H3C HDM2
テクノロジーホワイトペーパー

内容

はじめに 4
対象ユーザー 4
改訂履歴 4
適用製品 5
概要 6
HDMについて 6
参考：HDMシミュレーター 7
HDMの全体的なアーキテクチャ 8
HDM機能 10
製品の特長 12
アクセス機能と管理インターフェイス 12
サーバーアクセス 12
管理インターフェイス 13
HDMネットワーク構成 18
HDM時間設定 22
DNS 23
サーバー導入機能 25
背景 25
導入機能 26
技術的なポイント 26
コンフィギュレーション管理 28
ファームウェアのインストール 33
デバイスの移行および廃棄に関連する機能 37
アプリケーションシナリオ 37
サーバー管理機能 38
背景 38
技術的なキーポイント 39
アプリケーションシナリオ 43
サーバー監視機能 43
背景 43
技術的なキーポイント 44
アプリケーションシナリオ 48
SDSログ 48
スマート診断システム 49
背景 49
アーキテクチャ 50
技術的なキーポイント 51
予測アラーム 57
リモート診断 58
サポートされている障害のリスト 58
アプリケーションシナリオ 62
ホスト監視機能 63
ホストの運用能力の最適化ポイント 63
ホストのライフサイクル管理 63
ブートログ機能 65
ホストの再起動の理由 66
システムリソースの監視 66
ホストウォッチドッグメカニズム 69
最初のSMS 69
容量予測 71
ホストのセキュリティ 71
メンテナンス 72
操作ログ 72

イベントログ 72
シリアルポート接続 73
ブラックボックス(ログのダウンロード) 74
インテリジェントなセキュリティベゼル 75
BSoDスクリーンショット 76
ビデオ再生 77
アラートポリシー 77
ASD 78
ACD方式 79
iHDT 79
アラームの設定 79
電源ブラックボックス 81
HDMシステム保全性 81
ローカルO&M 82
USB Wi-Fi対応 82
サービスUSBデバイス 82
コンポーネント管理 83
FRUおよび資産情報の管理 83
ネットワークアダプターの管理 83
FC HBAの管理 84
GPU管理 84
インテル(R)オンデマンド 85
ストレージ管理 85
ストレージコントローラーの管理 86
論理ドライブの管理 87
ストレージコントローラーの物理ドライブ管理 88
NVMeドライブ 89
Marvell M.2ストレージコントローラー管理 90
組み込み型ドライブ管理 91
ドライブの位置LED 92
ストレージの保守性 93
ストレージプロトコルスタック 97
GPU管理 97
基本的なGPU情報の表示 97
GPUモジュールのアウトバンドアップグレード 98
GPUノードの消費電力上限 99
GPUモジュールの障害診断 99
エネルギー効率管理 99
サーバーの電源のオン/オフ 100
電源投入後のサーバーシステム起動ポリシーの設定 100
消費電力上限 101
電源装置の動作モード 103
コールドスタンバイ パワーサプライモニター 103
ダイナミックアクティブ/スタンバイ電源モード 104
過去の電力消費統計 104
省エネ設定 105
ファンの管理 105
パフォーマンスの最適化 106
リモートコントロール 109
キーボード、ビデオ、およびマウス 109
H5 KVM(キーボード、ビデオ、マウス) 109
KVM起動モード 110
仮想メディア 111
KVMからのスクリーンキャプチャ 111
KVMからのビデオ録画 112
ハードウェアのサポート 113

VNC ... 113
VNCについて ... 113
VNCセッションモード ... 113
VNCセッションの表示 ... 114
VNCの設定 ... 114
JViewerクライアント ... 114
セキュリティ管理 ... 115
セキュリティメカニズム ... 115
シャーシ侵入検知 ... 117
ハードウェア暗号化 ... 117
信頼のシリコンルート ... 118
ファームウェアのセキュリティ ... 119
リンクのセキュリティ ... 119
SDSログ ... 120
ファイアウォール ... 120
サービス管理 ... 121
SSL証明書の管理 ... 121
SSHキーペア ... 122
アカウントのセキュリティ ... 123
権限管理 ... 124
Two-Factor認証 ... 125
セカンダリ認証 ... 128
LDAPドメインユーザー ... 128
ADドメインユーザー ... 129
Kerberos ... 130
セキュリティ監視情報 ... 132
安全なデータ消去 ... 133
システムロック ... 134
略語 ... 136

はじめに

対象ユーザー

このマニュアルは、次の読者を対象としています。

- サーバーのプリセールスエンジニア
- 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
- ネットワーク管理者。

改訂履歴

日付	改訂版	説明	改訂者
2024年2月22日	V1.5	「OTP認証」が追加されました。	プラットフォームソフトウェア
2024年1月12日	V1.4	「Black box(log download)」が追加されました。	プラットフォームソフトウェア
2023年12月29日	V1.3	1. 次の機能のサポートが追加されました。 o HTTP 2.0のサポート o 2つのWebテーマ間の切り替え o IPv4およびIPv6スタティックルートコンフィギュレーション o BIOSブートサブオプションの設定 o HDMとBIOSアップグレードのリスクプロンプト o Intel On Demandのサポート o 電源ブラックボックス o HDMシステム保全性 o メモリーの偽造防止 o LDAP証明書のインポート o OSの迅速なインストール o PCIe帯域外管理を介したMCTPに対するAMDのサポートの追加 o NVMe-MIコントローラーの帯域外管理と残り寿命表示 2. 全体的なワークフローの更新 3. 編集された障害診断、MRT、およびその他の機能	プラットフォームソフトウェア
2023年10月24日	V1.2	古いソフトウェアバージョンに関連するクリアされた情報	プラットフォームソフトウェア
2023年10月19日	V1.1	「HDM全体アーキテクチャ」と「信頼のシリコンルート」にBMCチップのパラメーター情報を追加した。	プラットフォームソフトウェア
2023年7月25日	V1.0	最初のリリース	プラットフォームソフトウェア

適用製品

このマニュアルは、次のようなH3C G6サーバーに適用されます。

- H3C UniServer B5700 G6
- H3C UniServer R 3950 G6
- H3C UniServer R4300 G6
- H3C UniServer R4700 G6
- H3C UniServer R4700LE G6
- H3C UniServer R4900 G6
- H3C UniServer R4900 G6 Ultra
- H3C UniServer R4900LE G6 Ultra
- H3C UniServer R4950 G6
- H3C UniServer R5350 G6
- H3C UniServer R5300 G6
- H3C UniServer R5500 G6
- H3C UniServer R6700 G6
- H3C UniServer R6900 G6

概要

HDM(H3Cサーバー上のBMC)は、H3C UniServerシリーズサーバーのボードレベルのファームウェアです。データセンターから個々の顧客までのコンピューティングおよびストレージアプリケーションの要件を満たします。HDMは、HPC、AI、データベース、キャッシュサーバー、ファイルサーバー、ストレージサーバーなどの様々なシナリオに適用されます。数百万台のサーバー上で実行され、多数の実際のアプリケーションで検証されています。

HDM2は、HDMのアップグレードバージョンです。既存の機能を継承することに加えて、HDM2は複数のアプリケーションシナリオに最適化され、対応する互換性のある機能を提供します。デュアルコア統合の戦略をサポートするインテリジェント関連の属性が追加されます。また、メモリーのインテリジェントな修復、最大200台のデバイスの統合管理の拡張、Kerberos認証とシングルサインオン、ワンクリックでの廃棄、システム構成のロック、インテリジェントなチューニング、セキュリティ監視情報など、強化されたライセンスサービスも提供します。

便宜上、HDM2をHDMと称する。

HDMについて

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。HDMは、IPMI、SNMPおよびRedfish標準に準拠し、キーボード、ビデオおよび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および管理などの様々な機能を提供します。HDMは、表1に示す豊富な機能をサポートします。

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に対応します。
統合された管理	小規模で統一された制御を実装することにより、中小企業のサーバーの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、タッチ可能な3.5インチまたは2.5インチのLCDディスプレイがオプションで用意されています。
障害の監視と診断	保守のために障害の位置と診断を提供し、24×7デバイスの正しい動作を保証します。 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プロアクティブに報告できます。
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)が発生したときにスクリーンショットを撮るか、ビデオを録画します。
アウトオブバンドRAID管理	アウトオブバンドのRAID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、電力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	リモートサーバーのメンテナンスを容易にします。
DNS、LDAP、およびAD Kerberos	ドメイン管理およびディレクトリサービスをサポートして、サーバーネットワーク管理およびユーザー管理を簡素化します。Kerberosは、シングルサインオンを実装して、認証および認可の繰り返しを回避します。

USB Wi-Fiアダプター	外部のXiaomiまたは360ポータブルWi-Fiアダプターをサポートし、サーバーのニアフィールドメンテナンス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。

ファームウェアの更新	HDM、BIOS、CPLD、LCD(1.05より前のファームウェアパッケージ)、ドライブ、ネットワークアダプター、ストレージコントローラー、GPUモジュール、REPOパッケージなどのさまざまなアウトバンドファームウェア更新をサポートします。また、HDMのコールドパッチとホットパッチの更新もサポートしており、中断のない障害回復サービスを保証します。ファームウェア更新はファームウェアライブラリとキューをサポートしているため、オペレータは必要に応じてファームウェア更新をスケジュールでき、サービス操作への影響を最小限に抑えることができます。
ソフトウェアインベントリ	場所、名前、バージョン、更新時刻など、帯域外ファームウェアバージョン情報と帯域内オペレーティングシステムソフトウェアおよびドライバー情報の取得をサポートします。
サービスUSBデバイス	ログのダウンロードをサポートし、オンサイトでのメンテナンスと管理をシンプル化します。
資産管理	資産管理を合理化
セキュリティ管理	サービスアクセス、ユーザーアカウント、データ送信、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/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、シリコンルートオブトラスト、カスタムユーザー権限をサポートします。
ワンクリックでの廃棄	ワンクリックでサーバーコンポーネントをデフォルトにリストアし、安全な廃棄を実現します。

参考：HDMシミュレーター

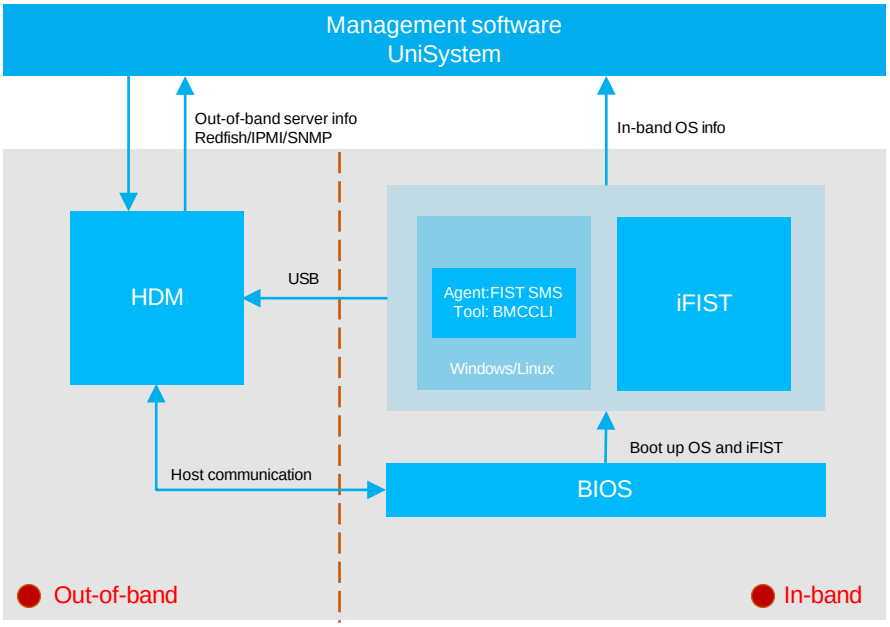
以下のサイトでHDMシミュレーターを提供していますので、お試しください。

https://simulator.h3c.com/simulator-hdm/hdm

HDMの全体的なアーキテクチャ

H3Cのサーバー管理ソフトウェアは、図1に示すとおりです。HDMは、ホストサーバーから独立して動作する組み込みシステムです。サーバー全体の帯域外管理に使用され、BIOS、UniSystem、iFIST、FIST SMS、hRESTなどのソフトウェアと連携して、サーバーの導入、監視、保守を行います。HDMは、インテリジェントなサーバーO&Mおよびライフサイクル管理の中核および基盤として機能します。

図1 H3Cサーバー管理ソフトウェア



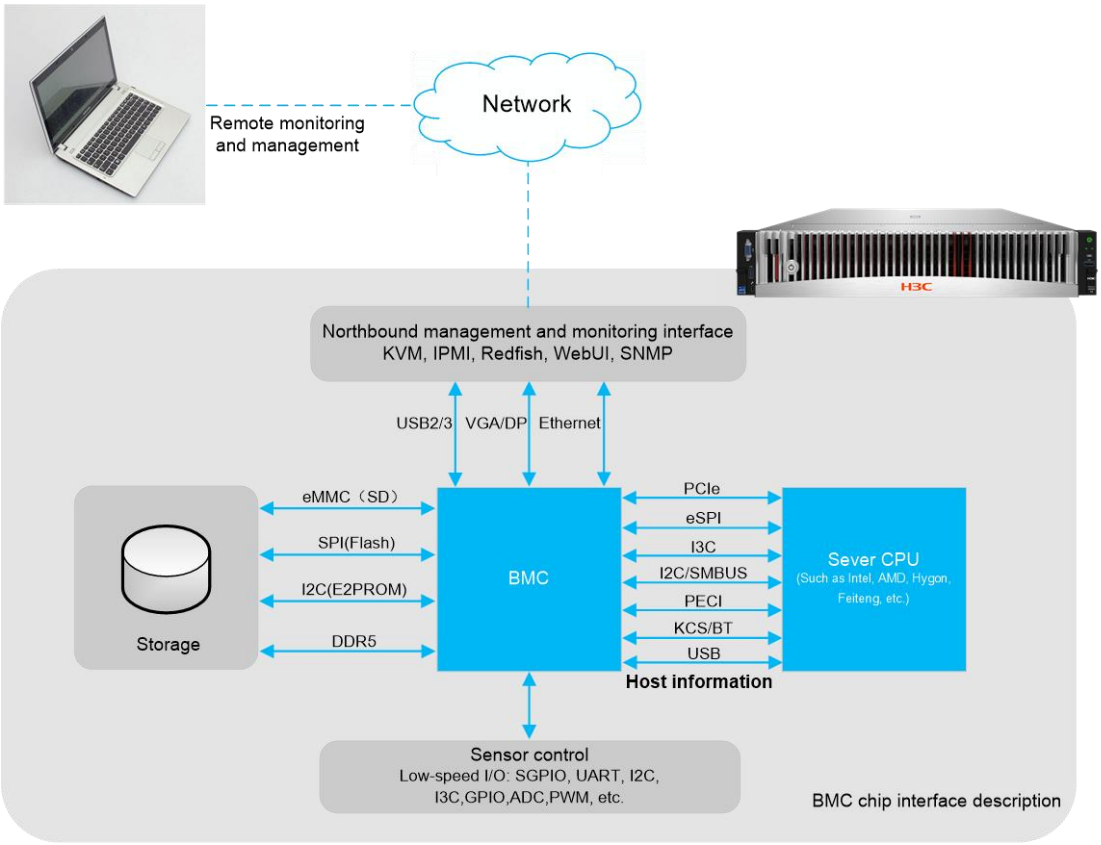
HDMのシステムアーキテクチャは、図2に示すとおりです。HDMは、サーバーハードウェアコンポーネントを効果的に管理するために、プロセッサーの主周波数1.2 GHzと合計メモリーサイズ1 GBのサーバー固有のシステムオンチップ(SoC)を採用しています。SoCは、KVM、64 MBのローカルVGAディスプレイ、専用および共有ネットワークポート、および次のようなさまざまなボードレベルの管理機能と周辺機器インターフェイスをサポートしています。

- **KVMリモートコントロール**: KVMモジュールを使用して、ビデオデータとキーボードおよびマウス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、圧縮し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およびマウスのデータを受信し、シミュレートされたUSBキーボードおよびマウスデバイスを使用して、そのデータをホストシステムに送信します。
- **LPC/eSPI通信およびIPMI管理**: サーバーとの通信用に従来のLPC/eSPI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。このインターフェイスを介して、ネットワーク経由でIPMI、Redfish、またはSNMPを使用してリモート管理を実装できます。
- **NCSIおよびVLANのサポート** :Network Controller Sideband Interface(NCSI;ネットワークコントローラー側波帯インターフェイス)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リダイレクト、テキストコンソールリダイレクト、リモート仮想メディア(オプ

ティカルドライバー、ドライブ、および端末のユーザーをサーバーにマッピングするために使用)、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。

- **センサーベースの監視と管理**: センサーを通じてサーバーの温度と電圧を監視し、ファンと電源(PSU)をインテリジェントな方法で管理します。
- **HDMに取り付けられた2枚のSDカード(ナンドフラッシュ):** SDカード1は、一部のサーバーではサポートされていないiFISTイメージを保存するためのカードとして挿入されます。SDカード2は、構成情報、操作ログ、イベントログなどのサーバーの操作および診断ログを記録するために使用されます。

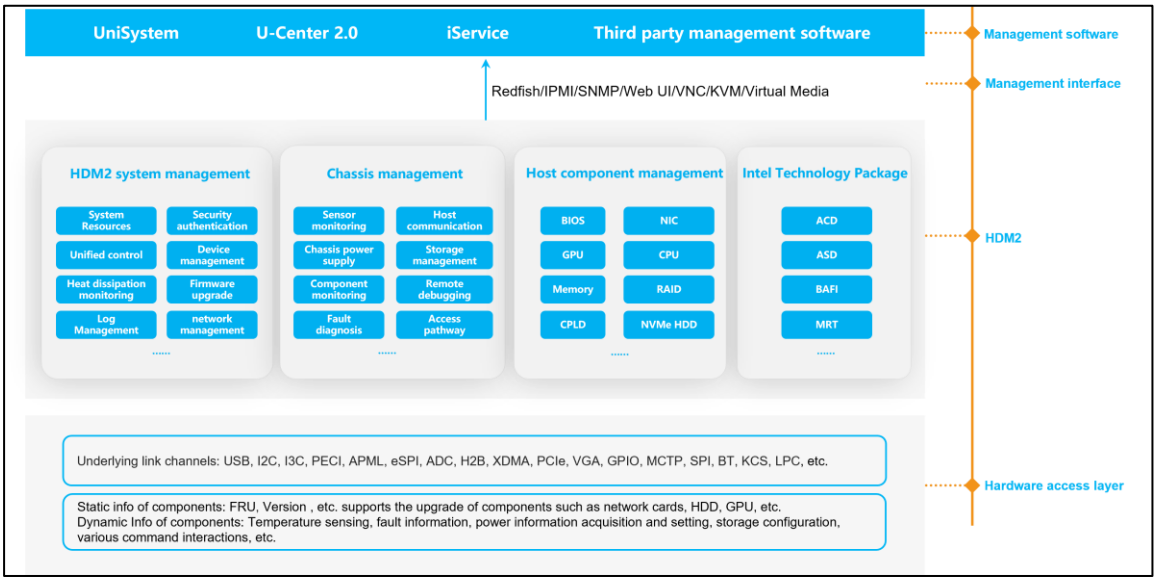
図2 HDMシステムのアーキテクチャ



HDMの主なソフトウェアアーキテクチャは図3に示すとおりです。HDMのソフトウェア機能には主に次のものが含まれます:

- **シャーシ管理**: センサー、電源装置、およびその他のコンポーネントを監視および管理します。
- **BMCシステム管理**: セキュリティ管理、時間管理、およびネットワーク管理を提供します。

図3 HDMソフトウェアアーキテクチャ



HDMは、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は、認証メカニズムと高度に安全な暗号化アルゴリズムを採用して、アクセスと伝送のセキュリティを確保します。

HDM機能

H3Cサーバーの全体的な戦略は、インテリジェントコンピューティングを強化するための組込みインテリジェンスを実装することです。この戦略を実装するために、AIプラットフォーム、多変量コンピューティングシステムプラットフォーム、およびインテリジェント管理プラットフォームの3つの主要なアンダーレイプラットフォームが使用可能です。これらのプラットフォームでは、サーバーは負荷を感知し、コンピューティングパワー要件を分析し、コンピューティングパワーを効率的に生成および集約し、アプリケーションを完全にデプロイするためにコンピューティングパワーをインテリジェントにスケジュールできます。サーバーの観点から見ると、HDMは、サーバーの日常の運用と保守の様々な側面に焦点を当てることによって、インテリジェント管理プラットフォームの実装をサポートします。HDMは、インテリジェントなデプロイ、チューニング、省エネルギー、診断、廃棄など、データセンターサーバーのライフサイクル全体にわたってインテリジェントな管理を提供します。これにより、企業の運用効率の向上と運用コストの削減に効果的に役立ちます。お客様は、特定のビジネスニーズに応じて柔軟にサーバーを構成およびデプロイし、独自の専用運用環境を作成し、対応するファームウェアサポートを提供してサーバーハードウェアの機能を最大化できます。サーバーのファームウェアには、主に次のタイプがあります。

- **サーバーホスト**: すべてのサーバーモデルでBIOSを使用し、一部のサーバーモデルではOS、iFIST、およびFIST SMSを使用します。
- **ハードウェア**: カードおよびコンポーネントのファームウェア。
- **帯域外管理ファームウェア**: HDM。

サーバー上のファームウェアは、ハードウェアリソースの管理インターフェイスおよびコンポーネントの外部アクセスインターフェイスとして機能します。ユーザーの観点から見ると、ファームウェアは、サービス要件を満たすだけでなく、次のようないくつかの機能を備えている必要があります。

- **アクセス機能と管理インターフェイス**: ユーザーがサーバーにアクセスする方法と、サーバーによって外部にエクスポートされたインターフェイスについて説明します。

- **導入**: オンボーディング、管理、移行、廃棄、およびパラメーター設定とファームウェアメンテナンスに関連するサポート機能を含む、デバイスのライフサイクル全体のサービスを対象とします。導入および管理機能には、主にデバイスのオンボーディング、設定、システム導入、ファームウェア更新、デバイスの移行、および廃棄が含まれます。
- **管理**: 資産管理、検査、デバイストポロジ検出、ファームウェア情報、デバイス管理、ハードウェアパラメーター設定、BIOSおよびBMC設定など、サーバーおよびサーバー内のさまざまなコンポーネントに対する外部管理機能を提供します。
- **監視**: センサー、ログサブシステム、イベントタイプ(特にアラームイベント)のレポートチャネル、システム監視ステータス、コンポーネントアラームおよび早期警告アラームのチャネル、ホスト監視機能など、サーバーの動作ステータスの外部監視を提供します。
- **診断**: 異常の関連するコンテキスト情報を収集し、障害診断のための複数の組み込みルールを利用して、障害ポイントを自動的に特定し、異常が発生した場合にサーバーに組み込まれた監視機能と連携して障害のあるコンポーネントを特定します。主な機能には、アラームソースの監視、障害処理メカニズム、障害レポート、および
保守容易性関連の機能
- **セキュリティ**: サーバーにセキュリティ機能を提供します。
- **パフォーマンス**: サーバーの帯域外応答機能が向上します。このドキ

ュメントでは、次の点に重点を置いています。

- H3Cサーバーが提供する対応ソリューションを、サーバーの使用方法から紹介します。
シナリオと要件。
- サーバーシャーシと主要なテクノロジーの観点から、各テクノロジーの背後にある原理を説明します。
- 各ソリューションとテクノロジーのアプリケーションシナリオを簡単に説明します。

製品の特長

アクセス機能と管理インターフェイス

サーバーアクセス

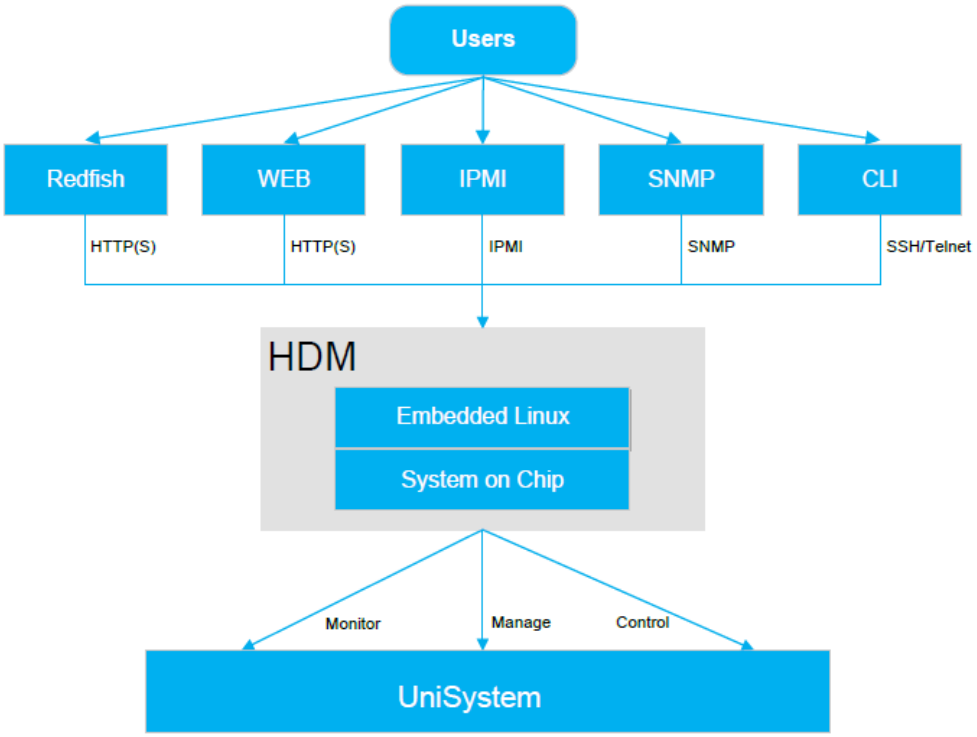
異なるシナリオにおける異なるユーザーの異なる焦点を考慮すると、H3Cサーバーは、さまざまな管理インターフェイスとアクセス機能を提供します。サーバークセス機能には、次のものがあります:

- **使いやすさ**: 便利で使いやすい構成機能により、ユーザーはすぐに作業を開始できます。
- **セキュリティ**: さまざまな手段を使用して、複数のセキュリティ研究所によって検証された各リンクのセキュリティを確保します。
- **ハイパフォーマンス**: 起動とインターフェイスアクセスの両方に関して、究極のパフォーマンスを継続的に追求します。
- **複数のアクセス方法**: 複数のアクセス方法は、さまざまなシナリオのニーズを満たします。
- **シナリオベースの最適化**: セキュリティや信頼性など、アプリケーションの構成を強化し、ユーザーに的を絞った最適化を容易にします。

アウトオブバンド監視

サーバーを監視する方法には、インバンドとアウトオブバンドがあります。HDMにアクセスするためのアウトオブバンドインターフェイスには、主にWebベースのHTTP/HTTPS、Redfish、IPMI、SNMPおよびCLIが含まれます。HDMアウトオブバンドインターフェイスの方法を図4に示します。

図4 HDMアウトオブバンドインターフェイス



使いやすさ

使いやすさに関して、HDMによって実装される主な機能は次のとおりです:

- UniSystemと併用すると、接続されているサーバーデバイスが自動的に検出されます。
- デバイスのデフォルトIPアドレスに基づくアクセス。

複数のアクセス方法

アクセスの多様性に関しては、サーバーは手動手段を通じてデバイスに直接アクセスする機能を提供します。提供される機能は次のとおりです:

- 共有ポート、専用ポート、またはUSB Wi-Fiを介したHDM Webページへのアクセス。
- VGA+キーボードを使用したBIOSへのアクセス
- デバイスインターフェイス(シリアルポート)を介したBIOSポートへのアクセス。
- デバイスインターフェイス(シリアルポート)を介したHDMシェルへのアクセス。

サーバーは、管理インターフェイスを介してHDMおよびBIOSにアクセスする機能も提供し、次の機能を提供します:

- OSのインターフェイスを介してBIOSおよびHDMにアクセスすることにより、ファームウェアのアップグレード、構成管理、ログのダウンロードなどの機能を含む、サーバーのインテリジェントなインバンド展開を実現できます。
- 帯域外ネットワーク経由でIPMIツールを使用してHDMにアクセスすると、外部管理ツールとの統合が可能になります。
- Redfishインターフェイスを使用すると、アウトオブバンドネットワーク経由でHDMにアクセスし、外部管理ツールを統合できます。
- 統合制御機能を使用すると、アウトオブバンドネットワークを介して他のデバイスのHDMにアクセスできる。
- BIOSは、帯域内ネットワークを介してネットワークサービスを使用して、対応するリソースにアクセスする。
- 対応するネットワークサービスによって提供されるリソースには、KVMインターフェイスを介してアクセスできます。

さらに、このデバイスは、LED、LCD表示パネル、およびユーザーが現場で機器の動作状態を確認するためのセキュリティベゼルを提供します。

特定のアクセス方法は製品によって異なる場合があることに注意してください。詳細は、対応する製品マニュアルを参照してください。

管理インターフェイス

HDMは、さまざまなシナリオのアクセスニーズを満たすために、サーバーハードウェアインターフェイスに基づいてインターフェイスをさらに拡張する。

Web管理インターフェイス

HDMは、HTTPSに基づくWebベースのビジュアル管理インターフェイスを提供します。

- これにより、ユーザーは簡単なインターフェイス操作でセットアップとクエリのタスクをすばやく完了できます。
- リモートコンソールを使用すると、OSの起動プロセス全体の監視、サーバー上でのOSタスクの実行、およびサーバー上でのオプティカルドライブ/フロッピードライブのマッピングを行うことができます。
- HDMはHTTP 2.0もサポートしています。HTTP 1.1と比較して、HTTP 2.0はWebパフォーマンスを大幅に改善し、ネットワークレイテンシを削減して、伝送の信頼性とセキュリティを向上させ

ます。

- 英語と中国語を切り替えることができます。HDMは、ミニマリストホワイトとスターリーブルーの2つのスキンテーマをサポートしています。

図5 ミニマリストホワイトのHDMホームページ

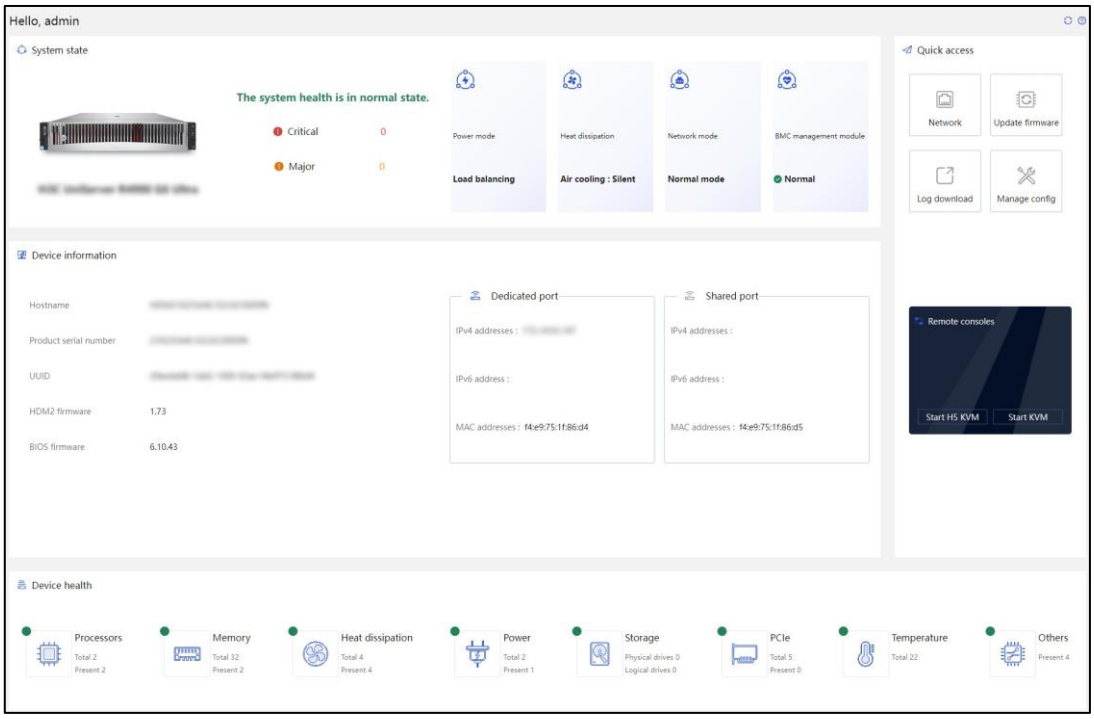
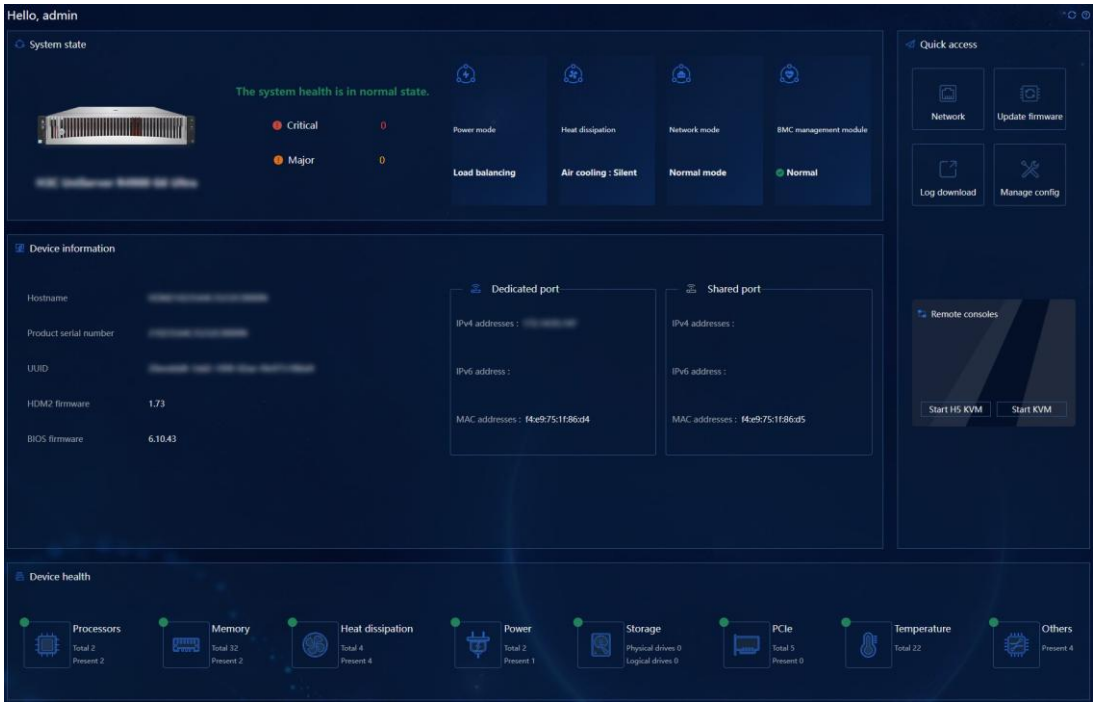


図6 starry ブルーのHDMホームページ



HDM Webのログインインターフェイスを開くには、HDMのネットワークポートのIPアドレス(IPv4または

IPv6)またはドメインアドレスをブラウザのアドレスバーに入力し、自分のアカウントでログインします。

サポートされているブラウザには、Firefox 90以上、Chrome 80以上、Edge 108以上、Safari 14以上が含まれる。

IPMI管理インターフェイス

HDMは、IPMI 1.5/IPMI 2.0仕様と互換性があります。データセンター管理インターフェイス(DCMI、サポートされているデータセンター管理インターフェイス)を使用すると、LPC/eSPIチャネルまたはLANチャネルに基づくサードパーティツール(ipmitoolなど)、またはUSBチャネルに基づくBMCCLIツールを使用して、サーバーを効果的に管理できます。

- **LPC/eSPIチャネル** :KCS/BTプロトコルを実行します。ipmitoolおよびその他のツールは、サーバーのローカルオペレーティングシステムで実行する必要があります。
- **LANチャネル**: UDP/IPプロトコルを実行します。ipmitoolおよびその他のツールを使用すると、サーバーをリモートで管理できます。
- **USBチャネル**: BMCCLIプロトコルを実行します。BMCCLIツールは、サーバーのローカルオペレーティングシステム上で実行する必要があります。

BMCCLIツールおよびサードパーティ製ツールは、WindowsおよびLinuxシステムをサポートしています。

HDM2でサポートされているIPMI機能の詳細については、H3C HDM2 IPMI Basics Command Referenceを参照してください。

SNMP管理インターフェイス

Simple Network Management Protocol(SNMP;簡易ネットワーク管理プロトコル)は、Management Process(NMS;管理プロセス)とAgent Process(Agent;エージェントプロセス)間の通信プロトコルです。SNMPは、標準化された管理フレームワーク、通信の共通言語、対応するセキュリティ、およびネットワーク環境でデバイスを監視および管理するためのアクセスコントロールメカニズムを指定します。

SNMPには、次の技術的な利点があります。

- トランスポート層プロトコルとしてUDPを使用する、TCP/IPベースの標準プロトコル。
- 自動化されたネットワーク管理。ネットワーク管理者は、SNMPプラットフォームを使用して、ネットワーク上のノードに関する情報の取得、情報の変更、トラブルシューティング、障害の診断、キャパシティプランニングの実行、レポートの生成を行うことができます。
- 異なるデバイス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するため、管理対象デバイスの物理特性や実際のネットワークタイプに比較的依存しない管理タスクが可能になり、異なるベンダーのデバイスの管理が可能になります。
- アクティブな通知モードと組み合わされた単純な要求-応答モード、タイムアウトおよび再送信メカニズム。
- 少数のパケットタイプと単純なパケット形式により、解決と実装が容易になります。
- SNMPv3バージョンは、認証および暗号化セキュリティメカニズムに加えて、ユーザベースのアクセスコントロール機能を提供し、セキュリティを強化します。
    - HDMは、SNMP Get/Set/Trap操作をサポートするSNMPベースのプログラミングインターフェイスを提供します。サードパーティの管理ソフトウェアは、SNMPインターフェイスをコールすることにより、サーバーを簡単に統合および管理できます。SNMPエージェントは、v1/v2c/v3バージョンをサポートします。
    - SNMPエージェントは、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、電力統計データ、資産情報、熱管理、ファームウェアバージョン情報、およびネットワーク管理に関するインターフェイスクエリーを提供します。

Redfish管理インターフェイス

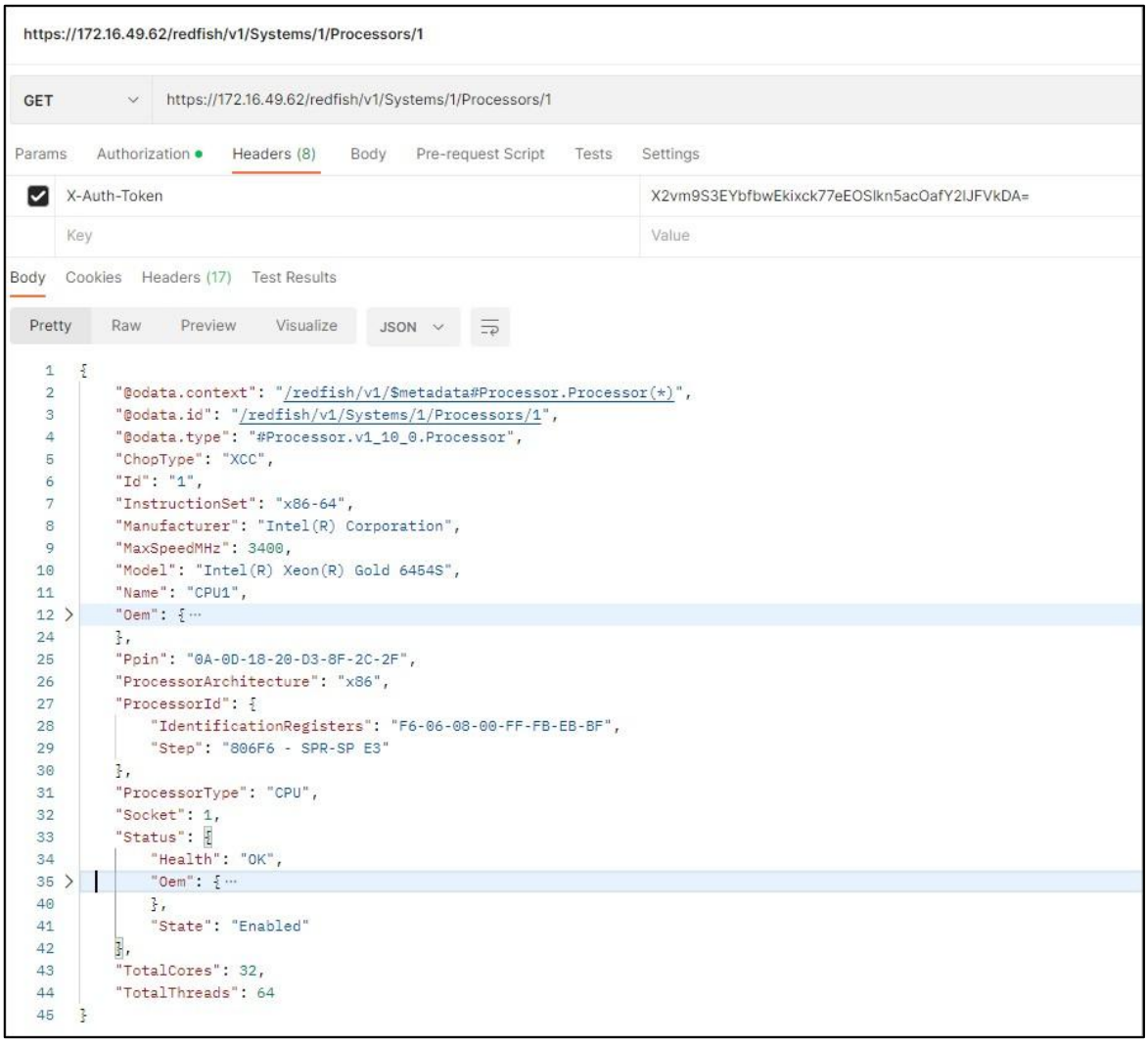
Redfishは、RESTfulインターフェイスを使用してデバイス管理を実現するHTTPSサービスに基づく管理標準である。各HTTPS操作は、UTF-8でエンコードされたJSON形式(JSONはキーと値のペアで構

成されるデータ形式)でリソースまたは結果を送信または返す。このテクノロジーには、開発の複雑さを軽減し、簡単に実装して使用でき、拡張性を提供するという利点があると同時に、設計の柔軟性も可能にする。

RedfishはREST APIとソフトウェア定義サーバー(データモデル)を使用しており、現在は標準組織であるDMTF(www.dmtf.org)によって管理されている。

HDMはRedfish 1.15.1仕様をサポートしており、ユーザー管理やサーバー情報および管理モジュール情報の取得など、一般的なHDMおよびBIOS設定を実装できます。図7に示すように、Redfishクライアントは HTTP要求を送信し、TokenまたはBasicを介して認証し、データベースからデータを取得し、読み取り結果を返します。データベースは、SELおよびIPMIを介してリアルタイムで内容を更新します。

図7 Redfishインターフェイスの操作例(プロセッサー情報の照会)



セキュアシェル(SSH)

HDMはSSHv2プロトコルをサポートし、安全なリモート管理を提供します。柔軟なシステム構成のための基本的な管理コマンドをサポートし、SSHを無効にしてセキュリティを強化できます。

HDM統合制御

HDM統合制御は、小規模なサーバーの集中管理を可能にし、中小企業のサーバー運用保守管理を簡素化する。HDM統合制御は、図8に示すように、主に以下の機能を提供する。

- **デバイスの追加**: 最大10台のデバイス(IPv6アドレスはサポートされていません)のシングルサー

バーまたはバッチサーバーの追加をサポートします。ライセンス認可を取得すると、この機能は最大200台のデバイスをサポートします。

- **デバイスの削除**: デバイスの個別削除またはバッチ削除をサポートします。
- **ステータスクエリ**: 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ステータスなど、デバイスの基本的なステータス情報の表示をサポートします。
- **電源管理**: 電源オン、電源オフ、再起動、その他の操作を含むデバイスの電源操作をサポートします。
- リモートアクセス:HDMおよびH5 KVMコンソールにアクセスするためのジャンプリンクを提供します。

図8 統合された制御インターフェイス

LCD表示画面

H3Cラックサーバーは、サーバー情報の表示または設定に使用される3.5インチまたは2.5インチのタッチ可能なLCD画面で設定できます。これにより、ローカルメンテナンスのシンプルさが向上し、オンサイトでの障害の特定と修復が迅速化されました。LCD画面ディスプレイは、中国語と英語の切り替えをサポートしています。

LCD画面には、主に次の機能があります。

- **情報ページ**: 図9に示すように、製品名、製品シリアル番号、およびHDM/BIOSファームウェアのバージョン番号が表示されます。
- **Statusページ**: サーバーの全体的なヘルスステータスとログ情報、およびプロセッサー、メモリー、ストレージ、ファン、電源、温度センサー、シャーシの消費電力などのコンポーネントを表示します。
- **モニタリングページ**: 吸気温度とCPU温度をリアルタイムで表示します。
- **設定ページ**: HDM管理インターフェイスネットワークの設定や管理者アカウントの復元などの操作をサポートします。

各コンポーネントは、Webと同じカラー表示ルールに従って、ステータスと正常性を示すために異なるカラーで表示されます。

- 緑: デバイスは正常です。
- オレンジ: デバイスに重大なアラームが発生しています。
- 赤: デバイスに緊急アラームがあります。
- グレー: デバイスが所定の位置にありません。

図9 LCDディスプレイ

HDMネットワーク構成

サーバーの一元的な運用とリモート運用のために、HDMは複数のネットワーク構成モードをサポートし、次のようなネットワーク構成の迅速なアクティブ化を保証します。

- 共有ポート、専用ポート、およびUSB Wi-Fiを介したネットワークアクセスを提供します。
- ポートのアクティブ/スタンバイモードと自動共有ポート選択を設定します。
- IPv4、IPv6、およびドメイン名のサポートを提供します。
- デバイスが起動すると、LLDP、SSDP、およびフリーARPメッセージが自動的に送信され、デバイスの外部識別と管理が容易になります。
- IPv4およびIPv6スタティックルートの設定をサポートして、さまざまなアプリケーションシナリオの要件を満たすクロスセグメントアクセスのためのより柔軟なネットワーク戦略を実現します。

HDMは、セキュリティの観点から次の機能を提供します。

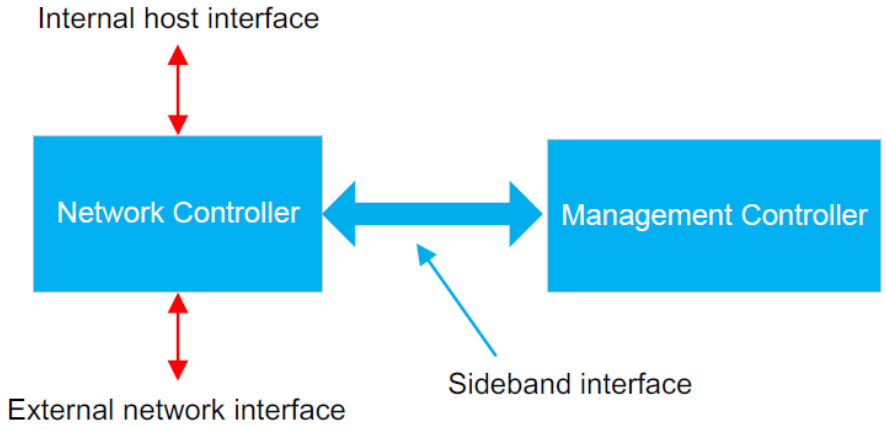
- 共有ポートブロックのサポート。
- ファイアウォールメカニズムを有効にするためのサポート。
- アプリケーションレベルのセキュリティメカニズムを提供します。

側波帯管理とNCSI技術

側波帯管理(共有ネットワークポート)とは、ネットワークコントローラー側波帯インターフェイス(側波帯NCSI)を使用して、ホストシステムの物理NICを管理システムと共有することです。これにより、1つのNICを介して管理操作とサービス処理を同時に行うことができ、ネットワーク構成が簡素化され、スイッチポートが節約されます。セキュリティ上の理由から、VLANテクノロジーを使用して管理とサービスを異なるネットワークセグメントに分離する必要があります。

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。NCSIバスは、RMIIバスと多重化され、RMIIバスの上にNCSIプロトコルを定義するネットワーク通信バスです。ネットワークコントローラー(NC)は、内部ホストインターフェイス、外部ネットワークインターフェイス、および外部通信用の側波帯インターフェイスに分割されます。BMCは、管理コントローラーとして、NCSI制御コマンドをNCに送信し、図10に示すように、NCおよび外部ネットワークインターフェイスを介してネットワークデータパケット通信を実現できます。

図10 側波帯管理図

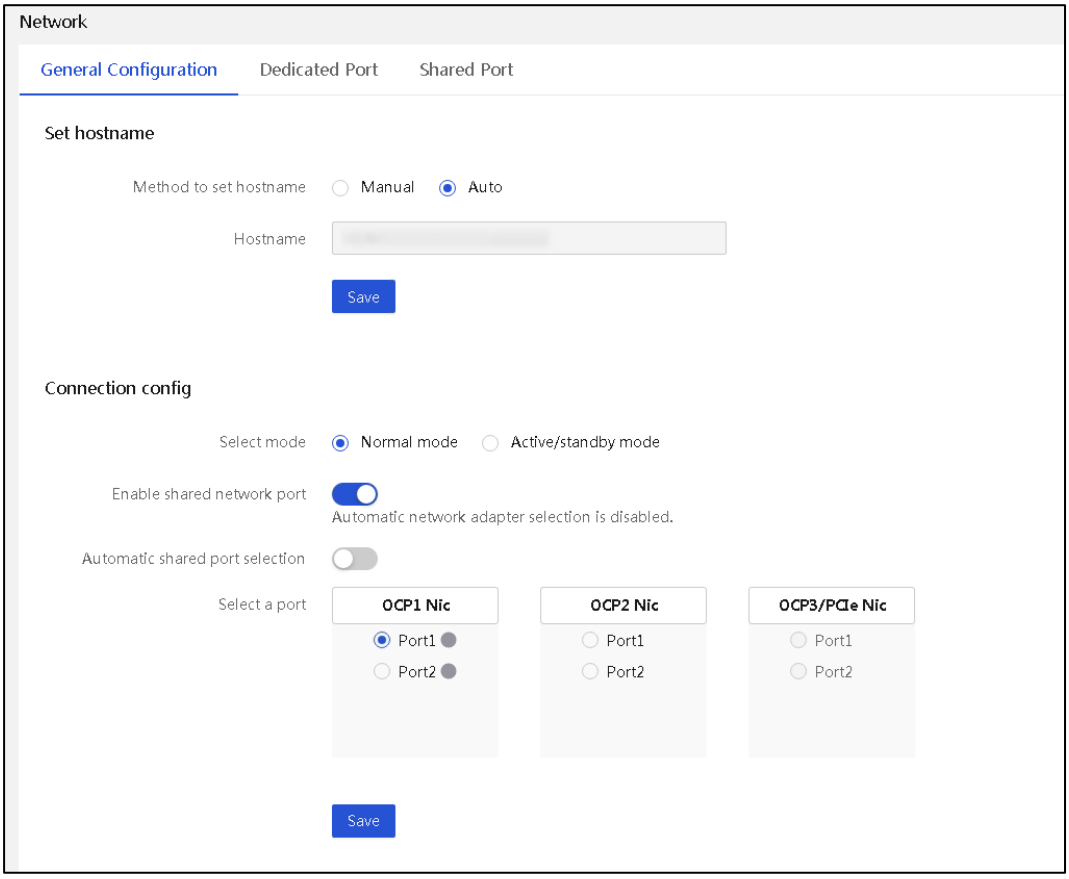


データフローの観点から見ると、HDMはMACを介して物理バスRMIIにネットワークメッセージを送信し、NCはRMIIを介してネットワークメッセージを受信して分析します。分析後、それがNCSIメッセージ(イーサタイプが0x88F8であることによって決定される)である場合は、NCSIで応答します。データを外部に送信するネットワークメッセージ(イーサタイプが0x88F8でないことによって決定される)である場合は、データを外部インターフェイスに転送します。

ネットワークポートモード

HDMは、図11に示すように、ネットワークインターフェイスに対して通常モードとポートアクティブ/スタンバイモードで構成できます。

図11 ネットワークの一般的な構成情報



- **Normal mode**: ユーザーは、共有ネットワークポートまたは専用ネットワークポートを介してHDMにアクセスできます。2つのポートのIPアドレスは、異なるサブネットに属している必要があります。
- **Port active/standby mode** :HDMは通信ポートとして専用ポートを優先し、共有ポートと専用ポートはアクティブ/スタンバイ状態になります。一度にHDMにアクセスするために使用できるポートのタイプは1つだけで、専用ポートの方が優先順位が高くなります。
  - 専用ネットワークポートがネットワークケーブルに接続されている場合は、共有ネットワークポートがネットワークケーブルに接続されているかどうかにかかわらず、専用ネットワークポートを通信ポートとして選択します。
  - 共有ネットワークポートがネットワークケーブルに接続されていて、専用ポートがネットワークケーブルに接続されていない場合は、共有ポートを通信ポートとして選択します。
  - アクティブ/スタンバイモードでは、共有ポートと専用ポートは同じIPアドレスとMACアドレスのセット(専用ポートMAC)を使用します。
- **Automatic shared port selection**: ネットワークアダプターポートの接続ステータスに基づいて、共有ポートを自動的に選択します。この機能には、次の利点があります:少なくとも1つのネットワークアダプターポートが接続されていれば、共有ポートを介してHDM管理を実行できます。
  - NCSIをサポートするすべてのOCPネットワークアダプターおよびPCIeネットワークアダプターは、この機能をサポートします。
  - 共有ポートを切り替えると、管理者は新しい共有ポートに接続し、共有ポートの切り替え後にHDMにアクセスできます。この機能には、次の利点があります。

-スムーズな切り替えを実現するために、ネットワーク全体でサーバーのネットワーク情報を変更する必要はありません。

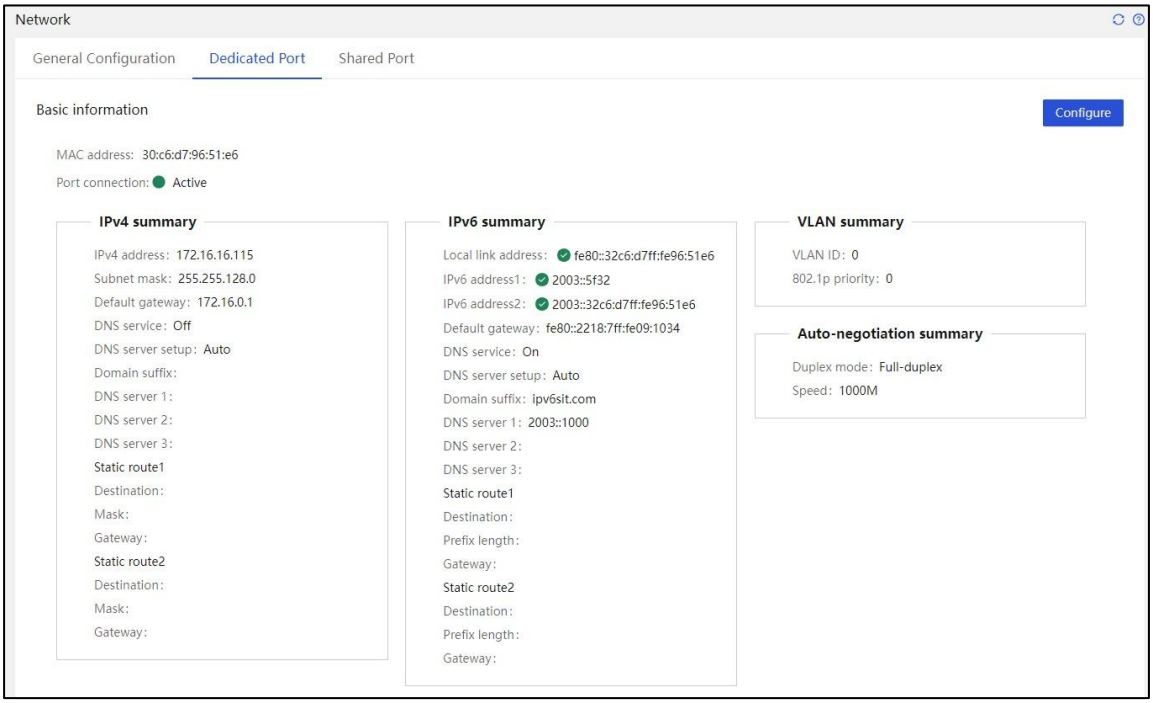
-メンテナンス効率を向上させるために、切り替え後に共有ポートのネットワーク情報(IPアドレスとVLANを含む)を再構成する必要はありません。

