操作の合計に対するドライブの読み取り/書き込み操作の割合。
   - **Drive Queue Depth (operations)**: 特定の時間単位におけるドライブの読み取り/書き

込み操作の平均キューの長さ。

- **Drive Throughput (kb/s)**指定された単位時間内の読み取りおよび書き込みスループット。
- **I/O Latency**: ドライブの読取り/書込み操作が特定の時間単位でキュー内で終了するまでの平均待機時間。
- **NFS Client Read/Write Speed**: 特定の時間単位におけるNFSクライアントの読取り/書込み操作のデータ量。
- **NFS Server Read/Write Speed**: 特定の時間単位におけるNFSサーバーの読取り/書込み操作のデータ量。
- **System Load**: 特定の時間単位でのコンピュータシステムの計算ワークロード。各線グラフは、3時間の期間に収集されたデータを示します。

図82 Server Performance Monitorページ(1)

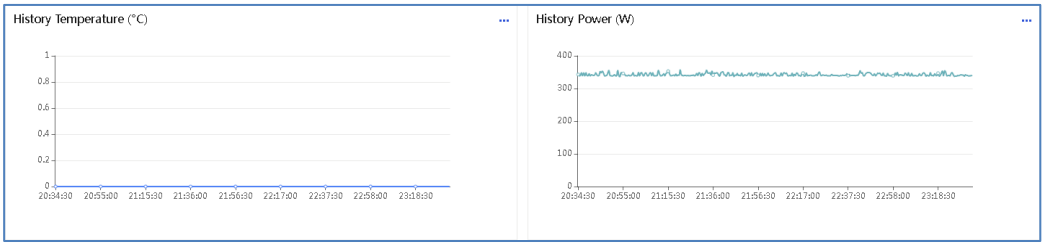


図83 Server Performance Monitorページ(2)



4. マウスホイールを回して、グラフのサイズを調整し、各監視期間のデータを表示します。
5. (オプション)**Advanced**をクリックします。サーバーの使用量アラームのしきい値を表示および設定できます。しきい値を設定すると、折れ線グラフでしきい値が赤い線でマークされます。

UniSystemによるサーバーのリモート管理

サーバーの電源のオン/オフ

このタスクについて

UniSystemからリモートでサーバーの電源をオンまたはオフにするには、次のタスクを実行します。

制約事項とガイドライン

UniSystemを使用して多数のサーバーに同時に電源を投入する場合、電流が大きすぎる可能性があります。ベストプラクティスとして、これらのサーバーを複数のバッチで動作させ、時差シフトでサーバーに電源を投入します。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーを選択し、**More**をクリックして、**Power Control**を選択します。
3. 必要に応じて、次の電源オプションのいずれかを選択します。
   - **Graceful Power-Off**:: サーバーの電源をグレースフルにオフにします。このボタンは、サーバーの電源ボタンを瞬間的に押す動作を模倣しています。
   - **Force Power-Off**: サーバーの電源を強制的にオフにします。このボタンは、サーバーの電源ボタンを物理的に押したままにした場合と同じ動作をします。
   - **Force System Restart**:: サーバーの電源を切らずにサーバーを再起動します。
   - **Force Power Cycle**: サーバーをただちに再起動します。
   - **Power On**: サーバーの電源をオンにします。このボタンは、サーバーの電源ボタンを瞬間的に押す動作を模倣しています。
4. 表示されたダイアログボックスで、**Operating instructions**を選択し、**OK**を選択します。

図84 サーバーの電源投入または電源切断



SDSログのダウンロード

このタスクについて

管理対象サーバーのSDSログをダウンロードしてローカルの.sdsファイルに保存するには、次のタスクを実行します。

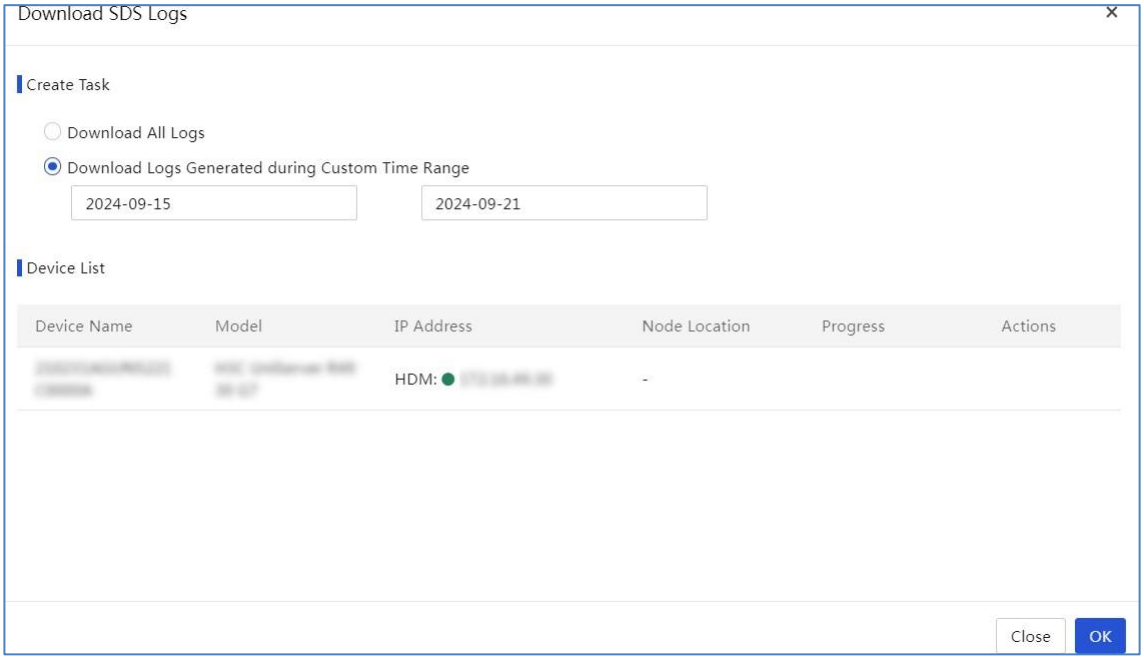
手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. SDSログをダウンロードするサーバーを選択し、**More**をクリックして**Download SDS Logs**を選択します。
3. すべてのSDSログをダウンロードするか、特定の時間範囲で生成されたSDSログのみをダウンロードするかを選択します。
4. 特定の時間範囲内に生成されたSDSログのみをダウンロードするには、必要に応じてログ生成時間範囲を指定します。
5. **OK**をクリックします。

   UniSystemは、選択したサーバーのSDSログのダウンロードを開始し、デバイスリストにデバイス

固有のダウンロードの進行状況を表示します。

図85 SDSログのダウンロード



サーバーの構成情報をエクスポートする

このタスクについて

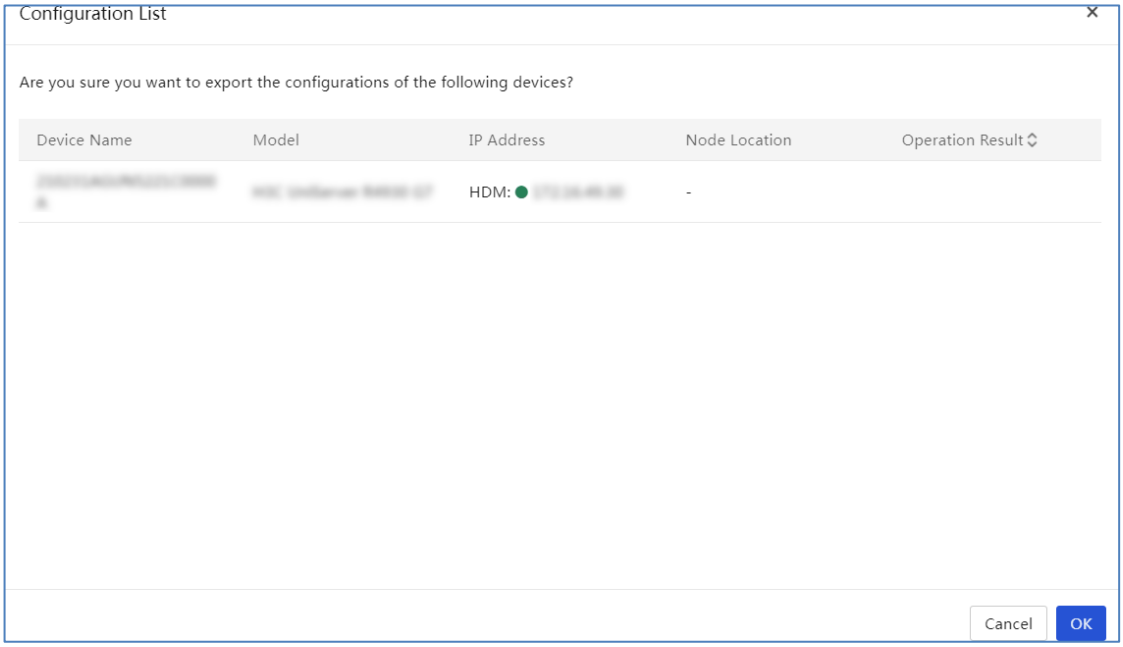
選択したサーバーの基本構成情報を.jsonファイルにエクスポートするには、次のタスクを実行します。エクスポートされる情報には、サーバーモデル、HDM IPアドレス、BIOS/HDMバージョン、プロセッサー、メモリー、ストレージおよびPCIeモジュール情報が含まれます。

UniSystemは、選択した各サーバーの構成情報を個別のファイルにエクスポートします。さらに、すべてのサーバー(名前で識別)とそのPCIeモジュール情報を記録するファイルを作成します。これらのファイルはすべてアーカイブに圧縮され、ローカルにダウンロードできます。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. 構成情報をエクスポートするサーバーを選択し、**More**をクリックして、**Configuration List**を選択します。
3. **OK**をクリックして、選択したサーバーの設定をエクスポートします。
4. エクスポートしたサーバーコンフィギュレーションファイルをローカルデバイスに保存します。

図86 選択したサーバーの構成情報のエクスポート



HDMの再起動

このタスクについて

選択したサーバーでHDMをリブートするには、次の作業を実行します。

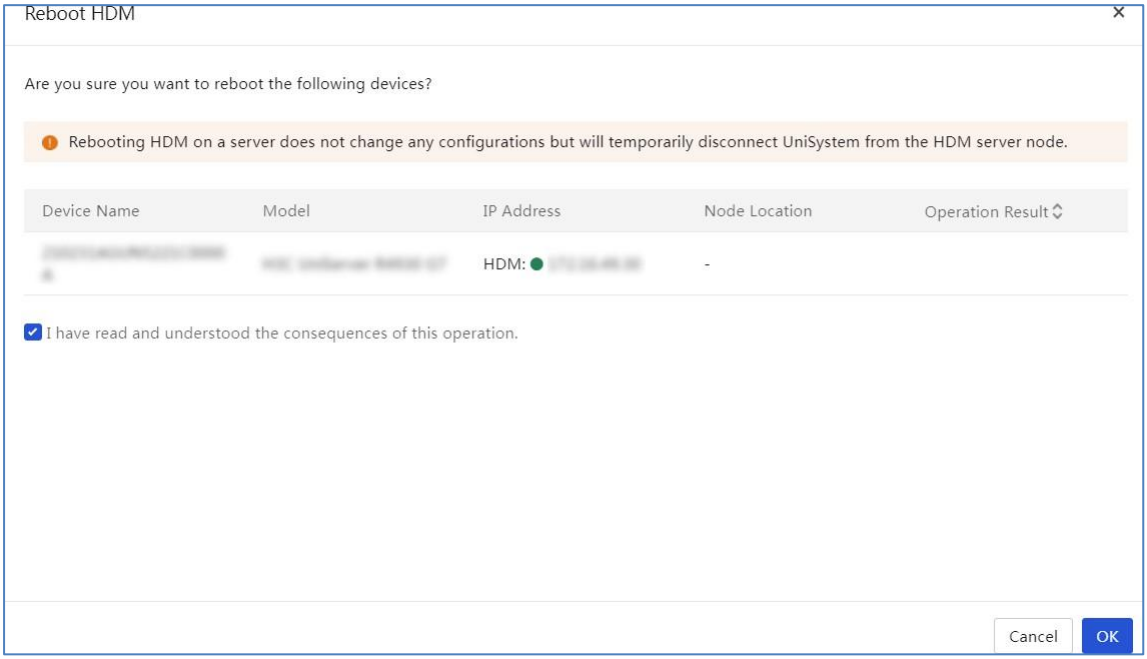
制約事項とガイドライン

- サーバーでHDMを再起動すると、サーバーがUniSystemから一時的に切断されます。HDMの起動後、接続は自動的に復元されます。
- ビデオファイルは、HDMの再起動後は存続できません。サーバーでHDMを再起動する前に、サーバー上のビデオファイルをバックアップしてください。
- HDMおよびオペレーティングシステムの異常を回避するために、HDMの再起動プロセス中は、サーバーの電源を入れたり切ったりしないでください。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーを選択して**More**をクリックし、**Reboot HDM**を選択します。
3. 操作情報を確認し、**I have read and understand the consequences of this operation**を選択します。
4. **OK**をクリックします。

図87 選択したサーバーでのHDMの再起動



漏洩処理戦略

この機能を使用して、液冷サーバーのリーク処理方式を設定します。設定に成功すると、この方式がデバイスに自動的に適用されます。自動シャットダウン方式を選択すると、液漏れの拡大やデバイスの損傷を防ぐために、UniSystemが自動的にサーバーをシャットダウンします。

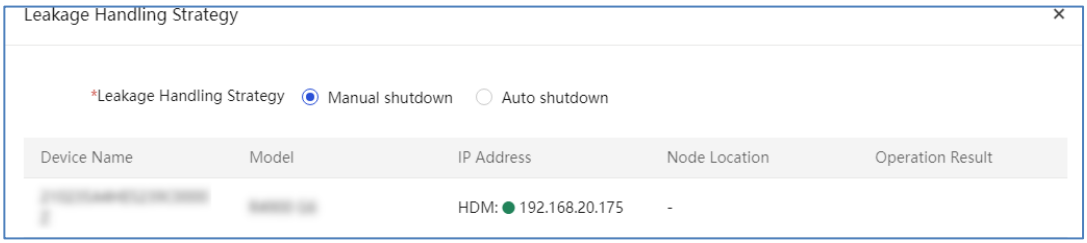
制約事項とガイドライン

- ストラテジに非水冷サーバーを選択した場合、サーバーのストラテジ設定は失敗しますが、これは正常な動作です。
- 設定が成功したら、UniSystemアラーム転送モジュールでアラーム監視を有効にして、リークアラーム情報を表示できます。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーを選択し、**More**をクリックして、**Leakage Handling Strategy**を選択します。
3. リーケージ処理方法を選択し、デバイスリストを確認して、**OK**をクリックします。

図88 リーケージ処理方法の設定



手動による障害レポート

このタスクについて

障害を手動でレポートするには、次の作業を実行します。

前提条件

修復パラメータを有効にして保存します。詳しくは、「リモコン」を参照してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
2. ターゲットサーバーを選択して**More**をクリックし、次に**Fault Report**を選択します。障害レポート操作が成功したことを示すメッセージが表示されます。
   障害修復タスクをチェックして、障害レポートのステータスを表示できます。

図89 手動故障報告



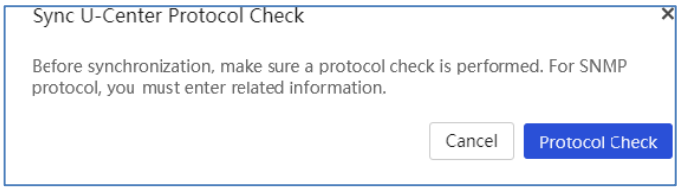
U-Centerを同期

統合O&MバージョンのUniSystemは、サーバーリスト内のデバイスをU-Centerの管理デバイスリストに同期させることをサポートします。

手順

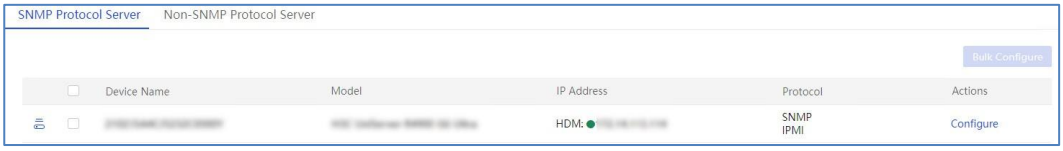
- ナビゲーションペインで、**Menu>Devices>Servers**を選択します。
- 同期するサーバーを選択し、**Actions**列の**More**をクリックして、**Sync U-Center**を選択します。
- 表示されたダイアログボックスで**Protocol Check**をクリックします。UniSystemは、U-centerとターゲットサーバーを同期するときにSNMPプロトコルをチェックするかどうかを確認します。

図90 プロトコルチェック



- SNMPプロトコルをチェックせずに、選択したサーバーをU-Centerに直接同期できる場合は、確認ダイアログボックスで**OK**をクリックします。
- 選択したサーバーでU-Centerと同期するためにSNMPプロトコルのチェックが必要な場合は、SNMP Protocol Serverページで**Configure**または**Bulk Configure**をクリックして、図91に示すようにSNMPを構成します。パラメータには、**SNMP Version**、**Read-Only Community String**および**Read/Write Community String**があります。**OK**をクリックして同期を完了します。

図91 プロトコル設定



スイッチの管理

UniSystemでは、次のモデルのスイッチを管理できます。

- H3C S6800-54QT
- H3C S 6850-56HF
- H3C S6800-54QF
- H3C UIS M8380-C
- H3C UIS M8310
- H3C S6850-56HF-CP
- H3C S6850-56HF-IM

スイッチ管理機能を使用する

スイッチを管理するには、次の作業を実行します。たとえば、スイッチの追加と削除、スイッチのユーザー設定の更新、およびスイッチのSSHコンソールへのログインを行うことができます。

スイッチを追加する

このタスクについて

管理用のスイッチをUniSystemに追加するには、次のタスクを実行します。最大30台のスイッチをUniSystemに追加できます。

前提条件

- スイッチの管理IPアドレスを取得します。
- スイッチを管理するadmin権限を持つシステムユーザーのユーザー名とパスワードを取得し、そのユーザーがHTTPサービスを使用できるように指定します。
- スイッチ上でNETCONF over SOAPをイネーブルにします。
- UniSystemが存在するネットワークと、追加するスイッチの管理ネットワークが相互に接続できることを確認します。

手順

1. スイッチの管理IPアドレス、およびスイッチを管理するadmin権限を持つシステムユーザーのユーザー名とパスワードを取得します。
2. スイッチのCLIにログインし、次の手順を実行します.

   #スイッチでNETCONF over SOAPを有効にします。

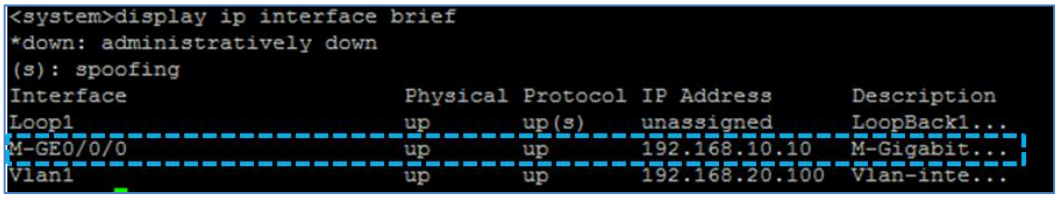
   ```
   [Sysname] netconf soap http enable
   ```

   #システムユーザービューを入力し、ユーザーがHTTPサービスを使用できることを指定します。この例では、ユーザー**admin**を使用します。

   ```
   [Sysname] local-user admin
   [Sysname-luser-manage-admin] service-type http
   ```

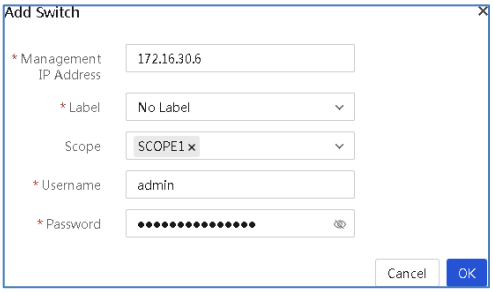
3. スイッチの管理ネットワークに属するセカンダリIPアドレスを追加します。
   a. スイッチ上で**display ip interface brief**コマンドを実行します。図92に示すように、M-GE0/0/0ポートのIPアドレスは、スイッチの管理IPアドレスです。

図92 スイッチの管理IPアドレスの取得



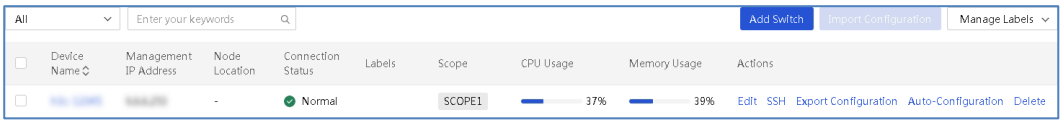
4. スイッチをUniSystemに追加します。
   a. UniSystemにログインします。
   b. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
   c. **Add Switch**をクリックします。表示されたダイアログボックスで、関連情報を入力し、**OK**をクリックします。

図93 スイッチの追加



   d. 新しく追加したスイッチが**Switches**ページに表示されていることを確認します。

図94 スイッチの追加



SSHコンソールからログインする

このタスクについて

SSHコンソールから、SSHを介して管理対象スイッチにログインし、スイッチのCLIを開くことができます。この機能を使用するには、管理対象スイッチでSSHサービスが有効になっており、ログインユーザーがSSHサービスをサポートしていることを確認します。

制約事項とガイドライン

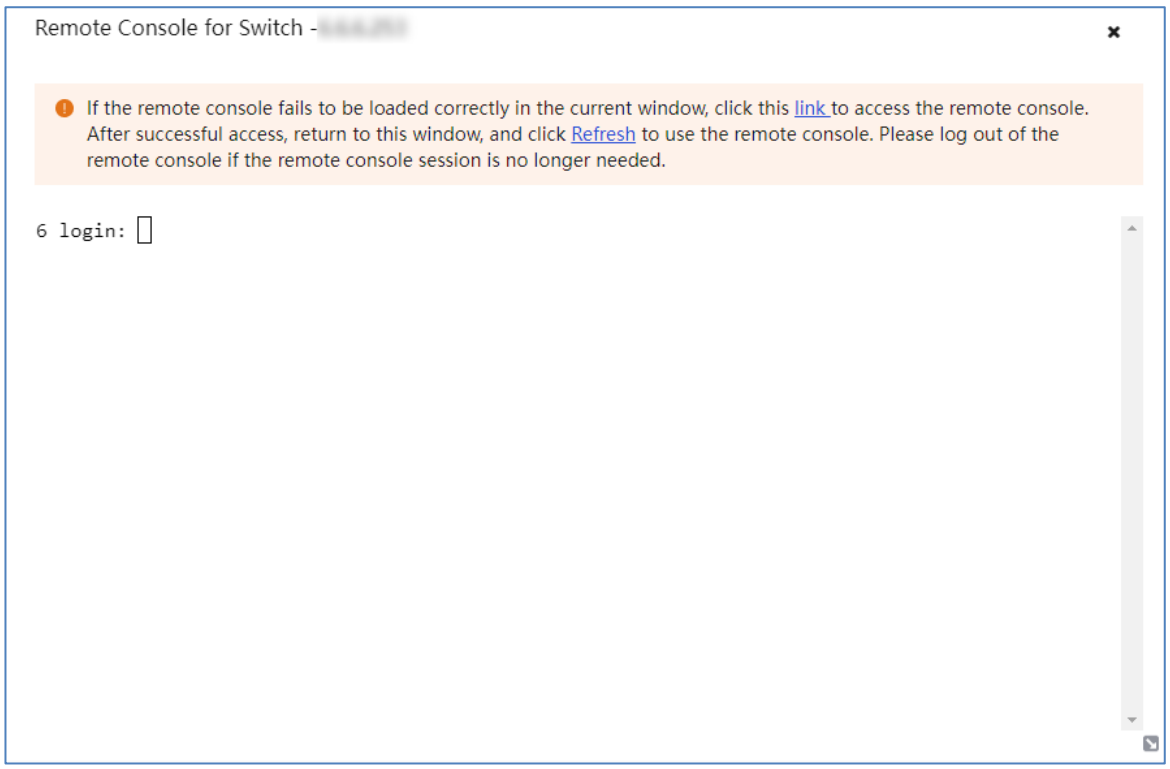
- SSHリモートコンソールウィンドウが正しく読み込まれない場合は、ウィンドウの下部にあるリンクをクリックして、新しいページで証明書を読み込みます。読み込みが完了したら、リモートコンソールウィンドウに戻り、**Refresh**をクリックします。SSHコンソールを長時間使用しない場合は、コマンドを実行してSSHコンソールを終了します。
- SSHコンソールを使用して管理対象スイッチのCLIにログインする場合は**Refresh**をクリックしません。そうでないと、ログアウトされます。
- WindowsオペレーティングシステムでUniSystem環境をセットアップし、UniSystemにスイッチを追加した場合、SSH機能は使用できません。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。

2. スイッチのActionsカラムでSSHをクリックします。

図95 SSHを介したスイッチへのログイン



スイッチの設定のエクスポート

このタスクについて

スイッチの設定をエクスポートし、**Menu>Templates>Switch Templates**ページのスイッチ設定テンプレートにエクスポートしたスイッチ設定を保存するには、次の作業を実行します。

この機能は、H3C S6850-56HFおよびH3C S6800-54Qスイッチでのみ使用できます。

制約事項とガイドライン

- UniSystemがスイッチ設定をエクスポートしている間は、(CLI、SNMP、またはその他の方法で)スイッチを操作しないでください。
- 設定のエクスポートは、リソースを大量に消費する操作です。設定をエクスポートする前に、スイッチに十分なリソースがあることを確認してください。
- スイッチ構成テンプレートの名前を**UniSystem.cfg**に設定しないでください。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. 設定をエクスポートするスイッチの**Actions**カラムで**Export Configuration**をクリックします。
3. 表示されるダイアログボックスで、次の操作を実行します。
   - 説明を入力します。
   - スイッチテンプレートが属するスコープを選択します。
4. **OK**をクリックします。

スイッチに設定をインポートする

このタスクについて

スイッチ設定テンプレート内の設定を管理対象スイッチにインポートするには、次の作業を実行します。この機能は、H3C S6850-56HFおよびH3C S6800-54Qスイッチでのみ使用できます。

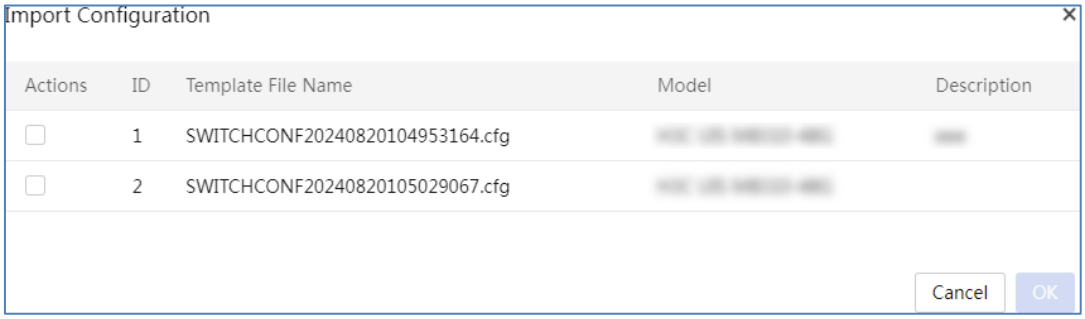
制約事項とガイドライン

- スイッチに構成をインポートした後、スイッチアドレスの競合が原因で、UniSystemがスイッチとの通信に失敗する場合があります。この問題を解決するには、スイッチのIPアドレスを手動で編集し、スイッチを再度UniSystemに追加します。
- コンフィギュレーションのエクスポート操作が進行中のスイッチには、コンフィギュレーションをインポートしないでください。
- スイッチに設定をインポートできるのは、スイッチモデルが一致するスイッチ設定テンプレートを使用する場合だけです。
- UniSystemがスイッチに設定をインポートしている間は、(CLI、SNMP、またはその他の方法で)スイッチを操作しないでください。
- 設定のインポートは、リソースを大量に消費する操作です。設定をインポートする前に、スイッチに十分なリソースがあることを確認してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. ターゲットスイッチを選択し、**Import Configuration**をクリックします。
3. 表示されたダイアログボックスで、スイッチにインポートする設定テンプレートを選択し、**OK**をクリックします。

図96 スイッチにインポートする設定テンプレートの選択



自動構成の構成

自動設定機能を使用すると、サーバーテンプレートをスイッチポートにバインドして、スイッチポートとそのポートに接続されているサーバーの自動設定をイネーブルにできます。

サーバーがUniSystemに追加されると、UniSystemは次の項目をチェックします。

- サーバーの管理ポートが、バインドされたサーバーテンプレートを持つスイッチポートに正しく接続されているかどうか。
- UniSystemで自動構成機能が有効になっているかどうか。

Yesの場合、UniSystemはバインドされたサーバーテンプレートをサーバーに自動的に適用し、サーバーテンプレートの接続設定に従ってスイッチポートを構成します。

制約事項とガイドライン

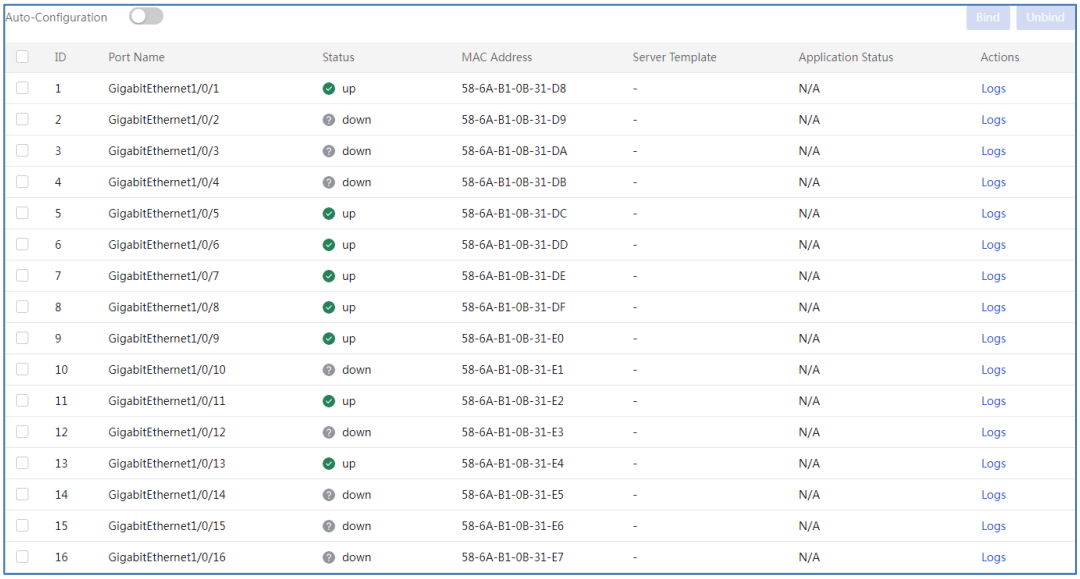
自動設定機能を正しく動作させるには、LLDPをグローバルにイネーブルにし、対応するスイッチポートでイネーブルにする必要があります。

UniSystemは、サーバーの電源がオフになっている場合にのみ、スイッチポートのバインドされたサーバーテンプレートを接続されているサーバーに適用できます。

手順

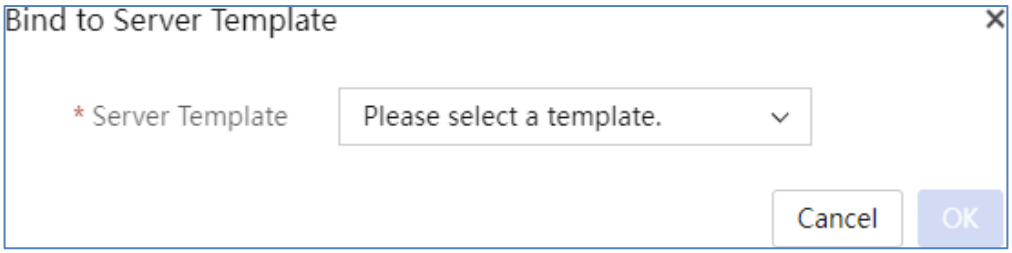
1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. スイッチのデバイス名をクリックすると、詳細ページが表示されます。
3. **Auto-Configuration**タブをクリックします。

図97 Auto-Configurationタブ



4. スイッチポートの一覧で、サーバーテンプレートをバインドするスイッチポートを選択し、**Bind**をクリックします。
5. 表示されたダイアログボックスで、選択したスイッチポートにバインドするサーバーテンプレートを選択し、**OK**をクリックします。

図98 選択したスイッチポートへのサーバーテンプレートのバインド



6. **Auto-Configuration**トグルスイッチをオンにして、自動構成機能を有効にします。
7. 一部のスイッチポートのサーバーテンプレートのバインドを削除するには、ポートを選択し、**Unbind**をクリックします。確認ダイアログボックスが表示されたら、**OK**をクリックします。
8. スイッチ ポートのサーバーテンプレート アプリケーション ログを表示するには、スイッチ ポートの **Actions** 列の**Logs**リンクをクリックします。

スイッチを削除する

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. 削除するスイッチの**Actions**カラムで**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

スイッチ情報を更新する

このタスクについて

ユーザー名とパスワードがスイッチのものと一致し、スイッチが認証を通過できるように、UniSystemでスイッチのユーザー名とパスワードを更新できます。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. 編集するスイッチの**Actions**カラムで**Edit**をクリックします。
3. 関連情報を入力し、**OK**をクリックします。

スイッチの検索

このタスクについて

名前、IP、およびその他の情報でスイッチを検索するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. 検索領域で、検索基準を選択し、検索キーワードを入力します。使用可能な検索基準は、デバイス名、IPアドレス、接続状態、CPU使用率およびメモリー使用量です。

キャビネットの詳細を表示する

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. ノードの場所列のキャビネット名のリンクをクリックします。キャビネットの詳細を表示します。

スイッチの詳細の表示

スイッチの概要、カード、ポート、およびインターフェイス情報の表示

このタスクについて

Switch Detailsページにアクセスするには、次の作業を実行します。このページには次のタブがあります。

- **Summary**:デバイス名、モデル、バージョン、管理IPアドレスなど、スイッチの基本情報を表示します。
- **Cards**:カード名、モデル、ステータス、CPU使用率、メモリー使用率など、スイッチ上のカードに関する情報を表示します。
- **Ports**: スイッチの物理イーサネットおよびFCポートに関する情報を表示します。このタブには、各物理ポートのPVID、リンクタイプ、MACアドレス、トラフィック統計情報、およびピアエンド情報が表示されます。
- I**nterfaces**:スイッチのカード上の論理インターフェイスに関する情報を表示します。サポートされている論理インターフェイスタイプには、レイヤ2/レイヤ3集約インターフェイス、VLANインターフェイス、ループバックインターフェイス、ヌルインターフェイス、InLoopbackインターフェイス、Register-Tunnelインターフェイス、VFCインターフェイス、およびHDLCリンクバンドルインターフェイスがあります。このタブには、各インターフェイスの名前、ステータス、IPアドレス、インターフェイスタイプ、およびその他の情報が表示されます。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. スイッチのデバイス名をクリックすると、詳細ページが表示されます。
3. **Summary**、**Cards**、**Ports**、または**Interfaces**タブをクリックして、スイッチに対応する情報を表示します。

図99 Switch Detailsページ



4. (任意) スイッチの名前を変更するには、**Summary**タブのデバイス名の横にある**Rename**アイコンをクリックします。表示されたダイアログボックスで、新しいデバイス名を入力し、**OK**をクリックします。

ポートまたはインターフェイスのトラフィック統計情報の表示

このタスクについて

送受信されたパケット数、パケットドロップ統計情報など、スイッチカード上の物理ポートまたは論理インターフェイスのトラフィック統計情報を表示するには、次の作業を実行します。

手順

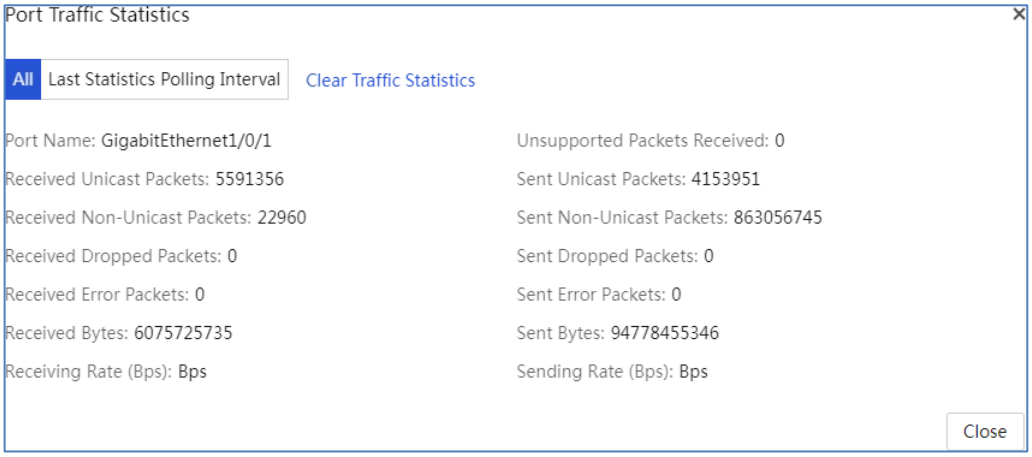
1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. スイッチのデバイス名をクリックすると、詳細ページが表示されます。
3. Portsタブまたは**Interfaces**タブをクリックし、ポートまたはインターフェイスの**Actions**カラムで**Traffic Details**をクリックします。

メモ:

スイッチ上のインターフェイスでは、集約インターフェイスに関する詳細なトラフィック統計情報だけを表示できます。

4. **Last Statistics Polling Interval**をクリックして、最後のポーリング間隔中にポートまたはインターフェイスに対して収集されたトラフィック統計情報を表示します。デフォルトのポーリング間隔は300秒です。

図100 インターフェイストラフィック統計情報



スイッチラベルの管理

スイッチラベルを追加、削除、および編集するには、次の作業を実行します。

スイッチラベルを追加する

必要に応じて、管理を容易にするためにスイッチにラベルを割り当てることができます。最大1000個のスイッチラベルを追加できます。

手順

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. **Manage Labels**をクリックし、**Create Label**を選択します。
3. 表示されるダイアログボックスで、関連する情報を入力し、**OK**をクリックします。

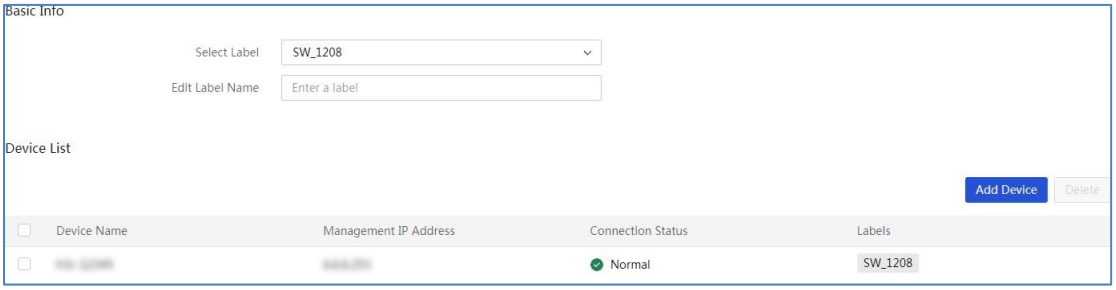
図101 スイッチラベルの追加



スイッチラベルを編集する

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. **Manage Labels**をクリックし、**Edit Label**を選択します。
3. **Basic Info**領域で、編集するラベルを選択し、新しいラベル名を入力します。
4. **Device List**領域で、**Add**をクリックして、このラベルを割り当てるデバイスを選択します。
5. 1つ以上のデバイスからラベルを削除するには、デバイスリストでデバイスを選択し、**Delete**をクリックします。
6. **OK**をクリックします。

図102 スイッチラベルの編集



スイッチラベルを削除する

1. ナビゲーションペインで、**Menu>Devices>Switches**を選択します。
2. **Labels**をクリックします。**Delete Label**をクリックします。
3. 表示されたダイアログボックスで、削除するラベルを選択し、**OK**をクリックします。

インフラストラクチャ

UniSystemは、分散型Cooling Distribution Unit(CDU)、集中型CDU、浸漬冷却型CDU、環境監視ホスト、リアドア熱交換器、およびノースバウンドインターフェイスとしてModbus TCPを使用するその他のデバイスなどのインフラストラクチャの管理をサポートしています。

- UniSystemが提供する事前設定された監視テンプレートCDU5204(分散)、ColdPlateCDU(集中)、およびImmersionCDU(浸漬冷却)を使用して、デバイスのIPアドレスと名前を入力することにより、デバイスをUniSystemに追加できます。
- また、UniSystemでは、Modbus TCPをノースバウンドインターフェイスとして使用する環境監視ホスト、リアドア熱交換器、およびその他のデバイスを管理するためのカスタム監視テンプレートの追加もサポートしています。カスタム監視テンプレートの追加の詳細については、「カスタム監視テンプレートの管理」を参照してください。

インフラストラクチャの管理

制約事項とガイドライン

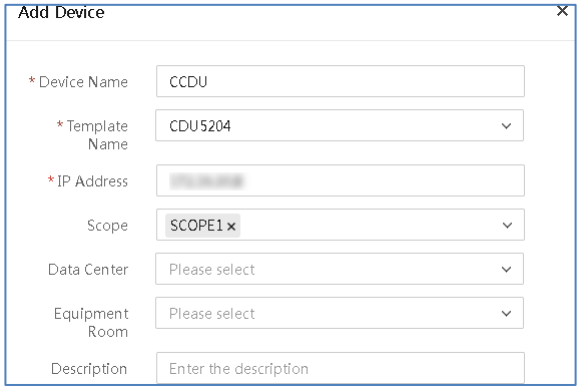
デバイス名は大文字と小文字が区別されます。デバイス名がインフラストラクチャリスト内で一意であることを確認し、リスト内のデバイスのIPアドレスとポート番号の組合せが異なることを確認してください。デバイス名またはIPアドレスとポート番号の組合せがすでに存在する場合、デバイスの追加操作は失敗します。

対応するインフラストラクチャがキャビン管理に追加されている場合は、デバイスを追加できません。

手順

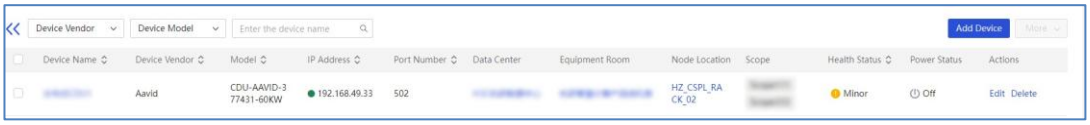
1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. **Add Device**をクリックします。表示されるダイアログボックスで、次の作業を実行します。
   a. デバイス名を入力します。
   b. テンプレートを選択します。内蔵のCDU5204テンプレートは、AavidベンダーのCDU-AAVID-377431-60KWデバイスにのみ適用できます。
   c. デバイス管理ポートのIPアドレスを入力します。
   d. スコープを選択します。
   e. (オプション)対応するデータセンターと機器室を選択し、説明を入力します。
3. **OK**をクリックします。

図103 CDUデバイスの追加



4. デバイスが正常に追加されると、図104に示すように、デバイス名、製造元、モデル、IPアドレス、ポート番号、ヘルスステータス、電源ステータスなど、CDUデバイスリストにインフラストラクチャのサマリーステータスと詳細が表示されます。

図104 CDUデバイスリスト



5. (任意)デバイスを編集または削除するには、デバイスの**Actions**カラムで**Edit**または**Delete**をクリックします。
6. (任意)リスト内のデバイスをフィルタリングするには、デバイスのベンダーとモデルを選択し、デバイス名のキーワードを入力します。

パラメータ

- **Device Name**: デバイスを追加するときは、デバイス名を入力する必要があります。名前は1～30文字の文字列で、大文字と小文字が区別されます。サポートされているのは、漢字、数字、文字、アンダースコア(_)およびハイフン(-)のみです。
- **Template Name**: デバイスにバインドされているモニタリングテンプレート。
- **IP Address**: デバイスの管理ポートのIPアドレス。IPv4アドレスだけがサポートされます。
- **Scope**: 追加するデバイスが属するスコープ。
- **Data Center**: デバイスが属するデータセンター。このフィールドはオプションです。
- **Equipment Room**: デバイスが存在する機器室。機器室を指定する場合は、対応するデータセンターも指定する必要があります。
- **Description**: デバイスの説明。説明の長さは64文字以内で、スペースで開始または終了することはできません。中国語の文字、数字、文字、アンダースコア(_)およびスペースのみがサポートされています。このフィールドはオプションです。

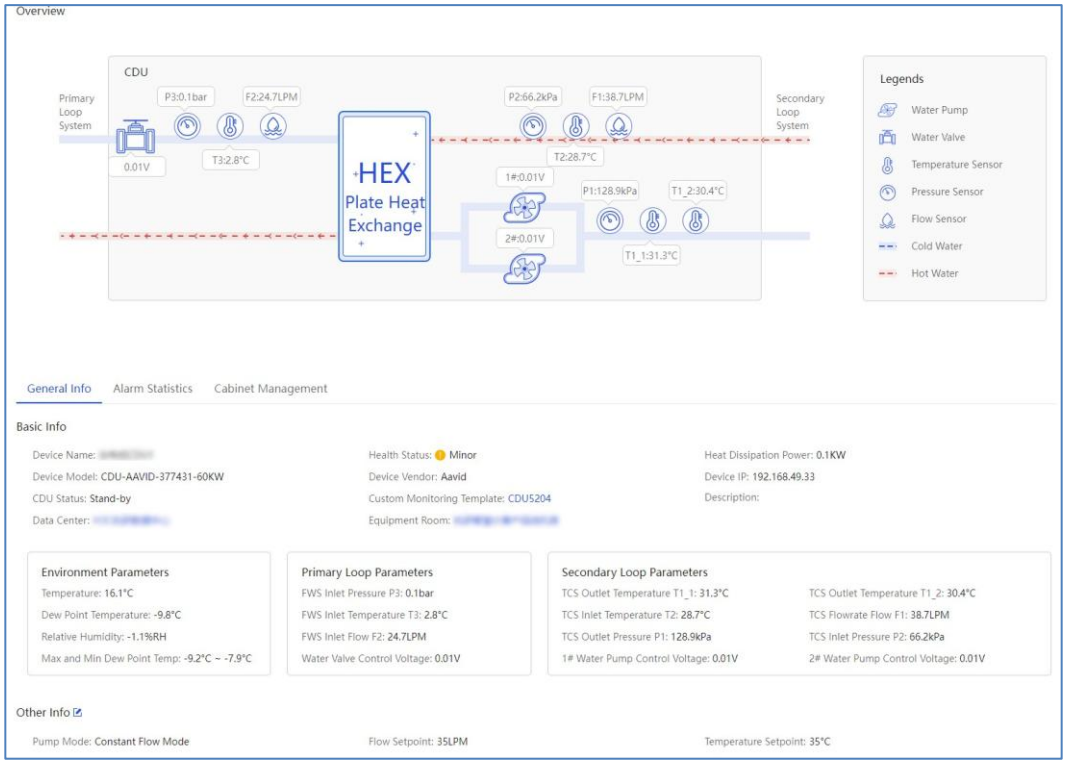
インフラストラクチャの詳細を表示

概要図、一般情報、アラーム統計情報など、インフラストラクチャデバイスに関する詳細情報を表示し、キャビネット管理を実行するには、次の作業を実行します。

インフラストラクチャ全体のステータスを表示

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. 図105に示すように、ターゲットデバイスの名前リンクをクリックして、その詳細を表示します。

図105 インフラストラクチャの詳細



3. 概要図と一般情報を表示します。

インフラストラクチャアラームの統計情報を表示する

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスの名前リンクをクリックすると、詳細が表示されます。
3. **Alarm Statistics**タブをクリックして、アラーム統計情報を表示します。
4. アラーム統計情報をクリアするには、**Alarm Clear**をクリックします。

キャビネット管理

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスの名前リンクをクリックすると、詳細が表示されます。
3. **Cabinet Management**タブをクリックします。インフラストラクチャに関連付けられているキャビネットのリストを表示できます。
4. キャビネットの詳細を表示するには、キャビネット名のリンクをクリックします。
5. キャビネットにデバイスを追加するには、**Bind Cabinet**をクリックします。操作方法はデバイスの種類によって異なります。
   - 集中型CDUおよび浸漬冷却型CDUの場合は、確認のダイアログボックスが表示されます。ターゲットキャビネットを選択し、**OK**をクリックします。
   - 分散CDUの場合は、キャビネットの詳細ページが開きます。キャビネットビューのボタンをクリックし、表示されたダイアログボックスにCDU情報を入力して**OK**をクリックします。
6. キャビネットからデバイスを削除するには、**Unbind**をクリックします。バインド解除操作は、デバイスのタイプによって異なります。
   - 集中CDUおよび浸漬冷却CDUの場合は、確認ダイアログボックスが表示されます。

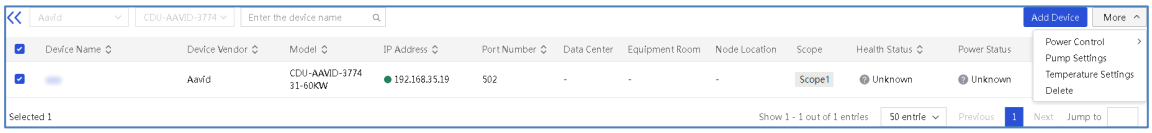
ダイアログボックスで**OK**をクリックします。

- 分散CDUの場合は、キャビネットの詳細ページが開きます。**Actions**列の**Delete**をクリックして、ターゲットデバイスを削除します。

インフラストラクチャデバイスのより多くのオプション

UniSystemは、デバイスの電源、水ポンプ、温度の制御、デバイスの一括削除など、インフラストラクチャデバイスの一括リモート管理をサポートします。

図106 Moreをクリック



電源操作の実行

このモジュールを使用すると、インフラストラクチャデバイスの電源ステータスをリモートで制御できます。

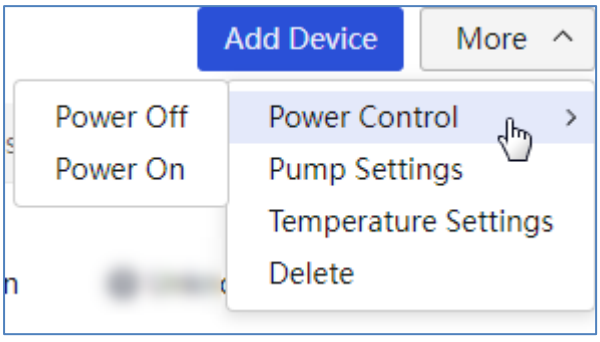
制約事項とガイドライン

電源管理操作を正常に実行するには、テクニカルサポートの指示に従って、カスタム監視テンプレートでPowerStatus、PowerOn、およびPowerOffセンサーを正しく設定します。これらのセンサーは、電源管理機能を実装するために重要です。

手順

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスを選択して**More**をクリックし、**Power Control**を選択して電源アクションをクリックします。

図107 電源操作の実行



3. 表示されるダイアログボックスで、管理するデバイスを確認し、ユーザー通知に同意することを選択して、**OK**をクリックします。

ポンプを設定する

このモジュールを使用すると、インフラストラクチャデバイス上で水ポンプをリモートで一括設定できます。

制約事項とガイドライン

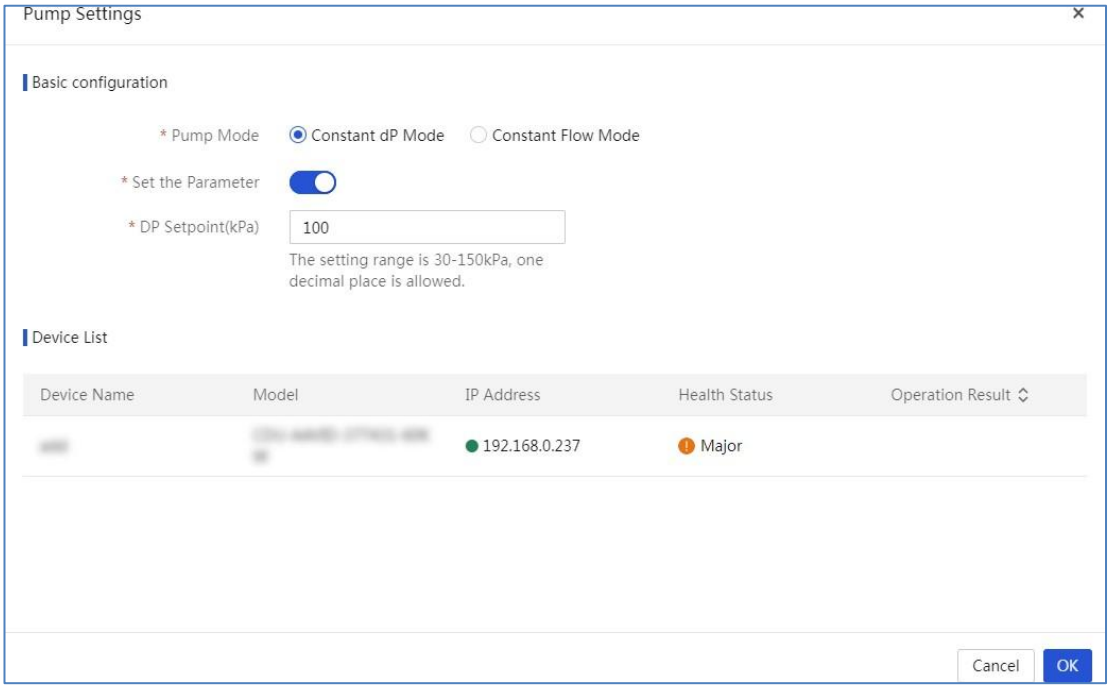
ポンプの設定をサポートしているのは、AavidベンダーのCDU-AAVID-377431-60KWデバイスだけです。

手順

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。

2. ターゲットデバイスを選択して**More**をクリックし、次に**Pump Settings**をクリックします。
3. 表示されたダイアログボックスで、ポンプの設定を行い、**OK**をクリックします。

図108 ポンプの構成



温度設定の構成

このモジュールを使用すると、インフラストラクチャデバイスの温度設定をリモートで一括して設定できます。

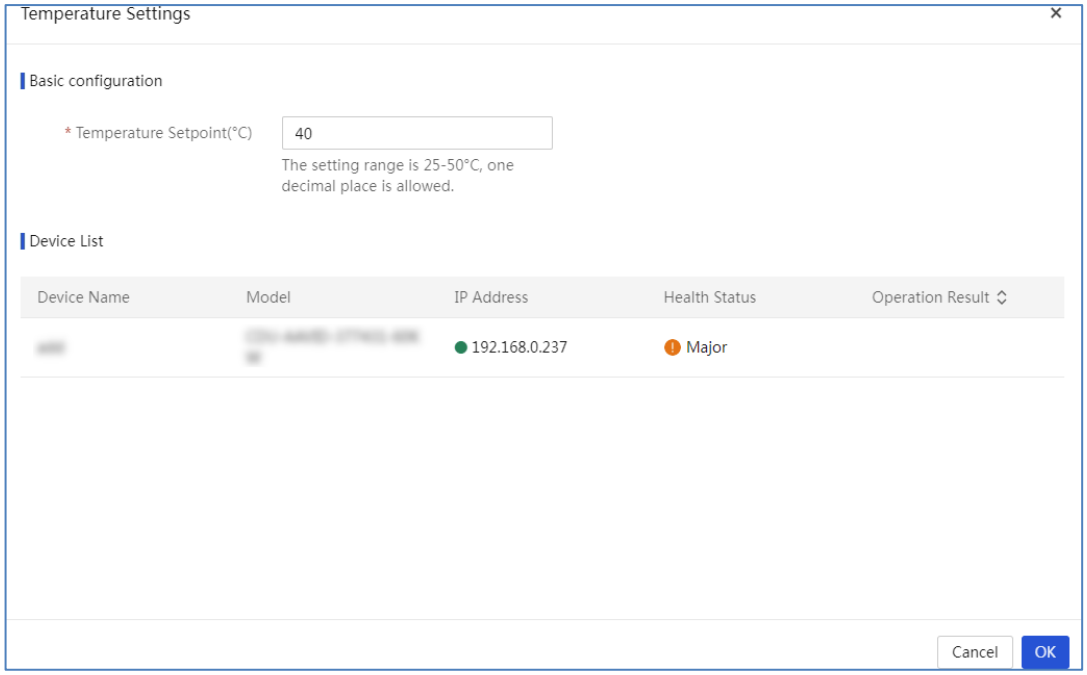
制約事項とガイドライン

温度設定をサポートしているのは、AavidベンダーのCDU-AAVID-377431-60KWデバイスだけです。

手順

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスを選択し、**More**をクリックしてから**Temperature Settings**をクリックします。
3. 表示されたダイアログボックスで、温度設定点を設定し、**OK**をクリックします。

図109 温度設定の構成



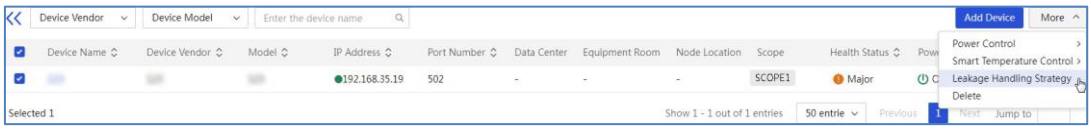
リーケージ処理戦略を構成する

この関数は、動的環境ホストのリーク処理方針を構成します。監視対象のキャビネットがリークアラームをトリガーすると、UniSystemは構成された方針に基づいてアクションを実行します。自動シャットダウンが選択されている場合、UniSystemはホストのソレノイドバルブを自動的に閉じて、リークの拡大や機器の損傷を防ぎます。

手順

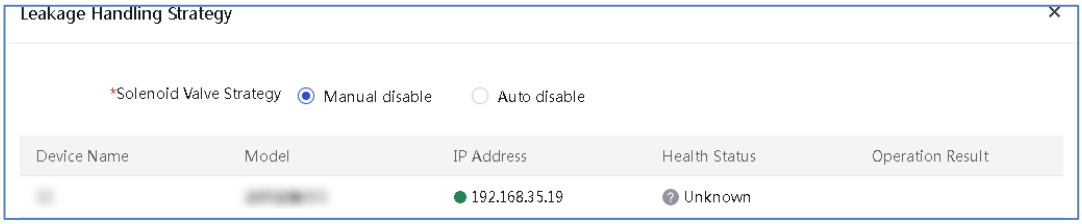
1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスを選択し、**More**をクリックしてから、**Leakage Handling Strategy**をクリックします。

図110 リーケージ処理方針



3. 表示されるダイアログボックスで、ソレノイドバルブストラテジーを選択します。

図111 ソレノイドバルブストラテジー



4. **OK**をクリックします。

スマート温度制御の設定

メモ:

この機能をサポートしているのは、H3C UniServer R5500 G7コールドプレートベースのサーバーだけです。

環境モニタリングシステムのスマート温度制御を有効または無効にするには、次の作業を実行します。この機能を有効にすると、システムと同じキャビネット内のコールドプレートベースのサーバーの温度が変化したときに、UniSystemはシステムによって制御されるバルブの開度をインテリジェントに調整して、液体冷却の消費電力を節約します。

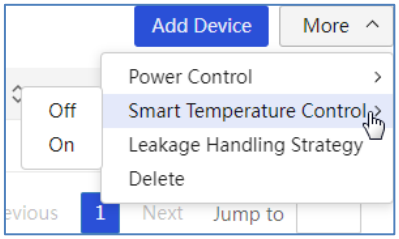
前提条件

この機能を有効にする前に、環境監視ホストの監視テンプレートでソレノイドバルブ開度センサーを構成してください。詳細については、「カスタム監視テンプレートの管理」を参照してください。

手順

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスを選択し、**More**をクリックして、**Smart Temperature Control**をクリックします。

図112 スマート温度制御の構成

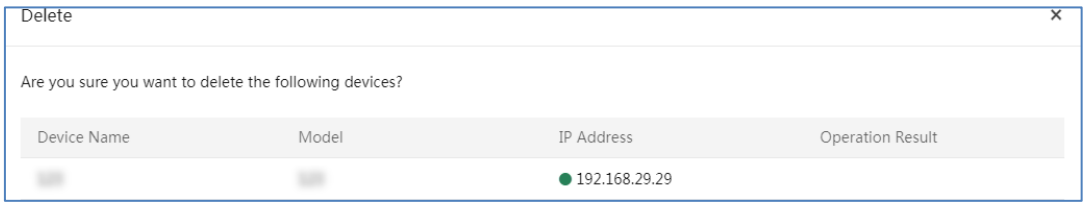


3. OKをクリックします。

デバイスを削除する

1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Infrastructure**を選択します。
2. ターゲットデバイスを選択し、**More**をクリックしてから**Delete**をクリックします。
3. 表示された確認ダイアログボックスで、**OK**をクリックします。

図113 デバイスの削除

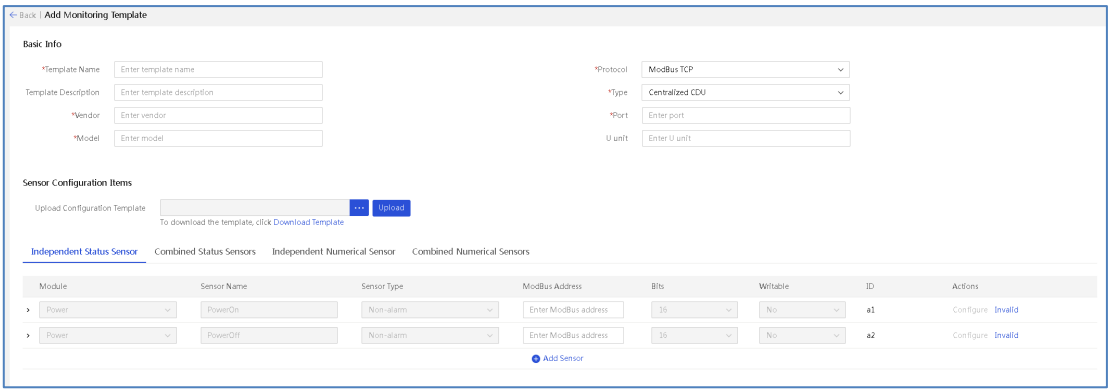


カスタム監視テンプレートの管理

手順

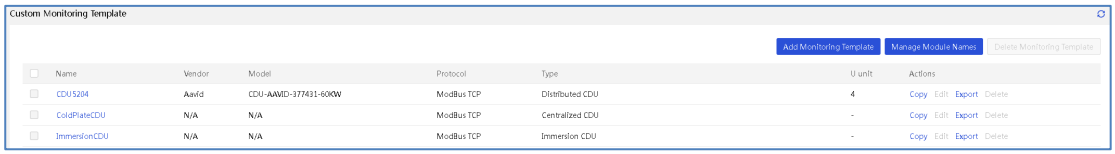
1. ナビゲーションペインで、**Menu>Devices>Manage Infrastructure>Custom Monitoring Template**を選択します。
2. **Add Monitoring Template**をクリックします。次に、基本情報とセンサー設定を設定します。
3. (オプション)**Download Template**をクリックして、カスタム監視テンプレート(.xlsxまたは.xls形式)をダウンロードします。テンプレートに入力してからアップロードします。

図114 カスタム監視テンプレートの追加



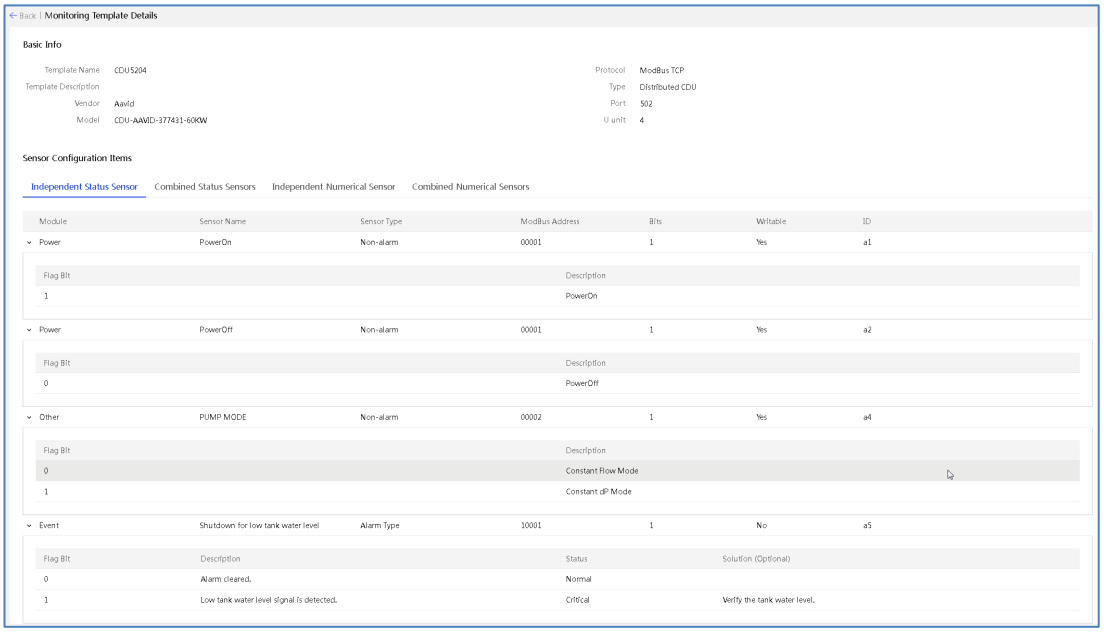
4. **OK**をクリックします。カスタム監視テンプレートリストに、正常に追加されたテンプレートに関する情報が表示されます。

図115 カスタム監視テンプレートリスト



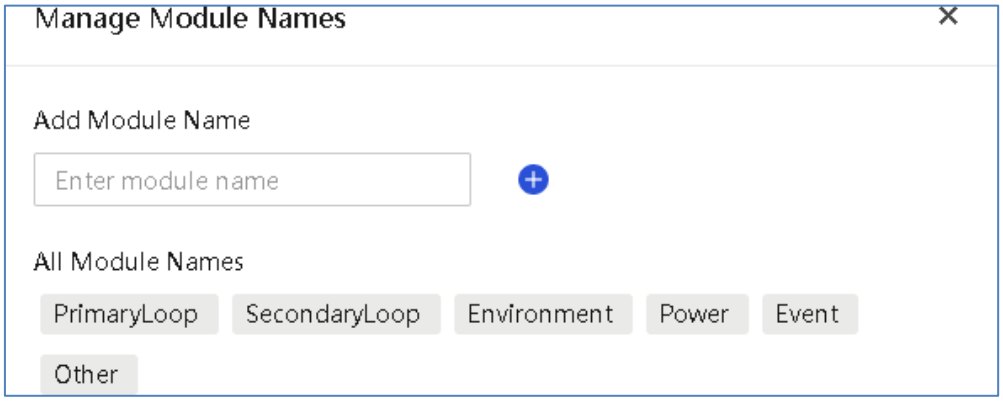
5. 監視テンプレートの詳細を表示するには、テンプレートの名前リンクをクリックします。

図116 カスタム監視テンプレート



6. モジュール名を管理するには、**Manage Module Names**をクリックします。表示されたダイアログボックスで、必要な情報を入力し、**OK**をクリックします。

図117 モジュール名の管理



7. 既存のテンプレートの設定を継承するテンプレートを作成する場合、またはテンプレートを編集または削除する場合は、**Actions**カラムで**Inherit Create**, **Edit**, または **Delete**をクリックします。

パラメータ

基本情報

- **Template Name**: 監視テンプレートの名前。名前は、大文字と小文字が区別される1文字から30文字の文字列です。サポートされているのは、漢字、数字、文字およびアンダースコア(_)のみです。
- **Template Description**: 監視テンプレートの説明。0から30文字の大/小文字を区別する文字列です。文字列の先頭または末尾にスペースを使用することはできません。サポートされ

ているのは、漢字、数字、文字、アンダースコア(_)およびスペースのみです。

- **Vendor**: 互換性のあるデバイスの製造元。大文字と小文字が区別され、1文字から30文字までの文字列です。サポートされているのは、中国語の文字、数字、文字およびアンダースコア(_)のみです。
- **Model**: 互換性のあるデバイスのモデル。大文字と小文字を区別し、1～30文字で指定します。サポートされているのは、漢字、数字、文字、アンダースコア(_)、ハイフン(-)、およびドット(.)だけです。
- **Protocol**: 互換性のあるデバイスのプロトコル。ModBus TCPプロトコルのみがサポートされています。
- **Type**: 互換性のあるデバイスのタイプ。オプションには、集中型CDU、分散型CDU、浸漬型CDU、リアドア熱交換器、および環境モニタリングホストがあります。
- **Port**: 互換性のあるデバイスのポート番号。
- **U Unit**: 互換性のあるデバイスのU位置。1～100の範囲の整数です。このフィールドは、分散CDUおよび環境モニタリングホストでは必須です。

独立したステータスセンサー

- **Module**: センサーが属するモジュール。モジュールが作成されていることを確認します。カスタムデバイス詳細では、アラームセンサーおよび電源センサーを除くすべてのセンサーが、それぞれのモジュールに分類されます。
- **Sensor Name**: 追加するセンサーの名前。1文字から100文字までの文字列で、大文字と小文字が区別されます。このフィールドは必須です。
- **Sensor Type**: センサーのタイプ(アラームまたは非アラーム)。
- **ModBus Address**: 追加するセンサーのModBusアドレス。5桁と6桁の両方のModBusアドレスがサポートされます。
- 5桁のアドレスは、00001～09999、10001～19999、30001～39999、または40001～49999の範囲である必要があります。
- 6桁のアドレスは、000001～065536、100001～165536、300001～365536、または400001～465536の範囲である必要があります。
- **Bits**: 追加するセンサーのビット番号。1ビットはコイル、16ビットはレジスタを表します。正しいModBusアドレスに基づいて、センサーのビット数を決定します。
- **Writable**: センサーが書き込み可能かどうかを示します。
- **ID**: センサーに対応するID(カスタムエクスプレッションの計算に使用)。
- **Valid Bits**: **Bits**フィールドで16ビットレジスタを選択した場合は、すべてのビットを選択するか、0～15の特定のビットを有効なビットとして選択できます。
- **Flag Bit**: 選択した有効ビットで表される実際の読取り値。16進文字列および文字列**other**のみがサポートされます。フラグビットは重複しないようにする必要があります。フラグビット値を**other**に設定すると、結果が他のフラグビットと一致しない場合、その結果は**other**フラグビットに分類されます。また、デバイス詳細ページのセンサー設定で**other**フラグビットを選択することはできません。
- **Description**: 追加するフラグビットの説明。1文字から200文字の範囲の文字列です。このフィールドは必須です。
- **State**: 追加されるフラグビットの状態。標準、マイナー、メジャーおよびクリティカルのみがサポートされます。このフィールドは、アラームセンサーに対してのみ使用可能です。
- **Solution**: 追加されるフラグビットで表される条件の解決(0から200文字の文字列)。このフィールドは、アラームセンサーに対してのみ使用でき、スペースのみを含めることはできません。
- 複合ステータスセンサー

- **Module**:センサーが属するモジュール。モジュールが作成されていることを確認します。カスタムデバイスの詳細では、すべてのセンサーがそれぞれのモジュールに分類されます。
- **Sensor Name**: 追加するセンサーの名前。1文字から100文字までの文字列で、大文字と小文字が区別されます。このフィールドは必須です。
- **Flag Bit**: カスタム式に対応する結果。16進文字列および文字列**other**のみがサポートされます。フラグビットは重複しないようにする必要があります。フラグビット値を**other**に設定すると、結果が他のフラグビットと一致しない場合、その結果は**other**フラグビットに分類されます。また、デバイス詳細ページのセンサー設定で**other**フラグビットを選択することはできません。
- **State**: 追加するセンサーの状態。標準、マイナー、メジャーおよびクリティカルのみがサポートされます。
- **Description**: 追加するセンサーの説明。1文字から200文字の範囲の文字列です。このフィールドは必須です。
- **Solution**: 追加するセンサーによって表される条件の解決策。0～200文字の文字列です。このフィールドにスペースのみを含めることはできません。
- **Custom Expression**: 異なる状態アラームセンサーのIDと数値の組み合わせの式。演算子()~+-*/&>><<のみがサポートされています。式は120文字以内で、最大32個のセンサーIDと数字を含めることができます。複合ステータスセンサーのカスタム式を設定する場合、すでに設定されているステータスセンサーのみを選択できます。

独立した数値センサー

- **Module**: センサーが属するモジュール。モジュールが作成されていることを確認します。カスタムデバイスの詳細では、すべてのセンサーがそれぞれのモジュールに分類されます。
- **Sensor Name**: 追加するセンサーの名前。1文字から100文字までの文字列で、大文字と小文字が区別されます。このフィールドは必須です。
- **ModBus Address**: 追加するセンサーのModBusアドレス。5桁と6桁の両方のアドレスがサポートされています。5桁のアドレスは、30001～39999の範囲である必要があります。
  40001-49999。6桁のアドレスは、300001-365536または400001-465536の範囲である必要があります。
- **Bits**: 追加するセンサーのビット数です。16ビットは1つのレジスタが1つの独立した数値センサーを表すことを示し、32ビットは2つのレジスタが1つの独立した数値センサーを表すことを示します。ModBusアドレスが39999、49999、365536、465536の場合、Bitsを32に設定することはできません。
- **Value Type**: 追加するセンサーの値のタイプ。整数と浮動小数点の両方のタイプがサポートされています。浮動小数点のタイプは、Bitsフィールドが32に設定されている場合にのみ使用できます。Bitsフィールドが16に設定されている場合、値のタイプは整数に固定されます。
- **With Symbol:** 追加するセンサーの値が符号付き数値かどうかを指定します。このフィールドは、Value TypeフィールドがIntegerに設定されている場合にだけ使用できます。
- **Decimal Precision**: センサーの値の小数点以下の桁数。小数点以下5桁までがサポートされています。このフィールドは、Bitsフィールドが32に設定され、Value Typeが浮動小数点の場合にのみ使用できます。
- **High Byte Position**: Bitsフィールドが32の場合(2つの16ビットレジスタが1つのセンサーを表すことを意味します)、どのレジスタの値が上位にあるかを示します。
- **Scale Factor**: レジスタから読み込んだ値に適用する乗数。0(除く)～100(含む)の範囲で指定します。小数点以下5桁まで指定できます。
- **Unit**: 追加するセンサーの単位。0～10文字の範囲の文字列です。文字列にスペースだ

けを含めることはできません。

- **Writable**: センサーのModBusアドレスに数字を書き込むことができるかどうかを指定します。このフィールドは、ModBusアドレスが40001～49999または400001～465536の範囲にある場合にだけ使用できます。
- **Limit Range**: センサーが書込み可能に設定されている場合の書込み可能な値の上限および下限。デフォルトは、値タイプでサポートされている上限および下限です。カスタム値および科学表記がサポートされています。

複合数値センサー

- **Module**: センサーが属するモジュール。モジュールが作成されていることを確認します。カスタムデバイスの詳細では、すべてのセンサーがそれぞれのモジュールに分類されます。
- **Sensor Name**: 追加するセンサーの名前。1文字から100文字までの文字列で、大文字と小文字が区別されます。このフィールドは必須です。
- **Unit**: 追加するセンサーの単位。0～10文字の範囲の文字列です。文字列にスペースだけを含めることはできません。
- **Decimal Precision**: センサーの値の小数点以下の桁数。小数点以下5桁までがサポートされています。このフィールドは、Bitsフィールドが32に設定され、Value Typeが浮動小数点の場合にのみ使用できます。
- **Custom Expression**: 独立したセンサー値と、このセンサーより前の複合センサーIDを組み合せた式。演算子()+-*/のみがサポートされています。式は120文字以内で、最大32個のセンサーIDと数字を含めることができます。複合数値センサーのカスタム式を構成する場合、すでに構成されている数値センサーのみを選択できます。

制約事項とガイドライン

- システムには、CDU5204、ColdPlateCDU、およびImmersionCDUの3つのデフォルトテンプレートが付属しており、これらは編集または削除できません。
- 重複した名前のテンプレートは追加できません。
- 同じベンダーとモデルのテンプレートを追加することはできません。
- 同じ名前のセンサーをテンプレート内に追加することはできません。
- PowerOnセンサーとPowerOffセンサー(電源装置の独立したステータスセンサー)は、大文字と小文字が区別されません。これらのセンサーはカスタムデバイスリストに表示され、操作される必要があるため、他のセンサーをこの名前にバインドすることはできません。センサーは独立したステータスセンサー。センサーがアクティブかどうかを設定する必要があります。センサーがアクティブな場合は、センサーの値も入力する必要があります。PowerOnおよびPowerOffセンサーのModBusアドレスは、00001～09999、40001～49999、000001～065536、または400001～465536の範囲である必要があります。フラグビットは**other**.にはできません。
- PowerStatusセンサー(電源装置の複合ステータスセンサー)は、大文字と小文字が区別されず、複合ステータスセンサーとしてのみ使用できます。センサーがアクティブかどうかを構成する必要があります。センサーがアクティブな場合は、センサーのカスタム式とフラグビットも入力する必要があります。
- 環境モニタリングホストデバイスタイプのモニタリングテンプレートを追加すると、ソレノイドオフ(ソレノイドバルブセンサー)、漏れ液体(漏れアラームセンサー)、およびソレノイド値(ソレノイドバルブセンサー)が予約済みセンサーとして自動的に表示されます。テンプレートの追加に失敗しないようにするには、センサーがアクティブなときにセンサー関連パラメータを設定する必要があります。
    - **SolenoidOff sensor**: デフォルトのモジュールは**other**で、他のセンサーと共有できない固定センサー名が付いています。デフォルトのセンサータイプは、編集不可、非アラームセンサーです。センサーのModBusアドレスは、40001～49999または400001～465536の範囲である必要があります。センサーは、2つのフラグビットの設定をサポートしています。リーク処理ポリシーを有効にするには、センサーが有効で適切に設定されていること、説明ソレノイドオフのフラ

グビットが0に設定されていること、説明ソレノイドオンのフラグビットが1に設定されていることを確認します。

- **LeakageLiquid sensor**: 環境モニタリングホスト用の専用モニタリングテンプレート。センサーはデフォルトでアラームモジュールに属し、固定された名前を持ちます。他のセンサーは同じ名前を使用できません。デフォルトのタイプはalarmで、センサーのModBusアドレスは40001～49999または400001～465536の範囲である必要があります。有効ビットとして0～15のビットを選択した場合、フラグビットを**other**に設定することはできません。フラグビットは1および0に設定する必要があります。0はリークアラームがクリアされたことを示し、1はリークアラームがトリガーされたことを示します。すべてのビットを有効ビットとして選択した場合、フラグビットは0、1、2、および3に設定できます。0はリークアラームがクリアされたことを示し、他の3つの値はリークアラームがトリガーされたことを示します。リーク処理ポリシーを有効にするには、センサーが有効であり、適切に設定されていることを確認します。
- **SolenoidValue sensor**::環境モニタリングホスト専用のモニタリングテンプレートです。デフォルトのモジュールは**other**で、他のセンサーと共有できない固定センサー名を使用します。他のセンサーは同じ名前を使用できません。デフォルトのタイプは非アラームセンサーで、固定係数は1、値の範囲は0～100に制限されています。その他のパラメータは、環境モニタリングホストの設定に合わせて設定できます。センサーのModBusアドレスは、40001～49999または400001～465536の範囲である必要があります。Smart温度制御ポリシーを有効にするには、センサーが有効で適切に設定されていることを確認してください。

- 独立ステータスセンサーの状態を書き込み可能に設定するには、アドレスのModBusアドレスが10001～19999、30001～39999、100001～165536、または300001～365536の範囲にないことを確認します。
- 独立ステータスセンサーの場合、フラグビットを**other**に設定できるのは、**Bits**フィールドが16のときだけです。その他のフラグビットは1つまで設定できます。
- 独立したステータスセンサーには、少なくとも1つのフラグビットが必要です。フラグビットが1つしか存在しない場合、**other**にすることはできません。
- 独立ステータスセンサーのModBusアドレスが00001～09999、10001～19999、000001～065536、または100001～165536の範囲にある場合、**Bits**フィールドは1になります。
  アドレスが30001-39999、40001-49999、300001-365536、または400001-465536の範囲にある場合
  Bitsフィールドは16です。
- PowerOnおよびPowerOff以外のセンサーの場合、独立ステータスセンサーのModBusアドレスは、00001～09999、10001～19999、000001～065536、または100001～165536の範囲内であれば一意である必要があります。アドレスが30001～39999、40001～49999、300001～365536、または400001～465536の範囲内であれば、ModBusアドレスと有効ビットの組み合わせは一意である必要があります。
- 独立したステータスセンサーのModBusアドレスは、独立した数値センサーのModBusアドレスと重複してはいけません。
- 独立ステータスセンサーのビットが1の場合、フラグビットは0または1にしか設定できません。
- 独立ステータスセンサーのビットが16の場合、フラットビットを**other**、または0～FFFFの範囲の16進文字列に設定できます。
- 独立ステータスセンサーのフラグビットは一意である必要があります。
- 独立ステータスセンサーのタイプが非アラームの場合、センサーの説明は一意である必要があります。
- センサータイプ、ModBusアドレス、および独立ステータスセンサーのビットは、センサーの設定と密接に関連しています。センサータイプ、ビット、またはModBusアドレスの最初の桁を変更すると、現在の設定は自動的にクリアされます。

- 独立センサーのモジュールがアラームの場合、センサーモジュールはデフォルトでアラームタイプに設定されます。
- 結合されたステータスセンサーには厳密な順序があります。後で設定されたセンサーは、前に設定されたセンサーを選択できますが、前に設定されたセンサーは、後に設定されたセンサーを選択できません。
- 複合ステータスセンサーでサポートされる演算子は、()+-*/&>><<です。
- 複合数値センサーには厳密な順序があります。後で設定されたセンサーは、前に設定されたセンサーを選択できますが、前に設定されたセンサーは、後に設定されたセンサーを選択できません。
- 複合数値センサーによってサポートされる演算子には、()+-*/が含まれる。
- 結合ステータスセンサーにバインドされると、エクスプレッション内の対応するサブステータスセンサーは削除できなくなります。
- 複合数値センサーにバインドすると、エクスプレッション内の対応するサブ数値センサーは削除できなくなります。

データセンター管理

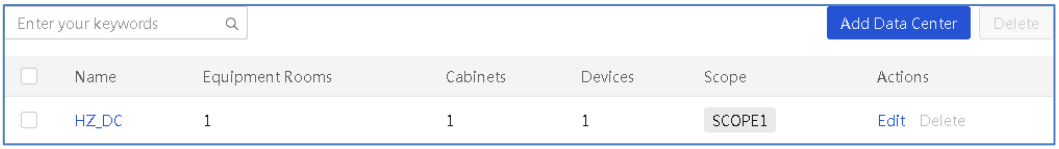
データセンターモジュールを使用すると、ユーザーは、サーバー、スイッチ、水冷装置(インフラストラクチャ)など、サポートされているデバイスを統一された方法で管理できます。これにより、ユーザーは、管理対象デバイスの稼働状態と温度状態をまとめて表示できます。ユーザーは、キャビネットの占有状態と電源状態を表示して、スペースを合理的に割り当て、電源リスクを適時に検出できます。

データセンター情報の表示

データセンターの概要を表示

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Data Center List**を選択します。
2. データセンターに関する概要情報を表示します。

図118 データセンターの概要の表示



データセンターの詳細の表示

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Data Center List**を選択します。
2. データセンターの詳細情報を表示するには、データセンター名をクリックします。

図119 データセンターの詳細の表示



データセンターの管理

データセンターを追加する

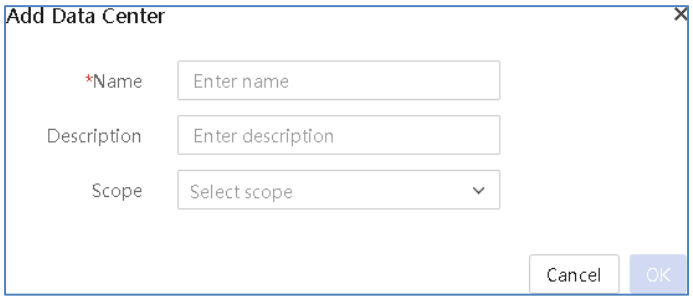
制約事項とガイドライン

データセンター名は一意である必要があります。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Data Center List**を選択します。
2. Add Data Centerをクリックします。表示されたダイアログボックスで、関連するパラメータを設定しわかりました。

図120 データセンターの追加



データセンターを編集する

制約事項とガイドライン

データセンター名は一意である必要があります。

手順

1. ナビゲーションペインで、**Menu>Devices>Data Center Management>Data Center List**を選択します。
2. データセンターの**Actions**列で**Edit**をクリックします。表示されたダイアログボックスで情報を編集し、**OK**をクリックします。

データセンターの削除

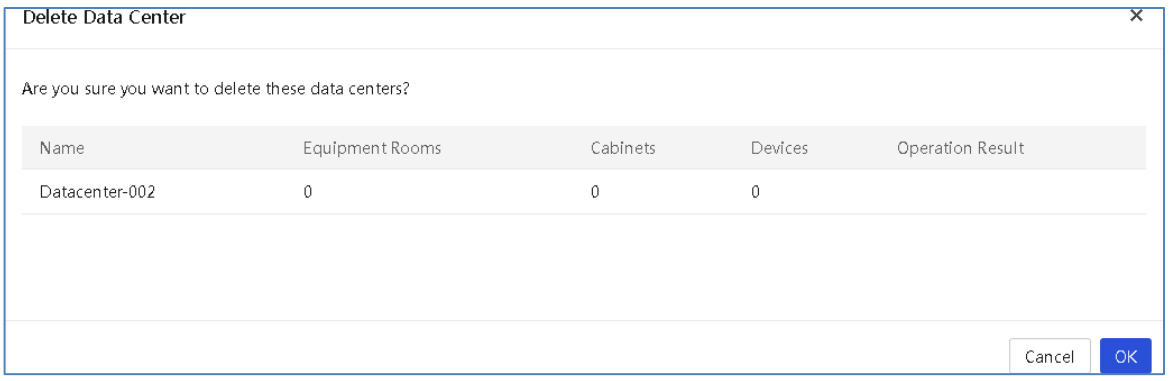
制約事項とガイドライン

機器室がデータセンターに追加されている場合、データセンターを直接削除することはできません。データセンターからすべての機器室を削除し、再度削除操作を実行してください。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Data Center List**を選択します。
2. データセンターをバッチで削除するには、ターゲットデータセンターを選択してDeleteをクリックします。表示されたダイアログボックスで、OKをクリックします。データセンターを削除するには、データセンターの**Actions**列で**Delete**をクリックします。

図121 データセンターの削除



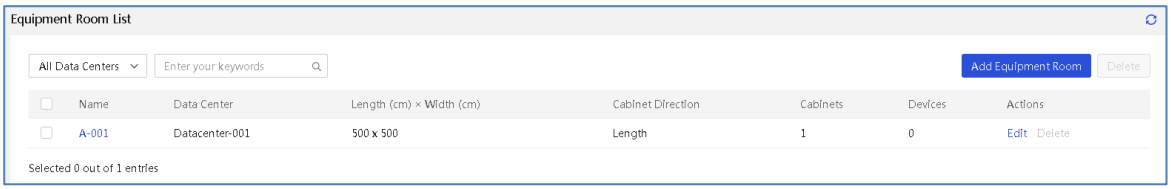
機器室情報を表示する

機器室の概要を表示する

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. 機器室に関する概要情報を表示します。

図122 機器室の概要の表示



機器室の詳細を表示する

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. 機器室の詳細情報を表示するには、機器室名をクリックします。

   機器室が属するデータセンターの**Data Center Details**ページで機器室名をクリックして、機器室の詳細を表示することもできます。

液体冷却フロー情報を表示する

この機能を使用すると、データセンターインフラストラクチャとキャビネット間の液体冷却フローに関する情報を表示できます。液体冷却フロービューでは、トポロジーマップを使用して、インフラストラクチャとキャビネット間の関連付け、およびインフラストラクチャ内のプライマリ側とセカンダリ側の温度センサーと圧力センサーに関連する情報が表示されます。

制約事項とガイドライン

キャビネットに関連付けられ、UniSystemの組み込みカスタム監視テンプレートによって管理されるインフラストラクチャのみが、トポロジーマップ機能をサポートします。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. ターゲット機器室の名前リンクをクリックして、詳細情報を表示します。
3. **Liquid Cooling Flow**タブをクリックして、情報を表示します。
4. (任意)キャビネットまたはインフラストラクチャに関する詳細情報を表示するには、フロートポロジマップでキャビネットまたはインフラストラクチャの名前をクリックします。
5. (オプション)ビューを拡大、縮小、または元の尺度にリセットするには、左上隅にある対応するアイコン  をクリックします。
6. (任意)センサー情報を表示するには、フロートポロジマップのパイプアイコンにカーソルを合わせます。
7. (任意)完全なインフラストラクチャ名、モデル、またはベンダー情報を表示するには、フロートポロジマップでインフラストラクチャの名前、モデル、またはベンダーにカーソルを合わせます。
8. (オプション)セカンダリ側の配管アイコン、インフラストラクチャ、またはキャビネットの上にカーソルを置くと、セカンダリ側の配管がハイライト表示されます。

機器室の管理

機器室を追加する

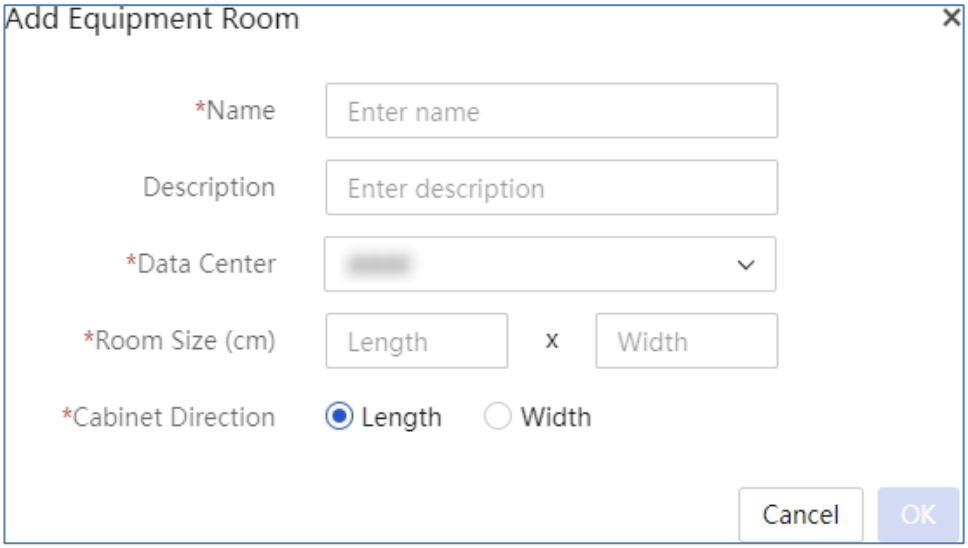
制約事項とガイドライン

機器室の名前は、データセンター内で一意である必要があります。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. **Add Equipment Room**をクリックします。表示されたダイアログボックスで機器室情報を設定し、OKをクリックします。

