H3Cサーバー
HDM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:HDM-2.29以上
ドキュメントバージョン:6W100-20210414

前書き

ここでは、マニュアルに関する次の項目について説明します。

- 対象読者
- 表記規則。
- ドキュメントのフィードバック。

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 Serverで作業するサーバー管理者。

表記規則

次に、この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

コンベンション	説明
ボールド体	太字のテキストは、図のように文字どおりに入力したコマンドとキーワードを表します。
斜体	イタリックのテキストは、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)を示します。
{ 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ます。この中から1つを選択します。
[x | y | ...]	角括弧で囲まれたオプションの構文選択肢は、縦棒で区切られます。この中から1つを選択するか、または何も選択しません。
{ x | y | ... } *	アスタリスクの付いた中括弧は、必要な構文の選択肢のセットを縦棒で区切って囲み、そこから最小1つを選択します。
[x | y | ...] *	角カッコで囲まれたアスタリスクは、オプションの構文の選択肢を縦棒で区切って示しています。この選択肢から、1つの選択肢、複数の選択肢、またはなしを選択します。
&<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。
#	シャープ記号(#)で始まる行はコメントです。

GUIの規則

コンベンション	説明
ボールド体	ウィンドウ名、ボタン名、フィールド名およびメニュー項目は太字で表示されます。たとえば、New userウィンドウがオープンしたら、OKをクリックします。

>	マルチレベルメニューは山括弧で区切られます。たとえば、File > Create > Folder。

記号

コンベンション	説明
⚠警告!	重要な情報に注意を喚起する警告で、それが理解されていない場合やそれに従っていない場合は、けがをする可能性があります。
△注意:	重要な情報に注意を喚起するアラートです。情報が理解されていない場合や情報に従っていない場合は、データの損失、データの破損、ハードウェアまたはソフトウェアの損傷につながる可能性があります。
ⓘ重要:	重要な情報に注意を喚起するアラート。
注:	追加または補足の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

コンベンション	説明
	ルーター、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。
	ルーターやレイヤ3スイッチなどのルーティング可能な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転送およびその他のレイヤ2機能をサポートするルーターを表します。
	アクセスコントローラー、統合有線WLANモジュール、または統合有線WLANスイッチ上のアクセスコントローラー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。
	全方向の信号を表します。
	指向性信号を表します。
	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。

本書に記載されている例

この文書の例では、ハードウェアモデル、構成、またはソフトウェアバージョンがデバイスと異なるデバイスを使用する場合があります。通常、例のポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイス上にあるものとは異なります。

ドキュメントのフィードバック

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。ご意見をいただければ幸いです。

内容

HDMについて

はじめに

Hardware Device Management(HDM)は、次の豊富な機能を提供するリモートサーバー管理システムです。

- さまざまな管理インターフェース
  - HDMは、さまざまなシステム統合要件を満たすために、IPMI、HTTPS、SNMP、およびRedfishを提供します。
  - HDMは、IPMI v1.5およびIPMI v2.0と互換性があり、標準管理システム統合用の標準管理インターフェースを提供します。
- リモートメンテナンス
  - HDMは、KVM(キーボード、ビデオ、マウス)および仮想メディアを介したサーバーへのリモートアクセスを提供し、便利なサーバーの監視と管理を可能にします。
  - HDMは、RAID構成の効率性と管理機能を向上させるために、帯域外RAIDの監視と構成をサポートします。
  - HDMは、リモートサーバーの管理効率を向上させるために、HDM、BIOS、またはRAID構成のインポートとエクスポートをサポートします。
- 障害の監視と診断
  - HDMは、今後のトラブルシューティングのために、システムがクラッシュしたときにスクリーンショットを撮るか、ビデオを録画することをサポートしています。
  - HDMでは、syslogメッセージ、tps、および電子メールを使用してtps、および電子メールの使用がサポートされています。
  - HDMは、サーバー全体の監視、警告、およびイベントロギングを提供します。サーバーの動作(CPUコア温度、電圧、ファン速度など)を監視し、メモリー障害、ドライブ障害、電源障害などのイベントが発生した場合にアラームおよびログを生成します。
  - HDMは、コンポーネントの障害診断用にSmart Hardware Diagnosis(SHD)をサポートしており、障害の特定とコンポーネントの交換が容易になります。
- ネットワーキング
  - HDMは、柔軟なネットワーク管理を可能にするVLANおよびサイドバンドテクノロジーをサポートします。
  - NTPは、サーバーの時間精度を向上させるために時間同期に使用できます。
  - HDMはドメインサーバーとディレクトリサーバーをサポートしているため、ユーザー管理が簡素化され、ユーザー管理のセキュリティが向上します。
- セキュリティ管理
  - HDMは、プライマリ/バックアップイメージのスイッチオーバーをサポートします。スイッチオーバーにより、システムがクラッシュした場合にバックアップイメージを使用して起動できるようになり、システムのアベイラビリティが向上します。
  - HDMは、ユーザーログインのセキュリティを確保するために、さまざまなユーザーインターフェースを提供します。
  - HDMは、証明書のアップロードと置換をサポートして、データ伝送のセキュリティを強化します。
  - Platform Firmware Resiliency(PFR)は、HDMを攻撃から保護するために使用されます。
- スマートな電源管理
  - HDMは、各サーバーの消費電力を正確に制御するための消費電力上限を提供し、エネルギー供給の調整に役立ちます。
  - HDMは、省電力を実現するために、プロセッサーの電源状態および電源装置の動作モードの設定をサポートします。
- 統合された制御

  HDMは、効率を向上させるためにサーバーの一括管理をサポートします。
- 液晶ディスプレイ
  - 一部のH3Cラックサーバーでは、ローカルメンテナンスを容易にするために、タッチ可能な3.5インチLCD

ディスプレイがオプションとして用意されています。

- LCDディスプレイは、HDMからサーバー情報を取得して、サーバーのヘルス状態を迅速に取得します。

さまざまな管理インターフェース

HDMは、Web、Redfish、IPMI、およびSNMPインターフェースを介した管理をサポートします。

HDM Webインターフェース

HDM Webインターフェースは、便利な構成クエリーンターフェースを提供します。ダッシュボード、システム、構成、リモートサービス、リモートO&M、ユーザーおよびセキュリティ、統合制御などの機能の実装に基づいて、複数のモジュールがHDM Webインターフェースに統合されます。

HDMは中国語と英語の両方をサポートしています。 または ボタンをクリックして、言語をそれぞれ中国語と英語に変更します。

オンラインヘルプを開くには、 ボタンをクリックします。

Redfish管理インターフェース

HDMは、標準のRedfish管理インターフェースをサポートします。Redfishクライアントは、PostmanなどのRedfishインターフェースツールとして、HTTPS要求をサーバーに送信し、GET、PATCH、POST、またはDELETEコマンドを使用して情報の照会、設定、および監視を実行します。

Redfishの詳細については、H3C HDM Redfish API Referenceを参照してください。

IPMI管理インターフェース

HDMはIPMI 1.5およびIPMI 2.0をサポートします。IPMIは、異なるタイプのハードウェア上でサーバー管理を提供するサーバー管理システム標準です。複数のプラットフォームに統合された管理を可能にします。

Baseboard Management Controller(BMC)は、システム管理ソフトウェアがサーバー管理のために情報を交換できるようにするIPMIのコアコントローラーです。

IPMIには、次のアウトオブバンド管理およびモニタリング機能があります。

- 資産管理。
- 障害監視。
- ロギング。
- リカバリ管理。

サポートされているIPMIコマンドについては、H3C HDM IPMI Basics Command Referenceを参照してください。

SNMP管理インターフェース

Simple Network Management Protocol(SNMP)は、標準管理フレームワーク、共通通信言語、ネットワーク内のデバイスの監視および管理のためのセキュリティおよびアクセス制御メカニズムを定義します。ネットワークデバイスのリモート管理および運用に広く使用されています。

HDMはSNMPベースのプログラミングインターフェースを提供します。SNMPはGETおよびSET操作とトラップ送信をサポートします。サードパーティ製の管理ソフトウェアは、SNMPインターフェースを使用してサーバーを集中管理できます。SNMPエージェントは、SNMPv1、SNMPv2c、およびSNMPv3をサポートします。

SNMPエージェントは、次の情報の表示をサポートします。システムヘルスステータス、ハードウェアステータス、メモリーおよびプロセッサーモデル、アラームレポート設定、電力統計情報、資産情報、放熱管理、ファームウェアバージョン、およびネットワーク管理。

対象製品

このドキュメントは、次の製品に適用されます。

- AE100。
- 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 R4100 G3
- H3C UniServer R4300 G3
- H3C UniServer R4400 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 B5700 G5
- H3C UniServer R4700 G5
- H3C UniServer R4900 G5
- H3C UniServer R4950 G5
- H3C UniServer R5300 G5
- H3C UniServer R5500 G5
- H3C UniServer R6900 G5

このドキュメントの使用

このドキュメントで使用されているハードウェアオプションの図は説明のためのものであり、お使いの製品とは異なる場合があります。

このドキュメントのスクリーンショットは、今後変更される可能性があります。

このドキュメントの一部のデータは例として使用されており、製品とは異なる場合があります。

開始する前に

HDM使用のガイドライン

- ベストプラクティスとして、専用のネットワークポートを使用してHDMを管理および設定します。
- HDMをインターネットに接続しないでください。
- 安全でないプロトコルやポートは使用しないでください。
- 操作ログを定期的に監査します。

デフォルトのパラメーター設定

表1に、デフォルトのパラメーター設定を示します。HDMへの最初のアクセス時にデフォルトのパラメーター値を変更し、定期的にデフォルトのパラメーター値を更新することをお薦めします。

表1デフォルトのパラメーター設定

パラメーター	デフォルト値
ユーザー名	admin
パスワード	Password@_
専用ネットワークポートのIPv4アドレス	192.168.1.2/24
SNMP読み取り専用コミュニティ名	rocommstr
SNMP読み取り/書き込みコミュニティ名	該当なし
トラップコミュニティ名	public

HDMユーザー

HDMは、次のタイプのユーザーをサポートします。

- ローカルユーザー: HDMは最大16のローカルユーザーをサポートします。ローカルアクセスモードは、研究所や中小企業などの小規模なシナリオに適しています。
- ドメインユーザー(LDAPユーザーおよびADユーザー): ドメインサーバーで構成および管理されているユーザーおよびユーザー権限の数。このアクセスモードは、多数のユーザーが存在する環境に適しています。

よくある質問

故障診断と部位

HDMは、システムクラッシュ時にBSoD(停止のブルースクリーン)のスクリーンショットとビデオ録画を行います。システムに障害が発生して再起動した場合は、BSoDのスクリーンショットまたはビデオを表示してトラブルシューティングを行うことができます。

HDM Webインターフェースアクセスの失敗

表2に、HDM Webインターフェースアクセス障害の考えられる原因と解決方法を示します。

表2 HDM Webインターフェースアクセス障害の原因と解決方法

HDM Webインターフェースアクセス失敗の理由		**解決方法**
ネットワーク接続の問題	HDMネットワークポートは切断されました。	HDMネットワークポート用のネットワークケーブルを正しく接続します。
	不正なHDM管理IPアドレスが使用されている。	アクセスには、HDM管理インターフェースのIPアドレスを使用します。
	ローカルPCおよびHDMネットワークポートが同じネットワークセグメントになっていない	ローカルPCおよびHDMネットワークポートが同じネットワークセグメントになっていることを確認します。
ブラウザーキャッシュがクリアされていません	HDMのファームウェアは最近アップグレードされましたが、ブラウザーキャッシュがクリアされていません。	ブラウザーのキャッシュをクリアしてから、HDMに再度ログインします。
不正なアクセス情報	ユーザー名が存在しません。	最初のログイン時に、デフォルトのユーザー名とパスワードを使用します。
	パスワードが正しくありません。	正しいパスワードを使用してください。パスワードでは大文字と小文字が区別されます。
ユーザー名またはパスワードを忘れた	新しいユーザー名またはパスワードがデフォルトのユーザー名またはパスワードを置き換えるように設定されています。 新しいユーザー名またはパスワードは忘れてしまいました。	システムメンテナンススイッチを使用します。システムメンテナンススイッチの詳細については、サーバーのユーザーガイドを参照してください。

HDMにサインインする

次に、HDMへのサインインが成功するための前提条件、デフォルトのサインインパラメーター、サインイン手順、およびすべてのページのグローバル操作について説明します。

ラックマウント型サーバーのHDMにサインインする

HDMサインインの準備

HDM Webインターフェースにサインインする前に、準備要件がすべて満たされていることを確認します。

HDMクライアントをセットアップする

HDMにはクライアントソフトウェアをインストールする必要はありません。Webブラウザーを使用してHDMにアクセスできます。

構成ターミナルのブラウザーと解像度の設定が、表3の要件を満たしていることを確認します。

表3ブラウザーと解像度の要件

ブラウザー	解像度
Google Chrome 48.0(以上) Internet Explorer 11(以上) Mozilla Firefox 50.0(以降)	最小:1366*768 推奨:1600*900(またはそれ以上)

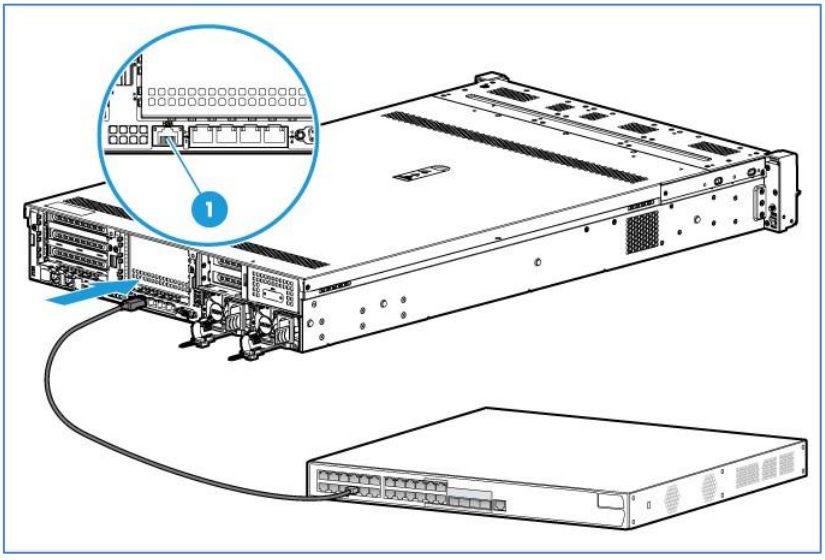
サーバーをネットワークに接続する

サーバー上の次のいずれかのネットワークポートをネットワークに接続します。

- HDM共有ネットワークポート: HDM管理トラフィックとサーバーデータトラフィックを同時に送信します。このポートはすべてのサーバーで使用できます。
- HDM専用ネットワークポート: HDM管理トラフィックだけを送信します。このポートはブレードサーバーおよびAEモジュールでは使用できません。

ラックサーバーまたはストレージサーバーのネットワークポート設定については、「ネットワーク」を参照してください。ブレードサーバーおよびAEモジュールのネットワークポート設定については、「共有ネットワークポートの設定」を参照してください。

図1 サーバーのネットワークへの接続(R4900のHDM専用ネットワークポート)



HDMサインイン設定を取得する

HDMにサインインするには、管理IPアドレスとユーザーカウント情報を取得する必要があります。

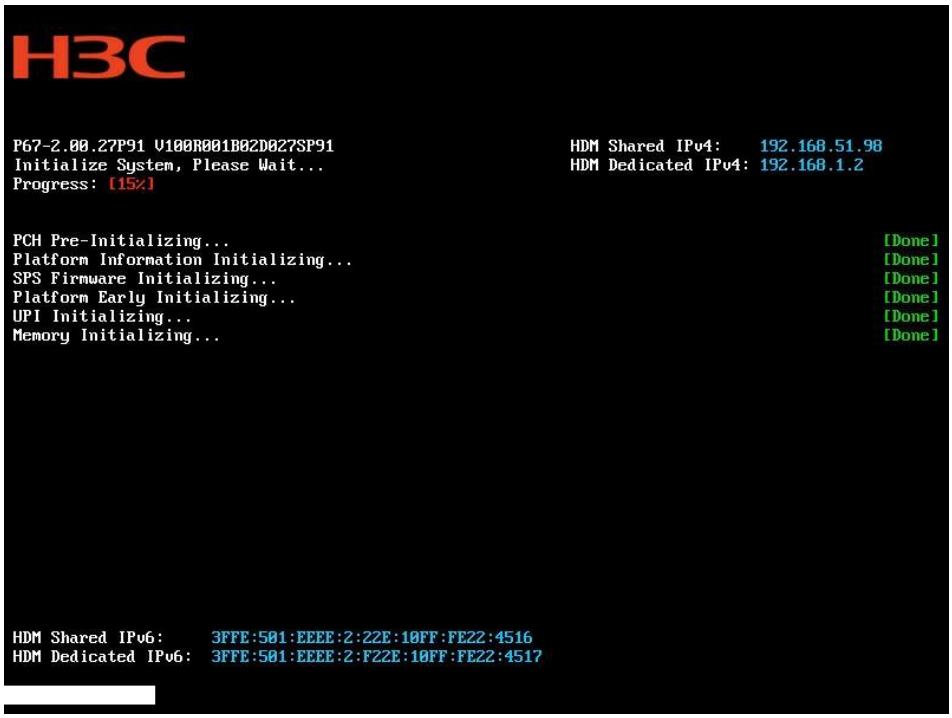
最初のサインインでは、表4のデフォルト設定を使用します。ログイン後に管理IPアドレスを変更するには、「ネットワーク」を参照してください。

表4デフォルトのHDMサインイン設定

項目	デフォルト設定
IPアドレス	HDM共有ネットワークポート: DHCP HDM専用ネットワークポート: 192.168.1.2/24
ユーザー名	admin
パスワード(大文字と小文字を区別)	Password@_

HDM管理IPアドレスは、BIOSのPOST画面から取得できます。図2に示すように、POST画面では共有および専用ネットワークポートのIPv4アドレスが右上に、IPv6アドレスが左下に表示されます。

図2 HDM管理IPアドレスの取得(BIOSバージョン2.00.27)



HDMにサインインする

制限事項とガイドライン

デフォルトでは、セッションタイムアウトは30分です。30分以内に操作が実行されない場合は、ログアウトされます。

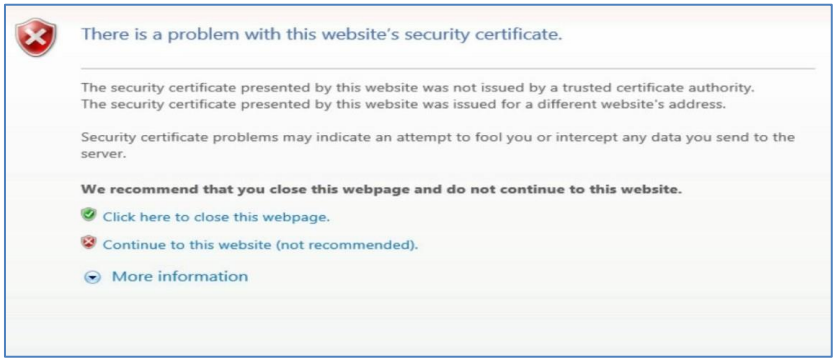
パスワードチェックが5回連続して失敗すると、アカウントは5分間ロックされます。

セキュリティ上の理由から、最初のログイン時にデフォルトのユーザー名とパスワードを変更し、パスワードを定期的に更新します。

手順

1. ブラウザーを開き、HDM管理IPアドレスを入力します。このセクションでは、例としてMicrosoft Internet Explorer 11.0を使用します。
2. 開いたセキュリティ証明書ページで、このWebサイトに進む(推奨しません)をクリックします。

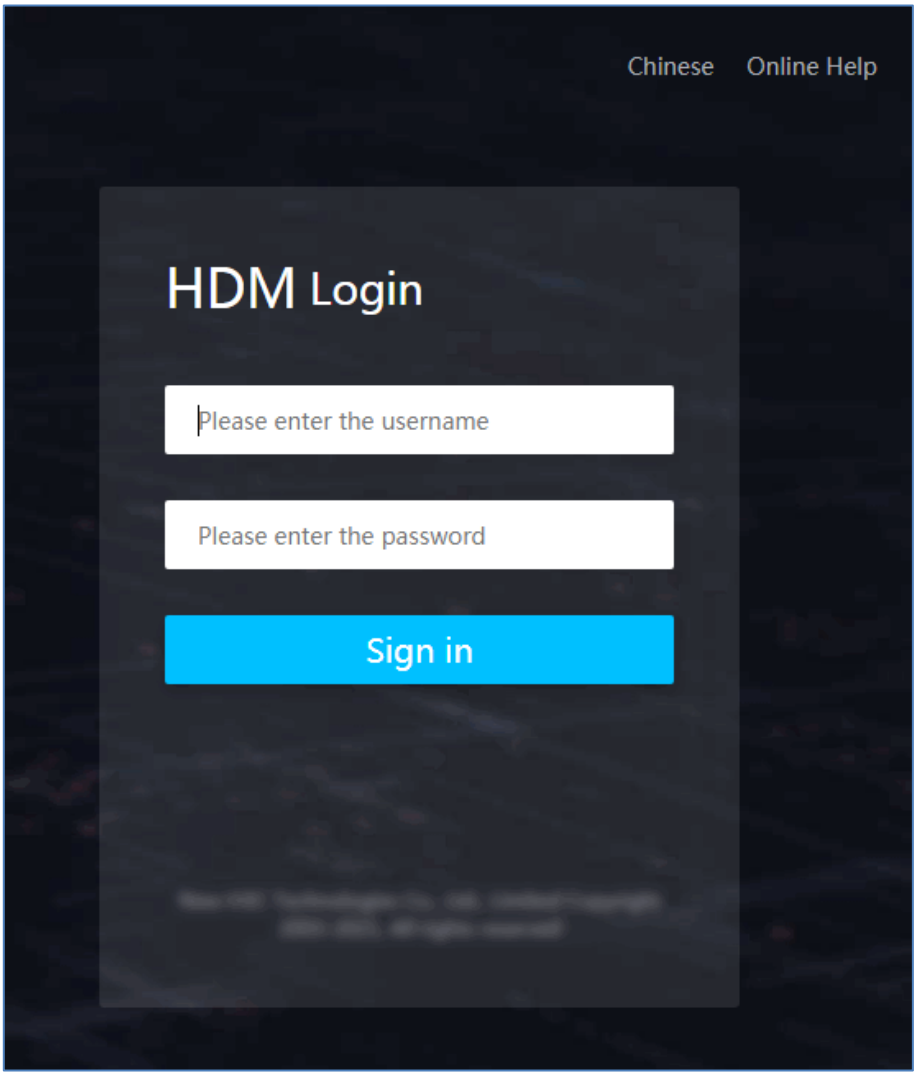
図3 セキュリティ証明書の確認ページ



3. サインインページで、ユーザー名とパスワードを入力し、Sign inをクリックします。

   これが最初のサインインである場合は、デフォルトのユーザー名(admin)とパスワード(Password@_)を入力します。パスワードは大文字と小文字が区別されます。

図4 HDMサインインページ



4. 必要に応じて、中国語または英語をクリックして言語を変更します。

5. これが最初のサインインである場合は、「ユーザーカウント」の説明に従って、セキュリティのためにユーザー名とパスワードを変更します。

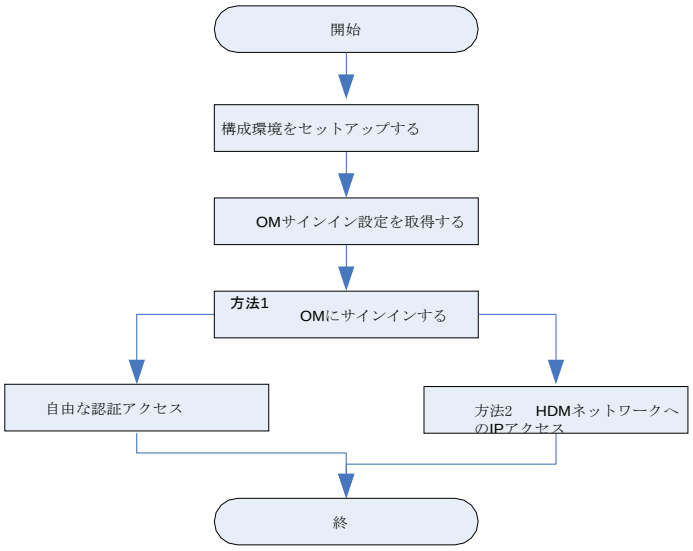
ブレードサーバーおよびAEモジュールのHDMにサインインします。

ブレードサーバーおよびAEモジュールの場合、HDMにアクセスできるのはOMだけです。HDMにアクセスするには、認証を受けずにRemote Consolesページからアクセスするか、ブレードサーバーの情報ページでHDMネットワークIPアドレスをクリックします。

HDMアクセス権限を持つOM管理者ユーザーおよびオペレータユーザーのみが、OMからHDMにアクセスできます。

HDMサインイン手順は、ブレードサーバーとAEモジュールで同じです。ここでは、ブレードサーバーの手順を例として使用します。

HDMサインインのフローチャート

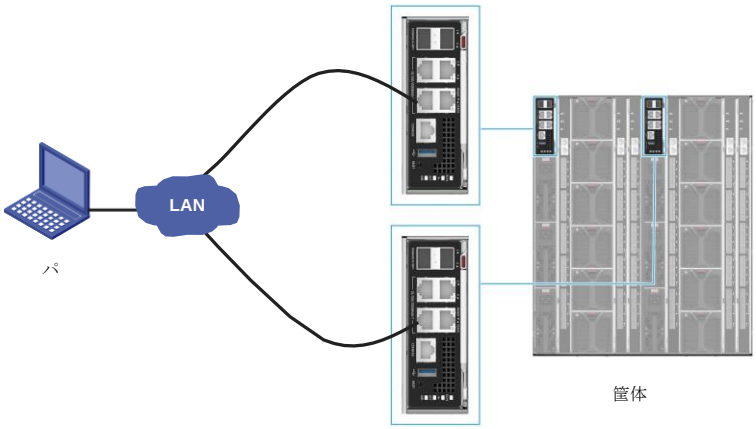


HDMサインインの準備

構成環境のセットアップ

図5に示すように、ローカルPCをHDMクライアントとして使用し、PCをアクティブおよびスタンバイOMモジュールの管理(MGMT)ポートに接続します。ポートの位置の詳細については、OMモジュールの前面パネルにあるラベルを参照してください。

図5 構成環境のセットアップ



OMサインイン設定を取得する

OM Webインターフェースにサインインするには、その管理IPアドレスとユーザーカウント情報を取得する必要があります。最初のサインインで、表5のデフォルト設定を使用します。

表5 OMサインインのデフォルト設定

項目	デフォルト設定
IPアドレス	192.168.100.100/24
ユーザー名	admin
パスワード(大文字と小文字を区別)	Password@_

HDMクライアントをセットアップする

HDMはクライアントソフトウェアのインストールを必要としません。Webブラウザーを使用してHDMにアクセスできます。ログインを成功させるには、次の制約事項に従ってください。

- HDMクライアントのIPアドレスが、OMモジュールおよびHDMの管理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。HDM管理IPアドレスは、OM Webインターフェースから取得できます。詳細は、OMオンラインヘルプを参照してください。
- 構成ターミナルのブラウザーと解像度の設定が表6の要件を満たしていることを確認します。

  表6ブラウザーと解像度の要件

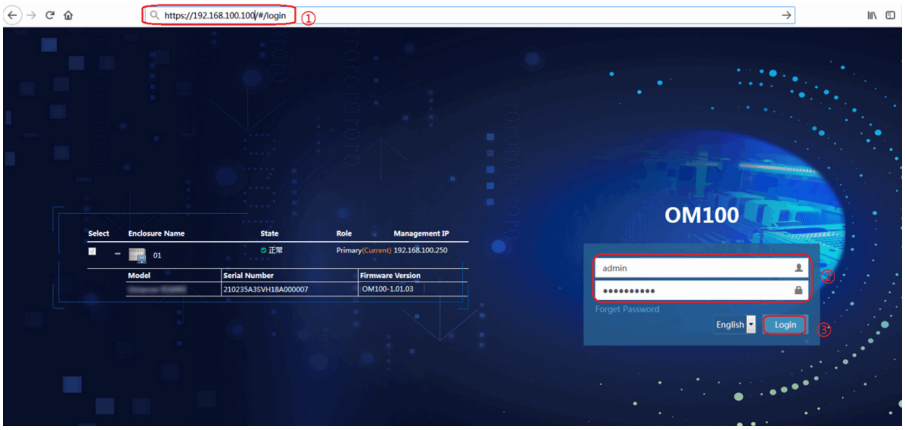
ブラウザー	解像度
Google Chrome 58.0(またはそれ以上)	推奨:1600*900(またはそれ以上)

OMにサインインする

1. ブラウザーを開き、次の形式でOM管理IPアドレスを入力します。
   https://OM_ip_address
2. サインインページで、ユーザー名とパスワードを入力し、Loginをクリックします。

   これが最初のサインインである場合は、デフォルトのユーザー名(admin)とパスワード(Password@_)を入力します。パスワードは大文字と小文字が区別されます。

図6 OMへのサインイン



HDMにサインインする

認証不要のアクセス

1. OM Webインターフェースのナビゲーションペインで、**Blade Servers**をクリックし、ターゲットサーバーを選択して、**Remote Consoles**をクリックします。
2. 図7に示すように、**Remote Consoles**タブで、**Access HDM**ボタンをクリックしてHDMにサインインします。

   これが最初のサインインである場合は、図8に示す**Proceed to**リンクをクリックして、開いたWebページを信頼します。

図7 認証不要のアクセス

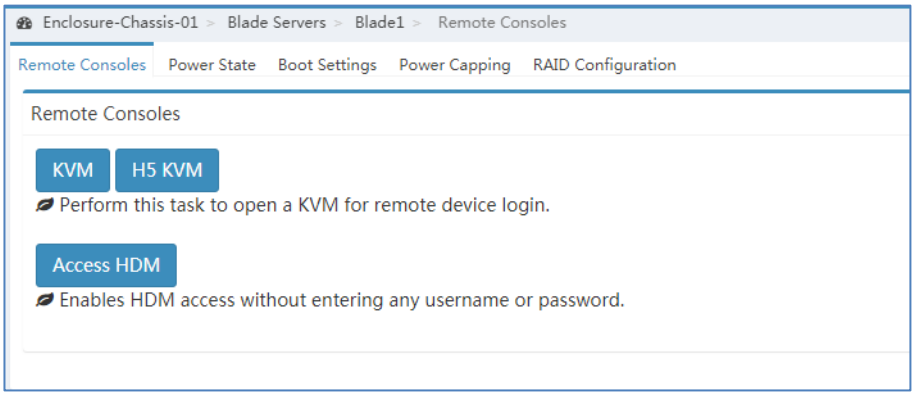
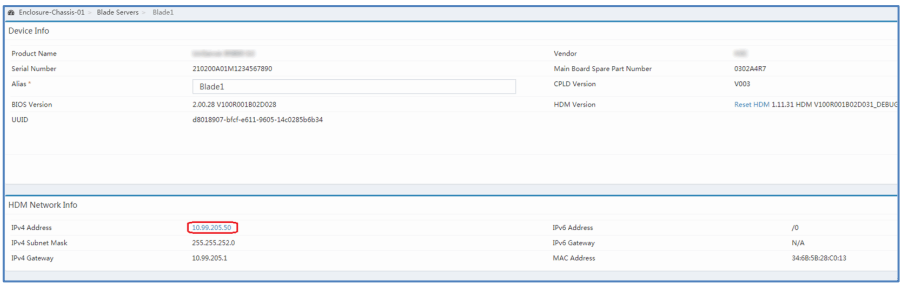
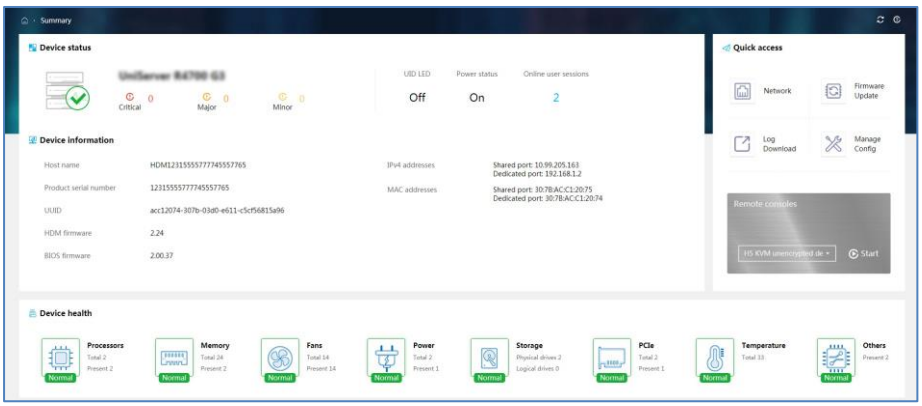


図8 接続の確認



HDM Webインターフェースが開きます。

図9 HDMのWebインターフェース

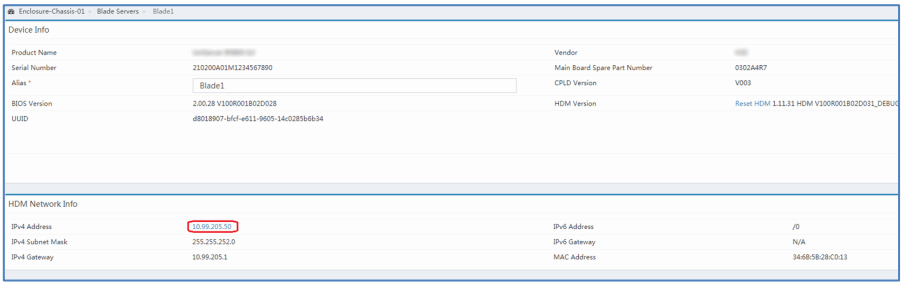


HDMネットワークのIPアクセス

1. OM Webインターフェースのナビゲーションペインで、**Blade Servers**をクリックし、ターゲットサーバーを選択します。
2. 図10に示すように、**HDM Network Info**セクションで、**IPv4 Address**フィールドのIPアドレスリンクをクリックします。

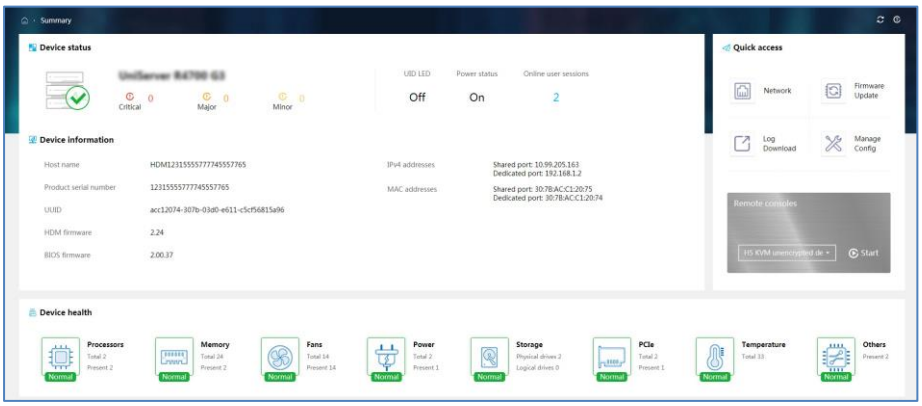
   これが最初のサインインである場合は、図8に示す**Proceed to**リンクをクリックして、開いたWebページを信頼します。

図10 HDMネットワークのIPアクセス



HDM Webインターフェースが開きます。

図11 HDMのWebインターフェース



グローバル設定

任意のHDMページで次の操作を実行できます。

- 言語を変更するには、英語 および中国語 をクリックします。
- HDMオンラインヘルプにアクセスするには、 をクリックします。
- ログアウトするには、 をクリックします。
- ページを更新するには、 をクリックします。

デバイス情報を表示する

デバイスに関するサマリー情報の表示

Dashboardには、デバイスに関する基本情報、システムアラームステータス、デバイスヘルス情報、目的の機能または機能メニューにすばやくアクセスするためのショートカットなど、デバイスに関する要約情報が表示されます。

注:

G3およびG5サーバーの**Dashboard**ページは、若干異なります。

手順

上部ナビゲーションバーの**Dashboard**を選択します。デバイスに関するサマリー情報が表示されます。

図12は、G3サーバーの要約情報を示しています。図13は、G5サーバーの要約情報を示しています。

図12 サマリー情報(G3サーバー)

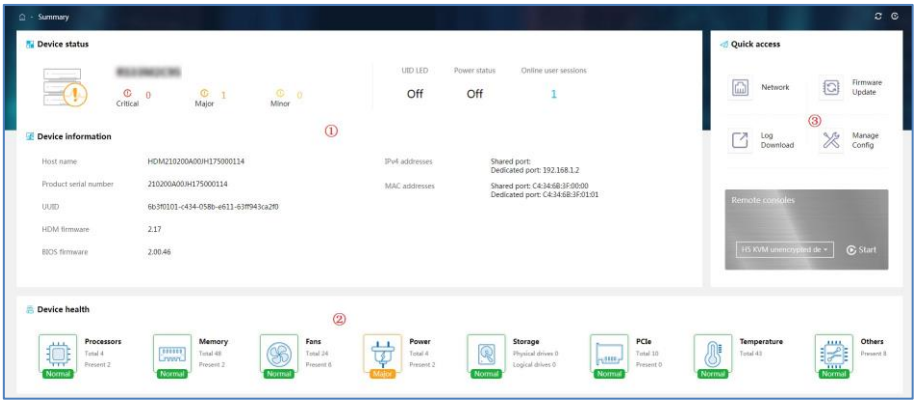
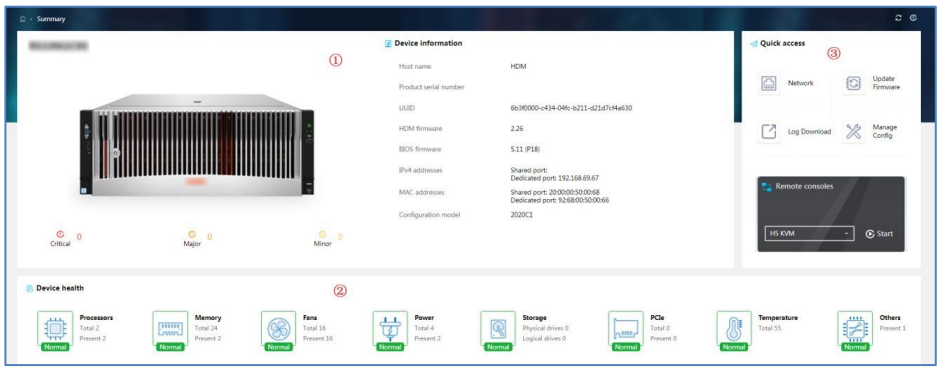


図13 サマリー情報(G5サーバー)



パラメーター

作業ウィンドウには、次のセクションがあります。

- セクション1-サーバーのステータスとサーバーに関する基本情報を表示します。
  - ヘルスステータス:サーバーのヘルスステータスを表示します。
    - **Normal** -すべてのサーバーコンポーネントが正常に動作しています。
    - **Critical**, **Major**:少なくとも1つのコンポーネントに問題が発生しています。
  - UID LED:サーバー上のUID LEDのステータスを表示します。
    - **点灯** - サーバーのUID LEDは青に点灯しています。
    - **点滅** - サーバーのUID LEDが青色で点滅しています。これは、サーバーがファームウェアをアップグレードしているか、サーバーのリモートコンソールが起動されていることを示します。
    - **消灯** - サーバーのUID LEDが消灯しています。
  - 電源ステータス:サーバーの電源ステータスを表示します。
    - **点灯** - サーバーの電源が入っています。
    - **消灯** - サーバーの電源がオフになっています。
  - 各重大度レベルのアラーム数
    - **Minor** - イベントはシステムにわずかな影響しか与えませんが、重大度のエスカレーションを回避するためには迅速なアクションが必要です。
    - **Major** - このイベントは一部のサブシステムに重大な影響を与え、サービスが中断される可能性があります。即時のアクションが必要です。
    - **Critical** - イベントによってシステムがクラッシュまたはシャットダウンする可能性があります。すぐに対処する必要があります。
  - サーバーに関する次のような基本的な情報
    - サーバーのホスト名。
    - サーバーの製品シリアル番号。
    - サーバーの汎用一意識別子(UUID)。
    - 現在のHDMファームウェアバージョン
    - 現在のBIOSファームウェアバージョン。
    - サーバー名。このフィールドをサポートするのはブレードサーバーとAEモジュールだけです。デフォルトでは、値は表示されません。
    - HDMネットワークポートのIPv4アドレス。ネットワークポートモードがnormalまたはアクティブ/スタンバイの場合、このフィールドには、HDM専用および共有ネットワークポートのIPv4アドレスが表示されます。ネットワークポートモードがbondingの場合、このフィールドにはbondポートBond0のIPv4アドレスが表示されます。
    - HDMネットワークポートのMACアドレス。
- セクション2 -デバイスコンポーネントのヘルスステータスを表示します。
  - 正常:コンポーネントは正常に動作しています。
  - メジャー:コンポーネントのパフォーマンスが大幅に低下します。
  - 重大:コンポーネントの損傷を防ぐために、サーバーがシャットダウンされる場合があります。

表7コンポーネントのヘルスステータス

構成要素	ヘルスステータス	説明
プロセッサー	正常	CPUは正常に動作している。
	メジャー	次のいずれかの条件が存在します。 • 過熱状態が発生しました。

構成要素	ヘルスステータス	説明
		• プロセッサー構成が正しくありません。
	クリティカル	次のいずれかの条件が存在します。 • プロセッサーの温度がクリティカルのしきい値を超えました。 • 回復不能なプロセッサーエラーが発生しました。 • プライマリプロセッサーがない。 • プロセッサーエラーが原因で、POST中にBIOSが停止しました。
メモリー	正常	メモリーは正常に動作している。
	メジャー	次のいずれかの条件が存在します。 • すべてのメモリーモジュールがないか、絶縁されている。 • 回復不能なメモリーエラーが発生しました。 • DIMMが正しく取り付けられていないか、DIMM互換性エラーが発生しました。
	クリティカル	メモリーエラーが原因で、POST中にBIOSが停止しました。
ファン	正常	ファンは冗長構成で正常に動作しています。重要な位置にあるファンに障害は発生していません。
	メジャー	2つ以上の重要な場所にあるファンに障害が発生したため、ファンの冗長性の問題が発生しています。
電源装置	正常	PSUは正常に動作している。
	メジャー	重大なPSUエラーが発生しました。
ストレージ	正常	すべての論理ドライブ、物理ドライブ、およびストレージコントローラーが正常に動作しています。
	メジャー	次のいずれかの条件が存在します。 • 論理ドライブエラーが発生しました。 • 重大な物理ドライブエラーが発生しました。 • ストレージコントローラーエラーが発生しました。
PCIeモジュール	正常	PCIeモジュール(ネットワークアダプター、GPU、FC HBA、およびQATカード)は正常に動作している。
	メジャー	バス修正不能エラー、バス致命的エラー、またはPCIeモジュール(ネットワークアダプター、GPU、FC HBA、またはQATカード)エラーが発生しました。
温度	正常	構成部品の温度はすべて標準範囲内です。 処置は必要ありません。
	メジャー	コンポーネントの温度がメジャーしきい値を超えましたが、クリティカルしきい値には達していません。早急な対応が必要です。
	クリティカル	コンポーネントの温度がクリティカルのしきい値を超えました。早急な対応が必要です。
その他	正常	すべてのコンポーネントが正常に動作している。
	メジャー	少なくとも1つのコンポーネントで重大なエラーが発生しました。
	クリティカル	少なくとも1つのコンポーネントで重大なエラーが発生しました。

- セクション3 - 目的の機能または機能メニューにすばやくアクセスするためのショートカットを提供します。
  リモートコンソールにアクセスするには、まずリモートコンソールタイプ(KVMまたはH5 KVM)を選択する必要があります。KVMおよびH5 KVMの起動モードについては、「KVMまたはH5 KVMリモートコンソールの起動」を参照してください。

ボタン

HDM Webインターフェースでは、右上にボタンがあります。表8に、ボタンに関する情報を示します。

表8ボタン

ボタン名	アイコン	説明
UID LED		サーバーのUID LEDは青に点灯。
		サーバーのUID LEDが青色で点滅している場合は、サーバーがファームウェアをアップグレードしているか、サーバーのリモートコンソールが起動していることを示しています。
		サーバーのUID LEDが消灯している。
サーバーの電源		サーバーの電源が入っています。このボタンをクリックすると、次の電源オプションが表示され、サーバーの電源状態を変更できます。 • **Force system reset** - ウォームリブートは、サーバーの電源を再投入せずに、サーバーをリブートします。 • **Force power-off** - 強制的にサーバーを即時にシャットダウンします。この操作は、サーバーの電源ボタンを5秒間押すのと同じです。 • **Graceful power-off** - 最初にオペレーティングシステムをシャットダウンしてから、サーバーの電源を切ります。 • **Power on** - サーバーを起動します。 • **Force power-cycle** - 電源をオフにしてから、サーバーの電源を入れます。
		サーバーの電源がオフになります。
言語		言語を中国語に変更します。
		言語を英語に変更します。
アラーム		アラームに関する詳細情報を表示します。
ユーザー		現在のユーザーの名前とログイン時間、およびオンラインユーザーの数が表示されます。 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、Detailsをクリックします。ログアウトするには、ログアウトLogoutをクリックします。
再表示		Webページを更新します。
オンラインヘルプ		オンラインヘルプを起動します。

システム

要約情報の表示

Summaryメニューでは、サーバー、ファームウェア、プロセッサー、メモリー、PCIeモジュール、センサー、およびその他のコンポーネントに関する情報を表示できます。

サポートされる設定は、サーバーモデルによって異なります。

注:

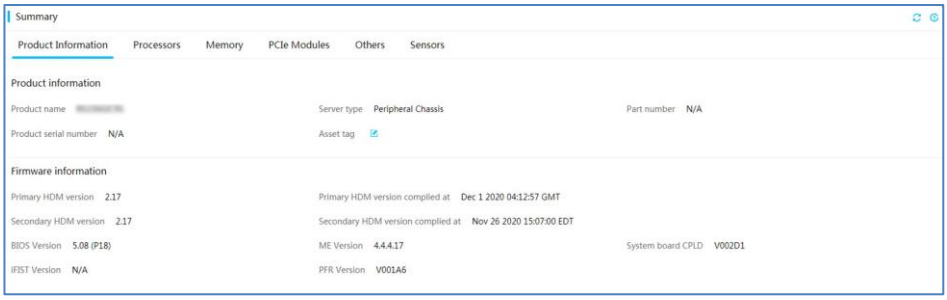
- HDMは、サーバーがPOSTを完了した後にのみ、正しい完全なプロセッサー、メモリー、およびPCIeモジュールの情報を表示できます。
- サーバーがオフの場合、HDMは最新のPOSTで取得されたプロセッサー、メモリー、およびPCIeモジュールの情報を表示します。

デバイス情報を表示する

手順

1. 上部のナビゲーションバーで、**System**をクリックします。**Summary**ページが表示されます。
2. **Product Information**タブをクリックして、デバイスおよびファームウェア情報を表示します。

図14 デバイス情報の表示



パラメーター

- **Product name**: サーバーモデル。
- **Server type**: サーバータイプ。
- **Part number**: サーバーの部品番号。サーバーモデルに対応します。システムがサーバー部品番号を取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Product serial number**: サーバーのシリアル番号。
- **Asset tag**: サーバーの資産タグ。このフィールドはオプションです。資産タグは1から48文字の文字列で、文字、数字、スペースおよび次の特殊文字のみを含めることができます:`
  ~!@#$%^&*()_+-={};':\",./<>?
- **Primary HDM version**:プライマリHDMイメージのファームウェアバージョン。
- **Primary HDM compiled at**:プライマリHDMイメージの最新の更新時刻。
- **Secondary HDM version**:バックアップHDMイメージのファームウェアバージョン
- **Secondary HDM complied at**:バックアップHDMイメージの最新の更新時刻。
- **BIOS Version**:Basic Input Output System(BIOS)のバージョン。
- **ME Version**:Intel Management Engine(ME)のバージョン。このフィールドは、インテルプロセッサーがインストールされているサーバーでのみ使用可能です。
- **System board CPLD version**:システムボードのComplex Programmable Logical Device(CPLD)のバージョン。

- **iFIST Version**:統合されたFast Intelligent Scalable Toolkit(iFIST)の現在のバージョン。HDMがiFISTバージョンを取得できなかった場合、システムはN/Aと表示します。
- **PFR Version**:PFRCPLDファームウェアのバージョン。このフィールドは、G5サーバーでのみ使用できます。

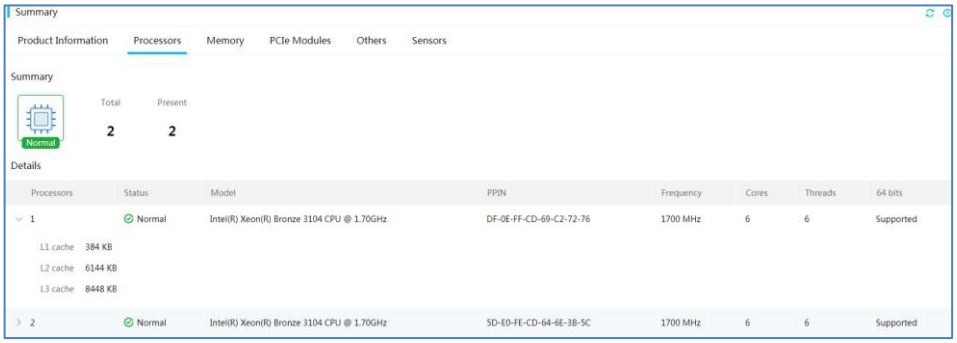
プロセッサー情報の表示

サマリーおよび詳細なプロセッサー情報とプロセッサーエラーを表示するには、次の作業を実行します。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。**Summary**ページが表示されます。
2. **Processor**タブをクリックして、プロセッサー情報を表示します。

図15 プロセッサー情報の表示



パラメーター

- **Status**:プロセッサーの動作ステータス。プロセッサーが異常状態にある場合は、障害の説明を表示してエラーを特定します。
- **Model**:プロセッサーのモデル。
- **PPIN**:製造業者によって割り当てられた一意の製品コード。HDMがPPINを取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Frequency**:プロセッサーの基本周波数。
- **Cores**:s:プロセッサーのコア。
- **Threads**:プロセッサーがサポートするスレッドの数。
- **64 bits**:プロセッサーが64ビットコンピューティングをサポートしているかどうかを示します。
- **L1 cache**:プロセッサーのL1キャッシュ。
- **L2 cache**:プロセッサーのL2キャッシュ。
- **L3 cache**:プロセッサーのL3キャッシュ。
- **Fault description**:プロセッサーエラーに対して生成されたアラーム。

メモリー情報の表示

サマリーおよび詳細なメモリー情報とメモリーエラーを表示するには、次の作業を実行します。

制限事項とガイドライン

メモリーモジュールの**Status**フィールドに存在しないと表示されている場合、残りのフィールドにはすべてティルダ(~)が表示されます。

メモリートレーニングエラーのためにDIMMが無効になっている場合は、同じチャネル内の他のDIMMも無効になります。

メモリーモジュールスロットには、装着されているメモリーモジュールの状態を示す色が付いています。色のオプションは次のとおりです。

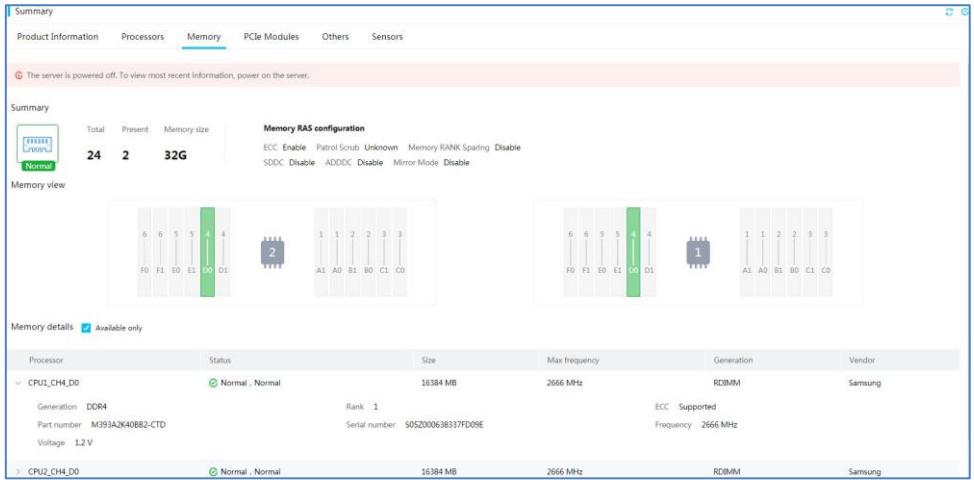
- **緑** - メモリーモジュールがあり、正常に動作しています。
- **グレー** - メモリーモジュールがありません。

- **グレーとストライプ** - メモリーモジュールが無効になっている。
- 黄色 - 軽微なメモリーエラーが発生しています。
- **オレンジ** - 重大なメモリーエラーが発生しています。
- 赤 - 重大なメモリーエラーが発生しています。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。**Summary**ページが表示されます。
2. メモリー情報を表示するには、**Memory**タブをクリックします。
3. (オプション)ターゲット計算モジュールを選択して、対応するメモリー情報を表示します。

図16 メモリー情報の表示



パラメーター

メモリーのRAS設定

- **ECC**: Error-Correcting Code(ECC)のサポート。
- **Patrol Scrub**: Patrolスクラブ設定。Patrolスクラブを使用すると、プロセッサーは修正可能なメモリーエラーを定期的に自動的に検索して修正できます。
- **Memory RANK Sparing**: メモリーRANKスペアリングの有効化ステータス。これは、DIMMに障害が発生した場合のバックアップとして、各チャネルにメモリーの一部を予約します。
- **SDDC**: DRAM Single Device Data Correction(SDDC)のイネーブルステータス。x4またはx8チップ内の複数のビットエラーを訂正できます。
- **ADDDC**: 2ビットメモリーエラーを修正できるAdaptive Double Device Data Correction Sparing(ADDDC)のイネーブルステータス。
- **Mirror Mode**: ミラーモード。次のオプションがあります。
  - **Disable**: メモリーミラーリングをディセーブルにします。
  - **Full Mirror Mode**: システム内の1 LMメモリー全体をミラーリングするように設定します。
  - **Partial Mirror Mode**: システム内の1 LMメモリーの一部をミラー化するように設定します。

メモリーの詳細(すべてのDIMMで利用可能)

- **Location**: DIMMのプロセッサーID、チャネルID、およびスロット番号。
- **Status**: メモリーモジュールのヘルスステータスと完全性ステータス。DIMMが異常状態の場合は、障害の説明を表示してエラーを特定します。完全性ステータスは、メモリーがベンダー認定されているかどうかを示します。使用可能なオプションは次のとおりです。
  - **Vendor certified**: モジュールは認定されています。
  - **Normal**: モジュールは認定されていません。
- **Size**: DIMMの容量。
- **Max frequency**: メモリーモジュールの主周波数。
- **Generation**: DIMMの世代。

- **Vendor: DIMMの製造元。**
- **Type**: DIMMタイプ。
- **Rank**: DIMMのランクタイプ。オプションには、SR DIMM、DR DIMM、およびQR DIMMがあります。
- **ECC**: Error-Correcting Code(ECC)のサポート。
- **Serial number**: 製造業者によって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Part number**: DIMMの部品番号。HDMが部品番号を取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Frequency**: メモリーが動作する周波数。
- **Voltage**: メモリーの電圧。

メモリーの詳細(帯域外管理をサポートするDCPMMsでのみ使用可能)

- **Operating mode**: DCPMMの動作モード。次のオプションがあります。
  - **Memory mode**: DCPMMsは揮発性システムメモリーとして動作し、取り付けられているすべてのRDIMMおよびLRDIMMはDCPMMs用のキャッシュとして動作しています。
  - **App direct mode:** ドDCPMMsおよびDRAM DIMMは、アプリケーションの直接ロードまたはストア制御下で独立したメモリーリソースとして動作します。RDIMMまたはLRDIMMは揮発性システムメモリーとして動作しています。DCPMM容量は、アプリケーションが直接アクセスできるバイトアドレス指定可能な永続メモリーとして使用されます。
  - **Mixed mode**: DCPMM容量の一部がメモリーモードで使用され、残りがアプリケーション直接モードで使用されます。
- **Controller firmware versionン**: DCPMMコントローラーのファームウェアバージョン。
- **DCPMM temperature**: DCPMMの温度。
- **Controller temperature**: DCPMMコントローラーの温度。
- **Remaining life (%)**: DCPMMの残存寿命(%)。
- **Power-on hours**: DCPMMの合計電源投入時間(時間単位)。
- **Memory**: 揮発性システムメモリーとしてのDCPMMの容量。
- **SSD capacity**: 永続的メモリーとしてのDCPMMの容量。
- **Fault description**: DIMMエラーに対して生成されたアラーム。

PCIeモジュール情報を表示する

制限事項とガイドライン

この機能は、PCIeモジュールが存在し、本発明のPCIeモジュールが情報取得をサポートする場合にのみ利用可能である。

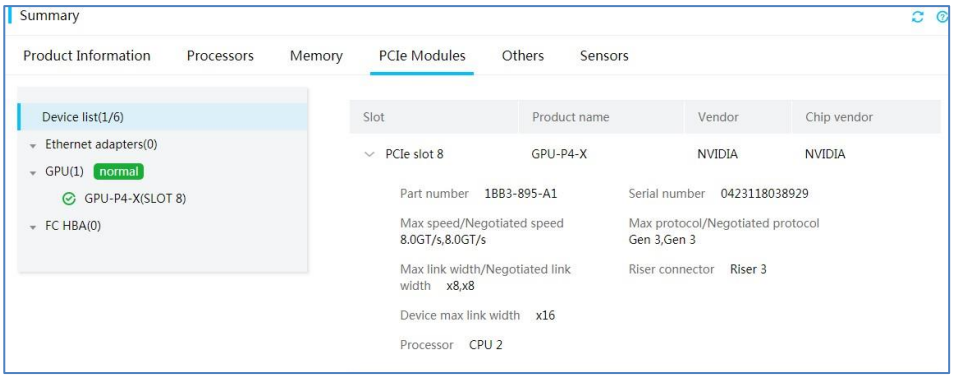
システムが現在の電源を取得できない場合は、GPUドライバがインストールされていることを確認します。

Management Component Transport Protocol(MCTP)機能をイネーブルにするには、最初にシステムファームウェアをMCTPをサポートするバージョンにアップデートします。次に、BIOSセットアップユーティリティにアクセスし、**Advanced > Platform Configuration > Server ME Configuration**メニューにアクセスし、MCTPプロキシをイネーブルにしてから、サーバーを再起動します。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。**Summary**ページが表示されます。
2. **PCIe Modules**タブをクリックして、PCIeモジュール情報を表示します。
3. PCIeモジュールのタイプに関する情報を表示するには、対応するタブをクリックします。

図17 PCIeモジュール情報の表示



パラメーター

デバイスリスト

- **Slot**: PCIeモジュールのスロット。スロットの位置について詳しくは、サーバーのユーザーガイドを参照してください。
- **Status**: PCIeモジュールのステータス(正常および異常を含む)。
- **Product name**: PCIeモジュールのモデル。
- **Module vendor**: PCIeモジュールの製造元。
- **Chip vendor** :PCIeモジュールのチップメーカー。
- **Serial number**: 製造業者によって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Part number**: PCIeモジュールの部品番号。PCIeモジュールのモデルに対応します。HDMが部品番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Max speed**: PCIeリンクの最大速度。
- **Negotiated speed**: 自動ネゴシエートされたPCIeリンクレート。
- **Max protocol**: サポートされている最新世代のPCIe標準。
- **Negotiated protocol**: PCIe標準の自動ネゴシエートされた生成。
- **Max link width**: PCIeスロットでサポートされている最大リンク幅。
- **Device max link width**: PCIeデバイスでサポートされる最大リンク幅。
- **Negotiated link width**: PCIeモジュールの自動ネゴシエートされたリンク幅。
- **Mezzanine slot**:メザニンPCIeモジュールのスロット番号。このフィールドはブレードサーバーに対してのみ表示されます。
- **Processor**:PCIeモジュールが従属するプロセッサー。このフィールドのサポートは、デバイスモデルによって異なります。
- **Riser connector**:PCIeモジュールが取り付けられているライザーカードのコネクター番号。

ネットワークアダプター

- **Product name**:ネットワークアダプターの名前。
- **Port**:ネットワークアダプターのポートタイプ。
- **Module vendor**:ネットワークアダプターの製造元。
- **Chip vendor**:ネットワークアダプターのチップメーカー。
- **Mezzanine slotト**:メザニンPCIeモジュールのスロット番号。このフィールドはブレードサーバーに対してのみ表示されます。
- **Firmware**:ネットワークアダプターのファームウェアバージョン。
- **Status**:ネットワークアダプターのヘルスステータス。ネットワークアダプターが異常な状態にある場合は、イベントログを調べてエラーを特定します。
- **Location**: ネットワークアダプターの物理的な場所。
- **Serial number**:製造業者によって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。

- **Part number**:PCIeモジュールの部品番号。PCIeモジュールのモデルに対応します。HDMが部品番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Network port**ト:ネットワークアダプター上のネットワークポート。
- **MAC address**:ネットワークポートのMACアドレス。
- **Negotiated speed**:ネットワークポートのネゴシエートされた速度。HDMがネゴシエートされた速度を取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Port type**:ネットワークポートタイプ。FiberおよびCopperオプションがあります。
- **Port connection**:ケーブルがネットワークポートに接続されているかどうかを表示します。オプションには、**Connected**と**Disconnected**があります。HDMが接続ステータスを取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Fault description**:PCIeモジュールのエラーに関するイベントログ情報。
- **LLDP**: ネットワークポートのLLDPの有効化ステータス。必要に応じてLLDPを有効または無効にできます。フィールドが設定できない場合、ネットワークポートはLLDPをサポートしません。

GPU

- **Product name**:GPUのモデル。
- **Vendor name**:GPUの製造元。
- **Firmware version**:GPUのファームウェアバージョン。
- **Status**:GPUヘルスステータス。GPUが異常状態の場合は、イベントログを確認してエラーを特定します。
- **Location**: GPUが存在するスロットの番号。スロットの場所については、サーバーのユーザーガイドを参照してください。
- **Part number**:GPUモジュールのモデルに対応するGPUの部品番号。HDMが部品番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Serial number**:ベンダーによって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Power**:GPUの現在の電力。
- **Fault description**:PCIeモジュールのエラーに関するイベントログ情報。

FC HBA

- **Product name**:FC HBAのモデル。
- **Vendor name**:FC HBAの製造元。
- **Firmware version**:FC HBAのファームウェアバージョン。
- **Status**:FC HBAのヘルスステータス。FC HBAが異常状態の場合は、イベントログを確認してエラーを特定します。
- **Location**: FC HBAの場所。
- **WWPN**:ネットワークポートのWorldwide Port Number(WWPN)。
- **WWNN**:ネットワークポートのワールドワイドノード名(WWNN)。
- **Port connection**:ケーブルがネットワークポートに接続されているかどうかを表示します。オプションには、**Connected**と**Disconnected**があります。HDMが接続状態を取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Speed:**ネットワークポートの速度。HDMが速度を取得できなかった場合、このフィールドにはN/Aと表示されます。
- **Fault description**:PCIeモジュールのエラーに関するイベントログ情報。

QATカード

- **Product name**:QATカードの機種。
- **Module vendor**:QATカードの製造元。
- **Chip vendor**:QATカードのチップメーカー。
- **Status**:QATカードのヘルスステータス。QATカードが異常状態の場合は、イベントログを調べてエラーを特定します。
- **Location** :QATカードが存在するスロットの番号。スロットの場所については、サーバーのユーザーガイドを参照してください。
- **Part number**:QATカードの部品番号。QATカードのモデルに対応します。HDMが部品番号の取得に失敗し

た場合、このフィールドにはN/Aと表示されます。

- **Serial number**:ベンダーによって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Fault description**:PCIeモジュールのエラーに関するイベントログ情報。

他のコンポーネントに関する情報を表示する

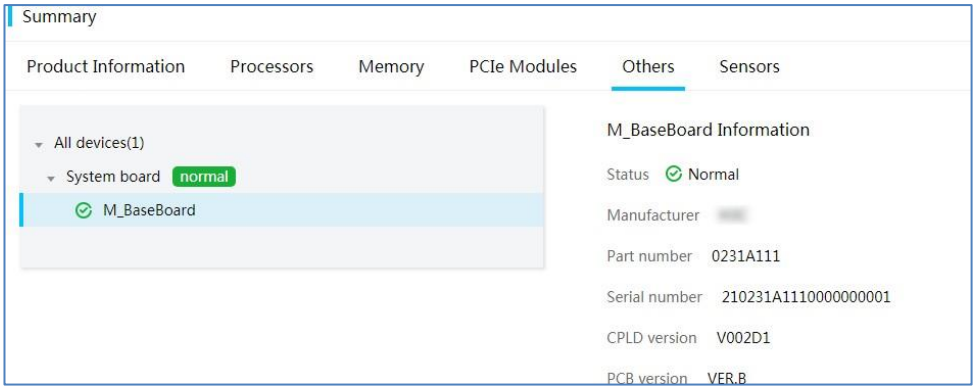
制限事項とガイドライン

HDMは、現在のコンポーネントに関するコンポーネント情報のみを表示します。サポートされるコンポーネントは、サーバーモデルによって異なります。

手順

1. 上部のナビゲーションバーで、Systemをクリックします。**Summary**ページが表示されます。
2. **Others**タブをクリックします。
3. 対応するコンポーネント情報を表示するには、ターゲットコンポーネントタイプを選択します。

図18 その他のコンポーネントに関する情報の表示



パラメーター

- **Status**:コンポーネントのヘルスステータス。コンポーネントが異常な状態にある場合は、イベントログを調べてエラーを見つけます。
- **Manufacturer**::構成部品のメーカー。
- **Part number**:構成部品の部品番号。構成部品モデルに対応します。HDMが部品番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **Serial number**:製造業者によって割り当てられた一意の製品コード。HDMがシリアル番号の取得に失敗した場合、このフィールドにはN/Aと表示されます。
- **CPLD version**:CPLDファームウェアのバージョン。
- **AUXCPLD version**:AUXCPLDファームウェアのバージョン。このフィールドは、一部のブレードサーバーでのみ使用できます。
- **PCB version**:Printed Circuit Board(PCB)ファームウェアのバージョン。
- **Module model**:ドライブバックプレーンのモデル。
- **Current firmware version**:ドライブバックプレーンのファームウェアバージョン。
- **Current configuration file version**:ドライブバックプレーンのコンフィギュレーションファイルのバージョン。
- **Bootloader version**:ドライブバックプレーンのブートローダーバージョン。
- **EEPROM version (for firmware)**: ドライブバックプレーンのElectrically Erasable Programmable Read Only Memory(EEPROM)バージョン。
- **Fault description**:コンポーネントのエラーに関するイベントログ情報。

センサー読み取りチャートを表示する

センサーの読み取り値を折れ線グラフで表示するには、次の作業を実行します。システムは、5分間隔でセンサーの読み取り値を収集します。

制限事項とガイドライン

R4950 G3およびR4950 G5サーバーは、平均センサー読み取り値の表示だけをサポートしています。

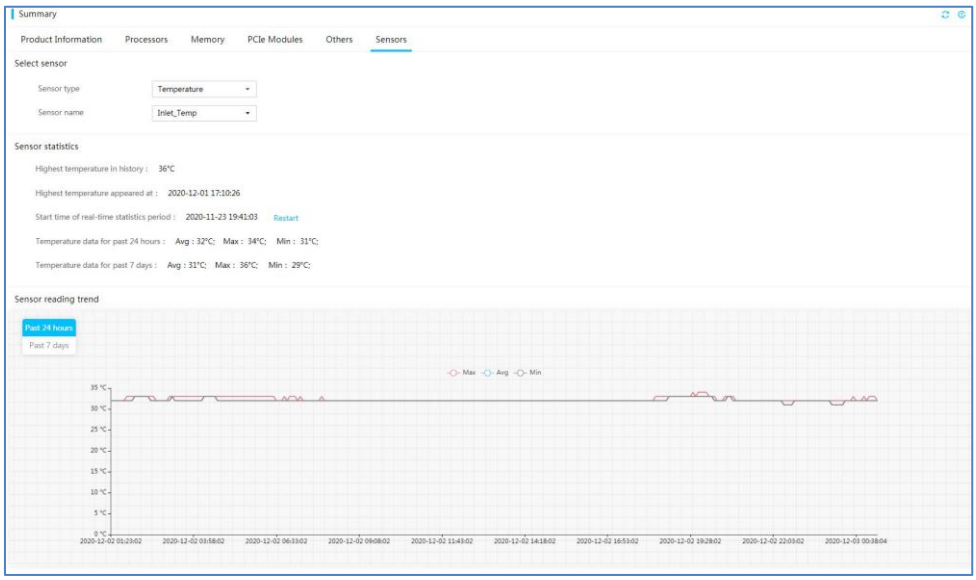
HDMは再起動中にセンサー読み取り値を取得できません。HDM設定を復元すると、センサー読み取り統計情報がクリアされます。この機能をサポートしているのはリニアセンサーだけです。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。**Summary**ページが表示されます。
2. **Sensors**タブをクリックして、対応する情報を表示します。
3. **Sensors**タブでセンサーの読み取り値を表示するには、センサーのタイプと名前を選択します。作業ウィンドウでは、次のタスクを実行できます。
   - 履歴の読み取りをクリアして新しい統計収集期間を開始するには、**Restart**をクリックします。
   - 折れ線グラフで過去24時間または過去7日間のセンサー読取値を表示するには、**Past 24 hours**または**Past 7 days**を選択します。グラフの線にカーソルを置くと、統計収集期間中の最小読取値、平均読取値および最小読取値を表示できます。
   - センサーの最大値、平均値、または最小値のみを表示するには、

     最大、平均、または最小 アイコンをそれぞれクリックします。

図19 センサー読み取りチャートの表示



ストレージ

Storageメニューでは、次のタスクを実行できます。

- ストレージコントローラー、論理ドライブ、物理ドライブ、およびストレージエラーに関する情報を表示します。
- 次のストレージコントローラーによって制御される物理ドライブおよび論理ドライブを帯域外方式で管理します。
  - RAID-LSI-9361-8i(1G)-A1-X
  - RAID-LSI-9361-8i(2G)-1-X
  - RAID-LSI-9361-8i(2G)
  - RAID-LSI-9460-8i(2G)

- RAID-LSI-9460-8i(4G)
- RAID-LSI-9460-16i(4G)
- HBA-LSI-9440-8i
- RAID-L460-M4
- RAID-P5408-Mf-8i-4GB
- RAID-P5408-Ma-8i-4GB
- HBA-H5408-Mf-8i
- RAID-LSI-9560-LP-16i-8GB
- RAID-LSI-9560-LP-8i-4GB

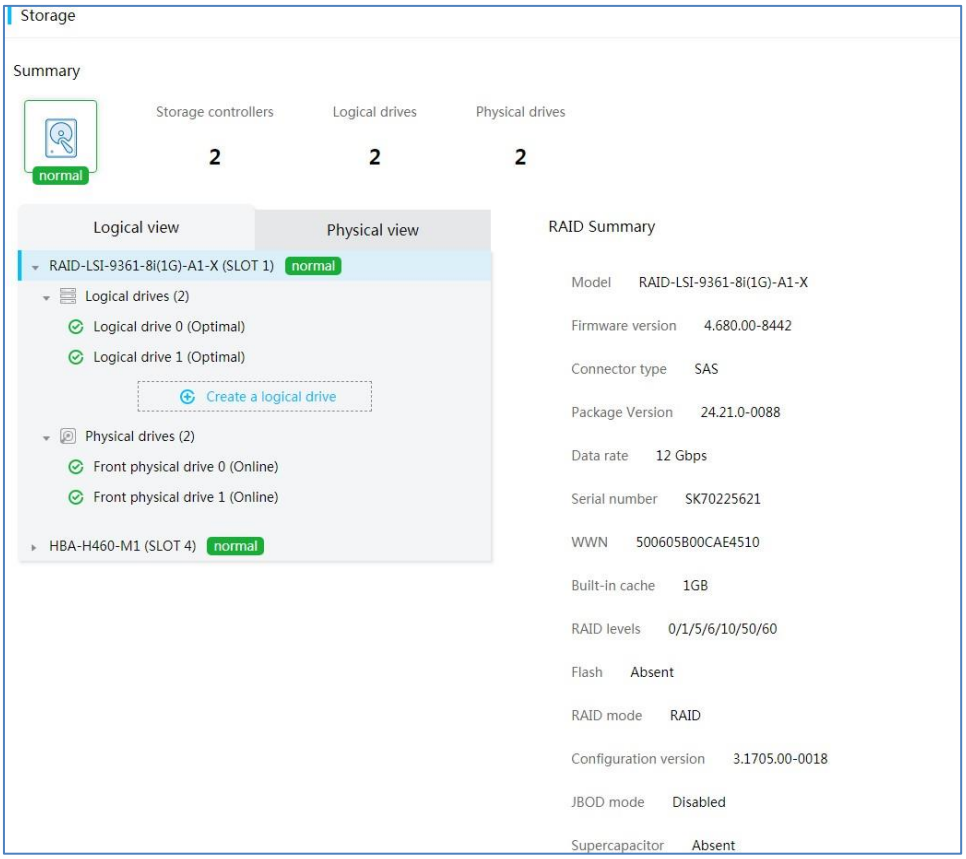
互換性の詳細については、OS互換性照会ツール (http://www.h3c.com/cn/Service/Document_Software/Document_Center/Server/)を参照してください。

ストレージサマリー情報の表示

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左側のナビゲーションペインで、**Storage**を選択します。
3. ストレージシステムのヘルスステータス、ストレージコントローラー、論理ドライブ、物理ドライブの数、障害の説明など、ストレージの概要情報を表示します。

