

H3C サーバー管理プラットフォーム概要v1.2



01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

サーバー関連日本語ドキュメント

☐ ハードウェア

H3Cサーバーオペレーティングシステムインストレーションガイド

H3C サーバー ストレージコントローラ ユーザーガイド

H3C サーバー ファームウェアアップグレードガイド

H3C サーバー トラブルシューティングガイド

※上記ドキュメント中のFISTは現在Unisystemと名称変更されています

☐ HDM

H3C HDM ユーザーガイドV1.0

H3C HDM syslogメッセージ

H3C HDM2 テクノロジーホワイトペーパー

注意：サーバー関連のドキュメントは更新が速いので、バージョンアップなどされる場合には最新の英語版を参照してください。

☐ iFIST

H3C サーバー iFISTユーザーガイド

☐ UniSystem

H3C サーバー UniSystemユーザーガイド

☐ U-Center

H3C U-Center 5.0 User Guide（英文）

H3C UniServer ポートフォリオ

UniServer 製品情報ページ

Intel Server(青字)

AMD Server(黒字)

H3C The Leader in Digital Solutions

	サイズ(高さ) 1U	2U	4U
プロセッサー数 1P	 R3750 G7(1U1P) 省スペース設計	 R3950 G6/G7(2U1P) R3900 G7(2U1P) ※R3900 G7 AP：リリース済み	
2P	 R4700 G6/G7(1U2P) ※R4700 G7 SP：リリース済み	 R4900 G6/G7(2U2P) R4900 G6 Ultra(2U2P) ※R4900 G7 SP：リリース済み ※R4900 G7 AP：26Q2 リリース予定  R4950 G6/G7(2U2P)	 R4300 G6/G7(4U2P) ※R4300 G7 SP：リリース済み  R4500 G6(4U2P)
4P			 R6900 G6/G7(4U4P) ※R6900 G7 SP：26Q2 リリース予定

LinSeer Server

リンサー・サーバー
企業向けのAI開発・大規模モデルの学習・推論などを行うプラットフォーム



LinSeer Cube DR4000



NVIDIA

ミニPC
LinSeer MegaCube

H3C UniServer R4900 G6 (2U2P)



R4900 G6

計算能力

- 2Uサイズに第4/第5世代インテル® Xeon® スケーラブル・プロセッサーを2基搭載可能(**1プロセッサーあたり、最大 64コア**、最大 TDP 385W)
- 前の世代と比べて CPU コア数が 60% 増加し、汎用計算性能が 87%向上
- クラウドワークロード性能を最適化し、前の世代と比べて性能が最大 79% 向上

I/O 最適化

- 8チャネルの 5,600MT/s DDR5 メモリにより、メモリ帯域幅が 75%向上
- 新しい Full-OCP アーキテクチャにより、ホットスワップ可能な 8つの OCP3.0 スロットをサポート
- 32個の U.2 / 8枚のリア E1.S 高速ストレージデバイスをサポート

マルチプロテクション

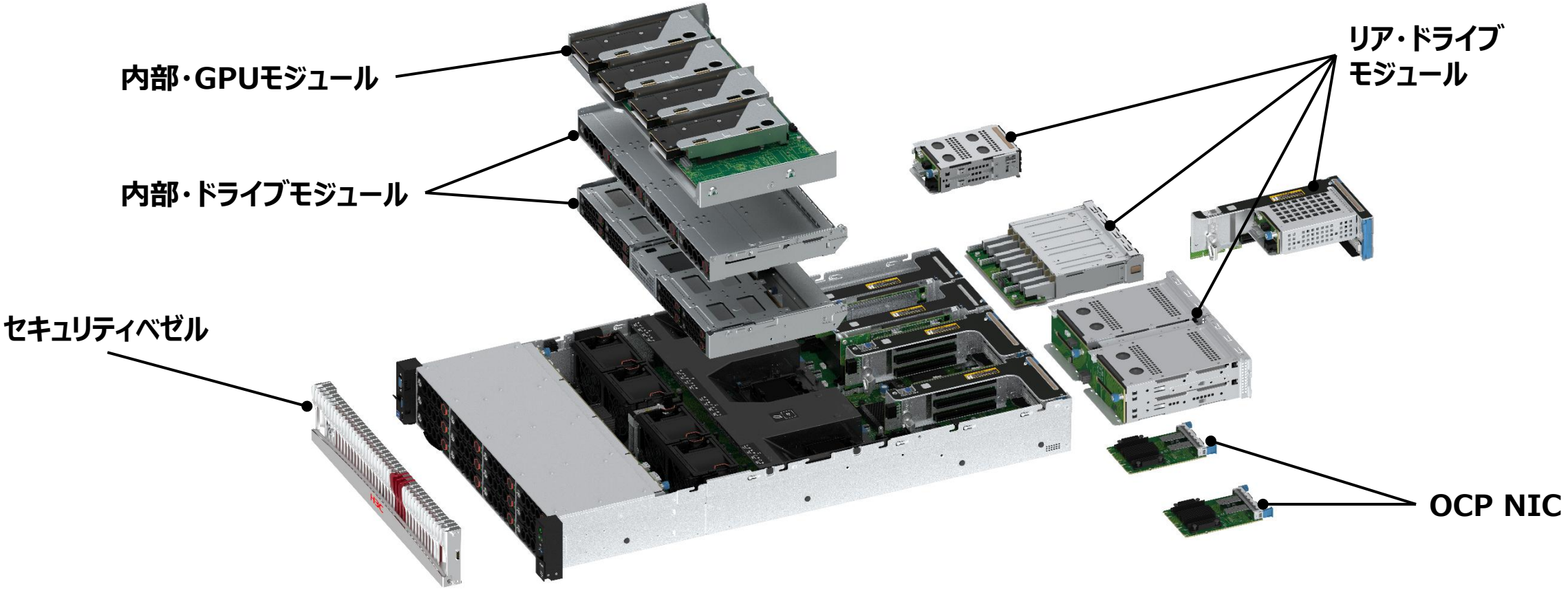
- インテル® ソフトウェア・ガード・エクステンションズ(SGX2.0)技術により、ビジネスデータを保護
- トラステッド・プラットフォーム・モジュール(TPM2.0)をサポート
- インテリジェントな故障診断と故障予測により、ビジネスの継続性をサポート

H3C UniServer R4900 G6 (2U2P)

CPU	**2 x Intel® Xeon® スケーラブル・プロセッサー**(第4世代 Sapphire Rapids または 第5世代 Emerald Rapids) 1プロセッサーあたり**最大 64コア**、最大 TDP 385W
メモリ	32 x DDR5 DDIMM メモリ、最大速度 5600MT/s、最大容量 **8TB**
ストレージ・コントローラ	標準オンボードコントローラ(SATA RAID 0/1/10/5対応) (オプション)専用スロットまたは標準 PCIeスロットベースの RAIDカードをサポート
ローカル・ストレージ	**最大20 x 3.5インチディスク**(フロント：12スロット、内部：4スロット、リア：4スロット) **最大45 x 2.5インチディスク**(フロント：25スロット、内部：10スロット、リア：10スロット) SATA/SAS ディスクをサポート、32 x NVMe U.2/8 x E1.S スロットをサポート (オプション)SATA/NVMe M.2 をサポート
ネットワーク	オンボードの 1 x 1GE 管理専用ポート **2 x OCP 3.0 NIC**(**4 x 1GE / 2 x 10GE / 2 x 25GE / 2 x 100GE**) PCIe 標準 NIC(1/10/25/100/200GE NIC、スマート NIC)
拡張スロット	**最大18 x PCIe 標準スロット**(11 x PCIe5.0 & 7 x PCIe4.0)、2 x OCP 3.0 スロット Full-OCP アーキテクチャー対応で最大8 x OCP3.0 スロット
GPU	**最大4 x デュアル幅 GPUカード** / 最大14 x シングル幅 GPUカード
電源	ホットスワップをサポート、1+1 冗長電源をサポート 800/1300/1600/2000/2400/2700W のプラチナ/チタニウムのランクをサポート
動作温度	5℃ ～ 45℃ (構成によって動作温度が異なります)
寸法(高 x 幅 x 奥行)	2U 筐体 87.5 x 445.4 x 780mm(セキュリティベゼルを除く) 87.5 x 445.4 x 808mm(セキュリティベゼルを含む)

H3C UniServer R4900 G6 (2U2P)

サーバ展開図

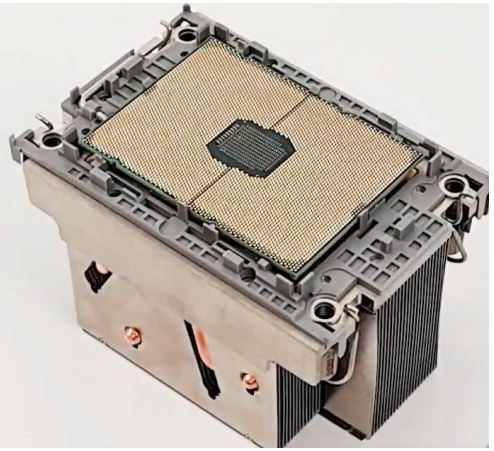


ハードウェア交換ビデオ

H3C UniServer R4900 G5 Hardware Options Installation and Replacement Videos-6W101



注意：このビデをはあくまでも参考としてみてください。ユーザーの方が自分でシャーシのパネルを開いてモジュールを抜き差しすることで障害が発生した場合、保証の対象外となります。



ヒートシンクとプロセッサー



01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

H3C サーバ管理ツール対応表

	H3C	DELL	Hewlett Packard Enterprise	Lenovo
統合オペレーション プラットフォーム	U-Center	-	-	-
複数サーバの ライフサイクル管理	UniSystem	OpenManage	OneView	LiCO (Lenovo Intelligent Computing Orchestration)
単体サーバの ライフサイクル管理	HDM (Hardware Device Management)	iDRAC (Integrated Dell Remote Access Controller)	iLO (Integrated Lights-Out)	XCC (Lenovo XClarity Controller)



H3C サーバ管理ツール

ネットワーク、サーバ、ストレージなどの
統合オペレーションプラットフォーム
(ネットワーク全体を統括管理、各種アップグレード、ステータス管理)



複数サーバのライフサイクル管理
(サーバクラスタの全体管理、各種アップグレード、ステータス管理)



単体サーバのライフサイクル管理
(単体サーバの管理、各種アップグレード、ステータス管理)



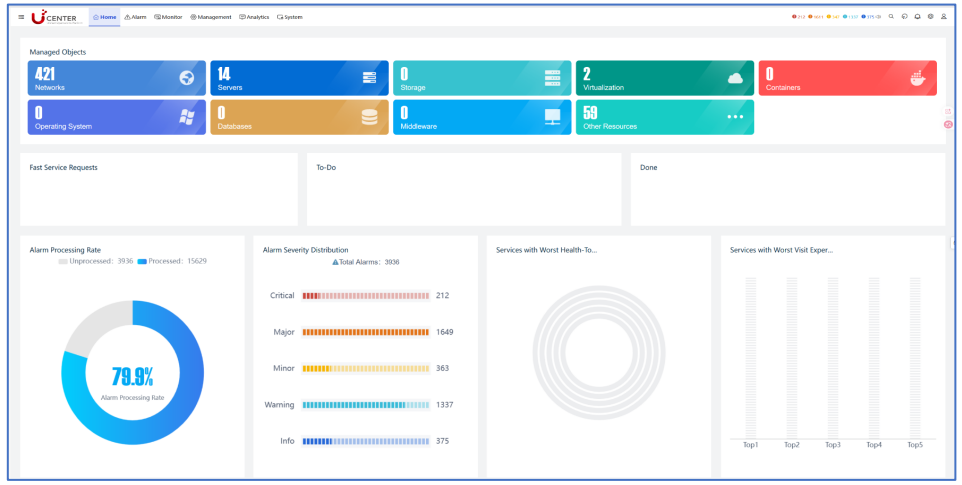
U-Center

UniSystem

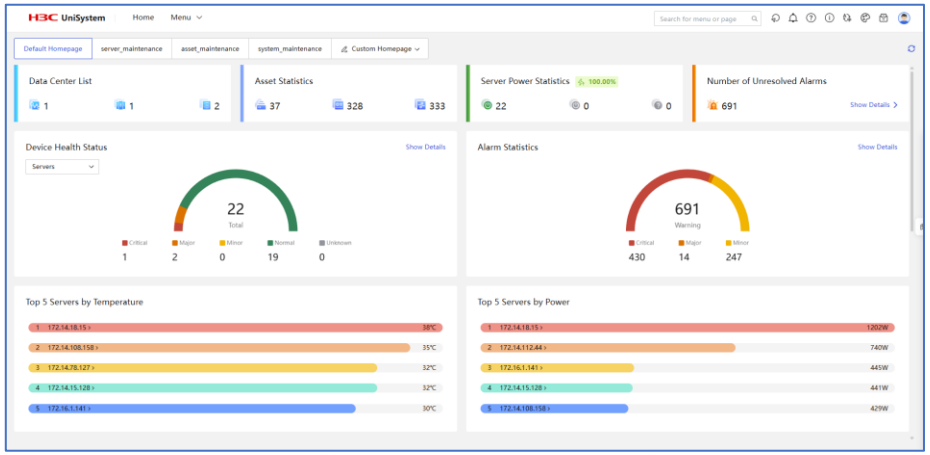
HDM

H3C サーバ管理ツール

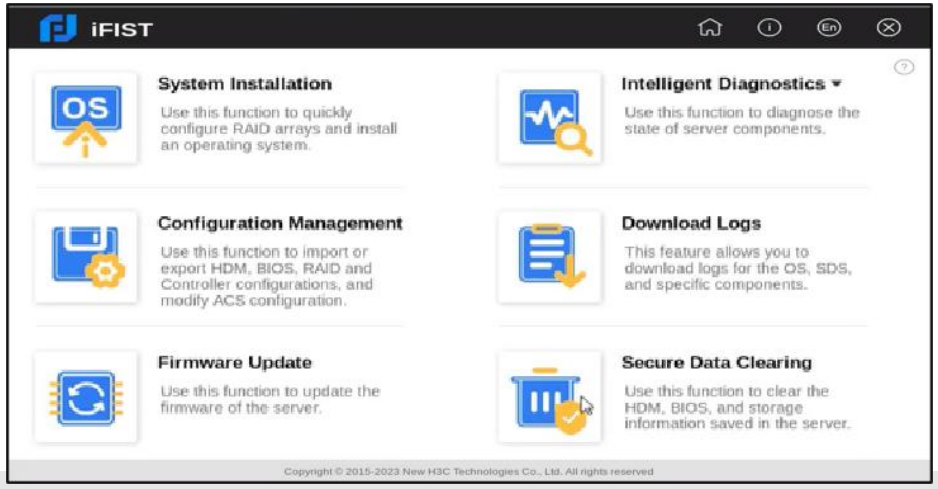
U-Center(ネットワーク全体を管理)



Unisystem(複数のハードウェア管理)



iFIST(構成管理や診断)



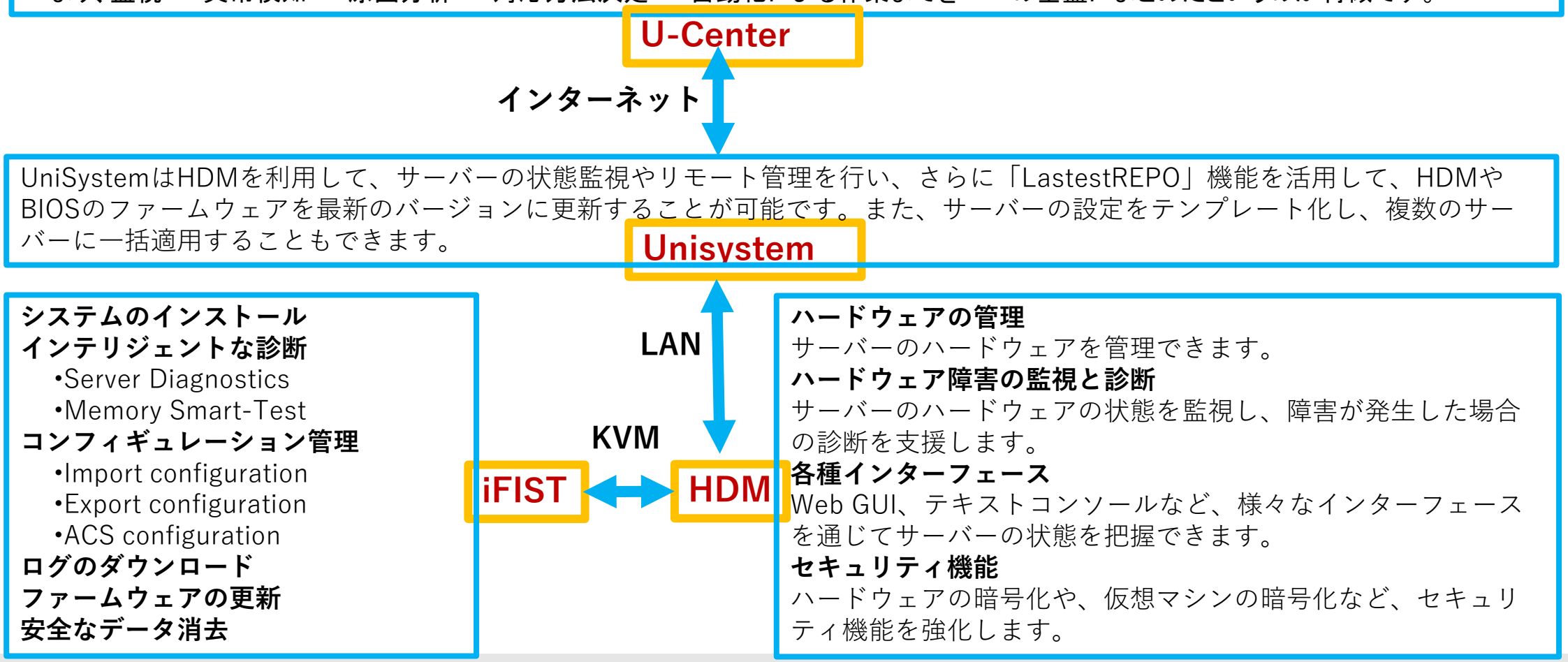
KVM

HDM(単体のハードウェア管理)

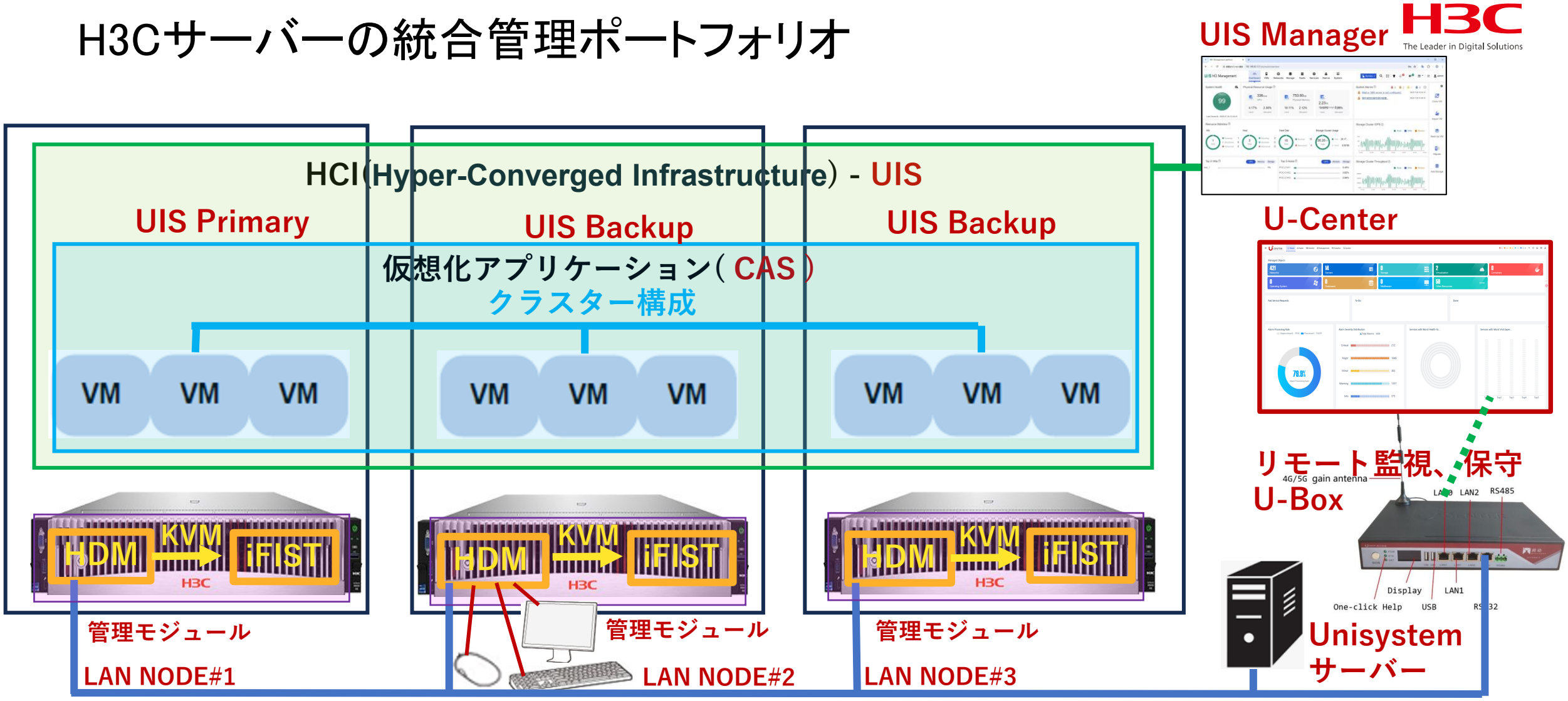


U-Center、Unisystem、HDM、iFISTの役割分担

ネットワーク機器だけでなく、**サーバー・ITリソース・サービスなどをまとめて監視・管理・運用自動化をする統合運用プラットフォーム**です。
U-Centerは単なる「監視画面」ではなくAIGC（生成AI）を活用したインテリジェント運用が可能です。
また、AOM(自動化・運用作業)ではOne Agentによる自動化作業を行います。
つまり、監視 → 異常検知 → 原因分析 → 対応方法決定 → 自動化による作業までを一つの基盤にまとめたというのが特徴です。



H3Cサーバーの統合管理ポートフォリオ



HDMはHardware Device Managementの略でハードウェア管理(ハードウエア+ファームウェア)
iFISTはintegrated Fast Intelligent Scalable Toolkitの略で構成管理や診断(ハードウエア+ファームウェア)

OSのインストール方法

アプリケーションシナリオ	OSのインストール方法	機能
単一サーバーへのOSのインストール	BIOSを使用したOSのインストール	最も一般的なOSインストール方法。各インストールフェーズを監視し、設定をカスタマイズできます。
	iFIST経由でのOSおよびドライバーのインストール	OSのインストールをシンプル化し、時間を節約します。
複数のサーバーへのOSの一括インストール	Unisystemを使用したOSおよびドライバーのインストール	大規模なネットワークにOSを一括インストールします。

ファームウェアのアップデート方法

Update 方式	アプリケーションのシナリオ	適用可能なファームウェア	備考
HDM2	1台のサーバーでのファームウェアの更新	HDM、BIOS、CPLD1、CPLD2、BPCPLD、BPPSoC、PFRCPLD、BMCCPLD、SWCPLD、TORSWCPLD、DBCPLD、FANCPLD、PDBCPLD、UBBKLCPLD、GPUCPLD、UBBMUXICPLD、UBBMUXISCPLD、PSU、GPUモジュールファームウェア、リタイマーファームウェア、ストレージコントローラーファームウェア、ネットワークアダプターファームウェア、およびドライブファームウェア	強制的な構成のリストア、工場出荷時設定復元、またはユーザー設定保持によるHDMおよびBIOSのアップデートをサポートします。
Unisystem	1台または複数台のサーバーで一括してファームウェアを更新	HDM、BIOS、CPLD、DBCPLD、STBCPLD、PDBCPLD、NDCPLD、AUXCPLD、PFRCPLD、ストレージコントローラファームウェア、ネットワークアダプタファームウェア、およびドライブファームウェア	ユーザーが構成した設定が保持されている場合のみ更新をサポート

H3Cサーバーファームウェアの名前と機能

CPLDはComplex Programmable Logic Deviceの略

ファームウェア名	説明説明
CPLD	サーバーのシステムボードのプライマリCPLDファームウェア。
• PFRCPLD • STBCPLD • AUXCPLD	サーバーのシステムボード用のセカンダリCPLDファームウェア。異なるタイプのCPLDファームウェアのサポートは、サーバーモデルによって異なります。詳細については、表4を参照してください。
DBCPLD	プロセッサーメザニンボード用のCPLDファームウェア。
PDBCPLD	PDBのプライマリCPLDファームウェア。
PDBSCPLD	PDB用のセカンダリCPLDファームウェア。
NDCPLD	コンピュートモジュールのCPLDファームウェア。
OCPCPLD	OCPネットワークアダプタ用のCLPDファームウェア。

OS / ファームウェア / ドライバーのリポジトリー(他社との比較)

H3C	HPE	Dell	Lenovo
REPO	**SPP**	**Repository/Catalog**	**UpdateXpress System Packs**
Server Firmware/Driverの Repository	Proliant向け Firmware/Driverをまとめたパッケージ	PowerEdge向け Firmware/Driverの更新パッケージ	ThinkSystem向け Firmware/Driver パッケージ



01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

エンタープライズ製品基本保証(Enterprise product Limited Warranties)

エンタープライズ製品基本保証

製品カテゴリー	詳細	保証タイプ	保証期間
ネットワーク製品	SOHO スイッチ (S1200/1850/S5000V3)	9×5×翌営業日発送 (スペアパーツ発送)	5 年
	ルーター		1年
	スイッチ		
	無線コントローラ		
セキュリティ製品	ファイアウォール		
ソフトウェア	ネットワーク製品 IMC/Director/ Controller/SMP Cloud製品 Cloud(CloudOS/CAS/ONEStor/UIS)	ソフトウェアメディア交換のみ	90 日

製品カテゴリー	詳細	保証タイプ	保証期間
エンタープライズサーバー	ラックサーバー	9×5×翌営業日発送 お客様自身での交換/返却	3 年
UIS Cell	UIS Cell 3000 G3/G5		

補足説明:

・基本保証は別途購入する必要はありません。

・詳細なサービス内容および他のH3Careサービスについては弊社HP「**エンタープライズ製品基本保証**」を参照してください。

・9x5(9時間: 9:00 – 18:00
5日:月曜から金曜日)

エンタープライズ製品基本保証(Enterprise product Limited Warranties)

付録: エンタープライズ製品CRU(顧客交換可能部品)ガイド

- CRU(Customer Replaceable Units)部品の交換:部品交換の必要がある場合、基本的には「**エンタープライズ製品顧客交換可能部品ガイド**」を参考し、H3Cテクニカルサポートセンターの指示に基づいて、**交換可能な部品をお客様独自にインストールまたは交換します、オンサイトサービスは提供しません。**
- CRU部品の詳細は右表に記載。
- H3Careに関する詳細は「**H3Care 保証サービスV2.1(H3Care Foundation Service)**」に準拠します。

✓ CRU部品の増減は「**エンタープライズ製品保証ポリシー V3.0**」に準拠します。

✓ Server&UIS Cell 製品に対するサービスレベルは5X9から7X24に変更。

- 「**エンタープライズ製品保証ポリシー V3.0**」は、2022年12月1日から有効になります。

製品カテゴリー	製品モデル	顧客交換可能部品(CRUs)	関連資料
ラックサーバー	R4300 G3	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6438972
	R6700 G3	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6439009
	R4900 G3/G5	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6439008
	R4700 G3/G5	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6438999
	R6900 G5	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6439010
UIS Cell	UIS-Cell3000	ディスクドライブ; 電源	https://download.h3c.com/download.do?id=6439008

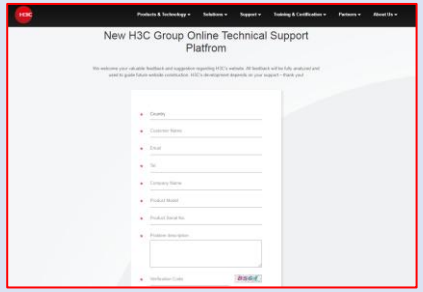
プロフェッショナルサービス – ICTインストール & 導入サービス

- 標準 ： 設置 & 導入サービス
- カスタマイズ: エンジニアリングオンサイトサポートサービス

カテゴリー	製品BOM	製品名	サービスの説明	サポート説明
設置 & 導入サービス	8814A0KV	SV-BC-EOS-OS	H3C Server 標準ハードウェアのインストールおよびスタートアップサービス - インターナショナル	• 導入準備 • キャビネットの設置 (有機的なキャビネット構成に適用) • オペレーティング システムのインストールと構成 • 製品ハードウェアの統合とラックへの設置 • 基本的な製品トレーニング
	8814A0R1	SV-BC-EOS-OS	高度なソフトウェア導入サービス	12500、16000機器の場合 • ソフトウェア導入技術ソリューションの構成 • ソフトウェアのデバッグと展開 • オンサイトトレーニング

テクニカル サポート チャネル概要

リモートテクニカルサポート







Web to Case(推奨)

- オンラインで問題特定
- 全製品に対応
- 7*24h サポート

サービスホットライン-H3C

- フリーダイヤル
- 日本語対応（営業時間内）
- 全製品に対応
- 7*24H サポート

Public Mailbox

- h3cts@h3c.com
  CC:&TS-INTL-JPN@h3c.com
- より詳細なフィードバックする際
- 7*24H サポート

セルフサポート



Webサイト(サポート – H3C)

- 製品情報
- 保証のお問い合わせ
- ライセンス関連
- マニュアル関連
- ソフトウェア関連

オンサイトサポート



オンサイトサポート（オプション）

・スペアパーツの交換
・デモンストレーション、実装、メンテナンス、トレーニングなど。

H3C サーバー トラブルシューティングガイド
H3C製品 障害情報収集クイックガイド(GUIを利用)



01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

H3C HDM(Hardware Device Management)概要

H3CのHDM（ハードウェアデバイス管理）は、H3Cサーバーのハードウェアを管理・監視するためのシステムで、通常BMCと呼ばれる範疇のものです。

キーボード、マウス、ビデオのリダイレクト、テキストコンソールのリダイレクト、リモートバーチャルメディア、ハードウェア監視など、様々な機能を提供します。

HDMは、H3Cサーバーのライフサイクル全体にわたって、ハードウェアの監視、管理、セキュリティ制御を行うことができます。また、IPMI、SNMP、Redfishなどの業界標準にも準拠しています

ハードウェアの管理:
サーバーのハードウェアを管理できます。

ハードウェア障害の監視と診断:
サーバーのハードウェアの状態を監視し、障害が発生した場合の診断を支援します。

各種インターフェース:
Web GUI、テキストコンソールなど、様々なインターフェースを通じてサーバーの状態を把握できます。

セキュリティ機能:
ハードウェアの暗号化や、仮想マシンの暗号化など、セキュリティ機能を強化します

HDMの初期設定

- 管理用のHDMのIPアドレス/デフォルトゲートウェイ/DNSサーバの設定
  - デフォルトは192.168.1.2/24　GW: 192.168.1.1/24

- NTPの設定
  - プライマリーとセカンダリーのNTPサーバーのIPアドレスを設定

- SNMPの設定
  - SNMPマネージャーのIPアドレスの設定
  - SNMPのコミュニティ名の設定
  - SNMP Trapするエラーレベルの設定

- Syslogの設定
  - syslogサーバーのIPアドレスの設定
  - trapするエラーレベルの設定

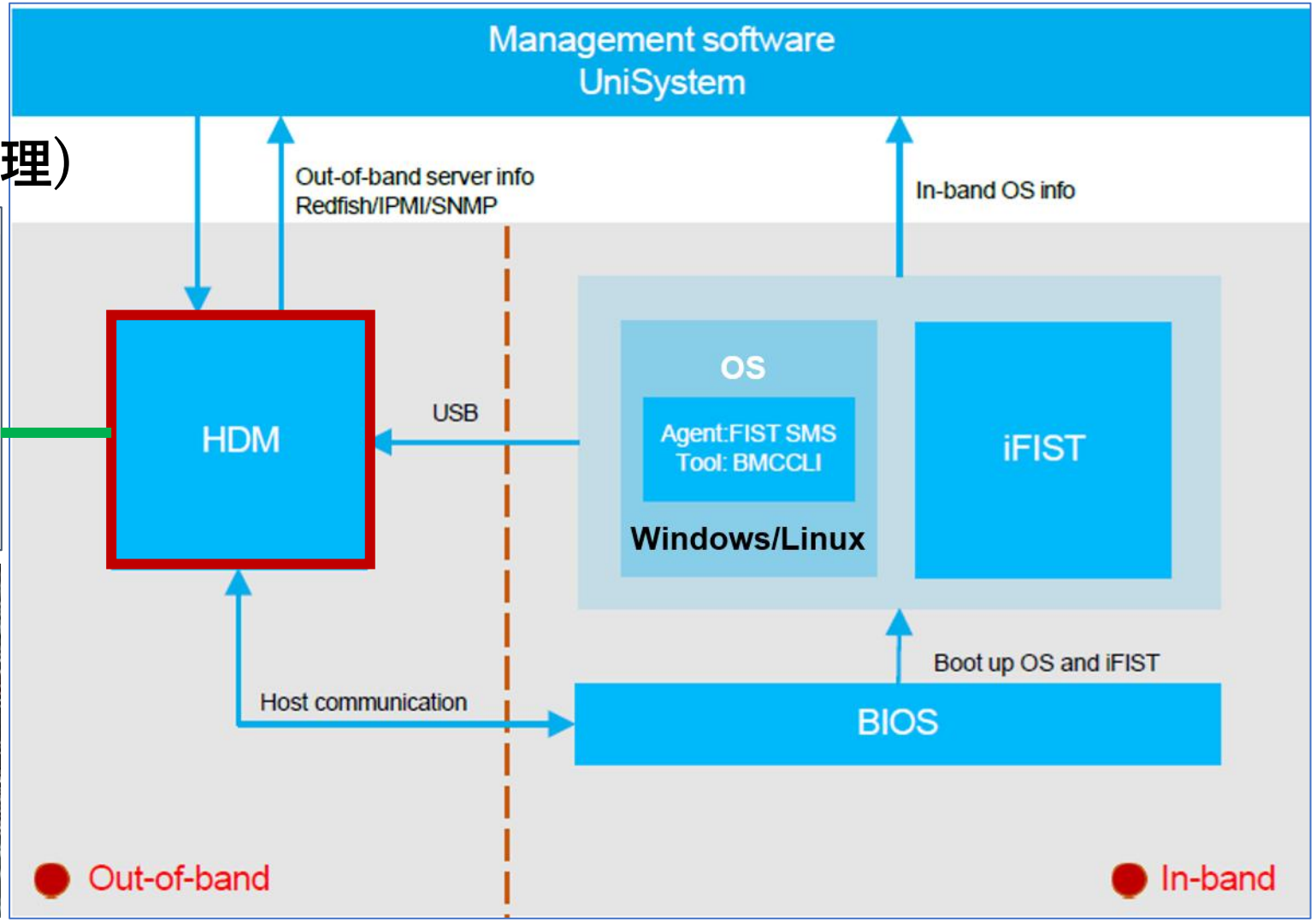
- SMTPの設定(障害のメール通知)
  - SMTPサーバーのIPアドレス
  - SMTPのポート番号
  - 送信するエラーレベルの設定

HDMのアーキテクチャー

HDM(単体のハードウェア管理)







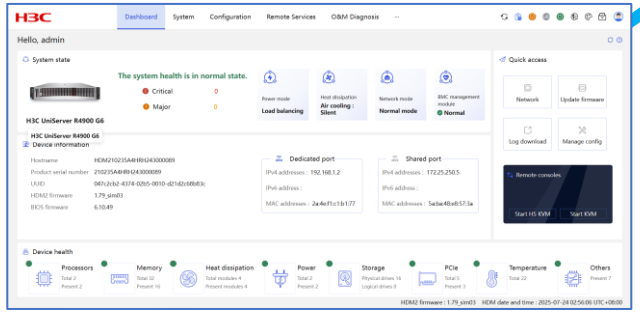
管理モジュールのHDMインタフェース



LAN

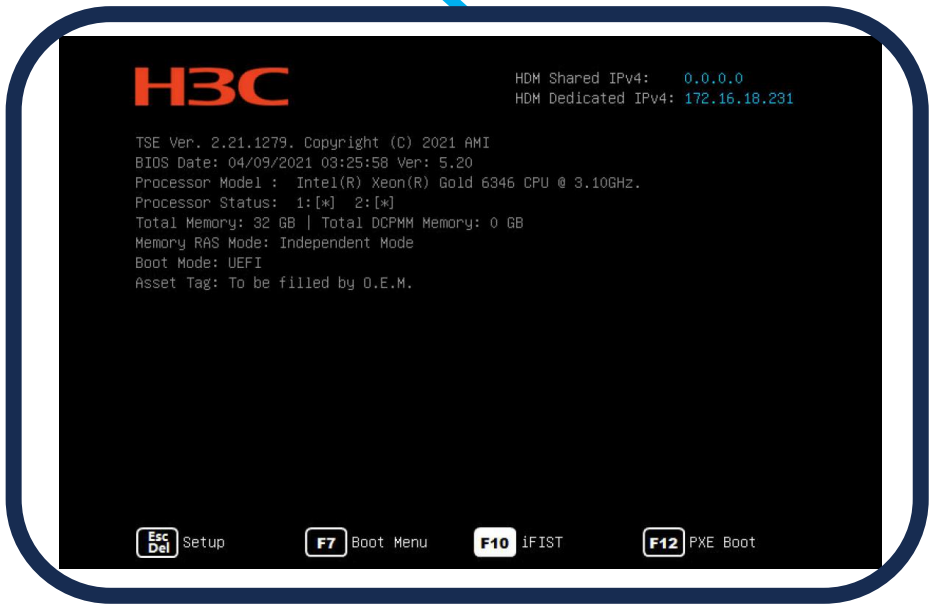
VGAコネクター

HDM用管理インタフェース
(192.168.1.2/24)



USB3.0コネクター





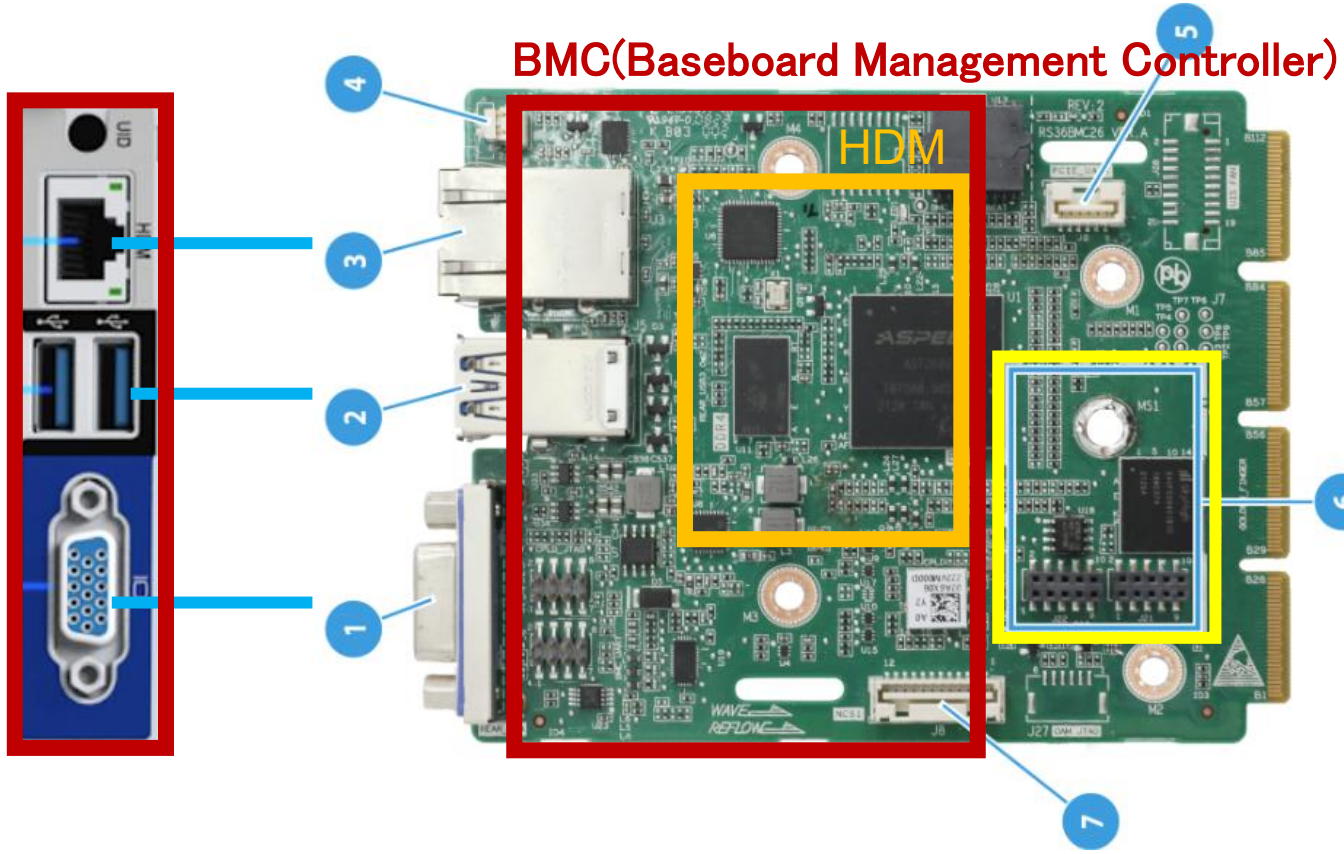
電源が落ちていても、電源コードが刺さっていれば、アクセスが可能

管理モジュール上のHDMとiFISTモジュール

HDM専用ネットワーク
インタフェース

２つのUSB3.0
コネクター

VGAコネクター



iFISTモジュール

サーバーではこのようなモジュールをメザニンカード(基板の上に「重ねるように」搭載する拡張基板)と呼ぶ

(1) VGA connector	(2) Two USB 3.0 connectors
(3) HDM dedicated network interface	(4) UID LED
(5) HDM serial port	(6) iFIST module
(7) NCSI connector	

H3C HDMの管理用デフォルトパラメーター

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

HDMのsyslogメッセージ

H3C HDM syslogメッセージ

電源装置障害が検出されました

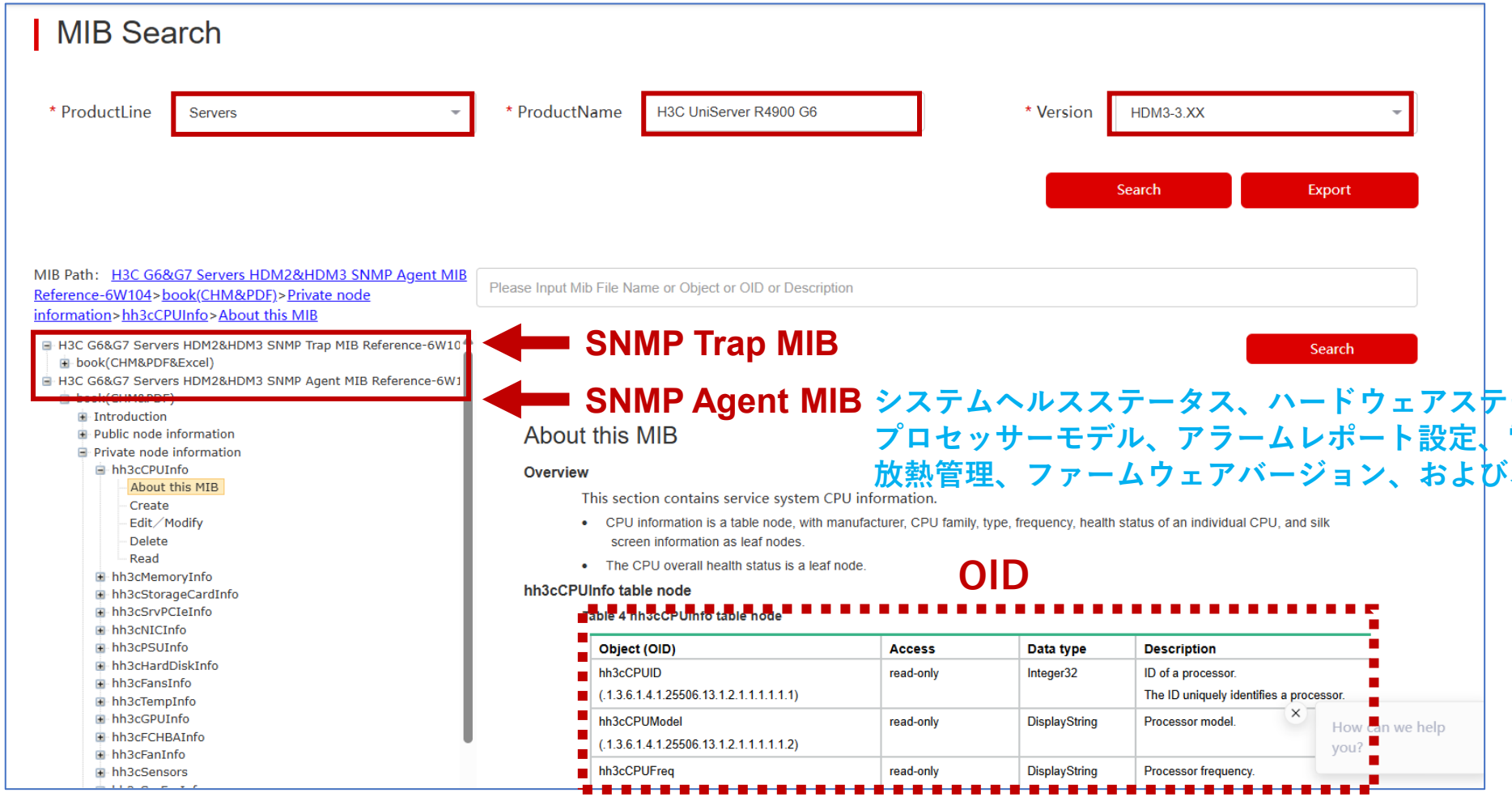
イベントコード	0x081000de
メッセージテキスト	電源装置障害が検出されました。
可変フィールド	該当なし
重大度レベル	メジャー
説明	電源モジュールの検出に失敗しました。
推奨処置	1. 環境が要求どおりであることを確認します。たとえば、周囲温度が要求どおりであり、ファンが正常に動作していることを確認します。 2. PSUを取り付け直します。 3. 障害のある電源装置を交換します。

電源装置の障害予測

イベントコード	0x082000de
メッセージテキスト	パワーサプライの障害予測。
可変フィールド	該当なし
重大度レベル	マイナー
説明	電源装置が故障しようとしていました。
推奨処置	1. 電源装置のLEDを調べて、電源装置が正常に動作していることを確認します。電源装置のファンがブロックされていないこと、および周囲温度が正常であることを確認します。 2. PSUを取り付け直します。 3. 障害のある電源装置を交換します。 4. 不平衡電力負荷が発生した場合は、パワーサプライを交換してください。

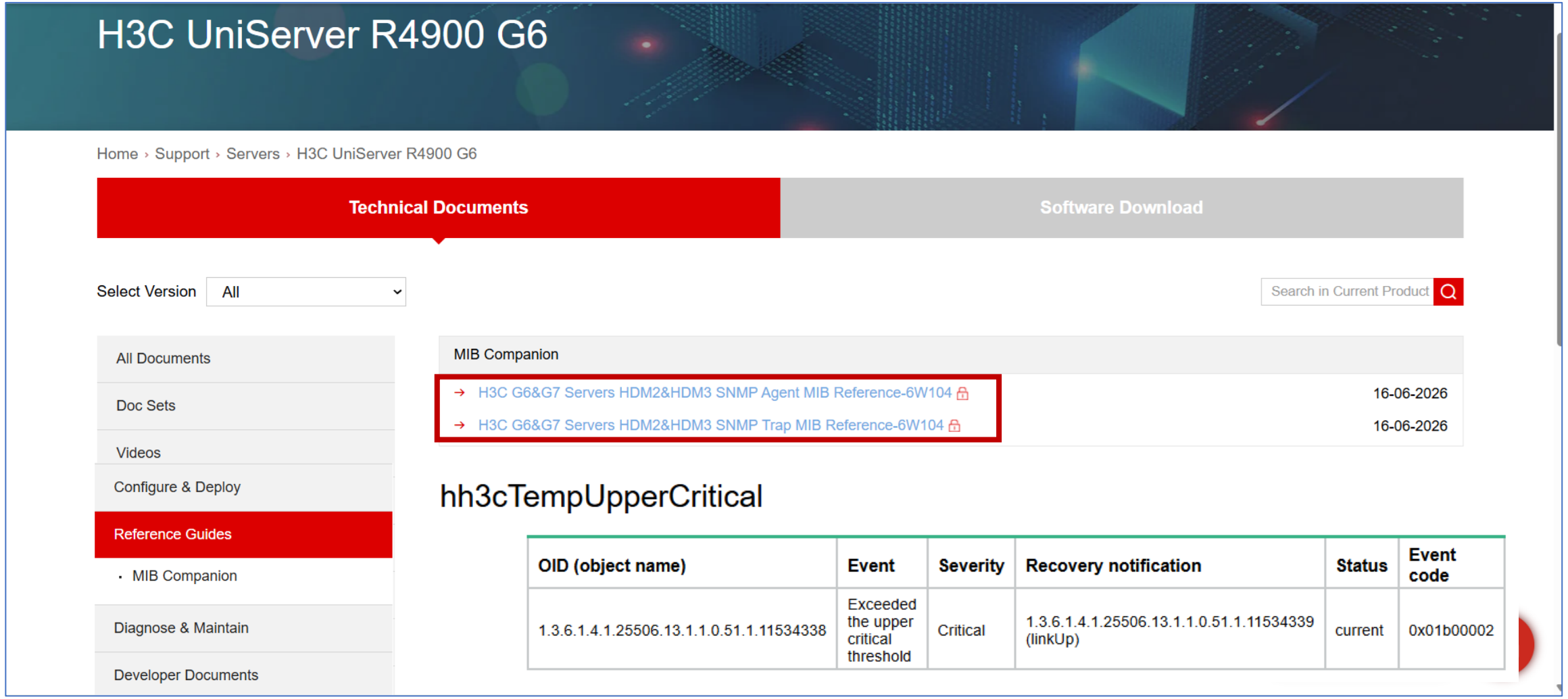
H3C HDMのMIBパラメーター検索

https://www.h3c.com/cn/BizPortal/QueryMIB/En_index.aspx



システムヘルスステータス、ハードウェアステータス、メモリーおよびプロセッサーモデル、アラームレポート設定、電力統計情報、資産情報、放熱管理、ファームウェアバージョン、およびネットワーク管理。

H3C HDMのMIBパラメータードキュメント

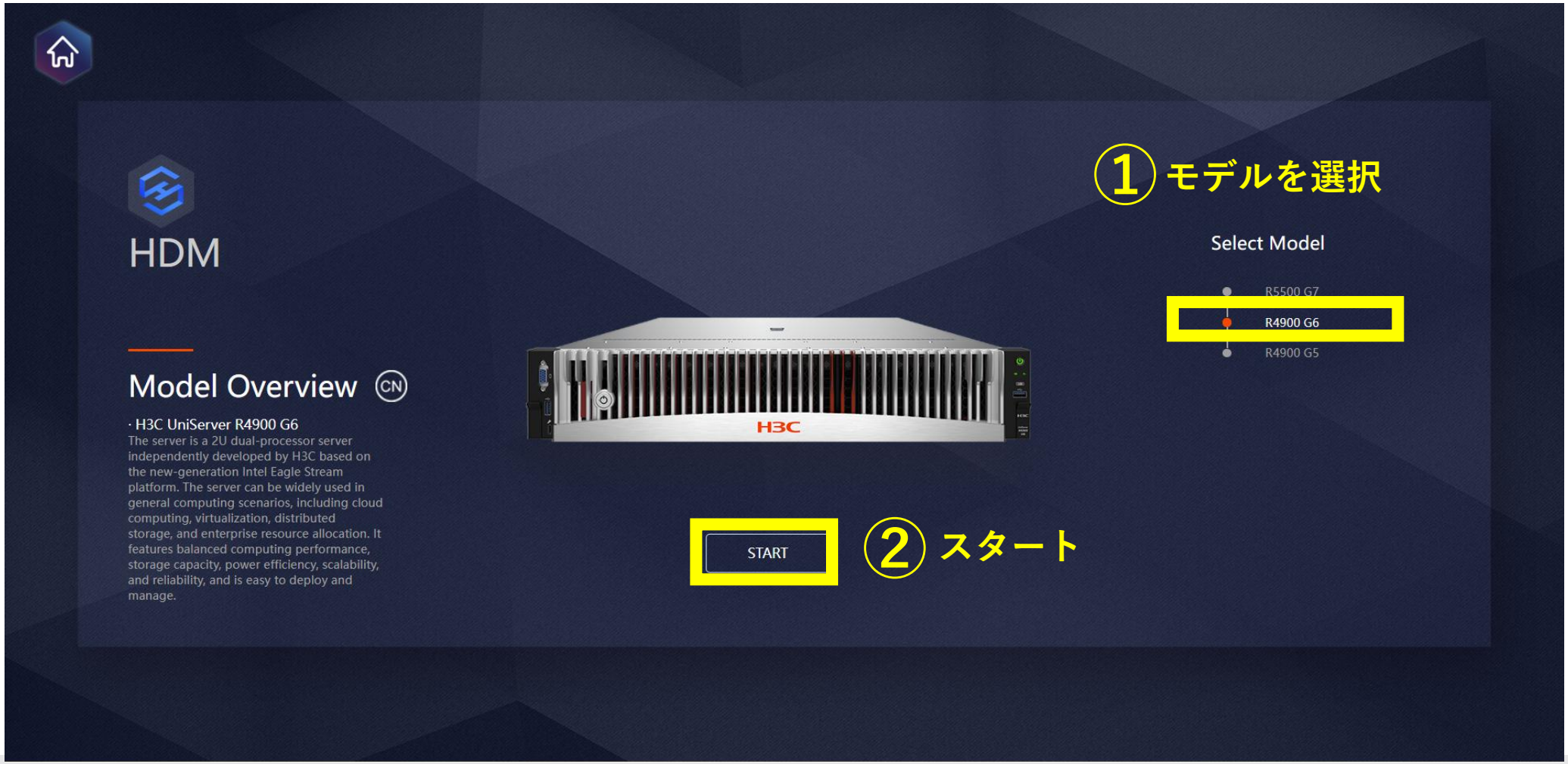


サーバーソフトウェアシュミレーター

https://simulator.h3c.com/

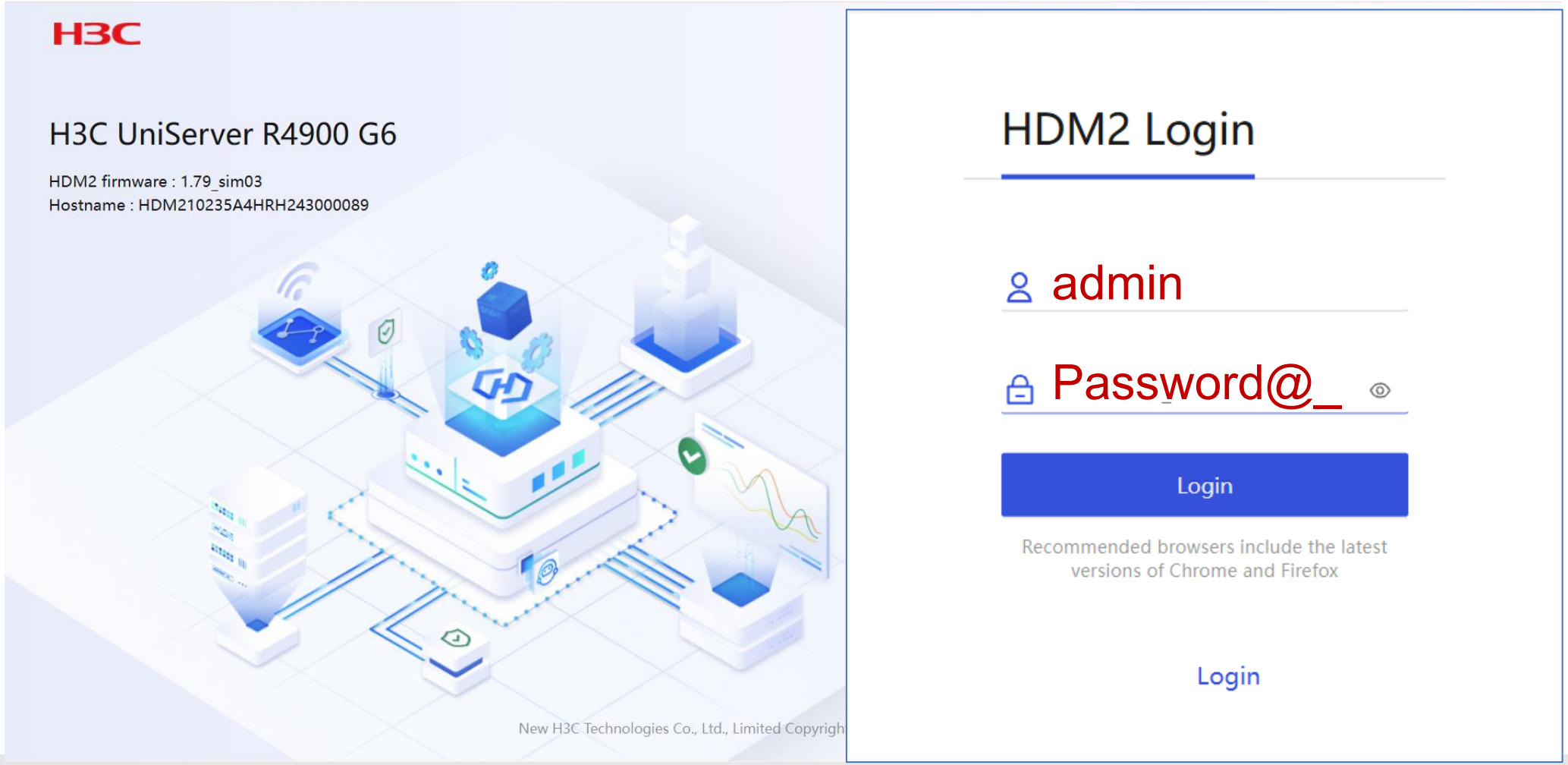


HDMシュミレーター(例えばR4900 G6)



HDMシュミレーター(例えばR4900 G6)

https://192.168.1.2/



ダッシュボード（言語切り替え/日本語）



ダッシュボード

ダッシュボードページでは、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。

デフォルトの管理IPアドレスの変更



ネットワーク
ネットワーク設定を変更します

HELPアイコンをクリックすると現在表示されている画面のマニュアルが表示されます

デフォルトの管理IPアドレスの変更



専用ポート

設定

HDMのLANポートのIPアドレス、デフォルトゲートウェイ、DNSサーバーのアドレスなどが設定されています。

デフォルトの管理IPアドレスの変更



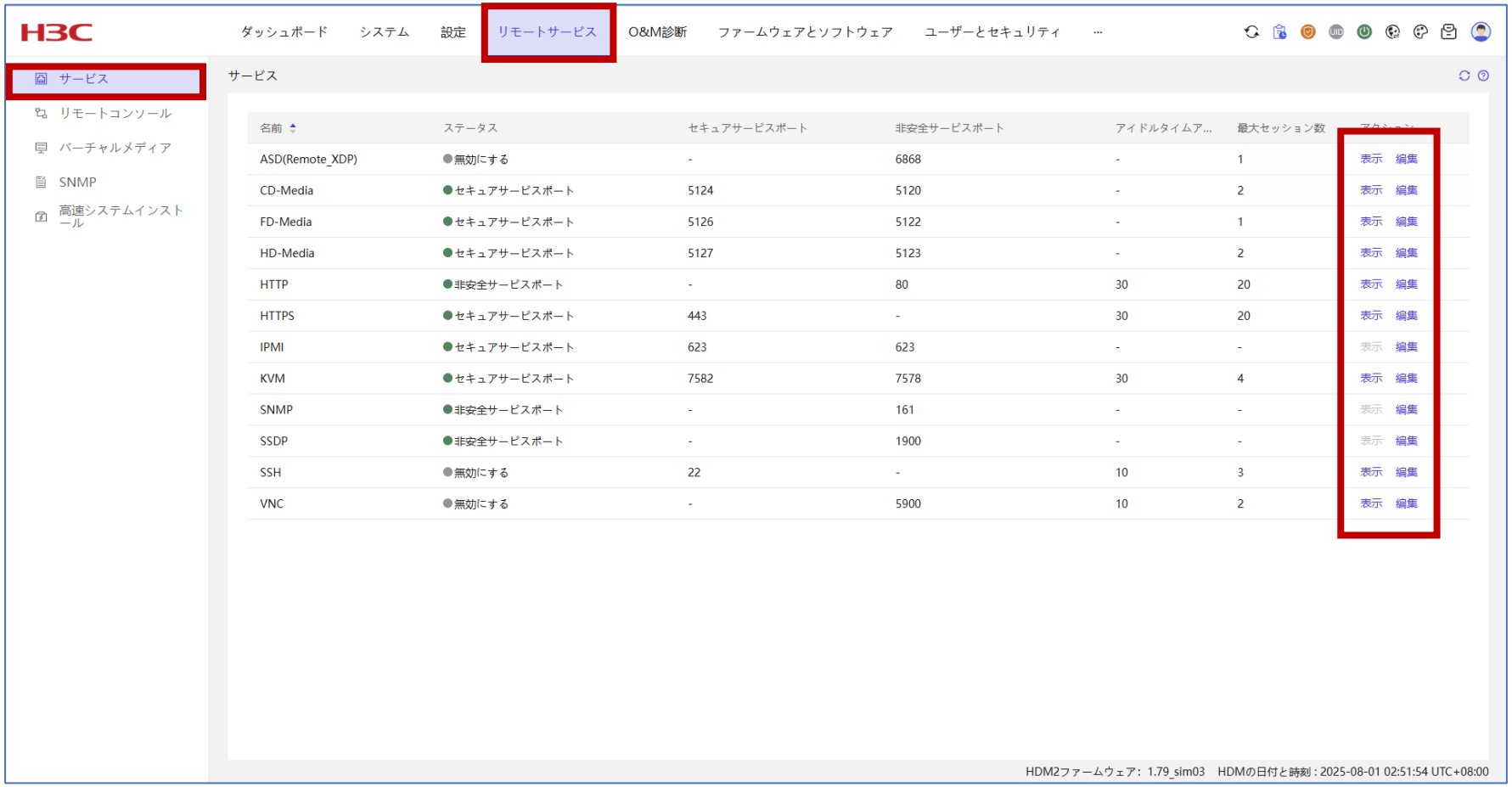
ネットワーク
IPv4
デフォルトのIPアドレス
192.168.1.2/24
ゲートウェイ
192.168.1.1/24

