Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0

解説書

CA92344-5874-03
2025年6月

まえがき

本書の目的

本書では、サーバー、ストレージ、スイッチなどのICT機器やファシリティー機器（PDUなど）を統合的に管理、運用する運用管理ソフトウェアである以下のソフトウェア製品の機能全般、導入方法および使用方法を説明します。

- Infrastructure Manager（以降、「ISM」と表記）
- Infrastructure Manager for PRIMEFLEX（以降、「ISM for PRIMEFLEX」と表記）

製品マニュアル

マニュアル名称	説明
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 入門書	本製品を初めて使用する利用者向けのマニュアルです。 本製品の製品体系／ライセンス、利用手順の概要について説明しています。 マニュアル内では、『入門書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 解説書	本製品の機能、導入手順、操作方法を説明したマニュアルです。 本製品の全機能、全操作を把握できます。 マニュアル内では、『解説書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 操作手順書	本製品の導入手順、利用シーンに応じた操作手順を説明したマニュアルです。 マニュアル内では、『操作手順書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 REST API リファレンスマニュアル	お客様が作成したアプリケーションと本製品を連携する際に必要なAPIの使用方法、サンプル、パラメーター情報などを説明したマニュアルです。 マニュアル内では、『REST API リファレンスマニュアル』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 メッセージ集	ISMおよびISM for PRIMEFLEX使用時に出力される各種メッセージの説明と、そのメッセージに対しての対処方法について説明しています。 マニュアル内では、『ISM メッセージ集』と表記します。
Infrastructure Manager for PRIMEFLEX V3.1.0 メッセージ集	ISM for PRIMEFLEX使用時に出力される各種メッセージの説明と、そのメッセージに対しての対処方法について説明しています。 マニュアル内では、『ISM for PRIMEFLEX メッセージ集』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 プロファイル管理機能 プロファイル設定項目集	管理対象機器のプロファイル作成の設定を行う際に選択する項目の詳細情報について説明しています。 マニュアル内では、『プロファイル管理機能 プロファイル設定項目集』と表記します。
Infrastructure Manager for PRIMEFLEX V3.1.0 クラスタ作成／拡張機能 設定値一覧	ISM for PRIMEFLEXで利用できるクラスタ作成機能、クラスタ拡張機能の自動設定内容や各機能で使用されるクラスタ定義パラメーターについて説明しています。 マニュアル内では、『ISM for PRIMEFLEX 設定値一覧』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 用語集	本製品を使用するうえで理解が必要な用語の定義を説明した用語集です。 マニュアル内では、『用語集』と表記します。

マニュアル名称	説明
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.1.0 Plug-in and Management Pack セットアップガイド	Infrastructure Manager Plug-inの以下の機能について、インストールから利用方法までと注意事項や参考情報を説明します。 ・ Infrastructure Manager Plug-in for Microsoft System Center Operations Manager ・ Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager ・ Infrastructure Manager Plug-in for VMware vCenter Server Appliance ・ Infrastructure Manager Plug-in for Microsoft Windows Admin Center マニュアル内では、『ISM Plug-in/MP セットアップガイド』と表記します。

上記マニュアルと併せて、ISMに関する最新情報については、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/

管理対象の各ハードウェアについては、各ハードウェアのマニュアルを参照してください。

PRIMERGYの場合は、「ServerView Suite ServerBooks」、またはPRIMERGYマニュアルページを参照してください。

https://www.fujitsu.com/jp/products/computing/servers/primergy/manual/

本書の読者

このマニュアルは、ハードウェアとソフトウェアについて十分な知識を持っているシステム管理者、ネットワーク管理者、ファシリティー管理者およびサービス専門家を対象とします。

本書の表記について

表記

キーボード

印字されない文字のキーストロークは、[Enter]や[F1]などのキーアイコンで表示されます。例えば、[Enter]はEnterというラベルの付いたキーを押すことを意味し、[Ctrl]+[B]は、CtrlまたはControlというラベルの付いたキーを押しながら[B]キーを押すことを意味します。

記号

特に注意すべき事項の前には、以下の記号が付いています。

ポイント

ポイントとなる内容について説明します。

注意

注意する項目について説明します。

変数:＜xxx＞

お使いの環境に応じた数値／文字列に置き換える必要のある変数を表します。

例:＜IPアドレス＞

略称

本書では、以下の例のとおりOSを略称で記載することがあります。

正式名称	略称	
Microsoft® Windows Server® 2022 Datacenter	Windows Server 2022 Datacenter	Windows Server 2022 またはWindows
Microsoft® Windows Server® 2022 Standard	Windows Server 2022 Standard	
Microsoft® Windows Server® 2022 Essentials	Windows Server 2022 Essentials	
Red Hat Enterprise Linux 9.3 (for Intel64)	RHEL 9.3	Red Hat Enterprise Linux またはLinux
SUSE Linux Enterprise Server 15 SP5 (for AMD64 & Intel64)	SUSE 15 SP5 (AMD64) SUSE 15 SP5(Intel64) または SLES 15 SP5(AMD64) SLES 15 SP5(Intel64)	SUSE Linux Enterprise Server またはLinux
SUSE Linux Enterprise Server 15 (for AMD64 & Intel64)	SUSE 15(AMD64) SUSE 15(Intel64) または SLES 15(AMD64) SLES 15(Intel64)	
VMware ESXi™ 8.0	VMware ESXi 8.0	VMware ESXi
VMware Virtual SAN	vSAN	
Microsoft Storage Spaces Direct	S2D	
AlmaLinux OS Foundation	AlmaLinux	

本書では、VMware by Broadcom社をVMwareと表記します。

用語

本書で使用している主な略語および用語については、『用語集』を参照してください。

PDF表示アプリケーション（Adobe Readerなど）での操作について

PDF表示アプリケーションで以下の操作を行った場合、表示アプリケーションの仕様により、不具合（余分な半角空白や改行の追加、半角空白や行末のハイフンの欠落、改行だけの行の欠落など）が発生することがあります。

- テキストファイルへの保存
- テキストのコピー&ペースト

高度な安全性が要求される用途への使用について

本製品は、一般事務用、パーソナル用、家庭用、通常の産業等の一般的用途を想定して開発・設計・製造されているものであり、原子力施設における核反応制御、航空機自動飛行制御、航空交通管制、大量輸送システムにおける運行制御、生命維持のための医療用機器、兵器システムにおけるミサイル発射制御など、極めて高度な安全性が要求され、仮に当該安全性が確保されない場合、直接生命・身体に対する重大な危険性を伴う用途（以下「ハイセイフティ用途」という）に使用されるよう開発・設計・製造されたものではありません。お客様は本製品を必要な安全性を確保する措置を施すことなくハイセイフティ用途に使用しないでください。また、お客様がハイセイフティ用途に本製品を使用したことにより発生する、お客様または第三者からのいかなる請求または損害賠償に対してもエフサステクノロジーズ株式会社およびその関連会社は一切責任を負いかねます。

安全にお使いいただくために

本書には、本製品を安全に正しくお使いいただくための重要な情報が記載されています。本製品をお使いになる前に、本書を熟読してください。また、本製品を安全にお使いいただくためには、本製品のご使用にあたり各製品（ハードウェア、ソフトウェア）をご理解いただく必要があります。必ず各製品の注意事項に従ったうえで本製品をご使用ください。本書は本製品の使用中にいつでもご覧になれるよう大切に保管してください。

改造等

お客様は、本ソフトウェアを改造したり、あるいは、逆コンパイル、逆アセンブルをともなうリバースエンジニアリングを行うことはできません。

免責事項

本製品の運用を理由とする損失、免失利益等の請求につきましては、いかなる責任も負いかねます。本書の内容に関しては将来予告なしに変更することがあります。

登録商標について

Microsoft、Windows、Windows Vista、Windows Server、Hyper-V、Active Directory、またはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標あるいは商標です。

Red Hat およびRed Hat をベースとしたすべての商標とロゴは、米国およびその他の国におけるRed Hat, Inc.の商標または登録商標です。

SUSEおよびSUSEロゴは、米国およびその他の国におけるSUSE LLCの商標または登録商標です。

VMwareおよびVMwareの製品名は、Broadcom Inc.の米国および各国での商標または登録商標です。

Intel、インテル、Xeonは、米国およびその他の国におけるIntel Corporationまたはその子会社の商標または登録商標です。

Java は、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。

Zabbixはラトビア共和国にあるZabbix LLCの商標です。

PostgreSQLはPostgreSQLの米国およびその他の国における商標です。

Apacheは、Apache Software Foundationの商標または登録商標です。

Ciscoは、米国およびその他の国における Cisco Systems, Inc. およびその関連会社の商標です。

Elasticsearchは、Elasticsearch BVの米国およびその他の国における登録商標または商標です。

Xenは、XenSource, Inc.の商標です。

Trend MicroおよびDeep Securityは、トレンドマイクロ株式会社の商標または登録商標です。

Nutanixは、米国およびその他の国におけるNutanix, Inc.の商標です。

その他の会社名と各製品名は、各社の商標、または登録商標です。

その他の各製品は、各社の著作物です。

著作権表示

改版履歴

版数	作成年月	変更内容	章・節・項	変更箇所
01	2025年3月	新規作成	―	―
02	2025年5月	AlmaLinuxの記載を追加	まえがき	表「略称」
	ISM 3.1.0.010 パッチ適用による変更	AlmaLinux 8.10/9.4/9.5に関する記載/記述を追加	2.14.6 仮想化管理ソフトウェア管理機能	-
			B.11 監視対象への設定手順（仮想化管理ソフトウェア：KVM）	「ポイント」
			B.11.3 KVM AlmaLinuxへの設定手順（ドメインユーザー使用時）	新規追加

版数	作成年月	変更内容	章・節・項	変更箇所
	2025年5月 主な構成変更や記事改善	ISM-VAを動作させるためにハイパーバイザーからISM-VAに割り当てる要件の説明を修正	1.3.1 ISM-VAを動作させるハイパーバイザーの要件	-
		仮想IOのプロファイル適用に関する記述を追加	2.4.5 仮想IO設定	「注意」
		Brocade FCスイッチのログ収集に関する記載を修正	2.5.1 収集可能なログの種類	表「ハードウェアログ」
			A.3.2 ログ管理機能利用時のディスク消費量の目安	表「1ノードあたりの1世代の保管ログの容量目安」
		ファームウェアデータのインポート方法に関する記述を追加	2.6.3.1 アップデート方法	アップデート方法と使用条件の表
03	2025年6月 主な構成変更や記事改善	ハイパーバイザーに関する記載を追加,削除	1.3.1 ISM-VAを動作させるハイパーバイザーの要件	ハイパーバイザー
		RedHat Enterprise Linux 10に関する記載/記述を追加	3.3.3 KVMへのインストール	手順
			3.7.1 ISM-VA全体に対する仮想ディスク割り当て	手順

目　次

第1章 Infrastructure Managerの概要

この章では、Infrastructure ManagerおよびInfrastructure Manager for PRIMEFLEXの機能概要とシステム要件を説明します。

1.1 主な機能概要

ISMの機能の概要を説明します。

1.1.1 ノード管理機能

ノード管理機能は、以下を行う機能です。

- 機器情報の管理

  モデル名／シリアル番号／IPアドレスなどの機器情報を管理します。

- 機器の登録

  ISMが管理対象として扱うノードを登録します。

ネットワークに接続されたノードを検出／登録でき、ノードの登録作業を効率的に行えます。また、データセンターのフロア上のラックの配置、ラック内のノードの配置、ノードの構成および状態を管理できます。フロアやラックのノードを可視化する機能（フロアビュー、ラックビュー）を使用して、ノードの管理業務を直観的に行えます。

ノード管理機能の詳細については、「2.2 ノード管理機能」を参照してください。

1.1.2 モニタリング機能

モニタリング機能は、以下のイベントを監視する機能です。

- ノードから発信されるSNMPトラップ
- ノードが持つ正常／異常を示すステータスの変化
- ノードから取得した吸気温度、CPU使用率、消費電力がISMに設定した正常範囲内であるかどうか

これらのイベントに対して利用者が作成したスクリプトの実行やメール送信などのアクションを設定でき、利用者の運用方法に合わせてノードを監視できます。

モニタリング機能の詳細については、「2.3 モニタリング機能」を参照してください。

アノマリ検知機能

アノマリ検知機能は、管理対象ノードを構成するハードウェア／ソフトウェアの普段とは異なる挙動を検知し、解決方法を示すことで運用を支援する機能です。

- しきい値設定では検出できないような、普段と異なる挙動を検知
- 検知した問題の解決方法を例示

アノマリ検知機能の詳細については、「2.3.6 アノマリ検知機能」を参照してください。

1.1.3 プロファイル管理機能

プロファイル管理機能は、管理対象ノードの設定情報をプロファイルとして作成、保存、適用する機能です。

- 管理対象ノードにハードウェア設定を実施
- 管理対象ノード（サーバー）にOSをインストール
- 管理対象ノード（サーバー）に仮想MACアドレス／仮想WWNの割当て、サーバーのブート設定を実施
- 管理対象ノード（ストレージ）にRAID／ホットスペアを作成

プロファイル管理機能によって、複数の管理対象ノードを一括して設定したり、新規に管理するノードの設定を容易にしたりできます。

プロファイル管理機能の詳細については、「2.4 プロファイル管理機能」を参照してください。

1.1.4 ログ管理機能

ログ管理機能は、管理対象ノードの各種ログ（ハードウェアログ、オペレーティングシステムログ、ServerView Suiteログ）の収集を一括して操作、採取した各種ログを一元管理する機能です。

- 各種ログの収集を自動化
- 収集したログの保有期間／世代の設定による管理の自動化
- 各種ログに含まれるメッセージの条件検出による異常調査の効率化

ログ管理機能によって、管理対象ノードの異常監視／調査の作業を効率的に行えます。

ログ管理機能の詳細については、「2.5 ログ管理機能」を参照してください。

1.1.5 ファームウェア管理機能

ファームウェア管理機能は、管理対象ノードのファームウェアアップデートを一括して操作、ファームウェアのバージョンを一元管理する機能です。

- ファームウェアのアップデートを自動化
- 管理対象ノードのファームウェアのバージョン管理を一元化

ファーウェア管理機能によって、管理対象ノードの保守作業の手間を軽減できます。

ファームウェア管理機能の詳細については、「2.6 ファームウェア管理機能」を参照してください。

1.1.6 ネットワーク管理機能

ネットワーク管理機能は、管理対象ノード間の物理的な接続状態、および仮想マシン、仮想スイッチ、仮想ルーターの仮想的な接続状態を管理する機能です。

ネットワークの結線や接続状態を表示するネットワークマップで以下を行えます。

- ネットワーク異常の影響範囲を視覚的に把握
- ネットワークの接続状態の変化を監視
- ネットワークの性能（トラフィック）をグラフで把握
- ネットワークスイッチの設定（VLAN設定、リンクアグリゲーション設定）を容易に変更

ネットワーク管理機能によって、管理対象ノード間のネットワークの異常監視、調査の作業を支援します。

ネットワーク管理機能の詳細については、「2.7 ネットワーク管理機能」を参照してください。

1.1.7 仮想リソース管理機能

仮想リソースとは、複数のストレージで構成された仮想的なストレージ（ストレージプール）のことを指します。

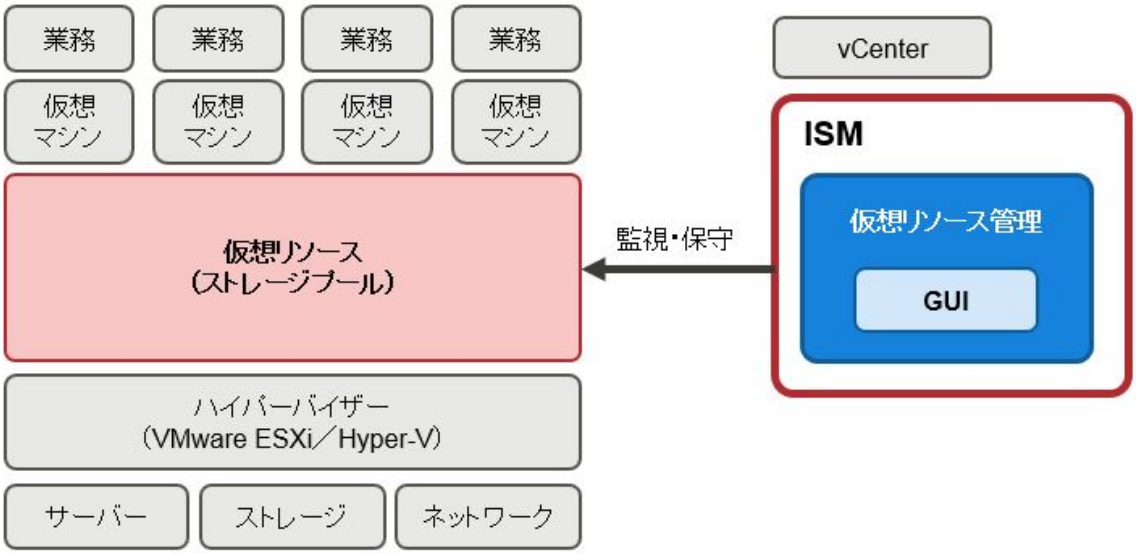
仮想リソース管理機能は、ストレージプールの状態や使用率を表示してストレージプールを管理する機能です。

- ストレージプールの使用状況や状態を、構成するハードウェア機器（ノード）の状態と連動して監視
- ストレージプールを画面上で一元管理することで、スムーズな保守を支援
- ストレージプールを画面上で一元管理することで、リソースの使用率を見える化し、リソースの再配置または追加（プロビジョニング）タイミングの予測を支援

仮想リソース管理機能によって、管理対象ノードとリソースプールの関連が容易に確認でき、異常監視、保守の作業を支援します。

仮想リソース管理機能の詳細については、「2.9 仮想リソース管理機能」を参照してください。

図1.1 仮想リソース管理機能の概要



1.1.8 仮想ネットワーク パケット分析機能

仮想ネットワークパケット分析機能は、収集したパケット情報からポートごと、ネットワークごと、ホストごとの通信量の傾向や通信品質の状況を表示する機能です。

- トラフィック状況を視覚的に把握
- 性能低下要因の特定を支援

仮想ネットワーク パケット分析機能によって、お客様自身によるネットワーク傾向の把握や、問題箇所の特定を支援します。

仮想ネットワーク パケット分析機能の詳細については、「2.11 仮想ネットワーク パケット分析機能」を参照してください。

1.1.9 クラスタ管理機能

クラスタ管理機能は、クラスタを構成するハードウェア機器の状態と連動した監視、およびストレージプールなどの仮想的なストレージ環境の監視を可能とし、クラスタを管理する機能を提供します。ISMの動作モードがAdvancedモードの場合に使用できます。

クラスタ管理機能の詳細については、「2.13.1 クラスタ管理機能」を参照してください。

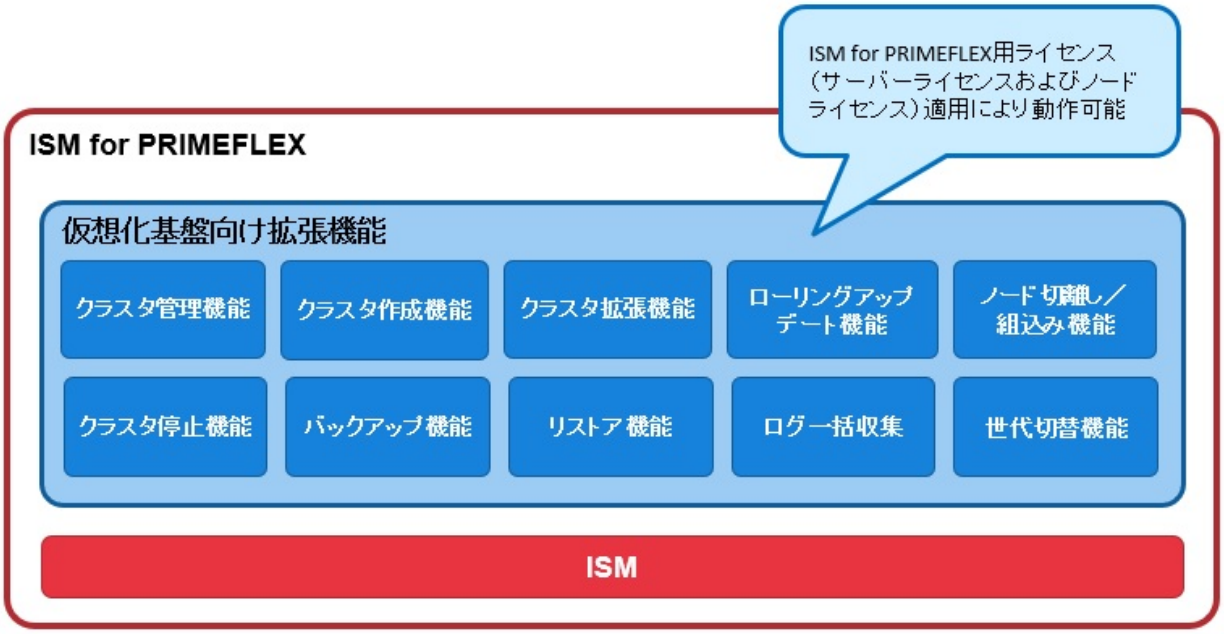
1.1.10 ISM for PRIMEFLEXの機能

ISM for PRIMEFLEXは、ISMの機能に加えて、仮想化基盤向け拡張機能を提供します。

ISM for PRIMEFLEXは、以下の環境を導入するインフラ管理ソフトウェアです。

- 垂直統合型 仮想化基盤 Integrated System PRIMEFLEX ハイパーコンバージドインフラストラクチャー（HCI）
  - Integrated System PRIMEFLEX HS
  - Integrated System PRIMEFLEX for VMware vSAN

図1.2 ISM for PRIMEFLEXの機能概要



ISM for PRIMEFLEXで提供される仮想化基盤向け拡張機能の概要を以下に示します。

凡例：〇 = サポート、ー = 未サポート

仮想化基盤向け拡張機能	機能概要	vSAN環境 [注1]
クラスタ管理機能	クラスタの情報、および関連する物理リソース／仮想リソースの各種情報を表示します。 クラスタ単位でのリソース管理が可能です。	〇
クラスタ作成機能	既存のクラスタとは異なる2つ目以降のクラスタ作成作業を自動化します。 「クラスタ作成」ウィザードを使用してクラスタを作成できます。	〇
クラスタ拡張機能	クラスタリソースの枯渇に伴い、クラスタ拡張時にサーバーを追加する作業を自動化します。 「クラスタ拡張」ウィザードを使用してクラスタを拡張できます。	〇
ローリングアップデート機能	仮想化基盤を構成している一連のサーバーに対して、業務を停止することなく、下記を自動化します。 「ローリングアップデート」ウィザードを使用して実行できます。	
	ファームウェアアップデート	〇
	ESXi修正パッチ適用	〇
	ESXiオフラインバンドル適用	〇
	vCSA修正パッチ適用	〇
	vCSAアップグレード	〇
ノード切離し／組込み機能	クラスタ内のサーバーに対して、業務を停止することなく、サーバーの再起動を伴う保守作業を自動化します。 「ノード切離し」画面、および「ノード組込み」画面からクラスタ内のサーバーを切離し／組込みできます。	〇
バックアップ機能	仮想化基盤を構成しているESXiの構成情報ファイルとvCSAのVAのバックアップを自動化します。	〇

仮想化基盤向け拡張機能	機能概要	vSAN環境 [注1]
	「バックアップ」画面からESXiとvCSAのバックアップができます。	
リストア機能	仮想化基盤を構成しているバックアップしたvCSAのVAのリストアを自動化します。 「リストア」画面からvCSAのリストアができます。	○
クラスタ停止機能 [注2]	クラスタを停止する作業を自動化します。 「クラスタ停止」画面からクラスタを安全に停止できます。	○
VMware vSANクラスタに関連するログ一括収集	クラスタに関連するログ収集を自動化します。 ISM-VA管理機能のコマンド「ismadm cluster logcollect」からログ収集ができます。	○
世代切替機能	現在のPRIMEFLEX の世代管理情報を後継モデルの世代管理情報に更新します。 「世代切替」画面からPRIMEFLEX世代の更新を行えます。	○

[注1] :vSAN環境は、以下の環境を示します。

- Integrated System PRIMEFLEX HS
- Integrated System PRIMEFLEX for VMware vSAN

[注2]:クラスタ起動機能は管理端末でクラスタ起動コマンドを実行することでクラスタを起動する作業を自動化します。

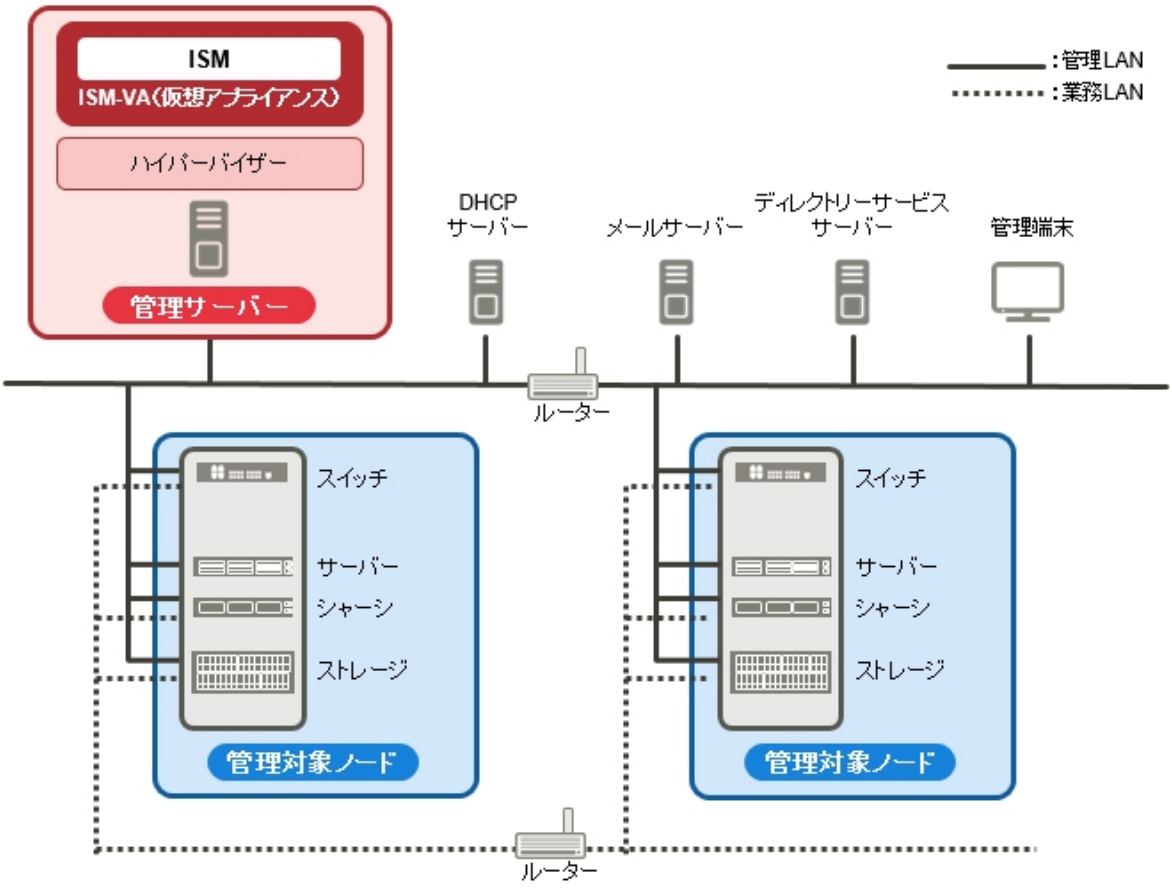
ISM for PRIMEFLEXの機能詳細については、「2.13 ISM for PRIMEFLEXの機能」を参照してください。

1.2 構成

ISMは、原則的に管理対象となるサーバーとは別に用意したサーバー上で動作します。本書では管理対象となる機器を「ノード」(または「管理対象ノード」)と呼び、ISMが動作しているサーバーを「管理サーバー」と呼びます。管理サーバーとノード間は、LANで接続します。

ISMのネットワークインターフェイスは、1つだけ定義できます。複数のネットワークを構成する場合は、ルーターを設定し、各ネットワーク間で通信可能な状態にしてください。

図1.3 ネットワーク構成



注意

- 「図1.3 ネットワーク構成」に記載しているISM外部で用意するサーバーやサービスについての詳細は、「1.3.3 ISMの運用に必要なサービス要件」を参照してください。
- ISMは、IPv6のネットワークには対応しておりません。

機器および機能		説明
ネットワーク	管理LAN	ISMが管理対象ノードの状態監視、制御、データ転送を行うために、管理対象ノードと通信するLANです。セキュリティ確保のため、閉じた接続環境にすることを推奨します。
	業務LAN	サーバーとクライアント間で業務データを転送するLANです。管理サーバーは接続しません。
管理サーバー	Infrastructure Manager(ISM)	本製品の動作基盤となるソフトウェアです。 ISMは、仮想マシンにパッケージ化した仮想アプライアンスとして提供されます。 ISMがパッケージ化された仮想アプライアンスを以降、ISM-VAと呼びます。 ハイパーバイザーにISM-VAをインストール後、ハイパーバイザーのコンソール、またはSSHクライアント経由でISM-VAを操作できます。
管理端末		管理LANを経由して、ISMを操作するためのパソコン、タブレットなどです。
管理対象ノード	スイッチ	ISMが状態監視、制御の対象とするノードです。

機器および機能		説明
	ストレージ	
	サーバー （管理対象サーバー）	ISMが状態監視、制御の対象とするノードです。 BMC（iRMC）を管理LANに接続します。ISMのすべての機能を利用するためには、オンボードLANまたはLANカードも管理LANに接続します。
	シャーシ	ISMが状態監視、制御の対象とするノードです。 MMBを管理LANに接続します。

ネットワーク構成の設計および詳細情報については、「A.1.1 プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定」を参照してください。

1.3 システム要件

ISMの動作環境となるISM-VA（仮想マシン）および管理端末のシステム要件について説明します。また、ISMの各種運用に必要な外部サービスについて説明します。

1.3.1 ISM-VAを動作させるハイパーバイザーの要件

ISM-VA（仮想マシン）を動作させるためにハイパーバイザーから割り当てる要件は、以下のとおりです。

項目	要件
適応機種	PRIMEQUESTシリーズ PRIMERGYシリーズ
ハイパーバイザー	Windows Server Azure Stack HCI OS VMware ESXi KVMがインストールされているRed Hat Enterprise Linux KVMがインストールされているSUSE Linux Enterprise Server Nutanix AHV
CPUコア数	2コア以上
メモリー容量	16GB以上
空きディスク容量	70GB以上
ネットワーク	1Gbps以上

メモリー容量は16GB以上、空きディスク容量は70GB以上です。また、CPUコア数、メモリー容量および空きディスク容量は、管理するノード数や使用する機能に応じて見積もる必要があります。

適応機種

上記表以外の機種であっても、下記のハイパーバイザーが動作するサーバーであれば、ISM-VAは動作可能です。ただし、サーバーおよびハイパーバイザー（ホストOS）はベンダーと保守契約されていることが前提となります。

ハイパーバイザー

- Hyper-Vの役割が含まれるWindows Serverの以下の版数をサポートします。
  - Windows Server 2016/2019/2022/2025
- Azure Stack HCIの以下の版数をサポートします。[注1]
  - Azure Stack HCI OS version 20H2/21H2/22H2/23H2

- VMware ESXiの以下の版数をサポートします。[注2]
  - VMware ESXi 7.0, 7.0b, 7.0 Update 1/2/3
  - VMware ESXi 8.0, 8.0 Update 1/2/3
- KVMがインストールされているRed Hat Enterprise Linuxの以下の版数をサポートします。
  - Red Hat Enterprise Linux 7.7
  - Red Hat Enterprise Linux 8.2, 8.4, 8.6, 8.8, 8.9, 8.10
  - Red Hat Enterprise Linux 9.2, 9.3, 9.4, 9.5, 9.6
  - Red Hat Enterprise Linux 10.0
- KVMがインストールされているSUSE Linux Enterprise Serverの以下の版数をサポートします。
  - SUSE Linux Enterprise Server 12 SP 5
  - SUSE Linux Enterprise Server 15, 15 SP 2/3/4/5/6/7
- Nutanix AHV [注2]

[注1]:管理端末にインストールされたHyper-Vマネージャーからリモート接続して操作する必要があります。
Hyper-Vマネージャーの詳細は、MicrosoftのWebサイトを参照してください。

https://docs.microsoft.com/ja-jp/windows-server/virtualization/hyper-v/manage/remotely-manage-hyper-v-hosts

[注2]:Nutanix Enterprise Cloud on PRIMERGYの場合は、AOS 5.15.5以降でサポートしているVMware ESXiまたはAHVのバージョンに対応しています。

CPUコア数

ノード数	CPUコア数
1～100	2
101～400	4
401～1000	8

仮想ネットワーク パケット分析機能を使用する場合

CPUコアの追加が必要です。

ノード数 [注]	総仮想マシン数	追加CPUコア数
1～10	100	1コア
11～40	400	4コア
41～60	600	8コア
61～100	1000	16コア

[注]:ISM-VAが管理する、仮想化管理ソフトウェアに登録されているノードの数

1ノードに対してパケット分析・ボトルネック分析機能を使用するには、さらに1コア追加する必要があります。

アノマリ検知機能を使用する場合

CPUコアの追加が必要です。アノマリ検知機能で追加が必要なCPUコア数については、「2.3.6.1 動作要件」を参照してください。

メモリー容量

使用するISMの機能に応じて、メモリー容量の追加が必要です。

ノードの手動検出に使用するメモリー容量

メモリー容量に応じて手動検出の対象とするIPアドレス個数には制限があります。手動検出の対象IPアドレスの個数が制限を超過する場合には、超過するIPアドレス個数分のメモリー容量(IPアドレス1個あたり200KB、1GBあたりIPアドレス5000個分)の追加が必要です。

メモリー容量が16GBの場合、手動検出の対象とするIPアドレス個数は7500(同時に複数ユーザーが検出可能な合計個数)となります。

注意

- 同時に複数ユーザーが手動検出を行う場合は、それぞれのユーザーが検出するIPアドレス個数を合計したメモリー容量が必要です。
- メモリーは一時的に使用され、手動検出を行ったユーザーのログアウト後に解放されます。

仮想ネットワーク パケット分析機能を使用する場合

メモリー容量の追加が必要です。

ノード数 [注]	総仮想マシン数	追加メモリー容量
1～10	100	1GB
11～40	400	2GB
41～60	600	3GB
61～100	1000	4GB

[注]:ISM-VAが管理する、仮想化管理ソフトウェアに登録されているノードの数

1ノードに対してパケット分析・ボトルネック分析機能を使用するには、さらに1GBの追加が必要です。

アノマリ検知機能を使用する場合

メモリー容量の追加が必要です。アノマリ検知機能で追加が必要なメモリー容量については、「2.3.6.1 動作要件」を参照してください。

空きディスク容量

管理するノード数および使用するISMの機能に応じて、ディスク容量を見積る必要があります。

ディスク容量の見積りについては、「3.2.1 ディスク資源の見積り」を参照してください。

仮想ネットワーク パケット分析機能を使用する場合

ディスク容量の追加が必要です。

ノード数 [注]	総仮想マシン数	追加ディスク容量
1～10	100	12GB
11～40	400	48GB
41～60	600	72GB
61～100	1000	120GB

[注]:ISM-VAが管理する、仮想化管理ソフトウェアに登録されているノードの数

1ノードに対してパケット分析・ボトルネック分析機能を使用する場合実施するには、さらに6GBの追加が必要です。

アノマリ検知機能を使用する場合

ディスク容量の追加が必要です。アノマリ検知機能で追加が必要なディスク容量については、「2.3.6.1 動作要件」を参照してください。

ISM-VAをバックアップする場合

ISM-VAのサイズと同等以上の空きディスク容量が必要です。

修正パッチまたはアップグレード適用後のシステムアップデート

以下の目安で空きディスク容量が必要になります。

＜全ノードのノードログ件数＞ × 500Byte

ノードログ件数の確認方法は、『操作手順書』の「9.1 修正パッチ／アップグレードプログラムを適用する」を参照してください。

1.3.2 管理端末のシステム要件

GUI(ブラウザー)のシステム要件

ISMのGUIが動作する管理端末のシステム要件は以下のとおりです。

項目	説明
デバイス	パソコン、サーバー、Windows 11タブレット、Androidタブレット、iPad
ディスプレイ	・ パソコン、サーバー、Windowsタブレット:1280×768ピクセル以上 ISM GUIを表示するブラウザーのウィンドウサイズを1280×768ピクセル以上にする必要があります。 ・ タブレット:上記デバイスが搭載するディスプレイ
ネットワーク	100Mbps以上
Webブラウザー	・ パソコン、サーバー、Windowsタブレット: － Microsoft Edge 125以降 － Mozilla Firefox 126以降 － Google Chrome 125以降 ・ Androidタブレット:Google Chrome 90以降 ・ iPad:Safari13以降 安定した動作のため、各ブラウザーは最新バージョンを利用してください。
関連ソフトウェア	Acrobat Reader(マニュアル表示用)

サポートするデバイス、Webブラウザーは以下のとおりです。

凡例:○＝サポート対象、－＝サポート対象外

Webブラウザー	デバイス			
	パソコン、サーバー	Windowsタブレット	Androidタブレット	iPad
Microsoft Edge	○[注3]	○[注1] [注3]	－	－
Mozilla Firefox	○[注3]	○[注1] [注3]	－	－
Google Chrome	○[注3]	○[注3]	○[注3]	－
Safari	－	－	－	○[注2] [注3]

[注1]:「3Dビュー」画面では、タッチ操作による回転、並行移動、拡大縮小はできません。

[注2]:以下の制約があります。

- ファイルは、保存できません。このため、監視データのCSVエクスポート、ノードログおよび保管ログのダウンロード、プロファイルのエクスポートは使用できません。
- ISMリストア、修正パッチ適用、ISM-VAのアップグレードはサポートしていません。

[注3]:ISM GUIからiRMC画面を開く場合、ポップアップブロックを解除する必要があります。ご使用のブラウザーで、ISMのURLに対してポップアップを許可してください。

ファイル転送用管理端末のシステム要件

管理対象ノードのセットアップに必要なデータやISMのログなど、ISM-VAとファイル転送を行う管理端末のシステム要件は以下のとおりです。

項目	説明
デバイス	パソコン、サーバー

項目	説明
空きディスク容量	8GB以上 ISM-VAをバックアップする場合は、ISM-VAと同等以上の空きディスク容量が必要です。
ネットワーク	100Mbps以上
必須ソフトウェア	FTPクライアントソフトウェア
関連ソフトウェア	SSHクライアントソフトウェア

多要素認証用携帯端末のシステム要件

多要素認証に必要な携帯端末のシステム要件は以下のとおりです。

- 任意の携帯端末に多要素認証クライアントアプリケーションをインストールすること

  ISMの多要素認証は、RFC6238に準拠しています。多要素認証クライアントアプリケーションは、Google Authenticator（iOS、Android）が推奨です。

1.3.3 ISMの運用に必要なサービス要件

ISMの各種運用に必要な外部サービスは、以下のとおりです。

項目	説明
メールサーバー（SMTPサーバー）	管理対象ノードの異常や状態の変化をメール送信する場合に、メールサーバーが必要です。 [イベント]-[アラーム]-[SMTPサーバー]で設定します。 ISMは暗号化方式のSTARTTLSをサポートします。(SMTPサーバーの設定に準拠) ISMはLOGIN/PLAIN/CRAM-MD5の認証方式をサポートします。 **注意** ISMに登録できるメールサーバーは1つだけです。
ディレクトリーサーバー	以下の用途で使用する場合に、ディレクトリーサーバーが必要です。 ・ ISMのユーザー管理で使用する場合 使用できるディレクトリーサービスは、以下の2種類です。 － OpenLDAP － Microsoft Active Directory 構築したサーバーを、[設定]-[ユーザー]-[LDAPサーバー設定]で登録します。 **注意** ・ ユーザー連携用のディレクトリーサーバーは、プライマリーとセカンダリーの2つを登録できます。 ・ Microsoft Active DirectoryまたはOpenLDAPのグループ連携用のドメインは、最大5つ登録できます。 ・ 監視対象ノードがディレクトリーサービスを使用している場合、監視対象ノードが属しているディレクトリーサービスとは連携していません。監視対象ノードにアクセスできるアカウントを個別に設定してください。
DHCPサーバー	以下の場合に、DHCPサーバーが必要です。 ・ プロファイル管理機能でOSインストールを行う場合

項目	説明
	・ ファームウェア管理機能のOfflineアップデートを使用する場合 管理対象のノード(サーバー)でPXEブートを可能とするため、ノードに適切なIPv4アドレスをリースできるように設定してください。 **ポイント** DHCPサーバーを別途準備する代わりに、ISM-VAに含まれているDHCPサーバー機能を利用することもできます。 ISM-VA内のDHCP機能の利用方法については、「4.15 ISM-VA内部のDHCPサーバー」を参照してください。
DNSサーバー	以下の用途で使用する場合に、DNSサーバーが必要です。 ・ ISMにホスト名 でアクセスしたい場合 ・ LDAP連携などISMの各種サーバー設定でFQDN を使う場合 DNSサーバーをISMに設定する方法は、「4.9 ネットワーク設定」の「DNSサーバー追加」を参照してください。 **ポイント** ・ DNSサーバーを使用せずにISMにホスト名でアクセスしたい場合は、ISM-VAに手動でホスト名を設定してください。手動でのホスト名設定方法は、「4.13 ホスト名変更」を参照してください。 ・ DNS サーバーを使用しない場合、LDAP連携などISMの各種サーバー設定は、すべてIPアドレスで設定してください。
NTPサーバー	ISMと、監視対象ノードおよび管理クライアント間の時間がずれないよう同期させる場合に、NTPサーバーが必要です。 NTPサーバーをISMに設定する場合は、ismadmコマンドまたはismsetupコマンドを使用してください。 設定方法は、「3.4.2 ISM-VAの初期設定」の「NTP同期有効無効設定」、「NTPサーバー追加削除」を参照してください。
Proxyサーバー	管理クライアントからProxyサーバーを経由してISMへアクセスする場合に、Proxyサーバーが必要です。 **注意** 監視対象ノードとISM間は、Proxyサーバーを経由して接続することはできません。
ルーター	ISMのネットワークインターフェイスは、1つだけ定義できます。 複数のネットワークを構成する環境でISMを使用する場合に、各ネットワーク間で通信可能な状態にルーターを設定しておく必要があります。 ゲートウェイをISMに設定する場合は、ismadmコマンドまたはismsetupコマンドを使用してください。 設定方法は、「4.9 ネットワーク設定」の「ネットワーク設定変更」を参照してください。

ネットワーク構成の設計および詳細情報については、「A.1.1 プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定」を参照してください。

クラスタ管理機能を使用するための要件

以下を参照してください。

- クラスタ管理環境の要件:「2.13.1.2 クラスタ管理機能のサポート対象」
- 事前設定要件:「3.8 仮想リソース／クラスタを管理するための事前設定」

1.3.4 ISM for PRIMEFLEXの動作要件

ISM for PRIMEFLEXの仮想化基盤向け拡張機能の動作要件

動作要件は、以下のとおりです。

- ISM for PRIMEFLEXの導入後に以下のライセンスを登録していること
  - Infrastructure Manager Advanced Edition for PRIMEFLEX サーバーライセンス V3
  - Infrastructure Manager Advanced Edition for PRIMEFLEX ノードライセンス V3

  ライセンスの登録方法については、「3.5 ライセンスの登録」を参照してください。

クラスタ管理機能を使用するための要件

以下を参照してください。

- クラスタ管理環境の要件:「2.13.1.2 クラスタ管理機能のサポート対象」
- 事前設定要件:「3.8 仮想リソース／クラスタを管理するための事前設定」

クラスタ作成機能／クラスタ拡張機能を使用するための要件

以下を参照してください。

- PRIMEFLEX HS、PRIMEFLEX for VMware vSANの要件:『操作手順書』の「6.8.1 動作要件」

  後継機種のクラスタ拡張については、「付録D PRIMEFLEX HS／PRIMEFLEX for VMware vSANのクラスタ作成およびクラスタ拡張の要件」を参照してください。

ローリングアップデート機能を使用するための要件

以下を参照してください。

- ローリングアップデートの要件:『操作手順書』の「6.7.1動作要件」

ノード切離し／組込み機能を使用するための要件

以下を参照してください。

- ノード切離し／組込みの要件:『操作手順書』の「6.11.1 動作要件」

バックアップ機能を使用するための要件

以下を参照してください。

- バックアップの要件:『操作手順書』の「6.12.1 動作要件」

リストア機能を使用するための要件

以下を参照してください。

- リストアの要件:『操作手順書』の「6.13.1 動作要件」

クラスタ停止機能を使用するための要件

以下を参照してください。

- クラスタ停止の要件:『操作手順書』の「6.14.1 動作要件」

世代切替機能を使用するための要件

以下を参照してください。

- 世代切替の要件:『操作手順書』の「6.15.1 動作要件」

ISM for PRIMEFLEX V3.1.0のサポート製品

ISM for PRIMEFLEX V3.1.0がサポートする製品に関する最新の情報は、当社の本製品Webサイトを参照してください。

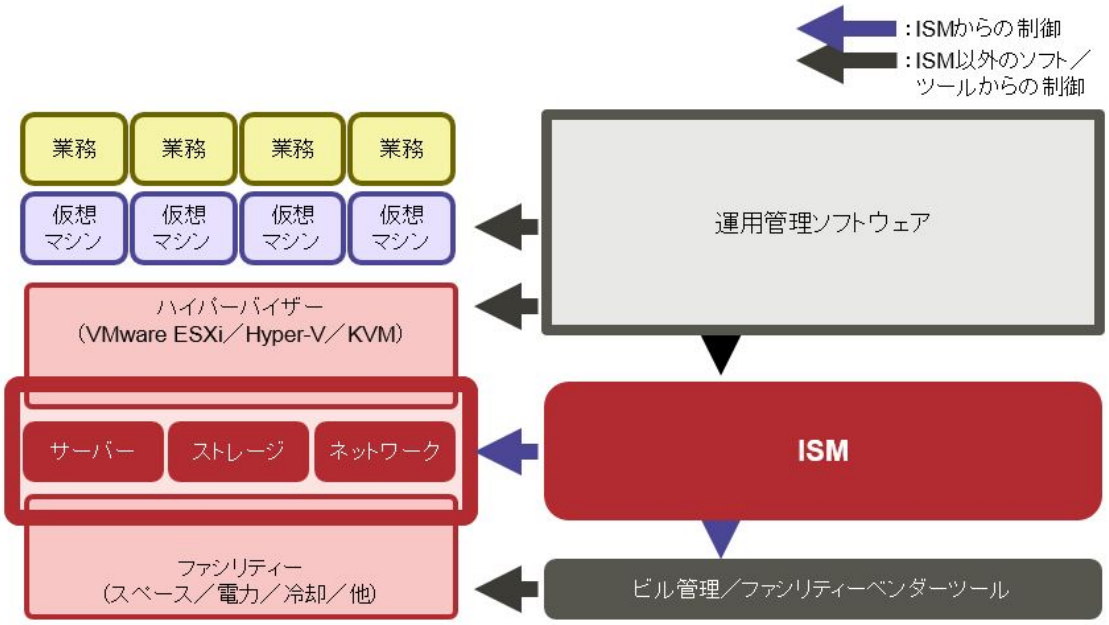
https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

1.4 他製品との連携

ISMは、サーバー、ストレージ、ネットワークなど、主にハードウェアの管理／運用を担います。データセンターの仮想化されたリソースを管理する運用管理ソフトウェアと連携できます。また、ISMでサポート対象とするUPS／PDUなどのファシリティーをISMから制御できます。

ISMと運用管理ソフトウェアと連携することによって、物理的なリソースと仮想化されたリソースのシームレスな運用管理を支援します。

図1.4 他製品との連携



ISMは、以下の製品との連携が可能です。

- 仮想化管理ソフトウェアからの連携
- 総合サーバーセキュリティ「Trend Micro Deep Security」との連携

仮想化管理ソフトウェアからの連携

以下の製品をISMと連携することで、仮想化された環境と物理的な環境をシームレスに運用・管理できます。

- Microsoft System Center Operations Manager
- Microsoft System Center Virtual Machine Manager
- VMware vCenter Server Appliance
- Microsoft Windows Admin Center

ISMでは、上記製品と連携するためのプラグインソフトウェアを提供します。

- Infrastructure Manager Plug-in for Microsoft System Center Operations Manager

- Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager
- Infrastructure Manager Plug-in for VMware vCenter Server Appliance
- Infrastructure Manager Plug-in for Microsoft Windows Admin Center

プラグインソフトウェアの詳細は、『ISM Plug-in/MP セットアップガイド』を参照してください。

Trend Micro Deep Securityとの連携

Trend Micro Deep Securityと連携することで、サーバーのセキュリティ監視情報をISMのGUIに表示できるようになり、サーバーの監視をISMで一元化できます。

Trend Micro Deep Securityとの連携について詳細は、「2.14.9 他ソフトウェア連携機能」を参照してください。

第2章 ISMの機能

この章では、ISMの機能を説明します。

ポイント

ユーザーがISMの各機能を利用するためには、登録されたユーザーグループに対する権限(ユーザーロール)を当該ユーザーに割り当てる必要があります。ユーザーと権限(ユーザーロール)については、「2.14.1 ユーザー管理機能」を参照してください。

ユーザーグループとユーザーロールの組合せと操作実行可否を、以下の表に示すアイコンで表記します。

ユーザーが属するユーザーグループ	ユーザーが持つユーザーロール	実行可能	実行不可
Administratorグループ	Administratorロール	Admin	
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor
Administratorグループ以外	Administratorロール	Admin	Admin
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor

操作を実行できるユーザーの属性を以下のように示します。

例)

- 上記の表示の場合、以下のユーザーグループとユーザーロールの組合わせで設定されたユーザーが実行できることを表します。
  - Administratorグループに属し、AdministratorロールまたはOperatorロールを持つユーザー
  - Administratorグループ以外のグループに属し、AdministratorロールまたはOperatorロールを持つユーザー
- グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。

2.1 ユーザーインターフェイス

ISMのユーザーインターフェイスについて説明します。

ISMは、ユーザーインターフェイスとして以下を提供します。

- GUI:ISMを操作するためのグラフィカルインターフェイス
- FTP:FTPクライアントとISM-VA間のファイル転送インターフェイス
- コンソール:ISM-VAを操作するためのコマンドラインインターフェイス
- REST API:利用者が作成したアプリケーションと連携するためのインターフェイス

2.1.1 GUI

ISMではWebブラウザーで動作するGUI(ISM GUI)を提供します。

ブラウザーごとの必要な設定

使用するブラウザーでCookie、JavaScript、およびDOMストレージを有効にする必要があります。

ご利用になるブラウザーに応じて必要な設定を実施してください。

Mozilla Firefoxを使用する場合

以下の設定が必要です。例としてバージョン126での手順を記載します。

1. Firefoxを起動します。メニューから[設定]を選択します。
2. [プライバシーとセキュリティ]を選択します。
3. [ブラウザープライバシー]配下の[強化型トラッキング防止機能]で[標準]か[カスタム]を選択します。
4. [カスタム]を選択した場合[Cookie]のチェックを外すか、[クロスサイトトラッキングCookie]または[クロスサイトトラッキング Cookieと、他のクロスサイトCookieの隔離]を選択します。
5. [セキュリティ]配下の[証明書]の[証明書を表示]を選択します。
6. [サーバー証明書]タブの[例外を追加]を選択します。
7. [URL]に「https://＜ISMサーバーIPアドレス＞または＜ISMサーバーFQDN名＞:25566/」を入力し、[証明書を取得]を選択します。
8. [次回以降にもこの例外を有効にする]にチェックが付いていることを確認し、[セキュリティ例外を承認]を選択します。
9. Firefoxのアドレスバーに「about:config」と入力します。
10. [javascript.enabled]を[true]に設定します。
11. [dom.storage.enabled]を[true]に設定します。

Google Chromeを使用する場合

以下の設定が必要です。例としてバージョン125での手順を記載します。

1. Google Chromeを起動します。メニューから[設定]を選択します。
2. [プライバシーとセキュリティ]を選択します。
3. [プライバシーとセキュリティ]配下の[サイトの設定]を選択します。
4. [コンテンツ]配下の[サードパーティ Cookie]を選択します。
5. [サードパーティのCookieを許可する]または[シークレットモードでサードパーティCookieをブロックする]を選択します。
6. 上部の[サードパーティ Cookie]の左の矢印を選択し、[サイトの設定]に戻ります。
7. [コンテンツ]配下の[JavaScript]を選択します。
8. [サイトがJavaScriptを使用できるようにする]を選択します。

ポイント

Google Chromeを使用している場合、使用端末のハードウェア性能やグラフィックドライバーなどによっては、WebGL機能（ブラウザーで3Dグラフィックスを表示するための機能）が無効化される場合があります。WebGL機能が無効化されている場合は、「3Dビュー」画面を表示できません。

WebGL機能の有効／無効は、以下の手順で確認できます。

1. Google Chromeを起動し、アドレスバーにchrome://gpuと入力します。
2. [Graphics Feature Status]配下の[WebGL]が[Hardware accelerated]と表示されていれば、WebGL機能は有効です。それ以外の場合は、WebGL機能は無効化されています。

Microsoft Edgeを使用する場合

以下の設定が必要です。例としてバージョン125での手順を記載します。

1. Microsoft Edgeを起動します。メニューから[設定]を選択します。
2. [Cookieとサイトのアクセス許可]を選択します。
3. [保存されたCookieとデータ]配下の[Cookieとサイトデータの管理と削除]を選択します。
4. [Cookieデータの保存と読み取りをサイトに許可する]を有効にします。
5. [サードパーティのCookieをブロックする]を無効にします。
6. 上部の[保存されたCookieとデータ]の左の矢印を選択し、[保存されたCookieとデータ]に戻ります。
7. [サイトのアクセス許可]配下の[JavaScript]を選択します。
8. [許可]を有効にします。

ISM GUIの起動方法

ISM GUIを起動する方法は、以下のとおりです。

1. ブラウザーを起動し、以下のURLを入力します。

   ```
   https://<ISMサーバーIPアドレス>または<ISMサーバーFQDN名>:25566/
   ```

   ログイン画面が表示されます。
2. ユーザー名、パスワードを入力し、[ログイン]ボタンを選択します。

   セキュリティ証明書の警告が表示された場合は、「4.7 証明書設定」を参照して証明書の設定を行ってください。

   初めてISMにログインする場合、「富士通ソフトウェア使用許諾契約書」画面が表示されます。
3. 内容を確認し、[上記内容を確認しました]にチェックを付けます。
4. [同意する]ボタンを選択します。

多要素認証を有効にしたユーザーでISM GUIを起動する方法は、以下のとおりです。

1. ブラウザーを起動し、以下のURLを入力します。

   ```
   https://<ISMサーバーIPアドレス>または<ISMサーバーFQDN名>:25566/
   ```

   ログイン画面が表示されます。
2. ユーザー名、パスワードを入力し、[ログイン]ボタンを選択します。

   セキュリティ証明書の警告が表示された場合は、「4.7 証明書設定」を参照して証明書の設定を行ってください。

   多要素認証を有効にしたユーザーが初めてISMにログインする場合、QRコードと緊急用コードが表示されます。

   緊急用コードは、認証コードを表示する携帯端末などが故障・紛失などで使用できなくなった際に使用します。一度しか表示されませんので、大切に控えてください。
3. 携帯端末などにインストールした多要素認証クライアントアプリケーションで、表示されたQRコードをスキャンします(初回ログインのみ)。

   多要素認証クライアントアプリケーションに認証コードが表示されます。
4. ISM GUIに認証コードを入力し、[ログイン]ボタンを選択します。

ポイント

初回ログイン時のユーザー名、パスワードは以下を使用してください。このユーザー名でログイン後、デフォルトユーザーのパスワード変更やユーザーの新規作成を行い運用してください。

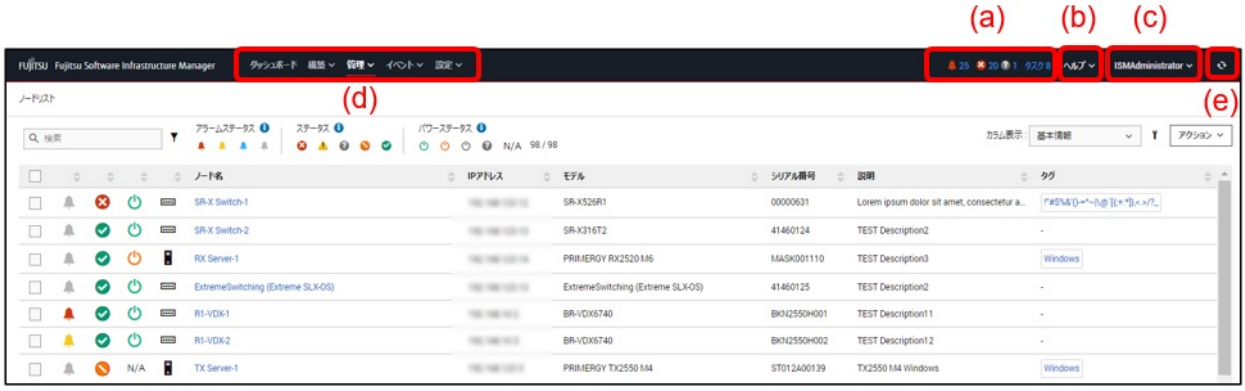
- ユーザー名:administrator
- パスワード:admin

注意

- WebブラウザーにISMのユーザー名、パスワードを保存しないでください。保存した場合は、ISMのユーザー名、パスワードを削除してください。
- 認証コードを表示する携帯端末などが故障・紛失などで使用できない場合で、かつ緊急用コードが不明な場合には、該当ユーザーの多要素認証を無効にします。新しい端末の準備ができたら再度多要素認証を有効にしてください。詳細情報については、「多要素認証 携帯端末故障・紛失時」を参照してください。
- 使用した緊急用コードは、再使用できません。

ISM GUIの画面構成

ISM GUIの画面構成は、以下のとおりです。



(a) **アラームステータス、ステータス、タスクアイコン**

アラームステータス:

Errorアラームステータスのノード数が表示されます。Errorアラームステータスのノードがない場合には、Warningアラームステータスアイコンと Warningアラームステータスのノード数が表示されます。

ErrorまたはWarningアラームステータスのノードがない場合には表示されません。

ステータス:

Errorステータスのノード数、およびUnknownステータスアイコンとUnknownステータスのノード数が表示されます。

Errorステータスのノードがない場合には、Warningステータスアイコンと Warningステータスのノード数が表示されます。

ErrorまたはWarning、Unknownステータスのノードがない場合には表示されません。

タスク:

実行中のタスク数が表示されます。

(b) **ヘルプ**

ヘルプおよびガイダンスを表示します。

(c) **ユーザー名**

ログイン中のユーザー名が表示されます。

ISMからログアウトする場合、ユーザー名にマウスポインターを合わせ[ログアウト]を選択します。

GUIでの表示言語、日付フォーマット、タイムゾーンの設定を変更する場合、[言語]を選択します。

ログイン中のユーザーのパスワードを変更する場合、[パスワード変更]を選択します。

(d) **グローバルナビゲーションメニュー**

ISMの各画面に遷移するためのメニューです。

(e) [更新]ボタン

選択すると画面全体を更新します。

ISM GUIでは、同一画面を表示している場合、画面の自動更新は行われません（画面を遷移した場合は、サーバーから情報の再取得が行われます）。

最新の情報を確認する場合、[更新]ボタンを選択して画面を更新してください。

以下の画面は、設定すると画面の自動更新が可能になります。

- 「ダッシュボード」画面
- 「ノード登録」画面
- 「タスク」画面
- 「ジョブ」画面

2.1.2 FTPアクセス

FTPクライアントを使用して、ISM-VA内のファイル転送用領域にFTPアクセスできます。

「3.4.2 ISM-VAの初期設定」で設定したIPアドレスを指定して接続します。

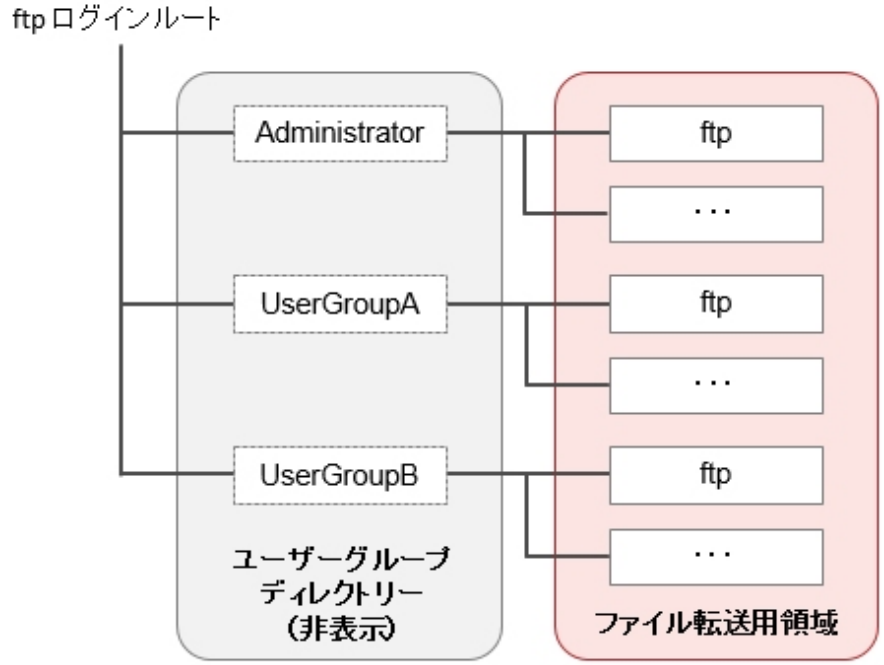
ログイン直後は、セキュリティ強化のためファイルおよびディレクトリーは非表示になっていますので、ログインユーザーが所属するグループ名のディレクトリーに移動し、ファイル転送用領域にアクセスします。

FTPで送受信するファイルの保存先は、図2.1のように「/＜ユーザーグループ名＞/ftp」となっています。

注意

- ユーザーグループ名として指定するディレクトリー名は、ISMのユーザーグループ管理機能で作成するユーザーグループ名またはAdministratorになります。詳しくは、『操作手順書』の「2.3.2 ユーザーグループを管理する」を参照してください。
- FTPでファイルを転送する際は、必ず＜ユーザーグループ名＞ディレクトリー配下の「ftp」ディレクトリー配下を使用してください。
- 既存ディレクトリーの変更／削除はしないでください。
- パッチファイルなどのバイナリデータを転送する際は、バイナリモードで転送してください。
- FTPSプロトコルで接続することはできません。
- Microsoft Active DirectoryまたはOpenLDAPと連携しているユーザーでFTPアクセスを行う場合、連携しているパスワードではなく、ISMに登録したパスワードを使用してください。

図2.1 ファイル転送用領域のディレクトリー構成



FTPアクセス実行例

Administratorグループに所属する、administratorユーザーでアクセスする場合

```
# ftp 192.168.1.50
Connected to 192.168.1.50 (192.168.1.50).
220 (vsFTPd 3.0.2)
Name (192.168.1.50:root): administrator
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.

ftp> ls
227 Entering Passive Mode (192,168,1,50,156,64).
150 Here comes the directory listing.
226 Transfer done (but failed to open directory).
          ※ログイン直後は何も表示されません

ftp> cd Administrator
250 Directory successfully changed.
          ※ログインユーザーの所属するグループ名のディレクトリーへ移動

ftp> ls
227 Entering Passive Mode (192,168,1,50,156,64).
150 Here comes the directory listing.
drwxr-sr-x    2 0        1001           33 Jun 16 20:36 bin
drwxrws---    3 992      989            26 Jun 16 21:54 elasticsearch
drwxrws---    3 0        1001           21 Jun 16 23:20 ftp
drwxrws---    2 0        0               6 Jun 16 20:36 imported-fw
drwxrws---    2 0        0               6 Jun 16 20:36 imported-os
drwxrws---    2 0        0               6 Jun 16 20:36 ismlog
drwxrws---    2 0        0               6 Jun 16 20:36 logarc
drwxrws---    8 0        0              75 Jun 17 14:03 profile
drwxrws---    2 0        0               6 Jun 16 20:36 tmp
```

```
drwxrws---    2 0        1001            6 Jun 16 20:36 transfer
226 Directory send OK.
```
※ファイル転送用領域にアクセス可能

2.1.3 コンソールアクセス

ハイパーバイザーのコンソール、またはSSHクライアント経由で、管理コマンドを実行できます。

SSHクライアント経由で接続する場合は、「3.4.2 ISM-VAの初期設定」で設定したIPアドレスを指定して接続します。

「2.14.1 ユーザー管理機能」で説明する、以下の権限を持つユーザーのみ使用可能です。

- 「Administratorグループ」に属し、「Administratorロール」を持つユーザー
- 全てのノードを管理する設定がされた「Administratorグループ」以外のグループに属し、「Administratorロール」を持つユーザー

使用可能なコマンドは、「2.14.5.1 ISM-VA管理機能のコマンド一覧」を参照してください。

注意

- [Tab]キーによるコマンドパラメーター補完には対応していません。
- 多要素認証を使用する場合は、SSH接続の際にキーボードインタラクティブ認証方式で接続してください。

  多要素認証については、「2.14.1 ユーザー管理機能」の「多要素認証」を参照してください。

  なお、ISMのSSHキーボードインタラクティブ認証が有効に設定されていない場合は、多要素認証の設定はできません。

2.1.4 REST API

ISMは、REST APIを備えています。これを使用して、ISMの機能を外部のプログラムから呼び出すことができます。詳細は、『REST APIリファレンスマニュアル』を参照してください。

2.2 ノード管理機能

ノード管理機能は、データセンター／フロア／ラック／ノードの4階層でノードを管理します。各階層は、以下の意味を持ちます。

- データセンター:データセンター施設の建屋
- フロア:データセンター施設内のマシンルーム
- ラック:フロア内に設置されているラック
- ノード:ラック内に搭載されている管理対象機器

以下の機能があります。

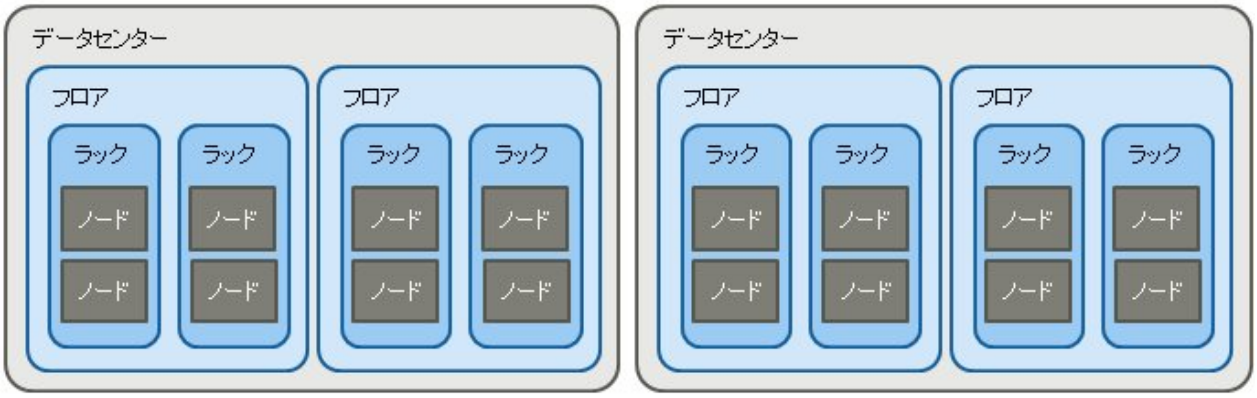
- 2.2.1 データセンター／フロア／ラック／ノードの登録
- 2.2.2 データセンター／フロア／ラック／ノードの確認
- 2.2.3 データセンター／フロア／ラック／ノードの編集
- 2.2.4 データセンター／フロア／ラック／ノードの削除

2.2.1 データセンター／フロア／ラック／ノードの登録

ISMでは、ノードの物理的な位置情報を管理できます。位置情報は、「データセンター > フロア > ラック > ノードのラック内搭載位置番号（スロット番号／パーティション番号）」という階層構造の中で一意に定められます。

ISMでは、データセンター、フロア、ラック、ノードの各個別情報と、相互の階層構造を設定管理します。

図2.2 データセンター、フロア、ラック、ノードの関係



以下の操作を行えます。

- 2.2.1.1 データセンター／フロア／ラックの登録
- 2.2.1.2 ノードの登録
- 2.2.1.3 ノード情報の管理
- 2.2.1.4 ノードのラック搭載位置情報の管理
- 2.2.1.5 ノードのOS情報の登録
- 2.2.1.6 ノードの検出
- 2.2.1.7 ノードへのタグ付け

2.2.1.1 データセンター／フロア／ラックの登録

ISMにデータセンター、フロア、およびラック情報を追加登録します。登録するデータセンター名、フロア名、ラック名にはISMで一意の名前を設定する必要があります。

フロアが登録されている場合、GUIで「フロアビュー」画面および「3Dビュー」画面を表示できます。

ラックが登録されている場合、GUIで「ラックビュー」画面を表示できます。

2.2.1.2 ノードの登録

ISMでノードを管理するためには、ISMにノードを登録する必要があります。

登録の際には、必要な情報を入力します。登録する情報の条件は以下のとおりです。

- ノード名は、ISMで一意な名前を設定する。

  すでにISMに登録されているノードと同じIPアドレスまたはシリアル番号を持つノードは登録できません。

  ノードがOntapクラスタの場合、同じクラスタUUIDを持つノードは登録できません。

- ノード情報として、ノードにアクセスするために必要なアカウント情報を設定する。

  ISMでは設定されたアカウント情報を使用してノードと通信を行い、ノードの情報取得や監視、プロファイル適用、ファームウェアアップデート、ログ収集などの処理を行います。

ノードがETERNUS AB/HBの場合、2つあるコントローラーの内、1つのコントローラーのIPアドレスを登録してください。登録したコントローラーが停止した場合は、もう一方のコントローラーにISMが自動でアクセスします。また、どちらのコントローラーからもトラップ受信可能です。

ノードがETERNUS NR1000の場合、ノードタイプ「storage」、モデル「OntapCluster」を選択してください。IPアドレスには、ETERNUS NR1000のネットワークインターフェイスの内、「管理ポート(e0M)で、かつロールがクラスタ管理」であるネットワークインターフェイスのIPアドレスを入力してください。

ノードがPRIMEQUEST 4000シリーズのパーティションの場合、管理対象のパーティションそれぞれについて、IPアドレスを登録してください。

ISM 2.9.0.020以降、ノードがETERNUS NR/AX/HXの場合、通信方法にHTTPSが追加されます。HTTPS接続可能なアカウントを登録してください。ISM2.9.0.030以降は、ノードがETERNUS ACの場合も同様です。ISM 2.9.0.010以前からETERNUS NR/AX/HXのノードが登録されている場合、ISM 2.9.0.020パッチ適用後、ノード編集画面からHTTPSアカウントを登録してください。HTTPSアカウントが登録されるまでは、ノードステータス監視はできません。

対象機種との通信に必要なアカウント情報や、ノードの登録を行う前に必要な設定については、「A.2.2 ノード設定詳細」を参照してください。

登録方法には以下の2種類があります。

- 必要な情報を設定して、手動で登録する
- ISMの検出機能によってノードを検出後、登録する

ISMに手動で登録する際の操作例を示します。検出機能を利用した登録方法は「2.2.1.6 ノードの検出」を確認してください。ノードを登録するためには、事前に登録する機器のモデル名や設定されているIPアドレスなどの情報を確認しておく必要があります。

注意

ノード登録する対象機種が以下の場合、iRMCのパスワードが工場出荷時のままでは、ISMで管理できません。

- PRIMERGY M7シリーズ
- PRIMERGY 1WAY M6
- PRIMERGY RX1440 M2
- PRIMERGY RX2450 M2
- PRIMEQUEST 4000シリーズ

以下のどちらかの方法で、パスワードを変更してください。

- ISMのノード登録時に[通信方法]の設定箇所で工場出荷時のパスワードと新しいパスワードを入力します。
- ISMのノード登録前にあらかじめ装置上でパスワードを変更します。その後、ノード登録時に変更後の新しいパスワードを入力します。

ISMと対象ノードが通信可能かを判断するためにICMP(Pingコマンド)を使用します。

ICMP通信ができるようにファイアウォールを設定してください。

ノードを登録する手順については、『操作手順書』の「3.1.2 ノードを直接登録する」の手順1～4を参照してください。

ポイント

- 複数のISMや監視ソフトウェアから同一のノードを監視することは推奨していません。ノードによって同時にアクセス可能なセッション数があるため、正しく監視できません。
- ISMに登録するノードには固定のIPアドレスを設定することを推奨します。ノードのIPアドレスが変わると管理できなくなります。
- ノードからSNMPv3でトラップ受信を行うには、SNMPトラップ受信設定が必要になります。「2.3 モニタリング機能」の「トラップ受信設定」を参照してください。

モデルの選択肢にない機器の登録

ISMがサポートしている機器は、ノード登録において「モデル」に選択肢があります。

「モデル」に選択肢がない機器を登録するために、以下の選択肢を用意しています。機器に備わっている機能にそって適切な選択肢を設定してください。

[モデル] 選択肢	説明
OntapCluster	ETERNUS NR/HX/AX/ACをノード登録する場合、こちらを選択してください。 [モデル] に選択肢があるサポート対象機器と比較して監視上の差異はありません。
Generic Server(SNMP)	SNMP監視機能を有している機器をノード登録する場合、これらを選択してください。 必要な設定、および監視項目については、『汎用監視機能操作手順書』を参照してください。
Generic Switch(SNMP)	
Generic Storage(SNMP)	
Generic Facility(SNMP)	
Generic Server(PING)	PINGコマンドに対して応答する機器をノード登録する場合、これらを選択してください。 PINGコマンドの応答結果により、ステータスに正常／異常が反映されます。
Generic Switch(PING)	
Generic Storage(PING)	
Generic Facility(PING)	
other	「Other」を指定した場合は、PINGコマンドによる死活監視を行います。 IPアドレスが指定されない場合、またはIPアドレスが正しくない場合、ステータスはUnknownと表示されます。 通信方法の入力欄が表示されますが、入力された通信方法での監視は行いません。

「モデル」に選択肢がある機器であっても、あえて上記の選択肢を指定しても構いません。ただし、ステータスの通知内容は制限されます。

2.2.1.3 ノード情報の管理

「ノードリスト」画面から[ノード]を選択してノード情報を確認できます。

ISMではノードに設定されているアカウント情報を使用して、約24時間周期でノードからノード情報を取得します。最新のノード情報を取得したい場合には、手動でノード情報を取得してください。

ノードの登録直後には、自動でノード情報取得が実行されます。

ノード情報取得の操作例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードのノード名を選択し、ノードの詳細画面を表示します。
3. [アクション]ボタンから[ノード情報取得]を選択します。

   ノード情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10020303」のログが出力されます。
4. [更新]ボタンを選択して、ノードの詳細画面の表示を更新します。

注意

- PRIMERGYのノード情報を取得する場合、iRMCにBIOSからの装置情報を反映する必要があります。ノード情報取得を実行する前にPRIMERGYの電源を起動し、対象ノードのBIOS画面が表示されたことを確認してください。

- PRIMERGY BXシャーシ(MMB)に対して電源起動直後にノード情報取得を実行した場合、BXサーバーブレード、コネクションブレードがラックビューに表示されないことがあります。

  時間をおいて再度ノード情報取得を実行してください。

- ノード情報は[アクション]ボタンの[ノード情報取得]からだけでなく、約24時間周期で定期的に取得されます。その際にOS情報も取得され、ノード詳細画面の [OS] タブの情報が更新されます。

  OS情報の取得はOSへのアクセスを伴うため停止することもできます。設定方法は、以下のとおりです。

  ー 「ノードリスト」画面で対象のノードにチェックを付け、[アクション]ボタンから[OS情報取得設定]を選択し、取得／停止を設定します。

  ー ノード詳細画面の[OS]タブで、[OSアクション]ボタンから[OS情報取得設定]を選択し、取得／停止を設定します。

  OS情報の取得を停止した場合、ノード詳細画面の[OS]タブの情報は更新されません。

ポイント

以下のいずれかで、ノード情報を約24時間周期で定期的に取得する時刻を設定できます。

- 「ノードリスト」画面で対象のノードにチェックを付け、[アクション]ボタンから[ノード情報取得設定]を選択し、時刻を設定します。
- ノード詳細画面で、[アクション]ボタンから[ノード情報取得設定]を選択し、時刻を設定します。

2.2.1.4 ノードのラック搭載位置情報の管理

ノードのラック搭載位置情報が設定されている場合、GUIの「ラックビュー」画面で確認できます。

ラック搭載位置情報が設定されていない場合、未搭載ノードとして表示されます。

ラック搭載位置情報の設定

ラック搭載位置情報はノードの登録時に設定できます。また、ノードの登録後に設定することもできます。

ノードの登録後、ラック搭載位置情報を設定する際の操作例を示します。

ラック搭載位置情報を設定する前に、ラックを登録しておく必要があります。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードを選択します。[アクション]ボタンから[ノード位置設定]を選択します。
3. ノードを搭載するラックを選択します。
4. ノードの配置場所を選択して、適用します。

2.2.1.5 ノードのOS情報の登録

ISMに登録しているサーバーにOSがインストールされている場合、OS情報を登録してください。

OS情報にはOSの種類、IPアドレス、およびOSに接続するためのアカウント情報などが含まれます。

ドメインユーザーIDを使用しサーバーを監視する際には、ドメインID欄はActive Directoryのレルム名のFQDNを入力し、ユーザー名にはレルム名を除いたユーザー名を入力してください。

ISMでは、登録されたOS情報を使用して、ノード上でOSの管理下に置かれている情報の取得が行われます。

サポート機器、OSに関する最新の情報は、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

注意

- サーバーOSをISMから監視対象にするためには、OSごとに導入手順が必要になります。

  アカウント情報にドメイン名、アカウントにドメインユーザーを登録した場合には、監視対象OSに別途ドメインユーザーで監視させるための設定を追加してください。

  導入手順については、「付録B 監視対象OS、仮想化管理ソフトウェアに対する設定」を参照してください。

- ドメインユーザーを使用してOSを監視するためには、DNSの設定およびドメイン環境の設定が必要になります。
  設定方法については、「3.4.2 ISM-VAの初期設定」を参照してください。

- OS情報が登録されていない場合、またはOSがシャットダウンされている場合、ノード情報を一部取得できなくなります。また、ノード上でOSの管理下に置かれている情報が取得できなくなります。

- OS情報を登録する際にはドメイン名を大文字で記入してください。

- OS情報のOSタイプ・OSバージョンが間違っている場合、以下の事象が発生することがあります。

  ー ノード情報取得がエラーとなることがあります。

  ー ノード情報取得の結果が表示されていても、アノマリ検知の対象にならないことがあります。

  OS情報のOSタイプ・OSバージョンはノードにインストールされているOSを確認し、正しく入力してください。

操作例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードのノード名を選択し、[OS]タブを選択します。
3. [OSアクション]ボタンから[OS情報編集]を選択します。
4. 必要な情報を入力し、適用します。
5. [アクション]ボタンから[ノード情報取得]を選択します。

   ノード情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10020303」のログが出力されます。
6. [更新]ボタンを選択して、[OS]タブの表示を更新します。

2.2.1.6 ノードの検出

ISMではネットワークに接続されているノードを検出できます。検出機能では、検出したノードから登録の際に必要な情報の一部を自動取得し、登録作業をサポートします。

ノード検出機能には、以下の種類があります。

- 手動検出
- 自動検出

手動検出の場合、検出を行う前に検出したいノードに対して、ノードと接続するために必要なアカウント設定を実行しておく必要があります。

対象ノードに応じて検出に使用されるプロトコルが異なります。

サポート機器、OSに関する最新の情報は、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ポイント

ISM-VAにDNSサーバーのIPアドレスを設定することで、以下の動作（処理）が有効になります。

- FQDNによるノード検出

  ノードをFQDNで検出できます。

- ホスト名によるノード検出

  ISM-VAと同一ドメインのノードをホスト名で検出できます。
  ISM-VAと別ドメインのノードを検索したい場合は、FQDNで検出してください。

  DNSサーバーのIPアドレスの設定に加え、ホスト名の設定が必要です。

- 検出されたノードのFQDN取得

  検出されたノードのFQDNが取得されます。ノードの登録時にノード名の初期値としてFQDNが設定されます。

DNSサーバーのISMへの設定方法は、「4.9 ネットワーク設定」の「DNSサーバー追加」を参照してください。
ホスト名のISMへの設定方法は、「4.13 ホスト名変更」を参照してください。

注意

検出ノードのIPアドレスのFQDN名取得時、DNSに逆引きゾーンが設定されていない場合、設定されている場合に比べてノード検出に時間がかかります。

この場合、DNSに逆引きゾーンを設定してください。

手動検出

手動でノード検出を行います。以下の操作が行えます。

- 手動検出実行
  - 検出設定を入力して手動検出実行
  - CSVファイルをアップロードして手動検出実行
- 手動検出結果の確認
- 検出したノードの登録

動作要件

対象機器側の以下の機能がオンであること

機器	機能
PRIMERGY 2/4/8WAY M7以降、PRIMERGY 1WAY M6以降、PRIMERGY RX1440/2450 M2 (HTTPS)	SSDP機能

ポイント

手動検出の詳細は、「A.2.2 ノード設定詳細」を参照してください。

検出設定を入力して手動検出実行

手動検出に必要な情報を設定します。指定したIPアドレス範囲に対して、ノードの検出が実行されます。また、設定したアカウント情報を使用して、登録に必要なノード情報の一部が取得されます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ノード登録]を選択し、「ノード登録」画面を表示します。
2. [アクション]ボタンから[検出]を選択します。

3. 検出に必要な情報を入力します。

項目	説明
IPアドレス検出範囲	検出対象とするIPアドレスの範囲、FQDN、またはホスト名を設定します。 IPアドレスの検出範囲は、第3オクテットまで指定できます。
検出対象	検出対象を選択します。
通信方法	検出対象に応じた通信方法のアカウント情報を入力します。検出対象を指定すると、入力が必要な通信方法の入力欄が表示されます。

4. 検出を実行します。

注意

IPアドレス検出範囲に第3オクテットの数字が異なるIPアドレス(例:10.10.0.1～10.10.4.255)を指定すると、手動検出の完了までに数時間以上かかる場合があります。最新の情報を確認する場合は[更新]ボタンを選択、または[自動更新]を設定してください。
手動検出を中止する場合は、「検出詳細」画面の[キャンセル]ボタンを選択します。なお、手動検出を中止した場合でも、中止した時点までの検出結果は表示されます。

CSVファイルをアップロードして手動検出実行

手動検出に必要な情報を記載したCSVファイルをアップロードします。CSVファイルに記載されている情報に対して、ノードの検出が実行されます。また、アカウント情報を使用して、登録に必要なノード情報の一部が取得されます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ノード登録]を選択し、「ノード登録」画面を表示します。
2. [アクション]ボタンから[検出]を選択します。
3. [検出方式]で「CSVアップロード」を指定します。
4. 検出に必要な情報を入力します。

項目	説明
ファイル選択方式	CSVファイルの指定方法を選択します。
ファイル	検出に使用するCSVファイルを選択します。
パスワード暗号化	CSVファイルのパスワード暗号化方式を選択します。
検出実行後の動作	検出実行後の動作を指定します。ファイル選択方式で「FTP」を選択すると表示されます。

5. 検出を実行します。

ポイント

- [ファイル選択方式]で「FTP」を選択する場合は、あらかじめFTPでCSVファイルをISM-VAの「/Administrator/ftp」のディレクトリー配下に転送しておく必要があります。

  FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。

- [パスワード暗号化]の設定は、CSVファイル内に記載しているアカウント情報のパスワードを暗号化している場合は「暗号化あり」を選択します。暗号化していない場合は「暗号化なし」を選択してください。

- [ファイル選択方式]で「FTP」を選択した場合、[検出実行後の動作]の[元のファイルを削除する]にチェックを付けると、検出実行後のCSVファイルが削除されます。

CSVファイル

ISMのGUIからCSVファイルのテンプレートをダウンロードします。

ダウンロードしたCSVファイルは、1行目に項目名、2行目に選択項目に対応する選択肢が記載されています。

検出対象ノードの情報をこのCSVファイルに追記してください。

CSVファイルのテンプレートのダウンロード手順は、以下のとおりです。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ノード登録]を選択し、「ノード登録」画面を表示します。
2. [アクション]ボタンから[検出]を選択します。
3. [検出方式]にCSVアップロードを指定します。
4. [テンプレート]で対象機種を指定し、[ダウンロード]ボタンを選択してダウンロードを実行します。
   複数の対象機種を指定できます。

注意

ダウンロードしたCSVファイルの2行目（選択肢の行）を、アップロード前までに削除してください。

CSVファイルの設定項目は、以下のとおりです。

項目名	説明
IpAddress	検出対象ノードのIPアドレス（IPv4、IPv6、FQDN名、またはホスト名）
IpmiAccount	iRMC／BMC（IPMI）のユーザー名
IpmiPassword	iRMC／BMC（IPMI）のパスワード
IpmiPort	iRMC／BMC（IPMI）のポート番号 指定がない場合、623（デフォルトポート番号）を使用
SshAccount	SSHのユーザー名
SshPassword	SSHのパスワード
SshPort	SSHのポート番号 指定がない場合、22（デフォルトポート番号）を使用
HttpsAccount	HTTPSのユーザー名
HttpsPassword	HTTPSのパスワード
NewHttpsPassword	HTTPSの新しいパスワード PRIMERGY M7シリーズ、PRIMERGY 1WAY M6、PRIMERGY RX1440 M2/RX2450 M2、PRIMEQUEST 4000シリーズ（iRMC）のパスワードを工場出荷時の状態から変更していない場合に新しいパスワードを指定してください（変更済の場合は指定不要です）。 このとき、「HttpsPassword」に工場出荷時のパスワードを指定してください。
HttpsPort	HTTPSのポート番号 指定がない場合、443（デフォルトポート番号）を使用
SnmpType	SNMPのバージョン 設定値：SnmpV1、SnmpV2、SnmpV3のどれか SNMPv2cを使用する場合は、SnmpV2を指定してください。
SnmpPort	SNMPのポート番号 指定がない場合、161（デフォルトポート番号）を使用
Community	コミュニティー名 SnmpTypeに、SnmpV1、SnmpV2のどちらかを設定した場合に必要
V3Account	SNMPv3のユーザー名
V3SecLevel	SNMPv3のセキュリティレベル

項目名	説明
	設定値:authPriv、authNoPriv、noAuthNoPrivのどれか
V3AuthProtocol	SNMPv3の認証プロトコル 設定値:MD5、SHAのどちらか
V3AuthPassword	SNMPv3の認証パスワード
V3PrivProtocol	SNMPv3の暗号化プロトコル 設定値:DES、AESのどちらか
V3PrivPassword	SNMPv3の暗号化パスワード
V3EngineId	SNMPv3のエンジンID
V3ContextName	SNMPv3のコンテキスト名

アカウント種別ごとの設定項目は、以下のとおりです。

凡例:◎＝設定必須、○＝省略可、－＝設定対象外

項目名	アカウント種別					
	IPMI	SSH	HTTPS	SNMP		
				V1	V2	V3
IpAddress	◎	◎	◎	◎	◎	◎
IpmiAccount	◎	－	－	－	－	－
IpmiPassword	◎	－	－	－	－	－
IpmiPort	○	－	－	－	－	－
SshAccount	－	◎	－	－	－	－
SshPassword	－	○	－	－	－	－
SshPort	－	○	－	－	－	－
HttpsAccount	－	－	◎	－	－	－
HttpsPassword	－	－	◎	－	－	－
NewHttpsPassword	－	－	○	－	－	－
HttpsPort	－	－	○	－	－	－
SnmpType	－	－	－	◎	◎	◎
SnmpPort	－	－	－	○	○	○
Community	－	－	－	◎	◎	－
V3Account	－	－	－	－	－	◎
V3SecLevel	－	－	－	－	－	◎
V3AuthProtocol	－	－	－	－	－	○ [注1]
V3AuthPassword	－	－	－	－	－	○ [注1]
V3PrivProtocol	－	－	－	－	－	○ [注2]
V3PrivPassword	－	－	－	－	－	○ [注2]
V3EngineId	－	－	－	－	－	○
V3ContextName	－	－	－	－	－	○

[注1]:V3SecLevelがauthPriv、authNoPrivの場合は必須です。

[注2]:V3SecLevelがauthPrivの場合は必須です。

CSVファイルの記載方法は、以下のとおりです。

- CSVファイル名は、任意の名称で作成します。
- 1行目に項目名を記載します。
- 2行目以降に検出対象ノードの情報を記載します。

  - 1行目に記載した項目名と対応する位置に設定値を記載してください。
  - IpAddress項目は、必ず記載してください。
  - 対象ノードの検出に必要のない項目の設定値は、省略してください。
  - すべての対象ノードで不要な項目は、項目名の列全体を削除できます。
  - 各パスワード(IpmiPassword、V3AuthPassword、V3PrivPassword、SshPassword、HttpsPassword)には、暗号化したパスワードを設定することを推奨します。

    暗号化していないパスワードを設定することもできます。

    パスワード暗号化の手順については、『REST API リファレンスマニュアル』を参照してください。

注意

CSVファイル内で、暗号化したパスワードと、暗号化していないパスワードは混在できません。どちらかに統一する必要があります。

CSVファイルの記載例を以下に示します。

```
"IpAddress","IpmiAccount","IpmiPassword","SnmpType","Community","SshAccount","SshPassword"
"192.168.10.11","admin1","********","","","","",""
"192.168.10.12","admin2","********","","","","",""
"ism.fujitsu.com","admin3","********","","","","",""
"192.168.10.21","","","SnmpV1","comm1","user1","********"
```

手動検出結果の確認

「ノード登録」画面の画面更新を行い、[検出進捗]に表示されている検出処理の完了を待ちます。完了後、検出されたノードを確認します。

設定したアカウント情報で検出に成功した場合、ステータスが成功となり、検出ノードを確認できます。

注意

- 検出ノード情報は、ISMにログインしている間、参照できます。再ログイン時には引き継がれません。
- 検出結果には、サポート対象外の機器も表示される場合があります。サポート対象外の機器は登録しないでください。
- VDXスイッチの場合、ノード検出およびノード登録対象はVCS Fabric(Brocade VCS Fabric)となります。ファブリックに設定している仮想IPアドレスを指定してノード検出およびノード登録を実行してください。物理スイッチは、ファブリックがノード登録されたあとで、ノード情報取得によって自動的に検出され、ノード登録されます。物理スイッチをノード検出した場合、検出結果は「自動登録のみ」となります。
- CFXスイッチをファブリックモードで動作させている場合、ノード検出およびノード登録の対象はファブリックに設定している仮想IPアドレスです。物理スイッチは、ファブリックがノード登録されたあとで、ノード情報取得によって自動的に検出され、ノード登録されます。

手動検出したノードの登録

ノードを登録する手順については、『操作手順書』の「3.1.1 ネットワーク内ノードを検出してノード登録する」の手順7～12を参照してください。

注意

- 機器に設定されているIPアドレスを変更できるのは、PRIMERGYサーバー、PRIMEQUEST 3000Bでかつ DHCP設定の場合のみです。
- IPアドレスを変更する場合、指定するIPアドレスがISMからアクセスできる範囲であることを確認してください。ISMからアクセスできないIPアドレスを指定した場合、機器に接続できなくなる可能性があります。
- Cisco Catalystスイッチの「ログ収集」や「ファームウェアアップデート」の機能を利用する場合は、ノード登録後、ノードの編集画面でSSH権限昇格パスワードを設定してください。

自動検出

自動検出の対象機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

自動検出機能では、以下の操作が行えます。

- 自動検出実行
- 自動検出結果の確認
- 検出したノードの登録

自動検出実行

自動検出は自動的に実行されます。ISMでは、設定変更項目はありません。

動作要件

以下の要件を満たす必要があります。

- 対象機器側の以下の機能がオンであること

機器	機能	検出間隔
PRIMERGYサーバー PRIMEQUEST [注1]	SSDP機能 [注2]	15分ごと
イーサネットスイッチ（10GBASE-T 48+6） イーサネットスイッチ（10GBASE 48+6）	Auto Discovery [注2]	10分ごと

[注1]: PRIMEQUEST 4000シリーズは、対象外です。

[注2]: 自動検出を抑制する場合は、無効に設定してください。

- 対象機器からのマルチキャスト送信パケットをISMが受信できるネットワーク構成であること

自動検出結果の確認

機器が検出されると、「ノード登録」画面の[検出ノードリスト]にノードが表示されます。

自動検出したノードの登録

ノードを登録する手順については、『操作手順書』の「3.1.1 ネットワーク内ノードを検出してノード登録する」の手順7～12を参照してください。

注意

- IPv6リンクローカルアドレスでは機器を管理できません。自動検出されたIPアドレスがIPv6リンクローカルアドレスのみの場合、IPアドレス設定が必要です。
- 機器に設定されているIPアドレスを変更できるのは、以下の場合のみです。

機器	説明
PRIMERGYサーバー PRIMEQUEST 3000B	機器がDHCP設定の場合のみ変更できます。
イーサネットスイッチ(10GBASE-T 48+6) イーサネットスイッチ(10GBASE 48+6)	機器が固定IPアドレス設定の場合のみ変更できます。 機器に正しいIPアドレスを設定し、登録してください。

- IPアドレスを変更する場合、指定するIPアドレスがISMからアクセスできる範囲であることを確認してください。ISMからアクセスできないIPアドレスを指定した場合、機器に接続できなくなる可能性があります。

検出したノードの登録時のハードウェア設定

ISMで対象ノードの監視に必要な設定を定義したポリシー(監視ポリシー)を事前に作成しておくと、ノードを自動または手動で検出して登録する際にそのポリシーを参照したプロファイルが自動で作成され、適用できます。

事前に参照するポリシーを作成しておくことで、ハードウェアの監視に必要な設定内容の誤りや漏れを防止できます。

注意

監視ポリシーを適用したノードは、モデル毎プロファイルを適用することはできません。モデル毎プロファイルを使用するには、監視ポリシーを適用しないでください。

本設定は、以下のノードに対して適用できます。

- PRIMERGY、PRIMEQUEST 3000B

検出したノードを登録するときのハードウェア設定の操作例を示します

1. 監視ポリシーを定義します。詳細については、「2.4.2 プロファイルとポリシー」を参照してください。
2. 検出したノードの登録と同じ手順を実施します。
   - 手動検出したノードの登録の場合

     手順1～4を実施します。
   - 自動検出したノードの登録の場合

     手順1～5を実施します。
3. [ノード登録時に監視ポリシーを適用する]にチェックを付け、[次へ]ボタンを選択します。

   監視ポリシーが設定されていない場合、または監視ポリシーを設定できるノードが存在しない場合、チェックを付けることができません。

   確認画面が表示されます。

   監視ポリシーを参照して自動で作成されるプロファイルの名前は、以下の優先度で設定されます。

   1. Default_Profile_<ドメイン名>
   2. Default_Profile_<シリアル番号>
   3. Default_Profile_<IPアドレス>
   4. Default_Profile_<日時>

   プロファイル名が既存のプロファイル名と重複していた場合、プロファイル名の末尾に"_数値(1～)"を付加して重複しない名前に変更され、登録されます。
4. 登録を実行します。

ポイント

定義できる監視の設定の詳細は、『プロファイル管理機能 プロファイル設定項目集』の「第8章 共通ポリシーの設定項目」を参照してください。

2.2.1.7 ノードへのタグ付け

ISMではノードに対して自由にタグを設定できます。タグはユーザーが自由にノードをグルーピングするための情報を付与する機能です。ノードをグルーピングするための機能としてノードグループも存在しますが、ノードグループはユーザーのアクセス制御を行います。それに対して、タグはアクセス制御とは絡めずに設定できます。また、ノードに対して複数のタグを設定できます。

例えば、同じ目的を持つノード群に対してタグを設定することで、フィルタリングにより同じタグを持つノードリストを表示して管理できます。

ノードへのタグ付けはノードの登録時に実行できます。また、ノードを登録したあとでも設定できます。

ノード登録後のタグ設定

ノード登録後、タグを設定する際の操作例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 対象ノード名を選択し、[プロパティ]タブを表示します。
3. [アクション]ボタンから[編集]を選択します。
4. タグ情報を編集します。
5. [適用]を実行し、編集内容を反映します。

複数ノードへの一括でのタグ編集

複数のノードに対して一括でタグを編集できます。一括でタグを編集する際の操作例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. タグを編集するノードを選択し、[アクション]ボタンから[タグ編集]を選択します。
3. タグ情報を編集します。
   - タグを追加する場合

     [タグ一括追加]欄に新規タグを入力するか、既存のタグを選択して[追加]を選択します。
   - タグを一括で削除する場合

     [タグ一括削除]欄からタグを選択し、[削除]を選択します。
   - 個別のタグを削除する場合

     [対象ノード]の[タグ]欄に表示されているタグの[x]を選択します。
4. [適用]を実行し、編集内容を反映します。

タグ指定によるフィルタリング

タグを指定してノードをフィルタリングする際の操作例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 画面左上の検索ボックスにフィルタリングしたいタグ名を入力します。検索ボックスに文字列を入力すると、検索対象の候補が表示されますので、「タグ:」を選択します。
   または、検索ボックス右の[⋮]ボタンを選択し、表示された画面でフィルタリングしたいタグ名を入力後、[フィルター]ボタンを選択します。

   フィルタリングが実行され、指定したタグが設定されているノードが「ノードリスト」画面に表示されます。

ポイント

フィルタリング結果のノードを選択し、[プロファイル適用]や[ファームウェア/ドライバーアップデート]を実行できます。プロファイル適用やファームウェア/ドライバーアップデートについては、「2.4 プロファイル管理機能」および「2.6 ファームウェア管理機能」を参照してください。

2.2.2 データセンター／フロア／ラック／ノードの確認

ISMに登録されている情報を確認します。

データセンター／フロア／ラックの確認

ISMのGUIでグローバルナビゲーションメニューから[管理]-[データセンター]を選択し、「データセンターリスト」画面を表示します。「データセンターリスト」画面で対象のデータセンターを選択し、画面右側の表示で確認します。

ポイント

確認可能なデータは、以下のとおりです。

- Administratorグループに属するユーザーの場合:

  すべてのデータを確認できます。

- Administratorグループに属していないユーザーの場合:

  自身の権限で閲覧可能なノードが1件以上登録されているデータのみ確認できます。

ノードの確認

ISMに登録されているノードを確認します。

ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。対象ノードのノード名を選択し、[プロパティ]タブを表示することで確認します。

ポイント

以下の設定によりWeb画面(iRMC)でログイン操作が不要となり、ノード(PRIMERGYサーバー)のWebURLを選択することでWeb画面を表示できます。

- Microsoft Active DirectoryまたはOpenLDAPのグループ連携によるユーザー管理設定
- 中央認証サービス(CAS)設定

詳細は、『操作手順書』の「3.7 サーバーのWeb画面のログインにCASベースのシングルサインオンを利用する」を参照してください。

なお、設定を行うユーザーは以下の2つの条件を満たす必要があります。

- 全ノードを管理するユーザーグループに属していること
- CAS設定で指定されているユーザーロール以上を持つこと

ノードのOS情報の確認

ノードにOSアカウント情報が登録されている場合には、OSからネットワーク、ディスク、カード情報を確認できます。

ドメインユーザーIDを使用して仮想化管理ソフトウェアを監視する際には、ドメインID欄はActive Directoryのレルム名のFQDNを入力し、ユーザー名にはレルム名を除いたユーザー名を入力してください。

その場合、GUIの表示項目には、そのドメインユーザーの権限で取得できる情報だけが表示されます。

監視対象OSに関する設定方法については、「付録B 監視対象OS、仮想化管理ソフトウェアに対する設定」を参照してください。

AIS Connect Support Gateway連携スクリプトファイルのダウンロード

管理対象ノード(PRIMERGYサーバーのみ)をAIS Connect Support Gateway(以降、「AIS Gateway」と表記)に登録するためのスクリプトファイルをダウンロードできます。

スクリプトファイルをダウンロードする操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
   「ノードリスト」画面が表示されます。
2. [アクション]ボタンから[AIS Gatewayスクリプト出力]を選択します。
   「AIS Gatewayスクリプト出力」画面が表示されます。
3. zipファイルのパスワードを設定します(任意)。
4. [出力]ボタンを選択します。
   ダウンロードファイル作成後、「結果」画面が表示されます。
5. 「ダウンロード」を選択します。

スクリプトファイルの概要

スクリプトファイルは、AIS GatewayをインストールしたOS(Windows/Linux)上で実行できます。

スクリプトファイルの実行結果は、AIS Gatewayにログインして設定情報を確認してください。

ダウンロードできるスクリプトファイルの種類は以下のとおりです。

OS	スクリプトファイル
Windows	バッチファイル
	PowerShellスクリプト
Linux	シェルスクリプト (bash)

AIS Gatewayに設定する項目および設定内容は以下のとおりです。

設定項目の追加、設定値の変更など必要に応じてスクリプトファイルを編集してください。

AIS Gateway項目	設定内容
AssetName	管理対象ノードのシリアル番号
Model	iRMC_ma
Description	管理対象ノードのノード名
IP Address	管理対象ノードのIPアドレス
SNMP Community	public

注意

- 以下の場合は、該当する管理対象ノードを登録する行がコメントアウトされます。
  必要に応じて対処を行い、再度ダウンロードしてください。または、スクリプトファイルを直接編集してください。
  - IPアドレスが設定されていない場合

    IPアドレスを設定してください。

IPアドレスの設定については、「2.2.3 データセンター／フロア／ラック／ノードの編集」の「ノードの編集」を参照してください。

ー シリアル番号が取得されていない場合

ノード情報取得を行い、シリアル番号を取得してください。

ノード情報の取得については、「2.2.1.3 ノード情報の管理」を参照してください。

・ 本スクリプトは、すでに管理対象ノードがAIS Gatewayに登録済みの場合、そのノードの設定情報を上書きします。

上書きしない場合、該当の管理対象ノードのシリアル番号を含む行をコメントアウト、または、削除してください。

2.2.3 データセンター／フロア／ラック／ノードの編集

ISMに登録されている情報を編集します。

データセンター／フロア／ラックの編集

データセンター、フロア、ラック情報を編集する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[データセンター]を選択し、表示される「データセンターリスト」画面で、対象のデータセンターまたはフロア、ラックを選択します。
2. [アクション]ボタンから[データセンター編集]または[フロア編集]、[ラック編集]を選択します。
3. 情報を編集します。
4. [適用]を選択し、編集内容を反映します。

ノードの編集

ノード情報を編集する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードのノード名を選択し、[プロパティ]タブを表示します。
3. [アクション]ボタンから[編集]を選択します。
4. ノード情報を編集します。

   モデル編集時に表示される選択肢は、編集前のモデルと同一のサービスをISMが提供できるモデルに限られます。
5. [適用]を実行し、編集内容を反映します。

ノードの一括編集

ノード情報を一括編集する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. [アクション]ボタンから[一括編集]を選択します。
3. ノード情報を編集します。

4. [適用]を実行し、編集内容を反映します。

IPMI有効／無効の設定

iRMCとの通信に使用するIPMIプロトコルの有効（使用する）／無効（使用しない）を設定できます。

対象機種は、以下のとおりです。

- PRIMERGY M7シリーズ
- PRIMERGY RX1440 M2
- PRIMERGY RX2450 M2
- PRIMEQUEST 4000シリーズ

ノード登録時のデフォルトは、IPMI無効です。

IPMI有効に設定する場合は、あらかじめ対象機種のiRMCでIPMIを有効化に設定（IPMI over LAN を有効にする）してください。その後、ISMでIPMI有効に設定してください。

2.2.4 データセンター／フロア／ラック／ノードの削除

ISMに登録されている情報を削除します。

データセンターの削除

データセンターを削除する場合、データセンター内にフロアが登録されていると削除できません。フロアを削除または移動してからデータセンターを削除してください。

フロアの削除

フロアを削除する場合、フロア内にラックが登録されていると削除できません。ラックを削除または移動してからフロアを削除してください。

ラックの削除

ラックを削除する場合、ラック内にノードが登録されていると削除できません。ノードを削除または移動してからラックを削除してください。

ノードの削除

ノードの監視情報やノード情報、ログ情報などが削除されます。ノードを削除する場合は、事前に以下の操作を完了させてください。

- 実行中のタスクがある場合は、完了を待ってください。
- 適用済みプロファイルは適用を解除してください。
- ダッシュボード画面の監視履歴ウィジェットを表示している場合は、「ウィジェット設定：監視履歴」画面で対象ノードから削除するノードを外してください。

ポイント

プロファイルが適用された状態でノードを削除すると、当該ノードは削除されません（プロファイルが適用済みの状態のまま残ります）。個別にプロファイルを適用解除してください。

注意

複数の端末からログインしている場合、データセンター、フロア、ラック、ノードを削除した際、削除していない端末で削除した対象に対して操作すると、「存在しないか、既に削除されています」などのエラーが発生することがあります。この場合、以下の方法で画面を更新してから操作を継続してください。

- ネットワークマップ以外の場合

  [更新]ボタンを選択します。

- ネットワークマップの場合

  [アクション]ボタンから[ネットワーク管理情報の取得]を実行します。

ポイント

フロアが登録されているデータセンター、ラックが登録されているフロア、ノードが登録されているラックは削除できません。これと異なり、ノードが登録されているシャーシを削除すると、シャーシとノードが同時に削除されます。

2.3 モニタリング機能

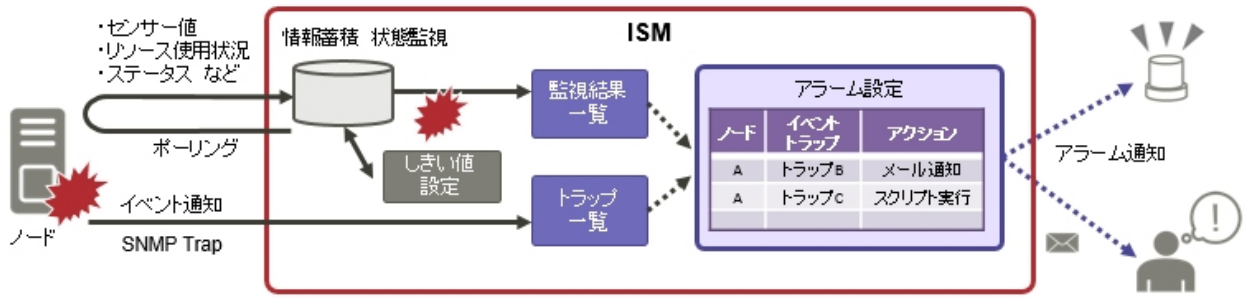
モニタリング機能は、以下の用途で利用する機能です。

- ノードの温度などのセンサーの値やCPU使用率などのリソース使用状況、ステータスなどの状態をポーリングし、情報を蓄積
- 事前に指定したしきい値とポーリング結果との比較、およびステータスの変化を監視
- ノードからのイベント通知（SNMP Trap）を受信
- 監視の結果およびノードからのイベント通知を、外部にアラームとして通知

  アラーム通知方法は、事前にアラーム設定のアクションとして設定します。

モニタリング機能の動作概要を以下に示します。

図2.3 モニタリング機能イメージ



ポーリングの監視周期は、デフォルトで180秒です。監視周期設定で変更できます。

モニタリングに関係する機能は、以下のものがあります。

- 2.3.1 監視項目／しきい値
- 2.3.2 ネットワーク統計情報監視
- 2.3.3 アクション設定
- 2.3.4 アラーム設定
- 2.3.5 監視履歴グラフ表示

・ 2.3.6 アノマリ検知機能

2.3.1 監視項目／しきい値

監視項目（値の取得対象の項目）としきい値を設定します。

以下の項目については、ノードの登録時にデフォルトで監視項目として登録されます（実際に管理可能な項目の詳細は機種によって異なります）。

デフォルトの監視対象	説明
統合ステータス	管理対象ノード自身が持つ、システム全体としてのステータス値（overall status）を監視します。 IPMIやSNMPのプロトコルを使用して、3分周期で各ノードにアクセスしてISMのGUIにステータスとして表示します。 ステータスを表示している箇所は、以下のとおりです。 ・ ノードリスト ・ ノード詳細画面の[プロパティ]タブ
消費電力	管理対象装置全体としての消費電力や部品ごとの消費電力を監視します。
温度情報	筐体内部の温度や、吸気口の温度などを監視します。
各種LEDステータス	Power LED, CSS LED, Identify LED, Error LEDを監視します。 対象はPRIMERGYのみとなります。
電源状態	電源状態を監視します。

監視項目の統合ステータスは、以下の値を取ります。

統合ステータス	ISM GUIでのアイコン表示	状態
Error（異常）		ノードに問題が発生し、使用継続が不可能な状態です。
Warning（注意）		ノードに問題は発生していますが、使用継続は可能な状態です。
Unknown（不明）		ノードに問題が発生し、状態が確認できない状態です。
Normal（正常）		ノードは正常な状態です。

以下の項目については、追加指定により監視できます。

追加の監視対象	説明
各種資源情報	CPU使用率、メモリー使用率、ディスク使用率などの資源状況を監視します。
FAN回転数	管理対象装置内にある各種FANの回転数を監視します。
温度情報（デフォルトの監視対象以外）	デフォルトの監視対象以外の温度（部品温度など）を監視します。

監視項目／しきい値の追加手順

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードのノード名を選択します。

3. [監視]タブを選択します。
4. [監視アクション]ボタンから[追加]を選択し、監視項目を追加します。

注意

- Brocade FCスイッチの場合、複数の吸気温度情報を監視対象として追加可能です。ただし、実際に監視できる温度は、装置に搭載されている温度センサーのみとなります。監視できない温度の場合、[最新値]に「N/A」が表示されます。
- CPU使用率、メモリー使用率、ディスク使用率などの各種資源情報を監視項目に追加するためには、ノードのOS情報を登録する必要があります。ノードのOS情報の登録については、「2.2.1.5 ノードのOS情報の登録」を参照してください。

2.3.2 ネットワーク統計情報監視

ネットワークスイッチについて、ポート単位で各種統計情報（トラフィックなど）を取得し、しきい値監視を設定できます。

[ネットワーク統計]タブで表示される監視項目は、以下のとおりです。

監視項目名	説明
Incoming Traffic	1秒あたりの受信ビット数
Outgoing Traffic	1秒あたりの送信ビット数
Incoming Packets	1秒あたりの受信パケット数
Outgoing Packets	1秒あたりの送信パケット数
Incoming Drop Packets	受信ドロップパケット数の差分
Outgoing Drop Packets	送信ドロップパケット数の差分
Incoming Error Packets	受信エラーパケット数の差分
Outgoing Error Packets	送信エラーパケット数の差分

[最新値]には、すべてのポートの中で最大の値が表示されます。

上記表の説明で記載している「パケット数の差分」とは、今回取得した全パケット数と前回取得した全パケット数の差分です。
おおよそ監視周期あたりのパケット数になります。

ネットワーク統計情報監視／しきい値監視の設定手順

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ネットワークスイッチのノード名を選択します。
3. [ネットワーク統計]タブを選択します。
4. [ネットワーク統計アクション]ボタンから[登録]または[編集]を選択し、ネットワーク統計情報監視を有効にします。

注意

ネットワーク統計情報監視を使用するためには、対象ノードのSNMPアカウントはv2cまたはv3を使用してください。

2.3.3 アクション設定

ISMがイベントを検出したとき、またはノードからトラップを受信したときに外部にアラームとして通知できます。

通知方法(アクション)のタイプとして以下のものがあります。

通知方法のタイプ	説明
リモートスクリプト実行	外部ホスト上に配置した任意のスクリプトを外部ホスト上で実行します。
メール送信	ユーザーが定義した任意の内容のメールを送信します。
トラップ送信／転送	受信したSNMPトラップを外部SNMPマネージャーに転送、またはISM内部で検出したイベントをSNMPトラップとして送信します。また、転送時の「転送タイプ」を以下から選択します。 ・ ISMを送信元として転送 転送されたSNMPトラップはISMから直接送信されたように処理されます。 送信元情報以外は受信したトラップ情報をそのまま転送します。 SNMPバージョンに応じて以下のように処理されます。 ― v1で転送された場合 トラップのagent-addrにISMのIPアドレスが設定されます。 ― v2c／v3で転送された場合 トラップのvariable-bindingsにトラップ送信元のIPアドレスが設定されます。 具体的には、1.3.6.1.6.3.18.1.3 (snmpTrapAddress)の値として、トラップ送信元(機器のiRMC)のIPアドレスが設定されます。 ・ 受信したトラップをそのまま転送 受信したトラップがそのままSNMPマネージャーに転送されます。
Syslog転送	外部Syslogサーバーに、イベント／トラップのメッセージを転送します。

ポイント

Syslog転送を使用する場合、外部Syslogサーバーに対して、ISMから転送されるSyslogを受信できるように設定する必要があります。設定方法については、『操作手順書』の「2.2 アラーム設定をする(ISM内部のイベント)」を参照してください。

マクロ

メール送信の件名や本文内、およびスクリプト実行時の引数指定に、以下に示すマクロ(自動変数)機能が使用できます。これらのマクロは、自動的にノード情報やイベント情報に置換されます。

また、アラーム設定を作成したときに指定した対象種別に応じて、使用できるマクロに差異があります。

各マクロの一覧と対象種別との対応関係は、以下のとおりです。

凡例:○＝使用できる、×＝使用できない

マクロ表記方法	概要	対象種別	
		ノード	システム
$_ISM	ISMホスト名	○	○
$_TRGID	イベントの対象(Node)のノードID	○	×

マクロ表記方法	概要	対象種別	
		ノード	システム
$_TRGTYPE	イベントの対象（SystemまたはNode）	○	○
$_TRG	イベントの対象名（ノード名）	○	×
$_IPA	ノードのIPアドレス	○	×
$_IDN	ノードのシリアル番号	○	×
$_MDL	ノードのモデル名	○	×
$_DC	ノードが設置されているデータセンター名	○	×
$_FLR	ノードが設置されているフロア名	○	×
$_RACK	ノードが設置されているラック名	○	×
$_POS	ノードのラック搭載位置 機器に応じて表示形式が異なります。 ・ 1Uサーバーが2Uに搭載されている場合 ：2U ・ CX400シャーシ（2U）が2Uに搭載されており、そのスロット2に対象のサーバーが存在する場合 ：2-3U slot#2 ・ BX900シャーシ（10U）が2Uに搭載されており、その背面スロット2に対象のコネクションブレードが存在する場合 ：2-11U CB#2 ・ PDUが搭載されている場合 ：PDU2 ・ RackCDUが搭載されている場合 ：表示なし	○	×
$_MIB	SNMPトラップのMIBファイル名	○	×
$_SPC	SNMPトラップのSpecific Trap Code SNMPトラップのOIDの最後の数字	○	×
$_TRP	SNMPトラップのMIBのTYPEに定義されている文字列	○	×
$_SEV	イベントの重大度 ・ イベントタイプがトラップの場合 Critical、Major、Minor、Informational、Unknown ・ イベントタイプがイベントの場合 Error、Warning、Info	○	○
$_EVT	イベントのメッセージID	○	○
$_MSG	イベントの説明	○	○
$_TIM	イベント発生時刻 UTC時刻をRFC3339形式で表示します。 （例：2018-01-01T00:00:00.000Z）	○	○
$_TIM2	イベント発生時刻 ローカル時刻を表示します。 （例：2018-01-01-00.00.00）	○	○

ポイント

マクロが使用できない場合（上記表で「×」のもの）や、置換するべき値が存在しない場合は、(none)と出力されます。

アクションの追加手順

詳細な手順については、『操作手順書』の「2.2.1.1 外部ホスト上に配置したスクリプトを実行する」の「アクション設定」を参照してください。

各アクションを使用するときに必要な準備作業

リモートスクリプト実行

詳細な手順については、『操作手順書』の「2.2.1.1 外部ホスト上に配置したスクリプトを実行する」の「事前設定」を参照してください。

メール送信

詳細な手順については、『操作手順書』の「2.2.1.2 メールを送信する」を参照してください。

トラップ送信／転送

詳細な手順については、『操作手順書』の「2.2.1.3 トラップ送信／転送を行う」を参照してください。

アクションのテスト実行手順

詳細な手順については、『操作手順書』の「2.2.2 アクション（通知方法）をテストする」を参照してください。

2.3.4 アラーム設定

アラーム設定とは、ISMがイベントを検出したとき、またはノードからトラップを受信したときに実行するアクションを事前に定義したものです。

アラームの追加手順

詳細な手順については、『操作手順書』の「2.2.3 ISM内部のイベントを対象にアラームを設定する」を参照してください。

イベントタイプ

イベントタイプには、以下の種類があります。

イベントタイプ	説明
イベント	ISM内部で検出した各種イベント。 アラームを発生させる対象となるイベントを重大度で指定するか、または個々のイベントを指定します（複数指定可）。
トラップ	監視対象装置から送信されるSNMPトラップ。 ISM-VA内に登録されているMIB情報を基に、受信可能なトラップの一覧が表示されます。 アラームを発生させる対象となるトラップを重大度で指定するか、または個々のトラップを指定します。 [対象種別]で「システム」を選択した場合は表示されません。