-アクティブ/スタンバイモードと自動共有ポート選択を同時に有効にしないでください。有効にすると、ネットワーク障害が発生する可能性があります。

IPv6

HDMはIPv6を完全にサポートしています。図12に示すように、専用ネットワークポートと共有ネットワークポート(NCSI)の両方が、物理チャネル上のIPv6アドレスを介したアクセスをサポートしています。

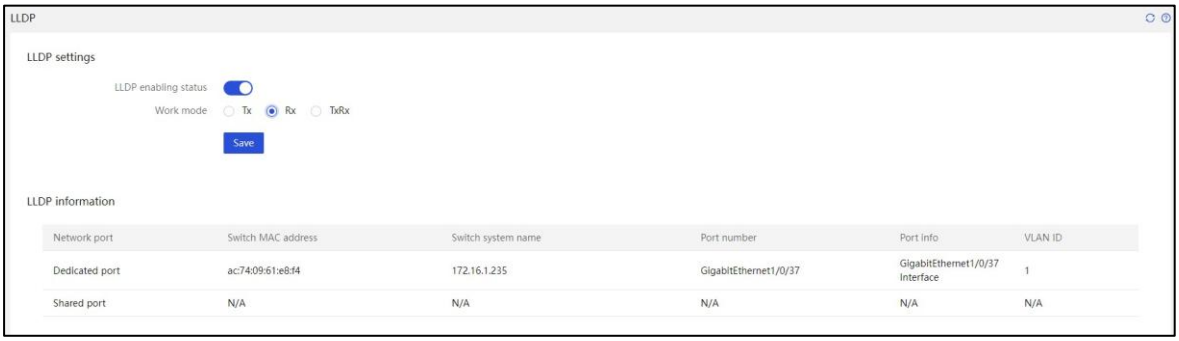
図12 専用ネットワークポートの構成



LLDP

Link Layer Discovery Protocol(LLDP)は、ネットワークデバイスを検出し、異なるベンダー間でシステムおよび構成情報を交換するための標準化された方法を提供します。これにより、ネットワーク管理システムは、レイヤー2ネットワークトポロジーおよび発生した変更に関する情報を迅速に収集できます。構成情報は、図13に示すとおりです。

図13 LLDPコンフィグレーション情報



HDMはLLDPプロトコルをサポートしており、ローカルネットワークのスイッチに関する関連情報を解析できます。

- **ネットワークインターフェイス**: サーバーがLLDP情報を受信するために使用するネットワークインターフェイス。
- **Switch MAC address**:アップリンクスイッチポートのMACアドレス。
- **Switch system name**: アップリンクスイッチシステム名。
- **接続ポート番号**: アップストリームスイッチのポート番号。
- **ポート情報**:アップストリームスイッチポート名。
- **ネットワークインターフェイス速度**: ネットワークインターフェイスの速度。

HDMは、LLDPメッセージのアクティブな送信をサポートし、隣接デバイスの検出を容易にします。

SSDP自動検出

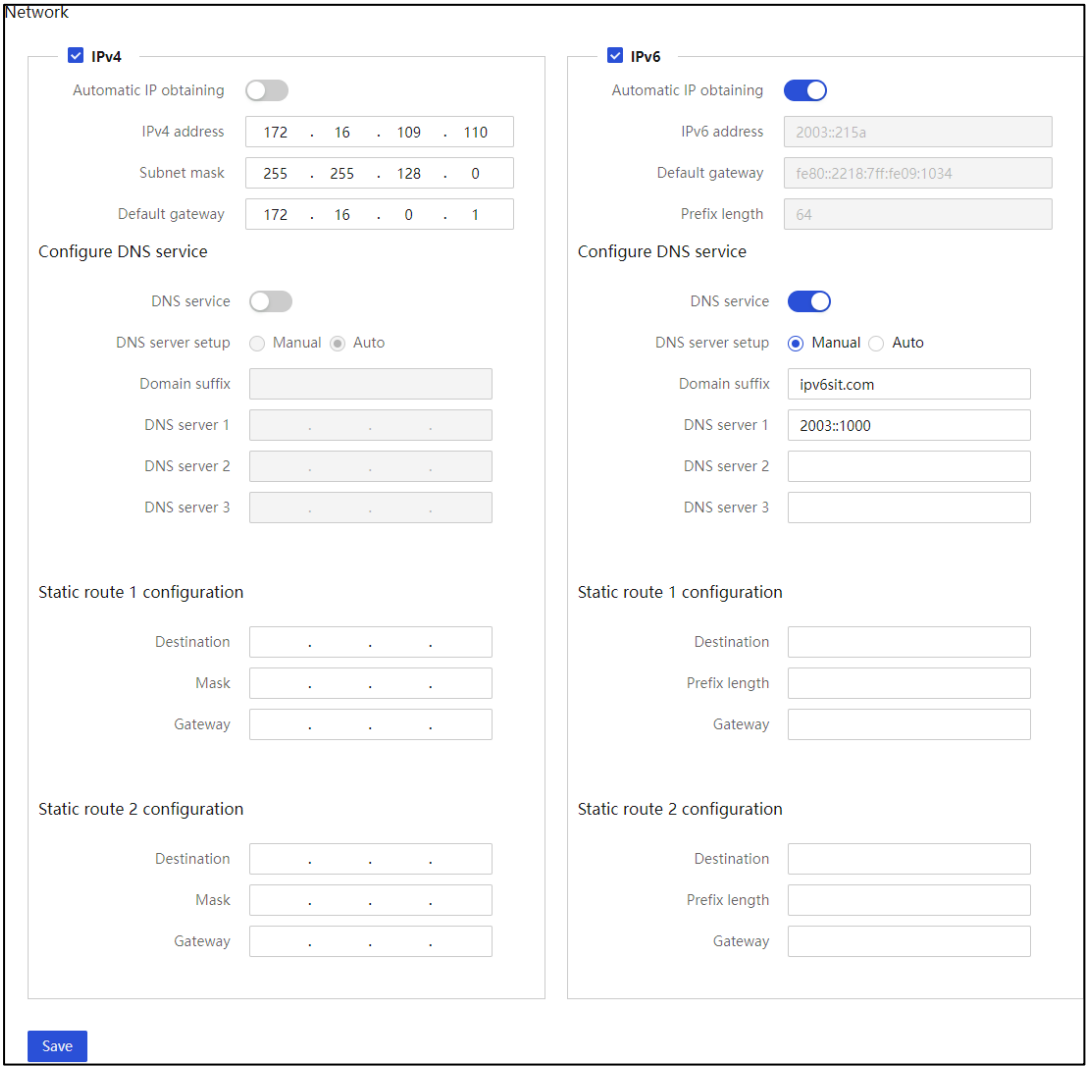
Simple Service Discovery Protocol(SSDP)は、アプリケーション層プロトコルであり、Universal Plug and Play(UPnP)テクノロジーを構成するコアプロトコルの1つです。

HDMはSSDPをサポートし、定期的にNOTIFYメッセージを送信します。これにより、上位レベルの運用および保守ソフトウェア(UniSystemなど)がすべてのBMCデバイスを自動的に検出できるようになり、初期セットアッププロセスでBMCデバイスを個別に構成するという問題点が解消されます。

スタティックルート

HDMは静的経路の設定をサポートします。IPv4とIPv6の両方の構成に対して別々に、専用ネットワークポートと共有ネットワークポートに2つの静的経路を構成して、ネットワークトラフィックを正確に制御および誘導し、クロスセグメント経路転送を実装できます。

図14 スタティックルートの設定



HDM時間設定

HDMでは、複数レベルの時間ソースが提供され、同期の優先順位を設定できます。次の時間同期方法がサポートされており、デフォルトの優先順位は降順です。

Primary NTP server > Secondary NTP server > Tertiary NTP server > DHCP server(acting as a NTP server) > Host ME(only for Intel products) > RTC on HDM。

時間管理

HDMでは、様々なソースから時間を取得して、様々な時間管理シナリオに対応できます。次のシナリオを使用できます。

- **NTP同期の手動設定**: 異なるHDMとホスト間で同じNTPサーバーを設定して、すべてのシステムがこのNTPサーバーから正しい時刻を取得し、常に一貫性を保つようにすることができます。
- **DHCPサーバーを使用してNTP同期を管理する**: DHCPサーバーのNTPサーバー(NTP server)フィールドを指定します。これにより、機器室のすべてのシステムが自動的に同じNTPサーバーを取得できるようになり、正確で統一された時刻を使用できるようになります。
- **ホスト時間の同期**: BIOSおよびMEコンポーネントを介してホスト時間をHDMに渡し、正確な時間を維持し、ホスト時間とHDM時間の一貫性を確保します。

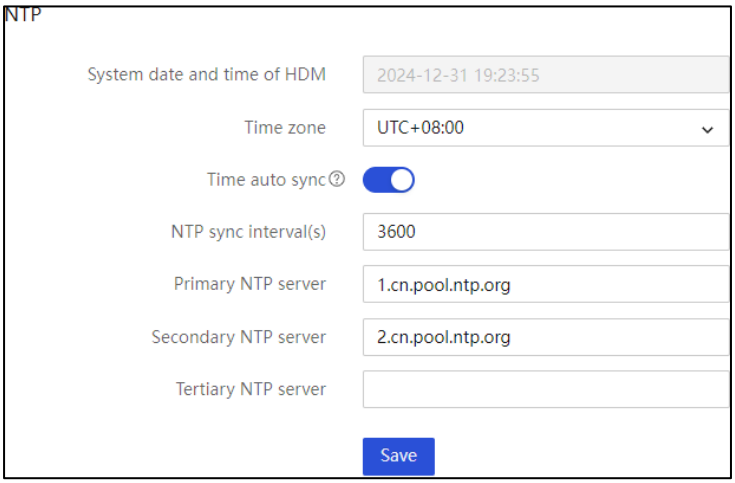
NTP同期

ネットワークタイムプロトコル(NTP)は、TCP/IPプロトコルスイートのアプリケーション層プロトコルです。一連の分散タイムサーバーとクライアント間でクロックを同期するために使用されます。

図15に示すように、HDMは3つのNTPサーバーの手動構成をサポートし、DHCPサーバーからのNTPサーバー構成の自動取得もサポートしています。すべてのNTPサーバーは優先度に基づいて管理され、優先度の高いサーバーが使用できない場合は、優先度の低いサーバーが自動的に使用され、定期的な自動同期が確保されます。

NTPサーバーは、IPv4アドレス、IPv6アドレス、およびFQDN(完全修飾ドメイン名)アドレスをサポートしています。

図15 NTP構成情報



DNS

DNSは、ドメイン名とIPアドレス間の変換サービスを提供するためにTCP/IPアプリケーションによって使用される分散データベースです。完全なドメイン名には、ホスト名と上位レベルが含まれます。

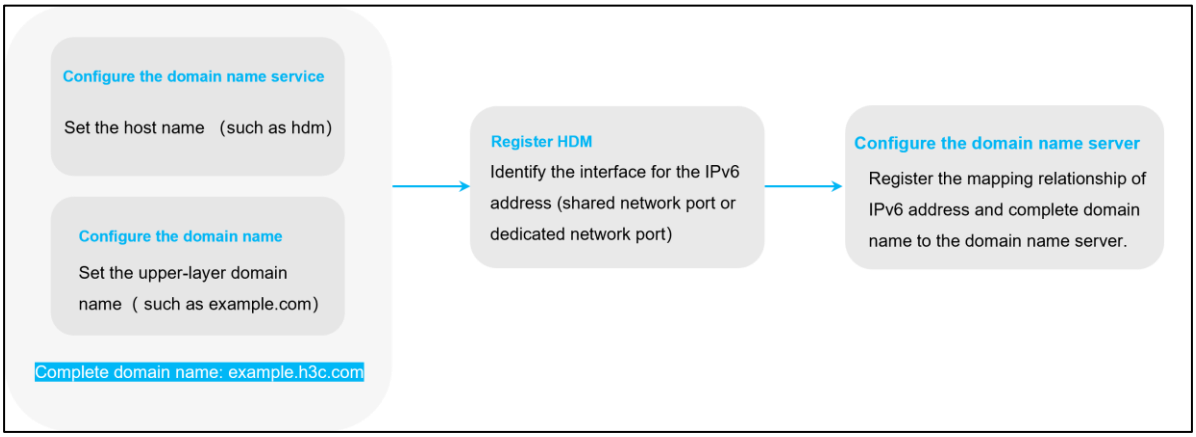
ドメイン名。HDMでは、ホスト名は手動で構成するか、サーバーのSN番号に基づいて自動的に生成できます。親ドメイン名も手動で構成するか、DHCPを使用して自動的に取得できます。

HDMは、共有ポートと専用ポートのIPアドレスのドメイン名へのマッピングをサポートし、このマッピングをネットワーク内のIP DNSサーバーに登録します。

登録方法には、nsupdateとFQDN/ホスト名があります。nsupdateを使用すると、クライアントはnsupdateコマンドを使用してDNSサーバーのゾーンファイルを直接更新できます。FQDN/ホスト名を使用すると、DHCPサーバーは、クライアントのネットワークアドレスの割り当てを確認した後、クライアント情報をDNSサーバーに動的に登録できます。

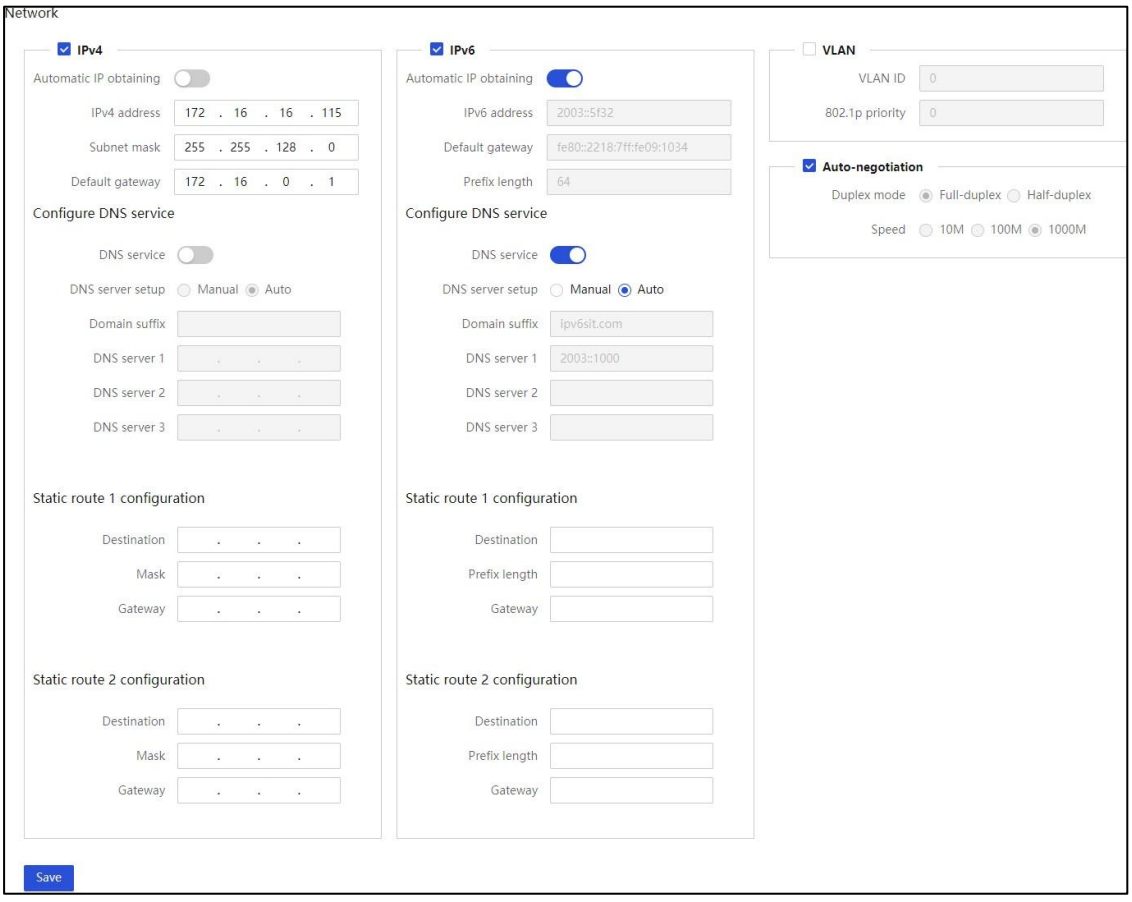
ユーザーは、すべての管理対象サーバーを統合管理ドメインに追加し、記憶に残るドメイン名を使用して管理対象サーバーのHDMにアクセスできます。

図16 DNS登録プロセス



HDMはDNS構成をサポートしています。図17に示すように、DNS情報は、専用ポートおよび共有ポートの下のIPv4およびIPv6インターフェイスに対して個別に構成できます。

図17 DNS構成情報



サーバー導入機能

背景

H3Cサーバーは、一般的な配置機能をサポートしており、PXEサーバーやDHCPサーバーなどの顧客の操作環境への迅速なアクセスを可能にします。H3Cは、顧客向けに多数の自動化配置ソフトウェアプログラムおよびツールを開発し、包括的で汎用性のある配置機能を提供しています。自動化ソフトウェアおよびツールは、顧客が手動操作時間を大幅に節約し、操作効率を高め、操作コストを削減するのに役立ちます。H3Cは、次の配置ソフトウェアおよび機能を提供できます。

- **HDM**:サーバースタンドアロンアウトオブバンド管理ツール。お客様は、オペレーティングシステムのKVMインストール、HDM/BIOS/RAID構成、およびファームウェアの更新など、HDMを使用して簡単なサーバー構成およびデプロイメントを実現できます。詳細は、このドキュメントの他の章を参照してください。
- **FIST SMS**:ファームウェアおよびドライバーのアップデートを含むインバンド導入機能を備えたサーバースタンドアロンプロキシソフトウェア。
- **iFIST**: サーバースタンドアロンの組み込み管理ソフトウェア。iFISTは、サーバーのストレージチップにプリインストールされており、インバンドのスタンドアロン導入機能を提供します。サポートされる導入機能には、オペレーティングシステムとドライバーの自動インストール、HDM/BIOS/RAID構成、ファームウェアの更新、マウント前のデバイス診断、および取り外し後のデータクリアランスが含まれます。
- **UniSystem**: サーバーの一括管理ソフトウェアです。HDM、FIST SMS、およびiFISTとともに使用すると、IP構成、オペレーティングシステムの自動インストール、クローンインストール、ファームウェアとドライバーの更新、およびソフトウェアインストールのプッシュやHDM/BIOS/RAIDの構成などのバッチ機能を含む、サーバーの一括導入機能を提供できます。UniSystemは、サーバーの自動シェルフアップをサポートしています。お客様は、UniSystemページでサーバーのソフトウェアとハードウェアの構成項目を事前に計画し、対応するサーバー構成テンプレートとバインディングルールを作成できます。サーバーが運用保守ネットワークにアクセスすると、UniSystemは自動的にサーバーを管理に組み込み、対応するサーバー構成テンプレートを発行して、プラグアンドプレイと心配のないシェルフアップの自動化効果を実現します。

サーバーの導入には、主に次のタスクが含まれます。

- デバイスラックマウント

  デバイス管理: ネットワークに参加している新しいデバイスまたはオフラインデバイスをすばやく識別できます。
- サーバー装置とそのコンポーネントのバッチ識別とバージョン管理を実行します。
  - デバイスのファームウェアとドライバーのバージョンを更新する必要があるかどうかを確認します。
  - ファームウェア更新:H3Cは、帯域内シングル/バッチ更新、帯域外シングル/バッチ更新、オフラインファームウェア更新など、複数のファームウェア更新方法をサポートしています。
  - ドライバーの更新:H3Cは、インバンドのシングル/バッチドライバー更新、オペレーティングシステムのインストール後の自動ドライバーインストールなど、複数のドライバー更新方法をサポートしています。
- 設定操作

  一元化されたHDM設定、BIOS設定、バッチのインポートとエクスポート、およびコンポーネント(ストレージコントローラーなど)のオンライン設定を実行します。
- オペレーティングシステムのインストール

  主流のオペレーティングシステムの自動バッチインストールを提供し、イメージファイルの”split”転送テクノロジーとイメージクローンテクノロジーをサポートします。従来のPXEインストール方法と比較して、UniSystemはオペレーティングシステムのインストール速度を大幅に向上させることができま

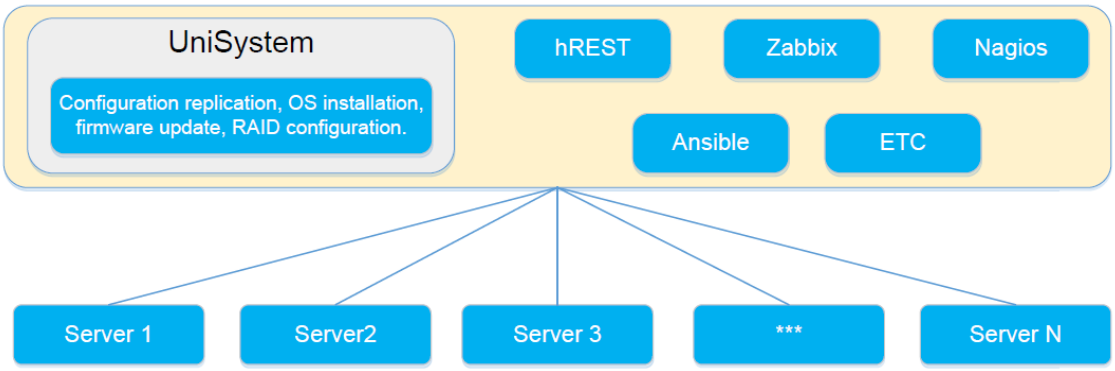
す。

- マウント前の機器診断など、その他のデバイス操作をサポートします。
- データ消去など、デバイスのアソシエーション解除後のセキュリティ操作をサポートします。

導入機能

サーバーの構成と配置には、複数の方法とツールが用意されています。UniSystemサーバー管理センターのサポートに加えて、ユーザー向けのバッチ管理、配置および更新機能を使用できます。詳細は、H3C UniSystemテクニカルホワイトペーパーを参照してください。

図18 導入機能の図



技術的なポイント

デバイス管理機能

HDMは、デバイスの組み込みを容易にするために次の機能をサポートしています。

- デバイスは、ネットワークに接続するときに、ARPパケットをアクティブに送信して、そのMACアドレスをネットワークにすばやくブロードキャストします。
- デバイスは、ネットワークに接続するときにSSDPおよびLLDPメッセージをアクティブに送信して、デバイスの外部識別を容易にします。
- DHCPはSN伝送をサポートし、サーバーの一意の識別を容易にします。
- HDMは、デバイス情報(モデル、バージョン、資産情報など)を取得するための外部管理ツールに豊富なAPIを提供する。

豊富な構成機能

HDMは、HDM/BIOS/コンポーネントパラメーターの設定を容易にするために、次の機能をサポートしています。

- 標準のIPMIコマンド、Redfishコマンド、およびSNMPコマンドを使用した設定をサポートします。
- BIOS設定に対して、1回限りの効果、永続的な効果、即時の効果、および次回の起動時の効果をサポートします。
- アラームログのカスタマイズとユーザー権限の設定をサポートします。
- HDM Webインターフェイスを介したBIOS設定の表示と構成をサポートします。
- HDM、BIOS、およびストレージコントローラー構成のバッチエクスポートおよびインポート操作をサポートし、構成の移行を容易にします。
- 工場出荷時設定へのリセットとワンクリックでの廃棄操作をサポートし、機器の移行と廃棄の要件に対応します。

- リモート設定とサービススイッチングをサポートします。

ファームウェアのインストール

HDMは、ファームウェア操作を容易にするために次の機能をサポートしています。

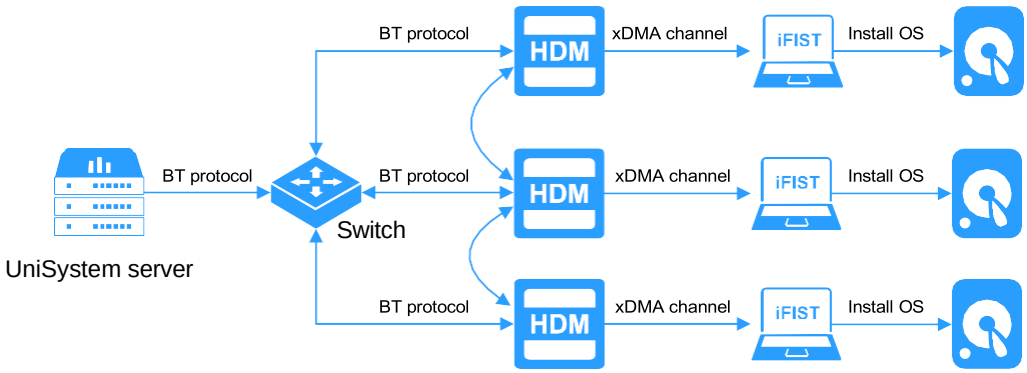
- バージョンを区別することなく1つのイメージを複数の製品に使用できるため、アップグレードが容易になります。
- ファームウェアタイプごとにイメージをカプセル化して、安全確認の要件と、ユーザーがファームウェアタイプを認識しないという要件を満たします。
- 帯域外ファームウェア管理操作をサポートします。
- 即時アップグレードとスケジュールされた非同期アップグレードをサポートします。
- 機能パッケージおよびパッチパッケージのインストールをサポートします。
- 複数のタイプのファームウェアを同時に更新するためのREPOアップグレードのサポート。
- ファームウェアのバックアップをサポートします。
- HDMおよびBIOSファームウェアの異常の自動リカバリをサポートします。
- ホストとHDMが異常から再起動した後のアップグレードタスクの再開をサポートします。
- 電源を切らないCPLDの再起動をサポートします。

OSとドライバーのデプロイメント

KVMまたはH5 KVMを使用したイメージマウントによるOSインストールとドライバーデプロイメントの従来の方法を除き、HDMは分散バルクOSインストールと高速OSインストールもサポートしています。これにより、さまざまなシナリオでの高速デプロイメント要件を満たすことができます。

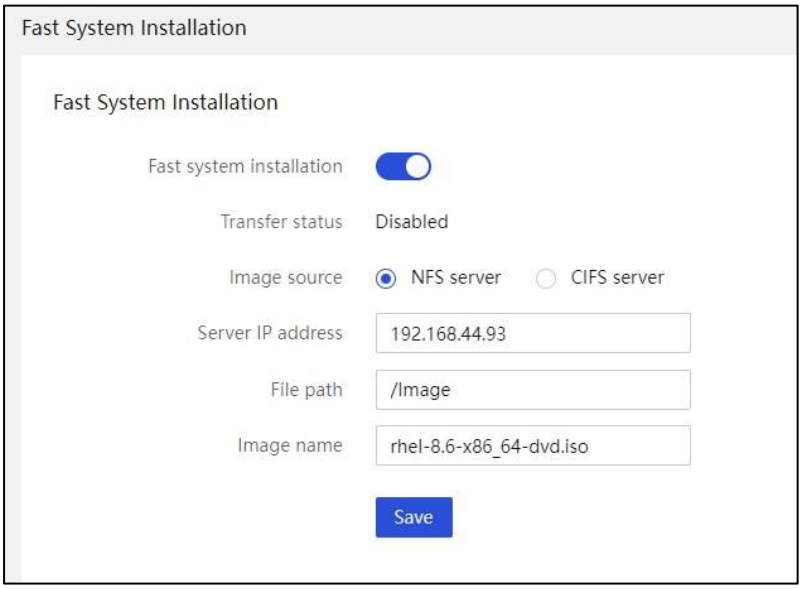
Distributed bulk OS installation: UniSystem は HDM と連携して、ファイル共有による分散イメージ転送による OS インストールをサポートします。これにより、ピアツーピア転送がサポートされ、ソフトウェア展開による帯域幅の制限が回避されます。これにより、従来のインストール方法と比較して、OS 展開機能が 10 倍以上向上します。

図19 分散バルクOSインストール



迅速なOSインストール:HDMは、迅速なOSインストールのためにNFSサーバーまたはCIFS(Samba)サーバーからイメージを選択することをサポートしています。この機能は、高パフォーマンスで低レイテンシのPCIeハードウェアリンク伝送チャネルを使用して、OSインストールの時間を短縮します。これにより、リモート仮想メディアに基づくOSインストール中にBMCからホスト側へのイメージ伝送速度が遅くなる問題が解決されます。

図20 OSの高速インストール



周辺機器ツール

HDMは、協調的なインターフェイスの豊富なエコシステムを提供し、多様なサーバー管理エコシステムを構築する。Ansibleオーケストレーションスクリプト、Zabbix、およびサードパーティの組み込み、監視、およびO&M管理のためのNagiosおよびNagios XIをサポートする。

表2 HDMがサポートするサードパーティ製プラットフォーム

サードパーティ製プラットフォーム	説明
VMWare vCenter	アラームの監視、情報の照会、OSのインストール、コンポーネントの更新、サーバーの構成
Microsoft System Centerオペレーションマネージャ(SCOM)	アラーム監視
Microsoft System Centerの設定マネージャ(SCCM)	OSのインストール、OSのアップグレード、システム構成
Ansible	情報照会、RAID構成、ネットワーク構成、BIOS構成
Zabbix	情報照会、アラーム監視
Microsoft管理センター	情報の照会、リソース使用率の監視
NagiosおよびNagios XI	情報照会、アラーム監視

コンフィギュレーション管理

設定ファイルのインポートとエクスポート

この機能を使用すると、HDM、BIOS、およびRAIDの構成を構成ファイルとしてエクスポートまたはインポートできるため、管理者は図21に示すように、リモートサーバーを簡単に構成できます。

この機能には、次の技術的な利点があります。

- HDM、BIOS、およびRAIDモジュールの構成オプションは、帯域外でバッチ構成できます。
- 設定可能なパラメーターは多数あり、HDM用の500以上のオプションとBIOS用の1100以上の

オプションが含まれています。この機能はRAIDレベルの変更もサポートしています。

- エクスポートされたコンフィギュレーションファイル構造は、読み取り、編集、および保存が可能です。
- エクスポートされたHDM構成アイテムは、自己注釈をサポートし、ユーザーが構成を理解できるようにする。
- これにより、同じ構成で複数のサーバーをバッチ導入できます。この機能により、操作が簡素化され、O&Mの効率が大幅に向上します。
- この機能は、パスワードのエクスポートおよびインポートをサポートしています。エクスポートされたパスワードは、暗号文形式で表示されます。

図22に示すように、構成ファイルは次のユースケースをサポートしています。

- コンフィギュレーションファイルをエクスポートし、変更を加えてから、設定を一括変更するためにインポートします。
- 同じモデルのサーバーに対して同じコンフィギュレーションファイルを使用することで、大規模デバイスの設定と展開を迅速に行うことができます。
- システムボードを交換するか、工場出荷時のデフォルト設定を復元した後は、エクスポートされた設定ファイルを使用して、カスタム設定を簡単に復元できます。

図21 構成ファイルのインポートとエクスポート

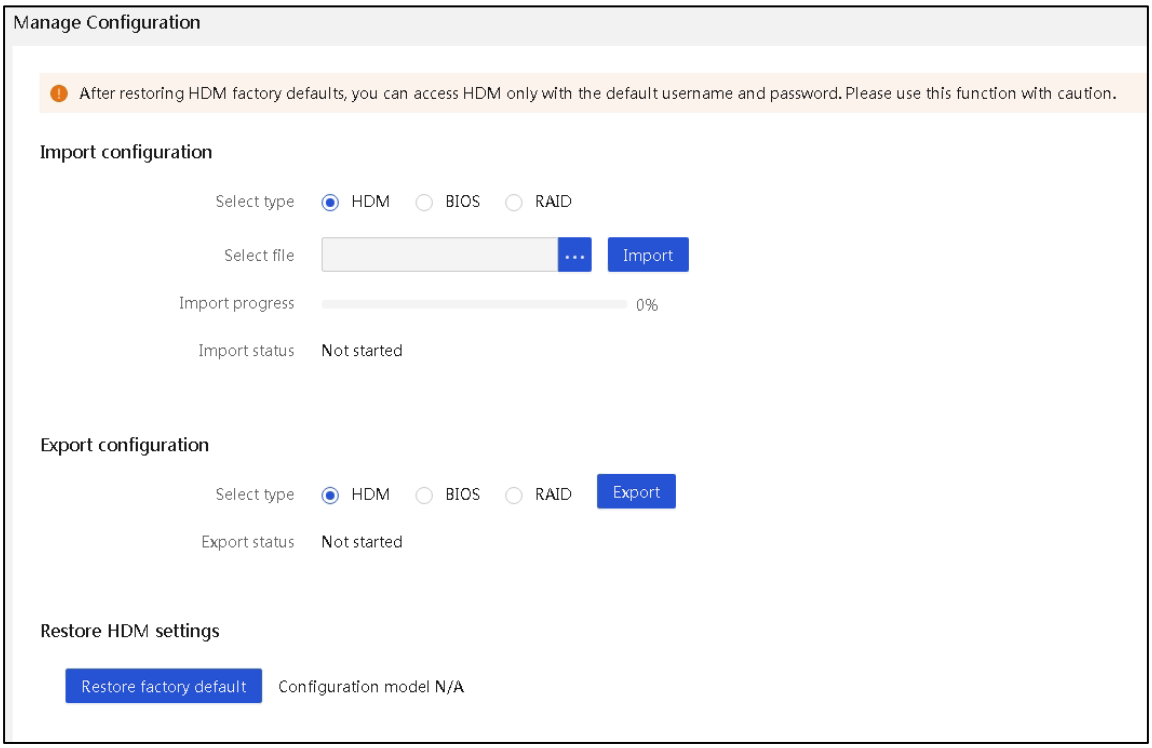
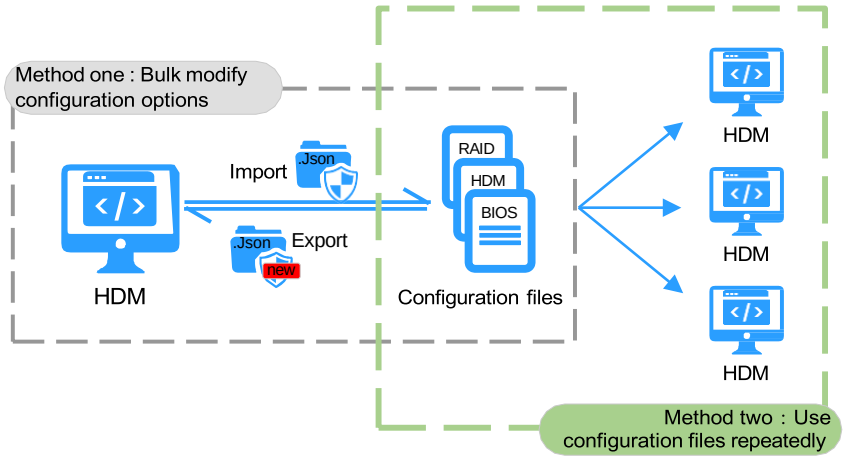


図22 構成ファイルのインポートとエクスポートの使用例



HDMの工場出荷時のデフォルト設定の復元

HDM設定を復元すると、HDMを工場出荷時のデフォルトに戻すことができ、HDMの再構成に使用できます。

BIOSオプションの設定

HDMは、BIOSオプションの便利なアウトオブバンド設定のために以下の機能をサポートしています。

- Webインターフェイスは、図23および図24に示すように、構造化された方法でBIOSオプションを表示することをサポートしています。Webインターフェイスは、ユーザーフレンドリーなBIOSセットアップユーティリティと一致しています。
- HDMは、異なるサーバープリケーションシナリオに対してBIOS構成テンプレートの1キーの変更をサポートしているため、関連するすべてのBIOS構成が自動的に変更されます。サポートされているアプリケーションシナリオは、図25に示すとおりです。

HDMは、強力な構成機能を備えた複数の帯域外設定方法をサポートしています。

- IPMIコマンドを使用した設定をサポートします。
- Support Redfishコマンドを使用してBIOSオプションを設定し、サポートされているすべてのオプションのパラメーターの説明をユーザーマニュアルに記載します。
- WebページまたはRedfishインターフェイスからのバッチ構成のインポートとエクスポートをサポートし、1100以上のオプションを提供します。
- 図26に示すように、有効期間、次のブートモード、次のブートデバイス、ブート順序、ブートサブオプション順序の構成など、ブートオプション設定の構成をサポートします。これにより、柔軟で使いやすいブート制御が実現されます。

図23 BIOS設定インターフェイス

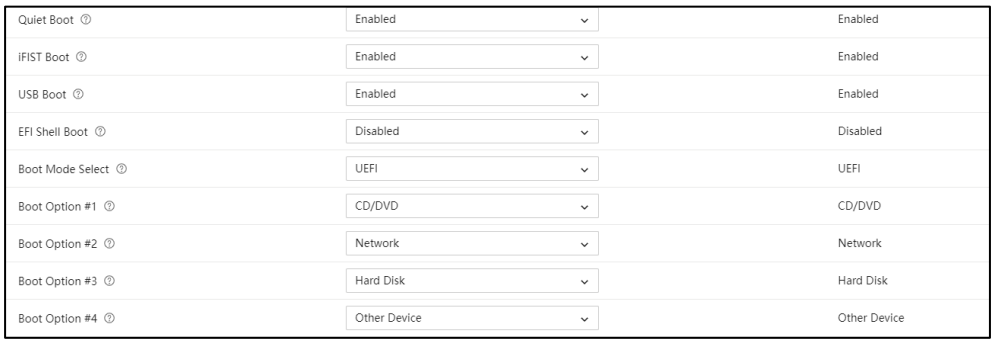


図24 BIOSセットアップユーティリティ

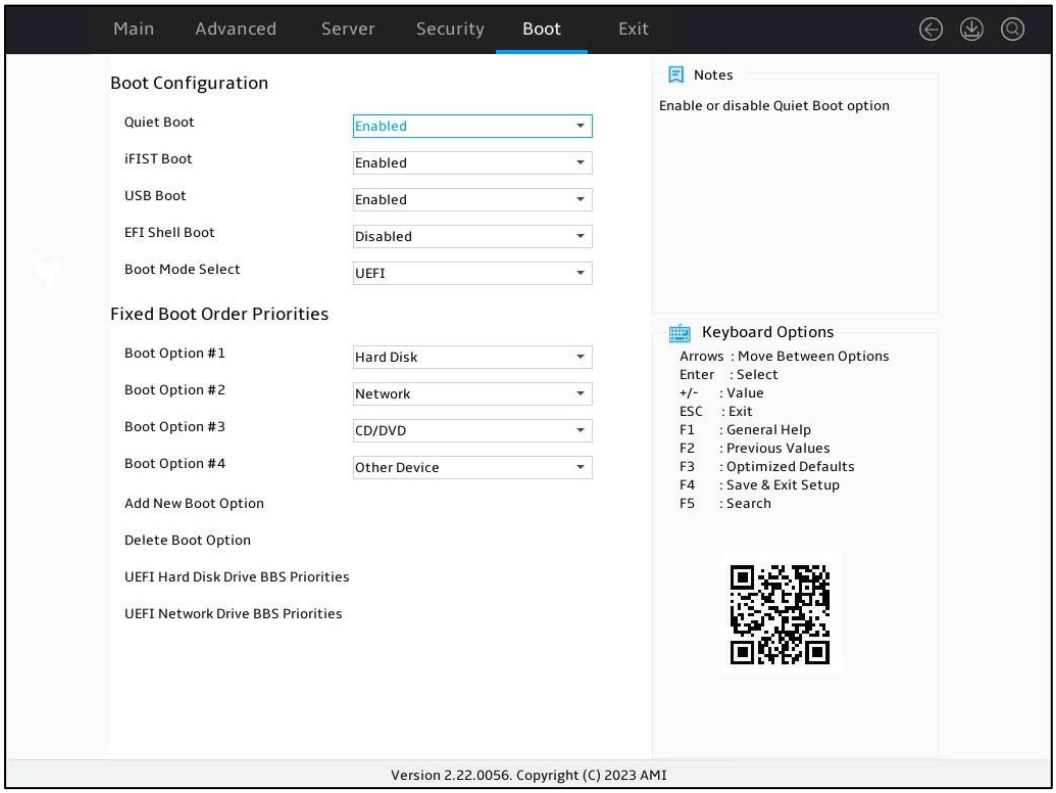


図25 BIOS設定テンプレート

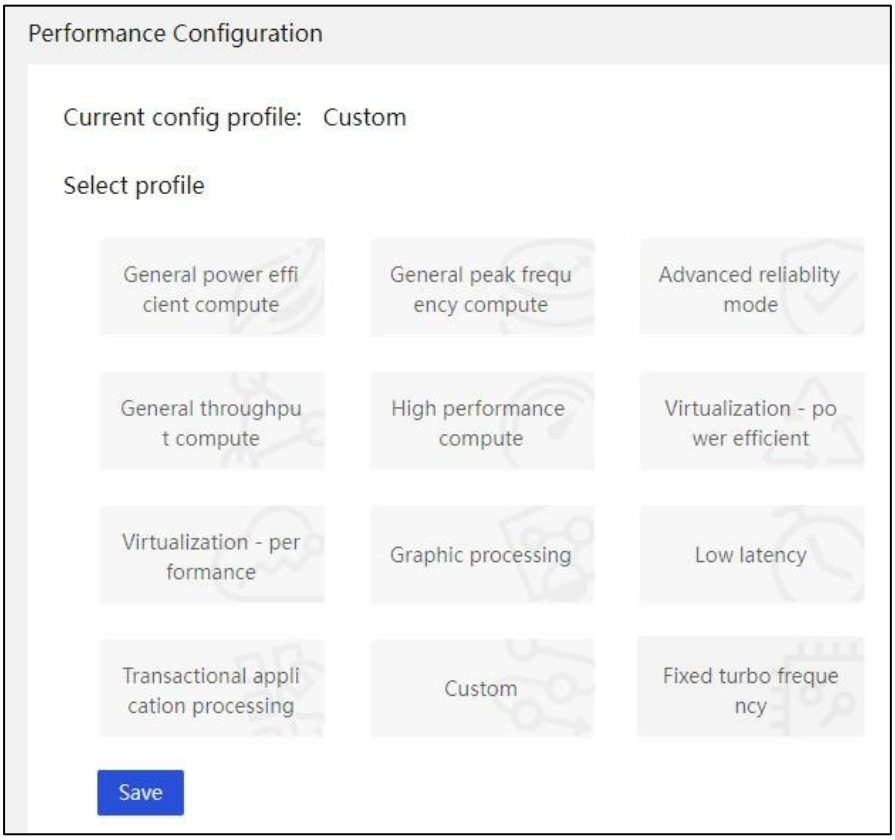
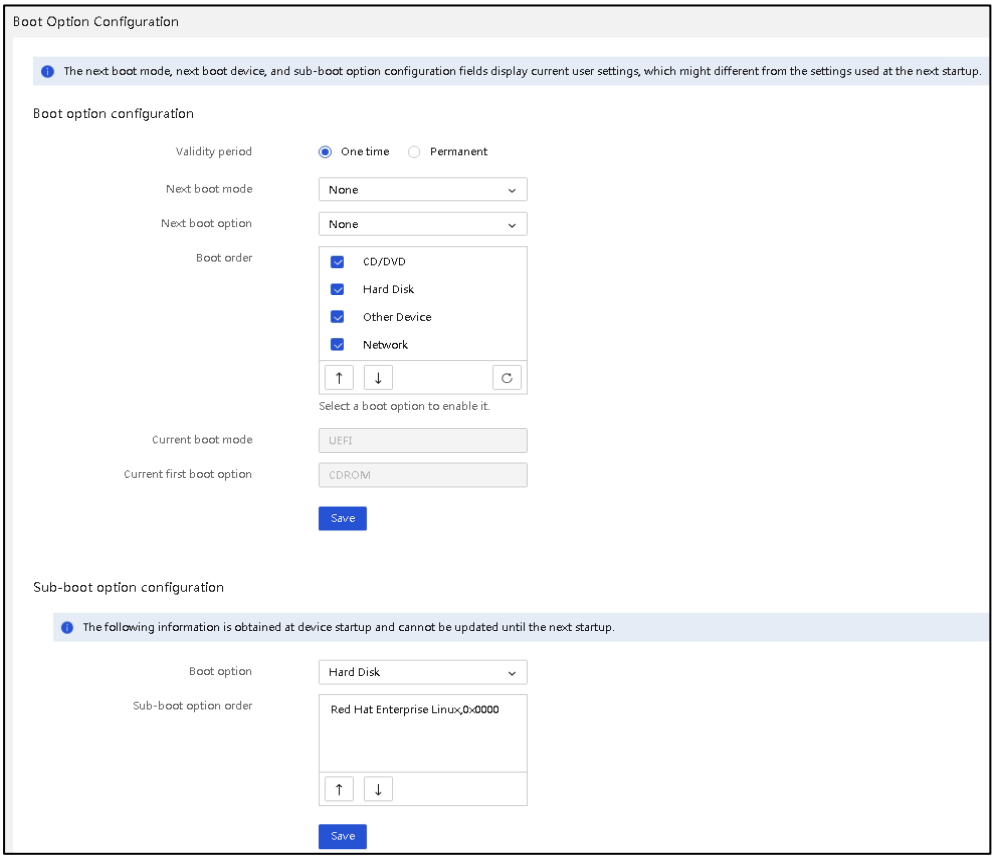


図26 ブートオプションの設定



ファームウェアのインストール

HDMアップグレードに関連するサービス機能には、次のものがあります。

- HDM、BIOS、CPLD、PSU、LCD、NIC、RAIDコントローラー、およびストレージドライブのファームウェアバージョンを照会します。
- サービスの中断や電源切断を伴わないHDMファームウェアのアップグレード。
- 複数の製品に対して同じHDMファームウェアイメージを使用でき、バージョンを区別する必要がないため、アップグレードの困難さが軽減されます。
- 署名付きbinファイルのファームウェアをアップグレードして、イメージが完全な状態であることを確認。
- REPOパッケージ(isoフォーマット)を使用して、複数のコンポーネント(PSU、LCD、NIC、RAIDコントローラー、ストレージドライブ、HDM、BIOS、およびCPLD)のファームウェアアップグレードを一度に実現することにより、中断のないアップグレードを実現します。
- 機能パッケージのアップグレードをサポートします。
- パッチパッケージのアップグレードをサポートします。
- スケジュールされたアップグレードをサポートします。
- ファームウェアリポジトリへのファームウェアのバックアップをサポートします。
- ファームウェアレポジトリ内のサポートファームウェアを有効にします。
- ファームウェアの異常検出をサポートします。
- HDMによるファームウェアのダンプをサポートし、エージェントツールを使用してオプションカードをアップグレードします。
- HDMおよびBIOSファームウェアの異常の自動リカバリをサポートします。
- 電源を切らないCPLDの再起動をサポートします。

ゴールデンイメージ

システムの信頼性を向上させるために、HDMはGolden Imageを使用してBMCのプライマリパーティションとバックアップパーティションを実装します。HDMファームウェアがアップグレードされるたびに、プライマリパーティションイメージのみがアップグレードされますが、Golden Imageは工場出荷時のバージョンのままです。プライマリパーティションでの操作中にフラッシュの誤動作またはストレージブロックの損傷が発生した場合、HDMは自動的にGolden Imageに切り替えてプライマリパーティションの異常なイメージを回復し、自動的にプライマリパーティションに戻すことができます。

ファームウェアのアップグレード

HDM、BIOS、CPLD、PSU、LCD、RAIDコントローラー、ドライブ、ネットワークアダプター、およびGPUのファームウェアアップグレードをサポートします。機能パッケージのアップグレードをサポートします。パッチパッケージのアップグレードをサポートします。bin、run、およびisoファイルを使用したアップグレードをサポートします。HDM、BIOS、CPLD、PSU、ストレージコントローラー、ネットワークアダプター、およびサーバー上のドライブなどのさまざまなコンポーネントのファームウェアを同時に更新できるREPOアップグレードをサポートします。Redfish URLおよびHTTP、HTTPS、NFS、TFTP、CIFS、SFTPなどのさまざまなファームウェアアップロード方法によるアップグレードをサポートします。

検証後に開くファームウェア情報ページでは、バックアップの選択とアップグレード実行時間の設定がサポートされています。HDMおよびBIOSファームウェアのアップグレードでは、手動および自動のアクティブ化方法がサポートされており、HDMおよびBIOSのアップグレード後の構成の予約または上書きがサポートされています。

1. イメージのバックアップ

   ファームウェア情報の確認ページでバックアップの有効化を選択すると、HDMは使用中のファームウェアイメージファイルをファームウェアレポジトリに自動的にバックアップします。

2. スケジュールされたタスク

ファームウェア情報の確認ページでは、アップグレード時間の設定を選択できます。HDMはタスクをバックグラウンドで保存し、事前設定された時間にアップグレードタスクを実行します。スケジュール済アップグレードタスクは、複数のタスクの同時発行をサポートします。事前に決定された時間より前の期間は、他のアップグレードタスクの通常の発行には影響しません。図27に、正常に発行されたアップグレードタスクを示します。

図27 スケジュールされたタスク

3. BIOSの自己アップグレード

   BIOSファームウェアを更新する場合、ユーザー設定を予約するか、ユーザー設定を上書きするかを選択できます。HDMは、BIOSのファームウェアファイルのみをeMMCにアップロードします。後でホストが再起動すると、BIOSはHDMを介してeMMCからファームウェアファイルを取得し、関連する構成戦略を実装するためにファームウェア自体をアップグレードします。

4. 差分機能パッケージ、コールドパッチ、およびホットパッチ

   インストールパッケージには、表3に示すように、機能パッケージとパッチパッケージ(コールドパッチとホットパッチを含む)が含まれています。

表3インストールパッケージの概要

インストールパッケージの種類		アプリケーションシナリオ	利点	制限事項
機能パッケージ		HDMシステムの増分サービスパッケージは、強化されたサービス機能を追加することができる。	• 基本サービスを中断することなく、増分サービスが自動的に有効になります。 • 増分的に変更されるコードの量は非常に大きくなる可能性があります。HDMは大規模な機能の増分アップグレードをサポートしています。	製品計画にもよるが、リリースサイクルは長い。
パッチ	ホットパッチ	パッチは、緊急のトラブルシューティングを必要とするオンサイトの問題を解決するために使用できます。サービスを中断することなく、リアルタイムの障害修復を提供できます。	• サービスを中断することなく、リアルタイムで障害を修正します。 • パッチのリリースサイクルは短く、ターゲットサイトにホットパッチを配信するには3日から10日かかります。	• 変更量には制限があり、通常は500行を超えるコード変更は必要ありません。 • システムの特定の機能では、ホットパッチがサポートされていません。

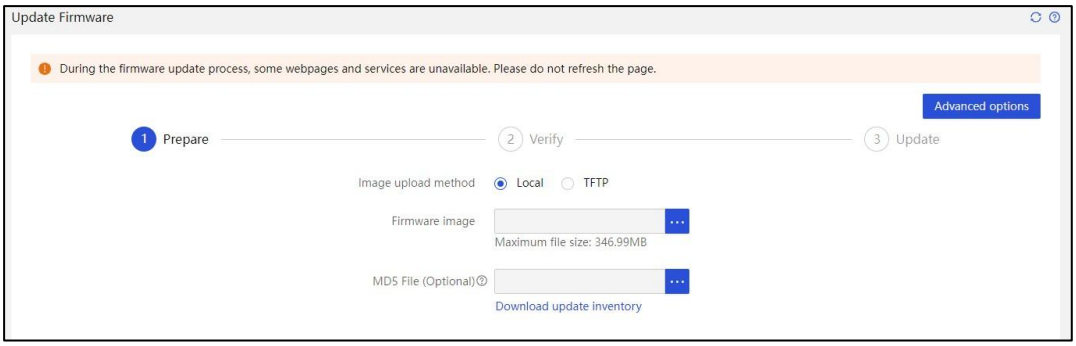
パッケージ	コールドパッチ	パッチを使用すると、緊急のトラブルシューティングが必要なオンサイトの問題を解決できます。障害のあるサービスは上位層のサービスであり、サービスプロセスを再起動できます。	• 障害が発生したサービスは、他のサービスに影響を与えることなく数秒以内に回復します • パッチのリリースサイクルは短く、ターゲットサイトにコールドパッチを配信するには3～10日かかる場合があります。	再起動をサポートしない基本的なコアサービスプロセスでは、コールドパッチをサポートできません。

機能パッケージおよびパッチには、次の利点があります。

- HDMファームウェアの多様性。基本ファームウェアに加えて、機能パッケージとパッチパッケージの提供により、アプリケーションシナリオが拡張されます。
- HDMファームウェア配信の適時性。基本的なファームウェア配信サイクルは、少なくとも1暦月です。パッチパッケージは、オンサイトの障害修復にタイムリーに対応できます。
- お客様向けにカスタマイズされた迅速な適応を実現できます。カスタマイズされた機能は、機能パッケージまたはパッチパッケージを通じて迅速に実装できます。

5. リスク通知のアップグレード
   - HDMに有効なHDMタスクまたはBIOSアップグレードタスクがある場合、Webインターフェイスはこれらのタスクに対応する通知を表示します。
   - HDMにスケジュールされたタスクがある場合、Webインターフェイスには、アップグレード時間、バージョン、アップグレードの実装方法など、これらのタスクに関する対応する通知が表示されます。
   - スケジュールされたタスクが複数存在する場合、HDMは最も近いアップグレード時間のタスクの内容を優先的に表示します。同じ時間にスケジュールされた複数のタスクの場合、優先順位は以前に登録されたタスクに与えられます。
   - HDMタスクとBIOSアップグレードタスクの両方が同時に存在する場合、HDMはBIOSアップグレードタスクの表示を優先する。
   - アップグレードリスク通知バーはWebページ上に固定されており、アップグレードタスクが有効になるとWebページの任意のタブに表示されます。

図28 アップグレードのリスク通知



6. ファームウェアのセキュリティ
   - **ファームウェア起動セキュリティ**: BMCファームウェアは、Golden Imageの冗長バックアップメカニズムを実装しています。動作中にフラッシュの誤動作またはストレージブロックの損傷が発生した場合、HDMをバックアップファームウェアに自動的に切り替えて動作させることができます。
   - **ファームウェア更新のセキュリティ**: HDMおよびBIOSを含む、外部からリリースされたすべてのファームウェアバージョンには、署名メカニズムがあります。ファームウェアがパッケージ化されると、SHA512アルゴリズムを使用してダイジェストが作成され、ダイジェストはRSA4096を使用して暗号化されます。ファームウェアのアップグレード中は、署名を確認することによって

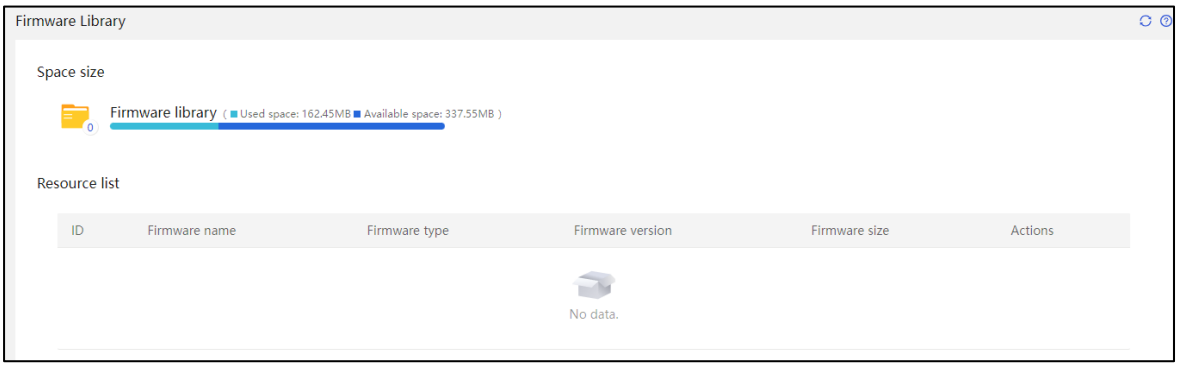
改ざんが防止されます。有効な署名を持つファームウェアのみがデバイスにアップグレードできます。

- **ファームウェア操作のセキュリティ**: 操作中、イメージが配置されている領域は書き込み保護され、書き込み操作を実行するには特別な方法が必要です。同時に、システムは各起動時にイメージファイルの整合性を検証し、必要に応じてイメージを復元します。

ファームウェアレポジトリ

ファームウェアのアップグレード時に、バックアップ機能が有効になっている場合、HDMはファームウェアイメージファイルをファームウェアリポジトリに自動的にバックアップします。バックアップが成功した後、ユーザーはファームウェアリポジトリページでバックアップファームウェアイメージファイルに関する情報を表示できます。使用可能な容量が不足している場合、ユーザーは新しいイメージのバックアップを続行できません。ファームウェアイメージファイルを手動で削除して、使用可能な領域を増やすことができます。ユーザーは、ターゲットイメージファイルに対応するApplyをクリックしてイメージを有効にすることを選択できます。その後、システムはファームウェアアップグレードのためにファームウェアの更新ページに自動的にアクセスします。