   ヘルスステータスが異常の場合は、障害の説明を確認し、イベントログを調べてエラーを特定します。

図20 ストレージサマリー情報の表示



ストレージコントローラー情報を表示する

ストレージコントローラーに関する情報を表示するには、次の作業を実行します。

制限事項とガイドライン

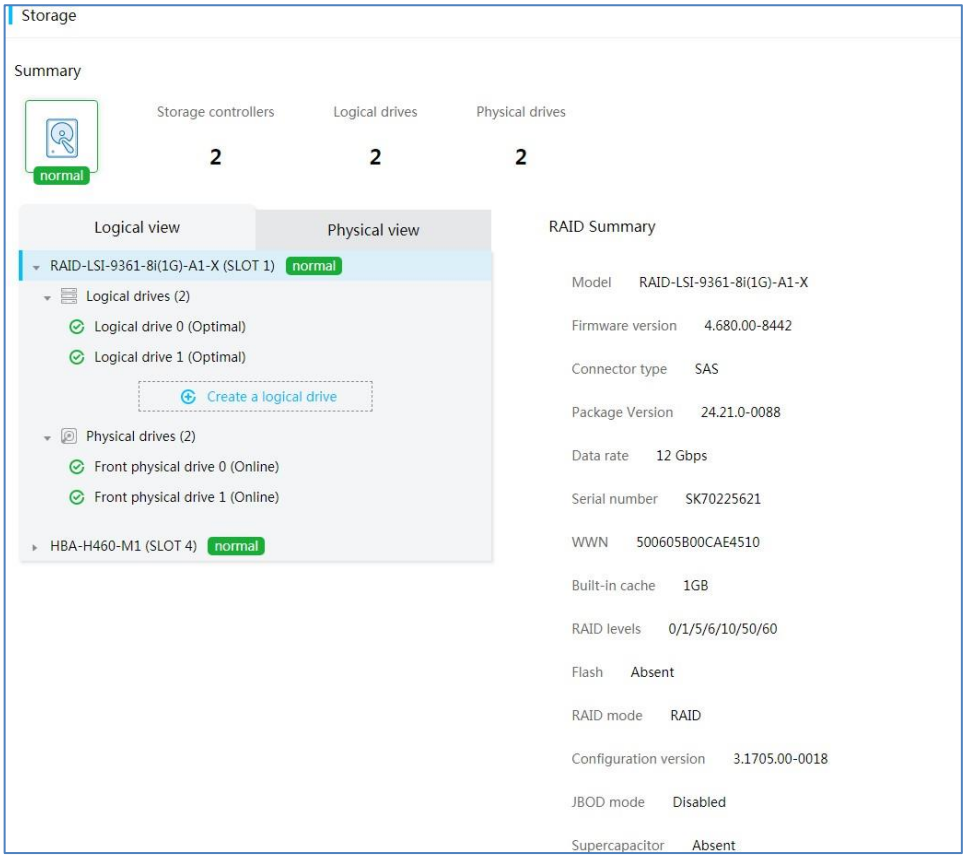
サーバーOSが正常に起動した後、**Storage**ページを更新して、最新のストレージ情報を取得します。

HDMは、帯域外管理をサポートしていないLSI HBAに関するストレージおよび温度情報を取得できません。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左側のナビゲーションペインで、**Storage**を選択します。
3. **Logical view**タブで、ストレージコントローラーを選択します。

図21 ストレージコントローラー情報の表示



パラメーター

ストレージコントローラー

- **Model**:ストレージコントローラーのモデル。
- **Vendor**::ストレージコントローラーのベンダー。
- **Firmware version**:ストレージコントローラーのファームウェアバージョン。
- **Package version**:ストレージコントローラーのソフトウェアパッケージバージョン。このフィールドは、一部のLSIストレージコントローラーでのみ使用できます。
- **Connector type**:ストレージコントローラーでサポートされているコネクタータイプ。
- **Data rate**:ストレージコントローラーのコネクターでサポートされるデータレート。
- **Serial number**::ストレージコントローラーのシリアル番号。
- **WWN**:ストレージコントローラーのSASアドレス。WWNは、LSI HBAカードが取り付けられている場合にのみ表示されます。
- **Built-in cache**:ストレージコントローラーに内蔵されているリード/ライトキャッシュの容量。
- **RAID levels**:ストレージコントローラーでサポートされるRAIDレベル。
- **Flash**:電源障害保護モジュールのフラッシュカードのステータス。
  - LSIストレージコントローラーの場合、ステータスオプションには次のものがあります。
    - **Normal**: フラッシュカードは正常に動作しています。

- **Abnormal**: フラッシュカードが正常に動作していません。
- **Absent**: フラッシュカードがスーパーキャパシターに接続されていないか、しっかりと取り付けられていないか、まったく取り付けられていません。

○ PMCストレージコントローラーの場合、ステータスオプションは次のとおりです。

- **Normal**: フラッシュカードは正常に動作しています。
- **Absent**: 電源障害モジュールのフラッシュカードが確実に取り付けられていないか、まったく取り付けられていません。
- **Abnormal_status code**: フラッシュカードが正常に動作していません。ステータスコードをチェックして、フラッシュカードが異常状態になる原因となる例外を特定できます。
- **Warning_status code**: フラッシュカードに警告が表示されます。ステータスコードをチェックして、フラッシュカードが警告状態になる原因となる例外を識別できます。

ステータスコードは16進数です。例外を識別するには、16進数のステータスコードを16桁の2進数(右から左へのビット0からビット15)に変換します。セットビットは、ビットが示す例外が存在することを意味します。セットビットとそれに対応する例外の詳細は、表9を参照してください。

たとえば、ステータスコードが0x500(バイナリ形式0000 0101 0000 0000)の場合、ビット8およびビット10で示される例外がフラッシュカードに存在します。

表9フラッシュカードの例外とそのセットビット

ビット番号	ビット状態	説明
0	1	GBサブシステムは現在初期化中です。
1	1	GBサブシステムは準備完了状態です。
2	1	GBサブシステムは学習サイクルを実行しています。学習サイクルは、通常の動作やデータ保護機能を妨げることはありません。
3	1	GBサブシステムに障害が発生しました。
4	1	スーパーキャパシターパックが最大温度しきい値を超えました。
5	1	スーパーキャパシターパックが警告温度のしきい値を超えました。
6	1	スーパーキャパシターパックが過電圧です。
7	1	スーパーキャパシターパックが最大充電電流を超えました。
8	1	GBサブシステムの学習サイクルが終了しました。
9	1	GBサブシステムの学習サイクルが失敗しました。
10	1	スーパーキャパシターパックが故障しました。
11	1	スーパーキャパシターパックの寿命が近づいています。交換をお勧めします。
12	1	スーパーキャパシターパックが寿命に達しました。交換が必要です。
13	1	スーパーキャパシターパックのキャパシターの1つがないようです。
14	該当なし	予約済み。
15	該当なし	予約済み。

注:

Greenバックアップ(GB)システムは、いくつかのタイプの動作ステータスの進行状況と健全性情報を報告します。

- **Mode**:ストレージコントローラーモード。
  - LSIストレージコントローラーでサポートされるオプションには、**RAID**およびJBODがあります。
  - PMCストレージコントローラーでサポートされるオプションには、**RAID**、**HBA**、**Mixed**があります。
- **Configuration version**:ストレージコントローラーの構成バージョン。
- **JBOD mod**:BIOSでのJBODモードの有効化ステータス。

- **Supercapacitor**:スーパーキャパシターの存在状態。
- **Charging status**:スーパーキャパシターで利用可能な残りの電力。

注:

FlashおよびChargingステータスフィールドは、電源障害保護モジュールがインストールされている場合にのみ使用できます。電源障害保護モジュールには、フラッシュカードとスーパーキャパシターが含まれています。システムの電源障害が発生した場合、このスーパーキャパシターは最低20秒間電力を供給できます。この間、ストレージコントローラーはデータをメモリーからフラッシュカードに転送します。フラッシュカードでは、データは無期限に、またはコントローラーがデータを取得するまで保持されます。

論理ドライブの管理

論理ドライブ情報を表示し、論理ドライブを作成するには、次の作業を実行します。

制限事項とガイドライン

論理ドライブを作成または削除したら、システムが操作を完了するまでしばらく待ち、ページを更新して操作の結果を確認します。

物理ドライブを使用して作成できる論理ドライブは1つだけです。

論理ドライブのデフォルトの最大容量は、設定可能な最大容量と多少異なる場合があります。論理ドライブの作成時にドライブ容量を指定しなかった場合、ドライブ容量は、システムによって計算されたデフォルトの最大容量です。

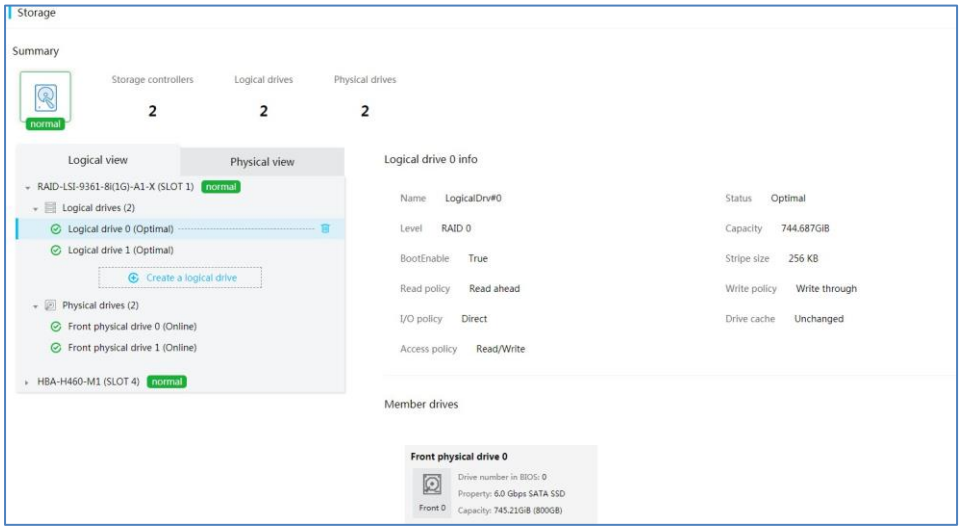
BIOSからJBODモードの有効化ステータスを表示および設定できるのは、RAIDモードの一部のLSIストレージコントローラーだけです。

ストレージコントローラーは、HDMを介して最大64台の論理ドライブを管理できます。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左側のナビゲーションペインで、**Storage**を選択します。
3. **Logical view**タブで、論理ドライブを選択してその情報を表示します。
4. 論理ドライブを削除するには、論理ドライブを選択し、アイコンをクリックします。
5. 論理ドライブを作成するには、**Create logical drive**をクリックし、ドライブパラメーターを指定して**save**。

図22 論理ドライブの情報



パラメーター

- **Name**:論理ドライブの名前で、0～15文字の文字列です。最良の方法として、文字と数字を使用し、感嘆符(!)、アットマーク(@)、シャープ記号(#)などの特殊文字は使用しないでください。PMCストレージコントローラーの場合、このフィールドは必須です。

- **Spans/Parity groups**:混合モードRAID(RAID 00、RAID 10、RAID 50、またはRAID 60)のスパンまたはパリティグループの数。
- **Initialization type**:初期化タイプを選択します。を選択します。次のオプションがあります。
  - **No** -論理ドライブを初期化しません。
  - **Fast** -論理ドライブの最初と最後の8 MBをドライブ作成時のデータ書き込み用に初期化し、次にバックグラウンドの残りの領域を初期化します。
  - **Full**-論理ドライブ内のすべての領域を初期化します。
- **Capacity**:ドライブの容量を入力します。論理ドライブの最小容量は100 MBです。容量を指定しない場合は、最大容量が使用されます。
- **Status**:論理ドライブのステータス。次のオプションがあります。
  - **Optimal** -論理ドライブは正常に動作しています。
  - **Degraded** -一部のRAIDメンバードライブが故障しており、すぐに交換する必要があります。
  - **Rebuilding** -RAIDアレイは、データを再構築し、縮退状態から回復するために再構築されています。
  - **Offline** -論理ドライブは破損しており、アクセスできません。
  - **Zeroing** -論理ドライブをフォーマットしています。この操作を行うと、すべてのデータが削除されます。
  - **Scrubbing** -論理ドライブ内のデータの連続性を維持するために、メンバードライブがスキャンされています。このフィールドは、RAID 5およびRAID 6論理ドライブなど、パリティビットを持つ論理ドライブで使用できます。
  - **Suboptimal** -RAID 6またはRAID 60論理ドライブの1つのメンバードライブに障害が発生しました。複数のメンバードライブに障害が発生した場合、論理ドライブは劣化状態になります。このフィールドは、RAID 6およびRAID 60論理ドライブで使用できます。
  - **Morphing** -データがドライブ間で移行されているか、RAIDアレイが新しいRAIDレベルに変更されています。
  - **Copying** -データはホットスペアディスクから障害が発生したドライブの交換用ドライブにコピーされます。この操作が完了すると、ホットスペアはホットスタンバイ状態に戻ります。
- **Level**:RAIDレベル。
- **BootEnable**:論理ドライブがブートドライブかどうかを示します。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。次のオプションがあります。
  - **True**-論理ドライブはブートドライブです。
  - **False**-論理ドライブはブートドライブではありません。
- **Stripe size**:各物理ドライブのストライプサイズ。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。
- **Read policy**:論理ドライブの読み取りポリシー。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。オプションは次のとおりです。
  - **No read ahead:** 先読み機能を無効にします。
  - **Read ahead**: 先読み機能を有効にします。この機能が有効になっている場合、コントローラーは要求されたデータを順次先読みし、追加データをキャッシュメモリーに格納します。
- **Write policy**:論理ドライブの書き込みポリシー。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。オプションは次のとおりです。
  - **Write through**:ドライブサブシステムがトランザクション内のすべてのデータを受信したときに、コントローラーがデータ転送完了信号をホストに送信できるようにします。
  - **Write back**:コントローラーキャッシュがトランザクション内のすべてのデータを受信したときに、コントローラーがデータ転送完了信号をホストに送信できるようにします。ストレージコントローラーにスーパーキャパシターが取り付けられていない場合、またはスーパーキャパシターに障害がある場合は、ライトスルーポリシーが使用されます。
  - **Always write back:** コントローラーキャッシュがトランザクション内のすべてのデータを受信したときに、コントローラーがデータ転送完了信号をホストに送信できるようにします。
- **I/O policy**:論理ドライブのI/Oポリシー。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。次のオプションがあります。
  - **Direct** -キャッシュモジュールがストレージコントローラーのすべての読み取りおよび書き込み操作を処理できるようにします。

- **Cached**-キャッシュモジュールがストレージコントローラー上で読み取りまたは書き込み操作を処理できないようにします。

- **Drive cache**:論理ドライブでドライブキャッシュが有効になっているかどうかを示します。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。次のオプションがあります。
  - **Unchanged**-デフォルトのドライブキャッシュポリシーが使用されます。
  - **Enable** -ドライブキャッシュが有効です。
  - **Disable** -ドライブキャッシュは無効です。
- アクセスポリシー:論理ドライブのアクセスポリシー。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。次のオプションがあります。
  - **Read/write**
  - **Read only**
  - **Blocked**
- **Acceleration method**:読み取り/書き込みキャッシュのステータス。このフィールドのサポートは、ストレージコントローラーモデルによって異なります。次のオプションがあります。
  - **Controller Cache:** 読み取り/書き込みキャッシュを有効にします。
  - **None** -読み取り/書き込みキャッシュを無効にします。
  - **IO Byp**ass-ストレージコントローラーがI/Oバイパスパスを使用して読み取り/書き込みパフォーマンスを向上できるようにします。この機能は、SSDでのみ使用できます。

物理ドライブ情報を表示する

制限事項とガイドライン

ストレージコントローラーまたはドライブバックプレーンが予想どおりに取り付けられていない場合は、物理ドライブ番号が正しくない可能性があります。

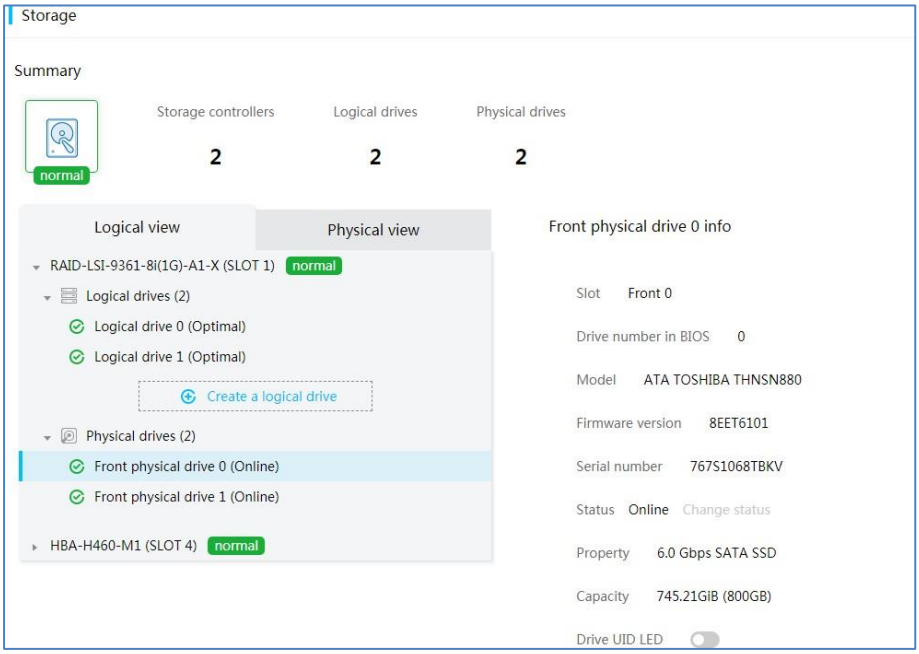
ドライブのステータスがFailedの場合は、ドライブ情報(ドライブのサイズ、速度、インターフェースタイプなど)が不正確になる可能性があり、参照用にのみ提供されます。

Unconfigured Good(Foreign)、Unconfigured Bad(Foreign)、またはOnline状態の物理ドライブの状態は変更できません。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左側のナビゲーションペインで、**Storage**を選択します。
3. 論理ドライブの作成に使用された物理ドライブに関する情報を表示するには、以下の手順に従ってください。
   a. **Logical view**タブで、ストレージコントローラーと論理ドライブを選択します。
   b. 物理ドライブを選択します。
   c. LSIストレージコントローラーが取り付けられている場合は、**Change status**をクリックして物理ドライブの状態を変更できます。
   d. (オプション)ドライブを特定するには、ドライブUID LEDを有効にします。この機能は、一部の物理ドライブでのみ使用できます。

図23 物理ドライブ情報の表示(論理ビュー)



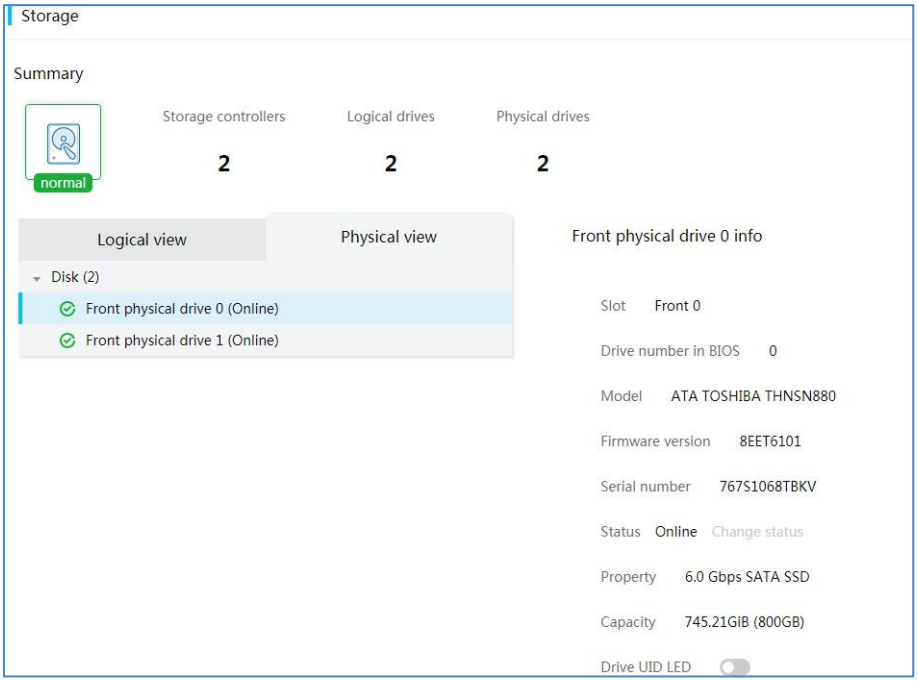
4. 論理ドライブの作成に使用されていない物理ドライブに関する情報を表示するには、以下の手順に従ってください。

   a. **Physical view**タブをクリックします。

   b. (オプション)物理ドライブの状態を変更するには、**Change status**をクリックします。この機能は、一部の物理ドライブでのみ使用できます。

   c. (オプション)ドライブを特定するには、ドライブUID LEDを有効にします。この機能は、一部の物理ドライブでのみ使用できます。

図24 物理ドライブ情報の表示(物理ビュー)



パラメーター

HDDおよびSSDドライブ

- **Slot**:物理ドライブのスロット番号。
- **Drive number in BIOS**:BIOSに表示されているドライブ番号。
- **Vendor**:物理ドライブのベンダー。
- **Model**:物理ドライブのモデル。
- **Firmware versionン**:物理ドライブのファームウェアバージョン。
- **Serial number**:物理ドライブのシリアル番号。
- **Status**:物理ドライブのステータス。次のオプションがあります。

  LSIストレージコントローラーが取り付けられている場合は、**Change status**をクリックして物理ドライブの状態を変更できます。

  - **Ready/Unconfigured Good**:物理ドライブは初期化されているか、まだ構成されておらず、RAID構成およびホットスペア設定に使用できます。ステータス名は、ストレージコントローラーモデルによって異なります。
  - **Unconfigured Bad:** 物理ドライブでエラーが発生したか、物理ドライブにRAID情報が残っています。障害のあるドライブを交換するか、残っているRAID情報をクリアする必要があります。
  - **Optimal/Online**:物理ドライブはすでにRAIDの作成に使用されています。ステータス名は、ストレージコントローラーモデルによって異なります。
  - **Offline** -物理ドライブは無効です。
  - **Rebuilding** -物理ドライブはRAID再構築で使用されています。
  - **Hot spare** -物理ドライブはすでにホットスペアとして使用されています。
  - **JBOD**-物理ドライブはパススルードライブであり、RAID構築なしでOSで直接使用できます。
  - **Failed** -物理ドライブに障害が発生しました。
  - **Predic**t_Fail/FPA: 物理ドライブは、考えられる障害を分析しています。ステータス名は、ストレージコントローラーモデルによって異なります。
  - **Ra**w-新しい物理ドライブまたは未構成の良好な状態の物理ドライブが初期化されていません。
  - **Normal** -物理ドライブは、ストレージ用の一般的なハードディスクとして使用されます。他の目的には使用されません。
  - **Copyback** -データがホットスペアディスクから障害が発生したドライブの交換用ドライブにコピーされます。この操作が完了すると、ホットスペアはホットスタンバイ状態に戻ります。このフィールドは、LSIストレージコントローラーに接続されている物理ドライブに対してのみ使用できます。
- **Rebuilding progress**:RAID再構築中の物理ドライブの再構築の進行状況。このフィールドは、物理ドライブが**Rebuilding**の場合にのみ表示されます。
- **Type**:物理ドライブのインターフェース速度、インターフェースタイプ、およびドライブタイプ。このフィールドには、一部のストレージコントローラーについて、インターフェース速度の代わりにネゴシエートされた速度が表示されます。
- **Capacity**:物理ドライブの容量。
- **Remaining life**:残りのドライブ寿命(%)。このフィールドは、次のドライブが、アウトオブバンドRAID構成をサポートするLSIストレージコントローラーに接続されている場合にのみ使用できます。
  - インテルSSD S4610ドライブ。
  - インテルSSD S4600ドライブ。
  - インテルSSD S4510ドライブ。
  - インテルSSD S4500ドライブ。
  - インテルSSD S3520ドライブ。
  - Micron SSD 5200ドライブ
  - Samsung SSDドライブ。
- **UID LED**:ドライブUID LEDの状態。このフィールドをクリックすると、ドライブUID LEDを管理できます。このフィールドは、ドライブがドライブバックプレーンに直接接続されている場合にのみ使用できます。

NVMeドライブ

- **Product name**:NVMeドライブの製品名。
- **Vendor**:NVMeドライブの製造元。
- **Status**:NVMeドライブステータス:
  - **Normal** -NVMeドライブは正常に動作しています。
  - **Abnormal** -NVMeドライブで、修正不可能なバスエラー、バス致命的エラー、またはPCIeエラーエラーが発生しました。
  - **Spare space below threshold**: NVMeドライブの使用可能なスペースがしきい値を下回っています。
  - **Temperature anomaly**: NVMeドライブの温度が上限しきい値を超えているか、下限しきい値を下回っています。
  - **Subsystem degraded:** ストレージメディアまたは内部エラーのため、NVMeサブシステムの信頼性が低下しています。
  - **Read-only mode**:NVMeドライブは読み取り専用モードになりました。
  - **Cache failed**-揮発性メモリーバックアップデバイスに障害が発生しました。
- **Firmware version**:NVMeドライブのファームウェアバージョン。HDMがNVMeドライブのファームウェアバージョンの表示をサポートしていない場合、このフィールドにはN/Aと表示されます。
- **Serial number**:NVMeドライブのシリアル番号。
- **Model**:NVMeドライブのモデル。
- **Interface type**:NVMeドライブのインターフェースタイプ。
- **Capacity**:NVMeドライブの容量。
- **Physical location** : NVMeドライブのスロット番号。
- **Slot number** -システムによってドライブに割り当てられたNVMeドライブスロット番号またはPCIeスロット番号。
- **Max speed**: NVMeドライブでサポートされる最大速度。
- **Percentage drive life used**:使用されたNVMeサブシステム寿命のパーセンテージの推定値。100より大きい値を指定できます。
- **UID LED**:ドライブUID LEDの状態。このフィールドをクリックすると、ドライブUID LEDを管理できます。このフィールドは、ドライブがドライブバックプレーンに直接接続されている場合にのみ使用できます。

電源管理

サーバーの電源をオンまたはオフにする

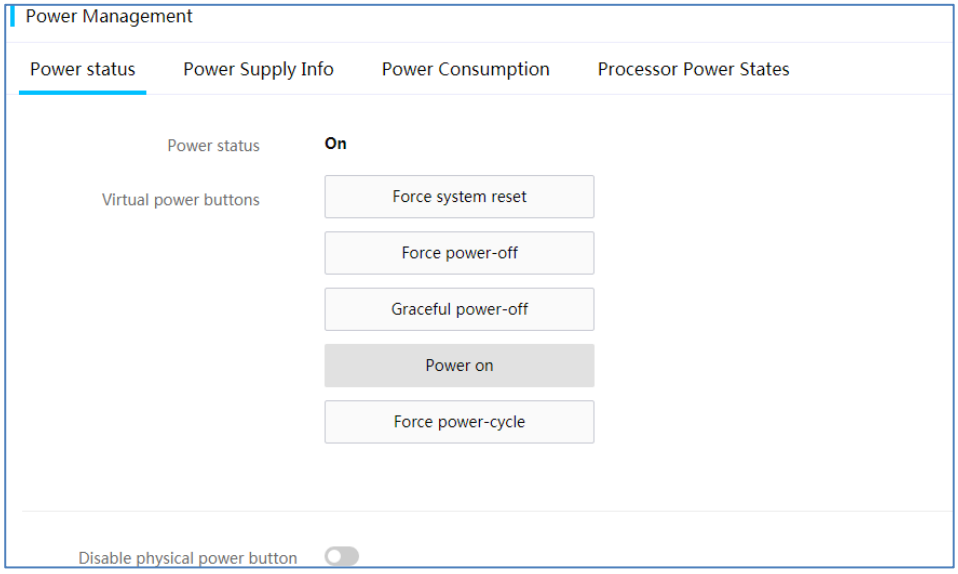
△注意:

強制電源切断、強制システムリセットおよび強制電源再投入の各アクションは、データの破損または損失の原因となる可能性があります。これらのアクションを実行するときは、サービスへの影響を十分に理解していることを確認してください。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. **Power status**タブをクリックして、サーバーの現在の電源ステータスを表示します。
4. 電源ステータスを変更するには、目的の操作をクリックします。
5. 必要に応じて、物理電源ボタンを有効にするか無効にするかを選択します。このボタンは、G5サーバー(ブレードサーバーを除く)でのみ使用できます。

図25 サーバーの電源投入または電源切断



パラメーター

- **Force system reset**::ウォームは、サーバーの電源を再投入せずに、サーバーをリブートします。
- **Force power-off**:強制的にただちにサーバーをシャットダウンします。これは、サーバーの電源ボタンを5秒間押した場合と同じです。
- **Graceful power-off**:最初にオペレーティングシステムをシャットダウンしてから、サーバーから電源を切断します。
- **Power on**:サーバーを起動します。
- **Force power-cycle**:サーバーの電源をオフにしてからオンにします。
- **Disable physical power button**:物理電源ボタンを制御します。電源ボタンが無効になっている場合、ユーザーは物理電源ボタンを使用してサーバーの電源ステータスを管理することはできません。

パワーサプライ情報の表示

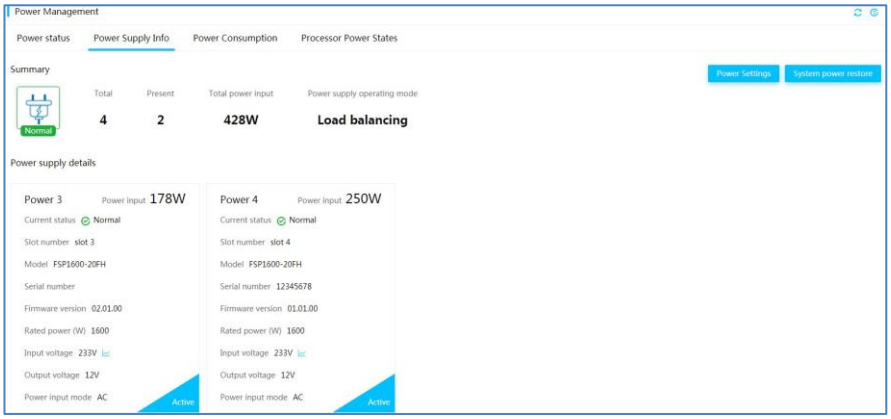
制限事項とガイドライン

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

手順

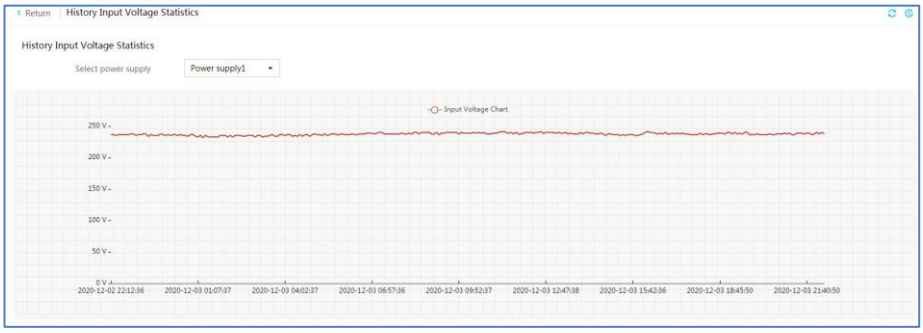
1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. **Power Supply Info**タブをクリックします。
4. 電源装置の概要および詳細情報を表示します。

図26 パワーサプライ情報の表示



5. 入力電圧の履歴を表示するには、電圧アイコンをクリックします。

図27 入力電圧履歴を表示する



パラメーター

- **Power mode**:電源装置の役割。オプションには、**Active**と**Standby**があります。アクティブな電源装置は通常どおりに電力を供給し、スタンバイ電源装置は低電力出力を供給します。
- **Power input**:電源装置の入力電力
- **Current status**:パワーサプライのステータス。パワーサプライが異常状態の場合は、イベントログを調べてエラーを特定します。
- **Slot number**:電源装置が存在するスロットの番号。
- **Model**:電源装置のモデル。
- **Serial number**:メーカーが割り当てた固有のコード。
- **Firmware version**ン:パワーサプライのファームウェアバージョン。
- **Rated power**:電源装置の定格電力。
- **Input voltage**:電源装置の入力電圧。
- **Output voltage**:電源の出力電圧。
- **Power input mode**:電源入力モード。次のオプションがあります。
  - **No input**し:電源装置が電源に接続されていません。
  - **AC**:電源装置はAC電源に接続されています。
  - **HVDC**:電源装置は高電圧DC電源に接続されています。電圧は192 Vから400 Vの範囲です。

- **LVDC**:電源装置は低電圧のDC電源に接続されています。電圧は12 Vから72 Vの範囲です。

- 障害の説明:電源装置エラーに関するイベントログ情報。

電源装置の動作モードを設定する

制限事項とガイドライン

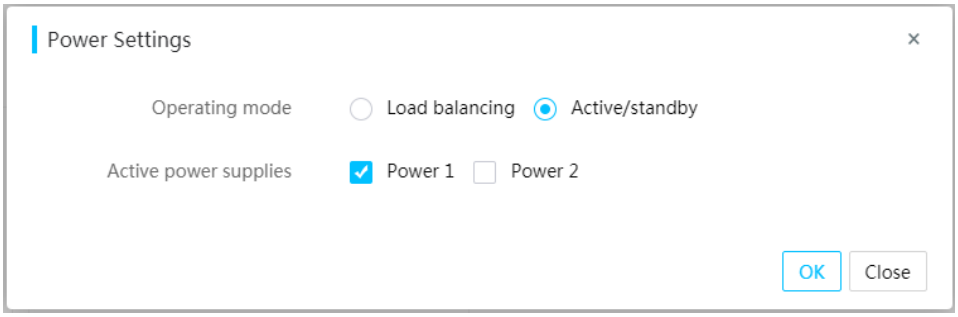
この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

複数の電源装置の動作モードを一括して設定できない場合、HDMはスロット番号が最も小さい電源装置に対してだけログメッセージを生成します。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. 作業ウィンドウで、**Power Supply Info**タブをクリックします。
4. **Power Settings**をクリックします。
5. 電源装置の動作モードを選択します。次のオプションがあります。
   - **Load balancing**:すべての電源装置がバランスのとれた方法で電力を供給できるようにします。
   - **Active/standby:** アクティブ電源装置が主に電力を供給できるようにします。このモードでは、少なくとも1つのアクティブ電源装置と少なくとも1つのスタンバイ電源装置を指定する必要があります。アクティブ電源装置に障害が発生すると、スタンバイ電源装置がアクティブになって電力を供給します。アクティブ電源装置の実際の電力消費量が最大定格電力消費量の62%を超えると、スタンバイ電源装置がアクティブになって電力を供給します。アクティブ/スタンバイスイッチオーバーは、元のアクティブ電源装置の電力消費量が低下した後は実行されません。
6. OKをクリックします。

図28 電源装置の動作モードの設定



パラメーター

障害の説明:電源装置エラーに関するイベントログ情報。

自動電源投入を構成する

サーバーが電源に接続されている場合に、サーバーの電源投入ポリシーを設定するには、次の作業を実行します。

制限事項とガイドライン

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

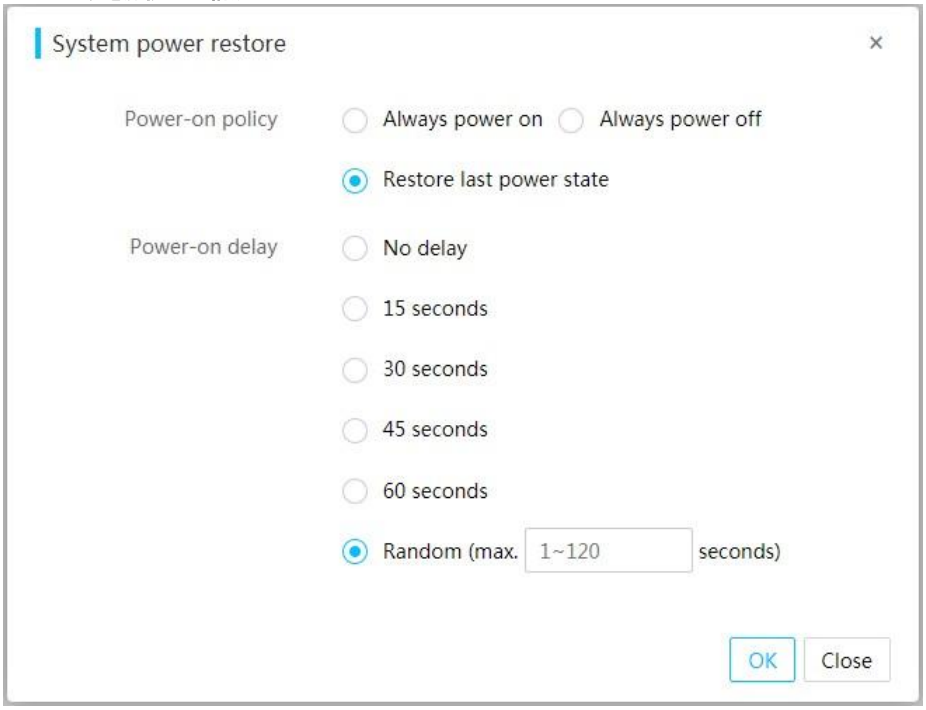
手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. 作業ウィンドウで、**Power Supply Info**タブをクリックします。
4. **System Power Restore**をクリックします。
5. 電源投入ポリシーを選択し、電源投入遅延を設定します。

- **Power-on policy**:サーバーが電源に接続されているときにサーバーを起動するかどうかを選択します。オプションには、**Always power on**、**Always power off**、および**Restore last power state**があります。
  - サーバーが電源に接続されているときに常に自動的に起動するようにするには、**Always power on**を選択します。
  - サーバーが電源に接続されているときにサーバーの電源を切らないようにするには、**Always power off**を選択します。
  - 前回の電源切断時にサーバーを電源状態に戻すには、**Restore last power state**を選択します。
- **Power-on delay:** 電源投入遅延時間を設定します。**Random**を選択すると、遅延時間の範囲をカスタマイズできます。

6. OKをクリックします。

図29 自動電源投入の構成



パラメーター

障害の説明:電源装置エラーに関するイベントログ情報。

消費電力情報を表示する

電力消費サマリー、消費電力上限情報、および電力消費履歴を表示するには、次の作業を実行します。最大、平均、および最小の電力消費を含む、過去24時間または7日間の5分間のサーバー電力消費統計を表示できます。

制限事項とガイドライン

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

R4950 G3、R4950 G5、およびR5500 G5サーバーは、平均センサー読み取り値の表示だけをサポートしています。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. 作業ウィンドウで、**Power Consumption**タブをクリックします。
4. 消費電力情報、消費電力上限値、および電源履歴情報を表示します。

- 履歴の読み取りをクリアして新しい統計収集期間を開始するには、**Restart**をクリックします。
- 最大、平均、最小の消費電力のみを表示するには、それぞれ **Max**、**Avg**、**Min**のアイコンをクリックします。

図30 電力消費情報の表示

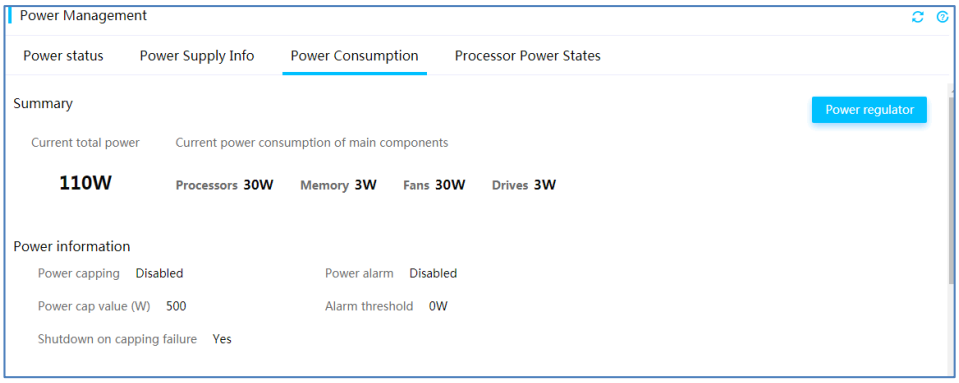


図31 電力消費履歴の表示

電源アラームを設定する

電源アラームを使用すると、サーバーの合計電力消費量がアラームしきい値を超えたときに、システムはアラームログを生成できます。

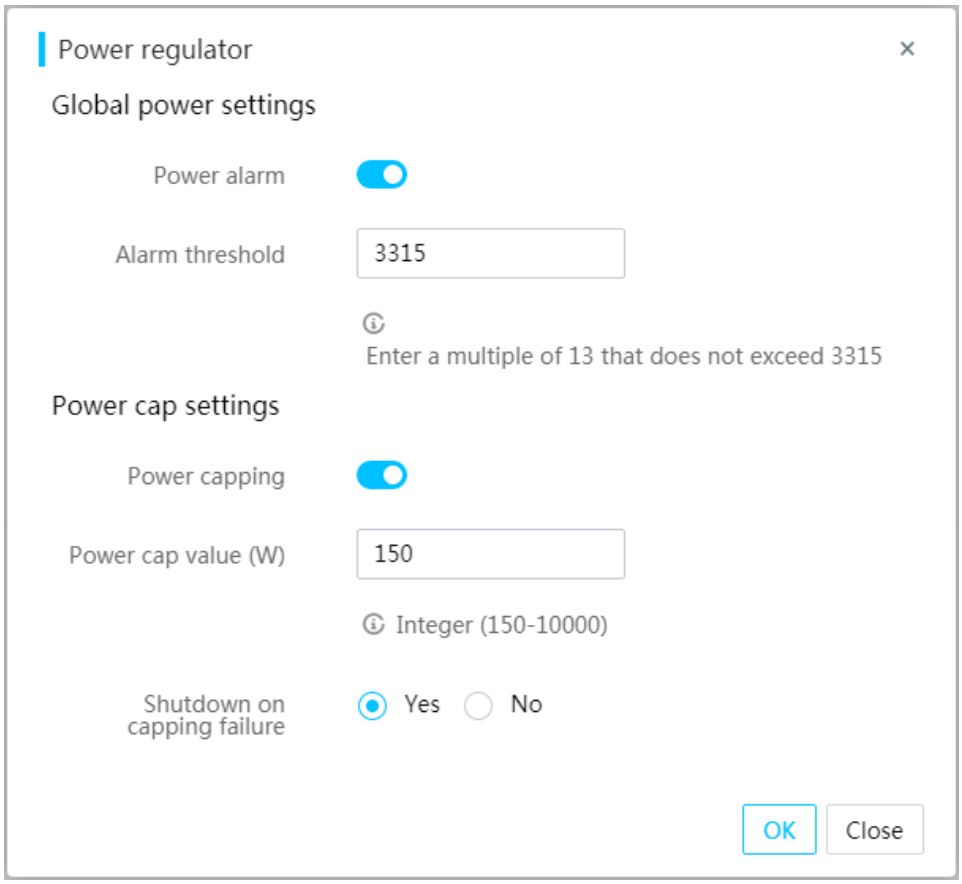
制限事項とガイドライン

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. 作業ウィンドウで、**Power Consumption**タブをクリックします。
4. **Power regulator**をクリックします。
5. 電源アラームをイネーブルにしてから、アラームしきい値を指定します。
6. **OK**をクリックします。

図32 電源アラームの設定



消費電力上限の設定

消費電力上限は、サーバーの消費電力上限値を、サーバーの最大定格電力以下に制限します。

消費電力上限値を超えると、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。消費電力が30秒以内に消費電力上限値を下回ることができない場合、消費電力上限は失敗します。

消費電力上限の障害が発生した場合にシャットダウンまたは実行を継続するようにサーバーを設定できます。

制限事項とガイドライン

△注意:

消費電力上限の設定に失敗した場合にサーバーがシャットダウンすると、サービスが中断されます。この機能を使用するには、その影響を理解しておく必要があります。

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

消費電力上限はシステムのパフォーマンスを犠牲にします。パフォーマンスの低下を避けるために、消費電力上限の値は慎重に選択してください。

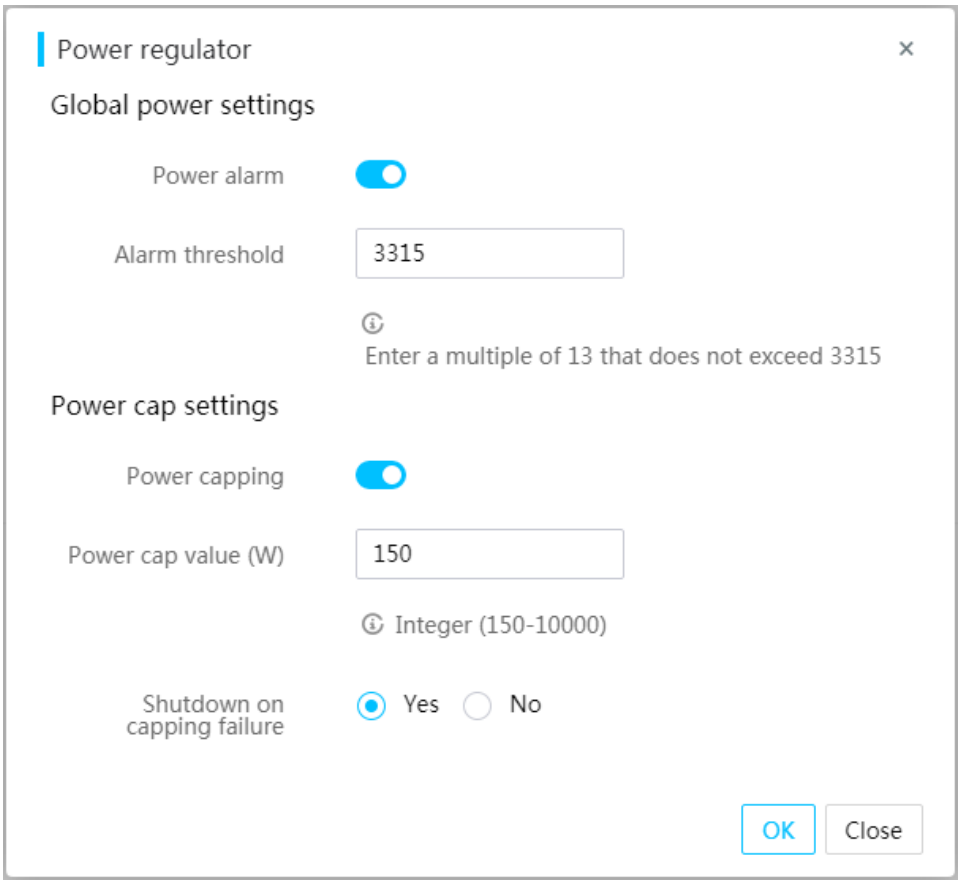
HDMは再起動中にサーバーの電源消費統計を取得できません。HDM消費統計を復元すると、電源設定がクリアされます。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。
3. 作業ウィンドウで、**Power Consumption**ブをクリックします。

4. **Power regulator**をクリックします。
5. 消費電力上限をイネーブルにし、消費電力上限値を設定してから、消費電力上限障害時に実行するアクションを設定します。
6. **OK**をクリックします。

図33 消費電力上限の設定



プロセッサーの電源状態の設定

プロセッサーの電源状態および電源装置の動作モードを設定するには、次の作業を実行します。

プロセッサーの電力状態を変更することにより、プロセッサーの消費電力を調整できます。

制限事項とガイドライン

この機能は、R4950 G3、E3200 G3、B5700 G3、B5800 G3、B7800 G3、B5700 G5、R4950 G5、R5500 G5 AMD、またはAE100では使用できません。

前提条件

電源状態を有効にするには、BIOSの**Socket Configuration** >**Advanced Power Management Configuration**で次のタスクを設定します。

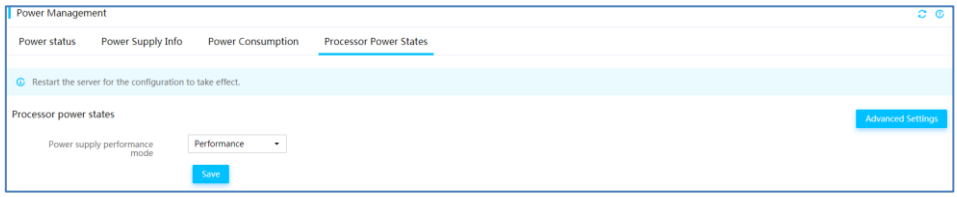
1. **EIST(P-States)およびSoftware Controlled T-Statesを**Enabled**に設定します。**
2. Tステートスロットルレベルを選択します。
3. **Hardware P-States**を**Disable**に設定します。
4. **Power Performance Tuning**を**BIOS Controls EPB**に設定します。

手順

1. 上部のナビゲーションバーで、**System**をクリックします。
2. 左ナビゲーションペインで、**Power Management**を選択します。

3. **Processor Power States**タブをクリックします。
4. **Advanced Settings**をクリックします。
5. 優先するP-stateまたはT-stateの値を調整し、**OK**をクリックします。使用可能な状態の値は、プロセッサーのモデルによって異なります。
6. パワーサプライのパフォーマンスモードを選択し、**save**をクリックします。パフォーマンスモードのオプションは次のとおりです。
   - **Performance**:パフォーマンスファーストモードを示します。
   - **Balanced**-パフォーマンスと消費電力のバランスモードを示します。
   - **Power**-プロセッサーの速度と消費電力をプロセッサーの使用量に合わせて自動的に調整します。このモードは総消費量を削減し、パフォーマンスへの影響はほとんどまたはまったくありません。
7. サーバーを再起動して、設定を有効にします。

図34 省電力の構成



パラメーター

- **P-state**:プロセッサーの動作周波数を定義します。P-state値が小さいほど動作周波数が高いことを表し、パフォーマンスと消費電力が高くなります。
- **T-state**:プロセッサーのデューティサイクルを定義します。T-stateの値が小さいほどデューティサイクルが高いことを表し、パフォーマンスと消費電力が高くなります。

熱管理

温度センサーのステータスと読み取り値を表示する

HDMでは、ヒートマップ形式とテーブル形式の両方で温度データが表示されるので、サーバーの冷却パフォーマンスの監視に役立ちます。

- 温度ヒートマップは、2Dおよび3Dビューでサーバーシャーシ内部の温度分布を示すために緑と赤の間の色を使用し、センサーを表すために円を使用します。緑は0°C(32°F)を示します。温度が高くなると、色は赤に変わるまで暖かくなります。温度ヒートマップを使用すると、冷却状態が悪いコンポーネントをすばやく識別できます。
- 温度センサーテーブルには、各センサーの温度読み取り値、ステータス、座標が表示されます。

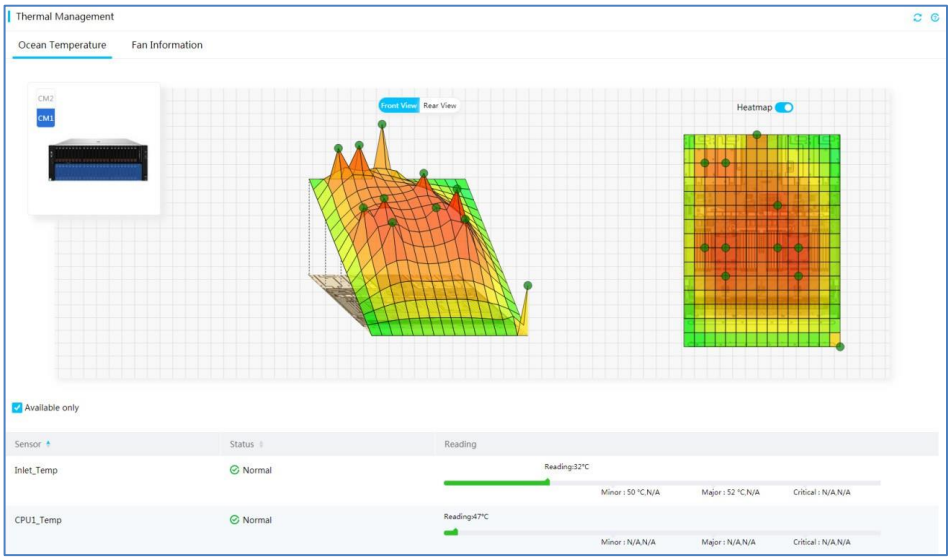
制限事項とガイドライン

温度ヒートマップには、値が負のセンサーは表示されません。

手順

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**Thermal Management**を選択します。
3. 温度ヒートマップおよびセンサーリストを表示します。

図35 温度センサの表示ステータスおよび読取値



パラメーター

- **Status**:構成部品の温度ステータス:
  - **Normal**:温度は正常で、マイナーしきい値の下限と上限の間です(排他的)。アクションは必要ありません。
  - **Minor** -温度は、下限メジャーしきい値(排他)と下限マイナーしきい値(含む)の間、または上限マイナーしきい値(含む)と上限メジャーしきい値(排他)の間にあります。管理上の注意が必要です。
  - **Major** -温度は、下限のクリティカルしきい値(排他的)と下限のクリティカルしきい値(包括的)の間、または上限のクリティカルしきい値(包括的)と上限のクリティカルしきい値(排他的)の間にあります。早急な対応が必要である。
  - **Critical** -温度が下限のクリティカルしきい値以下であるか、上限のクリティカルしきい値以上である。即時のアクションが必要です。
  - N/A-監視対象コンポーネントがインストールされていないか、温度センサーを読み取れません。
- **Reading**:現在の温度。HDMがセンサーの読み取りに失敗した場合、このフィールドにはN/Aと表示されます。
- **Thresholds**:温度しきい値:
  - **Critical** -下限および上限のクリティカルしきい値。温度がいずれかのしきい値に達すると、サーバーはコンポーネントの損傷を避けるために自動的にシャットダウンすることがあります。
  - **Major** -メジャーの下限および上限しきい値。温度がいずれかのしきい値に達すると、サーバーのパフォーマンスが著しく低下します。
  - **Minor** -下位および上位のマイナーしきい値。温度がいずれかのしきい値に達すると、サーバーのパフォーマンスがわずかに低下します。

ファンを管理する

ファン情報およびファンエラーを表示し、ファン速度モードを設定するには、次の作業を実行します。

ファン速度モードを調整して、冷却、ノイズ制御、およびエネルギー効率のパフォーマンスを最適化できます。

制限事項とガイドライン

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。

ファン速度モードを設定します。

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**Thermal Management**を選択します。
3. ファン情報を表示します。
4. **Fans**をクリックします。
5. ファン速度モードを選択します。
6. **OK**をクリックします。

図36 ファン情報の表示

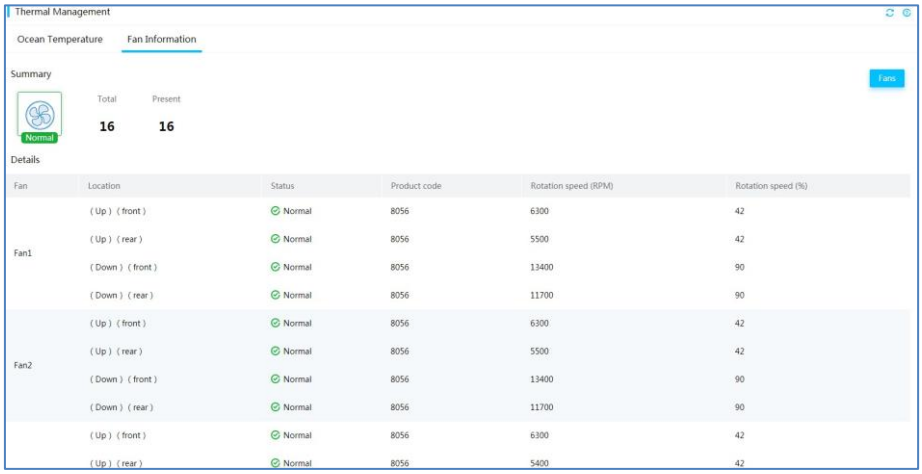
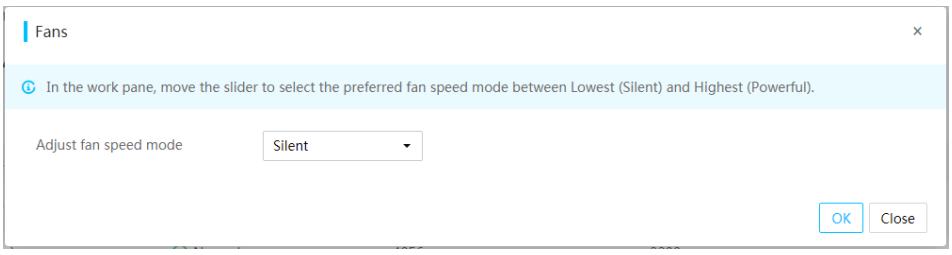


図37 ファンの管理



パラメーター

- **Status**:ファンの動作ステータス。
- **Model**:ファンモデル。
- **Rotation speed (RPM)**:現在の実際の回転速度。
- **Rotation speed (%)**:定格RPMに対する現在のRPMのパーセンテージ。
- **Fault description**:ファンエラーに対して生成されたアラーム。
- **Silent**:ファンは、サーバーの放熱に必要な最低速度で動作できるようになります。このモードは、ノイズ要件が高いシナリオに適しています。
- **Balanced**:ファンを高速で動作させて、バランスのとれたノイズ制御と冷却性能を実現します。
- **Powerful**:ファンを可能な限り高速で動作させることができます。このモードは、サーバーが高い冷却性能を

必要とするシナリオに適しています。たとえば、サーバーがビジーで、主要コンポーネント(プロセッサーなど)の負荷が高い場合や、周囲温度が頻繁に変化する場合などです。

- カスタム:カスタマイズされたファン速度レベルを指定します。レベルが高いほど、速度が高く、ノイズが大きいことを表します。

リソースの概要

リソース使用率アラームしきい値を設定する

プロセッサー、メモリー、およびディスク使用量のアラームしきい値を設定するには、次の作業を実行します。

制限事項とガイドライン

この機能を使用するには、サーバーのオペレーティングシステムにFIST SMSをインストールして実行する必要があります。詳細については、『H3C Servers FIST SMS User Guide』を参照してください。

HDMから帯域幅使用量のアラームしきい値を設定することはできません。このアラームしきい値を設定するには、IPMIコマンドを使用します。詳細については、『H3C HDM IPMI Basics Command Reference』を参照してください。

アラームが発生またはクリアされると、システムはログエントリを生成します。アラームはイベントログに表示できます。

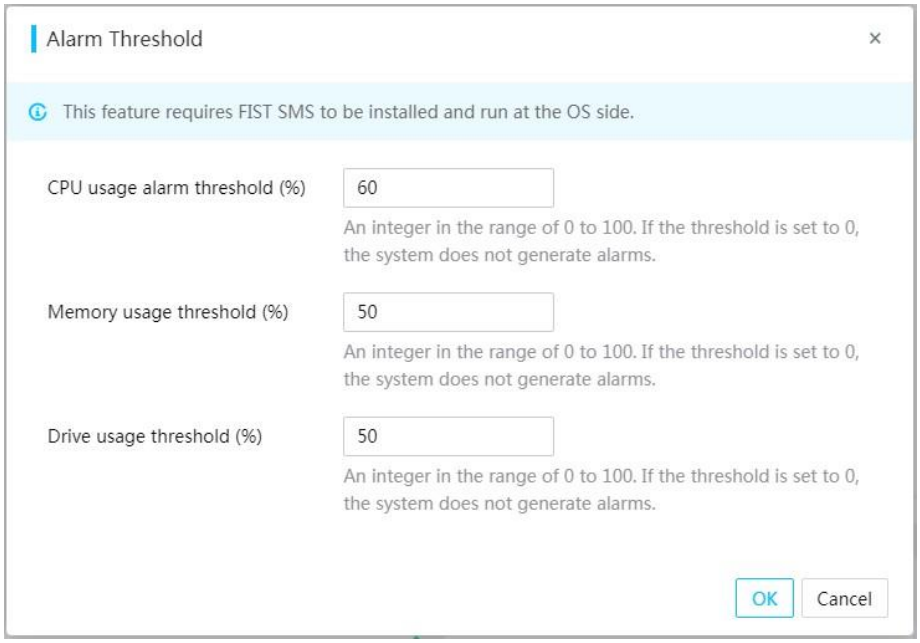
手順

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**Resource Summary**を選択します。
3. **Resource summary**タブをクリックして、現在のプロセッサー使用量、メモリー使用量、ディスク使用量、ディスクパーティションディレクトリ、使用済みディスク領域、および合計パーティションサイズを表示します。

   図38 リソースの概要の表示

4. **Advanced Settings**をクリックします。
5. プロセッサー使用量、メモリー使用量、およびディスク使用量のアラームしきい値を設定し**OK**をクリック。

図39 リソース使用率アラームしきい値の設定



パラメーター

ドライブ使用率のしきい値(%):パーティションの合計サイズに対する使用済みディスク領域の割合、ディスクパーティションディレクトリ、使用済み領域、およびパーティション領域の合計。

CUPS情報の表示

CUPS(Compute Usage Per Second)機能は、システム内のプロセッサー(CPU)、メモリーおよびI/Oの使用状況をリアルタイムで監視します。システムで実行されている主なサービスのタイプを示すために、CPU、メモリーおよびI/Oして、システムで実行されている主なサービスのタイプを示します。CUPSの負荷率は、OSで計算されたリソース使用状況とは相関しません。

CPU、メモリー、またはI/O CUPSの動的負荷係数が高い場合は、システムで実行されている主なサービスが、計算負荷、メモリー負荷、またはI/O負荷であることを示します。

制限事項とガイドライン

この機能は、R4950 G3、R4950 G5、またはR5500 G5 AMDサーバーでは使用できません。

折れ線グラフには、CPU、メモリーおよびI/O CUPのロードファクタの合計が表示されます。各ロードファクタの値を表示するには、グラフ内の線にカーソルを置きます。3つのロードファクタすべてが0%の場合、合計は0%です。

サーバーの電源がオフになっているか、オペレーティングシステムでサービスが実行されていない場合、CPU、メモリー、およびI/O CUPの動的負荷係数はすべて0%です。

CUPSモニタリングはアウトオブバンド機能であり、プロセッサーリソースを消費しません。HDM設定を復元

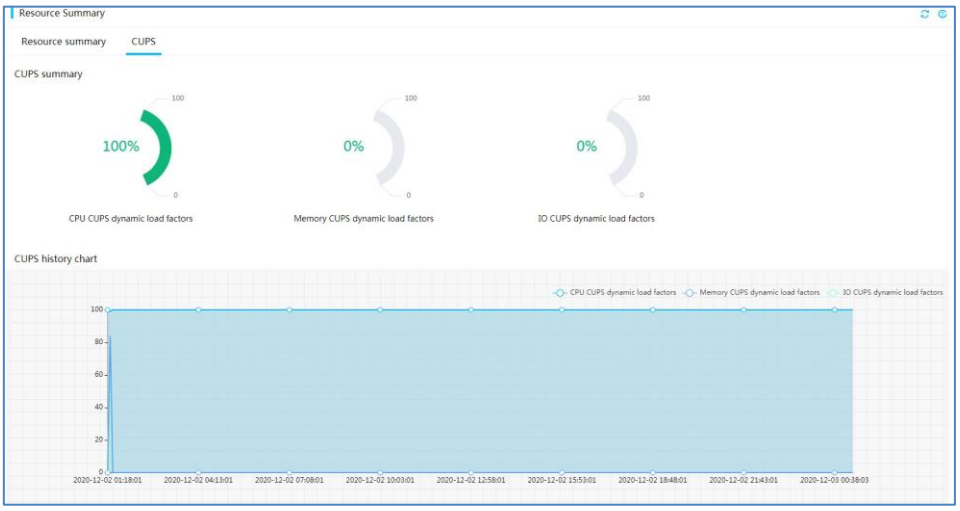
すると、CUPS統計情報がクリアされます。

CPUおよびMEM CUPSの動的負荷係数は、OSで計算されたCPUおよびMEMの使用率とは相関しません。

手順

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**Resource Summary**を選択します。
3. **CUPS**タブをクリックして、CUPS情報を表示します。

図40 CUPS情報の表示



パラメーター

- **CPU CUPS dynamic load factor**:CPUコアの累積使用率。CPU CUPS動的負荷率が高い場合は、システムで実行されている主なサービスが計算集約的であることを示します。
- **Memory CUPS dynamic load factor**:使用済メモリーに関連しないメモリーバスの累積転送率。メモリーCUPS動的負荷率が高い場合は、メモリーバスへのアクセス頻度が高いことを示します。OSのメモリー使用量は、合計メモリー容量を使用済メモリー容量で除算したものです。たとえば、8 GBのメモリーを2 GB使用する場合、メモリー使用量は25%です。
- **I/O CUPS dynamic load factor**:PCIeバスのI/O帯域幅使用率。I/O CUPS動的負荷率が高い場合は、システムで実行されている主なサービスがI/O集中型であることを示します。

システム設定

ブートオプションを設定する

サーバーが次回のリブート時に使用するブートモードおよびブートデバイスは**Boot Options**または**System Boot Order**セクション。

システムブート順序は、サーバーがブートしようとするデバイスの優先順位を定義します。

制限事項とガイドライン

- BIOSの起動フェーズでブートオプションを設定すると、設定が有効にならない場合があります。
- 永続ブートオプションがシステムブート順序設定と矛盾する場合は、永続ブートオプションが有効になります。
- ワンタイムブートオプションがシステムブート順序の設定と矛盾する場合、ワンタイムブートオプションは次のリブート時に有効になります。
- ブートオプションの設定をサポートしているのは、G5サーバーだけです。
- システムブート順序は、HDM-2.11以降でのみ設定できます。

前提条件

レガシーモードのハードディスクドライブから起動するようにサーバーを設定している場合は、ハードディスクドライブがレガシーモードをサポートしていることを確認します。

次回のリブート用にブートオプションを設定します。

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**System Settings**を選択します。
3. **Boot Options**タブをクリックします。

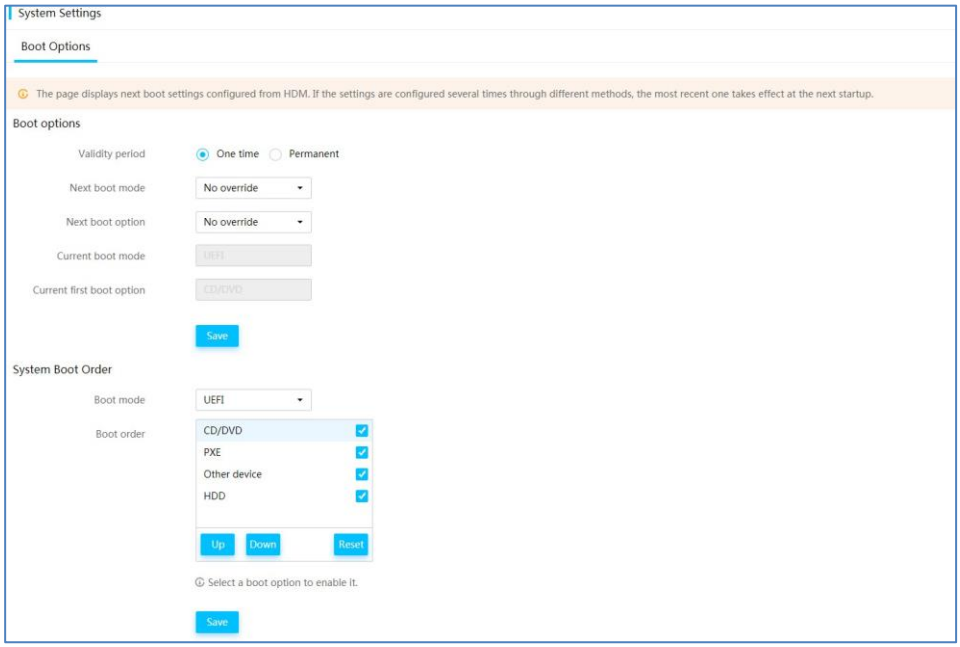
4. **System Boot Options**セクションで、次のブートモードおよびオプションの有効期間を選択します。
   - 次回の再起動時にのみ設定を有効にするには、**One time**を選択します。
   - その後のすべての再起動で設定を有効にするには、**Permanent**を選択します。

     Permanentオプションは、B5700 G3、B5800 G3、B7800 G3、B5700 G5、またはAE100では使用できません。
5. 次のブートモードを選択します。
   - UEFI互換のオペレーティングシステムから起動するには、**UEFI**を選択します。
   - レガシーBIOS互換モードで従来のオペレーティングシステムを起動するには**Legacy BIOS**を選択。

     AE100はレガシーモードをサポートしていない。
   - 次回の再起動時にBIOS設定を使用するには、**No override**を選択します。
6. **Boot option**リストから次のリブートに使用するブートデバイスを選択します。有効期間が**Permanent**の場合、**BIOS**オプションは使用できません。

   次回の再起動時にBIOS設定を使用するには、**No override**を選択します。
7. 保存をクリックします。

図41 次回再起動時のブートオプションの設定

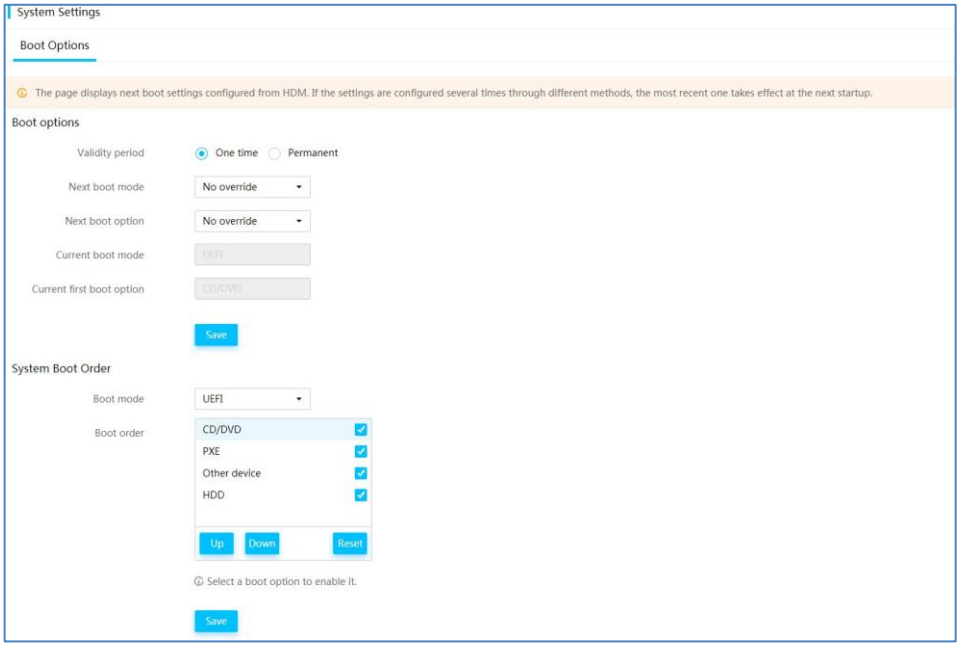


システムブート順序を設定する

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**System Settings**を選択します。
3. **Boot Options**タブをクリックします。
4. **System Boot Order**セクションで、ブートモードを選択します。
   - UEFI互換のオペレーティングシステムから起動するには、**UEFI**を選択します。
   - レガシーBIOS互換モードで従来のオペレーティングシステムを起動するには**Legacy BIOS**を選択。
5. ブートオプションのブート順序を変更するには、オプションを選択し、必要に応じて**Up**または**Down**をクリックします。

   Other deviceオプションには、BIOSで優先順位が定義されている次のブートデバイスが含まれます。
   - 埋め込みUEFIシェル。このオプションは、**EFI Shell Boot**がBIOSで**Enabled**になっている。
   - タイプが識別されていないその他のブートデバイス。
6. デフォルトのブート順序に戻すには、**Reset**をクリックします。
7. **save**をクリックします。

図42 システムブート順序の設定



パラメーター

- **Boot mode**:次の起動時のブートモードを選択します。
- **Boot option**:次回の起動時に使用するブートデバイスを選択します。
- **Current boot mode**:最新の起動のブートモードを表示します。
- **Current first boot option**:最新の起動の最初のブートデバイスを表示します。

パーティショニングモードを切り替える

サーバーのパーティション化モードを設定するには、次の作業を実行します。

単一システムパーティション化モードでは、サーバーは1つのシステムとして動作します。管理モジュール1のみが実行されています。サーバーは、管理モジュール1のHDM、BIOSおよびOSを介して管理できます。

デュアルシステムパーティション化モードでは、サーバーは2つの独立したシステムとして動作します。管理モジュール1と2の両方が実行されています。各システムは、HDM、対応する管理モジュールのBIOSおよびOSを使用して管理できます。このモードにより、サーバーの効率が向上します。

管理モジュールの詳細については、サーバーのユーザーガイドを参照してください。

一般的な制限事項とガイドライン

この機能は、R8900 G3サーバーだけで使用できます。

この機能は、HDM-2.08.00、BIOS-2.00.47、CPLD-V006、PDBCPLD-V005以降でのみ使用できます。

HDM、BIOS、CPLD、およびPDBCPLDバージョンのサーバーがこの機能をサポートしていることを確認します。

デュアルシステムモードでは、最初のシステムを正常に起動またはリブートした後にだけ、2番目のシステムを起動またはリブートできます。

ベストプラクティスとして、テクニカルサポートの指示に従ってこの機能を設定します。

シングルシステムモードからデュアルシステムモードへの切り替え

制限事項とガイドライン

パーティション化モードを切り替える前に、次の要件が満たされていることを確認します。

- サーバーの電源がオフで、HDMが更新されていない。

- HDM、BIOS、およびすべてのCPLDファームウェアは、パーティションモード設定をサポートし、相互に互換性があります。

前提条件

サーバーのすべてのファームウェアがパーティションモード設定をサポートしていない場合は、次の手順を実行してファームウェアを更新します。

1. HDM、BIOS、およびすべてのCPLDファームウェアを、パーティションモード設定をサポートするバージョンにアップデートします。
2. サーバーの電源を切り、管理モジュール1および2の位置を切り替えます。
3. サーバーの電源を入れ、HDM、BIOS、およびすべてのCPLDファームウェアをパーティションモード設定をサポートするバージョンに再度更新します。

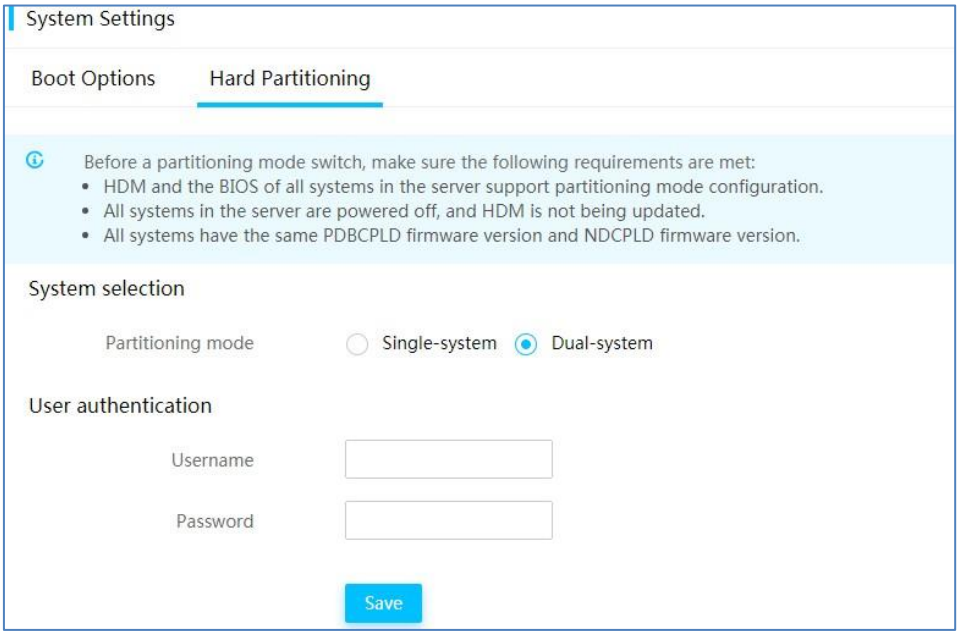
手順

1. 上部のナビゲーションバーで、**system**をクリックします。
2. 左側のナビゲーションペインで、**System Settings**を選択します。
3. **Hard Partitioning**タブをクリックします。
4. デュアルシステムモードを選択します。
5. ユーザーカウントのユーザー名とパスワードを入力します。

   ユーザーカウントに、管理者またはオペレータの役割またはリモート制御権限があることを確認します。
6. **save**をクリックします。

   パーティショニングモードの設定を有効にするには、電源を再接続してサーバーを再起動します。

図43 シングルシステムモードからデュアルシステムモードへの切り替え



パーティショニングモードの切り替え後にHDMにサインインする

シングルシステムモードからデュアルシステムモードに切り替えた後は、両方の管理モジュール1と2が実行されています。スイッチは、サーバー上の両方のシステムのHDMとBIOSをデフォルト設定に戻します。