注意

イベントタイプがトラップの場合、アラームを発生させる対象となるトラップは監視対象のハードウェアから送信されるSNMPトラップのみです。

アラームステータス

アラームステータスは各ノードに1つ存在する値で、そのノードに関して何らかのISMイベントやSNMPトラップが検出された場合に変化します。アラームステータスは以下の値を取ります。

アラームステータス	優先度	ISM GUIでのアイコン表示	説明
Error	高	 赤色のベルマーク	以下のイベントが検出された場合に表示されます。 ・ ErrorレベルのISMイベント ・ CRITICALレベルのSNMPトラップ
Warning	中	 黄色のベルマーク	以下のイベントが検出された場合に表示されます。 ・ WarningレベルのISMイベント ・ MAJORまたはMINORレベルのSNMPトラップ
Info	低	 青色のベルマーク	以下のイベントが検出された場合に表示されます。 ・ InfoレベルのISMイベント ・ INFORMATIONALレベルのSNMPトラップ
None	-	 白色のベルマーク	何もイベントが検出されていない状態です。

アラームステータスがInfo以上の値の場合、各レベルに対応したイベントを検出したことを意味します。ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択して、「イベントリスト」画面を表示し、各タブを選択して検出したイベントの内容を確認してください。

検出したイベントに対して対処／確認が完了した場合は、以下の手順でアラームステータスを解除してください。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面を表示します。
2. 対象ノードのノード名を選択します。
3. [アクション]ボタンから[アラーム解除]を選択します。

ポイント

- アラームステータスは、自動的には解除されません。検出された、より優先度の高いステータスが表示されます。
- ノードの保守作業時、計画的にノードを電源オフにすることがあります。保守作業による電源オフなどのアラームをISMが検出しないように、監視を一時的に停止する「メンテナンスモード」の機能があります。

  メンテナンスモードに変更されたノードに対しては、ISMのアラーム検出およびバックグラウンドの処理が抑止されるため、当該ノードで何度もアラームが発生することを防止できます。

  メンテナンスモードについては、「5.1 メンテナンスモード」を参照してください。

注意

PRIMERGY CXシリーズおよびPRIMEQUEST 4000シリーズの場合、シャーシに対してアラーム解除を実行しても、アラームステータスは解除されません。

PRIMERGY CXシリーズ、PRIMEQUEST 4000シリーズのシャーシに通知されるアラームステータスは、シャーシの配下に属するノードのアラームステータスを通知します。複数のノードが属する場合、いずれかのノードでイベントが検出されると、シャーシのアラームステータスに通知されます。複数のノードでイベントが検出されると、最も優先度の高いイベントがシャーシのアラームステータスに通知されます。

シャーシに属するすべてのノードに対してアラーム解除を行うと、シャーシのアラームステータスは解除された状態になります。

なお、PRIMERGY CXシリーズ、PRIMEQUEST 4000シリーズのシャーシ自体にイベントが検出されることはありません。このため、シャーシに対してアラーム解除を実行する必要はありません。

トラップ受信設定

SNMPトラップの受信プロトコルとしてv1、v2c、v3に対応しています。

SNMPトラップ受信設定の追加手順

詳細な手順については、『操作手順書』の「3.2.2 SNMPトラップ受信設定をする」を参照してください。

MIBファイル

MIBとは、SNMPで管理されるネットワーク機器の状態の公開情報のことであり、RFC 1213で規定されているMIB-2として標準化されています。MIBファイルは、この公開情報を定義したテキストベースのファイルを指します。SNMPトラップをやり取りするためには、受信側が機器側の提供するMIBファイルを保持しておく必要があります。

MIBファイルは、以下の場合に追加／更新します。

- ISM未サポートの当社外装置、CiscoスイッチやHPサーバーなどエフサステクノロジーズ以外のベンダーから提供されているハードウェアから、SNMPトラップを受信するために新規MIBファイルを追加したい場合
  ISMがサポートする機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。
  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/
- ファームウェアアップデートに伴い、すでにISMに登録済みのMIBファイルを更新したい場合

注意

- 登録されているMIBファイルは削除できます。ただし、削除したMIBファイルに定義されていたSNMPトラップを受信した場合、不明なトラップとして処理されます。
- 同一トラップが定義されたMIBファイルを複数登録しないでください。同一トラップが定義されたMIBファイルを複数登録した場合、同一トラップを複数受信したように扱われます。
- ISMがトラップの重要度などを扱うためには、取り込むMIBファイルが特定の書式で書かれている必要があります。指定外の書式で書かれたMIBファイルを取り込んだ場合、定義と異なる動作をする可能性があります。MIBファイルを取り込む前に書式に問題がないか確認してください。

  MIBファイルの書式に関する詳細は、「A.1.3 MIBファイルのインポートに関する注意」を参照してください。

MIBファイルの登録

ISMに登録されていないMIBファイルを新たに追加します。

1. MIBファイルを用意します。このとき、MIBファイルに依存関係のあるすべてのファイルが必要になります。
2. ISM-VAにMIBファイルを転送します。
3. ISM-VA管理機能からMIBの登録コマンドを実行します。

詳細は、「4.16 MIBファイル設定」を参照してください。

ポイント

すでにISMに登録されているMIBファイルと同名のファイルを登録することで、MIBファイルをアップデートできます。

MIBファイルの確認

ISMに登録されているMIBファイル名の一覧を確認します。MIBファイル名の一覧を確認するには、ISM-VA管理機能のMIBファイル表示コマンドを実行します。

詳細は、「4.16 MIBファイル設定」を参照してください。

MIBファイルの削除

ISMに登録されているMIBファイルの登録を解除するためには、該当するMIBファイルを削除します。MIBファイルを削除するには、ISM-VA管理機能のMIBファイル削除コマンドを実行します。

詳細は、「4.16 MIBファイル設定」を参照してください。

ポイント

MIBファイルを削除する場合、依存関係に注意してください。依存関係のあるMIBファイルを削除した場合、トラップを受信できなくなる可能性があります。

2.3.5 監視履歴グラフ表示

ISMのGUIでは、モニタリング機能で蓄積した監視項目の履歴をグラフ表示できます。グラフ表示することで、監視項目履歴の推移や傾向を容易に把握できます。ノードごとのグラフを表示する方法と、複数ノードのグラフをダッシュボードウィジェットに表示する方法があります。

詳しくは、『操作手順書』の「4.6 監視履歴をグラフ表示する」を参照してください。

2.3.6 アノマリ検知機能

アノマリ検知機能は、管理対象ノードを構成するハードウェア／ソフトウェアの動作やリソース消費状態を常時監視し、普段とは異なる挙動を検知し通知します。

アノマリ検知機能を開始すると、CPU使用率予測を行うことができます。有効に設定しておくことでCPUの使用率を監視し異常が発生する日時を予測して通知します。

アノマリ検知機能は、以下の物理サーバーの状態を監視します。

- VMware ESXiホスト
  vCenter ServerまたはvCenter Server Applianceで管理されたESXiホストが対象です。
  vCenter ServerまたはvCenter Server Applianceで管理されない単体のESXiホストは対象外です。
- Red Hat Enterprise Linuxサーバー
  Red Hat Enterprise Linuxが動作する物理サーバーが対象です。

詳細については、「2.3.6.1 動作要件」を参照してください。

以下の機能を提供します。

- アノマリ検知機能の開始／停止
- CPU使用率予測設定の有効／無効
- アノマリ検知情報の表示
- アノマリ検知履歴の表示
- アノマリ検知／回復のイベント通知
- 解決方法の表示
- アノマリ検知の抑制

対象とするサーバーから一定期間の情報を収集し、学習データ(予測モデル)を作成します。この学習データにより監視項目に対する普段の正常範囲を算出し、現在の測定値が正常範囲内であるかを判定(正常性範囲判定)します。判定は、以下のタイミングで行われます。

- VMware ESXiホスト:3分に1回
- Red Hat Enterprise Linuxサーバー:24時間に1回

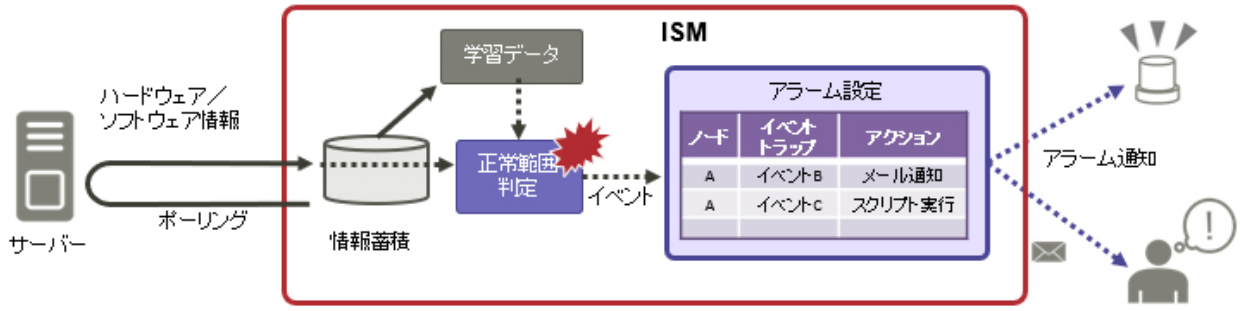
正常範囲から外れている場合、アノマリ検知イベントを発生させます。アノマリ検知のイベントは、設定によりアラームとして外部に通知することができます。

アノマリ検知した状況が持続する場合は、3分ごとにイベントが発生します。

「アノマリ検知の抑制」を行うことでイベントの発生を抑えることができます（VMware ESXiホストのみ）。

「アノマリ検知の抑制」は、通知されたアノマリ検知イベントに対し、判断基準を自動で変更し以降の検知を抑制します。

図2.4 アノマリ検知機能イメージ



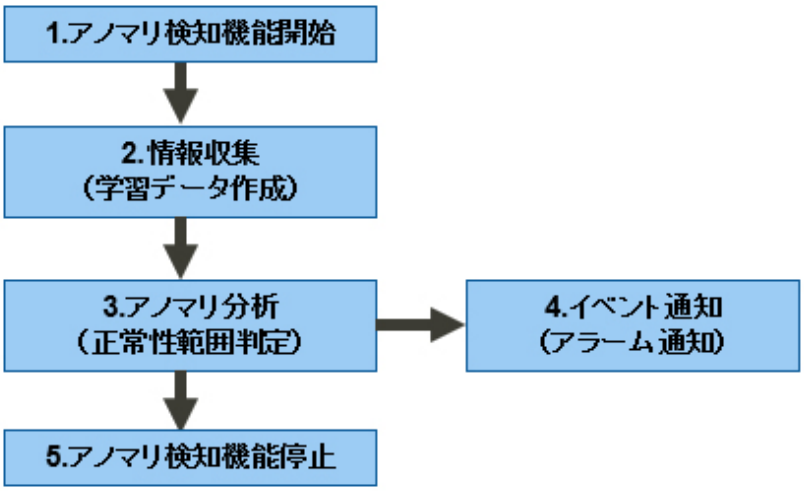
特長

- 監視のためのしきい値設定が不要
- 普段と異なる挙動をリアルタイムで検出
- しきい値設定では捉えられない潜在的な異常や予期しない箇所での障害を検知
- 検知した問題の解決を支援

アノマリ検知機能の動作フロー

アノマリ検知機能の動作の流れについて以下に示します。

図2.5 アノマリ検知機能の動作フロー



監視項目

以下に監視する項目の一覧を示します。監視項目ごとにアノマリ分析を行い、それぞれ個別のイベントを通知します。

表2.1 VMware ESXiホストの監視項目一覧

監視対象	監視項目名
メモリー	ディスクからメモリーに読み出される量
	メモリーからディスクに書き出される量
ストレージ	コマンドのキュー遅延時間
	ホストのディスクアクセス時間
	読み出し処理に要した時間
	書き込み処理に要した時間
物理NIC	送信ドロップ数
	受信ドロップ数
	送信エラー数
	受信エラー数
仮想マシン	CPU使用率
	実行待ち時間
仮想スイッチポート	送信ドロップ数
	受信ドロップ数
パケット受信スレッド	CPU使用率
	実行待ち時間
パケット送信スレッド	CPU使用率
	コンテキストスイッチ回数
	実行待ち時間

表2.2 Red Hat Enterprise Linuxサーバーの監視項目一覧

監視対象	監視項目名
CPU	IO待ち時間 [注]

[注]:NFSアクセスに関するIO待ち時間を監視対象とします。

予測項目

以下に予測する項目の一覧を示します。

表2.3 VMware ESXiホストの予測項目一覧

予測対象	予測項目
仮想マシン	CPU使用率
パケット受信スレッド	CPU使用率
パケット送信スレッド	CPU使用率

Red Hat Enterprise Linuxサーバーの予測項目一覧

なし

情報収集データ

アノマリ検知機能を開始するノードでは、アノマリ分析に必要な普段のふるまいを把握するための情報収集が行われます。この情報収集されたデータが情報収集データとなります。運用を続けていくことで情報収集データを蓄えていきます。

学習データ

学習データとは、アノマリ検知の判定基準となる「正常範囲」(ある程度の幅を持ったしきい値)の基準となるデータです。学習データは、情報収集データから作成されます。学習データの作成が完了するまでアノマリ分析は開始されません。

初回の学習データ作成に要する期間、学習データの更新タイミングは以下のとおりです。

項目	VMware ESXiホストのアノマリ検知	Red Hat Enterprise Linuxサーバーのアノマリ検知
初回の学習データ作成	約2日半	約7日
学習データの更新	12時間ごと	24時間ごと

学習データはアノマリ検知機能を停止した場合でも保持されます。ただし、以下の場合には学習データを再作成してください。

- アノマリ検知機能を開始するノードのハードウェアや仮想化管理ソフトウェアの構成およびOS情報に変更が入った場合
- アノマリ検知機能を開始するノードのリソース使用量が変わった場合
- アノマリ検知機能を1か月以上停止していた場合

アノマリ検知機能の開始時に、新しい学習データを作成するか以前の学習データをそのまま使用するかを選択できます。

新しく学習データを作成し直す場合は、アノマリ検知を開始するときに[情報収集データ初期化]の[初期化する]チェックボックスを選択します。初めてアノマリ検知機能を開始するノードは、チェックの有無にかかわらず学習データが作成されます。

予測用データ

予測用データとは、CPU使用率予測で予測を行うためのデータです。CPU使用率予測設定を有効に設定後、予測用データは情報収集データから最大3か月分作成され、更新されていきます。予測可能な期間は、予測用データが蓄積された期間(蓄積期間)に応じて異なります。以下に一覧を示します。

予測可能な期間	蓄積期間
予測実施なし	3週間未満
1週間	3週間以上、3か月分未満
1か月間	3か月間

注意

- CPU使用率予測設定を無効にした場合、予測用データは削除されます。
- ISMのバックアップ／リストア機能によりリストアした場合、CPU使用率予測設定は無効になります。作成済の予測用データは、バックアップ対象ではありません。

アノマリ検知の判定基準とする期間

ある一定期間の情報収集データを使用し、アノマリ検知の判定基準とする学習データを作成していきます。この期間を「アノマリ検知の判定基準とする期間」といいます。初期値は7日間です。

アノマリ検知の判定基準とする期間は、アノマリ検知機能の開始時に7日間と31日間で切り替えることができます。切り替え後、アノマリ検知状態は「情報収集中(学習データ作成中)」(5分～1日間)となります。情報収集後、アノマリ検知が動作します。

ポイント

- 情報収集は、以下のタイミングで更新されます。
  - VMware ESXiホスト:3分に1回
  - Red Hat Enterprise Linuxサーバー:24時間に1回(ISM-VAのタイムゾーンで設定されたローカルタイムのAM2:00)

- 学習データの作成(アノマリ検知機能の初回開始時や新しく学習データを作成し直す時)には、以下の時間を要します。

  ー VMware ESXiホスト:2日半程度

  ー Red Hat Enterprise Linuxサーバー:7日程度

  この期間に学習したデータがその後のアノマリ検知の基本データとなります。学習データの作成期間には、休日やサーバー保守などの稼働状態が普段とは異なる期間を含まないようにしてください。アノマリ検知結果の妥当性が疑われる場合には、アノマリ検知機能を停止し学習データを再作成してください。

- 学習データは、以下のタイミングで更新されています。

  ー VMware ESXiホスト:12時間ごと

  ー Red Hat Enterprise Linuxサーバー:24時間ごと

  これによりアノマリ検知の判定基準となる「正常範囲」が分析、設定されます。アノマリ検知機能を停止せずに継続して使用することで普段のふるまいとの違いをより高い精度で判定できるようになります。

- 1か月の期間にCPU使用率などの変動が大きい時期と小さい時期の混在が想定される場合、「アノマリ検知の判定基準とする期間」を31日間に設定することで、その期間(31日間)を基準とした、より的確なアノマリ検知が行われます。

- ISM 2.9.0.030において、アノマリ検知のアルゴリズムを改善しました。まれに発生する挙動をアノマリ検知の判定基準で正常範囲として判断できるようになります。この改善により、深夜や週末に行われるノードのバックアップ運用など、一時的に負荷かかる処理に対してアノマリと判定されにくくなります。

注意

- アノマリ検知機能は、ハードウェア故障などのすべての要因を検出するものではありません。また、アノマリ検知された場合でも必ずしも異常が発生しているとは限りません。通知された内容を元に、ハードウェアやソフトウェアの状態を確認し対応を検討してください。
- 仮想マシンを利用していない状態で学習すると、アノマリ検知時にその仮想マシンに対して正常値範囲が大きな値のアノマリ検知を示す場合があります。アノマリ検知結果の妥当性が疑われる場合には、再学習を実施してください。
- 本機能はvCenter ServerまたはvCenter Server Appliance(以降はまとめて「vCenter」と表記)から情報を収集します。そのため、vCenterの仕様としてvCenterのアクセスログにログイン、ログアウトが約3分に1回記録されます。
- 本機能はRed Hat Enterprise LinuxサーバーのOSからSSHにてログインを行い、監視項目の情報を収集します。そのため、OSのアクセスログにSSHのログイン、ログアウトが24時間に1回記録されます。
- ISMのバックアップ／リストア機能によりリストアした場合、すべてのノードのアノマリ検知機能は停止します。作成済の学習データは、バックアップ対象ではありません。

2.3.6.1 動作要件

アノマリ検知機能を利用するために必要な動作要件を示します。

対象ノード

アノマリ検知機能を開始できるノードは、対応するハイパーバイザーが動作し仮想化管理ソフトウェアで管理されているサーバー、または対応するOSが動作しているサーバーです。

対応するソフトウェア環境は、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ISM-VAに必要なリソース

アノマリ検知機能を使用するには、ISM-VAが動作するハイパーバイザーにリソースの追加が必要です。必要なリソースは、お使いの環境に応じて変動します。

アノマリ検知機能を使用する前に、以下の表を参照して必要なリソースを追加してください。また、開始後に環境が変化する場合は、あらかじめ増加する数を見込んだリソースを追加しておいてください。

表2.4 ISM-VAに必要なリソース（VMware ESXiホスト）

アノマリ検知の判定基準とする期間	リソース追加要件	追加単位	追加リソース		
			CPUコア数	メモリー容量	ディスク容量
7日間	同時にアノマリ検知機能を実施するノード数	10ノード当たり	0.4コア	1.3GB	4.0GB
	仮想マシンの総数 [注1]	100VM当たり	0.2コア	0.4GB	2.0GB
	仮想化管理ソフトウェアの総数 [注2]	1CMS当たり	-	1.0GB	-
31日間	同時にアノマリ検知機能を実施するノード数	10ノード当たり	0.4コア	2.5GB	4.0GB
	仮想マシンの総数 [注1]	100VM当たり	0.2コア	1.0GB	2.0GB
	仮想化管理ソフトウェアの総数 [注2]	1CMS当たり	-	2.5GB	-

[注1]：アノマリ検知機能を利用するノードに登録されている仮想マシン数の合計

[注2]：アノマリ検知機能を利用するノードを登録している仮想化管理ソフトウェア（CMS）数の合計

表2.5 ISM-VAに必要なリソース（Red Hat Enterprise Linuxサーバー）

アノマリ検知の判定基準とする期間	リソース追加要件	追加単位	追加リソース		
			CPUコア数	メモリー容量	ディスク容量
7日間	同時にアノマリ検知機能を実施するノード数	10ノード当たり	0.8コア固定 [注]	0.2GB固定 [注]	1.8GB
31日間	同時にアノマリ検知機能を実施するノード数	10ノード当たり	0.8コア固定 [注]	0.2GB固定 [注]	8.0GB

[注]：Red Hat Enterprise Linuxサーバーのアノマリ検知で必要なCPUコア数とメモリー容量は、ノード数によって変動しません。

VMware ESXiホストのCPU使用率予測を使用するには、上記に加えて、リソースの追加が必要です。以下の表を参照して必要なリソースを追加してください。

表2.6 CPU使用率予測を使用する場合にISM-VAに必要なリソース

リソース追加要件	追加単位	追加リソース		
		CPUコア数	メモリー容量	ディスク容量
CPU使用率予測を実施するノード数	10ノード当たり	0.1コア	0.6GB 固定 [注]	0.1GB

[注]：CPU使用率予測で必要なメモリー容量は、ノード数によって変動しません。

例1：PRIMEFLEXでの構成（ノード数：3、1ノード当たりの仮想マシン：31、仮想化管理ソフトウェア数：1）に基づいた場合

[総仮想マシン数] 3 * 31 = 93 台

[例1の構成で必要な追加リソース]

アノマリ検知の判定基準とする期間	CPU使用率予測設定	CPUコア数	メモリー容量	ディスク容量
7日間	無効	1.0（0.6）コア	2.7GB	6.0GB
31日間	無効	1.0（0.6）コア	6.0GB	6.0GB
7日間	有効	1.0（0.7）コア	3.3GB	6.1GB

アノマリ検知の判定基準とする期間	CPU使用率予測設定	CPUコア数	メモリー容量	ディスク容量
31日間	有効	1.0(0.7)コア	6.6GB	6.1GB

例2:PRIMEFLEXでの構成(ノード数:16、1ノード当たりの仮想マシン:31、仮想化管理ソフトウェア数:1)に基づいた場合

[総仮想マシン数] 16 * 31 = 496 台

[例2の構成で必要な追加リソース]

アノマリ検知の判定基準とする期間	CPU使用率予測設定	CPUコア数	メモリー容量	ディスク容量
7日間	無効	2.0(1.8)コア	5.6GB	18.0GB
31日間	無効	2.0(1.8)コア	12.5GB	18.0GB
7日間	有効	2.0コア	6.2GB	18.2GB
31日間	有効	2.0コア	13.1GB	18.2GB

例3:Red Hat Enterprise Linuxサーバー構成(ノード数:200)に基づいた場合

[例3の構成で必要な追加リソース]

アノマリ検知の判定基準とする期間	CPU使用率予測設定	CPUコア数	メモリー容量	ディスク容量
7日間	- [注]	1.0(0.8)コア	0.2GB	36.0GB
31日間	- [注]	1.0(0.8)コア	0.2GB	160.0GB

[注]:Red Hat Enterprise Linuxサーバー構成で必要なリソースは、CPU使用率予測設定によって変動しません。

注意

- お使いの環境に応じてISM-VAが動作するハイパーバイザーにリソースの追加を実施してください。リソースの追加が実施されない場合、GUIの操作に影響する場合があります。
- アノマリ検知を開始する最大ノード数は、以下のとおりです。
  - VMware ESXiホスト:最大100ノード(100ノード超過時はエラーとなります。)
  - Red Hat Enterprise Linuxサーバー:最大1000ノード

2.3.6.2 アノマリ検知機能の開始/停止

アノマリ検知機能の開始/停止は、ノード単位で行います。アノマリ検知機能を開始すると情報収集と分析が行われます。

アノマリ検知開始/停止の手順

アノマリ検知機能の開始/停止は、「ノードリスト」画面から対象ノードを選択し、[アクション]ボタンから操作します。また、ノードの詳細画面の[アノマリ検知]タブからも操作できます。

詳細は、『操作手順書』の「4.11.3 アノマリ検知機能を開始する」、「4.11.7 アノマリ検知機能を停止する」を参照してください。

アノマリ検知機能の開始時には、「アノマリ検知開始」画面で新しい学習データを作成するか以前の学習データをそのまま使用するかを選択できます。また、アノマリ検知の判定基準とする期間を選択できます。

注意

アノマリ検知機能を開始済のノードに対して以下の操作を行った場合、アノマリ検知機能は停止します。

- ISMのGUIからOS情報を削除した場合
- 仮想化管理ソフトウェアの登録を削除した場合
- 仮想化管理ソフトウェアの管理から外された場合
- メンテナンスモードに設定した場合

2.3.6.3 CPU使用率予測設定の有効／無効

CPU使用率予測の有効／無効の設定は、VMware ESXiホストのアノマリ検知を開始しているすべてのノードに適用されます。CPU使用率予測を有効に設定すると、予測データの蓄積を開始します。有効に設定してから3週間経過すると予測を開始します。
アノマリを検知し、CPU使用率が高使用率となる場合には、[アノマリ検知]タブの「解決方法」に予測される日時と値を表示します。

CPU使用率予測設定の有効／無効は、「ノードリスト」画面の[アクション]ボタンから操作します。

詳細は、『操作手順書』の「4.11.2 CPU使用率予測設定を有効にする」、「4.11.8 CPU使用率予測設定を無効にする」を参照してください。

注意

CPU使用率予測設定を無効にした場合、作成済の予測用データが削除されます。

2.3.6.4 アノマリ検知状態

各ノードに対して実施しているアノマリ検知の状態は、以下のいずれかになります。

表2.7 アノマリ検知状態

状態	説明
停止	アノマリ検知機能を開始していない状態（初期状態）
情報収集中(XX%)	アノマリ検知機能を開始し、学習データ作成に必要な情報を収集している状態 この状態ではアノマリの検知をしません。 アノマリ検知機能を初めて開始したノード、または情報収集データ初期化を指定して開始した場合、この状態になります。
情報収集中(学習データ作成中)	分析に必要な学習データを作成している状態 継続して学習データ作成に必要な情報を収集 この状態ではアノマリの検知をしません。 アノマリ検知の判定基準とする期間を切り替えた場合、この状態になります。
動作中(正常)	分析の結果、普段どおりのふるまいと判定されている状態（アノマリ検知の分析中の状態） 継続して学習データ作成に必要な情報を収集
動作中(アノマリ発生中)	分析の結果、普段と異なるふるまいを検知している状態（アノマリ検知の分析中の状態） 継続して学習データ作成に必要な情報を収集
エラー	なんらかの異常が発生しアノマリ検知機能が動作できない状態
-	アノマリ検知機能の対象外ノード（サーバー以外）

アノマリ検知状態が「エラー」の場合は、[アノマリ検知]タブの「アノマリ検知状態」にエラーメッセージが出力されます。メッセージ内容に従い対応してください。

表2.8 エラーメッセージ

メッセージ	対応
仮想化管理ソフトウェア(＜IPアドレス[注1]＞)でエラーを検出しました。仮想化管理ソフトウェアのログを確認してください。	vCenterのログを確認し対処してください。
仮想化管理ソフトウェア(＜IPアドレス[注1]＞)にログイン失敗しました。ISMの「仮想化管理ソフトウェアテスト」でテストを実行してください。	vCenterと接続できることを確認してください。
情報取得に失敗しました。vCenterでノード(OSのIPアドレス=＜IPアドレス＞)が正常に起動しているかを確認してください。	ノードがパワーオン状態であることを確認してください。また、ISMに登録したOSのIPアドレスが正しいことを確認してください。[注2]
VMware vCenter Server ＜バージョン＞ はアノマリ検知機能をサポートしていません。	対象外のvCenterバージョンです。「2.3.6.1 動作要件」を確認し、対応するバージョンでご利用ください。
VMware ESXi ＜バージョン＞ はアノマリ検知機能をサポートしていません。	対象外のESXiバージョンです。「2.3.6.1 動作要件」を確認し、対応するバージョンでご利用ください。
VMware ESXiのOSの版数を取得できませんでした。OS情報編集でOSバージョンを指定してください。	ESXiのバージョンが取得できませんでした。OS情報編集画面のOSバージョンで「Auto」以外を選択してください。
Red Hat Enterprise Linux ＜バージョン＞ はアノマリ検知機能をサポートしていません。	対象外のRed Hat Enterprise Linuxバージョンです。「2.3.6.1 動作要件」を確認し、対応するバージョンでご利用ください。
Red Hat Enterprise Linux ＜バージョン＞ の情報取得に失敗しました。ノード(＜OSのIPアドレス＞)が正常に起動しているかを確認してください。	ノードがパワーオン状態であることを確認してください。また、ISMに登録したOSのIPアドレスが正しいことを確認してください。
監視対象にアノマリ検知で必要なパッケージがインストールされていません(IPアドレス=＜OSのIPアドレス＞)。監視対象OSに不足しているパッケージをインストールしてください。	「B.1.3 監視対象OS、仮想化管理ソフトウェア設定時の留意事項」を確認し、監視対象OSにパッケージをインストールしてください。
ノード(＜OSのIPアドレス＞)にログイン失敗しました。アカウント名、パスワードのいずれかが不正です。ノードのOS設定を確認してください。	OS設定に登録したアカウント名、パスワードが正しいことを確認してください。

[注1]:仮想化管理ソフトウェアのIPアドレス

[注2]:ノードがvCenterの管理から外れた場合、ISMの仮想化管理ソフトウェア情報が更新されるまで本メッセージが出力されます。この場合は、アノマリ検知機能を停止してください。

2.3.6.5 アノマリ検知情報表示

アノマリ検知の情報は「ノードリスト」画面、ノードの詳細画面の[プロパティ]タブや[アノマリ検知]タブで確認します。

「ノードリスト」画面の表示

ノードリスト画面に「アノマリ検知状態」のカラムを表示できます。

初期状態では、「アノマリ検知状態」のカラムは表示されていません。表示するには、[カラム表示]で「基本情報」を選択し、右側にある[(カラム選択)]ボタンから [アノマリ検知状態]を追加してください。

アノマリ検知状態については、「2.3.6.4 アノマリ検知状態」を参照してください。

図2.6「ノードリスト」画面でのアノマリ検知状態の表示

[プロパティ]タブの表示

[アノマリ検知状態] で現在のアノマリ検知状態を表示します。また、[アノマリ検知ログ] で通知されたイベントの数を表示します。イベントの件数を選択することで対象ノードのアノマリ検知イベントを表示できます。

アノマリ検知状態については、「2.3.6.4 アノマリ検知状態」を参照してください。

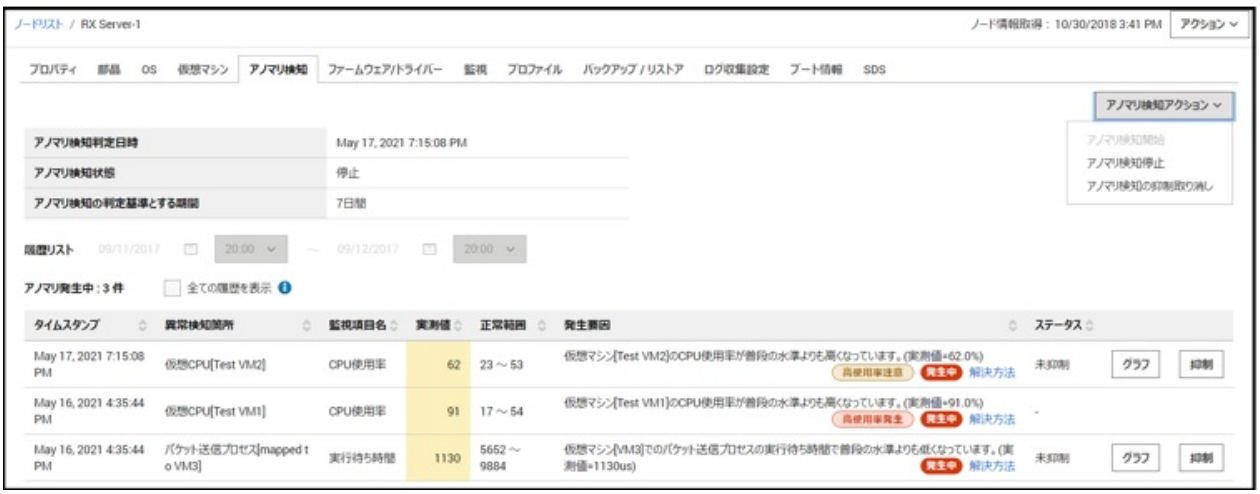
図2.7 [プロパティ] タブの表示

[アノマリ検知]タブの表示

[アノマリ検知]タブでは、以下の項目を表示します。

- アノマリ検知判定日時／アノマリ検知状態
- 履歴リスト

図2.8 アノマリ検知情報表示の画面



アノマリ検知判定日時／アノマリ検知状態

アノマリ検知を判定(アノマリ分析)した最新日時とその時点のアノマリ検知状態を表示します。アノマリ検知状態がエラーの場合は、エラーメッセージを合わせて表示します。

履歴リスト

過去のアノマリ検知の発生、回復の履歴を表示します。履歴の保持期間は、3か月分です。

画面を表示した時に現時点において回復していないアノマリ検知の履歴のみが表示されます。[全ての履歴を表示]チェックボックスにチェックを付け、年月日と時刻を設定することで、任意の期間の履歴を表示できます。

図2.9 任意期間の履歴を表示した場合

一度にリストに表示可能な件数は1000件です。1000件を超える場合は指定する期間を短縮してください。

表2.9 履歴リストの項目

項目	説明
タイムスタンプ	アノマリ検知／回復を検出した日時
異常検知箇所	アノマリ検知／回復した監視対象
監視項目名	アノマリ検知／回復した監視項目名
実測値	タイムスタンプの日時の監視項目の実測データ 正常範囲から外れている場合は黄色で網掛けします。
正常範囲	アノマリ検知の判定に使用した監視項目の実測データの正常範囲
発生要因	アノマリ検知／回復と判断した要因 「解決方法」を選択することで、解決方法を表示します。また、CPU使用率が高使用率となる場合、「解決方法」に予測される日時と値を表示します。
ステータス	アノマリ検知の抑制状態 「未抑制」:アノマリ検知が抑制されていない状態です。 「抑制中」:アノマリ検知が抑制中である状態です。 「-」:抑制不要、または抑制不可である状態です
[グラフ]ボタン [注]	該当のアノマリを検知した測定グラフを表示します。
[抑制]ボタン [注]	該当のアノマリを検知しないように正常範囲を再設定します。これによりアノマリ検知のイベント通知を抑えられます。 [ステータス]の表示が「抑制中」／「-」の場合は、本ボタンは無効です。

[注]:VMware ESXiホストのみ対応しています。

以下の履歴(イベント)については、ボタンが表示されません。

- アノマリからの回復
- 検知から1か月が経過したアノマリ

2.3.6.6 アノマリ検知イベント

アノマリ検知機能の開始／停止およびアノマリを検知、回復したときにイベントを通知します。

発生したイベントは「アノマリ検知ログ」として保持しており、ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択して、「イベントリスト」画面を表示し[アノマリ検知ログ]タブを選択することで確認します。

表2.10 イベントの種類

イベントの種類	内容	メッセージID	アラーム通知可否
アノマリ検知開始	アノマリ検知機能を開始	10038200	×
アノマリ検知停止	アノマリ検知機能を停止	10038201	×
CPU使用率予測が有効	CPU使用率予測が有効	10038202	×
CPU使用率予測が無効	CPU使用率予測が無効	10038203	×
アノマリ検知抑制	アノマリ検知の抑制	10038204	×
アノマリ検知抑制の取り消し	アノマリ検知の抑制の取り消し	10038205	×
アノマリ検知結果	アノマリ状態を検知、アノマリ状態から回復	10038100～10038199 [注1]	○
アノマリ検知イベント	アノマリ検知機能で発生するイベント情報 例:学習データを作成しました。	10038500～10038599 [注2]	×

[注1]:監視項目ごとに異なるメッセージIDとなります。アクション設定とアラーム設定により外部にアラームとして通知できます。アクション設定については「2.3.3 アクション設定」、アラーム設定については「2.3.4 アラーム設定」を参照してください。

[注2]:イベントごとに異なるメッセージIDとなります。

表2.11 表示項目

項目名	説明
重大度	「Info」固定
時間	イベントを通知した時間
種類	イベントの種類
メッセージID	イベントのメッセージID
ノード名	イベントが発生したノード名 ノード名を選択することで、対象ノードのアノマリ検知情報が表示できます。
操作者	アノマリ検知機能の開始、停止を実行したユーザー ユーザー操作によらないイベントの場合は「-」と表示されます。
説明	イベントの内容 「解決方法」を選択することで、解決方法を表示できます。アノマリ検知情報の保持期間を経過後は、その旨のメッセージが表示され解決方法は表示されません。

2.3.6.7 解決方法

アノマリ検知イベントまたはアノマリ検知情報表示の[履歴]から「解決方法」を選択することで、発生要因とその要因を解決する方法について例示します。内容を参考に対応について検討してください。

解決方法の実施によりアノマリ検知状態が「正常」となることを確認してください。

ポイント

アノマリの発生要因とvCenterのイベントログの情報から、アノマリを引き起こした原因と発生箇所を推定し解決方法を絞り込みます。

注意

ハイパーバイザーや仮想化管理ソフトウェアの版数により解決方法に記載された機能の名称や手順が異なることがあります。この場合は、それぞれのマニュアルを参照し読み替えてください。

2.3.6.8 アノマリ検知の抑制

アノマリ検知は学習データと運用状態によっては、通常の運用に対してもアノマリと検知して通知する場合があります。

アノマリ検知の抑制は、アノマリ検知の判定基準となる正常範囲を広げることによって、通常の運用に対してはアノマリとして検知しないようにイベントの発生を抑えることができます。

注意

アノマリ検知の抑制はVMware ESXiホストのみ対応しています。

アノマリ検知の確認

ノードの詳細画面の[アノマリ検知]タブに表示される各アノマリの[グラフ]ボタンを選択して、アノマリ検知時の測定値をグラフで確認できます。

グラフでは、アノマリ検知時を中心に前後90分の以下のデータが表示され、アノマリの状態を確認できます。

なお、アノマリ検知グラフで表示する実測値と、vCenterのパフォーマンスチャートで表示されるグラフのデータは一致しないことがあります。

- :抑制後正常範囲上限値
- :抑制後正常範囲下限値
- :正常範囲上限値
- :正常範囲下限値
- :実測値
- :アノマリ検知判定箇所

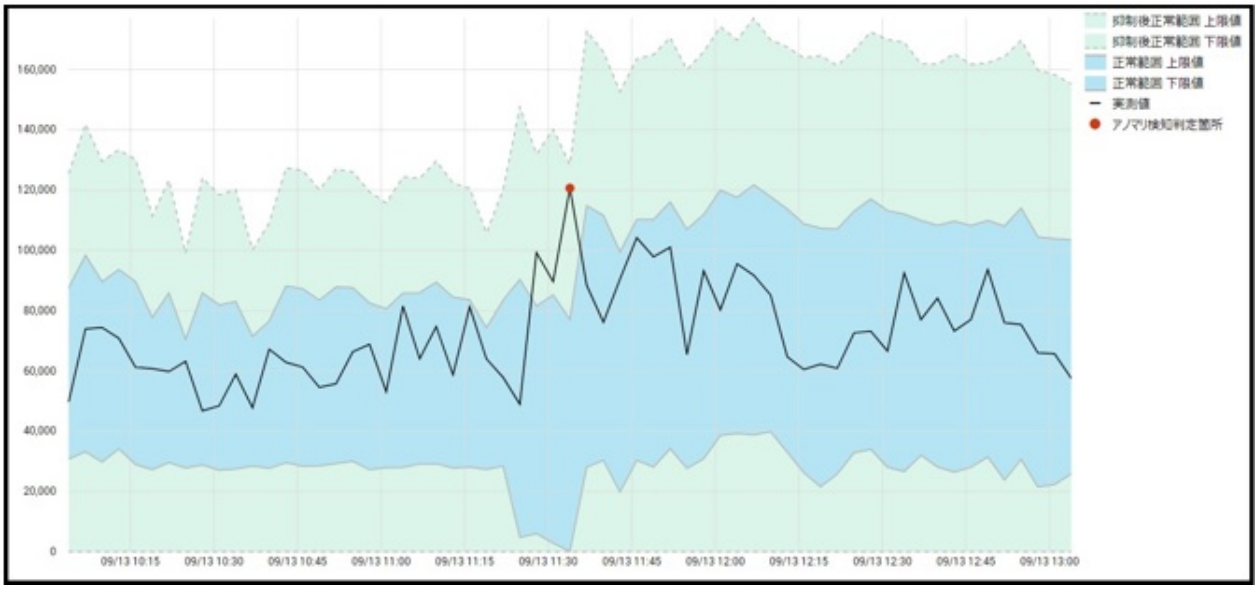
アノマリ検知の抑制が効果的であるかの判断基準

グラフ表示でアノマリ検知時の測定値を確認します。グラフに表示される「アノマリ検知判定箇所(赤丸)」が抑制後正常範囲(上限値と下限値の緑色範囲)の内側／外側にあるかで判断します。なお、抑制後正常範囲の上限値および下限値は、任意に設定できません。

アノマリ検知の抑制が効果があると判断できる場合

「アノマリ検知判定箇所(赤丸)」が抑制後正常範囲(上下限値の緑色範囲)の内側にある場合(下図)は、アノマリ検知の抑制は有効に動作します。

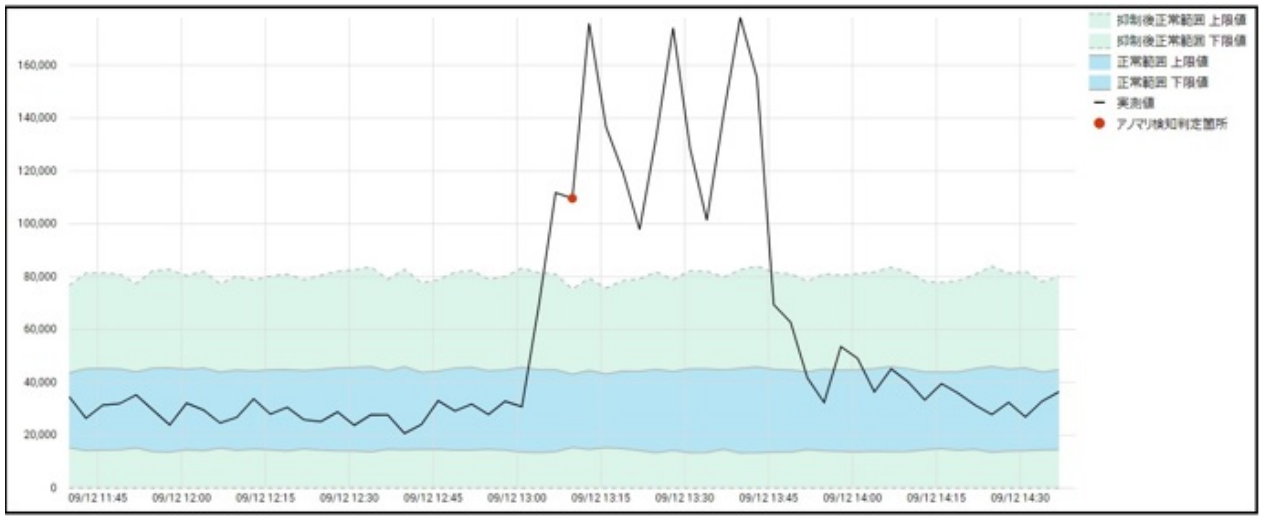
図2.10 アノマリ検知の抑制が有効であると判断できる場合



アノマリ検知の抑制が効果がないと判断できる場合

「アノマリ検知判定箇所(赤丸)」が抑制後正常範囲(上下限値の緑色範囲)の外側にある場合(下図)は、アノマリ検知を抑制しても有効に動作しません。抑制後の正常範囲でアノマリを判定するため、抑制後も常時監視で同様の測定結果が得られた場合は、アノマリ検知が出力されます。

図2.11 アノマリ検知の抑制が有効ではないと判断できる場合



ポイント

アノマリ検知対象機器を確認してください。アノマリ検知結果の妥当性が疑われる場合は、アノマリ検知機能を停止し学習データを再作成してください。

アノマリ検知の抑制

アノマリ検知の出力を抑制したい場合にアノマリ検知の[抑制]ボタンを選択します。抑制以降は常時監視で同様の測定結果に対して正常範囲内であると学習します。これにより、イベントの発生を抑制できます。

監視対象ごとにアノマリを抑制します。

アノマリ検知対象	
ノード	メモリー
ストレージ	ストレージ
ネットワークアダプター	物理NIC パケット受信スレッド パケット送信スレッド 仮想スイッチポート(送信ドロップ数)
仮想マシン	仮想マシン 仮想スイッチポート(受信ドロップ数)

例:仮想マシンが2つある場合、仮想マシン1のCPU使用率を抑制しても、仮想マシン2のCPU使用率は抑制されません。

アノマリ検知の抑制の取り消し

アノマリ検知の抑制を取り消すことで、抑制したアノマリ検知を抑制しない状態に戻すことができます。すべての監視項目について抑制を取り消します。

アノマリの発生状況の確認については、『操作手順書』の「4.11.6.1 アノマリの発生状況を確認する」を参照してください。

アノマリ検知の抑制方法については、『操作手順書』の「4.11.6.2 アノマリの検知を抑制する」を参照してください。

アノマリ検知の抑制の取り消しについては、『操作手順書』の「4.11.6.3 アノマリ検知に対する抑制を取り消す」を参照してください。

2.3.7 PRIMERGYのWebインターフェイスとの連携

ISMのGUIから下記の画面を表示できます。

- iRMCのWebインターフェイス画面
- AVR画面：Advanced Video Redirection（ビデオリダイレクション）

またiRMCのシステム情報やオペレーティングシステム情報を収集し、「資産管理情報」として「ノードリスト」画面およびノード詳細画面に表示することができます。

Webインターフェイスとビデオリダイレクションの表示内容や操作方法などの詳細については、以下のドキュメントを参照してください。

『ServerView Suite iRMC Sx Web インターフェース』（Sxには、S4以降の版数が入ります。）

iRMCのWebインターフェイスへのログインおよびAVRのアクセス環境は、ノード登録時の「通信方法」に指定したiRMCアカウントを使用します。

iRMC Webインターフェイスの表示は従来からある機能で、ノード詳細画面内「Web IF/URL」にiRMCのIPアドレスを登録しておきURLをクリックすることで表示できます。ただし、従来のこの操作は画面表示の都度、ログイン操作が必要です。
従来の操作と区別するため、新しい操作を「iRMCログイン」と呼びます。

2.3.7.1 iRMCログインによるWebインターフェイス画面表示

ISMのGUIからiRMCのWebインターフェイス画面をログイン操作せずに直接表示できます。
iRMC Webインターフェイス画面から、PRIMERGYの詳細情報（システム情報、OS情報、センサ情報など）を参照できます。

この機能で表示するWebインターフェイス画面は、情報参照権限で開きます。そのため設定操作は行えません。

iRMCログインによるWebインターフェイス画面表示の操作方法については、『操作手順書』の「3.8 ISMからiRMCに直接ログインする」を参照してください。

中継ルート設定について

iRMCログインは、管理端末から直接iRMCへアクセスできることが前提です。管理端末からiRMCへのアクセスがファイアウォールで制限されているネットワーク構成では、中継ルートを経由してiRMCログインができます。
つまり、中継ルートは、ISM内に中継用の経路を構築するための通信用ルートです。

以下のような特徴があります。

- 中継ルートは管理端末に対応付けて設定します。

  中継ルートを経由したiRMCログインを行う管理端末のIPアドレスを設定します。
  中継ルートの設定は、どの管理端末からでも行えます。

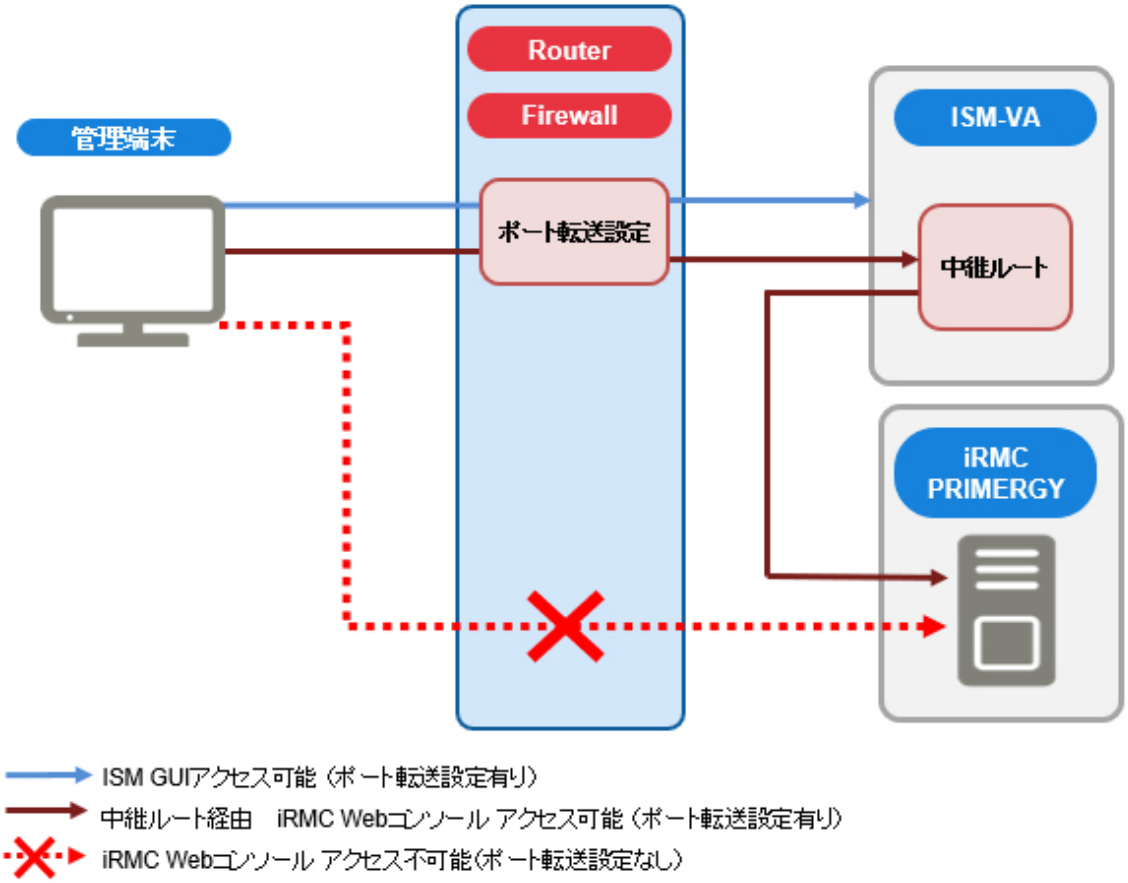
- 中継ルートは、ISMに3つまで設定できます。

  3つの中継ルートをそれぞれ別の管理端末に割り当てることも、すべての中継ルートを1台の管理端末に割り当てることもできます。

- 1つの中継ルートを経由したiRMC接続は、同時に1台です。

中継ルートを設定する管理端末は、ISM-VAが発行するクライアント証明書を管理端末のブラウザーにインストールする必要があります。
クライアント証明書の作成については、「4.28 中継ルート用クライアント証明書の作成」を参照してください。

図2.12 中継ルート設定



2.3.7.2 PRIMERGYのAVR（ビデオリダイレクション）画面表示

ISMのGUIからAVR画面をログイン操作せずに直接起動できます。

AVR画面表示の操作方法については、『操作手順書』の「6.16 ISMからiRMCのAVR画面を直接表示する」を参照してください。

AVR画面表示に関しては、中継ルートの設定をサポートしていません。

2.3.7.3 iRMCの資産管理情報の表示

iRMCのシステム情報やオペレーティングシステム情報を、ISM GUIの「ノードリスト」画面およびノード詳細画面に資産管理情報として表示します。

資産管理情報は「ノードリスト」画面の[カラム表示]で[資産管理情報]を選択するか、ノード詳細画面の[資産管理情報]タブを選択すると表示されます。

表示される内容は以下のとおりです。

項目	説明
ノード名	ノードの名前を表示します。

項目	説明
システム情報	以下のiRMCのシステム情報を表示します。 ・ モデル名 ・ シャーシタイプ ・ シリアル番号 ・ 部品番号 ・ 資産タグ ・ システムGUID ・ BIOSバージョン
オペレーティングシステム(OS)情報	以下のiRMCのオペレーティングシステム(OS)情報を表示します。 ・ ホスト名 ・ ホストIPアドレス ・ システム情報 ・ システムの場所 ・ システムの管理者 ・ OSの種類 ・ OSバージョン ・ OS稼働情報 ・ 管理ソフトウェア
タグ	ノードのタグを表示します。 「基本情報」画面のタグと同一です。

資産管理情報の表示が可能な機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

2.4 プロファイル管理機能

プロファイル管理機能は主にシステムの導入、構築で利用する機能です。

管理対象ノードとするサーバー、ネットワークスイッチおよびストレージの設定ができます。

プロファイル管理機能における、ノード種別ごとの対象ノード、およびその機能グループを以下に示します。

表2.12 プロファイル管理機能の対象ノードおよび機能グループ

ノード種別	対象ノード（例）	機能グループ
サーバー	PRIMERGY RX PRIMERGY TX PRIMERGY BX PRIMERGY CX	・ BIOS設定 ・ iRMC設定 ・ iRMC（ユーザー）設定 ・ OS設定 ・ 仮想IO設定 ・ RAID設定
	PRIMEQUEST 2000 シリーズ（Partition）	・ MMB設定 ・ OS設定
	PRIMEQUEST 2000B	・ MMB設定

ノード種別	対象ノード(例)	機能グループ
		・ OS設定
	PRIMEQUEST 3000シリーズ(Partition)	・ MMB設定 ・ OS設定 ・ 仮想IO設定(物理パーティションのみ)
	PRIMEQUEST 3000B	・ BIOS設定 ・ iRMC設定 ・ OS設定
	PRIMEQUEST 4000シリーズ(Partition)	・ BIOS設定 ・ iRMC設定 ・ iRMC(ユーザー)設定 ・ OS設定 ・ 仮想IO設定
ネットワークスイッチ	SR-X	・ 管理者パスワード設定 ・ SNMP、NTP、STP設定
	VDX イーサネットスイッチ(10GBASE-T 48+6) イーサネットスイッチ(10GBASE 48+6)	・ 管理者パスワード設定 ・ SNMP、NTP設定
	CFX	・ 管理者パスワード、AAA設定 ・ SNMP、Interface、NTP設定
ストレージ	ETERNUS DX	・ RAIDグループ／ボリューム作成 ・ グローバルホットスペア作成 ・ Host Affinity設定
	ETERNUS NR(Ontap) ETERNUS AX(Ontap) ETERNUS HX(Ontap) ETERNUS AC(Ontap)	・ SNMP、NTP設定

ここでは、以下について説明します。

- 2.4.1 プロファイルの利用方法
- 2.4.2 プロファイルとポリシー
- 2.4.3 RAID設定
- 2.4.4 OSインストールの設定
- 2.4.5 仮想IO設定
- 2.4.6 プール管理機能
- 2.4.7 ブート情報の確認
- 2.4.8 iRMC(ユーザー)設定

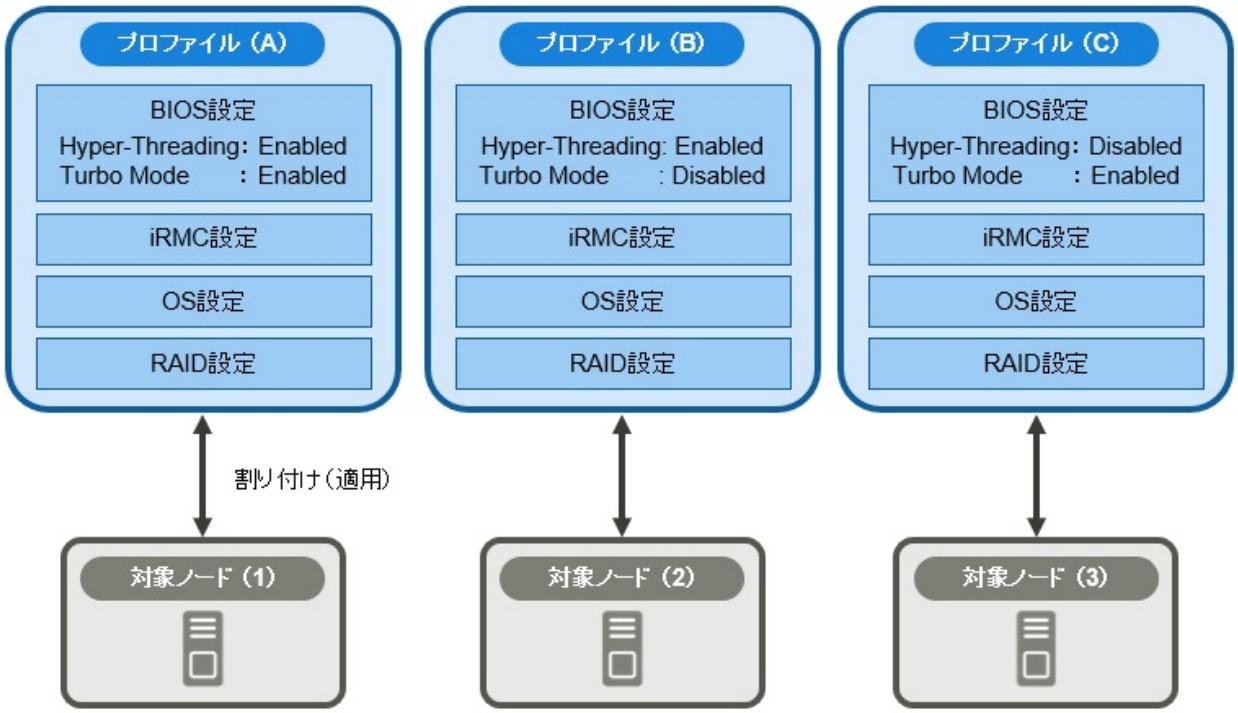
2.4.1 プロファイルの利用方法

プロファイル管理機能でノード設定を行う際は、事前作業としてノードのハードウェア設定やOSインストール時設定を「プロファイル」と呼ぶ設定の集合体に記述しておきます。

そのプロファイルをノードに割り付ける（適用する）操作を行うことで、設定がノードに反映されます。

プロファイルは管理対象のノードと1対1で適用されます。プロファイルを使って管理するノード1台につき1つのプロファイルが必要です。

図2.13 プロファイルと管理対象のノードの関係



注意

OS関連の設定が記述されたプロファイルをノードに適用すると、プロファイルの内容に従ってOSが新規にインストールされます。インストール済みの既存OSがある場合、設定が変更されるのではなく、既存OSおよびデータは消去されて新規インストールとなります。

図2.14「プロファイル作成」画面例（GUI）

2.4.2 プロファイルとポリシー

ポリシーは複数のプロファイル間で同一の設定内容となる部分を抜き出して、一括設定するための仕組みです。ポリシーはプロファイルと同様に設定を記述したファイルです。ただし、ポリシーを直接ノードに適用するのではなく、プロファイルがポリシーの内容を参照することで、間接的にノードに対して設定が行われます。1つのポリシーは複数のプロファイルから参照させることができます。

ノードから設定項目を取得することで、取得したモデルに限定したモデル毎プロファイル／ポリシーを作成できます。モデル毎プロファイル／ポリシーでは、より詳細なハードウェア設定を行えます。モデル毎プロファイル／ポリシーは、設定項目を取得した同一モデルに適用できます。

「プロファイル／ポリシー」と「モデル毎プロファイル／ポリシー」の違いは、以下のとおりです。

プロファイルの機能と必要な操作	プロファイル／ポリシー	モデル毎プロファイル／ポリシー
プロファイル適用範囲	PRIMERGY RXシリーズなど、同一シリーズに適用	指定された同一モデルに適用
プロファイル／ポリシーの作成	同一シリーズで共通の設定	モデル毎の詳細な設定
プロファイル作成前の操作	不要	プロファイルを作成するモデルのノード登録が必要
プロファイルのベリファイ	対応	対応
バックアップからプロファイル追加	対応	未対応
バックアップからポリシー追加	対応	未対応
監視ポリシー	対応	未対応

ポリシーは、従来のポリシー（一括設定のためのポリシー：BIOS、iRMC、MMB、OS、RAID）と監視用のポリシーがあります。

ノードの監視に必要な設定が定義された監視用のポリシー（監視ポリシー）を対象サーバーの種別に依存することなく作成できます。

監視ポリシーは、従来のポリシーと同様に、複数のプロファイルから参照することができます。また、従来のポリシーから監視ポリシーを参照することもできます。

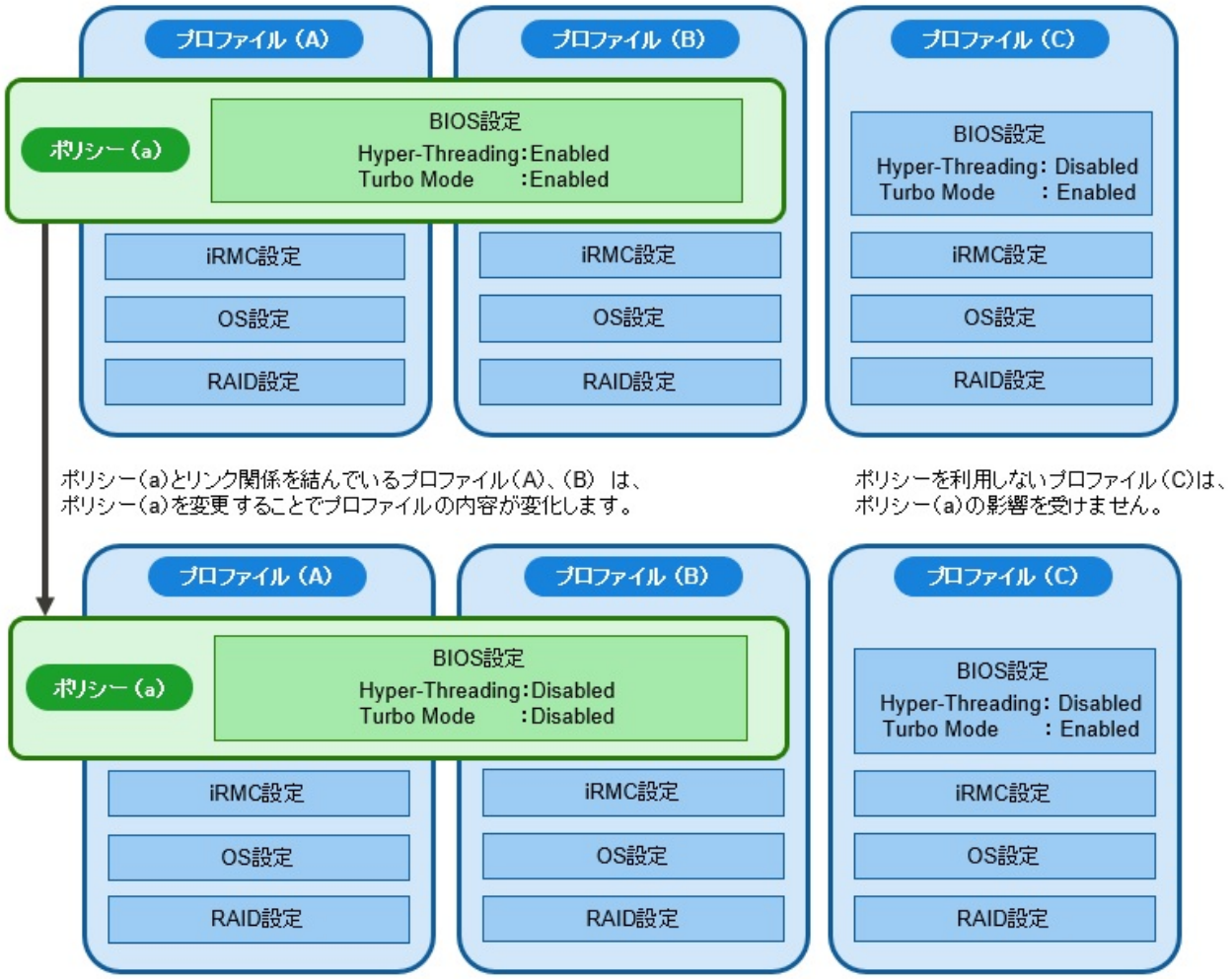
プロファイルが監視ポリシーを参照している場合、監視ポリシーと同じ設定項目を持つ従来のポリシーを参照することはできません。この場合、プロファイルから参照したい従来のポリシーと監視ポリシーを関連付け、プロファイルから従来のポリシーを参照する必要があります。

プロファイルは、ノード1台につき1個必要です。例えば、多数のノードのハードウェア設定を同一内容で設定する場合は、ノード台数分の同一設定のプロファイルを用意する必要があります。最初に1個のプロファイルを作成したあとに、プロファイルの参照作成機能でノード台

数分のプロファイルを作成できます。ただし、この方法では、全ノードの設定を同一内容で変更したい場合などに、すべてのプロファイルに対して修正を繰り返す必要があります。

このような場合は、事前にポリシー機能を利用してプロファイルを作成しておくことで、簡単に設定の一括変更ができます。

図2.15 プロファイルとポリシーの関係



プロファイル、従来のポリシー、監視ポリシーの関係

図2.16 プロファイルと従来のポリシーの関係

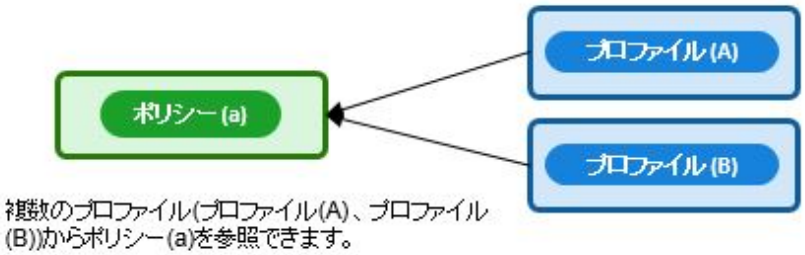


図2.17 プロファイルと監視ポリシーの関係

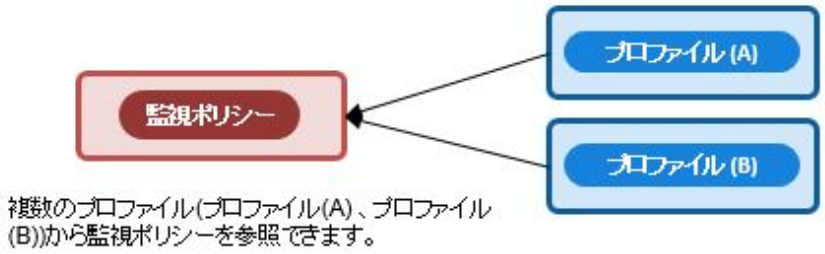
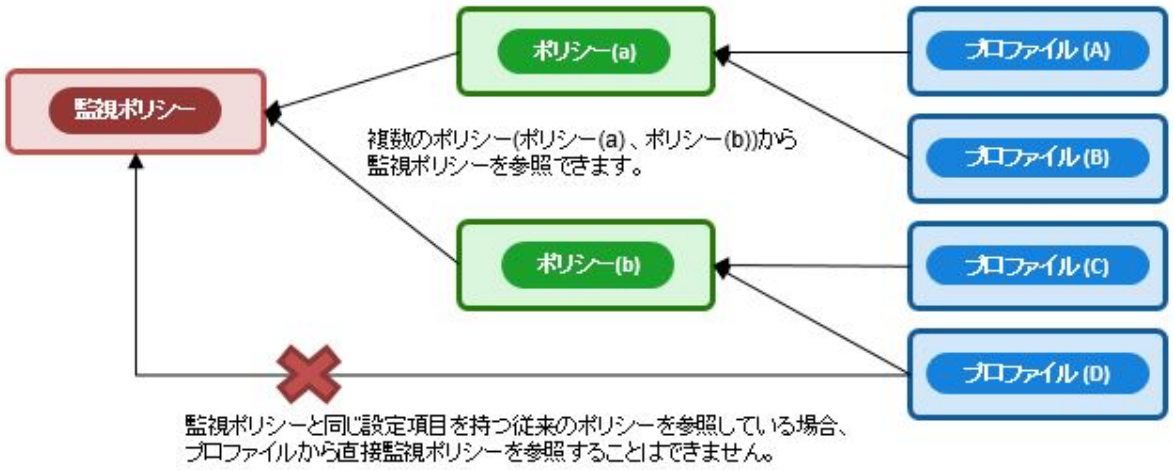


図2.18 プロファイル、従来のポリシー、監視ポリシーの関係



注意

- プロファイルとポリシーは、対象ノードでサポートされる一般的な設定項目を含みます。対象ノードのモデル種別やファームウェアバージョンによってはサポートされない設定項目も存在します。適用するノードでサポートされない項目は、プロファイルおよびポリシーでは設定しないでください。
- OSインストールを実行する場合、対象ノードおよび使用するServerView Suite DVDでサポートされていないOSはインストールできません。

ポイント

- ポリシーを利用する場合は、プロファイル作成前にポリシーを作成してください。
- ポリシーは、サーバーに対するOS設定、BIOS設定、iRMC設定、iRMC(ユーザー)設定、RAID設定、またはMMB設定に利用できます。
- モデル毎プロファイル／ポリシーは、サーバーに対するBIOS設定、iRMC設定、iRMC(ユーザー)設定に利用できます。モデル毎プロファイル／ポリシーは、従来のサーバー種別共通のBIOS設定やiRMC設定、iRMC(ユーザー)設定とは同時に利用できません。
- 監視ポリシーとプロファイルとの設定項目の関連については、『プロファイル管理機能 プロファイル設定項目集』の「8.1 監視ポリシー」を参照してください。
- プロファイル、またはポリシーを作成するときに監視ポリシーを利用する場合、監視ポリシーの[監視ポリシー有効]にチェックを付けてください。

プロファイルグループとポリシーグループ

プロファイル、ポリシーは、グループ単位で管理できます。業務用途別や導入時期別などの任意のグループを作成してプロファイル、ポリシーを所属させることで、管理が容易になります。

プロファイルはプロファイルグループ、ポリシーはポリシーグループに所属させることができます。

2.4.2.1 ポリシーグループ／ポリシーの作成

ポリシーグループの作成

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ポリシー設定]を選択します。
3. 画面左側のツリー部からポリシーグループ作成先を選択します。[アクション]ボタンから[グループ追加]を選択します。

ポリシーの作成

詳細な手順については、『操作手順書』の「3.3.4 ポリシーを作成してプロファイルの作成を簡略化する」の「従来のポリシーの作成手順」を参照してください。

監視ポリシーの作成

詳細な手順については、『操作手順書』の「3.3.4 ポリシーを作成してプロファイルの作成を簡略化する」の「監視ポリシーの作成手順」を参照してください。

注意

- 監視ポリシーは、Administratorグループのユーザーのみ作成、編集できます。
- 監視ポリシーを適用したノードは、モデル毎プロファイルを適用することはできません。モデル毎プロファイルを使用するには、監視ポリシーを適用しないでください。

2.4.2.2 プロファイルグループ／プロファイルの作成

プロファイルグループの作成

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のツリー部からプロファイルグループ作成先を選択します。[アクション]ボタンから[グループ追加]を選択します。

プロファイルの作成

詳細な手順については、『操作手順書』の「3.3.1 プロファイルでBIOS／iRMC／iRMC（ユーザー）／MMB／仮想IO／RAIDを設定する」の手順1～5を参照してください。

2.4.2.3 プロファイルの適用

注意

対象ノードのWeb操作画面やSSHにログインした状態でプロファイル適用を行うと、プロファイル適用がエラーになる場合があります。

詳細な手順については、『操作手順書』の「3.3.1 プロファイルでBIOS／iRMC／iRMC(ユーザー)／MMB／仮想IO／RAIDを設定する」の手順6～9を参照してください。

ポイント

プロファイルの内容によって、プロファイル適用完了までに長時間(例:1時間以上)必要な場合があります。プロファイル適用状況は「タスク」画面で確認できます。詳細は、「2.14.4 タスク管理」を参照してください。

2.4.2.4 プロファイルの編集と再適用

ノードに適用したプロファイルを再編集し、再度ノードに適用することにより、ノードの設定を変更できます。

プロファイルがノードに適用された状態でプロファイルの中身を再編集できます。そのとき、プロファイルを再編集してもノードの設定は連動して変化しません。ISM管理上、プロファイルの内容とノードの設定との不一致という状態となります。

任意のタイミングで再編集済みのプロファイルをノードに対して再適用してください。再適用が完了するとノードの設定が変更され、再びプロファイルとノードの設定が一致した正常状態になります。

プロファイルの再適用

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。
3. 編集対象のプロファイルを選択します。
4. [アクション]ボタンから[編集]を選択し、プロファイルを編集します。
5. プロファイル適用の対象ノードがサーバーの場合は、プロファイル適用前にサーバーの電源をオフにします。

   サーバー以外の場合は、電源をオンにします。
6. 適用対象のプロファイルを選択します。
7. [アクション]ボタンから[プロファイル適用/再適用]を選択します。

   「プロファイル適用」画面が表示されます。
8. 画面に従い、設定項目を入力します。

   設定項目の入力は、ISMのオンラインヘルプを参照してください。

適用後のプロファイルのステータス確認

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。

2. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。

3. ノード設定とプロファイルの一致を確認します。

   編集していないプロファイルは、[ステータス]に[適用済]と表示されます。

   BIOS／iRMC／仮想IO／RAID設定を編集したプロファイルは、[ステータス]に[要再適用]と表示されます。

   OS設定のみを編集したプロファイルは、[ステータス]に[適用済（差分あり）]と表示されます。

注意

[ステータス]が[適用済（差分あり）]の場合、通常の再適用ができません。

この場合、「プロファイル適用」画面で[高度な設定を有効にする]にチェックを付け、「プロファイルをノードに適用せず、ISM上で適用したことにする」をご使用ください。

2.4.2.5 プロファイルの適用解除と削除

以下の場合は事前にプロファイルの適用を解除してください。

- 適用済みのプロファイルを削除する場合
- プロファイル適用済みのノードをISMから削除する場合
- プロファイル適用済みのノードをノードグループから外す場合、ノードグループを変更する場合

  ノードグループについては、「2.14.1 ユーザー管理機能」を参照してください。

ポイント

装置自体をリプレースする場合には、プロファイルの適用解除は必要です。詳細については、「5.3 保守部品交換時の作業」を参照してください。
対象の装置のiRMCをリセットする場合は、プロファイルの適用解除は不要です。

プロファイルの適用解除

プロファイルの適用解除により、プロファイルで設定される設定値のうち仮想IO設定が適用前の状態に戻ります。仮想IO設定以外の設定は変化しません。また、定期的なプロファイルのベリファイは実施されなくなります。

1. 仮想IO設定を含むプロファイルの適用を解除する場合は、サーバーの電源をオフにします。
2. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
3. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。

4. 適用解除対象のプロファイルを選択します。
5. [アクション]ボタンから[プロファイル解除]を選択します。

プロファイルの削除

ISM上のプロファイルの定義情報が削除されます。ノード側には影響しません。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。

2. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。

3. 削除対象のプロファイルを選択します。

4. [アクション]ボタンから[削除]を選択します。

   ステータスが[未適用]のプロファイルのみ削除できます。

2.4.2.6 プロファイルのエクスポート／インポート

別の管理サーバーに導入されたISMにプロファイルを流用したい場合や、適用したプロファイルをISMから取り出して保管しておきたい場合などは、プロファイルをJSON形式で記述されたテキストファイルとしてエクスポート／インポートできます。

ポイント

ポリシーについても同様にエクスポート／インポートができます。

プロファイルのエクスポート

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。

3. エクスポート対象のプロファイルを選択します。
4. [アクション]ボタンから[エクスポート]を選択します。
5. パスワード暗号化キーを設定し（必須）、[エクスポート]ボタンでエクスポートを実行します。

プロファイルのインポート

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のツリー部からプロファイルの保存先を選択します。[アクション]ボタンから[インポート]を選択します。
3. [ファイル選択方式]でファイルの選択先を選択します。

   ― ローカル

   ローカルにあるプロファイルをインポートします。

   ― FTP

   ISM-VAのFTPサーバーからプロファイルをインポートします。

   あらかじめ、ISM-VAの「/＜ユーザーグループ名＞/ftp」のディレクトリー配下にプロファイルを転送しておく必要があります。

   FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。

4. [ファイル]でインポート対象のプロファイルを指定します。
5. [プロファイルタイプ]を選択します。
6. [プロファイルグループ名]を入力します。
7. [パスワード復号化キー]でエクスポート時に設定したパスワードの復号化キーを入力し（必須）、[インポート]ボタンでインポートを実行します。

ポイント

- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
- プロファイルにはパスワードなどのセキュリティ情報が含まれるため、エクスポートの際は、暗号化キーの指定が必須です。

2.4.2.7 プロファイルグループの編集／削除

プロファイルグループの編集

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のツリー部からプロファイルグループ編集先を選択して、右側の一覧からプロファイルグループを選択します。
3. [アクション]ボタンから[編集]を選択し、プロファイルグループを編集します。

プロファイルグループの削除

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のツリー部からプロファイルグループ削除先を選択して、右側の一覧からプロファイルグループを選択します。
3. [アクション]ボタンから[削除]を選択します。

2.4.2.8 ポリシーグループの編集／削除

ポリシーグループの編集

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ポリシー設定]を選択します。
3. 画面左側のツリー部からポリシーグループ編集先を選択して、右側の一覧からポリシーグループを選択します。
4. [アクション]ボタンから[編集]を選択し、ポリシーグループを編集します。

ポリシーグループの削除

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ポリシー設定]を選択します。
3. 画面左側のツリー部からポリシーグループ削除先を選択して、右側の一覧からポリシーグループを選択します。
4. [アクション]ボタンから[削除]を選択します。

2.4.2.9 プロファイル適用時の動作指定

プロファイルの適用／再適用時に[高度な設定を有効にする]にチェックを付けることで、プロファイル適用時の「適用モード」を指定できます。サーバーの場合は適用する範囲を機能グループ（BIOS設定、iRMC設定、iRMC（ユーザー）設定、MMB設定、OS設定、仮想IO設定、RAID設定）ごとに指定できます。

指定可能な「適用モード」は、以下のとおりです。

・「通常適用（新規、変更箇所のみ適用）」
デフォルトの適用モードです。[高度な設定を有効にする]を指定しない場合は、このモードになります。

・「変更がない箇所にも適用を行う」
ノードとプロファイル設定値の一致／不一致にかかわらずノードに対して設定を行います。
ただし「OS設定」「RAID設定」については設定を行いません。本モードはサーバーの電源状態に関わらず指定可能です。以下の点に注意してください。

　― 電源オンの状態でBIOS設定を含む指定をした場合、設定値は次回のサーバー再起動後に反映されます。

　― iRMC S4（バージョン9.xx以前）、もしくは、iRMC S6以降を搭載したサーバーでのみ本モードを使用できます。

・「電源オン状態でプロファイルを適用する」
サーバーに対する「適用モード」です。通常は対象ノードの電源をオフにした状態で適用を行いますが、対象ノードが電源オンの状態でプロファイル適用する際に指定します。以下の点に注意してください。

　― 設定値は次回のサーバー再起動後に反映されます。

　― iRMC S5搭載サーバーは、本モードを使用できません。

　― iRMC S4搭載サーバーでiRMCバージョンが9.xxF以降の場合は、本モードを使用できません。

・「プロファイルをノードに適用せず、ISM上で適用したことにする」
プロファイルの設定値とノード側の設定値が「不一致」のとき、ISM側でプロファイル上の設定値を変更し、プロファイル適用せず一致させるときこの指定を行います。プロファイルが編集されていないとこのモードは表示されません。

複数のノードを選択してプロファイル適用を行う場合、「適用モード」を一括変更用のプルダウンボックスで一括指定できます。また、機能グループに対応するチェックボックスにチェックを付けて一括指定することもできます。

2.4.2.10 プロファイルのベリファイ

プロファイル適用後、サーバーのBIOS／iRMC設定を直接変更した場合、プロファイルの内容とサーバーのBIOS／iRMC設定内容に差異が生じる可能性があります。プロファイルのベリファイを実行すると、プロファイルの内容とサーバーのBIOS／iRMC設定内容が一致しているかが検証され、差異がないか確認できます。ベリファイの実行はサーバーのみが対象です。

プロファイルのベリファイの実行状態、または実行結果がGUIの[ベリファイステータス]に表示されます。プロファイルの内容とサーバーのBIOS／iRMC設定内容に差異が生じている場合、イベントにその旨のメッセージが表示され、[ベリファイステータス]が[不一致]と表示されます。[ベリファイステータス]が[不一致]と表示されている場合、該当プロファイルで差異が生じている項目を確認し、サーバーの設定内容の変更が意図したものかを判断してください。プロファイルの内容とサーバーの設定内容に差異がないようにプロファイルの編集、プロファイルの再適用などを行い、[ベリファイステータス]を[一致]の状態にしてください。

プロファイルのベリファイは、以下の設定項目で利用できます。

サーバー	ベリファイ対象の機能グループ	ベリファイ対象外の機能グループ
PRIMERGY	・ BIOS設定 ・ iRMC設定 ・ iRMC（ユーザー）設定	・ OS設定 ・ 仮想IO設定 ・ RAID設定
PRIMEQUEST 3000B	・ BIOS設定 ・ iRMC設定	・ OS設定
PRIMEQUEST 4000	・ BIOS設定 ・ iRMC設定 ・ iRMC（ユーザー）設定	・ OS設定 ・ 仮想IO設定

プロファイルのベリファイは、以下のステータスのプロファイルに対して実行できます。

- 適用済
- 要再適用
- 適用済（差分あり）

本機能は、ISM-VA管理機能のプロファイルのベリファイ有効化／無効化設定コマンドを使用して、プロファイルのベリファイ機能（約24時間周期の定期的な自動実行、および任意のタイミングによる手動のプロファイルのベリファイ）を有効化、または無効化します。コマンドの詳細は、「4.24 プロファイルのベリファイ有効化／無効化設定」を参照してください。

無効化した場合、プロファイルのベリファイの対象となるプロファイルの[ベリファイステータス]が[-（ハイフン）]と表示されます。

有効化した場合、その直後はプロファイルのベリファイの対象となるプロファイルの[ベリファイステータス]が[ベリファイ失敗]と表示されます。定期的な自動実行、または任意のタイミングによる手動のプロファイルのベリファイを実行することで、適切な[ベリファイステータス]が設定されます。

ここでは、以下について説明します。

- 任意のタイミングによるプロファイルのベリファイの実行方法
- [ベリファイステータス]が[不一致]の場合に、差異が生じている項目の確認方法

任意のタイミングによるプロファイルのベリファイの実行方法

ISMは定期的（約24時間周期）にプロファイルのベリファイを自動実行します。また、ユーザーの任意のタイミングでプロファイルのベリファイを実行することもできます。

詳細な手順については、『操作手順書』の「3.3.5 適用済みのプロファイルとハードウェア設定を比較する」の「プロファイルのベリファイの実行方法」を参照してください。

[ベリファイステータス]が[不一致]の場合に、差異が生じている項目の確認方法

詳細な手順については、『操作手順書』の「3.3.5 適用済みのプロファイルとハードウェア設定を比較する」の「[ベリファイステータス]が[不一致]の場合に、差異が生じている項目の確認方法」を参照してください。

ポイント

- プロファイルのベリファイでBIOS設定を確認するには、BIOSパラメーターのバックアップファイルがサーバー上に保持されている必要があります。このため、プロファイル適用時にプロファイルのiRMC設定で[自動BIOSパラメーターバックアップ]を有効に指定してください。
- サーバーのiRMC設定で[自動BIOSパラメーターバックアップ]の項目を無効にしている場合や、項目が存在しないサーバーの場合、最新のBIOS設定でプロファイルのベリファイが実行されません。その場合、BIOSのハードウェア設定をバックアップしてから（「2.10.1 ハードウェア設定のバックアップ」参照）、プロファイルのベリファイを実行してください（「任意のタイミングによるプロファイルのベリファイの実行方法」参照）。サーバーのiRMC設定に[自動BIOSパラメーターバックアップ]の項目が存在するかの確認は、以下のマニュアルを参照してください。
  - 『ServerView Suite Remote Management iRMC S2/S3 - integrated Remote Management Controller』
  - 『ServerView Suite iRMC Sx Web インターフェース』（Sxには、S4以降の版数が入ります。）
- ノードがメンテナンスモードの場合、ISMによる定期的なプロファイルのベリファイは実行されません。この場合、プロファイルのベリファイは手動で実行してください。
- プロファイルのベリファイで対象外の設定項目があります。対象外の項目は、以下のとおりです。
  - iRMC設定[プロキシサーバー]-[パスワード]
  - iRMC設定[LDAP]-[認証LDAPパスワード]
  - iRMC設定[ユーザー管理]-[Adminパスワードの変更]
  - iRMC（ユーザー）設定[ユーザー追加・変更]-[ユーザー情報]-[パスワード]
  - iRMC（ユーザー）設定[ユーザー追加・変更]-[ユーザー情報]-[パスワード（確認）]
  - iRMC（ユーザー）設定[ユーザー追加・変更]-[ユーザー情報]-[説明]

- 「プロファイル適用」画面で以下の設定内容のプロファイルを適用した場合、[ベリファイステータス]は[ベリファイ失敗]と表示されます。手動でプロファイルのベリファイを実行してください。

  ー [適用モード]:[プロファイルをノードに適用せず、ISM上で適用したことにする]

    [適用モード]は、[高度な設定を有効にする]にチェックを付けた場合に選択できる項目です。

  ー 適用前の[ステータス]:[未適用]

注意

- iRMC設定でLDAPが有効で、ノードの詳細画面の[Web I/F URL]のプロトコルがHTTPのとき、iRMCのファームウェアバージョンによっては、プロファイルのベリファイがエラーとなることがあります。この場合、ノードを編集して[Web I/F URL]のプロトコルをHTTPSに設定してください。ノードの編集については、「2.2.3 データセンター／フロア／ラック／ノードの編集」を参照してください。
- 以下の場合サーバーの再起動を行う必要があります。

  ー 「変更がない箇所にも適用を行う」を選択しサーバーの電源がオンの状態で適用した場合

  ー 「電源オン状態でプロファイルを適用する」で適用した場合

  サーバーを再起動する前の状態では、以下の値が実際のサーバーの状態と異なるにも関わらず、[ベリファイステータス]が[一致]となる場合があります。この場合、iRMCのタスクマネージャ上に、実行中や保留中のタスクが残っている可能性があります。サーバーの再起動を行い、それらのタスクをすべて完了にしてください。その後、再度ベリファイの実行を行ってください。

  ー [ベリファイステータス]

  ー プロファイルの内容とサーバーのBIOS／iRMC設定内容の差異

- モデル毎プロファイルのBIOS設定のプロファイルを含む適用／再適用した場合、サーバーの再起動が必要となります。再起動前の状態では[ベリファイステータス]が[不一致]となります。不一致を解消するにはサーバーを再起動し、再度ベリファイの実行をしてください。

2.4.3 RAID設定

プロファイルでRAID構築を指定できます。
RAID構築の方法として、以下の2つの方法があります。ただし、指定できるのはどちらか一方です。「RAID設定」と「OS設定」を両方指定した場合、RAID構築は「RAID設定」にて実施されます。

- 「RAID設定」の中でRAIDを指定する方法
- 「OS設定」の中でRAIDを指定する方法

ここでは機能グループ「RAID設定」で指定する方法を説明します。

プロファイルの[RAID]タブで指定する方法です。RAIDの構築は、iRMCの処理の中で実施されます。
この指定方法では、あらかじめiRMCのGUI上でRAIDが構築されていない状態にする必要があります。

RAID構築に対する指定内容は、RAIDレベル、ディスク数、およびディスクグループ数です。ディスクグループ数はRAIDレベルがRAID1+0の場合に指定できます。

[RAID]タブでディスク数を手動で設定しない場合のRAID構築する際のディスク数は、以下のルールとなります。不足している場合はエラーとなります。余剰のディスクがある場合は使用されません。

RAIDレベル	ディスク数
RAID0	1
RAID1	2
RAID1+0	4
RAID1E	4
RAID5	3

RAIDレベル	ディスク数
RAID6	4

注意

- 「RAID設定」で構築したRAIDアレイは、プロファイル解除によって削除(初期化)されません。RAIDアレイを初期化するには、対象装置のiRMCを操作してRAIDアレイを削除してください。
- iRMCの設定上でRAIDアレイがすでに構築されている場合、「RAID設定」によるRAID構築はエラーとなります。対象装置のiRMCを操作してRAIDアレイを削除してください。
- 「RAID設定」で指定されたRAIDアレイが既に構築されているときに、設定で指定したディスク数分の余剰ディスクが接続されているとRAIDグループが追加で作成されます。

2.4.4 OSインストールの設定

プロファイルのOSインストールに関する設定をします。

OSインストールの方法として、以下の2つの方法があります。

- PXEブート機能を利用する方法

  PXEブート機能は、プロファイル管理機能でサーバーへOSをインストールする場合や、ファームウェア管理機能でサーバーまたは搭載PCIカードのOfflineアップデートを実行する場合に利用します。PXEブート機能を利用するための設定については、「A.1.1 プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定」を参照してください。

- ServerView embedded Lifecycle Managementを利用する方法

  ServerView embedded Lifecycle Management機能(以降、「eLCM」と表記)を利用したインストールでは、iRMCのeLCMと、eLCMで提供されているembedded Installation Management(以降、「eIM」と表記)を利用します。OSインストールの対象サーバーがPRIMERGY、PRIMEQUEST 3000B／PRIMEQUEST 4000シリーズの場合に利用できます。

  eLCMを利用するためには、Repository Serverの構築を推奨します。Repository Serverを利用することで、事前準備のeIMのダウンロード時間を短縮できます。

ポイント

Repository Server環境の構築方法、確認方法については、下記の当社マニュアルサイトから『ServerView Repository Server - Installation and User Guide』を参照してください。

https://support.ts.fujitsu.com/index.asp?lng=jp

参照手順

「製品を選択する」 - [製品の検索]を選択し、「Repository Server」と入力して、[次へ]を選択してください。
[Documentation] - [Setup Guide]からダウンロードしてください。

なお、参照手順は、予告なく変更されることがあります。

OSインストール時に必要な準備作業(共通)

- 事前にOSインストール媒体をISM-VA上のリポジトリ領域にコピーしておく必要があります。この作業を「インポート」と呼びます。

  OSインストール媒体のISOイメージをインポートする場合は、ユーザーグループに仮想ディスクを割り当ててください。

  詳細は、「3.7.2 ユーザーグループに対する仮想ディスク割当て」を参照してください。

OSインストール時に必要な準備作業（PXEブート機能を利用する場合）

- 事前にServerView Suite DVDをISM-VA上にインポートしておく必要があります。

  ServerView Suite DVDのインポートは、Administratorグループに属し、AdministratorロールまたはOperatorロールを持つユーザーで行ってください。全ユーザーグループで共有されるため、ユーザーグループごとのインポートは必要ありません。

  詳細は、「2.14.2 リポジトリ管理機能」を参照してください。

  注意

  複数のServerView Suite DVDがインポートされている場合、OSインストールに失敗することがあります。
  OSインストール先のサーバーに対応したServerView Suite DVDのみをインポートしてください。
  なお、複数インポートした場合は、使用しないServerView Suite DVDをすべて削除し、ISM-VAを再起動してください。

- 対象ノードでPXEブート機能を利用します。管理LANからPXEブートが可能なように、ネットワーク接続および対象サーバーのBIOS設定を事前に完了させてください。また、ネットワーク内に別途DHCPサーバーが必要です。PXEブート時に適切なIPv4アドレスを対象ノードにリースできるようにDHCPサーバーを設定してください。

  詳細は、「A.1.1 プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定」を参照してください。

OSインストール時に必要な準備作業（eLCMを利用する場合）

- 事前に以下の作業が必要です。

  ― 対象ノードで管理LANへのネットワーク接続を事前に完了

  OSインストール時に使用するLANポートを、ノードの詳細画面の[プロファイル]タブ、またはプロファイルの「管理LAN ネットワークポート設定」で設定してください。未設定の場合は、オンボードLANの先頭ポートが使用されます。

  また、ネットワーク内に別途DHCPサーバーが必要です。OSインストール時に適切なIPv4アドレスを対象ノードにリースできるようにDHCPサーバーを設定してください。DHCPサーバーは、ISM-VA内のDHCP機能を有効にするか、対象ノードと同じネットワークセグメント内でDHCPサーバーを動作させ、OSインストール用のLANポートに対して適切なIPv4アドレスがリースできるよう設定してください。その際、リース期間は60分以上に設定してください。

  例：ISM-VAが192.168.1.100/24 に接続している場合のスコープ設定例

  - リース範囲：192.168.1.128～192.168.1.159
  - リース期間：8日間

  ― 対象サーバーにeLCMの環境を構築

  ― 対象サーバーのiRMC上のbootable SDカードにeIMをダウンロード

  eLCMを利用する場合、ServerView Suite DVDをISM-VA上へインポートする必要はありません。

  eIMのダウンロードに必要なRepository Serverに関する設定に、iRMC設定のプロファイルを利用できます。詳細は、『プロファイル管理機能 プロファイル設定項目集』の「第1章 PRIMERGY・PRIMEQUEST 3000B / 4000Eサーバー用プロファイルのBIOS/iRMC設定項目」を参照してください。ISMからeIMを最新版数に更新できます。

  ― eLCMの環境構築、eIMのダウンロード後、手動でのノード情報取得

  詳細は、「2.2.1.3 ノード情報の管理」を参照してください。

ポイント

eLCMの環境の構築方法、確認方法、eIMのダウンロード方法については、下記の当社マニュアルサイトから『ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx - Overview』（xには、最新の版数が入ります。）を参照してください。

https://support.ts.fujitsu.com/index.asp?lng=jp

参照手順

「製品を選択する」- [カテゴリから探す]を選択し、eLCMの環境を構築するサーバーを選択してください。
[Server Management Controller]からダウンロードしてください。

なお、参照手順は、予告なく変更されることがあります。

注意

- eLCMで利用できるeIMのイメージバージョンは、13.19.07以降です。
- iRMC S4を搭載したサーバーの場合、eLCMを利用できるiRMCのファームウェアバージョンは9.xxF以降です。

プロファイルでRAID設定済のノードにOSをインストールする場合

RAID設定を実施した[適用済]のプロファイルに、OS設定を追加編集してから再適用を実施します(「2.4.2.4 プロファイルの編集と再適用」参照)。その際、サーバー側のRAID構築の状況は変化しませんが、RAID設定の内容をISMでは確認できません。設定したRAID設定の内容を確認したい場合は、対象ノードのiRMCで確認してください。

注意

- 設定済みのRAID設定は編集しないでください。RAID設定を編集した場合、指定したディスク数分の余剰ディスクが接続されているとRAIDグループが追加で作成されます。

OSインストールの注意事項(PXEブート機能を利用する場合)

ネットワーク環境や対象サーバーのBIOS設定などに問題がある場合はPXEブートに失敗して、対象サーバーでインストール済みOSが起動することがあります。この場合、OSインストール対象のサーバーに対して、ISMによるシャットダウン操作は行われません。プロファイル適用処理(タスク)はタイムアウト時間経過後にエラー終了します。

タイムアウトでエラー終了する前にプロファイル適用処理を強制的に中止するときには、タスクをキャンセルしてください。

OSインストール後に実行されるスクリプトの指定手順(共通)

OSインストール後に、指定したスクリプトを実行させる場合は、事前にスクリプトファイルをISM-VAに転送しておく必要があります。

1. OSインストール後に実行させたいスクリプトを用意します。
2. ISM-VAにFTPで接続し、スクリプトファイルを転送します。

   ftpディレクトリー配下にスクリプト用の任意のディレクトリーを作成し、その下にスクリプトを転送してください。

   FTP転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
3. プロファイルの追加または編集で、[インストール後のスクリプト実行]の項目にスクリプトファイルを格納したディレクトリーと実行するスクリプトファイル名を指定します。

2.4.5 仮想IO設定

仮想IO設定は、オンボードLAN、オンボードCNA(Converged Network Adaptor)、増設LAN、増設FC(Fibre Channel)の各ポートを仮想化する設定です。この設定により次のような利点があります。

- LANポートに対して、LANインターフェイスが保有している実MACアドレスの代わりに指定したMACアドレス(仮想MACアドレス)に変更して動作させることができます。
- FCポートに対して、FCインターフェイスが保有している実WWNの代わりに指定したWWN(仮想WWN)に変更して動作させることができます。
- FCoE ポートに対しても同様に、実MACアドレス／実WWNを仮想MACアドレス／仮想WWNに変更した設定ができます。

これらにより、システムボードやPCIカードを保守交換した際にもポートの設定を変更することなく運用が継続できます。また、仮想IO設定では各ポートのネットワークブートの設定値を指定できます。仮想IO設定はプロファイル適用によって実行されます。

ポイント

仮想MACアドレスや仮想WWNは、ISMで管理するすべてのノードにおいて一意となるように設定してください。

注意

- ServerView Virtual-IO Manager（VIOM）などの仮想IOを管理するソフトウェアが動作している場合、ISMとの競合に注意してください。
- VIOMが動作している場合は、競合を避けるため、ISMとVIOMでは同じノードを管理しないようにしてください。
- 仮想IOのUEFIブートモードで設定した設定値は、BIOSのCSM Configurationの設定に反映されます。UEFIブートモードの各設定値の詳細については、『プロファイル管理機能プロファイル設定項目集』の「4.2 ポート設定」を確認してください。
- PRIMERGY BXシリーズでMMBのファームウェア版数が5.71より前の場合、MMBから仮想IOの設定をリセットしないでください。
- PRIMEQUEST 3000シリーズ（Partition）の場合、拡張パーティションは対応していません。物理パーティションのみ設定できます。
- PRIMEQUEST 3000シリーズ（Partition）の場合、パーティションのiRMCのIPアドレスとユーザーアカウントの設定が必要です。設定方法、確認方法については、以下の参照先を確認してください。

  https://support.ts.fujitsu.com/index.asp?lng=jp

  『PRIMEQUEST 3000 シリーズ 運用管理ツールリファレンス (MMB)』

  「製品を選択する」- [製品の検索]を選択し、「PRIMEQUEST」と入力して、[次へ]を選択してください。
  PRIMEQUESTの該当するモデルを選択し、[Documentation] - [Manuals]からダウンロードしてください。

  なお、参照手順は、予告なく変更されることがあります。

  ー iRMC IPアドレス設定

    『PRIMEQUEST 3000 シリーズ 運用管理ツールリファレンス (MMB)』の「2.4.3.1 [IPv4 Console Redirection Setup] 画面」

  ー iRMC ユーザーアカウント設定

    『PRIMEQUEST 3000 シリーズ 運用管理ツールリファレンス (MMB)』の「3.2.78 set irmc use」

  また、パーティションのノードの編集で、iRMC情報を設定してください。
- PRIMEQUEST 3000シリーズ（Partition）の場合、BIOSのCSM設定を無効にしてください。
- PRIMEQUEST 3000シリーズ（Partition）の場合、UEFIを使用してください。UEFIの設定方法については、『プロファイル管理機能プロファイル設定項目集』の「4.2 ポート設定」を確認してください。
- PRIMERGY やPRIMEQUEST 3000シリーズ（Partition）の場合、仮想MACアドレスの設定で、LANカードのポートのブート数を1つ以上にする必要があります。ブート対象が複数ある場合（LANカードのポート以外にもある場合）は、意図したブートの優先順位になっているかを確認します。
- SNMPトラップ送信先にISMのIPアドレスが設定されたサーバーに適用済みの仮想IO設定を含むプロファイルを解除すると、SNMPトラップ送信先に設定されたISMのIPアドレスは削除されます。
- BIOSのSANブート設定が有効の場合、仮想IOのプロファイル適用が失敗して「プロファイルのノードへの適用に失敗しました。」(メッセージID:50100813)が表示されます。仮想IO設定のプロファイル適用前にBIOSのSANブートが無効に設定されていることを確認してください。

MACアドレス、WWNの仮想化

MACアドレスやWWNの仮想化は、サーバーの仮想IO（仮想MACアドレスや仮想WWNなど）の設定をプロファイルとして管理したり、プロファイルを適用することで利用できます。管理対象サーバーやPCIカードを交換する際に周辺機器の設定変更作業の手間を軽減し、ネットワーク情報の再設定作業も容易に行えます。

仮想IOを設定した管理対象サーバー、およびPCIカードの交換は、以下の手順で行うことを想定します。

図2.19 仮想IOを設定した管理対象サーバーの交換

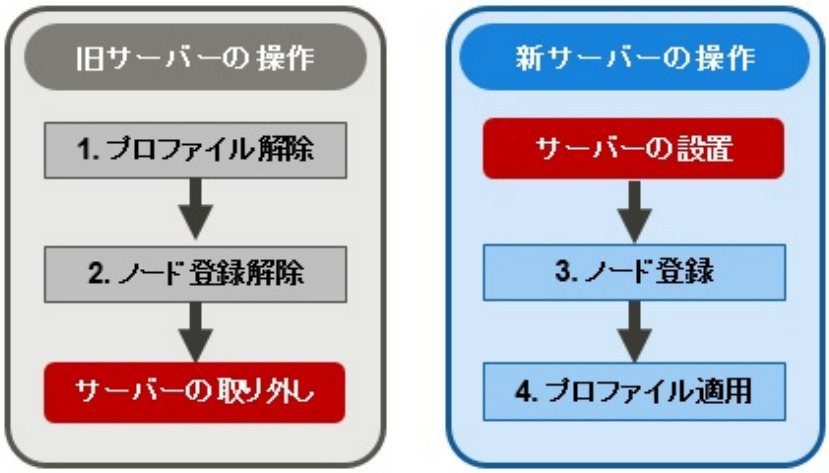
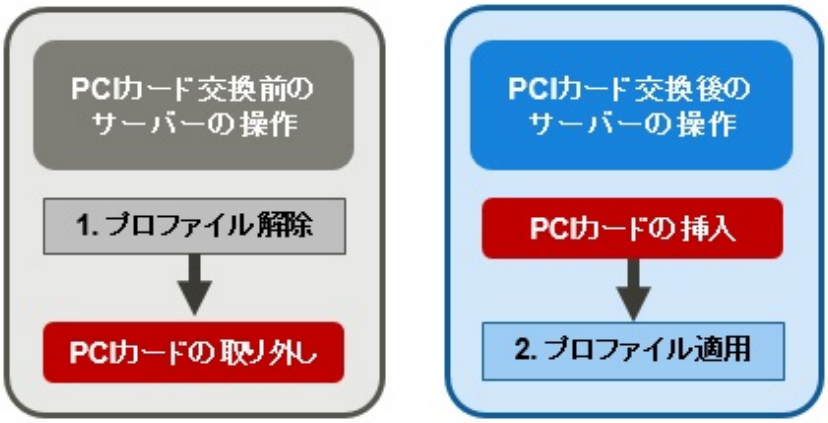


図2.20 仮想IOを設定したPCIカードの交換



注意

システムボードやPCIカードなどのノードの部品を保守交換した場合は、必ずノード情報取得を実施してください。ノード情報取得を実行する前に、PRIMERGYの電源を起動し、対象ノードのBIOS画面が表示されたことを確認してください。ノード情報取得により、ISMはノード内の実装状況を確認できます。プロファイルを適用する場合は、ノード情報取得の後に実施してください。ノード情報取得の方法については、「2.2.1.3 ノード情報の管理」を参照してください。

2.4.6 プール管理機能

プール管理機能は、アドレスリソースをプール化して管理する機能です。主に以下の機能があります。

- ユーザーが使用可能なアドレス範囲をプールとして設定
- 要求に応じて、プールから値を払い出し
- 不要になった値をプールに返却

プールの対象リソース

プールの対象とするリソースは、以下の仮想アドレスです。

- 仮想MACアドレス
- 仮想WWN

プール管理機能は、仮想IO設定で、上記の仮想アドレスを設定する際に使用します。

プロファイル作成時に上記の仮想アドレスを設定する場合、使用する仮想アドレスの値を入力しなくても自動的にプール範囲から値の払い出しができます。また、設定されているプール範囲から払い出す値を選択することもできます。

上記の仮想アドレスが設定されているプロファイルを削除すると、割当てが解除された仮想アドレスがプールに返却されます。

ここでは、以下の操作について説明します。

- プール設定の登録
- プール設定の確認
- プール設定の編集
- プール設定の削除

プール設定の登録

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 「プール登録」画面で必要な情報を設定し、[登録]を選択します。
   - プールタイプ

     設定するプールの種類を選択します。
   - 開始アドレスおよび終了アドレス

     設定するプール範囲の開始アドレスと終了アドレスを設定します。
   - 使用可能ユーザーグループ

     設定するプール範囲から値を払い出すことができるユーザーグループを選択します。

     [全てのユーザーグループ]を選択した場合、どのユーザーもここで設定したプール範囲から値を払い出すことができます。

プール設定の確認

ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択して、「プールリスト」画面を表示します。

「プールリスト」画面には、ユーザーが使用可能なプール設定が表示されます。また、残っている使用可能なアドレス数および払い出し済みのアドレスを確認できます。

残っている使用可能なアドレス数が0の場合、そのプール範囲からの払い出しはできません。「プール設定の登録」または「プール設定の編集」を実行してプール範囲を追加してください。

プール設定の編集

プール設定の編集では、開始アドレスおよび終了アドレスのみ編集できます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定] を選択します。

2. 編集するプール設定を選択し、[アクション]ボタンから[編集]を選択します。
3. 「プール編集」画面で必要な情報を設定し、[登録]を選択します。

注意

払い出し済みアドレスがある場合、払い出し済みアドレスがプール範囲外となる設定はできません。払い出し済みアドレスを確認して編集してください。

プール設定の削除

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]-[プール設定]を選択します。
2. 削除するプール設定を選択します。[アクション]ボタンから[削除]を選択します。
3. 削除対象を確認し、[削除]を選択します。

2.4.7 ブート情報の確認

仮想IOを設定したノードのブート情報を確認できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 「ノードリスト」画面の[カラム表示]欄で[ブート情報]を選択します。

2.4.8 iRMC(ユーザー)設定

iRMC(ユーザー)設定は、iRMCのローカルユーザーアカウントに対してユーザー情報の編集ができる機能です。主に以下の機能があります。

- 追加・変更

  ユーザー情報を指定することで、ユーザーの追加、もしくはユーザー情報の変更が可能です。

  プロファイル適用時に、対象のユーザーがiRMC上に存在するかを確認し、追加か変更が実行されます。

  追加または変更するiRMCのローカルユーザーアカウントを使用して、ISMからiRMCにアクセスすることがあります。

  ー 存在する場合、ユーザー情報を変更します。

  ー 存在しない場合、ユーザーを追加します。

- 削除

  ユーザー名を指定することで、ユーザーの削除が可能です。

  プロファイル適用時に、対象のユーザーがiRMC上に存在するかを確認し、削除が実行されます。

  ー 存在する場合、ユーザーを削除します。

  ー 存在しない場合、iRMCに対して操作を行いません。

注意

ISMに登録済みのノードのユーザーに対して操作する場合、以下の注意事項があります。

- 削除に指定した場合、プロファイルの適用がエラーになります。
- パスワードの変更を行う場合、ISMに登録済みのノードのパスワードも変更されます。

2.5 ログ管理機能

ログ管理機能は主に以下の用途で利用する機能です。

- ノードのログを、指定したスケジュールで定期的に収集
- ノードのログを、任意のタイミングで収集
- 収集したログをダウンロードして利用
- GUI画面上での参照やキーワード検索を実施

ISMでは、「取得するログの種類」や「収集スケジュール」をノードごとに設定できます。

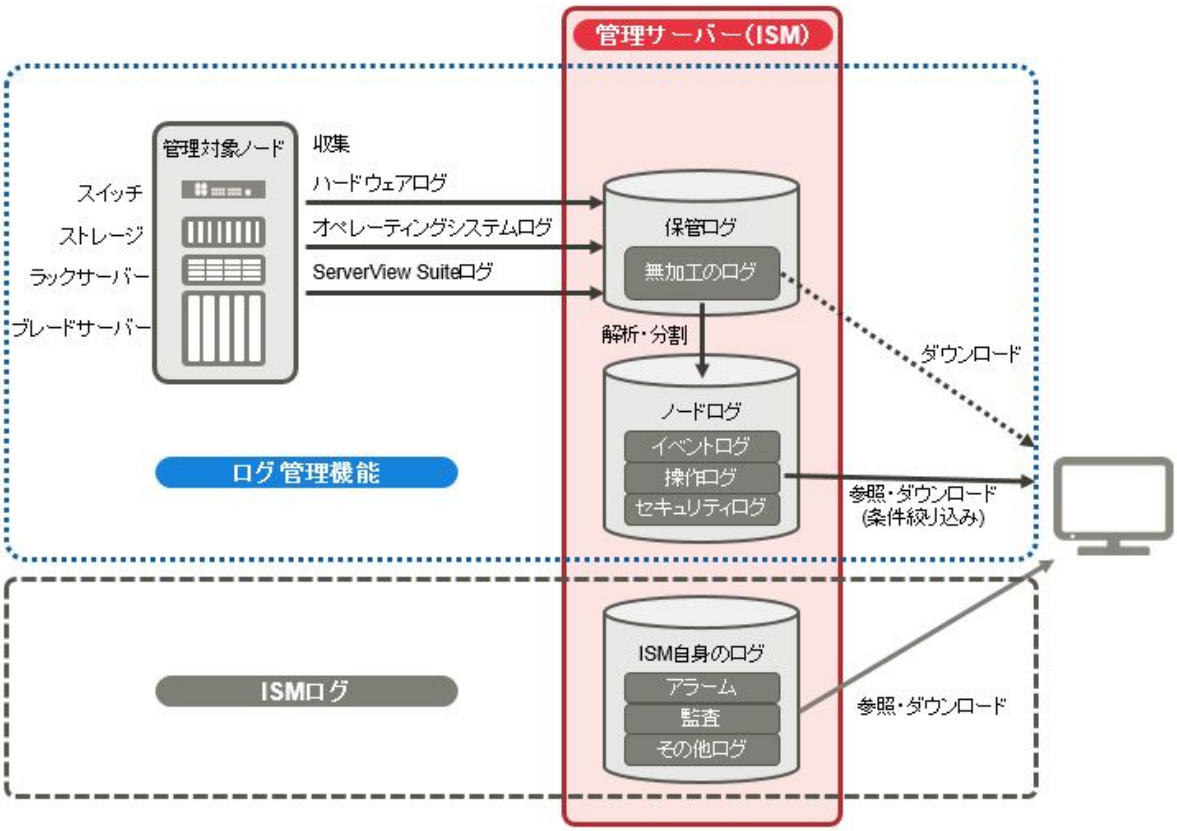
その設定に従ってノードから収集したログデータのひとかたまりを「保管ログ」と呼びます。

保管ログは、各ノードから収集されたログファイルがそのままのデータ形式で管理サーバー内に保管されます。任意のタイミングでISMのGUIを操作して、保管ログをzipファイルにして管理端末にダウンロードできます。

保管ログの任意のログファイルは、収集後直ちに、ISMの基準に従って「イベントログ」「操作ログ」「セキュリティログ」に分類されます。管理サーバー内には、GUIに一覧(検索)表示するための「ログ検索用データ」と、ダウンロードするための「ダウンロード用データ」として、別々に蓄積されます。ISMでは、この状態のログをまとめて「ノードログ」と呼びます。

「ノードログ」はGUIに一覧表示されます。さらに「イベントログ」「操作ログ」「セキュリティログ」での分類や発生日時などで表示内容をフィルタリングできます。また、フィルタリングされたログの一覧をCSVファイルやzipファイルとして、管理端末にダウンロードできます。

図2.21 ログ管理機能のイメージ



注意

ISMは保管ログのフォーマットを解析し、「イベントログ」「操作ログ」「セキュリティログ」に分類します。各ノードのログメッセージのフォーマットは、OSのデフォルト状態から変更しないでください。

例えばLinuxのオペレーティングシステムログの場合、OSのシステムログの設定でログメッセージのフォーマットが変更されると、ISMはそのログを認識できなくなり、正しいノードログを作成できなくなります。

以下について説明します。

2.5.1 収集可能なログの種類

ログ管理機能は、ハードウェアログ、オペレーティングシステムログ、ServerView Suiteログの3種類のログが収集可能です。サポートするハードウェアやOSなどの詳細は、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ハードウェアログ

各種管理対象ノードの装置ログを収集します。

種別	収集対象ノード	収集する保管ログ種類	解析および蓄積されるノードログ種類
サーバー	PRIMERGY（CX1430 M1、GXを除く）	SEL System Report （iRMC S4以降を搭載したサーバー）	SEL
	PRIMEQUEST 3000B		
	PRIMEQUEST 4000シリーズ（Partition）		
	PRIMERGY CX1430 M1	SEL（バイナリ）	なし
	PRIMERGY GX		
シャーシ	PRIMEQUEST 3000シリーズ（Partition）	SEL opelogviewコマンドの出力結果 selviewコマンドの出力結果 configviewコマンドの出力結果	SEL
ストレージ	ETERNUS DX/AF	export logコマンドの出力結果 show eventsコマンドの出力結果	show eventsコマンドの出力結果
	ETERNUS NR（NetApp）	event log showコマンドの出力結果	event log showコマンドの出力結果

種別	収集対象ノード	収集する保管ログ種類	解析および蓄積されるノードログ種類
	ETERNUS AB/HB	GET xxxx/devmgr/v2/storage-systems/1/audit-logの取得結果 GET xxxx/devmgr/v2/storage-systems/1/mel-eventsの取得結果	なし
スイッチ	SR-X	show tech-supportコマンドの出力結果	show logging syslogコマンドの出力結果 （show tech-supportコマンドの出力結果に含まれている）
	CFX		
	SR-S		
	イーサネットスイッチ（10GBASE-T 48+6） イーサネットスイッチ（10GBASE 48+6）	show tech-supportコマンドの出力結果	show logging persistentコマンドの出力結果 （show tech-supportコマンドの出力結果に含まれている）
	VDX	copy supportコマンドで作成される各種ファイル	show logging raslogコマンドの出力結果 show logging auditコマンドの出力結果 （copy supportコマンドで作成される＜任意の文字列＞.INFRA_USER.txt.gzファイルに含まれている）
	Cisco Catalyst	show tech-supportコマンドの出力結果	show loggingコマンドの出力結果 （show tech-supportコマンドの出力結果に含まれている）
	Cisco Nexus		
	Juniper QFX/EX	request support informationコマンドの出力結果	なし
	Brocade FC （7840/G610/G620を除く）	supportSaveコマンドで作成される各種ファイル	なし
IPCOM	IPCOM VX2	SEL System Report （iRMC S4以降を搭載したサーバー）	SEL
	IPCOM EX2	show tech-supportコマンドの出力結果	なし

オペレーティングシステムログ

管理対象サーバー上で動作しているOSのログを取得します。

取得対象のOS	収集するログ種類	
	OS上での名称	ISM上での分類
Windows	イベントログ（システムログ／アプリケーションログ）	オペレーティングシステムログ（イベントログ）
	イベントログ（セキュリティログ）	オペレーティングシステムログ（セキュリティログ）
Linux	システムログ（/var/log/messages）	オペレーティングシステムログ（イベントログ）
	システムログ（/var/log/secure）	オペレーティングシステムログ（セキュリティログ）
VMware ESXi	システムログ（syslog.log）	オペレーティングシステムログ（イベントログ）
IPCOM OS	システムログ（/var/log/messages）	オペレーティングシステムログ（イベントログ）
	システムログ（/var/log/secure）	オペレーティングシステムログ（セキュリティログ）
	テクニカルサポート情報	－

注意

仮想マシン上で動作しているOSは取得対象外です。

ServerView Suiteログ

管理対象サーバー上で動作しているソフトウェア（ServerView Suite製品）のログを取得します。

取得対象のソフトウェア	収集するノードログ種類
ServerView Agents	PrimeCollectコマンドの出力結果
ServerView Agentless Service	PrimeCollectコマンドの出力結果
ServerView RAID Manager	動作ログ（RAIDLog.xml、snapshot.xml）

注意

- 仮想マシン上で動作しているServerView Suiteログは取得対象外です。
- ServerView Suiteログは、ノードログ作成対象外です。

2.5.2 ログ保有期間の設定

ログの保有期間は、分類された「イベントログ」「操作ログ」「セキュリティログ」のそれぞれに対して別々に設定できます。また、分類前の「保管ログ」についても別途保有世代数を設定できます。

ログの保有期間は任意の値に設定できます。

「イベントログ」「操作ログ」「セキュリティログ」は、それぞれの保有期間を日数で設定します。指定した日数より古いタイムスタンプのログは削除されます。デフォルトでは過去30日分が保有される設定になっています。設定可能な範囲は1日～1830日（約5年分）です。

「保管ログ」はスケジュール動作または任意タイミングの収集を一回とカウントしたときに、過去何世代分を保有しておくかを設定します。設定した世代数より古い「保管ログ」は削除されます。デフォルトでは過去7世代分が保有される設定になっています。設定可能な範囲は1～366世代です。

ポイント

- 「イベントログ」「操作ログ」「セキュリティログ」「保管ログ」のそれぞれの保有期間、保有世代数は互いに影響しません。

  例えば、「イベントログ」「操作ログ」「セキュリティログ」のそれぞれの保有期間が30日に設定されている状態で、対象ノードには過去1年分のログが蓄積されている場合、ログ収集を実行すると、「保管ログ」には1年分すべてが保存されます。「イベントログ」「操作ログ」「セキュリティログ」は過去30日より古いログは保存されません。