図123 機器室の追加



機器室を編集する

制約事項とガイドライン

- 機器室の名前は、データセンター内で一意である必要があります。
- 機器室の長さまたは幅を編集する場合は、編集後の機器室が追加したキャビネットを収容できることを確認してください。そうでない場合は、機器室のサイズを編集できません。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. 機器室の**Actions**列で**Edit**をクリックします。表示されたダイアログボックスで、部屋情報を編集し、**OK**をクリックします。

機器室を削除する

制約事項とガイドライン

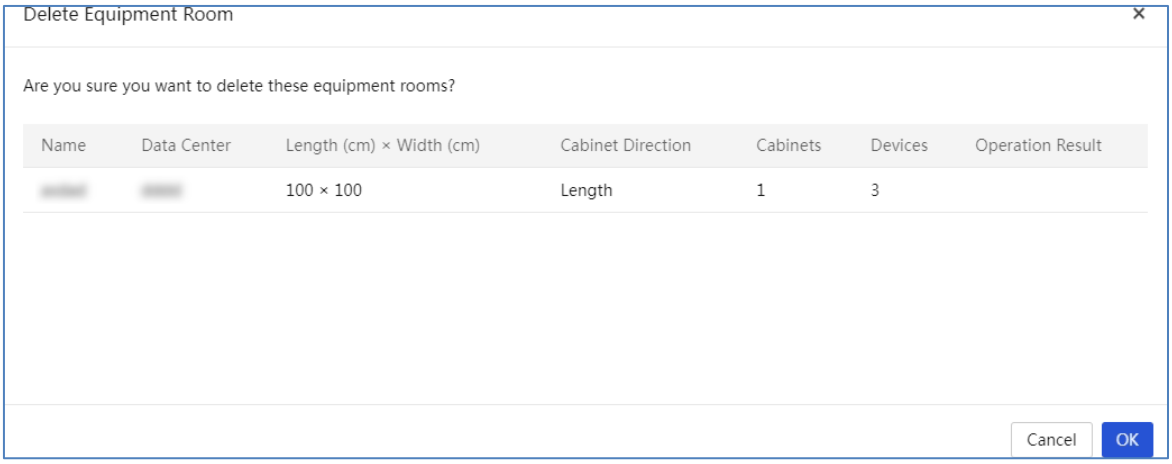
キャビネットが機器室に追加されている場合は、機器室を直接削除することはできません。機器室からすべてのキャビネットを削除し、削除操作を再度実行してください。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Equipment Room**を選択します。
2. 機器室をバッチで削除するには、対象の機器室を選択して**Delete**をクリックします。表示さ

れたダイアログボックスで**OK**をクリックします。機器室を削除するには、機器室の**Actions**列で**Delete**をクリックします。

図124 機器室の削除



パラメータ

- **Name**:機器室の名前。
- **Description**:機器室の摘要。このフィールドはオプションです。
- **Data Center**:機器室が属するデータセンター。
- **Room Size (cm)**:機器室の長さと幅。
- **Cabinet Direction**:機器室内のキャビネットの向き(縦または横)。

キャビネット情報の表示

制約事項とガイドライン

キャビネットのIPアドレスを変更する場合は、新しいIPアドレスが同様のデバイスのIPアドレスと競合していないことを確認してください。IPアドレスが競合している場合、デバイスが異常としてマークされ、電力および消費電力のデータが異常になる可能性があります。異常なデバイスが存在する場合は、それらを削除してから再度追加してください。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Cabinet**を選択します。
2. キャビネットに関する概要情報を表示します。
3. キャビネットの詳細情報を表示するには、キャビネット名をクリックします。

   機器室の詳細ページでキャビネット名をクリックして、キャビネットの詳細を表示することもできます。
4. (任意)関連付けられたインフラストラクチャに関する情報を表示するには、**Associated Infrastructure**タブをクリックします。

キャビネットの管理

キャビネットを追加する

制約事項とガイドライン

- キャビネットスペース情報には、キャビネットの座標とサイズが含まれています。データセンターは、

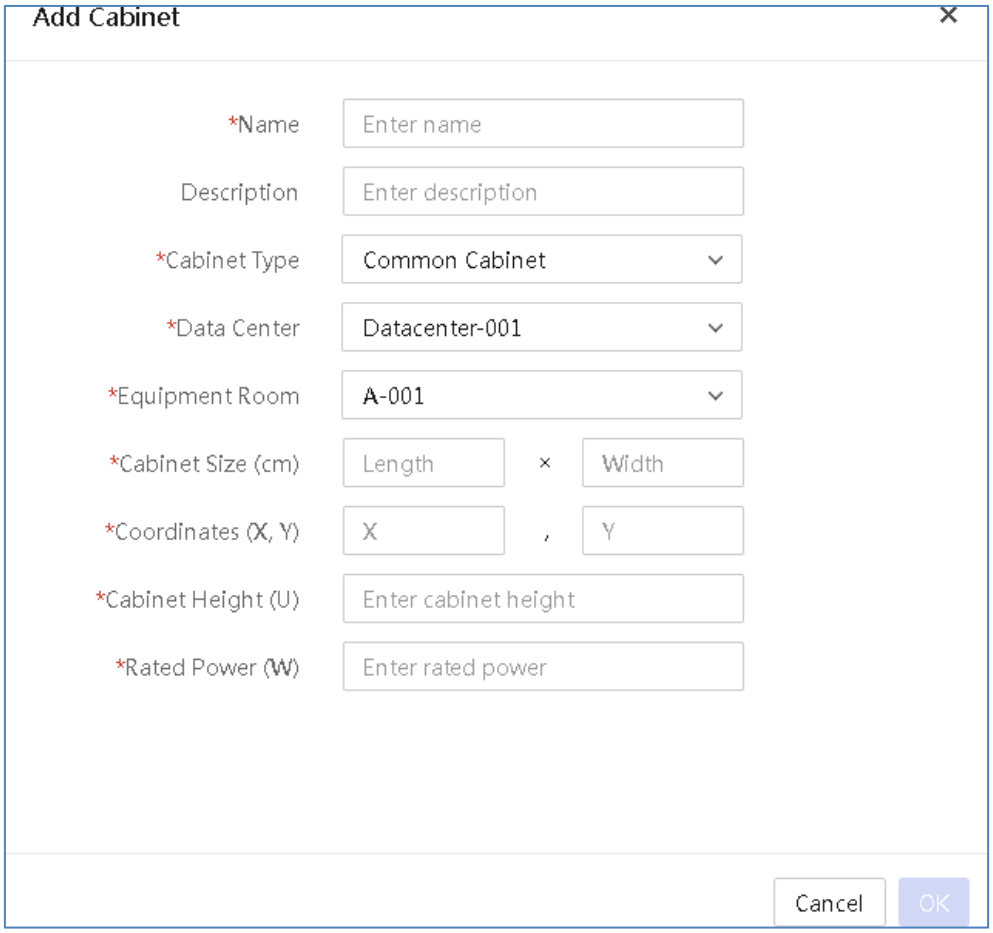
キャビネットスペース情報を検証して、キャビネットのスペースが他のキャビネットと競合していないか、スペースが許容範囲内にあるかを確認します。そうでない場合は、追加または編集操作を実行できません。

- キャビネット名は、機器室内で一意である必要があります。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Cabinet**を選択します。
2. キャビネットの追加をクリックします。表示されたダイアログボックスで、関連するパラメータを設定し、**OK**をクリックします。

図125キャビネットの追加



キャビネットの編集

制約事項とガイドライン

- キャビネットスペース情報には、キャビネットの座標とサイズが含まれています。データセンターは、キャビネットスペース情報を検証して、キャビネットのスペースが他のキャビネットと競合していないか、スペースが許容範囲内にあるかを確認します。そうでない場合は、追加または編集操作を実行できません。
- キャビネットで消費電力上限タスクが実行されている場合は、キャビネットを編集できません。
- キャビネットの定格電力を編集する場合は、新しい定格電力が、G6サーバー番号*150+非G6サーバーの合計予約電力の値より小さくならないようにしてください。そうしないと、キャビネットを編集できません。

- キャビネットの高さを編集する場合、では、新しい高さがキャビネット上の管理対象サーバーの高さ要件を満たしていることを確認します。満たしていない場合、キャビネットの高さは編集できません。
- キャビネットタイプを変更する前に、キャビネット内にデバイスが存在しないことを確認してください。キャビネット内にデバイスが存在する場合、変更は失敗します。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Cabinet**を選択します。
2. キャビネットの**Actions**」列で**Edit**をクリックします。表示されたダイアログボックスでキャビネット情報を編集し、**OK**をクリックします。

キャビネットの削除

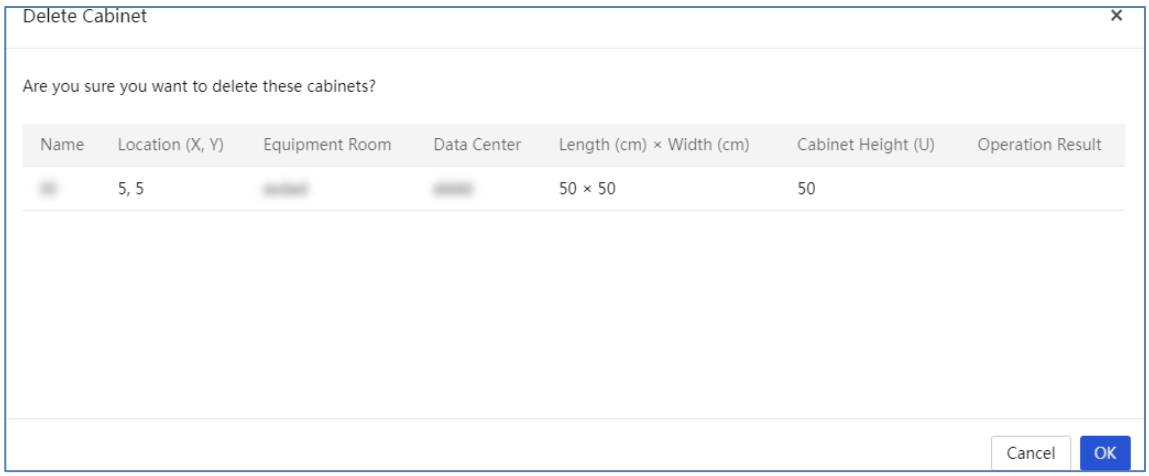
制約事項とガイドライン

キャビネットで消費電力上限タスクが実行されている場合は、キャビネットを削除できません。キャビネットがインフラストラクチャに関連付けられているか、消費電力上限を実行している場合は、キャビネットを削除できません。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Cabinet**を選択します。
2. キャビネットをバッチで削除するには、ターゲットキャビネットを選択してDeleteをクリックします。表示されたダイアログボックスで、OKをクリックします。キャビネットを削除するには、キャビネットの**Actions**列で**Delete**をクリックします。

図126キャビネットの削除



パラメータ

- **Name**キャビネット名。
- **Description**:キャビネットの説明。このフィールドはオプションです。
- **Cabinet Type**:共通および浸漬(TANK)を含むキャビネットタイプ。
- **Data Center**:キャビネットが属するデータセンター。
- **Equipment Room**:キャビネットが属する機器室。
- **Cabinet Size (cm)**:キャビネットの長さと幅。
- **Coordinates (X, Y)**:キャビネットの座標。
- **Cabinet Height (U)**:キャビネットの高さ。
- **Rated Power (W)**:キャビネットの定格電力。

デバイスの管理

この機能を使用すると、ユーザーはUniSystem管理デバイスおよびカスタムデバイスを、サーバー、スイッチ、インフラストラクチャなどのキャビネットに追加できます(動的環境ホストおよび分散CDUのみがサポートされます)。追加に成功したら、必要に応じてデバイスを削除できます。

サーバーの追加

すでにサーバーリストにあるサーバーを追加したり、カスタムサーバーをキャビネットに追加したりするには、次の作業を実行します。

制約事項とガイドライン

- キャビネットで消費電力上限タスクが実行されている場合は、新しいデバイスを追加できません。
- 使用可能なサーバーのリストには、オフラインのサーバー、ブレードサーバー、およびキャビネットに追加されたサーバーは表示されません。
- 使用可能なデバイスの一覧には、IP接続状態が異常であるか、キャビネットに追加された水冷デバイスは表示されません。
- 使用可能なデバイスの一覧には、接続ステータスが異常なスイッチやキャビネットに追加されたスイッチは表示されません。

手順

1. ナビゲーションペインで、**Menu > Devices > Data Center Management > Cabinet**を選択します。
2. 詳細ページにアクセスするには、キャビネット名をクリックします。
3. 開いたページで、キャビネット内のスペアベイを選択します。開いたダイアログボックスで**Add Device**で**Existing Devices**または**Add Custom Device**を選択します。
   - 既存のサーバーを追加するには、使用可能なリストからサーバーを選択し、非G 6サーバーの予約済み電力を指定して、**OK**をクリックします。
   - カスタムサーバーを追加するには、サーバー情報を設定し、**OK**をクリックします。

図127既存のデバイスの選択

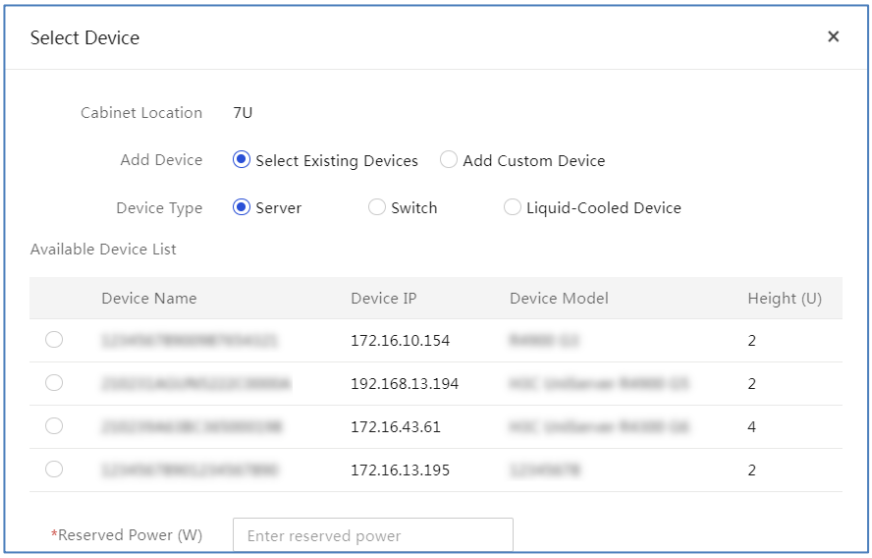
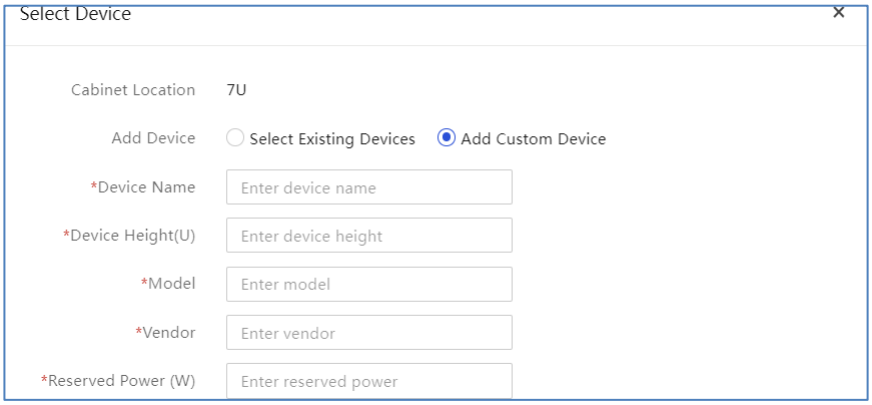


図128カスタムデバイスの追加



4. (オプション)デバイスを削除するには、ターゲットデバイスを選択し、**Delete**をクリックします。表示された確認ダイアログボックスで、**OK**をクリックします。

テンプレートの管理

UniSystemは、シャーシ、サーバー、HDM/BIOSなどのさまざまな構成タイプをカバーする包括的なテンプレート管理機能を提供します。これにより、企業は効率的なリソース構成管理を実現できます。

- 一元管理

  構成管理に統一されたテンプレートを使用すると、すべての構成の管理が簡素化および一元化され、構成の時間と複雑さが大幅に軽減されるため、デバイスの導入サイクルが短縮されます。

- 洗練されたスコープマネジメント

  部門や地域などのディメンションに基づいてスコープを分割することで、構成テンプレートはリソースとして異なるスコープに分類されます。ユーザーは、割り当てられたロールとスコープに従って、対応するテンプレートにのみアクセスして使用できます。これにより、構成の効率とセキュリティが向上します。

メモ:

- 範囲に基づいてテンプレートを管理するには、最初に範囲を構成する必要があります。詳細については、「スコープマネジメント」を参照してください。
- **All Resources**の値は、システム内のすべてのリソースを表します。これは、ユーザーがすべてのリソースを管理でき、範囲による制限を受けないことを示します。現在のユーザーがすべてのリソースを管理できる場合、共有構成はオプションです。

エンクロージャーテンプレートの管理

Templates > Enclosure Templatesページでは、エンクロージャーテンプレートを追加、コピー、削除、編集、および表示できます。

エンクロージャーテンプレートでは、エンクロージャー内のブレードサーバースロットにサーバーテンプレートをバインドできます。その後、選択したエンクロージャーにエンクロージャーテンプレートを適用できます。エンクロージャーテンプレートの適用について詳しくは、「エンクロージャーテンプレートの適用」を参照してください。

エンクロージャーテンプレート情報の表示

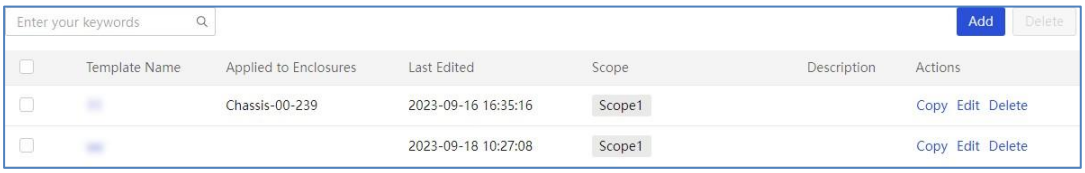
このタスクについて

エンクロージャーテンプレートリストおよびエンクロージャーに関する詳細情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu > Templates > Enclosure Templates**を選択します。

図129 エンクロージャーテンプレートリスト



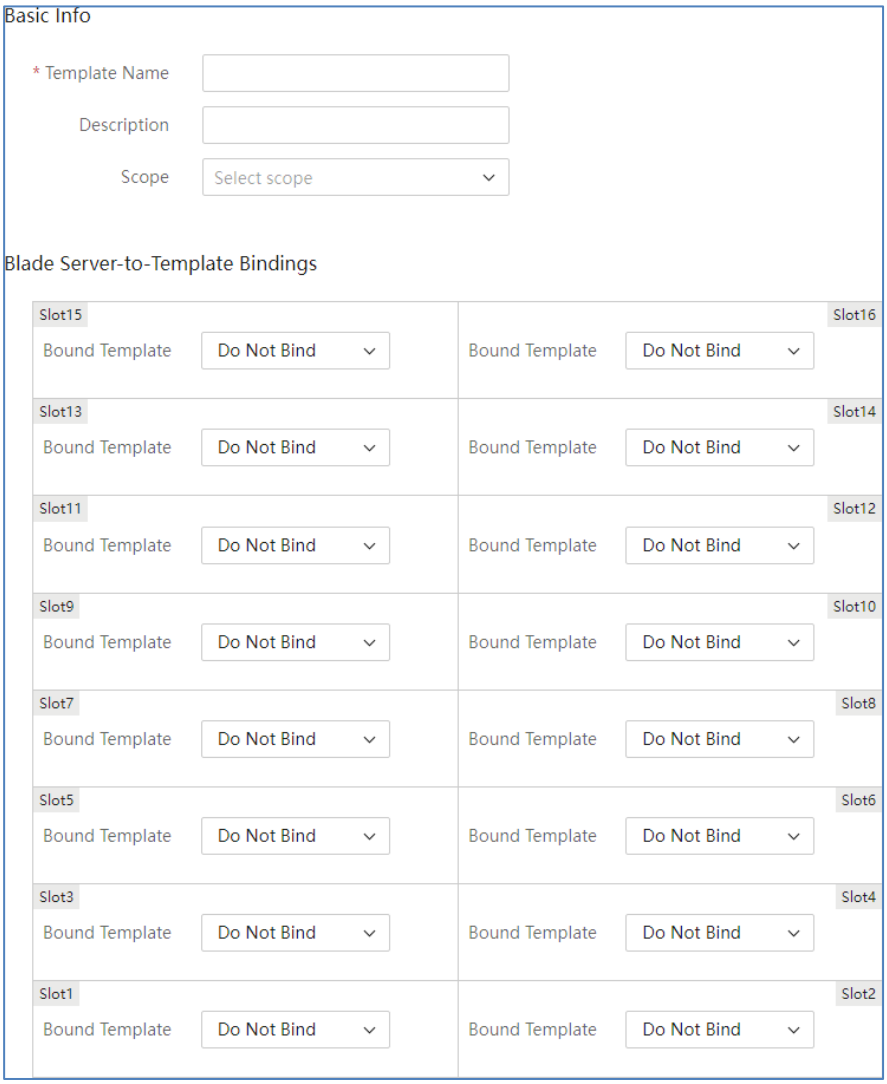
2. エンクロージャーテンプレートに関する詳細情報を表示するには、テンプレートの名前をクリックします。

エンクロージャーテンプレートを追加する

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Enclosure Templates**を選択します。
2. **Add**をクリックします。
3. **Basic Info**領域で、次の手順を実行します。
   a. テンプレートの名前と説明を入力します(オプション)。
   b. スコープを選択します。
4. **Blade Server-to-Template Bindings**領域で、各ブレードサーバースロットにバインドするサーバーテンプレートを選択します。サーバーテンプレートの構成について詳しくは、「サーバーテンプレートの管理」を参照してください。
5. **OK**をクリックします。

図130サーバーテンプレートの追加



エンクロージャーテンプレートの削除

1. ナビゲーションペインで、**Menu** > **Templates** > **Enclosure Templates**.を選択します。
2. 次のいずれかの手順を実行します。
   - エンクロージャーテンプレートを一括削除するには、ターゲットテンプレートを選択して**Delete**をクリックします。
   - 単一のエンクロージャーテンプレートを削除するには、テンプレートの**Actions**列で**Delete**をクリックします。
3. 表示されたダイアログボックスで、**OK**をクリックして操作を確認します。

エンクロージャーテンプレートをコピーする

1. ナビゲーションペインで、**Menu** > **Templates** > **Enclosure Templates**を選択します。
2. コピーするテンプレートの**Actions**列で**Copy**をクリックします。

3. 新しいテンプレートの名前を指定し、必要に応じてテンプレートの設定を編集します。
4. **OK**をクリックします。

エンクロージャーテンプレートを編集する

1. ナビゲーションペインで、**Menu** > **Templates** > **Enclosure Templates**を選択します。
2. 編集するテンプレートの**Actions**コラムで**Edit**をクリックします。
3. テンプレート設定を編集します。
4. **OK**をクリックします。

サーバーテンプレートの管理

サーバーテンプレートの管理について

Templates > **Server Templates**ページから、サーバーテンプレートを追加、コピー、削除、編集、および表示できます。

サーバーテンプレートでは、サーバーのHDM、BIOS、HDMオンライン、接続、RAIDおよびOSインストール設定を定義できます。次に、サーバーテンプレートをサーバーに適用することにより、テンプレート設定をサーバーに一括適用できます。サーバーテンプレートの適用の詳細は、「サーバーテンプレートの適用」を参照してください。

サーバーテンプレートを追加する

このタスクについて

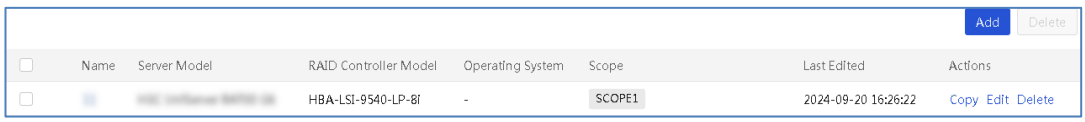
サーバーテンプレートは、次のいずれかの方法で追加できます。

- **Add a new server template**: **Add Server Template**ページでサーバーテンプレートを追加します。
- **Copy and modify an existing server template**: 既存のサーバーテンプレートをコピーして変更し、新しいサーバーテンプレートを生成します。

手順

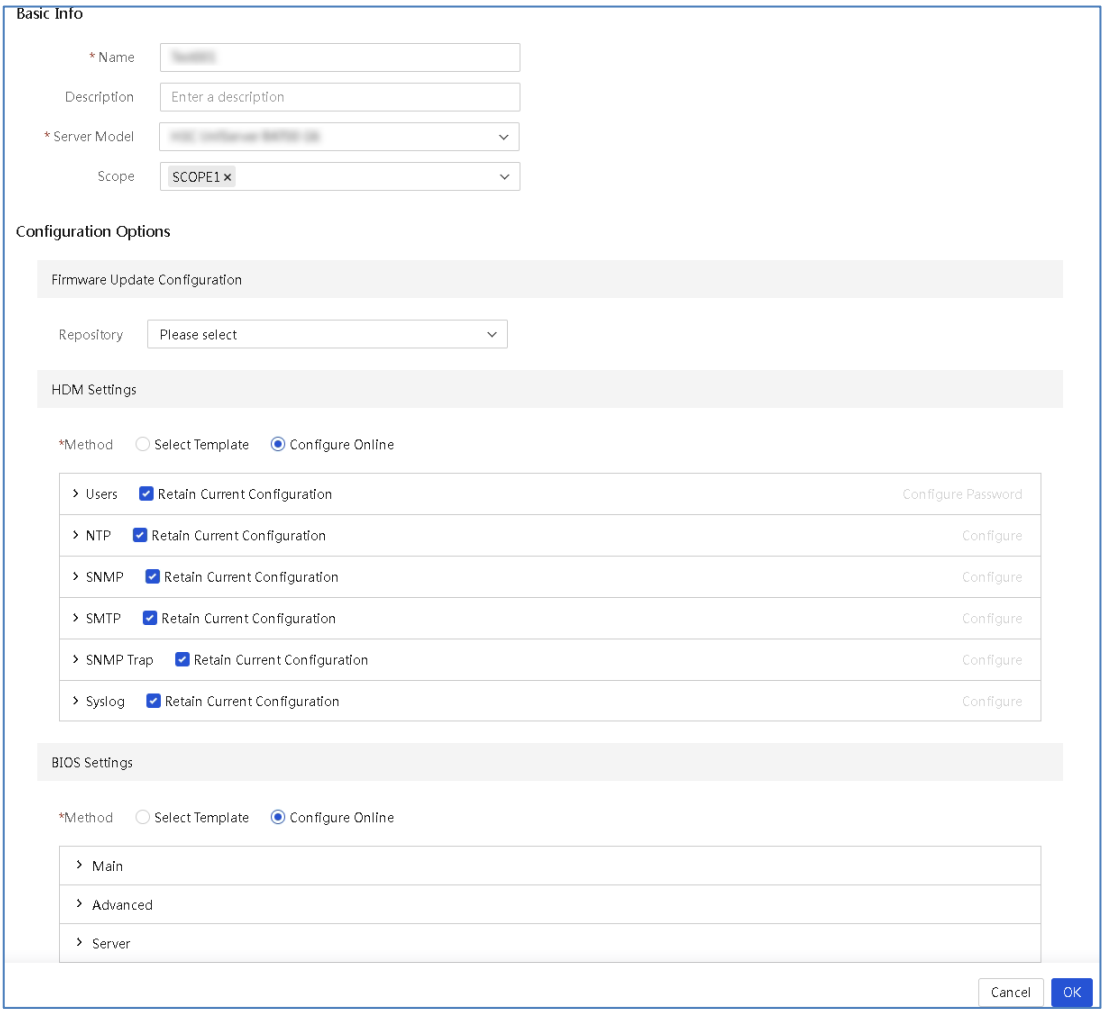
1. ナビゲーションペインで、**Menu** > **Templates** > **Server Templates**を選択して、図131に示すように**Server Templates**ページに入ります。

   図131Server Templatesページ

2. **Add**をクリックして、図132に示す**page**に入ります。

図132サーバーテンプレートの追加



3. (オプション) **existing**のテンプレートを基にしてサーバー テンプレートを作成するには、サーバー テンプレートの **Actions**列で**Copy**をクリックします。
4. **Basic Info**領域で、サーバーテンプレート名と**template**の説明(オプション)を入力し、**Server Model**リストから互換性のあるサーバーモデルを選択して、スコープを選択します。
5. **Firmware Update Configuration, HDM Settings**, **BIOS Settings**, **Connection Settings**, **RAID Settings**, そして **OS Settings**を構成します。詳細については、次のセクションを参照してください。
6. サーバーテンプレートの詳細を表示するには、サーバーテンプレートの名前をクリックします。OSの設定でサーバーテンプレートに対して**Use Answer File**を選択した場合は、**Download File**をクリックして、応答ファイルをダウンロードして表示します。

HDM/BIOSテンプレートの設定

このタスクについて

サーバーテンプレートでは、エクスポートされたHDMまたはBIOS構成テンプレートファイルを選択できます。次に、構成テンプレートファイルをサーバーテンプレートに保存し、テンプレートを複数のサーバーに一括適用できます。このようにして、複数のサーバーのHDM設定およびBIOS設定を同時に構成できます。

UniSystemでは、HDM設定またはBIOS設定を構成テンプレートファイルにエクスポートできます。

詳細は、「HDM/BIOSテンプレートの構成」を参照してください。

制約事項とガイドライン

- HDMまたはBIOS設定をサーバーに適用する前に、ターゲットサーバーのHDMまたはBIOSが正しく動作していることを確認してください。
- HDMテンプレートをサーバーに適用する前に、ターゲットサーバーのサーバーモデル、HDMバージョン、およびハードウェア構成がHDMテンプレートのものと同じであることを確認してください。
- BIOSテンプレートをサーバーに適用する前に、ターゲットサーバーのサーバーモデルとBIOSバージョンがBIOSテンプレート内のものと同じであることを確認してください。サーバーに適用されたBIOS設定は、サーバーの再起動後に有効になります。
- HDM設定がサーバーに正常に適用されると、サーバーのHDMが自動的に再起動します。HDM IPは変更される場合があります。HDM IPが変更されると、サーバーテンプレートの適用プロセス全体が事前に終了します。この場合、現在のHDM IPを表示し、HDMをUniSystemに再度追加します。

手順

1. ナビゲーションペインで、**Menu > Templates > Server Templates**を選択します。
2. **Add**.をクリックします。
3. (オプション)HDMテンプレートまたはBIOSテンプレートを設定するには、HDM/BIOS Templatesリンクをクリックします。
4. **HDM Settings**または**BIOS Settings**領域(この例では**HDM Settings**領域)でSelect Templateをクリックし、エクスポートされたHDMテンプレートを選択して、**OK**をクリックします。

図133 HDM/BIOSの設定



HDMをオンラインで構成

このタスクについて

このタスクでは、ユーザー、NTP、SNMP、SNMPトラップ、およびSyslog設定を含むHDMをオンラインで設定できます。

手順

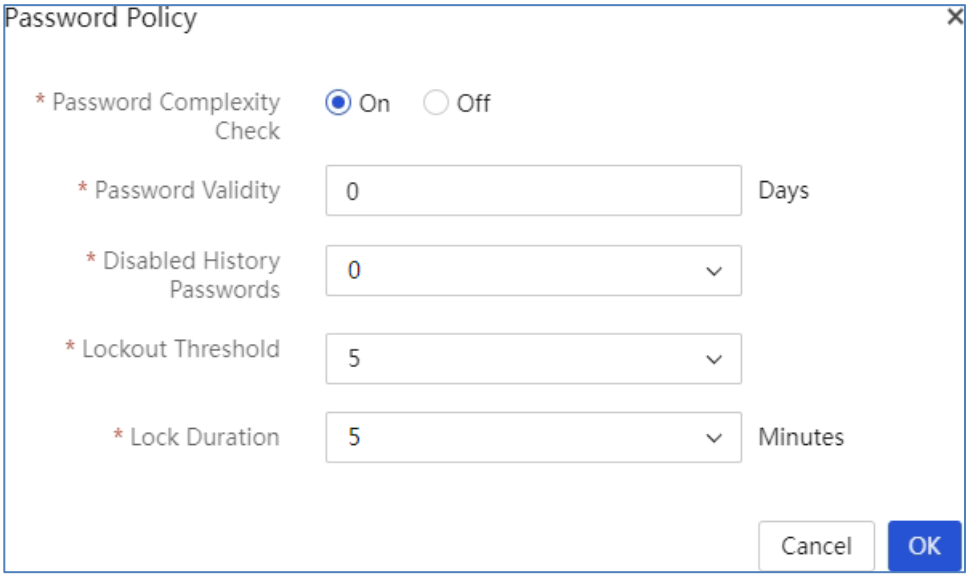
1. **ユーザーの構成:**

重要:

ユーザー**admin**のデフォルトパスワード(**Password@_**)を変更すると、HDM接続エラーが発生する場合があります。注意してください。

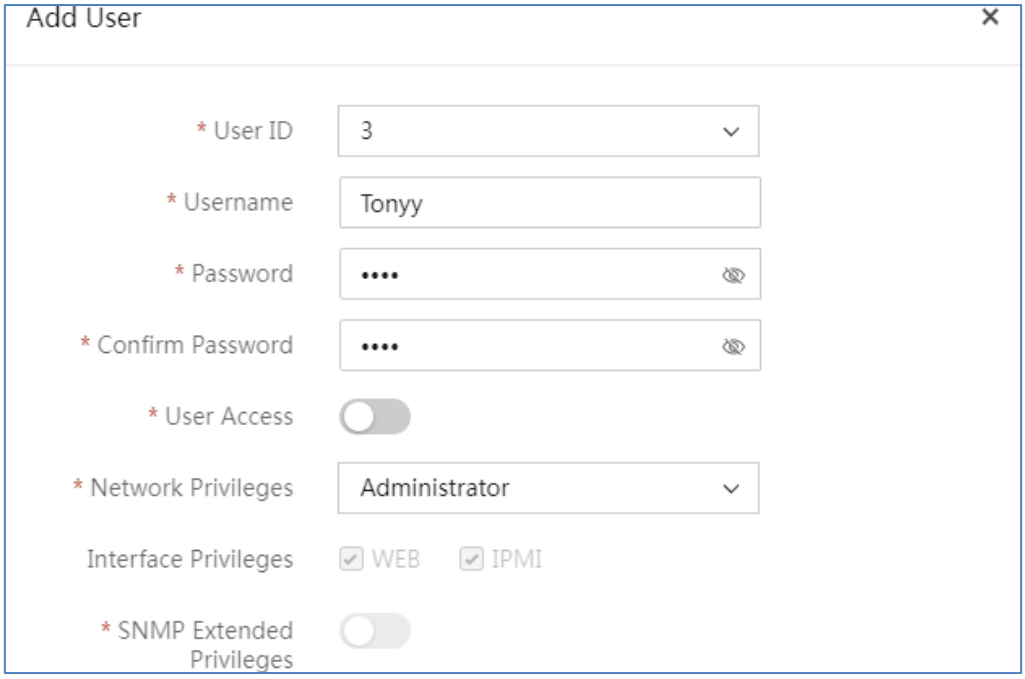
   a. **Users**フィールドで**Retain Current Configuration**の選択を解除します。
   b. **Configure Password**,をクリックし、パスワードポリシーを構成します。
      - パスワードの複雑度チェックを有効または無効にします。
      - パスワードの有効性など、パスワード設定を指定します。
      - **OK**をクリックします。

図134パスワードポリシーの構成



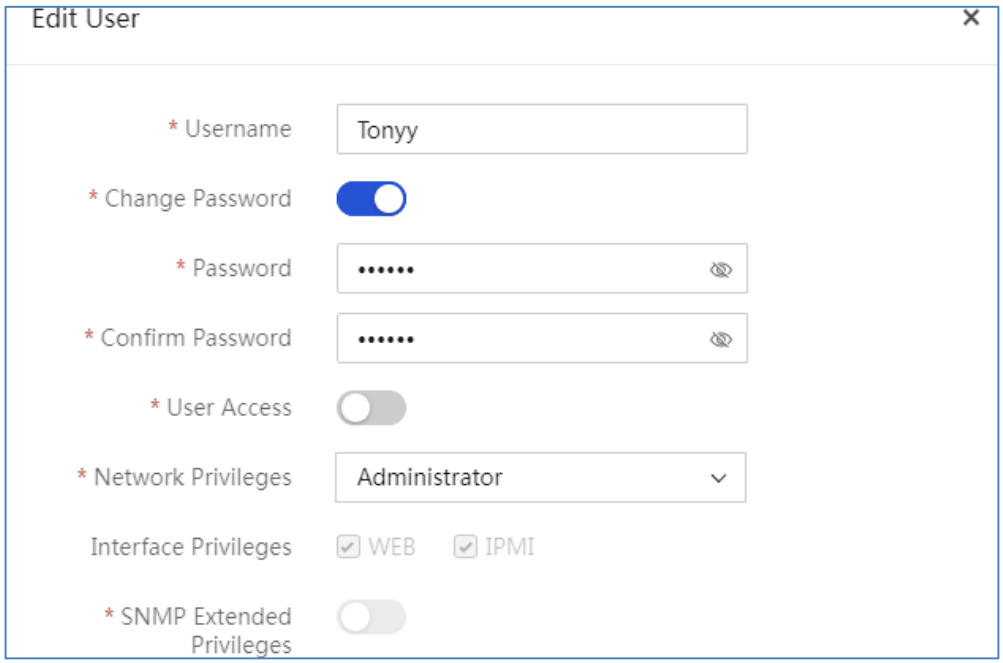
c. **Add User**をクリックし、ユーザー設定を構成して、**OK**をクリックします。

図135ユーザーの追加



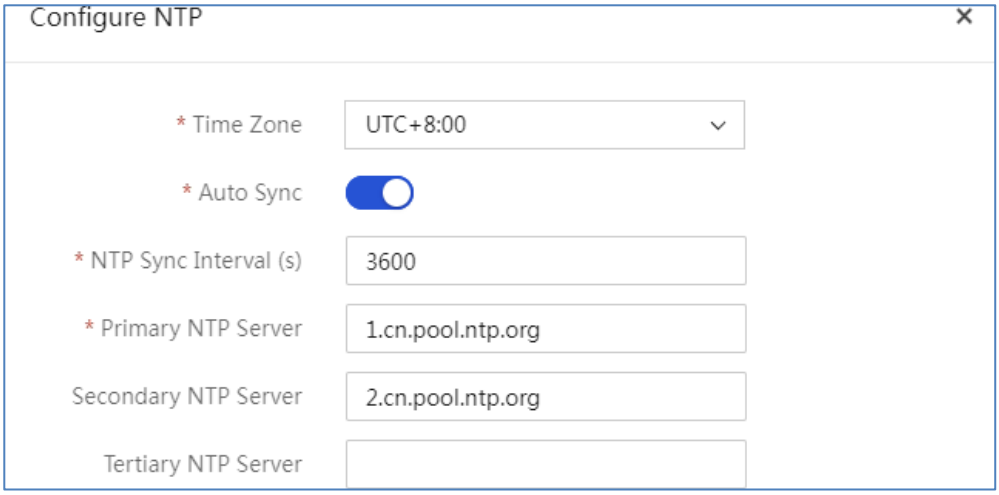
d. ユーザーエントリの**Edit**をクリックし、ユーザー設定を構成して、**OK**をクリックします

図136ユーザーの編集



2. **NTP**を設定します。
   a. **NTP**フィールドで**Retain Current Configuration**の選択を解除します。
   b. **Configure**をクリックして、NTPを設定します。
      – 自動同期を有効または無効にします。この機能を使用すると、システムはNTPサーバーから時間設定を同期できます。
      – 同期間隔を設定し、プライマリ、セカンダリ、およびターシャリNTPサーバーを指定します。
      – **OK**をクリックします。

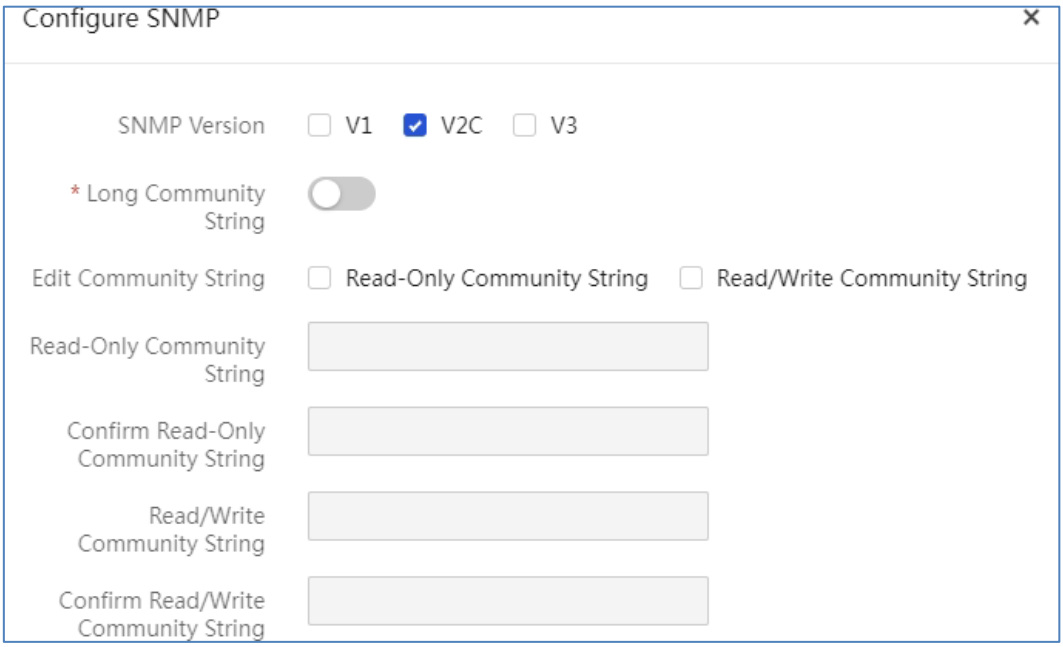
      図137 NTPの設定



3. **SNMP**を設定します。
   a. **SNMP**フィールドで**Retain Current Configuration**の選択を解除します。
   b. **Configure**をクリックして、SNMPを設定します。
      – SNMPバージョンを選択します。

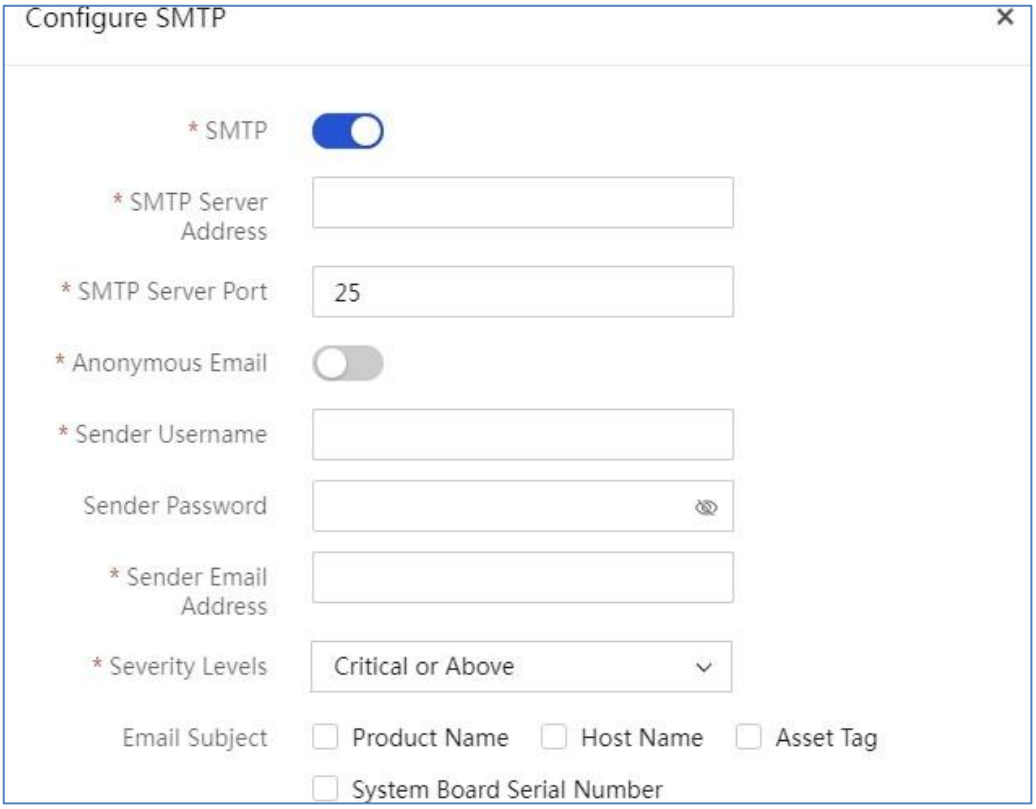
- 長いコミュニティストリング機能をイネーブルにするかどうかを選択します。
- **Read-Only Community String**または**Read/Write Community String**を選択し、文字列を指定します。
- **OK**をクリックします。

図138 SNMPの設定



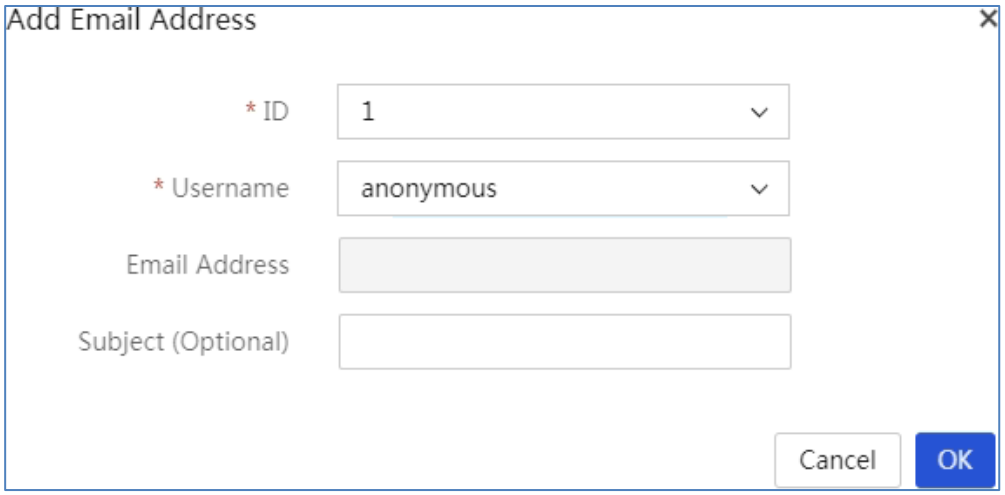
4. **SMTP**の設定:
   a. **SMTP**フィールドで**Retain Current Configuration**の選択を解除します。
   b. **Configure**をクリックして、SNMPを設定します。
      - SMTPを有効にします。
      - SMTPサーバードレスとサーバーポートを指定します。
      - 匿名電子メールを有効にするかどうかを選択します。アラート電子メールを匿名電子メールとして送信するには、この機能を有効にします。送信者のID情報を含むアラート電子メールを送信するには、この機能を無効にして、SMTPサーバーに接続するためのユーザー名とパスワードを入力します。ユーザー名は1～255文字の文字列です。
      - 送信者の電子メールアドレスを指定します。電子メールサービスがSMTPメールサーバーを使用していることを確認してください。
      - 重大度を選択します。オプションには、**Critical**、**Major+Critical**、**Minor+Major+Critical**および**All**があります。
      - 電子メールの件名を選択します。オプションには、**Product Name**, **Host Name**, **Asset Tag** および **System Board Serial Number**.。このフィールドは、G3およびG5サーバーでは使用できません。
      - **OK**をクリックします。

図139 SMTPの設定



c. **Add Email Address**をクリックし、受信者情報を設定します。
   - 受信者のユーザー名を選択します。ユーザーの電子メールアドレスが自動的に入力されます。これは、G3/G5サーバーでのみ使用できます。
   - 電子メールの件名を入力します。件名は、1から255文字の文字列です。
   - OKをクリックします。

図140電子メール受信者の追加



5. SNMPトラップの設定:
   a. **SNMP Trap**フィールドで**Retain Current Configuration**の選択を解除します。

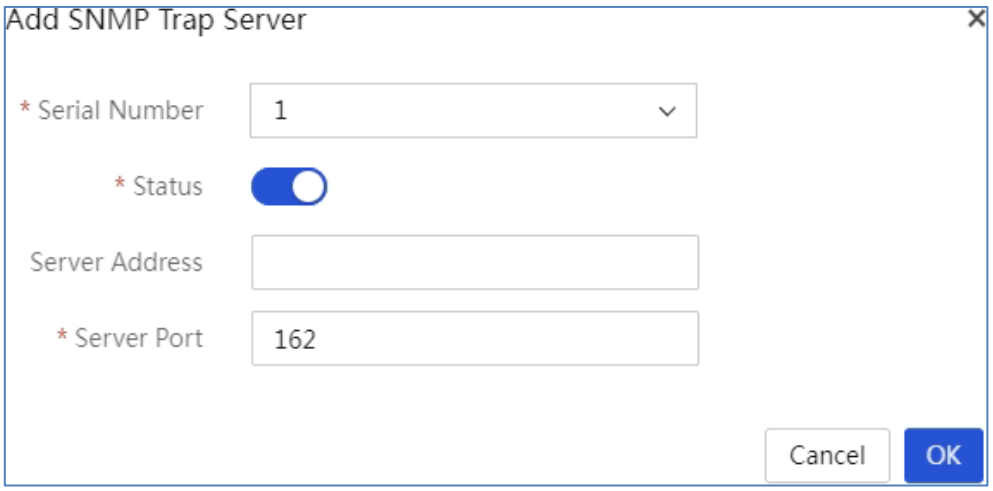
b. **Configure**をクリックして、SNMPを設定します。
   - SNMPトラップを有効にします。
   - SNMPトラップモードを選択します。オプションには、**Node OID**, **Event OID**, および **Event code OID**があります(このフィールドは、G3およびG5サーバーでは使用できません)。
   - SNMPトラップのバージョンを選択します。SNMPv3を選択した場合は、SNMPv3ユーザーも指定する必要があります。
   - (オプション)サーバーの場所と連絡先情報を入力します。
   - コミュニティストリングを指定し、アラームの重大度レベルを選択します。
   - **OK**をクリックします。

図141 SNMPトラップの設定



c. **Add SNMP Trap Server**をクリックし、SNMPトラップサーバーを設定します。
   - サーバー番号を選択します。
   - サーバーを有効にするかどうかを選択します。
   - (任意)サーバードレスを指定します。
   - ポート番号を指定します。
   - **OK**をクリックします。

図142 SNMPトラップサーバーの追加



6. **Syslog**の設定:

メモ:

Syslogを設定する場合、**Product serial number**オプションは、HDMバージョン2.80以降でのみ**Alarm log host ID**フィールドで使用できます。

a. **Syslog**フィールドで**Retain Current Configuration**の選択を解除します。
b. **Configure**をクリックし、SNMPを設定します。

アラームログ通知

- ログ通知を有効にします。
- アラームログのホストIDを選択し、伝送プロトコルを選択します。
- ログ形式を選択します。オプションには、**Simplified**, **RFC3164**, および **RFC5424**があります。このフィールドは、G3およびG5サーバーでは使用できません。

  Simplified形式を選択した場合は、カスタムログ形式を設定する必要があります。オプションには、**imestamp**, **Host Name**, および **Message**があります。デフォルトでは、**Message**が選択されています。このフィールドは、G3およびG5サーバーでは使用できません。

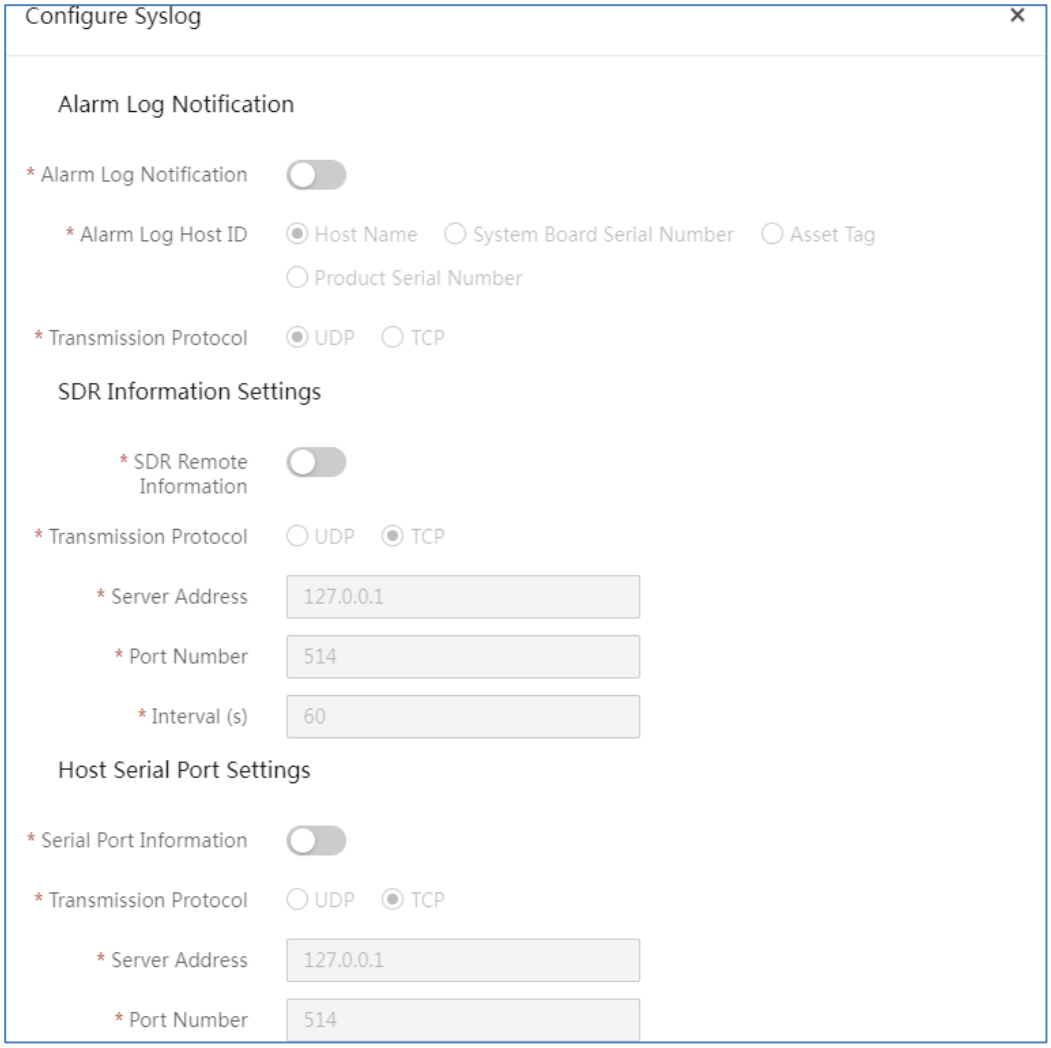
SDR情報設定(G3およびG5サーバー)

- SDRリモート情報をイネーブルにします。
- 伝送プロトコルを選択します。
- サーバードレス、ポート番号、および間隔を入力します。

ホストシリアルポート設定(G3およびG5サーバー)

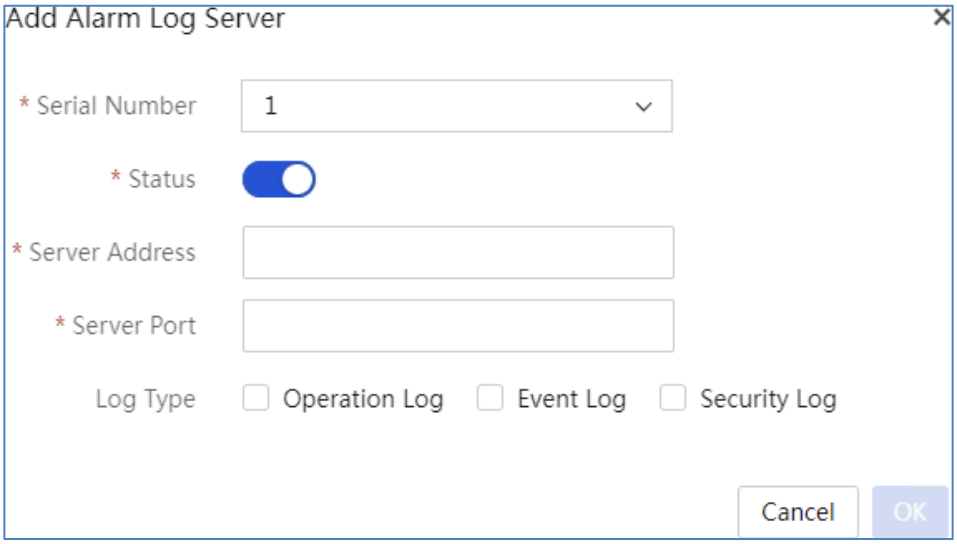
- シリアルポート情報を有効にします。
- 伝送プロトコルを選択します。
- サーバーのアドレスとポート番号を指定します。
- **OK**をクリックします。

図143 Syslogの設定



c. **Add Alarm Log Server**をクリックし、アラームログサーバーを設定します。
   - 番号を選択します。
   - サーバーの状態を選択します。
   - サーバー名を入力します。このフィールドは、G6サーバーでのみ使用できます。
   - サーバーのアドレスとポート番号を入力します。
   - ログの種類を選択します。
   - ログの重大度を選択します。このフィールドは、G6サーバーでのみ使用できます。
   - **OK**をクリックします。

図144アラームログサーバーの追加



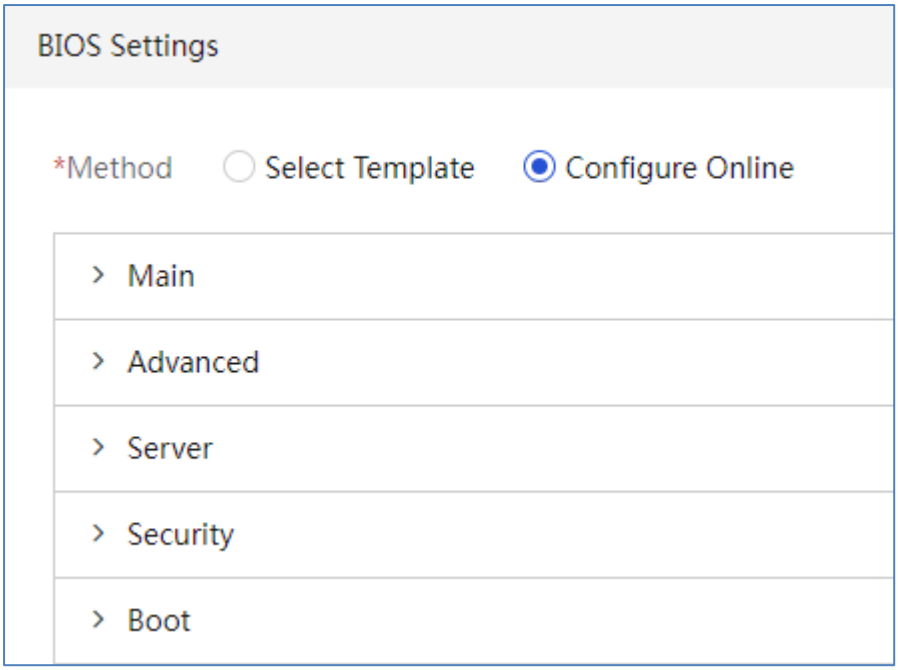
BIOSをオンラインで設定します。

このタスクでは、BIOSをオンラインで設定できます。

- R4900 G3、R4330 G5、R4900 G5、R4930 G5、R4950 G5 Milan、R4950 G5 Rome、B5700 G5、R4700 G5、R6900 G5、R5300 G5、R5500 G5 Intel、R5500 G5 Milan、R5500 G5のみ
  Rome、R4700 G6、R4900 G6、およびR5300 G6サーバーは、この機能をサポートしています。
- R4300 G6では、この機能はBIOS 6.00.33以降のバージョンで使用できます。
- R4900 G3の場合、この機能はBIOS 2.58以降のバージョンで使用できます。
- R4900 G5、B5700 G5、R4700 G5、R6900 G5、およびR5300 G5では、この機能はBIOS 5.45以降のバージョンで使用できます。
- R4330 G5およびR4930 G5では、この機能はBIOS 5.28以降のバージョンで使用できます。
- R4950 G5 Milan、R4950 G5 Rome、R5500 G5 Intel、R5500 G5 Milan、およびR5500 G5 Romeでは、この機能はBIOS 5.45以降のバージョンで使用できます。
- R4700 G6、R4900 G6、およびR5300 G6では、この機能はBIOS 6.00.22以降のバージョンで使用できます。
- R4950 G6では、この機能はBIOS 6.30.26以降のバージョンで使用できます。
- R5350 G6およびR5500 G6 AMDの場合、この機能はBIOS 6.30.31以降のバージョンで使用できます。
- R5500 G6 Intelの場合、この機能はBIOS 6.00.28以降のバージョンで使用できます。
- R6900 G6では、この機能はBIOS 6.00.34以降のバージョンで使用できます。

オンライン設定に使用できるBIOSオプションは、デバイスのモデルによって異なります。詳細については、デバイスのBIOSユーザーガイドを参照してください。

図145 BIOSのオンライン設定



接続設定の構成

このタスクについて

サーバーテンプレートでは、スイッチポートとサーバーポート間の接続を定義し、各接続にネットワークを割り当てることができます。次に、自動設定機能を使用してサーバーテンプレートを対応するスイッチポートにバインドし、スイッチポートの自動ネットワーク設定を有効にします。

制約事項とガイドライン

サーバーテンプレートの接続設定は、H3C S6850-56HFまたはH3C S6800-54QFスイッチのポートにだけ適用できます。

接続設定がポートに適用されると、スイッチポートはアクセスポートとして設定されます。

手順

構成手順はサーバーのモデルによって異なります。このセクションでは、これらの構成手順について個別に説明します。

接続の追加

1. ナビゲーションペインで、**Menu > Templates > Server Templates**を選択します。
2. **Add**をクリックして、サーバーテンプレートを追加するためのページを開きます。
3. **Connection Settings**領域で、**Add Connection for rack servers**をクリックします。表示されるダイアログボックスで、次のパラメータを設定します。
   a. **Connection Name**フィールドに接続名を入力します。
   b. **Network**リストから既存のネットワークを選択します。UniSystemでのネットワークの作成については、「ネットワークの管理」を参照してください。
   c. 接続のサーバー側のNICスロットとNICポートを選択します。HDM専用ネットワークポートは選択できません。
      NICスロットおよびNICポートの設定は、サーバー管理者がネットワーク計画時に参照する

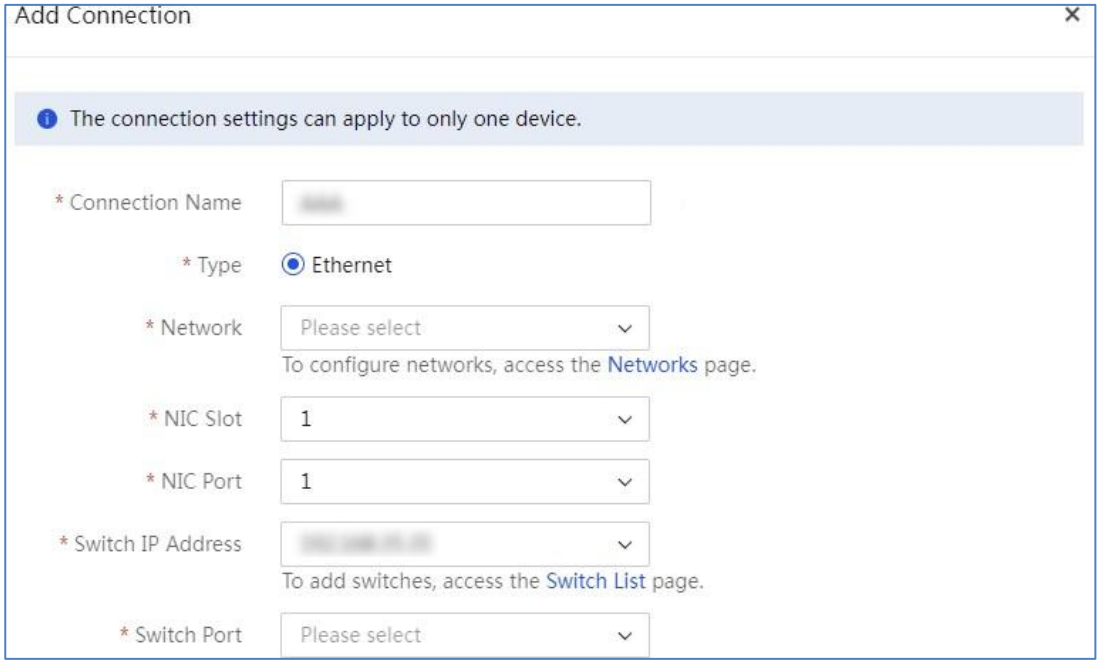
ためだけのものです。この設定は、テンプレートの適用プロセスで実際のサーバーに直接適用されることはありません。

d. 接続のスイッチ側で、スイッチのIPアドレスとスイッチポートを選択します。スイッチはUniSystemに追加されている必要があります。詳細は、「スイッチの追加」を参照してください。

接続が追加されたテンプレートは、1つのデバイスにのみ適用できます。

4. **OK**をクリックして接続を追加します。

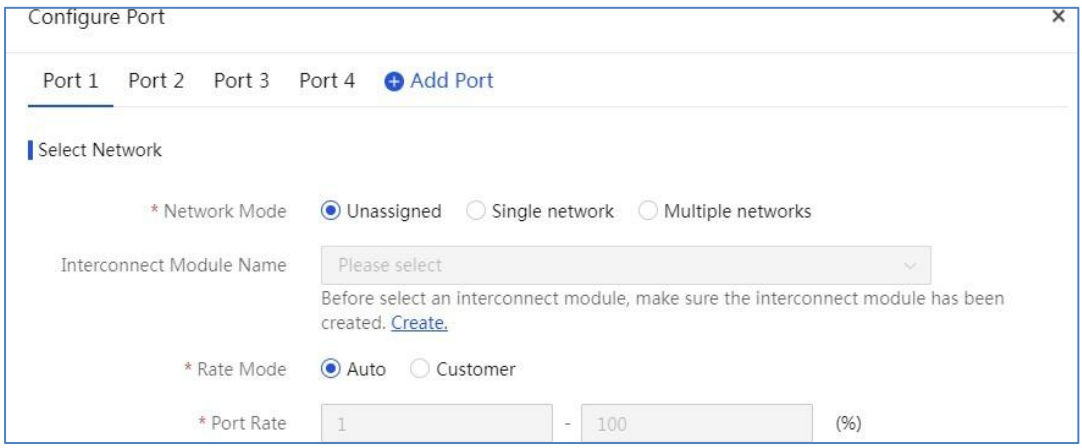
図146接続の追加



メザニンカードの追加

1. **Connection Settings**領域で、G3ブレードサーバー用の**Add Mezzanine Card**をクリックします。次の手順を繰り返して、複数のメザニンカードを追加できます。
2. メザニンカードのスロット番号とタイプを選択します。
3. **Actions**列で**Configure Port**をクリックします。開いたダイアログボックスで、必要に応じてポートを構成します(図147を参照)。

図147ポートの設定



4. ネットワークモードを選択します。**Multiple networks**を選択した場合は、サーバーのVLAN IDを設定する必要があります。
5. 作成したインターコネクトモジュールテンプレートを選択します。インターコネクトモジュールテンプレートの作成については、「インターコネクトモジュールテンプレートの管理」を参照してください。
6. レートモードを選択し、ポートレートを設定します。
7. **OK**をクリックします。

RAID構成テンプレートの構成

このタスクについて

RAID構成テンプレートを事前に構成することにより、サーバーのRAID設定を一括構成できます。

サポートされるストレージコントローラー

- HBA-1000-M2-1(RAID(Hide RAW)モードのみ)
- HBA-H460-B1
- HBA-H460-M1
- HBA-H5408-Mf-8i
- HBA-LSI-9440-8i
- RAID-L460-M4(RAIDモードのみ)
- HBA-LSI-9311-8i-A1-X
- RAID-LSI-9361-8i(1G)-A1-X
- RAID-LSI-9361-8i(2G)-1-X
- RAID-LSI-9460-16i(4G)
- RAID-LSI-9460-8i(4G)
- RAID-LSI-9460-8i(2G)
- HBA-LSI-9540-LP-8i
- RAID-LSI-9560-LP-8 i:4GB
- RAID-LSI-9560-LP-16 i:8GB
- RAID-P2404-Mf-4i-2GB
- RAID-P430-M1(RAID(Hide RAW)モードおよびRAID(Expose RAW)モード)
- RAID-P430-M2(RAID(Hide RAW)モードおよびRAID(Expose RAW)モード)
- RAID-P460-B2
- RAID-P460-B4
- RAID-P460-M2
- RAID-P460-M4
- RAID-P 4408-Mf-8 i:2GB
- RAID-P4408-Ma-8i-2GB
- RAID-P 4408-Mr-8 i:2GB
- RAID-P 5408-Mf-8 i:4GB
- RAID-P 5408-Ma-8 i:4GB

制約事項とガイドライン

- 構成するストレージコントローラーが、RAID設定で指定されているものと同じモデルであることを確認してください。RAID設定で2つのストレージコントローラーが指定されている場合は、

対応するスロットに、構成するサーバー上の一致するモデルのストレージコントローラーがあることを確認してください。

- RAIDメンバードライブが存在し、正常に動作していることを確認します。

手順

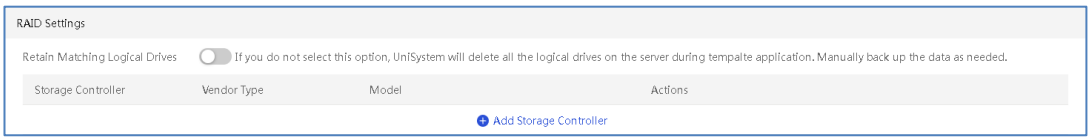
1. ナビゲーションペインで、**Menu > Templates > Server Templates**を選択します。
2. **Add**をクリックします。
3. **Basic Info**領域で、パラメータを設定します。
4. 図148に示すように、**RAID Settings**領域で**Retain Matching Logical Drives**を有効にするかどうかを選択します。このオプションを有効にしてサーバー上の論理ドライブを保持する場合は、論理ドライブのメンバードライブとRAIDレベルが、この領域で構成されている論理ドライブのものと一致していることを確認してください。このオプションを有効にしない場合、UniSystemはサーバー上の既存の論理ドライブを削除します。

   メモ:

   - **Retain Matching Logical Drives**を有効にすると、論理ドライブのメンバードライブとRAIDレベルがこの領域で設定されている論理ドライブのものと一致する場合、UniSystemはサーバー上の論理ドライブを保持します。UniSystemは保持された論理ドライブを変更しません。たとえば、保持された論理ドライブの構成ファイル内のRAID名が実際のRAID名と異なる場合、UniSystemは保持された論理ドライブのRAID名を変更しません。
   - 保持されている論理ドライブにオペレーティングシステムをインストールするには、**OS settings**領域のターゲットドライブのRAID名が、保持されている論理ドライブの元のRAID名と同じであることを確認します。
   - ホットスペアドライブを作成し、それを予約済み論理ドライブに割り当てるには、RAID名元の論理ドライブ名と一致する必要があります。一致しない場合、ホットスペアの作成は失敗します。

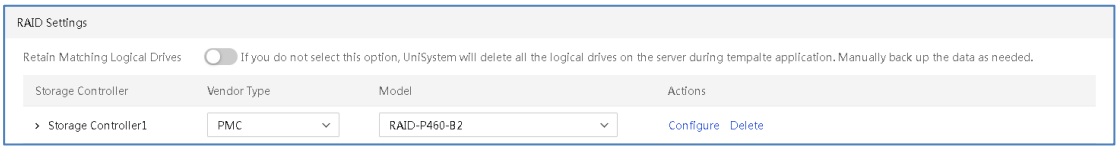
5. **Add Storage Controller**をクリックします。ストレージコントローラーのモデルを選択します。

   図148ストレージコントローラーの追加

6. 図149に示すように、ス**Slot Number**, **Vendor Type**, および **Model**から値を選択します。**Slot Number**は、選択したサーバーモデルが複数のストレージコントローラーをサポートしている場合にのみ使用できます。論理ドライブを設定するには、**Configure**をクリックします。

   図149 RAIDの設定

7. 図150に示すように開いたダイアログボックスで、**Add Logical Drive**をクリックします。
8. RAID名を入力し、RAIDレベルと物理ドライブを選択します。
9. (P 460チップストレージコントローラを搭載したラックサーバーのみ) **Add Hot Spare**をクリックし、ホットスペアのタイプ、論理ドライブ名、および物理ドライブを選択します。ホットスペア構成をサポートしているのは、P 460チップストレージコントローラによって管理される論理ドライブのみです(RAID 0アレイを除く)。

10. **OK**をクリックします。

図150 ストレージコントローラーの設定

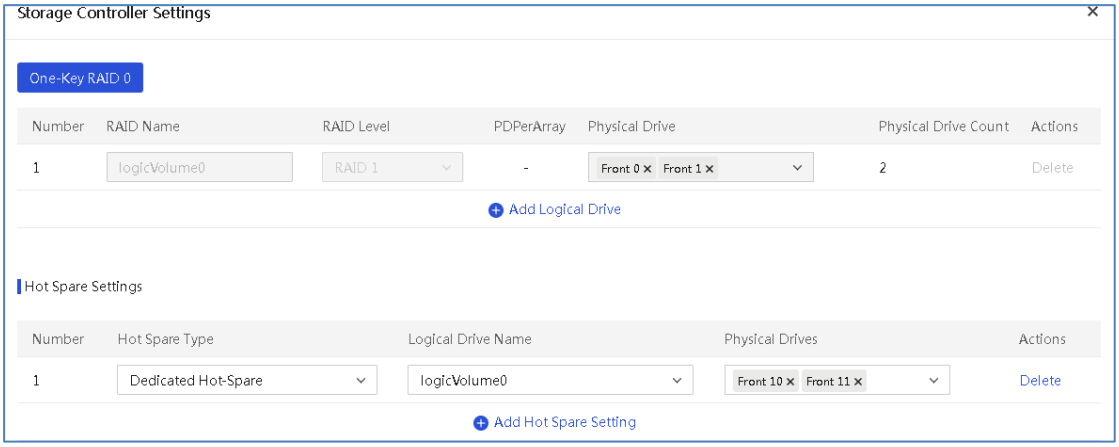


表12 RAID設定のパラメータ

パラメータ	備考
ワンキーRAID 0	RAIDアレイに追加されていない残りの物理ドライブを使用して、RAID 0またはシンプルボリュームを作成するには、このオプションを選択します。一部のストレージコントローラーは、One-Key RAID 0オプションをサポートしていません。
RAID名	作成するRAIDアレイ(論理ドライブ)の名前。同じストレージコントローラー上では、RAID名は一意である必要があります。
RAIDレベル	作成する論理ドライブのレベル。使用可能なRAIDレベルは、表13に示すように、ストレージコントローラーのモデルによって異なります。表13に記載されていないその他の使用可能なストレージコントローラーは、RAID 0、RAID 1、RAID 5、RAID 6、RAID 10、およびRAID 50です。
物理ドライブ	論理ドライブの作成に使用された物理ドライブ。
PDPerArray	サブRAIDアレイあたりの物理ドライブの数。このパラメータは、LSIコントローラ上のRAID 50アレイにのみ必要です。

表13ストレージコントローラーがサポートするRAIDレベル

ストレージコントローラー	RAIDレベル
HBA-1000-M2-1	RAID 0、RAID 1、およびRAID 10
HBA-H460-B1 HBA-H460-M1	RAID 0、RAID 1、RAID 5、およびRAID 10
HBA-H5408-Mf-8i	RAID 0、RAID 1、およびRAID 10
HBA-LSI-9311-8i-A1-X	RAID 0、RAID 1、およびRAID 10
RAID-P430-M1 RAID-P430-M2	RAID 0、RAID 1、RAID 5、RAID 6、RAID 10、RAID 50、シンプルボリューム
HBA-LSI-9440-8i	RAID 0、RAID 1、RAID 5、RAID 10、およびRAID 50
HBA-LSI-9540-LP-8i	RAID 0、RAID 1、およびRAID 10

OSの設定

このタスクについて

OSインストール用の構成テンプレートを作成するには、次のタスクを実行します。OSインストールテンプレートを構成する場合は、クローニング用にエクスポートされたOS、Linuxオペレーティングシステム、Windowsオペレーティングシステムおよび VMwareオペレーティングシステムをサポートするOS情報を構成する必要があります。

OSインストール用のサーバーテンプレートを正常に適用するには、**Menu > Templates > mages**ページでOSイメージファイルをアップロードする必要があります。

サポートされるオペレーティングシステム

サーバーテンプレートは、Red Hat Enterprise Linux、SUSE Linux Enterprise Server、CentOS、Oracle Linux、Ubuntu Server、VMware ESXi、CAS、penEuler、Kylin、Tianyi Cloud、Rocky Linux、H3LinuxおよびWindows Serverオペレーティングシステム(コアバージョンを除く)のインストールをサポートします。詳細は、表14を参照してください。

表14サポートされるオペレーティングシステム

OSの種類	バージョン
OSクローニング用にインポートされたイメージ	OSクローニングでサポートされるオペレーティングシステムについては、「クローンイメージ」を参照してください。
CentOS	CentOS 6.10(64ビット)
	CentOS 7.3(64ビット)
	CentOS 7.4(64ビット)
	CentOS 7.5(64ビット)
	CentOS 7.6(64ビット)
	CentOS 7.7(64ビット)
	CentOS 7.8(64ビット)
	CentOS 7.9(64ビット)
	CentOS 8.0(64ビット)
	CentOS 8.1(64ビット)
	CentOS 8.2(64ビット)
	CentOS 8.3(64ビット)
	CentOS 8.4(64ビット)
	Red Hat Enterprise Linux 6.7(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 6.8(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 6.9(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 6.10(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.2(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.3(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.4(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.5(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.6(64ビット)(KVMを含む)

Red Hat Enterprise Linux	Red Hat Enterprise Linux 7.7(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.8(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 7.9(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.0(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.1(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.2(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.3(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.4(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.5(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 8.6(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 9.0(64ビット)(KVMを含む)
	Red Hat Enterprise Linux 9.2(64ビット)(KVMを含む)
SUSE Linux Enterprise Server	SLES 11 SP4(64ビット)(XENおよびKVMを含む)
	SLES 12(64ビット)SP1(XENおよびKVMを含む)
	SLES 12(64ビット)SP2(XENおよびKVMを含む)
	SLES 12(64ビット)SP3(XENおよびKVMを含む)
	SLES 12(64ビット)SP4(XENおよびKVMを含む)
	SLES 12(64ビット)SP5(XENおよびKVMを含む)
	SLES 15(64ビット)(XENおよびKVMを含む)
	SLES 15(64ビット)SP1(XENおよびKVMを含む)
Ubuntuサーバー	Ubuntu Server 17.10(64ビット)-LTS
	Ubuntu Server 17.10.1(64ビット)-LTS
	Ubuntu Server 18.04(64ビット)-LTS
	Ubuntu Server 18.04.1(64ビット)-LTS
	Ubuntu Server 18.04.2(64ビット)-LTS
	Ubuntu Server 18.04.3(64ビット)-LTS
	Ubuntu Server 20.04.4(64ビット)-LTS
	Ubuntu Server 22.04(64ビット)-LTS
	Ubuntu Server 22.04.1(64ビット)-LTS
	Ubuntu Server 22.04.3(64ビット)-LTS
	Ubuntu Server 22.04.4(64ビット)-LTS
CAS	CAS 5.0 E0513
	CAS 5.0 E0526
	CAS 7.0 E0782
Oracle Linux 8.2	Oracle Linux 8.2
	Oracle Linux 8.6
	Oracle Linux 9.0
	VMware ESXi 6.5 U1(64ビット)

VMware ESXi	VMware ESXi 6.5 U2(64ビット)
	VMware ESXi 6.5 U3(64ビット)
	VMware ESXi 6.7(64ビット)
	VMware ESXi 6.7 U3(64ビット)
	VMware ESXi 7.0(64ビット)
	VMware ESXi 7.0 U2(64ビット)
	VMware ESXi 7.0 U3(64ビット)
	VMware ESXi 7.0 U2(64ビット)
CAS	CAS 5.0 E0513
	CAS 5.0 E0526
Oracle Linux	Oracle Linux 8.2
openEuler	openEuler 20.03 LTS SP3(x86_64用)
	openEuler 22.03 LTS(x86_64用)
	openEuler 22.03 LTS SP1(x86_64用)
Kylin	Kylinアドバンスドサーバーオペレーティングシステム V10 SP2
	Kylinアドバンスドサーバーオペレーティングシステム V10 SP3
Tianyi Cloud	CTyunOS 2.0.1 64ビット
Rocky Linux	Rocky Linux 8.6
	Rocky Linux 9.0
H3Linux	H3Linux 2.0.2-SP01
NingOS	NingOS V31.0.2306
	NingOS V31.0.2311
	NingOS V31.0.2403
Windows Server	Microsoft Hyper-V Server 2012 R2
	Microsoft Hyper-Vサーバー2016
	Microsoft Hyper-Vサーバー2019
	Microsoft Windows Server 2012 R2
	Microsoft Windows Server 2016
	Microsoft Windows Server 2019
	Microsoft Windows Server 2012 R2 Standard
	Microsoft Windows Server 2012 R2データセンター
	Microsoft Windows Server 2012 R2
	Microsoft Windows Server 2016 Essential
	Microsoft Windows Server 2016 Standard
	Microsoft Windows Server 2016データセンター
	Microsoft Windows Server 2019 Standardの場合
	Microsoft Windows Server 2019データセンター
	Microsoft Windows Server 2022 Standardの場合

	Microsoft Windows Server 2022データセンター

前提条件

- OSイメージファイルが存在し、サーバーテンプレートと同じOSが含ま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インストールするには、ターゲットドライブの容量がサーバーテンプレートのプライマリパーティションの要件を満たしていることを確認します。

手順

1. ページの**OS Settings**領域で、**Configure**をクリックします。
2. (省略可能)図151に示すように、RedHatまたはCentOSオペレーティングシステムを選択した場合は、応答ファイルの使用を選択できます。**Download Template**をクリックして、システムの応答ファイルテンプレートを取得します。必要に応じて応答ファイルテンプレートを変更し、応答ファイルの横にある.アイコンをクリックして、応答ファイルをアップロードします。

メモ:

OS Settings領域で**Use Answer File**を選択した場合は、テンプレートのダウンロードをクリックして、システムの応答ファイルテンプレートを取得します。応答ファイルを完全に自己定義すると、サーバーテンプレートは作成されません。応答ファイルの形式と使用方法については、次のガイドラインとテンプレートのreadmeファイルを参照してください。

図151応答ファイルの使用

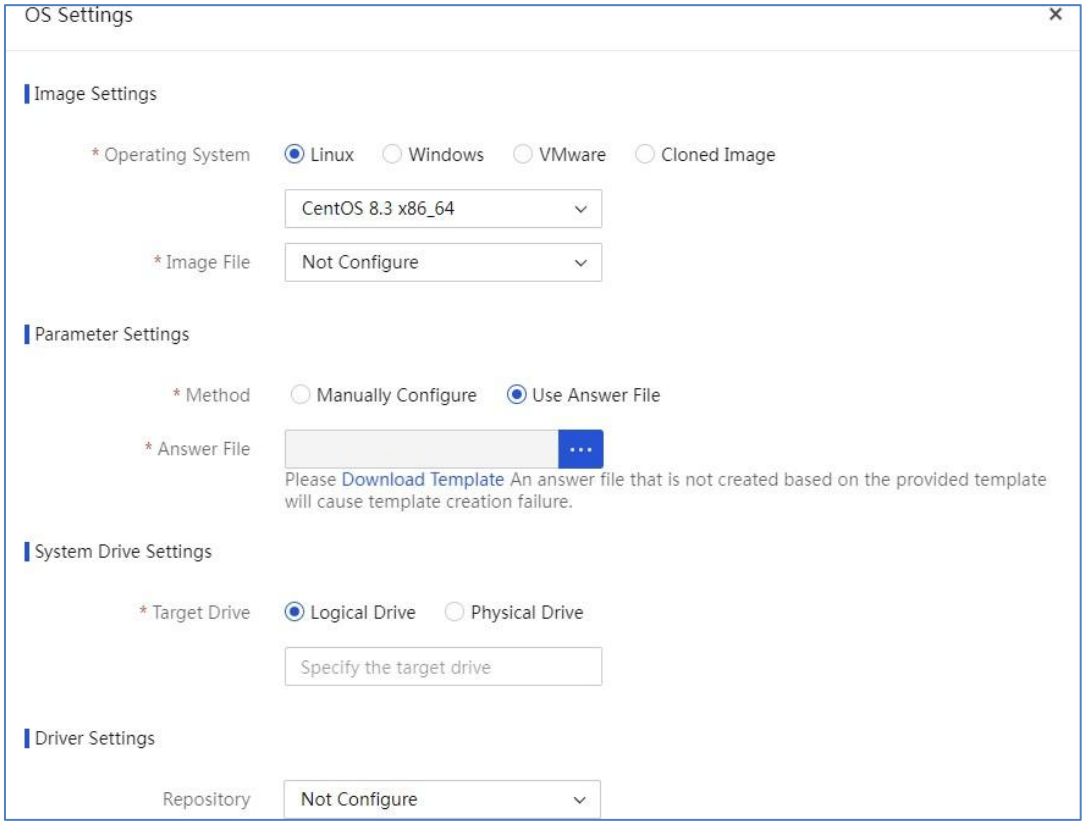


表15 応答ファイルを使用するためのパラメータ

パラメータ	備考
応答ファイル	オペレーティングシステムは、応答ファイルに従って自動的にインストールされます。ダウンロードしたテンプレートファイルに従って応答ファイルをカスタマイズできます(このオプションは、カスタム設定にのみ適用されます)。

3. OS関連のパラメータを構成します。使用可能なパラメータは、図152、図153および図154に示すように、OSのタイプによって異なります。必要に応じて、リポジトリからインストールするドライバーを選択できます。サーバーにオペレーティングシステムをインストールする場合、iFISTはオペレーティングシステムに必要な組込みドライバーも自動的にインストールします。iFIST組込みドライバーの詳細は、iFISTユーザーガイドを参照してください。

図152 Linux OSの設定

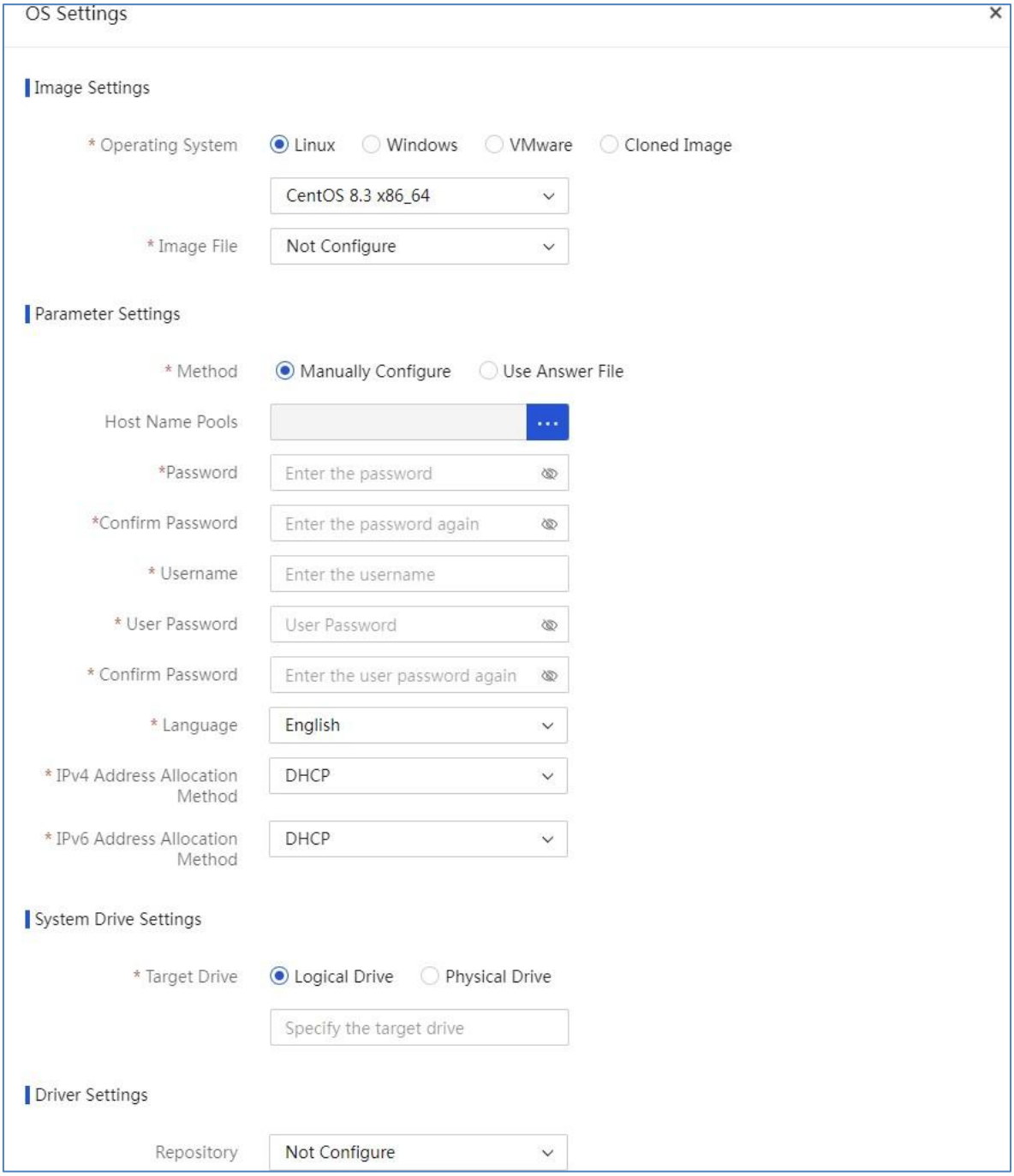


図153 VMware OSの設定

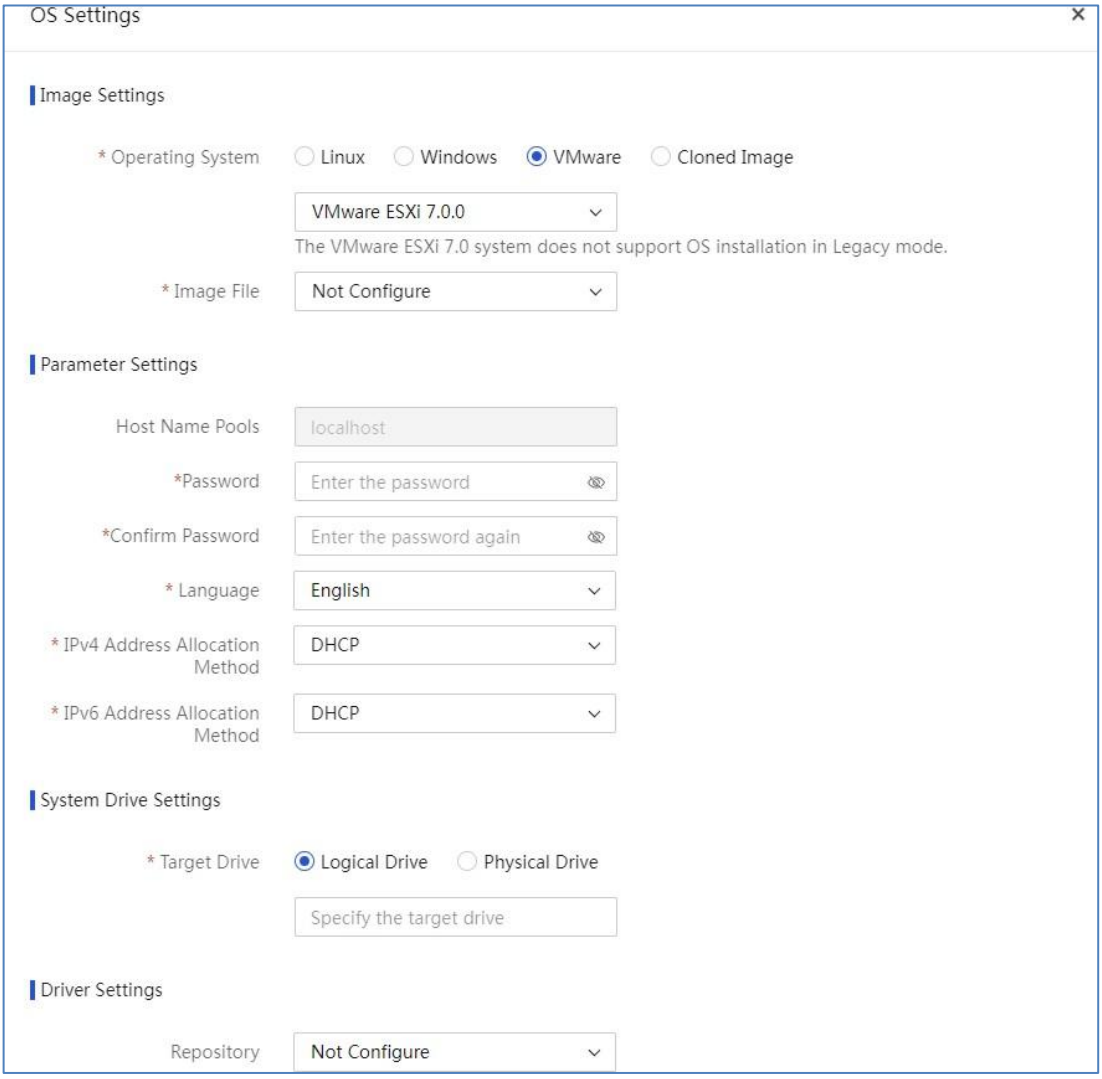


表16 OS設定のパラメータ

パラメータ	備考
オペレーティングシステム	オペレーティングシステムタイプおよびオペレーティングシステム名を選択します。OS Settingsは、選択したオペレーティングシステムタイプによって異なります。
管理ソフトウェアパッケージ(CAS 7.0システムのみ)	クラウドコンピューティング管理プラットフォームのインストールパッケージを選択します。オプションには、CVK、CVM-中国語、およびCVM-英語があります。 • サービスサーバー(VMが常駐する物理ホスト)をインストールする場合、Cloud Virtualization Kernel(CVK)を選択します。CVKは、インフラストラクチャ層と上位層のクライアントオペレーティングシステム間で実行される仮想化カーネルソフトウェアを表します。 • 管理サーバー(サービスサーバーを集中管理するサーバー)をインストールする場合は、Cloud Virtualization Manager(CVM)Cloud Virtualization Manager(CVM)□を選択します。CVMは主に、データセンター内のコンピューティング、ネットワークおよびストレージハードウェアリソースのソフトウェア仮想化管理を提供し、上位層アプリケーションに自動化されたサービスを提供します。
(オプション)ホスト	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の名前。