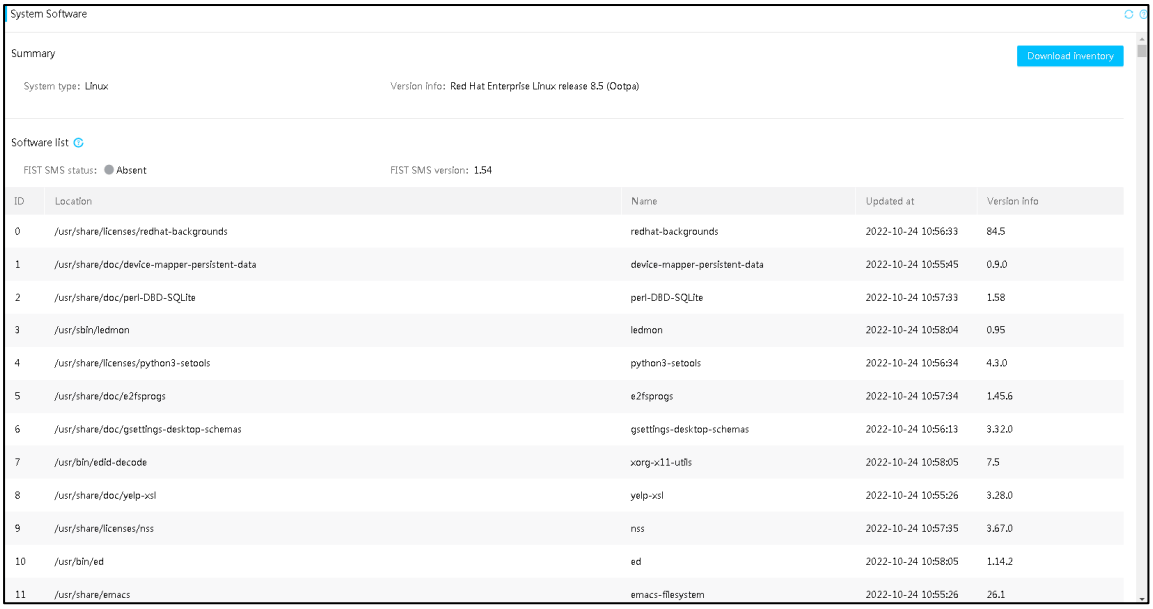
図29 ファームウェアレポジトリ



ソフトウェアインベントリ

ユーザーは、現在のサーバーオペレーティングシステムのシステムソフトウェアページで、場所、名前、バージョン、更新時刻(FIST SMSによって異なる)などのソフトウェア情報を表示およびダウンロードできます。

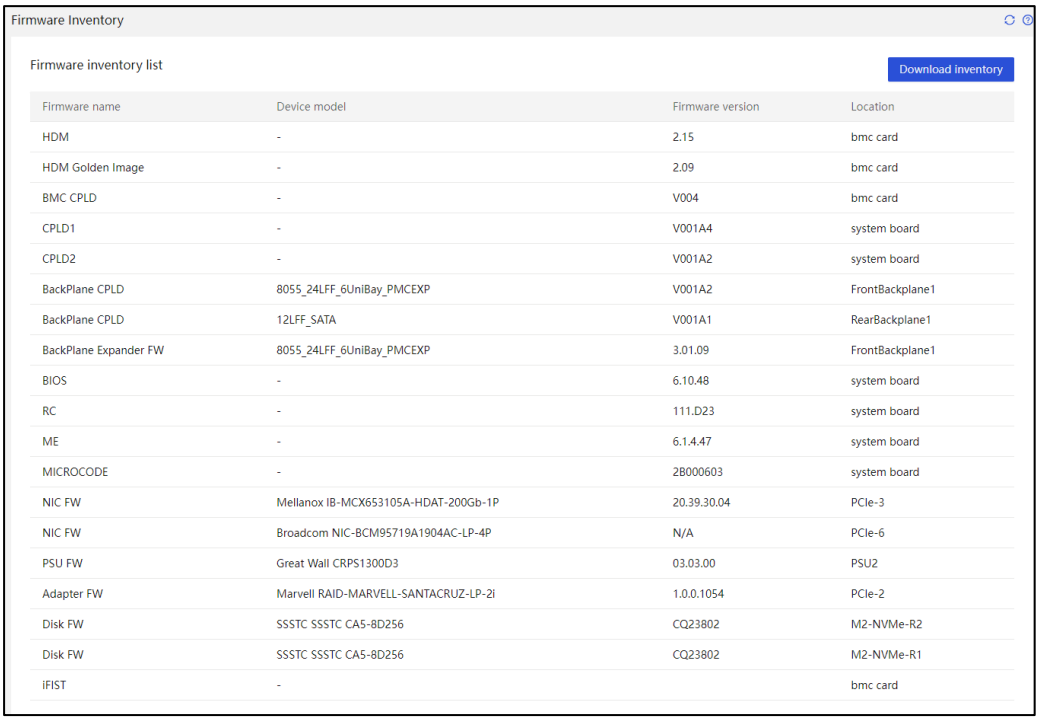
図30 ソフトウェアインベントリページ



ファームウェアインベントリ

ユーザーは、現在のサーバーにインストールされているファームウェアに関する情報(ファームウェア名、ファームウェアバージョン、ファームウェアインベントリ内の位置など)を表示およびダウンロードできます。

図31 ファームウェアインベントリページ



Firmware name	Device model	Firmware version	Location
HDM	-	2.15	bmc card
HDM Golden Image	-	2.09	bmc card
BMC CPLD	-	V004	bmc card
CPLD1	-	V001A4	system board
CPLD2	-	V001A2	system board
BackPlane CPLD	8055_24LFF_6UniBay_PMCEXP	V001A2	FrontBackplane1
BackPlane CPLD	12LFF_SATA	V001A1	RearBackplane1
BackPlane Expander FW	8055_24LFF_6UniBay_PMCEXP	3.01.09	FrontBackplane1
BIOS	-	6.10.48	system board
RC	-	111.D23	system board
ME	-	6.1.4.47	system board
MICROCODE	-	2B000603	system board
NIC FW	Mellanox IB-MCX653105A-HDAT-200Gb-1P	20.39.30.04	PCIe-3
NIC FW	Broadcom NIC-BCM95719A1904AC-LP-4P	N/A	PCIe-6
PSU FW	Great Wall CRPS1300D3	03.03.00	PSU2
Adapter FW	Marvell RAID-MARVELL-SANTACRUZ-LP-2i	1.0.0.1054	PCIe-2
Disk FW	SSSTC SSSTC CA5-8D256	CQ23802	M2-NVMe-R2
Disk FW	SSSTC SSSTC CA5-8D256	CQ23802	M2-NVMe-R1
iFIST	-		bmc card

ファームウェアの再起動

HDMインターフェイスは、BMCおよびCPLDの再起動をサポートします。

- ユーザーは、BMCファームウェアの更新が必要な場合、またはBMCファームウェアが誤動作した場合に、この機能を使用してBMCを再起動できます。すべてのセッションまたは接続は再起動中に中断され、再ログイン後に通常に戻ります。
- CPLDファームウェアの更新またはCPLDファームウェアの例外のためにCPLDを再起動するには、この機能を使用してCPLDファームウェアを再起動します。これにより、新しいファームウェアがすぐに有効になるか、CPLDファームウェアが正常に戻ります。CPLDのリセットサービスが影響を受けます。

デバイスの移行および廃棄に関連する機能

HDMは、帯域外ユーザーデータ消去によるサーバーコンポーネントのデフォルト状態へのワンクリックでの安全で信頼性の高い便利なリストアをサポートします。これにより、サーバーの安全な廃棄が実現されます。詳細は、セキュリティ管理の項の安全な消去の章を参照してください。

アプリケーションシナリオ

初めてデバイスをマウントする場合の推奨事項

デバイスをマウントした後、工場出荷時のデフォルト設定に基づいて調整が必要かどうかを確認するために、ベストプラクティスとして次の情報を確認してください。

- アウトオブバンドネットワークの接続ソリューション。
- 時間同期ソリューションの設定。
- 焦点に応じたパフォーマンステンプレートとセキュリティコンサルタントの設定。
- BMCサービス、ユーザー、および権限の構成。
- デバイスのステータスと、インストール後に仕様が要件を満たしているかどうか。
- ファームウェアのアップグレードが必要かどうか。

サービス中断を伴うファームウェアのバッチアップグレード

導入フェーズの開始時に、工場出荷時のファームウェアバージョンが要件を満たしていない場合は、統合された再導入または大規模なアップグレードが必要です。サービスが有効になっていない場合、または長時間の中断が可能な場合は、REPOパッケージを使用して、1回のクリックですべてのファームウェアを自動的にアップグレードします。または、UniSystemを使用して、すべてのサーバーを一括で導入します。

REPOアップグレードプロセスには時間がかかり、コンポーネントとホストの再起動がトリガーされます。ただし、ワンクリックでバックグラウンドで自動的に実装し、サーバー全体のファームウェアを指定された互換性のある状態にアップグレードできます。

サービス保証付きのファームウェアアップグレード

オンサイトメンテナンスで特定のファームウェアのみをアップグレードする必要がある場合は、指定されたコンポーネントのファームウェアパッケージを使用します。サポートされるコンポーネントには、ネットワークアダプターおよびRAIDコントローラーが含まれます。BMCファームウェアの更新後、対応するコンポーネントを再起動してプロセスを完了します。CPLDおよびBIOSなどのコンポーネントでは、ファームウェアの更新後にシステム全体を再起動する必要があります。

また、スケジュールされたアップグレード機能を使用して、低いサービスボリューム(早朝など)で時間を設定し、アップグレードプロセスを開始できます。

サービスを中断することなくファームウェアをアップグレード

重要なサービス環境では、オンサイトの運用に影響を与えることなくファームウェアのアップグレードの期待に応えるために、次の戦略が提供されます。

- BMCのアウトバンド監視を一時的に中断できる場合は、BMCファームウェアを直接更新できます。BMCの再起動には、BMCサービスのリストアにわずか1分しかかかりません。
- 新しいファームウェアがすぐに必要でない場合にBIOSファームウェアをアップグレードするには、新しいファームウェアが有効になる時間を遅らせて、次回のサーバーの再起動時にファームウェアが有効になるようにします。

サーバー管理機能

背景

多くのサーバーでは、安定した処理能力と信頼性の高いサービスを提供する必要があります。これは、安定性、信頼性、セキュリティ、保守性の向上と、管理能力の向上を意味します。

大まかに言えば、導入、監視、および診断はすべてデバイス管理の一部です。もちろん、保守中のスマート診断システム(SDS)ログからのオンサイト資料の識別、BMCのアクセス制御、BIOSまたはBMCの構成、およびさまざまなコンポーネントの保守もデバイス管理に分類されます。

HDMは、サーバーデバイスの次の管理機能をサポートしています。

- 資産管理:ユーザーは自分の資産を簡単に識別して管理できます。
- デバイス管理:
  - HDMは、CPU、メモリー、ハードドライブ、PCIeモジュール、電源、ファンなどのサーバーハードウェアを管理できます。
  - HDMは、オペレーティングシステムのステータスを監視できます。たとえば、リソース使用率を通じてシステムの実行ステータスを検出します。より詳細なリソース使用率情報を取得するには、HDMとFIST SMSの連携が必要です。
  - イベントログ管理:サーバーの動作は安定している必要があります。HDMはイベントログと早期警告を提供します。これにより、運用および保守担当者は異常なイベントを認識し、問題の根本原因を特定し、問題を迅速に解決できます。早期警告は、システムの停止時間の可能性を効果的に減らすのに役立ちます。
  - 操作ログ管理:HDMは、ログイン、ログアウト、ファームウェア更新、コンポーネント交換(CPU、メモリー、ハードドライブおよび電源など)、構成インポート/エクスポートおよびシステムロックなどの様々な操作をログに記録します。これらのログには、通常のサーバー使用時の構成、コンポーネントおよびバージョンの変更および変更の理由が直接表示されます。
  - リモート制御:HDMは便利なリモート制御を提供し、ユーザーはHDMページから直接システムを表示および制御できます。
  - ファームウェアインベントリ管理:ファームウェアインベントリには、さまざまなサーバーコンポーネントのファームウェア情報がまとめられています。Redfishインターフェイスを使用すると、ユーザーはデータセンター内のHDMによって管理されているすべてのサーバーのファームウェアバージョン情報を簡単に取得でき、統一されたクエリとアップグレードが容易になります。
- コンポーネント管理:
  - コンポーネント情報管理:HDMは、コンポーネントに関する静的情報と動的情報の両方を取得、表示および監視できます。情報はHDMページに表示されます。ユーザーは、様々なイベントログ警告を含むIPMI/Redfish/SNMPエージェントを介して、情報のレポートまたはコンテンツのプッシュをアクティブに監視することもできます。サーバーの動作サイクル中、定期的なサンプリングデータを通じて、HDMはセンサーをキャリアとして使用し
    さまざまなコンポーネントの動的な変化傾向。たとえば、温度センサーは、動作状態にあるコンポーネントの傾向を表示します。
  - 電源と消費電力の管理
- ホスト管理:
  - HDMは、KVM、H5 KVM、VNC、およびJViewerリモートコンソールをサポートします。また、電源制御、スクリーンキャプチャ、ビデオ記録などの操作もサポートします。
  - 仮想メディア:HDMは、ユーザーのマウントだけでなく、フロッピードライブ、CD/DVD、およびハードドライブ/USBデバイスの仮想メディアのマウントもサポートしています。
- 統合された管理:
  - HDMはサーバーの一括管理をサポートしています。デバイスの追加、デバイスの削除、デバイス情報の表示(IP、製品名、シリアル番号、ヘルスステータス

    サーバーの電源ステータス、およびUIDステータス)、HDMへのアクセス、電源操作、およびH5 KVMへのアクセス。

技術的なキーポイント

資産管理

H3Cサーバーの各専用コンポーネントには、設計時に一意の材料シリアル番号が割り当てられます。コンポーネントにEEPROMが搭載されている場合は、工場でFRU情報が書き込まれます。購入したコンポーネントについては、モデル、シリアル番号、部品番号、元のベンダー情報など、コンポーネントによって提供される基本情報に基づいて、一意の材料識別ソリューションを提供します。

各サーバーには、サーバーを区別するためのデバイスレベルのシリアル番号(3つのアイテムのシリアル番号を1つにまとめたもの)を割り当てます。さらに、資産情報を書き込むためのソリューションを提供し、サーバー資産管理のためにユーザー定義の情報を資産タグに書き込むことを容易にする。

デバイス管理

HDMのデバイス管理は、主に次の側面をカバーしている。

- デバイス上のさまざまなコンポーネントの接続トポロジーの識別。
- サーバーの電源と消費電力の管理。
- 冷却ソリューション(液体冷却、ファン制御など)
- 電源オン/オフ管理:
  - AC電源制御およびカスタマイズされた電源投入遅延ポリシー。
  - 物理電源ボタンの無効化のサポート。
  - ハードウェア設計に基づいて、HDMは、特定のPCIeスロットにあるS5ステータスのモジュールの電源ポリシーをサポートできます。このポリシーを有効にすると、そのようなスロットに取り付けられたスマートイーサネットアダプターの電源を入れることができ、対応するファンが速度を調整してスマートイーサネットアダプターの冷却ニーズを確保します。
  - 電源投入シーケンス制御のサポート(Smartイーサネットアダプターおよびシステムホストの電源投入シーケンス制御など)。

コンポーネント管理

操作ミスを防ぐために、HDMは、センサー、イベントログ、コンポーネント位置情報のマーク情報など、さまざまなコンポーネントのマーク情報の表示をサポートしている。

HDMがサポートするマークおよび位置情報は、次の要件を満たしています。

- HDMに表示されるマーク情報は、サーバー上のマーク情報と一致します。
- さまざまなHDMのAPIによって表示されるコンポーネントマーク情報は一貫しています。
- サーバーのCPUおよびメモリーモジュールの設置レイアウトと一致する視覚的なレイアウトを提供します。
- サーバー上とレイアウト位置が一致する温度センサーの視覚的な温度グラフを提供します。

HDMは、CPU、メモリー、ストレージカード、ハードドライブ、電源装置、ファン、ネットワークアダプター、GPUカードなどの様々なコンポーネントの管理をサポートします。サポートされる機能は次のとおりです:

- アウトオブバンド情報の読み取り、履歴情報の保存、特定のシナリオにおける履歴データに基づく予測。
- アウトオブバンド設定(サポートするストレージカードのアウトオブバンド管理、電源装置のアクティブモードまたはスタンバイモードの設定など)
- イベントのレポートと処理、特にコンテキスト情報の収集を含む保守性イベント。
- SMART情報の取得をサポートするハードドライブなど、一部のコンポーネントの平均寿命予測。

サーバーは、アウトバンド管理インターフェイスを介して、主要なサーバーコンポーネントに関する次の情報の読み取りをサポートします。

表4 主要なサーバーコンポーネント情報

コンポーネントタイプ	帯域外管理インターフェイスによって提供される情報	備考
プロセッサー(CPU)	• 完全に構成されたCPUと現在のCPU • スロット番号 • ベンダー • モデル • クロック速度と最大周波数 • コア数とスレッド数 • ヘルスステータス • マルチレベルキャッシュサイズ • アーキテクチャ • PPIN(インテル)	該当なし
メモリー	• 完全に構成されたメモリーモジュールと現在のメモリーモジュール • 位置 • 動作周波数と最大周波数 • 容量 • メモリー規格とメモリータイプ • ECC状態 • ベンダー名と部品番号 • ヘルスステータス	該当なし
ドライブ	• 完全に構成されたCPUと現在のCPU • ハードドライブの位置 • ベンダー(製造元) • モデル • インターフェイスのタイプとプロトコル • 容量 • ヘルスステータス • 残りの寿命(SSDハードドライブの場合) • ハードディスクドライブのSMART情報	該当なし
PCIeモジュール	• モジュールメーカーとチップベンダー • ファームウェアのバージョン • リソースの位置(モジュールが配置されているCPUおよびライザーカード) • 温度情報と帯域幅情報 • ネットワークアダプターの基本情報(ポート名、ポート番号、MACアドレス、ポートタイプなど) • MACアドレス、ルートBDF、BDF(ポート番号付き)、最大速度、接続速度、接続ステータス、インターフェイスタイプ、LLDPステータス、およびLLDP設定を含むネットワークポート情報 • ネットワークアダプターのポートトラフィック(FIST SMSがインストールされている場合) • 消費電力などのGPU情報	取得できる情報は、実際に取り付けられているPCIeモジュールによって異なります。 一般的なネットワークアダプターには、次のものがあります • オンボードネットワークアダプター • メザニンネットワークアダプター • PCIe標準形式のネットワークアダプター • OCP形式のネットワークアダプター • インテリジェントネットワークアダプター GPUアウトオブバンド

コンポーネントタイプ	帯域外管理インターフェイスによって提供される情報	備考
	GPUのメモリー使用量、GPU使用量、NVlink情報、ECCエラー監視ステータス セルフチェックレポート、消費電力上限、およびアラーム通知。 • ヘルスステータス	管理は、インストールされているGPUの機能によって異なります。
放熱装置: ファン	• 完全に構成されたファンと現在のファン • ファンの位置 • モデル • 速度比 • ヘルスステータス	ファン情報は、液浸液冷却モデルおよび非HDM制御ファンモデルのHDMページでは利用できません。
冷却装置: 液冷モジュール	• 完全に構成されたモジュールと現在のモジュール • リーク検知断線検知	液体冷却モデルでのみサポートされます。
光トランシーバモジュール	• 温度情報取得 • 速度調節における温度の関与	ネットワークアダプターと光トランシーバモジュールの両方が情報取得をサポートしている必要があります。
電源	• 完全に構成された電源装置と現在の電源装置 • 電源位置 • ベンダー • モデル • 定格出力 • 入力電圧 • 出力電圧 • 現在の電力値とヘルスステータス	ブレードサーバーおよびシャーシモデルサーバーでは使用できません。

サーバーは、帯域外管理インターフェイスを通じて、次のような電源制御ポリシーの管理をサポートします。

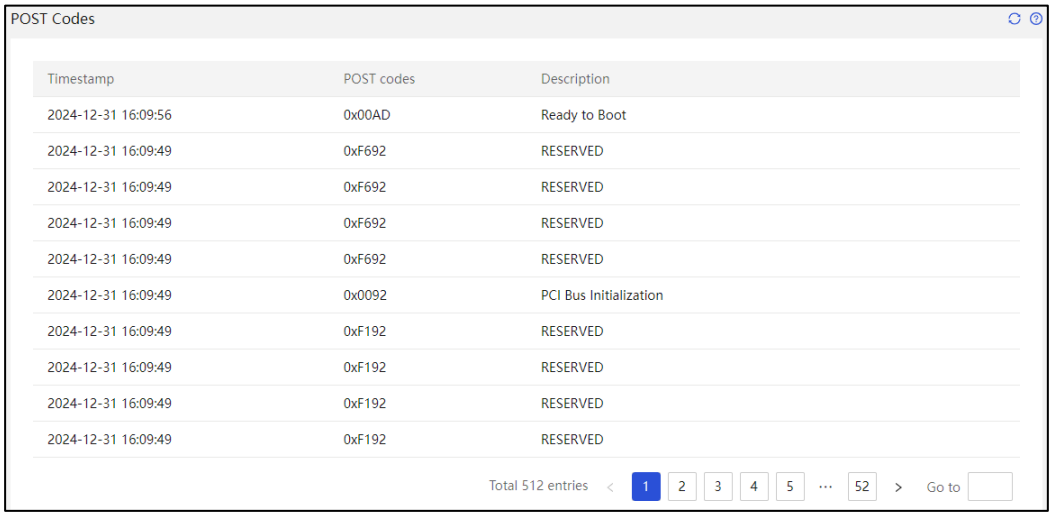
- サーバーの総消費電力の取得をサポートします。
- リモートでの電源オン、電源オフ、およびリセットをサポートします。
- サーバーの電源オン/オフ状態の取得をサポートします。
- 消費電力上限テクノロジーをサポートします。消費電力上限の有効化と無効化、消費電力上限値の設定、および消費電力上限障害時のシャットダウンを有効にするかどうかの指定を行うことができます。

ホスト管理

HDMは、次のホスト管理機能をサポートします。

- コンポーネントの識別:TPMのプレゼンスステータスおよびデュアルSDモジュールのプレゼンスステータスの取得。
- インバンド情報管理:BIOSバージョン、MEバージョン、BKCバージョン情報、ポストコード、ホストアドレス空間、SMBIOS情報、オペレーティングシステムバージョン、およびホストの動作ステータスの取得。
    - HDMでは、図32に示すように、POSTコードをクリアテキストで表示できます。各POSTコードの説明が直接表示されるため、ユーザーは障害の場所とタイプをすばやく特定できます。これにより、対象を絞ったトラブルシューティングが容易になり、時間が節約され、ユーザーフレンドリーなエクスペリエンスが提供されます。

図32 クリアテキストのBIOS POSTコード



OSエージェントを介した実装が必要な帯域内管理機能の場合、サーバーは、関連するファームウェア、ハードウェアドライバー、および開発インターフェイスを提供して、サードパーティ製の管理ソフトウェアが関連する帯域内管理機能を実装できるようにする必要があります。HDMは、帯域内管理を介した次の情報の取得をサポートします。

- サーバーのCPU使用率。
- サーバーの合計メモリー容量、使用中のメモリー容量、およびメモリー使用率。
- ネットワークポートの送信レートと受信レート。
- ネットワークアダプターファームウェアのバージョン番号。
- 光トランシーバモジュールのDDM情報。
- サーバーネットワークポートのIPv4およびIPv6アドレスリスト。
- ネットワークMACアドレスおよびネットワークポート名。

アプリケーションシナリオ

信頼性性能を向上させるための推奨事項

HDMは、全体的なサーバーの信頼性を高めるために、次の構成をサポートしています。

- IERRの発生時にポリシーを開始します。
- メモリー障害時の分離ポリシー。
- カスタマイズされた電源投入遅延。
- セキュリティ監視情報。
- 電源装置、ファン、およびモード切り替えのオンライン検出。
- ファンの冷却ポリシー。
- HDMの信頼性。

サーバー監視機能

背景

日常の運用と保守の要求を満たすために、サーバーは、デバイスの正常な動作を保証するために、ネットワーク管理システムによる継続的な監視のためのインターフェイスを提供する必要がある。

サーバーデバイスに異常が発生した場合、迅速な検出と迅速なトラブルシューティングのために、外部のメンテナンスシステムに障害を積極的に報告する必要がある。また、サーバーは、トラブルシューティングの目的で、それ自体のいくつかの主要なリソースを監視する必要がある。

さまざまなシナリオの監視要件に基づいて、HDMは次の主な機能を提供します。

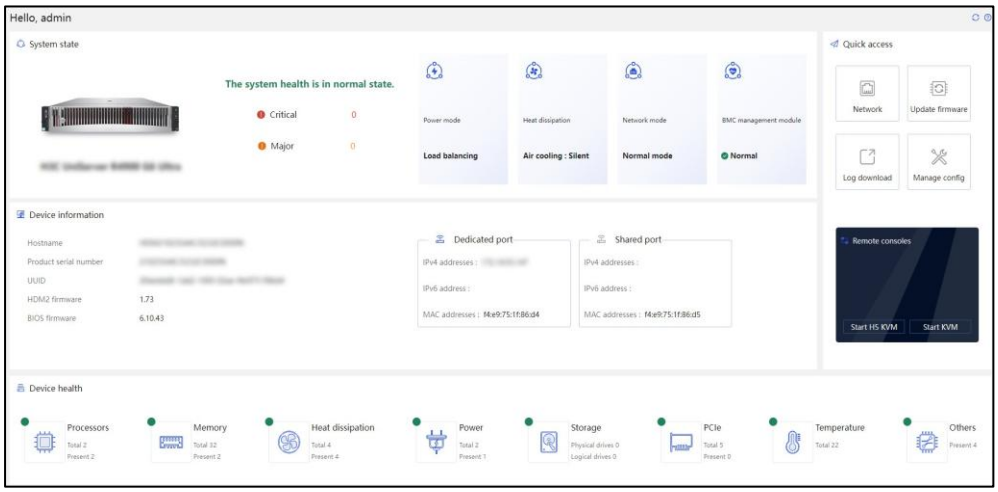
- 外部システムからサーバーハードウェアを継続的に監視するための複数のインターフェイスを提供し、次の機能を実現します。
  - 現在のステータスと履歴ステータスを表示できます。
  - デバイスステータスとサーバーステータスを提供します。
  - コンポーネントの監視をサポートし、特に、コンポーネントの寿命予測や障害警告などの機能を提供します。
- さまざまなシナリオの要件を満たす包括的なロギングソリューションを提供します。
  - 標準化されたコンポーネントベースのイベントログ、すべての関係者の操作を記録する操作ログ、安全に使用するための監査ログ、およびコンポーネント交換ログをユーザーに提供します。
  - SDSログによって提供される完全なライフサイクルレベルの操作パラメーターレコード。
  - オフラインロギングおよびリモート診断分析をサポートします。
- 製品ライン全体にわたる、統一された業界標準の包括的なアラームチャネル:
  - IPMI、Redfish、およびSNMPの管理要件を満たす標準化されたインターフェイス。
  - 電子メールとログに基づくサーバー上の直接アラームメカニズム。
- 主流のネットワーク管理システムと互換性があるため、サーバーデバイスを簡単に組み込むことができます。
- 包括的なホスト監視機能を提供します。詳細は、関連する説明を参照してください。

技術的なキーポイント

システムヘルスステータス

HDMでは、システムの全体的なヘルスステータスおよびシステム上の各コンポーネントのヘルスステータスを取得できます。ヘルスステータスは、Web、ヘルスLED、LCDパネルおよびインテリジェントセキュリティベゼルを介して表示されます。

図33 Webインターフェイスの要約情報



Dashboardページでは、サーバーの全体的なヘルスステータスとサマリーアラーム情報を表示できます。

サーバーの全体的なヘルスステータスは、プロセッサー、メモリー、ファン、パワーサプライ、ストレージ、PCIeモジュール、温度センサー、システムボード、バックプレーン、アダプターカードなど、関連するコンポーネントのヘルスステータスによって異なります。

コンポーネントの監視

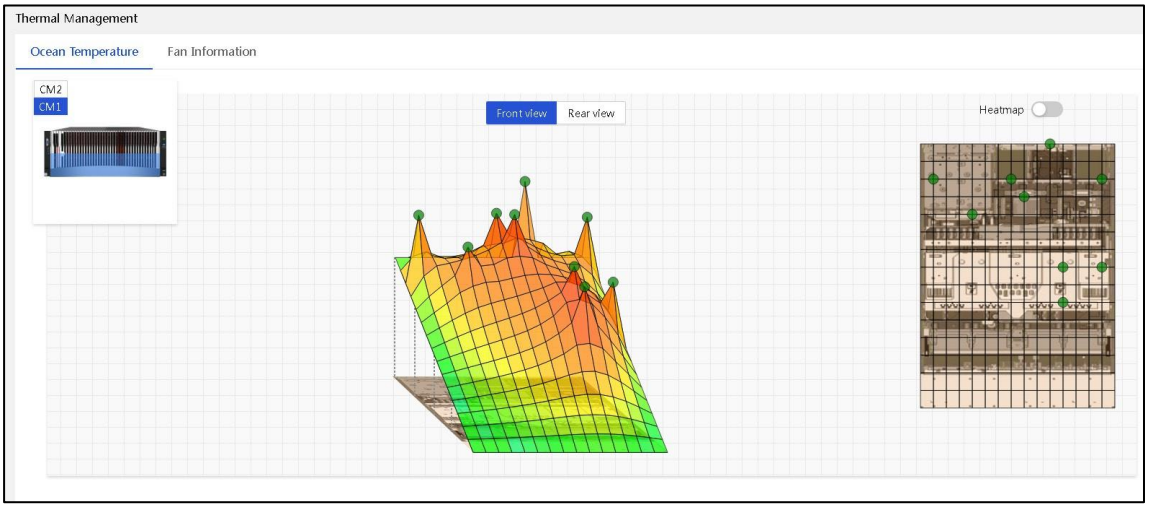
- 各コンポーネントに静的データクエリーインターフェイスを提供し、動的データを継続的に監視し、異常イベントを検出し、イベントタイプに基づいて対応する診断分析をトリガーします。
- コンポーネントに関連するさまざまな寸法情報を簡単に表示できる、使いやすいWebページを提供します。
- マルチロールコンポーネント(PCIeベースのネットワークおよびRAIDデバイスなど)、冗長コンポーネント(電源装置およびファンなど)、複合コンポーネント(RAIDコントローラー、スーパーキャパシター、OCPカード、および対応するファンなど)、マルチユニットコンポーネント(メモリーおよびハードドライブなど)のマルチレベル監視をサポートします。
- 監視情報はレベルごとに要約されます。最終的なシステムヘルスステータスは、デバイスへの影響に基づいて決定されます。

センサー

温度モニタリングでは、サーバーシャーシ内のさまざまなコンポーネントの温度センサーの分布図と値が表示されます。図34に示すように、参照用に物理構造図も提供されています。温度グラフでは、サーバーシャーシ内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ています。円の上にマウスを置くと、ターゲットセンサーの名前、ステータス、温度の読み取り値、およびしきい値を表示できます。緑は0°C(32°F)を示します。温度が高くなるにつれて、色は赤く変化するまで暖かくなります。座標の意味は次のとおりです。

- X: X軸上のセンサーの位置です。
- Y: Y軸上のセンサーの位置。
- Z: センサーが属するノード。(マルチノードおよびマルチレイヤー設計のモデルでは、異なるZ値が表示されます。)

図34 温度ヒートマップ



HDMでは、過去24時間、過去7日間または過去30日間のセンサーの測定値(温度、電流、電圧、ファン速度または電力)を折れ線グラフで表示できます。グラフの線の上にマウスを置くと、統計収集期間中の最大、平均および最小の測定値を表示できます。

図35 センサー読取りチャート

データをサンプリングしていないセンサーや、長期間にわたって監視の異常に遭遇したセンサーには、システムによって**not sampled**や**unavailable**などのラベルが割り当てられます。**Not sampled**は、通常、HDMが開始された後の最初のサンプリングポイントで見られます。**Unavailable**は、通常、既知の(監視されていないシナリオ)または異常な(リンクの異常によって引き起こされる監視の失敗)センサーが利用できない状況で見られます。

HDMは、サーバーの構成の識別をサポートし、識別結果に基づいて監視する必要があるセンサーを動的に生成し、これらのセンサーを監視します。予約された位置に物理的にインストールできるが、まだインストールされていない部品については、予約ステータスに関連するセンサーを表示できます。物理的にインストールできない部品(未インストールのライザーモジュールやバックプレーンなど)については、追加のセンサーは生成されないため、監視リソースがある程度節約されます。

標準ログ出力

H3Cのイベントログの実装には、次のような特徴があります。

- 互換性:標準のIPMIログを使用して、すべてのログをIPMIコマンドで検出できるようにします。
- 各アラームトリガーを対応するアラームクリアイベントと組み合わせて、外部管理操作を容易にします。
- クリアテキスト:すべてのイベントログを直接読み取ることができます。
- コンポーネント固有:各アラームログは対応するコンポーネントにリンクされており、迅速な識別とローカリゼーションに使用できます。
- 完全なライフサイクル記録:通常の保証期間中のイベントログ記録の要件を満たすように、すべてのイベントログを記録します。
- 柔軟な外部インターフェイスと統合機能:障害情報をレポートするための複数のインターフェイスをサポートし、上位レベルの運用および保守システムとの統合を容易にします。

複数チャネルによる同時監視

- サーバーのアラームチャネル

  アラームは、サーバー上の次のチャネルを通じて報告できます。

  - ハードウェアLED。主にサーバーの前面パネルと背面パネルに表示されます。各コンポーネントのLED、インテリジェントセキュリティベゼルのLED、LCDパネルのLED
    システムレベルのハードウェアLED
  - ソフトウェアデバイスのヘルスLED。主にWebページに表示され、IPMIコマンドを使用

して照会できます。

- SEL内のイベントログ、SDSログ、内部ポジショニングのためのSDS内のイベントログ、さまざまな監視チャネル(主にSNMPトラップ、SMTP、Redfish、およびリモートrsyslogを含む)を通じて表示される情報バリアント、および内部ログ情報を含む、イベントログベースのアラーム情報。
- センサーベースのアラーム情報。
- BIOSおよびOSのアラーム情報。

異常なイベントが発生した場合、前述の1つ以上のチャネルで監視できます。監視機能は、ハードウェアにイベントをレポートする機能があるかどうか、およびレポートチャネルがスムーズである(実装されており、例外がない)かどうかによって異なります。HDMは異常な情報を受信し、異常を処理し、コンテキストと組み合せてフォルトタイプを識別します。処理された情報は複数のインターフェイスに送信され、外部からアクセスできるようになります。異なるチャネルを介した伝送では、情報がマッピングおよび変換されるため、情報の損失や不整合が発生する可能性があります。これらの問題を回避するには、関連するルールを明確にする必要があります。

- イベントログ

  イベントログは、IPMI標準の定義に従って実装され、外部から標準のipmitoolを使用してアクセスおよび解析されます。これは、初期のサーバー管理における標準的な尺度です。HDMは、イベントログベースの監視をサポートし、ユーザーが使用できるイベントログに基づいてコンポーネントの説明を提供します。

  イベントログは、SMTP、SNMP、Redfish、およびsyslogと連携し、これらのアラームチャネルのトリガーおよびデータソースとして機能しますが、次のような違いがあります。

  - SNMPは、イベントログに基づいて、OID、SN、および拡張記述情報などの機能を追加します。
  - syslogメッセージは、イベントログの拡張情報を記述し、外部に送信されます。

- ハードウェアヘルスLED

  フロントシステムボードに障害が発生すると、CPLDロジックはハードウェアヘルスLEDを点灯させ、CPLDレジスタにフィードバックを提供します。ソフトウェアは、ロジックによって監視されているハードウェア障害を、中断の問合せと応答によって感知します。障害の処理後、ユーザーが認識する必要がある異常をソフトウェアが識別した場合、ソフトウェアはイベントログを出力し、センサーのステータスをマークします。情報はさらにソフトウェアLEDに送信されます。アラームステータスはロジックに書き込まれ、最終的にハードウェアLEDのステータスに反映されます。

  BMCの起動前は、ハードウェアの照明はシステムボードによって制御されています。BMCの起動後は、BMCによって制御されます。

- ソフトウェアヘルスLED

  ソフトウェアヘルスLEDは、デバイス(ハードウェア)の現在のヘルスステータスを示します。これは、メモリー、CPU、システムボード、PCIe、電源、放熱、ストレージ、および温度/電流/電圧(基本的にはシステムボードと各種カード)を含む各種コンポーネントの総合的なヘルスステータスを反映します。

  メモリー、CPU、およびPCIe情報は、主にBIOSによって送信されます。BIOSは、ポストステージとランタイムステージの両方でメモリー情報を送信できます。

  ソフトウェアヘルスLEDには、次の制約事項およびガイドラインが適用されます。

  - ヘルスLEDは、アラームタイプのイベントログにのみ関連付けられています。
  - マイナー重大度レベルのアラームは、ヘルスLEDに関連付けられません。
  - 純粋なソフトウェアアラーム情報は、ヘルスLEDに関連付けられていません。
  - デバイスのヘルスステータスは、各コンポーネントのヘルスステータスを組み合わせ、コンポーネントの障害がシステムに与える影響を評価することによって決定される。
  - ソフトウェアヘルスステータスはハードウェアヘルスLEDに書き戻され、ハードウェアとソフトウェアのヘルスLEDステータス間の一貫性が確保されます。

- センサー

  センサーは、特定のオブジェクトの現在の情報(存在、読み取り、および異常インジケータ)を記述するために使用され、オブジェクトの監視ステータスを識別できる。センサーの実装を定義するIPMI標準に従って、外部関係者はオープンソースツールのipmitoolを通じてセンサー情報を取得できる。センサーは、連続(しきい値ベース)と離散(しきい値ベースでない)のカテゴリに分類できる。連続センサーは、ハードウェア上の連続的な物理データ(温度、電圧、電流、回転速度、電力など)を監視するために使用される。離散センサーは主にイベントログの対象として機能し、さまざまなハードウェア監視ポイントの監視結果に関するフィードバックを提供する。

  センサーはイベントログを通じて変化するイベントを報告するため、ユーザーはイベントのトリガーまたはクリアを知ることができ、イベントログに含まれる情報に基づいて障害のソースとタイプを識別できる。センサー名は通常、コンポーネントの位置情報を反映できる文字列である。

  センサー関連の要素には、センサー名、センサーステータス、センサー読み取り値が含まれます。センサーの主な機能は次のとおりです。

  - センサー名は、関連するコンポーネントまたはその物理マークを識別します。
  - センサーステータスは、対応する監視対象オブジェクトのステータスを示します(ハードウェアコンポーネントである必要はありません)。
  - 連続的なセンサーの読み取り値とセンサーの単位を組み合わせて、センサーの値(たとえば、摂氏35度、220ボルト、または5400 RPM)を完全に理解できます。個別のセンサーの読み取り値は、個々のイベントがトリガーされた状態かクリアされた状態かを示します。

- その他のチャネル

  BIOSまたはOSが実行時にハードウェアの異常を検出すると、シリアルポートやVGAチャネルなどの従来のOSチャネルを介してエラー情報を出力します。HDMはワンクリックダウンロード機能を提供します。ダウンロードされたファイルには、Smart Hardware Diagnosis(SHD)の結果とブートログの起動情報が含まれます。

アプリケーションシナリオ

モニタリング機能の設定

次の監視ソリューションが用意されています。

- IPMIによる監視。
- SMTPによる電子メールの監視。
- syslogメッセージによるモニタリング。
- SNMPトラップによる監視。
- Redfish APIインターフェイスを介した監視。
- オフライン分析。

ログ解析方法

ログの主なアプリケーションシナリオは次のとおりです。

- 開発者と保守担当者は、ダウンロードされたSDSログに基づいてオフライン分析を実行する。
- 運用時には、インバンドコマンドを使用してアウトオブバンドソースからSELを取得し、障害情報が存在するかどうかを判断できます。
- iServiceは、イベントログ、センサーステータス、およびSHDの結果に基づいて、デバイスの状態レポートを生成する。
- Webページは、ログからSHDと履歴情報を抽出して表示する。

SDSログ

ユーザーのプライバシーを損なうことなくオフライン診断を実現するために、SDSログは、ライフサイクル全体を通じてBMCおよびホストからのデータを監視および記録します。記録される情報には、主に次のものが含まれます。

- デバイスのトポロジー構造を構築し、各コンポーネントのパラメーター情報を理解するために使用できるデバイスの静的情報。
- 未処理のSELログとクリアテキストのSDSログを含むイベントログ。
- 結果の解析中にMCAエラーが発生しました。具体的には、400以上の組み込みルールに基づく診断分析の結果です。
- SHD(各ハードウェアコンポーネントのスマート診断ログ情報を含む)
- 操作ログ、アップグレードログ、および再起動理由分析ログなどのデバイス操作レコード。
- BIOS、BMC、RAIDなどのデバイスの構成情報。
- BIOSのPOSTコード、smbios、ブートログなどのホスト実行データ。
- 再始動イベントに基づくデータ。
- BMCランタイムデータ。
- 内部障害診断に使用されるログ情報。
- センサー履歴データ情報。

外部関係者は、オフラインバージョンのSDSに基づいて関連情報を解析および取得するために、次の操作を実行できます。

- SDSログを日、月、期間、またはすべてのSDSログごとにダウンロードし、ダウンロードの進行状況をリアルタイムで表示し、SDSログに基づいてデバイスの静的情報を分析します。
- 障害の症状の把握。たとえば、再起動イベント(キーイベントの1つ)の原因と再起動が発生した時刻の取得。
- 操作ログ、監査ログ、イベントログ(SDL)、SHDログを時系列で整理し、障害発生前後のログ情報を取得する。
- インポートされた外部ルールを分析して、障害の場所を特定します。

スマート診断システム

背景

サービスへの影響を回避するためには、サーバーを確実に稼働させる必要があります。しかし、電子部品には一定の故障率があり、機器が異常に動作したり、さまざまな異常な動作を引き起こしたりします。異常な動作が異なれば、ユーザービジネスへの影響も異なります。H3Cは、設計、生産、加工、アフターサービスのすべてのプロセスとすべての側面において、機器の信頼性と故障診断能力を向上させます。HDMに統合されたスマート診断システム(SDS)は、すべての監視対象部品に対して統一された故障報告フォーマットを提供します。1500以上の故障診断事例を内部に統合することで、システムは95%以上の故障報告精度を達成しています。異常な故障が発生した場合に正確な故障情報が提供されるようにして、O&Mエンジニアが問題に適切に対処し、できるだけ早くサービスを再開できるようにします。

1. H3Cサーバーの管理が容易
    - 多層インターフェイスは、様々な外部O&Mシステムとのドッキングを容易にする。
    - 標準のIPMIおよびRedfishインターフェイスは、アラームおよび監視データを外部に表示するために使用されます。
    - パブリッククラウド管理プラットフォームを提供します。
2. ダウンタイムを短縮し、デバイスの信頼性を向上

- 予期しないシャットダウンの可能性を低減します。MRTの高度な修復により、予期しないメモリーダウンを40%以上防止できます。
- 重要な部分の障害を早期に検出して、潜在的なミスをより制御しやすくします。

3. 運用コストの削減とサービスの迅速なリストア
   - SDSは、問題の特定を迅速化し、障害回復時間を短縮します。
   - 複数の中断を避けるために、すべてのログを一度に取得します。

アーキテクチャ

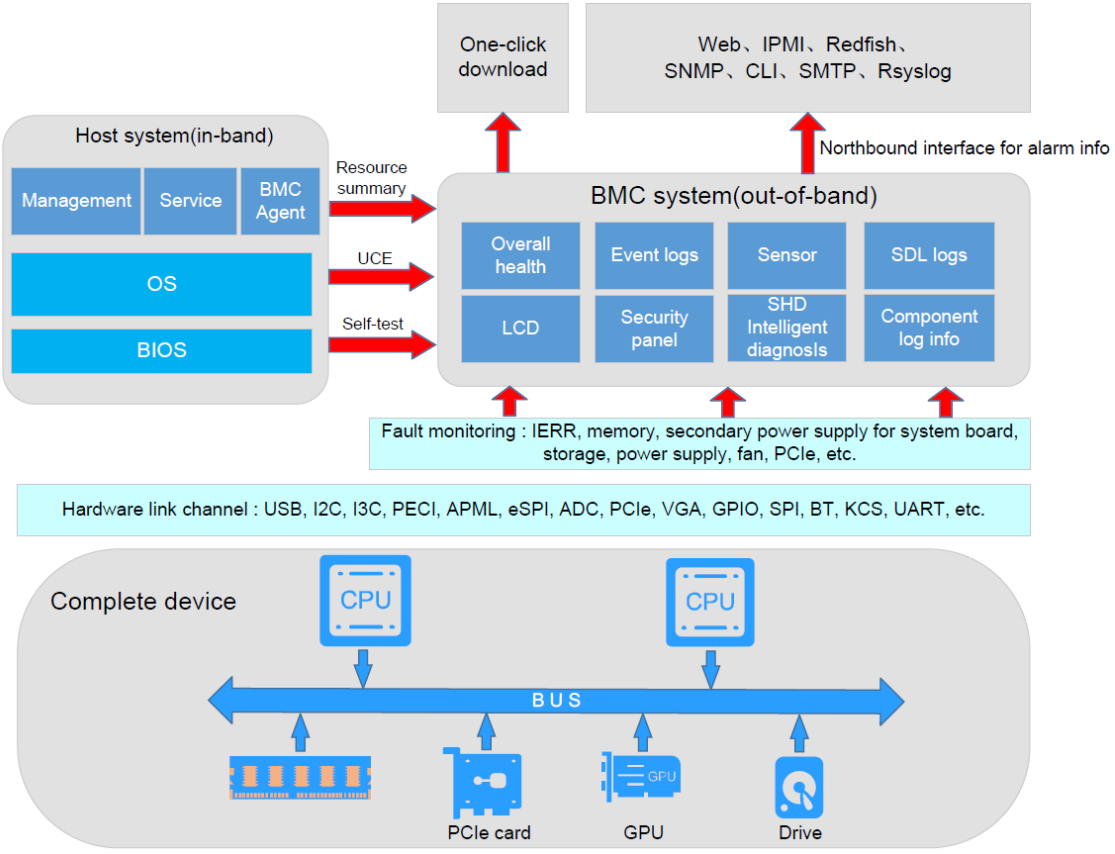
HDM SHDは、H3C HDMサーバー(レッドブランド)のライフサイクル全体のスマートデバイス診断システムであり、サーバー上の主要なハードウェアコンポーネントの障害を迅速かつ正確に特定し、診断することができる。

概要

SHDは、センサー、CPLD、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に関する情報を提供します。診断結果は、様々な次元の様々なタイプのユーザーの多様な使用要件を満たすために、様々な方法で表示されます。

診断機能は外部ネットワーク管理システムとの接続であり、故障アラーム診断機能は帯域外管理ソフトウェアの観点から考察したものであり、その主要なフレームワークは図36に示す通りである。

図36 SDS故障診断図



SHDは、サーバーの主要コンポーネントの総合的な監視を提供し、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、PCIeモジュール、またはシステムボードの障害を含む)
- 電源障害(電流、電圧、温度、電源ファン、IIC、および電流共有の障害を含む)
- システムボードの障害(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を含む)。
- 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チャネルの障害を含む)。
- 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、エクスパンダモジュール、キャッシュ、スーパーキャパシター、およびドライブの障害を含む)。

同時に、SHDは、主にログ記録と保守性機能として提供される多くの補助的な障害診断機能を提供する。補助的な診断には、サーバーシステムのスクリーンショット、HDMシリアルポートログ、ホストシリアルポートログ、IPMIプロセスデバッグログ、HDM再起動理由レコード、BIOSセルフテストコードのプレーンテキスト表示、および障害が発生したときのその他のログが含まれる。これらの補助的な障害診断機能により、ユーザーは障害が発生したときの状況をよりよく理解することができる。

技術的なキーポイント

包括的な障害ソースの認識と障害モードの分析

1. サーバーによってトリガーされるアラーム

   SDSには、サーバー情報、特にハードウェア監視情報を監視するためのさまざまな方法があります。現在のサーバーの主なアラームには、次のものがあります。

   - BIOSおよびOSによって送信されるアラーム情報。
   - MEによるCPUの監視
   - コンポーネントの帯域外アクセス機能を通じて直接取得されるアラーム。
   - CPLDで信号をモニタして検出したアラーム情報。
   - ハードウェアデバイスによって生成されるアラームに加えて、アラームは監視ソフトウェア内でも生成できます。

2. 別の方法で処理する必要がある障害タイプ

   異なるサーバー使用シナリオのため、システムで生成される異なるタイプのアラームは、異なる方法で処理する必要があります。差別化された処理が必要な障害のタイプには、次のものがあります。

   - **過去のデバイス障害**: アラームは解除されました。現在のシステムは正常に動作しています。ファームウェアは分離されています。業務は縮小され、再開されました。
   - **リダンダントコンポーネントの障害**: システムは動作していますが、ファンやパワーサプライなどのリダンダントパーツがありません。
   - ソフトウェア障害。
   - クラスフォルトのアセンブル。
   - 非ハードウェアエンティティの障害。

アラームの重大度レベル

サーバーコンポーネントに障害が発生した場合や、ダウンタイムや停電などの何らかの理由でサーバーが正しく動作しない場合、HDMは障害のあるモジュールごとに異なるタイプのアラームを生成し、同時にログを生成する。

アラームの重大度レベルには、次のものがあります。

- **Info** -イベントはシステムに影響を与えず、アクションは必要ありません。例としては、正常な状態の変化やアラームが削除されたイベントなどがあります。
- **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、サービスが中断される可能性があります。
- **Critical** -このイベントにより、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。直ちに対処する必要があります。

次の種類の障害を検出できます。

- **Processor faults**: IERRエラー、セルフテストエラー、構成エラー(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コアエラーを含む)、およびMCERRエラー。
- **Memory faults**: 修正可能なエラー、修正不可能なエラー、ADDDCおよび検査UCE-to-CEエラーのメモリー事前アラーム、Intel MRTベースのメモリー故障予知およびメモリーンテリジェント修復、過熱エラー、およびPOSTトレーニング障害。
- **Power supply faults** 電源検出、電源入力喪失(AD/DC)、予測障害、および電源セルフテストエラー。
- **Fan faults** -ファンの存在が検出されました。ファンに障害があり、ダウングレードに失敗しました。
- **Storage faults**: 検出されたドライブの存在、ドライブの障害、予測障害、重大なアレイエラー、およびアレイ障害エラー。
- **Overtemperature faults:** プロセッサー、メモリー、吸気口、電源装置、およびドライブの過熱状態。
- **Voltage faults** システムボードおよびその他のサーバーボードの電圧および電流障害。
- **Bus faults** -I2C、IPMB、またはQPI/UPIバスの障害。

ホスト中心の障害診断

ライブネットワークの解析に基づいて、ホスト中心の情報記録における故障は主にサービスに関係することが分かった。

- ブートログメカニズムは、各スタートアップのキーパラメーターを記録します。
- ホストの再起動理由の分析がサポートされている
- ホストのダウンタイム異常の分析がサポートされています。
- Webページには、ホストステータスの移行プロセスを表示できます。

アラーム処理機構

障害診断処理モジュールは、SHDの中核である。ハードウェア、BIOS、BMC、およびオペレーティングシステムのさまざまな次元からデータを収集および分析する。対応する標準、コード実装、および実際の障害データを調査および分析する。障害の識別、自己修復、分離、修復、事前アラーム、および処理などの次元をカバーする障害診断システムを徐々に改善および形成する。

H3Cには、専門的なビッグデータトレーニングチームとプラットフォームがあります。H3Cは、AIトレーニングに必要な主要コンポーネントトレーニングサンプルを収集し、業界の高度な機械学習技術に基づいてデータをトレーニングし続けています。開発されたモデルは、HDM、UniSystem、およびクラウドの運用および保守システムに完全に展開されます。すべてのサーバーコンポーネント、すべてのステータス、およびすべてのアウトオブバンド動作ステータスをリアルタイムで監視することを実現し、運用および保守作業をより簡単かつプロアクティブにします。

1. 障害の特定

   このモジュールは、サーバーを広範囲に監視し、組込みルールに基づいて障害を表示します。95%以上の精度で、特定のコンポーネントレベルまで障害を正確に識別します。次の方法を実行します:

   - サーバーのシステム全体の動作環境、各コンポーネント、およびホストの状態を継続的に監視します。サーバーの運用中に発生する可能性のあるさまざまなイベントやリスクの高いイベントを徹底的に記録します。
   - このシステムには1500以上の障害検出ポイントが組み込まれており、すべてのコンポーネントの既知のすべてのミスポイントをカバーしている。

- 診断には組み込みのエキスパートルールを使用し、コンポーネントレベルで検証することで、精度は95%以上に達する。

2. 障害の自動修復

   モジュールは、検出されたサーバー障害に対して自己修復操作を実行し、デバイスの保守期間を改善します。実装方法には、次のものがあります。

   - ハードウェアのRAS機能を完全に使用して、CEエラーおよび回復可能なUCEエラーから障害を自動的に回復または分離します。
   - 冗長性テクノロジーを採用してBMCとBIOSファームウェアのセキュリティを確保し、障害時に自動的にリストアを実行します。
   - 再起動復元メカニズムを採用して、I2CおよびBMC SDの障害を再起動および復元します。これにより、サービスが中断されることはありません。

   いくつかのシナリオでは、修復可能なエラーによって引き起こされる予期しないダウンタイムやビジネスの移行を回避し、本番環境への干渉を防ぐために、障害の自己復旧が実装される。

3. 障害の切り分け

   モジュール内で検出された障害を分離することで、現在のシステムへの影響を軽減し、仕様を削減しながらサービスの実行を継続できる。

   - 一部のメモリー障害シナリオでは、Linux OSのADDDC、PPR、およびSoft Page Offlineを使用して、障害のあるメモリー領域を分離し、その領域へのその後のアクセスによって引き起こされるシステムのダウンタイムを回避することができる。
   - 起動時に、メモリー、CPU、およびPCIEの障害が検出され、自動的に分離されます。サーバーは起動してシステムに入ることができます。

   継続的なサービスとビジネスの移行のニーズを満たすために、いくつかの障害を分離し、負荷を軽減した構成を使用してシステムを起動します。

4. 障害修復

   このモジュールは、各デバイスコンポーネントの可能性を完全に調査し、いくつかの障害を自動的に修復し、特定の障害を迅速に修正します。これにより、現在実行中のビジネスの中断が軽減または排除されます。

   - Intelプラットフォームでは、HDMはMRT方式を使用して、DDR5メモリーチップの状態をリアルタイムで監視し、障害を予測し、障害のあるメモリーの行と列のアドレスをシステムメモリーページの物理アドレスに変換する。次に、HDMはこのアドレス情報をBIOSを通じてOSに報告し、障害のあるメモリーページを分離し、効率的でインテリジェントな障害修復を実現する。
     システムのクラッシュを低減します。
   - BMCはパッチ操作をサポートしており、いくつかの小さな問題を迅速に修正できます。

   一部のシナリオでは、特定のサービスを停止できない場合の障害修復の要件を満たすために、CPUマイクロコードとBMCのオンラインアップグレードがサポートされています。

5. 予測アラーム

   このモジュールは、高度なAI技術を使用してシステムの動作データを監視および処理し、潜在的な欠陥のあるコンポーネントを事前に検出し、ユーザーが潜在的なリスクを戦略的に制御できるようにします。

   - このモジュールは、NVMeドライブの寿命の監視と寿命末期の障害の予測をサポートします。
   - このモジュールは、SATA HDDドライブのSMARTしきい値予測アラームをサポートします。
   - このモジュールは、BIOS検査とADDDCの使用をサポートしており、メモリー障害の検査と予測が可能です。

障害レポート

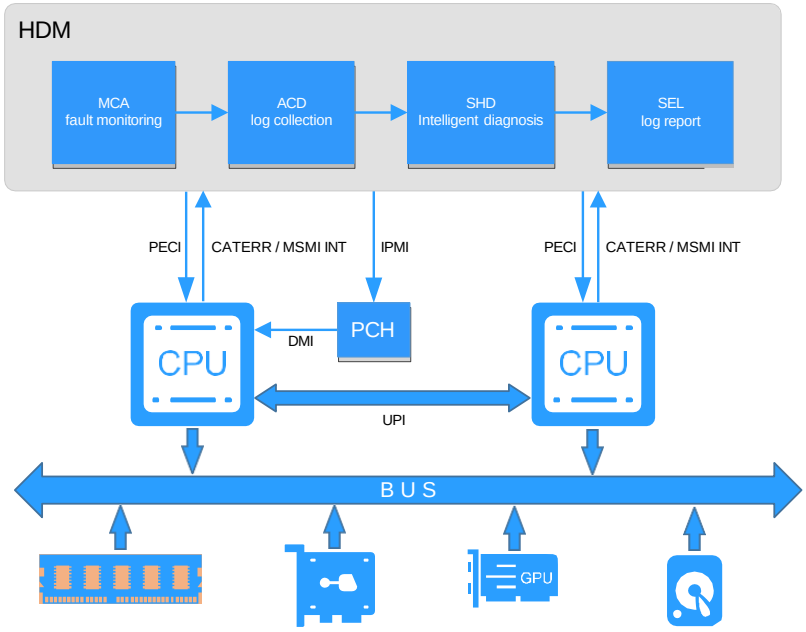
HDMは、ハードウェアとシステムの障害ステータスのリアルタイム監視をサポートし、障害イベントログをプロアクティブに報告する。報告チャネルには、SNMPトラップ、SMTP、Redfishイベントサブスクリプション、およびリモートSyslogが含まれる。

