H3C HDM

テクニカルホワイトペーパー

ソフトウェアバージョン:V2.2

内容

概要

ハードウェアデバイス管理(HDM)はリモートサーバー管理システムです。IPMI、SNMP、Redfish標準に準拠し、キーボード、ビデオ、マウスのリダイレクト、テキストコンソールのリダイレクト、SOL接続、リモートバーチャルメディア、信頼性の高いハードウェア監視と管理などのさまざまな機能を提供します。HDMは表1に示すような豊富な機能をサポートしています。

表1 HDMの特徴

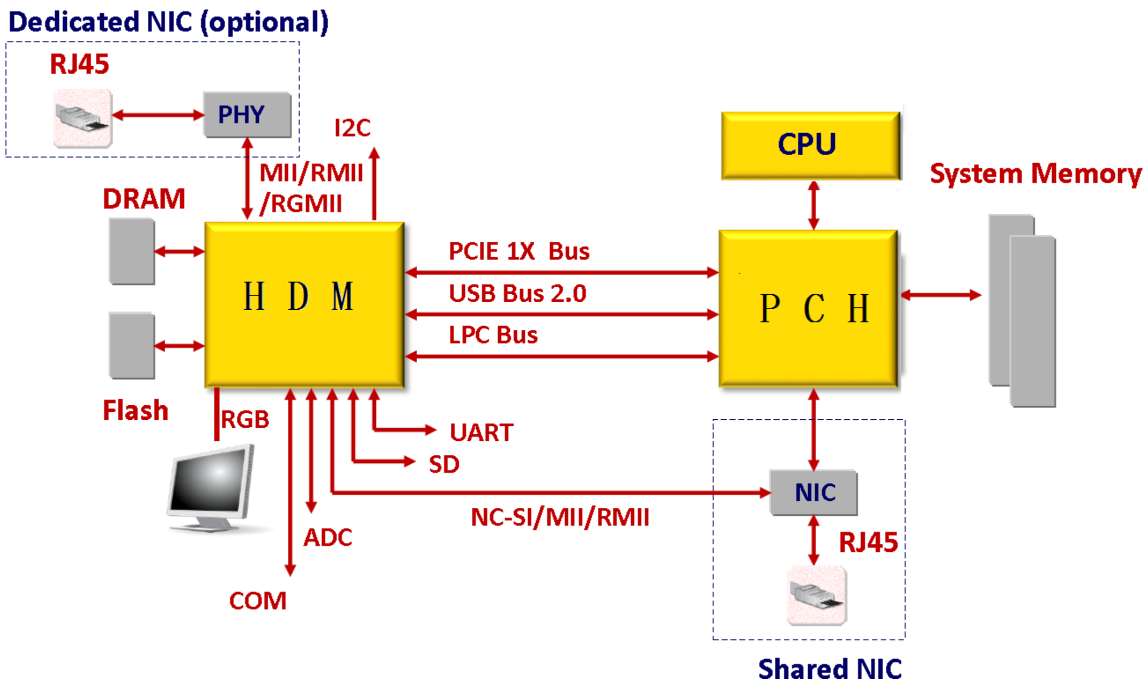
機能	説明
さまざまな管理インターフェイス	IPMI、HTTPS、SNMP、Redfishなどの豊富な管理インターフェイスを提供し、さまざまなシステム統合要件を満たします。
統一された制御	小規模で統一管理を実施することにより、中小規模のサーバーのO&Mコストを削減します。
LCDディスプレイ	一部のラックサーバーでは、オンサイトでの検査やメンテナンスを容易にするために、タッチ操作可能な3.5インチLCDディスプレイをオプションで使用できます。
障害の監視と診断	24×7デバイスの正常な動作を保証するために、メンテナンスのための障害の特定と診断を提供します。 障害ログは、SNMPトラップ、SMTP、Redfishイベントサブスクリプション、およびsyslogメッセージを通じて事前に報告できます。
重要なOSイベントのスクリーンショットとビデオ録画	将来のトラブルシューティングのために、重要なOSイベント(クラッシュなど)のスクリーンショットを撮ったり、ビデオを録画したりします。
アウトオブバンドRAID管理	アウトオブバンドRAIDの監視と構成をサポートし、RAID構成の効率と管理機能を向上させます。
スマートな電源管理	消費電力上限をサポートして導入密度を高め、動的な電源管理を提供して運用コストを削減します。
KVM、VNC、および仮想メディア	リモートサーバーメンテナンスを容易にします。
DNS、LDAP、およびAD	ドメイン管理とディレクトーリサービスをサポートし、サーバーネットワーク管理とユーザー管理をシンプル化します。
USB Wi-Fiアダプター	外部XiaomiポータブルWi-Fiアダプターをサポートし、サーバーの近距離保守と管理を容易にします。
プライマリ/バックアップイメージのスイッチオーバー	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します。これにより、システムの可用性が向上します。
サービス用USBデバイス	ログのダウンロードをサポートし、オンサイトでの保守と管理を容易にします。
資産管理	資産管理をシンプル化
セキュリティ管理	サービスアクセス、ユーザーカウント、データ伝送、ストレージに関するサーバーセキュリティを確保し、2要素認証、ホワイトリストとブラックリストルール(ファイアウォール)、管理インターフェイス、SSL、Silicon Root of Trust、カスタムユーザー権限をサポートします。

HDM設計

図1に示すように、HDMはサーバーハードウェアコンポーネントを効率的に管理するためにサーバー固有のシステムオンチップ(SoC)を採用しています。SoCは、KVM、64 MBローカルVGAディスプレイ(64 MBはG5シリーズでのみ使用可能)、専用および共有ネットワークポート、さまざまなボードレベルの管理機能と次のような周辺機器インターフェイスをサポートしています。

- **KVMリモートコントロール**: KVMモジュールを使用して、ビデオデータおよびキーボードとマウスのデータを次のように処理します。
  - **a.** KVMモジュールは、VGAコネクターを介してホストシステムからビデオデータを受信し、ビデオデータを圧縮してから、圧縮されたデータをリモートKVMクライアントに送信します。
  - **b.** KVMモジュールは、リモートKVMクライアントからキーボードとマウスのデータを受信し、シミュレートされたUSBキーボードとマウスデバイスを使用してデータをホストシステムに送信します。
- **LPC通信およびIPMI管理**: サーバーと通信するための従来のLPCシステムインターフェイスを提供し、標準のIPMI管理をサポートします。
- **GEインターフェイスを介したリモートアクセス**: 専用のGEインターフェイスを提供します。ネットワーク上でIPMI、Redfish、またはSNMPを使用してリモート管理を実装できます。
- **センサーベースの監視および管理**: センサーを使用してサーバーの温度と電圧を監視し、ファンと電源装置(PSU)をインテリジェントな方法で管理します。
- **NCSIおよびVLANのサポート**: Network Controller Sideband Interface(NCSI)およびVLANをサポートし、柔軟なネットワーク管理を可能にします。
- **リモートコンソール**: KVMリダイレクション、テキストコンソールリダイレクション、リモート仮想メディア(オプティカルドライバ、ドライブ、および端末フォルダをサーバーにマップするために使用)、およびIPMI 2.0ベースのハードウェア監視および管理をサポートします。
- **ソフトウェア冗長性**: 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、プライマリ/バックアップのスイッチオーバーを可能にします。
- **豊富なインターフェイス**: Webベースのユーザーインターフェイス、CLI、IPMIインターフェイス、Redfishインターフェイス、SNMPインターフェイスなど、豊富なユーザーインターフェイスを提供します。すべてのインターフェイスで、アクセスと伝送のセキュリティを確保するために、認証メカニズムと高度にセキュアな暗号化アルゴリズムが採用されています。
- **総合的なサーバー監視**: サーバーを監視し、プロセッサーコアの温度、電圧、ファン速度、電源装置の障害などに関するさまざまなアラームと詳細なログを提供します。また、HDMでは、プロセッサー、メモリー、およびドライブに関する情報を照会できます。
- **障害の位置**: 障害の位置に関するサーバーブレークダウン時の最新画面出力を保存し、サードパーティプログラムによって制御されるスケジュール済画面スナップショットをサポートします。これにより、手動による介入が不要になり、メンテナンス時間が短縮されます。

図1 HDMアーキテクチャ



HDM機能

さまざまな管理インターフェイス

Web管理インターフェイス

HDMでは、HTTPSベースのWebインターフェイスを使用して視覚的な管理を行い、サーバーの設定と情報フィルタリングを簡素化します。ユーザーは、GUIからリモートコンソールを使用して、OSの起動の監視、OS操作の実行、ドライバまたはフロッピードライバのマッピングの設定を行うことができます。

HDM Webインターフェイスにサインインするには:

1. ブラウザを開き、アドレスバーにHDM管理IPアドレスまたはドメイン名を入力します。
2. HDMサインインページでユーザー名とパスワードを入力します。

サポートされているブラウザには、Internet Explorer 11(以上)、Google Chrome 48(以上)、Mozilla Firefox 78(以上)があります。

IPMI管理インターフェイス

HDMはIPMI 1.5およびIPMI 2.0標準と互換性があり、Data Center Manageability Interface(DCMI)をサポートしています。HDMは、LPCチャネルまたはLANチャネルを介してIPMIToolなどのサードパーティ製ツールを使用することで、サーバーを効率的に管理できます。

- LPCチャネルでは、KCSが使用され、サードパーティ製ツールはサーバーのOS上で動作する必要があります。
- LANチャネルには、UDPまたはIPが使用され、サードパーティ製ツールがリモートでサーバーを管理できます。

サードパーティ製ツールがWindowsまたはLinuxをサポートしている必要があります。

IPMItoolコマンドは、ipmitool[interface][parameter]<command>形式です。たとえば、HDMからすべてのセンサーを表示するには、次のIPMItoolコマンドを実行します。

- **LPCベースのKCS**: **ipmitool sensor list**
- **LANベースのUDPまたはIP** :ipmitool -H *.*.*.* -I lanplus -U <*username*> -P <*password*> sensor list
  - **-H *.*.*.***: HDMネットワークポートのIPアドレスを指定します。*.*.*.*引数はIPアドレスを表します。
  - **-I lanplus**: 送信の暗号化ステータスを指定します。-I lanplusを指定して送信を暗号化するか、-I lan を指定すると送信を暗号化できません。
  - -U <*username*>: HDMユーザー名を指定します。<*username*>引数はユーザー名を表します。
  - -P <*password*>: HDMパスワードを指定します。<*password*>引数はパスワードを表します。
  - -L <*user role*>: ユーザー権限を指定します。デフォルトのユーザー役割はAdministratorです。

SNMP管理インターフェイス

Simple Network Management Protocol(SNMP)は、Network Management Services(NMS)とエージェント間の通信プロトコルで、標準的な管理フレームワークを定義します。

共通の通信言語、およびネットワーク内のデバイス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。

SNMPには、次の利点があります。

- TCP/IPベースの標準プロトコルで、UDPは伝送層プロトコルです。
- 自動ネットワーク管理を提供します。管理者は、情報の照会と編集、ネットワーク問題の識別と診断、キャパシティプランニングの実行、およびSNMPプラットフォームを使用するネットワークノードに関するレポートの生成を行うことができます。
- デバイス間の物理的な違いを遮蔽して、異なるベンダーの製品の自動管理を実現します。SNMPは基本的な機能セットのみを提供し、管理対象デバイスの物理的な機能と実際のネットワークテクノロジーの両方に比較的依存しない管理タスクを実現します。したがって、SNMPは異なるベンダーのデバイスの管理を実現します。
- 単純な要求応答モードとアクティブな通知モードを組み合わせ、再送信タイムアウトメカニズムを提供します。
- 少数のパケットタイプと単純なパケットフォーマットを必要とするため、解決と実装が容易になります。
- 認証および暗号化メカニズムを提供し、セキュリティ強化のためにSNMPv3のユーザーベースのアクセスコントロール機能を使用します。
- HDMはSNMPベースのプログラミングインタ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、システムヘルスイベント、ハードウェア情報、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。

Redfish管理インターフェイス

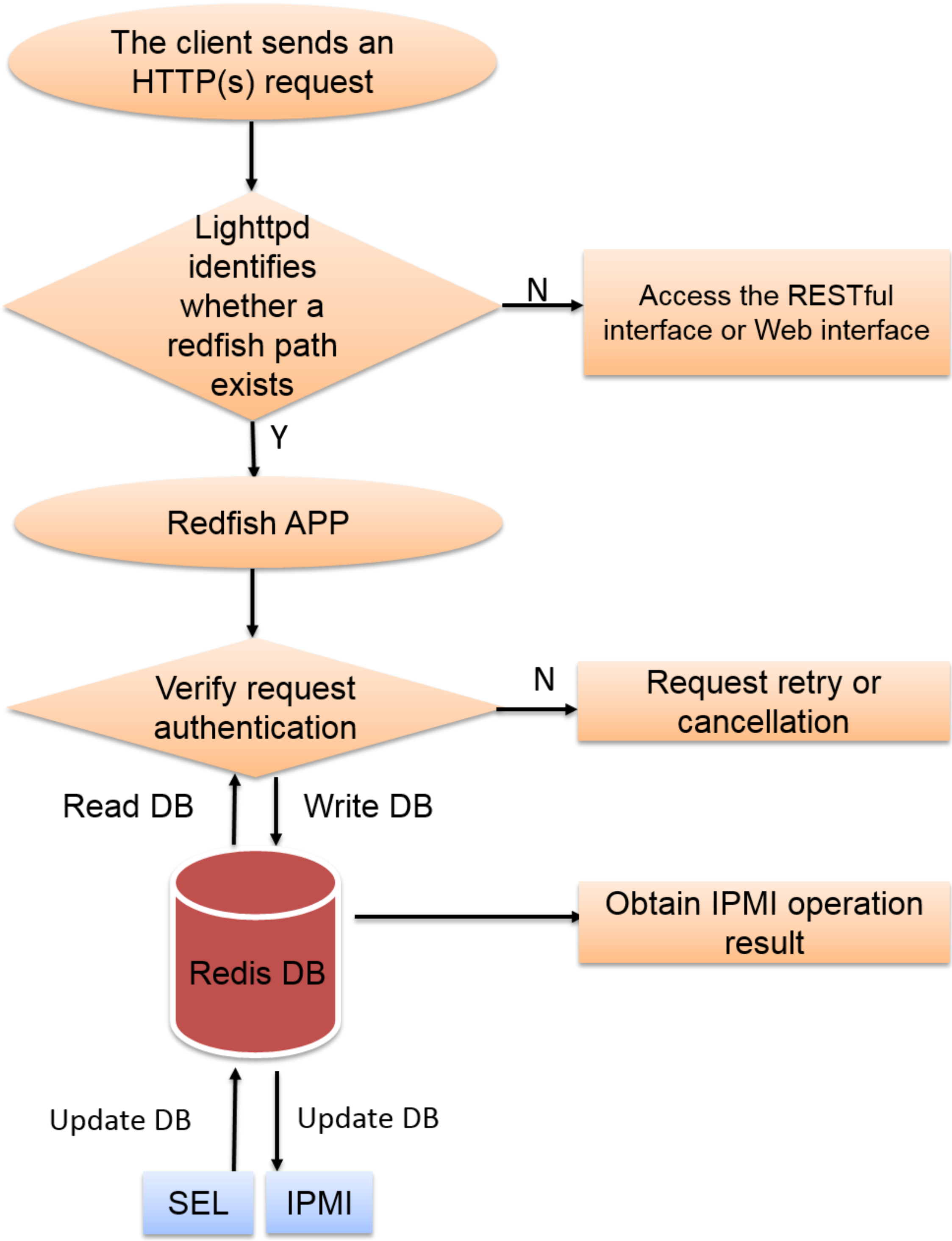
Redfishは、デバイス管理のためのHTTPSベースのRESTful APIを提供する。各HTTPSオペレーションは、リソースリクエストを送信するか、JSONフォーマットでUTF-8エンコードされたリソースレスポンスを取得する。これは、Webアプリケーションがブラウザ にHTMLファイルを返すプロセスに似ている。Redfishは、開発の複雑さを軽減し、実装、使用、拡張が容易である。Redfishインターフェイスを使用して、ユーザー管理、サーバー情報クエリ、管理モジュール情報クエリなど、一般的なHDMおよびBIOS設定を実装することができる。

Redfish はREST APIとソフトウェア定義サーバー(データモデル)を組み合わせたもので、DMTF(www.dmtf.org)によって定義されています。

図2に示すように、Redfishのワークフローは以下のとおりであり、RedfishデータベースはSELとIPMIを介してHTTPS操作ごとにリアルタイムで更新されます。

1. クライアントはHTTPS要求を送信します。
2. HTTPS要求は認証(認証トークンと基本認証)を渡し、データベースからデータを取得します。
3. Lighttpdはクライアントに応答を送信します。

図2 Redfishワークフロー

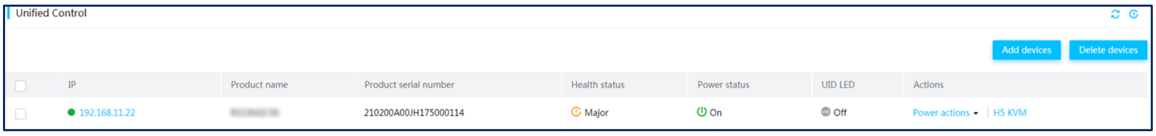


HDM統合制御

HDM統合制御は、小規模に統合制御を実装することで、中小企業のサーバーのO&Mを簡素化します。統合制御機能では、次のタスクを実行できます。

- 最大10台のデバイスを一括で追加します。
  現在のソフトウェアバージョンでは、IPv6アドレスはサポートされていません。
- 1つまたは複数のデバイスを一括で削除する。
- デバイス情報の表示(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)。
- サーバーの電源投入、電源切断、電源再投入などの電源操作の実行。
- H5 KVMリモートコンソールの起動

図3 Unified Controlメニュー



LCDディスプレイ

一部のH3Cラックサーバーでは、サーバー設定を表示または構成するために、タッチ式3.5インチLCDディスプレイをオプションで使用できます。LCDディスプレイは、ローカルメンテナンスの利便性を向上させるとともに、障害の特定とトラブルシューティングを迅速化します。

LCDディスプレイでは、次のタスクを実行できます。

- 製品名、製品シリアル番号、HDMまたはBIOSファームウェアバージョンなどの基本的なサーバー情報を表示します。
- サーバーシステムとサブシステム(プロセッサー、メモリー、ストレージ、ファン、電源装置、温度センサーなど)のヘルス状態とログを表示します。
- 吸気口とプロセッサーのリアルタイム温度の表示。
- HDM管理ネットワーク設定の構成や管理者アカウントの復元など、サーバー設定の構成

サーバーとそのコンポーネントの存在とヘルス状態は、次のように色で示されます。

- **緑色**: サーバーは正常です。
- **黄色**: マイナーアラームが発生しています。
- **オレンジ**: メジャーアラームが発生しています。
- **レッド**: クリティカルアラームが発生しています。
- **グレー**: コンポーネントがありません。

モニタリング

システムヘルス状態

HDMは、サーバーシステムとそのコンポーネントのヘルス状態を表示します。ヘルス状態は、ヘルスLED、LCD、診断パネル、セキュリティベゼルからも確認できます。

Dashboard > Summaryメニューには、図4または図5に示すように、サーバーの全体的なヘルス状態とアラームの概要が表示されます。ヘルス状態は、プロセッサー、DIMM、ファン、電源装置、ストレージデバイス、PCIeモジュール、温度センサー、システムボード、ドライブバックプレーン、ライザーカードなどのコンポーネントのヘルス状態によって決まります。

図4 G3サーバーの概要情報の表示

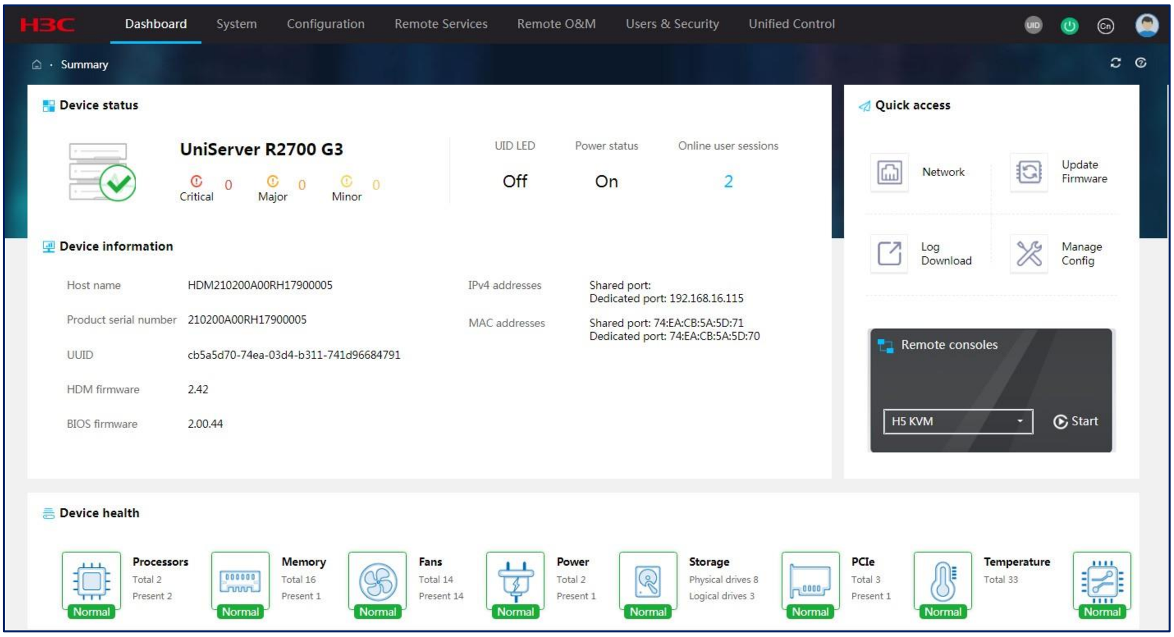
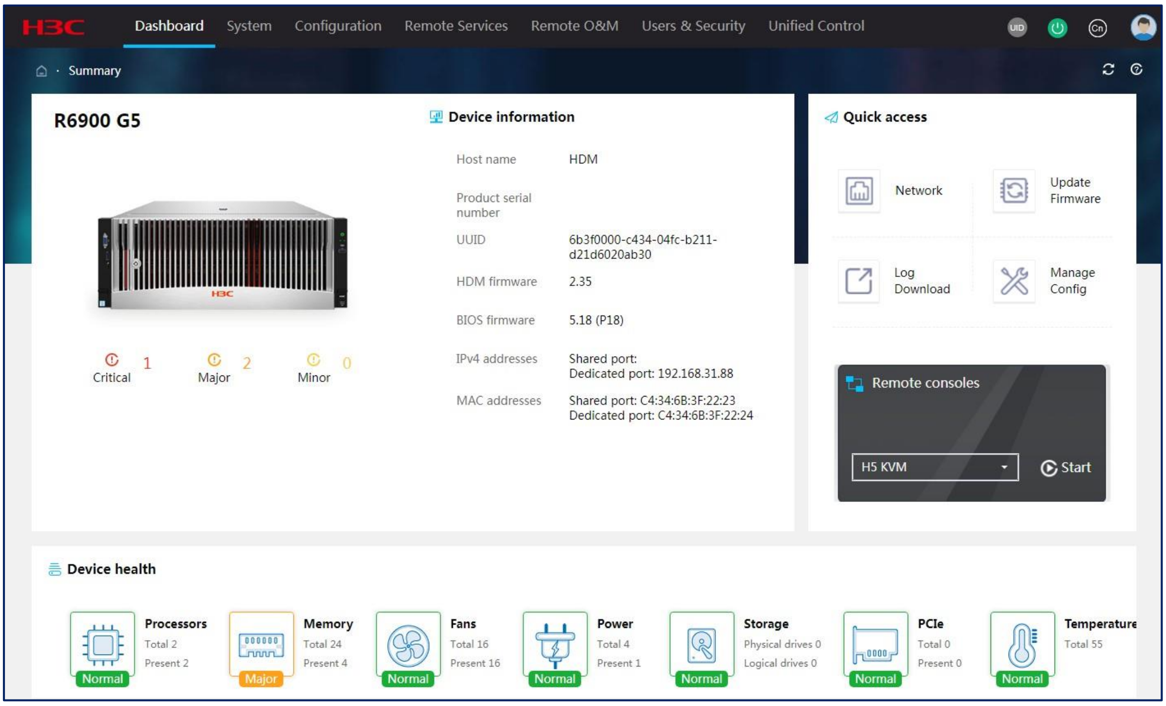


図5 G5サーバーの概要情報の表示



センサー

3Dビューの温度ヒートマップ

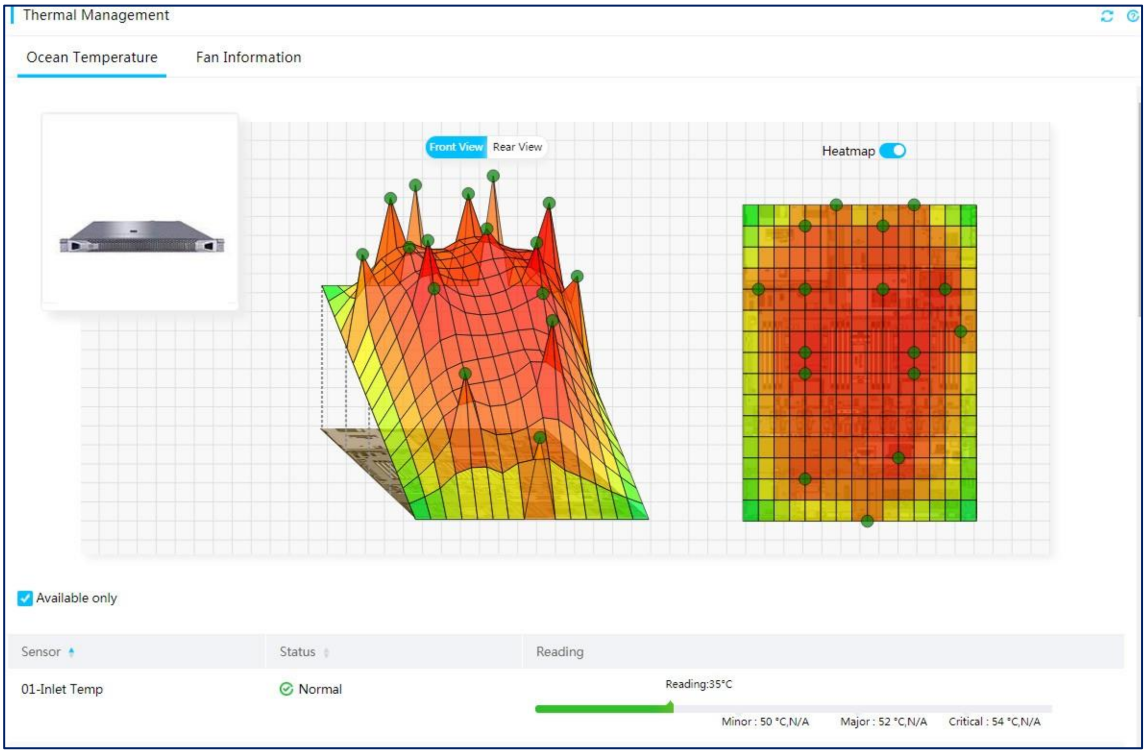
HDMでは、温度データがヒートマップ形式とテーブル形式の両方で表示されるため、サーバーの冷却パフォーマンスの監視に役立ちます。

- 温度ヒートマップでは、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が使用され、センサーを表すために円が使用されます。緑は0°C(32°F)を示します。温度が高くなるにつれて、色は暖かくなり

  赤。温度ヒートマップを使用すると、冷却状態の悪いコンポーネントをすばやく特定できます。
- 温度センサーテーブルには、各センサーの温度測定値、ステータス、座標、およびしきい値が表示されます。
  - **X**: X軸上のセンサーの位置。
  - **Y**: Y軸上のセンサーの位置。
  - **Z**: センサーが配置されているサーバー。

ある場所のセンサーの名前、ステータス、読み取り値、およびしきい値を取得するには、温度ヒートマップ上のその場所の円の上にマウスを移動します。

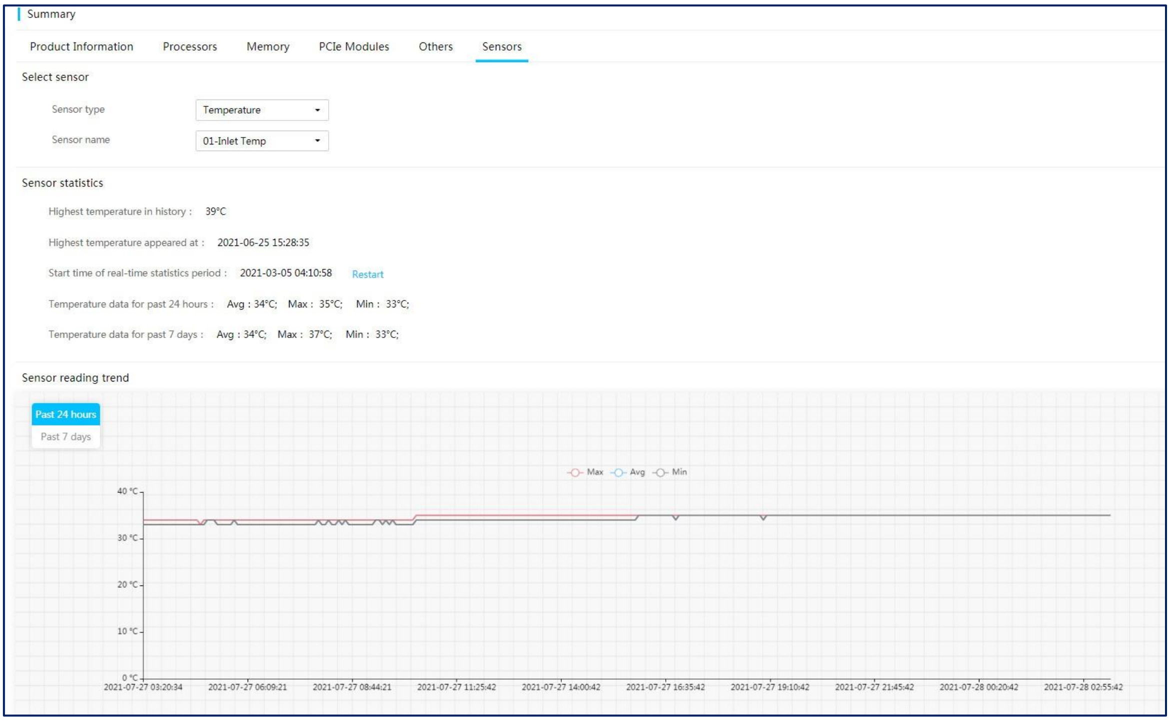
図6:温度センサー情報の表示



履歴センサー統計情報

HDMは、過去24時間または7日間に5分ごとに収集されたリニアセンサー(電圧、電流、温度およびファン速度センサー)の読み取り値の表示をサポートしています。ある時点でのリニアセンサーの最大、平均または最小センサー読み取り値も表示できます。