パラメータ	備考
Name	ホスト名プール内のホスト名範囲。ホスト名プールの詳細については、「ホスト名プールの管理」を参照してください。 Linuxオペレーティングシステムのデフォルトのホスト名はlocalhostです。 VMware ESXiオペレーティングシステムのIPv4アドレス割り当て方法としてDHCPを選択した場合、Host Nameフィールドは使用できません。 Operating SystemフィールドでCloned Imageを選択した場合、デフォルトのホスト名には、ソースオペレーティングシステムのホスト名が使用されます。
Password	システムにログインするためのパスワード。Linuxオペレーティングシステムを選択した場合、パスワードはrootパスワードです。
Username	root以外のユーザーのユーザー名。 **メモ:** • このオプションは、Linuxオペレーティングシステムにのみ適用されます。 • このオプションは、VMware ESXiまたはCASオペレーティングシステムには適用されません。 • Ubuntuシステムでユーザー名を構成する場合は、rootやadminなど、Ubuntuシステムの予約されたユーザー名を使用しないでください。
ユーザーパスワード	システムにログインするための非rootユーザーのパスワード。このオプションは、Linuxオペレーティングシステムにのみ適用されます。 このオプションは、VMware ESXiまたはCASオペレーティングシステムには適用されません。
言語	オペレーティングシステムの言語: • 簡体字中国語 • 英語。 **メモ:** このオプションは、VMware ESXiまたはCASオペレーティングシステムには適用されません。
IPv4アドレスの割り当て方法	オプションは、DHCPとStaticです。Staticを選択した場合、IPv4アドレスプールのアドレス範囲を選択する必要があります。IPv4アドレスプールの詳細は、「IPv4アドレスプールの管理」を参照してください。 **メモ:** CAS 5.0オペレーティングシステムはDHCPをサポートしていません。
IPv6アドレスの割り当て方法	オプションはDHCPと静的です。静的を選択した場合は、IPv6アドレスプールのアドレス範囲を選択する必要があります。IPv6アドレスプールの詳細については、「IPv6アドレスプールを管理する」を参照してください。 **メモ:** • VMware ESXiオペレーティングシステムは、DHCP方式のみをサポートします。 • CAS 5.0オペレーティングシステムはIPv6をサポートしていません。 • Ubuntuサーバーオペレーティングシステムは、IPv4アドレス割り当て方法が静的に設定されている場合はIPv6をサポートしません。また、IPv6アドレス割り当て方法が静的に設定されている場合はIPv4をサポートしません。
ターゲットドライブ	オペレーティングシステムをインストールするドライブ。
リポジトリ	リポジトリを選択します。使用可能なオプションは、リポジトリライブラリ内のリポジトリです。インベントリされたリポジトリを選択すると、OS Settingsページで選択したオペレーティングシステムに適用可能なドライバーがリストに表示されます。

図154 Windows OSの設定

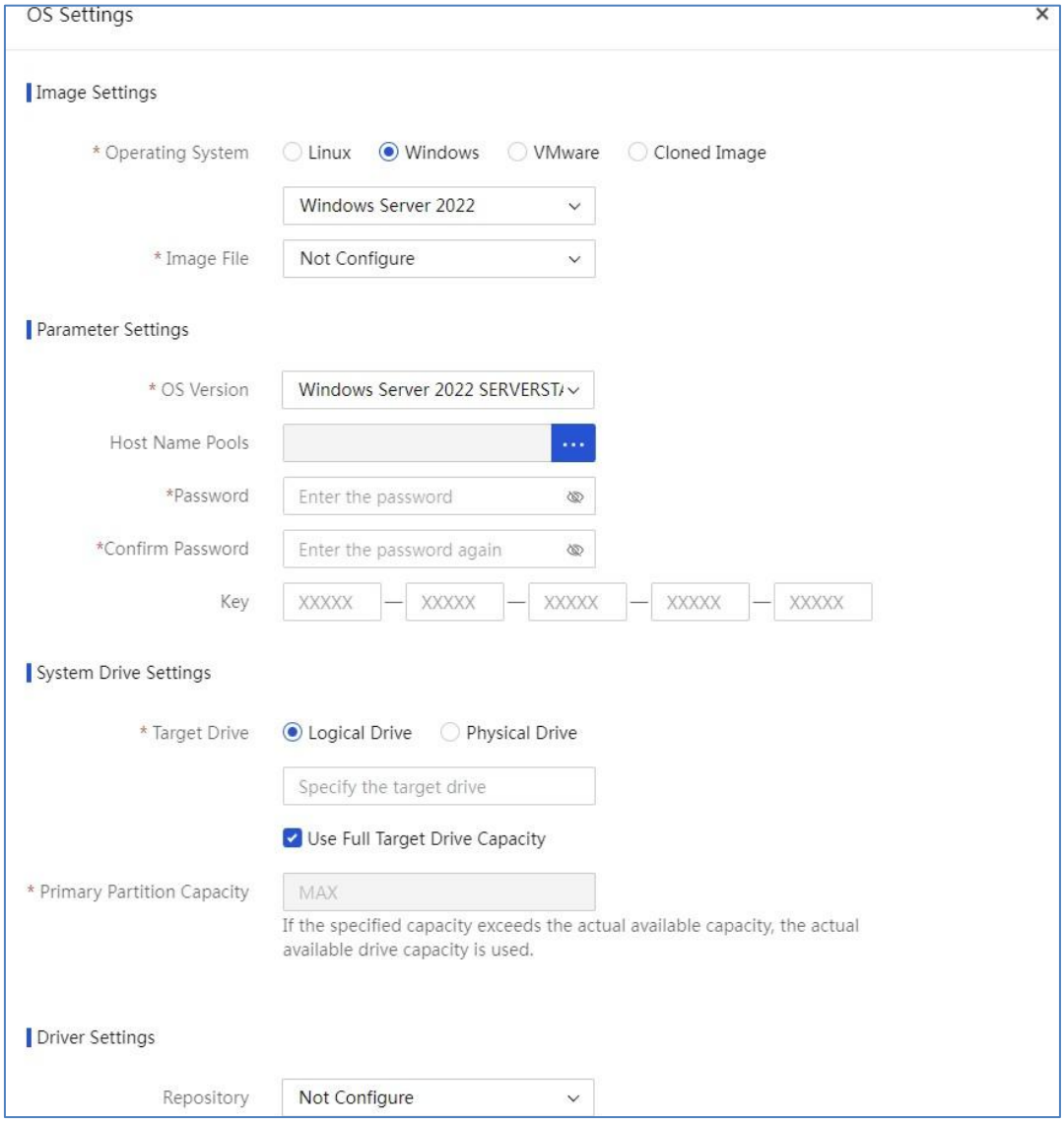


表17 Windows OS設定のパラメータ

パラメータ	備考
OSバージョン	OSのバージョンを選択します(このオプションは、複数のバージョンをサポートするオペレーティングシステムにのみ適用されます)。
(オプション)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の名前。このフィールドがWindowsオペレーティングシステムで空のままである場合、Windowsオペレーティングシステムは自動的にホスト名を割り当てます。
プライマリパーティションの容量	オペレーティングシステムがインストールされるシステムパーティションの容量(51200 MBから10485760 MBの範囲)。Use Full Logical Drive Capacity選択すると、プライマリパーティションの容量は使用可能な最大値に設定されます。オペレーティングシステムを正常にインストールするには、容量が50 GB以上であることを確認します。物理ドライブの容量が大きい場合は、プライマリパーティションの容量を最大値に設定することをお薦めします。(このオプションは、Windowsオペレーティングシステムにのみ適用されます。Linuxオペレーティングシステムでは、プライマリパーティションの容量は次のとおりです。 は表示されず、デフォルトで使用可能な最大値が使用されます。 必要な最小ドライブ容量は80 GBです)。

HDM/BIOSテンプレートの設定

このタスクについて

サーバーのHDM/BIOS設定をエクスポートして構成テンプレートファイルを生成するには、次のタスクを実行します。その後、構成テンプレートファイルを指定したサーバーに適用できます。この機能を使用すると、複数のサーバーのHDM設定およびBIOS設定を同時にコピーまたは構成できます。構成テンプレートファイルを使用して、サーバーの現在の設定をバックアップすることもできます。

この機能は、HDMインターフェイスに依存します。サーバーにインポートされたHDM設定は、HDMの再起動後に有効になります。サーバーにインポートされたBIOS設定は、サーバーの再起動後に有効になります。

メモ:

この機能を使用するには、最初にHDMサーバーノードをUniSystemに追加する必要があります。詳細は、「サーバーの管理」を参照してください。

HDM/BIOS設定のエクスポート

前提条件

- サーバーの設定をエクスポートする前に、サーバーのHDMまたはBIOSが正しく動作していることを確認します。
- 設定をエクスポートする権限は、HDMアカウントのネットワーク権限に依存します。ユーザーにこの操作の権限があることを確認してください。
- エクスポートプロセス中は、別のページに切り替えたり、ページをリフレッシュしたり、その他の構成管理操作を実行したりしないでください。
- 最大40個のHDM/BIOS設定テンプレートファイルを保存できます。上限に達した場合は、頻繁に使用しない設定テンプレートファイルを手動で削除してください。

手順

1. 図155に示すように、管理対象サーバーの**Export**列で**HDM Settings**または**BIOS Settings**をクリックします。

   ターゲットサーバーをすばやく除外するには、左側のナビゲーションウィンドウから動的グループと静的グループを使用するか、検索領域にキーワードを入力します。

   図155 HDM/BIOS設定テンプレート



2. 表示されるダイアログボックスで、テンプレートの説明を入力します(オプション)。
3. **OK**をクリックすると設定のエクスポートが開始されます。生成されるテンプレートファイルは自動的に**[HDM/BIOS]CONFCOPY+***設定がエクスポートされた時刻*.**json**という名前になります。

テンプレートの管理

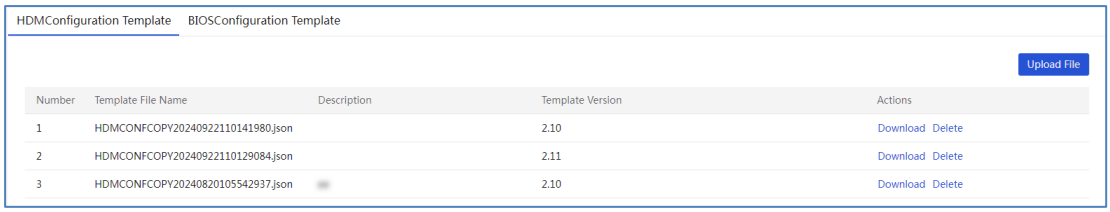
このタスクについて

設定テンプレートを削除、ダウンロード、およびアップロードするには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **HDM/BIOS Templates**を選択します。
2. 図156に示すように、**Templates**をクリックしてテンプレート管理ページに入ります。

   図156テンプレート



3. **HDM Templates**タブまたは**BIOS Templates**タブをクリックします。
4. **Upload File**をクリックします。
5. 表示されたダイアログボックスで、**Upload File**フィールドの...アイコンをクリックし、アップロードするコンフィギュレーションファイルを選択します。
6. (任意)テンプレートの説明を入力します。
7. OKをクリックします。

   図157ファイルのアップロード



8. (任意)設定テンプレートファイルをダウンロードするには、ダウンロードするテンプレートの**Download**をクリックし、設定テンプレートファイルを保存するパスを選択して、**OK**をクリックします。
9. (任意)設定テンプレートファイルを削除するには、削除するテンプレートの**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

リポジトリの設定

このタスクについて

レポジトリとは、各種オプションカードおよびシステムボード用の各種ドライバーと、各種HDM、BIOS、CPLD、ドライブ、およびオプションカード用のファームウェアが格納されている圧縮ファイル

です。ファームウェアとドライバーは、まとめてコンポーネントと呼ばれます。

このメニューから、リポジトリを追加、編集、削除、インベントリおよびカスタマイズできますAdd a repositoryを使用してリポジトリを手動でアップロードするか、Enable LastestREPO updateを使用してリポジトリを自動的にアップロードできます。

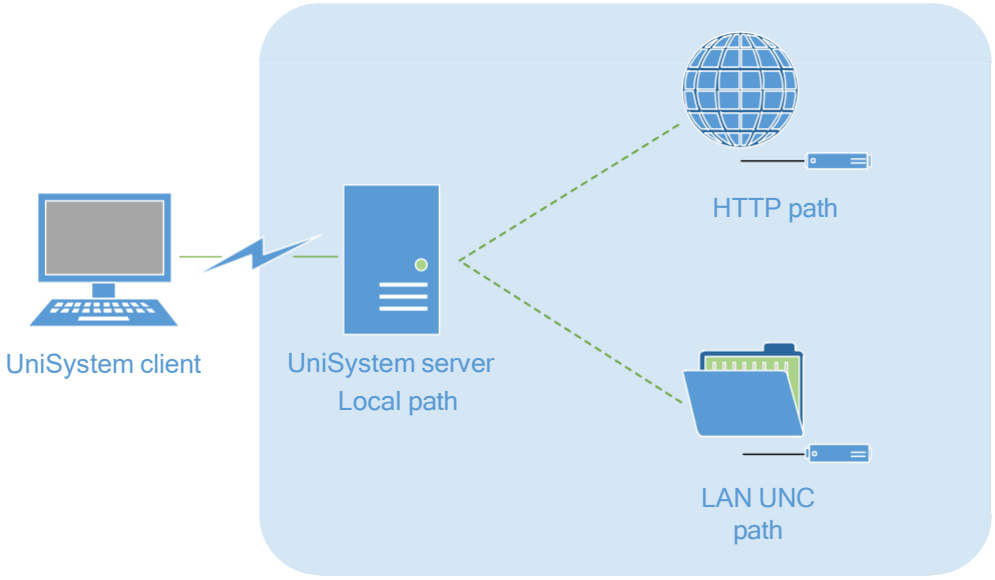
この機能をコンポーネントの更新機能と共に使用すると、サーバーのファームウェアとドライバーを一括更新できます。

重要:

コンポーネントの更新プロセスでドライバーを更新するには、管理対象サーバーにFIST SMSがインストールされていることです。

ネットワークダイアグラム

図158ネットワークダイアグラム



リポジトリを追加する

バージョン2.00.22では、リポジトリが追加されると、UniSystemは自動的にリポジトリをインベントリします。

前提条件

リポジトリを準備し、リポジトリを取得するためのパスタイプとパスを準備します。表18に示すように、リポジトリパスには3つのタイプがあります。

表18リポジトリのパスタイプ

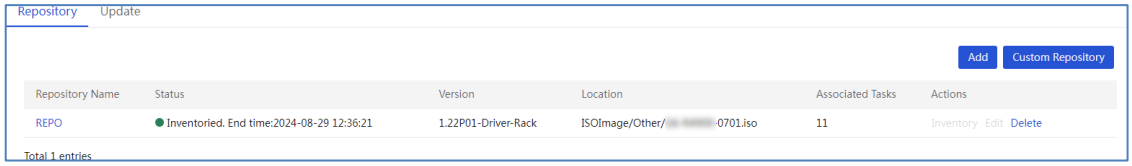
タイプ	備考
UNCパス	ネットワークパス。リソースを共有することで、LAN内のリポジトリリソースを取得できます。
HTTPパス	HTTPサーバーパス。このパスを介して、指定したHTTPサーバー上のリポジトリリソースを取得できます。

ローカルパス	ローカルパス。このパスを使用して、UniSystemクライアント上のリポジトリリソースを取得できます。

手順

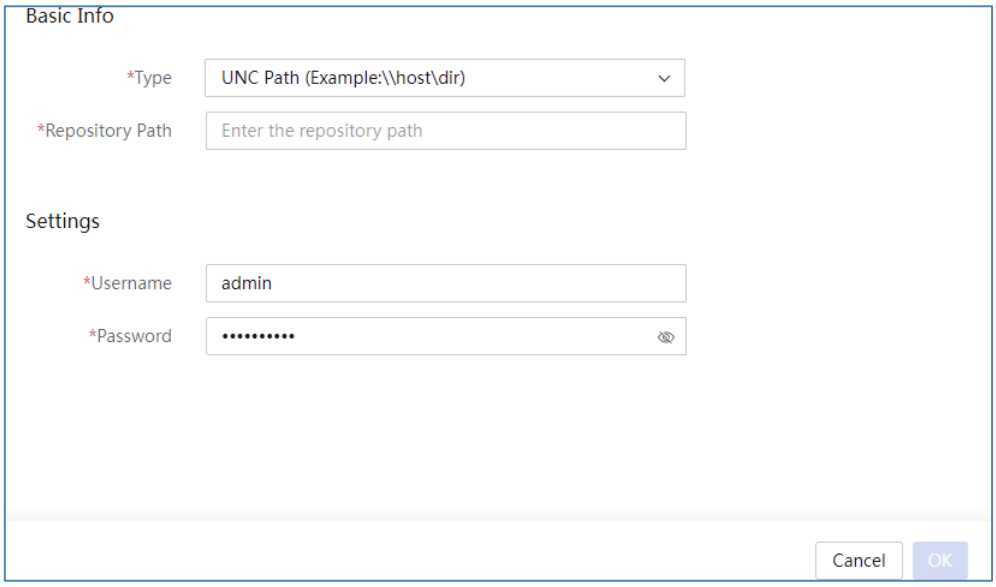
1. ナビゲーションペインで、**Menu** > **Templates** > **Repositories**を選択して、図159に示すページに入ります。

   図159リポジトリ管理ページ



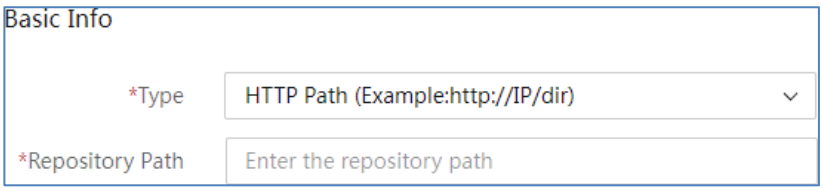
2. **Add**をクリックします。表示されたダイアログボックスで、必要に応じてパラメータを設定します。
   - 図160に示すように、**UNC Path**を選択した場合は、リポジトリのパス、ユーザー名、パスワードを入力し、**OK**をクリックする必要があります。

     図160 UNCパスでのリポジトリの追加



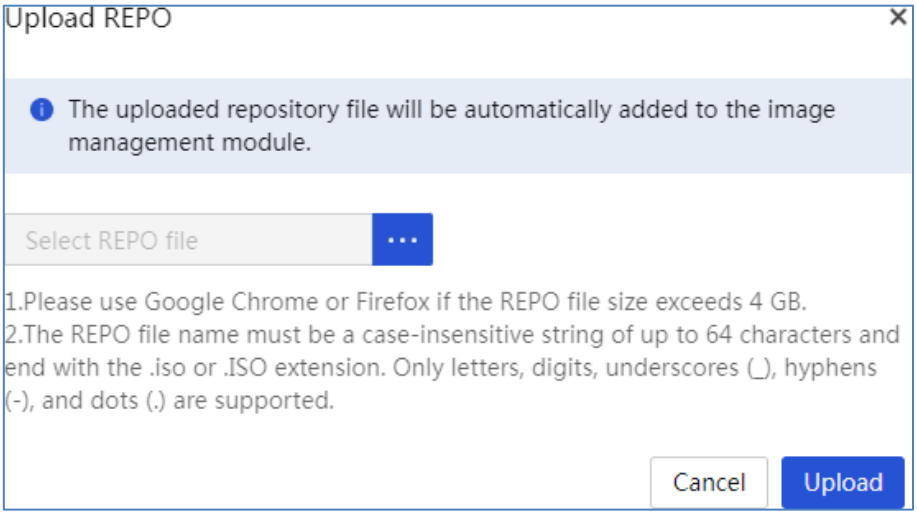
   - 図161に示すように**HTTP Path**を選択した場合は、次の手順を実行します。
     - リポジトリのパスを入力します。
     - プロキシを使用してHTTPサーバーに接続するには、**Menu** > **System** > **System** > **Proxy Settings**を選択します。
       詳細については、「プロキシ設定の構成」を参照してください。
     - **OK**をクリックします。

     図161 HTTPパスリポジトリ



- 図162に示すように**Local Path**を選択した場合は、次の手順を実行します。
  - **Upload**をクリックします。
  - 開いたダイアログボックスで、リポジトリファイルを選択し、**Upload**をクリックします。

図162ローカルパスへのリポジトリの追加



ローカルリポジトリをUniSystemに追加すると、リポジトリリストには新しく追加されたリポジトリが表示され、リポジトリは**Menu** > **Templates** > **Images**のイメージリストに自動的に追加されます。

リポジトリのインベントリを作成する

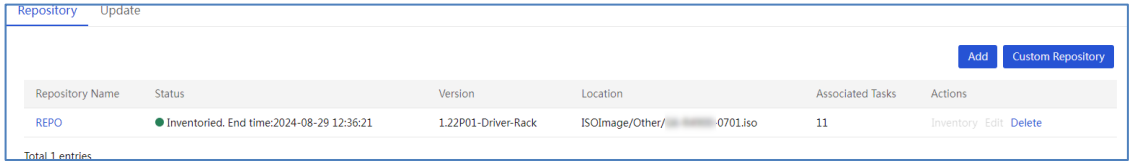
このタスクについて

リポジトリ内のすべてのコンポーネントをリストするには、次のタスクを実行します。リポジトリがインベントリされると、そのコンポーネントリストに対応するコンポーネントが表示されます。この場合、リポジトリは適切に使用できます。

手順

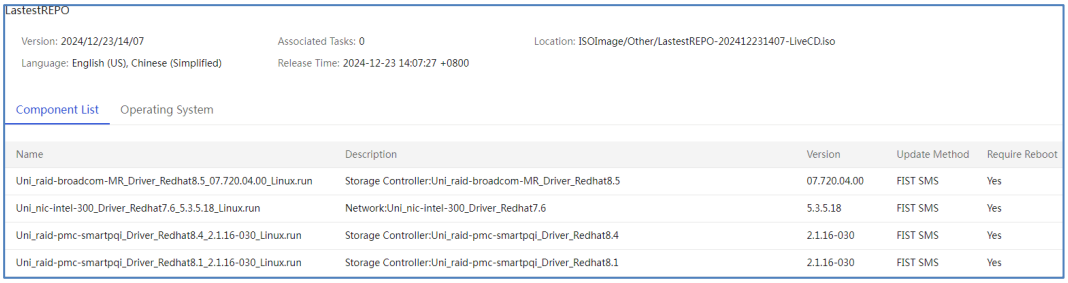
1. 図163に示すように、インベントリするリポジトリの**Actions**列で**Inventory**をクリックします。これにより、UniSystemは選択したリポジトリを自動的にインベントリします。

   図163 リポジトリのインベントリ



2. 図163に示すように、インベントリが完了すると、リポジトリの**Status**列に**Inventoried**とインベントリが完了した時刻が表示されます。
3. ターゲットリポジトリの**Repository Name**列のリンクをクリックします。図164に示すように、リポジトリの詳細ページが開き、リポジトリ情報が表示されます。

図164リポジトリの詳細



(オプション)カスタムリポジトリまたはISOファイルを作成します。

このタスクについて

追加およびインベントリされたリポジトリから指定したコンポーネントの更新パッケージを選択し、それらを使用してカスタムリポジトリまたはISOファイルを作成するには、このタスクを実行します。

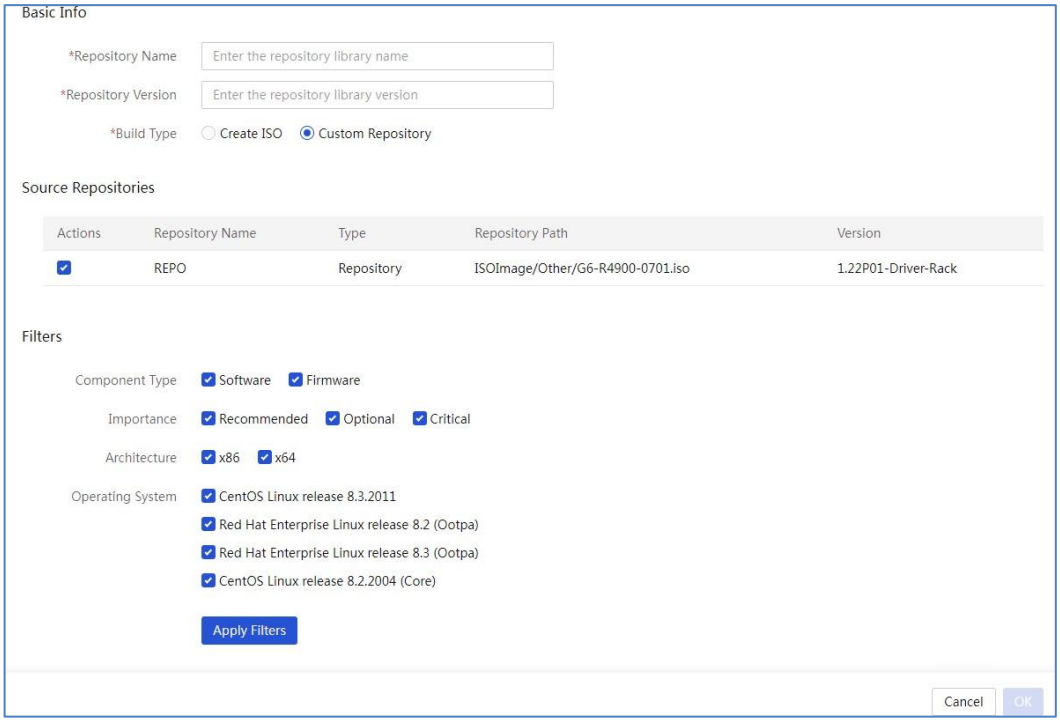
- カスタムリポジトリを作成したら、それを使用してコンポーネントをアップグレードできます。
- カスタムISOファイルを作成すると、ISOイメージファイルが生成されます。

バージョン2.00.22では、UniSystemはカスタムリポジトリが追加された後、自動的にカスタムリポジトリをインベントリします。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Repositories**を選択して、リポジトリ管理ページを開きます。
2. **Custom Repository**をクリックします。表示されるダイアログボックスで、次の手順を実行します。
   a. **Basic Info**領域で、リポジトリの名前とバージョンを入力し、**Create ISO**を選択します。または**Build Type**の**Custom Repository**。
   b. **Source Repositories**領域で、ターゲットリポジトリを選択します。
   c. **Filters**領域で、ターゲットアイテムを選択し、**Apply Filters**をクリックして一致するアイテムを表示します。
   d. コンポーネントリストで、ターゲットコンポーネントを選択します。

図165 カスタムリポジトリの作成



3. **OK**をクリックします。

リポジトリを編集する

このタスクについて

ユーザーによって追加されたがインベントリされていないリポジトリを編集するには、このタスクを実行します。カスタムリポジトリ、ローカルリポジトリまたはインベントリされたリポジトリは編集できません。リポジトリの追加方法に応じて、次のいずれかのタスクを実行できます。

- UNCパスを使用して追加されたリポジトリでは、共有サーバーのユーザー名とパスワードが変更された場合、UniSystem上の情報を同期的に編集する必要があります。
- HTTPサーバーパスを介して追加されたリポジトリの場合、HTTPサーバーのプロキシオプションが**No Proxy**と**Manually Configure**の間で変更されたときは、UniSystemの情報を同期的に編集する必要があります。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Repositories**を選択します。
2. 編集するリポジトリの**Actions**コラムで**Edit**をクリックします。
3. 表示されるダイアログボックスで、次のタスクを実行します。
   - UNCパスを使用して追加されたリポジトリの場合、編集できるのは共有サーバーのユーザー名とパスワードだけです。
   - HTTPサーバーパスを介して追加されたリポジトリの場合、プロキシオプションを**No Proxy**と**Manually Configure**の間で切り替え、関連するパラメータを構成できます。
4. **OK**をクリックします。

LastestREPO更新を有効にする

このタスクについて

この機能を有効にすると、UniSystemは、ユーザーが設定した更新間隔と時間に基づいて、LiveCDの最新バージョンとすべてのコンポーネントパッケージに関する情報をREPOオンラインプラットフォームから定期的に取得します。次に、システムは、管理対象サーバーに適したコンポーネントを除外し、イメージプール内の古いバージョンを置き換えるために新しいLiveCD REPOパッケージを生成します。また、REPOを置き換えるための自動同期もサポートしています。

- LastestREPO機能は、「サーバーテンプレートの管理」のスケジュールされた更新機能と組み合わせることで、サーバーコンポーネントを最新バージョンに自動的に更新できます。
- LastestREPO機能は、「コンポーネントの更新」機能と組み合わせることで、サーバーコンポーネントを最新バージョンにタイムリーに更新できます。

メモ:

- LastestREPOアップデートを有効にする前に、UniSystemサーバードレスとREPOオンラインプラットフォームのドメインアドレスが正しく通信できることを確認してください。
- LastestREPO更新機能は、ユーザーに手動でアップロードされたREPOパッケージには影響しません。

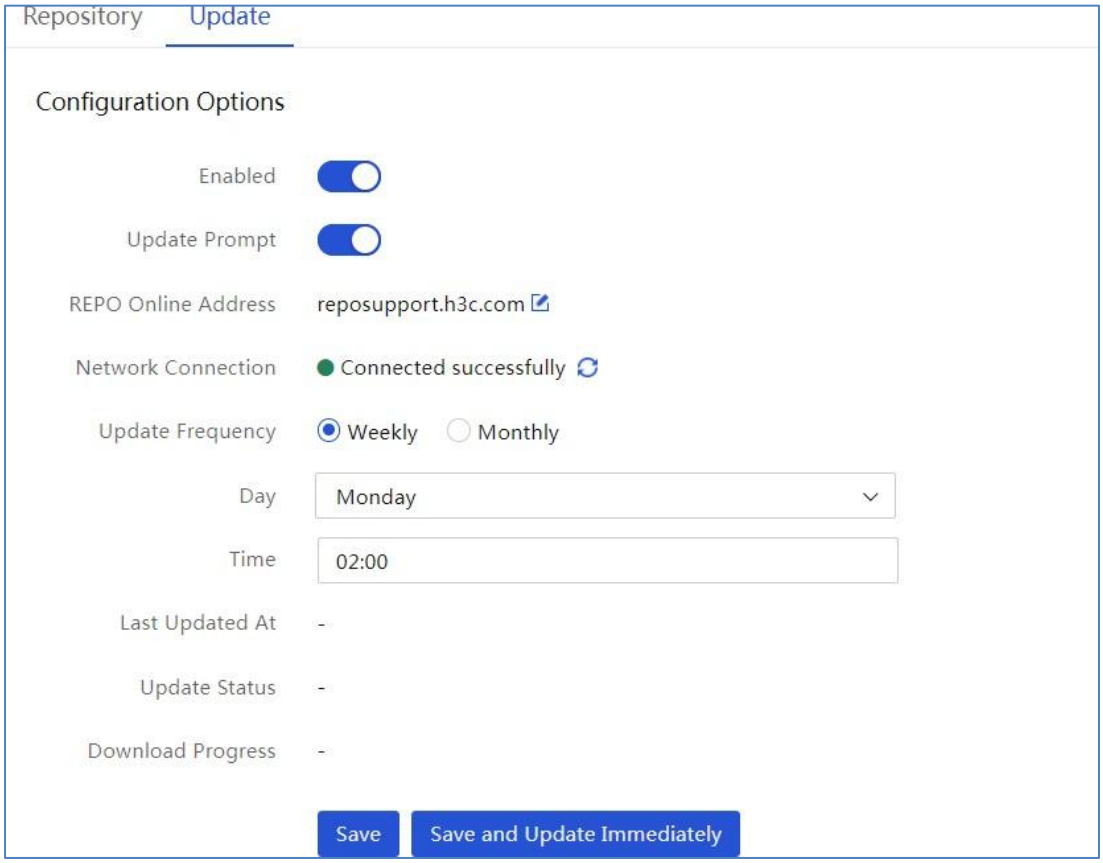
制約事項とガイドライン

更新プロンプトを有効にした後、UniSystemがREPOパッケージの最新バージョンのダウンロードと更新を開始すると、ダウンロードの進行状況または更新ステータスを確認するためのプロンプトがWebページに表示されます。このプロンプトは、ユーザーが手動でプロンプトをクリックするか、更新プロンプト機能を無効にした場合にのみ表示されます。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Repositories**を選択します。
2. **Update**タブをクリックします。

図166 LastestREPOの更新



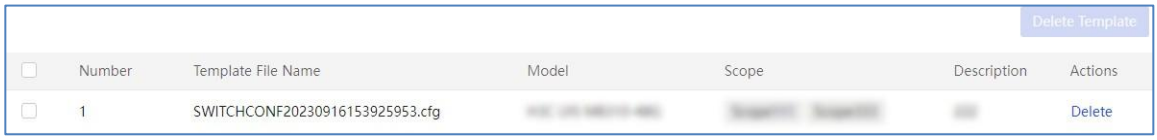
3. この機能を有効にします。
4. 更新プロンプトを有効にします。
5. アイコンをクリックし、REPO公式Webサイトのドメイン名アドレスを入力します。
6. アイコンをクリックすると、ネットワーク接続ステータスが更新されます。
7. ネットワーク接続に失敗した場合は、推奨されるアクションに基づいて問題をトラブルシューティングします。
8. 更新頻度を指定します。
9. **Save**をクリックします。更新構成が保存され、配布されます。
10. (オプション)**Save and Update Immediately**をクリックします。更新がただちに実行されます。

スイッチテンプレートの管理

スイッチテンプレートリストページにアクセスする

1. ナビゲーションペインで、**Menu > Templates > Switch Templates**を選択します。
2. スイッチテンプレートリストにあるスイッチテンプレートに関する情報を表示します。

図167スイッチテンプレートリストページ



スイッチテンプレートの削除

1. ナビゲーションペインで、**Menu > Templates > Switch Templates**を選択します。
2. 削除するスイッチテンプレートを選択し、右上隅にある**Delete Template**をクリックします。または、削除するスイッチテンプレートの**Actions**カラムで**Delete**をクリックします。
3. 表示された確認ダイアログボックスで**OK**をクリックします。

アドレスプールの管理

このメニューから、IPv4アドレスプール、IPv6アドレスプールおよびホスト名プールを作成、編集、削除および表示できます。アドレスプールを作成した後は、サーバーテンプレートの追加時に**OS Settings**領域でホスト名プール、IPv4アドレスプールまたはIPv6アドレスプールを手動で構成するのではなく、選択できます。この機能により、構成の効率が大幅に向上します。

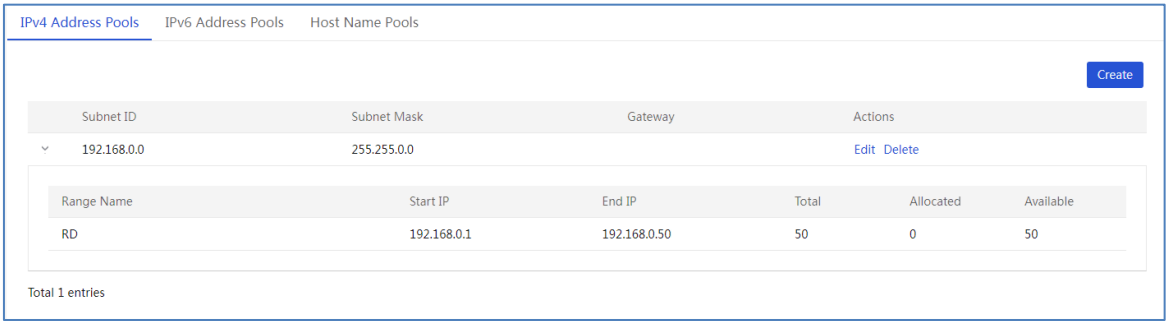
IPv4アドレスプールを管理する

IPv4アドレスプールの表示

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv4 Address Pools**タブをクリックします。IPv4アドレスプールの一覧が表示されます。

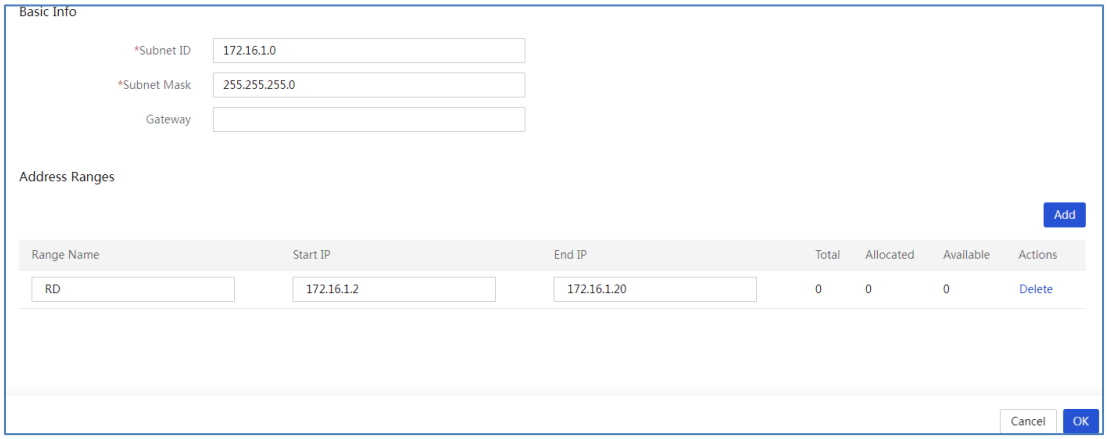
図168 IPv4アドレスプール



IPv4アドレスプールを作成する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv4 Address Pools**タブをクリックします。**Add**をクリックして、**Create IPv4 Address Pool**ページを開きます。

図169 IPv4アドレスプールの作成



3. IPv4サブネットID、サブネットマスク、およびゲートウェイ(オプション)を入力します。
4. **Address Ranges**領域で、**Add**をクリックします。アドレス範囲名、開始IP、および終了IPを入力します。
5. さらにアドレス範囲を追加するには、上記の手順を繰り返します。
6. **OK**をクリックします。

IPv4アドレスプールを編集する

制約事項とガイドライン

アドレス範囲を持つIPv4アドレスプールの場合、サブネットIDまたはサブネットマスクは編集できません。

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv4 Address Pools**タブをクリックします。
3. 編集するアドレスプールの**Actions**カラムで**Edit**をクリックします。必要に応じて、アドレスプールを編集します。
4. **OK**をクリックします。

IPv4アドレス範囲を削除する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv4 Address Pools**タブをクリックします。
3. 編集するアドレスプールの**Actions**カラムで**Edit**をクリックします。
4. **Address Ranges**領域で、削除するアドレス範囲の**Actions**カラムの**Delete**をクリックします。

IPv4アドレスプールを削除する

制約事項とガイドライン

IPv4アドレスプールを削除すると、IPv4アドレスプール内のすべてのアドレス範囲が削除されます。

手順

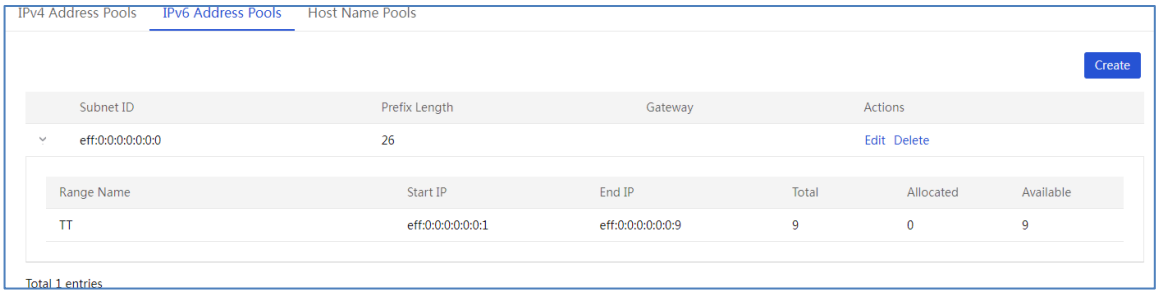
1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv4 Address Pools**タブをクリックします。
3. 削除するIPv4アドレスプールの**Actions**カラムで**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

IPv6アドレスプールを管理する

IPv6アドレスプールの表示

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv6 Address Pools**タブをクリックします。IPv6アドレスプールリストを表示します。

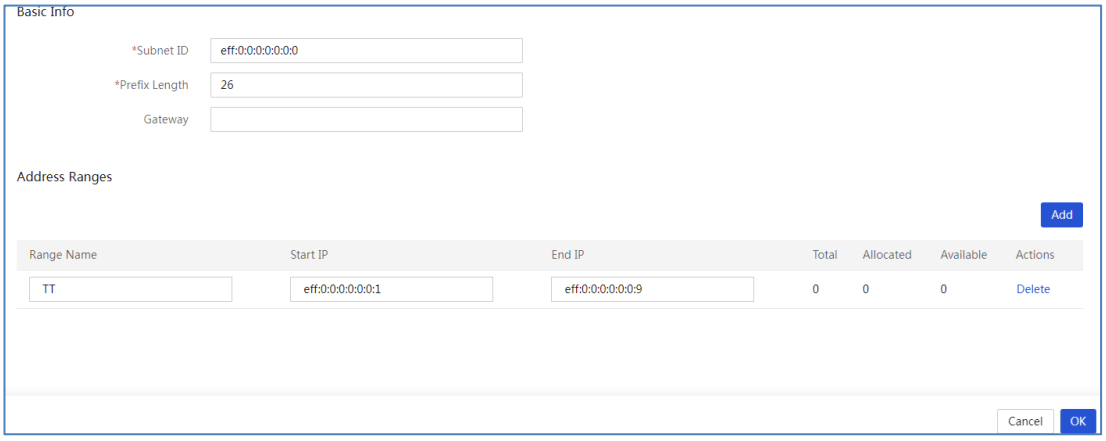
図170 IPv6アドレスプール



IPv6アドレスプールを作成する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Create IPv4 Address Pool**をクリックします。**Add**をクリックして、**Create IPv6 Address Pool**ページを開きます。

   図171 IPv6アドレスプールの作成



3. IPv6サブネットID、プレフィクス長、およびゲートウェイ(任意)を入力します。
4. **Address Ranges**領域で、**Add**をクリックします。アドレス範囲名、開始IP、および終了IPを入力します。
5. さらにアドレス範囲を追加するには、上記の手順を繰り返します。
6. **OK**をクリックします。

IPv6アドレスプールを編集する

制約事項とガイドライン

アドレス範囲のあるIPv6アドレスプールでは、サブネットIDまたはプレフィクス長を編集できません。

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。

2. **IPv6 Address Pools**タブをクリックします。
3. 編集するアドレスプールの**Actions**カラムで**Edit**をクリックします。必要に応じて、アドレスプールを編集します。
4. **OK**をクリックします。

IPv6アドレス範囲を削除する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv6 Address Pools**タブをクリックします。
3. 編集するアドレスプールの**Actions**カラムで**Edit**をクリックします。
4. **Address Ranges**領域で、削除するアドレス範囲の**Actions**カラムの**Delete**をクリックします。

IPv6アドレスプールを削除する

制約事項とガイドライン

IPv6アドレスプールを削除すると、IPv6アドレスプール内のすべてのアドレス範囲が削除されます。

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **IPv6 Address Pools**タブをクリックします。
3. 削除するIPv6アドレスプールの**Actions**カラムで**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

ホスト名プールの管理

サーバーテンプレートを追加する場合、OS Settings領域でホスト名プールを手動で構成するかわりに、ホスト名プールを直接選択できます。サーバーテンプレートを複数のサーバーに適用してこれらのサーバーにOSをインストールすると、手動で構成しなくても、接頭辞+索引+接尾辞の形式でこれらのサーバーのホスト名が生成されます。この機能を使用すると、サーバーを簡単に識別でき、構成の効率が向上します。

ホスト名プールの表示

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Host Name Pools**タブをクリックします。ホスト名プールリストが表示されます。

図172ホスト名プール

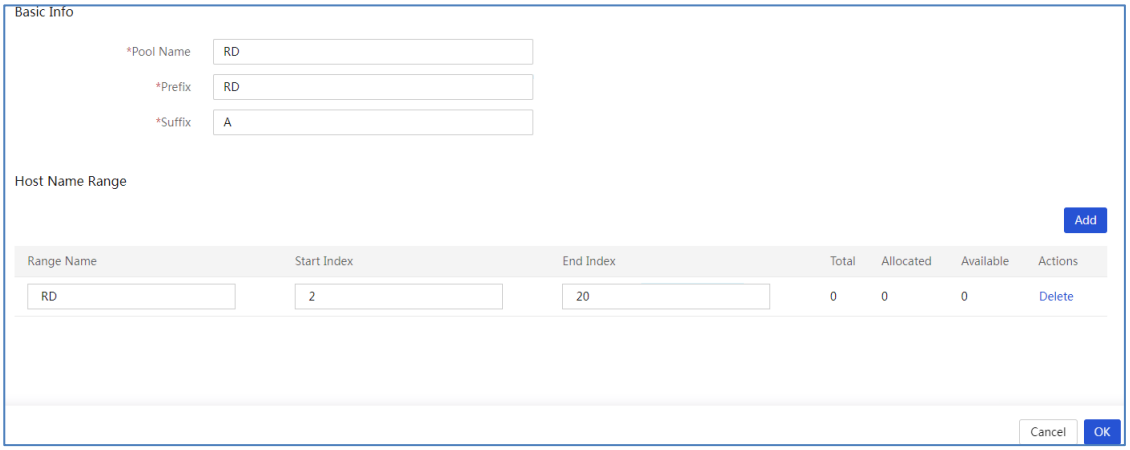


ホスト名プールを作成する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Host Name Pools**タブをクリックします。**Add**をクリックして、**Create Host Name Pool**ページに移

動します。

図173ホスト名プールの作成



3. ホスト名プール名、プレフィクス、およびサフィックスを入力します。
4. **Host Name Ranges**領域で、**Add**をクリックします。ホスト名範囲の名前、開始インデックス、および終了インデックスを入力します。
5. さらにホスト名範囲を追加するには、上記の手順を繰り返します。
6. **OK**をクリックします。

ホスト名プールを編集する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Host Name Pools**タブをクリックします。
3. 編集するホスト名プールの**Actions**列で**Edit**をクリックします。必要に応じて、ホスト名プールを編集します。
4. **OK**をクリックします。

ホスト名範囲を削除する

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Host Name Pools**タブをクリックします。
3. 編集するホスト名プールの**Actions**カラムで**Edit**をクリックします。
4. **Host Name Ranges**領域で、削除するホスト名範囲の**Actions**カラムの**Delete**をクリックします。

ホスト名プールを削除する

制約事項とガイドライン

ホスト名プールを削除すると、ホスト名プール内のすべてのホスト名範囲が削除されます。

手順

1. ナビゲーションペインで、**Menu > Templates > Address Pools**を選択します。
2. **Host Name Pools**タブをクリックします。
3. 削除するホスト名プールの**Actions**列で**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

ネットワークテンプレートを管理する

このメニューから、UniSystemのネットワークテンプレートまたはインターコネクトモジュールテンプレートを作成、編集、削除および表示できます。その後、次の場合にネットワークおよびインターコネクトモジュールテンプレートを使用できます。

サーバーテンプレートでの接続の構成。詳細については、「サーバーテンプレートを管理する」の接続設定を参照してください。

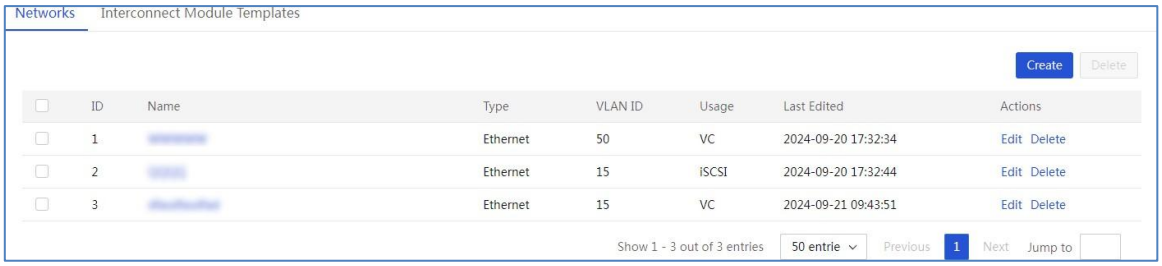
ネットワークの管理

このメニューから、UniSystemのネットワークを作成、編集、削除、および表示できます。

ネットワークを表示する

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
   タブをクリックします。
2. ネットワークリストのネットワークに関する情報を表示します。ネットワーク名の形式は、ネットワークの作成時に単一のVLAN IDが指定されたか、VLAN IDの範囲が指定されたかによって異なります。
   - VLAN IDの範囲を指定した場合、ネットワーク名はNetwork Name_VLAN IDの形式になります。たとえば、wl1_10となります。
   - 単一のVLAN IDが指定された場合、ネットワーク名はNetwork Nameの形式になります。たとえば、Testです。

図174 ネットワーク

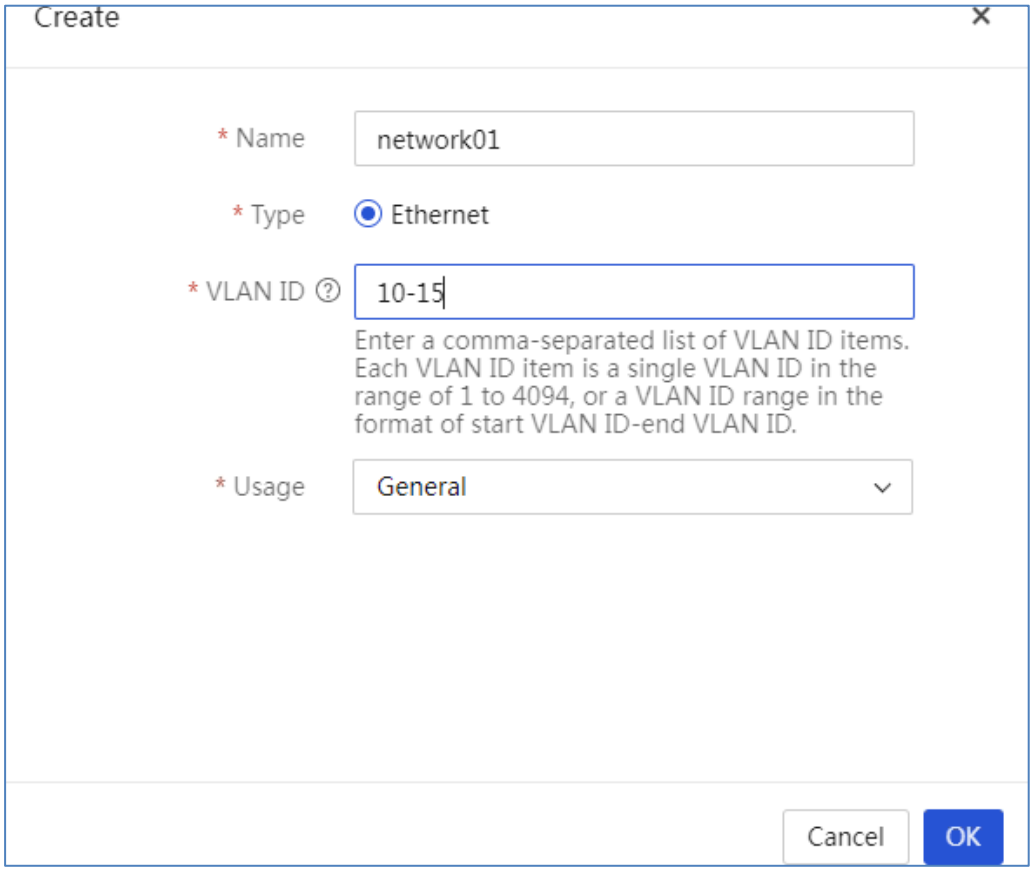


ネットワークを作成する

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
   タブをクリックします。
2. **Create**をクリックします。**Create Network**ダイアログボックスが表示されます。

   インターコネクトモジュールテンプレートを後で作成するには、**Usage**リストから**VC**を選択する必要があります。

図175 ネットワークの作成

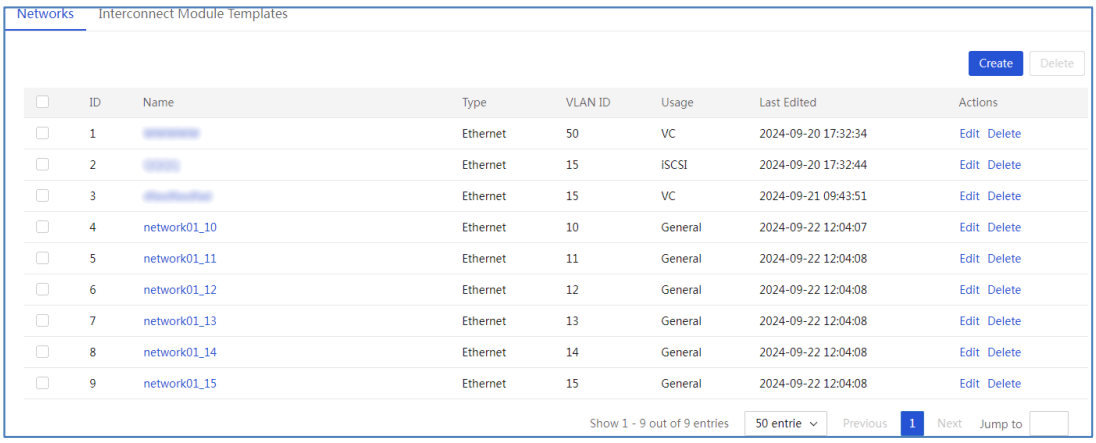


3. ネットワークパラメータを次のように設定します。
   - 単一のネットワークを作成するには、ネットワークのネットワーク名とVLAN IDを指定し、必要に応じてその他のパラメータを設定して、**OK**をクリックします。

     UniSystemは、指定されたネットワーク名を持つネットワークを1つだけ作成します。
   - 同じネットワーク名で異なるVLAN IDを持つ複数のネットワークを作成するには、ネットワーク名とVLAN IDリストを指定し、必要に応じて他のパラメータを設定して、**OK**をクリックします。

     UniSystemは、Network Name_VLAN IDの形式(たとえば、Blue_100)の名前で各VLANのネットワークを作成します。
4. 新しく作成したネットワークが**Networks**ページに表示されていることを確認します。

図176 作成されたネットワークの表示



ネットワークの編集

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
   タブをクリックします。
2. 編集するネットワークの**Actions**カラムで**Edit**をクリックします。
3. 必要に応じて、ネットワーク設定を編集します。
4. **OK**をクリックします。

ネットワークの削除

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
   タブをクリックします。
2. 次のいずれかの手順を実行します。
   - ネットワークを一括削除するには、ネットワークを選択して**Delete**をクリックします。
   - 単一のネットワークを削除するには、そのネットワークの**Actions**カラムで**Delete**をクリックします。
3. 表示されたダイアログボックスで、**OK**をクリックして操作を確認します。

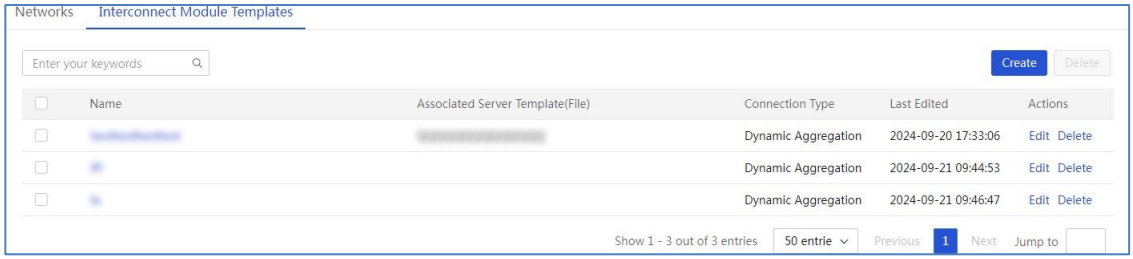
インターコネクトモジュールテンプレートの管理

このメニューから、インターコネクトモジュールテンプレートを作成、編集、または削除できます。

インターコネクトモジュールテンプレートを表示する

1. ナビゲーションペインで、**Menu >Templates > Network Templates**を選択します。**Interconnect Module Templates**タブをクリックします。
2. このタブでは、インターコネクトモジュールテンプレート情報を表示します。

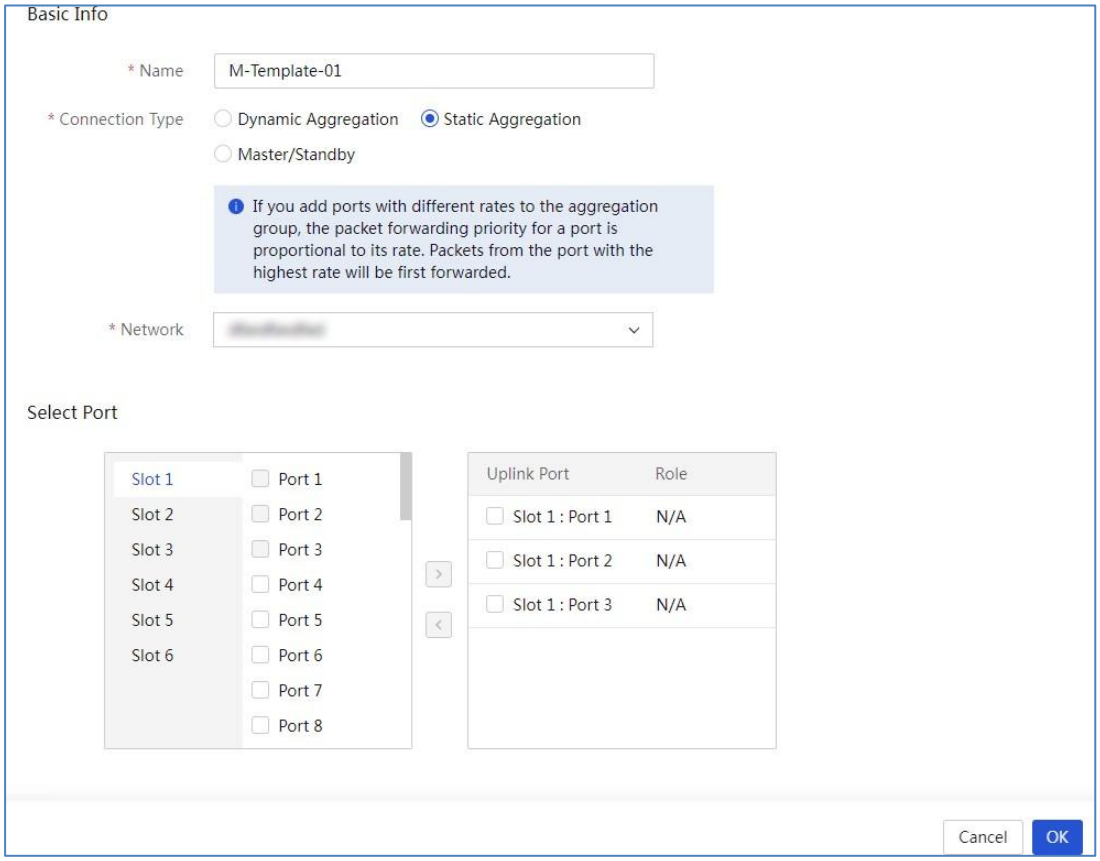
図177 インターコネクトモジュールテンプレートの情報ページ



インターコネクトモジュールテンプレートを作成する

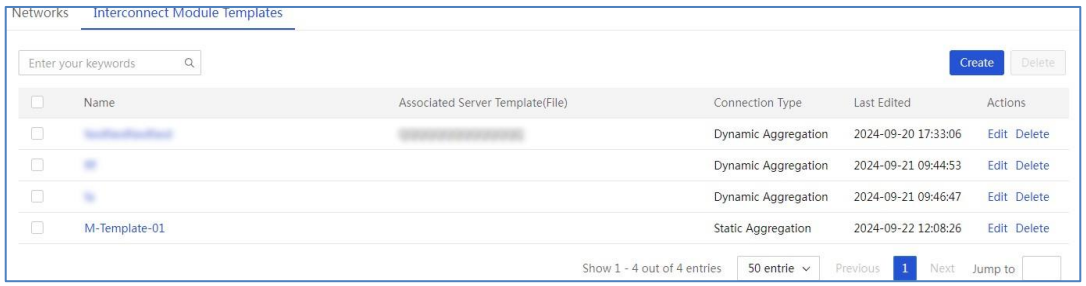
1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
2. **Interconnect Module Templates**タブをクリックします。
3. **Create**をクリックします。
4. 表示されるダイアログボックスで、インターコネクトモジュールテンプレートを設定します。
   Networkリストには、VCとして使用されているネットワークのみが表示されます。

図178 インターコネクトモジュールテンプレートの作成



5. **OK**をクリックします。

図179 インターコネクトモジュールテンプレートリスト



インターコネクトモジュールテンプレートを編集する

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
2. **Interconnect Module Templates**タブをクリックします。
3. 編集するインターコネクトモジュールの**Actions**列で**Edit**をクリックします。
4. **OK**をクリックします。

インターコネクトモジュールテンプレートを削除する

1. ナビゲーションペインで、**Menu > Templates > Network Templates**を選択します。
2. **Interconnect Module Templates**タブをクリックします。
3. 次のいずれかの手順を実行します。

- インターコネクトモジュールを一括削除するには、インターコネクトモジュールを選択して**Delete**をクリックします。
- 1つのインターコネクトモジュールを削除するには、そのインターコネクトモジュールの**Actions**列で**Delete**をクリックします。

4. 表示されたダイアログボックスで、**OK**をクリックして操作を確認します。

イメージの管理

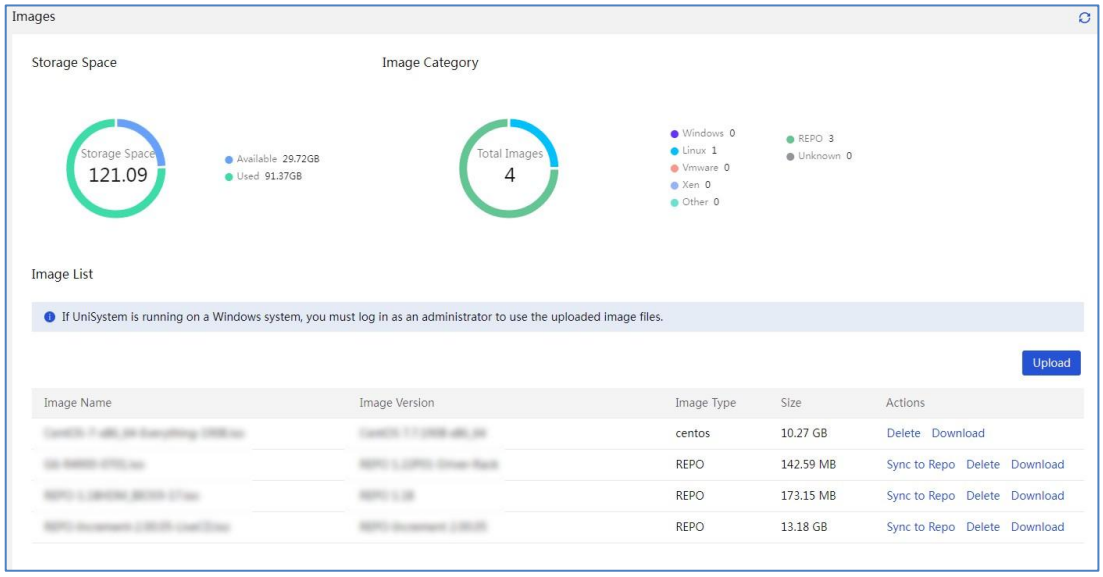
制約事項とガイドライン

- 空き容量が10G程度の場合は、イメージをアップロードできません。この場合は、不要なイメージを削除することをお勧めします。
- UniSystemをWindowsで実行する場合、アップロードしたイメージファイルを正しく使用するには、管理者としてUniSystemを実行する必要があります。
- アップロードするイメージファイルの名前には、ファイル拡張子を含めて最大64文字を使用できます。
- アップロードを成功させるには、アップロードするイメージの名前がイメージリスト上のイメージの名前と異なることを確認してください。
- アップロードを成功させるには、アップロードプロセス中にページを更新しないでください。
- オペレーティングシステムのインストール中の例外を避けるために、アップロードするイメージファイルが公式ウェブサイトからダウンロードされており、編集されていないことを確認してください。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Images**を選択して、図180に示すページに入ります。

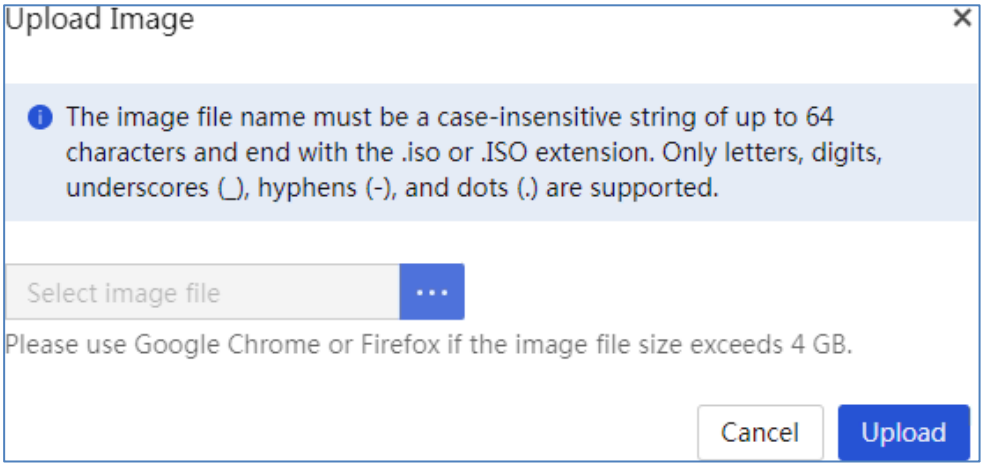
   図180 イメージ



2. イメージリストの右上隅にある**Upload**をクリックします。図181に示すように、**Upload**

Imageダイアログボックスが開きます。

図181 OSイメージのアップロード



3. **Browse**ボタンをクリックします。表示されたダイアログボックスで、アップロードするイメージファイルを選択します。
4. **Upload**をクリックして、OSイメージファイルをUniSystemサーバーにアップロードします。
   アップロードが完了すると、イメージ管理ページにOSイメージファイルが表示されます。
5. (任意)アップロードされたイメージファイルがリポジトリファイルの場合は、ファイルのActionsカラムで**Sync to Repo**をクリックして、**Menu > Templates > Repositories**ページにファイルを同期できます。

クローンイメージ

このタスクについて

重要:

- この機能は、UniSystemがAEモジュールまたはVMで実行されている場合にのみ使用できます。
- この機能を使用するには、最初にHDMサーバーノードをUniSystemに追加する必要があります。詳細は、「サーバーの管理」を参照してください。
- この機能を使用するには、管理対象サーバーにiFISTをインストールし、iFISTがUniSystemと通信できるシステムIPアドレスを持っていることを確認する必要があります。
- この機能は、バージョン2.00.13以降でサポートされています。
- この機能は、バージョン2.00.15以降のVMwareオペレーティングシステムをサポートしています。

この機能を使用すると、次のタスクを実行できます。

- **Export images for OS cloning**: サーバーの指定した論理ドライブ上のOSファイルをエクスポートし、そのファイルをイメージファイルとして保存するには、このタスクを実行します。この機能は、次のOSのエクスポートをサポートします。
  - KVMまたはUSBフラッシュドライブにマウントされたイメージを介して手動でインストールされたOS。
  - IficTを介してインストールされたOS。
  - サーバーテンプレートを使用してインストールされたOS。
  - PXEを介してインストールされたOS。

- **Manage images**:イメージファイルを管理します。イメージ関連情報の表示、イメージファイルの削除、およびブレードサーバーにイメージを適用するためのタグの削除を行うには、このタスクを実行します。

OSクローニング用にエクスポートされたイメージファイルは、サーバーテンプレートのOS設定に追加して適用できます。詳細は、「サーバーテンプレートの管理」および「サーバーテンプレートの適用」を参照してください。

表19に、オペレーティングシステムのOSクローニングのサポートを示します。

表19 オペレーティングシステムのOSクローニングのサポート

オペレーティングシステム	サーバー
• Red Hat Enterprise Linux 7.2(64 bit) • Red Hat Enterprise Linux 7.3(64 bit) • Red Hat Enterprise Linux 7.4(64 bit) • Red Hat Enterprise Linux 7.5(64 bit) • Red Hat Enterprise Linux 7.6(64 bit) • Red Hat Enterprise Linux 7.7(64 bit) • Red Hat Enterprise Linux 7.8(64 bit) • Red Hat Enterprise Linux 7.9(64 bit) • Red Hat Enterprise Linux 8.0(64 bit) • Red Hat Enterprise Linux 8.1(64 bit) • Red Hat Enterprise Linux 8.2(64 bit) • Red Hat Enterprise Linux 8.3(64 bit) • Red Hat Enterprise Linux 8.4(64 bit) • Red Hat Enterprise Linux 9.0(64 bit) • CentOS 7.4 (64 bit) • CentOS 7.5 (64 bit) • CentOS 7.6 (64 bit) • VMware ESXi 6.5 U1 (64 bit) • VMware ESXi 6.5 U2 (64 bit) • VMware ESXi 6.5 U3 (64 bit) • VMware ESXi 6.7 (64 bit) • VMware ESXi 7.0 (64 bit) • VMware ESXi 7.0 U3 (64 bit) • VMware ESXi 8.0 (64 bit)	• H3C UniServer B5700 G3 • H3C UniServer B5800 G3 • H3C UniServerB7800 G3 • H3C UniServer E3200 G3 • H3C UniServer R2700 G3 • H3C UniServer R2900 G3 • H3C UniServer R4700 G3 • H3C UniServer R4900 G3 • H3C UniServer R4950 G3 • H3C UniServer R5300 G3 • H3C UniServer R6700 G3 • H3C UniServer R6900 G3 • H3C UniServer R8900 G3 • H3C UniServer R4500 G3 • H3C UniServer R4900 G5 • H3C UniServer R4700 G5 • H3C UniServer R6900 G5 • H3C UniServer R4300 G5 • H3C UniServer R4950 G5 • H3C UniServer R4930 G5 • H3C UniServer R4330 G5 • H3C UniServer R5500 G5 • H3C UniServer B5700 G5 • H3C UniServer R5300 G5

制約事項とガイドライン

- この機能は、パーティションで暗号化されたOSをエクスポートできません。
- UniSystemは、RAIDモードで動作するLSIストレージコントローラーのみをサポートします(一部のLSIストレージコントローラーは、動作モードの設定を必要としません)。
- OSクローニング用にイメージをエクスポートする前に、サーバーのHDMが正しく動作し、オンになっていることを確認します。
- サーバー上の論理ドライブまたは物理ドライブからOSイメージをエクスポートする前に、ドライブが有効な状態で、オペレーティングシステムが1つだけインストールされていることを確認してください。
- 空き領域が10G以下の場合、クローニング用にイメージをエクスポートできません。この場合、ベストプラクティスとして、不要なイメージを削除してください。空き領域の詳細は、**Menu** > **Templates** > **Images**ページにアクセスしてください。クローニングおよびエクスポートプロセス中は、サーバーの電源をオフにしたり、再起動したりしないでください。クローニングおよび

エクスポートプロセスには数分かかります。辛抱強くお待ちください。

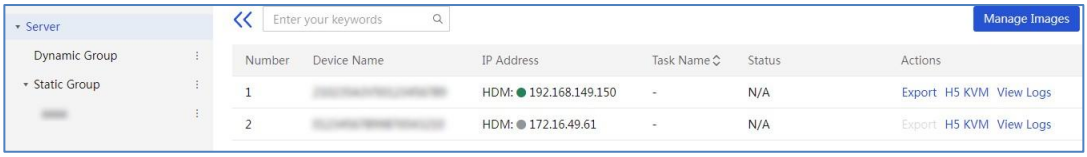
- OSクローニングのためにイメージをエクスポートする場合は、OSタイプに応じて次の制約事項およびガイドラインに従ってください。
  - Linux
    - サーバーがUEFIモードで動作している場合は、UEFIモードでインストールされているオペレーティングシステムのみをエクスポートできます。サーバーがレガシーモードで動作している場合は、レガシーモードでインストールされているオペレーティングシステムのみをエクスポートできます。
    - システムパーティション(/、**/usr**、**/usr/local**、**/var**および**/home**を含む)内のデータはエクスポートできます。**/run**、**/proc**、**/media**および**/sys**ディレクトリ内のファイルがエクスポートされない場合、他のパーティション(スワップおよびデータパーティションを含む)内のデータはエクスポートできません。
    - クローニングされたOSイメージファイルをサーバーに適用した後、サーバー上のパーティション情報はエクスポート前のOSと同じになります。サポートされるファイルシステムには、ext2、ext3、ext4、VFAT、XFSおよびLVMがあります。btrfsファイルシステムはサポートされません。LVMシンプロビジョニングは、ライナーモードのみをサポートします。
  - VMware ESXi
    - OSのクローニングのためにイメージをエクスポートする前に、OSの電源を強制的にオフにしてシャットダウンするのではなく、OSが一度正常にシャットダウンされていることを確認してください。これにより、OSはシステムステータスに関連する構成ファイルを保存できます。そうでない場合、イメージのクローニングおよびエクスポート時のイメージ内のネットワーク設定は有効になりません。
    - VMware ESXiオペレーティングシステムのデータファイルはエクスポートできません。ベストプラクティスとして、システムパーティションをデータパーティションから分離します。
    - クローンイメージファイルを適用した後、システム論理ドライブにデータパーティションを作成するには、手動で作成する必要があります。クローンOSイメージは、VMware ESXiオペレーティングシステムでのデータパーティションの保持をサポートしていません。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Images** > **Clone Images**を選択します。

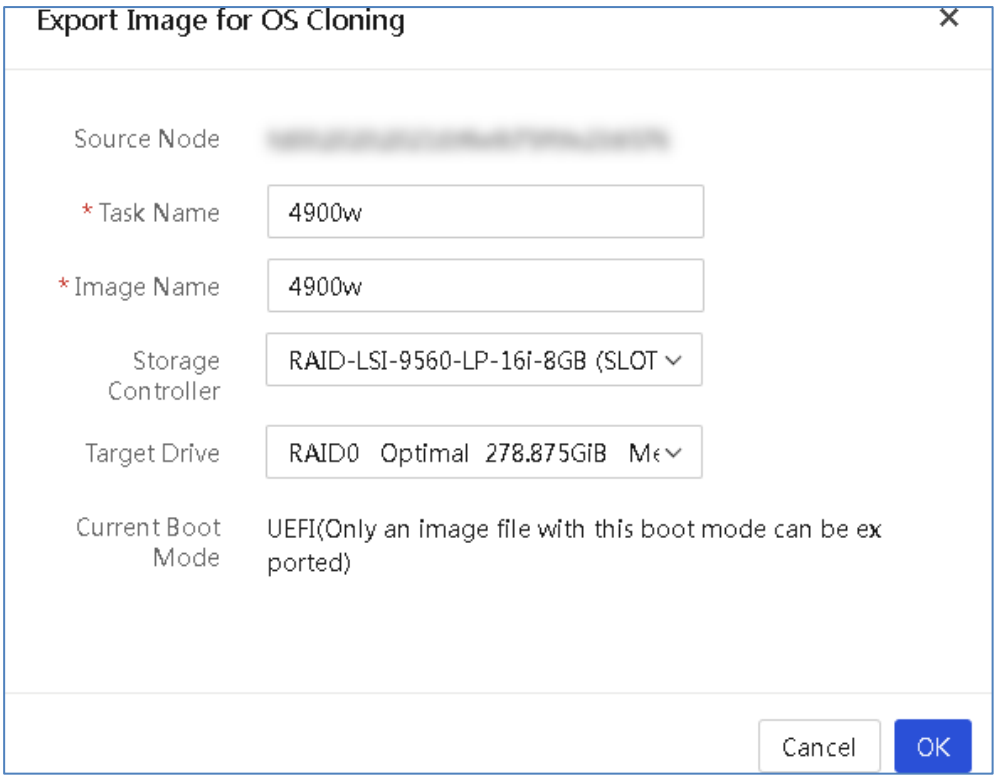
   ターゲットイメージをすばやく除外するには、左側のナビゲーションペインから静的グループと動的グループを使用するか、検索領域にキーワードを入力します。

   図182クローンイメージ



2. 図183に示すように、デバイスの**Actions**列で**Export**をクリックします。表示されるダイアログボックスで、クローンとエクスポートタスクの名前を指定し、エクスポートするOSイメージファイルの名前を指定し、ストレージコントローラーとターゲットドライブを選択して、**OK**をクリックしてクローン作成指示を発行します。

図183 OSクローニングのためのイメージのエクスポート



3. クローン作成の進行状況を確認するには、**Status**列を参照してください。
4. 図184に示すように、**Manage Images**をクリックしてイメージ管理ページに入ります。このページでは、エクスポートされた各イメージファイルのタイプとサイズを表示できます。

   図184 イメージの管理



5. (オプション)イメージを削除するには、削除するイメージの**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。
6. 詳細なログを表示するには、デバイスの**View Logs**をクリックします。

ディスクレスブートを構成する

はじめに

重要:

- この機能は、UniSystemがAEモジュールで実行されている場合にのみ使用できます。
- この機能は、バージョン2.00.13以降でサポートされています。

この機能は、iSCSIプロトコルに準拠し、ブレードサーバー用のリモートストレージボリュームを提供します。ストレージボリュームにオペレーティングシステムを手動でインストールして、ディスクレス

ブートを実装できます。リモートストレージボリュームに接続し、ボリュームにオペレーティングシステムをインストールする方法については、「付録」を参照してください。

ディスクレスブートを使用する場合は、ローカルドライブをデータドライブとしてのみ使用し、ローカルドライブにOSやシステムブートプログラムがインストールされていないことを確認することをお勧めします。そうしないと、OSのインストール後にディスクレスブートプロセスが影響を受ける可能性があります。

ディスクレスブート用のストレージボリュームは、BIOSがUEFIモードで動作している場合にのみ接続できます。

共通のファイルシステム(たとえば、ext4およびxfs)は、同時に複数のノードにマウントできません。したがって、特殊なクラスタファイルシステムを使用する場合を除き、2つのNICを使用して同じiSCSIボリュームに接続しないでください。2つのNICを使用すると、ファイルシステムが破損し、OSが起動しなくなる可能性があります。

サポートされるオペレーティングシステム

重要:

この機能は、バージョン2.00.15以降のVMwareオペレーティングシステムをサポートしています。

次のオペレーティングシステムは、ディスクレスブートをサポートしています。

- Red Hat Enterprise Linux 7.5(64ビット)
- Red Hat Enterprise Linux 8.2(64ビット)
- CentOS 7.5(64ビット)
- CentOS 8.2(64ビット)
- VMware ESXi 6.5 U2(64ビット)
- VMware ESXi 6.7(64ビット)
- VMware ESXi 7.0 U2(64ビット)

ボリュームを作成する

このタスクについて

iSCSIクライアントが接続するための空のiSCSIボリュームを作成するには、次のタスクを実行します。ストレージボリュームにオペレーティングシステムを手動でインストールして、ディスクレスブートを実装できます。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Diskless Boot**を選択して、図185に示すページに入ります。このページでは、既存のiSCSIボリュームを表示できます。

   図185 ディスクレスブート

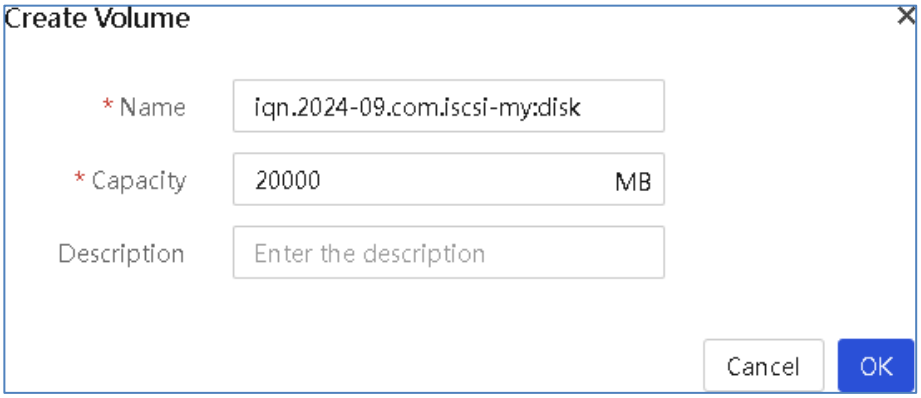


2. **Create Volume**をクリックします。表示されるダイアログボックスで、ボリュームの名前、容量、および説明を入力します。

メモ:

iSCSIボリューム名は、iqn.yyyy-mm.<reversed domain name>:identifierのようなiSCSI Qualified Name(IQN)形式に準拠している必要があります。たとえば、次のようになります。iqn.2014-10.dev.iscsi-target:diskです。

図186 ボリュームの作成



ボリュームをコピーする

このタスクについて

既存のiSCSIボリュームを変更せずにコピーします。サポートされているオペレーティングシステムがインストールされているiSCSIボリュームをコピーした後、そのオペレーティングシステムを直接使用できます。

ストレージボリュームは完全にコピーされ、ストレージボリュームにインストールされた純粋なソフトウェアパッケージが継承されます。ただし、ハードウェア関連の設定は、システムおよびハードウェア環境によって異なる場合があります。NIC設定を例に挙げます。ソースノードとターゲットノードの両方に同じ名前のNICがある場合、ソースノードのNIC設定はターゲットノードで有効になります。ソースノードが静的IPを使用する場合、ターゲットノードは同じ静的IPを使用する必要があり、ターゲットノードで手動で編集する必要があります。ストレージボリュームが多数のターゲットノードにコピーされる場合は、ベストプラクティスとして、IPアドレス割当てに対してDHCPを有効にします。

VMware ESXiオペレーティングシステムがインストールされているボリュームをコピーした後は、次の制約事項およびガイドラインに従ってください。

- ベストプラクティスとして、システムパーティションをデータパーティションから分離します。サービスデータ(VMデータなど)をディスクレスブートボリュームに格納しないでください。格納しないと、ボリュームのコピー後にエラーが発生する可能性があります。
- VMware ESXiオペレーティングシステムがインストールされているボリュームは、複数のブレードサーバーにわたって使用することはできません。
- VMware ESXiオペレーティングシステムのiSCSIブートボリュームを除き、手動で追加したiSCSIリモートストレージボリュームにデータを保存できます。iSCSIボリュームをコピーする前にこれを行うと、iSCSIボリュームのコピー後に、追加したデータストレージ構成情報が失われます。リモートボリュームに再接続するには、接続を手動で復元する必要があります。
- コピーされたVMware ESXiオペレーティングシステムは、最初の起動後に自動的に再起動する場合があります。これは正常です。システムは2回目の再起動後に正常に動作します。

手順

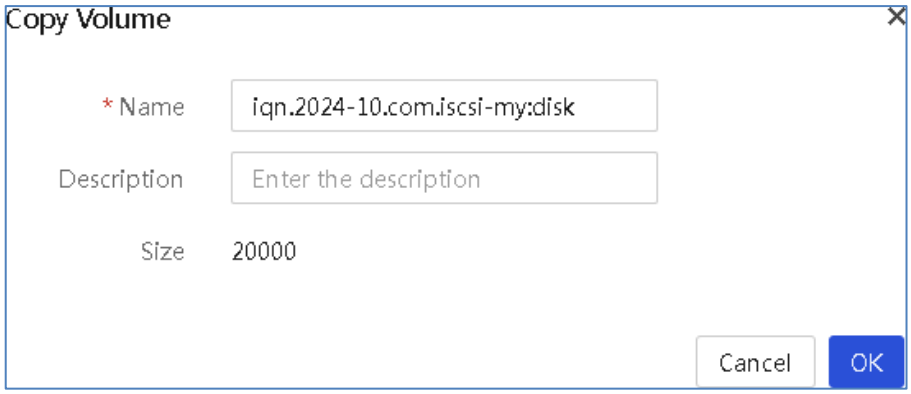
重要:

ソースノードとターゲットノードで完全なデータ整合性を確保するには、ベストプラクティスとして、次のものをコピーします。
ソースノードがサービスを実行していないとき、またはシャットダウンしているときのストレージボリューム。

ボリュームをコピーするには、次の手順に従います。

1. ナビゲーションペインで、**Menu** > **Templates** > **Diskless Boot**を選択して、図185に示すページに入ります。**Copy Volum**をクリックし、コピーするボリュームの右上隅をクリックします。
2. 図187に示すように開いたダイアログボックスで、ボリューム名を入力します。コピーによって生成されたボリュームのサイズは、コピーされたボリュームのサイズと同じであり、編集できません。

   図187 ボリュームのコピー



3. **OK**をクリックしてコピーを開始します。iSCSIボリュームのコピーには時間がかかります。コピー処理中は他のページに切り替えないでください。

ボリュームを削除する

このタスクについて

既存のiSCSIボリュームを削除するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Diskless Boot**を選択して、図185に示すページに入ります。
2. **Delete Volume**をクリックします。削除するストレージボリュームの右上隅にあるアイコンをクリックします。
3. 表示されたダイアログボックスで、**OK**をクリックしてストレージボリュームを削除します。

認証の設定

このタスクについて

iSCSI CHAP認証情報を設定します。この情報は、iSCSIストレージボリュームに接続するiSCSIクライアントの認証に使用されます。

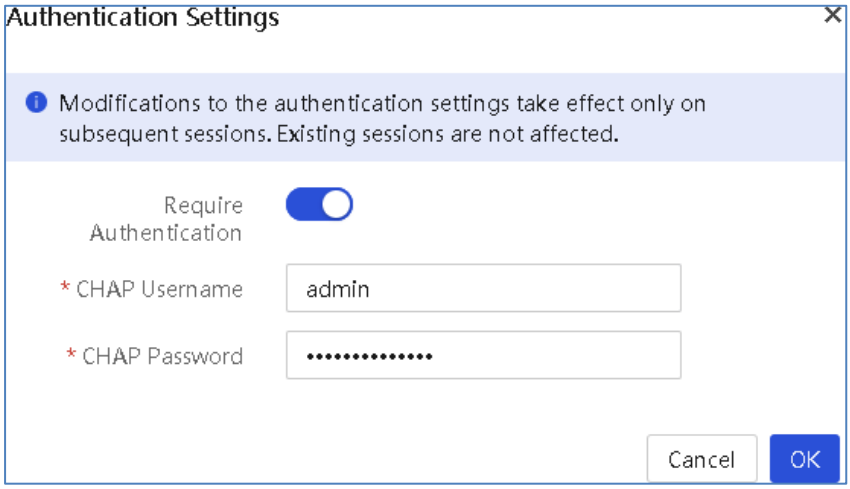
手順

1. ナビゲーションペインで、**Menu** > **Templates** > **Diskless Boot**を選択して、図185に示すペ

ージに入ります。

2. iSCSIボリュームの**Require Authentication**フィールドでまたはをクリックします。は、認証が設定されていることを示します。は、認証が設定されていないことを示します。
3. 表示されたダイアログボックスで、**Enable Authentication**を選択し、ストレージボリュームのユーザー名とパスワードを入力します。iSCSI CHAP認証パスワードは、12～16文字の文字列です。
4. **OK**をクリックします。