同時に、SDSログを使用して、オフラインの障害レポートおよび診断機能を実装することもできます。HDMのワンクリック収集機能を使用すると、SDSログで診断レポートを表示して、ハードウェア障害に関する詳細情報を取得できます障害診断

MCA Fault diagnosis(インテルプロセッサー搭載サーバー用)

マシンチェックアーキテクチャ(MCA)は、SHDの重要な部分です。MCA障害診断は、プロセッサー、メモリー、PCIeモジュール、およびシステムボードの障害検出と診断をサポートします。SHD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、SHDはAutonomous CrashDump (ACD)に通知して、基本的なオンサイトハードウェア障害情報をアウトバンド方式で収集します。収集されたデータと履歴ハードウェア障害診断データベースに基づいて、SHDはハードウェア障害の位置を特定して分析し、診断レポートを生成し、SELログを報告します。図37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37 MCA故障診断図



1. プロセッサー障害の検出

   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)を含む、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障害診断では、エラータイプを識別し、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タイプは次のとおりです。

   - リードエラー、ライトエラー、プリフェッチエラーなど、キャッシュの修正不可能なエラー。
   - 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修正不能エラー。
   - 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。

2. メモリー障害の検出

   メモリー障害には、修正可能なエラーと修正不可能なエラーがあります。システム内の修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、修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、修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

エラーアドレスが分析され、障害のあるDIMMが特定され、特定のプロセッサー、チャネル、およびDIMMの場所が特定されます。一般的な修正不可能なメモリーエラーの種類は次のとおりです。

- 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不正です。
- メモリーの書き込みまたは読み取りエラー。
- 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。

3. PCIe障害検出

   MCA障害診断は、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モジュールを特定し、特定のプロセッサーおよびスロットを特定することができる。

   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)。
   - 不正な形式のTLP。
   - Completer Abort(CA;完了中止)。
   - 完了タイムアウト(CTO)。
   - 毒を盛られたTLP
   - ACS違反。
   - フロー制御プロトコルのエラー。
   - データリンクプロトコルエラー。
   - Surprise Downエラー。

MCA障害診断(AMDプロセッサーを搭載したサーバーの場合)

AMD製品の場合、HDMはADDCとAPMLを統合します。OSがクラッシュすると、HDMはADDDCツールを使用して、アウトバンド方式でAPMLを介してCPUからクラッシュデータを収集します。HDMは生のCPERファイル情報を収集し、それをプレーンテキストに処理して永続的に記録します。記録されたデータは、専門家がクラッシュ後の環境データを分析するために使用できます。

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する。

1. プロセッサー障害の検出:
   - 修正不可能および修正可能なプロセッサーエラー。MCA障害診断では、特定のソケット上のエラーを特定できます。
   - SMNレジスタ内のエラー。コールドシステムの再起動を引き起こす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、特定のソケット上のエラーを特定できます。
2. 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メモリーエラーを特定できます。
   - 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上のエラーを特定できます。
3. PCIe障害検出
   - PCIeの修正可能なエラーと修正不可能なエラー。MCA障害診断では、スロット上のエラーを特定できます。

メモリー障害診断

メモリーの信頼性を向上させるために、メモリーおよびプロセッサーのサプライヤと緊密に協力して、メモリーRASの機能を調査した。メモリーの信頼性を向上させることを目的として、サーバー内のメモリーのライフサイクル全体を監視している。HDMがメモリーRASで採用した技術的ポイントは次のとおりである。

1. HDMに統合されたインテルMRTメモリーのインテリジェントな修復。

インテルMRTは、マイクロメモリーの故障分布に基づいて故障位置を予測する。OSのオフライン機能を使用して、故障点にプロアクティブに対処し、メモリーの信頼性を向上させることで、システムの安定性をさらに向上させることができる。

- 指針となる方針を持つ予測モデル

  インテルCPUとDDRメモリーメーカーの特徴に基づいて訓練された予測モデルは、従来の予測モデルと比較してより高い精度を達成した。

- OSのオフライン機能を最適化する

  メモリー予測結果をOSにリンクして、障害のあるページを分離および修復することもできます。この操作により、障害が修正不可能なエラーに発展してシステムクラッシュが発生するのを防ぐことができます。

- 不要なDIMM交換の削減

  メモリーエラーを分析し、潜在的なメモリー障害を予測し、ログおよびWebページ内のメモリー位置を正確に特定することで、エンジニアがDIMMの精度を特定するのに効果的に役立ちます。

2. インテルのメモリーに関連するRAS機能を完全に統合

   インテルRAS機能は、アプリケーションシナリオの要件に応じて、ADDC、メモリースペア、メモリーミラー、およびその他の技術的な機能を有効にするように構成できます。スペースを活用することで、メモリーの信頼性をさらに向上させ、パフォーマンスを向上させることもできます。

3. DDR5固有の監視機能を完全に統合

   たとえば、オンダイECC機能は、オンサイトのメモリーに固有のECCミス(主に宇宙線と外部の高速粒子の影響によって引き起こされる)を迅速に修正するためにデフォルトで有効になっている。

   アウトオブバンドは、I3Cバスを介してメモリー上のPMICユニットをリアルタイムで連続的に監視し、メモリーの動作環境をリアルタイムで制御する。

   ECSをサンプリングして分析することにより、ECSの結果に突然変異が存在するかどうかを検証し、記憶障害が発生するかどうかを予測することができる。

4. 動的メモリー情報のアウトオブバンド監視のサポート

   HDMは、メモリーの温度と電圧の主要なセンサーを監視するためのサポートを追加する。

5. メモリー認証と偽造防止のサポート

   HDMは、DIMMがH3C認証を受けているかどうかを識別するためのサポートを追加します。H3C認証を受けたDIMMの認証結果は図38に示されています。H3C認証を受けていないDIMMには、図39に示されている認証結果がありません。

図38 H3C認定DIMM

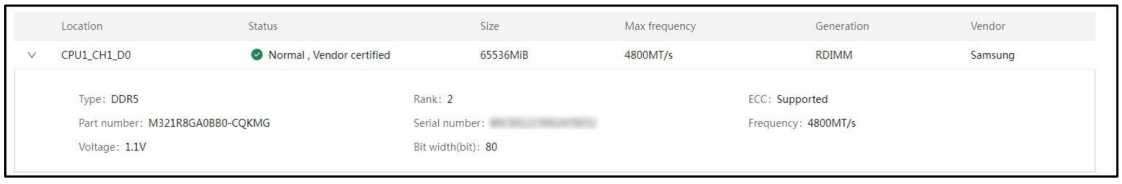
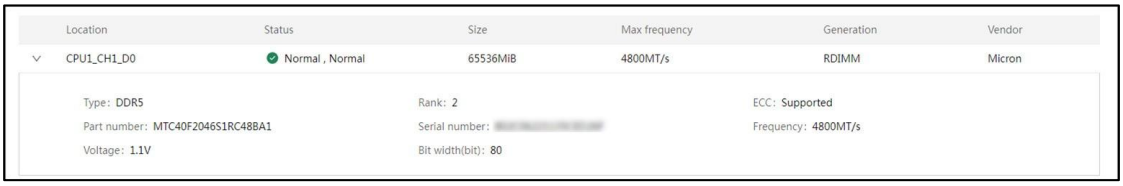


図39 非H3C認定DIMM



電源障害診断

SHD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電源を監視し、24種類の電源障害タイプのうち11種類を識別できます。11種類の障害タイプには、次のものがあります。

- 電源がありません。
- 入力電圧の障害(入力電圧不足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。
- 吸気口の温度異常(過熱警報および保護、低温警報および保護を含む)。
- 過電圧アラームおよび保護、低電圧アラームおよび保護を含む出力電圧障害。
- 過電流アラームおよび保護を含む出力電流障害。
- 電源装置のLEDが1 Hzで点滅しており、電源障害を示しています。
- IIC通信異常
- 不正なEEPROM情報(不正なFRU情報やH3C認証の欠如など)。
- 電源装置のモデルが一致しません。
- ロードバランシングが行われていません。

システムボードの障害診断

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統合されています。SHDは、次のような70種類以上のシステムボード関連の障害を特定します。

- プロセッサーおよび他のボードのセカンダリパワーサプライを含む、サーバーのセカンダリパワーサプライの障害。
- ファンの欠如とPWM速度制御の異常。
- 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。
- 異常な電圧または電流。

PCIe障害診断

SHD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の障害(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不在、およびネットワークアダプターの不在を含む)。
- ライザーカードの異常な存在。
- NCSIチャネルの異常な変化。

ストレージコントローラーの障害診断

SHD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種類の障害を特定できます。

- 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障害
- ドライブ障害。
- 電源障害保護モジュール障害。

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でアクティブな予測アラームをサポートします。

- **Processors**: 修正可能な構成エラー、過熱エラー、UPIバスエラー、およびDMAエラーに関する予測アラーム。
- **Memory**: 修正可能なECCメモリーエラー、検査エラー、およびADDDC事前アラームに関する予測アラーム
- **Drives** -HDDおよびSSDの予測障害、メディアエラー、およびPredfailに関する予測アラーム、HDDのみの不良セクタに関する予測アラーム、およびSSDまたはNVMeの残りの寿命に関する予測アラームと監視。
- **RAID card** -RAIDカードの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。アレイカードのバッテリの事前障害(低電圧)のアラーム。
- **Network adapters**: 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。
- **Power supplies**: 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、電源のセルフテストエラーに関する予測アラームなど、予測障害に関する電源のアラーム。

リモート診断

次のようなホストのリモート診断をサポートします。

- シリアルポートログ、ブルースクリーンスナップショット、およびブルースクリーン記録機能を使用して、ホスト情報を分析します。
- ASD(Intel)やiHDT(AMD)などのリモートデバッグメソッドをサポートします。

サポートされている障害のリスト

各コンポーネントでサポートされる主なアラームは次のとおりです。

表5 障害

コンポーネントタイプ	サポートされるキーアラーム
BMC	システムボード、各拡張ボードバックプレーン、ライザーカード、およびファンボードの消費電力が上限および下限のしきい値を超えたときに生成されるアラーム。
BMC	システムボード、各拡張ボードバックプレーン、ライザーカード、およびファンボードの電圧が上限および下限しきい値を超えたときに生成されるアラーム。
BMC	システムボード、各拡張ボードバックプレーン、ライザーカード、およびファンボードの電流が上限および下限のしきい値を超えたときに生成されるアラーム。
BMC	セルフテスト機能を使用したBMC管理システムプロセッサーのアラーム。
BMC	BMCは、監視対象のすべての電圧、電力、および温度に対して、メジャーアラームとクリティカルアラームのしきい値を設定します。
BMC	各電圧、電流、または消費電力センサーが読み取りに失敗した場合にアラームとログを記録します。
BMC	RAIDコントローラーのステータスの監視とアラーム通知。
BMC	RAIDカードのBBU(キャパシター)ステータスの監視と警告
BMC	ネットワークカードのステータスの監視と警告
BMC	ネットワークカード上のトランシーバモジュールのリンクステータスの監視とアラーム通知。

BMC	電子タグの読み取りに失敗した場合のアラームです。
BMC	BIOSまたはファームウェアROMの損傷に関するアラーム。
BMC	TPMまたはTCMの検出とアラーム
BMC	ビデオコントローラーの検出とアラーム。
BMC	BMC NANDフラッシュステータスの監視と警告
CPU	プロセッサーの状態が変化すると、HDMアラームがトリガーされ、ログに記録されます。
プロセッサー	CPUのコア電圧であるCPU_VCOREは、消費電力についてリアルタイムで監視されています。
プロセッサー	CPUサーマルスロットリング
プロセッサー	内部プロセッサーエラーの検出とアラーム
プロセッサー	プロセッサーPCIe MMIOリソースの検出とアラーム。
プロセッサー	プロセッサーの不一致
PCIe	PCIeの高度なエラー報告
PCIe	PCIeで修正されたエラーの報告
PCIe	PCIeリンクCRCエラーのチェックと再試行
PCIe	PCIe
PCIe	PCIeの停止と音
PCIe	PCI Expressのホットプラグ
PCIe	PCIまたはPCIEカードの状態が変化すると、障害診断パネルのアラームがトリガーされ、ログに記録されます。
PCIe	PCIeカードのセルフテスト状態の検出とアラーム。
PCIe	PCIeカードの初期化状態の検出とアラーム
PCIe	PCIeリタイマーまたはスイッチの検出とアラーム。
システム	ホットスワップをサポートするコンポーネントの場合、ホットスワップ信号には、ホットスワップ中のデバイスへのEOS損傷を回避するための分離回路が必要です。
システム	共有バス(IICなど)にアクセスするときの障害またはフリーズの検出。
システム	CPLDオンラインアップグレードインターフェイスのアラーム。
システム	CPLDカスタムバスアラーム。
システム	バックプレーン、エクスパンダ、ライザーなどの拡張ボードの状態を監視および警告します。
システム	取り付けイヤーの定位置状態の検出および警報。
システム	電源ケーブルの状態を検出し、アラームで知らせます。
システム	システム構成不一致アラーム。
システム	ウォッチドッグの検出とアラーム
システム	設計されたエラーレコード
システム	マシンチェックアーキテクチャ(MCA)のリカバリ-非実行パス*
システム	Enhanced Machine Check Architecture(EMCA):第1世代。
システム	Enhanced Machine Check Architecture(EMCA):第2世代*
システム	LCD状態の検査とアラーム
UPI	インテル(R)UPIリンクレベルリトライ*

UPI	UPIリンクCRC検証
UPI	ソーステキスト:インテルUPIプロトコルは、32ビットCRCを使用して保護されています。
UPI	インテル®UPIの修正済みおよび未修正の障害、修正済みエラーのしきい値処理(KTI、PCIe)*
UPI	インテルUPIウイルスモード*
電源	システム ソフトウェアによって設定された電力上限値は、構成された電源モジュール内の最小 PSU の 1つの定格電力値を超えることはできません。
電源	障害が発生した電源装置(PSU)の特定
電源	電源モジュールのプルアウトアラーム
電源	電源の冗長性不足アラームです。
電源	電源が識別できないことを示すアラーム。
電源	電源装置の内部ファンが停止します。
電源	電源装置とシステム間の通信障害のアラームです。
電源	電源モジュールの過電圧保護アラームです。
電源	電源モジュールの入力過電圧アラームです。
電源	電源モジュールの入力不足電圧保護アラームです。
電源	電源モジュールの入力不足電圧アラームです。
電源	電源モジュールの出力過電圧保護アラームです。
電源	電源モジュールの出力過電圧アラームです。
電源	電源モジュールの出力不足電圧保護アラームです。
電源	電源モジュールの出力不足電圧アラームです。
電源	電源モジュールはあるが、電源が入っていないか、電源入力が失われている。
電源	電源モジュールの過熱保護アラームです。
電源	電源モジュールの過熱アラームです。
電源	異なるモデルの混合電源モジュールアラーム。
電源	システムの電源切断理由の監視。
電源	電源PG/PWROKの監視警報
電源	電源投入時タイムアウトアラーム。
電源	スロースタート回路用MOSチューブの電圧降下の監視警報
ファン	ファン(シャーシ)の有無を変更すると、HDMアラームがトリガーされ、ログに記録されます。
ファン	ファン(シャーシ)の回転速度が変化すると、HDMアラームがトリガーされ、ログに記録されます。
ファン	ファンケーブル障害のアラームです。
ファン	ファンユニットとシステムボードの通信障害のアラーム。
ファン	システム起動時のファン障害の切り分け方法。
キー集積回路(IC)	CPLD障害アラーム。
キー集積回路(IC)	RTC障害アラーム。

キー集積回路(IC)	EEPROM障害アラーム。
キー集積回路(IC)	FLASHおよびSSRAMの障害を時間指定で検出するアラームです。
キー集積回路(IC)	PCH障害アラーム。
キー集積回路(IC)	クロック検出およびアラーム。
環境(Environment)	マイナーアラームまたはクリティカルアラームのしきい値を超えるデバイスの実際の動作温度は、HDMを介してアラートをトリガーし、ログに記録される必要があります。
環境(Environment)	デバイスの実際の動作温度が致命的なアラームのしきい値を超えると、HDMを介してアラームがトリガーされ、ログに記録されます。
環境(Environment)	監視プロセスでは、温度アラームと、リセットや電源切断などの異常保護を記録し、保護対策を実施する前に保護の原因を保存する必要があります。
環境(Environment)	デバイスが温度センサーにアクセスできない場合のアラーム。
環境(Environment)	温度センサー読み値異常データ異常
メモリー	メモリーサーマルスロットリング*
メモリー	メモリーアドレスパリティ保護
メモリー	メモリー要求とパトロールスクラビング
メモリー	メモリーSMBusハングからの復旧
メモリー	データスクランブリング
メモリー	メモリーのセルフリフレッシュ
メモリー	メモリー訂正エラーのレポート
メモリー	CPU0_DDR_VDDのコア電圧と消費電力をリアルタイムで監視しています。
メモリー	メモリーPFA
メモリー	メモリーの位置とステータスの変更は、障害診断パネルを通じて警告され、ログに記録されます。
メモリー	エラーのためにBIOSがメモリーモジュール内のランクまたはDDRコントローラー内のチャネルを無効にする原因となったインシデントは、SELに記録する必要があります。
メモリー	メモリーのECCエラーに関する詳細情報がログに記録されます。
メモリー	BIOSは、ECCの数を設定できるしきい値を提供する必要があります。システム内のECCの数がしきい値を超えると、BIOSはSELにログインします。
メモリー	NVDIMMステータスの監視とアラーム
メモリー	メモリータイプの検出とアラーム。
メモリー	メモリー互換性の検出とアラーム。
メモリー	メモリー初期化の検出とアラーム
ドライブ	ドライブの読み取りまたは書き込みに失敗すると、アラームがトリガーされます。
ドライブ	ドライブのリアルタイムSMART検出。障害が発生すると、アラームが発行され、適時に記録されます。
ドライブ	ドライブが切断されると、高レベルのアラームがトリガーされ、ユーザーにメンテナンスを求めるメッセージが表示されます。
ドライブ	論理ドライブの検出とアラーム。
ドライブ	ドライブ構成の検出とアラーム

ドライブ	RAIDステータスの検出とアラーム
ドライブ	SSDドライブの寿命検出とアラーム。

注:アスタリスク(*)が付いている項目は、プロセッサーキテクチャに関連しています。

アプリケーションシナリオ

UniSystemがデバイスログを一括取得

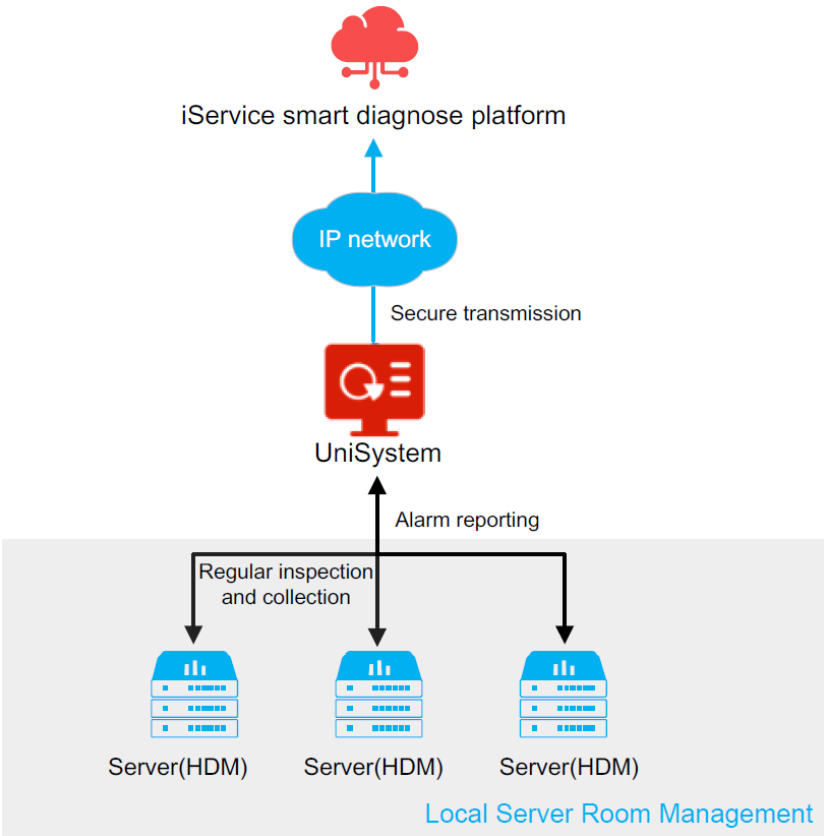
H3C UniSystemは、HDMのバルク管理をサポートし、HDMインテリジェント診断に基づくパトロールレポートを提供する。UniSystemは、バッチサーバー機器管理を完了し、サーバーバッチSDSログを1つのパッケージでリモートダウンロードして、お客様の運用とメンテナンスのニーズを満たすことができる。

顧客がSDSログを一括して迅速かつ便利にダウンロードできるようにするために、H3Cは、SDSログ用の帯域外一括ダウンロードツールを提供している。この機能は、スクリプトメソッドを使用してHDMが提供する帯域外インターフェイスを通じて実現でき、インストールや展開は必要ない。

リモート障害レポート

UniSystemは、手動および自動のリモート障害レポートを含むオートコール(リモート修復)機能をサポートしています。管理対象サーバーの障害が検出されると、リモート障害レポートを実行できます。即時レポート、定期レポートおよび障害トリガーレポートを含む複数のリモート障害レポートモードがサポートされています。

図40 障害レポートのフレームワーク図



FIST/HDMはiServiceに直接接続して、デバイス障害報告プロセスを完了します。ユーザーはiServiceアカウントを購入する必要があります。購入後は、定期的にログを転送したり、障害後に自動的にクラウドにアップロードしたり、インテリジェントなクラウドベースの操作の恩恵を受けたり、障害を予測したりできます。

ホスト監視機能

サーバーの主な目的は、ユーザービジネスのためのストレージ、コンピューティング、さらには通信サービスを提供することです。これらのサービス機能は、主にオペレーティングシステムとそのアプリケーションを通じて実現されます。同時に、ホストの動作ステータスを監視することも、次の2つの要件を満たすために非常に必要です:

- 監視要件:運用保守管理中に、ホスト情報を監視することにより、業務の運用状況を把握し、目標とする最適化処理を行うことができる。
- 障害記録の要件:主要なイベントとそのコンテキストを追跡して、潜在的な問題が発生した場合に根本原因を迅速に特定します。

上記の監視目的を達成するために、HDMはBIOSおよびFIST SMS、iFISTソフトウェアと連携して動作し、次の機能を提供します。

- ホストのライフサイクルを管理します。
- 各スタートアップのコンテキスト情報を簡単に理解できるように、ブートログ機能を提供します。
- 完全なホストアドレススペースリストを記録して、デバイスパラメーターの変更を便利に表示し、異常を検出します。
- ホストの再起動の理由を分析し、障害のあるコンポーネントをすばやく特定します。
- 特に異常な再起動後のダウンタイムコンテキストを収集し、いくつかの極端なシナリオに対処するための修復収集を行います。
- BMCを通じて、OSの導入、BIOS/コンポーネントの構成、およびグラフィックスカードのパラメーターの構成を行うことができます。
- BMCを通じてシステムの内部ステータスを理解するのに役立ちます(FIST SMSサポートが必要です)。
- ホスト容量の監視と予測を行います(FIST SMSのサポートが必要です)。

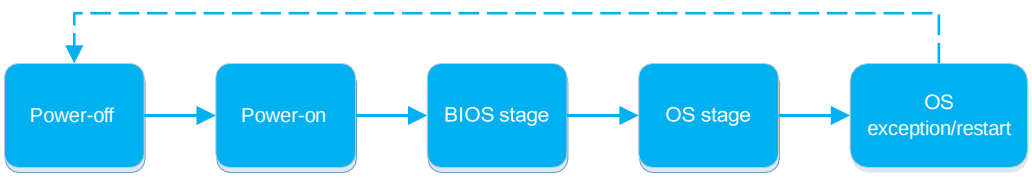
ホストの運用能力の最適化ポイント

1. HDMは64MのVRAMサイズをサポートし、サポートされる最大分解能は1920×1200 32 bpp@60 Hzです。これにより、オンボードグラフィックカードをBIOS経由で無効にすることができ、KVMおよびパネルVGAインターフェイスを介してホスト出力を表示できます。
2. ハードドライブスロットとPCIEカードスロットの情報は、バンドを介して取得できます。

ホストのライフサイクル管理

HDMは、サーバーの起動と操作を包括的に監視する。標準的なセンサーとイベントログ、2つの起動間の情報の比較、ファームウェアのドリフト検出、タイムアウトの監視、BIOSが送信したログのタイムリーなロギング、疑わしい障害コンテキストの抽出などを通じて、起動ごとに情報を記録して表示する。許可されたアクセスの範囲内で、ホストの動作を最大限に記録し、その後のトラブルシューティングに役立つ。

図41 ホストの再起動の状態



実際、上記のどの段階でもエラーが発生する可能性があり、システムが異常に起動したり、クラッシュしたりする可能性があります。

IPMI標準センサーは、ホストの主要な段階に対応するイベントを定義します。実装中、HDMは上記の情報に基づいて完全に拡張されます。

- ステージID。現在の起動状態を識別します。
- 異常な起動レコード。
- 起動タイムアウトの監視。
- 電源モジュールのステータス遷移レコード。
- 例外を実行しています。

HDMは、裏付けとなる標準情報に基づいて、主に以下を含む記録をさらに拡張する。

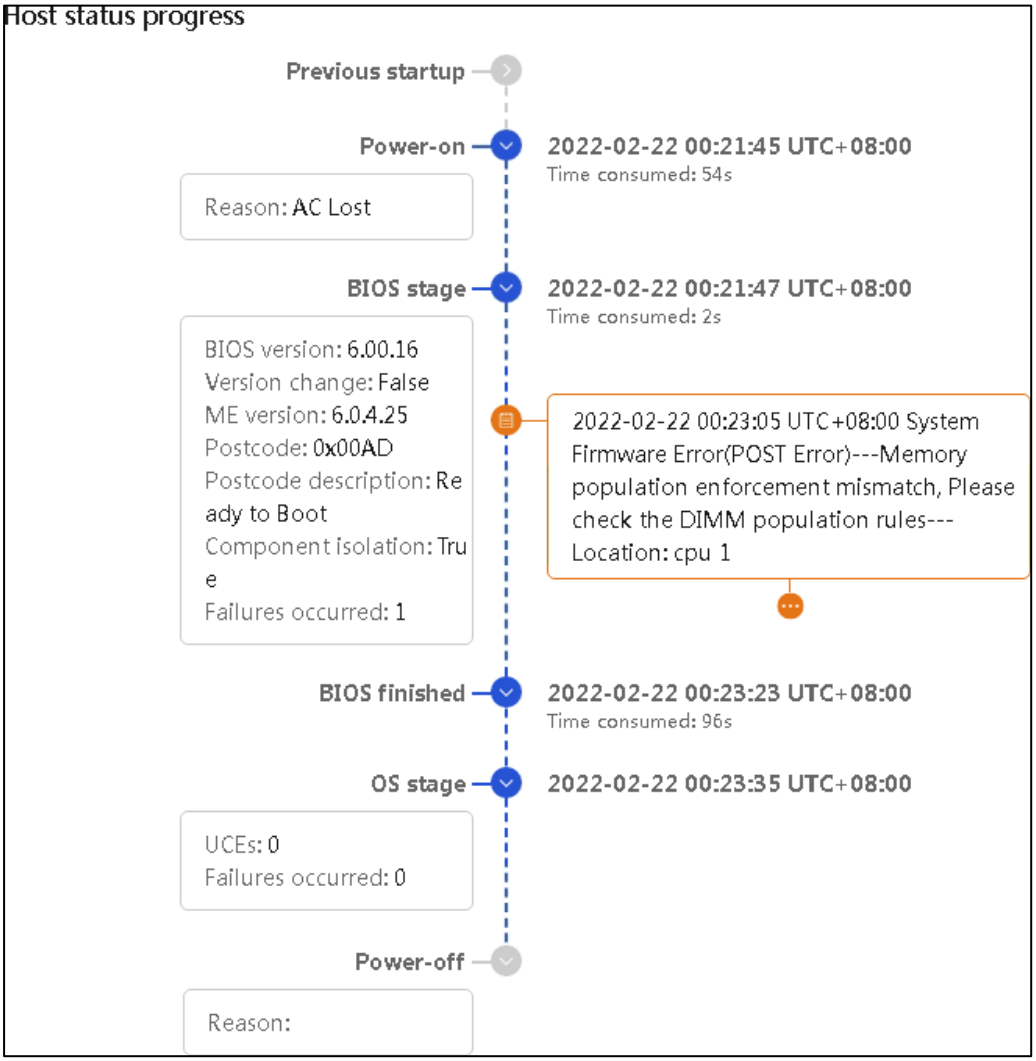
- ホストシリアルポートのロギング。
- 障害コンテキストログの収集。
- アドレススペースおよびデバイス情報の取得。ホストの電源がオンになると、HDMは次の処理を

実行します。

- CPUタイプ、PCIeデバイス、およびメモリーデバイスを識別します。デバイストポロジを編成します。BIOSによって渡されたメモリーマップ情報に基づく各デバイスの関係とトポロジー情報。
- ホスト上の電源投入イベントへのインターフェイスを提供し、さまざまなモジュールによって登録されたイベントを処理します。たとえば、以前の異常イベントの解決や一部のセンサー情報の更新などです。
- BIOSが起動された時刻を記録します。
- ホストのアドレス空間情報を記述します(後で簡単にトラブルシューティングおよび分析できるようにします)。

再起動プロセス中にホストが記録するさまざまな状態、期間、再起動の理由、および障害レコードを図42に示します。

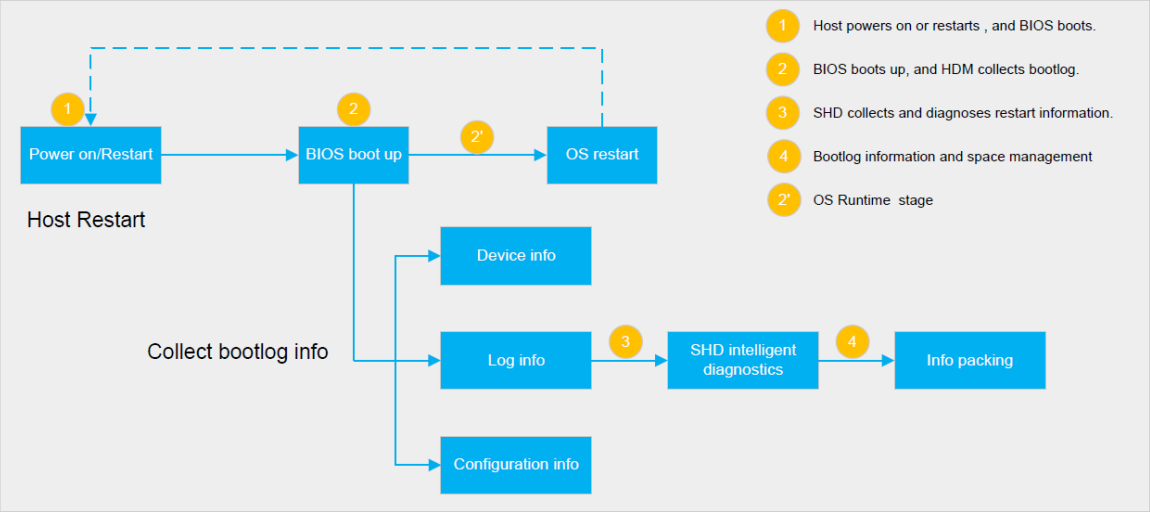
図42 ホストステータスの進行状況



ブートログ機能

ホストの再起動時には、再起動原因の迅速な特定を容易にするために、主にデバイス情報、構成情報、およびログ情報を含むブートログ情報を収集する必要があります。外部支援を使用して、2つの連続するホスト再起動間のデバイス情報の差を比較することによって、障害の差を特定できます。現在のブートログは、SDSログおよび電子メールアラートを通じて取得できます。

図43 ブートログレコード情報



ブートログ関連の情報は、SDSログに記録されます。

ホストの再起動の理由

ホストの再起動イベントはビジネスに重大な影響を与えるため、原因を迅速に特定する必要があります。たとえば、ソフトウェアの問題、運用上の問題、ハードウェアの問題のいずれであるかを特定します。より詳細な情報を入手して、問題を迅速に絞り込み、障害のあるユニットを特定します。

- **Power On**: 以前は電源オフ状態であったホストの電源をオンにするプロセスです。後続の実装を容易にするために、ユーザーが介入する電源オンアクションは、以前の状態とは無関係に、起動操作の新しいラウンドとみなされます。
- **システムクラッシュ**: システムが応答しなくなりましたが、電源が切れていません。手動またはBMC自動の電源切断操作が必要です。
- **電源OFF**: DC電源が遮断された状態になります。
- **Restart**: 一般に、ユーザーの場合、ホストの再起動イベントが発生しているかぎり、これはホストの再起動とみなされます。さらにセグメント化すると、ホストの再起動とホストの停止という2つのシナリオが含まれます。より具体的には、再起動にはウォームリセット、ソフトリセット、電源サイクルおよびその他の再起動方法が含まれます。

電源状態の変更については、業界は既存の標準定義に従って実装することで合意に達しています。HDM設計は、ACPI、Redfish、およびIPMI定義の説明に準拠しています。

- ACPI状態遷移。
- IPMIで定義されたユーザーインターフェイス。
- Redfishでのステータス定義。

システムリソースの監視

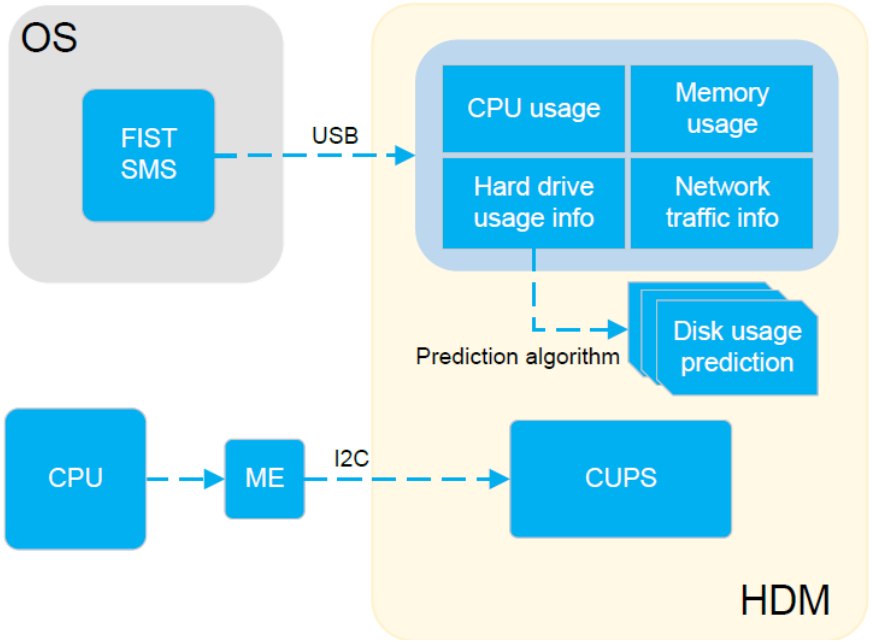
HDMは、複数の視点からのホストリソース使用の継続的な監視をサポートし、各リソースの使用履歴を内部的に記録し、統合された外部表示インターフェイスを提供します。監視タイプには、次のものがあります。

- CPUレベルの監視では、CPUのCUPSメカニズムを使用して、CPUレベルでリソースの使用状況を監視します。
- OSレベルの監視は、FIST SMSに依存してOSレベルでリソースを監視する。CPU占有、メモリー使用量、ドライブ使用量、ネットワーク使用量など、インバンドオペレーティングシステム内のリ

ソースの使用状況を検出できるリソースの使用状況に関する履歴データを提供し、将来のデータを予測します。一部のリソースで使用される履歴データに基づいて、将来のデータを予測してページに表示できるAI予測モデルを確立し、障害を事前に防止および処理します。

- 一部のリソースにしきい値とアラームメカニズムを提供します。
- ドライブの平均I/O待機時間を表示します。対応するドライブパーティションのI/Oパフォーマンスを評価するために使用できます。

図44 ホストリソースの監視情報



HDM O&Mおよび診断のシステムリソースページでは、システムリソースに関する監視情報を表示できます。FIST SMSが存在する場合は、CPU、メモリー、ドライブ、GPUおよびネットワークアダプターの豊富なリソース使用情報および履歴トレンド、ならびに周辺機器のモデルおよびインターフェイスレートを表示できます。また、CPU、メモリーおよびドライブ使用のアラームしきい値の設定もサポートしています。リソース使用率がアラームしきい値を超えると、システムはアラームを生成します。リソース使用率が正常に回復すると、システムはアラームを消去します。

図45 FIST SMSが存在する場合のリソースの概要

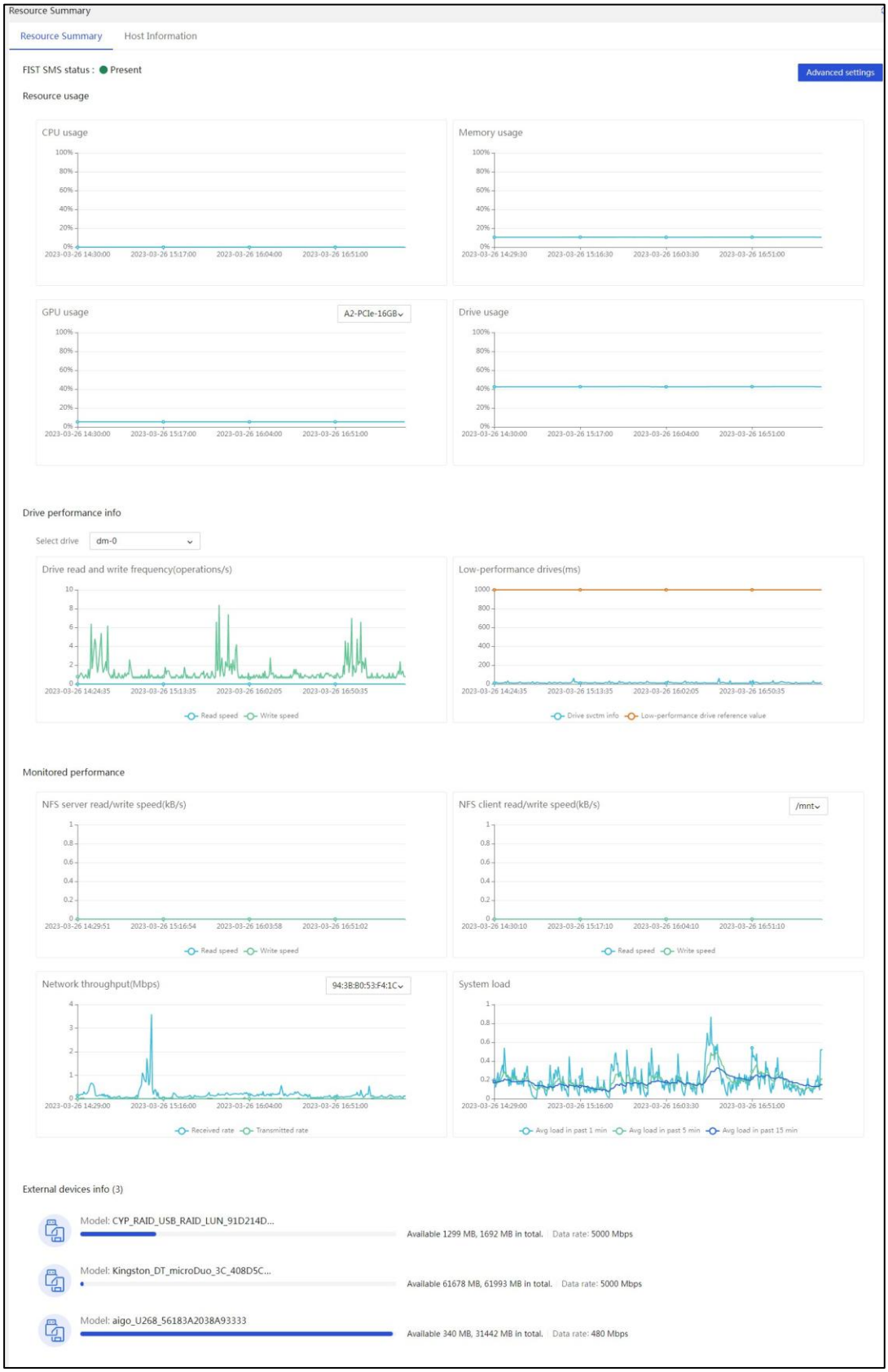
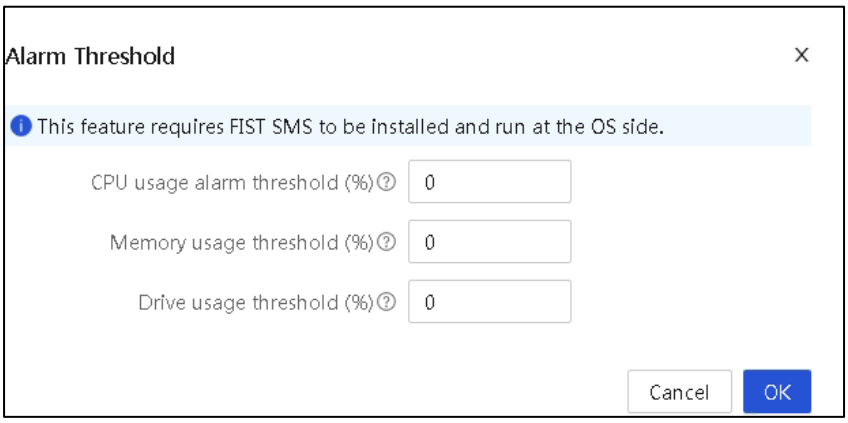


図46 FIST SMSが存在する場合のしきい値の設定



ホストウォッチドッグメカニズム

ホストのBIOSとOSがハングするのを防ぐために、HDMはホスト上のウォッチドッグを監視および処理する機能を提供し、BIOSまたはOSの異常が検出された場合には、ユーザー定義のポリシーに基づいて対応するアクションを実行できる。

主なサービスプロセスは次のとおりです。

1. BIOSおよびOSカーネルスイッチを介して対応するタイマーをイネーブルにします。
2. HDMは対応するWatchdogステータスを監視します。
3. HDMは、ユーザー定義の戦略(無視、再起動、シャットダウン、時限割り込みなど)に基づいてタイムアウトを処理する。

最初のSMS

FIST System Management Service(FIST SMS)は、HDMデバイス管理のサポートを提供するエージェントレス管理ソフトウェアです。FIST SMSは、オペレーティングシステム情報、使用率、ソフトウェアインストールインベントリなどの広範なサーバー情報を提供し、オペレーティングシステム情報およびアラート情報を通じて強化されたハードウェア監視および管理をお客様に提供します。

FIST SMSは、ホスト側でのHDM帯域外監視の監視機能を効果的に強化することができる。同時に、FIST SMSとHDMの間の仮想チャネルに基づいて、HDMのホスト側の監視と制御機能を完全に補完し、ホスト側への影響を効果的に軽減することができる。HDMは、ソフトウェアドライバーの名前やバージョン情報など、リソースの使用状況情報とホストソフトウェアリストを取得できる。

FIST SMSは、運用保守の一元管理の要求に応えるため、HDMの障害ログのOS側への転送をサポートし、OSシステム管理ログへの転送に加えて、転送パスとファイルの2つのカスタマイズ方法をサポートするとともに、ユーザーのカスタマイズニーズに合わせてログストレージの形式とレベルをカスタマイズするログ転送機能をサポートしている。

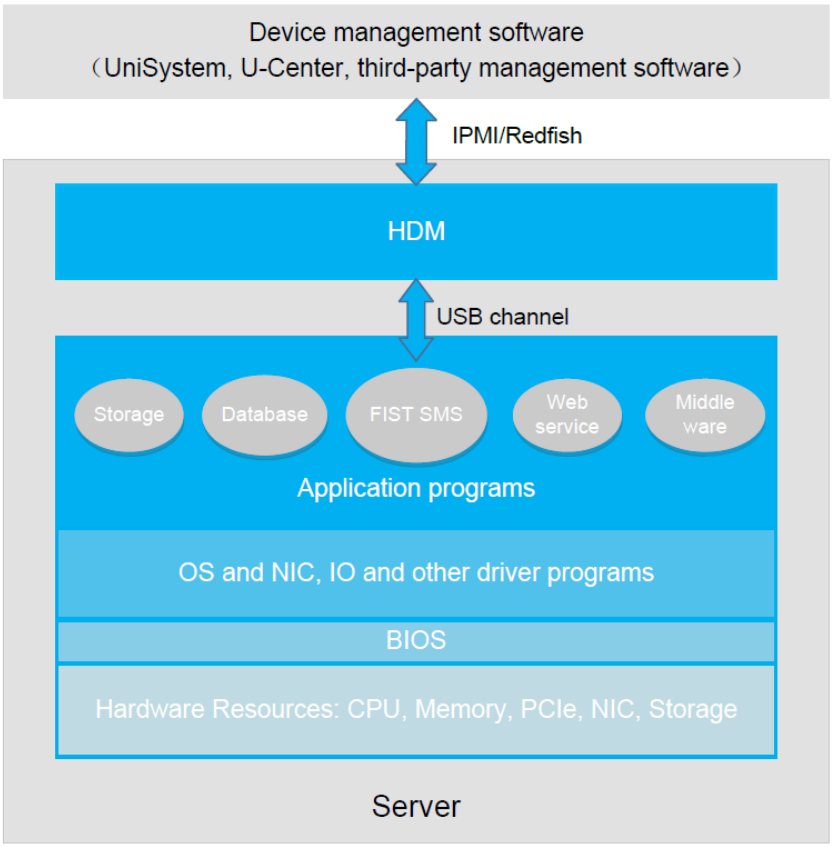
インストール後、FISTは次の機能をサポートします。

- ホストソフトウェアリスト。
- OSの内部リソース使用率を取得します。
- ネットワークカードポートのリンクアップおよびダウン情報。
- ドライブ容量の予測。
- GPUの使用とシステムの負荷。

FIST SMSの動作原理:FIST SMSは、HDMのアウトオブバンド監視機能を強化し、OS側でサーバー

ハードウェア障害を監視する機能も提供します。これにより、ユーザーは障害が発生するとすぐに検出できるため、迅速なビジネス移行とロードバランシングが可能になり、ビジネス障害の影響を効果的に軽減できます。

図47 FISTのSMS階層



FIST SMSがインストールされると、HDMは表6に示す追加情報を取得できます。

表6 FIST SMSで取得した情報一覧

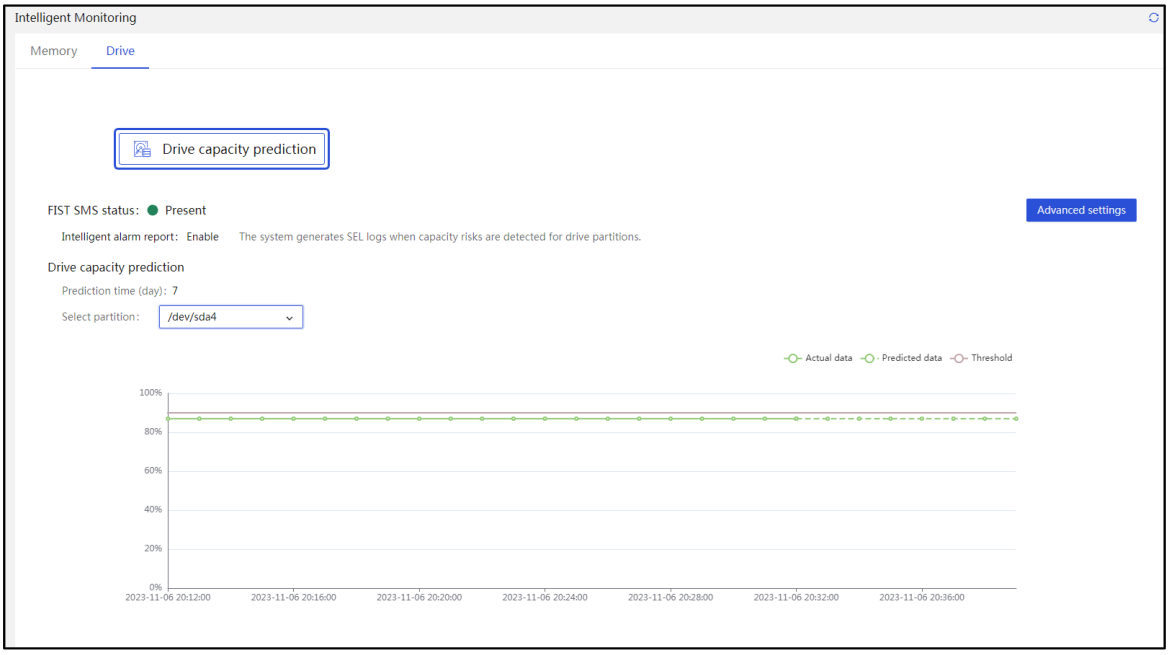
情報名	FIST SMSがインストールされていない	FIST SMSがインストールされている
OSレベルのCPU使用率	/	はい
OSレベルのメモリー使用量	/	はい
OSレベルのネットワークスループット	/	はい
ドライブの使用状況	/	はい
GPU使用率	/	はい
システム負荷	/	はい
NFSクライアントの読み取り/書き込み速度	/	はい
NFSサーバーの読み取り/書き込み速度	/	はい
周辺機器の情報	/	はい
トランシーバモジュール情報	/	はい
ドライブ容量の予測	/	はい
ソフトウェアリスト	/	はい

容量予測

計画された変更とハードドライブのアップグレードにより多くの時間を提供するために、HDMは、Holt-Winter時系列予測アルゴリズムを使用して、現在のシステムの論理ドライブ容量を7～21日前に予測する、論理ドライブ容量予測および警告機能を提供する。事前に予測することで、ユーザーは在庫計画を立て、資材を合理的に管理することができる。

注:この機能を使用するには、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します。

図48 ドライブ容量の予測



ホストのセキュリティ

ホストへのHDMアクセスに必要なセキュリティ要件は、ユーザーによって異なります。

- 通常、デフォルトのHDMユーザーはホストへのすべてのアクセス権を持っています。
- ベアメタルなどのシナリオでは、インバンドを介したアウトオブバンドアクセスの厳密な監査と制御が必要である。

ホストには、HDMに対するデフォルトのアクセス権があります。次に例を示します。

- 帯域内のHDMをアップグレードします。
- サーバーのシャットダウンやストレージメディアの設定など、デバイス内のBTまたはKCSチャネルを介してHDMが提供する機能を操作します。

HDMは、様々なアプリケーションシナリオを十分に考慮して設計されています。複数のデータセンターで検証されたアプリケーションのニーズを満たすための対応する機能を提供します。主な機能は次のとおりです:

- 操作ログの記録。後の監査に便利です。
- IPMIブラックリストおよびホワイトリストメカニズムを介してコマンドアクセス制御を提供します。

メンテナンス

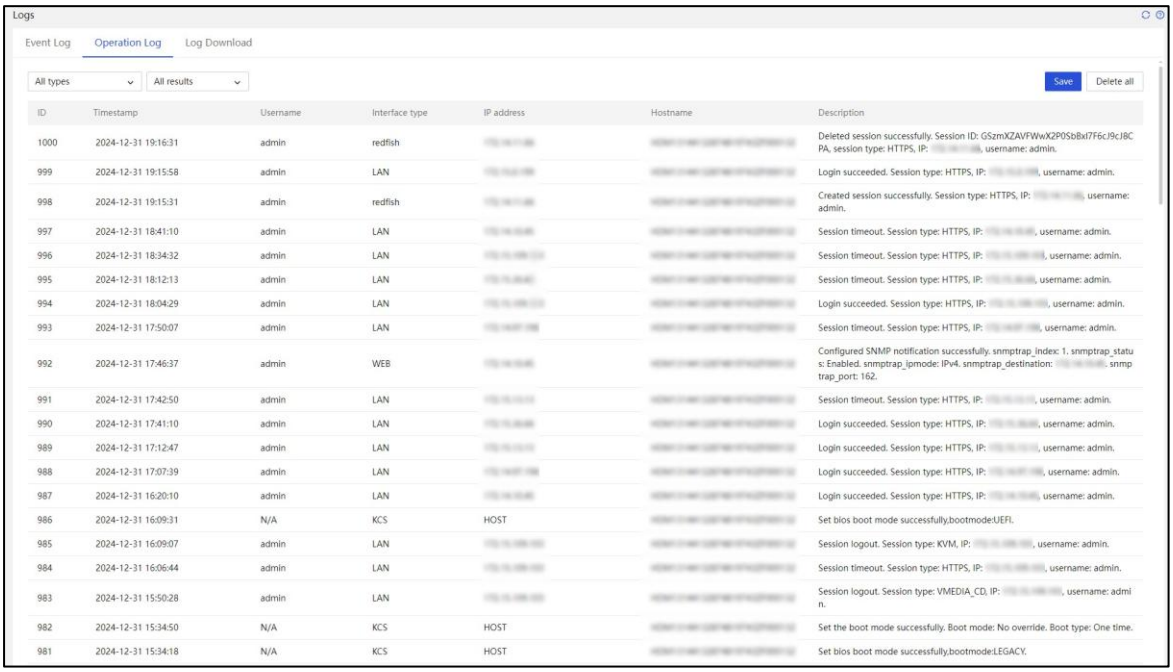
操作ログ

動作ログには、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、および設定ログエントリが含まれます。

- 監査ログエントリは、セキュリティ監査のためにHDM管理イベントを記録します。
- ファームウェア更新ログエントリには、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のエントリには、ハードウェア更新とその結果が記録されます。
- 設定ログエントリには、ユーザーの設定操作とその結果が記録されます。

ログエントリには、図49に示すように、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。イベントの重大度レベルには、成功および失敗が含まれます。

図49 Operation Logページ



イベントログ

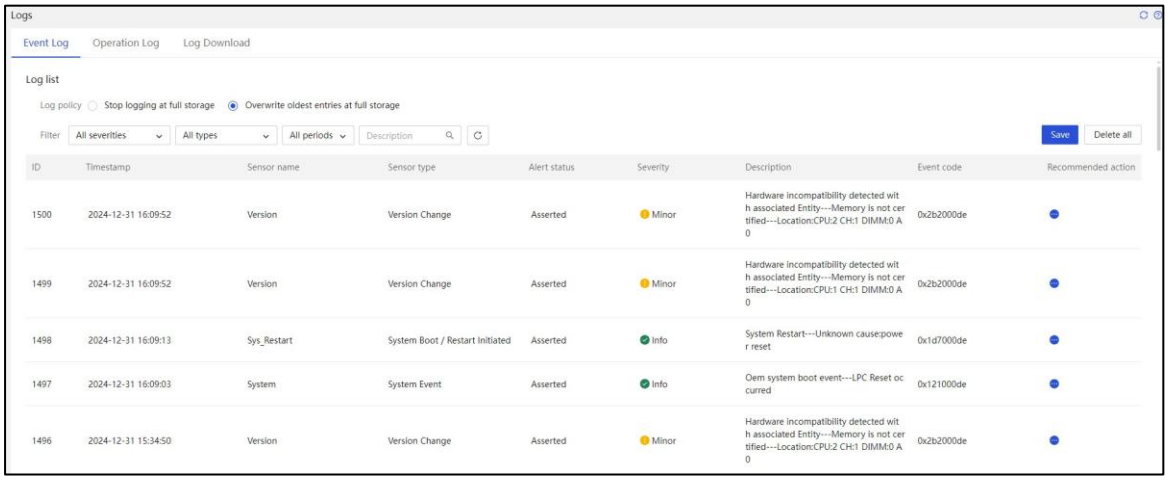
イベントログには、サーバーセンサーによって報告されたイベントが記録されます。イベントの重大度レベルには次のものがあります。

- **Info** -イベントはシステムに悪影響を及ぼしません。アクションは必要ありません。情報イベントの例には、予想される状態変更イベントやアラームが削除されたイベントなどがあります。
- **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** -このイベントにより、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** -このイベントにより、システム停止または電源障害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。