図7履歴センサー統計情報の表示



リソースの概要

図8に示すように、サーバーのプロセッサー、メモリーおよびディスク使用量情報を表示し、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できます。プロセッサー、メモリーまたはディスク使用量がしきい値を超えると、ログエントリーが生成されます。

リソース使用率のアラームしきい値は、図9に示すように設定できます。アラームしきい値を設定する前に、FIST SMSがインストールされており、FIST SMSがサーバーのオペレーティングシステムで実行されていることを確認してください。サポートされているオペレーティングシステムには、Redhat 6.8、Redhat 7.3およびWindows Server 2012 R2があります。

図8リソースサマリーの表示

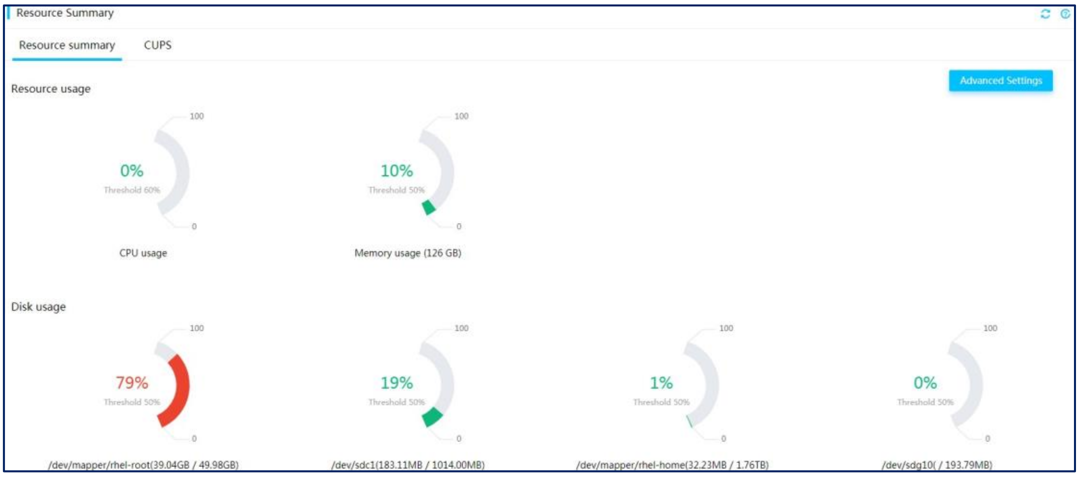
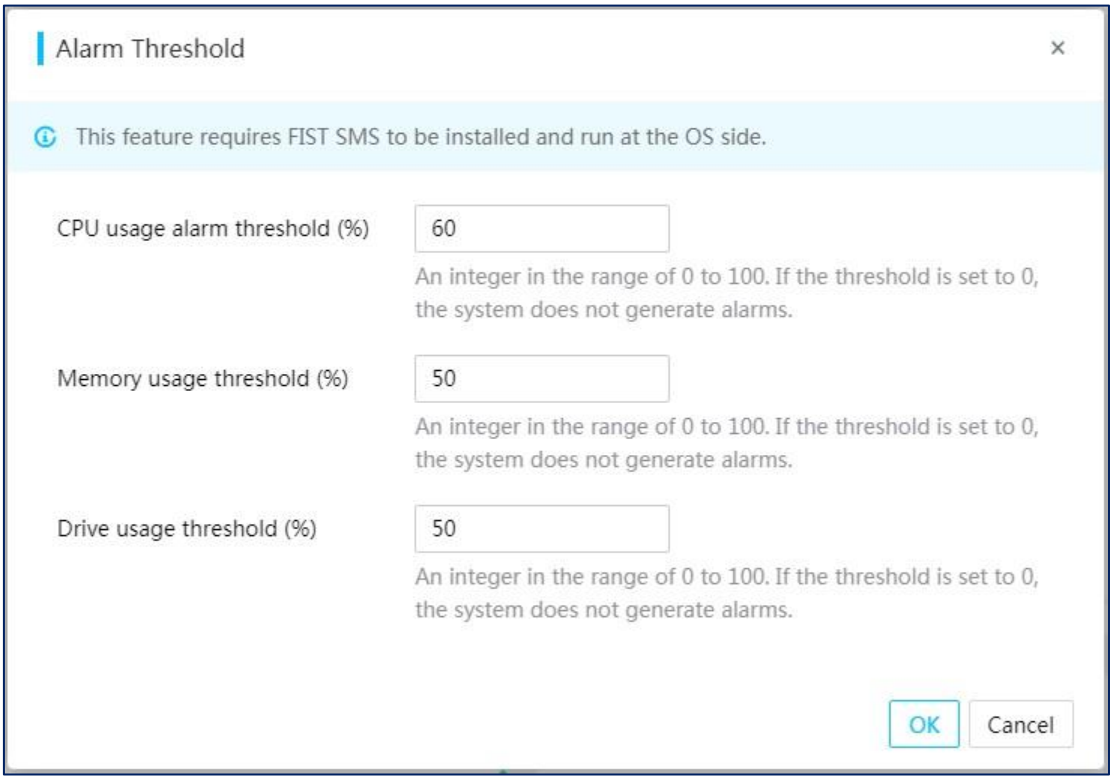


図9リソース使用率アラームしきい値の設定

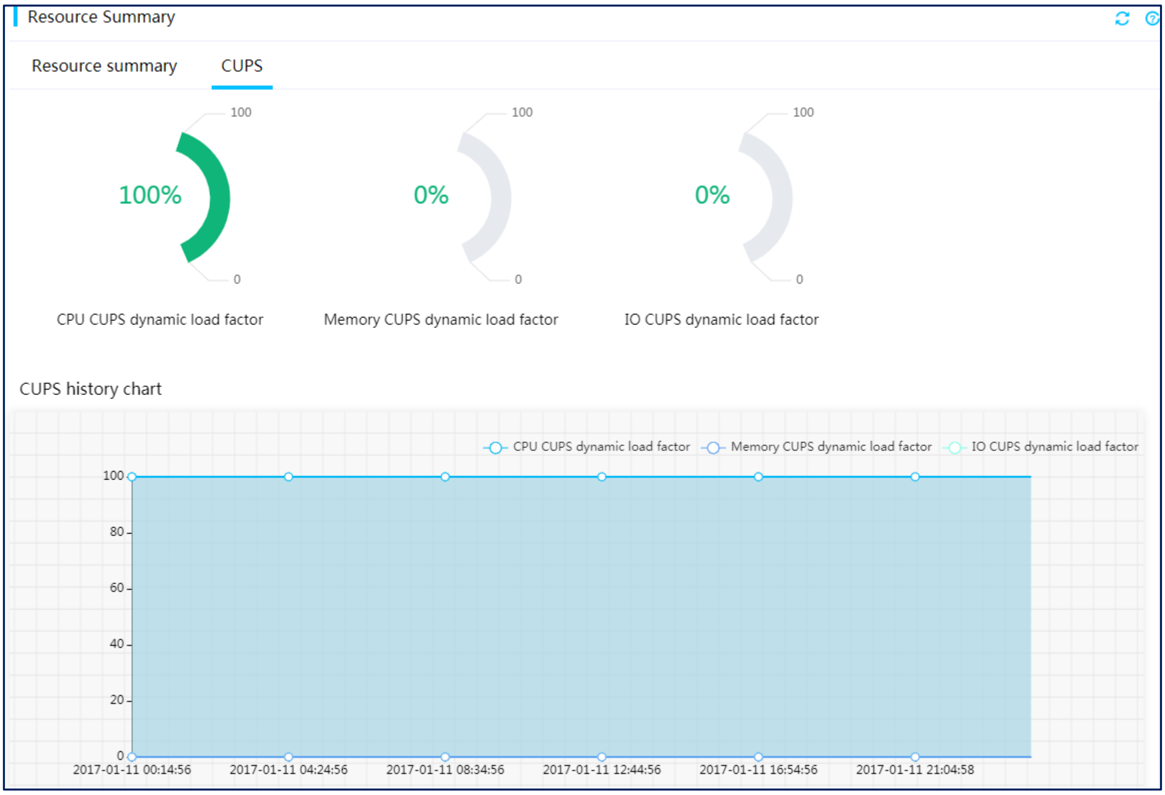


CUPS

CUPS機能は、システム内のプロセッサー、メモリーおよびI/O使用率をリアルタイムで監視します。プロセッサー、メモリーおよびI/O使用率の動的負荷率の比率を使用して、システムで実行されている主要サービスのタイプを示します。プロセッサー、メモリーおよびI/O CUPSの動的負荷率は、累積CPUコアデータ使用率、メモリーバス上の累積伝送速度およびPCIeバス上のI/O帯域幅使用率をそれぞれ表します。

プロセッサー、メモリーまたはI/O CUPSの動的負荷率が高い場合は、システムで実行されているメインサービスが計算集約型、メモリー集約型またはI/O集約型であることを示します。メモリーCUPSの負荷率が高い場合は、メモリーバスアクセス率が高いことを示し、メモリー使用量(使用済メモリー/合計メモリー)とは直接関係ありません。たとえば、合計8 GBメモリーのうち2 GBメモリーが使用されている場合、メモリー使用量は25%になります。

図10 CUPS情報の表示



アラーム管理

アラーム

サーバーコンポーネントに障害が発生した場合、または何らかの理由でサーバーが正しく動作しなかった場合、システムは、障害モジュールごとに異なるタイプのアラームを生成し、同時にログを生成します。

アラームの重大度には、次のレベルがあります。

- **Info**: イベントはシステムに影響せず、アクションは必要ありません。たとえば、通常の状態変化イベントやアラーム削除イベントなどです。
- **Minor**: イベントによるシステムへの影響は軽微ですが、重大度の上昇を回避するために迅速な処置が必要です。
- **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、サービスの中断を引き起こす可能性があります。早急な対応が必要です。
- **Critical**: -このイベントにより、システムクラッシュまたはシャットダウンが発生する可能性があり

ます。ただちに対処する必要があります。次のタイプの障害が検出されます。

- **プロセッサー障害**: IERRエラー、セルフテストエラー、設定エラー(プロセッサーUPIエラー、IoH UPIエラー、プロセッサーコアエラー、およびIoHコアエラー)、およびMCERRエラーです。
- **メモリー障害**:修正可能エラー、修正不可能エラー、過熱エラー、およびPOSTトレーニング障害。
- **パワーサプライ障害**:電源の検出、パワーサプライの入力損失(AD/DC)、予測障害、およびパワーサプライのセルフテストエラー。
- **ファン障害**:ファンの存在が検出されました。ファンに障害があり、ダウングレード障害が発生しました。
- **ストレージ障害**: ドライブの存在が検出されました、ドライブ障害、予測障害、クリティカルアレイ

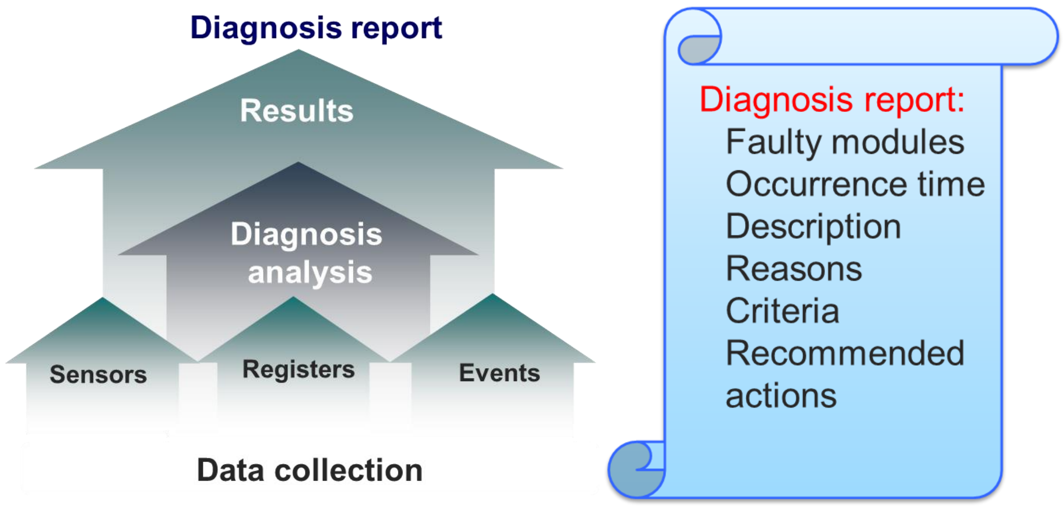
エラー、および障害アレイエラー。

- **過熱障害**: プロセッサー、メモリー、エアーインレット、パワーサプライ、およびドライブの過熱状態。
- **電圧障害**: システムボードおよびその他のサーバーボードの電圧障害。
- **バス障害**: I2C、IPMB、またはQPI/UPIバスの障害。

SDSの概要

HDM Smart Diagnose System(SDS)は、サーバー上の主要なハードウェアコンポーネントの障害を迅速かつ正確に特定して診断するライフサイクル全体のスマートデバイス診断システムです。SDSは、に示すように、センサー、CPLD、レジスタ、イベントログなどの基本的なハードウェア障害情報を収集し、履歴診断データベースに基づいて原因を特定し、診断レポートを生成します。診断レポートには、障害モジュール、障害発生時刻、障害タイプ、障害の説明、考えられる原因、診断基準、および解決策が記載されます。

図11 SDS図



SDSは、サーバーの主要コンポーネントを包括的に監視します。次のハードウェア障害を検出および診断できます。

- MCA障害(プロセッサー、メモリー、またはPCIeモジュールの障害など)。
- 電源障害(電流、電圧、温度、電源ファン、IIC、共有電流など)。
- マザーボードの障害(セカンダリパワーサプライ、ファン、ネットワークアダプター、電流、電圧、および温度センサーの障害など)。
- PCIeモジュールの障害(ネットワークアダプター、ライザーカード、およびNCSIチャネルの障害など)。
- ストレージコントローラーの障害(ストレージコントローラー、ケーブル、エクスパンダーモジュール、キャッシュ、スーパーキャパシター、ドライブの障害を含む)。

SDS故障診断

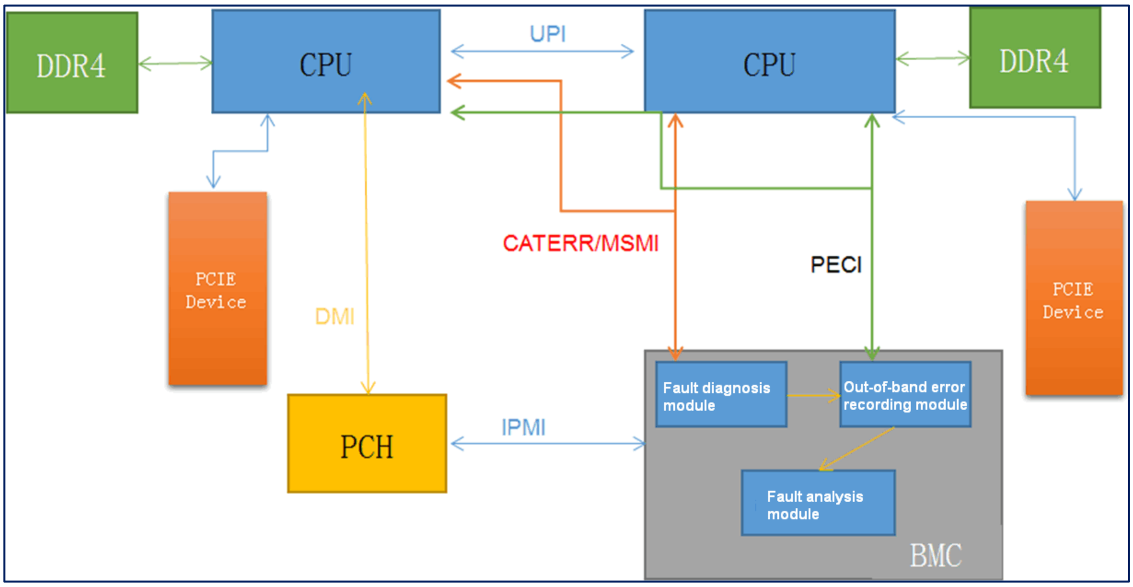
MCA障害診断(インテルプロセッサーを搭載するサーバーの場合)

Machine Check Architecture(MCA)はSDSの重要な部分です。MCA障害診断は、プロセッサー、メモリー、およびPCIeモジュールの障害検出と診断をサポートします。SDSは、ポーリング検出メカニズムを適用してMCAエラーを監視および診断します。つまり、ポーリングプロセス中にCATERRまたはMSMI信号を検出した後、SDSはPECIを通じて基本的なオンサイトハードウェア障害情報を収集します

チャネルをアウトオブバンド方式で使用します。基本情報には、主にエラー関連の銀行やCSRに関する情報が含まれており、収集されたデータと履歴ハードウェア故障診断データベースに基づいて、SDSはハードウェア故障を特定・分析し、診断レポートを作成します。

図12は、MCA障害診断メカニズムのワークフローを示しています。

図12 MCA故障診断図



次に、使用可能な障害検出のタイプについて説明します。

- プロセッサー障害検出。

  プロセッサー障害は、プロセッサー内部の内部エラーまたはメモリーおよびPCIeモジュールからの外部エラーによって発生する場合があります。MCA障害診断では、フェッチユニット(IFU)、データキャッシュユニット(DCU)およびデータ変換ルックアサイドバッファ(DTLB)など、プロセッサーの内部モジュールで発生したエラーを検出できます。

  MCA Fault Diagnosisでは、エラーの種類を特定し、疑わしいエラーの原因を包括的に分析し、障害のあるコンポーネントを特定できます。一般的なプロセッサー障害の種類は次のとおりです。

  - キャッシュ修正不可能エラー(読み取りエラー、書き込みエラー、プリフェッチエラーなど)。
  - ウォッチドッグタイムアウトエラー(スリーストライクタイムアウトエラーなど)。
  - UPI訂正不能エラー。
  - CPU内部の電源制御モジュールエラー。
  - プロセッサークセスタイムアウト。

- メモリー障害検出。

  メモリー障害には、訂正可能なエラーと訂正不可能なエラーがあります。システム内の訂正不可能なメモリーエラーはサービスに重大な影響を与えます。MCA障害診断では、訂正不可能なエラーの検出と診断に重点が置かれます。MCA障害診断では、エラー記録モジュールによって記録されたメモリーエラーアドレスを分析し、障害のあるDIMMを特定し、特定のプロセッサー、チャネル、およびDIMMを特定します。一般的な訂正不可能なメモリーエラーのタイプは次のとおりです。

  - メモリーアクセスアドレスまたはメモリーアクセスコマンドが正しくありません。
  - メモリーの書き込みまたは読み取りエラーです。
  - メモリーキャッシュ制御エラー。
  - メモリータイムアウトエラーです。

- PCIe障害検出。

MCA障害診断では、エラー記録モジュールによって記録されたPCIeエラーアドレスを分析し、障害のあるPCIeモジュールを識別し、特定のプロセッサーとスロットを特定できます。PCIe障害の一般的なタイプは次のとおりです。

- サポートされていない要求(UR)。
- 形式が正しくないTLP。
- Completer Abort(CA)。
- 完了タイムアウト(CTO)。
- 毒されたTLP
- ACS違反。
- フロー制御プロトコルエラー。
- データリンクプロトコルエラー。
- サプライズダウンエラー。

MCA障害診断(AMDプロセッサーを搭載するサーバー用)

HDMは、OBISによって送信された関連するAMD MCAデータを受け入れ、データを解析して以下の情報を取得します。

- プロセッサー障害の検出:
  - 訂正不能および訂正可能なプロセッサーエラー。

    MCA障害診断では、特定のソケットのエラーを検出できます。
  - SMNレジスタ内のエラー。コールドシステム再起動をトリガーする可能性のあるエラーは、SMNレジスタに記録されます。

    MCA障害診断では、特定のソケットのエラーを検出できます。
- メモリー障害の検出:
  - ECCおよび非ECCメモリーエラー。

    MCA障害診断では、DIMM上のECCメモリーエラー、またはチャネル上の非ECCメモリーエラーを検出できます。
  - MEMトレーニングエラーとMEMテストエラー。

    MCA障害診断では、DIMMのエラーを特定できます。
- PCIe障害検出:PCIe訂正可能および訂正不能エラー。MCA障害

  診断では、スロット上のエラーを検出できます。

電源障害診断

SDSは、割り込みレポートおよびポーリングメカニズムを使用してパワーサプライを監視し、24のパワーサプライ障害タイプのうち11を識別できます。11の障害タイプには次のものがあります。

- パワーサプライがありません。
- 入力電圧障害(入力低電圧アラームおよび保護、入力なし、電源コードの接続不良など)
- PSUファンの障害。
- 過熱アラームと保護、および低温アラームと保護を含む、吸気口の温度異常。
- 過電圧アラームおよび保護、低電圧アラームおよび保護などの出力電圧の障害。
- 過電流アラームと保護を含む出力電流障害。
- 電源装置のLEDが1 Hzで点滅します。これは電源障害を示します。
- 異常なIICコミュニケーション。
- FRU情報が正しくない、H3C認定がないなど、EEPROM情報が正しくない。
- パワーサプライのモデルが一致しません。

- ロードバランシングが達成されていません。

システムボード障害診断

システムボードには、サーバーハードウェアオプションが組み込まれています。SDSは、以下のような70種類以上のシステムボード関連の障害を特定します。

- サーバーのセカンダリパワーサプライ(プロセッサーおよびその他のボード用のセカンダリパワーサプライを含む)の障害。
- ファンが存在せず、PWM速度制御に異常がある。
- シャーシ、プロセッサー、またはその他のボードの温度異常。
- 電圧または電流の異常

PCIe障害診断

SDSは、主にネットワークアダプターとライザーカードの障害を特定します。次のような40種類以上の障害を特定できます。

- ネットワークアダプター障害(H3C mLOMネットワークアダプターおよび25-GE FLOMネットワークアダプターでの電源障害または温度異常の欠如、およびネットワークアダプターの欠如など)。
- ライザーカードに異常がある。
- 異常なNCSIチャンネル変化。

ストレージコントローラーの障害診断

SDSは、ストレージコントローラーに関するイベントログを分析することによって、PMCおよびLSIストレージコントローラーの障害を識別および診断します。次のような100種類の障害を検出できます。

- ストレージコントローラーの起動障害。
- ケーブル接続障害。
- メモリー障害
- スーパーキャパシター故障。
- ドライブの障害。
- 電源障害保護モジュール障害。

障害報告

障害報告

HDMはハードウェアとシステムのステータスをリアルタイムで監視し、イベントログをSNMPトラップ、SMTP経由の電子メール、Redfishイベントサブスクリプション、またはsyslogメッセージを介してリモート接続先ホストに報告します。

SDS故障診断

ログエントリーをHDMから.sdsファイルにダウンロードし、ダウンロードした.sdsファイル内の診断ファイルを確認して、ハードウェア障害の詳細を取得できます。

予測アラーム

HDMは、プロセッサー、メモリー、ドライブ、ストレージコントローラー、ネットワークアダプター、電源などのコンポーネントに関するアラームをプロアクティブにレポートする機能をサポートしています。

- **プロセッサー**: 修正可能な構成エラー、過熱エラー、QPI/UPIバスエラー、およびDMAエラーに対する予測アラーム。
- **Memory**: 訂正可能なECCメモリーエラーに対する予測アラームです。

- **ドライブ**: 予測障害、メディアエラー、およびHDDとSSDのプリフェイルに対する予測アラーム、HDDのみの不良セクタに対する予測アラーム、および残りのSSDまたはNVMe寿命に対する予測アラームと監視。
- **ストレージコントローラー**: ネットワークアダプターのPCIeリンクの修正可能なバスエラーの検出と予測アラーム。
- **パワーサプライ**: 予測障害(予測障害、負荷の不均衡、修正時間制限を超える消費電力上限値、パワーサプライのセルフテストエラーを含む)に関する警告。
- **システムボード**: システムボード上の電圧および温度エラーの予測アラーム。

メンテナンス

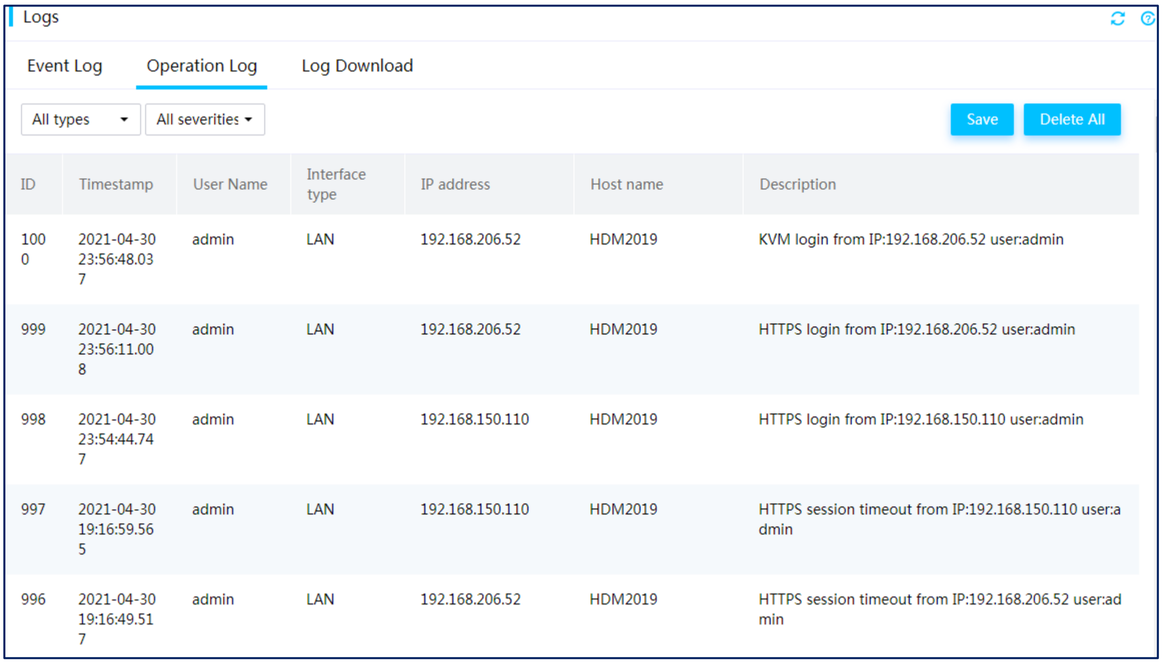
操作ログ

操作ログには、監査ログエントリー、ファームウェア更新ログエントリー、ハードウェア更新ログエントリー、および設定ログエントリーがあります。

- 監査ログエントリーには、セキュリティ監査用のHDM管理イベントが記録されます。
- ファームウェア更新ログエントリーには、HDMファームウェアの更新とその結果が記録されます。
- ハードウェア更新ログエントリーには、ハードウェア更新とその結果が記録されます。
- 設定ログエントリーには、ユーザー設定操作とその結果が記録されます。

ログエントリーには、タイムスタンプ、ホスト名、およびその他の詳細が含まれます(図13を参照)。イベントの重大度レベルには、InformationalとWarningがあります。

図13 操作ログページ



ID	Timestamp	User Name	Interface type	IP address	Host name	Description
1000	2021-04-30 23:56:48.037	admin	LAN	192.168.206.52	HDM2019	KVM login from IP:192.168.206.52 user:admin
999	2021-04-30 23:56:11.008	admin	LAN	192.168.206.52	HDM2019	HTTPS login from IP:192.168.206.52 user:admin
998	2021-04-30 23:54:44.747	admin	LAN	192.168.150.110	HDM2019	HTTPS login from IP:192.168.150.110 user:admin
997	2021-04-30 19:16:59.565	admin	LAN	192.168.150.110	HDM2019	HTTPS session timeout from IP:192.168.150.110 user:admin
996	2021-04-30 19:16:49.517	admin	LAN	192.168.206.52	HDM2019	HTTPS session timeout from IP:192.168.206.52 user:admin

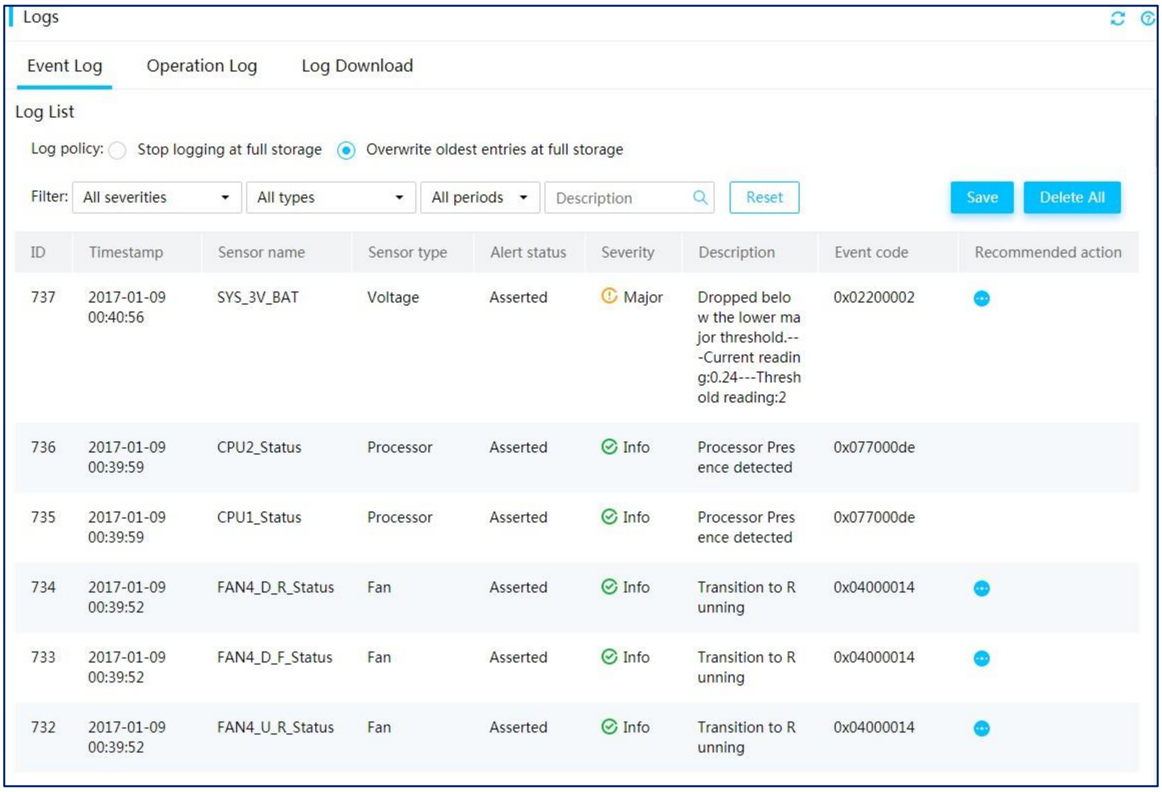
イベントログ

イベントログには、サーバーセンサーから報告されたイベントが記録されます。イベントの重大度レベルは次のとおりです。

- **Info**: イベントはシステムに悪影響を与えません。処置は必要ありません。情報イベントの例には、予期される状態変更イベントおよびアラーム削除イベントが含まれます。
- **Minor**: イベントによるシステムへの影響は軽微です。重大度の上昇を回避するには、迅速な対応が必要です。
- **Major**: このイベントによって、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。ただちに対処する必要があります。
- **Critical**: このイベントにより、システムの停止または電源障害が発生する可能性があります。直ちに対処する必要があります。