設定 > NTP



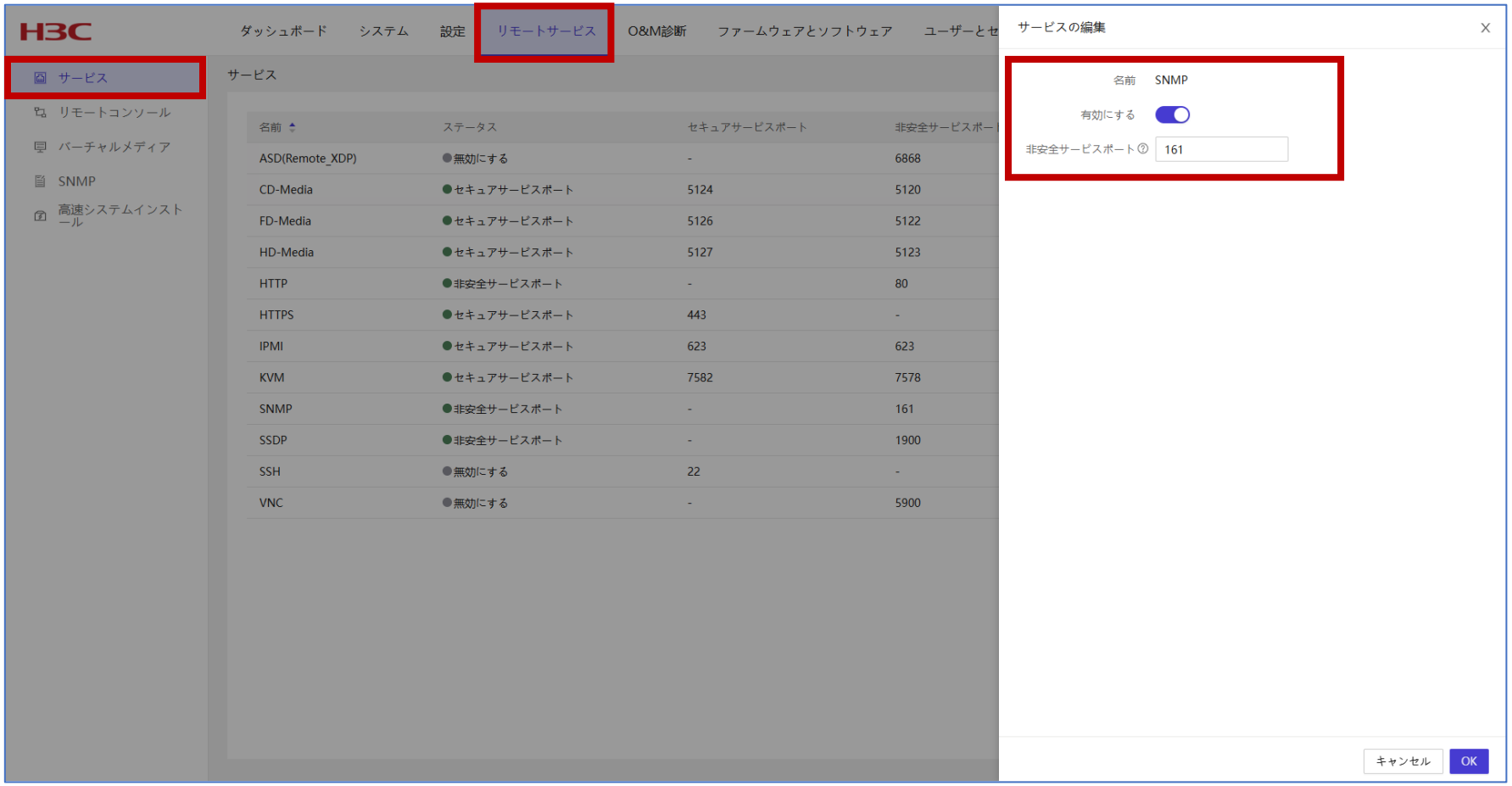
設定
　NTPサーバーの設定を忘れずに行ってください

リモートサービス > サービス



リモートサービス
サービス
HTTP, HTTPS, SNMP, SSH等を有効にする

リモートサービス > サービス > 編集



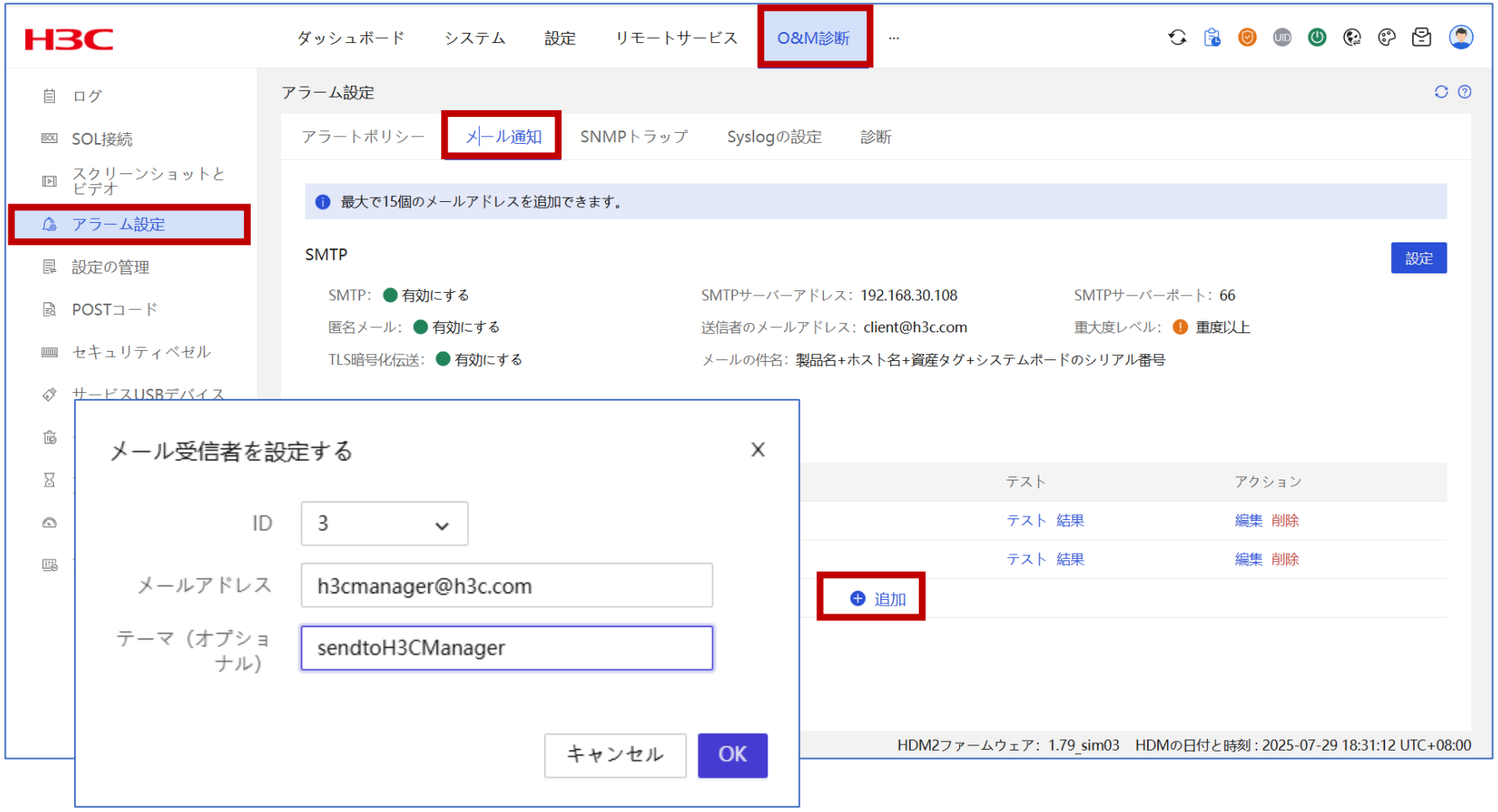
リモートサービス
サービス
HTTP, HTTPS, SNMP, SSH等を有効にする

リモートサービス > SNMP



リモートサービス
- SNMP
  - SNMPのコミュニティ名を変更することができます。読み取り専用コミュニティ名は recommstr

O&M診断 > アラーム設定 > メール通知 > 追加



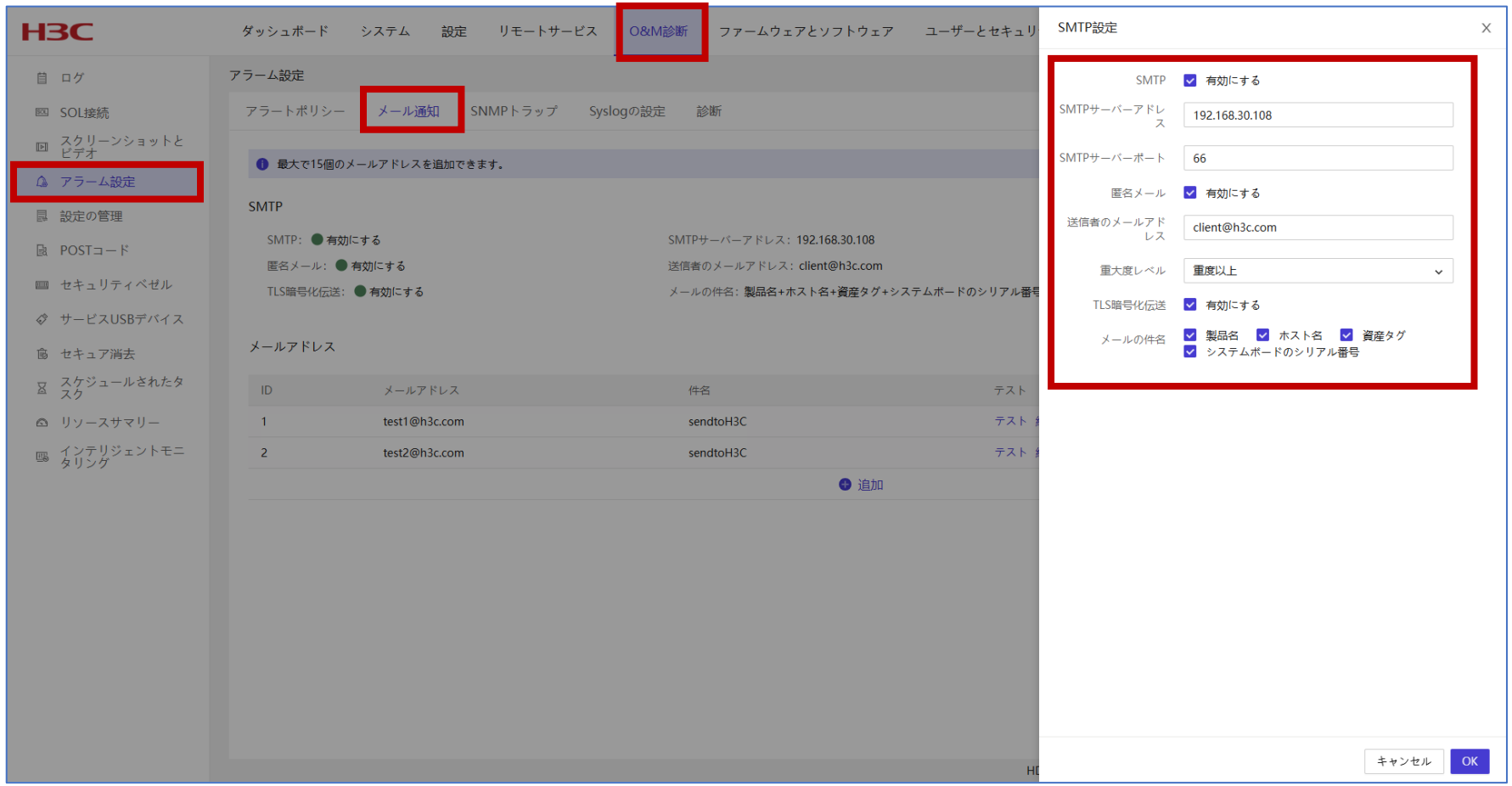
O&M診断
アラーム設定
HDMは、生成されたイベントログをサーバーから指定したユーザーに報告するための**アラート電子メールの送信をサポート**しており、ユーザーがサーバーの操作ステータスを監視するのに役立ちます。
SMTPサーバードレスには、IPv4アドレス、IPv6アドレスまたはドメイン名を使用できます。
HDMは、匿名ユーザーおよび認証ユーザーへのアラート電子メールの送信をサポートしており、**最大15人の受信者ユーザーを構成できます。**
HDMでは、重大度レベルに基づいてアラートイベントをレポートできます。

O&M診断 > アラーム設定 > メール通知 > 設定



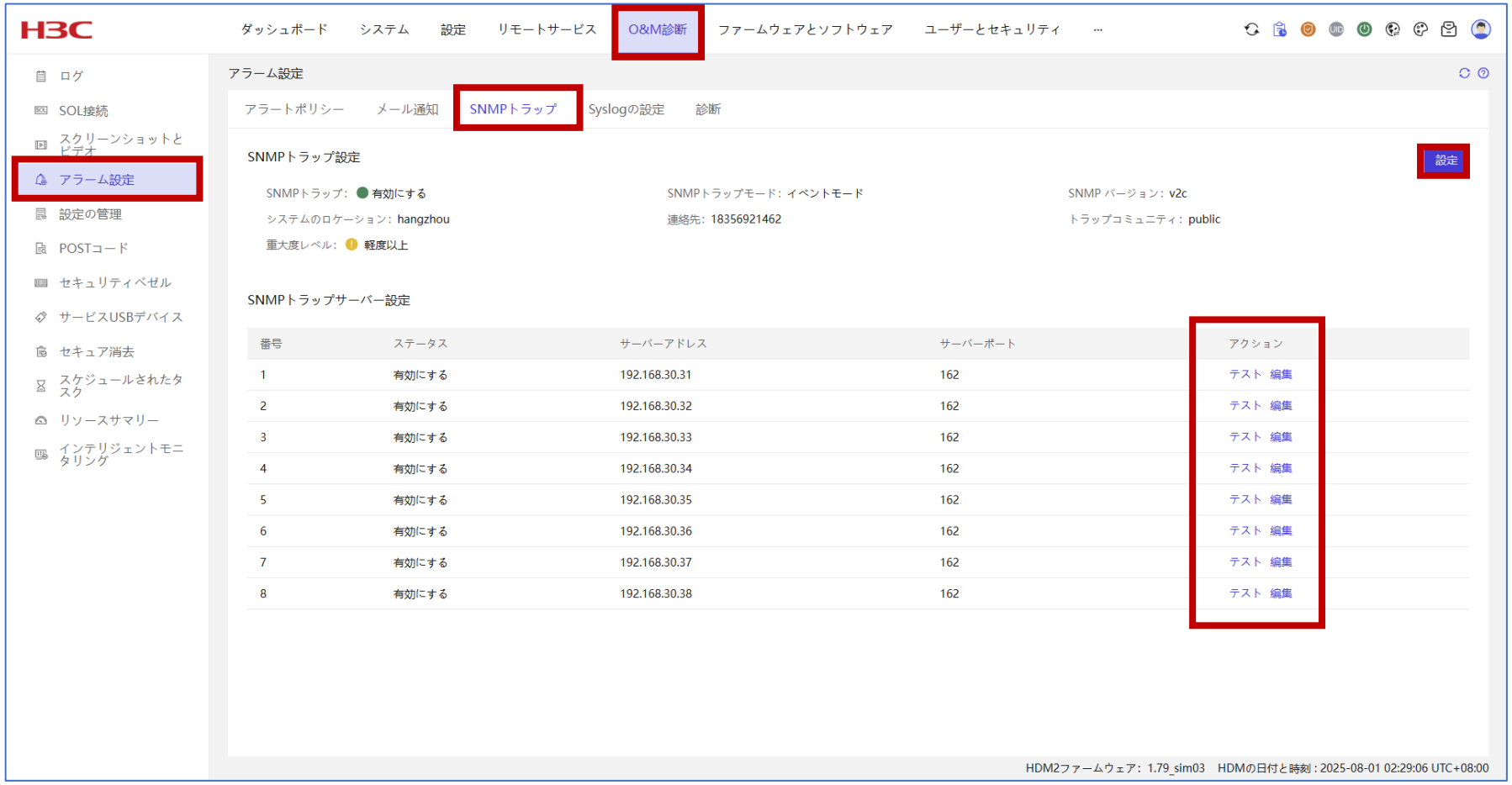
O&M診断
アラーム設定
メール通知
設定

O&M診断 > アラーム設定 > メール通知 > 設定



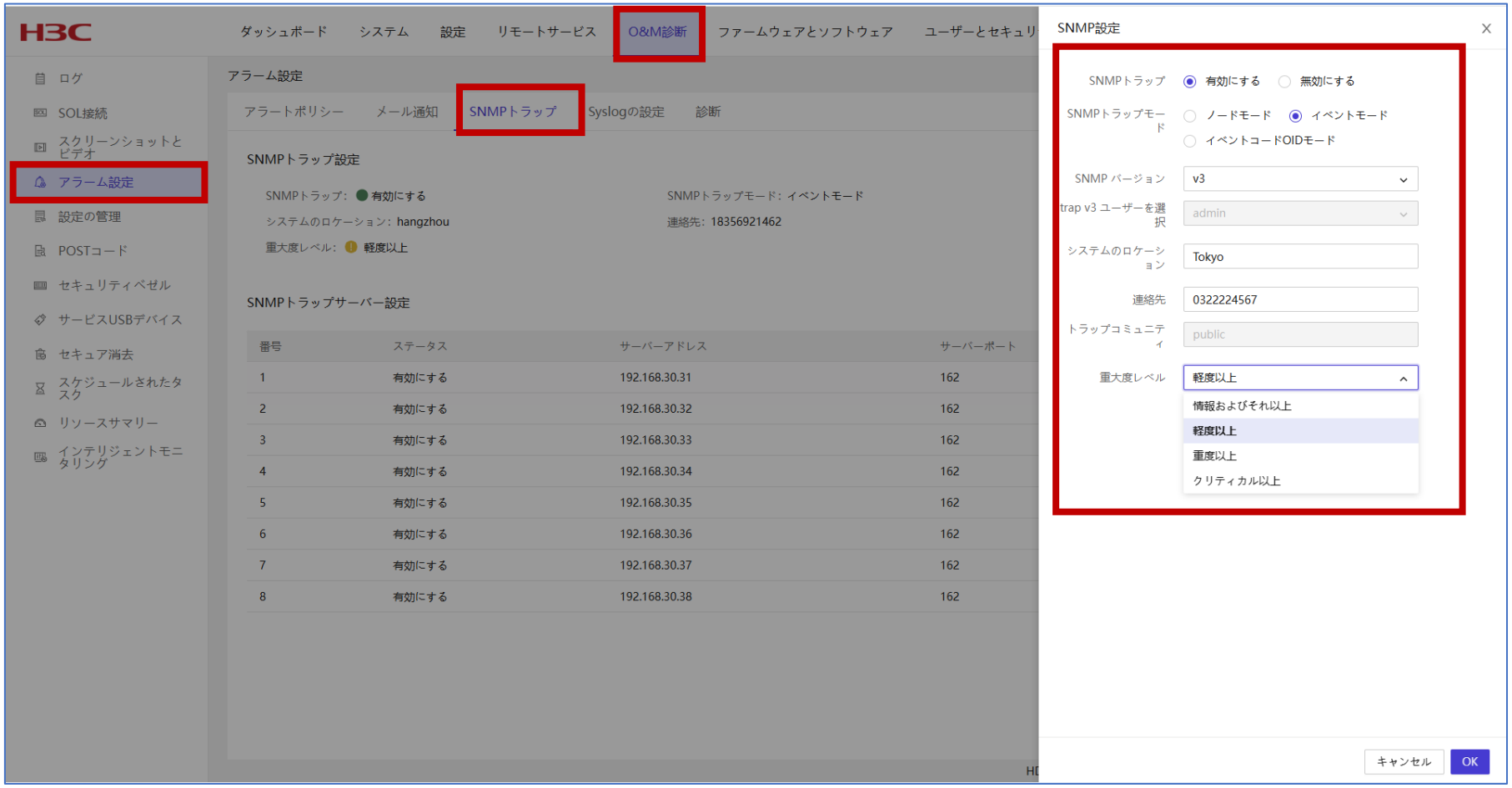
O&M診断
アラーム設定
メール通知
設定

O&M診断> アラーム設定 > SNMPトラップ > 設定



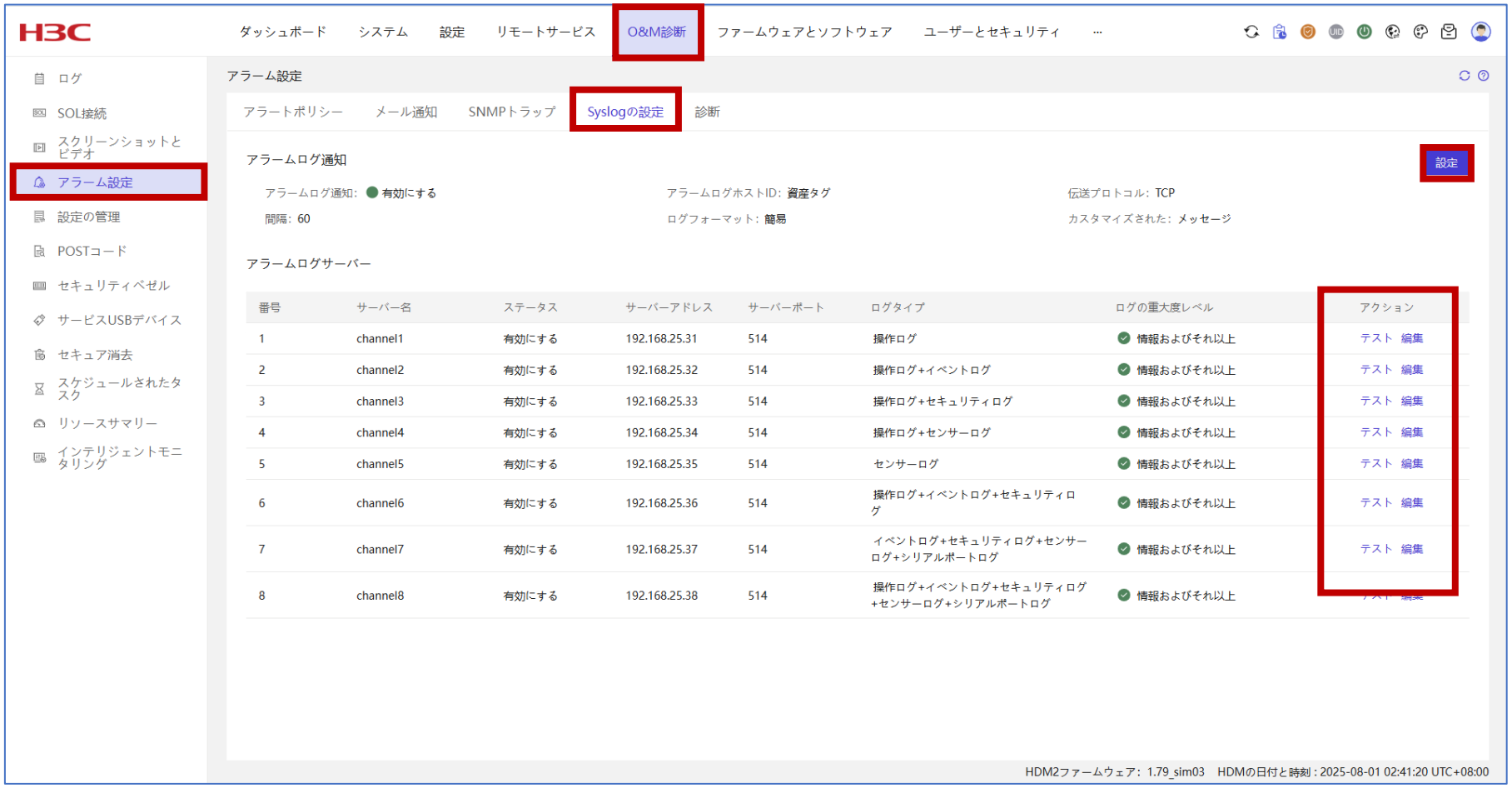
O&M診断
- アラーム設定
  - SNMPトラップ
  - SNMPトラップサーバー
    - 編集
      - 有効にする
      - サーバーアドレス
      - サーバーポート

O&M診断> アラーム設定 > SNMPトラップ > 設定



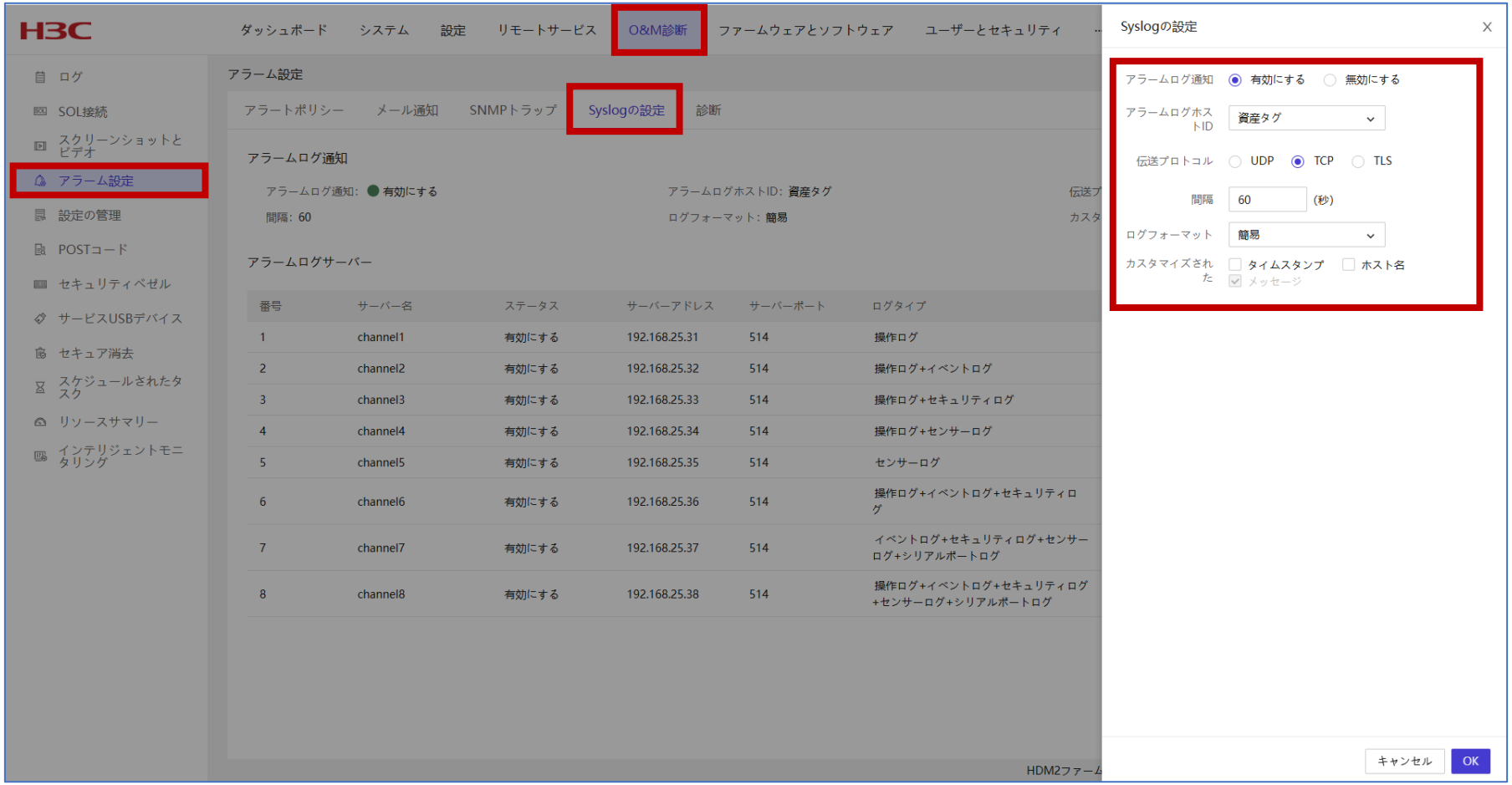
O&M診断
- アラーム設定
  - SNMPトラップ
  - 設定
  - SNMPバージョン
  - 重大度レベル
    - 情報及びそれ以上
    - 軽度以上
    - 重度以上
    - クリティカル以上

O&M診断> アラーム設定 > Syslogの設定 > 設定



O&M診断
- アラーム設定
  - Syslogの設定
    - アラームログサーバー
      - 有効にする
      - サーバー名
      - サーバーアドレス
      - サーバーポート
      - ログタイプ
      - ログの重大度レベル

O&M診断> アラーム設定 > Syslogの設定 > 設定



O&M診断
- アラーム設定
  - Syslogの設定
  - 設定
    - アラームログホストID
    - 伝送プロトコル
      - UDP/TCP/TLS
    - ログフォーマット
      - 簡易
      - RFC3164
      - RFC5424

システム > システム概要



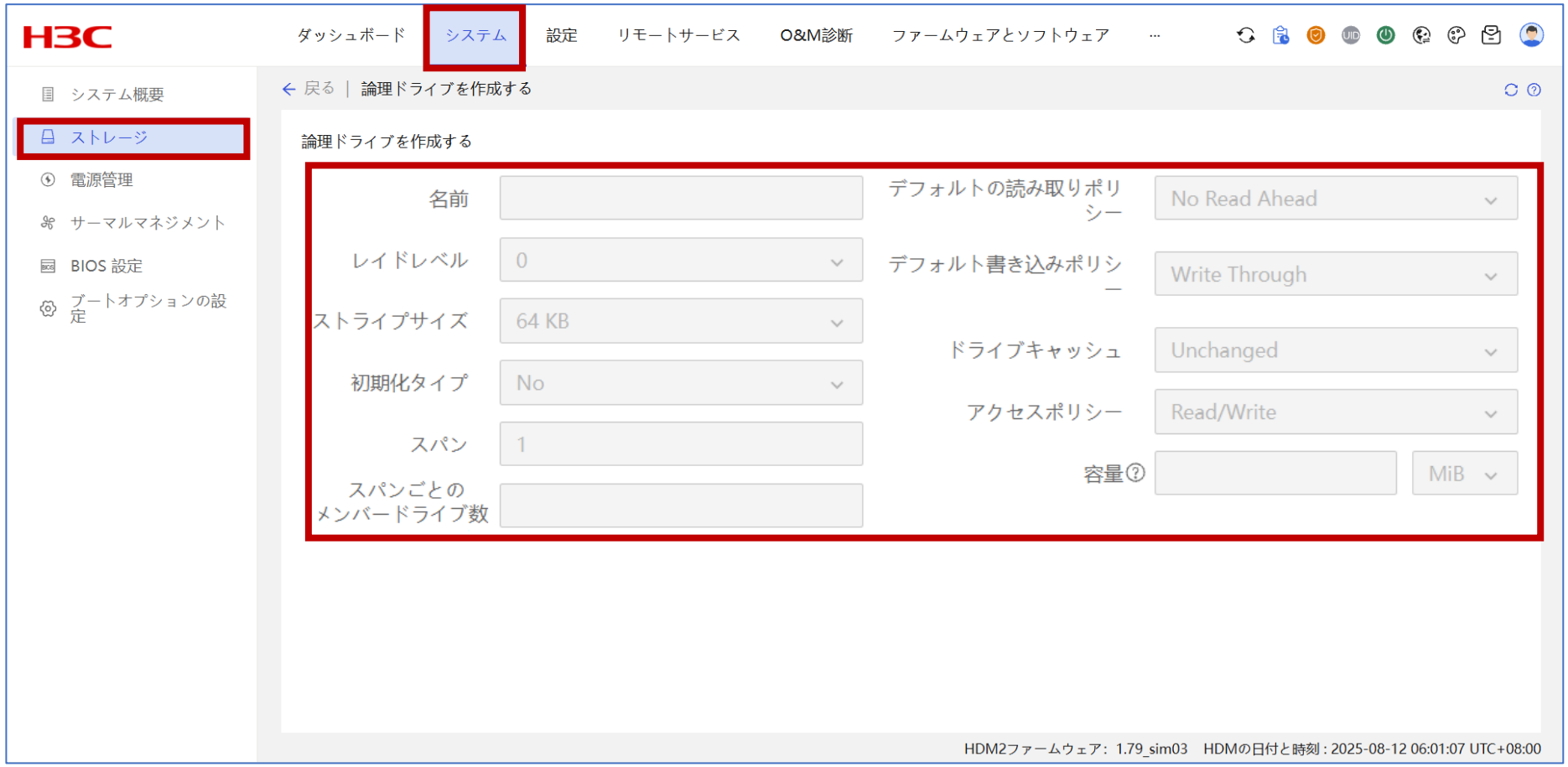
システム
- システム概要
  - 製品情報
  - プロセッサ
  - メモリ
  - PCIeモジュール
  - センサー
- ストレージ
- 電源管理
- サーマルマネージメント
- BIOS設定
- ブートオプションの設定

システム > ストレージ



システム
- ストレージ
  - ストレージコントローラ
  - **RAIDの設定**
    - **論理ドライブを作成**
- 電源管理
- サーマルマネージメント
- BIOS設定
- ブートオプションの設定

システム > ストレージ > 論理ドライブを作成する



システム
- ストレージ
  - ストレージコントローラ
  - **RAIDの設定**
    - **論理ドライブを作成**
- 電源管理
- サーマルマネージメント
- BIOS設定
- ブートオプションの設定

システム > ストレージ > 論理ドライブを作成する

論理ドライブを管理する

論理ドライブ情報を表示したり、論理ドライブを作成したりするには、このタスクを実行します

制限事項およびガイドライン

論理ドライブを作成または削除した後は、システムによる処理の完了を少し待ってからページを更新し、操作結果を確認してください。**1つの物理ドライブを使用して作成できる論理ドライブは1つだけです。**

論理ドライブのデフォルトの最大容量は、設定可能な最大容量とわずかに異なる場合があります。論理ドライブの作成時にドライブ容量を指定しない場合、ドライブ容量はシステムによって算出されたデフォルトの最大容量となります。

RAIDモードで動作する一部のLSIストレージコントローラについては、BIOSからJBODモードの有効/無効の状態を確認および設定できます。論理ドライブの容量単位は、MiBまたはMBで表示されます。どちらの単位も1024を基準として換算されます。表示上の違いは、実際の使用には影響しません。1つのストレージコントローラは、HDMから最大256個の論理ドライブを管理できます。この機能への対応状況は、ストレージコントローラの仕様によって異なります。

システム > ストレージ > 論理ドライブを作成する

- **名前**: 論理ドライブの名前。

- **レイドレベル**: 論理ドライブのRAIDレベル。DMウェブインターフェースでは、PMCストレージコントローラでサポートされているRAID1(Triple)およびRAID10(Triple)は、それぞれRAID1(ADM)およびRAID10(ADM)として表示されます。

- **ストライプサイズ**: 各物理ドライブのストライプサイズです。 この分野のサポートはストレージコントローラモデルによって異なります。

- **初期化タイプ**: 論理ドライブ作成時に使用される初期化タイプ。 選択肢には以下が含まれます:
  - **LSIストレージコントローラ**が管理する論理ドライブの場合:
    No—論理ドライブを初期化しません。
    Fast—ドライブ作成時に論理ドライブの最初と最後の100—ドライブ作成時に論理ドライブの最初と最後の100 MiBをデータ書き込み用に初期化し、残りの領域はバックグラウンドで初期化します。初期化後、論理ドライブの状態は最適(Optical)に変わります。
    Full—論理ドライブ内のすべての空き空間を初期化します。
  - **PMCストレージコントローラ**が管理する論理ドライブの場合:
    Default—論理ドライブを初期化しません。—論理ドライブを初期化しません。
    RapidParity—ドライブ作成時に論理ドライブの最初の10 MiBをデータ書き込みのために初期化し、残りの領域はバックグラウンドで初期化します。 初期化後、論理ドライブの状態は最適(Optical)に変わります。

システム > ストレージ > 論理ドライブを作成する

H3C
The Leader in Digital Solutions

- **スパン**: 混合モードRAID(RAID 00、RAID 10、RAID 50、RAID 60)のスパンまたはパリティグループの数。

- **デフォルトの読み取りポリシー**:論理ドライブのためにポリシーを読みましょう。 この分野のサポートは
  ストレージコントローラモデルによって異なります。 選択肢は以下の通りです:
  - **No read ahead**—先読み機能を無効にします。
  - **read ahead**—リードアップ機能を有効にします。 この機能を有効にすると、コントローラは要求されたデータの先行で順次読み込みを行い、追加データをキャッシュメモリに格納します。

- **デフォルトの書き込みポリシー**: 論理ドライブ用のポリシーを書く。 この分野のサポートは
  ストレージコントローラモデルによって異なります。 選択肢は以下の通りです:
  - **Write through**—ドライブサブシステムがトランザクションですべてのデータを受信した際に、
    コントローラがホストにデータ転送完了信号を送信できるようにします。
  - **Write back**—コントローラキャッシュがトランザクション内のすべてのデータを受信した際に、コントローラが
    ホストにデータ転送完了信号を送信できるようにします。
    ストレージコントローラにスーパーコンデンサが搭載されていないか、
    スーパーコンデンサに故障がある場合は、**Write through**ポリシーが使用されます。
  - **Always writeback**—コントローラキャッシュがトランザクション内のすべてのデータを受信した際に、
    コントローラがホストにデータ転送完了信号を送信できるようにします。

システム > ストレージ > 論理ドライブを作成する

- **ドライブキャッシュ**: 論理ドライブに対してドライブキャッシュが有効かどうかを示します。
  この分野のサポートはストレージコントローラモデルによって異なります。
  選択肢には以下が含まれます:
  - Unchanged—デフォルトのドライブキャッシュポリシーを使用します。
  - Enable—ドライブキャッシュが有効です。
  - Disable—ドライブキャッシュが無効化されます。

- **アクセスポリシー**: 論理ドライブのアクセスポリシー。 この分野のサポートはストレージコントローラモデルによって異なります。 選択肢には以下が含まれます:
  - Read/Write。
  - Read Only。
  - Blocked。

- **容量**: ドライブ容量。 LSIストレージコントローラで管理される論理ドライブの場合、最小容量は100 MiBです。
  PMCストレージコントローラで管理される論理ドライブの場合、最小容量は1GiBです。 容量を指定しない場合は最大容量が使われます。

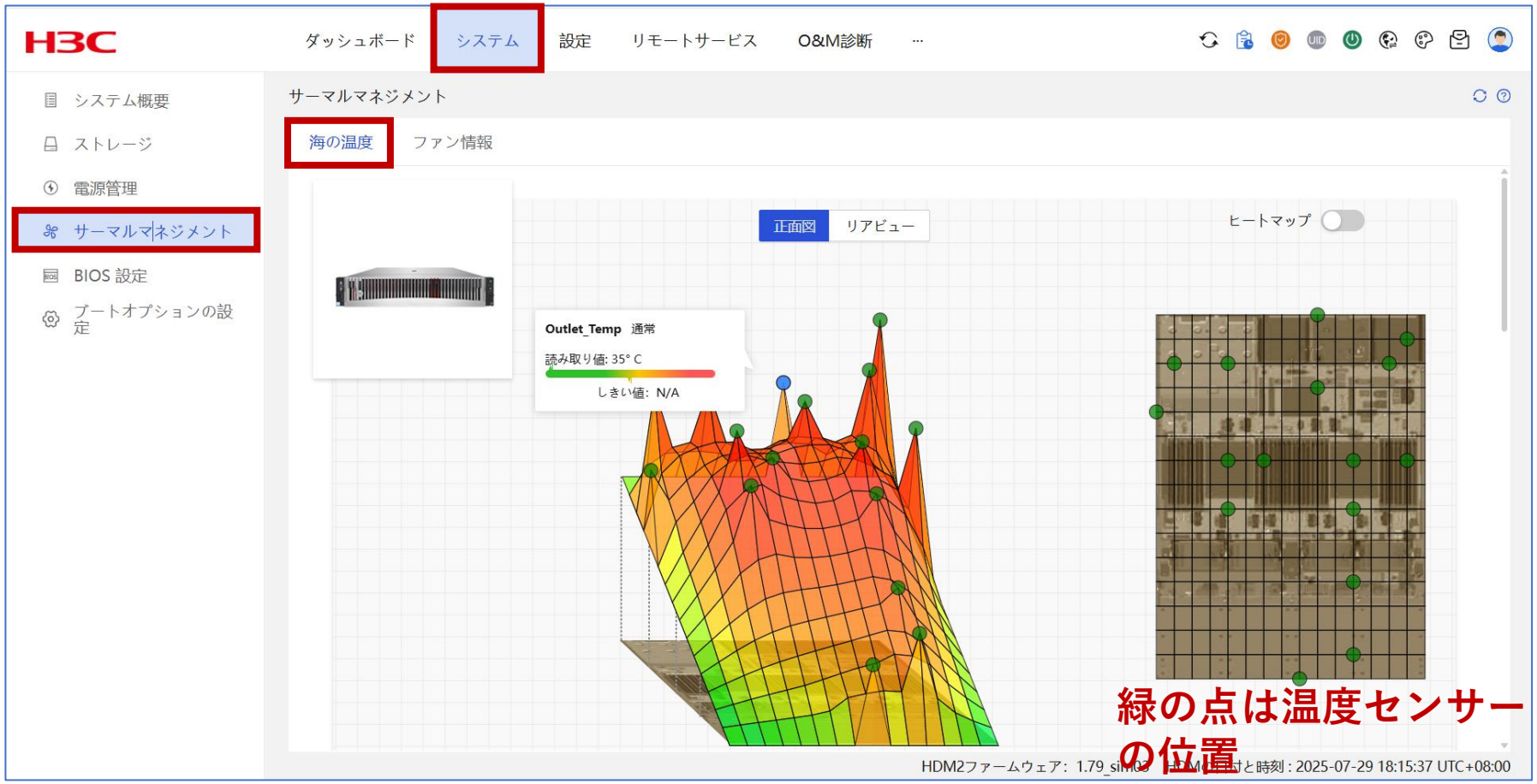
システム > 電源管理



システム
電源管理

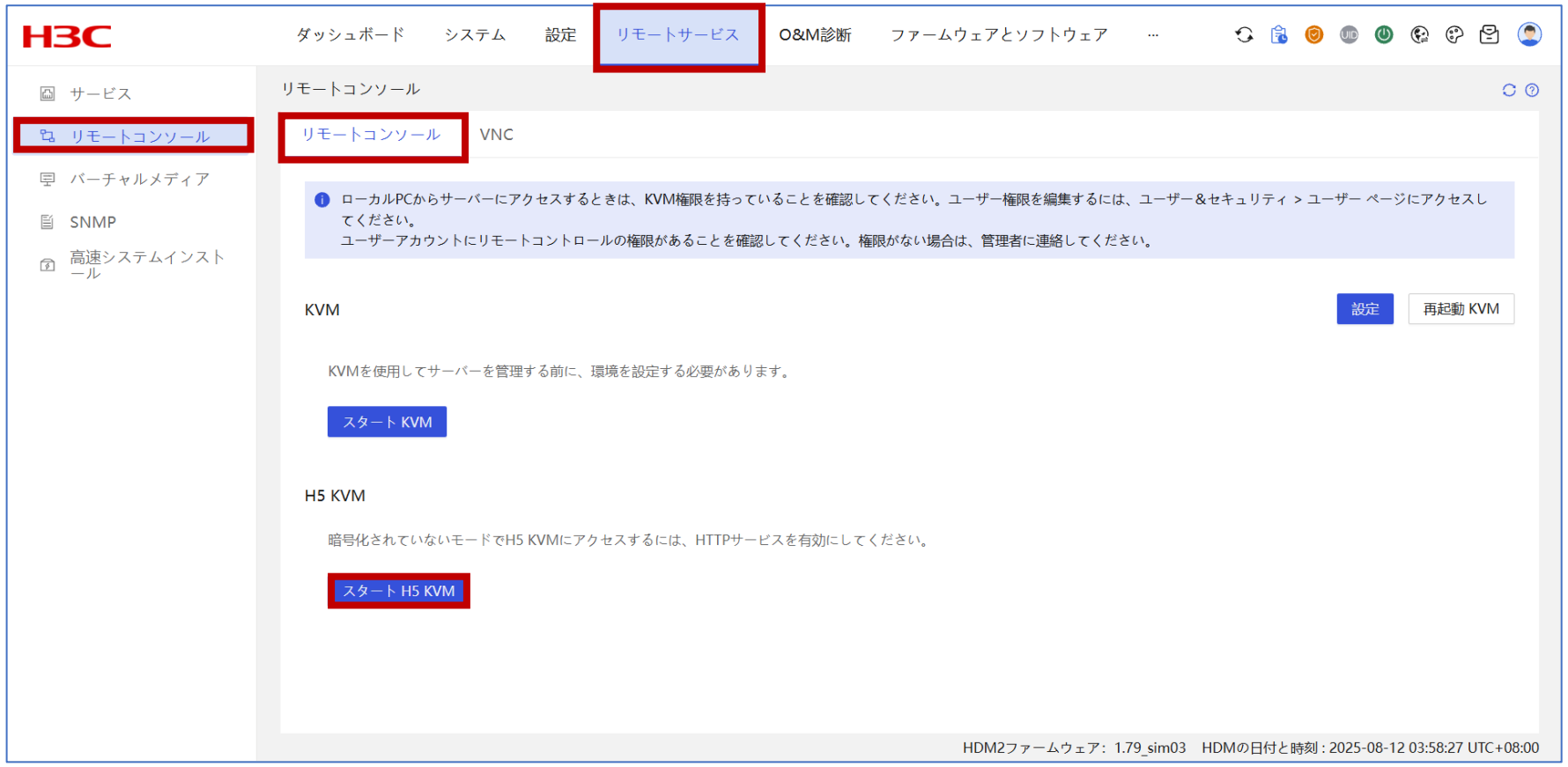
HDMは、UniSystemとの連携を通じて、データセンターサーバーのインテリジェント消費電力上限と非常用消費電力上限をサポートします。インテリジェント消費電力上限を使用すると、サービス特性に基づいてサーバーの消費電力上限値をインテリジェントに調整できるため、顧客サービスの導入を最適化するのに役立ちます。

システム > サーマルマネージメント



システム
サーマルマネージメント
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。

リモートサービス> リモートコンソール



リモートサービス
- リモートコンソール
  - KVM
  - H5 KVM

O&M診断 > ファームウェアとソフトウェア > ファームウェアの更新



O&M診断
ファームウェアを更新

・ファームウェアを更新

・ファームウェアを再起動

HDMを再起動すると、HDMへのすべてのセッションが切断されますが、この操作で設定が削除されることはありません。

CPLD(Complex Programmable Logic Device)のアップデート後、新しいバージョンを有効にするためにCPLDを再起動してください。サーバーが電源オフのときのみ、CPLDを再起動できます。

※CPLDは基板やドライブのバックプレーンの制御、LEDの点滅動作、リセット制御などを行うファームウェアで制御されるハードウェア

O&M診断 > ファームウェアとソフトウェア > ファームウェアの更新

ファームウェアの更新について

HDM、BIOS、CPLD、電源ユニット、REPO、およびストレージコントローラー、ネットワークアダプター、ドライブを含むサーバーコンポーネントのファームウェアを更新できます。サポートされるファームウェアは、サーバーのモデルによって異なります。

ファームウェア更新の制限事項とガイドライン

ファームウェアを正常に更新するために、更新中は以下の制限事項とガイドラインに従ってください。

HDMやオペレーティングシステムの誤動作を防ぐため、更新中はサーバーの電源操作（電源のオン/オフや再起動など）を行わないでください。

指示がない限り、更新中にHDMのWebページを更新（リフレッシュ）しないでください。更新を行うと、更新プロセスがリセットされてしまいます。

ファームウェアのアップグレード中は、アップグレードページを更新（リフレッシュ）しないでください。他のログインユーザーは、KVMアクセス、SDSログのダウンロード、イベントログの保存、操作ログの保存、アップグレードインベントリのダウンロード、KVM録画ビデオのダウンロード、および情報照会以外の操作を行うことはできません。

CPLDの更新に失敗すると、サーバーは使用できなくなります。サーバーにアクセスできなくなった場合は、テクニカルサポートにお問い合わせください。

HDMのストレージ容量には制限があるため、アップロードするイメージファイルのサイズは指定された上限を超えることはできません。サイズの大きいイメージファイルをアップロードするには、あらかじめファームウェアライブラリからバックアップイメージファイルを手動で削除してください。

O&M診断 > ファームウェアとソフトウェア > ファームウェアの更新

ファームウェア更新の前提条件

ファームウェアを更新する前に、以下の作業を行ってください。
テクニカルサポートへの問い合わせ、またはサーバーベンダーの公式Webサイトから、最新のサーバーファームウェアイメージを入手してください。**誤操作による設定の消失を防ぐため、設定をバックアップしてください。**HDMの設定をエクスポートしてバックアップすることができます。
他のユーザーがファームウェアを更新していないことを確認してください。ファームウェアの更新が進行中の場合、ファームウェアを更新することはできません。

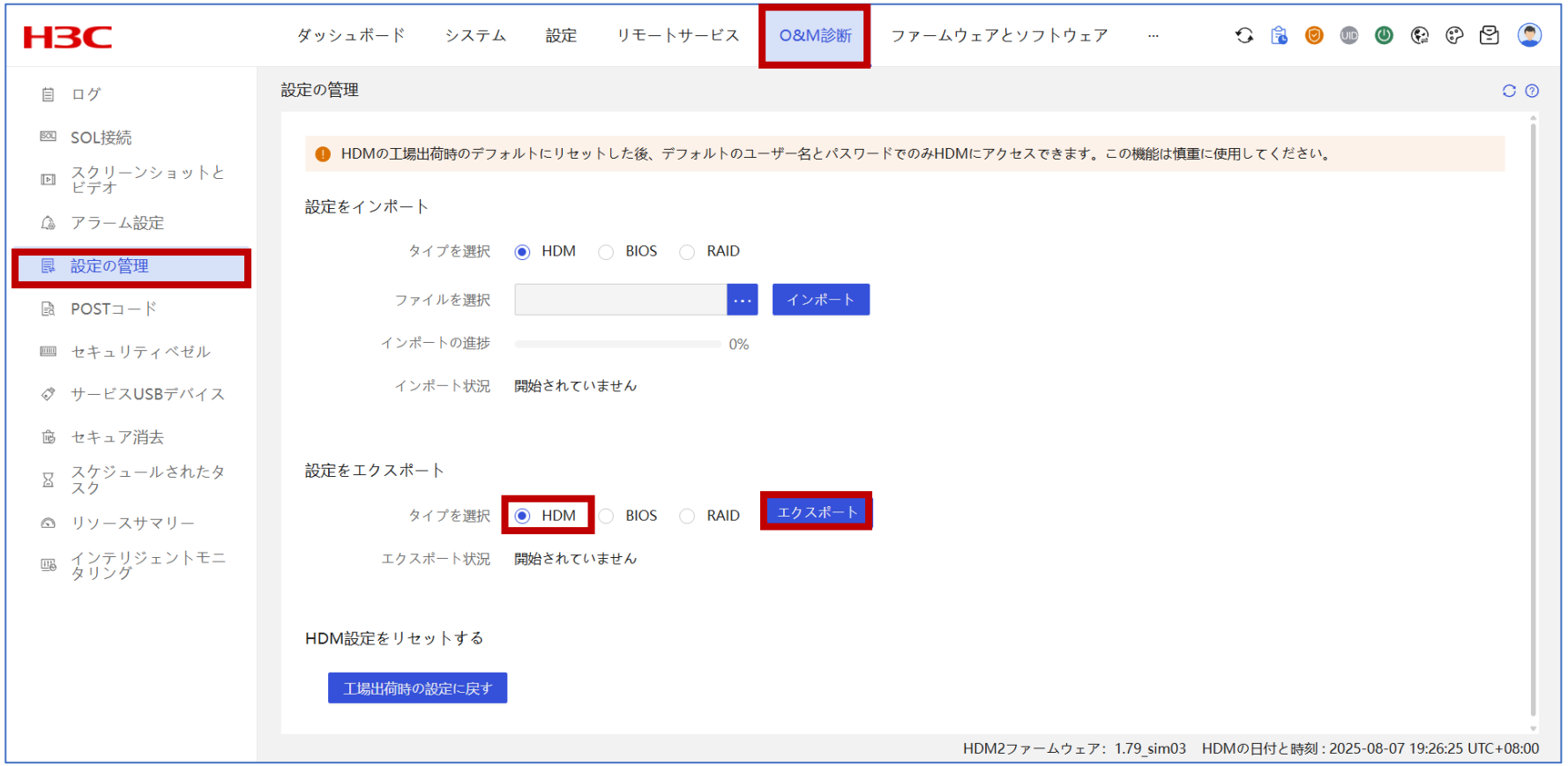
ファームウェア更新用REPOの更新

HDM、BIOS、CPLD、電源ユニット、およびストレージコントローラー、ネットワークアダプター、ドライブを含むサーバーコンポーネントのファームウェア更新用REPOを更新するには、このタスクを実行します。

制限事項とガイドライン

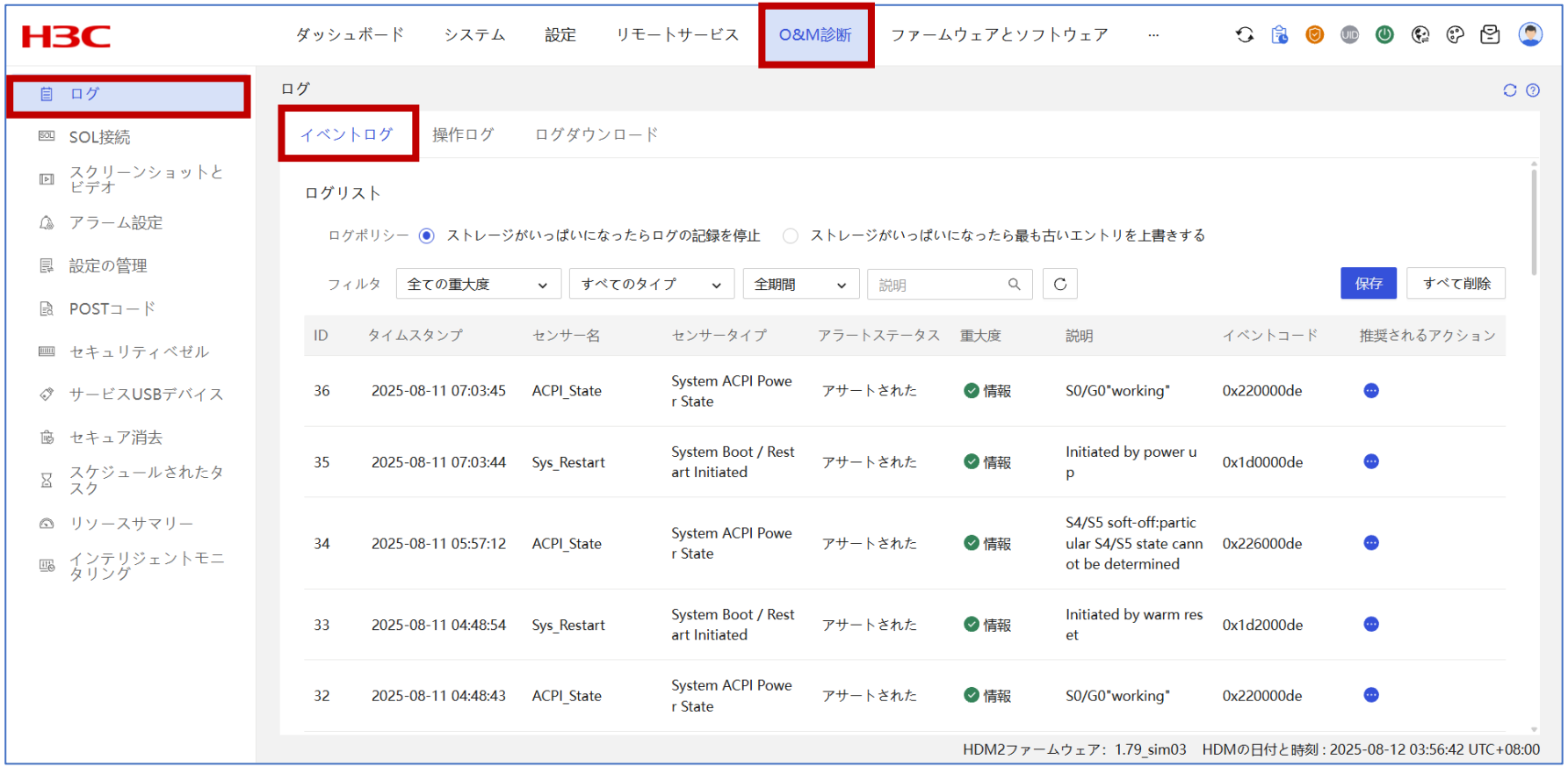
REPOの更新後に新しいファームウェアを適用（有効化）するには、サーバーのiFISTが必要です。iFISTのバージョンが現在のHDMのバージョンと互換性があることを確認してください。HDMとiFISTの互換性については、HDMまたはiFISTのリリースノートを参照してください。
HDMからREPOを更新した後、最初の再起動時に、サーバーコンポーネントの新しいファームウェアを適用するためにサーバーは自動的にiFISTを起動します。新しいファームウェアの適用後、サーバーは更新前に設定されていたブートオプションを使用して自動的に再起動します。
アップロードするREPOイメージファイルが指定された上限を超えていないこと、およびMD5ファイルが1024バイトを超えていないことを確認してください。

O&M診断> 設定の管理 > 設定をエクスポート



このタスクを実行すると、**HDM、BIOS、またはRAID構成のインポートとエクスポート**、HDMの工場出荷時設定への復元と表示ができます。

O&M診断 > ログ > イベントログ



O&M診断

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。

- **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。
- **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** -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** -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。

トラブルシュート: ダッシュボード > 製品シリアル番号



H3Cのサポートへの**トラブルシュート**を依頼する場合、**サーバーのシリアル番号**を伝えて頂く必要があります

トラブルシュート: O&M診断 > ログダウンロード > すべてをダウンロード



H3Cのサポートへの**トラブルシュート**を依頼する場合、**サーバーのシリアル番号**に加えて**ログをダウンロード**して、そのファイルを送っていただく必要があります。

他のHDMの管理: 統合コントロール > デバイス追加



この操作を実行すると、**他のHDMデバイス**を1台ずつ、またはまとめて追加できます。追加できるデバイスの**最大数は10台**です。

HDMのIPアドレスをクリックするとHDMにアクセスできます。

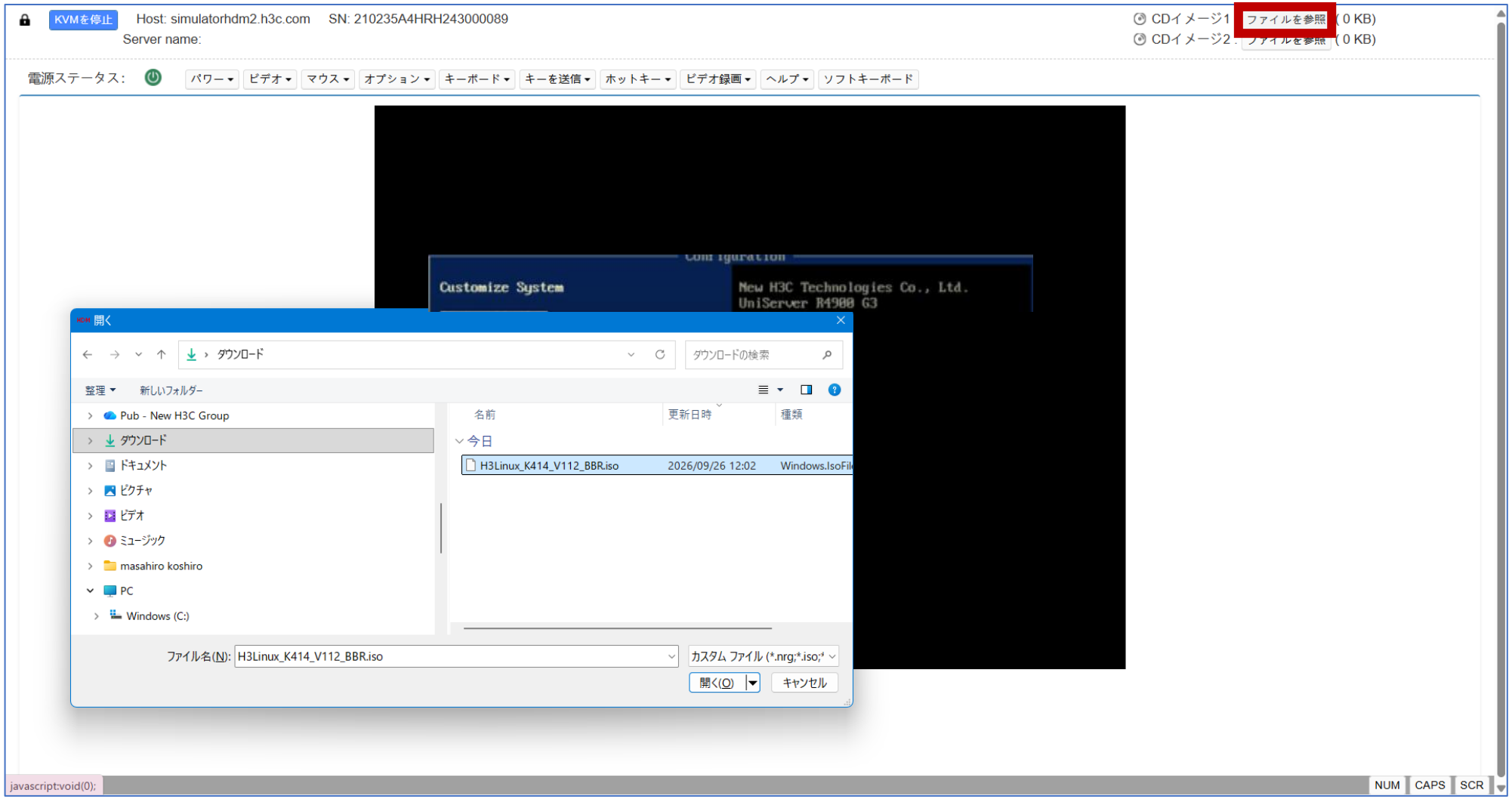
アクションにより強制電源オフ、強制システムリセット、強制電源サイクルといった操作ができます。