図188 認証設定



サーバーの導入

エンクロージャーテンプレートの適用

エンクロージャーテンプレートをエンクロージャーに適用するには、次の作業を実行します。

エンクロージャーテンプレートがエンクロージャーに適用されると、UniSystemはエンクロージャーテンプレートの設定に従ってサーバーテンプレートをブレードサーバースロットにバインドします。サーバーがエンクロージャーのスロットに取り付けられると、UniSystemがAEモジュールで実行されるときに、UniSystemはバインドされたサーバーテンプレートを使用してサーバーを自動的に設定します。

エンクロージャーテンプレートをエンクロージャーに適用すると、UniSystemは、適用されたテンプレートに基づいてエンクロージャーのエンクロージャー設定ファイルを自動的に作成します。

エンクロージャーテンプレートの適用によってサーバーテンプレートにバインドされているブレードサーバースロットごとに、UniSystemはエンクロージャースロット設定ファイルを作成します。

サーバーテンプレートが適用されるサーバーがUniSystemによって管理されていない場合、UniSystemは、バインドされたテンプレートを適用する前に、サーバーを管理対象サービスリストに追加します。

エンクロージャーテンプレートをエンクロージャーに適用する

制約事項とガイドライン

エンクロージャーテンプレートでは、2つのサーバーテンプレートをフル幅スロット領域の2つのハー

フ幅スロットにバインドできます。フル幅ブレードサーバーがフル幅スロットに取り付けられている場合、UniSystemは、左側のハーフ幅スロットにバインドされているサーバーテンプレートをサーバーに適用します。

エンクロージャーテンプレートの接続設定機能を有効にするには、エンクロージャーテンプレートを適用する前にVCを事前に設定する必要があります。

エンクロージャーのスロットが、VC設定を含むサーバー設定テンプレートにバインドされている場合、VC設定は、エンクロージャー設定テンプレートまたはファイルが適用されたときにのみ有効になります。サーバー設定テンプレートを直接適用した場合、VC設定は有効になりません。

設定テンプレートを適用する場合は、次の作業を実行しないでください。

- デバイスの電源をオフにするか、再起動します。
- KVMを使用してマウント操作を実行します。

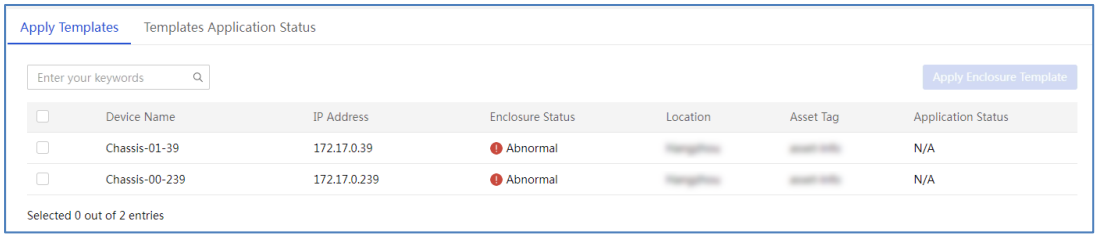
設定にHDM設定以外の設定が含まれている場合は、テンプレートが適用されているエンクロージャーがシャットダウンされていることを確認します。

HDM設定に消費電力上限設定が含まれている場合、テンプレートを適用するとエンクロージャーがシャットダウンされることがあります。

手順

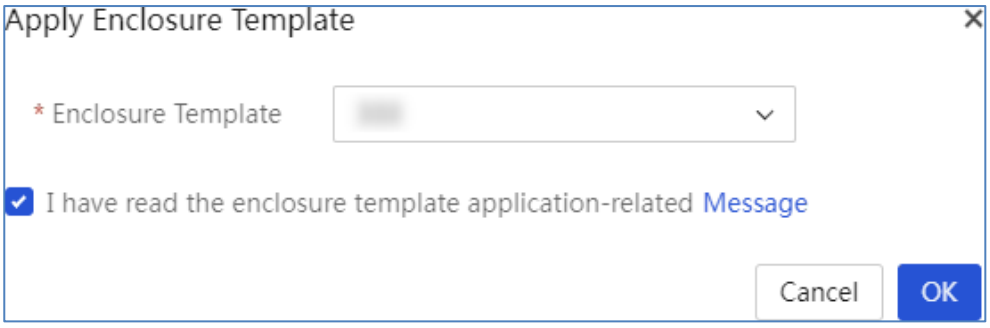
1. ナビゲーションペインで、**Menu > Deployment > Enclosures > Apply Enclosure Templates**を選択します。

   図189 Apply Enclosure Templatesページ

2. **Apply Enclosure Templates**を選択し、**Apply Enclosure Templates**をクリックします。エンクロージャーテンプレートの適用ダイアログボックスが開きます。

   図190 Apply Enclosure Templateダイアログボックス

3. 選択したエンクロージャーに適用するエンクロージャーテンプレートを選択し、**I have read the enclosure template application-related Message**を選択します。
4. **OK**をクリックします。

   Template Application Statusタブが開き、テンプレートアプリケーションのステータスと進行状況が表示されます。

5. サーバーに関するテンプレートアプリケーション情報を表示するには、サーバーの**Actions**列で**Logs**をクリックします。

エンクロージャー設定ファイル

このタスクについて

エンクロージャーテンプレートをエンクロージャーに適用すると、UniSystemは、適用されたテンプレートに基づいてエンクロージャーのエンクロージャー設定ファイルを自動的に生成します。

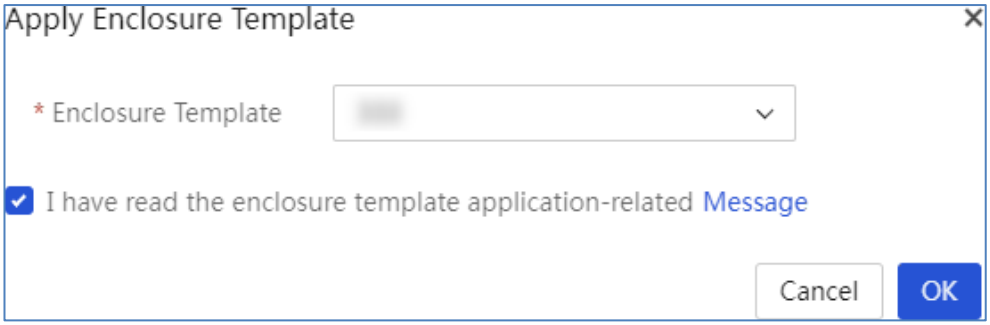
エンクロージャーテンプレートでは、2つのサーバーテンプレートをフル幅スロット領域の2つのハーフ幅スロットにバインドできます。フル幅ブレードサーバーがフル幅スロットに取り付けられている場合、UniSystemは、左側のハーフ幅スロットにバインドされているサーバーテンプレートをサーバーに適用します。

エンクロージャー設定ファイルには、エンクロージャーテンプレート内のすべての設定が含まれます。エンクロージャー設定ファイル内の設定を編集し、必要に応じて編集したファイルをエンクロージャーに適用できます。

手順

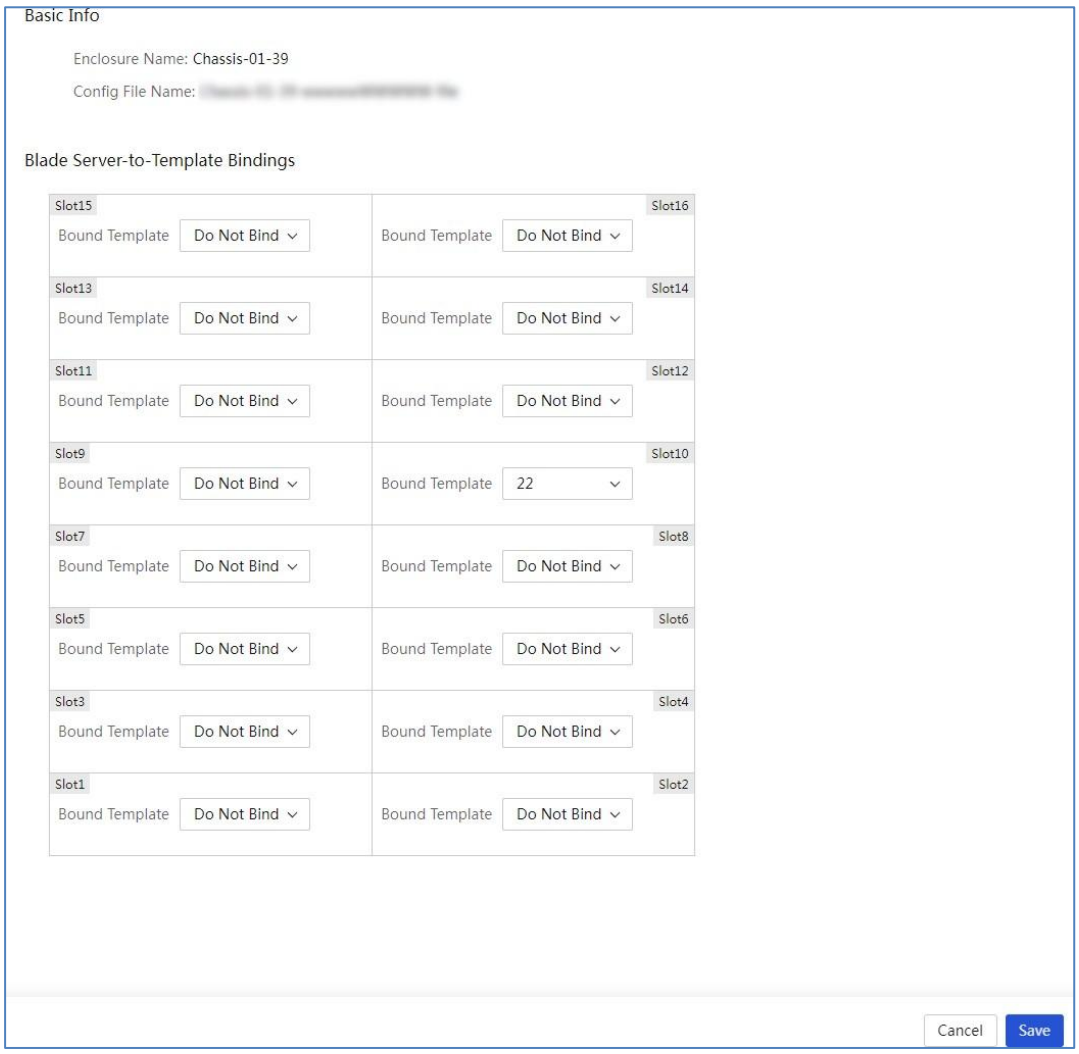
1. ナビゲーションペインで、**Menu > Deployment > Enclosures > Enclosure Config Files**を選択します。

図191 エンクロージャー構成ファイル



2. ファイル名をクリックすると、選択したエンクロージャー設定ファイルに関する詳細情報が表示されます。
3. (オプション)エンクロージャー設定ファイルを編集するには、ターゲットファイルの**Actions**列で**Edit**をクリックします。表示されたダイアログボックスで設定を編集し、**Save**をクリックします。

図192 エンクロージャー設定ファイルの編集



4. 適用するエンクロージャー設定ファイルの**Actions**列で**Apply**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。
5. (オプション)エンクロージャー設定ファイルを削除するには、ターゲットファイルの**Actions**列で**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

エンクロージャースロットコンフィギュレーションファイル

このタスクについて

UniSystemは、エンクロージャーテンプレートの適用によってサーバーテンプレートにバインドされている各ブレードサーバースロットに対して、エンクロージャースロット設定ファイルを自動的に作成します。

エンクロージャースロット設定ファイルの設定を編集し、必要に応じて、編集したファイルをブレードサーバーに適用できます。

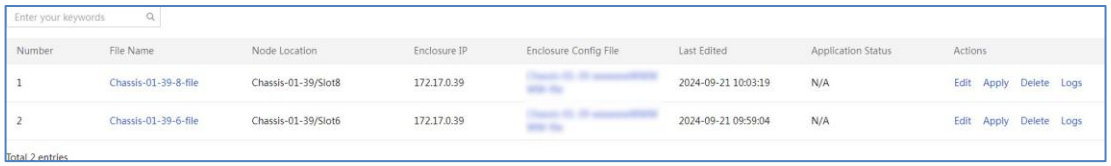
ノードの取り外しおよび接続後にエンクロージャースロット設定ファイル(またはエンクロージャー設

定ファイル)が自動的に適用される場合、VC設定はOM上のポリシーファイルを使用します。

手順

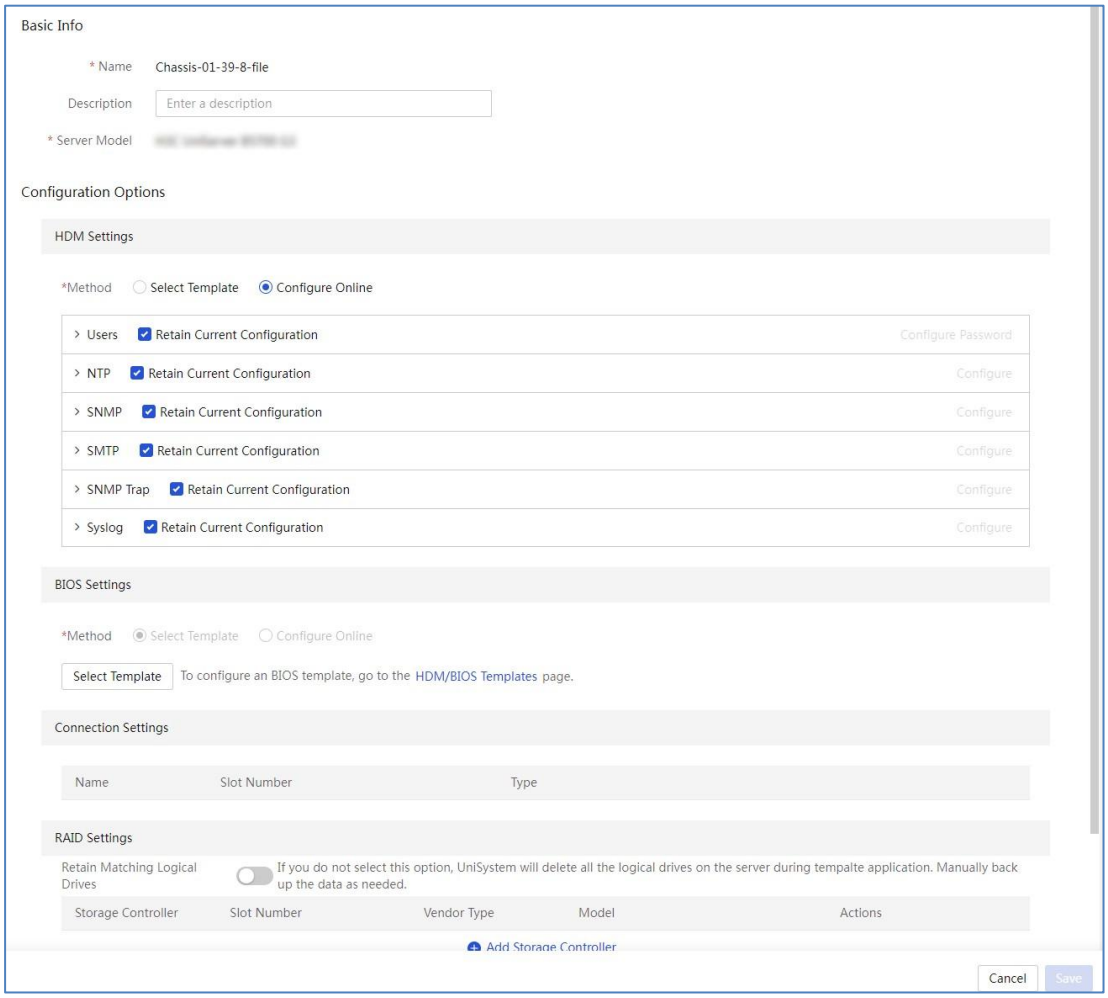
1. ナビゲーションペインで、**Menu** > **Deployment** > **Enclosures** > **Enclosure Slot Config Files**を選択します。

   図193 エンクロージャーのスロット設定ファイル



2. ファイル名をクリックすると、選択したエンクロージャースロットコンフィギュレーションファイルに関する詳細情報が表示されます。
3. (オプション)エンクロージャースロット設定ファイルを編集するには、ターゲットファイルの**Actions**列で**Edit**をクリックします。表示されたダイアログボックスで設定を編集し、**Save**をクリックします。

   図194 エンクロージャースロット設定ファイルの編集



4. 適用するエンクロージャースロット設定ファイルの**Apply**列で**Apply**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

5. エンクロージャースロット設定ファイルの**Actions**列で**Logs**をクリックして、アプリケーションログを表示します。
6. (オプション)エンクロージャースロットコンフィギュレーションファイルを削除するには、ターゲットファイルの**Actions**列で**Delete**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

サーバーテンプレートの適用

サーバーテンプレートをサーバーに適用する

サーバーテンプレートをサーバーに適用するには、次のタスクを実行します。サーバーテンプレートをサーバーに適用することにより、UniSystemは、テンプレート内のHDM、BIOS、接続、RAIDおよびOSインストール設定をサーバーにデプロイします。

重要:

- この機能を使用するには、最初にHDMサーバーノードをUniSystemに追加する必要があります。詳細は、「サーバーの管理」を参照してください。
- クローンイメージを含むテンプレートを使用するか、UniSystemを使用して、サーバーにOSをインストールするには
  2.00.26以前では、サーバーはiFISTのシステムIPアドレスを介してUniSystemと通信できる必要があります。iFISTは、サーバーと同じLAN上に存在するDHCPサーバーからシステムIPアドレスを取得します。
- バージョン2.00. 26では、この機能はHDM(HDM 2.11以降)およびiFIST(iFIST 1.01.26以降)で動作し、帯域外OSインストールを実装できます。
- HDM 2.11より前のバージョンのHDMおよびHDM 4.0より前のバージョンのiFISTを実行しているサーバー
  1.01.26、バージョン2.00.26では、サーバー上のiFISTと通信してOSをインストールできます。

制約事項とガイドライン

- 設定にHDM設定以外の設定が含まれている場合は、テンプレートが適用されているサーバーがシャットダウンされていることを確認します。
- HDM設定に消費電力上限設定が含まれている場合、テンプレートを適用すると、サーバーがシャットダウンされることがあります。
- テンプレートをサーバーに適用する前に、サーバーで進行中の操作がないことを確認してください。テンプレートの適用プロセス中は、設定に含まれる他の操作を実行しないでください。
- サーバーでのテンプレートの適用プロセス中は、次の操作を実行しないでください。
  - サーバーの電源をオフにするか、再起動します。
  - サーバーのHDMを更新、リセット、または工場出荷時のデフォルトに戻します。
  - KVMを介してマウント操作を実行します。
- HDM設定を適用する権限は、HDMアカウントのネットワーク権限に依存します。ユーザーにこの操作の権限があることを確認してください。
- HDM設定がターゲットサーバーに正常に適用されると、サーバーは自動的に再起動します。HDMステータスは数分後に復元されます。
- HDM設定またはBIOS設定をサーバーに正しく適用するには、テンプレート内のHDMまたはBIOSのバージョンが、サーバーのHDMまたはBIOSのバージョンと同じであることを確認します。
- バージョンHDM-1.11.19以前(すべてのHDM-1.10.XXバージョンを含む)のHDM設定を適用する場合、UniSystemの構成インポートポリシーはHDMのポリシーと同じになります。HDM

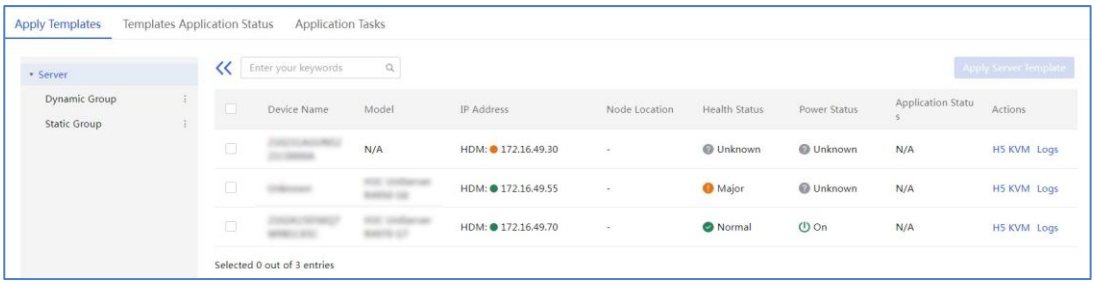
設定が複数のサーバーにコピーされる場合、サーバーのHDM IPが競合する可能性があります。この機能は注意して使用してください。

- バージョンHDM-1.11.20以降のHDM設定を適用する場合、UniSystemはHDM IP設定を編集しません。IPの競合を回避するために、複数のHDMに同じIPアドレスを設定しないでください。HDMテンプレートをサーバーに適用すると、HDMテンプレートのIP設定、VLAN設定、およびLLDP設定は、バージョンUniSystem-2.31以降のUniSystemでは有効になりません。
- UniSystemは、RAIDモードで動作するLSIストレージコントローラーのみをサポートします(一部のLSIストレージコントローラーは、動作モードの設定を必要としません)。
- 2 TB以上のディスクにテンプレートを適用してOSをインストールしないでください。このようなインストールは失敗する可能性があります。
- テンプレートを使用してサーバーの物理ドライブにオペレーティングシステムを正常にインストールするには、サーバーにバージョンiFIST-1.01.25以降のiFISTがインストールされていることを確認します。
- ソースサーバーのクローニングされたイメージを含むサーバーテンプレートをターゲットサーバーに適用することにより、サーバーのオペレーティングシステムを別のサーバーにクローニングできます。この操作を実行する際は、次のガイドラインに従ってください。
  - クローンイメージのターゲットサーバーとソースサーバーのハードウェアコンポーネントが一致していることを確認します。
  - テンプレートで指定されたIPアドレス設定は、UniSystemに接続されている最初のサーバーポートに適用されます。サーバー上の残りのネットワークポートは、クローンイメージファイルの設定を使用します。
  - Linuxシステムの場合、ソースサーバーのパーティション設定は、クローンイメージを介してターゲットサーバーにコピーされます。
  - VMware ESXiシステムでは、ターゲットサーバーのシステムドライブにデータパーティションを手動で作成する必要があります。VMware ESXi 7.0U2(64ビット)以降のバージョンでは、IPアドレスとホスト名の設定はサポートされていません。
- HDMからREPOを更新し、更新の実行後にサーバーを再起動していない場合、サーバーテンプレートを介してRAID設定またはOS設定をサーバーに適用できない可能性があります。この問題を解決するには、最初にサーバーを再起動してREPOの更新を完了してから、サーバーテンプレートをサーバーに適用します。
- 自動シャットダウン機能を使用できるのは、タイマー設定の繰り返しを設定している場合だけです。
- テンプレート設定でHDM設定だけが設定されている場合、自動シャットダウン機能はサーバーの電源をオフにしません。
- テンプレートを繰り返し適用すると、サーバーの現在の構成が変更される場合があります。気をつけてください。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Apply Server Templates**を選択して、図195に示すページに入ります。

図195 サーバーテンプレートの適用



2. ターゲットサーバーを選択し、**Apply Server Templates**をクリックします。表示されたページで、次のタスクを実行します。

   ターゲットサーバーをすばやく除外するには、左側のナビゲーションウィンドウから静的グループと動的グループを使用するか、検索領域にキーワードを入力します。

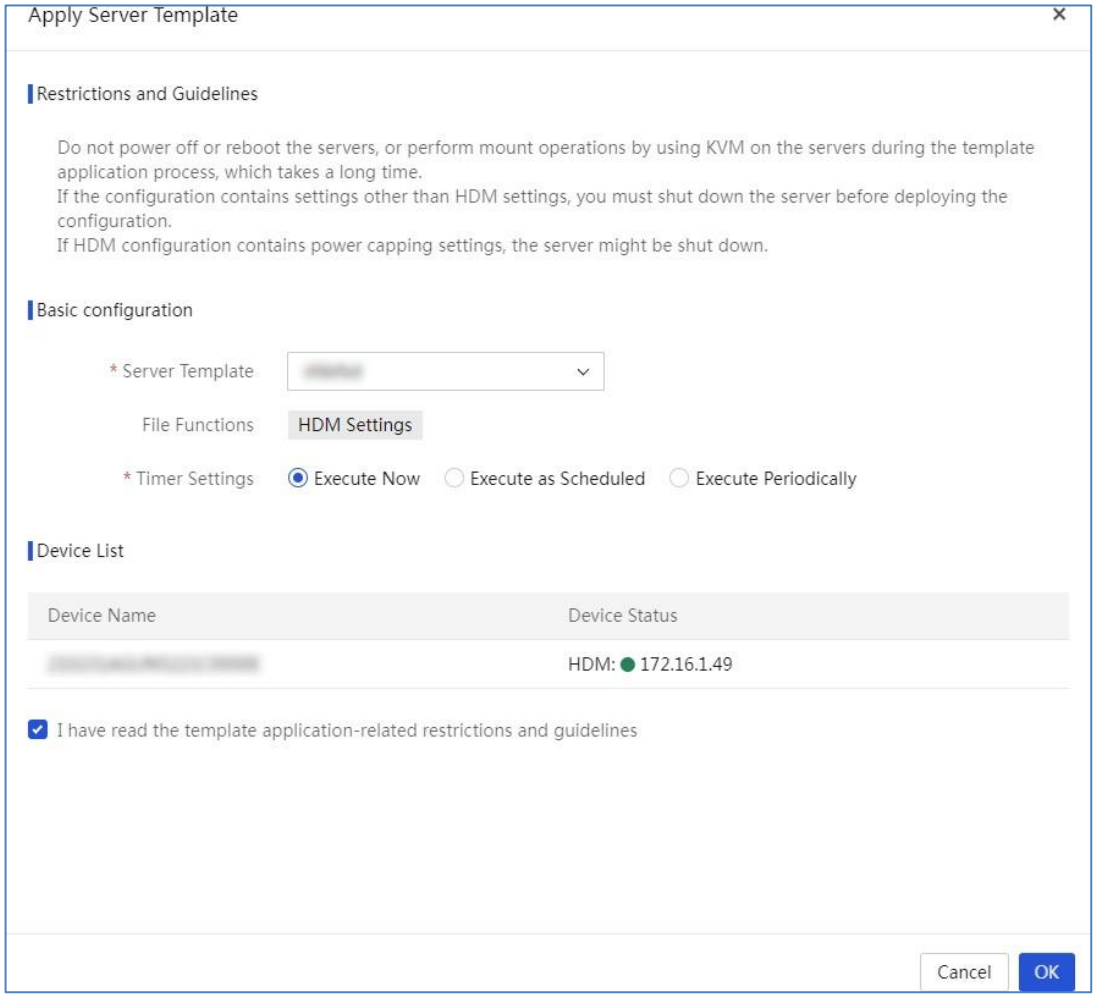
3. 図196に示すように表示されるダイアログボックスで、次のタスクを実行します。

   a. 適用するサーバーテンプレートを選択し、デバイス名とデバイスステータスを確認します。

   b. タイマーを設定します。

   - タイマー設定にカスタム設定を選択した場合は、**Timer Settings**フィールドで実行時間を指定します。UniSystemはスケジュールされた時間に展開を開始します。
   - タイマー設定の繰り返し設定を選択した場合は、更新頻度と更新時間を指定し、必要に応じて**Auto Shutdown Before Application**を有効にします。UniSystemは、設定に従ってテンプレートを展開します。
   - タイマー設定で**Execute Now**を選択した場合は、**OK**をクリックするとすぐにUniSystemが展開を開始します。

図196 サーバーテンプレートの適用



4. スケジュール済の配布の設定。スケジュール済の配布を有効にした場合、**Execution Time**フィールドからスケジュール済の時間を選択できます。UniSystemはスケジュール済の時間に配布を開始します。スケジュール済の配布を無効にした場合、**OK**をクリックすると、UniSystemはすぐに配布を開始します。
5. **I have read the template application-related restrictions and guidelines**を選択します。
6. **OK**をクリックして、選択したサーバーへのテンプレートの適用を開始します。

   Template Application Statuタブが開き、テンプレートアプリケーションのステータスと進行状況が表示されます。
7. サーバーに関する詳細なテンプレートアプリケーション情報を表示するには、**Actions**の**Logs**をクリックします。
   列に表示されます。
8. スケジュール済の配布を有効にすると、テンプレートの適用後にアプリケーションタスクページが開きます。このページで、タスクの実行状態を確認できます。
   - アプリケーションタスクを停止するには、そのタスクの**Actions**列で**Stop**をクリックします。
   - アプリケーションタスクを削除するには、そのタスクの**Actions**列で**Delete**をクリックします。

サーバー構成ファイル

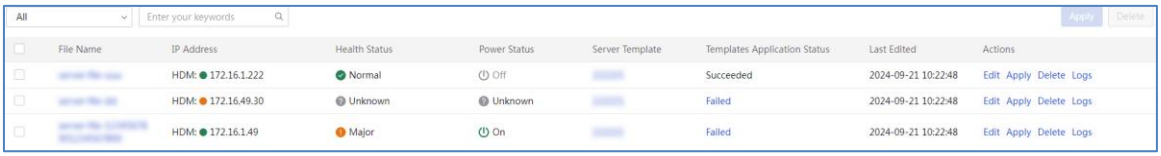
サーバー構成ファイルは、サーバーテンプレートが正常に適用された後に単一のサーバーに対して生成される構成ファイルです。サーバーテンプレートの適用方法は、「サーバーテンプレートの適用」を参照してください。

サーバーのサーバー構成ファイルを編集して、同じサーバーに再度適用できます。この機能を使用すると、サーバーテンプレートを編集しなくても、サーバーの構成をすばやく編集できます。

サーバー構成ファイルを表示する

ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Config Files**を選択して、UniSystemのサーバー構成ファイルを表示します。

図197 サーバー構成ファイル



サーバー構成ファイルを編集する

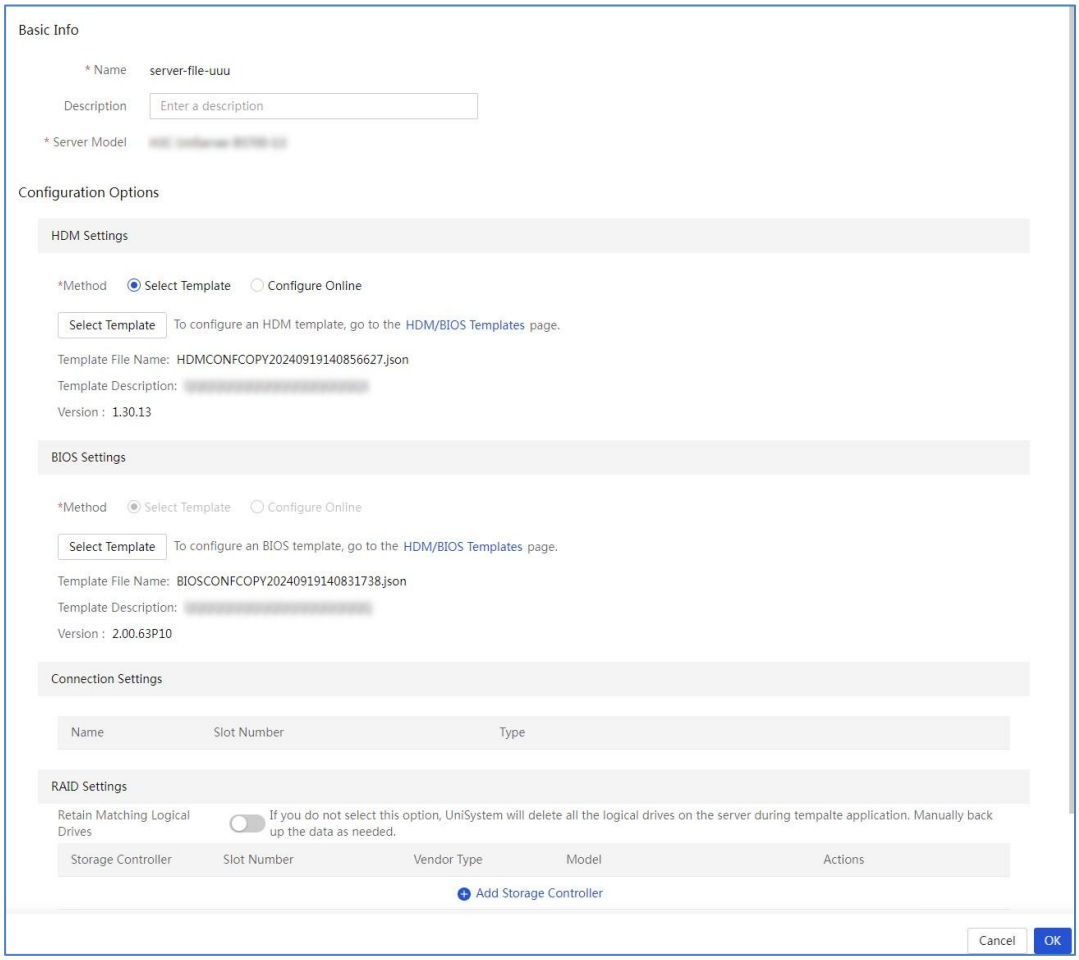
制約事項とガイドライン

サーバー構成ファイルのOS設定でIPアドレス、サブネットマスクまたはゲートウェイが変更されると、サーバーテンプレートによってサーバーに割り当てられていたIPアドレスが取り消されます。取り消されたIPアドレスは、サーバーテンプレートによって別のサーバーに割り当てることができます。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Config Files**を選択します。
2. 編集するサーバー構成ファイルの**Actions**列で**Edit**をクリックします。図198に示すページで、必要に応じてサーバー構成ファイルを編集します。

図198 サーバー構成ファイルの編集



3. 構成ファイルの変更を確認し、**OK**をクリックします。

サーバー構成ファイルの適用

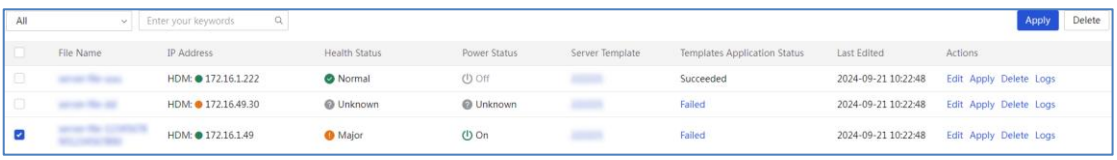
制約事項とガイドライン

サーバー構成ファイルのアプリケーションステータスがFailedの場合、アプリケーションログを参照してサーバー構成ファイルの詳細情報を取得します。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Config Files**を選択して、図199に示すページに入ります。

   図199 Server Config Filesページ



2. 次のいずれかの手順を実行します。
   - 1つのサーバー構成ファイルを適用するには、適用するサーバー構成ファイルの**Actions**列で**Apply**をクリックします。
   - サーバー構成ファイルを一括適用するには、適用するサーバー構成ファイルを選択し、右上隅にある**Apply**をクリックします。
3. 表示されたダイアログボックスで、**OK**をクリックして操作を確認します。

サーバー構成ファイルの削除

制約事項とガイドライン

サーバーのサーバー構成ファイルが削除されると、サーバーテンプレートがサーバーに割り当てたIPアドレスが取り消されます。取り消されたIPアドレスは、サーバーテンプレートによって別のサーバーに割り当てることができます。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Config Files**を選択します。
2. 次のいずれかの手順を実行します。
   - 1つのサーバー構成ファイルを削除するには、削除するサーバー構成ファイルの**Actions**列で**Delete**をクリックします。
   - サーバー構成ファイルを一括削除するには、削除するサーバー構成ファイルを選択し、右上隅にある**Delete**をクリックします。
3. 表示されたダイアログボックスで、**OK**をクリックして操作を確認します。

コンポーネントを更新する

このメニューから、ローカルノードおよびリモートノードのコンポーネントを更新できます。コンポーネントには、HDM、BIOS、CPLD、および一部のハードウェアのファームウェアとドライバーが含まれます。

ローカルノードはUniSystemサーバーを参照します。ローカルタスクにはローカルノードのみが含まれます。**Update Components**ページでは、**localhost**という名前のローカルタスクが自動的に追加されます。ローカルタスクは削除できません。

リモートノードとは、管理対象サーバーを指します。リモートノードには、HDMおよびFIST SMSが含まれます。

ヒント:

サーバーのHDMバージョンがHDM-1.11.08とHDM-1.30.18の間である場合、REPOを使用してUniSystemのFIST SMSを介してBIOSファームウェアをアップグレードすると、BIOS設定は維持されません。

タスクを追加する

このタスクについて

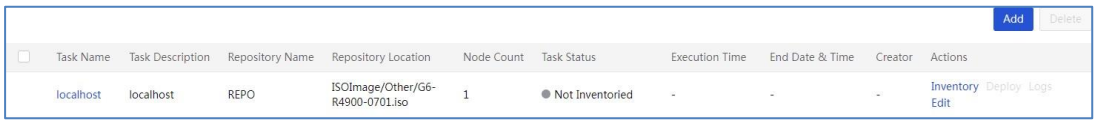
複数の管理対象サーバーをタスクに追加して、サーバーノードを一括更新できるようにするには、このタスクを実行します。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Update Components**を選択します。

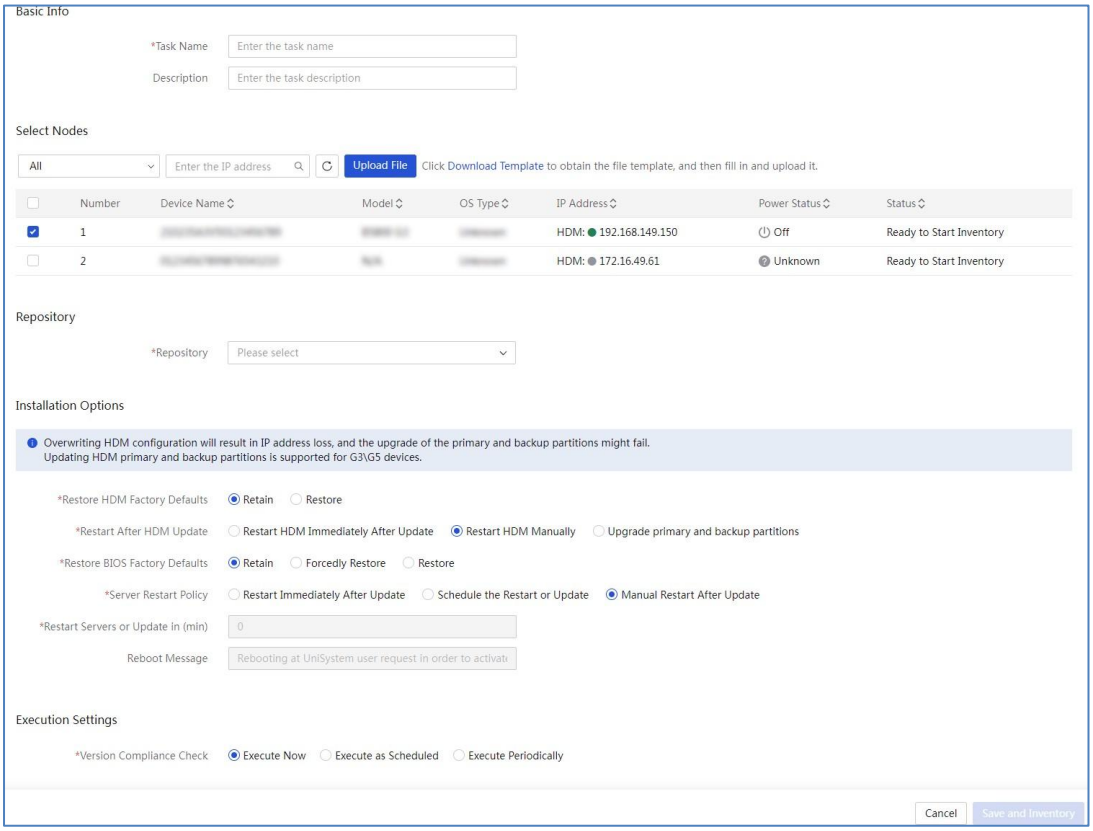
   ノードlocalhostは、UniSystemサーバーソフトウェアがインストールされているホストです。UniSystemがサーバーにインストールされると、**localhost**という名前のタスクが自動的に作成されます。**localhost**という名前のタスクは削除できません。**localhost**という名前の別のローカルタスクは追加できません。

   図200 コンポーネントの更新



2. **Add**をクリックして、図201に示すページに入ります。このページで、次の手順を実行します。
   a. タスク名と説明を入力します。
   b. ターゲットサーバーノードを選択します。次のいずれかの方法を使用して、ノードをすばやく検索できます。
      – IPアドレスバーで、ノードのHDMの管理IPアドレスを入力します。
      – **Download Template**をクリックしてファイルテンプレートをダウンロードし、ファイルテンプレートでノードのHDMの管理IPアドレスを指定します。次に、**Upload File**をクリックしてテンプレートをアップロードします。
   c. VMwareコンポーネントの更新タスクを追加するには、**File Template**リンクをクリックしてテンプレートをダウンロードします。HDM管理IP、VMware OS IP、およびVMware OSのrootユーザー名とパスワードを入力します。次に、**Upload File**をクリックして、テンプレートファイルをアップロードします。
   d. サーバーに割り当てるレポジトリを**Repository**リストから選択します。
   e. **Installation Options**領域で、HDM/BIOSファームウェア設定の保持ポリシーとサーバー再起動ポリシーを設定します。
   f. **Execution Settings**領域で、バージョンコンプライアンスチェックを設定します。
3. **Save and Inventory**をクリックします。
4. インベントリ後、必要に応じて次の操作を実行します。
   - タスクに対して**Execute Now**または**Execute as Scheduled**が選択されている場合は、コンポーネント情報を表示してコンポーネントを選択し、**Deploy**をクリックします。これにより、システムはすぐにコンポーネントの更新を開始するか、スケジュールに従ってコンポーネントの更新を開始します。
   - タスクに対して**Execute Periodically**が選択されている場合は、コンポーネント情報を表示して**OK**をクリックします。タスクが正常に作成されます。
   - タスクを編集するには、**Back to Edit**をクリックします。
5. 展開後、**Logs**をクリックします。表示されるダイアログボックスで、タスク展開ログを確認できます。

図201 タスクの追加



タスクのインベントリと展開

このタスクについて

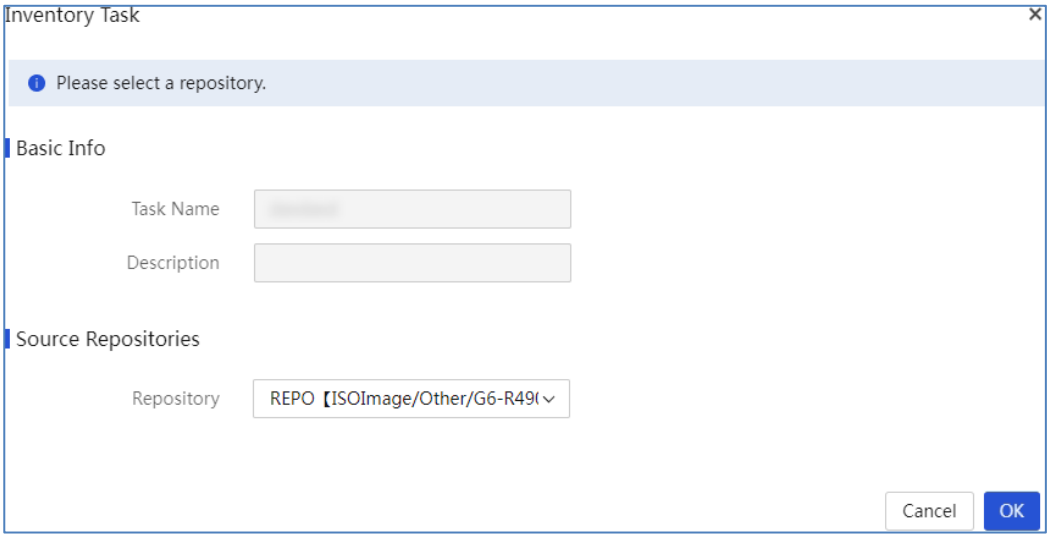
タスク内のノードのコンポーネントを更新するには、次のタスクを実行します。

- **Inventory a task**: タスク内の各ノードに関する情報を取得し、ノードに適用可能なコンポーネントをリポジトリから除外します。タスクをインベントリする前に、タスクにバインドされているすべてのリポジトリがインベントリされていることを確認します。
- **Deploy a task**: タスク内のノードに、更新するコンポーネントをインストールします。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Update Components**を選択します。
2. ターゲットタスクの**Actions**列で**Inventory**をクリックします。表示されたダイアログボックスで、**Repository**リストからターゲットリポジトリを選択します。

図202 タスクのインベントリ

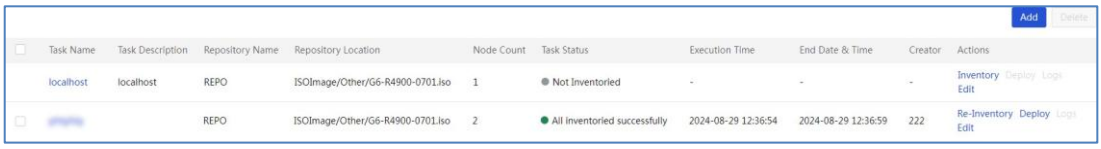


3. 図203に示すように、インベントリが完了すると、**Deploy**リンクが表示されます。**localhost**という名前のローカルタスクは、他のタスクと一緒に展開することはできません。

重要:

- タスク内の一部のノードでコンポーネントのインベントリまたは展開に失敗しても、インベントリおよび展開プロセス全体には影響しません。
- タスクがインベントリまたはデプロイされている場合、UniSystemはタスク内の異常な状態のノードを自動的にスキップします。タスク内のすべてのノードが異常な状態にある場合、タスクのインベントリまたはデプロイはできません。

図203インベントリの作成



4. Deployをクリックします。図204に示すページが開きます。コンポーネントのバージョンをチェックして、コンポーネントを更新するかどうかを決定します。コンポーネントの詳細を表示するには、コンポーネントの名前をクリックします。コンポーネントの依存アイテムに従って、現在のコンポーネントの依存コンポーネントを更新する必要があるかどうかを判断します。また、ターゲットコンポーネントを有効にするために再起動が必要かどうかも判断します。

重要:

Restart HDM Immediately After Updateを選択した場合、現在のHDMバージョンが**HDM-2.XX**形式であり、HDM-2.96よりも古い場合は、他のコンポーネントの展開に影響を与えないように、HDMアップデートを個別に展開します。

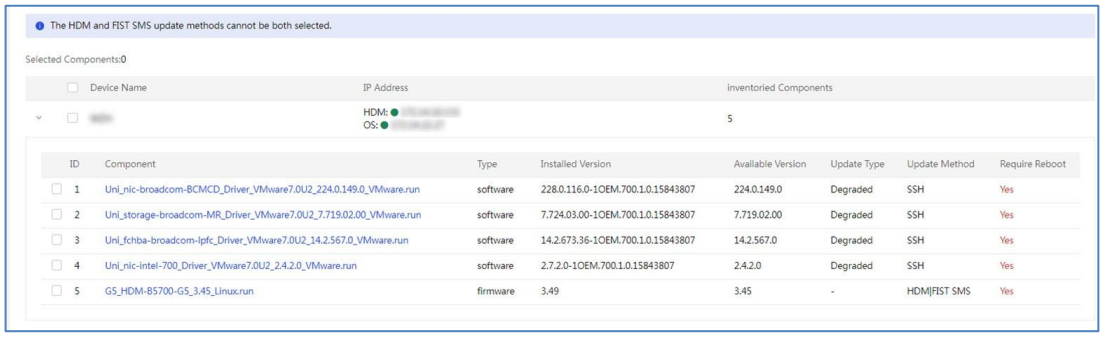
5. スケジュールされた展開を設定します。スケジュールされた展開を有効にすると、スケジュールされた時間を選択できます。UniSystemはスケジュールされた時間に展開を開始します。スケジュールされた展開を無効にすると、**OK**をクリックした後、UniSystemはすぐに展開を開始します。

重要:

- スケジュールされたデプロイメント機能を使用するときは、時間の混乱を避けるために、ブラウザーの時刻がサーバーの時刻と同じであることを確認してください。
- スケジュールされた展開が有効になっているタスクの場合、関連するリポジトリとタスクは次のようになります。
  UniSystemの再起動後に自動的にインベントリされます。

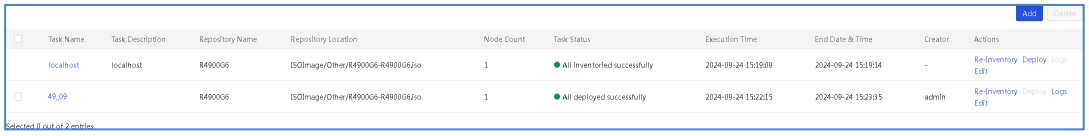
6. **OK**をクリックして、配置を開始します。

図204 タスクの導入



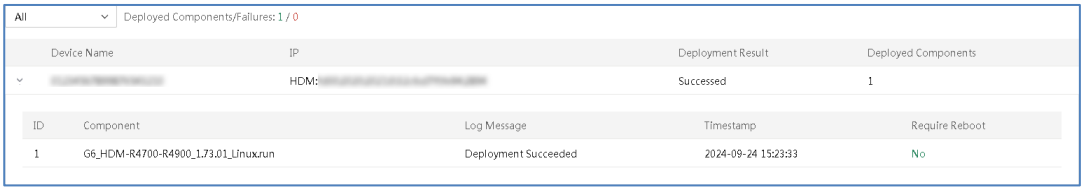
7. 図205に示すように、デプロイが完了したら、**Logs**をクリックしてデプロイログを表示します。

図20 5導入の完了



8. 図206に示すように、タスクデプロイメントログページを入力して、コンポーネントデプロイメントの結果を表示します。

図206 タスク展開ログ



タスクの詳細を表示する

このタスクについて

タスクの詳細を表示することで、ノードの配備状況や実行内容など、コンポーネントの更新タスクの詳細を直感的かつ容易に把握でき、ノードコンポーネントの更新状況を総合的に把握することができます。

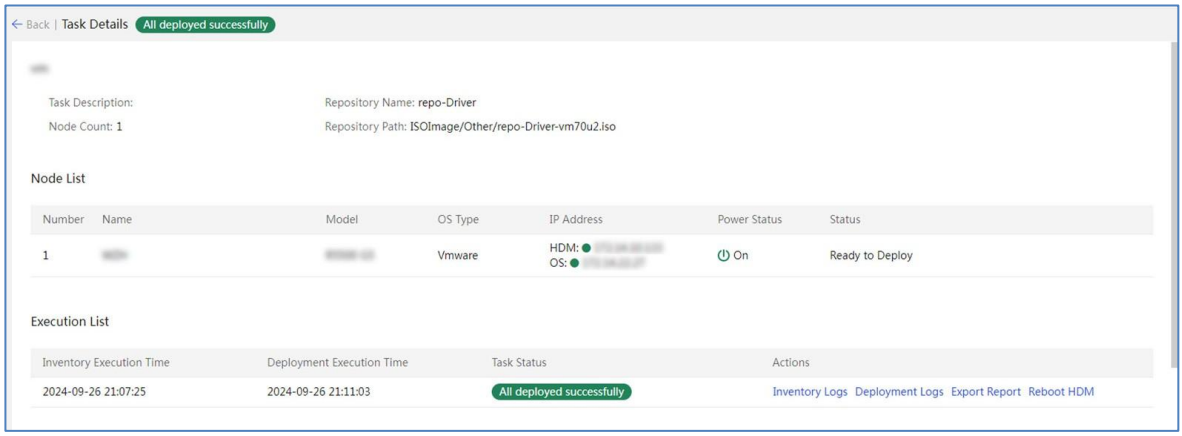
手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Update Components**を選択

します。このページでは、すべてのタスクを表示できます。

2. ターゲットタスクの**Task Name**列のリンクをクリックします。タスクの基本情報、実行リスト、ノードリスト、インストールオプションおよび実行設定が表示されます。
3. (任意)インベントリログ、展開ログ、エクスポートレポートを表示し、実行リストでHDMを再起動できます。

図207 タスクの詳細



タスクを編集する

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Update Components**を選択します。
2. 編集するタスクの**Actions**列で**Edit**をクリックします。表示されるダイアログボックスで、次の手順を実行します。
   a. **Basic Info**領域で、タスクの説明を編集します。
   b. **Select Nodes**領域で、編集するノードを選択します。
   c. **Repository**領域で、タスクに割り当てるリポジトリを**Repository**リスト。
   d. **Installation Options**領域で、HDM/BIOSファームウェア設定の保持ポリシーとサーバー再起動ポリシーを編集します。
3. **OK**をクリックします。

問題のトラブルシューティング

タスクインベントリ後に結果が表示されない

症状

コンポーネントの更新のためにタスクがインベントリされた場合、インベントリ結果は表示されません。

原因

- ユーザーが管理者またはrootユーザーとしてUniSystemを実行していない。
- UniSystemサーバーまたはFIST SMSが実行されているオペレーティングシステムでは、ファイアウォールは無効になっていません。

アクション

1. 管理者またはrootユーザーとしてUniSystemを実行します。Windowsでは、**FistLaunch_x64.bat**ファイルを右クリックし、**Run as administrator**を選択します。Linuxでは、rootユーザーに切り替えてUniSystemを実行します。
2. オペレーティングシステムでファイアウォールが無効になっていることを確認します。ファイア

ウォールが有効になっている場合は、ファイアウォールを無効にして、タスクインベントリを再度実行します。

3. 問題が解決しない場合は、テクニカルサポートに連絡してください。

コンポーネントの更新のためのタスクの展開中に、現在のコンポーネントのバージョンが不明と表示される

症状

コンポーネントの更新のためのタスクの展開中に、現在のコンポーネントが「不明」と表示されます。

原因

UniSystemが現在のサーバーコンポーネントのバージョンを取得できません。

アクション

アクションは必要ありません。デプロイ後、コンポーネントのバージョンを調べて、コンポーネントが正常に更新されたかどうかを確認できます。

HDMユーザー権限が不足しています

症状

コンポーネントの更新に失敗しました。理由は、HDMユーザーに特権がないためです。

原因

サーバーのHDMユーザーに管理者権限がありません。

アクション

Serversページでデバイスを編集し、管理者としてHDMユーザーの新しいユーザー名とパスワードを指定します。

オペレーティングシステムで満たされていないソフトウェア要件

症状

コンポーネントの更新に失敗しました。依存ソフトウェアがインストールされていないことを示すメッセージが表示されます。

原因

FIST SMSを使用してコンポーネントを更新すると、オペレーティングシステム内の更新に依存するソフトウェア(GNU Compiler Collection(GCC)など)はインストールされません。

アクション

FIST SMSが存在するオペレーティングシステムの指示に従って、ソフトウェアをインストールします。

UniSystemがサーバーに接続できない

症状

コンポーネントの更新に失敗しました。理由は、ログインに失敗したためです。

原因

- UniSystemサーバーとHDMの間のネットワーク接続でエラーが発生しました。
- HDMまたはFIST SMSにログインするためのユーザー名またはパスワードが正しくありません。

アクション

1. サーバーの電源が正しく入り、ネットワーク接続が正常であることを確認します。
2. サーバー情報を表示し、Serversページでデバイスを編集して、必要に応じての正しいユーザー名とパスワードを指定します。

コンポーネントの展開に失敗しました

症状

コンポーネントの更新に失敗しましたが、理由は表示されません。

原因

- FIST SMSを使用してドライブファームウェアを更新する場合、Python環境はインストールされません。
- PMem 200メモリー、Rack_NIC-360T-B2およびRack_NIC-560F-B2ネットワークアダプタなど、一部のコンポーネントのファームウェアには保護メカニズムがあり、繰り返しの更新をサポートしていません。
- FIST SMSを使用したファームウェアまたはドライバーの更新では、コンポーネントの元のドライバーバージョンが低すぎるため、更新が失敗します。

アクション

1. ドライブファームウェアでのインストールが失敗した場合は、オペレーティングシステムにPythonがインストールされ、Python環境が正常であることを確認します。

重要:

複数のPythonバージョンが使用可能な場合は、ln-sまたはupdate-alternativesコマンドを使用して、デフォルトのPythonバージョンを指定します。例:

- **Ln -s /usr/local/python3/bin/python3.7 /usr/bin/python**
- **sudo alternatives--python/usr/bin/python3を設定します。**

2. オペレーティングシステムを再起動して、前回の展開を有効にします。
3. インストールに失敗したコンポーネントのドライバーバージョンを特定し、必要に応じてドライバーを手動で更新します。
4. 問題が解決しない場合は、テクニカルサポートに連絡してください。

ファームウェアのアップデート

メモ:

- この機能を使用するには、最初にHDMサーバーノードをUniSystemに追加する必要があります。詳細は、「サーバーの管理」を参照してください。
- サーバーでファームウェアの更新が進行中の間は、サーバーでテンプレートの適用、コンポーネントの更新、またはその他の操作を実行しないでください。
- アップグレードの前に、ファームウェアを予想されるバージョンにアップグレードできることを確認するためのベストプラクティスとして、まずREPOで関連するファームウェアバージョン情報を確認します。

UniSystemでは、次の方法でファームウェアを更新できます。

- **Offline firmware update**: この方法では、UniSystemにアップロードされたREPO(LiveCDシステムを含む)を使用して、複数のサーバーのファームウェアを一括して自動的に更新します。この方法は、元のオペレーティングシステムの動作に影響します。
- **HDM out-of-band firmware update**: この方式では、HDMを使用してREPOを更新します。次のサーバー起動時に自動的にiFISTにアクセスしてファームウェア更新を実行します。

ファームウェアをオフラインで更新します。

このタスクについて

無人ファームウェア更新は、複数のサーバーで一括して実行できます。

この機能を使用する前に、LiveCDシステムを含むREPO(ISOファイル)をUniSystemにアップロードします。操作手順については、「イメージの管理」を参照してください。

制約事項とガイドライン

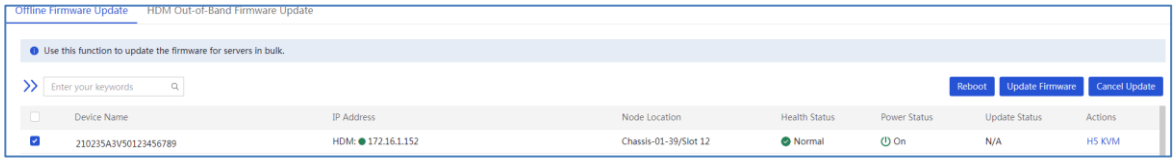
- アップデートを正常に実行するには、ターゲットサーバーにKVM経由でマウントされたイメージがなく、USBポートがUSBドライブに接続されていないことを確認します。
- ファームウェアの更新速度を保証するには、ベストプラクティスとしてHDM専用ポートを使用します。共有ネットワークポートを使用する場合は、UniSystemサーバー上の対応するNICのレートを100 Mbpsに設定します。
- アップデートプロセス中はネットワークを安定させてください。
- サーバー上で進行中の更新プロセスを中止し、新しい更新プロセスを開始するには、まずサーバーを選択し、**Cancel Update**をクリックします。
- 異常な状態のHDMサーバーノードはリブートできません。
- UniSystemは、レポジトリが更新に使用され、サーバーがHDM 2.11以降を実行している場合にのみ、サーバーのファームウェア更新の進行状況と結果を表示できます。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Firmware Update** > **Offline Firmware Update**を選択します。
2. ターゲットサーバーを選択し、**Update Firmware**をクリックします。

   ターゲットサーバーをすばやく除外するには、左側のナビゲーションウィンドウから静的グループと動的グループを使用するか、検索領域にキーワードを入力します。
3. 表示されたダイアログボックスで、更新するイメージファイルを選択し、**OK**をクリックします。
4. (オプション)サーバーのファームウェア更新の進行状況を表示するには、サーバーの**Actions**カラムの**H5 KVM**をクリックします。
5. (オプション)サーバーの更新が完了したら、サーバーの**Update Status**カラムの**Update Finished**または**Update Failed**リンクをクリックして、更新結果を表示します。
6. 一部のファームウェア製品では、有効にするために再起動する必要があります。更新されたサーバーを選択し**Reboot**をクリックして、サーバーを再起動します。

図208 オフラインでのファームウェアアップデート



HDM帯域外管理を使用してファームウェアを更新する

このタスクについて

HDM帯域外管理を使用すると、複数のサーバー上のREPOを一括で更新できます。

この機能を使用する前に、REPOをUniSystemにアップロードします。操作手順について詳しくは、「イメージの管理」を参照してください。

この機能を使用するには、次の要件を満たす必要があります。

- UniSystemは、HDMおよびiFISTとともに使用される。

- UniSystemは、UniSystem-2.32以降のバージョンです。
- HDMは、HDM-2.52以降のバージョンです。
- iFISTは、iFIST-1.32以降のバージョンです。

Update Configurationフィールドと**Update Options**フィールドは、G6サーバーでは使用できません。新しいバージョンを有効にするには、更新後にサーバーを手動で再起動する必要があります。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Firmware Update** > **HDM Out-of-Band Firmware Update**の順に選択します。

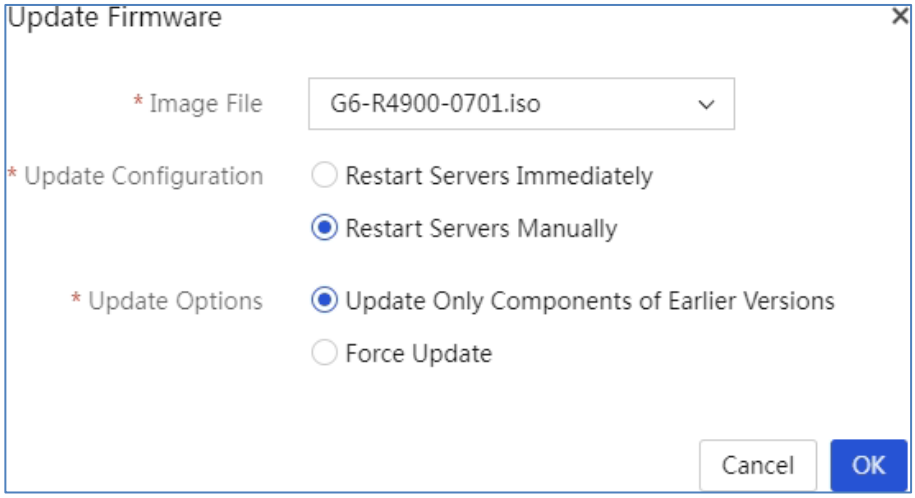
   図209 HDM帯域外ファームウェアアップデート



2. ターゲットサーバーを選択し、**Update Firmware**をクリックします。表示されるダイアログボックスで、更新するイメージファイル、ファームウェア更新後のサーバーの再起動方法、および更新オプションを選択します。

   ターゲットサーバーを検索するには、左側のナビゲーションペインから静的グループまたは動的グループを選択するか、検索ボックスにキーワードを入力します。

   図210 パラメータの設定



3. **OK**をクリックします。
4. サーバーで進行中のファームウェア更新操作をキャンセルするには、ターゲットサーバーを選択し、**Cancel Update**をクリックします。表示される確認ダイアログボックスで、OKをクリックします。

   サーバーがファイルの更新を確認している場合は、サーバー上で進行中のファームウェア更新操作を取り消すことはできません。

安全な消去

ライフサイクルの終了またはその他の理由でサーバーが停止した場合は、セキュリティで保護された消

去機能を使用してサーバーのHDM、BIOS、および記憶域データを消去し、ユーザーデータの漏洩を防ぐことができます。消去するデータの容量が大きい場合、データの消去処理に時間がかかる(1日以上)ことがあります。

この機能は、手動による介入なしに、サーバー上でのバッチの安全な消去操作をサポートします。消去プロセスは自動化されており、消去結果が表示されます。

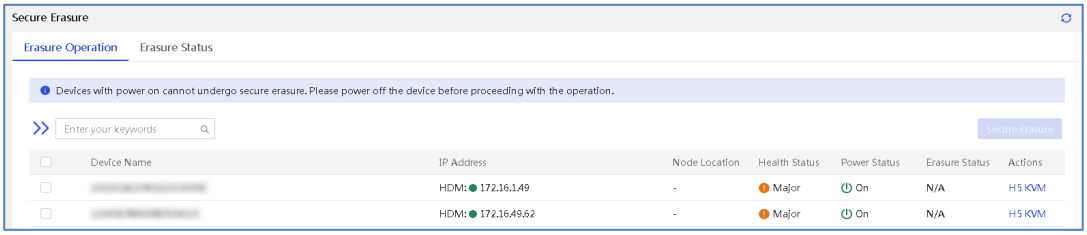
△注意:

- セキュリティで保護された消去機能を使用する場合は、注意が必要です。この機能を使用する前に、消去するデータが不要で安全に消去できることを確認してください。そうでない場合は、重要な情報が失われないように、事前にデータをバックアップしてください。
- データ消去を開始する前に、サーバーに接続されているすべての外部ストレージデバイス(外部ドライブを含むがこれに限定されない)を取り外して、誤ってデータを消去しないようにしてください。
- ストレージデータの消去プロセス中に、サーバーは自動的に再起動し、iFISTに入って消去操作を実行します。消去が完了すると、サーバーは再び再起動し、消去プロセスの前にシステムスタートアップ項目に入ります。
- データを正常に消去するには、データの消去を開始する前に、ターゲットサーバーのiFISTソフトウェアバージョンがiFIST-1.58以上であり、HDMソフトウェアバージョンがHDM2-1.57以上であることを確認してください。
- HDMデータを消去した後、HDM管理IPアドレスはデフォルトのアドレスに復元されます。これにより、ユーザーは UniSystem を介してサーバー上で他の操作を実行できなくなる可能性があります。

Secure Eraseを実行するには、次の手順

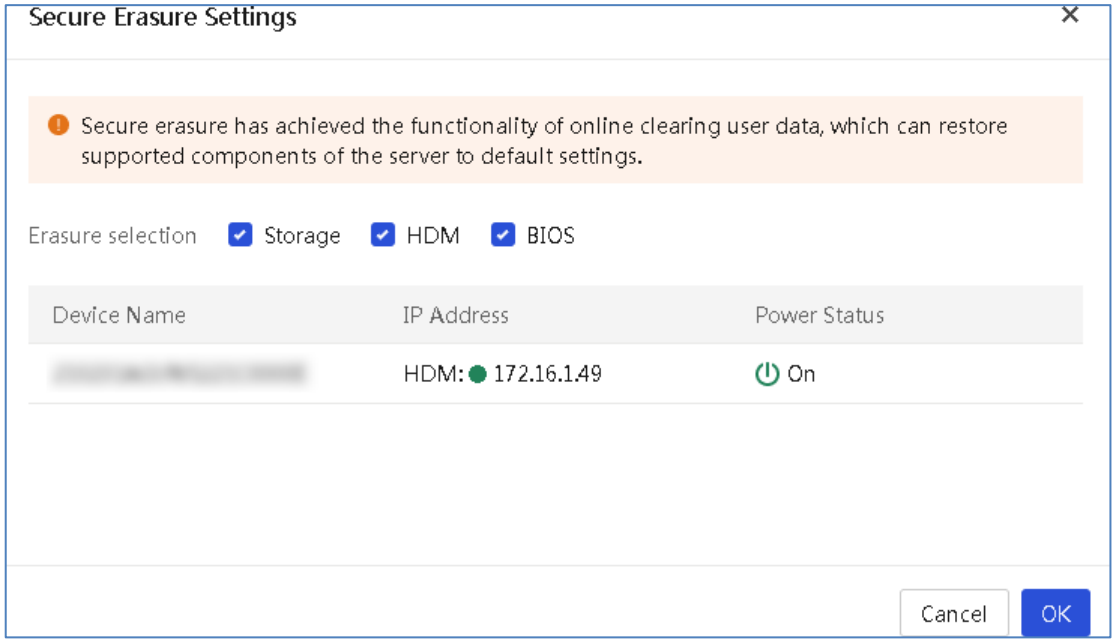
1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Secure Erasure**を選択します。

   図211 消去操作

2. ターゲットサーバーを検索するには、グループを選択し、検索ボックスにキーワードを入力します。
3. ターゲットサーバーを選択し、**Secure Erasure**をクリックします。**HDM**、**BIOS**、および**Storage**から消去する項目を選択します。

図212 消去オプションの選択



4. **OK**をクリックします。表示されたダイアログボックスで、UniSystemログインパスワードを入力します。
5. **OK**をクリックします。UniSystemはパスワードを確認し、確認に合格するとデータの消去を開始します。
6. データの消去を開始すると、ページは自動的に**Erasure Status**タブに移動し、現在のサーバー消去操作のステータスと進行状況が表示されます。表20に、使用可能な消去結果と、消去を有効にする方法を示します。

表20 消去の結果

項目	結果を消去	実施方法
HDM	HDMを工場出荷時のデフォルトに戻します。SDSログとフラッシュカードのデータは消去されます。	HDMが自動的に再起動します。
BIOS	• BIOSのデフォルト設定に戻します。 • BIOSの管理者パスワードとユーザーパスワードが消去されます。BIOSは、パスワードが消去されたユーザーが次の再起動時にBIOSセットアップユーティリティに入るためのパスワードを必要としません。 • サーバーの電源投入時パスワードがBIOSから消去されます。	サーバーを再起動します。
不揮発性DRAM(NVDIMM)	メモリーモードではないNVDIMMのデータは消去されます。消去後、すべてのNVDIMMはメモリーモードで動作します。	サーバーが自動的に再起動します。
ストレージコントローラー	• RSTe RAIDコントローラおよびVROCモジュールによって管理されているすべての論理ドライブが削除されます。 • 次のLSIストレージコントローラーによって管理されているすべての論理ドライブが削除されます。 • 消去前にLSIコントローラがRAIDモードで動作している場合、消去動作が終了すると、RAIDモードのJBOD属性がONに変更される。 ○ HBA-LSI-9311-8iの場合	サーバーが自動的に再起動します。

	○ HBA-LSI-9500-16iの場合 ○ HBA-LSI-9500-8iの場合 ○ HBA-LSI-9540-8iの場合 • 次のPMCストレージコントローラーによって管理されているすべての論理ドライブが削除されます。 ○ HBA-H460-B1の場合 ○ RAID-P 4408-Mf-8 i:2 GB以上 ○ RAID-P2404-Mf-4iの場合 ○ RAID-P460-B2の場合 ○ RAID-P460-B4の場合 • 以下のMARVELLストレージコントローラーによって管理されているすべての論理ドライブが削除されます。 ○ RAID-MARVELL-SANTACRUZ-2i(RAID-マーベル-サンタクルーズ-2 i)	
ドライブ	ドライブ内のすべてのデータが削除されます。	サーバーが自動的に再起動します。
SDカード	SDカード内のデータがすべて削除されます。	サーバーが自動的に再起動します。

サーバーソフトウェアライセンス管理

この機能は、G6以降のサーバーでのHDMライセンスの一括管理操作(表示、エクスポート、インストール、アンインストールなど)をサポートします。

ライセンスとは、特定のソフトウェア機能を使用するためにサーバーの製造元からユーザーに付与される法的な許可のことです。HDMライセンスが必要な機能とそのプロパティの一覧については、「H3C HDM Management Software License Matrixes」を参照してください。ライセンスの取得方法の詳細については、「H3C Servers HDM Licensing Guide」を参照してください。

制約事項とガイドライン

- ライセンスアクティベーションファイルは、サーバー製造元の公式チャネルから入手します。
- ライセンスアクティベーションファイルをインストールする前に、ターゲットサーバーのDIDコードが、要求されたライセンスアクティベーションファイルのDIDコードと一致していることを確認してください。
- 正式に認可されたライセンスアクティベーションファイルをインストールする前に、サーバーのライセンスが次のいずれかの状態であることを確認します。
  - サーバーには、別の公式ライセンスまたは試用ライセンスのアクティベーションファイルがインストールされていません。
  - 公式ライセンスがインストールされている場合は、最初にライセンスをアンインストールし、ライセンスアンインストールファイルをエクスポートします。
  - 試用ライセンスがインストールされている場合は、最初にライセンスアクティベーションファイルをアンインストールします。
- アクティベーションファイルをインストールする前に、サーバーにライセンスアクティベーションファイルがインストールされていないこと、およびアクティベーションファイルに対応するライセンスが有効期間内であることを確認してください。

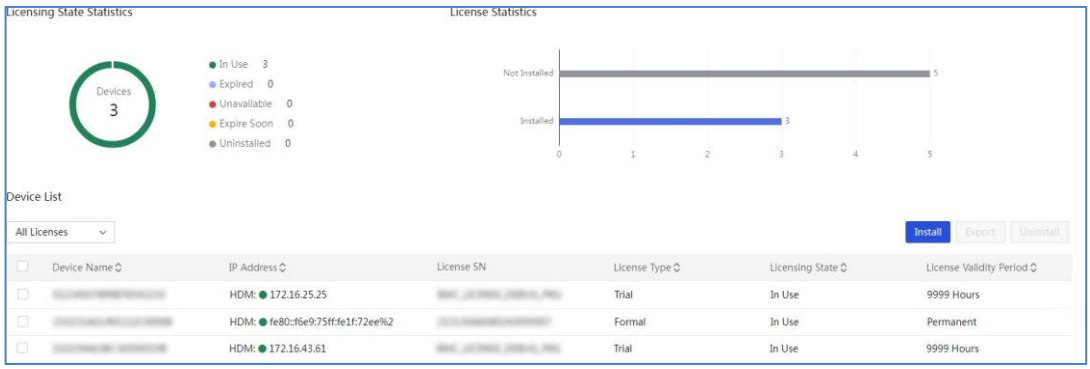
アンインストール後、UniSystemは、ライセンスが正常にマウント解除されたすべてのデバイス上の公式ライセンスのアンインストールファイルを自動的にパッケージ化してエクスポートします。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Manage Server Software**

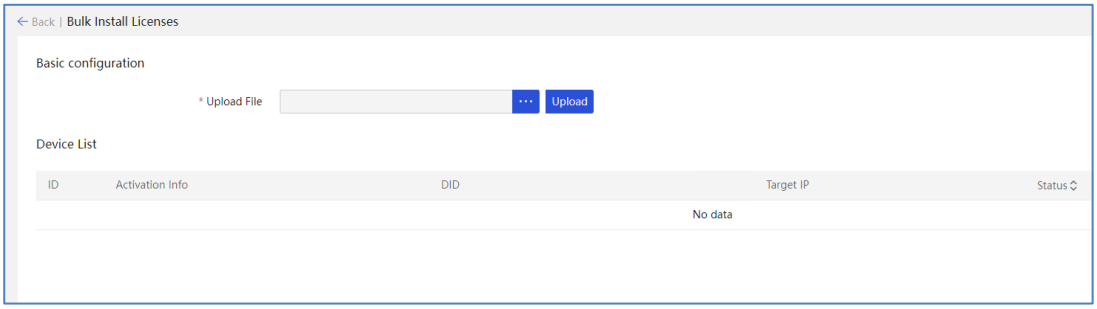
Licensesを選択します

図213 サーバーソフトウェアライセンス管理ページ



2. サーバーのライセンスステータスを表示します。
3. ライセンスステータスで情報をフィルタリングするには、**Device List**セクションでステータスオプションを選択します。
4. サーバーソフトウェアライセンス情報の概要をエクスポートするには、ターゲットサーバーを選択し**Export**をクリックします。
5. ライセンスをインストールするには、**Install**をクリックします。一括ライセンスインストールページが開きます。
   a. HDMライセンスアクティベーションファイルを.akまたは.zip形式でアップロードします。アップロードが完了すると、ライセンスインストールのターゲットデバイスに関する情報がページに表示されます。
   b. **Install**をクリックして、HDMライセンスのインストールを開始します。
   c. インストールが完了したら、**Finish**をクリックします。

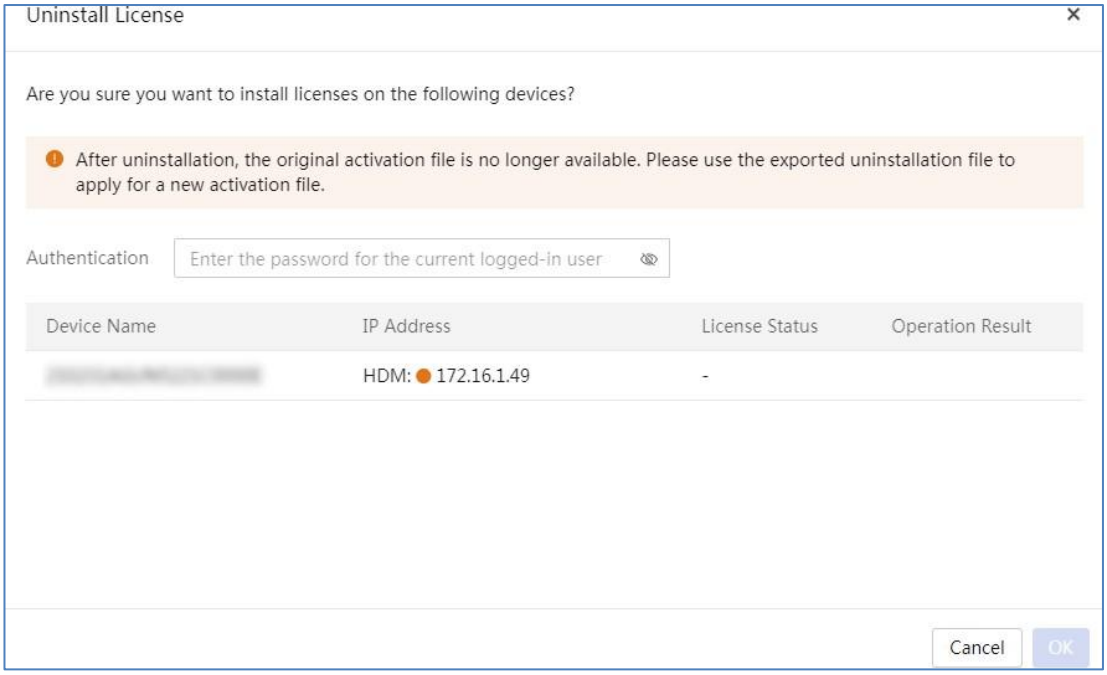
図214 ライセンスのインストール



ページ

6. ライセンスをアンインストールするには、ターゲットサーバーを選択し、**Uninstall**をクリックします。
   a. 現在のUniSystemユーザーのパスワードを入力します。
   b. **OK**をクリックします。UniSystemはパスワードを確認します。確認に成功すると、UniSystemはライセンスのアンインストールを開始します。

図215 ライセンスのアンインストールの確認



パラメータ

- **Device Name**: サーバーの名前。
- **IP Address**: サーバーのHDM管理IPアドレス。
- **License Serial Number**:ライセンスのシリアル番号。
- **ライセンスの種類:**
  - **Formal**: 公式ライセンスは、サーバー製造元の公式チャネルを通じてのみ取得できます。公式ライセンスは、インストール、アンインストール、および移行をサポートし、永続的に有効です。
  - **Trial**: サーバー製造元のテクニカルサポートに連絡して、試用ライセンスを入手できます。試用ライセンスは、インストールとアンインストールをサポートしますが、移行はサポートしません。試用ライセンスの有効期間は90日間です。試用ライセンスの有効期限が切れた後に特定のソフトウェア機能を使用するには、正規ライセンスを購入して適切な時期にインストールしてください。
- **ライセンスの状態:**
  - **In Use**: ライセンスアクティベーションファイルは正常に機能しています。
  - **Expired**: ライセンスアクティベーションファイルの有効期限が切れています。
  - **Unavailable**: ライセンスアクティベーションファイルは使用できません。テクニカルサポートに連絡してください。
  - **Expire Soon**: ライセンスアクティベーションファイルの有効期限が近づいています。
  - **Uninstalled**: ライセンスアクティベーションファイルがアンインストールされました。
  - **Not Installed**: サーバーにライセンスアクティベーションファイルがインストールされていません。
- **License Validity Period**: ライセンスアクティベーションファイルの有効期限。
- **DID:** サーバーのDevice Identification Code(DID)。
- **Target IP**: ライセンスをインストールするサーバーのHDM管理IPアドレス。
- **Status**: ライセンスのインストールステータス(Being Installed、Successed、Failedなど)。

サーバーの診断

メモ:

この機能をサポートするのは、デフォルトのadminユーザーと、すべてのリソースに対する管理者の役割と権限を持つユーザーのみです。

この機能は、高速診断およびストレステストサーバーの一括実行をサポートし、サーバー上のコンポーネントをスキャンし、各コンポーネントに関する情報を収集および整理し、各コンポーネントの動作およびヘルスステータスを診断します。これにより、タイムリーな問題のトラブルシューティング、デバイス使用リスクの軽減、および診断レポートのエクスポートが容易になります。

サーバーとそのコンポーネントのステータスとパフォーマンスを分析するレポートをダウンロードして表示できます。

診断タスクリストを表示する

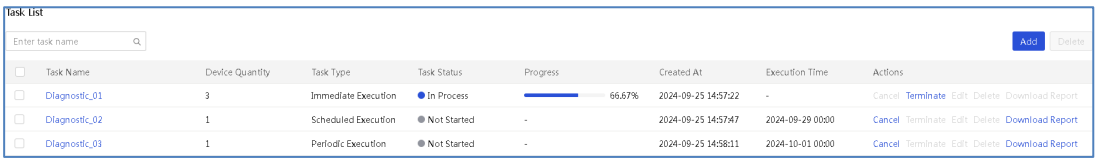
制約事項とガイドライン

- まだ開始されておらず、実行期間内にあるタスクを取り消すことができます。
- **In Progress**状態のタスクを終了できます。
- 進行中のタスク(進行中のタスク、キャンセルされていないスケジュールされたタスク、キャンセルされていない定期タスクなど)は編集できません。
- 開始されていないタスク、進行中のタスク、または不完全な定期タスクは削除できません。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Diagnostics**を選択します。
2. 追加したタスクと簡単なタスク情報を表示します。
3. タスクの編集、キャンセル、終了、削除、またはタスクのレポートのダウンロードを行うには、そのタスクの**Actions**コラムで対応するボタンをクリックします。

図216 サーバーの診断



パラメータ

- **Task Name**:タスク名。
- **Device Quantity**: タスクに含まれるデバイスの合計数。
- **Task Type**: **Immediate Execution**, **Scheduled Execution**, および **Periodic Execution**を含むタスク実行モード。
- **Task Status**: **Not Started**、**In Progress**、**All Succeeded**、**Partially Succeeded**、**All Failed**、**Expired**および**Progress**:タスクの進行中の実行の進行状況(パーセント)。
- **Created At**: タスクが最後に作成または編集された時刻。
- **Execution Time**: スケジュール済タスクまたは定期タスクが実行された時間。

診断タスクを構成する

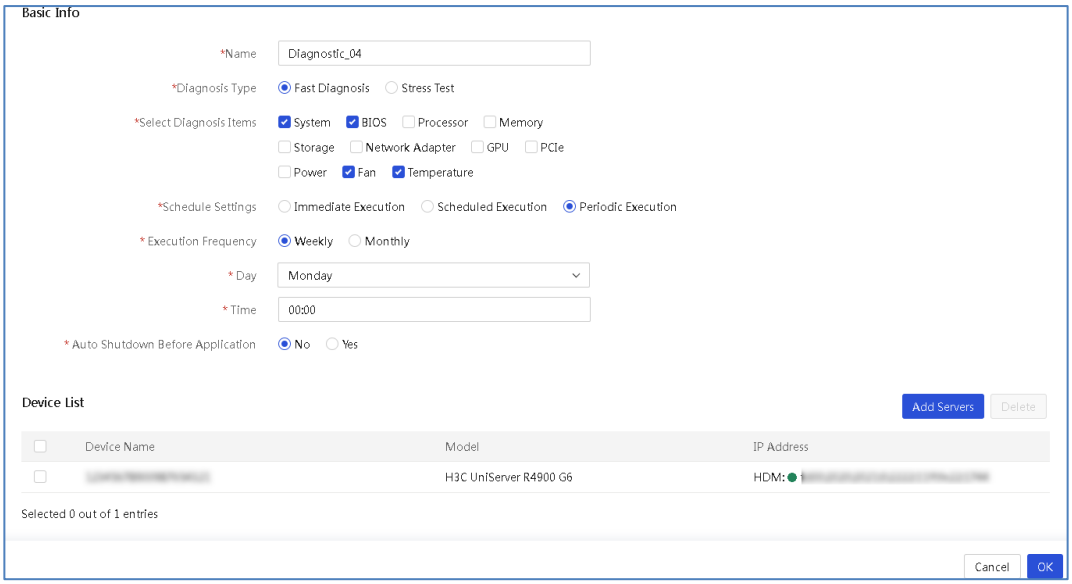
メモ:

この機能をサポートするのは、HDMによって管理されるG6以降のサーバーだけです。

診断タスクを追加する

1. ナビゲーションペインで、**enu** > **Deployment** > **Servers** > **Server Diagnostics**を選択します。
2. **Add**をクリックします。

   図217 タスクの追加



3. 基本的なタスク設定を構成します。
   a. タスク名を入力します。
   b. 診断タイプと診断項目を選択します。
   c. タスクスケジュール設定を構成します。
      - **Immediate Execution**:タスクが作成された直後にタスクを実行します。
      - **Scheduled Execution**:スケジュールされた時間に診断タスクを1回実行します。このオプションを選択した場合は、タスク実行時間を構成します。タスクが追加されると、システムはスケジュールされた時間にサーバー上で診断タスクを実行します。
      - **Periodic Execution** :定期タスクを実行する頻度を指定し、スケジュールされた実行時間の前に実行するアクションを指定します。
4. **Add Servers**をクリックします。表示されたページで、診断が必要なサーバーを選択し**OK**をクリックします。
5. **OK**をクリックします。

診断タスクの編集

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Diagnostics**を選択します。
2. ターゲットタスクの**Actions**列で**Edit**をクリックします。
3. 基本的なタスク設定を編集します。
4. 診断するデバイスの編集:
   - サーバーを追加するには、**Add Servers**をクリックします。表示されたページで、診断が必要なサーバーを選択し、**OK**をクリックします。

- リストからデバイスを削除するには、デバイスを選択して**Delete Device**をクリックします。

5. OKをクリックします。

診断タスクの削除

メモ:

- 進行中のタスク、キャンセルされていないスケジュールされたタスク、またはキャンセルされていない定期タスクは削除できません。
- タスクを削除すると、タスク関連のレポートも削除されます。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Diagnostics**を選択します。
2. 診断タスクを削除するには、次のいずれかのタスクを実行します。
   - 診断タスクを削除するには、そのタスクの**Actions**列で**Delete**をクリックします。
   - 診断タスクを一括削除するには、これらのタスクを選択し、右上隅にある**Delete**をクリックします。

パラメータ

- **Name**:サーバー診断タスクの名前。
- **Diagnosis Type**:サーバー診断タイプを選択します。オプションには、Fast DiagnosisおよびStress Testがあります。
- **Select Diagnosis Items**: タスク内の診断アイテムを選択します。
  - **Fast Diagnosis**を選択した場合は、可能な項目は**System**、**BIOS**、**Processor**、**Memory**、**Storage**、**Network Adapter**、**GPU**、**PCIe**、**Power**、**Fan**,そして**Temperature**があります。
  - 負荷テストを選択した場合は、プロセッサー、メモリー、ストレージなどの項目が表示されます。
- **Scheduled Settings**:診断タスクの実行設定を設定します。オプションは次のとおりです。
  - **Immediate Execution**:タスクが作成された直後にタスクを実行します。
  - **Scheduled Execution**:スケジュールされた時間に診断タスクを1回実行します。このオプションを選択した場合は、タスク実行時間を構成します。タスクが追加されると、システムはスケジュールされた時間にサーバー上で診断タスクを実行します。
    - **Execution Time**:タスクを実行する時間を指定します。
  - **Periodic Execution**:定期タスクを実行する頻度を指定します。
    - **Execution Frequency**:オプションには、**Weekly**および**Monthly**
    - **Day**/**Date**:実行日を指定します。
    - **Time**:実行時間を指定します。
    - **Auto Shutdown Before Application**:スケジュールされた実行時間の前にサーバーを自動的にシャットダウンするかどうかを選択します。
  - **Device List**:タスクが有効になるデバイスを指定します。
    - **Device Name**:サーバー名。
    - **Model:**サーバーモデル。
    - **IP Address**:サーバーのIPアドレス。

タスクの詳細を表示する

制約事項とガイドライン

- H5 KVMを使用するには、ログインアカウントにデバイス管理権限があることを確認してください。

- UniSystemをバージョン2.72にアップグレードすると、以前のバージョンのタスクの詳細で診断項目が表示されない場合があります。

手順

1. ナビゲーションペインで、**Menu** > **Deployment** > **Servers** > **Server Diagnostics**を選択します。
2. タスクの名前リンクをクリックすると、そのタスクの基本情報、デバイスリスト、およびタスク結果が表示されます。
3. デバイスのタスク実行履歴を表示するには、そのサーバーのIPアドレスの横にある > をクリックします。
4. デバイスのリモートコンソールを起動するには、そのデバイスの**Actions**カラムで**H5 KVM**をクリックします。

図218 タスクの詳細の表示



パラメータ

- **基本情報**
  - **Task Name**:タスク名。
  - **Creator:**タスクを最後に作成または編集したユーザーの名前。
  - **Total Devices**:タスクに含まれるサーバーの総数。
  - **Created At**:タスクが最後に作成または編集された時刻。
  - **End Time**:タスクが最後に実行された時刻。
  - **Total Duration**:最後に実行されたタスクの合計期間。
  - **Diagnosis Type**:サーバー診断タイプを選択します。オプションには、Fast Diagnosisとストレステストを含んでいます。
  - **Scheduled Settings**:タスク実行モード。
  - Execution Time:スケジュール済タスクまたは定期タスクが実行された時間。
  - **診断項目**
    - **Fast Diagnosis**を選択した場合は、可能な項目には**system**, **BIOS**, **Processor**, **Memory**, **Storage**, **Network Adapter**, **GPU**, **PCIe**, **Power**, **Fan**, そして**Temperature**が含まれます。
    - **Stress Test**を選択した場合、使用可能なアイテムは**Processor**、**Memory, Storage**。
- **デバイスリスト**
  - **タスクの結果**
    - :タスクが正常に実行されたデバイスの数。
    - :タスクが失敗したデバイスの数。
    - :不明な状態のデバイスの数。
  - **IP Address**:デバイスのIPアドレス。

- **Task Status**:デバイスの現在のタスクステータス。オプションには、**To Be Executed」、In Progress、Succeeded、Failed**および**Unknown**があります。
- **Succeeded Items**:正常に診断されたアイテムの数。
- **Failed Items**:診断に失敗したアイテムの数。
- **Canceled Items**:診断が取り消された、または実行されていない品目の数。
- **Time Consumed**:最新のタスク実行に消費された時間。
- **Details**:タスクに関する詳細情報。
  - タスクが正常に実行された場合は、レポートをダウンロードして情報を表示できます。
  - タスクが失敗した場合、このフィールドには失敗の原因が表示されます。