センサー名、重大度、およびログ生成時間によってイベントをフィルタリングできます。

図14 イベントログページ



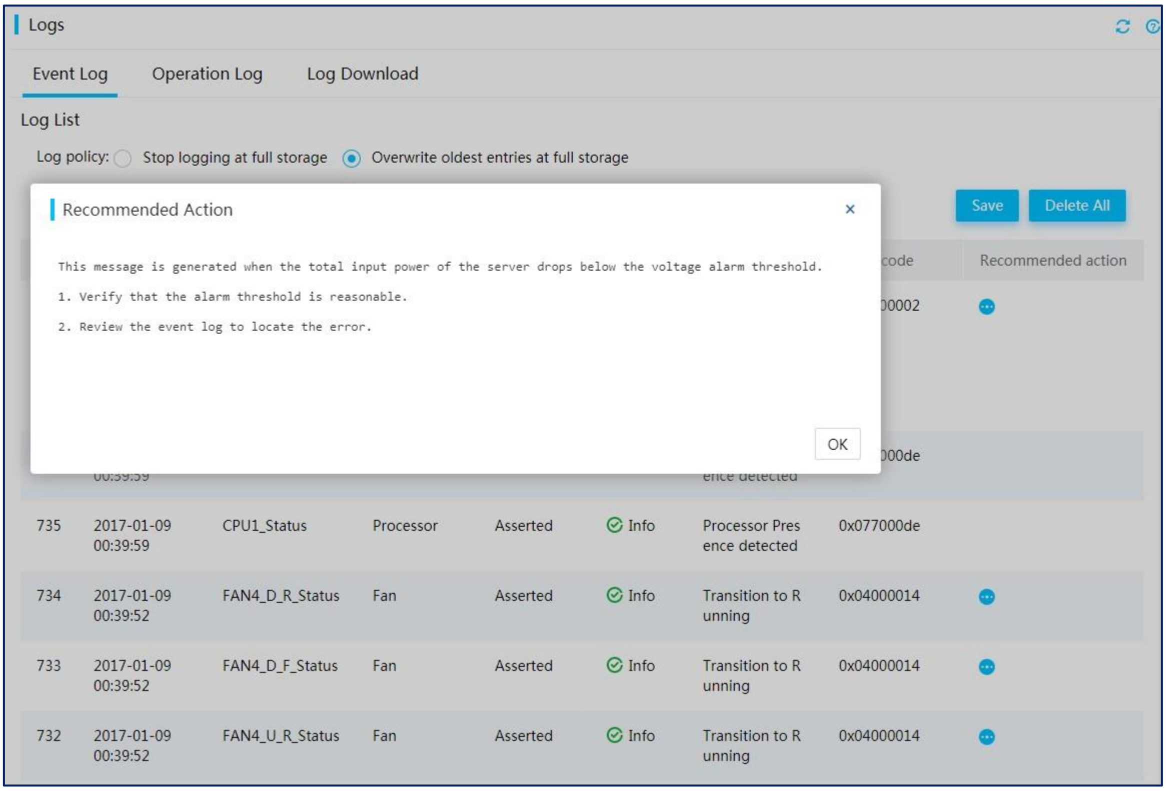
イベントコード

イベントコードは、HDM内の一意のイベントログエントリーを識別します。ユーザーは、イベントコードを通じてデバイスの障害タイプを見つけることができます。これにより、関連するログマニュアルで詳細を調べることができます。

推奨処置

HDM Webインターフェイスは、システムイベントに推奨されるアクションを提供します。これにより、ユーザーは関連する障害のトラブルシューティングの提案をすぐに取得できるため、障害の特定と修復が容易になります。

図15 推奨アクションの表示



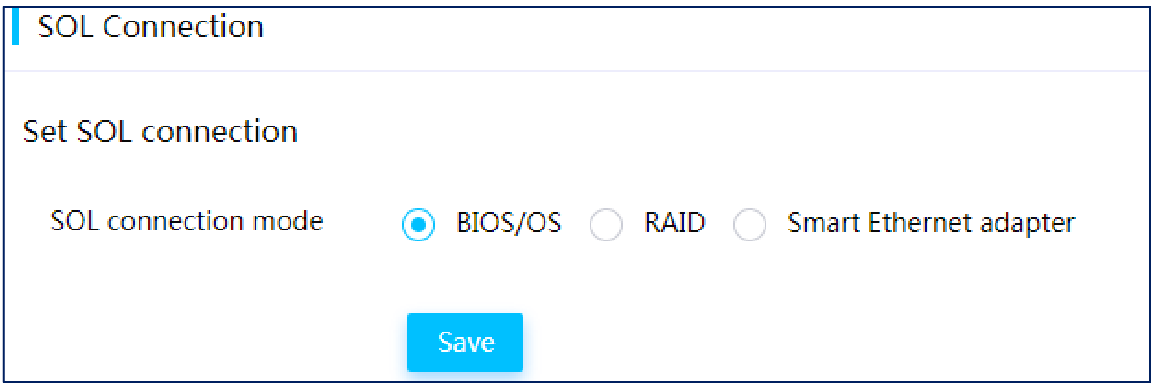
シリアルポート接続

HDMは、SOL機能が有効な場合に接続先のシリアルポートの選択をサポートします。SOL接続により、システムはサーバーパネル上のローカルシリアルポートから指定されたシリアルポートのリモートアクセスにアクセスをリダイレクトし、リモートネットワークデバイスの入力を受信できます。管理者は、ローカルデバイス上のシステムシリアルポート出力をリアルタイムで表示し、SOL接続モードをローカルで変更できます。

HDMからのSOL接続構成

BIOSまたはOSのシリアルポート、メザニンストレージコントローラー、またはスマートネットワークアダプターへの接続など、HDM WebインターフェイスでSOL接続モードを設定できます。

図16 SOL接続モードの設定



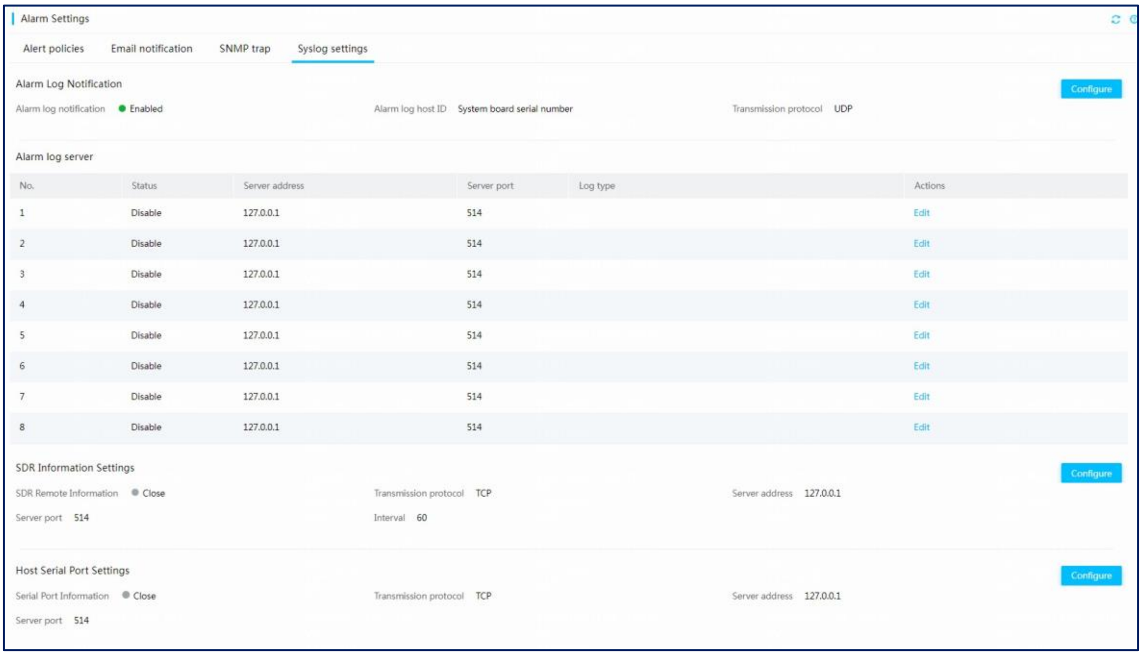
シリアルポート情報の記録

HDMは、システムシリアルポート出力のリアルタイム記録をサポートし、データを内部ストレージメディアに保存します。エラーが発生した場合は、分析のためにデータをローカルデバイスにダウンロードできます。

センサーデータレポート

HDMは、IPMIコマンドsdr elistからのシリアルポートデータおよびセンサーデータをsyslogサーバーに定期的に報告する機能をサポートしています。図17に示すように、SDR Information Settingsエリアからsyslogサーバーの IPアドレス、ポート番号、送信プロトコル、送信間隔を設定できます。

図17 Syslogサーバーの設定



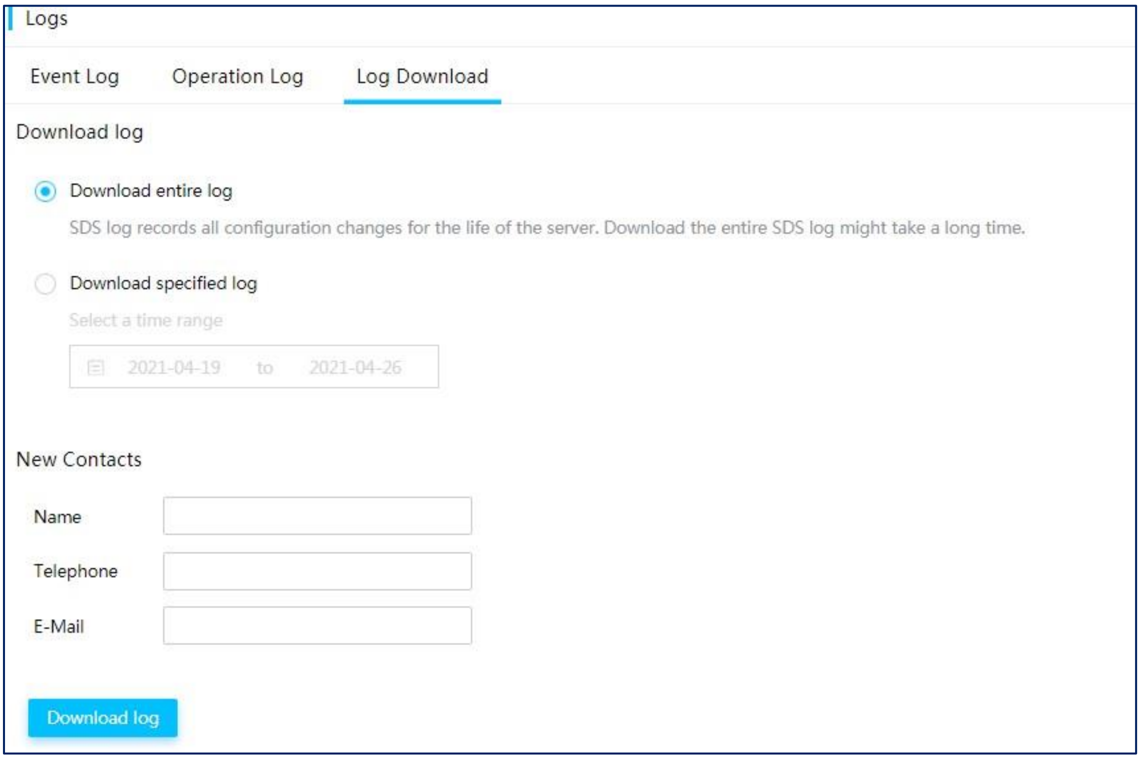
シリアルポートデータの監視

HDMでは、BIOSまたはOSシリアルポートに関するロギング情報をリモートのsyslogサーバーに送信してデータを監視することができます。syslogサーバーの構成方法については、図17のホストシリアルポート設定を参照してください。

ログのダウンロード

この機能を使用すると、イベントログエントリー、ハードウェア情報、およびSDS診断情報に関するレコードをサーバーのライフサイクル全体にわたってダウンロードできます。ダウンロードしたログを表示したり、ログ分析コンサルティング用の連絡先情報を追加したりできます。

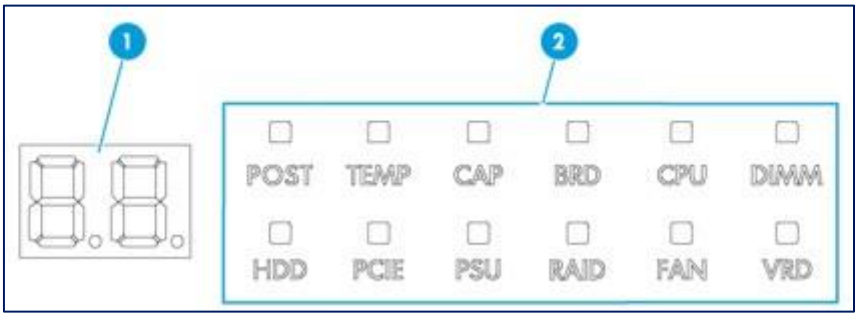
図18ダ ウンロードするログエントリーの指定



診断パネル

診断パネル(G3サーバーのみ)には、サーバーで発生した例外が表示されます。これらのコンポーネント障害は、HDMで生成されたイベントログと一致しています。

図19診断パネルの表示



診断パネルには、次の要素があります。

- **コンポーネントLED**: コンポーネントのステータスを示します。カラーオプションには次のものがあります。
  - **オレンジ/レッド**: コンポーネントでアラームが発生しました。
  - **緑色**: コンポーネントは正常に動作しています。
- **デジタル表示**: エラーコードを表示して、障害が発生したコンポーネントを示します。

  診断パネルには、一度に1つのコンポーネント障害のみが表示されます。複数のコンポーネント障害が存在する場合、診断パネルには、4秒間隔でこれらすべての障害が順番に表示されます。

コンポーネントLEDは、コンポーネントの障害を示すために使用できます。

- **POST**: POSTプロセスでエラーが発生し、表示されたフェーズで停止したことを示します。
- **TEMP**: コンポーネントの温度が上限しきい値を超えたか、下限しきい値を下回りました。
- **CAP**: システム消費電力が消費電力上限値を超えたことを示します。
- **BRD**: 対応するSMC、PDB、コンピュートモジュール、またはmLOMネットワークアダプターでエラーが発生したことを示します。
- **CPU**: プロセッサーでエラーが発生したことを示します。
- **DIMM**: DIMMでエラーが発生したことを示します。
- **HDD**: ドライブでエラーが発生したことを示します。
- **PCIe**: スロットのPCIeモジュールでエラーが発生したことを示します。
- **PSU**: パワーサプライでエラーが発生したことを示します。
- **RAID**: ストレージコントローラーでエラーが発生したことを示します。
- **FAN**: ファンモジュールでエラーが発生したことを示します。
- **VRD**: 対応するSMC、PDB、またはプロセッサーでパワーサプライエラーが発生したことを示します。

インテリジェントなセキュリティベゼル

インテリジェントセキュリティベゼルは、G5サーバーでのみ使用できます。

インテリジェントセキュリティベゼルの装飾LEDは、白、オレンジ、赤の3色で動作し、サーバーのヘルスステータスまたは電力負荷を示します。ユーザーは、装飾LEDからステータスまたは障害情報を直接取得できるため、オンサイト検査や障害の特定が容易になります。

図20 インテリジェントセキュリティベゼル

BSoDのスクリーンショット

この機能は、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、今後のトラブルシューティングのためにそのスクリーンショットをストレージスペースに保存します。HDMからBSoDスクリーンショットを表示できます。

HDMでは、最大10枚のBSoDスクリーンショットを指定した形式で保存できます。この機能を有効にする前に、KVMサービスがユーザーアカウントに対して有効になっていることを確認してください。

ビデオ再生

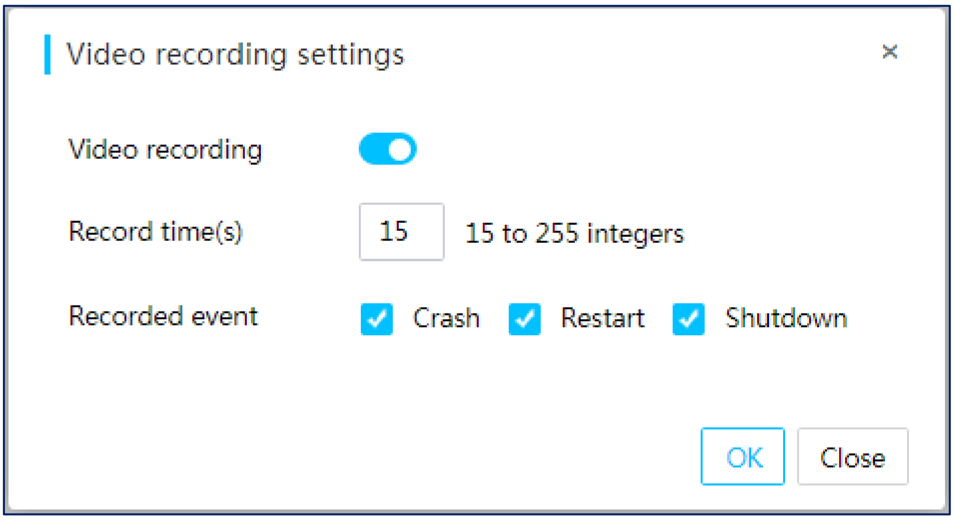
この機能を有効にすると、クラッシュ、再起動、シャットダウンなどの重大なOS例外が発生した場合、システムは例外の前に実行されたサーバー操作を記録します。これらのビデオを再生して、記録されたイ

ベントを分析またはトラブルシューティングできます。

HDMの動画再生ページでは、録画した動画の再生、ダウンロード、削除ができます。

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。この機能を有効にする前に、KVMサービスがユーザーアカウントに対して有効になっていることを確認してください。

図21 ビデオ再生設定の構成



アラートポリシー

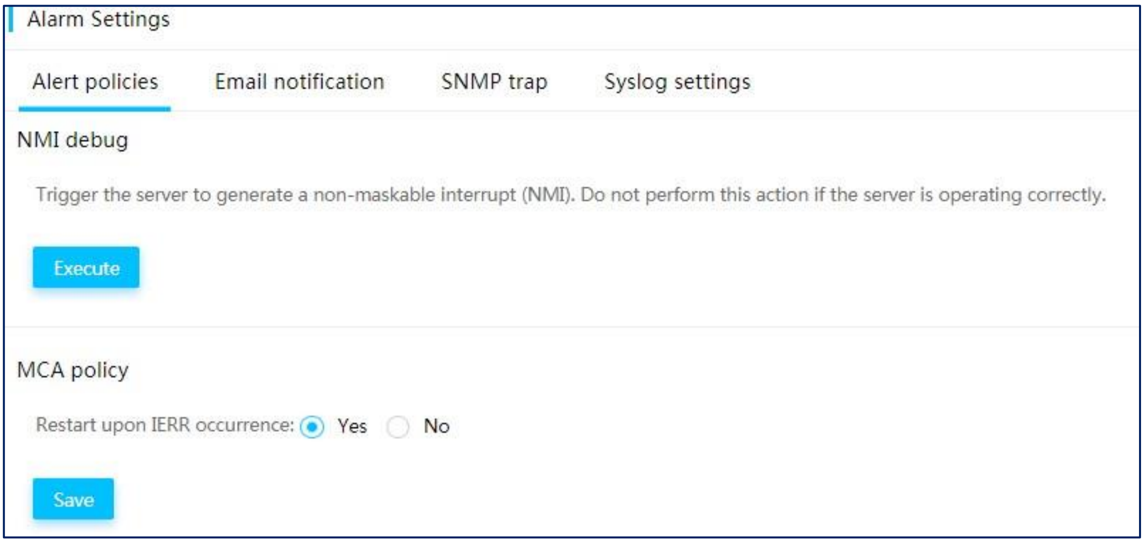
NMIデバッグ

マスク不可能割り込み(NMI)デバッグを使用すると、HDMはNMIをOSに送信してカーネルスタック情報を収集し、スタック情報を収集し、その情報をコンソールに送信してシステム例外を検出できます。

MCAポリシー

マシンチェックアーキテクチャ(MCA)を使用すると、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できます。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。

図22 NMIデバッグの有効化とMCAポリシーの設定

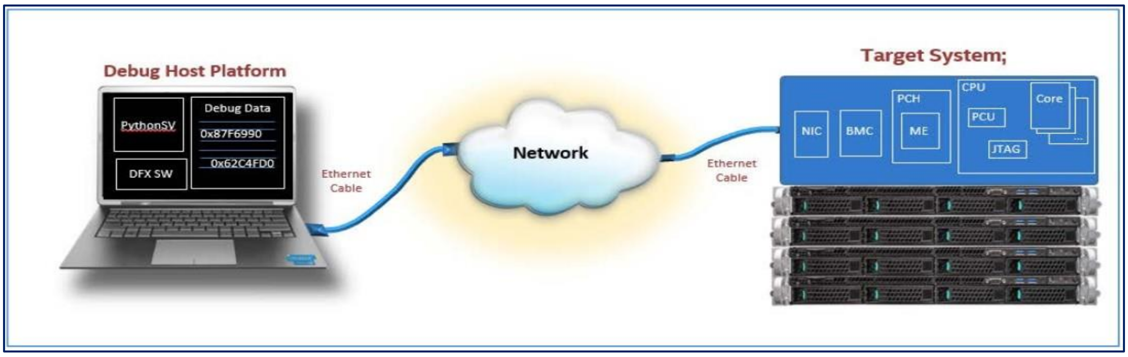


リモートXDP

ユーザーは、インテル固有のデバッガを購入したり、デバッガをターゲットサーバーに接続したりすることなく、インテルプロセッサー上でJTAGデバッグをリモートで実行できます。JTAGデバッグでは、プロセッサー、メモリー、PCIeモジュール、USBデバイスなどのサーバーコンポーネントに関するレジスタ情報を収集して、ハードウェアの問題を特定することができます。

この機能は、1つまたは2つのSkylake、Cooperlake、またはIceLake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できます。

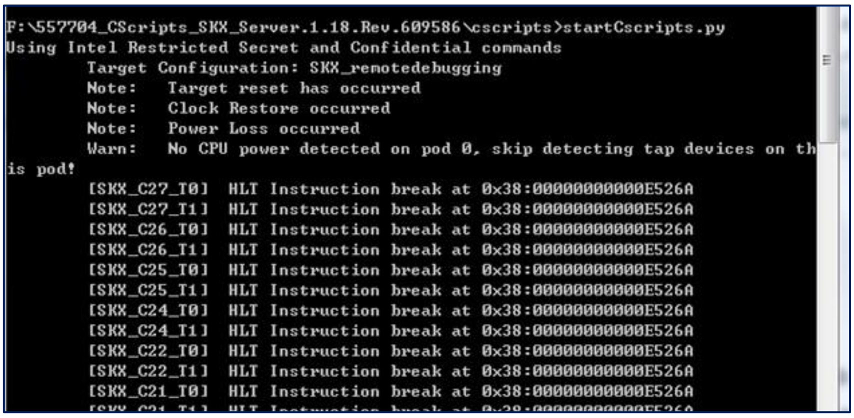
図23リモートXDP図



デバッグ環境を設定するには、次のタスクを実行します。

1. HDMからリモートXDPサービスを有効にします。
2. ローカルコンピュータにOpenIPCをインストールします。
3. Pythonをインストールし、Intelが提供するCscriptsをダウンロードします。
4. CMDを開き、図24に示すようにcscripts ディレクトリーでコマンドを実行します(図24を参照)。

図24 CMD内のコマンドの実行



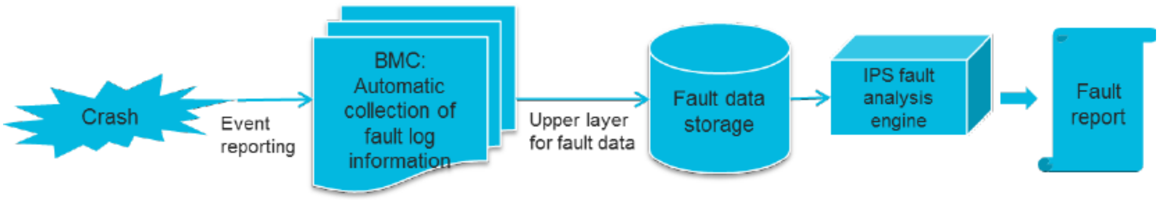
```
F:\557704_CScripts_SKX_Server.1.18.Rev.609586\cscripts>startCscripts.py
Using Intel Restricted Secret and Confidential commands
        Target Configuration: SKX_remotedebugging
        Note:   Target reset has occurred
        Note:   Clock Restore occurred
        Note:   Power Loss occurred
        Warn:   No CPU power detected on pod 0, skip detecting tap devices on th
is pod!
        [SKX_C27_T0]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C27_T1]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C26_T0]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C26_T1]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C25_T0]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C25_T1]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C24_T0]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C24_T1]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C22_T0]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C22_T1]  HLT Instruction break at 0x38:00000000000E526A
        [SKX_C21_T0]  HLT Instruction break at 0x38:00000000000E526A
```

ACD

HDMには、Intelプロセッサーを搭載したサーバー用のIntel Autonomous Crash-Dump(ACD)機能が統合されています。MCAエラーが発生すると、ACDはMCAおよびプロセッサー関連のレジスタ情報(プロセッサー、メモリー、PCIeの障害に関する情報など)をアウトオブバンド方式で収集します。次に、ACDはCScripts分析用にJSON形式で情報を保存します。これにより、Intelプラットフォーム用のMCAエラーを検出する機能が強化されます。

HDMは、IPMIインターフェイスを介したACDの有効化をサポートしています。

図25 Intel ACDメカニズム

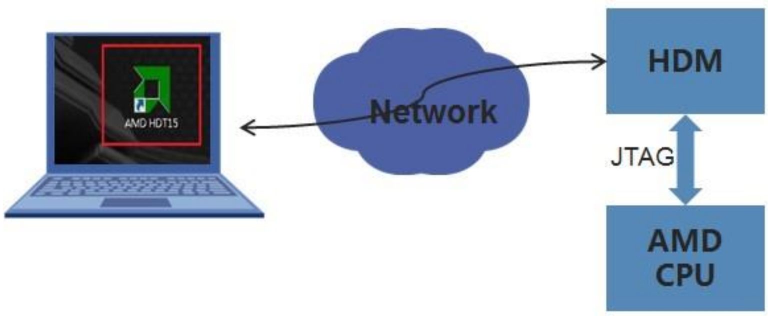


iHDT

iHDTサービスは、AMDによって提供されるハードウェアデバッグツール(HDT)を介してアウトオブバンド方式でAMDプロセッサーに対してリモートでJTAGデバッグを実行し、プロセッサー、メモリー、およびPCIe情報を収集する。

iHDTサービスは、G5 AMDサーバーで使用できます。iHDTサービスを使用する前に、HDMから有効にしてください。

図26 iHDTメカニズム



サービス用USBデバイス

G5サーバーのシャーシ耳は、HDMに直接接続されたUSB Type-Cコネクターと統合されています。Type-Cコネクターに接続されたUSBデバイスは、サービスUSBデバイスとして動作できます。HDMによって、Type-Cコネクターに接続されたUSBデバイスが識別され、ログのダウンロードにそのUSBデバイスを使用するかどうかが決定されます。

サービスUSBデバイスとは、USB診断ツールのイメージファイルに焼き付けられたUSBデバイスのことで、Unitoolを使ってサービスUSBデバイスを作ることができます。

図27 G5サーバーのUSB Type-Cコネクター

HDMタスクステータスクエリ

HDMは、ファームウェアの更新、SDSログのダウンロード、MCA収集、KVMイメージのマウント、構成のインポートとエクスポートなど、バックエンドBMCタスクのステータスの照会をサポートしています。次のタスク情報を使用できます。

- タスクタイプ。
- タスクの簡単な説明。
- タスクが開始されていない、処理中である、または完了したことを示すタスクステータス。
- 設定が有効になるトリガー条件(BMCリセット、システムウォームリセット、システム電源オフなど)。
- タスク処理時間の見積もり。

サーバー管理

FRUと資産管理

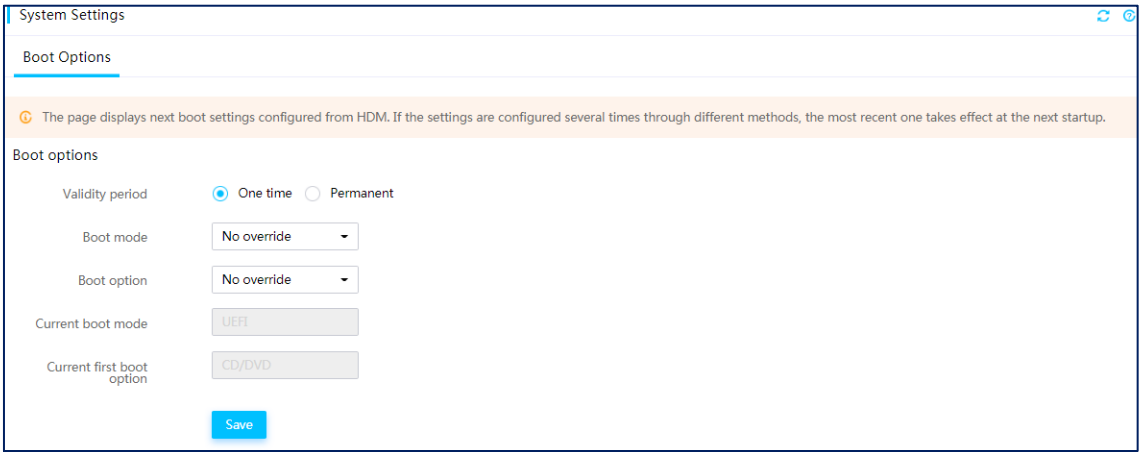
FRU情報には、現場交換可能ユニットに関するハードウェアでコード化された工場情報が含まれています。

資産管理の中核となるのは、サーバーコンポーネントの一意の製品コードを取得することです。H3C製品の場合、HDMはFRUから製品コードを取得できます。サードパーティ製品の場合、HDMはBIOSまたはアウトオブバンド方式から製品コードを取得できます。

システムブートオプション

ブートオプションでは、ワンタイムブートモード、次回の再起動時にサーバーが使用するブートデバイス設定、次回のブートモードとオプションの有効期間を指定します。

図28システムブートオプションの設定



ファン管理

HDMは、MSアルゴリズムとPID制御アルゴリズムの両方を使用したファン速度の調整をサポートしています。PID制御アルゴリズムの方がより正確です。

MSアルゴリズム

図29に示すように、ディレクトリーでMSアルゴリズムを使用して、.xml設定ファイル内の異なる温度におけるファン速度を指定できます。

図29 設定ファイルでのファン速度の指定

```
<algorithm1>
    <enable>true</enable>
    <type>ms</type>
    <args>
        <10>80</10>          //10°
        <20>80</20>          //20°
        <25>95</25>          //25°
        <27>100</27>         //27°
        <28>110</28>         //28°
        <30>120</30>
        <35>170</35>
        <40>230</40>
        <45>255</45>
        <128>255</128>
    </args>
    <setp>40</setp>
    <limit>
        <low>16</low>
        <high>255</high>
    </limit>
/algorithm1>
```