センサー名、重大度レベル、およびログ生成時間でイベントをフィルタリングできます。

図50 イベントログページ



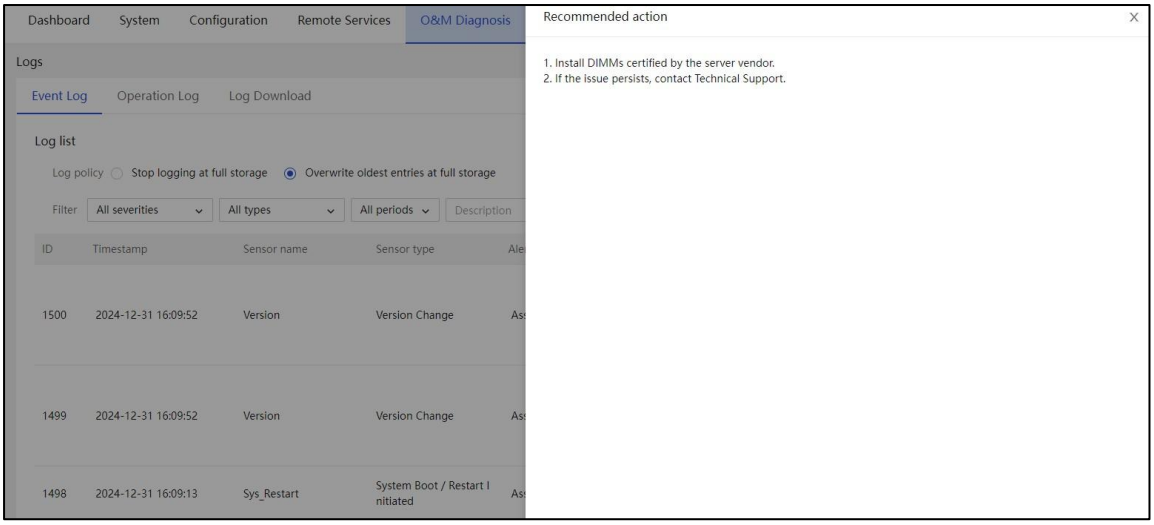
イベントコード

イベントコードは、HDM内の一意のイベントログエントリを識別します。ユーザーは、イベントコードを使用してデバイス上の障害タイプを特定できるため、関連するログマニュアルで詳細を簡単に照会できます。

推奨処置

HDM Webインターフェイスは、システムイベントに対して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51推奨処置の表示



シリアルポート接続

HDMは、SOL機能が有効になっている場合に接続する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。

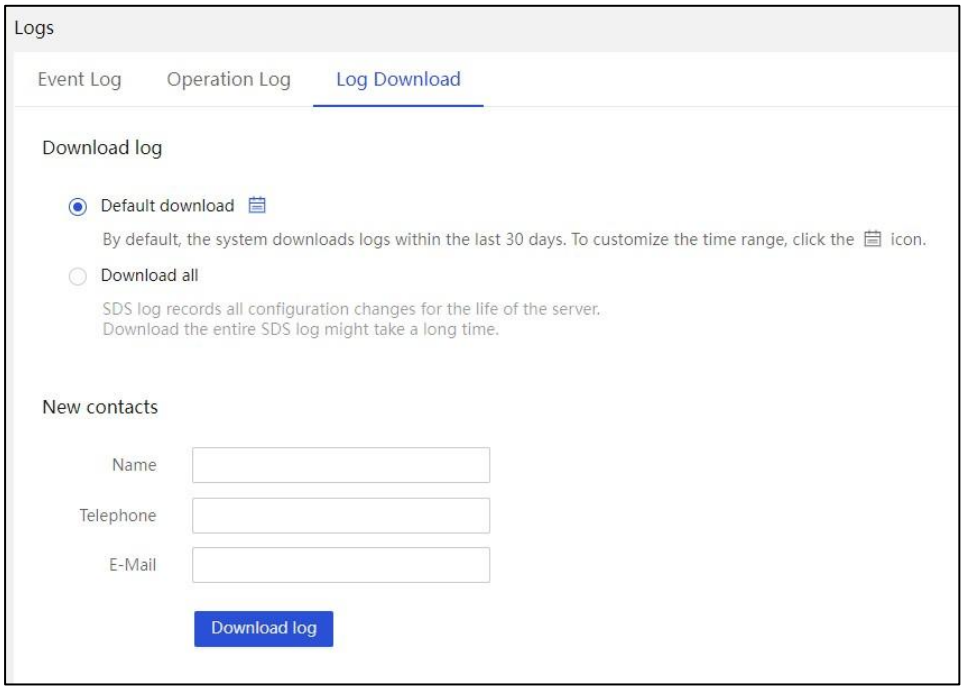
シリアルポート情報の記録

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。

ブラックボックス(ログのダウンロード)

この機能を使用すると、ユーザーはサーバーのライフサイクル全体にわたって、イベントログエントリ、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ダウンロードできます。ダウンロードしたログを表示して、サーバーの操作ステータスを取得できます。SDSログを完全にデコードするには、テクニカルサポートに連絡してください。ログのダウンロード時に連絡先情報を追加することをお薦めします。

図52 SDSログのダウンロード



一般的に収集されるログの内容と対応するパスを表7に示します。

表7 ログ情報

ログの内容	ファイルパス
ファームウェアのバージョン情報	static\firmware_version.json
BMCシステム構成情報	dump\bmcsys_info
サーバーのハードウェア情報	static\hardwareinfo.xml

BMC再起動理由レコード(シリアルポートの再起動、HDMの再起動、HDMパーティションの切り替え、IPMIコマンドの再起動、AC電源喪失またはUID長押しによる再起動、WDTタイムアウトによる再起動など)	sdmmc0p4\log\sysmanage\bmc_reboot.log
HDMとシステム再起動の詳細な記録	sdmmc0p4\log\emerg.log
BMCシステムプロセスの再起動の記録	sdmmc0p4\log\proj\debug_system_manage.log
BIOS再起動プロセスの記録:BIOS再起動プロセス中に生成されたPOSTコードを記録し、BOOTOSステージの前にPOSTコードを解析します。	dump\bios_info\biosprocess.log
イベントディレクトリ内のCSV形式ファイルレコード:CSVファイルは、イベントログを記録するためのプレーンテキスト形式です。イベントディレクトリ内の対応するファイルを表示できます。主に、SDSからSELログ、監査ログ、更新ログおよびSDLログに収集されたすべてのログ情報がCSVファイルに格納されます。ユーザーは、ログを確認するときにCSVファイルを直接表示できます。 osbootディレクトリ内のホスト再起動ログ:OSの再起動中に、ホスト構成の論理ステータス、シリアルポートログ、ハードウェア構成、およびPOSTコード情報を記録します。 shdディレクトリ内のハードウェアインテリジェント診断ログ:MCAなどのコンポーネントのインテリジェント診断ログの詳細情報と電源障害診断ログ情報を記録します。	daily\sds_ByDate\00001(Serial number)_20240106(YYYYMMDD)\event daily\sds_ByDate\00001(Serial number)_20240106(YYYYMMDD)\osboot daily\sds_ByDate\00001(Serial number)_20240106(YYYYMMDD)\shd
CPLDレジスタ情報	sdmmc0p4\log\cpldump.log
ユーザー関連の操作については、操作ログを参照してください。	sdmmc0p4\log\operate.log
入力および出力電圧および電流を含むセンサー情報	static\sensor_info.ini
FRU構成情報	static\FruInfo.ini
システムボードの設定情報	static\board_cfg.ini
ネットワーク構成情報	static\net_cfg.ini
NVMe情報	static\NVMe_info.txt
パワーサプライ構成情報	static\psu_cfg.ini
ネットワーク、SMTP、およびSNMPを含むBMC設定情報	static\bmc.json
BIOS設定情報	static\bios.json
コアダンプ情報レコード	sdmmc0p4\crash
BMCの内部動作状態	dump\bmcsys_info
BIOS/OS関連情報	dump\bios_info dump\os_info
ハードウェア関連の情報	dump\hw_info

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、G6サーバーでのみ使用できます。

図53に示すように、インテリジェントセキュリティベゼルの装飾LEDは、サーバーのヘルスステータス

または電力負荷を示すために、白、オレンジ、および赤の3色で動作できます。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して、オンサイト検査または障害位置の特定を容易にすることができます。詳細については、表8を参照してください。

図53 インテリジェントセキュリティベゼル

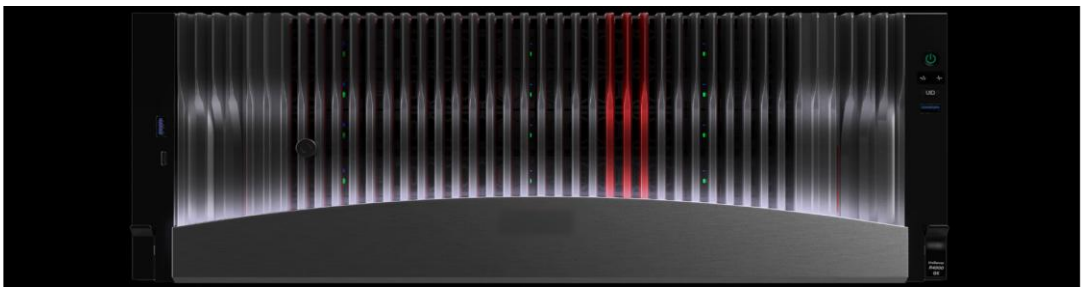


表8 インテリジェントセキュリティベゼルのステータス

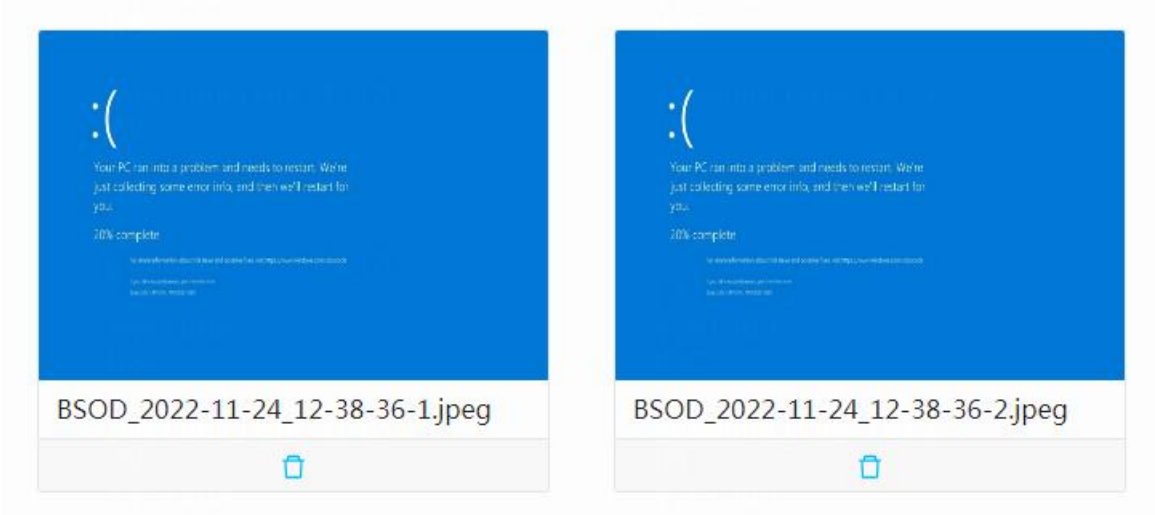
説明		装飾LEDステータス
スタンバイ	スタンバイ	白の点灯(LEDビーズの中央の3つのグループ)。
スタートアップ	ポストフェーズ	白いLEDが中央から両側に向かって徐々に点灯し、投稿の進行状況を反映しています。
	ポストが完了しました	白いLEDが中央から両側に3回ずつ交互に点灯します。
操作	正常(負荷レベルを表示)	白色LEDは、0.2 Hzの呼吸モードで点滅します。点灯したLEDビーズの数は負荷レベルを示します。全体的な電力負荷(PSU)が増加するにつれて、より多くのLEDビーズが中央から両側に向かって点灯します。負荷レベルは次のとおりです。 • 空負荷(10%未満) • 軽負荷(10%～50%) • 中負荷(50%から80%) • 高負荷(80%以上)
	事前アラート	1 Hzで白色にゆっくり点滅。
	メジャー障害	1 Hzでオレンジ点滅。
	重大な障害(電源障害を含む)	1 Hzで赤点滅。
リモート管理	リモート管理が進行中であるか、HDMがアウトバンドファームウェアアップグレードを実行しています。システムの電源を切らないでください。	1 Hzで白色点滅(すべてのLED)
	HDMが再起動しています	1 Hzで白色点滅(一部のLED)。

BSoD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死のブルースクリーン(BSoD)スクリーンショットを自動的に取得し、将来のトラブルシューティングのために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は、MCA障害時のスクリーンショットの取得をサポートしています。

HDMは、指定された形式で最大10個のBSoDスクリーンショットを保存できます。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。

図54 BSoDスクリーンショット



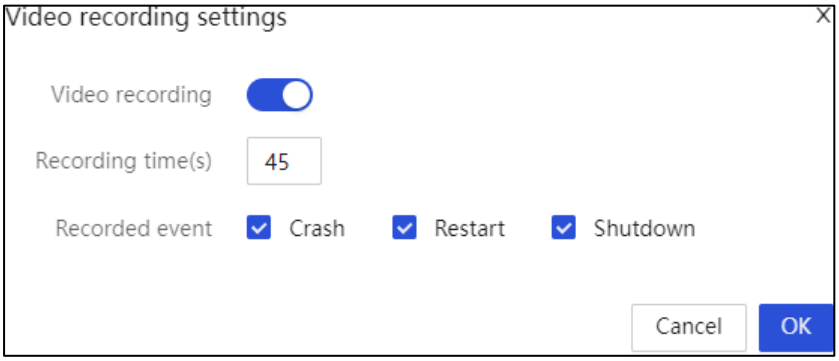
ビデオ再生

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のビデオ再生ページでは、図55に示すように、記録されたビデオを再生、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。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55 ビデオ再生設定の指定



アラートポリシー

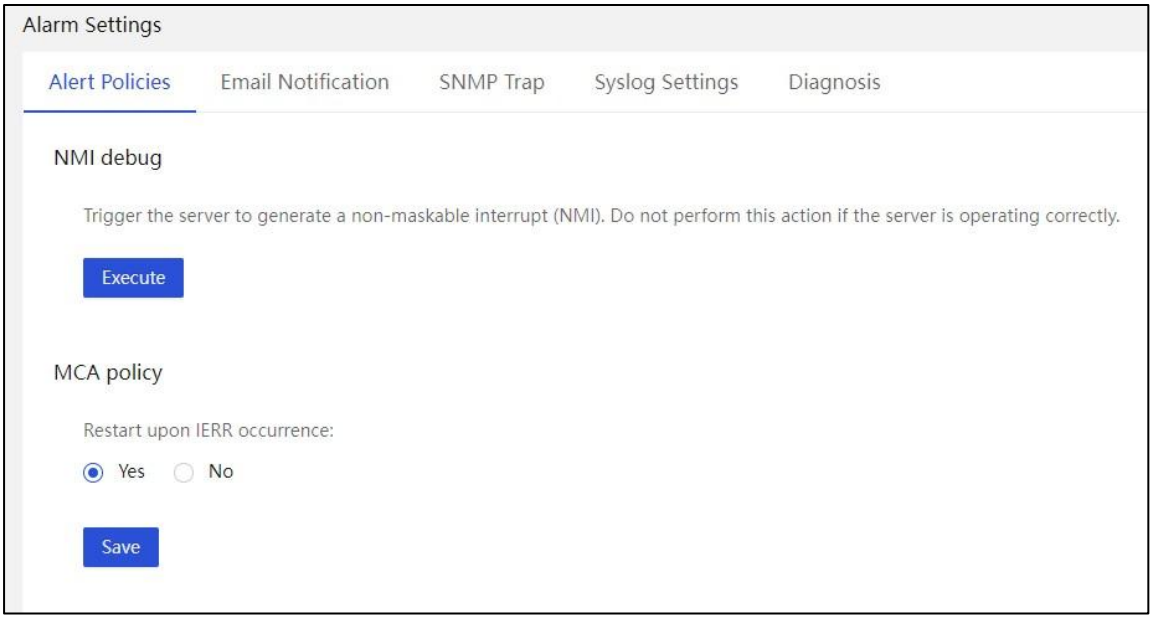
NMIデバッグ

ノンマスカブル割り込み(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、その情報をコンソールに送信してシステム例外を特定できます。

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。

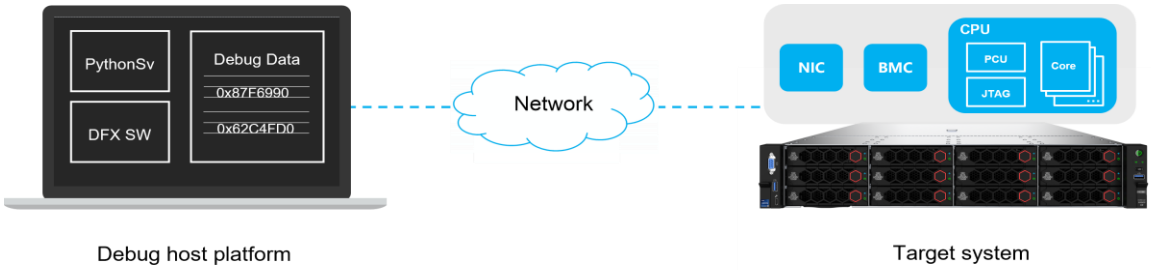
図56 MCAポリシーの設定



ASD

ユーザーは、インテル固有のデバッガーを購入したり、デバッガー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登録情報を収集して、ハードウェアの問題を特定するのに役立ちます。ASDはリモートXDPとも呼ばれます。

図57 ASD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。

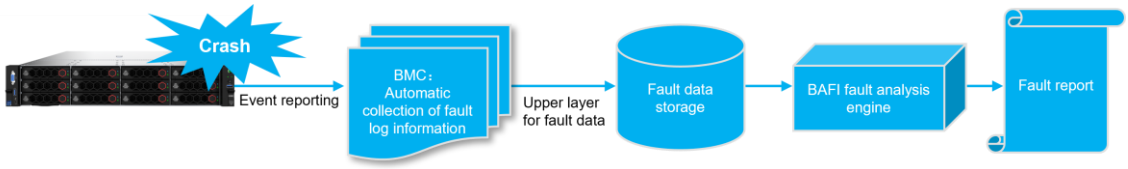
1. HDMからASDサービスを有効にします。
2. ローカルPCにPVTをインストールします。
3. Pythonをインストールし、Intelが提供するCscriptをダウンロードします。
4. CMDを開き、cscriptsディレクトリでコマンドを実行します。

ACD方式

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。図58に示すように、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、メモリーおよびPCIe障害に関する情報を含む)をアウトオブバンド方式で収集します。次に、ACDはCScripts分析用に情報をJSON形式で保存します。これにより、Intelプラットフォームの MCAエラーを特定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ます。

図58 Intel ACDメカニズム

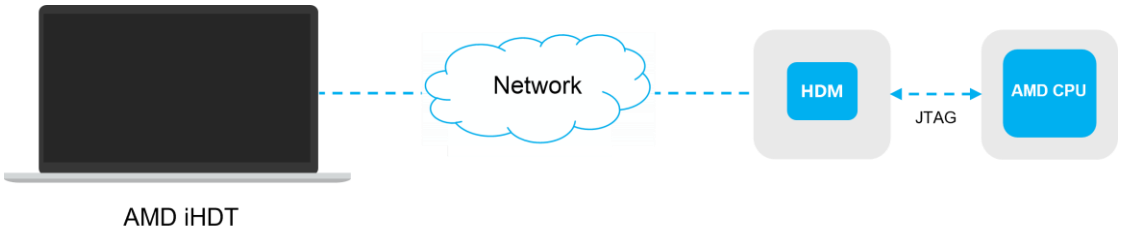


iHDT

図59に示すように、iHDTサービスは、AMDが提供するハードウェアデバッグツール(HDT)を使用してアウトバンド方式でAMDプロセッサーのJTAGデバッグをリモートで実行し、プロセッサー、メモリー、およびPCIe情報を収集します。

iHDTサービスは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59 iHDT機構



アラームの設定

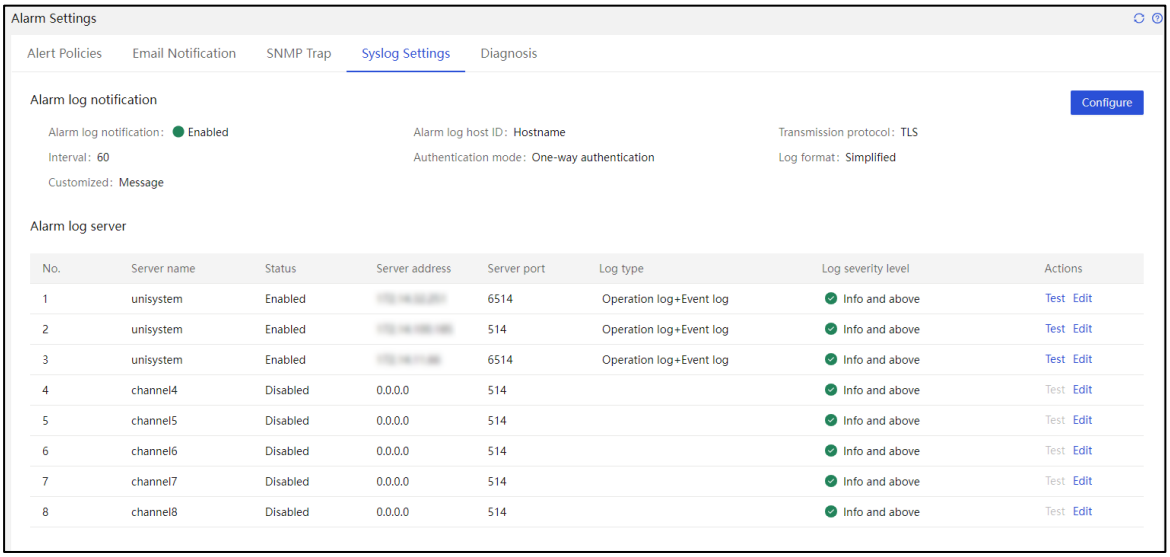
リモートsyslog

HDMを使用すると、リモートsyslogサーバーは、操作ログ、イベントログ、ホストコンソールログ、およびセンサー情報を取得できます。図60に示すように、リモートsyslogサーバーのポート番号、伝送プロトコル、ログタイプ、およびホスト識別子パラメーターを設定できます。

伝送プロトコルには、UDP、TCPおよびTLS暗号化伝送を使用できます。TLS暗号化伝送では、一方向認証と双方向認証の両方がサポートされます。

サポートされるログタイプには、操作ログ、イベントログ、セキュリティログ、コンソールログ、およびセンサーログがあります。

図60 リモートsyslogの設定

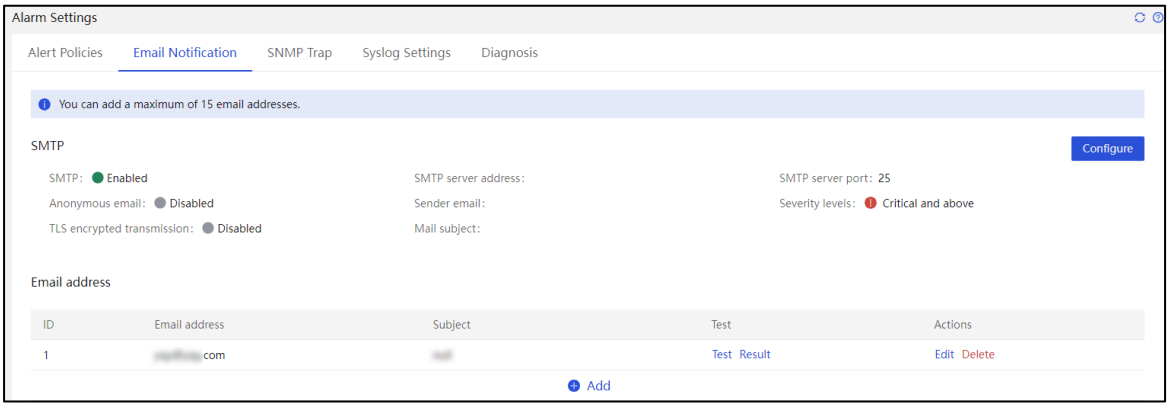


アラートメール

HDMは、生成されたイベントログをサーバーから指定したユーザーに報告するためのアラート電子メールの送信をサポートしており、ユーザーがサーバーの操作ステータスを監視するのに役立ちます。SMTP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使用できます。HDMは、匿名ユーザーおよび認証ユーザーへのアラート電子メールの送信をサポートしており、最大15人の受信者ユーザーを構成できます。

HDMでは、重大度レベルに基づいてアラートイベントをレポートできます。重大度レベルは、**Info**以上、**Minor**以上、**Major**以上および**Critical**以上です。

図61 アラートメールの設定



SNMPトラップ

HDMを使用すると、生成されたイベントログをサーバーからSNMPトラップを介して指定されたユーザーに送信できるため、サーバーの動作ステータスを監視するのに役立つ。

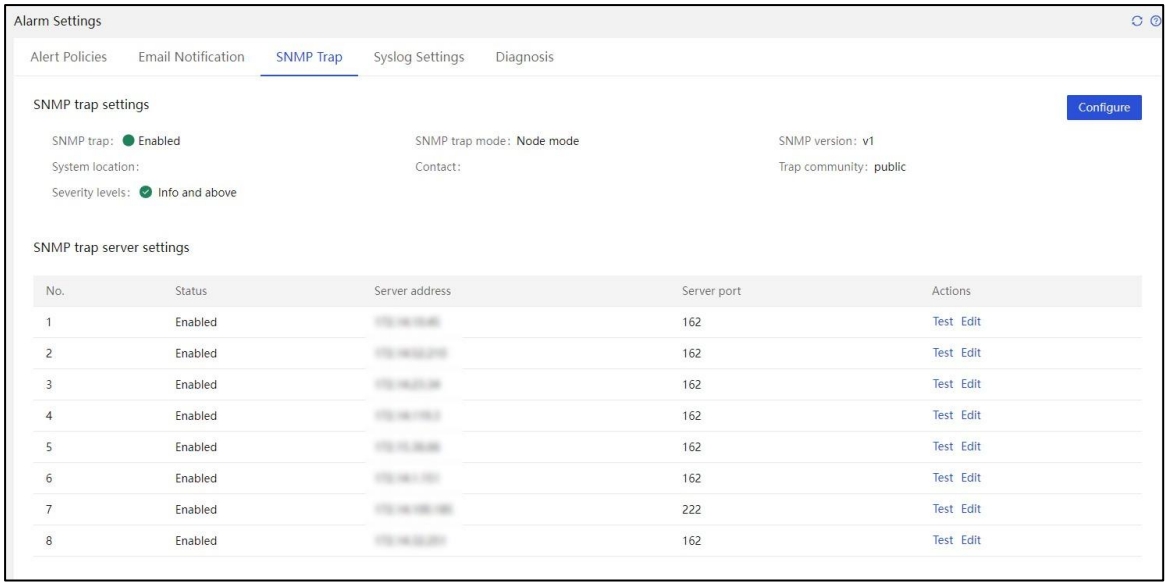
HDMは、重大度レベルに基づいてSNMPトラップをサーバーに送信できます。重大度レベルは、**Info**以上、**Minor**以上、**Major**以上および**Critical**以上です。SNMPトラップは、ノードモード、イベントモードまたはイベントコードOIDモードで構成できます。

- **Node mode** -モジュールのアラーム(センサータイプ別に分類)は、同じOIDに対応します。ユーザーは、OIDを使用して問題のあるモジュールを判別できます。
- **Event mode** - ノードモードに基づいて、各モジュールの各イベントアラームには独自のOIDが

あります。ユーザーは、アラームOIDに基づいてモジュール障害のタイプを判別できます。

- **Event code OID mode**: イベントコードはイベントのIDとして使用されます。

図62 SNMPトラップの設定



電源ブラックボックス

電源障害が発生したときにHDMによって収集される電源ブラックボックスデータには、各電源の最後の5つの障害からのデータが含まれます。障害情報は電源の不揮発性メモリーに保存され、長期間アクセスできるため、データが失われることはありません。

ブラックボックスデータには、障害時間と障害原因が含まれています。このデータは、デバイス障害診断ログSDSに含まれています。デバイス障害診断ログSDSを収集することにより、パワーブラック情報を取得できます。

HDMシステム保全性

HDMウォッチドッグ

HDMは、ウォッチドッグ機能を使用して、自身のシステム内のすべてのプロセスの実行ステータスを監視します。各プロセスは、定期的に監視モジュールにハートビートパケットを送信します。ハートビートパケットが連続して検出されない場合、システムは障害リカバリメカニズムをトリガーします。

HDMの起動後、システムは最初の10分間、1分ごとにハートビートパケットを監視します。ハートビートパケットが2回連続して検出されない場合、HDMはセカンダリイメージに切り替えます。HDMの起動後10分間、システムは2分ごとにハートビートパケットを監視します。ハートビートパケットが検出されない場合、プロセスは異常と見なされ、リカバリのための自動HDM再起動がトリガーされます。

HDM再開理由記録

各起動後、HDMは独自の再起動理由をデバイス障害診断ログ(SDS)に記録します。考えられるHDM再起動理由には、HDMバージョンのアップグレード、AC電源の停止、HDM工場出荷時のデフォルトの復元、カーネルの異常な再起動、UIDの長押し、およびウォッチドッグのタイムアウト再起動が含まれます。

HDM eMMCカードの監視

HDMは、emceeカードの寿命ステータスを定期的に監視し、eMMCカード情報を収集し、その寿命を

分析します。予測された寿命が変化するたびに、予測された寿命の変化を記述するSDL監視ログが生成されます。また、HDMは、予約されたブロックの消費が80%または90%を超えることを検出すると、SDL監視ログを生成します。HDMが、カードの寿命が枯渇しようとしている(残りの10%)、または枯渇したと予測すると、SDL監視ログも生成されます。

HDMメモリーの監視

HDM SOCチップは、ECCおよびUECCテクノロジーをサポートしています。メモリーのECCエラーまたはUCEエラーの数がHDMの特定のしきい値に達すると、SDLログが生成され、HDMが再起動されます。

ローカルO&M

USB Wi-Fi対応

G6サーバーのシャーシイヤーは、サードパーティのUSB Wi-Fiモジュールに接続してHDMのホットスポットを提供できるUSB Type-Cコネクターと統合されている。ユーザーは、携帯電話やポータブルデバイスを使用してHDMにログインし、HDM Mobileアプリやその他のツールを使用して操作や検査を実行できる。

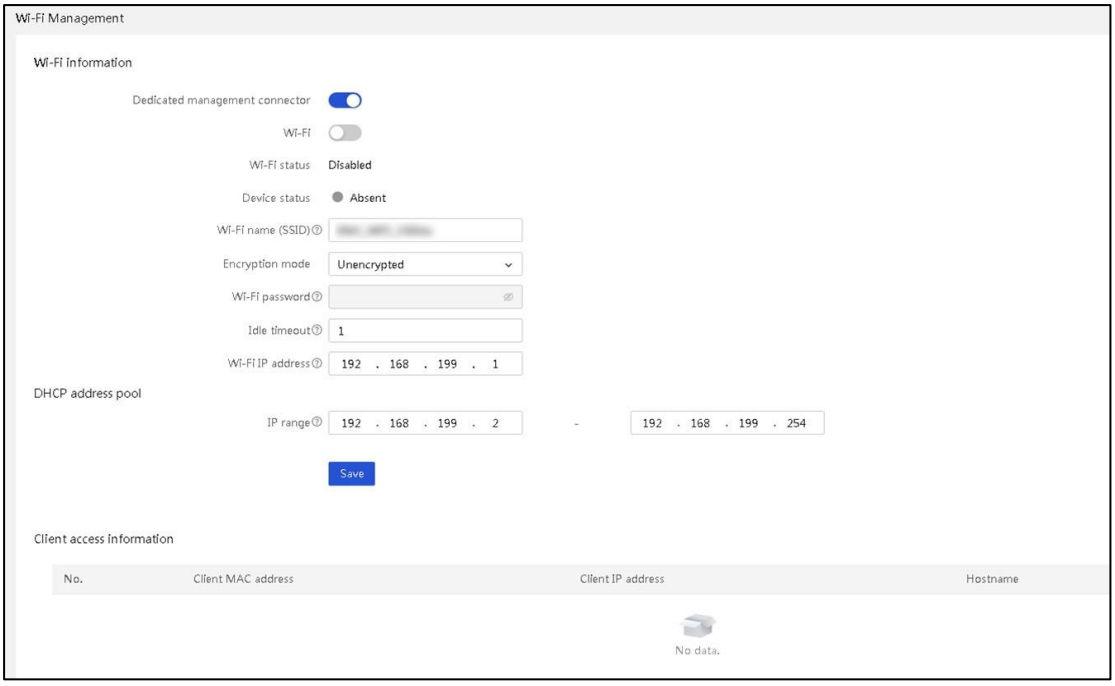
現在、Xiaomi Portable Wi-Fiと360 Portable Wi-Fiのみがサポートされています。Type-C to USBコンバータを使用して、ポータブルWi-Fiデバイスを接続します。

セキュリティを強化するために、2つのクライアントのみが同時に接続できます。Wi-Fiパスワードは、プラグアンドプレイを有効にするためにデフォルトでは暗号化されません。

図63に示すように、HDMからWi-Fi状態、WLAN名、暗号化方法、パスワード、スケジュールされたシャットダウン時間、WLAN管理インターフェイスIPアドレス、およびDHCPサーバードレスプールを設定できます。

HDMは、WLANインターフェイスでWeb、Redfish、IPMI、SSH、およびTelnetをサポートします。

図63 WLAN管理設定



サービスUSBデバイス

G6サーバーのシャーシイヤーは、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。図64に示すように、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可能です。HDM は Type-C コネクターに接続された USB デバイスを識別し、ログのダウンロードに USB デバイスを使用するかどうかを決定します。

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作成されたUSBデバイスです。Unitoolを使用してサービスUSBデバイスを作成できます。

図64 G6サーバーのUSB Type-Cコネクター

コンポーネント管理

FRUおよび資産情報の管理

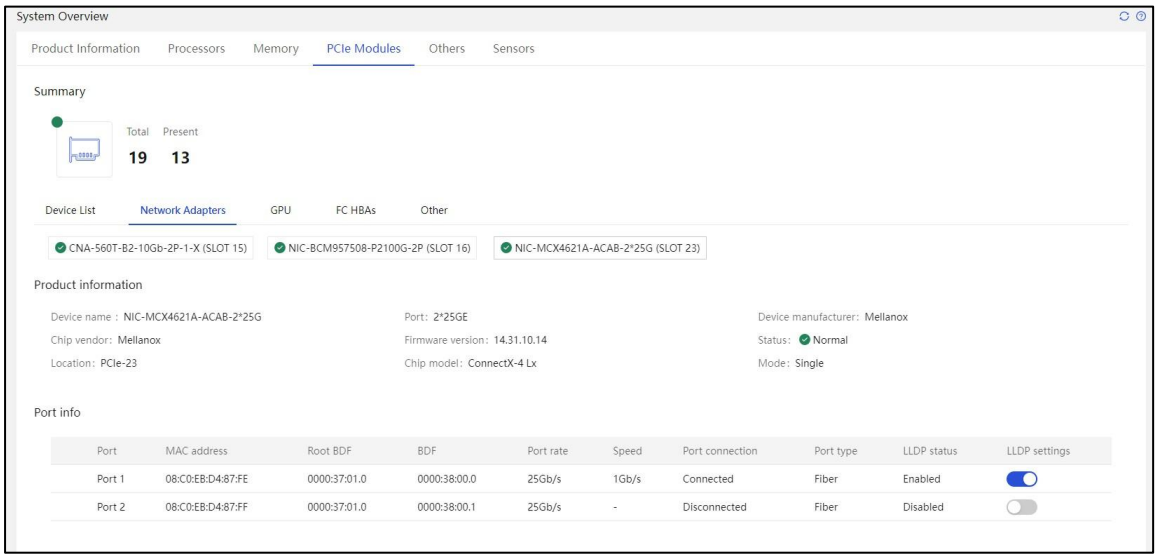
FRU情報とは、製造元、製品名、コンポーネントID、シリアル番号など、サーバーまたはコンポーネントの製造時にコンポーネントのEEPROMに書き込まれる静的情報を指します。HDMは、コンポーネントの現在のステータスに基づいてデバイスのFRU情報を取得します。これにより、IPMI、Redfish、SNMPエージェントなどの監視インターフェイスの戻り時間が短縮され、O&Mシステムの監視効率が向上します。

資産情報管理では、コンポーネントのシリアル番号が収集されます。HDMは、サーバー上のコンポーネントシリアル番号の収集をサポートし、顧客の資産管理システムまたはO&Mシステムと統合するためのIPMI、RedfishおよびSNMPエージェントインターフェイスを提供します。HDMにより、ユーザーは資産インベントリを迅速かつ効率的に実行でき、資産データの価値が向上します。

ネットワークアダプターの管理

HDMは、NCSI over MCTP(over PCIeまたはI2C)およびOCPネットワークアダプターをサポートするネットワークアダプターの帯域外管理を提供します。HDMは、MACアドレス、PCIeアドレス、リソース所有権、最大およびネゴシエートされたレート、リンクステータス、インターフェイスタイプ、およびLLDPステータスを含むネットワークアダプターのポート情報へのアクセスを提供します。HDMはまた、さまざまな運用シナリオの要件を満たすために、一部のネットワークアダプターの帯域外ファームウェアアップグレードをサポートします。

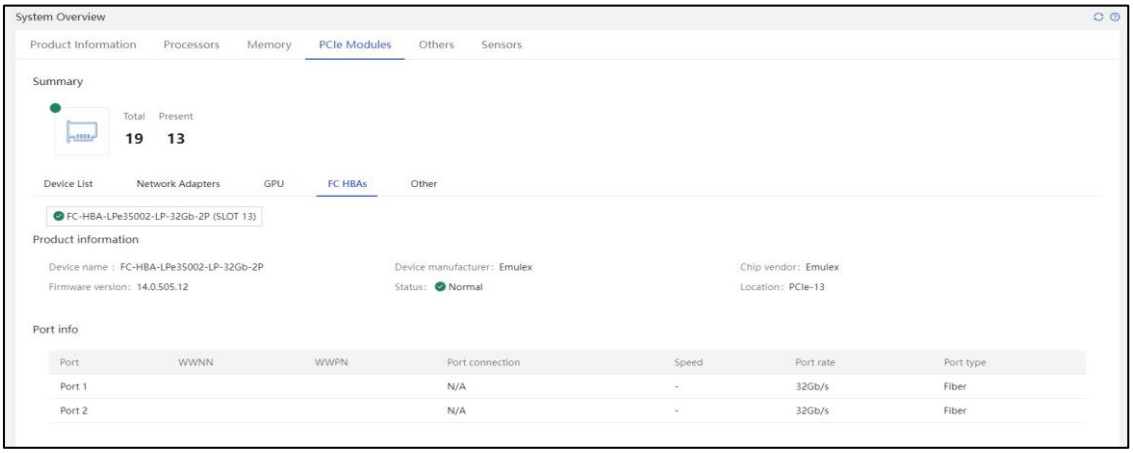
図65 ネットワークアダプター情報



FC HBAの管理

HDMは、PCIe上のMCTPを介して、一部のFC HBAの帯域外管理を可能にします。FC HBAのWWNN、WWPN、温度、ヘルスステータス、リンクステータス、および速度のリアルタイム検索をサポートします。また、特定のFC HBAモデルの帯域外ファームウェアアップグレードもサポートします。

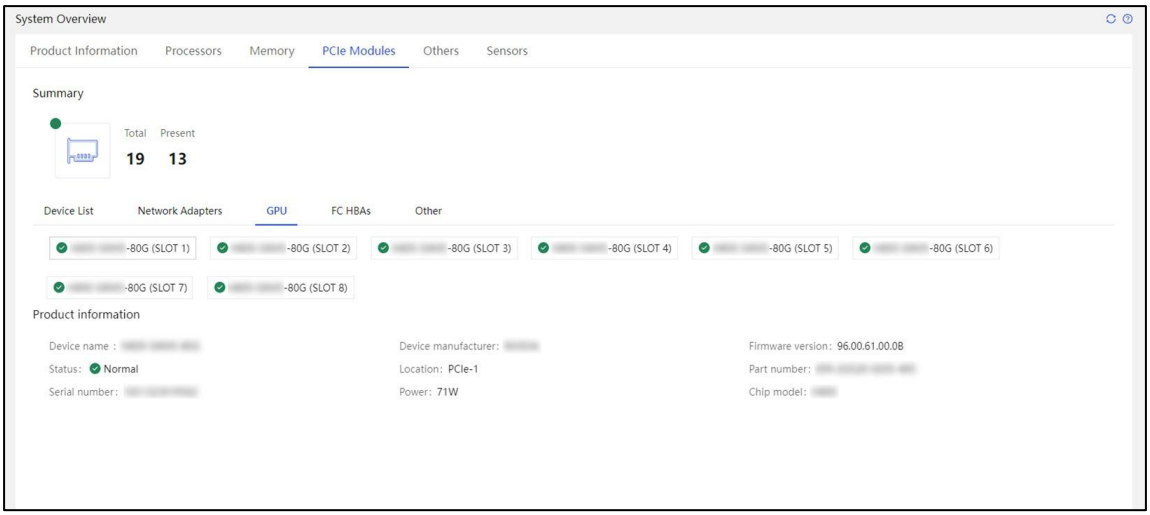
図66 FC HBAの情報



GPU管理

HDMのGPUの帯域外管理では、製品名、メーカー名、ベンダーID、ファームウェアバージョン、内部GPUの数、各内部GPUの温度値、消費電力などの情報を取得できる。
NVIDIA GPUにはドライバーが必要です。

図67 GPU情報



インテル(R)オンデマンド

インテルは、プロセッサーを交換せずにカスタムライセンスのインポートを可能にするITソリューションであるオンデマンドを提供しています。これは、動的なエンタープライズリソース割り当ての要件を満たしながら、材料費を節約することを目的としています。

HDMは、現在のIntel CPU On Demand機能セットと現在アクティブ化されている機能セットの取得をサポートします。また、Intelから取得したライセンスをアップロードし、アウトバンド方式でCPUステータスレポートをダウンロードすることにより、Intel CPUがサポートする機能をアクティブ化することもサポートします。

図68 インテル(R)オンデマンドマネジメントインターフェイス

ストレージ管理

HDMのストレージ管理モジュールは、ストレージコントローラーとドライブの帯域外管理を可能にします。その主な機能は次のとおりです。

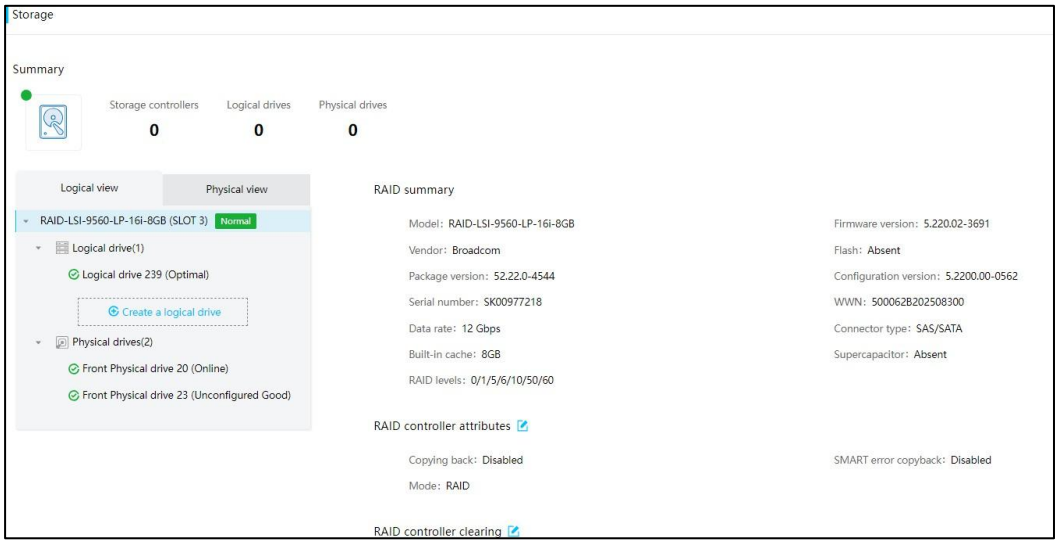
- ストレージコントローラーの管理
- 論理ドライブ管理。
- 物理ドライブの管理。
- ストレージの保守性

ストレージコントローラーの管理

HDMは、ストレージコントローラーの数、デバイス名、製造元、ファームウェアバージョン、インターフェイスタイプ、インターフェイス速度など、ストレージコントローラーに関する情報の取得をサポートします。

図69に示すように、製造元のシリアル番号、キャッシュ容量、モード、サポートされるRAIDレベル、スーパーキャパシターのステータス、およびフラッシュカードのステータス。

図69 ストレージコントローラーの管理



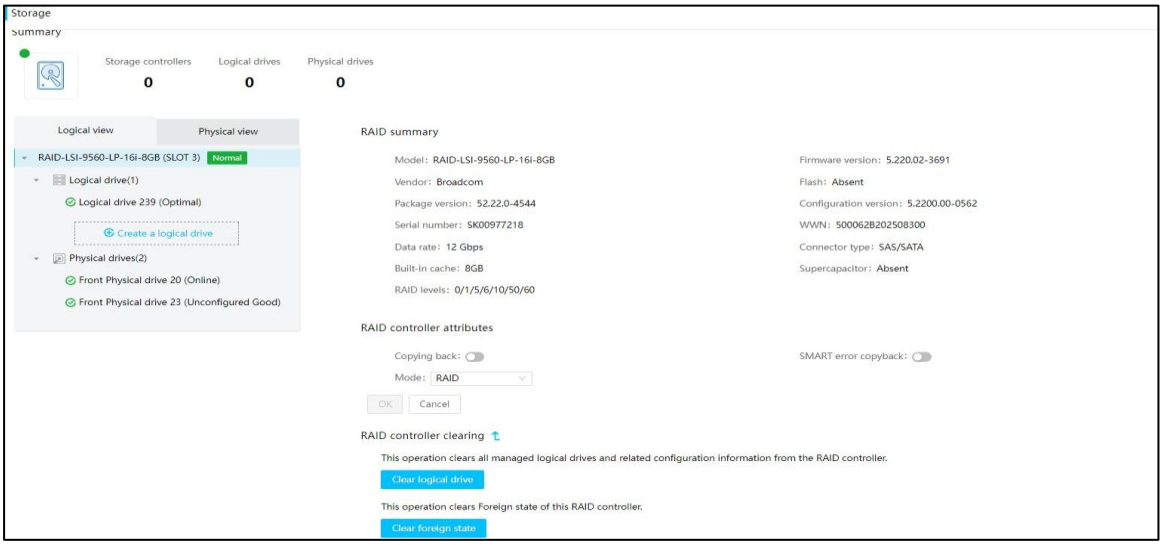
HDMは、MCTP Over PCIe帯域外管理モードにあるLSIおよびPMCストレージコントローラーの帯域外ファームウェアアップグレードをサポートします。

HDMは、次のようなストレージコントローラーのプロパティの設定をサポートしています。

- コピーバック構成。
- SMARTエラーのコピーバック設定。
- モードの切り替え
- JBODステータススイッチ。

HDMは、コントローラーによって管理されているすべての論理および物理ドライブの外部ステータスのワンクリッククリーンアップを含む、ストレージコントローラーのクリーンアップ操作を提供します。図70は、RAIDコントローラー情報を示しています。

図70 RAIDコントローラーの情報



論理ドライブの管理

HDMは、図71に示すように、論理ドライブ名、ステータス、RAIDレベル、容量、ブートドライブステータス、ストライプサイズ、読み取りポリシー、書き込みポリシー、キャッシュポリシー、デフォルト読み取りポリシー、デフォルト書き込みポリシー、物理ドライブキャッシュポリシー、アクセスポリシー、メンバードライブのリスト、メンバードライブ容量、およびメンバードライブ属性を含む、ストレージコントローラー上の論理ドライブに関する情報の取得をサポートします。

図71 論理ドライブ情報

HDMは、論理ドライブのアウトオブバンド作成、デフォルトの読み取りポリシー、デフォルトの書き込みポリシー、物理ドライブのキャッシュポリシー、アクセスポリシーの変更、およびRAID構成のエクスポートを含む、論理ドライブ属性の構成をサポートします。属性の構成には、アウトオブバンドRAID構成に対するストレージコントローラーのサポートが必要です。

図72 論理ドライブの作成

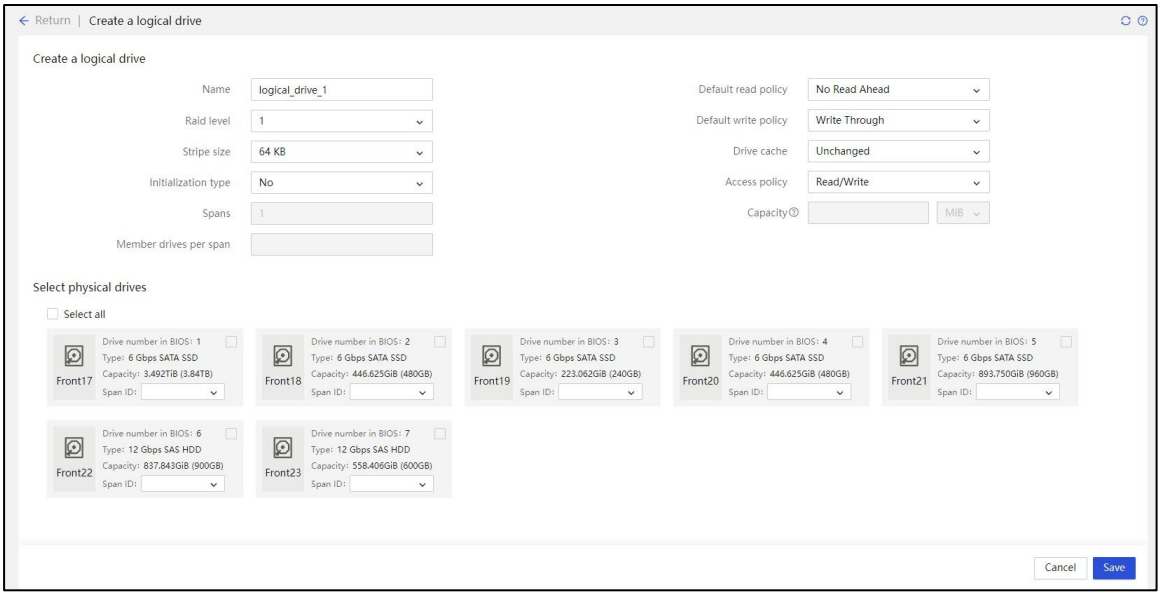
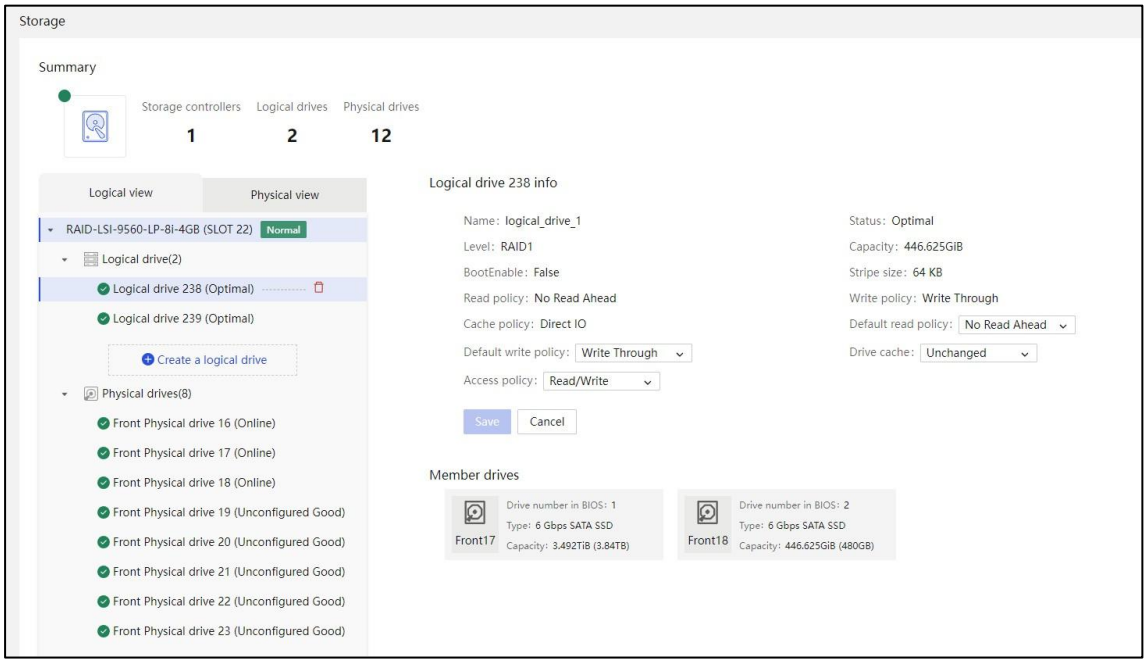


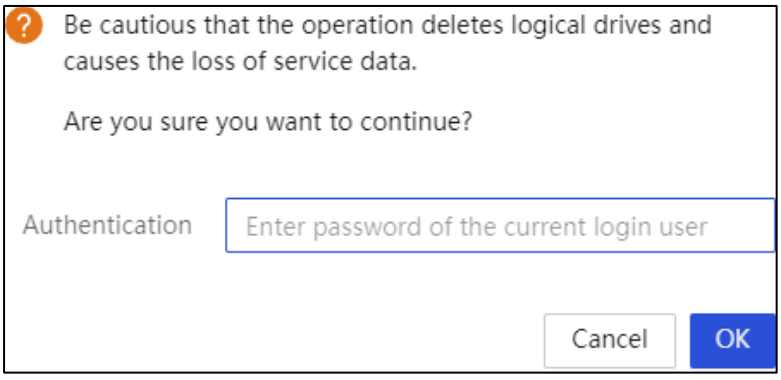
図73 論理ドライブの属性



HDM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。

図74に示すように、HDMは論理ドライブ削除のID検証をサポートしており、データの損失または漏洩を引き起こす可能性のある偶発的または不正な削除を防止します。許可されたユーザーのみがデータを削除できるため、データのセキュリティが保護されます。

図74 論理ドライブ削除のID確認



ストレージコントローラーの物理ドライブ管理

HDMは、スロット番号、メーカー名、モデル、ファームウェアバージョン、シリアル番号、ステータス、最大レート、プロトコル、メディアタイプ、容量、再構築の進行状況、HDD SMART情報(ストレージコントローラーのサポートが必要)、およびSSDの残りの寿命の割合(ストレージコントローラーのサポートが必要)など、PMCおよびLSIストレージコントローラーの物理ドライブ情報の取得をサポートします。

HDMは、次のようなストレージコントローラーの物理ドライブ情報の設定をサポートします。

- 物理ドライブのステータスの設定。
- ホットスペア構成(グローバルホットスペア、専用ホットスペア、ローミングホットスペアなど)
- ドライブの位置LEDの設定