パーティショニングモードの切り替え後にサーバーのシステムのHDMにサインインするには、次の手順を実行します。

1. HDMの管理IPアドレスを取得します。
   - HDM専用ネットワークポートが接続されている場合は、HDM専用ネットワークポートのデフォルトの管理IPアドレス(192.168.1.2/24)を使用します。
   - HDM共有ネットワークポートが接続されている場合、HDM共有ネットワークポートの管理IPアドレスを取得する方法はシステムによって異なります。
     - 下位パーティションのシステムでは、IPアドレスはDHCPサーバーによって自動的に割り当てられます。

IPアドレスはBIOSのPOST画面から取得できます。

- 上位パーティションのシステムでは、IPアドレスがスイッチの前に自動的に割り当てられた場合、IPアドレスはスイッチの後も同じままです。IPアドレスがスイッチの前に静的IPアドレスであった場合、新しいIPアドレスはDHCPサーバーによって自動的に割り当てられます。新しいIPアドレスは、BIOSのPOST画面から取得できます。

2. 各システムのHDMサインインページで、デフォルトのユーザー名(admin)とパスワード(Password@_)を入力します。パスワードは大文字と小文字が区別されます。

デュアルシステムモードからシングルシステムモードに切り替えます。

制限事項とガイドライン

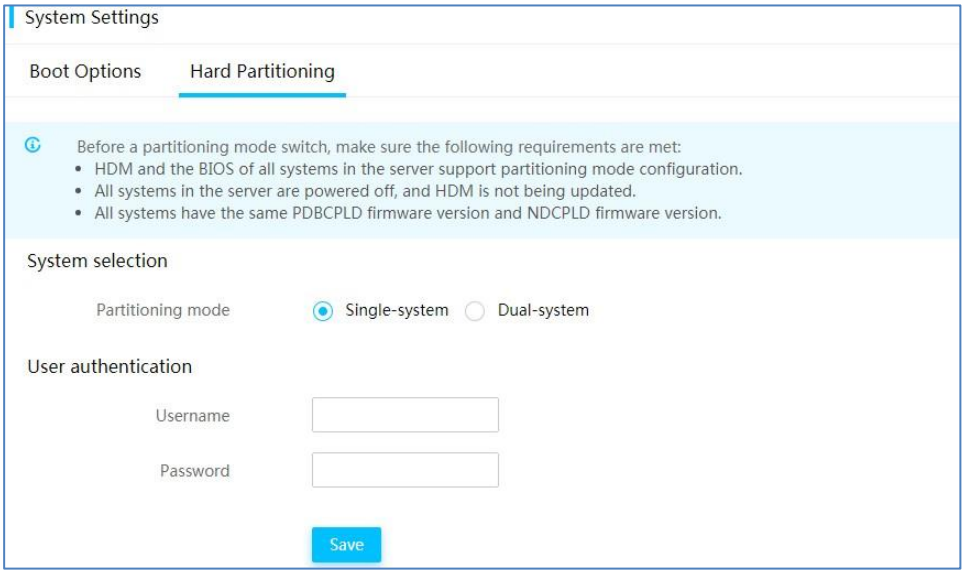
パーティション化モードを切り替える前に、次の要件が満たされていることを確認します。

- すべてのシステムの電源がオフになり、HDMは更新されていません。
- すべてのシステムに同じPDBCPLDファームウェアバージョンとNDCPLDファームウェアバージョンがあります。
- HDMおよびすべてのシステムのBIOSは、パーティション化モードの設定をサポートしています。
- パーティショニングモードの切り替えは、管理モジュール1のHDMからのみ実行できます。

手順

1. 管理モジュール1のHDMにログインします。
2. 上部のナビゲーションバーで、**system**をクリックします。
3. 左側のナビゲーションペインで、**System Settings**を選択します。
4. **Hard Partitioning**タブをクリックします。
5. シングルシステムモードを選択します。
6. ユーザーカウントのユーザー名とパスワードを入力します。
   ユーザーカウントに、管理者またはオペレータの役割またはリモート制御権限があることを確認します。
7. **save**をクリックします。
   パーティショニングモードの設定を有効にするには、電源を再接続してサーバーを再起動します。

図44 デュアルシステムモードからシングルシステムモードへの切り替え



パーティショニングモードの切り替え後にHDMにサインインする

デュアルシステムモードからシングルシステムモードに切り替えた後は、管理モジュール1だけが動作しています。スイッチはHDMとBIOSをデフォルト設定に戻します。

パーティション化モードの切り替え後にHDMにサインインするには、次の手順を実行します。

1. 管理モジュール1のHDMの管理IPアドレスを取得します。
   - HDM専用ネットワークポートが接続されている場合は、HDM専用ネットワークポートのデフォルトの

管理IPアドレス(192.168.1.2/24)を使用します。

- HDM共有ネットワークポートが接続されている場合、HDM共有ネットワークポートの管理IPアドレスを取得する方法は、スイッチ前のIPアドレス取得方法によって異なります。
  - IPアドレスがスイッチの前にDHCPサーバーによって自動的に割り当てられた場合、IPアドレスはスイッチの後に残ります。
  - スイッチの前にIPアドレスが静的IPアドレスであった場合は、新しいIPアドレスがDHCPサーバーによって自動的に割り当てられます。新しいIPアドレスは、BIOSのPOST画面から取得できます。

2. HDMサインインページで、デフォルトのユーザー名(admin)とパスワード(Password@_)を入力します。パスワードは大文字と小文字が区別されます。

構成

ネットワーク

重要:

HDM専用ネットワークポートは、AE100またはブレードサーバーでは使用できません。

HDM専用ネットワークポートまたはHDM共有ネットワークポートからHDMにログインできます。

専用ネットワークポートは、HDM管理トラフィックだけを処理できます。デフォルトでは、専用ネットワークポートはIPv4アドレス192.168.1.2/24を使用し、DHCPサーバーからIPv6アドレスを取得します。

共有ネットワークポートは、HDM管理トラフィックとサーバーデータトラフィックを同時に送信します。デフォルトでは、共有ネットワークポートは自動的にDHCPを介してIPアドレスを取得します。

ネットワーク構成に関する一般的な制限事項およびガイドライン

HDMに正常にアクセスできるようにするには、ネットワーク設定を設定するときに次の制約事項および注意事項に従ってください。

- HDM専用ネットワークポートと共有ネットワークポートが通常モードの場合は、専用ポート、共有ポート、およびWLANが異なるサブネットから異なるIPアドレスを使用していることを確認します。違反が発生すると、ネットワーク障害が発生する可能性があります。
- HDM専用ネットワークポートと共有ネットワークポートを同時に無効にしないでください。両方のネットワークポートが無効になっていると、HDM Webインターフェースにアクセスできなくなります。
- ネットワーク設定を変更すると、HDMユーザーセッションが切断され、有効になるまで数分かかる場合があります。ネットワーク設定を変更したら、プロンプトでHDM Webインターフェースに再接続します。

HDMのIPv6アドレスにログインできない場合は、ブラウザーでプロキシサーバーを無効にしてから再試行してください。

DHCPサーバーによって割り当てられた、またはステートレス自動設定によって設定されたIPアドレスは、64ビットプレフィクスだけをサポートします。

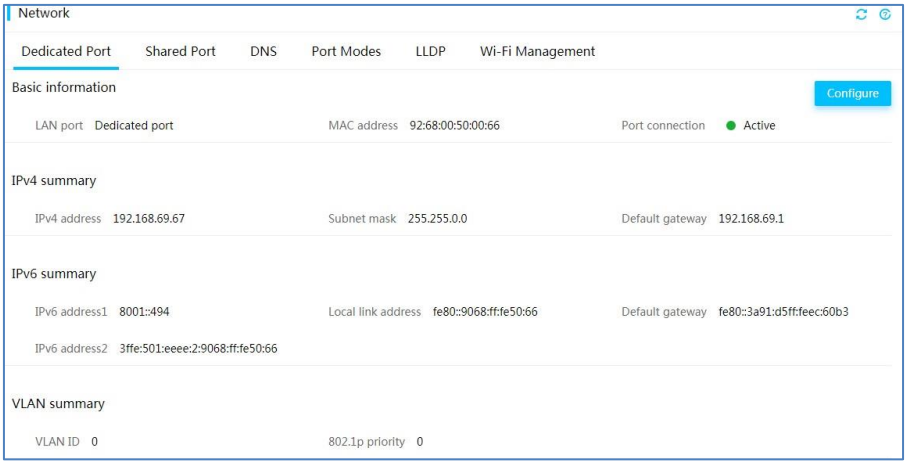
専用ネットワークポート情報を表示する

専用ネットワークポートに関する情報(ポート名、MACアドレス、IPアドレス、VLAN設定など)を表示するには、次の作業を実行します。

手順

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. Dedicated Portタブで、専用ネットワークポートに関する情報を表示します。

図45 専用ネットワークポートに関する情報の表示



パラメーター

- **Port state**:このフィールドは、ネットワークポートモードがアクティブ/スタンバイの場合にだけ使用できます。次のオプションがあります。
  - **Active**:ポートは接続されており、アクティブな状態です。
  - **Disconnected**:ポートは接続解除されています。
- ポート接続:ケーブルがポートに接続されているかどうかを表示します。次のオプションがあります。
  - **Disconnected**:ポートは接続解除されています。
  - **Active**:ポートは接続されており、アクティブステートです。

専用ネットワークポートを設定する

制限事項とガイドライン

「ネットワーク構成の一般的な制限とガイドライン」を参照してください。

ネットワークポートモードがアクティブ/スタンバイの場合、専用ネットワークポート上の任意のIP設定が共有ネットワークポートに同期されます。

前提条件

専用ネットワークポートがネットワークに物理的に接続されていることを確認します。

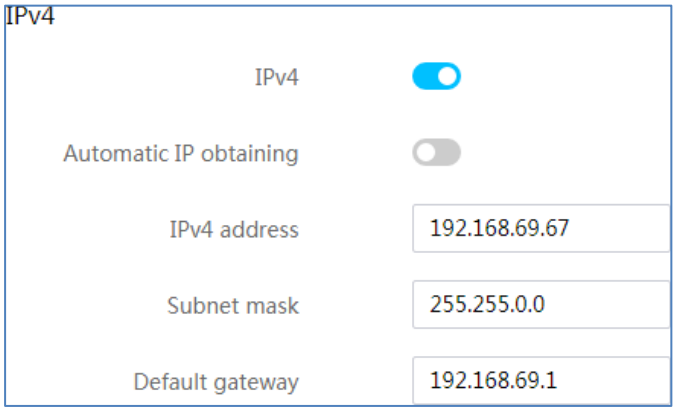
ネットワークポートモードがアクティブ/スタンバイの場合は、専用ネットワークポートがアクティブ状態であることを確認します。

IPv4設定を構成する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Dedicated Port**タブで、Configureをクリックします。
3. **Enable for IPv4**を選択して、IPv4ネットワークサービスを有効にします。
4. ポートのIPv4アドレスを設定します。
   - DHCPサーバーによって自動的に割り当てられたIPアドレスを使用するには、**Automatic IP obtaining**を選択します。
   - 静的IPアドレスを手動で構成するには、自動IP取得をオフにし、IPv4アドレス、サブネットマスク、およびデフォルトゲートウェイアドレスを入力します。

     HDM専用ネットワークポートのデフォルトIPアドレスは192.168.1.2/24です。ゲートウェイアドレスが**0.0.0.0**の場合、デフォルトゲートウェイが指定されていないことを示します。
5. **save**をクリックします。

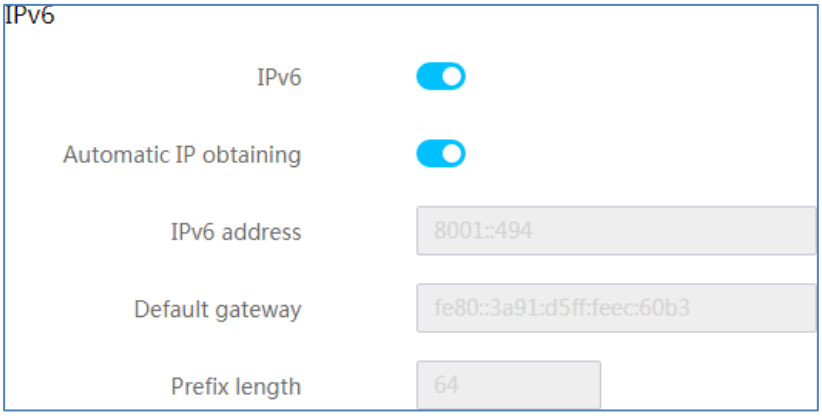
図46 IPv4設定の構成



IPv6設定を構成する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Dedicated Port**タブで、**Configure**をクリックします。
3. **Enable for IPv6**を選択して、IPv6ネットワークサービスを有効にします。
4. ポートのIPv6アドレスを設定します。
   - DHCPサーバーによって自動的に割り当てられたIPアドレスを使用するには、**Automatic IP obtaining**を選択します。
   - スタティックIPアドレスを手動で設定するには、**Automatic IP obtaining**をオフにし、IPv6アドレス、プレフィクス長(1～127の範囲)、およびデフォルトゲートウェイアドレス**fe80::9628:2 eff:fe9c:ffda**を入力します。
5. **save**をクリックします。

図47 IPv6設定の構成

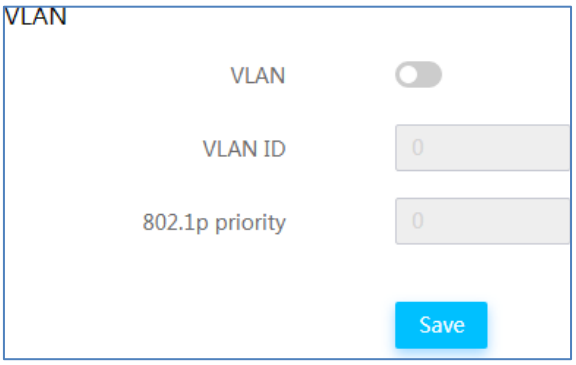


VLAN設定の構成

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Dedicated Port**タブで、**Configure**をクリックします。
3. **Enable for VLAN**を選択して、VLANサービスをイネーブルにします。
4. VLAN IDを2～4094の範囲で入力します。
5. 802.1pプライオリティを0～7の範囲で入力します。

   802.1pプライオリティは、輻輳が発生したときのVLANからのトラフィックの送信プライオリティを決定します。値が大きいほど、プライオリティが高くなります。
6. **save**をクリックします。

図48 VLAN設定の構成



共有ネットワークポート情報を表示する

次のタスクを実行できます。

- Network Controller Sideband Interface(NCDI)を有効または無効にします。
- 共有ネットワークポートに関する情報(ポート名、MACアドレス、IPアドレス、VLAN設定、NPSIが有効な場合のポート接続状態など)を表示します。

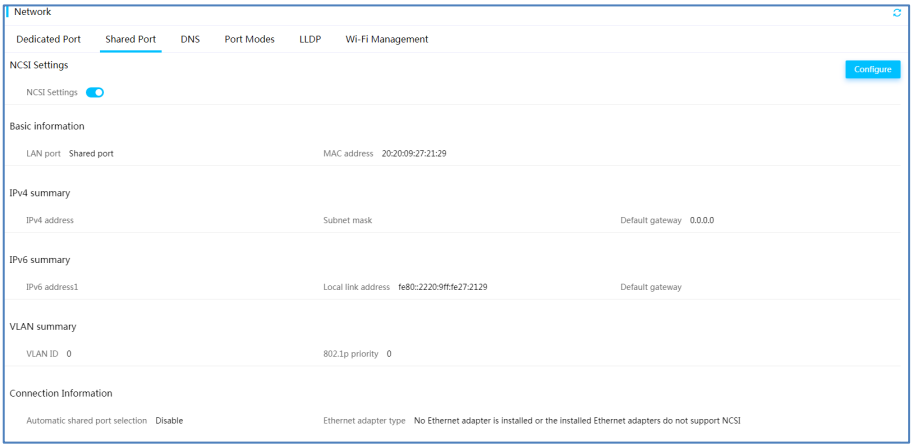
手順

1. 上部のナビゲーションバーで、**Configuration**.をクリックします。**Network**ページが表示されます。
2. **Shared Port**タブをクリックします。
3. 必要に応じてNSCIを有効または無効にし、表示されたダイアログボックスで**OK**をクリックします。

   設定を有効にするためにHDMが再起動し、現在のセッションが切断されます。

   - NPSIをイネーブルにした場合は、HDMに再ログインして共有ネットワークポートに関する情報を表示したり、共有ネットワークポートを設定したりできます。
   - NSCIを無効にした場合、共有ネットワークポートにはアクセスできません。

図49 共有ネットワークポートに関する情報の表示



パラメーター

- **Port state**:このフィールドは、ネットワークポートモードがアクティブ/スタンバイの場合にだけ使用できます。次のオプションがあります。
  - **Active**:ポートは接続されており、アクティブな状態です。
  - **Disconnected**:ポートは接続解除されています。
  - **Standby**:ポートは接続されており、スタンバイ状態です。
- **Connection Information** : 自動共有ポート選択状態、ネットワークアダプタータイプおよびネットワークポート

接続状態など、共有ネットワークポートに関する接続情報を表示します。このフィールドは、ネットワークアダプターがインストールされていない場合、またはインストールされたネットワークアダプターがNSCIをサポートしていない場合には使用できません。次のオプションがあります。

- **Disconnected**:ポートは接続解除されています。
- **Connected:**ポートは接続されていますが、アクティブステートではありません。
- **Active**:ポートは接続されており、アクティブステートです。

共有ネットワークポートを構成する

共有ネットワークポートのIPv4アドレス、IPv6アドレス、およびVLAN設定を設定したり、共有ネットワークポートを変更したり、NSCIがイネーブルになっているときに自動共有ポート選択をイネーブルにしたりするには、次の作業を実行します。

ポートを共有ネットワークポートとして指定するか、システムが自動的にポートを選択できるように、自動共有ポート選択を有効にできます。

共有ネットワークポートの変更では、ポートのネットワーク設定を再構成する必要はありません。DHCPを通じて取得されたIPアドレスを除くすべてのネットワーク設定は、変更後も引き続き有効になります。HDM共有ポートのIPアドレスがDHCPを通じて取得された場合、DHCPサーバーは変更後に共有ネットワークポートにIPアドレスを再割り当てします。

制限事項とガイドライン

「ネットワーク構成の一般的な制限とガイドライン」を参照してください。

AEモジュールおよびブレードサーバーは、VLAN設定または共有ネットワークポートの変更をサポートしません。

ネットワークポートモードがアクティブ/スタンバイの場合、共有ネットワークポート上のIP設定はすべて、他の共有ネットワークポートおよび専用ネットワークポートに同期されます。

自動共有ポート選択をディセーブルにし、共有ポートとしてインターフェースを指定しない場合、システムは機能をイネーブルにする前に指定された共有ポートを使用します。ポートがアップ状態であることを確認します。ポートがダウン状態である場合、HDMはアクセスできません。

ネットワークエラーを回避するには、自動共有ポート選択とアクティブ/スタンバイモードの両方をイネーブルにしないでください。

すべてのsLOM、mLOM、FLOM、およびOCPネットワークアダプター、およびNPSI対応のPCIeネットワークアダプターは、自動共有ポート選択をサポートします。

ネットワークポート選択およびネットワークポートモードを編集するために設定ファイルをインポートする前に、ファイルの内容が完全で正しいことを確認してください。

前提条件

共有ネットワークポートがネットワークに物理的に接続されていることを確認します。

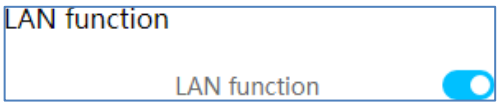
ネットワークポートモードがアクティブ/スタンバイの場合は、共有ネットワークポートがアクティブ状態であることを確認します。

共有ネットワークポートを手動で変更する前に、共有ネットワークポートとして使用するネットワークインターフェースがアップ状態であることを確認します。

LAN機能を有効にする

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Shared Port**タブをクリックします。
3. **Configure**をクリックします。
4. LAN機能を有効にし、**save**をクリックします。

図50 LAN機能の有効化

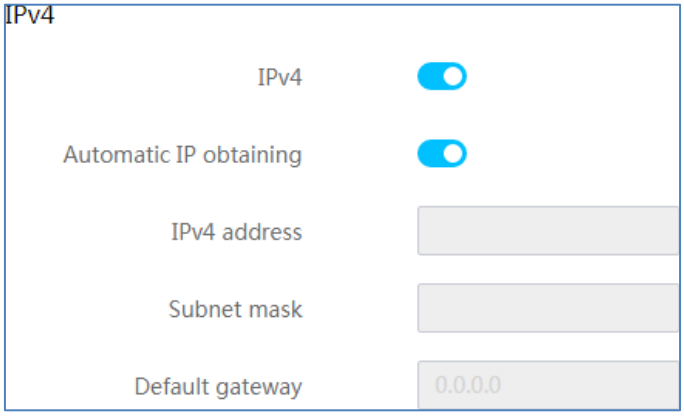


IPv4設定を構成する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**network**ページが表示されます。
2. Shared Portタブをクリックします。
3. **Configure**をクリックします。
4. **Enable for IPv4**を選択して、IPv4ネットワークサービスを有効にします。
5. ポートのIPv4アドレスを設定します。
   - DHCPサーバーによって自動的に割り当てられたIPアドレスを使用するには、**Automatic IP obtaining**を選択します。これはデフォルト設定です。
   - 静的IPアドレスを手動で構成するには、**Automatic IP obtaining**をオフにし、IPv4アドレス、サブネットマスク、およびデフォルトゲートウェイアドレスを入力します。

     0.0.0.0のゲートウェイは、デフォルトゲートウェイが指定されていないことを示します。
6. **save**をクリックします。

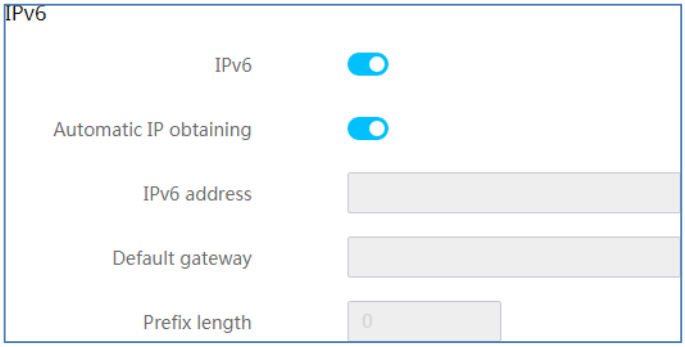
図51 IPv4設定の構成



IPv6設定を構成する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Shared Port**タブをクリックします。
3. **Configure**をクリックします。
4. **Enable for IPv6**を選択して、IPv6ネットワークサービスを有効にします。
5. ポートのIPv6アドレスを設定します。
   - DHCPサーバーによって自動的に割り当てられたIPアドレスを使用するには、**Automatic IP obtaining**を選択します。
   - スタティックIPアドレスを手動で設定するには、**Automatic IP obtaining**をオフにし、IPv6アドレス、プレフィクス長(1～127の範囲)、およびデフォルトゲートウェイアドレス**fe80::9628:2 eff:fe9c:ffda**を入力します。
6. **save**をクリックします。

図52 IPv6設定の構成

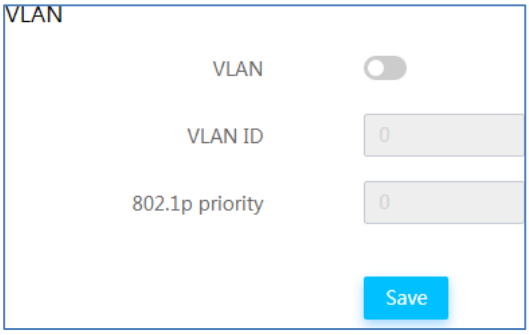


VLAN設定の構成

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Shared Port**タブをクリックします。
3. **Configure**をクリックします。
4. **Enable for VLAN**を選択して、VLANサービスをイネーブルにします。
5. VLAN IDを2～4094の範囲で入力します。
6. 802.1pプライオリティを0～7の範囲で入力します。

   802.1pプライオリティは、輻輳が発生したときのVLANからのトラフィックの送信プライオリティを決定します。値が大きいほど、プライオリティが高くなります。
7. **save**をクリックします。

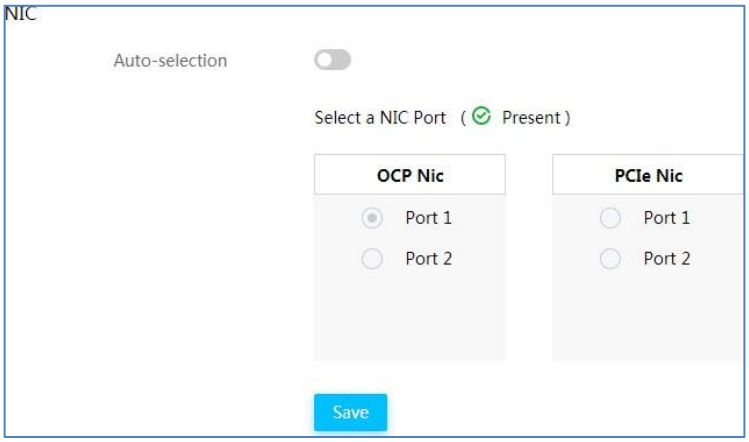
図53 VLAN設定の構成



共有ポートの自動選択を有効にする

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. 図49に示すように、Shared Portタブをクリックします。
3. **Configure**をクリックします。
4. **Enable for Auto-selection**を選択します。
5. **save**をクリックします。

図54共有ポートの自動選択の有効化



共有ポートを手動で指定する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Shared Port**タブをクリックします。
3. **Configure**をクリックします。
4. 図54に示すように、共有ネットワークポートとしてポートを指定します。
5. **save**をクリックします。

DNSの構成

HDMの管理IPアドレスの代わりにドメイン名を使用してHDMへのアクセスをイネーブルにするには、DNSを設定します。

制限事項とガイドライン

すべてのネットワークポートが静的IPアドレスを使用する場合は、DNSサーバーのIPアドレスを手動で指定します。

DNSサーバーのIPv6アドレスを手動で指定する場合は、グローバルIPv6アドレスを指定します。

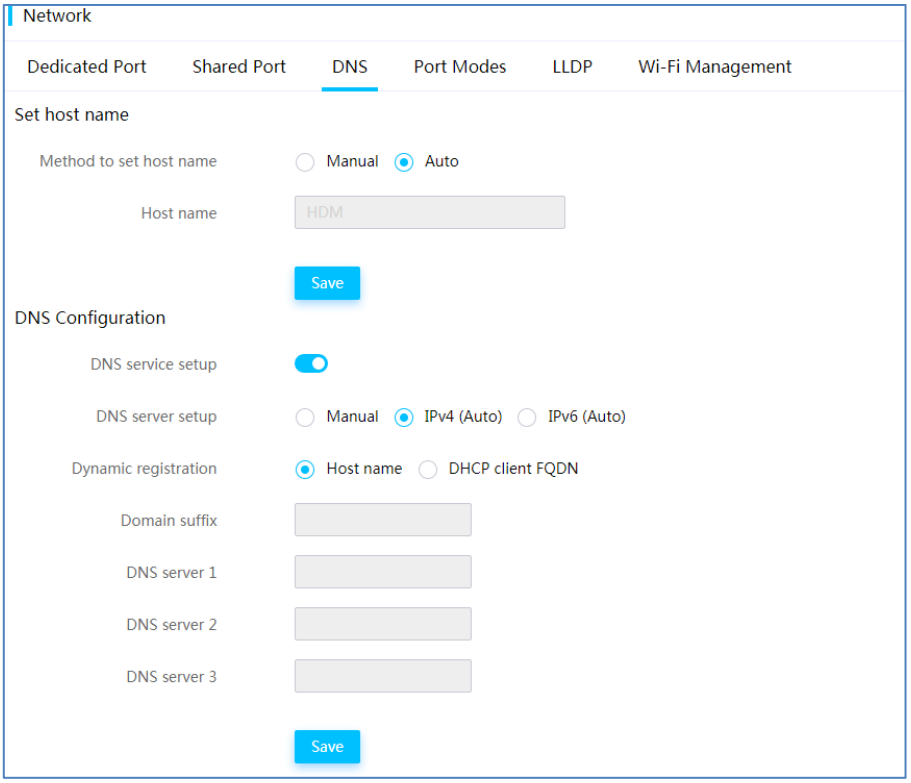
HDMのホスト名を設定する

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **DNS**タブをクリックします。
3. Set host name領域で、次のいずれかの方法を使用して、HDMのホスト名を設定します。
   - ホスト名を手動で構成するには、**Manual**を選択し、**Host name**フィールドにホスト名を入力します。

     ホスト名は1～48文字の文字列です。ハイフン(-)は使用できます。ただし、ハイフン(-)で開始または終了することはできません。
   - HDMがホスト名を自動的に設定できるようにするには、**Auto**を選択します。

     Host nameフィールドには、HDMとサーバーのシリアル番号を組み合わせたホスト名が自動的に入力されます。
4. 保存をクリックします。

図55 ホスト名の設定



DNSサービスを構成する

ドメインサフィックスを指定し、DNSサーバーのIPアドレスを指定するには、次のタスクを実行します。ドメインサフィックスを使用して、最上位および第2レベルのドメインを指定します。このドメインサフィックスは、HDMホスト名と自動的に結合され、HDMアクセス用の完全修飾ドメイン名が形成されます。

DNSサービスを設定するには、次の手順を実行します。

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **DNS**タブをクリックします。
3. **Configure DNS service**領域で、図55に示すように、**Enable for DNS service**を選択します。
4. **DNS server setup**フィールドで、**Manual**、**IPv4(Auto)**、または**IPv6(Auto)**を選択します。
   - **Manual**を選択した場合は、**Domain suffix**フィールドにドメインサフィックスを入力し、DNSサーバーのIPアドレスを入力します。**Domain suffix**フィールドはオプションです。

     最大3つのDNSサーバーを指定できます。DNSサーバー1、2、および3の優先順位は降順です。
   - **IPv4(auto)**または**IPv6(auto)**を選択した場合は、**Dynamic registration**フィールドから**Host name**または**DHCP Client FQDN**を選択し、登録情報を取得するネットワークポートを選択します。**Domain suffix**フィールドには自動的に値が入力され、HDMはDNSサーバーを自動的に検索します。

     Obtain registration info viaフィールドは、専用ネットワークポートと共有ネットワークポートの両方が、DHCPサーバーによって割り当てられたIPアドレスを使用している場合にだけ使用できます。
5. **save**をクリックします。

ネットワークポートモードを設定する

重要:

ネットワークポートモードは、AEモジュールまたはブレードサーバーでは使用できません。

HDMは、次のネットワークポートモードをサポートします。

- **Normal mode**:HDM専用および共有ネットワークポートは個別のIPアドレスを持ち、アクティブ/アクティブモードで動作します。HDMは両方のポートでアクセスできます。これはデフォルトモードです。
- **Bonding mode**:HDM専用および共有ネットワークポートは、論理結合ポートに集約されます。論理結合ポートは、専用ポートのIPアドレスとMACアドレスを使用します。HDMユーザーは、専用または共有ネットワークポートが稼動している限り、結合ポートを介してHDMにアクセスできます。
- **Active/standby mode**:HDM専用および共有ネットワークポートは、個別のIPアドレスを持ち、アクティブ/スタンバイモードで動作します。このモードでは、専用ポートがプライマリポートであり、共有ネットワークがセカンダリポートです。HDMは、専用ポートがアップしており、ネットワーク接続が確立されている限り、専用ポートからアクセスできます。専用ポートに障害が発生すると、HDMは共有ポートからアクセスできます。スタンバイモードでは、共有ポートは管理トラフィックを転送できませんが、データトラフィックは転送できます。

Bonding modeでは、VLAN設定はボンドポートでのみ構成可能です。専用ネットワークポートと共有ネットワークポートのVLAN設定はありません。

通常モードとアクティブ/スタンバイモードでは、2つのポートを異なるVLANに割り当てることができます。

制限事項とガイドライン

アクティブ/スタンバイモードをイネーブルにする前にボンディングモードがディセーブルになっていることを確認するか、またはネットワークポートボンディングをイネーブルにする前にアクティブ/スタンバイモードがディセーブルになっていることを確認します。2つのモードを同時にイネーブルにすることはできません。

ネットワークエラーを回避するには、自動共有ポート選択とアクティブ/スタンバイモードの両方をイネーブルにしないでください。

ネットワークポート選択およびネットワークポートモードを編集するために設定ファイルをインポートする前に、ファイルの内容が完全で正しいことを確認してください。

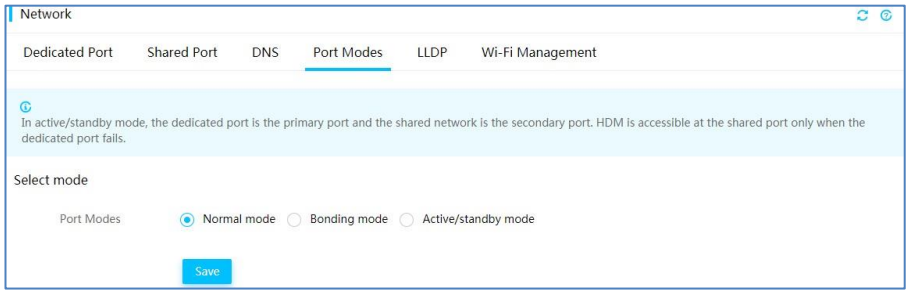
前提条件

- HDM専用および共有ネットワークポートにIPアドレスを割り当てるには、次のいずれかの方法を使用します。
  - ネットワークポートに手動でIPアドレスを割り当てます。ベストプラクティスとして、同じサブネット内のアドレスを使用します。異なるサブネット内のIPアドレスを使用すると、共有ネットワークポートに障害が発生した後にHDMにアクセスできなくなる可能性があります。
  - DHCPを使用して、IPアドレスをネットワークポートに自動的に割り当てます。
- ボンディングモードをイネーブルにする場合は、HDM専用または共有ネットワークポートにVLAN設定が設定されていないことを確認します。

手順

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Port Modes**タブをクリックします。
3. 作業ウィンドウで、ネットワークポートモードを選択します。
4. **save**をクリックします。

図56 ネットワークポートモードの設定



LLDPの設定

Link Layer Discovery Protocol(LLDP)は、異なるベンダーのネットワークデバイスがネイバーを検出し、システムおよび設定情報を交換できるようにする標準のリンク層プロトコルです。

サーバーがLLDPフレームを送信できるようにするには、次の作業を実行します。このページでは、受信したLLDP

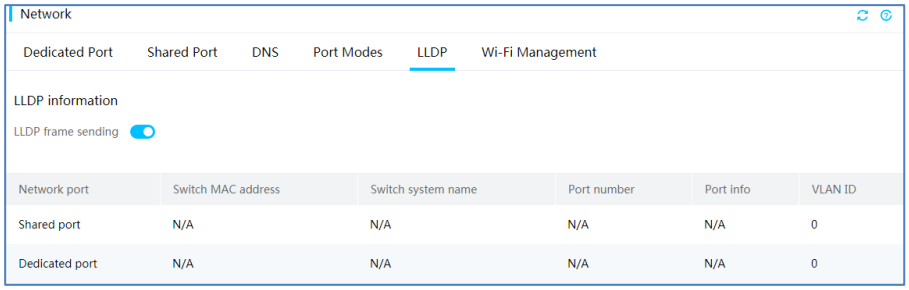
フレームに関する情報も表示できます。

手順

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. LLDPタブをクリックします。
3. **Enable**を選択し、**save**をクリックします。
4. 受信したLLDPフレームに関する情報を表示します。

   リストには、サーバーに接続されているすべてのデバイスに関する情報が表示されます。デバイスが到達不能であるか、またはLLDPフレームの送信をサポートしていない場合、対応するフィールドにはN/Aと表示されます。

   図57 LLDPの設定



パラメーター

- **Network port**:LLDPフレームを受信するサーバーのネットワークポート。
- **Switch MAC address**:接続されているスイッチのMACアドレス。
- **Switch system name**:接続されているスイッチのシステム名。
- **Port number**:接続されているスイッチポートの番号。
- **Port info**:接続されているスイッチポートに関する情報(ポート名など)。
- **VLAN ID**:サーバーポートが属するVLANのID。

Wi-Fi設定を構成する

USB Wi-Fiアダプターをサーバーに接続した後にWi-Fi設定を構成するには、次のタスクを実行します。これにより、ユーザーはワイヤレス接続を介してサーバーにアクセスし、オンラインのワイヤレスクライアントに関する情報を表示できます。

制限事項とガイドライン

この機能は、B5700 G5を除くG5サーバーでのみ使用できます。この機能は、HDM-2.14以降でのみ使用できます。

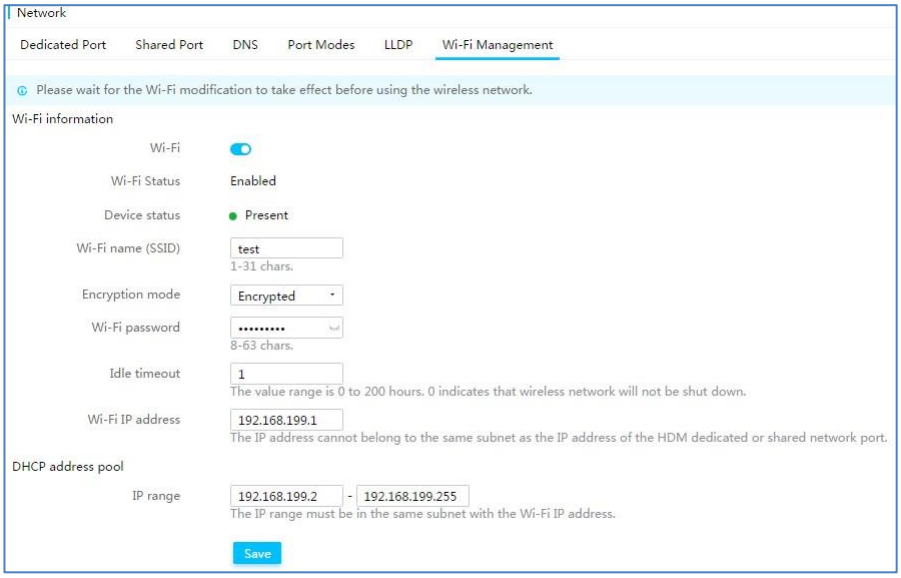
アイドルタイムアウトによってシャットダウンされたネットワークを復元するには、USB Wi-Fiアダプターを再接続するか、HDMにログインしてネットワークを有効にします。

手順

1. 上部のナビゲーションバーで、**Configuration**をクリックします。**Network**ページが表示されます。
2. **Wi-Fi Management** tタブをクリックします。

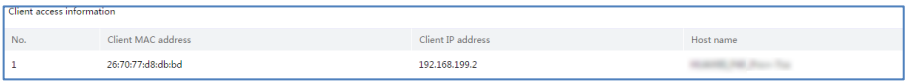
   開いたページには、現在のWi-Fi設定とオンラインワイヤレスクライアントに関する情報が表示されます。
3. 必要に応じてWi-Fi設定を構成します。
   - Wi-Fi名を入力します。
   - 暗号化方式を選択します。**Encrypted**を選択した場合は、Wi-Fiパスワードも指定する必要があります。
   - アイドルタイムアウトを指定します。
   - ワイヤレスネットワークのIPv4アドレスを入力します。
   - クライアントへのIPアドレス割り当てのIPv4アドレス範囲を指定します。
4. 保存をクリックします。

図58 Wi-Fi設定の構成



5. クライアントアクセス情報を表示します。

図59 クライアントアクセス情報の表示



パラメーター

- **Wi-Fi Status**: Wi-Fi機能の有効化ステータス。
- **Device status**:USB Wi-Fiアダプターのプレゼンスステータス。
- **Wi-Fi name (SSID)**: ワイヤレスネットワークの名前。大文字と小文字が区別される1～31文字の文字列です。使用できるのは、文字、数字、ドット(.)、ハイフン(-)およびアンダースコア(_)のみです。このフィールドは必須です。デフォルトでは、名前はデバイスのSNフォーマットのproduct name_last 10文字です。
- **Encryption mode**: ネットワークの暗号化を有効にするかどうか。デフォルトでは、ネットワークは暗号化されません。
- **Wi-Fi password**: ワイヤレスネットワークのパスワード。大文字と小文字が区別される8～63文字の文字列です。英字、数字、スペースおよび特殊文字`~!@#$%^&*()_+-=\{};':,./<>?のみ使用できます。暗号化モードが**Encrypted**の場合、このフィールドは必須です。
- **Idle timeout**: ネットワークがシャットダウンするまでの最大アイドル時間(0～200時間の範囲)。0は、ワイヤレスネットワークがシャットダウンされないことを示します。既定値は1です。オンラインクライアントが存在しない場合、ネットワークはアイドル状態と見なされます。
- **Wi-Fi IP address**: ワイヤレスネットワークのIPアドレス。デフォルトでは、IPアドレスは192.168.199.1です。サブネットマスクは255.255.255.0に固定されています。IPアドレスは、HDM専用または共有ネットワークポートのIPアドレスと同じサブネットに属することはできません。
- **IP range** : オンラインクライアントへのIPアドレス割り当てのIPv4アドレス範囲。IPアドレス範囲がWi-Fi IPアドレスと同じサブネット内にあることを確認します。サブネットマスクは255.255.255.0に固定されています。
- **No**. : オンラインクライアントの数。システムでは、同時に最大2つのクライアントをオンラインにできます。
- **Client MAC address**: オンラインクライアントのMACアドレス。
- **Client IP address**: オンラインクライアントのIPv4アドレス。
- **Host name**: オンラインクライアントのホスト名。

NTP

Network Time Protocol(NTP)は、ネットワーク上のデバイスのシステムクロックを同期化するために使用されるプロトコルです。

この機能を使用して、NTPサーバーから正しいシステム日付と時刻を取得します。

1つのプライマリNTPサーバー、1つのセカンダリNTPサーバーおよび1つのターシャリNTPサーバーを手動で指定できます。時刻をNTPと同期する場合、HDMは最初にプライマリNTPサーバーを使用します。プライマリNTPサーバーが使用できない場合、HDMはセカンダリNTPサーバーを使用します。プライマリサーバーもセカンダリサーバーも使用できない場合、HDMはターシャリNTPサーバーを使用します。

HDMでは、手動で指定したすべてのNTPサーバーが使用できない場合に、DHCPサーバーからNTPサーバー設定を取得するように選択することもできます。DHCPサーバーが使用できない場合、HDMは、最後に成功したNTP時刻同期で取得されたシステムの日付と時刻を使用するか、ローカルシステムの日付と時刻を使用します。

NTP設定の構成

制限事項とガイドライン

NTPサーバーにアクセスできないためにNTPサーバーとの時間同期が失敗した場合、Webインターフェースには、NTPサーバーから日付と時刻を取得できなかったことを示すエラーメッセージが表示されます。NTPサーバーがアクセス可能になった後でNTPサーバーと同期する場合、または新しい時間同期を開始する場合は、Saveを再度クリックする必要があります。HDMは、Saveアクションによってトリガーされないかぎり、時間同期を実行しません。

手順

1. 上部のナビゲーションバーで、**Configuration**をクリックします。
2. 左側のナビゲーションペインで、**NTP**を選択します。
3. 作業ウィンドウで、サーバーのタイムゾーンを選択します。
4. **Use manually specified**で**Enable** 又は **Disable**を選択してから、**DHCP advertised NTP servers**を選択します。
   - この機能を有効にすると、HDMは手動で指定したNTPサーバーと時刻設定を同期します。手動で指定したNTPサーバーが失敗した場合、HDMはDHCPサーバーから取得したNTPサーバーと設定を同期します。これはデフォルト設定です。
   - この機能を無効にすると、HDMは時刻設定をMEと同期します。BIOSがリブートした後、HDMはBIOSの時刻(UTC時刻)と指定された時間帯に基づいて時刻設定の同期を開始します。たとえば、指定された時間帯がUTC+8である場合、HDMはBIOSの時刻より8時間早い時刻を使用します。
5. **Enable for Use manually specified**、そして、**DHCP advertised NTP servers**を選択した場合は、NTP同期間隔の設定、およびプライマリ、セカンダリ、およびターシャリNTPサーバーのアドレスの入力が行われます。

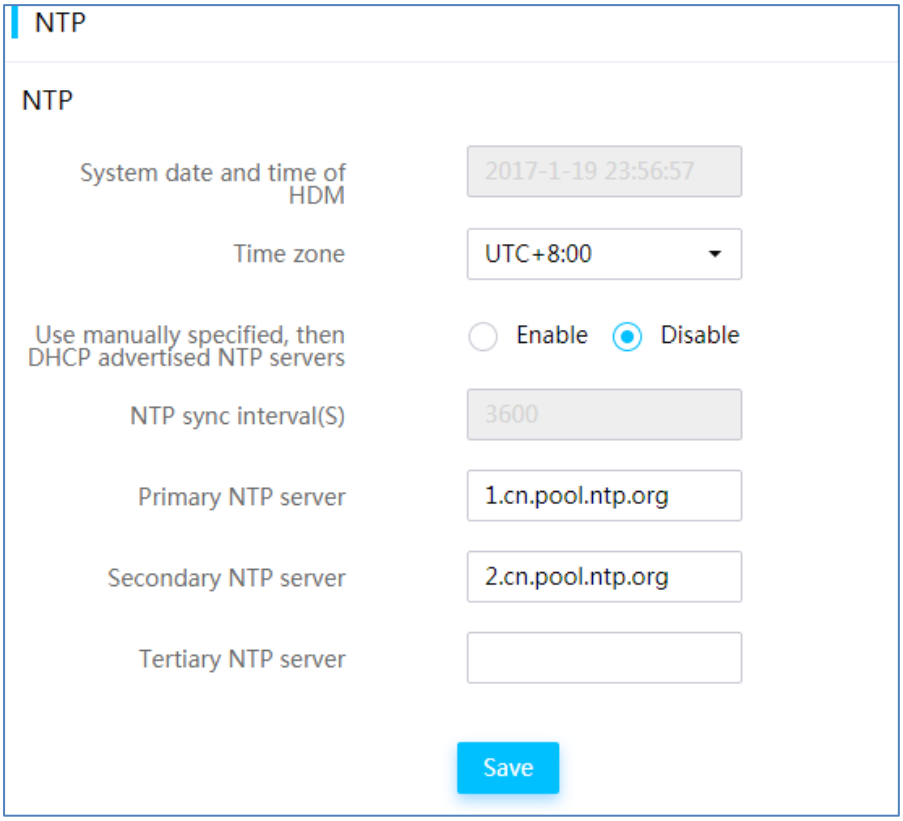
   サーバードレスには、IPv4アドレス、IPv6アドレス、またはドメイン名を指定できます。セカンダリサーバーとターシャリサーバーはオプションです。HDMサーバーはセカンダリNTPサーバーを使用します。

   プライマリNTPサーバーに障害が発生した場合にだけ使用され、セカンダリNTPサーバーとプライマリNTPサーバーの両方に障害が発生した場合にだけターシャリNTPサーバーを使用します。

   デフォルトでは、プライマリNTPサーバードレスは1.cn.pool.ntp.org、セカンダリNTPサーバードレスは2.cn.pool.ntp.orgで、ターシャリサーバードレスは指定されていません。
6. **save**をクリックします。

   HDMは時刻の同期を試みます。

図60 NTP設定の構成



パラメーター

NTP同期間隔:HDMがNTPサーバーからの時間を同期する間隔を設定します。デフォルトでは、間隔は3600秒です。値の範囲は600から2592000秒です。この設定は、NTPが構成されている場合にのみ有効です。

リモートサービスを構成する

アクセスサービス

サービスとユーザーセッションの表示

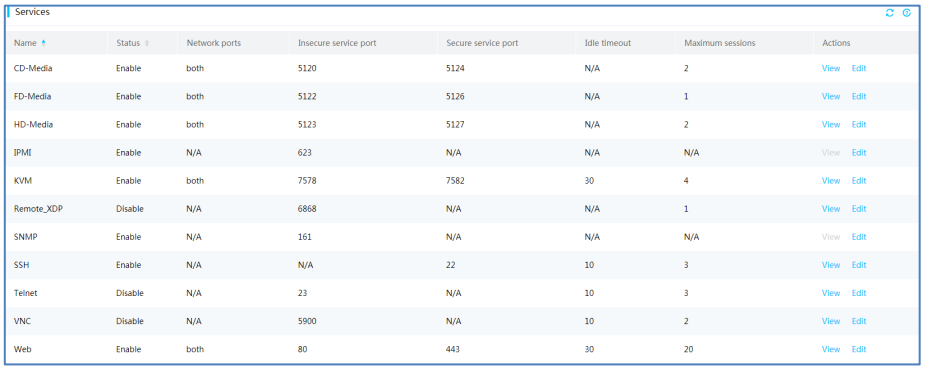
制限事項とガイドライン

利用可能なサービスは、サーバーモデルによって異なります。

手順

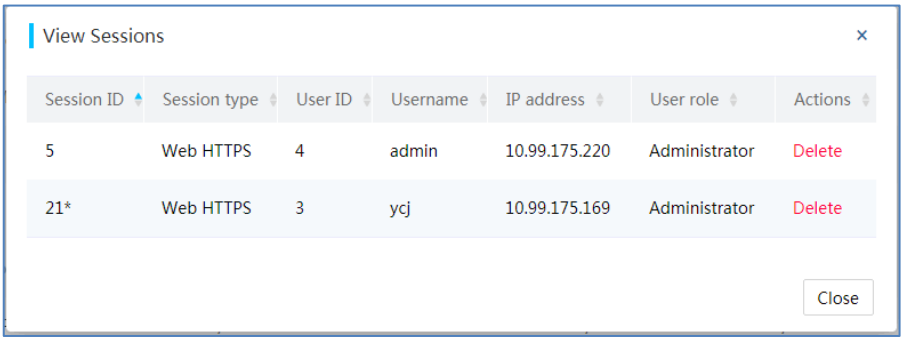
1. ナビゲーションペインで、**Remote Services > Services**を選択します。サービスリストページが開きます。
2. 図61に示すように、作業ウィンドウで**View**をクリックしてアクセスサービスの詳細情報を表示します。

図61 アクセスサービスエントリの表示



3. 開いたセッションリストで、図62に示すように、次のいずれかのタスクを実行します。
   - セッションを閉じるには、セッションの**Delete**をクリックします。
   - 前のページに戻るには、**Close**をクリックします。

図62 アクセスサービスの表示



パラメーター

- **Name**:サービスの名前。

  HDMは次のサービスを提供します。
  - **CD-Media**: 仮想CDおよびDVDへのアクセス。
  - **FD-Media**: 仮想ディスケットドライブへのアクセス。
  - **HD-Media** -仮想ディスクドライブおよびUSBにアクセスできます。
  - **iHDT**: Hardware Debug Tool(HDT)によるデバッグ。このサービスは、R4950 G5およびR5500 G5 AMDサーバーだけで使用できます。
  - **IP MI**: Remote Management Control Protocol(RMCP)またはHDMへのRMCP+接続。
  - **KVM**: リモートコンソールからサーバーにアクセスします。
  - **Remote_XDP**: XDPを介したリモートデバッグおよび診断。このサービスは、R2700 G3、R2900 G3、R4300 G3、R4400 G3、R4700 G3、R4900 G3、R5300 G3、R6700 G3、R4700 G5、R4900 G5、R5300 G5、およびB5700 G5サーバーでのみ使用できます。
  - **SNMP**: HDMへのSNMPアクセス。
  - **SSH**: HDMへのSSHアクセス。
  - **Telnet**: HDMへのTelnetアクセス。
  - **VNC**: Virtual Network Computing(VNC)クライアントからサーバーにアクセスします。
  - **Web**: HDM Webインターフェースへのアクセス。
- **Status**:サービスのステータス。オプションには次のものがあります。
  - **Disabled。**
  - **Enabled。**
- **Network portsト**:サービスに使用できるHDMネットワークポート。

    - **eth0**:共有ポート。
    - **eth1**: HDM専用ポート。
    - **both**:共有ポートとHDM専用ポートの両方。
    - **Bond0**-HDMボンドポート。
- **Insecure service port**:サービスの暗号化されていない通信に使用されるポート。
- **Secure service port**:サービスの暗号化された通信に使用されるポート。
- **Idle timeout**:ユーザーセッションのアイドルタイムアウト時間(分単位)。ユーザーセッションは、タイムアウトになると自動的に切断されます。
- **Maximum sessions**:サービスでサポートされるセッションの最大数。
- **Session ID**:HDMユーザーセッション間のセッションを識別するID。アスタリスク(*)マークは、クライアントが現在のWebインターフェースにアクセスするときに使用するIPアドレスを使用してセッションが確立されたことを示します。
- **Session type**:セッションのプロトコルタイプまたはサービスタイプ。
- **User ID**: Users&Security > User AccountsのユーザーリストにあるユーザーカウントのID page.0は、ユーザーがローカルユーザーでもドメインユーザーでもないことを示します。
- Username:ユーザーカウントのユーザー名。
- I**P address**:サービスを使用しているユーザーのIPアドレス。
- **User role**:ユーザーカウントのユーザーロール。アクセス権限のセットを表します。

アクセスサービスを編集する

制限事項とガイドライン

利用可能なサービスは、サーバーモデルによって異なります。

サービスのデフォルトのセキュアまたはセキュアでないサービスポートを変更する場合は、そのサービスを使用するときに次の注意事項に従ってください。

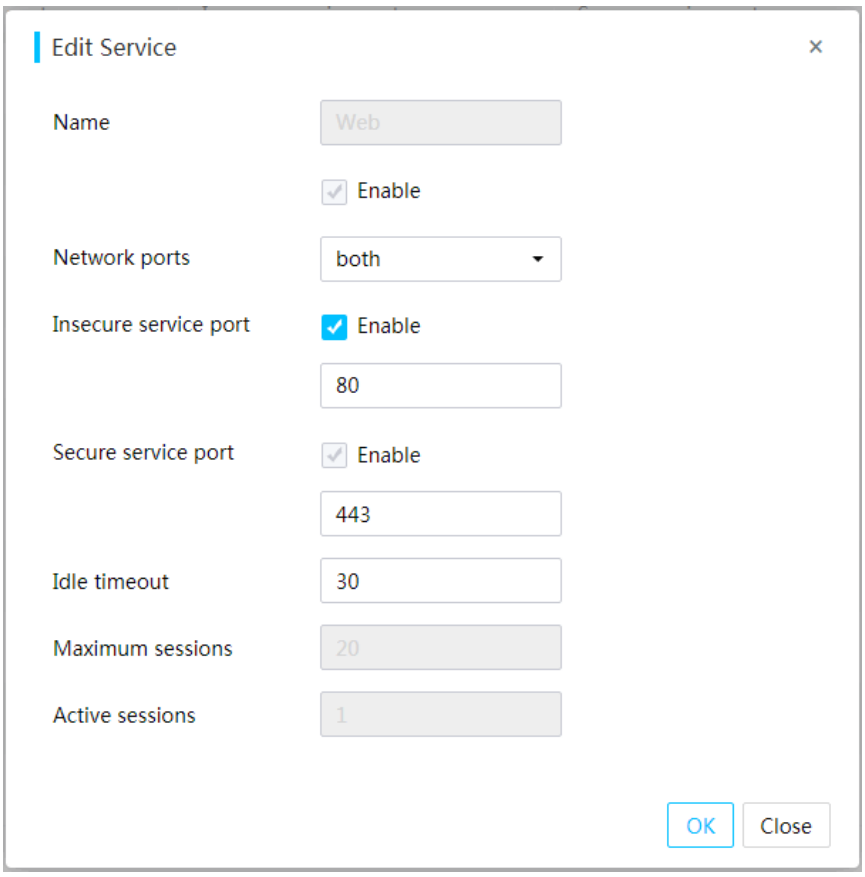
- デフォルトのIPMI非セキュアサービスポート番号(623)を変更する場合は、-p パラメーターを使用して、IPMIコマンドの実行時にポート番号を明示的に指定します。
- デフォルトのセキュアまたは保証Webサービスポート番号を変更する場合は、WebブラウザーからHDMにアクセスするときにWebサービスポートを明示的に指定する必要があります。HDMのURLアドレスフォーマットはhttps://ip_address:secureポートです。
- ユーザーが安全なWebサービスポートからのみHDMにアクセスできるように、安全でないWebサービスポートを使用不可にできます。安全でないWebサービスポートが使用不可になっている場合、H5 KVMに暗号化されていないモードでアクセスすることはできません。
- デフォルトのRemote_XDPサービスポート番号(6868)を変更する場合は、インストールディレクトリ\OpenIPC\Config\SKX\SKX_ASD_JTAG.xmlディレクトリにあるOpenIPCクライアントのポート番号の変更も更新する必要があります。installation directory引数は、OpenIPCクライアントのインストールディレクトリを表します。

サービスの設定を変更すると、サービスが再起動されます。再起動中、サービスは使用できません。iHDTサービスを有効にする前に、サーバーの電源が入ってい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、**Remote Services > Services**を選択します。
2. 作業ウィンドウで、ターゲットサービスの**Edit**をクリックします。
3. 図63に示すように、サービスパラメーターを編集します。

図63 アクセスサービスの編集



4. iHDTサービスを再起動するには、**Restart**をクリックします。
5. **OK**をクリックします。

   サービスが自動的に再起動し、サービスのすべてのアクティブセッションが切断されます。

パラメーター

- **Insecure service port:**サービスの暗号化されていない通信のサービスポート番号を設定します。VNC以外のアクセスサービスの場合、値の範囲は1～65535です。VNCの場合、値の範囲は100～65535です。
- **Secure service port**: サービスの暗号化通信用のサービスポート番号を設定します。値の範囲は1～65535です。

表10サポートされている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-Medis	5120	5124
FD-Media	5122	5126
HD-Media	5123	5127
iHDT	6123	該当なし

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
IPMI	623	該当なし
KVM	7578	7582
Remote_XDP	6868	該当なし
SNMP	161	該当なし
SSH	該当なし	22
Telnet	23	該当なし
VNC	5900	該当なし
Web	80	443

- アイドルタイムアウト:サービスのセッションアイドルタイムアウト時間を設定します。Web、KVM、SSH、TelnetおよびVNCサービスのタイムアウトを設定できます。SSHおよびTelnetサービスでは、同じアイドルタイムアウト時間が使用されます。SSHとTelnetの両方にアイドルタイムアウトを設定すると、最新の構成が有効になります。

表11サービスのタイムアウト値の範囲とデフォルトのタイムアウト設定

サービス名	タイムアウト値の範囲(分単位)	デフォルトのタイムアウト(分単位)
Web	5から30	30
KVM	5から30	30
SSH	1から30	10
Telnet	1から30	10
VNC	5から30	10

リモートコンソール

サーバーを管理し、リモートコンソールからオペレーティングシステム(OS)をインストールできます。

HDMは、最大4つのリモート制御セッションをサポートします。最初のセッションを確立する場合、ユーザーはプライマリユーザーです。後続のリモートコンソールユーザーはすべてセカンダリユーザーであり、プライマリユーザーからアクセス権を取得する必要があります。

HDMは、KVM、H5 KVM、およびVNCリモートコンソールをサポートします。このセクションでは、KVMおよびH5 KVMリモートコンソールの使用方法とVNCログインパスワードの設定方法について説明します。

制限事項とガイドライン

KVMを使用するには、まずOS環境を設定する必要があります。環境設定の構成は、OSのタイプによって異なります。

VNCを使用するには、VNC用のクライアントのインストールが必要です。

KVM用にWindows環境をセットアップする

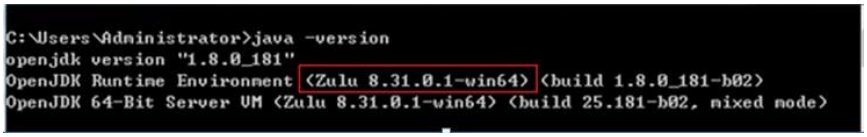
ベストプラクティスとして、Zulu OpenJDK 8およびIceDTea-Web 1.7.1を使用してKVMを実行します。インストールパッケージは、次のWebサイトで入手できます。

- Zulu OpenJDK:https://www.azul.com/downloads/zulu/
- IceDTea-Web:http://icedtea.wildebeest.org/download/icedtea-web-binaries/

KVM用のWindows環境をセットアップするには:

1. 次のように、OpenJDK Java環境をインストールします。
   a. Zulu OpenJDKのmsi.installationファイルを入手し、デフォルト設定でOpenJDKをインストールします。
   b. OpenJDKのバージョンを確認します。

図64 OpenJDKのバージョンの確認



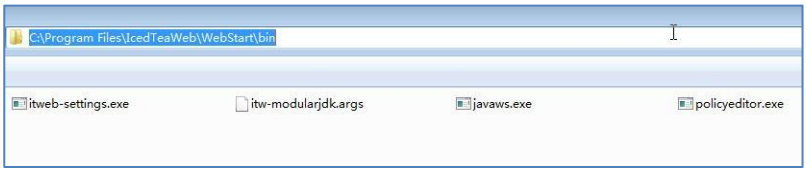
2. IceDTea-Webプラグインをインストールします。

   プラグインのターゲットバージョンの.msiインストールファイルを開き、デフォルト設定でプラグインをインストールします。

3. HDM KVMを実行する:

   a. IceDTea-Webプラグインのインストールディレクトリにアクセスします。この例では、ディレクトリを使用します。
   C:\Program Files\IcedTeaWeb\WebStart\bin.

   図65 IceDTea-Webプラグインのインストールディレクトリへのアクセス



   b. ディレクトリでCLIを開き、javaws jnlp_directoryコマンドを実行します。jnlp_directory引数は、ダウンロードされた.jnlpファイルのディレクトリを表します。この例では、ディレクトリはC:\Temp\KUM<31>.jnlpです。

   図66 コマンドの実行

   c. 表示されたダイアログボックスで、実行をクリックします。

   図67 コマンドの実行

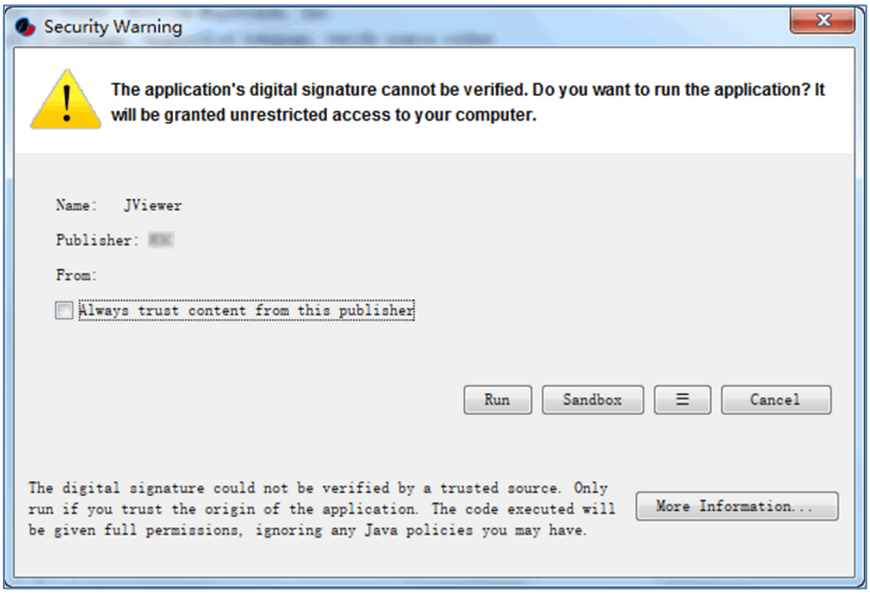
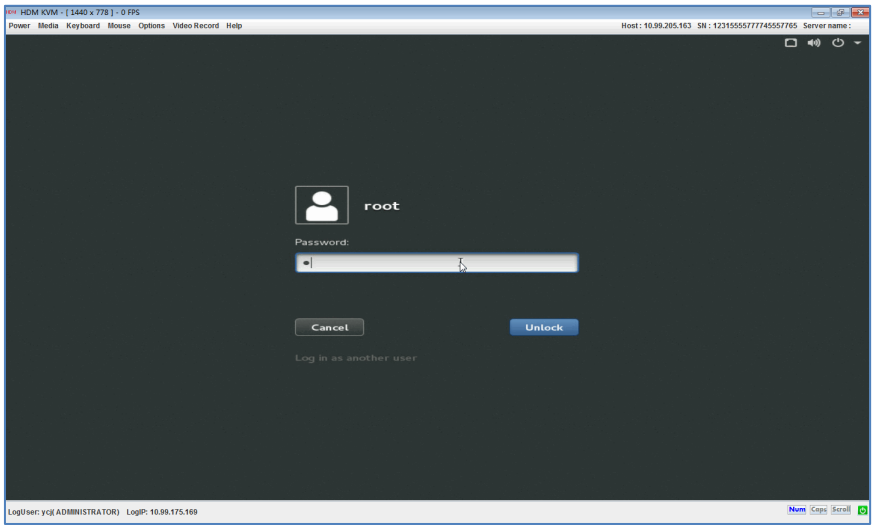


   図68に示すように、KVMログインウィンドウが開きます。KVMにアクセスするためのパスワードを入力できます。

図68 KVMリモートコンソールへの接続



Linux環境をセットアップする

ベストプラクティスとして、Zulu OpenJDK 8およびIceDTea-Webを使用してHDM KVMを実行してください。インストールパッケージは、次のWebサイトで入手できます。

- Zulu OpenJDK:https://www.azul.com/downloads/zulu/
- IceDTea-Web:http://icedtea.wildebeest.org/download/source/KVM用のLinux環境をセットアップするには:

1. IceDTea-Webプラグインをインストールします。

   yum install filenameコマンドを使用して、プラグインをインストールします。filename引数は、インストールパッケージの名前を表します。この例では、パッケージ名はicedtea-web.x86_64です。

   図69 IceDTea-Webプラグインのインストール

   ```
   [root@jys1235 ~]# yum install icedtea-web.x86_64
   ```

2. 次のように、OpenJDK Java環境をインストールします。

   a. OpenJDKをインストールするには、次のいずれかの方法を使用します。

   - rpmインストールパッケージをダウンロードした場合は、rpm-ivh xxx.rpmを実行します。コマンド。xxx.rpm引数はパッケージ名を表します。
   - tar.gzパッケージをダウンロードした場合は、パッケージを/usr/lib/jvmディレクトリに解凍し、次のコマンドを/etc/profileファイルの末尾に追加します。

     ```
     export JAVA_HOME=/usr/lib/jvm/zulu8.31.0.1-jdk8.0.181-linux_x64
     export PATH=$JAVA_HOME/bin:$PATH
     export CLASSPATH=.:$JAVA_HOME/lib/dt.jar:$JAVA_HOME/lib/tools.jar
     ```

   注:

   コマンド行は、Linuxのバージョンによって異なる場合があります。必要に応じて、コマンドのパラメーターを置き換えてください。

   b. OpenJDK 8がインストールされていることを確認します。

   図70 OpenJDKのバージョンの確認

   ```
   [root@jys1235 jvm]# java -version
   openjdk version "1.8.0_181"
   OpenJDK Runtime Environment (Zulu 8.31.0.1-linux64) (build 1.8.0_181-b02)
   OpenJDK 64-Bit Server VM (Zulu 8.31.0.1-linux64) (build 25.181-b02, mixed mode)
   [root@jys1235 jvm]#
   ```

3. HDM KVMを実行する:

ダウンロードしたKVM.jnlpファイルをダブルクリックし、開いたダイアログボックスで実行をクリックします。

図71 HDM KVMの実行

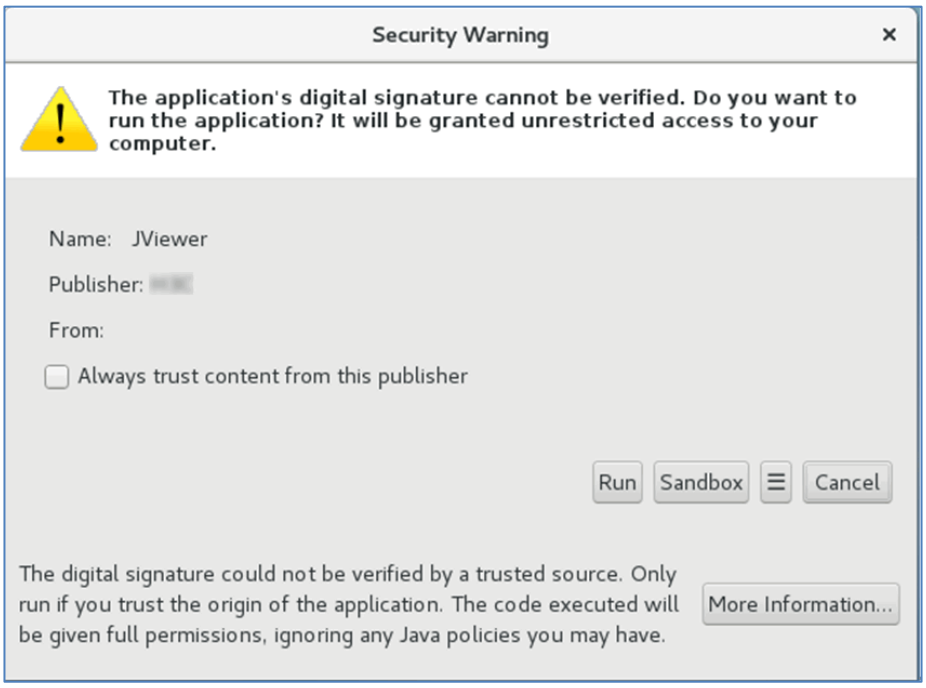


図68に示すように、KVMログインウィンドウが開きます。KVMにアクセスするためのパスワードを入力できます。

KVMまたはH5 KVMリモートコンソールを起動する

制限事項とガイドライン

KVMとH5 KVMを同時に使用したり、1台のPC上の複数のブラウザーでリモートコンソールを起動したりしないでください。

セキュリティ上の理由から、プライマリユーザーとしてリモートコンソールセッションを閉じるときは、信頼できるセカンダリユーザーに完全なアクセス許可を与えます。

セカンダリユーザーに完全な権限を付与すると、プライマリユーザーから完全な権限が削除されます。その後、プライマリユーザーは読取り専用の権限のみを持ちます。

プライマリユーザーは、KVMウィンドウを閉じるときに任意のセカンダリユーザーにフル権限を付与できます。プライマリユーザーが10秒以内にフル権限を付与しない場合、セカンダリユーザーの権限は変更されません。

リモートコンソールがアクティブな場合は、サーバーのUID LEDが点滅します。

前提条件

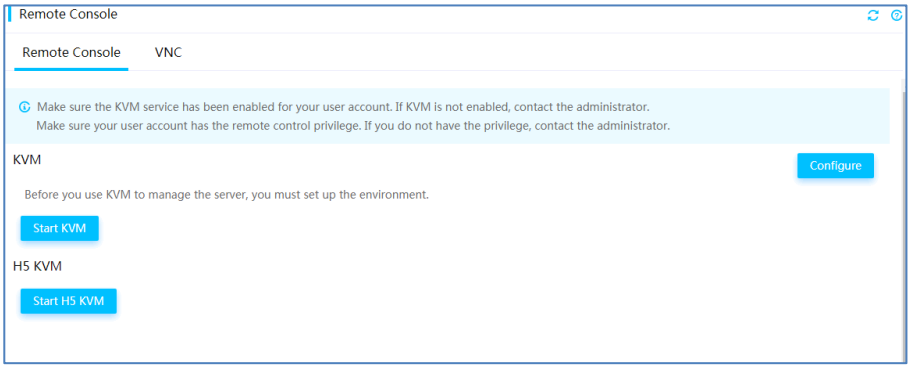
リモートコントロールコンソールを起動する前に、次のタスクを実行する必要があります。

- ユーザーカウントにリモート制御権限があることを確認します。リモート制御権限がない場合は、管理者に連絡してください。
- KVMコンソールを起動するには、ユーザーカウントにKVM拡張権限があることを確認します。H5 KVMコンソールを起動するには、アカウントにWebおよびKVM拡張権限があることを確認します。WebまたはKVM権限がない場合は、管理者に連絡してください。

手順

1. ナビゲーションペインで、図72に示すように、**Remote Services > Remote Console**を選択します。

図72 リモートコンソールページの入力

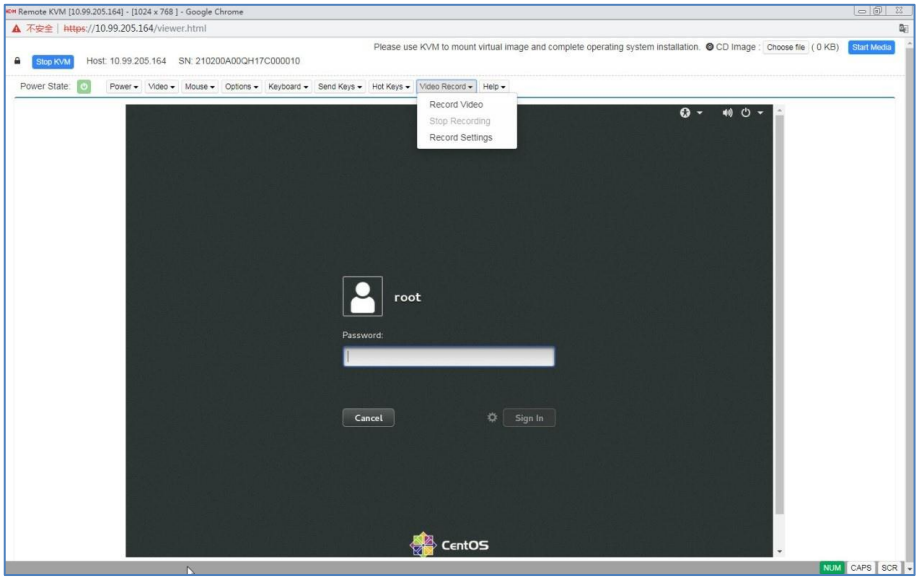


2. (オプション) **Configure**をクリックし、KVMおよびH5 KVMの起動モードを選択して、**OK**をクリックします。
3. リモートコンソールを起動します。
   - KVMリモートコンソールを起動するには、**Start KVM**をクリックします。
   - H5 KVMリモートコンソールを起動するには、**Start H5 KVM**をクリックします。

   暗号化モードでは、暗号化されたデータが送信され、セキュリティパフォーマンスが向上します。暗号化されていないモードでは、暗号化されていないデータが送信され、伝送速度が向上

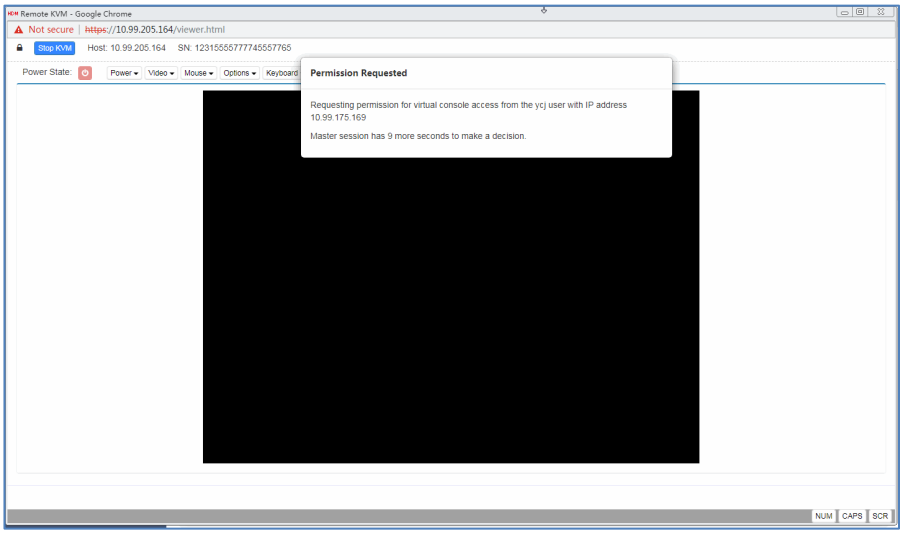
   リモートコンソールのログインページが開きます。

図73 リモートコンソールのサインインページ



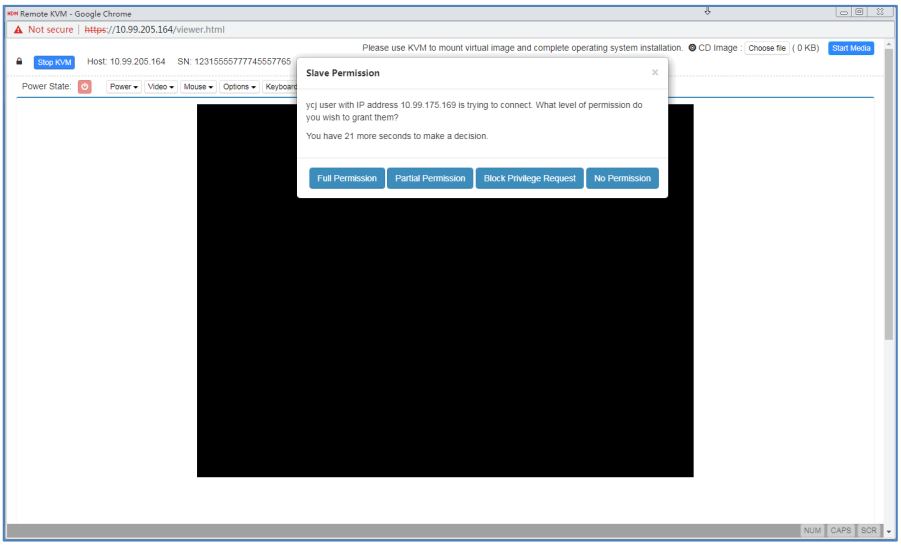
4. 共有モードでは、図74に示すように、最初のアクセスユーザーでない場合は、プライマリユーザーからのアクセス認可を待ちます。

図74 リモートコンソールアクセス許可の待機



プライマリユーザーである場合は、図75に示すように、他のユーザーにアクセス権を付与する必要があります。

図75 リモートコンソールアクセスの許可



パラメーター

- **Dedicated mode**: **Encrypted dedicated mode**と**Unencrypted dedicated mode**が含まれます。専用モードでは、1つのリモートコンソールセッションのみが許可され、ユーザーにフルアクセス許可が付与されます。専用モードでリモートコンソールを正常に起動できるのは、他のユーザーがリモートコンソールを使用していない場合のみです。
- **Shared mode**: **Encrypted shared mode**および**Unencrypted shared mode**が含まれます。共有モードでは、1次セッションおよび複数の2次セッションが可能です。最初にアクセスする場合

  ユーザーには、フルアクセス権限が割り当てられます。ユーザーがセカンダリユーザーの場合、付与される権限はプライマリユーザーによって次のように決定されます。

  - フルアクセス権限が付与されている場合は、情報を表示してサーバーを設定できます。
  - 読み取り専用のアクセス許可が付与されている場合は、ビデオとスクリーンショットの表示とビデオの録画だけが可能です。設定タスクは実行できません。
  - アクセスが拒否された場合KVMウィンドウが閉じます。

- プライマリユーザーが30秒以内に応答しない場合は、読み取り専用の権限が付与されます。

KVMからサーバーを操作する

前提条件

KVMリモートコンソールを起動します。

サーバーを起動またはシャットダウンする

⚠警告!