監視の構成

操作ログの表示

このタスクについて

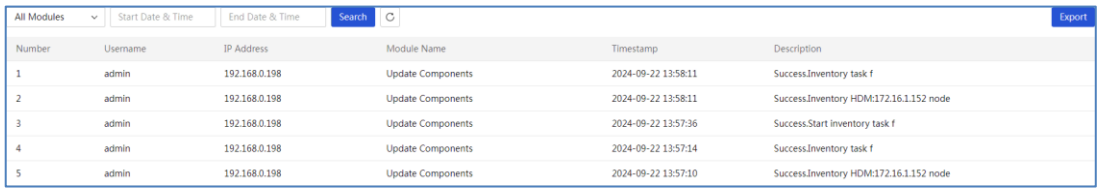
操作ログ機能は、ユーザーがUniSystem Webインタフェースで実行する操作をログに記録します。操作ログ情報には、操作ユーザー、操作タイムスタンプおよび操作結果が含まれます。フィルタを設定して、フィルタに一致する操作ログのみを表示できます。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Operation Logs**を選択します。

   Operation Logsページに、すべての操作ログが表示されます。

   図219 Operation Logsページ



2. 操作ログをフィルタリングするには、フィルタ項目を設定します。
   - ユーザーロールで操作ログをフィルタするには、ロールを選択します。
   - 操作ログをモジュールでフィルタするには、モジュールを選択します。
   - 操作ログを時間でフィルタするには、時間範囲を選択します。
3. Searchをクリックします。このページには、指定したすべてのフィルタ項目に一致する操作ログのみが表示されます。
4. 検索基準をクリアしてすべてのログを表示するには、をクリックします。
5. すべての操作ログをCSV形式でデバイスにダウンロードするには、**Export**をクリックします。

アラーム転送の設定

このモジュールでは、次のタスクを実行して、管理対象サーバーの動作ステータスを監視できます。

- サーバーイベントログを指定した受信者に電子メールで送信します。
- 管理対象サーバーからのSNMPトラップを受信し、指定されたホストにトラップを送信します。
- UniSystemは、WeCom、SMS、およびボイスメッセージを介して、管理対象サーバーのSNMPトラップをユーザーに送信することをサポートしています。

メモ:

この機能を使用するには、最初にHDMサーバーノードをUniSystemに追加する必要があります。詳細は、「サーバーの管理」を参照してください。

リスニング設定の構成

このタスクについて

ユーザーがサーバーステータスを監視できるように、管理対象サーバーから送信されるSNMPトラップを受信するには、次の作業を実行します。

UniSystemは、サーバーがSNMPトラップをUniSystemに送信するように、リスニング設定をすべての管理対象サーバーに適用します。次に、UniSystemは、受信したすべてのSNMPトラップを**Activity Logs**ページに記録します。

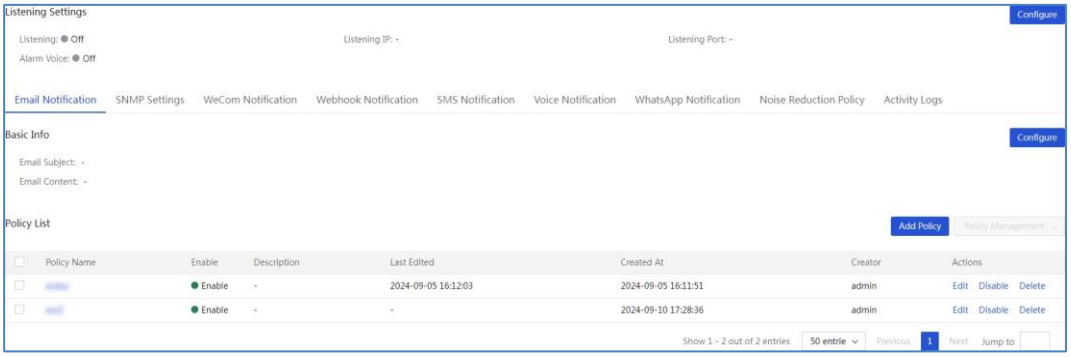
制約事項とガイドライン

- リスニングIPアドレスが、管理対象サーバーのHDM IPアドレスと同じネットワークセグメントにあることを確認します。
- listen設定が管理対象サーバーのHDMで有効になるのは、HDMユーザーが管理者ユーザーの役割を持っている場合のみです。
- アラーム音機能を有効にすると、現在のアラーム音が終了する前に新しいアラームが発生しても、音声は再度トリガーされません。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。

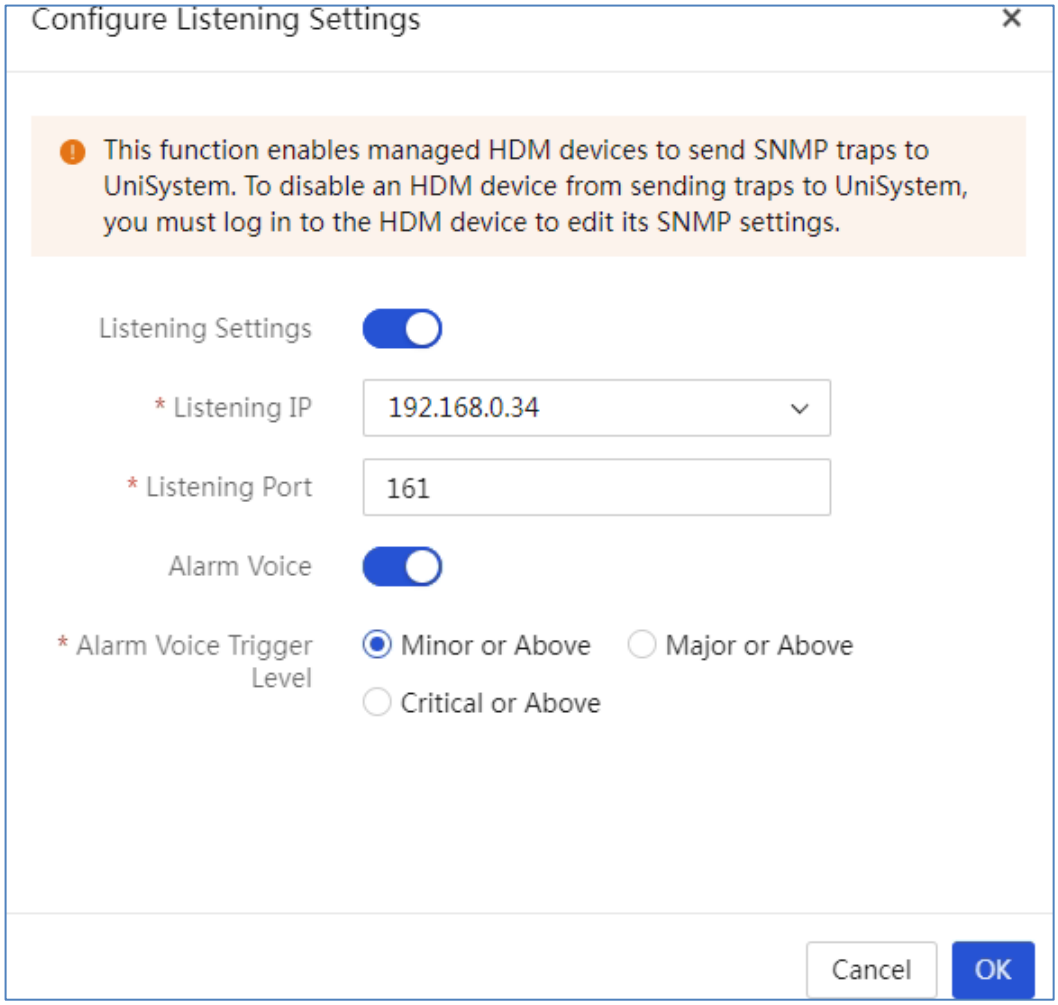
   図220 Alarm Forwardingページ



2. **Listening Settings**セクションで**Configure**をクリックします。表示されたダイアログボックスで、次の手順を実行します。
   a. **Listening Settings**で**On**を選択します。
   b. リスニングIPアドレスを選択します。
   c. リスニングポート番号を設定します。
   d. アラーム音を有効にします。

e. アラーム音のトリガーレベルを選択します。

図221 リスニング設定の構成



3. **OK**をクリックします。
4. **Activity Logs**タブをクリックします。管理対象サーバーがUniSystemに送信したSNMPトラップを表示できます。
5. (任意)SNMPトラップサーバーの指定されたIPアドレスはHDMの**Configuration** > **Alarm Settings** > **SNMP trap**ページ

パラメータ

- **Listening Port:**アラーム通知を受信するローカルホストのポート番号。ポート番号の範囲は1から65535です。
- **Listening IP**:サーバーからアラーム通知を受信するローカルホストのIPアドレス。統合O&MバージョンのUniSystemの場合は、サーバーからアラーム通知を受信するために使用するU-Centerノースバウンド仮想IPアドレスを入力します。
- **Alarm Voice**:アラーム音声を有効または無効にします。この機能は、CDU5204テンプレートのアラームを除く、サーバーラームとインフラストラクチャアラームをサポートします。UniSystemは、指定された重大度レベルのアラームを受信すると、アラーム音声をトリガーします。アラーム音声は、トリガーされるたびに5秒間隔で3回連続して鳴り、合計約12秒かかります。
- **Alarm Voice Trigger Level:**アラーム音声をトリガーできるアラーム重大度。

電子メール通知を構成する

このタスクについて

次の機能を実装するには、このタスクを実行します。

- 管理対象サーバーのイベントログを関係するユーザーに送信して、サーバーの動作ステータスを監視します。
- 管理対象サーバーのヘルスステータスを監視し、関係するユーザーにアラーム電子メールを送信して、ヘルスの変化を通知します。

前提条件

- 完全なSMTP構成。詳細については、「SMTP構成」を参照してください。
- UniSystemサーバーがアラーム電子メールを正しく送信するには、アラームリスニング機能を有効にし、リスニングIPアドレスとリスニングポート番号を設定します。詳細については、「リスニング設定の構成」を参照してください。

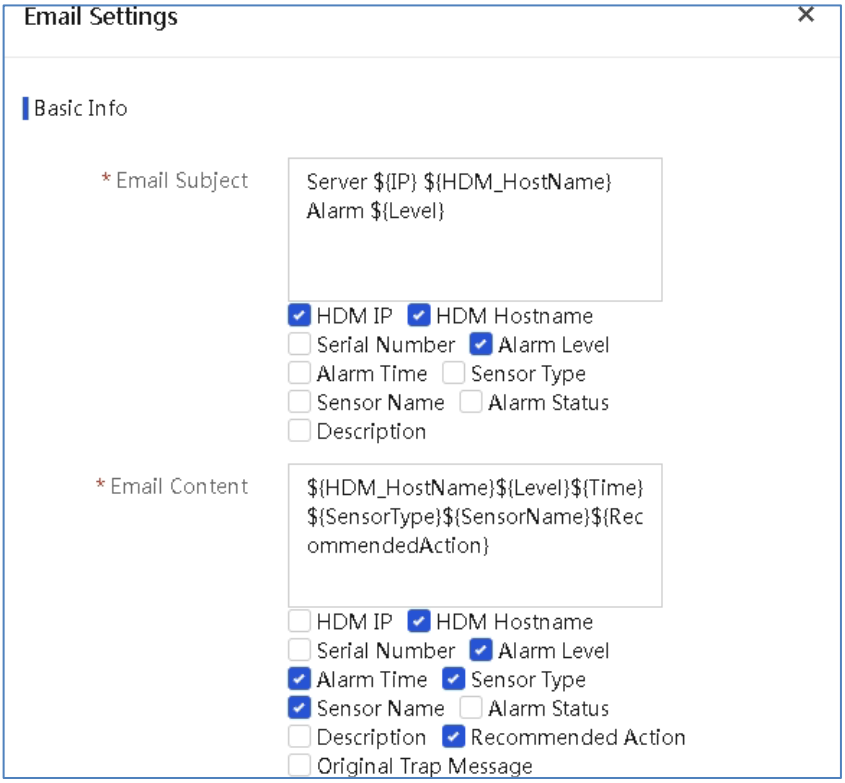
制約事項とガイドライン

- UniSystemは、監視機能が有効になっている場合にのみ、サーバーによって生成されたイベントログを受信できます。
- 次のいずれかのシナリオでは、サーバーがイベントログを生成した後に、ターゲットメールボックスがアラーム電子メールを受信する場合があります。
  - 監視機能が有効な場合、生成されるログの重大度は、アラーム通知の重大度と同じになります。
  - 監視機能を無効にすると、サーバーのヘルス状態が変更され、変更後のヘルス状態レベルがアラーム通知の重大度以上になります。
- アラーム通知の重大度がHDMで設定されている場合、UniSystem SMTP設定で設定されているアラーム通知の重大度によって、HDM設定に基づいてアラームメッセージがフィルタリングされます。

手順

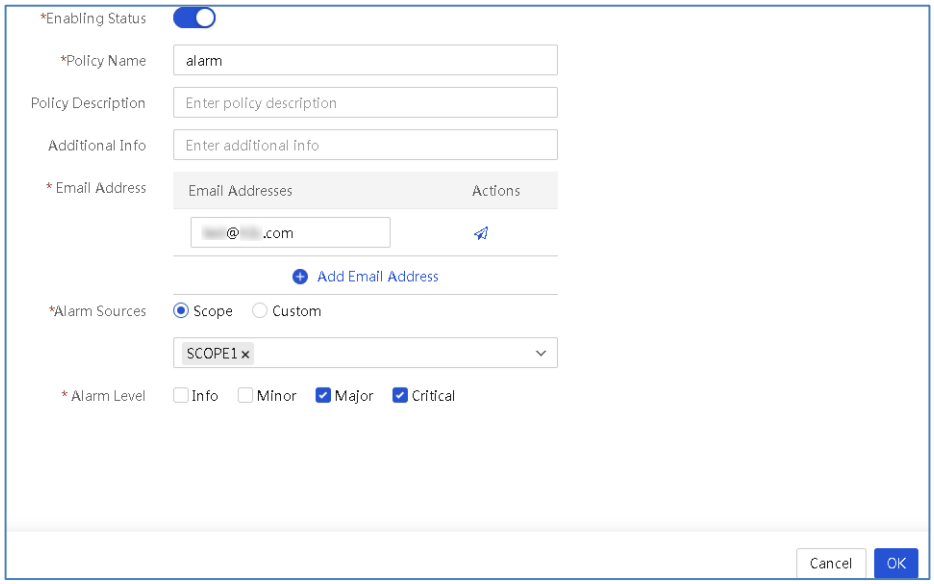
1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **Email Notification**タブをクリックします。
3. **Configure**をクリックします。表示されたダイアログボックスで、電子メールの件名と内容を入力し**OK**をクリックします。

図222 アラーム通知の設定



4. **Policy List**セクションで**Add Policy**をクリックします。表示されるダイアログボックスで、次のタスクを実行します。
   a. **Enabling Status**を選択し、ポリシー名、説明、および追加情報を入力します。
   b. 1つ以上の有効な電子メールアドレスを入力します。次に、をクリックしてテストアラーム電子メールを送信します。電子メールアドレスが重複していないことを確認してください。
   c. 次のいずれかのオプションを使用して、アラームソースを選択します。
      – **Scope**:このオプションを選択した場合は、ソースデバイスが属するスコープを選択します。複数のスコープを選択できます。
      – **Custom**:このオプションを選択した場合は、デバイスリストからソースデバイスを選択します。
   d. アラームレベルを選択します。
   e. **OK**をクリックします。

図223 ポリシーの追加



5. 特定のポリシーを編集、無効化、または削除するには、そのポリシーの**Actions**カラムで**Edit**, **Disable**, または**Delete**をクリックします。
6. 複数のポリシーを有効化、無効化、または削除するには、ポリシーを選択し、電源管理ドロップダウンリストで**Enable**, **Disable**, または**Delete**をクリックします。

パラメータ

- 電子メールの件名:サポートされている変数は次のとおりです。
  - **${IP}**:サーバーのHDM IPアドレス。
  - **${HDM_HostName}**:HDMホスト名。
  - **${SN}**:サーバーのシリアル番号。
  - **${Level}**:アラームの重大度。
  - **${Time}**:アラーム生成時刻。
  - **${SensorType}**:センサーのタイプ。
  - **${SensorName}**:センサー名。
  - **${AlertStatus}**:アラームステータス(トリガーおよびクリアを含む)。
  - **${Description}:**アラームの説明。
- 電子メールの内容:サポートされる変数は次のとおりです。
  - **${IP}**:サーバーのHDM IPアドレス。
  - **${HDM_HostName}**:HDMホスト名。
  - **${SN}**:サーバーのシリアル番号。
  - **${Level}**:アラームの重大度。
  - **${Time}**:アラーム生成時刻。
  - **${SensorType}**:センサーのタイプ。
  - **${SensorName}**:センサー名。
  - **${AlertStatus}:**アラームステータス(トリガーおよびクリアを含む)。
  - **${Description}**:アラームの説明。
  - **${RecommendedAction}**:推奨を処理します。

- **${TrapMessage}**:生のトラップメッセージ。

- **Policy Name**: UniSystemアラーム電子メールを転送するためのポリシーの名前。
- **Description**:UniSystemアラーム電子メールを転送するためのポリシーの説明。
- **Additional Info**:電子メールの最後に添付されている追加情報。
- **Email Address**:サーバーで生成されたアラームメッセージを受信するための電子メールアドレス。電子メールアドレスは繰り返し構成できません。
- **Alarm Sources**:アラーム電子メールを送信する送信元サーバー。
  - Range:ソースデバイスを選択する方法。
    - **Scope**を選択した場合、このフィールドには通知ポリシーが有効になるスコープが表示されます。
    - **Custom**が選択されている場合、このフィールドにはアラーム電子メールを送信する送信元サーバーが表示されます。
- **Alarm Level**:オプションには、HDMイベントログのアラーム重大度レベルに対応するInfo、Minor、Major、およびCriticalがあります。

SNMP設定の構成

このタスクについて

この機能は、UniSystem 2.00.17以降で使用できます。

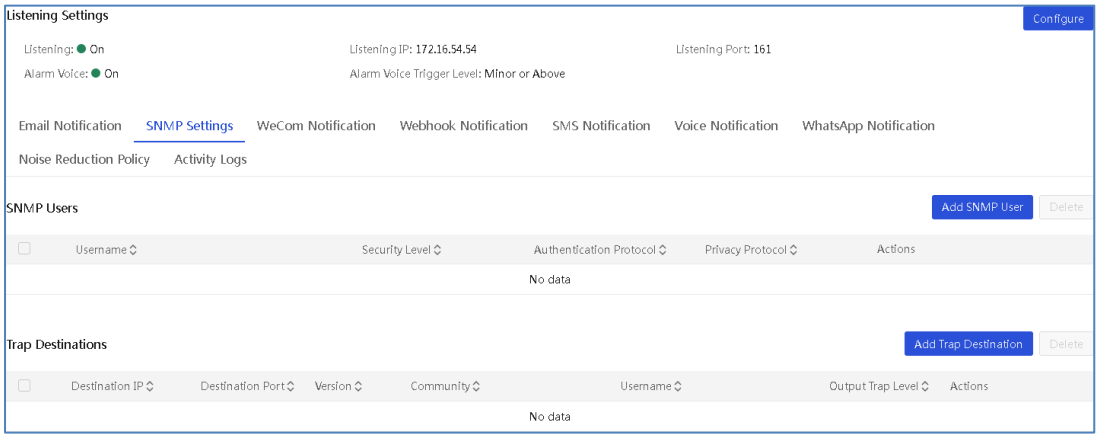
管理対象サーバーからSNMPトラップ(トラップ送信先)を受信するSNMPユーザーおよびターゲットホストを追加するには、次のタスクを実行します。

UniSystemは、指定されたレベル以上の重大度レベルを持つSNMPトラップを管理対象サーバーから受信し、そのトラップをターゲットトラップホストに転送します。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **SNMP Settings**タブをクリックします。

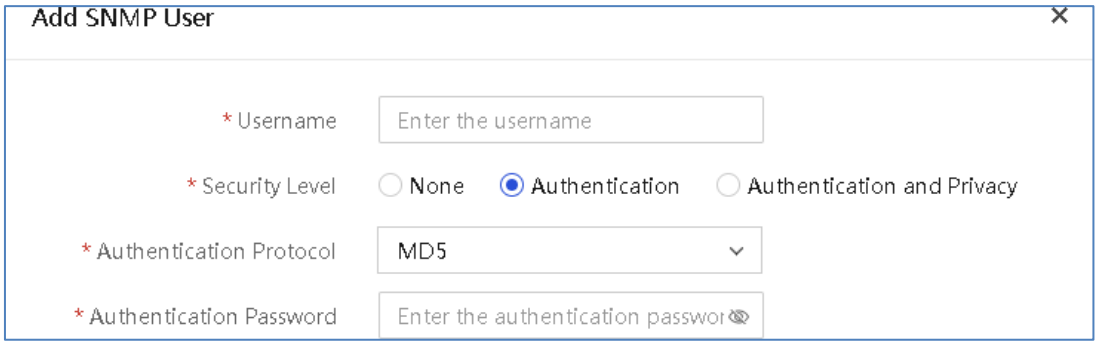
   図224 SNMP設定ページ



3. (任意)SNMPv3トラップを送信するには、**Add SNMP User**をクリックして、次のようにSNMPユーザーを追加します。
   a. ユーザー名を入力します。
   b. セキュリティレベルを選択します。

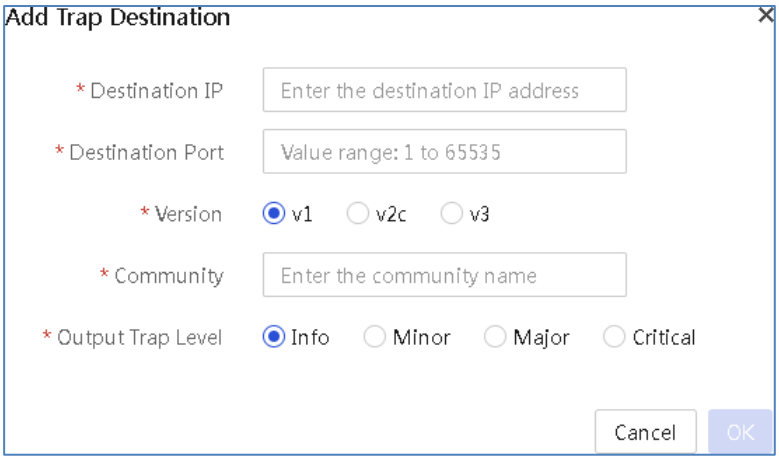
c. ユーザーの認証プロトコルを選択します。
d. ユーザーの認証パスワードを入力します。
e. **OK**をクリックします。

図225 SNMPユーザーの追加



4. **Add Trap Destination**をクリックし、次のようにトラップの宛先を設定します。
   a. 宛先IPアドレスを入力します。
   b. 宛先ポート番号を入力します。デフォルトの宛先ポート番号は162です。
   c. SNMPバージョンを選択します。
   d. コミュニティに入ります。
   e. 出力トラップレベルを選択します。

図226 トラップ送信先の追加



5. **OK**をクリックします。
6. (任意)テストアラームメッセージをトラップ送信先に送信するには、トラップ宛先**Actions**列で**Test**をクリックします。

WeCom通知の設定

このタスクについて

この機能は、バージョン2.34以降で使用できます。

WeCom通知を設定するには、次の作業を実行します。この機能を有効にすると、管理対象サーバーのSNMPトラップが、指定したWeComアプリケーションに送信されます。

制約事項とガイドライン

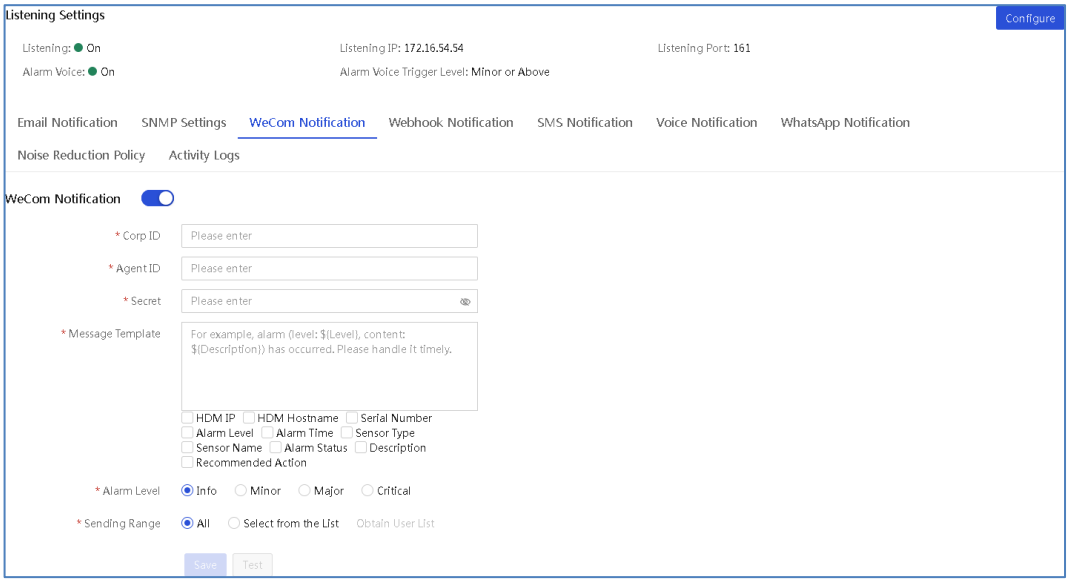
WeComパラメータを取得できるのは、WeCom管理者のみです。WeComパラメータを取得するには、API関連のWeComドキュメントを参照してください。

この機能を使用するには、HTTPS経由でインターネットにアクセスする必要があります。必要に応じてDNSとプロキシを構成してください。詳細については、「DNS情報を表示する」および「プロキシ設定を構成する」を参照してください。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **WeCom Notification**タブをクリックします。

図227 WeCom通知の設定



3. WeCom通知を有効にし、必要なパラメータを入力して、**Save**をクリックします。
4. (任意)**Test**をクリックして、指定したWeComアプリケーションに通知を送信できるかどうかをテストします。

パラメータ

- **WeCom Notification**: WeChat通知を有効または無効にします。
- **Corp ID**: 企業のWeCom corpid。各企業には一意のWeCom corpidがあります。corpidを取得するには、管理者としてmanagement backendの**My Company** > **Company Information**にアクセスします。
- **Agent ID**: WeCom agentid。各アプリケーションには一意のagentidがあります。agentidを取得するには、管理者としてmanagement backendの**App Management** > **Apps**にアクセスし、ターゲットアプリケーションプログラムをクリックします。
- Secret: WeComシークレット。データセキュリティを確保するためにエンタープライズアプリケーションで使用されるキーです。各アプリケーションには、一意のアクセスキーがあります。データセキュリティのため、シークレットは公開しないでください。シークレットを取得するには、管理者として管理バックエンドの**App Management** > **Apps**にアクセスし、ターゲットアプリケーションプログラムをクリックします。
- **Message Template**:アラームメッセージの内容をカスタマイズします。次の変数がサポートされています。これらの変数は、最終的に表示されるときに、実際の情報内のそのフィールドの内容に置き換えられます。

- **${IP}**:サーバーのHDM IPアドレス。
- **${HDM_HostName}**:HDMホスト名。
- **${SN}**:サーバーのシリアル番号。
- **${Level}**:アラームの重大度。
- **${Time}**:アラーム生成時刻。
- **${SensorType}**:センサーのタイプ。
- **${SensorName}**:センサー名。
- **${AlertStatus}**:アラームステータス(トリガーおよびクリアを含む)。
- **${Description}**:アラームの説明。
- ${**RecommendedAction}**:推奨を処理します。

- **Alarm Level**:オプションには、Info、Minor、Major、およびCriticalがあります。UniSystemは、上記の選択された重大度のアラームのみを転送します。
- **Sending Range**:アラームメッセージを表示できるWeComユーザー。**Obtain User List**をクリックして、WeComバックエンドの可視性範囲設定からユーザーリストを取得し、アラームメッセージを表示できるユーザーをさらにフィルタリングします。

webhook通知を構成する

メモ:

- 統合O&MバージョンのUniSystemでは、この機能はサポートされていません。
- この機能は、2.65以降のバージョンでサポートされています。

この機能について

この機能を使用して、WeComグループチャットボット通知を設定します。この機能を設定して有効にすると、管理対象サーバーから特定のWeComグループチャットにSNMPトラップメッセージを送信できます。

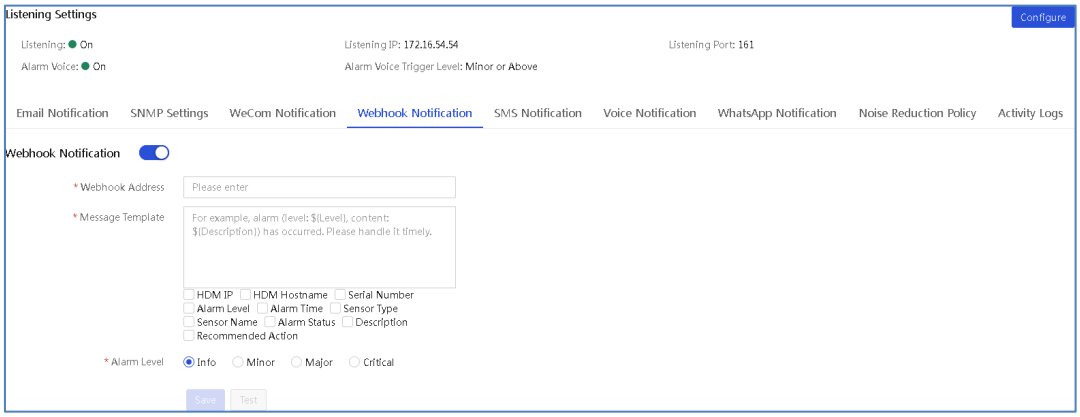
制約事項とガイドライン

- WeCom webhookアドレスに関連するパラメータを取得するには、WeComグループチャットが必要です。詳細については、「WeCom chatrobの構成」を参照してください。
- この機能を使用するには、HTTPS経由でインターネットにアクセスする必要があります。必要に応じて、DNSおよびプロキシサーバーを構成します。詳細は、「DNS情報の表示」および「プロキシ設定の構成」を参照してください。

手順

1. **Menu** > **Monitor** > **Alarm Forwarding**の順に選択し、**webhook Notification**タブをクリックします。

図228 webhookの通知



2. webhook通知をイネーブルにし、関連情報を入力して、**Save**をクリックします。
3. (任意)**Test**をクリックして、現在設定されているWeComグループチャットにテストアラームメッセージを送信します。

パラメータ

- **webhook Notification**: webhook通知をイネーブルまたはディセーブルにします。
- **Webhook Address**: WeComグループチャットボットの一意のwebhookアドレス。
  - モバイルクライアントを使用している管理者がwebhookアドレスを取得するには、グループチャットの右上隅にある3つの点をクリックし、Group Chatbotをクリックして、対応するロボットをクリックします。
  - パソコンを使用している管理者の場合、webhookアドレスを取得するには、グループチャットリストにアクセスし、対応するロボットを右クリックして詳細を表示します。
- **Message Template**: アラームメッセージの内容をカスタマイズします。次の変数がサポートされています。これらの変数は、最終的に表示されるときに、実際の情報内のそのフィールドの内容に置き換えられます。
  - **${IP}**:サーバーのHDM IPアドレス。
  - **${HDM_HostName}**:HDMホスト名。
  - **${SN}**:サーバーのシリアル番号。
  - **${Level}**:アラームの重大度。
  - **${Time}**:アラーム生成時刻。
  - **${SensorType}**:センサーのタイプ。
  - **${SensorName}**:センサー名。
  - **${AlertStatus}:**アラームステータス(トリガーおよびクリアを含む)。
  - **${Description}**:アラームの説明。
  - **${RecommendedAction}:**推奨を処理します。
- **Alarm Level**: オプションには、Info、Minor、Major、およびCriticalがあります。UniSystemは、上記の選択された重大度のアラームのみを転送します。

SMS通知を構成する

このタスクについて

この機能は、バージョン2.34以降で使用できます。

SMS通知を設定するには、次の作業を実行します。この機能を有効にすると、管理対象サーバー

のSNMPトラップがSMSを介して指定した受信者に送信されます。

現在のソフトウェアバージョンでは、Emayのみがサポートされています。SMSサービスの内容については、Emayにお問い合わせください。Emayでは、中国本土のSMSは、香港、マカオ、台湾、中国、およびその他の国または地域で提供されているSMSとは異なるサービスに属しています。異なるサービスの顧客IDを混在させないでください。その他の機能については、Emayカスタマーサービスにお問い合わせください。

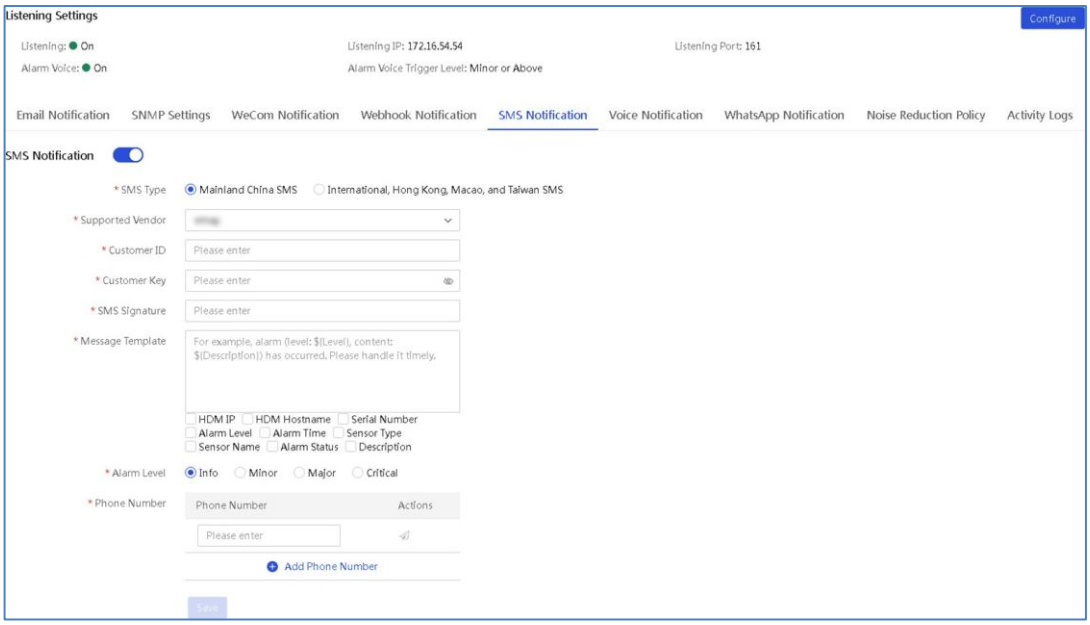
制約事項とガイドライン

この機能を使用するには、HTTPS経由でインターネットにアクセスする必要があります。必要に応じてDNSとプロキシを構成してください。詳細については、「DNS情報を表示する」および「プロキシ設定を構成する」を参照してください。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **SMS Notification**タブをクリックします。

   図229 SMS通知の設定



3. SMS通知を有効にし、必要なパラメータを入力します。
4. **Add Phone Number**をクリックし、電話番号を入力します。
5. (オプション)電話番号のアイコンをクリックして、その電話番号にSMS通知を送信できるかどうかをテストします。
6. (オプション)SMS通知を受信する電話番号を削除するには、電話番号のアイコンをクリックします。
7. **Save**をクリックします。

音声通知を設定する

このタスクについて

この機能は、バージョン2.34以降で使用できます。

音声通知を設定するには、次の作業を実行します。この機能をイネーブルにすると、管理対象サーバーのSNMPトラップがボイスメッセージを介して送信されます。

制約事項とガイドライン

ボイスメッセージを正常に送信するには、この機能を使用する前に、Emayにボイスメッセージテンプレートを通知します。詳細については、Emayカスタマーサービスにお問い合わせください。

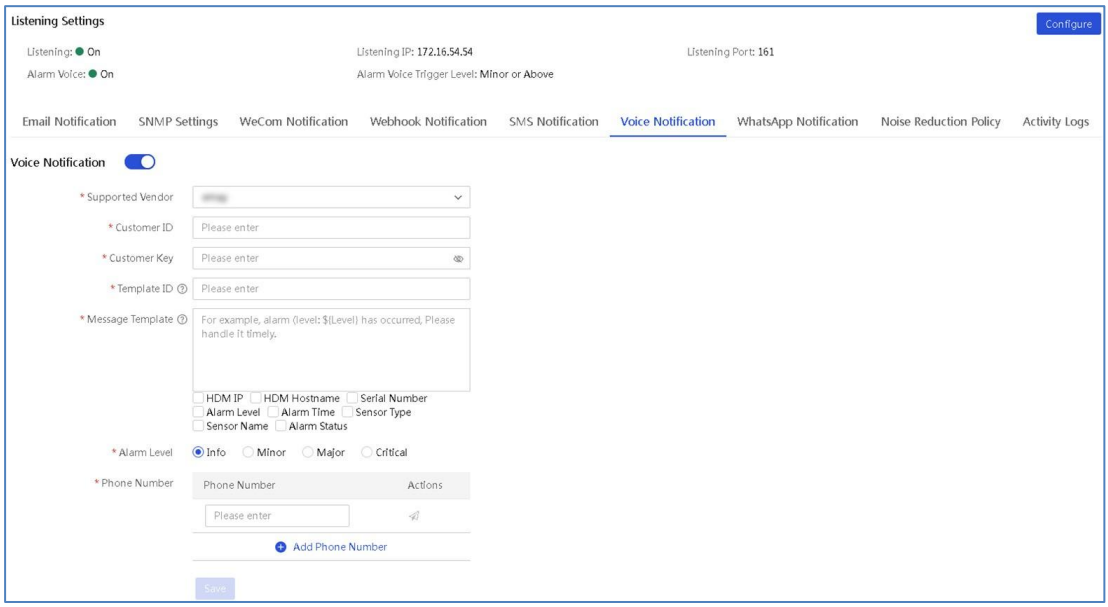
この機能を使用するには、HTTPS経由でインターネットにアクセスする必要があります。必要に応じてDNSとプロキシを構成してください。詳細については、「DNS情報を表示する」および「プロキシ設定を構成する」を参照してください。

ボイスメッセージテンプレートを編集するには、更新されたテンプレートをEmayに通知し、新しいテンプレートIDを取得します。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **Voice Notification**タブをクリックします。

   図230 音声通知の設定



3. 音声通知を有効にし、必要なパラメータを入力します。
4. **Add Phone Number**をクリックし、電話番号を入力します。
5. (任意)電話番号のアイコンをクリックして、その電話番号に音声通知を送信できるかどうかをテストします。
6. (任意)音声通知を受信する電話番号を削除するには、電話番号のアイコンをクリックします。
7. **Save**をクリックします。

WhatsApp通知を設定する

この機能について

WhatsApp通知を設定するには、この機能を使用します。この機能を設定して有効にすると、管理対象サーバーから特定のWhatsAppアカウントにSNMPトラップメッセージを送信できます。

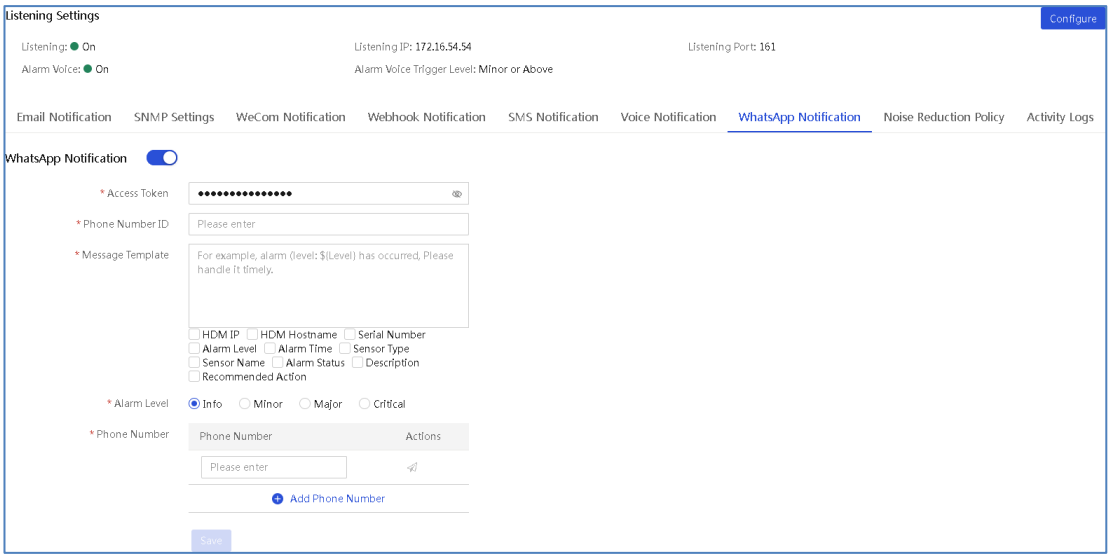
制約事項とガイドライン

- アクセストークンまたは電話番号IDを取得する場合、またはWhatsAppビジネスAPIを設定する場合は、テクニカルサポートにお問い合わせください。
- この機能を使用するには、HTTPS経由でインターネットにアクセスする必要があります。必要に応じて、DNSおよびプロキシサーバーを構成します。詳細は、「DNS情報の表示」および「プロキシ設定の構成」を参照してください。

手順

1. **Menu** > **Monitor** > **Alarm Forwarding**を選択し、**WhatsApp Notification**タブをクリックします。

   図231 WhatsAppの通知



2. WhatsApp通知を有効にし、関連情報を入力して**Save**をクリックします。
3. (任意)アイコンをクリックして、現在設定されているWhatsAppアカウントにテストアラームメッセージを送信します。

パラメータ

- **WhatsApp Notification**: WhatsApp通知を有効または無効にします。
- **Access Token**:アクセストークンは、WhatsApp Business APIへのアクセスを許可するために使用されるセキュリティ認証情報です。これは、APIリクエストの検証と許可に使用される長期的に有効なトークンです。アクセストークンを使用することで、APIクライアントはWhatsAppにリクエストを送信し、さまざまなアクションを実行できます。
- **Phone Number ID**: WhatsApp Business APIでは、APIリクエストと操作での識別と認識のために、登録された各電話番号に一意の電話番号IDが割り当てられます。
- **Message Template**::アラームメッセージの内容をカスタマイズします。次の変数がサポートされています。これらの変数は、最終的に表示されるときに、実際の情報内のそのフィールドの内容に置き換えられます。
  - **${IP}**:サーバーのHDM IPアドレス。
  - **${HDM_HostName}**:HDMホスト名。
  - **${SN}**:サーバーのシリアル番号。
  - **${Level}**:アラームの重大度。
  - **${Time}**:アラーム生成時刻。
  - **${SensorType}**:センサーのタイプ。

- **${SensorName}**:センサー名。
- **${AlertStatus}:**アラームステータス。トリガーされ、クリアされました。
- **${Description}**:アラームの説明。
- **${RecommendedAction}**:推奨を処理します。

- **Alarm Level**:オプションには、Info、Minor、Major、およびCriticalがあります。UniSystemは、上記の選択された重大度のアラームのみを転送します。
- **Phone Number**:受信者の国際電話番号。プラス記号(+)は不要ですが、番号には国(または地域)コードを含める必要があります。

ノイズ低減ポリシーを設定する

この機能について

ノイズリダクションポリシーが設定されている場合、UniSystemは、アラームのトリガー数がノイズリダクションしきい値に達した場合にのみ、アラームメッセージを転送し、アクティビティをログに記録します。

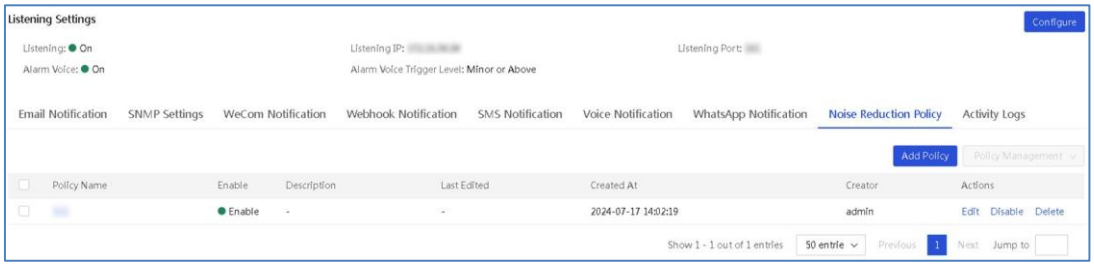
制約事項とガイドライン

アラーム転送に影響を与えることができるのは、有効になっているノイズ削減ポリシーのみです。UniSystemは、アラームのトリガー数がノイズ削減しきい値に達した後にのみアラームメッセージを転送するため、アラーム通知の数が減ります。

手順

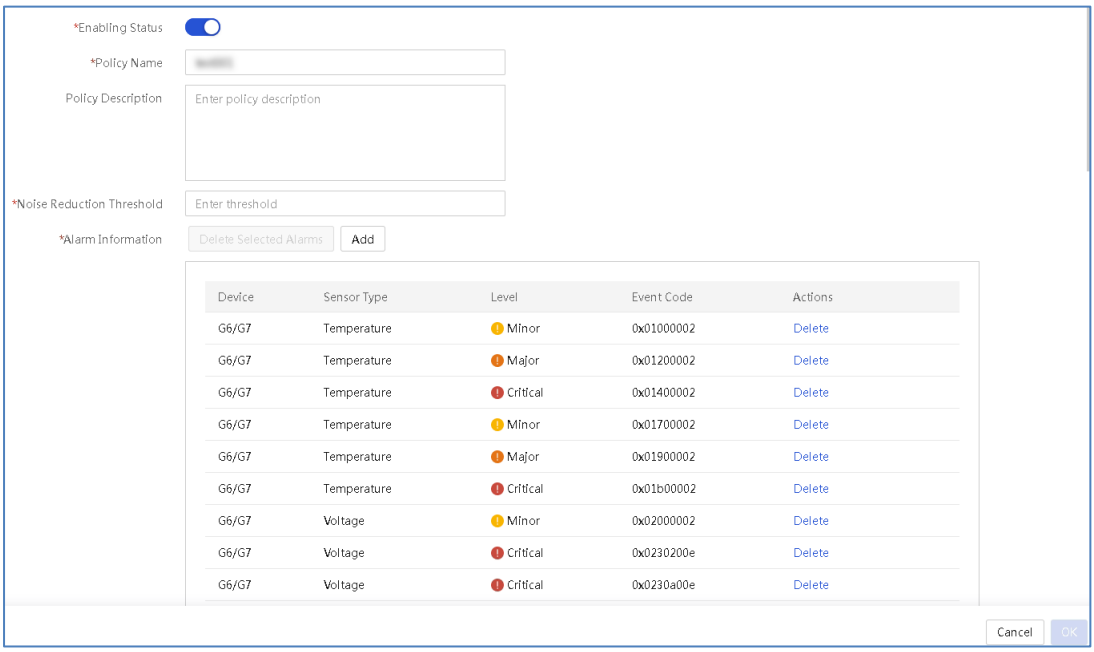
1. **Menu** > **Monitor**> **Alarm Forwarding**を選択します。
2. **Noise Reduction Policy**タブをクリックします。

   図232 騒音低減方針



3. **Add Policy**をクリックし、ダイアログボックスに次の情報を入力します。

図233 ポリシーの追加



a. このポリシーを有効にします。
b. ポリシー名とポリシーの説明を入力します。
c. ノイズ低減しきい値を入力します。
d. **Add**をクリックします。アラーム情報を選択します。
   - **G3/G5 Devices**タブで、Alarm information for G3/G5 devicesを選択し**OK**をクリックします。
   - **G6/G7 Devices**タブで、G6/G7デバイスのアラーム情報を選択し**OK**をクリックします。

   アラームログでは、アラーム重大度、センサータイプ、および入力キーワードによるフィルタリングがサポートされているため、対応する情報をすばやく見つけることができます。

4. (任意)選択したアラームを削除する場合にクリックします。削除すると、他のポリシーに対して選択したアラームがクリアされます。
5. **OK**をクリックします。
6. 特定のポリシーを編集、有効化、無効化、または削除するには、ポリシーの**Actions**列で**Edit**, **Enable**, **Disable**, もしくは **Delete**をクリックします。
7. 複数のポリシーを有効化、無効化、または削除するには、ポリシーを選択し、**Enable Selected**, **Disable Selected**, or **Delete Selected**.をクリックします。

パラメータ

- **Policy Name**:UniSystemアラームノイズ低減ポリシーの名前。
- **Policy Description**:UniSystemアラームノイズ削減ポリシーの説明。
- **Noise Reduction Threshold**: UniSystemがアラームログを送信する前に到達する必要があるアラームログのトリガー数。たとえば、ノイズ削減のしきい値を5に設定すると、UniSystemは、ログが5回トリガーされた後にのみアラームログを転送します。
- **Alarm Type**:ノイズ削減ポリシーが有効になるアラームのタイプ。タイプが一致しないログの場合、UniSystemは転送設定で定義されているアクティビティを転送して記録します。

アクティビティログの表示

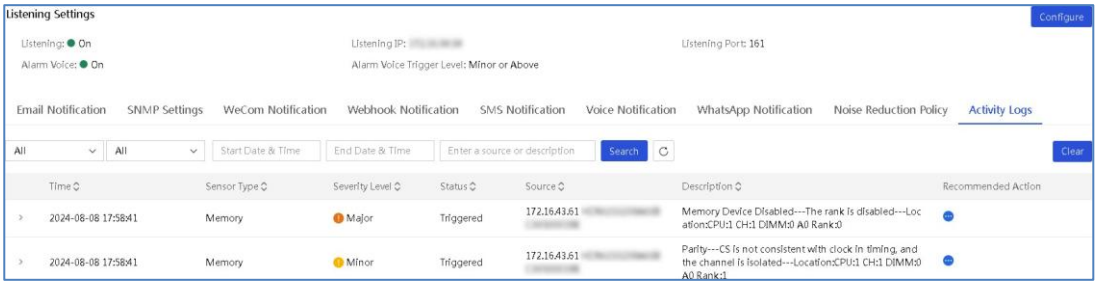
このタスクについて

このモジュールを使用すると、管理対象HDMサーバーノードによってUniSystemに送信されたSNMPトラップを表示できます。UniSystemホストは、アラームリスニング機能が有効になっている場合にのみSNMPトラップを受信できます。

手順

1. ナビゲーションペインで、**Menu** > **Monitor** > **Alarm Forwarding**を選択します。
2. **Activity Logs**タブをクリックします。このページには、UniSystemが受信したすべてのSNMPトラップが表示されます。
3. SNMPトラップをフィルタリングするには、重大度、時間範囲、またはその両方を選択するか、検索ボックスに送信元または説明を入力します。

   図234 SNMPトラップのフィルタリング



4. **Search**をクリックします。このページには、フィルタ条件に一致するSNMPトラップのみが表示されます。

故障予知

メモ:

- この機能は、G6以降のサーバーでのみ使用でき、サーバーにはサーバーソフトウェアライセンスがインストールされている必要があります。
- ドライブ予測は、SATA HDDのみをサポートします。

ドライブ予測

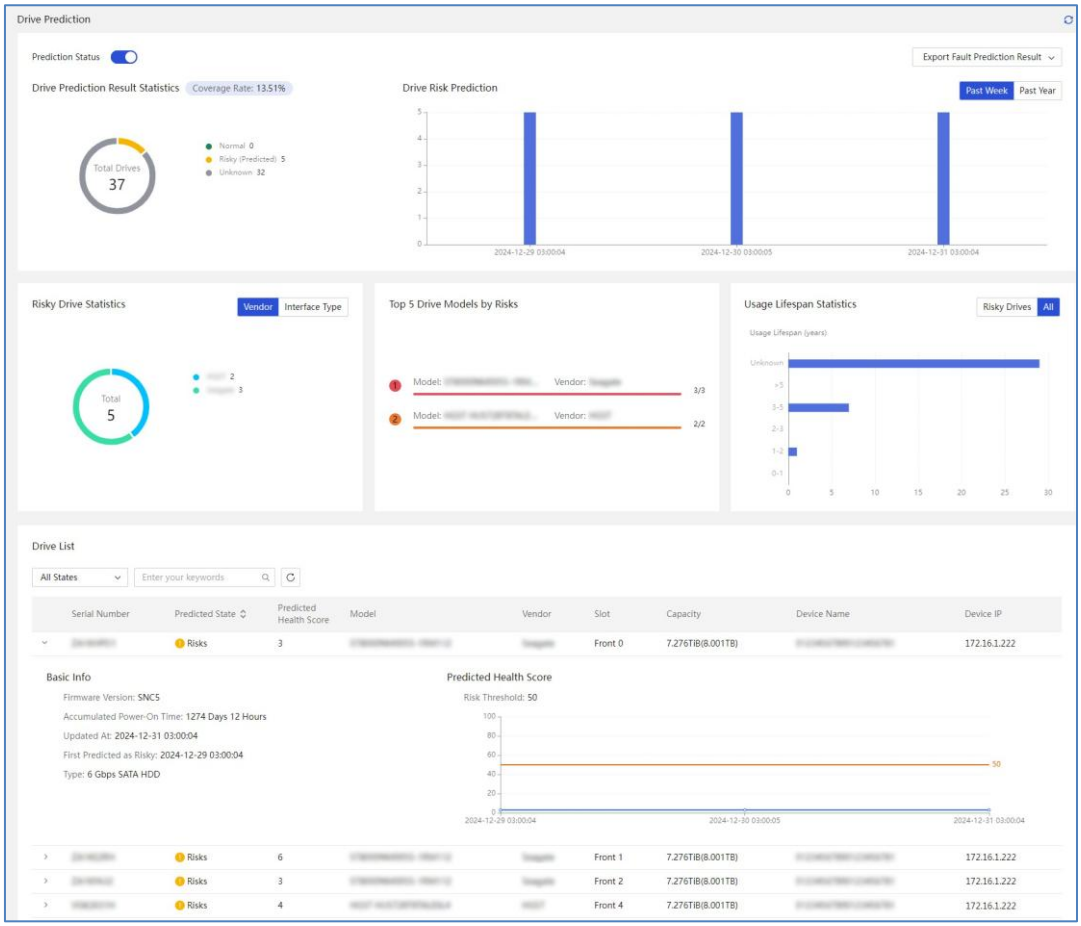
ドライブの数が多く、データストレージの容量が大きく、ドライブのライフサイクルが短いため、データセンターではドライブ障害が頻繁に発生します。ドライブは、他のサーバーコンポーネントと比較して障害発生率が高くなります。UniSystemは、ドライブからのS.M.A.R.T. データを調査し、データ分析と特徴抽出を利用して、潜在的なドライブ障害を予測し、その結果を提示します。ドライブのリスクに関する情報を常に入手できます。この機能は、ドライブ障害によって通常の運用が中断されるのを防ぐのに役立ちます。

手順

1. ナビゲーションペインで、**Menu** > **Fault Prediction** > **Drive Prediction**を選択します。
2. ドライブ予測機能を有効にします。

3. ドライブ予測結果の統計情報を表示します。

図235ドライブ予測結果の統計情報の表示



4. (オプション)予測結果をエクスポートします。
5. **Export Analysis Result**をクリックします。ターゲットドライブタイプに関する情報をエクスポートするには、**All Drives**、**Normal Drives**、**Risky(Predicted)Drive**または**Unknown Drive**。

説明

- **Drive Prediction Result Statistics**:正常なドライブ、危険な(予測される)ドライブ、および不明なドライブの数と、予測される状態別のドライブ構成を表示します。
  - **Normal**:潜在的なリスクのないドライブ。
  - **Risky (Predicted)**:潜在的なリスクがあるドライブ。
  - **Unknown**:ドライブのヘルスステータスが予測できません。次のような理由が考えられます。
    - サーバーはこの機能をサポートしていません。サーバーのモデルがG6より前です。
    - サーバーにライセンスがインストールされていない。
    - ドライブはSATA HDDではない。
    - 7日間連続してドライブデータを取得できない。
- **Drive Risk Prediction**: 過去1週間または1年間の期間ごとのリスクのあるドライブ数が表示されます。バーにカーソルを置くと、特定の期間のリスクドライブ情報が表示されます。
  - **Serial Number**:ドライブのシリアル番号。
  - **Vendor**:ドライブの製造元。

    - **Model**:ドライブモデル。
    - **First Predicted as Risky**: ドライブに潜在的なリスクがあると最初に予測された時刻。
    - **Presence**: ドライブのプレゼンスステータス。
- **Risky Drive Statistics**:危険性があると予測されるドライブの現在の数が表示されます。統計は、製造元またはインターフェイスタイプ別に表示されます。
- **Top 5 Drive Models by Risks**:最もリスクの高い上位5ドライブモデルとその製造元が表示されます。
- **Usage Lifespan Statistics**:危険性のあるドライブまたはすべてのドライブの寿命に関する統計情報を表示します。
- **Drive List**: UniSystemによって管理されるすべてのドライブに関する情報を表示します。ページごとに表示されるエントリ数の設定、ドライブのフィルタ、およびターゲットドライブの検索を行うことができます。基本的なドライブ情報と過去1週間の健全性統計の折れ線グラフを表示するには、シリアル番号の先頭にある山形のアイコン >をクリックします。
    - **Serial Number**: ドライブのシリアル番号。
    - **Predicted State**: ドライブの予測される状態。
    - **Predicted Health Score**: ドライブの予測ヘルススコア。
    - **Vendor**: ドライブの製造元。
    - **Model**: ドライブモデル。
    - **Slot**: ドライブが存在するスロット。
    - **Capacity**: ドライブの容量。
    - **Device Name**: ドライブが存在するデバイスの名前。
    - **Device IP**:: ドライブが存在するデバイスのIPアドレス。
    - **Firmware Version**: ドライブのファームウェアバージョン。
    - **Accumulated Power-On Time**: ドライブの累積電源投入時間。
    - **Updated At**: ドライブ予測が更新された時刻。
    - **First Predicted as Risky**: ドライブに潜在的なリスクがあると最初に予測された時刻。
    - **Type**: ドライブのデータ転送速度とインターフェイスのタイプ。

電力効率と予測の管理(G6以降のサーバー)

仮想マシンバージョンのUniSystemのみがこの機能をサポートしています。

エネルギー効率統計

効率統計について

ユーザーは、この機能を使用して、日単位および月単位の消費電力、電力使用量、Uスペース使用量の統計、電力消費統計、上位5つの電力消費者、および上位5つのUスペース占有率を、データセンター、機器室、およびラックビューで表示できます。さらに、インテリジェントな予測アルゴリズムにより、個々のラック、機器室全体、およびデータセンター全体の消費電力予測を確認できます。

消費電力予測は、履歴データに基づいて実行されます。予測が生成された後にデータセンター内のデバイスに対して特定のアクションが実行されると、実際の消費電力が予測消費電力と大きく異なる場合や、システムが特定の期間の予測消費電力を取得できない場合があります。これは、デバイスの動作には影響しません。

重要:

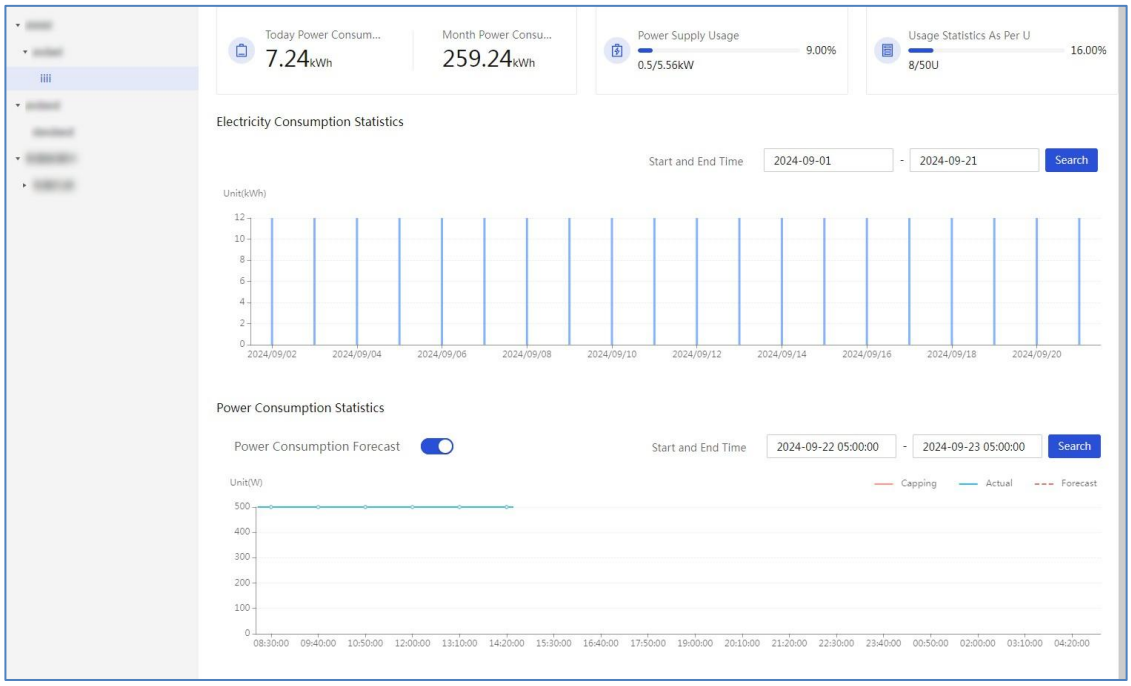
消費電力予測データは、次の両方の条件が満たされている場合にのみ表示できます。

- UniSystemによって取得された電力消費履歴データの日数が7日以上である。
- UniSystemによって取得された過去の消費電力データの量は、この期間の総データ量の理論値の70%以上です。

手順

1. ナビゲーションペインで、M **Menu** > **Energy and Prediction** > **Energy Efficiency Statistics**を選択します。
2. ナビゲーションペインからターゲットビューを選択します。
3. (任意)消費電力予測をイネーブルにするかどうかを選択します。
4. (オプション)開始時刻と終了時刻を指定し、**Search**をクリックします。

図236 電力効率性統計収集の有効化



エネルギー効率分析

このモジュールを使用すると、低負荷またはアイドル状態のサーバーを特定し、これらのサーバーに追加サービスを転送したり、これらのサーバーの電源をオフにしたりして、データセンター全体の消費電力を最適化できます。このモジュールは、NVIDIA GPUでのみ検出をサポートします。事前にNVIDIA GPUドライバーをインストールする必要があります。

この機能は、UniSystemがVM上で実行されている場合にのみ使用できます。

入口温度解析の設定

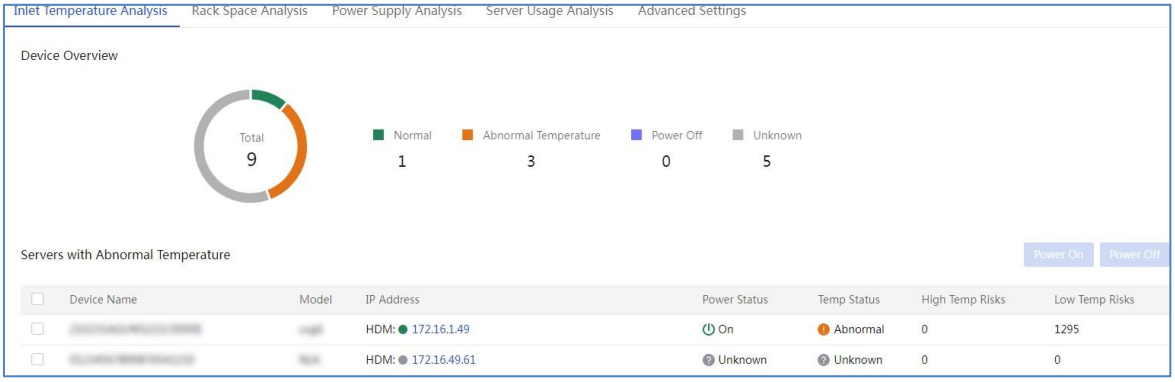
サーバー温度の概要情報を表示し、温度異常のあるサーバーを特定し、バッチでサーバーの電源をオン

またはオフにするには、次の作業を実行します。

入口温度情報の表示

1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **Energy Efficiency Analysis** >**Inlet Temperature Analysis**を選択します。
2. サーバーの吸気温度情報を表示します。

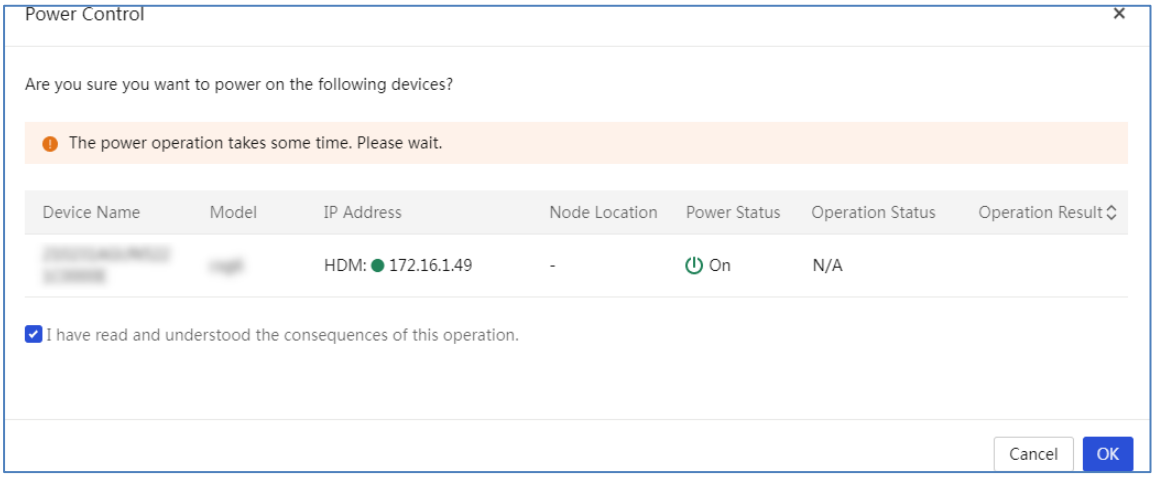
図237 入口温度解析



サーバーの電源を一括投入する

1. **Servers with Abnormal Temperature**リストからサーバーを選択します。
2. **Power On**をクリックします。表示されたダイアログボックスで、電源を入れるデバイスを確認し、操作結果の通知に同意して、**OK**をクリックします。

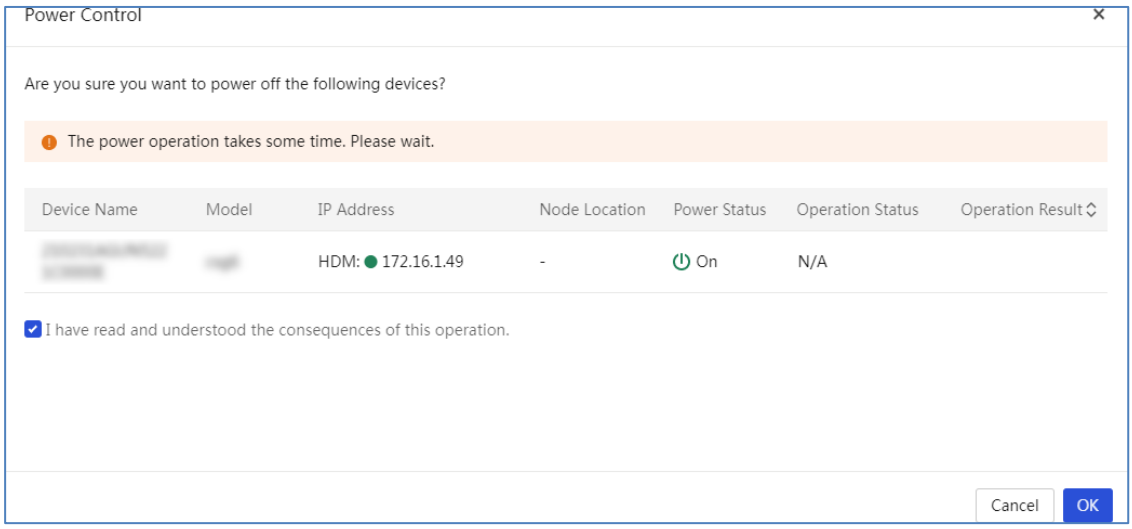
図238 サーバーのバッチ電源投入



サーバーの電源をバッチでオフにする

1. **Servers with Abnormal Temperature**リストからサーバーを選択します。
2. **Power Off**をクリックします。表示されたダイアログボックスで、電源をオフにするデバイスを確認し、操作結果の通知に同意して、**OK**をクリックします。

図239 バッチでのサーバーの電源切断



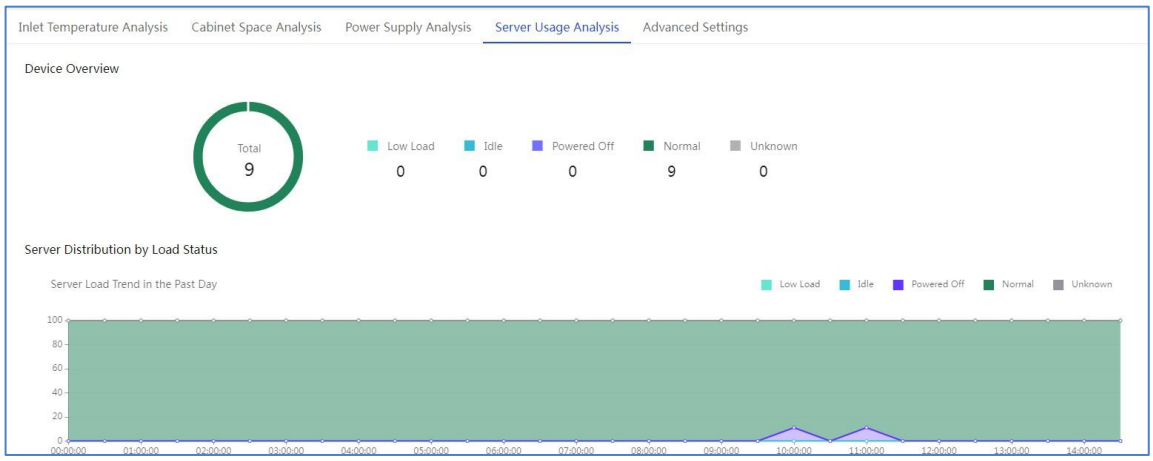
サーバー使用率分析の構成

このタスクを実行して、サーバーの概要情報、異常にロードされたサーバー、およびロードステータス別のサーバー分布を表示します。異常にロードされたサーバーのバッチでの電源オン/オフ、消費電力上限の構成、および過去1日のサーバー負荷の傾向の表示を行うことができます。

サーバーの使用状況情報を表示する

1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **Energy Efficiency Analysis** > **Server Usage Analysis**を選択します。
2. サーバーの使用情報を表示します。

図240 サーバー使用率の分析



サーバーの電源を一括投入する

1. 異常にロードされたサーバーのリストからサーバーを選択します。
2. **Power On**をクリックします。表示されたダイアログボックスで、電源を入れるデバイスを確認し、操作結果通知に同意して、**OK**をクリックします。

サーバーの電源をバッチでオフにする

1. 異常にロードされたサーバーのリストからサーバーを選択します。
2. **Power Off**をクリックします。表示されたダイアログボックスで、電源をオフにするデバイスを確認し、操作結果通知に同意して、**OK**をクリックします。

消費電力上限の設定

1. 異常にロードされたサーバーのリストからサーバーを選択します。
2. サーバーの**Power Cap Settings**をクリックします。消費電力上限パラメータを表示および構成します。
3. **OK**をクリックします。

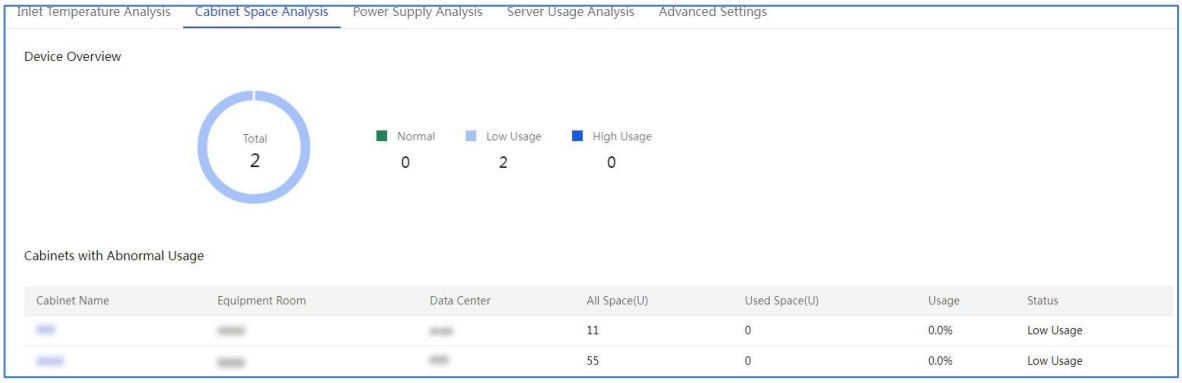
ラックスペースの分析

このモジュールでは、ラックスペースの使用状況に関する情報を表示できます。

手順

1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **Energy Efficiency Analysis**を選択します。
2. ラックスペース分析情報を表示します。

図241 ラックスペース分析の表示



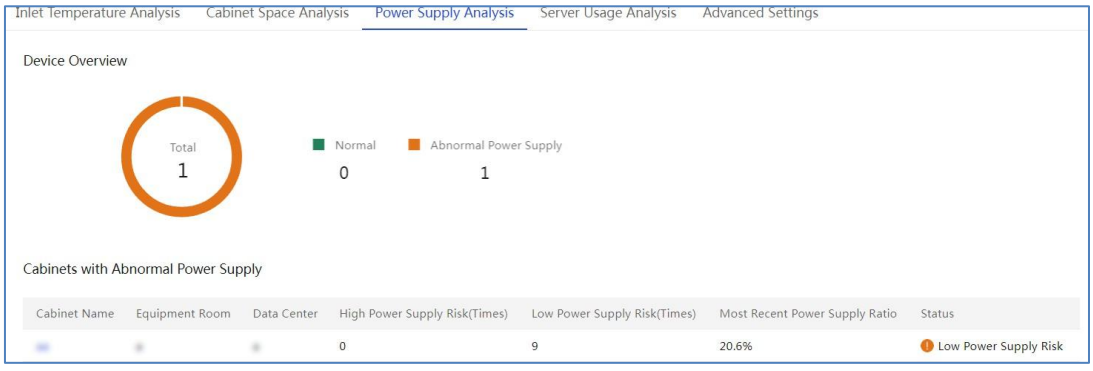
電源解析

このモジュールでは、ラックのパワーサプライ情報を表示できます。

手順

1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **Energy Efficiency Analysis**を選択します。
2. **Power Supply Analysis**タブをクリックします。
3. ラックスペース分析情報を表示します。

図242 電源の分析



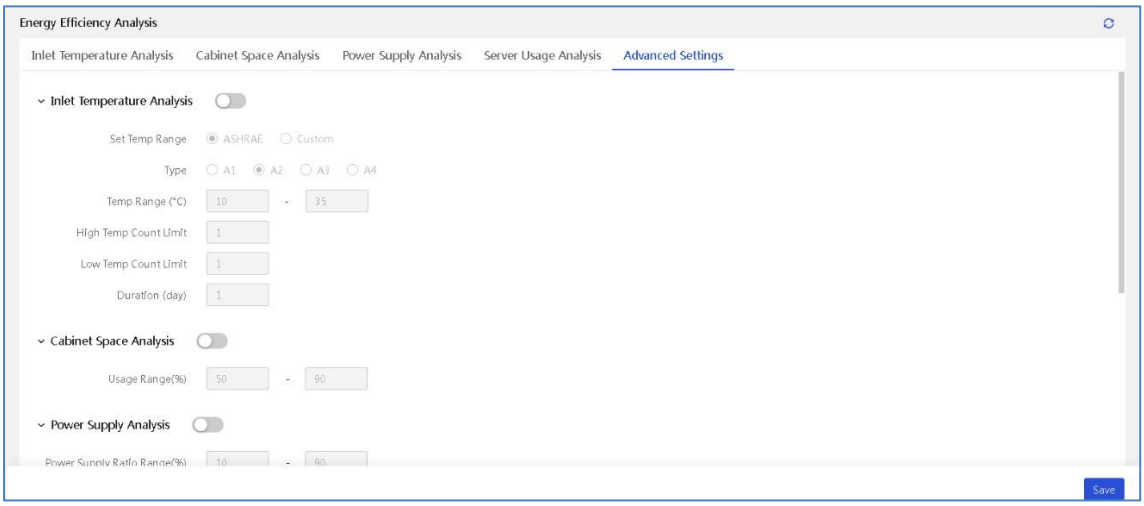
詳細設定を構成する

この機能を使用して、吸気温度分析、ラックスペース分析、パワーサプライ分析、およびサーバー使用率分析のパラメータを設定します。

手順

1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **Energy Efficiency Analysis** >**Advanced Settings**を選択します。
2. 入口温度解析を有効にします。**Set Temp Range**で**ASHRAE**または**Custom**を選択します。**ASHRAE**を選択した場合は、タイプ(A1、A2、A3、またはA4)を指定し、**High Temp Count Limit**、**Low Temp Count Limit**、および**Duration**を設定します。**Custom**を選択した場合は、温度範囲などのパラメータを設定します。
3. ラックスペース分析を有効にし、使用範囲を指定します。
4. 電源分析をイネーブルにし、電源比率範囲、電源上限、電源下限、および期間を指定します。
5. サーバー使用率分析を有効にします。必要に応じて、**Set Thresholds**で**CPU**、**GPU**、および**Memory**を選択し、アイドル状態および低負荷サーバーの**CPU Usage Lower Limit (%)**, **GPU Usage Lower Limit (%)**, **Memory Usage Lower Limit (%)**, および **Duration (day)**フィールドでそれぞれの値を指定します。
6. **Save**をクリックします。

図243 詳細設定の構成



ワンキー消費電力制限を行う

このタスクについて

機器室内の電源システムに障害が発生すると、非常用電源が有効になります。非常用電源での動作時間を延長するには、この機能を使用してサーバーの消費電力を低いレベルに制限します。この構成は、サーバーのパフォーマンスに影響を与えたり、サーバーを予期せずシャットダウンしたりする可能性があります。

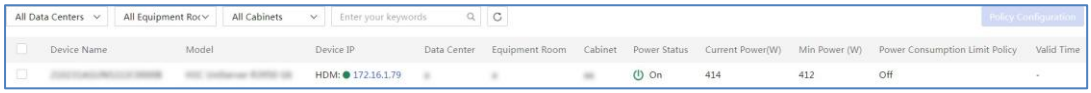
制約事項とガイドライン

- 消費電力ポリシーを設定し、現在のデバイスの最小消費電力が150 W未満の場合、システムはデフォルトで上限値を150 Wに設定します。
- 電源状態がオフの場合、またはHDMが異常な場合は、電力消費ポリシーを発行できません。

手順

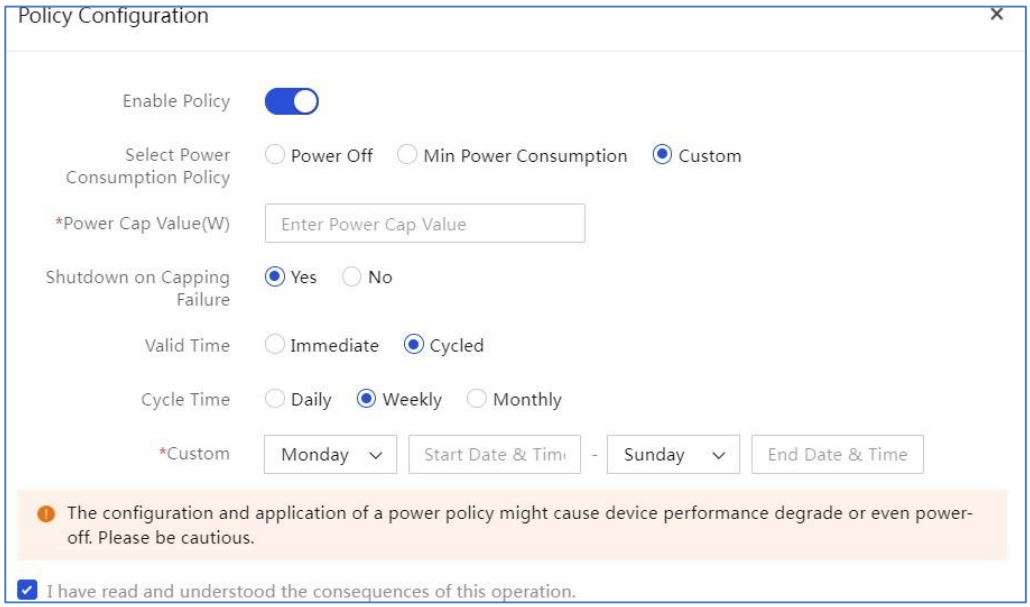
1. ナビゲーションペインで、**Menu** > **Energy and Prediction** > **One-Key Power Consumption Limit**を選択します。このページには、データセンターが管理するG6/G7サーバーに関する情報が表示されます。

   図244 One-Key Power Consumption Limitページ

2. サーバー情報をフィルタリングするには、データセンター、機器室、キャビネット、およびデバイス名を指定します。ファジーマッチングがサポートされています。
3. **Policy Configuration**をクリックして、設定するサーバーを選択します。

   図245 ポリシー編集方法の選択

4. **Apply Policy**をクリックします。表示されたダイアログボックスで、操作を確認するために**YES**と入力し、**OK**をクリックします。
5. 消費電力ポリシーを選択します。オプションには、Power Off、Min Power Consumption、および**Custom**が含まれます。
   - **Power Off**:サーバーがシャットダウンします。
   - **Min Power Consumption**:消費電力上限は最小消費電力に設定されます。
   - **Custom**:電力消費方法をカスタマイズします。
6. **Custom**を選択した場合は、消費電力上限の値を設定します。
   - サーバーの消費電力上限をカスタマイズして、有効範囲を150～10,000Wにします。
   - 消費電力上限を超えた場合にシャットダウン機能を有効にするかどうかを選択します。
   - アクティブ化の時間を設定します。オプションには、**Immediate**と**Cycled**があります。

7. Agreementチェックボックスをオンにします。これは、設定によって発生する可能性のある結果を理解していることを示します。
8. **OK**をクリックします。

説明

- **Device Name**:サーバーの名前。
- **Model**: サーバーのモデル。
- **Device IP**: UniSystemへの接続に使用されるHDM IPアドレス。
- **Data Center**: サーバーが属するデータセンター。
- **Equipment Room**: サーバーが存在する装置室。
- **Cabinet**: サーバーが置かれているキャビネット。
- **Power Status**: サーバーの電源ステータス。、、などがあり、それぞれ**Off**、**On**、**Unknown**を表します。
- **Current Power (W)**: サーバーの現在の電力。
- **Min Power (W):** サーバーの1日の最小電力。
- **Power Consumption Limit Policy**:次のオプションがあります。
  - オフ**Off**。
  - **Power Off**: サーバーの電源をオフにします。
  - **Min Power Consumption**: 消費電力上限値は、サーバーの最小消費電力です。
  - **Custom**: カスタムモードでは、次のパラメータを指定する必要があります。
    - **Power Cap Value (W)**:: 150～10000 Wの範囲の消費電力上限値。
    - **Shutdown on Capping Failure**: サーバーの電力が消費電力上限を超え、30秒以内にそれを下回らない場合、消費電力上限は失敗します**YES**を選択すると、サーバーは強制的にシャットダウンされます。**No**を選択すると、サーバーは実行を継続します。
    - **Valid Time**: 電力消費ポリシーの実行方法。オプションは**Immediate**および**Cycled**が含まれます。
    - **Cycle Time**: 有効時間が循環の場合の**Cycled**です。

キャビネットのインテリジェントな電源管理

キャビネットのインテリジェント電源管理について

このモジュールは、指定されたキャビネット内のすべてのG6デバイスの消費電力上限値を動的に調整できます。システムは、G6デバイスの履歴電力統計情報を使用して

次の30分間は30分ごと、5分ごとに消費電力上限を設定します。次に、システムは各G6デバイスの消費電力上限値を決定し、予測される消費電力と、非G6デバイスの予約電力の合計から差し引かれる電力制限の値に基づいて、値を動的に調整します。

制約事項とガイドライン

- 指定したキャビネットで消費電力上限を実行するには、キャビネットに少なくとも1台のG6サーバーがあり、設定された電力制限がG6サーバー番号*150+非G6サーバーの合計予約電力の値より小さくならないことを確認します。消費電力上限タスクの有効期間にサイクルまたは期間を設定し、システムが上記の要件が満たされていないことを検出した場合、タスクは

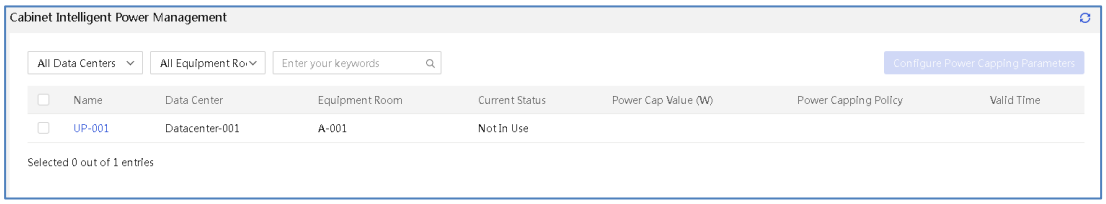
直接終了します。

- キャビネットの消費電力上限タスクは、異常なサーバーまたはG 6以外のサーバーでは有効になりません。
- 統計情報を正確に予測するには、この機能を使用する前に、キャビネット内のデバイスが2時間以上正しく動作していることを確認してください。
- キャビネットの消費電力上限タスクのトリガー時刻は、UniSystemシステムの時刻に依存します。タスクが予想どおりにトリガーされるようにするには、現在の時刻をUniSystemシステムの時刻と同期させます。
- キャビネットの消費電力上限機能は、AI予測アルゴリズムを統合したもので、サーバーの電力が定期的に変化するシナリオに適しています。動的消費電力上限方式を構成すると、サーバーの周波数が低下する可能性があります。サービスシナリオに基づいて注意して使用してください。

手順

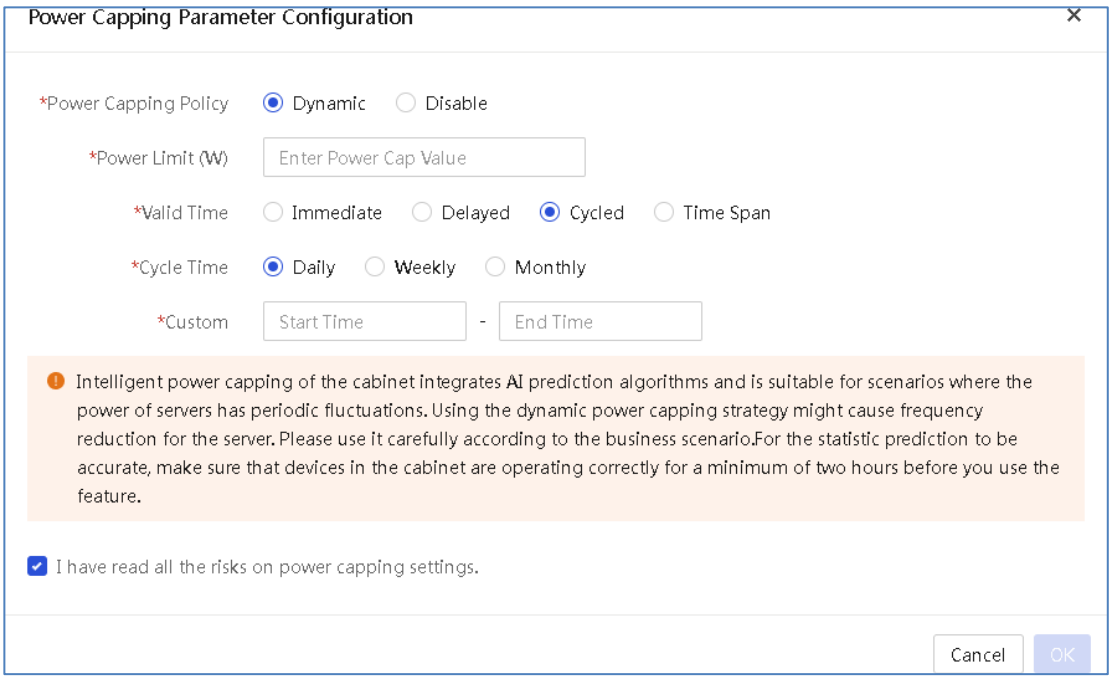
1. ナビゲーションペインで、Menu>Energy and Prediction>Cabinet Intelligent Power Managementをクリックします。

   図246 キャビネットのインテリジェント電源管理ページ



2. キャビネットを選択し、**Configure Power Capping Parameters**をクリックします。表示されたダイアログボックスでパラメータを構成し、**OK**をクリックします。

   図247 消費電力上限パラメータの設定



資産管理

資産管理メニューは、資産概要、資産インベントリ、資産検査を通じて、包括的なリアルタイムの監視および管理機能を提供し、ユーザーがリソースをより適切に制御および最適化できるようにします。ユーザーは、詳細な資産情報と状態を理解し、デバイス資産の変化をリアルタイムで監視し、資産検査と保守管理を効果的に実行して、資産の使用率を向上させ、運用コストを削減できます。

資産の概要

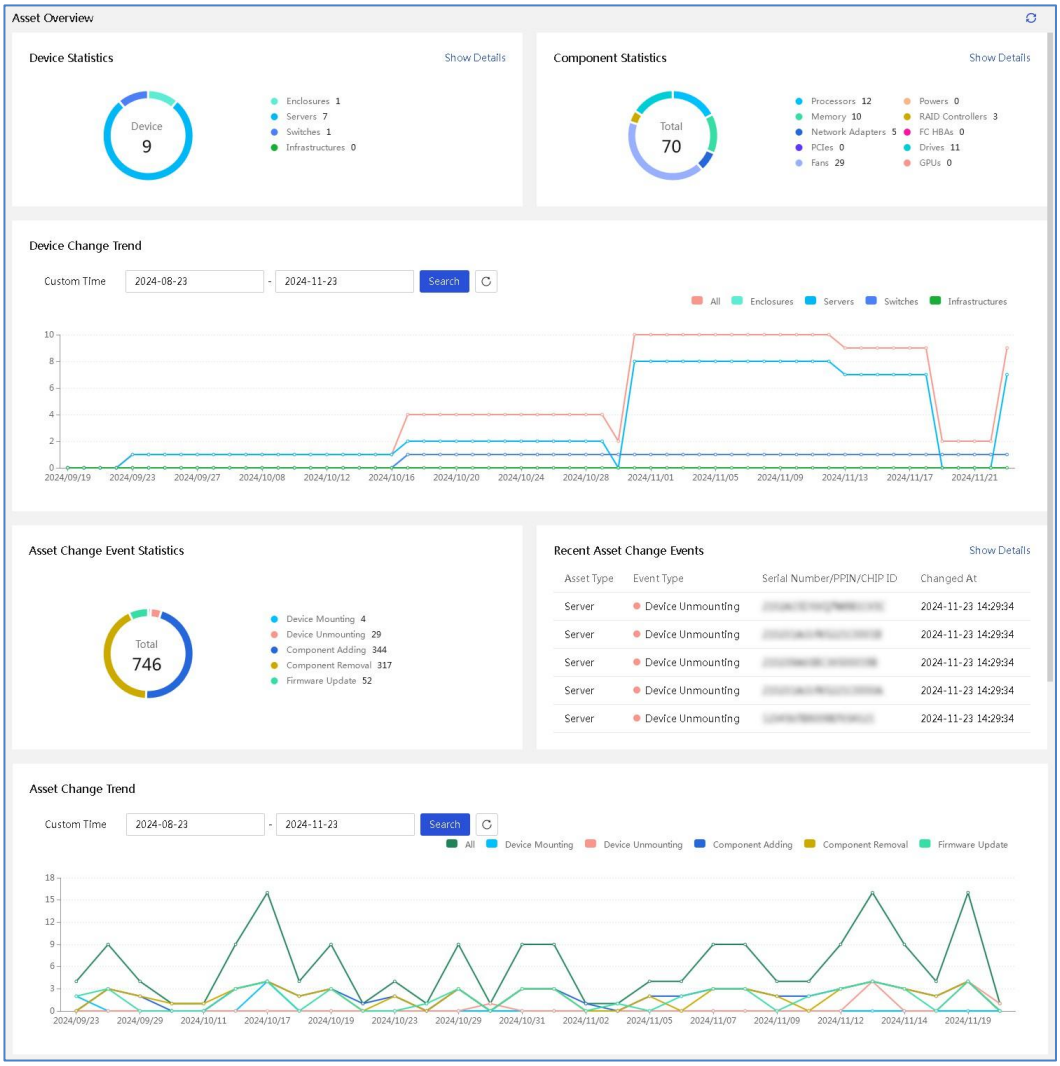
このタスクについて

この機能を使用して、デバイス統計、コンポーネント統計、デバイス変更トレンド、資産変更イベント統計、最近の資産変更イベントおよび資産変更トレンドを表示します。これにより、ユーザーは資産の使用効率および変更トレンドを迅速に理解できます。