PIDアルゴリズム

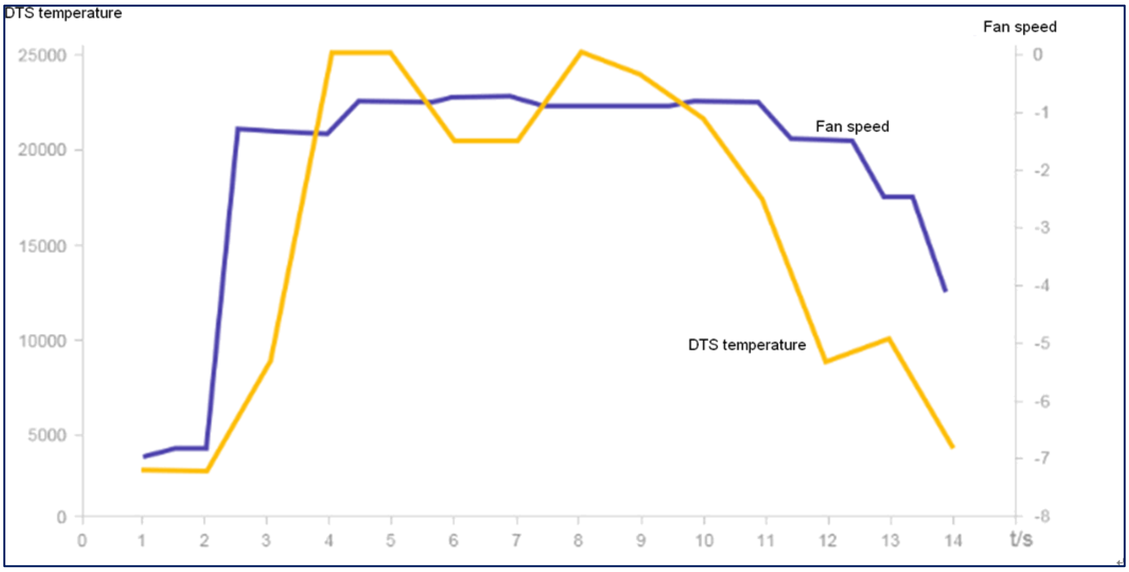
PIDアルゴリズムは、.xml設定ファイル内のセンサー速度パラメータとセンサー温度測定値を使用して、最適化されたファン速度をリアルタイムで計算し、ファン速度をより正確に調整できるアルゴリズムであり、図30に示すように動作する。

図30 PID制御アルゴリズム

$$\mathrm{u(t)} = \mathrm{kP}\left(\mathrm{e(t)} + \frac{1}{\mathrm{TI}\int e(t)dt} + \mathrm{TD} * \frac{\mathrm{de(t)}}{\mathrm{dt}}\right)$$

PIDアルゴリズムによるファン速度調整のシミュレーション図を図37に示すが、DTS温度が増減するとファン速度も増減する。

図31 PIDアルゴリズムによるファン速度調整



ファン速度モード

必要に応じて、次のファン速度モードのいずれかを選択できます。

- **Silent**: サーバーの放熱に必要な最低速度でファンを動作させることができます。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、バランスのとれた騒音制御と冷却性能を提供します。
- **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パフォーマンスを必要とするシナリオに適しています。たとえば、サーバーがビジー状態で、プロセッサーなどの主要コンポーネント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。
- **Custom**: カスタマイズしたファン速度レベルを1～20の範囲で指定します。レベルが高いほど、速度が速く、ノイズが大きいことを表します。

DCPMMs

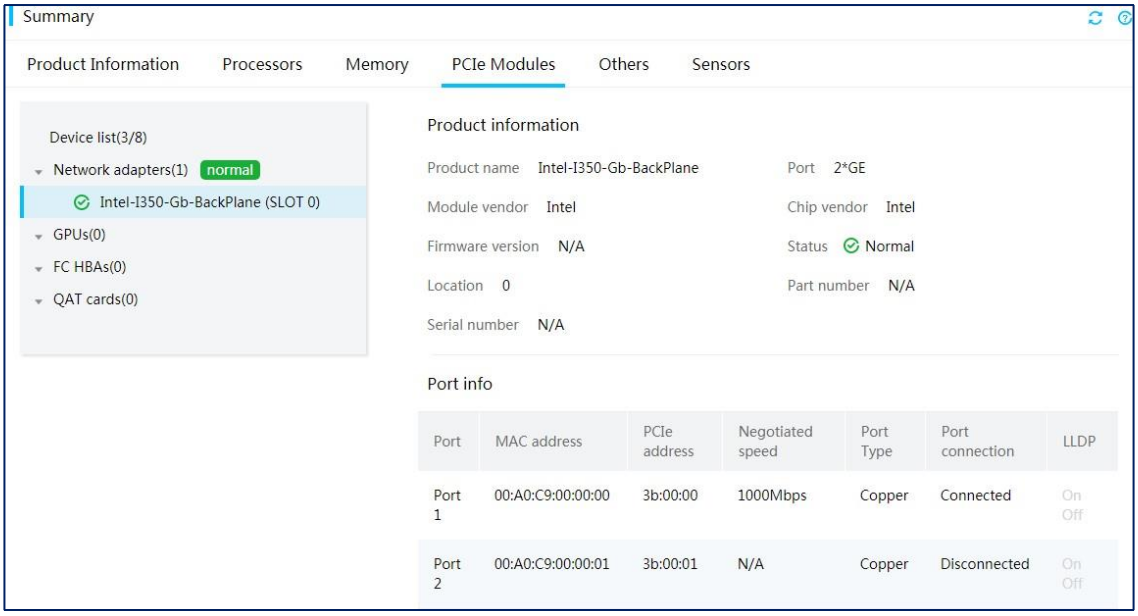
Intel Optane Data Center Persistent Memory Module(DCPMM)は、新しいタイプの不揮発性メモリーデバイスです。

HDMは、DCPMMコントローラのファームウェアバージョン、DCPMMの温度、DCPMMコントローラの温度、残りのDCPMM寿命、DCPMMの総パワーオン時間、揮発性システムメモリーとしてのDCPMMの能力、および永続メモリーとしてのDCPMMの能力を含む、BIOSおよびMCTP over MEを介してDCPMMsに関する情報を提示することができる。

ネットワークアダプター

HDMは、MCTP上でNCSIをサポートするPCIeネットワークアダプターおよびOCPネットワークアダプターの帯域外管理をサポートします。HDMから、MACアドレス、ポートタイプ、接続ステータス、ネゴシエート速度などのネットワークポート情報を取得できます。

図32 ネットワークアダプター情報の表示



FC HBA

HDMは、MCTP over PCIeを介したFC HBAの帯域外管理をサポートします。HDMから、WWN、温度、ヘルスステータス、リンクステータス、速度などのFC HBA情報を取得できます。

Lpe31002、Lpe31000、Lpe32002、およびLpe32000 FC HBAのみがサポートされています。

GPUモジュール

HDMはGPUモジュールの帯域外管理をサポートしています。メモリー容量、GPUモジュールコア、定格電力、製品名、ベンダー名、ベンダーID、ファームウェアバージョン、内蔵GPUモジュール数、内蔵GPUモジュールの温度センサー読み取り値などのGPUモジュール情報をHDMから取得できます。

NVIDIA GPUモジュール、Cambricon GPUモジュール、および一部のEnflame GPUモジュールのみがサポートされています。

利用可能なGPUモジュール情報は、GPUモジュールモデルによって異なります。

ハードパーティション化

H3C UniServer R8900 G3では、ハードパーティショニングがサポートされています。この機能により、8プロセッサーサーバーは、デュアルシステムパーティショニングモードで2台の4プロセッサーサーバーとして動作することができます。2台の4プロセッサーサーバーはハードウェアにおいて互いに独立しており、独自のBIOSを持ち、異なるプロセッサーやOSをインストールすることができます。サーバーは次のようにリソースを利用できます:

- 各4プロセッサーサーバーには、独自のプロセッサー、メモリー、ドライブ、ファン、ライザーカードがあります。各4プロセッサーサーバーのファンは、N+1冗長性をサポートしています。各サーバーには独自のHDMがあり、HDMを個別に更新できます。
- 2台の4プロセッサーサーバーは、電源装置とミッドプレーンを共有します。

Smartネットワークアダプター

HDMは、次の観点からスマートネットワークアダプターの帯域外管理をサポートします。

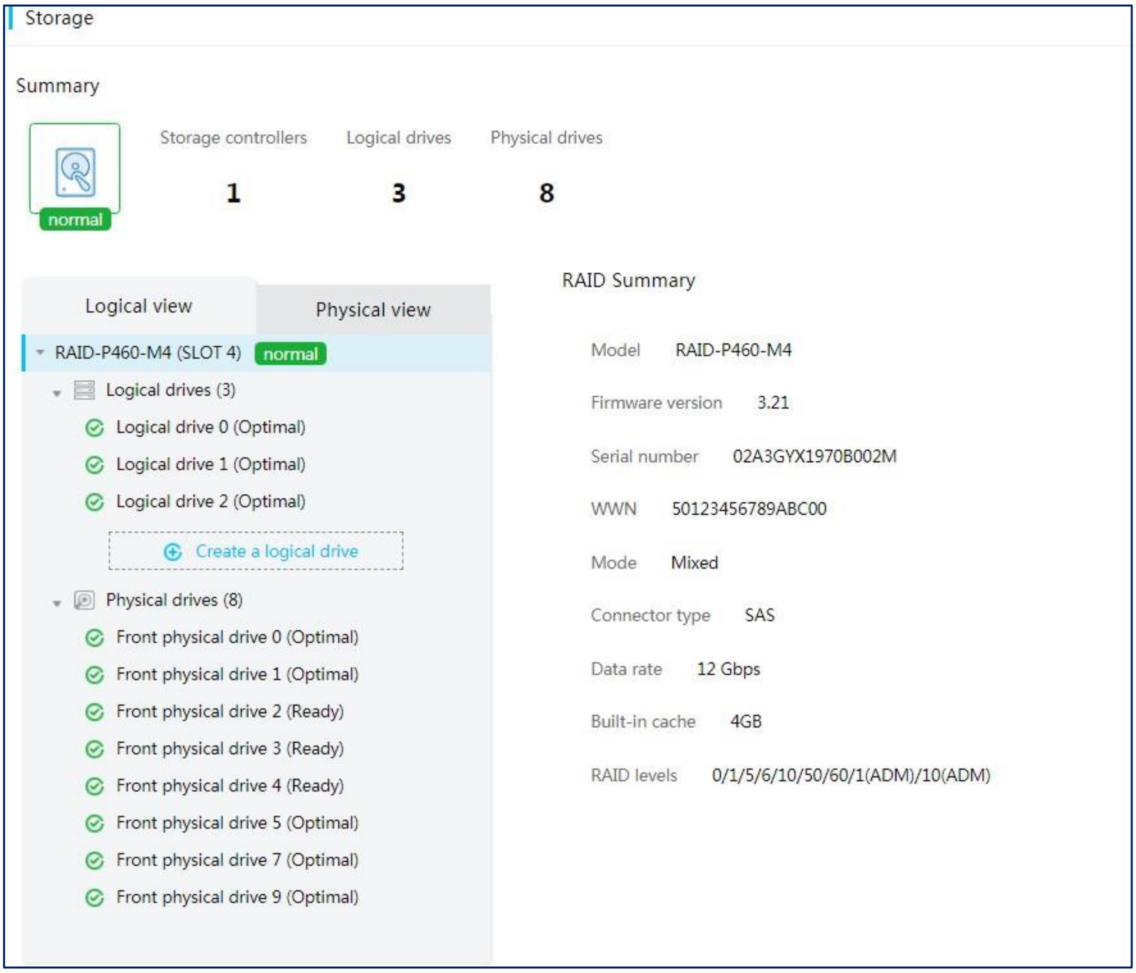
- センサーデータを表示して、ネットワークアダプターの電圧、電流、および電力を監視します。
- FRU書き込み保護ステータス、ネットワークアダプターID、BOM ID、PCB ID、ベンダーID、デバイスIDなど、HDMからスマートネットワークアダプター情報を提供します。
- スマートネットワークアダプターでのFRU書き込みおよび読み取り操作をサポートします。
- ネットワークアダプターの電源オン/オフ、ネットワークアダプターコントローラのリセット、FPGAのリセット、FRU書き込み保護の有効化ステータスなど、スマートネットワークアダプターの設定をサポートします。

ストレージ管理

ストレージコントローラーの管理

HDMでは、ストレージコントローラーの数、ストレージコントローラーモデル、ベンダー、ファームウェアバージョン、コネクタタイプ、データレート、シリアル番号、キャッシュ容量、モード、サポートされているRAIDレベルなどのストレージコントローラー情報を取得できます。

図33 ストレージコントローラー情報の表示



論理ドライブ管理

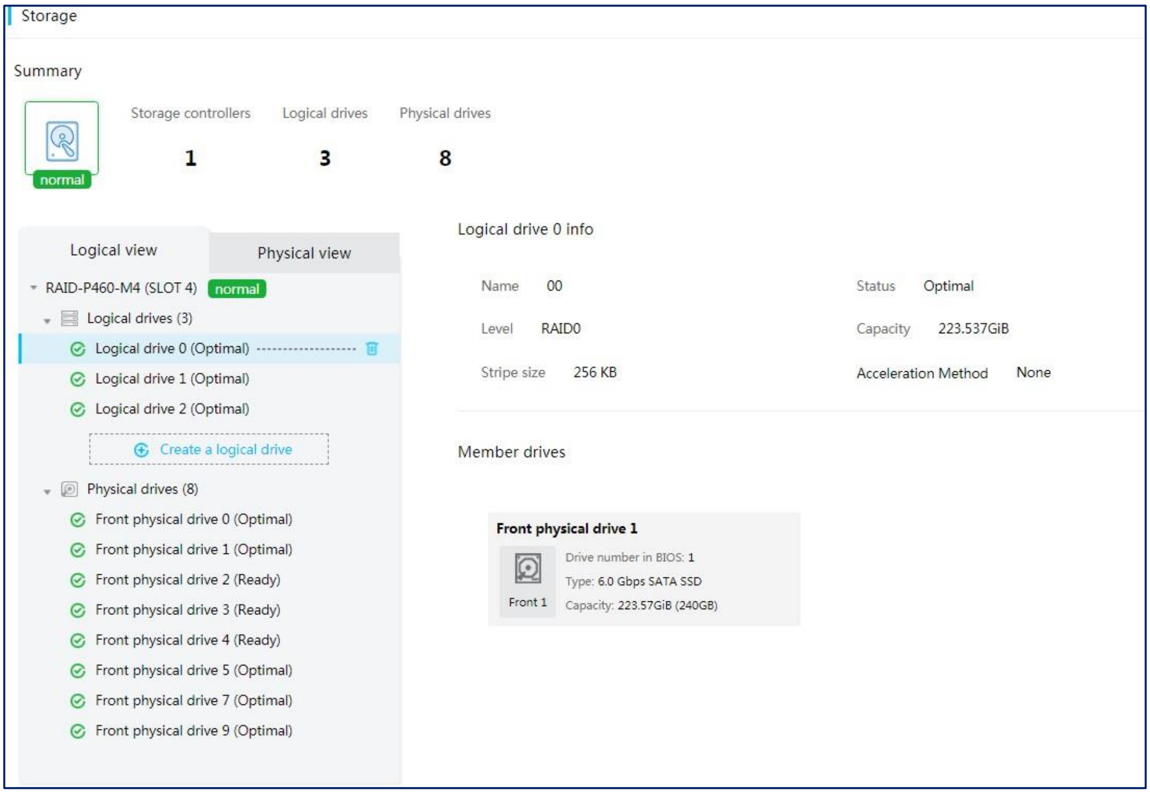
HDMは、次のストレージコントローラー用の論理ドライブの作成をサポートしています。

- 9300、9311、および9400シリーズのストレージコントローラーを除くLSIストレージコントローラー。
- MCTP over PCIeをサポートするP460およびH460シリーズPMCストレージコントローラー。

RAIDアウトオブバンド管理のサポートは、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によって異なります。

LSIストレージコントローラー(9300、9311、および9400シリーズのLSIストレージコントローラーを除く)に接続されている論理ドライブの読み取りまたは書き込みポリシーを変更できます。

図34 論理ドライブの管理



物理ドライブの管理

HDMでは、物理ドライブ情報(スロット番号、ドライブモデル、シリアル番号、ドライブステータス、ドライブ容量、インターフェイス速度、インターフェイスタイプ、ドライブタイプ、残りのドライブ寿命(LSIストレージコントローラーのみ)など)を取得できます。

LSIストレージコントローラー(9300、9311、および9400シリーズのLSIストレージコントローラーを除く)に接続されている物理ドライブの状態を、未構成良好、未構成不良、またはJBOD状態に変更できます。

ドライブのUID LEDを有効にすると、ドライブの位置を確認できます。

図35 物理ドライブの管理(論理ビュー)

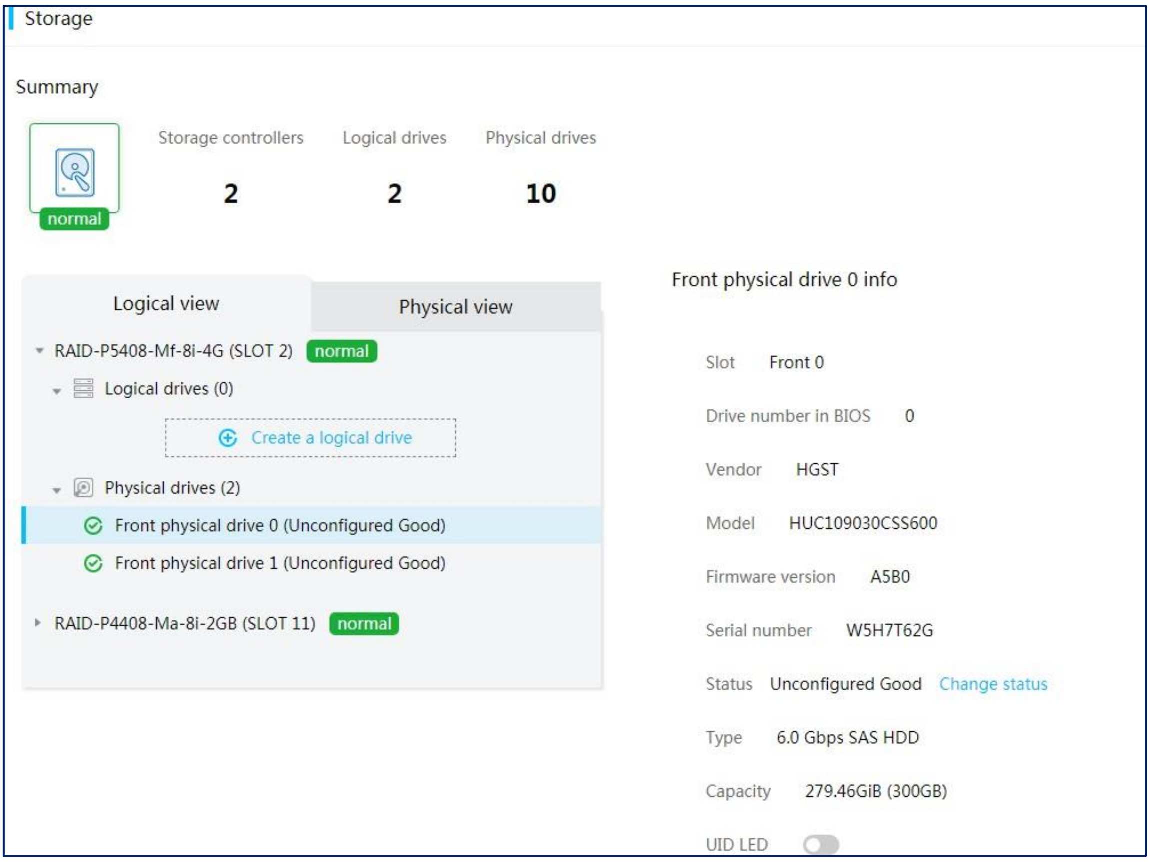
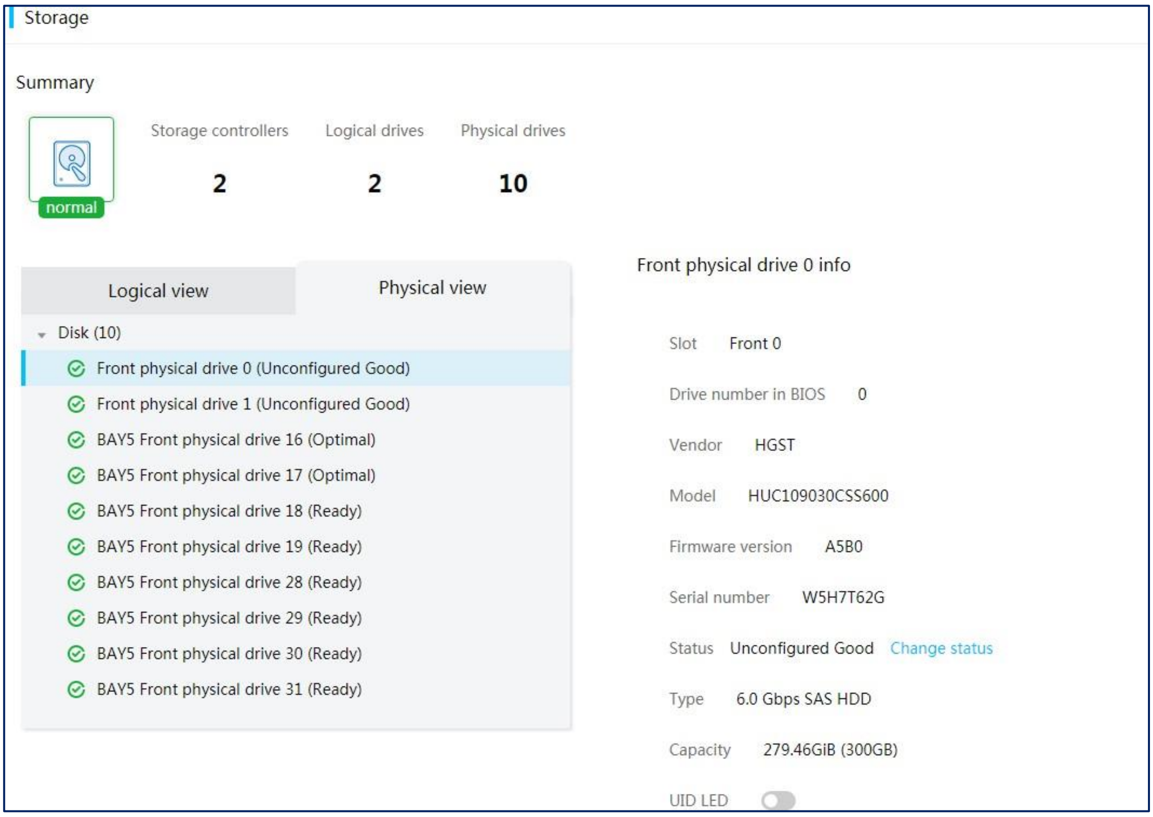


図36 物理ドライブの管理(物理ビュー)



ストレージのメンテナンス

アラーム

HDMは、ドライブの存在、ドライブ障害、予測障害、重大なアレイエラー、ストレージコントローラーエラーなど、複数のタイプの障害に関するアラームを報告できます。検出および報告できる障害は、コンポーネントタイプによって異なります。

- **HDDドライブ**: ドライブ障害、予測障害、ドライブメディアエラー、プリフェイル、訂正不能エラー、不良セクタ、およびドライブ不足ステータスの監視とアラーム。
- **SSDドライブ**: ドライブ障害、予測障害、ドライブメディアエラー、プリフェイル、訂正不能エラー、ドライブ不足ステータスの監視と警告、およびSSDの残り寿命と残り予約ブロックに関するデータ収集と警告。
- **NVMeドライブ**: NVMeの残りの寿命を監視およびアラームで知らせます。
- **ストレージコントローラー**: ストレージコントローラー障害およびRAID再構築障害。
- **スーパーキャパシター**: スーパーキャパシターの障害、予測障害(低電圧)、およびスーパーキャパシターの欠如。

SDSログと診断

SDSログ

HDMは、PBSIチャネルを介してPMCストレージコントローラーに関する情報を取得し、その情報をSDSログに記録できます。SDSログには、60種類以上のドライブ障害を記録できます。

I2Cトランスポートバインディングを介したMCTPによって取得されたSDSログには、LSIストレージコントローラーに関するログメッセージが含まれています。SDSは、RAIDコントローラ、スーパーキャパシター、ドライブ、論理ドライブ、およびドライブバックプレーンに関する200以上のログメッセージを記録できます。

SHD診断

SHD SDSは、PMC RAIDまたはHBAコントローラおよびLSI RAIDまたはHBAコントローラに関するログメッセージに基づいて障害理由を識別でき、対応するソリューションを提供します。SDSは、RAIDコントローラ、ケーブル、スーパーキャパシターおよび記憶媒体でサポートされています。SDSには、障害診断用の100エントリが用意されています。

SMART情報

HDMでは、SAS/SATA HDDドライブに関するSMART情報を取得できます。この情報は30日間保存でき、1日1回取得できます。

サポートされているLSIストレージコントローラーには、9361、9460、9440、9560、L460、RAID-P5408-Mf、RAID-P5408-Ma、およびHBA-H5408-Mfシリーズのストレージコントローラーがあります。

ログダウンロードは、HDMからSMART情報を取得するために使用されます。

ストレージコントローラーのシリアルポートログ

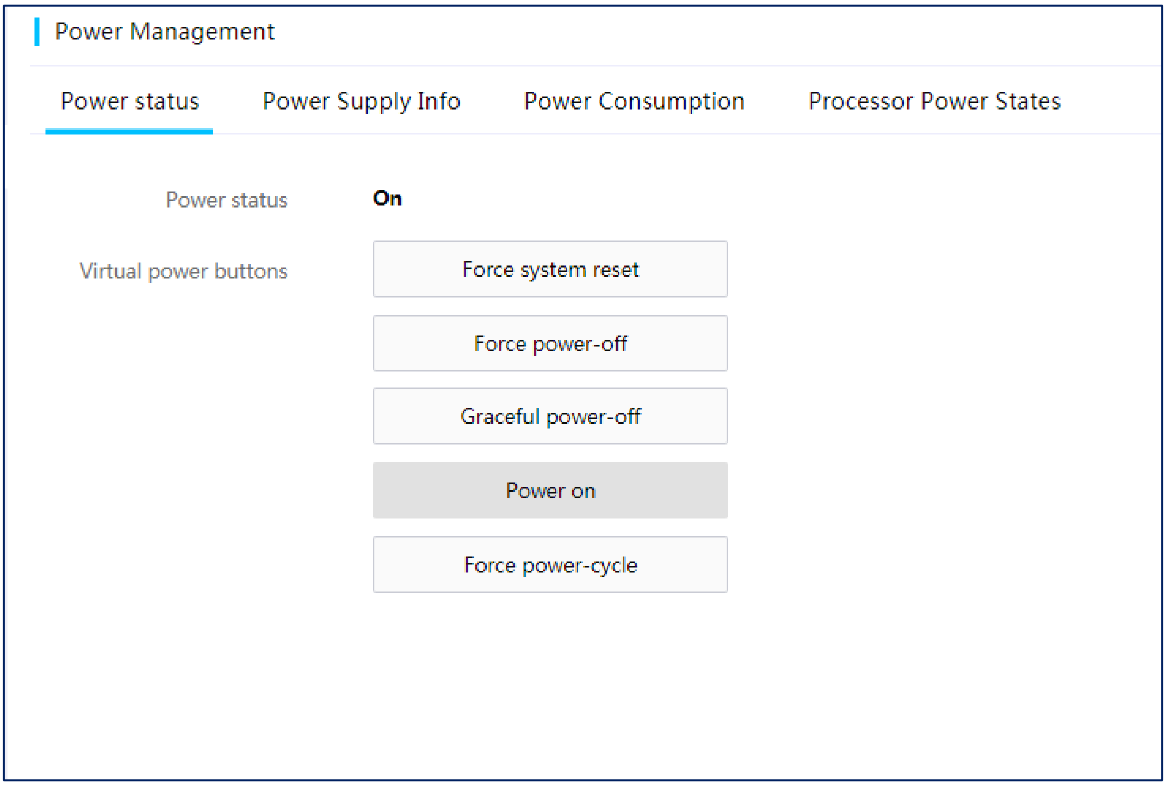
HDMは、メザニンRAIDコントローラおよびLSIストレージコントローラー(9300、9311、および9400シリーズLSIストレージコントローラーを除く)のシリアルポートログを取得できます。

Smart電源管理

電源ステータスの設定

図37に示すように、サーバーの電源ステータスをリモートで表示および変更できます。

図37 電源ステータスページ



サーバーの電源ステータスを制御するには、次のいずれかのオプションを選択できます。

- **Force System Reset**: サーバーのコールドリセットを実行します。HDMは、OSをシャットダウンせずにPCHを介してサーバーを直接リセットします。
- **Force power-off:** OSからの応答を待たずにサーバーの電源をオフにします。この動作は、サーバーの電源ボタンを押したままにした場合と同じです。
- **Graceful Power Off**: サーバーの電源をオフにします。HDMはOSにACPI割り込みを送信します。OSがACPI割り込みをサポートしている場合、HDMは実行中のすべてのプロセスを停止してOSをシャットダウンし、その後サーバーの電源をオフにします。OSがACPI割り込みをサポートしていない場合、HDMはグレースフル電源オフタイマーが満了した後にサーバーの電源を強制的にオフにします。この操作は、サーバーの電源ボタンを押してスタンバイモードにする操作と同じです。
- **Power On**: サーバーを起動します。
- **Force Power Cycle**: サーバーの電源をいったん切ってから入れ直します。

消費電力上限の設定

通常、従来のデータセンターでサービスの継続性を確保するには、過剰な電力供給が必要です。HDMは、各サーバーの電力消費を正確に制御するための消費電力上限を提供し、電力を節約し、過剰な電力供給の需要を排除します。