Force Power-Offおよび**Graceful Power-Off**オプションは、ほとんどの回路から電源を切断することによってのみサーバーをスタンバイモードにします。すべての電源を切断した状態でサーバーを維持するには、サーバーからすべての電源コードを取り外す必要があります。

1. トップメニューバーから電源メニューを選択します。
2. 必要に応じてメニューオプションを選択します。

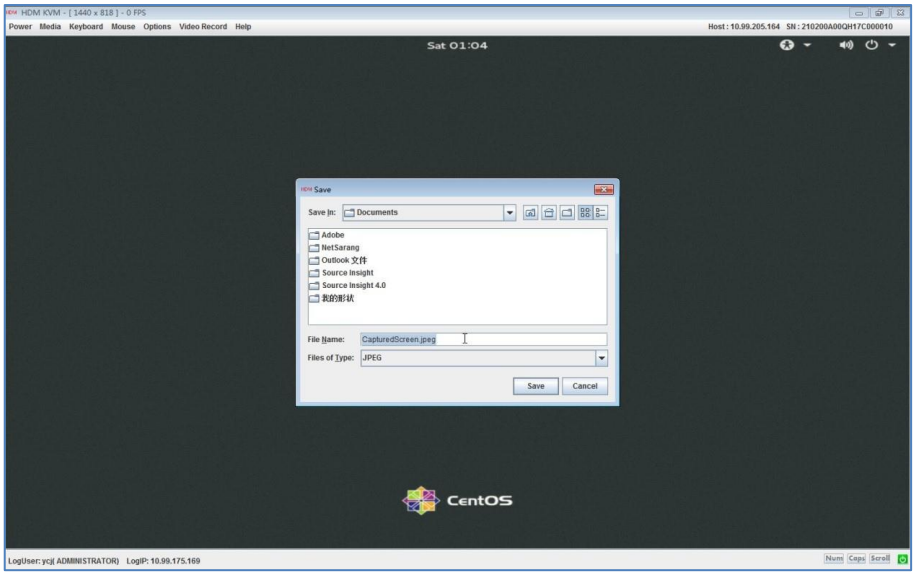
電源メニューオプション	目的
Force System Reset	ウォームリブートは、サーバーの電源を再投入せずにサーバーを再起動します。
Force Power-Off	強制的にただちにサーバーをシャットダウンします。これは、サーバーの電源ボタンを5秒間押して、サーバーをスタンバイモードにするのと同じ動作です。
Graceful Power-Off	まずオペレーティングシステムをシャットダウンし、次にサーバーから電源を切断してスタンバイモードにします。
Power On	サーバーを起動します。
Power On	サーバーの電源をオフにしてからオンにします。

3. コンソールの右下隅にある電源アイコンを使用して、サーバーの電源状態を確認します。
   - サーバーが起動している場合、アイコンは緑色で表示されます( )。
   - サーバーがダウンしている場合は、アイコンが赤で表示されます( )。

画面をキャプチャする

1. トップメニューバーから**Options > Capture Screen**を選択します。
2. 表示されたダイアログボックスで、スクリーンショットファイルのストレージパスを選択し、ファイル名を入力して、**save**をクリックします(図76を参照)。

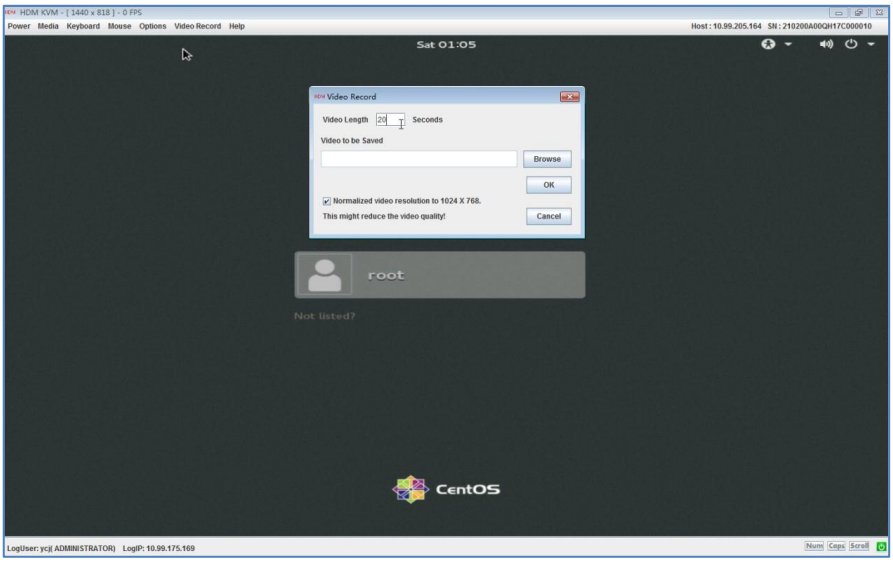
図76 画面のキャプチャ



ビデオを録画する

1. トップメニューバーから**Video Record** > **Settings**を選択します。
2. 図77に示すように、ビデオ記録パラメーターを設定します。
   - **Video Length**
   - **Video to be Saved**
   - **Normalized video resolution to 1024 × 768**

図77 ビデオ録画パラメーターの設定



3. **Video Record** > **Start Record**を選択して、ビデオ録画を開始します。
4. ビデオの録画を停止するには、**Video Record** > **Start Record**を選択します。

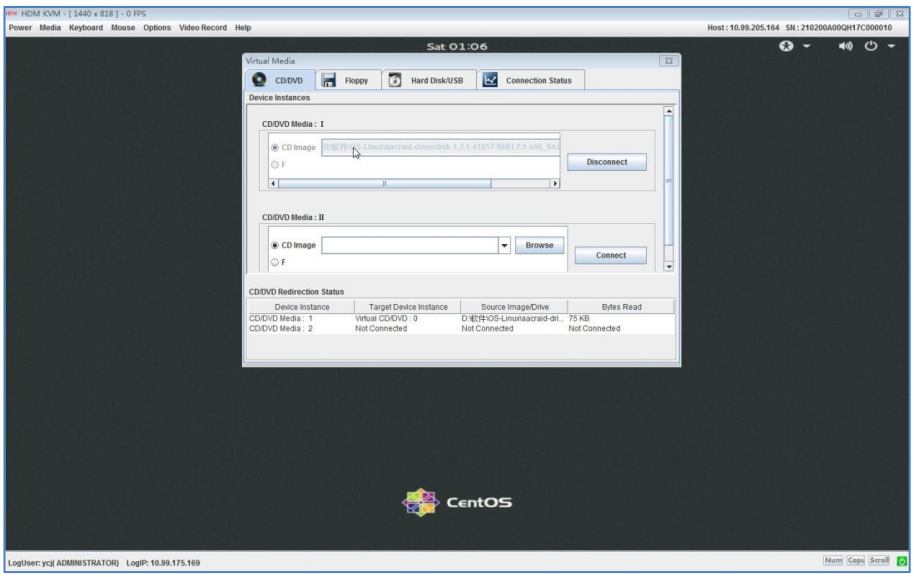
仮想ストレージメディアをマウントする

1. トップメニューバーから**Media** > **Virtual Media Wizard**を選択します。
2. 図78に示すように、仮想ストレージメディアをマウントします。
   - 仮想CD/DVDをマウントするには、**CD/DVD**タブをクリックし、**CD Image**フィールドの横にある**Browse**をクリックして、ローカルPCのCD/DVDファイルまたはCD/DVDドライブを選択し、**Connect**をクリックします。

- 仮想フロッピーディスクをマウントするには、**Floppy**タブをクリックし、**Floppy Image**の横にある**Browse**をクリックします。
  フィールドで、ローカルPCからフロッピーディスクファイルを選択し、接続をクリックします。
- 仮想ハードディスクドライブまたはUSBをマウントするには、**ard disk/USB**タブをクリックし、次のいずれかのタスクを実行します。
  - イメージがすでにハードドライブまたはUSBに存在する場合は、**HD/USB Imag**を選択し、**HD/USB Image**フィールドの横にある**Browse**をクリックし、ローカルPCのディスクファイルまたはUSBデバイスを選択して、**Connect**をクリックします。
  - イメージがハードドライブまたはUSBに存在しないが、マウントするファイルがローカルPCに存在する場合は、**Folder Path**を選択し、**Folder Path**フィールドの横にある**Browse**をクリックしてローカルPCからフォルダを選択します。次に、**Image Path**フィールドの横にある**Browse**をクリックして、選択したフォルダを使用して生成されたイメージを保存するためのハードドライブまたはUSBからのパスを選択し、**Connect**をクリックします。

    フォルダのサイズが600 M以下であること、およびイメージを保存するパスがフォルダを保存するパスと異なることを確認します。

図78 仮想記憶媒体のマウント



3. 仮想ストレージメディアをアンマウントするには、メディアタブにアクセスし、**Disconnect**をクリックします。

リモートコンソールを終了する

リモートコンソールを終了してHDMから切断するには、次のいずれかの方法を使用します。

- リモートコンソールウィンドウの閉じるボタン をクリックします。
- HDM Webインターフェースで**Logout**をクリックします。

仮想メディアがリモートコンソールを介してマウントされている場合、KVMアイドルタイムアウトは有効になりません。

KVMコンソールで周辺機器を設定する

- キーボード設定を構成するには、トップメニューバーから**Keyboard**メニューを選択し、目的のメニューオプションを選択します。

キーボードメニューオプション	タスク
Ctrl+Alt+Delキー	キーボードで**Ctrl**キー、**Alt**キー、および**Delete**キーを同時に押すのと同じ操作を実行します。
ホットキー	ホットキーを定義して使用します。 最大20個のホットキーを定義できます。各ホットキーは最大6個のキーの組み合わせです。

SoftKeyboard	ソフトキーボードを開きます。サポートされているのは、アメリカ英語のソフトキーボードだけです。

- マウスの設定を行うには、トップメニューバーからマウスメニューを選択し、目的のメニューオプションを選択します。

マウスメニューオプション	タスク
カーソルを表示	• マウスポインタの軌跡を表示するには、このオプションを選択します。 • マウスポインタの軌跡を非表示にするには、このオプションをオフにします。
マウスのキャリブレーション	相対マウスモードでマウスの位置を補正します。
マウスモード	マウスモードは、マウスの現在の位置を計算するために使用されます。次のオプションがあります。 • 絶対マウスモード画面の絶対座標に基づいてマウスの位置を計算します。 • 相対マウスモードマウス移動のオフセットに従ってマウスの位置を計算します。 • その他のマウスモードマウスから画面の中心までの距離に基づいて、マウスの位置を計算します。 サーバーオペレーティングシステムで推奨されるマウスモード: • Windows 2008、Windows 2012、Redhat 6.5、Redhat 7.0、CentOS 6.5、CentOS 7.1、Ubuntu 12.04、Ubuntu 15.04、SLES 11、およびSLES 13では、絶対マウスモードを使用します。 • Redhat 6、CentOS 6、またはFedora 14より前のバージョンでは、相対マウスモードを使用します。 • SLES 11インストールインターフェースでは、他のマウスモードを使用します。 • 上記以外のオペレーティングシステムでは、絶対マウスモードを使用します。 重要: • マウスモードを頻繁に変更しないことをお勧めします。 • マウスモードを**relative**モードまたは**other**モードから**absolute**モードに変更すると、**Show Cursor**機能が自動的に有効になります。

KVMコンソールで言語を変更する

1. トップメニューバーから**Options > GUI Languages**を選択します。
2. 言語を中国語または英語に変更します。

完全なアクセス許可要求をブロックする

プライマリユーザー(最初のコンソールセッションを確立したユーザー)の場合は、読み取り権限のみを持つリモートコンソールユーザーから完全な権限要求を受け取ることがあります。

完全なアクセス許可要求をブロックするには、トップメニューバーから**Options** > **Block Privilege Request**を選択します。

OSのインストールを迅速化

OSのインストールを高速化するには、トップメニューバーから**Options** > **CD/DVD Acceleration**を選択します。ベストプラクティスとして、次の要件が満たされている場合にのみCD/DVDアクセラレータを有効にしてください。

- ネットワーク内のすべてのスイッチおよびルータは1 Gbps以上で動作します。
- ユーザーは共有ネットワークポートを介してHDMにアクセスします。
- 仮想CD/DVDイメージがマウントされます。

この機能のサポートは、サーバーの設定によって異なります。

次回のブート用にブートオプションを構成する

次回のリブート時にサーバーが使用するブートオプション、ブートモード、およびブート順序を設定するには、トップメニューバーから**Options** > **Boot Options**を選択します。詳細については、「ブートオプションの設定」を参照してください。

バージョンおよび著作権情報を入手する

バージョンおよび著作権情報を入手するには、トップメニューバーから**Help** > **About HDM KVM**を選択します。

キーボードボタンを使用する

リモートコンソールには、右下に次のキーボードボタンがあります。

- **Num**:キーボードの**Num**キーを押した場合に相当します。
- **Caps** -キーボードの**Caps**キーを押すのと同じです。
- **Scroll**-キーボードの**Scroll**キーを押した場合に相当します。

H5 KVMからサーバーを操作する

前提条件

H5 KVMリモートコンソールを起動します。

サーバーを起動またはシャットダウンする

⚠警告!

Force Power Offおよび**Graceful Power Off**オプションは、ほとんどの回路から電源を切断することによってのみ、サーバーをスタンバイモードにします。すべての電源を切断した状態でサーバーを維持するには、サーバーからすべての電源コードを取り外す必要があります。

1. トップメニューバーから**Power**メニューを選択します。
2. 必要に応じてメニューオプションを選択します。

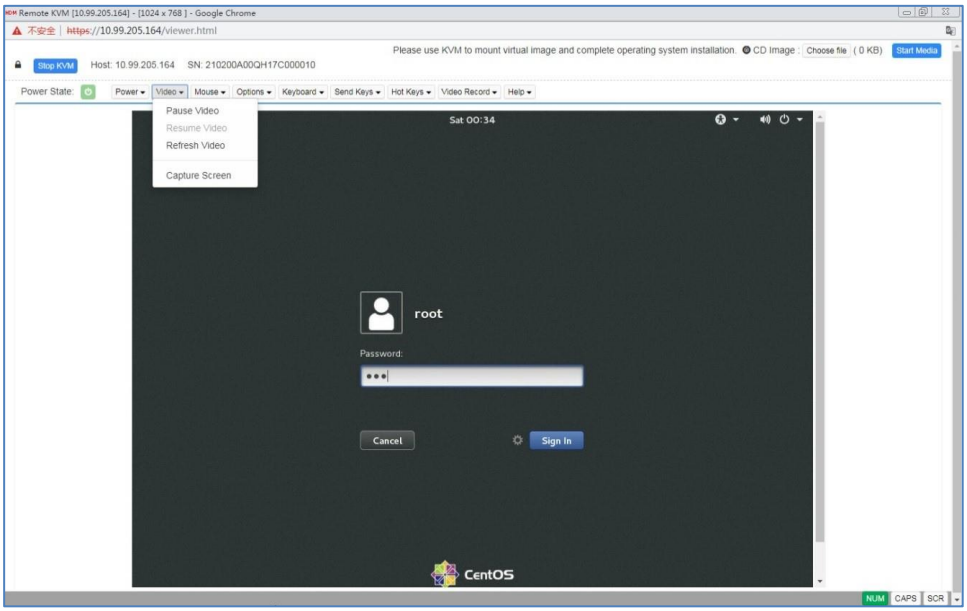
電源メニューオプション	目的
Immediate Reset	ウォームリブートは、サーバーの電源を再投入せずにサーバーを再起動します。
Force Power Off	強制的にただちにサーバーをシャットダウンします。これは、サーバーの電源ボタンを5秒間押して、サーバーをスタンバイモードにするのと同じ動作です。
Graceful Power Off	まずオペレーティングシステムをシャットダウンし、次にサーバーから電源を切断してスタンバイモードにします。
Power On	サーバーを起動します。
Power Cycle	サーバーの電源をオフにしてからオンにします。

3. コンソールの左上隅にある電源アイコンを使用して、サーバーの電源状態を確認します。
   - サーバーが起動している場合、アイコンは緑色で表示されます( )。
   - サーバーがダウンしている場合は、アイコンが赤で表示されます( )。

画面をキャプチャする

図79に示すように、トップメニューバーから**Video > Capture Screen**を選択します。

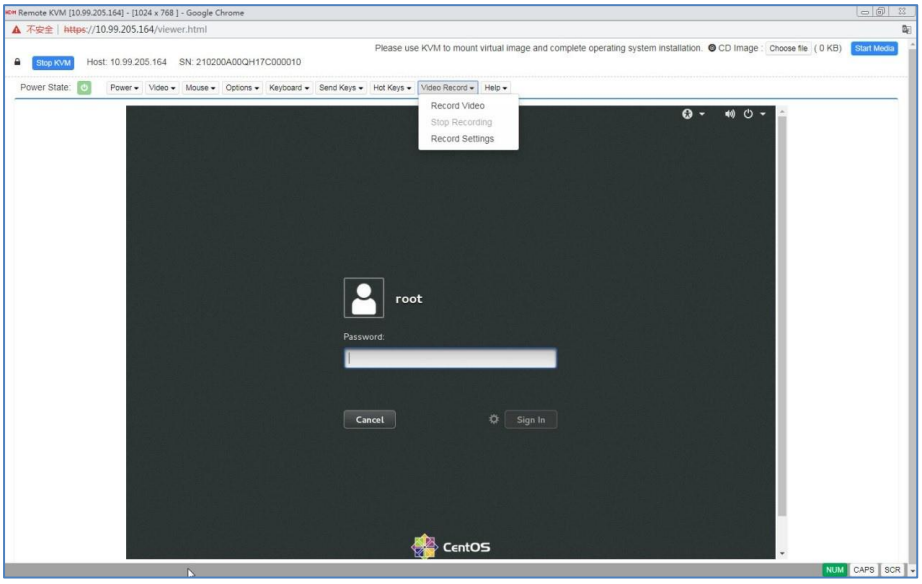
図79 画面のキャプチャ



ビデオを録画する

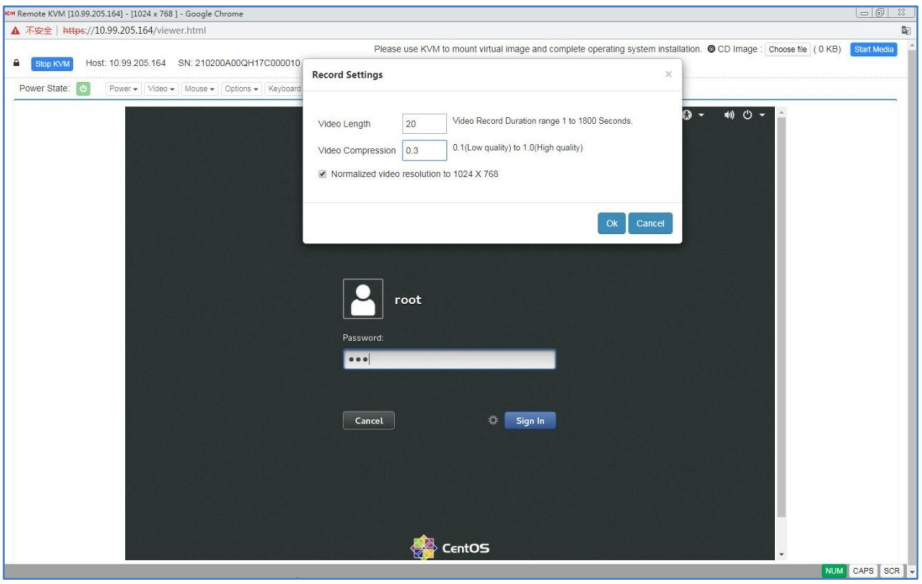
1. トップメニューバーから**Video Record** > **Record Settings**を選択します。

   図80 ビデオ録画パラメーターの設定



2. 図81に示すように、ビデオ記録パラメーターを設定します。
   - **Video Length**:ビデオの最大時間を入力します。値の範囲は1～1800秒です。
   - **Video Compression:** ビデオ圧縮率を設定します。値の範囲は0.1～1です。
   - **Normalized video resolution to 1024 × 768**

図81 ビデオ録画パラメーターの設定



3. **Video Record > Record Video**を選択して開始します。
4. ビデオの録画を停止するには、**Video Record** > **Stop Record**を選択します。

仮想メディアのマウント

H5 KVMは、.isoイメージのマウントのみをサポートしています。仮想メディアをマウントするには:

1. リモートコンソールの右上隅にある**Browse File**をクリックします。
2. isoイメージファイルを選択します。
3. **Start Media**をクリックします。
   仮想メディアをアンマウントするには、**Stop Media**をクリックします。

リモートコンソールを終了する

リモートコンソールを終了してHDMから切断するには、次のいずれかの方法を使用します。

- ベストプラクティスとして、リモートコンソールの左上隅にある**Stop KVM**をクリックします。
- HDM Webインターフェースで**Logout**をクリックします。

仮想メディアがリモートコンソールを介してマウントされている場合、KVMアイドルタイムアウトは有効になりません。

ビデオを再生する

1. トップメニューバーから**Video**メニューを選択します。
2. 必要に応じて次のメニューオプションを選択します。
   - ビデオの再生中にビデオを一時停止するには、**Pause Video**を選択します。
   - ビデオの再生を再開するには、**Resume Redirection**を選択します。
   - リモートコンソールに表示されているビデオを更新するには、**Refresh Video**を選択します。

H5 KVMコンソールで周辺機器を設定する

- マウスの設定を行うには、トップメニューバーから**Mouse**メニューを選択し、目的のメニューオプションを選択します。

マウスメニューオプション	タスク
クライアントカーソルを表示	• マウスポインタの軌跡を表示するには、このオプションを選択します。 • マウスポインタの軌跡を非表示にするには、このオプションをオフにします。

マウスモード	マウスモードは、マウスの現在の位置を計算するために使用されます。次のオプションがあります。 • Absolute Mouse Mode: 画面の絶対座標に基づいてマウスの位置を計算します。 • Other Mouse Mode: マウスから画面の中心までの距離に基づいて、マウスの位置を計算します。 サーバーオペレーティングシステムで推奨されるマウスモード: • Windows 2008、Windows 2012、Redhat 6.5、Redhat 7.0、CentOS 6.5、CentOS 7.1、Ubuntu 12.04、Ubuntu 15.04、SLES 11、およびSLES 13では、絶対マウスモードを使用します。 • Redhat 6、CentOS 6、またはFedora 14より前のバージョンでは、相対マウスモードを使用します。 • ベストプラクティスとして、SLES 11でKVMを使用し、マウスモードをotherに設定します。 重要: • マウスモードを頻繁に変更しないことをお勧めします。 • **Show Client Cursor**機能は、マウスモードを**other**から**absolute**に変更すると、自動的に有効になります。

- キーボード設定を構成するには、トップメニューバーから**Keyboard**メニューを選択し、目的のメニューオプションを選択します。

キーボードメニューオプション	タスク
英語U.S.	英語(U.S.)キーボードレイアウトを使用します。

- キーの送信操作を実行するには、トップメニューバーからキーを送信メニューを選択し、目的のメニューオプションを選択します。

Send Keysメニューオプション	説明
Hold Downセクション	
右Ctrlキー	キーボードの右Ctrlキーを押した場合と同じです。
右Altキー	キーボードの右Altキーを押す操作に相当します。
右Windowsキー	キーボードで右のWindowsキーを押す操作に相当します。
左Ctrlキー	キーボードの左Ctrlキーを押した場合と同じです。
左Altキー	キーボードの左Altキーを押した場合と同じです。
左Windowsキー	キーボードの左Windowsキーを押す操作に相当します。
Press and Releaseセクション	
Ctrl+Alt+Delキー	キーボードでCtrlキー、Altキー、およびDeleteキーを同時に押して放す操作に相当します。
左Windowsキー	キーボードの左Windowsキーを押して放す操作に相当します。
右Windowsキー	キーボードの右Windowsキーを押して放す操作に相当します。
コンテキストメニューキー	キーボードのコンテキストメニューキーを押して放す操作に相当します。
スクリーンキーを印刷	キーボードのPrScrnキーを押して放す操作に相当します。

- ホットキーを定義して使用するには、トップメニューバーから**Hot Keys**メニューを選択し**Add Hot Keys**を選択します。

完全なアクセス許可要求をブロックする

プライマリユーザー(最初のコンソールセッションを確立したユーザー)の場合は、読み取り権限のみを持つリモートコンソールユーザーから完全な権限要求を受け取ることがあります。

完全なアクセス許可要求をブロックするには、トップメニューバーから**Options** > **Block Privilege Request**を選択します。

H5 KVMコンソールで言語を変更する

1. トップメニューバーから**Options > GUI Languages**を選択します。
2. 言語を中国語または英語に変更します。

OSのインストールを迅速化

OSのインストールを高速化するには、トップメニューバーから**Options** > **CD/DVD Acceleration**を選択します。

ベストプラクティスとして、次の要件が満たされている場合にのみCD/DVDアクセラレータを有効にしてください。

- ネットワーク内のすべてのスイッチおよびルーターは1 Gbps以上で動作します。
- ユーザーは共有ネットワークポートを介してHDMにアクセスします。
- 仮想CD/DVDイメージがマウントされます。

この機能のサポートは、サーバーの設定によって異なります。

次回のブート用にブートオプションを構成する

次回のリブート時にサーバーが使用するブートオプション、ブートモード、およびブート順序を設定するには、トップメニューバーから**Options** > **Boot Options**を選択します。詳細については、「ブートオプションの設定」を参照してください。

キーボードボタンを使用する

リモートコンソールには、右下に次のキーボードボタンがあります。

- **Num**:キーボードの**Num**キーを押した場合に相当します。
- **Caps** -キーボードの**Caps**キーを押すのと同じです。
- **Scroll**-キーボードの**Scroll**キーを押した場合に相当します。

バージョンおよび著作権情報を入手する

バージョンおよび著作権情報を入手するには、トップメニューバーから**Help** > **About H5Viewer**を選択します。

VNCからサーバーを操作する

VNCについて

VNCはリモートデスクトップ共有のテクノロジーです。VNCシステムでは、クライアントはリモートフレームバッファ(RFB)プロトコルを使用してサーバーに接続し、サーバーのリモートデスクトップを制御できます。RFBは、グラフィカルユーザーインターフェースへのリモートアクセスに使用される単純なプロトコルです。フレームバッファレベルで機能し、WindowsやMacなどのすべてのウィンドウシステムおよびアプリケーションに適用できます。VNCを使用すると、HDMにログインせずにローカルPCからサーバーにアクセスして管理できます。

HDMは、IPv4とIPv6の両方のVNCセッションをサポートします。次のセッションモードを使用できます。

- **Shared mode** -最大2つの同時VNCセッションをサポートします。両方のセッションはマウスとキーボードにアクセスでき、サーバーのOSを制御できます。
- **Exclusive mode**: 1つのVNCセッションだけをサポートします。

VNCシステムで使用されるセッションモードは、VNCクライアントによって決定されます。

前提条件

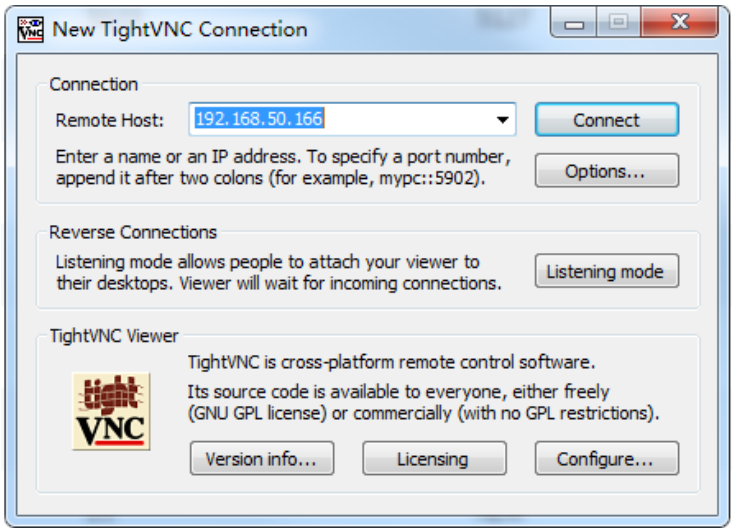
VNCを使用してサーバーを操作する前に、次のタスクを完了する必要があります。

- HDMにサインインし、**Remote Services > Services**ページでVNCサービスをイネーブルにします。
- VNCクライアントをインストールします。この例では、TightVNCを使用します。

手順

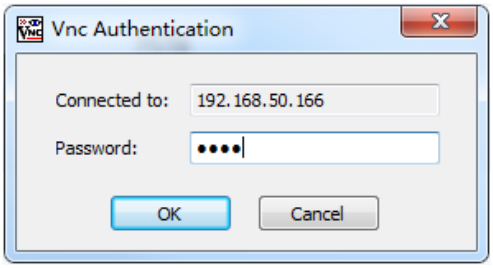
1. VNCクライアントを開き、アドレスバーにHDM管理IPアドレスを入力して図82に示すように接続します。

図82 ログインページの入力



2. 開いたウィンドウで、VNCパスワード(デフォルトは**root**)を入力し、図83に示すように**OK**をクリックします。

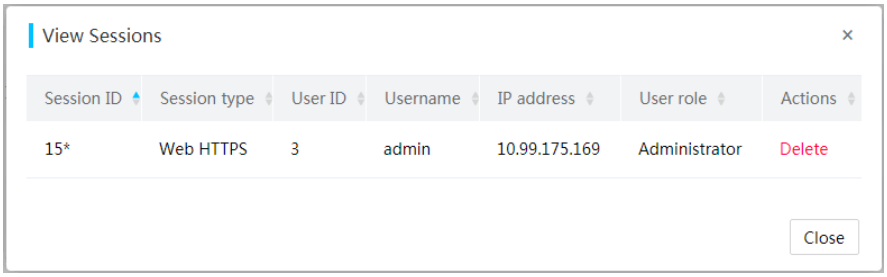
図83 VNCサーバーへの認証



VNCクライアントとVNCサーバーの間でVNCセッションが確立されます。VNCクライアントはサーバー画面を表示します。

確立されたVNCセッションは、HDMの**Remote Services > Services**ページから表示できます。VNCセッションのIPアドレスは、VNCクライアントのIPアドレスです。

図84 VNCセッション情報



3. 必要に応じてサーバーを操作します。

VNCログインパスワードを設定する

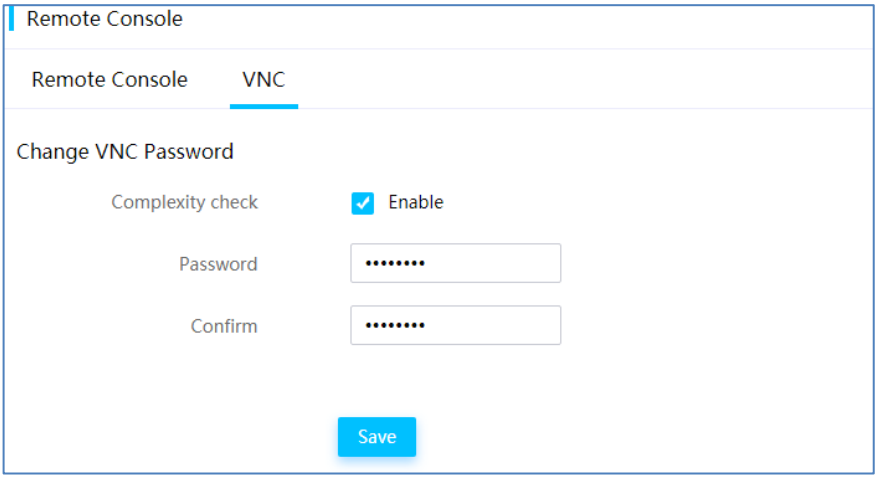
この機能を使用して、VNCクライアントログインのパスワードの設定を構成します。デフォルトでは、パスワードは**root**です。

手順

1. ナビゲーションペインで、**Remote Services > Remote Console**を選択します。

2. 作業ペインで、図85に示すように**VNC**タブをクリックします。

図85 VNCの構成



3. (オプション)**Enable for Complexity check**を選択します。
4. 新しいパスワードを入力し、新しいパスワードを確認します。
5. **save**をクリックします。

パラメーター

Complexity check:パスワードの複雑性チェックを無効または有効にします。

- この機能をディセーブルにする場合、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。
  - 1～8文字。
  - 大文字と小文字が区別されます。有効な文字は、文字、数字、スペースおよび特殊文字です。 `~!@#$%^&*()_+-=\{};':",./<>?
- この機能がイネーブルになっている場合、パスワードは次の拡張複雑度要件を満たす必要があります。
  - 8文字。
  - 大文字と小文字が区別されます。有効な文字は、文字、数字、スペースおよび特殊文字です。 `~!@#$%^&*()_+-=\{};':",./<>?
  - 大文字、小文字、数字の少なくとも2つのカテゴリの文字を含む必要があります。
  - スペースまたは特殊文字を少なくとも1つ含む必要があります。

リモートメディアマウント

イメージマウントでは、イメージファイルをリモートデバイスからサーバーのオペレーティングシステムにマウントします。この機能を使用すると、イメージファイルをマウントする前にイメージファイルをサーバーにコピーする必要はありません。

リモートコンソール(「リモートコンソール」を参照)またはイメージマウント機能を使用して、仮想メディアをマウントできます。次に、イメージマウントを使用してリモートメディアイメージファイルをマウントする方法を説明します。

リモートメディアをマウントする

リモートメディアをサーバーのオペレーティングシステムにマウントするには、次の作業を実行します。

前提条件

リモートメディアイメージマウントを設定する前に、次の作業を実行します。

1. マウントするイメージファイルが正しい形式であることを確認します。

   CD/DVDイメージファイルには.iso拡張子を使用し、ディスクイメージファイル(フロッピーディスク、HDD、SSDなど)には.imgまたは.ima拡張子を使用する必要があります。

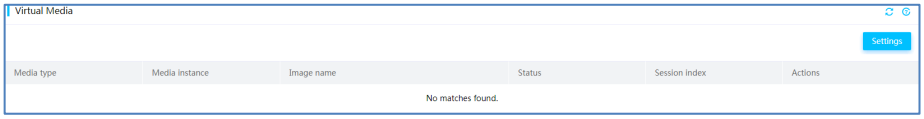
   フロッピーディスクイメージファイルは1.44 MBを超えることはできません。

2. NFSサーバーまたはCIFSサーバー上のソースディレクトリにあるCD/DVDイメージファイル、フロッピーイメージファイル、ディスクイメージファイルのそれぞれの数が60を超えていないことを確認します。
3. ユーザーカウントに、管理者またはオペレータの役割またはリモートメディア権限があることを確認します。アカウントが管理者でもオペレータでもなく、リモートメディア権限がない場合は、管理者に連絡して権限を取得します。
4. 必要な仮想メディアサービスがユーザーカウントに対して有効になっていることを確認します。有効になっていない場合は、管理者に連絡してください。CD-MediaとHD-Mediaを使用して2つのイメージファイルをマウントし、FD-Mediaを使用して1つのメディアだけをマウントすることができます。

手順

1. イメージマウント環境を設定します。詳細については、「仮想メディアを構成する」を参照してください。
2. ナビゲーションペインで、**Remote Services > Virtual Media**を選択します(図86を参照)。

図86 リモートメディアマウントページへのアクセス



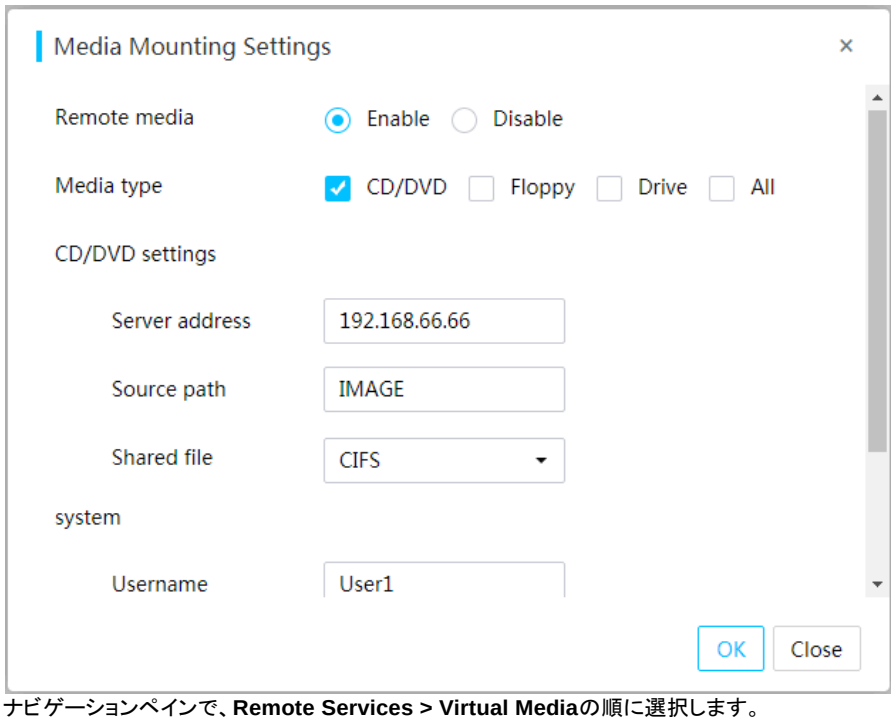
3. 作業ウィンドウで、**Settings**をクリックします。
4. 表示されたダイアログボックスで、リモートメディアを有効にし、メディアタイプを選択して**OK**をクリックします(図87を参照)。
   - 共有ファイルシステムとしてNFSを選択した場合は、サーバードレスとソースパスを入力します。
   - 共有ファイルシステムとしてCIFS(Samba)を選択する場合は、サーバードレス、ソースパス、ユーザー名、パスワードおよびドメイン名を入力します。ドメイン名フィールドはオプションです。

   イメージのマウントに失敗しないように、ポンド記号(#)などの不要な特殊文字は入力しないでください。

重要:

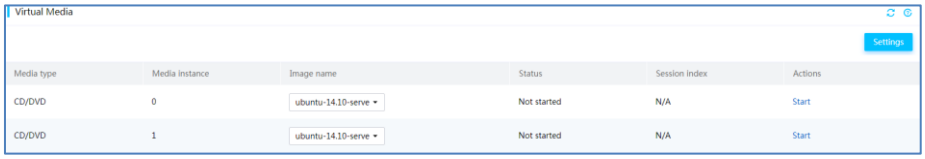
リモートメディアマウントがすでに有効になっている場合は、すべてのリモートメディアマウントを停止しない限り、メディア設定を変更することはできません。

図87 メディアマウント設定の構成



5. ナビゲーションペインで、**Remote Services > Virtual Media**の順に選択します。
6. リモートメディアリストからイメージファイルを選択し、**Start**をクリックします。イメージファイルをマウント解除するには、**Stop**をクリックします。

図88 リモートメディアマウントの開始または停止



パラメーター

- **Media type**:CD/DVD、フロッピー、ディスク(HDDとSSDの両方を含む)などのリモートメディアのタイプ。
- **Status**:リモートメディアのマウントステータス**(Started**および**Not Started**を含む)。開始していませんステータスの一般的な理由は次のとおりです。
  - **Opening error** - イメージファイルが無効です。
  - **Connection in use** - マウントセッションの最大数に達しました。
  - **Connection lost** - 仮想メディアサービスが失敗しました。
  - **Access error** - バーチャルメディアサービスが有効になっていません。
  - **Session terminated** - バーチャルメディアセッションが終了します。
- **Session index**:リモートメディアマウントセッションのインデックス。

リモートメディアを無効にする

1. ナビゲーションペインで、**Remote Services > Virtual Media**の順に選択します。
2. 作業ウィンドウで、**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、リモートメディアに対して**Disable**を選択し、OKをクリックします(図87を参照)。

SNMP

Simple Network Management Protocol(SNMP)は、リモート管理および運用に使用されるインターネットプロトコルです。これにより、ユーザーは、異なる物理特性を持つ異なるベンダーのデバイスおよびネットワーク内の相互接続テクノロジーをNMSを通じて管理できます。たとえば、デバイスステータスの監視、統計情報の収集、トラブルシューティングの実行などです。

SNMPバージョン、読み取り専用コミュニティストリング、および読み取り/書き込みコミュニティストリングなどのSNMP設定を設定するには、次の作業を実行します。

制限事項とガイドライン

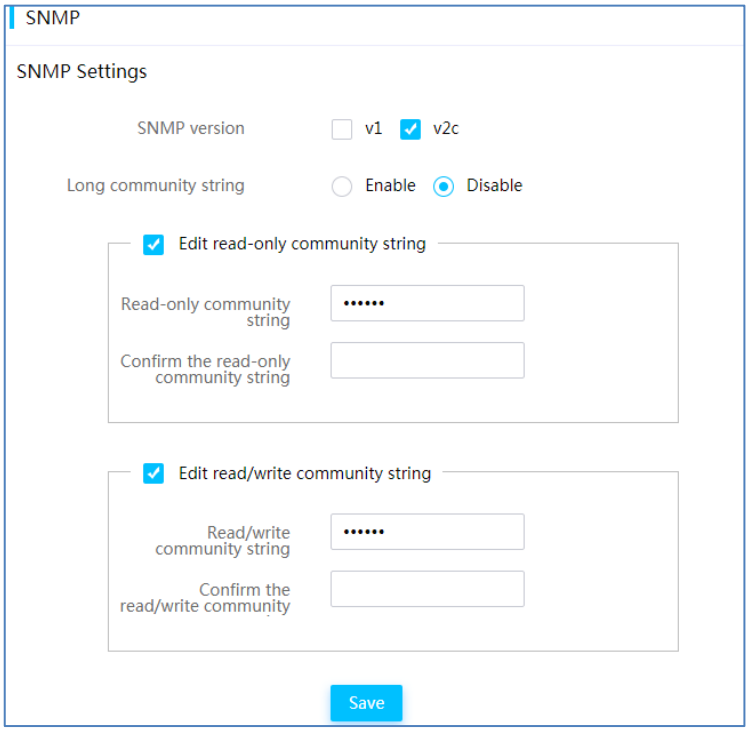
読み取り/書き込みコミュニティ名が空の場合、SNMP SET操作はサポートされません。読み取り/書き込みコミュニティ名と読み取り専用コミュニティ名を同じにすることはできません。

読み取り/書き込みコミュニティストリングと読み取り専用コミュニティストリングは、Webインターフェースから暗号文形式で表示されます。

手順

1. ナビゲーションペインで、**Remote Services > SNMP**を選択します。
2. 作業ウィンドウで、SNMP設定を構成します。
   a. SNMPバージョンを選択します。
   b. 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。
   c. **Edit read-only community string**または**Edit read/write community string**を選択し、読み取り専用または読み取り/書き込みコミュニティストリングを入力または削除します。
3. **save**をクリックします。

図89 SNMP設定の構成



パラメーター

- **SNMP version**: SNMP GETおよびSET操作で使用可能なSNMPバージョンを選択します。**v1**および**v2c**などのオプションがあります。SNMP v3はデフォルトでサポートされています。
- **Long community string**: 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。この機能はデフォルトでディセーブルになっています。

  長いコミュニティストリング機能をイネーブルにすると、コミュニティストリングの値の範囲は16～32文字になります。長いコミュニティストリング機能をディセーブルにすると、コミュニティストリングの値の範囲は1～32文字になります。長いコミュニティストリング機能がイネーブルになっているかどうかに関係なく、読み取り/書き込みコミュニティストリングを空のままにできます。
- **Read-only community string**: セキュリティ認証用の読み取り専用コミュニティストリングを入力します。デフォルトでは、このフィールドは空ですが、デフォルトの読み取り専用SNMPコミュニティストリングは**rocommstr**です。
- **Read/write community string**: セキュリティ認証の読み取り/書き込みコミュニティストリングを入力します。デフォルトでは、読み取り/書き込みSNMPコミュニティストリングは指定されていません。

備考

Read-only community stringフィールドと**Read/write community string**フィールドには、文字、数字、および特殊文字(`~!@$%^&*()_+-={}:、./?)のみを含めることができます。

リモートO&M

ログ

イベントログの管理

イベントログポリシーを設定し、イベントログを表示、ダウンロード、またはクリアするには、次の作業を実行します。

制限事項とガイドライン

イベントログが最大サイズ(3639)に達すると、新しいイベントのロギングアクションは、イベントログポリシーに依存

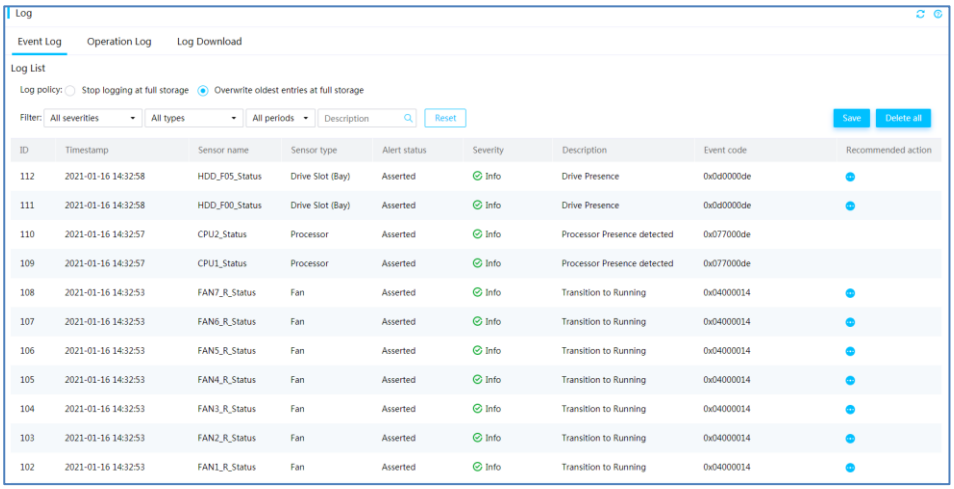
します。

すべてのイベントログエントリが削除されると、システムは削除を記録するログエントリを自動的に生成します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。**Logs**ページが表示されます。
2. **Event Log**タブで、**Log policy**フィールドからイベントログポリシーを選択します。
3. 作業ウィンドウで、次のいずれかの方法を使用してイベントをフィルタリングします。
   - イベントの重大度レベルを選択します。
   - センサーのタイプを選択します。
   - イベントが生成された期間を選択またはカスタマイズします。
   - キーワードを入力します。
4. キーワードに基づいてイベントをフィルタリングするには、キーワードを入力し、クエリーアイコンをクリックします。
5. 指定したすべてのフィルタ条件をクリアするには、**Reset**をクリックします。
6. イベントログエントリを.csvファイルに保存するには、**Save**をクリックします。
7. すべてのイベントログエントリを削除するには、**Delete all**をクリックします。削除されたイベントログエントリは復元できません。

図90 イベントログの管理



パラメーター

- **Stop logging at full storage**:イベントログがいっぱいになると、システムは新しいイベントへのロギングを停止します。
- **Overwrite oldest entries at full storage**:イベントログがいっぱいになると、古いエントリが新しいログエントリで上書きされます。
- **ID**:イベント番号。イベントは時間順に番号付けされます。デフォルトでは、イベントリスト内のイベントはイベント番号順に昇順にソートされます。
- **Timestamp**:イベントがログに記録された日付と時刻。
- **Alert status**:イベントのアラームステータス。**Cleared**は、イベントアラームがクリアされたことを示します。**Triggered**は、イベントが解決されることを意味します。
- **Severity**:イベントの重大度。
  - **Info** -イベントはシステムに悪影響を与えません。アクションは必要ありません。情報イベントの例には、予期される状態変更イベントやアラーム削除イベントなどがあります。
  - **Minor** -イベントはシステムにわずかな影響を与えます。重大度のエスカレーションを回避するには、迅速なアクションが必要です。
  - **Major** -イベントが原因でシステムの一部に障害が発生し、サービスが中断される可能性があります。即時のアクションが必要です。

- **Critical** -このイベントは、システムの停止または電源障害を引き起こす可能性があります。即時のアクションが必要です。

- **Event code**:HDM内のシステムイベントを識別するイベントコード。
- **Recommended action**:システムイベントに推奨される処置。

操作ログを管理する

操作ログには、監査ログエントリ、ファームウェア更新ログエントリ、ハードウェア更新ログエントリ、および構成ログエントリが含まれます。

- 監査ログエントリには、HDMへのアクセスやリモートコンソールの起動など、HDM管理イベントが記録されます。
- ファームウェアアップデートログエントリには、HDMファームウェアアップデートとその結果が記録されます。
- ハードウェアアップデートログエントリには、ハードウェアアップデートとその結果が記録されます。
- 設定ログエントリには、ユーザーの設定操作とその結果が記録されます。

制限事項とガイドライン

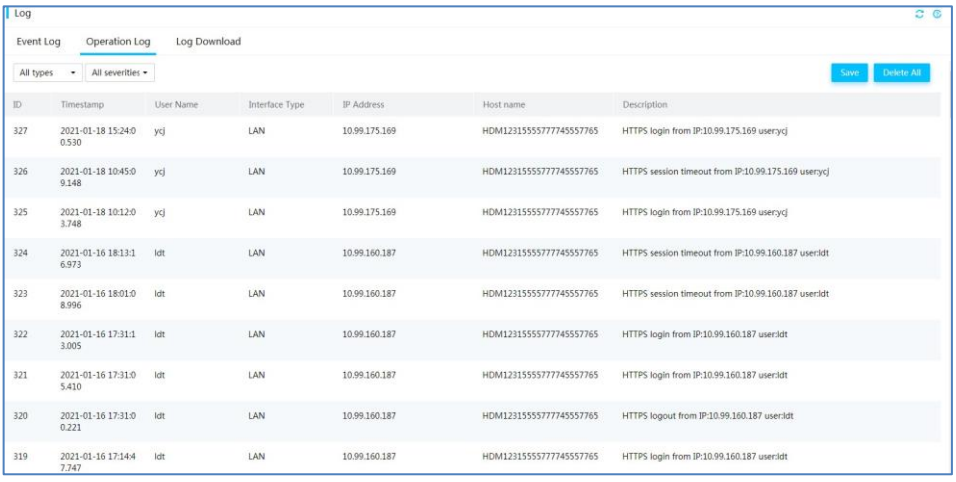
すべての操作ログエントリが削除されると、システムは削除を記録するログエントリを自動的に生成します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。**Logs**ページが表示されます。
2. **Operation Log**タブをクリックします。
3. 作業ペインで、次のようにイベントをフィルタリングするセンサータイプまたは重大度レベルを選択します。
   - 特定のタイプのセンサーによって生成されたイベントを表示するには、**All types**リストからそのセンサータイプを選択します。
   - 特定のレベルのイベントを表示するには、**All severities**リストから重大度を選択します。
4. 操作ログのエントリを.csvファイルに保存するには、**Save**をクリックします。
5. すべての操作ログエントリを削除するには、**Delete All**をクリックします。

   削除されたログエントリは復元できません。この機能は注意して使用してください。削除後、システムはログ削除ログメッセージを生成します。

図91 操作ログの管理



パラメーター

- **ID**:イベント番号。イベントは日付順に番号付けされます。デフォルトでは、イベントリスト内のイベントはイベント番号で昇順にソートされます。最大1000個のイベントログエントリを表示できます。
- **Timestamp**:イベントがログに記録された日付と時刻。
- **Interface type**:操作が実行されたインターフェースのタイプ。
- **IP address**:ユーザーIPアドレス。

- **Host name**:HDMホスト名。
- **Description**:ログエントリの説明。

ログのダウンロード

サーバーのSDSログをダウンロードするか、または連絡先情報を追加するには、次の作業を実行します。SDSログには、イベントログエントリ、ソフトウェアおよびハードウェア情報、診断情報が含まれます。

制限事項とガイドライン

複数ユーザーによる同時ログダウンロードはサポートされていません。

sdsファイルはログエントリをUTCで保存しますが、HDMはNTPサーバーから同期された日付と時刻を使用します。特定の期間のログエントリをダウンロードすると、HDMは指定された開始時刻と終了時刻をUTCに変換します。これにより、時差が発生する場合があります。

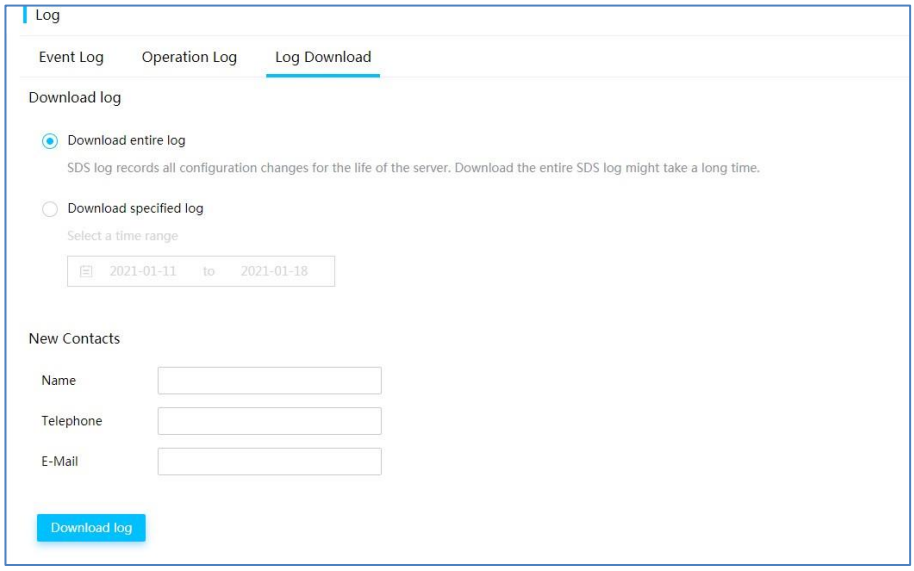
ダウンロードされたログエントリは.sdsファイルフォルダに保存されます。ファイルフォルダ内のファイルの詳細については、「付録Aダウンロードされたログファイル」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。**Logs**ページが表示されます。
2. **Log Download**タブをクリックします。
3. ダウンロードするログエントリを表示します。
   - 一定期間のログエントリをダウンロードするには、**Download specified log**領域で時間範囲を日単位で設定し、**Download specified log**をクリックします。
   - ログ全体をダウンロードするには、**Download entire log**をクリックします。

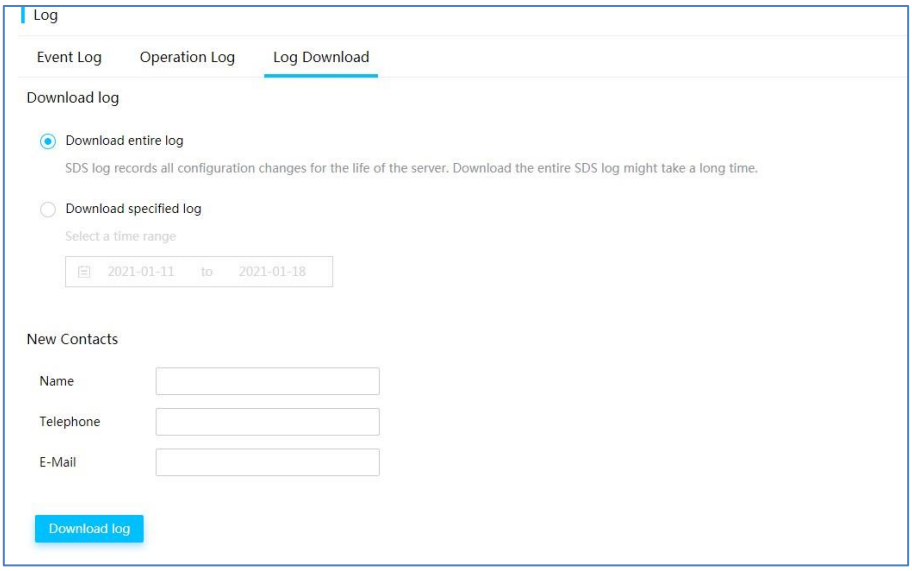
     開いたダイアログボックスにログエントリが表示されます。

図92 ログのダウンロード



4. (任意)名前、電話番号、電子メールアドレスなどの連絡先情報を追加します。
5. **Download log**をクリックしてログをダウンロードします。このページには、進行状況バーが表示されます。

図93ログのダウンロード



6. 表示されたログエントリをローカルサーバー上の.sdsファイルに保存します。

SOL接続

SOL機能がイネーブルになっているときに接続するシリアルポートを選択するには、次の作業を実行します。

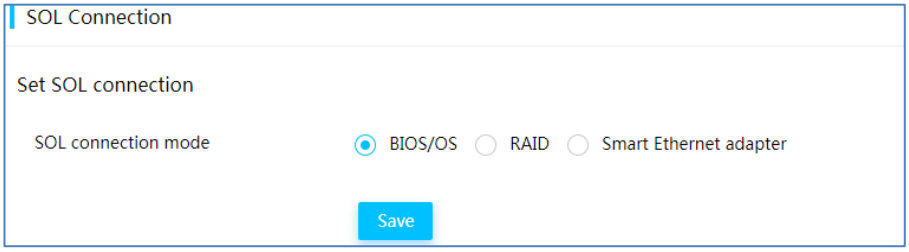
前提条件

SOL接続モードを設定する前に、SOL機能が無効になっていることを確認します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**SOL Connection**を選択します。
3. 作業ペインで、**SOL connection mode**フィールドからシリアルポートを選択します。
4. **save**をクリックします。

図94 SOL接続の設定



パラメーター

- **BIOS/OS**:BIOSまたはOSのシリアルポートに接続します。
- **RAID**:メザニンストレージコントローラーのシリアルポートに接続します。
- **Smart Ethernet adapter**:スマートネットワークアダプターのシリアルポートに接続します。一部のスマートネットワークアダプターのみがシリアルポート接続をサポートします。

スクリーンショットとビデオ

ビデオ録画を有効にする

この機能は、クラッシュ、再起動、シャットダウンなどの重大なオペレーティングシステムイベントが発生したときのサーバーのステータスを記録します。これらのビデオを再生して、記録されたイベントを分析またはトラブルシューティングできます。

前提条件

KVMサービスがユーザーカウントに対して有効になっていることを確認します。KVMが有効になっていない場合は、管理者に連絡してください。

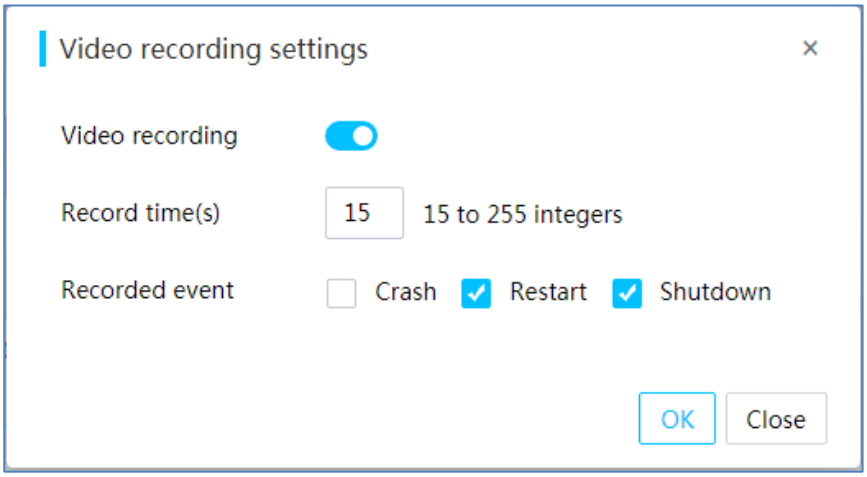
イベントがビデオ録画をトリガーしたときにリモートコンソールが開いている場合、ビデオ録画は失敗します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Screenshots & Videos**を選択します。
3. 作業ウィンドウで、**Configure**をクリックします。
4. 表示されたダイアログボックスで、ビデオ録画を有効にします。
5. ビデオ長を設定します。値の範囲は15～255秒です。
6. 記録するイベントのタイプ(クラッシュ、再起動、またはシャットダウン)を選択します。

   クラッシュイベントの記録は、WindowsおよびLinuxオペレーティングシステムで使用できます。
7. **save**をクリックします。

図95 ビデオ録画の設定



ビデオの再生と管理

ビデオ再生ページでは、録画したビデオを再生、ダウンロード、および削除できます。

システムは最大3つのビデオファイルをサポートします。3つのビデオファイルがすでに存在する場合は、新しいビデオファイルによって最も古いビデオファイルが上書きされます。ファイルの作成時間はファイルのプロパティに記録されます。

制限事項とガイドライン

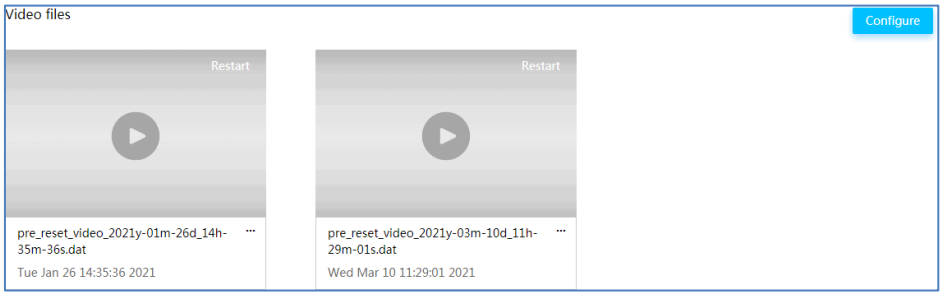
イベントが発生したときにオペレーティングシステムがスリープ状態であった場合、HDMはビデオの代わりにno signalメッセージを表示します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Screenshots & Videos**を選択します。

3. **Video files**セクションで、再生するビデオをクリックします。
4. ビデオをダウンロードするには、ビデオがロードされたら**Download**をクリックします。
5. ビデオを閉じるには、**Cancel**をクリックします。
6. ビデオを削除するには、ビデオの右下隅にあるアイコン ··· をクリックし、**Delete**をクリックします。

図96 ビデオを再生する



BSoDスクリーンショットの表示

この機能は、今後のトラブルシューティングのために、Windowsのシステムクラッシュ時に自動的にブルースクリーンオブデス(BSoD)スクリーンショットを取得します。HDMは最大10個のBSoDスクリーンショットを保存できます。これらのスクリーンショットには、シーケンス番号とスクリーンショット時間の名前が付けられます。スクリーンショットの最大数に達すると、新しいBSoDスクリーンショットによって最も古いものが上書きされます。

前提条件

KVMサービスがユーザーカウントに対して有効になっていることを確認します。KVMが有効になっていない場合は、管理者に連絡してください。

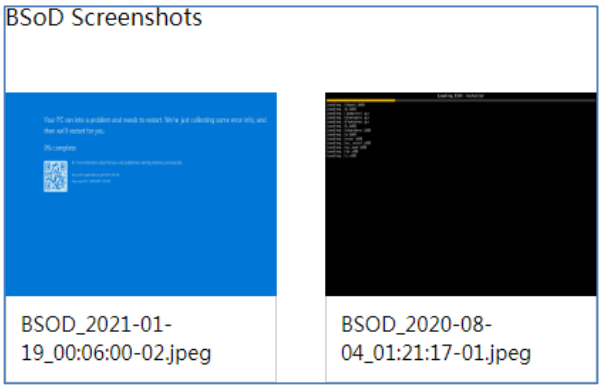
制限事項とガイドライン

サーバーにWindows以外のオペレーティングシステムがインストールされている場合は、サーバーがMCAエラーを検出したときに、HDMもMCAトリガーのスクリーンショットを取得します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Screenshots & Videos**を選択します。
3. ページに一覧表示されているBSoDスクリーンショットを表示します。

図97 BSoDスクリーンショットの表示



アラームの設定

この機能を使用して、次の操作を実行します。

- エラーが発生したおよびMCAポリシーなど、エラーが発生したときのサーバーのアラートポリシーを構

成します。

- 電子メール、SNMPトラップ、またはsyslogメッセージを送信して、関連するサーバー管理スタッフメンバーにサーバーイベントを通知し、迅速なアクションを実行します。
- サーバーのシステム診断を設定します。

アラートポリシーの管理

NMIデバッグを有効にする

この機能により、オペレーティングシステムデバッガは、マスク不可能な割り込みを生成することで、ソフトウェアのロックアップ問題をデバッグするのに役立ちます。

制限事項とガイドライン

Non Maskable Interrupt(NMI)デバッグ機能は、デバッグ専用です。サーバーが正常に動作している場合は、この機能を使用しないでください。

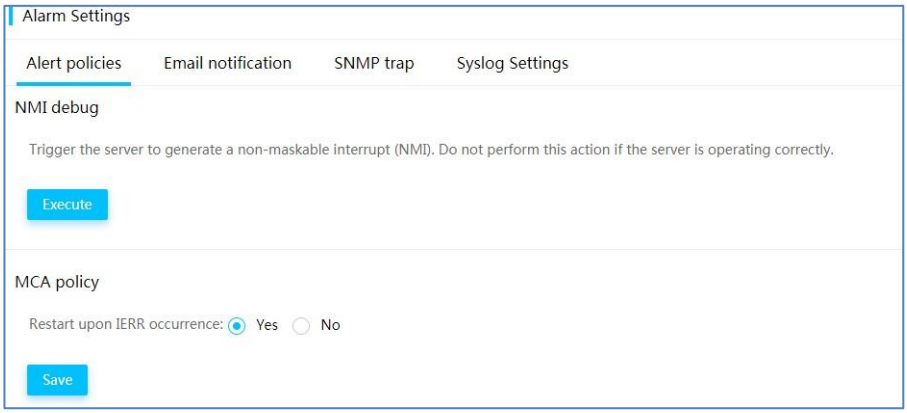
前提条件

オペレーティングシステムがNMIを処理できることを確認します。オペレーティングシステムがNMIを処理できない場合は、NMIデバッグを使用すると、オペレーティングシステムがクラッシュする可能性があります。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. 作業ウィンドウの**NMI debug**セクションで、**Execute**をクリックします。

図98 NMIデバッグの有効化



MCAポリシーを設定する

MCA(Machine Check Architecture)は、エラー報告とエラー回復を可能にするIntelのメカニズムです。IERRには、プロセッサーエラー、メモリーエラー、およびPCIeエラーが含まれます。IERRが発生したときにサーバーを自動的に再起動するかどうかを設定するには、次の作業を実行します。

R4950 G3、R4950 G5、およびR5500 G5 AMDサーバーは、MCAをサポートしません。

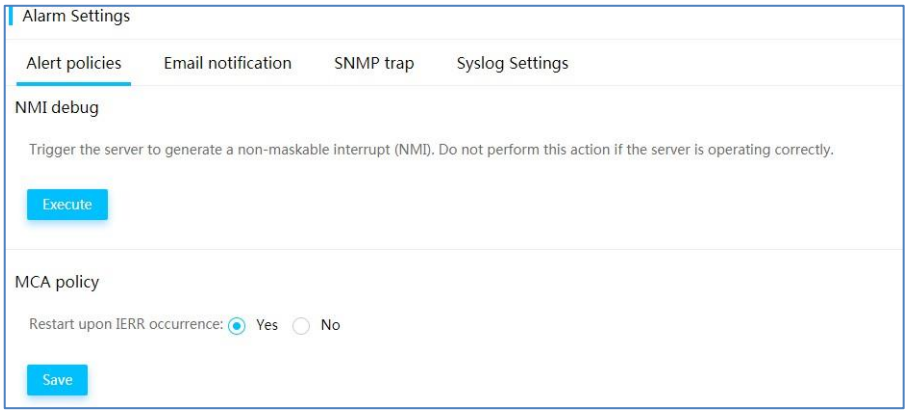
制限事項とガイドライン

MCAポリシーは、OS再起動ポリシーには影響しません。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. 作業ペインの**MCA policy**セクションで、**Restart upon IERR occurrence**フィールドから**Yes**または**No**を選択します。
4. **save**をクリックします。

図99 MCAポリシーの設定



アラートメールの管理

HDMは、Simple Mail Transfer Protocol(SMTP)を介してアラート電子メールを送信します。アラート電子メールをユーザーに送信するには、SMTPを設定し、そのユーザーを電子メール受信者として指定し、そのユーザーのアラートポリシーを設定する必要があります。

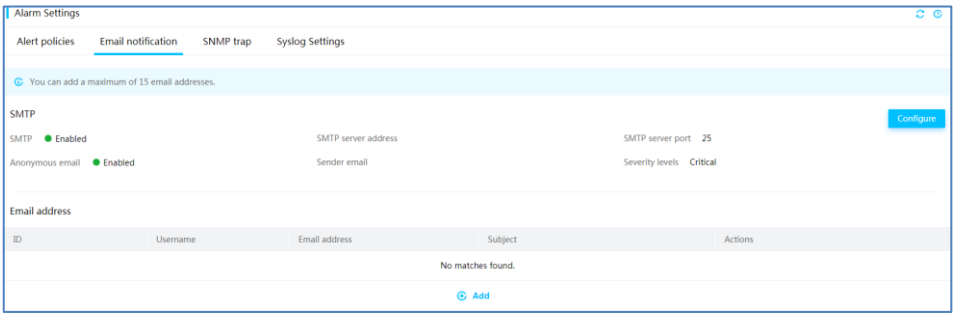
前提条件

電子メールの受信者のユーザーカウントに電子メールアドレスが指定されていることを確認します。ユーザーカウントの電子メールアドレスの追加の詳細は、「ユーザーカウント」を参照してください。

アラートメール用にSMTPを設定する

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **Email notification**タブをクリックします。
4. **SMTP**セクションで、**Configure**をクリックします。
5. 表示されたダイアログボックスで、SMTPを設定します。
   - **Enable for SMTP**を選択します。
   - SMTPサーバーのアドレスとポート番号を入力します。
   - 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、**Enable for anonymous email**を選択します。送信者のID情報を使用してアラート電子メールを送信するには、**Enable for anonymous email**を選択解除し、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。ユーザー名には、文字、数字、アンダースコア(_)およびアットマーク(@)のみを使用できます。
   - 送信者の電子メールアドレスを入力します。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ます。
   - 重要度レベルを選択します。オプションには、**Critical**、**Minor+Major+Critical**および**All**があります。
6. **OK**をクリックします。

図100 アラート電子メール用のSMTPの設定



アラート電子メール受信者を追加する

1. ユーザーにアラート電子メールを受信させるには、**Users & Security > User Accounts**ページでユーザーカウントを設定するときに、そのユーザーの電子メールアドレスを指定する必要があります。
2. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
3. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
4. **Email notification**タブをクリックします。
5. **Add**をクリックします。
6. 表示されたダイアログボックスで、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。電子メールアドレスを編集するには**Here**リンクがあります。
7. 電子メールの件名を入力します。電子メールの件名には、文字、数字およびアンダースコア(_)のみがサポートされています。
8. **Test**をクリックしてテスト用の電子メールを送信し、**Result**をクリックしてテスト結果を表示します。
9. 受信者の設定を編集するには、電子メールの受信者エントリで**Edit**をクリックします。
10. 受信者を削除するには、電子メールの受信者エントリで**Delete**をクリックします。

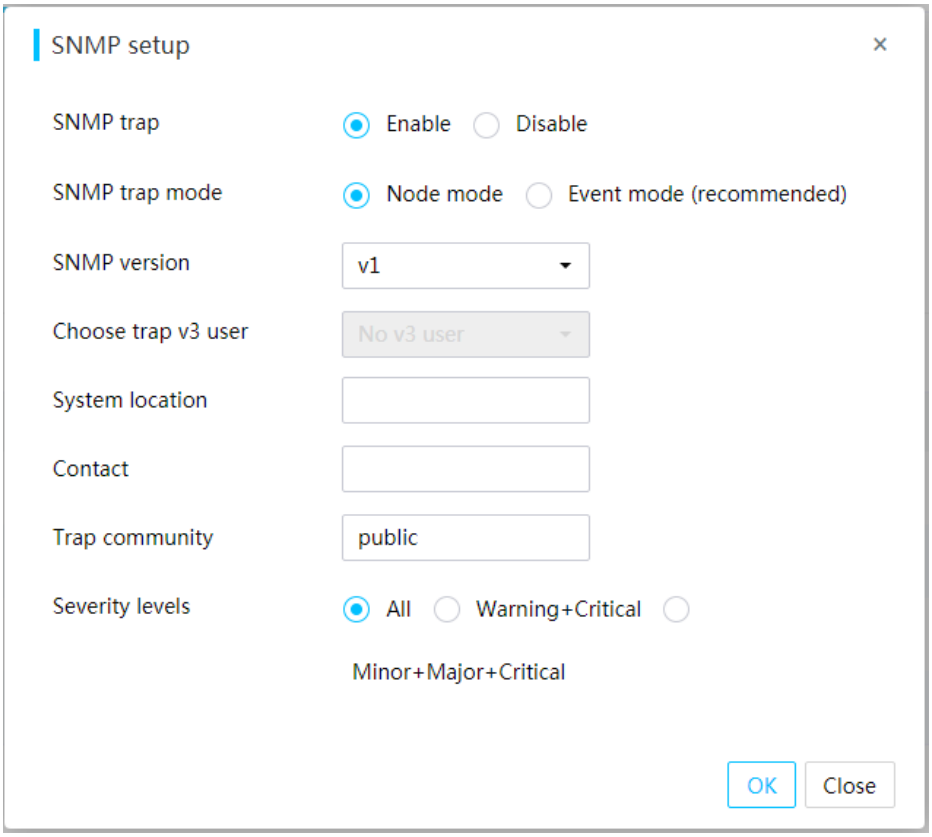
SNMPトラップの管理

SNMPトラップのサーバーイベントをSNMP管理ワークステーションに送信できます。

SNMPトラップ設定の構成

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **SNMP trap**タブをクリックします。
4. **SNMP trap settings**セクションで、**Configure**をクリックします。
5. 表示されたダイアログボックスで、SNMPトラップの設定を行います。
   a. **Enable for SNMP trap**を選択します。
   b. SNMPトラップモードを選択します。オプションには、**Node mode**と**Event mode**(推奨)があります。
   c. SNMPバージョンを選択します。SNMPv3が選択されている場合は、**Choose trap v3 user**フィールドにもSNMPv3ユーザーを指定する必要があります。
   d. (任意)サーバーの場所と連絡先情報を入力します。
   e. コミュニティ名を入力します。
   f. 重大度レベルを選択します。
6. **OK**をクリックします。

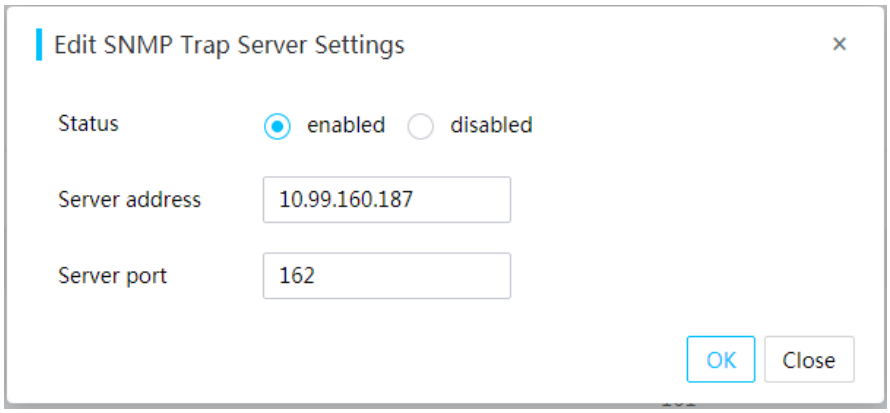
図101 SNMPトラップ設定の構成



SNMPトラップサーバー設定の構成

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **SNMP trap**タブをクリックします。
4. **SNMP trap server settings**セクションで、サーバーエントリの**Edit**をクリックします。
5. 表示されたダイアログボックスで、SNMPトラップサーバーのパラメーターを設定します。

図102 SNMPトラップサーバー設定の構成



6. **save**をクリックします。
7. (任意)サーバーエントリで**Test**をクリックして、テスト電子メールを送信します。

パラメーター

- **Node mode**: SNMPノードのOIDをトラップイベントのIDとして指定します。これはデフォルトモードです。
- **Event mode** (推奨):トラップイベントとのマッピング関係にあるSNMPノードのOIDをイベントのIDとして指定します。このモードで提供される情報の方が正確です。
- **SNMP version**: SNMPバージョンを選択します。オプションには、SNMPv1、SNMPv2c、およびSNMPv3があります。
- **Choose trap v3 user**: SNMPv3トラップを送信するためにシステムで使用されるユーザー名を選択します。
- **System location**: サーバーの場所(最大31バイトの文字列)を入力します。
- **Contact**: 連絡先情報を最大31バイトの文字列で入力します。
- **Trap community**: マネージャで認証するためのトラップコミュニティストリングを入力します。値の範囲は1～18文字です。デフォルト値は**public**です。
- **Severity levels:** Severityを選択します。オプションには、**Critical**、**Minor + Major + Critica**および**All**があります。
- **No.** : エントリ番号。各エントリに1つずつ、最大4つのサーバーを指定できます。このフィールドは編集できません。
- **Status**: 指定したサーバーに対してトラップ通知が有効かどうかを示します。
- **Server address** :宛先ホストのIPアドレスまたはドメインアドレス。
- **Server port**: 宛先ホストがSNMPトラップを受信するポート番号を入力します。値の範囲は1～65535です。デフォルトのポート番号は162です。

備考

System location、**Contact**、および**Trap community**フィールドには、文字、数字、および次の特殊文字だけを含めることができます。

`~!@$%^&*()_+-={}:,./?