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Overview**を選択します。
2. 次の情報を表示します。
   - **Device Statistics**:現在のデバイスの総数、各タイプのデバイスの数、および前日と比較した変更を表示します。
   - **Component Statistics**:現在のコンポーネントの合計数、各タイプのコンポーネント数および前日と比較した変更を表示します。コンポーネントタイプには、プロセッサー、メモリー、ネットワークアダプタ、PCIe、ファン、電源、ストレージコントローラー、FC HBA、ドライブおよびGPUが含まれます。
   - **Device Change Trend**:過去1年間の各日のデバイス数量の変更を表示します。
   - **Asset Change Event Statistics**:イベントの合計数、各変更タイプの頻度/割合など、資産変更の統計情報を表示します。
   - **Recent Asset Change Events**ト:最近の5つの資産変更イベントを表示します。次のタイプの資産変更イベントを使用できます。
     - **Device Mounting**: デバイスをUniSystem管理リストに追加します。
     - **Device Removal**: UniSystem管理リストからデバイスを削除します。
     - **Component Adding**: コンポーネントをサーバーにインストールします。
     - **Component Removal**:サーバーからコンポーネントを削除します。
     - **Firmware Update**: HDM(プライマリパーティション、ゴールデンイメージ、またはバックアップパーティション)、BIOS、ME、システムボードCPLD、またはiFISTファームウェアを更新します。
   - **Asset Change Trend**:過去1年間の日次資産変更頻度を表示します。

図248 資産の概要



3. 詳細を表示するには、**Device Statistics**、**Component Statistics**または**Recent Asset Change Events**セクションの**View Details**をクリックしてそれぞれのページに移動します。
4. 特定の時間範囲の統計情報を表示するには、**Device Change Trend**セクションまたは**Asset Change Trend**セクションにカスタム期間を入力し、**Search**をクリックします。

資産インベントリ

このタスクについて

UniSystemは、さまざまなデバイスやコンポーネントの詳細な統計情報を提供し、システム内の資産の管理と監視を容易にします。

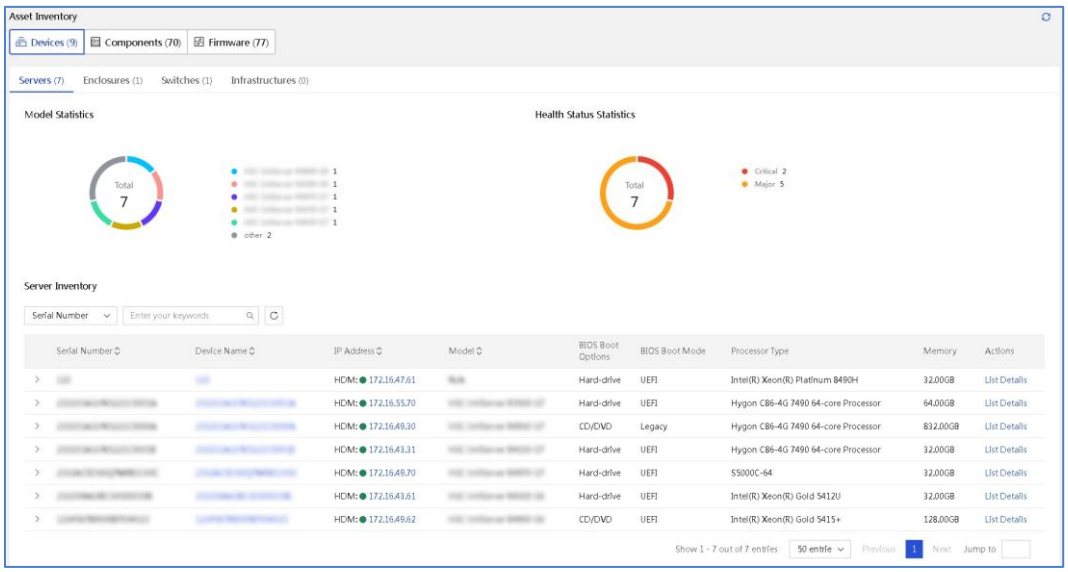
- デバイスタイプには、サーバー、エンクロージャー、スイッチ、インフラストラクチャなどがあります。
- コンポーネントタイプには、プロセッサー、メモリー、ドライブ、ネットワークアダプター、PCIe、ストレージコントローラー、GPU、電源、ファン、FC HBAなどがあります。

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Inventory**を選択します。
2. サーバー資産インベントリ情報を表示します。

a. **Devices**をクリックします。**Servers**タブが表示されます。

図249 サーバー資産インベントリ



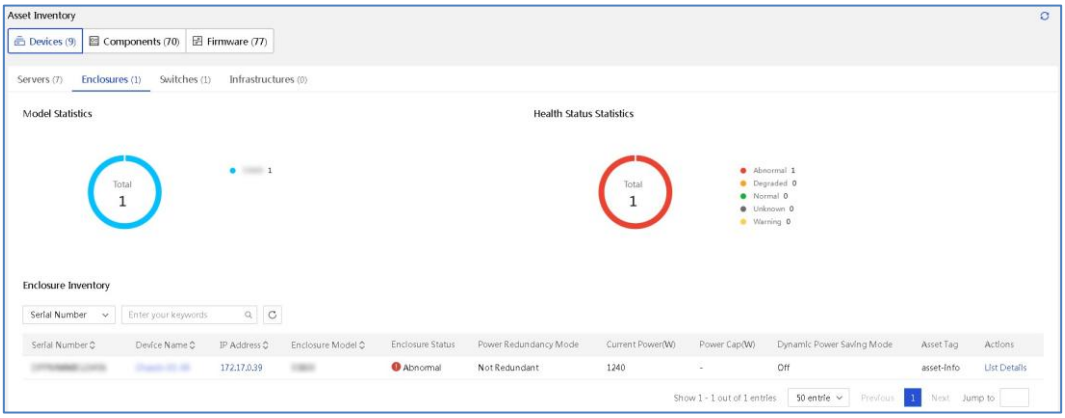
b. 必要に応じて、次のタスクを実行します。

- 資産のライフサイクルを表示するには、サーバーのシリアル番号の左にあるアイコン ＞をクリックします。開始時刻と終了時刻を入力し、**Search**をクリックして対応する変更レコードを表示できます。
- サーバーの詳細情報を表示するには、デバイス名のリンクをクリックします。詳しくは、「サーバー情報の表示」を参照してください。
- サーバーのHDMにログインするには、server IP addressリンクをクリックします。
- サーバーに含まれるコンポーネントのリストを表示するには、サーバーの**Actions**列の**List Details**をクリックします。

3. エンクロージャー資産インベントリ情報を表示します。

a. **Devices**をクリックし、**Enclosures**タブをクリックします。

図250 エンクロージャーの資産インベントリ



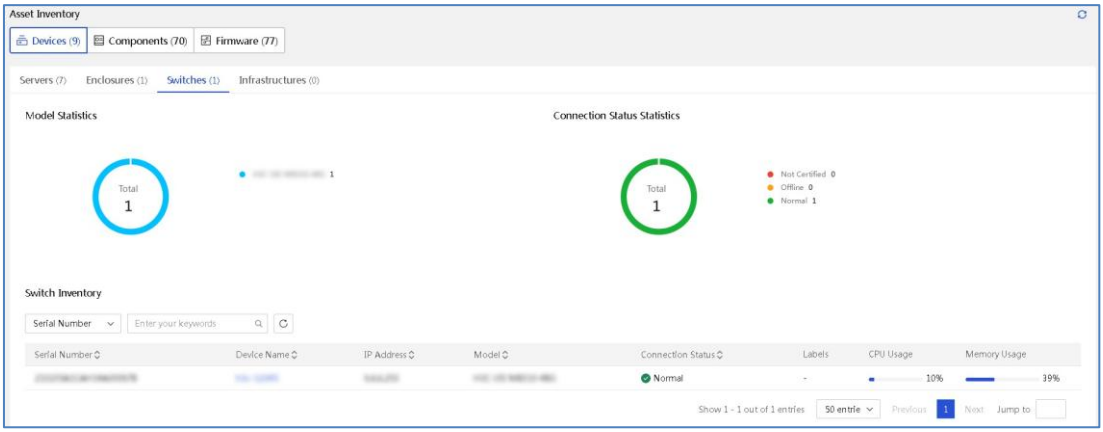
b. 必要に応じて、次のタスクを実行します。

- エンクロージャーに関する詳細情報を表示するには、デバイス名のリンクをクリックします。
- エンクロージャーのOMにログインするには、IPアドレスリンクをクリックします。
- サーバーに含まれるコンポーネントのリストを表示するには、**Actions**列の**List Details**をクリックします。

4. スイッチ資産インベントリ情報を表示します。

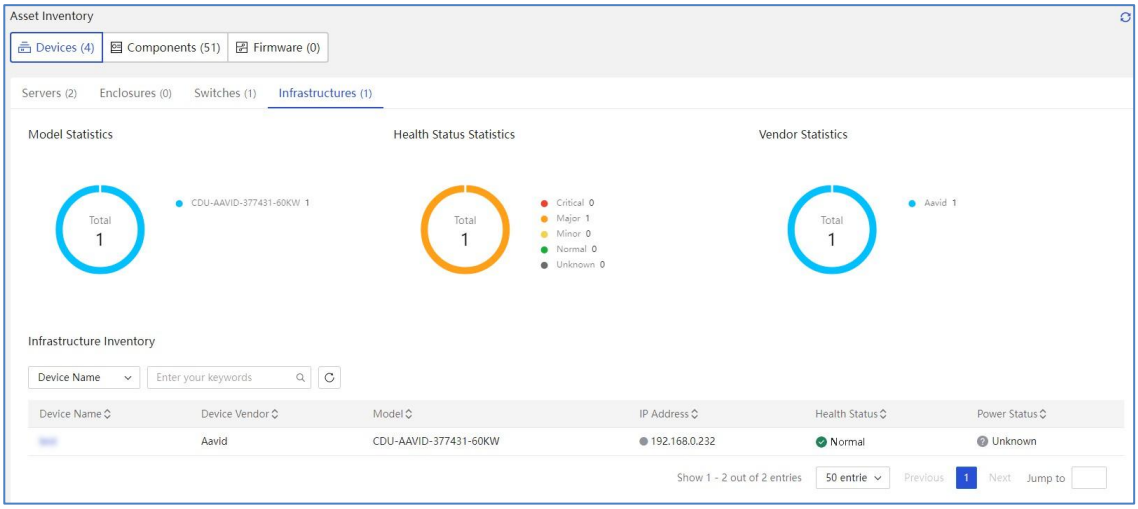
Devicesをクリックし、**Switches**タブをクリックします

図251 スイッチ資産インベントリ



5. インフラストラクチャ資産インベントリ情報を表示します。**Devices**をクリックし、**Infrastructures**タブをクリックします。

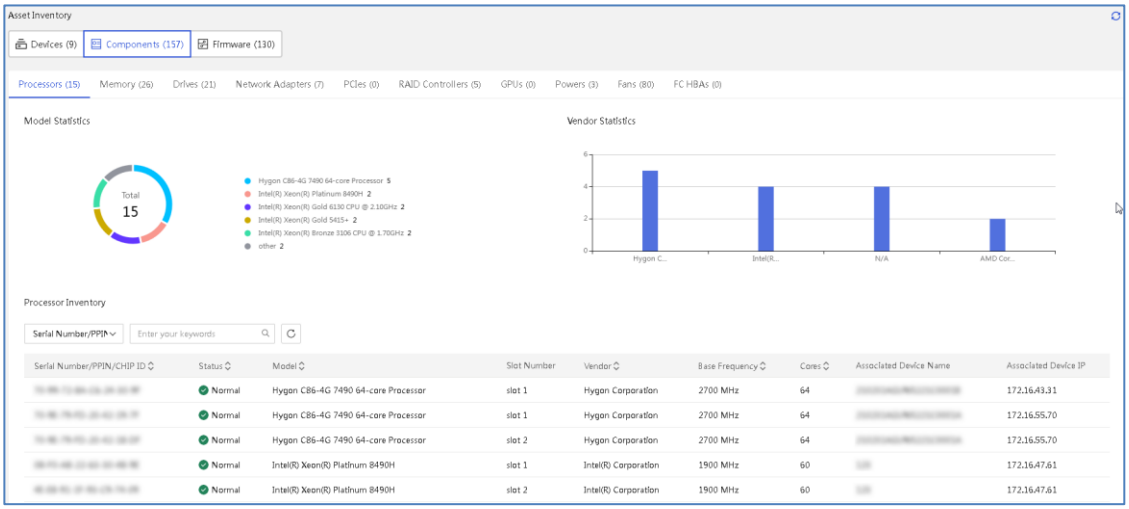
図252 インフラストラクチャ資産インベントリ



6. プロセッサー資産インベントリ情報を表示します。

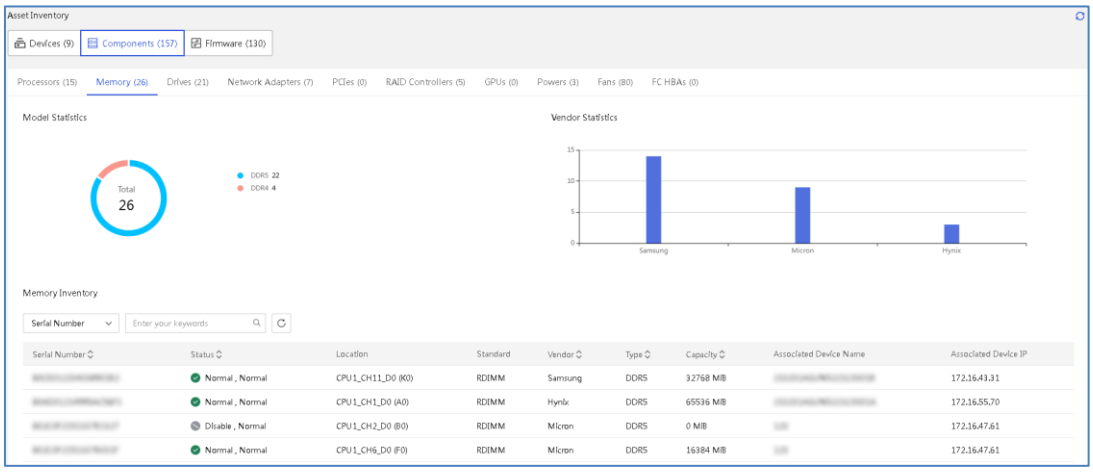
   Componentsをクリックします。**Processors**タブが表示されます。

   図253 プロセッサー資産インベントリ



7. メモリー資産インベントリ情報を表示します。**Components**をクリックし、**Memory**タブをクリックします。

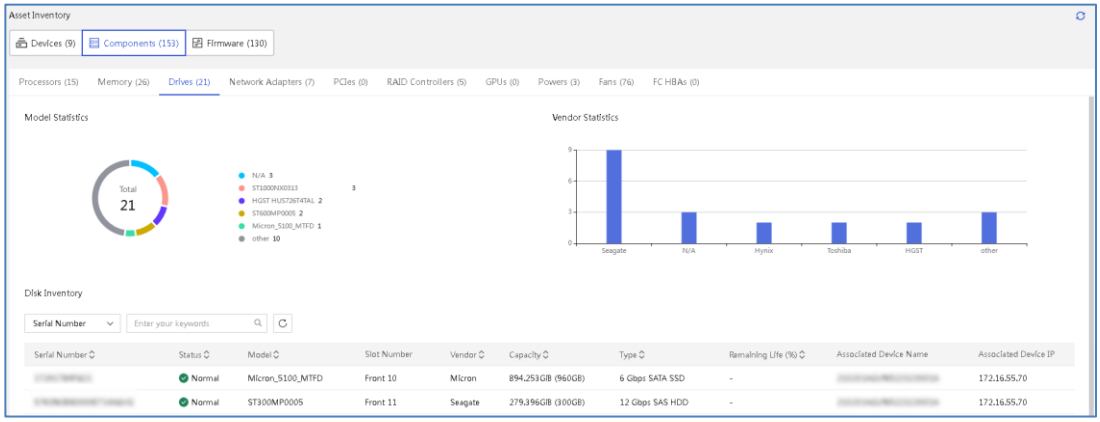
図254 メモリー資産インベントリ



8. ドライブ資産インベントリ情報を表示します。

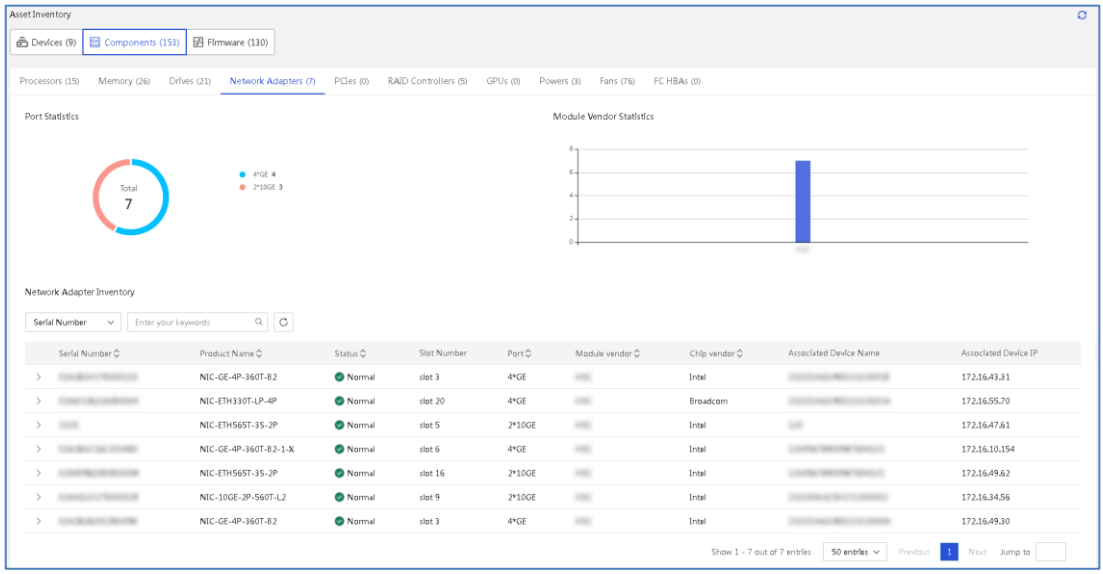
   Componentsをクリックし、**Drives**タブをクリックします。

   図255 ドライブ資産インベントリ



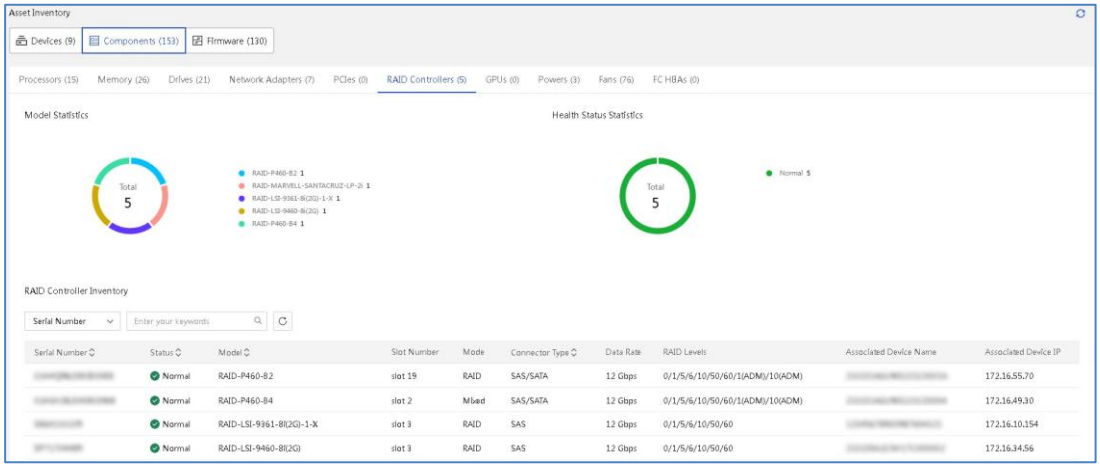
9. ネットワークアダプタ資産のインベントリ情報を表示します。**Components**をクリックし、**Network Adapters**タブをクリックします。

図256 ネットワークアダプタ資産インベントリ



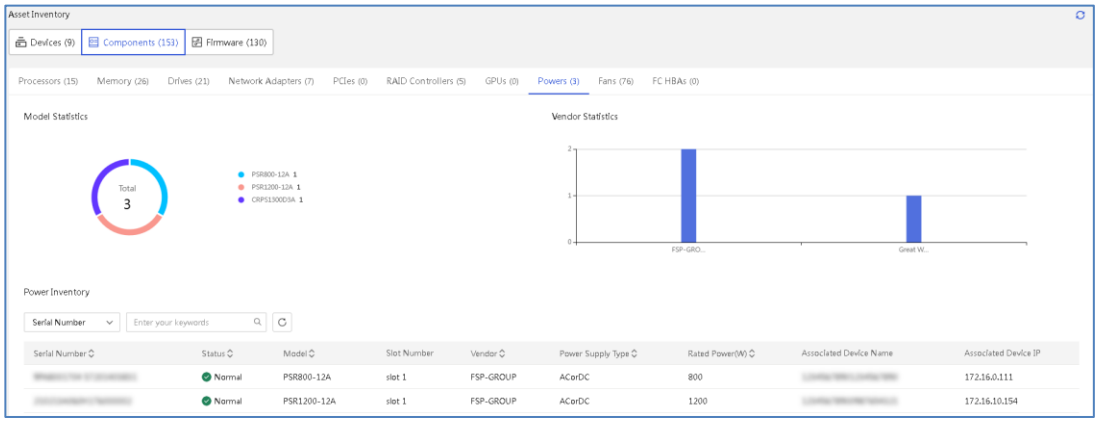
10. PCIe資産インベントリ情報を表示します。**Components**をクリックし、**PCIes**タブをクリックします。
11. RAIDコントローラ資産のインベントリ情報を表示します。**Components**をクリックし、**RAID Controllers**タブをクリックします。

図257 RAIDコントローラ資産インベントリ



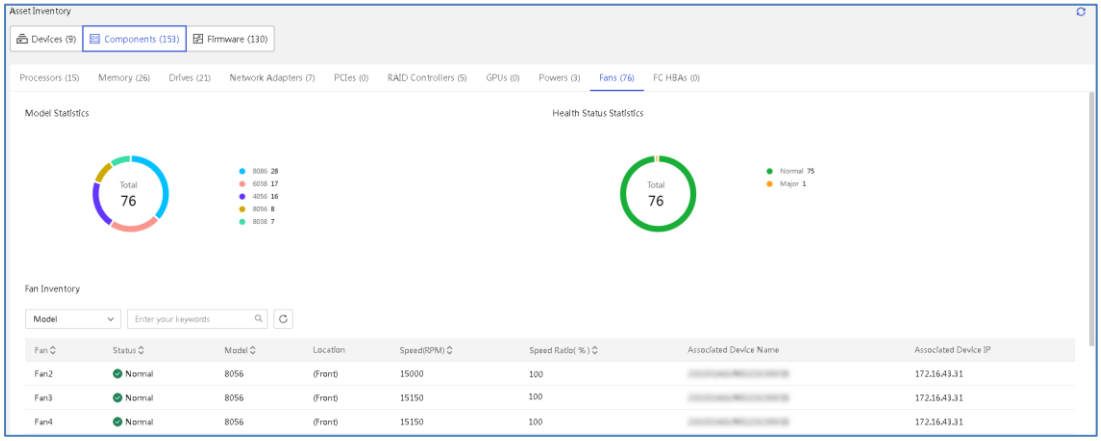
12. GPU資産インベントリ情報を表示します。**Components**をクリックし、**GPUs**タブをクリックします。
13. 電源資産のインベントリ情報を表示します。**Components**をクリックし、**Power**タブをクリックします。

図258 電源資産インベントリ



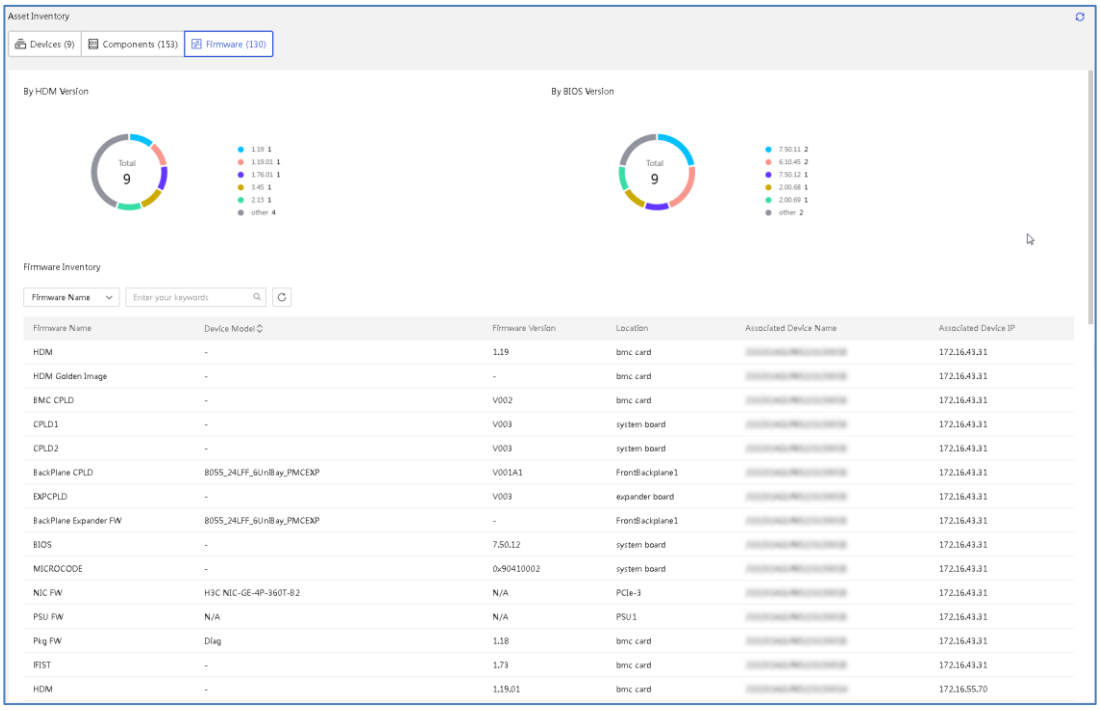
14. ファンの資産インベントリ情報を表示します。
    Componentsをクリックし、**Fans**タブをクリックします。

    図259 ファン資産インベントリ



15. FC HBA資産のインベントリ情報を表示します。**Components**をクリックし、**FC HBAs**タブをクリックします。
16. HDMおよびBIOSを含むファームウェアのインベントリ情報を表示します。**Firmware Inventory**をクリックします。

図260 ファームウェアインベントリ



パラメータ

- サーバー
  - **Serial Number**: サーバーのシリアル番号。
  - **Device Name**: サーバーの名前。
  - I **IP Address**: サーバーのHDM管理IPアドレス。
  - **Model**: サーバーのモデル。
  - **BIOS Boot Options**: サーバーのBIOSブートオプション。
  - **BIOS Boot Mode**: サーバーのBIOSブートモード。
  - **Processor Type**: サーバーに搭載されているプロセッサーのモデル。
  - **Memory**: サーバーのメモリー容量。
  - **Firmware**: HDM(プライマリパーティションとバックアップパーティション)、BIOS、ME、システムボードCPLD、およびiFISTファームウェアのバージョン情報。
- エンクロージャー
  - **Serial Number**: エンクロージャーのシリアル番号。
  - **Device Name**: エンクロージャーのデバイス名。
  - I**P Address**: OMモジュールの管理IPアドレス。
- エンクロージャーモデル: エンクロージャーのモデル。
  - **Enclosure Status**: エンクロージャーの全体的なヘルスステータス。
  - **Power Redundancy Mode**: エンクロージャーの現在の電源冗長モード。オプションには、N+1、N+N、および**Not Redundant**があります。
  - **Current Power**:: エンクロージャー内のすべてのデバイスが消費している総電力。
  - **Power Cap**: エンクロージャーの電力制限値。

- **Dynamic Power Saving Mode**:動的省電力モードの状態。
- **Asset Tag**:エンクロージャーの資産タグ。エンクロージャーを一意に識別するために使用されます。

- スイッチ
  - **Serial Number**: スイッチのシリアル番号。
  - **Device Name**: スイッチのデバイス名。
  - **IP Address**: スイッチの管理IPアドレス。
  - **Model**: スイッチのモデル。
  - **Connection Status**: スイッチの接続ステータス。次のオプションがあります。
    - **Normal**: 正常にログインしました。
    - **Offline**: UniSystemでスイッチとの通信異常が発生しています。
    - **Not Certified**:UniSystemはスイッチと正常に通信します。次のいずれかの条件が存在する場合、スイッチは未認証状態になります。
      ユーザー情報(ユーザー名とパスワード)の確認に失敗しました。UniSystemでユーザー情報を更新する必要があります。詳細については、「スイッチの管理」を参照してください。

      ユーザー切り替えは、HTTPサービスの使用を許可されていません。
- **Labels**:スイッチのデバイスラベル。
  - **CPU Usage**:スイッチのCPU使用率。
  - **Memory Usage**:スイッチのメモリー使用状況。
- インフラストラクチャ
  - **Device Name**:インフラストラクチャのデバイス名。
  - **Device Vendor**:インフラストラクチャの製造元。
  - **Model:** インフラストラクチャのモデル。
  - **IP Address**:インフラストラクチャの管理IPアドレス。
  - **Health Status**:インフラストラクチャの稼働状態。**Unknown**、**Normal**、**Minor**、**Major**および**Critical**などのオプションがあります。

資産の変更

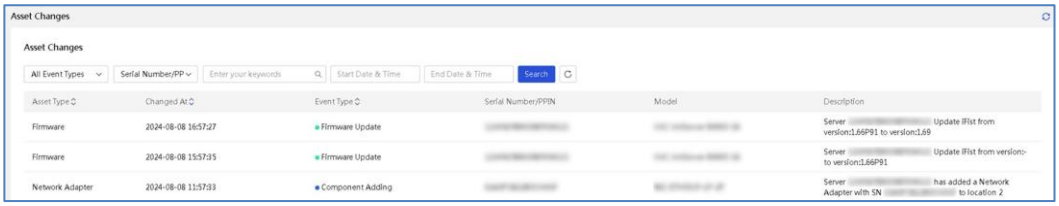
このタスクについて

UniSystemは、デバイスおよびコンポーネントの変更の包括的な記録と管理を提供します。資産の変更には、デバイスのインストール、デバイスの取り外し、コンポーネントの追加、コンポーネントの取り外し、ファームウェアの更新など、現在のデバイス資産の変更履歴が表示されます。これは、デバイスのライフサイクルと状態の変更を追跡するのに役立ちます。

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Changes**.を選択します。
2. 資産変更レコードをフィルタします。
   - イベントタイプを選択します。
   - **Menu** > **Asset Management** > **Asset Changes**.または**Model**を選択し、キーワードを入力してから、アイコンをクリックします。
   - 開始時刻と終了時刻を入力し、**Search**をクリックします。

図261資産の変更



パラメータ

- **Asset Type**:オプションには次のものがあります。
  - **Device types**:サーバー、エンクロージャー、スイッチ、およびインフラストラクチャ。
  - **Component types**:プロセッサー、メモリー、ディスク、ネットワークアダプタ、PCIe、RAIDコントローラ、GPU、電源、ファン、およびFC HBA。
- **Changed At**:資産が変更された時刻。
- **Event Type**:次のオプションがあります。
  - **Device Mounting**: デバイスをUniSystem管理リストに追加します。
  - **Device Removal**:UniSystem管理リストからデバイスを削除します。
  - **Component Adding**: コンポーネントをサーバーにインストールします。
  - **Component Removal**:サーバーからコンポーネントを削除します。
  - **Firmware Update**: HDM(プライマリパーティションまたはバックアップパーティション)、BIOS、ME、システムボードCPLD、またはiFISTファームウェアを更新します。
- **Serial Number/PPIN**: デバイスまたはコンポーネントのシリアル番号またはPPIN。
- **Model**:: デバイスまたはコンポーネントのモデル。
- **Description**: 資産変更の摘要。

資産検査

このタスクについて

資産検査は、デバイスの状態を自動的に監視およびチェックすることによって、資産の安定した運用を保証します。資産検査には、次の機能があります。

- **Configure inspection tasks**: 検査状態(有効または無効)の設定、検査名の定義、実行時間の指定、実行期間の設定、デバイスおよびコンポーネントタイプ(プロセッサー、メモリー、ネットワークアダプタ、PCIe、ストレージコントローラー、FC-HBA、ファン、電源、ドライブ、GPU、SNMPトラップなど)の選択、検査レポートおよび通知を受信するための電子メール連絡先情報の設定など、検査をガイドする検査ポリシーを設定します。
- **View the inspection records**: 実行済タスクの実行レコードの表示を許可します。レコードリストには、シリアル番号、状態(成功または失敗)、開始時間および完了時間が含まれ、ダウンロード、送信、削除および詳細表示操作がサポートされます。
- **Generate inspection reports**: デバイスのヘルスステータスの詳細な概要を示す検査レポートを提供します。G6以上のサーバーでは、PDFレポートには、イベントログ内のすべての未解決アラームに対する処理推奨事項も含まれます。G6未満のサーバーでは、または関連するアラームが見つからない場合、システムは、ユーザーがハードウェアの問題をトラブルシューティングしたり、テクニカルサポートに連絡したりする際のガイドとなるデフォルトの処理推奨事項を提供します。

- **Supports automated execution and notification**: 設定された期間中の指定された時間に自動実行をサポートします。同時に、システムはSMTPを介して指定された電子メール連絡先に検査レポートとアラーム通知を自動的に送信できるため、ユーザーはデバイスの状態の更新を迅速に受信できます。

前提条件

この機能を設定する前に、次の作業を完了してください。

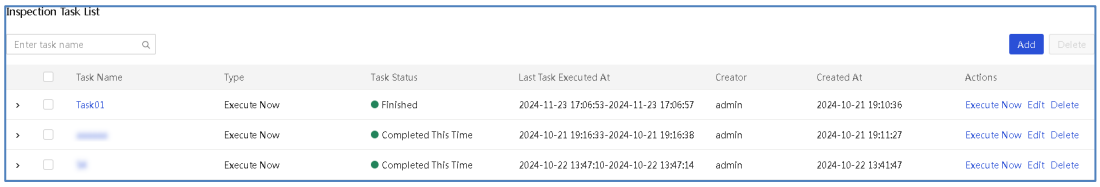
- SMTPの設定を完了します。詳細は、「SMTPの設定」を参照してください。
- 検査タスクがスコープに基づいて実行される場合は、最初にスコープを構成します。詳細については、「スコープマネジメント」を参照してください。

特定のタスクの表示

手順

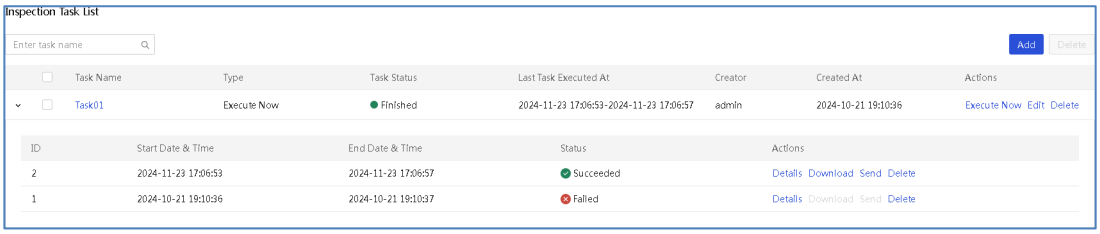
1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Inspection**をクリックします。

   図262 資産検査タスク

2. 追加したタスクおよびタスク情報を表示します。
3. タスクをフィルタするには、タスク名を入力し、検索アイコンをクリックします。
4. **Actions**列のリンクをクリックして、特定のタスクを実行します。
   - タスクをすぐに実行するには、**Execute Now**をクリックします。
   - タスクを編集するには、**Edit**.をクリックします。
   - タスクを削除するには、**Delete**をクリックします。
5. ›タスクの検査レコードを表示するには、タスクのアイコンをクリックし、実行履歴を展開します。
6. 特定のタスクを実行するには、履歴実行レコードのActions列のリンクをクリックします。
   - レコードの詳細を表示するには、**Details**をクリックします。
   - 実行レコードの圧縮レポートをダウンロードするには、**Download**をクリックします。
   - レポートを連絡先の電子メールアドレスに送信するには、**Send**をクリックします。
   - 履歴レコードを削除するには、**Delete**をクリックします。

図263 検査レコードの表示



パラメータ

- **検査タスクパラメータ**
  - **Task Name**: タスク名。
  - **Type: Execute NowExecute as Scheduled**よび**Execute Periodically**などのタスク実行タイプ。
  - **Task Status**: In Process、Pending、Completed This Time」およびCompleted。
  - **Last Task Executed At**: タスクが最後に実行された時刻。
  - **Creator**: タスクを作成したユーザー。
  - **Created At**: タスクの作成日時。
- **検査記録パラメータ**
  - **ID**: 検査レコードID。
  - **Start Date & Time**: 検査レコードの開始日時。
  - **End Date & Time**: 検査レコードの終了日時。
  - **Status**: 実行状態:次のオプションがあります。
    - **Succeeded**
    - **Inspecting**
    - **Failed**: リンクをクリックすると、失敗の理由を表示できます。
    - **Sending failed**: タスクは正常に実行されましたが、検査レポートの送信に失敗しました。ベストプラクティスとして、電子メール構成を確認してください。

制約事項とガイドライン

UniSystemでは、中国語と英語の両方での検査レポートのエクスポートがサポートされています。レポートの言語は、検査計画の構成時にWebインタフェースで使用される言語設定と一致します。

検査タスクを追加する

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Inspection**をクリックします。
2. **Add**をクリックし、次のようにインスペクションポリシーを設定します。
   a. 検査タスク名を入力します。
   b. 検査サイクルを選択します。
   c. 検査デバイスタイプを選択します。
   d. デバイス範囲を選択します。次のオプションがあります。
      - **Scope** 検査するデバイスが属する範囲を選択します。複数の範囲を選択できます。
      - **Custom**: 検査するデバイスを直接選択します。複数のデバイスを選択できます。

e. (オプション)連絡先の電子メールを入力します。有効な電子メールアドレスを入力すると、自動送信を有効にできます。

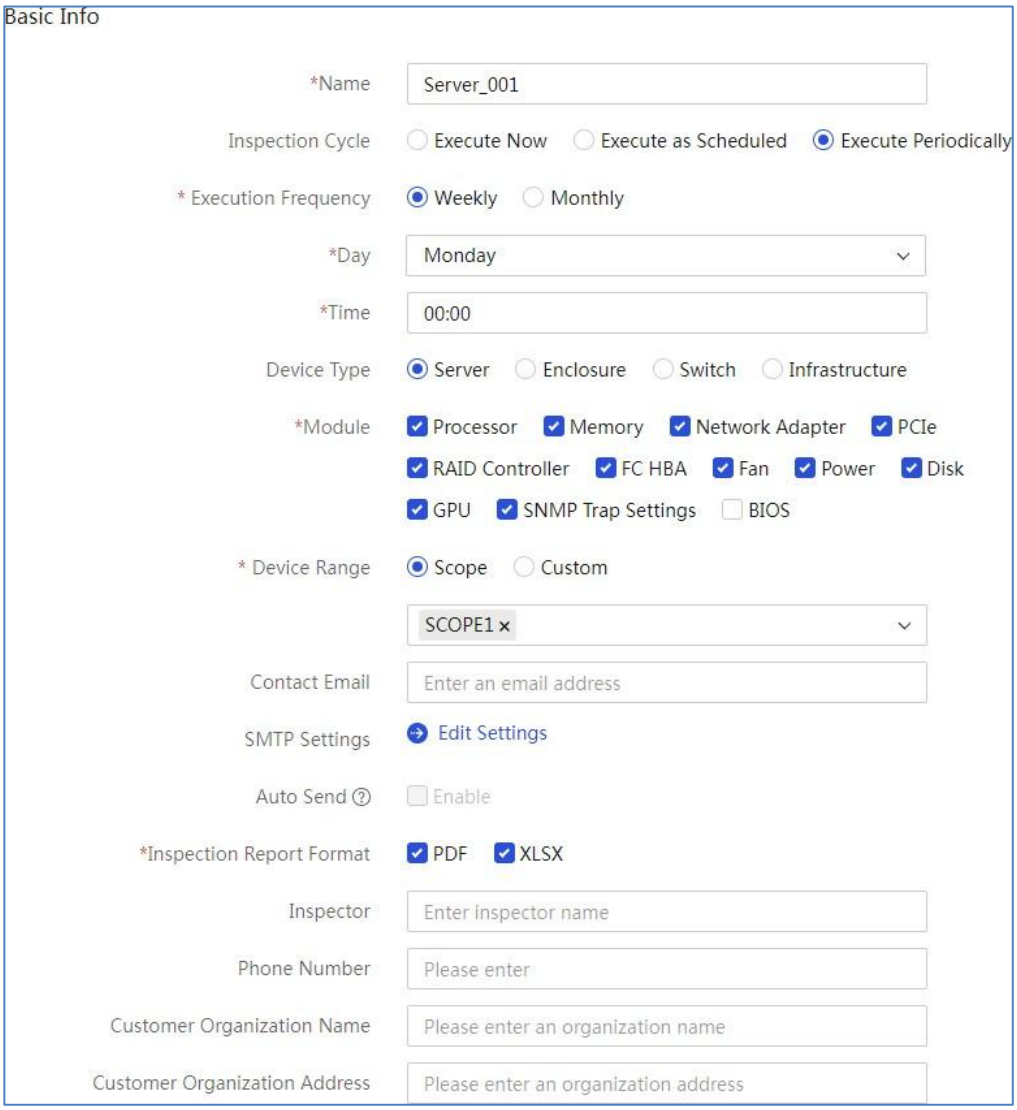
f. SMTP設定を編集するには、**SMTP Settings**フィールドで**Edit Settings**をクリックします。

g. 検査レポートの形式を選択します。両方の形式を選択できます。

h. (オプション)名前、電話番号、組織名、組織アドレスなどのインスペクタ情報を入力します。

3. **OK**をクリックします。

図264 検査タスクの追加



パラメータ

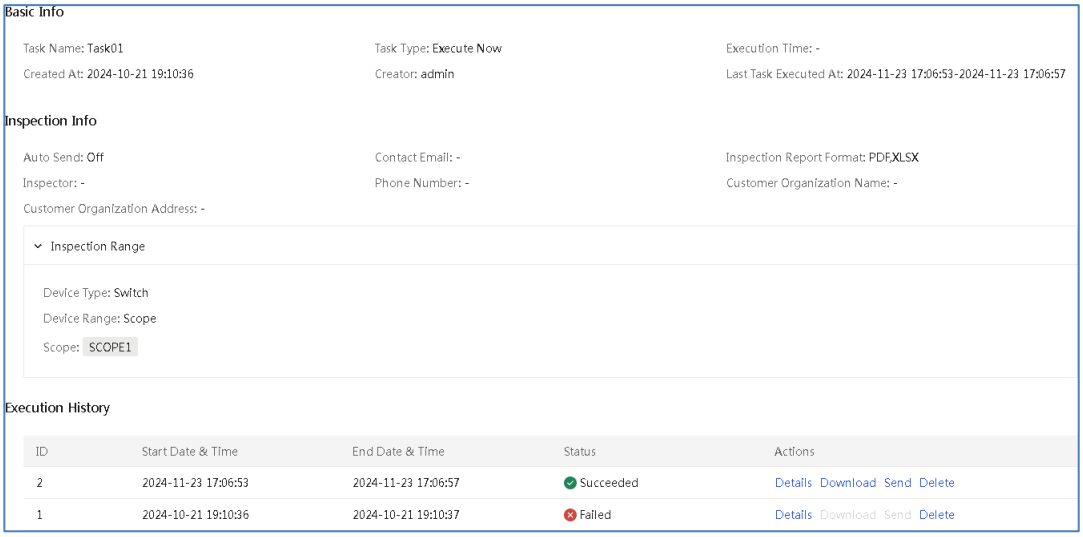
- **Name**: 検査タスクの名前。
- **Inspection Cycle**: 次のオプションがあります。
  - **Execute Now**: 資産検査が有効になった直後に検査タスクを実行します。
  - **Execute as Scheduled**: 設定した時間に検査タスクを実行します。実行時間を選択する必要があります。
  - **Execute Periodically** : 指定した期間内に、指定した間隔で検査タスクを実行します。実行の頻度と期間を指定する必要があります。
- **Inspection Device Type** : **Servers**、**Enclosure**、**Switch**、および**Infrastructure**が含まれます。

- **Module:** 検査デバイスタイプがServerの場合に検査するモジュールを選択します。使用可能なモジュールには、**Processor**、**Memory**、**Network Adapter**、**PCIe**、**RAID Controller**、**FC HBA**、**Fan**、**Power**、**Disk**、**GPU**、**SNMP Trap Settings**および**BIOS**があります。
- **Device Range**: **Scope**と**Custom**を含むデバイス範囲を選択します。
- **Contact Email**: 検査レポートの受信に使用する電子メールアドレスを入力します。
- **Auto Send**:: 検査タスクの完了時に、システムが検査レポートを連絡先の電子メールアドレスに自動的に送信できるようにします。
- **Inspector**: 検査レポートに表示される検査者の名前を入力します。
- **Inspection Report Format**: 検査レポートのフォーマットを選択します。オプションには、PDFと**XLSX**。BIOS構成を選択した場合、検査レポートの形式はXLSXのみをサポートします。
- **Phone Number**: 検査レポートに表示される検査担当の電話番号を入力します。
- **Customer Organization Name**: 検査レポートに表示する顧客の組織名を入力します。
- **Customer Organization Address**: 検査レポートに表示される顧客の組織所在地を入力します。

検査タスクに関する詳細情報の表示

1. ナビゲーションペインで、「メニュー」>「資産管理」>「資産検査」を選択します。
2. ターゲット検査タスクの名前リンクをクリックして、その詳細を表示します。

   図265 検査タスクに関する詳細情報の表示



3. ›検査対象デバイスの範囲を表示するには、**Inspection Range**の前にあるアイコンをクリックします。
   」ボックスで選択します

検査タスクの編集

制約事項とガイドライン

システムが資産検査タスクを実行しているときは、タスクを編集できません。

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Inspection**をクリックします。
2. ターゲットタスクの**Actions**コラムで**Edit**をクリックします。
3. 必要に応じてタスクを編集し、**OK**をクリックします。

検査タスクの削除

制約事項とガイドライン

- 実行中のタスクは削除できません。
- タスクを削除すると、関連する検査レコードとレポートも削除されます。

手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Asset Inspection**をクリックします。
2. 検査タスクを削除するには、次のいずれかを実行します。
   - 特定のタスクを削除するには、ターゲットタスクの**Actions**列で**Delete**をクリックします。
   - 複数のタスクをまとめて削除するには、タスクを選択し、**Delete**をクリックします。

保守管理

このタスクについて

メンテナンス管理により、ユーザーはデバイスのメンテナンス状態を管理し、保証情報を常に把握し、デバイスのメンテナンスや修理が必要な場合に迅速に対応できます。

メンテナンス管理には、次の機能があります。

- 保守ステータス統計

  UniSystemは、デバイスの保証に基づいて保守ステータスを6つのランクに分類し、各保守ステータスのデバイスに関する統計を収集することで、ユーザーがデバイスの保守の緊急性を迅速に理解できるようにする。
- 保守情報管理
  - **iService Synchronization**:: iServiceからの複数のデバイスのメンテナンス情報の自動バッチ同期をサポートし、デバイスメンテナンス情報のリアルタイムの精度を保証します。新しいサーバーを追加すると、UniSystemはiServiceからサーバーのメンテナンス情報を自動的に取得します。
  - **Import Data**: メンテナンスデータをExcelファイルに手動でインポートできるため、自動同期に依存することなく、デバイスのメンテナンス情報を柔軟に更新およびメンテナンスできます。
  - **Export Data**: メンテナンスデータのExcelファイルへのエクスポートをサポートし、オフラインでのデータの分析とバックアップを容易にします。

前提条件

この機能を構成する前に、まずiServiceの設定を完了します。詳細は、「iServiceの構成」を参照してください。

制約事項とガイドライン

- サーバーリストが更新されると、システムは更新をメンテナンスリストに同期させます。
- 新しいサーバーが追加されると、システムは5分以内にメンテナンス情報をiServiceと同期します。iServiceの同期を正常に動作させるには、事前にiServiceを正しく構成してください。自動同期が失敗した場合は、iServiceの構成を更新し、**iService Synchronization**をクリックして再試行してください。

- **Maintenance Management**ページに入ると、iService構成が自動的に検証されます。検証に失敗すると、**iService Synchronization**ボタンはグレー表示され選択できない状態になります。

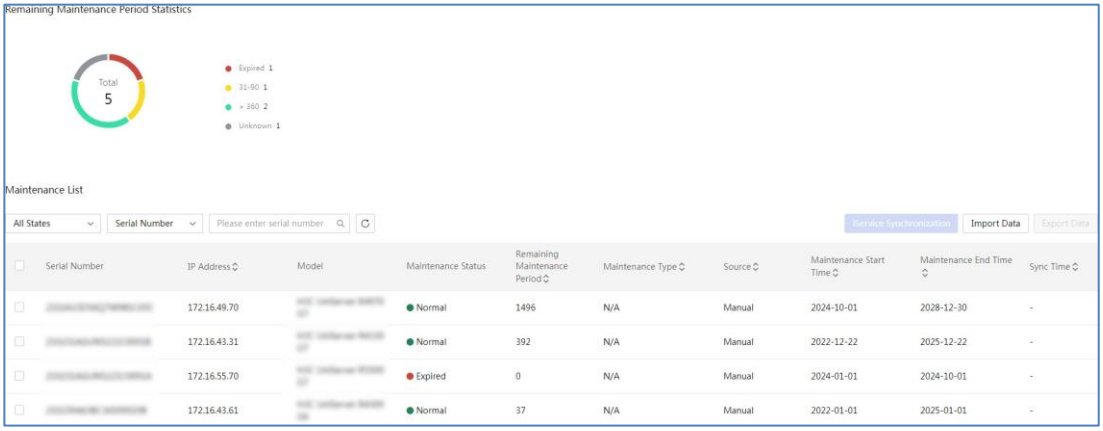
手順

1. ナビゲーションペインで、**Menu** > **Asset Management** > **Maintenance Management**を選択します。
2. iServiceのメンテナンス情報を同期します。

   メンテナンスリストで、同期するサーバーを選択し、**Service Synchronization**をクリックします。
3. メンテナンスデータをエクスポートします。

   メンテナンスリストで、ターゲットサーバーを選択し、**Export Data**をクリックします。データはExcelにエクスポートされ、ローカルに保存されます。
4. メンテナンスデータをインポートします。
   a. **Import Data**をクリックし、テンプレートをダウンロードして、メンテナンス情報を入力します。
   b. 完成したテンプレートをクリックして選択します。
   c. **Upload**をクリックします。アップロードが成功した後、メンテナンス情報を手動で同期化できます。

図266保守管理



パラメータ

- **Remaining Maintenance Period Statistics**: サーバーの合計数および残りのメンテナンス期間別のサーバー分布。タイプには、Expired、<30、31-90、91-180、181-360、>360および**Unknown**が含まれます。
- **Serial Number**: サーバーのシリアル番号。
- **IP Address**: サーバーのHDM管理IPアドレス。
- **Model**: サーバーのモデル。
- **Maintenance Status**: メンテナンスステータスは、Normal、Expire Soon、Expiredおよび**Unknown**の4つのカテゴリに分けることができます。
- **Remaining Maintenance Period**: サーバーの残りのメンテナンス期間(日数)。
- **Maintenance Type**: サーバーのメンテナンスサービスレベル。
- **Source**: マニュアルやiServiceなどのメンテナンス情報のソース。
- **Maintenance Start Time**: サーバー保証の開始時刻。
- **Maintenance End Time**: サーバー保証の終了時刻。

- **Sync Time**: メンテナンス情報が同期された時刻。

構成ツールDHCPサーバーを構成する

DHCPサーバーについて

重要:

DHCPサーバーを起動する前に、まず現在のLAN構成を確認し、次のことを確認します。
複数のDHCPサーバーが存在しないため、ネットワーク障害が発生します。

このモジュールを使用すると、DHCPサーバーを使用して、IPアドレスを自動的に割り当てたり、同じLAN上の各クライアントにIPアドレスを静的にバインドしたりできます。IPアドレスは、HDM管理IPアドレスまたはシステムIPアドレスとして使用できます。UniSystemでは、次のIPアドレス割り当て方法がサポートされています。

- **Dynamic method**: クライアントがDHCPサーバーにIPアドレスを要求すると、DHCPサーバーは自動的にIPプールからIPアドレスを選択し、そのIPアドレスをクライアントに割り当てます。
- **Static method**: IPアドレスをクライアントに手動でバインドします。クライアントがDHCPサーバーにIPアドレスを要求すると、DHCPサーバーはバインドされたIPアドレスをクライアントに割り当てます。

DHCPサーバー機能は、PXEデプロイメントのDHCP機能とは排他的です。ポートの競合が発生するため、2つの機能を同時に設定することはできません。

DHCPサーバーを設定する

このタスクについて

DHCPサーバーの設定を構成するには、次の作業を実行します。DHCPサーバーを使用すると、DHCPクライアントにIPアドレスを動的に割り当てることができます。

制約事項とガイドライン

- ネットワーク上に多数のDHCPクライアントが存在する場合は、リース時間をより大きな値に設定します。
- DHCPサーバーサービスを正常に開始するには、ポート番号67が別のサービス(dnsmasqなど)によって使用されていないことを確認します。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **DHCP Server**.を選択します。
2. **DHCP Service**をクリックします。表示されたダイアログボックスで、次の手順を実行します。
   a. **DHCP Server**で**On**を選択します。
   b. **Server IP**リストから最初のIPアドレスを選択します。
   c. 開始IPアドレスと終了IPアドレスを入力します。
   d. リース時間を入力します。
   e. ゲートウェイアドレスを入力します。このフィールドはオプションです。

   開始IPアドレスと終了IPアドレスが、DHCPサーバーと同じネットワークサブネット上にあること

を確認します。

図267 DHCPサーバーの設定



3. **OK**をクリックします。

DHCPクライアント情報を表示する

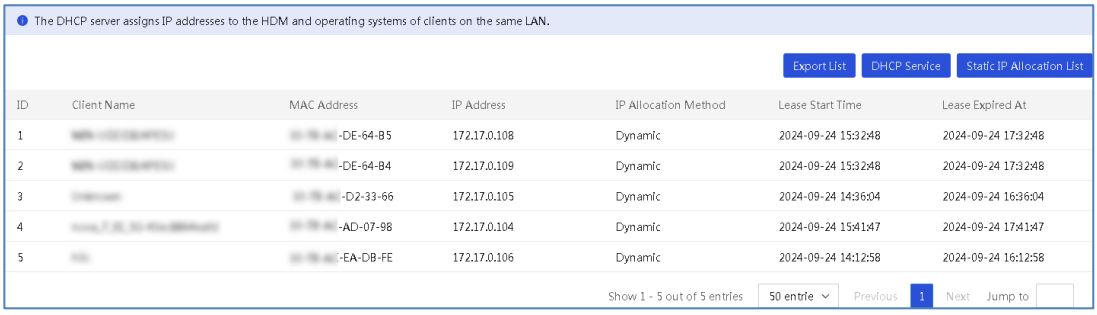
このタスクについて

DHCPサーバーからIPアドレスを取得するDHCPクライアントに関する情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **DHCP Server**を選択します。
2. **DHCP Service**をクリックします。このページには、すべてのDHCPクライアントに関する情報が表示されます。

図268 DHCPクライアント情報



3. (任意)DHCPクライアントのIPアドレスがDHCPサーバーによって静的に割り当てられている場合、このクライアントの**Lease Expired At**フィールドには**Release**と表示されます。**Release**をクリックすると、クライアントのIPアドレスとMACアドレスのバインドを解除できます。

パラメータ

- **Client Name**: DHCPクライアントの名前。
- **MAC Address**: DHCPクライアントのMACアドレス。
- **IP Address**: DHCPクライアントがDHCPサーバーから取得するIPアドレス。
- **IP Allocation Method**: DHCPクライアントがIPアドレスを取得する方法。オプションは次のとおりです。
  - **Dynamic**: DHCPサーバーは、IPアドレス範囲からIPアドレスを動的に選択して、DHCPクライアントに割り当てます。
  - **Static**: DHCPサーバーは、IPアドレスをDHCPクライアントに静的にバインドします。
- **Lease Start Time**: DHCPクライアントがIPアドレスを取得した時刻。
- **Lease Expired At**: IPアドレスの有効期限が切れる時刻。

静的IP割り当ての設定

このタスクについて

この機能を使用すると、DHCPクライアントに割り当てられたスタティックIPアドレスに関する情報の表示、DHCPクライアントへのスタティックIPアドレスの割り当て、およびスタティックIPアドレスの解放を行うことができます。

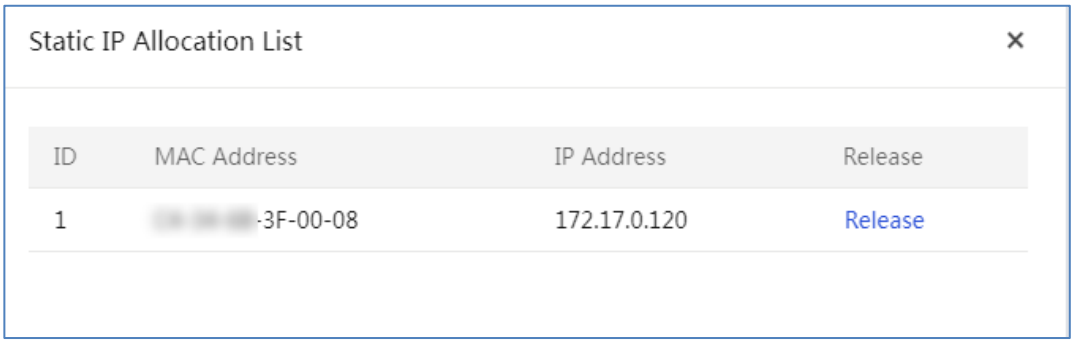
制約事項とガイドライン

静的IP割り当てが有効になるのは、DHCPサーバーがイネーブルになっている場合だけです。

手順

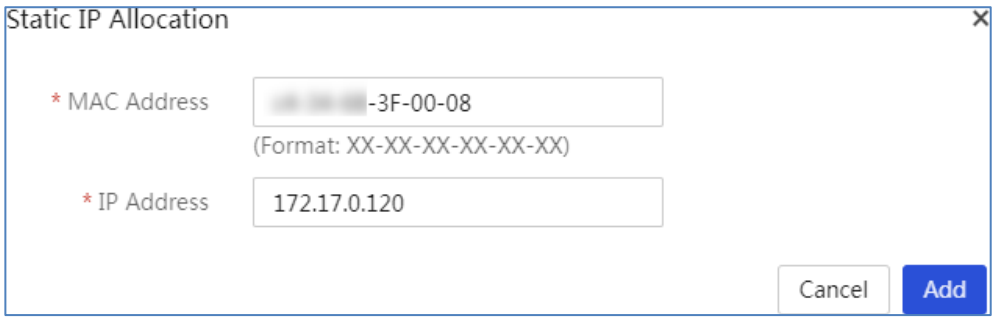
1. ナビゲーションペインで、**Menu** > **Tools** > **DHCP Server**を選択します。
2. **tatic IP Allocation List**をクリックします。表示されるダイアログボックスに、DHCPクライアントに割り当てられているすべての静的IPアドレスが表示されます。

   図269 Static IP Allocation Listページ



3. (任意)DHCPクライアントに割り当てられたIPアドレスを再要求するには、**Release**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。
4. (オプション) **Add**をクリックして、静的IPアドレスをDHCPクライアントに割り当てます。表示されたダイアログボックスで、MACアドレスとIPアドレスを入力します。

   図270 静的IP割り当ての設定



5. **Add**をクリックします。

パラメータ

- **MAC Address**: DHCPクライアントのMACアドレス。MACアドレスは、ブロードキャストまたはマルチキャストMACアドレスにはできません。
- **IP Address**: DHCPクライアントに静的に割り当てられたIPアドレス。IPアドレスには、次の制約事項があります。
  - IPアドレスは、DHCPサーバーと同じネットワークセグメント上にある必要がありますが、

DHCPサーバーのアドレスと同じにすることはできません。

- IPアドレスは、DHCPサーバーに指定されたIPアドレスの範囲外でもかまいません。
- IPアドレスをマルチキャストまたはブロードキャストアドレスにすることはできません。
- IPアドレスは未使用のIPアドレスである必要があります。

IP割り当て一覧をエクスポートする

このタスクについて

DHCPクライアントに割り当てられているIPアドレスのリストをローカルファイルにエクスポートするには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **DHCP Server**を選択します。
2. **Export List**をクリックします。UniSystemは、静的に割り当てられたIPアドレスをEXCELファイルにエクスポートします。

PXEデプロイメントの設定

このタスクについて

重要:

- PXEを使用してオペレーティングシステムを展開する必要がない場合は、PXE機能を有効にしないことをお勧めします。
- 別のデバイスがUniSystemと同じネットワーク上にあり、そのデバイスがDHCPを介して動的にIPアドレスを取得するように構成されている場合、PXE機能を有効にすると、デバイスのIPアドレスが変更されることがあります。ネットワーク上の他のデバイスに影響を与えないようにするには、UniSystem ネットワークと PXE 展開用デバイスのネットワークを分離する必要があります。

PXEデプロイメントを使用すると、PXEクライアントは必要なOSをネットワーク経由でダウンロードし、自動的に起動してOSをインストールできます。この機能は、AEモジュールでUniSystemが実行されている場合にのみ使用できます。

PXEインストールプロセスは次のとおりです。

1. PXEクライアントは、自身のPXEイーサネットアダプターから起動し、ネットワーク上のDHCPサーバーにIPアドレスとブートファイルの場所を要求します。
2. DHCPサーバーは、IPアドレスとブートファイルの場所をPXEクライアントに返します。
3. PXEクライアントは、ネットワーク上のTFTPサーバーからブートファイルをダウンロードして実行し、ブートファイルの実行結果に基づいて、TFTPサーバーからカーネルおよびファイルシステムをロードする。
4. PXEクライアントは、OSインストール画面に入り、HTTPを介してOSをインストールします。

この機能を使用してインストールされたRedHatおよびCentOSの場合、デフォルトのrootパスワードは**Password@**です。この機能を使用してインストールされたその他のLinux OSの場合、デフォルトのrootパスワードは**123456**です。

サポートされるOS

- CentOS 6.8(64ビット)
- CentOS 7.2(64ビット)
- CentOS 7.4(64ビット)
- Red Hat Enterprise Linux 6.3(64ビット)
- Red Hat Enterprise Linux 6.8(64ビット)
- Red Hat Enterprise Linux 7.2(64ビット)
- Red Hat Enterprise Linux 7.4(64ビット)
- Red Hat Enterprise Linux 7.5(64ビット)

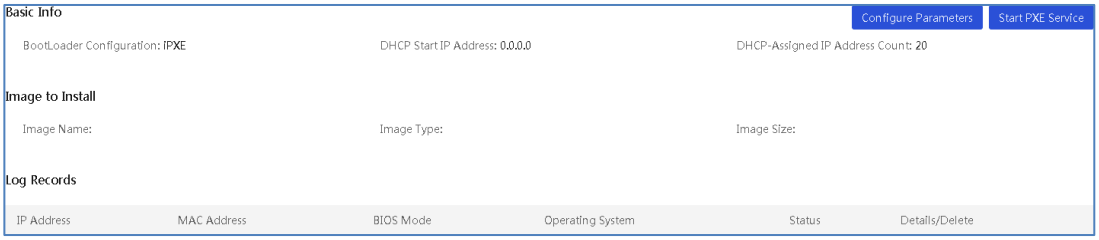
制約事項とガイドライン

- PXEクライアントには、PXE対応のEthernetアダプターが必要です。
- PXEクライアントは、PXE展開のDHCP機能を使用してIPアドレスを取得します。
- IP範囲には、ブロードキャストアドレスは含まれません。
- IP範囲内のIPアドレスは、ネットワーク上の既存のIPアドレスと競合しません。
- PXEデプロイメントでは、ポート番号67および69がそれぞれDHCPサービスおよびTFTPサービスとして使用されます。PXEデプロイメントを正常に開始するには、ポート番号67および69が他のサービスによって使用されていないことを確認してください。
- PXEデプロイメントのDHCP機能は、DHCPサーバー機能と排他的です。ポートの競合が発生するため、2つの機能を同時に構成することはできません。
- PXEデプロイメントを使用してブレードサーバーにOSをインストールする場合は、次の制約事項およびガイドラインに従ってください。
  - iPXEブートローダーを使用すると、メザニンカードとレガシーブートモードでインストールされたサーバーへのPXE展開が失敗します。この場合は、PXELINUXまたはGRUB2ブートローダーを使用してください。
  - IP範囲の開始IPアドレスは、AEモジュールのネットワークポート**vmng**のIPアドレスと同じサブネット上にある必要があります。
  - IP範囲には、AEモジュールのネットワークポート**vmng**のIPアドレスは含まれません。
  - 192.250.0.0～192.250.255.255の範囲のIPアドレスは、内部使用のために予約されています。これらのIPアドレスをIP範囲に含めないでください。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **PXE Deployment**を選択します。

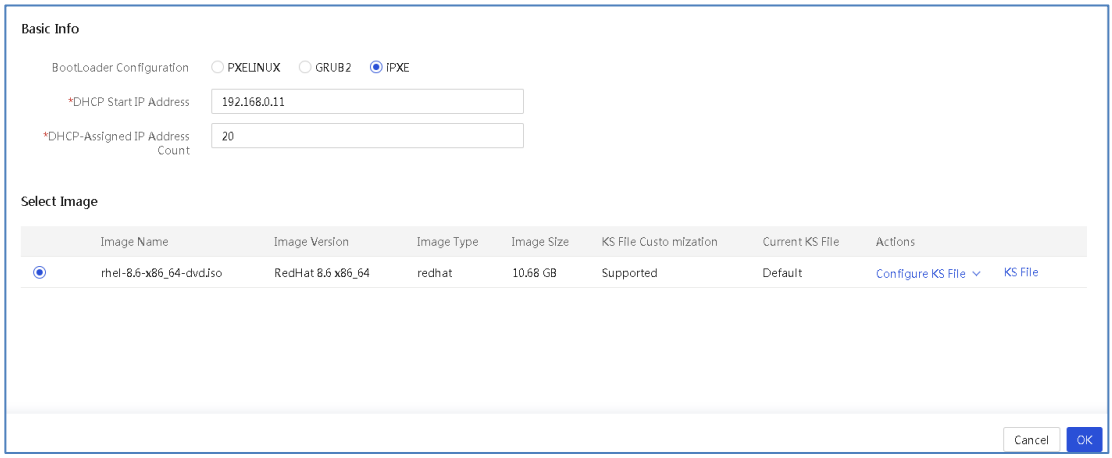
図271 PXEデプロイメントページ



2. **Configure Parameters**をクリックし、次のようにPXE展開パラメータを設定します。
   a. ブートローダーコンフィギュレーションモードを選択します。
   b. DHCP開始IPアドレスとDHCP割り当てIPアドレスカウントを入力します。

      PXEの展開中に、DHCPサーバーはこの範囲のIPアドレスをサーバーに割り当てます。OSのインストール後、サーバーはこのIPアドレスをシステムIPアドレスとして使用します。
   c. イメージリストからイメージを選択します。

図272 PXEインストールパラメーターの設定



3. **OK**をクリックします。

パラメーター

- **BootLoader Configuration**:サーバーにインストールするOSのブートローダー。
  - **PXELINUX**: SysLinuxから派生したPXELINUXを使用すると、クライアントはネットワークサーバーから起動できます。
  - **GRUB2**: GNU GRUBとも呼ばれます。GRUB2は、GNUプロジェクトのマルチOSブートローダーです。GRUB2を使用すると、クライアントは複数のOSを同時に使用し、想定されたOSからブートできます。
  - **iPXE**: 拡張PXE実装を提供します。複数のプロトコルと互換性があります。iPXEを使用することをお勧めします。
- **DHCP Start IP Address:** IP割り当てに使用されるIPプールの最初のIPアドレス。
- **DHCP-Assigned IP Address Count:** IP割り当てに使用されるIPプール内のIPアドレスの数。

PXE OSインストールパラメーターの設定

KSファイルには、rootパスワード、ユーザー名、ユーザーパスワード、パーティション設定、ソフトウェアパッケージ設定、言語など、サーバーのOSをインストールするためにPXEが使用するパラメーターが含まれています。

UniSystemには、PXE定義のデフォルトパラメーターを含むデフォルトKSファイルと、ユーザーがパラメーターを編集してデフォルト設定を復元できるカスタムKSファイルが用意されています。

現在のソフトウェアバージョンでは、UniSystemはRedHatとCentOSのKSファイルのみをサポートしています。

カスタムKSファイルを編集する

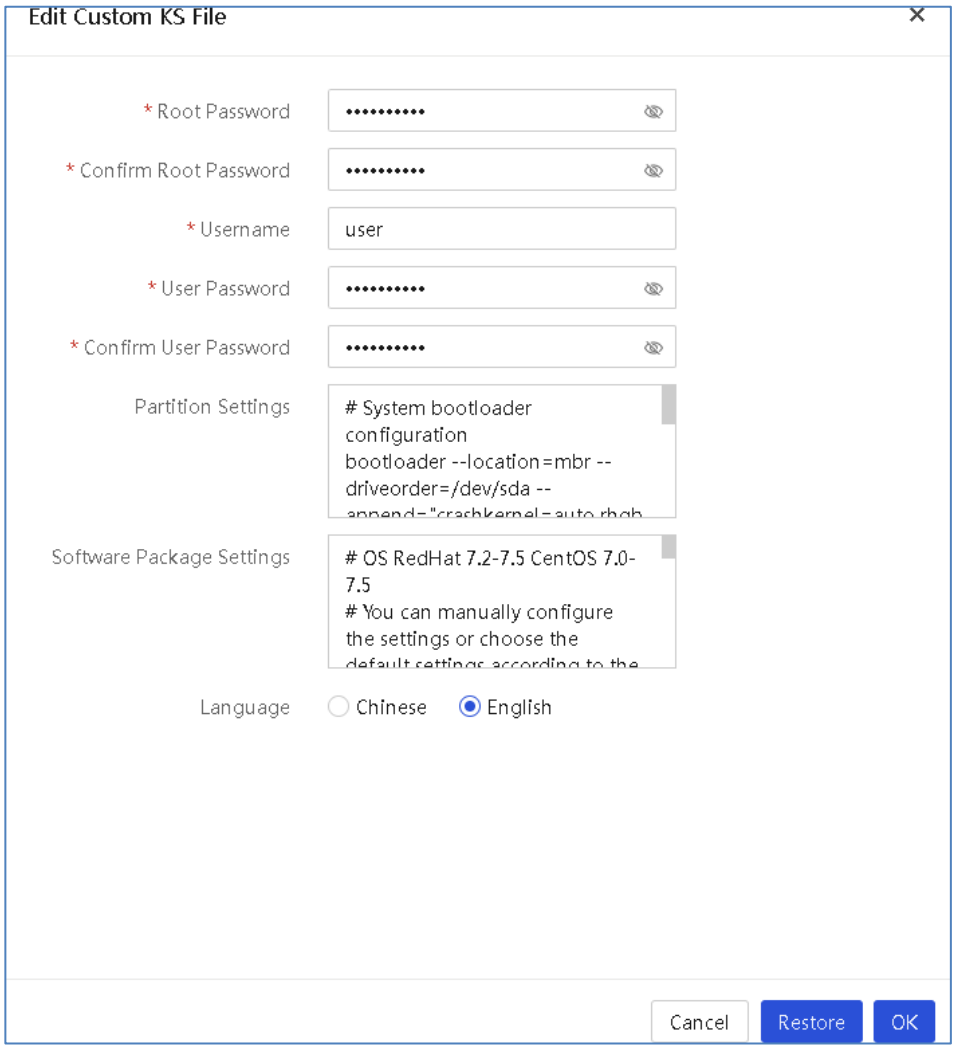
このタスクについて

カスタムKSファイルの設定を編集したり、ファイルのデフォルト設定を復元したりするには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **PXE Deployment**.を選択します。
2. **Configure Parameters**をクリックします。
3. イメージを選択し、イメージの**Actions**列で**Configure KS File**をクリックします。そして、**Configure Custom KS**を選択します。
4. **Edit Custom KS File**ページで、次のいずれかのタスクを実行します。
   - カスタムKSファイルを手動で編集するには、必要に応じてパラメータを編集し、**OK**をクリックします。
   - カスタムKSファイルのデフォルト設定を復元するには、**Restore**をクリックします。

図273 カスタムKSファイルの編集



パラメータ

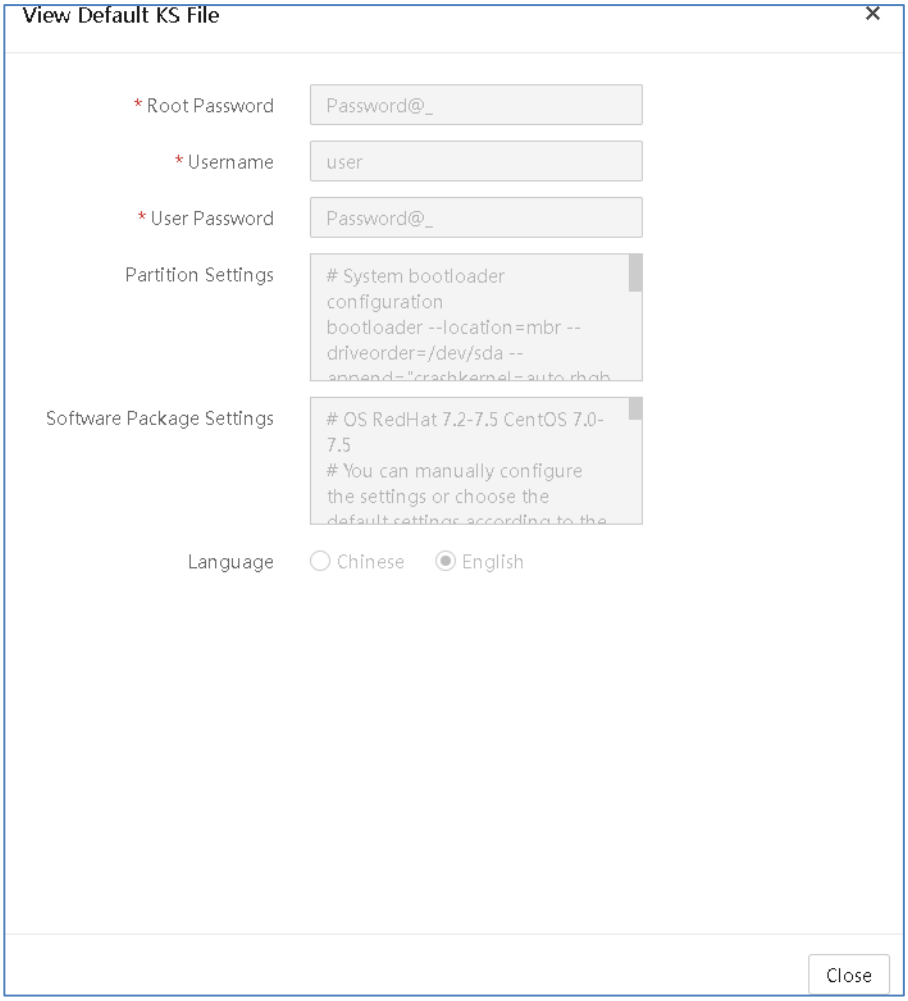
- **Root Password**: 管理者のパスワード。
- **Username**: 作成する新しいユーザーのユーザー名。
- **User Password**: ユーザーのパスワード。
- **Partition Settings**: OSインストール用のパーティション設定。
- **Software Package Settings**: OSのインストールに使用するソフトウェアパッケージの設定。
- **Language**: インストールするOSの言語。オプションには、中国語と英語があります。

既定のKSファイルを表示する

1. ナビゲーションペインで、**Menu** > **Tools** > **PXE Deployment**を選択します。
2. **Configure Parameters**をクリックします。
3. イメージを選択し、イメージの**Actions**列で**Configure KS File**をクリックして、**View Default KS**を選択します。

   デフォルトのKSファイルの設定は、開いたページで確認できます。

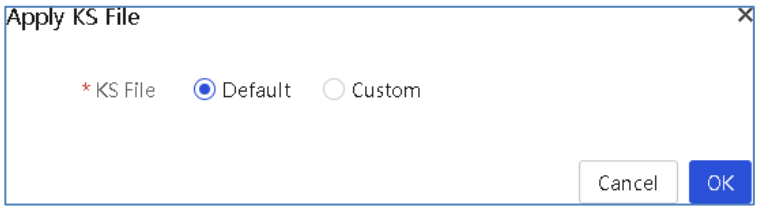
図274 デフォルトのKSファイルの表示



KSファイルを適用する

1. ナビゲーションペインで、**Menu** > **Tools** > **PXE Deployment**を選択します。
2. **Configure Parameters**をクリックします。
3. イメージを選択し、イメージの**Actions**列で**KS File**をクリックします。
4. KSファイルを選択します。オプションには、デフォルトとカスタムがあります。PXEは、指定されたKSファイルの設定を使用して、サーバーのOSをインストールします。

図275 KSファイルの適用



制約事項とガイドライン

- カスタムKSファイルは、システムがOSソフトウェアイメージをアップロードするときに自動的に生成されます。カスタムKSファイルのパラメータ設定は、デフォルトKSファイルのパラメータ設定と同じです。
- 使用中のOSでは、カスタムKSファイルを編集したり、KSファイルのデフォルト設定を復元したりすることはできません。
- 構成の復元中に、カスタムKSファイルのイメージ名とOSバージョンが復元に使用された構成ファイルのものと同じである場合、UniSystemはカスタムKSファイルを復元します。

ソフトウェアのプッシュとインストール

このタスクについて

このモジュールを使用すると、FIST SMSまたは汎用ソフトウェアをUniSystemが管理するサーバーのOSにリモートでインストールできます。

FIST SMSは、HDMおよびUniSystem管理を強化するために、管理対象サーバーのOSにインストールされるソフトウェアです。FIST SMSがサーバーのOSに正常にインストールされると、FIST SMSが自動的に実行され、UniSystemはこのサーバーをFIST SMSデバイスとして追加します。

汎用ソフトウェアとは、UniSystemにインストールするすべてのソフトウェアを指します。この機能は、ソフトウェアインストールパッケージをプッシュし、スクリプトをサーバーのOSにインストールし、インストールスクリプトを実行してソフトウェアをインストールします。

メモ:

- FIST SMSインストール機能は、バージョン2.00.16以降で使用できます。
- 一般的なソフトウェアインストール機能は、バージョン2.00.33以降で使用できます。
- この機能は、FIST SMS-1.03.08以降のバージョンだけをサポートしています。

制約事項とガイドライン

FIST SMSのインストールが失敗しないように、インストールパッケージを変更しないでください。

サーバーでファイアウォール機能が有効になっている場合、FIST SMSをサーバーにインストールした後、システムは自動的に次のタスクを実行します。

- FIST SMSで使用されるポート(ポート12580および6900)をファイアウォールの許可リストに追加します。これらのポートは、FIST SMSサーバーの再起動後も許可リストに残ります。
- ファイアウォール設定でICMPv 4受信規則を有効にして、FIST SMSサーバーをUniSystemで管理できるようにします。

前提条件

FIST SMSをインストールするには、次のガイドラインに従ってください。

- FIST SMSを使用してインストールするサーバーにOpenJDK 1.8(64ビット)をインストールします。FISTから
SMS-1.37では、FIST SMSをWindowsオペレーティングシステムにインストールする場合、事前にOpenJDKソフトウェアを構成する必要はありません。
- FIST SMSを正常に起動するには、FIST SMS専用のポート12580を使用します。
- Windowsサーバーでwinrmサービスが正しく構成されていること、またはLinuxサーバーでsshdサービスが開始されていることを確認します。

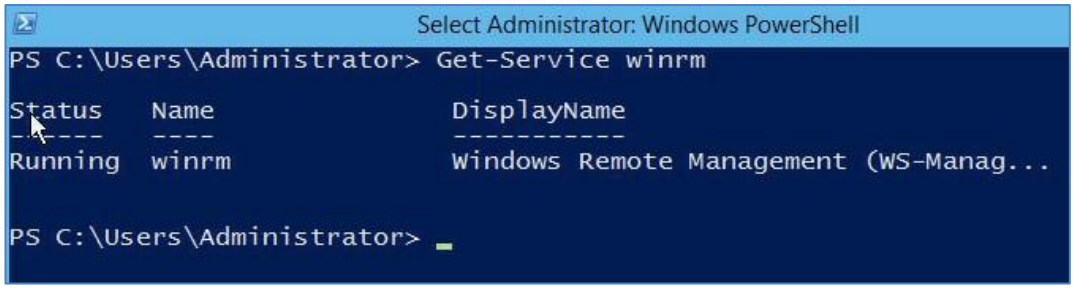
一般的なソフトウェアをインストールするには、次のガイドラインに従ってください。

- ソフトウェアインストールパッケージとインストールスクリプトを事前に準備し、.tar.gz形式のインストールファイルにまとめてパッケージ化します。
- 次の理由により、一般的なソフトウェアをインストールできない場合があります。
    - インストールスクリプトの実行時間が上限を超えています。インストールスクリプトの実行時間の上限は、Windowsシステムでは20秒、Linuxシステムでは20分です。
    - インストールスクリプトには、pauseステートメントなどの対話式ステートメントが含まれています。
- インストールスクリプトの拡張子は、OSの種類によって異なります。
    - Windowsオペレーティングシステムでは、インストールスクリプトに**install.bat**という名前を付ける必要があります。
    - Linuxオペレーティングシステムでは、インストールスクリプトに**install.sh**という名前を付ける必要があります。
- Windowsサーバーでwinrmサービスが正しく構成されていること、またはLinuxサーバーでsshdサービスが開始されていることを確認します。

Windowsサーバーでwinrmサービスの状態を確認する

1. Windowsシステムに管理者としてログインし、PowerShellを起動します。
2. **`Get-Service winrm`**コマンドを実行して、winrmサービスの状態を確認します。
    - サービスのステータスが**Running**の場合、アクションは必要ありません。
    - サービスの状態が**Stopped**の場合は、次の手順に進みます。

図276 winrmサービスの状態の確認



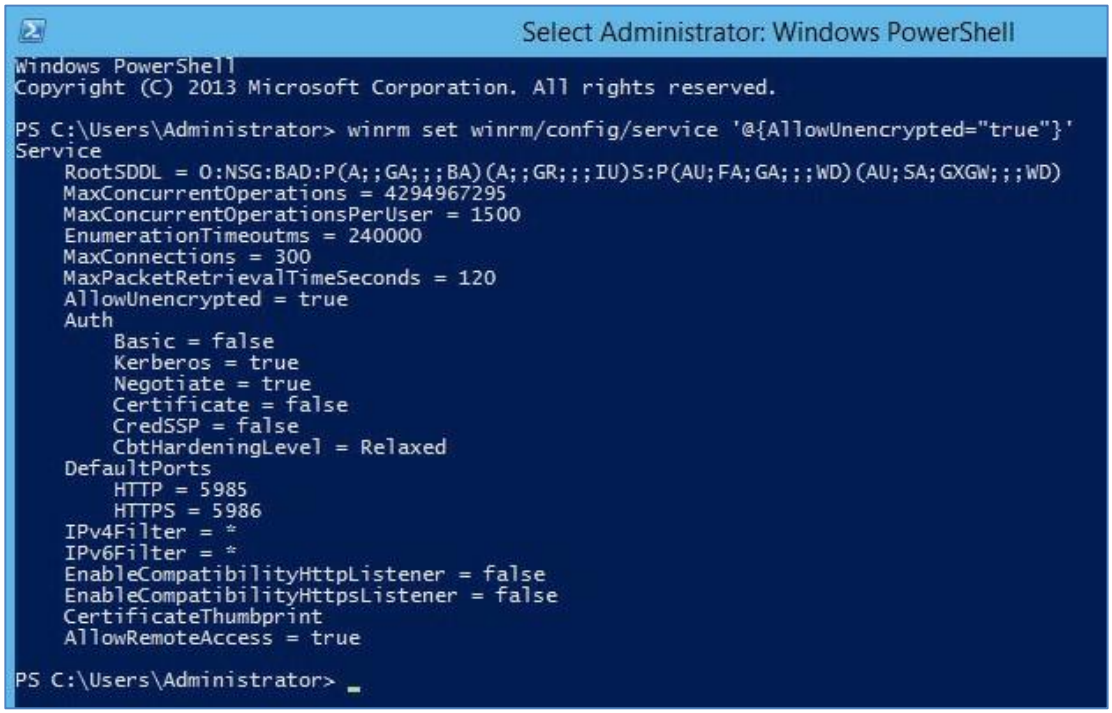
3. **`winrm quickconfig`**コマンドを実行して、winrmサービスを開始します。

図277 winrmサービスの起動



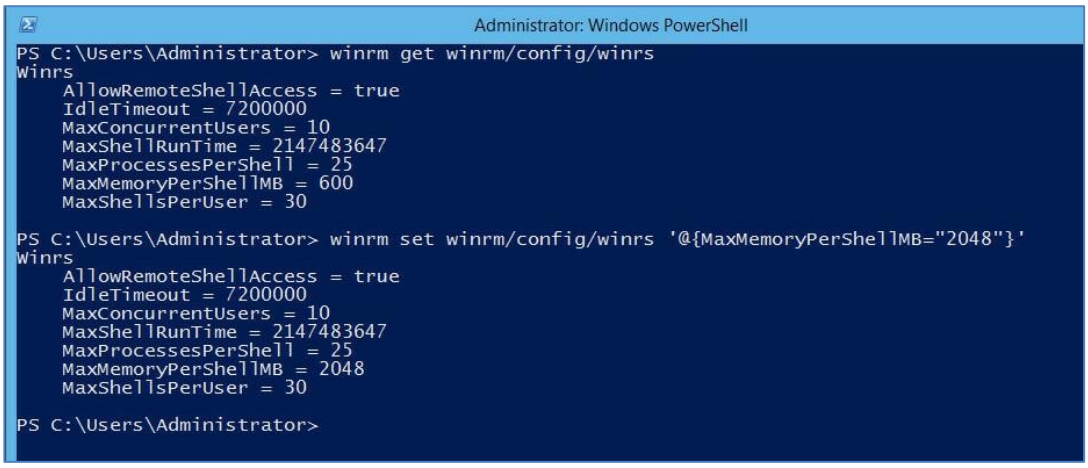
4. 暗号化されていない送信を許可するには、**`winrm set winrm/config/service '@{AllowUnencrypted="true"}'`**コマンドを実行します。

図278 暗号化されていない送信の許可



5. **winrm set winrm/config/winrs** '@{**MaxMemoryPerShellMB="***memory-size***"}'コマンドを実行して、PowerShellの最大メモリーサイズをサーバーの物理メモリーの1/16より大きい値に設定します。

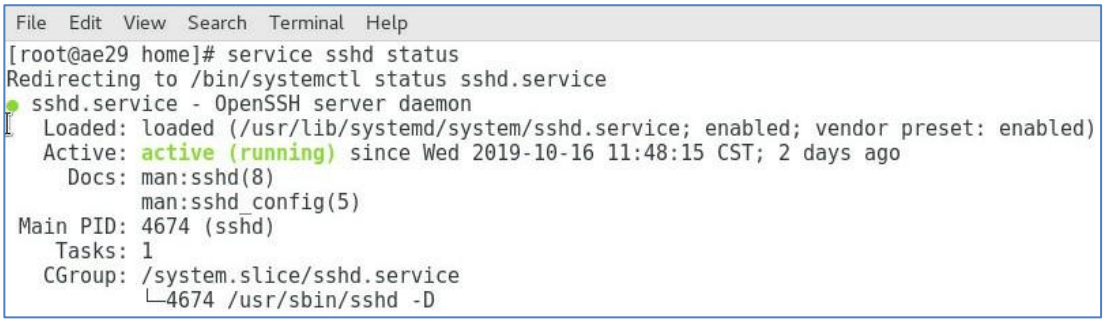
図279 PowerShellの最大メモリーの設定



Linuxサーバーでのsshdサービスのステータスの確認

1. Linuxシステムに管理者としてログインします。
2. sshdサービスをインストールし、**service sshd start**コマンドを実行してサービスを開始します。サービスがインストールされている場合は、**service sshd status**コマンドを実行してsshdサービスのステータスを確認します。
   - サービスステータスが**active**の場合、アクションは必要ありません。
   - サービスステータスが**inactive**の場合は、次の手順に進みます。

   図280 sshdサービスステータスの確認



3. **service sshd start**コマンドを実行して、sshdサービスを開始します。sshdがインストールされていないことを示すメッセージが表示された場合は