消費電力上限が設定されている場合、システム電力が消費電力上限値を超えると、電力が適切に分配されるように特定のアクションがトリガーされます。

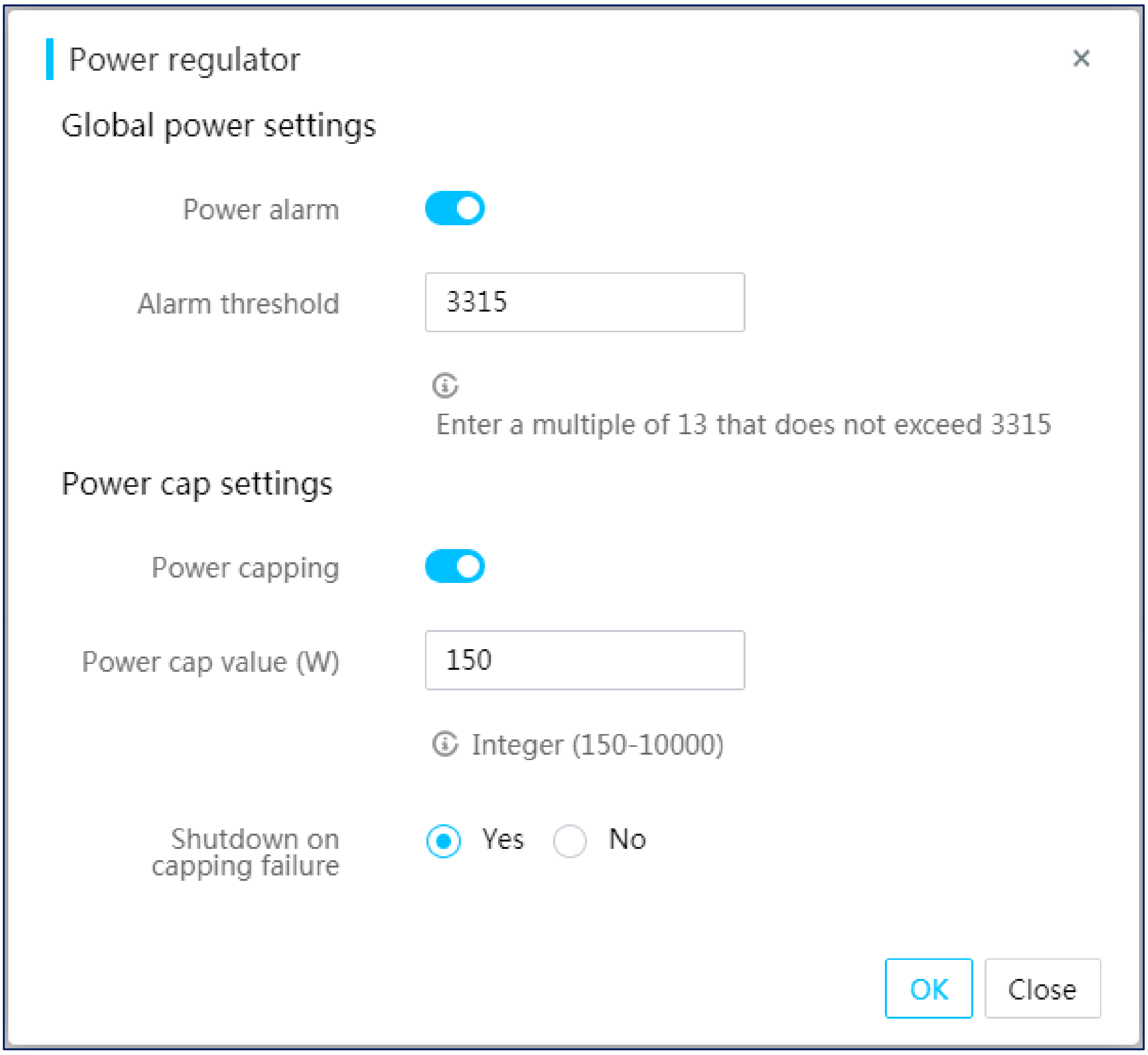
消費電力上限に失敗した場合は、次の操作が実行されます。

- **Event Logging**: デフォルトでは、消費電力上限の障害に関する情報をシステムイベントログファイルに記録します。
- **Shutdown on capping failur**e: 消費電力上限障害時にサーバーをシャットダウンします。

この操作はオプションです。

HDMは、インテルおよびAMDプロセッサーの消費電力上限をサポートしています。

図38 消費電力上限の設定



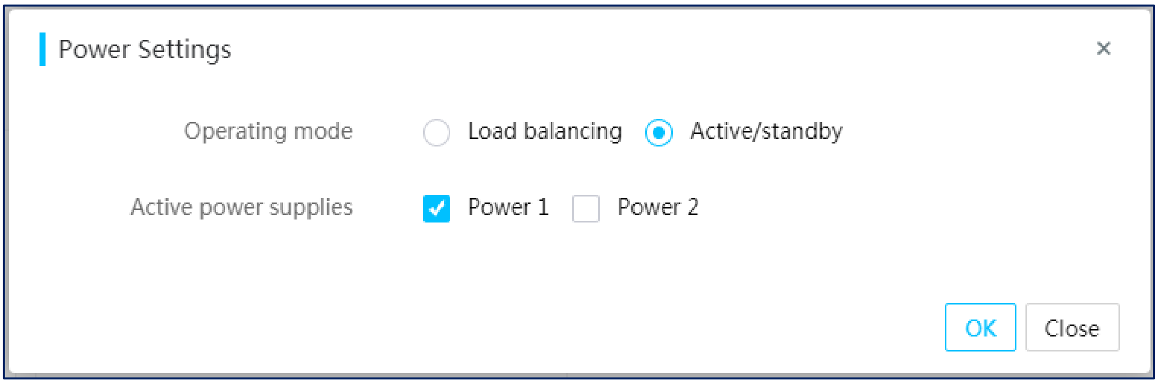
電源装置の動作モードの設定

本システムは,一部の電源をホットスタンバイ状態にすることにより,電力変換効率を改善できる。

電源装置の動作モードはHDMから設定できます。以下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よく電力を供給できるようにします。
- **Active/Standby**: アクティブパワーサプライが主に電力を供給できるようにします。このモードでは、最低1つのアクティブパワーサプライと最低1つのスタンバイパワーサプライを指定する必要があります。アクティブパワーサプライが故障すると、スタンバイパワーサプライがアクティブになって電力を供給します。アクティブパワーサプライの実際の消費電力が最大定格消費電力の62%を超えると、スタンバイパワーサプライがアクティブになって電力を供給します。

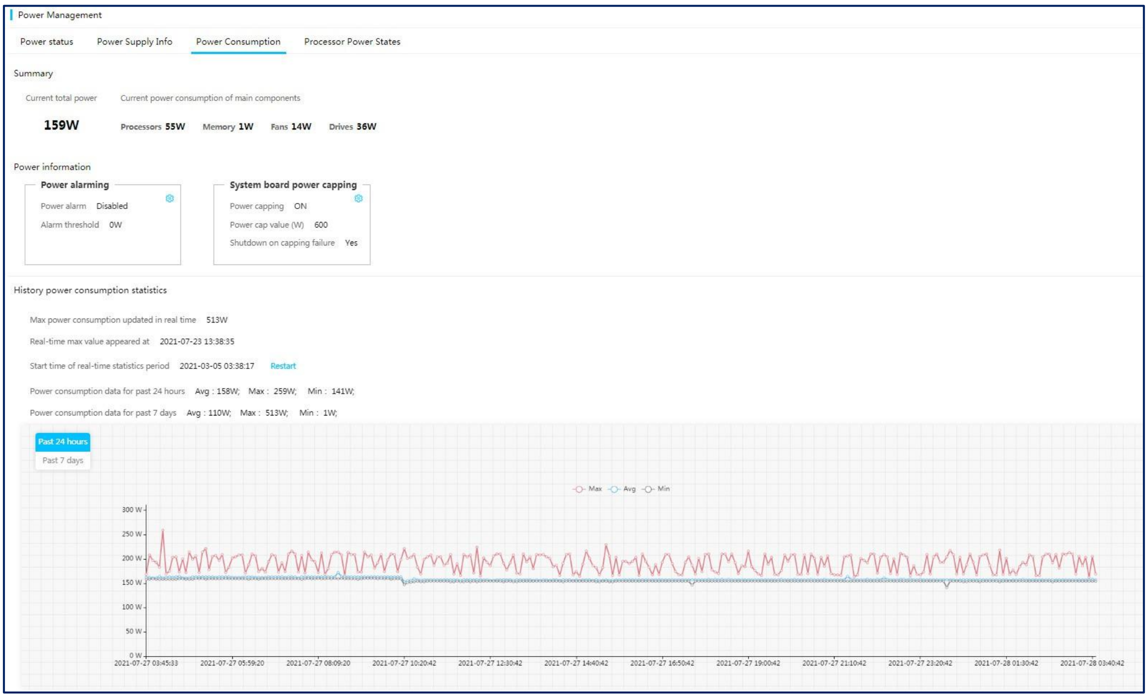
図39パワーサプライ動作モードの設定



電力消費履歴統計の表示

HDMは、サーバーの消費電力履歴の統計情報とグラフを表示します。これにより、消費電力と放熱状態を把握できます。消費電力履歴データに基づいて消費電力を調整できます。

図40 電力消費履歴統計の表示

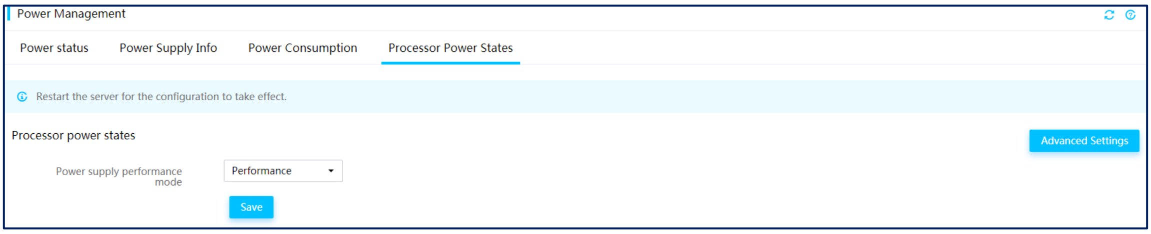


パワーサプライのパフォーマンスモードの設定

さまざまなサーバーパフォーマンス、消費電力、およびノイズの要件を満たすために、パワーサプライに対して次のいずれかのパフォーマンスモードを選択できます。

- **Performance**: パフォーマンス優先モードを示します。
- **Balanced Performance。**
- **Balanced Power。**
- **Power**: 省電力モードを示します。

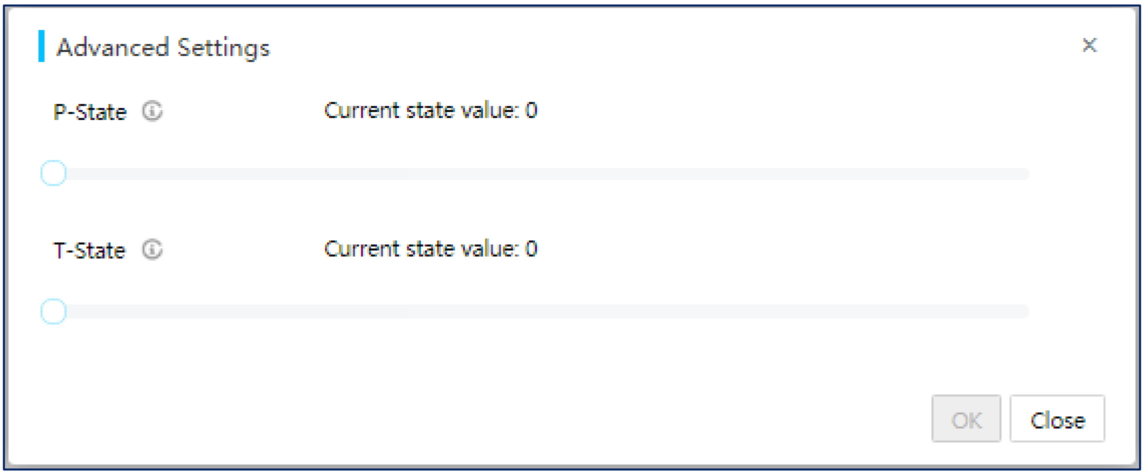
図41 動作モードの選択



プロセッサーの電源状態の設定

優先Pステートまたは優先Tステート値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。

図42プロセッサーの電源状態の設定



自動電源投入の設定

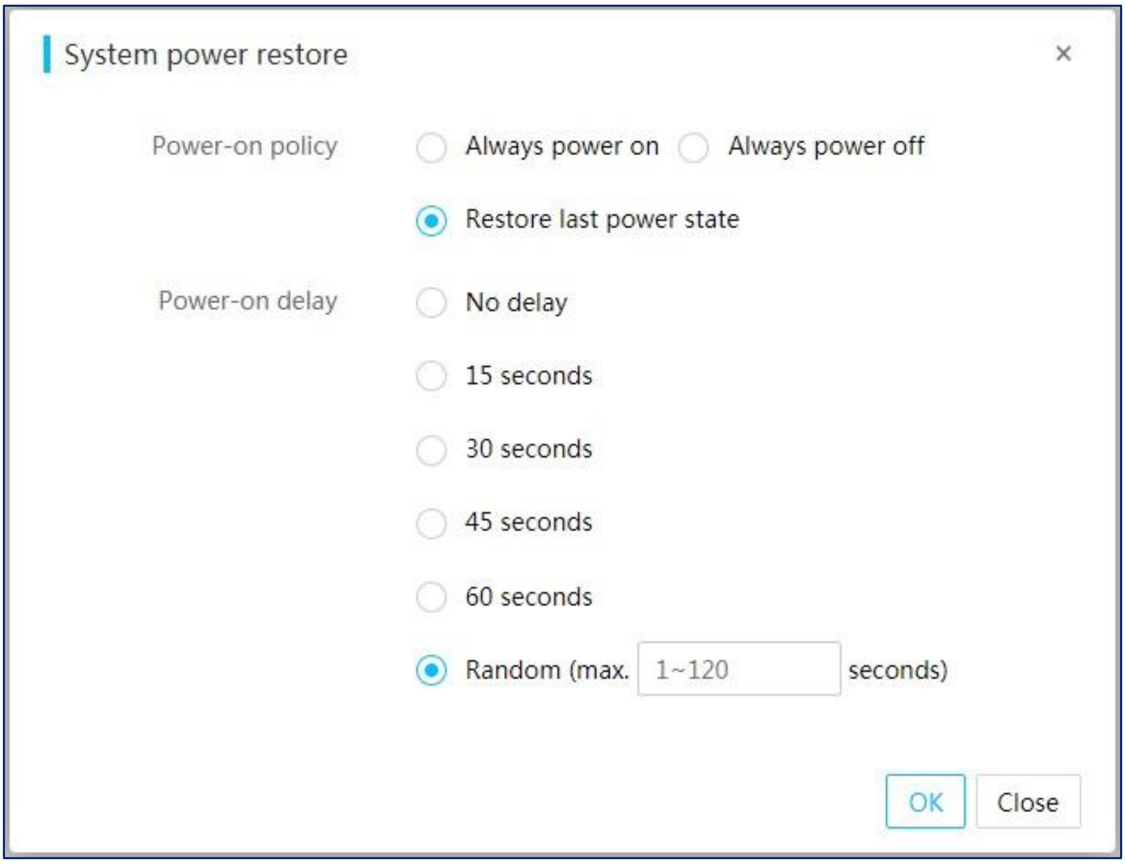
サーバーが電源に接続されている場合にサーバーの電源オンポリシーを設定するには、次の作業を実行します。

次のフィールドを使用できます。

- **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。オプションは、**Always power on**、**Always remain off**、および**Restore last power state**です。
    - 電源に接続に接続した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。
    - 電源に接続しているときにサーバーの電源をオフのままにするには、**Always Remain Off**を選択します。
    - サーバーを前回の電源切断時の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。オプションは、**No delay**、**15 seconds**、**30 seconds**、**45 seconds**、**60 second**s、**Random**(最大120秒)です。

  電源投入遅延は、ピークシフトによってサーバーの電源投入を可能にし、機器室でのサーバー電源投入時の瞬時消費電力を低減する。

図43 自動電源オンの設定



BMC制御によるサーバーの電源投入

この機能は、一部のサーバーでのみ使用できます。

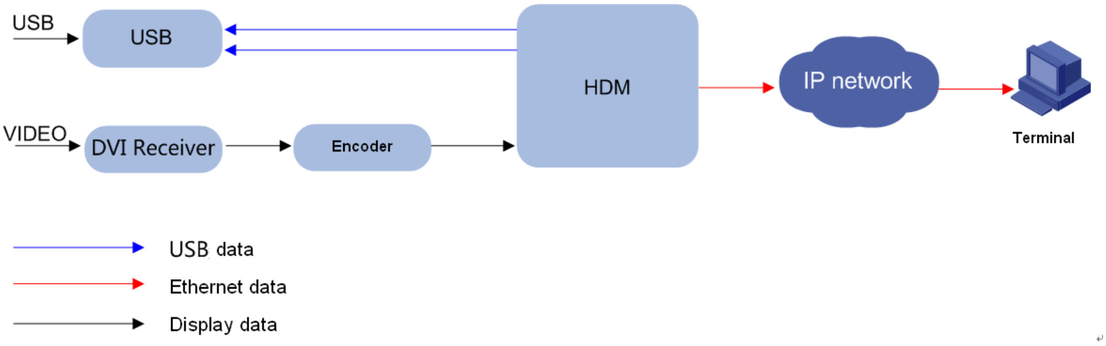
サーバーの電源オンはBMCによって決定されます。サーバーがAC電源に接続された後、まずシステムボードのスタンバイ電源が電源を供給してBMCを起動します。次に、BMCは設定された電源オンポリシーに基づいてサーバーを起動するかどうかを決定します。

KVMおよびバーチャルメディア

KVM

KVMを使用すると、ローカルクライアントを使用してリモートデバイスをリアルタイムで監視および制御できます。KVMを介してリモートデバイスを操作できます。

図44 KVMの図

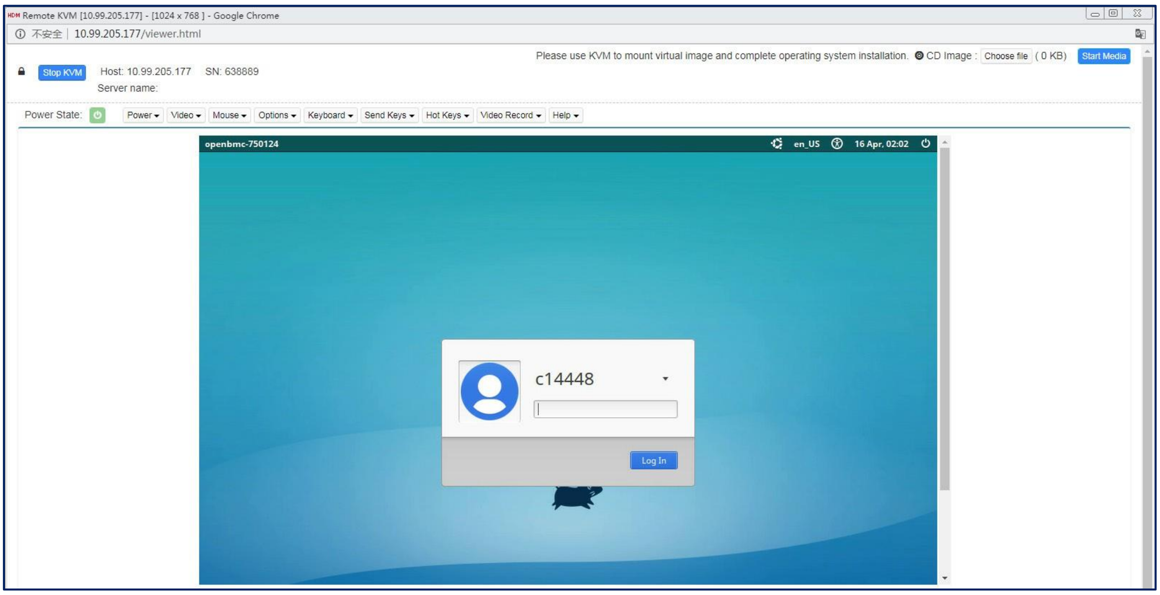


H5 KVM

KVMと比較すると、H5 KVMはプラグインを必要としません。HTTPS経由でH5 KVMリモートコンソールにアクセスして、サーバーをリモート管理できます。

HDMは、以下の形式でIPアドレス、ユーザー名、およびパスワードを入力することにより、H5 KVMへのアクセスをサポートします。
ブラウザのアドレスバーのhttp://*ip_addr*/viewer.html?u=*user_name*&p=*user_password*。

図45 H5 KVMへの直接アクセスの例



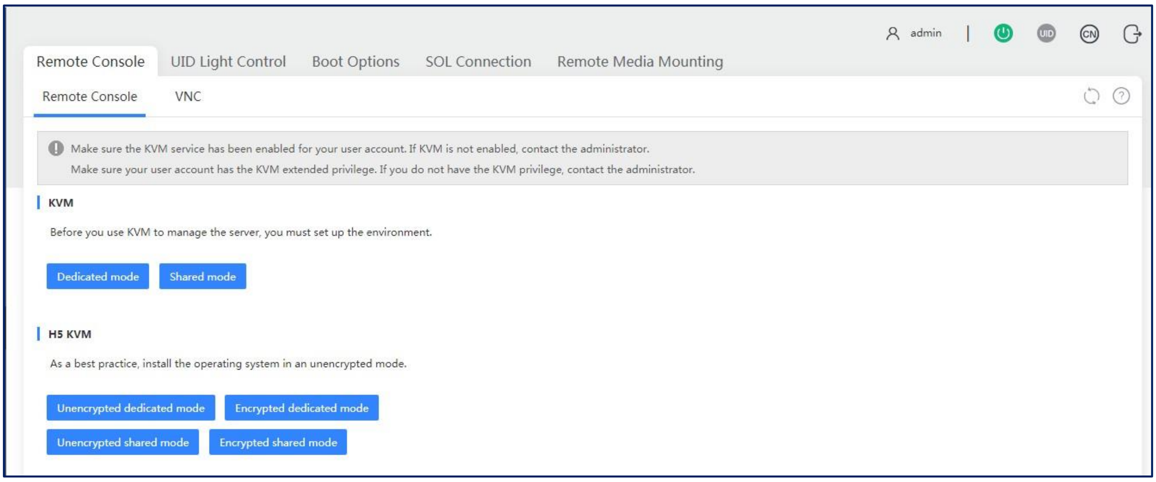
KVM起動モード

次のKVM起動モードを使用できます。

- **Dedicated mode**: 暗号化専用モードと暗号化されていない専用モードがあります。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。
- **Shared mode**: 暗号化共有モードと暗号化されていない共有モードが含まれます。共有モードでは、プライマリセッションと複数のセカンダリセッションが許可されます。プライマリユーザーの場合は、フルアクセス権限が割り当てられます。セカンダリユーザーの場合は、読取り専用権限のみが与えられ、ビデオの表示、スクリーンショットの撮影およびビデオの記録のみが可能です。

暗号化モードは、H5 KVMでのみ使用できます。暗号化モードでは、クライアントとサーバー間の暗号化後にデータが送信されるため、セキュリティパフォーマンスが向上します。非暗号化モードでは、暗号化されていないデータが送信されるため、伝送速度が向上します。OSのインストール時には、非暗号化モードを使用することをお薦めします。

図46 KVM起動モードの選択



バーチャルメディア

バーチャルメディア機能を使用すると、仮想USB DVD-ROMドライブまたはフロッピーディスクドライブを使用して、ネットワーク経由でローカルメディアにリモートアクセスできます。ローカルメディアは、DVD-ROMドライブ、フロッピーディスクドライブ、DVD-ROMイメージファイル、フロッピーディスクイメージファイルまたはハードドライブフォルダです。バーチャルメディアデータは、aes128-cbc暗号化アルゴリズムを使用して暗号化できます。バーチャルメディアを使用するには、ローカルクライアント上のメディアデバイスをネットワーク経由でリモートサーバー上のメディアデバイスに仮想化します。

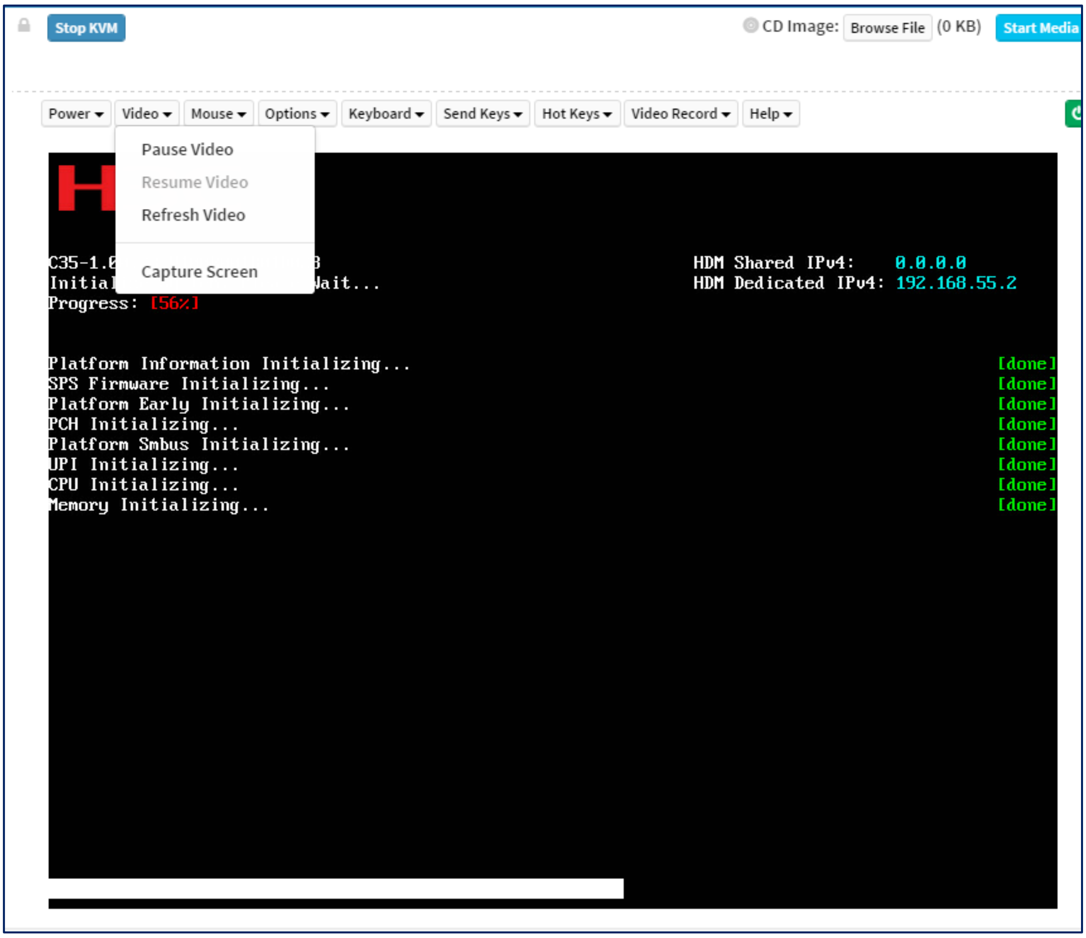
次の仮想記憶メディアを使用できます。

- CD/DVDドライブ。
- ISOファイルとIMGファイル。
- ローカルPCからサーバーにマウントされた仮想フォルダ。
- USBキー。

KVMからの画面キャプチャ

KVMリモートコンソールのスクリーンショットをキャプチャし、スクリーンショットを.jpeg形式でローカルPCに保存できます。

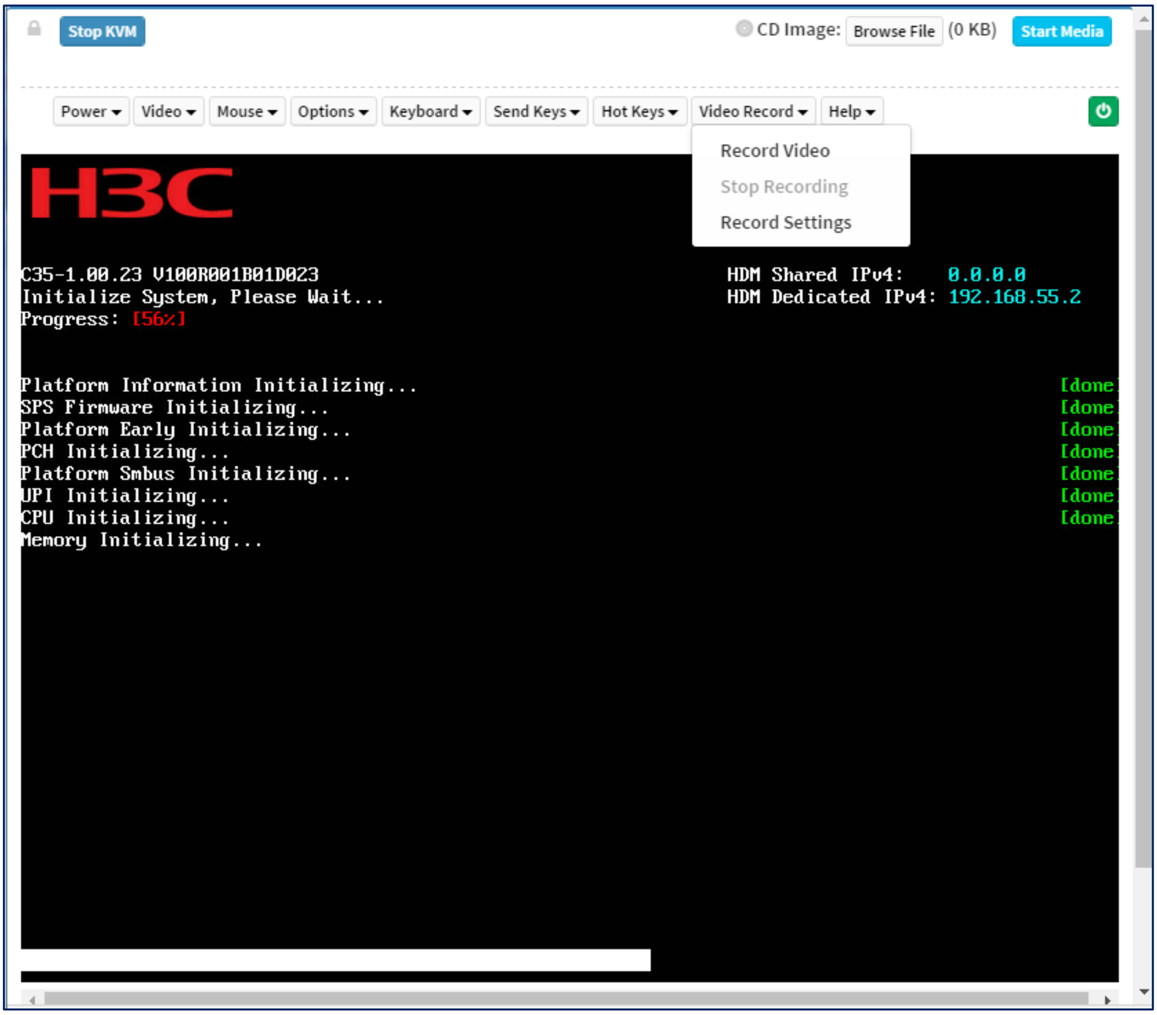
図47 スクリーンショットのキャプチャ



KVMからのビデオ録画

KVMリモートコンソールにビデオを記録し、スクリーンショットをローカルPCに.avi形式で保存できます。ビデオは仮想KVM操作を記録して、セキュリティを確保な要件を満たすために、仮想KVM操作を記録できます。ビデオ記録が有効になっている場合、KVMリモートコンソールは、画面に表示されたすべての情報と実行されたすべての操作を自己定義ビデオファイルに自動的に記録します。ローカルプレーヤーを使用してビデオを再生できます。

図48 KVMからのビデオ録画の有効化



VNCセッション

VNCについて

Virtual Network Console(VNC)は、サーバーの元のイメージをクライアントに送信します。VNCを使用すると、HDMにログインしなくても、ローカルPCからサーバーにアクセスして管理できます。