Syslog設定の管理

Syslogメッセージを使用して、宛先ホストに動作、イベント、およびセキュリティログをレポートするには、次の作業を実行します。

制限事項とガイドライン

syslog通知設定を変更すると、syslogサーバー設定はデフォルトに復元されます。

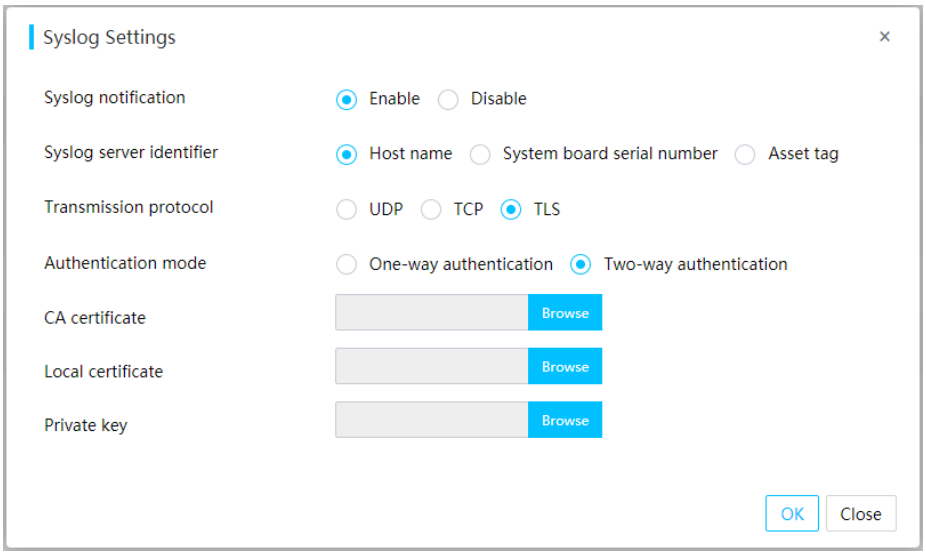
前提条件

syslog通知をイネーブルにする前に、syslogサーバーが使用可能であることを確認します。

syslog通知設定を構成する

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **Syslog Settings**タブをクリックします。
4. **Syslog notification settings**セクションで、**Configure**をクリックします。
5. 表示されたダイアログボックスで、**Enable** for **Syslog notification**を選択します。
6. syslogサーバーの識別子を選択します。
7. 伝送プロトコルを選択します。**TLS**を選択する場合は、認証モードを選択し、CA証明書、ローカル証明書、および秘密キーファイルをアップロードする必要があります。
8. **OK**をクリックします。

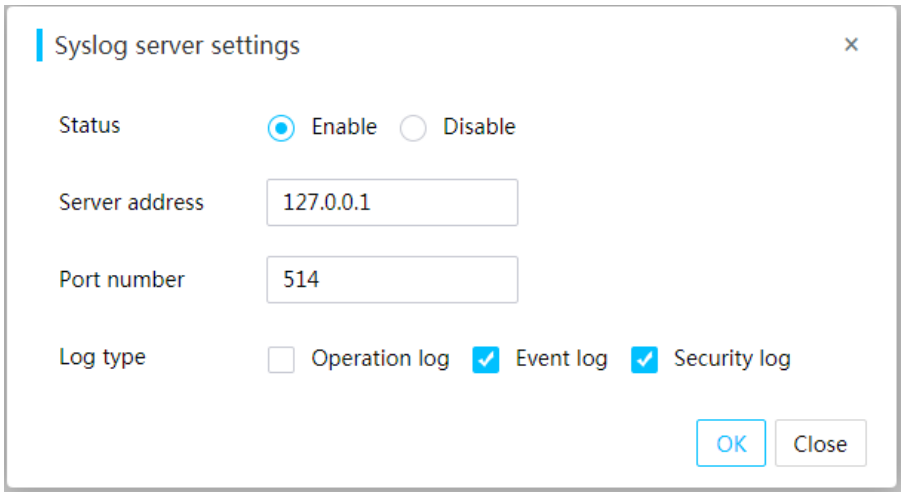
図103 syslog通知設定の構成



syslogサーバー設定の構成

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **Syslog Settings**タブをクリックします。
4. **Syslog server settings**セクションで、サーバーエントリの**Edit**をクリックします。
5. 表示されたダイアログボックスで、syslogサーバーのパラメーターを設定します。
6. **save**をクリックします。

図104 Syslogサーバーの設定



パラメーター

- **Syslog server identifier**: syslogサーバー識別子を選択します。オプションには、**Host name**、**System board serial number**、および**Asset tag**があります。
- **Transmission protocol**: syslogメッセージの送信に使用する送信プロトコルを選択します。次のオプションがあります。
  - **TCP**: データ送信の前に送信側と受信側の間で接続を確立する必要があるコネクション型プロトコル。
  - **UDP**: データ送信前に送信側と受信側の間で接続を確立する必要のないメッセージ指向プロトコル。
  - **TLS**:コネクション型のプロトコルで、送信側と受信側の間にプライバシーとデータの整合性を提供します。

- **Authentication mode**:認証モードを選択します。次のオプションがあります。
  - **One-way authentication**:syslogサーバーだけを認証します。
  - **Two-way authentication**:HDMログインに使用されるsyslogサーバーとクライアントの両方を認証します。
- **CA certificate**: syslogサーバーから送信されるパケットを認証するために、PEM形式のCA証明書をアップロードします。
- **Local certificate**: ローカル証明書をPEM形式でアップロードします。この証明書の情報は、HDMによってsyslogサーバーに送信されるパケットで伝送され、サーバーがHDMログインに使用されるクライアントを認証するために使用されます。
- **Private key**: 秘密キーファイルをPEM形式でアップロードして、ローカル証明書を復号化します。
- **No.** : エントリ番号。各エントリに1つずつ、最大4つのサーバーを指定できます。このフィールドは編集できません。
- **Server Address**: 宛先ホストのIPアドレスを入力します。デフォルトのIPアドレスは127.0.0.1です。
- **Server port**: 宛先ホストがsyslogメッセージを受信するポート番号を入力します。値の範囲は1～65535です。デフォルトのポート番号は514です。
- **Log Type**: レポートされるログのタイプ。オプションには、Operation Log、Event LogおよびSecurity log。

システム診断を構成する

ハードウェア交換エラーのためにサーバーがPOSTフェーズでスタック状態になった場合に、最小構成の起動または診断の隔離を実行するには、次の作業を実行します。

最小構成スタートアップにより、システムは、1つのCPU、1つのコア、および1つのチャネル内のメモリーモジュールを使用して、SATA M.2 SSDにインストールされたUEFI SHELLまたはOSを起動できます。

診断の分離により、システムはハードウェアコンポーネントを診断し、障害が発生したコンポーネントを分離してから起動できます。

制限事項とガイドライン

この機能は、HDM-2.26以降でのみ使用できます。

この機能は使用できるのは、R4700 G5、R4900 G5、およびR5300 G5サーバーだけです。この作業を実行する

前に、BIOSが更新されていないことを確認してください。

最小設定の起動と診断の隔離の両方をイネーブルにすると、診断の隔離だけが有効になります。

このセクションでのサーバーの再起動は、**Power Management**ページの**Force power-cycle**オプションをクリックしてトリガーされる電源再投入を参照します。

最小構成スタートアップモードまたは診断隔離モードでは、サーバーのUSBコネクターが無効になり、HDMにワイヤレスでアクセスできなくなります。最小構成スタートアップモードまたは診断隔離モードを有効にする前に、必要に応じてバックアップネットワークアクセスを準備します。

診断プロセスには長い時間がかかります。プロセスを中断するには、最初にWebインターフェースからの診断の分離を無効にし、次にサーバーを再起動します。診断の分離モードを変更するには、Webインターフェースからの診断の分離を無効にし、サーバーを再起動して現在のモードを終了し、新しいモードを設定し設定してから、サーバーを再起動します。

診断の前に、システムはサーバー上で事前チェックを実行します。サーバーが正常に起動した場合、または事前チェック中にUEFI SHELL最小起動が失敗した場合、システムは診断プロセスを終了します。

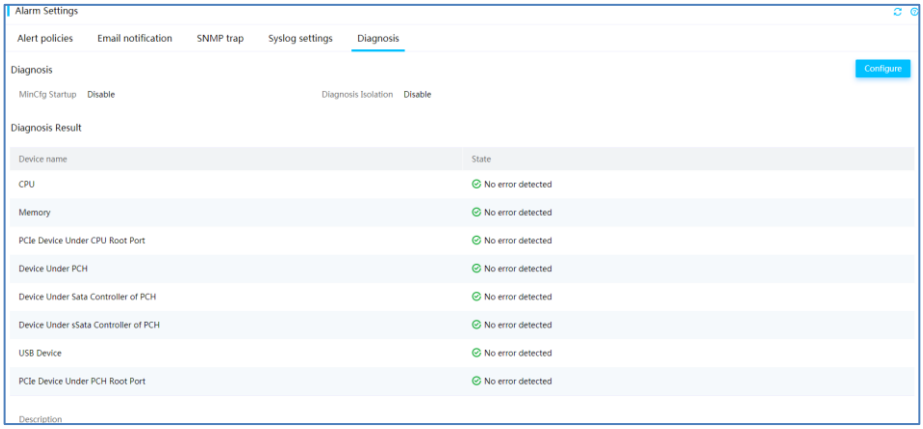
最小構成の起動では、起動しないデバイスはBIOSによって分離され、HDMでは識別できません。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Alarm Settings**を選択します。
3. **Diagnosis**タブをクリックします。

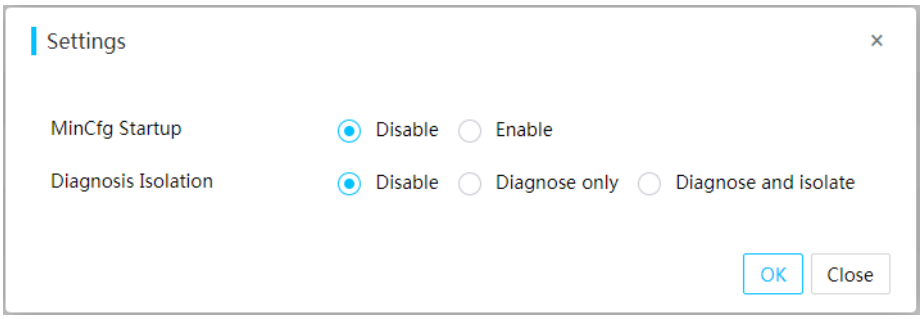
   開いたページには、現在の最小構成のスタートアップ構成と診断の分離構成が表示されます。

   図105 システム診断の表示



4. **Configure**をクリックします。
5. 表示されたダイアログボックスで、最小構成の起動を有効にするか、診断分離モードを選択します(図106を参照)。

   図106 システム診断の構成



6. **OK**をクリックします。
7. サーバーを再起動します。設定された最小構成スタートアップモードまたは診断分離モードは、再起動後すぐに有効になります。

パラメーター

Diagnosis isolation : 診断の分離モードを選択します。次のオプションがあります。

- **Disable** : 診断の隔離をディセーブルにします。
- **Diagnose only** : コンポーネントの起動失敗の原因となるエラーを調べ、診断結果を表示します。
- **Diagnose and isolate**: コンポーネントの起動失敗の原因となるエラーを調べ、診断結果を表示してから、失敗したコンポーネントを分離します。

構成

HDM、BIOS、またはRAID設定をインポートおよびエクスポートし、HDM設定を復元するには、次の作業を実行します。

制限事項とガイドライン

HDM、BIOS、またはRAID構成のエクスポート

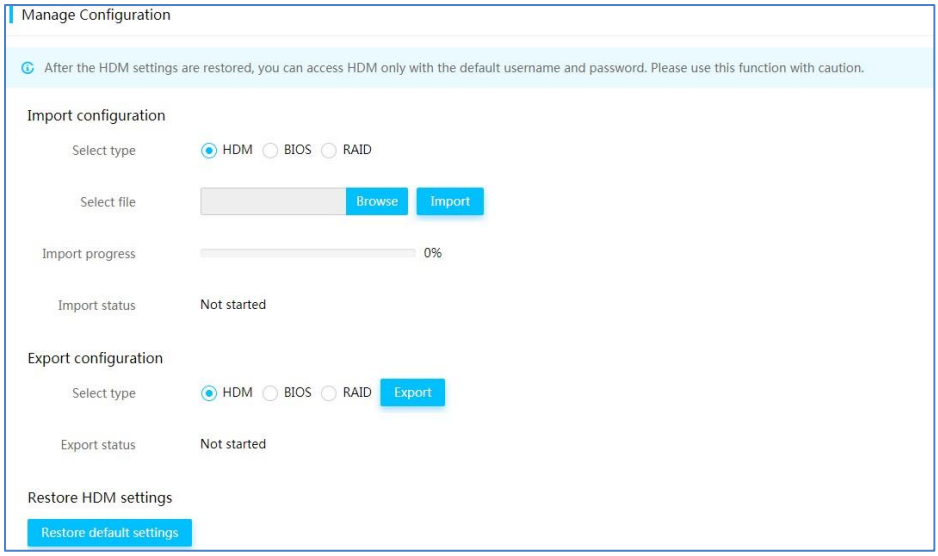
制限事項とガイドライン

RAID構成をエクスポートする前に、ストレージコントローラーが初期化されていることを確認してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Manage Configuration**を選択します。
3. **Export configuration**セクションで、**Select type**からターゲットコンフィギュレーションタイプを選択します。
4. **Export**をクリックします。

図107 HDM、BIOS、またはRAID構成のエクスポート



HDM、BIOS、またはRAID構成のインポート

一般的な制限事項とガイドライン

HDMおよびオペレーティングシステムの異常を避けるために、インポートプロセス中はサーバーで電源操作を実行しないでください。

設定のインポートに失敗した場合は、指示に従って失敗につながる問題をトラブルシューティングしてから、設定を再度インポートします。

インポートの失敗を避けるために、構成ファイルを変更するときは、構成が有効であることを確認してください。

インポートする前に、コンフィギュレーションファイル内のすべてのコメント文を削除していることを確認します。

インポートする構成のパスワードが空で、構成が別のサーバーからのものである場合は、パスワードを手動で追加する必要があります。新しいパスワードはインポート後に有効になります。

HDM設定のインポートに関する制約事項およびガイドライン

インポートする構成ファイル内のサーバーモデルが実際のサーバーモデルと一致していることを確認してください。

インポートする構成ファイルの結合モード設定が、ターゲットサーバーの結合モード設定と一致していることを確認してください。

インポート操作は、インポートするコンフィギュレーションファイルに含まれていないHDMコンフィギュレーションには影響しません。

インポートされたHDM設定にネットワーク設定が含まれている場合、HDMは設定を有効にするためにインポート後に自動的に再起動します。インポートされたHDM設定にネットワーク設定が含まれていない場合、設定はインポート後すぐに有効になります。

BIOS設定のインポートに関する制限事項およびガイドライン

構成ファイル内のサーバーモデルとハードウェア構成(たとえば、ストレージコントローラーとドライブ構成)が実際の構成と一致していることを確認します。

インポートされたBIOS設定を有効にするには、インポート後にサーバーを再起動します。

RAID構成のインポートに関する制限事項およびガイドライン

RAID構成をインポートする前に、サーバーの電源が入っており、ストレージコントローラーがRAIDモードになっていることを確認します。

構成ファイル内のサーバーモデルとハードウェア構成(たとえば、ストレージコントローラーとドライブ構成)が実際の構成と一致していることを確認します。

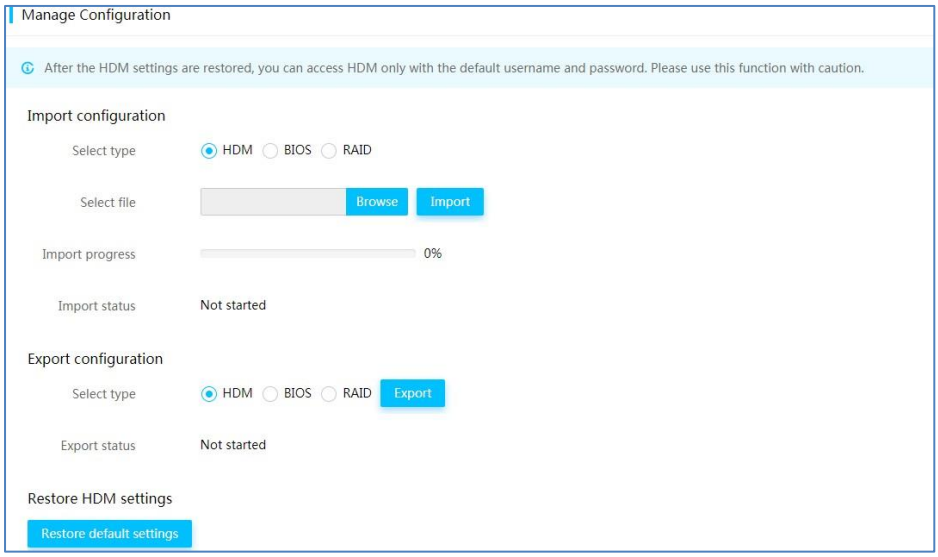
インポートの失敗を回避するには、RAID構成をインポートする前に、BIOSから既存のRAID構成をクリアします。

RAID構成のインポート後、インポートされたファイルが有効になるまで約40秒かかります。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Manage Configuration**を選択します。
3. **Import configuration**セクションで、**Select type**フィールドから**HDM**を選択します。
4. ターゲットコンフィギュレーションファイルを選択し、**Import**をクリックします。
5. 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108 HDM、BIOS、またはRAID構成のインポート



HDM設定の復元

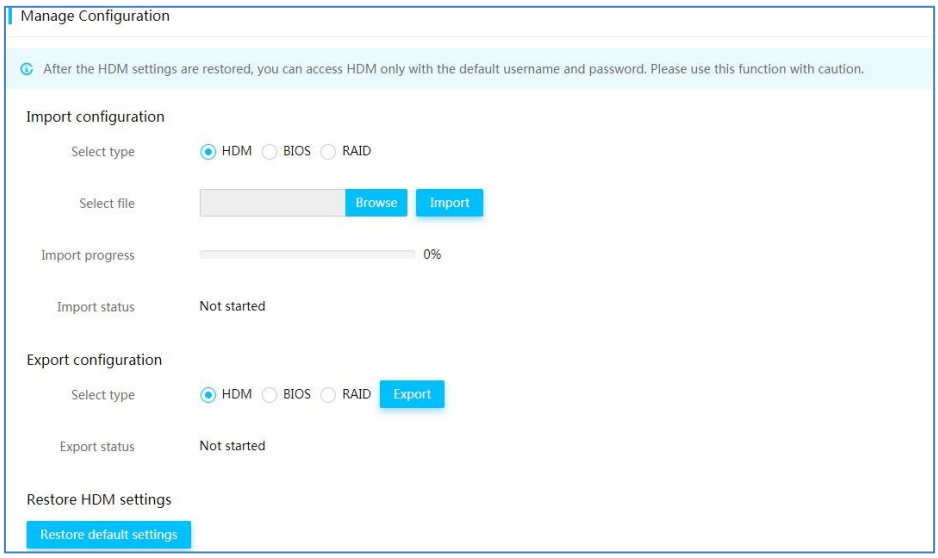
△注意:

- HDM設定が復元された後は、デフォルトのユーザー名とパスワードでのみHDMにアクセスできます。この機能は注意して使用してください。
- HDM設定が復元されているときは、Webページを更新しないでください。ページを更新すると、HDMにアクセスできなくなる可能性があります。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Manage Configuration**を選択します。
3. **Restore HDM settings**セクションで、次のいずれかのタスクを実行します。
   - HDMをデフォルト設定に戻すには、**Restore default settings**をクリックします。
   - HDMを工場出荷時のデフォルトに戻すには(ある場合)、**Restore factory defaults**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。設定が復元されると、HDMが再起動します。

図109 HDM設定の復元



ファームウェアの更新

HDM、BIOS、CPLD、電源装置、LCD、またはGPUFPGAのファームウェアを更新できます。表12は、サーバーモデルとそれらがサポートするファームウェアタイプを示しています。

表12サーバーモデルおよびサポートされるファームウェアタイプ

サーバーモデル	ファームウェアタイプ
• R2900 G3 • R4100 G3 • R4400 G3 • E3200 G3 • B5700 G3 • AE100	• HDM • BIOS • CPLD
R4900 G3	• HDM • BIOS • CPLD • BPCPLD • PSU
• R2700 G3 • R4300 G3 • R4700 G3 • R4950 G3 • B5800 G3	• HDM • BIOS • CPLD • BPCPLD
R5300 G3	• HDM • BIOS • CPLD

	• PSU • GPUCPLD • BPCPLD
R6700 G3	• HDM • BIOS • CPLD • DBCPLD • STBCPLD • LCD • BPCPLD
R6900 G3	• HDM • BIOS • CPLD • PDBCPLD • NDCPLD • BPCPLD • LCD
R8900 G3	• HDM • BIOS • CPLD • BPCPLD • PDBCPLD • NDCPLD • PDBSCPLD • LCD
B7800 G3	• HDM • BIOS • CPLD • AUXCPLD
• R4700 G5 • R4900 G5 • R4950 G5	• HDM • BIOS • CPLDI • BPCPLD • PSU • LCD • PFRCPLD
R5300 G5	• HDM • BIOS • CPLD • BPCPLD • PSU • PFRCPLD • OCPCPLD • GPUFPGA
R5500 G5	• HDM • BIOS • CPLD • BPCPLD • PFRCPLD • PSWCPLD

	• PSU
R6900 G5	• HDM • BIOS • CPLD • DBCPLD • BPCPLD • PSU • LCD • PFRCPLD • OCPCPLD
B5700 G5	• HDM • BIOS • CPLD • PFRCPLD

ファームウェア更新の制限とガイドライン

ファームウェアを正常に更新するには、更新中に次の制約事項および注意事項に従ってください。

- 更新中は、サーバーの電源を入れたり切ったりしないでください。HDMエラーまたはオペレーティングシステムエラーが発生する可能性があります。
- 指示がない限り、更新中にHDM Webページを更新しないでください。更新を行うと、更新プロセスがリセットされます。

一度に1人のユーザーのみがファームウェアを更新できます。複数のユーザーがファームウェアを更新しようとした場合、この操作を実行できるのは最初に更新を開始したユーザーのみです。ファームウェアの更新が正常に開始されると、HDMは自動的に他のすべてのWebページを無効にし、他のすべてのユーザーをサインアウトします。サインアウトされたユーザーは、更新が完了した後にのみ再度サインインできます。

更新イメージファイルにベンダーの署名が含まれていない場合、または更新イメージファイルが破損している場合は、ファームウェアの更新が失敗する可能性があります。このような場合は、目的のファームウェアイメージファイルを入手して、再度実行してください。

ファームウェアを正常に更新するには、更新プロセス中にWebインターフェースから次のタスクを実行しないでください。

- 専用および共有ネットワークポート、VLAN、ネットワークポートモード、ネットワークアダプター、DNS、およびWi-Fi設定などのネットワーク設定を変更します。
- リモートサービスを設定します。
- NTP設定を構成します。
- アクセスサービス、ファイアウォール、SSLなどのユーザーおよびセキュリティ設定を構成します。
- サーバーの電源ステータスを設定するか、消費電力上限設定を変更します。
- 次のリモート操作およびメンテナンスタスクを実行します。
  - NMI制御を行います。
  - 設定をインポートまたはエクスポートします。
  - HDM設定を復元します。
  - HDMを再起動します。
  - プライマリ/バックアップスイッチオーバーを実行します。
  - CPLDを再起動します。

CPLDの更新に失敗すると、サーバーは使用できなくなります。サーバーにアクセスできない場合は、テクニカルサポートに連絡してください。

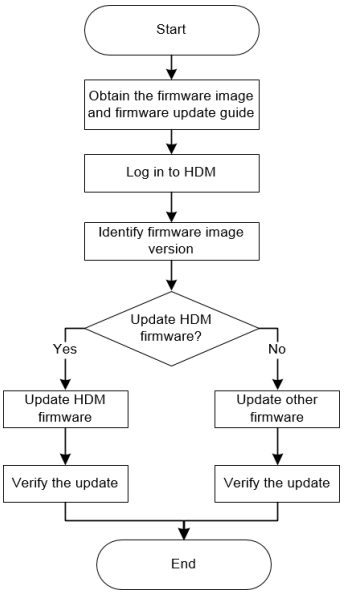
次のリモートコンソールメニューは、更新中は使用できません。

- KVMコンソールの**Keyboard**メニュー。
- H5 KVMコンソールの**Send Keys**および**Hot Keys**メニュー。

ファームウェア更新のワークフロー

図110に、ファームウェア更新ワークフローを示します。

図110 ファームウェアの更新ワークフロー



ファームウェア更新の前提条件

ファームウェアを更新する前に、次の作業を実行します。

1. 最新のサーバーファームウェアイメージを入手します。イメージがファームウェアタイプと一致していることを確認します。
2. 不注意による設定の損失を避けるために、設定をバックアップします。バックアップ用にHDM設定をエクスポートできます。
3. ファームウェアを更新しているユーザーがいないことを確認します。ファームウェアの更新が進行中の場合は、ファームウェアを更新できません。

HDMファームウェアの更新

HDMは、1つのプライマリファームウェアイメージと1つのバックアップファームウェアイメージをサポートし、常にプライマリイメージを実行します。

HDMサービスへの影響を最小限に抑えるために、HDMは次の方法を使用してHDMファームウェアを更新します。

1. HDMファームウェアを更新すると、HDMはバックアップファームウェアイメージをアップロードされた更新イメージで置き換えます。
2. HDMを再起動するか、プライマリ/バックアップのスイッチオーバーを実行すると、HDMはプライマリおよびバックアップHDMイメージのロールを変更します。その後、HDMは更新イメージ(現在はプライマリイメージ)で再起動します。

制限事項とガイドライン

Restore factory defaultsオプションが選択されている場合は、HDMのファームウェアが更新された後の最初のサインインで、デフォルトのユーザーカウント設定を使用する必要があります。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

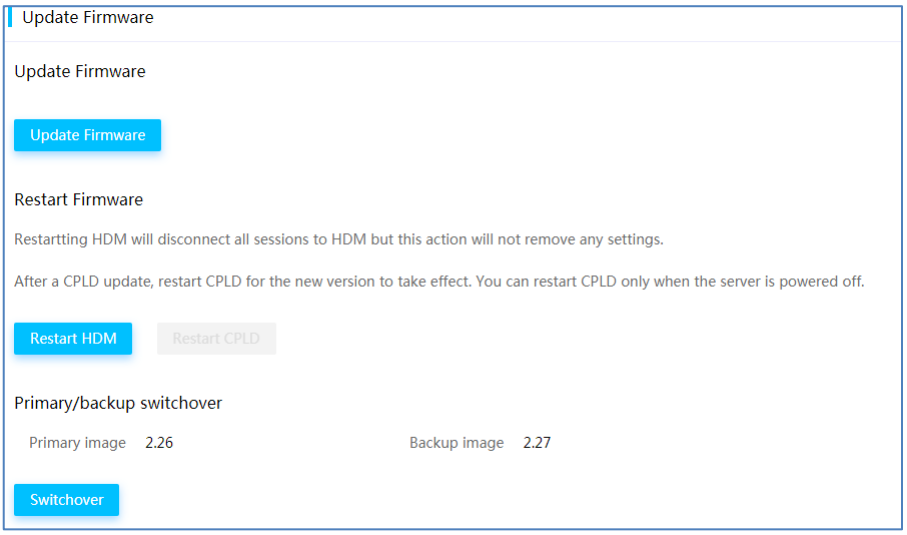
前提条件

「ファームウェア更新の前提条件」を参照してください。

手順

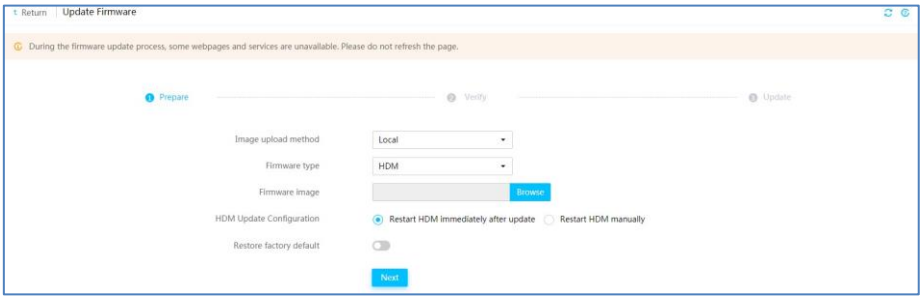
1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。図111に示すページが開きます。

図111 ファームウェアの更新



3. **Update Firmware**セクションで、**Update Firmware**をクリックします。
   図112に示すファームウェアイメージファイルのアップロードページが開きます。

図112 ファームウェアイメージファイルのアップロード



4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**HDM**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択した場合は、ファイルのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**HDM**を選択します。イメージ名にはサフィックスを含める必要があり、45文字を超えることはできません。
   b. 更新完了後にHDMを再起動する方法を選択します。更新完了時にHDMを自動的に再起動することも、後でHDMを手動で再起動することもできます。
   c. (任意)HDMファームウェアの更新後にユーザーが設定したすべての設定を削除するには、**Restore factory default**オプションをイネーブルにします。
   d. **Next**をクリックします。

△注意:

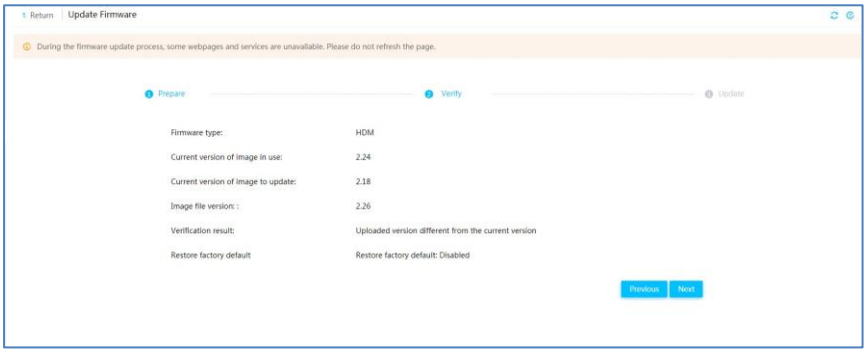
Restore factory defaultsオプションを選択すると、HDMが新しいファームウェアで起動したときに、ユーザーが構成したすべての設定が削除され、工場出荷時のデフォルトに戻ります。ファームウェアに工場出荷時のデフォルトが設定されていない場合、システムはファームウェアのデフォルト設定を復元します。このオプションを選択するときは、サービスへの影響を理解してください。

5. 使用中のイメージの現在のパーティションバージョン、更新するイメージの現在のパーティションバージ

ョン、およびイメージファイルのバージョンが正しいことを確認し、**Next**をクリックします(図113を参照)。

ファームウェアの更新が開始され、更新の進行状況が表示されます。

図113 ファームウェア情報の確認



6. システムの指示に従って更新を完了します。
7. 手動再起動を選択した場合は、次のいずれかの方法を使用して、新しいファームウェアイメージを有効にします。
   - HDMを再起動します。
   - プライマリとバックアップのHDMファームウェアイメージを切り替えます。自動再起動を選択した場合、HDMは自動的に再起動します。
8. (任意)ブラウザーキャッシュをクリアしてから、HDMに再サインインします。

   ブラウザーキャッシュをクリアすると、HDMに再サインインした後にWebページの内容が正しく表示されます。
9. 更新を確認します。
   a. 上部のナビゲーションバーで、**Dashboard**をクリックします。
   b. 左側のナビゲーションペインで、**Summary**を選択します。
   c. 作業ウィンドウの**Device information**セクションで、HDMファームウェアが更新されていることを確認します。

BIOSファームウェアの更新

制限事項とガイドライン

アップデートエラーを回避するには、アップデート前に電源装置の冗長性が正常であることを確認します。

Restoreまたは**Forcedly restore**オプションを選択した場合は、アップデート後にBIOSのブートモードがデフォルト(UEFI)に変更されます。

更新後、新しいファームウェアを有効にするには、サーバーを再起動する必要があります。再起動中は、BIOSの更新を再度実行しないでください。実行すると、BIOSエラーが発生する可能性があります。

Intelプロセッサーを搭載したサーバーの場合は、**Forcedly restore**オプションを指定してBIOSを更新した後に、HDMから適切な電源オフを実行してサーバーを再起動しないでください。適切な電源オフを実行すると、ME例外が発生する可能性があります。

mLOMネットワークアダプターの設定はBIOSに保存されるため、BIOSの更新後に失われます。

BIOSファームウェアをダウングレードすると、ユーザーが設定したすべてのBIOS設定が失われます。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

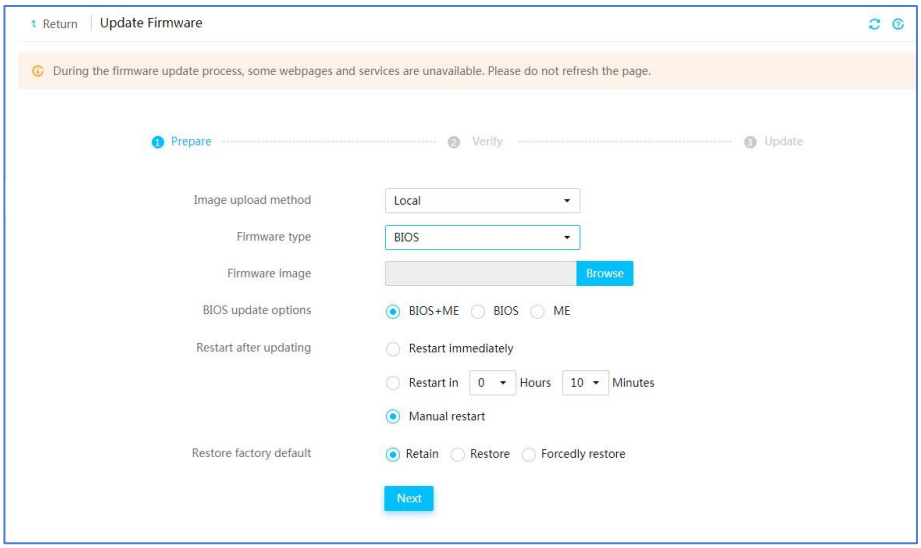
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

図114に示すファームウェアイメージファイルのアップロードページが開きます。

図114 ファームウェアイメージのアップロード



4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**BIOS**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択する場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**BIOS**を選択します。イメージ名にはサフィックスが含まれている必要があります。
   b. サーバーが起動している場合は、更新の完了後にサーバーをリブートする方法を選択します。

      サーバーをすぐに自動的に再起動することも、スケジュールされた時刻に再起動することもできます。または、**Manual restart**を選択して、サーバーを手動で再起動することもできます。
   c. 更新するファームウェアを選択します。オプションには、**BIOS+ME**、**BIOS**、および**ME**があります。デフォルトは**BIOS + ME**。
      この手順は、インテルプロセッサーを搭載したサーバーでのみ使用できます。
   d. 更新後にデフォルトのBIOS設定を復元するかどうかを選択します。更新するファームウェアとしてMEだけを指定した場合、この手順は使用できません。
      - ユーザー設定のBIOS設定を保持するには、**Retain**を選択します。
      - ユーザーが設定したBIOS設定を削除して工場出荷時のデフォルトに戻すには**Restore**を選択します。工場出荷時のデフォルトが存在しない場合、システムはデフォルト設定を復元します。
      - ユーザーが設定したBIOS設定を削除してデフォルト設定に戻すには、**Forcedly restore**を選択します。このオプションを使用すると、HDMはBIOSフラッシュを書き換えることができ、BIOSが正しく動作しておらず、他の方法で更新できない場合に使用できます。
   e. **Next**をクリックします。

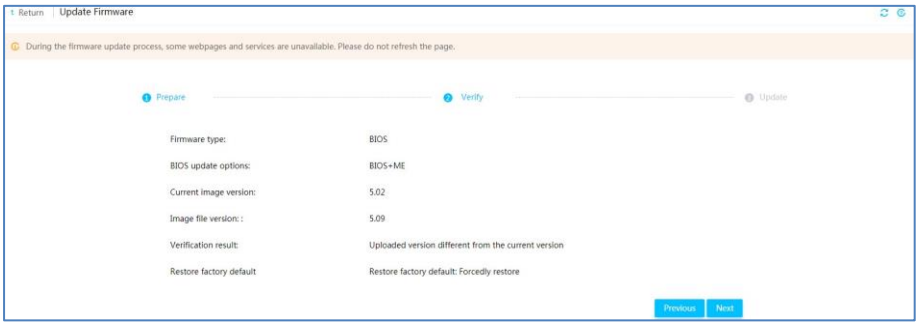
△**注意:**

Forcedly restoreオプションは、工場出荷時のデフォルト(ある場合)またはBIOSのデフォルト設定をリストアします。このオプションを選択する前に、サーバーがOSに移行しているか、電源がオフになっていることを確認してください。そうでない場合は、BIOSの例外が発生する可能性があります。このオプションを選択するときは、サービスへの影響を理解してください。

5. 図115に示すように、現在のイメージのバージョンとイメージファイルのバージョンが正しいことを確認し、**Next**をクリックします。

   ファームウェアの更新が開始され、更新の進行状況が表示されます。

   図115 ファームウェア情報の確認



6. システムの指示に従って更新を完了します。
7. サーバーの電源を再投入します。

   サーバーが起動していて、自動再起動オプションを選択した場合、サーバーは自動的に再起動します。
8. BIOSの以前のブートモードがレガシーである場合は、起動時にBIOSメニューにアクセスしてブートモードをレガシーモードに変更し、サーバーの起動を続行します。

   BIOSのブートモードは、ファームウェアを更新するたびに自動的にデフォルト(UEFI)に復元されます。この手順は、レガシーモードでインストールされたオペレーティングシステムを正常に再起動するために必要です。
9. POSTフェーズが正常に終了したら、HDMに再サインインして更新を確認します。
   a. 上部のナビゲーションバーで、**Dashboard**をクリックします。
   b. 左側のナビゲーションペインで、**Summary**を選択します。
   c. 作業ウィンドウの**Device information**セクションで、BIOSファームウェアが更新されていることを確認します。

CPLDファームウェアの更新

CPLDファームウェアのタイプ(CPLD、DBCPLD、STBCPLD、AUXCPLD、PDBCPLD、NDCPLD、PDBSCPLD、PFRCPLD、OCPCPLD)を更新するには、次の作業を実行します。

制限事項とガイドライン

「ファームウェア更新の制限とガイドライン」を参照してください。

前提条件

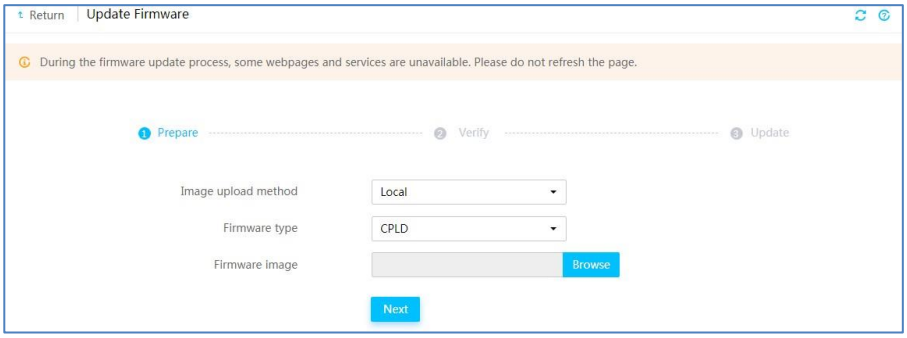
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

   図116に示すファームウェアイメージファイルのアップロードページが開きます。

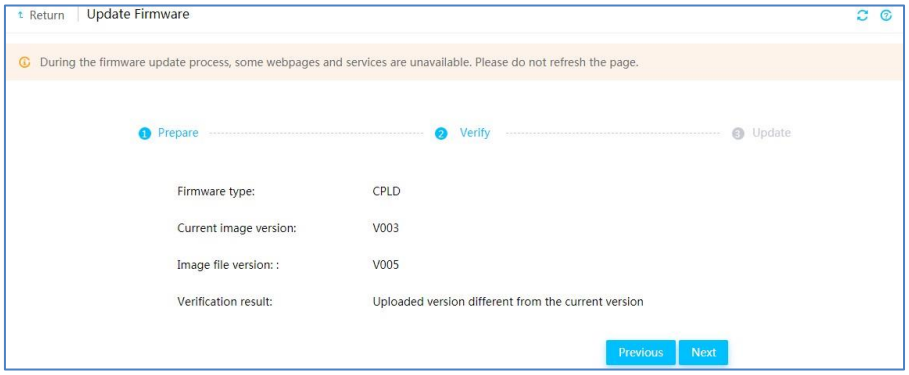
図116 ファームウェアイメージのアップロード



4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**CPLD**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択する場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**CPLD**を選択します。イメージ名にはサフィックスが含まれている必要があります。
   b. **Next**をクリックします。
5. 図117に示すように、現在のイメージのバージョンとイメージファイルのバージョンが正しいことを確認し、**Next**をクリックします。

   ファームウェアの更新が開始され、更新の進行状況が表示されます。

   図117 ファームウェア情報の確認



6. デバイスモデルに基づいて対応するタスクを実行して、新しいCPLDファームウェアバージョンを有効にします。詳細については、サーバーのファームウェアアップデートガイドを参照してください。

ドライブバックプレーンファームウェアを更新する

このタスクは、R2700 G3、R4300 G3、R4700 G3、R4900 G3、R4950 G3、R5300 G3、R6700 G3 R6900 G3、R8900 G3、B5800 G3、およびB5700 G5を除くすべてのG5サーバー。

制限事項とガイドライン

更新操作では、アップロードされたBPCPLDイメージファイルでサポートされるドライブバックプレーンだけが更新されます。

ドライブバックプレーンの交換後にファームウェアを更新するには、最初にサーバーの電源を入れて、新しく取り付けたドライブバックプレーンを識別します。

ドライブバックプレーンの更新が失敗した場合は、システムは再試行します。各ドライブバックプレーンに対して、最大3回の更新試行が許可されます。

現在の更新が失敗した後で、新しい更新を開始することができます。複数の更新が失敗した場合は、テクニカルサ

ポートに連絡して、ファームウェアを更新する別の方法を使用してください。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

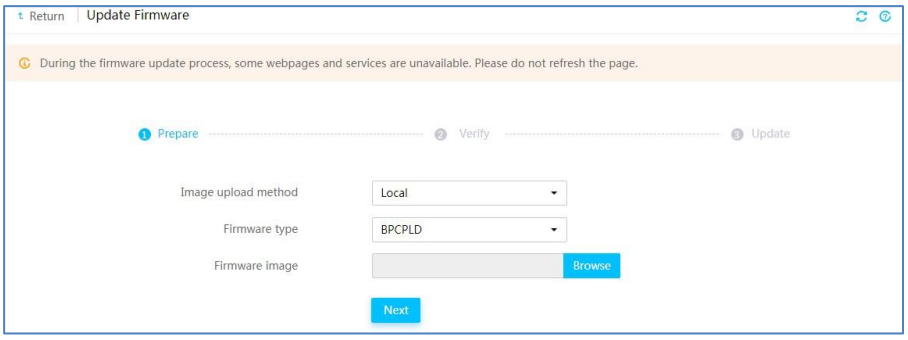
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

   図118に示すファームウェアイメージファイルのアップロードページが開きます。

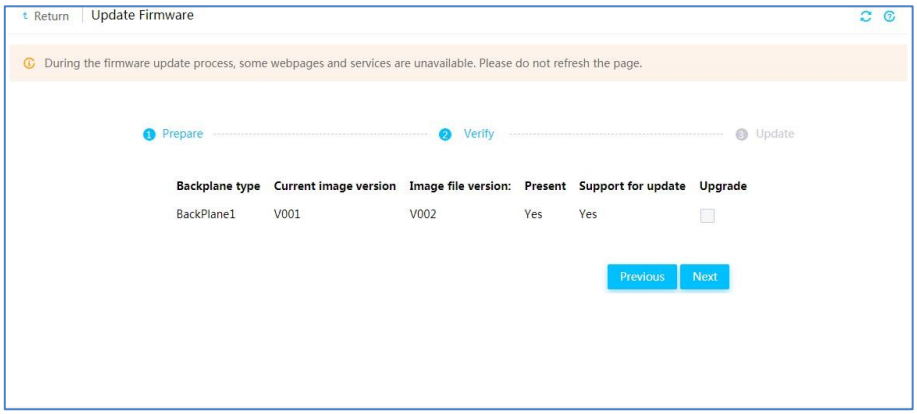
   図118 ファームウェアイメージのアップロード



4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**BPCPLD**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択した場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**BPCPLD**を選択します。イメージ名にはサフィックスが含まれている必要があります。

   b. **Next**をクリックします。
5. 更新するドライブバックプレーンを選択し、図119に示すように、現在のイメージバージョンとイメージファイルバージョンが正しいことを確認してから、**Next**をクリックします。

   図119 ファームウェア情報の確認



6. サーバーの電源がオンになっている場合は、サーバーの電源をオフにします。ファームウェアの更新は、サーバーの電源がオフになってから9秒後に開始されます。
7. 更新が完了したら、HDMを再起動して新しいBPCPLDを有効にします。

PCIeスイッチボードファームウェアの更新する

PCIeスイッチボードのファームウェアを更新するには、次の作業を実行します。

制限事項とガイドライン

この機能は、R5500 G5サーバーでのみ使用できます。この機能は、HDM-2.17以降でのみ使用できます。

更新が失敗した場合、システムは再試行します。最大2回まで再試行できます。

現在の更新が失敗した後で、新しい更新を開始することができます。複数の更新が失敗した場合は、テクニカルサポートに連絡して、ファームウェアを更新する別の方法を使用してください。

PCIeスイッチボードの交換後にファームウェアを更新するには、新しく取り付けたPCIeスイッチボードを識別できるように、まずサーバーの電源を入れます。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

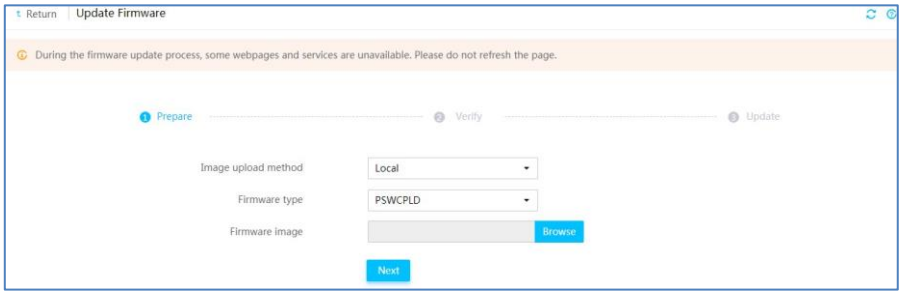
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **pdate Firmware**セクションで、**pdate Firmware**をクリックします。

   図120に示すファームウェアイメージファイルのアップロードページが開きます。

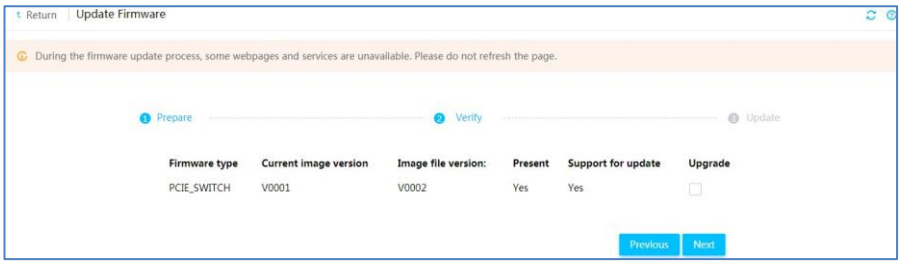
   図120 ファームウェアイメージのアップロード

4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**PSWCPLD**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択した場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**PSWCPLD**を選択します。イメージ名にはサフィックスが含まれている必要があります。

   b. **Next**をクリックします。
5. 更新するPCIeスイッチボードの情報、現在のイメージバージョン、およびイメージファイルバージョンが図121のように正しいことを確認し、**Next**をクリックします。

図121 ファームウェア情報の確認



6. サーバーの電源がオンになっている場合は、サーバーの電源をオフにします。ファームウェアの更新は、サーバーの電源がオフになってから9秒後に開始されます。
7. 更新が完了したら、電源コードを再接続してサーバーを再起動し、新しいファームウェアを有効にします。

パワーサプライファームウェアの更新

このタスクは、R4900 G3、R5300 G3、R4400 G3、R4700 G5、R4900 G5、R4950 G5、R5300 G5、R5500 G5、およびR6900 G5だけに適用されます。

制限事項とガイドライン

システムは、イメージファイルで定義されているものと同じモデルを使用するパワーサプライのファームウェアだけを更新し、パワーサプライを1つずつ更新します。

更新中のパワーサプライはサーバーに電力を供給できません。少なくとも1つの電源装置が存在し、更新プロセス中に電源装置がシステムボードに電力を供給できることを確認してください。

アップデートの前に、現在の電源装置が正しく動作していることを確認します。

R5500 G5では、システムボードとGPUモジュールは異なる電源セットを使用します。電源セットは個別に更新する必要があります。

電源装置ファームウェアは、次の更新方法をサポートしています。

- **Immediate update:** 新しいファームウェアイメージのバージョンが確認されたら、ただちに開始します。

  電源エラーを回避するには、更新中にサーバーの電源をオンまたはオフにしたり、電源を切断したりしないでください。
- **Update after server power-off:** サーバーの電源をオフにしてから9秒後に開始します。

  電源エラーを回避するには、更新中にサーバーの電源を投入したり、電源装置を取り外したりしないでください。

ファームウェアの更新方法は、イメージファイルによって決定されます。更新の前に、テクニカルサポートに連絡して更新方法を確認してください。

更新プロセスに時間がかかる場合があります。

電源装置の更新が失敗すると、電源装置が動作しなくなる可能性があります。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

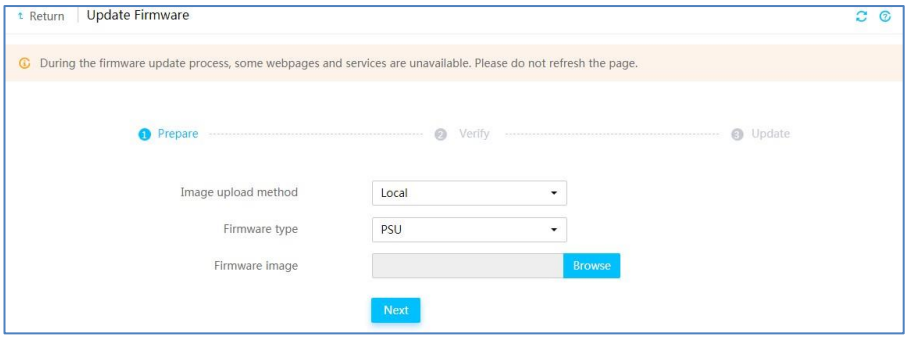
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

図122に示すファームウェアイメージファイルのアップロードページが開きます。

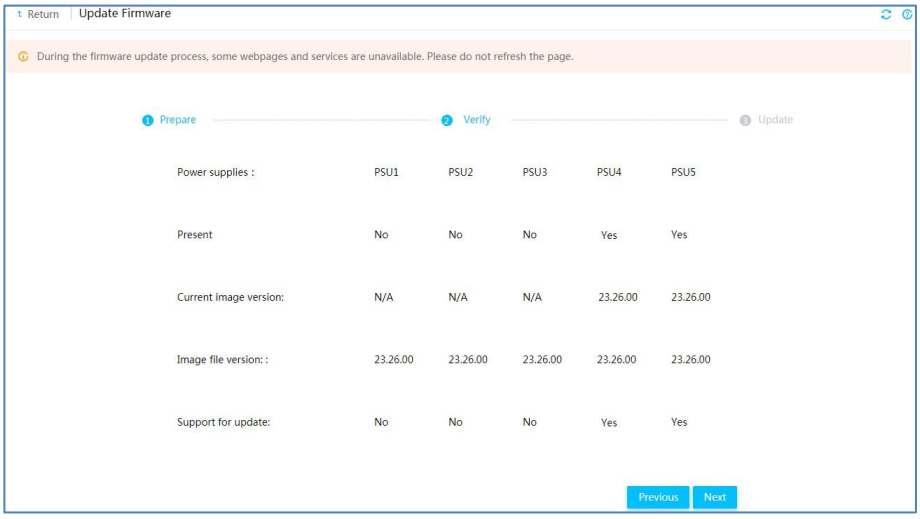
図122 ファームウェアイメージのアップロード



4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**PSU**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択する場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**PSU**を選択します。イメージ名にはサフィックスが含まれている必要があります。
   b. **Next**をクリックします。
5. 図123に示すように、現在のイメージのバージョンとイメージファイルのバージョンが正しいことを確認し、**Next**をクリックします。

   Presentフィールドは、パワーサプライが存在するかどうかを示します。

   図123 ファームウェア情報の確認



6. サーバーは、新しいファームウェアイメージの更新方法に応じて、ただちに更新を開始するか、サーバーの電源を切った後に更新を開始します。

   各電源装置の更新結果を表示するには、**Operation Log**ページにアクセスします。新しいファームウェアは、更新が完了すると自動的に有効になります。

LCDファームウェアの更新

LCDファームウェアの更新をサポートしているのは、HDM-2.09以降のバージョンだけです。この作業は、R6700 G3、R6900 G3、R8900 G3、R4700 G5、R4900 G5、R4950 G5、およびR6900 G5に適用されます。

制限事項とガイドライン

更新に失敗すると、LCDが動作しなくなる可能性があります。この場合は、LCDファームウェアの更新を再試行してください。更新プロセスに時間がかかる場合があり、更新中にLCDが使用できなくなります。

アップデートが完了すると、LCDが自動的に再起動し、新しいファームウェアが有効になります。

LCDファームウェアイメージをアップロードしてLCDファームウェアを更新できるのは、LCDがサーバーに接続された後だけです。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

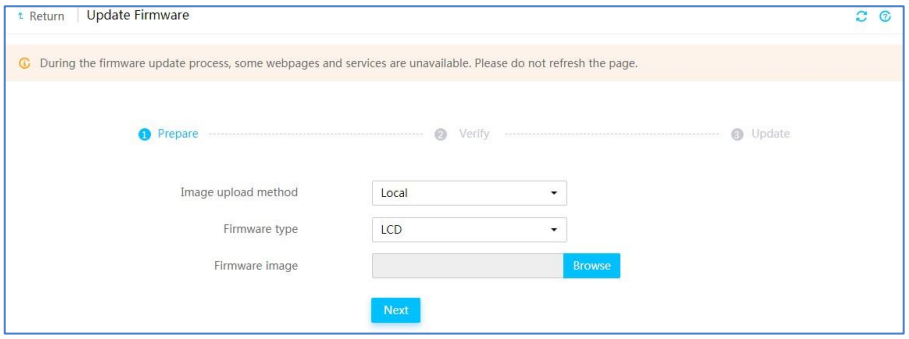
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

   図124に示すファームウェアイメージファイルのアップロードページが開きます。

   図124 ファームウェアイメージのアップロード

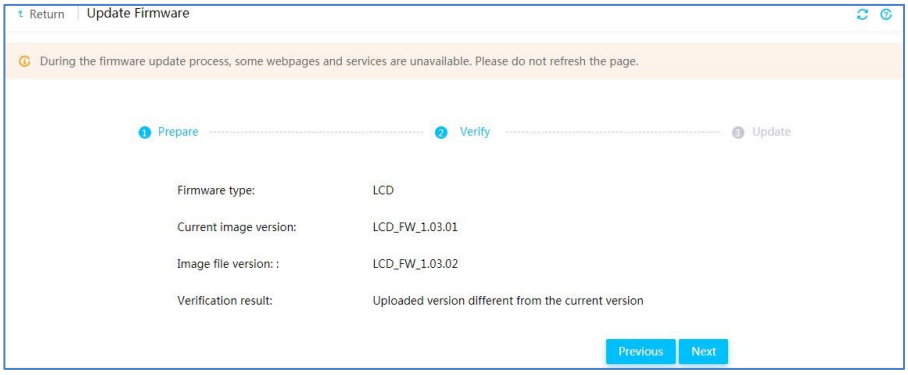
   

4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**LCD**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択した場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**LCD**を選択します。イメージ名にはサフィックスが含まれている必要があります。

   b. **Next**をクリックします。
5. 図125に示すように、現在のイメージのバージョンとイメージファイルのバージョンが正しいことを確認し、**Next**をクリックします。

   ファームウェアの更新が開始され、更新の進行状況が表示されます。

   図125 ファームウェア情報の確認

GPUCPLDファームウェアの更新

GPUのCPLDファームウェアを更新するには、次の作業を実行します。

制限事項とガイドライン

この機能は、R5300 G3サーバーでのみ使用できます。この機能は、HDM-2.16以降でのみ使用できます。

この機能は特定のGPUに対してのみ使用できます。複数のGPUが存在する場合は、アップロードされたGPUCPLDイメージでサポートされるGPUだけが更新されます。

GPUの更新が失敗した場合、システムは再試行します。システムは最大2回まで再試行できます。BIOSは更新プロセス中に複数回再起動します。

この機能は、サーバーの電源が入っている場合にのみ使用できます。更新プロセス中は、サーバーの電源を切ったり、サーバーから電源を取り外したりしないでください。これを行うと、更新が失敗するか、GPUが識別されなくなる可能性があります。

その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

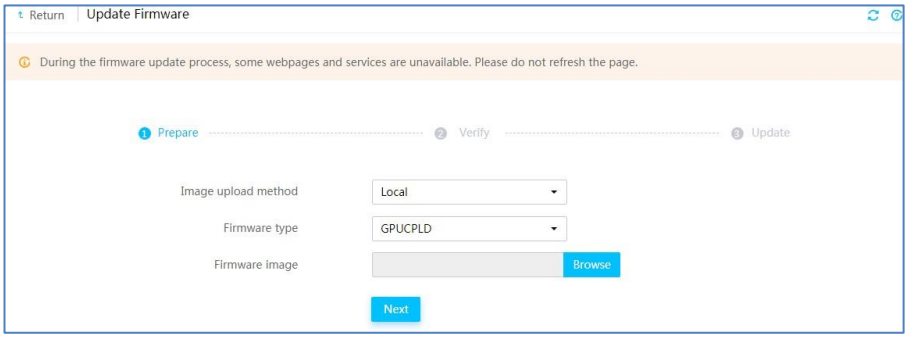
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

   図126に示すファームウェアイメージファイルのアップロードページが開きます。

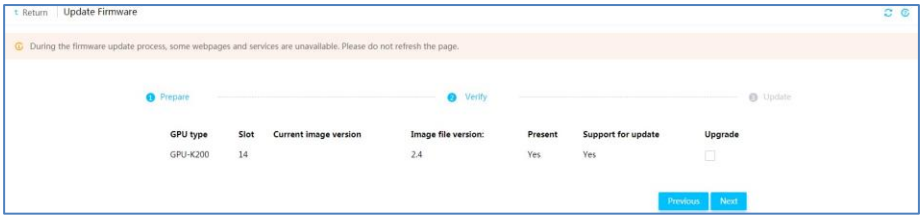
   図126 ファームウェアイメージのアップロード

4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      - **Local**を選択した場合は、ファームウェアタイプとして**GPUCPLD**を選択します。次に、更新イメージファイルを参照して選択します。
      - **TFTP**を選択した場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**GPUCPLD**を選択します。イメージ名にはサフィックスが含まれている必要があります。

   b. **Next**をクリックします。
5. ターゲットGPUを選択し、GPU情報、現在のイメージバージョン、およびイメージファイルバージョンが正しいことを確認してから、**Next**をクリックします。

図127 ファームウェア情報の確認



6. 更新後、新しいファームウェアを有効にするために、電源コードを再接続してサーバーの電源を再投入します。

GPUFPGAファームウェアの更新

GPUのField Programmable Gate Array(FPGA)ファームウェアを更新するには、次の作業を実行します。

制限事項とガイドライン

この機能は、HDM-2.25以降でのみ使用できます。この機能は、R5300 G5でのみ使用できます。

この機能は特定のGPUに対してのみ使用できます。複数のGPUが存在する場合は、アップロードされたGPUFPGAイメージでサポートされるGPUだけが更新されます。

この機能は、サーバーの電源が入っている場合にのみ使用できます。更新プロセス中は、サーバーの電源を切ったり、サーバーから電源を取り外したりしないでください。これを行うと、更新が失敗するか、GPUが識別されなくなる可能性があります。

GPUの更新が失敗すると、システムは再試行します。システムは最大2回まで再試行できます。その他の制限事項およびガイドラインについては、「ファームウェア更新の制限事項およびガイドライン」を参照してください。

前提条件

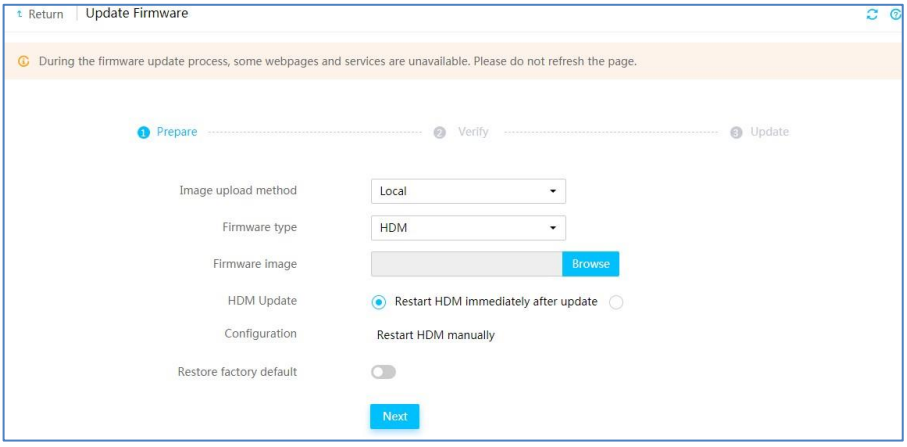
「ファームウェア更新の前提条件」を参照してください。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。
3. **Update Firmware**セクションで、**Update Firmware**をクリックします。

   図128に示すファームウェアイメージファイルのアップロードページが開きます。

   図128 ファームウェアイメージのアップロード



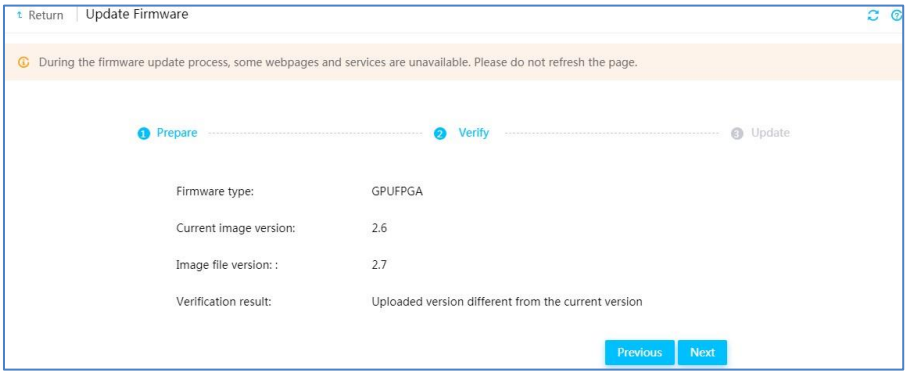
4. 作業ウィンドウで、次のタスクを実行します。
   a. イメージのアップロード方法を選択します。
      – **Local**を選択した場合は、ファームウェアタイプとして**GPUFPGA**を選択します。次に、更新イメージファイルを参照して選択します。

– **TFTP**を選択した場合は、イメージのアップロードに使用するインターフェースのIPアドレスとイメージ名を入力します。次に、ファームウェアタイプとして**GPUFPGA**を選択します。イメージ名にはサフィックスが含まれている必要があります。

b. **Next**をクリックします。

5. ターゲットGPUを選択し、GPU情報、現在のイメージバージョン、およびイメージファイルバージョンが正しいことを確認してから、**Next**をクリックします。

図129 ファームウェア情報の確認



6. 更新後、新しいファームウェアを有効にするために、サーバーの電源を再投入します。

HDMを再起動する

HDMを再起動して、ファームウェアの更新後、またはHDMが誤動作しているときに新しいファームウェアイメージを有効にすることができます。

HDMが再起動されると、すべてのHDMユーザーセッションが閉じられます。これらのセッションは、HDMの起動後に自動的に再確立されます。

HDMを再起動しても、HDM設定は削除されません。

制限事項とガイドライン

HDMの再起動操作中は、サーバーの電源を入れたり、切ったり、再投入したりしないでください。再投入すると、一部のHDM機能の誤動作やオペレーティングシステムエラーの原因となる可能性があります。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。

2. 左側のナビゲーションペインで、**Update Firmware**を選択します。図111に示すページが開きます。

3. **Restart Firmware**セクションで、**Restart HDM**をクリックし、**OK**をクリックして操作を確認します。

CPLDを再起動する

CPLDを再起動して、ファームウェアの更新後に新しいCPLDまたはPFRCPLDファームウェアイメージを有効にすることができます。

CPLDの再起動は、R2700 G3、R2900 G3、R4400 G3、R4700 G3、R4900 G3、R5300 G3、およびB5700 G5を除くすべてのG5サーバーでサポートされています。

制限事項とガイドライン

CPLDを再起動するには、サーバーの電源がオフになっている必要があります。CPLDを再起動すると、HDMすぐに再起動します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。

2. 左側のナビゲーションペインで、**Update Firmware**を選択します。図111に示すページが開きます。

3. **Restart Firmware**セクションで、**Restart CPLD**をクリックし、OKをクリックして操作を確認します。

プライマリHDMファームウェアイメージとバックアップHDMファームウェアイメージの切り替え

HDMは、1つのプライマリファームウェアイメージと1つのバックアップファームウェアイメージをサポートします。これらのイメージは異なるストレージ領域に格納されます。プライマリファームウェアイメージが破損している場合は、イメージスイッチオーバーを実行して、バックアップファームウェアイメージにプライマリの役割を引き継ぐことができます。

制限事項とガイドライン

HDMの再起動操作中は、サーバーの電源を入れたり、切ったり、再投入したりしないでください。再投入すると、一部のHDM機能の誤動作やオペレーティングシステムエラーの原因となる可能性があります。

プライマリHDMファームウェアイメージを更新したら、プライマリ/バックアップスイッチオーバーを実行してから、プライマリHDMファームウェアイメージとバックアップHDMファームウェアイメージ間のバージョンの一貫性を保つためにファームウェアを再度更新します。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Update Firmware**を選択します。図111に示すページが開きます。
3. **Primary/backup switchover**セクションで、プライマリおよびバックアップのファームウェアイメージのバージョンを確認し、**Switchover**をクリックします。

   HDMは元のバックアップイメージ(現在はプライマリイメージ)を使用して自動的に再起動します。

POSTコード

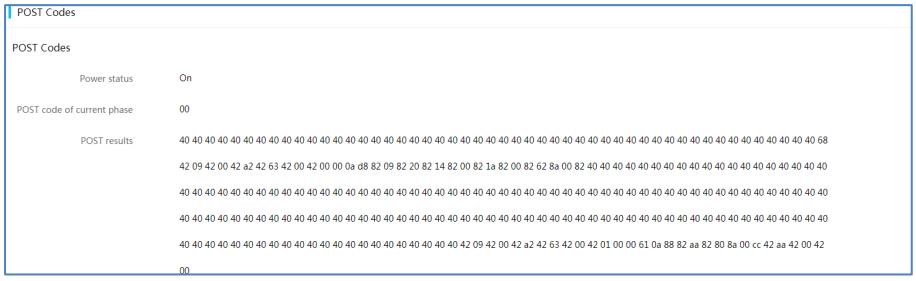
システムは電源投入時自己診断(POST)コードを生成して、サーバー起動の各フェーズでの状態を記録します。POSTコードの詳細については、「付録B POSTコード」を参照してください。

POSTコードの表示

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**POST Codes**を選択します。
3. 図130に示す作業ウィンドウで、システムのPOSTコードを表示します。

   図130 POSTコード



パラメーター

- **POST code of current phase:** コードシステムの現在の起動フェーズのPOSTコード。
- **POST results**: システムの現在または最新の起動中に生成されたすべてのPOSTコード。

インテリジェントセキュリティベゼルを管理する

インテリジェントセキュリティベゼルのプレゼンスステータスを識別し、セキュリティベゼル設定を設定するには、次の作業を実行します。

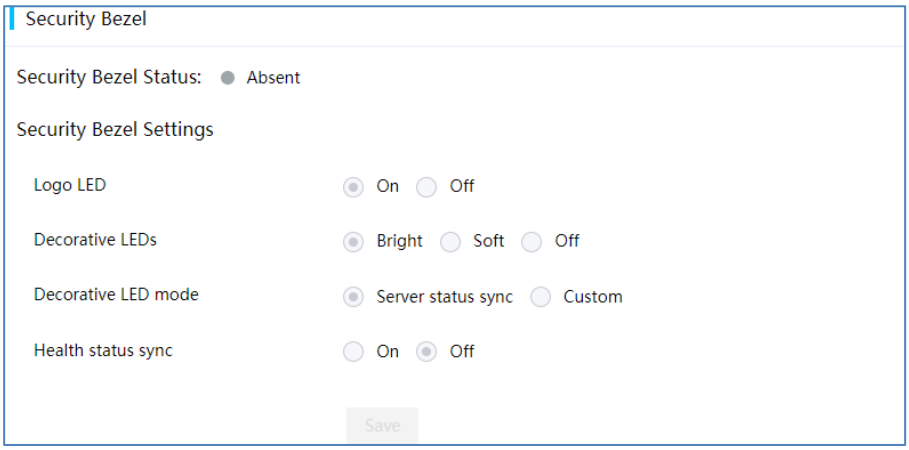
制限事項とガイドライン

この機能は、R5300 G5およびB5700 G5を除くG5サーバーでのみ使用できます。この機能は、HDM-2.13以降でのみ使用できます。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Security Bezel Control**を選択します。
   セキュリティベゼルコントロール設定ページが開きます(図131を参照)。
3. インテリジェントセキュリティベゼルがあるかどうかを確認します。
   - 装飾用LEDモードを**Server status sync**に設定した場合、装飾用LEDの点滅モードと色は、サーバーの動作ステータスの変化に応じて変化します。
   - 装飾LEDモードを**Custom**に設定した場合は、装飾LEDの点滅モードと色を設定できます。
4. **save**をクリックします。