H5 KVMこのタスクを実行すると、H5 KVMリモートコンソールからサーバーを操作できます

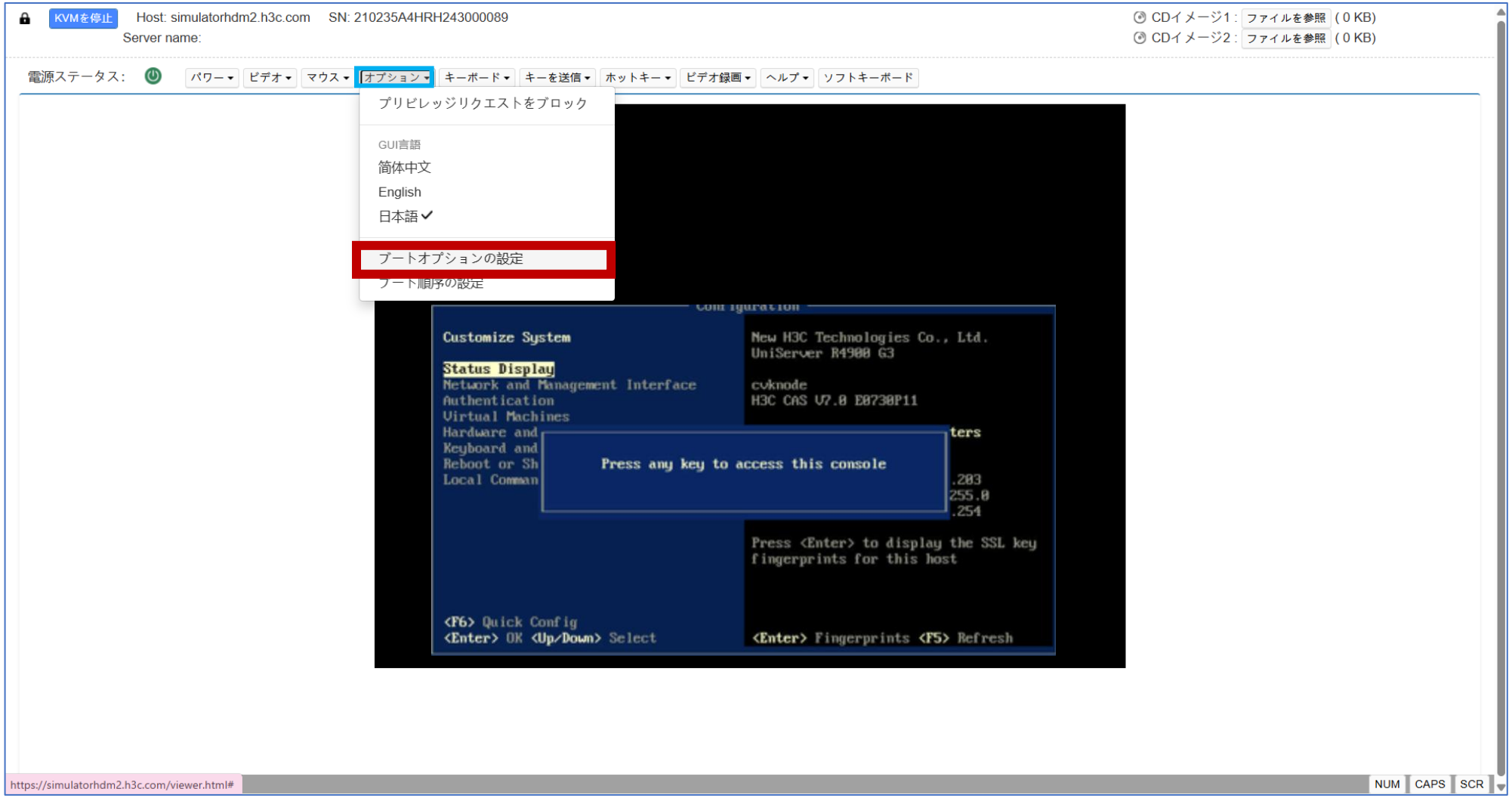
OSのインストール：スタート H5 KVM > BIOSを呼び出す



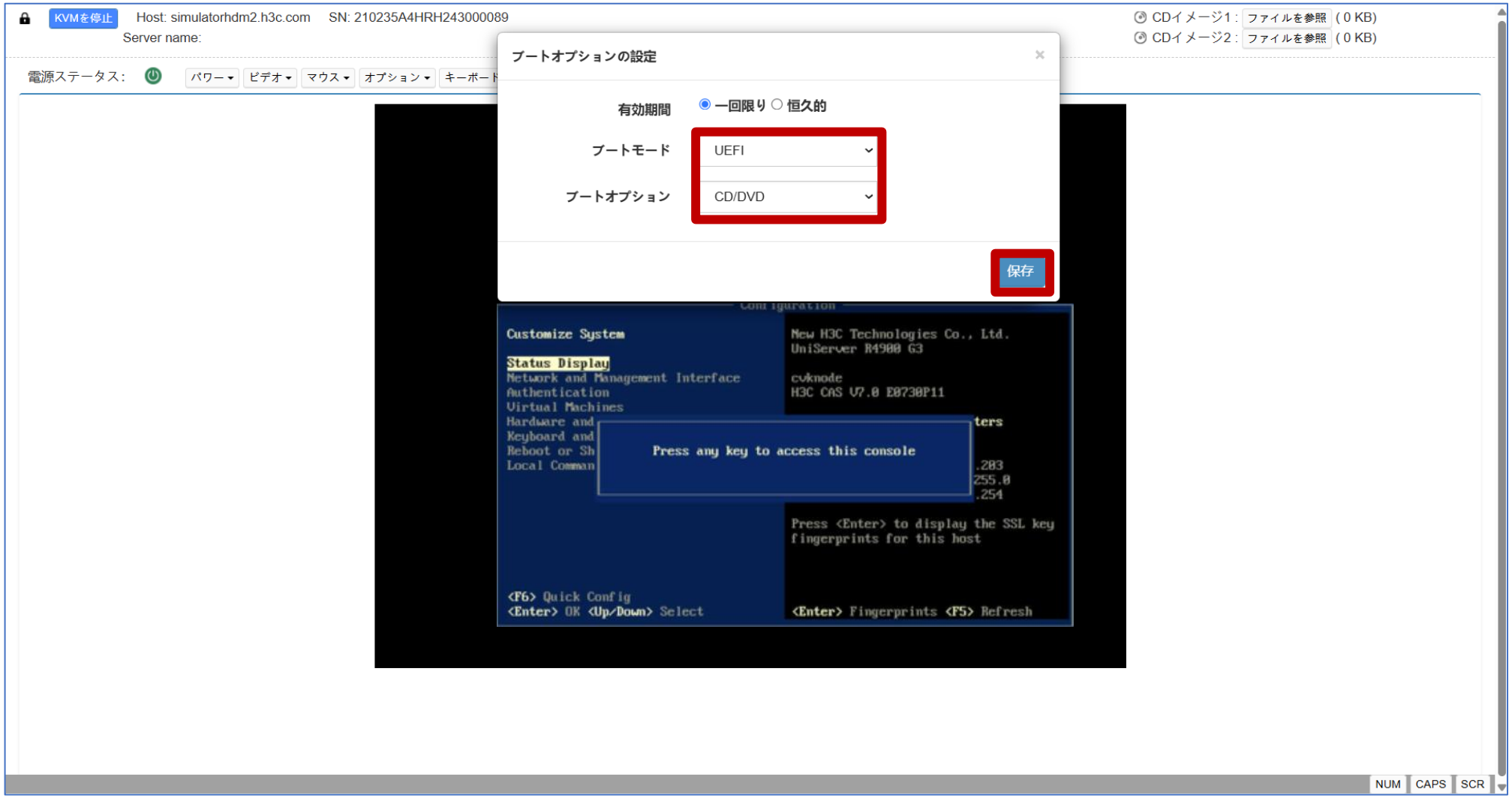
OSのインストール：CDイメージを選択します



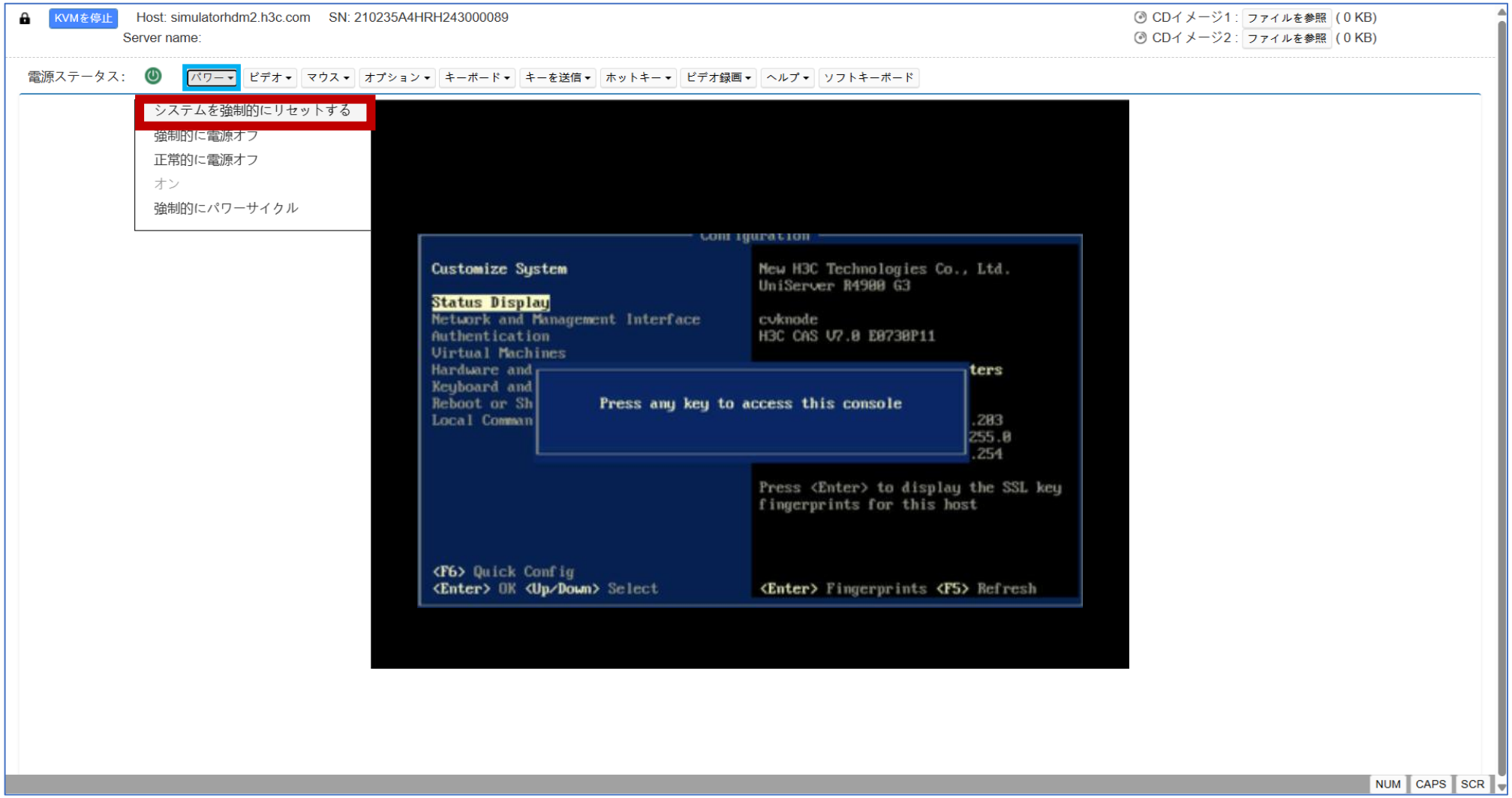
OSのインストール：CDドライブを優先します



OSのインストール：ブートオプションの設定



OSのインストール：サーバーを再起動します



IPMI (アイ･ピー･エム･アイ)

HDMは、IPMI 1.5/IPMI 2.0仕様と互換性があります。**IPMIは従来からあるサーバ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。

IPMIコマンド：シャーシの状態

CLI > **ipmitool -I lanplus -H 192.168.2.4 -U admin -P admin@H3CU chassis status**
System Power : off
Power Overload : false
Power Interlock : inactive
Main Power Fault : false
Power Control Fault : false
Power Restore Policy : previous
Last Power Event : command
Chassis Intrusion : inactive
front-Panel Lockout : inactive
Drive Fault : false
Cooling/Fan Fault : false
Sleep Button Disable : allowed
Diag Button Disable : allowed
....
CLI >

Redfish(レッド・フィッシュ)

Redfishは、RESTful APIを使用してサーバー管理を実現するHTTPSサービスに基づく新しい管理標準である。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。**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。

Redfishコマンド

RedfishのコマンドはactionとURLIが含まれます

リクエストのactionをRedfishクライアントが受け付けます

- **GET** Getや問い合わせを表します
- **POST** 作成を表します
- **PATCH** 現在の設定の更新を表します
- **DELETE** 削除を表します

共通のURIは**https://device_ip/redfish/v1/path**

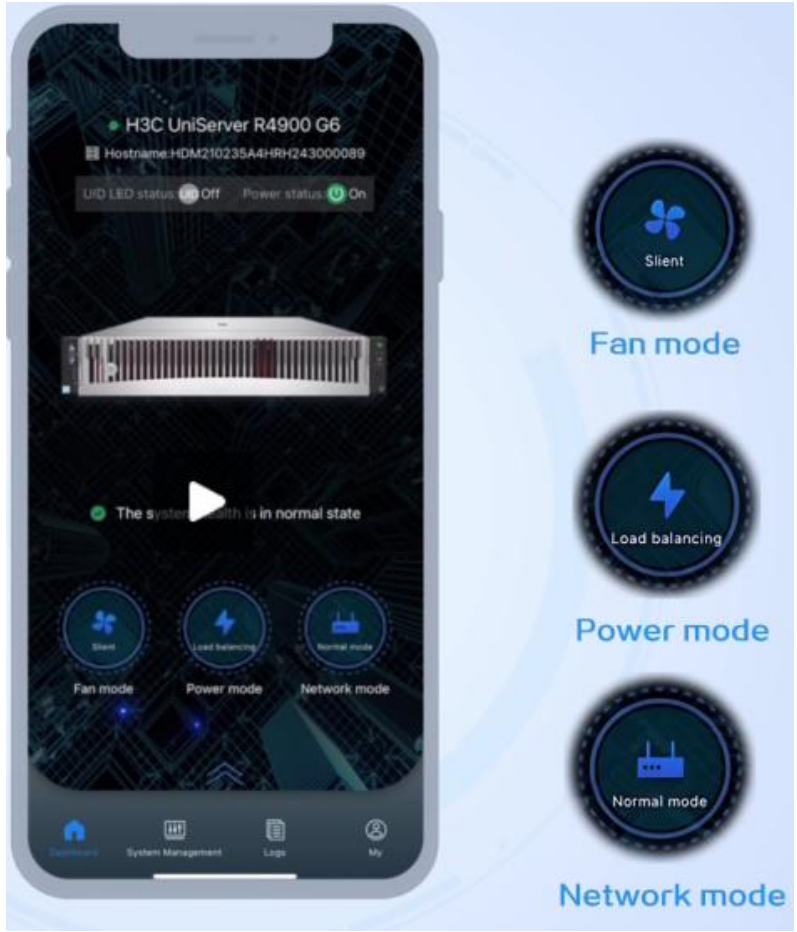
[https://device_ip]: URIアドレス、device_ipはターゲットサーバーのHDMIアドレス
[/redfish/v1]: サービスとバージョン、Redfishバージョンはv1
[/path/]: リソースへのパス

Redfishコマンドの例


```
{
        "@odata.context": "/redfish/v1/$metadata#ServiceRoot.ServiceRoot",
        "@odata.etag": "W/¥"1599071386¥"",
        "@odata.id": "redfish/v1/",
        "@odata.type": "#ServiceRoot.v1_1_1.ServiceRoot",
        "AccountService": {
                "@odata.id": "/redfish/v1/AccountService"
        },
        "Chassis": {
                "@odata.id": "/redfish/v1/Chassis"
        },
        "Description": "The service root for all Redfith requests on this host"
        "EventService": {
                "@odata.id": "/redfish/v1/EventService"
        },
        "Id": "RootService",
        <<Some contents are omitted>
}
```

スマフォアプリ **HDM Mobile**(iosとandroid)

HDMの接続されているLANに接続できるWiFiアクセスポイントの電波にスマフォでWiFi接続することで
HDMにアクセスが可能となります









01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

H3C iFIST(integrated Fast Intelligent Scalable Toolkit)概要

1.　障害検知と診断

iFISTはリアルタイムでネットワークやデバイスの状況を監視し、異常を検知します。

・自動障害検知：ネットワーク内でのパフォーマンス低下や障害を即座に識別します。

・問題の根本原因解析（RCA）：AIやデータ分析技術を活用し、問題の原因を特定します。

2.　インテリジェントなトラブルシューティング

・問題解決のためのガイダンスを提供し、迅速に対応可能です。

・デバイスログの自動収集・解析により、運用負担を軽減します。

3.　ネットワークの健全性評価

・過去のデータを分析して、ネットワーク全体のパフォーマンスを評価します。

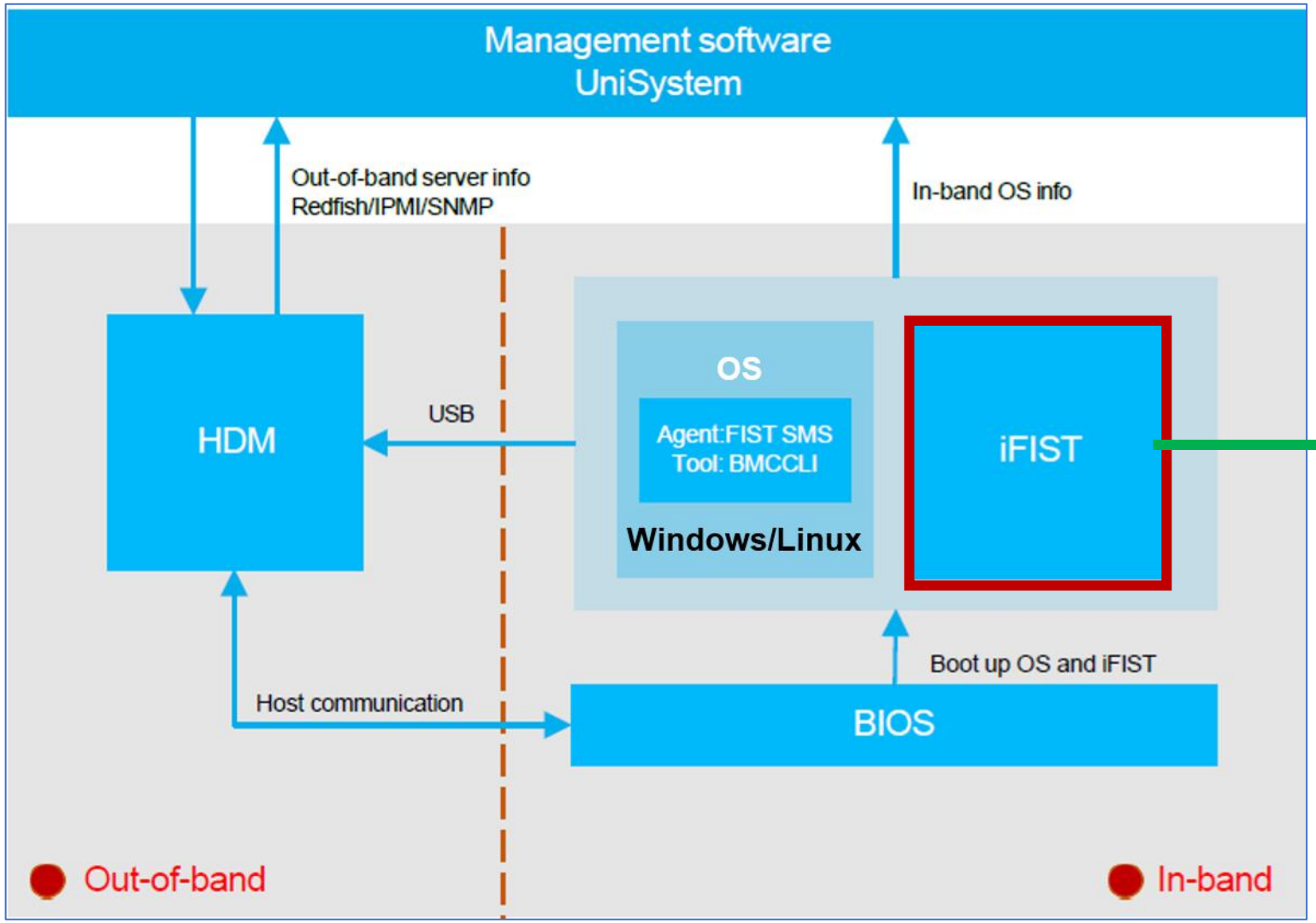
・将来的な問題の発生を予測し、予防措置を推奨します。

4.　統合されたダッシュボード

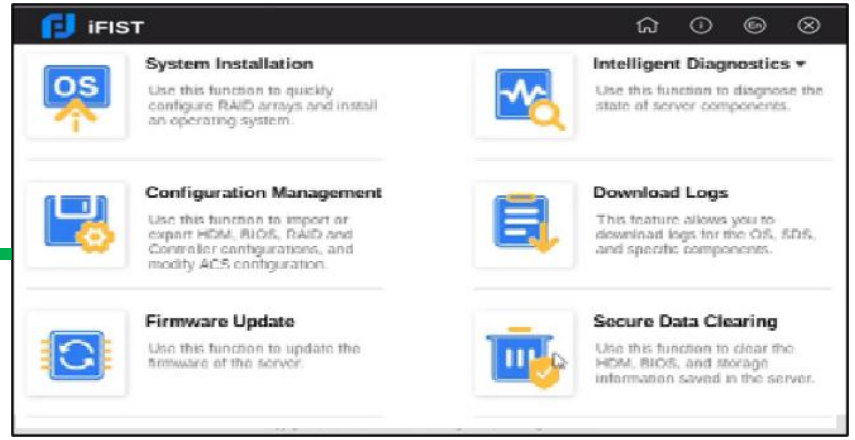
・視覚的なデータ表示で、ネットワークの状態を一目で把握可能。

・シンプルで直感的な操作インターフェースを提供します。

iFISTのアーキテクチャー



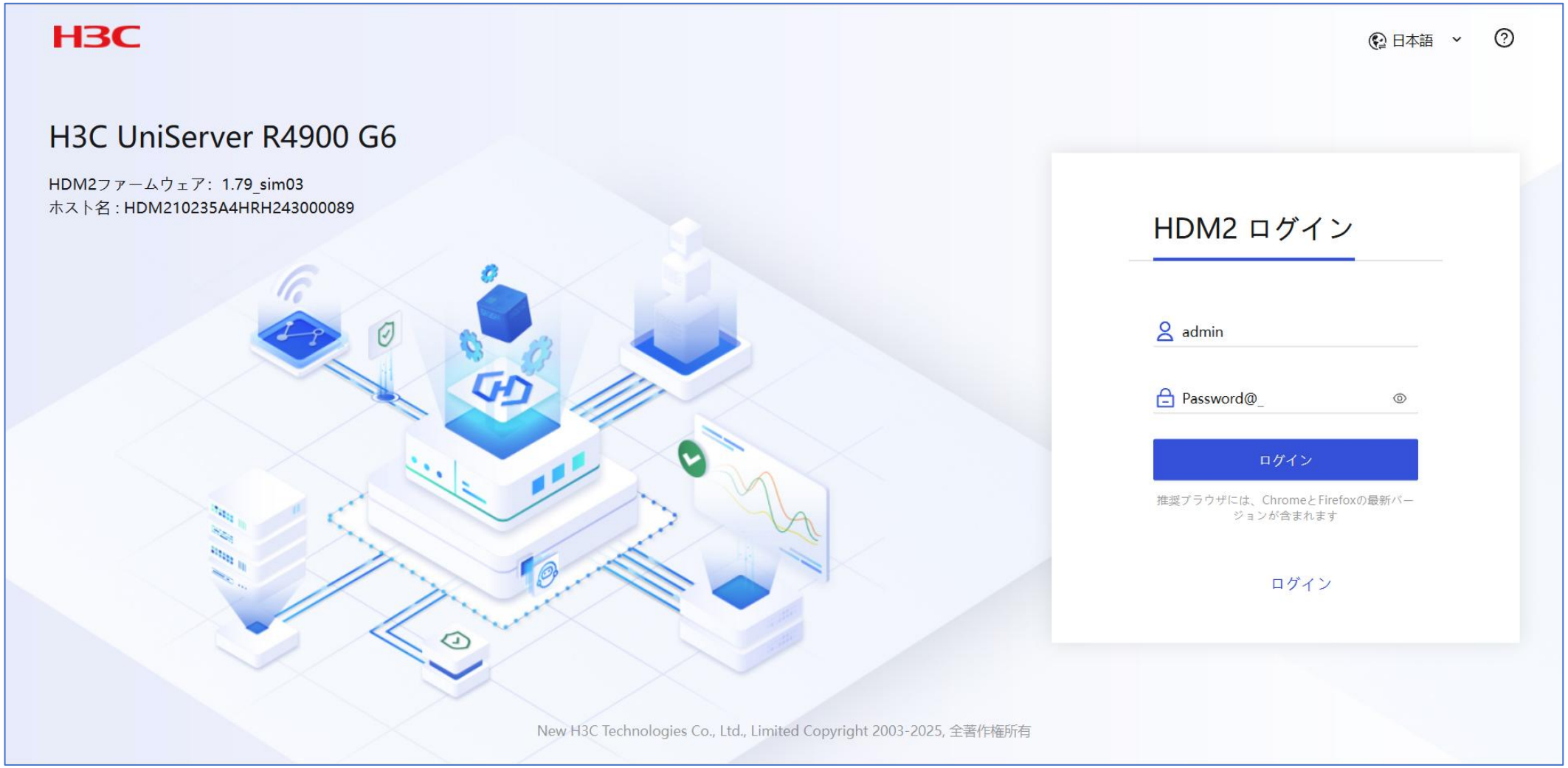
iFIST(構成管理や診断)



iFISTとUnisystemのソフトウェアの違い

ソフトウェア	インストール	機能
iFIST	**H3Cサーバーのハードウェア上のプロセッサーに組み込まれている**ため、マニュアルでインストールする必要はありません。	iFISTで管理できるのは、**ローカルサーバーのみ**です。
Unisystem	**管理デバイス**(PC、仮想マシンまたはサーバー)**にマニュアルでインストールする必要**があります。	Unisystemは**複数のサーバーを管理**できます。

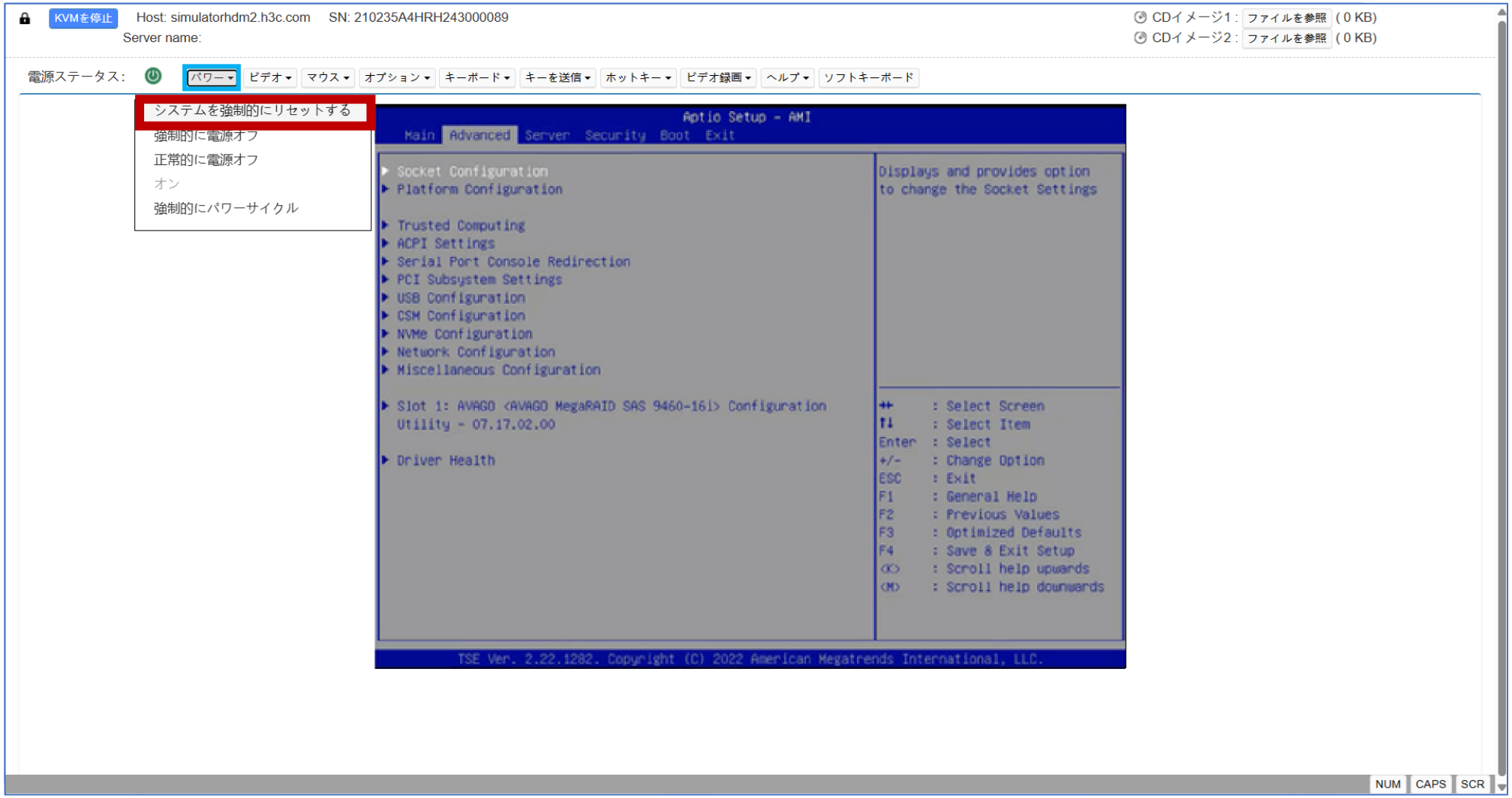
HDMホームページ経由のログイン



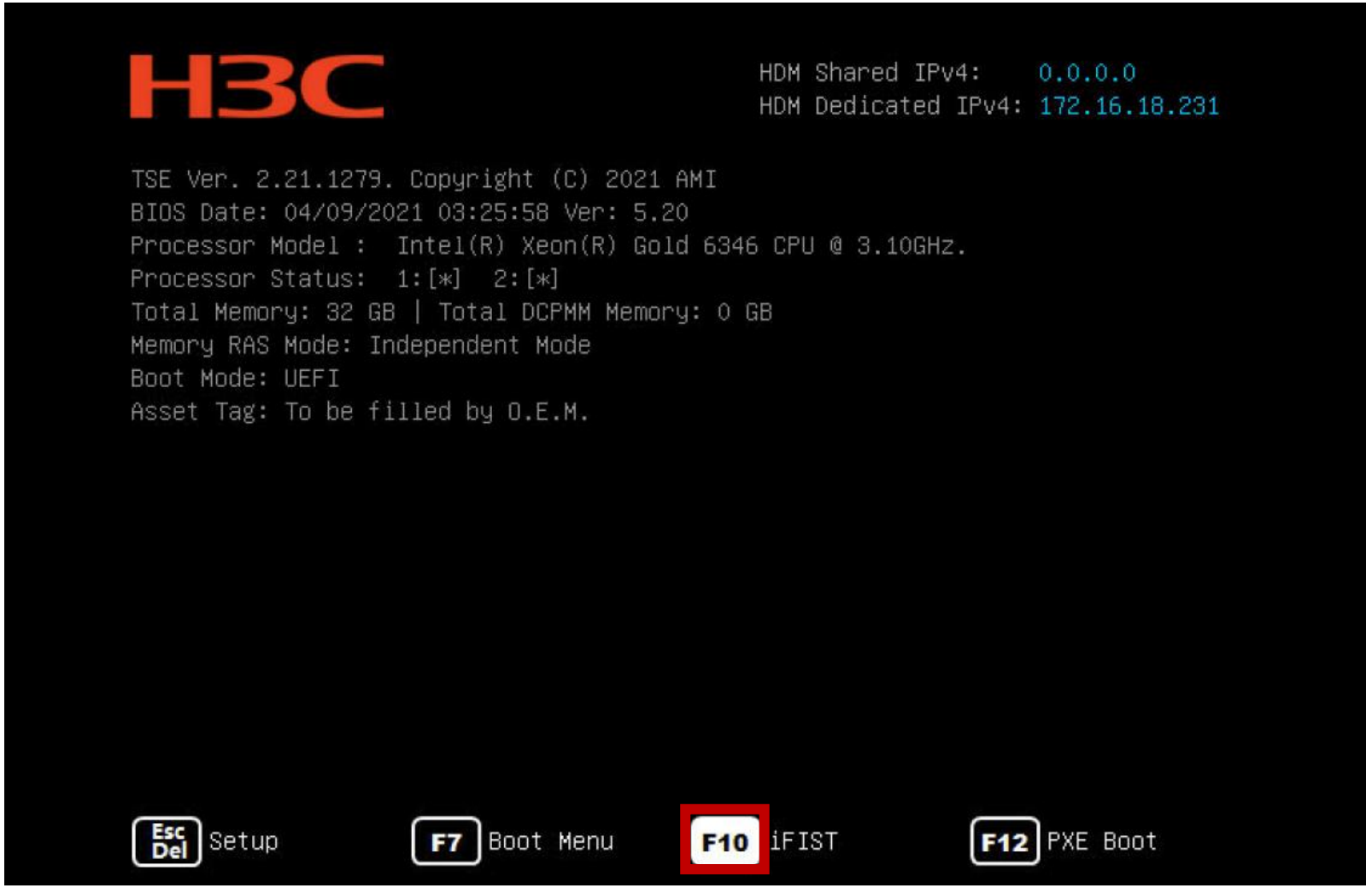
HDMホームページ経由のログイン ➡ スタート H5 KVM



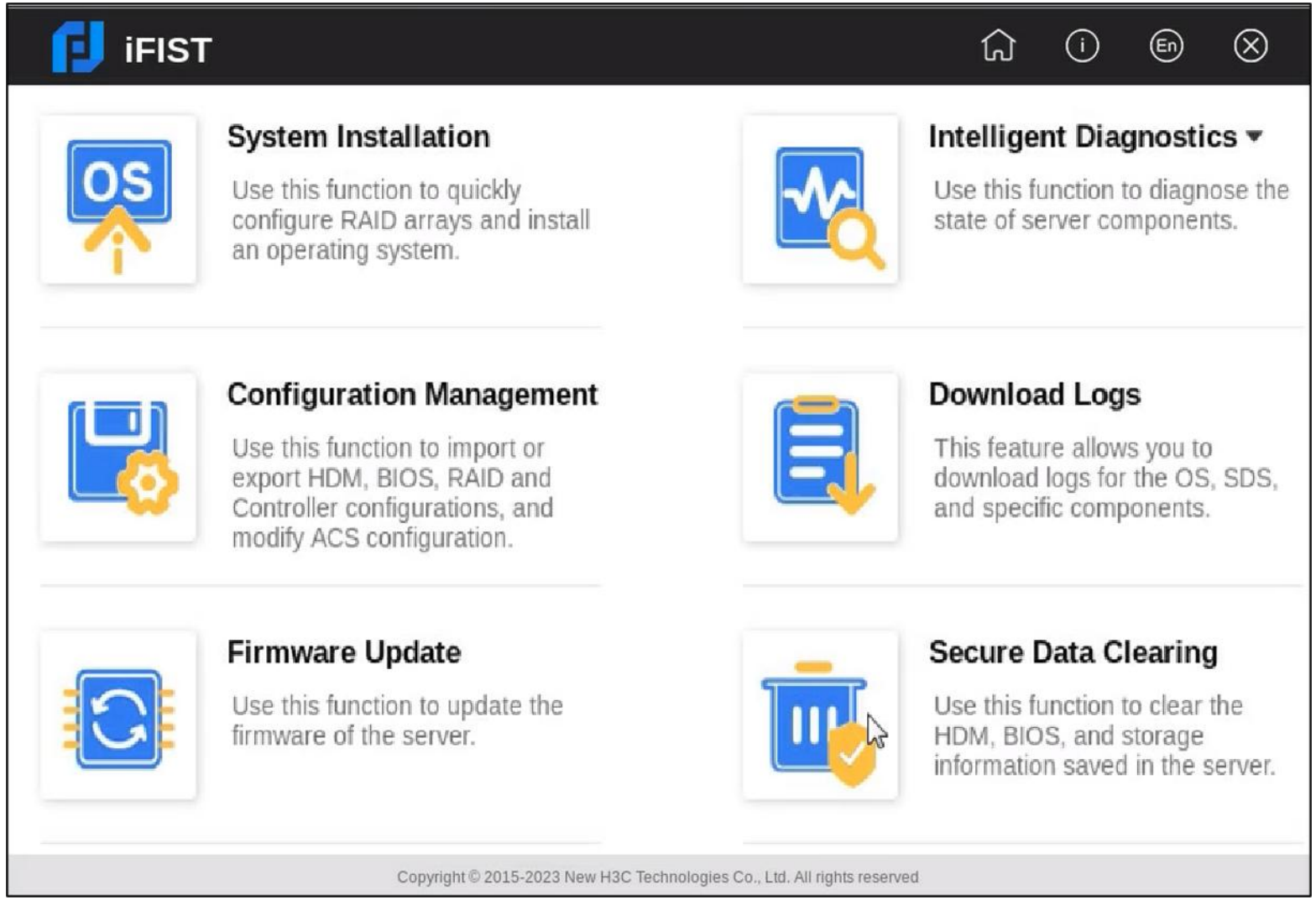
KVMページ ➡ パワー ➡ システムを強制的にリセットする



BIOS起動画面 ➡ F10をクリック



iFISTホームページ



- システムのインストール
- インテリジェントな診断
- コンフィギュレーション管理
- ログのダウンロード
- ファームウェアの更新
- 安全なデータ消去

iFIST機能一覧

コンフィギュレーション管理
この機能を使用して、次のタスクを実行します。
•**Import configuration**: USBフラッシュドライブ内のHDM、BIOSまたはRAID構成ファイルをシステムにインポートして、既存の構成を上書きします。USBフラッシュドライブ内のコントローラー構成ファイルをストレージコントローラーにインポートして、既存の構成を上書きすることもできます。
•**Export configuration**: 現在のHDM、BIOS、RAID、またはコントローラー設定をエクスポートし、コンフィギュレーションファイルを生成して、USBフラッシュドライブのルートディレクトリにあるiFIST/ConfManageディレクトリに保存します。
•**ACS(Auto Configuration Server) configuration**: ACS機能およびACS制御を設定します。

ログのダウンロード
この機能を使用して、OSログ、SDSログ、システム運用ログ、および特定のコンポーネントをダウンロードし、サーバーに挿入されているUSBフラッシュドライブのiFIST/LogDownloadディレクトリに保存します。

ファームウェアの更新
この機能を使用して、サーバーおよびコンポーネント(**HDM、BIOS、CPLD、ストレージコントローラー、ネットワークアダプター、ドライブ**など)のファームウェアを更新します。

安全なデータ消去
この機能を使用して、サーバーに保存されているHDM、BIOS、およびストレージデータをクリアし、ユーザーデータの侵害を回避します。

iFIST機能一覧

システムのインストール

従来、管理者はサーバーにオペレーティングシステムをインストールするために、さまざまな機能ページにアクセスして複雑な一連のタスクを完了する必要がありました。
iFISTは、OSインストールタスクをOSインストールウィザードに統合し、統一されたインターフェイスから段階的にインストールプロセスを案内します。OSインストールウィザードは、操作の複雑さと設定ミスの可能性を軽減します。
iFISTのOSインストールウィザードを使用して、RAIDアレイの設定、ドライバーのインストール、および設定ファイルのエクスポートとインポートを行うことができます。インストールの設定が完了すると、iFISTは自動的にオペレーティングシステムをサーバーにインストールします。

インテリジェントな診断

この関数を使用して、次のタスクを実行します。
•**Server Diagnostics**: サーバー上のコンポーネントをスキャンして、コンポーネントベースのパフォーマンスおよび正常性診断の統計を収集します。これにより、サーバーのトラブルシューティングが容易になり、サーバーの使用中に予期しない問題が発生するリスクが軽減されます。サーバー診断は、CPU、PSU、ファン、HDM、メモリー、およびPCIeデバイスなど、サーバー上のさまざまなコンポーネントの診断をサポートします。
•**Memory Smart-Test**: BIOSに組み込まれたメモリーテストツールを使用して、POSTメモリー初期化段階でメモリーをテストおよび修復します。

OSの自動インストール(概念)

OSの手動インストールプロセス中に、次の問題が発生することがよくあります。

• ストレージコントローラードライバーがOSイメージに統合されていないため、インストールプロセス中にハードディスクドライブが認識されません。

• OSのインストールプロセス中に手動による介入(インストールパラメータの設定など)が必要になるため、O&M時間が長くなります。

• オペレーティングシステムのインストール後、ユーザーは必要なドライバを手動でインストールする必要があります。

上記の問題に対処するために、iFISTでは、サーバーへのOSの自動インストールを提供しています。
ユーザーは、iFIST WebインターフェイスですべてのOSインストールパラメータを構成できます。これにより、手動で操作することなく、サーバーにオペレーティングシステムが自動的にインストールされます。

OSの自動インストール（機能概要）

Configure system settingsページを開くと、iFISTは次の操作を実行します。

1. **ユーザー定義のイメージソースに従って、インストールするOSイメージのタイプを決定します。**サポートされているイメージソースには、CD(物理CDまたはHDM仮想メディア)およびUSBフラッシュドライブが含まれます。

2. **ユーザーが選択したレポジトリ(CDまたはUSBフラッシュドライブ)とiFIST内蔵ドライバーを識別します。次に、iFISTは、OSに一致し、レポジトリにインストールできるドライバーをConfigure system settingsページに表示します。**リポジトリはH3Cによってリリースされ、サーバ用のドライバとファームウェアのインストールパッケージのバンドルが含まれています。

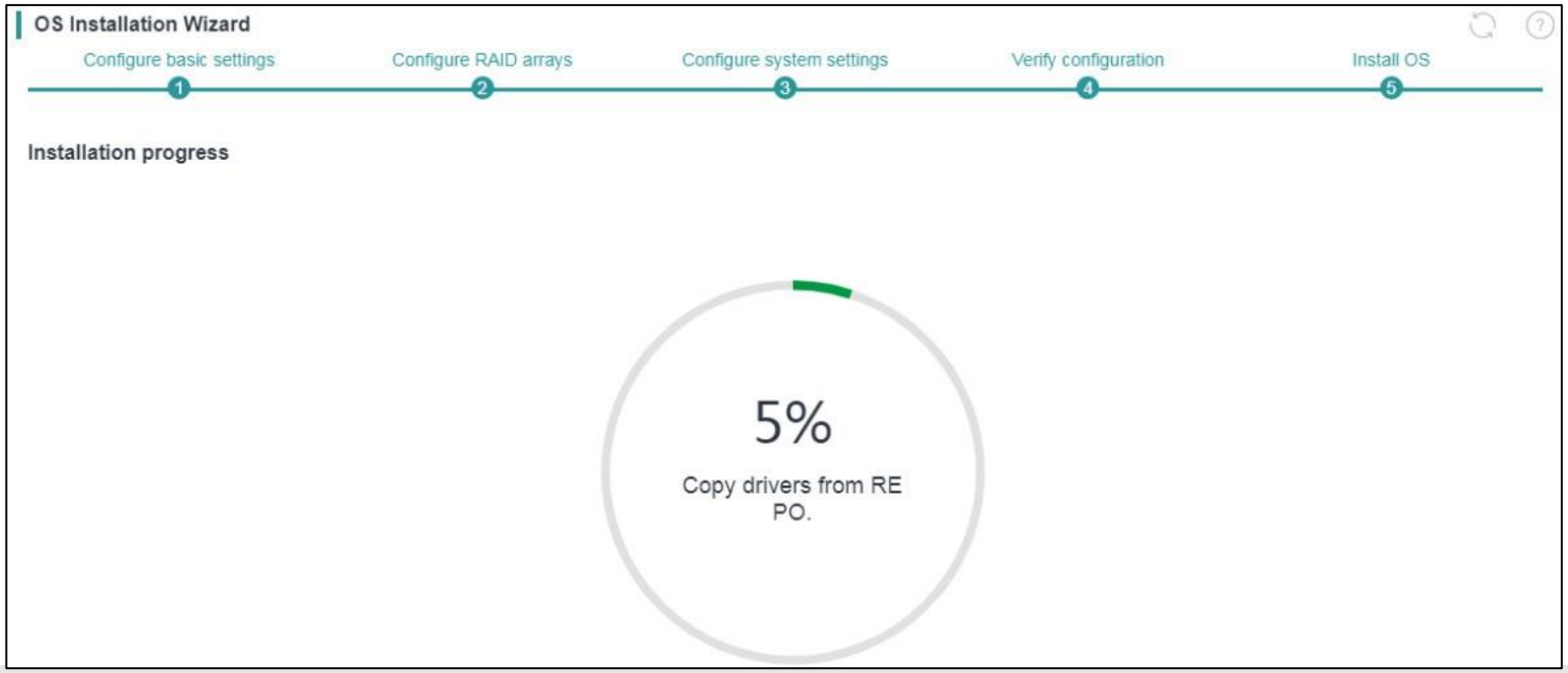
このページで構成可能なOSインストールパラメータは、OSタイプによって異なります。たとえば、Windowsオペレーティングシステムをインストールするには、次のタスクを実行します。
- **インストールするドライバを選択**します。
- **インストールするOSイメージファイルを選択**します。たとえば、イメージソースに2つのイメージファイル(Standard EditionとDatacenter Edition用のWindows Server 2012 R2 ISOファイル)が含まれている場合、どちらをインストールするかを選択できます。
- **オペレーティングシステムのホスト名、パスワード、およびキーを指定**します。
- **OSインストールのターゲットドライブ(物理または論理)を指定し、ドライブ容量を設定します。**ランダムなドライブにOSをインストールするのとは対照的に、指定したドライブにオペレーティング・システムをインストールすると、データ損失のリスクを軽減できます。

OSの自動インストール（サポートされるOS）

- Red Hat Enterprise Linux
- SuSE Linux Enterprise Server
- CentOS
- Ubuntu Server
- VMware ESXi
- CAS
- Oracle Linux
- Windows Server(Windows Core OSを除く)

OSの自動インストール（手順）

各OSベンダーは、Linux用のks.cfgファイルベースのメカニズムやWindows用のunattend.xmlファイルベースのメカニズムなど、**独自の自動OSインストールメカニズムを実装しています。ベンダー固有の自動OSインストールメカニズムの詳細な分析に基づいて、iFISTは自動OSインストール機能を提供し、ほとんどの主要なオペレーティングシステムの自動インストールを可能にします。**この機能は、互換性のあるストレージコントローラドライバがないために発生するハードドライブ認識の問題も解決します。iFISTの自動OSインストール機能は、OSインストールプロセスを大幅に高速化し、サーバのO&Mコストを削減します。



OSの自動インストール

Linux用のks.cfgの例

```
# 1. システム設定（コマンドセクション）
# ----------------------------------------
# インストールモード（新規インストール、テキストモード）
install
text
# インストールメディアの指定（CD-ROM / ISOイメージ）
cdrom
# 言語とキーボードの設定
lang ja_JP.UTF-8
keyboard jp106
# ネットワークの設定（DHCPで自動設定の例）
network --bootproto=dhcp --device=eth0 --onboot=yes
# タイムゾーンの設定
timezone Asia/Tokyo --isUtc
# ルートパスワードの設定（プレーンテキスト、または暗号化文字列）
rootpw --plaintext YourSecurePassword123
# ファイアウォールとSELinuxの設定
firewall --enabled --ssh
selinux --enforcing
# ディスクパーティションの初期化と自動構築
bootloader --location=mbr
clearpart --all --initlabel
autopart
# 2. インストールするパッケージの指定
# ----------------------------------------
%packages
@core              # 最小限のシステム環境（Minimal Install）
vim-enhanced       # 追加で入れたいパッケージ
chrony             # 時刻同期ツール
%end
# 3. インストール直後に実行するスクリプト（任意）
# ----------------------------------------
%post --log=/root/ks-post.log
# 一般ユーザーの追加
useradd myuser
echo "password123" | passwd --stdin myuser
# SSHの設定変更（例：Rootログインの禁止など）
sed -i 's/#PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config
%end
```