VNCシステムには、VNCサーバー、VNCクライアント、およびVNCプロトコルが含まれます。

- **VNC Server** :HDM側で実行され、サーバー画面をキャプチャして共有します。オペレーティングシステムの実行ステータスとは関係ありません。
- **VNC client**: VNCビューアでもあります。VNCクライアントはローカルPCにインストールされ、リモートでVNCサーバーに接続します。サードパーティのVNCクライアントはRealVNC、TightVNC、またはnVNCです。

HDMは、IPv4とIPv6の両方のVNCセッションをサポートします。

VNCセッションモード

HDMは最大2つの同時VNCセッションをサポートし、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。両方のセッションがマウスと

キーボードにアクセスし、サーバーのOSを制御します。

- **Exclusive mode**: 1つのVNCセッションのみをサポートします。共有モードのセッションが接続されていて、排他モードのセッションを確立しようとすると、共有モードのセッションは強制的に切断されます。VNCセッションがすでに存在する場合は、他のVNCセッションに対する後続の要求は拒否されます。

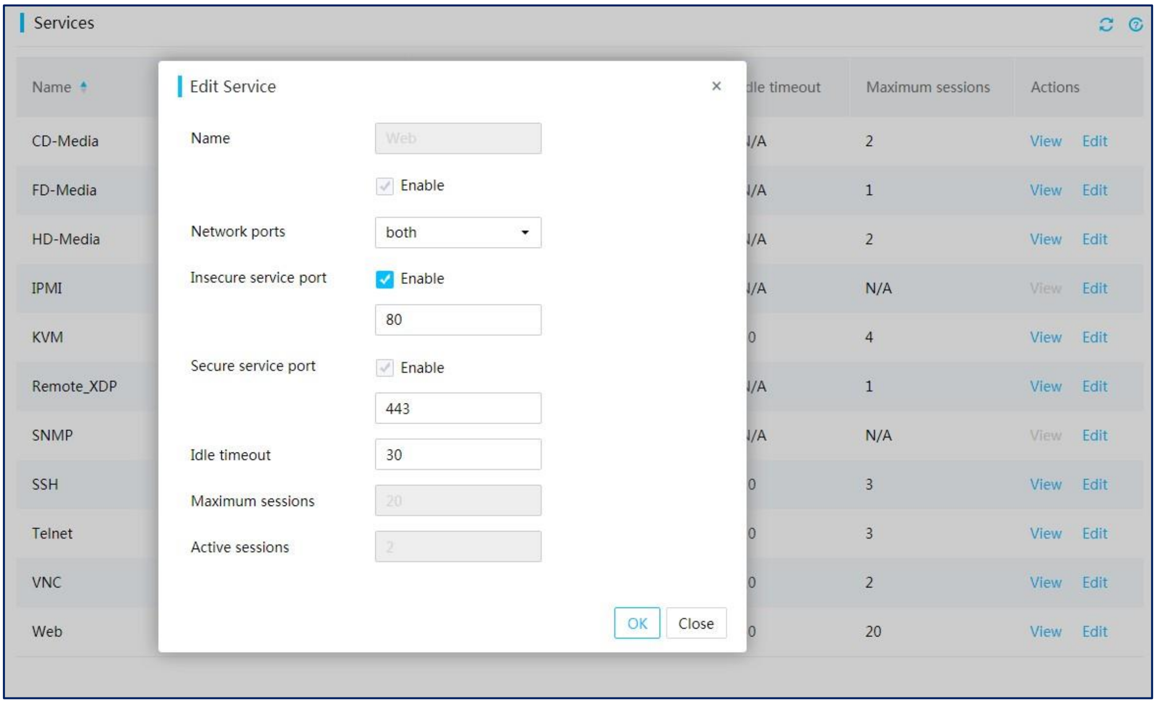
VNCシステムで使用されるセッションモードは、VNCクライアントによって決定されます。

VNCの有効化

デフォルトでは、VNCサービスは無効になっています。

VNCサービスを有効にするには、**Security > Services**ページに移動します。

図49 VNCサービスの有効化



セキュアでないVNCセッションの確立

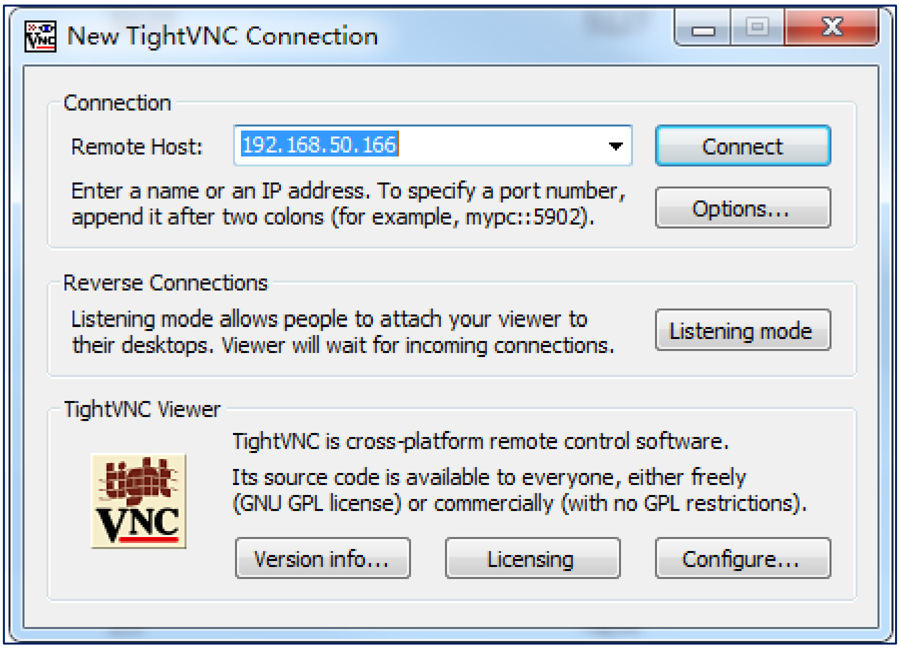
HDMからのVNCの有効化

HDMにログインし、VNCサービスを有効にします。

VNCクライアントでのVNCセッションの確立

VNCクライアント(VNCビューア)を開き、VNCパスワードを入力してVNCセッションを確立します

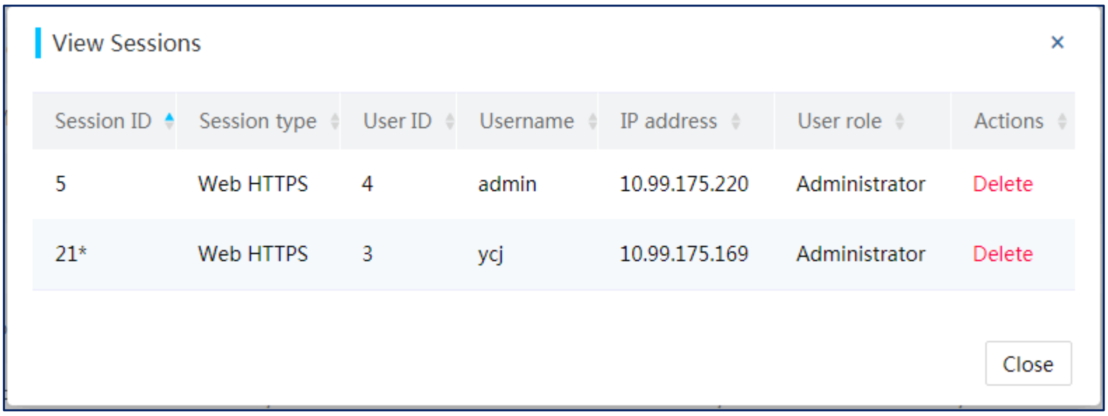
図50 VNCサーバーへの認証



VNCセッションの表示

確立されたセキュアでないVNCセッションは、**HDMのSecurity > 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。VNCクライアントでは、IPv4アドレスとIPv6アドレスの両方がサポートされています。

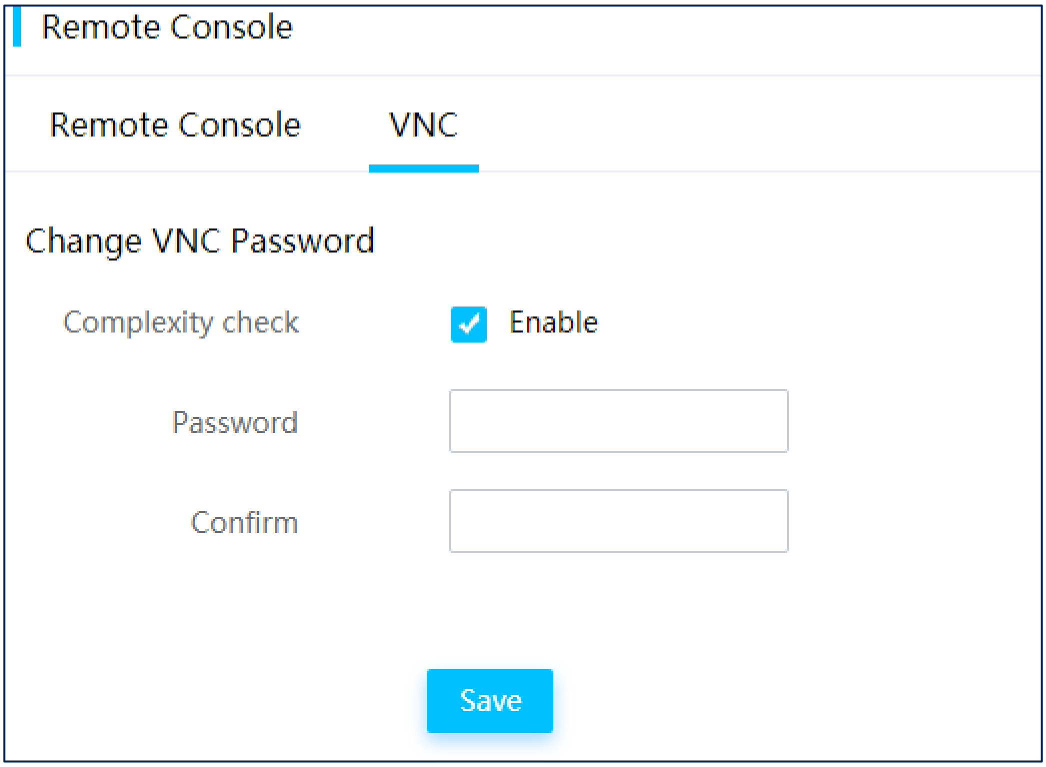
図51 VNCセッションの表示



VNCの設定

この機能を使用すると、パスワードの複雑度チェックを有効または無効にできます。パスワードの複雑度チェックが有効な場合、パスワードの長さは8文字にする必要があります。パスワードの複雑度チェックが無効な場合、パスワードの長さは1から8文字にする必要があります。

図52 VNCの構成



HDMネットワーク

サイドバンド管理とNCSI

サイドバンド管理を使用すると、管理システムとサーバーシステムは、NCSIテクノロジーを使用してサーバー上の物理ネットワークポートを共有できます。サイドバンド管理は、管理およびサービス処理を実装し、ネットワーキングを簡素化し、スイッチ上のポート使用率を低減します。セキュリティ上の理由から、サイドバンド管理では、VLANテクノロジーを使用して管理およびサービスを異なるネットワークセグメントに分割します。

NCSIは、物理バスRMIIに基づく帯域外管理バスプロトコルです。共通ネットワーク管理バスはMDC/MDIOバスであり、物理バスとして追加ピンを必要とします。NCSIはネットワーク通信バスRMIIとバスを共有し、NCSIプロトコルはRMIIバスに基づいて定義され、物理ピンを削減します。

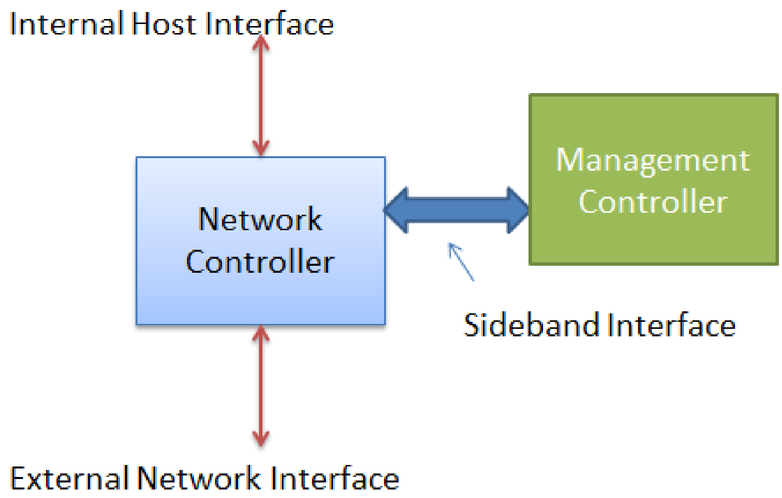
Network Controller(NC)は、通信のために次のインターフェイスに分割されます。

- **Internal host interface**: サーバーオペレーティングシステムへの接続を提供します。
- **External network interface**: 外部ネットワークへの接続を提供します。これをポートと呼びます。
- **Sideband interface**: NCSIを使用してHDMへの接続を提供しま

す。ネットワークポートの設定後、HDMはパケットをNCに送信できます。

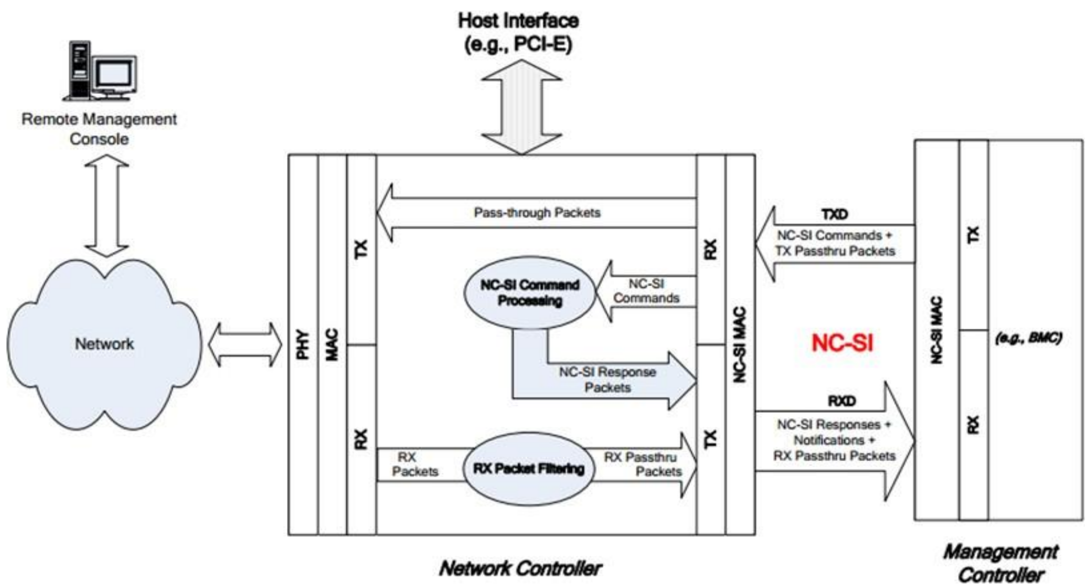
- リンク層では、NCSIパケットとネットワーク通信パケットは同じ物理バスRMIIを共有します。RMIIバスはHDMに接続し、NCの帯域外管理ネットワークポート(サイドバンドインターフェイス)として機能します。

図53 サイドバンド管理フレームワーク



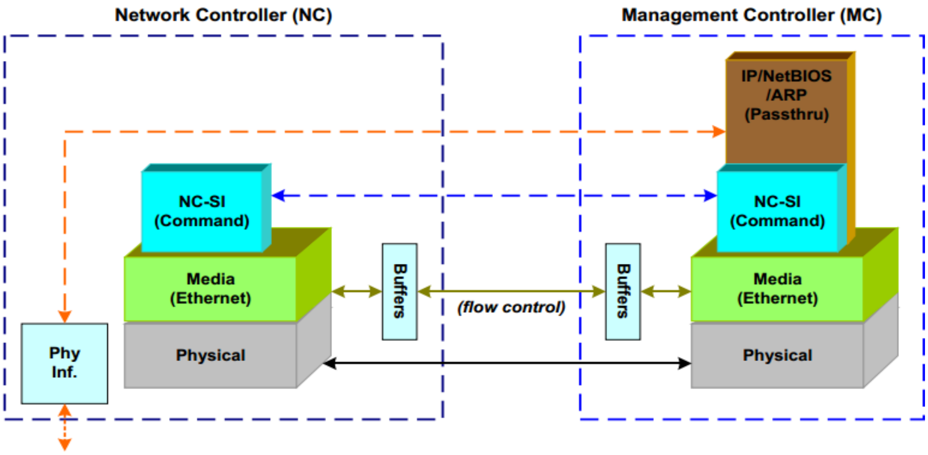
- データフローに関して、HDMはMACを介して物理バスRMIIにネットワークパケットを送信し、NCはパケット解析のためにRMIIを介してパケットを受信します。解析後、NCはパケットタイプに応じてパケットを処理します。
  - NCSIパケット(0x88F8でコード化されたエーテルタイプ)である場合、NCはNCSI応答を送信する。
  - 外部ネットワークに送信されたネットワークパケット(エーテルタイプが0x88F8でコーディングされていない)である場合、NCはそのパケットを外部ネットワークインターフェイスに転送します。

図54 サイドバンド管理データフロー図



- プロトコルに関して、NCSIは、ネットワークタイプコードが0x88F8であるネットワーク層プロトコルである。

図55 NCSIプロトコル

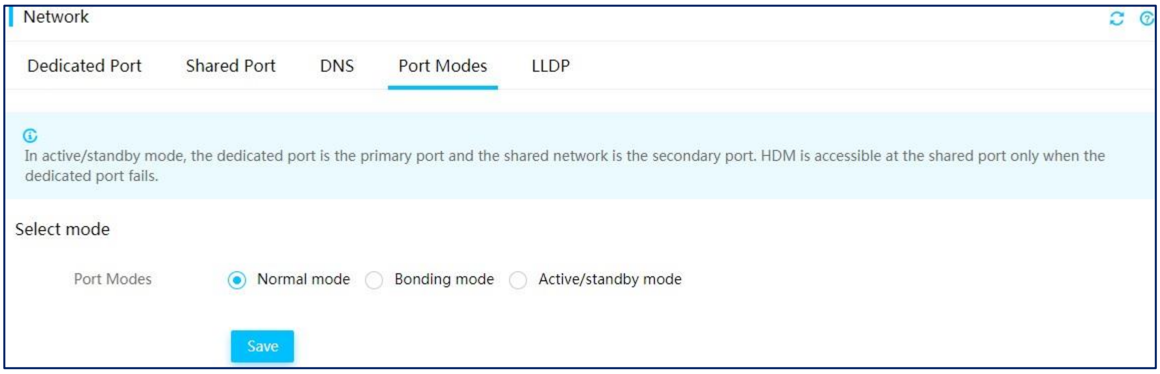


ネットワークポートモード

Normal mode

通常モードでは、HDM専用ネットワークポートと共有ネットワークポートは別々の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。

図56 normal modeの有効化



Bonding mode

Bonding modeでは、HDMはHDM専用ネットワークポートおよび共有ネットワークポートを、専用ポートのIPアドレスおよびMACアドレスを使用する論理結合ポートにバインドします。ユーザーは、専用ポートまたは共有ポートが起動しているかぎりHDMにアクセスできます。これにより、HDMアクセスの信頼性が向上します。

Active/standby mode

アクティブ/スタンバイモードでは、専用ポートがプライマリポートで、共有ネットワークがセカンダリポートです。HDMは、専用ポートが起動して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、共有ポートからHDMにアクセスできます。

Automatic shared port selection

この機能により、システムが自動的にポートを選択するための自動共有ポート選択が可能になります。共有ネットワークポートがアップ状態である限り、HDMにアクセスできます。

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NCSI対応PCIeネットワー

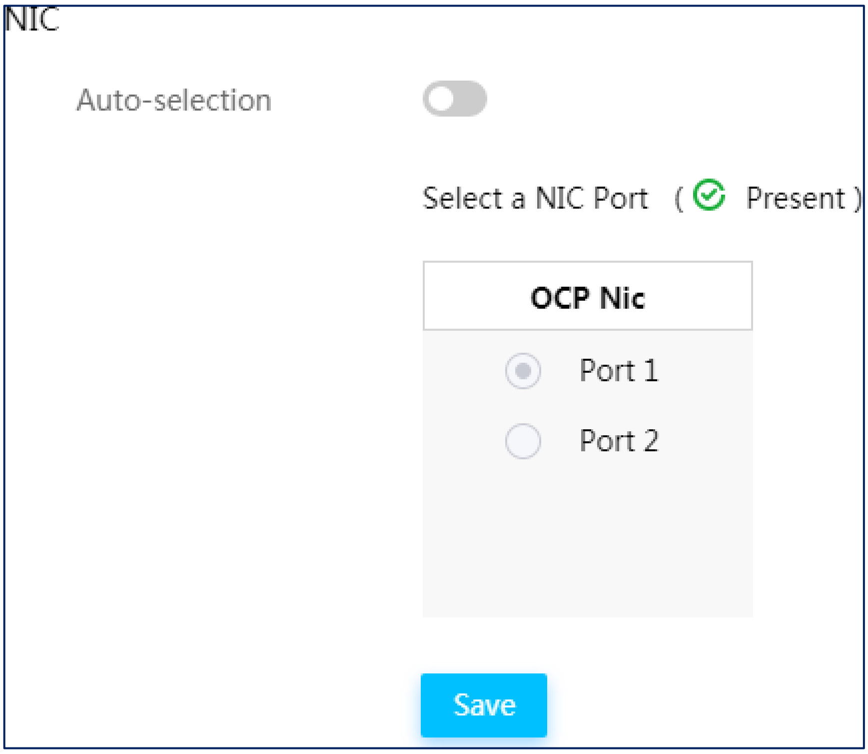
クアダプターは、自動共有ポート選択をサポートしています。

自動共有ポート選択には、次の利点があります。

- サーバーのネットワーク設定を再設定することなく、スムーズなポート変更を実現します。
- ポート変更後も共有ポートネットワーク設定(IPおよびVLAN設定)を保持するため、メンテナンスの効率が向上します。

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。

図57 自動共有ポート選択の有効化



IPv6

HDMはIPv6をサポートし、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IPv6をサポートします。

図58 共有ネットワークポートのIPv4およびIPv6設定の表示

NTP時間管理

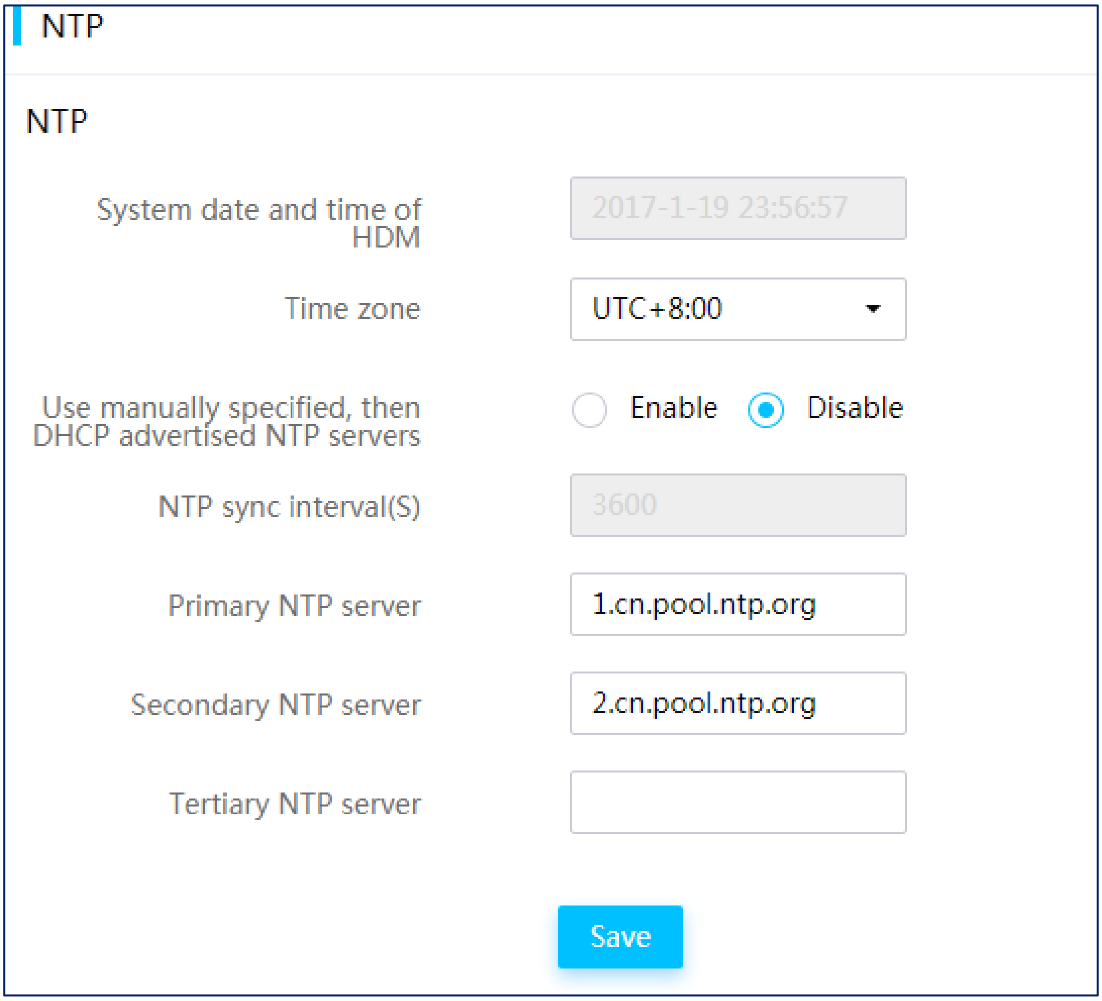
Network Time Protocol(NTP;ネットワークタイムプロトコル)は、ネットワーク内のデバイスのクロック時間を同期するために使用されるTCP/IPプロトコルファミリのアプリケーション層プロトコルです。HDMからサーバーが配置されているタイムゾーンを指定し、1つのプライマリNTPサーバーと1つのセカンダリNTPサーバーを手動で指定できます。

HDMでは、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。IPv4アドレスとIPv6アドレスの両方がサポートされ、NTPサーバーを手動で指定する場合はFQDNもサポートされます。

時刻を同期する場合、HDMは次の順序で時刻ソースを使用します。

- プライマリNTPサーバー。
- セカンダリNTPサーバー。
- DHCPサーバーをNTPサーバーとして使用します。
- ME(インテル製品でのみ利用可能)
- BMC上のRTC。

図59 NTP設定の構成



DNS

ドメインネームシステム(DNS)は、ドメイン名をIPアドレスに変換するためにTCP/IPアプリケーションで使用される分散データベースです。完全なドメイン名は、ホスト名とトップレベルドメインおよびセカンドレベルドメインで構成されます。HDMの場合、ホスト名は手動で構成するか、サーバーのシリアル番号に基づいて自動的に移入できます。トップレベルドメインおよびセカンドレベルドメインは、DHCPサーバーを介して手動で構成または自動的に割り当てることもできます。

HDMは、共有ネットワークポートおよび専用ネットワークのIPアドレスをドメイン名にマッピングし、このマッピング関係をDNSサーバーに登録することをサポートします。

次の登録方法を使用できます。

- **nsupdate**: HDMクライアントは、DNSサーバーのゾーンファイルを更新するために nsupdateコマンド。
- **FQDN\hostname**: DHCPサーバーは、HDMクライアント上のIPアドレス割り当てを確認した後、HDMクライアント情報をDNSサーバーに動的に登録します。

覚えやすいドメイン名を使用して、すべての管理対象サーバーを管理ドメインに追加し、サーバーのHDMにアクセスできます。

リモートsyslogサーバー

HDMでは、syslogメッセージを使用して操作ログおよびイベントログを宛先ホストに報告できます。サーバーポート、伝送プロトコル、ログタイプ、および資産タグを設定できます。

伝送プロトコルにはUDP、TCP、TLSがあります。TLSは一方向認証と双方向認証をサポートしています。

図60 Syslog設定ページ

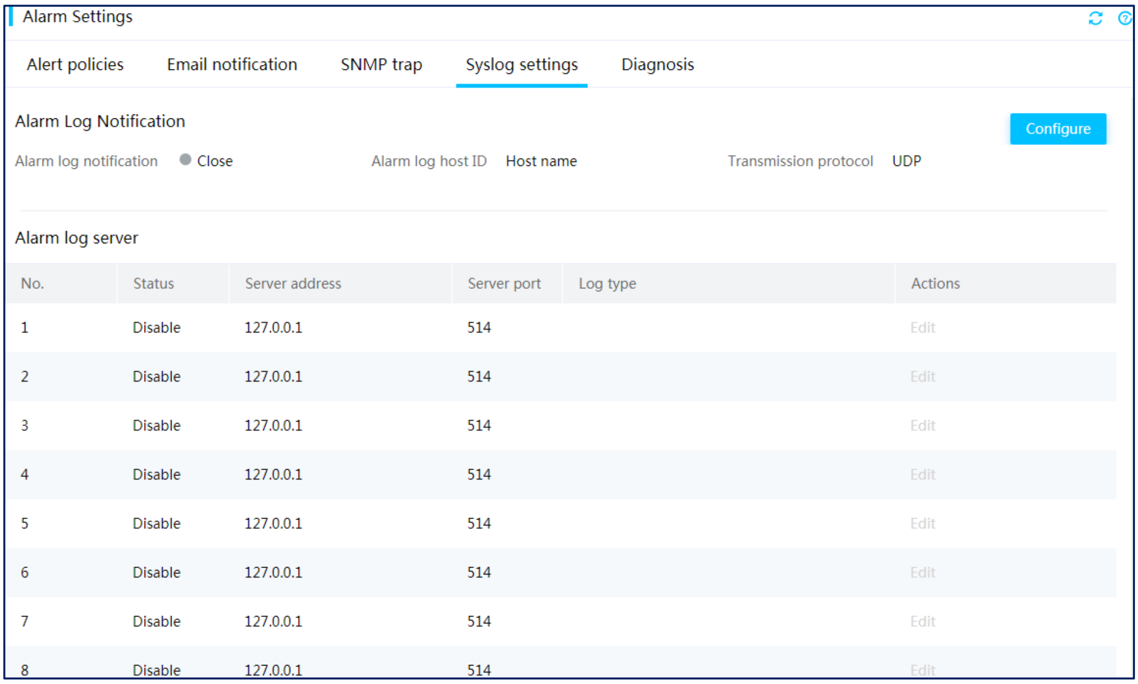
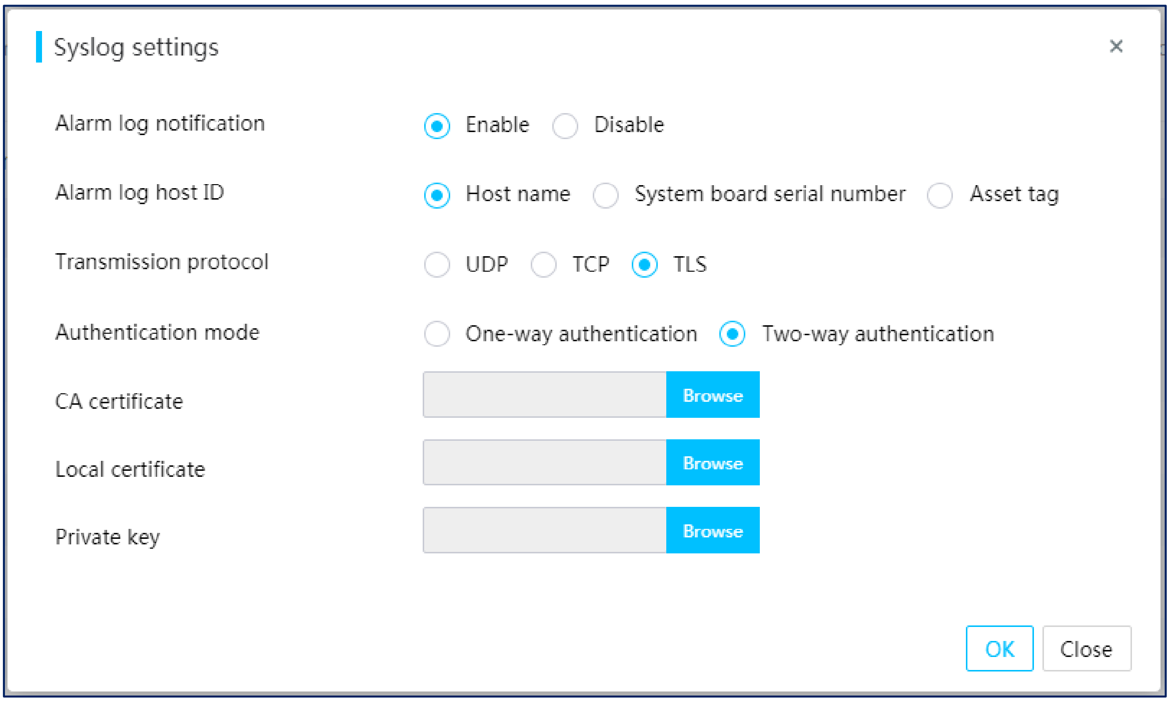