図131セキュリティベゼルのコントロール設定



パラメーター

- **Decorative LEDs**: **Bright**、**Soft**、および**Off**のオプションがあります。装飾用LEDを有効にする場合は、消費電力を減らすためのベストプラクティスとしてSoftを選択します。
- **Health status sync**: サーバーのヘルスステータスに基づいて装飾LEDを点滅させます。この機能を使用するには、**Server status sync**オプションが選択されていることを確認します。詳細については、サーバーのユーザーガイドを参照してください。

サービスUSBデバイスを管理する

サービスUSBデバイスは、USB診断ツールのイメージファイルで焼き付けられたUSBデバイスです。このようなデバイスをサーバーに接続してSDSログを自動的にダウンロードし、必要に応じてHDMからサービスUSBデバイスを管理できます。

制限事項とガイドライン

この機能は、B5700 G5を除くG5サーバーでのみ使用できます。この機能は、HDM-2.25以降でのみ使用できます。

サービスUSBデバイスを接続するときにユーザーがSDSログをダウンロードしている場合、システムはサービスUSBデバイスを取り出します。進行中のダウンロードプロセスが終了するのを待ってから、サービスUSBデバイスを再接続できます。

サービスUSBデバイスを接続する前に、デバイスの使用可能な領域が500 MBを超えていることを確認します。

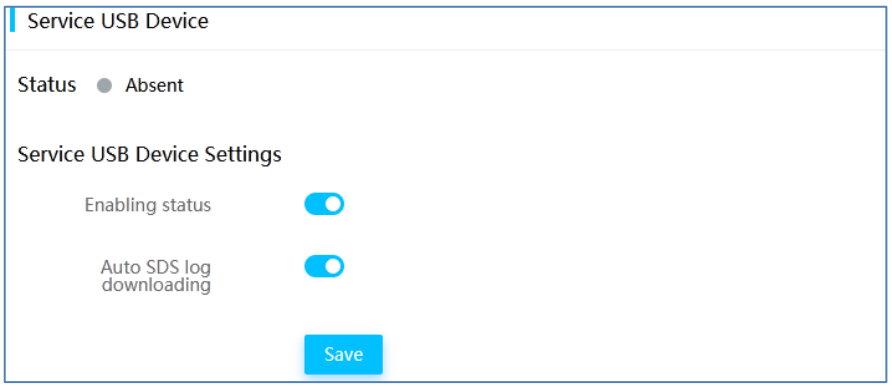
USB例外を回避するために、動作中のサービスUSBデバイスを強制的に削除しないでください。USB例外を回避するために、サービスUSBデバイスを頻繁に接続または削除しないでください。

複数のサービスUSBデバイスをサーバーに接続する場合、サーバーは最初に接続されたデバイスだけを識別できます。

手順

1. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
2. 左側のナビゲーションペインで、**Service USB Device**を選択します。
   開いたページには、サービスUSBデバイスのステータスが表示されます。
3. サービスUSBデバイスを有効にするかどうかを選択します。
4. SDSログの自動ダウンロードを有効にするかどうかを選択します。
5. **save**をクリックします。
6. サービスUSBデバイスが動作している場合は、動作が終了するまで待ってから、サービスUSBデバイスを再接続して設定を有効にします。

図132 USBデバイスの管理



パラメーター

- **Status**: サービスUSBデバイスのステータス。オプションには、現在、不在、および動作中があります。
- **Auto SDS log downloading**: この機能をイネーブルにすると、サービスUSBデバイスをサーバーに接続したときに、そのデバイスのSds_And_SmartTest/ServerUdiskディレクトリにSDSログが自動的にダウンロードされます。

ユーザーとセキュリティ

ユーザーカウント

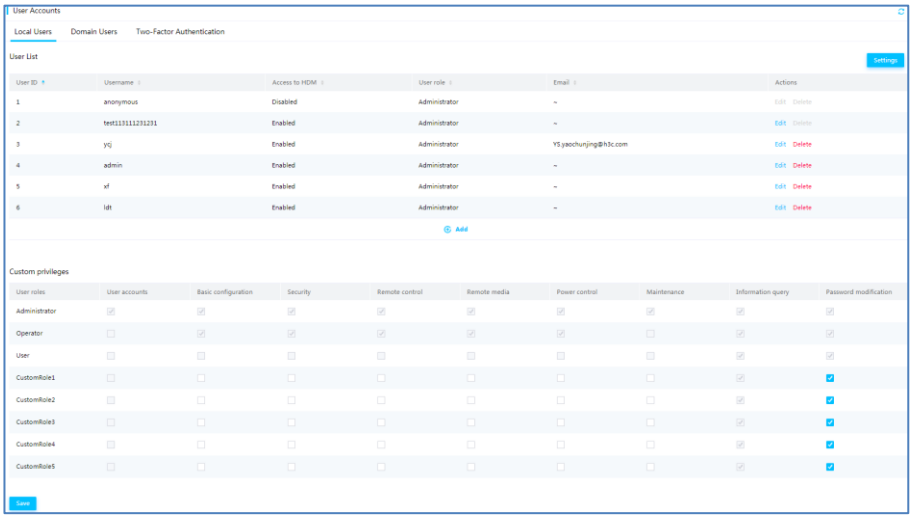
ローカルユーザー、LDAPユーザー、およびADグループを含むユーザーカウントを設定して、HDMへのアクセスを制御します。

ローカルユーザー情報を表示する

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. 作業ウィンドウで、HDMユーザーに関する情報をユーザーリストに表示します。

図133 ローカルユーザー情報の表示



パラメーター

- **User ID**:ユーザーのID。
- **Username**:ユーザーの名前。
- **Access to HDM**: ユーザーがHDM Webインターフェースにアクセスできるかどうか。
- **User role**:ユーザーのロール。ユーザーのネットワークアクセス権限を決定します。
  - **Administrator**:ユーザーはすべての機能に対する読み取りおよび書き込み権限を持っています。
  - **Operator**:ユーザーはすべての機能に対する読み取り権限と一部の機能に対する書き込み権限を持っています。
  - **User:** ユーザーは読み取り専用のアクセス許可を持っています。
  - **CustomRole*N***: ユーザーは、管理者ユーザーによってカスタムロールに指定された権限を持ちます。システムは、最大5つのカスタムユーザーロールをサポートします。
  - **None** : ユーザーにはネットワークアクセス権限がありません。このロールは特別な用途に使用されます。ロールをユーザーに割り当てないでください。
- **Email**: ユーザーが連絡を受ける電子メールアドレス。

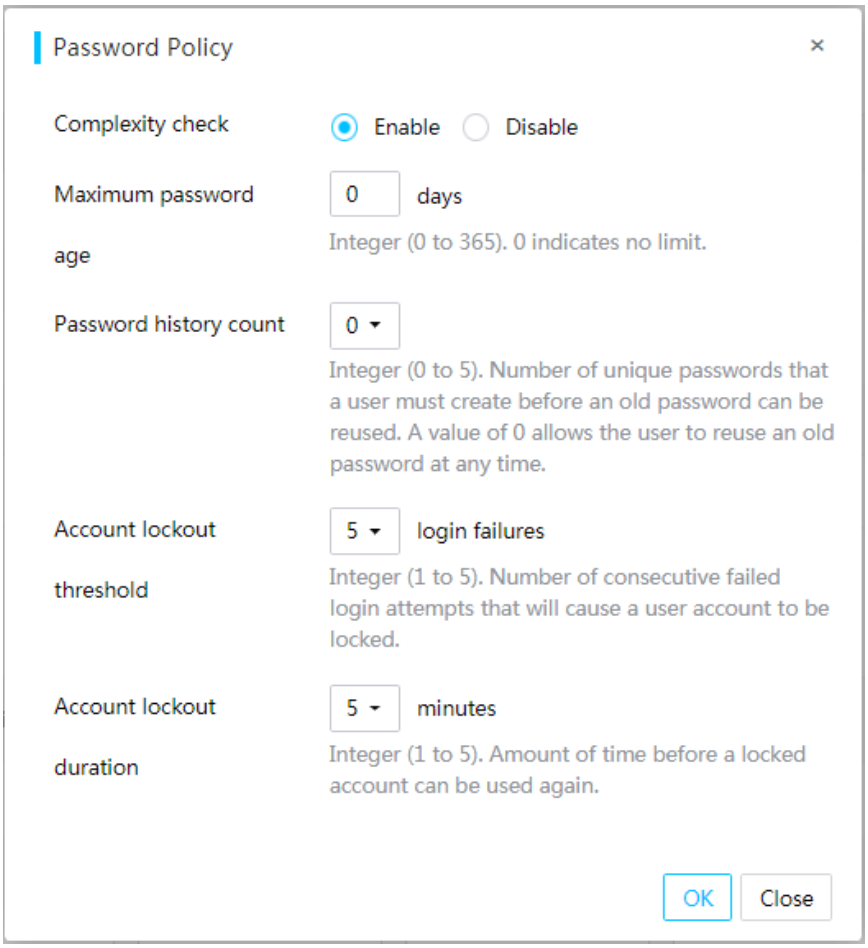
ローカルユーザー用のパスワードポリシーを構成する

ユーザーカウントのパスワードが従う必要がある規則を設定して、HDMアクセスセキュリティを強化するには、次の作業を実行します。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. 作業ウィンドウで、**Advanced Settings**をクリックします。
4. 表示されたダイアログボックスで、パスワードポリシーを設定し、**OK**をクリックします。

図134 パスワードポリシーの構成



パラメーター

- **Complexity check**: パスワードの複雑性チェックを無効または有効にします。
  - この機能をディセーブルにする場合、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。
    - 2～20文字。
    - 大文字と小文字が区別されます。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:`~!@#$%^&*()_+-={};':",./<>?
  - この機能がイネーブルになっている場合、パスワードは次の拡張複雑度要件を満たす必要があります。
    - 8～20文字。
    - 大文字と小文字が区別されます。有効な文字は、複雑性チェックが無効な場合にサポートされる文字と同じです。
    - 大文字、小文字、数字の少なくとも2つのカテゴリの文字を含む必要があります。
    - スペースまたは特殊文字を少なくとも1つ含む必要があります。
    - ユーザー名と同じであったり、ユーザー名を逆にしたりしないでください。
    - 古いパスワードの再利用要件を満たす必要があります。
- **Maximum password age**: パスワードを使用できる最大日数。パスワードが期限切れになると、HDMはユーザーにパスワードの変更を要求します。デフォルト管理者のパスワードは期限切れになりません。
- **Password history count**: 古い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。
- **Account Lockout Threshold**: ユーザーカウントがロックされる原因となる連続したログイン失敗の回

数。

- **Account lockout duration**: ロックされたアカウントを再び使用できるようになるまでの時間。

カスタムユーザーの権限を設定する

カスタムユーザーの特権を設定するには、次の作業を実行します。

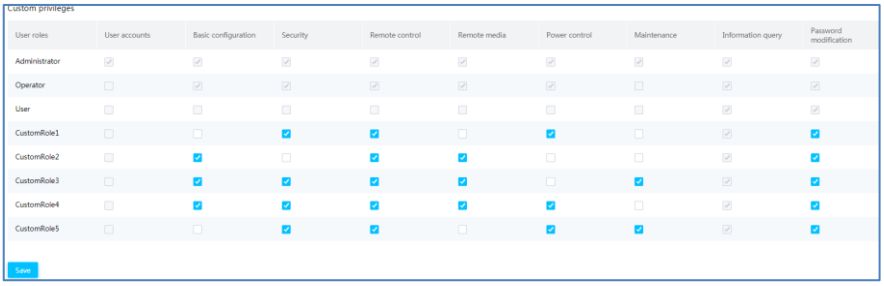
ハードウェアとソフトウェアのバージョンの互換性

このタスクは、HDM-2.03以降でのみサポートされています。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Custom privileges**セクションで、図135に示すように、必要に応じてカスタムユーザー**CustomRole1**から**CustomRole5**のアクセス権限を選択します。
4. **save**をクリックします。

図135 カスタムユーザーの権限の構成



パラメーター

- **User roles**: ネットワークおよびサービスアクセス権限のセットを表すユーザーロール。
- **CustomRole*N***: カスタムユーザーロールの名前。システムは最大5つのカスタムユーザーロールをサポートします。デフォルトでは、カスタムユーザーロールには情報問合せ権限のみがあります。
- **User accounts**: ローカルユーザー、LDAPユーザー、およびADグループを管理する特権を指定し、Two-Factor認証、インポートおよびエクスポート設定を設定し、統合制御を実行します。
- **Basic configuration**: 資産タグ、ネットワーク設定、NTP設定、SNMP設定、およびアラーム設定(SMTP設定、SNMPトラップ設定、およびsyslog設定)、イベントログ、動作ログ、ビデオ再生、およびインテリジェントセキュリティベゼルを管理する特権を指定します。
- **Security**: アクセスサービス、ファイアウォール、SSL証明書、PFR、およびログイン設定のセキュリティヒントを設定する特権を指定します。
- **Remote control**: ストレージ構成(RAID構成および物理ドライブ管理)、システムリソースの監視、KVM、H5 KVM、VNCクライアントログインのパスワード設定、システムブートオプション、UID LED、SOL接続モード、およびMCAポリシーを管理する権限を指定します。電源制御およびメディアイメージのマウントの権限は含まれません。
- **Remote media**: 仮想メディア設定、KVMコンソールからのメディアマウント、およびH5 KVMコンソールからのメディアマウントを設定する権限を指定します。
- **Power control**: 電源構成、NMI制御、およびファン設定を管理する権限を指定します。
- **Maintenance**: ドライブUID LED、BSoDスクリーンショット、ビデオ再生、ファームウェア更新、HDM設定復元、HDMプライマリ/バックアップスイッチオーバー、HDM再起動、CPLD再起動、およびサービスUSBデバイス設定を管理する特権を指定します。
- **Information query**: ユーザーの情報表示権限を指定します。管理者ユーザーの場合、この権限によりユーザーはすべてのユーザーに関する情報を表示できます。管理者以外のユーザーの場合、この権限によりユーザーは自身の情報を表示できます。
- **Password modification**: ローカルユーザー自身のパスワードを変更する権限を指定します。

ローカルユーザーアカウントを管理する

制限事項とガイドライン

セッション内のユーザーのユーザー名を変更したり、そのようなユーザーを削除したりすることはできません。セッション内のユーザーを削除することはできません。

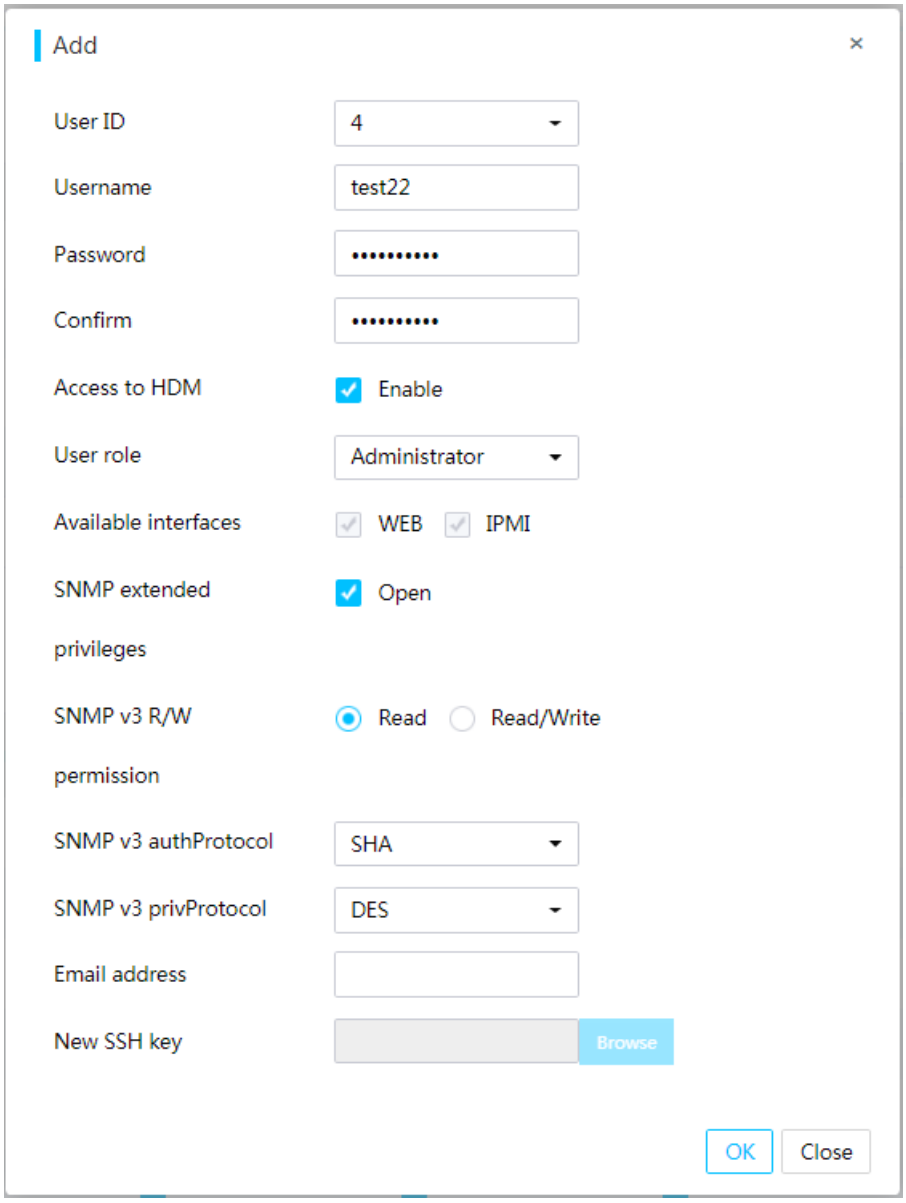
前提条件

管理者ロールでサインインしていることを確認します。

ユーザーアカウントを追加する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Add**をクリックします。
4. 表示されたダイアログボックスで、ユーザーパラメーターを設定します。

図136 ユーザーアカウントの追加

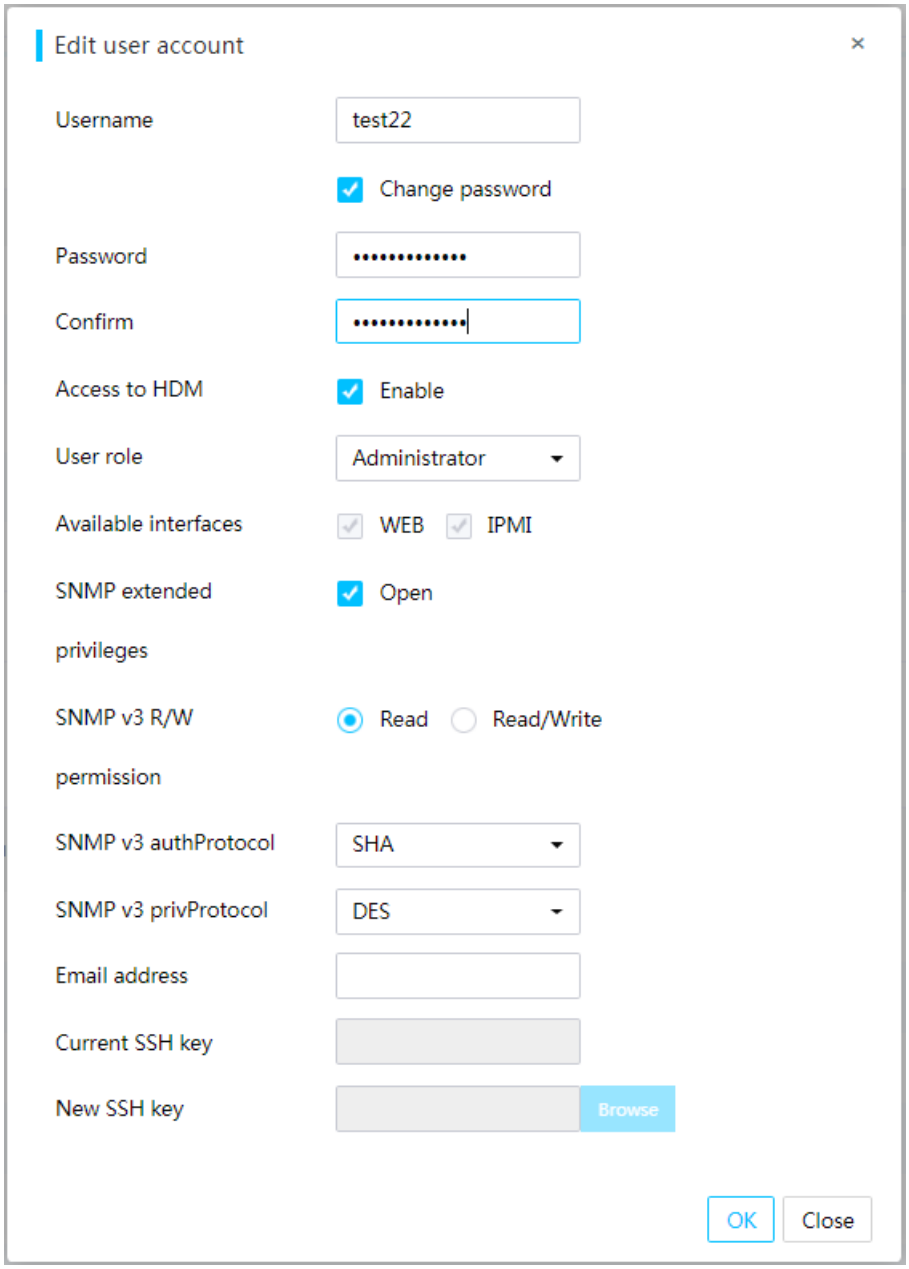


5. **OK**をクリックします。

ユーザーアカウントを編集する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. ユーザーアカウントエントリー**Edit**をクリックします。
4. 表示されたダイアログボックスで、ユーザーパラメーターを設定します。

図137ユーザーアカウントの編集



5. **OK**をクリックします。

ユーザーカウントを削除する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。

2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. ユーザーカウントエントリで**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**をクリックします。

パラメーター

- **User ID**: ユーザーのID。
- **Username**: ユーザーカウントのユーザー名を指定します。ユーザー名は、大文字と小文字が区別される1文字から16文字の文字列です。有効な文字は、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(@)です。
- **Password**: ユーザーカウントのパスワードを指定します。このパスワードは、「ローカルユーザーのパスワードポリシーの構成」で説明されているパスワードポリシーに準拠する必要があります。
- **Confirm**:確認のために再度パスワードを入力します。
- **Access to HDM**: ユーザーがHDM Webインターフェースにアクセスできるようにするには、**Enable**を選択します。ユーザーアクセスを有効化しない場合、ユーザーはHDM Webインターフェースにアクセスできません。
- **User role** :ネットワークおよびサービスアクセス権限のセットを表すユーザーロールを選択します。使用可能なユーザーロールは次のとおりです。
  - **Administrator**: ユーザーはすべての機能に対する読み取りおよび書き込み権限を持っています。
  - **Operator**: ユーザーはすべての機能に対する読み取り権限と一部の機能に対する書き込み権限を持っています。
  - **User**: ユーザーは読み取り専用のアクセス許可を持っています。
  - **CustomRole*N***: ユーザーは、管理者ユーザーによってカスタムロールに指定された権限を持ちます。システムは、最大5つのカスタムユーザーロールをサポートします。
  - **None**: ユーザーにはネットワークアクセス権限がありません。このロールは特別な用途に使用されます。ロールをユーザーに割り当てないでください。
- **Available interfaces**: 必要に応じて、ユーザーのWebおよびIPMIアクセス権限を選択します。

  WebおよびIPMIアクセスは、デフォルトで管理者およびオペレータ
  に許可されており、取り消すことはできません。
- **SNMP extended privileges**: SNMP拡張権限をユーザーに付与するかどうかを選択します。権限を付与するには、HDMへのユーザーアクセスを有効にし、ユーザーパスワードに8文字以上を含める必要があります。**SNMP extended privileges**を選択する場合は、**SNMP v3 R/W permission**フィールドから権限を選択します。次のオプションがあります。
  - **Read**: ユーザーは読取り専用権限を持っています。これにより、ユーザーはGET操作を実行し、トラップを受信できます。
  - **Read/Write**: ユーザーに読取りおよび書込み権限があります。これにより、ユーザーはGETおよびSET操作を実行し、トラップを受信できます。
- **SNMP v3 authProtocol**: SNMP v3認証プロトコルを選択します。オプションには、SHAとMD5があります。デフォルトのプロトコルはSHAです。
- **SNMP v3 privProtocol**: SNMP v3プライバシープロトコルを選択します。オプションには、DESとAESがあります。デフォルトのプロトコルはDESです。
- **Email address**: ユーザーが連絡を受ける電子メールアドレスを入力します。アドレスは63文字を超えることはできません。このアドレスを使用して、ユーザーカウントのパスワードを取得できます。アラート電子メールをユーザーに送信するには、そのユーザーのユーザーカウントに電子メールアドレスを指定する必要があります。アラート電子メールは、「アラーム設定」メニューから構成できます。
- **New SSH key**: このフィールドは将来の使用のために予約されています。

ユーザーの役割と権限のマトリックス

サポートされる機能または機能メニューは、サーバーモデルによって異なります。

次に、ユーザーロールが持つ権限について説明します。ユーザーロールがその機能または機能メニューを使用する権限を持っていない場合、機能または機能メニューにアクセスできません。

メニュー/機能	Administrator	Operator	user
User accounts			
Configure a local user account	√	×	×
Configure LDAP settings	√	×	×
Configure AD settings	√	×	×
Configure two-factor authentication	√	×	×
Import and export configurations	√	×	×
Perform unified control	√	×	×
Basic configuration			
Configure the HDM dedicated network port	√	√	×
Specify the HDM shared network port	√	√	×
Configure DNS settings	√	√	×
Configure network port mode settings	√	√	×
Configure LLDP	√	√	×
Configure Wi-Fi settings	√	√	×
Configure NTP servers	√	√	×
Configure SNMP settings	√	√	×
Manage alert emails	√	√	×
Configure SNMP trap settings	√	√	×
Configure syslog settings	√	√	×
Manage event log (configure the event log policy, save event log, and delete event log entries)	√	√	×
Save operation log in CSV format or delete operation log entries	√	√	×
Configure advanced settings for videoreplay (download and play videos)	√	√	×
Configure the intelligent security bezel	√	√	×
Configure the HDM dedicated network port	√	√	×
Security			
Configure services	√	√	×
Configure the firewall	√	√	×
Configure SSL	√	√	×
PFR	√	√	×
Security tip for login	√	√	×
Remote console			
Manage storage configuration (RAID configuration and physical drive management)	√	√	×
Configure the alarm thresholds for system resource monitoring	√	√	×
Use KVM remote console (except power control and media mounting)	√	√	×
Use H5 KVM remote console (except power control and media mounting)	√	√	×

Configure password settings for VNC client login	√	√	×
Configure boot options	√	√	×
Switch SOL connection mode	√	√	×
Set the UID LED	√	√	×
Set the MCA policy	√	√	×
Remote media			
Configure virtual media settings	√	√	×
Mount media images from KVM	√	√	×
Mount media images from H5 KVM	√	√	×
Power control			
Power on or power off the server	√	√	×
NMI control	√	√	×
Meter power (operating mode and power-on policy)	√	√	×
Physical power button control	√	√	×
Configure global power settings (alarm threshold for the global power consumption and power capping)	√	√	×
Configure fan settings	√	√	×
Configure processor power states	√	√	×
Maintenance			
Set the drive UID LED	√	×	×
Restart collection of CUPS statistics	√	×	×
Manage event log (configure the event log policy, save event log, and delete event log entries)	√	×	×
Save operation log in CSV format	√	×	×
Configure advanced settings for video replay (download and play videos)	√	×	×
Update firmware	√	×	×
Restore HDM settings	√	×	×
Restart HDM	√	×	×
Change between the primary and backup HDM images	√	×	×
Restart CPLD	√	×	×
Manage service USB device settings	√	×	×

Information query			
View basic server information	√	√	√
View basic server status information	√	√	√
View server health state	√	√	√
View HDM user sessions	√	√	√
View storage information	√	√	√
View system information	√	√	√
View temperature heatmaps	√	√	√
View fan configuration	√	√	√
Display system boot options	√	√	√
View system resource monitoring statistics	√	√	√
Download and view the log	√	√	√
View event log	√	√	√
View operation log	√	√	√
View BSoD screenshots	√	√	√
Play videos	√	√	√
View information about the HDM dedicated network port	√	√	√
View information about the HDM shared network port	√	√	√
View DNS settings	√	√	√
View network port mode settings	√	√	√
View LLDP information	√	√	√
View information about the current local user	√	√	√
View information about the other local users	√	×	×
View NTP servers	√	√	√
View LDAP settings	√	√	√
View AD settings	√	√	√
View SNMP settings	√	√	√
View alarm settings	√	√	√
View service information	√	√	√
View firewall settings	√	√	√
View PFR settings	√	√	√
View the SSL certificate	√	√	√
View UID LED status	√	√	√
View system boot options	√	√	√
View SOL connection mode	√	√	√
information			
View virtual media information	√	√	√
View intelligent security bezel settings	√	√	√
View service USB device settings	√	√	√
View the security tip for login	√	√	√
Display power status	√	√	√
View two-factor authentication settings	√	√	√

View the security module status	√	√	√
View power information	√	√	√
Display power configuration (operating mode and power-on policy)	√	√	√
Display global power settings (alarm threshold for the global power consumption and power capping)	√	√	√
View history power consumption statistics	√	√	√
View POST codes	√	√	√
View fan configuration	√	√	√
View processor power states	√	√	√
View unified control information	√	√	√
Toggle between languages	√	√	√
Access online help	√	√	√
Refresh a page	√	√	√
View most recent event notifications	√	√	√
Sign out HDM	√	√	√
Password modification			
Modify the current user's password (for local users only)	√	√	√

LDAP設定の構成

Lightweight Directory Access Protocol(LDAP)を使用すると、IPネットワークを介して分散ディレクトリ情報サービスに効率的にアクセスして維持できます。

LDAPサーバー上のLDAPロールグループのユーザーカウントを使用して、LDAP認証とHDMへのアクセスをイネーブルにできます。

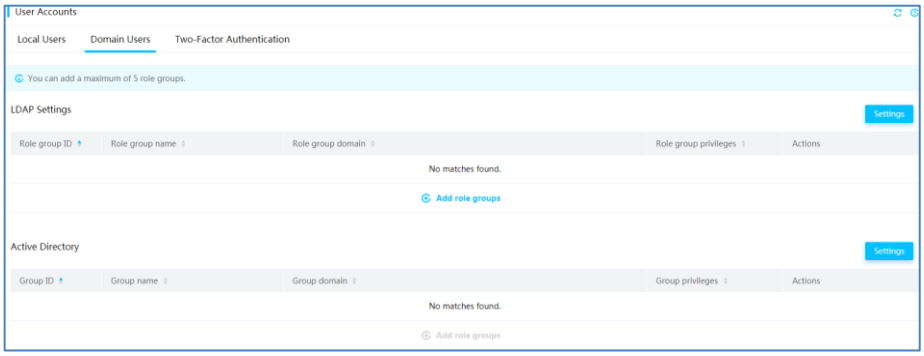
前提条件

LDAP設定を構成する前に、LDAPサーバーが使用可能であることを確認します。詳細は、「LDAPサーバーの設定」を参照してください。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。

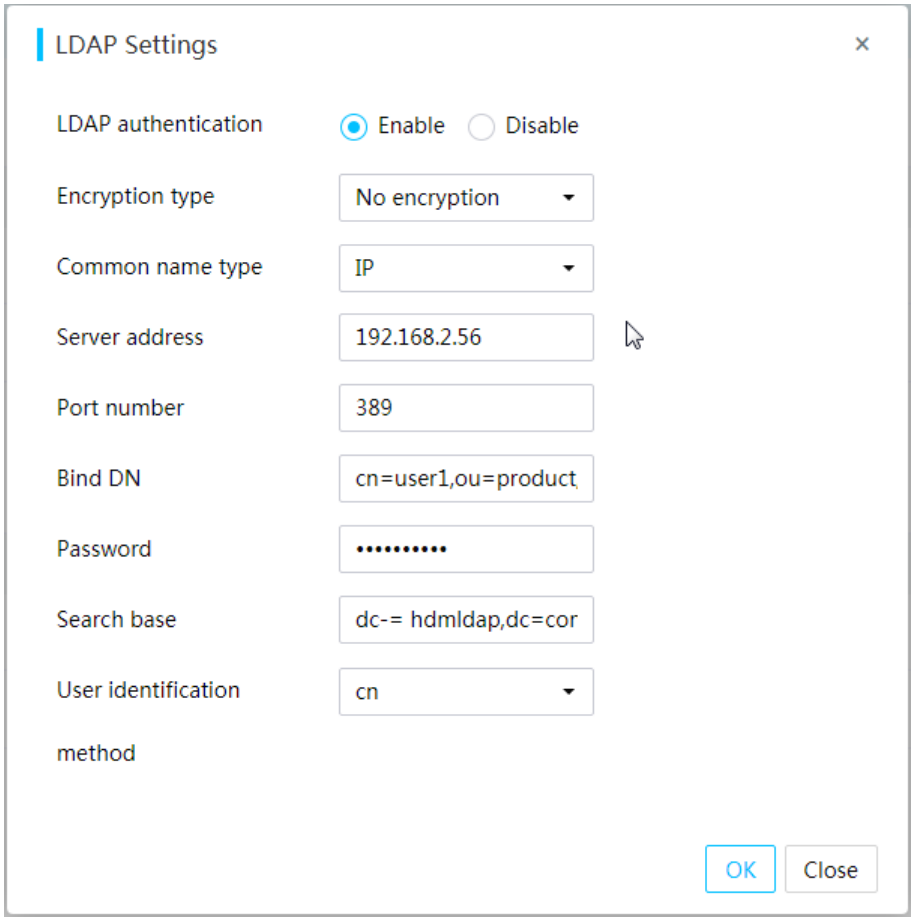
   図138 Domain Usersタブ

4. LDAP設定セクションで、**Settings**をクリックします。

5. 表示されたダイアログボックスで、LDAP認証を有効にし、LDAPパラメーターを設定します。

図139 LDAPパラメーターの構成



6. **OK**をクリックします。

パラメーター

- **Encryption type**:暗号化タイプを選択します。
  - No Encryption: LDAPサーバーとの暗号化されていない接続を確立します。
  - SSL: LDAPサーバーとのSSL暗号化接続を確立します。
- **Common name type**: IPアドレスまたはドメイン名。
- **Server address**: LDAPサーバーのIPv4アドレス、IPv6アドレス、またはドメイン名。
- **Port number**: 1～65535の範囲のLDAPサービスポート番号。SSL接続の場合、ポート番号はデフォルトで636です。残りのタイプの接続の場合、ポート番号はデフォルトで389です。ポート番号がすべてのサービスで一意であることを確認してください。
- **Bind DN**: LDAPサーバーおよびHDMにバインドされているLDAPユーザーのDN情報。最大長は255バイトです。DN情報には、次のカンマで区切られたアイテムが含まれます。
  - CN:ユーザーログイン名。
  - **UID**: ユーザーID。
  - **OU**: レベルの昇順の組織単位。
  - **DC**: ユーザーが属するドメインの名前。
- **Password**: LDAPユーザーのディレクトリパスワード。
- **Search base**: LDAPサーバー上のバインドDNにあるLDAPユーザーの検索ベース(ディレクトリ)。最大長は255バイトです。
- **User identification method**: LDAPサーバーで使用されるユーザー識別方法。サポートされる方法はCN

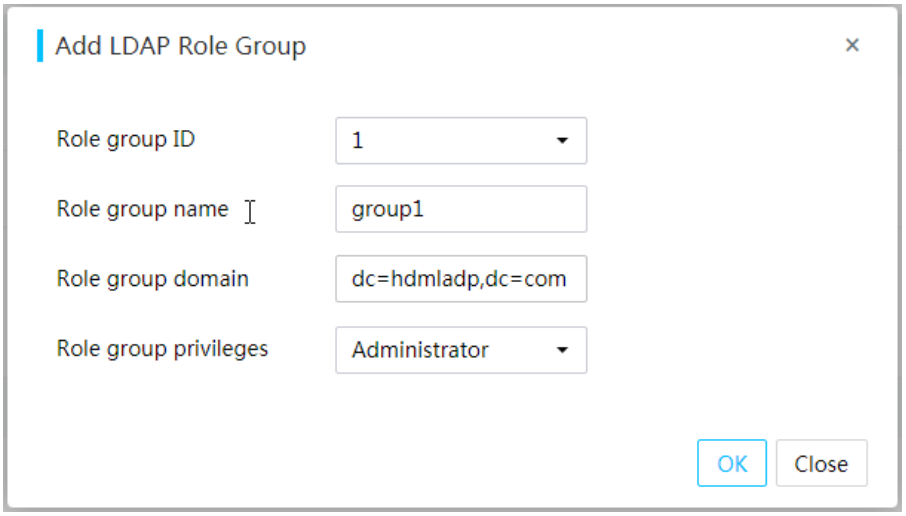
およびUIDです。ユーザー識別方法はバインドDN内のLDAPユーザー情報と一貫性がある必要があります。

LDAPロールグループを管理する

役割グループを追加する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **LDAP Settings**セクションで、**Add role groups**をクリックします。
5. ロールグループパラメーターを設定します。

図140 役割グループの追加

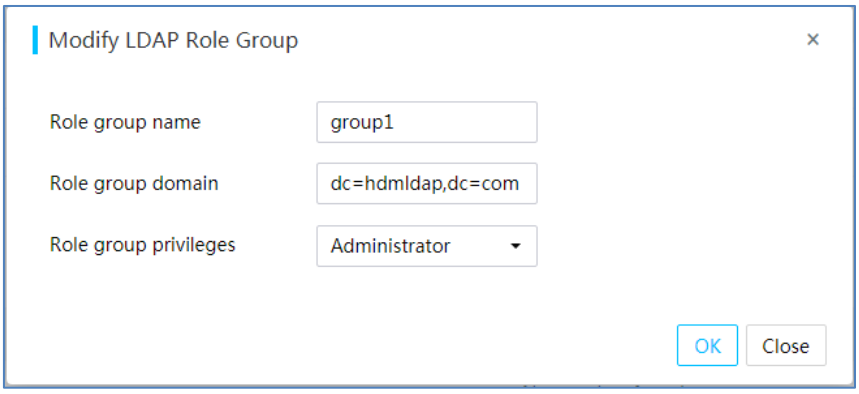


6. **OK**をクリックします。

ロールグループを編集する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **LDAP Settings**セクションで、変更するロールグループエントリの**Edit**リンクをクリックします。
5. パラメーターを修正します。

図141 役割グループの編集



6. OKをクリックします。

ロールグループを削除する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. LDAP Settingsセクションで、削除するロールグループエントリの**Delete**をクリックします。

パラメーター

- **Role group ID**: ロールグループのID。
- **Role group name**: LDAPサーバー上の既存のロールグループの名前。
- **Role group domain**: LDAPサーバー上のロールグループのベース(ディレクトリ)を検索します。最大長は255バイトです。
- **Role group privileges**: グループのネットワーク権限。

AD認証を設定する

ADサーバーに設定された有効なActive Directory(AD)グループ内のユーザーカウントのユーザー名とパスワードを使用して、ユーザーがHDMIにアクセスできるようにするには、次の作業を実行します。

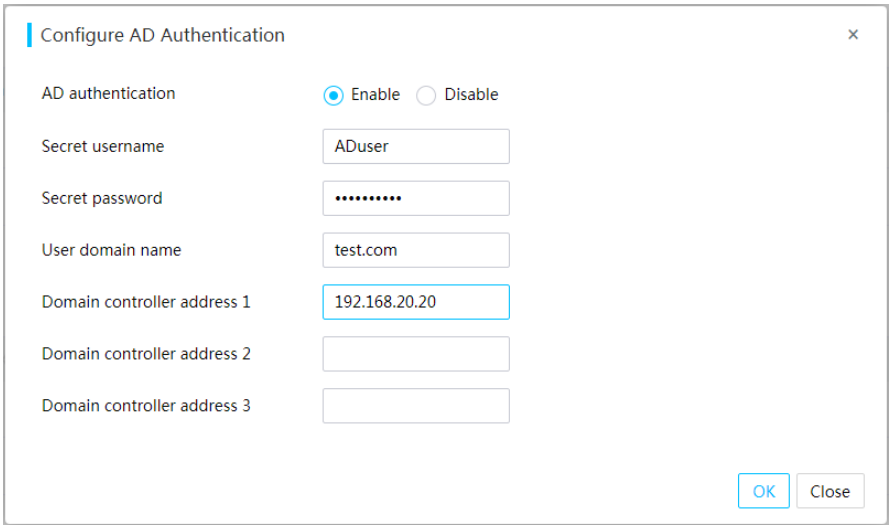
前提条件

AD設定を構成する前に、ADサーバーが使用可能であることを確認します。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **Active Directory**セクションで、**Settings**をクリックします。
5. **AD authentication**の**Enable**または**Disable**を選択します。**Enable**を選択した場合は、必要に応じてAD認証パラメーターを構成します。

図142 AD認証パラメーターの構成



6. **OK**をクリックします。

パラメーター

- **Secret username**: ADサーバーへのログインに使用するユーザー名を、最大64文字の文字列で入力します。ユーザー名には、数字、文字、またはその両方を含めることができ、先頭は文字である必要があります。ユーザー名は任意です。
- **Secret password**: ADサーバーへのログインに使用するパスワードを6～127文字の文字列で入力します。パスワードはオプションです。
- **User domain name**:ユーザードメイン名を入力します。
- **Domain controller address**: ADサーバーのIPアドレスまたはドメイン名を入力します。ドメインコントローラードレス1は必須です。

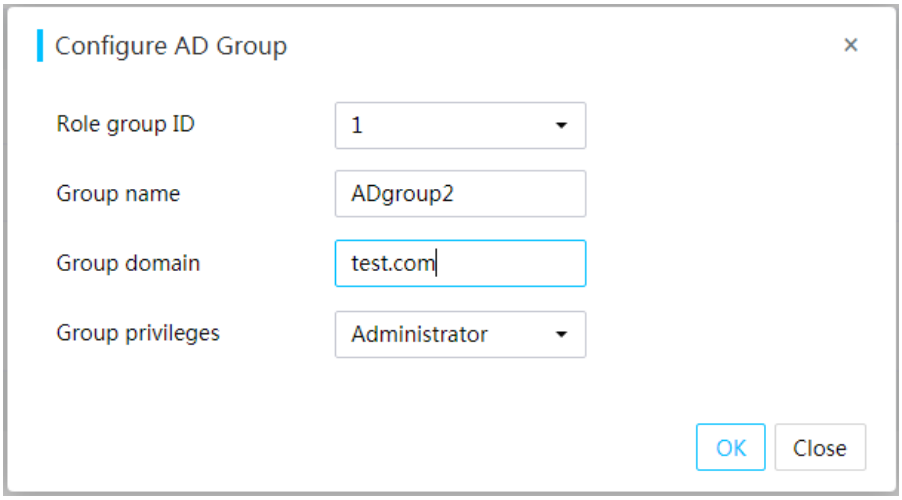
ADグループを管理する

ADグループを追加、編集、または削除するには、次の作業を実行します。

ADグループを追加する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、User Accountsを選択します。
3. **Domain Users**タブをクリックします。
4. **Active Directory**セクションで、**Add role groups**をクリックします。
5. 表示されたダイアログボックスで、ADグループパラメーターを設定します。

図143 ADグループの追加

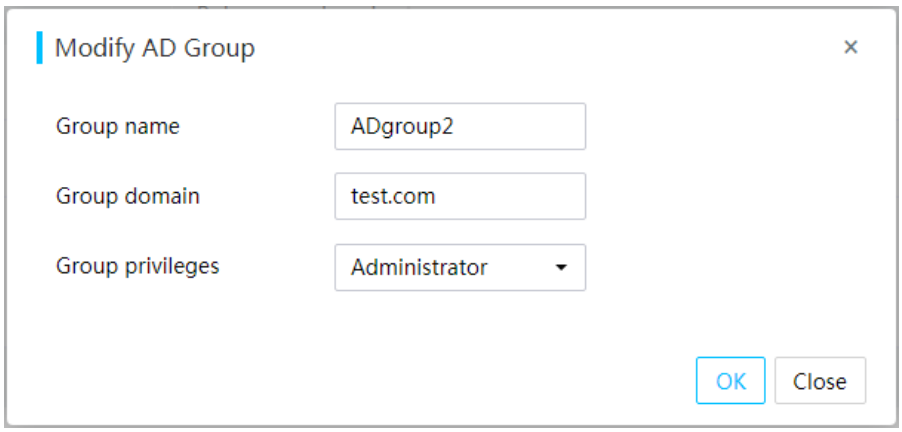


6. **OK**をクリックします。

ADグループを編集する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **Active Directory**セクションで、ADグループリストからターゲットADグループの**Edit**をクリックします。
5. 表示されたダイアログボックスで、ADグループパラメーターを編集します。

図144 ADグループの編集



6. **OK**をクリックします。

ADグループを削除する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **Active Directory**セクションで、ADグループリストからターゲットADグループの**Delete**をクリックします。

パラメーター

- **Role group ID**: ADグループのID。
- **Group name**: ADサーバー上の既存のグループの名前で、1～64文字の文字列です。数字、文字、下線(_)、およびハイフン(-)のみ使用できます。

- **Group domain**: グループが属するドメインの名前で、1～255文字の文字列です。使用できるのは、数字、文字、アンダースコア(_)、ハイフン(-)およびドット(.)のみです。
- **Group privileges**: グループのネットワーク権限。

Two-Factor認証を構成する

Two-Factor認証では、ネットワークセキュリティを強化するために、ログイン試行ごとに静的パスワードと動的パスワードが必要です。

HDMはDKEYトークンをサポートしており、One-Time Password(OTP)サーバーと連携して、ユーザーログインのための2要素認証を提供できます。この機能が設定されている場合、ユーザーはHDMにログインするために、携帯電話またはハードウェアトークンから取得した正しいユーザー名、スタティックパスワード、およびダイナミックパスワードを入力する必要があります。

制限事項とガイドライン

△注意:

この機能は注意して使用してください。2要素認証をイネーブルにすると、HDMログインに影響する可能性があります。

この機能は、ブレードサーバーまたはAEモジュールでは使用できません。この機能は、HDM-2.25以降でのみ使用できます。

2要素認証をイネーブルにする前に、OTPサーバーが使用可能であり、関連する設定がOTPサーバーで設定されていることを確認します。必要な設定には、HDM管理IPアドレス、HDMユーザーカウント(ローカルユーザーおよびドメインユーザー)、認証ポリシー、およびトークンが含まれます。

不正なダイナミックパスワードが原因でユーザーログインが失敗した回数がアカウントロックアウトのしきい値に達した場合、HDMはユーザーをロックしません。

2要素認証をイネーブルにすると、サーバー管理に次のような影響があります。

- 2要素認証をサポートしていない管理ソフトウェアまたは機能(FIST、HDM Mobile、他のサーバーのHDM統合制御など)を使用して、HDM管理アドレスを介して現在のサーバーを管理することはできません。
- 表13に示すように、既存のセッションが終了し、新しいセッションが確立できない場合があります。ただし、これらのインターフェースの設定は変更されません。2要素認証をディセーブルにすると、これらのインターフェースは2要素認証がイネーブルにされる前の状態に戻ります。

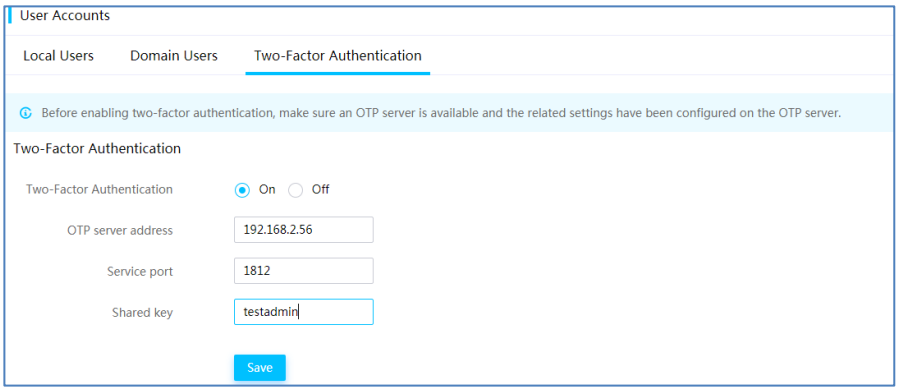
表13セッションの一貫性と確立

インターフェース	既存のセッションまたは接続を切断する	新しいセッションまたは接続をブロックする
Web	しない	しない
SSH	しない	はい
Telnet	しない	しない
VNC	はい	はい
Redfish	しない	はい
IPMI	はい	はい
SNMPv3	しない	はい
SOL	はい	はい

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. ナビゲーションペインで、**User Accounts**を選択します。
3. **Two-Factor authentication**タブをクリックします。
4. **Two-Factor authentication**を設定します。
   a. **Two-factor authentication**をイネーブルにします。
   b. OTPサーバードレス、サービスポート、および共有キーを入力します。

   図145 Two-Factor認証の構成



5. **save**をクリックします。

パラメーター

- **OTP server address**: OTPサーバーのIPv4アドレスまたはドメインアドレスを入力します。
- **Service port**: OTPサーバーのサービスポート番号を入力します。デフォルトは1812です。
- **Shared key**: HDM管理IPアドレスをOTPサーバーに追加するときに設定された共有キーを入力します。共有キーは、大文字と小文字が区別される1～64文字の文字列です。使用できるのは、英字、数字、および特殊文字`~!@$%^&*()_+-=\{};':",./?のみです。

セキュリティ

ファイアウォールを設定する

ファイアウォールは、許可またはブロックされるアクセスを識別するファイアウォール規則に基づいて、HDMを攻撃から保護します。

ファイアウォール設定が不適切なためにHDMにアクセスできない場合は、BIOSからHDMのデフォルト設定を復元して、ファイアウォール規則をクリアできます。詳細については、サーバーのBIOSユーザーガイドを参照してください。

ファイアウォール規則のタイプと優先順位

次のファイアウォール規則を作成できます。

- **Blacklist rules:** 特定のIPアドレスまたはMACアドレスからのHDMサーバーへのアクセスをブロックします。指定した時間範囲内で有効になるようにブラックリスト規則を設定できます。
- **Whitelist rules**: MACアドレスの特定のIPアドレスからHDMサーバーへのアクセスを許可します。指定した時間範囲で有効になるようにホワイトリストルールを構成できます。

ブラックリストルールは、ホワイトリストルールよりも優先されます。

ブラックリストルールの管理

指定されたIPアドレスおよびMACアドレスからのアクセスをブロックするには、ブラックリスト規則を使用します。

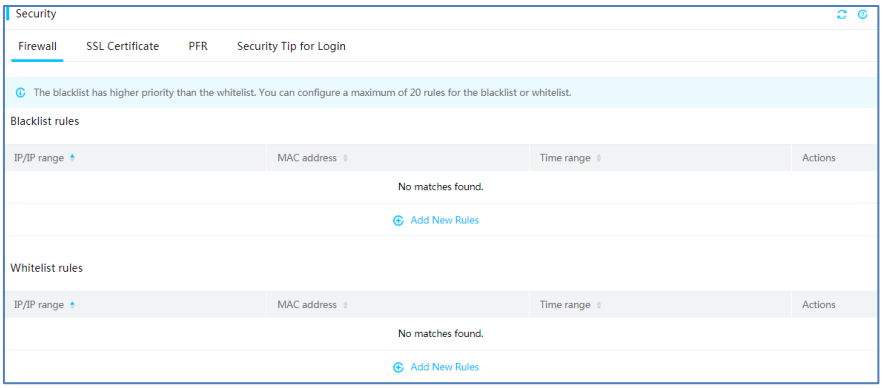
制限事項とガイドライン

- ブラックリストルールには、IPアドレス/IP範囲、MACアドレス、またはその両方を指定する必要があります。
- 時間範囲の設定は、HDMサーバーのシステム時間に基づいて有効になり、HDMと同じタイムゾーンを使用します。HDMサーバーの現在の時間を識別するには、**Dashboard > Summary**に移動します。
- 同じ内容で複数のブラックリスト規則を作成した場合は、そのうちの1つだけが表示されます。

ブラックリストルールを追加する

1. 上部のナビゲーションバーで、**Users & Security**.をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Blacklist rules**セクションで、Add New Rulesをクリックします。図146ブラックリストルールの追加
4. 表示されたダイアログボックスで、IPアドレス/IP範囲、MACアドレス、またはその両方を入力し、ルールが有効になる時間範囲を設定します。デフォルトでは、有効期間は設定されず、ルールは永続的に有効です。

   図147 ブラックリスト規則のパラメーターの設定



5. **OK**をクリックします。

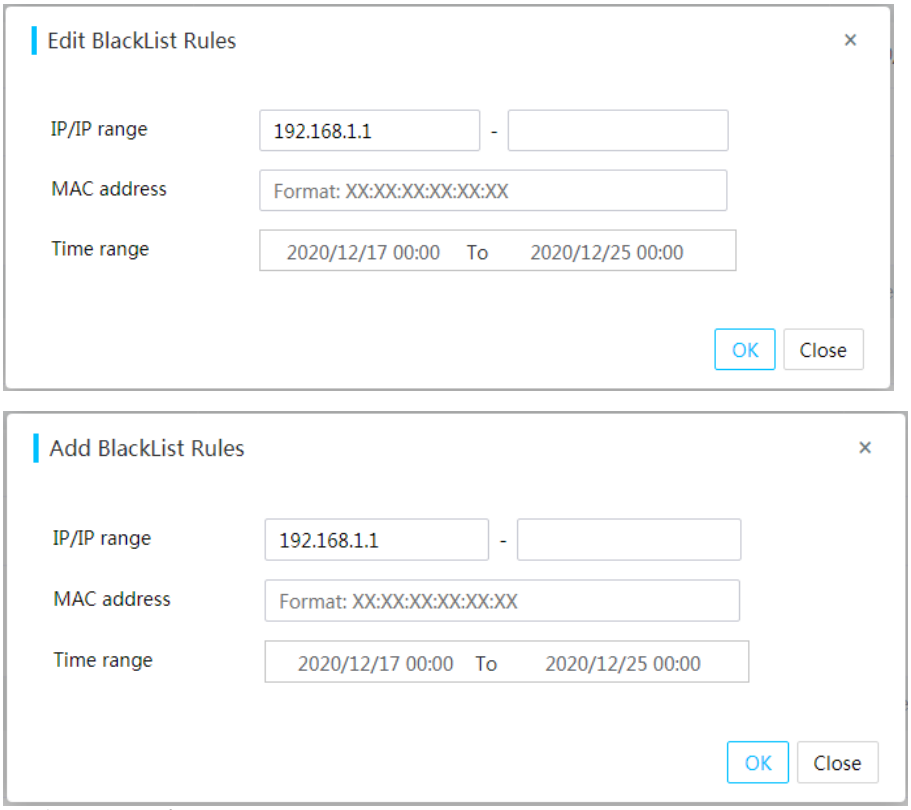
ブラックリストルールを削除する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Blacklist rules**セクションで、ターゲットルールの**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**をクリックします。

ブラックリストルールの編集

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Blacklist rules**セクションで、ターゲットルールの**Edit**をクリックします。
4. 開いたダイアログボックスで、必要に応じてルールを編集します。

図148 ブラックリストルールの編集



5. OKをクリックします。

ホワイトリストルールを管理する

指定されたIPアドレスおよびMACアドレスからのアクセスを許可するには、ホワイトリスト規則を使用します。

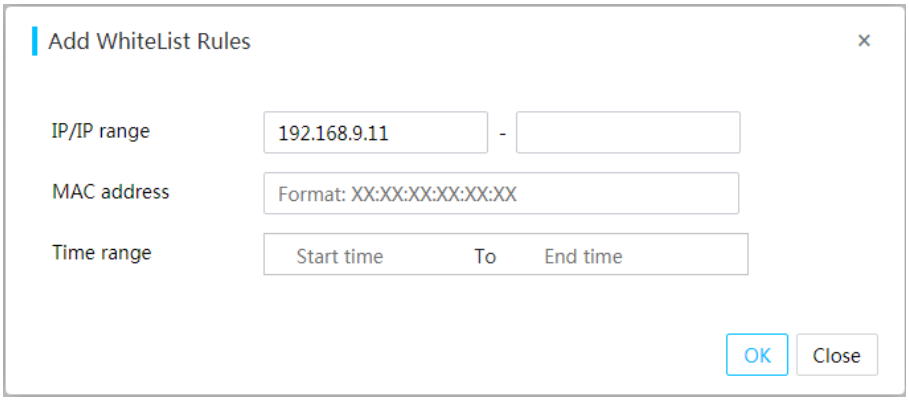
制限事項とガイドライン

- 他のホワイトリスト規則を追加する前に、最初にローカルデバイスのIPアドレスとMACアドレスをホワイトリストに追加します。そうしないと、ローカルデバイスからHDMにアクセスできません。
- ホワイトリスト規則が存在する場合、アドレスがホワイトリストに追加されているデバイスだけがHDMにアクセスできます。
- ホワイトリスト規則を削除するときは、操作の影響を十分に理解していることを確認してください。
- ホワイトリスト規則には、IPアドレス/IP範囲、MACアドレス、またはその両方を指定する必要があります。
- 時間範囲の設定は、HDMサーバーのシステム時間に基づいて有効になり、HDMと同じタイムゾーンを使用します。HDMサーバーの現在の時間を識別するには、**Dashboard > Summary**に移動します。
- 同じコンテンツで複数のホワイトリスト規則を作成した場合は、そのうちの1つだけが表示されます。

ホワイトリストルールを追加する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Whitelist rules**セクションで、**Add New Rules**をクリックします。
4. 表示されたダイアログボックスで、IPアドレス/IP範囲、MACアドレス、またはその両方を入力し、ルールが有効になる時間範囲を設定します。デフォルトでは、有効期間は設定されず、ルールは永続的に有効です。

図149 ホワイトリストルールの追加



5. OKをクリックします。

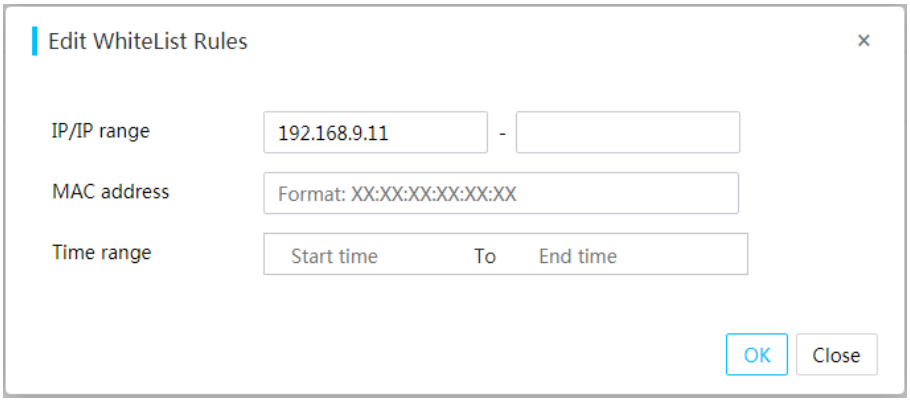
ホワイトリストルールを削除する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Whitelist rules**セクションで、ターゲットルールの**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**をクリックします。

ホワイトリストルールを編集する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **Whitelist rules**セクションで、ターゲットルールの**Edit**をクリックします。
4. 開いたダイアログボックスで、必要に応じてルールを編集します。

図150 ホワイトリストルールの編集



5. OKをクリックします。

SSL証明書を管理する

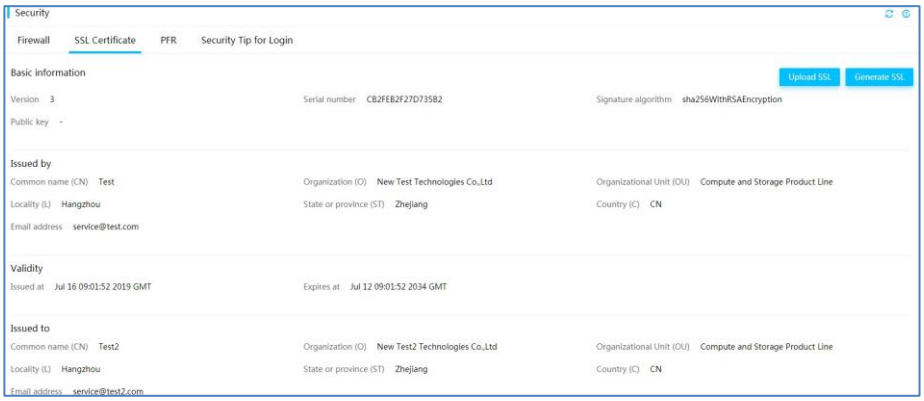
Secure Sockets Layer(SSL)は、HTTPなどのTCPベースのアプリケーション層プロトコルを使用して、インターネットを介してプライベートデータを安全に送信するためのプロトコルです。キーを使用してデータを暗号化および復号化します。SSLを使用すると、Webサーバーおよびクライアントは安全なデータ送信を行い、データソースのアイデンティティを検証し、データの整合性を確保できます。

SSLはHDMアクセスを盗聴やデータ改ざんから保護し、HDMユーザーがSSL証明書認証を通じてHDMサーバーを認証できるようにします。

SSL証明書の表示

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **SSL Certificate**タブをクリックします。
4. 現在のSSL証明書に関する情報を表示します。

図151 SSL証明書の表示



SSL証明書およびキーをHDMにアップロードする

前提条件

SSL証明書をアップロードする前に、次の作業を実行します。

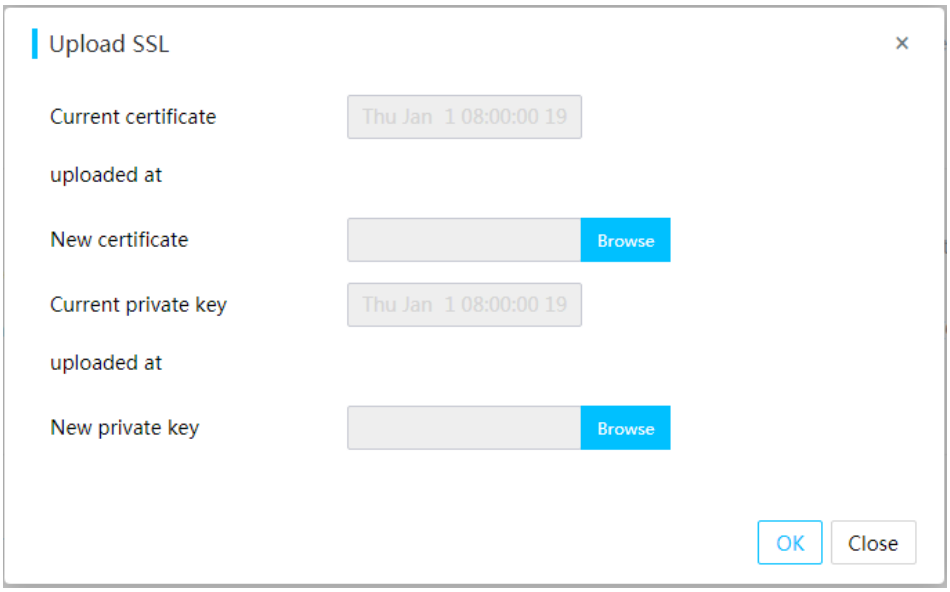
- 管理者ロール、オペレータロール、またはセキュリティ設定を構成する権限を持つユーザーカウントでサインインしていることを確認します。
- **Dashboard > Summary**ページでHDMの日付と時刻を特定し、HDMシステム時刻が証明書の有効期間内であることを確認します。HDMシステム時刻が証明書の有効期間内でない場合、SSL認証は失敗します。
- 証明書ファイルと秘密キーファイルがPEM形式であることを確認します。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **SSL Certificate**タブをクリックします。
4. **Upload SSL**をクリックします。
5. 現在の証明書と秘密キーに関する情報を調べて、新しい証明書と秘密キーのセットが必要かどうかを判断します。
   - **Current certificate uploaded at**: 現在の証明書がアップロードされた日時。
   - **Current private key uploaded at**: 現在の秘密キーがアップロードされた日時。
6. **New certificate**フィールドの横にある**Browse**をクリックし、SSL証明書ファイルを選択します。
7. **New private key**フィールドの横にある**Browse**をクリックし、秘密キーファイルを選択します。
8. **OK**をクリックします。

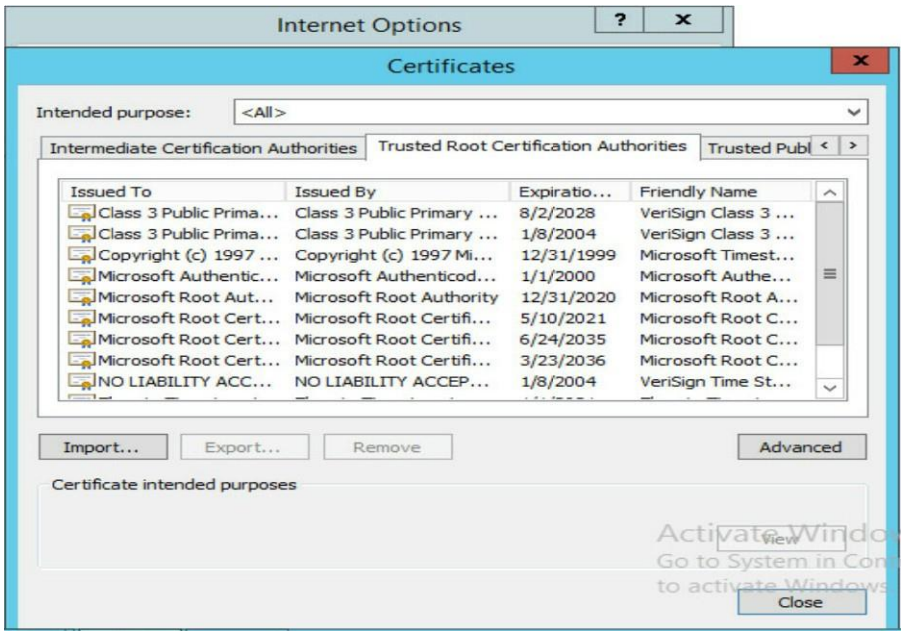
   証明書がアップロードされると、ユーザーセッションは切断されます。HDMサーバーは、その後のサインイン時に新しいSSL証明書を認証に使用します。

図152 SSL証明書およびキーのアップロード



9. 自分で生成したSSL証明書をアップロードした場合は、対応するルート証明書がクライアントブラウザーにすでに存在していることを確認します。この項では、認証局のルート証明書を表示してブラウザーに追加する方法を示すために、IE 11.0を使用します。
   a. ブラウザーを開きます。
   b. ツールバーの**Tools**をクリックし、**Internet options**を選択します。
   c. 表示されたダイアログボックスで、**Content**タブをクリックし、**Certificate**をクリックします。
   d. 信頼されたルート証明機関とルート証明書の有効期限を表示するには、**Trusted Root Certification Authorities**タブをクリックします。
   e. 証明機関がリストにない場合は、Importをクリックしてルート証明書をインポートします。

図153ルート証明書の表示と追加



SSL証明書を生成する

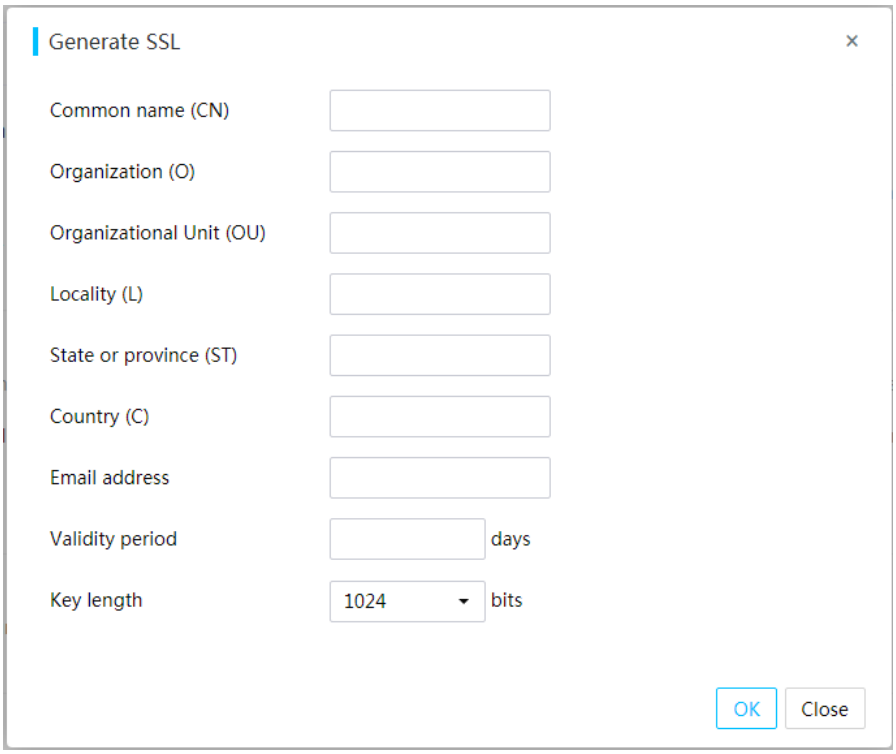
前提条件

SSL証明書を生成するには、管理者の役割が必要です。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**Security**を選択します。
3. **SSL Certificate**タブをクリックします。
4. **Generate SSL**をクリックします。
5. 証明書パラメーターを設定します。

   図154 証明書パラメーターの構成



6. **OK**をクリックします。
7. 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。

   証明書が生成された場合は、成功結果メッセージが表示されます。

   HDMサーバーは、その後のサインイン時に認証に新しいSSL証明書を使用します。

パラメーター

- **Common name (CN)**: HDMサーバーの完全ドメイン名で、1～64文字の文字列です。文字、数字、スペース、アンダースコア(_)、ハイフン(-)、およびドット(.)のみ使用できます。共通名に数字のみの文字列は使用できません。
- **Organization (O)**: HDMサーバーを所有する組織の名前。1から64文字の文字列です。文字、数字、スペース、アンダースコア(_)、ハイフン(-)およびドット(.)のみ使用できます。組織名は数字のみの文字列にはできません。
- **Organizational Unit (OU)**: 組織内でHDMサーバーを所有する単位の名前で、1～64文字の文字列です。使用できるのは、文字、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。組織単位名は数字のみの文字列にはできません。
- **Locality (L)**: HDMサーバーが存在する市または郡(1～128文字の文字列)。文字、数字、スペース、アンダースコア(_)、ハイフン(-)およびドット(.)のみ使用できます。地域名は数字のみの文字列にはできません。
- **State or province (ST)**: HDM存在する都道府県。1～128文字の文字列。文字、数字、スペース、アンダースコア(_)、ハイフン(-)およびドット(.)のみ使用できます。都道府県名は数字のみの文字列にはできません。

- **Country (C)** :HDMサーバーが存在する国または地域。国/地域は2文字のコードで表されます。
- **Email address**: HDMサーバーのオーナーに連絡できる電子メールアドレス。
- **Validity period**: SSL証明書の有効期間(1～5475日の範囲)。
- **Key length**: 証明書のキーの長さ。
- **Basic information**: 現在のSSL証明書に関する基本情報。
  - **Version**: 証明書のバージョン番号。
  - **Serial number**: 証明書のシリアル番号。この番号はCertificate Authority(CA)によって割り当てられます。
  - **Signature algorithm**: 証明書の署名アルゴリズム。
  - **Public key**: 証明書の公開キー情報。
- **Issued by**: 証明書を発行した認証局。
- **Validity**: 証明書の有効期限。
  - **Issued at**: 証明書の最初の有効な日付。
  - **Expires at**: 証明書の有効期限日。
- **Issued to** :証明書の発行先のエンティティ。

PFRの設定

Platform Firmware Resiliency(PFR)は、HDMを攻撃から保護するために使用されるテクノロジーです。PFRがイネーブルの場合、PFRはHDMの起動時にHDMファームウェアイメージを確認します。

- プライマリHDMファームウェアイメージが検証に合格した場合、HDMはプライマリイメージから開始します。
- プライマリHDMファームウェアイメージが破損している場合、PFRはバックアップHDMファームウェアイメージを検証します。バックアップイメージが検証に合格した場合、HDMはバックアップイメージから開始します。
- プライマリおよびバックアップHDMファームウェアイメージの両方が破損していても、プライマリイメージへの破損がHDMの起動に影響しない場合、HDMはプライマリイメージから起動します。

ハードウェアと機能の互換性

この機能をサポートしているのは、G5シリーズサーバーだけです。

ソフトウェアのバージョンと機能の互換性

この機能は、HDM-2.13以降でのみサポートされています。

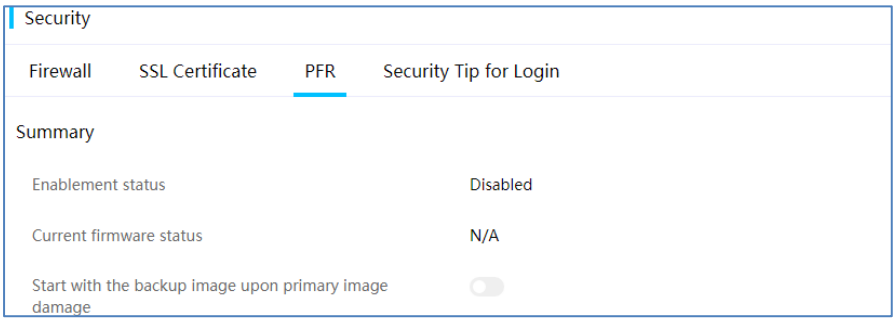
制限事項とガイドライン

- 破損したファームウェアイメージを更新して修正できます。
- PFRをイネーブルにすると、HDMの起動時間が延長されます。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. ナビゲーションペインで、**Security**を選択します。
3. **PFR**タブをクリックします。
4. プライマリイメージが破損したときに、HDMがバックアップイメージから開始できるようにするかどうかを選択します。

図155 PFRタブ



パラメーター

- **Enablement status**: PFRのイネーブル化ステータス。
- **Current firmware status**: この起動時にHDMファームウェアイメージを検証した結果。
- **Start with the backup image upon primary image damag**始: HDMをバックアップファームウェアイメージから開始できるかどうかを選択します。この機能はデフォルトで無効になっています。この機能を有効にすると、プライマリイメージが検証に失敗し、バックアップイメージが検証に合格した場合に、HDMはバックアップファームウェアイメージから開始できます。

ログインのセキュリティヒントを設定します

ログインページに表示されるセキュリティヒントを設定するには、次の作業を実行します。

ソフトウェアのバージョンと機能の互換性

この機能は、HDM-2.13以降でのみサポートされています。

制限事項とガイドライン

セキュリティヒントには、1～1024バイトを含めることができます。有効な文字は、英字、数字、漢字、および特殊文字です。ただし、左山カッコ(<)と右山カッコ(>)は除きます。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. ナビゲーションペインで、**Security**を選択します。
3. **Security Tip for Login**タブをクリックします。
4. **Display security tip at login**を有効にします。
5. (任意)セキュリティヒントを設定します。
6. **save**をクリックします。