- 最初のログ収集を実行する前に、保有期間の設定が運用に最適な値となっていることを確認してください。

  デフォルトでは、「イベントログ」「操作ログ」「セキュリティログ」のそれぞれの保有期間は30日に設定されています。

  最初のログ収集でノードから「保管ログ」を取得したとき、30日分より古いログは「イベントログ」「操作ログ」「セキュリティログ」のそれぞれには蓄積されません。

  2回目以降のログ収集の前に保有期間を30日より大きな値に変更しても、30日以前のノードログはさかのぼって蓄積されることはありません。

  過去30日より前のログを蓄積したい場合は、最初のログ収集を実行する前に、ログ保有期間の設定を30日より大きな任意の値に変更してください。

2.5.3 ログ収集対象と収集日時の設定

ISMに登録したノードにログ収集の設定をすることで、ノードから各種ログを収集することができます。

各ノードに以下の内容を設定してください。

- ログ収集ターゲット

  収集対象とするログの種類を「ハードウェア」「オペレーティングシステム」「ServerView Suite」の中から任意に組み合わせて指定します。

  収集対象ノードがサーバー以外の場合は、「ハードウェア」だけが指定できます。

  1つも選択しなければログの収集は行われません。

- 保有期間(すべて必須)

  イベントログ:保有しておく最大日数を設定します。

  操作ログ:保有しておく最大日数を設定します。

  セキュリティログ:保有しておく最大日数を設定します。

  保管ログ:保有しておく最大世代数を設定します。

ノードからのログ収集は、以下の2通りの実行方法があります。

- 任意のタイミングで手動実行する
- スケジュールに従って自動実行する

ログの取得をスケジュールに従って定期的に自動実行したい場合は、それぞれのノードで実行スケジュールを設定します。

注意

ISMは、ノードからの情報を取得し確認したうえで、そのノードが「ハードウェアログ」「オペレーティングシステムログ」「ServerView Suiteログ」の各種ログの収集対象として有効であるかどうかを判定します。

ログ収集ターゲットの設定において、本来は設定可能であるべき「ハードウェアログ」「オペレーティングシステムログ」「ServerView Suiteログ」が設定不可能な状態になっている場合は、そのノードからの情報取得が正常に完了していない可能性があります。

- 「ハードウェアログ」が設定不可能な場合は、管理サーバーとノードとのネットワーク接続や、ノードプロパティの設定(特にネットワーク関連項目)を再度確認します。その後、[ノード情報取得]を再実行してください。
- 「オペレーティングシステムログ」「ServerView Suiteログ」が設定不可能な場合は、ノードのOS情報の内容が正しく登録されているかを確認します。その後、[ノード情報取得]を再実行してください。
- 「ServerView Suiteログ」は、ログ収集に対応したServerView Suite製品(ServerView Agents、ServerView Agentless Service、ServerView RAID Manager)がインストールできるOSである場合のみ設定可能な状態となります。

定期ログ収集を行う場合は、スケジュールを設定します。

ノード1台ごとに設定したスケジュールで、指定した種類のログを収集し、ISM-VAの定められた領域に保管しておくことができます。

収集スケジュールの指定は以下の2種類が可能です。

- 曜日指定

  曜日ごとにログ取得の時刻を指定します。ログを取得する曜日と時刻を「毎週○曜日の○時○分」のように指定します。また、「毎月の第△○曜日の○時○分」といった指定も可能です。

  例1) 毎週日曜日23:00にログ取得

  例2) 毎月の第一月曜日の12:10にログ取得

  例3) 毎週水曜日の11:00と金曜日の18:00にログ取得

・ 日付指定

毎月の決まった日、または最終日ごとにログ取得の時刻を指定します。

例1）毎月10日の11:00と20日の18:00にログ取得

例2）毎月最終日の23:50にログ取得

GUIを使った設定操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ収集設定]を選択します。
3. 設定対象のノードにチェックを付けます。複数のノードにチェックすると、同様の内容を一度に設定できます。
4. [アクション]ボタンから[ログ収集設定編集]を選択します。

ポイント

ログ収集設定編集操作は、以下の手順で表示される画面でも同様の操作が行えます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 以下のどちらかを行います。
   - ノードリストの[カラム表示]から[ログ収集設定]を選択します。
   - ノードリストで対象の[ノード名]を選択し、[ログ収集設定]タブを選択します。

注意

ログ収集設定編集のスケジュールに設定する時間は、ISM-VAのタイムゾーンの時間で設定してください。

ISM GUIのタイムゾーンの時間を設定した場合、期待したスケジュール時間に定期ログ収集が実行されないことがあります。

スケジュール設定後、[次回実行日時]欄で、期待したスケジュール時間が設定されていることを確認してください。

ISM-VAのタイムゾーンについては、ISM管理者に確認してください。

2.5.4 ログ収集の動作

定期ログ収集

定期ログ収集は、ノードのログを指定したスケジュールで定期的に収集して蓄積します。

定期ログ収集を行うためには、ログ収集のスケジュール設定を行う必要があります。

スケジュール設定時刻になると、自動的にログ収集が開始されます。

注意

・ 定期ログ収集では収集開始時刻にログ収集できない状態だった場合は、収集がスキップされます。ログ収集は、次回のスケジュール日時で取得されます。

ログ収集できない状態の例を示します。

- ノードからのログ収集が正常に実施できない（電源がオフになっている、ネットワーク通信できないなど）
- ノードに対してISMで別の操作を実施している

ー ノードがメンテナンスモードになっている（手動での取得は可能）

ー ISMが停止している

ログ収集できなかった場合は、ISMの[イベント]-[イベント]-[運用ログ]にエラーイベント（メッセージIDが「5014」で始まるログ）が登録されます。メンテナンスモードになっているためにログ収集ができなかった場合はエラーイベントが登録されません。

- ノードの種類によっては、ログ収集に時間がかかることがあります。そのため、ログ収集のスケジュール時刻と保有しているログのタイムスタンプに大きな差が生じる場合があります。
- 定期ログ収集開始後は、ログ収集を途中でキャンセルできません。そのため、対象ノードに対してファームウェア/ドライバーアップデート、プロファイル適用などのメンテナンスが予定され、定期ログ収集の実行時刻と重なる場合、メンテナンスが行えなくなる可能性があります。事前に定期ログ収集を無効にするか、スケジュール設定時刻の変更を推奨します。
- 同時にログ収集可能なノード数には上限があります。上限数のログ収集が実行中の場合、あとから開始するログ収集はすぐに実行されず、先に実行しているログ収集が終了してから実行されます。
- ログ削除実行中のノードに対して実行されたログ収集は、ログ削除が完了するまで保留されます。ログ削除完了後に実行されます。

手動ログ収集

ノードのログを任意のタイミングで収集して蓄積します。

操作方法については、『操作手順書』の「5.3 管理対象ノードのログを収集する」を参照してください。

ログ保管先のディスク容量監視機能

ログファイルは、ノードが所属しているユーザーグループのログ保存領域に保管されます。

本機能はユーザーグループのログ保存領域の容量を監視します。

ISMが保管する各種ログファイル（保管ログ、ノードログ（ダウンロード用データ）、ノードログ（ログ検索用データ））の総容量の上限（サイズ制限）とディスク容量監視（しきい値監視）の設定値はユーザーグループ設定に設定されています。ユーザーグループ設定については、『操作手順書』の「2.3.2 ユーザーグループを管理する」を参照してください。

各種ログファイルの総容量が設定値に近づくと、グローバルナビゲーションメニューの[イベント]-[イベント]の[運用ログ]タブに警告イベントが登録されます。設定値を超えた（エラーイベントが登録された）場合は、新たなログは保管されません。

エラーイベントが登録された場合、イベントが発生したノード、または同じユーザーグループに所属している別ノードに対して、手作業で不要なログを削除するか、保管期限を超えたログが自動削除されて空き領域が増えると、新しいログが保管されるようになります。

条件	動作
ログファイルの総容量がディスク容量監視の設定値の容量を超えた場合 例） 上限設定値が10GB、ディスク容量監視の設定値が80%の場合、ログファイルの総容量が8GBを超えると右記動作を行います。	• ログ収集は行う。 • [イベント]-[運用ログ]に警告イベントが出力される。 表示されるメッセージは以下のような内容になります。 ー 保管ログの場合 ノード（＜ノード名＞）のログ収集中に、ユーザーグループ（＜ユーザーグループ名＞）の保管ログ保存領域が（xxMB）となり、しきい値（xx%）（xxMB）を超過しました。 「2.5.9 保管ログの削除」参照 ー ノードログ（ダウンロード用データ）の場合 ノード（＜ノード名＞）のログ収集中に、ユーザーグループ（＜ユーザーグループ名＞）のノードログ（ダウンロード用データ）保存領域が（xxMB）となり、しきい値（xx%）（xxMB）を超過しました。 「2.5.8 ノードログの削除」参照 ー ノードログ（ログ検索用データ）の場合 ノード（＜ノード名＞）のログ収集中に、ノードログ（ログ検索用データ）保存領域が（xxMB）となり、しきい値（xx%）（xxMB）を超過しました。

条件	動作
	「2.5.8 ノードログの削除」参照
ログファイルの総容量が上限設定値を超えた場合 例） 上限設定値が10GBの場合、ログファイルの総容量が10GBを超えると右記動作を行います。	• ログ収集を行わない。 • [イベント]-[運用ログ]にエラーイベントが出力される。 表示されるメッセージは以下のような内容になります。 ― 保管ログの場合 ノード（＜ノード名＞）のログ収集中に、ユーザーグループ（＜ユーザーグループ名＞）の保管ログ保存領域が設定容量（xxMB）に達しました。 「2.5.9 保管ログの削除」参照 ― ノードログ（ダウンロード用データ）の場合 ノード（＜ノード名＞）のログ収集中に、ユーザーグループ（＜ユーザーグループ名＞）のノードログ（ダウンロード用データ）保存領域が設定容量（xxMB）に達しました。 「2.5.8 ノードログの削除」参照 ― ノードログ（ログ検索用データ）の場合 ノード（＜ノード名＞）のログ収集中に、ノードログ（ログ検索用データ）保存領域が設定容量（xxMB）に達しました。 「2.5.8 ノードログの削除」参照

2.5.5 ノードログの検索

蓄積された「ノードログ」から、指定したキーワードを含むログを検索して表示できます。

「ノードログ」画面を開いた初期状態では、ノードごとに蓄積された「ノードログ」がひとまとめに一覧表示されます。

GUIを使ったログの検索操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ノードログ検索]を選択します。
3. GUI上の検索用テキストボックスにキーワードを入力します。

   入力したキーワードを含むログが表示されます。

次にGUIを使ったログのフィルタリング操作については、『操作手順書』の「4.8 ノードログを表示する」を参照してください。

ポイント

ログの簡易的なダウンロード機能として、GUI画面の現在の表示内容をCSVファイルとして出力できます。CSV出力は、[アクション]ボタンから[CSVエクスポート]を選択することで実行できます。

2.5.6 ノードログのダウンロード

蓄積しているノードログを期間、種別を指定してダウンロードできます。期間はISM-VAのタイムゾーンの日付で指定します。

また、複数のノードのログをまとめてダウンロードできます。

ダウンロードファイルは、1つのzipファイルに圧縮されます。

また、zipファイルにパスワードを設定することもできます。

GUIを使ったログのダウンロード操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[ノードログ]タブを選択します。
3. 対象のノードにチェックを付けます。
4. [アクション]ボタンから[ダウンロードファイル作成]を選択し、画面に従ってダウンロードファイル作成を実行します。

   「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。
5. ダウンロード用ファイルの作成完了を待ちます。

   作成状況は、画面上部に表示されるダウンロードファイル項目で確認します。
   または、グローバルナビゲーションメニュー上部の[タスク]を選択し、処理状況を確認します。

   タスクタイプは、[Creating Node Log download file]と表示されます。

   タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。
6. ダウンロードファイルの作成が完了したら、[ダウンロード]ボタンを選択します。

ポイント

- ノードログのダウンロード操作は、以下の手順で表示される画面でも同様の操作が行えます。
  1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
  2. 以下のどちらかを行います。
     - ノードリストの[カラム表示]から[ログ収集設定]を選択します。
     - ノードリストで対象の[ノード名]を選択し、[ログ収集設定]タブを選択します。
- 複数のノードを選択した場合でも、ダウンロードファイルは1つのzipファイルにまとめられます。

注意

- ノードログのダウンロードファイル作成で指定する期間の日付は、ISM-VAのタイムゾーンの日付で指定してください。ISM GUIのタイムゾーンの日付を指定した場合、期待した日時のノードログがダウンロードされないことがあります。ISM-VAのタイムゾーンについては、ISM管理者に確認してください。
- ISMでは、ダウンロードファイルは常に1つしか保持できません。そのため、ログのダウンロード操作を連続で実行した場合、以前に作成されたダウンロードファイルは削除されます。
- ログ収集中のノードに対するダウンロードファイル作成は実行できません。ログ収集完了後にダウンロードファイル作成を実行してください。

ダウンロードしたログは、以下のファイル名になります。

- ダウンロードファイル名

  NodeLog_＜ダウンロード指定期間＞.zip

  ＜ダウンロード指定期間＞のフォーマットは＜指定開始日＞-＜指定終了日＞となり、それぞれYYYYMMDD（年月日）で表示されます。

  例）2017年11月1日～2017年11月7日の期間を指定した場合

```
NodeLog_20171101-20171107.zip
```

zipファイルの展開後のフォルダー構成は以下のとおりです。

- フォルダー構成

```
＜ノード名＞_＜ノードID＞¥＜カテゴリー＞¥＜ログ種別＞
```

＜カテゴリー＞のフォーマットは、「hardware/os」です。

＜ログ種別＞のフォーマットは、「event/operation/security」です。

2.5.7 保管ログのダウンロード

保管ログをダウンロードできます。また、同一ノードの複数の世代のログや複数ノードのログをまとめてダウンロードできます。ダウンロードファイルは、1つのzipファイルに圧縮されます。また、zipファイルにパスワードを設定することもできます。

保管ログをダウンロードする手順については、『操作手順書』の「4.9 保管ログをダウンロードする」を参照してください。

ダウンロードしたログは、以下のファイル名になります。

- ダウンロードファイル名

```
ArchivedLog_＜ダウンロードファイル作成日時＞.zip
```

zipファイルの展開後のフォルダー構成は以下のとおりです。

- フォルダー構成

```
＜ノード名＞_＜ノードID＞¥＜日時＞_＜ノード名＞_＜ノードID＞¥＜カテゴリー＞
```

＜日時＞のフォーマットは、「YYYYMMDDhhmmss（年月日時分秒）」です。

＜カテゴリー＞のフォーマットは、「hardware/software」です。

2.5.8 ノードログの削除

設定した保有期間を経過したノードログ（ダウンロード用データ、およびログ検索用データ）は自動的に削除されます。手動で任意のノードログを個別に削除することもできます。その場合、ノード名や期間、ログの種類を条件として、対象を絞り込んだうえで削除を実行します。

ダウンロード用データ、およびログ検索用データは、同じ対象のデータが同時に削除されます。

GUIを使ったノードログの削除操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[ノードログ]タブを選択します。
3. 対象のノードにチェックを付けます。

   複数のノードを選択できます。
4. [アクション]ボタンから[ノードログファイル削除]を選択し、画面に従ってログの削除を実行します。

   「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。
5. グローバルナビゲーションメニュー上部の[タスク]を選択し、処理状況を確認します。

   タスクタイプは、[Deleting Log files]と表示されます。

タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。

注意

- ノードログの削除には時間がかかることがあります。このため、削除処理が完了するまで、GUIに削除対象としたノードログの情報が表示される場合があります。この場合、「タスク」画面の該当タスクでノードログの削除処理完了を確認し、本画面を再表示してください。
- 大量のノードログを一度に削除するときは、削除に数分から数時間かかる場合があります。なお、選択したノードのすべてのログを削除してもよい場合は、削除条件の[種類]にすべてのログ種類を選択し、[期間]に削除当日の日付を指定することで、短時間で削除できます。
- ログ収集実行中のノードに対して実行されたノードログ削除は、ログ収集が完了するまで保留されます。ノードログ削除は、ログ収集完了後に実行されます。

2.5.9 保管ログの削除

設定した保有回数を超えた保管ログは自動的に削除されます。手動で任意の保管ログや保有世代を指定して蓄積された保管ログを個別に削除することもできます。

GUIを使った保管ログの削除操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ログ収集]を選択します。
2. ログ収集メニューから[ログ管理]-[保管ログ]タブを選択します。
3. 対象のノードにチェックを付けます。

   複数のノードを選択できます。
4. [アクション]ボタンから[保管ログファイル削除]を選択し、画面に従って削除を実行します。

   「結果」画面が表示されます。この画面に表示されるタスク詳細の番号を控えておきます。

   また、[アクション]ボタンから[保管ログファイル確認]を選択し、表示された画面からでも削除操作が行えます。
   この場合は、削除するファイルにチェックを付けます。複数のファイルにチェックを付けると、一度に削除できます。
5. グローバルナビゲーションメニュー上部の[タスク]を選択し、処理状況を確認します。

   タスクタイプは、[Deleting Log files]と表示されます。

   タスクIDは、「結果」画面で控えたタスク詳細の番号を確認してください。

注意

- 保管ログの削除には時間がかかることがあります。このため、削除処理が完了するまで、GUIに削除対象とした保管ログの情報が表示される場合があります。この場合、「タスク」画面の該当タスクで保管ログの削除処理完了を確認し、本画面を再表示してください。
- ログ収集実行中のノードに対して実行された保管ログ削除は、ログ収集が完了するまで保留されます。保管ログ削除は、ログ収集完了後に実行されます。

2.6 ファームウェア管理機能

ファームウェア管理機能は主に以下の用途で利用する機能です。

- 管理対象ノードで現在動作しているファームウェアバージョンをISMのGUI上に表示
- ファームウェアデータに添付されているドキュメントを確認
- ファームウェアデータを利用して管理対象ノードのファームウェアをアップデート

- ServerView embedded Lifecycle Managementを利用して管理対象ノードのファームウェア／ドライバーをアップデート

ファームウェア管理機能の対象ノードは以下のとおりです。

- サーバーおよび搭載されるPCIカード類
- ストレージ
- スイッチ

対象ノードの詳細については、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ここでは、以下について説明します。

- 2.6.1 ファームウェアバージョンの確認
- 2.6.2 ファームウェアデータに添付されているドキュメントの確認
- 2.6.3 ファームウェア／ドライバーのアップデート
- 2.6.4 ジョブ管理
- 2.6.5 ファームウェアベースライン

2.6.1 ファームウェアバージョンの確認

GUIを使った操作例を示します。

1. 対象ノードの現在のノード情報を取得します。

   ノード情報取得の詳細は、「2.2.1.3 ノード情報の管理」を参照してください。

2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
3. [カラム表示]欄で[ファームウェア/ドライバー]を選択します。
4. 現行バージョン欄を確認します。

   現行バージョン欄が現在動作中のファームウェアバージョンを表しています。

2.6.2 ファームウェアデータに添付されているドキュメントの確認

ファームウェアデータに添付されているドキュメントを以下のどれかの手順で確認できます。

ポイント

- ISMを使用したアップデートの方法は、ファームウェアデータに添付されているドキュメントに記載されている方法とは異なります。
- サーバーのiRMC／BIOSのOnlineアップデート方法は、ファームウェアデータに添付されているドキュメントの「オンラインアップデート」とは異なります。サーバーのiRMC／BIOSのOnlineアップデート方法は、「リモートアップデート」に相当する処理が行われます。ファームウェアデータはISM-VA内のFTPサーバーから、対象サーバーのiRMC Webインターフェイスを利用して転送されます。

ISMに登録されているノードを選択してドキュメントを確認する場合

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[アップデート]を選択します。

3. ドキュメントを確認したいノードの[現行バージョン]欄、[Online最新]欄、および[Offline最新]欄を選択します。

   「ファームウェア ドキュメントリスト」画面が表示されます。

4. [ドキュメント]欄で確認したいドキュメントを選択し、ドキュメントを確認します。

ポイント

以下の手順で表示される画面でも同様の操作が行えます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. ノードリストで対象の[ノード名]を選択し、[ファームウェア/ドライバー]タブを選択します。

   以降の手順は上記と同様です。

インポートされているファームウェアデータを選択してドキュメントを確認する場合

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[インポート]を選択し、[ファームウェアデータ]タブを選択します。
3. ドキュメントを確認したいノードの [バージョン]欄を選択します。

   ファームウェア ドキュメントリスト画面が表示されます。

4. [ドキュメント]欄で確認したいドキュメントを選択し、ドキュメントを確認します。

ファームウェアアップデートを実行する際にドキュメントを確認する場合

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. アップデートを行うノードにチェックを付けます。[アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。
3. プルダウンメニューから更新バージョン、インポートデータを選択して、[次へ]ボタンを選択します。
4. [ドキュメント]欄で確認したいドキュメントを選択し、ドキュメントを確認します。

ポイント

以下の手順で表示される画面でも同様の操作が行えます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 以下のどちらかを行います。

   － ノードリストの[カラム表示]から[ファームウェア/ドライバー]を選択します。

   － ノードリストで対象の[ノード名]を選択し、[ファームウェア/ドライバー]タブを選択します。

3. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。

   以降の手順は上記と同様です。

2.6.3 ファームウェア／ドライバーのアップデート

2.6.3.1 アップデート方法

ファームウェア管理機能では、5種類のアップデート方法が使用できます。

アップデート方法と使用条件

管理するノードの運用方法と以下の使用条件にあったアップデート方法を選択してください。

・ Onlineアップデート

  ー BIOS／iRMCの場合
  OS稼働状態を問わずファームウェアアップデートが可能です。
  iRMCに対してファームウェアアップデートを実行します。

  ー PCIカードの場合
  OSが稼働した状態でファームウェアアップデートを実行します。
  OS上で対象コンポーネントの自己展開型ソフトウェアパッケージを実行し、ファームウェアをアップデートします。

・ Offlineアップデート
  PXEブートで専用のOSを一時的に起動し、OS上で対象コンポーネントの自己展開型ソフトウェアパッケージを実行してファームウェアをアップデートします。

・ eLCM Onlineアップデート
  eLCMの機能により、OS上で実行中のServerView Agents、またはAgentless Serviceと連携して、OS稼働状態でファームウェア/ドライバーおよび、ソフトウェアのアップデートを実行します。
  対象のファームウェア版数を選択することなく、最新にすることが可能です。

・ eLCM Offlineアップデート
  eLCMの機能により、iRMC上で専用イメージを一時的に起動し、対象コンポーネントの自己展開型ソフトウェアパッケージを実行してファームウェアをアップデートします。
  対象のコンポーネントとファームウェア版数を選択することなく、最新にすることが可能です。

・ eLCM Offlineアップデート(SimpleUpdate)
  eLCMの機能により、iRMC上で専用イメージを一時的に起動し、対象コンポーネントの自己展開型ソフトウェアパッケージを実行してファームウェアをアップデートします。

アップデート方法	使用条件				
	使用するファームウェアデータ	対象コンポーネントの任意選択	実行時のサーバーの電源状態	対象サーバー側のeLCMライセンス	留意事項
Online アップデート	ISM内にインポートしたデータ データ形式 ・ BIOS／iRMCの場合: バイナリデータ ・ PCIカードの場合: ASP [注]	可	・ BIOS／iRMCの場合: 電源オンまたは電源オフ ・ PCIカードの場合: 電源オン	不要	・ BIOSの場合、ファームウェアデータを個別インポートする際には、当社Webサイトからオフライン／リモートアップデートツールを入手してください。 ・ iRMCの場合、ファームウェアデータを個別インポートする際には、当社Webサイトからリモートアップデートツールを入手してください。 ・ PCIカードの場合、以下の留意事項があります。 ー ISMで対象ノードのOSにログインできるように設定されている必要があります。 ー 対象ノードのOSがWindowsとLinuxの場合のみサポートします。カード種別によってサポートOSは異なります。 ー ファームウェアデータを個別インポートする際には、当社WebサイトからOSに

アップデート方法	使用条件				
	使用するファームウェアデータ	対象コンポーネントの任意選択	実行時のサーバーの電源状態	対象サーバー側のeLCMライセンス	留意事項
					応じて対象コンポーネントのASPを入手してください。 － アップデート終了後に対象ノードのOSを再起動する必要があります。
Offline アップデート	ISM内にインポートしたデータ データ形式：ASP [注]	可	電源オフ	不要	・ 対象ノードのOSからISMにネットワーク接続できる必要があります（iRMCとの接続のみでは不可）。 ・ PXEブートの専用OSはServerView Suite Update DVDに収録されています。事前に当該DVDをISMにインポートしておく必要があります。 ・ PXEブートの専用OSはLinux系OSです。ファームウェアデータを個別にインポートする際には、当社Webサイトから対象コンポーネントのASPを入手してください。 － BIOS／iRMCの場合、ファームウェアデータを個別インポートする際には、当社Webサイトからオンラインアップデートツールを入手してください。
eLCM Online アップデート	iRMCがファームウェアリポジトリサーバーからダウンロードしたデータ データ形式：ASP [注]	可	電源オン	要	・ 対象ノードのOSがWindowsおよび、Red Hat Enterprise Linux、SUSE Linux Enterprise Serverの場合のみサポートしています。 ・ 対象ノードのOSにServerView Agents、またはAgentless Serviceがインストールされている必要があります。
eLCM Offline アップデート	iRMCがファームウェアリポジトリサーバーからダウンロードしたデータ データ形式：ASP [注]	不可 対象ノード内のすべてのコンポーネントが対象	電源オフ	要	
eLCM Offline アップデート (SimpleUpdate)	ISM内にインポートしたデータ データ形式：ASP [注]	可	・ 次回起動時にアップデートする場合： 電源オン	要	・ PCIカードの場合、事前にファームウェアツールをISMにインポートしておく必要があります。

アップデート方法	使用条件				
	使用するファームウェアデータ	対象コンポーネントの任意選択	実行時のサーバーの電源状態	対象サーバー側のeLCMライセンス	留意事項
			・即時にアップデートする場合：電源オフ		・iRMCの専用イメージはLinux系OSです。 ファームウェアデータを個別インポートする際には、当社のWebサイトから対象コンポーネントのASPを入手してください。 － BIOS／iRMCの場合、ファームウェアデータを個別インポートする際には、当社Webサイトからオンラインアップデートツールを入手してください。

[注]：ASP（Autonomous Support Packages）は、自己展開型ソフトウェアパッケージのファームウェアアップデートプログラムです。

アップデート対象としてサポートする機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

Offlineアップデートに必要な準備作業

サーバー（BIOS／iRMC／搭載PCIカード）にOfflineアップデートを行う場合、以下の準備が必要です。

- 事前にServerView Suite Update DVDをISM-VA上のリポジトリ領域にコピーしておく必要があります。この作業を「インポート」と呼びます。

  ServerView Suite Update DVDのISOイメージをインポートする場合は、ユーザーグループのLVMボリュームサイズを拡張してください。

  詳細は、「2.14.2 リポジトリ管理機能」を参照してください。

- 対象ノードでPXEブート機能を使用します。

  PXEブートで使用する管理LANは、ノードの詳細画面の[ファームウェア/ドライバー]タブで設定できます。また、「ファームウェア」画面で対象のノードを選択した場合に表示される「ノード情報」画面からも設定できます。未設定の場合は、オンボードLANの先頭ポートが使用されます。

  管理LANからPXEブートが使用できるように、ネットワーク接続および対象サーバーのBIOS設定を事前に完了させてください。また、ネットワーク内に別途DHCPサーバーが必要です。PXEブート時に適切なIPv4アドレスを対象ノードにリースできるようにDHCPサーバーを設定してください。詳細については、「A.1.1 プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定」を参照してください。

- BIOS設定では、ブートモードを確認してください。

  Offlineアップデート実行時の「ファームウェア/ドライバーアップデート」ウィザードで選択する[ブートモード]は、BIOS設定と同じモードにしてください。BIOS設定と選択した[ブートモード]が異なっている場合、PXEブートがエラーになることがあります。

注意

「Onlineアップデート」と「Offlineアップデート」では、必要となるファームウェアデータが異なる場合があります。また、機器に応じてサポート範囲が異なります。詳細は、当社の本製品Webサイトを参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

2.6.3.2 ファームウェアアップデート時の動作

ファームウェアアップデートの対象ノードの種別に応じて、アップデート時およびアップデート後の動作が異なります。

以下に示す表に従ってアップデートを実施してください。

表2.13 Onlineアップデートの場合

種別	アップデート時およびアップデート後の動作
サーバー（iRMC）	サーバーの電源がオン／オフどちらの状態でもアップデートされます。
サーバー（BIOS）	サーバーの電源がオン／オフどちらの状態でもアップデートされます。 ・ 電源オンの状態でアップデートした場合 新しいファームウェア（BIOS）に切り替えるためにサーバーの再起動、および電源をオンにする操作が必要です。再起動は任意のタイミングで行ってください。再起動時に自動でファームウェアの適用が行われ、その後サーバーの電源がオフになります。 電源オフになったあとで、ISMのノードの詳細画面などで電源をオンにすることで新しいファームウェアに切り替わります。 その後、以下を確認してください。 － サーバーのBIOSのバージョンが上がっていること － iRMCのシステムイベントログでアップデート時にエラーとなっていないこと ・ 電源オフの状態でアップデートした場合 新しいファームウェア（BIOS）に切り替えるためにサーバーの電源をオンにする操作が必要です。ファームウェアのアップデートが完了したタイミングで自動的に電源がオンの状態になり、その後サーバーの電源がオフになります。 電源オフになったあとで、ISMのノードの詳細画面などで電源をオンにすることで新しいファームウェアに切り替わります。 その後、以下を確認してください。 － サーバーのBIOSのバージョンが上がっていること － iRMCのシステムイベントログでアップデート時にエラーとなっていないこと
サーバー（PRIMEQUEST本体ファームウェア。PRIMEQUEST 4000シリーズは除く）[注]	サーバーの電源がオンの状態でアップデートされます。
サーバー（搭載PCIカード）	サーバーで、サポート対象OSが動作している場合にアップデートを実施できます。新しいファームウェアが動作するのは再起動後になります。再起動は任意のタイミングで行ってください。
スイッチ（CFX以外） ストレージ	ノードの電源がオンの状態でファームウェアアップデートを実施します。ファームウェアアップデート後にノードの再起動が実施される場合があります。
スイッチ（CFX）	ノードの電源がオンの状態でファームウェアアップデートを実施します。新しいファームウェアに切り替えるためにノードの再起動が必要です。再起動は任意のタイミングで行ってください。再起動を行う際、システム構成によっては通信が遮断される場合があります。システム構成を考慮したうえで再起動を行ってください。

[注]：PRIMEQUEST本体ファームウェアは、以下のファームウェアが含まれている統合ファームウェアです。

- PRIMEQUEST 2000/3000シリーズの場合：BIOSファームウェア、iRMCファームウェア、MMBファームウェア
- PRIMEQUEST 4000シリーズの場合：BIOSファームウェア、iRMCファームウェア

  統合ファームウェアに含まれている個々のファームウェアを個別にアップデートすることはできません。

表2.14 Offlineアップデートの場合

種別	アップデート時およびアップデート後の動作
サーバー（iRMC）	サーバーの電源がオフの状態でアップデートされます。
サーバー（BIOS）	
サーバー（搭載PCIカード）	

種別	アップデート時およびアップデート後の動作
	ファームウェアアップデート中はサーバーの電源投入および再起動が行われ、ファームウェアアップデート完了後は電源がオフになります。「アップデート設定」画面で[アップデート後にノードの電源をONにする]を選択した場合は、アップデート完了後に電源がオンになります。 ファームウェアアップデート完了後に自動で新しいファームウェアに切り替わります。 アップデート完了後に、バージョン表示が更新されないサーバーがあります。サブタスクに以下のメッセージが表示された場合、サーバーの電源をオン状態にした後、ISMのノード詳細画面でノード情報を取得してください。 Action: To check if the firmware update is complete, you must restart the device. Restart the device according to the procedures for the device. Check that the device is powered on, and then check that the firmware is updated to execute [Get Node information] on the [Details of Node] screen.
サーバー(PRIMEQUEST本体ファームウェア)[注]	サーバーの電源がオフの状態でアップデートされます。PRIMEQUEST 4000シリーズの場合、全パーティションの電源がオフの状態でアップデートされます。 ファームウェアアップデート中はサーバーの電源投入および再起動が行われ、ファームウェアアップデート完了後は電源がオフになります。 ファームウェアアップデート完了後に自動で新しいファームウェアに切り替わります。

[注]:PRIMEQUEST本体ファームウェアは、以下のファームウェアが含まれている統合ファームウェアです。

- PRIMEQUEST 2000/3000シリーズの場合:BIOSファームウェア、iRMCファームウェア、MMBファームウェア
- PRIMEQUEST 4000シリーズの場合:BIOSファームウェア、iRMCファームウェア

  統合ファームウェアに含まれている個々のファームウェアを個別にアップデートすることはできません。

2.6.3.3 アップデート時のスクリプト実行

対象ノードのアップデート開始前と完了後に、外部ホスト上に配置した任意スクリプトを実行できます。

Offlineアップデートしようとしている対象ノードを事前にシャットダウンする場合や、Onlineアップデート完了後に再起動する場合などに利用できます。

マクロ

スクリプト実行時の引数指定に、以下に示すマクロ(自動変数)機能を使用できます。これらのマクロは、自動的にノード情報に置換されます。

各マクロの詳細は以下のとおりです。

マクロ表記方法	概要
$_TRGID	アップデート対象ノードのノードID
$_TRG	アップデート対象ノードのノード名
$_IPA	アップデート対象ノードのIPアドレス
$_MDL	アップデート対象ノードのモデル名
$_OSIP	アップデート対象ノードのOSのIPアドレス
$_OSTYPE	アップデート対象ノードのOSタイプ
$_PSKIND	スクリプトの種類

ポイント

アップデート対象ノードにOS情報が登録されていない場合は、(none)と出力されます。

リモートスクリプトを実行するときに必要な準備作業

準備作業については、「2.3.3 アクション設定」の「各アクションを使用するときに必要な準備作業」の「リモートスクリプト実行」を参照してください。

スクリプトの登録手順

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[スクリプト]を選択します。
   「スクリプトリスト」画面が表示されます。
3. [アクション]ボタンから[追加]を選択します。
4. 画面に従ってリモートスクリプトを登録します。
5. ファームウェアアップデート画面で、アップデート時に実行するスクリプトを選択します。

ポイント

- アップデートのスクリプト設定画面でpreアップデートスクリプト、およびpostアップデートスクリプトに待機時間を秒単位で設定できます。
  - preアップデートスクリプトの待機時間は、pre scriptの実行からアップデートの実行開始までの待ち時間です。
  - postアップデートスクリプトの待機時間は、アップデートの完了からpost scriptの実行開始までの待ち時間です。
- ファームウェア/ドライバーアップデートのスクリプト設定画面で「ファームウェア/ドライバーアップデートが異常終了した場合でも実行する」を有効にすると、アップデートが異常終了しても設定したpostアップデートスクリプトが実行されます。
  なお、以下のときは設定を有効にしていても、postアップデートスクリプトが実行されません。
  - preアップデートスクリプトの実行が異常終了している。
  - 対象機器の電源状態によりアップデートが異常終了している。

スクリプトのテスト実行手順

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[スクリプト]を選択します。
   「スクリプトリスト」画面が表示されます。
3. 「スクリプトリスト」からテストを実行するスクリプトを選択します。
4. 画面右側の[アクション]ボタンから[テスト]を選択します。
   「スクリプトテスト」画面が表示されます。
5. 画面右側の[テスト]ボタンを選択し、スクリプトのテストを実行します。

テスト実行時には、スクリプト情報に設定したマクロは以下の文字列に置換されます。

マクロ	置換後の文字列
$_TRGID	TEST_TRGID
$_TRG	TEST_TRG
$_IPA	TEST_IPA
$_MDL	TEST_MDL
$_OSIP	TEST_OSIP
$_OSTYPE	TEST_OSTYPE
$_PSKIND	TEST_PSKIND

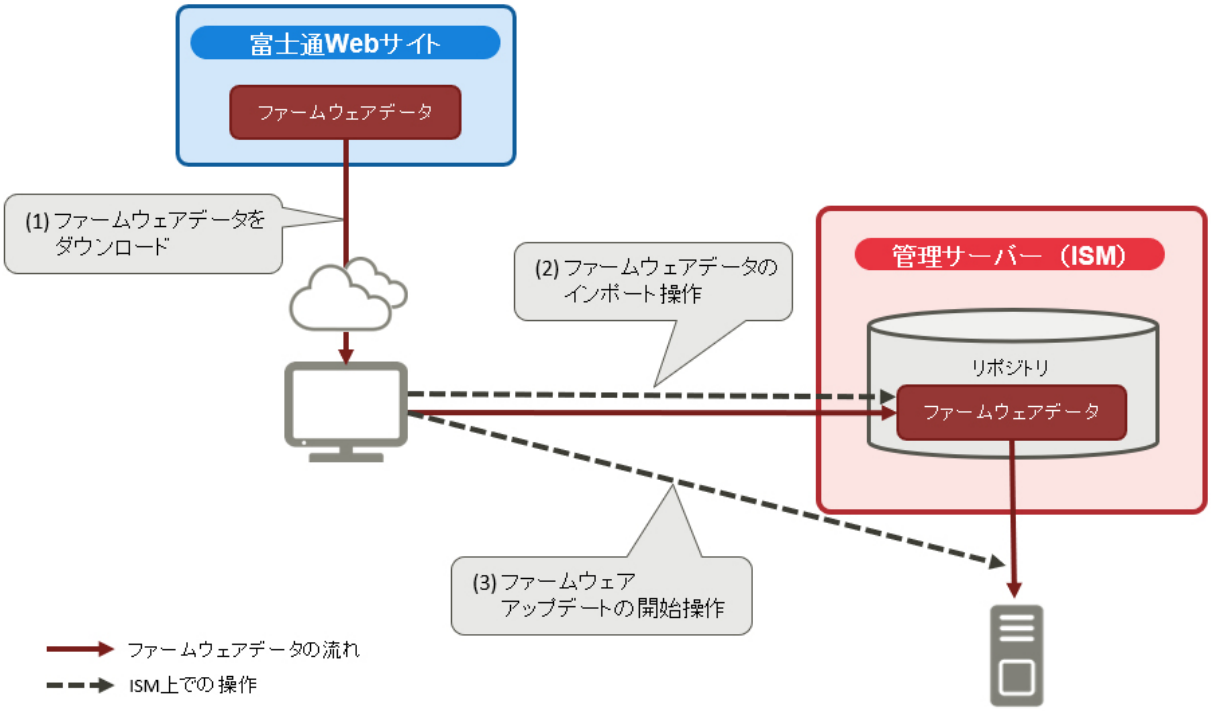
2.6.3.4 ファームウェアデータを利用したファームウェアアップデート

ファームウェアデータを利用してファームウェアをアップデートする場合は、事前にファームウェアデータをISMにインポートする作業が必要となります。

ファームウェアデータを当社のWebサイトなどからダウンロードし(下図(1))、それをISM-VA上のリポジトリに転送します(下図(2))。ISMはリポジトリに配置されたファームウェアデータを使用して対象ノードのアップデートを実行します(下図(3))。

リポジトリへファームウェアデータを転送する操作の詳細、「2.14.2 リポジトリ管理機能」を参照してください。

図2.22 ファームウェアデータを利用したファームウェアアップデートの流れ



ファームウェアアップデートの実施

注意

アップデートに関する共通の注意

- アップデート中は以下の事項を遵守してください。
  - 対象ノードの電源操作を行わない。
  - 対象ノードの再起動、リセットを行わない。
  - ISMと対象ノードの間のネットワークを切断しない。
  - 管理サーバーを再起動しない。管理サーバーの電源をオフにしない。
  - リポジトリからインポートデータ、ファームウェアデータを削除しない。
- アップデート開始前に、ファームウェアデータ添付のドキュメントなどに記載されている注意事項を確認してください。

- アップデート操作の前に、対象ノードに対して適用可能なファームウェアデータを保存しておく必要があります。

  ファームウェアデータの保存については、「2.14.2 リポジトリ管理機能」を参照してください。

- 一部のノードは、ファームウェアアップデートを段階的に適用する必要があります。各ファームウェアデータに添付されるドキュメントを参照してください。

- ファームウェアアップデート処理が正常に開始できない場合やアップデートに失敗した場合、通常はISMのアップデート処理はエラー終了します。しかし、アップデート途中で対象ノードが応答しなくなる場合などはタイムアウトエラーの検出は行いません。

  想定される作業時間を大きく超えても処理が完了しない場合は、対象ノードの状態を直接確認してください。異常の場合は、ISM上のファームウェアアップデートのタスクをキャンセルしてください。

  目安となるファームウェアアップデートの処理時間については、Webに記載される情報を参照してください。

- 同時にファームウェアアップデート可能なノード数には上限があります。この上限数はISM-VA全体で50です。上限数より多いノードを指定してファームウェアアップデートを行った場合、はじめに上限数分のノードのファームウェアアップデートが実行されます。残りのノードは先に実行しているファームウェアアップデートが終了してから実行されます。

  上限数のファームウェアアップデートを実行中にファームウェアアップデートを行った場合、先に実行しているファームウェアアップデートが終了してから実行されます。

Offlineアップデートに関する注意

- サーバー(BIOS／iRMC／搭載PCIカード)のOfflineアップデートでは、PXEブート機能を使用します。「ファームウェア/ドライバーアップデート」ウィザードの[ブートモード]では既定で「出荷時設定」が選択されており、ISMはPXEブートを以下のモードで実行します。

  ー iRMC S4以前を搭載したサーバー:LegacyBIOS互換モード

  ー iRMC S5以降を搭載したサーバー:UEFIブートモード

  サーバーのBIOS設定が上記と異なっている場合、PXEブートがエラーになることがあります。設定が異なっているときには、「ブートモード」画面の[ブートモード]で、サーバーのBIOS設定と同じブートモードを選択してください。

- Offlineアップデートの場合、インポートしたServerView Suite Update DVDの版数によっては、ファームウェアアップデートができないことがあります。「2.14.2.1 ファームウェアデータの保存と削除」を参照し、ServerView Suite Update DVDイメージをISMにインポートしてください。

- PRIMERGY GXのBIOS／BMCのOfflineアップデートを実行すると、サーバー側でのファームウェアの設定項目が初期化されます。お客様が変更した設定項目および設定値に関して、Offlineアップデート実施後に、BIOS／BMCを再設定してください。なお、再設定が完了するまでは、当該ノードの監視ができません。

Onlineアップデートに関する注意

- Onlineアップデートを使用したサーバー搭載のPCIカードおよびサーバーのBIOSのアップデートでは、ISM上でアップデート処理が完了しても古いファームウェアで動作しています。新しいファームウェアに動作を切り替えるために、以下の手順を行ってください。

  ー サーバー搭載のPCIカードをアップデートした場合は、新しいファームウェアに切り替えるためにサーバーの再起動が必要です。再起動は任意のタイミングで行ってください。

  ー 電源オンの状態でサーバーのBIOSをアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバーの再起動、および電源をオンにする操作が必要です。再起動は任意のタイミングで行ってください。再起動時に自動でファームウェアの適用が行われ、その後サーバーの電源がオフになります。電源オフになったあとで、ISMのノードの詳細画面などで電源をオンにすることで新しいファームウェアに切り替わります。

  ー 電源オフの状態でサーバーのBIOSをアップデートした場合は、新しいファームウェア(BIOS)に切り替えるためにサーバーの電源をオンにする操作が必要です。ファームウェアのアップデートが完了したタイミングで自動的に電源がオン状態になり、その後サーバーの電源がオフになります。電源オフになったあとで、ISMのノードの詳細画面などで電源をオンにすることで新しいファームウェアに切り替わります。

ネットワークスイッチのアップデートに関する注意

- CFX以外のネットワークスイッチのアップデート後、スイッチはリセットされるため、通信が一時的に切断されます。ネットワークを冗長化している場合は冗長構成の片側ずつ順番にアップデートするなどしてください。

- VDXスイッチの場合、VCS Fabric(Brocade VCS Fabric)を指定してファームウェアアップデートを行うことはできません。配下のVDXファブリックスイッチそれぞれに対して、ファームウェアアップデートを行ってください。

- Ciscoスイッチ（Catalyst、Nexus）は、モデルによるファームウェアデータの管理は行いません。

  ファームウェアデータのインポート画面で入力するバージョンの形式は自由です。

  入力したバージョンが現行バージョンと異なる場合、すべてアップデート対象となります。[Online最新]には、インポートされたファームウェアの最新と判断されるバージョンを表示します。

- Cisco Nexus9000シリーズのOnlineアップデートを実施する場合、SFTPプロトコルを使用してファームウェアデータを転送してください。

  Cisco Nexusスイッチのファームウェアデータの転送では、TFTPプロトコルを使用する場合、ファイルサイズの上限は約1.6GBです。

  Cisco Nexus9000シリーズの場合、ファームウェアデータ（バージョン9.3(5)）は約1.9GBになるため、TFTPプロトコルで転送できません。初期設定はTFTPプロトコルであるため、SFTPプロトコルに切り替える必要があります。

  Cisco NexusスイッチのOnlineアップデートでの使用プロトコルの確認／変更のコマンドは、「A.3.3 ファームウェアアップデートに使用するプロトコルの変更」を参照してください。

ストレージのアップデートに関する注意

- ETERNUS DX/AFのファームウェアアップデートを行う際は、ノード情報のSSHのユーザー名、パスワードに、ETERNUS DX/AFのMaintainerのロールを持つアカウントを指定する必要があります。

PCIカードのアップデートに関する注意

- PCIカードのファームウェアアップデートを行う際は、PCIカードが搭載されているサーバーのOS情報がISMに登録されている必要があります。

  サーバー（ノード）のOS情報の登録については、「2.2.1.5 ノードのOS情報の登録」を参照してください。また、PCIカードのファームウェアアップデートは、OSタイプが以下のもののみ対応しています。

  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - Windows

- サーバーに搭載されるPCIカードのファームウェアアップデートは、搭載されている同一種類のカードすべてに対して実行されます。

  同一種類のカードが複数存在する場合、カードごとに異なるファームウェアバージョンを指示したり、一部のカードだけをアップデート対象としたりすることはできません。ISM画面上で一部のカードだけをアップデート対象に指定した場合や、それぞれ異なるファームウェアバージョンを指定した場合も、同一種類のカードはすべてファームウェアアップデートが実行されます。アップデートされるバージョンは指示したファームウェアバージョンの中において、最も新しいバージョンとなります。

- Linux上のPCIカード（FC／CNA／LANカード）のファームウェアアップデートを行うためには、対象サーバーのOS上にEmulex OneCommand Manager CLI、またはQLogic QConvergeConsole CLIがインストールされている必要があります。

  Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLIの導入については、「2.14.3 Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLIの導入」を参照してください。

- 一部のノードおよびPCIカードは、[現行バージョン]と[Online最新]や[Offline最新]に表示されるバージョンの表示形式が異なります。

  該当するノードおよびPCIカードと、表示状態については、当社の本製品Webサイトを参照してください。

  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

- 一部のPCIカードは、現行バージョンの表示ができず、「-」と表示されます。

  その場合は、当該PCIカード用にインポートした、すべてのバージョンのファームウェアがアップデート対象になります。最新バージョンには、当該PCIカード用にインポートしたすべてのファームウェアの中から、最も新しいバージョンが表示されます。

- Intel LANカードは現行バージョンにeTrack-IDという識別子を表示します。

  eTrack-IDは、iRMCのWebインターフェイスで表示されるファームウェアバージョンです。

  アップデート対象を判断するため、現行バージョンとインポートしたファームウェアのバージョンを比較します。

  現行バージョンと比較するファームウェアのバージョンの表示形式は、以下のとおりになります。

  - ServerView Suite Update DVD（12.19.07版以降）からインポートした場合

    Intel LANカードのファームウェアは、ファームウェアバージョンの他に、適用前のeTrack-IDの値と適用後のeTrack-IDの情報を含んでいます。インポートしたファームウェアのバージョンとして、eTrack-IDの情報を含んだ次の形式で表示しています。

表示形式:適用前のeTrack-ID-適用後のeTrack-ID (ファームウェアファイルのファームウェアバージョン)

適用前のeTrack-IDが現行バージョンと一致した場合、アップデート対象となります。

ー 公開サイトからダウンロードしたファームウェアをインポートした場合/ISM 2.6.0.020より前にインポートしたファームウェアの場合

表示形式:(インポートしたファームウェアバージョン(eTrack-IDは含まれない))

現行バージョンによらず、アップデート対象となります。

現行バージョンによらずアップデートした場合、アップデートに成功しても、以下のケースでは現行バージョンは変わりません。

- すでに適用済みのファームウェアでアップデートした。
- バージョンをダウングレードしようとするファームウェアでアップデートした。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. アップデートを行うノードをメンテナンスモードに設定します。
   a. ノード名を選択し、「ノード情報」画面を表示します。
   b. [メンテナンスモード切替]ボタンで対象ノードをメンテナンスモードに設定します。
3. アップデートを行うノードの[現行バージョン]欄、[Online最新]欄、および[Offline最新]欄を確認します。

注意

[Offline最新]欄にファームウェアデータの版数が表示されていない場合は、インポートしたServerView Suite Update DVDの版数が適切でない可能性があります。「2.14.2.1 ファームウェアデータの保存と削除」を参照し、ServerView Suite Update DVDイメージをISMにインポートしてください。

4. [更新モード:]欄で[Onlineアップデート]または[Offlineアップデート]を選択し、アップデートを行うファームウェアにチェックを付けます。
5. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。
6. 画面表示に従い、操作を実行します。

   ー 日時を指定してファームウェアアップデートする場合

   「アップデート設定」画面で[アップデートを指定した時刻に開始する]を選択して実行する日時を指定してください。作業がISMのジョブとして登録されますので、作業の状態を「ジョブ」画面で確認してください。実行後の結果確認ダイアログボックスの「ジョブリスト:」欄にジョブIDが表示されます。ISMのGUIでグローバルナビゲーションメニューから[構築]-[ジョブ]を選択すると、ジョブ一覧が表示されます。ジョブIDを基に対象のジョブを識別してください。

   ー ファームウェアアップデートをすぐに開始する場合

   「アップデート設定」画面で[アップデートをすぐに開始する]を選択してください。アップデート開始後、作業がISMのタスクとして登録されますので、作業の状況を「タスク」画面で確認してください。実行後の結果確認ダイアログボックスの「タスク詳細:」欄にタスクIDが表示されます。

   ファームウェアアップデートのタスクには、以下のタスクタイプが登録されます。

   - Onlineアップデートの場合:Updating firmware
   - Offlineアップデートの場合:Updating firmware(Offline mode)

   ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、タスクの一覧が表示されます。タスクID、タスクタイプを基に対象のタスクを識別してください。

7. 該当タスクの完了を確認後、対象ノードのメンテナンスモードを解除します。

ポイント

- ファームウェアアップデートは、以下の手順で表示される画面でも同様の操作ができます。
  1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。

2. 以下のどちらかを行います。

   - 「ノードリスト」画面の[カラム表示]から[ファームウェア/ドライバー]を選択します。

   - 「ノードリスト」画面で対象の[ノード名]を選択し、[ファームウェア/ドライバー]タブを選択します。

- 「ファームウェア/ドライバーアップデート」ウィザードの「アップデート設定」画面で[アップデート時にメンテナンスモードに設定する]を選択した場合、アップデートの直前でメンテナンスモードに設定され、アップデート完了後にメンテナンスモードを解除します。日時を指定してアップデートする場合に利用してください。

2.6.3.5 ServerView embedded Lifecycle Managementを利用したOfflineファームウェアアップデート

ServerView embedded Lifecycle Management（以降、「eLCM」と表記）を利用して行うアップデートです。

Repository Serverまたは当社Webサイトのファームウェアデータを利用する方法と、ISMにインポートしたファームウェアデータを利用する方法があります。

違いは下表のとおりです。

項目	アップデートに利用するファームウェアデータ		
	Repository Server上のファームウェアデータ	当社Webサイト上のファームウェアデータ	ISMにインポートしたファームウェアデータ
ファームウェアアップデートの対象	サーバーコンポーネント（BIOS／iRMC／搭載PCIカード）		
ファームウェアアップデート対象（BIOS／iRMC／搭載PCIカード）の個別選択	不可	不可	可
Repository Serverの構築	必要	不要	不要
ISMへのファームウェアデータのインポート操作	不要	不要	必要

2.6.3.5.1 Repository Serverまたは当社Webサイトのファームウェアデータを利用したアップデート

ファームウェアアップデートの対象が、サーバー（BIOS／iRMC／搭載PCIカード）のときに利用できます。

この方法では、「2.6.3.4 ファームウェアデータを利用したファームウェアアップデート」に記載されているファームウェアデータをISMにインポートする作業は必要ありません。

eLCMは、ファームウェアアップデートの実行時に、Repository Serverまたは当社Webサイトから、必要なファームウェアデータをアップデート対象サーバーのiRMC上のbootable SDカードにダウンロードします。その後、SDカード上にダウンロードしたファームウェアデータからISOを作成します。作成したISOを使用して、サーバーのアップデートを実行します。

なお、選択できるアップデートの実行方法は以下のとおりです。

- ファームウェア/ドライバーを準備する
  ファームウェアデータをRepository Serverまたは当社Webサイトから、アップデート対象サーバーのiRMC上のbootable SDカードにダウンロードします。

- アップデートを実行する
  iRMC上のbootable SDカードにダウンロードしたファームウェアデータから作成したISOを使用して、アップデートします。

- ファームウェア/ドライバーの準備完了後、アップデートを実行する
  ファームウェアデータの準備完了次第、適用します。

eLCMを利用するためには、Repository Serverの構築を推奨します。Repository Server上のファームウェアデータを利用することで、処理時間を短縮できます。

ポイント

各環境の構築方法や確認方法については、下記の当社マニュアルサイトから該当のマニュアルを参照してください。

https://support.ts.fujitsu.com/index.asp?lng=jp

- eLCMの環境の構築方法、確認方法については、『ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx - Overview』(xには、最新の版数が入ります。)を参照してください。

  参照手順

  「製品を選択する」- [カテゴリから探す]を選択し、アップデート対象のサーバーを選択してください。
  [Server Management Controller]からダウンロードしてください。

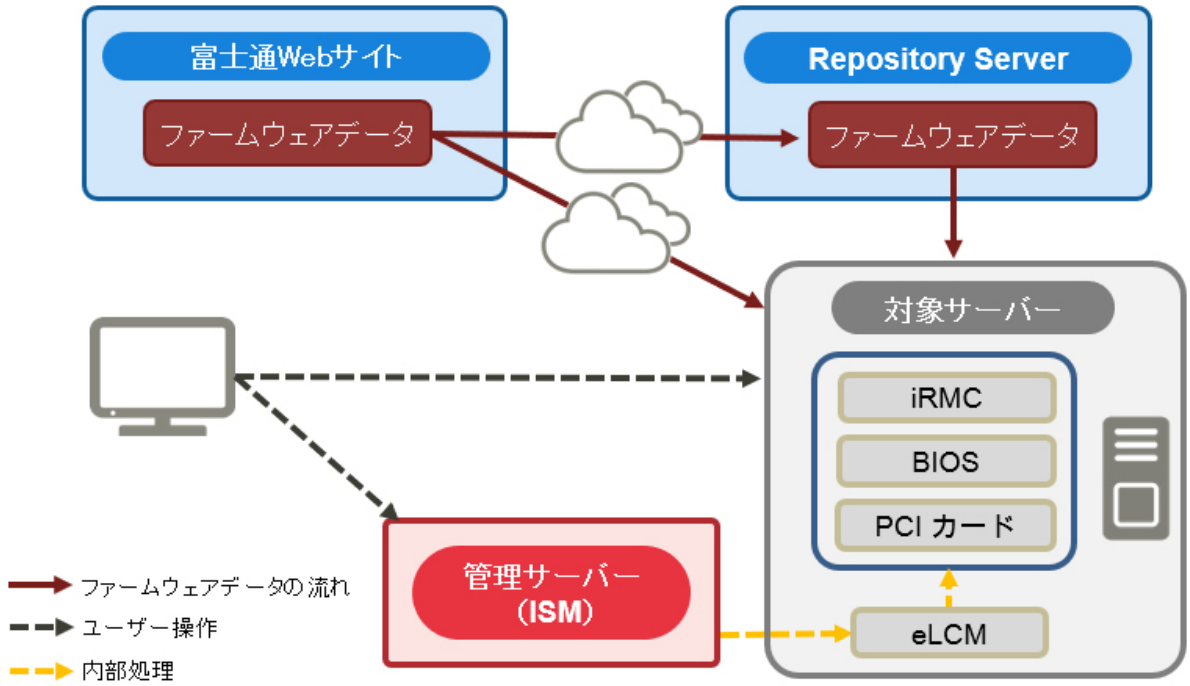
- Repository Server環境の構築方法、確認方法については、『ServerView Repository Server - Installation and User Guide』を参照してください。

  参照手順

  「製品を選択する」- [製品の検索]を選択し、「Repository Server」と入力して、[次へ]を選択してください。
  [Documentation] - [Setup Guide]からダウンロードしてください。

上記のマニュアルサイトの参照手順は、予告なく変更されることがあります。

図2.23 Repository Serverまたは当社Webサイトのファームウェアデータを利用したアップデートの流れ



Repository Serverまたは当社Webサイトのファームウェアデータを利用したアップデートに必要な準備作業

- Repository Serverの構築(推奨)
- eLCMを利用するためのファームウェアアップデート対象サーバーの環境設定
- ファームウェアアップデート対象サーバーの電源オフ

ファームウェアアップデートの実施

注意事項については、「2.6.3.4 ファームウェアデータを利用したファームウェアアップデート」を参照してください。

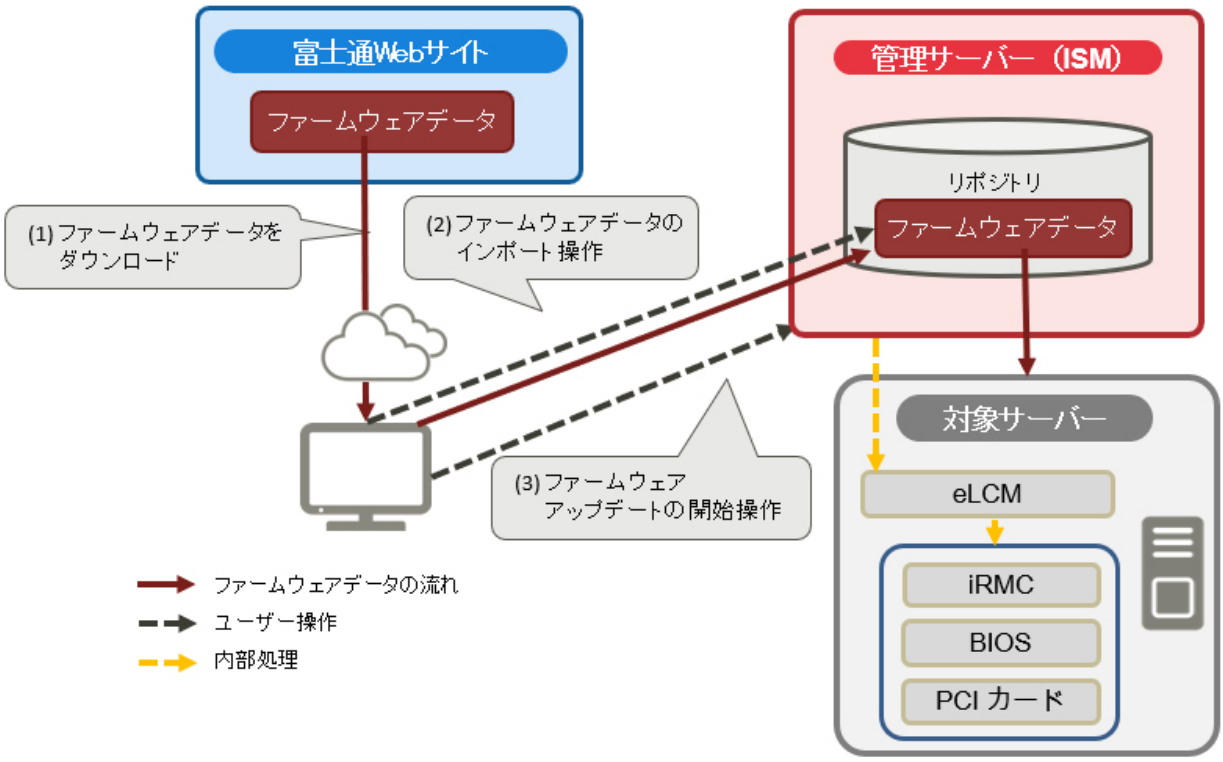
詳細な手順については、『操作手順書』の「6.4.2.1 Repository Serverのファームウェアデータを利用してアップデートする」の手順4～5を参照してください。

2.6.3.5.2 ISMにインポートしたファームウェアデータを利用したアップデート

ISMにインポートしたファームウェアデータと、eLCMを利用して行うアップデートです。

この方法では、「2.6.3.4 ファームウェアデータを利用したファームウェアアップデート」に記載されているファームウェアデータをISMにインポートする作業が必要です。

図2.24 ISMにインポートしたファームウェアデータを利用したアップデートの流れ



ISMにインポートしたファームウェアデータを利用したアップデートに必要な準備作業

- eLCMを利用するためのファームウェアアップデート対象サーバーの環境設定
- ファームウェアアップデート対象サーバーの電源オフ
- PCIカードをアップデートする場合、eLCM Offlineアップデート(SimpleUpdate)ツールをインポート

ファームウェアアップデートの実施

注意事項については、「2.6.3.4 ファームウェアデータを利用したファームウェアアップデート」を参照してください。

詳細な手順については、『操作手順書』の「6.4.2.2 ISMにインポートしたファームウェアデータを利用してアップデートする」の「ファームウェアをアップデートする」の手順4～6を参照してください。

2.6.3.6 eLCMを利用したOnlineファームウェア／ドライバーアップデート

eLCMとeLCMの環境構築については、「2.6.3.5 ServerView embedded Lifecycle Managementを利用したOfflineファームウェアアップデート」を参照してください。

- eLCM Onlineアップデートは、対象ノードのOS種別によってアップデート対象が異なります。
  - Windowsの場合、Windows用のPSP（PrimSupportPack-Win）として提供されるドライバーパッケージおよび、ServerView Agents等のソフトウェアをアップデートできます。
  - Red Hat Enterprise Linux、SUSE Linux Enterprise Serverの場合、ServerView Agents等のソフトウェアをアップデートできます。
- 対象ノードのOS上のServerView Agentsまたは、ServerView Agentless Serviceが利用可能なアップデートを検出し、その結果をiRMCに通知します。ISMは、iRMCから取得した当該情報に基づいて、アップデート可能なドライバーパッケージやソフトウェアを表示します。
- アップデート対象として選択しなくても、PrimSupportPack-Win/FSC_SCAN等の更新が必須なパッケージは、自動的にアップデートします。

eLCMを利用したOnlineファームウェア／ドライバーアップデートの流れ

eLCMを利用したOfflineファームウェアアップデートと同様です。「2.6.3.5.1 Repository Serverまたは当社Webサイトのファームウェアデータを利用したアップデート」を参照してください。

eLCMを利用したOnlineファームウェア／ドライバーアップデートに必要な準備作業

詳細な準備作業については、『操作手順書』の「6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する」を参照してください。

2.6.3.6.1 アップデート時の動作

- サーバーの電源がオンの状態でアップデートされます。
- サーバーで、サポート対象OSが動作している場合にアップデートが実施されます。
- アップデート中に、リブート処理が実施されることがあります。
- アップデート後に、ノードの再起動は必要ありません。

2.6.3.6.2 ファームウェア／ドライバーアップデートの実施

注意事項については、「2.6.3.4 ファームウェアデータを利用したファームウェアアップデート」を参照してください。

詳細な手順については、『操作手順書』の「6.4.3 ServerView embedded Lifecycle Managementを利用してファームウェア／ドライバーをOnlineアップデートする」を参照してください。

2.6.4 ジョブ管理

日時を指定してファームウェア/ドライバーアップデートを行う場合、その処理はジョブとして管理されます。

それぞれのジョブの状態は、操作した画面ではなく、「ジョブ」画面で一括表示されます。

以下の操作も「ジョブ」画面から行います。

- 実行中の処理の中止（キャンセル）
- 実行前の処理の削除
- 実行後の処理の削除

注意

- ジョブの数には上限があります。ISM-VA全体で100を超えるジョブは登録できません。上限を超えないよう、不要なジョブは削除してください。
- ジョブは10分間隔で実行されます。ジョブが実行される時間は、指定した時間よりも遅く実行されることがあります。最大9分です。

2.6.5 ファームウェアベースライン

ファームウェアベースラインは、管理対象ノードのファームウェアバージョンと定義したファームウェアバージョンを比較する機能です。ユーザーが定義したファームウェアバージョンと比較して、ノードが意図したファームウェアバージョンで動作しているかどうかを表示します。それにより、ユーザーが意図した動作環境に統一することを支援します。

ファームウェアベースライン定義は、ノードに適用するべきファームウェアバージョンの定義です。この定義と管理対象ノードのファームウェアバージョンを比較して、ファームウェアが適合／不適合／比較不可のノードを判定します。不適合のノードを選択して、一括で定義されたファームウェアバージョンにファームウェアアップデートできます。

ISMでは、PRIMERGYなどのハードウェアに対するHardware compatibility List（以降、「HCL」と表記します）をダウンロードし、HCLに記載されているコンポーネントとファームウェアバージョンからベースラインを作成できます。

作成したベースラインをノードに割り当てると、ファームウェアバージョンがHCLに適合しているかを判定できます。

ポイント

HCLは、Fujitsu Webサーバー（https://support.ts.fujitsu.com/globalflash/）に公開されています。HCLには、OS（VMware ESXiバージョン）と互換性があり、動作することが証明されているファームウェアの一覧が記載されています。

ファームウェアベースラインの状態

ファームウェアベースラインに定義したコンポーネント、およびコンポーネントのファームウェアバージョンと、管理対象ノードのコンポーネント／ファームウェアバージョンを比較した状態を以下のように表します。

適合

すべてのコンポーネントでファームウェアバージョンが一致

不適合

一部またはすべてのコンポーネントでファームウェアバージョンが不一致

比較不可

以下のいずれかの状態

- ファームウェアベースラインで定義した一部またはすべてのコンポーネントが、管理対象ノードに存在しない
- 管理対象ノードの一部、またはすべてのコンポーネントでファームウェアバージョンが不明
  この場合は、対象のコンポーネントとファームウェアベースライン定義を確認してください。対象のコンポーネントのファームウェアバージョンが取得できない場合、ファームウェアベースライン定義から対象のコンポーネントの定義を削除してください。

ノードが「不適合」のコンポーネントと「比較不可」のコンポーネントを含む場合、ノードの状態は「不適合」と表示されます。

ファームウェアベースラインで管理可能な機器（コンポーネント）については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

ここでは、以下について説明します。

2.6.5.1 ファームウェアベースライン定義の作成

管理しているノードに適用されているファームウェアバージョンに統一するために、ファームウェアベースラインでモデルごとに対応したファームウェアバージョンの定義を作成します。

ファームウェアベースライン定義を作成する方法は、3種類あります。

- ファームウェアデータをServerView Suite Update DVDからインポートするときに自動で作成
- リポジトリで管理しているファームウェアを利用して手動で作成
- Hardware compatibility Listをダウンロードして手動で作成

ファームウェアデータをServerView Suite Update DVDからインポートするときに自動で作成

ファームウェアデータをServerView Suite Update DVDからインポートするときにファームウェアベースライン定義を自動で作成する手順を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[インポート]を選択します。
3. [アクション]ボタンから[DVDインポート]を選択します。
4. 画面表示に従い、操作を実行します。

ポイント

- ファームウェアベースラインに定義された各コンポーネントのファームウェアバージョンは、すべて比較の対象となります。不要な定義が存在するとノードが適合となりません。必要に応じてファームウェアベースライン定義を修正してください。
- ServerView Suite Update DVDに含まれないモデルのファームウェアを管理する場合は、ファームウェアベースライン定義を手動で作成、または編集してください。

リポジトリで管理しているファームウェアを利用して手動で作成

リポジトリで管理しているファームウェアを利用して、手動で作成する手順を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. [アクション]ボタンから[作成]を選択します。
4. 画面表示に従い、操作を実行します。

ポイント

- ファームウェアベースラインに定義された各コンポーネントのファームウェアバージョンは、すべて比較の対象となります。不要な定義が存在するとノードが適合となりません。
- ファームウェアベースライン定義を手動で作成する場合は、事前にファームウェアをリポジトリに登録しておいてください。詳細は、「2.14.2.1 ファームウェアデータの保存と削除」を参照してください。

Hardware compatibility Listをダウンロードして手動で作成

Hardware compatibility Listをダウンロードして手動で作成する手順を示します。

1. グローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。

2. 画面左側のメニューから[ベースライン]を選択します。
3. [アクション]ボタンから[インポート(HCL)]を選択します。
4. 画面表示に従い、操作を実行します。

ポイント

- ファームウェアベースラインに定義された各コンポーネントのファームウェアバージョンは、すべて比較の対象となります。不要な定義が存在するとノードが適合となりません。必要に応じてファームウェアベースライン定義を修正してください。
- HCLをダウンロードする接続先の「Web Repository Address」には、以下のFujitsu Webサーバーの URLが初期表示されます。

  http://support.ts.fujitsu.com/globalflash/

  「Web Repository Address」には、上記URL以外にServerView Repository Server(リポジトリサーバー)を使用して構成されたWebサーバーのアドレスも指定できます。「2.6.3.5.1 Repository Serverまたは当社Webサイトのファームウェアデータを利用したアップデート」などで、すでにリポジトリサーバーを構築している場合、そのサーバーが使用できます。使用環境に合わせて、接続先を変更してください。「Web Repository Address」に、ISMから接続可能な、versionTree.txtやhclVMWareAll.xmlが配置されているリポジトリのルートのアドレスを指定する必要があります。

  詳細は、Webサーバーの管理者に問い合わせてください。
- Web Repository Addressに接続する際にプロキシを経由する場合はプロキシ設定が必要です。プロキシ設定を使用する場合は、以下の手順で設定してください。
  1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]を選択します。
  2. 画面左側のメニューから[プロキシ設定]を選択します。
  3. [アクション]ボタンから[追加]を選択します。
  4. 画面表示に従い、操作を実行します。

注意

ファームウェアタイプ:LAN ファームウェア名:MCXxxxxのバージョンは()で囲まれています。()内のバージョンは、ベースラインの状態が、必ず不適合になります。このファームウェアに対してベースラインの定義が必要な場合は、ベースラインを作成した後、ベースライン定義を編集してバージョンを修正してください。

ベースライン定義の編集を実行する前に、このファームウェアを、HCLをダウンロードする接続先のWeb Repository Addressからダウンロードして、リポジトリに登録しておいてください。詳細は、「2.14.2.1 ファームウェアデータの保存と削除」を参照してください。

リポジトリへのファームの登録後、ベースライン定義の編集を実行してください。ベースライン定義の編集の詳細は、「2.6.5.5 ファームウェアベースライン定義の編集」を参照してください。

eTrack-IDで定義されるファームウェアに対してファームウェア版数を指定した場合、ファームウェアを適用しても、ベースラインで定義したバージョンにならないことがあります。

eTrack-IDで定義されるファームウェアは、次のファームウェアです。

ファームウェアタイプ	LAN
ファームウェア名	X550-T2、X710、X722 LOM、E810

上記の場合、ベースラインの判定は不適合となります。ベースラインで定義したバージョンのeTrack-IDを変更してください。eTrack-IDとファームウェア名の対応関係については、下記の当社マニュアルサイトから『Intel LAN Controller Firmware Versions』を参照してください。

https://support.ts.fujitsu.com/index.asp?lng=jp

参照手順

「製品を選択する」- [カテゴリから探す]を選択し、ベースライン対象モデルのサーバーを選択してください。
[LAN]からダウンロードしてください。

なお、参照手順は、予告なく変更されることがあります。

2.6.5.2 ファームウェアベースライン定義の割当て

作成したファームウェアベースライン定義をノードに割り当てます。ファームウェアベースライン定義を選択して対象のノードに割り当てることで、対象ノードとファームウェアベースライン定義のファームウェアバージョンとの比較ができます。

ファームウェアベースライン定義を割り当てる例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. ベースラインの一覧から対象のベースラインを選択します。
4. [アクション]ボタンから[ノード割り当て]を選択します。
5. 画面表示に従い、操作を実行します。

注意

- ファームウェアベースライン定義をノードに割り当てる際、「対象ノードの選択」ウィザードの「1.ノード選択」画面のノード一覧には、ISMでファームウェアアップデート対象外のノードも表示されます。ファームウェアアップデート対象のノードを選択してください。ファームウェアアップデート対象については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。[サーバー・シャーシ]シートの「メンテナンス支援機能」-「ファームウェア版数管理」でサポートされている機種が対象となります。
  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/
  対象外のノードを選択して、ファームウェアベースライン定義の割り当てを適用すると、エラー（メッセージID：30113300）になります。
- ServerView Suite Update DVDを利用してファームウェアベースライン定義を作成する場合は、インポート時に管理しているノードにファームウェアベースライン定義を割り当てるかを選択します。ファームウェアベースラインがすでに割り当てられている場合は、上書きされます。
- ノードの自動検出で登録したノードに対してファームウェアベースライン定義を割り当てる際、登録したノードのモデル名とファームウェアベースライン定義のモデル名が異なっていると割当てに失敗します。ノードのモデル名をファームウェアベースライン定義のモデル名に変更してください。

2.6.5.3 ファームウェアベースライン定義の割当て解除

すでにファームウェアベースライン定義が割り当てられているノードに別のファームウェアベースライン定義を割り当てる場合は、ファームウェアベースライン定義の割当てを解除する必要があります。割当てを解除したノードに別のファームウェアベースライン定義を割り当てることができます。

ファームウェアベースライン定義の割当て解除をする例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. ベースラインの一覧から対象のベースラインを選択します。
4. [アクション]ボタンから[ノード割り当て解除]を選択します。
5. 画面表示に従い、操作を実行します。

2.6.5.4 ファームウェアベースライン定義を利用したファームウェアアップデート

不適合と判定されたノードを、ファームウェアベースラインに定義したファームウェアバージョンと一致させる場合に、ファームウェアベースラインを利用したファームウェアアップデートを実施します。

注意

実行時には、事前にISMにインポートしたファームウェアデータを利用してファームウェアアップデートを行います。

ファームウェアベースライン定義を利用したファームウェアアップデートの例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. ベースラインの一覧から対象のベースラインを選択します。
4. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。
5. 画面表示に従い、操作を実行します。

2.6.5.5 ファームウェアベースライン定義の編集

作成したファームウェアベースライン定義にモデルを追加、削除する場合や、定義したファームウェアバージョンを変更する場合に、ファームウェアベースライン定義の編集をします。

ファームウェアベースライン定義を編集する例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. ベースラインの一覧から対象のベースラインを選択します。
4. [アクション]ボタンから[編集]を選択します。
5. 画面表示に従い、操作を実行します。

2.6.5.6 ファームウェアベースライン定義の削除

ファームウェアベースライン定義を削除する例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[ベースライン]を選択します。
3. ベースラインの一覧から対象のベースラインを選択します。
4. [アクション]ボタンから[削除]を選択します。

5. 画面表示に従い、操作を実行します。

ポイント

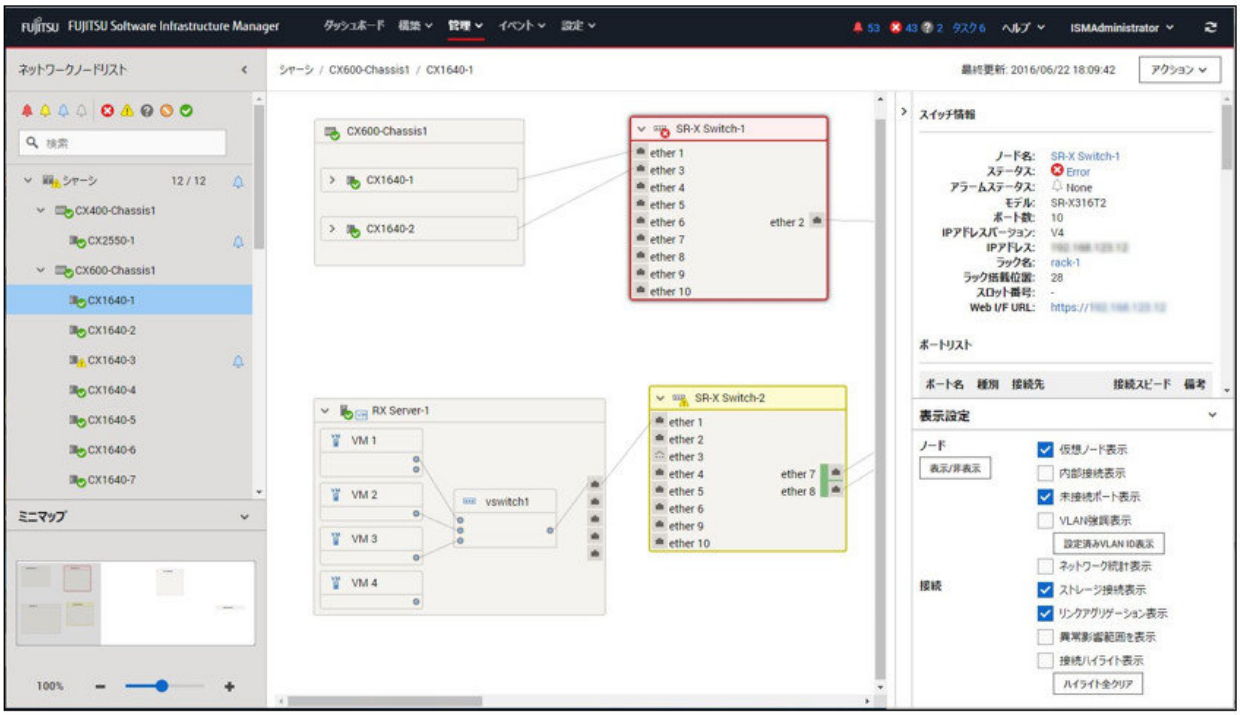
ファームウェアベースライン定義を削除すると、ファームウェアベースライン定義の割当てが解除されます。

2.7 ネットワーク管理機能

ネットワーク管理機能は主に以下の用途で利用する機能です。

- 管理対象ノード間の物理のネットワーク接続情報やポートの情報をネットワークマップで確認
- 管理対象ノード間のネットワーク接続情報の変化を確認
- 管理対象ノードの物理的なポートとそのノード上の仮想マシンや仮想スイッチ、仮想ルーターの仮想的なポートとの仮想的な接続関係をネットワークマップで確認
- 管理対象ノードのネットワーク統計情報をネットワークマップで確認
- ネットワークスイッチのVLAN、リンクアグリゲーション設定の確認、設定変更の実行

図2.25 ネットワークマップ



以下について説明します。

- 2.7.1 ネットワーク接続情報の表示
- 2.7.2 ネットワーク管理情報の更新
- 2.7.3 ネットワーク接続の変化情報の確認
- 2.7.4 ネットワーク接続の変化情報の基準設定
- 2.7.5 ネットワーク統計情報の表示
- 2.7.6 VLAN、リンクアグリゲーション設定の確認
- 2.7.7 VLAN設定の変更

- 2.7.8 リンクアグリゲーション設定の変更
- 2.7.9 手動でのネットワーク接続情報の設定

2.7.1 ネットワーク接続情報の表示

管理対象ノード間のネットワーク接続情報をネットワークマップとしてグラフィカルに確認できます。簡単な操作で各管理対象ノードやそのポートの状態を含む詳細な情報が表示されます。サーバー、ネットワークスイッチ、ストレージの接続関係を1つの画面で確認できます。加えて、管理対象ノードの物理的なポートとそのノード上の仮想マシンや仮想スイッチ、仮想ルーターの仮想的なポートとの仮想的な接続関係が確認できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

   ネットワークノードリストは、[<]アイコンを選択することで左端に格納できます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

ネットワークマップの表示の切替え

「表示設定」パネルでネットワークマップに表示する情報を切り替えることができます。

表示設定名	説明
仮想ノード表示	ネットワークマップ上での仮想ノード(仮想マシン、仮想スイッチ、仮想ルーター、CNAポート)の表示／非表示を切り替えます。
内部接続表示	ネットワークマップ上での内部接続(ファブリック内部接続、BXシャーシ内部接続)の表示／非表示を切り替えます。
ストレージ接続表示	ネットワークマップ上でのストレージとの接続に利用されるポートおよび結線の表示／非表示を切り替えます。
リンクアグリゲーション表示	ネットワークマップ上でのリンクアグリゲーション設定の表示／非表示を切り替えます。
異常影響範囲を表示	ネットワークマップ上での異常の影響範囲の表示／非表示を切り替えます。エラーなど異常がある管理対象ノードが持つ接続、隣接する接続先ノードの外枠、および接続先ポートが黄色で表示されます。なお、接続先ノードに仮想ネットワークが構築されている場合、影響がある仮想ネットワークも黄色で表示されます。
未接続ポート表示	ネットワークマップ上でのリンクダウンポートの表示／非表示を切り替えます。
接続ハイライト表示	ネットワークマップ上でのハイライト表示機能のON／OFFを切り替えます。ハイライト表示機能がONの場合、管理対象ノードまたはそのポートを選択すると、それらが持つ接続がハイライト表示されます。また、[ハイライト全クリア]を選択すると、ハイライト表示がすべてクリアされます。
VLAN強調表示	ネットワークマップ上でのVLAN強調表示の表示／非表示を切り替えます。テキストボックスに入力したVLAN IDが設定されたノード、ポートが緑色で強調表示されます。また、[設定済みVLAN ID表示]ボタンにより、ネットワークマップに表示中のノードに設定されているVLAN IDの一覧が確認できます。
ネットワーク統計表示	ネットワークマップ上でのネットワーク統計表示の表示／非表示を切り替えます。しきい値を超えた値を検出したポートおよび接続が、オレンジ色(異常しきい値超過)または黄色(警告しきい値超過)で表示されます。しきい値の設定については、「2.3.2 ネットワーク統計情報監視」を参照してください。 表示する監視項目は、本項目にチェックを付けたときに表示される選択ボックスのリストから変更できます。

表示設定名	説明
[表示/非表示]ボタン	ネットワークマップ上に表示される各ノードの表示／非表示を切り替えます。 ネットワークノードリスト、またはネットワークマップのノード名の右位置の  アイコンを選択することで、表示／非表示の切り替えができます。

ネットワークマップの表示設定の保存

ネットワークマップの表示設定を保存します。次回以降「ネットワークマップ」画面を表示する際に、保存した表示設定で「ネットワークマップ」画面が表示されます。

以下の手順でネットワークマップの表示設定を保存できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
2. [アクション]ボタンから[ネットワークマップの保存]を選択します。

   ネットワークマップの表示設定が保存されます。

ポイント

- [アクション]ボタンから[ネットワークマップの再配置]を選択することにより、ネットワークマップの表示設定を初期設定に戻せます。
- ネットワークマップでは、ネットワークノードリストから選択したノードと接続関係にあるノードが表示されます。ネットワークマップ上のノード名を選択すると、ノード内のポートが展開表示されます。
- ネットワークマップの表示設定は、ユーザーごとに保存されます。

注意

- ネットワークの物理的な接続情報は、LLDP（Link Layer Discovery Protocol）を利用して取得されます。LLDPに対応していないノードやLLDPが無効になっている場合、実際に接続が存在していても接続情報は取得できません。ノードのLLDP対応の有無、ノードのLLDP設定の有効／無効の確認方法については、各ノードの仕様を確認してください。
- 表示されるネットワークマップは、前回の[ネットワーク管理情報の取得]操作時に取得した状態、またはISMによる1日1回の定期的なネットワーク管理情報の更新時の状態になります。ノード登録後、接続変更後または異常発生時などに最新状態を確認する場合は[アクション]ボタンから[ネットワーク管理情報の取得]を実行してください。
  また、ノードのハードウェア構成変更後は、対象ノードの詳細画面で[ノード情報取得]を実行後に、[ネットワーク管理情報の取得]を実行してください。定期的なネットワーク管理情報の更新は、ローカルタイムのAM4:00に実行が開始されます。
- 仮想スイッチ、仮想マシンの接続関係を表示するためには、管理対象ノードを管理している仮想化管理ソフトウェア、および管理対象ノードのOS情報をISMに登録しておく必要があります。仮想化管理ソフトウェアの登録については「2.14.6 仮想化管理ソフトウェア管理機能」を参照してください。OS情報の登録については「2.2.1 データセンター／フロア／ラック／ノードの登録」を参照してください。
- 管理対象ノードにおいて、チーミング（ボンディング）設定されているポートのリンクステータスの表示、およびそのポートと仮想スイッチとの接続関係を表示できます。

2.7.2 ネットワーク管理情報の更新

ネットワーク接続情報は定期的に最新情報に更新されます。また、ユーザーの任意のタイミングで更新することもできます。以下はネットワーク管理情報の更新の操作手順です。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
2. [アクション]ボタンから[ネットワーク管理情報の取得]を選択します。

3. [ネットワーク管理情報の取得]ボタンを選択します。

注意

ネットワーク管理情報の更新中に、ネットワーク接続情報の取得および各ノードへの設定はできません。情報更新の完了後に操作してください。

ポイント

- ネットワーク管理情報の更新を実行する前に各管理対象ノードのノード情報を最新化してください。ノード情報の取得については、「2.2.1.3 ノード情報の管理」を参照してください。
- ネットワーク管理情報の更新は、管理対象ノードの数に応じて時間がかかります。
  - 情報更新の完了は、イベント／タスクの運用ログで更新の完了を示すイベントを確認してください。
  - ネットワーク管理情報の最終更新時刻は、ネットワークマップの右上に表示されます。
    ここで表示される時刻は、最後に行った情報の更新処理が完了した時刻です。
- ネットワーク管理情報は、1日に1度、ローカルタイムのAM4:00に定期的に更新されます。
- ネットワーク管理情報の更新は、各ノードの情報の更新後に実行することで最新化できます。

2.7.3 ネットワーク接続の変化情報の確認

ネットワークマップでは、設定された基準時点からのネットワーク接続の状態変化を確認できます。状態変化の種類には「追加」と「削除」があります。

- 追加

  接続の追加など、新規接続が検出された場合です。「追加」された接続は、ネットワークマップ上に太実線で表示されます。

- 削除

  接続断や接続の撤去により、これまで検出していた接続が存在しなくなった場合です。「削除」された接続はネットワークマップ上に太破線で表示されます。

本機能を使用してネットワーク接続の変化を捉え、ネットワークの接続断を検出し、その箇所を特定できます。

また、以下の操作手順により、ネットワーク接続の変化情報をリスト形式で確認できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. [アクション]ボタンから[接続変化情報の確認]を選択します。

   「削除」された接続情報、「追加」された接続情報をそれぞれ確認できます。

ポイント

現在設定されている「基準時点」は、「接続情報変化の確認」画面の[最終更新]の日時で確認できます。

注意

「接続情報変化の確認」画面で[更新]ボタンを選択した場合、基準時点が更新されて、変化情報が削除されます。

2.7.4 ネットワーク接続の変化情報の基準設定

ネットワーク接続の変化情報は、ある基準時点からの変化(追加、削除)を表示したものです。この基準時点を更新できます。基準時点はネットワーク接続の構成を変更した場合などに設定します。基準時点を更新すると、その時点から「追加」または「削除」によって変化したネットワーク接続情報が表示されます。

以下の操作手順で更新できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. [アクション]ボタンから[接続変化情報の確認]を選択します。最終更新の日時が現在設定されている基準時点です。

4. [更新]ボタンを選択します。

   確認画面が表示されます。

5. 内容を確認し、[はい]ボタンを選択します。

   基準時点が更新操作を実行した時刻に更新されます。

2.7.5 ネットワーク統計情報の表示

ネットワークスイッチのポートの各種統計情報(トラフィックなど)をネットワークマップ上で視覚的に確認できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. 「表示設定」パネルの[ネットワーク統計表示]にチェックを付けて、確認したいネットワーク統計情報監視項目を選択します。

   各ネットワーク統計情報監視項目に対してあらかじめ設定されたしきい値を超過したポートおよび接続が、オレンジ色(異常しきい値超過)または黄色(警告しきい値超過)で表示されます。しきい値の設定については、「2.3.2 ネットワーク統計情報監視」を参照してください。

ポイント

過去の各種統計情報(トラフィックなど)を確認するには、ネットワークスイッチのポートを選択して表示される「ポート情報」から、「ネットワーク統計情報」の[グラフ]ボタンを選択します。[グラフ]ボタンは、ネットワーク統計情報の各監視項目の値が取得できているときに表示されます。

2.7.6 VLAN、リンクアグリゲーション設定の確認

ネットワークスイッチに設定されたVLAN、リンクアグリゲーションの設定状態をネットワークマップ上で視覚的に確認できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. 確認する対象に応じて以下の操作をします。

   - VLANの場合

     「表示設定」パネルの[VLAN強調表示]にチェックを付けて、VLAN IDのテキストボックスに表示したいVLAN IDを入力します。

     指定したVLAN IDが設定されているポートおよび接続が、ネットワークマップ上に緑色で表示されます。

   - リンクアグリゲーションの場合

     ネットワークマップ上のノードのノード名を選択します。

     ノード内のポートが展開表示され、リンクアグリゲーションの設定が表示されます。

ポイント

- 「表示設定」パネルの[ID表示]を選択すると、設定済みVLAN情報を確認できます。
- 「表示設定」パネルの[リンクアグリゲーション表示]でネットワークマップ上のリンクアグリゲーション設定の表示／非表示を切り替えることができます。
- ネットワークスイッチによっては、リンクアグリゲーションではなく別の呼称(EtherChannelなど)で扱われる場合があります。ISMでは、総称してリンクアグリゲーションの名称で扱います。

2.7.7 VLAN設定の変更

ネットワークスイッチのVLAN設定を変更できます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
2. ネットワークノードリストから、設定したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. [アクション]ボタンから[VLAN一括設定]を選択します。

4. 同じVLAN IDを設定したいポートをそれぞれ選択してチェックを付け、右上の[設定]ボタンを選択します。
5. 設定するVLAN IDを入力、内容を編集し、[確認]ボタンを選択します。
6. 設定の変更内容を確認し、[登録]ボタンを選択します。

   VLAN設定が変更されます。

ポイント

VLAN設定は、ノード単位でも変更できます。[アクション]ボタンから[VLAN設定]を選択してください。

注意

- VLAN設定の内容によって、VLAN設定完了までに時間が必要な場合があります。VLAN設定完了後に画面を更新してください。VLAN設定状況は「タスク」画面で確認できます。詳細は、「2.14.4 タスク管理」を参照してください。
- VLAN設定は、ネットワークスイッチのモデルに応じて仕様が異なる場合があります。装置仕様を確認したあと、設定してください。
- 1つのポートに設定可能なVLAN IDの数は100個までとなります。
- ネットワークスイッチのモデルに応じて予約済みのVLAN IDが存在します。予約済みのVLAN IDは、設定変更できません。各ノードの仕様を確認してください。

2.7.8 リンクアグリゲーション設定の変更

ネットワークスイッチのリンクアグリゲーション設定を変更できます。

以下は、リンクアグリゲーション設定を追加する操作例です。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。
2. ネットワークノードリストから、設定したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。
3. [アクション]ボタンから[リンクアグリゲーション設定]を選択します。
4. リンクアグリゲーションを設定する対象のノード名を選び、リンクアグリゲーション設定の[追加]ボタンを選択します。
5. LAG名、動作モードを入力し、リンクアグリゲーションの設定を行うポートにチェックを付け、[確認]ボタンを選択します。
6. リンクアグリゲーションの設定内容を確認し、[登録]ボタンを選択します。

注意

- リンクアグリゲーション設定は、ネットワークスイッチのモデルに応じて仕様が異なる場合があります。装置仕様を確認したあと、設定してください。
- ネットワークスイッチのモデルに応じて設定可能なLAG名や動作モードが異なります。設定可能なLAG名の範囲や動作モードについては、各ノードの仕様を確認してください。
- VLAN IDが異なるポート同士でリンクアグリゲーションを組むことはできません。ポート同士が同じVLAN設定となっていることを確認してリンクアグリゲーション設定を変更してください。

- 異なるノード間でマルチシャーシリンクアグリゲーションを設定する場合、各スイッチに対してリンクアグリゲーション設定を変更する必要があります。マルチシャーシリンクアグリゲーションを設定するためには、ノード間でピアリンク接続しておくなど、管理対象ノードの設定を事前に行ってください。
- マルチシャーシリンクアグリゲーションの呼称(MLAGやvPCなど)、および事前設定の内容は、ネットワークスイッチの種類に応じて異なります。装置仕様を確認したあと、設定してください。

2.7.9 手動でのネットワーク接続情報の設定

自動的に物理ネットワークの接続情報が取得できない場合は、手動でネットワーク接続情報を設定できます。以下は手動での接続情報設定の操作手順です。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ネットワークマップ]を選択します。

   画面左側のネットワークノードリストに、ネットワークマップ表示対象のノード一覧がツリー構造で表示されます。

2. ネットワークノードリストから、確認したいネットワーク接続のポイントとなるノードを選択します。

   ネットワークマップを開いた時点では、ネットワークノードリストの一番上のノードが選択された状態になっています。

   画面中央にネットワークマップが表示されます。

3. [アクション]ボタンから[手動接続編集]を選択します。
4. 設定を行う両端のポートを選択し、[追加]ボタンを選択します。

   注意

   [追加]ボタンを選択したあとに、手動で行った設定をキャンセルしたい場合は、[クリア]ボタンを選択します。

5. 設定したいすべての接続情報を追加したあと、[保存]ボタンを選択します。
6. 編集内容が正しいことを確認し、[保存]ボタンを選択します。

2.8 電力制御機能(ISM 3.0.0から使用できません)

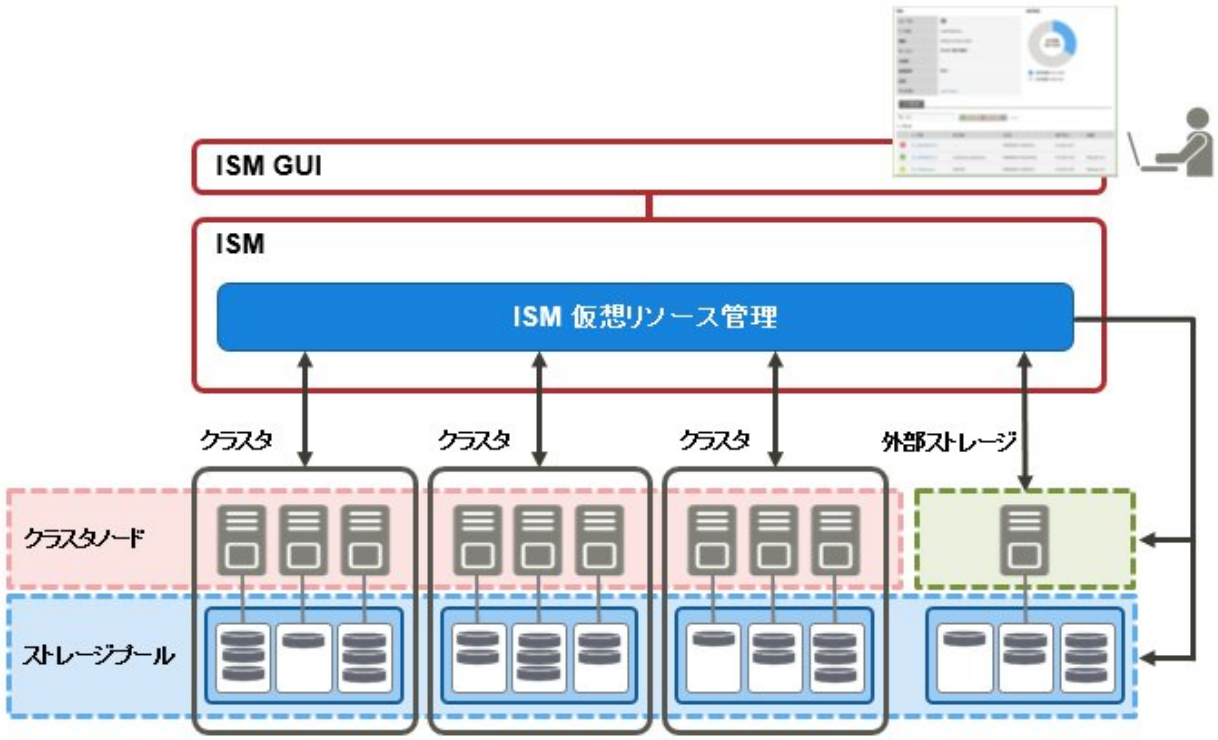
本機能は、ISM 3.0.0から使用できません。

2.9 仮想リソース管理機能

仮想リソース管理機能は、仮想リソースとして管理される要素の管理／監視を行う機能です。

本機能が動作する環境構成について、以下に示します。

図2.26 仮想リソース管理機能の動作環境の構成



注意

仮想リソース管理機能の事前設定については、「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

2.9.1 サポート対象の仮想リソース

本機能がサポートする仮想リソースは、VMware Virtual SAN および Microsoft Storage Spaces Directを構成するストレージプール、ETERNUS ストレージプールです。

ソフトウェア環境

仮想リソース管理機能が動作可能なソフトウェア環境は、SDS（Software Defined Storage）の種類とそのバージョンに依存します。また、SDSの種類に応じて必要となるハイパーバイザー、および仮想化管理ソフトウェアは異なります。

仮想リソース管理機能がサポートするソフトウェア環境は、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

注意

事前にCredSSP認証を有効にする必要があります。仮想リソース管理機能の事前設定については、「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

ETERNUSストレージ

ETERNUSのストレージについて、ISM GUIに属性情報やステータスなどを表示します。

仮想リソース管理機能がサポートするETERNUSストレージは、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

注意

ETERNUSのシン・プロビジョニングプールの表示はサポートしていません。

RAIDグループがシン・プロビジョニングプールに組み込まれている場合でも、シン・プロビジョニングプールで使用されている容量は反映されません。

シン・プロビジョニングプールの参照および管理については、ETERNUS Web GUIを使用してください。

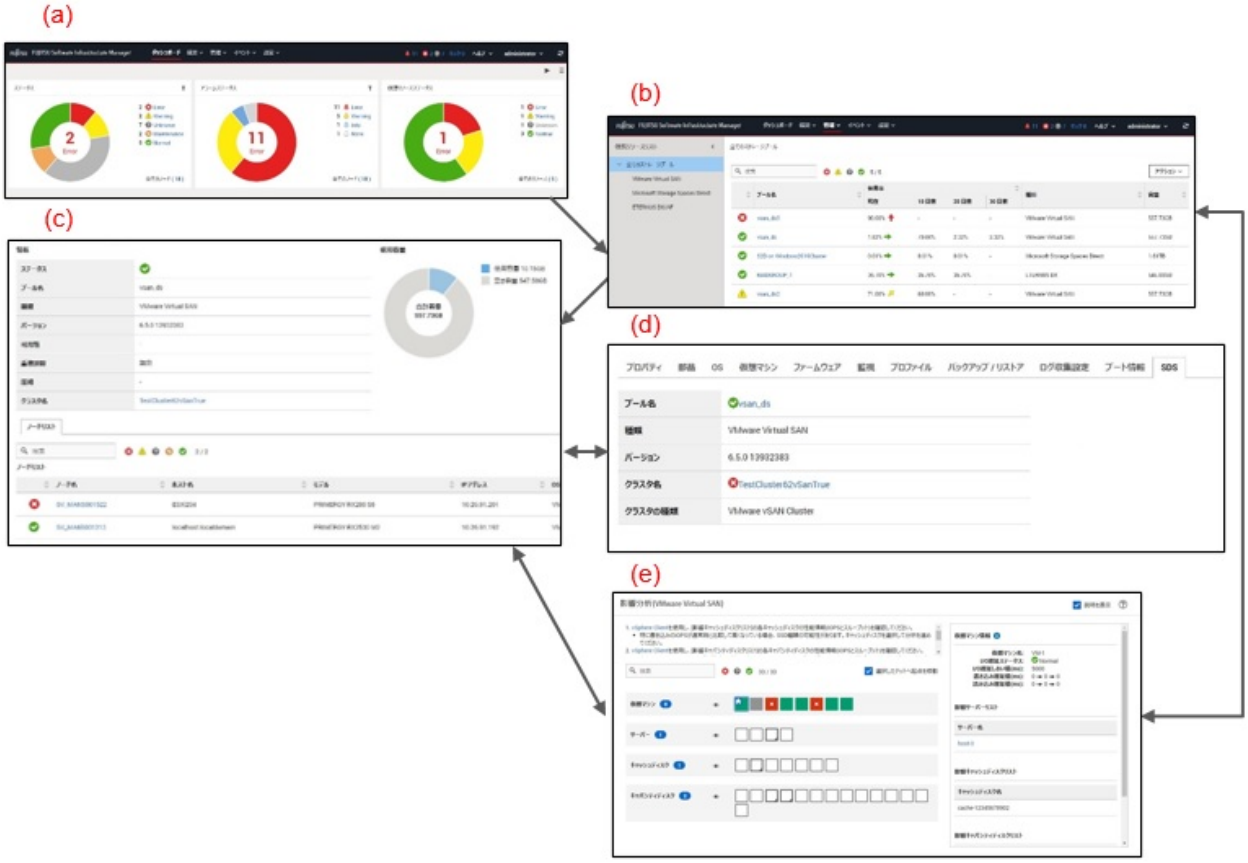
2.9.2 仮想リソース管理機能のGUI

仮想リソース管理機能のGUI画面を表示するには、グローバルナビゲーションメニューから[管理]-[仮想リソース]を選択してください。

なお、ISMのダッシュボード上に、仮想リソースリストを[ウィジェット追加]で追加することで、当該画面に遷移することもできます。

GUIの各画面の機能と、相互の表示関係について以下に示します。

図2.27 仮想リソース管理機能のGUI



(a) 仮想リソースのウィジェット表示

ISMのダッシュボード上に、ISMで管理するすべての仮想リソースの状態がウィジェットで表示されます。

(b) 仮想リソースの一覧表示

ISMで管理するすべての仮想リソースの状態一覧が表示されます。

また、リソースの使用状況が矢印の向きおよび色で表示されます。

(c) 仮想リソースの詳細情報表示

選択した仮想リソースに関して仮想リソースの設定情報や使用容量など、詳細情報が表示されます。

仮想リソースを構成する物理ノードが表示され、関連画面を表示できます。

vSANの場合、「バージョン」にはESXiのバージョンとビルド番号が表示されます。このバージョンとビルド番号から以下のサイトでvSANバージョンが確認できます。

https://kb.vmware.com/s/article/2150753

(d) ノード情報上の仮想リソース情報表示([SDS]タブ)

ノードの詳細画面にvSANまたはS2Dで構成される仮想リソースの情報を示す[SDS]タブが表示されます。

[SDS]タブを選択すると、vSANまたはMicrosoft Storage Spaces Directのノードと関連する仮想リソースの情報が表示されます。

vSANの場合、「バージョン」にはESXiのバージョンとビルド番号が表示されます。このバージョンとビルド番号から以下のサイトでvSANバージョンが確認できます。

https://kb.vmware.com/s/article/2150753

(e) 仮想マシンのvSANディスク影響の表示

[アクション]ボタンから[影響分析(VMware Virtual SAN)]を選択することで、vSANを利用している仮想マシンおよびvSANを構成するサーバーと物理ディスク(キャッシュディスク／キャパシティディスク)が一覧で表示されます。

影響分析(VMware Virtual SAN)の表示は、vSAN OSAのみサポートします。

本画面では、仮想マシンが利用しているvSANの物理ディスクと物理ディスクを搭載しているサーバーの関連を表示します。

また、仮想マシンが利用する仮想ディスクのI/O遅延情報が確認できます。

仮想マシンのI/O遅延のステータスが色で表示されます。I/Oの遅い仮想マシンを容易に把握できます。

2.9.3 仮想リソース管理の操作

仮想リソース管理機能の操作方法について説明します。

- 2.9.3.1 ストレージプールの使用状況の監視
- 2.9.3.2 ストレージプールの異常の特定
- 2.9.3.3 仮想リソース情報の更新
- 2.9.3.4 仮想マシンのvSANディスク影響の表示

ポイント

ISMで監視を行う前に、仮想リソース環境をISMに登録する必要があります。登録は、以下の手順で実施します。

1. ストレージプール(クラスタ)を構成しているノードがISMに登録済みであることを確認します。

   ノードの登録方法および情報の確認方法については、「2.2 ノード管理機能」を参照してください。

2. 仮想化管理ソフトウェアがISMに登録済みであることを確認します。

   仮想化管理ソフトウェアの登録方法および情報の確認方法については、「2.14.6 仮想化管理ソフトウェア管理機能」を参照してください。

3. 仮想リソース情報の更新を行います。

   更新方法については、「2.9.3.3 仮想リソース情報の更新」を参照してください。

   仮想リソース管理機能のGUIにストレージプール情報が表示されます。

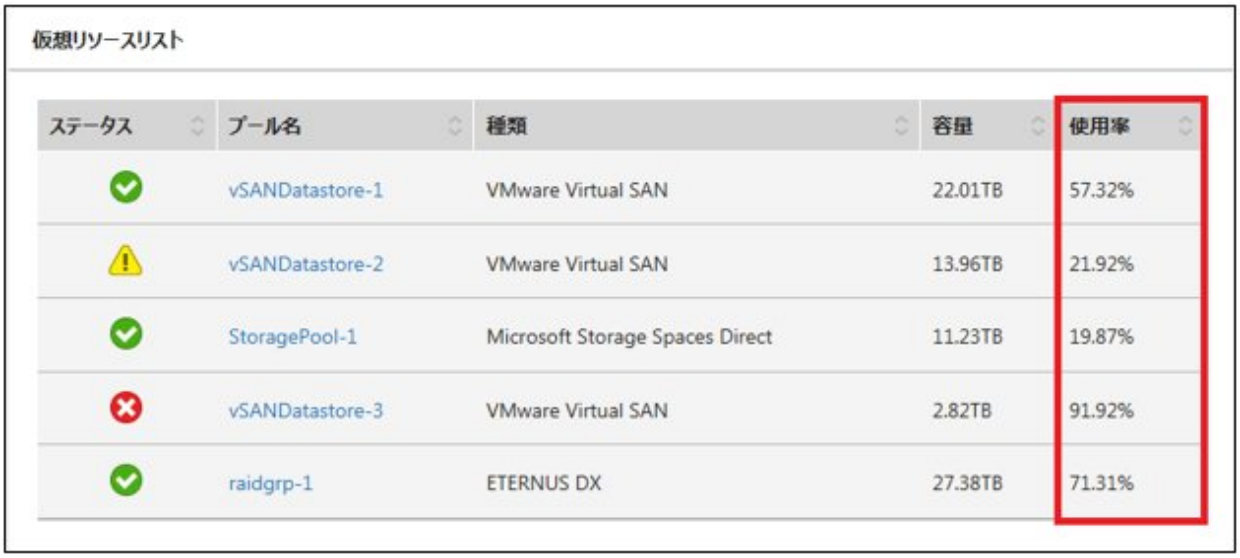
2.9.3.1 ストレージプールの使用状況の監視

ストレージプールの使用状況の監視方法について説明します。

1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択し、仮想リソースのウィジェット「仮想リソースリスト」を表示します。

   ウィジェット追加方法については、ISMのオンラインヘルプを参照してください。

   ー 「使用率」でストレージプールの現在の使用率を参照できます。



   ー 仮想リソースの一覧表示画面で、より詳しい使用状況の確認ができます。

   現在の使用率の状況を、矢印の向きおよび色から把握できます。

   ISMのGUIでグローバルナビゲーションメニューから[管理]-[仮想リソース]を選択します。ISMにより管理できる仮想リソースの一覧が、リソースの種類別にツリー表示、およびリスト表示されます。

   使用状況の見方は以下のとおりです。

   - 矢印の色

     現在の全体の使用率を示します。

     緑:使用率70%未満

     黄:使用率70%以上～90%未満

     赤:使用率90%以上

- 矢印の向き

  使用率について、10日前と比較しての増加率を表現します。

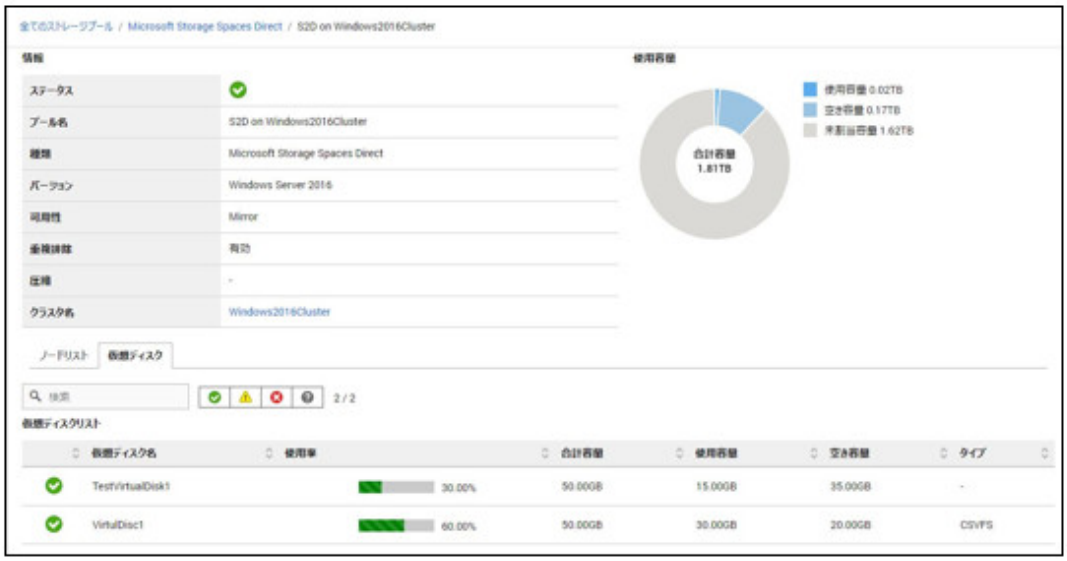
  横向き:使用率が横ばい、微増(使用率が5%未満の増加)、または減少

  斜め上向き:使用率が増加(使用率が5%以上～15%未満の増加)

  上向き:使用率が大幅に増加(使用率が15%以上の増加)

2. 詳細な情報を確認したい場合は、対象のプール名を選択して詳細情報画面を表示し、「使用容量」で使用中の容量および空き容量を確認します。

   Microsoft Storage Spaces Directの場合は、記憶域プールの容量情報に加え、記憶域プール上に作成されている仮想ディスクとその容量情報を確認できます。



   Microsoft Storage Spaces Directの使用状況の円グラフに示される各容量情報の意味は、以下のとおりです。

   ー 使用容量:記憶域プール上に存在する仮想ディスクの使用容量の合計を示します。

   ー 空き容量:記憶域プール上に存在する仮想ディスクの空き容量の合計を示します。

   ー 未割当容量:仮想ディスクが作られていない、記憶域プールの未割当ての容量を示します。

   また、[仮想ディスク]タブを選択すると、記憶域プール上に存在する仮想ディスクの一覧と、使用容量などの情報が表示されます。

   表示される内容の詳細については、ISMのオンラインヘルプを参照してください。

ポイント

[仮想ディスク]タブに表示される容量の情報は、仮想ディスクに設定された冗長性が反映されています。

「使用容量」の円グラフに表示される容量は、仮想ディスクの各容量に冗長性を考慮した値となります。

3. 空き容量が不足する場合は、以下の対処を実施します。

   ー ストレージを追加します。

     ノード一覧に、ストレージプールを構成しているノードが表示されています。空き容量が不足している場合は、これらのノードが保有するストレージの空きが少なくなっている可能性があります。

     ノードへディスクを増設するか、ノードを新たに追加して、空き容量の不足を解消します。

   ー ノードに異常が見られる場合は、必要な保守作業を実施します。

     ノード一覧に示されるステータスが異常を示している場合、そのノードのストレージが使用不可能であり、容量不足となっている可能性があります。

対象のノードに関する事象をイベントログなどで確認し、適切な保守を実施します。

2.9.3.2 ストレージプールの異常の特定

実行できるユーザー	Administratorグループ			その他のグループ		
	Admin	Operator	Monitor	Admin	Operator	Monitor

ストレージプールの異常の検出、および原因を特定する手順を説明します。

ステップ1

仮想リソースの情報を更新します。

[アクション]ボタンから、[仮想リソース情報の更新]を選択します。詳細は、「2.9.3.3 仮想リソース情報の更新」を参照してください。

GUI上の仮想リソースの情報が最新に更新されます。異常が発生している場合は、ステータスの表示が変化します。

ステップ2

異常の検出／特定を行います。

リソースの異常は、仮想リソースの一覧表示画面から確認できます。また、ダッシュボードに「仮想リソースステータス」ウィジェットを表示させている場合、そのウィジェット上に、リソースの異常が表示されます。

(1)仮想リソースの一覧表示画面から異常箇所を特定する場合

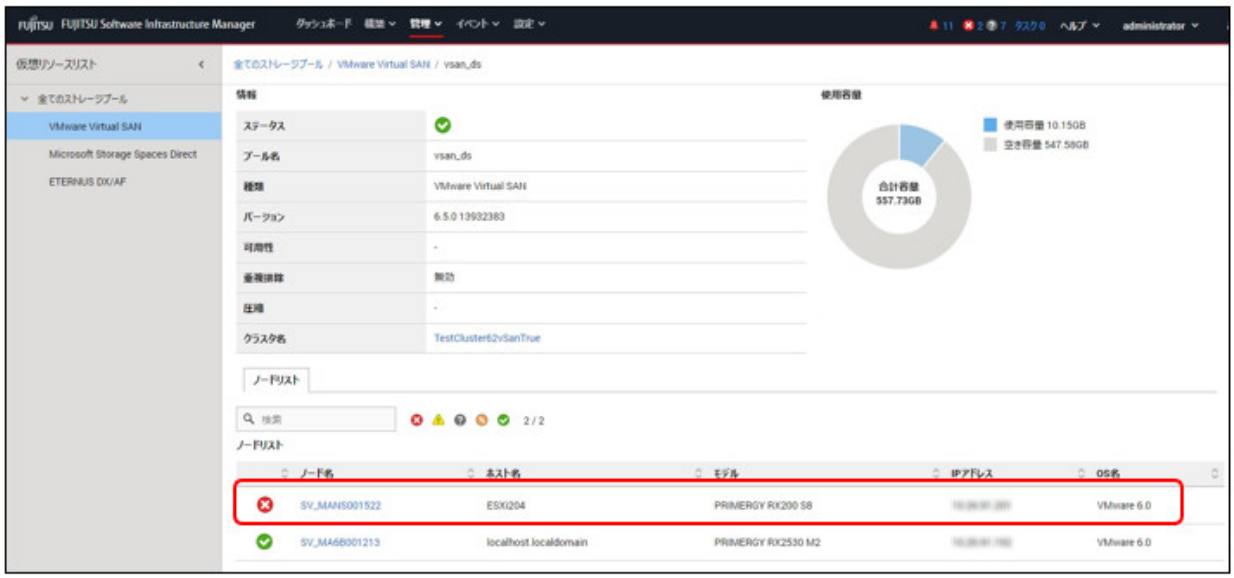
1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[仮想リソース]を選択します。

   仮想リソースの一覧表示画面が表示されます。

画面上部のステータスの絞り込みアイコンで、指定したステータスの仮想リソースを絞り込めます。

2. プール名を選択します。

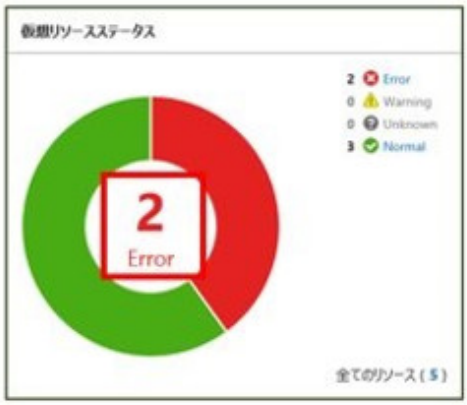
   仮想リソースの詳細情報画面が表示されるので、「ノードリスト」で、異常を示しているノード名を確認します。



(2)ダッシュボードから異常箇所を特定する場合

1. ISMのダッシュボードで、「仮想リソースステータス」ウィジェット中央に表示される数字を選択します。

   異常状態のリソース一覧が表示されます。



2. プール名を選択します。

   仮想リソースの詳細情報画面が表示されるので、「ノードリスト」で、異常を示している機器名を確認します。

ステップ3

発生している異常について、詳細を確認します。

(1)仮想リソースのステータスに異常が示されている場合

ストレージプールのステータスに異常が示されている場合、以下の状態が想定されます。

ステータス異常が発生した層	状態
物理的な層	物理的なコンポーネント(HDD、SSD、ノード)の問題により、ストレージプールに異常が発生している状態です。 SDSの種類によって、以下の状態となっています。 ・ vSANの場合、vSANの健全性に異常が発生している ・ S2Dの場合、記憶域プールを構成する物理ディスクまたはノードに異常が発生している

ステータス異常が発生した層	状態
	・ ETERNUSの場合、RAIDグループ、物理ディスク、またはETERNUS装置に異常が発生している
仮想的な層	仮想リソース(データストア)のレイヤーで異常が発生している状態です。