図61 Syslog通知設定の構成

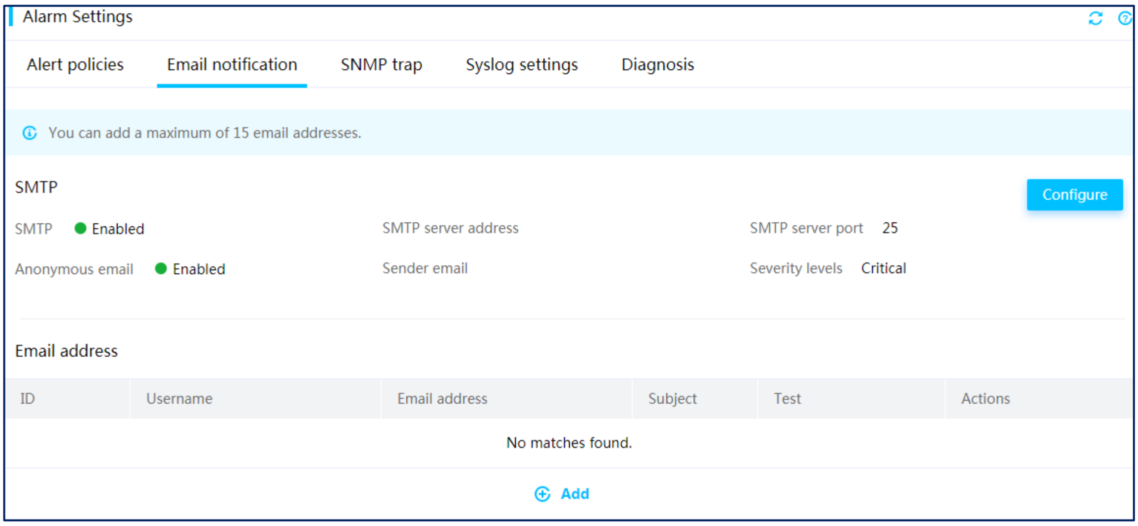


警告メール

HDMはサーバーステータスを監視し、サーバーによって生成されたイベントログを電子メールで指定されたユーザーに報告します。SMTPサーバーでは、IPv4アドレスとIPv6アドレスの両方を使用できます。アラート電子メールを匿名電子メールとして送信するか、送信者ID情報とともにアラート電子メールを送信できます。サーバーの監視では、最大16の電子メール受信者がサポートされています。

サーバーイベントは重大度レベルに基づいてレポートされ、次の中から重大度レベルを選択できます。**All、Critical、およびMinor + Major + Critical。**

図62 SMTPの設定



SNMPトラップ

HDMからSNMPトラップ設定を構成し、SNMPトラップ内のサーバーイベントをサーバー監視用のユーザーに送信できます。

HDMは、SNMPサーバーの構成をサポートします。サーバーイベントは重大度レベルに基づいてレポートされ、「すべて」、「クリティカル」、「マイナー+メジャー+クリティカル」から重大度レベルを選択できます。

サーバーイベントは、次のモードで報告されます。

- **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。ユーザーはOIDを使用して障害モジュールを特定できます。
- **Event mode**: トラップイベントと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。イベントのOIDを使用して障害タイプを識別できます。

図63 SNMPトラップの設定ページ

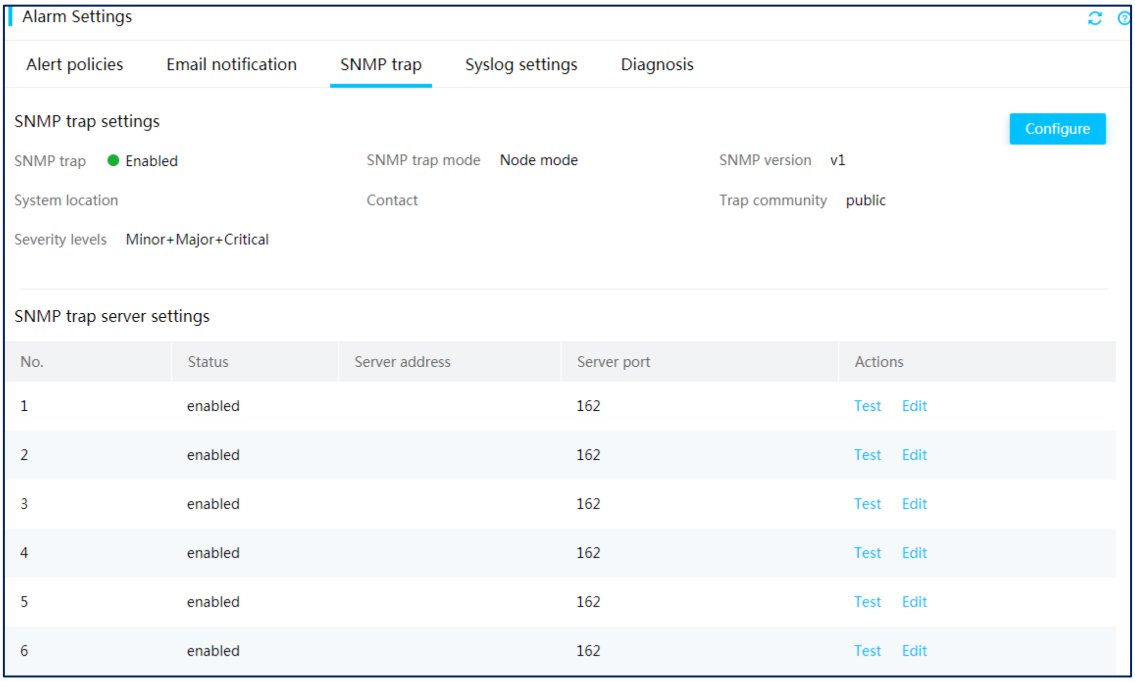
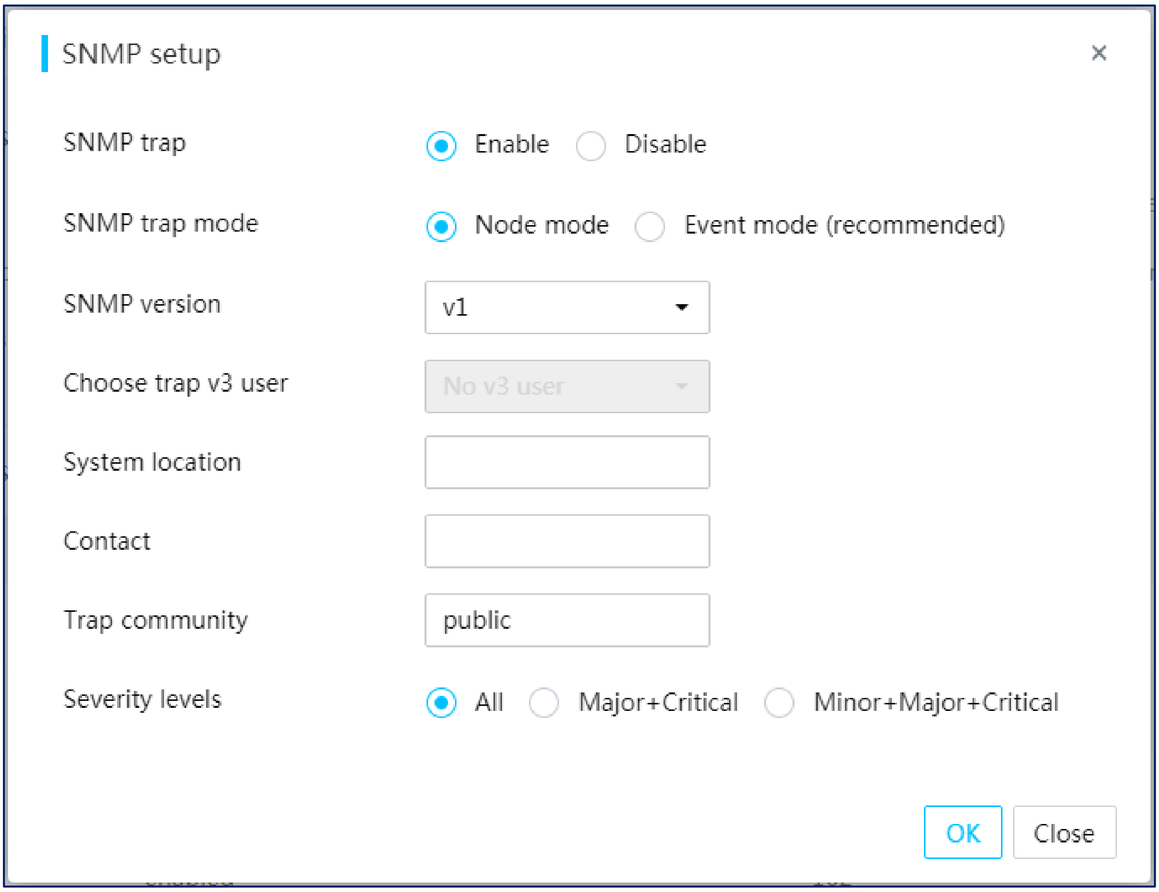


図64 SNMPトラップ設定の構成



USB Wi-Fi

HDMは、G5サーバーのシャーシイヤーにあるUSB Type-Cコネクターに接続する他社製USB Wi-Fiアダプターをサポートしています。USB Wi-Fiアダプターは、HDM用のワイヤレスホットスポット機能を提供します。携帯電話やラップトップを使って、ワイヤレスネットワーク経由でHDMにアクセスしたり、HDM Mobileなどで保守・点検を行うことができます。

XiaomiポータブルWi-Fiアダプターのみがサポートされており、アダプターはUSBケーブルを介してサーバーのType-Cコネクターに接続されている必要があります。

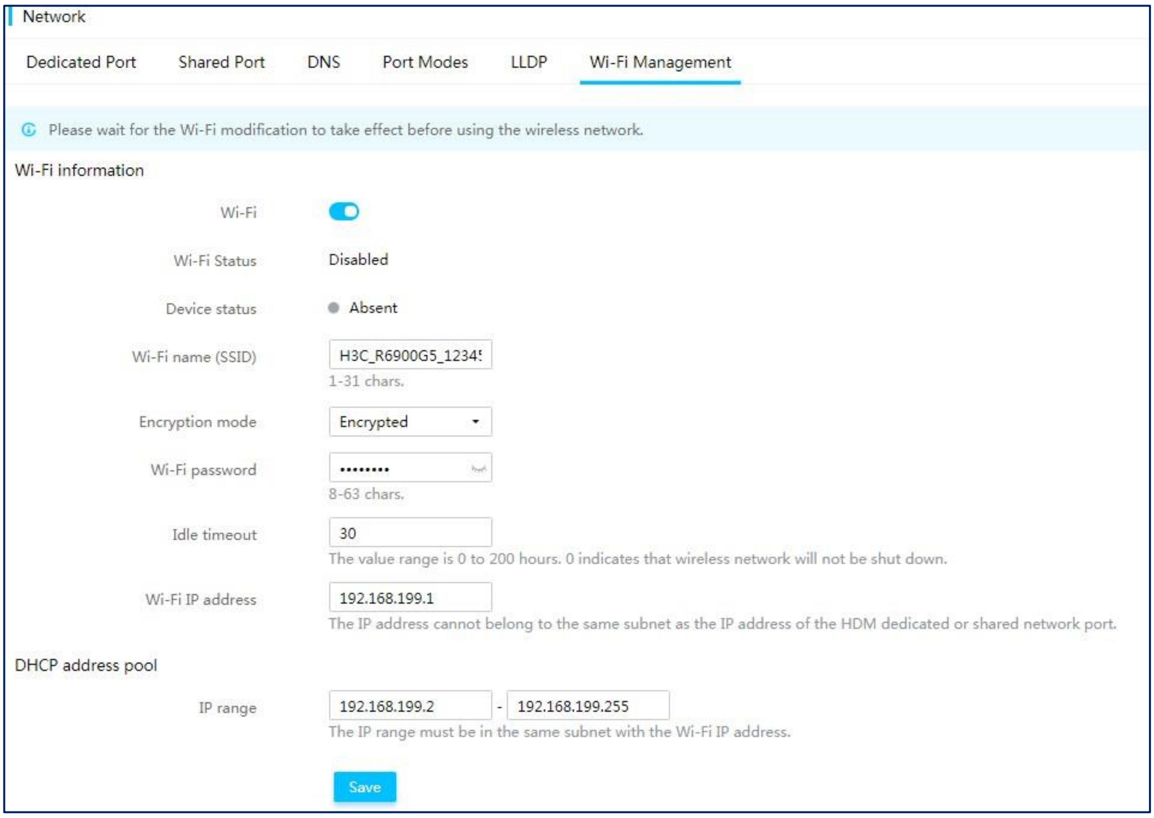
セキュリティを向上させるために、システムでは最大2つのクライアントを同時にオンラインにすることができます。

Wi-Fiの有効化ステータス、Wi-Fi名、暗号化モードとWi-Fiパスワード、アイドルタイムアウト、Wi-Fi IPアドレス、DHCPアドレスプールなどのWi-Fi設定をHDMから構成できます。デフォルトでは、次の設定が適用されます:

- Wi-Fi名は、デバイスSNフォーマットの製品名_最後の10文字です。
- ワイヤレスネットワークは、プラグアンドプレイ操作を実現するために暗号化されません。

HDMは、ワイヤレスネットワーク経由でWeb、Redfish、IPMI、SSH、およびTelnetのネットワークプロトコルをサポートしています。

図65 Wi-Fi設定の構成



LLDP

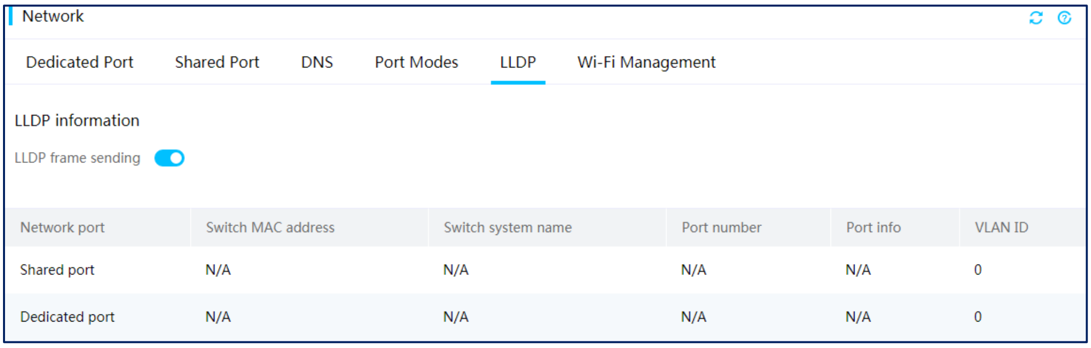
Link Layer Discovery Protocol(LLDP)は、異なるベンダーのネットワークデバイスがネイバーを検出し、システムおよび設定情報を交換できるようにする標準リンク層プロトコルです。ネットワークが変更された場合、ネットワーク管理システムはトポロジの変更を迅速に検出し、レイヤ2でトポロジ情報を更新できます。

接続されたデバイスがサーバーを識別するために、サーバーがHDMからLLDPフレームを送信できるようにすることができます。

HDMはLLDPをサポートし、ローカルネットワークで次のスイッチ情報を取得します。

- **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)。
- **Port rate**: サーバーポートのレート。
- **VLAN ID**: サーバーポートが属するVLANのID。

図66 LLDPの設定



セキュリティ

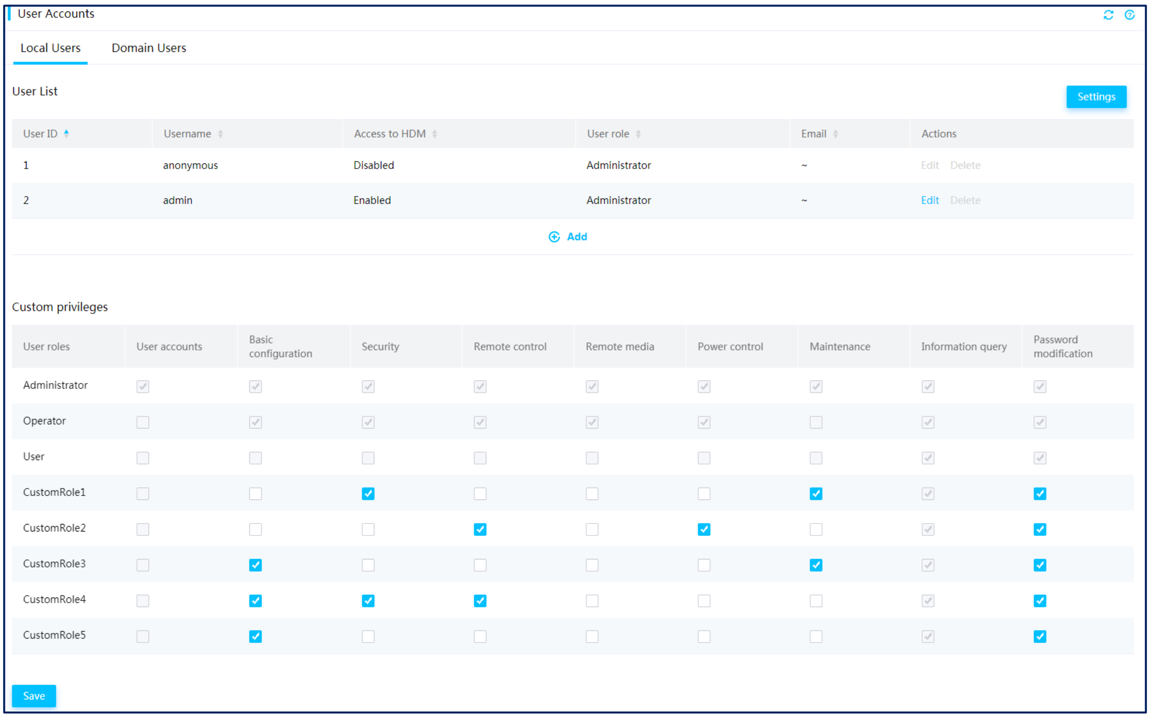
ユーザー権限

ローカルユーザーおよびドメインユーザー(LDAPユーザーおよびADユーザー)を含むユーザーカウントを設定して、**User Accounts**ページでHDMへのアクセスを制御できます。

ユーザーのネットワークおよびサービスアクセス権限は、ユーザーロールによって決定されます。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して読み取り権限を持ち、一部の機能に対して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アクセス権を持っています。
- **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。システムでは、最大5つのカスタムユーザーロールがサポートされます。

図67 ユーザーアカウントのカスタム権限の構成



管理インターフェイスとHDMモジュール

HDMは、RedfishやIPMIインターフェイスなどの機能やインターフェイスをネットワークアクセス権限用の異なるモジュールに分割することで、セキュリティを向上させます。使用可能なモジュールには、ユーザーカウント、基本設定、リモートコンソール、リモートメディア、セキュリティ、電源制御、メンテナンス、パスワード変更、および情報クエリなどがあります。

表2に各HDMモジュールの代表的な特徴を示す。

表2 HDMモジュールの特徴

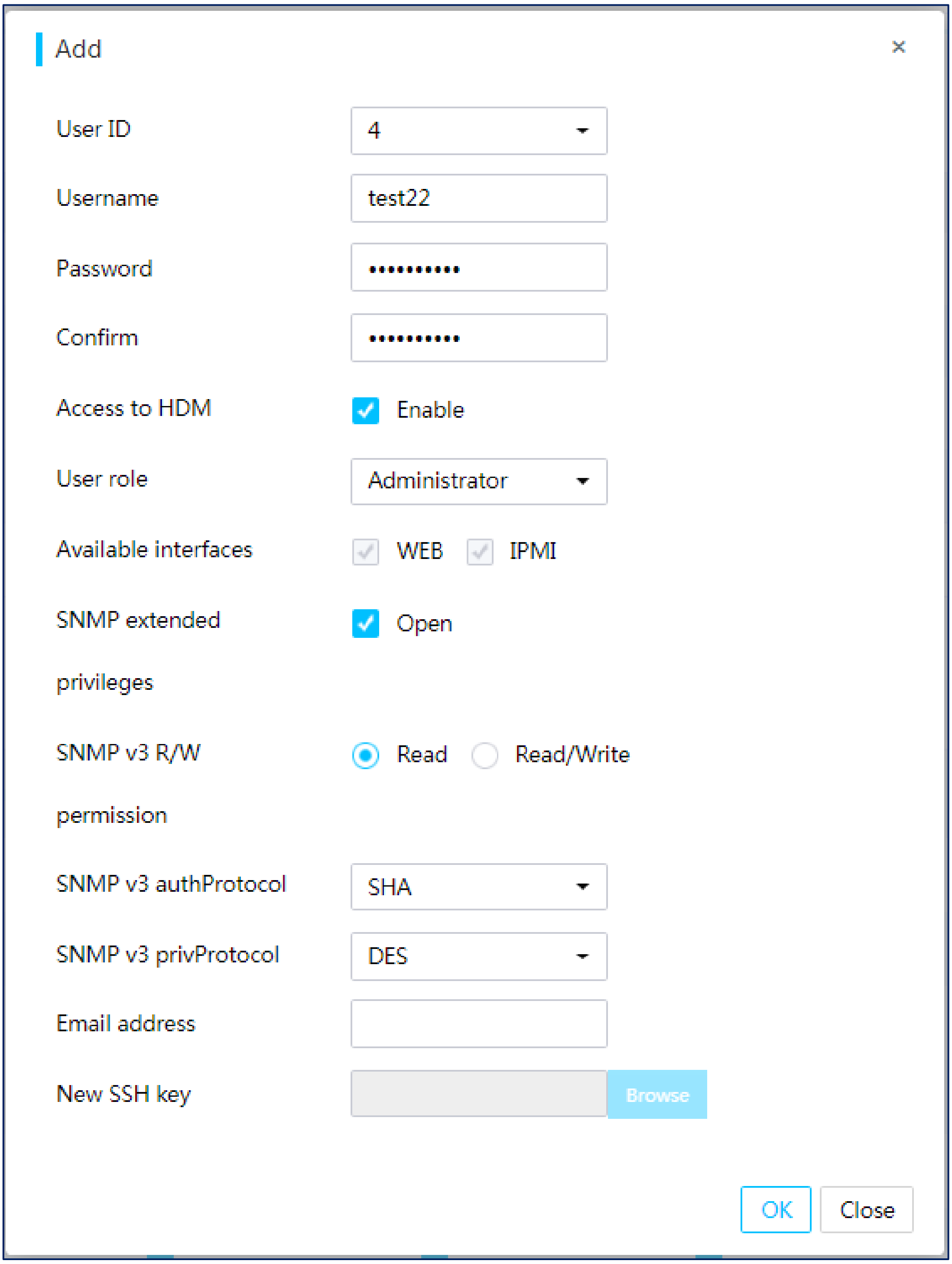
モジュール	説明
ユーザーアカウント	ユーザー管理、パスワードポリシー構成、ディレクトリー管理、構成のインポートとエクスポート、統合制御などが含まれます。
基本設定	ネットワークの確認(ネットワークポート、NTP、SNMP、LLDP、syslogなど)および資産タグ設定が含まれます。
リモートコントロール	ストレージ管理、ハードパーティショニング、リソース監視、KVM(電源制御とイメージマウントを除く)、VNC構成、システムブートオプション、UID LED管理、SOL接続、MCAポリシー、セキュリティベゼル構成を含みます。
リモートメディア	リモートメディアおよびKVMイメージのマウントが含まれます。
セキュリティ	アクセスサービス設定、ファイアウォール、SSL、PFR、およびログイン用のセキュリティヒントが含まれます。
電源制御	電源管理、ファン管理、NMI制御、および物理的な電源ボタン制御が含まれます。
メンテナンス	ドライブUID LEDの管理、CUPS、ビデオ録画とスクリーンショット、ファームウェア管理(ファームウェアの更新、再起動、プライマリ/バックアップのスイッチオーバー)、工場出荷時のデフォルトへの復元、リアルタイムの監視が含まれます。
パスワードの変更	現在のユーザーのパスワードの変更が含まれます。

情報クエリ	通常、GETインターフェイスでサポートされます。

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ており、ローカルユーザーに対して使用可能なアクセス特権(IPMIおよびWeb)とSNMP拡張特権を選択できます。

図68 ユーザーアカウントの編集

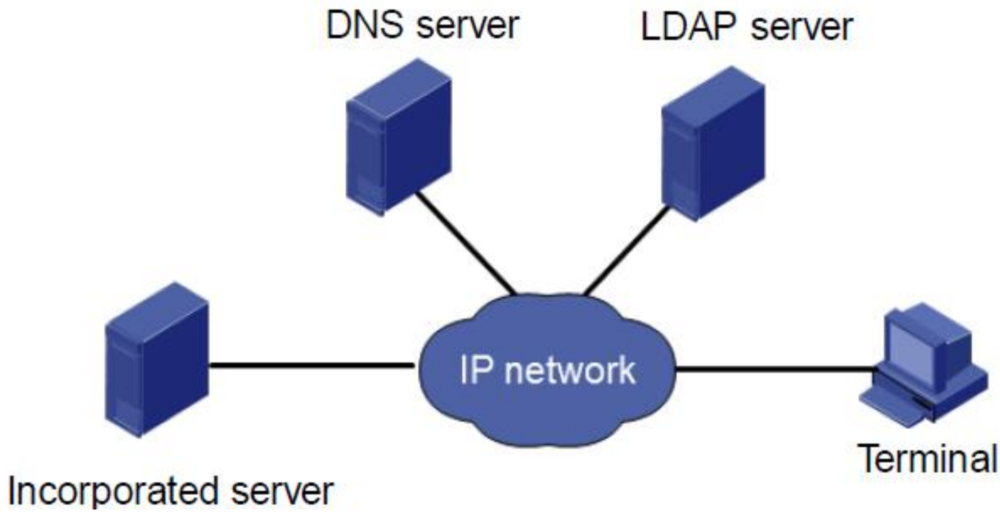


LDAPユーザー

Lightweight Directory Access Protocol(LDAP)を使用すると、IPネットワークを介してオンラインディレクトリーサービスに効率的にアクセスできます。電子メールアドレスや電子メールルーティング情報などの複数のタイプのデータをLDAPディレクトリーに保存し、一元化された便利な方法でフィルタ処理できます。

図69に示すように、LDAPディレクトリーサービスを使用可能にすると、ユーザー、許可、有効期間の管理がLDAPサーバーに一元化されるため、構成の重複が減り、管理効率が向上し、システムセキュリティーが向上します。

図69 LDAPディレクトリーサービスダイアグラム



LDAPには、次の利点があります。

- **高いスケーラビリティ**: すべてのHDMに対して、LDAPサーバー上のユーザーを同時に動的に追加します。
- **セキュリティの強化**: LDAPサーバーにユーザーパスワードポリシーを実装します。SSL暗号化がサポートされています。
- **リアルタイムパフォーマンス**: LDAPサーバー上のユーザーカウントの更新をすべてのHDMに直ちに適用します。
- **効率性の向上**: HDMのユーザー管理を統合することで、ユーザー設定タスクの繰り返しを最小限に抑え、管理効率を向上させせます。

ADユーザー

Active Directory(AD)は、Windows OS用に開発されたディレクトリーサービスです。グループを集中管理し、ネットワークリソースにアクセスするディレクトリーサービスを提供し、ネットワークトポロジとプロトコルをユーザーに対して透過的にします。

Active Directoryはドメインの論理構造に基づいて管理されているため、拡張性があります。

HDMはAD認証をサポートしています。この機能により、ユーザーはADサーバーに構成された有効なActive Directory(AD)グループのユーザー名とパスワードを使用してHDMにアクセスできます。ユーザーの権限は、ユーザーが属するADグループによって決定されます。