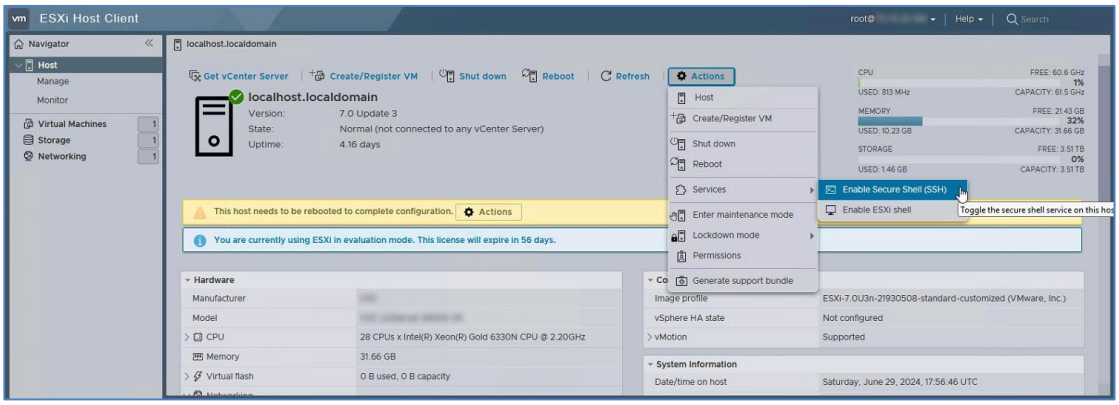
VMware ESXiホストの設定

SSHサービスを有効にする

VMware ESXiホストにソフトウェアをインストールする場合は、次の手順に従ってSSHを使用できるようにします。

1. vSphereクライアントを管理者として使用して、VMware ESXiホストにログインします。
2. 左側のナビゲーションペインで、**Host**を選択します。

図281 SSHサービスの有効化



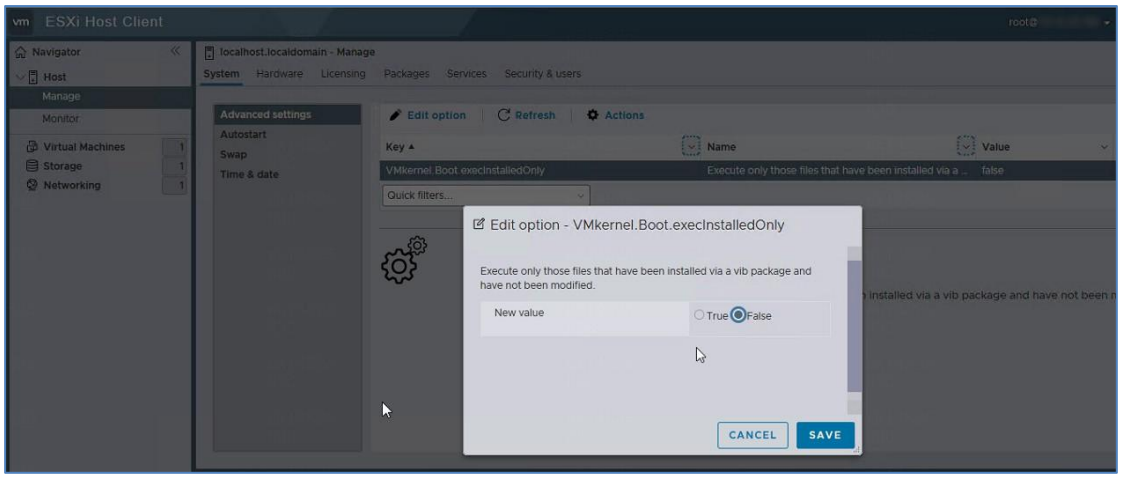
3. **Actions** > **Services** > **Enable Secure Shell (SSH)**を選択します。
4. SSHサービスが開始されると、SSHクライアントを使用してESXiホストに接続できます。

execInstalledOnlyを無効にする

VMware ESXiオペレーティングシステムにソフトウェアをインストールする場合は、execInstalledOnlyオプションを無効にする必要があります。execInstalledOnlyを無効にするには、以下の手順に従ってください。

1. vSphereクライアントを管理者として使用して、VMware ESXiホストにログインします。
2. 左側のナビゲーションペインで、**Host** > **Manage** > **System**を選択します。
3. **VMkernel.Boot.execInstalledOnly**を選択し、**Edit**をクリックします。
4. **False**を選択し、**Save**をクリックします。

図282 execInstalledOnlyの無効化



手順

1. ナビゲーションペインで、**Menu** > **Tools** > **Push and Install Software**を選択します。
2. インストールファイルの種類を選択します。
3. デバイスリストをアップロードするには、次の手順を実行します。

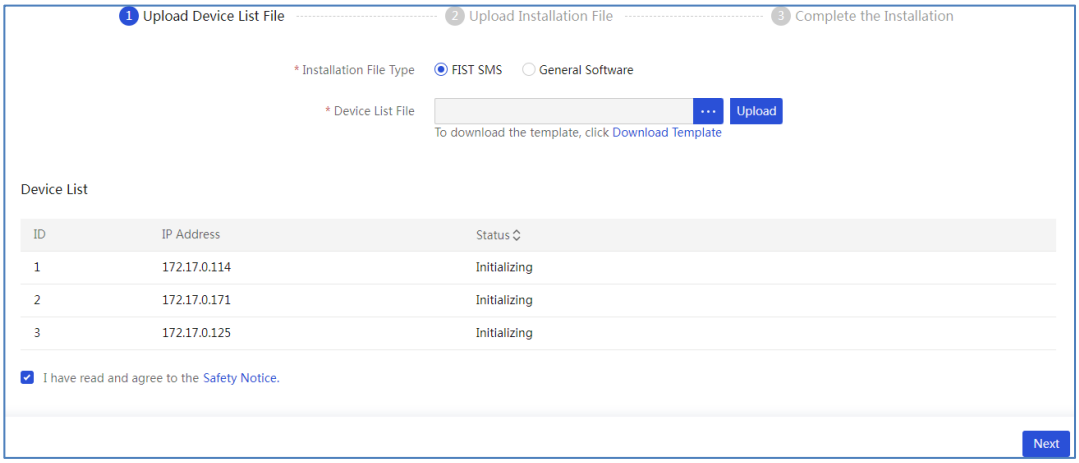
a. (任意)**Device List File**の下の**Download Template**をクリックして、デバイスリストテンプレートをダウンロードし、デバイスリストテンプレート内のデバイスを編集します。

b. **Device List File**フィールドで…をクリックします。

c. 表示されたダイアログボックスで**Browse**をクリックし、デバイスリストファイルを選択して**OK**をクリックします。

d. **Upload**をクリックします。**Device List**領域には、FIST SMSまたは汎用ソフトウェアをインストールできるデバイスのリストが表示されます。

図283 FIST SMSのインストール



4. **Next**をクリックします。

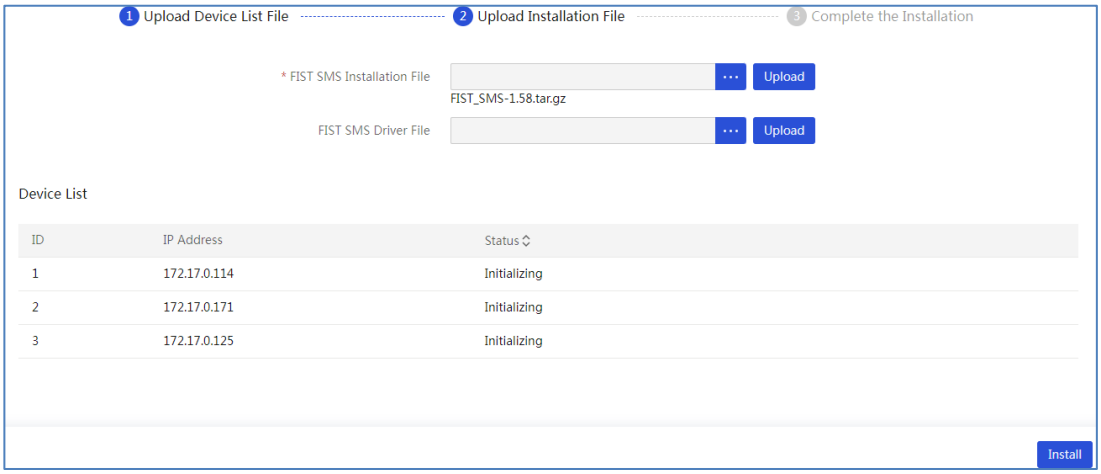
5. FIST SMS、汎用ソフトウェアインストールファイル、またはFIST SMSドライバファイルをアップロードするには、次の作業を実行します。

   a. **FIST SMS Installation File**、**General Software Installation File**、または**FIST SMS Driver File**フィールドで…をクリックします。

   b. 表示されたダイアログで、**Browse**をクリックし、ターゲットファイルを選択して**OK**をクリックします。

   c. **Upload**.をクリックします。アップロードされたファイルの名前が表示されます。

図284 インストールファイルのアップロード



6. **Install**をクリックします。システムは、デバイスリスト内のサーバーにFIST SMSまたは一般ソフトウェアのインストールを開始します。時間がかかりますので、手続きが終わるまでお待ちください。

一般的なソフトウェアを正常にインストールした後、**Logs**列に情報を表示できます。詳細なログを表示するには、デバイスリストでデバイスを選択し、**Download**をクリックします。

7. **Finish**をクリックします。

リモートコマンド

メモ:

デフォルトのadminユーザー、および管理者の役割とすべてのリソースに対する権限を持つユーザーのみはこの機能をサポートしていません。

この機能により、ユーザーは、バルク電源オンやバルク電源オフなどのバルクコマンド実行のニーズを満たすために、基本的なデバイス情報を照会して取得できます。この機能により、ユーザーは、管理ソフトウェアまたはツールを切り替えることなく、タスクを実行したり、情報を取得したりできます。これにより、管理ソフトウェアのO&M機能とユーザーエクスペリエンスが向上します。

pingコマンド

このタスクについて

pingは、ターゲットデバイスにデータパケットを送信し、その応答を待ってネットワーク接続を評価することにより、ネットワーク接続性をテストするためのツールです。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **Remote Commands**を選択します。次に、**Ping Commands**をクリックします。
2. **Execute Commands**フィールドにIPアドレスを入力します。
3. **Execute**をクリックします。次に、実行が終了するまで待ちます。

   Executeボタンの下に実行結果が表示されます。
4. 実行結果をクリアするには、**Clear**をクリックします。

制約事項とガイドライン

- pingコマンドは、IPv4、IPv6、およびfe80アドレスをサポートしますが、ドメインアドレスはサポートしません。
- pingコマンドは、WindowsとLinuxをサポートしています。
- pingコマンドの実行結果は一時的なデータです。ページを更新すると、実行結果はクリアされます。

IPMIコマンド

この機能を使用すると、デバイスに対してIPMIコマンドをリモートで実行できます。IPMIコマンドは、複数のデバイスに対して一括して実行できます。この機能を使用すると、リモートデバイスの管理と監視、再起動、電源制御、温度センサークエリなどのIPMIコマンドの実行が容易になり、デバイスのリモート操作と管理が可能になります。

手順

1. ナビゲーションペインで、**Menu>Tools>Remote Commands**を選択し、**IPMI Commands**をクリックします。
2. **Execute Commands**フィールドには、IPMIコマンドのコマンド部分だけを入力します。

- コマンドパーツを追加するには、まず⊕をクリックして新しい入力ボックスを追加します。
- 入力ボックスを削除するには、アイコン🗑をクリックします。

3. **Select**をクリックします。表示されたページで、一覧のデバイス名の横にあるチェックボックスをオンにしてデバイスを追加し、**OK**をクリックします。
4. **Execute**をクリックします。次に、実行が終了するまで待ちます。デバイスリストが更新されます。
5. デバイスの詳細な実行結果を表示するには、リストでデバイスのIPアドレスの横にある矢印アイコンをクリックします。
6. 実行結果をExcelファイルにエクスポートするには、**Export Result**をクリックします。
7. 実行結果をクリアするには、**Clear**をクリックします。

制約事項とガイドライン

- 一度に最大3つのコマンドを実行できます。システムはこれらのコマンドの有効性を確認しません。
- IPMIコマンドを一度に実行する場合、最大100台のデバイスを選択できます。
- IPMIコマンドが実行されると、システムは今後のクエリーのために履歴データを一時的に保存します。**Clear**をクリックするか、サービスを再起動すると、履歴データがクリアされます。別のIPMIコマンドを実行するには、まず履歴データをクリアする必要があります。

Redfishコマンド

この機能を使用すると、デバイスに対してRedfishコマンドをリモートで実行できます。Redfishコマンドは複数のデバイスで一括して実行できます。Redfishコマンドを実行すると、システムに結果が表示され、エクスポート機能が提供されるため、ユーザーは簡単に分析と処理を行うことができます。

手順

1. ナビゲーションペインで、**Menu** > **Tools** > **Remote Commands**を選択します。次に、**Redfish Commands**をクリックします。
2. コマンドの種類を選択します。
3. Redfishコマンドのコマンド部分のみを入力します。
4. **GET**以外のコマンドタイプを選択した場合は、**Request Parameter**フィールドのためにJSON形式でリクエストパラメーターを入力します。
5. **Select**.をクリックします。表示されたページで、一覧のデバイス名の横にあるチェックボックスをオンにしてデバイスを追加し、**OK**をクリックします。
6. **Execute**をクリックします。次に、実行が終了するまで待ちます。デバイスリストが更新されます。
7. ›デバイスの詳細な実行結果を表示するには、リストでデバイスのIPアドレスの横にあるアイコンをクリックします。
8. 実行結果をExcelファイルにエクスポートするには、**Export Result**をクリックします。
9. 実行結果をクリアするには、**Clear**をクリックします。

制約事項とガイドライン

- 一度に実行できるRedfishコマンドは1つだけです。1つのRedfishコマンドに対して、最大100個のオンラインデバイス(G6以降)を選択できます。
- Redfishコマンドが実行された後、システムは将来のクエリーのために履歴データを一時的に保存します。**Clear**をクリックするか、サービスを再起動すると、履歴データがクリアされます。別のRedfishコマンドを実行するには、まず履歴データをクリアする必要があります。
- RedfishコマンドのリクエストパラメーターはJSONフォーマットである。ベストプラクティスとし

て、関連するRedfishドキュメントに従ってリクエストパラメーターを指定する。

UniSystemをUniSystemプラグインとしてvCenter Serverに組み込む

この機能について

UniSystemをプラグインとしてvCenter Serverに組み込むことができます。その後、vCenter Serverインスタンスに直接接続できるアプリケーションであるvSphere Clientを介してUniSystemにアクセスできます。

前提条件

vCenter ServerのIPアドレス、ログインユーザー名、およびパスワードを取得します。

制約事項とガイドライン

- Google Chrome 85以降のバージョンを使用している場合は、次のように入力します。図285に示すように、デフォルトの**SameSite by default cookies**を無効にするには、アドレスバーに**chrome://flags/#same-site-by-default-cookies**を入力します。別のブラウザを使用してUniSystemログインプロセスに行き詰まった場合は、同様の方法でブラウザのキャッシュ設定を編集してみてください。

  図285 ブラウザのキャッシュ設定の編集



- UniSystemの登録が完了した後、以前のバージョンまたは同じバージョンのUniSystemを再度登録する必要がある場合は、まず登録されているUniSystemプラグインをアンインストールします。以前に登録されたUniSystemプラグインをアンインストールせずにUniSystemを直接登録すると、vCenter Serverは新しく登録されたUniSystemプラグインを展開しません。

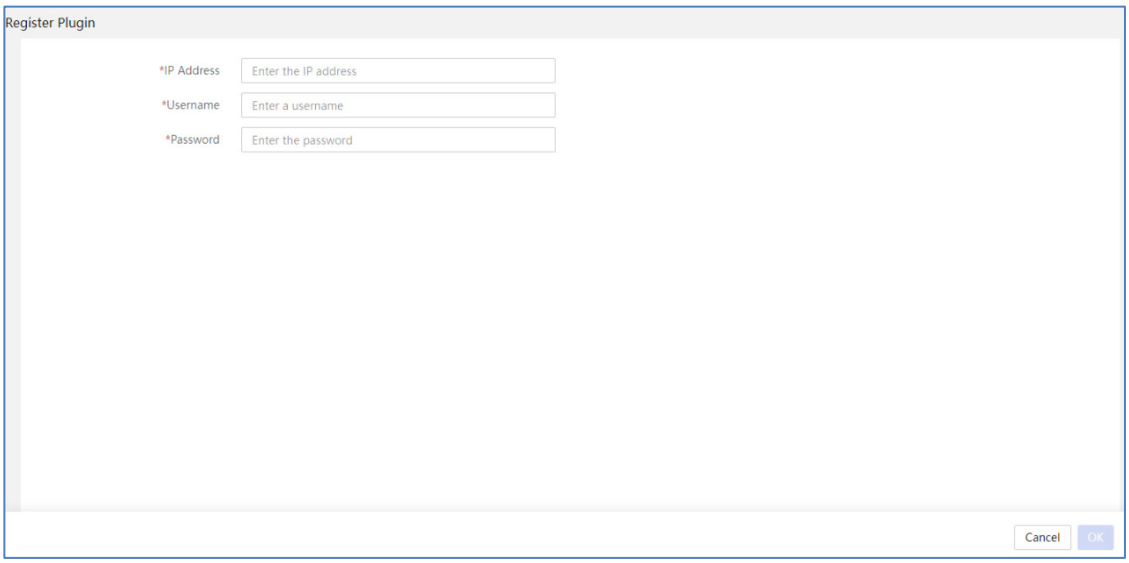
UniSystemプラグインのインストール

1. UniSystemにログインするには、アドレスバーに**https://***UniSystem ip address*:*https port*と入力します。次に、図286に示すように、アドレスバーに**https://***UniSystem ip address*:*https port*/**server/0/register-plugin**と入力して、**Register Plugin**ページにアクセスします。

重要:

UniSystemプラグイン登録後にUniSystemに正常にアクセスするには、HTTPSを使用してUniSystemにログインします。

図286 Register Pluginページ



2. vCenter ServerのIPアドレス、ユーザー名、およびパスワードを入力し、**OK**をクリックします。
3. 登録が完了したら、vSphere Clientにログインします。vSphere Client 経由で UniSystem にアクセスするには、**Shortcuts**ページの UniSystem アイコンをクリックします。

UniSystemプラグインのアンインストール

vCenter 7.0からのUniSystemプラグインのアンインストール

デプロイされたUniSystemプラグインをアンインストールするには、vCenter Serverが提供するvSphere Client SDKを使用します(詳細については、https://www.vmware.com/support/developer/webclient/index.htmlのページにアクセスしてください)。アンインストールには、拡張登録ツールを使用します。

- UniSystemプラグインをアンインストールするコマンド:

  ```
  $tools/extension-registration.bat -action unregisterPlugin -k sample.plugin -url
  https://vc-svr.example.com/sdk -u administrator@vsphere.local -p secret
  ```

- コマンドパラメータの説明:
  - **-action**: 実行するアクションを指定します。この例では**unregisterPlugin**です。
  - **-k** *sample.plugin*: ターゲットプラグインの識別子(この例では**com.h3c.fist.localui**)を指定します。
  - **-url** *https://vc-svr.example.com/sdk*: vCenter Serverが提供するSDKリソースのURLを指定します(例:https://192.168.128.117/sdk)。
  - **-u** *administrator@vsphere.local:* vCenter Serverのログインユーザー名を指定します。
  - **-p** *secret:* vCenter Serverのログインパスワードを指定します。
- UniSystemプラグインをアンインストールするコマンドの例:

  ```
  D:\vsphere-client-sdk-6.7.0.40000-14186396\html-client-sdk\tools\vCenter
  plugin registration\prebuilt>extension-registration.bat -action
  unregisterPlugin -k com.h3c.fist.localui -u administrator@vsphere.local -
  p ***** -url https:// 192.168.128.117/sdk
  ```

vCenter 8.0からのUniSystemプラグインのアンインストール

デプロイされたUniSystemプラグインをアンインストールするには、vCenter Serverが提供する

vSphere Client SDKを使用します(詳細については、https://www.vmware.com/support/developer/webclient/index.htmlのページにアクセスしてください)。アンインストールには、拡張登録ツールを使用します。

- UniSystemプラグインをアンインストールするコマンド:

```
$tools/extension-registration.bat -action unregisterPlugin -k
sample.plugin -url https://vc-svr.example.com/sdk -u
administrator@vsphere.local -p secret -vct vcenterServerThumbprint
```

- コマンドパラメータの説明:
  - **-action**: 実行するアクションを指定します。この例では**unregisterPlugin**です。
  - **-k** sample.plugin:ターゲットプラグインの識別子を指定します。この例では、**com.h3c.unisystem.remote**です。
  - **-url** *https://vc-svr.example.com/sdk*: vCenter Serverが提供するSDKリソースのURLを指定します(例:https://192.168.128.117/sdk)。
  - **-u** *administrator@vsphere.local:* vCenter Serverのログインユーザー名を指定します。
  - **-p** *secret*:vCenter Serverのログインパスワードを指定します。
  - **-vct** vcenterServerThumbprin:vCenter Serverのプラグインフィンガープリント。
- UniSystemプラグインをアンインストールするコマンドの例:

```
D:\vsphere-client-sdk-6.7.0.40000-14186396\html-client-sdk\tools\vCenter
plugin registration\prebuilt>extension-registration.bat -action
unregisterPlugin -k com.h3c.unisystem.remote -u administrator@vsphere.local
-p***** -url https://192.168.21.27/sdk -vct
C2:74:43:D2:1F:9D:CC:52:E5:6A:98:DF:50:C7:ED:0E:60:FD:B7:1C:F7:D6:8F:D6:E3:9
0:6C: 3C:A8:2C:B5:1E
```

システム設定を構成する

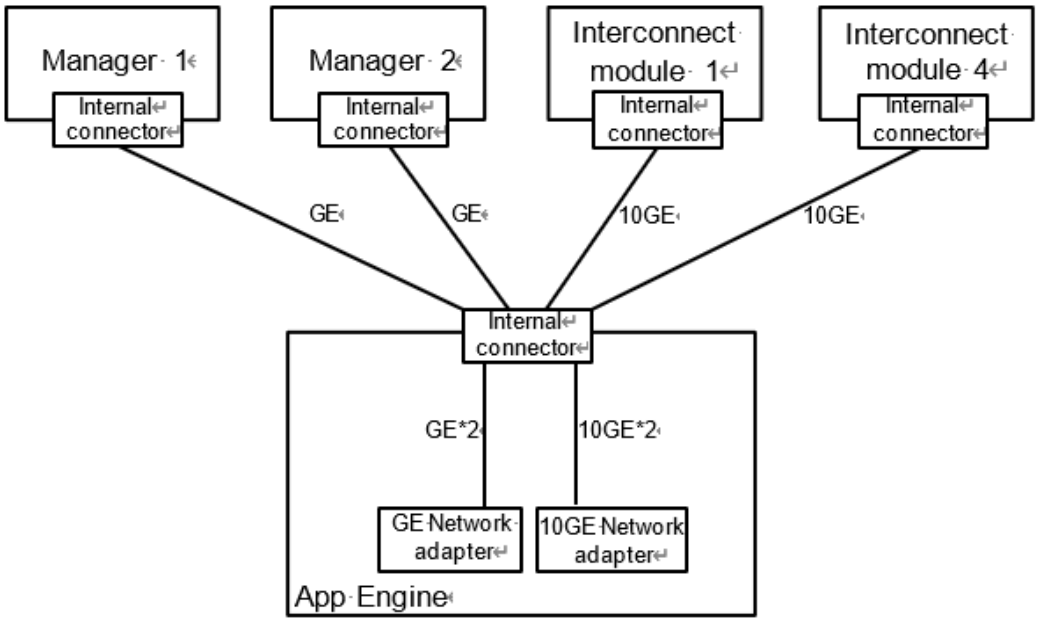
ネットワーク設定を構成する

このモジュールは、UniSystemがAEモジュールまたはVMで実行されている場合にのみ使用できます。

このモジュールを使用すると、基本的なイーサネットアダプタモジュール情報とルーティングエントリの表示、ネットワークポートのIPアドレスの管理、およびネットワーク接続のテストを行うことができます。

図287に示すように、AEモジュールには、GEイーサネットアダプターと10-GEイーサネットアダプターがあります。GEイーサネットアダプターの2つのGEインターフェイスは、それぞれOMモジュール1とOMモジュール2に接続します。10-GEイーサネットアダプターの2つの10-GEインターフェイスは、それぞれインターコネクトモジュール1とインターコネクトモジュール4に接続します。

図287 サーバーエンクロージャー内のモジュール間の接続



Ethernetアダプターの基本情報を表示する

UniSystemサーバー上のイーサネットアダプタモジュールの基本情報を表示するには、次の作業を実行します。

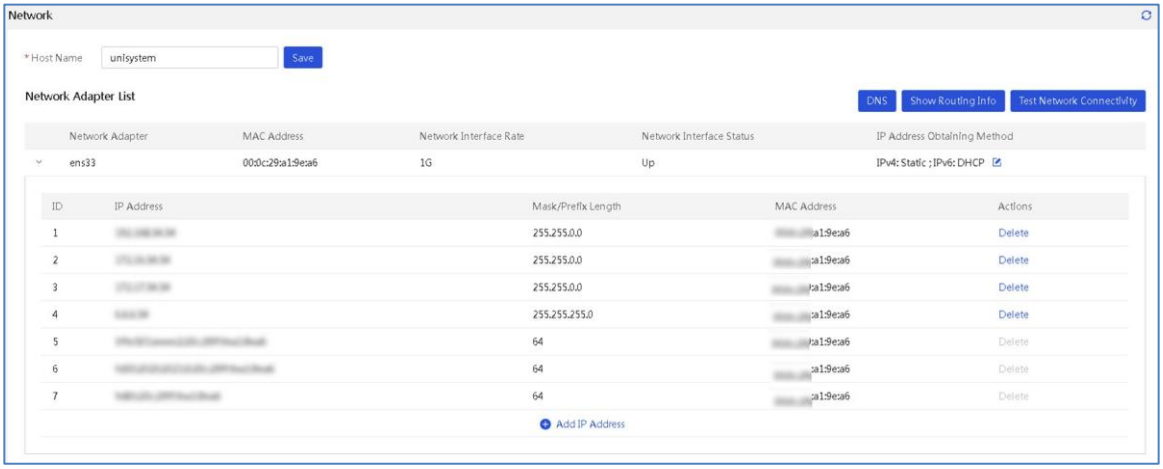
UniSystemサーバーがAEモジュールで実行されている場合は、次のネットワークポートを使用できます。

- **vmng**: メンバポートがOMモジュールのネットワークポートである集約インターフェイス。ネットワークポートはVLAN 1に属します。
- **vmng.om**: OMモジュールとの通信に使用される仮想ネットワークポート。仮想ネットワークポートは4094に属します。
- **enp5s0f0**:インターコネクトモジュール1に接続されているネットワークポート。
- **enp5s0f1**:インターコネクトモジュール4に接続されているネットワークポート。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Network**を選択します。
2. Ethernetアダプタモジュールの基本情報を表示します。パラメータの詳細は、オンラインヘルプを参照してください。

図288 ネットワーク設定



UniSystemのホスト名を設定する

UniSystemサーバーに使用されるホスト名を表示または設定するには、次のタスクを実行します。この機能は、UniSystemサーバーがAEモジュールで実行されている場合にのみ使用できます。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Network**を選択します。
2. ホスト名を入力します。
3. **Save**をクリックします。

ネットワークポートのIPアドレス取得方法とDNSサーバードレスを設定します。

IPv4およびIPv6アドレスの構成では、静的方法とDHCP方法の両方がサポートされています。ネットワークポートのIPアドレス取得方法がDHCPに設定されている場合は、DHCP/DHCPv6を有効にしてDNSサーバードレスを取得できます。IPアドレス取得方法が静的に設定されている場合は、DNSサーバードレスを手動で構成する必要があります。

DHCP方式を使用する場合、ネットワークアダプタはDHCP要求を送信します。次に、手動で更新ボタンをクリックして、ページに新しいIPアドレスを表示します。IPv4 DHCPの場合、DHCPサーバーとの通信に異常が発生すると、システムは約1分間待機した後、自動的に静的モードに切り替わります。

UniSystemの一部の機能はインターネットへのアクセスを必要とするため、サーバーはDNSサーバーを使用してドメイン名を解決する必要があります。ネットワーク環境が正しく動作するように、実際の状況に基づいてDNSサーバーを構成します。

制約事項とガイドライン

ネットワークポートのIPアドレス取得方法をDHCPに設定すると、ネットワークポートは静的IPアドレスを使用しなくなります。この方法を静的に戻すと、ネットワークポートは以前に指定した静的IPアドレスを使用します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Network**を選択します。

2. ネットワークポートのボタンをクリックします。表示されたダイアログボックスで、IPアドレスの取得方法とDNSアドレスの取得方法を設定し、**OK**をクリックします。
   - DHCPモードを選択した場合は、DHCP/DHCPv6を使用してDNSサーバードレスを取得するかどうかを選択できます。
   - スタティックモードを選択した場合は、DNSサーバーのIPアドレスを手動で入力する必要があります。
3. **OK**をクリックします。
4. ネットワークポートの**Add New IP**をクリックします。表示されたダイアログボックスで、IPv4またはIPv6を選択し、IPアドレスとサブネットマスクまたはプレフィックスの長さを入力します。**OK**をクリックします。

   メモ:

   IPv6アドレスを追加する場合、IPv4アドレスに埋め込まれたIPv6アドレス(::192.168.0.1など)や、IPv4アドレスに埋め込まれているように見えるアドレスに省略できるIPv6アドレス(::c3:3など)は追加できません。

5. ネットワークポートのIPアドレスを削除するには、**Actions**列の**Delete**をクリックし、**OK**をクリックします。リンクローカルアドレスは編集または削除できません。

DNS情報を表示する

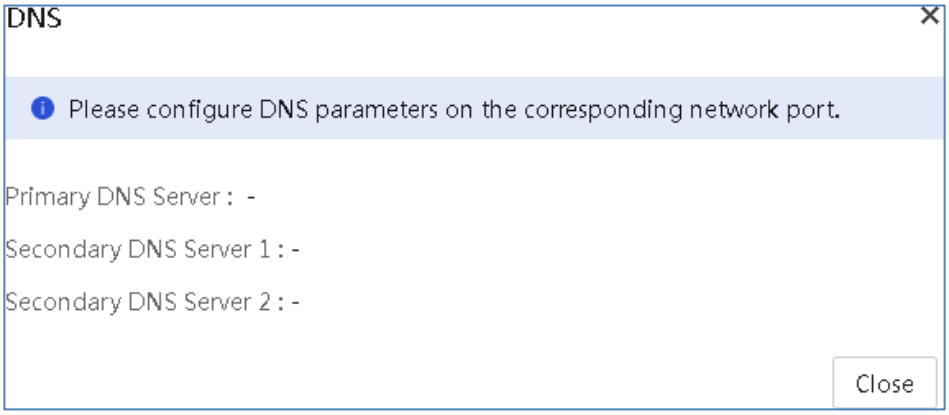
このタスクについて

この機能は、バージョン2.34以降で使用できます。DNSサーバー情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Network**を選択します。
2. **DNS**をクリックします。

   図289 DNS情報の表示



3. 表示されたダイアログボックスで、DNSサーバー情報を確認します。

ネットワーク接続のテスト

UniSystemサーバーとIPアドレス間のネットワーク接続をテストし、UniSystemサーバーのルーティ

ングエントリを表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Network**を選択します。
2. **Test Network Connectivity**をクリックし、IPアドレスを入力します。
3. Pingをクリックします。返されたpingの結果を表示します。
4. (任意)**Show Routing Info**をクリックして、ルーティング情報を表示します。

プロキシ設定の構成

このタスクについて

この機能は、バージョン2.34以降で使用できます。

このモジュールでは、プロキシサーバーを設定できます。したがって、UniSystemは外部通信にHTTPまたはHTTPSプロトコルを使用できます。

現在のソフトウェアバージョンでは、ユニシステムは次の機能に対してのみプロキシサーバーを使用できます。

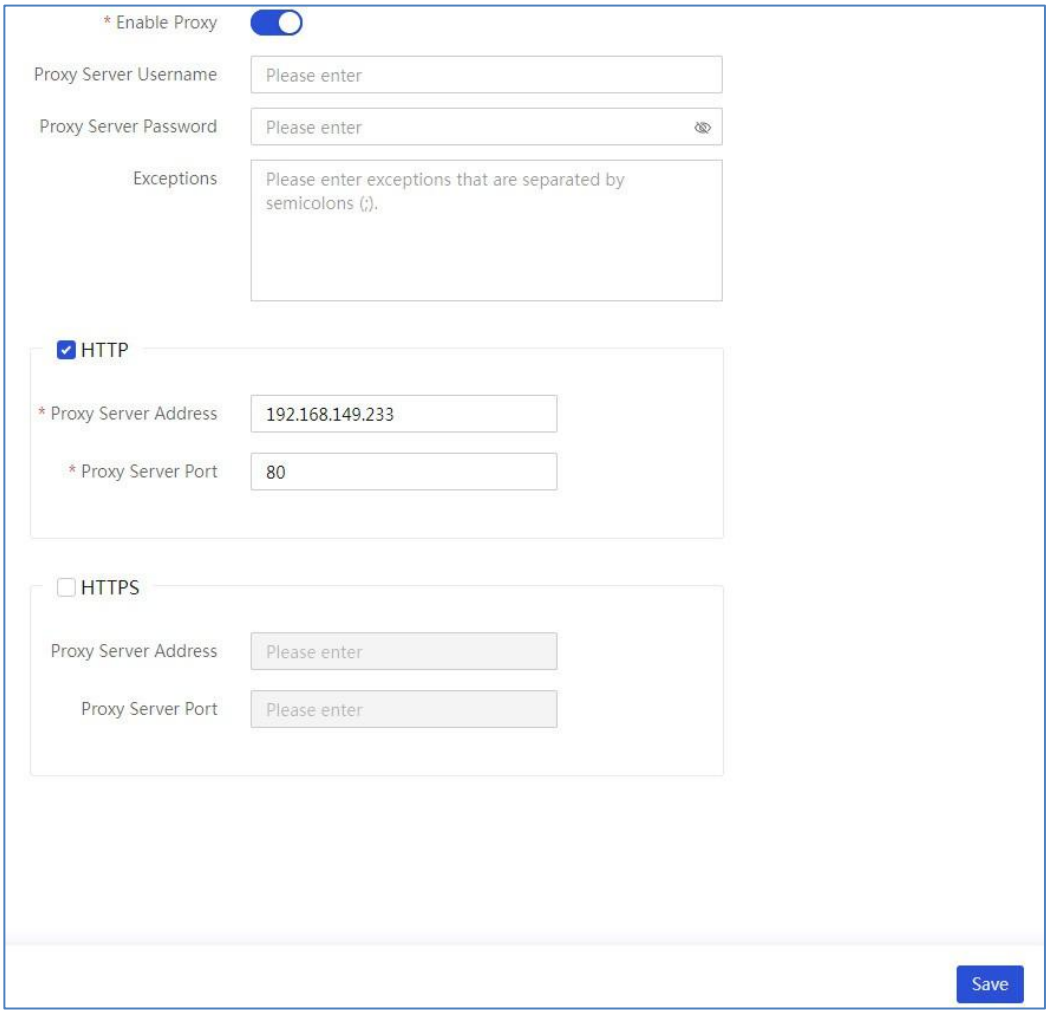
- リポジトリライブラリにUniSystemタイプのリポジトリを追加し、REPO更新を有効にします。
- WeCom通知、SMS通知、または音声通知を設定します。
- リモートサポートで修復レポートを設定します。

デフォルトでは、UniSystemの上記の機能以外の機能を使用する場合、プロキシは使用されません。

手順

1. ナビゲーションペインで、**Menu** > **System** > **System** > **Proxy Settings**を選択します。

図290 プロキシ設定の構成



2. プロキシを有効にするかどうかを選択します。
3. プロキシサーバーのパラメータを入力します。
4. (任意)HTTPプロキシをイネーブルにするには、HTTPを選択します。
5. (任意)HTTPSプロキシをイネーブルにするには、HTTPSを選択します。
6. **Save**をクリックします。

システム時刻の設定

このタスクについて

この機能は、バージョン2.00.17以降で使用できます。

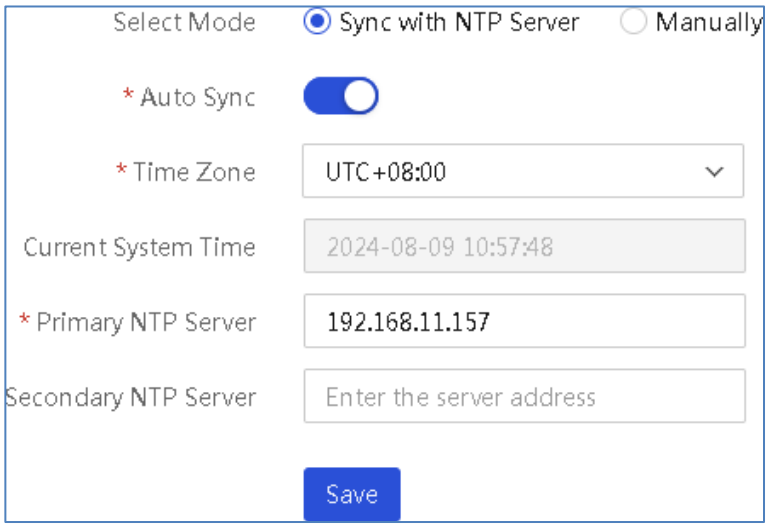
このモジュールを使用すると、UniSystemのシステム時刻を表示または設定できます。この機能は、UniSystemがAEモジュールまたはVM上で実行されている場合にのみ使用できます。

UniSystemは、システム時刻をNTPサーバーと同期するように設定することも、手動でシステム時刻を設定することもできます。

NTPサーバーとのシステム時刻の同期

1. ナビゲーションペインで、**Menu** > **System** > **System** > **System Time Settings**を選択します。
2. **Sync with NTP Server**を選択します。
3. **Auto Sync**オプションを有効にします。
4. 現在のタイムゾーンを表示します。必要に応じて、タイムゾーンを手動で選択できます。
5. プライマリNTPサーバーとセカンダリNTPサーバーのIPアドレスを入力します。

   図291 システム時刻の設定

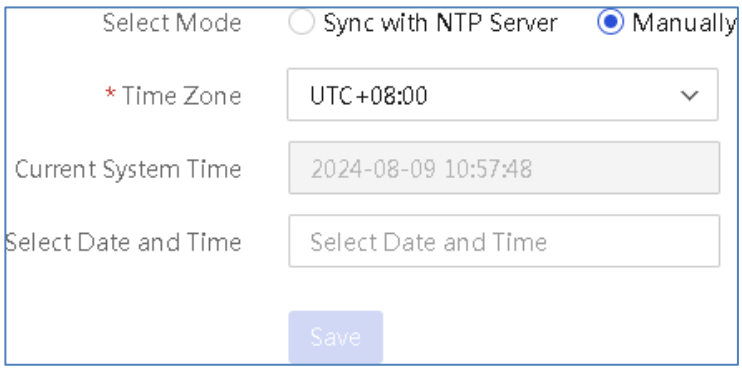


6. **Save**をクリックします。

システム時刻を手動で設定する

1. ナビゲーションペインで、**Menu** > **System** > **System** > **System Time Settings**を選択します。
2. **Manually**を選択し、UniSystemが使用する日付と時刻を選択します。

   図292 システムの手動設定



3. 現在のタイムゾーンが表示されます。必要に応じてタイムゾーンを選択できます。
4. **Save**をクリックします。

クラスタを構成する

このタスクについて

この機能は、バージョン2.00.17以降で使用できます。

このモジュールを使用すると、AEモジュールのクラスタを作成または管理して、高可用性を実装できます。UniSystemは、プライマリノードのステータスを自動的に監視します。プライマリノードに障害が発生すると、UniSystemはセカンダリノードでの実行に切り替わり、プライマリAEモジュールの障害によるサービスの中断を回避します。

前提条件

クラスタの作成にはデータの同期が必要です。データの同期を正しく行うには、プライマリノードとセカンダリノードの時間差が10秒未満であることを確認してください。システム時間の設定方法の詳細は、「システム時間の構成」を参照してください。

クラスタを作成する場合は、次の条件が満たされていることを確認します。

- プライマリノードとセカンダリノードが相互に通信できることを確認します。ベストプラクティスとして、プライマリノードとセカンダリノードが相互に通信するポートに静的IPアドレスを割り当て、ポートのサブネットマスクが同じであることを確認します。
- プライマリノードとセカンダリノードのそれぞれに、UniSystemアクセス用の一意のホスト名が設定されていることを確認します。ホスト名を**localhost**またはすべて数字の文字列に設定しないでください。
- 各ネットワークポートに対して、同じサブネット上で複数のIPアドレスを設定しないでください。

ホスト名とネットワーク設定の設定方法について詳しくは、「ネットワーク設定を構成する」を参照してください。

制約事項とガイドライン

- クラスタ内のセカンダリUniSystemノードは、クラスタの作成中に停止します。
- クラスタの作成中は、AEモジュールの電源を切ったり、ネットワークを切断したりしないでください。データの同期には時間がかかります。すべての処理が完了するまでお待ちください。
- クラスタの作成中は、プライマリノードのUniSystemで他の操作を実行しないでください。
- クラスタの作成後は、UniSystemのホスト名、ネットワーク、またはシステム設定を編集しないでください。
- UniSystemをクラスターモードからスタンドアロンモードに戻すことはできません。
- クラスタで使用されるAEモジュールのホスト名は、localhostまたはすべて数字にすることはできません。
- 通信に使用する主ノードと二次ノードのポートには、固定IPアドレスを使用することをお勧めします。
- クラスタの作成に失敗すると、UniSystemが使用できなくなります。クラスタの作成を再試行してください。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Cluster**を選択します。

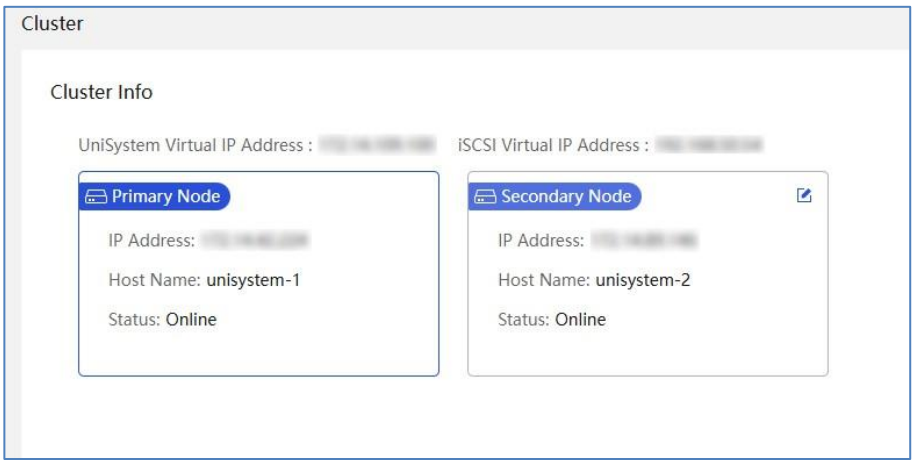
2. **Create Cluster**リンクをクリックします。
3. 開いたページで、作成するクラスタの次のパラメータを設定します。
   - **Secondary Node Address**: セカンダリノードがプライマリノードと通信するために使用するIPアドレス。ネットワークポート**vmng.om**またはセカンダリAEモジュールの10-GEネットワークポートのIPアドレスを使用することをお勧めします。
   - **UniSystem Virtual IP Address**: クラスタの作成後にユーザーがUniSystemにアクセスするための仮想IPアドレス。
   - **iSCSI Virtual IP Address**: ISCSIサービスの設定に使用されるIPアドレス。入力したiSCSI仮想IPアドレスが、プライマリAEモジュールの10-GEネットワークポートのIPアドレスと同じネットワークセグメント上にあることを確認します。

図293 クラスタの作成



4. **OK**をクリックします。進行状況バーから作成の進行状況を確認できます。クラスタ作成の詳細情報を表示するには、View Logをクリックします。
5. クラスタが正常に作成されると、UniSystemは自動的に再起動します。UniSystemの仮想IPアドレスを使用してUniSystemにログインします。
6. **Cluster**ページで、プライマリノードおよびセカンダリノードに関する情報を表示します。

図294 Cluster Infoページ



7. セカンダリノードの横にある**Edit**アイコンをクリックします。表示されたダイアログボックスで、現在のセカンダリノードを置換するノードのIPアドレスを入力し、**OK**をクリックします。置換の進行状況は、進行状況バーで確認できます。

保守とアップグレード

このタスクを実行して、UniSystemデータをバックアップおよび復元し、UniSystemソフトウェアをアップグレードします。

UniSystemデータのバックアップと復元

このタスクについて

この機能は、バージョン2.00.14以降で使用できます。

このモジュールでは、UniSystemデータのバックアップと復元、システム操作ログのダウンロード、およびデフォルトのUniSystem設定の復元を行うことができます。

バックアップまたは復元できるUniSystemデータには、デバイス情報、コンポーネント更新タスク情報、構成テンプレートまたはファイル情報、アドレスプール情報、およびユーザー情報が含まれます。次のデータはバックアップできません:リポジトリ、イメージリストにアップロードされたイメージファイル、クローンイメージ、ディスクレスブートボリューム、リスニング設定、DHCP設定、およびUniSystemバージョン更新ページにアップロードされたバージョン更新ファイル。

デフォルト設定を復元すると、UniSystemサーバーでバックアップ可能な情報がクリアされ、ユーザー設定がデフォルトに復元されます。

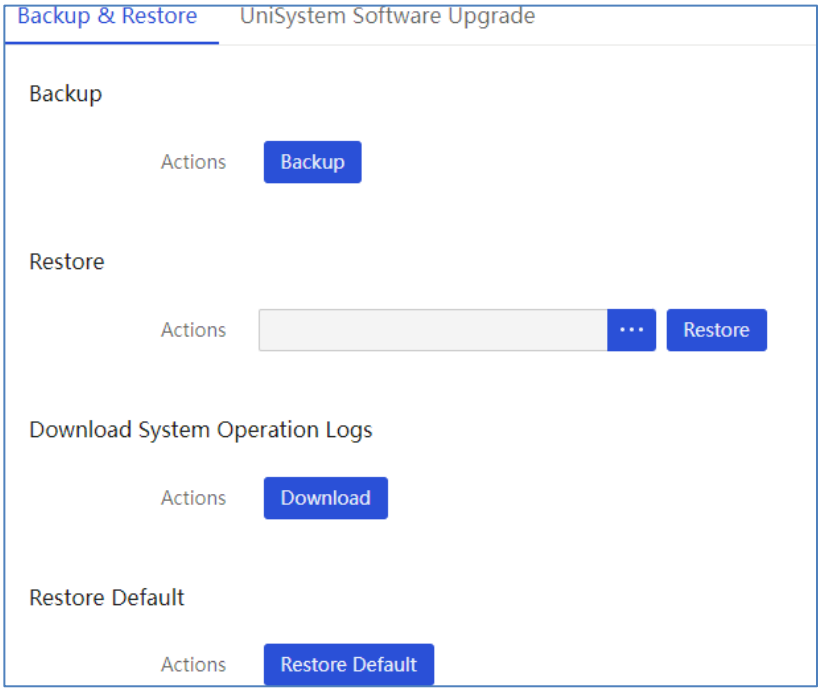
制約事項とガイドライン

- UniSystemデータを復元する前、またはUniSystemのデフォルト設定を復元する前に、現在のUniSystemデータをバックアップします。
- 復元の失敗を避けるために、UniSystemデータの復元またはデフォルトのUniSystem設定の復元中は、復元に影響を与える可能性のある操作を実行しないでください。
- UniSystemが正常に動作するようにするには、UniSystemデータを復元した後、またはUniSystemのデフォルト設定を復元した後に、手動でUniSystemを再起動する必要があります。バージョン2.39以降では、UniSystemデータの復元またはデフォルトのUniSystem設定の復元後に、パッケージバージョンのUniSystemが自動的に停止され、VMまたはAEモジュール上のUniSystemが再起動されます。
- データの復元中にコンフィギュレーションファイルの確認が失敗しないようにするには、バックアップコンフィギュレーションファイルを変更しないでください。
- システム設定にイメージファイルまたはリポジトリが含まれている場合、サーバーテンプレートまたはサーバー構成ファイルは、バックアップまたはリストア後に無効になります。サーバーに適用する前に、テンプレートまたはファイルを再構成する必要があります。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Maintain and Upgrade**を選択します。**Backup & Restore**タブをクリックします。

図295 バックアップと復元ページ



2. 実行コンフィギュレーションをバックアップするには、Backupをクリックします。システムは、実行コンフィギュレーションを圧縮ファイルにエクスポートします。
3. 構成ファイル内の構成を復元するには、**Restore**の横にある.をクリックし、ターゲット構成ファイルを選択して**Restore**をクリックします。
4. 圧縮ファイル内のUniSystemシステム操作ログをローカルホストにダウンロードするには**Download**をクリックします。
5. 既定の設定に戻すには、**Restore Default**をクリックします。表示されたダイアログボックスで、**OK**をクリックします。

UniSystemソフトウェアのアップグレード

このタスクについて

この機能は、バージョン2.39以降で使用できます。

この機能を使用すると、UniSystemソフトウェアバージョンをアップグレードまたはダウングレードできます。UniSystemソフトウェアのアップグレードによってUniSystemデータが失われることはありません。ただし、ベストプラクティスとして、UniSystemをアップグレードする前に重要なデータをバックアップしてください。

UniSystemアップグレードインタフェースは、VMまたはAEモジュールで実行されているUniSystemでのみ使用できます。パッケージバージョンのUniSystemをインストールする必要はありません。パッケージバージョンのUniSystemをアップグレードするには、新しいパッケージを古いパッケージに置き換えます。

制約事項とガイドライン

- UniSystemを正常にアップグレードできるようにするには、UniSystemをアップグレードする前に、実行中の他のUniSystem操作を停止します。
- UniSystemをアップグレードすると、現在のユーザーを除くすべてのログインユーザーがログアウトされます。また、UniSystemのアップグレードプロセス中は、他のユーザーはログイン

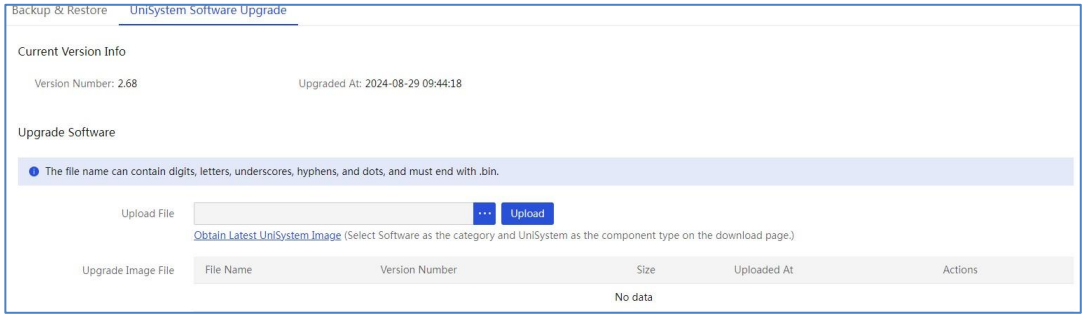
できません。

- UniSystemをアップグレードすると、UniSystemがインストールされているシステムの関連プロセスが中断または再起動されます。これらのプロセスが使用されている場合、関連サービスが中断される可能性があります。

手順(VMまたはAEモジュール上のUniSystemの場合)

1. ナビゲーションペインで、**Menu** > **System** > **Maintain and Upgrad**を選択し、**UniSystem Software Upgrade**タブをクリックします。

   図296 UniSystem Software Upgradeページ



2. (オプション)**Obtain Latest UniSystem Image**をクリックして、必要なUniSystemソフトウェアアップグレードパッケージを公式Webサイトからダウンロードします。
3. ソフトウェアアップグレード操作の…ボタンをクリックし、UniSystemアップグレードパッケージを選択し、**Upload**をクリックしてアップグレードパッケージをアップロードします。
4. **Start Upgrade**をクリックします。表示されたダイアログボックスで、**OK**をクリックしてUniSystemのアップグレードを開始します。

   アップグレードが完了すると、UniSystemは自動的に再起動し、ログインページに戻ります。UniSystemが再起動したら、ページを更新し、新しいUniSystemバージョンを使用するためにログインします。

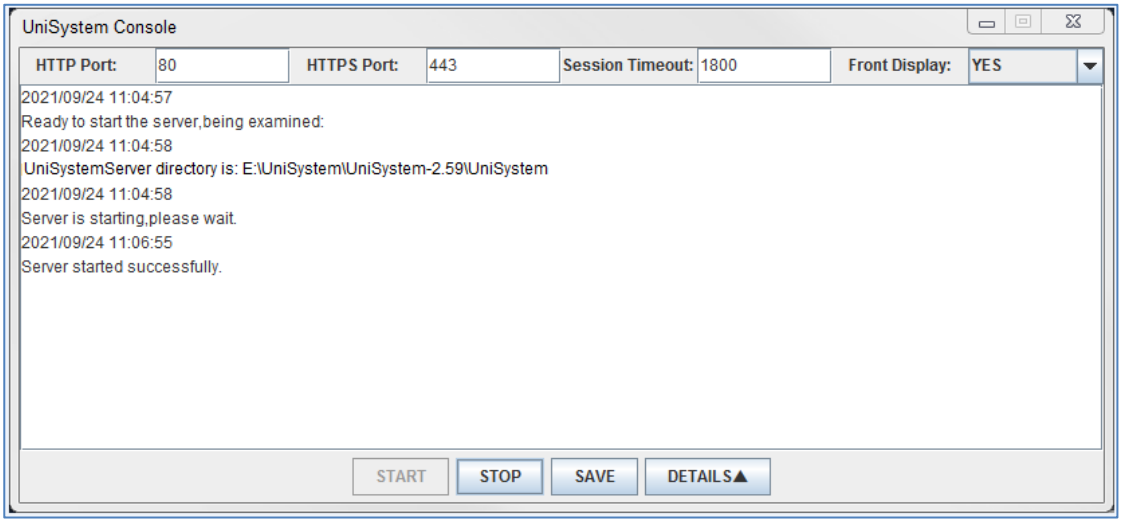
Procedure(パッケージバージョンのUniSystemの場合)

重要:

アップグレード後は、ポート設定を保持できません。

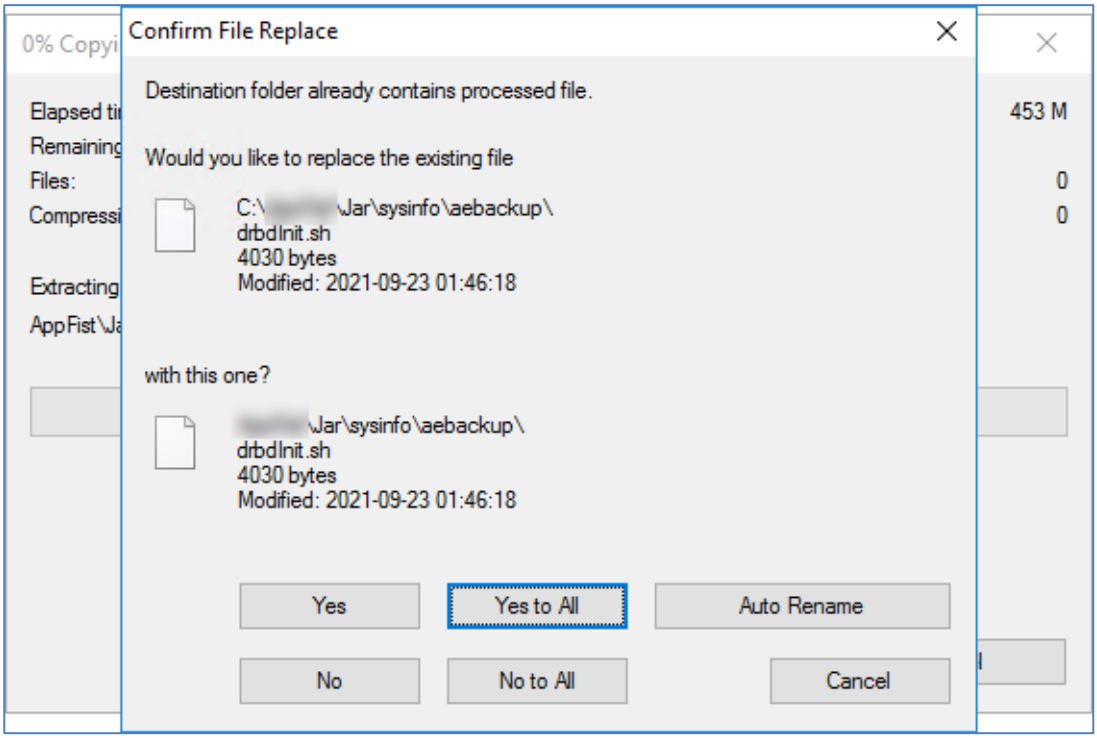
1. 公式WebサイトからUniSystemアップグレードパッケージを入手し、図297に示すように、STOPをクリックしてUniSystemを停止します。

図297 UniSystemコンソール



2. 新しいUniSystemアップグレードパッケージを選択し、パッケージを解凍し、元のUniSystemディレクトリを上書きします。次に、図298に示すように、指示に従ってすべてのファイルを置換することを選択します。

図298 すべてのファイルの置換



3. UniSystemを再起動します。

ログイン時のセキュリティヒントを設定する

このタスクについて

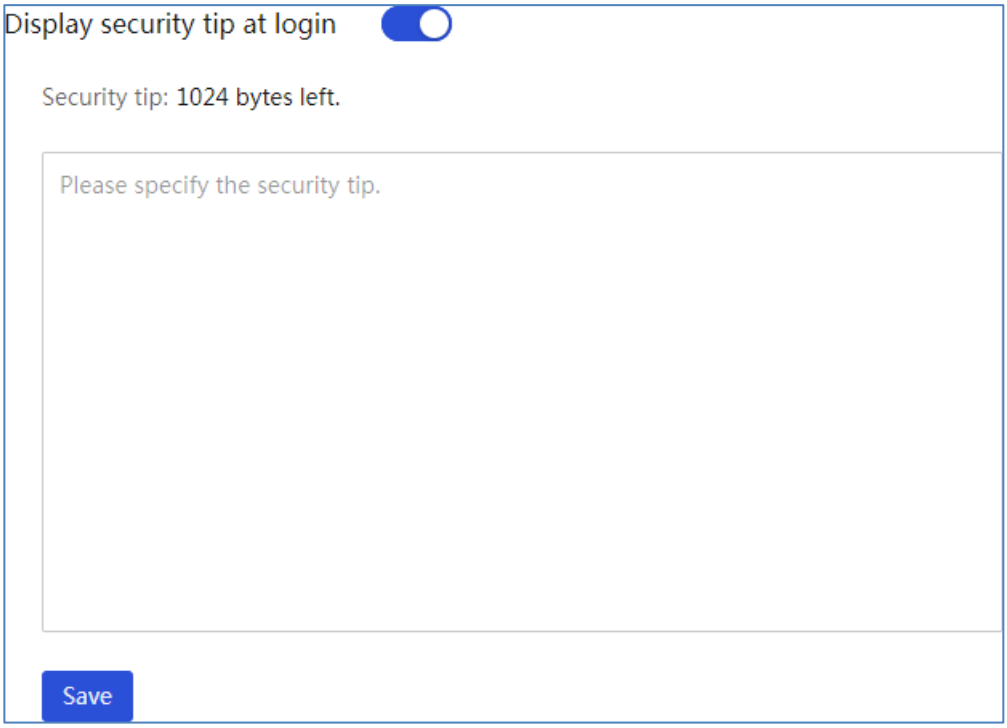
この機能は、バージョン2.34以降で使用できます。

このモジュールを使用すると、ログインのセキュリティヒントを有効にして設定できます。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **Security Tip for Login**を選択します。

   図299 ログイン時のセキュリティヒントの設定



2. **Display security tip at login**を有効にする、を選択します。
3. セキュリティヒントを入力するか、セキュリティヒントフィールドを空のままにします。
4. **Save**をクリックします。

   セキュリティヒントを正常に保存すると、設定したセキュリティヒントがログインページに表示されます。

リモートコントロール

この機能を使用すると、組み込まれたサーバーの状態を監視するための修復設定を有効にできます。システムでサーバー例外が検出されると、修復タスクが自動的に起動され、対応するSDSログがiServiceにアップロードされます。

修復設定を有効にする

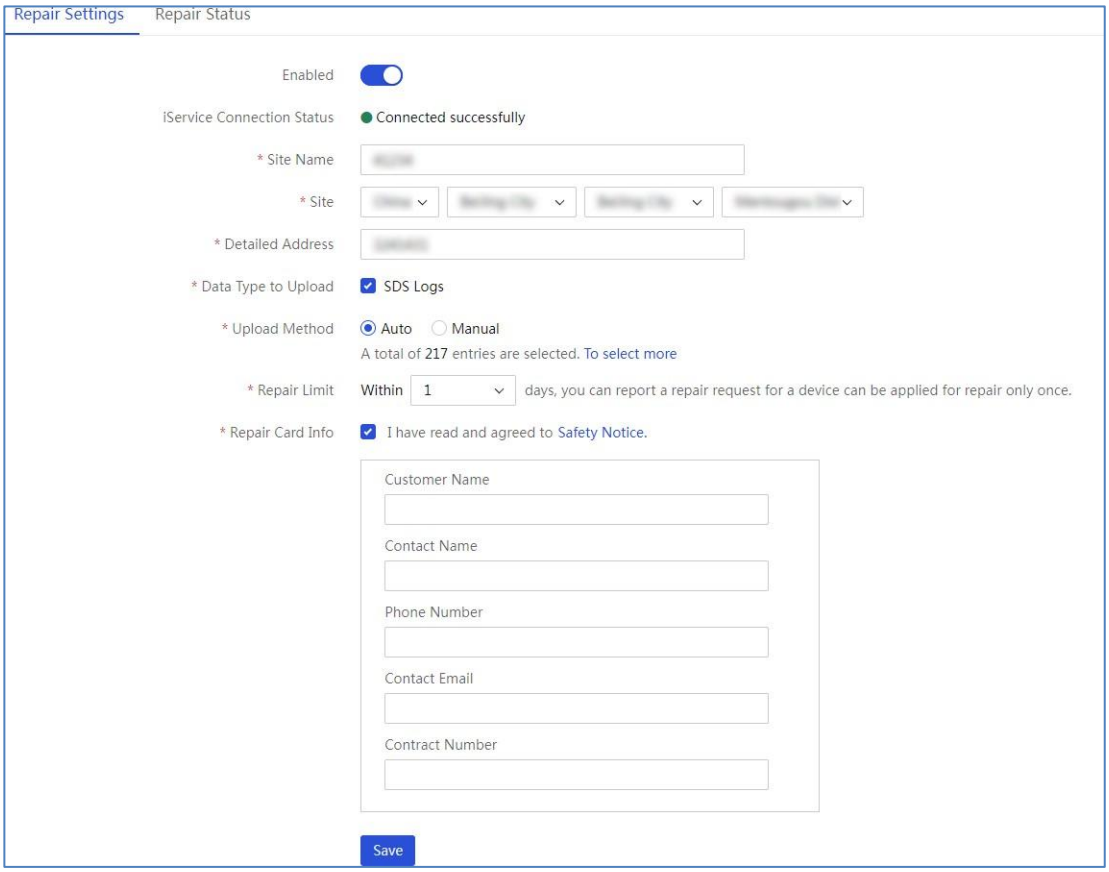
制約事項とガイドライン

アップロード方法が手動の場合は、手動修復レポートだけがサポートされます。

手順

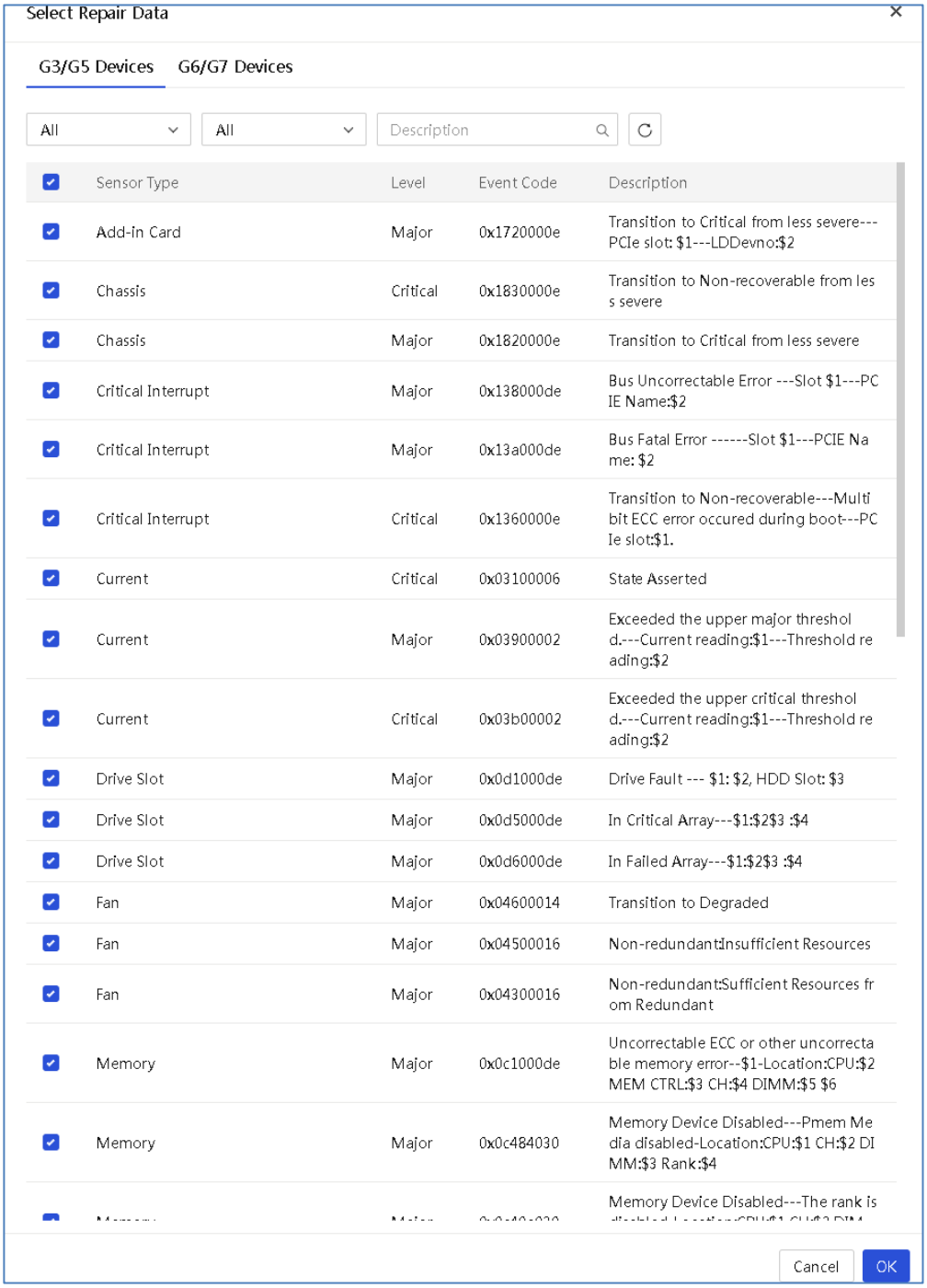
1. ナビゲーションペインで、**Menu** > **System** > **Remote Control**を選択し、**Repair Settings**タブをクリックします。

   図300 修復設定



2. 修復設定を有効にします。
3. UniSystemサーバーがあるサイトの名前を入力します。
4. UniSystemサーバーが配置されているサイト情報と詳細アドレスを入力します。
5. アップロードするデータのタイプとアップロード方法を選択します**Auto**選択した場合は、次の操作を実行します。
   a. (省略可能) **To select more**をクリックします。表示されたダイアログボックスで、対応するタブの修復データを選択します。

図301 修理データの選択



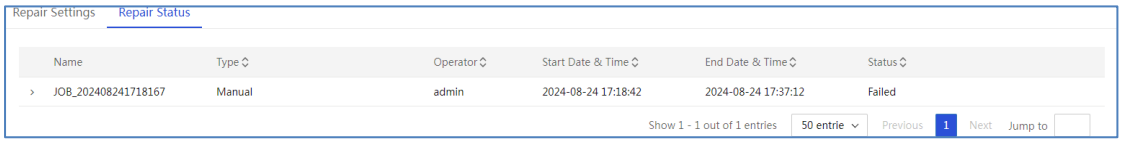
b. 修復リクエスト数の制限を設定します。オプションは次のとおりです。
   - **Unlimited**: 1日以内のアラームを制限しません。自動修復が満たされている限り、修復レポートは迅速に処理できます。
   - **1**: 過去1日から自動修復要求の時刻までのすべてのアラームを処理します。
   - **2**: 過去2日間から自動修復要求の時刻までのすべてのアラームを処理します。
   - **3**: 過去3日間から自動修復要求の時刻までのすべてのアラームを処理します。
c. **I have read and agree to the repair service process**を確認し、保証情報を記入します。

6. **Save**をクリックします。

修復ステータスの表示

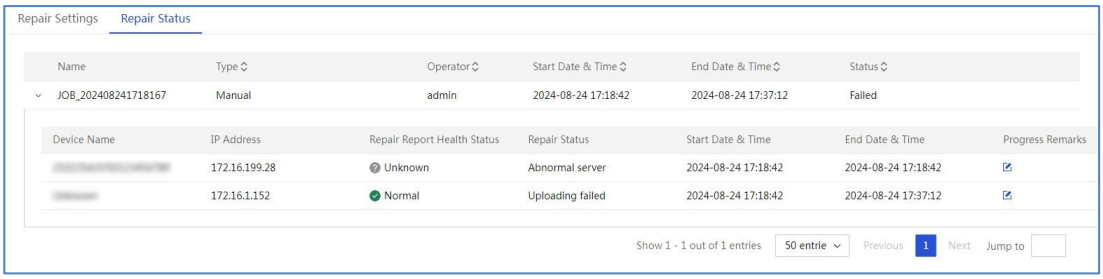
1. ナビゲーションペインで、**Menu** > **System** > **Remote Control**の順に選択し、**Repair Status**タブをクリックします。

   図302 修復ステータスの表示



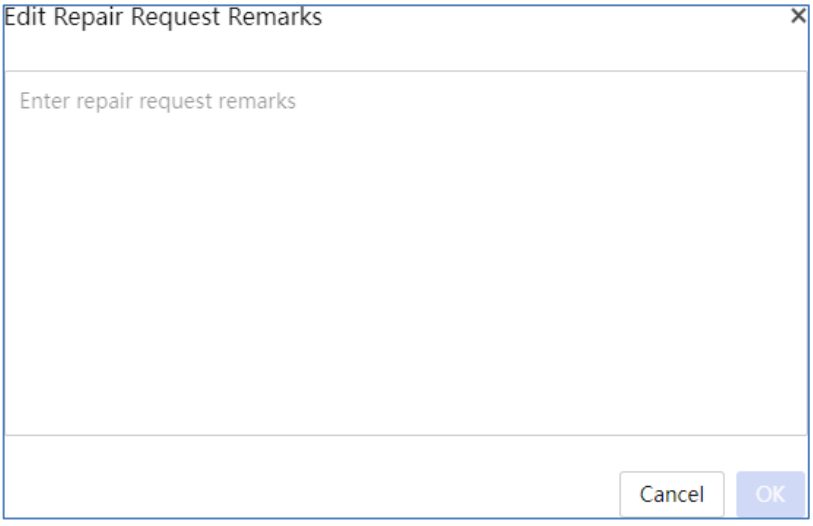
2. 修復タスク内の各デバイスに関する修復情報を表示するには、タスク名をクリックします。

   図303 修理情報の表示



3. 修復タスクのコメントを編集するには、タスクが終了するのを待ってから**Progress Remarks**カラム

   図304 修理依頼の備考の編集



カスタムメニュー

トップナビゲーションバーに表示されるメニュー項目をカスタマイズするには、次のタスクを実行します。

現在のメニューとすべてのメニュー項目を表示する

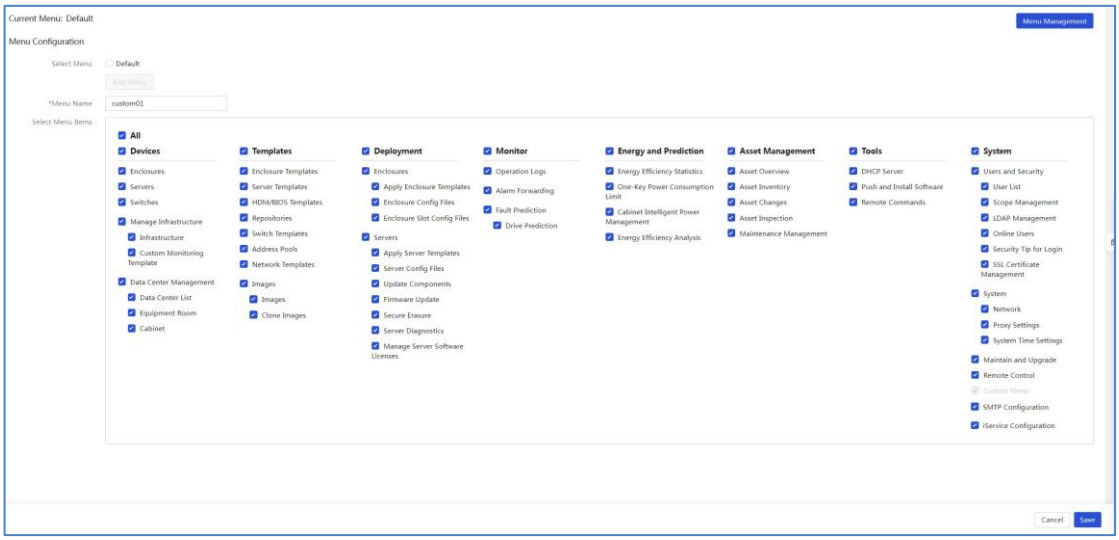
制約事項とガイドライン

- デフォルトメニューには、すべてのメニュー項目が含まれています。**Default**を選択すると、**Custom Menu**ページにメニュー項目は表示されません。
- デフォルトでは、UniSystemはデフォルトメニューを使用します。デフォルトメニューは、メニューバーにすべてのメニュー項目を表示します。
- 使用中のカスタムメニューにショートカット項目が含まれていない場合、**Shortcuts**項目を削除することはできません。ショートカット項目を削除するには、既定のメニューに切り替えてから項目を削除し、カスタムメニューに戻ります。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Custom Menu**を選択します。
2. 現在のメニューを表示します。
3. すべてのメニュー項目を表示するには、**Add Menu**をクリックします。**Select Menu**ボックスに、選択可能なすべてのメニュー項目が表示されます。

図305 現在のメニューとすべてのメニュー項目の表示



カスタムメニューを作成する

制約事項とガイドライン

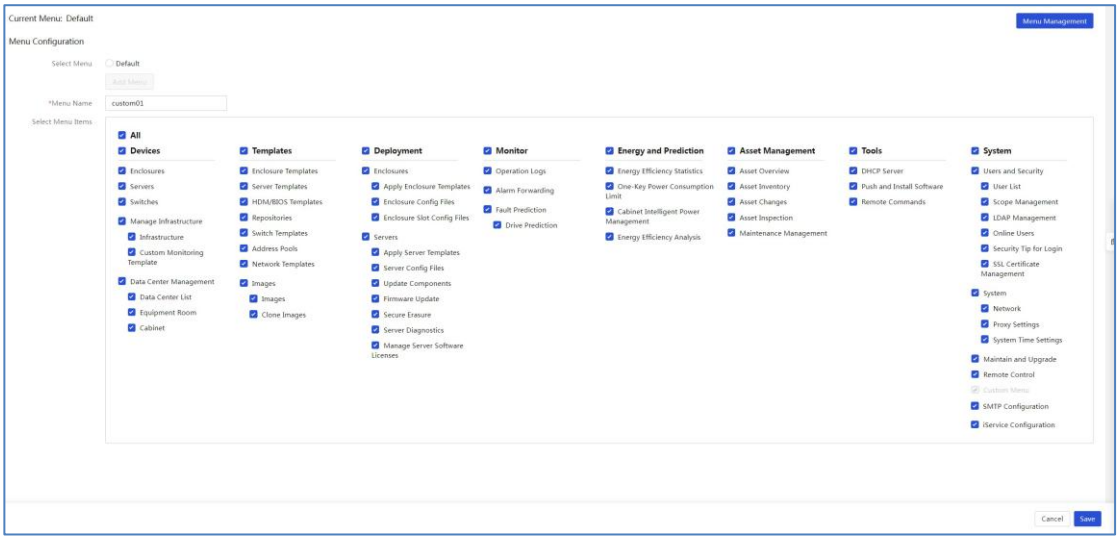
- メニュー名は、大文字と小文字が区別される1～10文字の文字列で、数字、文字、アンダースコア(_)、ハイフン(-)のみを使用できます。メニュー名には、**Default**、または”default”を意味する大文字と小文字の組み合わせは使用できません。
- 既定のメニューに加えて、最大4つのカスタムメニューを作成できます。
- 同じ名前で2つのメニューを作成することはできません。

- メニューアイテムは関連している場合があります。メニューアイテムを選択すると、関連するメニューアイテムも選択されます。ただし、メニューアイテムを選択解除すると、そのアイテムのみが選択解除され、関連するメニューアイテムには影響しません。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Custom Menu**を選択します。
2. **Add Menu**をクリックして、新しいカスタムメニューを作成します。
3. 条件を満たすメニュー名を入力し、メニュー項目を選択します。

   図306 カスタムメニューの作成



4. **Save**をクリックし、表示されたダイアログボックスで**OK**をクリックしてメニューを保存します。ページが自動的に更新され、選択したメニュー項目がメニューバーに表示されます。

カスタムメニューを編集する

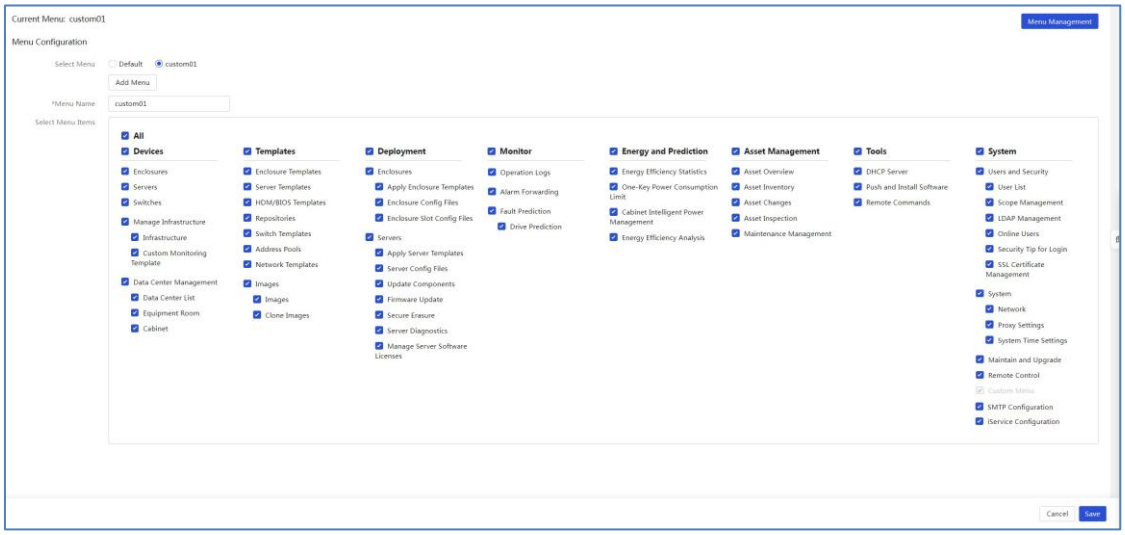
制約事項とガイドライン

- メニュー名は、大文字と小文字が区別される1～10文字の文字列で、数字、文字、アンダースコア(_)、ハイフン(-)のみを使用できます。メニュー名には、Default、または「default」を意味する大文字と小文字の組み合わせは使用できません。
- 同じ名前で2つのメニューを作成することはできません。
- デフォルトメニューは編集できません。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Custom Menu**を選択します。
2. カスタムメニューを選択します。
3. **Edit**をクリックして、カスタムメニューを編集します。

図307 カスタムメニューの編集



4. (オプション)要件を満たすメニュー名を入力し、メニュー項目を選択します。
5. **Save**をクリックし、表示されたダイアログボックスで**OK**をクリックしてメニューを保存します。ページが自動的に更新され、選択したメニュー項目がメニューバーに表示されます。

カスタムメニューを削除する

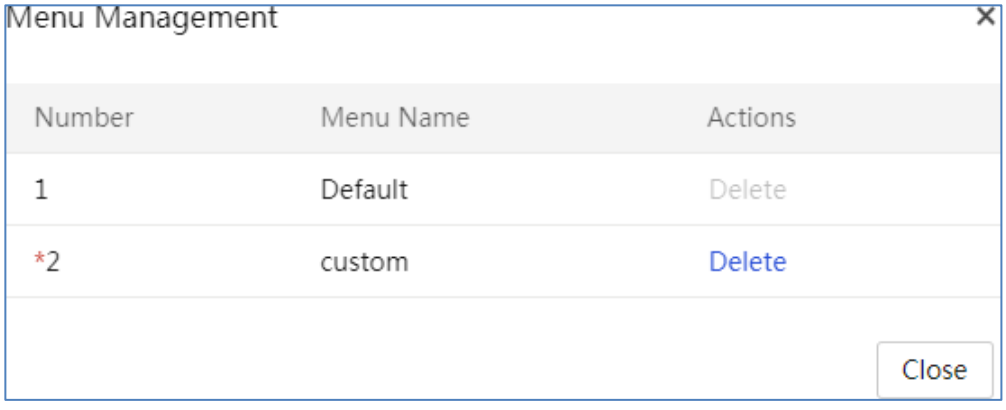
制約事項とガイドライン

- デフォルトメニューは削除できません。
- 使用中のカスタムメニューを削除すると、システムはデフォルトメニューに切り替わり、ページが更新されます。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Custom Menu**を選択します。
2. **Menu Managemen**をクリックします。開いたページに、すべてのメニューが表示されます。

図308 カスタムメニューの削除



3. 削除するメニューのActions列で**Delete**をクリックし、表示されたダイアログボックスで**OK**をクリックします。

SMTP設定

このタスクについて

UniSystemは、Simple Mail Transfer Protocol(SMTP)機能を使用して、アラームメッセージ、検査レポート、メンテナンス情報の更新など、電子メールサービスを通じてさまざまなシステム通知を送信できます。これにより、ユーザーは重要な情報を迅速に受け取ることができます。

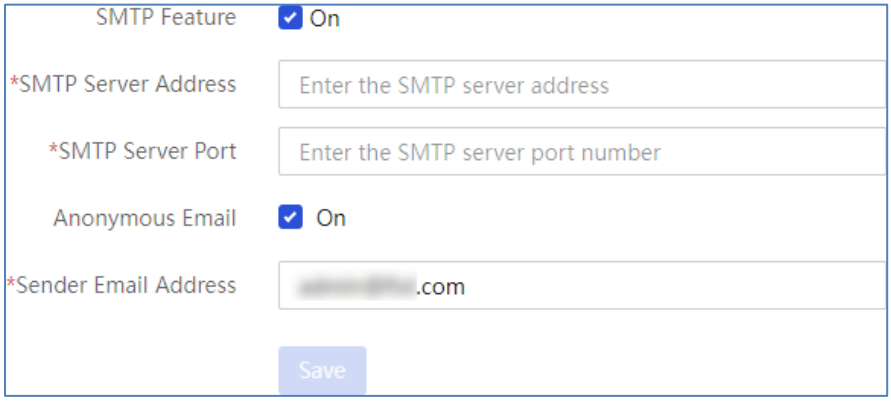
前提条件

SMTPを設定する前に、まずSMTPサーバーのIPアドレスとポート番号を取得し、UniSystemサーバーのIPアドレスがSMTPサーバーと正常に通信できることを確認します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **SMTP Configuration**を選択します。

   図309 SMTP構成

2. SMTP関連情報を設定します。
   - SMTPを有効にします。
   - SMTPサーバーのアドレスを指定します。
   - SMTPサーバーのポートを指定します。
   - 匿名の電子メール送信を有効にするかどうかを選択します。
     - **On**を選択すると、電子メール通知が匿名で送信されます。
     - **On**を選択しない場合は、暗号化プロトコルも選択し、SMTPサーバーに接続する電子メール送信者が使用するユーザー名、パスワード、および暗号化プロトコルを入力する必要があります。
   - 電子メールの送信者の電子メールアドレスを指定します。
3. **Save**をクリックします。

iService構成

このタスクについて

iService機能を使用してiServiceプラットフォームに接続すると、メンテナンス情報の同期化と自動障害レポートが可能になり、手動による介入が減り、メンテナンスの効率が向上します。

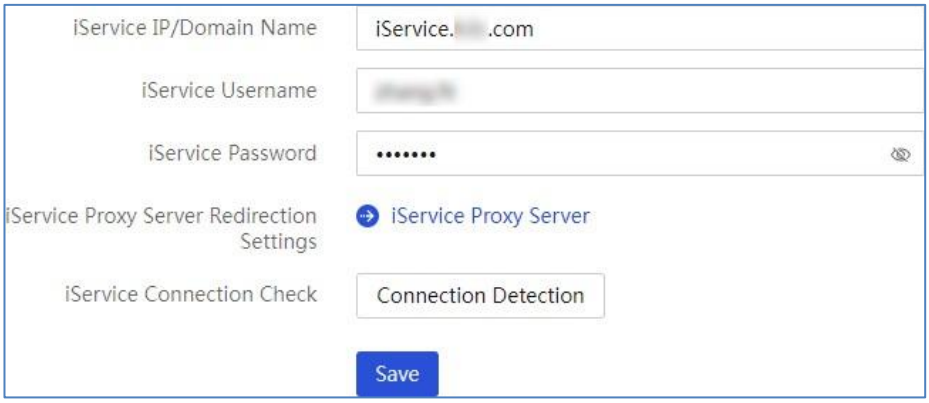
- **Real-time update of maintenance information**: ユニシステムがデバイスメンテナンス情報のリアルタイム更新を取得できるようにし、資産管理の自動化レベルを向上させます。

- **Automatic fault reporting**: デバイスに障害またはアラームが発生した場合に、システムが自動的にiServiceに修復要求を送信できるようにします。これにより、障害処理の適時性が向上します。

手順

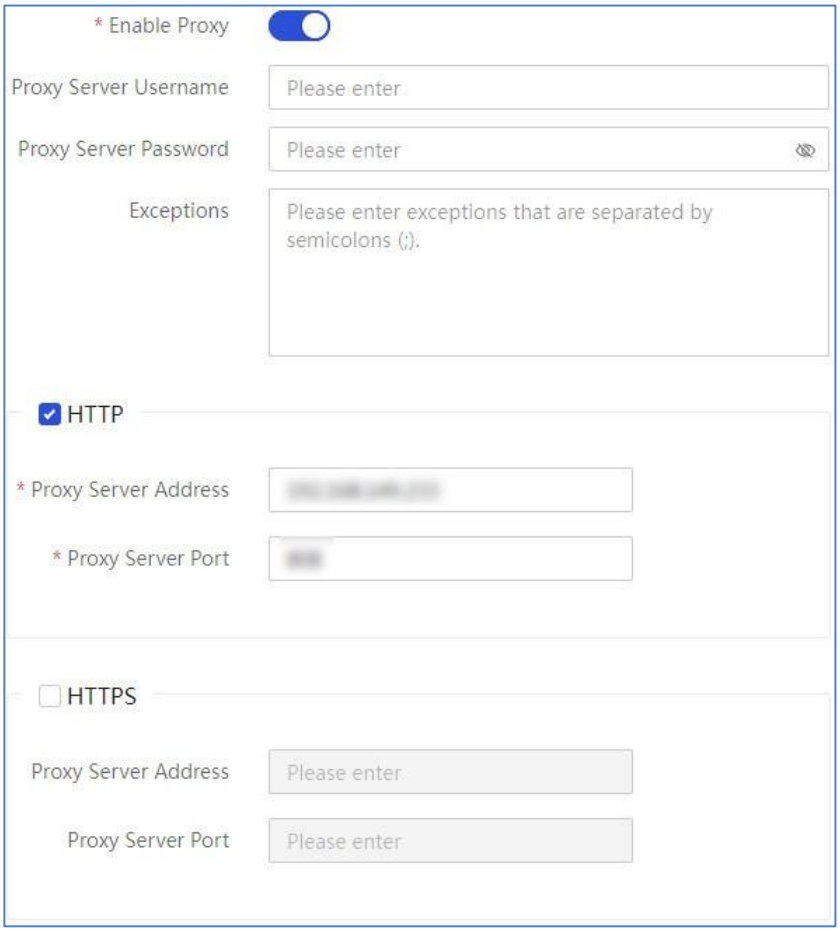
1. ナビゲーションペインで、**Menu** > **System** > **iService Configuration**を選択します。

   図310 iService構成

2. iService関連の情報を設定します。
   - iServiceのIPアドレスまたはドメイン名を指定します。
   - iService公式Webサイトに登録されているユーザー名を入力します。
   - iServiceユーザー名のパスワードを入力します。
   - iServiceプロキシサーバーを設定するには、**iService Proxy Server**をクリックし、関連情報を指定します。
   - **Save**をクリックします。

図311 プロキシ設定の構成



3. Connection Detectionをクリックして、UniSystemとiService間の接続をテストします。
4. **Save**をクリックします。

スコープマネジメント

スコープマネジメントでは、部門や地域などのディメンションに基づいてリソースが異なるスコープに分割されます。これにより、異なるユーザーまたはユーザーグループに役割と権限を割り当てることができ、ユーザーは権限を付与されたリソースにのみアクセスして管理できるため、リソースの詳細な管理とセキュリティの分離が実現します。

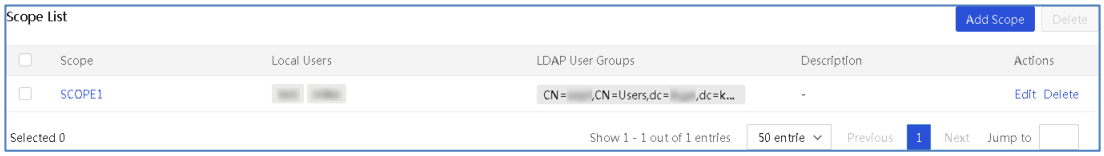
リソースには、エンクロージャー、サーバー、スイッチ、インフラストラクチャ、データセンター、エンクロージャー設定テンプレート、サーバー設定テンプレート、スイッチ設定テンプレート、およびスコープが含まれます。

スコープを表示する

手順

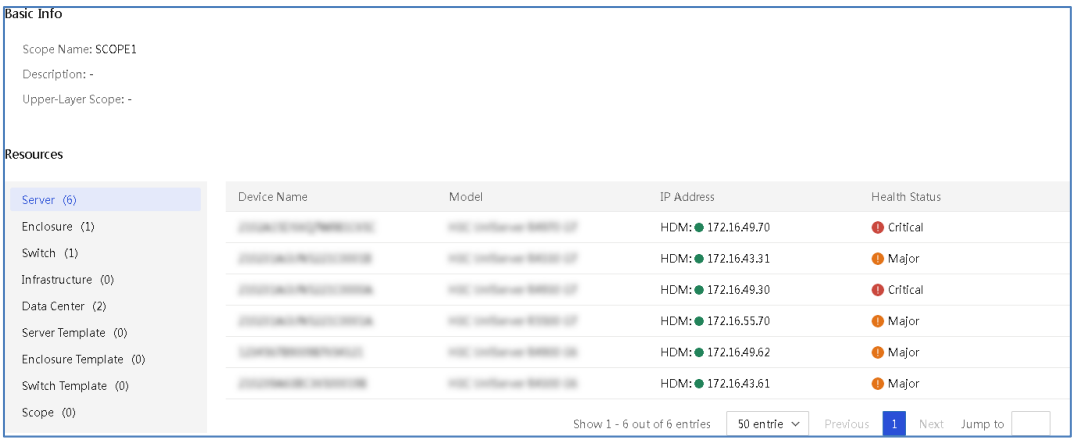
1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **Scope Management**を選択します
2. スコープ情報を表示します。