ステータス別のストレージプールの状態は、それぞれ以下のとおりです。

ステータス	ISM GUIでのアイコン表示	状態
Error(異常)		ストレージプールに問題が発生し、使用継続が不可能な状態です。
Warning(注意)		ストレージプールに問題は発生していますが、使用継続は可能な状態です。
Unknown(不明)		ストレージプールに問題が発生し、状態が確認できない状態です。
Normal(正常)		ストレージプールは正常な状態です。

ポイント

物理的または仮想的な層の異常によりストレージプールの容量が減少したときは、ストレージプールとして使用継続が不可能な「異常」のステータスと判断される場合があります。

異常の詳細および発生箇所については、以下のように確認します。

ポイント

詳細な異常箇所の特定や対処、または異常の復旧については、各製品のマニュアルなどに従って実施してください。

vSANの場合

ISM GUIおよびvSphere Web Clientから、ストレージビューのvSANデータストアの状態、およびvSANの「健全性」を確認します。

1. ISM GUIの仮想リソースの一覧または詳細画面から、「プール名」と「クラスタ名」を確認します。
2. vSphere Web Clientにサインインし、手順1で確認したプール名の状態の表示を[ストレージビュー]タブで確認します。

   正常ならば無印、異常ならば赤くマークされます。
3. 手順1で確認したクラスタ名を[ホストおよびクラスタ]タブで選択します。
4. [監視]タブから[Virtual SAN]-[健全性]を選択します。

   vSANの健全性の「テスト結果」を参照し、異常の内容を特定してください。

異常を復旧したあとは、以下を実施してください。

1. vSphere Web Clientにサインインし、「ホストおよびクラスタ」でクラスタ名を選択します。
2. [監視]タブから[vSAN]-[健全性]を選択して[再テスト]を実行し、テスト結果が「失敗」から「パス」に変わったことを確認します。
3. [ストレージビュー]タブを選択して表示されるデータストア一覧から、vSANデータストアの状態が正常であることを確認します。
4. ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

S2Dの場合

ISM GUIおよび管理サーバー上のサーバーマネージャーから、記憶域プールの状態、および物理ディスクの状態を確認します。

1. ISM GUIの仮想リソースの一覧または詳細画面から、「プール名」を確認します。

2. 管理サーバー上でサーバーマネージャーを開き、[ファイルサービスと記憶サービス]-[記憶域プール]を選択し、手順1で確認したプール名の状態を確認します。また、異常を示している物理ディスクを「物理ディスク」から確認します。

異常を復旧したあとは、以下を実施してください。

1. 管理サーバー上でサーバーマネージャーを開き、[ファイルサービスと記憶サービス]-[記憶域プール]を選択し、記憶域プールおよび物理ディスクが正常であることを確認します。

   表示内容が古い場合があるため、画面上部の[更新]ボタンを選択し、最新の状態にしたうえで確認してください。

2. ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

ETERNUSストレージの場合

Webブラウザーから ETERNUS Web GUIを開き、RAIDグループおよび物理ディスクの状態を確認します。

ETERNUS Web GUIのURLは、仮想リソースの詳細画面の「ノード一覧」から、ETERNUSの機種名を選択して表示されるノード情報から確認できます。

異常を復旧したあとは、ISM GUIの仮想リソース一覧画面で、[アクション]ボタンから[仮想リソース情報の更新]を選択し、ステータスが正常に戻ったことを確認します。

(2)「ノード一覧」でノードの異常が示されている場合

ISMのイベントログで、異常の詳細を確認します。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択します。

   「イベントリスト」画面が表示されます。

2. 検索ボックスに「ノード名」を入力して対象ノードのイベントを検索し、異常の内容を確認します。

2.9.3.3 仮想リソース情報の更新

仮想リソース一覧画面の[アクション]ボタンから[仮想リソース情報の更新]を実行します。

注意

タスクタイプが「Refresh Virtual Resource」のタスクはキャンセルできません。終了を待ち合わせてください。

ポイント

- GUIに表示されている情報が古いままの場合がありますので、最新状態を確認する際は必ず情報の更新を実行してください。

  更新処理はISMのタスクに登録されます。タスクのステータスが「完了」になるまでは、情報の取得が完了していません。

- GUIに表示されている情報は、以下のように定期的に自動更新されます(タスク表示はされません)。
  - ― すべての情報は、毎日ローカルタイムのAM0:00に自動更新されます。新規に登録した仮想化管理ソフトウェアで管理される情報も対象となります。
  - ― ステータスは、3分おきに自動更新されます。登録済みの仮想化管理ソフトウェアで管理される情報が対象となります。
  - ― 仮想化管理ソフトウェアをイベント出力抑止モードに設定している場合、自動更新されません。仮想化管理ソフトウェアのイベント出力抑止モードを無効にすると自動更新されます。

    仮想化管理ソフトウェアのイベント出力抑止モードについては、「2.14.6.5 仮想化管理ソフトウェアのイベント出力抑止モードの変更」を参照してください。

2.9.3.4 仮想マシンのvSANディスク影響の表示

仮想マシンのリソース影響分析(VMware Virtual SAN)の画面について説明します。

仮想マシンのリソース影響分析(VMware Virtual SAN)の画面は、vSANストレージに生成した仮想マシンにおいて、使用する物理ディスク(キャッシュディスクおよびキャパシティディスク)とこれら物理ディスクを搭載するサーバーを表示します。

サーバーの停止や物理ディスク(キャッシュディスクおよびキャパシティディスク)の性能低下が発生した時に影響を与える仮想マシンを表示します。

ポイント

仮想マシン、サーバー、キャッシュディスクおよびキャパシティディスクの構成や詳細情報を表示するためには、vSANデータストアおよびサーバーを管理している仮想化管理ソフトウェア(vCenter ServerまたはvCenter Server Appliance)、および管理対象ノードのOS情報をISMに登録しておく必要があります。

仮想化管理ソフトウェアの登録については、「2.14.6 仮想化管理ソフトウェア管理機能」を参照してください。OS情報の登録については、「2.2.1.1 データセンター／フロア／ラックの登録」を参照してください。

「影響分析(VMware Virtual SAN)」画面を表示する手順については、『操作手順書』の「6.2.4 仮想マシン／vSANストレージの状態を確認する」を参照してください。

「影響分析(VMware Virtual SAN)」画面は、仮想マシンとvSANディスク、サーバーの構成を表示する画面左側の構成表示エリアと、構成表示エリアで選択したドットの詳細を表示する画面右側の詳細情報表示エリアで構成されます。

注意

- 影響分析(VMware Virtual SAN)の表示は、vSAN OSAのみサポートします。vSAN ESAの場合は「データがありません。」と表示されます。
- 表示される「影響分析(VMware Virtual SAN)」画面の仮想マシンとvSANディスクの構成表示は、前回の[仮想リソース情報の更新]操作時に取得した状態、またはISMによる1時間1回の定期的な更新時の状態になります。

  仮想リソース管理の情報を更新した場合は、最新情報に更新する必要があります。

  ー 仮想化管理ソフトウェア(vCenter ServerまたはvCenter Server Appliance)をISMに登録または削除した場合は、以下の手順を実施します。

  ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択します。[仮想化管理ソフトウェア情報取得]を選択し、[実行]を選択します。

  ー 仮想マシンを追加または削除した場合は、以下の手順を実施します。

  ISMのGUIでグローバルナビゲーションメニューから[管理]-[仮想リソース]を選択します。「仮想リソースリスト」画面で[アクション]-[仮想リソース情報の更新]を選択し、[はい]を選択します。

  「影響分析(VMware Virtual SAN)」画面に「データがありません」が表示される場合があります。「影響分析(VMware Virtual SAN)」画面を閉じて上記の手順を実施して最新情報に更新した後、再度「影響分析(VMware Virtual SAN)」画面を表示してください。
- 「影響分析(VMware Virtual SAN)」画面は自動更新されません。最新情報を表示したい場合は「影響分析(VMware Virtual SAN)画面」を閉じて、再度「影響分析(VMware Virtual SAN)」画面を表示してください。

構成表示エリア

構成表示では、仮想マシン、サーバー、キャッシュディスク、キャパシティディスクをドットで表記します。

仮想マシンは、以下のドットで表示されます。

ステータス	ISM GUIでのドットの表示	状態
Error（異常）	 （赤色）	仮想マシンのディスク遅延が発生（I/O遅延しきい値を超えている）状態です。 ディスクの性能劣化またはデータの輻輳が考えられます。
Unknown（不明）	 （灰色）	仮想マシンのディスク遅延情報が取得できない状態です。
Normal（正常）	 （緑色）	仮想マシンは正常な状態です。

仮想マシン、サーバー、キャッシュディスクおよびキャパシティディスクは、以下のドットを表示します。

ドットの意味	ISM GUIでのドットの表示	状態
影響ありドット	 （ドット右下に三角マーク）	選択中のドットに影響することを意味します。 ドットの右下に三角マークが付きます。
影響なしドット	 （四角枠）	選択中のドットとは影響がないことを意味します。

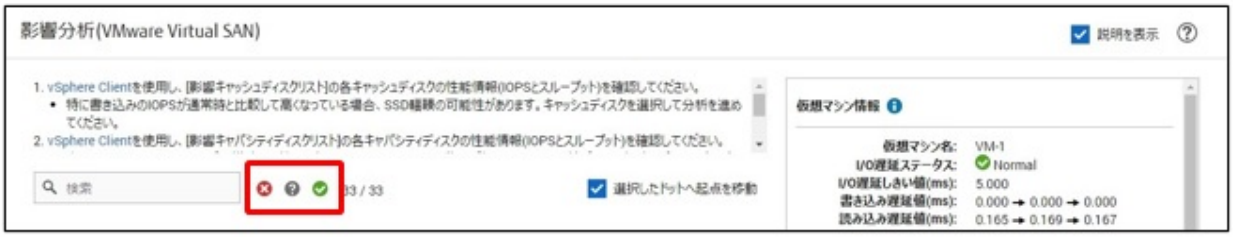
初回表示は、仮想マシンの左端のドットを選択状態で表示します。

選択中のドットには、左上に  のマークが表示され、ドットに青枠が表示されます。

表示されているドットは、フィルタリングすることができます。

「フィルター」に条件を入力することで、表示内容をフィルタリングできます。フィルターに入力された文字列に当てはまらないドットは、グレーのドットとなり選択できなくなります。

また、「フィルター」の右側にあるステータスの絞り込みアイコンで、指定したステータスのドットに絞り込めます。



仮想マシン、サーバー、キャッシュディスク、キャパシティディスクの右位置の  ／  アイコンを選択することで、対象ドットの表示／非表示の切り替えができます。

影響表示について

- [選択したドットへ起点を移動]にチェックを付けると、選択したドットに影響あるオブジェクトの表示が更新されます。
- [選択したドットへ起点を移動]のチェックを外すと、ドットの選択を変更しても影響あるオブジェクトの表示は更新されません。
- 仮想マシンを選択した場合、仮想マシンの仮想ディスクが構成するキャッシュディスク、キャパシティディスクおよび、これらのディスクを構成するサーバーが影響ありドットで表示されます。
- サーバーを選択した場合、サーバーが構成するキャッシュディスク、キャパシティディスクおよびこれらのディスクで構成される仮想マシンが影響ありドットで表示されます。
- キャッシュディスクおよびキャパシティディスクを選択した場合、選択したディスクを構成するサーバーおよび、選択したディスクで構成される仮想マシンが影響ありドットで表示されます。

詳細情報表示エリア

仮想マシンとvSANディスクの構成表示エリアで選択したドットの詳細情報を表示します。

また、影響する仮想マシン名、サーバー名、キャッシュディスク名およびキャパシティディスク名の一覧を表示します。

仮想マシンを選択した場合（仮想マシンのドットを選択した場合のみ表示）

仮想マシン名、I/O遅延ステータス、I/O遅延しきい値(ms)、書き込み遅延値(ms)、読み込み遅延値(ms)を表示します。

影響するサーバー名、キャッシュディスクの一覧、キャパシティディスクの一覧を表示します。

影響するサーバー名に表示されている[サーバー名]を選択するとそのサーバー情報のプロパティを表示します。

仮想マシン情報のI/O遅延ステータスは、以下の状態で表示されます。

ステータス	ISM GUIでのアイコン表示	状態
Error（異常）	（赤色）	ディスクのI/O遅延が発生し、ディスクのパフォーマンスが低下している状態です。
Unknown（不明）	（灰色）	ディスクのI/O遅延の情報が取得できない状態です。
Normal（正常）	（緑色）	ディスクのI/O遅延はなく、ディスクのパフォーマンスは正常な状態です。

I/O遅延ステータスが"Error(異常)"となっている仮想マシンを選択し、仮想マシンの稼働に影響するサーバー、キャッシュディスクおよびキャパシティディスクを表示します。

書き込み遅延値(ms)と読み込み遅延値(ms)は、10分前から15分前の遅延値→5分前から10分前の遅延値→最新5分間の遅延値の順で表示します。

サーバーを選択した場合（サーバーのドットを選択した場合のみ表示）

サーバー名、OSタイプを表示します。

サーバー名に表示されている[サーバー名]を選択すると、そのサーバー情報のプロパティを表示します。

影響する仮想マシンの一覧、キャッシュディスの一覧、キャパシティディスクの一覧を表示します。

キャッシュディスクを選択した場合（キャッシュディスクのドットを選択した場合のみ表示）

キャッシュディスク名、ディスク種別、影響サーバー名を表示します。

影響するサーバー名に表示されている[サーバー名]を選択すると、そのサーバー情報のプロパティを表示します。

影響する仮想マシン名の一覧、キャパシティディスクの一覧を表示します。

キャパシティディスクを選択した場合（キャパシティディスクのドットを選択した場合のみ表示）

キャパシティディスク名、ディスク種別、影響サーバー名を表示します。

影響するサーバー名に表示されている[サーバー名]を選択すると、そのサーバー情報のプロパティを表示します。

影響する仮想マシン名の一覧、キャッシュディスクの一覧を表示します。

影響するサーバー、キャッシュディスクおよびキャパシティディスクの情報からディスク性能低下の原因を分析してください。

I/O遅延のステータス表示について

I/O遅延しきい値(ms)は、5.000固定です。

I/O遅延ステータスの初期状態は、"Normal(正常)"です。

I/O遅延ステータスが"Error(異常)"と判断する条件は、以下です。

- 読み込み遅延値の3つの値すべてがI/O遅延しきい値以上の場合。
- 書き込み遅延値の3つの値すべてがI/O遅延しきい値以上の場合。

I/O遅延ステータスが"Normal(正常)"と判断する条件は、以下です。

- 読み込み遅延値の3つの値および書き込み遅延値の3つの値の合計6つの値すべてがI/O遅延しきい値未満である場合。

上記の条件以外はI/O遅延ステータスは更新されません。

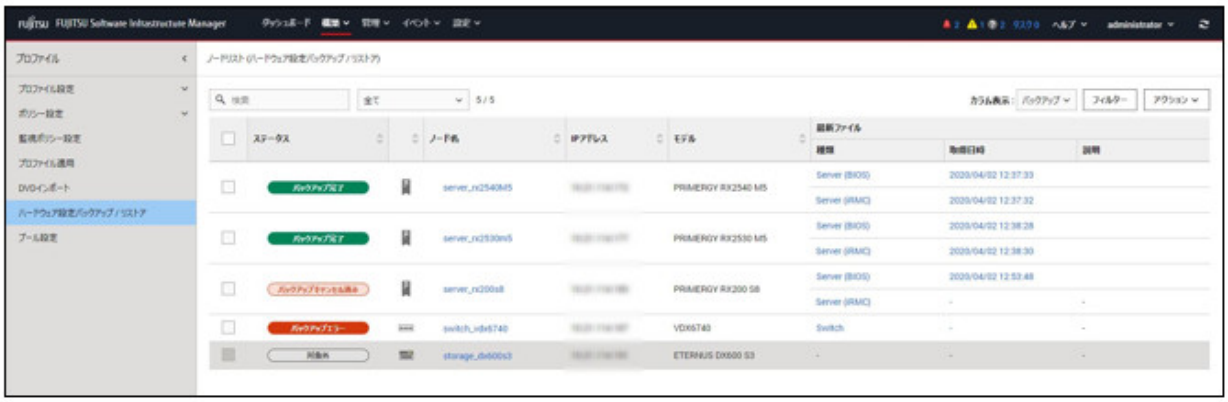
2.10 ハードウェア設定バックアップ／リストア機能

本機能は、ハードウェアの設定をファイルとして保存し、保存したファイルをエクスポートできます。対象となるハードウェア設定は、以下のとおりです。

- PRIMERGY、PRIMEQUEST 3000B、PRIMEQUEST 4000シリーズのBIOS／iRMCの設定
- VDXのスイッチの設定

エクスポートしたファイルを別のISMへインポート後、対象の機器に反映できます。インポートしたBIOS／iRMC設定のファイルをPRIMERGY、PRIMEQUEST 3000B、PRIMEQUEST 4000シリーズへ反映できます。インポートしたスイッチ設定のファイルは、VDXへ反映できます。

図2.28「ハードウェア設定バックアップ / リストア」画面例（GUI）



ポイント

- ハードウェア設定のファイルは、BIOSとiRMCで別々に保存されます。
- BIOSのハードウェア設定をバックアップする場合は、バックアップ前にサーバーの電源をオフにする必要があります。
- スイッチ設定をバックアップする場合は、バックアップ前にハードウェアの電源をオンにする必要があります。

2.10.1 ハードウェア設定のバックアップ

実行できるユーザー

Administratorグループ			その他のグループ		
Admin	Operator	Monitor	Admin	Operator	Monitor

指定したノードからハードウェア設定のバックアップを取得します。

詳細な手順については、『操作手順書』の「7.1.1 サーバーの設定をバックアップする」または「7.2.1 スイッチやストレージの設定をバックアップする」を参照してください。

2.10.2 ハードウェア設定バックアップファイルのエクスポート

実行できるユーザー

Administratorグループ			その他のグループ		
Admin	Operator	Monitor	Admin	Operator	Monitor

指定した登録済みバックアップファイルをエクスポートします。

詳細な手順については、『操作手順書』の「7.1.1 サーバーの設定をバックアップする」または「7.2.2 スイッチやストレージの設定をエクスポートする」を参照してください。

2.10.3 ハードウェア設定バックアップからのプロファイル追加

指定した登録済みバックアップをプロファイルに変換して追加します。

詳細な手順については、『操作手順書』の「7.1.2 バックアップファイルからプロファイルを作成する」を参照してください。

2.10.4 ハードウェア設定バックアップからのポリシー追加

指定した登録済みバックアップをポリシーに変換して追加します。

詳細な手順については、『操作手順書』の「7.1.3 バックアップファイルからポリシーを作成する」を参照してください。

2.10.5 ハードウェア設定バックアップファイルのインポート

エクスポートしたバックアップファイルをインポートします。

詳細な手順については、『操作手順書』の「7.1.4 サーバーの設定をインポートする」を参照してください。

2.10.6 ハードウェア設定のリストア

指定した登録済みバックアップのハードウェア設定をノードへ反映します。

詳細な手順については、『操作手順書』の「7.1.5 サーバーの設定をリストアする」を参照してください。

2.10.7 ハードウェア設定バックアップファイルの削除

指定した登録済みバックアップを削除します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ / リストア]を選択します。
3. 削除対象ノードの[最新ファイル]欄のリンクを選択します。
4. 削除対象のハードウェア設定を選択します。[アクション]ボタンから[削除]を選択します。

ポイント

複数のハードウェア設定バックアップファイルを選択して削除できます。

2.11 仮想ネットワーク パケット分析機能

本機能は、仮想ネットワークのトラフィック状況および性能情報を可視化します。

取得した情報により、ポートごと、ネットワークごと、ホストごとの通信量の傾向が確認できます。さらに通信品質の状況を確認することで、問題箇所の特定を容易にし、通信品質改善を支援します。

以下のような機能を提供します。

- 監視対象ホストから取得した性能統計情報の表示
- 送受信エラー率、ドロップ率のしきい値監視
- パケット分析による通信量および通信品質情報の表示 [注]
- ボトルネック分析によるネットワーク品質低下要因の特定・改善の支援 [注]

[注]:監視対象ホストのハイパーバイザーに対して分析VMをデプロイします。

ポイント

仮想化環境のトラフィックを解析するための仮想マシンを「分析VM」と呼びます。

2.11.1 サポート対象

本機能が対応するソフトウェア環境は、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

注意

仮想ネットワークアダプターを監視するにあたり、対象のハイパーバイザー、仮想化管理ソフトウェアにあらかじめ設定が必要な場合があります。

2.11.2 分析VMの確認

本機能がサポートする分析VMバージョンは以下のとおりです。

- Infrastructure Manager 分析VM for VMware V2.0.0

本機能を使用するためには、分析VMが動作するホストに以下のリソースが追加で必要です。

追加CPUコア数	追加メモリー容量	追加ディスク容量
2コア	16GB	40GB

2.11.3 仮想ネットワーク パケット分析機能の表示項目

本機能は、仮想ネットワークにおける以下の情報を可視化します。なお、データ保持期間は1か月以内です。

表2.15 監視対象ホストから取得した性能統計情報

表示項目	説明
CPU使用率	対象ホスト上の物理CPUの使用率を表示します。
VM vCPUの使用率	対象ホスト上で動作する仮想マシンごとの仮想CPUの使用率を表示します。

表示項目	説明
仮想ネットワークアダプターのCPU使用率 [注]	仮想ネットワークアダプター単位でのCPU使用率を表示します。
仮想ネットワークアダプターの通信量 [注]	仮想ネットワークアダプターごとの送受信パケットの送受信量、エラーパケット数、ドロップ数を表示します。

[注]:監視できる仮想ネットワークアダプターの上限は1000です。

表2.16 パケット分析による通信量および通信品質情報

分析VM監視対象	説明
ポートごとの通信量	TCP/UDPのポートごとの送受信パケット情報を表示します。
ネットワークごとの通信量	サブネットごとの送受信パケット情報を表示します。
ホストごとの通信量	ホストごとの送受信パケット情報を表示します。
ホストごとの通信品質	ホストごとのTCPの通信品質(ロス数、遅延時間など)を表示します。

2.11.4 仮想ネットワーク パケット分析機能の機能差

仮想ネットワーク パケット分析機能のサポート機能は以下のとおりです。

サポート機能	表示項目
監視対象ホストから取得した性能統計情報	CPU使用率 [注1]
	VM vCPUの使用率
	仮想ネットワークアダプターのCPU使用率 [注2]
	仮想ネットワークアダプターの通信量 [注3]
パケット分析による通信量および通信品質情報	ポートごとの通信料
	ネットワークごとの通信量
	ホストごとの通信量
	ホストごとの通信品質

[注1]:プロセスのCPU利用情報は表示できません。

[注2]:CPUスケジューラ情報は表示できません。

[注3]:ドロップパケット数のみ表示できます。

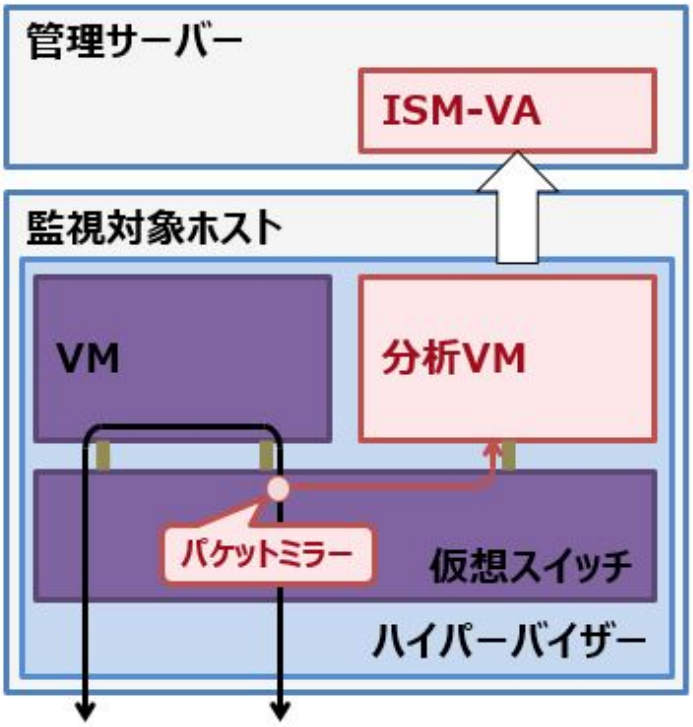
Xenは利用できません。

2.11.5 仮想ネットワーク パケット分析機能の動作

仮想ネットワーク パケット分析機能を利用するには、通信性能の低下が発生している監視対象ホスト上のハイパーバイザーに対して、分析VMをデプロイします。分析VMが仮想スイッチ上に流れる実パケットを分析し、性能低下原因の特定に必要な情報を取得します。取得対象は以下のとおりです。

- ポート番号(TCP/UDP)ごと、端末(VM)ごと、セッションごとの性能情報
- 通信量、パケットロス数、通信遅延量などの品質劣化情報

図2.29 仮想ネットワーク パケット分析の動作イメージ



ポイント

- 分析VMは、キャプチャしたパケットのヘッダ情報（L2, L3, L4 ヘッダ）のみ解析しています。
- ヘッダ情報の解析後は、キャプチャした情報を保存せずに破棄しており、保持することはありません。

2.11.6 仮想ネットワーク ボトルネック分析機能の表示項目

仮想ネットワーク ボトルネック分析機能は、仮想ネットワークパケット分析機能で取得した情報を元に性能低下原因を分析し、その要因を表示します。

想定される要因として表示される項目は以下のとおりです。

表2.17 ボトルネック分析によって表示される要因

要因	説明
送信スレッドの過負荷	送信スレッドのCPU使用率が高いため、分析対象VMに関する通信でパケットロスが発生していると思われます。
VMの過負荷	分析対象VMのCPU使用率が高いため、分析対象VMに関する通信でパケットロスが発生していると思われます。
送信スレッドのリソース競合	他プロセスによる影響により分析対象VMに関する通信でパケットロスが発生していると思われます。
VMのリソース競合	他プロセスによる影響により分析対象VMに関する通信でパケットロスが発生していると思われます。
仮想NICの送信バッファサイズ不足	仮想NICの送信バッファのサイズが小さいために分析対象VMに関する通信でパケットロスが発生していると思われます。
仮想NICの受信バッファサイズ不足	仮想NICの受信バッファのサイズが小さいために分析対象VMに関する通信でパケットロスが発生していると思われます。

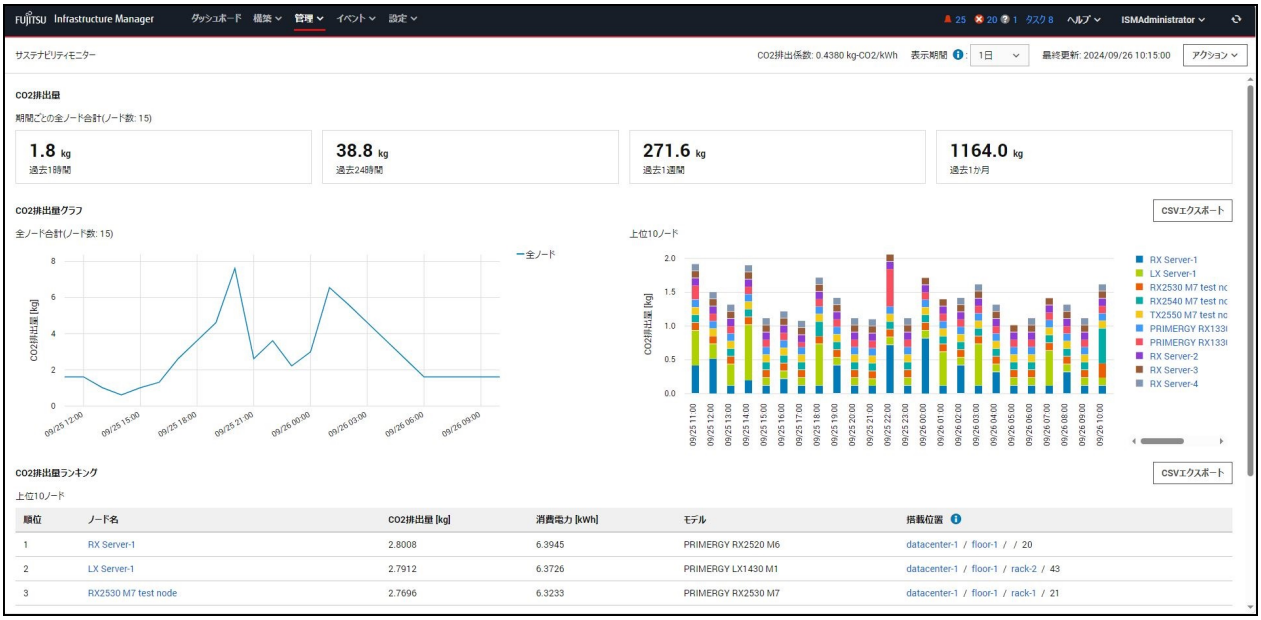
2.12 サステナビリティモニター機能

サステナビリティモニター機能は、ノードの消費電力を監視し、1時間当たりのCO2排出量に換算したデータを可視化・提供する機能です。

例として以下のような用途に利用できます。

- CO2の排出実績を過去1か月前まで遡って確認
- CO2の排出傾向を分析し、サーバーの電力制御設定を実施
- 年ごとのCO2削減効果を測定するために、年間のCO2総排出量を集計

図2.30 サステナビリティモニター



2.12.1 サポート対象

本機能の対象機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

注意

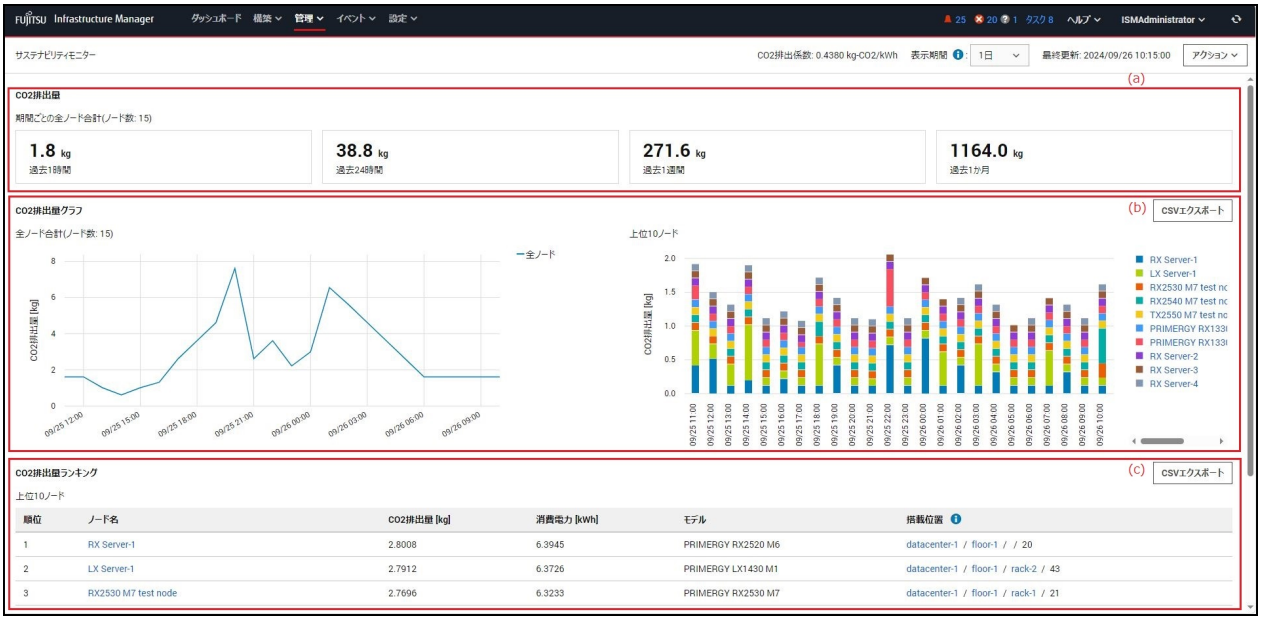
- ノードの監視項目の消費電力を削除している場合は、本機能の対象となりません。
- 以下の場合、データを取得できません。該当する期間のデータは0になります。
  - ー ノードがメンテナンスモードになっている場合
  - ー ISMのサービスが停止している場合

2.12.2 サステナビリティモニターのGUI

サステナビリティモニターのGUI画面を表示するには、グローバルナビゲーションメニューから[管理]-[サステナビリティモニター]を選択してください。

GUI画面の内容について、以下に示します。

図2.31 サステナビリティモニターのGUI



(a) CO2排出量

全てのノードのCO2排出量の合計値が期間毎に表示されます。合計値は、過去1時間、過去24時間、過去1週間、過去1か月の4種類になります。

直近のCO2排出量を容易に把握できます。

(b) CO2排出量グラフ

「表示期間」のプルダウンボックスで選択した期間内のCO2排出量がグラフ化して表示されます。

選択した期間のCO2排出量の推移が確認できます。

表示されるグラフは以下の2種類となります。

- 全ノード合計

  全てのノードのCO2排出量の合計値が折れ線グラフで表示されます。

- 上位10ノード

  CO2排出量が多い上位10ノードのCO2排出量が積み上げ棒グラフで表示されます。また、各ノードのグラフまたは、凡例のノード名を選択すると、ノード詳細画面が表示され、選択したノードの詳細情報を確認できます。

「表示期間」のプルダウンボックスを変更すると、グラフの表示単位が変更されます。

- 1日:過去24時間分のデータを1時間単位で表示
- 1週間:過去7日分のデータを1日単位で表示
- 1か月:過去30日分のデータを1日単位で表示

(c) CO2排出量ランキング

「表示期間」のプルダウンボックスで選択した期間内のCO2排出量が多い上位10ノードがランキングで表示されます。

選択した期間のCO2排出量が多いノードを容易に把握できます。

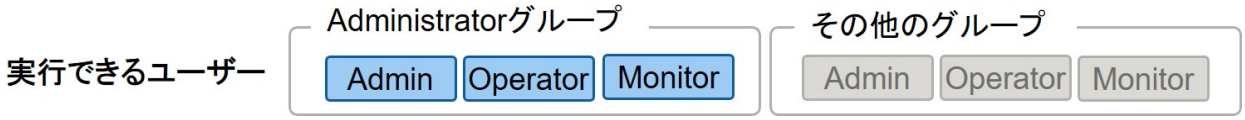
ノード名を選択すると、ノード詳細画面が表示され、選択したノードの詳細情報を確認できます。また、搭載位置を選択すると、それぞれ「データセンター詳細」画面、「フロア詳細」画面、「ラック詳細」画面が表示されます。

2.12.3 CO2排出係数の設定

CO2排出量の計算に使用するCO2排出係数をユーザーが設定することができます。CO2排出係数は利用する電気事業者毎に異なるため、ユーザーが適切な係数を調べて設定する必要があります。CO2排出係数は各国の省庁や電気事業者等が公開している情報を別途確認してください。初期値は0.438です。

詳細な手順については、『操作手順書』の「4.12.1 CO2排出係数を設定する」を参照してください。

2.12.4 CSVのエクスポート



サステナビリティモニター機能で表示しているデータをCSV形式でエクスポートすることができます。

CSVファイルの設定項目、記載例は、以下のとおりです。

表2.18 ノード毎のCO2排出量・消費電力量の推移

項目名	説明
Node Name	ノード名
CO2 Emissions	ノードのCO2排出量
Power Consumption	ノードの消費電力量
Model Name	ノードのモデル名
Mounting Position	ノードの搭載位置
Date and Time	集計日時 ISM GUIのタイムゾーンの日時で出力されます。

CSVファイルの内容は、ノード毎の1時間単位のCO2排出量・消費電力量データです。
1時間単位や1日単位でCO2排出量の合計値を算出することで、CO2排出量グラフ - 全ノード合計の折れ線グラフを再現することができます。

表2.19 ノード毎のCO2排出量・消費電力量の推移のデータ例

Node Name	CO2 Emissions [kg]	Power Consumption [kWh]	Model Name	Mounting Position	Date and Time
Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31	2024-08-01 12:00:00
Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33	2024-08-01 12:00:00
Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35	2024-08-01 12:00:00
Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31	2024-08-01 11:00:00
Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33	2024-08-01 11:00:00
Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35	2024-08-01 11:00:00
…	…	…	…	…	…

表2.20 CO2排出量ランキング

項目名	説明
Collection Period	集計期間 設定値:one day、one week、one monthのいずれか
Ranking	集計期間でのCO2排出量の順位
Node Name	ノード名
CO2 Emissions	ノードのCO2排出量
Power Consumption	ノードの消費電力量
Model Name	ノードのモデル名
Mounting Position	ノードの搭載位置

CO2排出量ランキングに表示されているランキングデータです。
1日、1週間、1か月の期間毎のデータを含みます。

表2.21 CO2排出量ランキングのデータ例

Collection Period	Ranking	Node Name	CO2 Emissions [kg]	Power Consumption [kWh]	Model Name	Mounting Position
one day	1	Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31
one day	2	Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33
one day	3	Server003	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35
…	…	…	…	…	…	…
one day	10	Server010	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 30-31
one week	1	Server001	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 32-33
one week	2	Server002	1.2345	2.3456	PRIMERGY RX2530 M7	DC1 / Floor1 / Rack1 / 34-35
…	…	…	…	…	…	…

詳細な手順については、『操作手順書』の「4.12.2 CO2排出量や消費電力のデータをエクスポートする」を参照してください。

また、エクスポートに必要なディスク容量の見積り方については、「3.2.1.7 サステナビリティモニター機能のCSVエクスポートに必要な容量の見積り」を参照してください。

2.13 ISM for PRIMEFLEXの機能

ISM for PRIMEFLEXの機能は、ISMに仮想化基盤向け拡張機能を追加したものです。ISMの機能に加えて、以下の機能を提供します。
ISMの動作モードがAdvanced for PRIMEFLEXモードで使用できる機能です。ISMの動作モードがAdvancedモードの場合「クラスタ管理機能」を使用できます。

- 2.13.6 バックアップ機能
- 2.13.7 リストア機能
- 2.13.8 クラスタ停止機能
- 2.13.9 VMware vSANクラスタに関連するログ一括収集
- 2.13.10 世代切替機能

ISM for PRIMEFLEXの機能を使用するためには、『PRIMEFLEXデザインガイド』、『PRIMEFLEXオペレーション&メンテナンスガイド』、『PRIMEFLEXサーバ増設ガイド』を事前に確認してください。

入手先:

- PRIMEFLEX HSV1.0/V1.1、PRIMEFLEX for VMware vSAN V1

  当社担当営業までお問い合わせください。

- PRIMEFLEX for VMware vSAN V2、PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

入手できない場合には、当社担当営業までお問い合わせください。

2.13.1 クラスタ管理機能

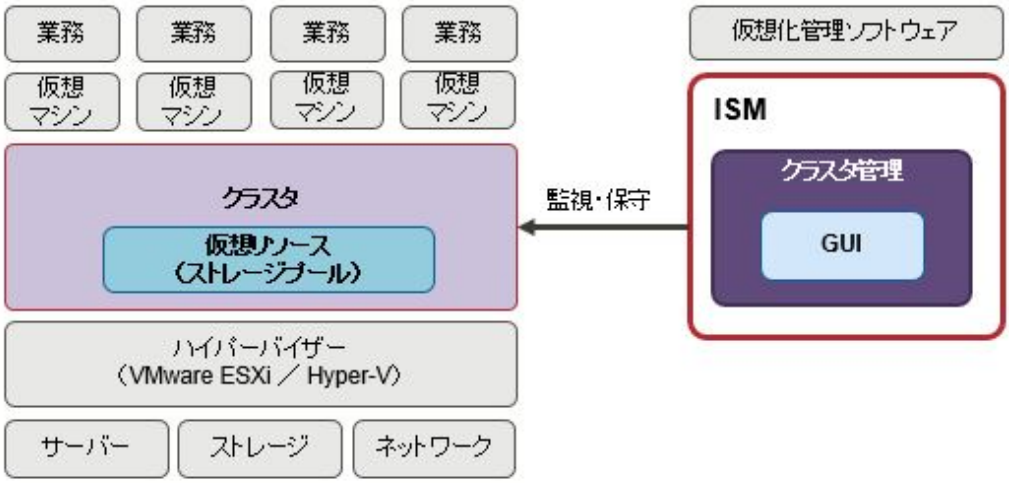
クラスタ管理機能は、クラスタの状態を表示する機能を提供します。

クラスタを構成するハードウェア機器(ノード)の状態と連動した監視、およびストレージプールなどの仮想的なストレージ環境(Software Defined Storage(以降、「SDS」と表記))の監視を可能とし、クラスタのスムーズな保守やリソースの追加(プロビジョニング)の判断に活用できます。

管理可能なクラスタの種類と要件については、「2.13.1.2 クラスタ管理機能のサポート対象」を参照してください。

ISMの動作モードがAdvancedモードの場合に使用できます。

図2.32 クラスタ管理機能の動作概要



クラスタ管理機能は、以下のような機能を備えます。

- クラスタの一覧表示と、クラスタの状態などのサマリ表示
- クラスタの詳細情報の表示

  クラスタの構成情報について、以下のような情報を表示します。

  ー クラスタのノード情報

  ー クラスタ上の仮想リソースの情報

ー クラスタ作成およびクラスタ拡張のパラメーター設定情報（Advancedモードでは使用できません）

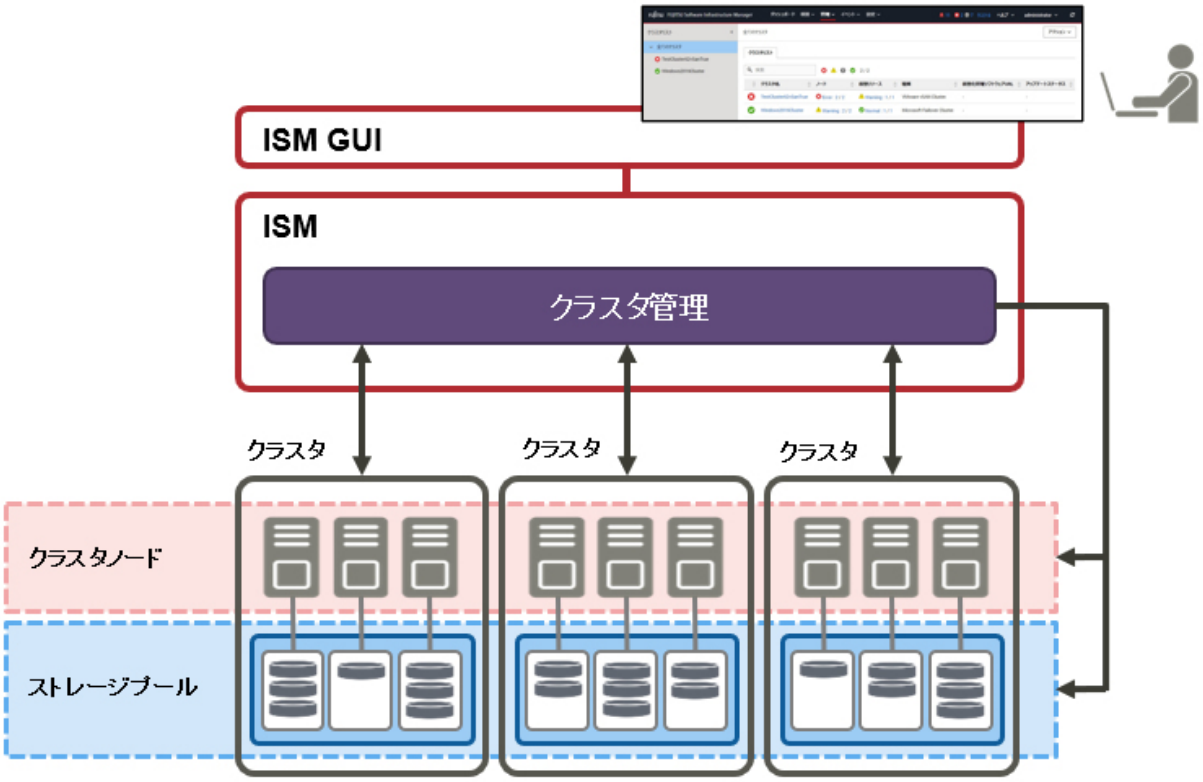
- ダッシュボードからのクラスタ監視を可能とするウィジェット

2.13.1.1 クラスタ管理機能のGUI

ISM GUIで、クラスタの監視および管理ができます。

クラスタ管理機能が動作する環境の構成について、以下に示します。

図2.33 クラスタ管理機能の動作環境の構成



各画面の機能と、相互の表示関係について以下に示します。

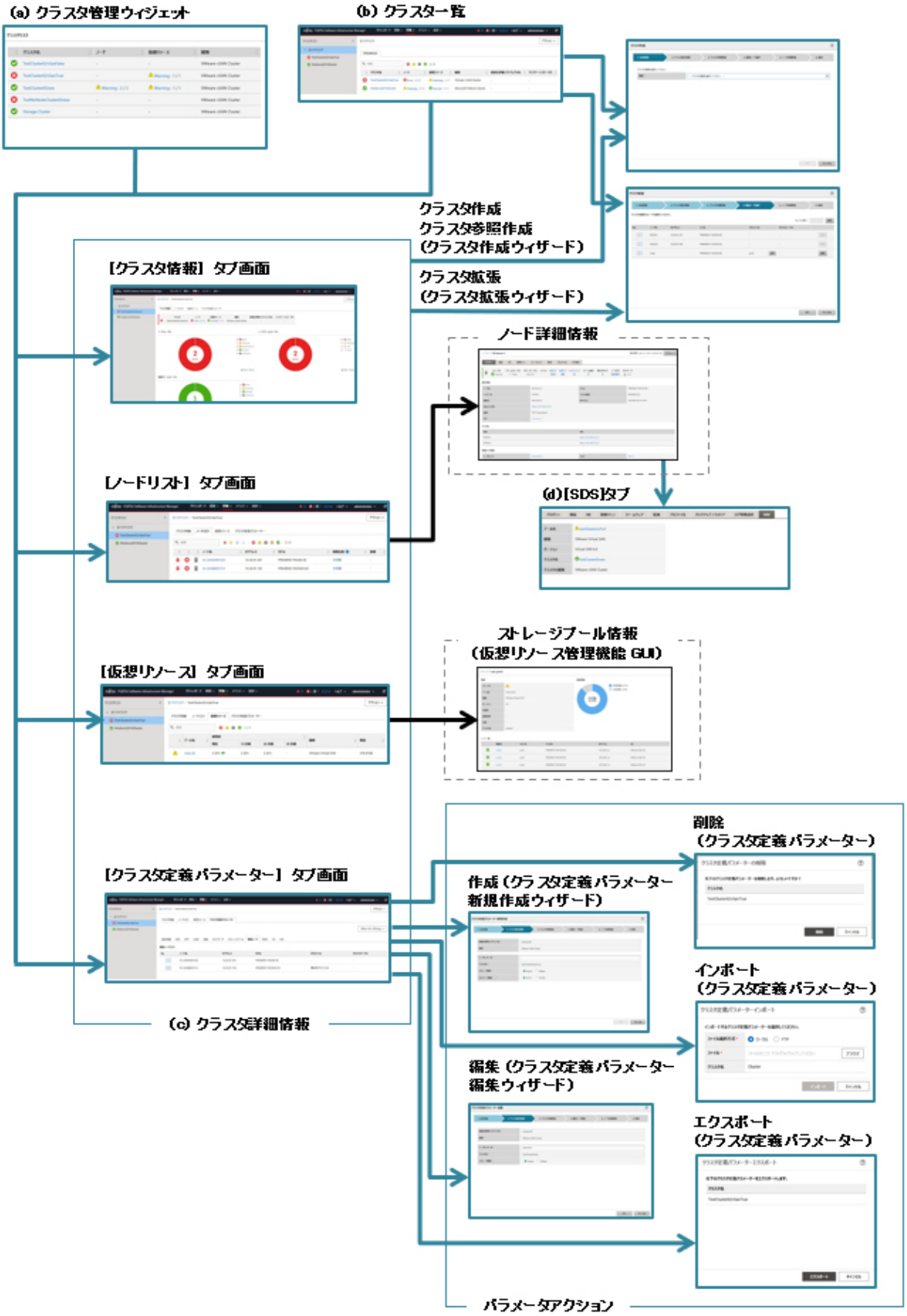
クラスタ管理機能のGUI（図2.34 クラスタ管理機能のGUI中の(a)～(d)）でクラスタに関する各種情報を表示します。

また、ノード情報（「ノードリスト」画面）や仮想リソース情報（仮想リソース管理機能のGUI）などとも連携し、より詳細な情報の確認ができます。

ノードリスト、および仮想リソース管理機能のGUIについては、「2.9.2 仮想リソース管理機能のGUI」を参照してください。

また、GUIの表示項目と説明については、ISMのオンラインヘルプを参照してください。

図2.34 クラスタ管理機能のGUI



(a) クラスタ管理ウィジェット

ISMのダッシュボード上に、クラスタ管理のウィジェットが表示されます。

ウィジェットからISM上で監視されているクラスタの情報や状態などが確認できます。

詳細は、「ダッシュボードとの連携」を参照してください。

(b) クラスター覧

クラスタの一覧が表示されます。

クラスタ名を選択すると、「(c) クラスタ詳細情報」の各種管理画面が表示されます。

(c) クラスタ詳細情報

クラスタおよびクラスタを構成する各要素の情報を、タブの切替えにより表示します。

タブ表示される画面の詳細については、「クラスタの詳細画面(タブ表示画面)」を参照してください。

(d) ノード情報上のクラスタ情報([SDS]タブ)

ノードの詳細画面に仮想リソースの情報を示す[SDS]タブが表示されます。

[SDS]タブを選択すると、ノードと関連するクラスタの情報が表示されます。詳細は、「ノード情報との連携([SDS]タブ)」を参照してください。

クラスタ管理機能のGUIの内容について、以下に説明します。

クラスター覧画面

ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択すると、クラスター覧画面が表示されます。

ISMにより管理できるクラスタの一覧がリスト表示されます。

リスト表示では、クラスタおよびクラスタを構成する各要素の状態が表示されます。

図2.35 クラスター覧画面

クラスタの詳細画面(タブ表示画面)

クラスター覧画面のクラスタ名を選択するとクラスタの詳細画面が表示され、クラスタおよびクラスタを構成する各要素の情報を確認できます。

この画面では、リソースの設定、使用状況、リソースを構成するノード一覧など、クラスタ管理に関する情報が表示されます。

[クラスタ情報]タブ

クラスタおよびクラスタを構成する要素の情報がサマリ表示されます。

クラスタの情報(クラスタ名)、ノードの状態(ステータス、アラーム)、仮想リソースの状態が表示されます。

[ノードリスト]タブ

クラスタを構成するノードの情報が一覧表示されます。ノードの状態、位置情報などが表示されます。

ノード名を選択すると、ノードの詳細画面へ遷移し、ハードウェア情報など詳細なノードの状態や構成情報を確認できます。

ノードの詳細画面の説明については、ISMのオンラインヘルプを参照してください。

[仮想リソース]タブ

クラスタ内に作成されるSDSのストレージプール情報が一覧表示されます。

ストレージプール名を選択すると、仮想リソースの詳細情報画面が表示され、ストレージプールの情報が表示されます。

仮想リソース管理機能のGUIについては、「2.9.2 仮想リソース管理機能のGUI」、またはISMのオンラインヘルプを参照してください。

[リソース変動予測]タブ

[リソース変動予測アクション]ボタンを選択し、メニューを選択すると起動されるウィザードに従って予測を実施します。

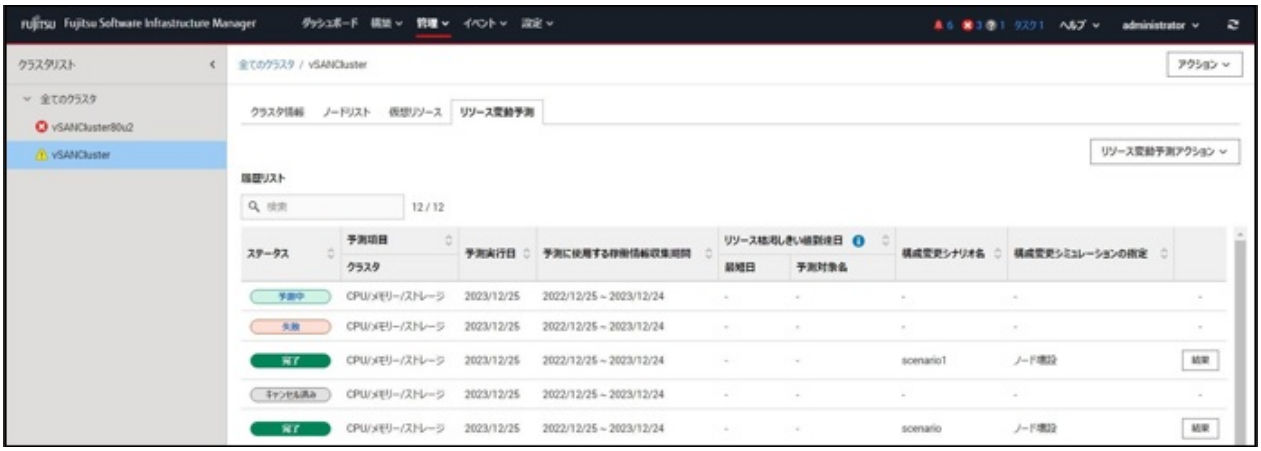
また、構成変更シミュレーションを利用することで、将来のリソース変動を見積ることができます。

構成変更シミュレーションとは、リソースに対して周期性やトレンドの変化を考慮した予測結果から構成変更時のリソース量を考慮した使用量および使用率の予測結果を出力する機能です。

履歴リストに、実施したリソース変動の予測結果が表示されます。

[結果]ボタンを選択すると、予測をグラフ化して表示します。

リソース変動予測の画面の説明については、ISMのオンラインヘルプを参照してください。



[クラスタ定義パラメーター]タブ（Advancedモードでは非表示）

クラスタの作成、およびクラスタへサーバーを拡張する際に参照されるパラメーターの情報が表示されます。

パラメーター情報は、以下のタブの切替えにより参照できます。

表示される情報については、『ISM for PRIMEFLEX 設定値一覧』、またはISMのオンラインヘルプを参照してください。

タブ名	説明
CMS	仮想化管理ソフトウェアの情報が表示されます。
基本情報	クラスタ名などクラスタの基本情報が表示されます。
DNS	クラスタのDNS情報が表示されます。
NTP	クラスタのNTP情報が表示されます。[注1]
LDAP	クラスタのLDAP情報が表示されます。
機能	vSANおよびvSphereの設定情報が表示されます。[注1]
ネットワーク	クラスタのネットワーク情報が表示されます。[注2]

タブ名	説明
ストレージプール	クラスタのストレージプールの情報が表示されます。
構成ノード	クラスタを構成するノードの情報が表示されます。
iRMC	iRMCのユーザーの設定情報が表示されます。
OS	OSのローカルユーザーの設定情報が表示されます。
vDS	分散仮想スイッチ(vDS:virtual Distributed Switch)の設定情報が表示されます。[注1]
仮想スイッチ	仮想スイッチの設定情報が表示されます。[注3]

[注1]:クラスタの種類が「VMware vSAN Cluster」の場合に表示されます。

[注2]:クラスタの種類が「VMware vSAN Cluster」と「Microsoft Failover Cluster」の場合に固有情報が表示されます。

[注3]:クラスタの種類が「Microsoft Failover Cluster」の場合に表示されます。

また、[パラメーターアクション]ボタンから、以下のパラメーター操作ができます。

[パラメーターアクション]ボタンを選択し、メニューを選択すると起動されるウィザードまたは画面に従って設定値を入力します。

ウィザードの設定項目については、『ISM for PRIMEFLEX 設定値一覧』を参照してください。また、詳細な設定方法については、ISMのオンラインヘルプを参照してください。

ー 作成

「クラスタ定義パラメーター新規作成」ウィザードが表示され、パラメーターを作成できます。

ー 編集

「クラスタ定義パラメーター編集」ウィザードが表示され、パラメーターを編集できます。

ー 削除

「クラスタ定義パラメーター削除」画面が表示され、パラメーターを削除できます。

ー インポート

「クラスタ定義パラメーターインポート」画面が表示され、パラメーターをインポートできます。

ー エクスポート

「クラスタ定義パラメーターエクスポート」画面が表示され、パラメーターをエクスポートできます。

アクションメニュー

画面右上の[アクション]ボタンを選択すると以下のメニューが表示され、クラスタに関する操作を行うことができます。

- クラスタ情報取得・更新

  本メニューを選択すると、クラスタ情報取得、または情報を更新します。

  操作方法については、「2.13.1.3 クラスタ情報の取得と更新」を参照してください。

- クラスタ作成(Advancedモードでは非表示)

  本メニューを選択すると、「クラスタ作成」ウィザードが起動されます。ウィザードに従ってクラスタを作成します。

  詳細については、「2.13.2 クラスタ作成機能」を参照してください。手順については、『操作手順書』を参照してください。

- クラスタ参照作成(Advancedモードでは非表示)

  本メニューを選択すると、「クラスタ作成」ウィザードが起動されます。ウィザードに従ってクラスタを参照作成します。

  詳細については、「2.13.2 クラスタ作成機能」を参照してください。手順については、『操作手順書』を参照してください。

- クラスタ拡張(Advancedモードでは非表示)

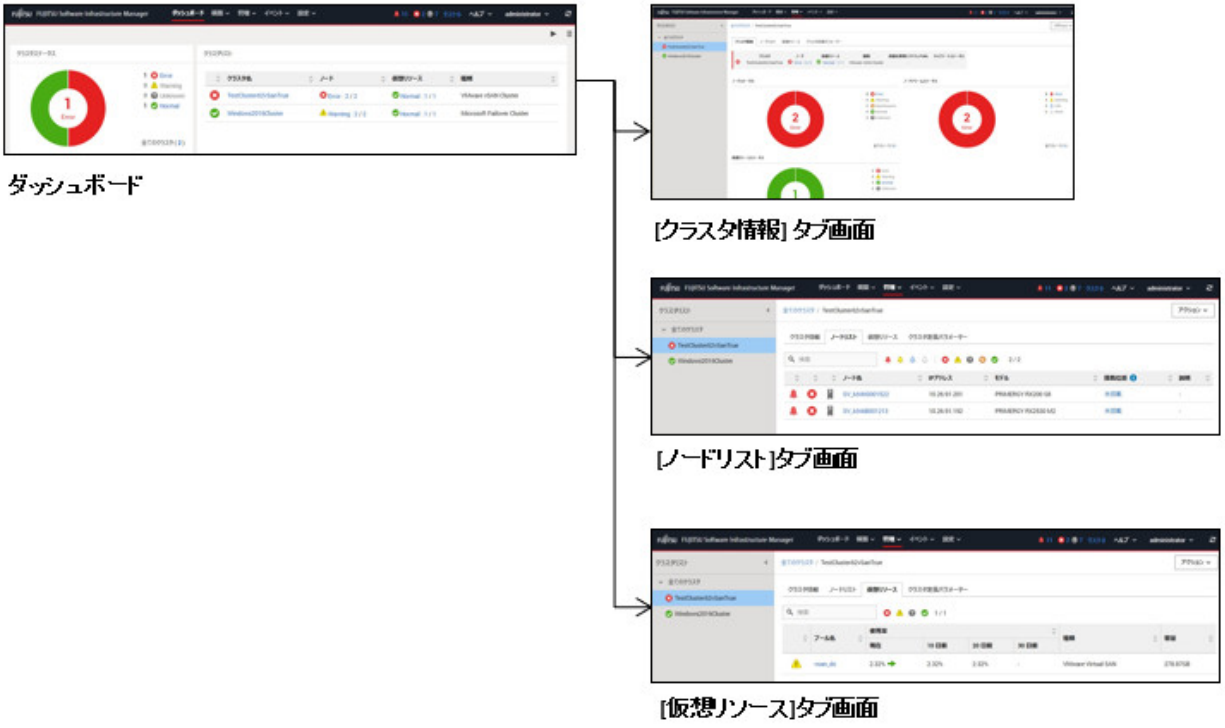
  本メニューを選択すると、「クラスタ拡張」ウィザードが起動されます。ウィザードに従ってクラスタへサーバーを追加します。

  詳細については、「2.13.3 クラスタ拡張機能」を参照してください。手順については、『操作手順書』を参照してください。

ダッシュボードとの連携

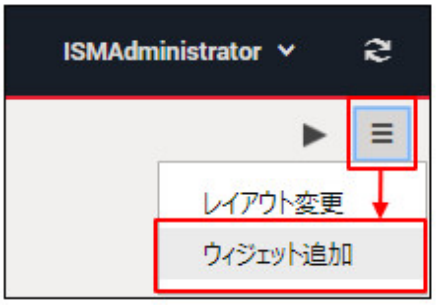
ISMのダッシュボード上に、クラスタ管理に関する情報表示画面(ウィジェット)を追加することで、ダッシュボードから直接、詳細を確認したい対象のクラスタおよびクラスタを構成する各種要素の情報(ノード、ストレージプール)を表示できます。

図2.36 ダッシュボードとの連携



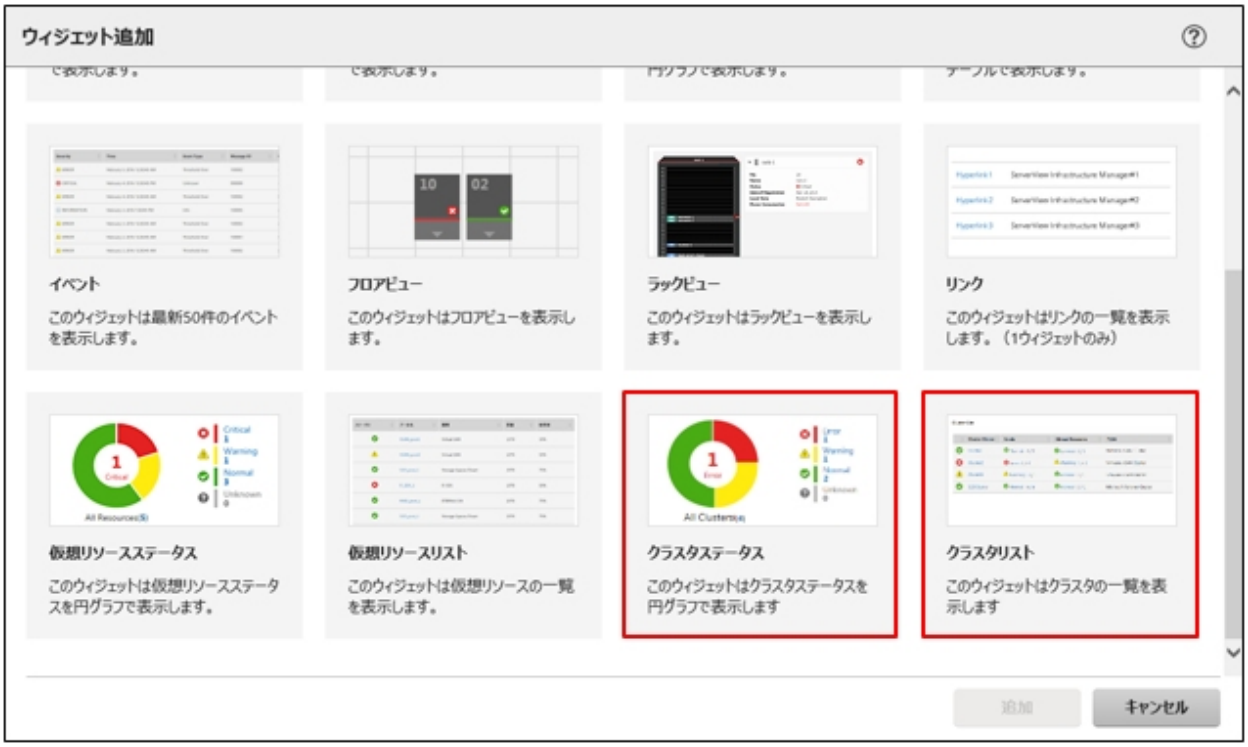
ISMのダッシュボードにウィジェットを追加する方法は以下のとおりです。

1. 上部にある[☰]から[ウィジェット追加]を選択します。

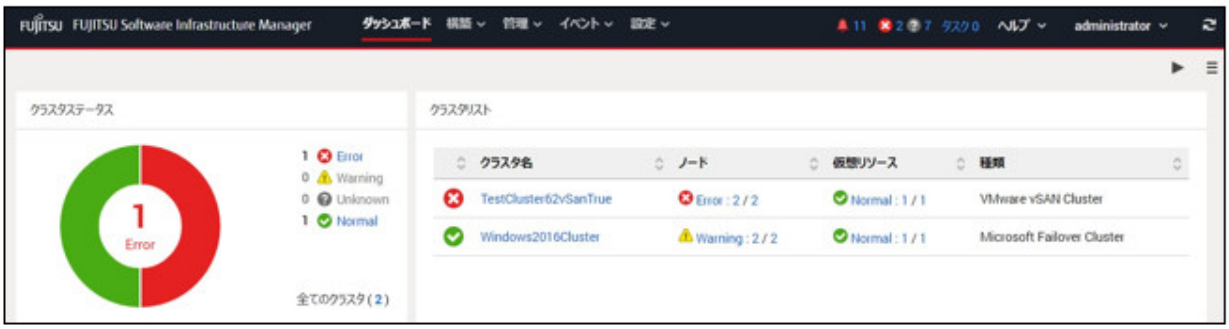


ウィジェット追加メニューが表示されます。

2. 「クラスタステータス」、「クラスタリスト」がクラスタの表示用ウィジェットです。どちらかを選択し、[追加]ボタンを選択します。



選択したウィジェットがダッシュボードに表示されます。



ノード情報との連携（[SDS]タブ）

ノードの詳細画面に仮想リソース管理情報を組み込み、相互に連携します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択し、「ノードリスト」画面でノード名を選択します。

   ノードの詳細画面に、[SDS]タブが表示されます。

   [SDS]タブは、SDSが構成されたノードにのみ表示されます（SDSを構成していないノードについては表示されません）。

2. [SDS]タブを選択します。

   ノードと関連するSDSの情報が表示されます。

SDSを構成するストレージプール名およびクラスタ名が表示されます。

クラスタ名を選択すると、クラスタ情報画面が表示されます。

また、プール名を選択すると、ストレージプールの詳細情報画面が表示されます。

画面の説明については、「2.9.2 仮想リソース管理機能のGUI」を参照してください。

2.13.1.2 クラスタ管理機能のサポート対象

クラスタ管理機能は、以下の環境をサポートします。

- VMware Virtual SANクラスタ

VMware Virtual SANクラスタ

VMware Virtual SANクラスタ(以降、「vSANクラスタ」と表記)は、ハイパーバイザーとしてVMware ESXiが導入された複数のサーバーから構成されるシステムです。

管理ソフトウェアとしてvCenter Server Appliance(以降、「vCenter Server」と表記)が利用され、クラスタ管理機能はvCenter Serverからクラスタに関する情報を取得し、ISM GUIへ反映します。

また、vSANクラスタには、各サーバーに搭載されるストレージを集約して仮想ストレージ「vSANストレージプール」が構成されます。vSANストレージプールの監視はISMから実施できます。

クラスタ管理機能がサポートするvSANクラスタ環境は、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

2.13.1.3 クラスタ情報の取得と更新

ISM GUI上に仮想化基盤の情報を取得、または表示内容を最新化するためには、ISM GUIからの情報更新が必要です。

クラスタ管理機能のGUIより仮想リソースの状態を確認する場合は、表示情報を更新します。

[アクション]ボタンから[クラスタ情報取得・更新]を実行します。

クラスタ情報がISM GUIに表示されます。表示される画面内容については、「2.13.1.1 クラスタ管理機能のGUI」を参照してください。

注意

タスクタイプが「Refresh Virtual Resource」のタスクはキャンセルできません。終了を待ち合わせてください。

ポイント

クラスタ情報の更新契機については、「2.9.3.3 仮想リソース情報の更新」を参照してください。

2.13.1.4 クラスタの管理／監視

クラスタ管理機能を利用して、クラスタの監視や運用を実施できます。

クラスタ管理機能のGUIを利用して、以下の監視ができます。

- クラスタの監視
- クラスタノードの監視
- クラスタ上の仮想リソースの監視

ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択すると、「クラスタリスト」画面が表示されます。

ISMで管理されているクラスタの一覧が表示されます。

クラスタの状態のほか、クラスタを構成しているノードの状態、およびクラスタ上に構成されたストレージプールの状態も確認できます。

クラスタ名を選択すると、クラスタの詳細画面へ遷移します。

詳細画面では、クラスタに関するサマリ([クラスタ情報]タブ画面)、クラスタのノード、仮想リソース、クラスタ定義パラメーターの各情報が表示されます。

クラスタを構成するノードについては、[ノードリスト]タブ画面で確認できます。

また、クラスタ内に構成されているストレージプールは、[仮想リソース]タブ画面で確認できます。

「クラスタリスト」画面で表示するステータス(クラスタ、ノード、仮想リソース)の重要度は以下のとおりです。

ステータス	アイコン表示	重要度	説明
Error(異常)		高	監視対象に致命的な異常が発生している状態です。 すべてのステータス中で、最優先で表示されます。
Warning(注意)		中	監視対象に問題が発生している状態です。 「Error」の対象が存在しない場合に、優先して表示されます。
Unknown(不明)		低	監視対象が不明な状態です。 「Error」「Warning」の対象が存在しない場合に、優先して表示されます。
Normal(正常)		―	監視対象に問題がなく、正常な状態です。

ノードおよび仮想リソースのステータスに該当する数は、以下の書式で表示されます。

[ステータスに該当する管理対象の数] / [管理対象の総数]

[ステータスに該当する管理対象の数]は、最も重要度の高いステータスに該当する対象の数を示します。

「クラスタリスト」画面のノードおよび仮想リソースの管理対象の数字を選択すると、クラスタの詳細画面のタブ画面へ遷移します。異常な状態にある対象について、絞り込み表示されます。

異常を示すクラスタの構成要素を把握することで、クラスタ運用に耐えられる状況であるかを迅速に把握します。

また、ISMのダッシュボードからクラスタ管理ウィジェットによる監視ができます。

クラスタ管理ウィジェットについては、「2.13.1.1 クラスタ管理機能のGUI」の「ダッシュボードとの連携」を参照してください。

クラスタの監視

[クラスタ情報]タブを選択すると、クラスタの詳細画面が表示されます。

画面内容については、「2.13.1.1 クラスタ管理機能のGUI」の「クラスタの詳細画面(タブ表示画面)」を参照してください。また、表示情報の詳細については、ISMのオンラインヘルプを参照してください。

ポイント

詳細な異常箇所の特定や対処、または異常の復旧については、各製品のマニュアルなどに従って実施してください。

クラスタの異常の詳細および発生箇所については、以下のように確認します。

VMware Virtual SANクラスタ

ISM GUIおよびvSphere Web Clientから、vSANの「健全性」を確認します。

1. ISM GUIのクラスタの一覧から、「クラスタ名」を確認します。
2. vSphere Web Client にサインインし、手順1で確認したクラスタ名を[ホストおよびクラスタ]タブで選択します。

   正常ならば無印、異常ならば赤くマークされます。

3. [監視]タブから[vSAN]-[健全性]を選択します。
4. 「テスト結果」を参照し、異常の内容を特定します。

異常を復旧したあとは、以下を実施してください。

1. vSphere Web Clientにサインインし、「ホストおよびクラスタ」でクラスタ名を選択します。
2. [監視]タブから[vSAN]-[健全性]を選択して[再テスト]を実行し、テスト結果が「失敗」から「パス」に変わったことを確認します。
3. ISM GUIのクラスター覧画面で、[アクション]ボタンから[クラスタ情報取得・更新]を選択し、ステータスが正常に戻ったことを確認します。

クラスタノードの監視

[ノードリスト]タブを選択すると、クラスタを構成しているクラスタノードの一覧が表示されます。

画面内容については、「2.13.1.1 クラスタ管理機能のGUI」の「[ノードリスト]タブ」を参照してください。また、表示情報の詳細については、ISMのオンラインヘルプを参照してください。

ノードの詳細情報は、ISMのノードリスト情報を利用します。

ノード名を選択すると、ノードリストの詳細画面へ遷移し、ハード構成やその状態についてより詳細な情報を確認できます。ノードリストの情報については、ISMのオンラインヘルプを参照してください。

ノードの異常の詳細は、以下のように確認します。

1. 異常を示しているノードのアラームステータスを選択すると、ノードの「関連イベント」画面を表示します。
2. 「関連イベント」画面で列名「重大度」を選択して並び替えを行い、重要度が高いイベントを確認します。

クラスタ上の仮想リソースの監視

[仮想リソース]タブを選択すると、クラスタ内に構成されているSDSのストレージプールが表示されます。

ストレージプールの状態、およびストレージの使用率などが表示されます。

画面内容については、「2.13.1.1 クラスタ管理機能のGUI」の「[仮想リソース]タブ」を参照してください。また、表示情報の詳細については、ISMのオンラインヘルプを参照してください。

ストレージプール名を選択すると、仮想リソースの詳細情報画面へ遷移し、ストレージプールのより詳細な情報を確認できます。

また、仮想リソースの監視については、「2.9 仮想リソース管理機能」を参照してください。

仮想リソースの異常の詳細および発生箇所については、「2.9.3.2 ストレージプールの異常の特定」を参照してください。

2.13.1.5 リソース変動予測

リソース変動予測機能は、vCenter Serverから過去のvSANクラスタのリソースの稼働情報を収集し、1年後までのリソースの使用予測をグラフ化して表示します。周期性やトレンドの変化を考慮した予測結果を元に、いつリソースが不足するかを示します。

また、構成変更シミュレーションを利用することで、将来のリソース変動を見積ることができます。

仮想化基盤のリソース増設に関する予算策定や運用を支援します。

リソース変動予測は、以下のvSANクラスタのリソース使用量と使用率の推移を表示します。

- vSANクラスタのストレージ
- CPU
- メモリー

リソースの稼働情報は、vCenter Serverから取得する稼働情報を利用しています。稼働情報は仮想マシンが利用するリソース情報および利用可能なリソース情報です。物理サーバーが搭載するCPU量、メモリー量およびストレージ量とは異なる可能性があります。

2.13.1.5.1 リソース変動予測の実行

リソース変動予測は、クラスタ単位で行います。リソース変動予測を実行すると、ISMは仮想化管理ソフトウェアから過去のリソースの稼働情報を取得して、1年後までのリソース使用状況の予測を行います。

実行結果は[リソース変動予測]タブの「履歴リスト」に結果リストとして追加されます。

リソース変動予測の実行手順

リソース変動予測の実行は、「クラスタ」画面から対象クラスタを選択し、[リソース変動予測]タブの[リソース変動予測アクション]ボタンから操作します。

リソース変動予測の実行手順は、『操作手順書』の「6.3.1 リソース変動予測を実行する」を参照してください。

ポイント

- 予測完了までに時間(目安:10分程度)が必要です。予測状況は「タスク」画面で確認できます。リソース変動予測のタスク状況の確認については、「2.14.4 タスク管理」を参照してください。
- 予測を行うには、仮想化管理ソフトウェアに予測に使用する稼働情報の収集期間の開始日から1日ごとに最低2週間の稼働情報が保存されている必要があります。リソース変動予測では1日ごとに最大で1年間の稼働情報を使用して予測を行います。
- 仮想化管理ソフトウェアで稼働情報が有効になっているかは、「3.8.2 vCenter Serverの統計収集間隔の事前設定」を参照してください。

注意

- 同時に予測可能なクラスタ数には上限があります。この上限数はISM-VA全体で10です。上限数より多いクラスタを対象に予測を同時に実施した場合、はじめに上限数分の予測が実行されます。残りのクラスタは先に実行している予測が終了してから実行されます。
- 同じクラスタを対象に同時に予測を行うことはできません。同じクラスタで同時に予測を行うと後から実行した予測がエラーとなります。

2.13.1.5.2 リソース変動予測の結果表示

リソース変動予測の実行が完了すると、「履歴リスト」の結果リストに[結果]ボタンが表示されます。実行結果を表示させるには、[結果]ボタンを選択します。

構成変更シミュレーションを実施した場合の予測結果は、追加したディスク、CPU、メモリーを含んだキャパシティサイズで計算された使用率および使用量が表示されます。

履歴リストに表示される予測のステータスは以下です。

表2.22 予測のステータス

ステータス	説明
待機	予測を開始していない状態
予測中	予測をしている状態 クラスタにこの状態があると、そのクラスタでは別の予測を開始することはできません。
完了	予測が完了した状態 [結果]ボタンを選択すると、予測がグラフ化されて表示されます。
キャンセル中	予測をキャンセルしている状態
キャンセル済み	予測のキャンセルが完了した状態
失敗	なんらかの異常が発生し予測が失敗した状態 運用ログにエラー原因が出力されます。

ポイント

履歴リストは1クラスタに最大100履歴記録されます。100履歴を超えて予測を実施すると、古いものから削除されます。

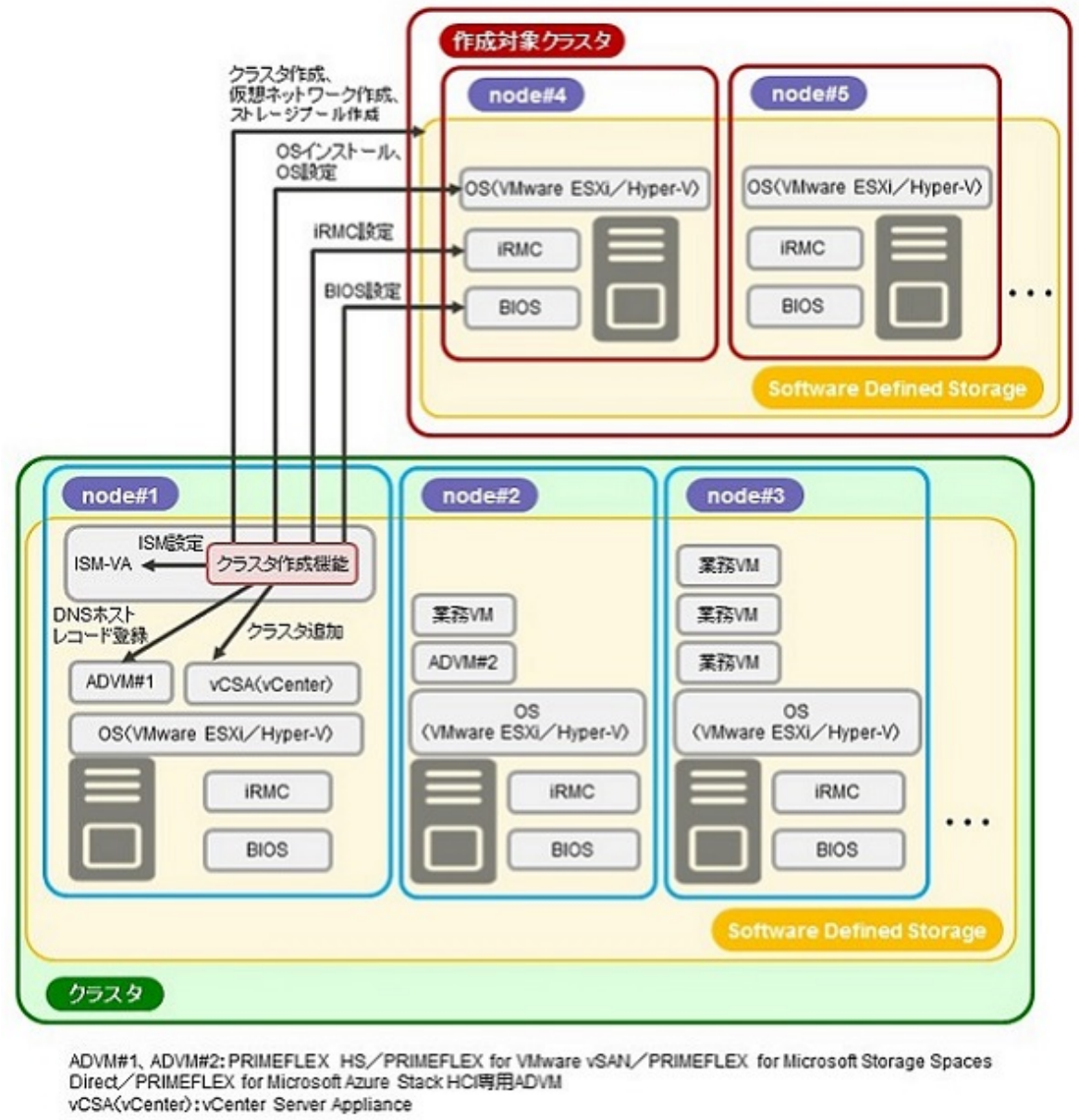
2.13.2 クラスタ作成機能

クラスタ作成機能は、PRIMEFLEX HS／PRIMEFLEX for VMware vSANの仮想化基盤環境に対して、新規にクラスタを作成してリソースを増やす機能です。本機能は、ISMのプロファイル管理機能と連携して、クラスタ作成と作成したクラスタに追加する対象サーバーのOSインストールからクラスタに追加するまでの手順を自動化することで、お客様の作業を削減します。

クラスタ作成機能は、主に以下の用途で利用する機能です。

- 新規クラスタ作成
- 新規クラスタの仮想ネットワーク作成
- 新規クラスタのストレージプール作成
- 新規クラスタを構成するサーバーのOSのインストールと設定
- 新規クラスタを構成するサーバーを新規クラスタ環境に追加

図2.37 クラスタ作成機能の動作概要



ADVM#1、ADVM#2：PRIMEFLEX HS／PRIMEFLEX for VMware vSAN／PRIMEFLEX for Microsoft Storage Spaces Direct／PRIMEFLEX for Microsoft Azure Stack HCI専用ADVM
vCSA(vCenter)：vCenter Server Appliance

2.13.2.1 自動設定項目

クラスタ作成機能を使用することにより、以下の項目が自動で設定されます。

表2.23 PRIMEFLEX for VMware vSANの自動設定項目一覧

自動設定順番	自動設定項目	説明
1	プロファイル適用	1. 新規クラスタを構成するサーバーのBIOSの設定 2. 新規クラスタを構成するサーバーのiRMCの設定 3. 新規クラスタを構成するサーバーのOSのインストール
2	ESXiパッチ適用	1. VMware ESXiパッチファイルとVMware ESXiパッチ適用前後に実行するスクリプトの転送 2. VMware ESXiパッチ適用前に実行するスクリプトの実行 3. OSの再起動 4. VMware ESXiパッチの適用

自動設定順番	自動設定項目	説明
		5. VMware ESXiパッチ適用時に実行するスクリプトの実行 6. OSの再起動 7. VMware ESXiパッチファイルの削除 8. VMware ESXiパッチ適用前後に実行するスクリプトの再転送 9. VMware ESXiパッチ適用後に実行するスクリプトの実行 10. OSの再起動 11. VMware ESXiパッチ適用前後に実行するスクリプトの削除
3	DNSホストレコード登録	1. 新規クラスタを構成するサーバーのESXiのDNS登録（PRIMEFLEX構成のADVMを使用していない構成時は登録しない）
4	OS設定	1. ESXiシェルの有効化と起動 2. SSHサービスの有効化と起動 3. VMware SMIS Providerの適用（PRIMERGY M4シリーズおよびVMware ESXi 6.5の場合のみ設定） 4. ixgbenドライバーの有効化（PRIMERGY M4シリーズおよびVMware ESXi 6.5、VMware ESXi 6.5 Update 1の場合のみ設定） 5. ローカル管理ユーザーの追加 6. ホスト名をFQDNに設定 7. SSL v3の有効化（PRIMERGY M4シリーズ／PRIMERGY M5シリーズの場合のみ設定） 8. IPv6の無効化 9. セカンダリーDNSサーバーのIPアドレスの設定 10. DNSサフィックスの設定 11. NTPサーバーのIPアドレスの設定 12. NTPクライアントのファイアウォールの設定 13. NTPクライアントサービスの実行 14. ホストの電源管理を高パフォーマンスに設定 15. OSの再起動 16. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）へアダプターを追加 17. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）へNICの設定 18. Management NetworkへNICの設定 19. 新規クラスタを構成するサーバーのESXiのActive Directory認証設定（PRIMEFLEX構成のADVM、またはお客様環境のADサーバーを使用したActive Directory連携を行わない構成時は設定しない） 20. ESXiシェルの無効化と停止 21. SSHサービスの無効化と停止
5	iRMC設定	1. ローカルユーザー（pflocaladmin）の作成 2. adminユーザーのパスワード変更

自動設定順番	自動設定項目	説明
		3. 新規クラスタを構成するサーバーのiRMCのActive Directory認証設定（PRIMEFLEX構成のADVM、またはお客様環境のADサーバーを使用したActive Directory連携を行わない構成時は設定しない） 4. 新規クラスタを構成するサーバーのiRMCのリセット
6	クラスタへのサーバー追加	1. 新規クラスタを構成するサーバーを管理用分散仮想スイッチへ登録 2. 新規クラスタを構成するサーバーを業務用分散仮想スイッチへ登録 3. 分散仮想スイッチの設定 4. SSDのキャパシティデバイスの設定（All Flash環境時） 5. ディスクグループの追加 6. 新規クラスタを構成するサーバーをクラスタに追加
7	ISM設定	1. ISMに登録されているiRMCのadminユーザーのパスワードの変更 2. ISMに登録されているiRMCのWebインターフェイスURLの変更 3. ISMのログ管理機能によるログ収集対象と収集日時の設定
8	クラスタ作成	1. クラスタの作成
9	仮想ネットワーク作成	1. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）の作成 2. NIOCの有効化 3. ポートグループの作成と設定 4. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）のNIOCの設定
10	ストレージプール作成	1. vSANの有効化 2. デデュープおよび圧縮の設定
11	仮想リソース更新	1. クラスタ情報の更新

2.13.2.2 プロファイル管理機能との連携

ISMのプロファイル管理機能は、サーバーのハードウェア設定（BIOS、iRMC）やOSインストールの設定を行います。

クラスタ作成機能は、プロファイル管理機能と連携して、クラスタ作成処理を自動化します。

事前に作成したプロファイルを「クラスタ作成」ウィザードから選択することで、クラスタ作成機能の実行時にプロファイルを適用してハードウェア設定とOSインストールを実行します。

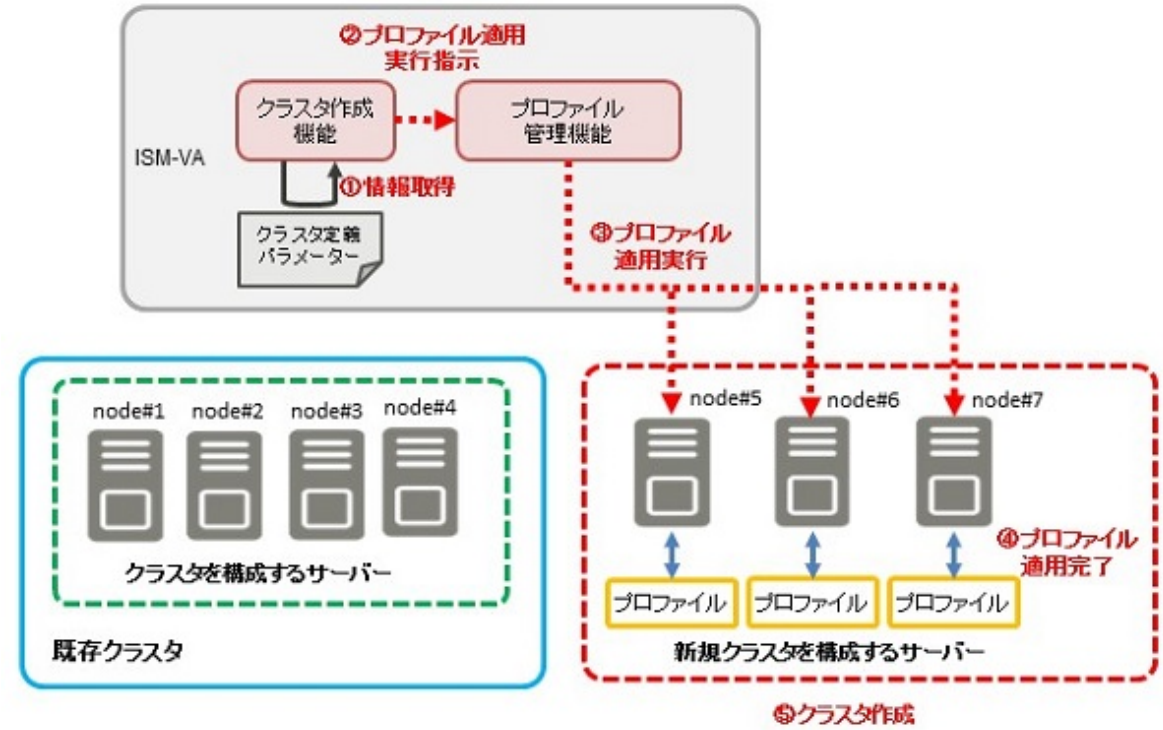
プロファイル適用の完了後、プロファイル管理機能の1つである「インストール後のスクリプト実行機能」により、OS設定スクリプトが実行されます。続けて、対象のクラスタに対して新規クラスタを構成するサーバーの登録処理を行います。

ポイント

OS設定スクリプトとは、クラスタ作成機能の処理中に、ISMから新規クラスタを構成するサーバーのOSに接続するために必要な設定を実行するスクリプトです。

以下にクラスタ作成機能とプロファイル管理機能の関係図を示します。

図2.38 クラスタ作成機能とプロファイル管理機能の連携



2.13.2.3 クラスタ定義パラメーター

クラスタ定義パラメーターは、クラスタ作成機能を実行する際に使用するパラメーターです。新規クラスタやクラスタを構成するノードの設定情報を保持できます。クラスタ作成時には、新規クラスタ部分のパラメーターを入力して実行します。

クラスタ定義パラメーターをISM外（管理端末）に保管しておきたい場合など、クラスタ定義パラメーターをJSON形式で記述されたテキストファイルとしてエクスポート／インポートできます。詳細な手順については、『操作手順書』の「6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する」を参照してください。

クラスタ定義パラメーターの詳細については、『ISM for PRIMEFLEX 設定値一覧』を参照してください。

2.13.2.4 タスク一覧

クラスタ作成機能は、「クラスタ作成」ウィザードから実行できます。クラスタ作成の処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。クラスタ作成機能のタスク名は「Cluster Creation」です。タスク一覧からタスクタイプが「Cluster Creation」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、新規クラスタを構成するサーバーごとに表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.24 PRIMEFLEX for VMware vSANのサブタスクの処理一覧

処理名	実施内容
PrepCheck Represent TaskItemSet	Prep Checkで行う処理を登録します。
Prep Check	クラスタ作成の実行条件をチェックします。
OS Installation	新規クラスタを構成するサーバーのOSインストールとパッチ適用、スクリプト実行を行います。
DNS Settings	新規クラスタを構成するサーバーのDNSホストレコードを登録します。
iRMC Settings	新規クラスタを構成するサーバーのiRMC設定とISMの設定を行います。

処理名	実施内容
OS Settings	新規クラスタを構成するサーバーのOS設定を行います。
Cluster Settings	新規クラスタを構成するサーバーのクラスタ設定(前半設定)を行います。
Ism Settings	新規クラスタを構成するサーバーのISMの設定を行います。
Cluster Creation	新規クラスタを作成します。
Virtual Network Creation	新規クラスタの仮想ネットワークを作成します。
Storage Pool Creation	新規クラスタのストレージプールを作成します。
Cluster Settings	新規クラスタを構成するサーバーのクラスタ設定(後半設定)を行います。
Cluster Post Settings	新規クラスタを構成するサーバーのクラスタ設定(事後設定)を行います。
ResourceList Registration	新規クラスタ情報を更新します。
ESXi Host Post Settings	新規クラスタを構成するサーバーのOS設定(事後設定)を行います。

実施内容は、「表2.23 PRIMEFLEX for VMware vSANの自動設定項目一覧」を参照してください。

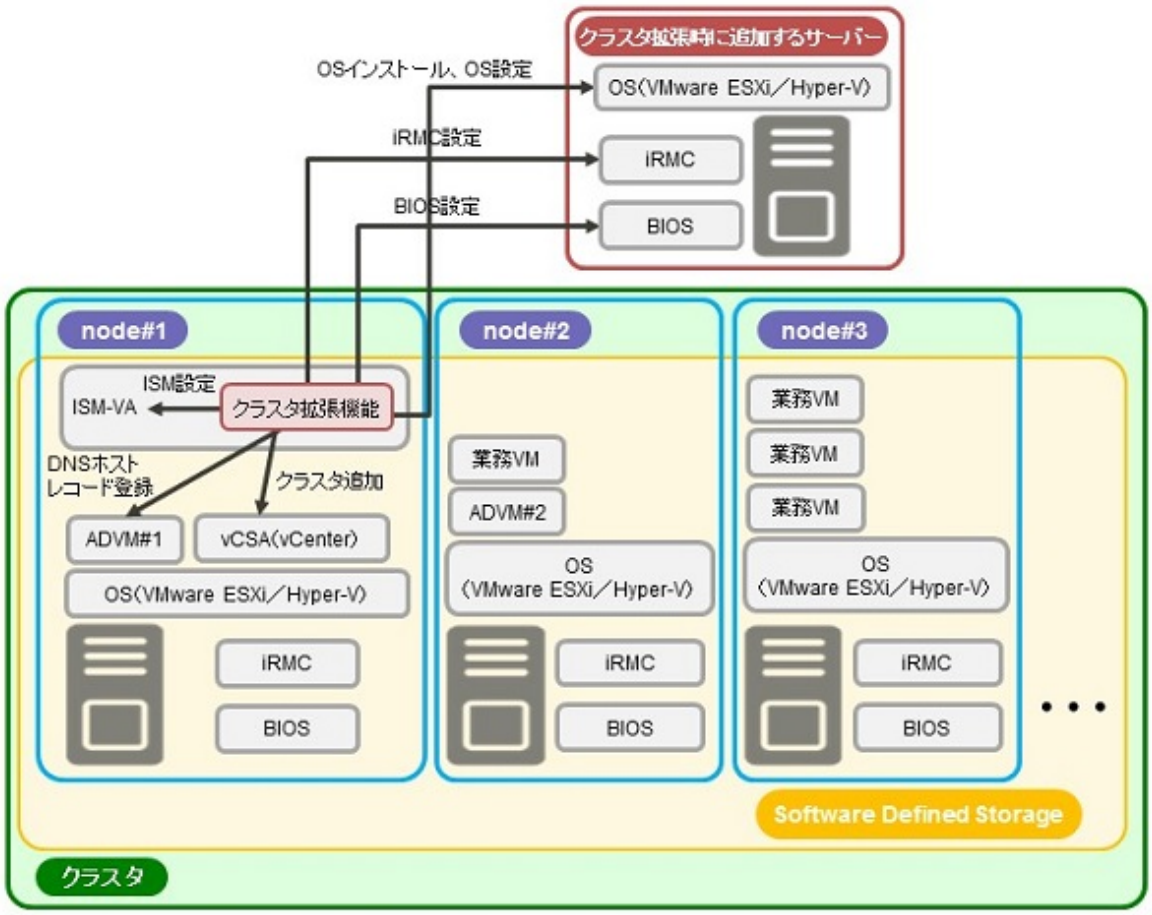
2.13.3 クラスタ拡張機能

クラスタ拡張機能は、VMware vSANのストレージリソースが枯渇した際に、PRIMEFLEX HS／PRIMEFLEX for VMware vSANの仮想化基盤環境に対して、新規にサーバーを追加してリソースを増やす機能です。本機能は、ISMのプロファイル管理機能と連携して、OSインストールからクラスタに追加するまでの手順を自動化することで、お客様の作業を削減します。

クラスタ拡張機能は、主に以下の用途で利用する機能です。

- クラスタ拡張時に追加するサーバーのOSのインストールと設定
- クラスタ拡張時に追加するサーバーを既存のクラスタ環境に追加

図2.39 クラスタ拡張機能の動作概要



ADVM#1、ADVM#2:PRIMEFLEX HS／PRIMEFLEX for VMware vSAN／PRIMEFLEX for Microsoft Storage Spaces Direct／PRIMEFLEX for Microsoft Azure Stack HCI専用ADVM
vCSA(vCenter):vCenter Server Appliance

2.13.3.1 自動設定項目

クラスタ拡張機能を使用することにより、以下の項目が自動で設定されます。

表2.25 PRIMEFLEX HS／PRIMEFLEX for VMware vSANの自動設定項目一覧

自動設定順番	自動設定項目	説明
1	プロファイル適用	1. クラスタ拡張時に追加するサーバーのBIOSの設定 2. クラスタ拡張時に追加するサーバーのiRMCの設定 3. クラスタ拡張時に追加するサーバーのOSのインストール
2	ESXiパッチ適用	1. VMware ESXiパッチファイルとVMware ESXiパッチ適用前後に実行するスクリプトの転送 2. VMware ESXiパッチ適用前に実行するスクリプトの実行 3. OSの再起動 4. VMware ESXiパッチの適用 5. VMware ESXiパッチ適用時に実行するスクリプトの実行 6. OSの再起動 7. VMware ESXiパッチファイルの削除 8. VMware ESXiパッチ適用前後に実行するスクリプトの再転送

自動設定順番	自動設定項目	説明
		9. VMware ESXiパッチ適用後に実行するスクリプトの実行 10. OSの再起動 11. VMware ESXiパッチ適用前後に実行するスクリプトの削除
3	DNSホストレコード登録	1. クラスタ拡張時に追加するサーバーのESXiのDNS登録（PRIMEFLEX構成のADVMを使用していない構成時は登録しない）
4	OS設定	1. ESXiシェルの有効化と起動 2. SSHサービスの有効化と起動 3. VMware SMIS Providerの適用（PRIMERGY M4シリーズおよびVMware ESXi 6.5の場合のみ設定） 4. ixgbenドライバーの有効化（PRIMERGY M4シリーズおよびVMware ESXi 6.5、VMware ESXi 6.5 Update 1の場合のみ設定） 5. ローカル管理ユーザーの追加 6. ホスト名をFQDNに設定 7. SSL v3の有効化（PRIMERGY M2シリーズ／PRIMERGY M4シリーズ／PRIMERGY M5シリーズの場合のみ設定） 8. IPv6の無効化 9. セカンダリーDNSサーバーのIPアドレスの設定 10. DNSサフィックスの設定 11. NTPサーバーのIPアドレスの設定 12. NTPクライアントのファイアウォールの設定 13. NTPクライアントサービスの実行 14. ホストの電源管理を高パフォーマンスに設定 15. OSの再起動 16. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）へアダプターを追加 17. 分散仮想スイッチ（業務用分散仮想スイッチ／管理用分散仮想スイッチ）へNICの設定 18. Management NetworkへNICの設定 19. クラスタ拡張時に追加するサーバーのESXiのActive Directory認証設定（PRIMEFLEX構成のADVM、またはお客様環境のADサーバーを使用したActive Directory連携を行わない構成時は設定しない） 20. ESXiシェルの無効化と停止 21. SSHサービスの無効化と停止
5	iRMC設定	1. ローカルユーザー（pflocaladmin）の作成 2. adminユーザーのパスワード変更 3. クラスタ拡張時に追加するサーバーのiRMCのActive Directory認証設定（PRIMEFLEX構成のADVM、またはお客様環境のADサーバーを使用したActive Directory連携を行わない構成時は設定しない） 4. クラスタ拡張時に追加するサーバーのiRMCのリセット
6	クラスタへのサーバー追加	1. クラスタ拡張時に追加するサーバーを管理用分散仮想スイッチへ登録 2. クラスタ拡張時に追加するサーバーを業務用分散仮想スイッチへ登録

自動設定順番	自動設定項目	説明
		3. 分散仮想スイッチの設定 4. SSDのキャパシティデバイス設定（All Flash環境時） 5. ディスクグループの追加 6. クラスタ拡張時に追加するサーバーをクラスタに追加
7	ISM設定	1. ISMに登録されているiRMCのadminユーザーのパスワードの変更 2. ISMに登録されているiRMCのWebインターフェイスURLの変更 3. ISMのログ管理機能によるログ収集対象と収集日時の設定

2.13.3.2 プロファイル管理機能との連携

クラスタ拡張機能は、プロファイル管理機能と連携して、処理を自動化します。

事前に作成したプロファイルを「クラスタ拡張」ウィザードから選択することで、クラスタ拡張機能実行時にプロファイルを適用してハードウェア設定とOSインストールを実行します。

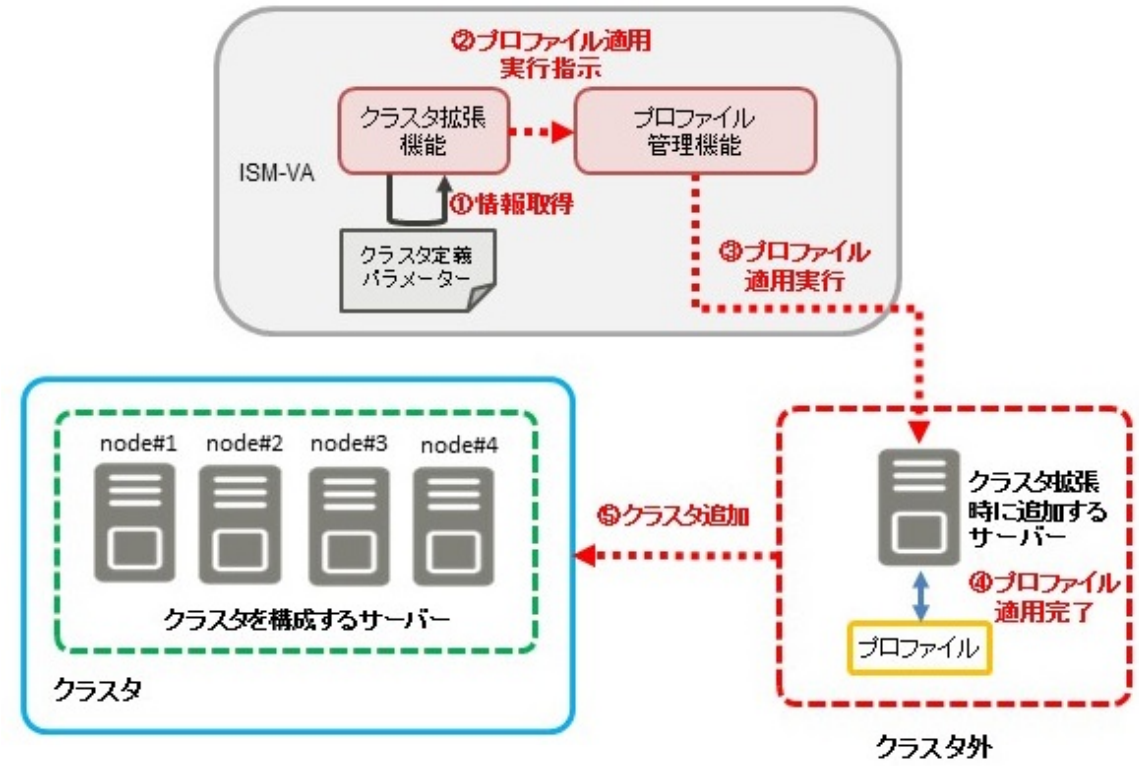
プロファイル適用の完了後、プロファイル管理機能の1つである「インストール後のスクリプト実行機能」により、OS設定スクリプトが実行されます。続けて、対象のクラスタに対してクラスタ拡張時に追加するサーバーの登録処理を行います。

ポイント

OS設定スクリプトとは、クラスタ拡張機能の処理中に、ISMからクラスタ拡張時に追加するサーバーのOSに接続するために必要な設定を実行するスクリプトです。

以下にクラスタ拡張機能とプロファイル管理機能の関係図を示します。

図2.40 クラスタ拡張機能とプロファイル管理機能の連携



2.13.3.3 クラスタ定義パラメーター

クラスタ定義パラメーターは、クラスタ拡張機能を実行する際に使用するパラメーターです。拡張対象のクラスタや、クラスタを構成するノードの設定情報を保持できます。クラスタ拡張時に追加するサーバー部分のパラメーターを入力して実行します。

クラスタ定義パラメーターをISM外（管理端末）に保管しておきたい場合など、クラスタ定義パラメーターをJSON形式で記述されたテキストファイルとしてエクスポート／インポートできます。詳細な手順については、『操作手順書』の「6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する」を参照してください。

クラスタ定義パラメーターの詳細については、『ISM for PRIMEFLEX 設定値一覧』を参照してください。

2.13.3.4 タスク一覧

クラスタ拡張機能は、「クラスタ拡張」ウィザードから実行できます。クラスタ拡張の処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。クラスタ拡張機能のタスク名は「Cluster Expansion」です。タスク一覧からタスクタイプが「Cluster Expansion」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、クラスタ拡張時に追加するサーバーごとに表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.26 PRIMEFLEX HS／PRIMEFLEX for VMware vSANのサブタスクの処理一覧

処理名	実施内容
PrepCheck Represent TaskItemSet	Prep Checkで行う処理を登録します。
Prep Check	クラスタ拡張の実行条件をチェックします。
OS Installation	クラスタ拡張時に追加するサーバーのOSインストールとパッチ適用、スクリプト実行を行います。
DNS Settings	クラスタ拡張時に追加するサーバーのDNSホストレコードを登録します。
iRMC Settings	クラスタ拡張時に追加するサーバーのiRMC設定とISMの設定を行います。
OS Settings	クラスタ拡張時に追加するサーバーのOS設定とISMの設定を行います。
Cluster Settings	クラスタ拡張時に追加するサーバーのクラスタ設定を行います。
Ism Settings	クラスタ拡張時に追加するサーバーのISMの設定を行います。
ESXi Host Post Settings	クラスタ拡張時に追加するサーバーのOS設定（事後設定）を行います。

実施内容は、「表2.25 PRIMEFLEX HS／PRIMEFLEX for VMware vSANの自動設定項目一覧」を参照してください。

2.13.4 ローリングアップデート機能

ローリングアップデート機能とは、仮想化基盤を構成しているクラスタに対して業務を停止することなく以下のアップデートを行う機能です。

凡例：○ = サポート、－ = 未サポート

ローリングアップデートで行われる処理	PRIMEFLEX HS PRIMEFLEX for VMware vSAN
ファームウェアアップデート	○
ESXi修正パッチ適用	○
ESXiオフラインバンドル適用	○
vCSA修正パッチ適用	○
vCSAアップグレード	○

本機能は、クラスタを構成するすべてのサーバーに対して上記の処理を自動化することで、お客様の作業を削減します。ファームウェアのアップデートは、ISMのファームウェア管理機能と連携して自動化します。

ローリングアップデート機能に対応しているファームウェアデータは、以下のとおりです。

種別	アップデート方法
iRMCファームウェア（サーバー）	Offlineアップデート
BIOSファームウェア（サーバー）	Offlineアップデート
LAN／CNA／SASカードファームウェア（サーバー）[注]	Offlineアップデート

[注]：PRIMEFLEX HS／PRIMEFLEX for VMware vSANでサポートしているLAN／CNA／SASカードが対象です。
LAN／CNA／SASカードの対象機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。
https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

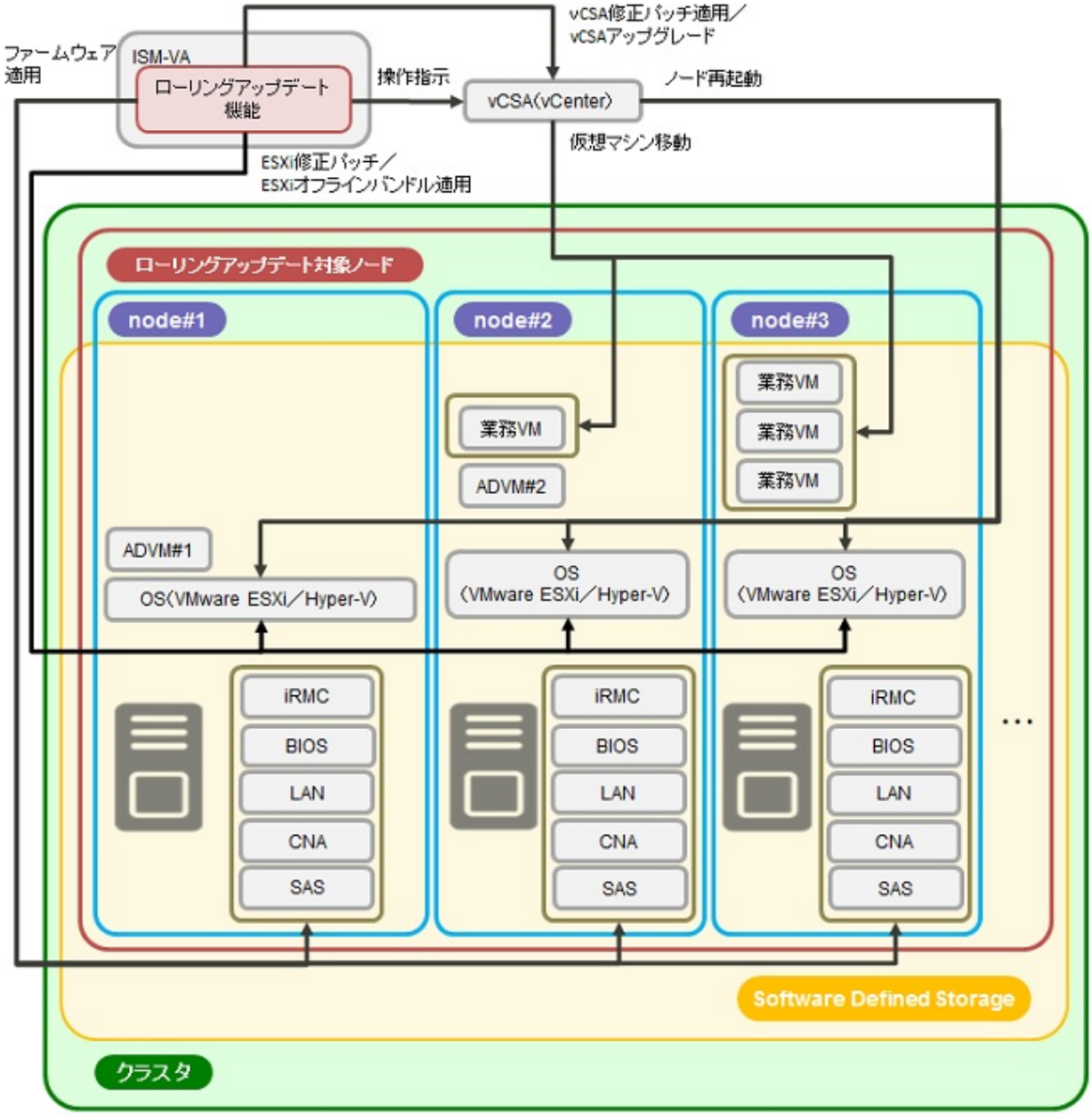
ローリングアップデート機能でESXiに適用可能な種別は、以下のとおりです。

- 修正パッチ
- オフラインバンドル

ローリングアップデート機能でvCSAに適用可能な種別は、以下のとおりです。

- 修正パッチ
- アップグレード

図2.41 ローリングアップデート機能の動作概要



ADVM#1、ADVM#2: PRIMEFLEX HS／PRIMEFLEX for VMware vSAN／PRIMEFLEX for Microsoft Storage Spaces Direct／PRIMEFLEX for Microsoft Azure Stack HCI専用ADVM
vCSA(vCenter):vCenter Server Appliance

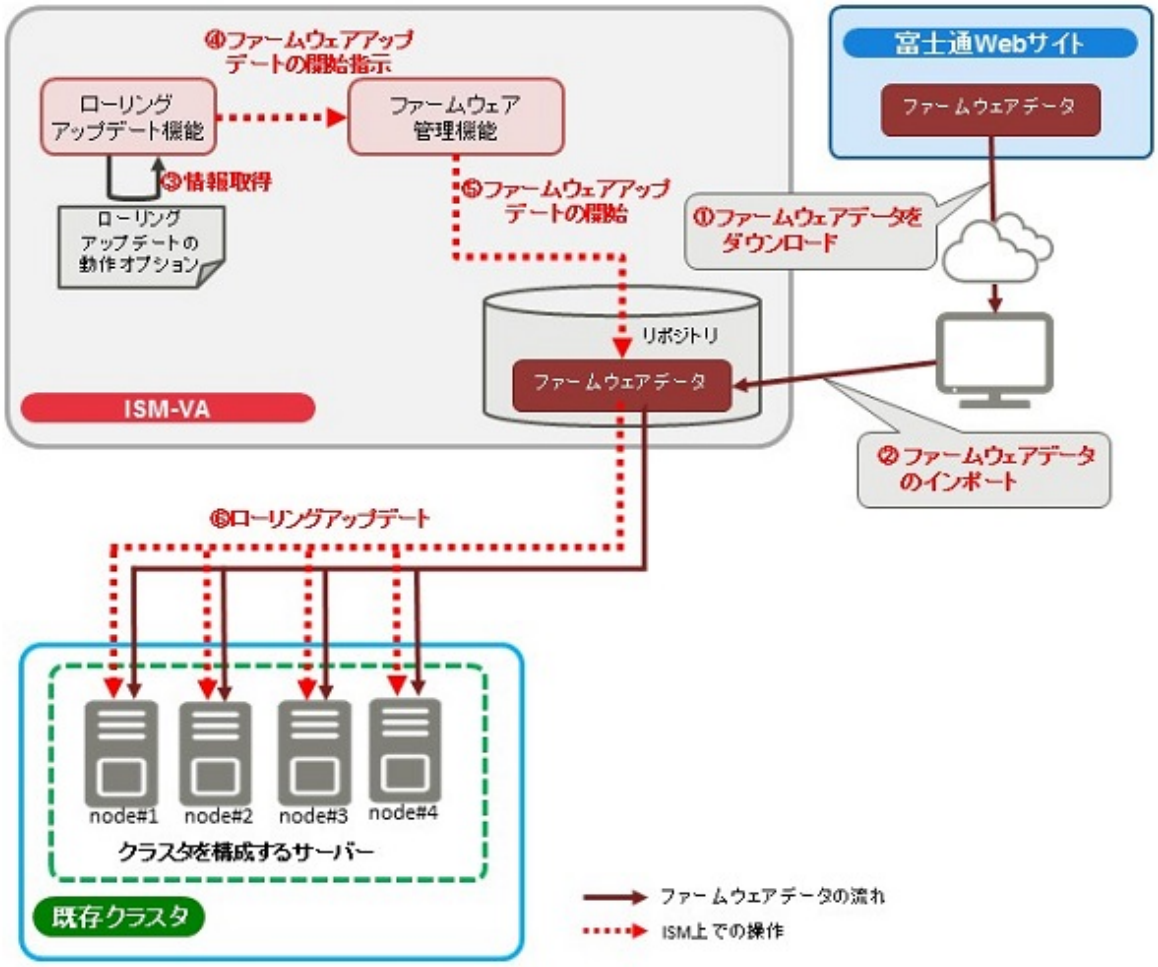
2.13.4.1 ファームウェア管理機能との連携

ローリングアップデート機能は、ファームウェア管理機能と連携して、ファームウェアのローリングアップデートを自動化します。

事前にインポートしたファームウェアデータの中から最新のファームウェアが適用されます。

以下にローリングアップデート機能とファームウェア管理機能の関係図を示します。

図2.42 ローリングアップデート機能とファームウェア管理機能の連携



2.13.4.2 タスク一覧

ローリングアップデート機能は、「ローリングアップデート」ウィザードから実行できます。ローリングアップデートの処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。ローリングアップデート機能のタスク名は「Rolling Update」です。タスク一覧からタスクタイプが「Rolling Update」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、ファームウェアのアップデートとESXi修正パッチの適用対象ノードごとに表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.27 Offlineアップデートサブタスクの処理一覧

処理名	設定項目名	設定項目内容
Rolling Update Prep Check （ローリングアップデートの事前確認を行います）	1. Prep Check	1. ローリングアップデートの実行条件をチェックします。
Rolling Update Presetting （ローリングアップデートの事前設定とvCSA修正パッチ適用、vCSAアップグレードを行います）	1. Enable Ssh and ESXishell 2. File transfer to OS 3. Check Dry Run 4. Update vCSA Patch	1. SSHサービスとESXiシェルを有効に設定します。[注2] 2. 対象ノードに以下のファイルを転送します。[注2]

処理名	設定項目名	設定項目内容
	5. Upgrade vCSA	ー ESXi修正パッチファイル ー ESXiオフラインバンドル ー 上記ファイルの適用前後に実行するスクリプト 3. ESXi修正パッチまたはESXiオフラインバンドルの適用を確認します。[注2] 4. vCSA修正パッチを適用します。[注2] 5. vCSAをアップグレードします。[注2]
Rolling Update （アップデート対象ノードのファームウェアアップデート、ESXi修正パッチまたはESXiオフラインバンドル適用と再起動を行います）	1. Migrate VM to Another Node & Set Maintenance Mode 2. Migrate VM to Another Node & Set Maintenance Mode 3. Script Execution (Prep) 4. Reboot Node 5. Update ESXi Patch 6. Script Execution (Post1) 7. Shutdown Node 8. Update Firmware (offline) 9. Boot Node 10. File retransfer to OS 11. Script Execution (Post2) 12. Delete File 13. Disable Ssh and ESXishell 14. Reboot Node 15. Unset Maintenance Mode & Migrate VM to Target Node 16. Unset Maintenance Mode & Migrate VM to Target Node 17. Post Check	1. 対象ノード上で稼働しているVMを退避ノードへ移動します。[注1] 2. ノードをメンテナンスモードに設定します。 3. ESXi修正パッチまたはESXiオフラインバンドル適用前のスクリプトを実行します。[注2] 4. ノードを再起動します。[注2] 5. ESXi修正パッチまたはESXiオフラインバンドルを適用します。[注2] 6. ESXi修正パッチまたはESXiオフラインバンドル適用時のスクリプトを実行します。[注2] 7. ノードをシャットダウンします。 8. ファームウェアデータをOfflineで適用します。 9. ノードを起動します。 10. 対象ノードに以下のファイルを再転送します。[注2] ー ESXi修正パッチファイル ー ESXiオフラインバンドル ー 上記ファイルの適用前後に実行するスクリプト 11. ESXi修正パッチまたはESXiオフラインバンドル適用後のスクリプトを実行します。[注2] 12. 対象ノードから以下のファイルを削除します。[注2] ー ESXi修正パッチファイル ー ESXiオフラインバンドル ー 上記ファイルの適用前後に実行するスクリプト 13. SSHサービスとESXiシェルを無効に設定します。[注2] 14. ノードを再起動します。[注2]