OSの自動インストール
Windows用のunattend.xmlの例

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <!-- 1. 初期インストーラー（windowsPE）の設定 -->
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS" xmlns:wcm="http://microsoft.com" xmlns:xsi="http://w3.org">
            <!-- 言語とキーボードを日本に設定 -->
            <SetupUILanguage>
                <UILanguage>ja-JP</UILanguage>
            </SetupUILanguage>
            <InputLocale>0411:00000411</InputLocale>
            <SystemLocale>ja-JP</SystemLocale>
            <UILanguage>ja-JP</UILanguage>
            <UserLocale>ja-JP</UserLocale>
        </component>
        <component name="Microsoft-Windows-Setup" processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS" xmlns:wcm="http://microsoft.com" xmlns:xsi="http://w3.org">
            <!-- ライセンス条項への同意 -->
            <UserData>
                <AcceptEula>true</AcceptEula>
                <!-- 必要に応じて汎用プロダクトキーを入力（任意） -->
                <!-- <ProductKey><Key>XXXXX-XXXXX-XXXXX-XXXXX-XXXXX</Key></ProductKey> -->
            </UserData>
        </component>
    </settings>
```

OSの自動インストール
Windows用のunattend.xmlの例(続き)

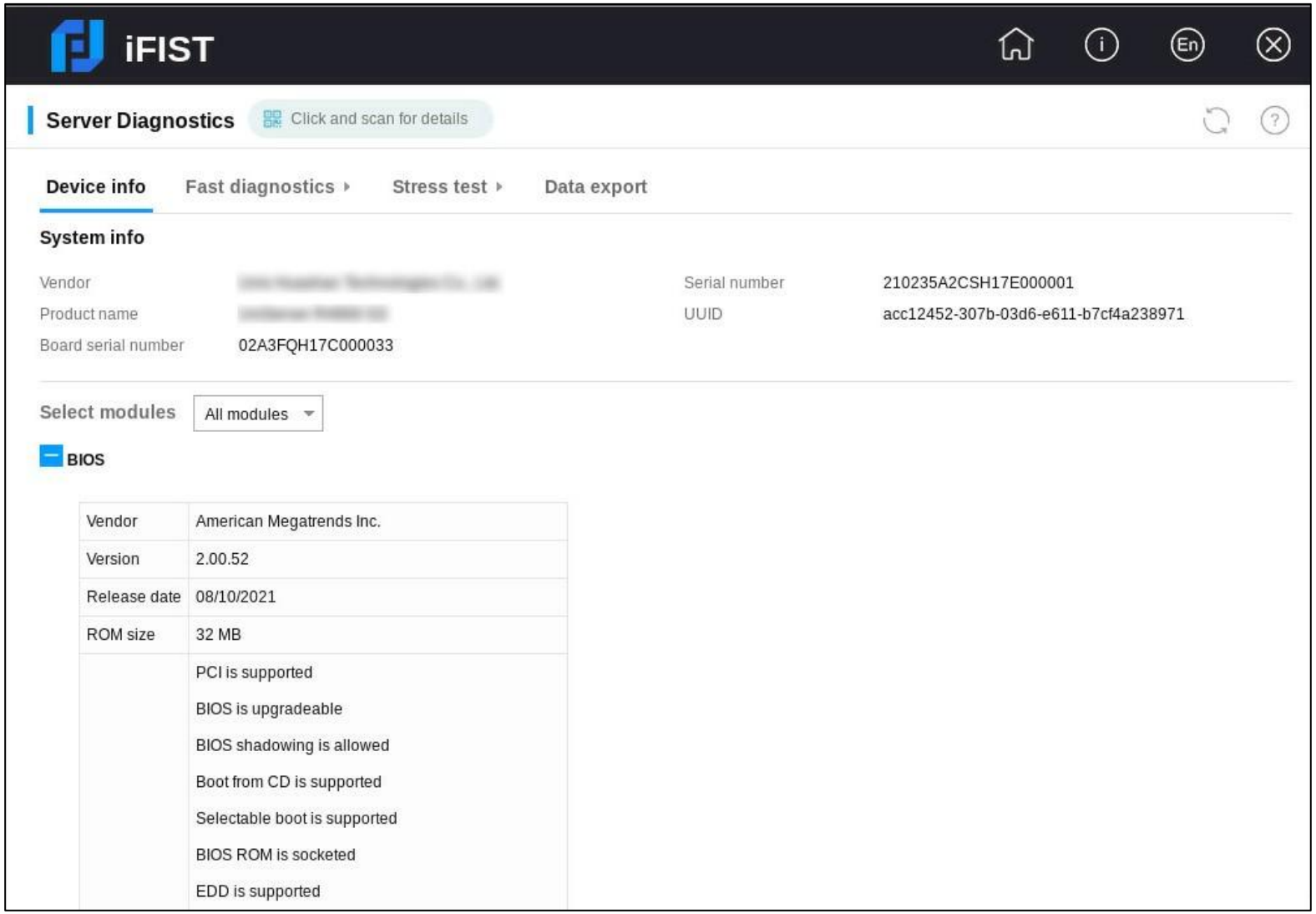
```
    <!-- ローカルアカウントの作成 -->
        <UserAccounts>
          <LocalAccounts>
            <LocalAccount wcm:action="add">
              <!-- ユーザー名（例: AdminUser） -->
              <Name>AdminUser</Name>
              <Group>Administrators</Group>
              <DisplayName>Administrator</DisplayName>
              <Password>
                <!-- パスワード（例: P@ssword123） -->
                <Value>P@ssword123</Value>
                <PlainText>true</PlainText>
              </Password>
            </LocalAccount>
          </LocalAccounts>
        </UserAccounts>
        <!-- 初回のみ自動ログインする設定 -->
        <AutoLogon>
          <Password>
一部省略
        </AutoLogon>
      </component>
    </settings>
</unattend>
```

OSの自動インストール（手順）

ドライバの自動インストール

サーバーにオペレーティング・システムをインストールした後、iFISTはオペレーティングシステムに必要なドライバのインストールに進むことができます。ユーザーは、ドライバパッケージを含むリポジトリをサーバーにマウントし、OSインストール設定でインストールするドライバを選択するだけです。その後、**OSのインストールが完了すると、iFISTは自動的にドライバをインストールします**。

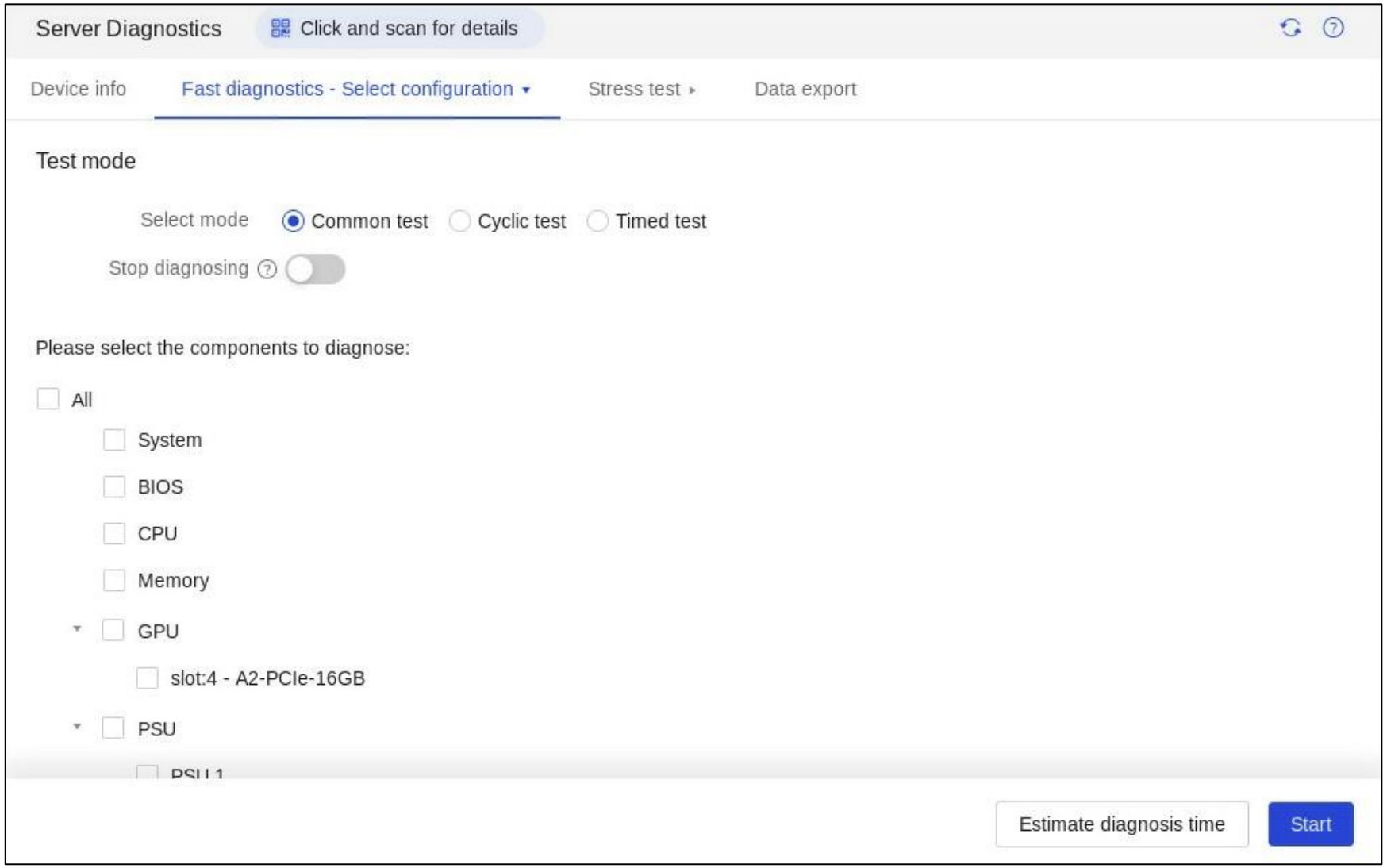
iFIST:インテリジェントな診断



サーバー診断機能は、サーバーモジュールをスキャンして統計情報を収集し、モジュールごとのパフォーマンスと健全性の診断を行います。これにより、サーバーのトラブルシューティングが容易になり、サーバー使用中の予期せぬ問題発生のリスクを軽減できます。

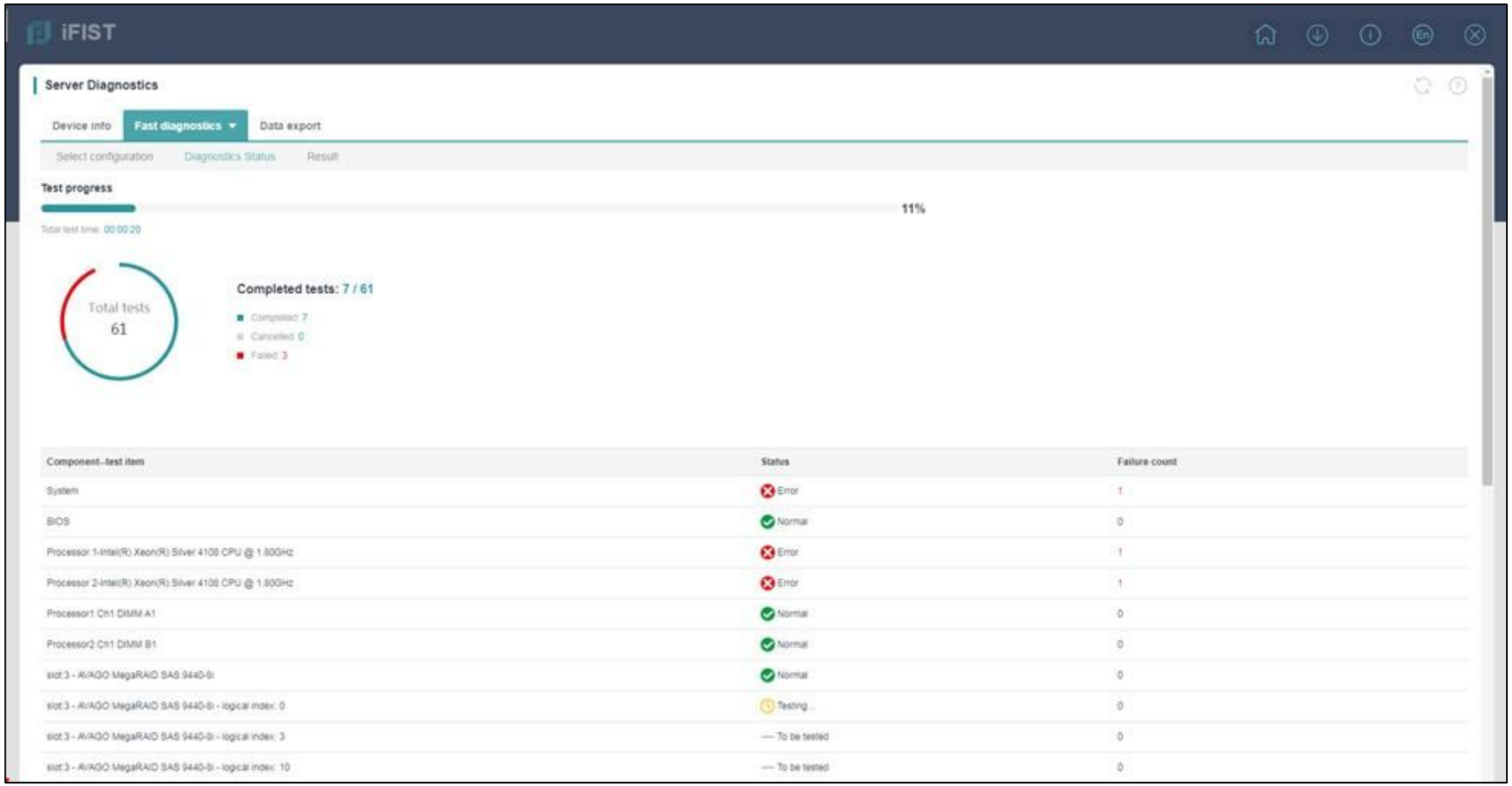
サーバー診断機能は、BIOS、CPU、メモリ、ハードディスク、ストレージコントローラ、論理ドライブ、ネットワークアダプタ、GPU、その他のPCIeデバイス、電源ユニット、ファン、温度など、サーバー上のさまざまなモジュールの診断をサポートします。

iFIST:高速診断の実行



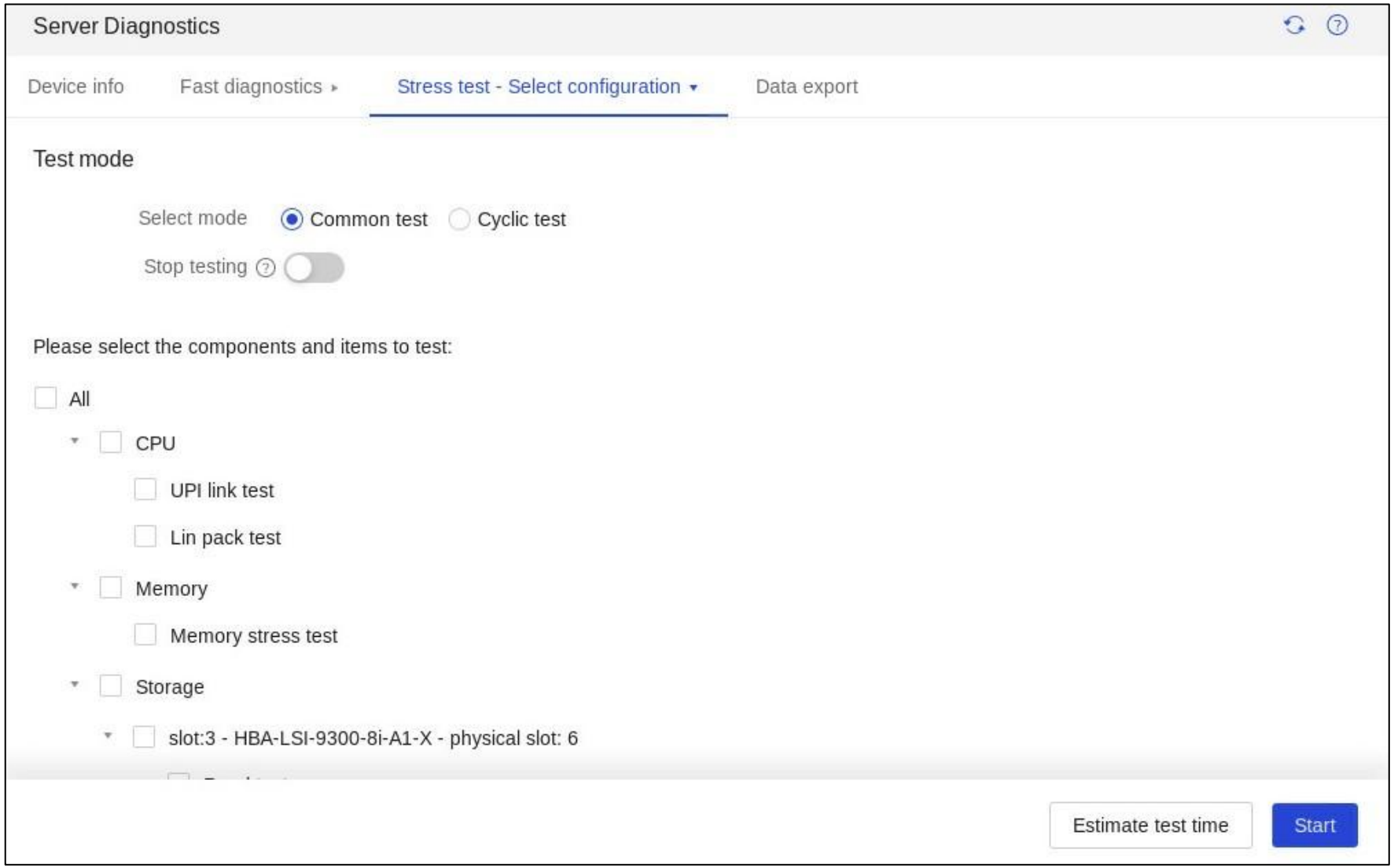
この機能を使用すると、選択したサーバーモジュールの包括的な動作状況と健全性チェックを実行できます。
診断プロセスで検出された障害があれば、トラブルシューティングと修正のための手順が提供されます。

iFIST:高速診断の実行結果



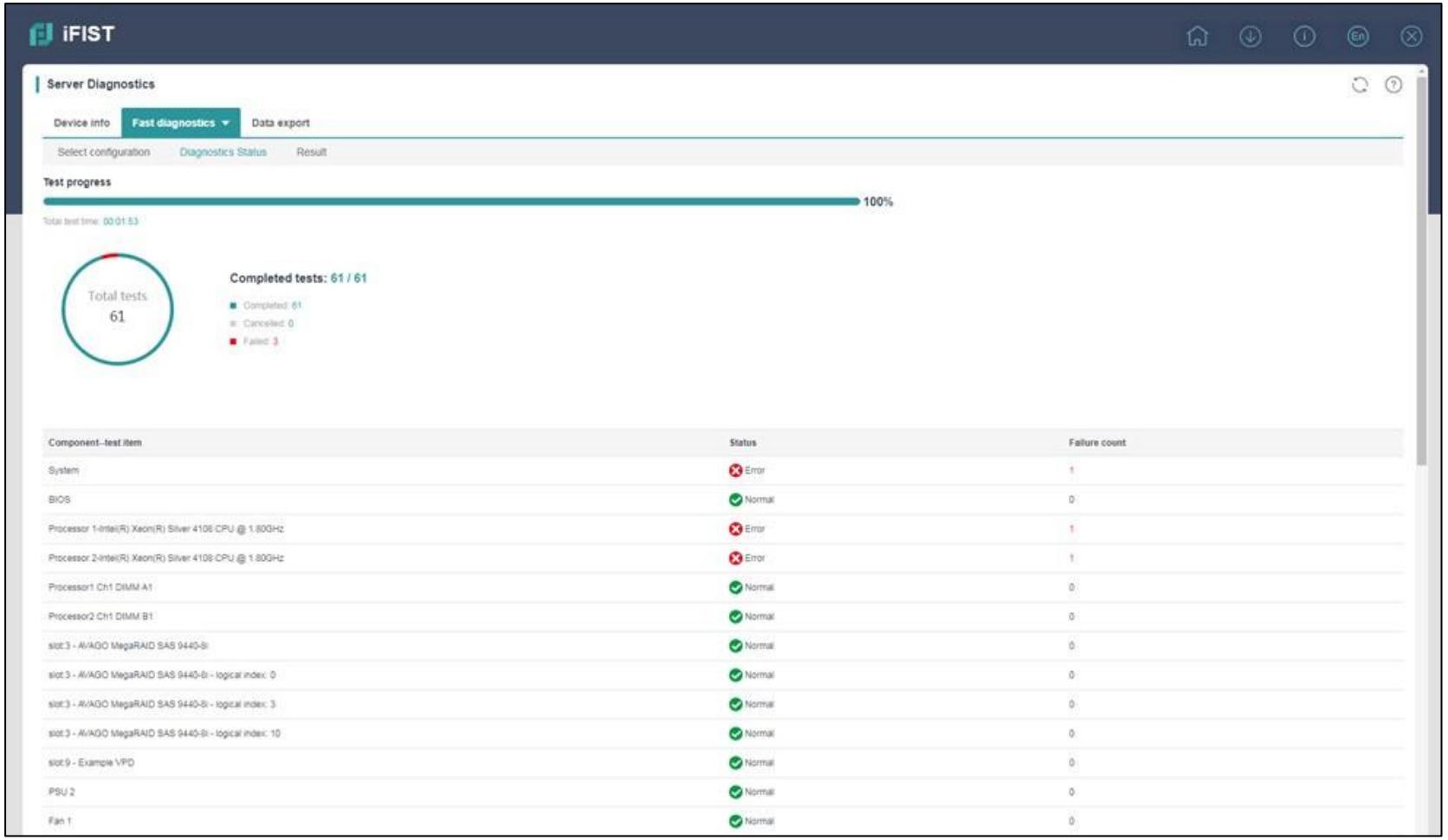
iFISTは、診断プロセスの開始時に、診断ステータスページを開きます。このページには、**進行中の診断テストに関する情報（テストの進行状況、テスト統計の概要、モジュール固有のテスト結果など）が表示されます**。

iFIST: 負荷テストの実行



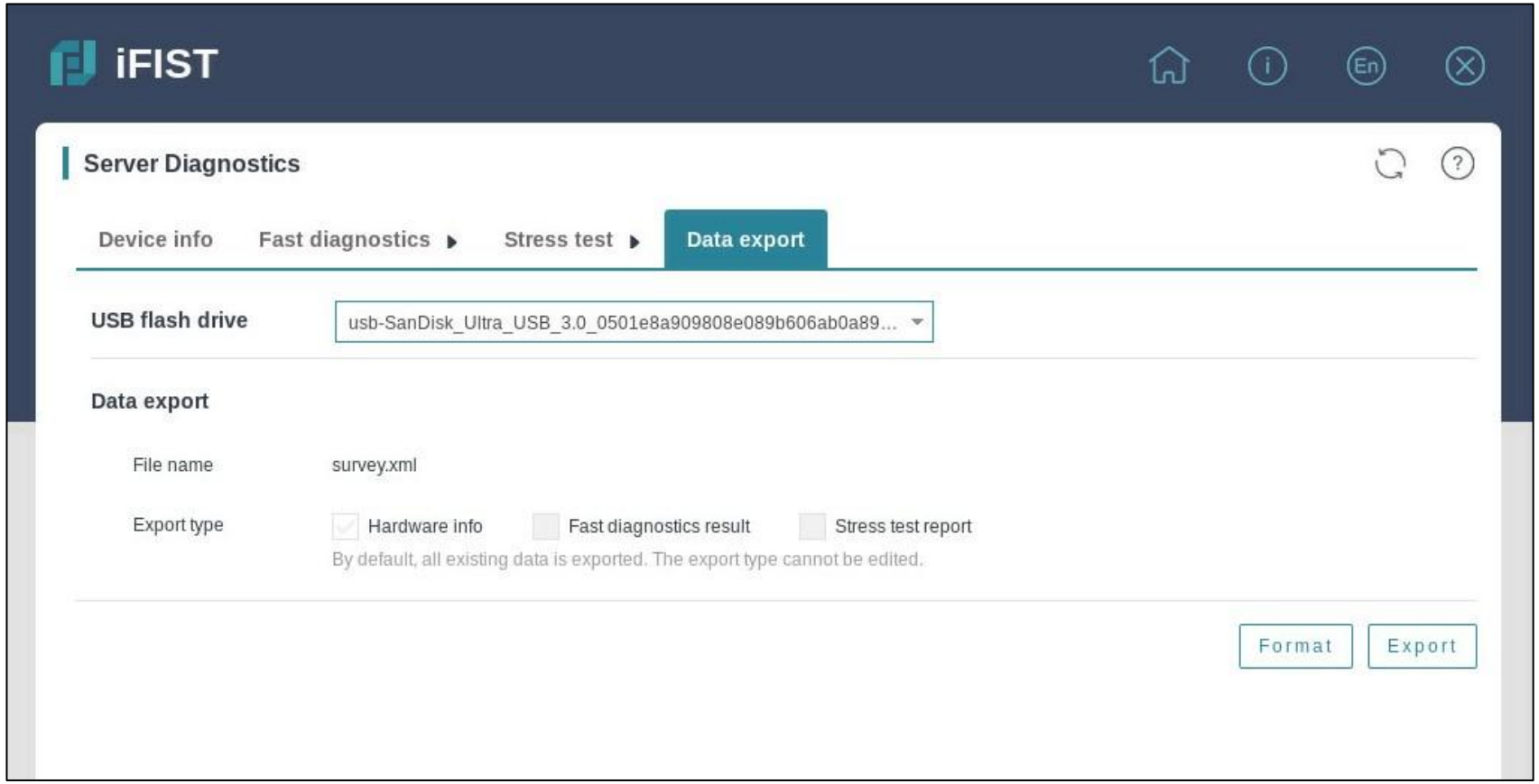
この機能を使用すると、選択したサーバーコンポーネントに対してストレステストを実行できます。**テスト結果には検出された問題と、必要に応じて問題の修正に関する推奨事項が表示されます。**テスト前にテスト時間の見積もりを選択できるため、必要に応じてテスト時間をより適切に調整できます。

iFIST: 負荷テストの実行結果



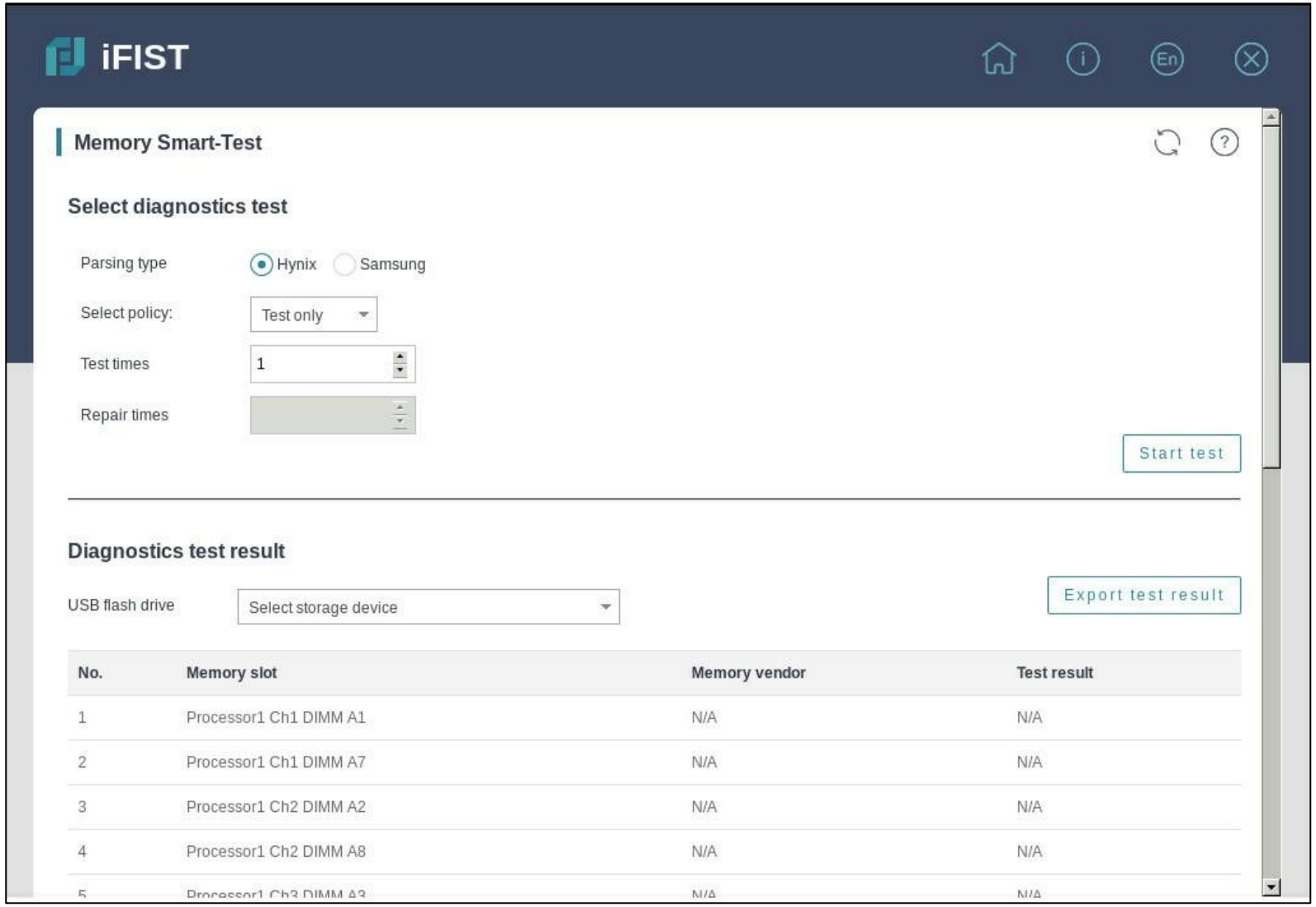
高速診断プロセスが完了したら、**Result**をクリックして診断結果を表示します。
Resultタブには、各コンポーネントのテスト結果が表示され、図2に示すように、テスト結果が**Error**の場合は、失敗の理由と推奨される修正方法が表示されます。

iFIST: データのエクスポート



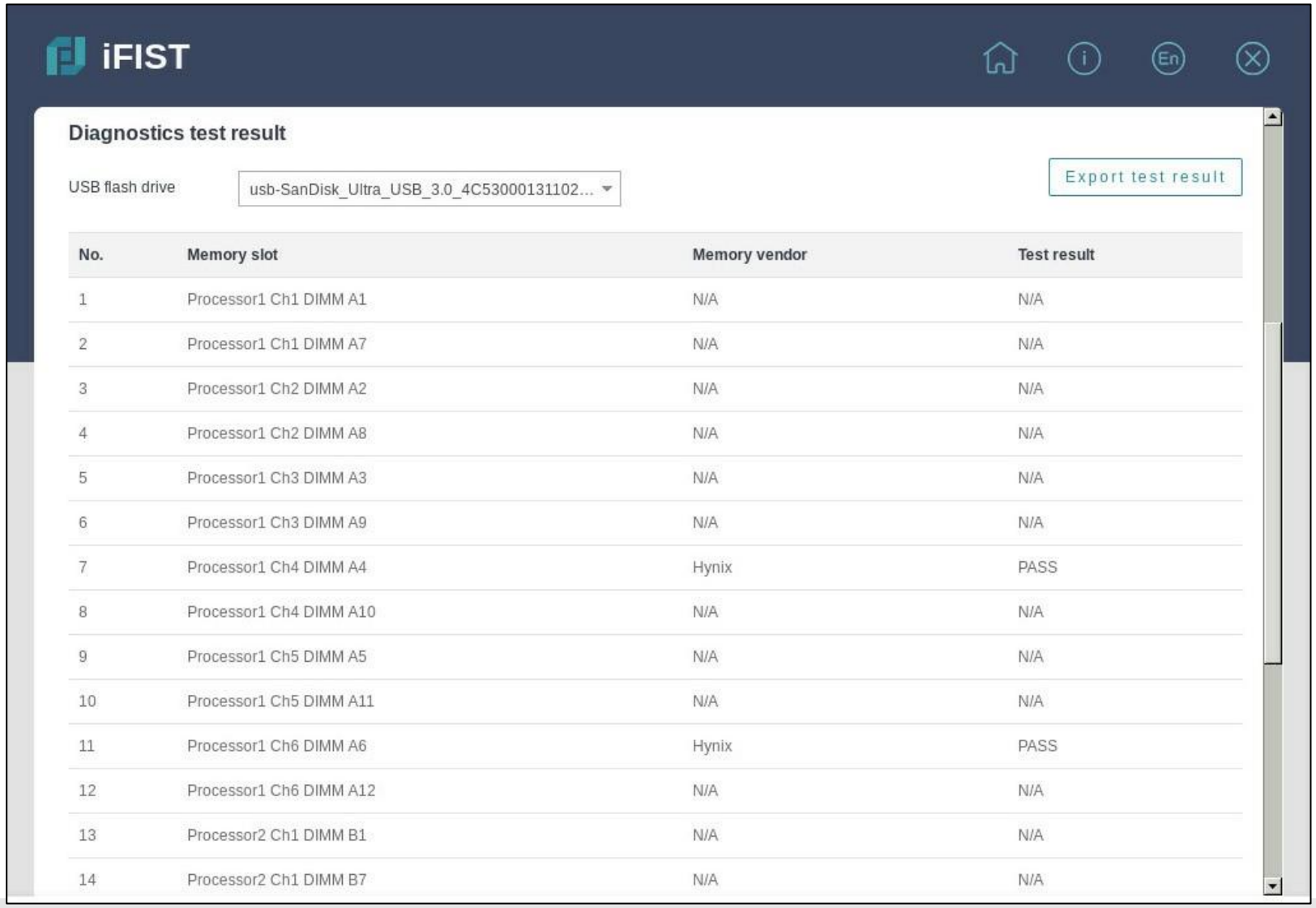
サーバーモジュール情報、サーバー診断データ、および操作ログデータをUSBフラッシュドライブにエクスポートして、さらに分析することができます。

iFIST: メモリースマートテスト



メモリースマートテスト機能は、BIOSに組み込まれたメモリーテストツールを使用して、POSTメモリー初期化段階でメモリーをテストします。現在のソフトウェアバージョンでは、Hynix、Samsung、およびMicronメモリーチップのみがサポートされています。テスト後、テスト結果をiFISTで確認できます。

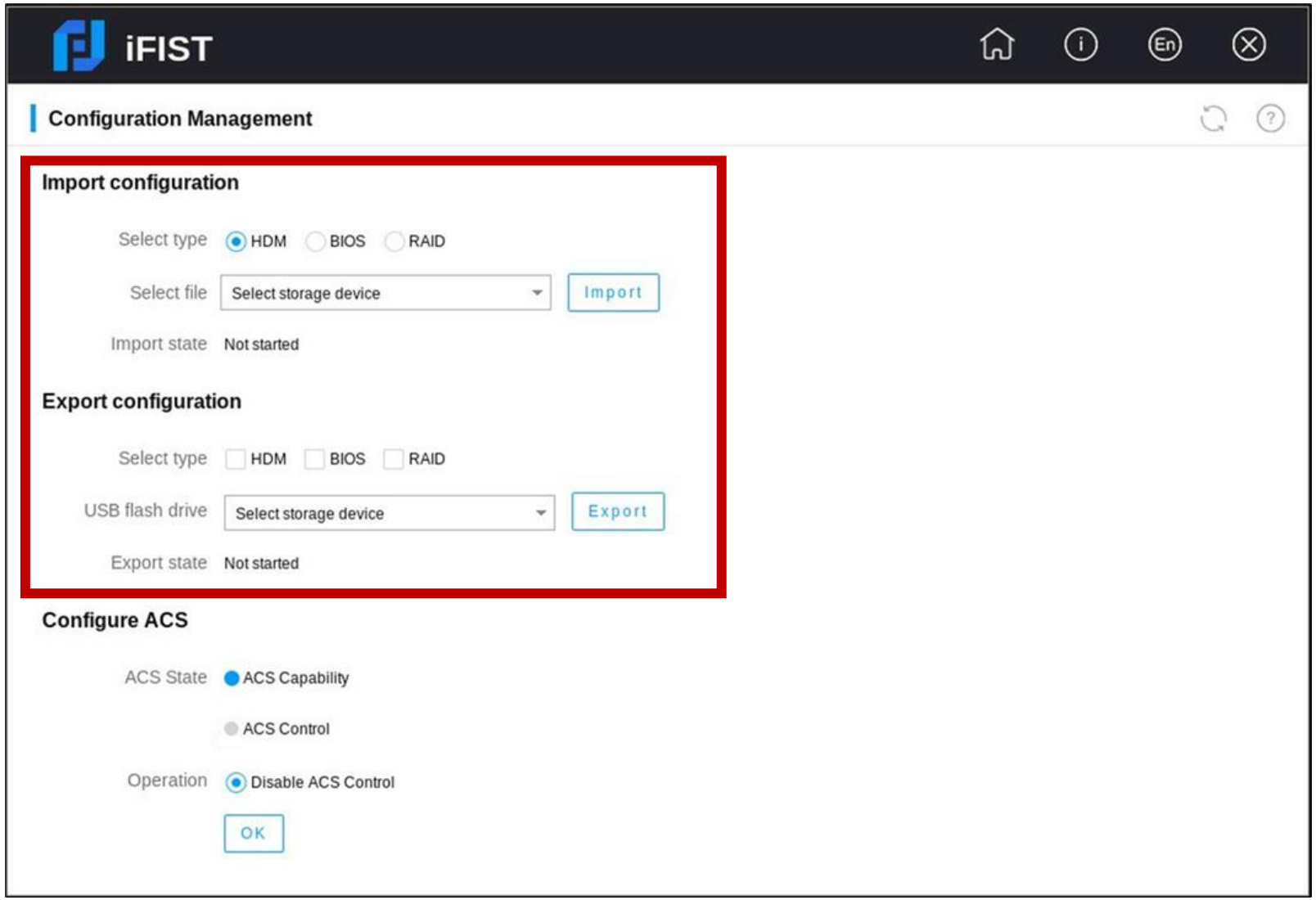
iFIST: メモリースマートテストの実行結果



No.	Memory slot	Memory vendor	Test result
1	Processor1 Ch1 DIMM A1	N/A	N/A
2	Processor1 Ch1 DIMM A7	N/A	N/A
3	Processor1 Ch2 DIMM A2	N/A	N/A
4	Processor1 Ch2 DIMM A8	N/A	N/A
5	Processor1 Ch3 DIMM A3	N/A	N/A
6	Processor1 Ch3 DIMM A9	N/A	N/A
7	Processor1 Ch4 DIMM A4	Hynix	PASS
8	Processor1 Ch4 DIMM A10	N/A	N/A
9	Processor1 Ch5 DIMM A5	N/A	N/A
10	Processor1 Ch5 DIMM A11	N/A	N/A
11	Processor1 Ch6 DIMM A6	Hynix	PASS
12	Processor1 Ch6 DIMM A12	N/A	N/A
13	Processor2 Ch1 DIMM B1	N/A	N/A
14	Processor2 Ch1 DIMM B7	N/A	N/A

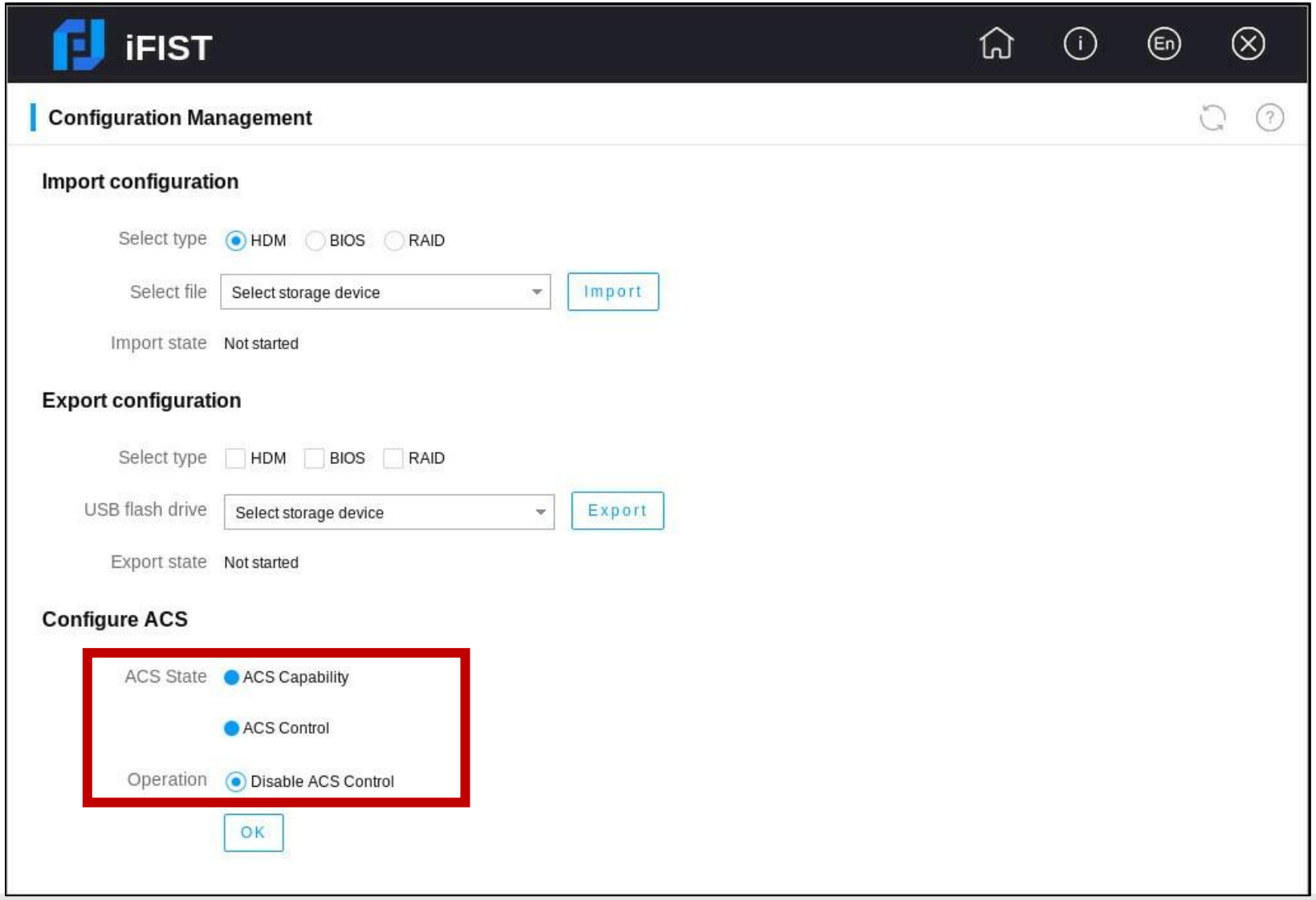