図70 AD認証の構成

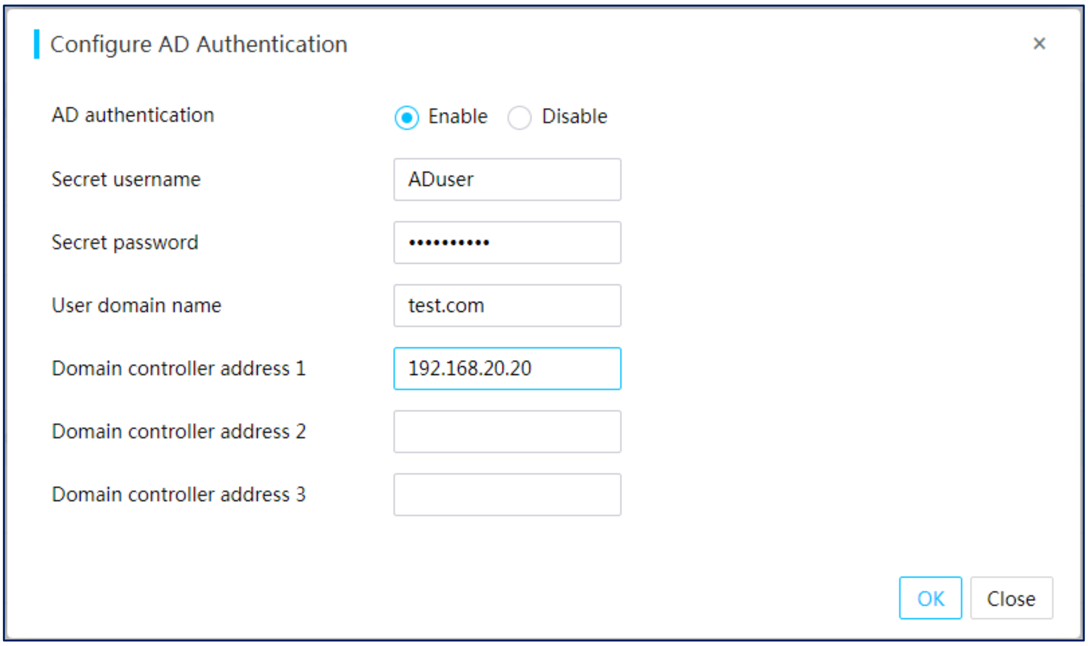
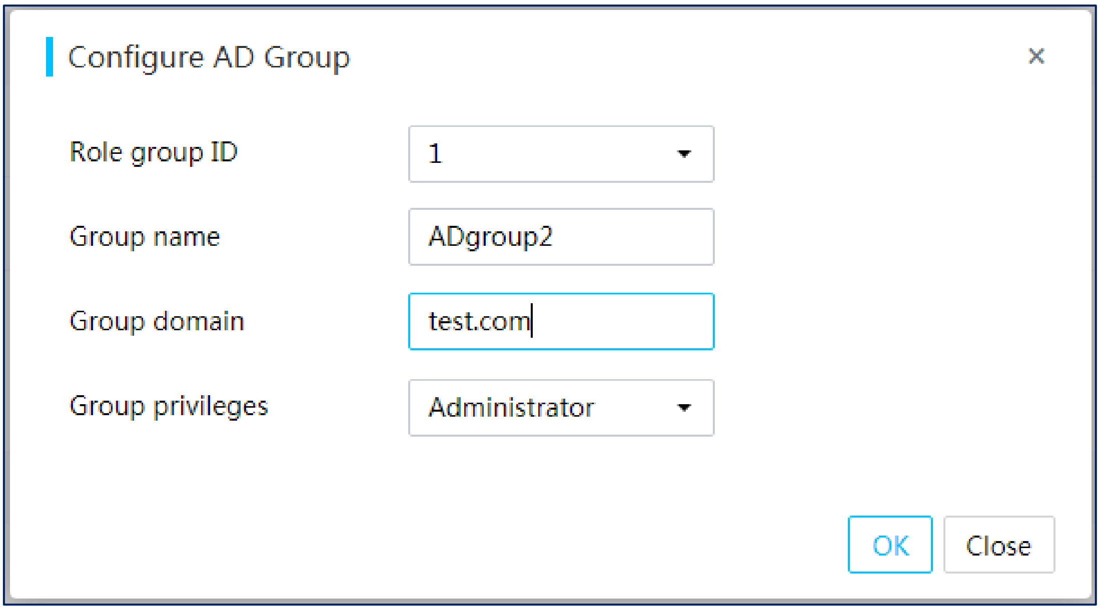


図71 ADグループの追加



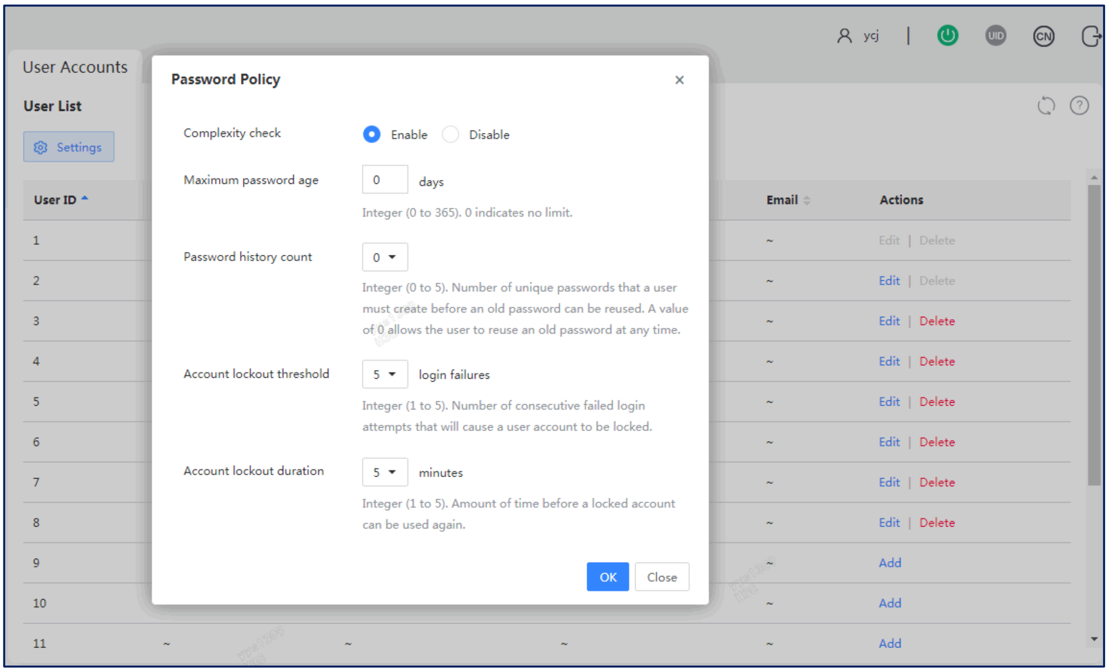
パスワードポリシー

ユーザーカウントのパスワードがパスワードポリシーで従う必要がある規則を設定することによって、HDMアクセスセキュリティを強化できます。

手順

1. ナビゲーションペインで、**Configuration > User Accounts**を選択します。
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、パスワードポリシーを構成し、**OK**をクリックします(図72)。

図72 パスワードポリシーの構成



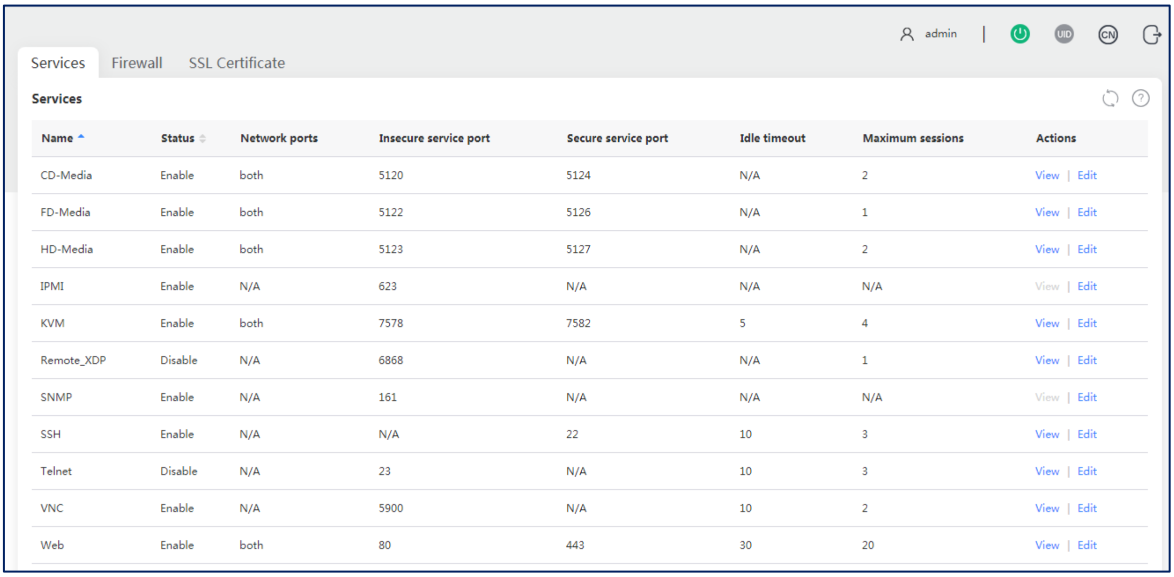
パラメータ

- 複雑度チェック:パスワードの複雑度チェックをディセーブルまたはイネーブルにします。
  - この機能をイネーブルにする場合、パスワードは次の拡張された複雑さの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、文字、数字、スペース、および特殊文字`~!@#$%^&*()_+-=[]\{};':",./<>?
    - 大文字、小文字、および数字のカテゴリの少なくとも2つからの文字を含む必要があります。
    - 少なくとも1つのスペースまたは特殊文字を含む必要があります。
    - ユーザー名と同じにしたり、逆のユーザー名にすることはできません。
    - 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求めるメッセージを表示します。
- **Password history count**: 古いパスワードを再利用できるようにするために、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回数。
- **Account lockout duration**: ロックされたアカウントが再度使用されるまでの時間。

アクセスサービス

サービスおよびセキュリティ要件を満たすために、HDMでは、CD-Media、FD-Media、HD-Media、IPMI、KVM、Remote_XDP、iHDT、SNMP、SSH、Telnet、Web、およびVNCの各サービスの有効化ステータスを表示および制御できます。

図73 アクセスサービスの構成



Name	Status	Network ports	Insecure service port	Secure service port	Idle timeout	Maximum sessions	Actions
CD-Media	Enable	both	5120	5124	N/A	2	View | Edit
FD-Media	Enable	both	5122	5126	N/A	1	View | Edit
HD-Media	Enable	both	5123	5127	N/A	2	View | Edit
IPMI	Enable	N/A	623	N/A	N/A	N/A	View | Edit
KVM	Enable	both	7578	7582	5	4	View | Edit
Remote_XDP	Disable	N/A	6868	N/A	N/A	1	View | Edit
SNMP	Enable	N/A	161	N/A	N/A	N/A	View | Edit
SSH	Enable	N/A	N/A	22	10	3	View | Edit
Telnet	Disable	N/A	23	N/A	10	3	View | Edit
VNC	Enable	N/A	5900	N/A	10	2	View | Edit
Web	Enable	both	80	443	30	20	View | Edit

ファイアウォール

ファイアウォールは、アクセスを許可またはブロックするように識別するファイアウォール規則に基づく攻撃からHDMを保護します。

次のファイアウォール規則を作成できます。

- **Black list rule**: 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ルールを設定できます。

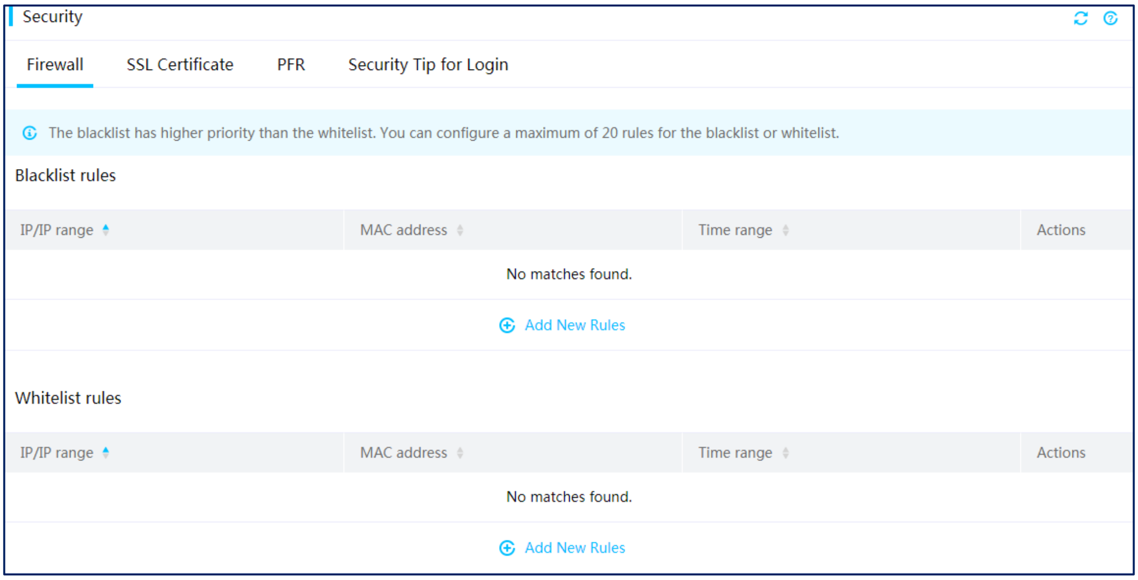
  最大20個のブラックリストルールがサポートされます。

- **White list rule**: 特定のIPアドレスまたはMACアドレスからHDMサーバーへのアクセスを許可します。ホワイトリストルールは、指定した時間範囲内で有効になるように設定できます。

  最大20個のブラックリストルールがサポートされます。

ブラックリスト規則は、ホワイトリスト規則よりも優先されます。

図74 ファイアウォール設定の構成



SSL証明書

SSL証明書をアップロード、生成、または表示することによって、SSL証明書を管理できます。

SSL証明書情報には、証明書ユーザー、証明機関、有効期間、およびシリアル番号が含まれます。

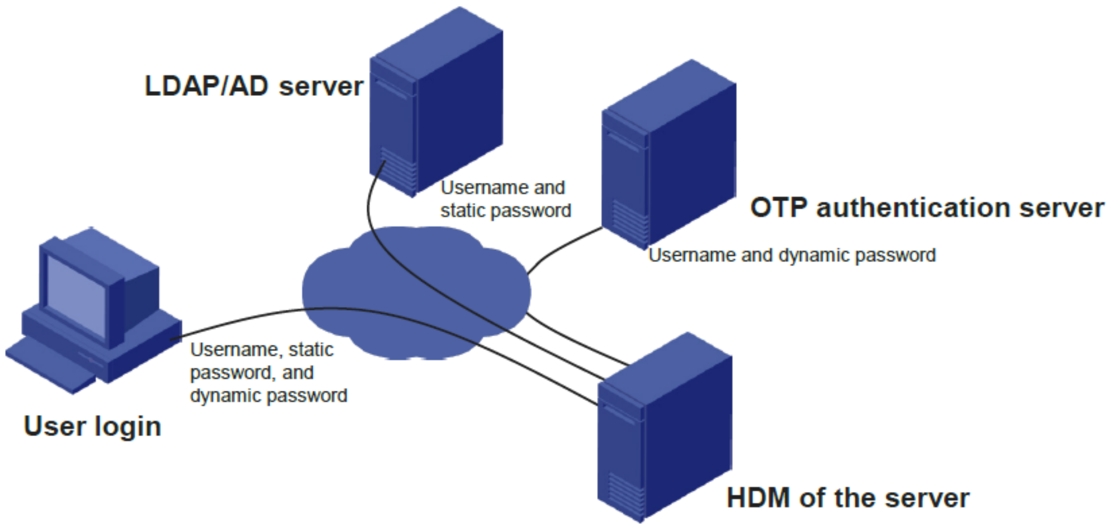
HDMには、独自のデフォルトのSSL証明書が付属しています。セキュリティ強化のベストプラクティスとして、デフォルトのSSL証明書を独自の証明書と公開鍵のペアに置き換えます。

2要素認証

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。

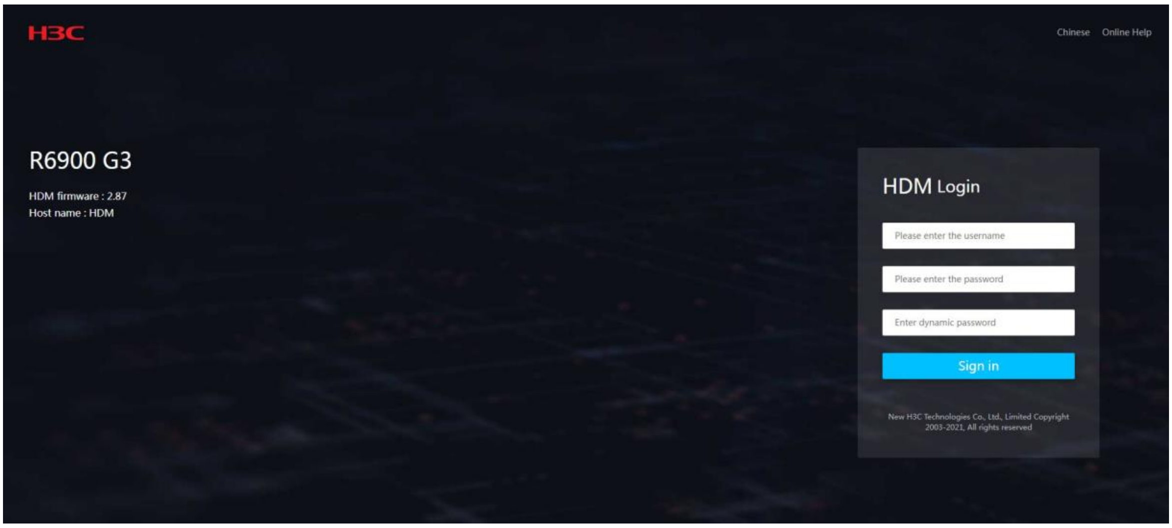
HDMはDKEYトークンをサポートしており、ワンタイムパスワード(OTP)サーバーとコラボレーションしてユーザーログインの2要素認証を提供できます。DKEYトークンはGMアルゴリズムもサポートしており、GMアルゴリズムの認証を取得しています。この機能が構成されている場合、ユーザーはHDMにログインするために、携帯電話またはハードウェアトークンから取得した正しいユーザー名、静的パスワードおよび動的パスワードを入力する必要があります。静的パスワードはOTPサーバーでの認証を通過する必要があります。

図75 二要素認証のネットワーク図



Two-Factor認証を有効にすると、図76に示すように、HDMログインページに動的パスワードの入力ボックスが追加されます。

図76 Two-Factor認証のHDMログインページ



WebサービスとTelnetサービスは、二要素認証をサポートします。

Two-Factor認証で使用してください。二要素認証を有効にすると、SSH、VNC、IPMI、SNMPv3、Redfishなどの一部のインターフェイスとサービスが無効になります。

信頼のシリコンルート

インテルプラットフォームファームウェアレジリエンス(PFR)は、ファームウェアの保護と検査を提供することにより、システムセキュリティーの信頼性を向上させます。

Intel PFRは、Intel Xeonプロセッサーおよびシステムのフ PFR CPLDにRoot of Trust(RoT)を配置し、HDM ubootの検証にシリコンRoTを使用します。HDM ubootはさらに、HDMファームウェアの検証を実行して、信頼できるシステムセキュリティーを実現します。

ハードウェア暗号化

HDMのSoCは、セキュリティ関連機能のパフォーマンスを強化するハードウェアセキュリティアクセラレーションをサポートします。アクセラレーションモジュールは、主に認証とデータの暗号化および復号化に適用されます。HDMは、AES、DES、3 DES、RC4、MD5、SHA1、SHA224、SHA256、HMAC-MD5、HMAC-SHA1、HMAC-SHA224およびHMAC-SHA256のアルゴリズムをサポートします。

ファームウェア

HDMからは次のタスクを実行できます。

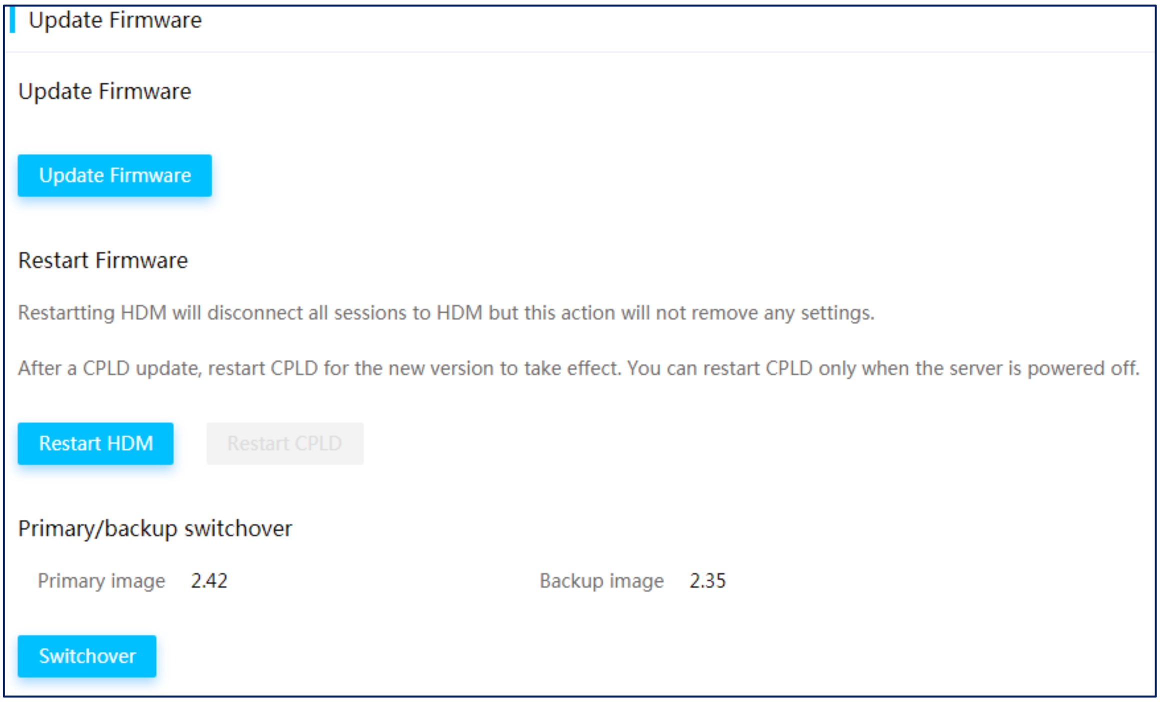
- HDM、BIOS、CPLD、LCD、およびパワーサプライのファームウェアバージョンを表示します。
- サーバーの電源切断やサービスの中断なしでHDMファームウェアを更新できます。
- BIOS、CPLD、LCD、およびパワーサプライのファームウェアをアップデートします。
- プライマリ/バックアップスイッチオーバーを実行します。

ファームウェアを更新するには、新しいイメージにベンダーの署名が含まれていて、変更されていないことを確認します。

プライマリイメージとバックアップイメージ

HDMでは、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がサポートされています。フラッシュの誤動作またはストレージブロックの破損が発生した場合は、イメージスイッチオーバーを実行してバックアップイメージでHDMを実行できます。

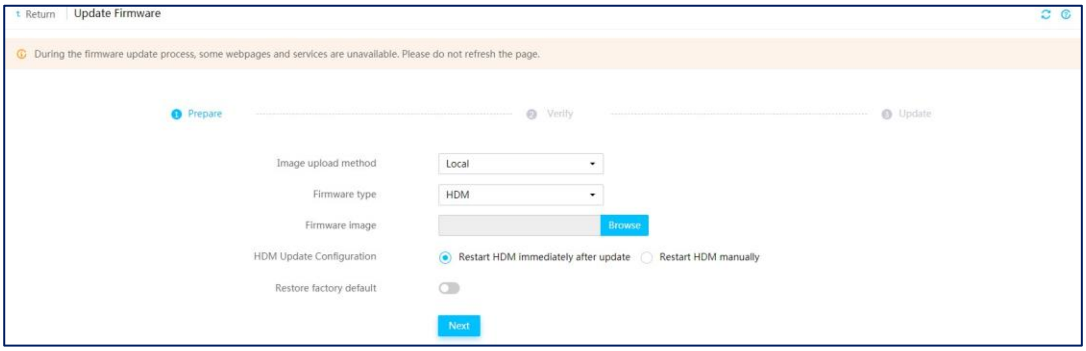
図77 プライマイメージとバックアップイメージの表示



ファームウェアの更新

HDM、BIOS、CPLD、LCD、または電源のファームウェアを更新できます。互換性のベストプラクティスとして、HDMのプライマリファームウェアイメージとバックアップファームウェアイメージを同じバージョンに更新します。

図78 Update Firmwareページ



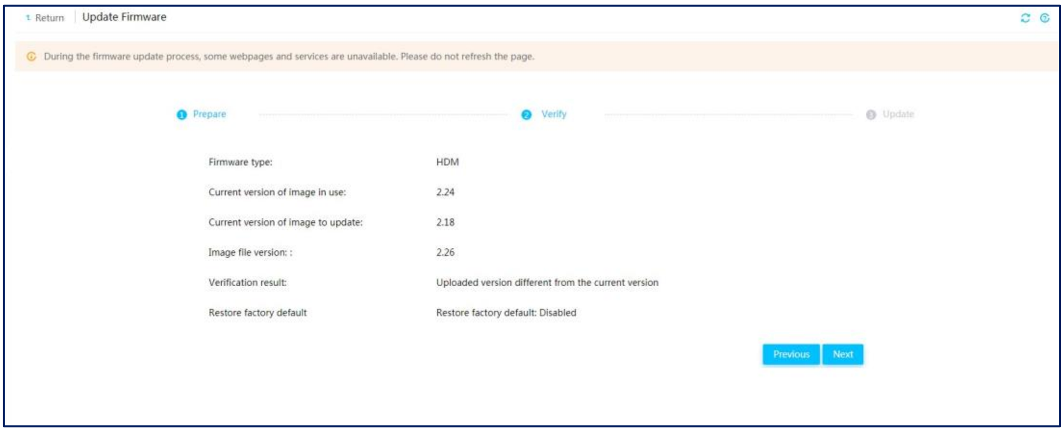
新しいHDMファームウェアを有効にするには、更新が完了したらHDMを自動的に再起動させるか、後で手動でHDMを再起動します。

新しいBIOSファームウェアを有効にするには、サーバーを即時またはスケジュールされた時間に自動的に再起動するように設定できます。または、サーバーを手動で再起動するように設定することもできます。

HDMとBIOSの両方で、ファームウェアの更新後にユーザー設定のすべての設定を削除するかどうかを選択できます。

パワーサプライのファームウェアアップデートは、DPS-2000 AB-2Gパワーサプライでのみ利用できます。

図79 ファームウェア更新設定の確認



自動BIOSアップデート

[Update Firmware]ページの[Restore factory default]フィールドで[Retain]または[Restore]を選択した場合、BIOSファームウェアイメージファイルはeMMCドライブにのみアップロードされます。サーバーを再起動すると、eMMCドライブからイメージファイルを取得してBIOSアップデートが自動的に実行されます。

構成管理

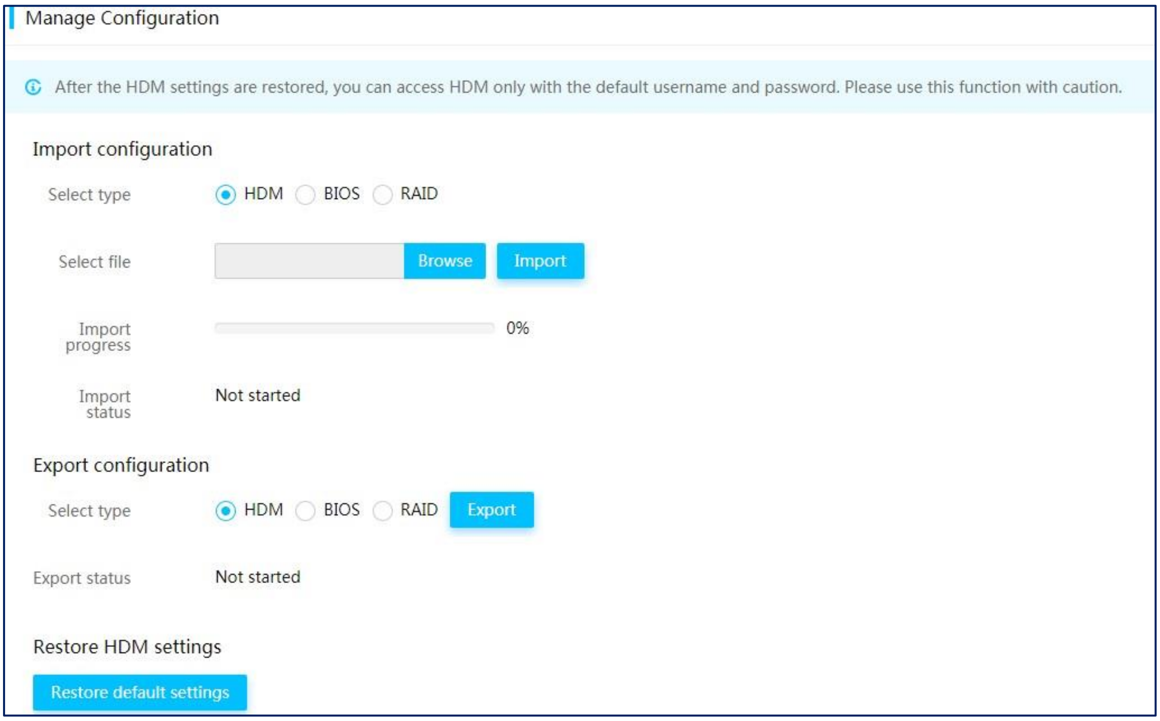
設定のインポートとエクスポート

コンフィギュレーションファイルを使用してHDM、BIOS、またはRAID設定をインポートおよびエクスポートし、工場出荷時のデフォルトHDM設定を復元するには、次の作業を実行します。

この機能には、次の利点があります。

- **アウトオブバンド管理**: HDM、BIOS、およびRAIDの設定をアウトオブバンド方式で設定できます。コンフィギュレーションファイルには、コンフィギュレーション項目の完全なセットが用意されています。
- **読み取り可能および書き込み可能コンフィギュレーションファイル**: 複数のサーバーのコンフィギュレーションファイルの設定項目を表示、編集、および保存できます。
- **使いやすさ**: 設定ファイルの管理が容易で、管理効率が向上します。
- **高速インポート**: 構成ファイルをインポートするのにわずか2分、HDM、BIOS、RAID構成をすべてインポートするのにわずか6分かかります。
- **強力な構成のカスタマイズ**: HDMは100以上の構成可能アイテムをサポートし、BIOSは1000以上の構成可能アイテムをサポートします。RAIDレベル0、1、5、6、10を構成することもできます。

図80 Import/Export Configページ



構成ファイルは、次のシナリオで適用できます。

- 設定項目をまとめて編集するには、設定ファイルをエクスポートし、設定項目を編集してから、設定ファイルをインポートします。
- 同じモデルの複数のサーバーを設定および展開するには、これらのサーバーに同じ設定ファイルを適用します。
- システムボードを交換した後は、すぐにユーザー設定の設定を適用するか、工場出荷時のデフォルト設定に戻してください。

HDMのデフォルト設定への復元

HDMはデフォルトへの復元をサポートします。

付録

G3サーバーとG5サーバーの機能の違い

機能	G3サーバー	G5サーバー	備考
LCDディスプレイ	サポート対象	サポート対象	一部のラックサーバーでサポート
[診断]パネル	サポート対象	サポートされていません	該当なし
セキュリティベゼル	サポートされていません	サポート対象	一部のG5ラックサーバーでサポート
iHDT	サポートされていません	サポート対象	一部のG5 AMDサーバーでサポート
USB Wi-Fi	サポートされていません	サポート対象	シャーシの耳にUSB Type-Cコネクターがある G5サーバーでサポートされます。
サービス用USBデバイス	サポートされていません	サポート対象	シャーシの耳にUSB Type-Cコネクターがある G5サーバーでサポートされます。
信頼のシリコンルート	サポートされていません	サポート対象	G5 Intelサーバーでサポート