図75 物理ドライブの論理ビュー

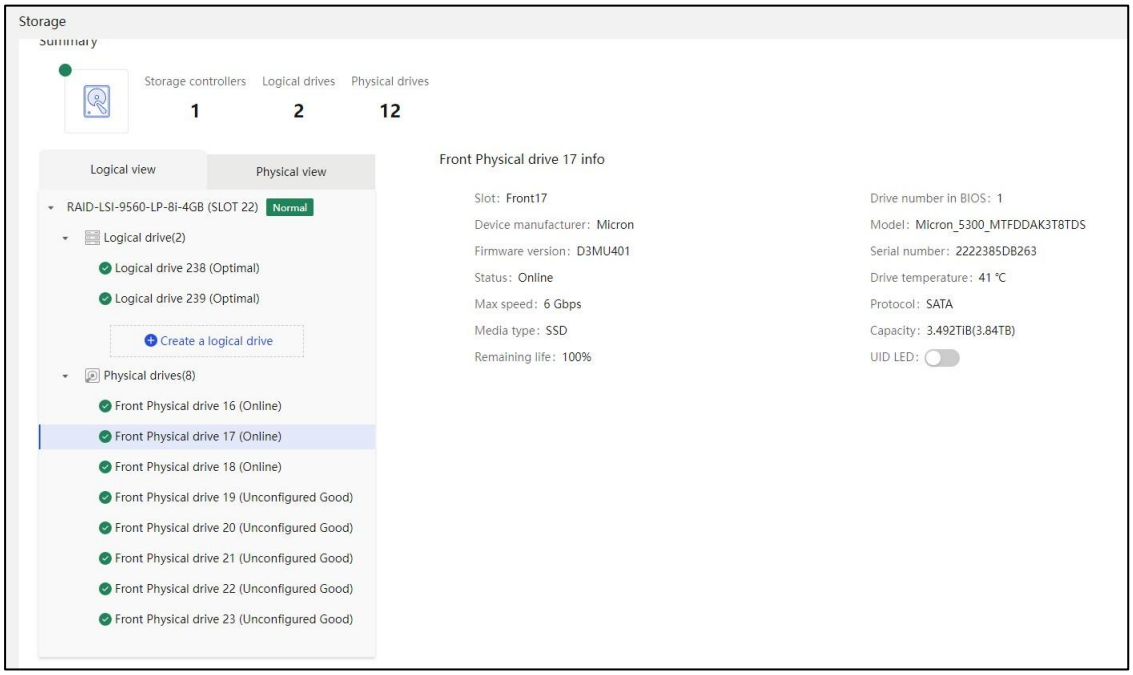
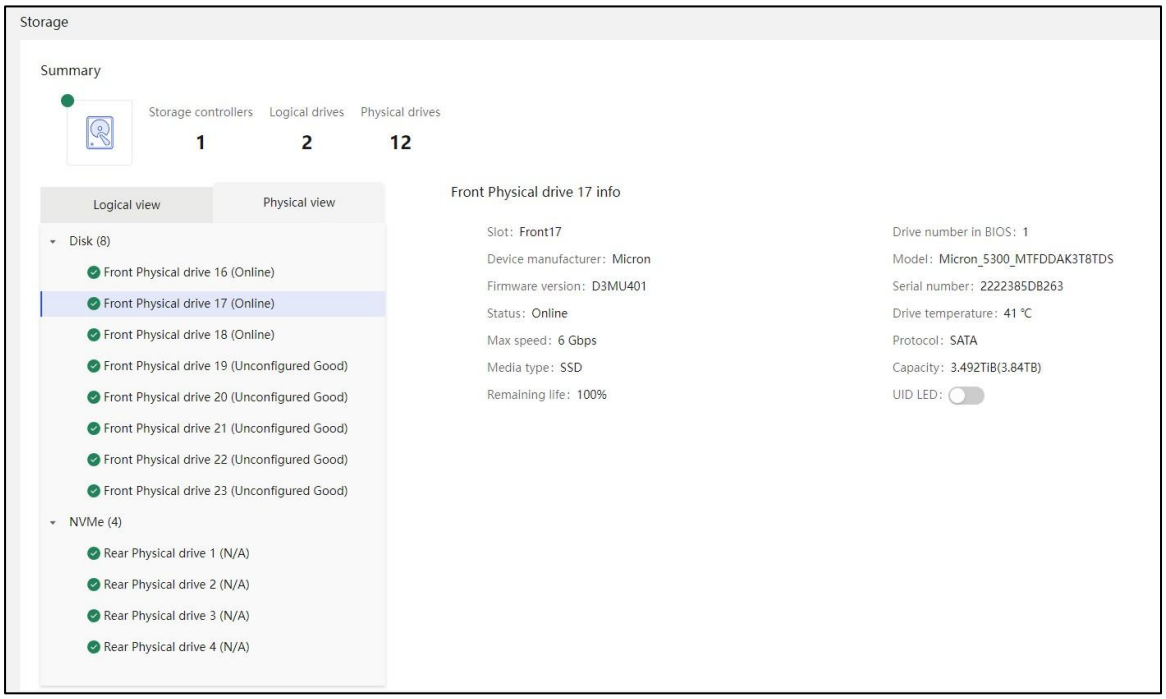


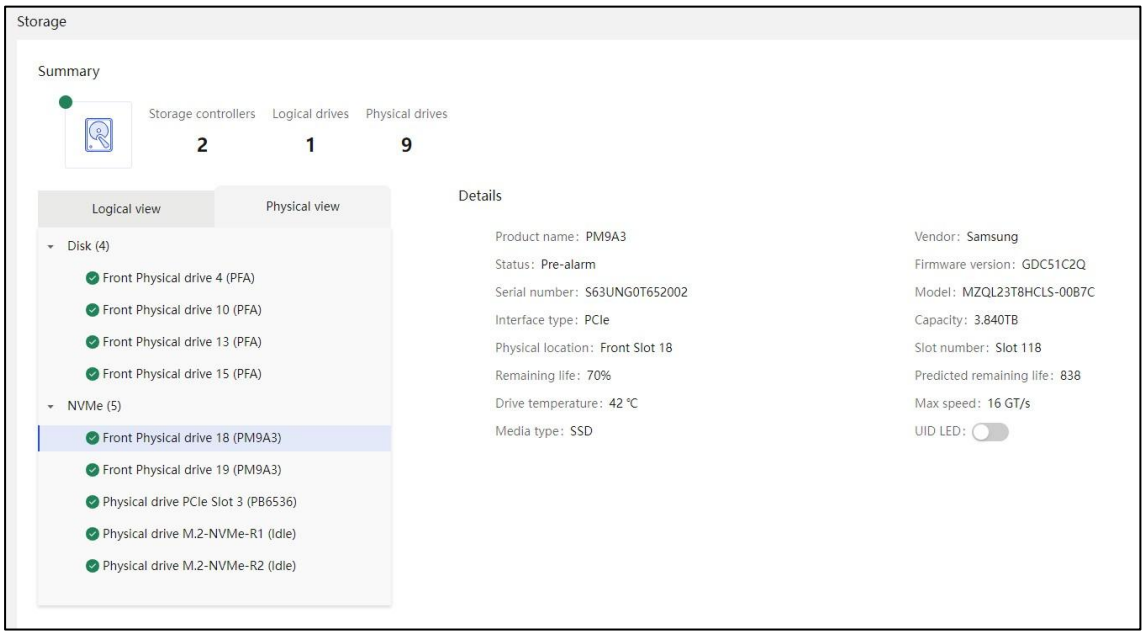
図76 物理ビューの物理ドライブ情報



NVMeドライブ

HDMは、図77に示すように、製品名、製造元、ステータス、ファームウェアバージョン、シリアル番号、モデル、インターフェイスタイプ、容量、物理スロット、PCIeスロット、残りの寿命、最大速度、メディアタイプ、および予測される残りの寿命(日数)を含むNVMeドライブ情報の取得をサポートします。

図77 NVMeドライブの情報



HDMは、NVMeドライブの残りの寿命の予測をサポートします。

HDMは、NVMeドライブの動作ステータスとパフォーマンスメトリックを監視して、残りの寿命の割合に関するデータを定期的に収集します。収集されたデータは、期間ごとに正規化され、分析され、モデル化されて、変化の割合の傾向が決定されます。この傾向を分析することにより、HDMはドライブの残りの寿命を日単位で推定できます。従来の割合のデータと比較して、予測された残りの寿命(日単位)は、ユーザーが意思決定を行うためのより直感的な理解を提供します。

HDMは、位置LEDを点灯させることによってNVMeドライブの位

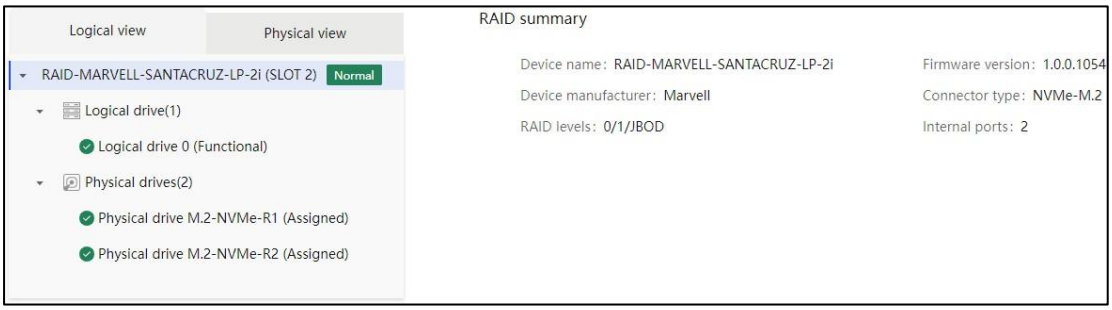
置を特定することをサポートします。HDMは、論理ドライブの作成

をサポートします。

Marvell M.2ストレージコントローラー管理

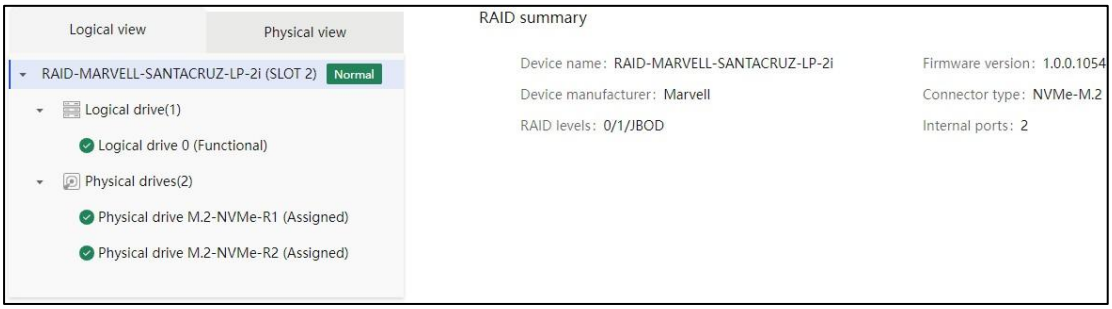
HDMは、図78に示すように、ストレージコントローラー名、ファームウェアバージョン、ベンダー、インターフェイスタイプ、サポートされるRAIDレベル、およびヘルスステータスを含むMarvellストレージコントローラー情報の取得をサポートします。

図78 Marvellストレージコントローラーの情報



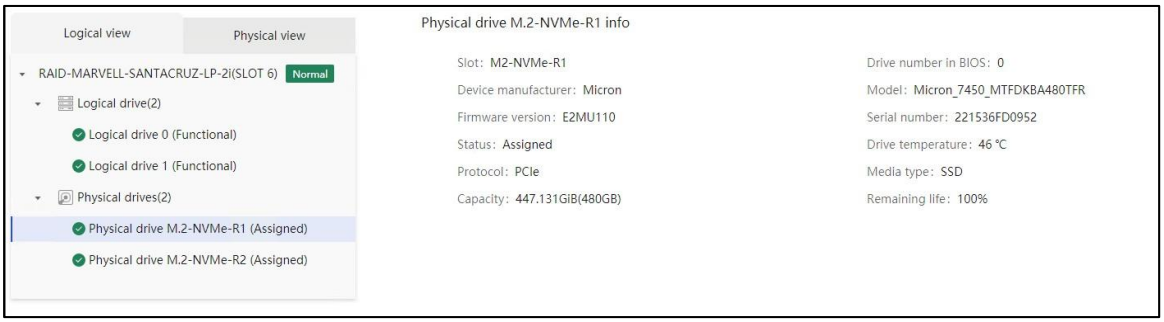
HDMは、論理ドライブ名、ステータス、レベル、容量、ストライプサイズ、およびメンバードライブ情報を含む、Marvellストレージコントローラーの論理ドライブ情報の取得をサポートします。図79に示すように、HDMは論理ドライブ障害の監視をサポートして、論理ドライブのダウングレードと障害ステータスを識別し、時間内にアラームを生成します。

図79 Marvell論理ドライブ情報



HDMは、図80に示すように、スロット番号、BIOS番号、ベンダー、モデル、ファームウェアバージョン、シリアル番号、ステータス、ドライブ温度、プロトコル、メディアタイプ、容量、残りの寿命、温度、およびドライブSMART情報を含む、Marvellストレージコントローラーの下でのM.2物理派生情報の取得をサポートしています。HDMはまた、物理ドライブの障害を監視して、物理ドライブの障害を特定し、時間内にアラームを生成することもサポートしています。さらに、HDMは、物理ドライブの残りの寿命に関するアラーム通知の送信をサポートしており、データの損失を防ぐために、寿命が尽きる前にドライブを交換するようユーザーに通知します。

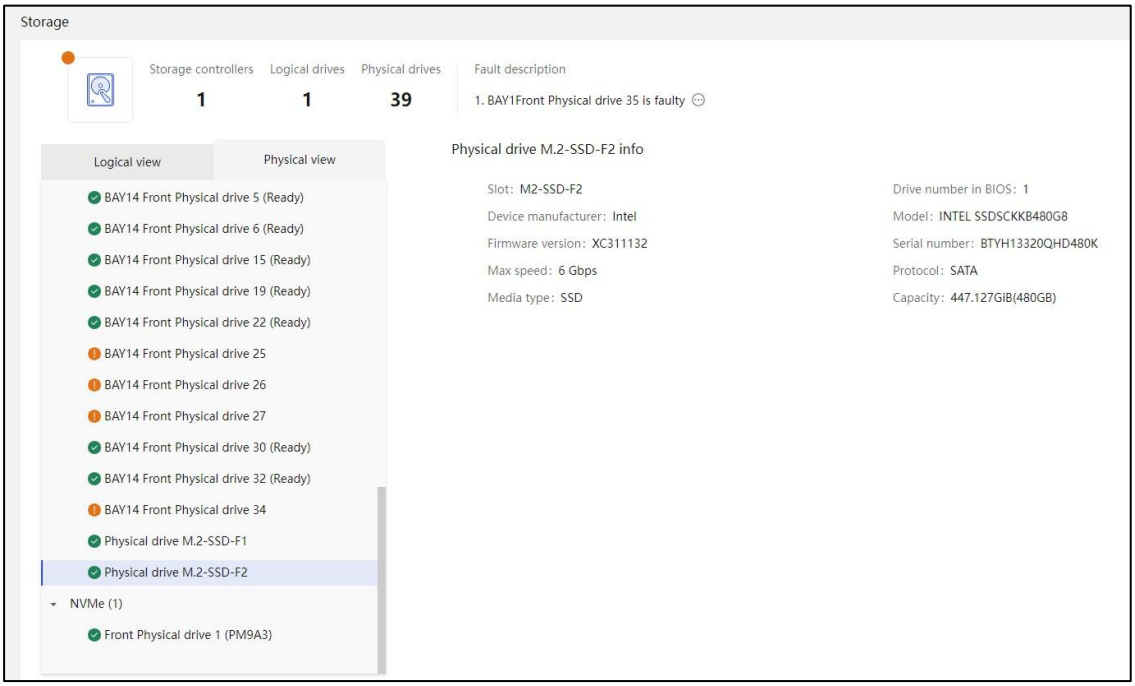
図80 Marvellの物理ドライブ情報



組み込み型ドライブ管理

HDMは、RAIDコントローラー管理に依存することなく、オンボード物理ドライブ(SATAおよびM.2)に関する情報の取得をサポートします。図81に示すように、情報には、ドライブの物理スロット、モデル、ファームウェアバージョン、容量、最大速度、およびメディアタイプが含まれます。

図81 内蔵ドライブの情報



ドライブの位置LED

ドライブ位置LED機能は、ストレージコントローラーで管理されるドライブ、マザーボードに直接接続されたオンボードドライブ、およびオンボードNVMeドライブに適用されます。この機能は、ドライブ管理の効率と精度を向上させ、ドライブLEDの使用を拡大するというさまざまなユーザーのニーズに対応します。

図82 ストレージコントローラーのドライブ位置LED

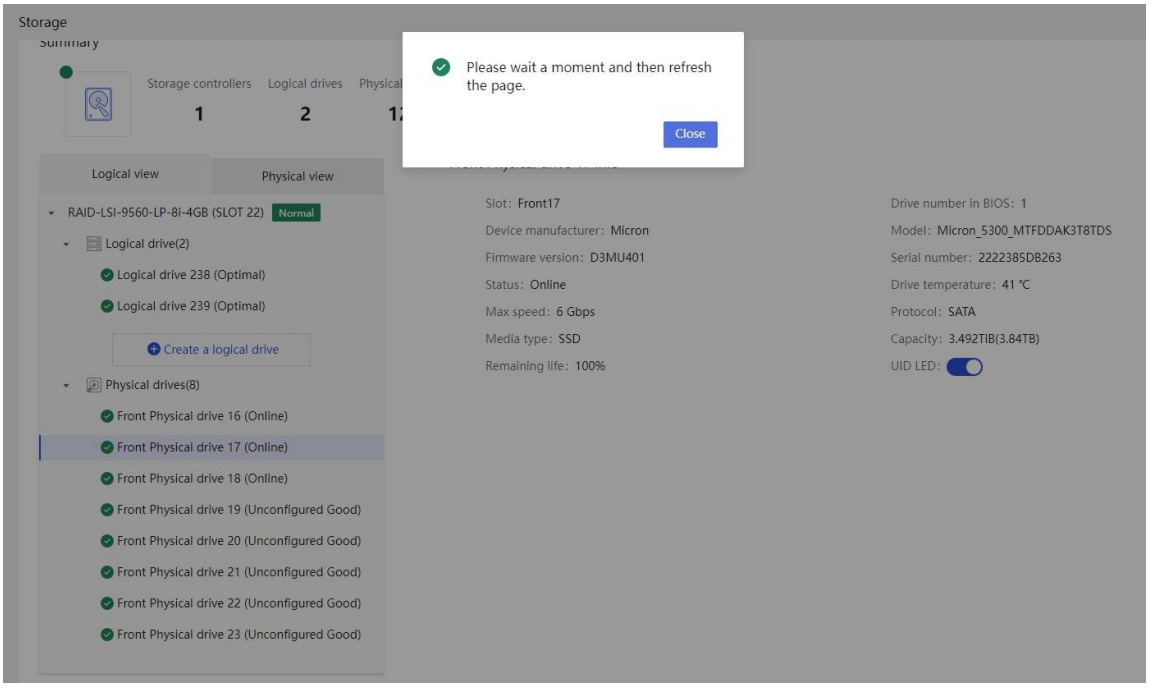


図83 オンボードドライブのドライブ位置LED

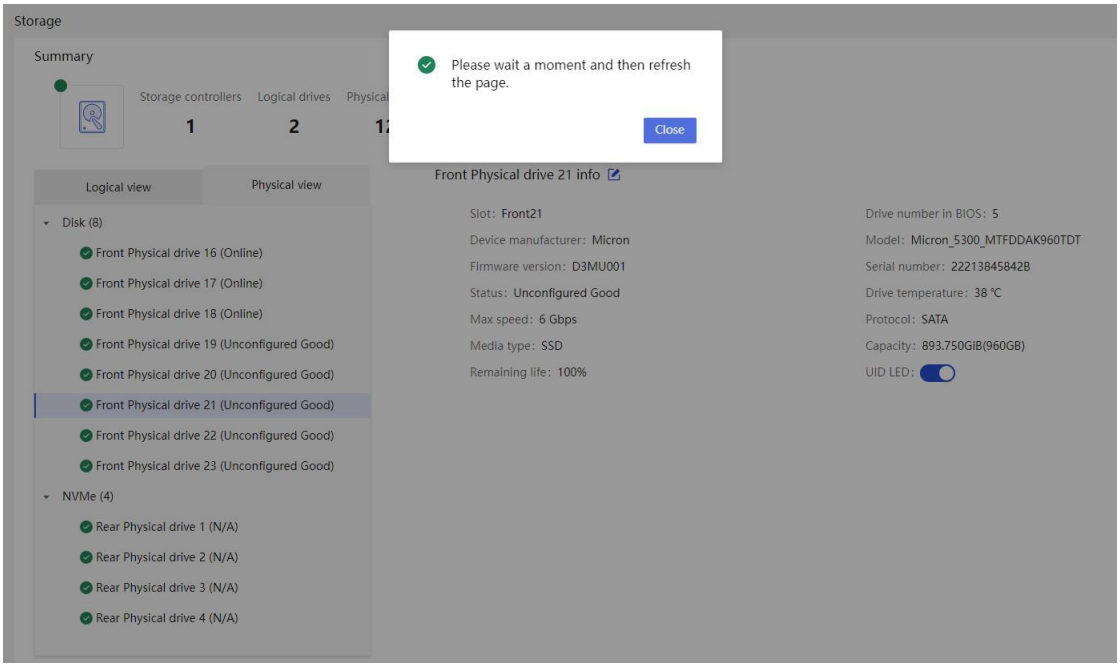
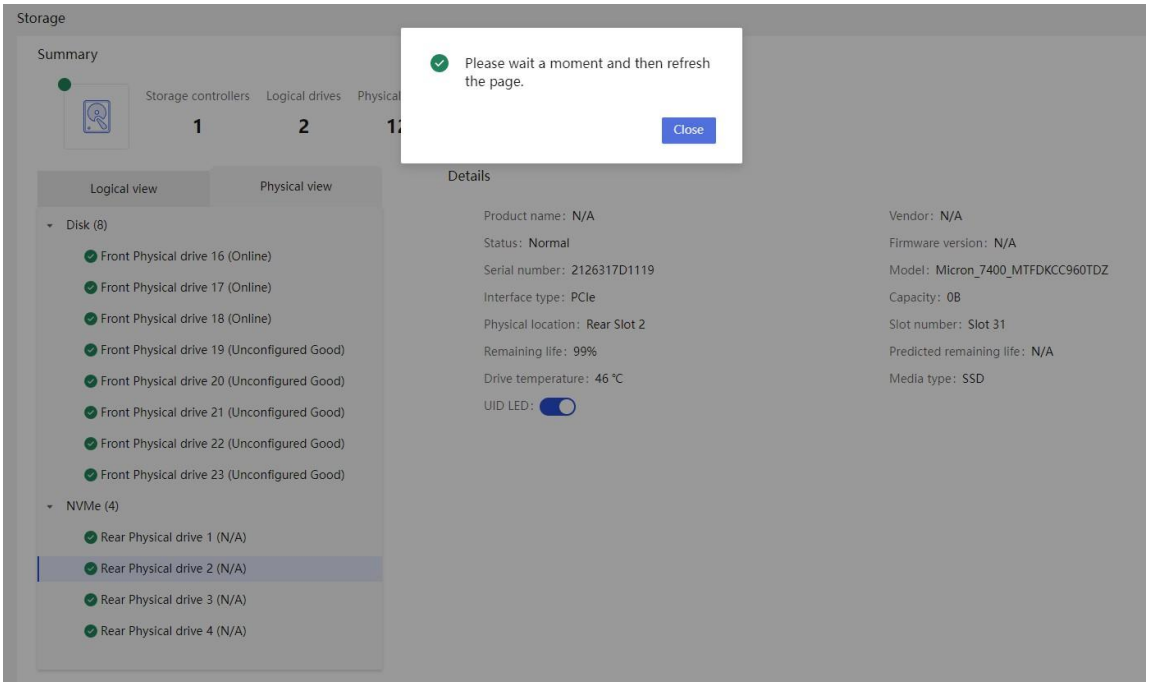


図84 オンボードNVMeドライブのドライブ位置LED



ストレージの保守性

障害アラーム

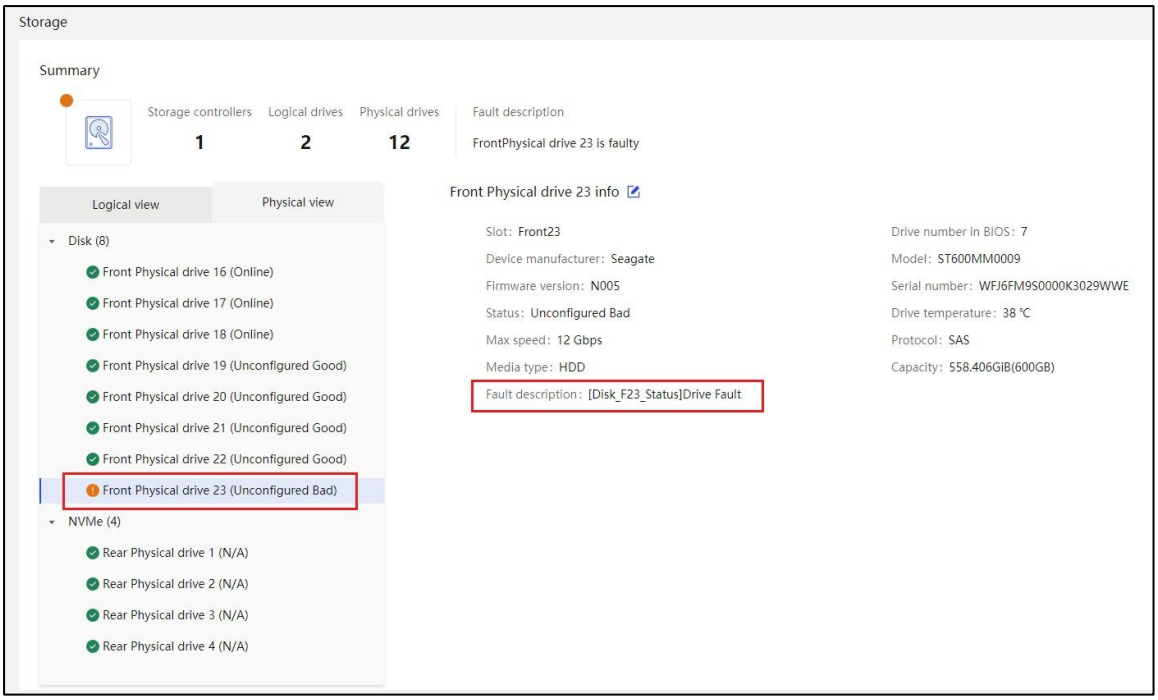
HDMは、ドライブの存在、障害、事前障害、およびアレイ障害を検出できます。

- **HDD** -HDDを監視し、物理的な障害、事前障害、構成エラー、ファームウェアステータスの異常、メディアエラー、事前障害状態、UNCエラー、不良セクタ、ドライブステータスの欠落、およびアレ

イの重大/障害状態に関するアラームを生成します。

- **SSD** -SSDを監視し、物理的な障害、事前障害、構成エラー、ファームウェアステータスの異常、メディアエラー、事前障害状態、UNCエラー、ドライブステータスの欠落、およびSSDの寿命と残りの予約ブロックに関するアラームを生成します。
- **NVMe drives**: NVMeドライブを監視し、NVMeドライブの摩耗寿命に関するアラームを生成します。
- **Storage controller**: ストレージコントローラーの障害アラームを生成します。
- **BBU**: BBU障害、事前障害(低電圧)、および非インプレースBBUのアラームを生成します。

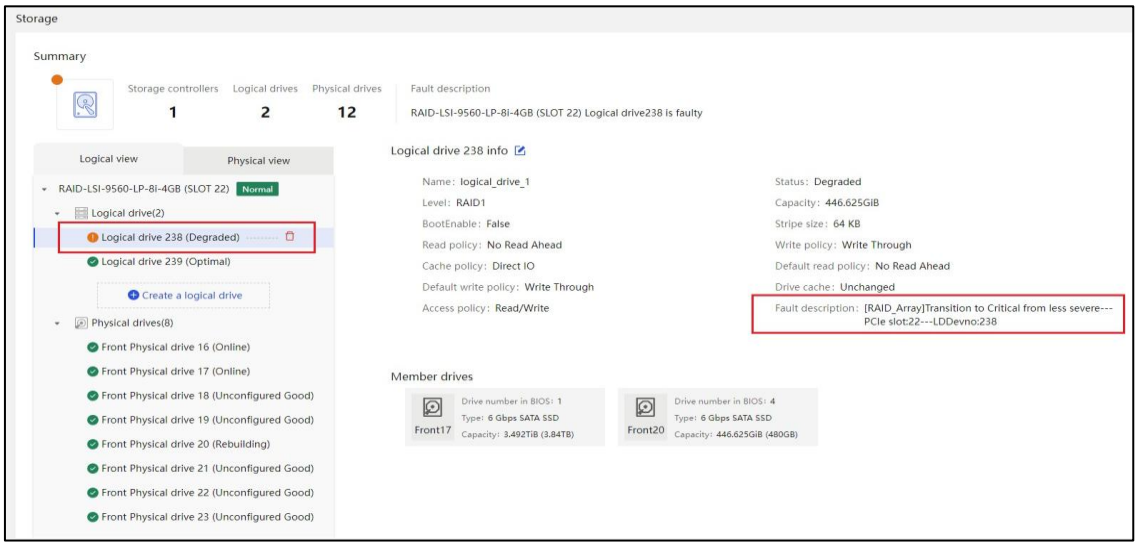
図85 物理ドライブのアラーム



論理ドライブのアラーム

HDMは、ストレージコントローラーを介して論理ドライブの現在のステータスを取得し、ドライブのステータスが正常かどうかを判断できます。ステータスが異常な場合は、対応するアラームがSELを介して報告され、問題を迅速に処理するようにユーザーに通知されます。

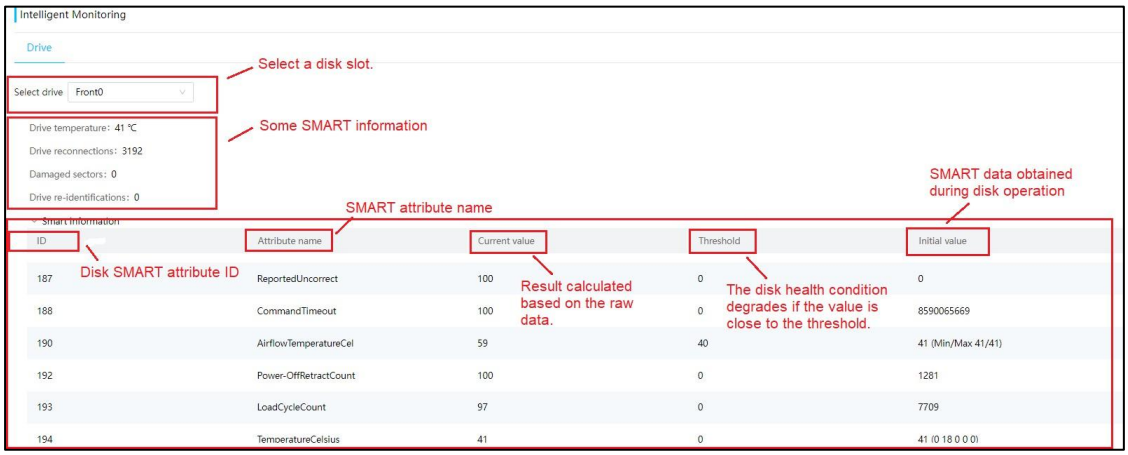
図86 論理ドライブのアラーム



HDDドライブのSMARTパラメーターのグラフィカル表示

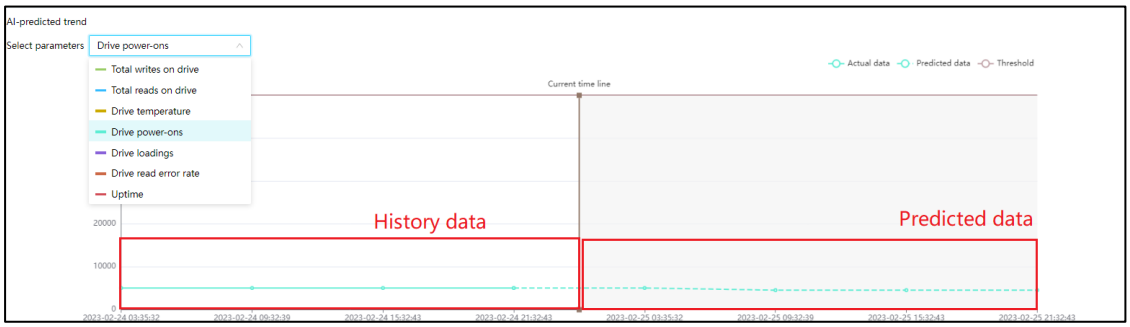
HDMは、各ドライブの属性、現在の値、しきい値、生データ情報などのSMARTパラメーターデータをグラフィカルに表示できます。

図87 SMART情報監視の推進



HDMは、HDDドライブからSMARTデータを収集し、KPIトレンド予測アルゴリズムを使用して、次の1日のSMARTデータパラメータートレンドを予測することをサポートしています。予測は、Webインターフェイスにグラフィカルに表示されます。

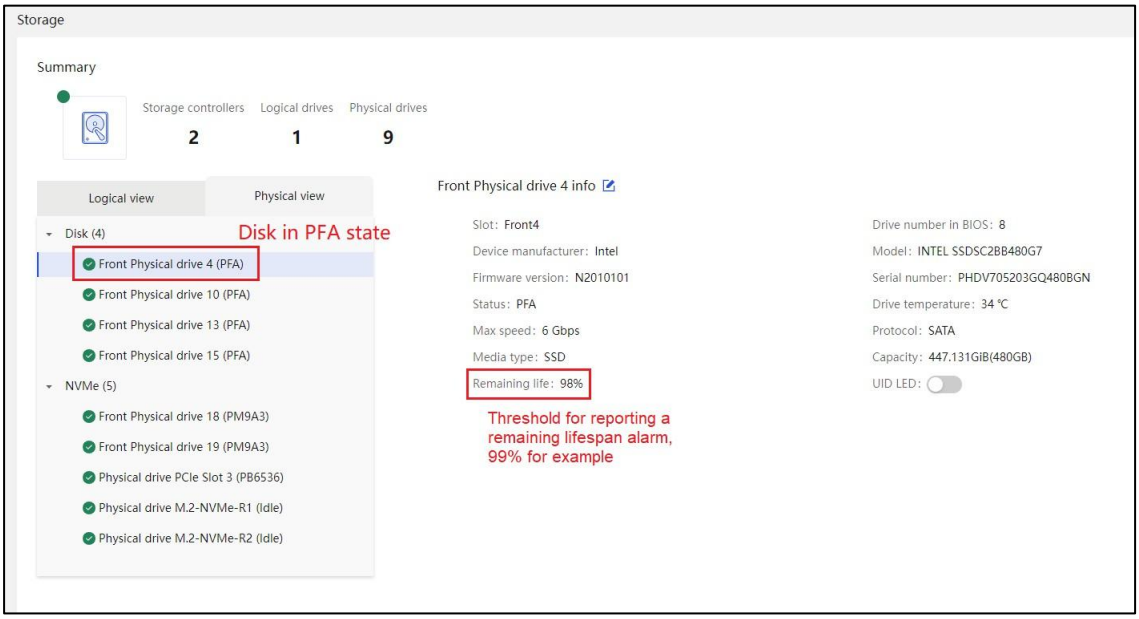
図88 SMART情報予測の推進



NVMe/SSDの残り寿命アラーム

HDMは、NVMeおよびSSDドライブの残りの寿命の割合をリアルタイムで表示できます。NVMeまたはSSDドライブの寿命がアラームしきい値に達すると、HDMは事前アラームを報告し、データの損失とドライブの障害を防ぐためにドライブを迅速に交換するようユーザーに通知します。ユーザーは、必要に応じて独自のアラームしきい値を柔軟に設定できます。

図89 NVMe/SSDの残りの寿命アラーム



ドライブの事前障害アラーム

ストレージコントローラーによって管理されるドライブは、事前障害アラームをサポートしているため、サーバーは潜在的な障害の兆候を検出し、事前にアラームを報告できます。これにより、ダウンタイムとサービスの中断が軽減され、システムの可用性と信頼性が向上します。

SHDロギングと診断

SHDは、PBSIチャネルを介してPMCストレージコントローラーのログ情報を取得できます。これには、60種類以上のストレージ関連の障害が含まれます。また、SHDは、MCTP(over PCIe)チャネルを介してPMCストレージコントローラーのログ情報を取得できます。これには、10種類以上のストレージ関連の障害が含まれます。

SHDは、LSIストレージコントローラーのログ情報を取得して、RAIDコントローラー、BBU、物理ドライブ、論理ドライブ、およびバックプレーンの障害に関連する500を超えるログを提供できます。

SHD診断は、PMCおよびLSI RAID/HBAログ情報の診断、対応するエラー原因の特定、およびソリューションの提供をサポートします。サポートされるモジュールには、RAIDコントローラー、ケーブル、BBU、およびストレージメディアが含まれます。

SMART情報収集診断

HDMは、SAS/SATA HDDおよびSSDドライブからSMART情報を取得し、HDD SMART情報に基づいて障害診断を提供できます。

ストレージコントローラーログ

ストレージコントローラーのログ(9300、9311、9400、および9500を除く)は、ワンクリックダウンロードで取得できます。

誤接続の検出

HDMは、AUXポートケーブル、SASケーブル、オンボードNVMeケーブルなどの誤って接続されたハードウェアケーブルを検出できます。この機能は、ケーブル関連の障害をタイムリーに特定して解決するのに役立ちます。

ストレージプロトコルスタック

PCIe上のMCTP

PCIe上の管理コンポーネントトランスポートプロトコル(MCTP)は、管理コンポーネント間の通信のためのプロトコルです。これにより、PCIeバスを介して異なるデバイス間で管理情報を転送し、対話することが可能になります。PCIe上のMCTPは、PCIeトランスポート層を使用し、管理コンポーネント間の通信のためにPCIeトランザクション層でMCTPメッセージフォーマットを定義します。このプロトコルにより、管理コンポーネントは、監視、構成、管理、障害診断を実装し、システム内のさまざまな管理情報を効率的に送信できます。

HDMは、IntelおよびAMD Genoaプラットフォームの両方でMCTP over PCIeをサポートしています。これは、HDMがAMDモデルでMCTP over PCIeを使用したコンポーネントの管理をサポートしていることを示しています。これには、次のものが含まれますが、これらに限定されません。

- アウトオブバンド方式でのPMCストレージコントローラーのRAID設定の作成/削除
- 論理ドライブ属性の設定。
- ストレージコントローラーとドライブのアウトオブバンドアップグレード
- LSIストレージコントローラーおよびドライブのアウトオブバンドアップグレード
- ネットワークアダプターのアウトオブバンドアップグレード

HDMのMCTP over PCIeソリューションは、IntelおよびAMDプロセッサーキテクチャの統合管理を可能にし、お客様に柔軟でスケーラブルなオプションを提供します。これにより、お客様はさまざまなハードウェアプラットフォームにわたってシステムを均一に管理および監視し、システムの安定性と信頼性を向上させることができます。

I2C上のMCTP

MCTP Over I2Cは、I2Cハードウェアバス上で動作する管理コンポーネントトランスポートプロトコルです。MCTP Over PCIeプロトコルとの主な違いは、物理チャネルです。

HDMは、MCTP Over I2CプロトコルによるMarvellストレージコントローラーとネットワークアダプターの帯域外管理をサポートしています。帯域外管理方法はより柔軟で、より多くのオプションを提供します。MCTP Over PCIeがサポートされていないサーバープラットフォームまたはデバイスでは、MCTP over I2Cを使用すると、関連デバイスの帯域外機能が適切に機能し、多様な顧客ニーズを満たすことができます。

NVMe-MI

NVMe管理インターフェイス(NVMe-MI)は、特にNVMeデバイスを管理するためのもので、システムがNVMe SSDドライブやその他のストレージデバイスを含む、接続されたNVMeデバイスを管理および監視できるようにします。NVMe-MIは、デバイス管理、監視、およびエラーロギングのための一連のコマンドとデータ構造を定義します。

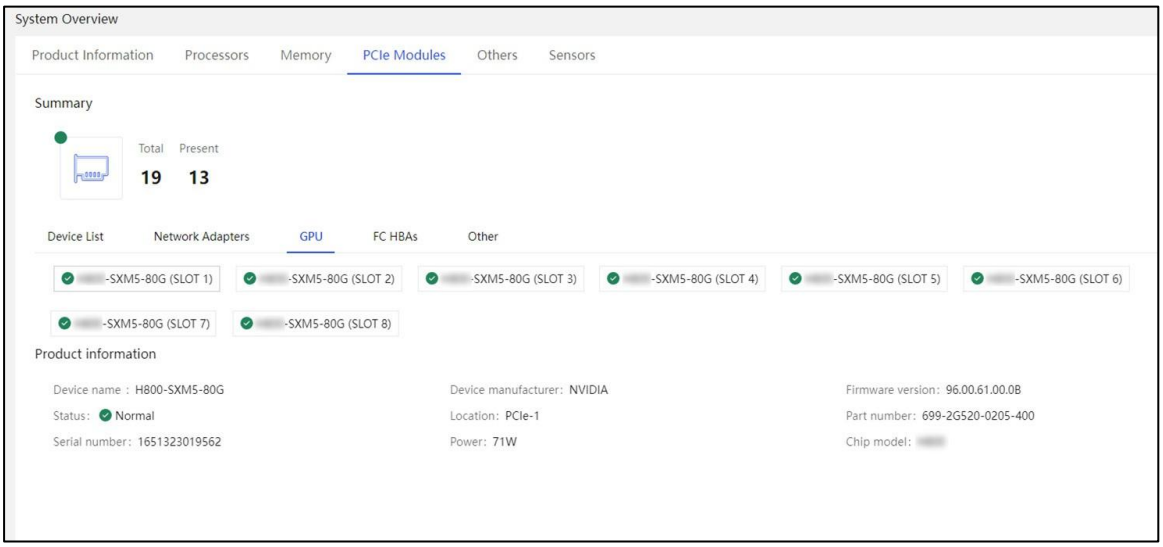
HDMは、NVMe-MIを介してMarvellストレージコントローラーおよび一部のNVMeドライブの帯域外管理をサポートします。これには、Marvellストレージコントローラー、論理ドライブ、および物理ドライブの基本情報の取得、障害ステータスの監視、および一部のNVMeドライブのSMART情報の取得が含まれます。

GPU管理

基本的なGPU情報の表示

HDMは、GPUのモデル、製造元、ファームウェアバージョン、ヘルスステータス、位置、部品番号、シリアル番号、電源、チップモデルなど、GPUの基本情報をPCIeタブに表示することをサポートしている。

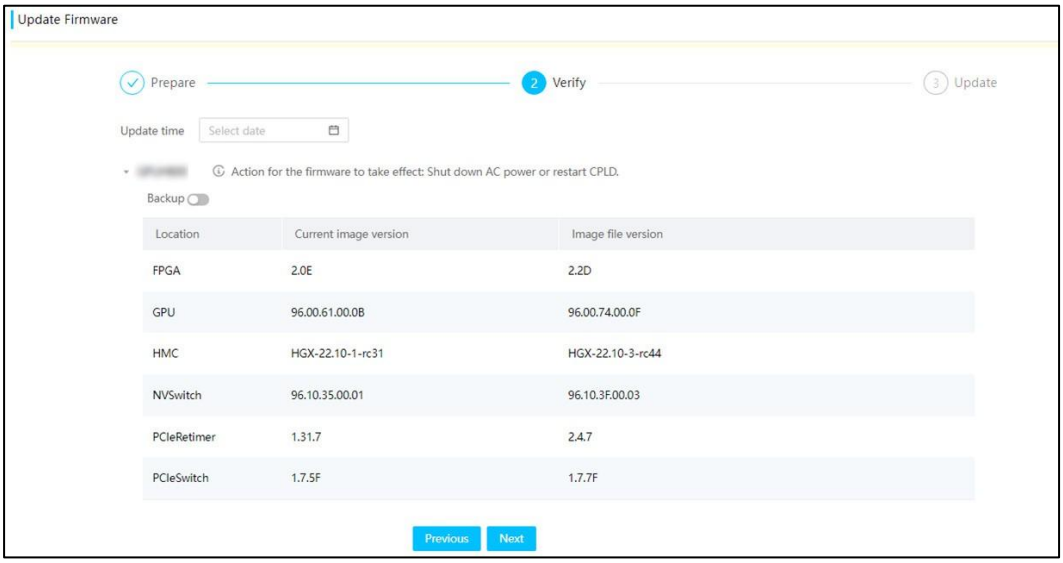
図90 基本的なGPU情報の表示



GPUモジュールのアウトバンドアップグレード

HDMは、GPUモジュール内のすべてのノードのファームウェアのアウトオブバンドバルクアップグレードをサポートする。ファームウェアには、HMC、FPGA、GPU、NVSwitch、PCIeSwitch、およびPCIeRetimerが含まれる。

図91 GPUファームウェア情報



GPUモジュールのアウトオブバンドアップグレードには、次の利点があります。

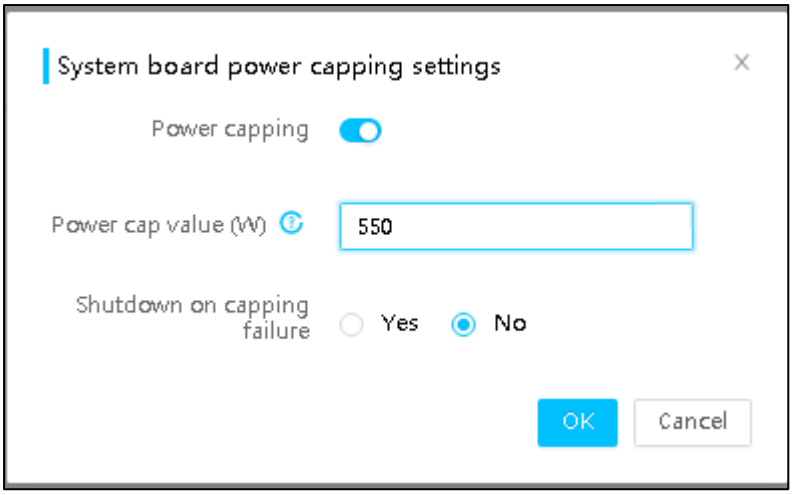
- 複数のGPUノードのファームウェアの一括アップグレードをサポートします。これにより、コンポーネントファームウェアの不一致によって引き起こされる制御不能なモジュールの問題が防止され、GPUメンテナンスの効率と安定性が大幅に向上します。
- イメージプールのバックアップをサポートしているため、1回のクリックでファームウェアを交換できます。

GPUノードの消費電力上限

GPU消費電力上限は、GPU電力制限とも呼ばれ、GPU管理テクノロジーです。GPUの熱設計電力(TDP)を制限できるため、GPUが制限されていても安定した状態を維持できます。

ヒートシンク。GPUの消費電力上限を設定することは、GPUの消費電力を制限し、過熱を防ぎ、GPUの安定性と信頼性を向上させることができるため、重要なタスクである。

図92 GPUノードの消費電力上限値の設定



GPUモジュールの障害診断

HDMを使用すると、ウェブインターフェイスからワンクリックでSDSをダウンロードすることで、GPUモジュール上のコンポーネントのすべての異常ステータスと自己検査レポートをエクスポートできる。

Redfishインターフェイスを通じてGPUモジュールによって生成されたアラームイベントを表示し、アラームレベルによってアラームイベントをフィルタリングすることができる。GPUの帯域外障害監視機能に応じて、HDMは、過熱、異常なGPUインプレーステータス、Power_goodステータス異常、PCIeインターフェイスステータス異常、ECC/UCE、重大なNVLink/NVSwitchエラー、XIDエラーメッセージ、HMCサービス異常、PCIe回復可能エラー、再起動時のHMC回復など、さまざまなアラームイベントをサポートする。

GPUの使用状況をリアルタイムで監視できます(FIST SMSのインストールが必要です)。

エネルギー効率管理

現在のデータセンターの規模が拡大するにつれて、そのエネルギー消費も増加しており、サーバーのエネルギー消費が高い割合を占めている。したがって、サーバーのエネルギー効率を達成することは、データセンターの効率的な運用に不可欠である。

HDMは、複数のインテリジェントな省エネルギー技術を統合することにより、サーバーのエネルギー消費を効果的に削減し、キャビネットの電力使用量と導入密度を向上させ、新しいインフラストラクチャ産業のグリーンな発展を促進するのに役立つ。さらに、HDMは、複数のH3C液冷サーバーと組み合わせて、お客様の液冷データセンターの正常な運用を確保するためのリーク検出などのサポートを提供する。

HDMは、CPU、メモリー、ファン、およびドライブのコンポーネントレベルのエネルギー消費を監視できます。

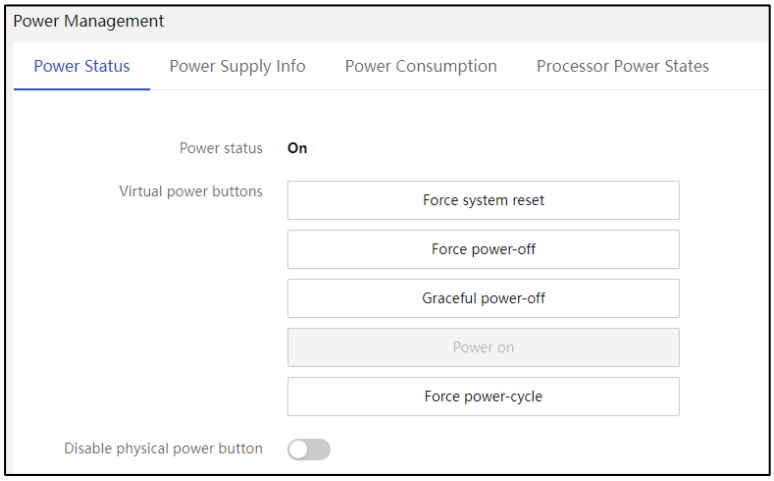
HDMからは、Redfish、IPMI、SNMPなどの複数のインターフェイスを介して消費電力データをリアルタイムで監視できます。デバイスの電源のオンとオフを制御したり、AC電源が復旧した後のサーバーシステムの起動ポリシーを設定したり、消費電力上限と電源装置の動作モードを設定したりできます。

HDMは、電力履歴消費統計、省エネ設定、ファン管理、パフォーマンスの最適化など、さまざまな機能もサポートしています。

サーバーの電源のオン/オフ

HDM Webインターフェイスからサーバーの電源をオンまたはオフにできます。

図93 サーバーの電源のオン/オフ



次の電源オプションを使用して、サーバーの電源ステータスを制御できます。

- 強制システムリセット:サーバーのコールドリセット。HDMは、通常のオペレーティングシステムのシャットダウンプロセスをバイパスして、PCHを直接プルしてシステムをリセットします。
- 強制的に電源をオフにする:OSの応答を待たずにサーバーをシャットダウンし、通常のオペレーティングシステムのシャットダウンプロセスをバイパスします。この効果は、サーバーパネルの電源ボタンを長押しした場合と同じです。
- グレースフルパワーオフ:サーバーを安全にシャットダウンします。HDMはOSにACPI割り込みを送信します。OSがACPIサービスをサポートしている場合は、まず通常のオペレーティングシステムのシャットダウン(実行中のすべてのプロセスを閉じる)を実行してから、システムの電源を切ります。OSがACPIサービスをサポートしていない場合は、電源切断のタイムアウトまで待機してから、システムを強制的にシャットダウンします。この効果は、サーバーパネルの電源ボタンを短く押すのと同じです。
- 電源オン:サーバーを起動します。
- 強制的に電源を入れ直す:サーバーの電源を切ってから入れ直します。
- 物理電源ボタンを無効にする:物理電源ボタンを無効にするために使用します。このオプションをオンにすると、物理電源ボタンの機能が無効になり、現場での電源ボタンの偶発的なトリガーによるサービスの中断が防止されます。

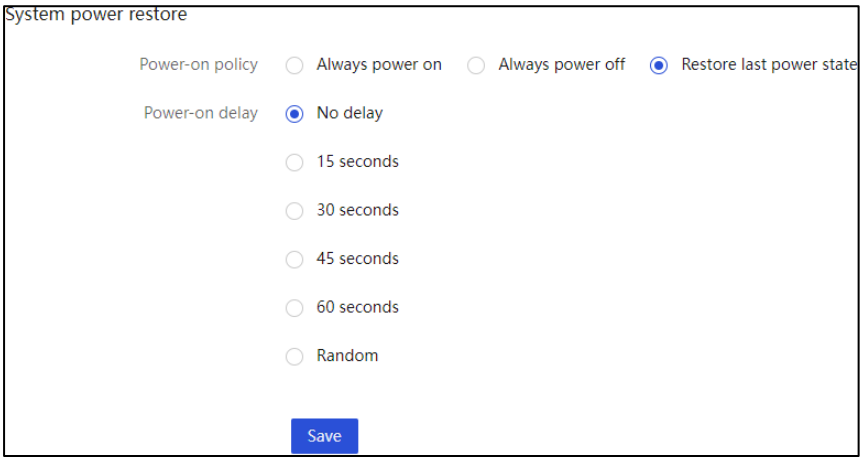
電源投入後のサーバーシステム起動ポリシーの設定

このタスクは、電源投入後のサーバーシステムの起動ポリシーを構成します。次のオプションがあります:

- 常に電源を入れる:電源を入れると、サーバーシステムが自動的に起動します。
- 常に電源を切る:電源を入れた後も、サーバーシステムの電源は切れたままになります。

- 最後の電源状態の復元:電源投入後、サーバーシステムは最後の停電前の状態に戻ります。サーバーはデフォルトでこのモードになっています。
- 電源投入遅延:起動遅延時間。オプションは、15秒、30秒、45秒、60秒、およびランダム(1～120秒)です。起動遅延は、サーバーの電源投入をずらすために使用でき、機器室でのサーバー起動プロセス中の瞬間的な電力消費を削減します。

図94 電源投入後のサーバーシステム起動ポリシーの構成



システムを起動する最後のコマンドは、HDMによって制御されます。電源投入後、最初にシステムボード上の予備電源が供給されます。その後、HDMが起動し、起動ポリシーに基づいてシステムを起動するかどうかを決定します。

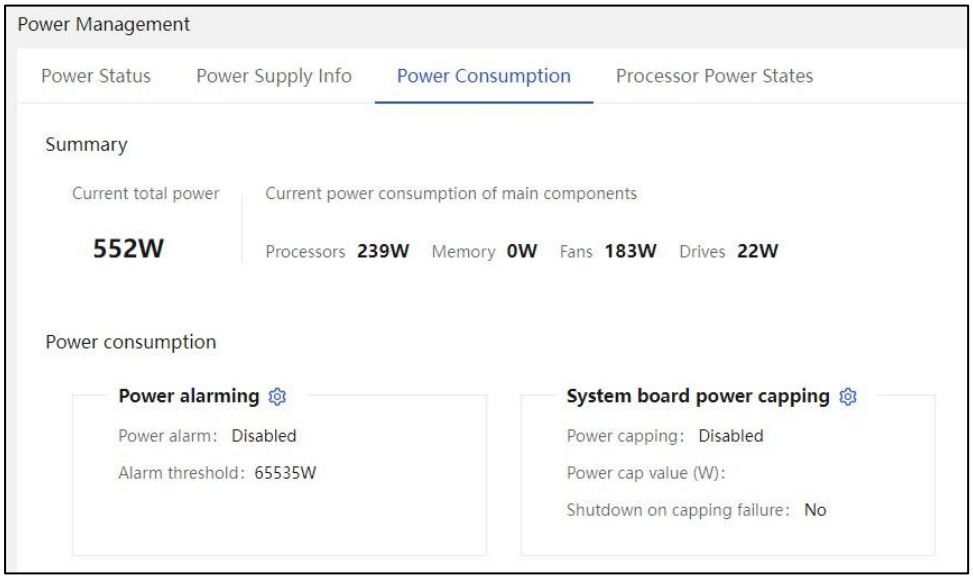
消費電力上限

消費電力上限機能は、予想されるシステム電力の上限を設定することによって機能します。システム電力がこの上限を超えると、アクションがトリガーされ、シャーシ内の電力が適切に分配されます。

上限設定が失敗した場合のアクションは次のとおりです。

- イベントロギング:ログは、上限設定の失敗後にシステムイベントファイルに記録されます。このアクションはデフォルトで実行されます。
- シャットダウン(オプション):上限設定の失敗後、システムは強制的な電源切断操作を実行します。

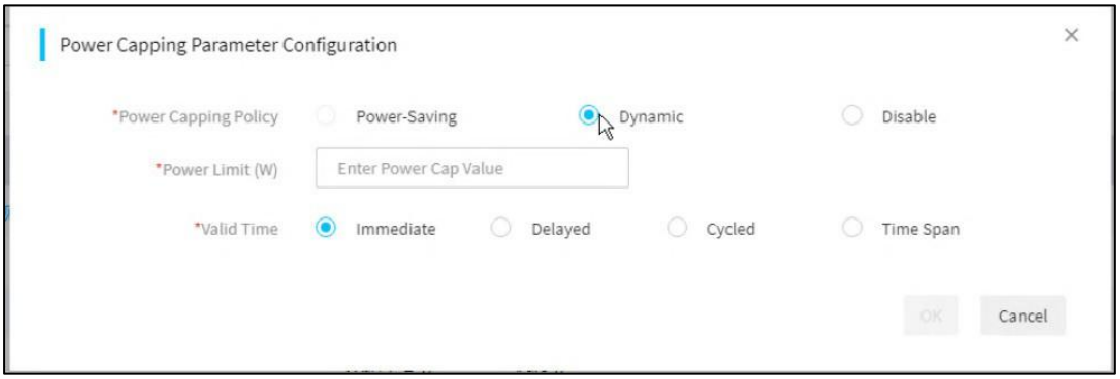
図95 システムボードの消費電力上限設定



HDMは、UniSystemとの連携を通じて、データセンターサーバーのインテリジェント消費電力上限と非常用消費電力上限をサポートします。

インテリジェント消費電力上限を使用すると、サービス特性に基づいてサーバーの消費電力上限値をインテリジェントに調整できるため、顧客サービスの導入を最適化するのに役立ちます。

図96インテリジェント消費電力上限の設定



緊急ワンクリック消費電力上限を使用すると、データセンターで緊急の電源障害が発生した場合に、ワンクリックで各サーバーの消費電力上限値を設定できます。これにより、データセンターサーバーの消費電力を迅速に削減し、主要なコアサービスサーバーへの電力供給を確保し、顧客の重大な損失を防ぐことができます。