現在のソフトウェアバージョンでは、診断テスト結果は、FAT32またはNTFSファイルシステムを使用してフォーマットされたUSBフラッシュドライブにエクスポートできます。

iFIST: コンフィギュレーション管理



- **Import configuration** : USBフラッシュドライブ内のHDM、BIOSまたはRAID構成ファイルをシステムにインポートして、既存の構成を上書きします。USBフラッシュドライブ内のコントローラー構成ファイルをストレージコントローラーにインポートして、既存の構成を上書きすることもできます。
- **Export configuration**: 現在のHDM、BIOS、RAID、またはコントローラー設定をエクスポートし、コンフィギュレーションファイルを生成して、USBフラッシュドライブのルートディレクトリにあるiFIST/ConfManageディレクトリに保存します。
- **ACS configuration**: ACS機能およびACS制御を設定します。

iFIST: ACS(Auto Configuration Server)の設定



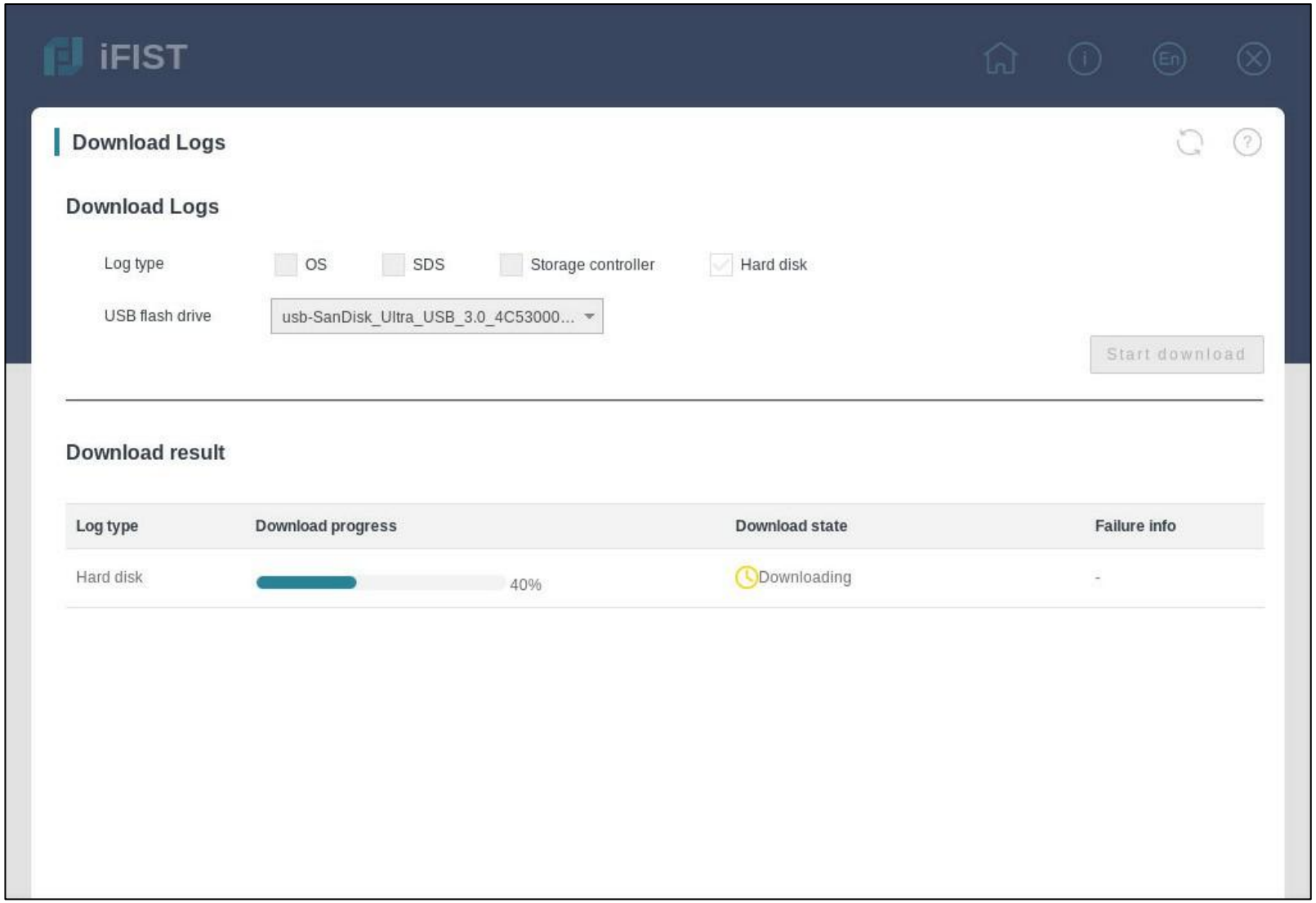
ACS機能の活用例

サーバーの一括構成：複数のサーバーに対して、事前に用意した構成ファイルを用いて一括で設定を適用できます。

迅速な再構成：サーバーの再展開や設定変更時に、保存された構成ファイルを使用して迅速に再構成が可能です。

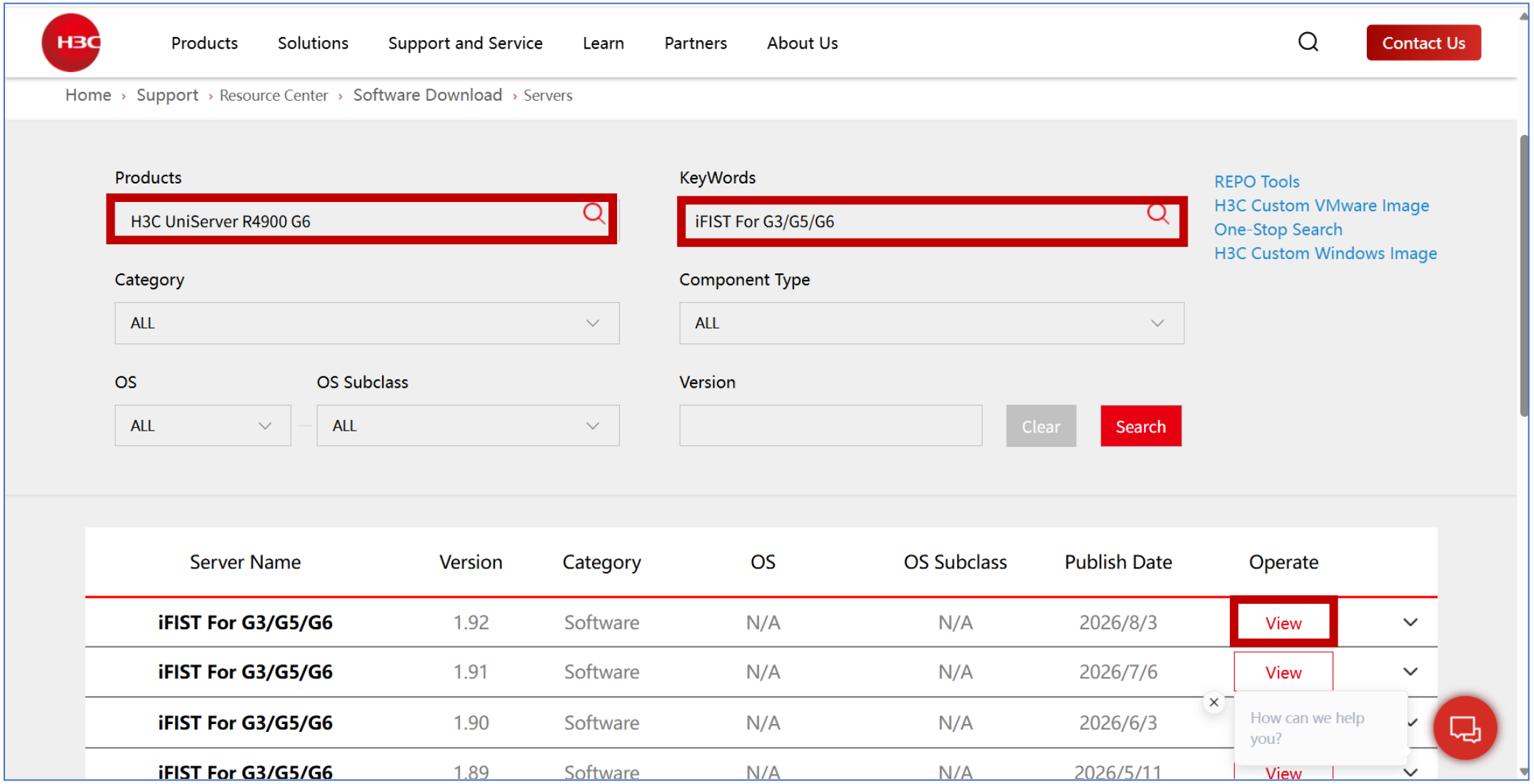
設定のバックアップと復元：重要な設定をエクスポートしてバックアップし、必要に応じて復元することで、システムの安定運用を支援します。

iFIST: ログのダウンロード

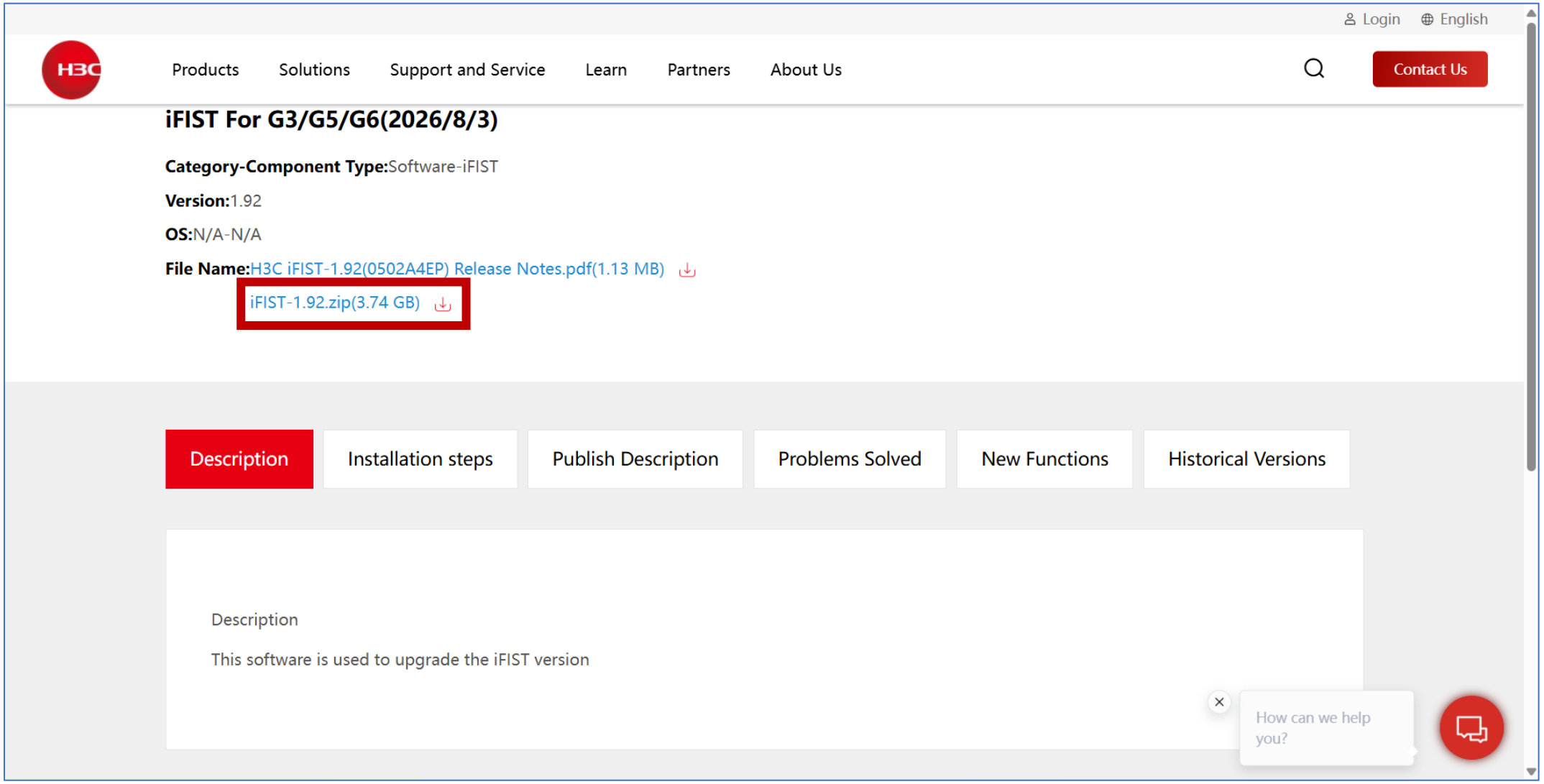


この機能を使用して、OSログ、SDSログ、システム運用ログ、および特定のコンポーネントをダウンロードします。**ダウンロードしたログおよび情報は、サーバーに挿入されているUSBフラッシュドライブのiFIST/LogDownloadUniTool/LogDownloadディレクトリに保存されます。**

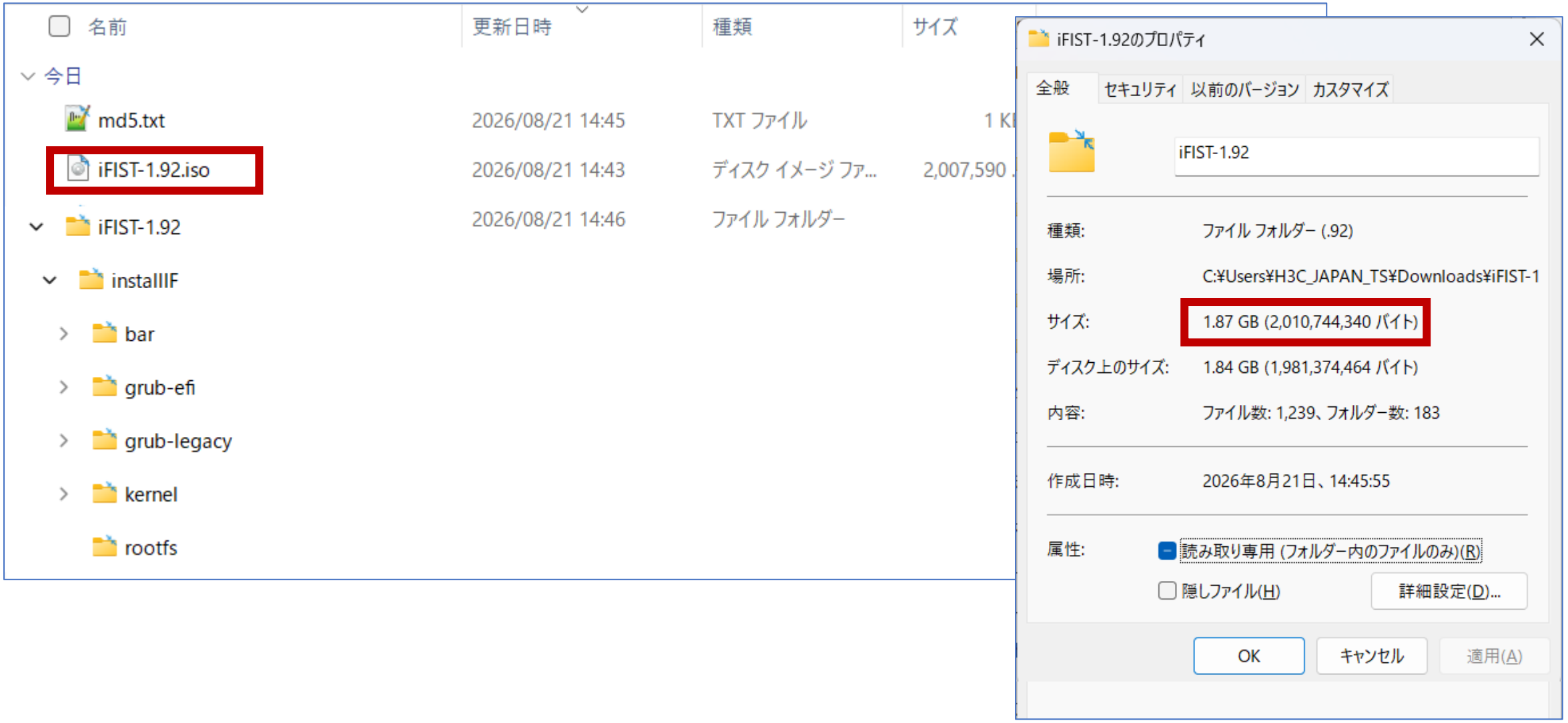
iFISTファームウェア(サポート>リソースセンター>ソフトウェアダウンロード>サーバー)



iFISTファームウェア



iFISTファームウェア





01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

H3C Unisystem概要

H3C UniSystem（H3C統合システム）は、H3C社が提供する様々なITインフラを統一的に管理するためのプラットフォームです。

主に、ネットワーク機器、サーバー、クラウド、仮想化などのリソースを統合的に管理し、効率化と最適化を図る目的で利用されます。

具体的には、リソースのインベントリ管理、運用管理、セキュリティ管理、パフォーマンスモニタリング、自動化などの機能を提供します。

H3C UniSystemの主な機能と特徴

統合管理:
ネットワーク機器、サーバー、クラウド、仮想化など、様々なITリソースを単一のプラットフォームで管理します。

データセンターのライフサイクル管理:
サーバーの導入、構成、チューニング、省エネ、診断、廃止措置といったライフサイクル全体をインテリジェントに管理します.

運用と保守の効率化:
運用と保守の作業を自動化し、効率化を促進します.

セキュリティ管理:
ネットワークセキュリティを強化し、脆弱性対策を講じます。

自動化:
運用タスクの自動化、再起動、リソースの割り当てなど、様々なタスクを自動化します。

クラウド管理:
クラウドリソースのインベントリ管理、リソースの割り当て、セキュリティ管理などをサポートします。

仮想化管理:
仮想化環境のインベントリ管理、仮想マシンの管理、リソースの割り当てなどをサポートします。

Unisystemの初期設定

- 管理用のUnisystemのIPアドレス/デフォルトゲートウェイ/DNSサーバの設定
  - デフォルトは192.160.0.190/16

- NTPの設定
  - プライマリーとセカンダリーのNTPサーバーのIPアドレスを設定

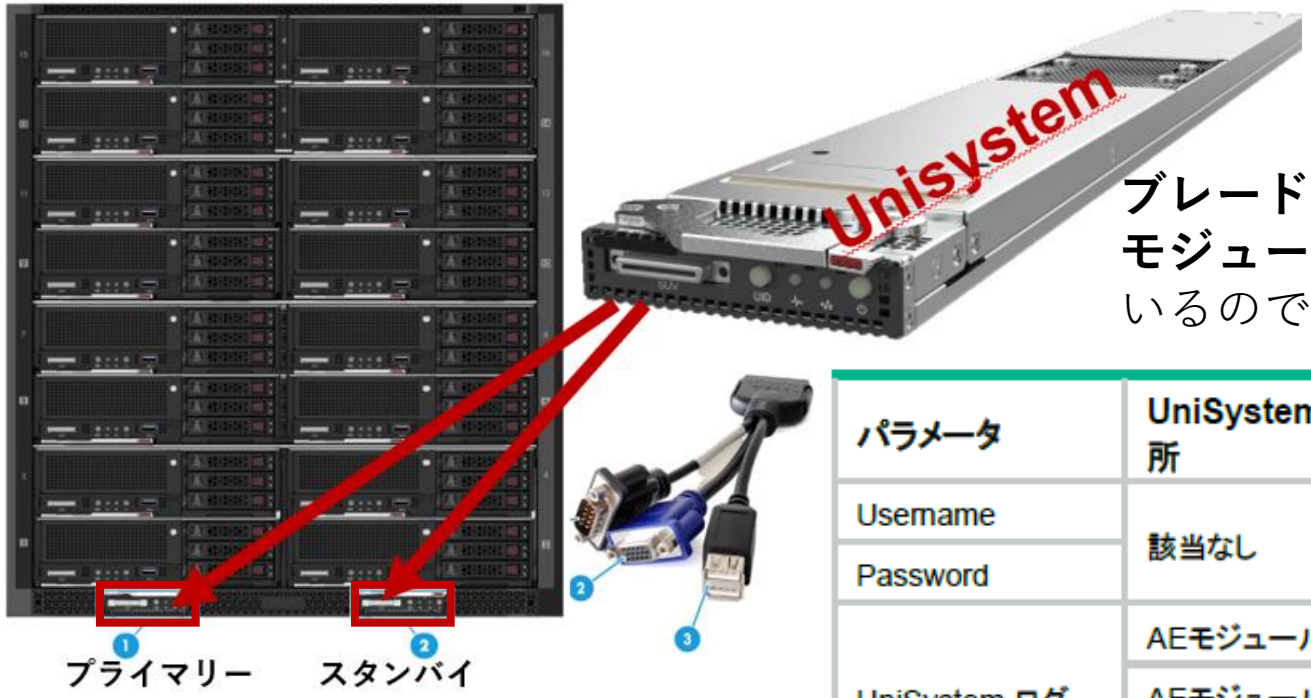
- SNMPの設定
  - SNMPマネージャーのIPアドレスの設定
  - SNMPのコミュニティ名の設定
  - SNMP Trapのエラーレベルの設定

- Syslogの設定
  - syslogサーバーのIPアドレスの設定
  - trapするエラーレベルの設定

- SMTPの設定(障害のメール通知)
  - SMTPサーバーのIPアドレス
  - SMTPのポート番号
  - 送信するエラーレベルの設定

管理IPの設定

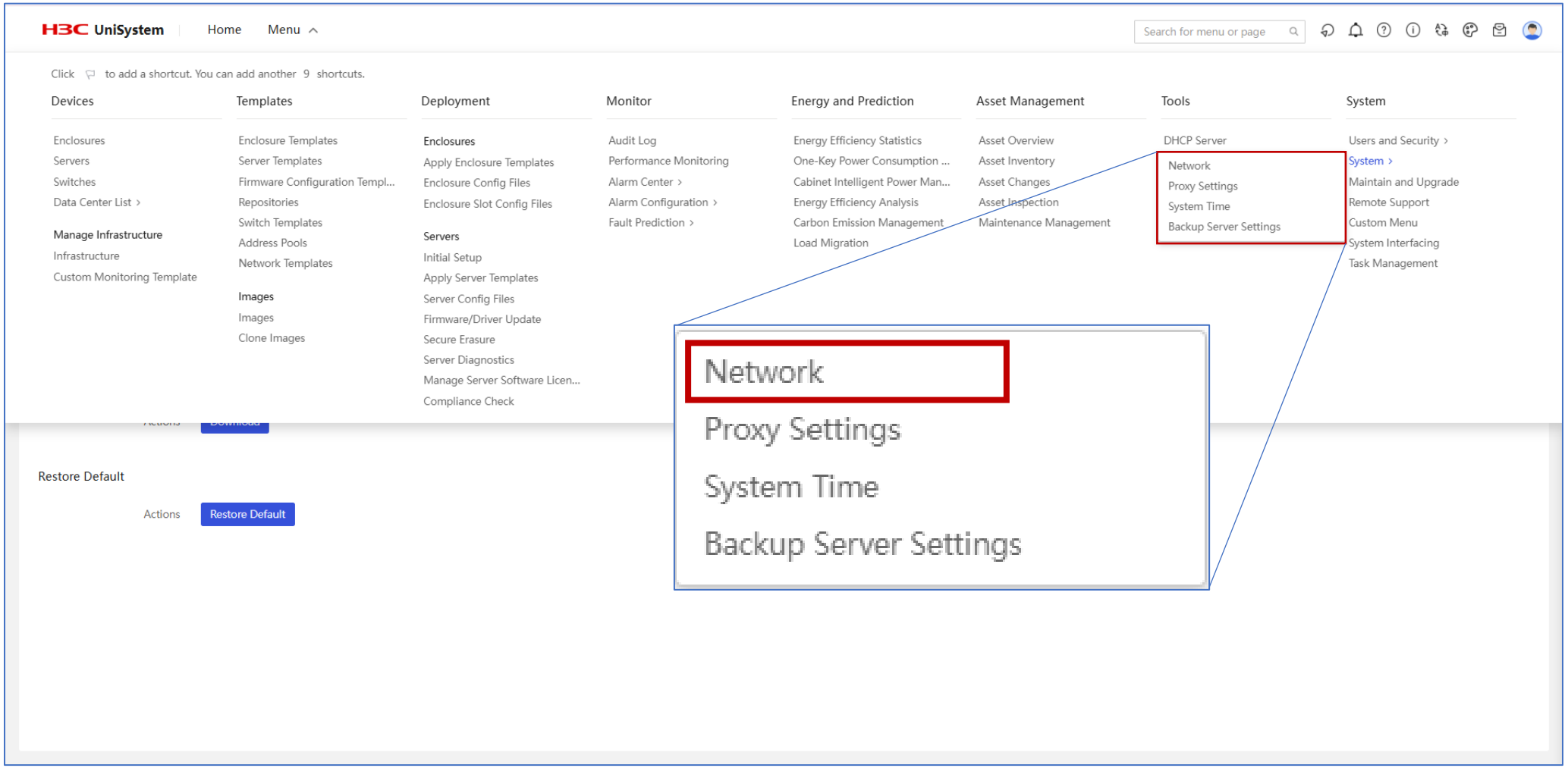
Unisystemは単体のサーバーにインストール(Windows/Linux及びVMware)して利用する場合は、**サーバーのNICに割り当てた**アドレスが管理IPとなります。



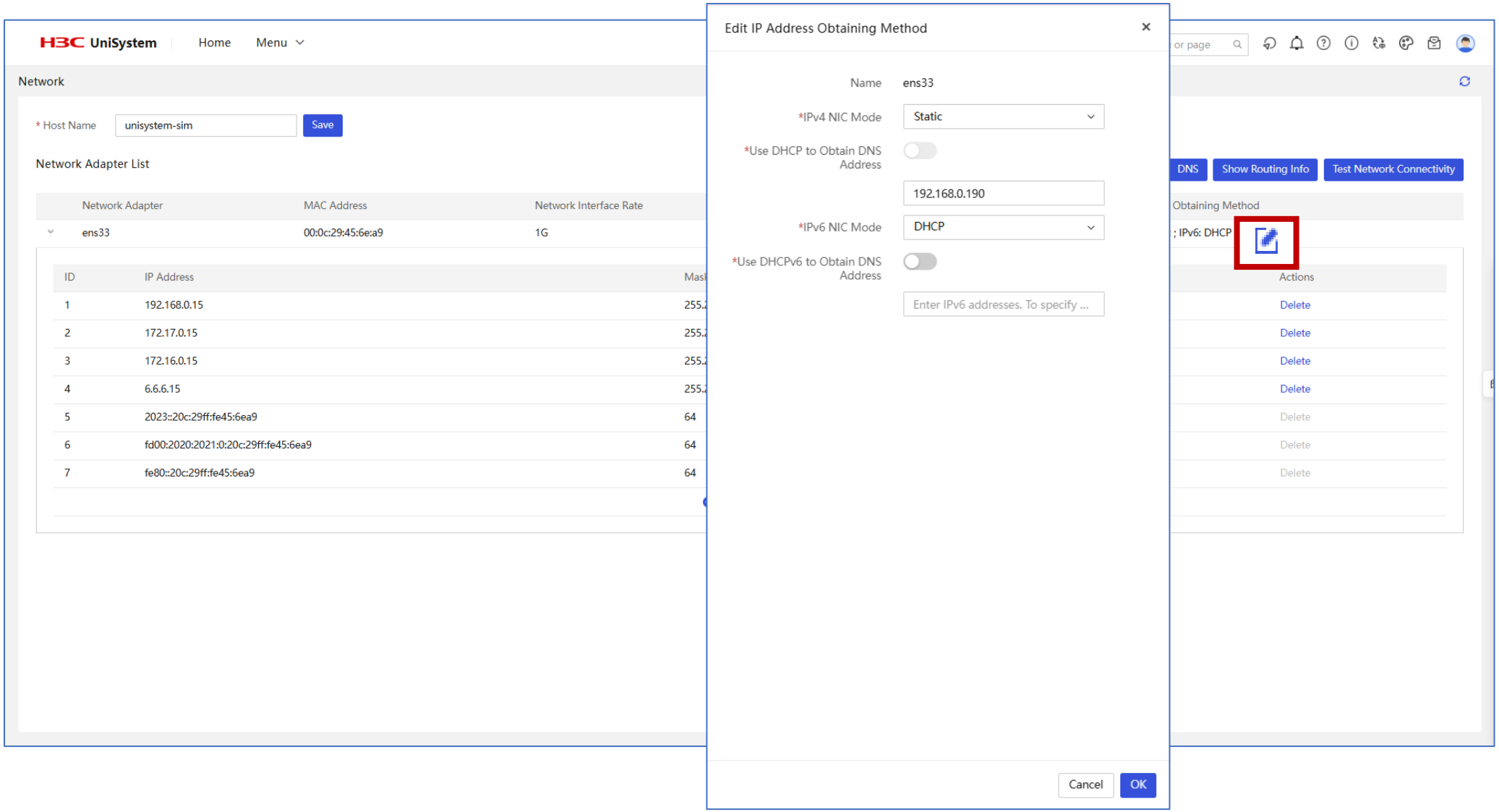
ブレードサーバーの場合、**AE(Application Engine)モジュール**というモジュールにUnisystemが組み込まれているので、その場合は次のページのように設定します。

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

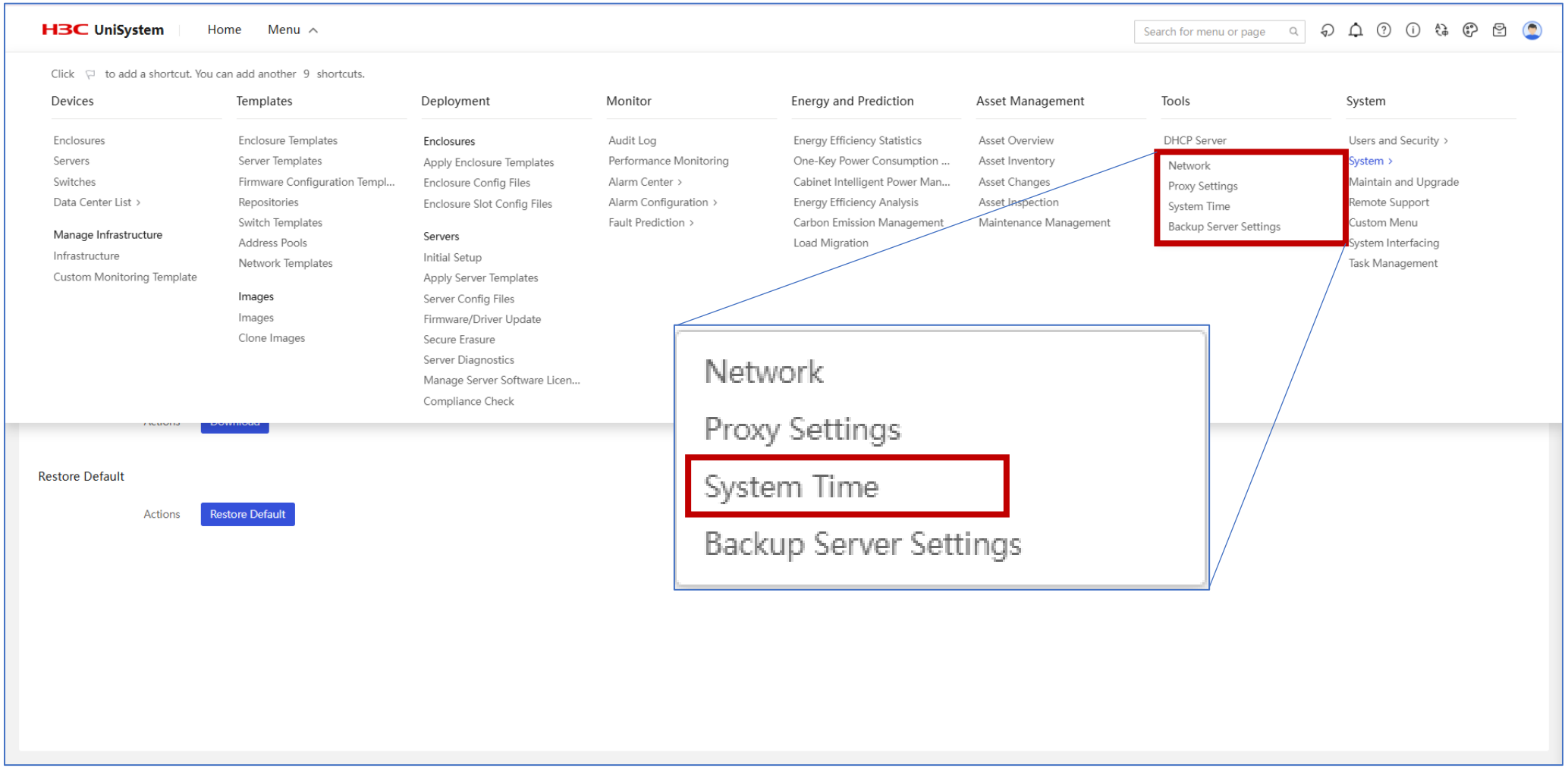
ネットワークの設定: Menu > System > Network



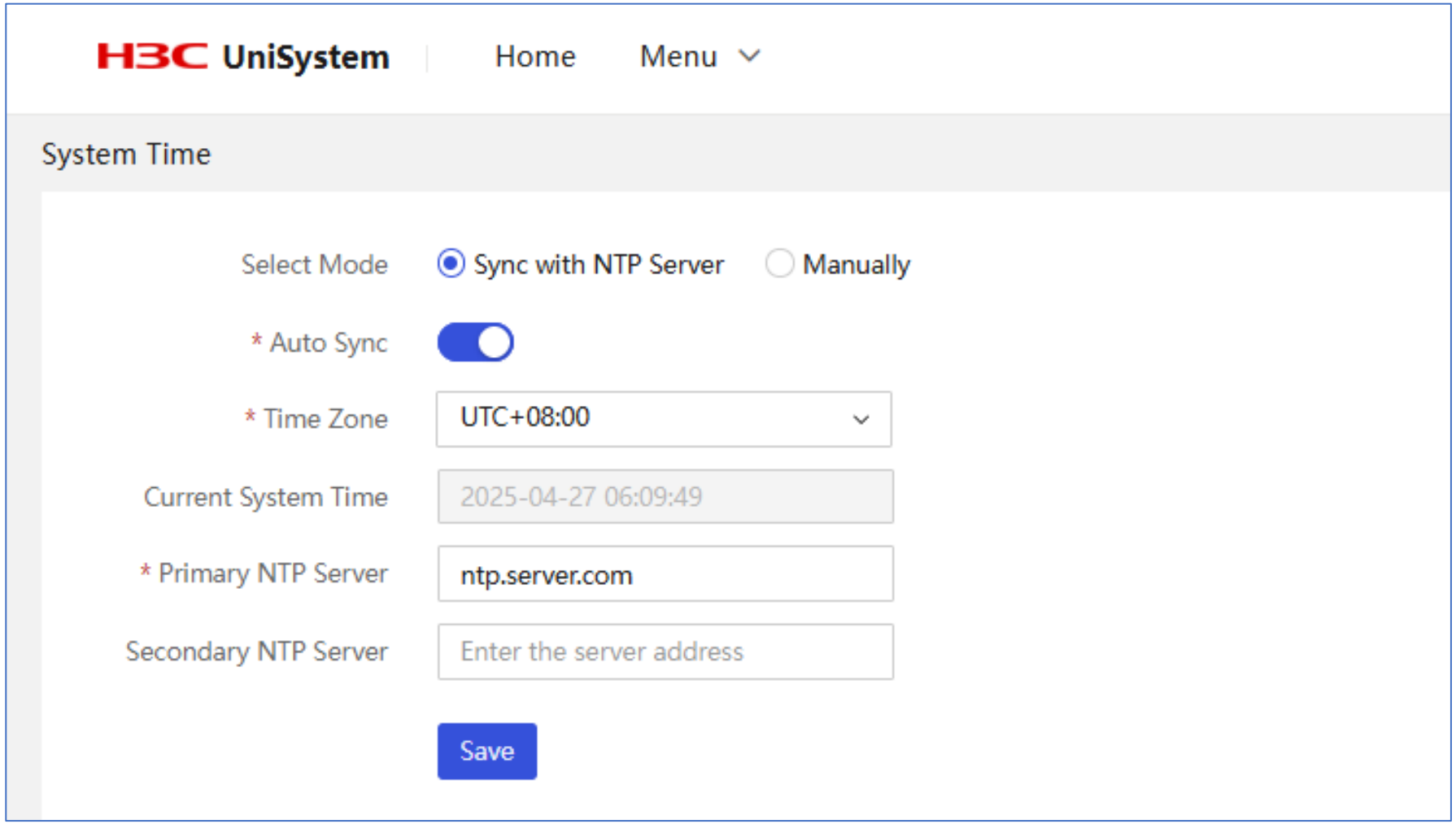
管理IPの設定: をクリック



NTPの設定: Menu > System > System Time

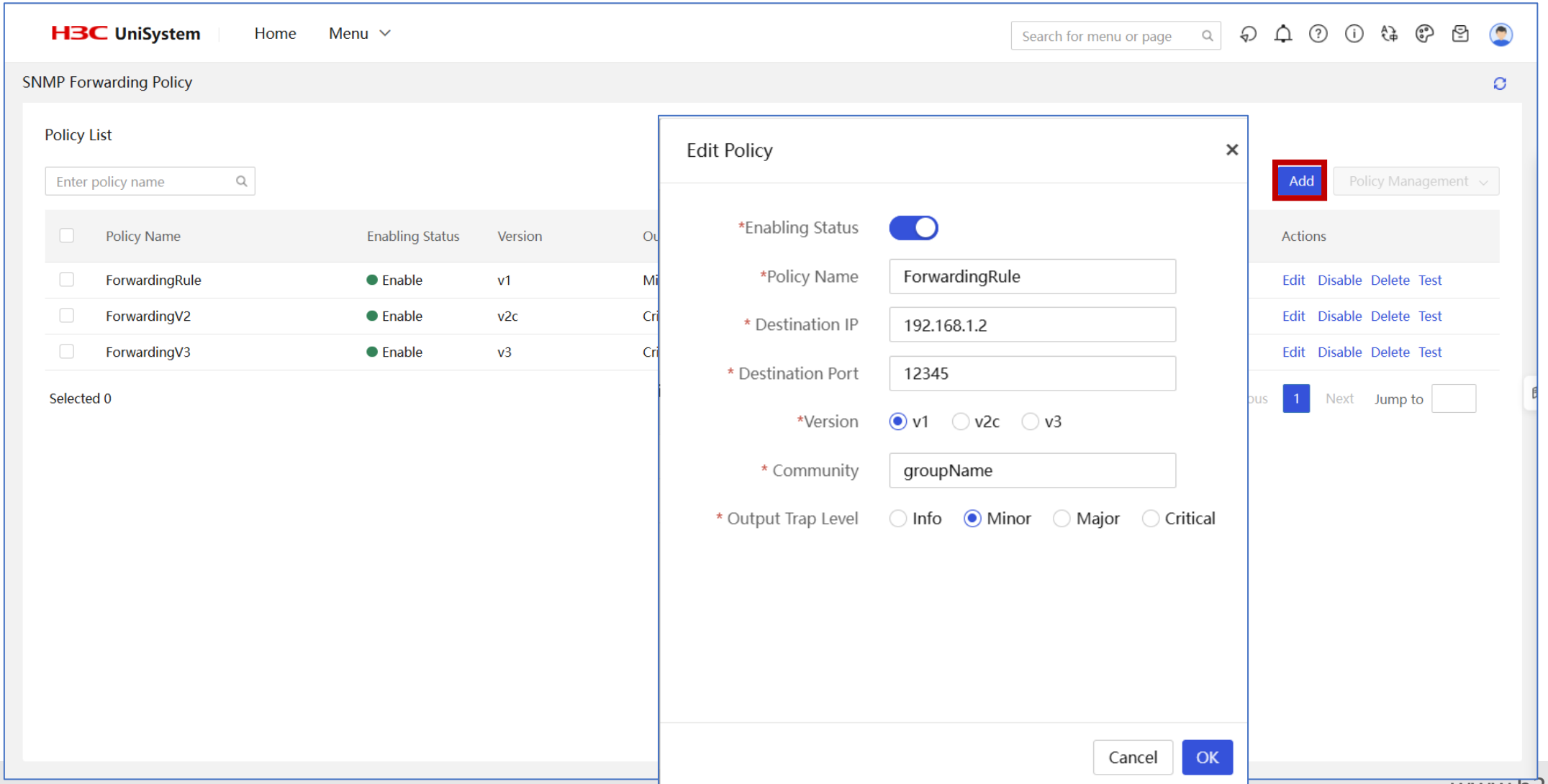


NTPの設定: Primary NTP Server

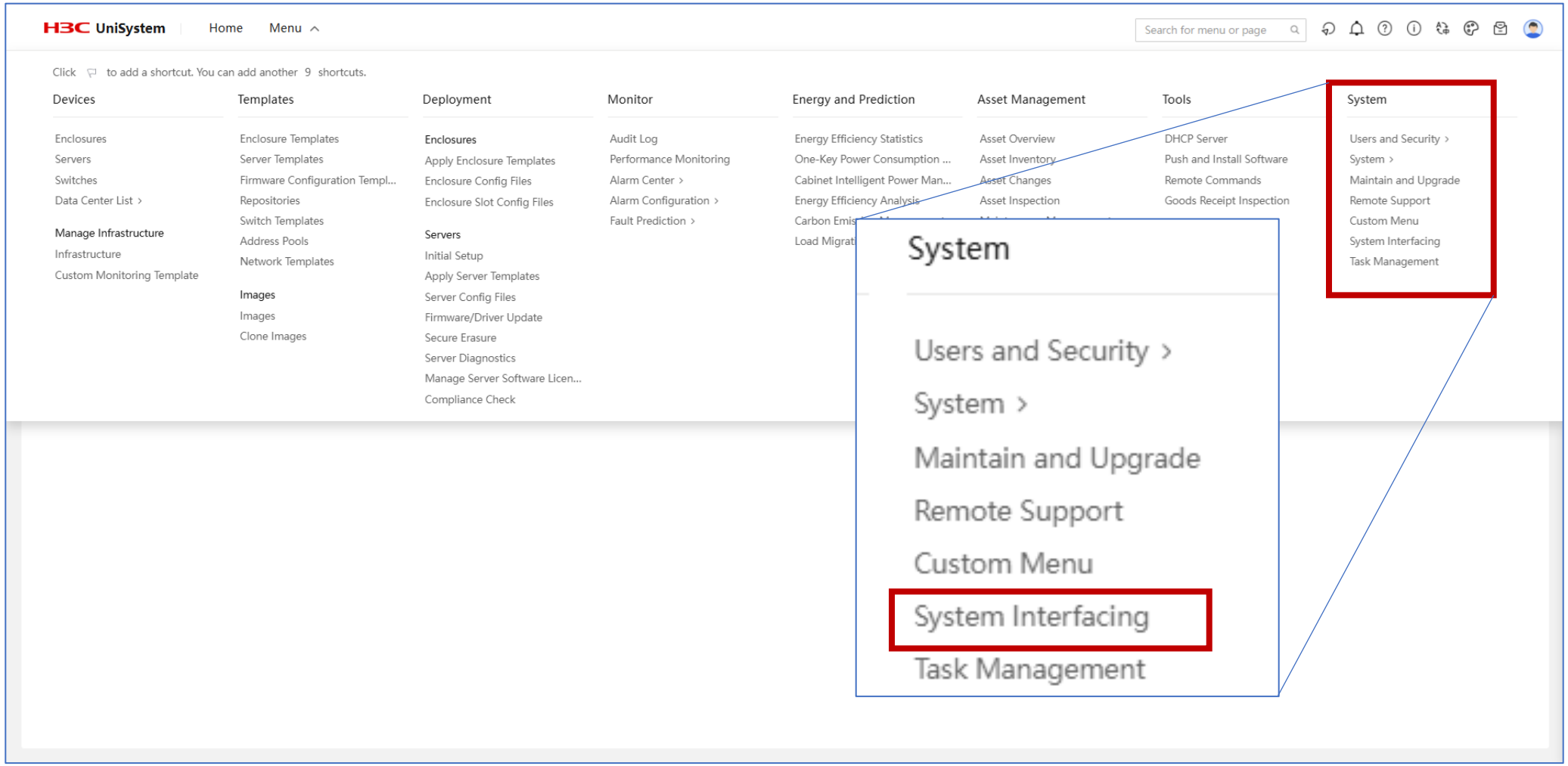


SNMPの設定:

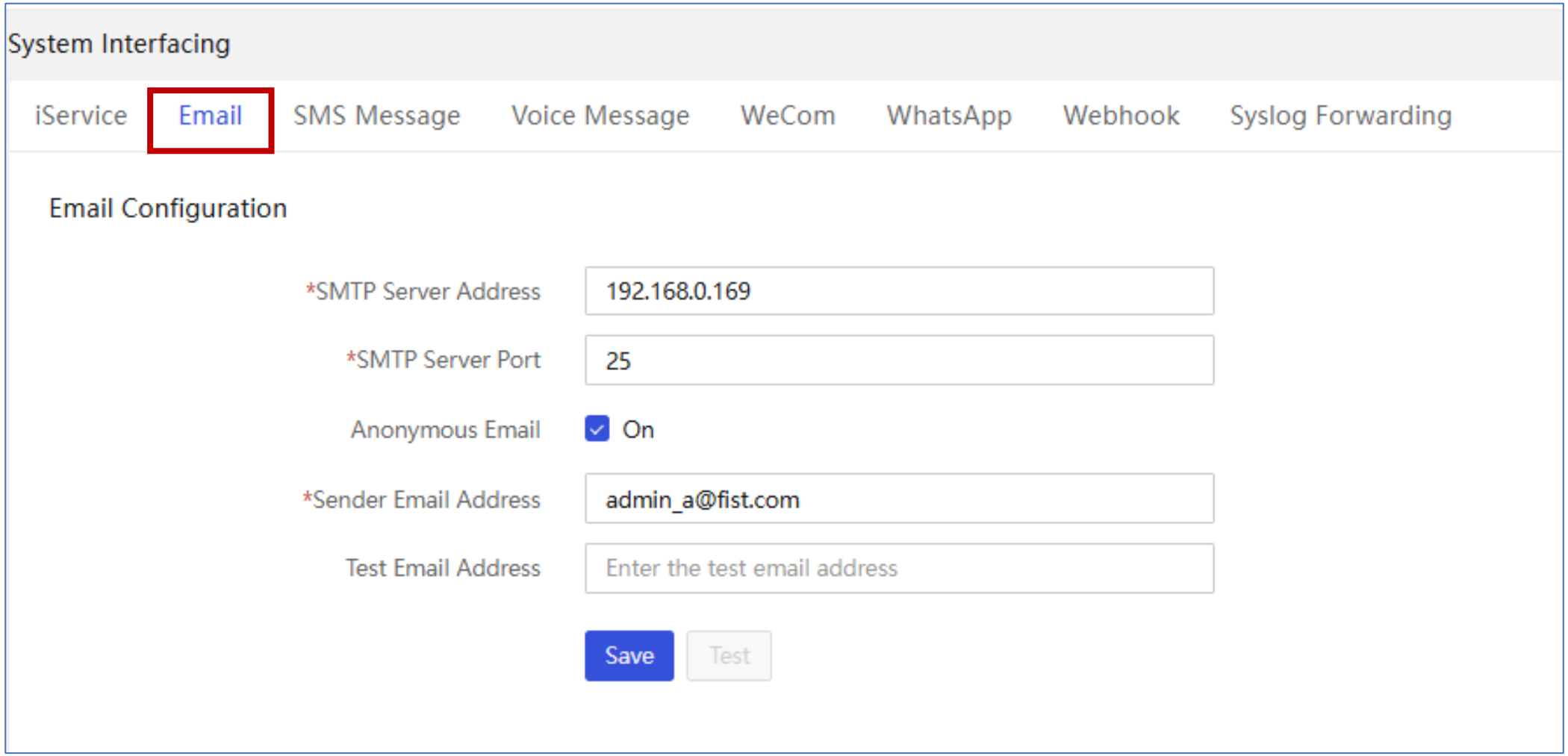
Menu > Monitor > Alarm Configuration > SNMP Forwarding Policy



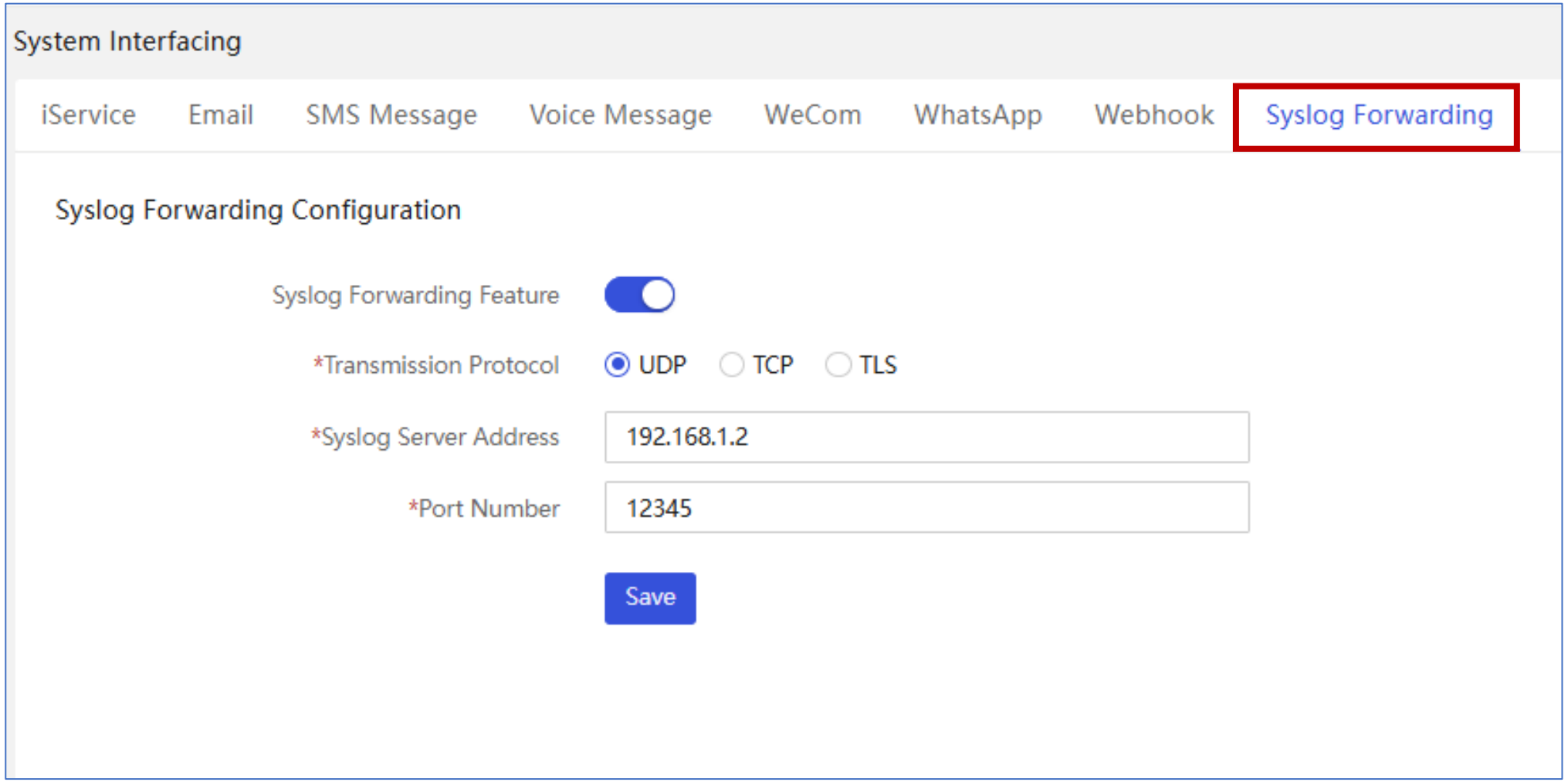
インタフェースの設定: Menu > System > System Interfacing



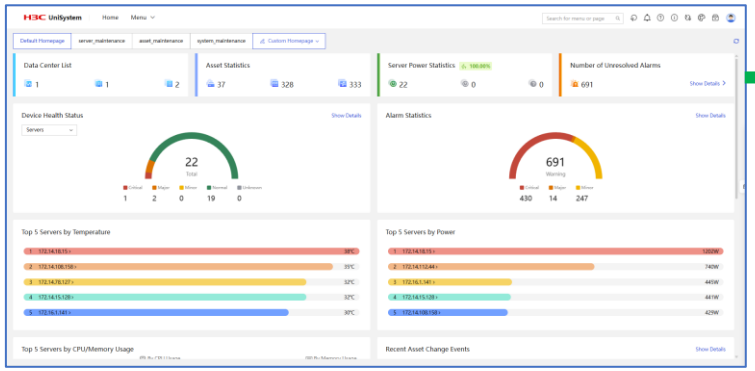
SMTPの設定

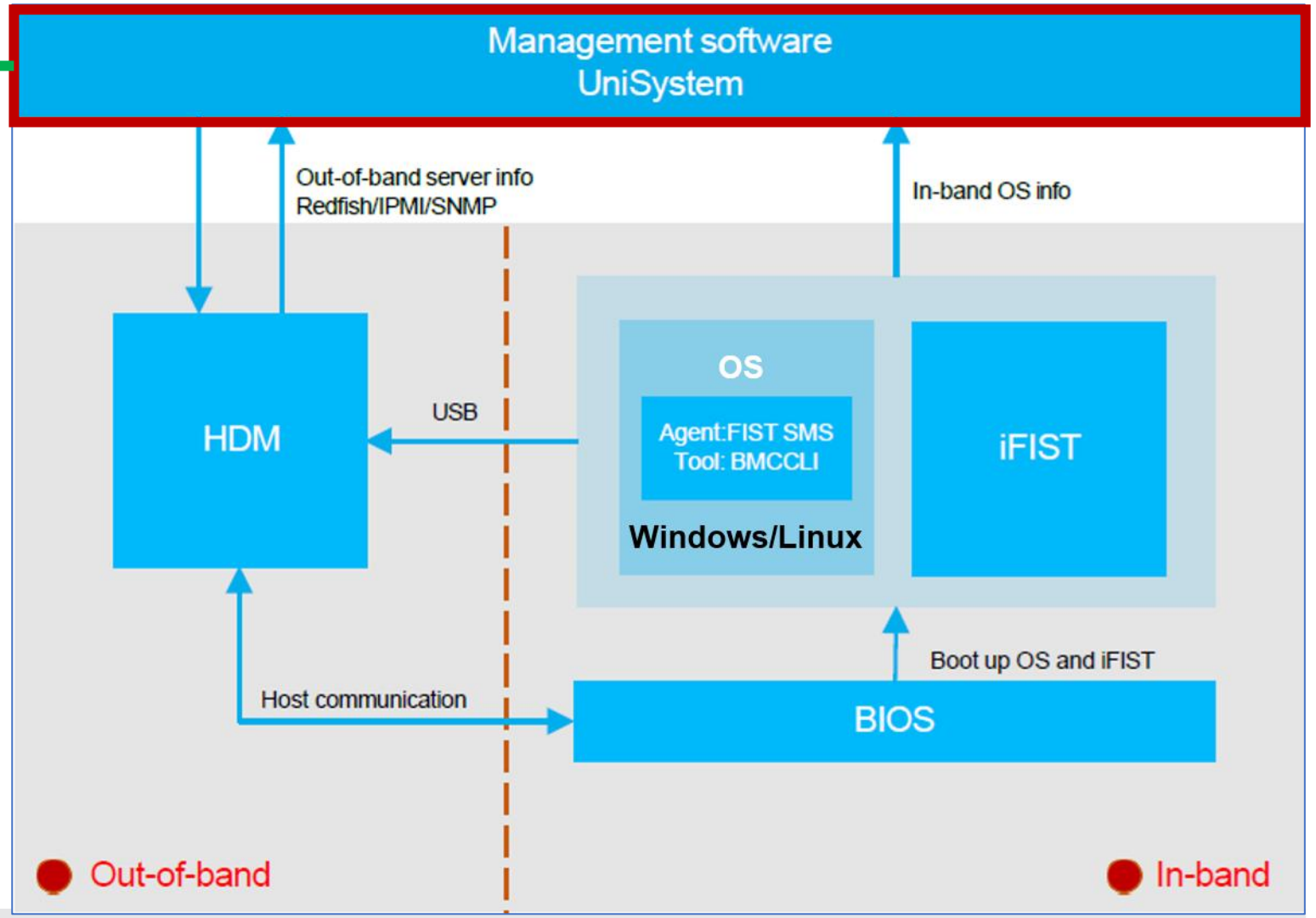

System Interfacing
iService
Email
SMS Message
Voice Message
WeCom
WhatsApp
Webhook
Syslog Forwarding
Email Configuration
*SMTP Server Address
192.168.0.169
*SMTP Server Port
25
Anonymous Email
On
*Sender Email Address
admin_a@fist.com
Test Email Address
Enter the test email address
Save
Test

Syslogの設定

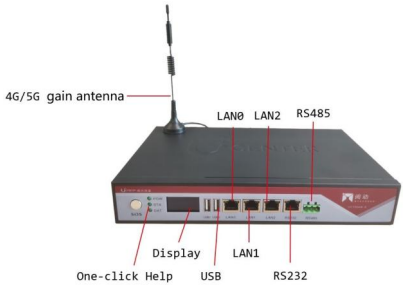

System Interfacing
iService
Email
SMS Message
Voice Message
WeCom
WhatsApp
Webhook
Syslog Forwarding
Syslog Forwarding Configuration
Syslog Forwarding Feature
*Transmission Protocol
UDP
TCP
TLS
*Syslog Server Address
192.168.1.2
*Port Number
12345
Save

Unisystemのアーキテクチャー
Unisystem(複数のハードウェア管理)



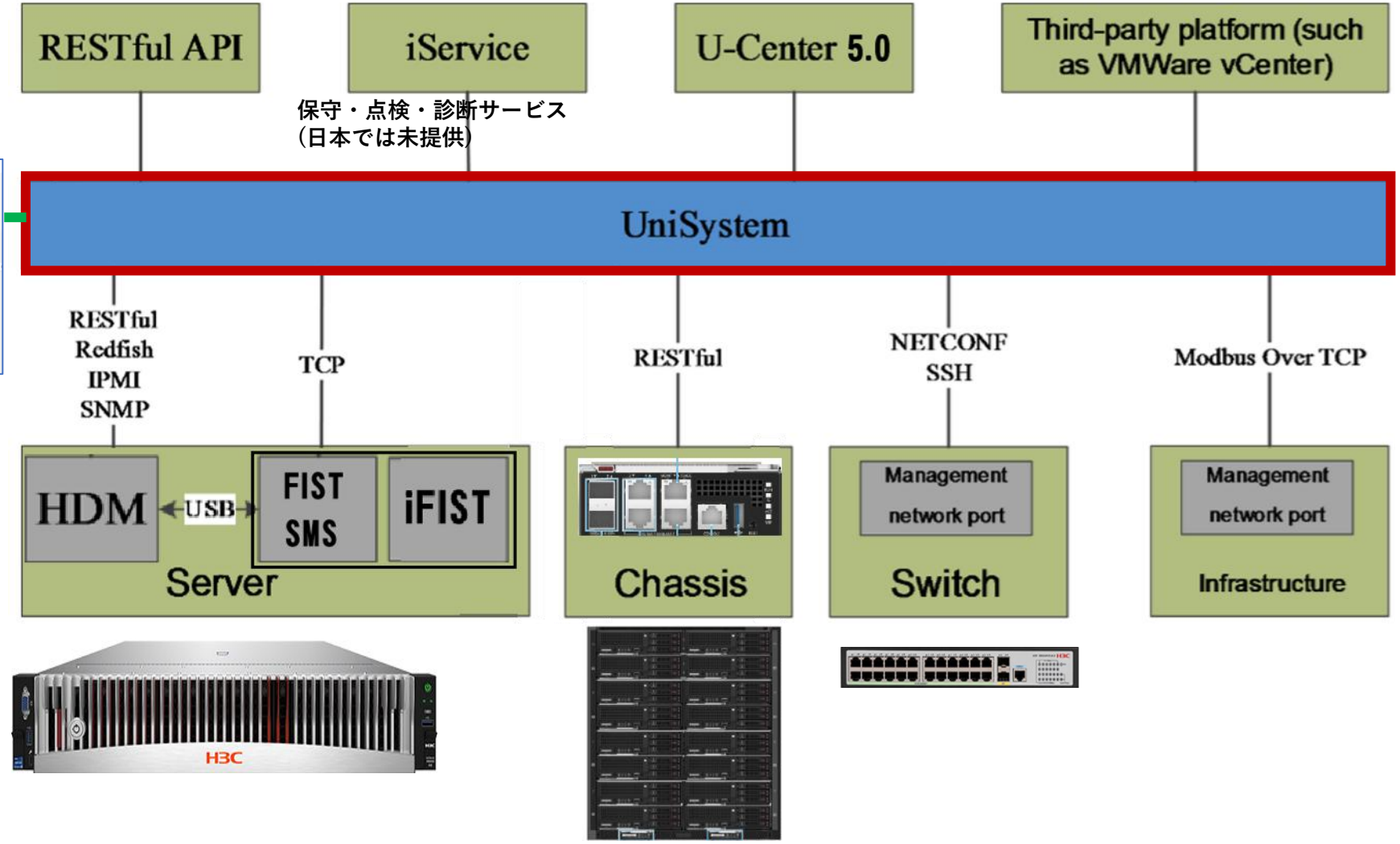


Unisystemのアーキテクチャー



UnisystemのGUI





サーバーソフトウェアシュミレーター

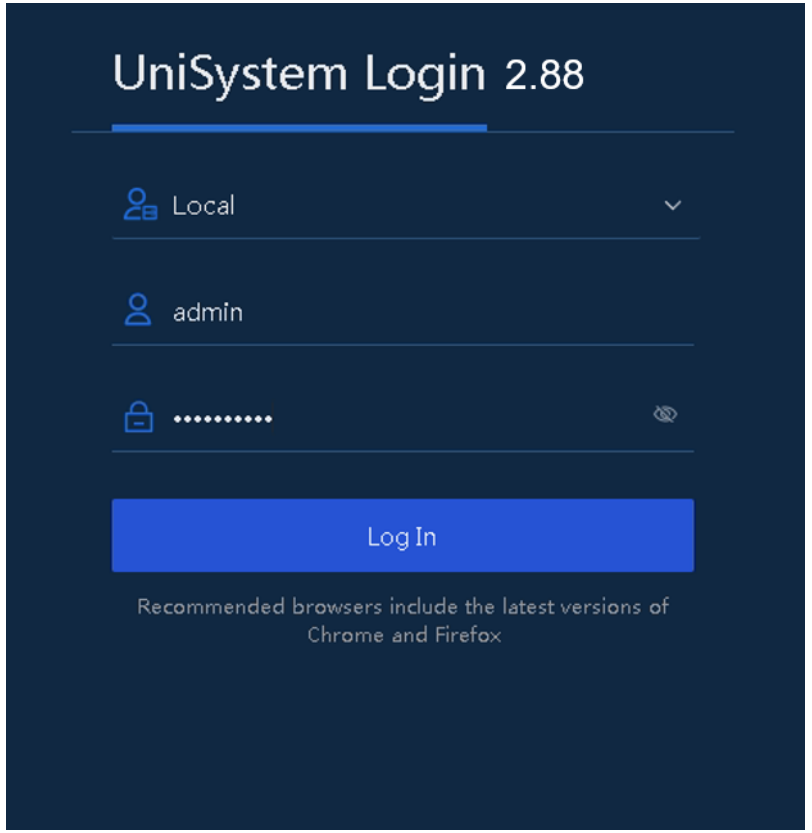
https://simulator.h3c.com/



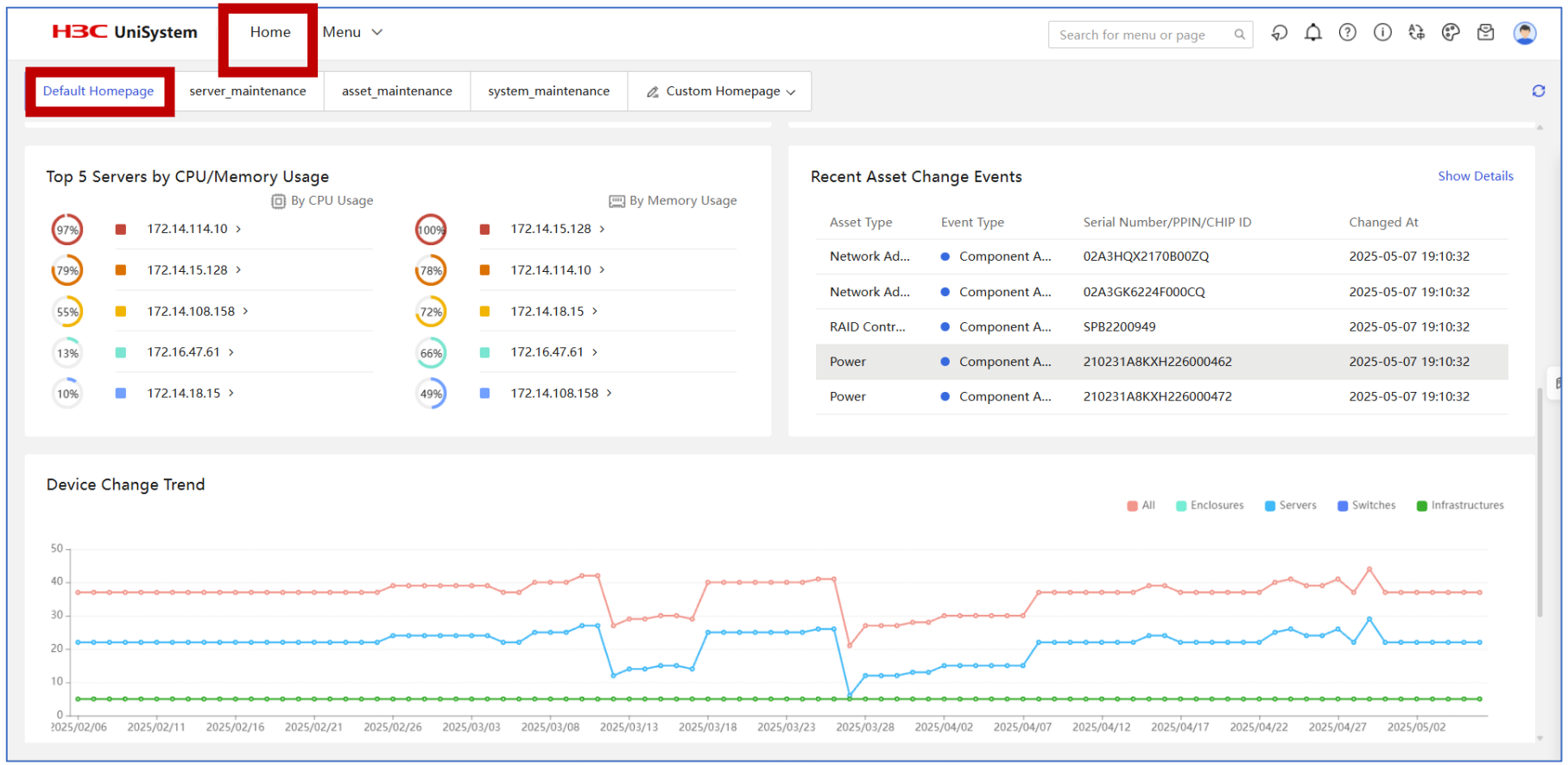
Unisystemへのログイン

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

   UniSystemサービスの起動設定で、UniSystemのHTTPポートおよびHTTPSポートを構成できます。詳細は、H3C Servers UniSystem Installation Guideを参照してください。