処理名	設定項目名	設定項目内容
		15. ノードのメンテナンスモードを解除します。 16. 退避ノードへ移動しておいたVMを対象ノードへ戻します。[注1] 17. ローリングアップデートの事後条件をチェックします。
Refresh Resource Information （仮想化管理ソフトウェア情報取得とノード情報取得を行います）	1. Refresh Resource Information 2. Refresh Virtual Inventory	1. 仮想化管理ソフトウェア情報を取得します。 2. ノード情報を取得します。

[注1]：vSANクラスタでDRS機能が有効の場合には実施しません。

[注2]：vSANクラスタの場合に実施します。

2.13.5 ノード切離し／組込み機能

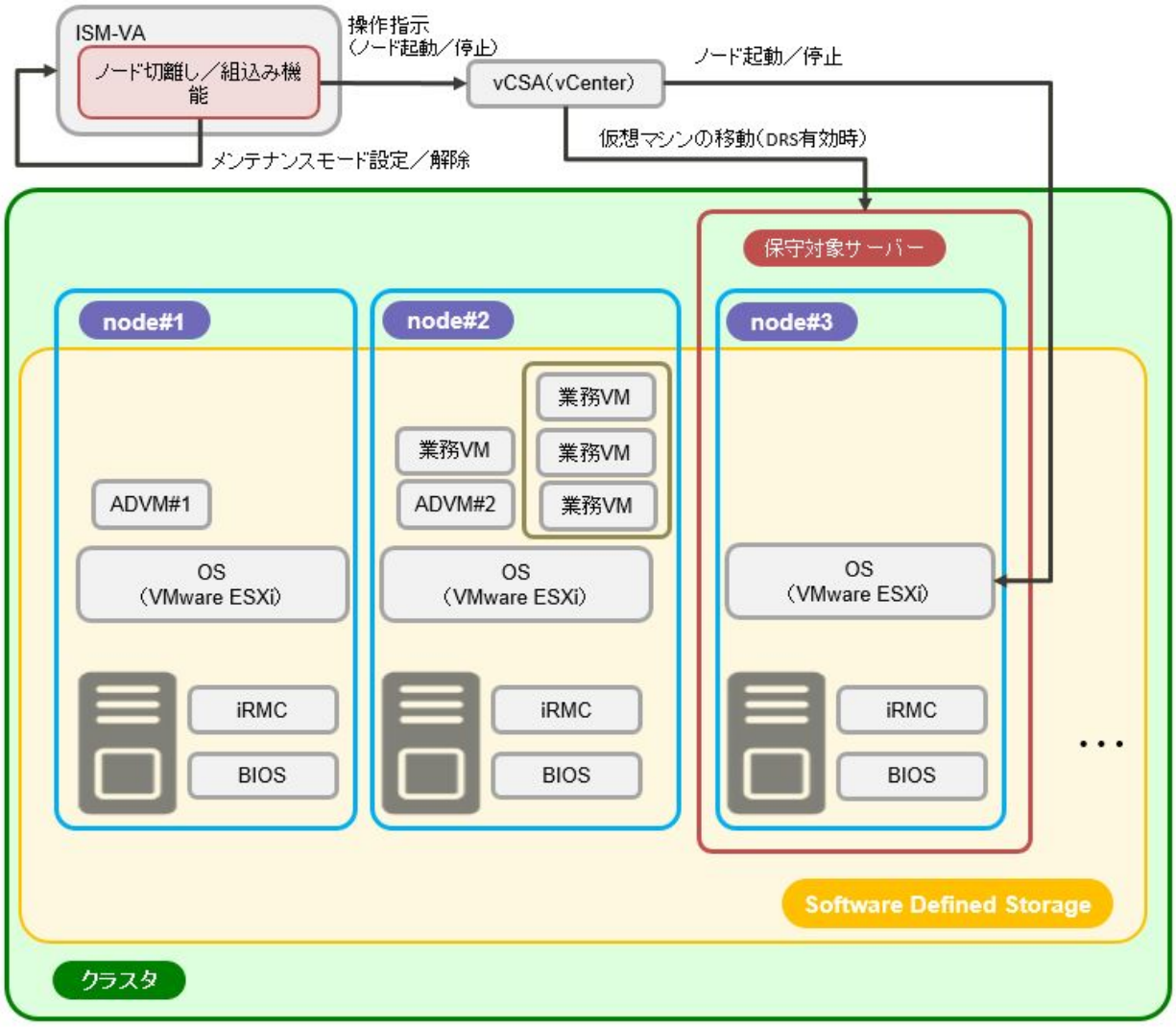
ノード切離し／組込み機能とは、PRIMEFLEX for VMware vSANの仮想化基盤を構成しているクラスタに対してサーバーの停止が必要な保守の場合でも、業務を停止することなく1ノードずつ切離しと組込みを行う機能です。

本機能は、拡張ボードの交換などのサーバーの再起動を伴う保守作業の一部を自動化することで、お客様の作業を削減します。

ノード切離し／組込み機能は、以下の一連の操作（「3. 保守作業の実行」を除く）を自動化します。

1. ISMのメンテナンスモードの設定
2. 保守対象サーバーの停止
3. 保守作業の実行（手動での作業）
4. 保守対象サーバーの起動
5. ISMのメンテナンスモードの解除

図2.43 ノード切離し／組込み機能の動作概要



ADVM#1、ADVM#2：PRIMEFLEX for VMware vSAN専用ADVM
vCSA（vCenter）：vCenter Server Appliance

注意

PRIMEFLEX HSでは、ノード切離し／組込み機能は使用できません。

2.13.5.1 タスク一覧

ノード切離し／組込み機能は、クラスタ管理機能のGUIから実行できます。ノード切離し／組込みの処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。ノード切離し／組込み機能のタスク名は「Node Disconnection」と「Node Reintegration」です。タスク一覧からタスクタイプが「Node Disconnection」、または「Node Reintegration」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、ノード切離し／組込みの適用クラスタごとに1つ表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.28 ノード切離しサブタスクの処理一覧

処理名	設定項目名	設定項目内容
Node Disconnection （ノード切離し対象サーバーのメンテナンス設定とサーバーの停止を行います）	1. Target Server VM Existence Check 2. Enabling ISM Maintenance Mode 3. Target Server Turn On LED 4. Enabling Maintenance Mode 5. Stopping Target Server	1. 対象サーバーのVMが存在しないことを確認する 2. 対象サーバーをISMのメンテナンスモードに設定する 3. 対象サーバーのLED点灯 4. 対象サーバーをESXiのメンテナンスモードに設定する 5. 対象サーバーを停止する

表2.29 ノード組込みサブタスクの処理一覧

処理名	設定項目名	設定項目内容
Node Reintegration （ノード組込み対象サーバーのサーバー起動とメンテナンスモード解除を行います）	1. Starting Target Server 2. Disabling Maintenance Mode 3. Disabling ISM Maintenance Mode 4. Target Server Turn Off LED 5. Reconfigure vSphere HA	1. 対象サーバーを起動する 2. 対象サーバーをESXiのメンテナンスモードから解除する 3. 対象サーバーをISMのメンテナンスモードから解除する 4. 対象サーバーのLED消灯 5. 対象サーバーのvSphere HAを再構成する

2.13.6 バックアップ機能

バックアップ機能とは、PRIMEFLEX for VMware vSANの仮想化基盤を構成しているクラスタに対してESXiサーバーとvCSAのバックアップを行う機能です。

本機能は、障害発生時のシステム復旧のために、ESXiサーバーとvCSAのバックアップ作業を自動化することで、お客様の作業を削減します。

バックアップ機能は、以下の操作を自動化します。

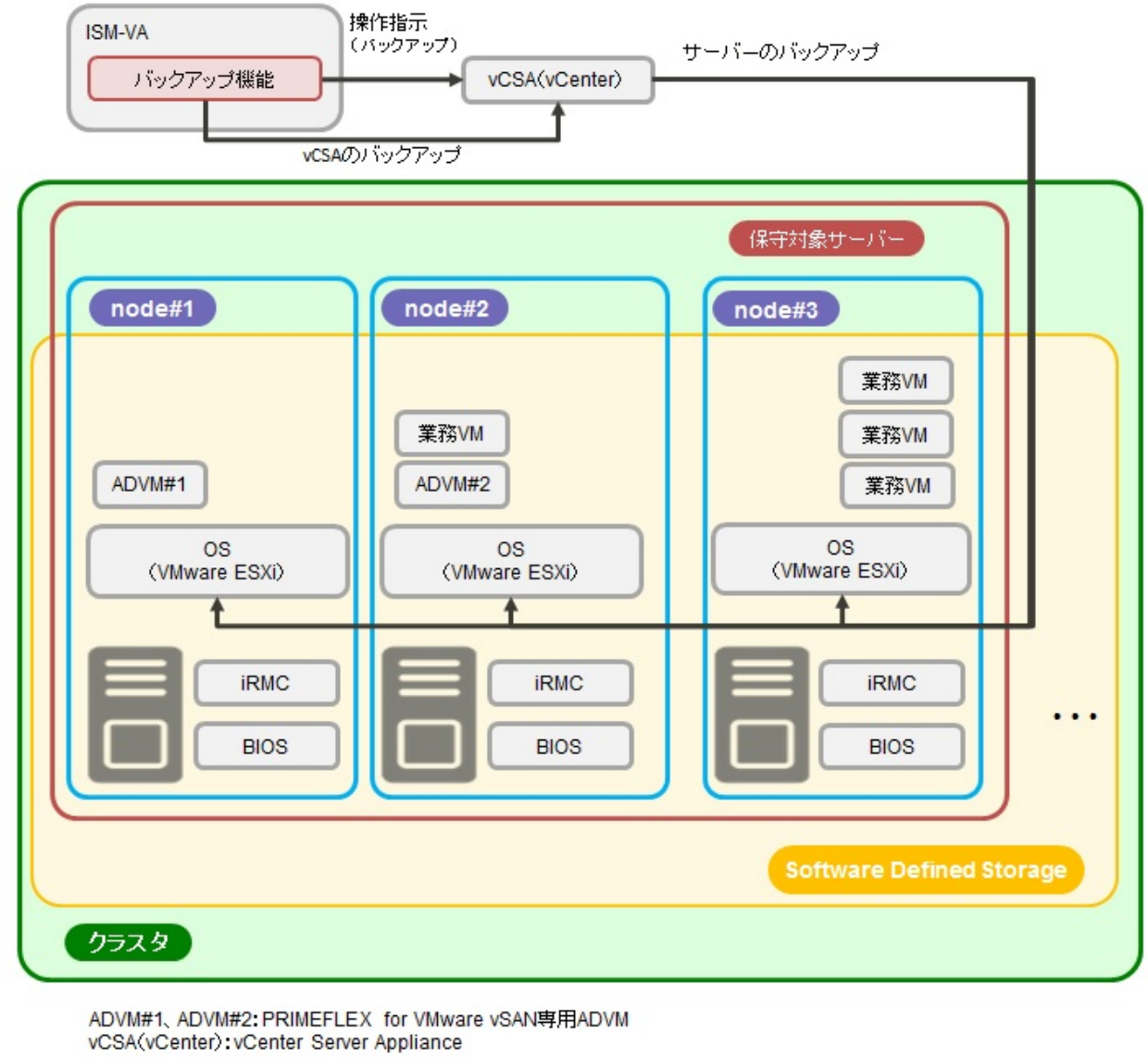
1. バックアップ先のマウント
2. 対象サーバーのSSHサービスを有効化
3. 対象サーバーのバックアップ
4. 対象サーバーのSSHサービスを無効化
5. 対象vCSAのバックアップ
6. バックアップ先のアンマウント

バックアップ機能でバックアップ可能な対象は、以下のとおりです。

凡例：○＝対応、×＝未対応

対象	対応可否
クラスタを構成するノード	○
クラスタを構成するvCSA	○

図2.44 バックアップ機能の動作概要



ADVM#1、ADVM#2:PRIMEFLEX for VMware vSAN専用ADVM
vCSA(vCenter):vCenter Server Appliance

注意

PRIMEFLEX HSでは、バックアップ機能は使用できません。

2.13.6.1 タスク一覧

バックアップ機能は、クラスタ管理機能のGUIから実行できます。バックアップの処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。バックアップのタスク名は「Backup」です。タスク一覧からタスクタイプが「Backup」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、バックアップの適用クラスタごとに1つ表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.30 バックアップサブタスクの処理一覧

処理名	設定項目名	設定項目内容
Backup （バックアップ対象サーバーとvCSAのバックアップを行います）	1. Mount Backup Destination 2. Check Backup Destination 3. Backup Server 4. Backup vCSA 5. Unmount Backup Destination	1. バックアップ先をマウントする 2. バックアップ先の容量をチェックする 3. サーバーをバックアップする[注] 4. vCSAをバックアップする 5. バックアップ先をアンマウントする

[注]:サーバーのバックアップでは、バックアップ対象のサーバーに対して、事前にSSHサービスを有効化し、バックアップした後、SSHサービスの無効化を行います。

2.13.7 リストア機能

リストア機能とは、PRIMEFLEX for VMware vSANの仮想化基盤を構成しているクラスタに対してvCSAのリストアを行う機能です。

本機能は、障害発生時のシステム復旧のために、vCSAのリストア作業を自動化することで、お客様の作業を削減します。

リストア機能は、以下の操作を自動化します。

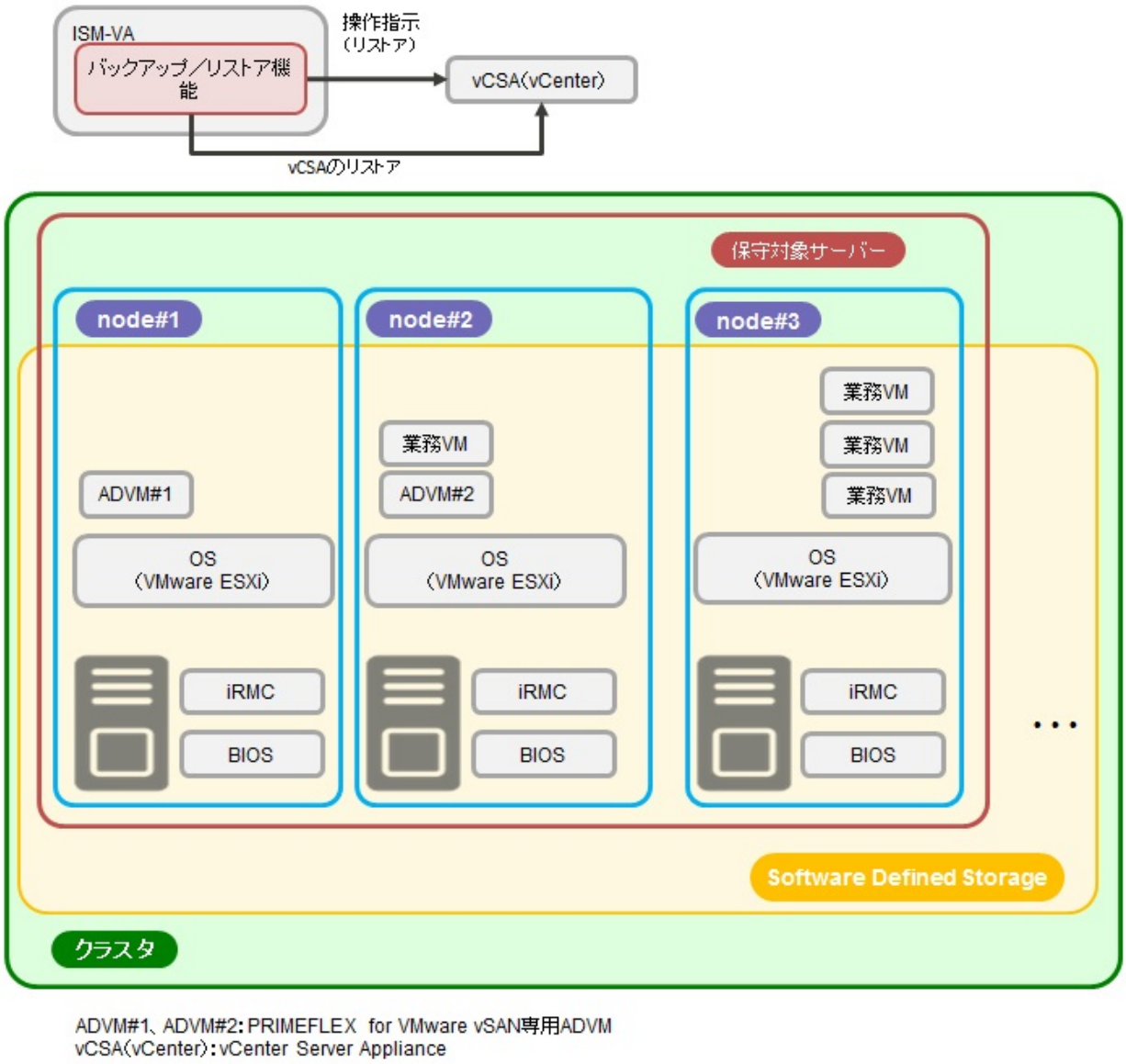
1. リストア先のマウント
2. vCSAをリストアするサーバーのSSHサービスを有効化
3. 対象vCSAのリストア
4. vCSAをリストアするサーバーのSSHサービスを無効化
5. 対象vCSAのvDSのリストア
6. リストア先のアンマウント

リストア機能でリストア可能な対象は、以下のとおりです。

凡例:○＝対応、×＝未対応

対象	対応可否
クラスタを構成するノード	×
クラスタを構成するvCSA	○

図2.45 リストア機能の動作概要



注意

- PRIMEFLEX HSでは、リストア機能は使用できません。
- ESXiのリストア機能は使用できません。

2.13.7.1 タスク一覧

リストア機能は、クラスタ管理機能のGUIから実行できます。リストアの処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。リストア機能のタスク名は「Restore」です。タスク一覧からタスクタイプが「Restore」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、リストアの適用クラスタごとに1つ表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.31 リストアサブタスクの処理一覧

処理名	設定項目名	設定項目内容
Restore （vCSAのリストアを行います）	1. Mount Restore Destination 2. Check Restore Destination 3. Restore vCSA 4. Restore vDS 5. Unmount Restore Destination	1. リストア先をマウントする 2. リストア先の容量をチェックする 3. vCSAをリストアする[注] 4. vDSをリストアする 5. リストア先をアンマウントする

[注]:vCSAのリストアでは、vCSAをリストアするサーバーに対して、事前にSSHサービスの有効化を行い、リストアした後にSSHサービスの無効化を行います。

2.13.8 クラスタ停止機能

クラスタ停止機能とは、PRIMEFLEX for VMware vSANの仮想化基盤を構成しているクラスタに対して停止を行う機能です。

クラスタ内のすべてのノードをシャットダウンして電源断の状態にします。

クラスタ停止機能を使って停止したクラスタの起動は、クラスタ起動コマンドによって行います。

クラスタ停止機能の設定を変更した場合は、通常の手作業によるクラスタ起動には対応しません。

クラスタ起動コマンドは、下記のSupportDesk-Webからダウンロードしてください。なお、ダウンロードにはSupportDesk-Webの契約が必要です。SupportDesk-Webの利用については、当社担当営業にお問い合わせください。

ファイルダウンロード［SupportDesk-Web］

URL: https://eservice.fujitsu.com/supportdesk/svpflex/download/clus_cmd.html

SupportDesk > Infrastructure Manager for PRIMEFLEX > ダウンロード > クラスタ停止・起動コマンド

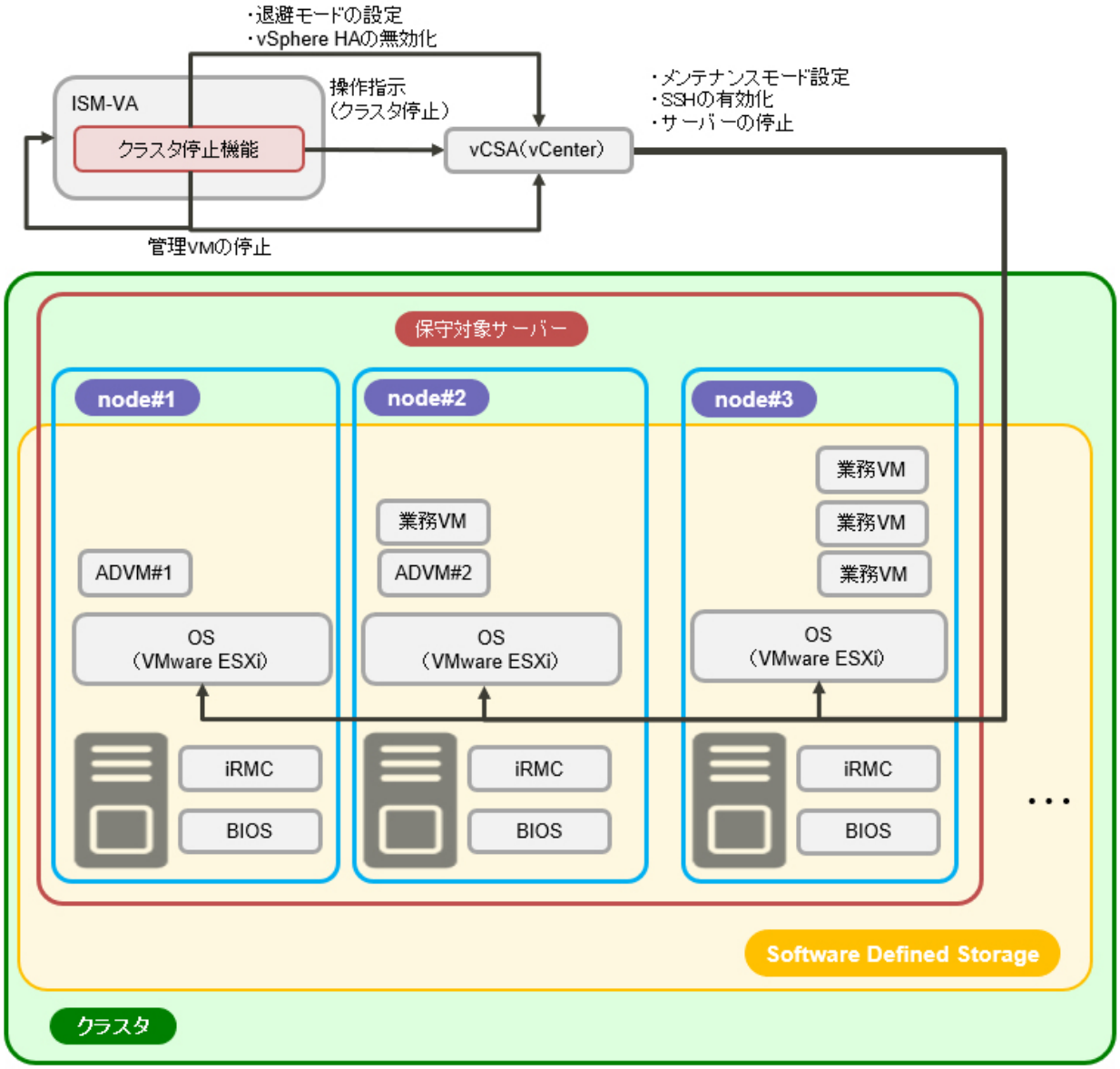
クラスタ起動コマンドの使用方法とクラスタ停止機能の設定変更については、以下を参照してください。

『Infrastructure Manager for PRIMEFLEX クラスタ停止・起動機能 操作手順書』

クラスタ停止機能は、以下の操作を自動化します。

1. 対象クラスタの退避モードの設定（vSphere 7.0 Update 1以降の場合）
2. 対象クラスタのvSphere HAの無効化
3. 対象クラスタの全ノードに対してISMのメンテナンスモードの設定
4. 対象クラスタの全ノードのSSHサービスを有効化
5. 対象クラスタの全ノードに対してESXi停止・起動プログラムを配備
6. 対象クラスタのvSANストレージ再同期中コンポーネントの確認
7. 対象クラスタ内のISM-VAをシャットダウン
8. 対象クラスタ内のvCSAをシャットダウン
9. 対象クラスタの全ノードに対してESXiのメンテナンスモードの設定
10. 対象クラスタの全ノードのシャットダウン

図2.46 クラスタ停止の動作概要

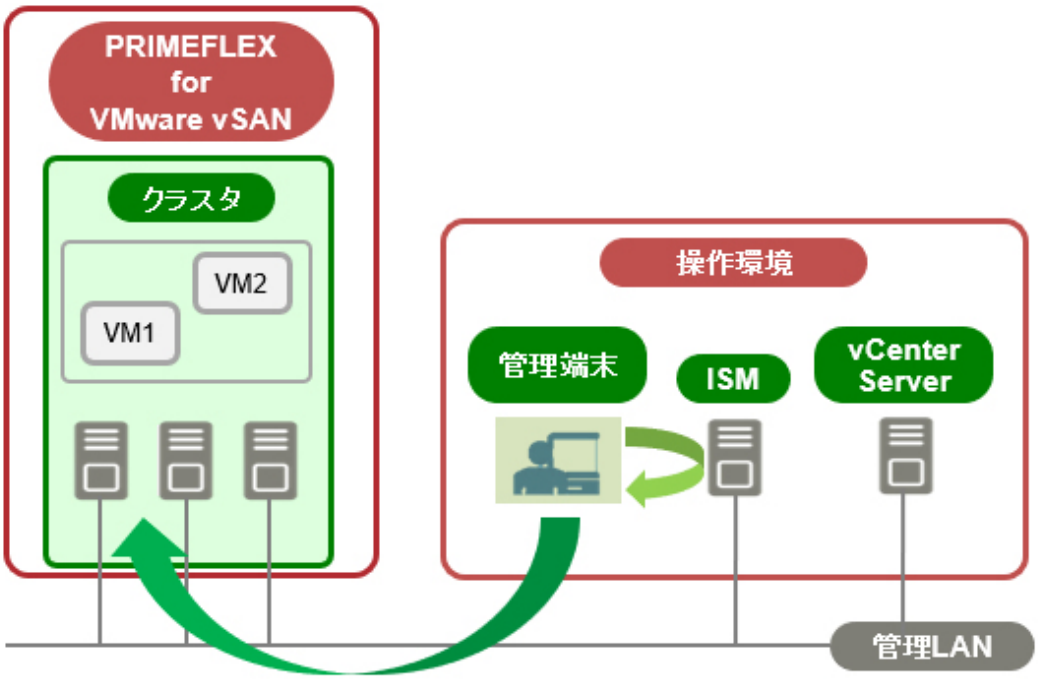


ADVM#1、ADVM#2：PRIMEFLEX for VMware vSAN専用ADVM
vCSA(vCenter)：vCenter Server Appliance

動作説明

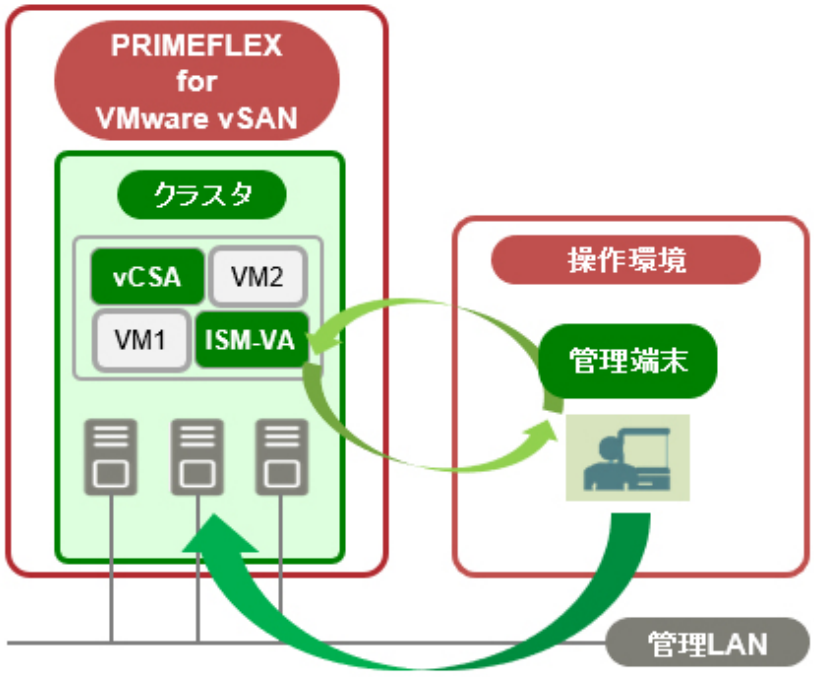
クラスタ停止機能は、「図2.47 クラスタ停止機能の動作」に示す構成で動作します。

図2.47 クラスタ停止機能の動作



本機能は、ISM-VAとvCSAを同一のクラスタ内に配置する構成(「図2.48 ISM-VAとvCSAをクラスタに配置した構成での動作」)にも対応しています。本構成は前記の構成(「図2.47 クラスタ停止機能の動作」)の特殊なケースに相当します。

図2.48 ISM-VAとvCSAをクラスタに配置した構成での動作



ISM-VAとvCSAを配置したクラスタは、PRIMEFLEXで起動中の最後のクラスタであるときにのみクラスタ停止機能で停止できます。クラスタ内のISM-VAとvCSAは、クラスタの停止処理に伴い、自動で停止されます。

2.13.8.1 タスク一覧

クラスタ停止機能は、クラスタ管理機能のGUIから実行できます。クラスタ停止の処理は、ISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、「タスク」画面にタスク一覧が表示されます。クラスタ停止機能のタスク名は「Cluster Stop」です。タスク一覧からタスクタイプが「Cluster Stop」の[タスクID]を選択すると、「タスク」画面にタスク情報とサブタスクリストの一覧が表示されます。サブタスクリストの一覧は、クラスタ停止の適用クラスタごとに1つ表示されます。

サブタスクリストのメッセージ欄に以下の形式で表示される各処理名とその実施内容を以下に示します。

＜処理名＞：＜設定項目名＞

表2.32 クラスタ停止サブタスクの処理一覧

処理名	設定項目名	設定項目内容
Cluster Stop （クラスタ停止の事前処理と対象クラスタ内のサーバーの停止を行います）	1. Check Condition For Stopping Cluster 2. Enable Retreat Mode 3. Preset For Stopping Cluster 4. Disable vSphere HA 5. Enable ISM Maintenance Mode 6. Stop Cluster	1. クラスタ停止の事前チェック 2. 対象クラスタの退避モードを設定する（vSphere 7.0 Update 1以降の場合） 3. 対象クラスタ内のサーバーに停止事前処理の実施をする [注] 4. 対象クラスタのvSphere HAを無効化する 5. 対象クラスタ内のサーバーをISMのメンテナンスモードに設定する 6. 対象クラスタの停止

[注]：事前処理では、SSHサービスの有効化やクラスタ情報収集を行います。

2.13.9 VMware vSANクラスタに関連するログ一括収集

vSANクラスタを構成するリソース（ノード、仮想化管理ソフトウェア、ハイパーバイザー）に異常が発生した場合、問題箇所を調査するために必要なPRIMEFLEX for VMware vSANのクラスタに関連するログを一括で取得します。本機能の利用によりログ採取の作業手順を軽減できます。

収集するログ

クラスタに関連する以下のログを収集します。

収集ログ	内容
ハードウェアログ	クラスタを構成するノードのハードウェアログ
オペレーティングシステムログ	クラスタを構成するノードのオペレーティングシステムログ
vm-support	クラスタを構成するノードのESXiから取得するサポートログ [注]
vc-support	vCenterから取得するサポートログ [注]
RVC（VMware Ruby vSphere Console Command）コマンド	vCenter Server Appliance上で実行したRVCコマンド「vsan.support_information」の実行結果

[注]：ログ詳細は、VMwareのWebサイトを確認してください。

https://kb.vmware.com/s/article/2032892

注意

- ISMの動作モードがAdvanced for PRIMEFLEXモードではない場合、vSANログ一括収集操作時に「system License type error.」が出力されます。ISMの動作モードを確認してください。

- ISMのサービスが起動していない場合、vSANログ一括収集操作時に「ISM Service is not running.」が出力されます。ISMサービスの起動後に実施してください。ISMサービス起動の詳細は、「4.1.4 ISMのサービス起動と停止」を参照してください。
- 対象クラスタがVMware vSAN クラスタではない場合でもvSANログ一括収集の実施は可能です。ただし、vm-support, vc-support, RVCコマンドのログは取得できません（vc-supportおよびRVCコマンドの収集状態がErrorとなります）。
- 起動していないサーバーやメンテナンスモードのサーバーのログは収集されません。
- vCenter Server Applianceに対してSSHによるアクセスができない場合、RVCコマンドは収集されません。

2.13.9.1 vSANログ一括収集操作

コンソールからadministratorグループユーザーでISM-VAにログインし、下記コマンドを実行します。

ISM-VA管理機能のコマンドに操作オプションを組み合わせて指定します。

表2.33 vSANログ一括収集のコマンド

機能	コマンド
vSANログ一括収集	ismadm cluster logcollect ＜操作オプション＞

表2.34 vSANログ一括収集コマンドの操作オプション

操作名	操作オプション	内容
クラスタ名確認	-listcluster	クラスタ名の一覧を表示します
収集開始	-collect	vSANログ一括収集を開始します
収集状態確認	-status	vSANログ一括の収集状態を表示します

各操作オプションについて解説します。

クラスタ名確認(-listcluster)

ログ収集の対象クラスタのクラスタ名を確認するためのコマンドです。ISMに登録されているクラスタの一覧（クラスタ名、クラスタの種類）を表示します。

VMware vSAN クラスタの場合はクラスタの種類に「VMware」と表示されます。

```
# ismadm cluster logcollect -listcluster
```

例：クラスタ名確認の実行結果（クラスタが3つ設定されていた場合）

```
# ismadm cluster logcollect -listcluster
Cluster List:
 TestCluster62vSanTrue              VMware
 Cluster-1                          VMware
 S2DCluster                         Hyper-V
```

「Cluster List:」の下に ＜クラスタ名＞と＜クラスタの種類＞が1行ずつ表示されます。

収集開始(-collect)

vSANログ一括収集を開始します。

```
# ismadm cluster logcollect -collect -dir ＜ディレクトリー＞ -file ＜ファイル名＞ -port ＜ポート番号＞
```

引数	必須	説明	備考
-dir ＜ディレクトリー＞	○	ログを出力するディレクトリー	/Administrator/ftp 配下のディレクトリーを指定します。
-file ＜ファイル名＞	○	ファイル名	出力するログファイル名 例： Cluster62vSanLog.zip

引数	必須	説明	備考
			（拡張子.zipがない場合は、ログファイル名に.zipが付与されます）
-port ＜ポート番号＞		ポート番号	vCenterのsshポート番号を22以外に設定している場合に指定します。

コマンド実行後に表示されるコマンドプロンプトに以下を指定します。

プロンプト	必須	説明	備考
ClusterName:	○	クラスタ名	ログ収集したいクラスタ名を指定します。
Password:		zipパスワード	収集ログファイルにパスワードを設定する場合に指定します。省略した場合はパスワードなしとなります。

最後に「'クラスタ名' Collect Start?(Y/N)」と表示された後、入力した内容に問題なければ「Y」を入力します。収集を開始すると「Cluster log collection started. Please wait for completion.」が出力されます。

入力した内容を訂正する場合は、「N」を入力し再度コマンドを実行してください。

注意

- vSANログ一括収集を開始すると完了するまで停止することはできません。
- クラスタの操作を行っている場合は、クラスタの操作が完了してからvSANログ一括収集を開始してください。
- 指定したクラスタ名が存在しない場合は、「The specified cluster name does not exist.」が出力されます。クラスタ名を確認してください。
- vSANログ一括収集を実施中のクラスタに対して収集開始することはできません。実施した場合は、「Already running on the same cluster.」が出力されます。
- Administratorユーザーグループの仮想ディスクの空き容量が不足している場合は「capacity directory error.」が出力されます。この場合は、仮想ディスクの空き容量を拡張してください。必要な空き容量は、4ノード構成で約6Gbyteです。vm-support、vc-supportのログサイズによってはさらに多くの容量が必要となる場合があります。
- -dir で指定したログ出力先ディレクトリーが存在しない場合は、「Target directory does not exist.」が出力されます。存在するディレクトリーを指定してください。
- RVCコマンドが収集エラーとなる場合は、vCenter Server Applianceのsshポートが-portで指定したポート番号（指定しない場合は22）と合っていることを確認してください。
- vSANログ一括収集を実施中にISM-VA再起動や停止を実施した場合は収集動作が中止されます。ISM-VA起動後、収集状態確認を実施した場合は中止した時点の収集状態が表示されますが、新たに収集を開始することが可能です。

ポイント

vSANログ一括収集は複数のクラスタに対して同時に実施することが可能です。それぞれのクラスタに対して収集開始コマンドを実行してください。ただし、収集時間はそれぞれのクラスタ分を合計した時間がかかります。

収集時間

収集時間の目安はクラスタを構成するノード 4ノードの場合で約60分です。

vSANログ一括収集ではvSANクラスタを構成する各ノードや仮想化管理ソフトウェアからログを収集します。そのため、クラスタの構成やログサイズによっても収集時間は変動します。また、複数クラスタで同時に収集した場合はさらに時間がかかります。

収集の状態は「収集状態確認(-status)」で確認してください。

収集状態確認(-status)

vSANログ一括収集の動作状態を確認します。

```
# ismadm cluster logcollect -status
```

プロンプト	必須	説明	備考
ClusterName:		クラスタ名	省略した場合はISMに登録されているすべてのクラスタの収集状態を表示します。

収集状態出力内容

クラスタごとに以下の項目が出力されます。

項目	説明
ClusterName	クラスタ名
Directory	収集開始(-collect)で指定したディレクトリー名
FileName	収集開始(-collect)で指定したファイル名
Status	vSANログの収集状態 ・ Wait:収集待ちです ・ Collecting:収集中です ・ Complete:収集が完了しました ・ Error:エラーが発生しました
CollectStartTime	収集開始時間(ISM-VAに設定されているタイムゾーンの時刻)
CollectEndTime	収集終了時間(ISM-VAに設定されているタイムゾーンの時刻。収集が完了するまでは空文字)
CheckSum	チェックサム用ハッシュ値(SHA-256ハッシュ値)
[CmsStatus]	vc-supportおよびRVCコマンドの収集状態 表示される値(Wait／Collecting／Complete／Error)の内容は「Status」の説明と同様です。
[NodeStatus]	各ノードのログの収集状態(ノード数分表示) 表示される値(Wait／Collecting／Complete／Error)の内容は「Status」の説明と同様です。

vSANログ一括収集を実施していないクラスタは"'クラスタ名'is not collecting."と出力されます。

2.13.9.2 出力ファイル

収集状態確認でvSANログの収集状態が「Complete」となった場合、収集開始時に指定したディレクトリーにログファイルと収集結果の情報ファイルが作成されます。「Error」となった場合は、ログファイルは作成されません。

ファイル	ファイル名	内容
ログファイル	＜指定ファイル名＞.zip [注]	収集したログをzipで圧縮したファイル パスワードを指定している場合は、指定パスワードで暗号化されます。
収集結果の情報ファイル	＜指定ファイル名＞.Result	収集結果の情報をテキストで記載したファイル

[注]:指定ファイル名の末尾に「.zip」が付いている場合は、「.zip」は重複して付与されません

収集したログファイルの構成

ログファイルには、以下のファイルが格納されます。

ファイル	内容
Storagelog.zip	ハードウェアログ、オペレーティングシステムログ、vm-supportログ

ファイル	内容
Cmslog.zip	vc-supportログ、RVCコマンドログ

収集結果の情報ファイルの内容

収集結果の情報ファイルには、以下の項目が設定されます。

項目	説明
ClusterName	クラスタ名
Directory	収集開始(-collect)で指定したディレクトリー名
FileName	収集開始(-collect)で指定したファイル名
Status	vSANログの収集結果 ・ Complete：収集完了 ・ Error：エラー終了
CheckSum	チェックサム用ハッシュ値（SHA-256ハッシュ値）
CollectStartTime	収集開始時間（ISM-VAに設定されているタイムゾーンの時刻）
CollectEndTime	収集終了時間（ISM-VAに設定されているタイムゾーンの時刻）
[CmsStatus]	vc-supportおよびRVCコマンドの収集結果 ・ Complete：正常に収集 ・ Error：収集エラー
[NodeStatus]	各ノードのログの収集結果（ノード数分表示） ・ Complete：正常に収集 ・ Error：収集エラー

2.13.10 世代切替機能

世代切替機能とは、現在のPRIMEFLEX の世代管理情報を後継モデルの世代管理情報に更新する機能です。
世代管理情報とは、ISM内で保持する以下の情報を指します。

- PRIMEFLEXの仮想化基盤構築機能やクラスタ作成機能で構築したPRIMEFLEXの世代（登録世代）
- ノードがPRIMEFLEXに参加した契機（登録契機）
- ISMの世代切替機能を実行した後の世代（切替世代）

世代切り替えにより、システムを継続使用しながらサーバーの後継機種への入れ替えができます。
世代切替機能を実施するには、切り替えるPRIMEFLEX世代よりも古い世代のサーバーをすべて減設する必要があります。

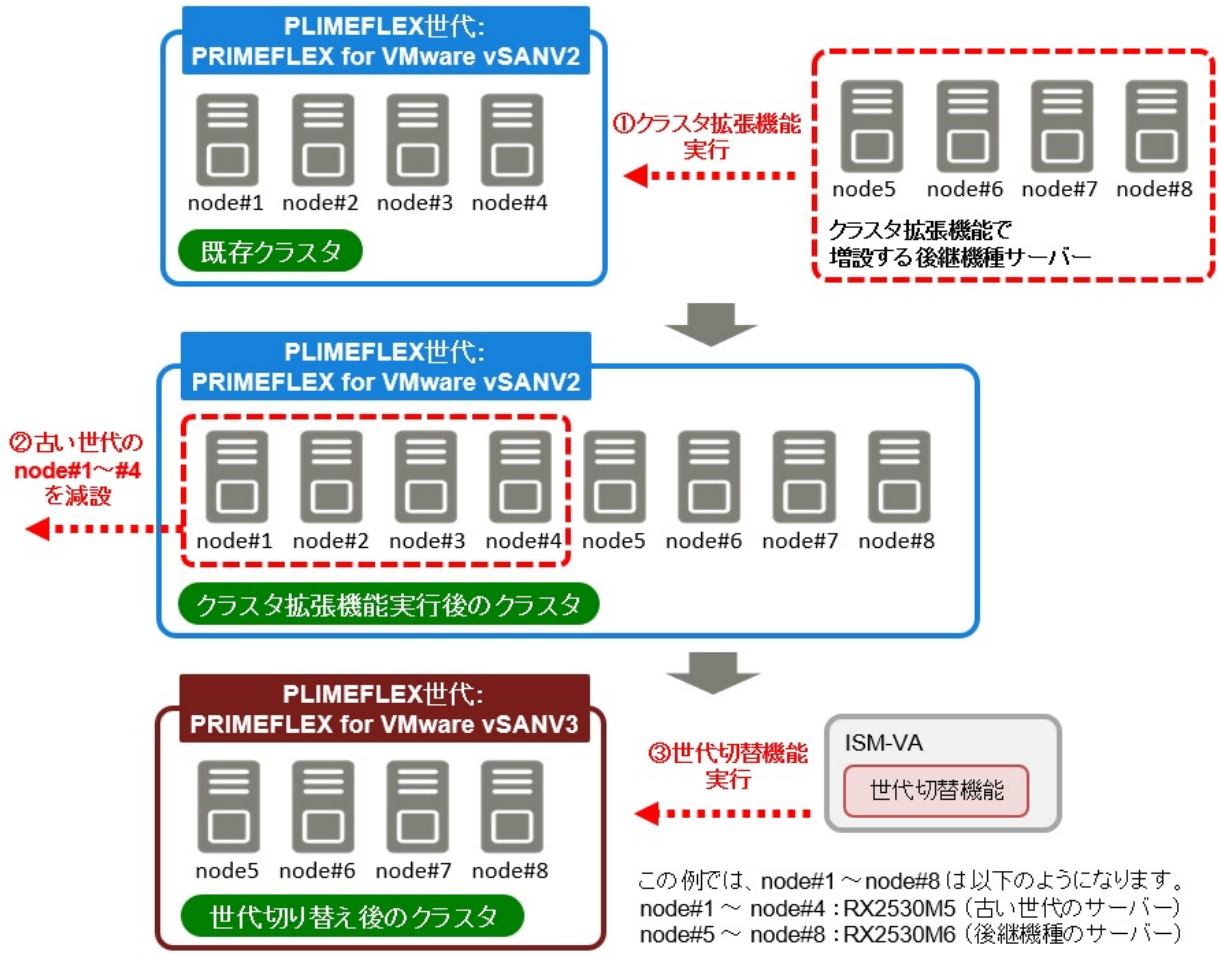
複数世代のサーバーが混在する場合、世代は最も古い世代のサーバーに対応したものとなります（例：世代切り替えを未実施の状態でM4／M5サーバーが混在したシステムの場合、世代は PRIMEFLEX for VMware vSAN V1 となります）。

世代切り替えを実施する場合は、PRIMEFLEX専用SupportDesk契約が必要となります。詳細は、PRIMEFLEX for VMware vSANの『サーバー増設／世代切り替えガイド』を参照してください。

https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

なお、PRIMEFLEX専用SupportDeskを未契約で世代切り替えを実施した場合、世代管理情報を初期化することが可能です。

図2.49 世代切替機能の全体像



世代切替機能によりPRIMEFLEXの世代管理情報を更新するには、既存クラスタに対して後継機種のサーバーを増設し、古い世代をすべて減設する必要があります。

2.14 ISM運用基盤の機能

ISMの運用基盤となる機能について説明します。

- 2.14.1 ユーザー管理機能
- 2.14.2 リポジトリ管理機能
- 2.14.3 Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLIの導入
- 2.14.4 タスク管理
- 2.14.5 ISM-VA管理機能
- 2.14.6 仮想化管理ソフトウェア管理機能
- 2.14.7 共有ディレクトリー管理機能
- 2.14.8 ISM連携管理機能
- 2.14.9 他ソフトウェア連携機能

2.14.1 ユーザー管理機能

ISMのユーザーは、以下のように管理されています。

- ユーザーごとにユニークなログイン名とパスワードが割り当てられます。
- ユーザーロールという権限によって、ノードに対するアクセス方法や、各機能の実行が制限されます。
- ユーザーをグループ化(以降、ユーザーグループと表記)することによって、ユーザーグループ単位で、各機能のアクセス範囲が制限されます。
- ノードをグループ化(以降、ノードグループと表記)し、ユーザーグループと対応付けることによって、ユーザーのアクセスできるノードの範囲が制限されます。

ユーザーグループとノードグループの関係を、「図2.50 ユーザーグループ、ノードグループ、ロールの関係」で示します。

ここでは、以下について説明します。

- ユーザーグループの種別と、そのユーザーグループに属するユーザーのアクセスできる範囲
- ユーザーロールの種別と、そのロールを持つユーザーが実行できる操作
- セキュリティポリシーの設定
- ユーザー管理機能の操作
- Microsoft Active DirectoryまたはOpenLDAPとの連携
- 多要素認証

ユーザーグループの種別と、そのユーザーグループに属するユーザーのアクセスできる範囲

ユーザーグループをノードグループに対応付けることで、ユーザーグループに属するユーザーのアクセス範囲を定義します。

ユーザーグループ名	管理対象ノード	アクセス範囲
Administratorグループ	全てのノードを管理	すべてのノード、およびノードに関連する資源(ログなど)にアクセスできます。 ISMの全体管理用のユーザーグループです。
Administratorグループ以外	全てのノードを管理	すべてのノード、およびノードに関連する資源(ログなど)にアクセスできます。 ISMの全体管理用のユーザーグループです。
	指定ノードグループ内	ユーザーグループと対応付けたノードグループ内のノードおよびノードに関連する資源(ログなど)にアクセスできます。
	管理ノードなし	すべてのノード、およびノードに関連する資源(ログなど)がありません。

ポイント

以降の説明では、管理対象ノードが「全てのノードを管理」と指定されているユーザーグループは、Administratorグループとみなしてください。

注意

管理対象ノードが「全てのノードを管理」の場合、変更はできません。また、管理対象ノードが「指定ノードグループ内」「管理ノードなし」の場合、「全てのノードを管理」への変更はできません。

ユーザーロールの種別と、そのロールを持つユーザーが実行できる操作

アクセス範囲内のノードに対してユーザーが実行できる操作は、ユーザーロールに応じて以下のように定義されます。

ユーザーロール	アクセスの種類
Administratorロール	ノード、ユーザー、および各種設定の追加、変更、削除、および閲覧ができます。

ユーザーロール	アクセスの種類
Operatorロール	ノード、各種設定の変更、および閲覧ができます。 ユーザー管理はできません。
Monitorロール	ノード、各種設定の閲覧ができます。 ユーザー管理、ノードの追加、変更、削除はできません。

ポイント

- Operatorによる設定の変更可否は、本マニュアルでの各種機能の記載内容（アイコン表記）を参照してください。アイコン表記については、以下の説明を参照してください。
- 以降の説明では、Administratorグループに属し、Administratorロールを持つユーザーのことを「ISM管理者」と表記します。

ユーザーがアクセス可能な権限の説明を行うため、以降ではユーザーが属するユーザーグループと、そのグループ内でユーザーが持つユーザーロールに分類して以下のアイコンで示します。

ユーザーグループ	ユーザーロール	実行可能	実行不可
Administratorグループ	Administratorロール	Admin	
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor
その他のグループ （Administratorグループ以外）	Administratorロール	Admin	Admin
	Operatorロール	Operator	Operator
	Monitorロール	Monitor	Monitor

操作を実行できるユーザーの属性を以下のように示します。

例）

― 上記の表示の場合、以下のユーザーグループとユーザーロールの組合わせで設定されたユーザーが実行できることを表します。

- Administratorグループに属し、AdministratorロールまたはOperatorロールを持つユーザー
- Administratorグループ以外のグループに属し、AdministratorロールまたはOperatorロールを持つユーザー

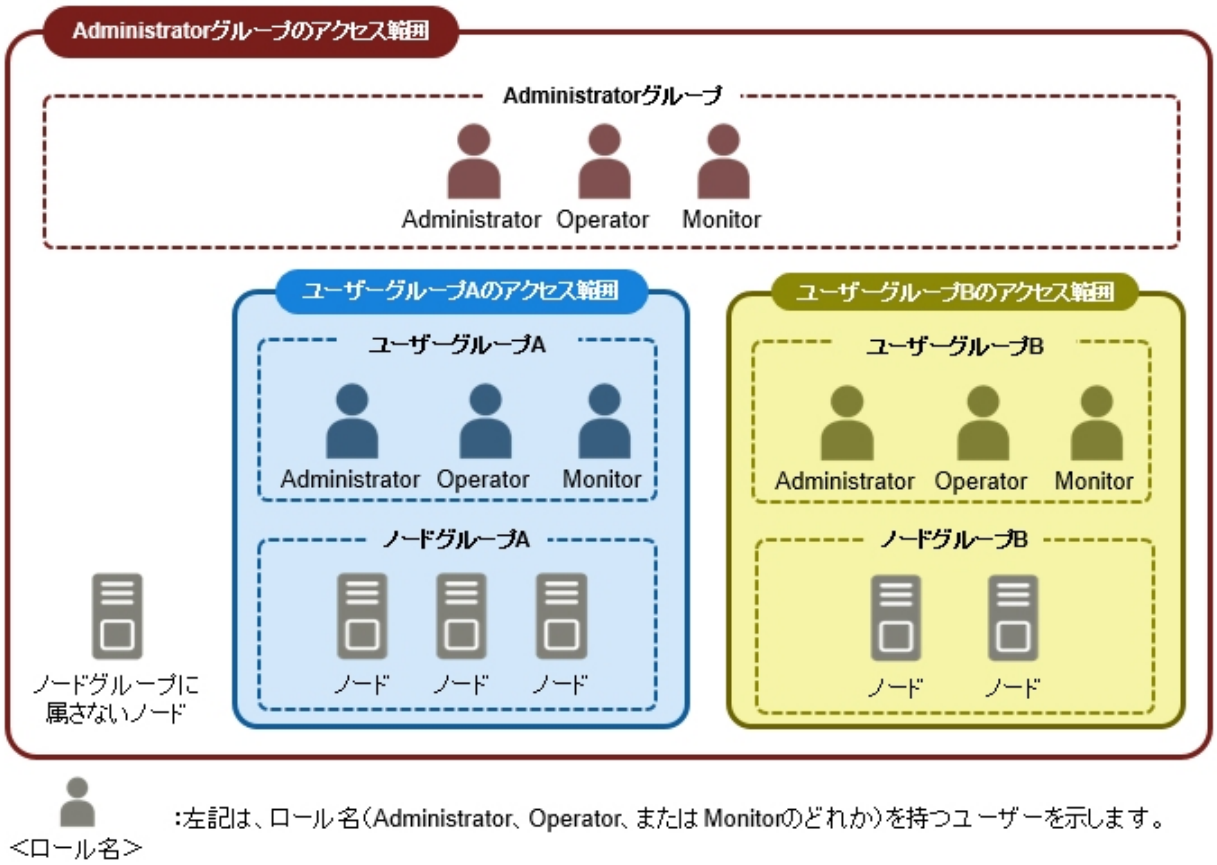
― グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。

注意

Administratorグループに属し、Administratorロールを持つユーザーは、ISMの全体管理を行う特別なユーザー（ISM管理者）です。

Administratorグループに属し、OperatorロールまたはMonitorロールを持つユーザーは、Administrator以外のグループに属し、OperatorロールまたはMonitorロールを持つユーザーとはアクセス範囲が異なります。ただし、実行できる操作は同じです。

図2.50 ユーザーグループ、ノードグループ、ロールの関係



セキュリティポリシーの設定

セキュリティポリシーの設定は、以下の手順で行います。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[セキュリティポリシー]を選択します。
3. [編集]ボタンを選択し、セキュリティポリシーを設定します。

セキュリティポリシーには、ユーザーパスワードポリシーとログインポリシーがあります。

ユーザー管理で扱うパスワードと、ログインの制限を設定できます。

セキュリティポリシーはISM全体で1つ設定できます。セキュリティポリシーを強固に設定することで、よりセキュアな運用が可能となります。
設定項目は以下のとおりです。

ユーザーパスワードポリシー

項目	設定値	設定後の動作
以前のパスワードの使用	・ 使用可能(推奨値) ・ 過去n回のパスワードの使用禁止 (1≦n≦24)	「ユーザー追加」画面、および「ユーザー設定編集」画面で、パスワードを設定するときにチェックされます。
パスワードの長さ	1～80(バイト) (推奨値:8(バイト))	

項目	設定値	設定後の動作
使用文字種類	• 限定しない(推奨値) • 数字、小文字、大文字、特殊文字[注2]のうち最低n種類使用する(2≦n≦4)	
ユーザー名と同じパスワード	• 許可する • 禁止する(推奨値)	
使用禁止文字列 [注1]	最大256個まで指定可能	
有効期限	• 無期限 • 1～365(日) (推奨値:90(日))	「無期限」以外を設定してログインした場合、以下のように動作します。 • 有効期限に達した場合 期限超過後のアクションが実行されます。 • 有効期限まで2週間に達した場合 警告メッセージが出力されます。 • Administratorの場合 初期設定パスワードを変更していない場合、警告メッセージが出力されます。
期限超過後のアクション	• 警告メッセージのみ出す • ログインを無期限にロックする(推奨値)	

[注1]:使用できないパスワードを設定します。設定した文字列と完全一致するパスワードが使用禁止となります。

[注2]:特殊文字として利用できる文字は、!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ です。

ポイント

[デフォルト]ボタンを選択すると、上記の表の推奨値に値が設定されます。

注意

ー パスワード有効期限に「無期限」以外を設定し、期限超過後のアクションに「ログインを無期限にロックする」を設定した場合の注意事項を以下に示します。

- ログインの制限は、ISMへのログインに限られます。FTPやISM-VAへのログインについては制限されないため、注意してください。
- パスワードの有効期限超過後、ISMへの初めてのログインは成功します。このときにパスワードを変更してください。パスワードを変更しなかった場合、ログインが無期限にロックされます。
- ログインが無期限にロックされた場合、ISM管理者にパスワードを再設定してもらうと、ロックが解除できます。
- ISM管理者は、ログインが無期限にロックされることはありません。警告メッセージのみ出力されます。

ログインポリシー

項目	設定値	説明
セッション有効時間	2～1440(分) (初期値:30(分))	何の操作も行わなかった場合、セッションがタイムアウトとなるまでの時間です。

項目	設定値	説明
アカウントロックしきい値	6～256(回) (初期値:6(回))	アカウントがロックされる操作の失敗回数と、アカウントがロックされる期間を指定します。 アカウントがロックされる操作を以下に示します。 ・ ログインを連続して失敗する ・ パスワード変更時に指定する現在のパスワードを連続して間違える アカウントがロックされた場合、ログインが禁止されます。
アカウントロック期間	1～1440(分) (初期値:30(分))	

注意

- ログインを連続して失敗した回数は、以下の場合にリセットされます。
  - ログインが成功した場合
  - 最後にログインが失敗したときからロック時間経過した場合
- パスワード変更時に指定する現在のパスワードを連続して失敗した回数は、以下の場合にリセットされます。
  - 現在のパスワードの指定が成功した場合
  - 最後に失敗したときからロック時間経過した場合
- ユーザーのセッション有効時間を設定した場合、ユーザーのセッション有効時間が優先されます。
- セッション有効時間を設定時に、特定の画面において画面の自動更新を設定している場合、自動更新されるごとにセッションが更新されます。そのため、画面の自動更新の間隔がセッション有効時間より短い場合、セッション有効時間を過ぎてもタイムアウトされません。画面の自動更新の設定は各画面で独立しているため、設定は画面ごとに無効にする必要があります。以下を設定することで、画面の自動更新を無効にすることができます。

画面	画面表示方法	操作
「ダッシュボード」画面	[ダッシュボード]選択	一時停止マークを選択する。
「ノード登録」画面	[構築]-[ノード登録]選択	自動更新の[停止]ボタンを選択する。
「ジョブ」画面	[構築]-[ジョブ]選択	
「タスク」画面	画面上部の[タスク]選択	

カスタムログインメッセージ

項目	設定値	説明
ログイン画面にメッセージを表示	有効または無効	メッセージ表示の有効／無効の設定です。
メッセージ	0～1024文字	表示するメッセージを設定します。任意の文字を登録できます。

ユーザー管理機能の操作

ユーザー管理機能は、主に以下の用途で利用する機能です。

- ISMのユーザーを管理
- ユーザーグループを管理
- ISMのユーザー認証を実施
- Microsoft Active DirectoryまたはOpenLDAPと連携
- ノードグループを管理

- administratorユーザーの有効／無効を設定

ユーザー管理機能では、操作ユーザーに応じて操作対象が異なります。

操作ユーザー	操作対象
Administratorグループに属し、Administratorロールを持つユーザー	存在するユーザーグループのすべてが操作対象です。
Administrator以外のグループに属し、Administratorロールを持つユーザー	操作ユーザーが所属するユーザーグループが操作対象です。

注意

グループ変更

ノードグループに所属するノードを、別のノードグループに所属させる場合や、ノードグループから解除する場合は、事前に以下の操作を完了させてください。

- 当該ノード上で実行中のタスクがある場合は、完了を待ってください。
- 当該ノードに適用済みのプロファイルがある場合は、適用を解除してください。
- 当該ノードのログ収集スケジュールは、削除してください。
- 当該ノードから取得し保存しているログは、削除してください。
- 当該ノードに関するアラーム設定は、削除してください。
- ユーザーグループに所属するユーザーがプロファイルを設定していた場合、そのユーザーからプロファイルの設定を参照／変更できなくなります。その場合、Administratorグループのユーザーでプロファイルを削除してください。
- 保存したログを削除し忘れた場合は、一度ノードを元のユーザーグループに戻してから削除してください。

ユーザーグループ削除

ユーザーグループに所属するユーザーがプロファイル、ログ関連操作を設定していた場合、そのユーザーからプロファイル、ログ関連操作の設定を参照／変更できなくなります。その場合は、Administratorグループのユーザーで修正してください。

ユーザーグループを削除する場合は、事前に以下の操作を完了させてください。

- 適用済みプロファイルは適用を解除してください。
- ユーザーグループに含まれるプロファイル、プロファイルグループ、ポリシー、ポリシーグループは削除してください。
- インポートしたOSメディア、ServerView Suite DVDはリポジトリから削除してください。
- ログ収集スケジュールは削除してください。
- 保存したログは削除してください。

ユーザーグループ名の変更

ユーザーグループ名を変更する場合は、事前に以下のタスクが実行中でないことを確認してください。

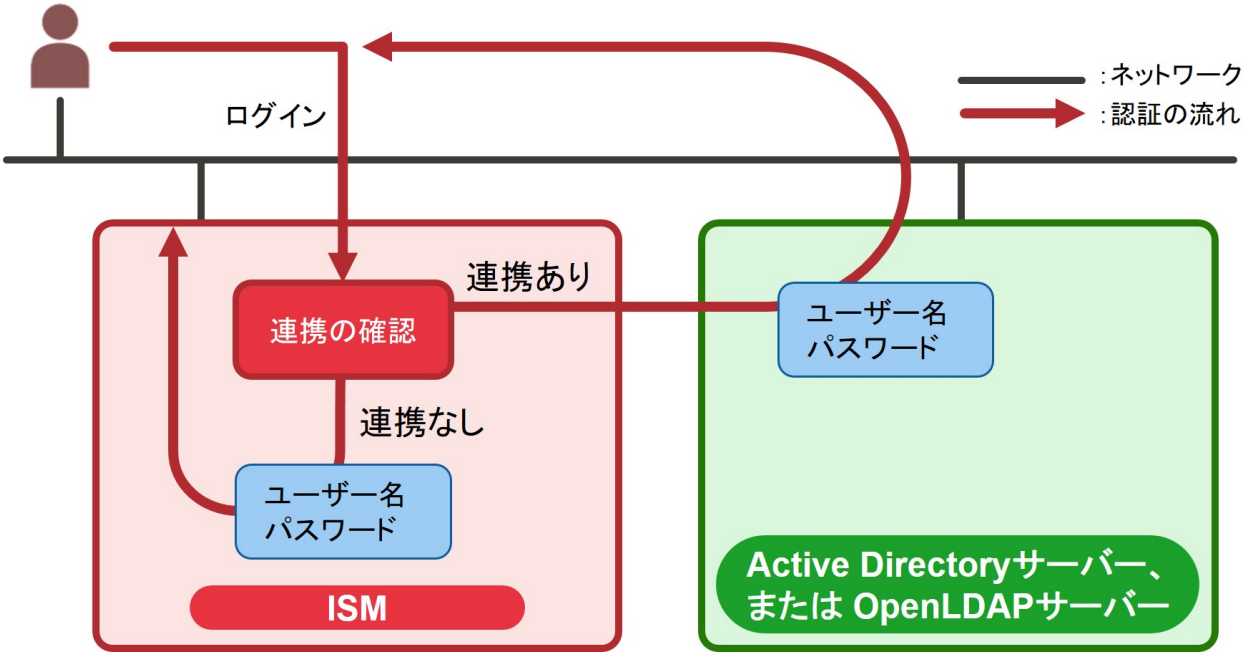
- ファームウェアデータのインポート操作
- ファームウェアのアップデート操作
- OSインストールファイルのインポート操作
- プロファイルの適用
- 手動ログ収集
- 定期ログ収集

Microsoft Active DirectoryまたはOpenLDAPとの連携

Microsoft Active DirectoryまたはOpenLDAPと連携することで、複数サービスのユーザーとパスワードを一元的に管理できます。

連携した場合の概要を以下に示します。

図2.51 ISMとMicrosoft Active Directory／OpenLDAPとの連携イメージ



- ユーザーが連携対象であった場合

  Microsoft Active DirectoryまたはOpenLDAPで認証を行います。

  ディレクトリーサーバーを使ったユーザーとパスワードの管理方法には、以下の2種類があります。

  ー ユーザー連携

  ISMで作成したユーザーのパスワードを、ディレクトリーサーバーで管理します。

  ー Microsoft Active DirectoryまたはOpenLDAPとのグループ連携

  ディレクトリーサーバーでユーザーとパスワードを管理します。

- ユーザーが連携対象でない場合

  ISMで認証を行います。

ポイント

- ユーザー連携とグループ連携で登録できるディレクトリーサーバー数は、以下のとおりです。

  ー ユーザー連携用のディレクトリーサーバーは、プライマリーとセカンダリーの2つを指定できます。

  ー グループ連携用のドメインは、最大5つ指定できます。

- アクティブになっているディレクトリーサーバーから応答がなくなったときは、スタンバイ中のディレクトリーサーバーがアクティブになります。

注意

- administratorユーザーは、Microsoft Active DirectoryまたはOpenLDAPと連携できません。
- ユーザーの認証方法が「Infrastructure Manager(ISM)」であるユーザーは、Microsoft Active DirectoryまたはOpenLDAPと連携できません。
- Microsoft Active Directory名またはOpenLDAPサーバー名にFQDN名を指定する場合、事前にDNSサーバーをISMに設定する必要があります。

- [設定]-[ユーザー]-[LDAPサーバー設定]で指定した内容で、ディレクトリーサーバーと接続できない場合、ディレクトリーサーバー情報はエラーとなって設定できません。
- SSL証明書の設定についての注意事項を以下に示します。
  - SSL証明書は、事前にAdministrator/ftpディレクトリーにアップロード後、設定してください。
  - 設定後、アップロードしたSSL証明書は不要ですので削除してください。
  - SSL証明書に記載されたURLをLDAPサーバー名に指定してください。
- ディレクトリーサーバーとの接続にSSLを使用したい場合の注意事項を以下に示します。
  - LDAPサーバー名は、ldaps://から指定してください。
  - ポート番号をSSL通信用のポート番号(例:636)を指定してください。
  - SSL証明書を設定してください。
- ディレクトリーサーバーで、バインドDNで指定したユーザーのパスワードを変更した場合、ISMの設定には反映されません。ISMのLDAPサーバーの設定で、パスワードを変更してください。

多要素認証

多要素認証は、ユーザー認証を強化する機能です。ユーザー名とパスワードに加えて、認証コードを用いて認証します。多要素認証の対象になるユーザーインターフェイスは、GUI、REST API、SSHです。FTP、ハイパーバイザーのコンソールは多要素認証の対象外です。

多要素認証を使用するには、以下の動作要件を満たす必要があります。

- 任意の携帯端末に多要素認証クライアントアプリケーションをインストールすること

  ISMの多要素認証は、RFC6238に準拠しています。多要素認証クライアントアプリケーションは、Google Authenticator(iOS、Android)が推奨です。
- ISM-VAと多要素認証クライアントアプリケーションをインストールした携帯端末の時刻が同じであること

  ISM-VAと携帯端末の時刻は、最大6分ずれていても認証が成功します。
- ISMのSSHキーボードインタラクティブ認証が有効であること

  SSHキーボードインタラクティブ認証を有効にする方法については、「4.26.1 SSHセキュリティ設定」を参照してください。

多要素認証を有効にしたユーザーがISMにログインすると、QRコードが表示されます。QRコードを多要素認証クライアントアプリケーションにスキャンすることで、認証コードが表示されます。以後は、ユーザー名とパスワードに加えて認証コードを用いてログインします。

ポイント

- 多要素認証の利用において、ISMと多要素認証クライアントアプリケーションをインストールした携帯端末、およびその他の外部サーバーの間で通信はありません。ISMは、ISMと携帯端末で共有する「セットアップキー」と呼ぶ文字列と時刻から認証コードを生成し、認証コードの一致性により認証を行います。セットアップキーは、多要素認証を有効にしたユーザーがISMにログインする際に表示されるQRコードに含まれています。
- セットアップキーは、ユーザーごとに異なります。
- ISMに保存されたセットアップキーは多要素認証を無効にすると削除されます。携帯端末に設定したセットアップキーは手動で削除してください。

注意

- 認証コードは30秒に1回更新されます。一度認証に成功した認証コードを再使用できません。
- 認証コードによる認証失敗は、ログインポリシーの設定値の影響を受けません。認証コードによる認証に失敗しても、アカウントがロックされる操作としての失敗回数にはカウントされません。
- 認証コードによる認証が、30秒間に3回失敗すると、その後30秒間はログインできません。

・ 認証方法が「Open LDAP/Microsoft Active Directory(LDAP)」であるユーザーは、多要素認証を有効にできます。

多要素認証 携帯端末故障・紛失時

多要素認証に使用する携帯端末などが故障した場合は、認証コードの代わりに緊急用コードを入力してISMにログインできます(使用した緊急用コードは、再使用できません)。

なお、緊急用コードが不明な場合、または携帯端末などを交換・紛失した場合には、該当ユーザーの多要素認証を無効にしてください。そのユーザーのセットアップキーは無効になります。新しい携帯端末の準備ができたら再度、多要素認証を有効にしてください。ISMのログイン時に新しいQRコードが表示されます。

すべてのユーザーでログインできなくなった場合は、ハイパーバイザーのコンソールからadministratorでISM-VAにログインし、以下のコマンドを実行して、セットアップキーを再作成します。

```
# ismadm account mfa-reconf -user ＜ユーザー名＞
```

セットアップキーを再作成したユーザーがISMにログインすると、新しいQRコードが表示されます。

QRコードを多要素認証クライアントアプリケーションにスキャンすることで、認証コードが表示されます。

ユーザーのセッション有効時間

ユーザー毎にセッション有効時間を設定することができます。

ユーザー毎に設定したセッション有効時間は、ログインポリシーのセッション有効時間より優先されます。

2.14.2 リポジトリ管理機能

リポジトリは、ISMが利用する各種リソースを保管する場所です。各種リソースは、ユーザーグループに関連しています。主に以下の用途で利用します。

・ ファームウェアアップデート用のファームウェアデータ、およびServerView Suite Update DVDを保管

「2.6 ファームウェア管理機能」で利用されます。

・ OSインストール用のOSインストール媒体を保管

「2.4 プロファイル管理機能」で利用されます。

・ OSインストールおよびOfflineアップデートに使用するServerView Suite DVDを保管

「2.4 プロファイル管理機能」、「2.6 ファームウェア管理機能」で利用されます。

注意

リポジトリのディスク領域が不足している場合、リポジトリ管理機能の各種データの保存に失敗します。以下を参照してリポジトリに対して十分なディスク領域を割り当ててください。

・ 3.2.1.2 リポジトリに必要なディスク容量の見積り

・ 3.7 仮想ディスクの割当て

・ 『操作手順書』の「2.3.2 ユーザーグループを管理する」

2.14.2.1 ファームウェアデータの保存と削除

ファームウェアデータの保存

管理対象ノードに適用するファームウェアデータをリポジトリに保存する方法としては、2種類あります。

- DVDで提供されるファームウェアデータのISOイメージファイルをリポジトリに取り込みます。
- 当社のWebサイトに公開された各ノードのファームウェアデータをリポジトリに取り込みます。

ファームウェアアップデート対象に応じて使用するファームウェアデータが異なります。下表のDVD、ファームウェアデータを準備します。データがDVD形式の場合は、ISOイメージファイルを準備してください。

対象ファームウェア	ファームウェア タイプ（種類）	使用するファームウェアデータ／入手先
PRIMERGY本体 iRMC	iRMC	ServerView Suite Update DVD [注1] または以下のWebサイトからダウンロード可能なファームウェアデータ https://support.ts.fujitsu.com/ ISMは、11版（11.15.09以降）から17版のServerView Suite Update DVDに対応しています（14.21.09を除く）。
PRIMERGY本体 BMC	BMC	
PRIMERGY本体 BIOS	BIOS	
PCIカード	FC	
	CNA	
	SAS	
	RAID	
	LAN	
PRIMEQUEST本体	本体ファームウェア	以下のWebサイトからダウンロード可能なファームウェアデータ https://www.fujitsu.com/jp/products/computing/servers/primequest/download/
ネットワークスイッチ 基本ソフトウェア	LAN Switch （SR-Xモデル）	以下のWebサイトからダウンロード可能なファームウェアデータ https://www.fujitsu.com/jp/products/network/download/sr-x/firm/
	LAN Switch （VDXモデル）	以下のWebサイトからダウンロード可能なファームウェアデータ https://eservice.fujitsu.com/supportdesk/ [注2]
	LAN Switch （X440/460-G2モデル）	以下のWebサイトからダウンロード可能なファームウェアデータ https://support.ts.fujitsu.com/
	LAN Switch （CFXモデル）	以下のWebサイトからダウンロード可能なファームウェアデータ https://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/
	LAN Switch （Cisco Systems Nexusシリーズ、Cisco Systems Catalystシリーズ）	当社担当営業／SE、またはサポートに連絡して入手してください。
ストレージ コントローラー	ETERNUS DX/AF	以下のWebサイトからダウンロード可能なファームウェアデータ https://eservice.fujitsu.com/supportdesk/ [注2] https://www.fujitsu.com/jp/products/computing/storage/download/ [注3]

[注1]：以下のWebサイトからServerView Suite Update DVDイメージを入手してください。

https://azby.fmworld.net/app/customer/driversearch/ia/drviaindex

PRIMERGYダウンロード検索画面で、「製品名」欄でご利用の製品名を選択し、「添付ソフト／ドライバー名称（部分一致可）」欄に「Update DVD」と入力して検索してください。

[注2]：ご利用にはSupportDesk契約が必要です。

[注3]：ご利用には「エフサステクノロジーズID（登録無料）」が必要です。

ファームウェアデータをDVDからインポートする場合

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[インポート]を選択します。

3. [インポートデータリスト]タブの[アクション]ボタンから[DVDインポート]を選択します。
4. [ファイル選択方式]でファイルの選択先を選択します。
   - ローカル

     ローカルにあるISOイメージをインポートします。
   - FTP

     ISM-VAのFTPサーバーからISOイメージをインポートします。

     あらかじめ、ISM-VAの「/＜ユーザーグループ名＞/ftp」のディレクトリー配下にISOイメージを転送しておく必要があります。

     FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
   - 共有ディレクトリー

     共有ディレクトリーからISOイメージをインポートします。

     あらかじめ、インポート対象のISOイメージが格納された共有ディレクトリーをマウントしておく必要があります。

     共有ディレクトリーの設定、マウント方法の詳細は、「2.14.7 共有ディレクトリー管理機能」を参照してください。
5. [ファイル]でISOイメージを指定します。
6. [適用]ボタンでインポートを実行します。

   DVDインポートには時間がかかることがあります。インポートの開始後、作業がISMのタスクとして登録されます。作業の状況は「タスク」画面で確認してください。

   ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択すると、タスクの一覧が表示されます。

ポイント

- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
- [ファイル選択方式]で「FTP」を選択した場合、[元のファイルを削除する]にチェックを付けると、インポートが完了したあとISM-VAのFTPサーバー上にあるインポート元のファイルが削除されます。
- [ファイル選択方式]で「共有ディレクトリー」を選択した場合、[共有ディレクトリーのマウントを解除する]にチェックを付けると、インポートが完了したあと共有ディレクトリーとのマウントを解除します。

当社のWebサイトからダウンロードしたファームウェアデータをインポートする場合

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[インポート]を選択します。
3. [インポートデータリスト]タブの[アクション]ボタンから[ファームウェアインポート]を選択します。
4. [ファイル選択方式]でファイルの選択先を選択します。
   - ローカル

     ローカルにあるファームウェアデータをインポートします。
   - FTP

     ISM-VAのFTPサーバーからファームウェアデータをインポートします。

     あらかじめ、ISM-VAの「/＜ユーザーグループ名＞/ftp」のディレクトリー配下にファームウェアデータを転送しておく必要があります。

     FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
5. [ファイル]でインポート対象を指定します。
6. [種類]でファームウェアの種類を選択します。
7. [モデル]でファームウェアのモデルを選択します。

8. [バージョン]でファームウェアのバージョンの取得方法を選択し、[適用]ボタンでインポートを実行します。

- 自動で取得する

  インポート時にファームウェアからバージョンの情報を取得します。
  このオプションで下表のファームウェアがインポートできます。インポートができない場合には、「手動で入力する」を選択してインポートを行ってください。

種類	モデル
iRMC	・ PRIMERGY（iRMC S4以降を搭載したサーバー） ・ PRIMEQUEST 3800B
BIOS	・ PRIMERGY（iRMC S3以降を搭載したサーバー） ・ PRIMEQUEST 3800B [注]

  [注]：モードがOfflineのもののみインポートされます。

- 手動で入力する

  インポート時にファームウェアのバージョンを手動で入力します。
  入力するバージョンは、下記の表に従って入力してください。

  バージョンについては、リリースノートまたはファイル名を参照してください。

種類	モデル	バージョン
PRIMEQUEST	PRIMEQUEST 2400L3など	本体ファームウェアのバージョン
FC	LPe1250、LPe12002、MC-FC82E	BIOSとFWのバージョン
	LPe16000以降、MC-FC162E	ファームウェアのバージョン
	QLE2560、QLE2562	BIOSのバージョン
	QLE2670、QLE2672、QLE2690、QLE2692、QLE2740、QLE2742	BIOSとFWのバージョン
	QLE2770およびQLE2772以降	FWのバージョン
CNA	OCe10102、OCe14102、MC-CNA112Eなど	ファームウェアのバージョン
SAS	PSAS CP200i、PSAS CP400i、PSAS CP400eなど	
RAID	PRAID CP400i、PRAID EP420e、PY SAS RAID Mezz Card 6Gbなど	
LAN	MCX415、MCX416など	
LAN Switch	SR-Xモデル	基本ソフトウェアのバージョン
	VDXモデル	ファームウェアのバージョン
	CFXモデル	
	Cisco Systems Nexusシリーズ	NX-OSのバージョン
	Cisco Systems Catalystシリーズ	IOSのバージョン
ETERNUS DX/AF	ETERNUS DX/AFモデル	ファームウェアのバージョン

ポイント

ー [ファイル選択方式]で「ローカル」を選択する場合、[ファイル]にはファームウェアデータ、手順書などのすべてをzip圧縮したzipファイルを指定しインポートしてください。

  ファームウェアが自己解凍形式(exe)で提供されている場合、一度解凍します。展開されたファイル、フォルダーを、すべて、zip圧縮し、インポートしてください。

- [ファイル選択方式]で「FTP」を選択する場合、ISM-VAのFTPサーバーにファームウェアデータ、手順書などのすべてが格納されたフォルダーを転送し、[ファイル]には転送したフォルダーを指定しインポートしてください。

  ファームウェアが自己解凍形式(exe)で提供されている場合、一度解凍します。解凍時に作成されたファームウェアデータ、手順書などのすべてをzip圧縮し、ISM-VAに転送し、インポートしてください。

- ISM-VAのFTPサーバーにファイルを配置する場合は、FTPコマンドまたはFTPクライアントソフトウェア（FFFTP、WinSCPなど）を使って転送してください。その際、文字コードがUTF-8で変換されるように設定してください。Windows Explorerを使用すると文字コードが正しく扱われないため、使用しないでください。

- [ファイル選択方式]で「FTP」を選択し、インポートが正しく行われない、インポートしたドキュメントが表示されないなどの場合は、以下の対処を行ってください。

  1. インポート済みのファームウェアデータおよび、ISM-VA上へFTP転送したファイルを削除します。
  2. 文字コード変換の設定を見直します。
  3. 再度インポートを行います。

- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。

- [種類]で「BIOS」を選択した場合、[モデル]の選択肢に「RX2530 M4_A1」、「RX2530 M4_C1」のように同じモデルでも複数の選択肢が表示されることがあります。

  この場合、ファームウェアアップデートを行うノードがどの種類のファームウェアデータで動作しているかを確認し、それに合わせて選択する必要があります。

  また、インポートするファームウェアデータもファームウェアアップデート対象で動作しているファームウェアデータの種類と同じものを入手し、インポートしてください。

  ISMに登録しているノードがどの種類のファームウェアデータで動作しているかは、以下の手順で確認できます。

  1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
  2. 「ノードリスト」画面の[カラム表示]欄で「ファームウェア/ドライバー」を選択します。
  3. [FW/ドライバー名]欄を確認します。

リポジトリからのファームウェアデータの削除

GUIを使用した操作の例を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
2. 画面左側のメニューから[インポート]を選択します。
3. 以下のどちらかを行います。
   - ファームウェアデータをDVDからリポジトリに保存していた場合
     a. [インポートデータリスト]タブを選択します。
     b. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
     c. 画面表示に従い、操作を実行します。
   - 当社のWebサイトからダウンロードしたファームウェアデータをリポジトリに保存していた場合
     a. [ファームウェアデータ]タブを選択します。
     b. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
     c. 画面表示に従い、操作を実行します。

2.14.2.2 OSインストールファイルの保存と削除

OSインストールファイルの保存

プロファイル管理機能は、リポジトリにインポートしたOSインストール媒体を使用してインストール作業を行うため、インポート後は、OSインストール媒体を直接使用しません。

インポートは以下の手順で実施します。

1. OSインストール媒体のISOイメージを用意します。ESXiの場合はエフサステクノロジーズカスタムイメージを用意します。
2. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
3. 画面左側のメニューから[DVDインポート]を選択します。
4. [アクション]ボタンから[DVDインポート]を選択します。
5. [ファイル選択方式]でファイルの選択先を選択します。
   - ローカル

     ローカルにあるISOイメージをインポートします。
   - FTP

     ISM-VAのFTPサーバーからISOイメージをインポートします。

     あらかじめ、ISM-VAの「/＜ユーザーグループ名＞/ftp」のディレクトリー配下にISOイメージを転送しておく必要があります。

     FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。
   - 共有ディレクトリー

     共有ディレクトリーからISOイメージをインポートします。

     あらかじめ、ISOイメージが格納された共有ディレクトリーをマウントしておく必要があります。

     共有ディレクトリーの設定、マウント方法の詳細は、「2.14.7 共有ディレクトリー管理機能」を参照してください。
6. [ファイル]でISOイメージを指定します。
7. [メディアタイプ]で適切なOS種類を選択し、[適用]ボタンでインポートを実行します。

ポイント

- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
- [ファイル選択方式]で「FTP」を選択した場合、[元のファイルを削除する]にチェックを付けると、インポートが完了したあとISM-VAのFTPサーバー上にあるインポート元のファイルが削除されます。
- [ファイル選択方式]で「共有ディレクトリー」を選択した場合、[共有ディレクトリーのマウントを解除する]にチェックを付けると、インポートが完了したあと共有ディレクトリーとのマウントを解除します。

リポジトリからのOSインストールファイルの削除

削除は以下の手順で行います。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[DVDインポート]を選択します。
3. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
4. 画面表示に従い、操作を実行します。

2.14.2.3 ServerView Suite DVDの保存と削除

ServerView Suite DVDの保存

プロファイル管理機能がOSのインストールを行う際、対象ノードを制御するプログラム、および対象ノードにインストールするドライバー、アプリケーションなどのファイルは、ServerView Suite DVDから取得します。

対象ノードおよびインストールするOSをサポートするServerView Suite DVDを事前にインポートしてください。

インポートは以下の手順で行います。

1. ServerView Suite DVDのISOイメージを用意します。
2. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
3. 画面左側のメニューから[DVDインポート]を選択します。
4. [アクション]ボタンから[DVDインポート]を選択します。
5. [ファイル選択方式]でファイルの選択先を選択します。

   ー ローカル

   ローカルにあるISOイメージをインポートします。

   ー FTP

   ISM-VAのFTPサーバーからISOイメージをインポートします。

   あらかじめ、ISM-VAの「/＜ユーザーグループ名＞/ftp」のディレクトリー配下にISOイメージを転送しておく必要があります。

   FTP接続および転送方法の詳細は、「2.1.2 FTPアクセス」を参照してください。

   ー 共有ディレクトリー

   共有ディレクトリーからISOイメージをインポートします。

   あらかじめ、ISOイメージが格納された共有ディレクトリーをマウントしておく必要があります。

   共有ディレクトリーの設定、マウント方法の詳細は、「2.14.7 共有ディレクトリー管理機能」を参照してください。
6. [ファイル]でISOイメージを指定します。
7. [メディアタイプ]で[ServerView Suite DVD]を選択し、[適用]ボタンでインポートを実行します。

ポイント

- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。
- [ファイル選択方式]で「FTP」を選択した場合、[元のファイルを削除する]にチェックを付けると、インポートが完了したあとISM-VAのFTPサーバー上にあるインポート元のファイルが削除されます。
- [ファイル選択方式]で「共有ディレクトリー」を選択した場合、[共有ディレクトリーのマウントを解除する]にチェックを付けると、インポートが完了したあと共有ディレクトリーとのマウントを解除します。

リポジトリからのServerView Suite DVDの削除

削除は以下の手順で行います。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[DVDインポート]を選択します。
3. 削除を行う対象にチェックを付け、[アクション]ボタンから[削除]を選択します。
4. 画面表示に従い、操作を実行します。

2.14.3 Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLIの導入

注意

- Linux上のPCIカードのファームウェアアップデートをするためには、対象サーバーのOS上にEmulex OneCommand Manager CLI、または、QLogic QConvergeConsole CLIがインストールされ、対象のPCIカード情報が取得できる状態である必要があります。インストール、操作方法は、Emulex One Command Manager CLIのマニュアル、QLogic QConvergeConsole CLIのマニュアルを参照してください。

  Emulex OneCommand Manager CLI、QLogic QConvergeConsole CLIのインストールが必要になるPCIカードは、当社の本製品Webサイトを参照してください。

  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

- Linux上のPCIカードのファームウェアアップデートをするためには、対象サーバー上のLinuxでlspciコマンドが実行できる必要があります。

Emulex OneCommand Manager CLI、またはQLogic QConvergeConsole CLIは、最新のものを利用してください。

以下のPRIMERGYダウンロード検索画面で製品名の欄にご利用の製品名を選択し、添付ソフト／ドライバー名称（部分一致可）の欄に「OCManager」、「HBA Manager」または「QConverge」と入力して検索し、最新のものをダウンロードしてください。

http://jp.fujitsu.com/platform/server/primergy/downloads/

2.14.4 タスク管理

ISMでは時間がかかる処理を行う場合、その処理はタスクとして管理されます。それぞれのタスクの状態は操作した画面ではなく、「タスク」画面で一括参照します。

実行中の処理を中止（キャンセル）する場合も「タスク」画面から操作します。

「タスク」画面では、下表の処理がタスクとして参照できます。

機能	処理
ファームウェア管理機能	ファームウェアデータのインポート ファームウェアのアップデート
プロファイル管理機能	OSインストールメディアのインポート プロファイルの適用 プロファイルの再適用 プロファイルの適用の解除 eIMの最新版数への更新
ログ管理機能	ログ収集 ログ削除 ダウンロードファイルの作成
ネットワーク管理機能	VLAN設定の変更
仮想リソース管理機能	仮想リソース情報の更新
クラスタ管理機能	リソース変動予測

注意

eIMの最新版数への更新処理が開始された（サブタスクの進捗が1%以上）場合、ISMからキャンセル実行してもeIMの最新版数への更新処理は継続されます。eIMの最新版数への更新処理が完了したあと、タスクのステータスが「キャンセル完了」として表示されます。

eIMの最新版数への更新処理をキャンセルしたい場合は、対象サーバーの以下のドキュメントを参照し、「タスクマネージャ」から実行中のタスクを削除してください。

『ServerView Suite iRMC Sx Web インターフェース』（Sxには、S4以降の版数が入ります。）

下記の当社マニュアルサイトから参照してください。

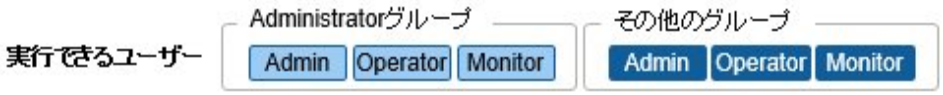
https://support.ts.fujitsu.com/index.asp?lng=jp

参照手順

「製品を選択する」- [カテゴリから探す]を選択し、対象のサーバーを選択してください。
[Server Management Controller]からダウンロードしてください。

なお、参照手順は、予告なく変更されることがあります。

「タスク」画面の表示方法



1. ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択します。

2.14.5 ISM-VA管理機能

ISM-VA管理機能は、ISMの導入／サービス運用およびメンテナンス時に使用する機能です。

以下について説明します。

- ISM導入時に使用する機能
- メンテナンス時に使用する機能

また、ISM-VA管理機能で使用できるコマンドについては、「2.14.5.1 ISM-VA管理機能のコマンド一覧」で説明します。

ISM導入時に使用する機能

機能名	機能概要
初期設定機能	ISM-VAをインストール後、最初に起動した際にハイパーバイザーのコンソール上で基本的な設定を行う機能を提供します。 ・ ネットワーク設定 ・ 時刻設定 ・ 初期ロケール設定
ライセンス設定機能	ISMのライセンスキーを設定する機能を提供します。
証明書設定機能	Webブラウザーでアクセスする際の証明書管理機能を提供します。

メンテナンス時に使用する機能

機能名	機能概要
ISM-VAサービス制御機能	ISM-VAの停止／再起動や、内部で動作しているサービスの制御を行えます。
基本設定機能	導入後にISM-VAの設定変更を行う機能を提供します。 ・ ネットワーク設定 ・ 時刻設定 ・ ロケール設定 ・ 仮想ディスク設定 ・ ホスト名変更
保守機能	ISM-VAの保守機能を提供します。 ・ バージョン確認 ・ 修正パッチ適用 ・ 保守ログ採取

機能名	機能概要
	・ デバッグフラグ切替え

2.14.5.1 ISM-VA管理機能のコマンド一覧

ISM-VA管理機能のコマンド一覧を以下に示します。

コンソール管理メニュー

機能	コマンド
ISM-VA基本設定メニュー	ismsetup

ネットワーク設定

機能	コマンド
ネットワークデバイス表示	ismadm network device
ネットワーク設定変更	ismadm network modify
ネットワーク設定表示	ismadm network show
ネットワーク疎通確認	ismadm network ping

時刻設定

機能	コマンド
時刻設定表示	ismadm time show
設定可能タイムゾーン表示	ismadm time list-timezones
タイムゾーン設定	ismadm time set-timezone
日時／時刻設定	ismadm time set-time
NTP同期有効／無効設定	ismadm time set-ntp
NTPサーバー追加	ismadm time add-ntpserver
NTPサーバー削除	ismadm time del-ntpserver

ロケール／キーマップ設定

機能	コマンド
ロケール／キーマップ表示	ismadm locale show
設定可能ロケール表示	ismadm locale list-locales
ロケール設定	ismadm locale set-locale
設定可能キーマップ表示	ismadm locale list-keymaps
キーマップ設定	ismadm locale set-keymap

ライセンス設定

機能	コマンド
ライセンス表示	ismadm license show
ライセンス登録	ismadm license set
ライセンス削除	ismadm license delete

証明書設定

機能	コマンド
SSL証明書配置	ismadm sslcert set
SSL証明書表示	ismadm sslcert show
SSL証明書出力	ismadm sslcert export
自己署名証明書作成	ismadm sslcert self-create

ISM-VAサービス制御

機能	コマンド
ISM-VA再起動	ismadm power restart
ISM-VA停止	ismadm power stop
ISM公開サービスポート変更	ismadm service modify
内部サービス一覧表示	ismadm service show
内部サービス個別起動	ismadm service start
内部サービス個別停止	ismadm service stop
内部サービス個別再起動	ismadm service restart
内部サービス個別ステータス表示	ismadm service status
内部サービス個別有効化設定	ismadm service enable
内部サービス個別無効化設定	ismadm service disable

仮想ディスク設定

機能	コマンド
LVMボリューム追加	ismadm volume add
ユーザーグループにLVMボリューム割当て	ismadm volume mount
ユーザーグループのLVMボリューム割当て解除	ismadm volume umount
ボリューム設定表示	ismadm volume show
LVMボリュームサイズ拡張	ismadm volume extend
システムのLVMボリュームサイズを拡張	ismadm volume sysvol-extend
LVMボリューム削除	ismadm volume delete

保守機能

機能	コマンド
保守ログ採取	ismadm system snap
システム情報の表示	ismadm system show
修正パッチ適用	ismadm system patch-add
プラグイン適用	ismadm system plugin-add
ISM-VAのアップグレード	ismadm system upgrade
ISM-VAのマイグレート	ismadm system migrate
ホスト名変更	ismadm system modify
障害調査ログ切替え	ismadm system set-debug-flag

機能	コマンド
ISMバックアップ	ismadm system backup
ISMリストア	ismadm system restore
ISM-VA統計情報表示	ismadm system stat

coreファイルの採取ディレクトリー設定

機能	コマンド
採取ディレクトリー表示	ismadm system core-dir-show
採取ディレクトリー設定	ismadm system core-dir-set
採取ディレクトリー解除	ismadm system core-dir-reset

アラーム通知設定

機能	コマンド
アラーム通知メール用証明書登録	ismadm event import
アラーム通知メール用証明書表示	ismadm event show
アラーム通知メール用証明書削除	ismadm event delete

MIBファイル設定

機能	コマンド
MIBファイル登録	ismadm mib import
MIBファイル表示	ismadm mib show
MIBファイル削除	ismadm mib delete

セキュリティ関連設定

機能	コマンド
SSL/TLS有効化状態表示（GUI／REST）	ismadm security show-tls
SSL/TLS有効化状態表示（FTPS）	ismadm security show-tls-ftp
SSL/TLS有効化設定（GUI／REST）	ismadm security enable-tls
SSL/TLS有効化設定（FTPS）	ismadm security enable-tls-ftp
暗号スイート設定表示（GUI／REST）	ismadm security show-sslcipher
暗号スイート設定（GUI／REST）	ismadm security set-sslcipher
SSHセキュリティ設定確認	ismadm security show-ssh-conf
SSHセキュリティ設定	ismadm security set-ssh-conf
SSHログイン状態表示	ismadm security show-ssh-loginfail
SSHログイン失敗ユーザーロック解除	ismadm security reset-ssh-userlock
SSH接続元IPアドレス追加	ismadm security add-ssh-clientip
SSH接続元IPアドレス削除	ismadm security delete-ssh-clientip
SSH公開鍵登録	ismadm security set-ssh-pubkey
SSH公開鍵表示	ismadm security show-ssh-pubkey
SSH公開鍵削除	ismadm security delete-ssh-pubkey

機能	コマンド
コンソール自動ログアウト設定表示	ismadm security show-console-timeout
コンソール自動ログアウト設定	ismadm security set-console-timeout
接続元IPアドレス制限確認（GUI／REST）	ismadm security show-gui-conf
接続元IPアドレス制限確認（Samba）	ismadm security show-smb-conf
接続元IPアドレス制限確認（FTP）	ismadm security show-ftp-conf
接続元IPアドレス制限確認（TFTP）	ismadm security show-tftp-conf
接続元IPアドレス制限確認（9213ポート）	ismadm security show-svs-conf
接続元IPアドレス制限確認（SNMPトラップ）	ismadm security show-snmp-conf
接続元IPアドレス制限確認（HTTPSデータ）	ismadm security show-https-data-conf
接続元IPアドレス制限確認（SSDP）	ismadm security show-ssdp-conf
接続元IPアドレス制限設定（GUI／REST）	ismadm security set-gui-conf
接続元IPアドレス制限設定（Samba）	ismadm security set-smb-conf
接続元IPアドレス制限設定（FTP）	ismadm security set-ftp-conf
接続元IPアドレス制限設定（TFTP）	ismadm security set-tftp-conf
接続元IPアドレス制限設定（9213ポート）	ismadm security set-svs-conf
接続元IPアドレス制限設定（SNMPトラップ）	ismadm security set-snmp-conf
接続元IPアドレス制限設定（HTTPSデータ）	ismadm security set-https-data-conf
接続元IPアドレス制限設定（SSDP）	ismadm security set-ssdp-conf
接続元IPアドレス追加（GUI／REST）	ismadm security add-gui-clientip
接続元IPアドレス追加（Samba）	ismadm security add-smb-clientip
接続元IPアドレス追加（FTP）	ismadm security add-ftp-clientip
接続元IPアドレス追加（TFTP）	ismadm security add-tftp-clientip
接続元IPアドレス追加（9213ポート）	ismadm security add-svs-clientip
接続元IPアドレス追加（SNMPトラップ）	ismadm security add-snmp-clientip
接続元IPアドレス追加（HTTPSデータ）	ismadm security add-https-data-clientip
接続元IPアドレス追加（SSDP）	ismadm security add-ssdp-clientip
接続元IPアドレス削除（GUI／REST）	ismadm security delete-gui-clientip
接続元IPアドレス削除（Samba）	ismadm security delete-smb-clientip
接続元IPアドレス削除（FTP）	ismadm security delete-ftp-clientip
接続元IPアドレス削除（TFTP）	ismadm security delete-tftp-clientip
接続元IPアドレス削除（9213ポート）	ismadm security delete-svs-clientip
接続元IPアドレス削除（SNMPトラップ）	ismadm security delete-snmp-clientip
接続元IPアドレス削除（HTTPSデータ）	ismadm security delete-https-data-clientip
接続元IPアドレス削除（SSDP）	ismadm security delete-ssdp-clientip
ISMセッション認証のIPアドレス制限設定確認	ismadm security show-ismauth-conf
ISMセッション認証のIPアドレス制限設定変更	ismadm security set-ismauth-conf

他ソフトウェア連携設定

機能	コマンド
他ソフトウェア連携用証明書登録	ismadm security import-software-cert
他ソフトウェア連携用証明書表示	ismadm security show-software-cert
他ソフトウェア連携用証明書削除	ismadm security delete-software-cert

プロファイル関連設定

機能	コマンド
プロファイルのベリファイ有効化／無効化設定	ismadm system set-profile-verify
プロファイルのベリファイ有効化／無効化状態表示	ismadm system show-profile-verify

アカウント関連設定

機能	コマンド
多要素認証情報の再設定	ismadm account mfa-reconf -user

中継ルートのポート設定

機能	コマンド
中継ルートのポート設定	ismadm relayroute port-change
中継ルートのポート表示	ismadm relayroute port-show

中継ルート用のクライアント証明書作成

機能	コマンド
中継ルート用のクライアント証明書の作成	ismadm relayroute clientcert-create
中継ルート用のクライアント証明書の表示	ismadm relayroute clientcert-show

注意

時刻設定により過去の時刻に戻した場合、ISM-VAを再起動する必要があります。

2.14.6 仮想化管理ソフトウェア管理機能

仮想化管理ソフトウェアとの連携機能を利用する場合は、ISMに仮想化管理ソフトウェアを登録します。

サポートする仮想化管理ソフトウェアは、以下のとおりです。

- VMware vCenter Server 7.0
- VMware vCenter Server 8.0
- Microsoft System Center 2012
- Microsoft System Center 2012R2
- Microsoft System Center 2016
- Microsoft System Center 2019
- Microsoft System Center 2022
- Microsoft System Center 2025
- Microsoft Failover Cluster (Windows Server 2012) [注]

- Microsoft Failover Cluster (Windows Server 2012R2) [注]
- Microsoft Failover Cluster (Windows Server 2016) [注]
- Microsoft Failover Cluster (Windows Server 2019) [注]
- Microsoft Failover Cluster (Windows Server 2022) [注]
- Microsoft Failover Cluster (Windows Server 2025) [注]
- Microsoft Failover Cluster (Azure Stack HCI) [注]
- KVM (Red Hat Enterprise Linux)
- KVM (AlmaLinux)（ISM 3.1.0.010以降）
- KVM (SUSE Linux Enterprise)
- IPCOM OS 1.x
- OpenStack (Red Hat Enterprise Linux)

[注]：Microsoft Failover Clusterでは、クラスタの役割として登録された仮想マシンのみ表示されます。

2.14.6.1 仮想化管理ソフトウェアの登録

詳細な手順については、『操作手順書』の「6.2.1 仮想化管理ソフトウェアを登録する」を参照してください。

2.14.6.2 仮想化管理ソフトウェアからの情報取得

ISMでは、ノード上で動作している以下の情報を取得して確認できます。

- 仮想マシン情報

  仮想化管理ソフトウェアから取得した仮想マシン情報を、ノードの詳細画面の[仮想マシン]タブで確認できます。

- 仮想スイッチ情報

  仮想化管理ソフトウェアから取得した仮想スイッチ情報は、「ネットワークマップ」画面で確認できます。

  仮想化管理ソフトウェアの種類がVMware vCenter Server、System Center、Microsoft Failover Cluster、またはOpenStackの場合に取得できます。KVMの場合はサポート外となります。

- 仮想ルーター情報

  仮想化管理ソフトウェアから取得した仮想ルーター情報は、「ネットワークマップ」画面で確認できます。

  仮想化管理ソフトウェアの種類がOpenStackの場合に取得できます。VMware vCenter Server、System Center、Microsoft Failover Cluster、またはKVMの場合はサポート外となります。

注意

ISMは、登録されている仮想化管理ソフトウェア情報と、ノードのOS情報を紐づけて仮想マシン、仮想スイッチ、および仮想ルーター情報を管理します。仮想マシン、仮想スイッチ、および仮想ルーター情報を取得するにはそれぞれを設定してください。

ISMは、仮想マシン、仮想スイッチ、および仮想ルーター情報を24時間周期で取得します。

任意の時点で情報を取得する手順については、『操作手順書』の「6.2.2 管理対象サーバー上の仮想マシンの情報を確認する」の手順1～6を参照してください。

情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10021503」のログが出力されます。情報取得に失敗した仮想化管理ソフトウェアが存在する場合、追加で[イベント]-[イベント]-[運用ログ]にログが出力されます。エラーが出力されていないかを確認し、仮想マシン、仮想スイッチ、および仮想ルーター情報を確認してください。

注意

- System Centerと、そのSystem Centerに登録されているMicrosoft Failover Clusterの両方をISMに登録している場合、ISMではSystem Centerから情報取得を行い、Microsoft Failover Clusterからは情報取得を行いません。
- Microsoft Failover Clusterをご使用の環境で、仮想マシンをHyper-Vマネージャーから削除した場合は、その仮想マシンをフェイルオーバークラスタマネージャーの役割からも削除してください。

2.14.6.3 仮想化管理ソフトウェアの編集

ISMに登録されている仮想化管理ソフトウェア情報を編集する手順については、『操作手順書』の「6.2.1.1 仮想化管理ソフトウェア情報を編集する」を参照してください。

2.14.6.4 仮想化管理ソフトウェアの削除

ISMに登録されている仮想化管理ソフトウェアを削除する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想化管理ソフトウェアを選択します。
2. [アクション]ボタンから[削除]を選択します。
3. [削除]を実行し、仮想化管理ソフトウェアを削除します。

注意

仮想化管理ソフトウェアの削除後、メッセージID「50170511」が出力されることがあります。
メッセージが出力された場合は、「2.9.3.3 仮想リソース情報の更新」を実施してください。

2.14.6.5 仮想化管理ソフトウェアのイベント出力抑止モードの変更

仮想化管理ソフトウェアのイベント出力抑止モードとは、仮想化管理ソフトウェアの保守作業による操作（ホストの設定変更、パスワード変更など）や状態変更などの影響で発生するイベント（アラーム）を、ISMが検出してしまうのを抑止するための設定です。

仮想化管理ソフトウェアの保守作業を行う場合、ISMに登録している対象の仮想化管理ソフトウェアに対してインベント出力抑止モードの設定を有効にすることをお勧めします。

仮想化管理ソフトウェアのインベント出力抑止モードを有効にすると、ISMが定期的に行っている仮想化管理ソフトウェアからの情報取得を停止します。このため、ISMの以下の情報が自動的に更新されなくなります。

- 仮想リソースの情報

  詳しくは、「2.9.3.3 仮想リソース情報の更新」および「2.9.3.4 仮想マシンのvSANディスク影響の表示」を参照してください。

- クラスタ情報

  詳しくは、「2.13.1.3 クラスタ情報の取得と更新」を参照してください。

- 仮想化管理ソフトウェアからの情報

  詳しくは、「2.14.6.2 仮想化管理ソフトウェアからの情報取得」を参照してください。

仮想化管理ソフトウェアのイベント出力抑止モードを有効にした場合、上記の情報取得以外の機能には影響しません。以下の機能は、仮想化管理ソフトウェアのイベント出力抑止モードを有効にしても仮想管理ソフトウェアからの情報取得は停止しません。

- アノマリ検知機能

  アノマリ検知機能の詳細については、「2.3.6 アノマリ検知機能」を参照してください。

- 仮想ネットワークパケット分析機能

  仮想ネットワークパケット分析機能の詳細については、「2.11 仮想ネットワーク パケット分析機能」を参照してください。

このため、上記の機能が動作することによって、仮想化管理ソフトウェアからの情報取得によるイベント(アラーム)が発生することがあります。

ISMに登録されている仮想化管理ソフトウェアのイベント出力抑止モードを有効にする場合

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想化管理ソフトウェアを選択します。
2. [アクション]ボタンから[イベント出力抑止モード有効]を選択します。

   確認画面が表示されるので、対象の仮想化管理ソフトウェア名を確認し、[はい]ボタンを選択します。
3. 仮想化管理ソフトウェアが管理しているノードがアノマリ検知を開始している場合、ノードをメンテナンスモードに設定します。

   詳細は、「5.1 メンテナンスモード」の「メンテナンスモード設定手順」を参照してください。
4. 仮想化管理ソフトウェアが管理しているノードの仮想ネットワークアダプターのしきい値監視状態が有効の場合、仮想ネットワークアダプターのしきい値監視状態を無効に設定します。

   詳細は、『操作手順書』の「6.6.1 仮想アダプターのしきい値を設定する」を参照してください。

ISMに登録されている仮想化管理ソフトウェアのイベント出力抑止モードを無効にする場合

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想化管理ソフトウェアを選択します。

   イベント出力抑止モードが有効になっている場合、「仮想化管理ソフトウェア名」の前に()が表示されています。
2. [アクション]ボタンから[イベント出力抑止モード無効]を選択します。

   確認画面が表示されるので、対象の仮想化管理ソフトウェア名を確認し、[はい]ボタンを選択します。
3. 必要に応じて、ノードをメンテナンスモードから解除します。

   詳細は、「5.1 メンテナンスモード」の「メンテナンスモード解除手順」を参照してください。
4. 必要に応じて、仮想ネットワークアダプターのしきい値監視状態を有効にします。

   詳細は、『操作手順書』の「6.6.1 仮想アダプターのしきい値を設定する」を参照してください。

2.14.7 共有ディレクトリー管理機能

DVDインポートで使用する共有ディレクトリーを追加します。

2.14.7.1 共有ディレクトリーの追加

新しく共有ディレクトリーを追加する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリー]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 必要な情報を入力します。

項目	説明
ホスト名/IPアドレス	共有ディレクトリーのIPアドレスまたはホスト名を設定します。
ドメイン	共有ディレクトリーのドメイン名を設定します。ドメイン名は大文字で設定します。
共有ディレクトリーパス	共有ディレクトリーのパスを設定します。
種類	共有ディレクトリータイプをSMB/CIFS、NFSから選択します。
アカウント名	共有ディレクトリーのアカウント名を設定します。
パスワード	共有ディレクトリーのパスワードを設定します。
ユーザーグループ名	共有ディレクトリー情報が所属するユーザーグループを選択します。

4. [登録]ボタンを選択します。

   「共有ディレクトリーリスト」画面に追加した共有ディレクトリーが表示されます。

注意

- ユーザーグループごとに5つまで共有ディレクトリー情報を追加できます。
- 指定した共有ディレクトリー情報で、共有ディレクトリーをマウントできない場合はエラーとなります。

2.14.7.2 共有ディレクトリーの編集

ISMに登録されている共有ディレクトリー情報を編集する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリー]を選択します。
2. 以下のどちらかを行います。
   - 編集したい共有ディレクトリーにチェックを付け、[アクション]ボタンから[編集]を選択します。
   - 編集したい共有ディレクトリーを選択し、表示された情報画面で[アクション]ボタンから[編集]を選択します。
3. 情報を編集します。

項目	説明
ホスト名/IPアドレス	共有ディレクトリーのIPアドレスまたはホスト名を設定します。
ドメイン	共有ディレクトリーのドメイン名を設定します。ドメイン名は大文字で設定します。
共有ディレクトリーパス	共有ディレクトリーのパスを設定します。
種類	共有ディレクトリータイプをSMB/CIFS、NFSから選択します。

項目	説明
アカウント名	共有ディレクトリーのアカウント名を設定します。
パスワード	共有ディレクトリーのパスワードを設定します。

4. [登録]を選択し、情報の内容を反映します。

注意

共有ディレクトリーがマウント中の場合は、編集できません。

2.14.7.3 共有ディレクトリーの削除

ISMに登録されている共有ディレクトリーを削除する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリー]を選択します。
2. 以下のどちらかを行います。
   - 削除したい共有ディレクトリーにチェックを付け、[アクション]ボタンから[削除]を選択します。
   - 削除したい共有ディレクトリーを選択し、表示された情報画面で[アクション]ボタンから[削除]を選択します。
3. [削除]を選択します。

注意

共有ディレクトリーがマウント中の場合は、削除できません。

2.14.7.4 共有ディレクトリーのマウント

ISMに登録されている共有ディレクトリー情報にマウントする場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリー]を選択します。
2. 以下のどちらかを行います。
   - マウントしたい共有ディレクトリーにチェックを付け、[アクション]ボタンから[マウント]を選択します。
   - マウントしたい共有ディレクトリーを選択し、表示された情報画面で[アクション]ボタンから[マウント]を選択します。

注意

- マウントしたディレクトリーの権限について、以下に示します。
  - 読込み専用でマウントします。
  - SMB/CIFSの場合

    共有ディレクトリー情報を作成したユーザーグループの権限と同じユーザー権限でマウントします。
  - NFSの場合

    root権限でマウントします。

- 以下の場合、マウントは解除されます。
  - ISM-VAを再起動、または停止した場合
  - ISMのサービスを停止した場合
- マウントした共有ディレクトリー情報を持つユーザーグループは、以下の操作ができません。
  - ユーザーグループ名の変更
  - ユーザーグループの削除

2.14.7.5 共有ディレクトリーのマウント解除

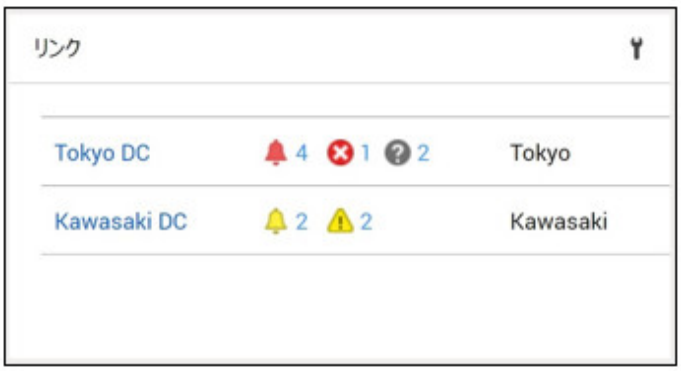
マウントされた共有ディレクトリー情報をマウント解除する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[共有ディレクトリー]を選択します。
2. 以下のどちらかを行います。
   - マウント解除したい共有ディレクトリーにチェックを付け、[アクション]ボタンから[マウント解除]を選択します。
   - マウント解除したい共有ディレクトリーを選択し、表示された情報画面で[アクション]ボタンから[マウント解除]を選択します。

2.14.8 ISM連携管理機能

2.14.8.1 他ISMのステータス情報のリンク表示

別の管理サーバーに導入されたISMのステータス情報（アラームステータス／ステータス）を、ダッシュボードに表示できます。



ステータス（アラームステータス／ステータス）の詳細は、「2.1.1 GUI」を参照してください。

他ISMのステータスをダッシュボードに表示する場合の操作方法を示します。

1. 他ISMのステータスをダッシュボードに表示したいユーザーを設定します。

   なお、このユーザーは、他ISMにも同じユーザー名、パスワードで登録されている必要があります。

   a. Administratorグループに属し、Administratorロールを持つユーザーでISMにログインします。
   b. 他ISMのステータスをダッシュボードに表示したいユーザーの編集を行って、以下を設定します。
      - [ISM連携]で[連携用のユーザーとして設定する]を選択
      - パスワード

2. 表示したい他ISMのCA証明書を登録します。

   詳細は、「2.14.8.2 他ISMのリンク用の証明書管理」の「証明書の登録」を参照してください。

3. GUIのダッシュボードに[リンク]を追加します。

   a. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。

      [リンク]が表示されている場合、手順fへ進みます。

      [リンク]が表示されていない場合、以下の手順でリンクを追加してください。

   b. 上部にある[☰]から[ウィジェット追加]を選択します。

   c. 表示される[ウィジェット追加]から[リンク]を選択し、[追加]ボタンを選択します。

   d. [☰]から[レイアウト変更]を選択します。

   e. [レイアウト変更中]の[保存]を選択します。

   f. ダッシュボードに表示される[リンク]の[🔧]を選択します。

   g. 「ウィジェット設定:リンク」画面で、以下を設定します。

      - 名前:ウィジェットで表示したい名前を指定します。
      - URL:他ISMへのURLを以下のように指定します。

        https://＜対象ISMのIPアドレス、またはFQDN名＞:＜ポート番号＞
      - 説明:説明(コメント)を自由に指定してください。

ウィジェット追加方法、およびウィジェットの内容の詳細については、ISMのオンラインヘルプを参照してください。

2.14.8.2 他ISMのリンク用の証明書管理

ウィジェットのリンク機能で、他ISMにアクセスする場合のCA証明書を追加します。

証明書の登録

新しく証明書を追加する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[CA証明書]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 必要な情報を入力します。

   ー インポート完了後の動作

   元のファイルを削除するかどうかを選択します。

   ー ファイル

   アクセスしたい他ISMのCA証明書をアップロードし、アップロードしたファイルを設定してください。

   ー ホスト名/IPアドレス

   アクセスしたい他ISMのホスト名、またはIPアドレスを設定してください。

4. [登録]ボタンを選択します。

   結果画面が表示され、「CA証明書リスト」画面に登録した証明書が表示されます。

注意

- 登録する証明書は、CA証明書です。CA証明書は、「4.7.5 CA証明書のダウンロード」を参照してください。
- 登録した証明書で、実際に他ISMにアクセスできるかはチェックされません。

証明書の削除

ISMに登録されている証明書を削除する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[CA証明書]を選択します。
2. 以下のどちらかを行います。
   - 削除したい証明書にチェックを付け、[アクション]ボタンから[削除]を選択します。
   - 削除したい証明書を選択し、表示された情報画面で[アクション]ボタンから[削除]を選択します。
3. [削除]を実行し、証明書を削除します。

注意

ウィジェットのリンク機能を使用中の場合でも、証明書は削除できます。

2.14.9 他ソフトウェア連携機能

ISMからほかのソフトウェアへ連携し、ソフトウェアが管理する情報をISM GUIのダッシュボード画面にウィジェットで表示できます。

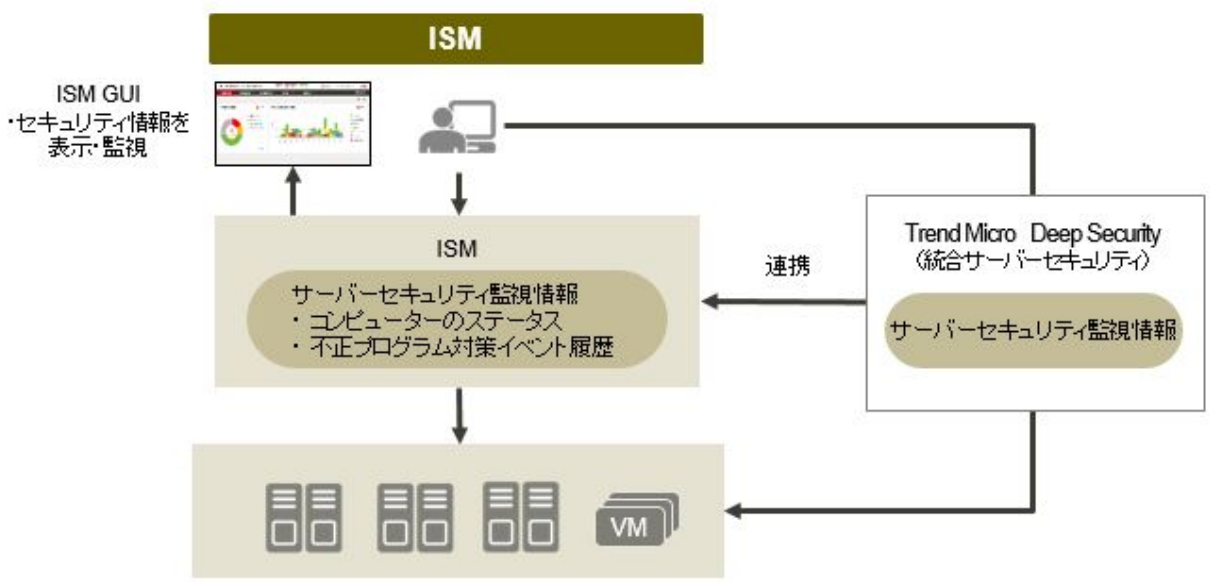
連携可能なソフトウェアは以下のとおりです。

- Trend Micro Deep Security v10.0以降

  統合サーバーセキュリティソフトウェアです。物理マシンおよび仮想マシンのセキュリティを統合監視します。

  Trend Micro Deep Securityの管理モジュールであるDeep Security Managerと連携し、ISMで管理している機器のセキュリティ状況を監視できます。