図312 スコープ



3. スコープの詳細を表示するには、名前リンクをクリックします。

図313 スコープの詳細



パラメータ

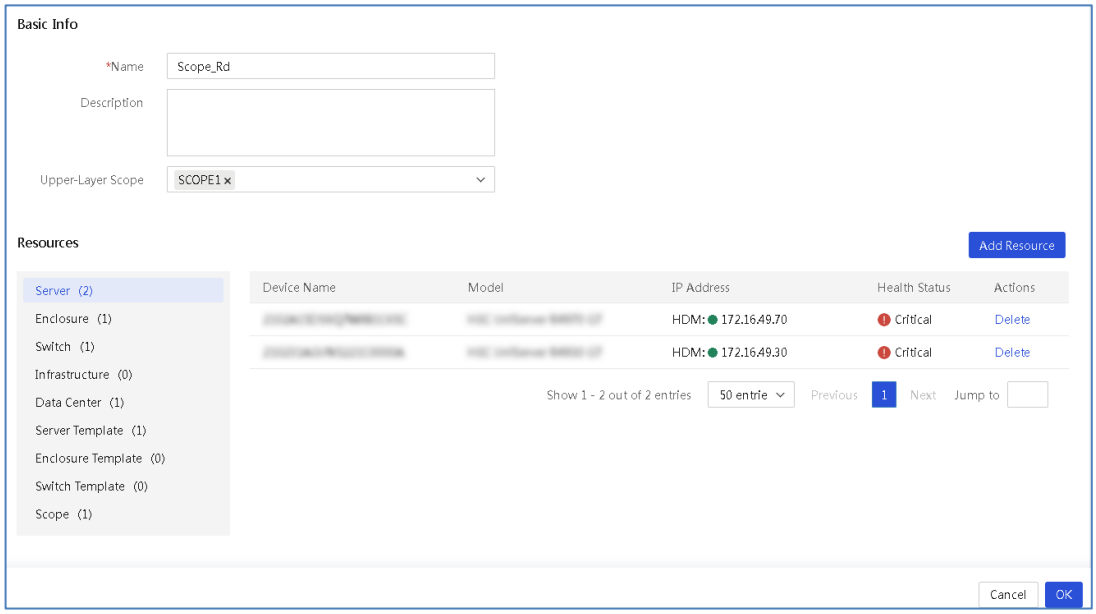
- **スコープリスト**
  - **Scope**:スコープの名前。
  - **Local Users**: スコープに関連付けられているローカルユーザー。
  - **LDAP User Groups**: スコープに関連付けられたLDAPユーザーグループ。
  - **Description**: スコープの説明。
- **範囲の詳細**
  - **Scope Name**: スコープの名前。
  - **Description**: スコープの説明。
  - **Upper-Layer Scope**: スコープの上位層スコープ。
  - **Resources**: スコープによって管理されるリソース。

スコープを追加する

手順

1. ナビゲーションペインで、**Menu > System > Users and Security > Scope Management**を選択します
2. **Add Scope**をクリックします。

図314 スコープの追加



3. 次のようにスコープを設定します。
   - スコープ名を入力します。
   - (任意)スコープの説明を入力します。
   - (オプション)上位層のスコープを選択します。
4. **Add Resources**をクリックして、次のタスクを実行します。
   a. リソースタイプを選択します。
   b. スコープに関連付けるリソースを選択します。検索ボックスを使用して、リソースをフィルタできます。
   c. **OK**をクリックします。
5. **OK**をクリックします。

パラメータ

- 名前: スコープの名前を入力します。
- **Description**: スコープの説明を入力します。
- **Upper-Layer Scope**: 上位層の有効範囲を選択します。上位層の有効範囲に関連付けられているユーザーは、有効範囲を管理できます。
- **Resources**: スコープに関連付けるリソースを選択します。オプションには、エンクロージャー、サーバー、スイッチ、インフラストラクチャ、データセンター、エンクロージャー設定テンプレート、サーバー設定テンプレート、スイッチ設定テンプレート、およびスコープがあります。

スコープを編集する

1. ナビゲーションペインで、**Menu > System > Users and Security > Scope Management**を選択します
2. ターゲットスコープの**Edit**をクリックし、必要に応じてスコープを編集します。
3. **OK**をクリックします。

範囲を削除する

制約事項とガイドライン

ユーザーまたはユーザーグループに関連付けられたスコープは削除できません。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **Scope Management**を選択します
2. 次のいずれかのタスクを実行します。
   - 複数の範囲を削除するには、削除する範囲を選択し、**Delete**をクリックします。
   - 特定のスコープを削除するには、そのスコープの**Delete**をクリックします。
3. 表示された確認ダイアログボックスで、**OK**をクリックします。

LDAPの管理

UniSystemはLDAPサーバーと連携して、サーバー上のLDAPユーザーに迅速なアクセスを提供できます。

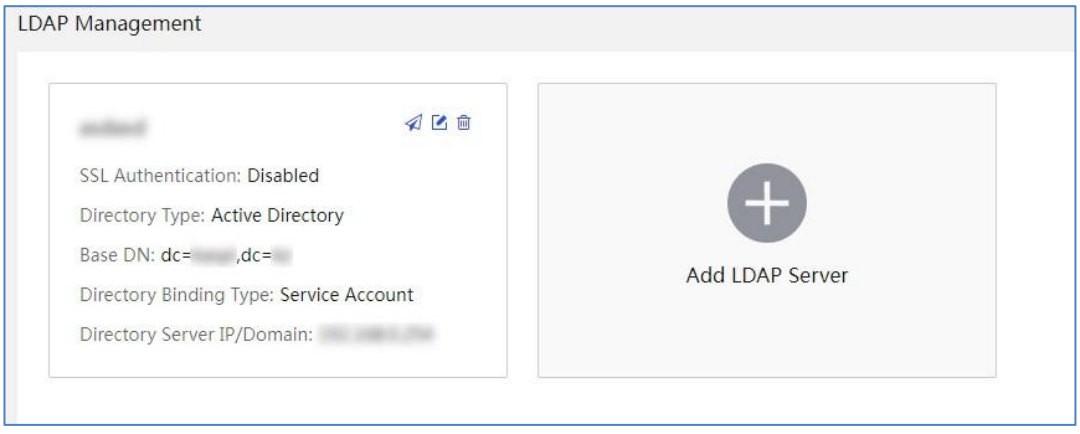
LDAPサーバーをUniSystemに追加してから、LDAPサーバー上のLDAPユーザーグループをUniSystemに追加できます。LDAPユーザーグループ内のメンバーユーザーは、LDAPサーバーに保管されている資格証明を使用して、UniSystemに直接ログインできます。

LDAPサーバー情報の表示とサーバーへの接続のテスト

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **LDAP Management**の順に選択します。

   LDAP Settingsタブには、システムに設定されているLDAPサーバーに関する情報が表示されます。各サーバーは個別のカード上にあります。

   図315 LDAP settingsタブ



2. (オプション)LDAPサーバーへの接続をテストするには、LDAPサーバーカードの右上隅にあるアイコンをクリックします。**User Account**ディレクトリバインディングタイプを使用するLDAPサーバーの場合、疎通確認用のユーザー名とパスワードを入力するように求められます。

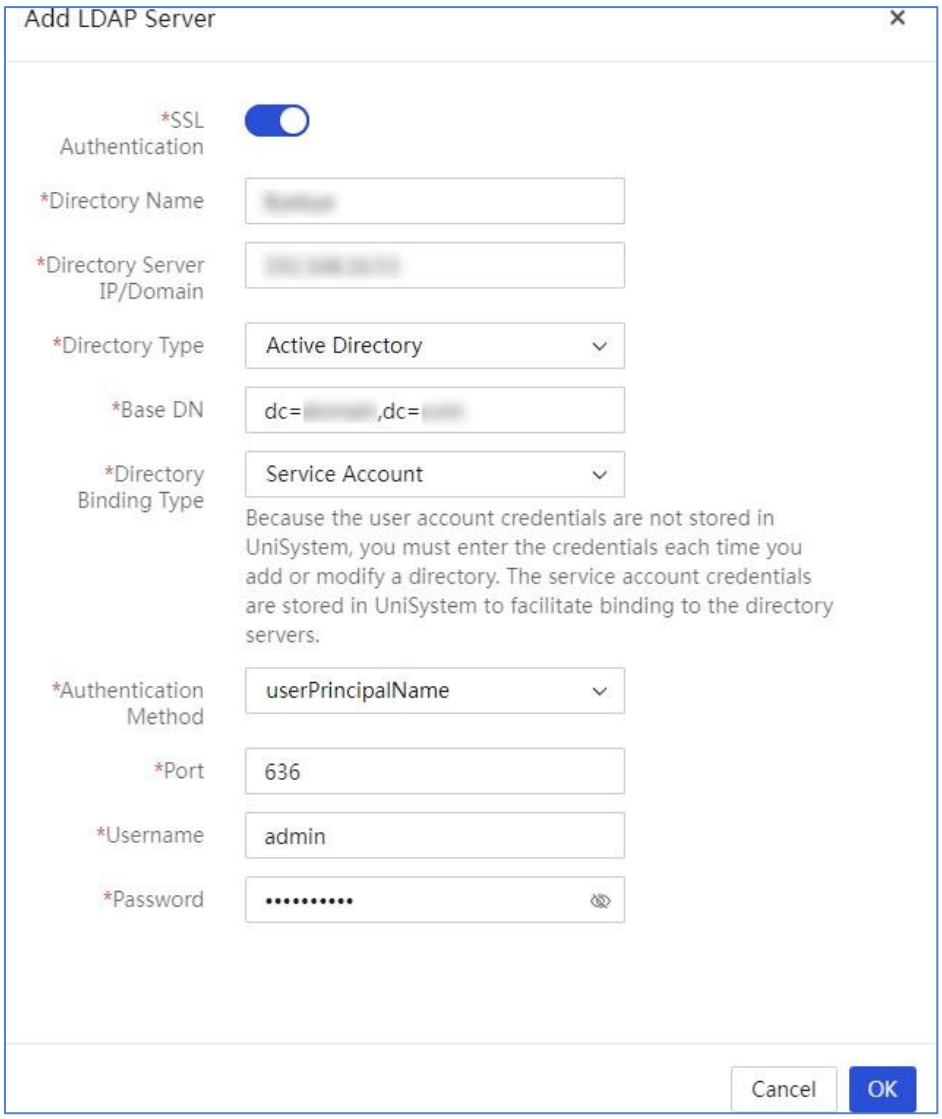
LDAPサーバーを追加する

LDAPサーバーをUniSystemに追加するには、次の作業を実行します。UniSystemは、最大100のLDAPサーバーをサポートします。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **LDAP Management**の順に選択します。
2. **Add LDAP Server**をクリックします。
3. 表示される**Add LDAP Server**ダイアログボックスで、LDAPサーバーのパラメータを設定します。

   図316 Add LDAP serverダイアログボックス



4. **OK**をクリックします。

LDAPサーバーの編集

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **LDAP Management**の順に選択します。

2. ターゲットLDAPサーバーの**Actions**列にある**Edit**アイコンをクリックします。
3. 表示された**Edit LDAP Server**ダイアログボックスで、LDAPサーバーのパラメータを編集し、OKをクリックします。

LDAPサーバーを削除する

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **LDAP Management**.の順に選択します。
2. ターゲットLDAPサーバーの**Actions**列で**Delete**アイコンをクリックします。
3. 表示された確認ダイアログボックスで、**OK**をクリックします。

SSL証明書の管理

Secure Sockets Layer(SSL)は、ネットワーク通信を暗号化するためのプロトコルであり、インターネットを介したデータ伝送のセキュリティと整合性を確保するために使用されます。SSL証明書は、SSLプロトコルでWebサイトのIDを修飾するデジタル証明書です。SSL証明書は、暗号化アルゴリズムとデジタル署名テクノロジを使用して、WebサイトのIDの真正性と信頼性を保証します。これにより、伝送中にデータが安全で改ざんされないことが保証されます。

カスタムSSL証明書をアップロードした後、HTTPS経由でWebサイトにアクセスしてシステムセキュリティを強化します。

UniSystem SSL証明書管理は、次の機能を提供します。

- **Self-signed certificate**: デフォルトでは、UniSystemは自己署名証明書を使用したHTTPSアクセスをサポートしています。
- **Certificate upload**: ユーザーはカスタムSSL証明書をアップロードできます。システムは、アップロードされた証明書をHTTPSアクセスに使用します。これにより、システムのセキュリティと柔軟性が向上します。
- カスタム証明書の有効期限が切れた場合、UniSystemは起動時に有効期限の状態を自動的に検出し、提供されたデフォルトの証明書の使用に戻ります。これにより、どのような状況でも安全な通信が保証されます。

SSL証明書情報の表示

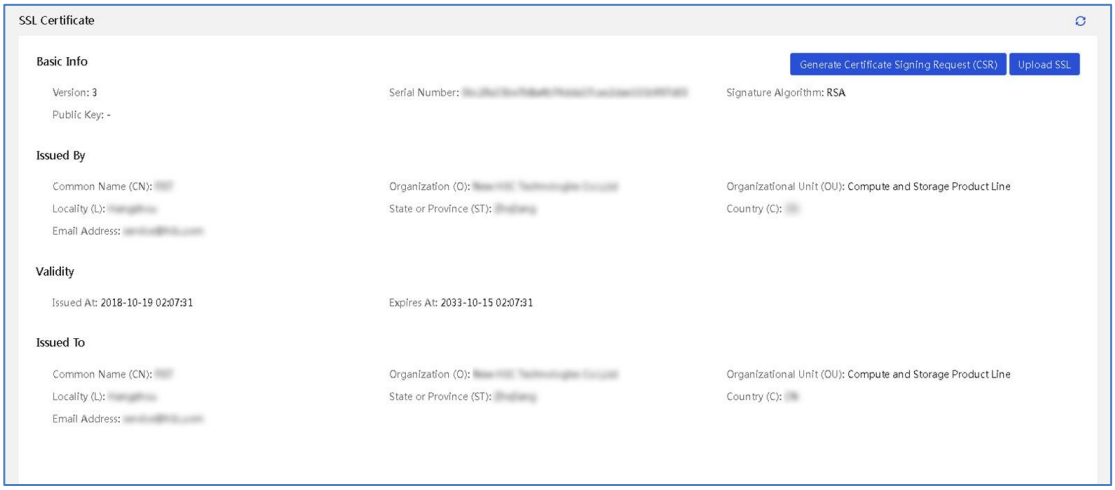
このタスクについて

UniSystemで使用されている現在の証明書に関する情報を表示するには、次のタスクを実行します。デフォルトでは、UniSystemは自己署名証明書を使用します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **SSL Certificate Management**を選択します。
2. 現在のSSL証明書の詳細情報を表示します。

図317 SSL証明書の管理



パラメータ

- 基本情報: 現在のSSL証明書の基本情報。
  - **Version**: SSL証明書のバージョン。
  - **Serial Number**: Certificate Authority(CA)によって証明書に割り当てられたシリアル番号。
  - **Signature Algo**rithm: SSL証明書が署名に使用する暗号化アルゴリズム。
  - **Public Key**: パブリックキー情報。
- **Issued By**: SSL証明書を発行したCAに関する情報。
- **Validity**: SSL証明書の有効期間。
  - **Issued At**: 証明書が有効になる最初の日。
  - **Expires At**: 証明書の有効期限。
- **Issued To**: 証明書の発行先エンティティ。

カスタム証明書をアップロードする

このタスクについて

UniSystemは、より信頼できるカスタムSSL証明書のアップロードをサポートし、より高いセキュリティと信頼性を提供します。

UniSystemでカスタム証明書をアップロードするプロセスは次のとおりです。

1. **Generate a certificate signing request**: UniSystemで証明書署名要求(CSR)を生成し、要求をダウンロードします。
2. **Submit the CSR to the corporate CA**: 生成されたCSRを署名のために企業CAに送信し、証明書チェーンファイルを取得します。
3. **Upload the custom certificate**: 証明書チェーンをUniSystemにアップロードします。再起動後、アップロードされた証明書を使用して、HTTPS経由でUniSystemにアクセスします。

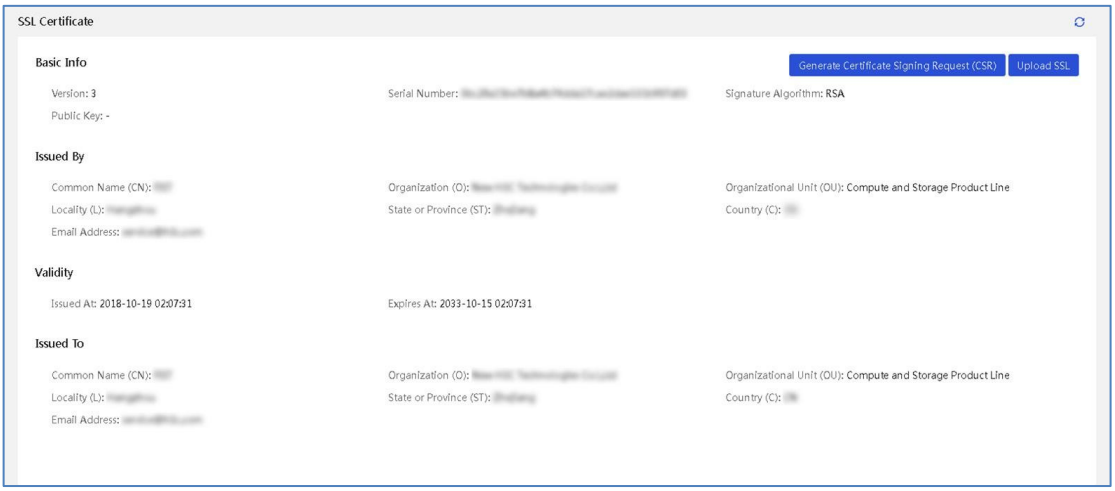
制約事項とガイドライン

- カスタムSSL証明書の有効期限が切れたら、できるだけ早く証明書を再アップロードして、その有効性を確認します。
- UniSystemは、起動時に期限切れの証明書を検出すると、組み込みのデフォルト証明書を使用します。

手順

1. ナビゲーションペインで、**Menu** > **System** > **Users and Security** > **SSL Certificate Management**.を選択します。

図318 SSL証明書の管理

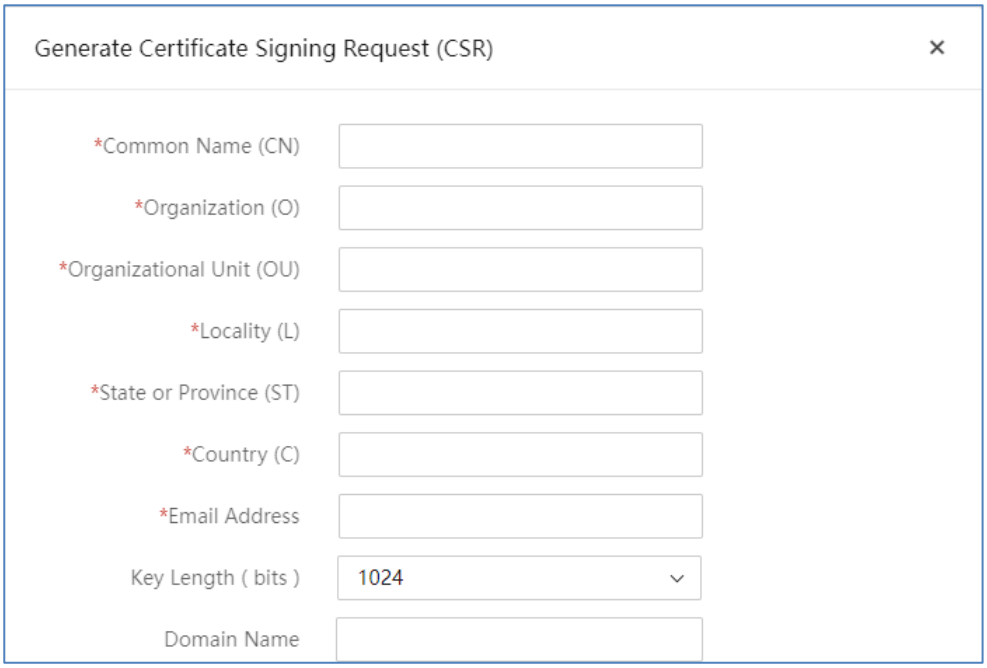


2. CSRを生成します。
   a. **Generate Certificate Signing Request(CSR)**をクリックします。
   b. CSR生成関連情報を設定します。
   c. **OK**をクリックしてCSRを生成し、ダウンロードします。

メモ:

SSL証明書をアップロードする前に、まずCSRを社内CAにアップロードし、署名プロセスを完了して、CAによって署名された証明書チェーンファイルを取得する必要があります。

図319 CSRの生成



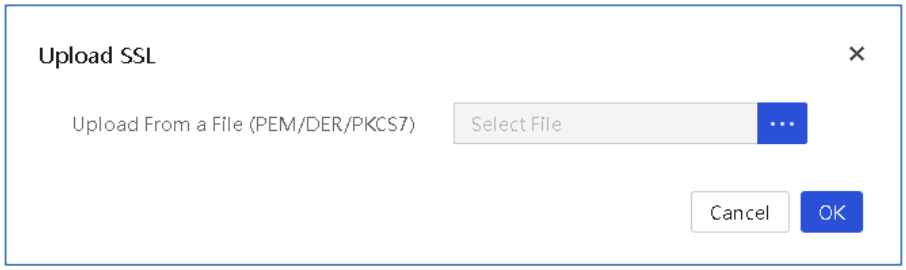
3. SSL証明書をアップロードします。

a. **Upload SSL**をクリックします。

b. アイコン…をクリックし、SSL証明書チェーンファイルを選択します。サポートされているファイル形式は、PEM、DERおよびPKCS7です。

c. **OK**をクリックします。証明書は、UniSystemの再起動後に有効になります。

図320 証明書のアップロード



パラメータ

- **Common Name(CN)**: サーバー所有者のフルドメイン名。
  - 文字列の範囲は1～64文字です。
  - 文字列に数字だけを含めることはできません。
  - サポートされているのは、文字、ロシア語、数字、スペース、アンダースコア(_)、ハイフン(-)、およびドット(.)のみです。
- **Organization (O)**: このサーバーを所有する会社または組織の名前。
  - 文字列の範囲は1～64文字です。
  - 文字列に数字だけを含めることはできません。
  - サポートされているのは、文字、ロシア語、数字、スペース、アンダースコア(_)、ハイフン(-)、ドット(.)、およびカンマ(,)のみです。
- **Organization Unit (OU)**: このサーバーを所有する会社または組織の単位。
  - 文字列の範囲は1～64文字です。
  - 文字列に数字だけを含めることはできません。
  - サポートされているのは、文字、ロシア語、数字、スペース、アンダースコア(_)、ハイフン(-)、およびドット(.)のみです。
- **Locality (L)**: このサーバーを所有する会社または組織がある市または郡。
  - stringの範囲は1～128文字です。
  - 文字列に数字だけを含めることはできません。
  - サポートされているのは、文字、ロシア語、数字、スペース、アンダースコア(_)、ハイフン(-)、およびドット(.)のみです。
- **State or Province(ST)**: このサーバーを所有する会社または組織がある州、自治体、または自治区。
  - stringの範囲は1～128文字です。
  - 文字列に数字だけを含めることはできません。
  - サポートされているのは、文字、ロシア語、数字、スペース、アンダースコア(_)、ハイフン(-)、およびドット(.)のみです。
- **Country (C)**: このサーバーを所有する会社または組織が存在する国または地域。国コードまたは地域コードには2文字しか使用できません。

- **Email Address**: このサーバーを所有する会社または組織の電子メールアドレス。
- **Key Length**: 証明書キーの長さ。
- **Domain Name**: SSL証明書には、様々なWebサイトのセキュリティ要件を満たすために、ドメイン名またはワイルドカードドメイン名を含めることができます。ドメイン名はSSL証明書の一部であり、証明書が指定されたドメインにのみ適用されることを保証し、そのドメインのセキュリティ保護を提供します。

略語

表21 頭字語

用語	定義
BIOS	基本入出力システム
CPLD	複合プログラマブル論理デバイス
CPU	中央処理装置
DHCP	動的ホスト構成プロトコル
FIST SMS	FIST System Management Serviceは、サーバーを管理するためにUniSystemとともに使用されるソフトウェアパッケージです。
GUI	グラフィカルユーザーインタフェース
HBA	ホストバスアダプタ
HDM	ハードウェアデバイスの管理
IPMI	インテリジェントなプラットフォーム管理インターフェイス
OS	オペレーティングシステム
PXE	プリブート実行環境
RAID	独立したディスクの冗長アレイ
SDS	セキュア診断システム
UEFI	ユニファイドエクステンシブルファームウェアインタフェース

付録Aディスクレスブート互換OSのインストール

概要

iSCSIに準拠して、UniSystemが提供するディスクレスブートを使用すると、サーバーはローカルドライブではなくリモートストレージボリュームからオペレーティングシステムをブートできます。ストレージボリュームにオペレーティングシステムを手動でインストールして、ディスクレスブートを実装できます。

ディスクレスブートをサポートするOSは、次のとおりです。

- Red Hat Enterprise Linux 7.5(64ビット)
- CentOS 7.5(64ビット)
- VMware ESXi 6.5 U2(64ビット)
- VMware ESXi 6.7(64ビット)

制約事項とガイドライン

ディスクレスブートを使用する場合は、ローカルドライブをデータドライブとしてのみ使用し、ローカルドライブにOSやシステムブートプログラムがインストールされていないことを確認することをお勧めします。そうしないと、OSのインストール後にディスクレスブートプロセスが影響を受ける可能性があります。

手順

UniSystemのインストール

UniSystemのインストール方法については、「UniSystem Installation Guide」を参照してください。

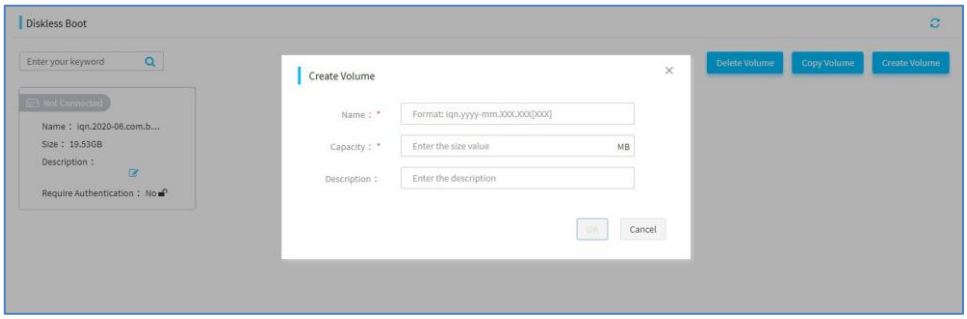
OSイメージファイルを準備する

OSの公式WebサイトからOSの.isoイメージファイルをダウンロードします。

ストレージボリュームを作成する

1. UniSystemにログインします。
2. ナビゲーションペインで、**Menu** > **Templates** > **Diskless Boot**を選択します。
3. **Create Volume**をクリックして、ボリュームを作成します。

図1 ボリュームの作成



AEモジュールのIPアドレスを設定します。

UniSystemサーバーがAEモジュールで実行されている場合は、次のネットワークポートを使用できます。

- **vmng**: OMモジュールのサービスネットワークポートに接続されているネットワークポート。
- **vmng. Om**: OMモジュールの管理ネットワークポートに接続されているネットワークポート。
- **enp5s0f0**: インターコネクトモジュール1に接続されているネットワークポート。
- **enp5s0f1**: インターコネクトモジュール4に接続されているネットワークポート。

UniSystemをサーバーに接続するネットワークポートのIPアドレスを構成する必要があります。このIPアドレスは、iSCSIサーバーのIPアドレスとして使用されます。

制約事項とガイドライン

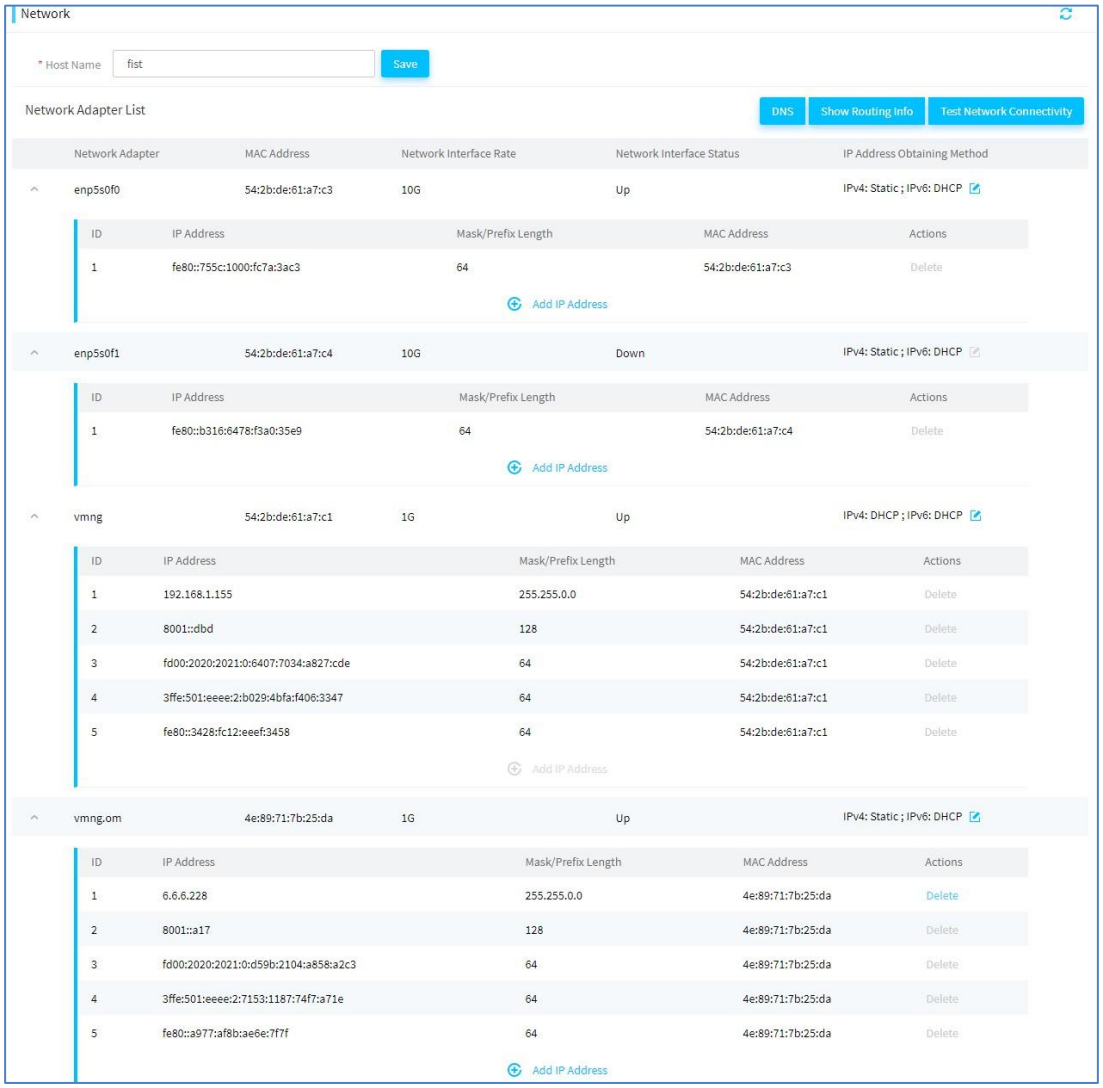
ストレージボリュームが作成されるサーバーとAEモジュールが同じエンクロージャー内にある場合は、サーバーのEthernetアダプターがインターコネクトモジュール1または4に接続されていることを確認してください。

ストレージボリュームを作成するサーバーとAEモジュールが異なるエンクロージャーにある場合は、AEモジュールのEthernetアダプターがスイッチを介してサーバーに接続されていることを確認してください。

手順

1. UniSystemにログインします。
2. ナビゲーションペインで、**Menu** > **System** > **Network**を選択します。
3. UniSystemをサーバーに接続するネットワークポートを識別します。
4. **Add IP Address**をクリックして、ネットワークポートのIPアドレスを設定します。

図2 AEモジュールのIPアドレスの設定

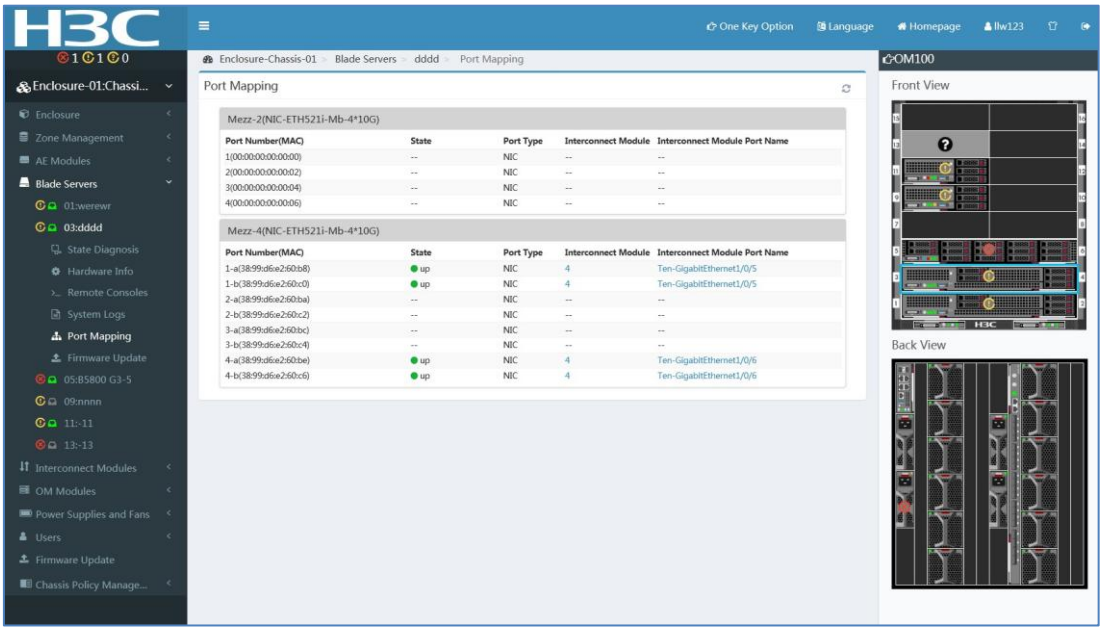


BIOSを使用してサーバーのEthernetアダプターを設定します。

手順

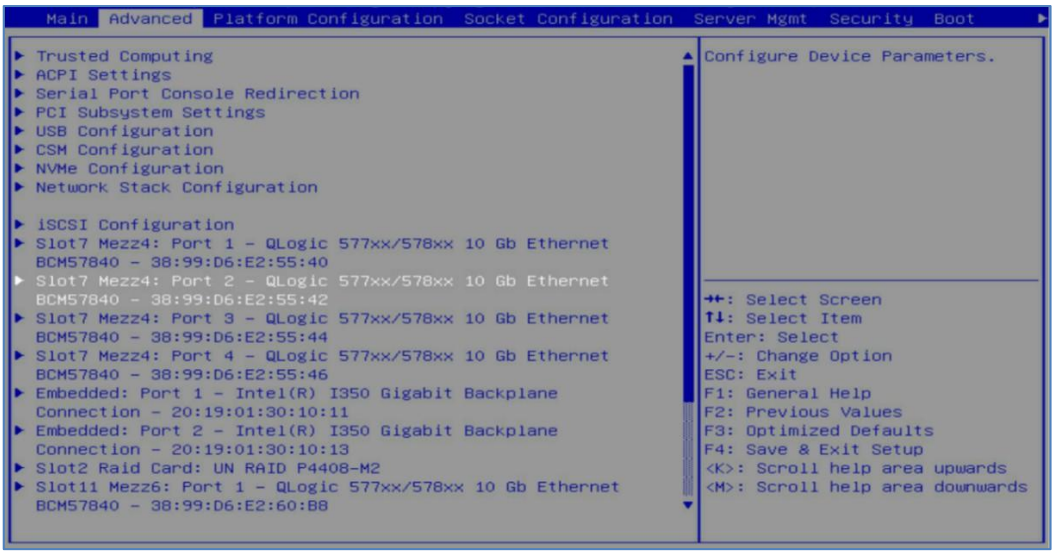
1. サーバーのOMにログインし、**Blade Servers** > ***Blade_Server*** > **Port Mapping**を選択します。次に、ディスクレスブートを実行するサーバーのイーサネットアダプターの場所を特定し、イーサネットアダプターに接続されているインターコネクトモジュールが存在することを確認します。

図3 OMでのポートマッピング



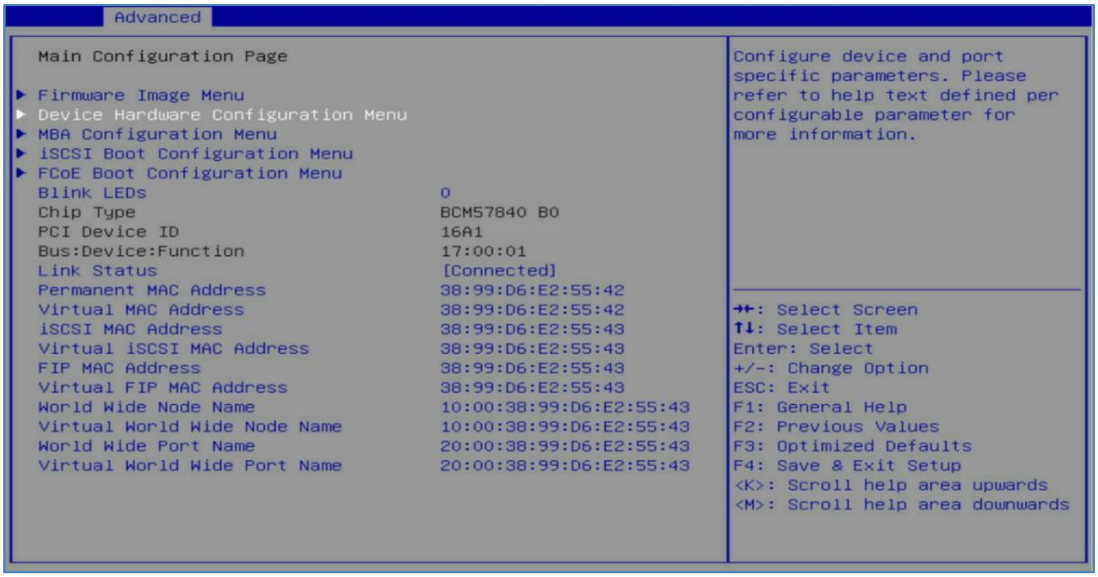
2. BIOSセットアップユーティリティを起動し、**Advanced**を選択し、Ethernetアダプターの**Slot x Port x**エントリを選択して、**Enter**キーを押します。

図4 Advanced画面



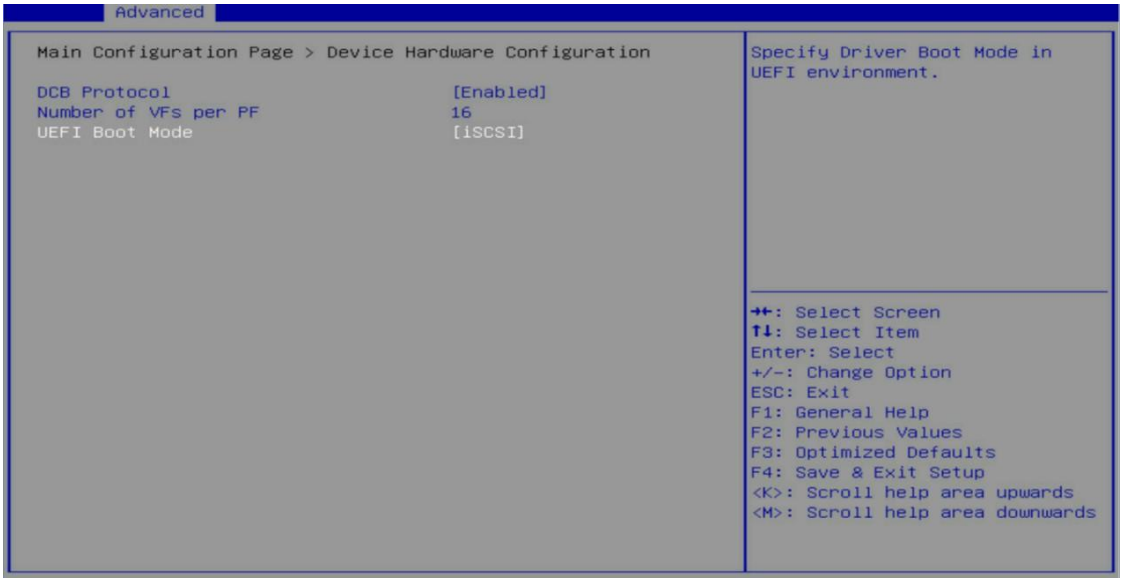
3. リンクのステータスが**Connected**であることを確認し、**Enter**キーを押します。

図5 Main Configuration Page画面



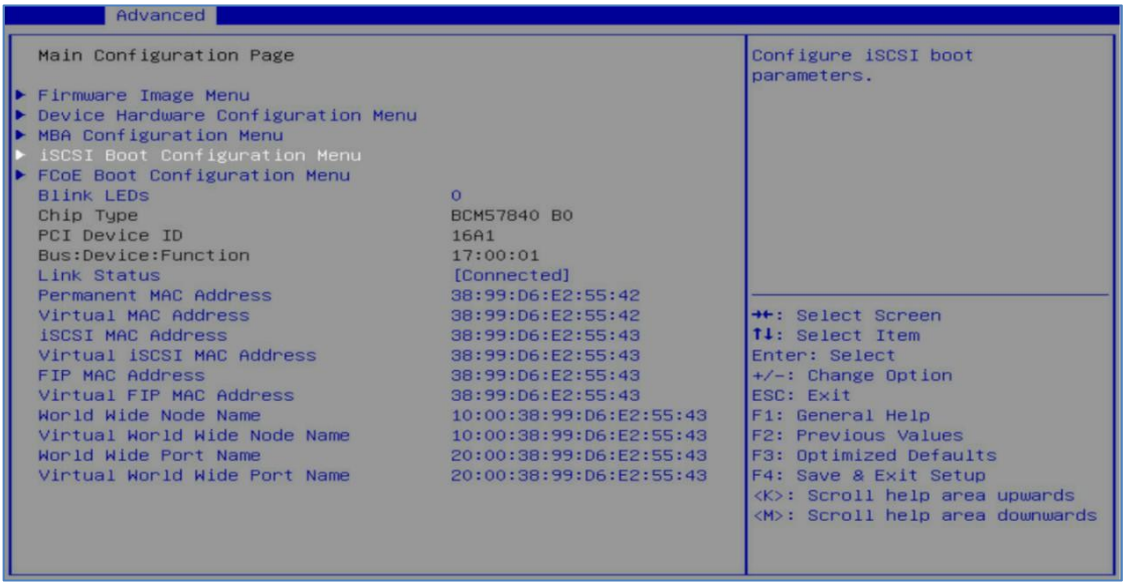
4. UEFIブートモードを**iSCSI**に設定し、**Enter**キーを押します。

図6Device Hardware Configuration(デバイスハードウェア設定)メニュー



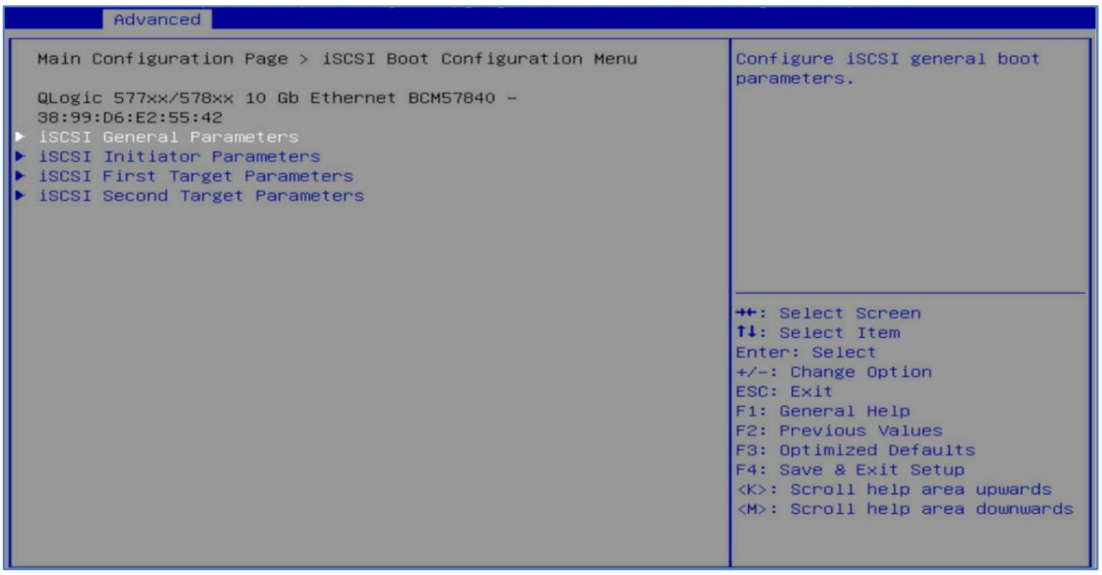
5. **Esc**キーを押し、**iSCSI Boot Configuration Menu**を選択して、**Enter**キーを押します。

図7 メイン設定ページのメニュー画面



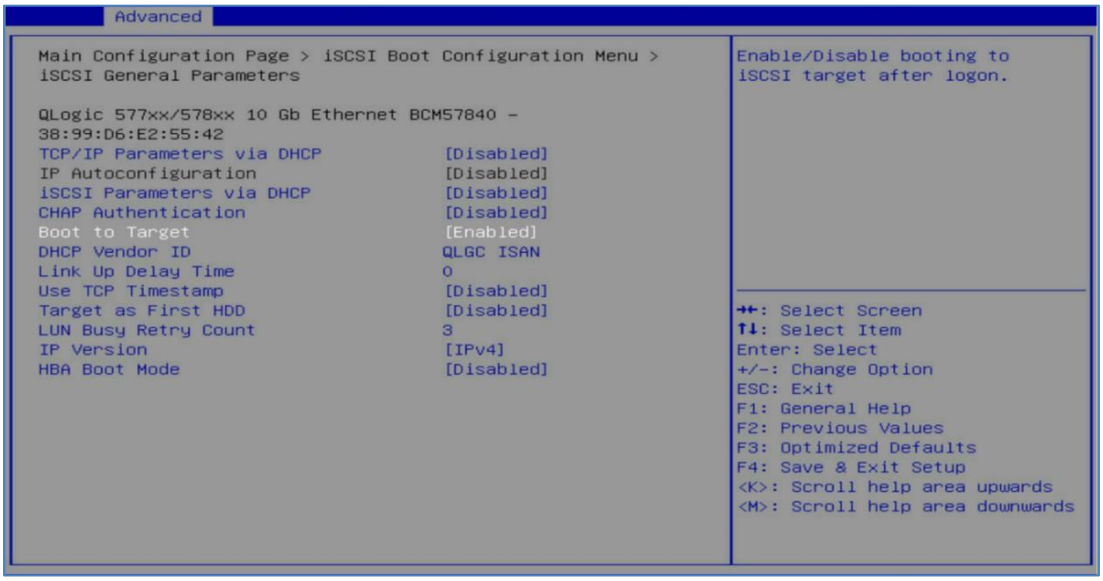
6. **iSCSI General Parameters**を選択し、**Enter**キーを押します。

図8 iSCSI Boot Configuration Menu画面



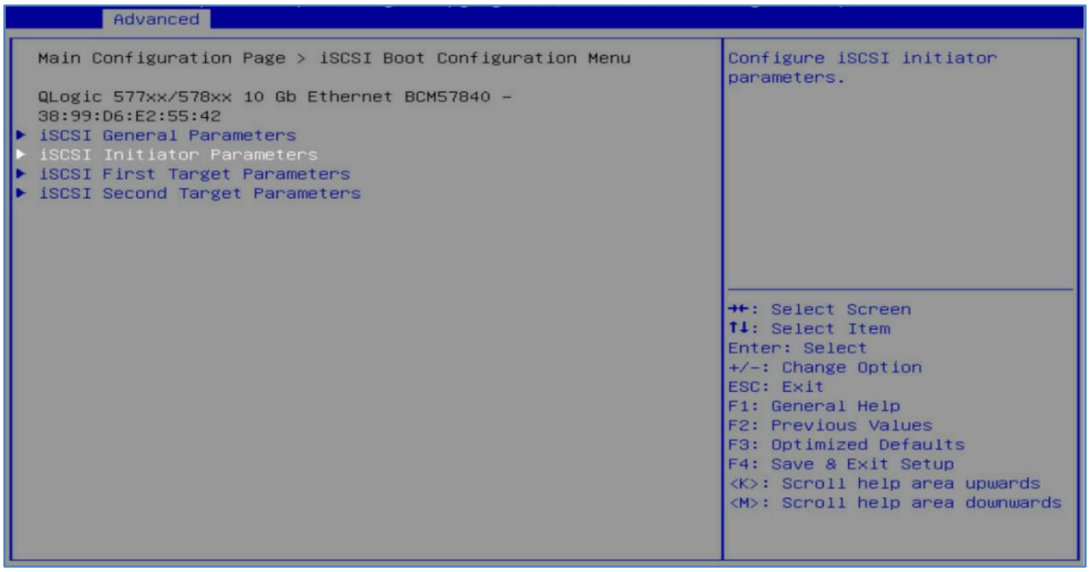
7. 一般的なiSCSIパラメータを次のように設定します。
   a. DHCPを使用してネットワークポートにIPアドレスを割り当てる場合は、**TCP/IP Parameters via DHCP**を有効にします。IPアドレスを静的に割り当てるには、このパラメータを無効にします。
   b. ストレージボリュームで認証が有効になっている場合は、**CHAP Authentication**を有効にします。
   c. **Boot to Target**を有効にします。
   d. その他のパラメータについては、既定の設定を使用します。
   e. **Enter**を押します。

図9 iSCSI General Parametersサブメニュー画面



8. **Esc**キーを押し、**iSCSI Initiator Parameters**を選択して、**Enter**キーを押します。

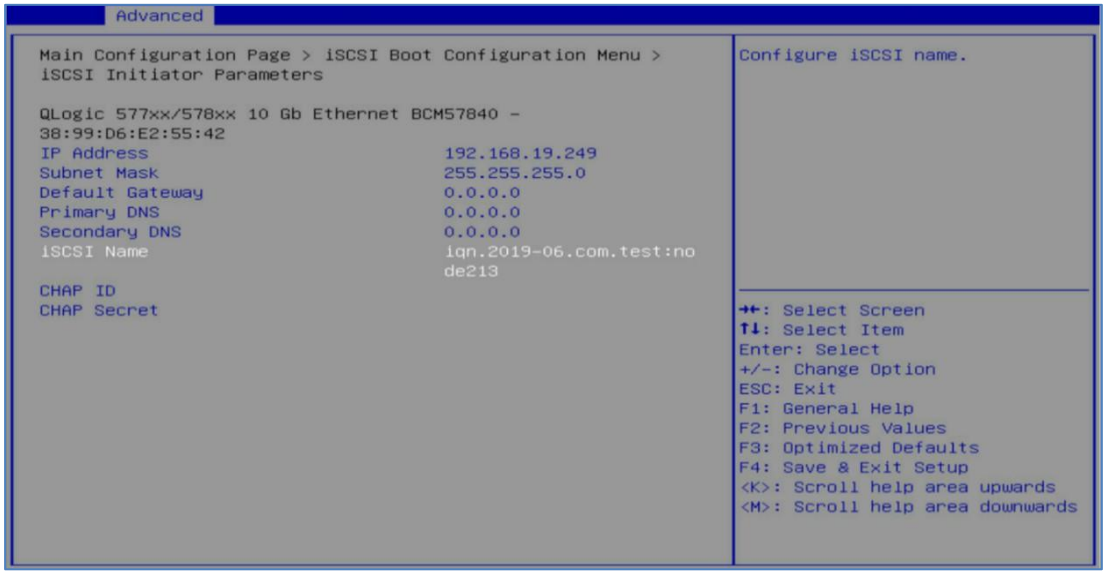
図10 iSCSI Boot Configuration Menu画面



9. iSCSIイニシエータパラメータを次のように構成します。
   a. (オプション。) **TCP/IP Parameters via DHCP**が無効になっている場合は、IPアドレスとサブネットマスクを設定します。Ethernetアダプタは、IPアドレスを使用してストレージボリュームと通信します。
   b. (任意)必要に応じて、デフォルトゲートウェイとDNS設定を設定します。
   c. iSCSI名を設定します。これは、Ethernetアダプターがストレージボリュームへの接続に使用する一意のIQN名です。
   d. (オプション)ストレージボリュームに対してCHAP認証が有効になっている場合は、CHAP IDとCHAPシークレット(ストレージボリュームの認証情報)を設定します。

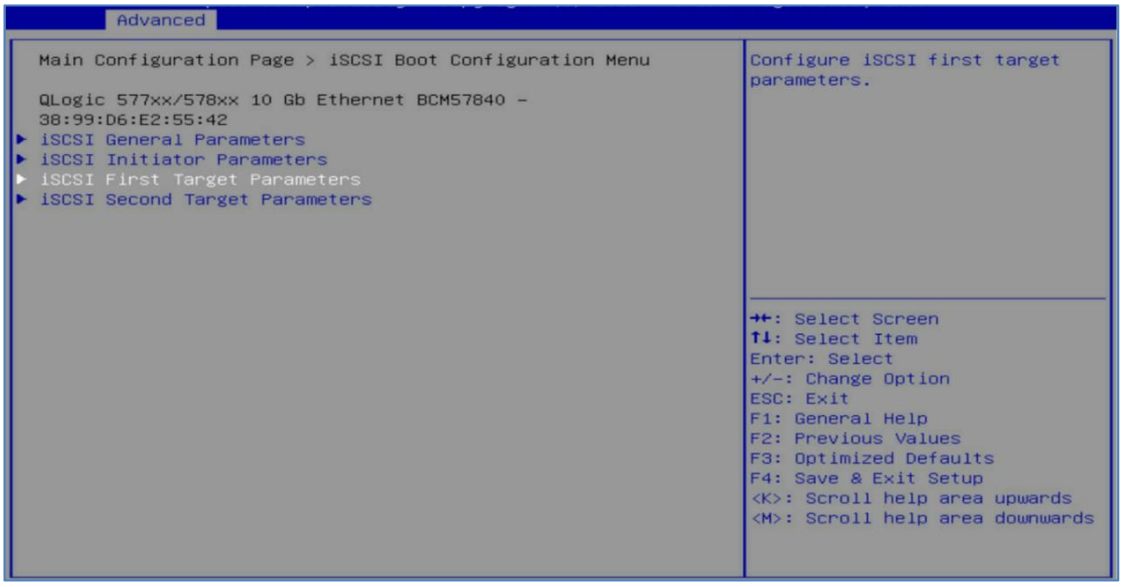
      iSCSIターゲットパラメータを編集するたびに、CHAP IDとCHAPシークレットをリセットする必要があります。

図11 iSCSI Initiator Parametersサブメニュー画面



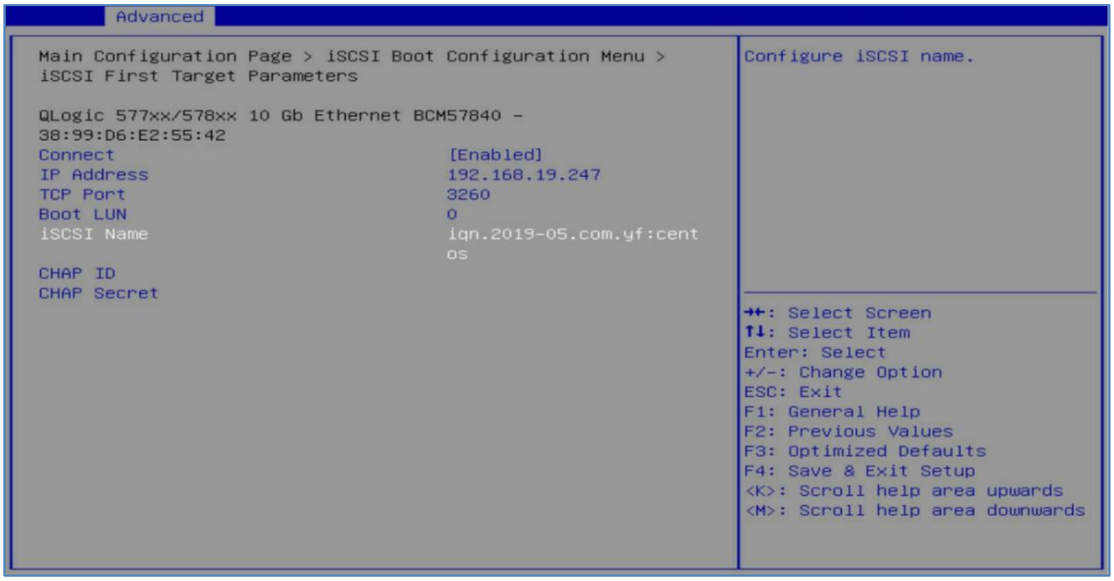
10. **Esc**キーを押し、**iSCSI First Target Parameters**を選択して、**Enter**キーを押します。

図12 iSCSI Boot Configuration Menu画面



11. iSCSIターゲットのパラメータを次のように設定します。
    a. 接続設定を有効にするには、**Connect**を有効にします。
    b. iSCSIサーバーのIPアドレスを設定します。これは、「AEモジュールのIPアドレスを設定する」で設定したAEモジュールのネットワークポートのIPアドレスです。
    c. iSCSI名(AEモジュールで作成されたストレージボリュームのIQN名)を設定します。
    d. その他のパラメータについては、既定の設定を使用します。
    e. **Enter**を押します。

図13i SCSI First Target Parametersサブメニュー画面



12. サーバーを再起動して、設定変更をコミットします。

OSのインストール

必要に応じて、様々な方法でOSをインストールできます。この例では、サーバーのKVMにマウントされたインストールイメージを使用します。

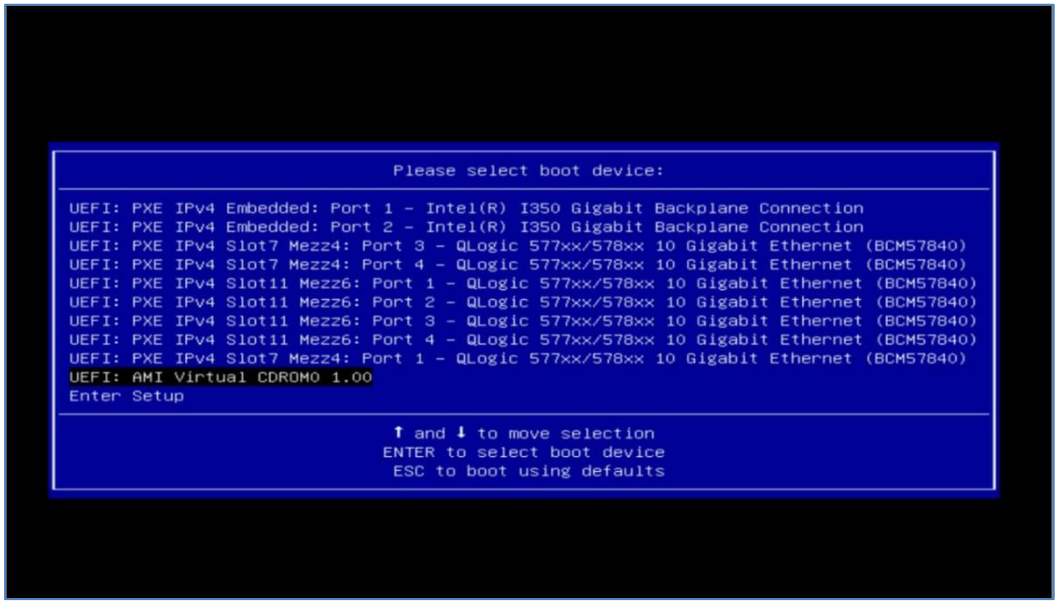
前提条件

サーバーのKVMを起動し、標準インストールイメージをマウントして、サーバーを再起動します。

Redhat/Centos7.5のインストール

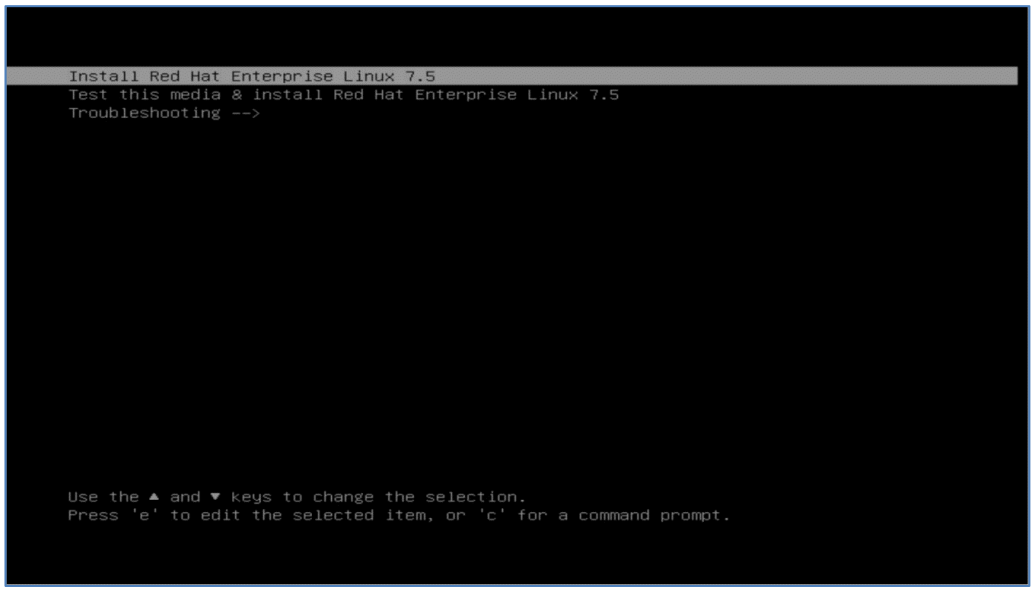
1. サーバーのBIOSセットアップユーティリティを起動します。
2. ブートデバイスとして仮想CDROMを選択し、**Enter**キーを押します。

図14 Bootメニュー



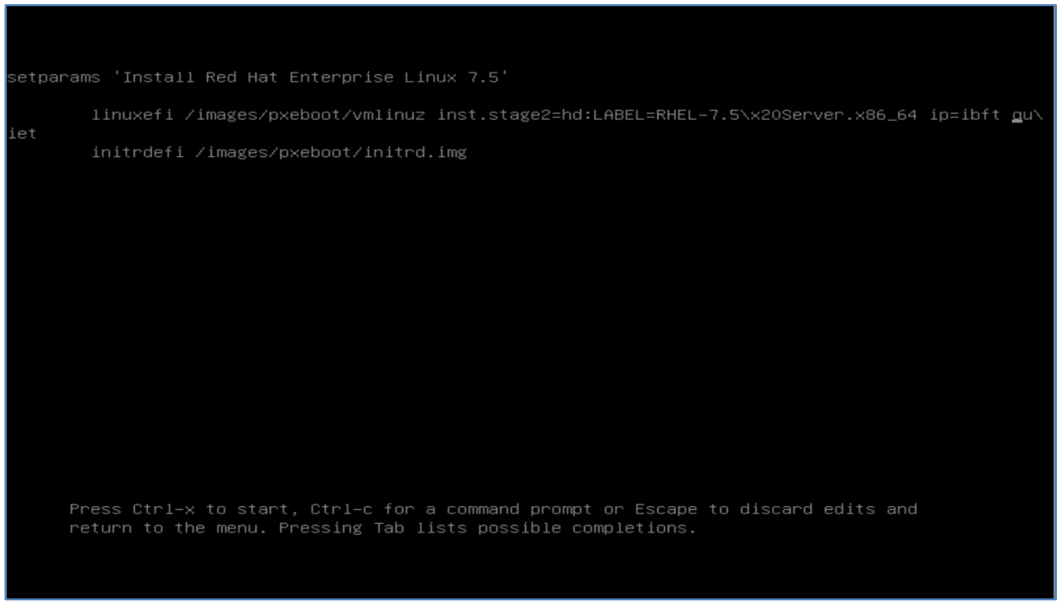
3. 起動時のスプラッシュ画面で、最初または2番目の項目を選択し、**e**キーを押します。

図15 起動時のスプラッシュ画面



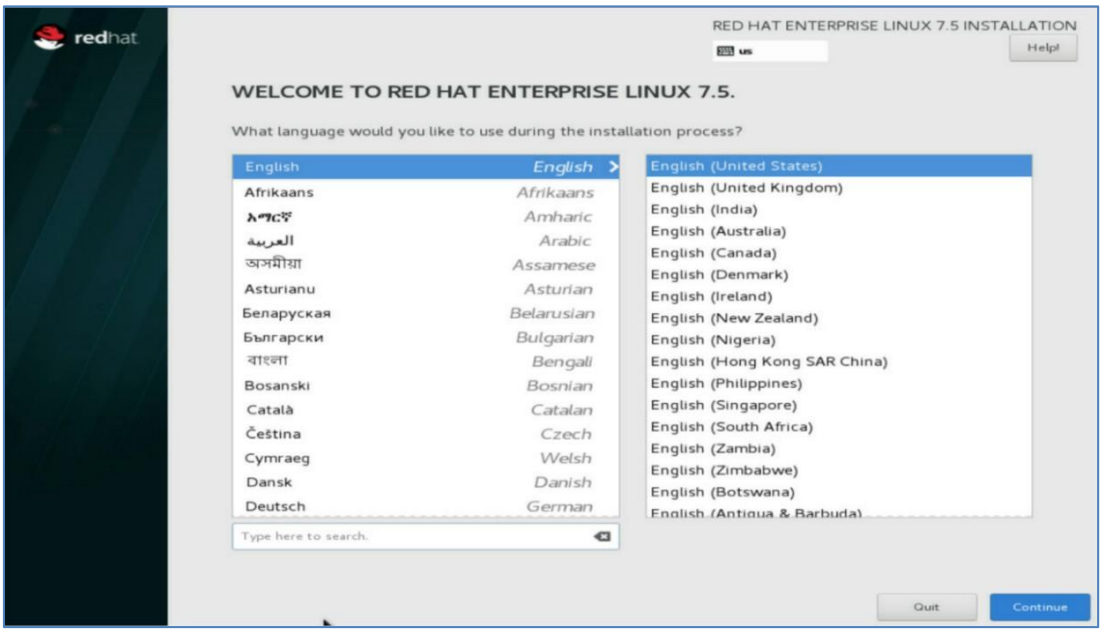
4. 2行目で、**ip=ibft**と入力し、**quit**の前にスペースを入れます。
Ctrl+xを押します。

図16 パラメータ設定画面



5. ようこそ画面で言語を選択し、**Continue**をクリックします。

図17 初期画面



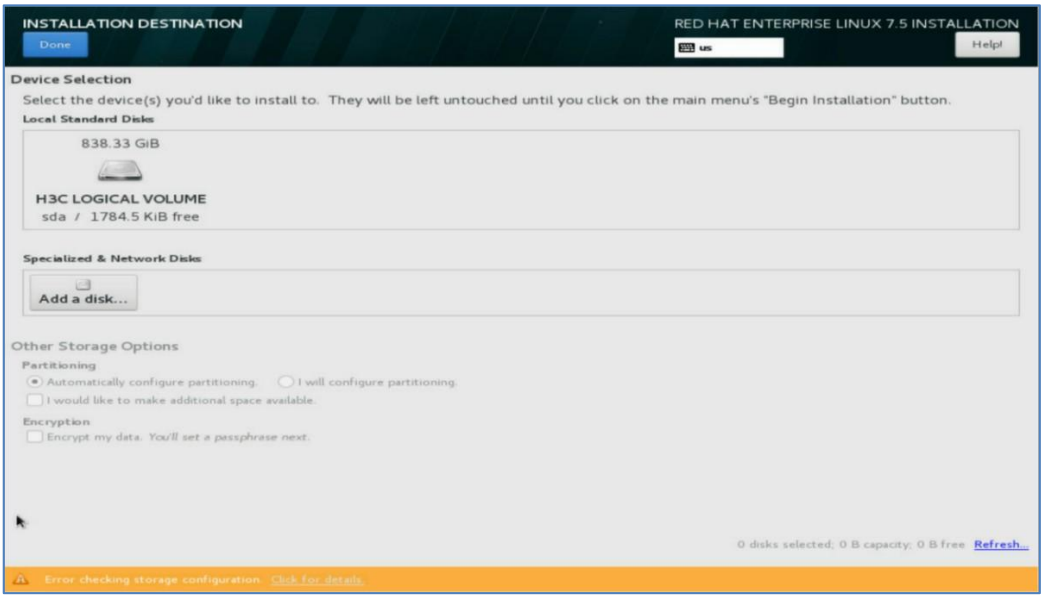
6. インストールの概要画面で、**NETWORK & HOSTNAME**セクションに**ibft0 connected**が表示されていることを確認します。これはシステムがBIOSでEthernetアダプターの設定を取得していることを示します。

図18 インストールの概要画面



7. **INSTALLATION DESTINATION**をクリックして、ターゲットインストールドライブを選択します。この例では、AEモジュールで作成されたストレージボリュームが使用されます。
8. **INSTALLATION DESTINATION**画面で、**Specialized & Network Disks**セクションの**Add a disk**をクリックします。**Local Standard Disks**でローカルディスクを選択しないでください。

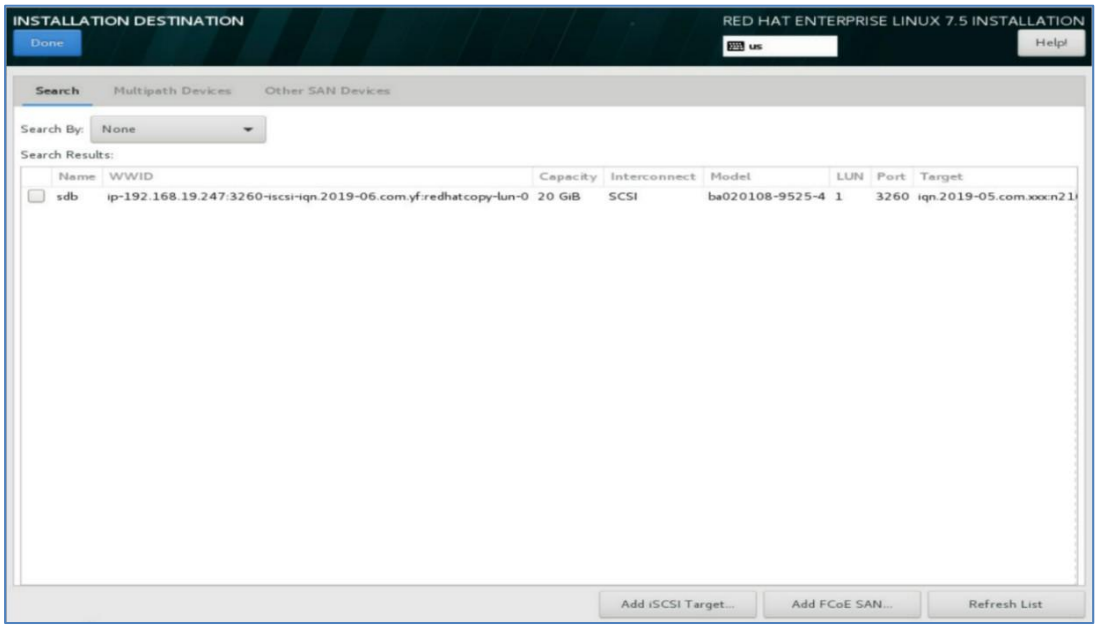
   図19 INSTALLATION DESTINATION画面



9. **Add a disk**画面で、iSCSIストレージコントローラーのIQN名と容量が正しいことを確認します。次に、このiSCSIストレージコントローラーを選択し、**Done**をクリックします。

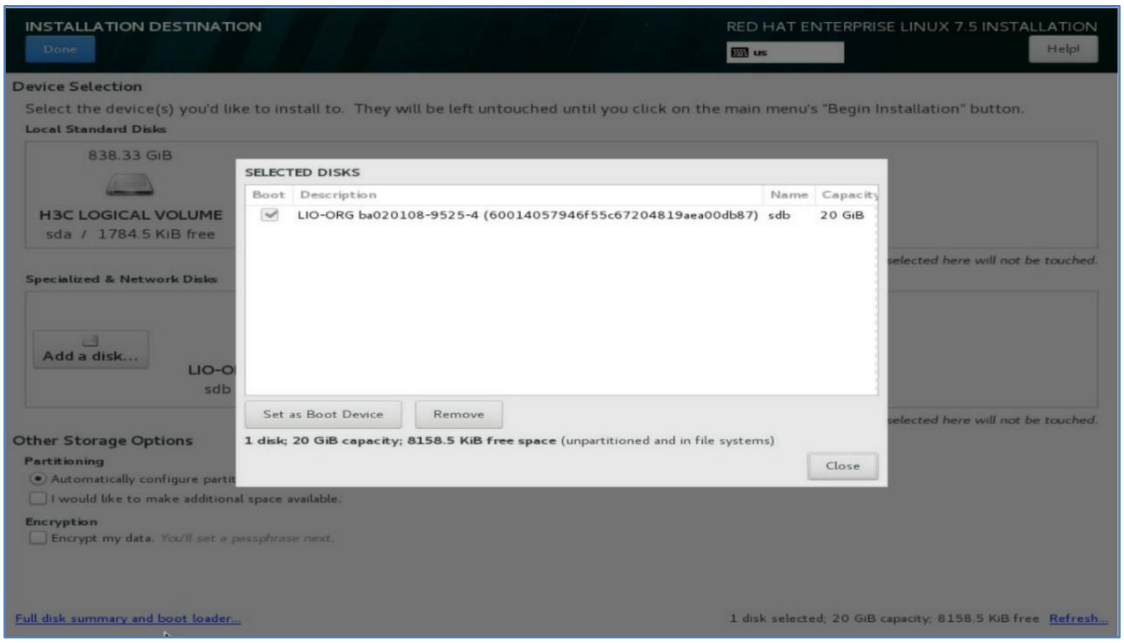
   iSCSIストレージコントローラーが表示されない場合は、Ethernetアダプターが正しく設定され、ネットワーク環境が正しくセットアップされていることを確認してください。

図20 ディスクの追加画面



10. **INSTALLATION DESTINATION**画面の左下隅にある**Full disk summary and boot loader**をクリックします。表示されたダイアログボックスで、iSCSIストレージボリュームのブートデバイスが正しいことを確認し、ブートデバイスを選択して**Close**をクリックします。

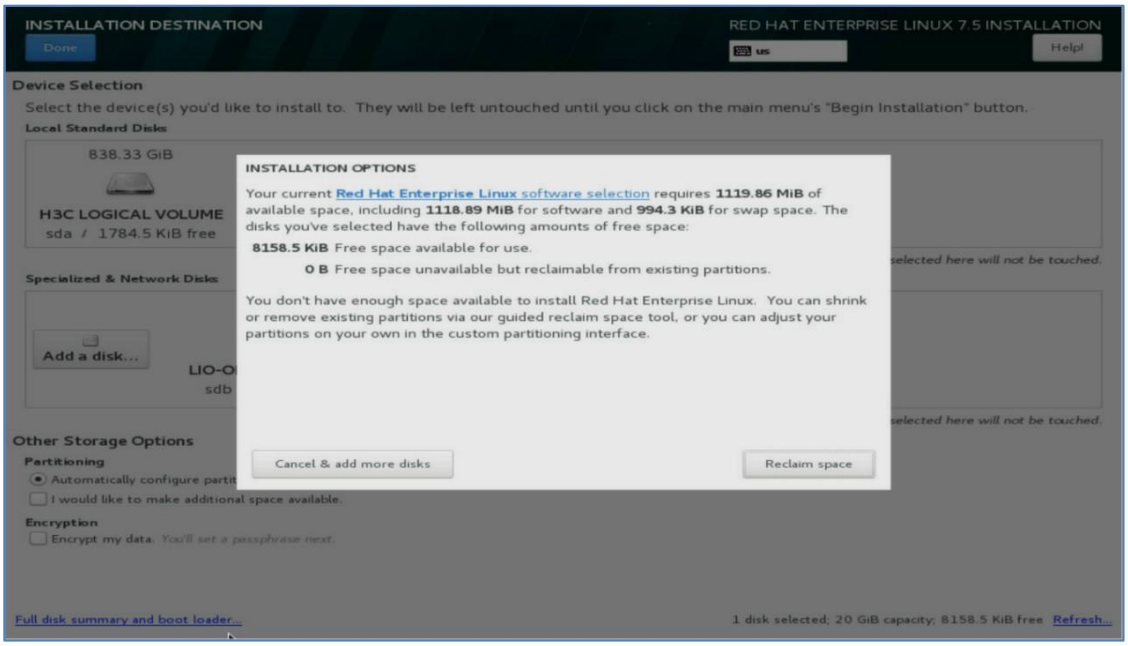
    図21 SELECTED DISKSダイアログボックス



11. **Other Storage Options**セクションで、**Partitioning**パラメータの分配法を選択します。この例では、自動パーティション化を使用しています。

    iSCSIストレージボリュームにすでにパーティションがある場合は、パーティションの再分割を求めるメッセージが表示されます。**Reclaim space**をクリックしてから、iSCSIストレージボリュームのパーティションを再分割します。

図22 INSTALLATION OPTIONS画面



12. 必要なインストールイメージを選択し、その他のインストールパラメーターを構成します。詳細は、『H3C Servers Operating System Installation Guide』を参照してください。
13. **Begin Installation**をクリックし、インストールが完了するまで待ちます。

図23 インストールの概要画面



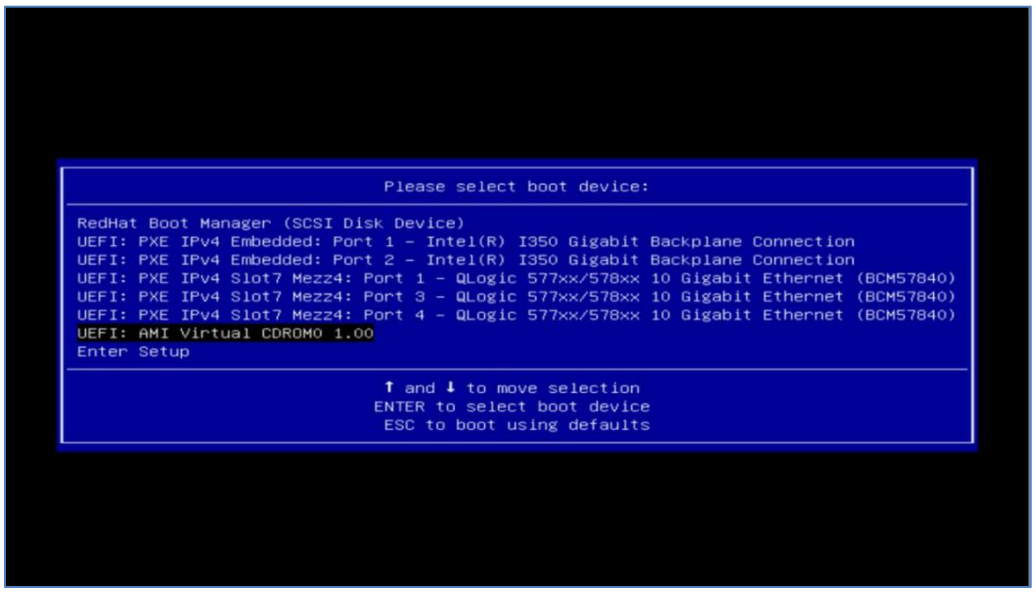
14. サーバーを再起動します。
15. (オプション)iSCSIストレージボリュームをコピーして、UniSystem内の他のサーバーでディスクレスブートを実行できます。

VMware ESXi 6.5 U2/ESXi 6.7のインストール

1. サーバーのBIOSセットアップユーティリティを起動します。
2. ブートデバイスとして仮想CDROMを選択し、**Enter**キーを押します。この例では、ESXi 6.5

U2を使用しています。ESXi 6.7の場合、インストール手順は同じです。

図24 起動メニュー画面



3. ESXiインストーラーのロードが完了するまで待ちます。

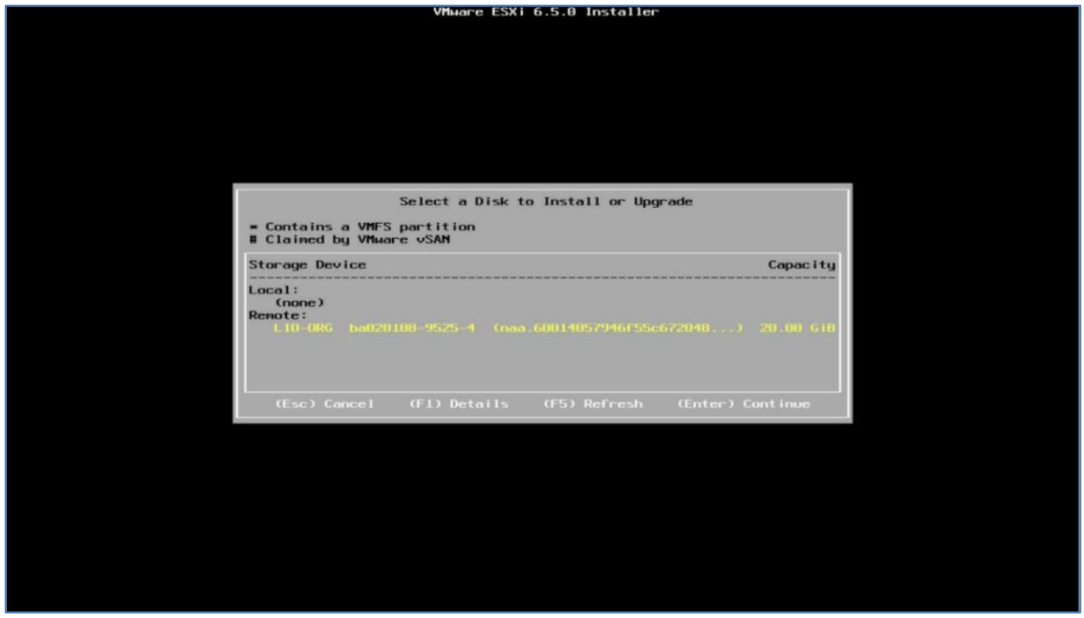
図25 ESXiインストーラーのロード画面



4. 表示されたダイアログボックスで、iSCSIストレージボリュームを選択し、**Enter**キーを押します。

   iSCSIストレージボリュームが表示されない場合は、Ethernetアダプターが正しく構成され、ネットワーク環境が正しく設定されていることを確認します。

図26 OSをインストールするドライブの選択



5. (オプション)表示された**Confirm Disk Selection**ダイアログボックスで、**OK**をクリックします。iSCSIストレージボリュームにすでにパーティションがある場合、システムはストレージボリュームを上書きします。

図27 ドライブ上のパーティションの上書き

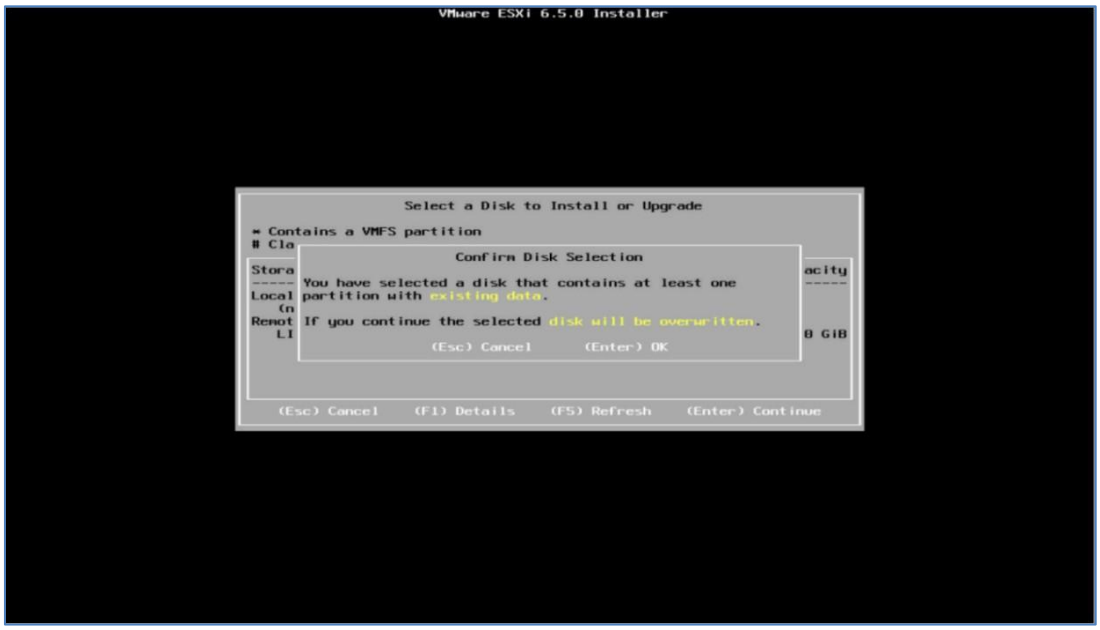


図28 ドライブのパーティションの再設定



6. 言語やrootパスワードなど、その他のインストールパラメーターを設定します。
7. インストールを開始し、インストールが完了するまで待ちます。
8. サーバーを再起動して、ESXiシステムを起動します。
9. (オプション)iSCSIストレージボリュームをコピーして、UniSystem内の他のサーバーでディスクレスブートを実行できます。

付録B:UniSystem VGAを使用

UniSystemがAEモジュールまたはバーチャルマシンにインストールされた後、UniSystemサーバーのWebインターフェイスによって提供される機能は、UniSystemビデオグラフィックスアレイ(VGA)と呼ばれます。UniSystem VGAのWebインターフェイスでは、サーバーIPを設定し、ブレードサーバーシステムを表示できます。

UniSystem VGAにアクセスするには、UniSystemサーバーを起動するだけです。パスワードは必要ありません。

Webインターフェイスのレイアウト

UniSystem VGAのWebインターフェイスは、図29に示すとおりです。Webインターフェイスには、表1に示すように、上部のバーセクションと作業セクションが含まれています。

図29 UniSystem VGAのWebインターフェイス

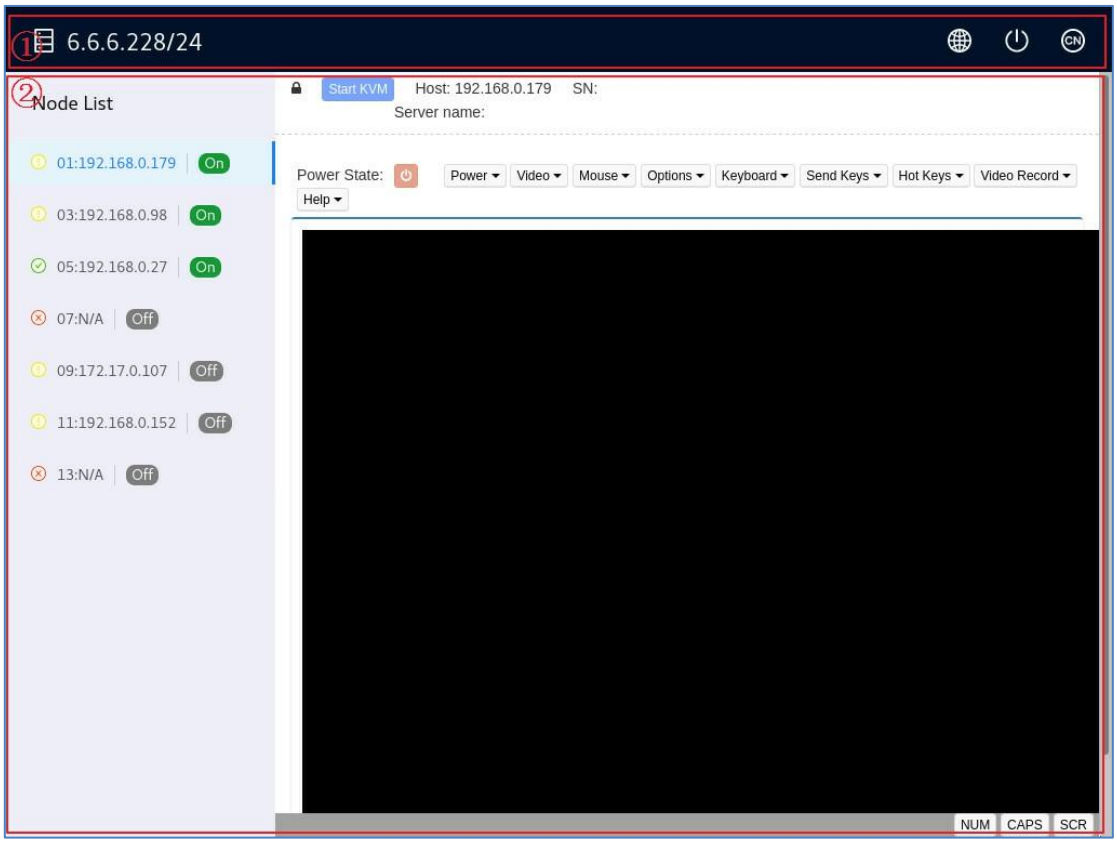


表1 Webインターフェイスのレイアウト

項番	セクション	説明
1	ヘッダーセクション	UniSystemサーバーのIPアドレスが左側に表示されます。右側には次のボタンがあります。 • : UniSystem サーバーの IP アドレスを設定するためにネットワークウィンドウを開くことができるボタン。 • :電源ボタン。
2	作業セクション	左ペインのノードリストには、AEモジュール内のブレードサーバーノードとそのステータスが表示されます。 右側のペインには、左側のペインで選択したブレード サーバーの KVM コンソールが表示されます。 メモ: 仮想マシンにインストールされたUniSystemの場合、作業セクションは空白です。

関数

ブレードサーバーのKVMコンソールへのアクセス(AEモジュールの場合のみ)

1. UniSystem VGAのWebインターフェイスにアクセスします。

   左側のノードリストには、AEモジュール内のすべてのブレードサーバーノードのHDM IPアドレスが表示されます。
2. ブレードサーバーノードを選択します。

   ブレードサーバーのKVMコンソールが右側のペインに表示されます。

UniSystemサーバーのIPアドレスの構成

1. UniSystem VGAのWebインターフェイスにアクセスします。
2. 右上隅にある**Network Settings**アイコン をクリックします。
3. 開いた**Network**ウィンドウで、UniSystemサーバーのシステムIPアドレスを設定します。

図30 UniSystemサーバーのIPアドレスの構成