2. UniSystemログインページで、UniSystemユーザーのユーザー名とパスワードを入力します。デフォルトのアカウント: username/password: **admin** / **Password@_**

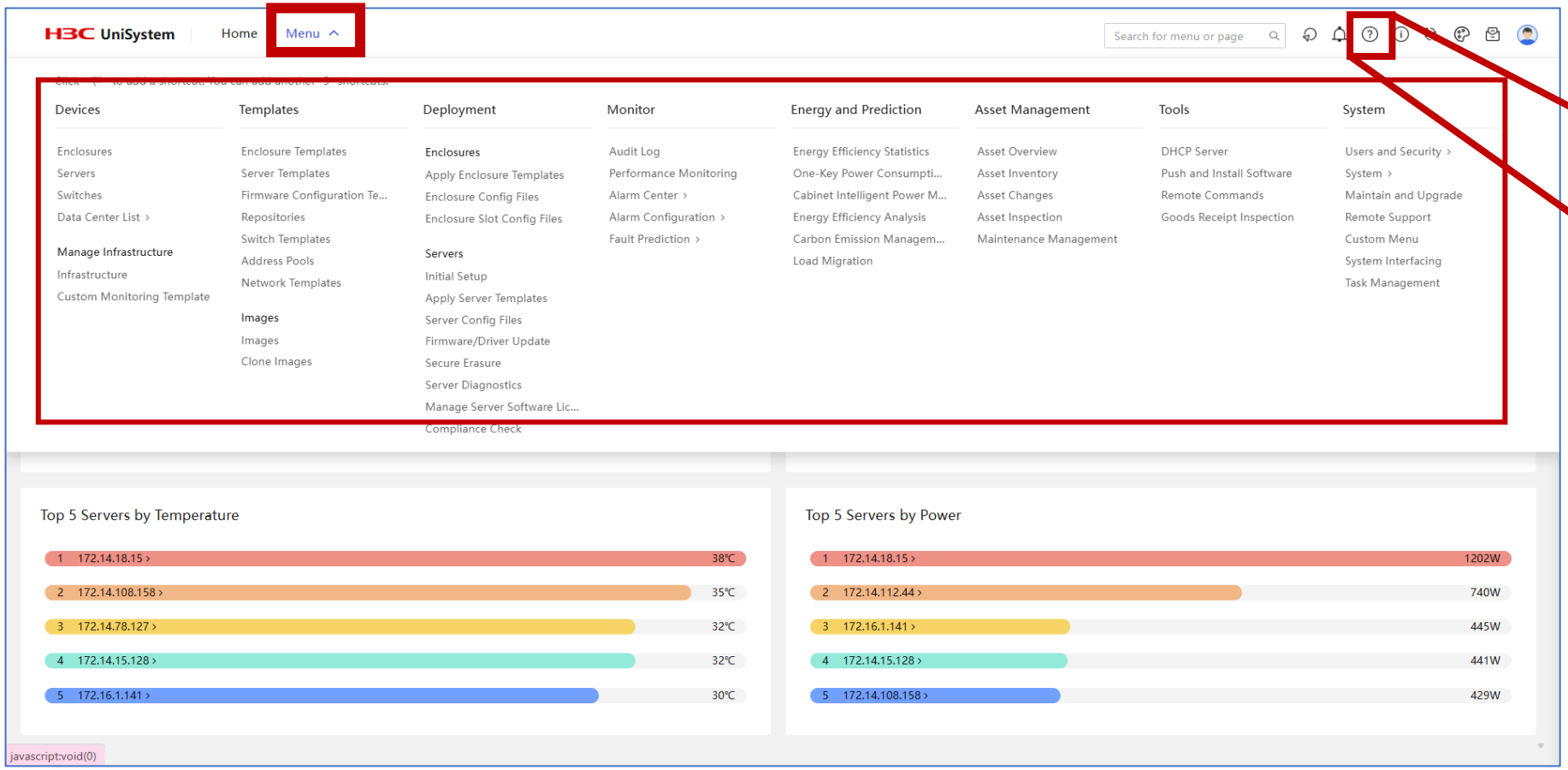


Unisystemホームページ



ダッシュボードページでは、**デバイス概要、サーバーアラーム、 資産統計、温度上位5台のサーバー、電力上位5台のサーバー、 CPU/メモリ使用量上位5台のサーバー（G6サーバーの場合）** など、動的なウィジェットを通じてシステム情報を表示できます。
ショートカットを使用すると、指定したメニューに直接アクセスできます 。

Menu(ほとんどの機能はメニューから選択します)

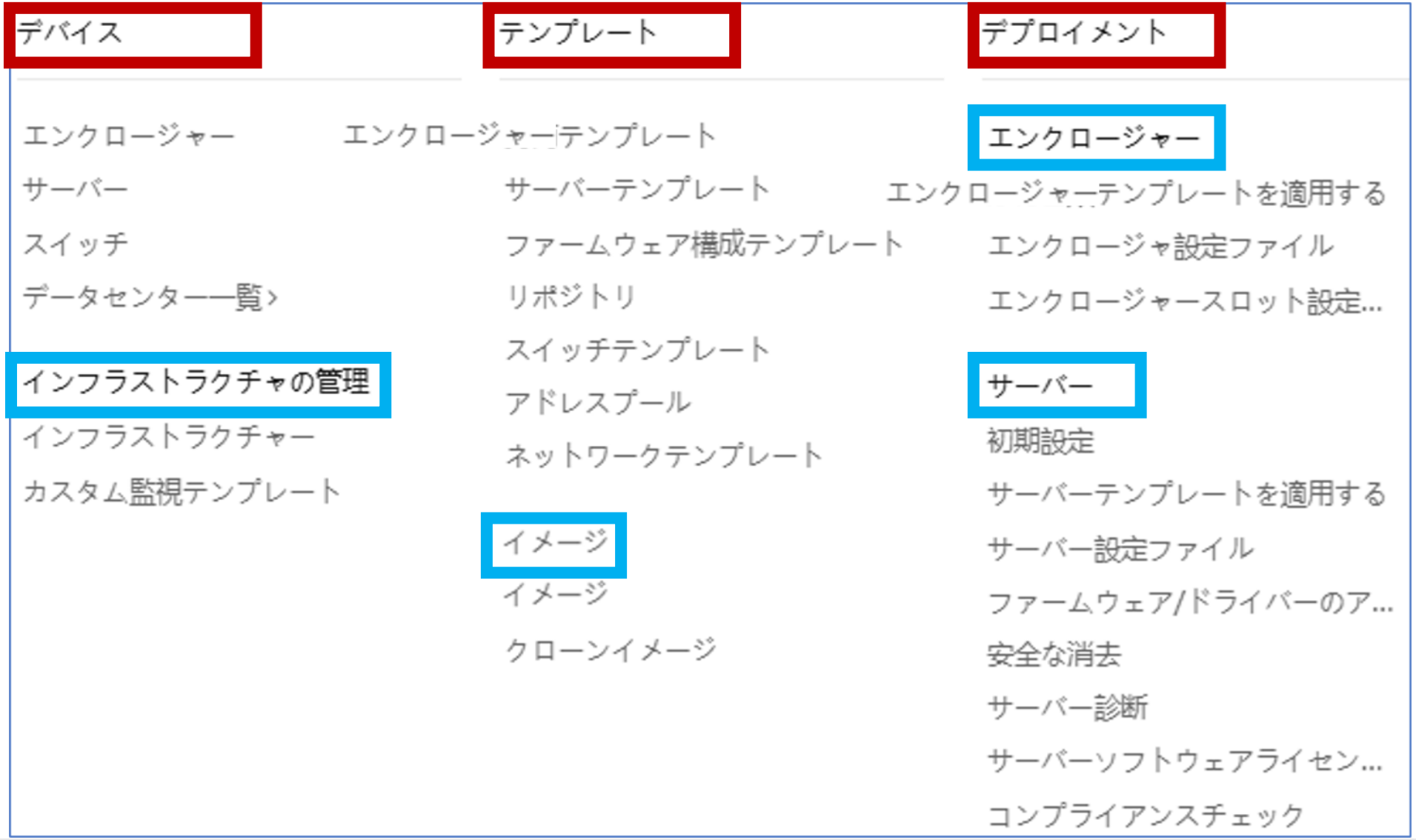


メニューの詳細は次ページに紹介



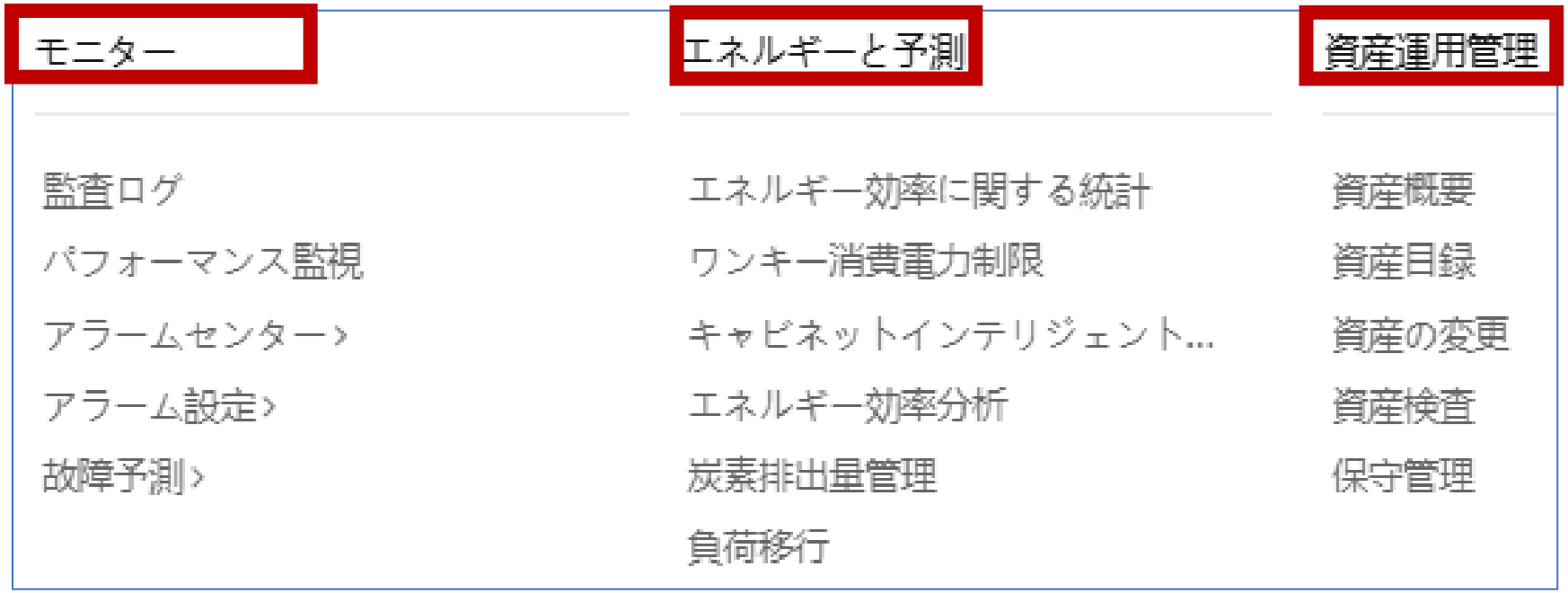
HELPアイコンをクリックすると現在表示されている画面のマニュアルが表示されます

Menu



デバイス
テンプレート
デプロイメント

Menu



モニター
エネルギーと予測
資産運用管理

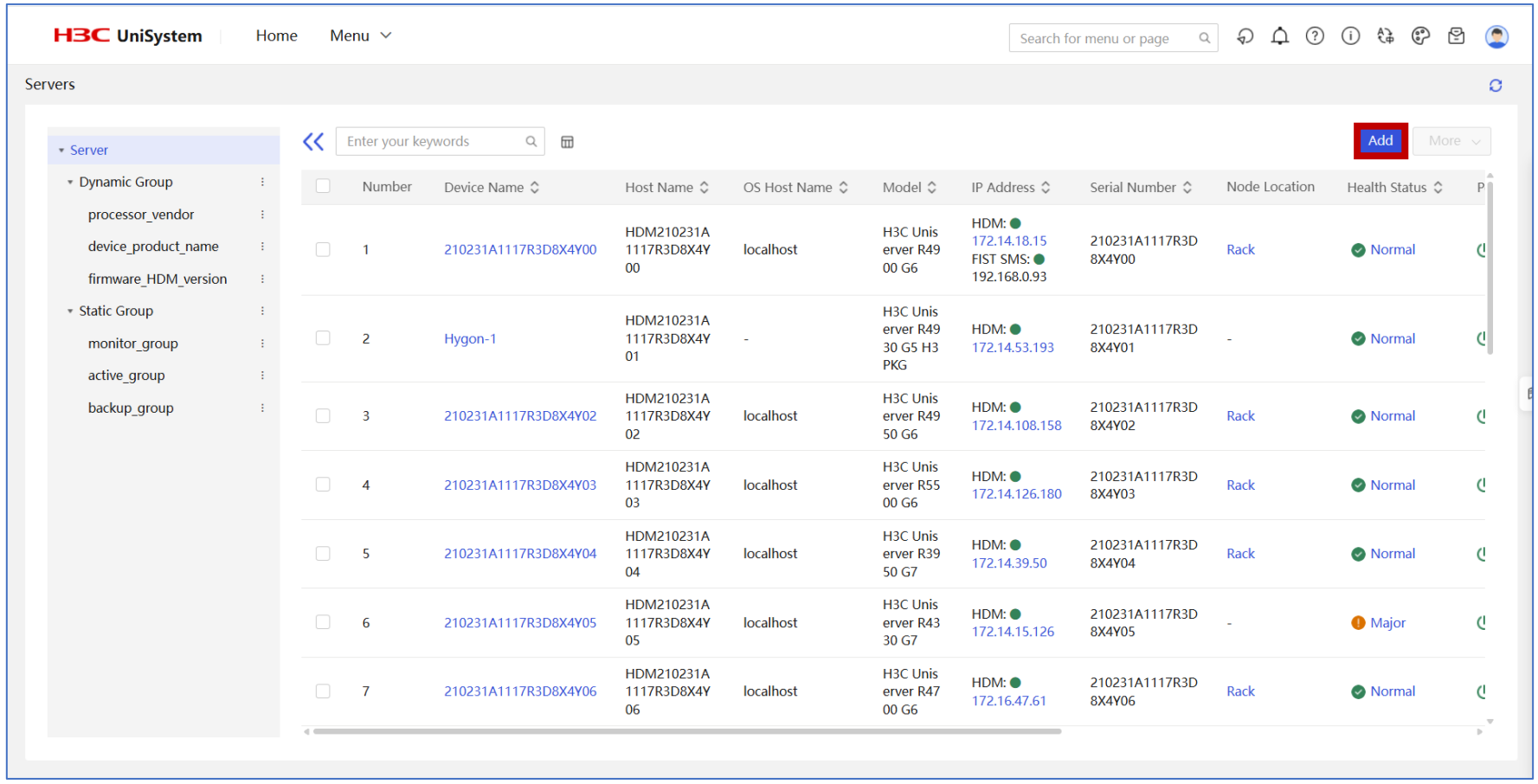
Menu



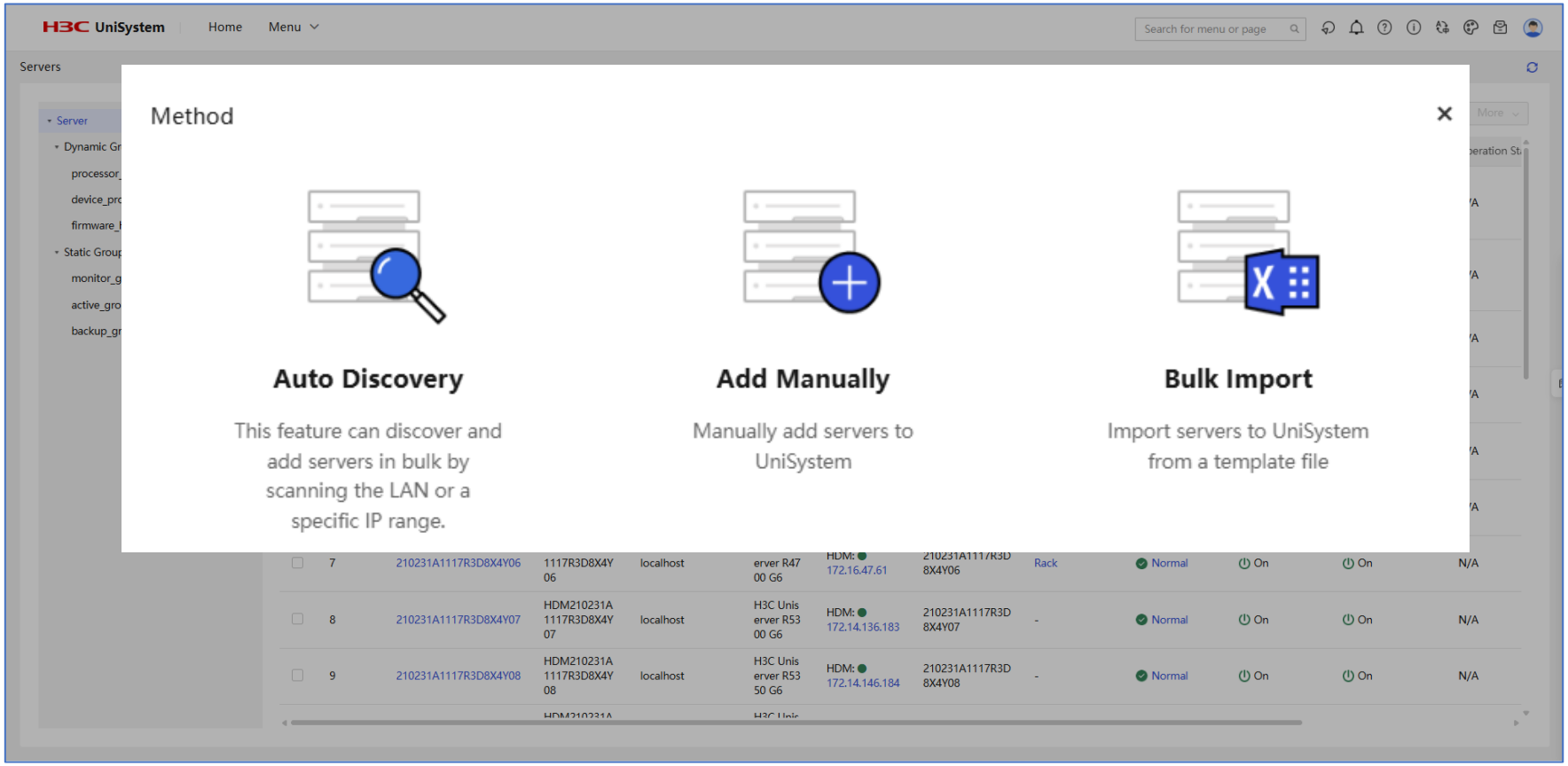
ツール
システム

最初に管理するサーバーを登録します

Menu > Devices > Servers > Add



サーバーの登録方法を選択します

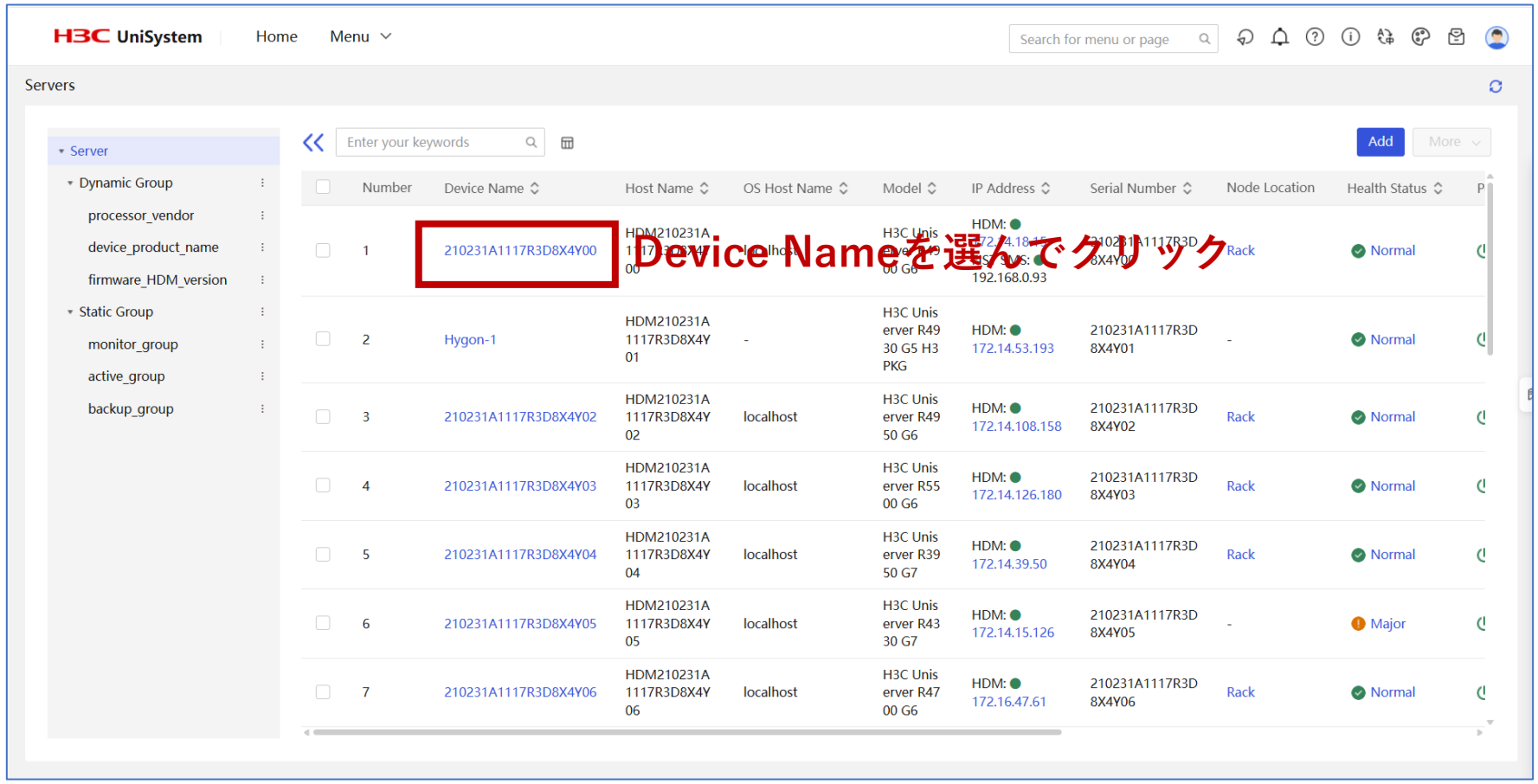


Auto Discovery: LANスキャンまたはIPサブネットスキャンを使用してネットワーク上のサーバーを検索し、検出されたサーバーをUniSystemに追加できます。HDMサーバーノードとFIST SMSサーバーノードの両方を自動検出で追加できます。

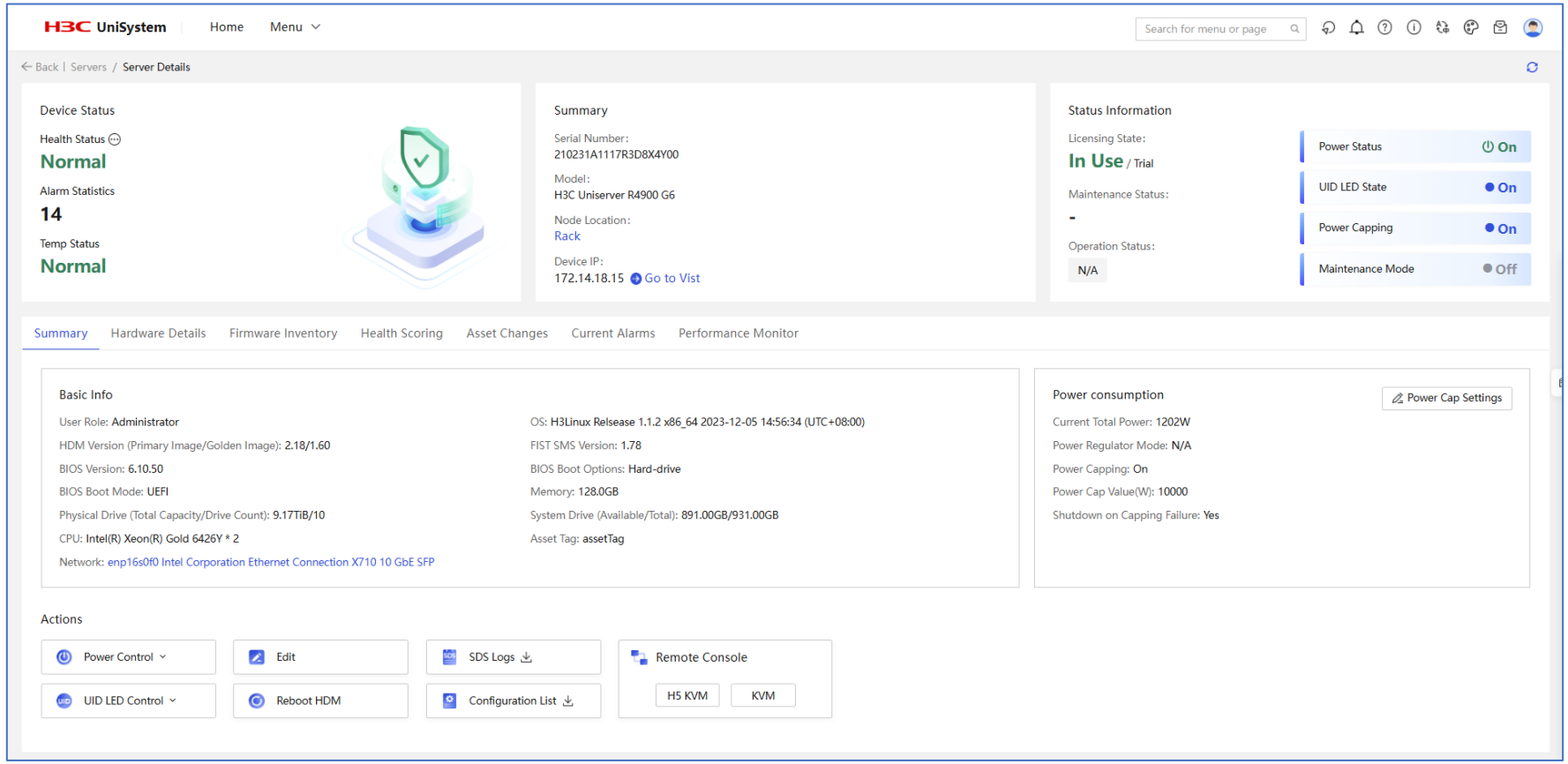
Add Manually: HDMサーバーノードを追加するにはDevice Typeで「HDM」を選択します。HDMのIPアドレス、HDMのログインユーザー名とパスワード、およびサーバー名を指定します。FIST SMSサーバーノードを追加するには、Device Typeで「FIST SMS」を選択します。FIST SMSのIPアドレスとサーバー名を指定します。

Bulk Import: UniSystemにサーバーをインポートする前に、まずインポート対象のサーバー情報を含む有効なインポートファイルを用意してください。「デバイスのインポート（Import Devices）」ページからインポートファイルのテンプレートをダウンロードし、そのテンプレートに記載されている制限事項やガイドラインに従ってデバイス情報を入力します。なお、現在UniSystemがサポートしているHDMユーザー名は、1～16文字の範囲内のものに限られます。これ以外のユーザー名を使用すると、追加に失敗する可能性があります。

登録したサーバーの詳細を確認する



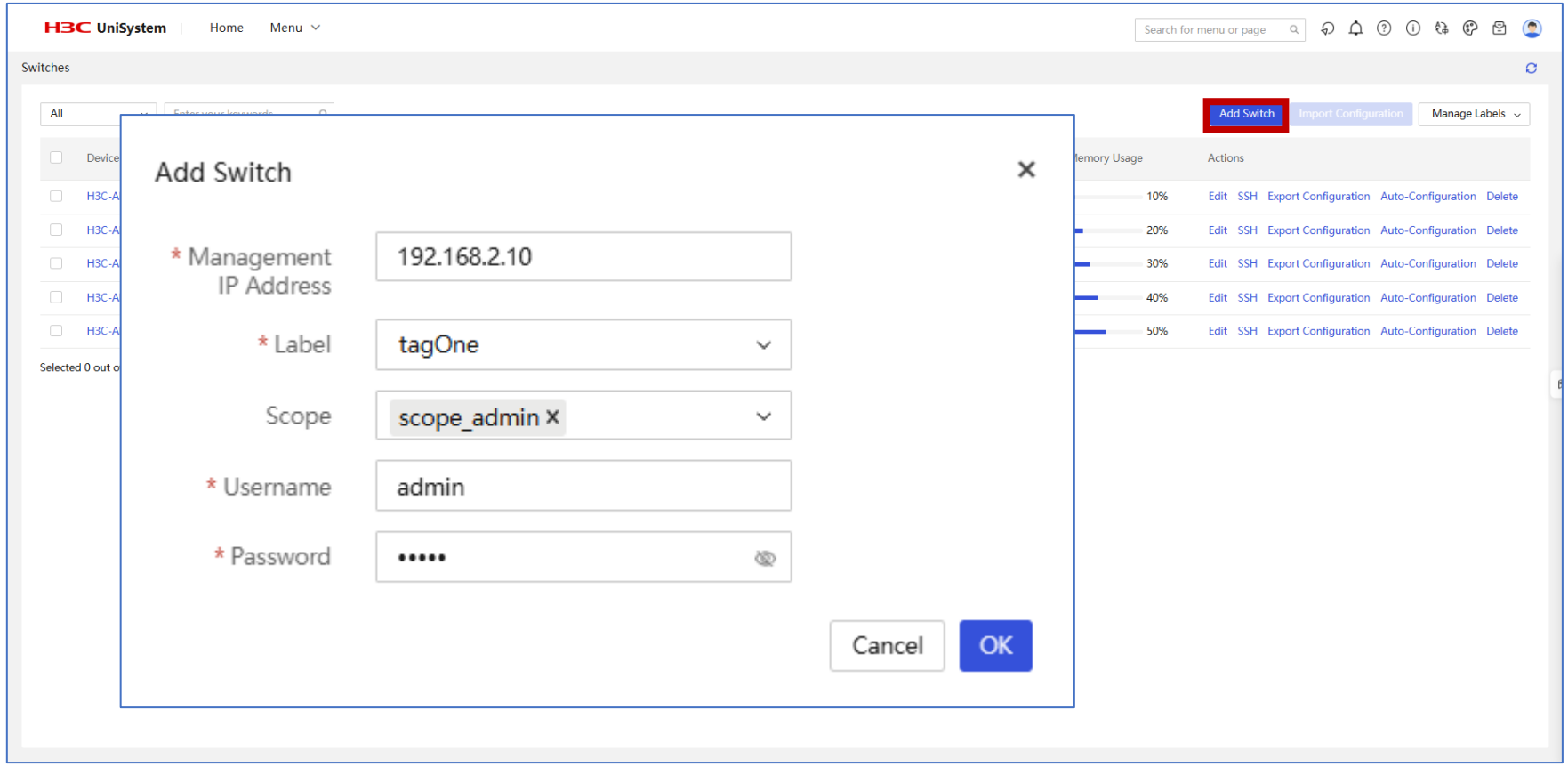
Menu > Devices > Servers > Server Details



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

最初に管理するスイッチを登録します

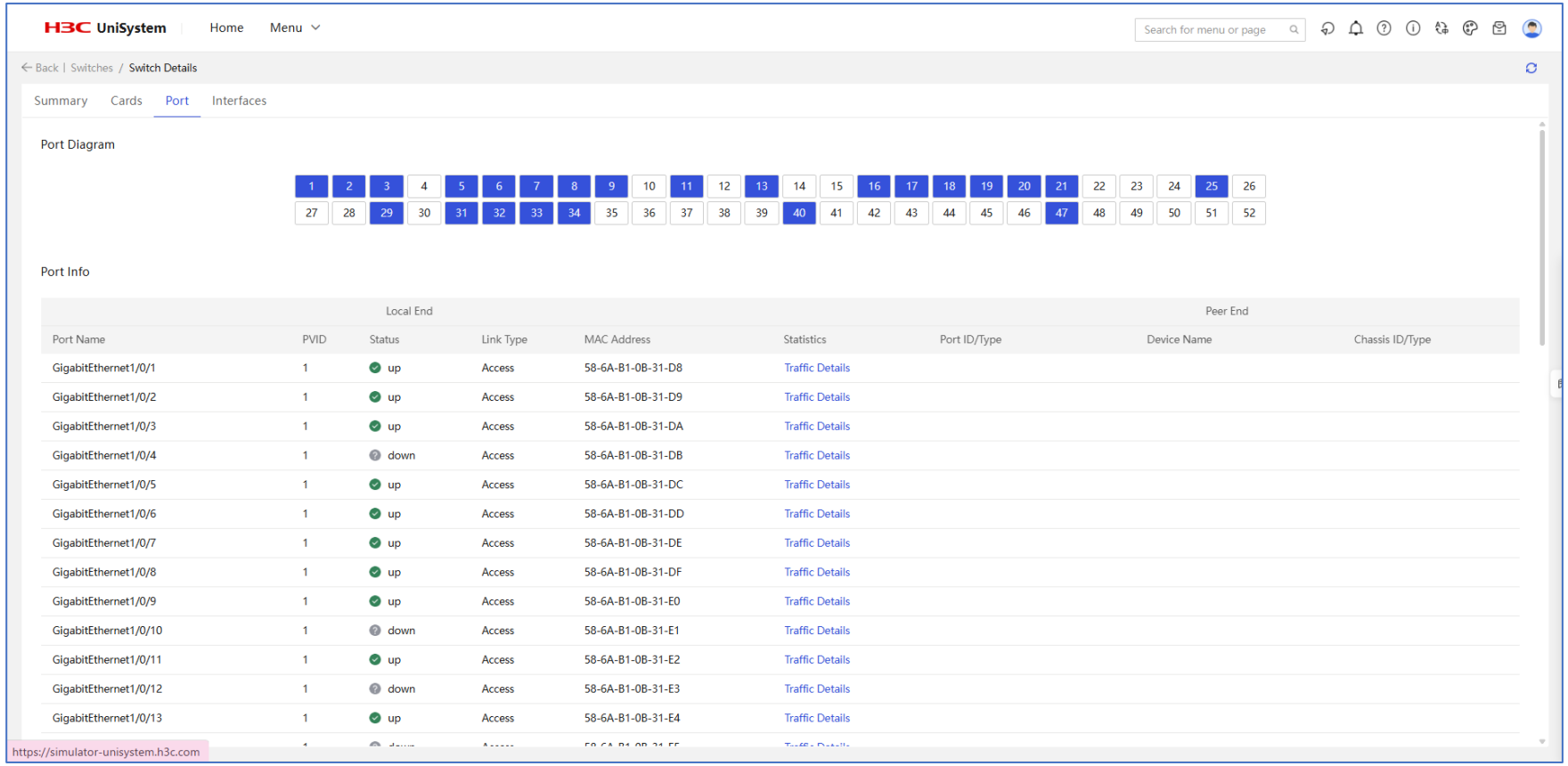
Menu > Devices > Swiches > Add



注意：対象となるスイッチはブレードサーバーの場合に適用されます。

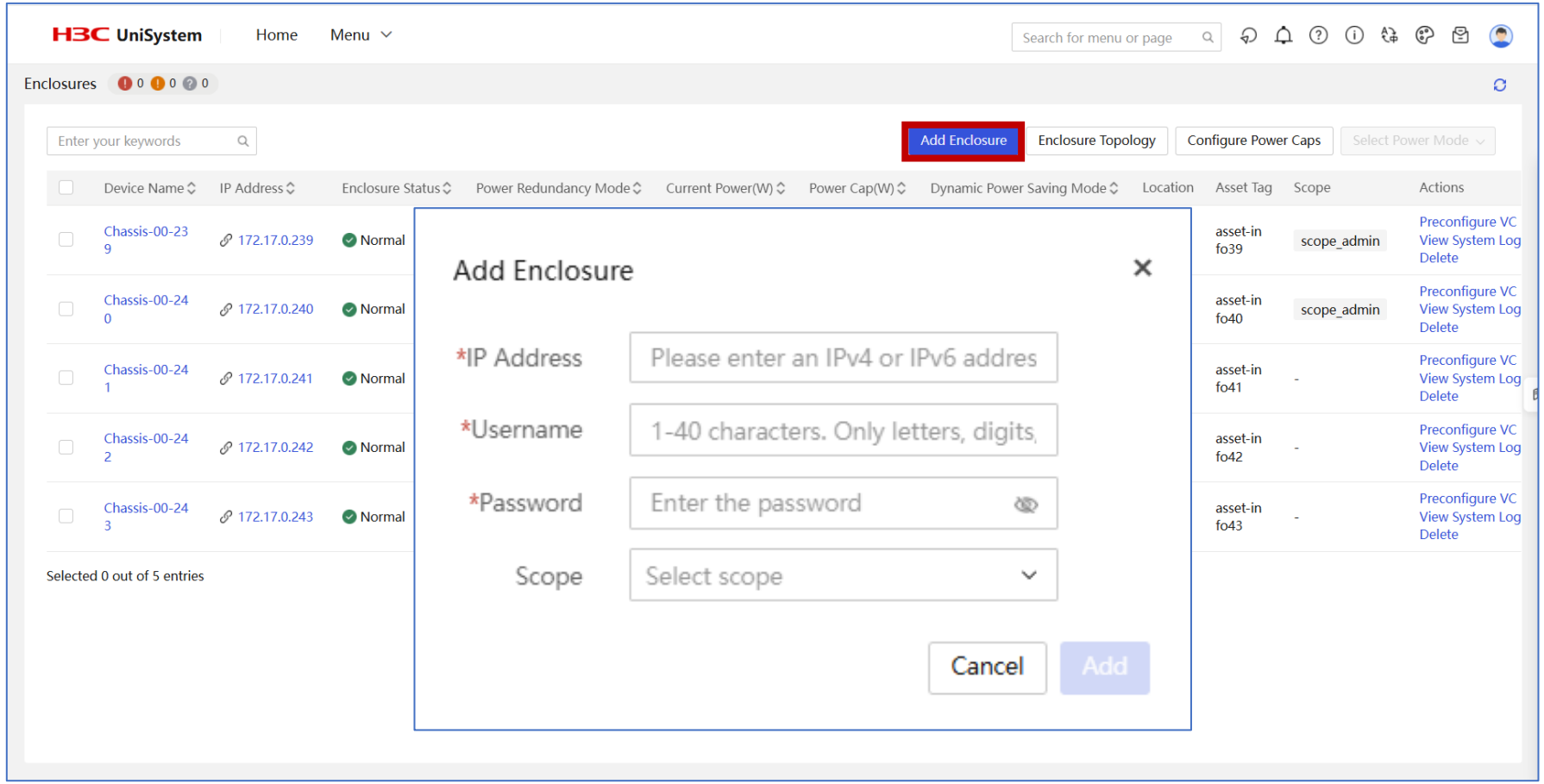
ユーザーがエンクロージャーのOMモジュールの管理ポート経由で、AEモジュールにデプロイされたUniSystemに正常にアクセスできるようにするには、UniSystemの管理IPアドレスが割り当てられているポートにセカンダリIPアドレスを追加し、そのセカンダリIPアドレスが追加対象のスイッチの管理ネットワーク範囲内にあることを確認します。デフォルトでは、UniSystemの管理IPアドレスは「vmng.om」という名前のNICに割り当てられています。

Menu > Devices > Switches > スイッチを選択 > Port



- **Summary**:デバイス名、モデル、バージョン、管理IPアドレスなど、スイッチの基本情報を表示します。
- **Cards**:カード名、モデル、ステータス、CPU使用率、メモリー使用率など、スイッチ上のカードに関する情報を表示します。
- **Ports**: スイッチの物理イーサネットおよびFCポートに関する情報を表示します。このタブには、各物理ポートのPVID、リンクタイプ、MACアドレス、トラフィック統計情報、およびピアエンド情報が表示されます。
- **Interfaces**:スイッチのカード上の論理インターフェイスに関する情報を表示します。

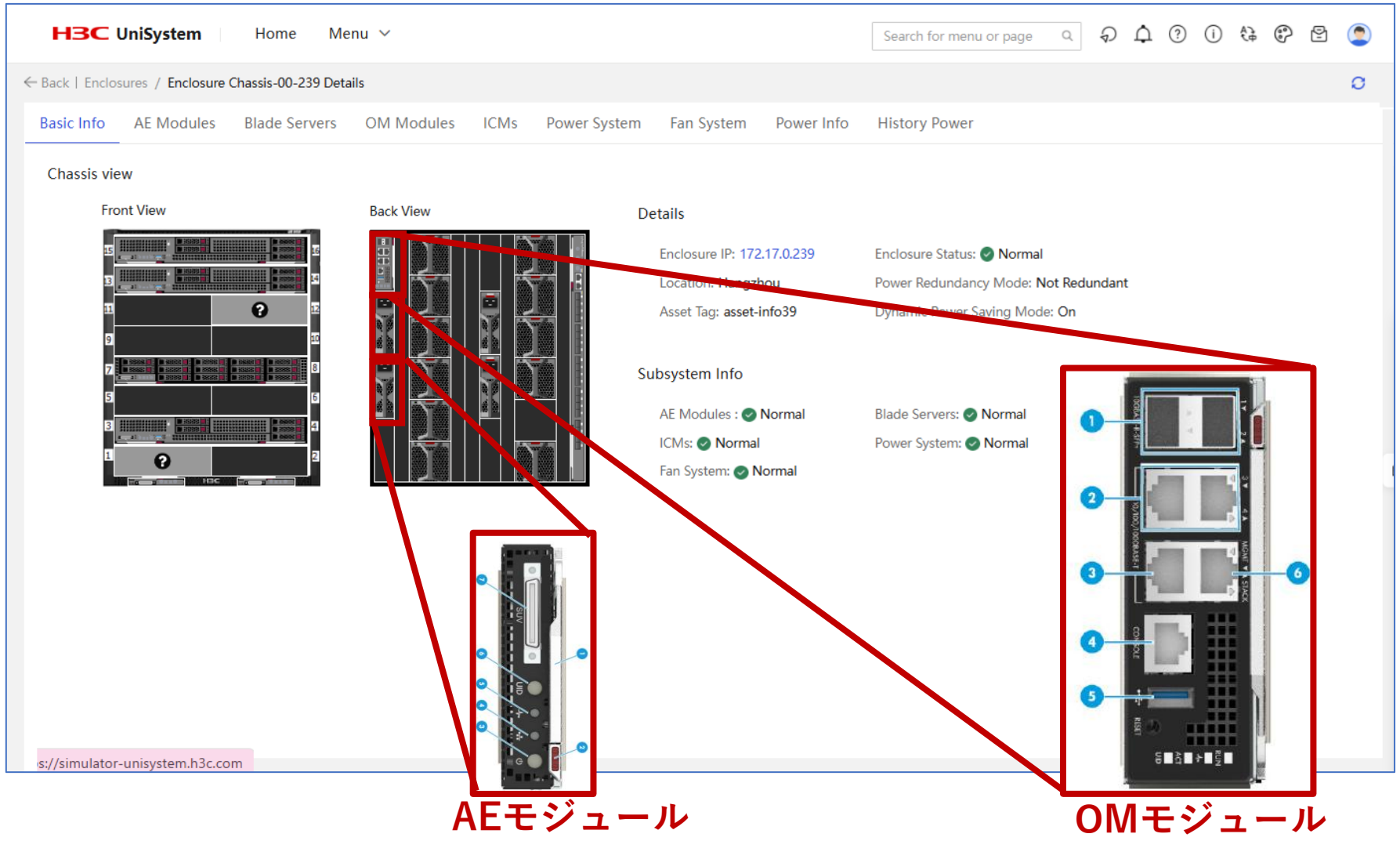
Menu > Device > Enclosures > Add Enclosure



エンクロージャーとはブレードサーバーを収容する筐体の事でOMモジュールのIPアドレスで管理します。

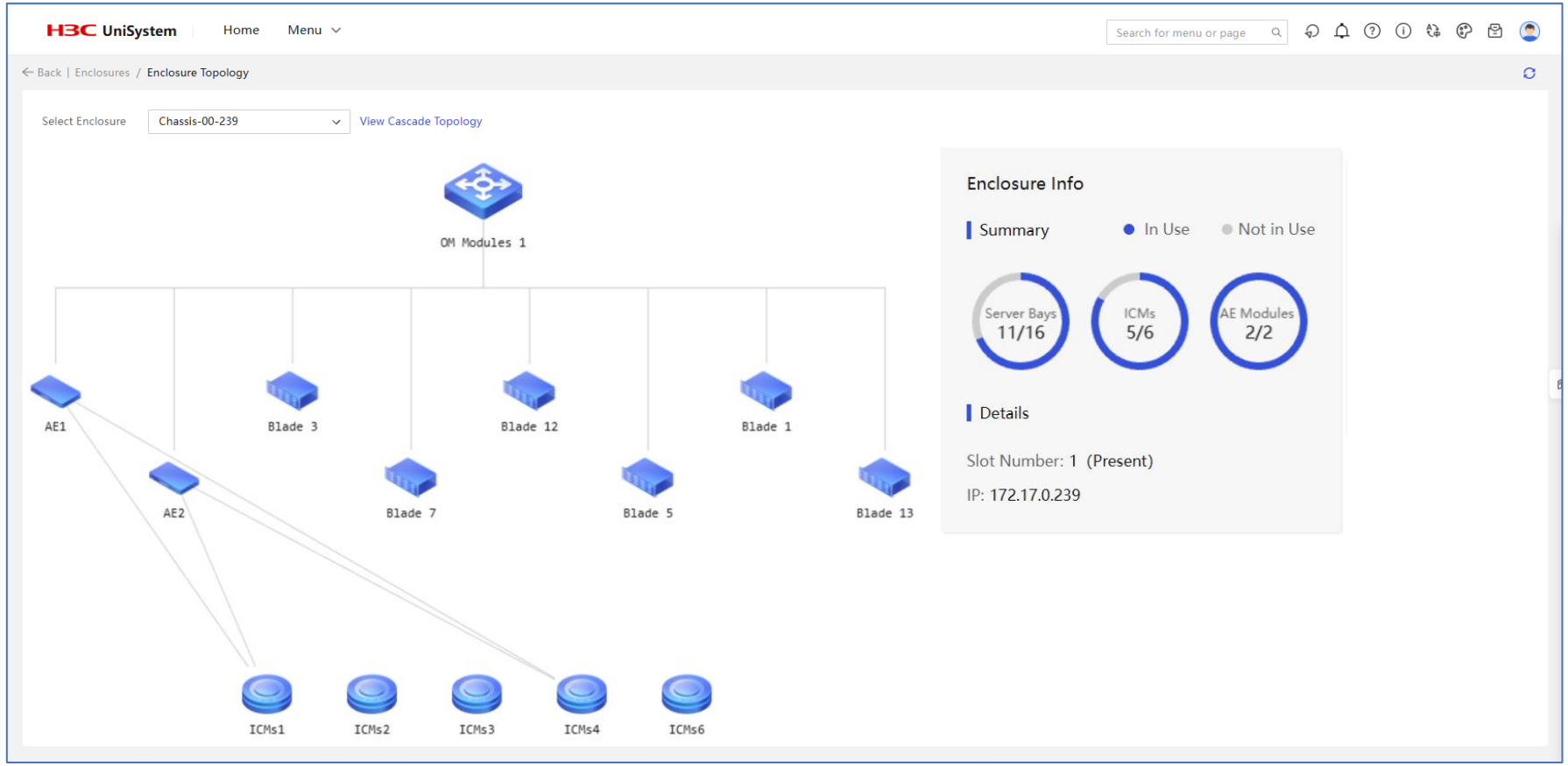
UniSystemにエンクロージャを追加するには、このタスクを実行します。追加するエンクロージャにカスケード接続されたエンクロージャがある場合、UniSystemはそれらのカスケード接続されたエンクロージャも自動的に追加します。

Menu > Device > Enclosures > Device Nameをクリック



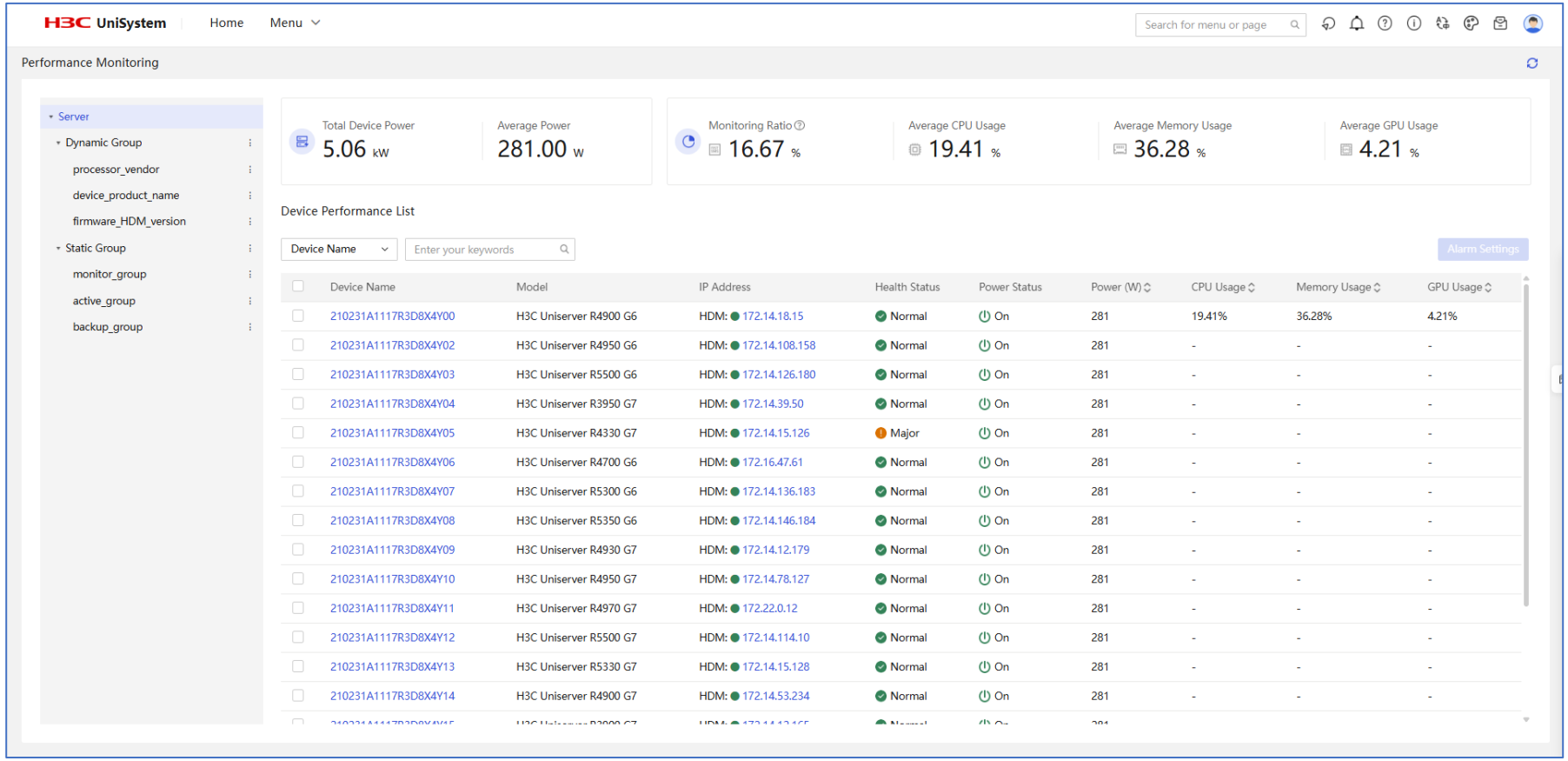
UniSystemがAEモジュール内で動作している場合、そのAEモジュールが搭載されているエンクロージャは自動的にUniSystemに追加され、削除することはできません。 Unisystemがインストールされている**AEモジュール**にも2つのIPアドレスが設定されています。

Menu > Device > Enclosures > Enclosure Topologies



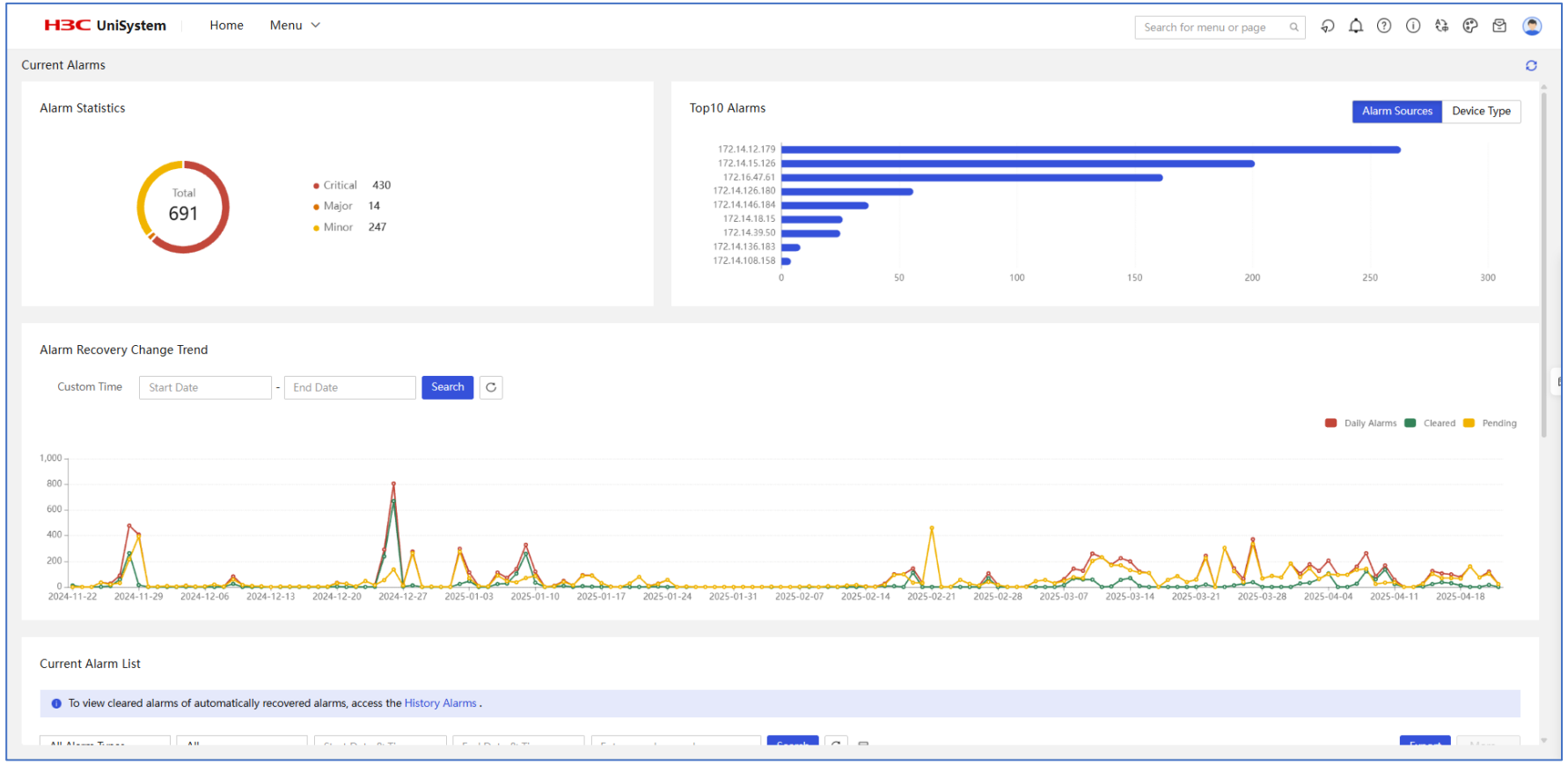
エンクロージャを追加する前に、**追加するエンクロージャの OM 管理アドレスが UniSystem サーバー（AE モジュール）と同じサブネット上にあることを確認してください。**追加するエンクロージャの OM 管理アドレスが UniSystem とは異なるサブネット上にある場合は、UniSystem がエンクロージャと通信できるようにネットワーク設定を構成する必要があります。

Menu > Monitor > Performance Monitoring



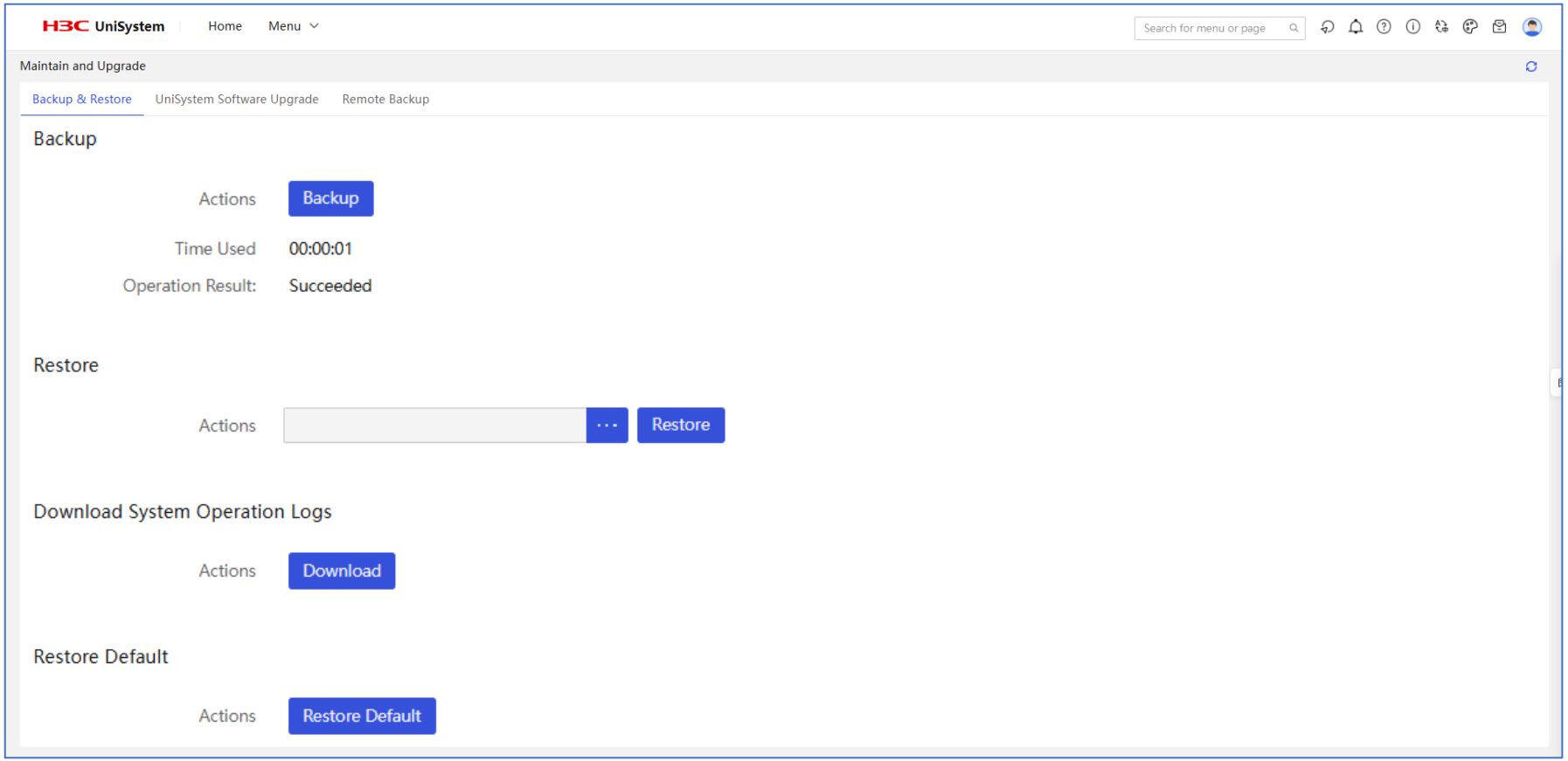
高速診断およびストレステストサーバーの一括実行をサポートし、サーバー上のコンポーネントをスキャンし、各コンポーネントに関する情報を収集および整理し、各コンポーネントの動作およびヘルスステータスを診断します。これにより、タイムリーな問題のトラブルシューティング、デバイス使用リスクの軽減、および診断レポートのエクスポートが容易になります。

Menu > Monitor > Alarm Center > Current Alarms



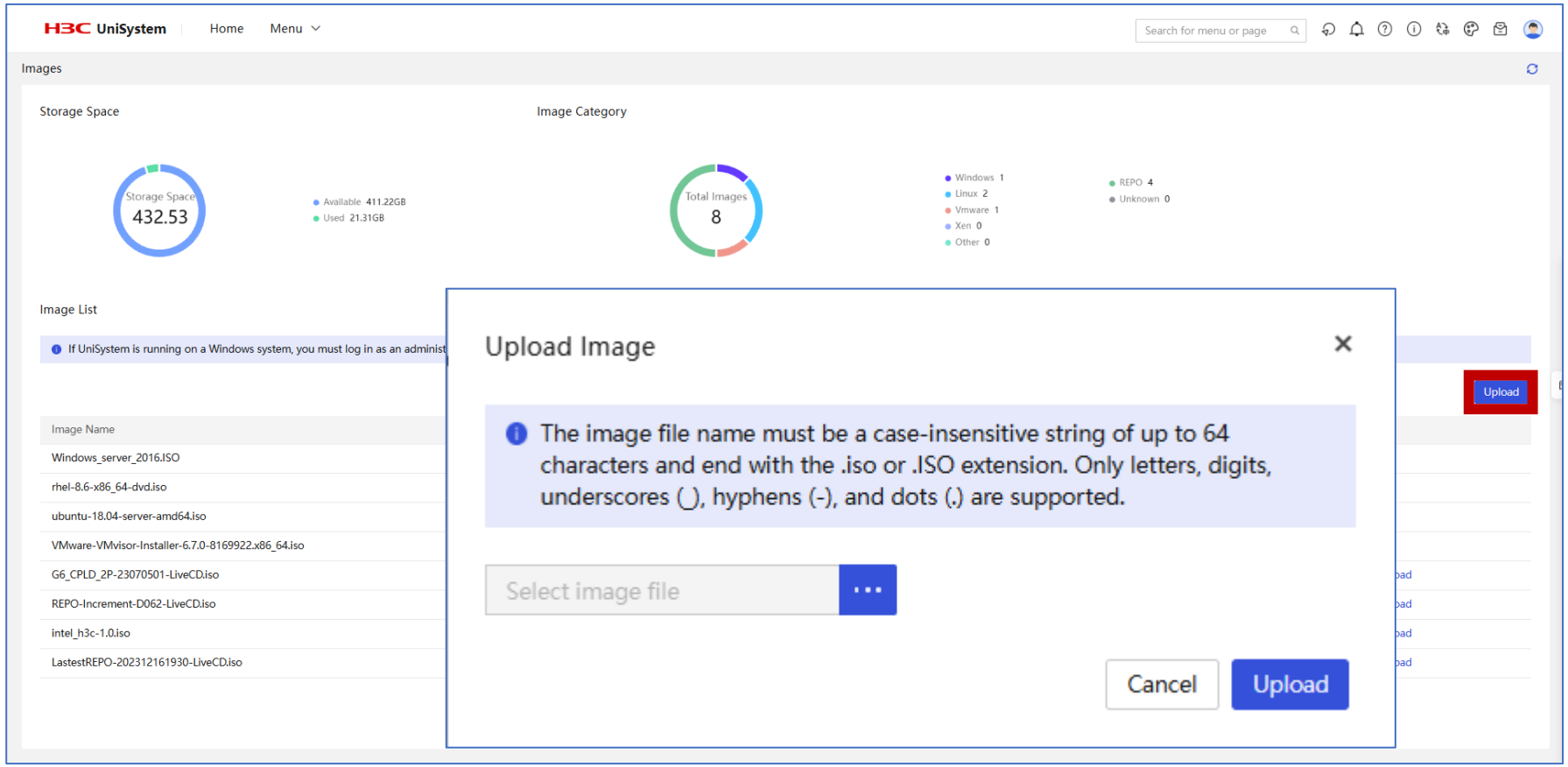
UniSystemは、デバイスアラームの中央集約型表示、照会、抑制、圧縮、ノイズ低減、再定義をサポートしています。**アラーム通知は、電子メール、SMSメッセージ、音声メッセージ、WeCom、DingTalk、Telegram、WhatsAppを通じて配信でき、SNMP転送もサポートされている**ため、アラームの中央集約型管理と迅速な対応が容易になります。

Menu > System > Maintenance and Upgrade > backup & Restore



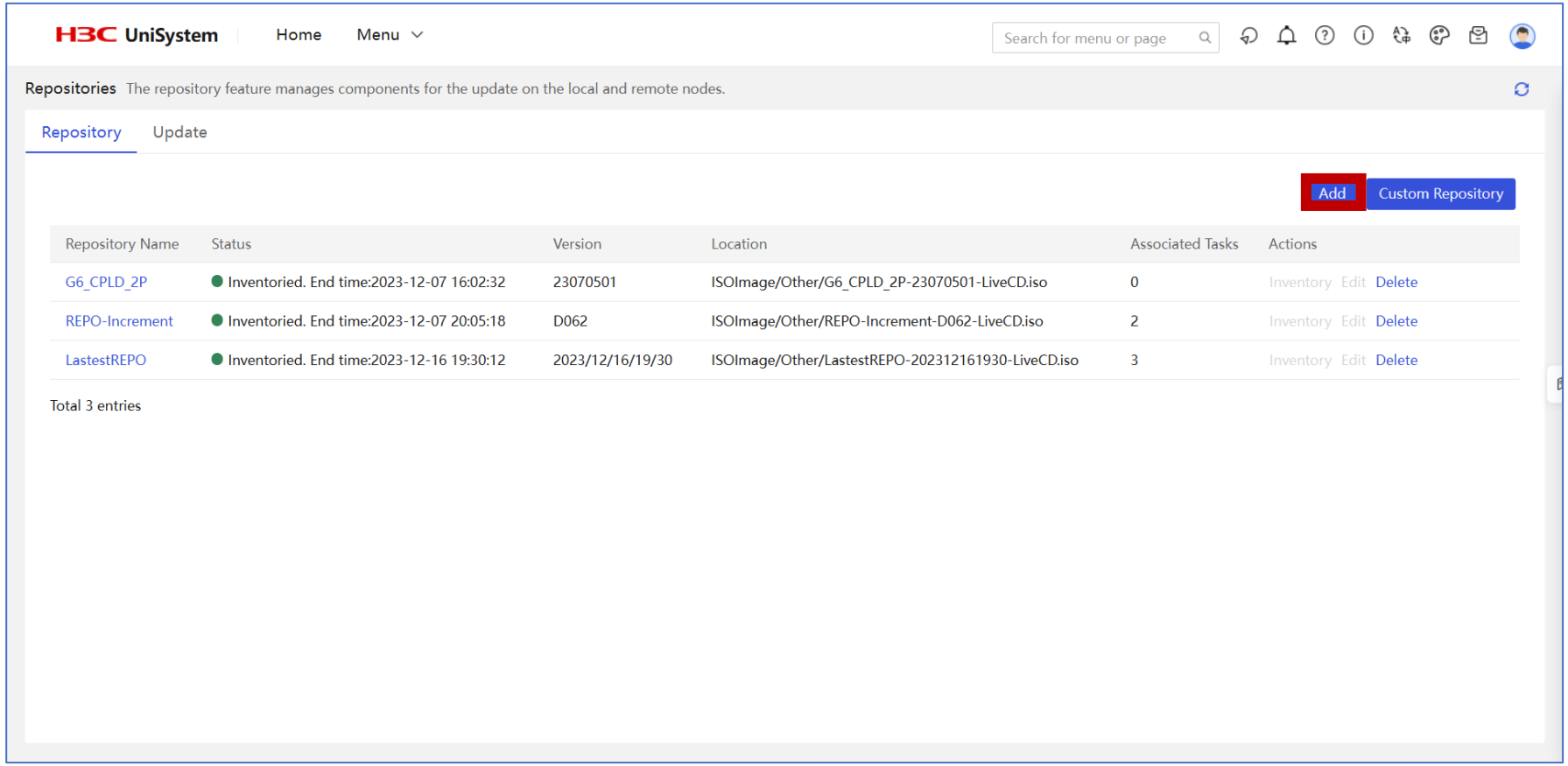
バックアップとリストア

Menu > Images



イメージリストの右上隅にある**Upload**をクリックします。
Upload Imageダイアログボックスが開きます。
Browseボタンをクリックします。表示されたダイアログボックスで、アップロードするイメージファイルを選択します。
Uploadをクリックして、**OSイメージファイルをUniSystemサーバーにアップロード**します。
アップロードが完了すると、**イメージ管理ページにOSイメージファイルが表示されます**。

Menu > templates > Repository