図2.52 Trend Micro Deep Securityとの連携イメージ



ISM GUIのダッシュボードで表示できるウィジェットは以下のとおりです。

- コンピューターのステータスウィジェット

  Deep Security Managerが管理するコンピューターのセキュリティステータスをグラフ表示します。グラフを選択すると、Deep Security ManagerのGUIが起動され、詳細情報が確認できます。

- 不正プログラム対策イベント履歴ウィジェット

  Deep Security Managerの不正プログラム対策イベント履歴を時系列グラフ表示します。グラフを選択すると、Deep Security ManagerのGUIが起動し、詳細情報を確認できます。

図2.53 Deep Security連携ウィジェット

2.14.9.1 Deep Security連携の事前準備

注意

事前にDeep Securityの準備が必要です。詳細はTrend Micro社のWebサイトのドキュメントを参照してください。なお、Deep Security ManagerのIPアドレスがIPv6リンクローカルアドレスの場合、ISMとの連携はできません。

1. Deep Security ManagerのGUIより、以下の設定を行います。

   a. Deep Security Managerのユーザーアカウントを設定します。
   ユーザーの役割に「Webサービス API へのアクセスを許可」のアクセスの種類を設定してください。

   b. Deep Security Managerのタイムゾーンの確認をします。
   画面上部に表示されているユーザー名からユーザープロパティを選択します。タイムゾーンが表示されますので書き留めてください。

   詳細はTrend Micro社のWebサイトのDeep Security REST APIの使用に関するドキュメントを参照してください。

2. Deep Security Managerの証明書を取得します。

   Webブラウザーから証明書をエクスポートします。エクスポートファイルの形式は「Base 64 encoded X.509(.CER)」を選択してください。

   ポイント

   Webブラウザーごとの証明書のエクスポート方法は以下のとおりです。WebブラウザーでDeep Security ManagerのGUIを表示し、以下の手順でエクスポートします。

   ー Google Chromeの場合

   1. アドレス横の鍵のアイコンを選択し、「証明書」を選択します。
   2. [詳細]タブから[ファイルにコピー]を選択します。
   3. 証明書のエクスポートウィザードが起動します。以下を指定してエクスポートします。
      - 「エクスポートファイルの形式」の「Base 64 encoded X.509(.CER)(S)」
      - 「エクスポートするファイル」のファイル名および保存場所

ー Firefoxの場合

1. アドレス横の鍵のアイコンを選択します。Deep Security Managerのホスト名（IPアドレスまたはFQDN）を選択し、[詳細を表示]を選択します。
2. [証明書を表示]を選択し、[詳細]タブを選択します。
3. [エクスポート]を選択します。「証明書をファイルに保存」で以下を指定してエクスポートします。
   - ファイルの種類の「X.509証明書（PEM）」
   - ファイル名および保存場所

注意

エクスポートファイルの形式は必ず「Base 64 encoded X.509(.CER)」を指定してください。ほかの形式の証明書は使用できません。

3. 証明書ファイルをISM-VAにアップロードします。
   アップロード方法の詳細は、『操作手順書』の「1.4.1 ISM-VAにファイルをアップロードする」を参照してください。アップロード時、ファイルタイプに「他ソフトウェア連携用証明書」を指定します。
4. ISM-VAへ証明書を登録します。

   コンソールからadministratorでISM-VAにログインし、以下のコマンドを実行します。

   Deep Security Managerのホスト名（IPアドレスまたはFQDN）の種類に応じて実行例が異なります。

   ー IPv4アドレスの場合

   ```
   # ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv4 -server ＜Deep Security ManagerのIPv4アドレス＞ -file ＜証明書ファイル名＞
   ```

   ー IPv6アドレスの場合

   ```
   # ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv6 -server ＜Deep Security ManagerのIPv6アドレス＞ -file ＜証明書ファイル名＞
   ```

   ー FQDNの場合

   ```
   # ismadm security import-software-cert -software TrendMicroDeepSecurity -type fqdn -server ＜Deep Security ManagerのFQDN＞ -file ＜証明書ファイル名＞
   ```

   例：Deep Security Managerのホスト名がIPv4形式で「192.168.100.5」、証明書ファイル名が「DSManager.pem1」の場合

   ```
   # ismadm security import-software-cert -software TrendMicroDeepSecurity -type ipv4 -server 192.168.100.5 -file DSManager.pem1
   ```

2.14.9.2 Deep Securityへの連携手順

1. ISMのGUIにログインし、ダッシュボード画面を開きます。
2. 画面の右上に表示されているユーザー名から[言語]を選択します。
3. Deep Security Managerに設定されているタイムゾーンと同じタイムゾーンを設定します。
4. 画面の右上端にある[☰]から「ウィジェット追加」を選択します。
5. 「ウィジェット追加」画面から[その他のウィジェット]パネルを選択します。
   「その他のウィジェット」画面に[Trend Micro連携ウィジェット] が表示されます。
6. [Deep Securityコンピューターのステータス]パネル、または[Deep Security 不正プログラム対策イベント履歴]パネルを選択し、[追加]ボタンを選択します。

7. Trend Micro連携ウィジェットを新規に表示する場合、Deep Security Managerの情報を設定します。表示された画面から、以下の情報を入力します。

項目	入力内容
ホスト名	Deep Security ManagerのIPアドレスまたはFQDN
アカウント名	Deep Security Managerのユーザーアカウント
パスワード／パスワード（確認）	Deep Security Managerのパスワード
ポート番号	Deep Security Managerのポート番号 デフォルトは4119です。4119から変更している場合は、変更したポート番号を入力します。

8. 情報を入力後、[適用]ボタンを選択します。

   Deep Security Managerの情報がすでに登録されている場合は、登録済みのDeep Security Managerの一覧が表示されます。ウィジェットを表示するDeep Security Managerにチェックを付け、[適用]ボタンを選択します。

   ウィジェットがダッシュボード画面に表示されます。

   ウィジェットの表示内容の説明については、ISM GUIのオンラインヘルプを参照してください。

ポイント

- Deep Security連携ウィジェットの表示に問題がある場合、ウィジェット上にメッセージが表示されます。

  表示されるメッセージの内容と説明は以下のとおりです。

メッセージ	対処方法
証明書を登録してください。	Deep Security Managerの証明書が登録されていません。 「2.14.9.1 Deep Security連携の事前準備」の手順を実施しISMへ証明書を登録してください。
証明書ファイルが存在しません。証明書を再登録してください。	証明書ファイルがDeep Security Managerの証明書ファイルではありません。 「2.14.9.1 Deep Security連携の事前準備」を参照して再度証明書の取得を行い、ISMへ登録してください。
証明書ファイルが有効ではありません。証明書ファイルを確認してください。	期限切れなど、証明書ファイルが有効な状態ではありません。 「2.14.9.1 Deep Security連携の事前準備」を参照して再度証明書の取得を行い、ISMへ登録してください。
ログインに失敗しました。管理ソフトウェアからエラーが返却されました。	Deep Security Managerとの接続に問題があります。以下のような原因が考えられます。 ・ ISM GUIから入力したDeep Securityのユーザー名またはパスワードに誤りがある。 ・ 証明書ファイルの形式に誤りがある。または証明書ファイルのホスト情報が接続対象のDeep Securityのホスト名でない。 ・ Deep Securityとの通信ができない。 ・ Deep Securityのセッション数が許容数を超過している。 詳細な原因についてはDeep Securityのシステムイベントを確認してください。

  問題が解決しない場合、または上記以外のメッセージが表示される場合はISMの保守資料を採取して当社技術員に連絡してください。

- Deep Security連携ウィジェットのリンクを選択してDeep Security Managerのログオン画面が表示された場合は、必ずログオンを行ってください。またログオン後はログアウトをしないでください。

  上記を行わない場合、以下のような現象となることがあります。その場合は対処方法に示す操作を実施してください。

現象	対処方法
Deep Security Managerの画面が真っ白になる。	画面が表示されたウィンドウのアドレスに以下のURLを入力します。 https://＜Deep Security ManagerのIPアドレス＞:＜Deep Security Managerのポート番号＞ Deep Security Managerのログオン画面が表示されますのでログオンを行ってください。
ISMのGUI画面が表示されていたウィンドウにDeep Security Mangerの画面が表示される。	ブラウザーの[戻る]ボタンを選択するとISMのGUI画面が表示されます。 ウィジェットのリンクを選択するとDeep Security Managerのログオン画面が表示されますのでログオンを行ってください。

- Deep Security Managerのログオン画面からログオンしたあと、Deep Security Managerのダッシュボード画面が表示されることがあります。この場合は再度ウィジェットのリンクを選択してください。詳細情報を表示できます。

第3章 導入

この章では、ISMの導入方法を説明します。

ポイント

ISM for PRIMEFLEXを使用して仮想化基盤システムを構築する場合、ISMの導入方法については、以下を参照してください。

- PRIMEFLEX for VMware vSANを構築する場合

  『Integrated System PRIMEFLEX for VMware vSAN V1 インストレーションガイド』の「3. 仮想化基盤システムの導入」

- PRIMEFLEX for VMware vSAN V2／PRIMEFLEX for VMware vSAN V3／PRIMEFLEX for VMware vSAN V4を構築する場合

  『Integrated System PRIMEFLEX for VMware vSAN V2 インストレーションガイド』または『Integrated System PRIMEFLEX for VMware vSAN V3 デプロイメントガイド』または『Integrated System PRIMEFLEX for VMware vSAN V4 デプロイメントガイド』の「仮想化基盤の構築」

3.1 ISM導入の流れ

ISMの導入の流れについて説明します。

(1)導入設計

ISMを導入するにあたって事前に準備しておくべき作業は以下のとおりです。

- ディスク資源の見積り
- リポジトリの設定
- ネットワークの設計
- ノード名の設計
- ユーザーの設計

作業内容については、「3.2 ISMの導入設計」を参照してください。

(2)ISM-VAのインストール

ISM-VAを管理サーバーにインストールします。

インストール手順については、「3.3 ISM-VAのインストール」を参照してください。

(3)ISM-VAの環境設定

インストールしたISM-VAの動作環境を設定します。

環境設定手順の内容については、「3.4 ISM-VAの環境設定」を参照してください。

(4)ライセンスの登録

ISMの使用に必要なライセンスを登録します。

ライセンスの登録作業については、「3.5 ライセンスの登録」を参照してください。

(5)ユーザーの登録

ISMの利用者をユーザーとして登録します。

ユーザーを登録する作業については、「3.6 ユーザーの登録」を参照してください。

(6)仮想ディスクの割当て

ISM-VAのディスク容量を拡張するため、仮想ディスクを割り当てます。

「3.7 仮想ディスクの割当て」を参照して、ISM-VA全体とAdministratorユーザーグループに対して仮想ディスクを割り当ててください。

注意

ISM-VA導入後は、すぐに「3.7.2 ユーザーグループに対する仮想ディスク割当て」手順でAdministratorグループ用の仮想ディスク割当てを行ってください。

(7)仮想化管理ソフトウェアの登録

管理対象ノードに構築された仮想マシンや仮想スイッチを管理する場合、仮想化管理ソフトウェアを登録します。

仮想化管理ソフトウェアの登録作業については、「2.14.6 仮想化管理ソフトウェア管理機能」を参照してください。また、仮想化管理ソフトウェア管理機能を使用するために必要な事前設定については、「付録B 監視対象OS、仮想化管理ソフトウェアに対する設定」を参照してください。

(8)仮想リソース／クラスタを管理するための事前設定

仮想リソース管理機能、ISM for PRIMEFLEXのクラスタ管理機能を使用するためには、事前に設定が必要です。

「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

3.2 ISMの導入設計

ISMを円滑に運用するには、事前の導入設計が重要です。以下を設計してください。

- 3.2.1 ディスク資源の見積り
- 3.2.2 ネットワークの設計
- 3.2.3 ノード名の設計
- 3.2.4 ユーザーの設計

3.2.1 ディスク資源の見積り

ISMの利用にあたっては、下表のディスク領域の使用量見積りと事前の追加割当てを行ってください。

用途	保管されるデータ	容量算出方法	種別	
			システム領域	ユーザー領域
ログ保存	ログ管理機能で取得したログ、およびアーカイブしてダウンロードする際のファイル 「2.5 ログ管理機能」	ログを採取するノード数、採取するログの種類、採取頻度、保管期間に応じて算出 「3.2.1.1 ログ保存容量の見積り」	○[注1]	○
リポジトリ（ServerView Suite DVDを除く）	DVDイメージやファームウェアデータ 「2.4 プロファイル管理機能」 「2.6 ファームウェア管理機能」	インポートするDVD数、ファームウェアデータ量に応じて算出 「3.2.1.2 リポジトリに必要なディスク容量の見積り」	○[注1]	○
リポジトリ（ServerView Suite DVDのみ）	DVDイメージ 「2.4 プロファイル管理機能」 「2.6 ファームウェア管理機能」	インポートするDVD数に応じて算出 「3.2.1.2 リポジトリに必要なディスク容量の見積り」	○	－
ノード管理データ	ISMが内部動作に使用するデータ	管理するノード数に応じて算出 「3.2.1.3 ノード管理データ容量の見積り」	○	－

用途	保管されるデータ	容量算出方法	種別	
			システム領域	ユーザー領域
障害調査ログ	トラブル発生時の調査などに使用するログ	管理するノード数に応じて算出 「3.2.1.4 障害調査ログ容量の見積り」	○	―
保守資料	障害調査ログをアーカイブして取り出す際のファイル 「4.5 保守資料の採取」	管理するノード数および資料を保管する世代に応じて算出 「3.2.1.5 保守資料容量の見積り」	○[注1]	○[注2]
ISMバックアップ／リストア	ISMバックアップファイル 「4.4 ISMのバックアップとリストア」	管理するノード数に応じて算出 「3.2.1.6 ISMバックアップ／リストアに必要な容量の見積り」	○[注1]	○[注2]
サステナビリティモニター機能のCSVエクスポート	CO2排出量・消費電力データをCSV形式で出力したファイル 「2.12.4 CSVのエクスポート」	サステナビリティモニター機能の対象ノード数およびセッション数に応じて算出 「3.2.1.7 サステナビリティモニター機能のCSVエクスポートに必要な容量の見積り」	○[注1]	○[注2]

[注1]:ユーザーグループに領域が割り当てられている場合、そのユーザーグループでは割り当てられた領域が使用されます。領域が割り当てられていないユーザーグループではシステム領域が使用されます。

[注2]:Administratorユーザーグループのリポジトリ領域に出力されます。

注意

- ISM-VAの運用中は、ディスク容量を動的に拡張できません。このため、運用中にディスク容量が不足すると、ログ管理機能のログ収集やリポジトリ、バックアップの運用に影響します。ディスクの容量が不足しないように、事前に見積っておくことが重要です。

  見積ったディスク容量は、仮想ディスクとして作成し、ISM-VAに割り当てます。

  システム領域に対する仮想ディスクの作成、割当て方法については、「3.7.1 ISM-VA全体に対する仮想ディスク割当て」を参照してください。

  ユーザーグループに対する仮想ディスクの作成、割当て方法については、「3.7.2 ユーザーグループに対する仮想ディスク割当て」を参照してください。

- ディスクの容量不足を回避するため、不要になったリポジトリのデータやバックアップデータなどを定期的に削除するといった運用も併せて設計してください。

- 現在使用中のディスク容量は、以下の手順で確認できます。

  1. コンソールからadministratorでISM-VAにログインします。
  2. ディスクの使用状況を確認します。

     ```
     ismadm volume show -disk -r
     ```

     /dev/mapper/centos-rootを確認します。

     例:

     ```
     # ismadm volume show -disk -r
     Filesystem              Size  Used Avail Use% Mounted on
     /dev/mapper/centos-root   31G  4.2G   27G  14% /
     devtmpfs                3.9G     0  3.9G   0% /dev
     tmpfs                   3.9G  4.0K  3.9G   1% /dev/shm
     tmpfs                   3.9G  225M  3.7G   6% /run
     tmpfs                   3.9G     0  3.9G   0% /sys/fs/cgroup
     /dev/sda1               497M  172M  326M  35% /boot
     tmpfs                   783M     0  783M   0% /run/user/1005
     ```

```
tmpfs                   783M     0  783M   0% /run/user/0
tmpfs                   783M     0  783M   0% /run/user/1001

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
  /dev/sda3  centos lvm2 a--  15.00g    0
#
```

3.2.1.1 ログ保存容量の見積り

ログ管理機能で出力するログのディスク容量は、管理対象のノード数、ログの保有期間、または保有回数に依存します。将来的に増設するノード数を考慮して見積ってください。

また、ログをダウンロードする際に使用するディスク容量も同様に見積ってください。

ログ管理機能で出力するログのディスク容量の見積り方法については、「A.3.2 ログ管理機能利用時のディスク消費量の目安」を参照してください。

また、ログ管理機能で出力するログとは別に「運用ログ」「監査ログ」「SNMPトラップ」があります。
これらの最大保管数と容量は、以下となります。これらの容量はノード数に依存しません。

- 運用ログ、監査ログ

  最大保管数:各1,000,000件(各200MB)

- SNMPトラップ

  最大保管数:100,000件(300MB)

これらの容量は、「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」の空きディスク容量に含まれます。

3.2.1.2 リポジトリに必要なディスク容量の見積り

プロファイル管理機能やファームウェア管理機能の運用には、ISM-VAにリポジトリの準備が必要です。リポジトリには、以下のデータが格納されます。

- ファームウェアのデータ
- OSのイメージファイル
- 作業ファイル

リポジトリに必要なディスク容量は、管理対象ノードにインストールするOSの種類やインポートするServerView Suite Update DVDの数に応じて異なります。通常は、20GB以上が使用されます。下表を参照して必要なディスク容量を見積ってください。

用途	操作	必要なディスク容量
ファームウェアデータの格納	ServerView Suite Update DVDのインポート	ServerView Suite Update DVD1枚当たり14GB程度
	その他のファームウェアデータのインポート	インポートデータに依存 ～100MB程度
OSインストールメディアのファイル格納	Windowsインストールメディアのインポート	OS1種当たり3～8GB程度 プロファイル管理機能でインストールするOS種のみインポートが必要
	VMware ESXiインストールメディアのインポート	OS1種当たり0.5GB程度 プロファイル管理機能でインストールするOS種のみインポートが必要
	Linuxインストールメディアのインポート	OS1種当たり4GB程度
ServerView Suite DVDの格納	ServerView Suite DVDのインポート	ServerView Suite DVD1枚当たり8GB程度
作業用ファイルの作成／保管	特になし	0.5GB程度
coreファイル採取／保管	ismadm system core-dirでの設定	1GB程度

ポイント

- ユーザーグループとノードグループを関連付けることで、ノードグループごとに分離してISMを運用できます。この場合、ユーザーグループごとにリポジトリを準備します。ユーザーグループ数の分だけ、リポジトリにServerView Suite DVD以外の必要なディスク容量を見積る必要があります。
- ServerView Suite DVDは、システム領域に格納されます。使用するServerView Suite DVDの数に応じて、システム領域のLVMボリュームに必要なディスク容量を見積る必要があります。

3.2.1.3 ノード管理データ容量の見積り

ISM-VAで管理するノード数に応じて、ノード管理データ領域のためのディスク容量を見積ってください。

以下は、管理対象ノード数とノード管理データ領域に必要なディスク容量の目安です。

管理対象ノード数	必要なディスク容量
100ノード以下	20GB
400ノード以下	80GB
1000ノード以下	200GB

注意

上記は、ノード登録時の初期監視項目から変更しなかった場合の目安です。

上記に加えて以下を利用する場合には、ディスク容量の追加が必要です。以下を参照し必要なディスク容量を追加してください。

- アノマリ検知機能

  詳細は、「2.3.6.1 動作要件」を参照してください。

- ネットワーク統計情報

  以下の記載を確認してください。

ネットワーク統計情報の監視設定が有効の場合

ネットワーク統計情報を監視する場合、さらに以下の容量の見積りが必要です。必要となるディスク容量は、ネットワーク機器に応じて異なります。

分類	ディスク容量
1ポートあたりのディスク容量 監視データは、最大1年分保存します。	240MB
ネットワーク統計表示をサポートしているスイッチ1台当たりのディスク容量	スイッチが持つポート数×240MB
ISM全体で必要となるディスク容量	管理しているスイッチのディスク容量の総和

注意

スイッチのポートを未使用の場合でも、監視対象となります。

ネットワーク統計表示をサポートしているスイッチについては、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

以下に、ネットワーク統計情報を監視する場合の見積り例を示します。

- 監視スイッチ:イーサネットスイッチ10GBASE-T 48+6/10GBASE 48+6 × 10台
- 1ポートあたり、1カ月で20MB、1年で240MBのディスク容量が必要
- 監視スイッチ1台当たりのポート数:54個
- ISM全体で必要となるディスク容量

＜1ポートあたりのディスク容量＞ × ＜スイッチのポート数＞ × ＜スイッチ台数＞

＝ 240 × 54 × 10

＝ 129600 MB

＝ 129.6 GB

ネットワーク統計情報については、「2.7 ネットワーク管理機能」を参照してください。

3.2.1.4 障害調査ログ容量の見積り

ISM-VAで管理するノード数に応じて、障害調査ログレベルの設定を変更し、ディスク容量を見積ってください。

以下は、管理対象ノード数とログ領域に必要なディスク容量の目安です。

管理対象ノード数	障害調査ログレベル	必要なディスク容量
100ノード以下	small(初期値)	10GB
400ノード以下	medium	40GB
1000ノード以下	large	100GB

ログレベルの切替え方法については、「4.5.2.2 障害調査ログレベル切替え」を参照してください。

3.2.1.5 保守資料容量の見積り

ISM-VAで管理するノード数に応じて、障害調査ログレベルの設定を変更し、ディスク容量を見積ってください。

以下は、管理対象ノード数と保守資料領域に必要なディスク容量の目安です。

管理対象ノード数	障害調査ログレベル	必要なディスク容量
100ノード以下	Small(初期値)	15GB
400ノード以下	Medium	50GB
1000ノード以下	Large	120GB

ログレベルの切替え方法については、「4.5.2.2 障害調査ログレベル切替え」を参照してください。

3.2.1.6 ISMバックアップ／リストアに必要な容量の見積り

ISM-VAで管理するノード数に応じて、ISMバックアップ／リストアに必要なディスク容量を見積ってください。

以下は、管理対象ノード数とISMバックアップ／リストアに必要なディスク容量の目安です。

管理対象ノード数	必要なディスク容量
100ノード以下	15GB
400ノード以下	60GB
1000ノード以下	150GB

ネットワーク統計情報の監視情報が有効場合

ネットワーク統計情報を監視する場合、さらに追加容量のな見積りが必要です。
ネットワーク統計情報のディスク容量については、「3.2.1.3 ノード管理データ容量の見積り」を参照してください。

3.2.1.7 サステナビリティモニター機能のCSVエクスポートに必要な容量の見積り

ISM-VAで管理するノードのうちサステナビリティモニター機能の監視対象ノード数に応じて、1セッション当たりのCSVエクスポートに必要なディスク容量を見積もってください。

以下は、監視対象ノード数とサステナビリティモニター機能のCSVエクスポートに必要なディスク容量(1セッション当たり)の目安です。

監視対象ノード数	必要なディスク容量	一時的に必要になるディスク容量
100ノード以下	125MB	205MB
400ノード以下	490MB	810MB
1000ノード以下	1.3GB	2.1GB

注意

複数のセッションでCSVエクスポートを実施する場合、セッション数に応じたディスク容量が必要になります。

3.2.2 ネットワークの設計

ISMがサーバーを管理するには、以下の2種類の管理LANを使用します。

2種類の管理LANをISMで使用するネットワークと繋げてください。

- iRMC Management LANに接続するネットワーク

  主にサーバーの制御やBIOS、iRMC、MMB、仮想IOの設定などに使用します。

- オンボードLANまたはLANカードに接続するネットワーク

  主にOSのインストールやOSをインストールしたあとの接続などに使用します。

また、スイッチやストレージの管理にもネットワークの接続が必要です。それらは物理的/論理的に分割することも、1つに統合することも可能です。

注意

ISM-VAは、デフォルトで「192.168.1.101」のIPアドレスが有効になった状態で起動します。ネットワーク内のほかの装置との競合に注意してください。

IPアドレスが競合する場合は、以下のような手順でIPアドレスを変更することにより、競合を解消できます。

1. 本番環境以外のハイパーバイザーにISM-VAをインストール
2. ISM-VAのIPアドレスを変更
3. ISM-VAをハイパーバイザーでバックアップ(エクスポート)
4. バックアップ(エクスポート)したISM-VAを本番環境のハイパーバイザーにリストア(インポート)

ポイント

- 業務に利用するネットワーク(業務LAN)は、これらの管理LANとは別に用意することを推奨します。
- ユーザーグループとノードグループを関連付けることで、ノードグループごとに分離してISMを運用できます。この場合、ノードグループごとにネットワークを分けて設計してください。ノードグループ間のネットワークにファイアウォールを設けてグループ間の通信を分離することで、ほかのノードグループに属するノードの参照や操作を抑止できます。
- ISMのネットワークインターフェイスは、1つだけ定義できます。複数のネットワークを構成する場合は、ルーターを設定し、各ネットワーク間で通信可能な状態にしてください。

- 物理ネットワークインターフェイスの冗長化のためにISMのネットワークインターフェイスを複数定義できません。

  ISM-VAが動作するハイパーバイザー上でボンディングやチーミングなどを使用して物理ネットワークインターフェイスの冗長化を設定してください。

3.2.3 ノード名の設計

ノードを登録する際に、必要になるノード名およびプロファイル名のルールを決定します。

ノードを登録するときは、1台ごとに固有のノード名を設定します。

ノード名には最大64文字の文字列が設定できます。

ただし以下の文字は使用できません。

スラッシュ(/)、バックスラッシュ(¥)、コロン(:)、アスタリスク(*)、クエスチョンマーク(?)、ダブルクォーテーション(“)、山括弧(<>)、パイプライン(|)

3.2.4 ユーザーの設計

各ユーザーの業務や職務に応じて、適切なユーザーロールやユーザーグループを設定してください。ノードの増設や監視、保守などの業務に合わせてユーザーロールを設定したり、ノードの資源を実際に使用する利用者を組織単位にユーザーグループを設定したりして、ユーザーの役割や体制に合わせたユーザーの設定を推奨します。

ユーザーグループごとにノードの運用を分離する場合には、ユーザーグループが運用／管理するノードをノードグループとして定義し、ユーザーグループとノードグループを関連付けてください。このとき、ユーザーグループには、Administratorロールを持つユーザーを作成してください。

ユーザーグループ、ユーザーの詳細は、「2.14.1 ユーザー管理機能」を参照してください

ノード管理のセキュリティを堅持するため、不要になったユーザーの削除やパスワードを定期的に変更するなどの運用も併せて設計することを推奨します。

ユーザーロール、ユーザーグループの設定方法およびパスワードの変更方法などについては、ISMのオンラインヘルプを参照してください。

3.3 ISM-VAのインストール

ISMソフトウェアは、Infrastructure Manager 各製品のメディアパックに同梱されています。

インストール先に応じてインストールします。

注意

ISM-VAのインストール後、ISMのバックアップファイルのリストア先として使用するISM-VAをバックアップしてください。
ISM-VAのバックアップは、ISMが動作しているハイパーバイザーでバックアップ(エクスポート)してください。

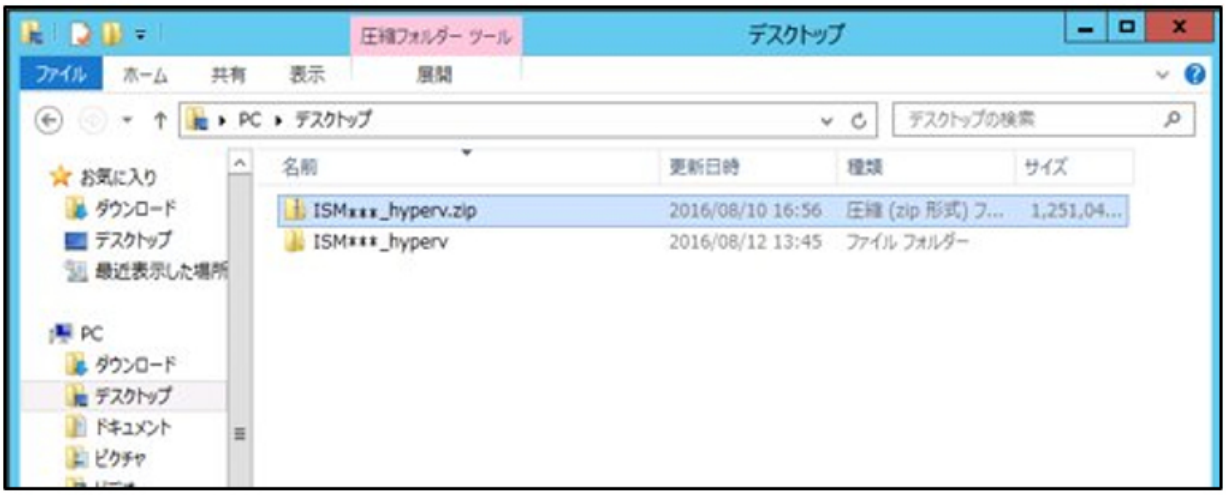
以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMへのインストール手順を説明します。

- 3.3.1 Microsoft Windows Server Hyper-Vへのインストール
- 3.3.2 VMware vSphere Hypervisorへのインストール
- 3.3.3 KVMへのインストール

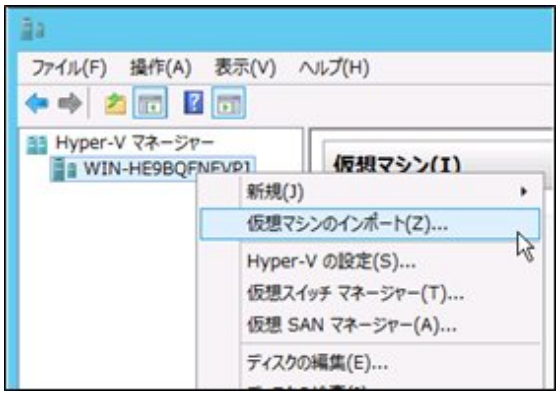
3.3.1 Microsoft Windows Server Hyper-Vへのインストール

DVDメディアに含まれるISM-VAイメージ圧縮ファイル(ISM＜Version＞_hyperv.zip)を使用してインストールします。インストールの途中で指定するインストール先やネットワークアダプターの選択の詳細は、Hyper-Vのマニュアルを参照してください。

1. DVDメディアに含まれるzipファイルを、Hyper-Vホストであるwindowsサーバーの一時展開場所に展開します。

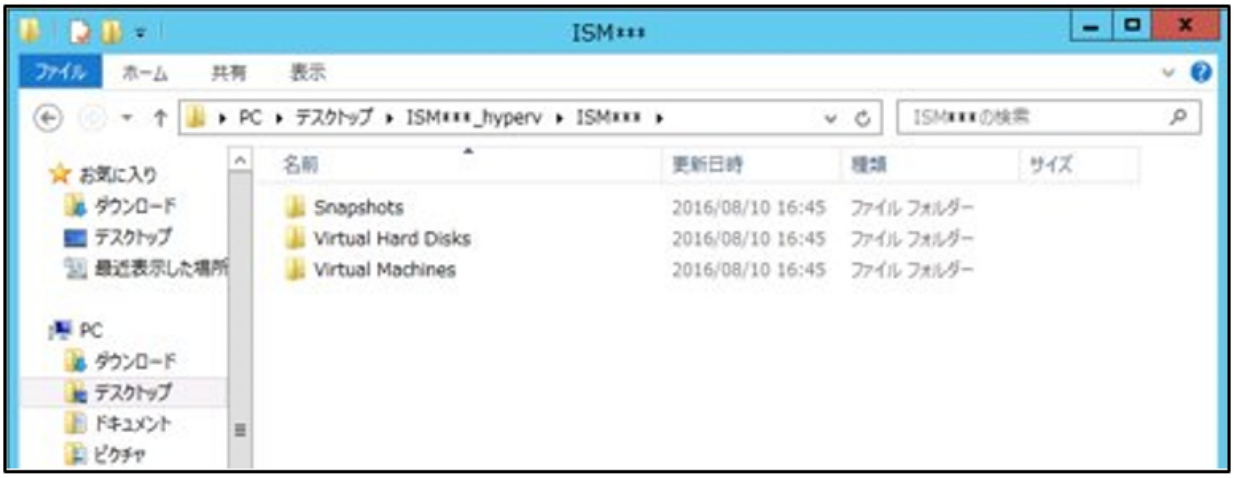


2. Hyper-Vマネージャーを起動し、Hyper-VホストであるWindowsサーバーを右クリックして[仮想マシンのインポート]を選択します。

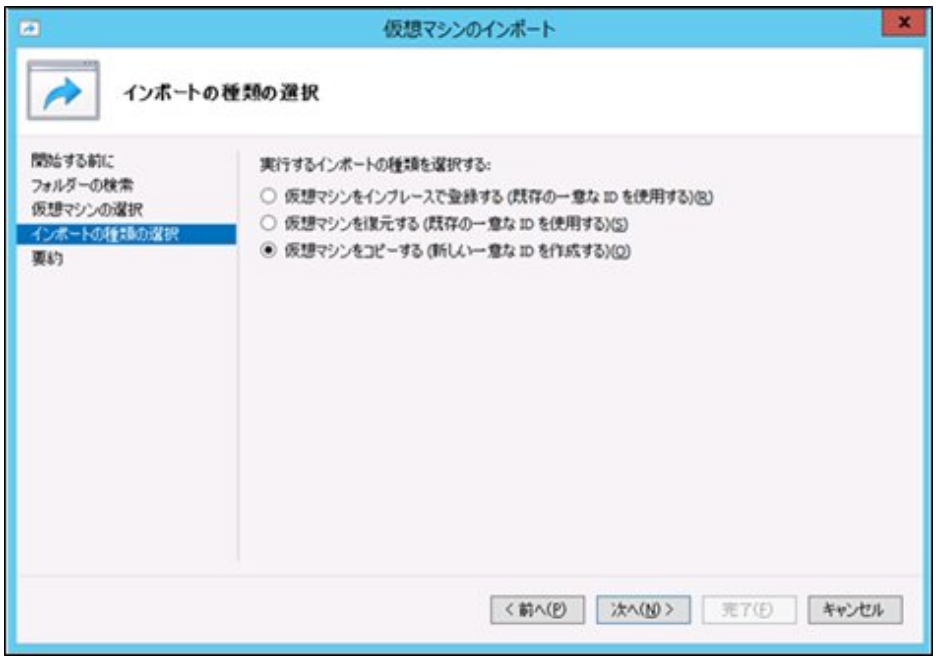


3. 「フォルダーの選択」画面で、手順1で展開したディレクトリーを選択します。

   選択するディレクトリーは、「Snapshots」、「Virtual Hard Disks」、「Virtual Machines」というディレクトリーの親ディレクトリーです。

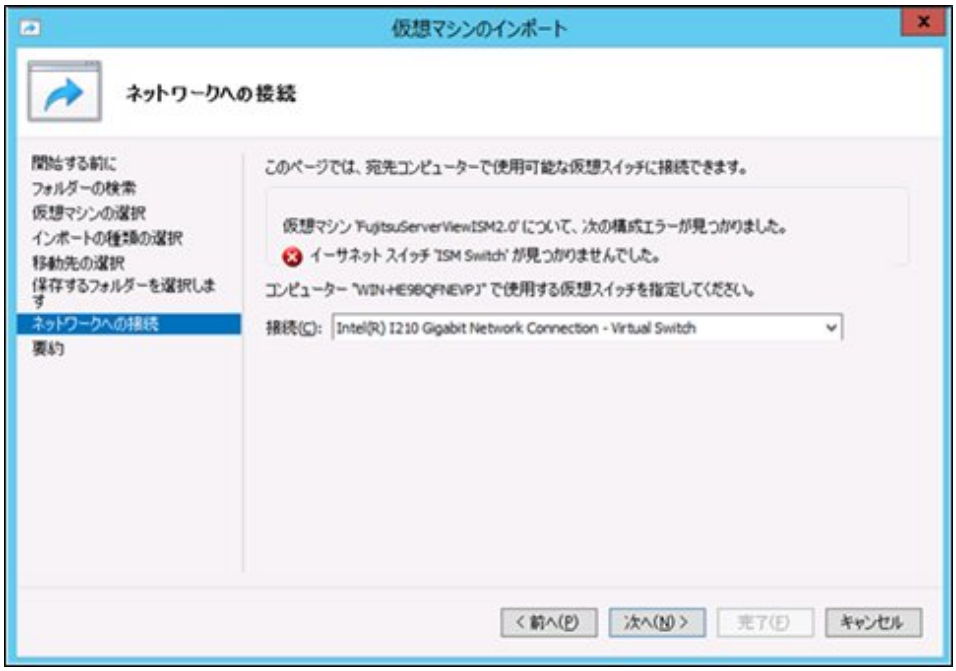


4. 「インポートの種類の選択」画面で、[仮想マシンをコピーする(新しい一意なIDを作成する)]を選択し、[次へ]を選択します。



5. 「移動先の選択」画面と「保存するフォルダーの選択」画面では、ISM-VAのインポート先を選択します。デフォルトの場所が表示されていますので、必要に応じて変更してください。

6. 「ネットワークへの接続」画面で、ISM-VAで使用する仮想スイッチを選択し、[次へ]を選択します。



7. [完了]を選択し、インポートウィザードを完了させます。

8. ISM-VAのインポート完了後、ハードディスクを固定容量に変換します。変換方法の詳細は、Hyper-Vのマニュアルを参照してください。

9. ISM-VAの仮想マシンの構成バージョンを、インポートしたWindowsサーバーが対応する最新のバージョンにアップグレードしてください。構成バージョンのアップグレード方法の詳細は、Hyper-Vのマニュアルを参照してください。

3.3.2 VMware vSphere Hypervisorへのインストール

DVDメディアに含まれるISM-VA定義ファイル（ISM＜Version＞.ovf）とISM-VAイメージファイル（ISM＜Version＞-disk1.vmdk）を使用してインストールします。

VMware ESXiへ直接インストールするかVMware vCenter経由でインストールするかによって、使用するovfファイルが異なります。

- VMware ESXiへ直接インストール

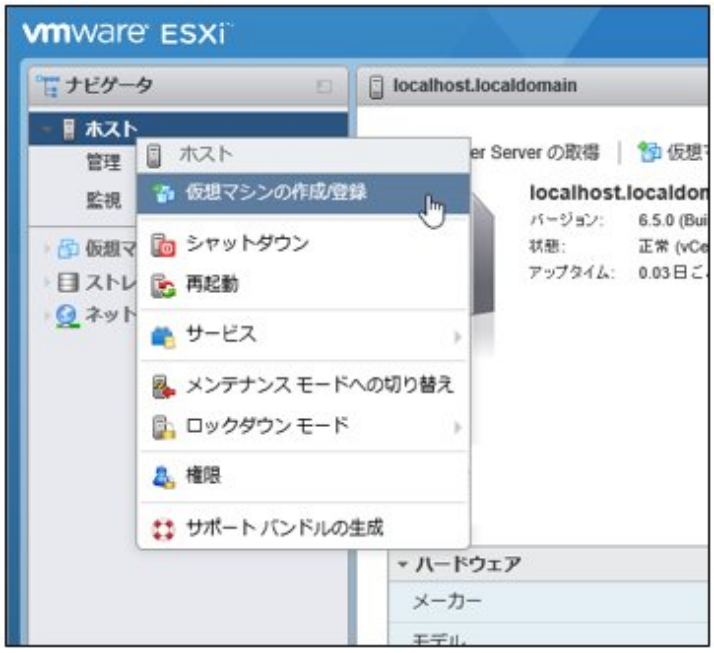
  ISM＜Version＞.ovfを使用

- VMware vCenter経由でインストール

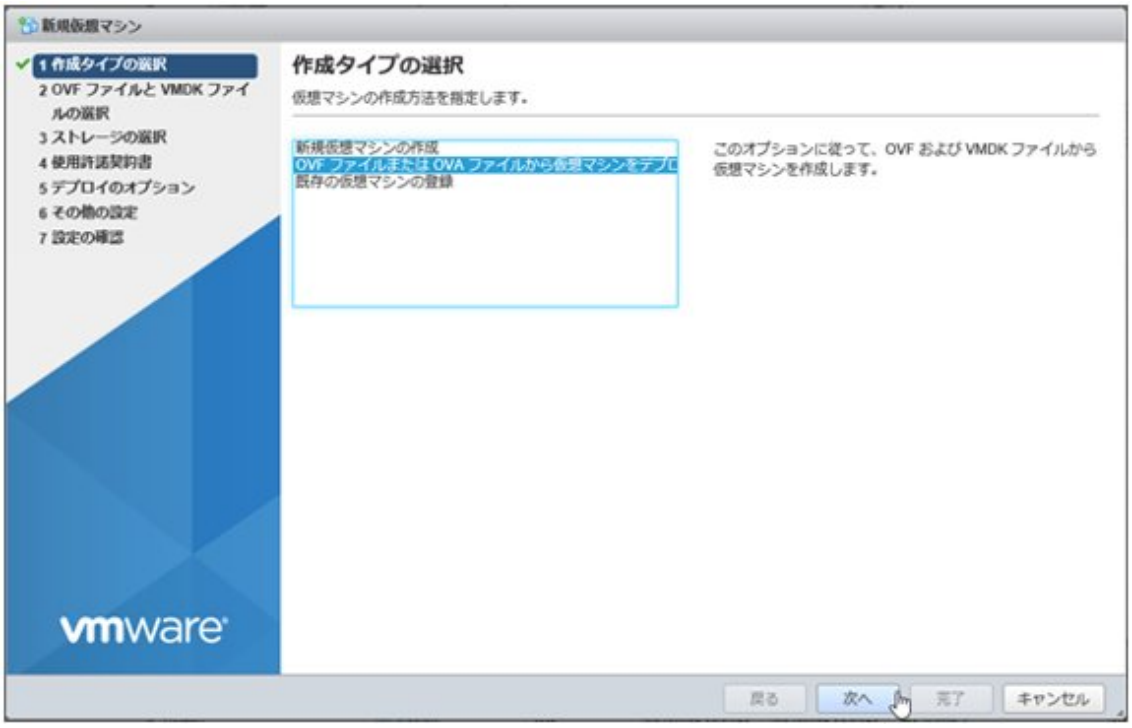
  ISM＜Version＞_vcenter.ovfを使用

  VMware vCenter経由でインストールする場合、インストール途中でISM-VAのネットワーク設定ができます。

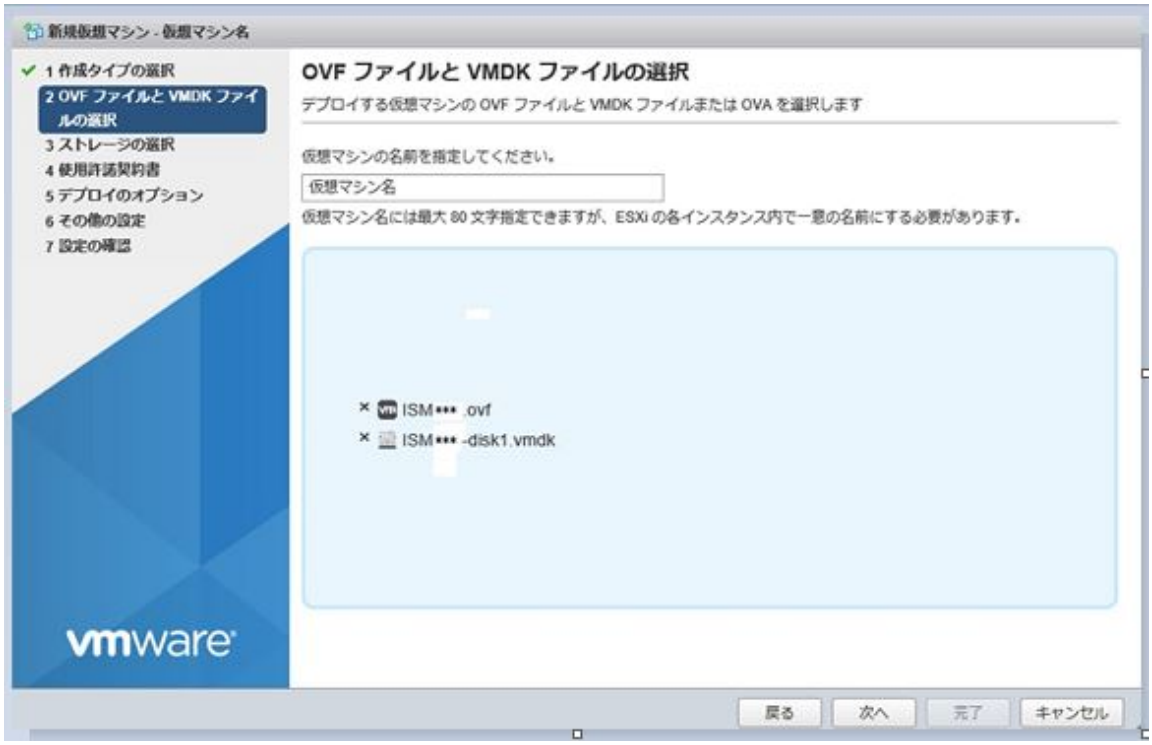
1. vSphere Client（HTML5）を起動し、ナビゲータの[ホスト]を右クリックして、[仮想マシンの作成/登録]を選択します。



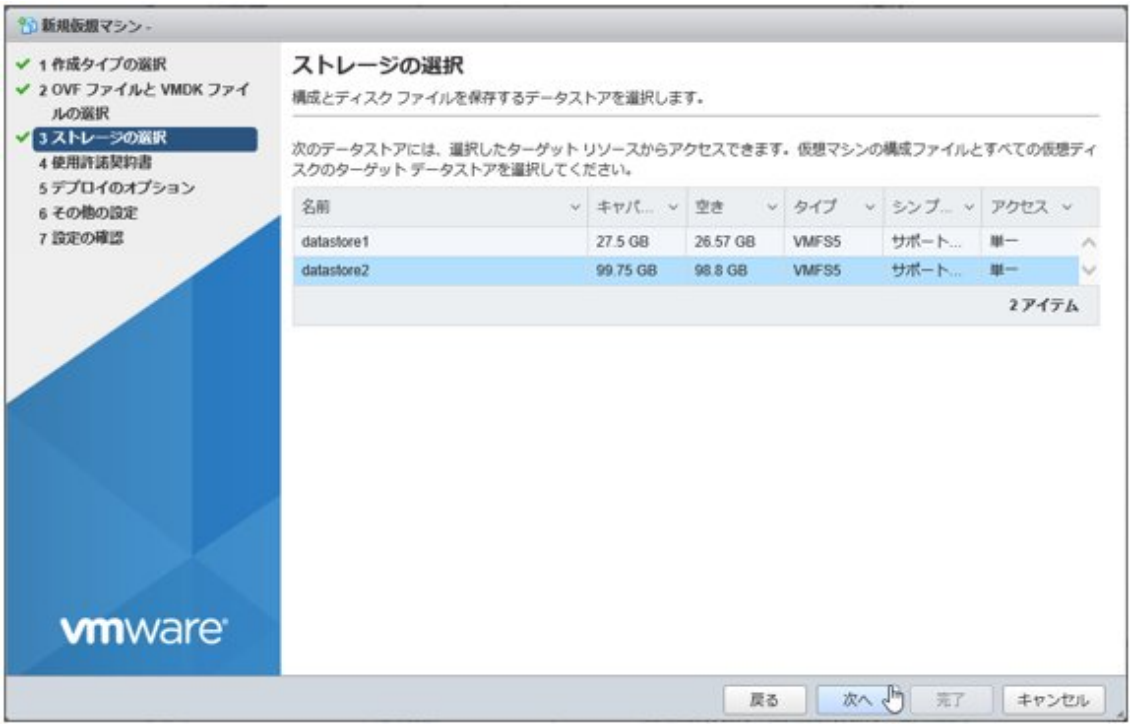
2.「作成タイプの選択」画面で[OVFファイルまたはOVAファイルから仮想マシンをデプロイ]を選択し、[次へ]を選択します。



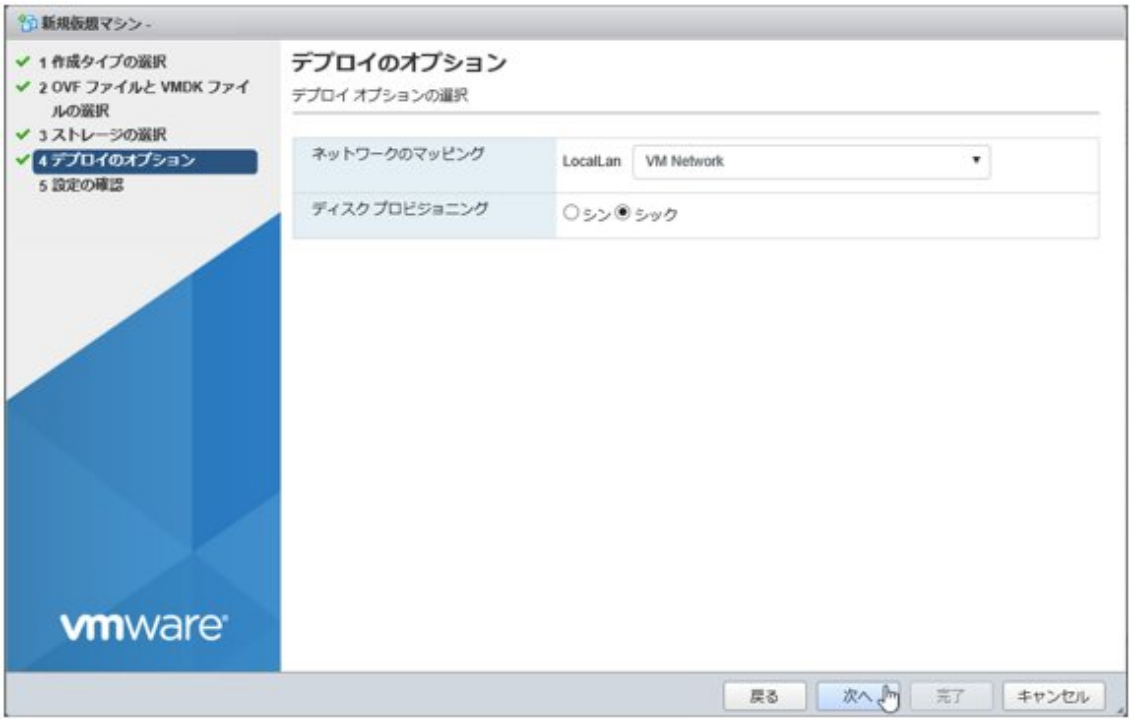
3.「OVFファイルとVMDKファイルの選択」画面で仮想マシンに任意の名称を指定し、DVDメディアに含まれるovfファイルとvmdkファイルをデプロイ設定して、[次へ]を選択します。



4. 「ストレージの選択」画面でデプロイ先のデータストアを選択し、[次へ]を選択します。



5. 「デプロイのオプション」画面で使用するネットワークを選択し、ディスクプロビジョニングは「シック」を選択して、[次へ]を選択します。



6. 「設定の確認」画面で設定内容を確認し、[完了]を選択してデプロイを完了させます。

ポイント

OVFファイル（OVFテンプレート）のデプロイ途中にネットワーク項目を設定した場合、初回電源投入からISM-VA（仮想マシン）が起動するまで10～15分間かかります。初回電源投入後、10分～15分経過後にismsetupまたはismadmコマンドを使用して設定したネットワーク項目を確認してください。設定した内容と異なる場合、数分待ってから再度確認してください。

表3.1 ネットワーク設定項目一覧

項目	説明
01 IP Address	ISM-VAのIPアドレス
02 Netmask	サブネットマスクまたはプレフィックス長（例：255.255.255.0 または 24）
03 Gateway	デフォルトゲートウェイ
04 Hostname	ISM-VAのホスト名（DNSを使用する場合はFQDNで指定する必要があります）
05 Primary DNS	プライマリーDNS（任意設定）
06 Secondary DNS	セカンダリーDNS（任意設定）

3.3.3 KVMへのインストール

DVDメディアに含まれるISM-VAイメージ圧縮ファイル（ISM＜Version＞_kvm.tar.gz）を使用してインストールします。

- Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合
- Nutanix AHVの場合

Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合

1. KVMホストの任意のディレクトリーにtar.gzファイルを転送し展開します。

```
# tar xzvf ISM＜Version＞_kvm.tar.gz
ISM＜Version＞_kvm/
ISM＜Version＞_kvm/ISM＜Version＞_kvm.qcow2
```

```
ISM<Version>_kvm/RedHat7/ISM<Version>.xml
ISM<Version>_kvm/RedHat8/ISM<Version>.xml
ISM<Version>_kvm/RedHat9/ISM<Version>.xml
ISM<Version>_kvm/RedHat10/ISM<Version>.xml
ISM<Version>_kvm/SLES12/ISM<Version>.xml
ISM<Version>_kvm/SLES15/ISM<Version>.xml
```

＜Version＞部分は、ISM-VAのバージョンに応じた表記になります。

2. 展開されたディレクトリーに含まれるファイルをそれぞれ所定の場所にコピーします。

   a. qcow2ファイルを/var/lib/libvirt/imagesにコピーします。

   ```
   # cp ISM<Version>_kvm.qcow2 /var/lib/libvirt/images
   ```

   b. xmlファイルを/etc/libvirt/qemuにコピーします。

   使用するxmlファイルは、インストールするKVMホストに対応するものを使用してください。

   ```
   # cp ISM<Version>.xml /etc/libvirt/qemu
   ```

ポイント

同一ネットワークでISM-VAを複数使用する場合は、KVMホストのvirshコマンドを使用してxmlファイルを編集し、MACアドレスを変更してください。

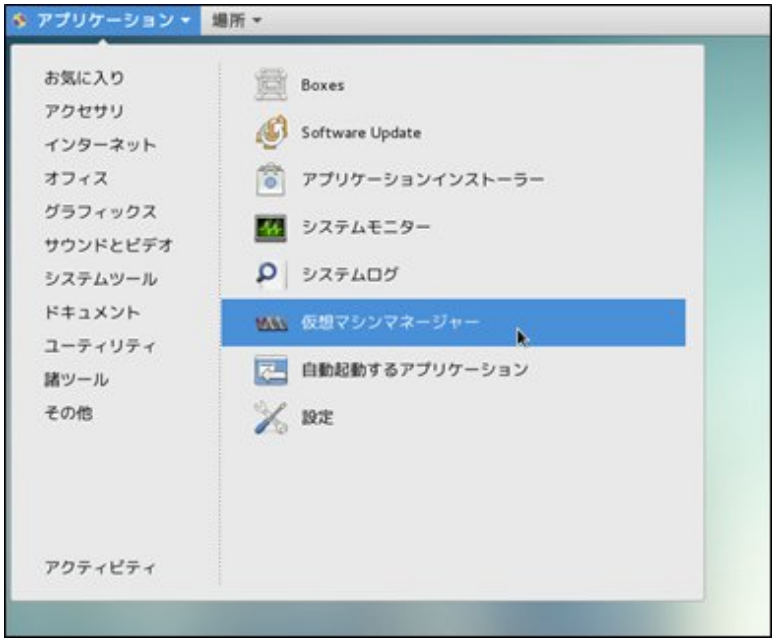
MACアドレス変更方法については、ハイパーバイザーのドキュメントを参照してください。

3. xmlファイルを指定してISM-VAを登録します。

```
# virsh define /etc/libvirt/qemu/ISM<Version>.xml
```

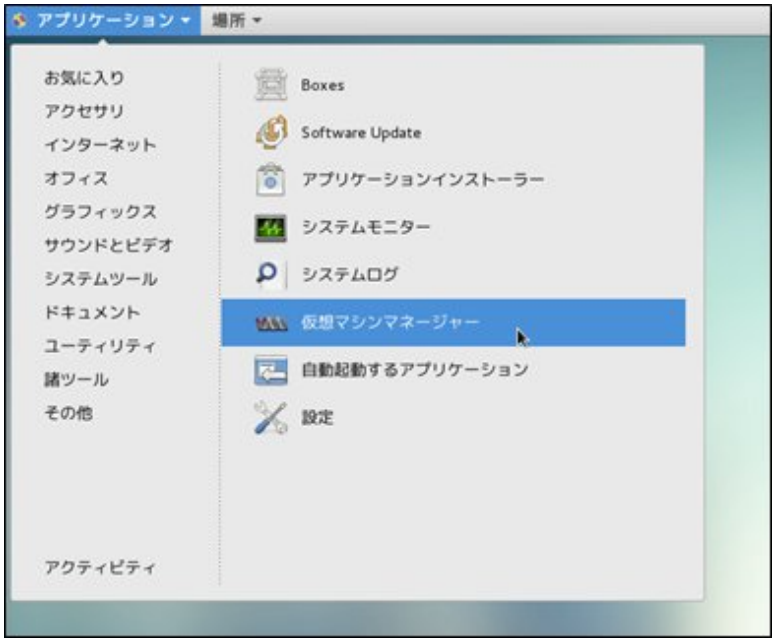
4. 仮想マシン管理ツールを開きます。

Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Serverの場合、[アプリケーション]から[仮想マシンマネージャー]を開きます。



Red Hat Enterprise Linux 10の場合、RHEL Webコンソールの[仮想マシン]を開きます。

RHEL Webコンソールで仮想マシンを使用するための設定は、Red Hat Enterprise Linuxのドキュメントを参照してください。

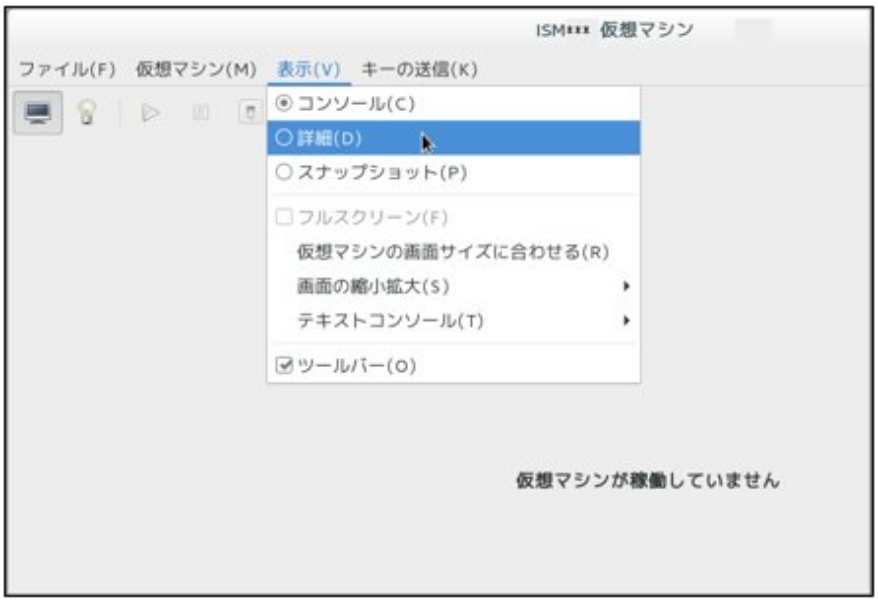


5. 仮想マシン管理ツール上でISM-VAを選択します。

   Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Serverの場合、仮想マシンマネージャー上でISM-VAを選択し、[開く]を選択します。

   Red Hat Enterprise Linux 10の場合、RHEL Webコンソール上でISM-VAの名前を選択します。

6. Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Serverの場合、ISM-VA仮想マシン画面の[表示]メニューから[詳細]を選択します。



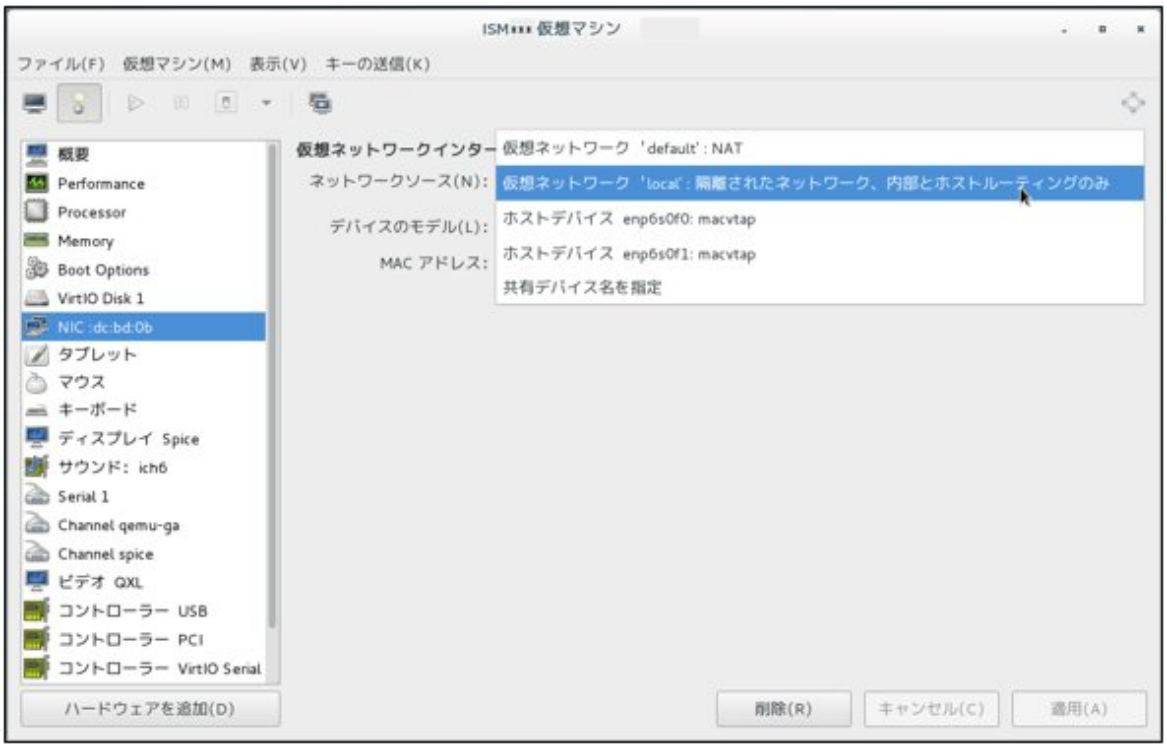
7. ISM-VAを接続するネットワークソースを選択します。

   ネットワークソースは、ISM-VA仮想マシンに対して外部から接続可能なネットワークソースを選択してください。

   ネットワークソースの名称および設定方法はインストールするOSの版数によって異なる場合がありますので、詳細はRed Hat Enterprise ServerまたはSUSE Linux Enterprise Serverのドキュメントを参照してください。

   Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Serverの場合、外部から接続可能なネットワークソースは「ブリッジデバイス」および「Macvtapデバイス」と表示されますので、いずれかを選択してネットワークデバイスを設定してください。

   仮想ネットワークデバイスのモデルは、「virtio」を選択してください。



Red Hat Enterprise Linux 10の場合、[ネットワークインターフェース]の[編集]ボタンを押し、インターフェース形式およびソースを設定してください。

8. ノードの自動検出機能を使用する場合はUDPマルチキャストがISM-VA仮想マシンに届く必要があるため、インストールするOS上で以下のコマンドを実行してください。

```
# ip link set dev ＜デバイス名＞ allmulticast on
```

＜デバイス名＞は、手順7で設定したデバイス名を指定してください。

実行例:

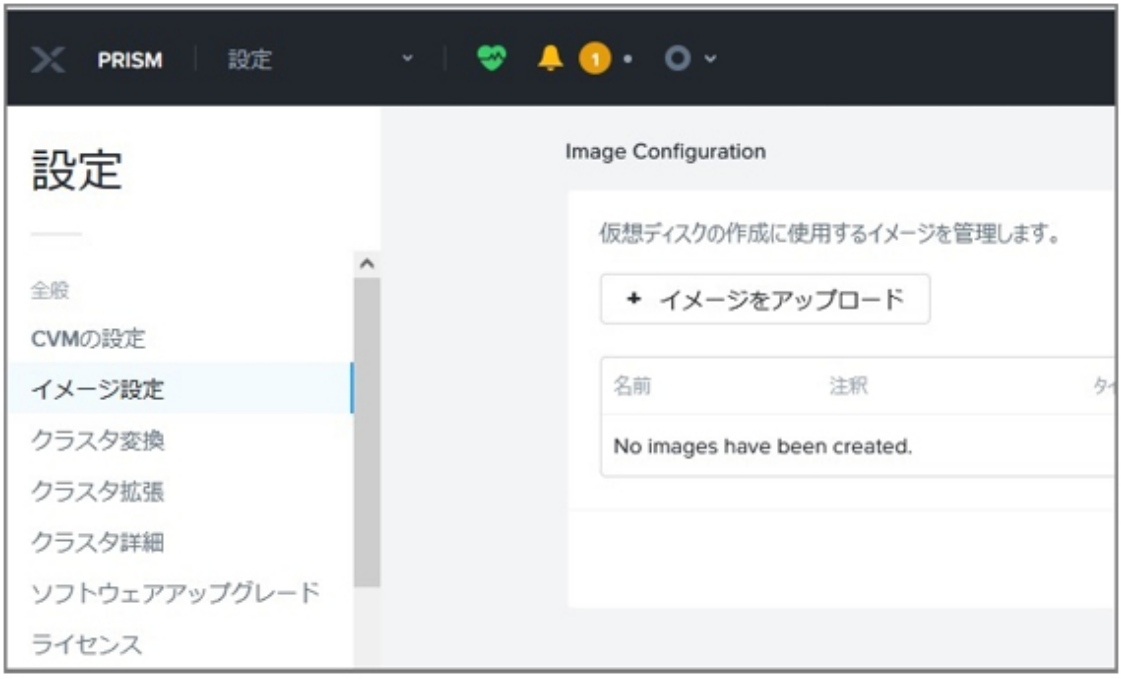
```
# ip link set dev eno1 allmulticast on
```

Nutanix AHVの場合

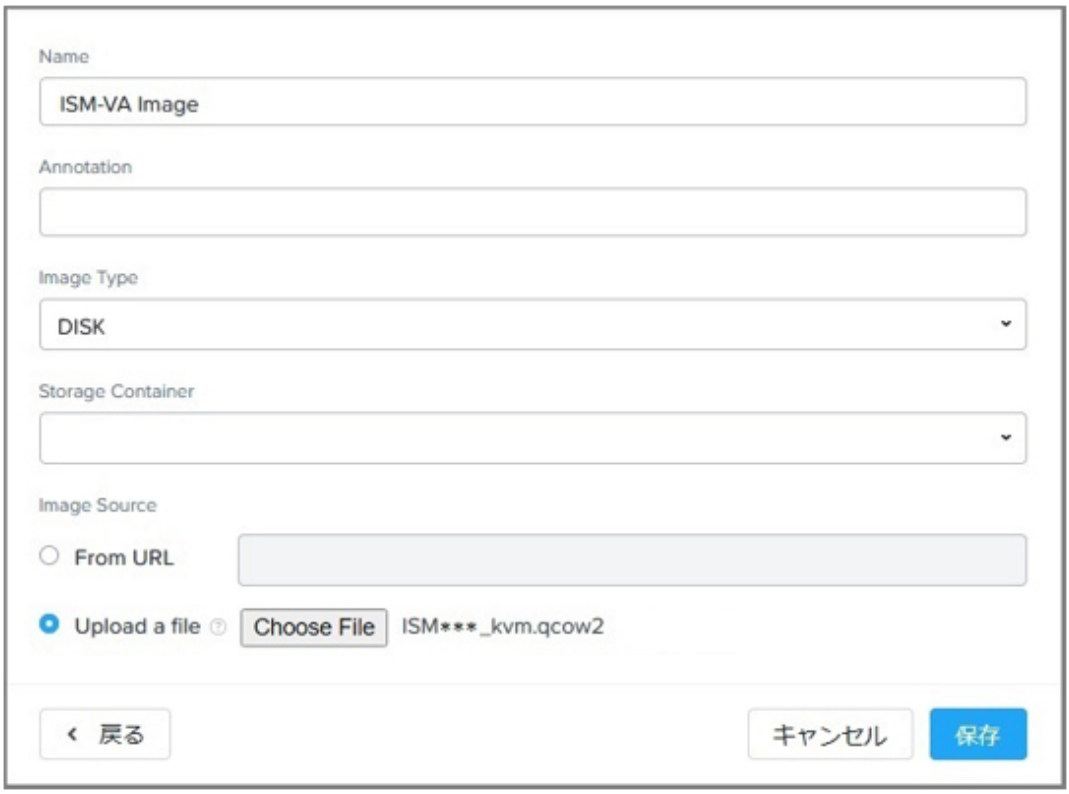
1. 管理端末上の任意のディレクトリーで、tar.gzファイルから拡張子がqcow2のファイルを展開します。

   管理端末上でtar.gz形式のアーカイブを展開できるツールが必要です。

2. NutanixのPRISMで、[設定]メニュー - [イメージ設定]を選択します。



3. [イメージをアップロード]ボタンを選択してqcow2ファイルをアップロードします。



アップロード時のパラメーターは、以下を設定してください。設定後、[保存]ボタンを選択します。

- Name：任意のイメージ名を入力（例：ISM-VA Image）
- Annotation：任意のコメントを入力

- Image Type：[DISK]を選択
- Storage Container：ISM-VAの仮想ディスクイメージを格納するコンテナを選択
- Image Source：[Upload a file]を選択し、手順1で展開したqcow2ファイルを指定

4. NutanixのPRISMで、[仮想マシン]メニューの[仮想マシンを作成]でISM-VAの仮想マシンを作成します。

以下のパラメーターを設定し、最後に[Save]ボタンを選択することによりISM-VAの仮想マシンが作成されます。

- General Configuration
  - Name：任意の仮想マシン名を入力（例：ISM + [ISMのバージョン]）
  - Description：任意のコメントを入力
  - タイムゾーン：タイムゾーンを選択
  - この仮想マシンをエージェント仮想マシンとして使用：チェックしない
- Compute Details
  - vCPU(s)：管理するノード数および使用する機能に応じてvCPU数を入力（最低 2vCPU）
  - Number Of Cores Per vCPU：1を入力
  - Memory：管理するノード数および使用する機能に応じてメモリー量を入力（最低 16GB）

  [vCPU(s)]と[Memory]に設定する値については、「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」を参照してください。

— Disks

- CD-ROM：[x]を選択して削除
- [Add New Disk]を選択してISM-VAで使用するDISKを追加

  追加時のパラメーターは、以下を指定してください。

項目	説明
タイプ	[DISK]を選択
オペレーション	[イメージサービスからクローン]を選択
バスタイプ	[SCSI]を選択
イメージ	手順3でアップロードしたISM-VAのイメージを指定
サイズ(GiB)	変更不可
インデックス	[次に使用可能]を選択

— Boot Configuration

- [Legacy BIOS]を選択
- Set Boot Priority：[DISK (scsi.0)]を選択

— Network Adapters (NIC)

[Add New NIC]を選択してISM-VAに接続するNetworkを追加してください。

追加時のパラメーターは、以下を指定してください。

項目	説明
Network Name	接続するネットワーク名を指定
ネットワークの接続状態	[接続済み]を選択

— 仮想マシンホストアフィニティ

[アフィニティを設定]を選択して、ISM-VAを動作させるノードを1ノード以上選択してください。

— Custom Script

チェックしない

3.4 ISM-VAの環境設定

ISM-VAインストール後の初期設定を行います。

3.4.1 ISM-VAの初回起動

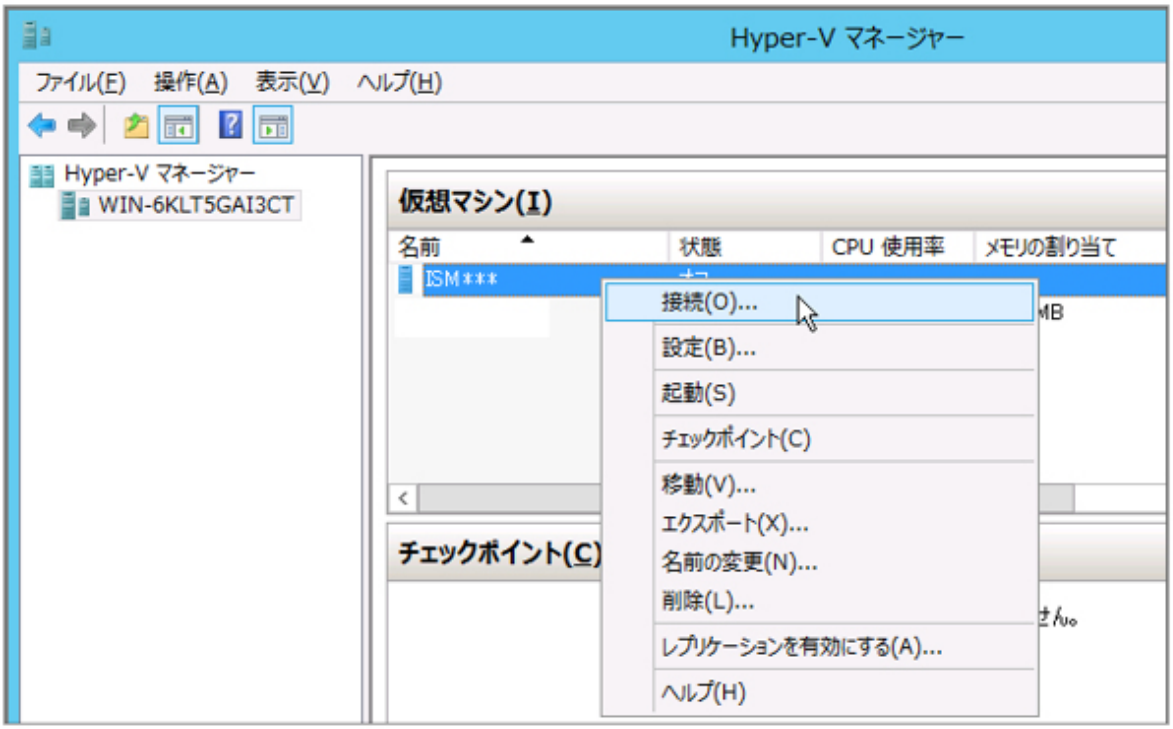
インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでの起動手順を説明します。

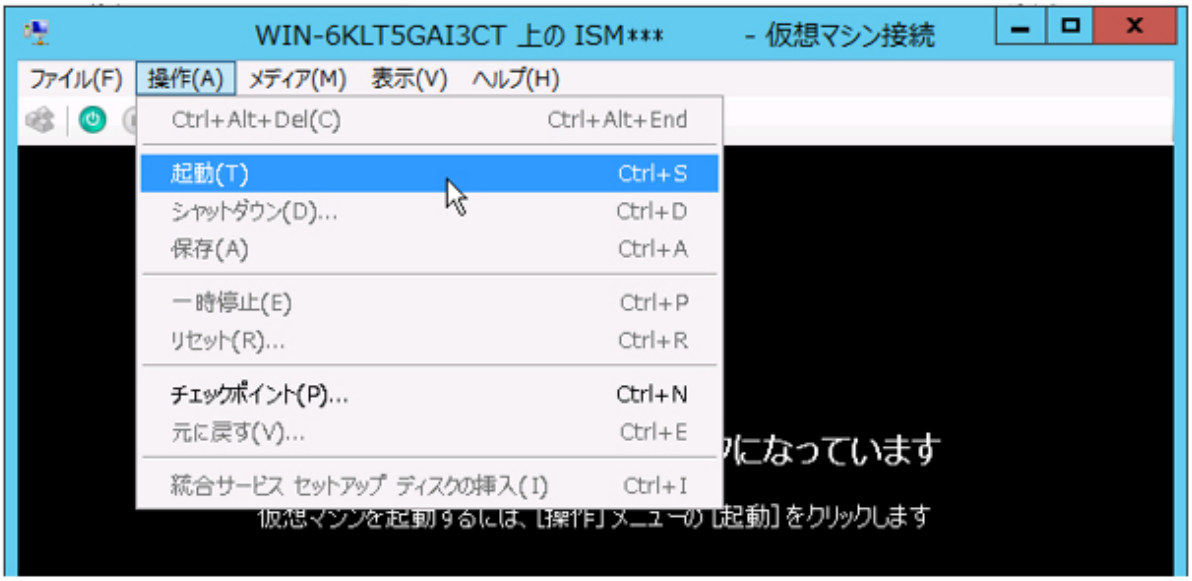
- 3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（初回）
- 3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（初回）
- 3.4.1.3 KVMで動作するISM-VAの場合（初回）

3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（初回）

1. Hyper-Vマネージャーで、インストールしたISM-VAを右クリックし、[接続]を選択します。

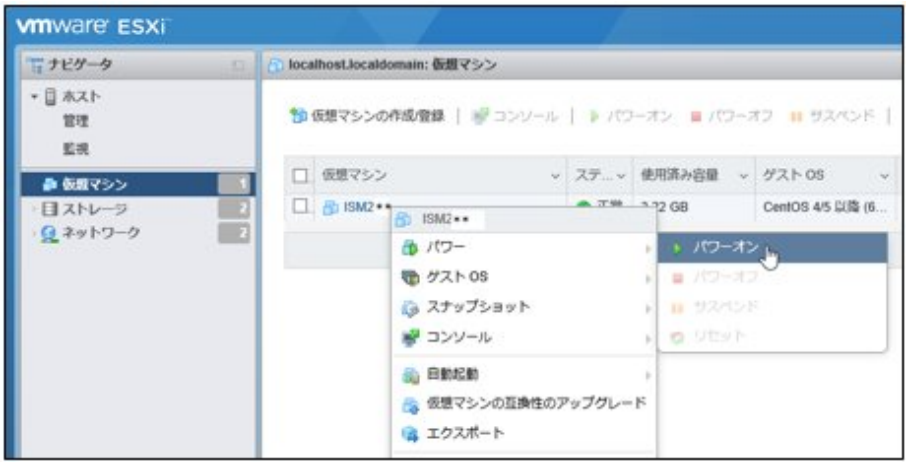


2. 「仮想マシン接続」画面の[操作]メニューから[起動]を選択し、ISM-VAを起動します。

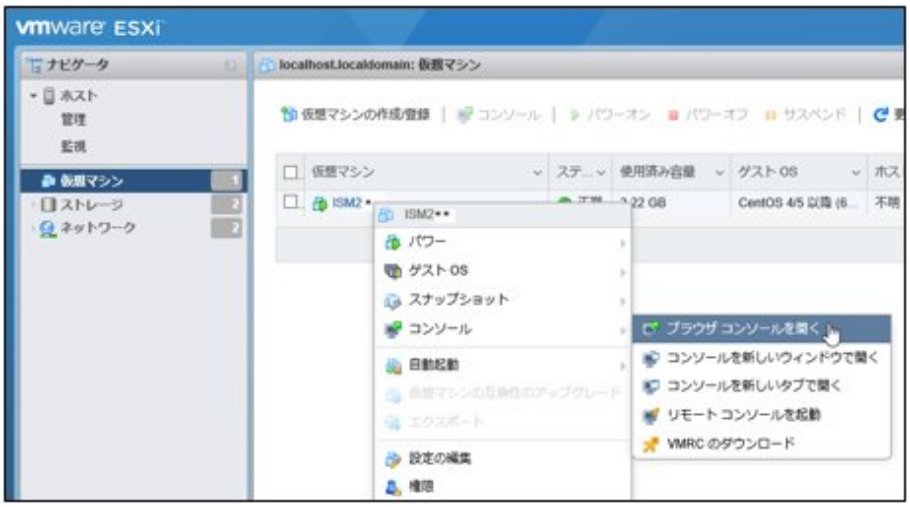


3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（初回）

1. vSphere Client（HTML5）で、インストールしたISM-VAを右クリックし、[パワーオン]を選択します。



2. インストールしたISM-VAを右クリックし、[ブラウザコンソールを開く]またはほかのコンソールを選択します。



ポイント

ISM-VA起動時に以下のメッセージが表示される場合がありますが、ISM-VAの設定はVMware ESXi 6.5/6.7上での動作に最適化されており、問題はありません。

> この仮想マシンに設定されたゲストOS（CentOS 4/5以降（64ビット））は、現在実行中のゲスト（CentOS 7（64ビット））と一致しません。ゲスト固有の最適化を許可するには、正しいゲストOSを指定する必要があります。

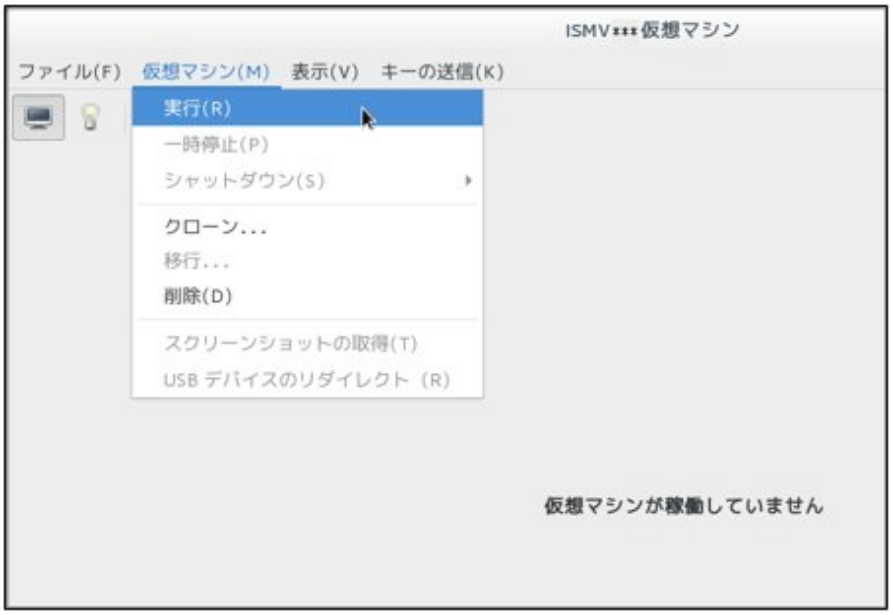
3.4.1.3 KVMで動作するISM-VAの場合（初回）

- Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合
- Nutanix AHVの場合

Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合

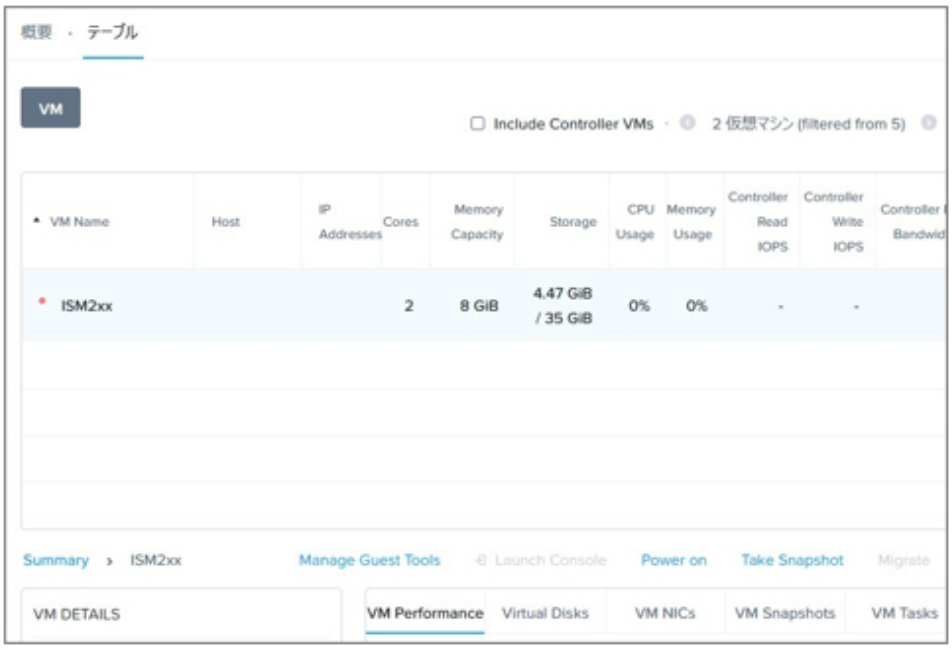
1. 仮想マシンマネージャーで、インストールしたISM-VAを右クリックし、[開く]を選択します。

2. ISM-VA仮想マシン画面の[仮想マシン]メニューから[実行]を選択し、ISM-VAを起動します。



Nutanix AHVの場合

1. NutanixのPRISMで、[仮想マシン]画面の[テーブル]表示を選択します。



2. ISM-VAの仮想マシンを選択し、[Power on]を選択します。
3. [Launch Console]を選択し、ISM-VAのコンソールを開きます。

3.4.2 ISM-VAの初期設定

ISM-VA起動後、コンソールの基本設定メニューまたはismadmコマンドを使用して、ISM-VAの基本的な設定を行います。

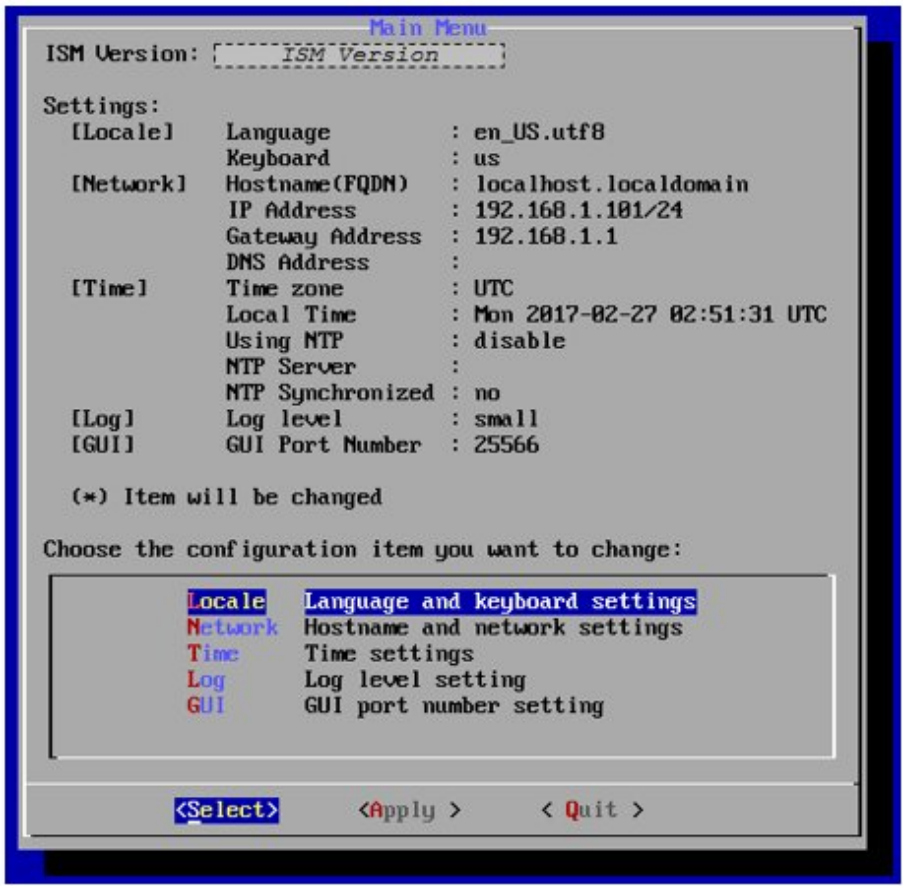
3.4.2.1 基本設定メニューを使用した初期設定

1. 管理者アカウントと初期パスワードを使用し、コンソールにログインします。
   - 管理者アカウント:administrator
   - 初期パスワード:admin
2. 以下のコマンドを実行し、基本設定メニューを起動します。

```
# ismsetup
```

ハイパーバイザーのコンソールからの初回ログイン時は自動で起動されます。

以下の画面が表示されます。



3. ISM-VAの設定を行います。

   基本設定メニューでは、以下の項目を設定できます。

   ― ロケール

   ― ネットワーク

   ― NTPサーバー

   ― ログレベル

   ― Web GUIポート番号

   基本設定メニューの詳細は、「4.2 ISM-VA基本設定メニュー」を参照してください。

   ドメイン環境の設定が必要な場合は、「3.4.2.2 ismadmコマンドを使用した初期設定」の手順5を実行してください。

3.4.2.2 ismadmコマンドを使用した初期設定

1. 管理者アカウントと初期パスワードを使用し、コンソールにログインします。

   ― 管理者アカウント:administrator

   ― 初期パスワード:admin

2. コンソールで、ネットワークを設定します。

   ― LANデバイス名を確認

```
# ismadm network device
デバイス  タイプ     状態       接続
eth0      ethernet   接続済み   eth0
lo        loopback   管理無し   --
```

ー ネットワーク／ホスト名を設定

```
# ismadm network modify ＜LANデバイス名＞ ipv4.method manual ipv4.addresses ＜IPアドレス＞/＜マスクビット＞
ipv4.gateway ＜ゲートウェイIPアドレス＞ +ipv4.dns ＜DNSサーバー＞

# ismadm system modify -hostname ＜ホスト名（FQDN）＞
```

実行例:

```
# ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway 192.168.1.1
+ipv4.dns 192.168.1.2

You need to reboot the system to enable the new settings.
Immediately reboots the system.  [y/n]:

# ismadm system modify -hostname ismva2.domainname
You need to reboot the system to enable the new settings.
Immediately reboots the system. [y/n]:
```

コマンド終了後に、システムを再起動するかどうかを確認するメッセージが表示されます。「y」を入力してシステムを再起動してください。

ネットワーク設定とホスト名設定を同時に行う場合は、あとに行った設定の際に一度のみ再起動してください。

ネットワーク／ホスト名設定後の操作は、ハイパーバイザーのコンソールでも、SSH経由のコンソールでも同じように実行できますので、操作性のよいSSH経由でのアクセスを推奨します。

ポイント

VMware vSphere Hypervisor版ISM-VAをVMware vCenter経由でインストールする場合、インストール途中でネットワーク設定を行うことにより本ネットワーク設定を省略できます。

注意

- ホスト名として使用可能な文字は英小文字、数字、ハイフン(-)、ピリオド(.)です。ハイフンおよびピリオドは、ホスト名の先頭および末尾の文字として使用できません。使用可能な文字以外を使用した場合、ISMは正常に動作しません。
- IPアドレスには、IPv4のアドレスを設定してください。
  IPv6はサポートしていません。IPv6のアドレスを設定した場合、プロファイル管理機能やファームウェア管理機能など、ISMの機能は動作しません。

3. コンソールで、System LocaleとKeymapを設定します。

現在の設定の確認方法は以下のとおりです。

```
# ismadm locale show
            System Locale: LANG=ja_JP.UTF-8
            VC Keymap: jp
            X11 Layout: jp
```

現在の設定を変更するには、以下のコマンドを使用します。

ー System Localeの設定

```
# ismadm locale set-locale LANG=＜ロケール名＞
```

実行例:

```
# ismadm locale set-locale LANG=en_US.utf8
```

ー 設定可能な＜ロケール名＞の表示

```
# ismadm locale list-locales
```

ー Keymapの設定

```
# ismadm locale set-keymap ＜キーマップ名＞
```

実行例:

```
# ismadm locale set-keymap us
```

ー 設定可能な＜キーマップ名＞の表示

```
# ismadm locale list-keymaps
```

表3.2 キーマップ一覧

言語名	キーマップ名
日本語	jp
英語	us
ドイツ語	de-nodeadkeys
中国語	cn
韓国語	kr
フィリピン語	ph

System Localeの変更は、ISM-VAの再起動後に有効になります。

4. コンソールで、日付／時間の設定をします。

現在の設定の確認方法は以下のとおりです。

```
# ismadm time show
       Local time: 木 2016-06-09 16:57:40 JST
   Universal time: 木 2016-06-09 07:57:40 UTC
         Time zone: Asia/Tokyo (JST, +0900)
       NTP enabled: no
  NTP synchronized: no
   RTC in local TZ: no
        DST active: n/a

NTP Servers:
506 Cannot talk to daemon
```

現在の設定を変更するには、以下のコマンドを使用します。

ー タイムゾーン設定

```
# ismadm time set-timezone ＜タイムゾーン＞
```

実行例:

```
# ismadm time set-timezone America/New_York
```

ー 設定可能タイムゾーン表示

```
# ismadm time list-timezones
```

ー 日時／時刻設定

```
# ismadm time set-time ＜日付＞ ＜時間＞
```

実行例:

```
# ismadm time set-time 2016-06-09 17:10:00
```

- NTP同期有効／無効設定

  有効設定

```
# ismadm time set-ntp 1
```

  無効設定

```
# ismadm time set-ntp 0
```

- NTPサーバー追加／削除

  NTPサーバー追加

```
# ismadm time add-ntpserver ＜NTPサーバー＞
```

  NTPサーバー削除

```
# ismadm time del-ntpserver ＜NTPサーバー＞
```

5. コンソールで、ドメイン環境の設定をします。

   ドメイン環境を使用しない場合には本設定は不要です。

- ドメイン設定情報を追加する

```
# ismadm kerberos add -d <Domain Name> -r <Realm> -n <Controller Name>
```

  実行例:

```
# ismadm kerberos add -d sample.local -r SAMPLE.LOCAL -n adsvr.sample.local
```

- ドメイン設定情報を表示する

```
# ismadm kerberos show
```

- ドメイン設定情報を1つ前の状態に戻す

```
# ismadm kerberos restore
```

  2つ以上前の状態に戻すことはできません。

- ドメイン設定情報を初期化する

```
# ismadm kerberos init
```

3.5 ライセンスの登録

ライセンスには、以下の2種類があります。

- サーバーライセンス

  ISMを使用するために必要なライセンスです。

- ノードライセンス

  ISMに登録可能なノード数に関するライセンスです。ISM-VA管理機能で登録したノードライセンスのライセンス数を超える数のノードは登録できません。ノードライセンスを追加登録してから、追加するノードをISMに登録してください。

ISMでは、サーバーライセンスとノードライセンスの両方の登録が必要です。ライセンスは、ISM-VAのインストール後、ISM-VA管理機能で登録します。

ライセンスの登録は、以下の2通りの方法があります。

- 3.5.1 コンソールからライセンスを登録する方法

- 3.5.2 ISMのGUIからライセンスを登録する方法

ISMのライセンスの種類についての詳細は、『入門書』の「1.2 製品体系とライセンス」を参照してください。

3.5.1 コンソールからライセンスを登録する方法

コンソールからadministratorでISM-VAにログインして行います。

1. サーバーライセンスを登録します。

```
# ismadm license set -key <ライセンスキー>
```

2. ノードライセンスを登録します。

```
# ismadm license set -key <ライセンスキー>
```

3. ライセンスの登録結果を確認します。

```
# ismadm license show
```

実行例:

```
# ismadm license show
Operation Mode : Advanced
#   [Type]  [Edition] [#Node]  [Reg.Date]  [Exp.Date]  [Status]       [Licensekey]
1   Server  Adv.            -  2024-05-29  2025-05-29  Valid          **********************==
2   Node    Adv.           10  2023-08-28  2024-08-27  Expires soon   **********************==
3   Node    Adv.           10  2023-05-30  2024-05-29  Expired        **********************==

*Reg.Date(RegistrationDate[yyyy-mm-dd])
*Exp.Date(ExpirationDate[yyyy-mm-dd])

You have an expired license.
Delete the expired license and register a new license.
```

コマンド出力結果の詳細については、「4.8 ライセンス設定」を参照してください。

4. ISM-VAを再起動します。

```
# ismadm power restart
```

3.5.2 ISMのGUIからライセンスを登録する方法

事前に「3.4.2 ISM-VAの初期設定」を行います。

1. ISM-VAを再起動します。
2. Webブラウザーで動作するGUIを起動します。
3. GUIからadministratorでログインします。

   ソフトウェア使用許諾契約書の画面が表示されます。
4. 内容を確認し、[上記内容を確認しました]にチェックを付けます。
5. [同意する]ボタンを選択します。
6. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]を選択します。
7. 画面左側のメニューから[ライセンス]を選択します。
8. [アクション]ボタンから[登録]を選択します。

   「ライセンス登録」画面が表示されます。
9. ライセンスキーを登録します。
   a. 入力フィールドに、ライセンスキーを指定します。

b. ほかに登録するライセンスキーがある場合、[追加]ボタンを選択して入力フィールドを追加します。

c. 手順a～bを繰り返し、すべてのライセンスを登録後、[適用]ボタンを選択します。

10. [アクション]ボタンから[ISM-VA再起動]を選択して、ISM-VAを再起動します。

ポイント

- ライセンスを追加登録する場合は、上記の手順6～手順9を実施します。
- 登録したライセンスを削除する場合は、対象のライセンスを選択し、[アクション]ボタンから[削除]を選択します。

3.6 ユーザーの登録

「3.2.4 ユーザーの設計」に基づいて、ISMの運用に必要なユーザーを登録します。

詳細な手順については、『操作手順書』の「2.3 ISMのユーザーを設定する」を参照してください。

ポイント

ISMの初期状態では、[Administratorグループ]の[Administratorロール]のユーザー（ISM管理者）だけが登録されています。

ユーザー名	パスワード	ユーザーグループ名	ユーザーロール	用途
administrator	admin[注]	Administrator	Administrator	ISM全体管理

[注]：運用前にパスワードを変更してください。

ユーザーの登録は、以下の手順で行います。

1. ISM管理者でISMにログインします。
2. ノードグループを作成します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ノードグループ]を選択します。
   c. [アクション]ボタンから[ノードグループ追加]を選択します。
3. ノードグループに所属するノードを登録します（ノードはあとからでも登録できます）。
   a. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。
   b. 画面左側のノードグループリストからノードグループを選択します。
   c. 画面右側でノードを選択し、[ノードアクション]ボタンから[ノードグループへ割り当て]を選択します。
   d. 「ノードグループへの割り当て」画面で、[選択]ボタンを選択します。
   e. 「ノードグループ選択」画面で[＜新たに割り当てるノードグループ＞]を選択し、[選択]ボタンを選択します。
   f. 「ノードグループへの割り当て」画面で[適用]ボタンを選択します。
4. ユーザーグループを作成します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ユーザーグループ]を選択します。
   c. [アクション]ボタンから[追加]を選択します。
5. ユーザーグループに所属するユーザーを登録します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ユーザー]を選択します。

c. [アクション]ボタンから[追加]を選択します。

3.7 仮想ディスクの割当て

仮想ディスクは、ISM-VAのディスク容量を増設するための資源です。ログやリポジトリ、バックアップの格納には大容量のディスク資源が必要になります。また、それらの運用方法や管理対象ノードの規模などに応じて容量が異なります。大容量の資源を仮想ディスクに割り当てることで、ISM-VAのディスク容量や負荷の影響を回避します。仮想ディスクには必要十分な容量を確保しておくことで、ログやリポジトリ、バックアップの運用を円滑に行えます。

ISM-VA全体またはユーザーグループに対して、仮想ディスクの割当てができます。

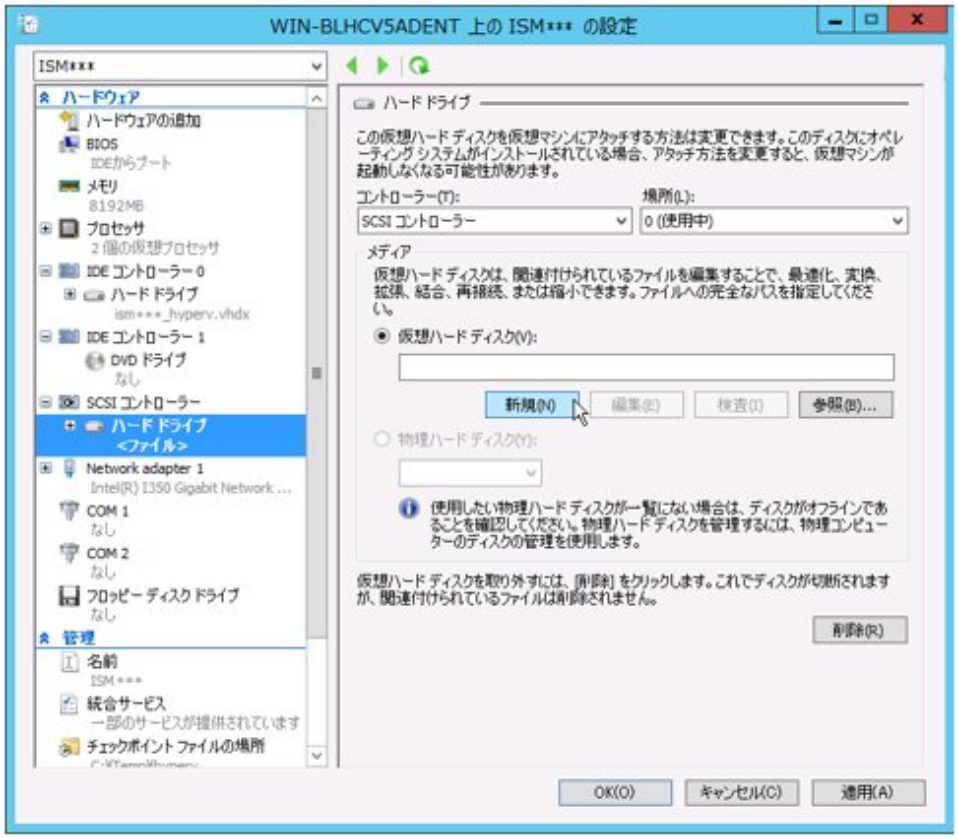
3.7.1 ISM-VA全体に対する仮想ディスク割当て

Administratorユーザーグループを例として、仮想ディスク割当ての手順を示します。

1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA(仮想マシン)に接続します。

   ー Microsoft Windows Server Hyper-Vの場合

   仮想ディスクは、SCSIコントローラーの配下に作成してください。

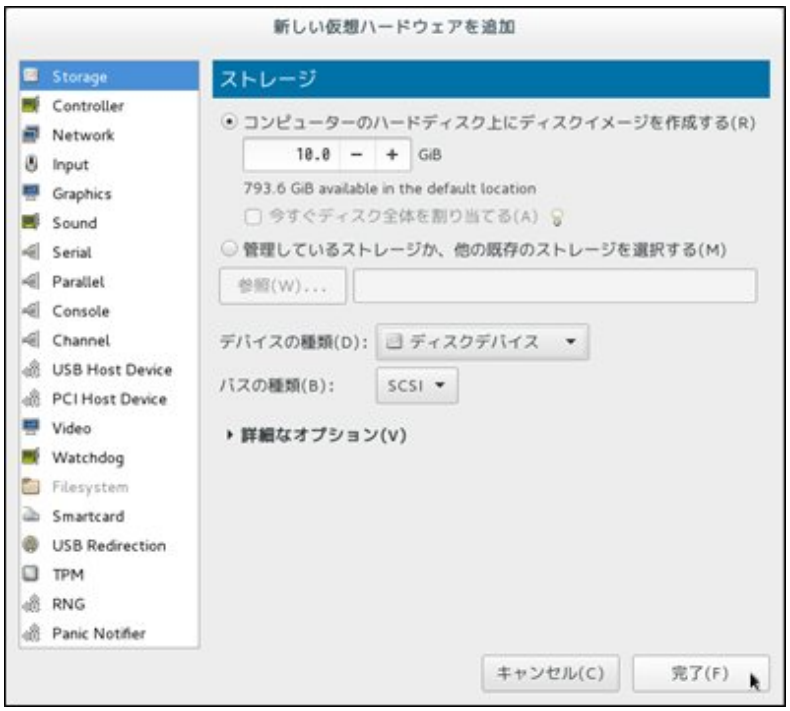


－ VMware vSphere Hypervisor 6.5以降の場合

作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

－ KVM（Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Server）の場合

バスの種類は、SCSIを選択してください。



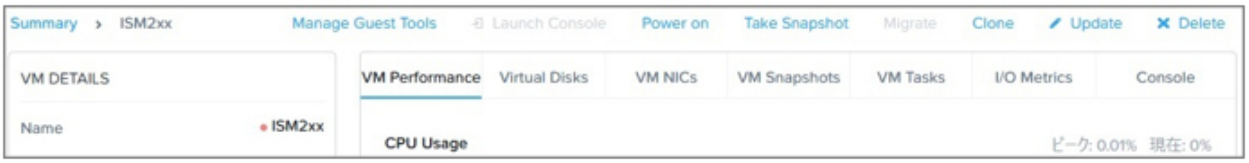
－ KVM（Red Hat Enterprise Linux 10）の場合

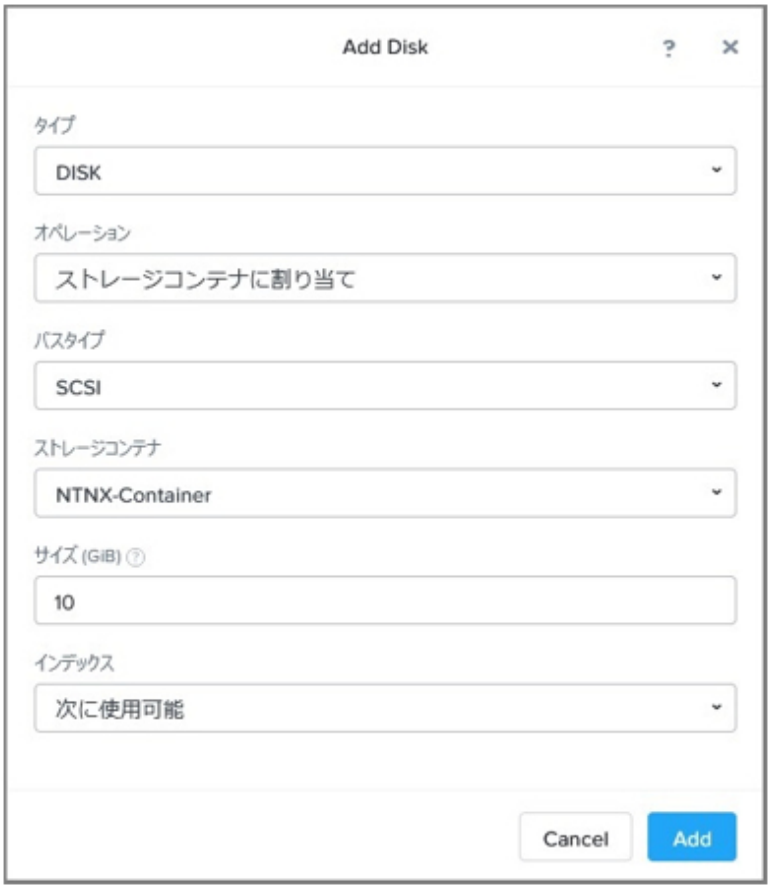
追加ディスクの格納先であるプールを指定し、フォーマットはqcow2、バスはscsiをそれぞれ選択してください。

プールは事前に作成してあるものを選択する必要があります。

ー Nutanix AHVの場合

仮想マシンの[Update]を選択し、[Add New Disk]から仮想ディスクを追加してください。





バスタイプはSCSIを選択してください。

2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。

3. 仮想ディスク割当てのため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

4. 手順1で追加した仮想ディスクが認識されているか確認します。

例:

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
/dev/sdb                                       (Free 10.7 GB)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
```

この例では、/dev/sdbが追加され未使用領域と認識されています。

5. 追加した仮想ディスクをISM-VA全体のシステムボリュームに割り当てます。

```
# ismadm volume sysvol-extend -disk /dev/sdb
```

6. 仮想ディスク設定を確認します。

新規追加したボリューム(/dev/sdb)が、システムボリューム用(centos)として設定されていることを確認してください。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    26G  2.5G   23G   10% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
tmpfs                     380M     0  380M    0% /run/user/0

  PV         VG       Fmt  Attr PSize  PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  centos   lvm2 a--  10.00g    0
```

7. ISM-VAを再起動します。

```
# ismadm power restart
```

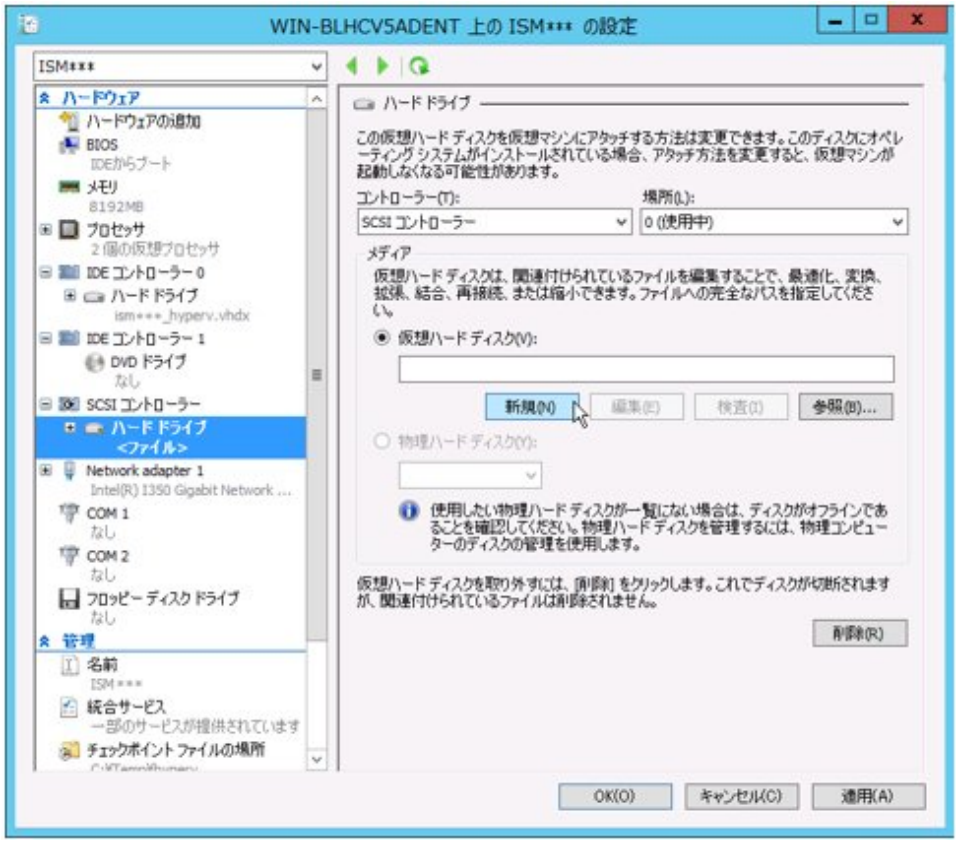
3.7.2 ユーザーグループに対する仮想ディスク割当て

Administratorユーザーグループを例として、仮想ディスク割当ての手順を示します。

1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA（仮想マシン）に接続します。

   － Microsoft Windows Server Hyper-Vの場合

   仮想ディスクは、SCSIコントローラーの配下に作成してください。

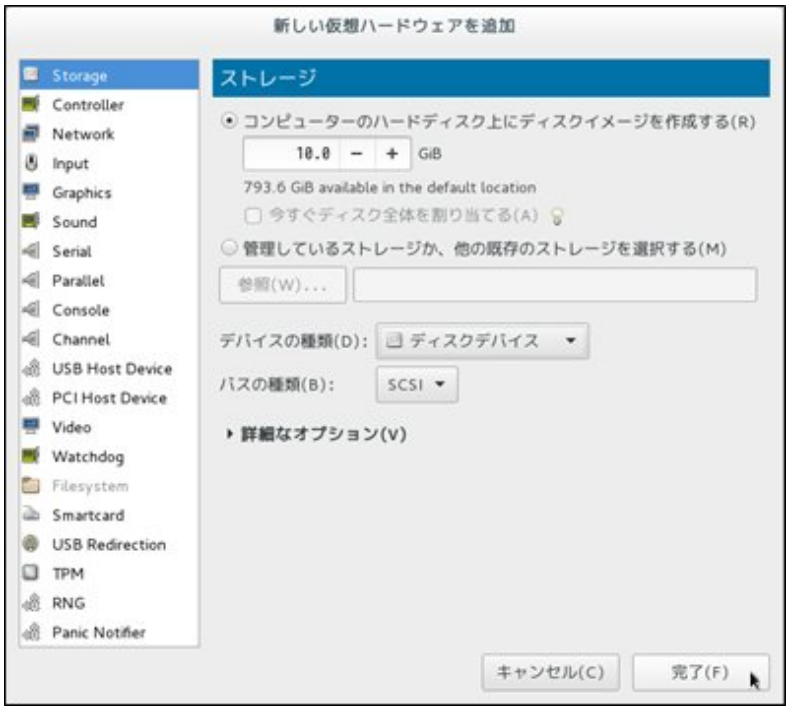


   － VMware vSphere Hypervisor 6.5以降の場合

   作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

－ KVM（Red Hat Enterprise Linux 7/8/9またはSUSE Linux Enterprise Server）の場合

バスの種類は、SCSIを選択してください。



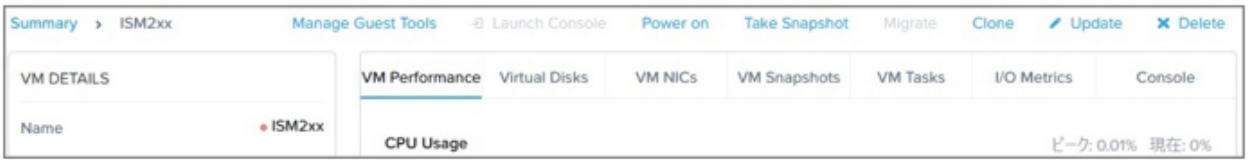
－ KVM（Red Hat Enterprise Linux 10）の場合

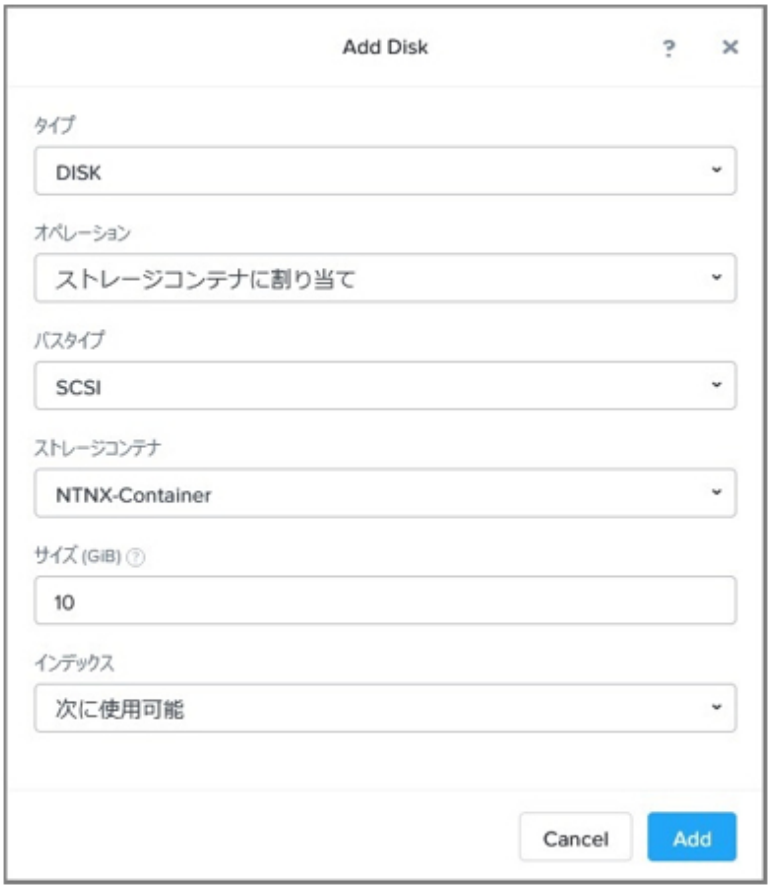
追加ディスクの格納先であるプールを指定し、フォーマットはqcow2、バスはscsiをそれぞれ選択してください。

プールは事前に作成してあるものを選択する必要があります。

－ Nutanix AHVの場合

仮想マシンの[Update]を選択し、[Add New Disk]から仮想ディスクを追加してください。





バスタイプはSCSIを選択してください。

2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
3. 仮想ディスク割当てのため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

4. 手順1で追加した仮想ディスクが認識されているか確認します。

実行例:

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
/dev/sdb                                       (Free 8589 MB)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g    0
```

この例では、/dev/sdbが追加され未使用領域と認識されています。

5. Administratorグループ用の追加ボリューム名を任意の名称(例:「adminvol」など)で作成し、新規追加した仮想ディスク(/dev/sdb)に関連付けます。

```
# ismadm volume add -vol adminvol -disk /dev/sdb
Logical volume "/dev/mapper/adminvol-lv" created.
```

6. 手順5で作成した追加ボリューム(以下例では「adminvol」)を、実際にAdministratorグループ用として使用できるように有効化します。

```
# ismadm volume mount -vol adminvol -gdir /Administrator
```

7. 仮想ディスク設定を確認します。

   新規追加したボリューム(/dev/sdb)が、Administratorグループ用として設定されていることを確認してください。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/1001
tmpfs                     380M     0  380M    0% /run/user/0
/dev/mapper/adminvol-lv   8.0G   39M  8.0G    1% 'RepositoryRoot'/Administrator

  PV         VG       Fmt  Attr PSize  PFree
  /dev/sda2  centos   lvm2 a--  19.51g    0
  /dev/sdb1  adminvol lvm2 a--   8.00g    0
```

8. ISM-VAを再起動します。

```
# ismadm power restart
```

3.8 仮想リソース／クラスタを管理するための事前設定

仮想リソース管理機能、クラスタ管理機能の運用管理のため、事前に必要となる設定について説明します。

3.8.1 vSANの事前設定

vSANホスト間のネットワークの接続が切れた場合にvSANデータストアの異常を検出できるようにするため、vSANアラーム定義が必要です。
また、vSANを構成するディスクの遅延監視を行うためにvSANモニタリング機能の有効化が必要です。