   設定が正常に完了したら、ログインページで設定済みのセキュリティヒントを表示できます。

図156 ログインのためのセキュリティヒントの構成

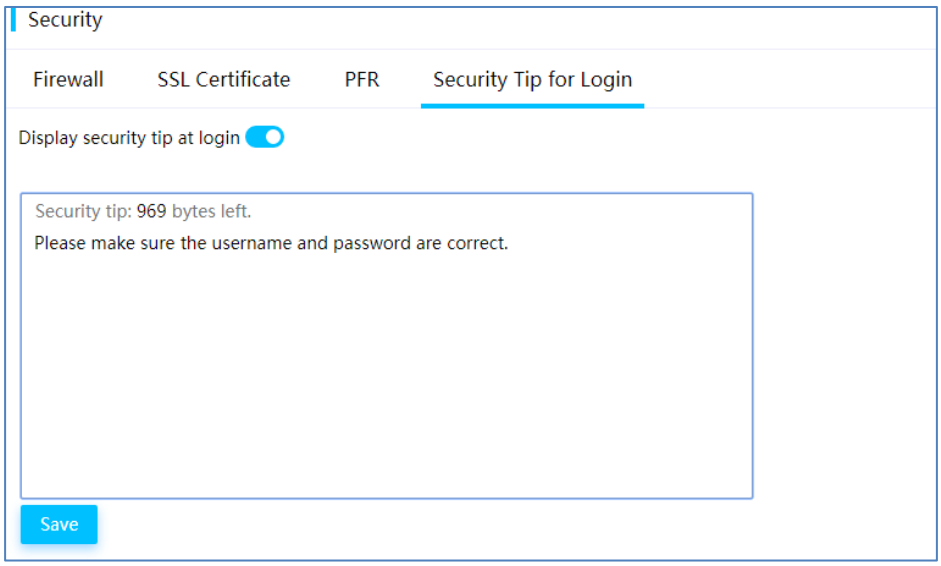
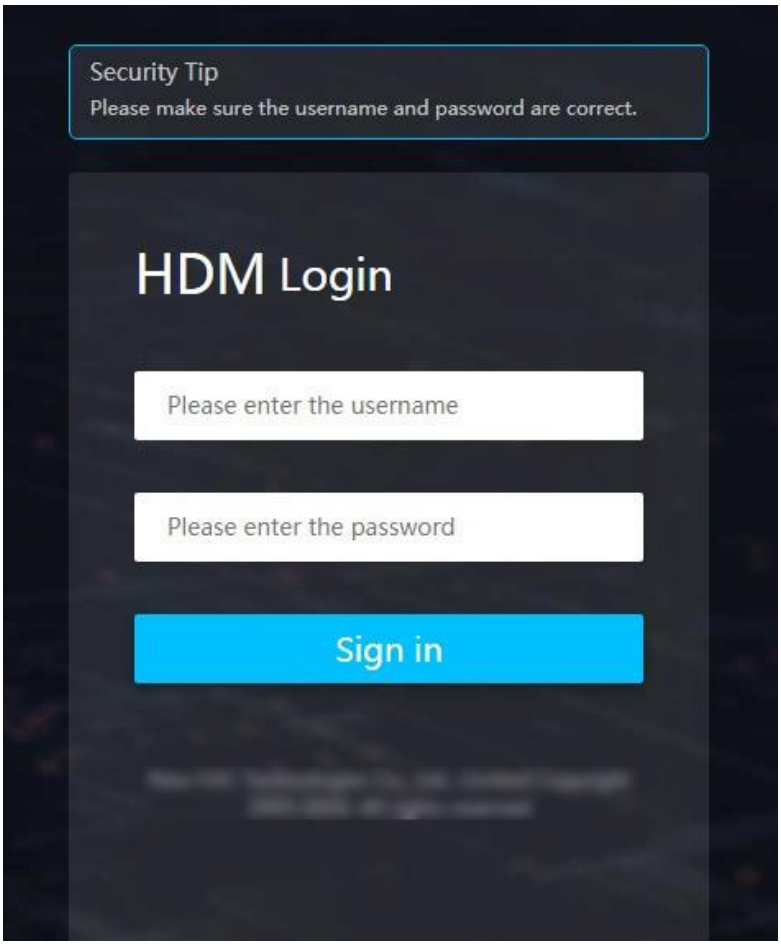


図157 ログイン時のセキュリティのヒント



セキュリティモジュール

TPM/TCMステータスの表示

トラステッドプラットフォームモジュール(TPM)は、システムボードに組み込まれたマイクロチップです。TPMには、サーバーのハードウェアおよびソフトウェアを認証するための暗号化情報(暗号化キーなど)が格納されています。トラステッド暗号化モジュール(TCM)は、保護された記憶域を持つトラステッドコンピューティングプラットフォームベースのハードウェアモジュールで、プラットフォームがパスワード計算を実装できるようにします。TPM/TCMモジュールの詳細については、サーバーのユーザーガイドを参照してください。

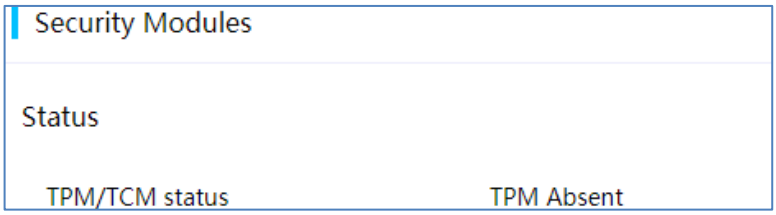
制限事項とガイドライン

この機能は、HDM-2.14以降でのみ使用できます。

手順

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. ナビゲーションペインで、**Security Modules**を選択します。
3. 開いたタブで、TPMまたはTCMのステータスを表示できます。TPMとTCMの両方がサポートされていない場合、このフィールドには**N/A**と表示されます。

   図158 TPMまたはTCMのステータスの表示



統合された制御

統合制御を使用して、バルクで最大10台のデバイスを管理します。次のタスクを実行できます。

- デバイスを追加する
- デバイス情報を表示する
- HDMにアクセスする
- 電源操作を実行する
- H5 KVMリモートコンソールを起動する
- デバイスの削除

デバイスを追加する

デバイスを1つずつ、またはまとめて追加するには、次の作業を実行します。

制限事項とガイドライン

指定されたIP範囲には、最大255個のIPアドレスを含めることができます。

指定されたIP範囲に10を超えるデバイスのIPアドレスが含まれている場合、システムは最初に情報を取得した10のデバイスを追加します。

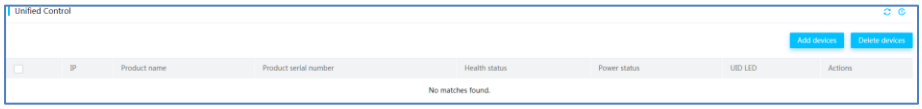
デバイスのHDMログインユーザー名またはパスワードを統合制御に追加した後に変更した場合、デバイスは統合制御インターフェースからアクセスできなくなります。

一度にデバイスを追加できるユーザーは1人だけです。

手順

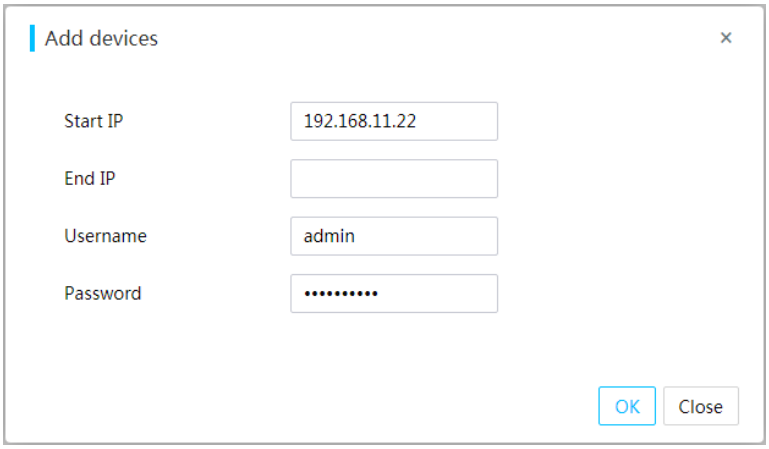
1. ナビゲーションペインで、**Unified Control**を選択します。

図159 統合制御ページ



2. **Add devices**をクリックします。
3. 表示されたダイアログボックスで、デバイスの開始および終了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。

図160 デバイスの追加



パラメーター

- **Start IP**:HDM管理IPアドレスまたはHDM管理IP範囲の開始IPアドレスを入力します。サポートされているのはIPv4アドレスだけです。このフィールドは必須です。
- **End IP**:エンドHDM管理IPアドレスを入力します。IPv4アドレスだけがサポートされます。このフィールドはオプションです。
- **Username**: HDMログインのユーザー名を入力します。ベストプラクティスとして、管理者ユーザーのユーザー名を入力します。管理者以外のユーザーのユーザー名を入力すると、一部の機能が使用できなくなります。
- **Password**:HDMログイン用のパスワードを入力します。

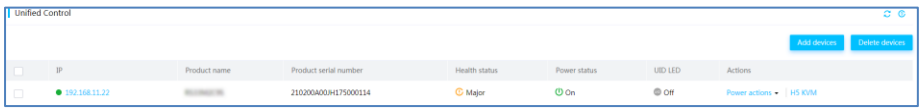
デバイス情報を表示する

追加されたデバイスに関する情報(IPアドレス、製品名、製品シリアル番号、ヘルスステータス、電源ステータス、UID LEDステータスなど)を表示するには、次の作業を実行します。

手順

ナビゲーションペインでUnified Controlを選択し、追加されたデバイスに関する情報を表示します。

図161 デバイス情報の表示



パラメーター

- **IP**:サーバーのHDM管理IPアドレス。
- **Health status**:サーバーのヘルスステータス。
  - **Normal**: すべてのサーバーコンポーネントが正常に動作しています。
  - **Critical**、**Major**、または**Minor**: 少なくとも1つのコンポーネントで問題が発生しています。

- **Power status**:サーバーの電源ステータス。
  - **On** -サーバーの電源が入っています。
  - **Off** -サーバーの電源がオフになっています。
- **UID LED**:UID LEDのステータス。
  - **On** -サーバーのUID LEDは青色に点灯しています。
  - **Off** -サーバーのUID LEDが消灯しています。
  - **Flashing** -サーバーのUID LEDが青色で点滅しています。サーバーがファームウェアを更新しているか、リモートコンソールが起動されています。

HDMにアクセスする

特定のサーバーのHDMインターフェースにアクセスするには、次の作業を実行します。

前提条件

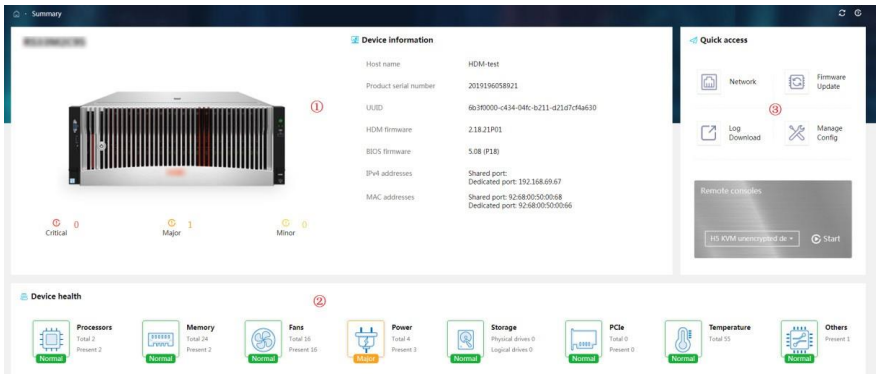
デバイスに指定されたユーザーカウントにHDMへのアクセス権限があることを確認します。ユーザー権限はユーザーロールによって決定されます。

手順

1. ナビゲーションペインで、**Unified Control**を選択します。
2. ターゲットサーバーのIPアドレスリンクをクリックします。

   図162に示すように、サーバーのHDMインターフェースが開きます。

   図162 指定されたサーバーのHDMインターフェース



電源操作を実行する

△注意:

強制電源切断、強制システムリセットおよび強制電源再投入の各アクションは、データの破損または損失の原因となる可能性があります。これらのアクションを実行するときは、サービスへの影響を十分に理解していることを確認してください。

サーバーの電源ステータスを管理するには、次の作業を実行します。

前提条件

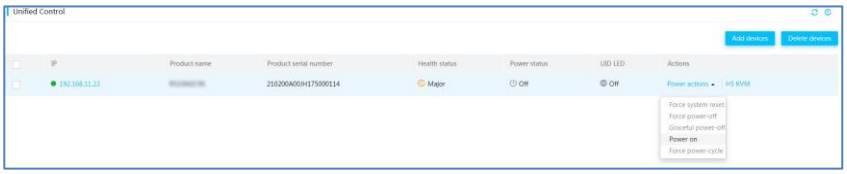
デバイスに対して指定したユーザーカウントに、管理者、オペレータ、または電源制御の役割があることを確認します。

手順

1. ナビゲーションペインで、**Unified Control**を選択します。
2. ターゲットサーバーのエントリーを識別します。

3. 図163に示すように、サーバーの電源操作を選択します。
   - サーバーの電源を再投入せずにサーバーをウォームリブートするには、**Force system reset**を選択します。
   - 強制的にサーバーをただちにシャットダウンするには、**Force power-off**を選択します。この操作は、サーバーの電源ボタンを5秒間押し続けるのと同じです。
   - 最初にオペレーティングシステムをシャットダウンしてからサーバーの電源を切るには**Graceful power-off**。
   - サーバーを起動するには、**Power on**を選択します。
   - サーバーの電源をオフにしてからオンにするには、**Force power-cycle**を選択します。

図163 電源操作の実行



H5 KVMリモートコンソールを起動する

H5 KVMリモートコンソールからサーバーを操作するには、次の作業を実行します。

前提条件

H5 KVMリモートコンソールを起動する前に、次のタスクを実行する必要があります。

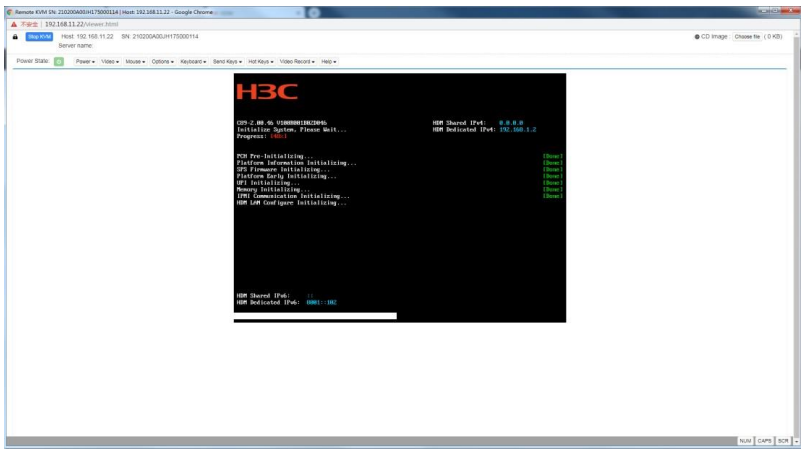
- デバイスに指定されたユーザーカウントにKVM拡張権限があることを確認します。ユーザーカウントに権限がない場合は、ユーザーカウントを編集します。詳細は、「ユーザーカウントの編集」を参照してください。
- デバイスに指定されたユーザーカウントがKVMサービスで使用可能であることを確認します。KVMが使用可能でない場合は、最初にKVMサービスを使用可能にします。詳細は、「アクセスサービスの編集」を参照してください。

手順

1. ナビゲーションペインで、**Unified Control**を選択します。
2. ターゲットサーバーエントリーの**H5 KVM**をクリックします。

   H5 KVMリモートコンソールの詳細については、「リモートコンソール」を参照してください。

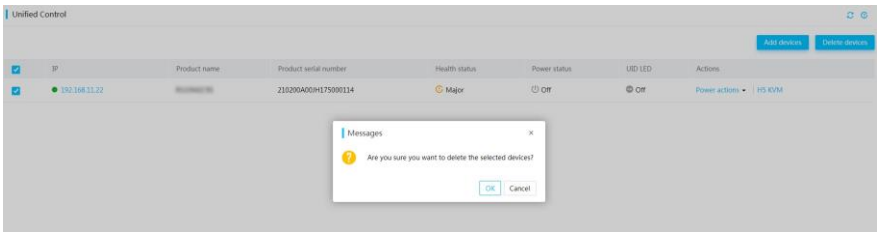
図164 セカンダリユーザーのリモートコンソール



デバイスの削除

1. ナビゲーションペインで、**Unified Control**を選択します。
2. 1つまたは複数のサーバーを選択します。
3. **Delete devices**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**をクリックします。

図165デバイスの削除



共通の操作

ここでは、HDM設定での一般的な操作について説明します。

仮想メディアを構成する

Windows CIFSサーバーを使用したイメージのマウント

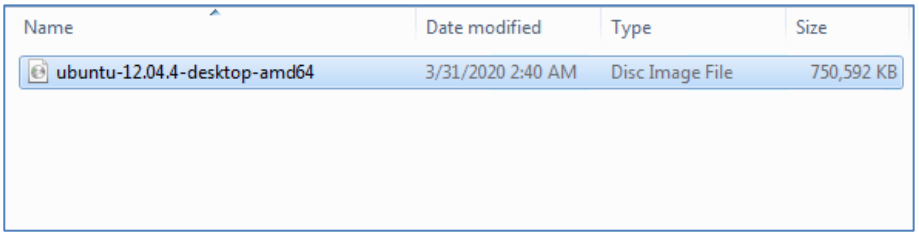
Common Internet File System(CIFS)を使用すると、HDMはリモートサーバー上のファイルにアクセスできます。Windows OSにはCIFSソフトウェアが組み込まれており、CIFSのインストールは必要ありません。

このセクションでは、例としてWindows 7を使用します。

Windows CIFSサーバーを介してイメージをマウントするには、次の手順を実行します。

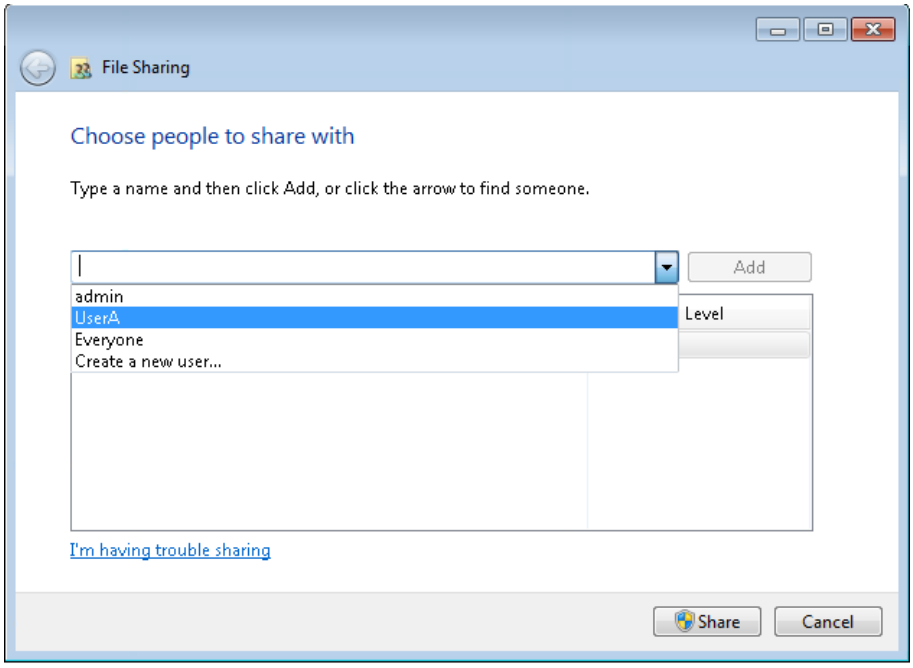
1. ターゲットイメージファイルをローカルパスにコピーします。このセクションでは、例として**D:\IMAGE 2**を取り上げます。

   図166イメージファイルをローカルパスにコピーする

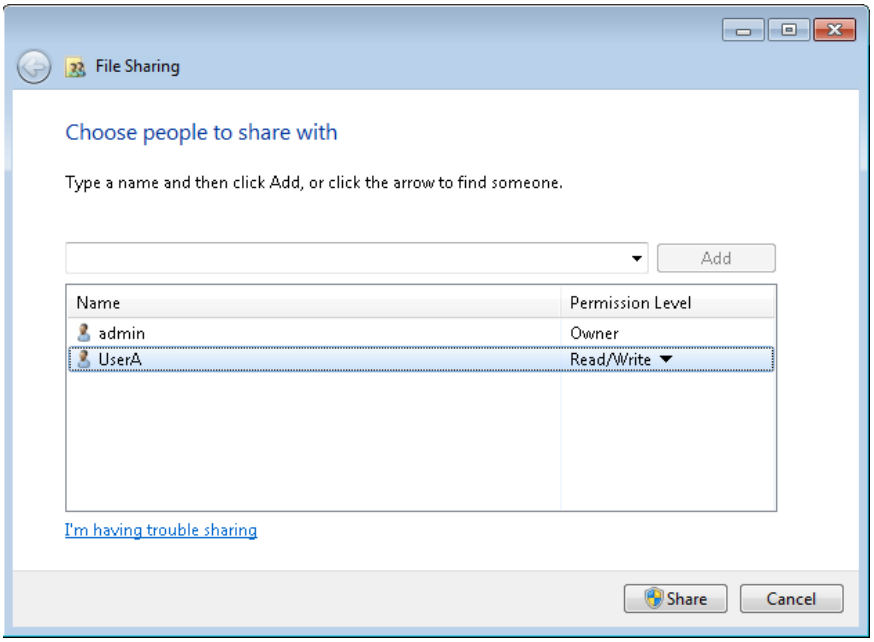
2. ファイル共有を設定します。
   a. **IMAGE 2**ファイルフォルダを右クリックし、**Share with > Specific people**を選択します。
   b. 必要に応じてユーザーを追加します。このセクションでは、例として**UserA**を使用します。

図167ファイル共有設定の構成



c. **Permission Level**列から各ユーザーの読み取り/書き込みアクセス許可を選択します。

図168ユーザーの追加

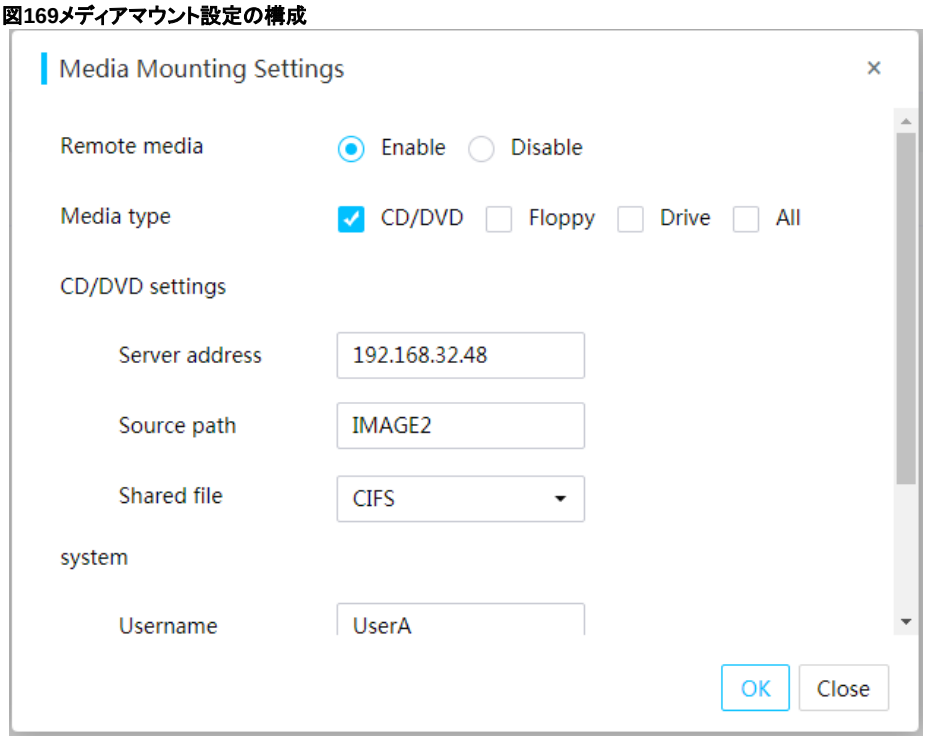


3. HDMにアクセスし、メディアマウント設定を構成します。
   a. 上部のナビゲーションバーで、**Remote Services**をクリックします。
   b. 左側のナビゲーションペインで、**Virtual Media**を選択します。
   c. 作業ウィンドウで、**Settings**をクリックします。
   d. 表示されたダイアログボックスで、リモートメディアを有効にします。
   e. メディアタイプとして**CD/DVD**を選択します。
   f. CIFSサーバーのIPアドレスとソースパスとして**IMAGE2**を指定します。この例では、サーバーアドレスは192.168.32.48です。

g. 共有ファイルシステムとして**CIFS**を選択します。

h. 共有イメージファイルにアクセスするためのユーザー名とパスワードを入力します。

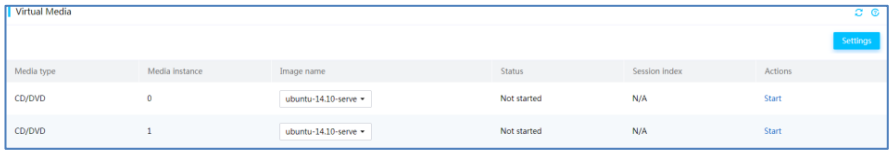
図169メディアマウント設定の構成



4. **OK**をクリックします。

仮想メディアページには、マウントされているイメージが表示されます。

図170 仮想メディアページ



Linux CIFSサーバー経由でイメージをマウントする

Common Internet File System(CIFS)は、Server Messages Block(SMB)のオープンバージョンであり、アプリケーションがリモートサーバー上のファイルにアクセスできるようにします。

Linux CIFSサーバーを設定するには、デバイスにSambaソフトウェアをインストールする必要があります。このセクションでは、例としてRed Hat Enterprise Linux 7.3を使用します。

Sambaのインストールと設定

1. **yum-y install samba samba-common samba-client**コマンドを実行して、Sambaをインストールします。

   samba-commonキーワードと**samba-client**キーワードは、それぞれSambaサーバーとSambaクライアントを表します。サーバーとクライアントの両方をインストールするには、両方のキーワードを指定することをお勧めします。

2. **yum list installed | grep samba**コマンドを実行して、SambaサーバーとSambaクライアントの両方が正常にインストールされていることを確認します。

3. **testparm**コマンドを実行して、Sambaが図171に示すように正しく構成されていることを確認します。

図171 Sambaパラメーターの確認

```
[root@localhost ~]# testparm
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Registered MSG_REQ_POOL_USAGE
Registered MSG_REQ_DMALLOC_MARK and LOG_CHANGED
Load smb config files from /etc/samba/smb.conf
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)
Processing section "[homes]"
Processing section "[printers]"
Processing section "[print$]"
Loaded services file OK.
Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        printcap name = cups
        security = USER
        workgroup = SAMBA
        idmap config * : backend = tdb
        cups options = raw


[homes]
        browseable = No
        comment = Home Directories
        inherit acls = Yes
        read only = No
        valid users = %S %D%w%S


[printers]
        browseable = No
        comment = All Printers
        create mask = 0600
```

4. **systemctl start smb**コマンドを実行してSambaサービスを開始し
   systemctl status smbコマンドを使用して、サービスが正常に動作していることを確認します。
5. ファイアウォールとSELinuxを無効にします。
   systemctl stop firewall getenforce
   setenforce 0
6. **pdbedit-L**コマンドを実行して、Sambaユーザーが存在することを確認します。ユーザーが存在しない場合は、**smbpasswd-a username**コマンドを実行してユーザーを追加します。この例では、ユーザー名は**ldt**です。

   追加したユーザーがサーバーOSにすでに存在していることを確認します。OSの既存のユーザーを表示するには、**cat /etc/passwd**コマンドを実行します。

   図172 Sambaユーザーの追加

```
[root@localhost ~]# smbpasswd -a ldt
New SMB password:
Retype new SMB password:
Added user ldt.
```

7. **smbclient -L** //OS_IP_addressコマンドを実行して、Sambaサーバーにアクセスします。この例では、アドレスは10.99.205.165です。

図173 Sambaサーバーへのアクセス

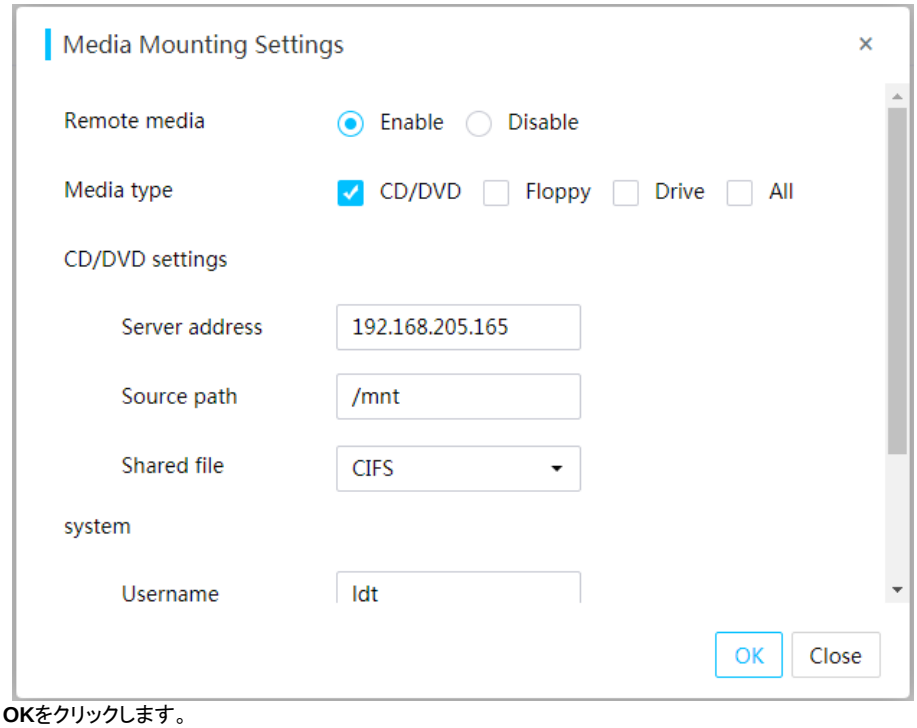
```
[root@localhost ~]# smbclient -L//10.99.205.165
Enter SAMBA\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        mnt             Disk      /mnt dir
        IPC$            IPC       IPC Service (Samba 4.9.1)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
```

8. **/etc/samba/smb.conf**構成ファイルを編集して、共有ファイルパスを作成します。この例では、パスは**/test**です。
   vi /etc/samba/smb.conf
   [mnt]comment=/mnt dir path=/test
9. **systemctl restart smb**コマンドを実行して、Sambaを再起動します。
10. ファイルをアップロードしてパスに共有します。この例では、ファイルの名前は**test.iso**です。

イメージをHDMにマウントする

1. HDMにアクセスします。
2. 上部のナビゲーションバーで、**Remote Services**をクリックします。
3. 左側のナビゲーションペインで、**Virtual Media**を選択します。
4. 作業ウィンドウで、**Settings**をクリックします。
5. 表示されたダイアログボックスで、リモートメディアを有効にします。
   a. メディアタイプとして**CD/DVD**を選択します。
   b. SambaサーバーのIPアドレスおよび**/mnt**をソースパスとして指定します。この例では、サーバーアドレスは10.99.205.165です。
   c. 共有ファイルシステムとして**CIFS**を選択します。
   d. Sambaユーザーのユーザー名とパスワードを入力します。
   e. (任意)ドメイン名を入力します。

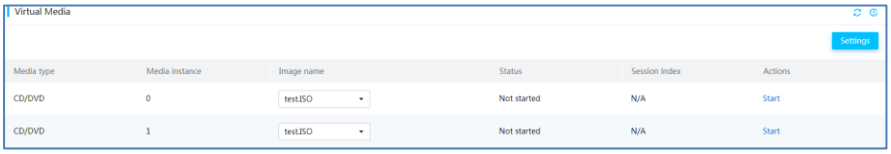
図174メディアマウント設定の構成



6. **OK**をクリックします。

   Virtual Mediaページには、マウントされているイメージが表示されます。

図175仮想メディアページ



HDM設定のインポート

HDMユーザーカウントをインポートする

制限事項とガイドライン

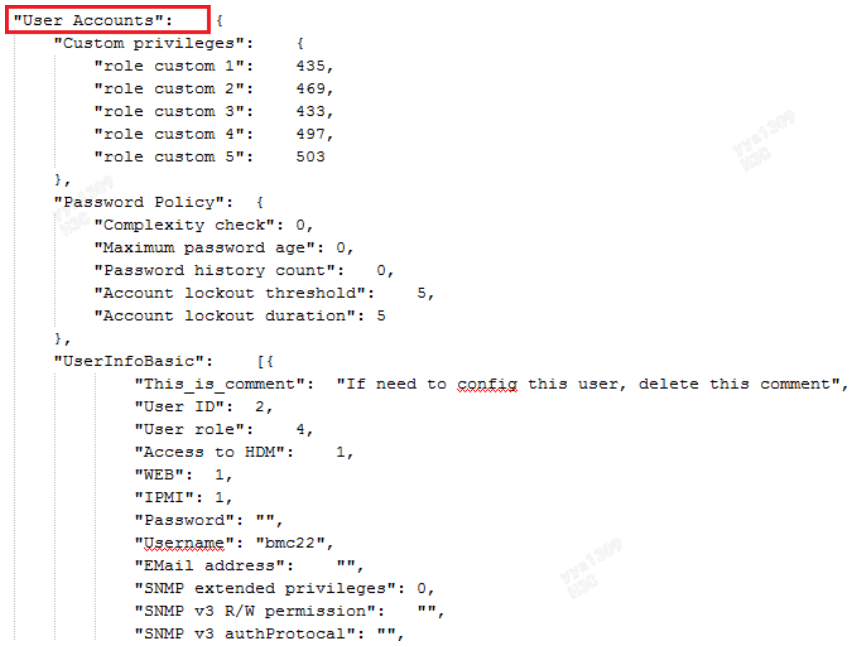
インポートする構成ファイル内のサーバーモデルが実際のサーバーモデルと一致していることを確認してください。

サーバーからエクスポートされた構成ファイルのパスワードフィールドは空です。構成ファイルをそのソースサーバーにインポートするには、パスワードフィールドを空のままにするか、必要に応じてパスワードを指定します。構成ファイルを同じモデルの別のサーバーにインポートするには、構成ファイルでパスワードを指定する必要があります。

手順

1. 構成ファイルを開き、**User Accounts**を検索します。

図176ユーザーカウント情報の検索



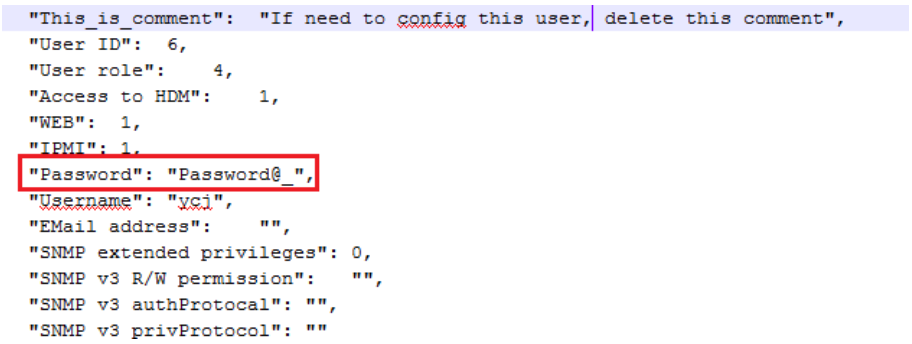
```
"User Accounts":    {
    "Custom privileges":    {
        "role custom 1":    435,
        "role custom 2":    469,
        "role custom 3":    433,
        "role custom 4":    497,
        "role custom 5":    503
    },
    "Password Policy":  {
        "Complexity check": 0,
        "Maximum password age": 0,
        "Password history count":   0,
        "Account lockout threshold":    5,
        "Account lockout duration": 5
    },
    "UserInfoBasic":    [{
            "This_is_comment":  "If need to config this user, delete this comment",
            "User ID":  2,
            "User role":    4,
            "Access to HDM":    1,
            "WEB":  1,
            "IPMI": 1,
            "Password": "",
            "Username": "bmc22",
            "EMail address":    "",
            "SNMP extended privileges": 0,
            "SNMP v3 R/W permission":   "",
            "SNMP v3 authProtocal": "",
```

2. 既存のユーザーのパスワードを編集するには、そのユーザーのcomment文を削除してから、新しいパスワードを設定します。

   既存のユーザーのパスワードを保持するには、ユーザーのパスワードフィールドを空のままにします。

   図176の複雑性チェックフィールドに1と表示されている場合は、入力するパスワードが複雑性要件を満たしていることを確認します。

図177 新しいパスワードの構成



```
"This_is_comment":  "If need to config this user, delete this comment",
"User ID":  6,
"User role":    4,
"Access to HDM":    1,
"WEB":  1,
"IPMI": 1,
"Password": "Password@_",
"Username": "yci",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocal": "",
"SNMP v3 privProtocol": ""
```

3. 新しいユーザーカウントを追加するには、ユーザーのコメント文を削除してから、ユーザー名とパスワードを指定します。

   新しいユーザーカウントには、ユーザー名フィールドとパスワードフィールドが必要です。

   図176の複雑性チェックフィールドに1と表示されている場合は、入力するパスワードが複雑性要件を満たしていることを確認します。

図178 コメント文の削除

```
"This_is_comment":  "If need to config this user, delete this comment",
"User ID":  7,
"User role":    15,
"Access to HDM":    0,
"WEB":  1,
"IPMI": 1,
"Password": "",
"Username": "",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocal": "",
"SNMP v3 privProtocol": ""
```

図179 ユーザー名とパスワードの設定

```
"User ID":  7,
"User role":    15,
"Access to HDM":    0,
"WEB":  1,
"IPMI": 1,
"Password": "Password@123",
"Username": "Test33",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocal": "",
"SNMP v3 privProtocol": ""
```

4. ユーザーの役割を構成し、HDMへのアクセスを有効にするには、「ユーザーの役割」フィールドと「HDMへのアクセス」フィールドをそれぞれ設定します。フィールドでサポートされるオプションについては、表14を参照してください。

図180 ユーザー権限の構成

```
"User ID":  7,
"User role":    4,
"Access to HDM":    1,
"WEB":  1,
"IPMI": 1,
"Password": "Password@123",
"Username": "Test33",
"EMail address":    "",
"SNMP extended privileges": 0,
"SNMP v3 R/W permission":   "",
"SNMP v3 authProtocal": "",
"SNMP v3 privProtocol": ""
```

5. 必要に応じてその他の設定を変更します。

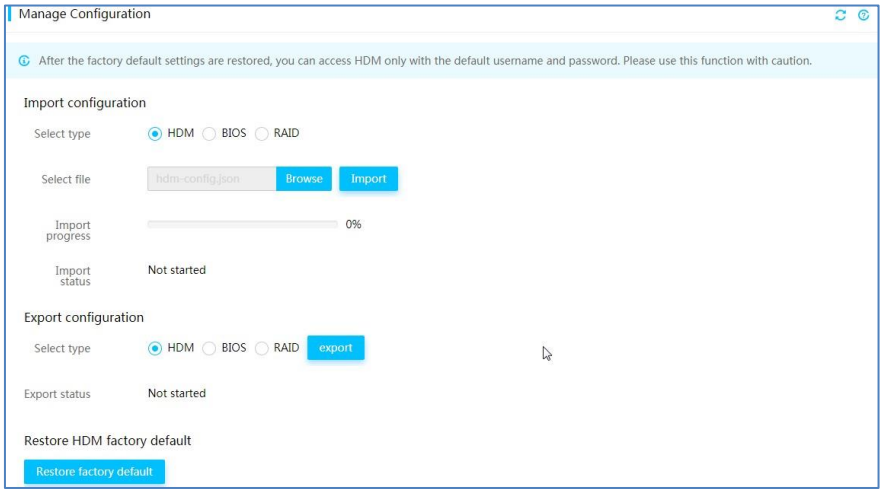
   設定可能なフィールドの詳細については、表14を参照してください。

表14構成可能アイテムの説明

項目	説明
Role customs 1から5	カスタムユーザーロール1から5の権限。各ロールカスタムフィールドには、9ビットのバイナリ番号に相当する10進数が表示されます。各ビットは次のように権限を表します。 • **Bit** 0:リモートコントロール。 • **Bit** 1:リモートメディア。 • **Bit** 2:セキュリティ設定。 • **Bit** 3:ユーザーカウントの設定。 • **Bit** 4:基本設定。 • **Bit** 5-電力制御。 • **Bit** 6-メンテナンス。 • **Bit** 7:情報クエリー。 • **Bit** 8:パスワードの変更。 ビット値は、特権のイネーブル化ステータスを次のように示します。 • 1:イネーブル。 • 0:ディセーブル。
ユーザーID	ユーザーID(2～16)。ユーザーIDは一意である必要があります。
ユーザーロール	ユーザーの役割を指定します。 • 2: user。 • 3: operator。 • 4: Administrator。 • 6-CustomRole 1 • 7-CustomRole 2 • 8-CustomRole 3 • 9-CustomRole 4 • 10-CustomRole 5 • 15:なし。
HDMへのアクセス	HDMへのアクセスを無効または有効にするには、0または1を入力します。
Web	0または1を入力して、Web拡張には、または1を入力します。
IPMI	0または1を入力して、IPMI拡張特権をディセーブルまたはイネーブルにします。

6. 構成ファイルを保存してインポートします。
   a. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
   b. 左側のナビゲーションペインで、**Manage Configuration**を選択します。
   c. 構成ファイルをインポートします。
      インポート操作が終了すると、HDMは自動的に再起動します。

図181構成ファイルのインポート



7. 設定を確認するには、HDMの再起動後にHDMに再度サインインし、**Users & Security > User Accounts**ページにアクセスしてHDMユーザーカウントを表示します。

図182 HDMへの再サインイン

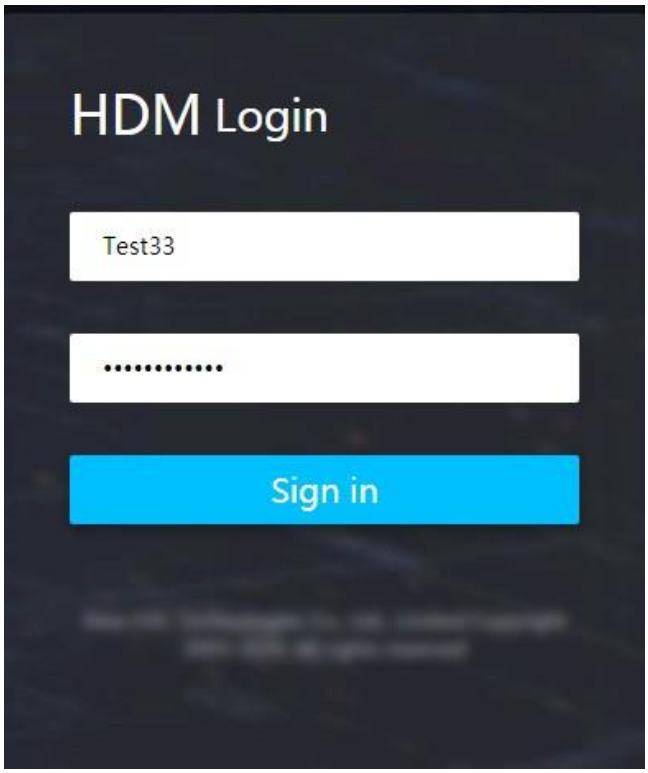
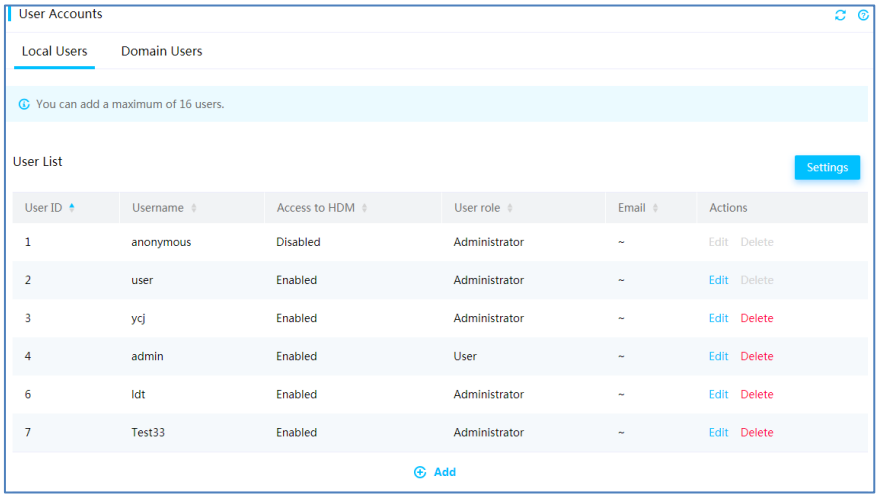


図183ユーザーカウントの表示



SNMPトラップ設定をインポートする

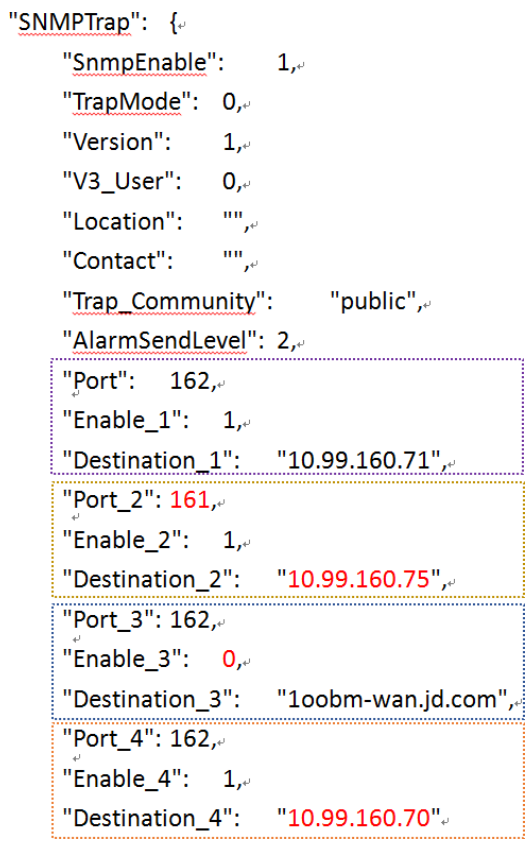
1. 設定ファイルを開き、**SNMPTrap**を検索します。

図184 SNMPトラップ設定の検索

```
"SNMPTrap": {
    "SnmpEnable":   1,
    "TrapMode": 0,
    "Version":  1,
    "V3_User":  0,
    "Location": "",
    "Contact":  "",
    "Trap_Community":   "public",
    "AlarmSendLevel":   2,
    "Port": 162,
    "Enable_1": 1,
    "Destination_1":    "10.99.160.71",
    "Port_2":   162,
    "Enable_2": 1,
    "Destination_2":    "10.99.160.72",
    "Port_3":   162,
    "Enable_3": 1,
    "Destination_3":    "1oobm-wan.jd.com",
    "Port_4":   162,
    "Enable_4": 1,
    "Destination_4":    ""
```

2. SNMPトラップサーバーの設定を変更します。次に例を示します。
   - **Destination_2**アドレスを**10.99.160.75**に、**Port_2**フィールドを**161**に設定します。
   - **Enable_3**フィールドを**0**に設定して、SNMPトラップサーバーをディセーブルにします。
   - **Destination_4**アドレスを**10.99.160.70**に設定します。

図185 SNMPトラップサーバーの設定の変更



3. 必要に応じて、その他のSNMPトラップ設定を変更します。
   設定可能なSNMPトラップ設定の詳細については、表15を参照してください。

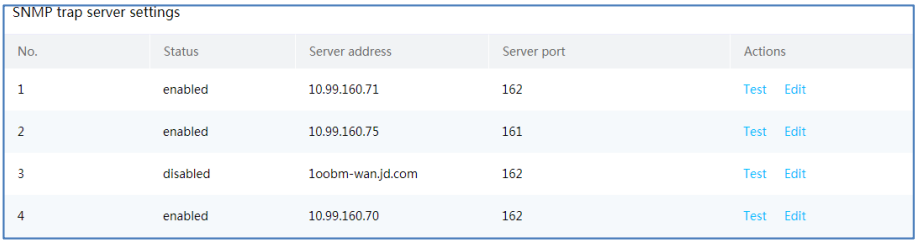
表15構成可能アイテムの説明

項目	説明
SnmpEnable	0または1を入力して、SNMPトラップ通知をディセーブルまたはイネーブルにします。
Trap Mode	SNMPトラップモードを開始します。次のオプションがあります。 • 0: Node mode • 1: Event mode
Version	SNMPバージョンを入力します。次のオプションがあります。 • 0-v1 • 1-v2c • 2-v3
V3_User	システムがSNMPv3トラップを送信するために使用するユーザー名を入力します。
Location	サーバーの場所(最大31バイトの文字列)を入力します。
Contact	連絡先情報(最大31バイトの文字列)を入力します。

項目	説明
Trap_Community	マネージャで認証するためのトラップコミュニティストリングを入力します。値の範囲は1～18文字です。デフォルト値はpublicです。
AlarmSendLevel	SNMPトラップの重大度。次のオプションがあります。 • 0: **Minor + Major + Critical** • 1: **Critical** • 2: **All**
Port_2/3/4	宛先ホストがSNMPトラップを受信するポート番号を入力します。値の範囲は1～65535です。デフォルトのポート番号は162です。
Enable_1/2/3/4	SNMPトラップサーバーをディセーブルまたはイネーブルにするには、0または1を入力します。
Destination_1/2/3/4	SNMPトラップを受信する宛先ホストのIPアドレスまたはドメインアドレス。

4. 構成ファイルを保存してインポートします。
   a. 上部のナビゲーションバーで、**Remote O&M**をクリックします。
   b. 左側のナビゲーションペインで、**Manage Configuration**を選択します。
   c. 構成ファイルをインポートします。
      インポート操作が終了すると、HDMは自動的に再起動します。
5. 設定を確認するには、HDMの再起動後にHDMに再度サインインし、SNMPトラップ設定を表示します。

図186 SNMPトラップ設定の表示



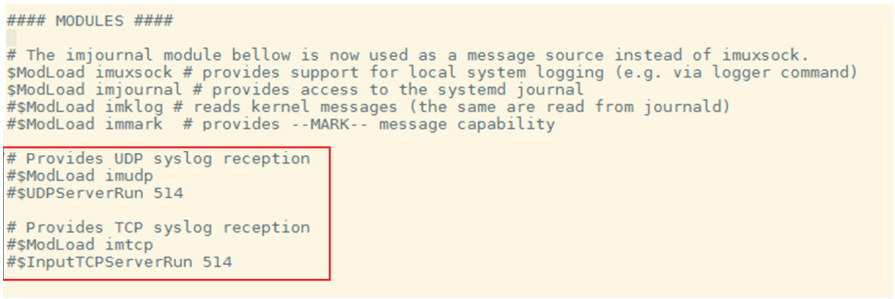
syslogサーバーを設定する

このセクションでは、例としてRed Hat Enterprise Linux 7.7を使用します。UDP、TCP、またはTLSに基づいてLinux syslogサーバーを設定できます。

UDPまたはTCPに基づいてLinux syslogサーバーを設定する

1. /etc/rsyslog.conf構成ファイルを開きます。

図187構成ファイルを開く



2. UDPおよびTCP syslog受信をイネーブルにします。
   a. 図187に示すように、行のコメントを解除します。
   b. UDPサーバーポート、TCPサーバーポート、またはその両方を設定します。両方のポートを指定する

場合は、指定したポートが異なることを確認します。この例では、UDPポートは514、TCPポートは518です。

c. リモートログを保存するパスを**/var/log/hdm/messages.log**として指定します。

図188 UDPおよびTCP syslog受信設定の構成

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514

# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 518

$template RemoteLogs,"/var/log/hdm/messages.log"
*.* ?RemoteLogs
#&~
```

注:

- **$template RemoteLogs**ディレクティブは、rsyslogデーモンに、すべてのリモートメッセージを収集し、/var/logディレクトリに格納されている個別のファイルに書き込むように指示します。
- *.* **?RemoteLogs**ディレクティブは、RemoteLogsテンプレートがすべてのログメッセージの受信に使用されることを示します。
- &~ ディレクティブは、rsyslogデーモンにローカルファイルへのメッセージの書き込みを停止し、messages.logディレクトリにのみメッセージを書き込むように指示します。

3. コマンドを実行してrsyslogを再起動し、そのステータスを表示します。

図189 rsyslogの再起動とステータスの表示

```
[root@localhost ~]# systemctl restart rsyslog.service
[root@localhost ~]#
[root@localhost ~]# systemctl status rsyslog.service
● rsyslog.service - System Logging Service
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-03-09 13:44:46 CST; 8s ago
     Docs: man:rsyslogd(8)
           http://www.rsyslog.com/doc/
 Main PID: 11171 (rsyslogd)
    Tasks: 9
   CGroup: /system.slice/rsyslog.service
           └─11171 /usr/sbin/rsyslogd -n

Mar 09 13:44:46 localhost.localdomain systemd[1]: Starting System Logging Service...
Mar 09 13:44:46 localhost.localdomain rsyslogd[11171]:  [origin software="rsyslogd" swVersion="8.24.0-38.el7" x-pid="11171" x-info="http://www.rsyslog.com"] start
Mar 09 13:44:46 localhost.localdomain systemd[1]: Started System Logging Service.
[root@localhost ~]#
```

4. HDM Webインターフェースでsyslog設定を行います。

a. HDM Webインターフェースにサインインします。

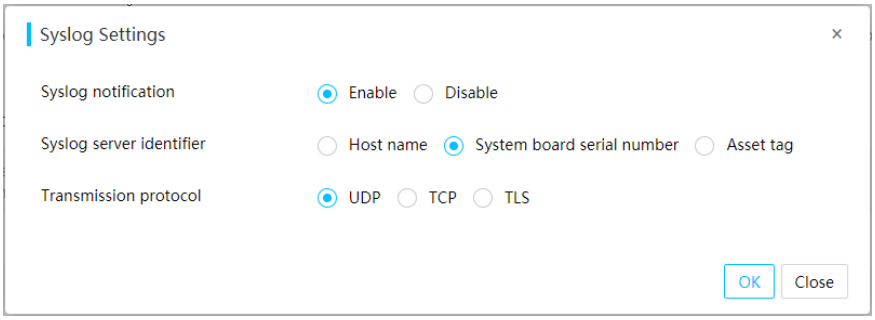
b. 上部のナビゲーションバーで、**Remote O&M**をクリックします。

c. 左側のナビゲーションペインで、**Alarm Settings**を選択します。

d. **Syslog Settings**タブをクリックします。

e. **Syslog notification settings**セクションで、**Enable for Syslog notification**を選択し、Syslogサーバー**ID**を選択し、送信プロトコルとして**UDP**を選択して、OKをクリックします。

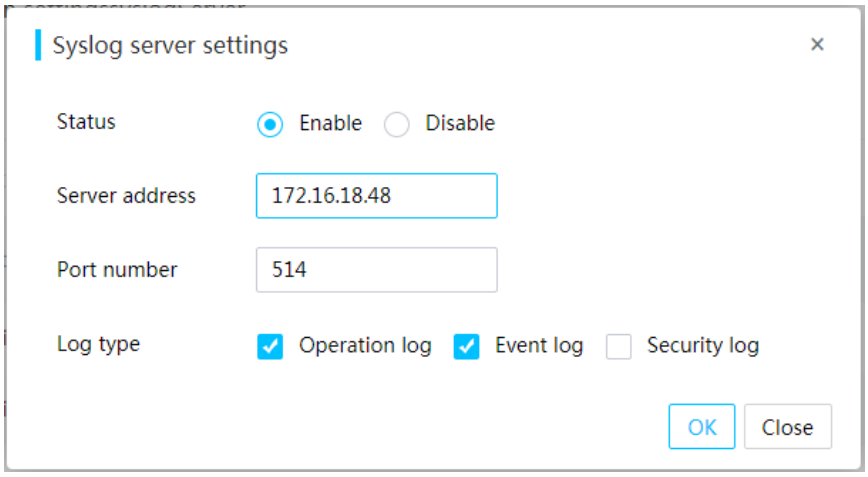
図190 syslog通知設定の構成



f. **Syslog server settings**セクションで、syslogサーバーの**Edit**をクリックします。syslogサーバーのパラメーターを設定し、OKをクリックします。

HDM管理アドレスではなく、サーバーのOS IPアドレスを必ず指定してください。

図191 syslogサーバーのパラメーターの設定



TLSに基づいてLinux syslogサーバーを設定する

TLSは暗号化された伝送プロトコルであり、次の認証モードをサポートします。

- **One-way authentication**: Syslogサーバーだけを認証します。
- **Two-way authentication**: HDMログインに使用されるsyslogサーバーとクライアントの両方を認証します。

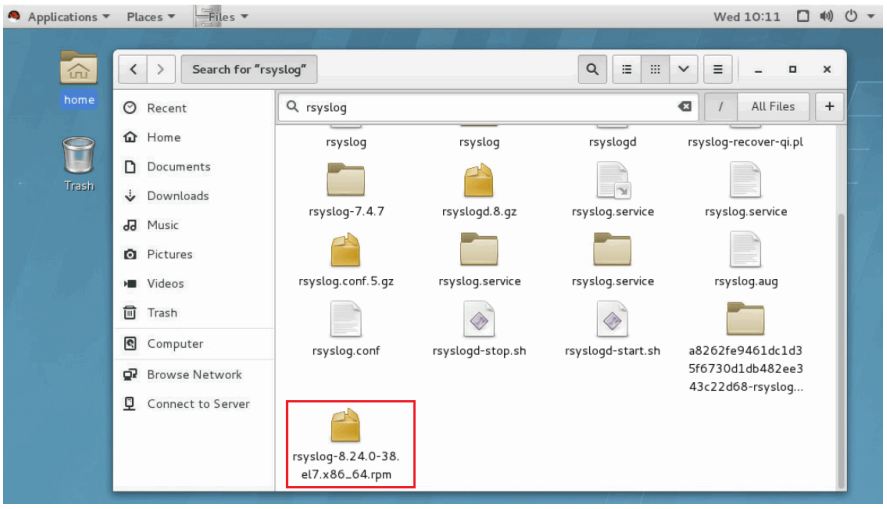
前提条件

サーバーにOSをインストールします。Rsyslogは、デフォルトでOSにインストールされます。

手順

1. TLS転送用の**rsyslog-gnutls**パッケージをダウンロードします。
   - サーバーがネットワークに接続されている場合は、**sudo yum install-y rsyslog-gnutls**コマンドまたは**apt**コマンドを使用してパッケージをダウンロードします。
   - サーバーがネットワークから切断されている場合は、図192に示すように、OSイメージからパッケージを取得します。

図192 OSイメージからのrsyslog-gnutlsパッケージの取得



2. **rsyslog-gnutls**パッケージをインストールします。

図193 rsyslog-gnutlsパッケージのインストール

```
[root@localhost Packages]#
[root@localhost Packages]# rpm -ivh rsyslog-g
rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm
rsyslog-gssapi-8.24.0-38.el7.x86_64.rpm
[root@localhost Packages]# rpm -ivh rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm
warning: rsyslog-gnutls-8.24.0-38.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:rsyslog-gnutls-8.24.0-38.el7     ################################# [100%]
[root@localhost Packages]#
```

3. 自己署名CA証明書を生成します。デスクトップを右クリックし、**Open Terminal**を選択して、次のタスクを実行します。

   a. 秘密キーファイルをPEM形式で生成します。

   # cd /root/Desktop # mkdir tls

   # cd tls

   # mkdir server # mkdir client

   # openssl genrsa -out cakey.pem 2048

   b. ルート証明書署名要求(CSR)ファイルを生成します。

   #openssl req-new-key cakey.pem-out ca.csr-subj"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=MyCA"

   c. 自己署名ルート証明書を生成します。

   #openssl x509-req-days 365-sha 1-extensions v3_ca-signkey cakey.pem-in ca.csr -out cacert.pem

4. サーバーの秘密キーと証明書を生成します。デスクトップを右クリックし、ターミナルを開くを選択して、次のタスクを実行します。

   a. 秘密鍵ファイルを生成します。

   #cd server

   #openssl genrsa-out key.pem 2048

   b. 証明書要求ファイルを生成します。ここでは、例としてIPアドレス172.16.18.48(サーバーのOS IPアドレス)を使用します。

   #openssl req-new-key key.pem-out server.csr-subj"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=172.16.18.48"

   c. ルート証明書を使用して、サーバー証明書を発行します。

   #openssl x509-req-days 365-sha 1-extensions v3_req-CA./cacert.pem -CAkey./cakey.pem-CAserial ca.srl-CAcreateserial-in server.csr-out cert.pem

   d. CA証明書を使用して、サーバー証明書を確認します。

#openssl verify-CAfile./cacert.pem cert.pem

5. クライアントの秘密キーと証明書を生成します。デスクトップを右クリックし、ターミナルを開く、を選択して、次のタスクを実行します。

   a. 秘密鍵ファイルを生成します。

      #cd ../clientト

      #openssl genrsa-out key.pem 2048

   b. 証明書要求ファイルを生成します。ここでは、例としてIPアドレス172.16.20.168を使用します。

      #openssl req-new-key key.pem-out client.csr-
      subj"/C=CN/ST=myprovice/L=mycity/O=myorganization/OU=mygroup/CN=172.16.20.168"

   c. ルート証明書を使用して、クライアント証明書を発行します。

      #openssl x509-req-days 365-sha 1-extensions v3_req-CA./cacert.pem
      -CAkey./cakey.pem-CAserial./server/ca.srl-CAcreateserial-in client.csr-out cert.pem

   d. CA証明書を使用して、クライアント証明書を確認します。

      #openssl verify-CAfile./cacert.pem cert.pem

6. rsyslog.conf構成ファイルを構成します。

   a. TCPとUDPの設定は変更せずに、図194に示すようにマークされた行を変更します。

      図194構成ファイルの構成

```
#### MODULES ####

# The imjournal module bellow is now used as a message source instead of imuxsock.
$ModLoad imuxsock # provides support for local system logging (e.g. via logger command)
$ModLoad imjournal # provides access to the systemd journal
#$ModLoad imklog # reads kernel messages (the same are read from journald)
$ModLoad immark  # provides --MARK-- message capability


#make gtls driver the default
$DefaultNetstreamDriver gtls

#cerificate files
$DefaultNetstreamDriverCAFile /root/Desktop/tls/cacert.pem
$DefaultNetstreamDriverCertFile /root/Desktop/tls/server/cert.pem
$DefaultNetstreamDriverKeyFile /root/Desktop/tls/server/key.pem

$ModLoad imtcp # load TCP listener
$InputTCPServerRun 516

#shuangxiangrenzheng
$InputTCPServerStreamDriverAuthMode x509/certvalid

#danxiangrenzheng
#$InputTCPServerStreamDriverAuthMode anon

$InputTCPServerStreamDriverMode 1 # run driver in TLS-nly mode

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 518
```

   b. サーバーポートを516に設定します。

   c. 一方向認証の場合は、次の行をファイルに追加します。

      InputTCPServerStreamDriverAuthMode anon

   d. 双方向認証の場合は、ファイルに次の行を追加します。

      $InputTCPServerStreamDriverAuthMode×509/certvalid

7. ファイアウォールをオフにします。次のコマンドを実行し、**SELinux**を**disabled**に設定します。

   #systemctl stop firewalld

   #setenforce 0
   #sed-i's#SELINUX=enforcing#SELINUX=disabled#g'/etc/selinux/config

8. rsyslogを再起動し、そのステータスを表示します。systemctl restart rsyslog systemctl status rsyslog
9. HDM Webインターフェースでsyslog設定を行います。

   a. ステップ3～5で生成された証明書を、HDMアクセスに使用されるホストにコピーします。

   b. HDMにサインインします。

   c. 上部のナビゲーションバーで、**Remote O&M**をクリックします。

   d. 左側のナビゲーションペインで、**Alarm Settings**を選択します。

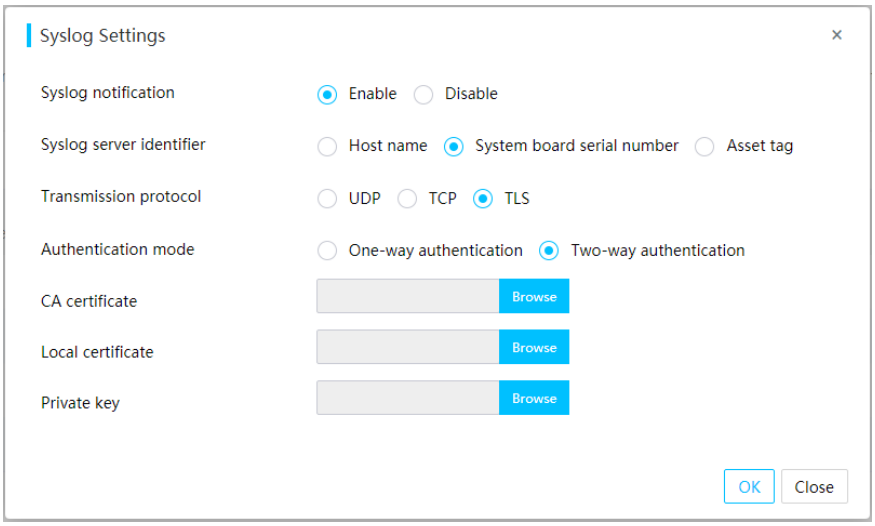
   e. **Syslog Settings**タブをクリックします。

   f. **Syslog notification settings**セクションで、**Enable for Syslog notification**を選択し、図190に示すように、Syslogサーバー IDとTLSを選択します。

- **One-way authentication**を選択した場合は、ステップ3で生成された自己署名CA証明書をアップロードします。
- **Two-way authentication**を選択した場合は、ステップ3および5で生成された自己署名CA証明書、ローカル証明書、および秘密キーファイルをアップロードします。

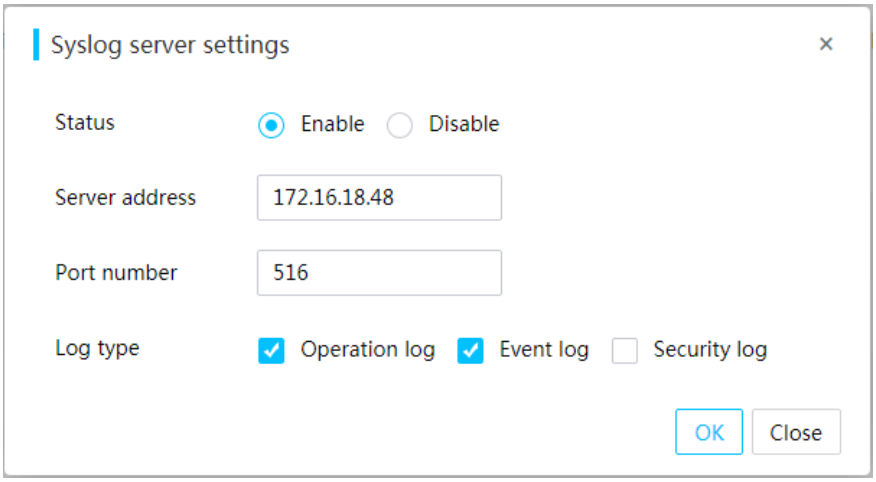
g. **OK**をクリックします。

図195 syslog通知設定の構成



h. syslogサーバーのパラメーターを設定し、**OK**をクリックします。

図196 syslogサーバーのパラメーターの設定



rsyslogログの表示

1. SSHを介してrsyslogサーバーにログインします。

   この例では、サーバーのIPアドレスは172.16.18.48です。

2. /var/log/hdm/messages.logパスにあるログエントリを表示します。

図197 rsyslogログの表示