リポジトリは、ファームウェアやドライバといったコンポーネント群の更新パッケージを格納するものです。**UniSystemは、リポジトリ内のコンポーネント更新パッケージを使用して、ローカルサーバーやリモートサーバーを更新します。**公式Webサイトから最新のリポジトリを入手してUniSystemに追加したり、UniSystem内でカスタムリポジトリ（.isoファイル）を作成したりすることが可能です。また、「LatestREPO」イメージに対して自動更新機能を有効にすることもできます。この機能を有効にすると、システムはREPO公式Webサイトから最新のリポジトリをダウンロードし、それに基づいて「LatestREPO」イメージを自動的に生成します。

Repositoryの活用

ファームウェアの更新手順

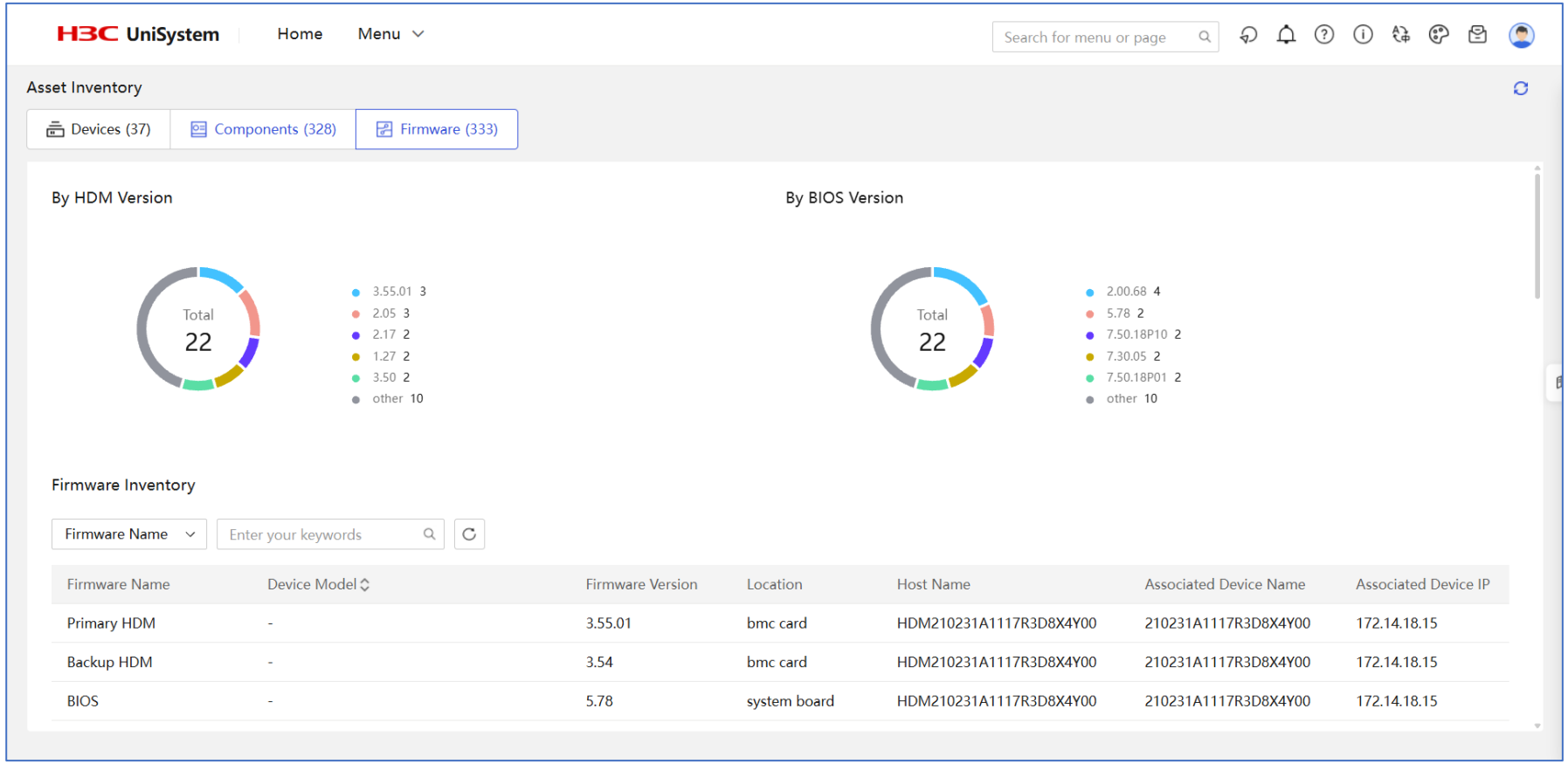
H3C Webサイト(REPO)から、サーバーの機種・構成に適したREPOをPCへダウンロードします。
REPOには、BIOS、HDM、CPLD、RAIDコントローラー、NIC、SSD/HDDなどのファームウェアやドライバーが含まれます。

UniSystemを起動し、**Template > Repository > Add Repository**から、PCにダウンロードしたREPOをUniSystemへアップロードします。**REPOの登録完了後、UniSystemによってInventoryが実行されます。**

OSをインストールする場合は、**Template > Server Template > Add**から、OSおよびドライバーのインストールに使用するServer Templateを作成します。

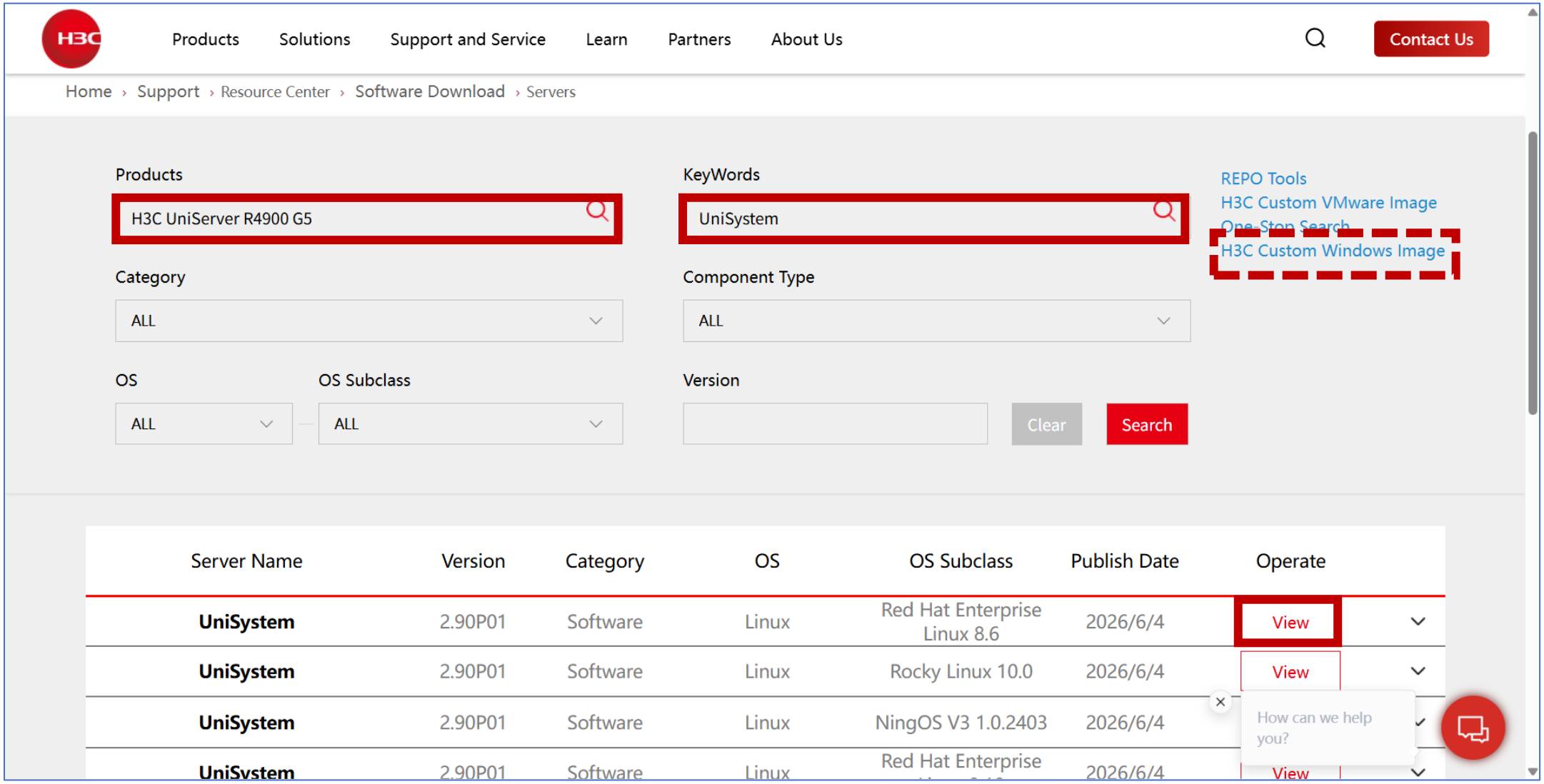
注意：「OS設定」ページで「応答ファイルを使用する」方法を選択した場合は、「テンプレートのダウンロード」をクリックして、そのシステム用の応答ファイルテンプレートを入手してください。その後、テンプレートに同梱されているREADMEファイルの指示に従って、応答ファイルの設定を定義します。形式が正しくない応答ファイルや無効な設定を含む応答ファイルを使用すると、サーバーテンプレートの作成に失敗する可能性があります。

Menu > Asset Management > Asset Inventory

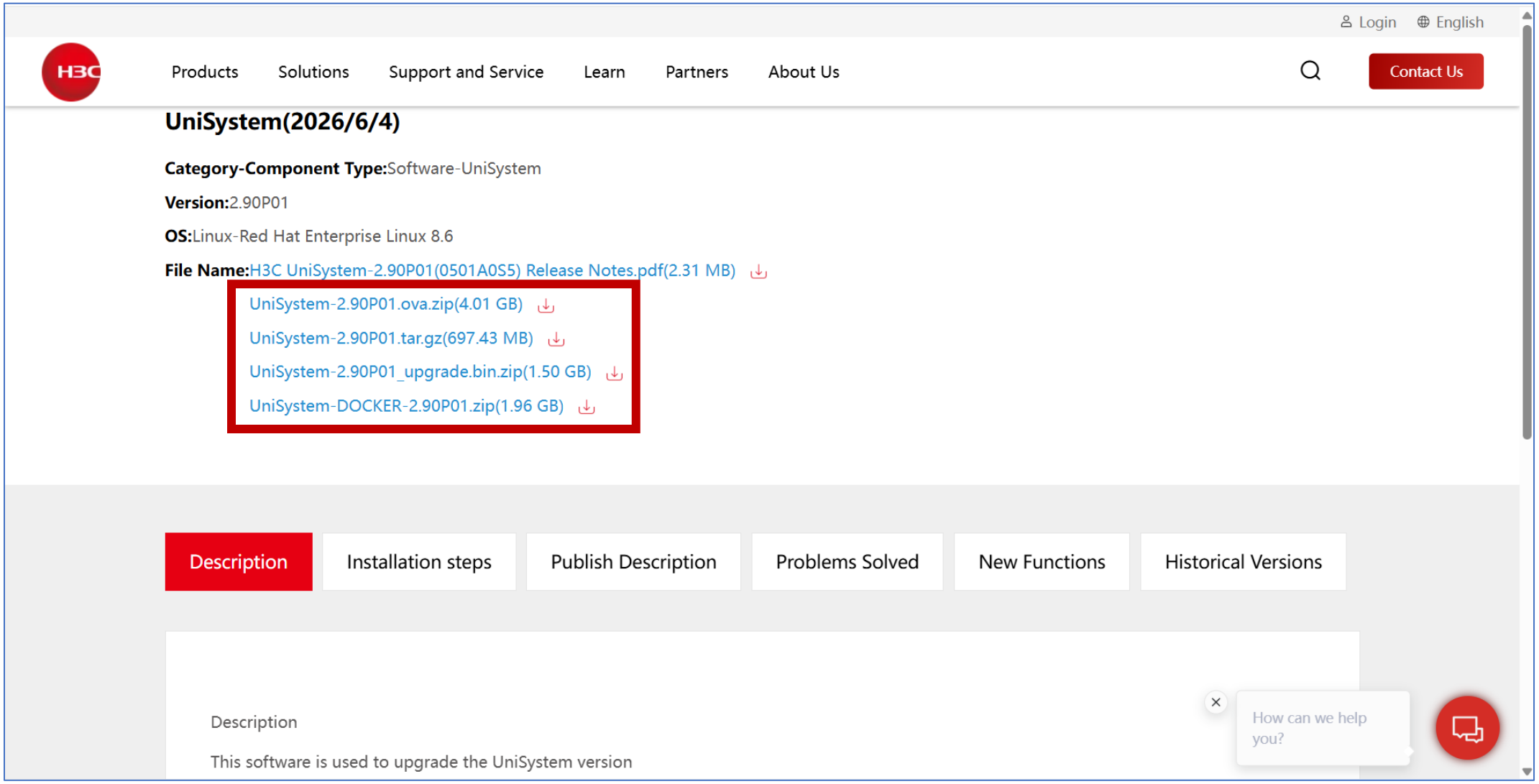


デバイスインベントリページでは、モデル、健全性ステータス、メーカー（インフラストラクチャのみ）に関する統計情報や、デバイスの詳細情報を確認できます。また、このページでは以下の操作も可能です。シリアル番号の左側にあるアイコンをクリックすると、資産のライフサイクルを確認できます。開始日と終了日を入力して「検索」をクリックすると、該当する変更履歴を検索できます。「アクション」列の「リスト」をクリックすると、そのデバイスの全コンポーネントのリストを表示できます。コンポーネントインベントリページでは、モデル、メーカー（ファンおよびRAIDコントローラーを除く）、健全性ステータス（ファンおよびRAIDコントローラーのみ）に関する統計情報や、コンポーネントの詳細情報を確認できます。「ファームウェアインベントリ」エリアでは、HDMおよびBIOSに関する統計情報や、ファームウェアの詳細情報を確認できます。

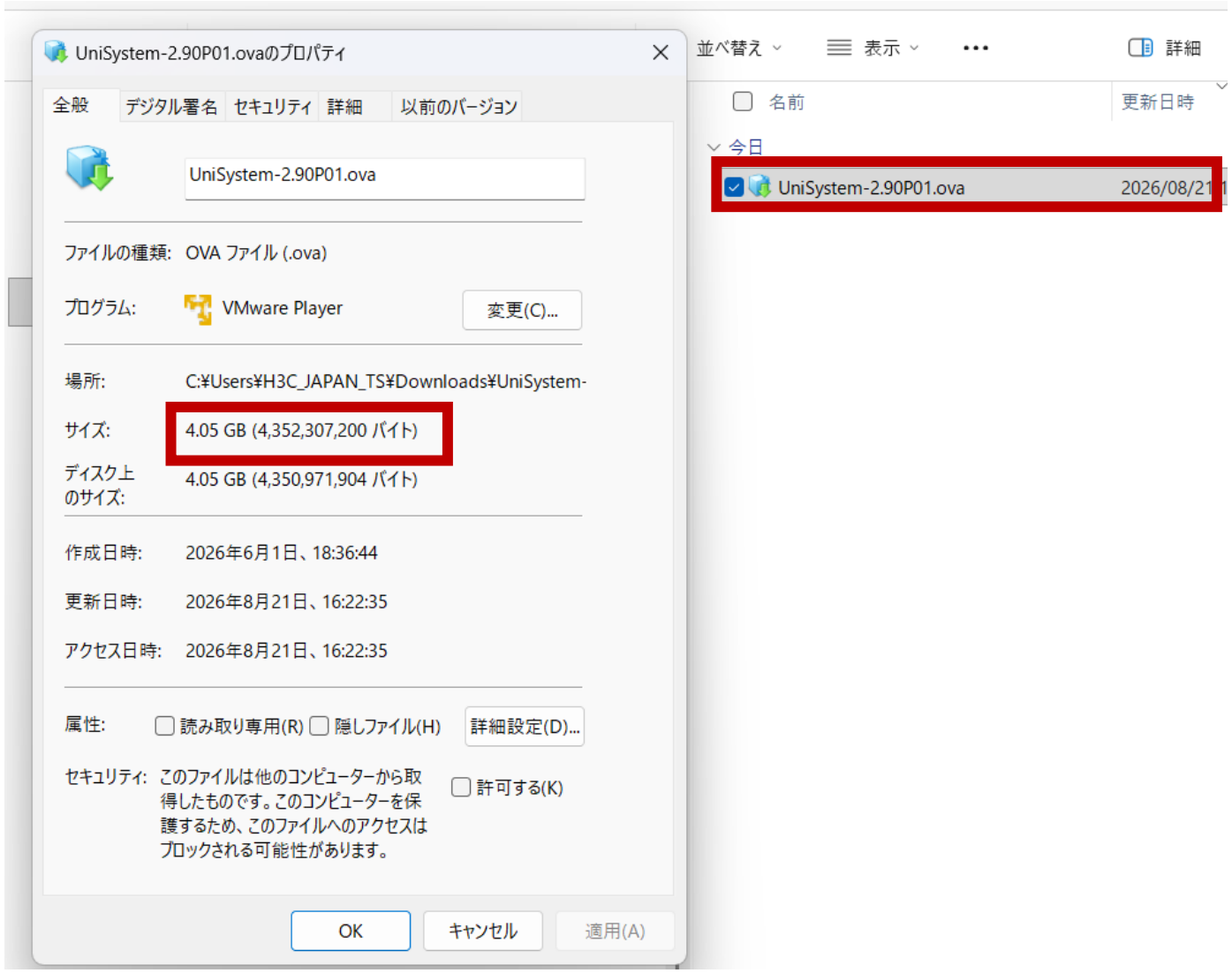
Unisystemファームウェア(サポート>リソースセンター>ソフトウェアダウンロード>サーバー)



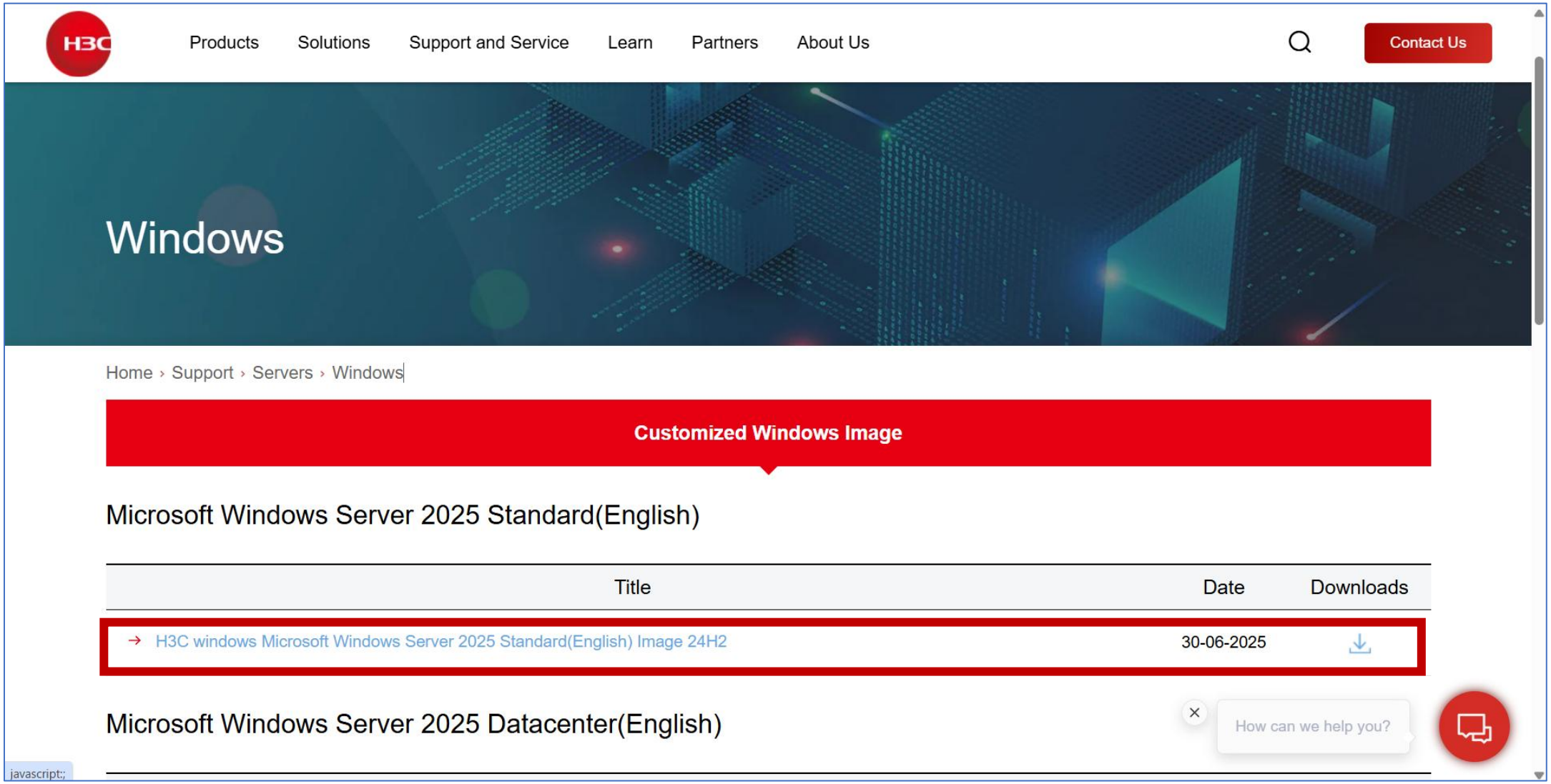
Unisystemファームウェア



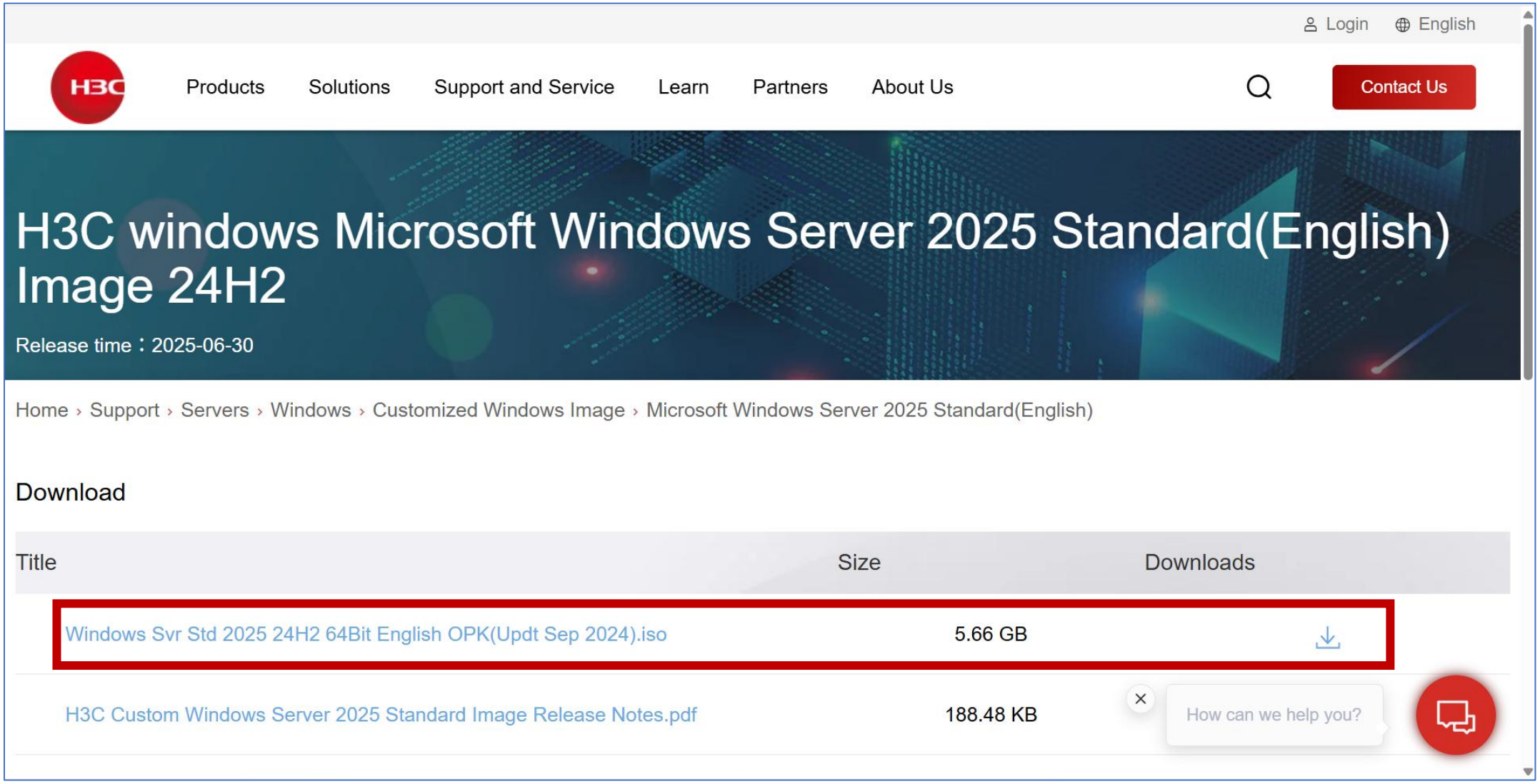
Unisystemファームウェア(Vmwareの場合)



Customized Windows Server Image for H3C Servers



Customized Windows Server Image for H3C Servers





01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

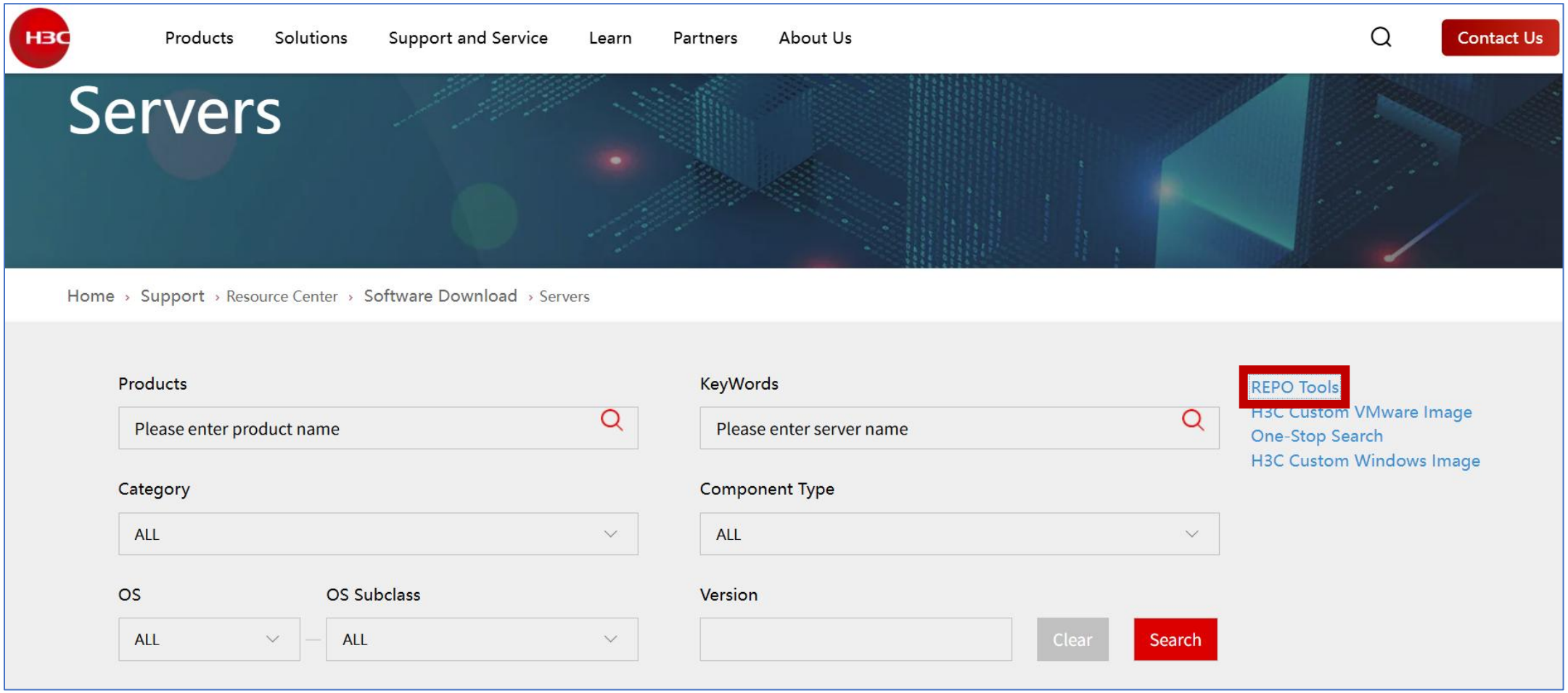
07 REPO

08 U-Center

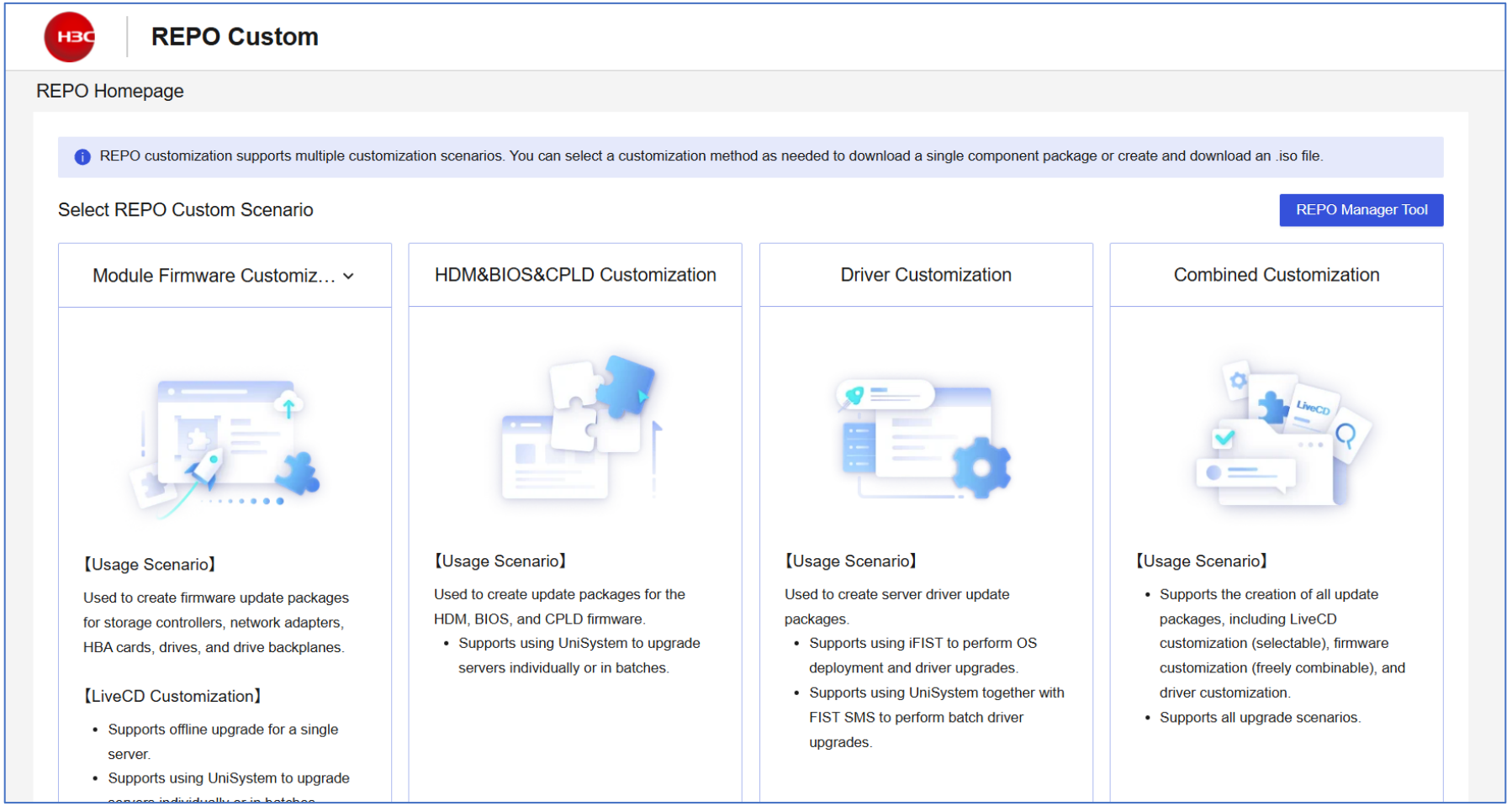
09 ドキュメント

Repositoryの活用

Support > Resource Center > Software Download > Servers

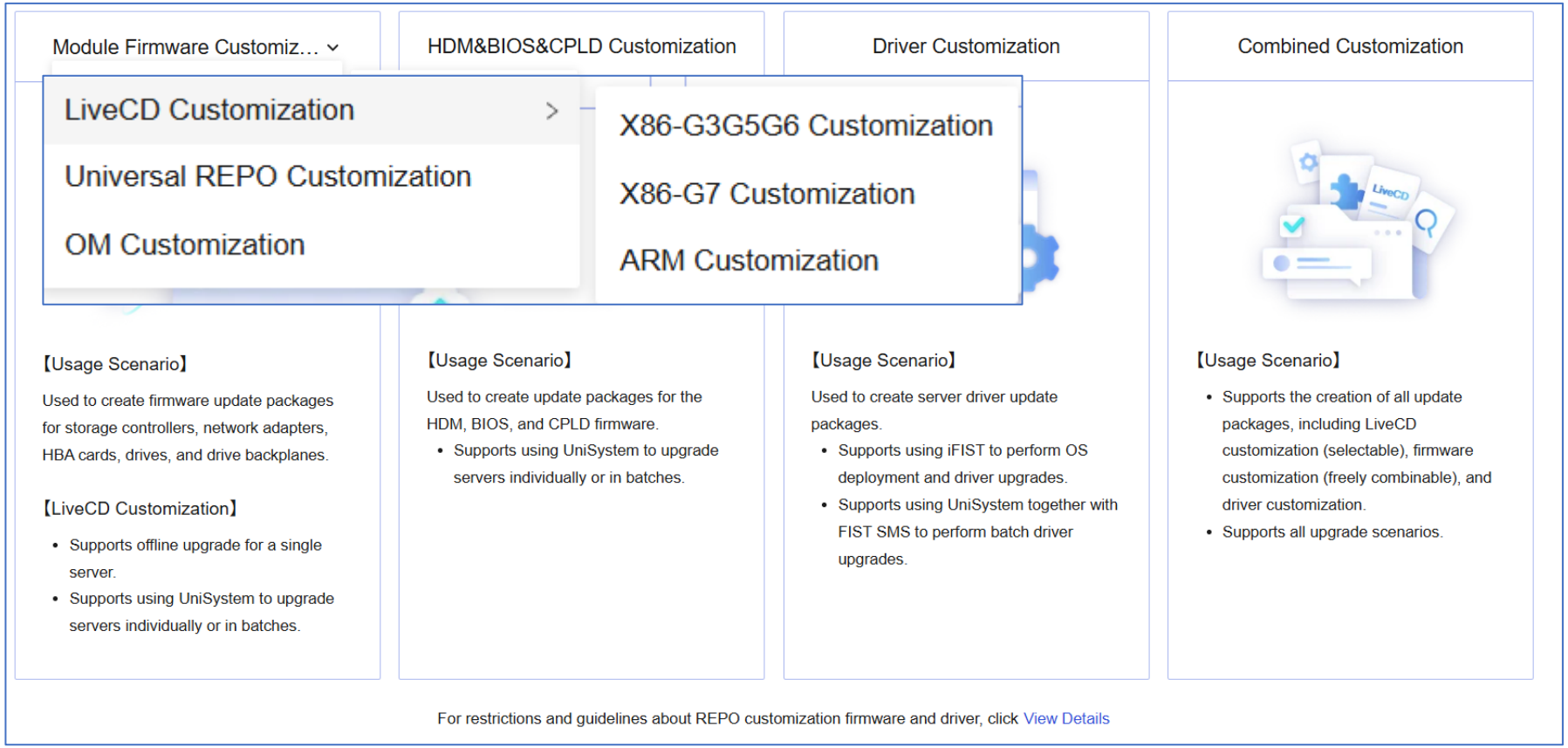


Repositoryの活用



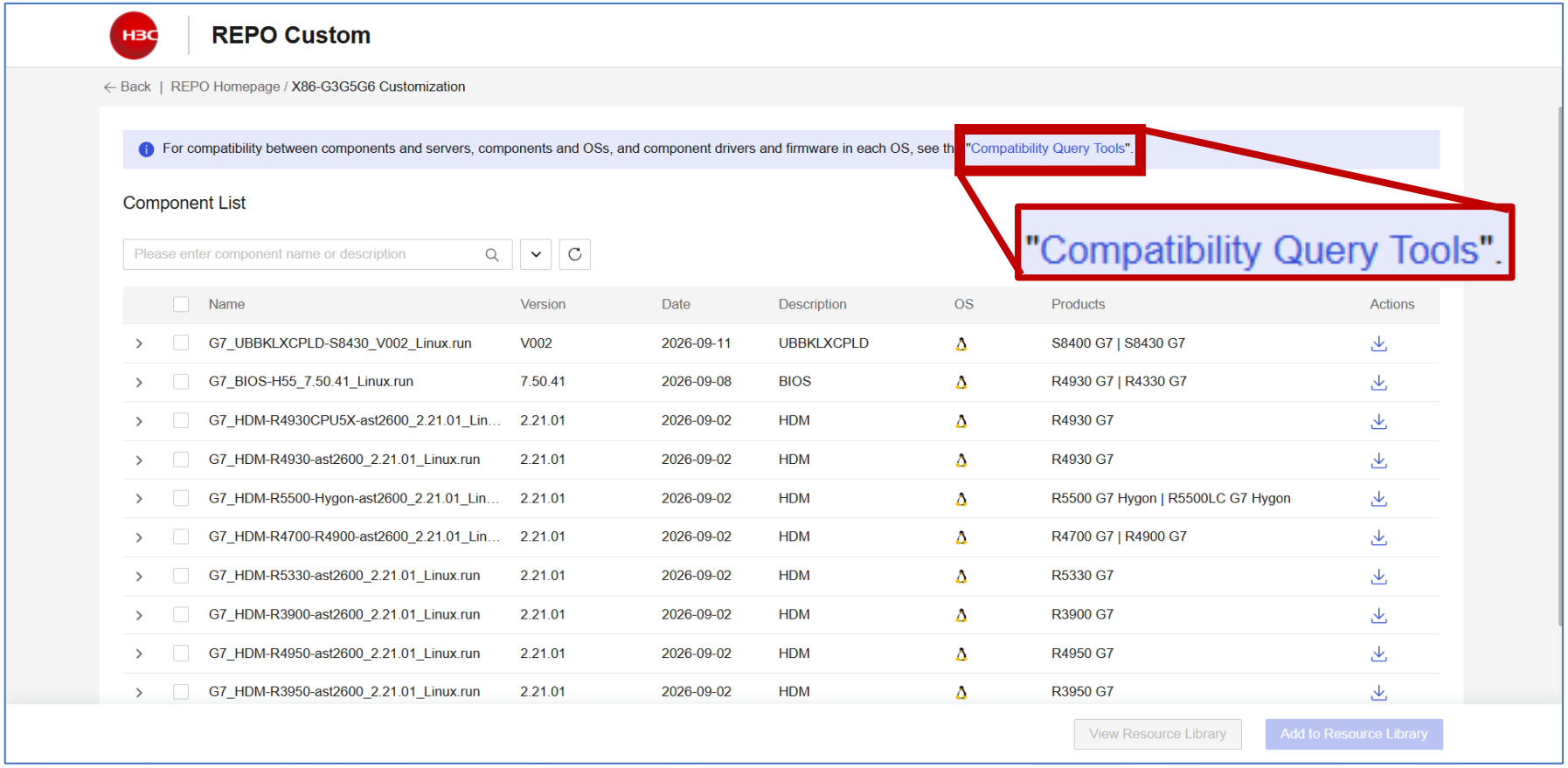
H3Cサーバーの **REPO** は、単純な「ファイル置き場」ではなく、**サーバーのBIOS、HDM、CPLD、RAID、NIC、HDD/SSDなどのファームウェアやドライバーをまとめたリポジトリ**です。

Repositoryの活用: Module Firmware Customization



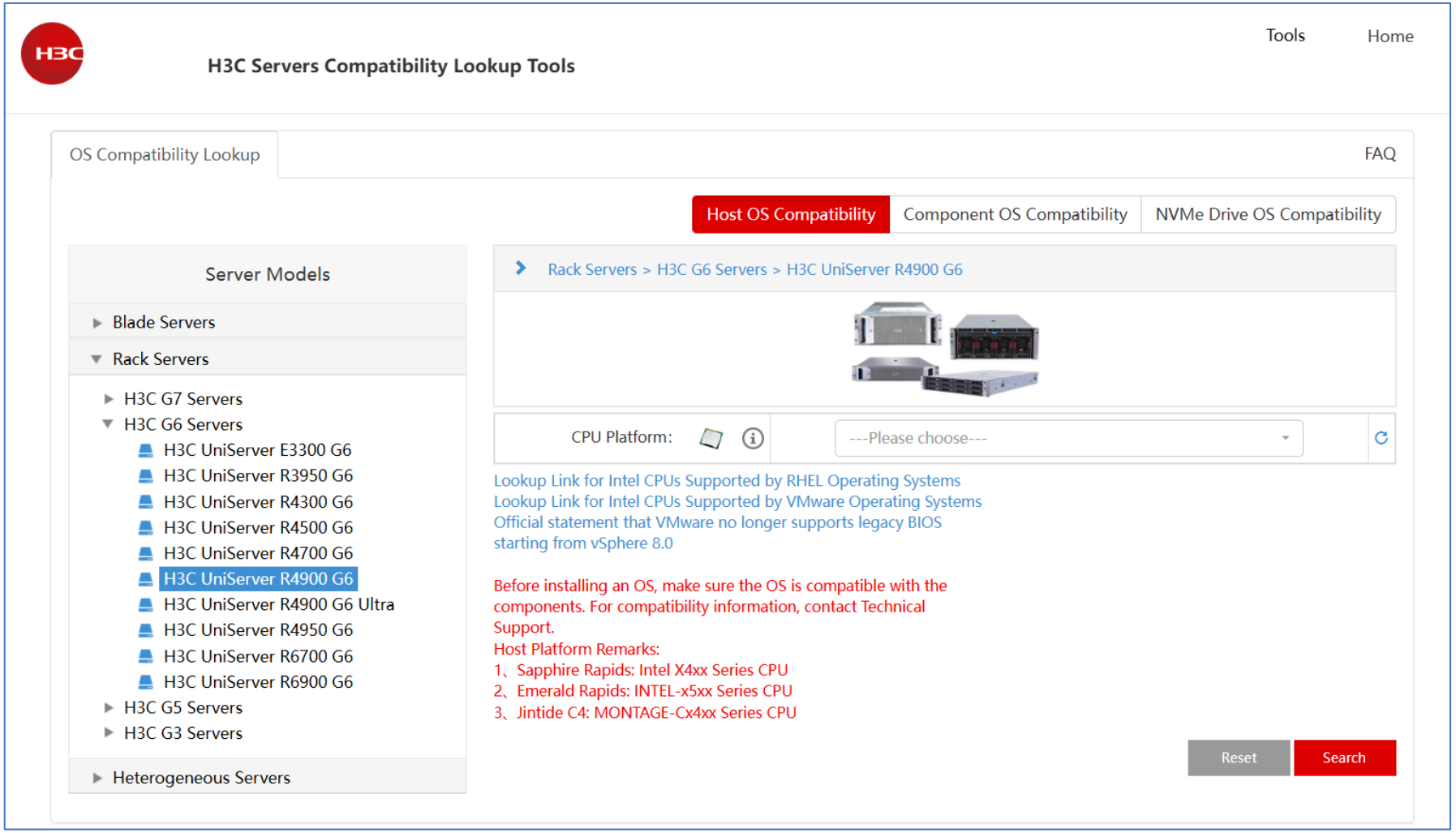
ストレージコントローラ、ネットワークアダプタ、HBAカード、ドライブ、およびドライブバックプレーン用のファームウェアアップデートパッケージを作成するために使用されます。

Repositoryの活用: Module Firmware Customization



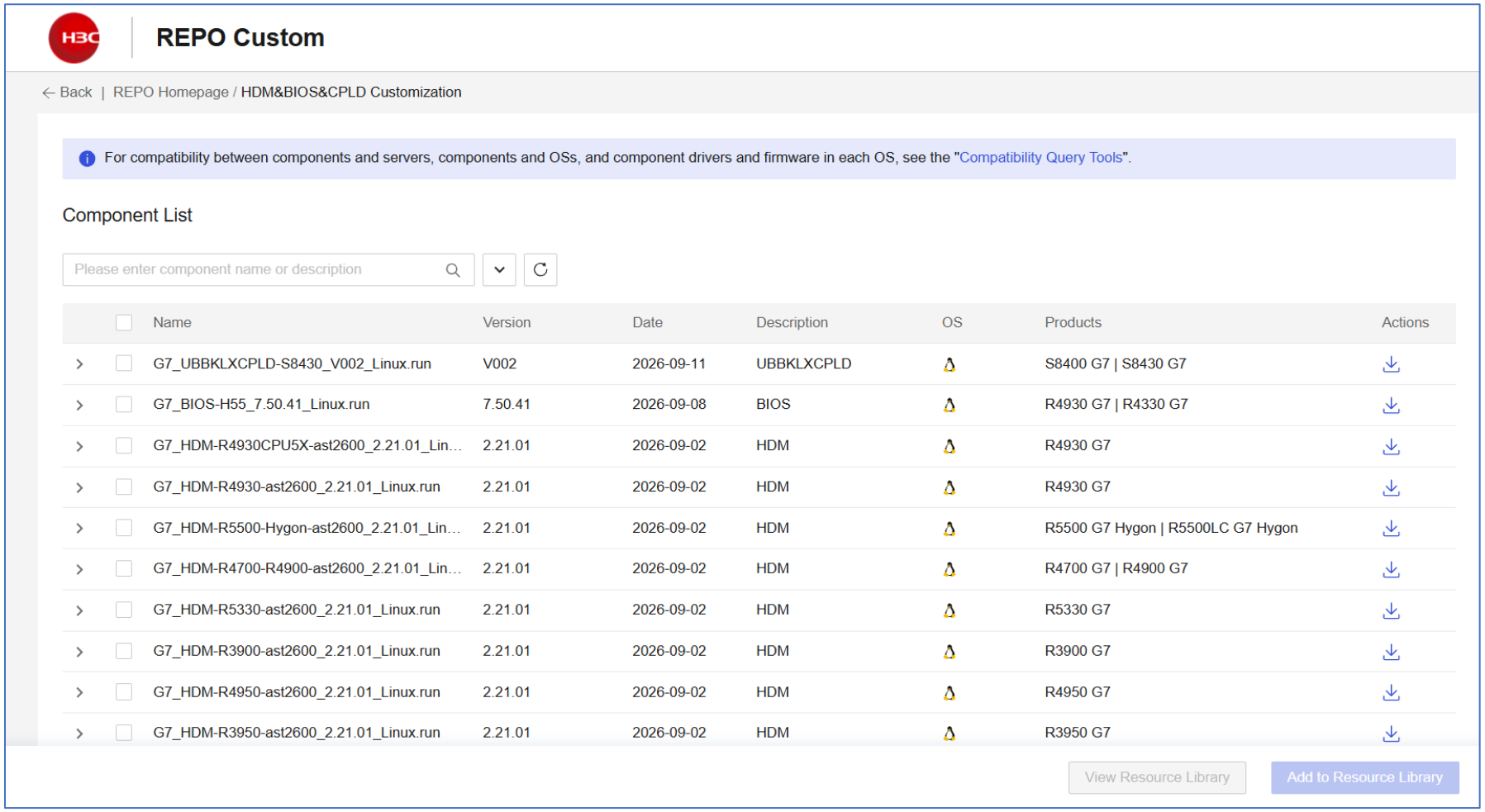
コンポーネントとサーバー間、コンポーネントとOS間、および各OSにおけるコンポーネントドライバとファームウェア間の互換性については、「互換性照会ツール」を参照してください。

Repositoryの活用: 互換性紹介ツール

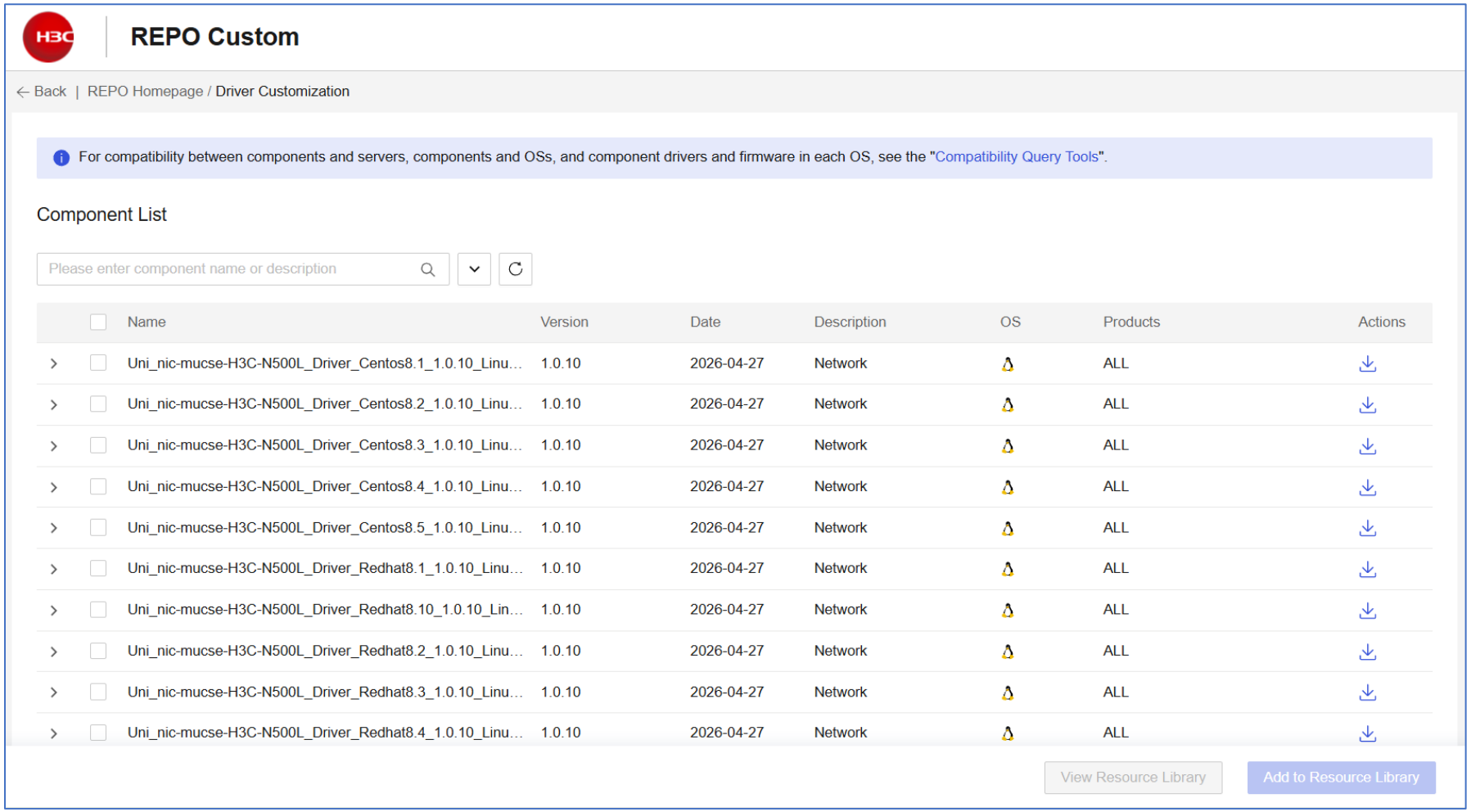


RHELオペレーティングシステムでサポートされているIntel製CPUの検索リンク VMwareオペレーティングシステムでサポートされているIntel製CPUの検索リンク VMwareはvSphere 8.0以降、旧バージョンのBIOSをサポートしなくなったことを公式に発表しています。OSをインストールする前に、そのOSが各コンポーネントと互換性があることを確認してください。互換性に関する情報については、テクニカルサポートにお問い合わせください。ホストプラットフォームに関する備考：1. Sapphire Rapids：Intel X4xxシリーズCPU、2. Emerald Rapids：Intel X5xxシリーズCPU、3. Jintide C4：Montage Cx4xxシリーズCPU

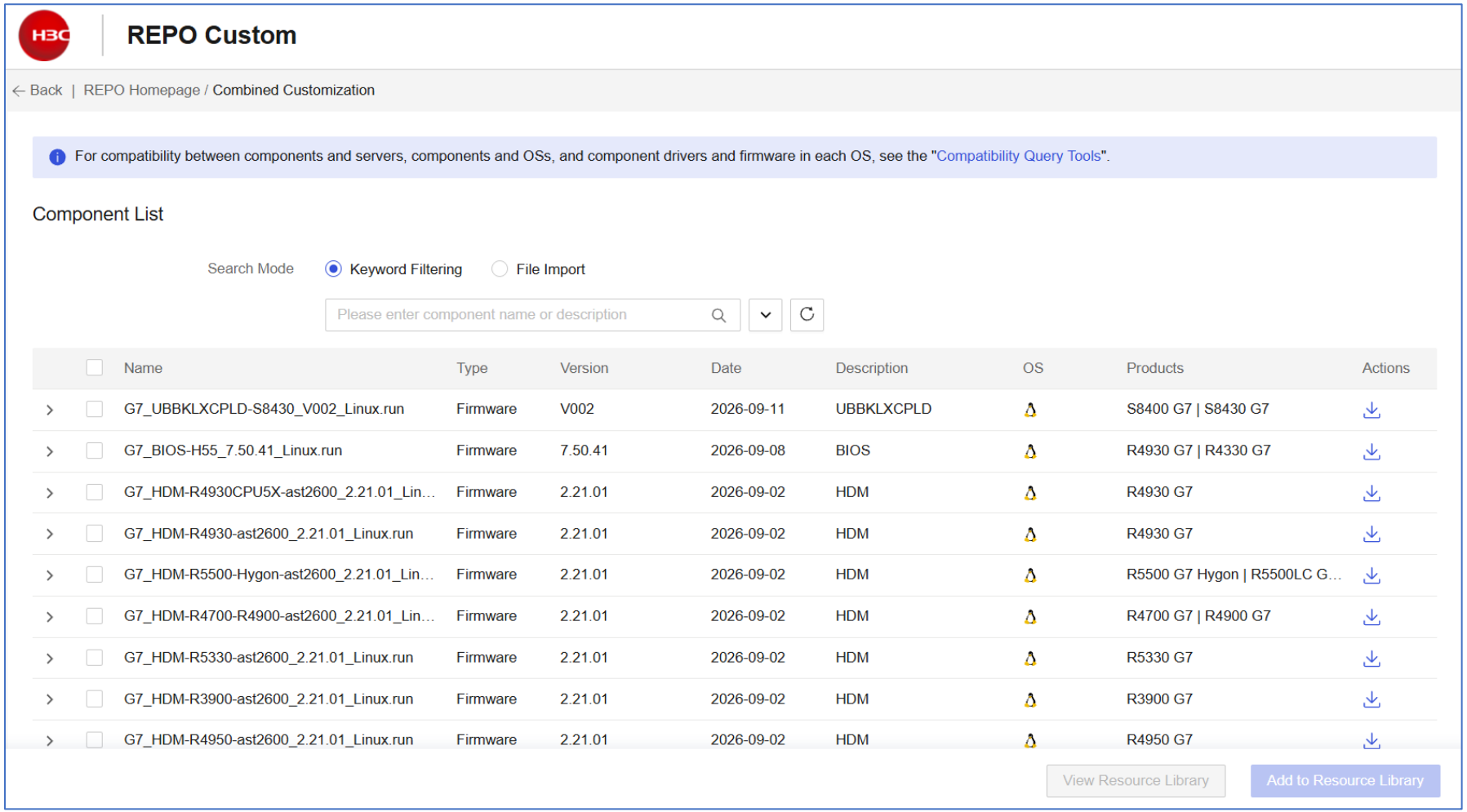
Repositoryの活用: HDM&BIOS&CPLD Customization



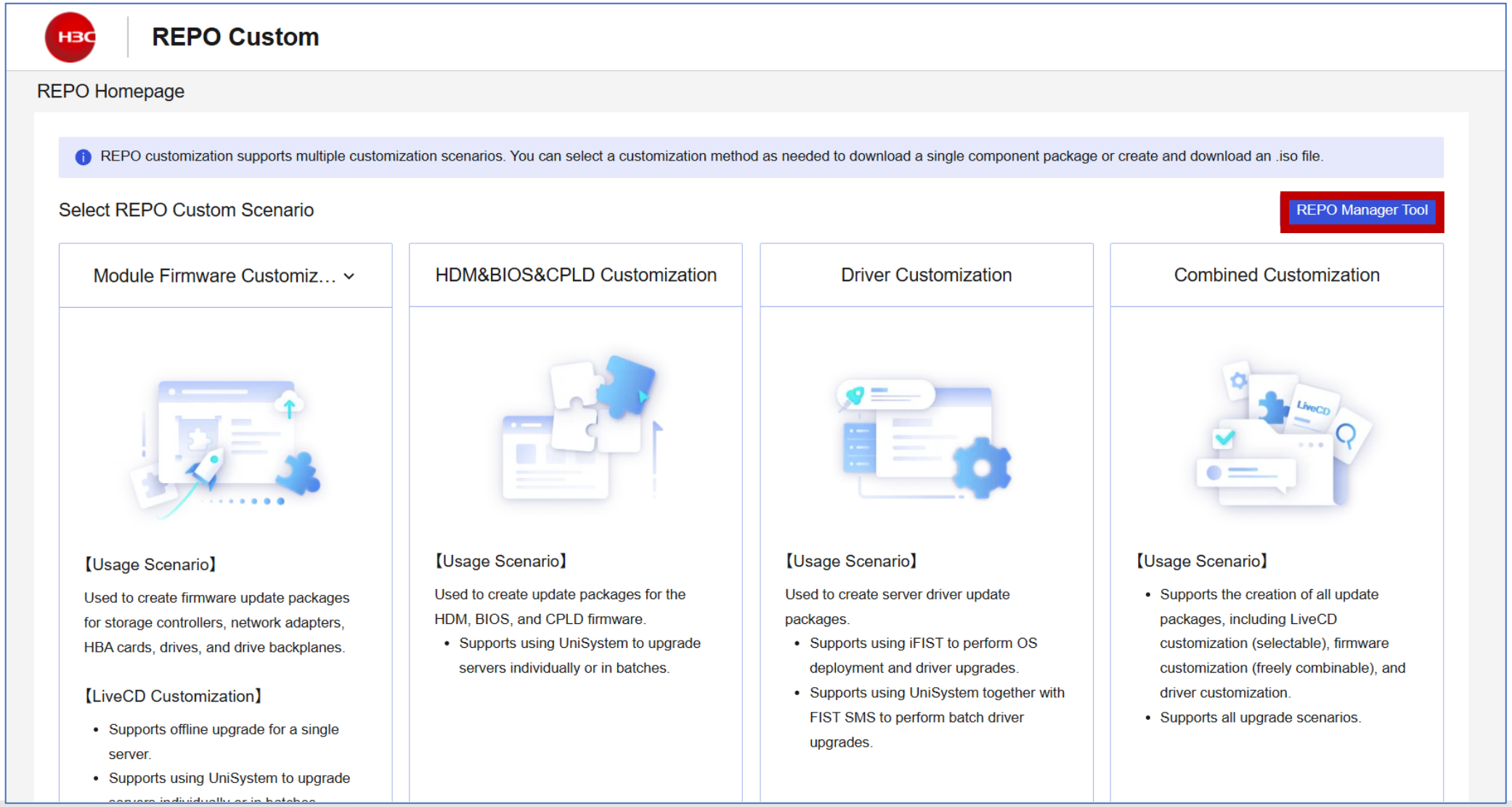
Repositoryの活用: Driver Customization



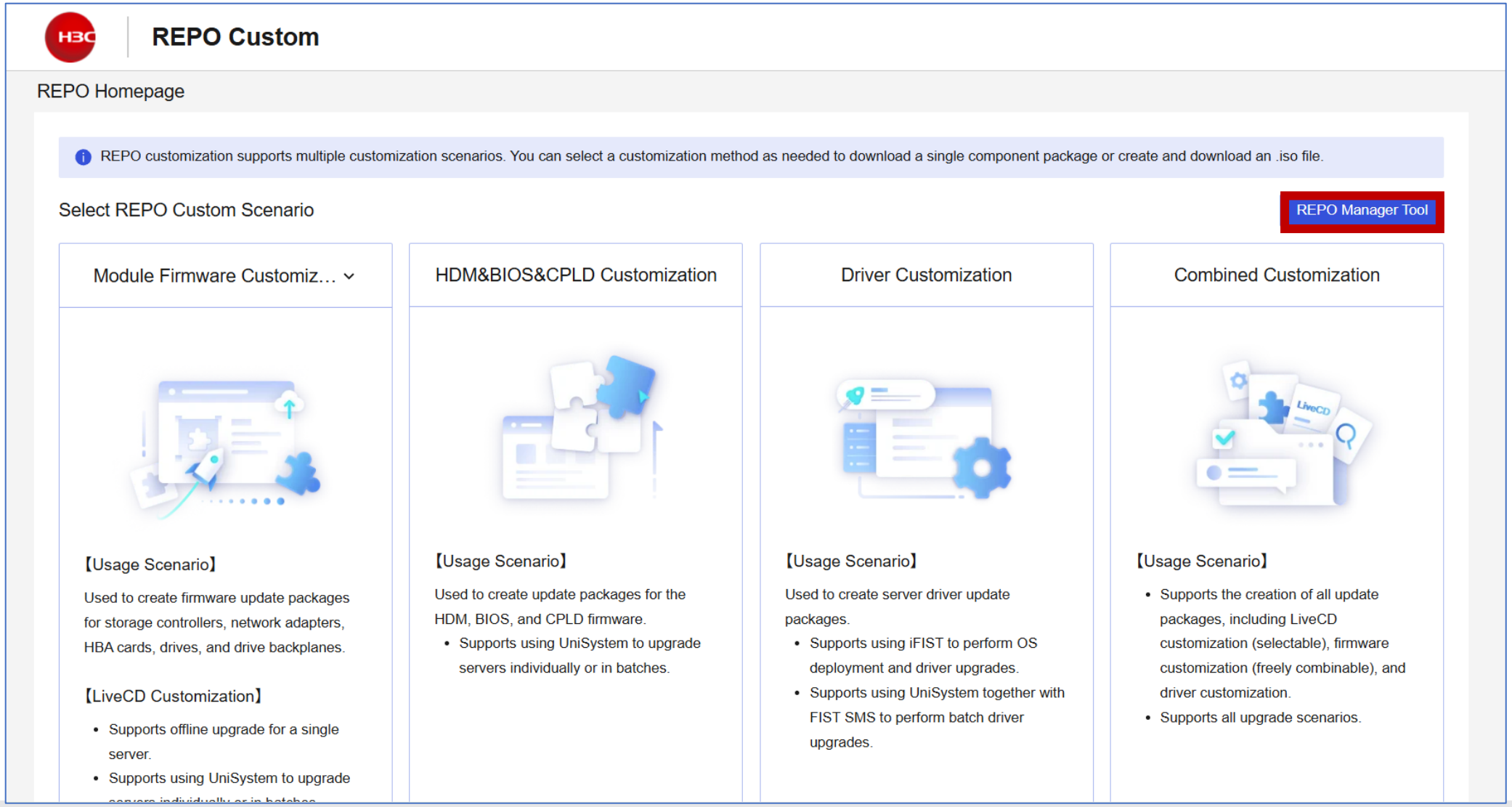
Repositoryの活用: Combined Customization



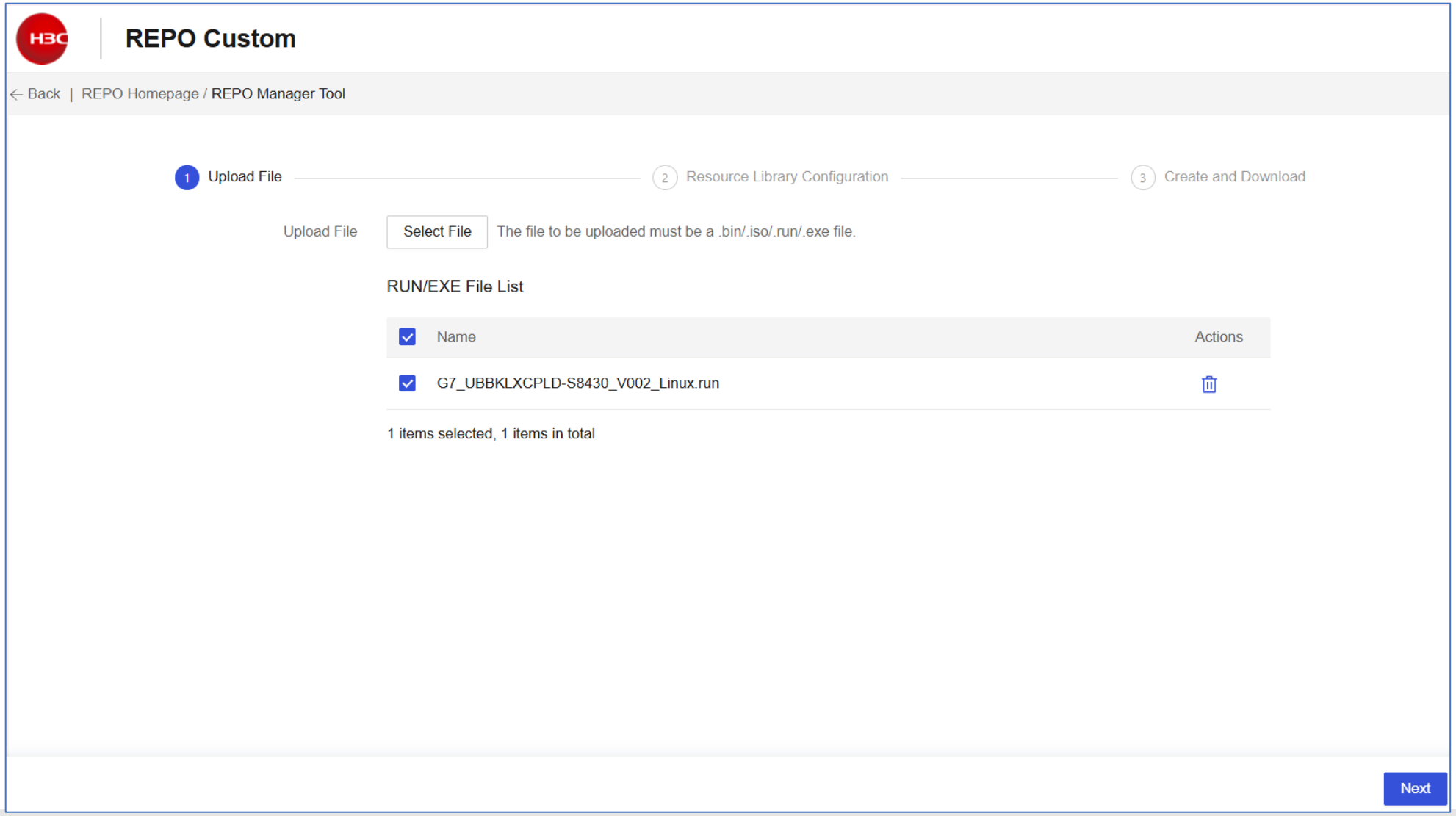
Repositoryの活用: REPO Manager Tool



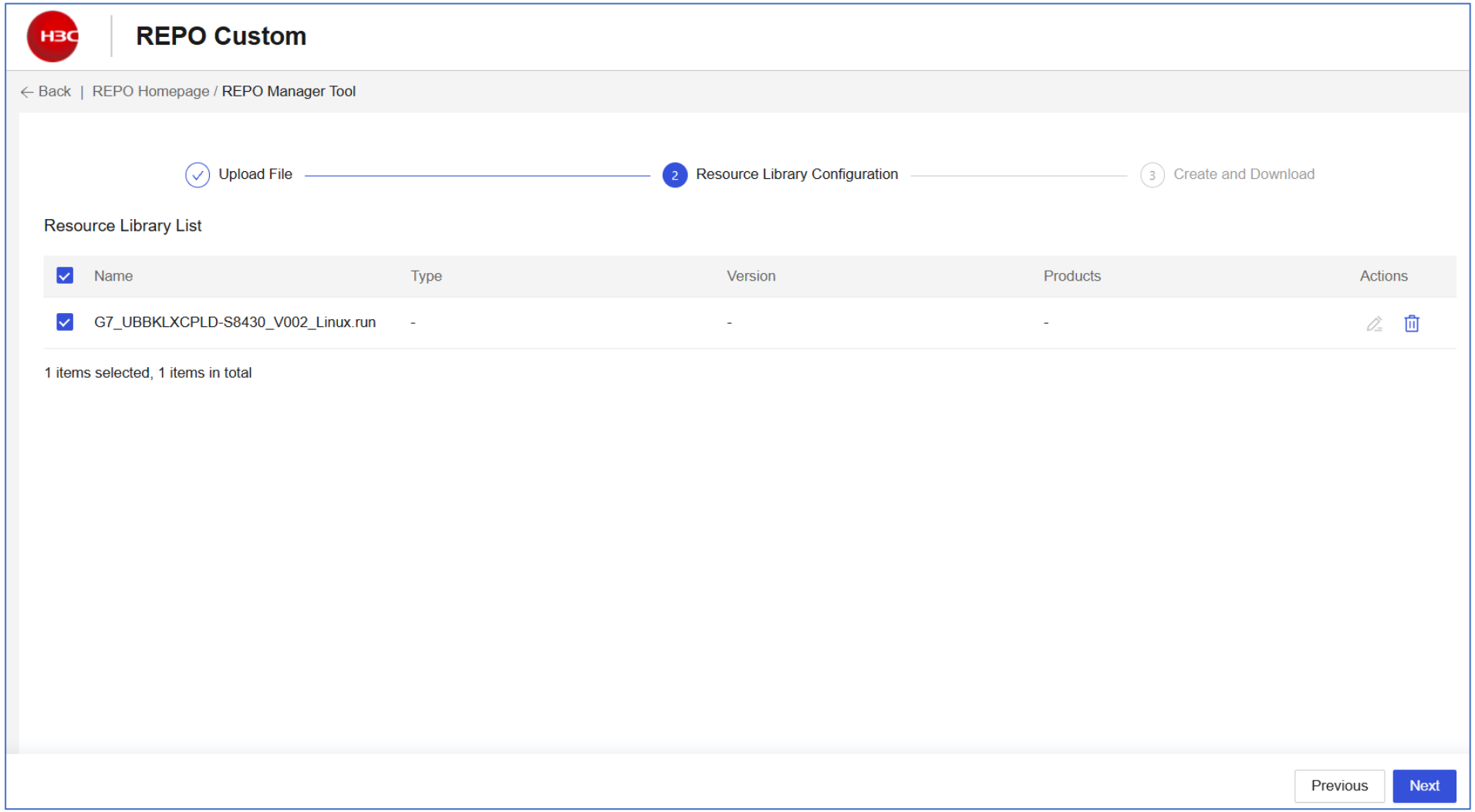
Repositoryの活用: REPO Manager Tool



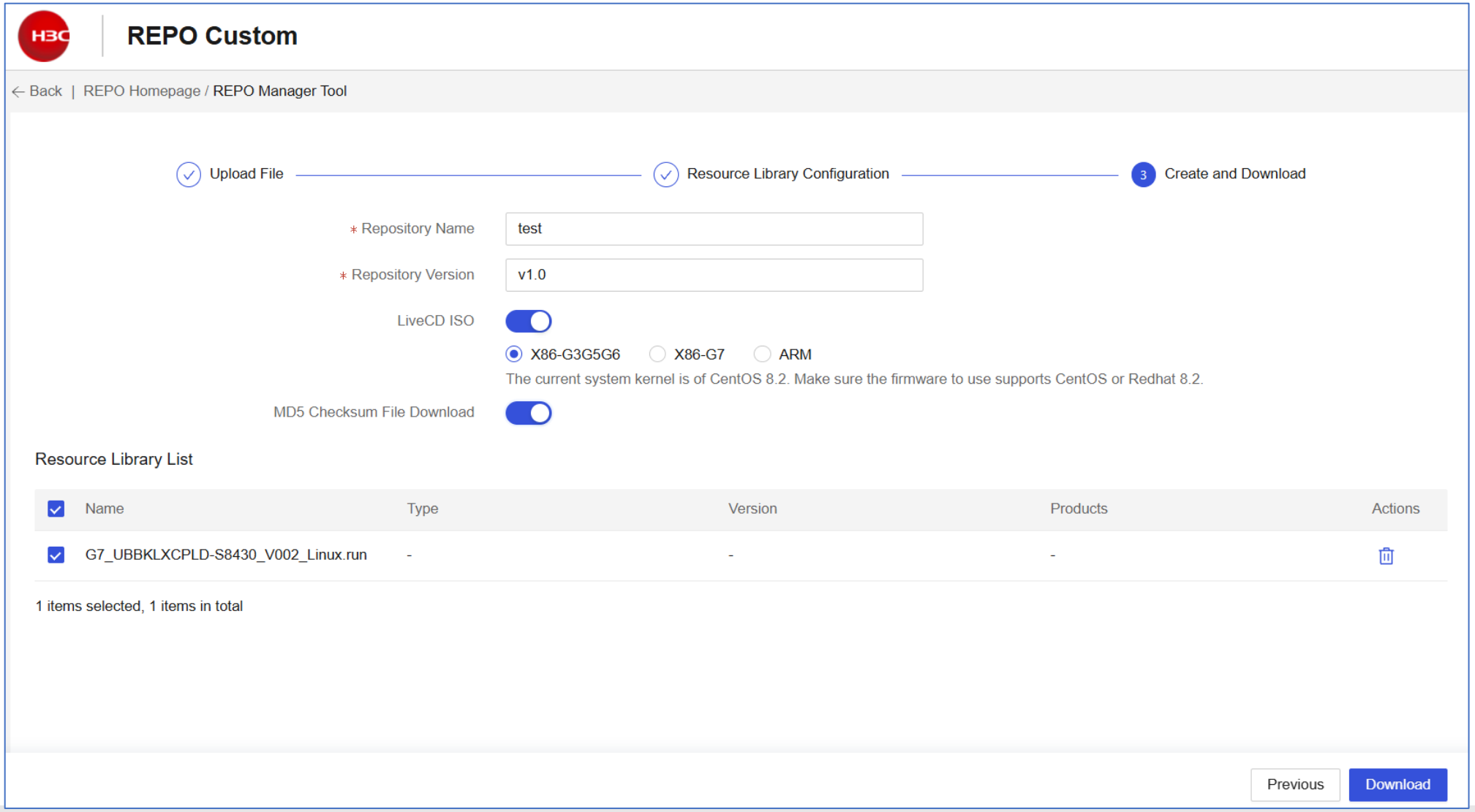
Repositoryの活用: REPO Manager Tool > Upload File



Repositoryの活用: REPO Manager Tool > Resource Library Configuration



Repositoryの活用: REPO Manager Tool > Create and Download





01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

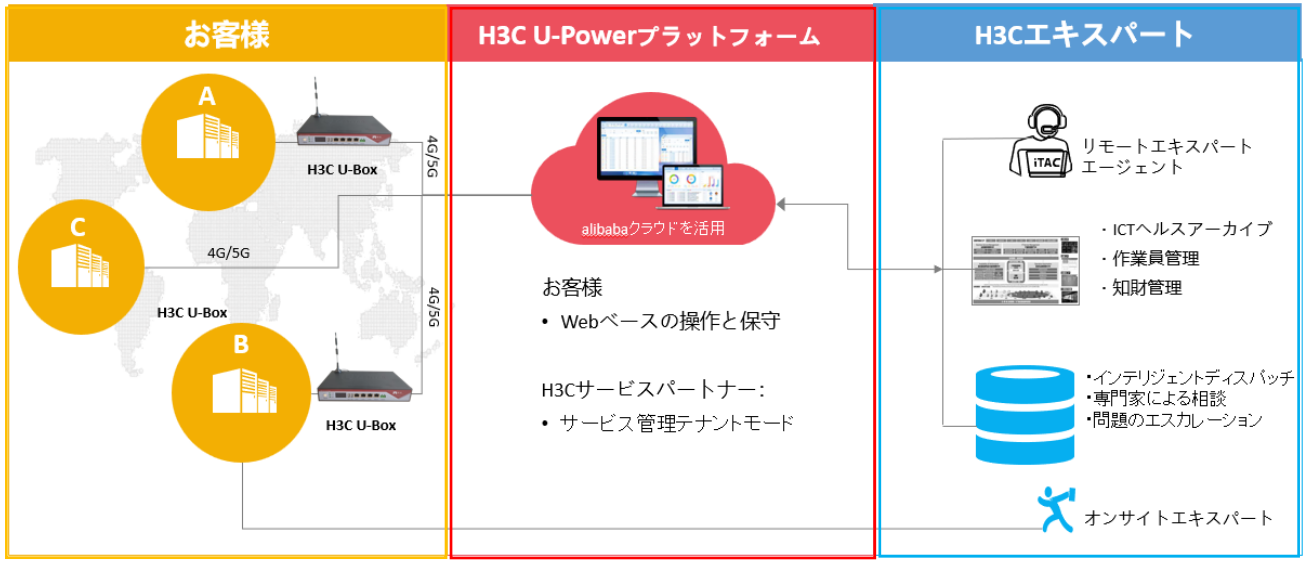
06 Unisystem

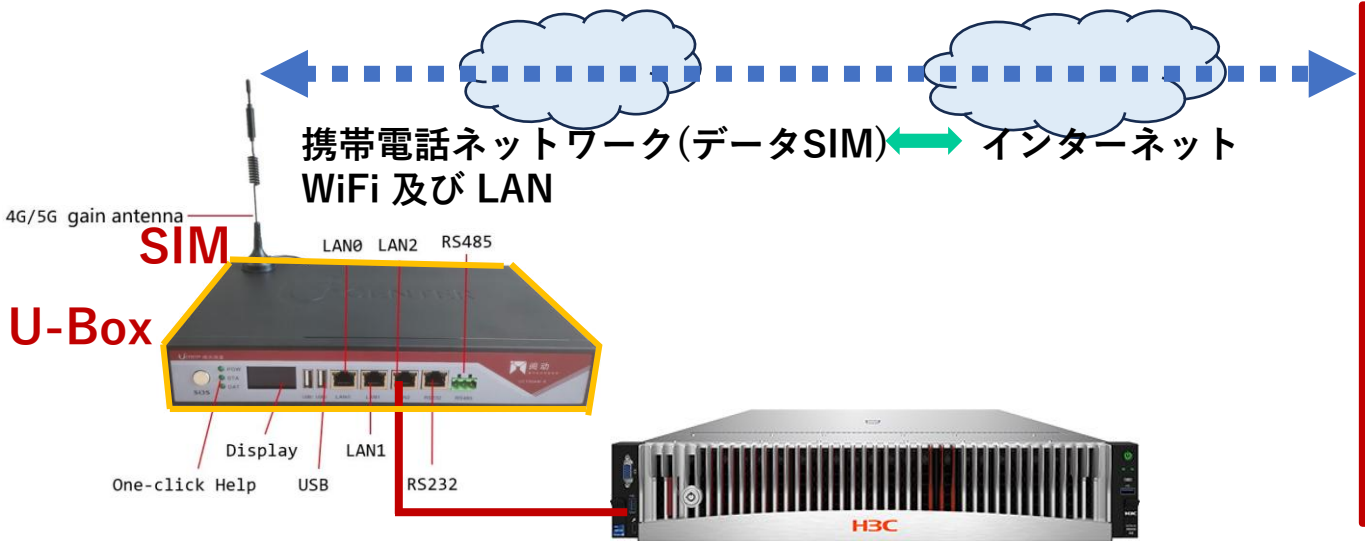
07 REPO

08 U-Center

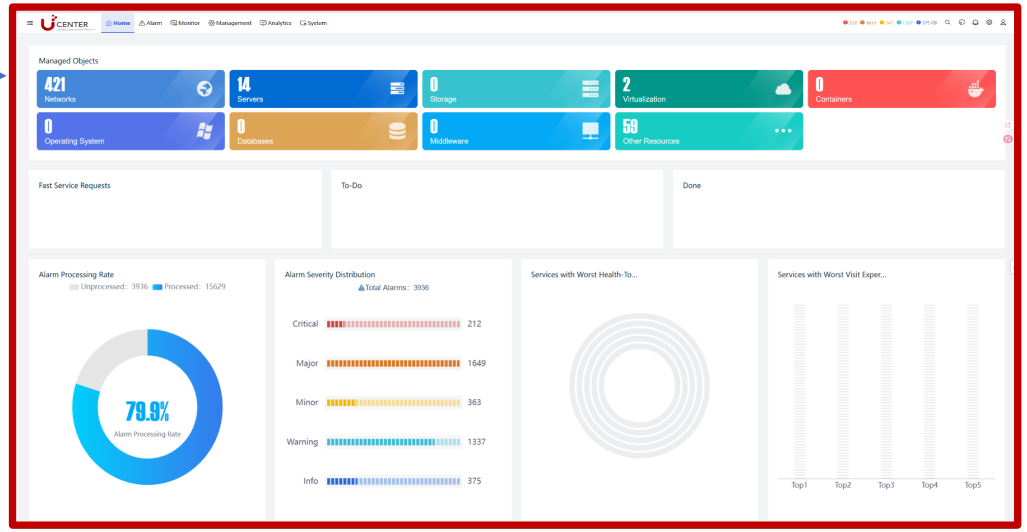
09 ドキュメント

U-Centerはサーバーを含めたネットワーク機器の監視、運用、保守





U-Centerプラットフォーム
テクニカルサポートにて監視、保守



U-Center概要

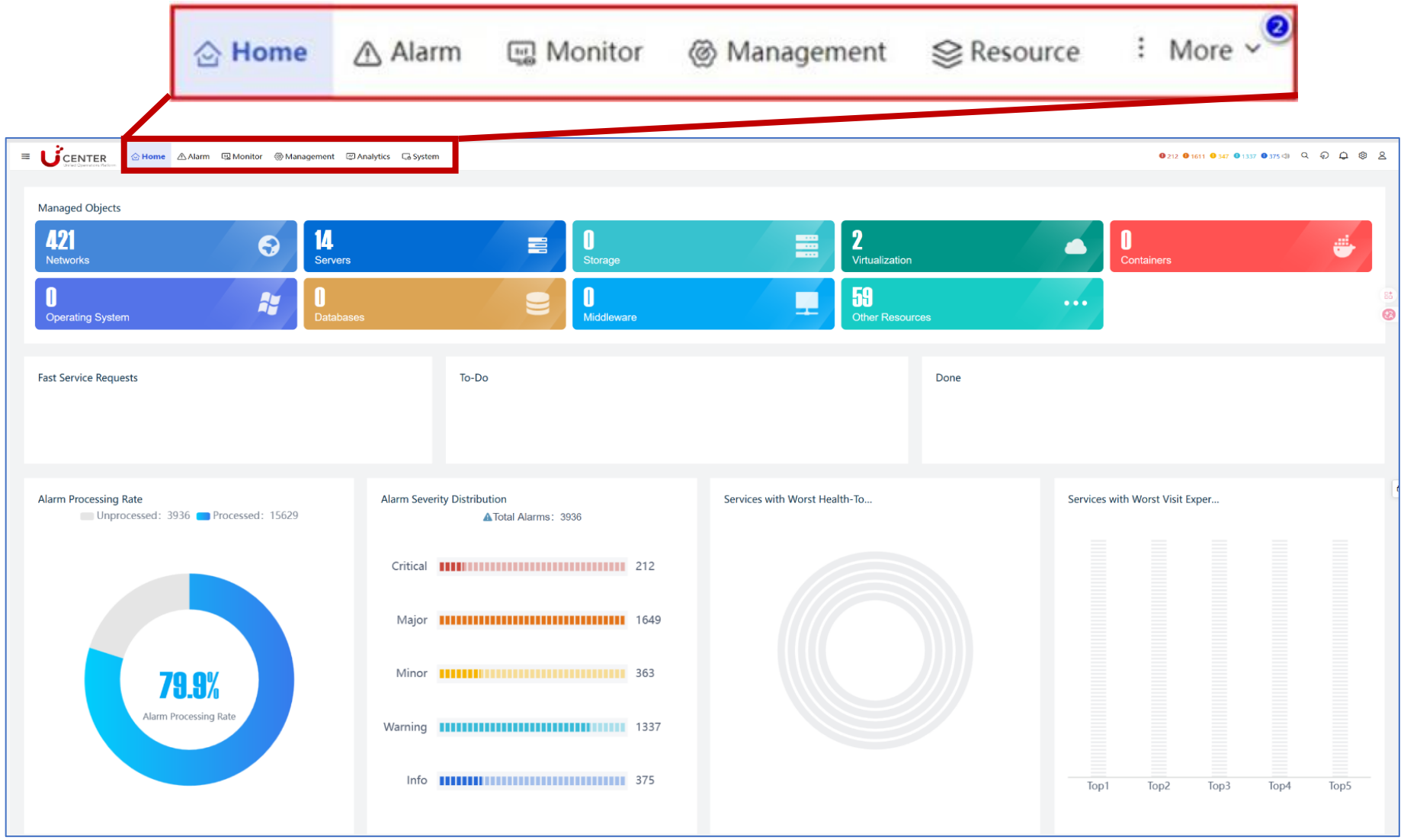
ネットワーク機器だけでなく、サーバー・ITリソース・サービスなどをまとめて監視・管理・運用自動化をする統合運用プラットフォームです。

U-Center 5.0の運用

① リソースを登録・発見する
② 監視設定を作る
③ 監視データを収集する
④ 障害・性能・状態を確認する
⑤ アラームやイベントを処理する
⑥ レポート・分析を行う
⑦ 必要に応じて自動化・運用作業を実行する

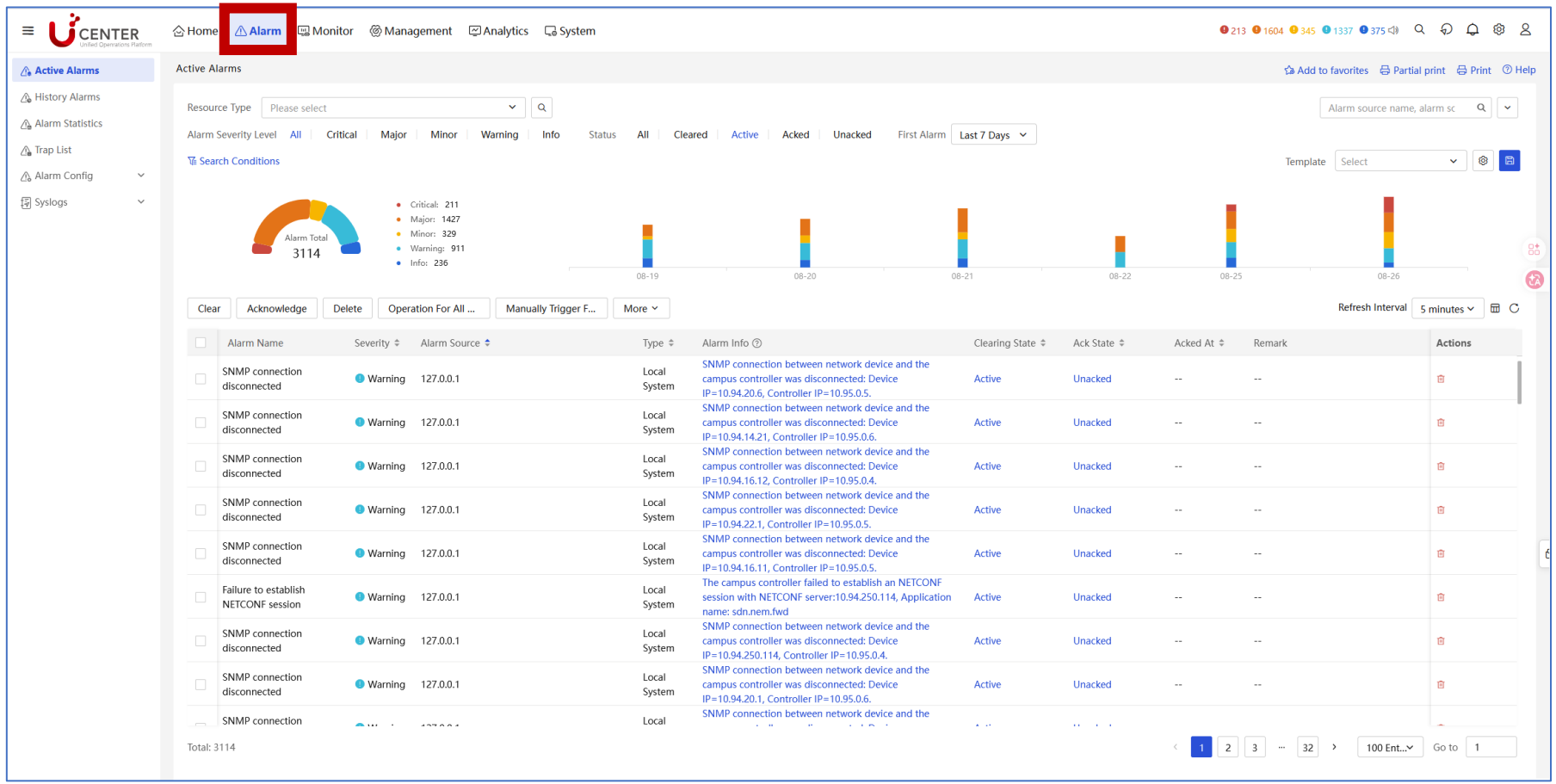