図97 緊急時のワンクリック消費電力上限設定

電源装置の動作モード

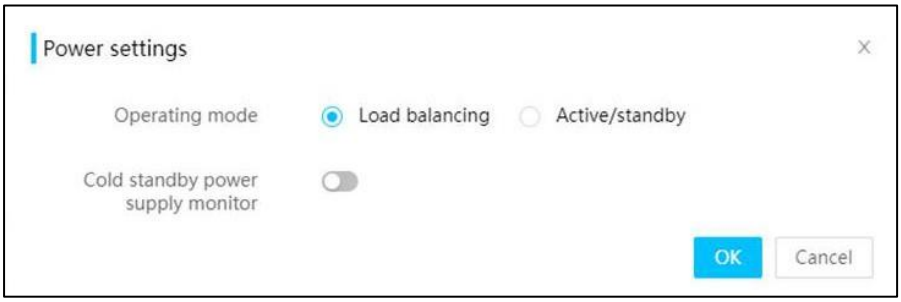
サービスの電力消費が満たされているという前提の下で、一部のパワーサプライをホットスタンバイモードで動作するように構成して、電力変換効率を向上させることができます。HDMから、サーバーパワーサプライの動作モードを設定できます。オプションは、**Load balancing**および**Active/Standby**です。

Active/standbyモードでは、最低1つのアクティブ電源装置と最低1つのスタンバイ電源装置を指定する必要があります。

- アクティブな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。
- アクティブな電源装置の実際の消費電力が最大定格消費電力の62%を超えると、スタンバイ電源装置がアクティブになって電力を供給します。

ロードバランシングモードでは、存在するすべての電源装置がアクティブモードになり、負荷分散が行われます。

図98 電源装置の動作モードの設定



コールドスタンバイ パワーサプライモニター

コールドスタンバイ電源装置モニタ(検査)を有効にすると、現在のすべてのコールドスタンバイ電源装置がアクティブモードで動作しているときに正しく電力を出力できることを確認するために、月に1回テストされます。検査中は、電源装置モードがロードバランシングモードに切り替えられ、電源装置グループの全体的な出力が正常かどうかがチェックされます。異常な場合は、SELアラームが報告されます。

- 検査結果が正常であれば、電源装置の動作モードはユーザー設定モードに戻ります。
- 検査結果が異常な場合、電源装置の動作モードはロードバランシングモードのままになります。

コールドバックアップ電源装置の検査をイネーブルにするには、次の条件が満たされていることを確認します。

- 電源グループは正常で、アラームは発生していません。
- グループ内の現在の電源の数は2つ以上です。

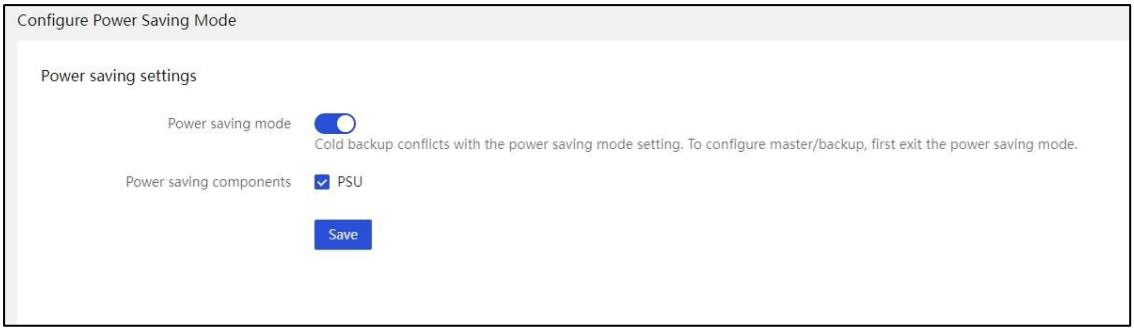
両方の電源装置動作モードで、コールドバックアップ電源装置検査をイネーブルにできます。

コールドバックアップ電源装置検査は、電源装置の健全性と安定度を確保し、システムの信頼性と安定度を向上させることができます。

ダイナミックアクティブ/スタンバイ電源モード

インテリジェント省電力モード(動的アクティブ/スタンバイ電源モード)では、HDMはサーバーの総電力に基づいてリアルタイムで電源動作モードを動的に調整し、電源サブシステムが最高の効率でサーバーの通常動作を維持し、省エネルギーと消費削減の目標を達成することを保証します。サーバーの総電力が高い場合、電源は自動的に負荷分散モードに切り替わります。サーバーの総電力が低い場合、電源は自動的にアクティブ/スタンバイモードに切り替わります。

図99 動的なアクティブ/スタンバイパワーサプライモードの設定



注:

現在この機能をサポートしているのは、2台の電源装置を搭載したサーバーモデルだけです。

過去の電力消費統計

HDMは、正確な電力消費の監視と曲線による統計を提供し、管理者が電力と冷却リソースの実際の使用状況を深く理解できるようにします。ユーザーは、履歴データに基づいてサーバーのエネルギー効率を最適化できます。

このページは、最近30日間の電力消費情報の表示をサポートしています。

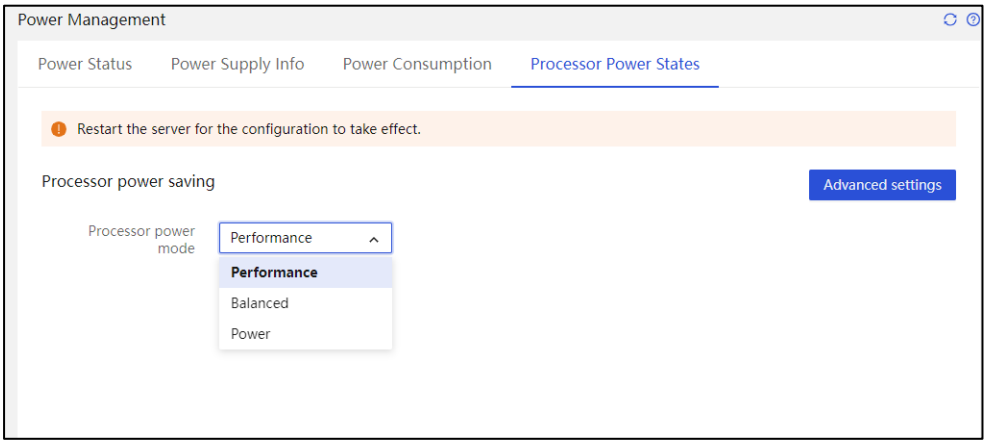
図100 電力履歴消費統計

省エネ設定

HDMからは、パフォーマンスモード、省電力モード、バランスモードなどの電力パフォーマンスモードをワンクリックで設定でき、サーバーのパフォーマンス、消費電力、およびノイズに関するさまざまなお客様のニーズやシナリオに対応できます。

CPUの最大動作周波数(Pステート)を調整することで、システムの消費電力を削減できます。HDMは、さまざまな製品のニーズを満たす柔軟な選択のための複数の調整レベルを提供します。

図101 省エネ設定



ファンの管理

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てファン速度を調整すること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

MSアルゴリズムを使用して、さまざまな温度でのファン速度を.xmlコンフィギュレーションファイルに指定できます。

PIDアルゴリズム

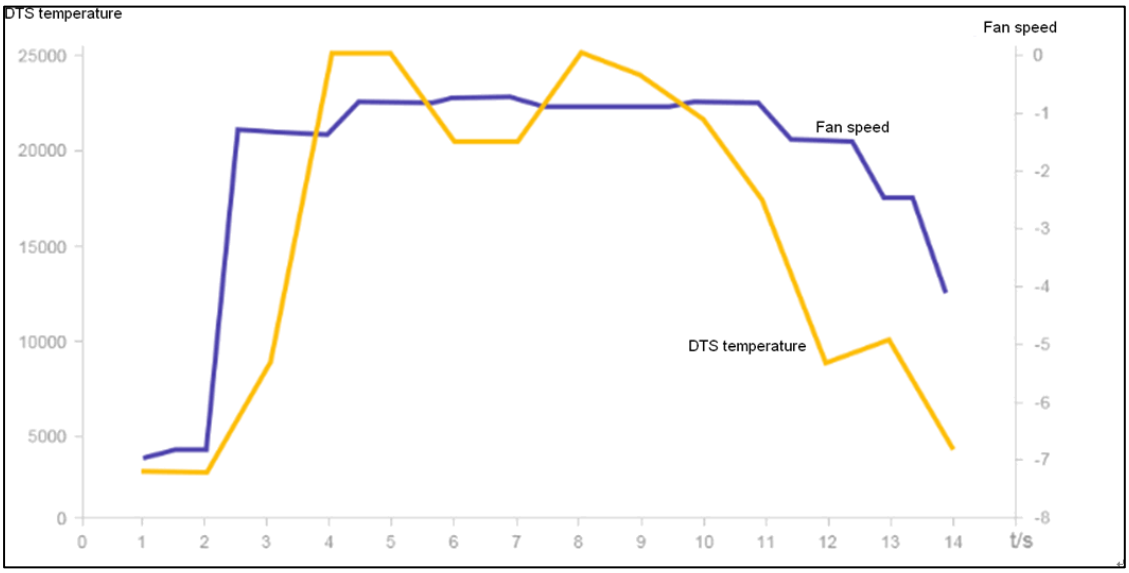
PIDアルゴリズムは、.xml構成ファイル内のセンサー速度パラメーターとセンサー温度測定値を使用して、リアルタイムで最適化されたファン速度を計算するために使用されます。PIDアルゴリズムは、より正確な方法でファン速度を調整できます。PID制御アルゴリズムは、図102に示すように動作します。

図102 PID制御アルゴリズム

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

図103に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示すが、DTSの温度が増減すると、それに応じてファン速度も増減する。

図103 PIDアルゴリズムによるファン速度の調整



ファン速度モード

ユーザーは、さまざまなシナリオに応じてファン速度制御設定を構成できます。システムは、固定ファン速度の手動設定、負荷および冷却条件に基づく自動速度制御、および必要に応じたファン速度モードの設定をサポートします。

- **Silent** -サーバーの熱放散に必要な最低速度でファンを動作させます。このモードは、高ノイズ要件のシナリオに適しています。
- **Balanced** -ファンをより高速で動作させて、バランスのとれたノイズ制御と冷却パフォーマンスを提供します。
- **Powerful** -ファンを可能な限り高速で動作させます。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**: 1～20の範囲で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、速度が速くなり、ノイズが大きくなります。

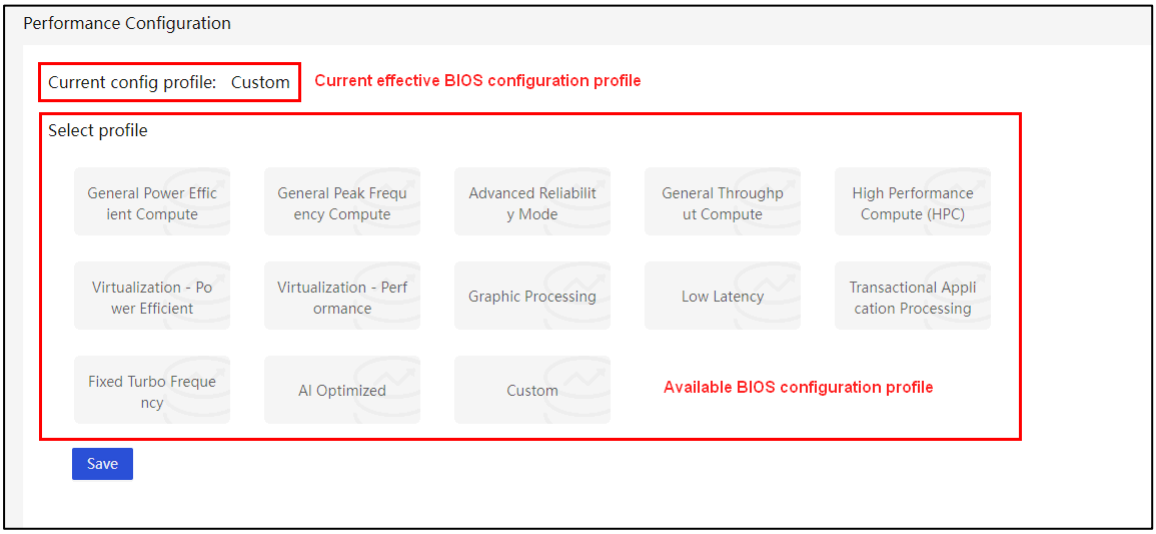
パフォーマンスの最適化

サーバーのデフォルトのBIOS設定は、パフォーマンスと電力効率のバランスを実現します。これらの設定は、特定のアプリケーションワークロードに合わせて調整できるため、お客様はアプリケーションのパフォーマンスを向上させることができます。この機能はインテルのモデルでのみサポートされており、一部の機能はライセンス制御されています。

パフォーマンス構成

BIOS構成プロファイルは、予想されるサーバープリケーションに適応するためのBIOS構成オプションの集合です。HDMは、ユーザーが独自のアプリケーションシナリオに最も適したBIOS設定をデプロイするのに役立つ10を超えるBIOS構成プロファイルを提供します。

図104 パフォーマンス構成



HDMは、ユーザーがワークロード固有の構成プロファイルに基づいてBIOSを設定する際に役立つ次のBIOS構成プロファイルを提供します。構成プロファイルがデプロイ済のワークロードと一致する場合、BIOSのデフォルト値を使用するよりもパフォーマンスが向上する可能性があります。

- 一般的な省電力コンピューティング

  ほとんどのアプリケーションに適用され、省電力に重点が置かれています。このプロファイルにより、プロセッサーは省電力ステータスで動作し、プロセッサーチップはスリープモードに入り、仮想化構成が無効になります。これは一般的な省電力構成です。

- 一般的なピーク周波数の計算

  ワークロードをサポートするためにプロセッサーまたはメモリーを必要とするシナリオに適用されます。単一のコアで最大周波数を使用可能にします。省電力および仮想化構成を使用不可にすることで、このプロファイルは、プロセッサーコアがC0/C1アクティブステータスで動作できるようにします。

- 高度な信頼性モード

  パフォーマンスポリシーを採用して、ウェイクアップによる待ち時間を短縮し、エラー発生時のシステムのレスポンスタイムを短縮することにより、保守性を向上させます。ベストプラクティスとして、X4メモリーを使用し、ADDDCスペアリングを有効にします。X8グラニュラーメモリーが設定されている場合、ADDDC機能はサポートされません。

- 一般的なスループット計算

  継続的に最大のワークロードスループットを必要とするシナリオに適しています。このプロファイルにより、プロセッサーは使用可能なすべてのコアにわたって最大の使用率で継続的に動作できます。SNCを有効にすることで、LLCへの平均アクセス速度が向上します。Non Uniform Memory Access(NUMA)を介した一部のワークロードへのアクセスにより、パフォーマンスが向上し、最適なスループットが可能になります。

- ハイパフォーマンスコンピューティング

  高パフォーマンスの構成を必要とするシナリオに適用できます。通常、各ノードが最大の効率で動作して大規模なワークロードに対処するクラスタ環境で使用されます。このプロファイルは、仮想化がサーバーに展開されていない場合に仮想化IOのサポートを無効にし、省電力関連の設定を無効にします。

- 仮想化-省電力性

  省電力を優先する仮想化シナリオに適用できます。このプロファイルにより、利用可能なすべての仮想オプションが有効になり、プロセッサーチップがスリープモードに入ることができます。

- 仮想化のパフォーマンス

  高いパフォーマンス要件を持つ仮想化シナリオに適用できます。このプロファイルにより、仮想化をサポートするためのすべての仮想化関連オプションが有効になり、省電力オプションを無効にしてより高速にすることで、システムをより高い周波数で動作させることができます。

- グラフィック処理

  GPUサーバーに適用できます。GPUは通常、I/Oとメモリー間の最大帯域幅に依存します。このプロファイルは、I/Oとメモリー間のリンクに影響を与える電源管理機能を無効にし、ピアツーピア通信を確保するために仮想化を無効にします。

- 低レイテンシ

  最小の計算レイテンシを必要とするアプリケーションに適しています。全体的な計算レイテンシを削減するために、このプロファイルは、最大の実行速度とスループットを犠牲にすることによって計算レイテンシを引き起こす可能性のある電力管理およびその他の管理機能を無効にします。

- トランザクションアプリケーション処理

  データベースシステムなどのサービスアプリケーションシナリオに適用できます。ピーク頻度とスループットの要件のバランスをとることができます。

- 固定ターボ周波数

  固定ターボ周波数が使用されるシナリオに適用されます。このプロファイルはアウトバンド方式で実装されます。OSは周波数調整に参加しません。

- AI最適化

  大量のコンピューティングリソースでの人工知能推論またはトレーニングを含むシナリオに適用できます。このプロファイルは、CPUを最高のパフォーマンスレベルにロックすることにより、人工知能推論またはトレーニングアプリケーションシナリオのサーバーパフォーマンスを向上させます。

- カスタム(Custom)

  BIOSのデフォルト設定を使用します。ユーザーは必要に応じてオプション設定を変更できます。

パフォーマンスコンサルタント

サーバーリソースの使用状況に基づいてBIOS設定を調整してワークロードのパフォーマンスを向上させることは、多くの場合、直感的ではなく、コストがかかります。この問題を解決するために、HDMにはパフォーマンスコンサルタント機能が用意されています。パフォーマンスコンサルタントは、多数の重要なサーバーパフォーマンスインディケータを監視し、推奨されるワークロードプロファイルを提供します。

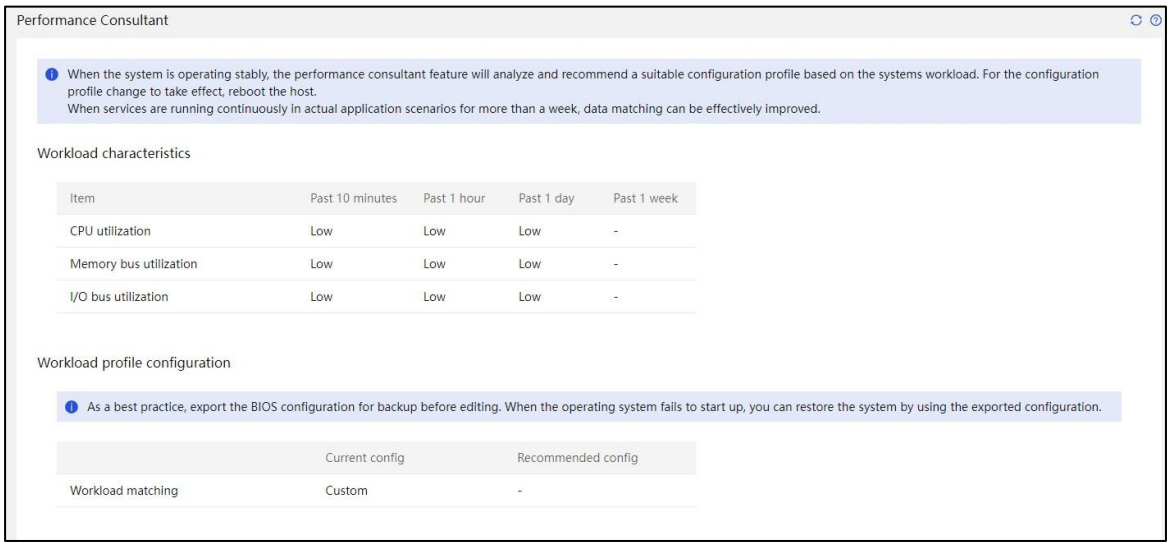
推奨されるワークロードプロファイルは、ワークロードに使用される実際のサーバーリソースに基づいています。この機能はパフォーマンス構成に依存しており、ユーザーは設定をさらにカスタマイズできます。

パフォーマンスコンサルタントは、マルチステージアプローチを使用して、ワークロードオペレーション中のシステム動作を分析します。

- パフォーマンスコンサルタントは、パフォーマンス監視インディケータを分析して、一連の使用状況または動作特性レポートにワークロードをマッピングします。これらの特性は単純な場合もありますが(高いメモリー使用量など)、潜在的なリソース使用量のボトルネックを特定するための開始点となります。
- パフォーマンスコンサルタントが推奨するBIOSプロファイルを使用すると、より理想的な効果を得ることができます。

パフォーマンスコンサルタントを使用すると、ユーザーはワークロードの特性を理解し、ワークロードの特性に基づいて構成プロファイルを推奨できます。

図105 ワークロードのプロファイルの推奨

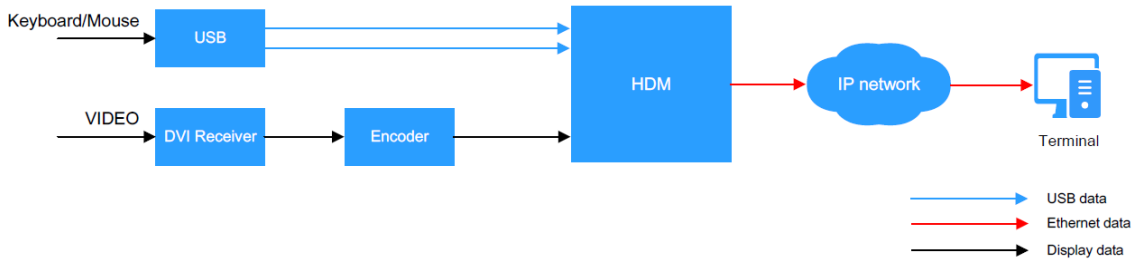


リモートコントロール

キーボード、ビデオ、およびマウス

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106 KVMの図

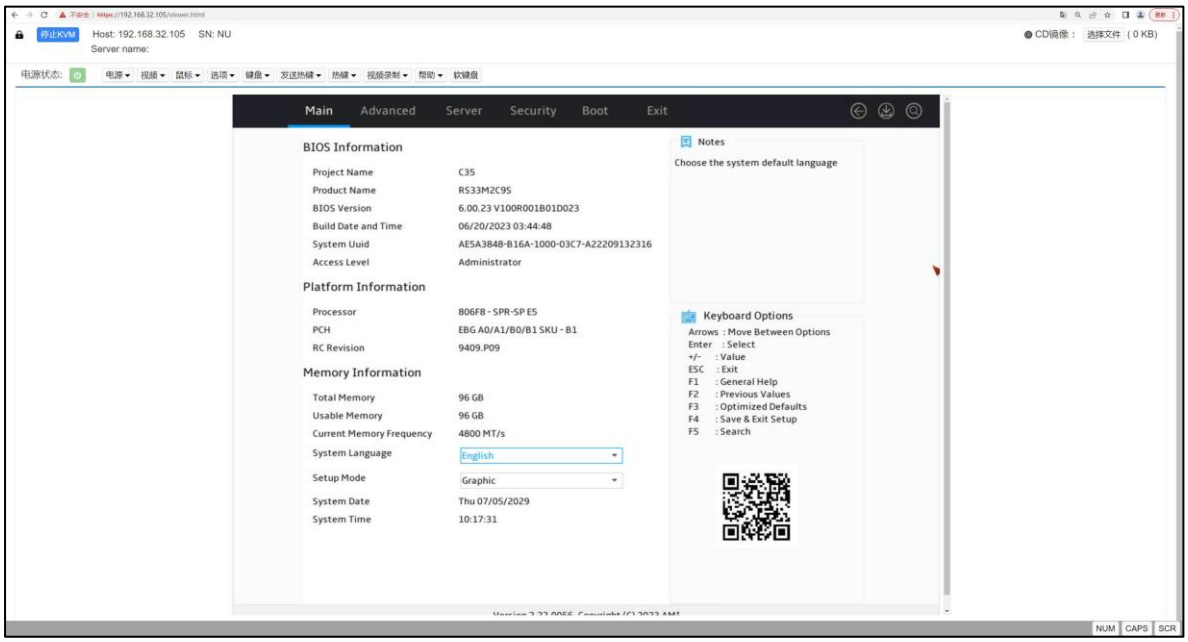


H5 KVM(キーボード、ビデオ、マウス)

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で管理できます。H5 KVMは、デュアルCDイメージのマウントをサポートしています。

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https://ip_addr/viewer.html?u=user_name&p=user_passord。

図107 H5 KVMへの直接アクセスの例

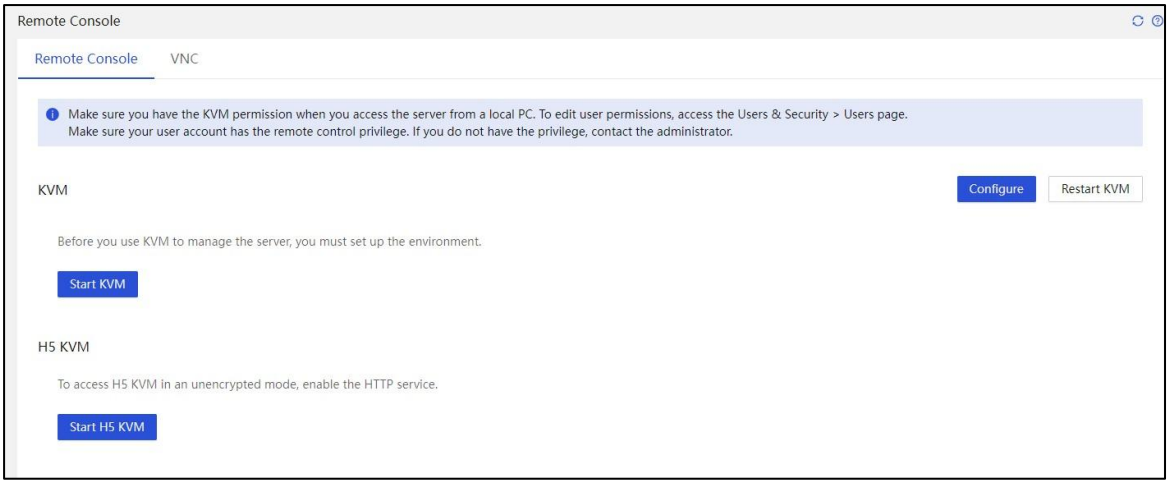


KVM起動モード

次のKVM起動モードを使用できます。KVMを有効または無効にするには、Remote Services > Servicesページに移動します。

- **Dedicated mode**: 専用モードでは、1つのリモートコンソールセッションだけが許可され、ユーザーにフルアクセス権限が付与されます。
- **Shared mode** - 共有モードでは、1つの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可能です。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付与され、ビデオの表示、スクリーンショットの取得およびビデオの記録のみが可能です。

図108 KVM起動モードの選択



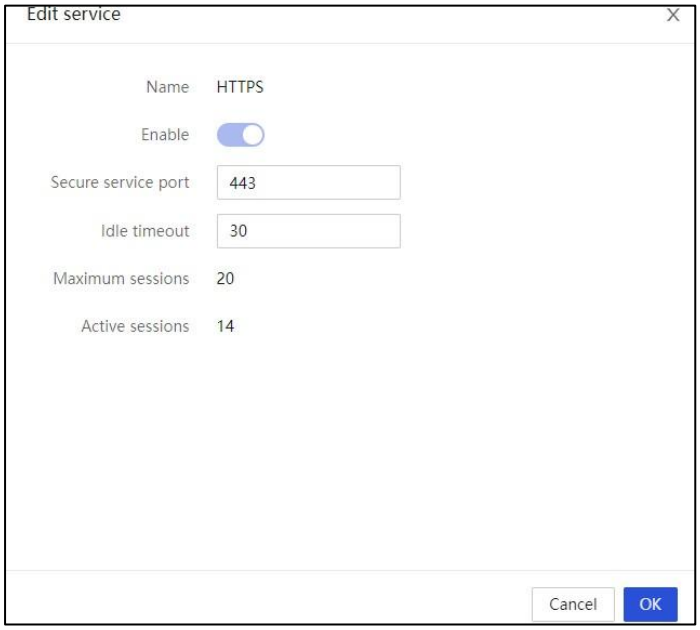
KVMのイネーブル化ステータスを変更するには、Remote Services > Servicesページに移動します。KVMをイネーブルにする場合は、KVMポートも選択できます。

- **Secure service port**: データ伝送のセキュリティを強化するには、このオプションを選択した後

に暗号化モードを有効にして、クライアントとサーバー間のセキュアな通信を確保します。

- **Insecure service port**: データ送信の適時性を向上させるには、このオプションを選択した後に暗号化モードを無効にして、大量のデータ送信を容易にします。

図109 KVMサービスの編集



仮想メディア

仮想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。ローカルメディアには、DVD-ROMドライブ、フロッピードライブ、DVD-ROMイメージファイル、フロッピードライブイメージファイル、またはハードドライブユーザーがあります。仮想メディアデータは、aes128-cbc暗号化アルゴリズムを使用して暗号化できます。仮想メディアを使用すると、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できます。

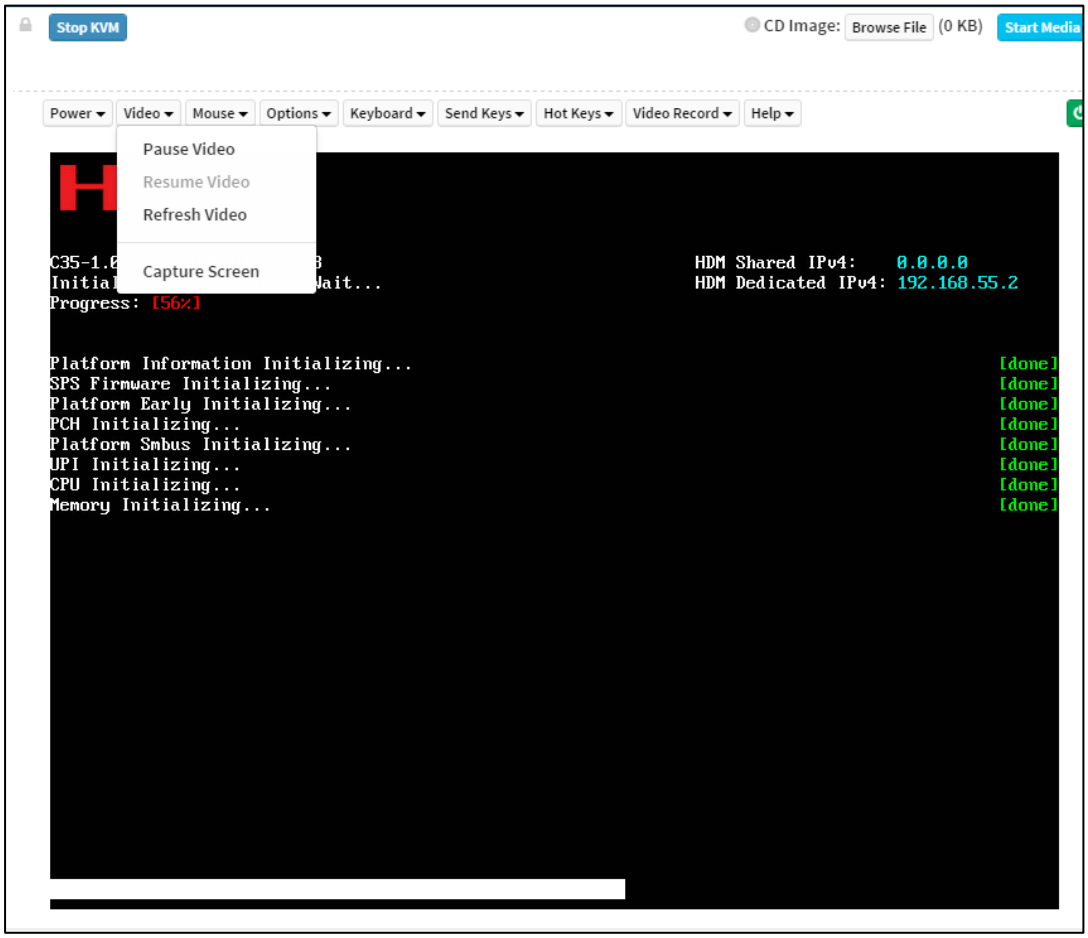
次の仮想ストレージメディアを使用できます。

- 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ユーザー。
- USBキー。

KVMからのスクリーンキャプチャ

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、その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。

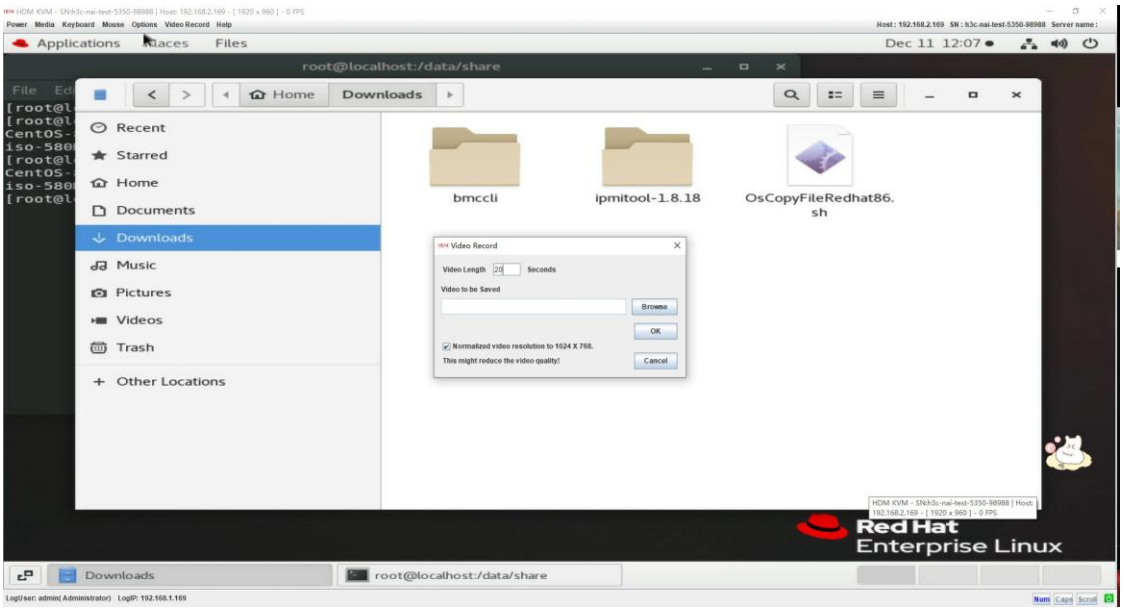
図110 スクリーンショットのキャプチャ



KVMからのビデオ録画

KVMリモートコンソールでビデオを録画し、スクリーンショットを.avi形式でローカルPCに保存できます。ビデオは、仮想KVM操作を記録して、セキュリティを確保したり、その他の特別な要件を満たすことができます。ビデオ録画が有効になっている場合、KVMリモートコンソールは、画面に表示されるすべての情報と実行されたすべての操作を自動的に自己定義のビデオファイルに記録します。ビデオは、ローカルプレイヤーを使用して再生できます。

図111 KVMからのビデオ録画の設定



ハードウェアのサポート

KVMの伝送パフォーマンスを向上させるために、差分フレームとハードウェアカーソルがサポートされています。

VNC

VNCについて

仮想ネットワークコンソール(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。

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、VNCサーバーにリモートで接続します。サードパーティのVNCクライアントには、RealVNC、TightVNCまたはNoVNCがあります。

HDMはIPv4とIPv6の両方のVNCセッションをサポートします。

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。どちらのセッションも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る場合、排他モードで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、別のVNCセッションに対する後続の要求

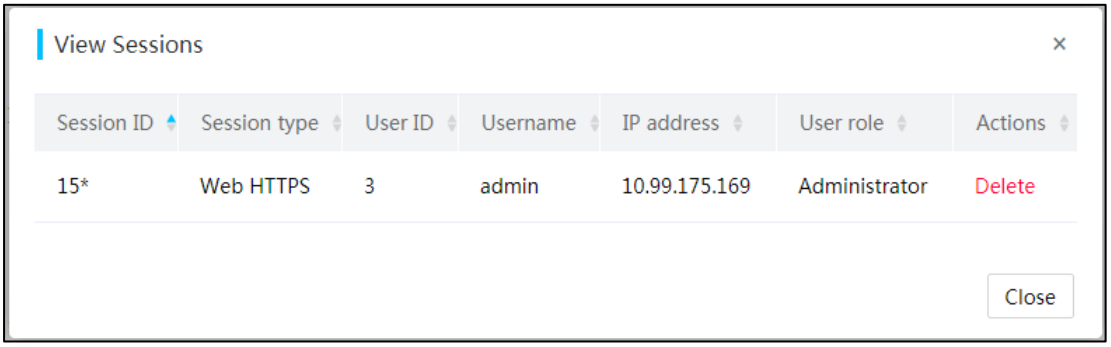
は拒否されます。

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セッションの表示

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。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。

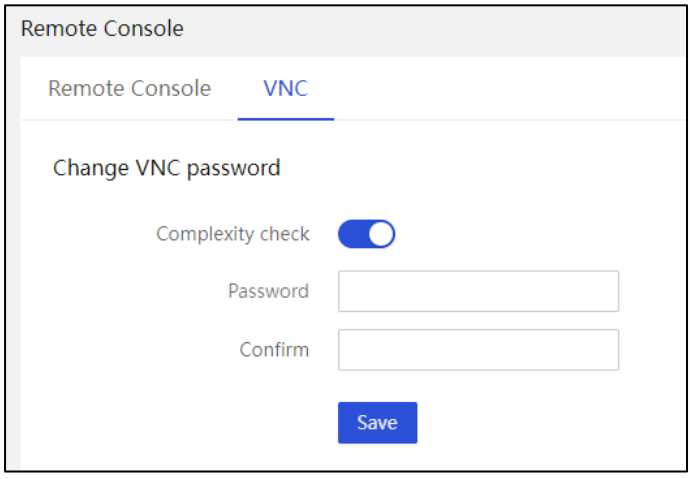
図112 VNCセッション情報



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文字である必要があります。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文字から8文字である必要があります。

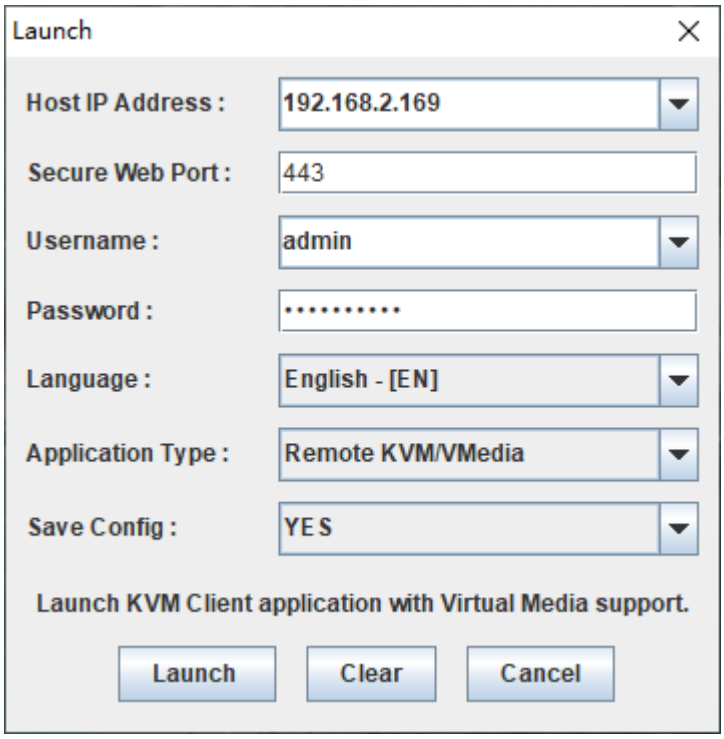
図113 VNC設定



JViewerクライアント

JViewerクライアントは、HDMにログインしなくてもサーバーにアクセスして制御できます。このクライアントは、WindowsとLinuxの両方のオペレーティングシステムと互換性があり、将来のユーザーログインのためにサーバー接続設定を保持します。セキュリティを確保するために、構成内のパスワードは、SM4国家暗号化アルゴリズムを使用して処理された後に保存されます。

図114 JViewerクライアント

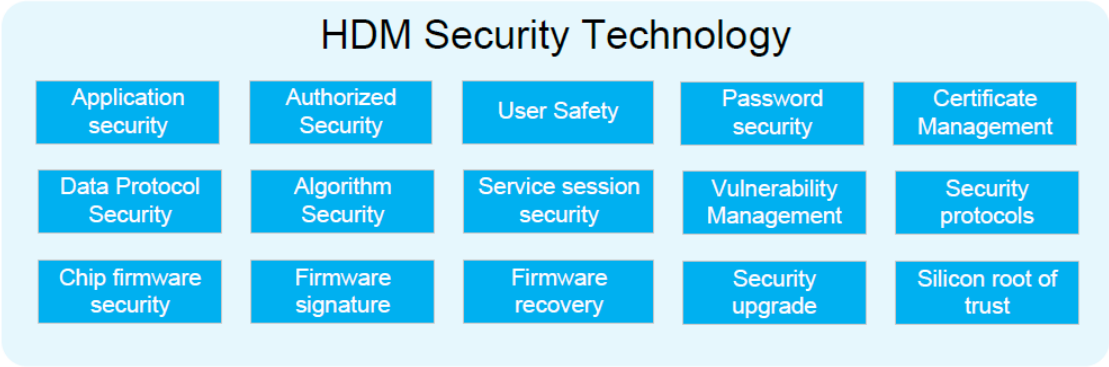


セキュリティ管理

HDMはサーバー管理システムであり、データセンター管理ネットワークのサブネットである。HDMの脆弱性が悪意を持って悪用されると、サーバーの安全な運用に脅威を与え、データセンター全体の安全な運用に影響を与える可能性がある。

HDMは、運用上の利便性を提供するだけでなく、一連のセキュリティ技術を通じてシステムを保護し、サーバーの安全な運用を保証する。サーバーの安全な運用は、データセンター全体の安全な運用に不可欠である。HDMのセキュリティ技術には、ソフトウェアセキュリティ、ファームウェアセキュリティ、インターフェイスセキュリティ、および機密データセキュリティが含まれる。

図115 HDMセキュリティ技術



セキュリティメカニズム

サーバーの帯域外管理ファームウェアは、次のセキュリティメカニズムをサポートしています。

ログ管理

すべてのユーザーアクセスに対して、システムはその後の管理者による管理と分析のためにすべての情報をログに記録します。ログ管理はデバイスの情報ハブであり、さまざまなモジュールによって生成されたログを受信します。受信したログは、モジュールとレベルに応じてコンソール、監視端末、ログホストに出力できます。これにより、管理者がデバイスの動作を監視し、ネットワーク障害を診断するための強力なサポートが提供され、TOEの安全な動作とログ追跡が保証されます。

証明書とキーの管理

HDMは、SSL証明書の暗号化と証明書の置換をサポートしています。Webページで証明書を置換できます。

セキュリティを向上させるためのベストプラクティスとして、独自の証明書と公開キーと秘密キーのペアを使用し、証明書を迅速に更新してその有効性を確認します。

HDMはまた、LDAP証明書のインポートをサポートし、データ送信のための認証暗号化を提供して、システムセキュリティを強化します。

プロトコルとデータ伝送のセキュリティ

プロトコルおよびポートの攻撃を防ぐために、HDMは最小限の数のネットワークサービスポートを開きます。使用されていないネットワークサービスポートを閉じ、サービスが正式に使用されている場合はデバッグのためにネットワークサービスポートを閉じます。安全でないプロトコルのポートはデフォルトで閉じられます。

HDMは、リモートコンソールを使用する場合の安全なデータ伝送のためにKVM暗号化をサポートします。また、仮想メディアデータ伝送のための暗号化もサポートし、データ伝送のセキュリティを確保します。HDMは、NCSIを使用して、サーバーのサービスプレーンから管理プレーンを分離します。HDMは、NCSI帯域外ネットワークポート機能を通じて、サービスプレーンと同じNICを共有できます。物理層では、管理プレーンとサービスプレーンはインターフェイスを共有します。ソフトウェア層では、管理プレーンとサービスプレーンはVLANによって分離され、互いに見えません。

アクセス制御とユーザー認証

HDMは、シナリオに基づいてログイン制御を実装し、時間、場所(IP/MAC)およびユーザーの観点からサーバー管理インターフェイスのアクセスを最小範囲に制御します。HDMは、Webインターフェイスに基づいてログインも制御します。必要に応じて、最大3つのログインルールをサポートするログインルールを使用して許可リストを設定できます。ログインルールが一致すると、ログインが許可されます。HDMは、パスワードの複雑さ、脆弱なパスワードディクショナリ、パスワードの最大妥当性、パスワードの最小妥当性、非アクティブ制限、エマージェンシーログインユーザー、履歴パスワードの無効化およびアカウントロックアウトのしきい値などの機能を使用して、アカウントのセキュリティを確保します。

例外処理

このシステムは、主に故障データの収集、リアルタイム故障解析、故障予知警告、解析予測結果の提示など、デバイスのライフサイクル全体を通じてインテリジェントな診断を行う。さらに、ネットワーク管理システムの設定に基づいて、HDMは積極的にトラップを送信し、システム管理者に事前予防のための情報を提供する。

定期的な自己点検

このシステムは、TOEのCPU、メモリー、ハードドライブなどのコンポーネントを定期的に検査し、しきい値を超えるアラームにリアルタイムで応答します。また、サーバー統計の収集と視覚化、およびハードウェアセキュリティとパフォーマンス調整のための多次元しきい値制御もサポートします。

HDMがサポートするセキュリティ標準

HDMが参加して策定された基準は表9のとおりである。

表9 HDMが参加した基準

識別子	タイトル	標準
1	情報セキュリティ技術サーバーセキュリティの技術要件及び評価基準	中国国家規格-GB/T 39680-2020
2	グリーンコンピューティングのための技術要件サーバーの信頼性	業界標準-GCC 1001-2020
3	グリーンコンピューティングサーバーのベースボード管理コントローラー(BMC)の技術要件	業界標準-GCC 3002-2020
4	ネットワークキーデバイスセキュリティの一般的な検出方法	グループ基準-T/TAF 088-2021

HDMによって取得される認定には、次のものがあります。

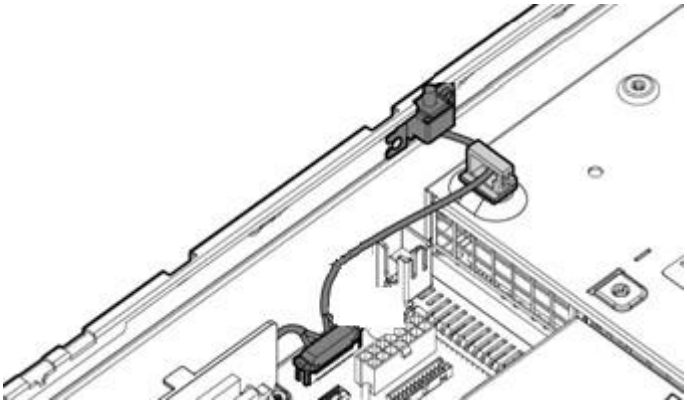
- Evaluation Assurance Level(EAL)4証明書
- ソフトウェア著作権証明書
- China Telecommunication Technology Labs(CTTL)証明書

HDMは、最高のEAL 4証明書であるChina Cybersecurity Review Technology and Certification Center(CCRC)の最も厳格な標準証明書を取得しています。認証プロセスでは、CCRCはタイプテスト+工場検査+認証後監督モデルを採用し、H3C HDMのセキュリティと信頼性を検証するだけでなく、工場検査と認証後監督を通じてソフトウェア製品の完全なプロセス安定性と信頼性を確保しています。これにより、HDMはユーザーにとって信頼できる信頼性の高いサーバーリモート管理システムになります。

シャーシ侵入検知

サーバーのアンボックス検出モジュールがアンボックス信号をトリガーすると、ソフトウェアはハードウェアGPIOピンから送信された信号を受信してソフトウェア割り込みをトリガーし、現在の信号がアンボックス信号であるかボクシング信号であるかを判断する。アンボックス信号またはボクシング信号が確認されると、HDMはセンサーを介してイベントログを生成する。

図116 開梱検出モジュール



ハードウェア暗号化

HDMのSOCチップは、HACE暗号化エンジンを使用してハードウェアデータ暗号化を内部でサポートするハードウェアセキュリティアクセラレーションモジュールをサポートしている。ソフトウェア暗号化をハードウェア暗号化に置き換えることで、HDMは複雑な暗号化操作を回避し、暗号化効率を向上させ

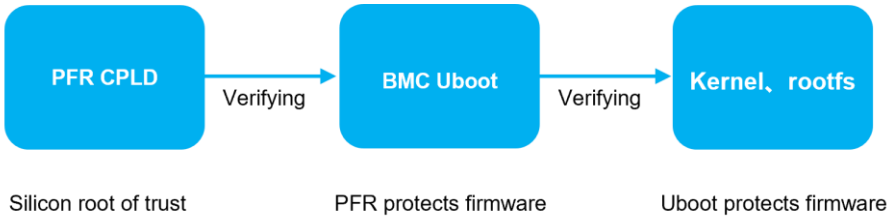
ることができる。

この機能は、主に認証、データの暗号化と復号化、およびその他のセキュリティアプリケーションで使用され、AES、DES、3 DES、RC4、MD5、SHA1、SHA224、SHA256、HMAC-MD5、HMAC-SHA1、HMAC-SHA224、およびHMAC-SHA256アルゴリズムを実装します。

信頼のシリコンルート

Intel PFRは、ファームウェアの保護、検出、およびリカバリ機能を提供し、システムのセキュリティと信頼性を強化します。このメカニズムは、Intelプロセッサーおよびプラットフォームの PFR CPLDに信頼のルートを配置し、この信頼のシリコンルートを使用してHDM-Ubootを検証およびリカバリします。次に、HDM-UbootはHDMファームウェアをさらに検証およびリカバリして、システム全体のセキュリティと信頼性を実現します。このメカニズムは、図117に示すように説明されています。

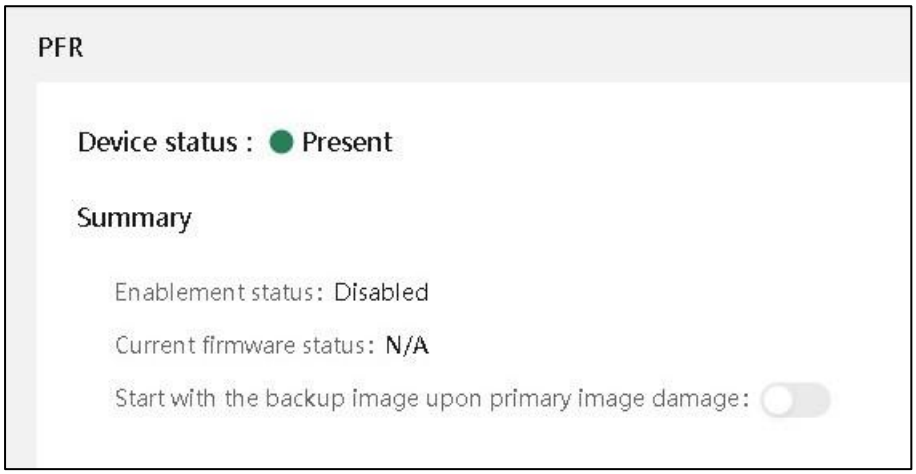
図117 シリコンルートオブトラストの仕組み



PFRファームウェア保護機能をイネーブルにすると、HDMの起動時にPFRによってファームウェアイメージファイルが確認されます。

- プライマリイメージが検証に合格すると、HDMはプライマリイメージから直接起動します。
- 検証に失敗した場合のバックアップイメージからの起動を有効にした後、HDMがプライマリイメージでファームウェアの損傷を検出した場合、HDMはバックアップ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すると、HDMはバックアップイメージから起動します。
- プライマリイメージとバックアップイメージの両方で破損が検出され、プライマリイメージの破損が通常の起動に影響しない場合でも、HDMはプライマリイメージから起動します。
- プライマリイメージが破損していることが検出され、通常の起動に影響があり、検証失敗時のバックアップイメージからの起動が無効になっている場合、HDMは起動できません。

図118 PFRファームウェアの保護



ファームウェアのセキュリティ

ファームウェア起動時のセキュリティ

1. デュアルイメージバックアップ

   HDMイメージが保存されているフラッシュ領域などの重要なファームウェアの場合は、デュアルイメージ設定が使用されます。操作中にフラッシュの誤操作またはストレージブロックの損傷が発生した場合、HDMはバックアップイメージに切り替えることができます。

2. 異常なファームウェアの復旧

   クリティカルファームウェアの場合、HDMイメージとBIOSイメージの両方で異常なリカバリメカニズムがサポートされています。HDMは、プライマリイメージでの操作中に異常な再起動または不完全な起動が発生すると、アクティブにゴールデンイメージに切り替えてプライマリイメージをリストアし、その後元に戻します。HDMは、BIOSの起動タイムアウトまたは不完全な起動を検出すると、アクティブにBIOSファームウェアイメージをリストアし、BIOSを再度起動します。

ファームウェア更新のセキュリティ

1. ファームウェア署名の暗号化

   外部でリリースされたすべてのHDMおよびBIOSファームウェアバージョンには、署名メカニズムが付属しています。ファームウェアのパッケージ化中、ファームウェアはSHA256アルゴリズムを使用して要約され、RSA2048で暗号化されます。ファームウェアのアップグレード中は、署名の検証によって改ざんが防止され、署名要件を満たすファームウェアのみがデバイスにアップグレードできます。

2. 再起動時のアップグレードタスクのリストア

   HDMは、異常な再起動時のファームウェアアップグレードタスクの復元をサポートしています。このメカニズムにより、マシンの異常によってアップグレードプロセスが中断されることはありません。電源切断またはHDMの異常な再起動。HDMが再起動した後、再起動前に完了していなかったコンポーネントのアップグレードタスクの実行が続行されます。

セキュリティを実行するファームウェア

システムの動作中、イメージが存在する領域は書き込み保護されているため、書き込み操作を実行するには特別な方法が必要です。同時に、ホストが起動するたびにイメージファイルの整合性がチェックされ、必要に応じてリカバリが実行されます。

リンクのセキュリティ

HTTPSリンク

HDMは、HTTPS経由でアクセスできるWebベースのビジュアル管理インターフェイスを提供し、HDM経由でアクセスされるデータがスパイされないようにします。HDMは現在、TLSv1.0、TLSv1.1、およびTLSv1.2をサポートしています。サポートされているセキュリティアルゴリズムスイートには、次のものがあります。

- RSA_WITH_AES_128_CBC_SHA256
- RSA_WITH_AES_256_CBC_SHA256
- RSA_WITH_CAMELLIA_256_CBC_SHA
- RSA_WITH_AES_128_GCM_SHA256
- RSA_WITH_AES_256_GCM_SHA384

TLSv1.1以下のセキュリティリスクのため、HDMのHTTPSリンクはデフォルトでTLSv1.2セキュア伝送プロトコルを使用する。

仮想KVM

ユーザーが接続したサーバーの情報がリンク上に漏洩しないように、また対話プロセスの情報が監視されないようにするために、セキュアポートが有効になっているKVMリンクチャネルを介してデータが送信されるときにデータが暗号化されます。

同時に、H5 KVMモードでは、シングルポート認証機能がサポートされています。仮想KVMおよび仮想メディアに関連する機能は、Webサービスインターフェイスを介してエクスポートされます。これにより、オープンなWebインターフェイスを削減し、セキュリティリスクを最小限に抑えることができます。

仮想メディア

仮想メディアへの安全なアクセスを確保し、リンク上でデータが傍受されないようにするために、データは安全なポートを介して暗号化されて送信されます。

VNC

VNCクライアントとVNCサーバーの間でセッションが確立されると、リモートコンピュータのIPアドレス(IPv4/IPv6)およびVNCパスワードが必要になります。サーバーは16バイトのランダムコードをクライアントに送信し、クライアントはVNCパスワードをDES暗号化のキーとして使用してこのランダム文字列を暗号化し、検証のためにサーバーに送信します。進行中のアクセス中に、選択した接続タイプに基づいて、リンク内のデータを暗号化するかどうかを決定できます。

特定のバージョンでは、必要に応じて次のタイプのVNCセキュア接続を選択できます。

- SSHを介したVNC(データはSSHチャネルを介して送信されます)
- stunnelを介したVNC。(データはstunnelによって確立されたTLS/SSLチャネルを介して送信されます。)

SMTPアラート電子メール

TLS暗号化送信により、SMTP経由で送信されるアラート電子メールの機密性と整合性が確保される。

Syslogアラート

デバイスとsyslogサーバー間のトラフィックのセキュリティと信頼性を確保するために、データ送信時にTLS単方向認証とTLS双方向認証がサポートされます。これにより、syslog組織のネットワークまたはアプリケーションにログインするユーザーにセキュリティの追加レイヤーが提供され、ログインプロセスに従わないデバイス接続も認証できます。

SDSログ

SDSログのパッケージ化時に機密情報の漏洩を防ぐために、障害診断ログ、ブートログ、定期的に収集される統計情報(温度検知、電力など)、内部デバッグログなどのコンテンツに対して暗号化が実行されます。ログを表示するには、ライセンスとともにインストールされたSDSViewerが必要です。