3.8.1.1 vSANアラーム定義の追加方法

vSANのアラーム定義の追加方法について説明します。

なお、vCenter Server Appliance 6.5の場合は「vSphere Client (HTML5) - 一部の機能」を選択してログインしてください。

1. vSphere Client画面を表示し、メニューから[ストレージ]を選択して、作成したvSANデータストアを選択します。

   以下はvSANデータストア名が「vsan_ds」の場合です。

   表示された画面右側の[設定]タブから[詳細]-[アラーム定義]を選択します。

   表示された画面で「アラーム名」を確認します。「アラーム名」に「Breaking of a network between the host」が存在する場合は、以降の手順は不要です。

表示された画面の[追加]を選択します。

2. ウィザード画面が表示されるので、「アラーム名」と「説明」に下表のように入力して、[次へ]ボタンを選択します。

項目	入力内容
アラーム名	ホスト間ネットワークの断線
説明	ホスト間のネットワークが断線した場合のアラーム

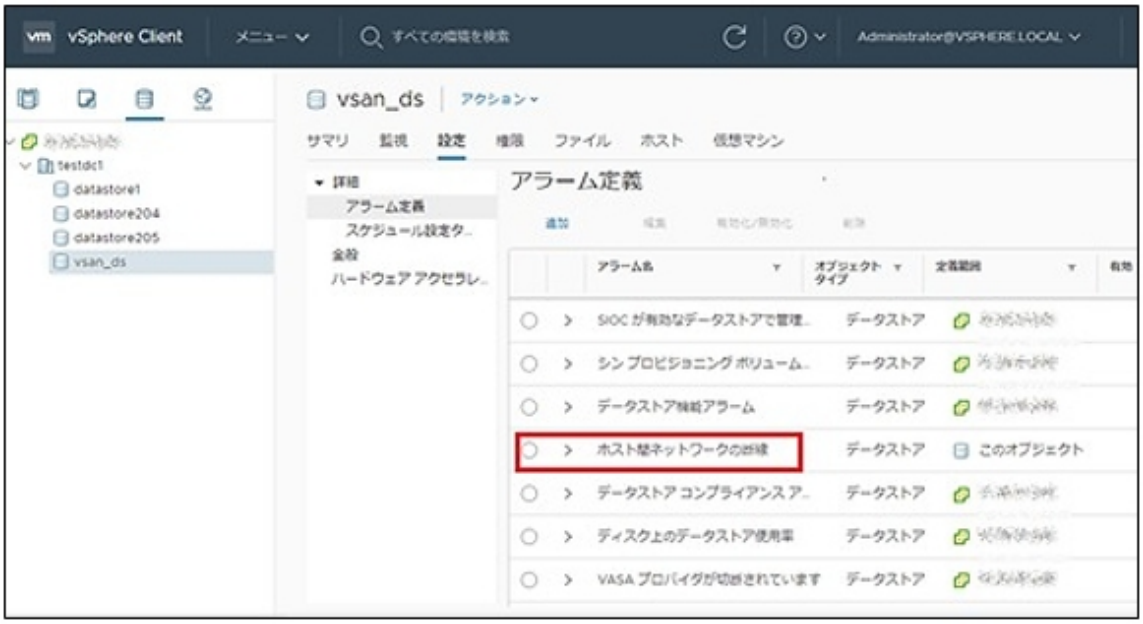
3. 以下の画面で各項目を下表のように設定して、[次へ]ボタンを選択します。

項目	設定値
トリガー	すべてのホストに対するデータストアの状態
演算子	次の値と等しい
オプション	切断状態
アラームの重要度	重大として表示

4. ルールのリセット1は設定不要です。[次へ]ボタンを選択します。

5. 以下の画面で[作成]ボタンを選択します。

完了すると、アラーム定義に新しい定義が追加されます。



3.8.1.2 vSANモニタリング機能の有効化手順

vSANのモニタリング機能を有効化する方法について説明します。VMware vCenter Server Applianceのバージョンに応じて操作が異なります。該当するバージョンの参照先をご覧ください。

- vCenter Server Appliance 6.5（Flash）以前の場合
- vCenter Server Appliance 6.7（HTML5）以降の場合

vCenter Server Appliance 6.5（Flash）以前の場合

1. vSphere Web Client画面を表示し、メニューから[ホストおよびクラスタ]を選択して、作成したクラスタを選択します。
2. 表示された画面右側の[設定]タブから[vSAN]-[健全性とパフォーマンス]を選択します。

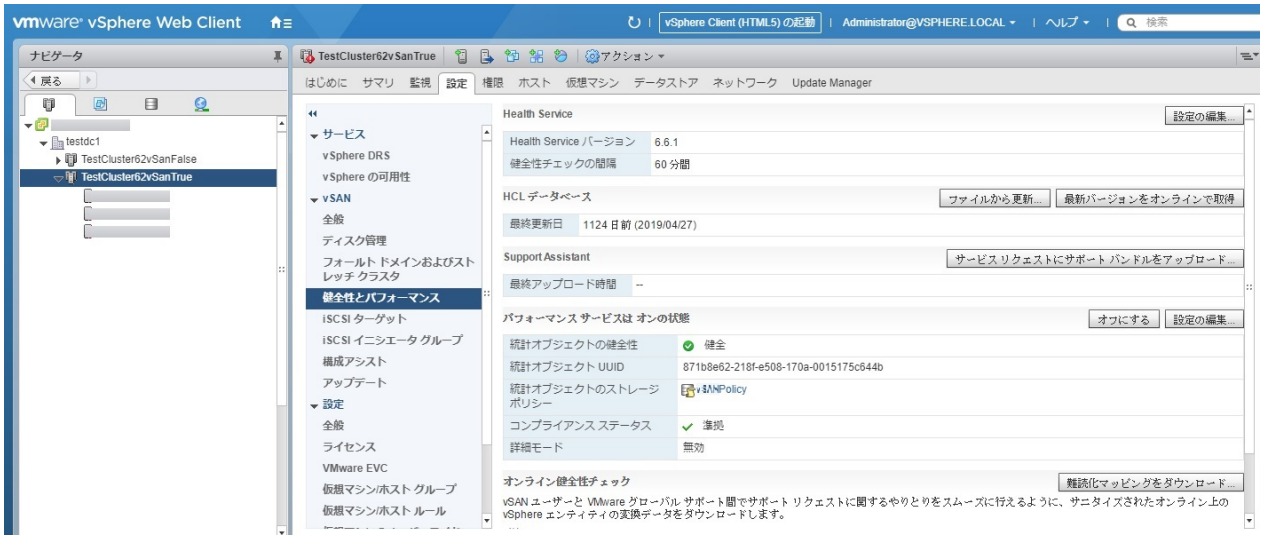
   表示された画面で「パフォーマンス サービス」を確認します。「パフォーマンスサービスはオフの状態」である場合は、「オン」にするために以下の操作をします。

ステータスが「オン」である場合は、以降の操作は不要です。

ステータス表示の右側にある[編集]を選択します。

3. 「vSAN パフォーマンス サービスをオンにする」にチェックを入れ、ストレージポリシーを選択して[OK]ボタンを選択します。

完了すると、パフォーマンス サービスが「パフォーマンスサービスはオンの状態」に表示されます。



4. vSANを構成するクラスタすべてに、同様の手順を適用します。

vCenter Server Appliance 6.7（HTML5）以降の場合

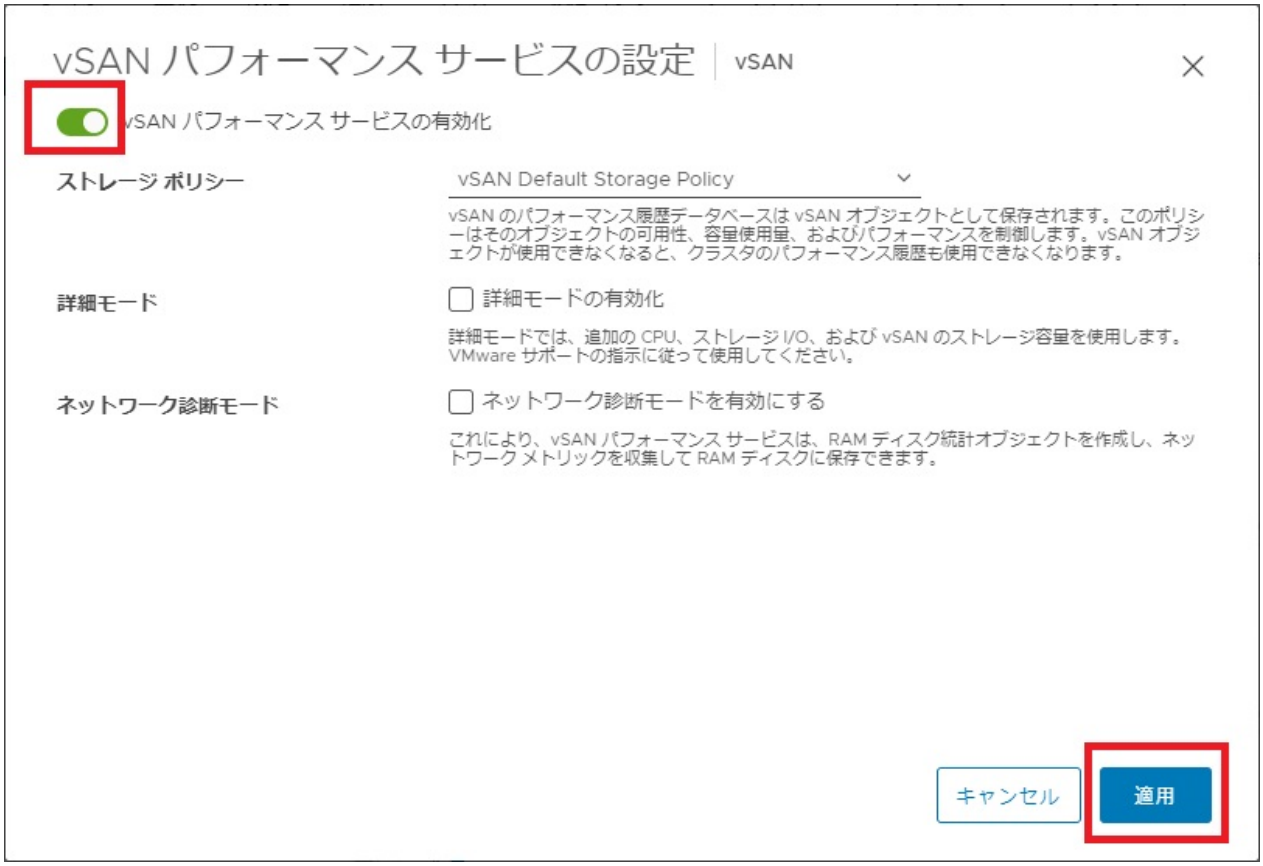
1. vSphere Client画面を表示し、メニューから[ホストおよびクラスタ]を選択して、作成したクラスタを選択します。
2. 表示された画面右側の[設定]タブから[vSAN]-[サービス]を選択します。

   表示された画面で「パフォーマンス サービス」を確認します。「無効」である場合は、「有効」にするために以下の操作をします。

   ステータスが「有効」である場合は、以降の操作は不要です。

   パフォーマンスサービスにある[有効化]を選択します。

3. 「vSAN パフォーマンス サービスの有効化」をクリックして有効化し、[適用]ボタンを選択します。



完了すると、パフォーマンス サービスが「有効」と表示されます。

4. vSANを構成するクラスタすべてに同様の手順を適用します。

3.8.2 vCenter Serverの統計収集間隔の事前設定

リソース変動予測を行う場合、vCenter Serverにて統計情報の有効化が必要です。統計情報を有効化する方法について説明します。

1. vSphere Client画面を表示し、vCenter Serverを選択します。
2. 表示された画面右側の[設定]タブから[全般]-[統計情報]を選択します。

   表示された画面で有効が「はい」であることを確認します。

   「はい」でない場合は、次の操作をします。

   有効が「はい」である場合は、以降の操作は不要です。
3. vCenter Server 設定の[編集]を選択します。

4. [有効]を選択してチェックを付け、[保存]ボタンを選択します。

5. 統計情報の有効が「はい」と表示されます。

   統計情報の[間隔]の「1日」は必ず有効にしてください。

3.8.3 ISMへの事前設定

ISMへ必要な設定を実施します。仮想化管理ソフトウェアの登録、およびOS情報の登録を行います。

仮想化管理ソフトウェアの登録

仮想化管理ソフトウェアをISMに登録します。

詳細については、「2.14.6 仮想化管理ソフトウェア管理機能」を参照してください。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 登録に必要な情報を入力します。

   情報の内容については、ISMのオンラインヘルプを参照してください。

   注意

   ー タイプは以下を指定します。

   - vSANの場合

     お使いのバージョンのVMware vCenter Serverを指定してください。

   - S2D／MAS HCIの場合

     お使いのWindows Serverバージョンの Microsoft Failover Clusterを指定してください。

   ー Microsoft Failover Clusterを指定した場合、ドメイン名を必ず大文字で入力してください。

4. [登録]ボタンを選択します。

   仮想化管理ソフトウェアリスト画面に登録した仮想化管理ソフトウェアが表示されます。

OS情報の登録

ノードのOS情報を登録します。

OS情報には、OSの種類やIPアドレス、OSに接続するためのアカウント情報などが含まれます。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。

   「ノードリスト」画面が表示されます。

2. 対象ノードを選択し、[OS]タブを選択します。
3. [OSアクション]ボタンから[OS情報編集]を選択します。
4. 登録に必要な情報を入力します。

   ー OSタイプ、OSバージョンは以下を指定します。

   - vSANの場合

     OSタイプ：VMware ESXi

     OSバージョン：お使いのVMware ESXiのバージョン

   - S2Dの場合

     OSタイプ：Windows Server

     OSバージョン：お使いのWindows Serverのバージョン

   ー OS IPアドレスを入力します。

   ー アカウントには、ローカルユーザーアカウントを入力します。

5. 情報の入力後、[適用]ボタンを選択します。

   「基本情報」、「OSからの取得情報」が表示されることを確認します。

注意

ドメイン名は設定せず、空欄にしてください。

ISMとOS間の操作はローカルユーザーアカウントを使用するため、ドメイン名の設定は不要です。

第4章 基本操作

この章では、ISMの操作を説明します。

4.1 ISMの起動と終了

保守などのため、ISMの起動／終了操作が必要になることがあります。

4.1.1 ISM-VAの起動

インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでの起動手順を説明します。

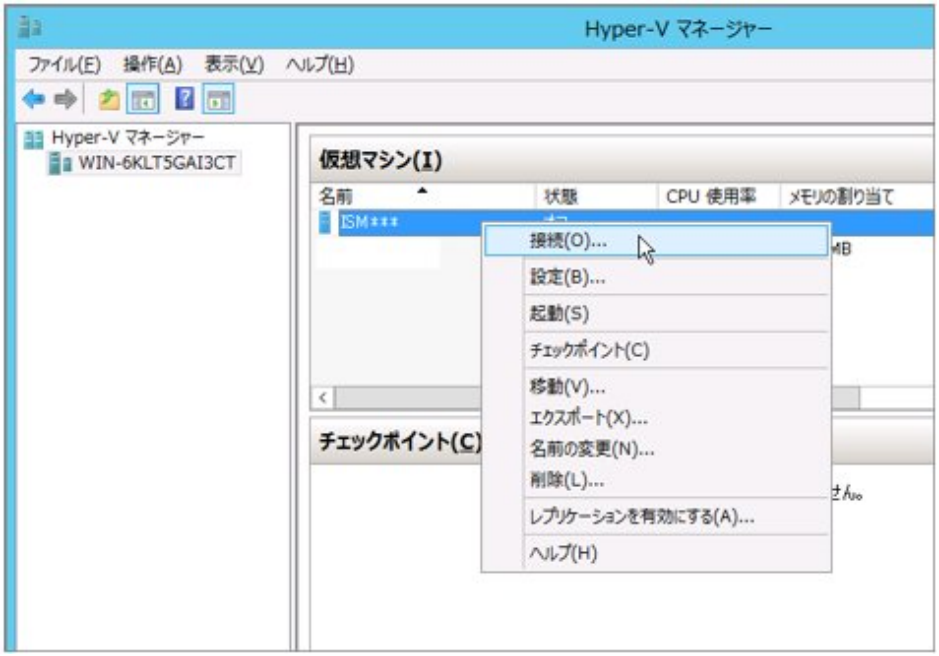
- 4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（導入後）
- 4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（導入後）
- 4.1.1.3 KVMで動作するISM-VAの場合（導入後）

ポイント

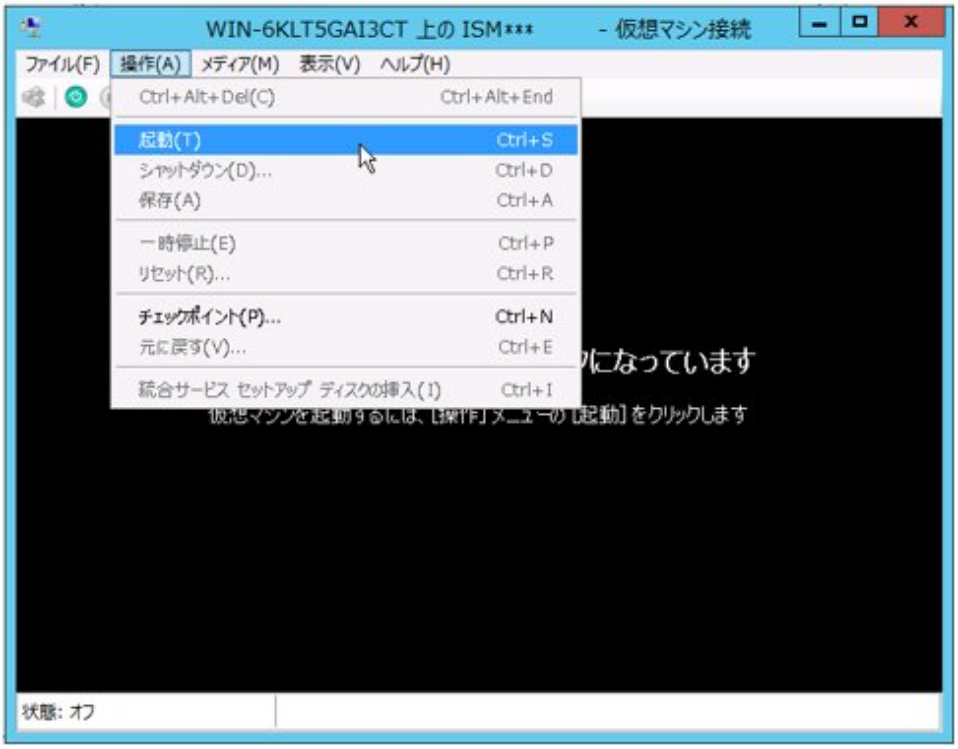
ISM-VAの起動には数分かかることがあります。しばらく待ってからGUIにログインできることを確認してください。

4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合（導入後）

1. Hyper-Vマネージャーで、インストールしたISM-VAを右クリックし、[接続]を選択します。

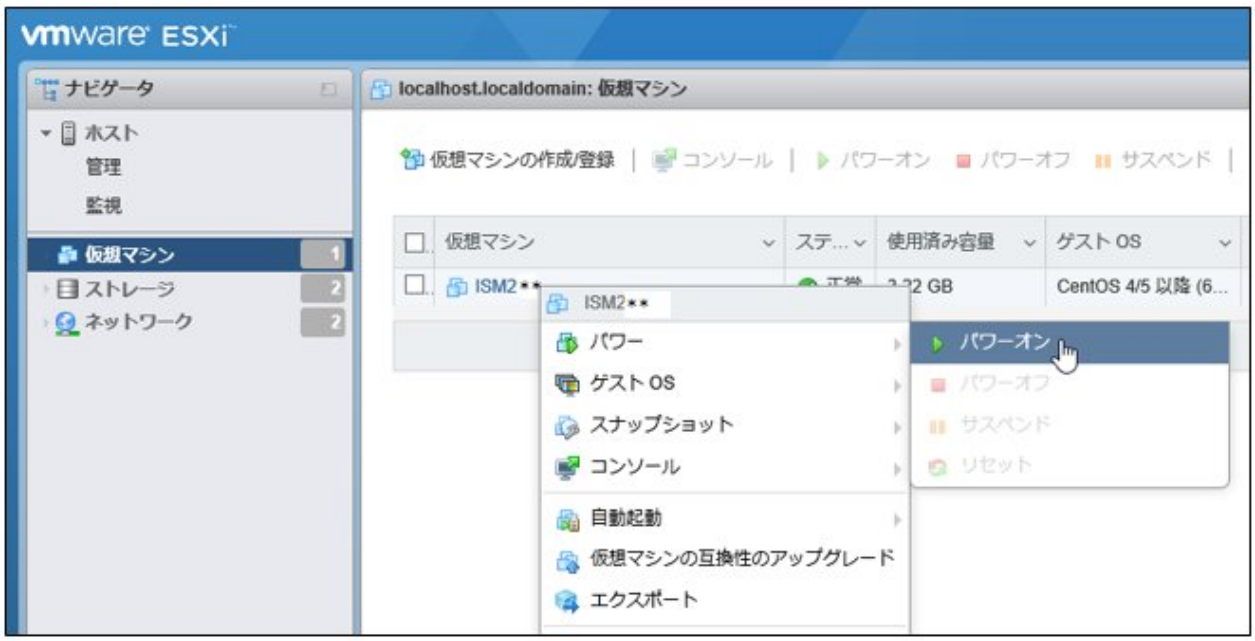


2. 「仮想マシン接続」画面の[操作]メニューから[起動]を選択し、ISM-VAを起動します。

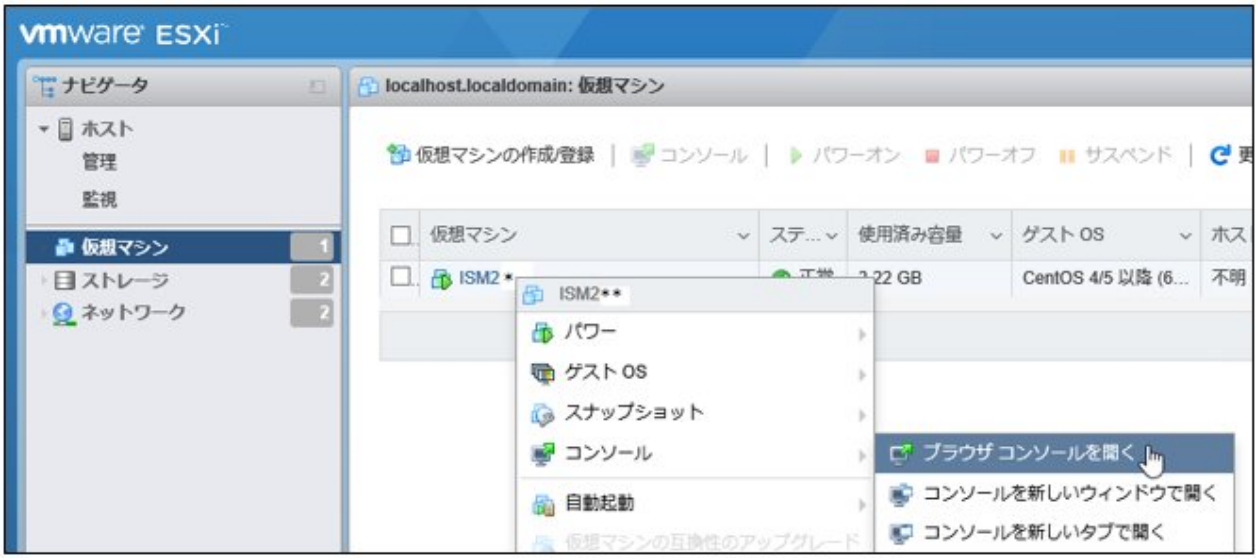


4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合（導入後）

1. vSphere Client（HTML5）で、インストールしたISM-VAを右クリックし、[パワーオン]を選択します。



2. インストールしたISM-VAを右クリックし、[ブラウザコンソールを開く]またはほかのコンソールを選択します。



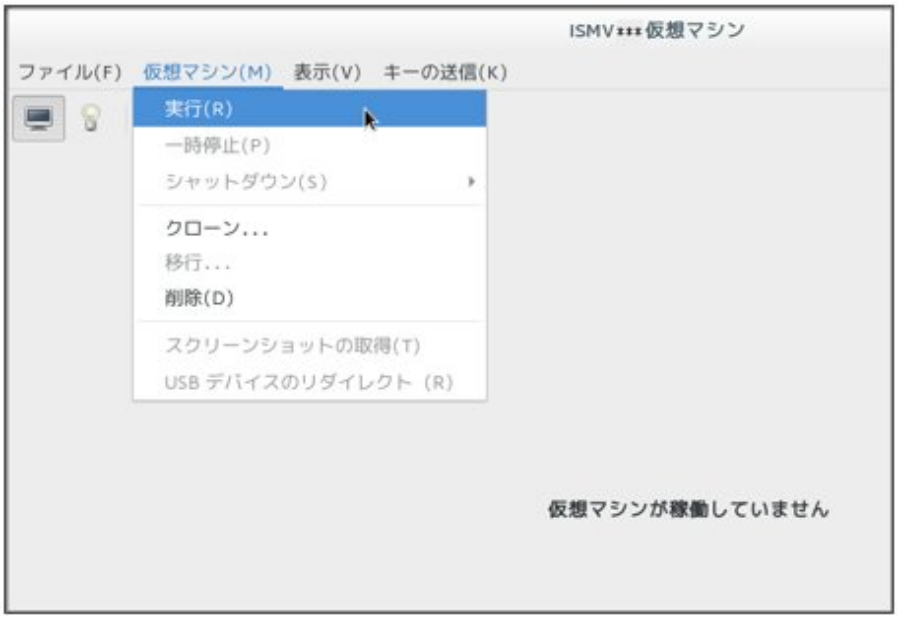
4.1.1.3 KVMで動作するISM-VAの場合（導入後）

- Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合
- Nutanix AHVの場合

Red Hat Enterprise LinuxまたはSUSE Linux Enterprise Serverの場合

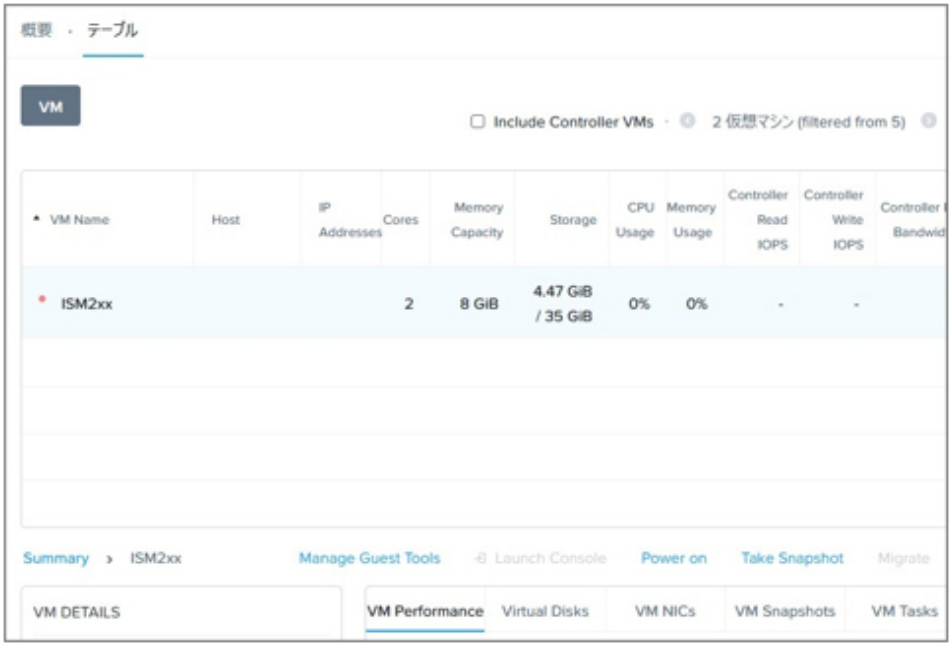
1. 仮想マシンマネージャーで、インストールしたISM-VAを右クリックし、[開く]を選択します。

2. 「ISM-VA仮想マシン」画面の[仮想マシン]メニューから[実行]を選択し、ISM-VAを起動します。



Nutanix AHVの場合

1. NutanixのPRISMで、[仮想マシン]画面の[テーブル]表示を選択します。



2. ISM-VAの仮想マシンを選択し、[Power on]を選択します。

4.1.2 ISM-VAの終了

ISM-VAのコマンドを使用して、ISM-VAを終了します。

1. GUIを起動します。

   GUIには、ISM管理者でログインしてください。

2. 運用を終了します。

   「タスク」画面を参照して、タスクが終了していることを確認します。

a. ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択します。

b. 「タスク」画面で、ステータスが「完了」または「キャンセル完了」になっていることを確認します。

c. 「完了」または「キャンセル完了」でないタスクは、終了を待ち合わせるか、タスクをキャンセルします。

タスクをキャンセルする場合、実行中のタスクを選択して、[アクション]ボタンから[キャンセル]を選択します。実行中のすべてのタスクに対してキャンセルします。

タスクタイプが「Updating firmware」(ファームウェアのアップデート処理)のタスクは、キャンセルしても処理を中止できない場合があります。この場合、処理の終了を待ち合わせます。

注意

タスクが終了していない状態でISM-VAを終了すると、タスクの処理が異常な状態で中断され、以降の運用で正しく動作しないことがあります。

必ずタスクの終了を待ち合わせるか、タスクをキャンセルして処理が終了してからISM-VAを終了してください。

3. ISMのGUIをログアウトして、GUIを終了します。
4. コンソールを起動し、ISM管理者のユーザーでログインします。
5. ISM-VAの終了コマンドを実行し、ISM-VAを終了します。

```
# ismadm power stop
```

注意

ISM-VAを終了(ismadm power stop コマンド実行)せずに、ISM-VAの仮想マシンを直接シャットダウンしないでください。

4.1.3 ISM-VAの再起動

ISM-VAの再起動は、主にISM-VAへの修正パッチ適用時に行います。

1. ISMのタスクとGUIを終了し、コンソールにログインします。

   ISMのタスクとGUIの終了方法については、「4.1.2 ISM-VAの終了」を参照してください。

2. 以下のコマンドを実行し、ISM-VAを再起動します。

```
# ismadm power restart
```

4.1.4 ISMのサービス起動と停止

ISM-VAを起動すると、ISMのサービスは自動的に起動されます。

ISMのサービス起動／停止は、コンソールからadministratorでISM-VAにログインし、ISM-VAのコマンドを使用して行います。

ISMのサービス起動

1. 以下のコマンドを実行し、ISMのサービスを起動します。

```
# ismadm service start ism
```

ISMのサービス停止

1. ISMのタスクとGUIを終了します。

   ISMのタスクとGUIの終了方法については、「4.1.2 ISM-VAの終了」を参照してください。

2. 以下のコマンドを実行し、ISMのサービスを停止します。

```
# ismadm service stop ism
```

4.2 ISM-VA基本設定メニュー

ISM-VAの基本的な設定を、メニュー選択および項目選択方式で簡単に実行できます。

ISM-VA基本設定メニューで設定できる項目を以下に示します。

項目		設定／表示内容	対応するismadmコマンド
Locale	Language	内部言語設定	ismadm locale set-locale
	Keyboard	キーボードキーマップ設定	ismadm locale set-keymap
Network	Hostname(FQDN)	ホスト名設定	ismadm network modify
	IP Address	IPアドレス設定	
	Gateway Address	ゲートウェイ設定	
	DNS Address	DNSサーバー設定	
Time	Timezone	タイムゾーン設定	ismadm time set-timezone
	Local Time	ローカルタイム表示	ismadm time show
	Using NTP	NTP有効／無効設定	ismadm set-ntp
	NTP Server	NTPサーバー設定	ismadm add-ntpserver ismadm del-ntpserver
	NTP Synchronized	NTP同期表示	ismadm time show
Log	Log level	障害調査ログレベル設定	ismadm system change-log-level
GUI	GUI port number	Web GUI接続ポート設定	ismadm service modify -port

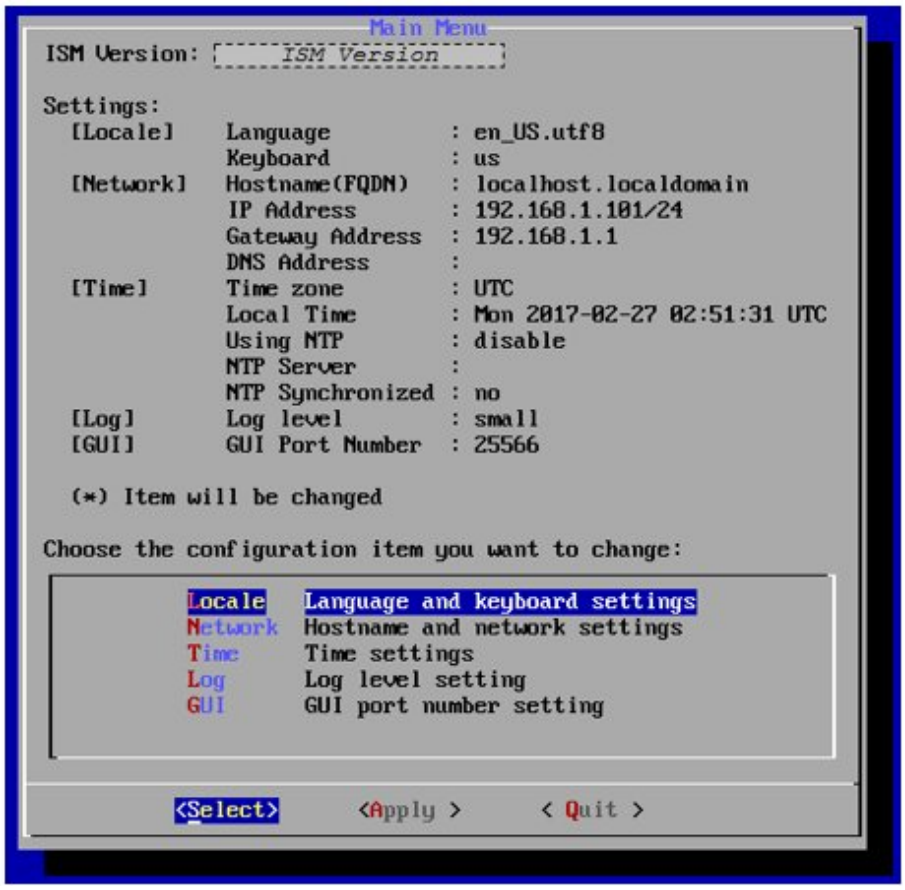
ISM-VAのMTUサイズ変更は、「4.9 ネットワーク設定」の「ISM-VAのMTUサイズ変更」を参照してください。

ISM-VA基本設定メニューの実行方法を以下に示します。

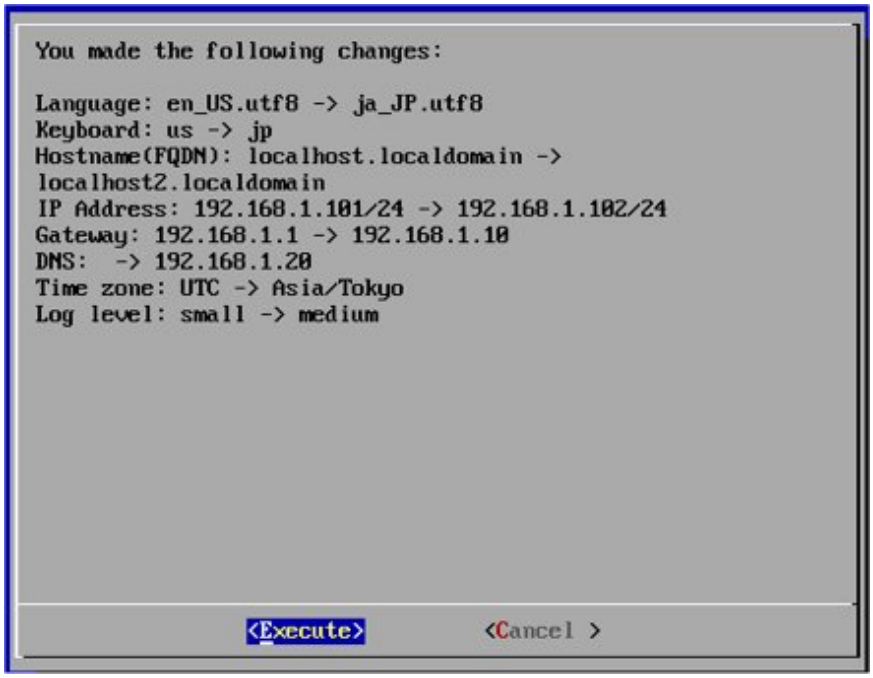
1. コンソールからadministratorでISM-VAにログインします。
2. ISM-VA基本設定メニューコマンドを実行します。

```
# ismsetup
```

以下の画面が表示されます。



3. 設定項目を選択し、設定値の入力または選択を行います。
4. 設定項目を入力後、[Apply]を選択します。
5. 変更内容を確認し、[Execute]を選択します。



変更処理終了後、変更結果が表示されます。

6. [Reboot ISM-VA]を選択してISM-VAを再起動し、変更を反映させます。

4.3 ISM公開サービスポートの変更

Webブラウザーで GUIへ接続する際のデフォルトポート番号(25566)を変更できます。

1. administratorユーザーでコンソールにログインします。
2. 以下のコマンドを実行し、ISMのサービスを停止します。

```
# ismadm service stop ism
```

3. 以下のコマンドを実行し、ISM公開サービスポートを変更します。

```
# ismadm service modify -port <サービスポート番号>
```

実行例:

```
# ismadm service modify -port 35566
You need to reboot the system to enable the new settings.
Immediately reboots the system.  [y/n]:
```

コマンド終了後に、再起動するかどうかを確認するメッセージが表示されますので、「y」を入力してISM-VAを再起動してください。

再起動完了後に新しいサービスポート番号でGUIが接続できるようになります。

4.4 ISMのバックアップとリストア

ISMのバックアップ／リストアの目的は、ISMで設定したデータの保存と復元です。

トラブルによるISMの設定データの破損や誤操作による設定データの消失などに備えて、ISMの設定値およびノード登録データなどを退避しておき、必要に応じて復元します。

注意

- ISMのバックアップは同一版数のISMにリストアします。異なる版数にはリストアできません。
- ISMのバックアップは設定値と登録データの一部をバックアップします。すべてのデータをバックアップするには、仮想化管理ソフトウェアのハイパーバイザーによるISM-VA全体のバックアップをしてください。

4.4.1 ISMのバックアップ

ISMのバックアップは、ユーザーが設定したISMの設定値と、監視のために登録したノード登録データなどの情報データをファイル化して外部に取り出すことができます。ISMのバックアップには次の方法があります。

ISMのバックアップは、以下の操作方法があります。

- ISM-VA管理コマンドを使用したISMのバックアップ
- GUIを使用したISMのバックアップ
- REST APIを使用したISMのバックアップ
  『REST API リファレンスマニュアル』を参照してください。

ISMのバックアップによって収集した情報データは、以下のディレクトリーにバックアップファイルが作成されます。

ディレクトリー：/Administrator/ftp

ファイル名：ism2.9.0-backup-202310102723.tar.gz（ファイル名は一例です）

ISMのバックアップ対象の情報データは、以下です。

凡例：○＝バックアップ対象、×＝バックアップ対象外

分類	情報データ内容	対象	備考
ISM-VAユーザー設定情報	ISM-VA基本設定メニューの設定項目	○	
	アカウントの管理データ	○	
	セキュリティポリシー設定	○	
	LDAPサーバー設定	○	
	ログ収集（スケジュール設定）	○	
	アラーム設定	○	
	ライセンス情報	○	
	SSL証明書、CA証明書	○	
	中継ルート用クライアント証明書	×	リストア時に再設定が必要です。
ISM-VAカスタマイズ情報	ダッシュボード設定	○	
	ノードリストカスタマイズ選択	○	
	仮想ディスクの割当て情報	○	
	プラグイン	×	再インストールが必要です。
ノード登録情報	ノード登録データ（ノードリスト）	○	
	ノード詳細情報（通信設定、OS情報）	○	
	ノードグループ、ユーザーグループ	○	
	アラーム設定	○	
監視データ	ISMイベント（監査ログ、運用ログ、SNMPトラップ、アノマリ検知ログ）	○	ISMイベントはバックアップします。
	保管ログ、ノードログ	×	リストア時に削除されます。
	アノマリ学習データ	×	
リポジトリ	ServerView Suite DVD	×	リポジトリ内はすべて対象外です。リストア後再構築が必要です。
	OSイメージ	×	
	ファームウェアアップデートファイル	×	
作業用ファイル	CSVエクスポートデータ	×	リストア時に作業用ファイルはすべて初期化されます。
	イベントエクスポートデータ	×	
	保守資料採取データ	×	

4.4.2 ISMのリストア

ISMのリストアは、ISMのバックアップで作成したバックアップファイルから、ユーザーが設定したISMの設定値と、監視のために登録したノード登録データなどの情報データを復元する操作です。

以下のディレクトリーに格納されるISMのバックアップファイルから復元します。

ディレクトリー:/Administrator/ftp

4.5 保守資料の採取

トラブルが発生した場合に、調査に必要な保守資料を採取できます。

4.5.1 必要な保守資料

ISMや仮想化基盤の拡張機能にトラブルが発生した場合に必要な保守資料の採取方法は、以下のとおりです。

ISMで運用するシステムにおいて、調査の目的に応じた保守資料を採取します。

調査目的	保守資料	採取方法
ISMやISM-VAの誤動作を調査 ISM for PRIMEFLEX機能共通の誤動作を調査	• 障害調査ログ • ISM-VA オペレーティングシステムログ • データベース情報	これらの保守資料を調査の目的に応じて採取したり、一括して採取したりできます。 GUIを利用して採取する方法と、コマンドを実行して採取する方法があります。 詳しくは、『操作手順書』の「8.2 保守資料を採取する」を参照してください。
仮想リソース管理機能／クラスタ管理機能の誤動作を調査	vSANのログ	vCenterからvc-supportログを採取します。 vc-supportログの採取方法
クラスタ作成機能／クラスタ拡張機能の誤動作を調査	OSインストール後のOS設定スクリプトの実行ログ	OSインストール後のOS設定スクリプトの実行ログ採取方法
	Windows Server上で実行したPowerShellスクリプトの実行ログ	Windows Server上で実行したPowerShellスクリプトの実行ログ採取方法

保守資料の採取は、ISM管理者が行います。ISM管理者は、採取した保守資料を調査担当者(当社技術員)に提供します。

注意

データベース情報の採取には、数時間かかることがあります。また、ISM-VAに大容量の空きディスク容量が必要です。これらを採取する場合、または保守資料を一括して採取する場合、当社技術員の指示に従ってください。

vc-supportログの採取方法

詳細は、以下のURL(英語ページ)の「To collect ESX/ESXi and vCenter Server diagnostic data」の手順を参照してください。

https://kb.vmware.com/s/article/2032892

上記URLに記載されたログ収集の手順で、ログをエクスポートする対象ESXiホストの選択手順では、問題が発生しているvSANクラスタのESXiホストをすべて選択してください。

ポイント

vSANクラスタに関連するログを一括で取得できます。詳細は、「2.13.9 VMware vSANクラスタに関連するログ一括収集」を参照してください。

OSインストール後のOS設定スクリプトの実行ログ採取方法

ログの採取方法は、環境に応じて以下となります。容量の目安は、約30KBです。

- PRIMEFLEX HS／PRIMEFLEX for VMware vSAN版

  ESXiホスト上の以下の場所より取得してください。

  /vmfs/volumes/datastore1_error/post_script.log

Windows Server上で実行したPowerShellスクリプトの実行ログ採取方法

対象サーバー[注]の以下ファイルをすべて取得してください。

- C:¥FISCRB¥Log¥＜PowerShellスクリプトファイル名＞_yyyymmdd-hhmmssmmm.log
- C:¥FISCRB¥Log¥配下の.log

[注]:対象サーバーは、環境および機能に応じて以下となります。

- PRIMEFLEX HS／PRIMEFLEX for VMware vSAN版

  DNSサーバー

4.5.2 ログ出力設定の変更

障害調査で使用するログ出力については、以下のような設定が可能です。

- 4.5.2.1 障害調査ログ切替え
- 4.5.2.2 障害調査ログレベル切替え
- 4.5.2.3 coreファイル採取ディレクトリーの指定

4.5.2.1 障害調査ログ切替え

障害調査で使用するログ出力の有効／無効を切り替えることができます。初期導入時のログ出力は無効になっています。

1. コンソールからadministratorでISM-VAにログインします。
2. 障害調査ログ切替えコマンドを実行します。

   ー ログ出力有効化

   ```
   # ismadm system set-debug-flag 1
   ```

   ー ログ出力無効化

   ```
   # ismadm system set-debug-flag 0
   ```

4.5.2.2 障害調査ログレベル切替え

障害調査で使用するログの出力レベルを切り替えることができます。

出力レベルを切り替えることにより、出力されるログの容量を制限できます。初期導入時は「small」に設定されています。

ログレベル	出力されるログ容量の目安	管理対象ノード数
small（初期値）	10GB	100ノード
medium	40GB	400ノード
large	100GB	1000ノード

注意

- 下位レベル(管理対象ノード数が少ない設定)から上位レベル(管理対象ノード数が多い設定)への切替えのみ有効です。
- ログレベルの切替え後は、ISM-VAの再起動が必要です。

1. コンソールからadministratorでISM-VAにログインします。
2. ISMサービスを停止させます。

   「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。
3. 障害調査ログレベル切替えコマンドを実行します。

   ー mediumへの切替え

   ```
   # ismadm system change-log-level medium
   ```

   ー largeへの切替え

   ```
   # ismadm system change-log-level large
   ```
4. 障害調査ログレベルの設定を確認します。

   システム情報の表示コマンドで確認できます。

   ```
   # ismadm system show
   ISM Version      : <Version>
   GUI Port Number : 25566
   Hostname         : localhost
   Log Level        : medium
   ```

   <Version>部分は、ISM-VAのバージョンが表示されます。
5. 以下のコマンドを実行し、ISM-VAを再起動します。

   ```
   # ismadm power restart
   ```

   ISM-VA起動後に、新しい障害調査ログレベルが有効になります。

ポイント

障害調査ログレベル切替えは、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

4.5.2.3 coreファイル採取ディレクトリーの指定

保守資料としてcoreファイルが出力される際の採取/保管先のディレクトリーを設定できます。未設定の場合は、ISM-VA内部のシステム領域のディレクトリーが使用されます。

出力されたcoreファイルは、「4.5 保守資料の採取」の対象として採取されます。

1. コンソールからadministratorでISM-VAにログインします。
2. ISM-VAサービス制御コマンドを実行します。

   ー 採取ディレクトリー表示

   ```
   # ismadm system core-dir-show
     Core Directory: Default Internal Directory
     Store Size: 713596
   ```

   現在設定されているcoreファイル採取ディレクトリーの場所と、使用されているディレクトリーサイズが表示されます。

   採取ディレクトリーの場所が未設定の場合は、「Default Internal Directory」と表示されます。

ー 採取ディレクトリー設定

```
# ismadm system core-dir-set -dir ＜ディレクトリー＞
```

ftpクライアントを使用して、事前に/Administrator/ftp/などの配下にディレクトリーを作成し、そのディレクトリーを指定してください。

例:

```
# ismadm system core-dir-set -dir /Administrator/ftp/coredump/
```

注意

作成した採取ディレクトリーは、coreファイル出力専用として使用し、ほかにファイルを配置しないでください。

ー 採取ディレクトリー解除

```
# ismadm system core-dir-reset
```

採取ディレクトリーを未設定状態に戻します。

4.6 仮想ディスクの管理

仮想ディスクの割当て解除や、仮想ディスクの追加割当てができます。

4.6.1 仮想ディスクの割当て解除

「3.7.2 ユーザーグループに対する仮想ディスク割当て」で割り当てた仮想ディスクの割当て解除ができます。

注意

- 割当て解除を行うと、ユーザーグループに保存されていたデータはすべて失われます。
- Administratorグループに割り当てた仮想ディスク割当ては解除できません。
- 「3.7.1 ISM-VA全体に対する仮想ディスク割当て」で割り当てたISM-VA全体に対する仮想ディスク割当ては解除できません。

以下、usrgrp1というユーザーグループに割り当てた仮想ディスクの割当て解除操作例を示します。

1. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
2. 仮想ディスク割当て解除のため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

3. usrgrp1へ仮想ディスクが割り当てられていることを確認します。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.5G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/0
tmpfs                     380M     0  380M    0% /run/user/1001
/dev/mapper/usrgrp1vol-lv  10G   33M   10G    1% 'RepositoryRoot'/usrgrp1

  PV         VG          Fmt  Attr PSize  PFree
  /dev/sda2  centos      lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  lvm2 a--  10.00g    0
```

この例では、usrgrp1volというVGが、usergrp1に割り当てられています。

4. ユーザーグループ名を指定し、仮想ディスクをアンマウントします。

```
# ismadm volume umount -gdir usrgrp1
```

5. usrgrp1用のボリューム名(usrgrp1vol)を指定し、仮想ディスクを削除します。

```
# ismadm volume delete -vol usrgrp1vol
  Logical volume "usrgrp1vol" successfully removed.
```

6. 仮想ディスク設定を確認します。

usrgrp1用の仮想ディスクが設定されておらず、使用されていた/dev/sdbが未使用状態(Free)であることを確認してください。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.5G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M     0  380M    0% /run/user/0
tmpfs                     380M     0  380M    0% /run/user/1001
/dev/sdb1                                    (Free 10.7 GB)

  PV         VG     Fmt  Attr PSize  PFree
  /dev/sda2  centos lvm2 a--  19.51g     0
  /dev/sdb1         lvm2 ---  10.00g 10.00g
```

7. ISM-VAを再起動します。

```
# ismadm power restart
```

4.6.2 ISM-VA全体に対する仮想ディスクの追加割当て

「3.7.1 ISM-VA全体に対する仮想ディスク割当て」と同様の方法で、複数の仮想ディスクをISM-VA全体に追加割当てできます。

4.6.3 ユーザーグループに対する仮想ディスク追加割当て

「3.7.2 ユーザーグループに対する仮想ディスク割当て」で割り当てた仮想ディスクに対し、追加の仮想ディスクを割り当てることができます。

以下、usrgrp1というユーザーグループに割り当てた仮想ディスクの追加割当ての操作例を示します。

1. 仮想ディスクに接続します。

「3.7.2 ユーザーグループに対する仮想ディスク割当て」の手順1の操作を行ってください。

2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。

3. 仮想ディスク追加割当てのため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

4. 手順1で追加した仮想ディスクが認識されているか確認します。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.5M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  169M  329M   34% /boot
```

```
/dev/mapper/usrgrp1vol-lv  10G  33M   10G    1% 'RepositoryRoot'/usrgrp1
tmpfs                     380M     0  380M    0% /run/user/0
/dev/sdc                                      (Free 5368 MB)

  PV         VG      Fmt  Attr PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol  lvm2 a--  10.00g    0
```

この例では、/dev/sdcが追加され、未使用領域と認識されています。

5. 仮想ディスク追加割当てコマンドを実行し、追加した仮想ディスクをusrgrp1volに割り当てます。

```
# ismadm volume extend -vol usrgrp1vol -disk /dev/sdc
  Logical volume "/dev/mapper/usrgrp1vol-lv" resized.
```

6. 仮想ディスク設定を確認します。

   新規追加したボリューム(/dev/sdc)が、usrgrp1用(usrgrp1vol)として設定されていることを確認してください。

```
# ismadm volume show -disk
ファイルシステム          サイズ 使用  残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G   13G   17% /
devtmpfs                  1.9G     0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G     0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
/dev/mapper/usrgrp1vol-lv  15G   33M   15G    1% 'RepositoryRoot'/usrgrp1
tmpfs                     380M     0  380M    0% /run/user/0
tmpfs                     380M     0  380M    0% /run/user/1001

  PV         VG      Fmt  Attr PSize  PFree
  /dev/sda2  centos  lvm2 a--  19.51g    0
  /dev/sdb1  usrgrp1vol lvm2 a--  10.00g    0
  /dev/sdc1  usrgrp1vol lvm2 a--   5.00g    0
```

7. ISM-VAを再起動します。

```
# ismadm power restart
```

4.7 証明書設定

ISMのGUIを使用する際にWebブラウザーに設定する、SSL証明書の管理ができます。

4.7.1 SSL証明書配置

セキュリティを考慮して認証機関などで発行されたSSL証明書を使用する場合、以下の手順で設定できます。

SSL証明書のRSA公開鍵長に上限はありません。

1. SSL証明書をISM-VAへ転送します。

   転送先:/Administrator/ftp

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。

3. SSL証明書を配置します。

   転送した「key」ファイルと「crt」ファイルを指定し、コマンドを実行してください。

```
# ismadm sslcert set -key /Administrator/ftp/server.key -crt /Administrator/ftp/server.crt
```

4. ISM-VAを再起動します。

```
# ismadm power restart
```

ポイント

ローカルネットワーク内で使用する独自のホスト名に対応した独自SSL証明書は、openssslコマンドがインストールされたLinuxサーバー上で、以下のコマンドで作成できます。

```
# openssl genrsa -rand /proc/uptime 2048 > server.key
# openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM -extensions v3_req -out server.crt
```

- 証明書のファイル名（server.key/server.crt）は任意のファイル名を指定
- daysオプションは証明書の有効日数を指定
- ホスト名は、openssl reqコマンド実行後の「Common Name」入力時に指定

4.7.2 SSL証明書表示

ISM-VAに設定されているSSL証明書を表示します。

1. コンソールからadministratorでISM-VAにログインします。
2. SSL証明書表示コマンドを実行します。

```
# ismadm sslcert show
```

4.7.3 SSL証明書出力

ISM-VAに設定されているSSL証明書を出力します。

1. コンソールからadministratorでISM-VAにログインします。
2. SSL証明書出力コマンドを実行します。

```
# ismadm sslcert export -dir /Administrator/ftp
```

出力されたファイルは、FTPでダウンロードできます。

4.7.4 自己署名証明書作成

ISM-VAで設定済みのIPアドレスまたはFQDNを元に、自己署名証明書を作成します。

1. コンソールからadministratorでISM-VAにログインします。
2. 自己署名証明書作成コマンドを実行します。

   ー IPアドレスでSSLアクセスする場合

   ```
   # ismadm sslcert self-create -cnset ip
   ```

   ー FQDNでSSLアクセスする場合

   ```
   # ismadm sslcert self-create -cnset fqdn
   ```

3. ISM-VAを再起動します。

```
# ismadm power restart
```

4.7.5 CA証明書のダウンロード

自己署名証明書を作成した場合、CA証明書を以下のURLからダウンロードできます。

https://＜ISM-VAのIPアドレス＞:25566/ca.crt

Google Chromeを使用する場合、表示された内容に対して、[名前を付けて保存] を実施し、ファイル名を"ca.crt"に変更します。
保存時のファイルの種類は、「すべてのファイル」を選択してください。

実行例:curlコマンドがインストールされたLinuxサーバー上でダウンロードする場合

```
# curl -Ok https://192.168.10.20:25566/ca.crt
```

4.8 ライセンス設定

ISM-VAのサーバーライセンスおよびノードライセンスの登録／表示／削除が行えます。

1. コンソールからadministratorでISM-VAにログインします。
2. ライセンス設定コマンドを実行します。

   ー ライセンス登録

   ```
   # ismadm license set -key ＜ライセンスキー＞
   ```

   ー ライセンス表示

   ```
   # ismadm license show
   ```

   実行例:

   ```
   # ismadm license show
   Operation Mode : Advanced
   #   [Type]  [Edition] [#Node]  [Reg.Date]  [Exp.Date]  [Status]       [Licensekey]
   1   Server  Adv.            -  2024-05-29  2025-05-29  Valid          **********************==
   2   Node    Adv.           10  2023-08-28  2024-08-27  Expires soon   **********************==
   3   Node    Adv.           10  2023-05-30  2024-05-29  Expired        **********************==

   *Reg.Date(RegistrationDate[yyyy-mm-dd])
   *Exp.Date(ExpirationDate[yyyy-mm-dd])

   You have an expired license.
   Delete the expired license and register a new license.
   ```

表4.1 コマンド出力結果の説明

項目	説明
[Operation Mode]	ISMの動作モードが表示されます。 ・ Essential ・ Advanced ・ Advanced for PRIMEFLEX
[Type]	サーバーライセンスの場合は「Server」、ノードライセンスの場合は「Node」が表示されます。
[Edition]	ライセンス種別が表示されます。 ・ Adv.:ISMライセンス ・ I4P:ISM for PRIMEFLEXライセンス
[#Node]	そのライセンスで管理可能となるノード数が表示されます。ライセンスタイプが「Server」の場合は常に"-"が表示されます。
[Reg.Date]	ライセンスを登録した日付が表示されます。

項目	説明
[Exp.Date]	ライセンスの有効期限が切れる日付が表示されます。 無期限の場合は常に"-"が表示されます。
[Status]	ライセンスのステータスが表示されます。 ・ Valid :有効 ・ Expires soon:期限切れ間近(30日以内) ・ Expired :期限切れ
[Licensekey]	登録済みライセンスキーの文字列が表示されます。

ー ライセンス削除

```
# ismadm license delete -key <ライセンスキー>
```

ポイント

ー ライセンスの登録、種別を含む表示内容の確認、および削除は、ISMのGUIでグローバルナビゲーションメニューの[設定]-[全般]-[ライセンス]からも行えます。

ー ライセンスの登録／削除において、動作モードが変更しない場合には、ISM-VAの再起動は不要です。

4.9 ネットワーク設定

ネットワークの設定／表示、および疎通確認を行います。

ネットワークの設定／表示

1. コンソールからadministratorでISM-VAにログインします。
2. ネットワーク設定コマンドを実行します。

ー ネットワークデバイス表示

```
# ismadm network device
```

ー ネットワーク設定変更

```
# ismadm network modify <LANデバイス名> ipv4.method manual ipv4.addresses <IPアドレス>/<マスクビット>
ipv4.gateway <ゲートウェイIPアドレス>
```

注意

ネットワーク設定変更後は、ISM-VAの再起動が必要です。

実行例:

```
# ismadm network modify eth0 ipv4.method manual ipv4.addresses 192.168.1.101/24 ipv4.gateway 192.168.1.1
```

ー DNSサーバー追加

```
# ismadm network modify <LANデバイス名> +ipv4.dns <DNSサーバー>
```

実行例:

```
# ismadm network modify eth0 +ipv4.dns 192.168.1.2
```

ー DNSサーバー削除

```
# ismadm network modify ＜LANデバイス名＞ -ipv4.dns ＜DNSサーバー＞
```

実行例:

```
# ismadm network modify eth0 -ipv4.dns 192.168.1.2
```

ー ISM-VAのMTUサイズ変更

```
# ismadm network modify ＜LANデバイス名＞ 802-3-ethernet.mtu ＜MTUサイズ＞
```

設定済みのMTUサイズは、ネットワーク設定表示コマンドの出力で「802-3-ethernet.mtu」の項目に表示されます。

コマンド実行後、設定表示コマンドの出力にはすぐに反映されますが、実際にMTUサイズ変更を有効化するためにはISM-VAの再起動が必要です。

MTUサイズのデフォルトは、1500です。ネットワーク設定表示コマンドの出力では「auto」と表示されます。

MTUサイズは、1280から65535の範囲で変更できます。

注意

ISMを使用するネットワークに適合しないMTUサイズを設定した場合、通信不能や通信速度の低下が発生する可能性があります。MTUサイズを変更する必要がある場合のみ変更してください。

実行例:

```
# ismadm network modify eth0 802-3-ethernet.mtu 1460
```

ー ネットワーク設定表示

```
# ismadm network show ＜LANデバイス名＞
```

実行例:

```
# ismadm network show eth0
```

ポイント

ネットワーク設定は、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

ネットワークの疎通確認

ISM-VAと管理LANでつながっている機器との疎通を確認します。

1. コンソールからadministratorでISM-VAにログインします。
2. ネットワーク疎通確認コマンドを実行します。

```
# ismadm network ping -host ＜IPアドレス or FQDN＞
```

ISM-VAにDNSサーバーが設定されている場合は、IPアドレスの代わりにFQDNを指定できます。

実行例:疎通成功の場合

```
#ismadm network ping -host 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.038 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.066 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.039 ms
```

```
--- 192.168.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2999ms
rtt min/avg/max/mdev = 0.038/0.049/0.066/0.014 ms
```

実行例:疎通失敗の場合

```
# ismadm network ping -host 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.1.101 icmp_seq=1 Destination Host Unreachable
From 192.168.1.101 icmp_seq=2 Destination Host Unreachable
From 192.168.1.101 icmp_seq=3 Destination Host Unreachable
From 192.168.1.101 icmp_seq=4 Destination Host Unreachable
```

4.10 アラーム通知設定

モニタリング機能のアラーム通知時に使用する証明書を登録できます。

アラーム通知メール用証明書登録

1. 証明書を転送します。

   転送先:/＜ユーザーグループ名＞/ftp/cert

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。
3. アラーム通知メール用証明書登録コマンドを実行します。

```
# ismadm event import -type cert
```

ポイント

ISM-VAに登録されたアラーム通知メール用証明書を表示／削除する場合は、以下のコマンドを実行します。

- アラーム通知メール用証明書表示

```
# ismadm event show -type cert
```

- アラーム通知メール用証明書削除

```
# ismadm event delete -type cert  -file ＜証明書ファイル＞ -gid ＜ユーザーグループ名＞
```

4.11 ISM-VAサービス制御

ISM-VAの停止／再起動や、内部で動作しているサービスの制御を行えます。

1. コンソールからadministratorでISM-VAにログインします。
2. ISM-VAサービス制御コマンドを実行します。

   ー ISM-VA再起動

```
ismadm power restart
```

   ー ISM-VA停止

```
ismadm power stop
```

ー 内部サービス一覧表示

```
ismadm service show
```

ー 内部サービス個別起動

```
ismadm service start ＜サービス名＞
```

実行例:FTPサーバーの個別起動

```
# ismadm service start vsftpd
```

ー 内部サービス個別停止

```
ismadm service stop ＜サービス名＞
```

実行例:FTPサーバーの個別停止

```
# ismadm service stop vsftpd
```

ー 内部サービス個別再起動

```
ismadm service restart ＜サービス名＞
```

実行例:FTPサーバーの個別再起動

```
# ismadm service restart vsftpd
```

ー 内部サービス個別ステータス表示

```
ismadm service status ＜サービス名＞
```

実行例:FTPサーバーの個別ステータス表示

```
# ismadm service status vsftpd
```

ー 内部サービス個別有効化設定

```
ismadm service enable ＜サービス名＞
```

実行例:FTPサーバーの個別有効化設定

```
# ismadm service enable vsftpd
```

ー 内部サービス個別無効化設定

```
ismadm service disable ＜サービス名＞
```

実行例:FTPサーバーの個別無効化設定

```
# ismadm service disable vsftpd
```

4.12 システム情報の表示

コンソールからISM-VAの内部システム情報を表示できます。

1. コンソールからadministratorでISM-VAにログインします。
2. システム情報の表示コマンドを実行します。

```
# ismadm system show
ISM Version     : ＜Version＞
GUI Port Number : 25566
Hostname        : localhost
Log Level       : small
```

＜Version＞部分は、ISM-VAのバージョンが表示されます。

4.13 ホスト名変更

ISM-VAのホスト名を変更できます。

1. コンソールからadministratorでISM-VAにログインします。
2. ホスト名変更コマンドを実行します。

```
# ismadm system modify -hostname ＜ホスト名（FQDN）＞
```

実行例：

```
# ismadm system modify -hostname ismva2.domainname
You need to reboot the system to enable the new settings.
Immediately reboots the system.  [y/n]:
```

注意

- ホスト名として使用可能な文字は英小文字、数字、ハイフン(-)、ピリオド(.)です。ハイフンおよびピリオドは、ホスト名の先頭および末尾の文字として使用できません。使用可能な文字以外を使用した場合、ISMは正常に動作しません。
- コマンド実行後に再起動が必要です。
- ホスト名の初期値「localhost」を変更する場合は、「4.7 証明書設定」に記載された手順に従い、変更するホスト名に対応した証明書をISM-VAに配置する必要があります。

ポイント

ホスト名変更は、「4.2 ISM-VA基本設定メニュー」で行うこともできます。

4.14 プラグイン操作

ISM-VAにプラグインの適用、削除および、適用しているプラグインの表示を行うことができます。

4.14.1 プラグイン適用

1. プラグインファイルをISM-VAへ転送します。

   転送先：/Administrator/ftp

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

   プラグインファイルはバイナリモードで転送してください。
2. コンソールからadministratorでISM-VAにログインします。
3. プラグイン適用のため、一時的にISMサービスを停止させます。

   「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。
4. プラグイン適用コマンドを実行します。

   プラグインファイルを指定してコマンドを実行してください。

```
# ismadm system plugin-add -file ＜プラグインファイル＞
```

実行例：

```
# ismadm system plugin-add -file /Administrator/ftp/FJSVsvism-ext-1.0.0-10.tar.gz
```

4.14.2 プラグイン表示

適用されているプラグインのバージョンを表示します。

```
# ismadm system plugin-show
  FJSVsvism-ext 1.0.0
```

「プラグイン名 バージョン」の形式で表示されます。

ポイント

「4.12 システム情報の表示」の「ismadm system show」コマンドでもプラグインの情報が表示されます。

```
# ismadm system show
ISM Version     : ＜Version＞
GUI Port Number : 25566
Hostname        : localhost
Log Level       : small
Plugin          : FJSVsvism-ext 1.0.0
```

＜Version＞部分は、ISM-VAのバージョンが表示されます。

Pluginには、適用されているプラグイン名とバージョンが表示されます。

4.14.3 プラグイン削除

適用したプラグインをアンインストールします。

1. プラグイン削除コマンドを実行します。

   ```
   # ismadm system plugin-del -name ＜プラグイン名＞
   ```

   プラグイン名は、「4.14.2 プラグイン表示」で記述されているコマンドの出力で表示されます。

   実行例:

   ```
   # ismadm system plugin-del -name FJSVsvism-ext
   Uninstall plugin <FJSVsvism-ext 1.0.0> ?
   [y/n]:
   ```

   コマンド実行後に、プラグインのアンインストールの確認画面が表示されます。

2. [y]を入力して、アンインストールを確定させます。

4.15 ISM-VA内部のDHCPサーバー

ISM-VA内部のDHCPサービスを起動することで、ISM-VAをDHCPサーバーとして使用できます。

DHCPサーバーは、プロファイル管理機能でOSインストールを行う場合に必要です。外部のDHCPサーバーを使用することも、以下の手順で設定したISM-VAをDHCPサーバーとして使用することも、どちらでも可能です(その場合、「4.15.4 DHCPサーバーの切替え」で示されている手順により、どちらのDHCPサーバーを使用するかを指定します)。

外部のDHCPサーバーのみを使用する場合は、以下の設定は不要です。

4.15.1 ISM-VA内部のDHCPサーバーの設定

ISM-VA内部のDHCPサーバーの設定をします。設定後、DHCPサービスを停止、起動することにより設定が反映されます。

注意

DHCPサーバーの設定変更を行った場合は、DHCPサービスの停止と起動を行ってください。

サービスの停止、起動の方法は、「4.15.2 ISM-VA内部のDHCPサービスの操作」を参照してください。

DHCPサーバーの設定には、2つの方法があります。運用に合わせてどちらかの方法で設定してください。

- ismadm dhcpsrv コマンドのパラメーター指定による設定

  ISM-VAのプロファイル適用に必要なDHCPサーバーの設定を行います。

- confファイルによる設定

  ISM-VAのプロファイル適用で使用する設定に限らず、一般的なDHCPサーバーの設定を行います。

ismadm dhcpsrv コマンドのパラメーター指定による設定

```
# ismadm dhcpsrv set-simple -subnet ＜サブネット＞
                            -netmask ＜サブネットマスク＞
                            -start ＜割当て開始アドレス＞
                            -end ＜割当て終了アドレス＞
                            -broadcast ＜ブロードキャストアドレス＞
                            [-dns ＜DNSサーバーのIPアドレス＞]
                            [-gw ＜ゲートウェイのIPアドレス＞]
```

コマンドは1行で入力してください。

以下のパラメーターは指定が必須です。

-subnet

-netmask

-start

-end

-broadcast

実行例:

```
# ismadm dhcpsrv set-simple -subnet 192.168.1.0 -netmask 255.255.255.0 -start 192.168.1.150 -end 192.168.1.160 -
broadcast 192.168.1.255 -dns 192.168.1.200 -gw 192.168.1.250

---------------- New Configuration ----------------
ddns-update-style none;
default-lease-time 86400;
max-lease-time 259200;

shared-network LOCAL-NET {
  subnet 192.168.1.0 netmask 255.255.255.0 {
     range 192.168.1.150 192.168.1.160;
     option subnet-mask 255.255.255.0;
     option broadcast-address 192.168.1.255;
     option vendor-class-identifier "PXEClient";
     option domain-name-servers 192.168.1.200;
     option routers 192.168.1.250;
          }
       }
---------------------------------------------------
Update DHCP configureation ? (Current settings are discarded)
[y/n]:
```

コマンドを実行すると、設定する値を確認するメッセージが表示されるので、「y」を入力して設定を確定させてください。

confファイルによる設定

記述済みのconfファイルをアップロードし、コマンドで取り込みます。

GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

```
# ismadm dhcpsrv set -file ＜confファイル＞
```

実行例:

```
# ismadm dhcpsrv set -file /Administrator/ftp/dhcpd.conf.new
```

4.15.2 ISM-VA内部のDHCPサービスの操作

ISM-VA内部のDHCPサービスの状態の表示、起動、停止を行います。

- DHCPサービスの状態を確認

```
# ismadm service status dhcpd
```

コマンド出力（※部以降の文言は、実際の画面には表示されません。）

```
Active : active(running)                          ※DHCPサービス起動状態
Active : inactive(dead)                           ※DHCPサービス未起動状態
/usr/lib/systemd/system/dhcpd.service; enable;    ※ISM-VAブート時起動設定
/usr/lib/systemd/system/dhcpd.service; disabled;  ※ISM-VAブート時未起動設定
```

- DHCPサービスの手動起動

```
# ismadm service start dhcpd
```

注意

ー ISM-VA内部のDHCPサービスを起動する前に、DHCPサーバーの設定を行ってください。

DHCPサーバーの設定方法は、「4.15.1 ISM-VA内部のDHCPサーバーの設定」を参照してください。

ー DHCPサーバーが起動状態設定で「(dead)」状態になっている場合は、「4.15.3 ISM-VA内部のDHCPサーバー情報の確認」の「DHCPサーバーメッセージ表示」でエラーが出ていないかどうか確認してください。

- DHCPサービスの手動停止

```
# ismadm service stop dhcpd
```

- ISM-VA起動時にDHCPサービスを起動するように設定

```
# ismadm service enable dhcpd
```

- ISM-VA起動時にDHCPサービスを起動しないように設定

```
# ismadm service disable dhcpd
```

4.15.3 ISM-VA内部のDHCPサーバー情報の確認

ISM-VA内部のDHCPサーバーの情報を表示します。

現在設定されているDHCPサーバーの内容の表示、DHCPサーバーのメッセージの表示、現在の設定内容（confファイル）をftpアクセス可能な場所へエクスポート、サンプルconfファイルをftpアクセス可能な場所へエクスポートできます。

- 現在設定されているDHCPサーバーの内容を表示

```
# ismadm dhcpsrv show-conf
```

・ DHCPサーバーのメッセージ表示

```
# ismadm dhcpsrv show-msg [-line]
```

オプションなしで実行した場合、20行表示します。

オプション[-line] を指定した場合、表示行数を指定できます。

実行例:

```
# ismadm dhcpsrv show-msg -line 50
```

・ 現在の設定内容(confファイル)をftpアクセス可能な場所へエクスポート

```
# ismadm dhcpsrv export-conf -dir /Administrator/ftp
```

・ 設定内容(confファイル)のサンプルをftpアクセス可能な場所へエクスポート

```
# ismadm dhcpsrv export-sample -dir /Administrator/ftp
```

4.15.4 DHCPサーバーの切替え

プロファイル管理機能でDHCPサーバーを使用する場合に、ISM-VA内部のDHCPサーバーを使用するか、外部のDHCPサーバーを使用するかを切り替えることができます。

・ 現在の設定の表示

```
# ismadm dhcpsrv show-mode
```

コマンド出力(※部以降の文言は、実際の画面には表示されません。)

```
DHCP mode: local          ※プロファイル管理機能はISM内部のDHCPサーバーを使用します。
DHCP mode: remote         ※プロファイル管理機能は外部のDHCPサーバーを使用します。
```

・ 設定の切替え

－ ISM-VA内部のDHCPサーバーを使用してプロファイル適用を行うように設定

```
# ismadm dhcpsrv set-mode local
```

－ 外部のDHCPサーバーを使用してプロファイル適用を行うように設定

```
# ismadm dhcpsrv set-mode remote
```

4.16 MIBファイル設定

任意のトラップ受信を可能にするMIBファイルを、ISM-VA内に取り込むことができます。

MIBファイル登録

1. MIBファイルを転送します。

   転送先:/Administrator/ftp/mibs

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。

3. MIBファイル登録コマンドを実行します。

```
# ismadm mib import
```

ポイント

ISM-VAに登録されたMIBファイルを表示／削除する場合は、以下のコマンドを実行します。

- MIBファイル表示

```
# ismadm mib show
```

- MIBファイル削除

```
# ismadm mib delete -file <MIBファイル名>
```

4.17 修正パッチ適用

ISM-VAに修正パッチを適用できます。

注意

- 修正パッチを適用する前に、ISMが動作しているハイパーバイザーでISM-VAをバックアップしてください。
- システムをアップデートするためにISM-VAのディスク容量を使用します。必要なディスク容量は、以下を参照してください。

  「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」の「修正パッチまたはアップグレード適用後のシステムアップデート」

  『操作手順書』の「9.1 修正パッチ／アップグレードプログラムを適用する」

ismadmコマンドを使用した適用方法

1. 修正ファイルをISM-VAへ転送します。

   転送先:/Administrator/ftp

   修正ファイル(tar.gz形式)は、公開ファイル(zip形式)に含まれています。
   公開ファイルを解凍し、修正ファイルを取り出してください。

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

   修正ファイルはバイナリモードで転送してください。

2. コンソールからadministratorでISM-VAにログインします。
3. 修正パッチ適用のため、一時的にISMサービスを停止させます。

   「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。

4. 修正パッチ適用コマンドを実行します。

   修正ファイルを指定してコマンドを実行してください。

   ```
   # ismadm system patch-add -file <修正ファイルのパス>
   ```

   実行例:

   ```
   # ismadm system patch-add -file /Administrator/ftp/ISM240x_S20190901-01.tar.gz
   ```

   コマンド実行が成功した場合、以下のメッセージが表示されます。

   ```
   ----------------------------------------
    Update finished successfully.
    Please restart ISM-VA.
   ----------------------------------------
   ```

5. 修正パッチ適用後、ISM-VAを再起動します。

```
# ismadm power restart
```

6. コンソールからadministratorでISM-VAにログインし、以下のコマンドを実行します。

   修正パッチが適用され、適用した修正パッチの版数が表示されていることを確認します。

```
# ismadm system show
```

GUIを使用した適用方法

詳細な手順については、『操作手順書』の「9.1 修正パッチ／アップグレードプログラムを適用する」の手順4～10を参照してください。

4.18 ISM-VAのアップグレード

ismadmコマンドを使用した適用方法

1. アップグレードファイルをISM-VAへ転送します。

   転送先:/Administrator/ftp

   アップグレードファイル名は、アップグレードプログラム内に格納されているreadme.txtまたはreadme_en.txtを確認してください。

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。
3. アップグレードのため、一時的にISMサービスを停止させます。

   「4.1.4 ISMのサービス起動と停止」のISMのサービス停止手順に従い、ISMサービスを停止させてください。

4. アップグレードコマンドを実行します。

   アップグレードファイルを指定してコマンドを実行してください。

```
# ismadm system upgrade -file ＜アップグレードファイルのパス＞
```

   実行例:

```
# ismadm system upgrade -file /Administrator/ftp/ISM240x_S20190901-01.tar.gz
```

   コマンド実行が成功した場合、以下のメッセージが表示されます。

```
---------------------------------------
 Update finished successfully.
 Please restart ISM-VA.
---------------------------------------
```

5. アップグレード後、ISM-VAを再起動します。

```
# ismadm power restart
```

6. コンソールからadministratorでISM-VAにログインし、以下のコマンドを実行します。

   アップグレードが適用され、選択したバージョンが表示されていることを確認します。

```
# ismadm system show
```

GUIを使用した適用方法

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]を選択します。

2. 画面左側のメニューから[修正パッチ／アップグレードプログラム]を選択します。

   現在のISMのバージョンが表示されます。

3. [ISMを更新する]ボタンを選択します。

4. 「修正パッチ／アップグレードプログラム」画面に従い設定項目を入力し、[確認]ボタンを選択します。

5. 表示内容を確認し、[はい]ボタンを選択します。

6. アップグレードが完了するまで待ちます。

   アップグレードの完了後、キャッシュをクリアし、ログイン画面に移動してください。

7. ログイン後、アップグレードされたことを確認します。

   ISMのGUIでグローバルナビゲーションメニューから[ヘルプ]-[ISMについて]を選択します。
   選択したバージョンが表示されていることを確認します。

注意

- アップグレードする前に、ISMが動作しているハイパーバイザーでISM-VAをバックアップしてください。
- システムをアップデートするためにISM-VAのディスク容量を使用します。必要なディスク容量は、以下を参照してください。

  「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」の「修正パッチまたはアップグレード適用後のシステムアップデート」

4.19 ISM-VAの統計情報表示

ISM-VAのCPU使用率／メモリー使用率／スワップ使用回数の統計情報を表示します。

4.19.1 統計情報の概要表示

収集されている全データ(約1か月分)を1日単位で集計して表示します。

```
# ismadm system stat
```

表4.2 出力内容

表示項目	説明
DATE	日付
CPU-avg	平均CPU使用率
CPU-max	最大CPU使用率
MEM-total	ISM-VAに割り当てられている物理メモリー量(MB)
MEM-avg	平均メモリー使用率(OSが使用しているキャッシュは除外)
MEM-max	最大メモリー使用率(OSが使用しているキャッシュは除外)
SWAP-avg	1秒当たりの平均スワップ使用回数
SWAP-max	1秒当たりの最大スワップ使用回数

実行例:

```
# ismadm system stat
    DATE      CPU-avg   CPU-max   MEM-total  MEM-avg   MEM-max   SWAP-avg   SWAP-max
2018/04/01    32.43     35.18       7823     57.96     58.71      0.00       0.00
2018/04/02    32.85     36.99       7823     57.52     58.66      0.00       0.00
2018/04/03    33.00     38.33       7823     56.14     58.17      0.00       0.00
2018/04/04    32.64     38.65       7823     54.22     55.22      0.00       0.00
2018/04/05    32.64     37.76       7823     53.84     54.97      0.00       0.00
```

```
2018/04/06    29.90    37.72    7823    54.62    56.28    0.00    0.00
2018/04/07    18.75    44.33    7823    55.01    56.13    0.00    0.00
```

4.19.2 統計情報の詳細表示

指定した日付のデータを1時間単位で表示します。指定する日付は、個別指定または範囲指定できます。all指定で収集されているすべての日付のデータを詳細表示します。

```
# ismadm system stat -date {DATE or all}
```

表4.3 出力内容

表示項目	説明
DATE	日付
HOUR	時間(1時間単位)
CPU-avg	平均CPU使用率
CPU-max	最大CPU使用率
MEM-total	ISM-VAに割り当てられている物理メモリー量(MB)
MEM-avg	平均メモリー使用率(OSが使用しているキャッシュは除外)
MEM-max	最大メモリー使用率(OSが使用しているキャッシュは除外)
SWAP-avg	1秒当たりの平均スワップ使用回数
SWAP-max	1秒当たりの最大スワップ使用回数

・ 実行例(個別指定の場合):

```
# ismadm system stat -date 2018/04/01,2018/04/02,2018/04/03
    DATE     HOUR    CPU-avg    CPU-max    MEM-total MEM-avg    MEM-max    SWAP-avg    SWAP-max
2018/04/01 00:00      31.57      33.87       7823      54.31      54.76       0.00       0.00
2018/04/01 01:00      31.97      34.25       7823      54.26      54.80       0.00       0.00
2018/04/01 02:00      32.13      34.13       7823      54.25      54.88       0.00       0.00
```

・ 実行例(範囲指定の場合):

```
# ismadm system stat -date 2018/04/01-2018/04/05
    DATE     HOUR    CPU-avg    CPU-max    MEM-total MEM-avg    MEM-max    SWAP-avg    SWAP-max
2018/04/01 00:00      31.57      33.87       7823      54.31      54.76       0.00       0.00
2018/04/01 01:00      31.97      34.25       7823      54.26      54.80       0.00       0.00
2018/04/01 02:00      32.13      34.13       7823      54.25      54.88       0.00       0.00
```

・ 実行例(all指定の場合):

```
# ismadm system stat -date all
    DATE     HOUR    CPU-avg    CPU-max    MEM-total MEM-avg    MEM-max    SWAP-avg    SWAP-max
2018/04/01 00:00      31.57      33.87       7823      54.31      54.76       0.00       0.00
2018/04/01 01:00      31.97      34.25       7823      54.26      54.80       0.00       0.00
2018/04/01 02:00      32.13      34.13       7823      54.25      54.88       0.00       0.00
```

4.19.3 リアルタイムの情報表示

現在動作中の情報を1秒間隔で集計し、指定した回数表示します。指定できる回数は、1から600の範囲内です。

```
# ismadm system stat -real {COUNT}
```

表4.4 出力内容

表示項目	説明
DATE	日付

表示項目	説明
TIME	時間
CPU-avg	平均CPU使用率
MEM-total	ISM-VAに割り当てられている物理メモリー量(MB)
MEM-avg	平均メモリー使用率(OSが使用しているキャッシュは除外)
SWAP-avg	1秒当たりの平均スワップ使用回数

実行例:

```
# ismadm system stat -real 10
    DATE      TIME      CPU-avg   MEM-total  MEM-avg    SWAP-avg
2018/04/10 08:00:25      0.51       7823       63.28      0.00
2018/04/10 08:00:26      1.02       7823       63.28      0.00
2018/04/10 08:00:27      1.52       7823       63.28      0.00
2018/04/10 08:00:28      0.51       7823       63.28      0.00
2018/04/10 08:00:29      1.52       7823       63.28      0.00
2018/04/10 08:00:30      2.02       7823       63.29      0.00
2018/04/10 08:00:31      1.02       7823       63.29      0.00
2018/04/10 08:00:32      1.51       7823       63.29      0.00
2018/04/10 08:00:33      1.02       7823       63.29      0.00
2018/04/10 08:00:34      1.52       7823       63.29      0.00
```

4.19.4 統計情報ファイル出力

画面出力と同一の内容をファイルに出力します。

統計情報概要表示／統計情報詳細表示／リアルタイム情報表示と組み合わせて使用します。

出力先:/Administrator/ftp/ismva_stat.txt

```
# ismadm system stat -file
```

```
# ismadm system stat -date {DATE or all} -file
```

```
# ismadm system stat -real {COUNT} -file
```

4.20 SSL/TLSプロトコルのバージョンの変更

利用可能なSSL/TLSプロトコルのバージョンを設定できます。プロトコルのバージョンを変更できる接続は、GUI、RESTとノードのログ収集で使用されるFTPS接続です。

デフォルトで設定されている利用可能なSSL/TLSバージョンは、以下のとおりです。

凡例:○ = 利用可能、- = 利用不可

接続方法	ISMの環境	利用可能なSSL/TLSバージョン			
		SSLv3	TLSv1	TLSv1.1	TLSv1.2
GUI／REST接続	ISM 2.3.0より前	○	○	○	○
	ISM 2.3.0以降	- [注1] [注2]	- [注1] [注2]	- [注1] [注2]	○
FTPS接続	ISM 2.7.0.020～ ISM2.9.0.020	- [注2]	○	- [注2]	○
	ISM 2.9.0.030以降	- [注2]	-	- [注2]	○

[注1]:ISMをアップグレードした場合には、アップグレード前のISMのバージョンで利用可能なSSL/TLSバージョンが引き継がれます。

例:ISM 2.3.0より前からISM 2.7.0.020にアップデート／アップグレードした場合に利用可能なSSL/TLSバージョン

SSLv3, TLSv1, TLSv1.1, TLSv1.2

[注2]:SSL/TLS有効化設定コマンド実行時に ＜利用を許可するバージョン＞ に指定することで、利用可能となります。

1. コンソールからadministratorでISM-VAにログインします。
2. SSL/TLS有効化設定コマンドを実行します。

   ー GUI／REST接続のSSL/TLSプロトコルのバージョンを変更する場合

   ```
   # ismadm security enable-tls ＜利用を許可するバージョン＞
   ```

   ー ノードのログ収集で使用されるFTPS接続のSSL/TLSプロトコルのバージョンを変更する場合

   ```
   # ismadm security enable-tls-ftp ＜利用を許可するバージョン＞
   ```

   コマンド実行時に、利用を許可するバージョンをカンマ区切り(空白なし)で指定してください。

   指定可能なバージョン:SSLv3, TLSv1, TLSv1.1, TLSv1.2

   ただし、ISM 2.9.0.030以降は、FTPS接続のTLSv1を除きます。

   注意

   Windows OSでログ収集およびOnlineアップデートをする際は、TLSv1.2を有効にしておく必要があります。

   実行例:GUI／REST接続の利用を許可するバージョンにTLSv1.1、TLSv1.2を設定する場合

   ```
   # ismadm security enable-tls TLSv1.1,TLSv1.2
   You need to reboot the system to enable the new settings.
   Immediately reboots the system.  [y/n]:
   ```

   コマンド終了後に、再起動するかどうかを確認するメッセージが表示されます。
3. 「y」を入力してISM-VAを再起動します。

   再起動完了後に指定したSSL/TLSプロトコルのバージョンが有効になります。指定しなかったバージョンは無効になります。

4.21 暗号スイート設定の変更

GUI/REST接続とFTPS接続の、暗号スイートタイプを設定できます。

暗号スイートタイプは、以下の値を設定できます。

設定値	OpenSSLでの相当の暗号スイート設定 [注]	備考
1	HIGH、MEDIUM(ただし aNULL除外、MD5除外)	
2	HIGH(ただし SHA1除外、aNULL除外)	
3	HIGH	デフォルト値

[注]:OpenSSLでの相当の暗号スイート設定は、以下のとおりです。

- HIGH:鍵長が128bit以上の暗号を使用します。
- MEDIUM:鍵長が128bitの暗号を使用します。
- aNULL:匿名のための認証を行わない暗号設定です。

詳細は、OpenSSLのマニュアルの『CIPHER STRINGSのリスト』を参照してください。

1. コンソールからadministratorでISM-VAにログインします。

2. 暗号スイート設定コマンドを実行します。

   ー GUI／REST接続の暗号スイートを変更する場合

   ```
   # ismadm security set-sslcipher 1
   ```

   ー FTPS接続の暗号スイートを変更する場合

   ```
   # ismadm security set-sslcipher-ftp 1
   ```

   ただし、ISM 2.9.0.030以降は、FTPS接続の暗号スイートを変更できません。

注意

コマンド終了後に、HTTPサーバーは自動で再起動します。そのため、GUIなどで通信中の場合通信が途切れることがあります。

4.22 他ソフトウェア連携設定

他ソフトウェア連携時に使用する証明書を登録できます。

1. 証明書を転送します。

   転送先:/Administrator/ftp/software/cert

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. コンソールからadministratorでISM-VAにログインします。

3. 他ソフトウェア連携用証明書の登録コマンドを実行します。

   ```
   # ismadm security import-software-cert -software ＜ソフトウェア名＞ -type ＜ipv4、ipv6またはfqdn＞ -server ＜ソフトウェアをインストールしたサーバーのIPアドレスまたはFQDN＞ -file ＜証明書ファイル名＞
   ```

   指定できるソフトウェア名は以下のとおりです。

他ソフトウェアの種類	softwareに指定するソフトウェア名
Trend Micro Deep Security	TrendMicroDeepSecurity

注意

- Trend Micro Deep Security連携で使用する証明書は、Webブラウザーの証明書のエクスポートウィザードから「Base 64 encoded X.509(.CER)」を選択して取得してください。「Base 64 encoded X.509(.CER)」以外を選択して取得した証明書は使用できません。
- Trend Micro Deep Security連携で使用する証明書を登録するためには、ウィジェットにTrend Micro Deep Securityの情報が設定されている必要があります。

ポイント

ISM-VAに登録された他ソフトウェア連携用証明書を表示／削除する場合は、以下のコマンドを実行します。

- 他ソフトウェア連携用証明書表示

  ```
  # ismadm security show-software-cert -software ＜ソフトウェア名＞
  ```

・ 他ソフトウェア連携用証明書削除

```
# ismadm security delete-software-cert -software ＜ソフトウェア名＞ -type ＜ipv4、ipv6またはfqdn＞ -server ＜ソフトウェアをインストールしたサーバーのIPアドレスまたはFQDN＞
```

4.23 GUIを使用したファイルアップロード

ISMの各機能で使用するファイルを、GUIを使用してISM-VAのファイル保存先へアップロードおよび削除できます。

・ ファイルの保存先は、FTPによるアップロードの保存先と同じです。詳細については「2.1.2 FTPアクセス」を参照してください。

・ ファイルのアップロード方法は、『操作手順書』の「1.4.1 ISM-VAにファイルをアップロードする」を参照してください。

ポイント

GUIを使用した場合、以下の作業はできません。FTPを使用して実施ください。

・ ファイル保存先のファイルのダウンロード

・ ファイル保存先のディレクトリーの新規作成、名称変更、および削除

注意

アップロードするファイル名、ディレクトリー名に以下の文字が含まれる場合、FTPでアップロードしてください。ファイル名、ディレクトリー名に以下の文字を含まない場合、GUIを使用したアップロードができます。

[使用できない文字]

・ %（半角パーセント）

・ &（半角アンパーサンド）

・ '（半角シングルクォーテーション）

・ `（半角バッククォート）

・ "（半角ダブルクォーテーション）

ファイル名やディレクトリー名に上記の文字が含まれていると、GUIを使用したファイルアップロードはエラー（メッセージID：50990004または50190263）となります。

4.24 プロファイルのベリファイ有効化／無効化設定

プロファイルのベリファイ機能を有効化、または無効化します。

・ 無効化する場合

  ― 定期的な自動実行、および手動のプロファイルのベリファイが無効となります。

  ― プロファイルのベリファイの対象となるプロファイルの[ベリファイステータス]が[-（ハイフン）]と表示されます。

・ 有効化する場合

  ― 定期的な自動実行、および手動のプロファイルのベリファイが有効となります。

  ― プロファイルのベリファイの対象となるプロファイルの[ベリファイステータス]が[ベリファイ失敗]と表示されます。定期的な自動実行、または手動で実行することで、適切な[ベリファイステータス]が設定されます。

1. コンソールからadministratorでISM-VAにログインします。
2. ISMのサービスを停止します。詳細は、「4.1.4 ISMのサービス起動と停止」を参照してください。

3. プロファイルのベリファイ有効化／無効化設定コマンドを実行します。

   ー 有効化する場合

```
# ismadm system set-profile-verify enable
```

   ー 無効化する場合

```
# ismadm system set-profile-verify disable
```

4. ISMのサービスを起動します。詳細は、「4.1.4 ISMのサービス起動と停止」を参照してください。

4.25 プロファイルのベリファイ有効化／無効化状態表示

プロファイルのベリファイ機能の有効化／無効化状態を表示します。

1. コンソールからadministratorでISM-VAにログインします。
2. プロファイルのベリファイ有効化／無効化状態表示コマンドを実行します。

```
# ismadm system show-profile-verify
```

コマンド出力（※部以降の文言は、実際の画面には表示されません。）

```
Profile verify status: enable      ※プロファイルのベリファイは有効です。
Profile verify status: disable     ※プロファイルのベリファイは無効です。
```

4.26 ネットワーク接続のセキュリティ設定

ネットワーク接続のセキュリティを強化できます。

4.26.1 SSHセキュリティ設定

以下の設定変更および状態表示できます。

- SSHログイン失敗時のロック設定

  一定期間内に5回ログインを失敗しているユーザーはロック状態になりSSH接続ができなくなります。GUIやftpへのログインは本設定の影響を受けません。

- SSH接続元IPアドレス制限

  外部からISM-VAの22/TCPポートへの接続を制限します。

- SSHキーボードインタラクティブ認証設定

  デフォルトのパスワード認証方式を、よりセキュリティの高いキーボードインタラクティブ認証方式に変更します。

  多要素認証を使用する場合は、有効に設定する必要があります。

- SSH公開鍵接続設定

  公開鍵ベースのSSH認証方式を使用するための設定をします。設定後も、ユーザーID／パスワードを使用してログインできます。

- コンソール自動ログアウト設定

  SSH接続またはハイパーバイザーのコンソールからログインした際、一定時間無操作が続いた場合に自動的にログアウトする時間（分）を設定できます。

SSHセキュリティ設定確認

SSH接続元IPアドレス制限／SSHログイン失敗時のロック／SSHキーボードインタラクティブ認証の各設定を確認できます。各設定は、設定変更後にログインしたユーザーに対して適用されます。

```
# ismadm security show-ssh-conf
```

実行例:

```
# ismadm security show-ssh-conf
client ip address limitation : enable
client ip address to use : 192.168.2.20,192.168.1.0/24
userlock at login failure : enable
keyboard-interactive authentication : enable
```

15分間で5回ログインを失敗するとロックされSSH接続ができなくなります。ロックの解除は「SSHログイン失敗ユーザーロック解除」コマンドを使用してロックを解除してください。

SSHセキュリティ設定

SSHログイン失敗時のロック／SSH接続元IPアドレス制限／SSHキーボードインタラクティブ認証の有効／無効設定できます。

- SSH接続元IPアドレス制限設定

```
# ismadm security set-ssh-conf -iplimit [enable or disable]
```

- SSHログイン失敗時のロック設定

```
# ismadm security set-ssh-conf -userlock [enable or disable]
```

- SSHキーボードインタラクティブ認証設定

```
# ismadm security set-ssh-conf -keyboard [enable or disable]
```

SSHログイン状態表示

一定期間内でのユーザー毎のSSHログインの履歴が表示されます。正しいパスワードでログインできず、かつログイン履歴が残っている場合はロックされていますので、「ismadm security reset-ssh-userlock」コマンドでロックを解除してください。

```
# ismadm security show-ssh-loginfail
```

ユーザー名および以下の項目が出力されます。

表4.5 コマンド出力結果の説明

項目	説明
When	ログイン日時
Type	接続タイプ(”RHOST”固定)
Source	接続元
Valid	”V”または”I”表示(内部情報)

SSHログイン失敗ユーザーロック解除

SSHログイン失敗でロックされたユーザーのロックを解除できます。

```
# ismadm security reset-ssh-userlock -user ＜ユーザー名＞
```

本コマンドはハイパーバイザーのコンソールまたは、ロック状態ではないAdministratorユーザーグループAdministratorロールのユーザーが実行できます。

SSH接続元IPアドレス追加

SSH接続元IPアドレス制限機能が有効な場合に接続許可するIPアドレスまたはサブネットを追加できます。

```
# ismadm security add-ssh-clientip -ip ＜IPアドレス or サブネット＞
```

IPアドレス指定例: 192.168.1.250

サブネット指定例: 192.168.1.0/24 [ネットマスクのビット値込みで指定]

SSH接続元IPアドレス削除

SSH接続元IPアドレス制限機能が有効な場合に接続許可するIPアドレスまたはサブネットを削除できます。

```
# ismadm security delete-ssh-clientip [-ip ＜IPアドレス or サブネット＞] [-all]
```

IPアドレス指定例: 192.168.1.250

サブネット指定例: 192.168.1.0/24 [ネットマスクのビット値込みで指定]

-all指定:一括削除

-ipまたは-allのいずれかを指定してください。

SSH公開鍵登録

登録できる公開鍵はRFC4716形式、またはOpenSSH形式の公開鍵です。公開鍵は、Tera Term／PuTTY／OpenSSHなどのSSHツールで作成できます。SSH接続するユーザーごとに以下の方法で公開鍵を作成してください。

- Tera Termを使用する場合は、「鍵生成」機能の「公開鍵の保存」で出力されるファイルを使用。
- PuTTYを使用する場合は、puttygenコマンドの「Save public key」で出力されるファイルを使用。
- OpenSSHを使用する場合は、ssh-keygenコマンドで出力される「*.pub」形式のファイルを使用。

セキュリティ上問題があるため、RSA1形式で作成された公開鍵は使用できません。

1. SSH公開鍵ファイルを以下のファイル名に変更し、ISM-VAへ転送します。

   ファイル名:sshkey_＜SSH接続するユーザー名＞.pub

   転送先:/Administrator/ftp

   GUIでの転送方法は、「4.23 GUIを使用したファイルアップロード」を参照してください。

   FTPでの転送方法は、「2.1.2 FTPアクセス」を参照してください。

2. SSH公開鍵を登録するユーザーでコンソールにログインし、SSH公開鍵登録コマンドを実行します。

   ```
   # ismadm security set-ssh-pubkey
   ```

   実行例:

   ```
   # ismadm security set-ssh-pubkey
   User name       : administrator
   Import key file : /Administrator/ftp/sshkey_administrator.pub
   Fingerprint     : RSA 2048 SHA256:*********************************************
   Import SSH public key? [y/n]: y
   Public key import succeeded.
   ```

SSH公開鍵表示

SSH公開鍵を表示するユーザーでコンソールにログインし、SSH公開鍵表示コマンドを実行します。

```
# ismadm security show-ssh-pubkey
```

実行例:

```
# ismadm security show-ssh-pubkey
User name   : administrator
Fingerprint : RSA 2048 SHA256:*********************************************
```

SSH公開鍵削除

SSH公開鍵を削除するユーザーでコンソールにログインし、SSH公開鍵削除コマンドを実行します。

```
# ismadm security delete-ssh-pubkey
```

実行例:

```
# ismadm security delete-ssh-pubkey
User name   : administrator
Fingerprint : RSA 2048 SHA256:*****************************************
Delete SSH public key? [y/n]: y
Public key delete succeeded.
```

コンソール自動ログアウト設定確認

ユーザーがSSHまたはハイパーバイザーのコンソールにログイン後、一定時間無操作が続いた場合に自動的にログアウトする時間(分)を確認できます。

```
# ismadm security show-console-timeout
```

実行例:

```
# ismadm security show-console-timeout
Console login timeout: 30 (minute)
```

コンソール自動ログアウト設定

ユーザーがSSHまたはハイパーバイザーのコンソールにログイン後、一定時間無操作が続いた場合に自動的にログアウトする時間(分)を設定できます。設定時間は、設定変更後にログインしたユーザーに対して適用されます。

```
# ismadm security set-console-timeout -time <タイムアウト時間（分）>
```

デフォルト:30分

設定可能時間:2～60分

実行例:

```
# ismadm security set-console-timeout -time 60
Console login timeout: 60 (minute)
```

4.26.2 ISM通信ポートの制限

以下の設定変更、および状態表示できます。

- GUI／REST接続元IPアドレス制限

  外部からISM-VAのGUIポート(デフォルト:25566/TCPポート)への接続を制限できます。

- Samba接続元IPアドレス制限

  外部からISM-VAの445/TCPポートへの接続を制限できます。

- FTP接続元IPアドレス制限

  外部からISM-VAの21/TCPポートへの接続を制限できます。

- TFTP接続元IPアドレス制限

  外部からISM-VAの69/UDPポートへの接続を制限できます。

- 9213ポート接続元IPアドレス制限

  外部からISM-VAの9213/TCPポートへの接続を制限できます。

- SNMPトラップ接続元IPアドレス制限

  外部からISM-VAの162/UDPポートへの接続を制限できます。

・ HTTPSデータ接続元IPアドレス制限

外部からISM-VAの25613/TCPポートへの接続を制限できます。

・ SSDP接続元IPアドレス制限

外部からISM-VAの1900/UDPポートへの接続を制限できます。

ISM通信ポートセキュリティ設定確認

ISM通信ポート接続元IPアドレス制限設定を確認できます。

・ GUI／REST接続元IPアドレス制限確認

```
# ismadm security show-gui-conf
```

・ Samba接続元IPアドレス制限確認

```
# ismadm security show-smb-conf
```

・ FTP接続元IPアドレス制限確認

```
# ismadm security show-ftp-conf
```

・ TFTP接続元IPアドレス制限確認

```
# ismadm security show-tftp-conf
```

・ 9213ポート接続元IPアドレス制限確認

```
# ismadm security show-svs-conf
```

・ SNMPトラップ接続元IPアドレス制限確認

```
# ismadm security show-snmp-conf
```

・ HTTPSデータ接続元IPアドレス制限確認

```
# ismadm security show-https-data-conf
```

・ SSDP接続元IPアドレス制限確認

```
# ismadm security show-ssdp-conf
```

実行例:

```
# ismadm security show-gui-conf
client ip address limitation : enable
client ip address to use : 192.168.2.20,192.168.1.0/24
```

ISM通信ポートセキュリティ設定

ISM通信ポート接続元IPアドレス制限の有効／無効を設定できます。有効／無効を切り替えた場合、設定後に接続される通信に対して適用されます。

・ GUI／REST接続元IPアドレス制限設定

```
# ismadm security set-gui-conf -iplimit [enable or disable]
```

・ Samba接続元IPアドレス制限設定

```
# ismadm security set-smb-conf -iplimit [enable or disable]
```

・ FTP接続元IPアドレス制限設定

```
# ismadm security set-ftp-conf -iplimit [enable or disable]
```

・ TFTP接続元IPアドレス制限設定

```
# ismadm security set-tftp-conf -iplimit [enable or disable]
```

・ 9213ポート接続元IPアドレス制限設定

```
# ismadm security set-svs-conf -iplimit [enable or disable]
```

・ SNMPトラップ接続元IPアドレス制限設定

```
# ismadm security set-snmp-conf -iplimit [enable or disable]
```

・ HTTPSデータ接続元IPアドレス制限設定

```
# ismadm security set-https-data-conf -iplimit [enable or disable]
```

・ SSDP接続元IPアドレス制限設定

```
# ismadm security set-ssdp-conf -iplimit [enable or disable]
```

ISM通信ポート接続元IPアドレス追加

ISM通信ポート接続元IPアドレス制限機能が有効な場合に、接続許可するIPアドレスまたはサブネットを追加できます。IPアドレスまたはサブネットは、カンマ区切りで複数指定できます。

「ISM通信ポートセキュリティ設定」で接続元IPアドレス制限設定が有効(enable)の場合は、追加したIPアドレスまたはサブネットの接続は、即時に可能となります。

・ GUI／REST接続元IPアドレス追加

```
# ismadm security add-gui-clientip -ip ＜IPアドレス or サブネット＞
```

・ Samba接続元IPアドレス追加

```
# ismadm security add-smb-clientip -ip ＜IPアドレス or サブネット＞
```

・ FTP接続元IPアドレス追加

```
# ismadm security add-ftp-clientip -ip ＜IPアドレス or サブネット＞
```

・ TFTP接続元IPアドレス追加

```
# ismadm security add-tftp-clientip -ip ＜IPアドレス or サブネット＞
```

・ 9213ポート接続元IPアドレス追加

```
# ismadm security add-svs-clientip -ip ＜IPアドレス or サブネット＞
```

・ SNMPトラップ接続元IPアドレス追加

```
# ismadm security add-snmp-clientip -ip ＜IPアドレス or サブネット＞
```

・ HTTPSデータ接続元IPアドレス追加

```
# ismadm security add-https-data-clientip -ip ＜IPアドレス or サブネット＞
```

・ SSDP接続元IPアドレス追加

```
# ismadm security add-ssdp-clientip -ip ＜IPアドレス or サブネット＞
```

IPアドレス指定例: 192.168.1.250

サブネット指定例: 192.168.1.0/24 [ネットマスクのビット値込みで指定]

ISM通信ポート接続元IPアドレス削除

ISM通信ポート接続元IPアドレス制限機能が有効な場合に、接続許可するIPアドレスまたはサブネットを削除できます。IPアドレスまたはサブネットは、カンマ区切りで複数指定できます。

「ISM通信ポートセキュリティ設定」で接続元IPアドレス制限設定が有効(enable)の場合は、削除したIPアドレスまたはサブネットの接続は、即時に不可能となります。

- GUI／REST接続元IPアドレス削除

```
# ismadm security delete-gui-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- Samba接続元IPアドレス削除

```
# ismadm security delete-smb-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- FTP接続元IPアドレス削除

```
# ismadm security delete-ftp-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- TFTP接続元IPアドレス削除

```
# ismadm security delete-tftp-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- 9213ポート接続元IPアドレス削除

```
# ismadm security delete-svs-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- SNMPトラップ接続元IPアドレス削除

```
# ismadm security delete-snmp-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- HTTPSデータ接続元IPアドレス削除

```
# ismadm security delete-https-data-clientip [-ip <IPアドレス or サブネット>] [-all]
```

- SSDP接続元IPアドレス削除

```
# ismadm security delete-ssdp-clientip [-ip <IPアドレス or サブネット>] [-all]
```

IPアドレス指定例: 192.168.1.250

サブネット指定例: 192.168.1.0/24 [ネットマスクのビット値込みで指定]

-all指定:一括削除

-ipまたは-allのいずれかを指定してください。

4.26.3 ISMセッション認証の設定

ISMセッション認証とは、GUIのログイン認証またはREST APIのセッション認証のことです。

ISMセッション認証のIPアドレス制限設定を有効にした場合、ISMセッション認証時、ログイン時と同一のIPアドレスからのアクセスに限定できます。

ISMセッション認証のIPアドレス制限設定確認

ISMセッション認証のIPアドレス制限設定を確認できます。

```
# ismadm security show-ismauth-conf
```

実行例:

```
# ismadm security show-ismauth-conf
source ip address limitation : enable
```

ISMセッション認証のIPアドレス制限設定変更

ISMセッション認証のIPアドレス制限設定の有効／無効を設定できます。

```
# ismadm security set-ismauth-conf -iplimit [enable or disable]
```

4.27 中継ルートのポート番号

中継ルートは、iRMCログインを行う際の中継用の経路です。中継ルートにはポートを割り当てられます。

中継ルートに割り当てられているポート番号の確認や割り当ての変更ができます。

デフォルトのポート番号は、以下です。

中継ルート番号(id)	ポート番号(port) (デフォルト設定)
1	63000
2	63001
3	63002

4.27.1 中継ルートのポート番号の確認

iRMCログインで使用する中継ルートのポート番号を表示できます。

1. コンソールからadministratorでISM-VAにログインします。
2. 以下のコマンドを実行し、中継ルートのポート番号を表示します。

   ```
   # ismadm relayroute port-show
   ```

   実行例:

   ```
   # ismadm relayroute port-show
   id    port
   1     63000
   2     63001
   3     63002
   ```

4.27.2 中継ルートのポート番号の変更

iRMCログインで使用する中継ルートのポート番号を変更する必要がある場合は、以下の方法により設定変更できます。

設定可能なポート番号の範囲は、50000～63999です。

1. コンソールからadministratorでISM-VAにログインします。
2. 以下のコマンドを実行し、中継ルートのポートを設定します。

   ```
   # ismadm relayroute port-change -id ＜中継ルート番号＞ -port ＜ポート番号＞
   ```

   実行例:

   ```
   # ismadm relayroute port-change -id 1 -port 53000
   ```

注意

iRMCログインで使用中の中継ルートのポート番号を変更した場合、iRMCとの通信が切断されます。GUIから再度iRMCログインを実施してください。

4.28 中継ルート用クライアント証明書の作成

中継ルート用のクライアント証明書は、ISM-VAが発行する中継ルートアクセスに対する証明書です。

中継ルートを使用するには、中継ルート用のクライアント証明書をあらかじめ管理端末にインストールします。

4.28.1 クライアント証明書の作成

ISM-VAに中継ルート用のクライアント証明書を作成する手順は、以下のとおりです。

1. コンソールからadministratorでISM-VAにログインします。
2. クライアント証明書の作成コマンドを実行します。

   ー パスワードなしで作成する場合

   ```
   # ismadm relayroute clientcert-create
   ```

   ー パスワードありで作成する場合

   ```
   # ismadm relayroute clientcert-create -password
   Enter Export Password: ＜パスワード入力＞
   Verifying - Enter Export Password: ＜確認パスワード入力＞
   ```

   クライアント証明書ファイル（PKCS#12形式：拡張子「.p12」）が以下に出力されます。

   /Administrator/ftp/relayroute/ism_relay_client.p12

注意

- 中継ルートを複数の管理端末用に設定した場合でも、クライアント証明書は共通です。ISM-VAでの作成は、1度だけです。ISM-VAでクライアント証明書を再作成した場合、それまでのクライアント証明書は無効になります。
- デバイスにiPad、Webブラウザーに Safariを使用する場合は、クライアント証明書に必ずパスワードを設定してください。

4.28.2 中継ルート用クライアント証明書のダウンロード

ISM-VAで作成した中継ルート用クライアント証明書は、FTPまたはHTTPSで管理端末にダウンロードします。

FTPでのダウンロード

以下のクライアント証明書ファイルをFTPでダウンロードできます。

/Administrator/ftp/relayroute/ism_relay_client.p12

HTTPSでのダウンロード（curlコマンドを使用）

以下のURLからクライアント証明書ファイルをダウンロードできます。

https://＜ISM-VAのIPアドレス＞:25566/ism/data/export/Administrator/transfer/ism_relay_client.p12

実行例：curlコマンドがインストールされたLinuxサーバー上でダウンロードする場合

```
# curl -O "https://192.168.10.20:25566/ism/data/export/Administrator/transfer/ism_relay_client.p12"
--cacert /tmp/certificate.crt
-b "X-Ism-Authorization=123456789"
```

注意

- クライアント証明書ファイルをFTP転送する際は、バイナリモードで転送してください。

- curlコマンドを使用してクライアント証明書ファイルをダウンロードする場合、HTTPS通信を行うための認証操作が必要です。認証操作については、『REST API リファレンスマニュアル』の「3.1 認証」を参照してください。

4.28.3 中継ルート用クライアント証明書のインストール

ダウンロードしたクライアント証明書を管理端末へインストールします。

インストールする手順は、以下のとおりです。使用するデバイス、Webブラウザーに応じて手順は異なります。

デバイス：パソコン、サーバーまたはWindowsタブレット、Webブラウザー：Microsoft EdgeまたはGoogle Chromeの場合

手順はWindows OSのバージョンに応じて変わる可能性があります。以下はWindows 10での手順です。

1. ダウンロードしたクライアント証明書をダブルクリックまたはダブルタップし、証明書のインポートウィザードを起動します。保存場所を選択して[次へ]を選択します。保存場所は任意です。
2. [インポートする証明書ファイル]でファイル名にism_relay_client.p12が指定されていることを確認し、[次へ]を選択します。
3. パスワードが設定されているクライアント証明書の場合は、[秘密キーの保護]でパスワードを入力し、インポートオプションは変更せずに[次へ]を選択します。
4. [証明書ストア]で、[証明書の種類に基づいて、自動的に証明書ストアを選択する]を選択し、[次へ]を選択します。
5. [証明書のインポートウィザードの完了]で[完了]を選択します。

デバイス：パソコン、サーバーまたはWindowsタブレット、Webブラウザー：Mozilla Firefoxの場合

手順はMozilla Firefoxのバージョンに応じて変わる可能性があります。以下はバージョン113.0（64ビット）での手順です。

1. Mozilla Firefoxのメニューから[設定]を選択します。
2. [プライバシーとセキュリティ]から[セキュリティ]-[証明書]の[証明書を表示]を選択します。

   証明書マネージャーが起動します。
3. [インポート]からism_relay_client.p12 を選択し、[開く]を選択します。
4. パスワードが設定されているクライアント証明書の場合は、[パスワードを入力してください]でパスワードを入力し、[ログイン]を選択します。
5. [あなたの証明書]タブに、証明書名が「ISM RELAY ROUTE CLIENT」の証明書が追加されたことを確認し、[OK]を選択します。

デバイス：Androidタブレット、Webブラウザー：Google Chromeの場合

手順はAndroid OSのバージョンに応じて変わる可能性があります。以下はAndroid OS 11での手順です。

1. ホーム画面で[設定]アイコンをタップします。
2. [セキュリティ]-[暗号化と認証情報]-[証明書のインストール]-[VPNとアプリユーザー証明書]の順にタップします。
3. ism_relay_client.p12をタップします。
4. パスワードが設定されているクライアント証明書の場合は、[証明書を抽出]でパスワードを入力し、[OK]をタップします。
5. 必要に応じて証明書名を変更して、[OK]をタップします。

デバイス：iPad、Webブラウザー：Safariの場合

手順はiOSのバージョンに応じて変わる可能性があります。以下はiOS 13での手順です。

1. ホーム画面で[設定]アイコンをタップします。
2. [一般]-[プロファイル]をタップします。
3. [ID証明書: 1]を選択して[インストール]をタップします。
4. [パスコードを入力]にパスコードを入力し、[完了]をタップします（パスコードはiPadのロック解除に使用するコードです）。
5. [警告]で[インストール]をタップします。続いて表示される画面で[インストール]をタップします。
6. [パスワードを入力]でパスワードを入力し、[次へ]をタップします。
7. [完了]をタップします。

4.28.4 中継ルート用クライアント証明書の表示

ISM-VAで作成した中継ルート用クライアント証明書を表示します。

1. コンソールからadministratorでISM-VAにログインします。
2. クライアント証明書表示コマンドを実行します。