U-Centerは単なる「監視画面」ではなくAIGC（生成AI）を活用したインテリジェント運用が可能です。
また、AOM(自動化・運用作業)ではOne Agentによる自動化作業を行います。
つまり、監視 → 異常検知 → 原因分析 → 対応方法決定 → 自動化による作業までを
一つの基盤にまとめたというのが特徴です。

Home



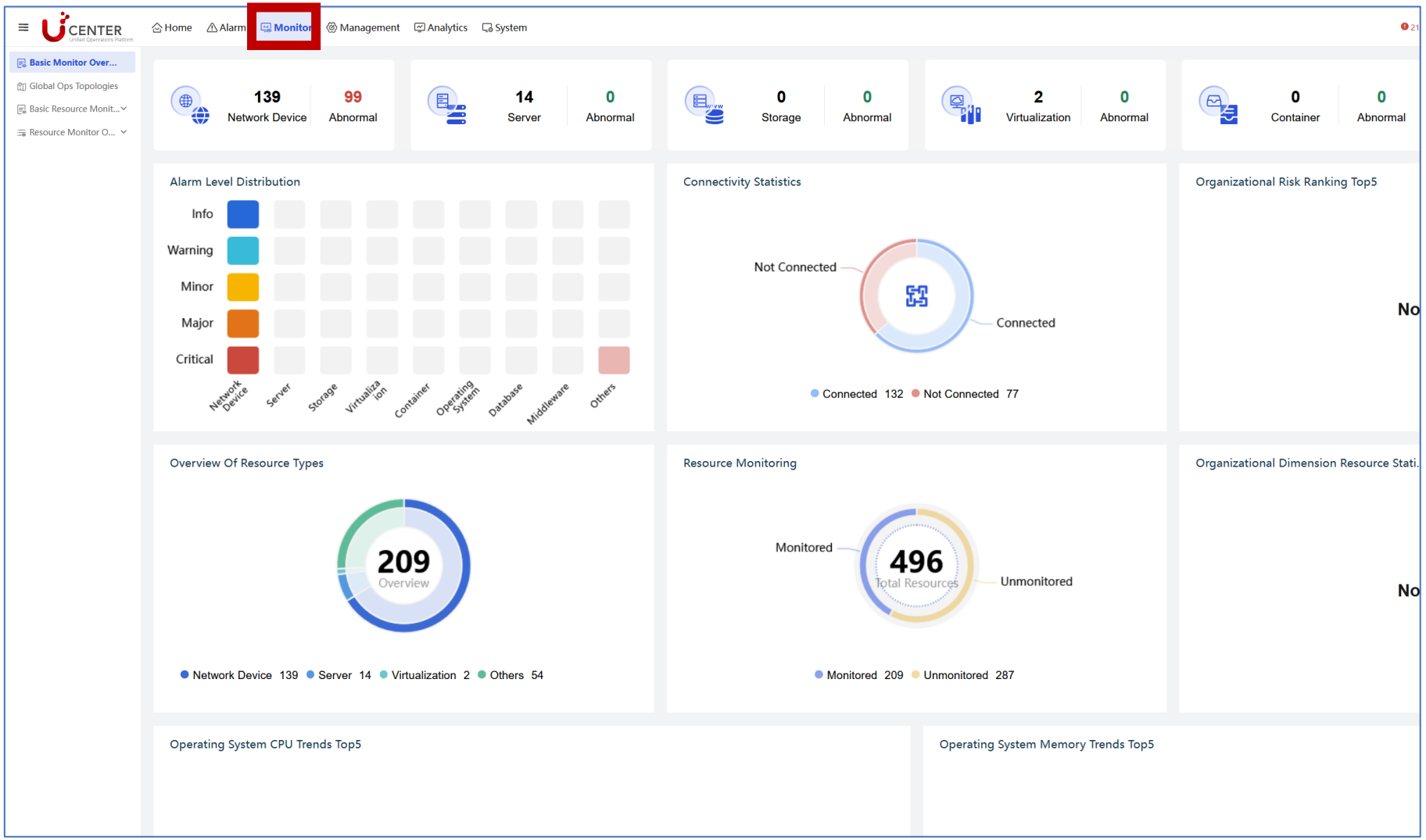
- Home
- Alarm
- Monitor
- Management
- Resource

Alarm



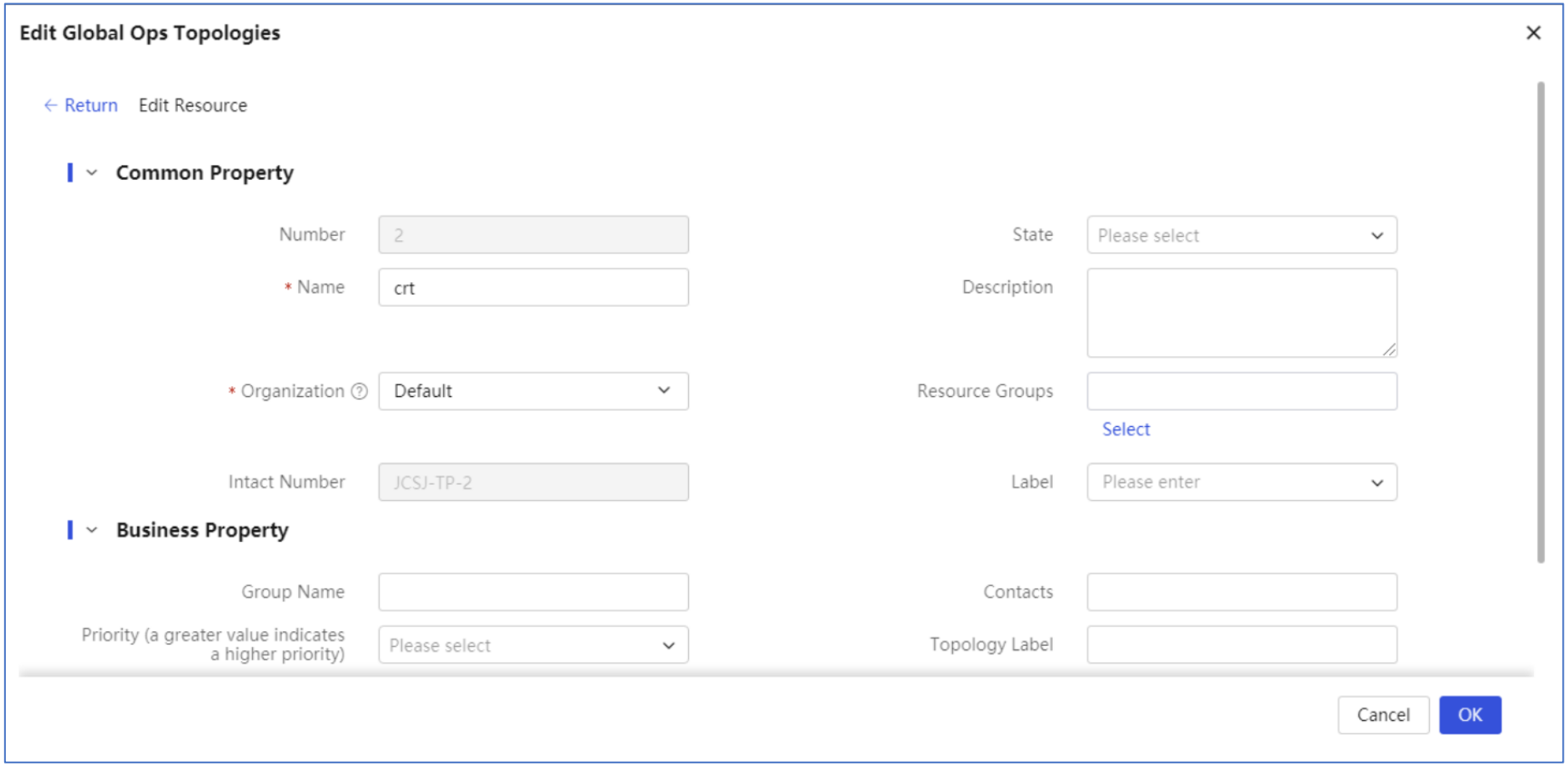
- Active Alarms
- History Alarms
- Alarm Statistics
- Trap List
- Alarm Config
- Syslogs

Monitor > Basic Monitor Overview



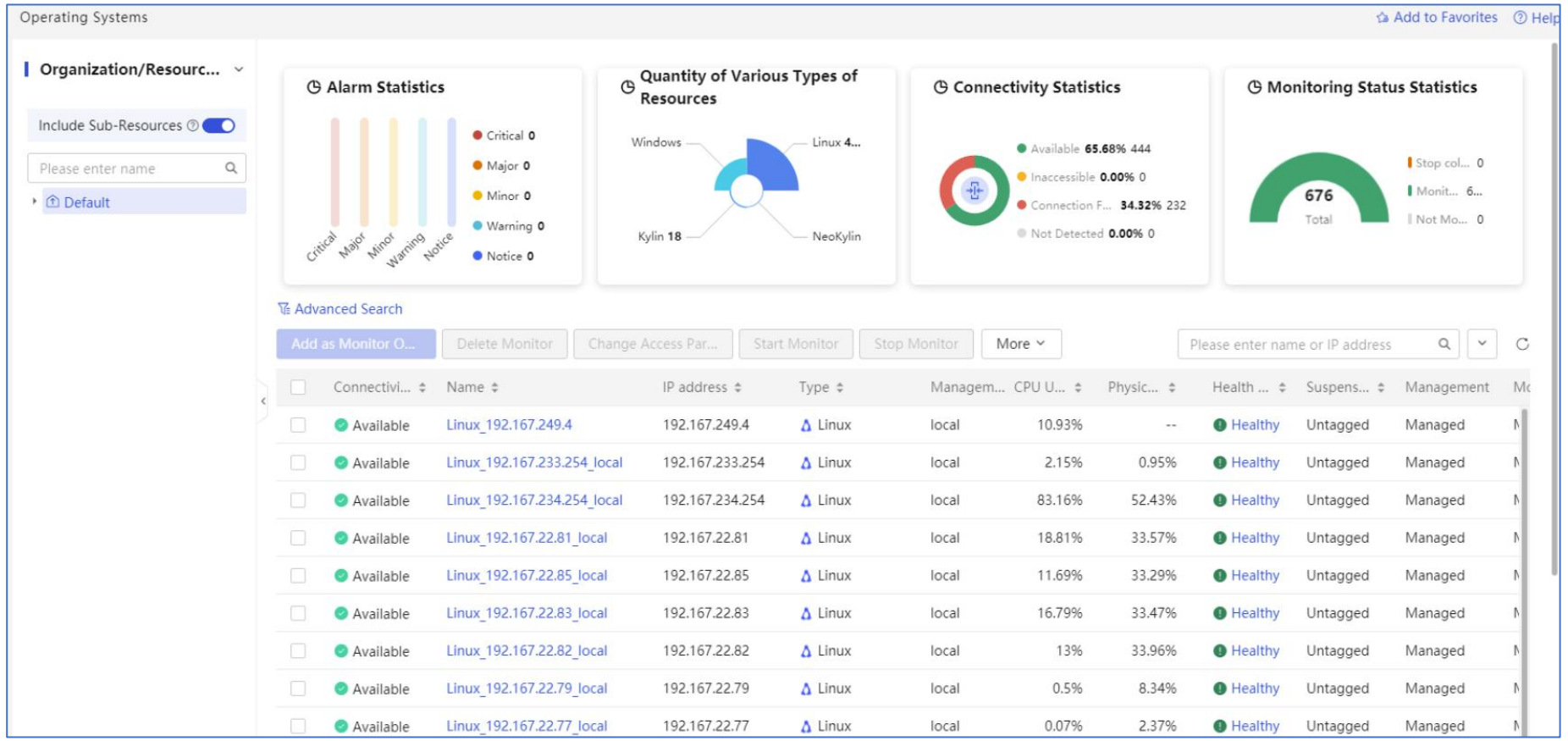
- **Basic Monitor Overview**(包括的なICTリソースの監視および管理機能を提供)
- **Global Ops Topologies**(CIデータやアラームデータなど、CI関連情報を表示および編集できます)
- **Basic Resource Monitor**(さまざまな種類のリソースに関するアラーム、リソース量、接続性、および監視ステータスの統計情報の収集と分析をサポート)
- **Resource Monitor options**(モニターテンプレートの追加)

Monitor > Global ops Topologies



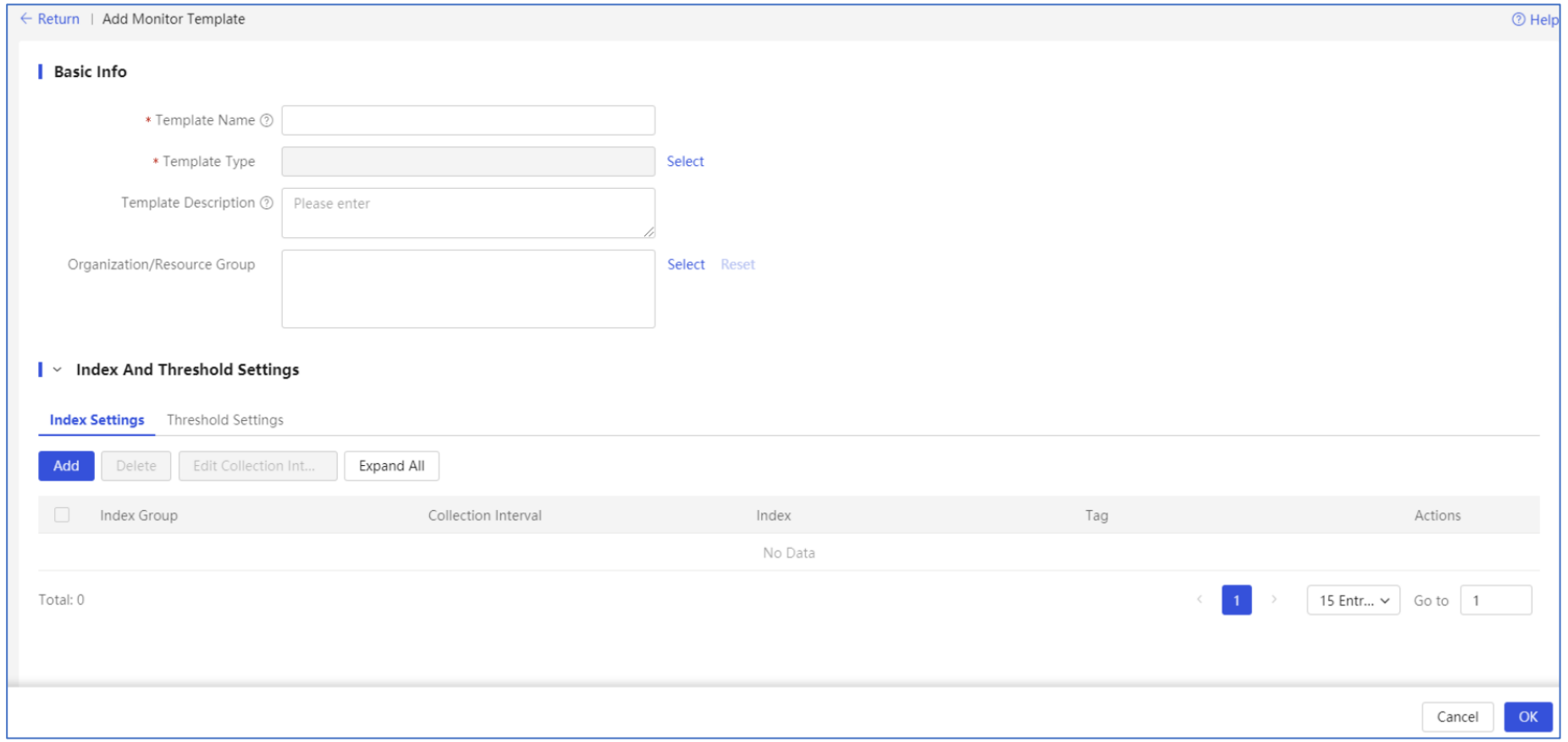
グローバル運用トポロジ機能により、**ネットワーク全体のリソースのトポロジ表示とオーケストレーションが可能**になり、リソースビューの統合管理が実現します。

Monitor > Basic Resource Monitor



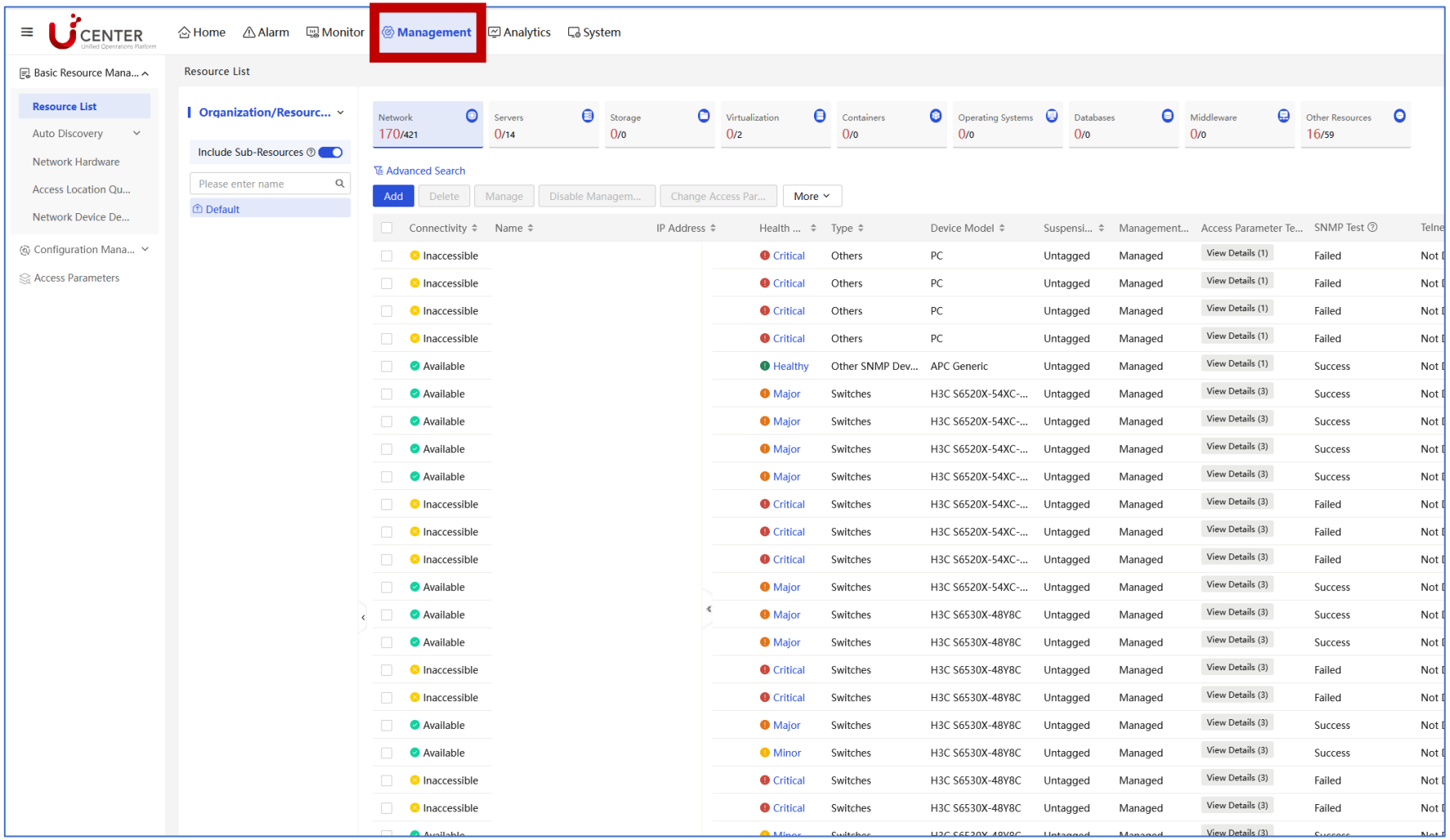
モニターコンポーネントは、さまざまな種類のリソースを監視し、モニターインデックスがアラームしきい値を超えた場合にアラームモジュールを介して通知を送信できます。

Monitor > Resource Monitor Options



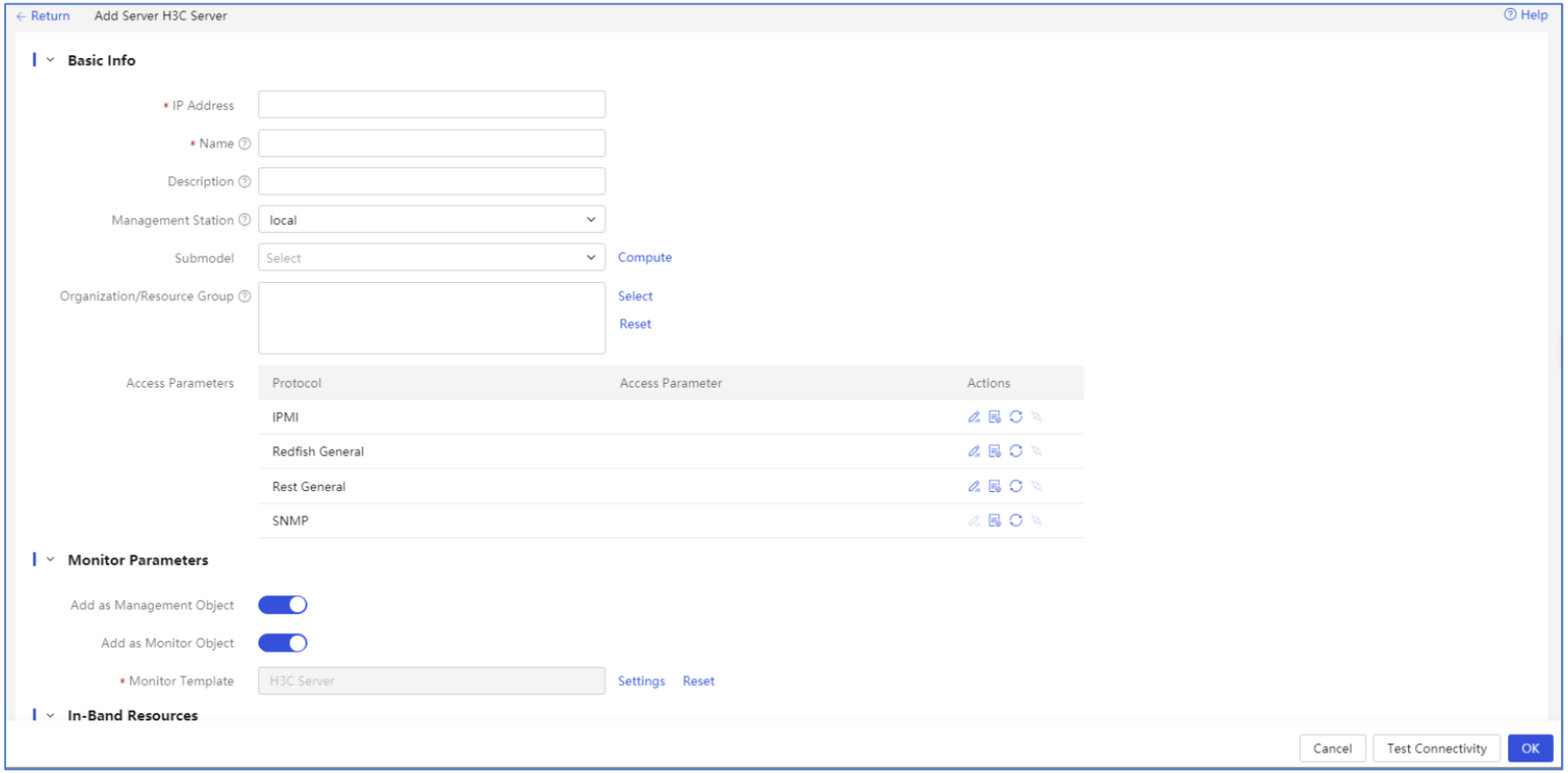
この機能は、テンプレートベースの集中型モニター設定管理を実現します。また、テンプレートベースのモニターインデックス選択、しきい値設定、および収集間隔設定も提供します。モニターテンプレートは、モニターコンポーネントと自動検出コンポーネントで選択できます。

Management



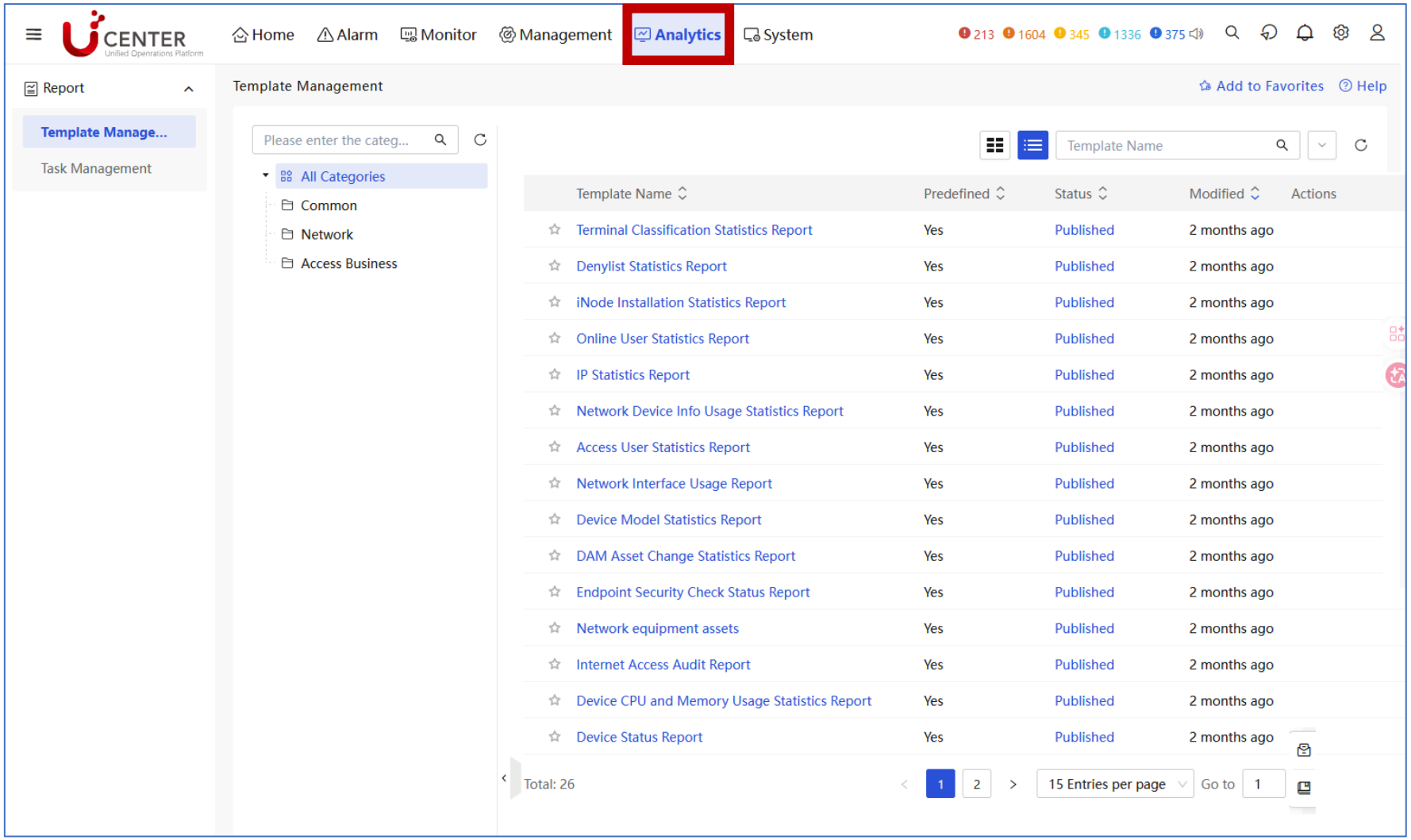
- Basic Resource Management
  - Resource List
  - Auto Discovery
  - Network Hardware
  - Access Location
  - Network Device
- Configuration Management
- Access Parameters

Management > Basic Resource Management



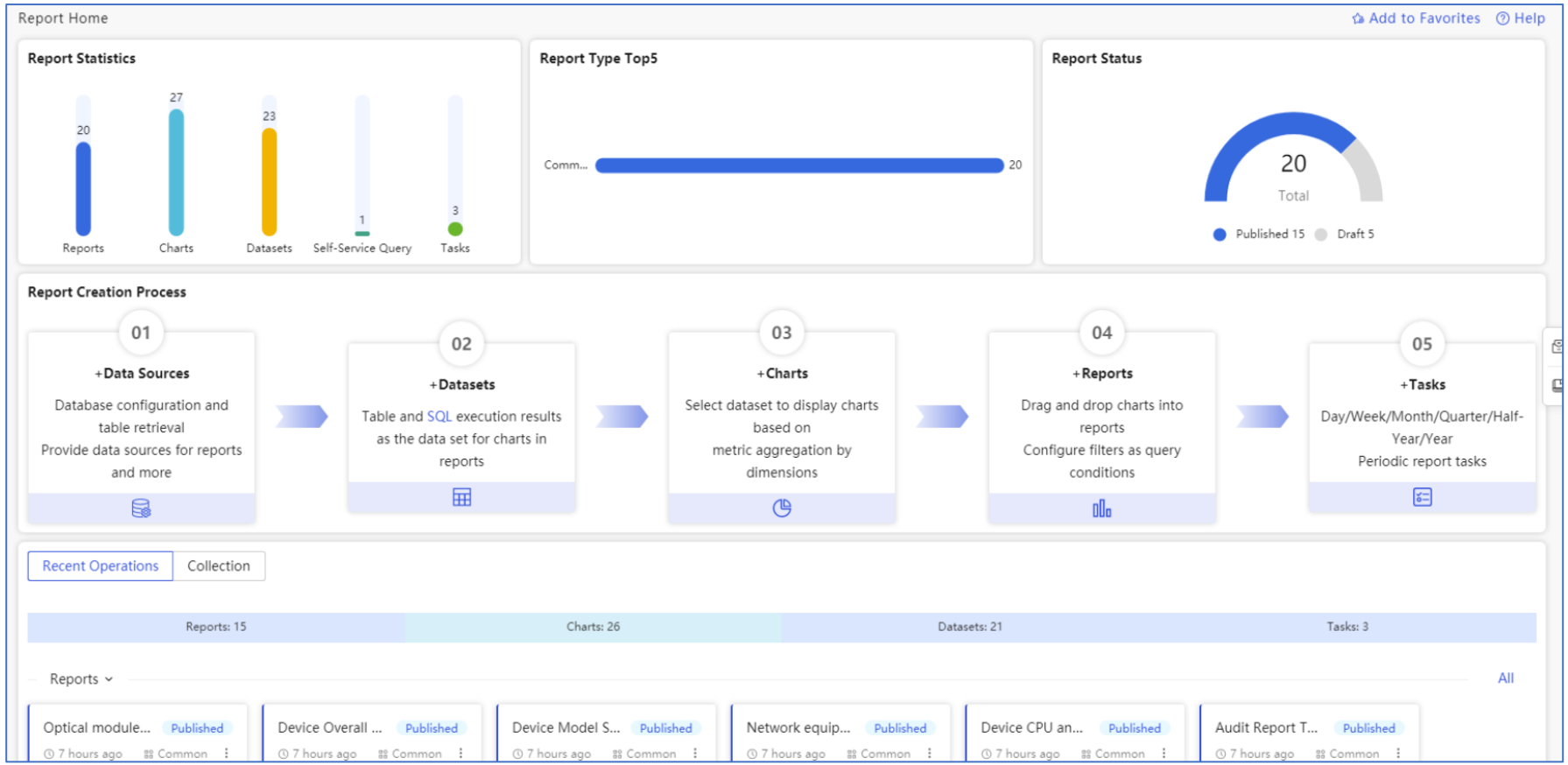
リソースを管理する際は、以下の制限事項とガイドラインに従ってください。
・監視および管理が正しく機能するためには、ユーザーは監視テンプレートおよびアクセスパラメータテンプレートに対する権限を持っている必要があります。
・追加、削除、編集、即時収集、収集の有効化、収集の無効化、インポート、およびテンプレートの変更操作を実行するには、ユーザーは関連する権限を持っている必要があります。

Analytics



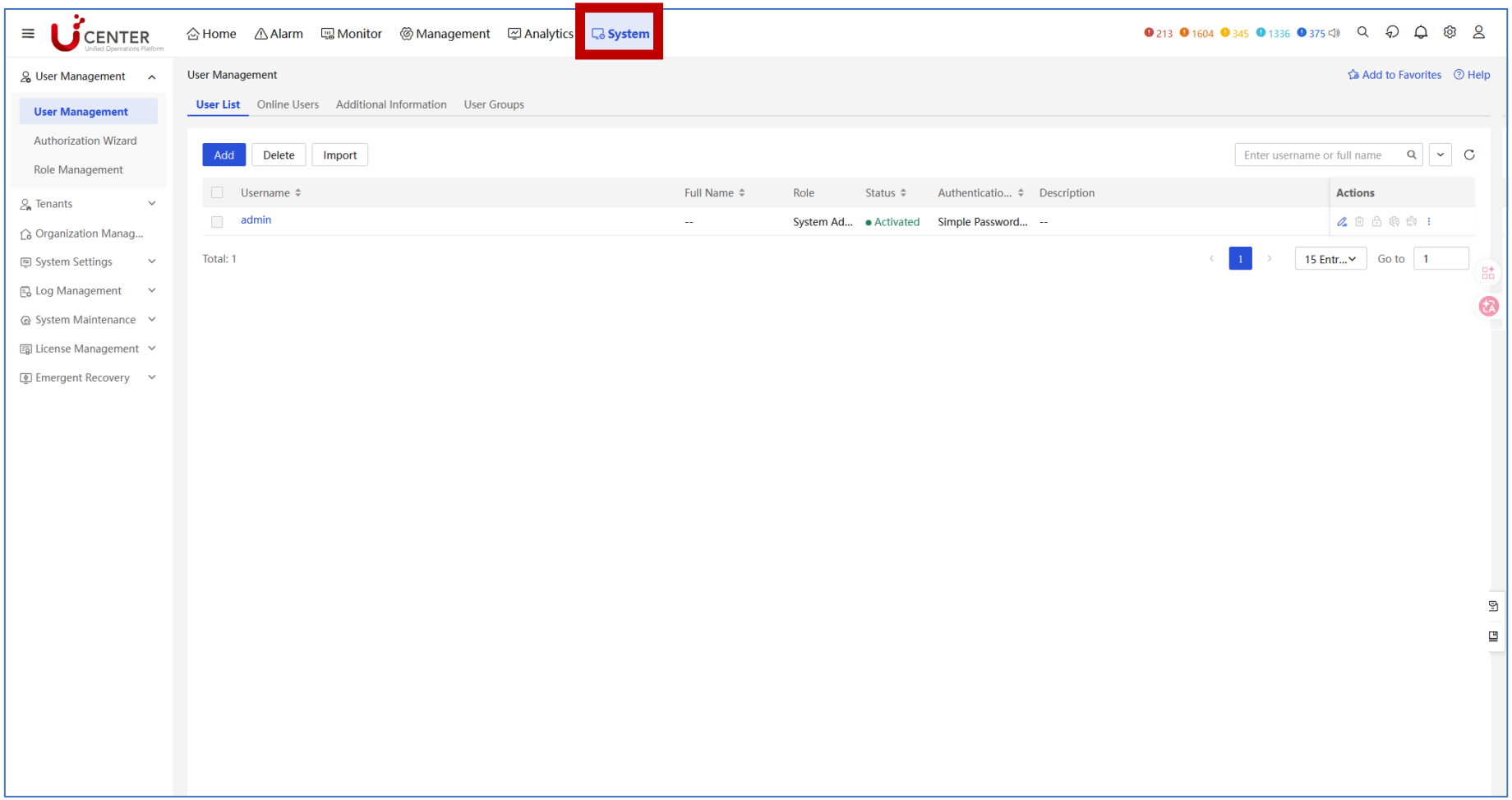
- **Report**
  - **Template Management**
  - **Task Management**

Analytics > Report



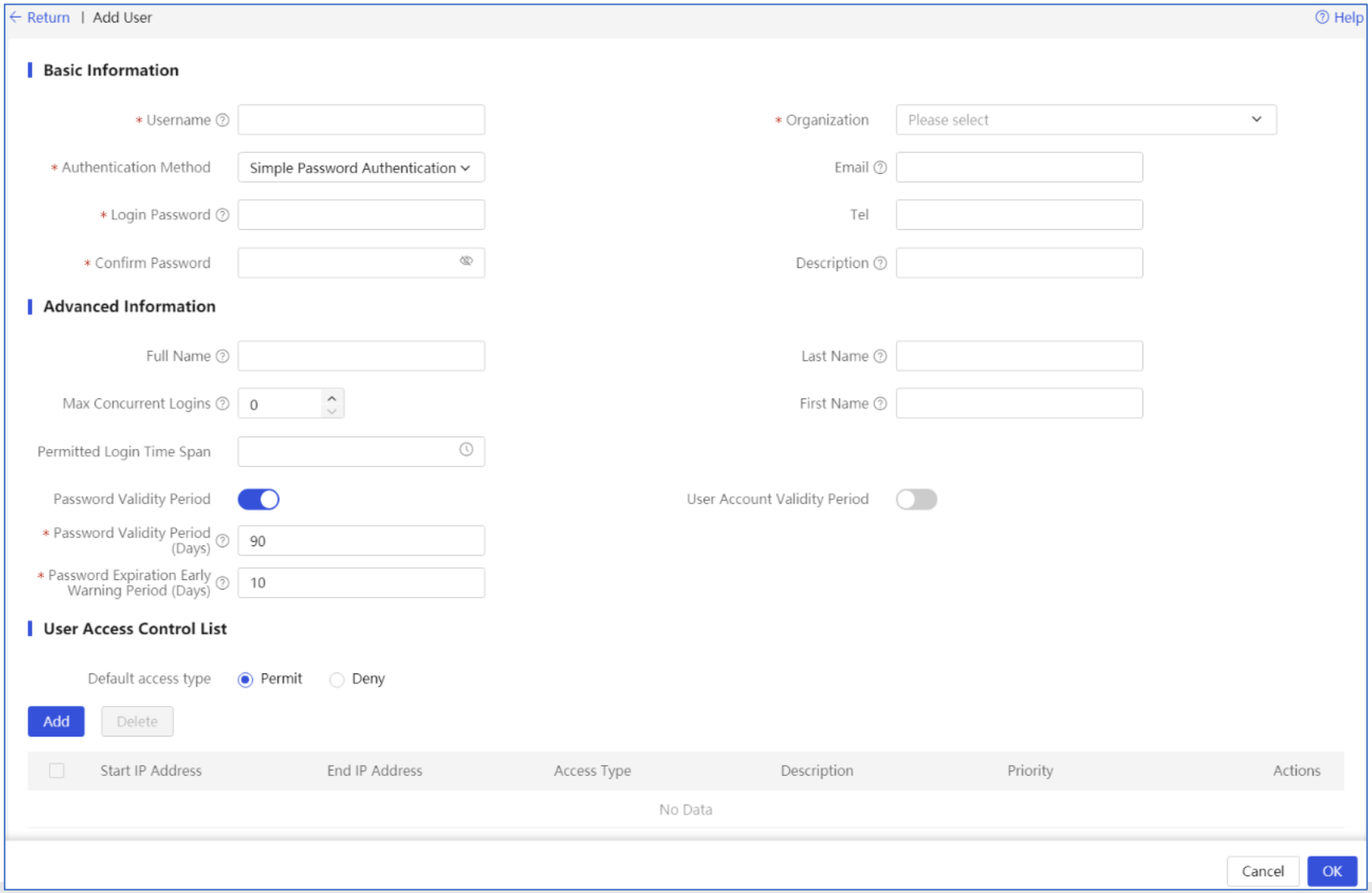
レポートホームページには、統計情報、上位5つのレポートタイプ、レポートステータス、レポート作成ワークフローなど、さまざまな種類のレポートに関するデータの概要が表示されます。

System



- User Management
  - User Management
  - Authorization Wizard
  - Role Management
- Tenants
- Organization Management
- System Settings
- Log Management
- System maintenance
- Ucenter Management
- Emergency Recovery

System > Add User



中規模または大規模のネットワークを管理するには、セキュリティ保護された運用に必要な権限を持つ複数のユーザーを追加できます

U-Center導入手順

1. U-Centerの構成・ライセンスを理解
2. ログインしてGUIを確認
3. adminパスワード変更
4. ユーザー/ロール作成
5. ネットワーク機器をResourceとして登録
6. SNMP等のAccess Parameterを設定
7. Monitor Templateを確認
8. Monitorを開始
9. CPU・Memory・Interfaceなどの監視を確認
10. Alarmを発生させて動作確認
11. Topology/Resource/Alarmを使った障害調査
12. Report/Analysisを確認
13. 必要に応じてNTA(ネットワークトラフィック分析)、CMDB(構成情報管理)、ITSM(ITサービス管理)、AOM(自動化・運用作業)などを追加



01 サーバー　ハードウェア概要

02 サーバー管理プラットフォーム概要

03 保証及びテクニカルサポート

04 HDM

05 iFIST

06 Unisystem

07 REPO

08 U-Center

09 ドキュメント

日本語マニュアル、FAQなど

https://knowledge-jp.h3c.com/TechDoc/index

製品別検索

ルーター	スイッチ	WLAN	セキュリティ (ファイアウォール)
クラウドコンピューティング UIS(仮想化)	ネットワーク管理 (snmpベースiMC)	AD-NET ソリューション	サーバ
CloudNet (Cloud管理)	Cloud Lab (シュミレーター)	テクニカルサポート	Others

英文マニュアルのダウンロードサイト

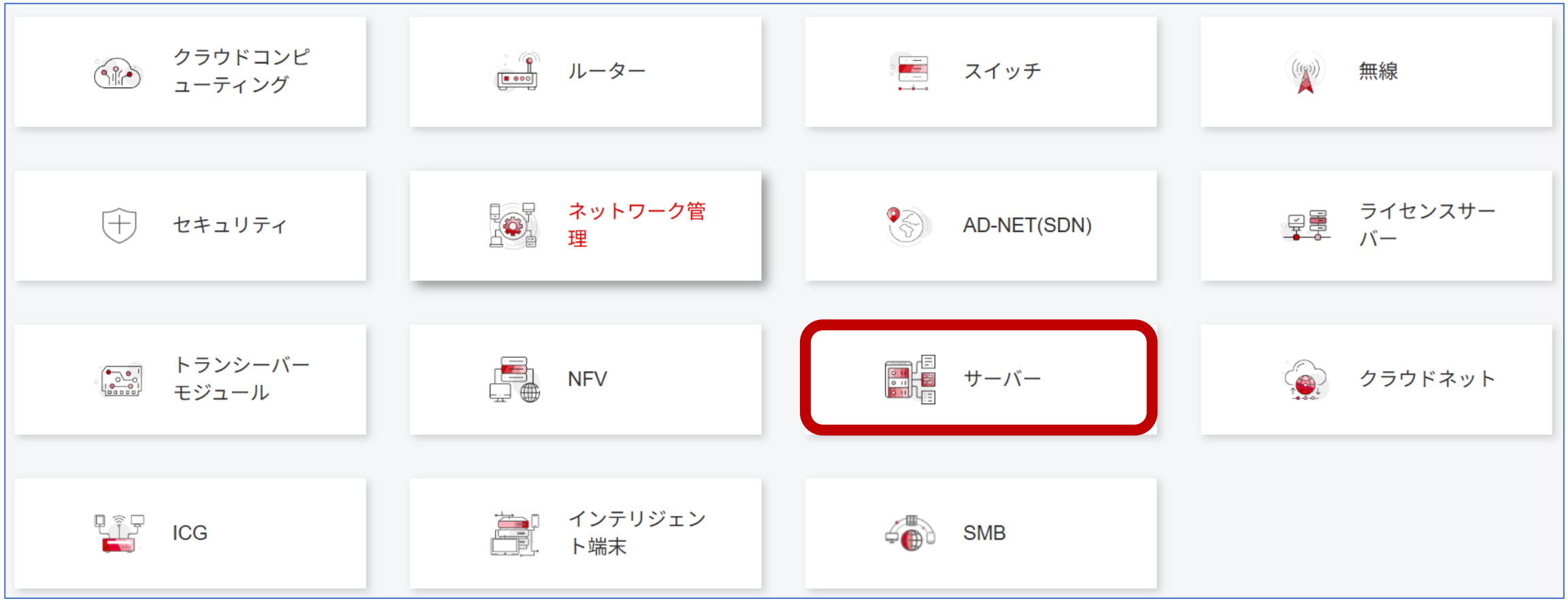
https://www.h3c.com/jp/

①　→　②

http://www.h3c.com/en/Support/Resource_Center/Technical_Documents/



製品カテゴリーの選択


クラウドコンピューティング
ルーター
スイッチ
無線
セキュリティ
ネットワーク管理
AD-NET(SDN)
ライセンスサーバー
トランシーバーモジュール
NFV
サーバー
クラウドネット
ICG
インテリジェント端末
SMB

個別製品の選択

Server

AI Appliance

→ LinSeerCube Appliance

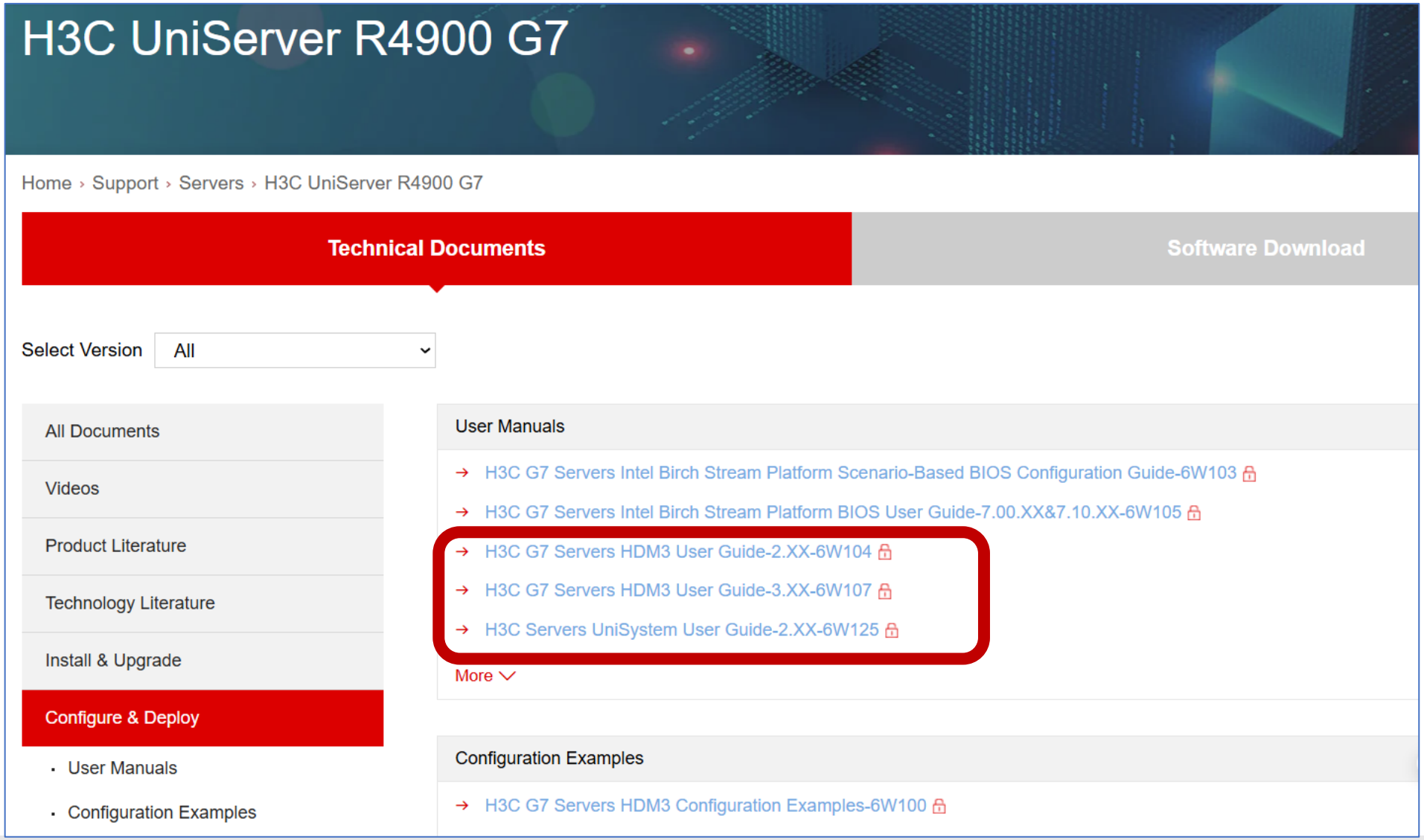
Blade Server

→ H3C UniServer B16000

Rack Server

→ H3C UniServer R6900 G7
→ H3C UniServer R4900 G7
→ H3C UniServer R4500 G7
→ H3C UniServer R3950 G7
→ H3C UniServer R3750 G7
→ H3C UniServer R4500 G6
→ H3C UniServer R4900 G6
→ H3C UniServer R4950 G6
→ H3C UniServer R4700 G5
→ H3C UniServer R6900 G5
→ H3C UniServer R6700 G6
→ H3C UniServer R4950 G7
→ H3C UniServer R4700 G7
→ H3C UniServer R4300 G7
→ H3C UniServer R3900 G7
→ H3C UniServer R3350 G7
→ H3C UniServer R4900 G6 Ultra
→ H3C UniServer R4700 G6
→ H3C UniServer R4300 G6
→ H3C UniServer R4900 G5
→ H3C UniServer R6900 G6
→ H3C UniServer R3950 G6

設置、コマンド、コンフィグ、保守マニュアル





The Leader in Digital Solutions

www.h3c.com