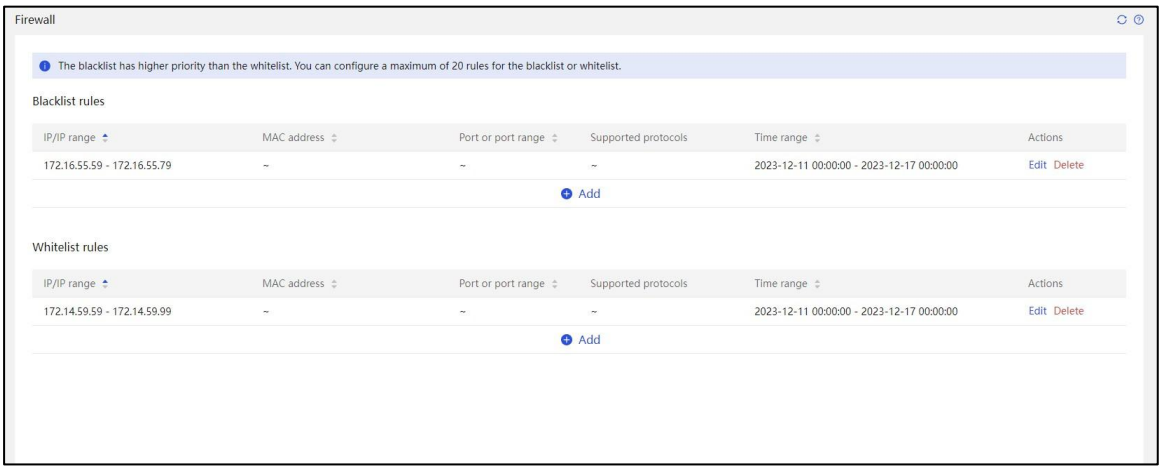
ファイアウォール

HDMは、シナリオベースのログイン管理を実現するファイアウォール機能を提供します。この機能は、Web、SSH、SNMP v1/v2c/v3、およびIPMI LANインターフェイスのログイン制御に適用できます。HDMは、時間、IPアドレスおよびIPプロトコルバージョン(IPv4/IPv6)、MAC、ポート、およびプロトコル(TCP/UDP)の5つの次元から最小範囲でサーバー管理インターフェイスアクセスを制御できます。ファイアウォールのdenylistおよびallowlistルールを設定することにより、HDMは特定のデバイスからのアクセスを許可します。

- denylistルールは、IPアドレス、IPアドレス範囲およびMACアドレスに関して、特定のデバイスからのアクセスを拒否します。denylistルールの有効期間を設定できます。denylistルールに一致しないデバイスはHDMにアクセスできます。HDMは最大20のdenylistルールをサポートします。
- 許可リストルールは、IPアドレス、IPアドレス範囲、MACアドレスおよびプロトコル(UDP/TCP)に関して、特定のデバイスからのアクセスを許可します。許可リストルールの有効期間を設定でき

ます。許可リストルールを構成した後は、許可リストルールに一致しないデバイスはHDMにアクセスできません。HDMは最大20の許可リストルールをサポートします。

図119 ファイアウォール情報



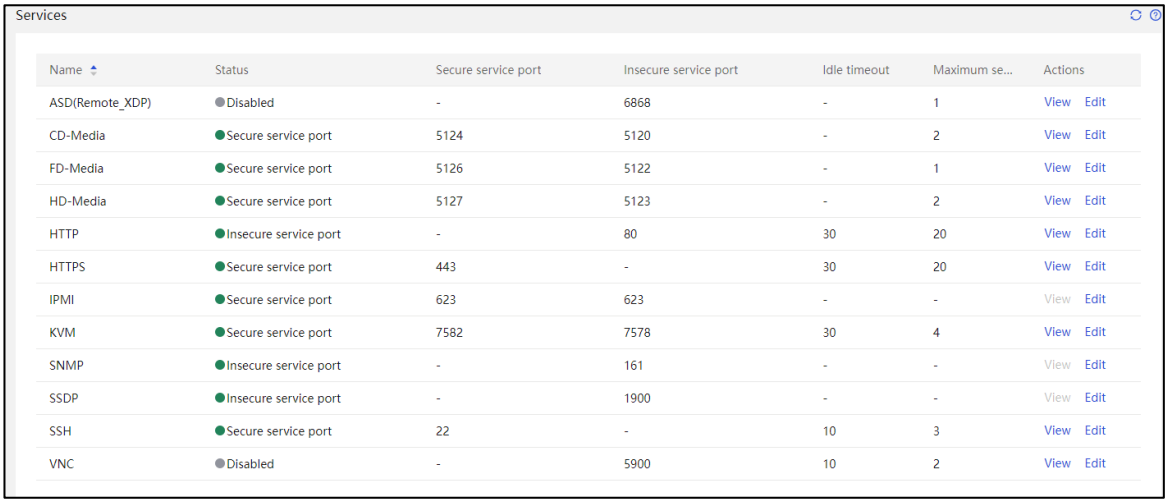
必要に応じて、ユーザーログイン許可リストを構成できます。ログインルールが一致すると、ログインが許可されます。ログインルールは、すべてのローカルユーザーおよびLDAPユーザーグループに適用されます。

denylistは、allowlistよりもプライオリティが高くなります。デバイスのIPアドレスがdenylistとallowlistの両方にある場合、アクセスは拒否されます。

サービス管理

顧客のサービスおよびセキュリティ要件を満たすために、HDMはサービスポートの可用性を制御するスイッチを提供します。表示および変更のためにHDMによってサポートされるサービスには、CD-Media、FD-Media、HD-Media、IPMI、KVM、SSDP、ASD(Remote_XDP)iHDT、SNMP、SSH、Telnet、VNCおよびWebがあります。

図120 HDMサービス情報

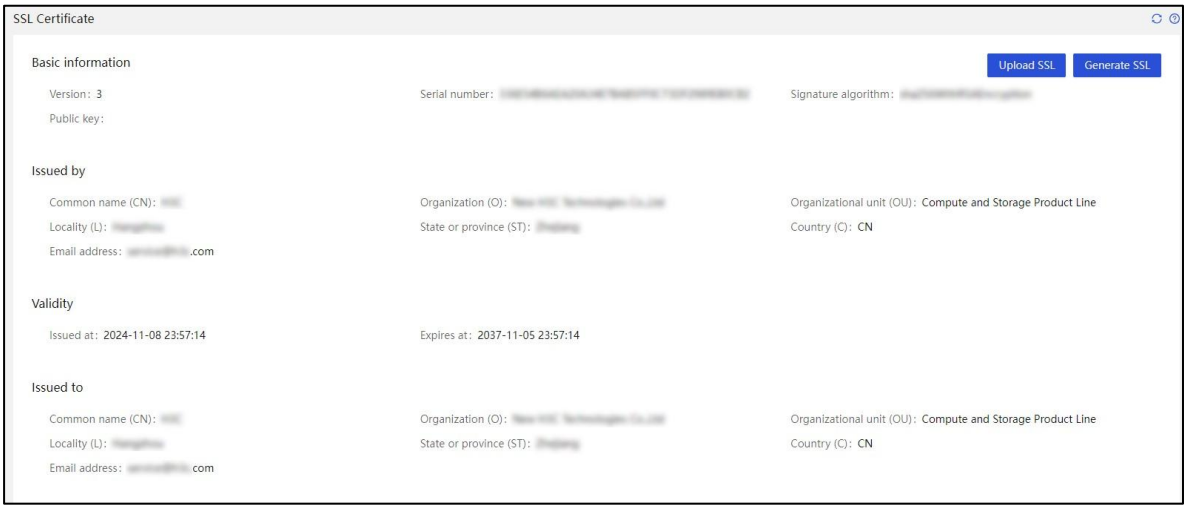


SSL証明書の管理

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、

プライベートデータをインターネット経由で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、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することによって、安全なデータ転送を行うことができます。

図121 SSL証明書情報



SSL証明書管理の場合、HDMは次の操作をサポートします。

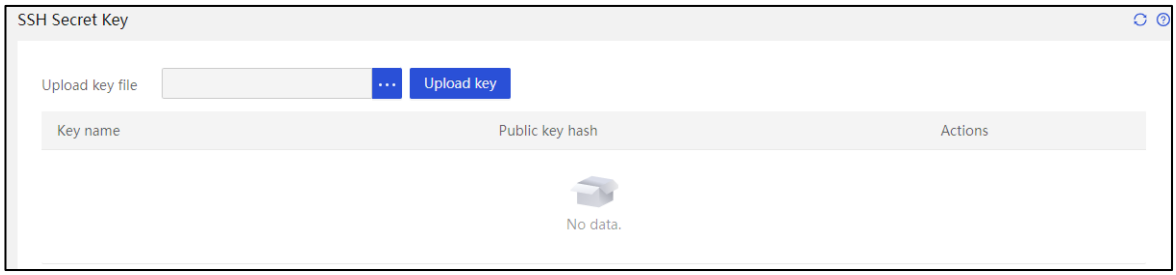
- ユーザー、発行者、有効期間、シリアル番号など、現在のSSL証明書に関する詳細情報を表示します。
- SSL証明書をアップロードします。
- SSL証明書を生成します。

HDMにはSSL証明書が付属しています。セキュリティを向上させるため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。

SSHキーペア

SSHパブリックキー認証は、自動化された構成ツールに適しています。SSHパブリックキー認証は、パスワードの入力を必要とせず、キーの長さが長いため推測が困難です。セキュリティを強化するには、SSHパブリックキー認証を有効にした後、SSHのパスワード認証を無効にします。

図122 SSHの秘密鍵



HDMは、SSHシークレットキーのアップロードと、HDMログインのためのローカルユーザーへのSSHシークレットキーのバインドをサポートしています。BMC CLIクライアントでのキー生成時にパスワードが指定されている場合は、アクセス試行時にキーのパスワードも入力する必要があります。パスワードが指定されていない場合は、BMC CLIに直接ログインできます。現在のソフトウェアバージョンでは、RSA、ECDSAおよびED25519キーがサポートされています。SSHキーの長さは、キーの形式によっ

て次のように異なります:

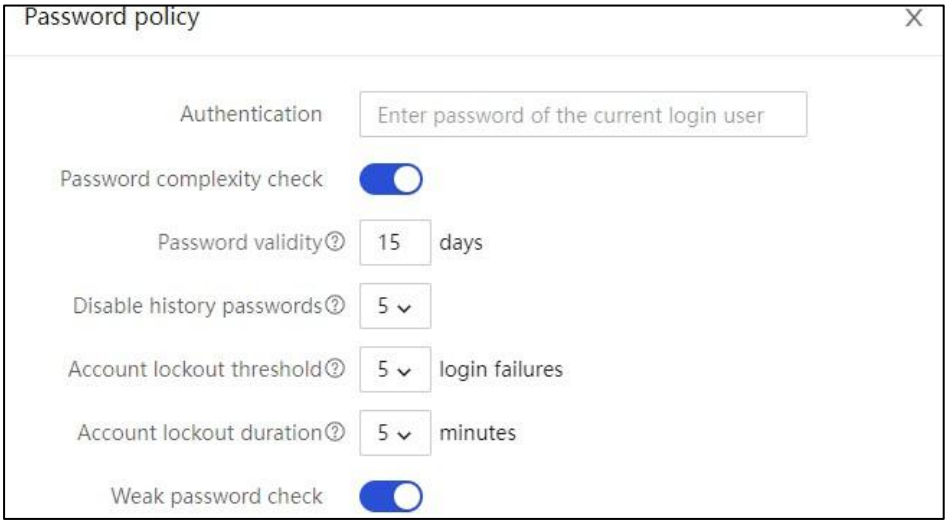
- RSA SSHキーの場合、長さは1024、2048、または4096バイトになります。
- ECDSA SSHキーの場合、長さは256、384、または521バイトになります。
- ED25519 SSHキーの場合、長さは256バイトのみです。

アカウントのセキュリティ

アカウントセキュリティには、パスワードの複雑度チェック、パスワードの最大有効性、履歴パスワードの無効化、アカウントロックアウトのしきい値、アカウントロックアウトの期間、および脆弱なパスワードのチェックが含まれます。**Users&Security > Users > Settings**ページにアクセスして、パスワードポリシーを設定します。

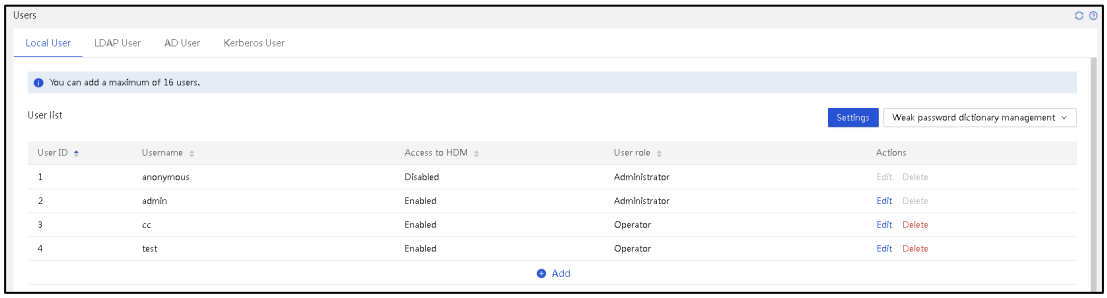
- **Complexity check**: この機能を有効にする場合、パスワードは次の複雑度要件を満たす必要があります。
  - 8～40文字。大文字と小文字が区別されます。有効な文字は、文字、数字、スペース、および次の特殊文字です:`~!@#$%^&*()_+-=\{};':",./<>?
  - 大文字、小文字、および数字のうち、少なくとも2つのカテゴリの文字を含める必要があります。
  - 少なくとも1つのスペースまたは特殊文字が含まれている必要があります。
  - ユーザー名と同一であったり、ユーザー名の逆であったりすることはできません。
  - password history countパラメーターで設定された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。パスワードの有効期限が近づくと、HDMはユーザーにパスワードの変更を要求します。
- **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**: ユーザーアカウントがロックされる原因となる連続ログイン失敗数。
- **Account lockout duration**: ロックされたアカウントを再度使用できるようになるまでの時間。
- **Weak password check**: 脆弱なパスワード辞書を使用して
  ユーザー構成パスワードは脆弱なパスワードです。この機能を有効にした後は、ユーザー構成パスワードを脆弱なパスワード辞書に含めることはできません。

図123 HDMパスワード設定インターフェイス



- **Weak password dictionary management**: なパスワードディクショナリをインポートおよびエクスポートできます。複雑度チェックと脆弱なパスワードチェックの両方が有効になっている場合、ユーザー構成のパスワードを脆弱なパスワードディクショナリに含めることはできません。

図124 弱いパスワード辞書の管理



権限管理

権限管理の要件は、顧客ごとに異なります。管理者、オペレータおよび共通ユーザーのロールをサポートするだけでなく、様々な機能の権限を定義する必要があります。HDMはユーザー指向の権限管理を提供し、IPMI、RedfishまたはWebを介してKVM、VMedia、Web、IPMIおよびSNMPなどの機能の権限を制御できます。

HDMは最大16人の異なるローカルユーザーをサポートします。ユーザー設定ページでローカルユーザーとドメインユーザー(LDAPおよびADユーザーを含む)を設定し、これらのユーザーがHDM Webインターフェイスにアクセスできるようにすることができます。

ユーザーが持つアクセス権限は、ユーザーが属するロールグループによって異なります。異なるロールグループには、その特性に一致する機能権限が割り当てられ、対応するHDM機能モジュールを操作できます。HDMでは、次のロールグループがサポートされています。

- **Administrator**: ユーザーは、HDMでの設定と制御のすべての権限を持っています。
- **Operator**: 管理者と比較して、ユーザー管理および保守診断を除くすべての設定および制御権限を持ち、特定の機能の日常の基本操作に関する設定権限を持ちます。
- **User**: 読み取り専用アクセス権があり、HDM構成を変更できません。
- **CustomRoleN**: 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。管理者は、カスタムユーザーが持つ権限を構成できます。

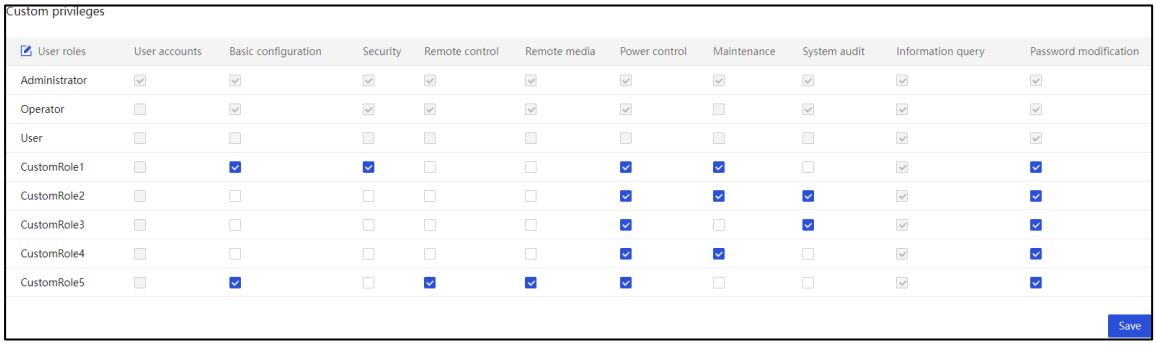
HDMは、インターフェイスのセキュリティを強化するために、すべての機能とインターフェイス(Redfish、IPMI)を異なる権限モジュールに分割します。権限モジュールには、ユーザー構成、一般構成、リモート制御、リモートメディア、セキュリティ構成、電源制御、保守と診断、自己構成および問合せモジュールが含まれます。表10に示すように、異なる権限モジュールには主な機能が含まれます。

表10特権モジュール設計関数の説明

特権モジュール名	特権モジュール機能の説明
ユーザーアカウント	ローカルユーザー、LDAPユーザー、ADユーザー、OTP認証、証明書認証、SSHキー、安全な消去の構成、構成のインポート/エクスポート、一元管理の実行
メンテナンス	イベントログのクリア、インストールパッケージの管理、ファームウェアの更新、ファームウェアライブラリの管理、スケジュールされたタスクの管理、HDM設定の復元、HDMの再起動、CPLDの再起動、およびサービスUSBデバイス設定の管理

リモートコンソール	ストレージ、ハードドライブのパーティション設定、システムリソースの監視、KVM(電源制御とイメージのマウントを除く)、VNCパスワード設定、システム起動項目、UID LED、SOL接続モード、MCA Policyおよびセキュリティパネルの管理
リモートメディア	KVMからのバーチャルメディア設定とメディアイメージのマウント
セキュリティ	サービス、ファイアウォール、SSL、ログインセキュリティ情報の構成
電源制御	電源、ファン設定、NMI制御、および物理電源ボタン制御の管理
基本構成	ネットワークポート、NTP、SNMP、LLDP、DNS、およびSyslogの設定、および資産タグの設定
パスワードの変更	現在のユーザーのパスワードを変更する
システム監査	イベントログ、操作ログの閲覧保存、SDSログのダウンロード管理
情報照会	すべての情報クエリメニューと機能

図125 ユーザー権限の設定ページ



Two-Factor認証

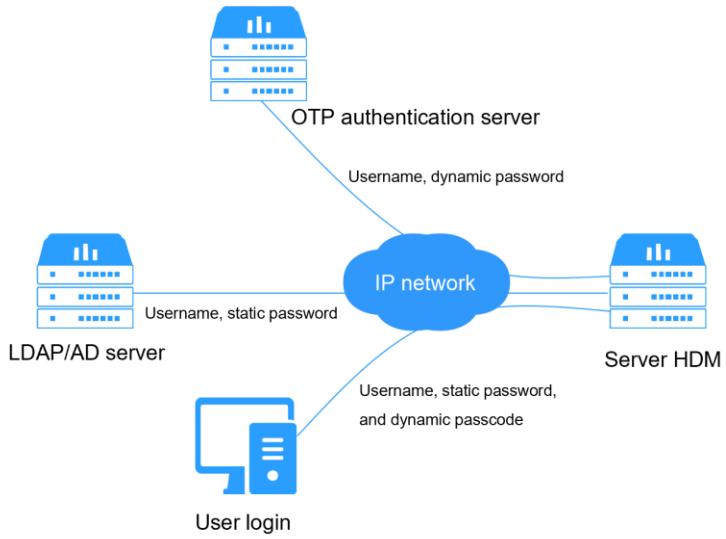
従来のプラットフォームログインでは、ユーザー名とパスワードのみが必要です。ユーザーパスワードはシステムに対する唯一の保護バリアであり、セキュリティ管理は比較的脆弱です。2要素認証では、ユーザー名とパスワードだけでなく、管理システムへのログインに別の要素も必要です。これにより、セキュリティに対するHDMの信頼性が向上し、ユーザー情報の漏洩が回避されます。

HDMは、証明書認証とOTP認証という2要素認証方式をサポートしています。両方を同時に有効にすることはできません。2要素認証を有効にすると、Telnet、SSH、VNC、IPMI、Redfish、SNMPv3、SOLなどのインターフェイスまたはサービスが無効になるため、2要素認証を有効にする場合は注意が必要です。

OTP認証

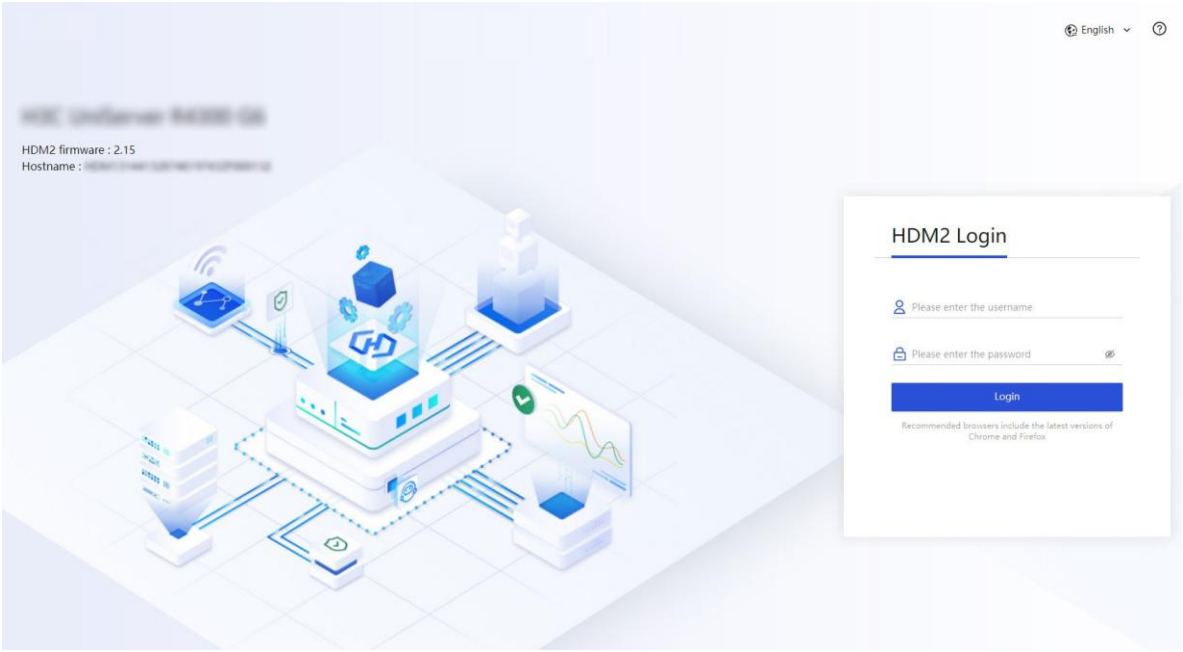
HDMは、ワンタイムパスワード(OTP)認証とRADIUSを使用します。OTPでは、強化されたネットワークセキュリティを提供するために、ログイン試行ごとに固定パスワードと動的パスワードが必要です。HDMはDKEYトークンをサポートし、OTPサーバーと連携してユーザーログインの二要素認証を提供できます。この機能が構成されている場合、ユーザーは、図126に示すように、HDMにログインするためにモバイル電話またはハードウェアトークンから取得した正しいユーザー名、固定パスワードおよび動的パスワードを入力する必要があります。

図126 OTP二要素認証ネットワーク図



二要素認証を有効にすると、図127に示すように、HDMのログインページに追加の動的パスワード入力フィールドが表示されます。

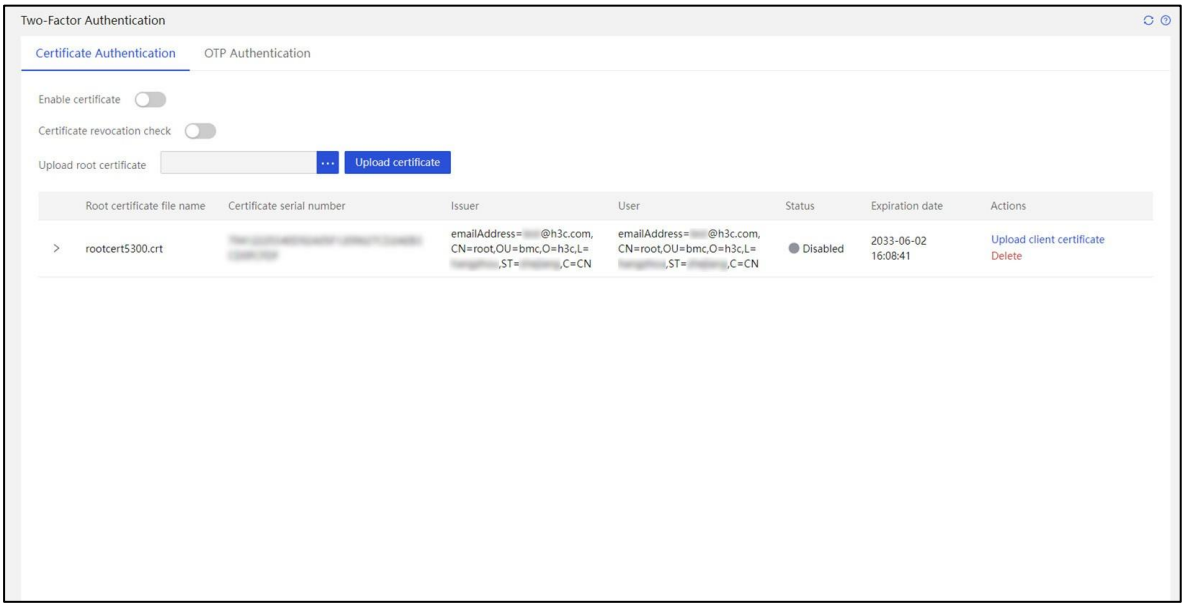
図127 Two-Factor認証を有効にしたログインページ



証明書の認証

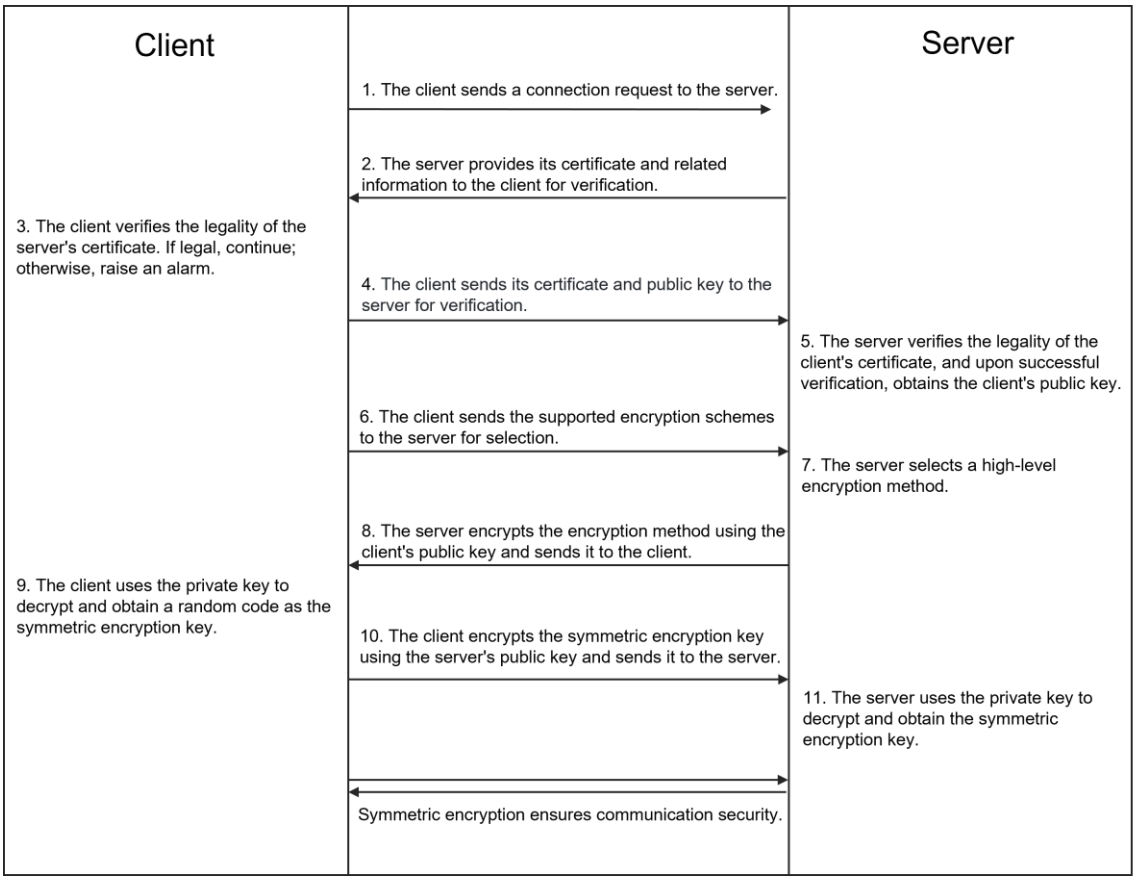
セキュリティに対するHDMの信頼性を向上させ、ユーザー情報の漏洩を回避するために、HDMは、ログインごとにクライアント証明書とクライアントプライベートキーを必要とする証明書認証を提供する。

図128 証明書のTwo-Factor認証



ルート証明書およびクライアント証明書ファイルを認証局に申請した後、証明書認証を使用してこれらをHDMにアップロードし、ローカルHDMユーザーを各クライアント証明書にバインドできます。バインドに成功した後、ブラウザを開き、クライアントのプライベートキー証明書をアップロードします。プライベートキー証明書がアップロードされると、HDMログインページに入り、プロンプトに従ってクライアント証明書を選択し、図129に示すように、クライアント証明書にバインドされたローカルユーザーとしてHDMにログインできます。

図129 証明書認証プロセス



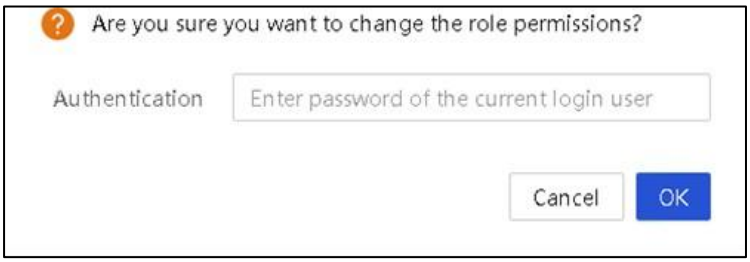
各ルート証明書に対して、最大20のルート証明書および16のクライアント証明書をアップロードできます。HDMは、アップロード用に最大20のクライアント証明書をサポートし、各クライアント証明書は1人のHDMローカルユーザーにのみバインドできます。Base64でコード化されたルート証明書および.cer、.crtまたは.pemの形式のクライアント証明書をアップロードする必要があります。ブラウザは、.p12形式のクライアント秘密鍵のみをサポートします。

証明書失効チェックを有効にする前に、Webサーバーとオンライン証明書ステータスプロトコル(OCSP)サーバーが相互にアクセスできることを確認してください。認証の失敗を回避するには、HDM Webインターフェイスにアクセスする権限を持つHDMローカルユーザーをバインドします。

セカンダリ認証

ユーザー構成、権限構成および公開鍵のインポートなどの重要な管理操作では、ログインしたユーザーに対して2次認証が実行されます。認証が渡された後にのみ、重要な操作を実行できます。これにより、ユーザーが接続を切断せずにログインしている間に、権限のないユーザーが悪意のある操作または偶発的な操作を実行するのを防止できます。

図130 セカンダリ認証ページ



LDAPドメインユーザー

Lightweight Directory Access Protocol(LDAP)を使用すると、IPネットワークを介して分散されたディレクトリ情報サービスに効率的にアクセスして管理できます。LDAPの既存の認証および認可モードを利用することで、ユーザー構成タスクの反復が回避され、管理効率が向上し、アクセス認証の集中管理が強化されるため、HDMのセキュリティが向上します。

LDAPでは、特定のロールに対応する権限を割り当てるロールベースのアクセス制御もサポートしています。すべてのユーザーに最高レベルの権限(管理者)を割り当てるのではなく、ロールベースのアクセス制御にロールグループを使用することをお薦めします。

HDMはまた、SSL暗号化の完全性を保証するためにLDAP証明書のインポートをサポートし、LDAPドメインユーザーのログインセキュリティを強化します(図132)。

図131 LDAPサーバーの動作メカニズム

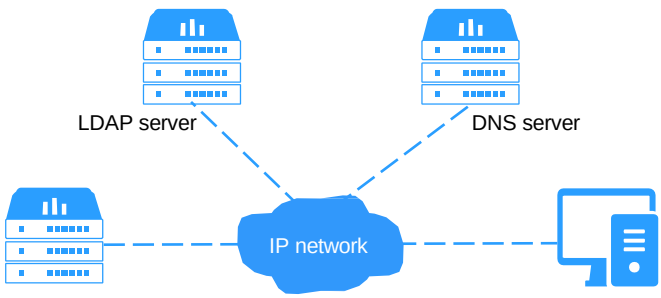
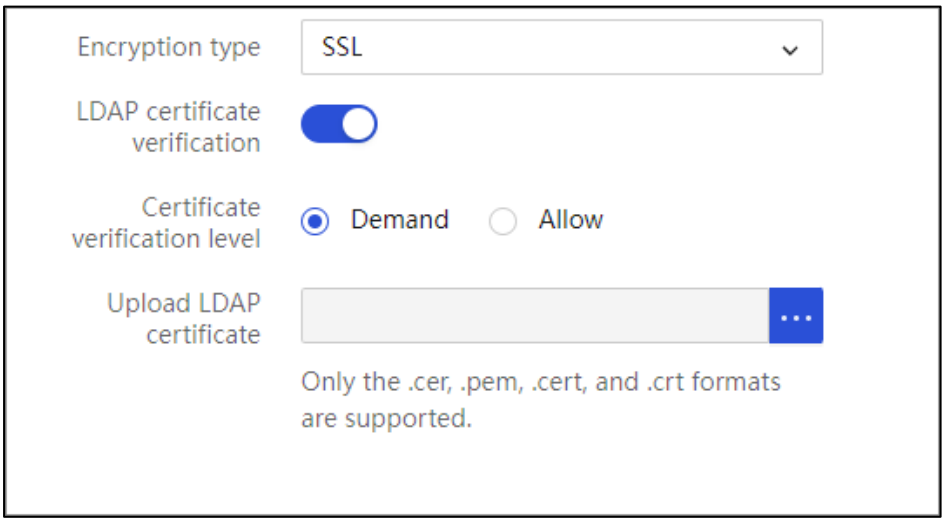


図132 LDAP証明書のインポート



LDAPのメリット:

- **Scalable**: アカウントはLDAPサーバー上で動的に管理でき、変更はすべてのHDMに反映されます。
- **Secure**: ユーザーパスワードポリシーがLDAPサーバーに実装されます。LDAPはSSLをサポートします。
- **Real-time**: LDAPサーバー上のアカウントの更新は、すべてのHDMに即座に適用されます。
- **Efficient**: すべてのHDMのユーザー管理、権限の割り当て、および有効期間の管理をディレクトリサーバーに集中させることができるため、ユーザー構成タスクの繰り返しを回避し、管理効率を向上させることができます。

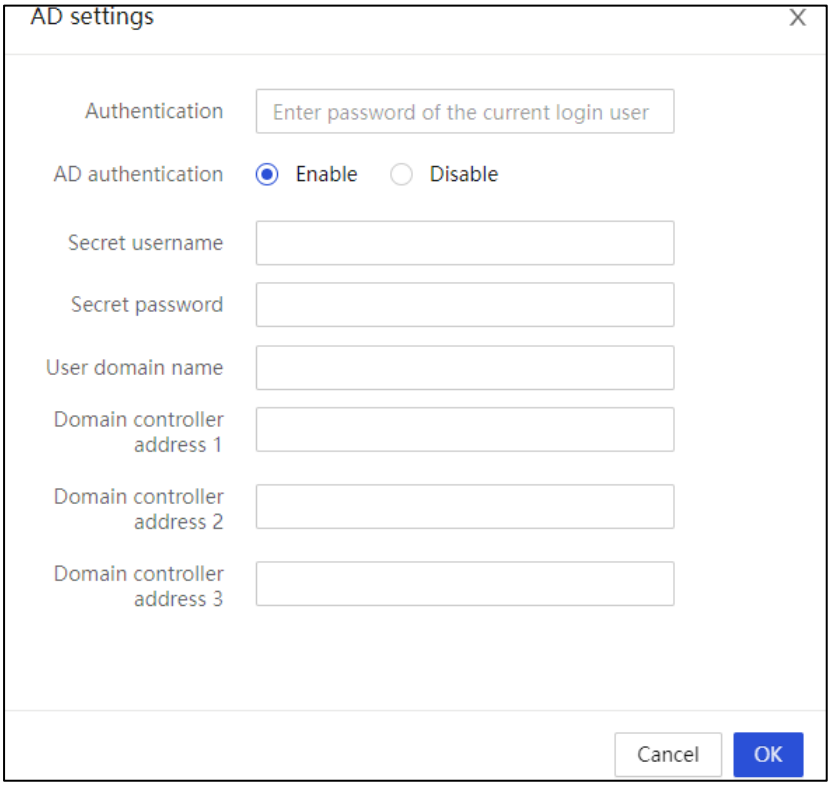
ADドメインユーザー

Active Directory(AD)は、Windowsサーバーオペレーティングシステムのディレクトリサービスを指します。一元化された組織管理とネットワークリソースへのアクセスを提供し、ネットワークトポロジーとプロトコルをユーザーに対して透過的にします。

ADは管理のためにドメインに分割されます。この構造により、会社の成長に合わせて拡張できます。

HDMはAD認証をサポートしています。図133に示すように、AD認証を有効にしてADグループを構成できます。構成が完了すると、ユーザーはADディレクトリサーバーで構成されたユーザー名とパスワードを使用してHDMに直接アクセスできます。

図133 ADサーバーの設定



Kerberos

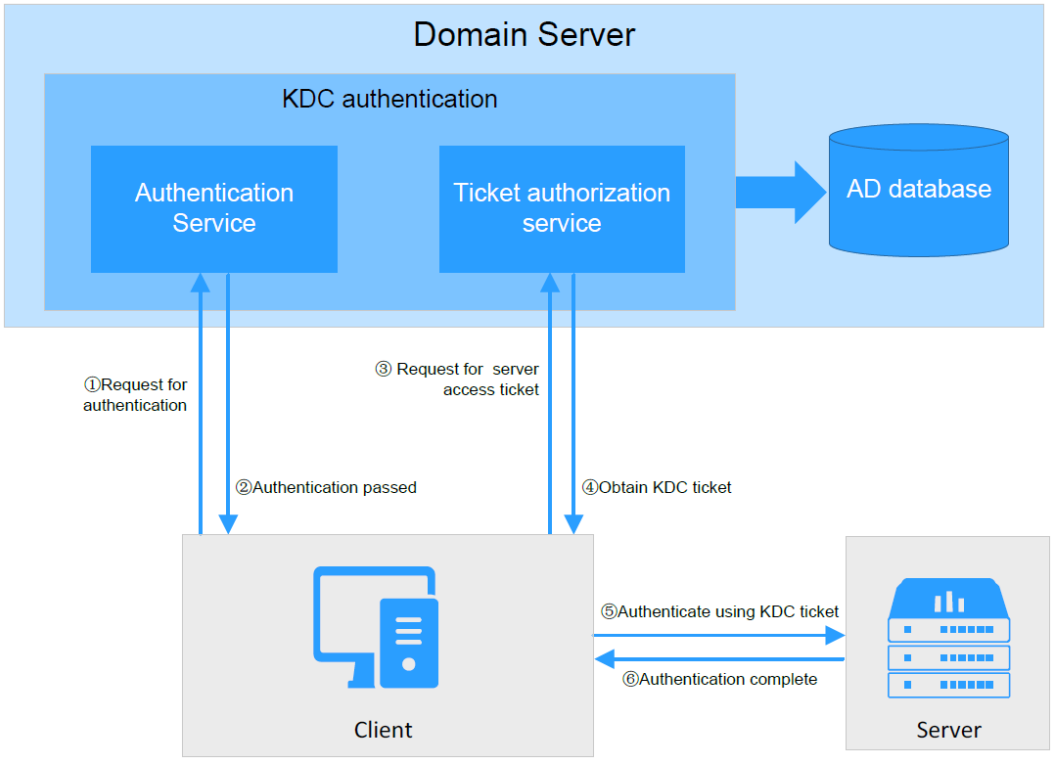
Kerberosは、厳密な本人確認サービスを提供するネットワーク認証プロトコルであり、通信者の本人確認の信頼性とセキュリティを保証します。このプロトコルの認証プロセスは、ホストオペレーティングシステムの認証に依存せず、ホストアドレスに基づく信頼を必要とせず、ネットワーク上のすべてのホストの物理的セキュリティを必要としません。ネットワーク上で送信されるデータパケットは、任意に読取り、変更および挿入できることを前提としています。Kerberosは、共有鍵などの従来の暗号技術を使用して認証サービスを実行します。

HDMのKerberos認証機能にはライセンスが必要です。Kerberosを有効にし、関連するパラメーターを構成すると、Kerberosディレクトリサーバーで構成されたユーザー名とパスワードを使用してHDMに直接アクセスできます。ドメインに参加したPCでKerberosを構成すると、ユーザー名やパスワードを入力しなくても、シングルノードログインを介してHDMに直接アクセスできます。HDMの権限は、ユーザーのロールグループの権限によって決定されます。

1. 認証管理の一元化

   KDCドメイン認証サービスを使用すると、ドメインサーバー上でユーザーポリシーを構成するだけで簡単に拡張できるため、一元管理が可能になります。データセンターデバイスは同じポリシーセットを共有し、認証ポリシーへの変更は内部ネットワークにすぐに反映されるため、管理が容易になります。

図134 Kerberos認証プロセス



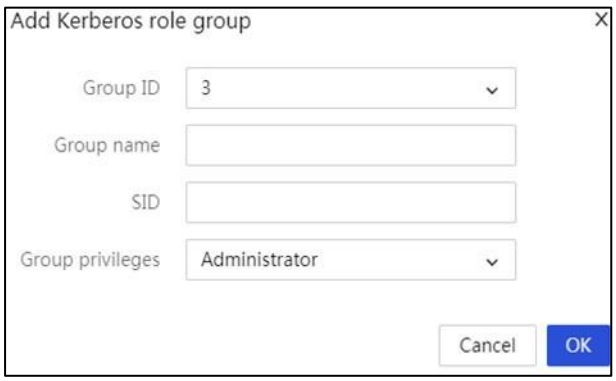
2. シングルサインオン

   HDMはKerberosを統合し、ユーザーがサーバーに一度ログインすると、パスワードを再度入力しなくてもネットワーク内のすべてのHDMにアクセスできるようにします。Kerberosベースのシングルサインオン機能により、認証中にキーがネットワークを介して転送されないことが保証されます。キーはセッションごとに生成され、セッションが終了すると無効になり、より安全になります。ユーザーがサービスにログインすると、Kerberosはチケット認可チケット(TGT)を生成し、サービスIDとTGTを認証センターに自動的に送信してキーを取得します。次に、このキーを使用して、サーバーにログインするためのユーザーのアカウント情報を暗号化します。これにより、パスワードを入力する必要がなくなり、操作がより便利になります。これは、数千のサーバーが異なるリージョンに配置され、複数のサーバー間で頻繁に切り替える必要がある場合に特に便利です。

3. ユーザーグループ管理

   異なる権限を持つ最大5つのユーザーグループがサポートされています。Kerberos役割グループの権限は、SIDに基づいて割り当てられます。各グループには一意のSIDがあるため、Kerberos認証プロセスがより安全になります。

   図135 Kerberosロールグループの追加



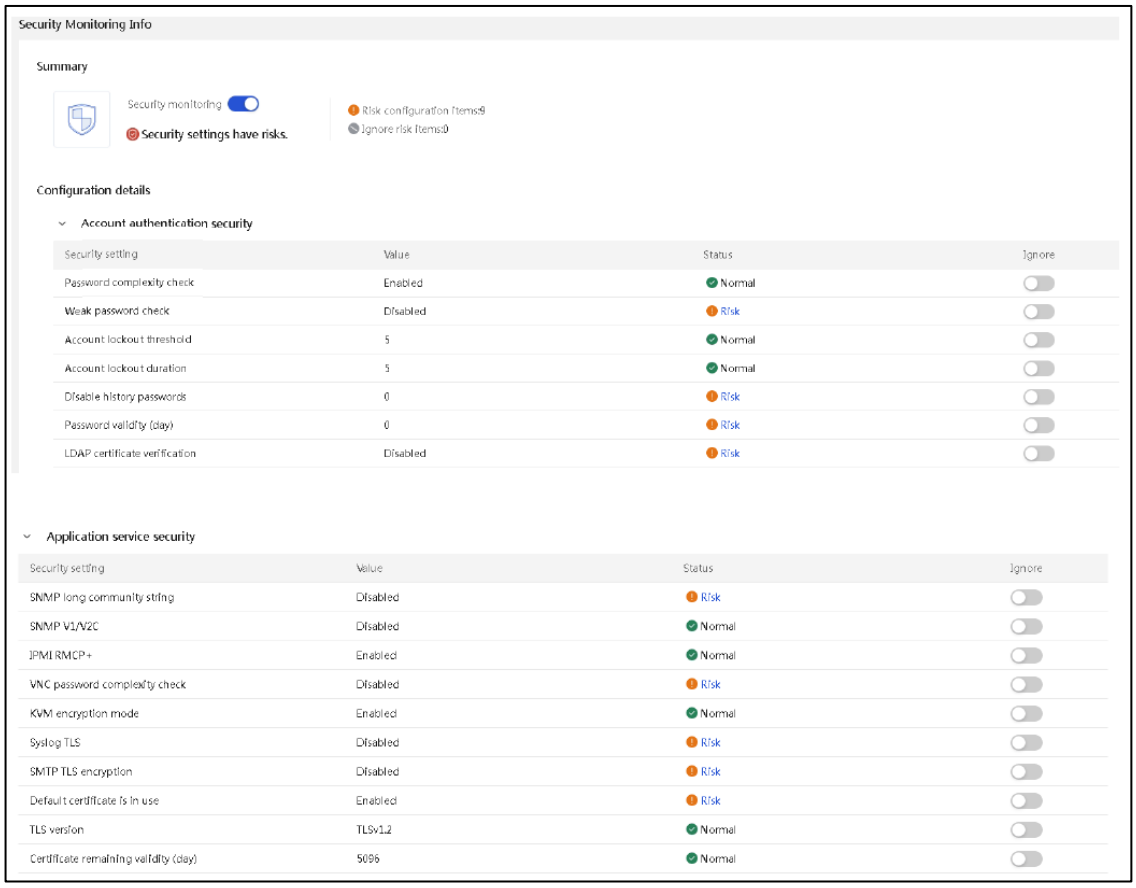
セキュリティ監視情報

セキュリティ監視情報を使用すると、重要なセキュリティ設定のステータスを表示し、HDM静的セキュリティ設定に潜在的なリスクが存在するかどうかを確認できます。リスクが検出された場合、この機能を使用して詳細と提案を表示できます。図136に示すように、HDMは、アカウント認証セキュリティとアプリケーションサービスセキュリティの側面から現在のシステムのセキュリティを包括的に評価し、対応するリスクレベルプロンプトを提供します。

現在のセキュリティ手段には、次の4つのリスクレベルがあります。

- セキュリティ設定にリスクはありません。
- セキュリティモニタリングはディセーブルです。
- リスクは、すべてのセキュリティ設定で無視されます。
- セキュリティ設定にはリスクが存在します。

図136 安全計器の情報表示



セキュリティ設定がリスクステータスにある場合、設定の警告を表示するには、ステータスのリスクをクリックします。
の場合よりも間隔が

図137 HDMセキュリティリスクステータス

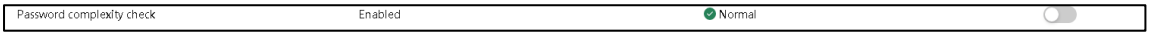
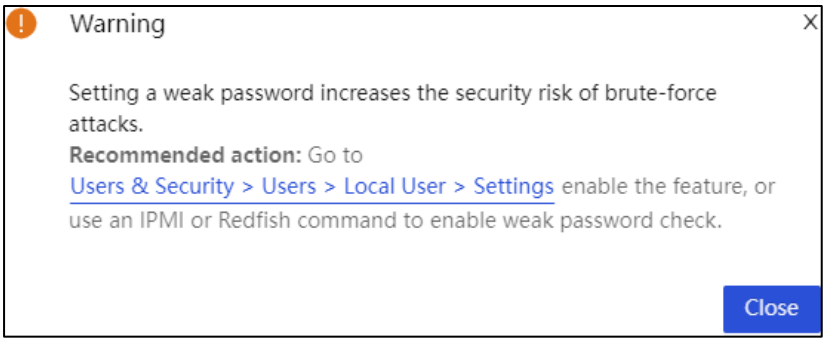


図138 HDMセキュリティリスクのヒント



安全なデータ消去

セキュア消去機能を使用すると、サーバーのHDM、BIOS、およびストレージデータを消去して、サーバーの使用期間が終了したとき、またはサーバーの操作が終了したときにデータが漏れるのを防ぐことができます。この機能にはライセンスが必要です。

図139 安全なデータ消去ページ

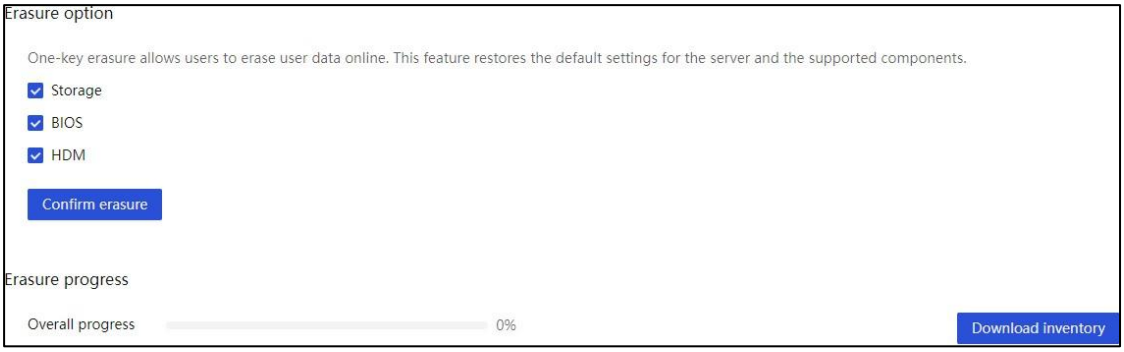


表11は、コンポーネントの消去結果を示しています。

表11 安全なデータ消去

項目	消去結果
ハードディスク	HDMを工場出荷時のデフォルトに戻します。SDSログとフラッシュカードデータは消去されます。
バイオス	• BIOSをデフォルト設定に戻します。 • BIOSの管理者パスワードとユーザーパスワードが消去されます。BIOSは、パスワードが消去されたユーザーが次の再起動時にBIOSセットアップユーティリティに入るためにパスワードを要求しません。 • サーバーの電源投入時パスワードがBIOSから消去されます。
不揮発性DRAM(NVDIMM)	メモリーモードになっていないNVDIMMのデータは消去されます。消去後、すべてのNVDIMMはメモリーモードで動作します。
ストレージコントローラー	RSTe RAIDコントローラーおよびVROCコントローラーによって管理されているすべての論理ドライブが削除されます。RAID-P460-B2ストレージコントローラーによって管理されているすべての論理ドライブが削除されます。
ドライブ	ドライブ内のすべてのデータが削除されます。

SDカード	SDカード内のデータがすべて削除されます。

確実に消去するには、サーバーがiFIST-1.38以降を使用していることを確認してください。

システムロック

システムロック機能は、特定のサーバー機能、構成およびファームウェアバージョンをロックして、誤った変更または悪意のある変更を回避します。この機能にはライセンスが必要です。図140に示すように、この機能は、電源制御、ハードウェア構成、BIOS構成、インバンドアクセスおよびアウトオブバンドアクセス、HDM構成およびファームウェアバージョンなどのロックオブジェクトを提供します。ロックオブジェクトの詳細は、表12を参照してください。

図140 システムロックページ

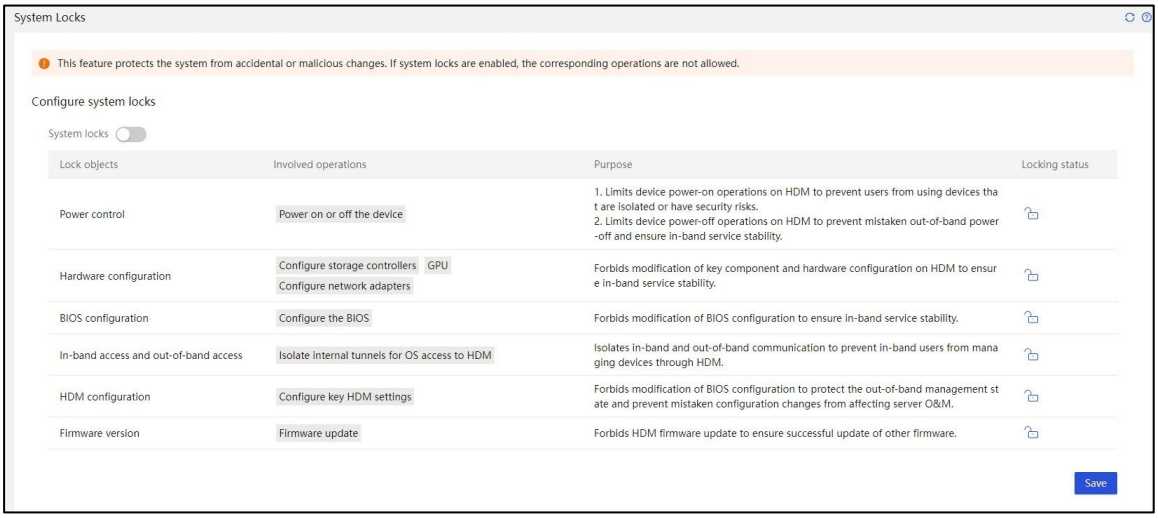


表12 システムロックオブジェクト

システムロックオブジェクト	説明
電源制御	HDMから、または物理的なボタンを押すことによって、システムのリセットを制御します。
ファームウェアのバージョン	HDMからのファームウェアバージョンの更新を制御します。
ハードウェア構成	ストレージコントローラー、GPU、およびネットワーク構成をHDMから制御します。オプションには次のものがあります。 • ストレージコントローラー、GPU、およびネットワークアダプターを設定します。 • RAID構成ファイルをインポートします。 • ストレージの安全な消去を実行します。
BIOS設定	HDMからBIOS設定を制御します。オプションには次のものがあります: • BIOS設定を構成します。 • BIOS設定ファイルをインポートします。 • ユーザー定義の設定を復元するか、強制的に復元してBIOSを更新します。 • BIOSの安全な消去を実行します。

システムロックオブジェクト	説明
HDM構成	HDM構成のリモート変更を制御します。次のオプションがあります: • ユーザー設定の構成(エクスポート構成と統合制御の実行を除く) • 一般的な設定(イベントログのクリアとビデオ再生を除く) • セキュリティ設定の構成(ログインセキュリティ情報の構成を除く) • 電源制御(サーバーの電源オン/オフおよびNMI制御を除く) • リモート制御(MCAポリシーの設定) • メンテナンス(HDMの工場出荷時のデフォルトを復元し、工場出荷時のデフォルトを復元してHDMを更新します)
インバンドアクセスとアウトオブバンドアクセス	OSがHDMにアクセスするための内部トンネルを分離し、HDMが独立した環境で動作できるようにします。

略語

頭字語	フルネーム
HDM	ハードウェアデバイス管理
BMC	ベースボード管理コントローラー
iFIST	統合されたFast Intelligent Scalable Toolkit
FIST SMS	Fast Intelligent Scalable Toolkitのシステム管理サービス
BIOS	基本入出力システム
MCTP	管理コンポーネント転送プロトコル
ME	管理エンジン
RAID	独立ディスクの冗長アレイ
RAS	信頼性、可用性、保守性
SEL	システムイベントログ
VGA	ビデオグラフィックスアレイ
IPMI	インテリジェントなプラットフォーム管理インターフェイス
SDS	スマート診断システム
EEPROM	電気的消去可能プログラマブル読み出し専用メモリー
SN	シリアル番号
PN	部品番号
SSD	ソリッドステートドライブ
LLDP	リンク層検出プロトコル
SSDP	Simple Service Discovery Protocol(簡易サービス検出プロトコル)
PCIe	Peripheral Component Interconnect Express(周辺機器相互接続)
SHD	スマートハードウェア診断
ADDC	自律的なデバッグデータ収集
APML	Advanced Platform Management link