```
[root@localhost ~]# ls -lh /var/log/hdm/messages.log
-rw-------. 1 root root 3.1M Mar  9 13:41 /var/log/hdm/messages.log
[root@localhost ~]#
[root@localhost ~]#
```

LDAP設定の構成

Lightweight Directory Access Protocol(LDAP)は、IPネットワークを介して分散ディレクトリ情報サービスにアクセスして維持するためのアプリケーションプロトコルです。LDAPは、ユーザーのクエリー要求に迅速に応答でき、統合されたユーザー認証管理の実装に使用できます。

HDMはWindows Active DirectoryとLinux OpenLDAPの両方をサポートしています。このセクションでは、LDAP構成を説明する例としてWindows Server 2012 R2 Datacenterを使用します。

OSをインストールする

Windows Server 2012 R2 Datacenterをインストールします。詳細については、「H3C Servers Operating System Installation Guide」を参照してください。

LDAPサーバーをセットアップする

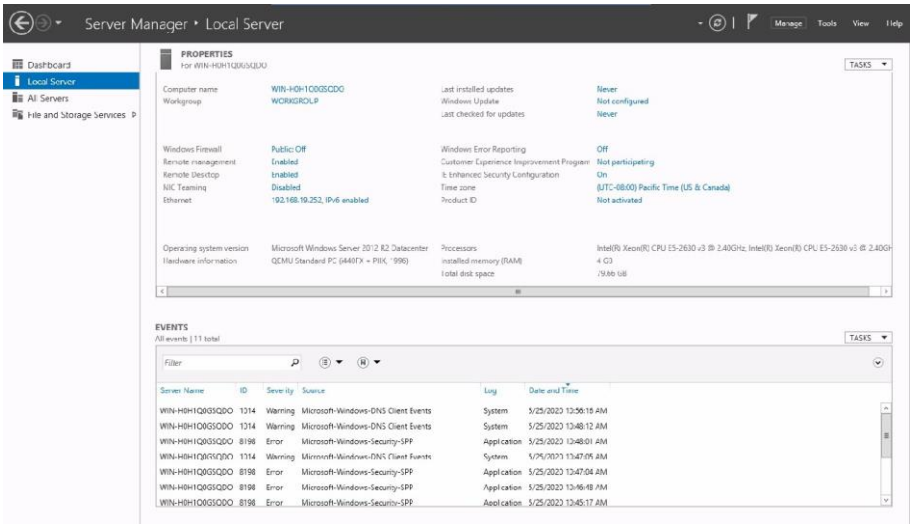
前提条件

OSをインストールし、管理者としてOSにアクセスします。

DNSサーバーをインストールする

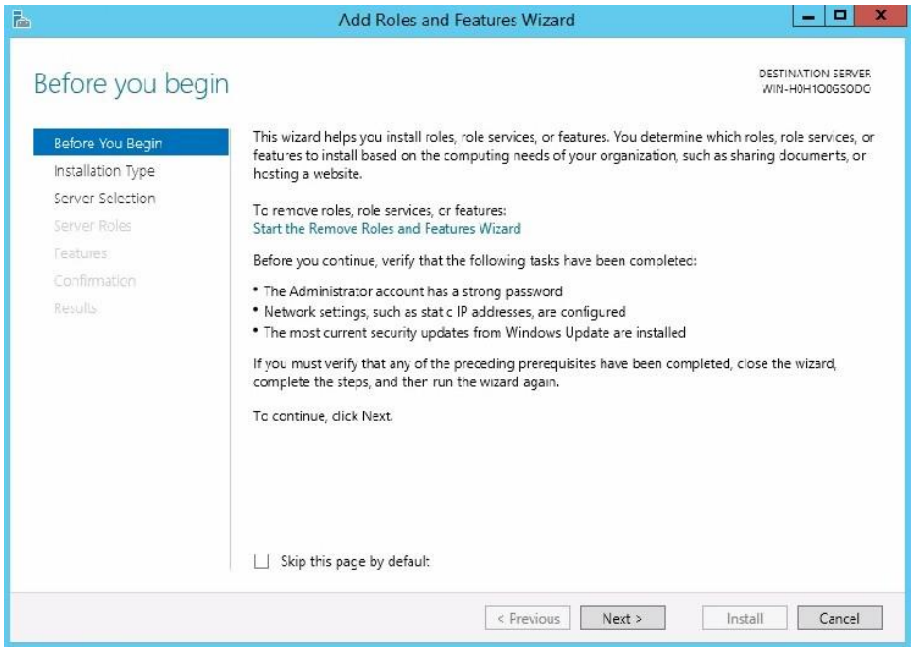
1. サーバーマネージャを開きます。
2. 左側のナビゲーションペインで**Local Server**を選択して、ローカルサーバーの**PROPERTIES**ページに入ります。

   図198ローカルサーバーのPROPERTIESページ



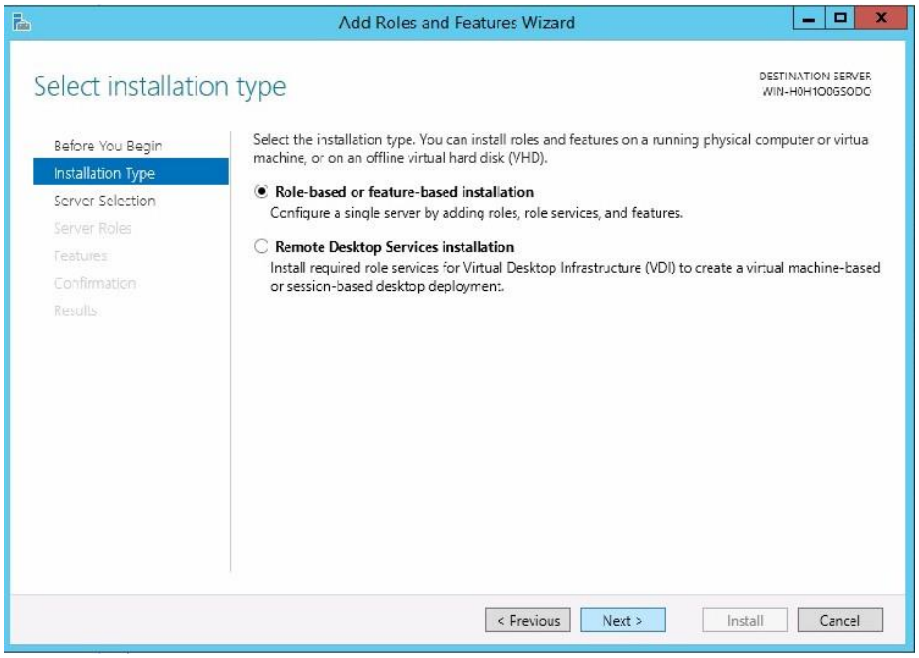
3. 右上の**Manage**をクリックし、**Add Roles and Features**を選択します。
4. 表示されたウィンドウで、**Next**をクリックします。

図199 役割と機能の追加ウィザード



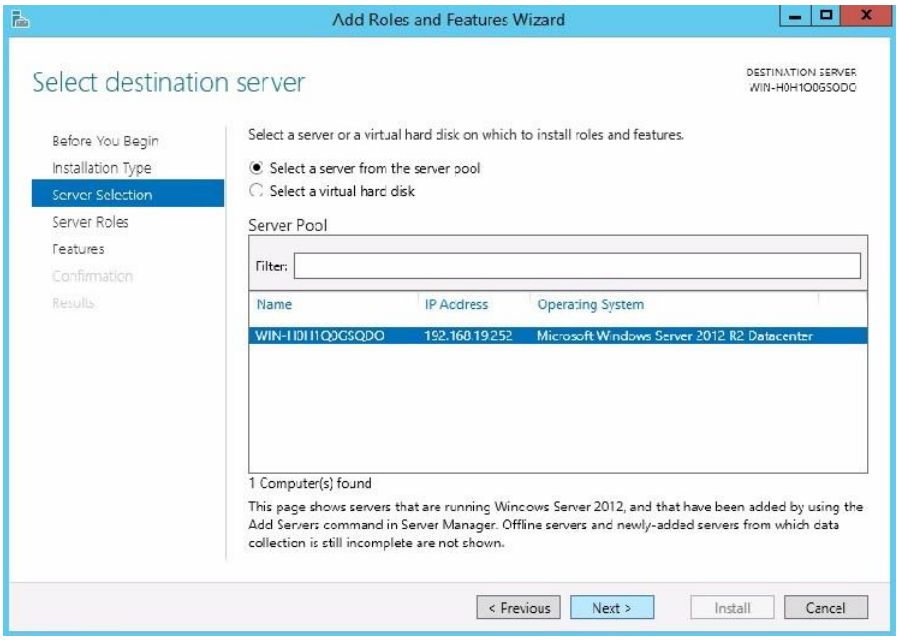
5. インストールの種類として**Role-based or feature-based installation**を選択し、**Next**をクリックします。

図200 インストールタイプの選択



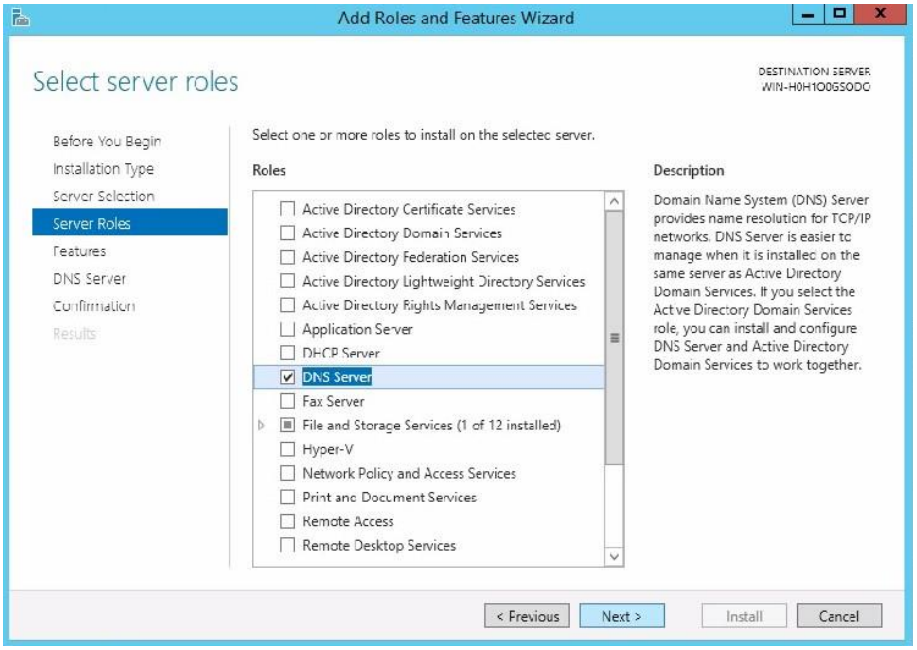
6. **Select a server from the server pool**を選択し、現在のサーバーを宛先サーバーとして選択して、**Next**をクリックします。

図201ターゲットサーバーの選択



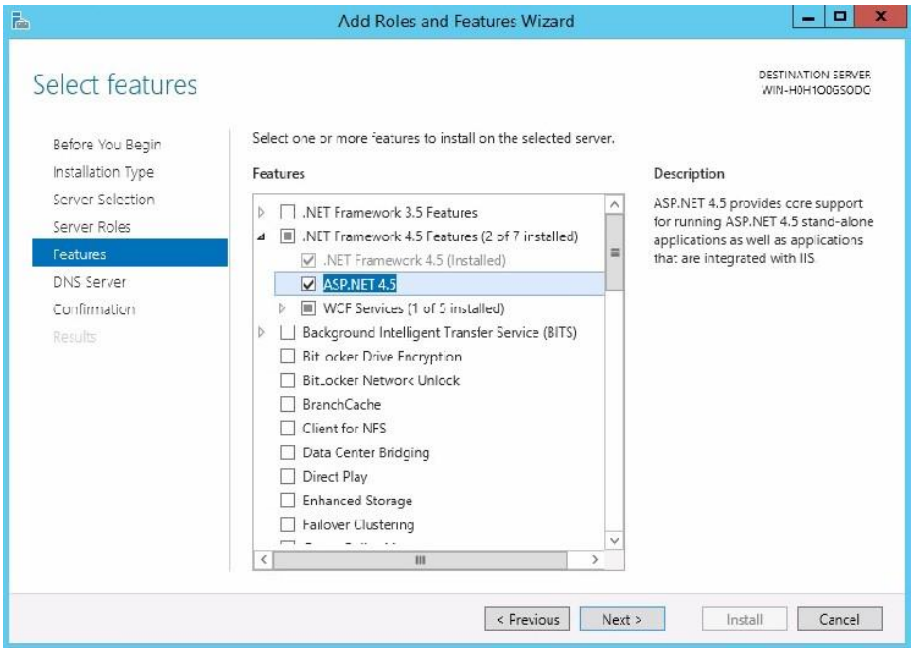
7. サーバーの役割としてt **DNS server**を選択し、**Next**をクリックします。

図20 2サーバーの役割の選択



8. **NET Framework 4.5 Features**を選択し、**Next**をクリックします。

図203サーバーの機能の選択

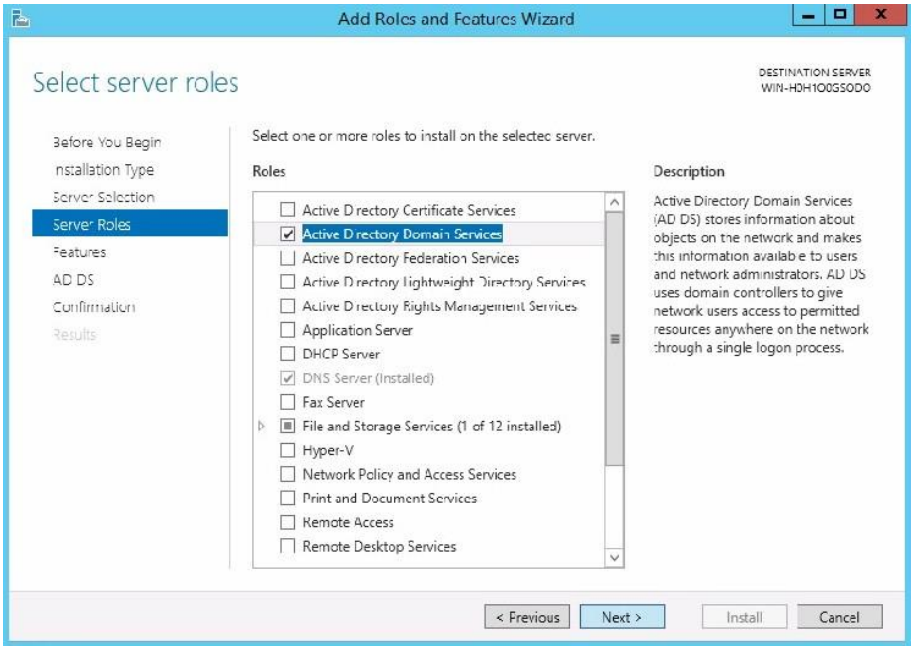


9. **DNS Server**タブで、**Next**をクリックします。
10. サーバーの構成が正しいことを確認し、**Install**をクリックします。

サーバーへのActive Directoryドメインサービスのインストール

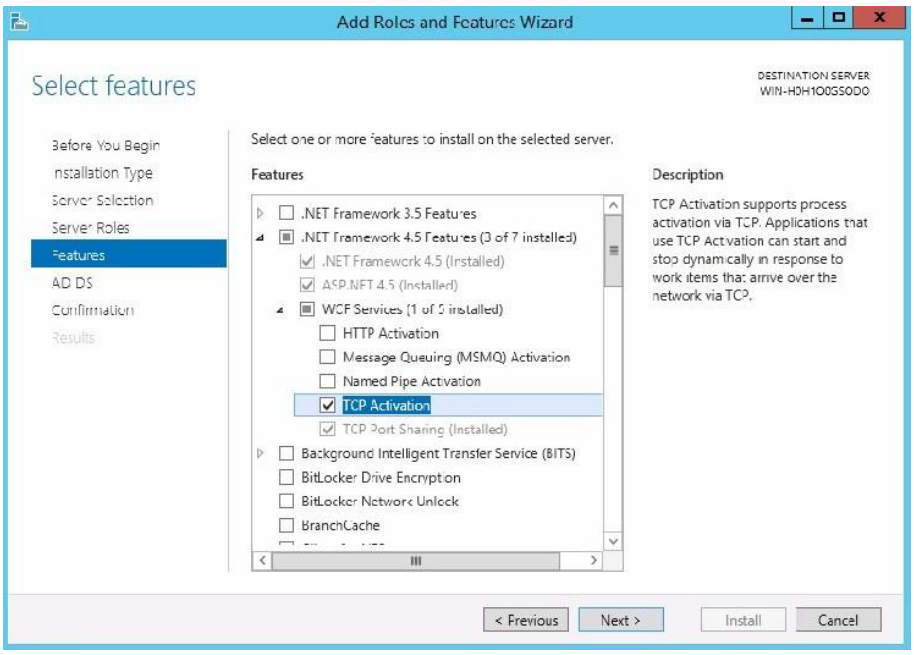
1. DNSサーバーのインストールで手順1～6を繰り返します。
2. **Server Roles**タブで、**Active Directory Domain Services**を選択し、**Next**をクリックします。

Next図204サーバーの役割の選択



3. **NET Framework 4.5 Features**を選択し、**Next**をクリックします。

図205サーバーの機能の選択

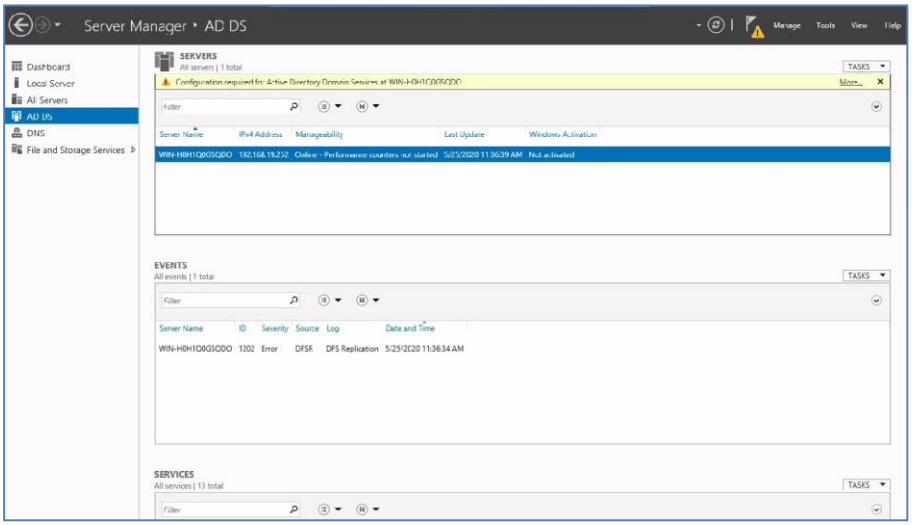


4. **AD DS**タブで、**Next**をクリックします。
5. サービス設定が正しいことを確認し、**Install**をクリックします。

Active Directoryドメインサービスを構成する

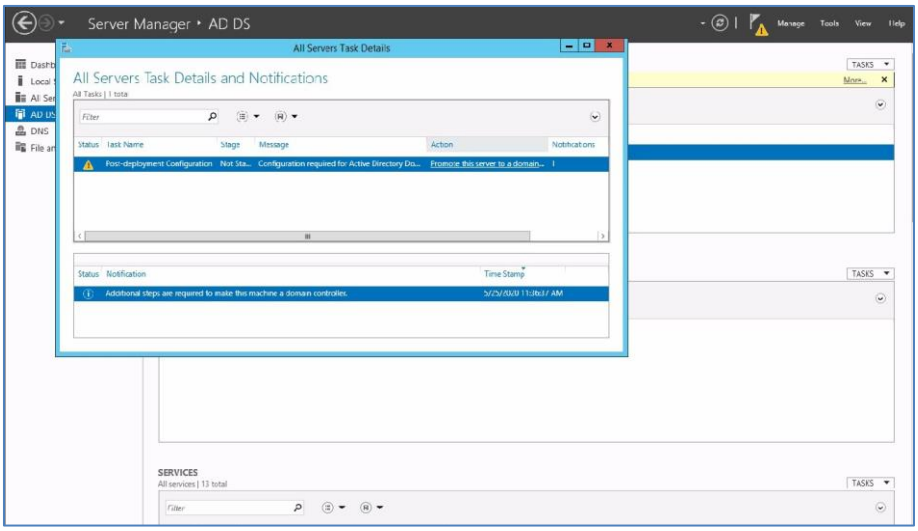
1. 左側のナビゲーションウィンドウで**AD DS**を選択し、**More...**をクリックします。

図206 AD DSメニュー



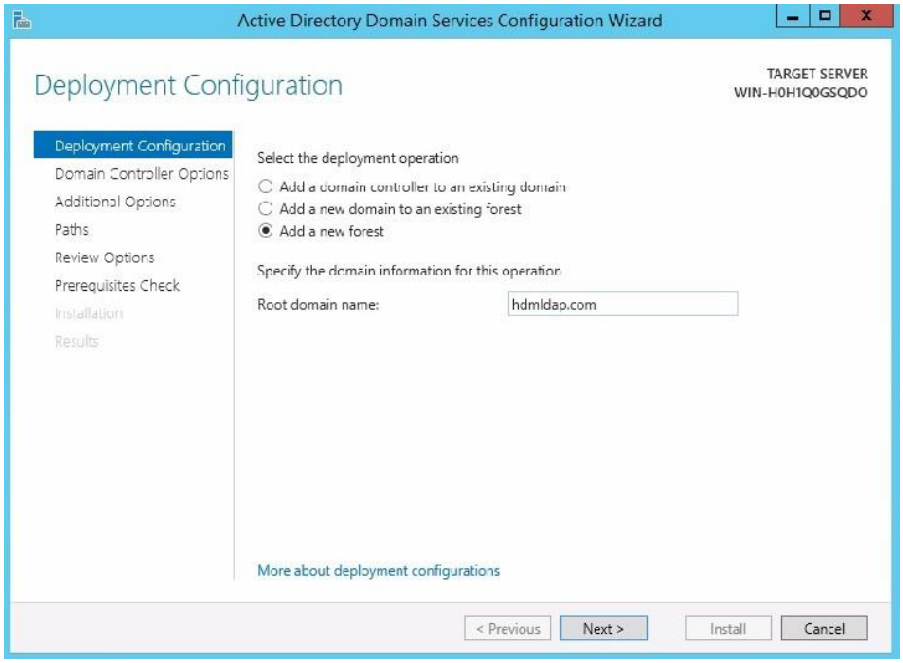
2. 表示されたダイアログボックスで、**Action**の**Promote this server to a domain controller**をクリックします。**Action**列をクリックして、AD DS構成ウィザードを開きます。

図207 All Servers Task Detailsダイアログボックス



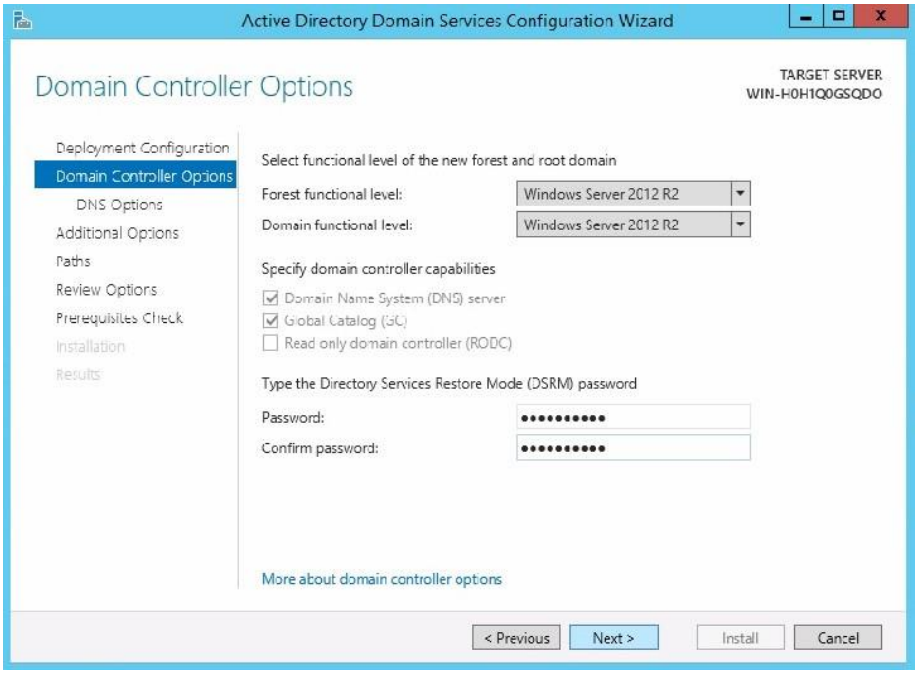
3. **Add a new forest**を選択し、**Root domain name**にActive Directoryドメイン名を入力します。例えば、**hdmldap**などをクリックし、**Next**をクリックします。

図208 Active Directoryドメインサービス構成ウィザード



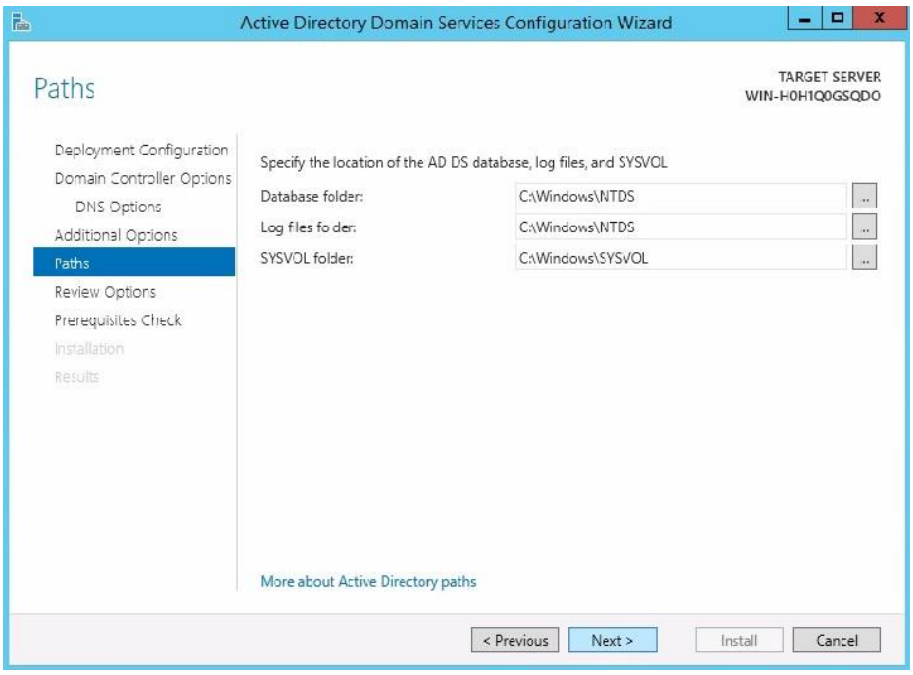
4. **Domain Controller Options**タブで、ドメインコントローラーのパスワードを入力し、**Next**をクリックします。

図209 Domain Controller Optionsメニュー



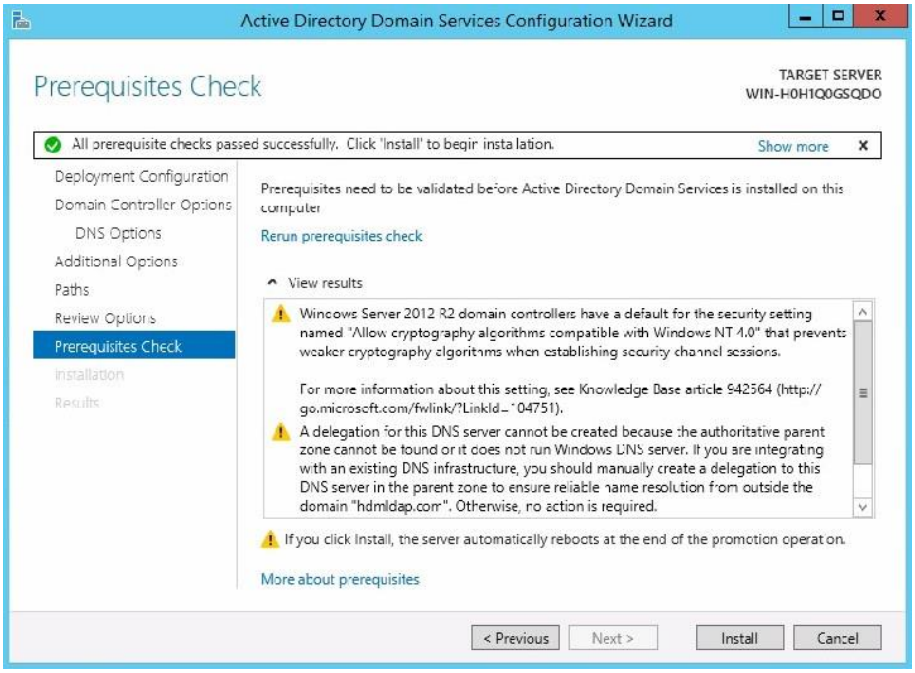
5. **Paths**タブが表示されるまで、指示に従って**Next**をクリックします。AD DSデータベース、ログファイル、およびSYSVOLの場所を指定し、**Next**をクリックします。

図210 Active Directoryパスの構成



6. **Prerequisites Check**タブが表示されるまで指示に従って**Next**をクリックし、次に**Install**をクリックします。インストールが完了すると、OSが自動的に再起動します。

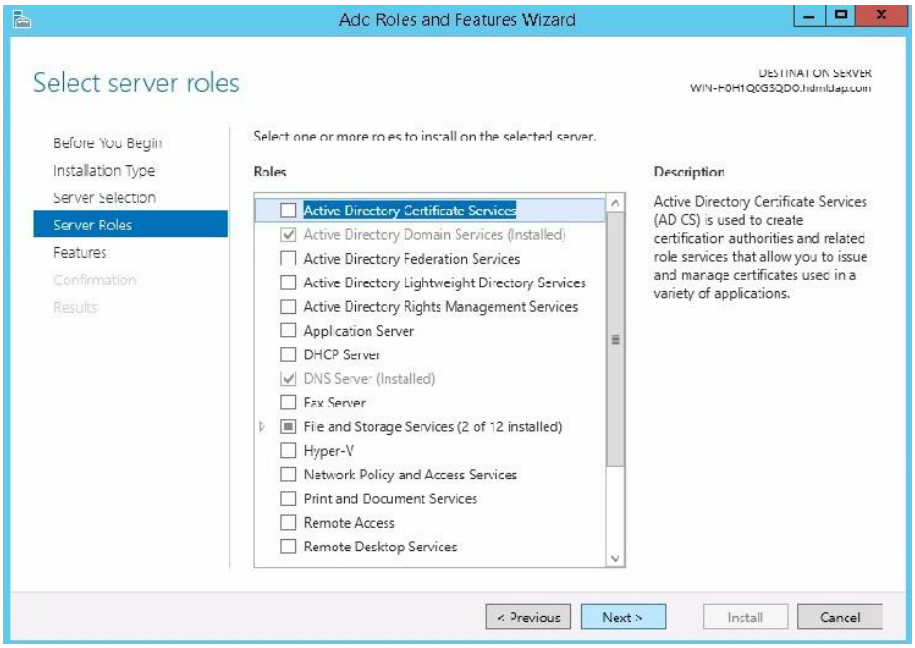
図211 Prerequisites Checkメニュー



サーバーへのActive Directory証明書サービスのインストール

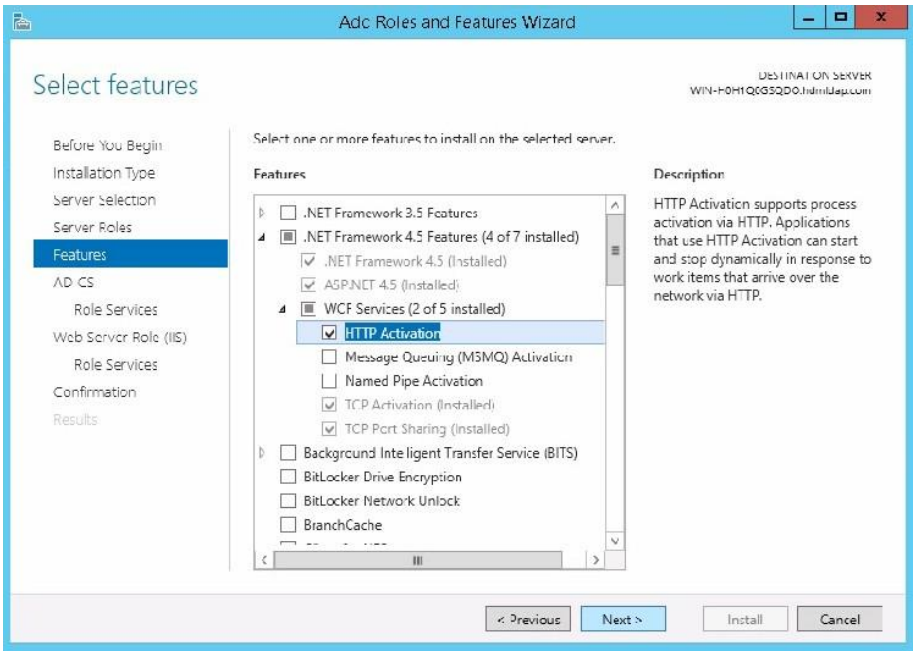
1. 管理者としてOSにアクセスします。
   OSに正常にアクセスするには、ユーザー名の前にドメイン名を追加する必要があります。
2. DNSサーバーのインストールで手順1～6を繰り返します。
3. **Server Roles**タブで、**Active Directory Certificate Services**を選択し、**Next**をクリックします。

図212 サーバーの役割の選択



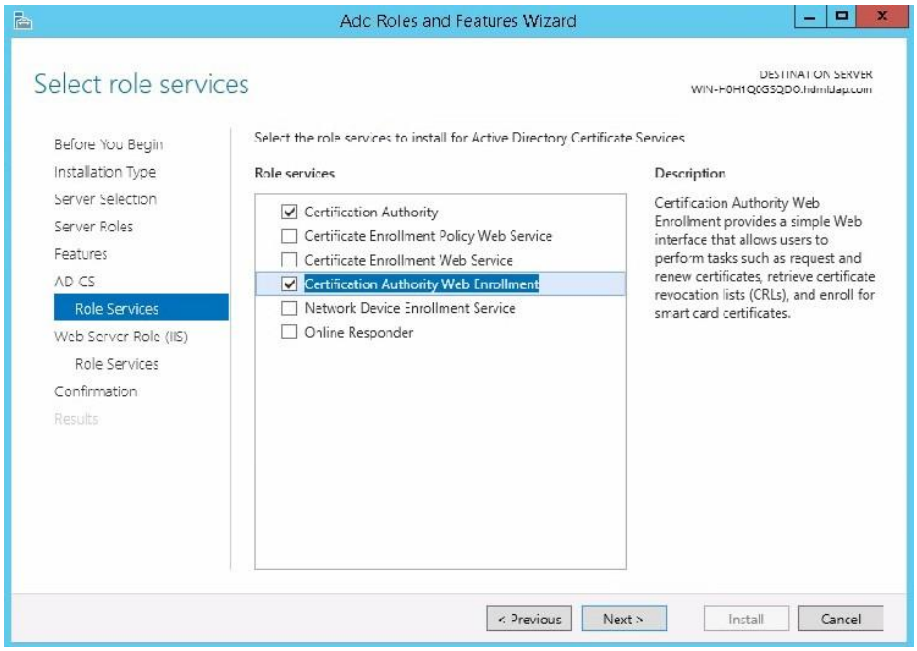
4. **NET Framework 4.5 Features**を選択し、**Next**をクリックします。

図213 サーバーの機能の選択



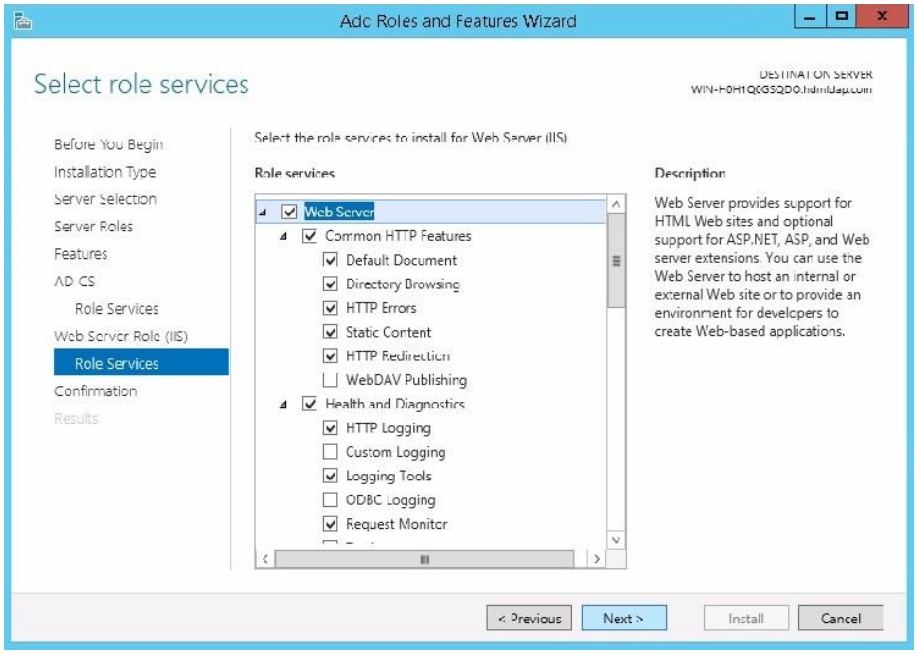
5. **AD CS**タブで、**Next**をクリックします。
6. **Role Services**タブで、**Certification Authority**および**Certification Authority Web Enrollment**を選択し、**Next**をクリックします。

図214 AD CSの役割サービスの選択



7. **Web Server Role (IIS)**タブで、**Next**をクリックします。
8. **Role Services**タブで、Webサーバーの役割サービスを選択し、**Next**をクリックします。ベストプラクティスとして、既定の役割サービスを使用します。

図215 Webサーバー用の役割サービスの選択

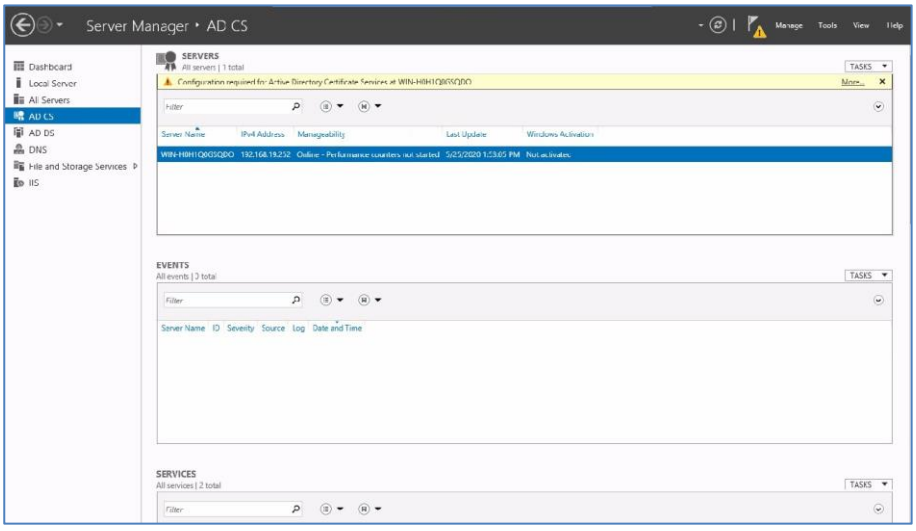


9. **Confirmation**タブで、**Install**をクリックします。

Active Directory証明書サービスの構成

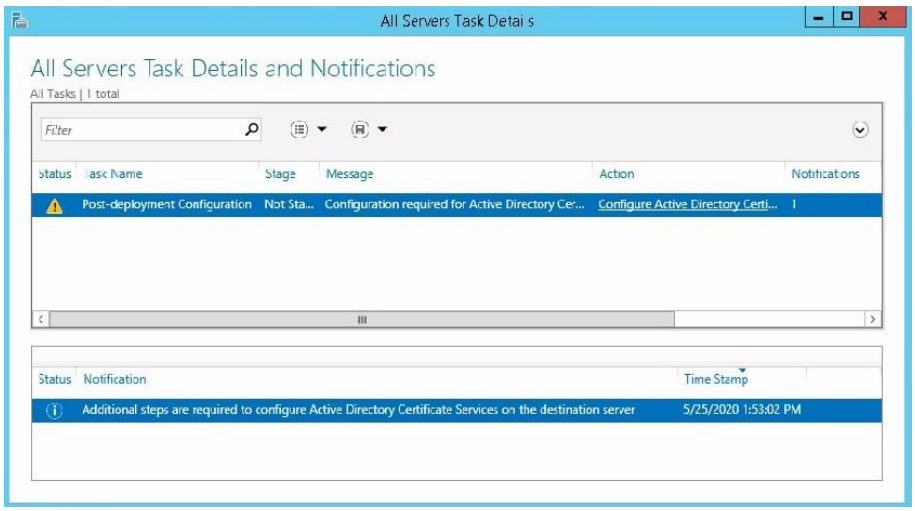
1. 左側のナビゲーションウィンドウで**AD CS**を選択し、**More...**をクリックします。

図216 AD CSメニュー



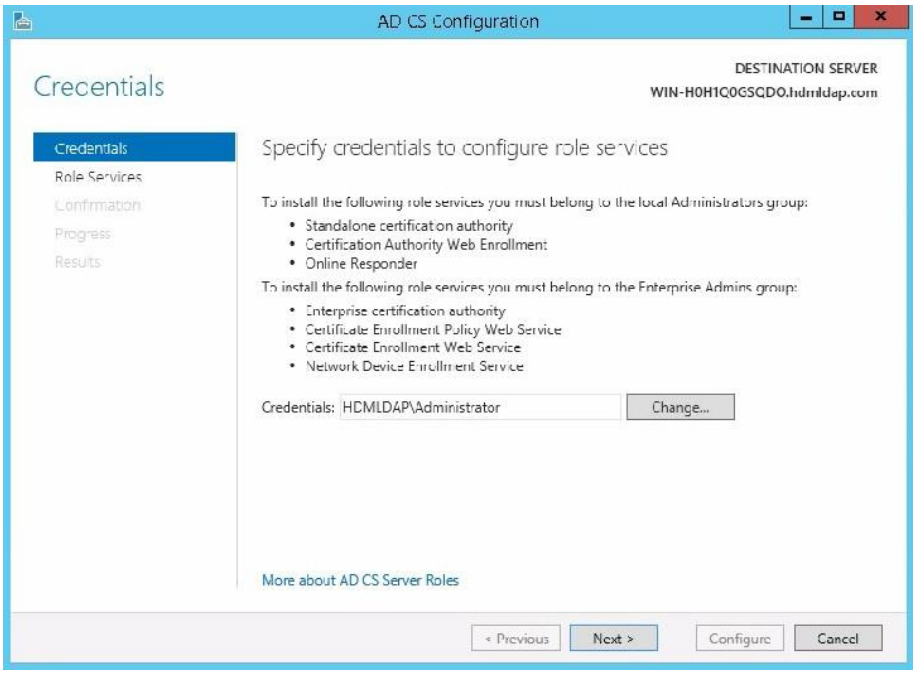
2. 表示されたダイアログボックスで、**Action**列の**Configure Active Directory Certificate Services on the server**をクリックして、AD CS構成ウィザードを開きます。

図217All Servers Task Detailsダイアログボックス



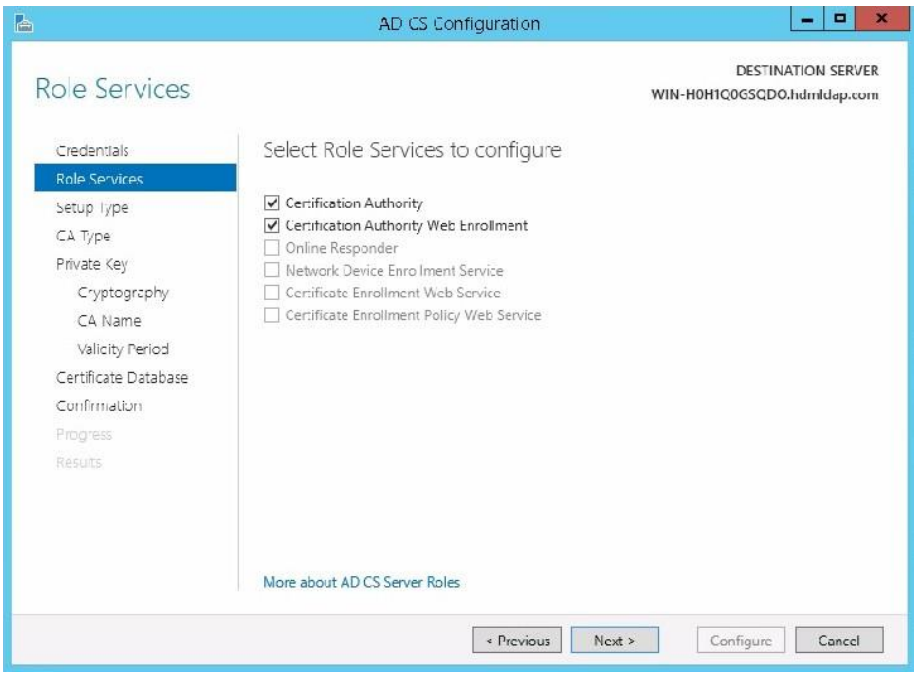
3. **Credentials**タブで、**Next**をクリックします。

図218 AD CS構成ウィザード



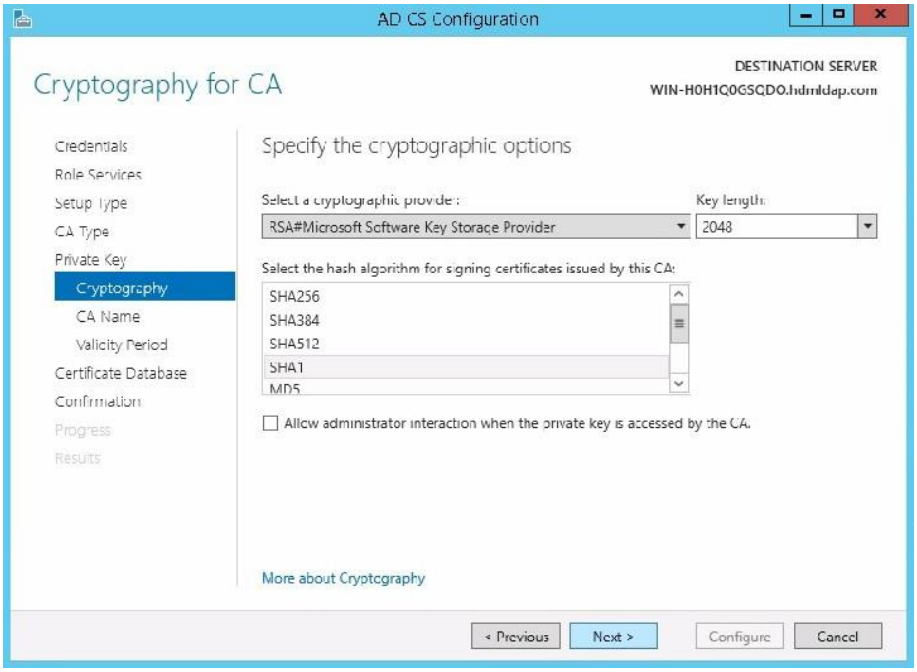
4. **Role Services**タブで、**Certificate Authority**および**Certificate Authority Web Enrollment**を選択し、**Next**をクリックします。

図219 役割サービスの選択



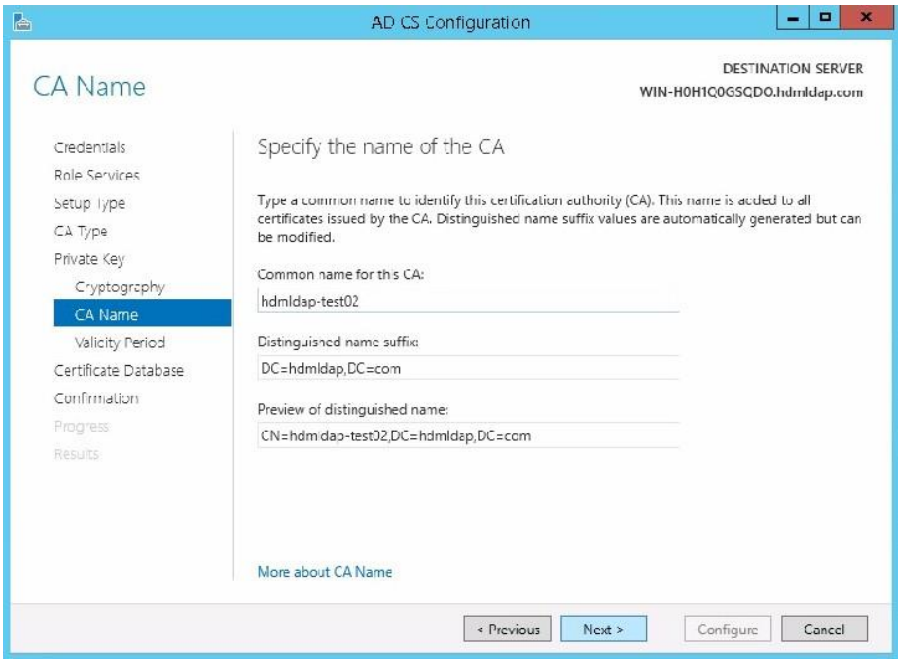
5. **Setup Type**タブで、**Enterprise CA**を選択し、**Next**をクリックします。
6. **CA Type**タブで、**Root CA**を選択し、**Next**をクリックします。
7. **Private Key**タブで、**Create a new private key**を選択し、**Next**をクリックします。
8. 暗号化プロバイダとして**RSA**、キーの長さとして**2048**、ハッシュアルゴリズムとして**SHA1**を選択し、**Next**をクリックします。

図220 暗号化オプションの指定



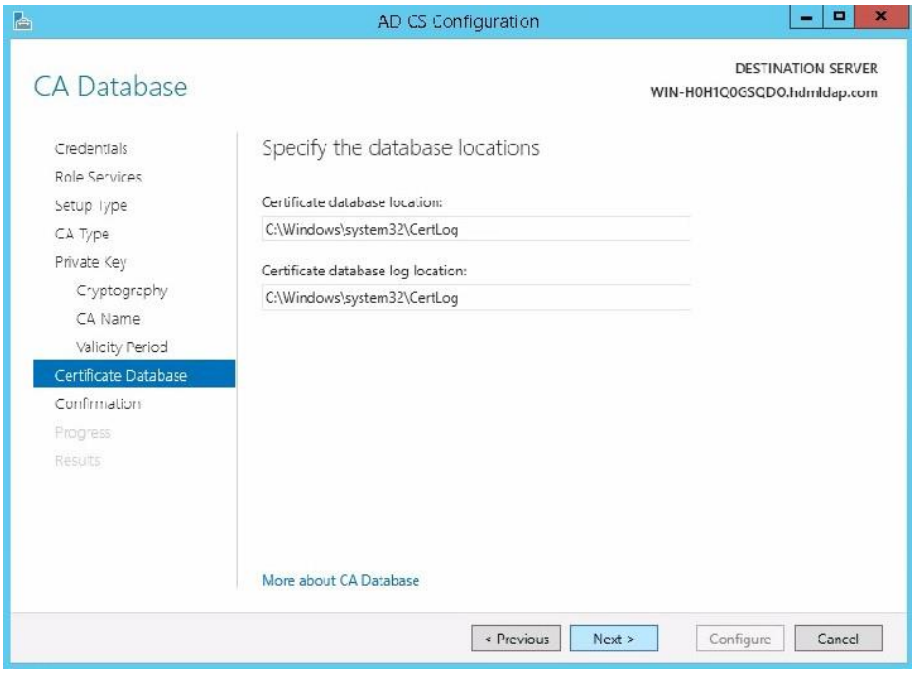
9. **hdmldap-test02**をCA名として指定し、**Next**をクリックします。

図221 CA名の指定



10. 有効期間を入力して、**Next**をクリックします。デフォルトの有効期間は5年です。
11. **Certificate Database**タブで、データベースの場所を指定し、**Next**をクリックします。

図222 データベースの場所の指定



12. 設定が正しいことを確認し、**Configure**をクリックします。
    設定が完了したら、サーバーを再起動して設定を有効にします。

LDAPサーバーを構成する

前提条件

OSが再起動したら、管理者としてOSにアクセスします。OSに正常にアクセスするには、ユーザー名の前にドメイン名を追加する必要があります。

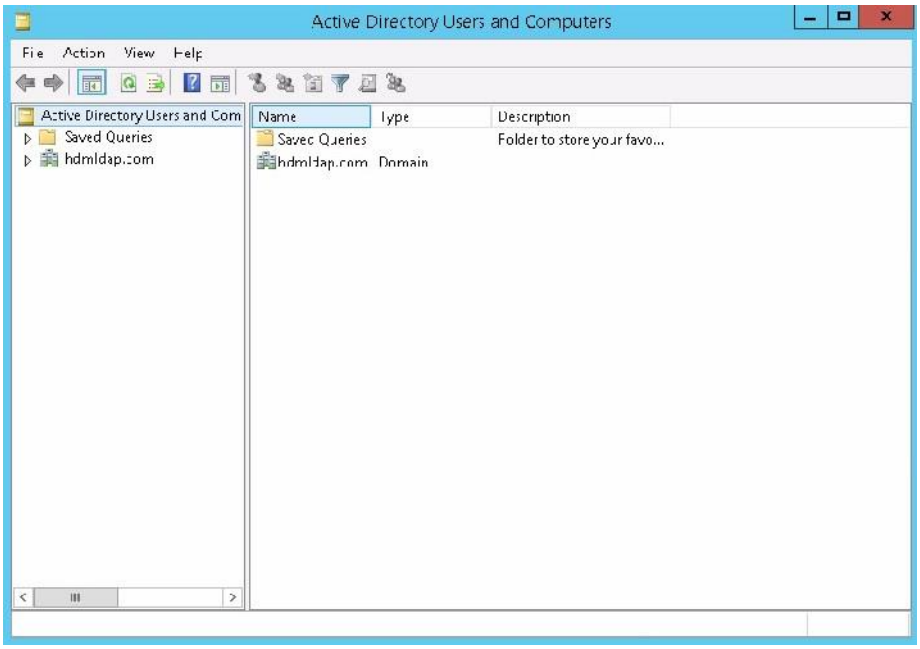
組織単位を作成する

LDAPは組織単位のレベルをサポートしています。必要に応じて任意のレベルの組織単位を作成できます。この項では、例として第1レベルの組織単位とその第2レベルの組織単位を作成します。

組織単位を作成する手順は、次のとおりです。

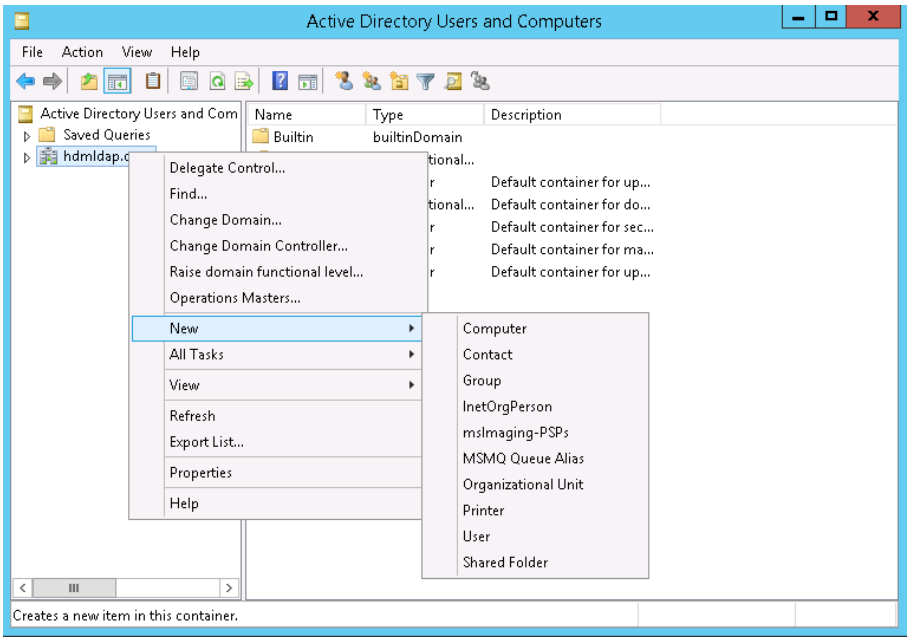
1. サーバーマネージャを開きます。
2. 右上隅の**Tasks**ボタンをクリックし、**Active Directory Users andComputers**を選択します。

図223 Active Directory Users and Computersウィンドウ



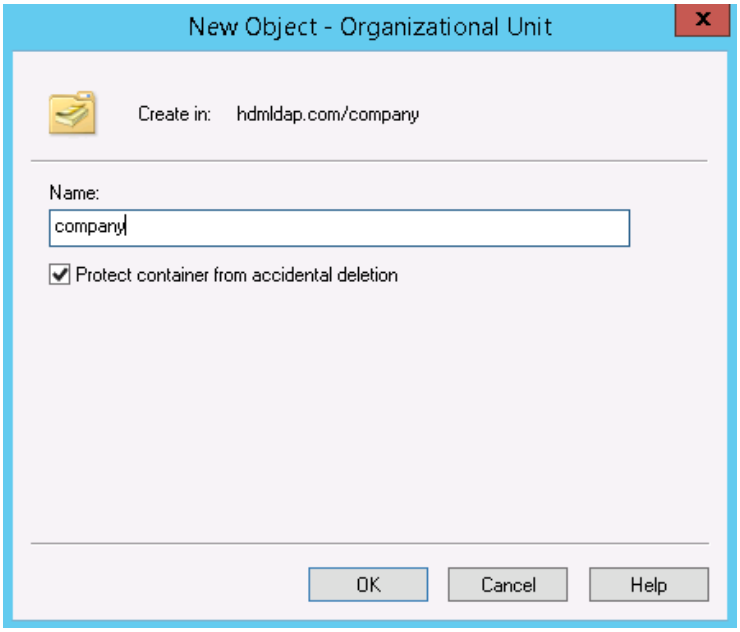
3. 左側のナビゲーションペインで**hdmldap.com**を右クリックし、**New > Organizational Unit**を選択します。

図224 ドメイン名を右クリック



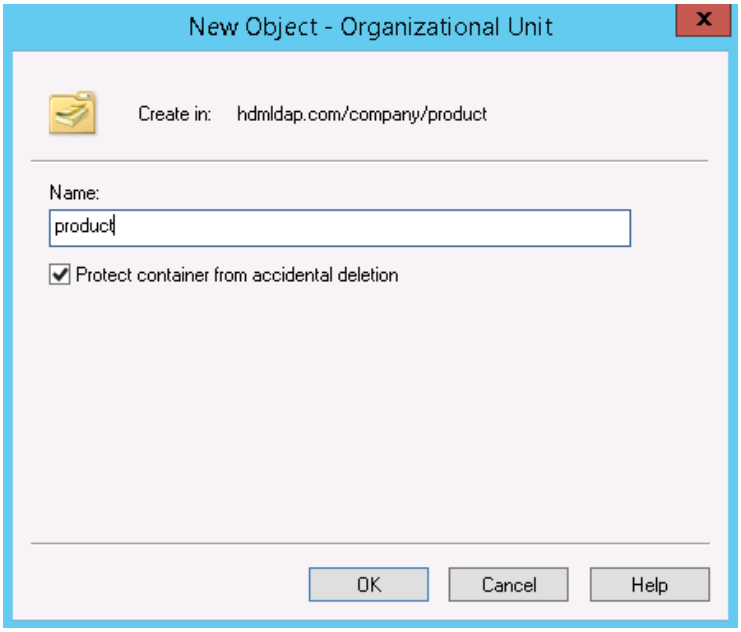
4. 表示されたダイアログボックスで、**company**などの組織単位名を入力し、**OK**をクリックします。
   第1レベルの組織単位**company**が正常に作成されました。

図225 第1レベルの組織単位の作成



5. 第1レベルの組織単位に対して第2レベルの組織単位を作成するには**company**を選択し、**New** > **Organizational Unit**を選択します。
6. 表示されたダイアログボックスで、組織単位名に例えば、**product**などを入力し、**OK**をクリックします。
   第2レベルの組織単位プロダクトが正常に作成されました。

図226 第2レベルの組織単位の作成



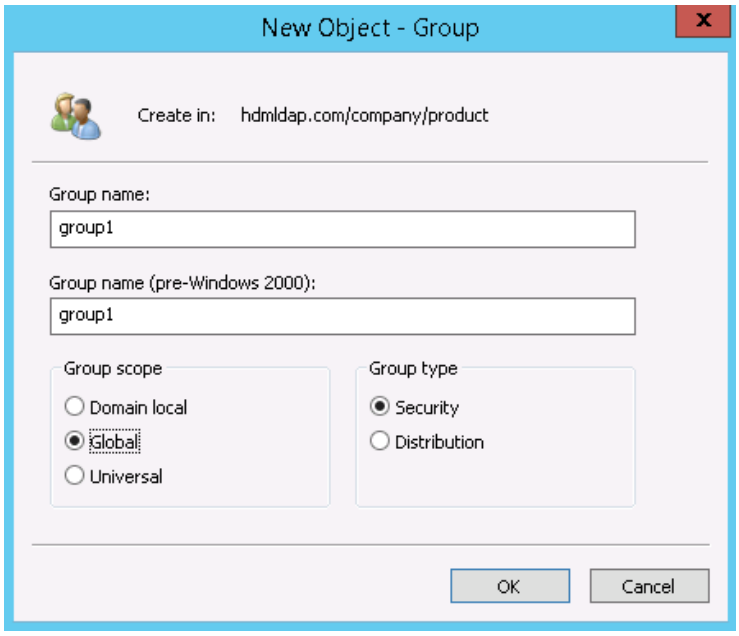
ロールグループを作成する

任意のレベルの組織単位に対してロールグループを作成できます。ロールグループを作成する手順は、次のとおりです。

1. 組織単位を右クリックして、**New** > **Group**を選択します。このセクションは第2レベルを取ります。
   例として組織単位製品を挙げます。
2. 表示されたダイアログボックスで、グループ名、例えば、**group1**などを入力し、グループスコープとグループタイプを選択して、**OK**をクリックします。

   ベストプラクティスとして、**Group name**フィールドと**Group name(pre-Windows 2000)**フィールドに同じグループ名を指定します。

図227 役割グループの作成



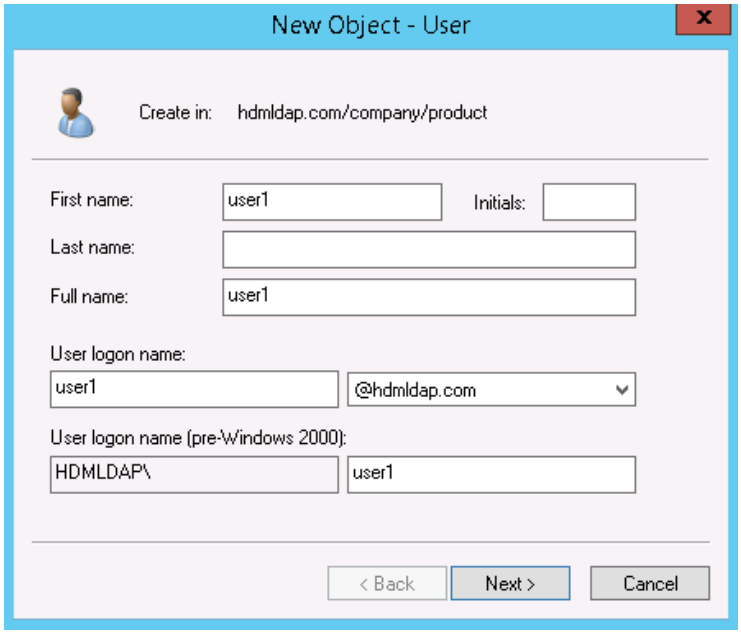
ユーザーの作成

任意のレベルの組織単位に対してユーザーを作成できます。ユーザーを作成する手順は、次のとおりです。

1. 組織単位を右クリックし、**New** > **User**を選択します。このセクションでは、第2レベルを取り上げます。例として**product**を挙げます。
2. 表示されたダイアログボックスで、必要に応じてユーザー設定を構成し、**Next**をクリックします。

   User logon nameおよび**User logon name(pre-Windows 2000)**フィールドのユーザー名は、HDMログインに使用されます。

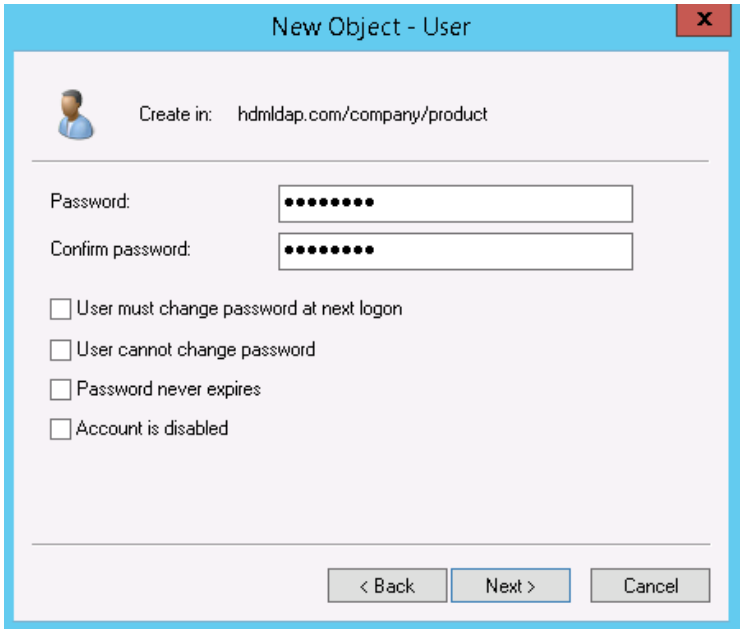
   図228 ユーザーの作成



3. パスワードを設定し、ユーザーは**User must change password at next logon**オプションをキャンセルして**Next**をクリックします。

   パスワードはHDMログインに使用されます。

   図229 パスワードの設定



4. ユーザー設定が正しいことを確認し、**Finish**をクリックします。

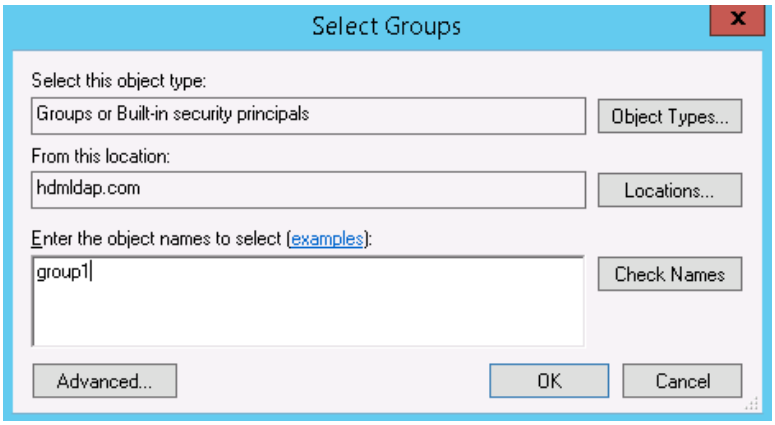
ロールグループにユーザーを追加する

ロールグループにユーザーを追加するには、ロールグループを設定するか、ユーザーを設定します。この項では、ユーザーを例として設定します。

ユーザーをユーザーグループに追加する手順は、次のとおりです。

1. ターゲットユーザー、例えば**user1**などを右クリックし、**Add to a group**を選択します。
2. 表示されたダイアログボックスで、役割グループ名、例えば**group1**などを入力し、**OK**をクリックします。

図230 役割グループの選択



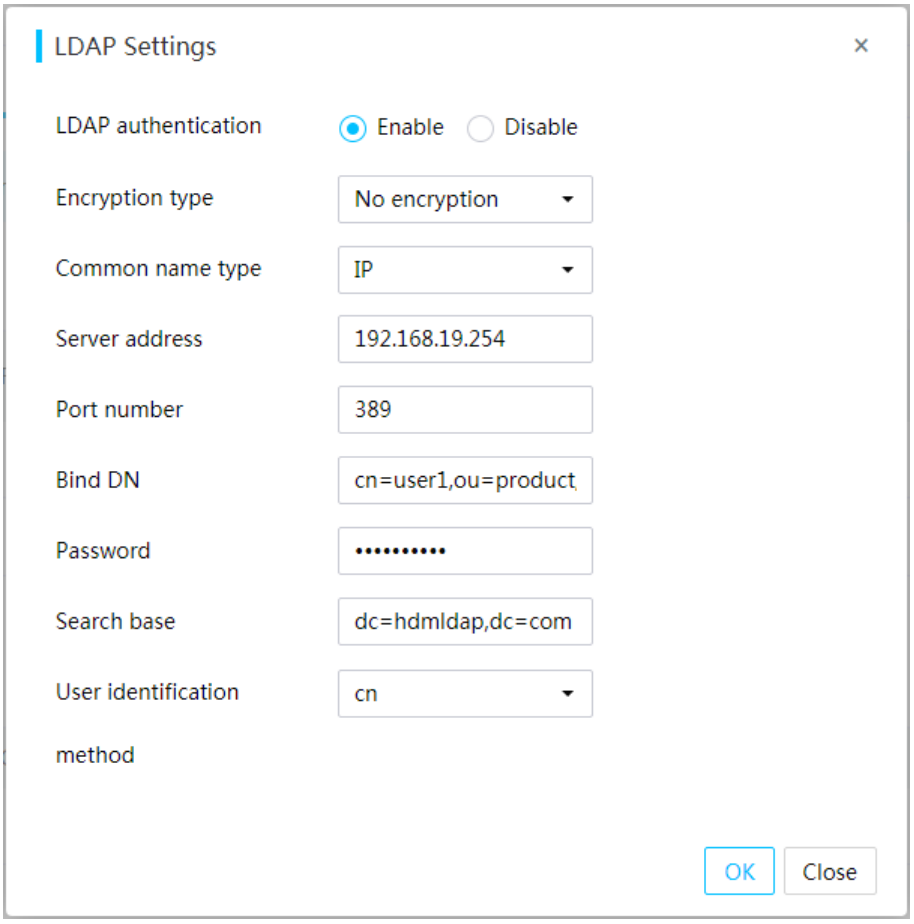
HDMからLDAP設定を構成する

LDAP設定の構成

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **LDAP Settings**セクションで、**Settings**をクリックします。
5. 表示されたダイアログボックスで、LDAP認証を有効にし、次のLDAPパラメーターを設定します(図231を参照)。
   a. 暗号化タイプとして**No encryption**を選択します。
   b. 共通名タイプとして**IP**を選択します。
   c. **Server address**フィールドに、LDAPサーバーのOS IPアドレスを入力します。
   d. デフォルトのポート番号を使用します。
   e. ユーザーのDN情報、例えば、**user1**などを入力します。これには、共通名、レベルの昇順の組織単位およびドメイン名が含まれます。これらのパラメーターはカンマで区切ります。

      この例では、**cn=user1,ou=product,ou=company,dc=hdmldap,dc=com**と入力します。
   f. ユーザーのパスワードを入力します。
   g. **Search base**フィールドにユーザーのドメイン情報を入力します。
   h. ユーザー識別方法として**cn**を選択します。

図231 LDAPパラメーターの構成

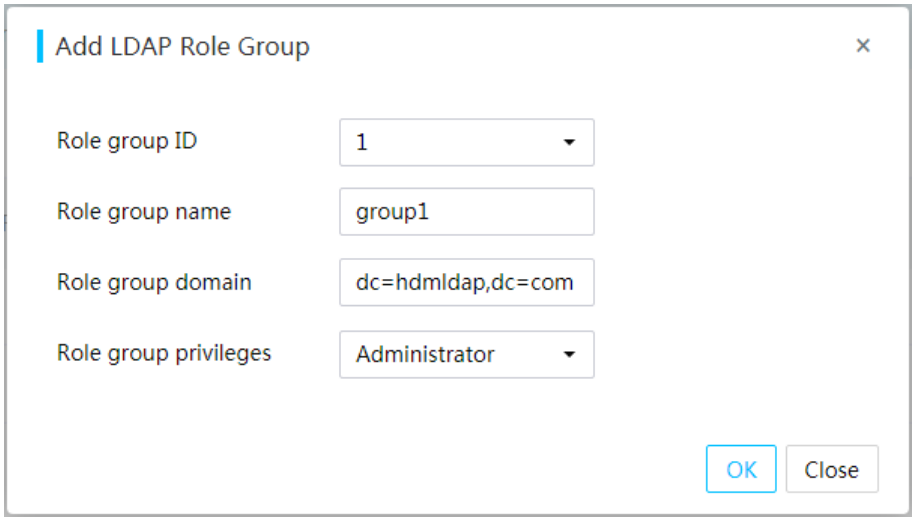


6. **OK**をクリックします。

役割グループを追加する

1. 上部のナビゲーションバーで、**Users & Security**をクリックします。
2. 左側のナビゲーションペインで、**User Accounts**を選択します。
3. **Domain Users**タブをクリックします。
4. **LDAP Settings**セクションで、**Add role groups**をクリックします。
5. 図232に示すように、役割グループのパラメーターを構成します。
6. **OK**をクリックします。

図232 役割グループの追加

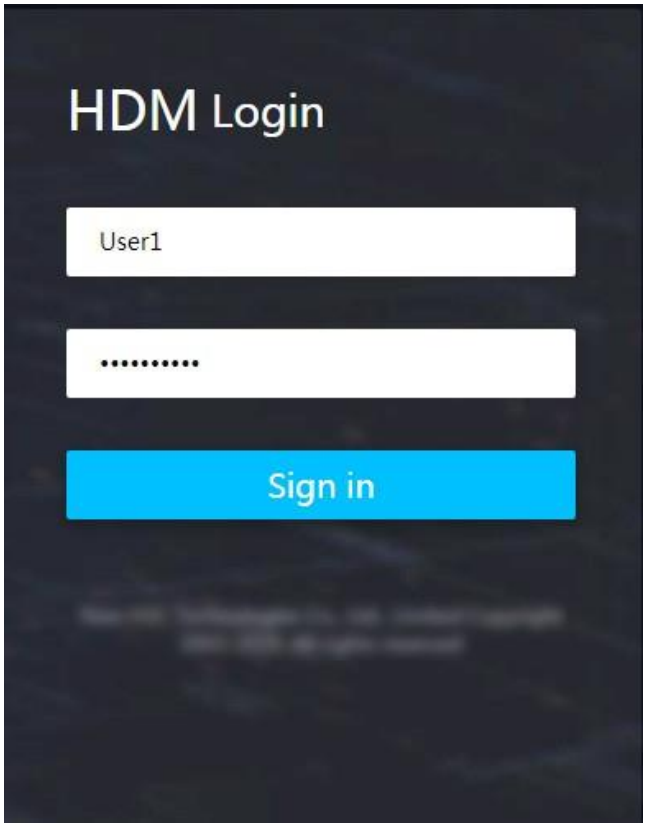


LDAP設定を確認する

LDAP設定が完了し、有効になっていることを確認するには、次の作業を実行します。LDAP設定を確認するには、次の手順を実行します。

1. ロールグループ**group1**のユーザー名とパスワードを使用してHDMにサインインします。このセクションでは、ユーザー例として**user1**を使用します。

   図233 HDMへのサインイン

2. LDAP設定を表示します。

LDAPキーワード

キーワード	フルネーム	説明
dc	Domain component	ドメイン名。たとえば、ドメイン名example.comは dc=example,dc=comに変換できます。
Uid	User ID	ユーザーのID。
ou	Organizational unit	ユーザーやグループなどのActive Directoryオブジェクトを管理できるActive Directoryのコンテナ。
cn	Common name	該当なし
sn	Surname	該当なし
dn	Distinguished name	ディレクトリ内のエントリを一意に識別する識別名。
c	Country	国または地域コード。例:CN。
o	Organization	組織名。

付録A ダウンロードされたログファイル

レベル1	レベル2	ファイル名	説明
dump		Dump_end	ダンプ終了時刻
		HDM_SDS_DUMP_DUP_01	暗号化情報のダンプ
		HDM_SDS_DUMP_DUP_02	暗号化情報のダンプ
		HDM_SDS_DUMP_DUP_03	暗号化情報のダンプ
		HDM_SDS_DUMP_DUP_04	暗号化情報のダンプ
event		*.sbe	イベントログの内部レコード
		*.csv	イベントログの内部レコード
Hdm		pack.info	SDSログ圧縮情報
sdmmc0p4	ログ	Auth	HDMログイン認証情報
		Operate	操作ログ
		Update	ログの更新
		Visible	監査ログ
static		board_cfg	システムボードまたはメインボード情報
		hdm.json	HDM設定
		bios.json	BIOS設定
		raid.json	RAID構成
		Firmware_version	システムファームウェアのバージョン情報
		FruInfo	FRU情報
		hardware.info	ハードウェア情報
		Hardware_info	ハードウェア情報
		net_cfg	ネット構成
		nvme_info	NVMeドライブ情報
		psu_cfg	電源構成
		Semsor_info	センサーリスト
		Test	SDSログ

付録B POSTコード

表16 SECフェーズのポストコード

POSTコード	説明
00	使用されない
01	電源オン
02	マイクロコードの初期化
03	キャッシュの初期化
04	キャッシュの初期化が完了し、有効化
05	SBSP\PBSPブランチの初期化
06	SEC CPU初期化CompleteCPU

表17 PEIフェーズのPOSTコード

POSTコード	説明
10	PEIコアが開始しました
11	プリメモリーCPU初期化が開始される
12から14	CPU用に予約済み
15	プリメモリーNB 初期化
16から18	NB用に予約済み
19	プリメモリーSB 初期化
1aから1c	SB用に予約済み
1dから2a	OEM用に予約済み
2b	メモリー初期化-SPD読み取り
2c	メモリー初期化開始
2d	残りのSPDデータの収集
2e	DDRのトレーニング
2	ハードウェアメモリーテストおよび初期化
30	AML用に予約済み
31	メモリーの初期化が完了しました
32	CPU POST-メモリー初期化
33	CPUキャッシュの初期化
34	アプリケーションプロセッサー(AP)の初期化
35	BSP選択
36	SMMの初期化
37	メモリーNB 初期化後
38から3a	NB用に予約済み
3b	POST メモリーSB 初期化

3cから3e	SB用に予約済み
3fから4e	OEM用に予約済み
4	DXE IPL開始
60	DXEコアが開始されました
リカバリ	
f0	リカバリ-ファームウェア別
f1	リカバリ-ユーザー別
f2	リカバリが開始されました
f3	リカバリカプセルが見つかりました
f4	リカバリカプセルロード済み
S3	
e0	S3再開を開始しました
e1	S3ブートスクリプトの実行
e2	ビデオの再投稿
e3	OS S3スリープ状態解除ベクトル呼び出し

表18 DXEフェーズのPOSTコード

POSTコード	説明
60	DXEコアが開始されました
61	NVRAMの初期化
62	SBランタイムのインストール
63	CPU DXEの初期化
64から67	CPU用に予約済み
68	PCI HB初期化
69	NB DXEの初期化
6a	NBDXESMM初期化
6bから6f	NB用に予約済み
70	SB DXEの初期化
71	SB DXE SMM初期化
72	SBデバイスの初期化
73から77	SB用に予約済み
78	ACPIモジュールの初期化
7aから7f	AMI用に予約されています
80から8f	OEM用に予約済み
90	開始したBDS
91	ドライバを接続する
92	PCIバスの初期化
93	PCIバスホットプラグコントローラーの初期化

POSTコード	説明
94	PCIバスの列挙
95	PCIバスリクエストリソース
96	PCIバスリソースの割り当て
97	コンソール出力デバイスの接続
98	コンソール入力デバイスの接続
99	SIOの初期化
9a	USBの初期化
9b	USBリセット
9c	USB検出
9	USB有効
9eから9f	AMI用に予約されています
a0	IDE初期化が開始されました
a1	IDEリセット
a2	IDE検出
a3	IDE有効
a4	SCSIの初期化
a5	SCSIリセット
a6	SCSI検出
a7	SCSIイネーブル
a8	セットアップパスワードの確認
a9	セットアップの開始
Aa	AML用に予約済み
Ab	SetupキーPress Wait
Ac	AML用に予約済み
Ad	起動準備完了
Ae	レガシーブートイベント
Af	ブートサービスを終了する
b0	仮想アドレスの開始
b1	仮想アドレスの終了
b2	レガシーオプションROMの初期化
b3	システムリセットが開始されました
b4	USBホットプラグ
b5	PCIバスホットプラグ
b6	NVRAMのクリーンアップ
b7	構成のリセット
b8からbf	AMI用に予約されています
c0からcf	OEM用に予約済み

POSTコード	説明
d0	DXE CPU初期化エラー
d1	DXE NB初期化エラー
d2	DXE SB初期化エラー

d3	一部のアーキテクチャプロトコルは使用できません
d4	「Insufficient PCI Resources error」、「Cause:Insufficient PCI MMIO Resource」、「Solution:Need to remove PCI card」
d5	レガシーOpROM用の十分なスペースがありません
d6	ConOutなし//BDS報告
d7	ConInなし//BDSによる報告
d8	パスワードが無効です
d9	ブートオプションのロードに失敗しました
da	ブートオプションが失敗しました
db	フラッシュの更新に失敗しました
dc	リセットプロトコルは使用できません
deからdf	AMI用に予約されています

表19 PEIエラーコード

PEIエラーコード	説明
50	SPD読み取りに失敗しました
53	"Memory Not Detected/Not Use Full.","考えられる原因:No Memory Found","解決方法:DIMMを挿入するか、既存のDIMMを交換してください"
54	「ハードウェアメモリーテスト障害(SIMULATED)」、「原因:メモリーテスト障害」、「解決策:CPU 0の下のスロット6にあるDIMMを交換してください。」
55	メモリーが装着されていない
56	無効なCPUタイプ/速度
57	「CPU Mismatch(SIMULATED)」、「考えられる原因:Cbo Count/List mismatch」、「ソリューション:CPUに同じCbo Countを設定する」
58	CPUセルフテスト失敗/キャッシュエラー
59	マイクロコード/マイクロコードの更新に失敗しました
5a	CPU内部エラー
5b	PPIのリセットは使用できません
f8	リカバリPPIが見つかりません
f9	リカバリカプセルが見つかりません
fa	リカバリカプセルが無効です
e8	S3の再開に失敗しました
e9	S3 Resume PPIが見つかりません
ea	S3 Resume Boot Scriptエラー
ef	OS S3ウェイクアップエラー