```
# ismadm relayroute clientcert-show
```

第5章 ノードの保守

この章では、ノードの保守を説明します。

5.1 メンテナンスモード

ノードの故障が検出されてノードの保守作業を行う場合、ISM上で対象ノードをメンテナンスモードに変更することをお勧めします。

メンテナンスモードに変更されたノードに対しては、ISMのアラーム検出およびバックグラウンドでの処理が抑止されるため、故障したノードで何度もアラームが発生することを防止できます。

メンテナンスモード中のISMの動作は以下のとおりです。

影響を受ける機能	メンテナンスモード中の動作
センサーしきい値監視	センサー状態の取得が停止します。
SNMPトラップの監視	トラップは受信され、トラップログに入りますが、アラームは発生しません。
ノード情報取得	ISMが定期的に実行するノード情報取得は停止します。 必要に応じて、ノード情報取得を手動で実行してください。
ノードログ収集	スケジュール設定されたログ収集はスキップされます。 必要に応じて、ノードログ収集を手動で実行してください。
アノマリ検知	開始しているアノマリ検知機能を停止します。

ポイント

メンテナンスモード中でも、上記以外の機能は利用可能です。例えば、メンテナンスモードになっているノードに対しても、以下の操作は実行できます。

- プロファイルの適用、再適用、適用解除
- ファームウェアアップデート
- 手動ノード情報取得
- 手動ノードログ収集

メンテナンスモード設定手順

1. ノードの詳細画面を表示します。
2. [アクション]ボタンから[メンテナンスモード設定]を選択します。

   確認画面が表示されるので、ノード名を確認して[はい]を選択します。

メンテナンスモード解除手順

1. ノードの詳細画面を表示します。
2. [アクション]ボタンから[メンテナンスモード解除]を選択します。

注意

- PRIMEQUEST 4000シリーズを除き、PRIMEQUESTをメンテナンスモード設定／解除すると、配下のパーティションおよび拡張パーティションもメンテナンスモード設定／解除されます。パーティションおよび拡張パーティションを指定してメンテナンスモード設定／解除することはできません。

- PRIMERGY CXシリーズおよびPRIMEQUEST 4000シリーズの場合、シャーシに対してメンテナンスモード設定／解除を実行しても、シャーシの配下に属するノードのメンテナンスモードは設定／解除されません。シャーシの配下に属するノードを指定してメンテナンスモード設定／解除を実行してください。

  なお、PRIMERGY CXシリーズ、PRIMEQUEST 4000シリーズのシャーシ自体は機能を持たないため、ISMはシャーシに対して処理を抑止することはしません。このため、シャーシに対してメンテナンスモード設定／解除を実行する必要はありません。

- VCS Fabric（Brocade VCS Fabric）をメンテナンスモード設定／解除すると、配下のVDXファブリックスイッチもメンテナンスモード設定／解除されます。VDXファブリックスイッチを指定してメンテナンスモード設定／解除することはできません。

5.2 エラー発生時の調査方法

ISMでは、ノード単位での障害検出を行っています。

[イベント]-[イベント]-[運用ログ]に記載されているものよりも詳細な情報については、各機器にアクセスして調べる必要があります。各機器のWebUIのSELログや部品情報などを確認してエラー要因を特定してください。

5.3 保守部品交換時の作業

ノードの保守部品を交換する場合、交換部品に応じて作業手順が異なります。

以下の作業例を参考に、交換部品に応じた手順を実施してください。

表5.1 保守部品に応じた交換方法

保守部品の交換方法	装置状態	交換部品例
A：ホットプラグ可能な部品の交換	装置の監視は継続	HDD、SSD
B：OSをシャットダウンして交換	iRMCは停止しない	LANカード、RAIDカード、ソフトウェア／ドライバー／BIOSのアップデート
C：装置の電源をオフして交換	iRMCは停止するが記憶領域保持	電源ユニット、FAN、iRMCファームウェアのアップデート
D：物理的な交換	iRMCは停止し、記憶領域保持なし	サーバー装置、システムボード

保守部品交換時の作業フロー

保守部品の交換方法（A～D）は、上記の表を参照ください。

凡例：◎ = 必須、○ = 必要に応じて実施

作業順	作業先	装置に対する操作	説明	保守部品の交換方法			
				A	B	C	D
1	ISM	ハードウェア設定バックアップ 「2.10 ハードウェア設定バックアップ／リストア機能」	装置のBIOS／iRMCの設定値を装置から取得してISMに保持します。 システムボードの交換時に有効です。				◎
2	ISM	ノードのメンテナンスモード設定 「5.1 メンテナンスモード」	ISMの監視動作（定期ノード情報取得、ログ収集、アノマリ検知）を停止します。メンテンナンスモード設定中は、SNMPトラップを受信しますが、受信時のアラーム通知は行われません。 ノードのメンテナンスモード設定はISM側の設定であり、装置側の状態は変わりません。	◎	◎	◎	○
3	ISM	プロファイル適用解除 「2.4.2.5 プロファイルの適用解除と削除」	プロファイル解除はプロファイルで設定した装置設定情報（iRMC、BIOS、仮想IO、RAID設定）のうち、仮想IO設定のみ元に戻します。 また、定期的なプロファイルのベリファイは実施されなくなります。				◎

作業順	作業先	装置に対する操作	説明	保守部品の交換方法			
				A	B	C	D
			ノード登録情報とプロファイルの不整合を防ぐために必要となります。				
4	ISM	登録ノードの削除 「2.2.4 データセンター／フロア／ラック／ノードの削除」	装置をISMの監視対象から外します。 保守部品交換において、登録ノードの削除操作は必須ではありません。登録ノードの削除は、登録状態・監視状態の不整合をリセットする目的で実施します。PRIMERGYサーバーのノードで部品交換した際、交換の前後で以下が同じ場合は、ノードの削除、再登録は不要となります。 ・ PRIMERGYモデル ・ iRMCのIPアドレス／ユーザー／パスワード				○
5	ISM	プロファイル削除 「2.4.2.5 プロファイルの適用解除と削除」	作成済みのプロファイルをISMから削除します。 プロファイル設定内容が大幅に変更となる場合は、削除して作成し直すことが有効です。 登録ノードを削除し、プロファイルが残っていた場合は、必ずプロファイルを削除します。				○
6	装置	保守部品交換作業の実施 周辺機器の電断などを含む詳しい手順に関しては装置のメンテナンスマニュアルに従って実施してください。	交換部品の種類によっては、以下の作業が必要です。 ・ OSのシャットダウン／起動 ・ 電源プラグ切断／接続 保守部品交換の後にOSの再インストールが必要な場合は、プロファイルの再適用で実施します。	◎	◎	◎	◎
7	装置	iRMCのIPアドレス設定	装置側のiRMCのIPアドレスを設定します。 ノード登録によりiRMCのIPアドレスは、ISM側に登録されています。ISM側の設定は不要です。				◎
8	ISM	ハードウェア設定リストア 「2.10 ハードウェア設定バックアップ／リストア機能」	ハードウェア設定バックアップを行った場合、リストアによりISMからハードウェア設定を復元します。 ハードウェア設定リストア後のiRMC再起動は不要です。				◎
9	ISM	ノード再登録 「2.2.1 データセンター／フロア／ラック／ノードの登録」	登録ノードを削除した場合は、必ずノードを再登録します。 ノード登録を削除していなければ、ノード登録は不要です。				○
10	ISM	プロファイル再作成 「プロファイルの作成」 「2.4.2.4 プロファイルの編集と再適用」	プロファイルを再作成、または設定値を見直します。 プロファイルを削除した場合は、必ず再作成します。プロファイルを削除していなければ、プロファイル再作成は不要です。 必要に応じてプロファイルの設定内容を見直します。				○
11	ISM	ノード情報取得 「2.2.1.3 ノード情報の管理」	保守部品交換後に、必ず手動でノード情報取得を行います。ノード登録された装置の状態情報、装置の構成情報（CPU、DIMM、OS、拡張カード実装情報、ステータス情報）を取得します。 通常はノード登録された装置に対し、1日1回ISMはiRMCから情報取得しています。	◎	◎	◎	◎
12	ISM	プロファイルの再適用	プロファイルを解除した場合は、プロファイルの再適用は必須です。				◎

作業順	作業先	装置に対する操作	説明	保守部品の交換方法			
				A	B	C	D
		「2.4.2.4 プロファイルの編集と再適用」	プロファイルを解除していない場合でも、プロファイルのベリファイで不一致があれば再適用します。				
13	ISM	ノードのメンテナンスモード設定解除 「5.1 メンテナンスモード」	ノードのメンテナンスモードを設定した場合は、設定を解除します。	◎	◎	◎	○

付録A　ノードを管理・運用するための環境設定詳細

ISMの機能を利用するうえで必要な事前設定、環境設定の情報と、管理・運用の対象となるノードの設定や参考情報などを提供します。

A.1　ISMの動作環境設定

ISMの機能を使用するうえで必要な環境設定と注意点を説明します。

A.1.1　プロファイル管理機能・ファームウェア管理機能使用時のDHCP／PXE設定

下記の機能を使用する場合は、PXEブート機能を利用します。

- プロファイル管理機能で、サーバーへOSをインストールする
- ファームウェア管理機能で、サーバーまたは搭載PCIカードのOfflineアップデートを実行する。

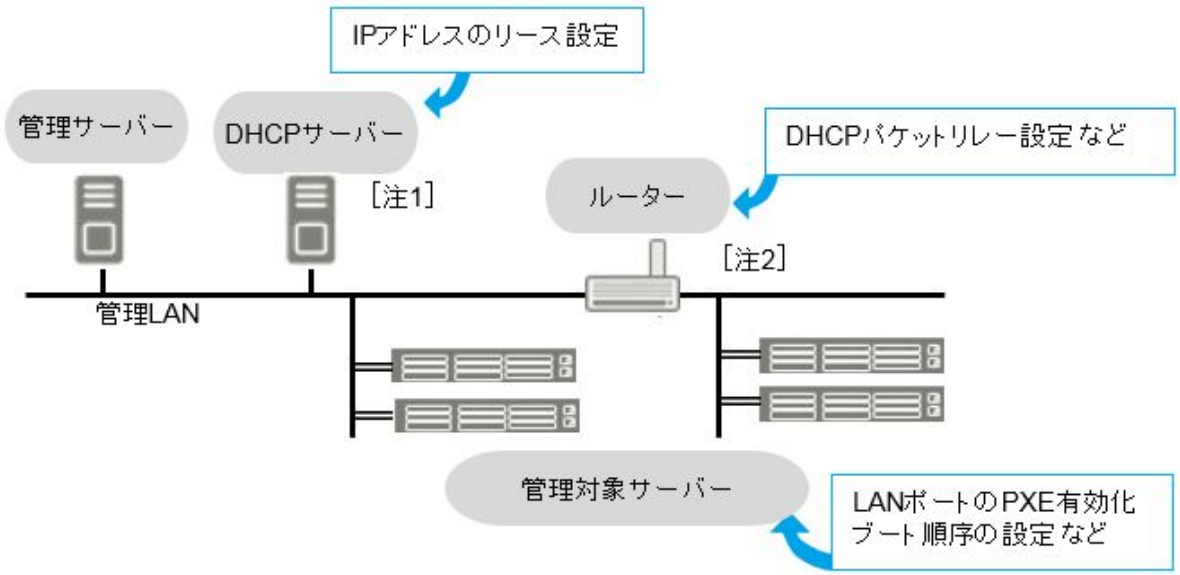
PXEブートを正しく動作させるためには、事前に管理対象サーバー（ノード）およびネットワーク構成について適切な準備が必要です。ここではPXEブートに必要な作業について情報を提供します。

なお、OSインストール以外のプロファイル適用や、ファームウェアのOnlineアップデートの実行については、本作業は不要です。

ネットワーク構成例

以下にPXEブート機能利用時のネットワーク構成例と主な事前準備作業を示します。

図A.1 ネットワーク構成例



[注1]: 外部にDHCPサーバーを用意する代わりに、ISM-VA（管理サーバー）内のDHCPサーバー機能の使用も可能です。

外部のDHCPサーバーと管理サーバー内部のDHCPサーバー機能はどちらか一方を使用してください。

[注2]: ネットワークセグメントを分割しない場合、ルーターは不要です。

必要な準備作業

管理対象サーバー

PXEブート機能は、オンボードLAN[注1]またはLANカードのポートを使用します。

必要に応じてBIOS設定などを変更し、使用するLANポートからのPXEブートを有効にします[注2]。

[注1]: 管理対象サーバーのモデルによっては、「Dynamic LoM」と記載される場合があります。

[注2]: 使用するLANポートの指定は、各ノードの「PXEブートポート」で設定します。

注意

事前設定

- LANポートおよびPXE機能を有効に設定してください。

  オンボードの場合、これらの設定は工場出荷時に有効に設定されています。無効に変更した場合は有効に戻してください。LANカードの場合は各カードのマニュアルなどを参照してください。

- 使用するLANポートの指定をISMの「PXEブートポート」で設定する場合、指定方法の「ポート選択」(スロット番号およびポート番号による指定)でLANポートが一意とならないときは、「MACアドレス選択」で指定してください。

DHCPサーバー／ルーター

ISM-VA内のDHCP機能を有効にするか、管理サーバーと同じネットワークセグメント内でDHCPサーバーを動作させ、PXEブート用のLANポートに対して適切なIPv4アドレスがリースできるよう設定してください。その際、リース期間は60分以上に設定してください。

例) ISM-VAが192.168.1.100/24 に接続している場合のスコープ設定例

- リース範囲:192.168.1.128～192.168.1.159
- リース期間:8日間

管理対象サーバーが別セグメントのネットワークに接続されている場合は、PXEブートに必要なDHCPパケットなどがセグメント間で相互に通信可能になるようルーターを設定してください。

その他、ISMが使用する各種ポートも通信可能に設定してください。

ISM(管理サーバー)

PXEブート以外に必要な主な作業を記載します。本書に従って実施してください。

- ISM-VA全体に対する仮想ディスク割当て／ユーザーグループに対する仮想ディスク割当て
- OSインストールDVDのインポート (OSインストールの場合)
- ServerView Suite Update DVDのインポート (Offlineアップデートの場合)
- ServerView Suite DVDのインポート
- 管理対象サーバーのISMへの登録

  ※ ISMに登録する際は「OEM」または「Administrator」権限を持つiRMCユーザーを登録してください。

注意

ROR(ServerView Resource Orchestrator)がISMと同じ管理LAN上に構築されている場合、RORのPXEサービスを停止する必要があります。下記のマニュアルサイトから該当のRORバージョンを選択し、PXEサービス停止のコマンドを確認してください。

http://software.fujitsu.com/cgi-bin/manualps.cgi?langtype=ja&viewtype=icon&keyword=ServerView+Resource+Orchestrator&ostype=all

ServerView Resource Orchestrator Express/Virtual Editionの『リファレンスガイド(コマンド編)』の"rcxadm pxectl"コマンドを参照してください。

A.1.2 ETERNUS DX/AF/AB/HB 各種エンクロージャの表示

ISMは、ETERNUS DX/AF/AB/HB が内包する各種エンクロージャをノードとして管理します。

ここでは各種エンクロージャの管理をするために必要な設定について情報を提供します。

ISMで管理するエンクロージャ(子ノード)のモデルによる違いは、『操作手順書』の「表2.4 ノード間で親子の繋がりが設定されるモデル」を参照してください。

エンクロージャの登録

各種エンクロージャは、ETERNUS本体をノード登録し、その後のノード情報収集により自動的に ISM にノード登録されます。

エンクロージャのノード詳細情報

ISMでは、各種エンクロージャの詳細情報を、ETERNUS本体のノード詳細情報に表示します。

エンクロージャのステータス

各種エンクロージャのステータスは、ETERNUS AB/HBとETERNUS DX/AFで異なります。

- ETERNUS AB/HBの場合、ドライブエンクロージャのステータスは常に Unknown が表示されます。ドライブエンクロージャはコントローラーエンクロージャによって集約管理されているため、コントローラーエンクロージャのステータスを参照してください。
- ETERNUS DX/AFの場合、コントローラーエンクロージャから取得した、それぞれの各種エンクロージャステータスが表示されます。各種エンクロージャのステータスを表示するには、ETERNUS DX/AFでSMI-S機能を有効にする必要があります。SMI-S機能を有効にしなかった場合、ETERNUS AB/HBと同様の表示となります。

エンクロージャの削除

各種エンクロージャは、以下の場合にノードリストから削除されます。

- ドライブエンクロージャがコントローラーエンクロージャから切断された場合、その後のノード情報取得後にドライブエンクロージャはノード詳細から削除されます。
- ISM からETERNUS本体のノードを削除した場合、各種エンクロージャのノードも削除されます。

注意

ISM 2.9.0.020以前にETERNUS DX900 S5をノード登録した場合、当該ノードを削除後、再度ノード登録することにより、各種エンクロージャ情報を表示することができます。この操作を実施しない場合、プロパティ、監視タブのみの表示となり、子ノードの各種エンクロージャ情報も表示されません。

A.1.3 MIBファイルのインポートに関する注意

ISMでのMIBのインポートに関する注意事項について説明します。

MIBの形式について

MIBのトラップ定義に特定形式の注釈を記述することにより重要度などを取り扱うことが可能ですが、内容によっては定義どおりに処理されない場合があります。ここではインポートするMIBの形式について説明します。

MIBのトラップ定義(TRAP-TYPE/NOTIFICATION-TYPE)の注釈の形式は、Novell NMSで提唱の形式に準じています。

例:

```
sniScVoltageTooHigh TRAP-TYPE
ENTERPRISE sniServerMgmt
VARIABLES {
trapServerName,
trapTime,
trapCabinetNumber,
trapObjectNumber,
trapString
}
DESCRIPTION
    "Power supply voltage is too high."
--#TYPE     "Voltage too high"
--#SUMMARY "Power supply voltage %d (%s) in cabinet %d at server %s is too high."
```

```
--#SEVERITY     CRITICAL
::= 652
```

コメントフィールドの記述

項目	内容
--#TYPE	トラップのショートネーム。この名前には、最大40文字を使用できます。ISM上ではトラップメッセージの一部として使用します。
--#SUMMARY	プレースホルダーを含むトラップの説明、およびトラップで渡される実際のパラメーターの書式情報。ISM上ではトラップメッセージの一部として使用します。
--#ARGUMENTS	SUMMARY文字列に代入するパラメーターのリスト。パラメーターは、リストに表示された順序で代入されます。リストの各要素は、VARIABLES句のパラメーターのインデックス(ゼロベース)です。
--#SEVERITY	トラップに割り当てられるデフォルトの重要度。次のいずれかになります。 情報(INFORMATIONAL) 軽度(MINOR) 重度(MAJOR) 危険(CRITICAL)

注意

- --#TYPEの記載がない場合、オブジェクト名が代用されます。
- --#SUMMARYの記載がない場合、DESCRIPTIONの内容が代用されます。
- --#SEVERITYの記載がない場合、またはINFORMATIONAL/MINOR/MAJOR/CRITICALのいずれにも該当しない重要度が定義されている場合、トラップの重要度はINFORMATIONALとして扱われます。

Unknownトラップを受信した場合の対処

トラップを受信した場合、対応するMIBが登録されていないと重要度がUnknownとなりメッセージが正しく表示されません。Unknownトラップを受信した場合最新のMIBを取得し更新してください。更新後もUnknownトラップを受信する場合、対象の装置に異常がないか確認してください。なお、ISMで管理していないノードのトラップを受信しても、メッセージは正しく表示されません。

A.1.4 ISMで使用するポート番号一覧

ISMの各種機能が通信に必要なポート番号の情報を提供します。

表A.1 ISM機能ごとの使用ポート番号

機能	プロトコル	使用ポート番号	接続方向
SSHコンソールアクセス	SSH	22/tcp	管理端末→ISM
FTPによるファイル転送領域アクセス	FTP	21/tcp	管理端末→ISM
	FTPデータ	64872-65002/tcp	管理端末→ISM
NTPサーバーを使用した時刻補正	NTP	123/udp	ISM→NTPサーバー
DNSサーバーを使用したホスト名解決	DNS	53/udp	ISM→DNSサーバー
ディレクトリーサーバーを用いたユーザー管理	LDAP	389/tcp ※ISMで変更可能	ISM→ディレクトリーサーバー
	LDAPS	636/tcp ※ISMで変更可能	
ISMがイベントを検出した際のリモートスクリプト実行	SSH	22/tcp	ISM→外部ホスト

機能	プロトコル	使用ポート番号	接続方向
スクリプトを実行する外部ホストOS: Red Hat Enterprise Linux SUSE Linux Enterprise Server AlmaLinux		※ISMで変更可能	
ISMがイベントを検出した際のリモートスクリプト実行 スクリプトを実行する外部ホストOS: Windows	HTTPS	5986/tcp ※ISMで変更可能	ISM→外部ホスト
ISMがイベントを検出した際のメール送信	SMTP	25/tcp ※ISMで変更可能	ISM→メールサーバー
		587/tcp	
ISMがイベントを検出した際のトラップ送信／転送	SNMPTRAP	162/udp ※ISMで変更可能	ISM→外部SNMPマネージャー
ISMがイベントを検出した際のSyslog転送	syslog	514/udp ※ISMで変更可能	ISM→外部Syslogサーバー
外部共有ディレクトリマウント（SMB/CIFS）	SMB/CIFS	445/tcp	ISM→SMB/CIFSサーバー
		445/udp	
	NETBIOS	137/tcp	
		138/udp	
		139/tcp	
外部共有ディレクトリマウント（NFS）	NFS	2049/tcp	ISM→NFSサーバー

A.2 管理対象ノードの設定詳細

ISMで使用するポート番号と管理対象ノードに設定が必要な接続情報を説明します。

A.2.1 使用ポート番号一覧

ISMは装置と通信する必要があります。ここでは通信に必要な使用ポート番号の情報を提供します。機器や環境に合わせて設定してください。

記載している使用ポート番号は、デフォルトのポート番号です。接続方向がISM→ノードの場合、使用ポート番号はノードの設定により変更できます。

表A.2 対象機器ごとのISM使用ポート番号

対象機器	機能	プロトコル	使用ポート番号	接続方向
PRIMERGY (RX/CX/TX)（PRIMERGY CX1430 M1, PRIMERGY RX2450 M1を除く） PRIMEQUEST 3000B PRIMEQUEST 4000シリーズ（Partition） IPCOM VX2	ノード情報取得	IPMI	623/udp	ISM→ノード
		HTTPS	443/tcp	ISM→ノード
	自動検出	SSDP	1900/udp	ノード→ISM
	モニタリング	IPMI	623/udp	ISM→ノード
		HTTPS	443/tcp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	CAS	HTTPS	25593/tcp ※ISMで変更可能	ノード→ISM
	ファームウェアアップデート（Onlineアップデート）	IPMI	623/udp	ISM→ノード

対象機器	機能	プロトコル	使用ポート番号	接続方向
	（iRMC S3未対応）	TFTP （iRMC S4）	69/udp	ノード→ISM
		TFTPデータ （iRMC S4）	any/udp	ISM→ノード
		HTTPS （iRMC S5以降）	443/tcp	ISM→ノード
	ファームウェアアップデート （Offlineアップデート）	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
		DHCP	67/udp	ノード→ISM
		TFTP	69/udp	ノード→ISM
		TFTPデータ	any/udp	ISM→ノード
		PXE	4011/udp	ノード→ISM
		HTTPS	443/tcp	ISM→ノード
		HTTPSデータ	25613/tcp	ノード→ISM
	ファームウェアアップデート （eLCM Offlineアップデート(SimpleUpdate)） （iRMC S5以降）	HTTPS	25566/tcp ※ISMで変更可能	ノード→ISM
		HTTPS	443/tcp	ISM→ノード
	ログ収集	IPMI	623/udp	ISM→ノード
		SSH （iRMC S3のみ）	22/tcp	ISM→ノード
		HTTPS （iRMC S4以降）	443/tcp	ISM→ノード
	プロファイル適用（全般） [注1]	IPMI	623/udp	ISM→ノード
		HTTP	80/tcp	ISM→ノード
		HTTPS	443/tcp	ISM→ノード
	プロファイル適用（OSインストール時のみ） [注2]	FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
		DHCP	67/udp	ノード→ISM
		TFTP	69/udp	ノード→ISM
		TFTPデータ	any/udp	ISM→ノード
		SMB	445/tcp	ノード→ISM
		PXE	4011/udp	ノード→ISM
		HTTPSデータ	25613/tcp	ノード→ISM
		独自	9213/tcp	ノード→ISM
		独自	5001/tcp	ISM→ノード
PRIMERGY CX1430 M1	ノード情報取得	IPMI	623/udp	ISM→ノード
PRIMERGY GX2460 M1		HTTPS	443/tcp	ISM→ノード
PRIMERGY GX2570 M6	モニタリング	IPMI	623/udp	ISM→ノード
PRIMERGY GX2560 M7	ログ収集	IPMI	623/udp	ISM→ノード

対象機器	機能	プロトコル	使用ポート番号	接続方向
PRIMERGY RX2450 M1				
PRIMERGY GX2570 M5	ノード情報取得	IPMI	623/udp	ISM→ノード
		HTTPS	8080/tcp	ISM→ノード
	モニタリング	IPMI	623/udp	ISM→ノード
	ログ収集	IPMI	623/udp	ISM→ノード
PRIMERGY LX1430 M1	ノード情報取得	IPMI	623/udp	ISM→ノード
	モニタリング	IPMI	623/udp	ISM→ノード
	ログ収集	IPMI	623/udp	ISM→ノード
PRIMEQUEST 3000シリーズ（Partition）	ノード情報取得	SNMP	161/udp	ISM→ノード
		IPMI	623/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
		IPMI	623/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
		IPMI	623/udp	ISM→ノード
PRIMEQUEST 2000シリーズ（Partition） PRIMEQUEST 2000B	ノード情報取得	SNMP	161/udp	ISM→ノード
		IPMI	623/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
		IPMI	623/udp	ISM→ノード
	トラップ受信	SNMP (Trap)	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
ETERNUS DX/AF （ISM2.9.0.030より前にノード登録されたETERNUS DX900 S5を除く）	ノード情報取得	SNMP	161/udp	ISM→ノード
		SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
		SMI-S（HTTPS） [注3]	5989/tcp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	プロファイル適用	SSH	22/tcp	ISM→ノード

対象機器	機能	プロトコル	使用ポート番号	接続方向
ETERNUS NR (NetApp) ETERNUS HX/AX ETERNUS AC	ノード情報取得	SNMP	161/udp	ISM→ノード
		SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
		HTTPS	443/tcp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
ETERNUS AB/HB	ノード情報取得	SNMP	161/udp	ISM→ノード
		HTTPS	443/tcp	ISM→ノード
	モニタリング	HTTPS	443/tcp	ISM→ノード
	ログ収集	HTTPS	443/tcp	ISM→ノード
ETERNUS CS800 S7 ETERNUS CS800 M1 ETERNUS LT ETERNUS DX900 S5 (ISM2.9.0.030より前にノード登録された場合)	ノード情報取得	SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
SR-X	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	FTP	21/tcp	ISM→ノード
		FTPデータ	any/tcp	ISM→ノード
		SSH	22/tcp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
	プロファイル適用	SSH	22/tcp	ISM→ノード
	VLAN/リンクアグリゲーション設定	SSH	22/tcp	ISM→ノード
SR-S	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
	VLAN/リンクアグリゲーション設定	SSH	22/tcp	ISM→ノード
イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	自動検出	SSDP	1900/udp	ノード→ISM
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	FTP	21/tcp	ノード→ISM

対象機器	機能	プロトコル	使用ポート番号	接続方向
		FTPデータ	64872-65002/tcp	ノード→ISM
		SSH	22/tcp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
	プロファイル適用	SSH	22/tcp	ISM→ノード
	VLAN/リンクアグリゲーション設定	SSH	22/tcp	ISM→ノード
VDX	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	プロファイル適用	SSH	22/tcp	ISM→ノード
	VLAN/リンクアグリゲーション設定	SSH	22/tcp	ISM→ノード
Catalyst	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
Nexus Series	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		SFTP [注1]	22/tcp	ISM→ノード
		TFTP	69/udp	ノード→ISM
		TFTPデータ	any/udp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
Juniper QFX/EX	ノード情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM

対象機器	機能	プロトコル	使用ポート番号	接続方向
IPCOM EX2スイッチ	ノード情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
		FTP	21/tcp	ノード→ISM
		FTPデータ	64872-65002/tcp	ノード→ISM
Arista 7000 Family	ノード情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
CFX2000F/R	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	FTP	21/tcp	ISM→ノード
		FTPデータ	any/tcp	ISM→ノード
		SSH	22/tcp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
	プロファイル適用	SSH	22/tcp	ISM→ノード
Brocade FCスイッチ	ノード情報取得	SSH	22/tcp	ISM→ノード
		SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ログ収集	SSH	22/tcp	ISM→ノード
		SCP	22/tcp	ノード→ISM
ExtremeSwitching X440/460-G2	ノード情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM
	ファームウェアアップデート	SSH	22/tcp	ISM→ノード
		TFTP	69/udp	ノード→ISM
		TFTPデータ	any/udp	ISM→ノード
	VLAN/リンクアグリゲーション設定	SSH	22/tcp	ISM→ノード
Schneider Electric Switched Rack PDU /Schneider Electric Smart-UPS	ノード情報取得	SNMP	161/udp	ISM→ノード
	モニタリング	SNMP	161/udp	ISM→ノード
	トラップ受信	SNMP（Trap）	162/udp	ノード→ISM

[注1]：BMC（iRMC）との通信に使用します。

[注2]：オンボードLANまたはLANカードとの通信に使用します。

[注3]：ドライブエンクロージャステータス取得のため、コントローラーエンクロージャとの通信に使用します。

表A.3 対象OSごとのISM使用ポート番号

対象OS	機能	プロトコル	使用ポート番号	接続方向
Windows	OS情報取得	HTTPS	5986/tcp	ISM→ノード
	モニタリング	HTTPS	5986/tcp	ISM→ノード
	ファームウェアアップデート（Onlineアップデート）	HTTPS	5986/tcp	ISM→ノード
		FTPS	21/tcp	ノード→ISM
		FTPSデータ	64872-65002/tcp	ノード→ISM
	ログ収集	HTTPS	5986/tcp	ISM→ノード
		FTPS	21/tcp	ノード→ISM
		FTPSデータ	64872-65002/tcp	ノード→ISM
Red Hat Enterprise Linux / SUSE Linux Enterprise Server	OS情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SSH	22/tcp	ISM→ノード
	ファームウェアアップデート（Onlineアップデート）	SSH	22/tcp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
AlmaLinux	OS情報取得	SSH	22/tcp	ISM→ノード
	モニタリング	SSH	22/tcp	ISM→ノード
	ログ収集	SSH	22/tcp	ISM→ノード
VMware ESXi	OS情報取得	HTTPS	443/tcp	ISM→ノード
			5989/tcp	ISM→ノード
	モニタリング	HTTPS	443/tcp	ISM→ノード
	ログ収集	HTTPS	443	ISM→ノード

表A.4 対象仮想化管理ソフトウェアごとのISM使用ポート番号

対象仮想化管理ソフトウェア	機能	プロトコル	使用ポート番号	接続方向
vCenter	情報取得	HTTPS	443/tcp	ISM→ノード
SystemCenter	情報取得	HTTPS	5986/tcp	ISM→ノード
FailOverCluster	情報取得	HTTPS	5986/tcp	ISM→ノード
KVM	情報取得	SSH	22/tcp	ISM→ノード
OpenStack	情報取得	HTTPS	5001/tcp	ISM→ノード
		SSH	22/tcp	ISM→ノード

A.2.2 ノード設定詳細

ISMでノードを管理するためには、ノード側で接続情報を設定する必要があります。ここでは設定に必要な接続情報を提供します。

接続情報

ノードと接続するには、ノード登録を行う前にノード側で以下の設定が必要です。設定方法については、それぞれの装置のマニュアルを参照してください。

表A.5 対象機器と接続情報

ノード	接続情報			
	IPMIの アカウント [注1]／ パスワード	SSHの アカウント／ パスワード	SNMPの 必須入力情報 [注2]	HTTPSの アカウント／ パスワード
PRIMERGY(RX/CX/TX) M6以前（PRIMERGY CX1430 M1, PRIMERGY RX2450 M1, PRIMERGY 1WAY M6, PRIMERGY RX1440 M2/ RX2450 M2を除く）	○	-	-	- [注4]
PRIMERGY(RX/CX/TX) M7 PRIMERGY 1WAY M6 PRIMERGY RX1440 M2 PRIMERGY RX2450 M2	- [注6]	-	-	○
PRIMERGY CX1430 M1 PRIMERGY RX2450 M1	○	-	-	○
PRIMERGY GX	○	-	-	○
PRIMERGY LX	○	-	-	-
PRIMEQUEST 2000シリーズ（Partition）	○	○	○	-
PRIMEQUEST 2000B	○	○	○	-
PRIMEQUEST 3000シリーズ（Partition）	○	○	○	-
PRIMEQUEST 3000B	○	-	-	- [注4]
PRIMEQUEST 4000シリーズ（Partition）	- [注6]	-	-	○
ETERNUS DX/AF （ISM2.9.0.030より前にETERNUS DX900 S5をノード登録する場合を除く）	-	○	○	- [注5]
ETERNUS NR ETERNUS HX/AX ETERNUS AC	-	○	○	○
ETERNUS AB/HB	-	-	○	○
ETERNUS CS800 S7 ETERNUS CS800 M1 ETERNUS LT ETERNUS DX900 S5 (ISM2.9.0.030より前にノード登録する場合)	-	-	○	-
SR-X	-	○	○	-
イーサネットスイッチ(10GBASE-T 48+6 / 10GBASE 48+6)	-	○	○	-
VDX	-	○	○	-
Brocade FCスイッチ	-	○	○	-
Cisco Catalyst	-	○	○	-

ノード	接続情報			
	IPMIの アカウント [注1]／ パスワード	SSHの アカウント／ パスワード	SNMPの 必須入力情報 [注2]	HTTPSの アカウント／ パスワード
Cisco Nexus	-	○	○	-
Arista 7000 Family	-	○	○	-
Juniper QFX/EX	-	○	○	-
CFX2000F/R	-	○	○	-
Schneider Electric Switched Rack PDU	-	-	○	-
SchneiderElectric Smart-UPS	-	-	○	-
IPCOM EX2スイッチ	-	○	○	-
SR-S	-	○	○	-
ExtremeSwitching X440/460-G2	-	○	○	-

凡例：○= 必須、-= 不要

動作確認済みのモデルについては、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

[注1]: アクセス権限がAdministrator、またはOEMを持つアカウントをご使用ください。

[注2]: SNMP v1またはv2の場合は、コミュニティー名の入力が必須です。SNMP v3の場合は、ユーザー名、セキュリティレベル、認証プロトコル（認証使用時）、認証パスワード（認証使用時）、暗号化プロトコル（暗号化使用時）、暗号化パスワード（暗号化使用時）の入力が必須です。

[注3]: シャーシ（MMB）の接続情報設定が必要となります。

[注4]: アカウント／パスワードはIPMIと同じものが使用されます。HTTPSのポート番号のみ指定できます。

[注5]: アカウント／パスワードはSSHと同じものが使用されます。

[注6]: アカウント／パスワードはHTTPSと同じものが使用されます。IPMIのポート番号のみ指定できます。

手動検出のために必要な設定

PRIMERGY 2/4/8WAY M7以降、PRIMERGY 1WAY M6以降、PRIMERGY RX1440/2450 M2以降のサーバーで手動検出をおこなうためには、iRMCのWeb UIのSSDPを有効にしてください。

確認方法は以下のとおりです。

[サービス] - [SSDP] - [SSDPを有効にする]にチェックが付いていることを確認します。

管理のために必要な設定

接続情報の設定に加えて、以下の設定を行ってください。

【PRIMERGY】

PRIMERGY S8／M1／M2／M3世代のサーバーでiRMC S4ファームウェアのバージョンが9.00以上をご使用の場合、ISMのノード詳細のSASカードに関する情報を取得するためには、iRMCのWeb UIのIPMI権限／許可 の変更が必要です。変更方法は以下のとおりです。

1. [ユーザ管理] - [iRMC S4ユーザ管理] - [IPMI権限/許可] - [Redfish Enabled] にチェックを付けます。
2. [ユーザ管理] - [iRMC S4ユーザ管理] - [IPMI権限/許可] - [Redfish Role] をAdministratorに変更します。

【PRIMERGY GX2460 M1】

- BMCの固定ユーザー（root）のデフォルトパスワードを変更し、変更したパスワードをノード登録時に指定してください。

・ HTTPSの固定ユーザー（Administrator）のデフォルトパスワードを変更し、変更したパスワードをノード登録時に指定してください。

【SR-X】

LLDP設定を有効にしてください。

【VDX】

・ LLDP設定を有効にしてください。

・ スイッチごとに管理LANポートのIPアドレスを設定してください。

【Brocade FCスイッチ】

・ AGモードを無効にしてください。

・ SW-MIBを有効にしてください。

実行例:

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

【Arista 7000 Family】

LLDP設定を有効にしてください。

【ETERNUS DX/AF】（ISM2.9.0.030より前にETERNUS DX900 S5をノード登録する場合を除く）

・ ISMと接続するためのポートは、Control Module のメンテナンスポートを使用してください。

リモートポートに接続した場合、ファームウェアアップデート機能、ログ収集機能、およびプロファイル適用機能が動作しないことがあります。

・ SMI-S機能を有効にしてください。

【ETERNUS NR1000】

クラスタ管理IPとノード管理IPは、同じネットワークセグメントに設定してください。

【ETERNUS NR/AX/HX/AC】

HTTPSのパスワード認証でログイン可能なユーザアカウントを追加してください。

【PRIMEQUEST 2000/3000シリーズ（Partition）、PRIMEQUEST 2000B】

・ ISMのMMBのアカウント設定（IPMI接続のアカウント設定）では、PRIMEQUESTのWeb UIの[Network Configuration]-[Remote Server Management] に登録したアカウントを使用してください。その際PrivilegeはAdminまたはCEである必要があります。

・ ISMのSSHのアカウント設定では、PRIMEQUESTのWeb UIの[User Administration]-[User List]に登録したアカウントを使用してください。その際PrivilegeはAdminまたはCEである必要があります。

【PRIMEQUEST 4000シリーズ（Partition）】

ISMのHTTPSのアカウント設定では、PRIMEQUESTのパーティションごとに設定したアカウントをご使用ください。

【ExtremeSwitching X440/460-G2】

・ LLDP設定を有効にしてください。

・ Admin権限のSSHアカウントを作成し、そのアカウントをノード登録時に設定してください。

通知のために必要な設定

接続情報 および、管理のために必要な情報の設定に加えて、SNMPトラップの設定を行ってください。詳細については各機器のマニュアルを参照してください。

なお、ISMのトラップ通知受信設定で対象ノードとして選択した際に、エンジンIDが自動的に入力される対応機器は以下のとおりです。

表A.6 対応機器

ノード	エンジンIDの自動入力
PRIMERGY(RX/CX/TX) （PRIMERGY CX1430 M1を除く）	○

ノード	エンジンIDの自動入力
PRIMERGY CX1430 M1	-
PRIMERGY GX	-
PRIMERGY LX	-
PRIMEQUEST 2000シリーズ（Partition）	-
PRIMEQUEST 2000B	○
PRIMEQUEST 3000シリーズ（Partition）	○
PRIMEQUEST 3000B	○
PRIMEQUEST 4000シリーズ（Partition）	○
ETERNUS DX/AF	○
ETERNUS NR ETERNUS HX/AX ETERNUS AC	-
ETERNUS AB/HB	-
SR-X	○ [注1]
イーサネットスイッチ(10GBASE-T 48+6) イーサネットスイッチ(10GBASE 48+6)	○
VDX	○
Brocade FCスイッチ	○
Cisco Catalyst	○
Cisco Nexus	○
Juniper QFX/EX	○
CFX2000F/R	○ [注1][注2]
Schneider Electric Switched Rack PDU	-
SchneiderElectricSmart-UPS	-

凡例：○ = 対応、- = 非対応

[注1]: 以下の機器に対してSNMP v3 engine IDを設定しない場合、ISMのトラップ通知受信設定で対象ノードを選択した際に、エンジンIDが自動的に入力されません。

自動的に入力されるようにするには、機器に対して事前にsnmpv3 engine IDを設定してください。

- CFX2000F/R
- SR-X

[注2]: ファブリックを組み、かつ、機器に対してSNMP v3 engine IDを設定している場合、ファブリック全体でengine IDを同じ値に設定してください。

A.3 ノードの運用に関するその他の情報

管理対象ノードの運用に関するその他の情報を説明します。

A.3.1 ファームウェアアップデート時間の目安

ISMのファームウェア管理機能を使用したファームウェアのアップデートには、長時間を要する場合があります。ここではファームウェアアップデートに要する時間の目安を提示します。

ファームウェアアップデートの作業計画を立てる際は以下の時間を参考にしてください。また、ファームウェアアップデート完了前に中断しないでください。

注意

以下に記載された時間は現行ファームウェアを標準的な構成でアップデートした際の時間です。ファームウェアバージョンや、ネットワーク構成、ネットワーク負荷状態などで変動する場合がありますので、作業計画を立てる際には万一のトラブル発生時の対応時間も含め、十分な余裕を持った設計を推奨します。

表A.7 ファームウェアアップデート時間の目安

アップデート対象	1台当たりの目安	備考
PRIMERGYのiRMC ファームウェアアップデート	Onlineアップデート 15～30分	
	Offlineアップデート 20～40分	ファームウェアを適用後、サーバーの電源がオンになる設定にしている場合、さらに15分必要。
PRIMERGYのBIOS ファームウェアアップデート	Onlineアップデート 5～10分	ファームウェアを適用するためにサーバーの電源オフ・オン操作の時間が別途必要。
	Offlineアップデート 20～40分	ファームウェアを適用後、サーバーの電源がオンになる設定にしている場合、さらに15分必要。
PRIMERGY GXのBMC ファームウェアアップデート	Offlineアップデート 15～30分	ファームウェアアップデート実行後、サーバー側でBMCおよびBIOSの設定項目が初期化されるため、再設定する時間が別途必要。
PRIMERGY GXのBIOS ファームウェアアップデート	Offlineアップデート 15～30分	
PRIMEQUEST 3800BのiRMC ファームウェアアップデート	Onlineアップデート 10～20分	
PRIMEQUEST 3800BのBIOS ファームウェアアップデート	Onlineアップデート 5～15分	ファームウェア適用にはサーバーの電源オフ・オン操作の時間が別途必要。
PRIMEQUEST 2000/3000シリーズ (Partition)の本体ファームウェアアップデート	70～130分	
PRIMEQUEST 4000シリーズ(Partition)の本体ファームウェアアップデート	70～130分	
ネットワークスイッチ SR-Xの ファームウェアアップデート	2～10分	
ファブリックスイッチCFX2000R/F、コンバージドファブリックスイッチブレードの ファームウェアアップデート	10～20分	
コンバージドスイッチ VDXの ファームウェアアップデート	15～30分	
コンバージドスイッチ X440/460-G2の ファームウェアアップデート	10～20分	
イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)の ファームウェアアップデート	20～30分	
Cisco Systems Nexusシリーズの ファームウェアアップデート	30～50分	

アップデート対象	1台当たりの目安	備考
Cisco Systems Catalystシリーズの ファームウェアアップデート	10～20分	
PCIカードの ファームウェアアップデート	Onlineアップデート 10～20分	ファームウェア適用でサーバーの電源オフ・オン操作の時間が別途必要。左記はカード1枚当たりの時間。
	Offlineアップデート 20～40分	左記はカード1枚当たりの時間。
ETERNUS DX/AFシリーズの ファームウェアアップデート	10～60分	ユニファイド機構有り、またコントローラーエンクロージャ多数搭載の場合、アップデート時間が長くなる。

A.3.2 ログ管理機能利用時のディスク消費量の目安

ログ管理機能を利用し、ノードからログを定期的に収集してISM-VA上に蓄積できます。ここでは収集したログの蓄積場所、および蓄積されるデータ量の目安に関する情報を提供します。

収集したログはユーザーグループに割り当てられている仮想ディスク上のログ保存領域に蓄積されます。ISM-VAの各ユーザーグループへの仮想ディスク割当ての参考にしてください。

注意

- ログ保有期間、世代数はデフォルトで以下が設定されています。必要に応じてログ保有期間、世代数を変更してください。

保管ログ	ノードログ（ダウンロード用データ / ログ検索用データ）
7世代	30日

- 本書に記載された容量は特定の構成・運用を行った場合の参考値です。実際の使用状況により大きく異なる場合があります。

管理するログの種別および蓄積場所について

ログ管理機能はログを収集した際、保管ログ、ノードログ（ダウンロード用データ）、ノードログ（ログ検索用データ）を作成します。

各ログは、それぞれ以下のログ保存領域に蓄積されます。

ログ種別	保存領域
保管ログ	ノードが所属するノードグループが関連付けられているユーザーグループのログ保存領域 [注1]
ノードログ（ダウンロード用データ）	
ノードログ（ログ検索用データ）	Administratorグループのログ保存領域 [注2]

[注1]：ノードグループがユーザーグループに関連付けられていない場合は、Administratorグループのログ保存領域に蓄積されます。

[注2]：すべてのノードのノードログ（ログ検索用データ）がAdministratorグループのログ保存領域に蓄積されます。ノードグループがAdministratorグループ以外のユーザーグループに関連付けられている場合もAdministratorグループのログ保存領域に蓄積されます。

ログ容量の目安

表A.8 1ノードあたりの1世代の保管ログの容量目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY	1KB
		PRIMEQUEST 3000B	1KB
		PRIMEQUEST 4000シリーズ（Partition）	50KB
	Chassis	PRIMEQUEST 3000シリーズ（Partition）	50KB

ログ収集ターゲット			容量の目安
	Switch	SR-X	50KB
		CFX	100KB
		イーサネットスイッチ （10GBASE-T 48+6 / 10GBASE 48+6）	350KB
		VDX	50MB
		Cisco Catalyst	1MB
		Cisco Nexus	10MB
		Juniper QFX/EX	1MB
		SR-S	50KB
		Brocade FC	100MB
	IPCOM	IPCOM VX2	1KB
		IPCOM EX2	2MB
	Storage	ETERNUS DX/AF ETERNUS DX900 S5 （ISM2.9.0.030以降にノード登録された場合）	10MB
		ETERNUS NR/AX/HX (Ontap)クラスタ ETERNUS AC (Ontap)クラスタ	100KB
		ETERNUS AB/HB	80MB
オペレーティング システム	Windows		5MB
	Linux		5MB
	VMware ESXi		3MB
	IPCOM OS		50MB
ServerView Suite	ServerView Agents		Windows：10MB Linux：80MB
	ServerView Agentless Service		
	ServerView RAID Manager		

表A.9 1ノードあたりの30日間分のノードログの容量目安

ログ収集ターゲット			ノードログの容量の目安	
			ダウンロード用データ	検索用データ
ハードウェア	Server	PRIMERGY （CX1430 M1 を除く）	50KB	500KB
		PRIMEQUEST 3000B	50KB	500KB
		PRIMEQUEST 4000シリーズ （Partition）	50KB	500KB
	Chassis	PRIMEQUEST 3000シリーズ （Partition）	50KB	500KB
	Switch	SR-X	100KB	1MB
		CFX	100KB	1MB
		イーサネットスイッチ （10GBASE-T 48+6 / 10GBASE 48+6）	150KB	1MB

ログ収集ターゲット			ノードログの容量の目安	
			ダウンロード用データ	検索用データ
		VDX	100KB	1MB
		Cisco Catalyst	50KB	500KB
		Cisco Nexus	50KB	500KB
		SR-S	100KB	1MB
	IPCOM	IPCOM VX2	50KB	500KB
	Storage	ETERNUS DX/AF ETERNUS DX900 S5 （ISM2.9.0.030以降にノード登録された場合）	100KB	1MB
		ETERNUS NR/AX/HX (Ontap) クラスタ ETERNUS AC (Ontap) クラスタ	200KB	2MB
オペレーティングシステム	Windows		1MB	15MB
	Linux		1MB	15MB
	VMware ESXi		4MB	50MB
	IPCOM OS		1MB	15MB

A.3.3 ファームウェアアップデートに使用するプロトコルの変更

Nexus Seriesはファームウェアアップデートに使用するプロトコルを変更することができます。

指定可能なプロトコルは、TFTPとSFTPです。初期設定はTFTPです。

現在の設定の確認方法は以下のとおりです。

```
# ismadm security show-protocol -item nexus-fwup
```

設定を変更するには、以下のコマンドを使用します。

```
# ismadm security set-protocol -item nexus-fwup -value ＜変更するプロトコル＞
```

ファームウェアアップデートに使用するプロトコルをSFTPに設定する実行例:

```
# ismadm security set-protocol -item nexus-fwup -value SFTP
```

ファームウェアアップデートに使用するプロトコルをTFTPに設定する実行例:

```
# ismadm security set-protocol -item nexus-fwup -value TFTP
```

付録B　監視対象OS、仮想化管理ソフトウェアに対する設定

ISMでOSおよび仮想化管理ソフトウェアを管理するためには、OS、仮想化管理ソフトウェア側に設定が必要です。この章では、設定に必要な情報について説明します。

B.1　監視対象OS、仮想化管理ソフトウェアごとに必要な設定一覧

ISMから仮想マシン情報、装置情報表示（OS情報、ディスクボリューム）、ログ管理機能（OSログ収集）、ファームウェアアップデート（オンラインPCIカード）を使用するためには、各OS、仮想化管理ソフトウェアに設定が必要となります。以下の表に従い、設定を変更してください。

B.1.1　監視対象OSごとに必要な設定

凡例：○＝設定必要、×＝設定不要、－＝該当なし

OS	サービス		セキュリティ		ドメイン	
	sshd	WinRM	Firewall	PowerShell	SPN	ISM-VA設定
Windows Server	－	○	○	○	○	○
Red Hat Enterprise Linux	○	－	×	－	－	○
SUSE Linux Enterprise Server	○	－	○	－	－	○
AlmaLinux	○	－	×	－	－	○
VMware ESXi	－	－	－	－	－	○
Azure Stack HCI	－	○	○	○	○	○

各OSで必要な設定の詳細については、以下を参照してください。

- B.2 監視対象への設定手順（OS：Windows）
- B.3 監視対象への設定手順（OS：Red Hat Enterprise Linux）
- B.4 監視対象への設定手順（OS：SUSE Linux Enterprise Server）
- B.5 監視対象への設定手順（OS：AlmaLinux）
- B.6 監視対象への設定手順（OS：VMware ESXi）
- B.7 監視対象への設定手順（OS：Azure Stack HCI）

B.1.2　監視対象仮想化管理ソフトウェアごとに必要な設定

凡例：○＝設定必要、×＝設定不要、－＝該当なし

仮想化管理ソフトウェア	各ホスト・仮想マシンへの設定		ドメイン		
	sshd	WinRM	SPN	ISM-VA設定	Kerberos委任構成
vCenter Server[注1]	－	－	－	○	－
Microsoft Failover Cluster[注2]	－	○	○	○	○
Microsoft Failover Cluster (Azure Stack HCI)[注3]	－	○	○	○	○
Microsoft System Center[注4]	－	○	○	○	○
KVM Red Hat	○	－	－	○	○
KVM SUSE Linux Enterprise	○	－	－	○	○
KVM AlmaLinux[注5]	○	－	－	○	○

仮想化管理ソフトウェア	各ホスト・仮想マシンへの設定		ドメイン		
	sshd	WinRM	SPN	ISM-VA設定	Kerberos委任構成
OpenStack	「B.12 監視対象への設定手順（仮想化管理ソフトウェア：OpenStack）」を参照				

[注1] vCenter Server 5.5以降をサポートします。

[注2] Windows Server 2012以降をサポートします。

[注3] Red Hat 20H2以降をサポートします。

[注4] SUSE Linux Enterprise 2012以降をサポートします。

[注5] AlmaLinux8.10以降をサポートします。

各仮想化管理ソフトウェアで必要な設定の詳細については、以下を参照してください。

- B.8 監視対象への設定手順（仮想化管理ソフトウェア：vCenter Server）
- B.9 監視対象への設定手順（仮想化管理ソフトウェア：Microsoft Failover Cluster）
- B.10 監視対象への設定手順（仮想化管理ソフトウェア：Microsoft System Center）
- B.11 監視対象への設定手順（仮想化管理ソフトウェア：KVM）
- B.12 監視対象への設定手順（仮想化管理ソフトウェア：OpenStack）
- B.13 監視対象への設定手順（仮想化管理ソフトウェア：IPCOM）
- B.14 監視対象への設定手順（仮想化管理ソフトウェア：Microsoft Failover Cluster（Azure Stack HCI））

B.1.3 監視対象OS、仮想化管理ソフトウェア設定時の留意事項

- 対象サーバーを監視するためには、管理者権限を持つユーザーアカウントでOS情報を登録する必要があります。
- Windows／Linuxに搭載されるEmulex LAN/FC/CNAカードを管理するためには、対象サーバーのOSにEmulex OneCommand Manager CLIが導入されている必要があります。
- Windows／Linuxに搭載されるQLogic FCカードを管理するためには、対象サーバーのOSにQLogic QConvergeConsole CLIが導入されている必要があります。
- Emulex OneCommand Manager CLI、またはQLogic QConvergeConsole CLIは最新のものを利用してください。LAN/FC/CNAカードには最新のドライバーを適用してください。
- Linuxに搭載されるLAN/FC/CNAカードを管理するために、対象サーバーのOSにpciutilsおよびethtoolパッケージが導入されている必要があります。
- Linuxのディスク速度、ネットワーク速度、CPUコアごとのCPU使用率の性能監視、物理サーバーのアノマリ検知のために、対象サーバーのOSにsysstatパッケージが導入されている必要があります。
- Linuxのオペレーティングシステムログ、ServerView Suiteログを収集するために、対象サーバーのOSにzipパッケージが導入されている必要があります。

  また、オペレーティングシステムログを収集するために、対象サーバーのOSにrsyslogパッケージなどのsyslogデーモンが導入されている必要があります。
- Linuxの一般ユーザーアカウントでOSを管理するために、対象サーバーのOSにsudoパッケージが導入されている必要があります。
- Active Directoryからドメインユーザーのパスワード変更した場合、ISMでもパスワードを変更してください。
- ドメインユーザーアカウントを正しく使用するには、対象サーバーとISMの時刻を合わせる必要があります。

B.2 監視対象への設定手順（OS：Windows）

ISMは、Windows Serverがインストールされている監視対象機器に対してWS-Managementプロトコルを使用します。通信方式はhttpsプロトコル+Basic認証を使用します。必要な設定は、以下のとおりです。

- B.2.1 WinRMサービスの起動確認

- B.2.2 WinRMサービスの設定
- B.2.3 ファイアウォールのポート開放
- B.2.4 Windows PowerShellの実行ポリシー変更
- B.2.5 ドメインユーザーアカウント使用時の設定

B.2.1 WinRMサービスの起動確認

1. 管理者権限でコマンドプロンプトを開いて以下のコマンドを実行し、WinRMサービスの起動を確認します。

```
>sc query winrm
```

2. 以下の結果を確認し、STATEがRUNNINGになっていることを確認します。

```
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

3. WinRMサービスが起動されていない場合、以下のコマンドを実行し、WinRMサービスを起動します。

```
>sc start winrm
```

4. WinRMサービスを遅延自動起動(delayed-auto)に設定します。

```
>sc config winrm start=delayed-auto
```

B.2.2 WinRMサービスの設定

WinRMサービスの設定

ポイント

初期設定ではBasic認証が許可されていないため、Basic認証の許可の設定を行います。

以下のコマンドを実行します。

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

https通信を使用するためBasic認証の通信は暗号化されます。

1. 管理者権限でコマンドプロンプトを開き、以下のコマンドを実行します。

```
>winrm quickconfig
```

「WinRM サービスは、既にこのコンピューターで実行されています。このコンピューター上でのリモート管理には、WinRM が既に設定されています。」と表示された場合は、すでに設定が完了しているため「https通信の設定」に進んでください。

2. 「y」を入力後、[Enter]キーを押します。

```
WinRM サービスは、既にこのコンピューターで実行されています。
WinRM は、管理用にこのコンピューターへのリモート アクセスを許可するように設定されていません。
次の変更を行う必要があります:

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成してください。
変更しますか [y/n]? y
```

以下のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成しました。
```

3. 対象サーバーのOSがWindows Server 2008 R2の場合、以下のコマンドを実行して、カードの種類や数に応じてMaxConcurrentOperationsPerUserの数値を大きくします。

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="数値"}
```

例:1500に設定した場合(Windows Server 2012/2012R2では、デフォルトが1500であるため1500を推奨します。)

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

https通信の設定

https通信をするためには、証明書の設定が必要になります。

1. 必要なツールの準備

   証明書を作成するために必要なツールは2つあります。証明書は実行環境に依存せず作成できます。

   - .NET Framework 4.5 以降(ダウンロードサイト)

     https://www.microsoft.com/ja-jp/download/details.aspx?id=30653

   - Windows Software Development Kit(ダウンロードサイト)

     https://developer.microsoft.com/ja-jp/windows/downloads/windows-sdk/

   注意

   - 上記URLのWindows Software Development Kitの対応OSについては、上記URL内のシステム要件を確認してください。その他のOSにインストールする場合は、適切なWindows Software Development Kitをインストールしてください。
   - Windows Software Development Kitには、証明書を作成するために必要な2つのツールが含まれています。
     - 証明書作成ツール(makecert.exe)

       https://msdn.microsoft.com/ja-jp/library/bfsktky3(v=vs.80).aspx

     - 個人情報交換ファイル作成ツール(pvk2pfx.exe)

       https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx

2. 証明書の作成

   証明書作成ツール、個人情報交換ファイル作成ツールを使用し、以下の3つのファイルを作成します。

   - CERファイル(証明書)
   - PVKファイル(秘密鍵ファイル)
   - PFXファイル(サービス証明書)

   より詳細な証明書作成の流れについては、下記のURLを参照してください。

   https://blogs.technet.microsoft.com/junichia/2010/11/09/azure-for-itpro-3

   a. 証明書、秘密鍵ファイルの作成

      証明書、秘密鍵ファイルの作成では、対象サーバーの環境に合わせてコマンドを実行する必要があります。

      以下は、対象サーバーのサーバー名を"192.168.10.10"に設定し、証明書の有効期間を2017年3月30日に設定した場合のコマンド例です。

      ```
      >makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2017 -eku 1.3.6.1.5.5.7.3.1 -ss My
      -sr localMachine -sky exchange <証明書のファイル名.cer> -sv <秘密鍵のファイル名.pvk>
      ```

      証明書の構成に関する詳しい設定については、下記のURLを参照してください。

https://technet.microsoft.com/ja-jp/library/ms186362(v=sql.105).aspx

b. サービス証明書の作成

以下のコマンドを実行します。

```
>pvk2pfx.exe -pvk ＜秘密鍵のファイル名.pvk＞ -spc ＜証明書のファイル名.cer＞ -pfx ＜サービス証明書のファイル名.pfx＞
```

3. 証明書、サービス証明書の登録

証明書スナップインを起動し、手順2で作成した証明書を登録します。

a. 対象サーバーでmmc.exeを実行します。

b. [ファイル]-[スナップインの追加と削除] を選択します。

c. [利用できるスナップイン]から、「証明書」を選択し、[追加]します。

d. 「コンピューター アカウント」を選択し、[次へ]-[完了]を順に選択します。

e. [OK]を選択します。

4. SSL証明書を信頼されたルート証明機関に登録

＜証明書のファイル名.cer＞を信頼されたルート証明機関に登録します。

a. [コンソールルート]-[証明書（ローカルコンピューター）]-[信頼されたルート証明機関]を右クリックします。

b. [すべてのタスク]-[インポート]から、<証明書のファイル名.cer>ファイルを選択し、「証明書のインポートウィザード」画面を完了します。

c. [コンソールルート]- [証明書（ローカルコンピューター）]-[信頼されたルート証明機関]-[証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバー名となっていること、[目的]が「サーバー認証」となっていることを確認します。

5. SSL証明書を個人に登録

＜サービス証明書のファイル名.pfx＞を個人に登録します。

a. [コンソールルート]-[証明書（ローカルコンピューター）]-[個人]を右クリックします。

b. [すべてのタスク]-[インポート]から、<サービス証明書のファイル名.pfx>ファイルを選択し、「証明書のインポートウィザード」画面を完了します。

c. [コンソールルート]-[証明書（ローカルコンピューター）]-[個人]-[証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバー名となっていること、[目的]が「サーバー認証」となっていることを確認します。

WinRMサービスへの証明書に記載された拇印を登録

1. 拇印（Thumbprint）の確認

以下は、LocalMachine¥myに証明書を保存した場合の確認方法です。

a. コマンドプロンプトからPowerShellを起動します。

b. 拇印を確認します。以下のコマンドを実行します。

```
>ls cert:LocalMachine¥my
```

以下のように表示されます。

```
PS C:¥Windows¥system32> ls cert:LocalMachine¥my

ディレクトリ: Microsoft.PowerShell.Security¥Certificate::LocalMachine¥my
Thumbprint                                Subject
----------                                -------
1C3E462623BAF91A5459171BD187163D23F10DD9  CN=192.168.10.10
```

2. WinRMリスナーに証明書に記載された拇印を登録

PowerShellを終了し、以下のコマンドを実行します。’HTTPS’と’@’の間にはスペースが必要です。

```
>winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="＜証明書を作成したときに設定したCN名＞
":CertificateThumbprint="＜作成した証明書の拇印＞"}
```

3. WinRMリスナーの登録確認

   以下のコマンドを実行します。

```
>winrm get winrm/config/listener?Address=*+Transport=HTTPS
```

   以下のようなコマンド結果が返ってくれば、WinRMのリスナーが登録できています。

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 192.168.10.10
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
    ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

B.2.3 ファイアウォールのポート開放

WinRMサービスがリクエストの受付をできるように、WinRMリスナーで設定したポートを開放する必要があります。https通信のデフォルトポート番号は、5986です。

Windows Server 2012 / 2012R2 / 2016 / 2019 / 2022の場合

管理者権限でWindows PowerShellを開き、以下のコマンドを実行します。

```
>New-NetFirewallRule -DisplayName ＜ファイアウォールルール名＞ -Action Allow -Direction Inbound -Enabled True -Protocol TCP
-LocalPort ＜ポート番号＞
```

例:ポート番号5986を開放するルールに、"WinRM"という名前を設定します。

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort 5986
```

注意

ファイアウォールの設定は、対象サーバーの環境に応じて異なります。

B.2.4 Windows PowerShellの実行ポリシー変更

1. 管理者権限でWindows PowerShellを開き、以下のコマンドを実行します。

```
>set-executionpolicy remotesigned
```

2. 以下のメッセージが表示された場合、「Y」を入力後、[Enter]キーを押します。

```
実行ポリシーの変更
実行ポリシーは、信頼されていないスクリプトからの保護に役立ちます。実行ポリシーを変更すると、about_Execution_Policies
のヘルプ トピック http://go.microsoft.com/fwlink/?LinkID=135170
で説明されているセキュリティ上の危険にさらされる可能性があります。実行ポリシーを変更しますか?
[Y] はい(Y)  [N] いいえ(N)  [S] 中断(S)  [?] ヘルプ (既定値は "Y"): Y
```

B.2.5 ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントでは、複数の異なるドメイン環境を同時に監視することはできません。

1. Active DirectoryへのWinRMサービスのSPNの追加

   以下のコマンドを実行してActive DirectoryにWinRMサービスのSPNが登録されていることを確認します。

```
>setspn -L ＜監視対象ホスト名＞
```

   以下のようにWSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されれば、WinRMサービスのSPNが登録できています。

```
>setspn -L  ＜監視対象ホスト名＞
    WSMAN/＜監視対象ホスト名＞
    WSMAN/＜監視対象ホストのFQDN名＞
```

   WSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されない場合は、監視対象サーバーに対して以下のコマンドを実行してWinRMサービスを再起動してください。

```
>net stop winrm
```

```
>net start winrm
```

   WinRMサービスの再起動後に、WSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されない場合は、WinRMサービスのサービスプリンシパル名（SPN）を正しくActive Directoryに登録する必要があります。以下の手順を実行し、WinRMサービスのサービスプリンシパル名を登録してください。

```
>setspn -S WSMAN/＜監視対象ホスト名＞ ＜監視対象ホスト名＞
```

```
>setspn -S WSMAN/＜監視対象ホストのFQDN名＞ ＜監視対象ホスト名＞
```

2. Active Directoryへの監視対象サーバーのSPNの追加

   ドメインユーザーアカウントで監視するには、監視対象サーバーのサービスプリンシパル名（SPN）を正しくActive Directoryに登録する必要があります。以下の手順を実行し、監視対象サーバーのサービスプリンシパル名を登録してください。

```
>setspn -S HTTP/＜監視対象IPアドレス＞ ＜監視対象ホスト名＞
```

   ポイント

   ー 確認方法

```
>setspn -L ＜監視対象ホスト名＞
```

   ー 削除方法

```
>setspn -D HTTP/＜監視対象IPアドレス＞ ＜監視対象ホスト名＞
```

3. ISM-VAへドメイン情報の追加

   ドメインユーザーアカウントで監視するには、「3.4.2 ISM-VAの初期設定」を実施してください。

4. ISM-VAへDNS情報の追加

   ドメインユーザーアカウントで監視するには、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.3 監視対象への設定手順（OS：Red Hat Enterprise Linux）

ISMは、Red Hat Enterprise Linuxがインストールされている対象サーバーとssh（Secure Shell service）を使って通信します。必要な設定は、以下のとおりです。

- B.3.1 sshサービスの起動確認
- B.3.2 rootユーザーによるssh接続の有効化設定

- B.3.3 ドメインユーザーアカウント使用時の設定
- B.3.4 一般ユーザーアカウント使用時の設定
- B.3.5 ユーザーアカウント共通の設定

B.3.1 sshサービスの起動確認

sshdを起動するように設定してください。OSのバージョンに応じて、コマンドが異なります。

Red Hat Enterprise Linux 7 / 8 / 9 の場合

1. 以下のコマンドを実行して、sshdの自動起動を確認します。

```
# systemctl is-enabled sshd
```

以下のように表示された場合は、sshdの自動起動が無効になっています。

```
disabled
```

2. sshdの自動起動が無効になっている場合は、以下のコマンドを実行します。

```
# systemctl enable sshd
```

対象サーバーの次回起動時から、sshdが自動起動します。

3. sshdを起動します。

```
# systemctl start sshd
```

B.3.2 rootユーザーによるssh接続の有効化設定

Red Hat Enterprise Linux 9 以降の場合、デフォルトではssh経由でパスワードを使用してrootユーザーでログインすることが無効となっています。rootユーザーで監視をする場合は、以下の設定を実施してください。

1. 以下のコマンドを実行して設定ファイルを開きます。

```
# vi /etc/ssh/sshd_config
```

2. ファイル内のAuthentication のセクションに「PermitRootLogin yes」を追記します。

例:

```
# Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

3. sshdを再起動します。

```
# service sshd restart
```

再起動後、sshコマンドでrootによるログインが可能になります。

B.3.3 ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントで監視する場合、以下の点に注意してください。

ISM-VAへドメイン情報の追加

ドメインユーザーアカウントで監視するには、「3.4.2 ISM-VAの初期設定」を実施してください。

ISM-VAへDNS情報の追加

ドメインユーザーアカウントで監視するには、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

ドメインユーザーアカウント名の制約

Active Directoryに登録したドメインユーザー名をLinuxで使用する場合は、Linuxのユーザー名の制限についても注意してください。

- Linuxユーザー名として使えない代表例

  大文字、先頭文字の数字、ドットなどの記号は使用不可

Emulexカード情報収集時の制限

Avago/Emulex社製カードが搭載された機器では、「hbacmd」を使用しカード情報を収集します。

ドメインユーザーアカウントでカード情報を収集する場合は、「hbacmd」に管理者権限を付与してください。

詳しくは、『OneCommandManager Command Line Interface User Manual』を参照してください。

QLogicカード情報収集時の制限

ドメインユーザーアカウントではQLogic社製カードが搭載された機器の情報取得はできません。「OS情報編集」画面からrootユーザーを登録し、情報取得を行ってください。

ServerViewログ収集時の制限

ドメインユーザーアカウントではServerViewログの収集はできません。「OS情報編集」画面からrootユーザーを登録し、情報収集を行ってください。

ファームウェアアップデート時の制限

ドメインユーザーアカウントではオンラインファームアップデートを実施できません。「OS情報編集」画面からrootユーザーを登録し、ファームウェアアップデートを行ってください。

B.3.4 一般ユーザーアカウント使用時の設定

rootユーザー以外の一般ユーザーアカウントで監視する場合、以下の点に注意してください。

sudoコマンドの設定

該当ユーザーアカウントが、一般ユーザーアカウントのログインパスワードでsudoコマンドが実行できるように監視対象サーバーの設定を変更する必要があります。

以下は、user1のログインパスワードでsudoコマンドが実行できるように設定する場合の例です。

1. /etc/sudoersファイルを編集します。

```
# visudo
:
#Defaults targetpw           ・・・コメントアウト
root    ALL=(ALL)       ALL
user1   ALL=(ALL)       ALL   ・・・user1を追加
:
```

2. user1ユーザーで、監視対象サーバーにsshでログインします。

   sudoコマンドを実行した際にuser1のパスワードが求められれば、設定完了です。

環境変数の設定

該当アカウントで、監視対象サーバーにsshでログインしたあと、プロンプト表示文字列が、下記の条件を満たしていることを確認してください。下記の条件を満たしている場合、プロンプト表示文字列の設定を変更しないでください。環境変数PS1の値を変更することでプロンプト表示文字列を変更できます。

- ログイン時に、ホームディレクトリーに移動すること
- ログイン時のプロンプト表示文字列に"~"が含まれていること
- ログイン時のプロンプト表示文字列の"~"のあとに"$"、または"#"が含まれていること

例:[user1@localhost ~]$

環境変数PS1の設定値例:

```
[user1@localhost ~]$  echo $PS1
[¥u@¥h ¥W]¥$
```

B.3.5 ユーザーアカウント共通の設定

ログインシェルの設定

ユーザーアカウントのログインシェルは、/bin/bashを設定してください。ログインシェルを変更できない場合は、別のユーザーアカウントをLinux上で作成し、ISMに登録されたOS情報を更新してください。

該当ユーザーアカウントで監視対象サーバーにsshでログインし、以下のコマンドを実行してログインシェルを確認します。

```
# echo $SHELL
```

コマンド結果が/bin/bashでない場合は、以下のコマンドを実行してください。

```
# chsh -s /bin/bash
```

「.bashrc」の設定

1. 該当アカウントのホームディレクトリーにある「.bashrc」ファイルを開きます。

   「.bashrc」ファイルがない場合は、作成してください。

   ```
   # vi ~/.bashrc
   ```

2. 「.bashrc」ファイルに「/sbin」、「/usr/sbin」、「/usr/local/sbin」のパスを追記します。

   ```
   PATH=$PATH:/sbin
   PATH=$PATH:/usr/sbin
   PATH=$PATH:/usr/local/sbin
   ```

環境変数の設定

ServerViewのログ収集機能を実行するためには、該当アカウントの環境変数PS1の設定が必要です。「B.3.4 一般ユーザーアカウント使用時の設定」の「環境変数の設定」を参考に環境変数PS1を設定してください。

B.4 監視対象への設定手順(OS:SUSE Linux Enterprise Server)

ISMは、SUSE Linux Enterprise Serverがインストールされている対象サーバーとssh(Secure Shell service)を使って通信します。必要な設定は、以下のとおりです。

B.4.1 sshサービスの起動確認

SUSE Linux Enterprise Serverでは、デフォルトではsshdの起動が無効になっています。

sshdを起動するように設定してください。OSのバージョンに応じて、コマンドが異なります。

SUSE Linux Enterprise Server 12 / 15

1. 以下のコマンドを実行して、sshdの自動起動を確認します。

```
# systemctl is-enabled sshd
```

以下のように表示された場合は、sshdの自動起動が無効になっています。

```
disabled
```

2. sshdの自動起動が無効になっている場合は、以下のコマンドを実行します。

```
# systemctl enable sshd
```

対象サーバーの次回起動時から、sshdが自動起動します。

3. sshdを起動します。

```
# systemctl start sshd
```

B.4.2 ファイアウォールのポート開放

ファイアウォールを有効にしている場合、ファイアウォールの設定から、sshの通信を許可してください。

SUSE Linux Enterprise Serverのファイアウォールは、デフォルトでsshのポートを閉じています。

ファイアウォールの設定は、対象サーバーの環境に応じて異なります。

SUSE Linux Enterprise Server 12

以下は、YaSTを使用した場合のファイアウォールの設定例です。

1. 以下のコマンドを実行して、YaST Control Centerを表示します。

```
# yast
```

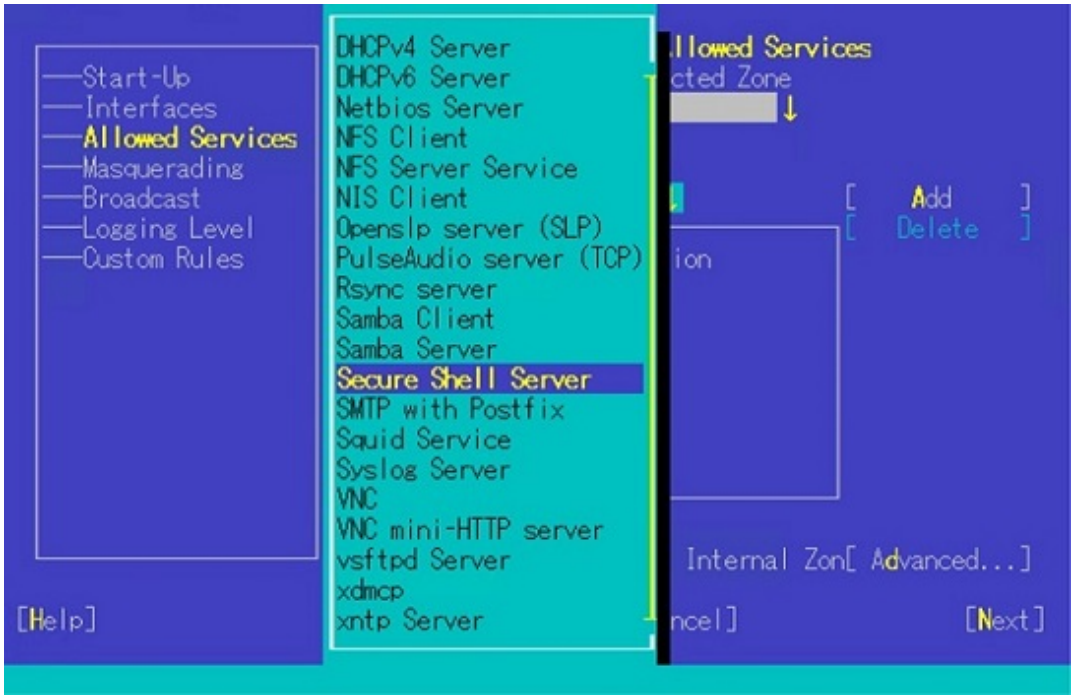
yast内での項目は、矢印キーと[TAB]キーを組み合わせて選択します。

2. [Security and Users]-[Firewall]を選択し、[Enter]キーを押します。

3. 「Start-Up」画面から、[Service Start]の状態を「Enable Firewall Automatic Starting」にします。

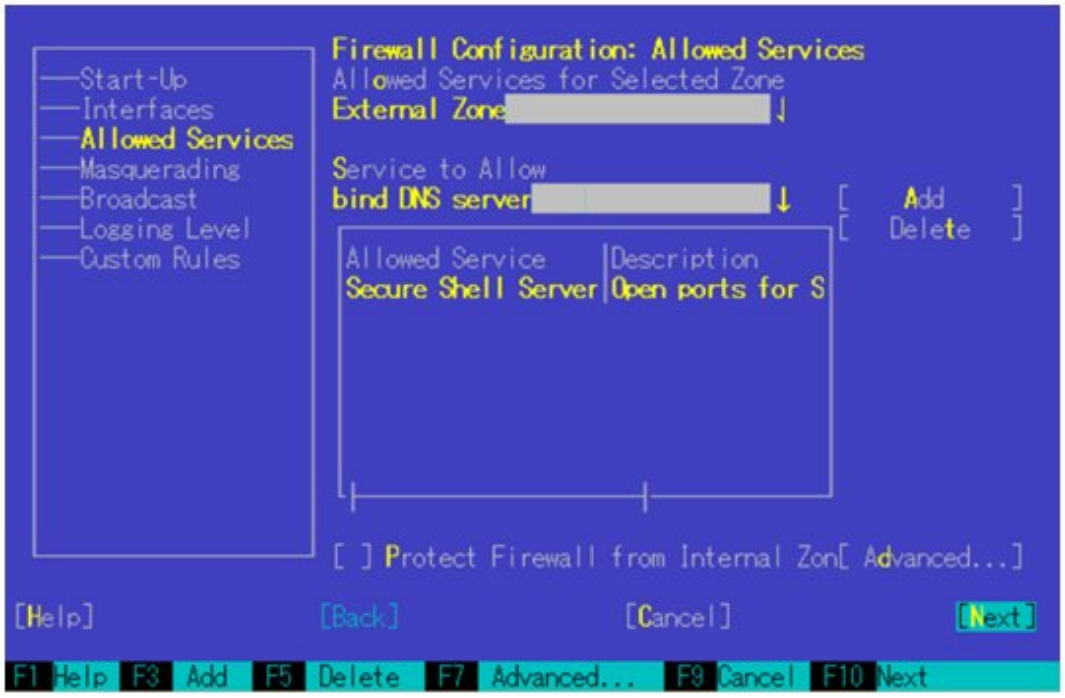
4. [Allowed Services]-[Service to Allow]へ移動し、下矢印のキーを押します。

5. 「Secure Shell Server」を選択し、[Enter]キーを押します。



6. [Add]へ移動し、[Enter]キーを押します。

7. [Allowed Service]に「Secure Shell Server」が追加されているのを確認し、[Next]へ移動して[Enter]キーを押します。



8. 「Firewall Configuration: Summary」画面が表示されたあと、[Finish]へ移動し、[Enter]キーを押して、ファイアウォールの設定を完了します。

9. [Quit]へ移動し、[Enter]キーを押して、YaST Control Centerを終了します。

SUSE Linux Enterprise Server 15

SUSE Linux Enterprise Server 15は、YaSTを使用したFirewallの設定をサポートしていません。「firewall-cmd」を使用してファイアウォールを設定します。

1. firewalldを起動します。

```
# systemctl start firewalld
```

2. 以下のコマンドを実行し、sshの通信を許可します。

```
# firewall-cmd --permanent --add-service=ssh
# firewall-cmd --reload
```

B.4.3 ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントで監視する場合、以下の点に注意してください。

ISM-VAへドメイン情報の追加

ドメインユーザーアカウントで監視するには、「3.4.2 ISM-VAの初期設定」を実施してください。

ISM-VAへDNS情報の追加

ドメインユーザーアカウントで監視するには、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

Emulexカード情報収集時の制限

Avago/Emulex社製カードが搭載された機器では「hbacmd」を使用しカード情報を収集します。

ドメインユーザーアカウントでカード情報を収集する場合は、「hbacmd」に管理者権限を付与してください。

詳しくは、『One Command Manager Command Line Interface User Manual』を参照してください。

QLogicカード情報収集時の制限

ドメインユーザーアカウントでは、QLogic社製カードが搭載された機器の情報取得はできません。「OS情報編集」画面からrootユーザーを登録し、情報取得を行ってください。

ServerViewログ収集時の制限

ドメインユーザーアカウントでは、ServerViewログの収集はできません。「OS情報編集」画面からrootユーザーを登録し、情報収集を行ってください。

ファームウェアアップデート時の制限

ドメインユーザーアカウントでは、オンラインファームアップデートを実施できません。「OS情報編集」画面からrootユーザーを登録し、ファームウェアアップデートを行ってください。

B.4.4 一般ユーザーアカウント使用時の設定

rootユーザー以外の一般ユーザーアカウントで監視する場合、以下の点に注意してください。

sudoコマンドの設定

該当ユーザーアカウントが、一般ユーザーアカウントのログインパスワードでsudoコマンドが実行できるように監視対象サーバーの設定を変更する必要があります。

以下は、user1のログインパスワードでsudoコマンドが実行できるように設定する場合の例です。

1. /etc/sudoersファイルを編集します。

```
# visudo
:
#Defaults targetpw           ・・・コメントアウト
root    ALL=(ALL)       ALL
user1   ALL=(ALL)       ALL   ・・・user1を追加
:
```

2. user1ユーザーで、監視対象サーバーにsshでログインします。

   sudoコマンドを実行した際にuser1のパスワードが求められれば、設定完了です。

環境変数の設定

該当ユーザーアカウントで、監視対象サーバーにsshでログインしたあと、プロンプト表示文字列が、下記の条件を満たしていることを確認してください。下記の条件を満たしている場合、プロンプト表示文字列の設定を変更しないでください。環境変数PS1の値を変更することでプロンプト表示文字列を変更できます。

- ログイン時に、ホームディレクトリーに移動すること
- ログイン時のプロンプト表示文字列に"~"が含まれていること
- ログイン時のプロンプト表示文字列の"~"のあとに"$"、または"#"が含まれていること

例:[user1@localhost ~]$

環境変数PS1の設定値例:

```
[user1@localhost ~]$ echo $PS1
[¥u@¥h ¥W]¥$
```

B.4.5 ユーザーアカウント共通の設定

ログインシェルの設定

ユーザーアカウントのログインシェルは、/bin/bashを設定してください。ログインシェルを変更できない場合は、別のユーザーアカウントをLinux上で作成し、ISMに登録してあるOS情報を更新してください。

該当ユーザーアカウントで監視対象サーバーにsshでログインし、以下のコマンドを実行してログインシェルを確認します。

```
# echo $SHELL
```

コマンド結果が/bin/bashでない場合は、以下のコマンドを実行してください。

```
# chsh -s /bin/bash
```

「.bashrc」の設定

1. 該当アカウントのホームディレクトリーにある「.bashrc」ファイルを開きます。

   「.bashrc」ファイルがない場合は、作成してください。

   ```
   # vi ~/.bashrc
   ```

2. 「.bashrc」ファイルに「/sbin」、「/usr/sbin」、「/usr/local/sbin」のパスを追記します。

   ```
   PATH=$PATH:/sbin
   PATH=$PATH:/usr/sbin
   PATH=$PATH:/usr/local/sbin
   ```

環境変数の設定

ServerViewのログ収集機能を実行するためには、該当アカウントの環境変数PS1の設定が必要です。「B.4.4 一般ユーザーアカウント使用時の設定」の「環境変数の設定」を参考に環境変数PS1を設定してください。

B.5 監視対象への設定手順（OS：AlmaLinux）

ISMは、AlmaLinuxがインストールされている対象サーバーとssh（Secure Shell service）を使って通信します。必要な設定は、「B.3 監視対象への設定手順（OS：Red Hat Enterprise Linux）」を参考にしてください。

B.6 監視対象への設定手順（OS：VMware ESXi）

ISMは、VMware ESXiがインストールされている対象サーバーとvSphere API、CIMプロトコルを使用して通信します。必要な設定は、以下のとおりです。

B.6.1 VMware ESXiのロックダウンモード有効時に必要な設定

VMware ESXiのロックダウンモードが有効になっている場合、ISM-VAでは監視できません。

現象としてはノード情報の取得に失敗します。

回避方法としてVMware ESXiのログインアカウントを例外ユーザーリストに追加することで、ロックダウンモードが有効な場合でもISM-VAで監視できます。例外ユーザーリストへの登録はvSphere Client から実施します。

B.6.2 ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントで監視する場合、以下の点に注意して実施してください。

ISM-VAへドメイン情報の追加

ドメインユーザーアカウントで監視するには、「3.4.2 ISM-VAの初期設定」を実施してください。

ISM-VAへDNS情報の追加

ドメインユーザーアカウントで監視するには、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.7 監視対象への設定手順(OS:Azure Stack HCI)

ISMは、Azure Stack HCIがインストールされている監視対象機器に対してWS-Managementプロトコルを使用します。通信方式はhttpsプロトコル+Basic認証を使用します。必要な設定は、以下のとおりです。

- B.7.1 WinRMサービスの起動確認
- B.7.2 WinRMサービスの設定
- B.7.3 ファイアウォールのポート開放
- B.7.4 Windows PowerShellの実行ポリシー変更
- B.7.5 ドメインユーザーアカウント使用時の設定

B.7.1 WinRMサービスの起動確認

1. 管理者権限でコマンドプロンプトを開いて以下のコマンドを実行し、WinRMサービスの起動を確認します。

```
>sc query winrm
```

2. 以下の結果を確認し、STATEがRUNNINGになっていることを確認します。

```
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

3. WinRMサービスが起動されていない場合、以下のコマンドを実行し、WinRMサービスを起動します。

```
>sc start winrm
```

4. WinRMサービスを遅延自動起動(delayed-auto)に設定します。

```
>sc config winrm start=delayed-auto
```

B.7.2 WinRMサービスの設定

WinRMサービスの設定

ポイント

初期設定ではBasic認証が許可されていないため、Basic認証の許可の設定を行います。

以下のコマンドを実行します。

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

https通信を使用するためBasic認証の通信は暗号化されます。

1. 管理者権限でコマンドプロンプトを開き、以下のコマンドを実行します。

```
>winrm quickconfig
```

「WinRM サービスは、既にこのコンピューターで実行されています。このコンピューター上でのリモート管理には、WinRM が既に設定されています。」と表示された場合は、すでに設定が完了しているため「https通信の設定」に進んでください。

2. 「y」を入力後、[Enter]キーを押します。

```
WinRM サービスは、既にこのコンピューターで実行されています。
WinRM は、管理用にこのコンピューターへのリモート アクセスを許可するように設定されていません。
次の変更を行う必要があります:

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成してください。
変更しますか [y/n]? y
```

以下のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成しました。
```

3. 以下のコマンドを実行して、カードの種類や数に応じてMaxConcurrentOperationsPerUserの数値を大きくします。

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="数値"}
```

例:1500に設定した場合(Azure Stack HCIでは、デフォルトが1500であるため1500を推奨します。)

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

https通信の設定

https通信をするためには、証明書の設定が必要になります。

1. 自己署名ルート証明書の作成、登録

   クライアント証明書に署名するための自己署名ルート証明書を作成します。

   詳細な証明書作成の流れについては、下記のURLを参照してください。

   https://docs.microsoft.com/ja-jp/azure/vpn-gateway/vpn-gateway-certificates-point-to-site

   a. コマンドプロンプトからPowerShellを起動します。

   b. 自己署名ルート証明書を作成します。

      対象サーバーの環境に合わせてコマンドを実行する必要があります。

      PowerShellで以下のようなコマンドを実行します。

      以下は、対象サーバーのサーバー名を"192.168.10.10"に設定し、証明書の有効期間を10年に設定した場合のコマンド例です。

      ```
      >$cert = New-SelfSignedCertificate `
      -Subject "CN=192.168.10.10" -NotAfter $(Get-Date).AddDays(3650) `
      -CertStoreLocation cert:¥LocalMachine¥My `
      -KeyUsage CertSign,CRLSign
      ```

   c. 信頼するルート証明書として登録します。

      PowerShellで以下のようなコマンドを実行します。

      ```
      >Export-Certificate -Cert $cert -FilePath <証明書のファイル名.cer>
      ```

      ```
      >Import-Certificate -Cert cert:¥LocalMachine¥Root -FilePath <証明書のファイル名.cer>
      ```

2. クライアント証明書の作成、登録

   手順1で作成した証明書を元にクライアント証明書を作成します。

   a. クライアント証明書を作成します。

      PowerShellで以下のようなコマンドを実行します。

      以下は、対象サーバーのサーバー名を"192.168.10.10"に設定し、証明書の有効期間を10年に設定した場合のコマンド例です。

```
>$cert = Get-ChildItem `
-Path cert:¥LocalMachine¥My | where { $_.Subject -eq "CN=192.168.10.10" }
```

```
>$client= New-SelfSignedCertificate `
-Subject "CN=192.168.10.10, C=Japan" `
-NotAfter $(Get-Date).AddDays(3650) `
-CertStoreLocation cert:¥LocalMachine¥My `
-Signer $cert `
-TextExtension @( `
"2.5.29.37={text}1.3.6.1.5.5.7.3.1" `
)
```

b. クライアント証明書を登録します。

PowerShellで以下のようなコマンドを実行します。

以下は、パスワードを"password"とした場合のコマンド例です。

```
>$password = ConvertTo-SecureString -String "password" -Force -AsPlainText
```

```
>Export-PfxCertificate -Cert $client -FilePath ＜証明書のファイル名.pfx＞ -Password $password
```

WinRMサービスへの証明書に記載された拇印を登録

1. 拇印(Thumbprint)の確認

以下は、LocalMachine¥myに証明書を保存した場合の確認方法です。

a. コマンドプロンプトからPowerShellを起動します。

b. 拇印を確認します。以下のコマンドを実行します。

```
>ls cert:LocalMachine¥my
```

以下のように表示されます。

```
PS C:¥Windows¥system32> ls cert:LocalMachine¥my

ディレクトリ: Microsoft.PowerShell.Security¥Certificate::LocalMachine¥my
Thumbprint                                Subject
----------                                -------
1C3E462623BAF91A5459171BD187163D23F10DD9  CN=192.168.10.10
```

2. WinRMリスナーに証明書に記載された拇印を登録

PowerShellを終了し、以下のコマンドを実行します。"HTTPS" と "@" の間にはスペースが必要です。

```
>winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="＜証明書を作成したときに設定したCN名＞
";CertificateThumbprint="＜作成した証明書の拇印＞"}
```

3. WinRMリスナーの登録確認

以下のコマンドを実行します。

```
>winrm get winrm/config/listener?Address=*+Transport=HTTPS
```

以下のようなコマンド結果が返ってくれば、WinRMのリスナーが登録できています。

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 192.168.10.10
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
```

```
    ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

B.7.3 ファイアウォールのポート開放

WinRMサービスがリクエストの受付をできるように、WinRMリスナーで設定したポートを開放する必要があります。https通信のデフォルトポート番号は、5986です。

管理者権限でWindows PowerShellを開き、以下のコマンドを実行します。

```
>New-NetFirewallRule -DisplayName ＜ファイアウォールルール名＞ -Action Allow -Direction Inbound -Enabled True -Protocol TCP
-LocalPort ＜ポート番号＞
```

例:ポート番号5986を開放するルールに、"WinRM"という名前を設定します。

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort 5986
```

注意

ファイアウォールの設定は、対象サーバーの環境に応じて異なります。

B.7.4 Windows PowerShellの実行ポリシー変更

1. 管理者権限でWindows PowerShellを開き、以下のコマンドを実行します。

```
>set-executionpolicy remotesigned
```

2. 以下のメッセージが表示された場合、「Y」を入力後、[Enter]キーを押します。

```
実行ポリシーの変更
実行ポリシーは、信頼されていないスクリプトからの保護に役立ちます。実行ポリシーを変更すると、about_Execution_Policies
のヘルプ トピック http://go.microsoft.com/fwlink/?LinkID=135170
で説明されているセキュリティ上の危険にさらされる可能性があります。実行ポリシーを変更しますか?
[Y] はい(Y)  [N] いいえ(N)  [S] 中断(S)  [?] ヘルプ (既定値は "Y"): Y
```

B.7.5 ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントでは、複数の異なるドメイン環境を同時に監視することはできません。

1. Active DirectoryへのWinRMサービスのSPNの追加

   以下のコマンドを実行してActive DirectoryにWinRMサービスのSPNが登録されていることを確認します。

```
>setspn -L ＜監視対象ホスト名＞
```

   以下のようにWSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されれば、WinRMサービスのSPNが登録できています。

```
>setspn -L  ＜監視対象ホスト名＞
    WSMAN/＜監視対象ホスト名＞
    WSMAN/＜監視対象ホストのFQDN名＞
```

   WSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されない場合は、監視対象サーバーに対して以下のコマンドを実行してWinRMサービスを再起動してください。

```
>net stop winrm
```

```
>net start winrm
```

WinRMサービスの再起動後に、WSMAN/＜監視対象ホスト名＞、WSMAN/＜監視対象ホストのFQDN名＞が出力されない場合は、WinRMサービスのサービスプリンシパル名（SPN）を正しくActive Directoryに登録する必要があります。以下の手順を実行し、WinRMサービスのサービスプリンシパル名を登録してください。

```
>setspn -S WSMAN/＜監視対象ホスト名＞ ＜監視対象ホスト名＞
```

```
>setspn -S WSMAN/＜監視対象ホストのFQDN名＞ ＜監視対象ホスト名＞
```

2. Active Directoryへの監視対象サーバーのSPNの追加

   ドメインユーザーアカウントで監視するには、監視対象サーバーのサービスプリンシパル名（SPN）を正しくActive Directoryに登録する必要があります。以下の手順を実行し、監視対象サーバーのサービスプリンシパル名を登録してください。

```
>setspn -S HTTP/＜監視対象IPアドレス＞ ＜監視対象ホスト名＞
```

ポイント

ー 確認方法

```
>setspn -L ＜監視対象ホスト名＞
```

ー 削除方法

```
>setspn -D HTTP/＜監視対象IPアドレス＞ ＜監視対象ホスト名＞
```

3. ISM-VAへドメイン情報の追加

   ドメインユーザーアカウントで監視するには、「3.4.2 ISM-VAの初期設定」を実施してください。

4. ISM-VAへDNS情報の追加

   ドメインユーザーアカウントで監視するには、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.8 監視対象への設定手順（仮想化管理ソフトウェア：vCenter Server）

ISMは、vCenter Serverに対して通信します。必要な設定は、以下のとおりです。

B.8.1 ISM-VAへDNS情報の追加

vCenterにESXiホストをFQDNで登録している環境で監視を行う際には、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.8.2 ドメインユーザーアカウント使用時の設定

vCenter Serverから情報を取得するためには、vCenter Serverに登録されている各ホストへの設定が完了している必要があります。「B.6 監視対象への設定手順（OS：VMware ESXi）」を参照し、各ホストへの設定を実施してください。

B.9 監視対象への設定手順（仮想化管理ソフトウェア：Microsoft Failover Cluster）

ISMは、Microsoft Failover Clusterに対して通信します。必要な設定は、以下のとおりです。

B.9.1 ドメインユーザーアカウント使用時の設定

1. クラスタを構成する各ホストへのWinRM設定

   Microsoft Failover Clusterから情報を取得するためには、クラスタを構成する各ホストへの設定が完了している必要があります。「B.2 監視対象への設定手順（OS：Windows）」を参照し、各ホストへの設定を実施してください。

2. Active DirectoryへのSPNの追加

   ドメインユーザーアカウントを使用しWindows Serverの監視をする際には、監視対象クラスタのサービスプリンシパル名（SPN）を正しくActive Directoryに登録する必要があります。以下の手順を実行し、監視対象クラスタのサービスプリンシパル名を登録してください。

```
> setspn -S HTTP/＜監視対象クラスタIP＞ ＜監視対象クラスタ名＞
```

ポイント

確認方法

```
> setspn -L ＜監視対象クラスタ名＞
```

コマンド実行結果に以下が出力されていれば、正しく登録されています。

```
HTTP/＜監視対象クラスタIP＞
```

3. ISM-VAへドメイン情報の追加

   ドメインユーザーアカウントでの監視を行う際には、「3.4.2 ISM-VAの初期設定」を実施してください。

4. ISM-VAへDNS情報の追加

   ドメインユーザーアカウントでの監視を行う際には、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

5. Active Directoryへ Kerberos委任の構成

   a. Active Directory サーバーにログオンします。

   b. サーバーマネージャーを開きます。

   c. [ツール]ボタンから[Active Directoryユーザーとコンピューター]を選択します。

   d. ドメインを展開し、[コンピューター]フォルダーを展開します。

   e. 右側ウィンドウで、クラスタノード名またはクラスタ名を右クリックし、[プロパティ]を選択します。

   f. [委任]タブで、[任意のサービスへ委任でこのコンピューターを信頼する]にチェックを付けます。

   g. [OK]を選択し、すべてのクラスタノードおよびクラスタに対して手順e～fを実施します。

B.10 監視対象への設定手順（仮想化管理ソフトウェア：Microsoft System Center）

「B.2 監視対象への設定手順（OS：Windows）」を参照し、Microsoft System Centerのインストールされている各ホスト、仮想マシンに対して設定を実施してください。

B.11 監視対象への設定手順（仮想化管理ソフトウェア：KVM）

ポイント

ドメインユーザー使用時の場合、仮想化管理ソフトウェアに応じて手順が異なります。以下から該当する手順を参照してください。

- B.11.1 KVM Red Hat Enterprise Linuxへの設定手順（ドメインユーザー使用時）
- B.11.2 KVM SUSE Linux Enterprise Serverへの設定手順（ドメインユーザー使用時）
- B.11.3 KVM AlmaLinuxへの設定手順（ドメインユーザー使用時）

B.11.1 KVM Red Hat Enterprise Linuxへの設定手順(ドメインユーザー使用時)

KVM情報を取得するため、監視対象でSSSDサービスを設定します。

必要なパッケージを以下に示します。

- krb5-workstation
- samba
- samba-client
- samba-common
- sssd

以降は、ターミナルよりrootユーザーで設定してください。

1. 「/etc/hosts」の編集

   a. 「/etc/hosts」ファイルを開きます。

   ```
   # vi /etc/hosts
   ```

   b. 以下を追記します。

   - 監視対象となるKVMサーバーのIPアドレスとFQDN、ホスト名
   - ISM-VAのIPアドレス

   例:

   ```
   192.168.30.222 rhel73.win2016.local rhel73
   192.168.30.228
   ```

   この設定はローカル(ホスト内)でのホスト名には反映されません。ただし、この設定がないと後述のActive Directoryへの参加コマンド実行時にエラーとなります。

2. 「/etc/krb5.conf」の編集

   a. 「/etc/krb5.conf」ファイルを開きます。

   ```
   # vi /etc/krb5.conf
   ```

   b. [libdefaults]セクションのdefault_realmにドメイン名を大文字で設定します。

   例:

   ```
   [libdefaults]
    dns_lookup_realm = true
    dns_lookup_kdc = true
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    default_realm = WIN2016.LOCAL
   ```

   c. [realms]セクションを設定します。

   例:

   ```
   [realms]
    WIN2016.LOCAL = {
     kdc = 192.168.30.69
     admin_server = WIN2016-ADVM.WIN2016.LOCAL
    }
   ```

kdcには、Kerberosのチケットを発行するサーバーのIPアドレスを設定します。

admin_serverには、Kerberos管理サーバーのFQDNを設定します。

通常、kdcとadmin_serverは、DNSサーバーとActive Directoryサーバーと同じサーバーです。

d. [domain_realm]セクションを設定します。

例:

```
[domain_realm]
 win2016.local = WIN2016.LOCAL
 .win2016.local = WIN2016.LOCAL
```

大文字・小文字は上記の例のようにし、実際に使用しているドメイン名を設定してください。

3. 「/etc/samba/smb.conf」の編集

a. 「/etc/samba/smb.conf」ファイルを開きます。

```
# vi /etc/samba/smb.conf
```

b. [global]セクション以外をすべて削除し、[global]セクションを以下のように設定します。

例:

```
[global]
   workgroup = WIN2016
   client signing = yes
   client use spnego = yes
   kerberos method = secrets and keytab
   log file = /var/log/samba/%m.log
   realm = WIN2016.LOCAL
   security = ads
```

workgroupとrealmは、実際に使用しているドメイン名を設定してください。

4. 「/etc/sssd/sssd.conf」の作成

a. 「/etc/sssd/sssd.conf」ファイルを開きます。初期状態では存在しないので、新規作成します。

```
# vi /etc/sssd/sssd.conf
```

例:

```
[sssd]
config_file_version = 2
services = pam,nss
domains = WIN2016.LOCAL

[pam]

[nss]
filter_groups = root
filter_users = root

[domain/WIN2016.LOCAL]
id_provider = ad
auth_provider = ad
enumerate = false
```

```
cache_credentials = false
case_sensitive = false
```

注意

[sssd]セクションのdomainsと[domain/WIN2016.LOCAL]セクションのセクション名は、実際に使用しているドメイン名を設定してください。

b. ドメインユーザーのログイン時にホームディレクトリーを自動作成する場合、「/etc/sssd/sssd.conf」の[domain/ドメイン名]セクションに以下を追加します。

```
fallback_homedir = /home/%u
```

5. 「/etc/sssd/sssd.conf」のパーミッションの変更

「/etc/sssd/sssd.conf」のパーミッションを600に変更します。

```
# chmod 600 /etc/sssd/sssd.conf
```

注意

600以外はsssdサービス起動時にエラーとなるので注意してください。

6. ローカル(ホスト上)のホスト名設定

以下のコマンドで、ローカル(ホスト上)のホスト名を設定します。

```
# hostnamectl set-hostname <ホストのFQDN>
```

例:

```
# hostnamectl set-hostname rhel73.win2016.local
```

注意

この設定はローカル(ホスト内)でのホスト名の設定です。ネットワーク上でのホスト名には反映されません。ホストのFQDNは、手順1で設定した「/etc/hosts」のホストのFQDNと一致させてください。

7. DNSサーバーのIPアドレス設定

a. 以下のコマンドで、DNSサーバーのIPアドレスを設定し、インターフェイスを再起動します。

```
# nmcli connection modify <インターフェイス名> ipv4.dns <DNSサーバーのIPアドレス>
# systemctl restart NetworkManager
```

b. インターフェイス名を調べるには、以下のコマンドを実行します。

```
# ip addr
```

c. 設定を確認するには、以下のコマンドを実行します。

```
# host <Kerberos管理サーバー名>
```

例:

```
# host WIN2016-ADVM.WIN2016.LOCAL
```

出力にIPアドレスが含まれていれば正しく設定されています。

8. Kerberos発券許可証の入手

   a. 以下のコマンドで、Kerberos発券許可証を入手します。

   ```
   # kinit Administrator
   ```

   b. パスワードの入力を要求されるので、ドメイン管理ユーザーAdministratorのパスワードを入力します。

   c. 設定を確認するには、以下のコマンドを実行します。

   ```
   # klist
   ```

   ドメイン情報が出力されれば、正しく設定されています。

   失敗した場合は、「/etc/krb5.conf」を確認してください。

9. Active Directoryへの参加

   a. 以下のコマンドで、Active Directoryに参加します。

   ```
   # net ads join -U Administrator
   ```

   b. パスワードの入力を要求されるので、ドメイン管理ユーザーAdministratorのパスワードを入力します。

   c. 設定を確認するには、以下のコマンドを実行します。

   ```
   # net ads info
   ```

   サーバー情報（LDAP serverと表示されます）とドメイン情報が出力されれば、正しく設定されています。

   失敗した場合は、ホスト名の設定と「/etc/samba/smb.conf」の設定を確認してください。または、手順13のポイントを参照してください。

10. システム認証の設定

    以下のコマンドで、システム認証（監視先サーバーの認証）の設定を行います。

    このコマンドによって、関連設定ファイルが自動的に更新されます。

    ー ドメインユーザーのホームディレクトリーを自動作成しない場合

    ```
    # authconfig --enablesssd --enablesssdauth --enablelocauthorize --update
    ```

    ー ドメインユーザーのホームディレクトリーを自動作成する場合

    あらかじめ、手順4内の手順bを実施後、以下を実行してください。

    ```
    # authconfig --enablesssd --enablesssdauth --enablelocauthorize --enablemkhomedir --update
    ```

注意

Red Hat Enterprise Linux8.0 以降では、authconfigの代わりにauthselectが推奨されています。

authselectを使用するためには、以下のコマンドを実行してください。

```
# authselect select sssd with-mkhomedir
```

ドメインユーザーでログイン時ホームディレクトリーが自動で作成されないときは、手動で作成してください。

11. SSSD（System Security Services Daemon）サービスの起動

    a. 以下のコマンドでSSSDサービスを起動します。

    ```
    # systemctl enable sssd
    # systemctl start sssd
    ```

b. サービスの起動を確認するには、以下のコマンドを実行します。

```
# systemctl status sssd
```

正常に起動していれば、正しく設定されています。

失敗した場合は、「/etc/sssd/sssd.conf」の内容とファイルパーミッションを確認してください。

12. ドメインユーザーでのログイン確認

以下のコマンドのどちらかを使用して、SSHプロトコルでのログイン確認ができます。ドメインユーザー名の表記方法については、下記のポイントを参照してください。

```
# ssh ＜ドメインユーザー名＞@＜監視対象サーバーIPアドレス＞
```

```
# ssh -l ＜ドメインユーザー名＞ ＜監視対象サーバーIPアドレス＞
```

例:

```
# ssh administrator@192.168.30.222
```

```
# ssh 'administrator@win2016'@192.168.30.222
```

```
# ssh -l 'win2016.local¥administrator' 192.168.30.222
```

どの方法でもログインできれば、正しく設定されています。

ポイント

ー ドメインユーザー名の表記方法

ドメインユーザー名の表記方法は、以下の表のようにいくつか書き方があります。なお、「/etc/sssd/sssd.conf」の[domain/WIN2016.ドメイン名]でcase_sensitive = falseとしているため、大文字・小文字は区別しません。

ドメインユーザー名の表記	表記例
ユーザー名	administrator
'ドメインプレフィックス¥ユーザー名'	'win2016¥administrator'
'ドメインプレフィックス.ドメイン名サフィックス¥ユーザー名'	'win2016.local¥administrator'
'ユーザー名@ドメインプレフィックス'	'administrator@win2016'
'ユーザー名@ドメインプレフィックス.ドメイン名サフィックス'	'administrator@win2016.local'

ー ドメインユーザーの存在確認

以下のコマンドのどちらかを使用して、ドメインユーザーの存在確認ができます。ドメインユーザー名は、上記のドメインユーザー名の表記方法のどれを使用しても結構です。

```
# id ＜ドメインユーザー名＞
```

```
# getent passwd ＜ドメインユーザー名＞
```

ユーザー情報が表示されれば、正しく設定されています。

13. ドメインユーザーの設定

「B.11.4 一般ユーザーアカウント使用時の設定」に従って、ドメインユーザーの設定を行ってください。

ポイント

ホスト名を変更後ログインできなくなった場合

ネットワーク上のホスト名とローカルのホスト名の両方を変更したあと、以下の2つのコマンドを実行します。

```
# net ads join -U Administrator
# systemctl restart sssd
```

それでもログインに失敗する場合は、過去の設定が「/etc/krb5.keytab」に残っている可能性があるため、以下のコマンドで/etc/krb5.keytabを削除してから、上記のコマンドを再実行します。

```
# rm /etc/krb5.keytab
```

14. ISM-VAへドメイン情報の追加

    「3.4.2 ISM-VAの初期設定」を実施してください。

15. ISM-VAへDNS情報の追加

    「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.11.2 KVM SUSE Linux Enterprise Serverへの設定手順(ドメインユーザー使用時)

KVM情報を取得するため、監視対象でSSSDサービスを設定します。

以降の設定は、ターミナルよりyastコマンドを使うか、GUIのメニューよりYaSTを使って行ってください。ここでは、yastコマンドを使用した方法について示します。

1. yastコマンドの起動

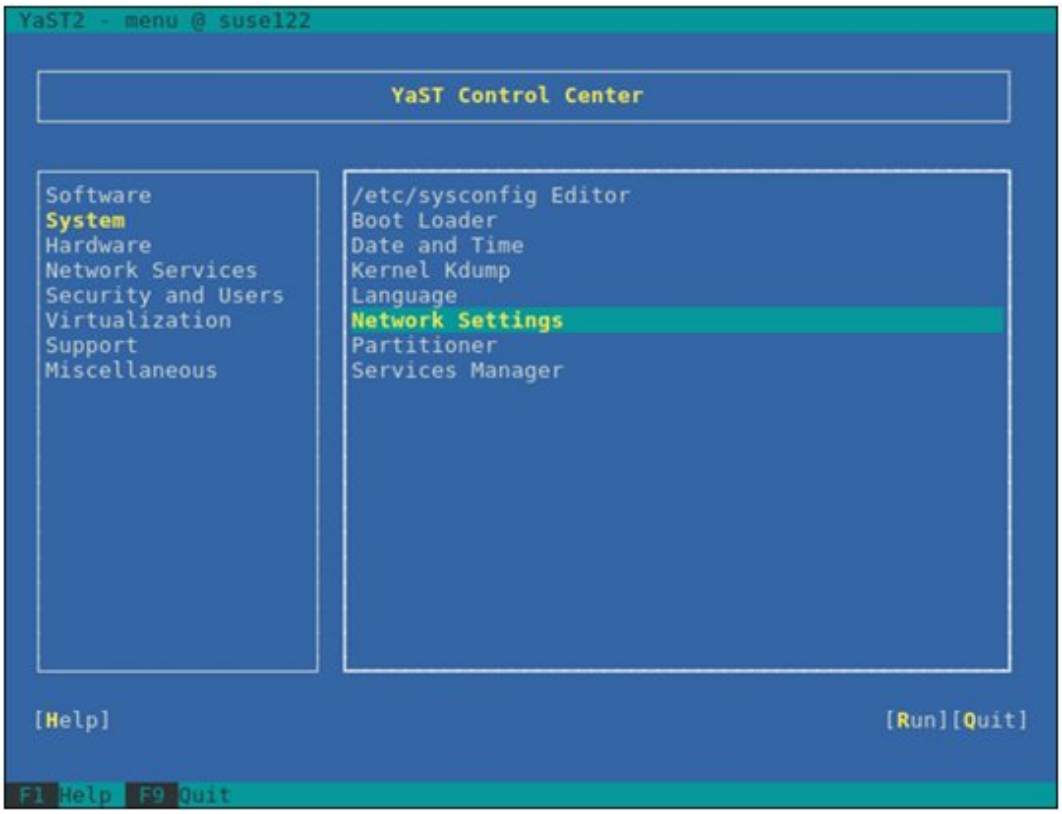
   ターミナルよりrootユーザーで以下のコマンドを実行します。

   ```
   # yast
   ```

   yast内での項目の選択は、矢印キーと[Tab]キーを組み合わせて選択します。

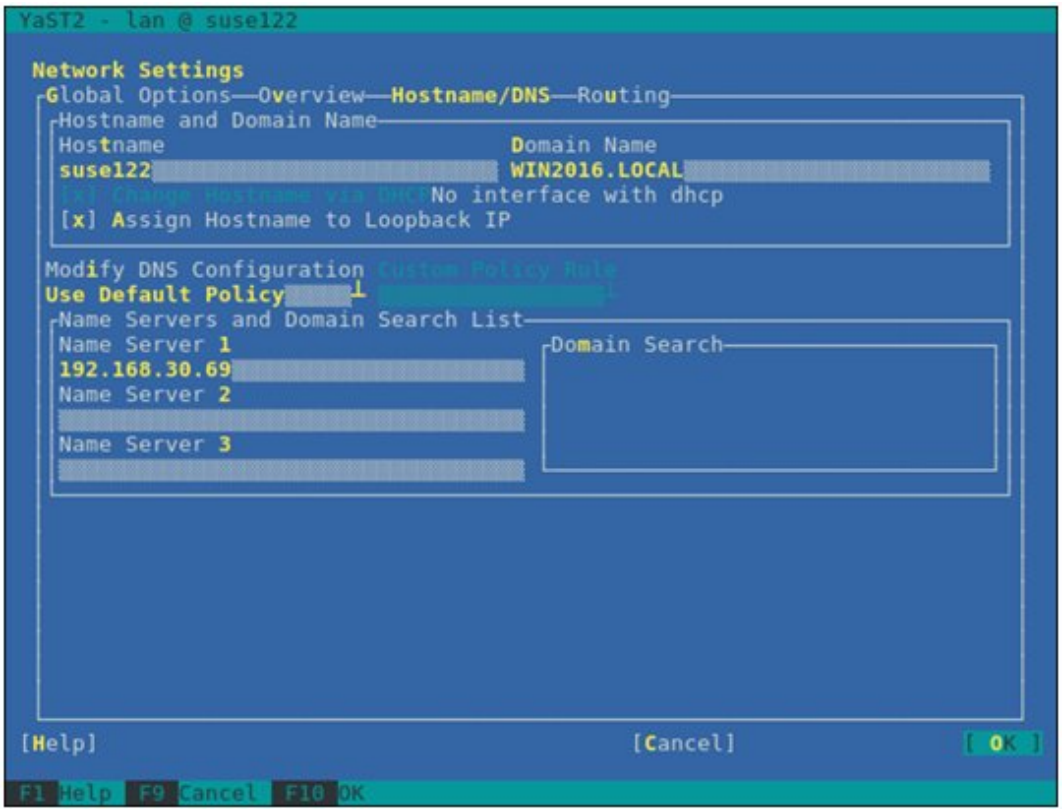
2. ホスト名／DNSの設定

   a. [System]-[Network Settings]を選択し、[Enter]キーを押します。



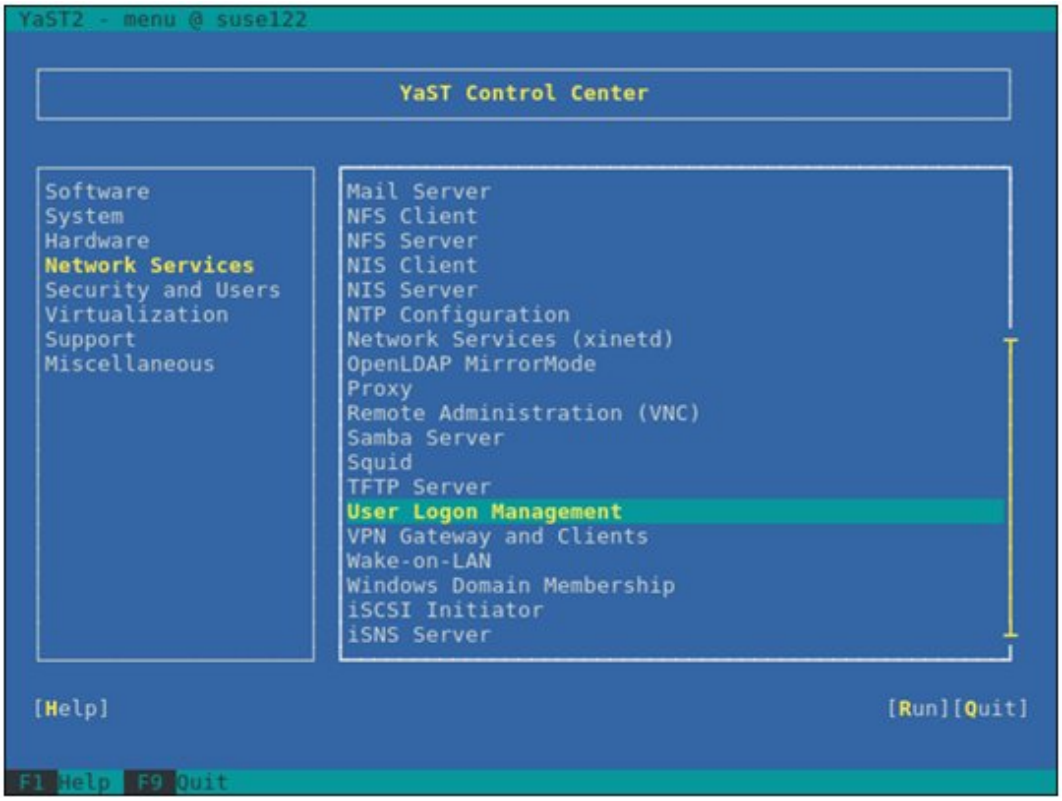
b. Hostname/DNSを選択し、以下の項目を設定してから[OK]を選択し、[Enter]キーを押します。

- Hostname
- Domain Name
- Assign Hostname to Loopback IP
- Name Server 1

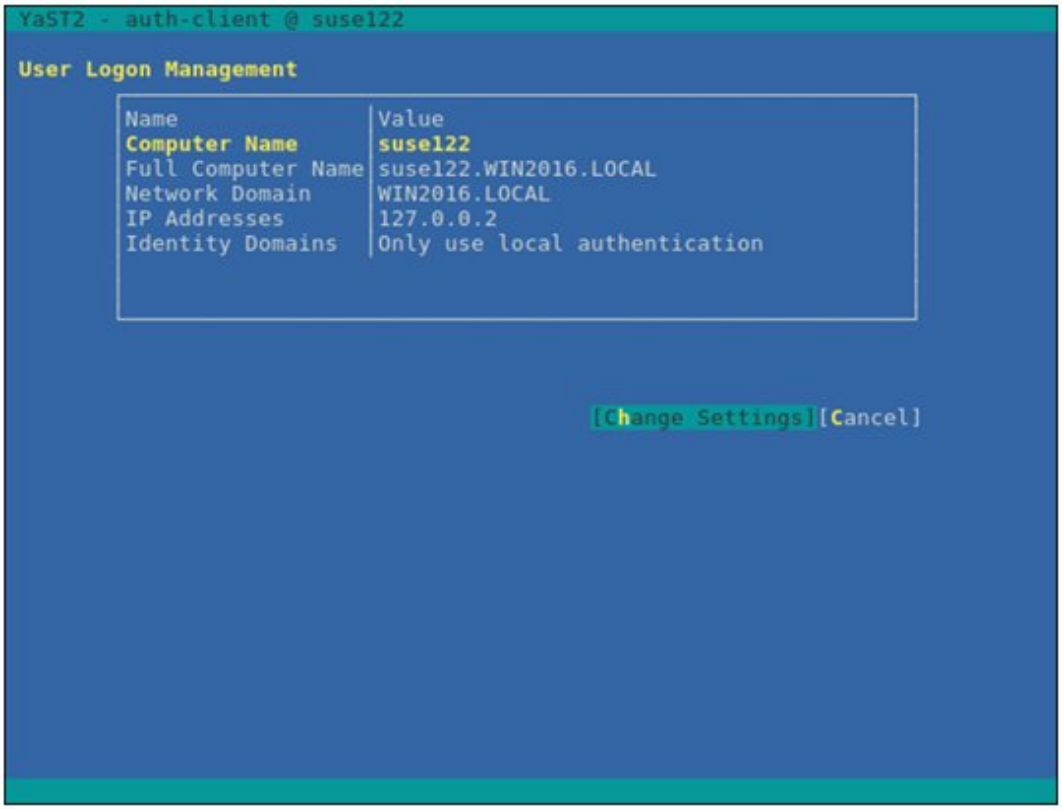


3. SSSDサービスの設定

a. [Network Services]-[User Logon Management]を選択し、[Enter]キーを押します。

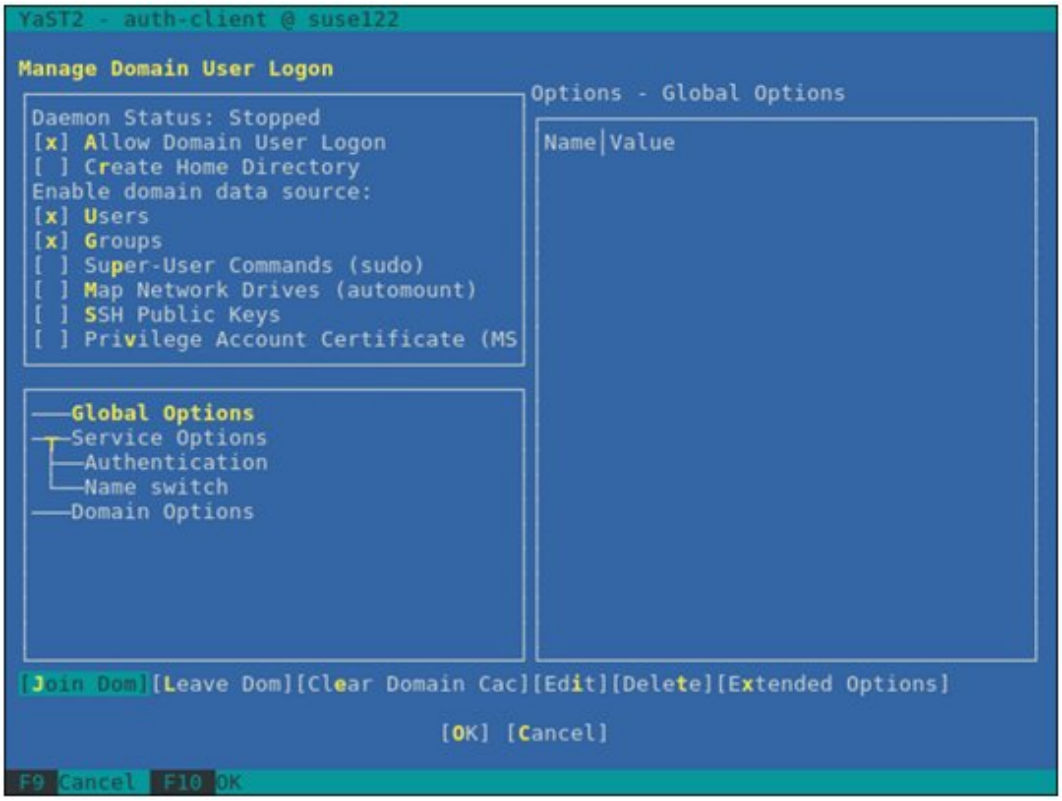


b. [Change Settings]を選択し、[Enter]キーを押します。



c. 以下の項目にチェックを付け、[Join Dom]を選択し、[Enter]キーを押します。

- Allow Domain User Logon
- Users
- Groups



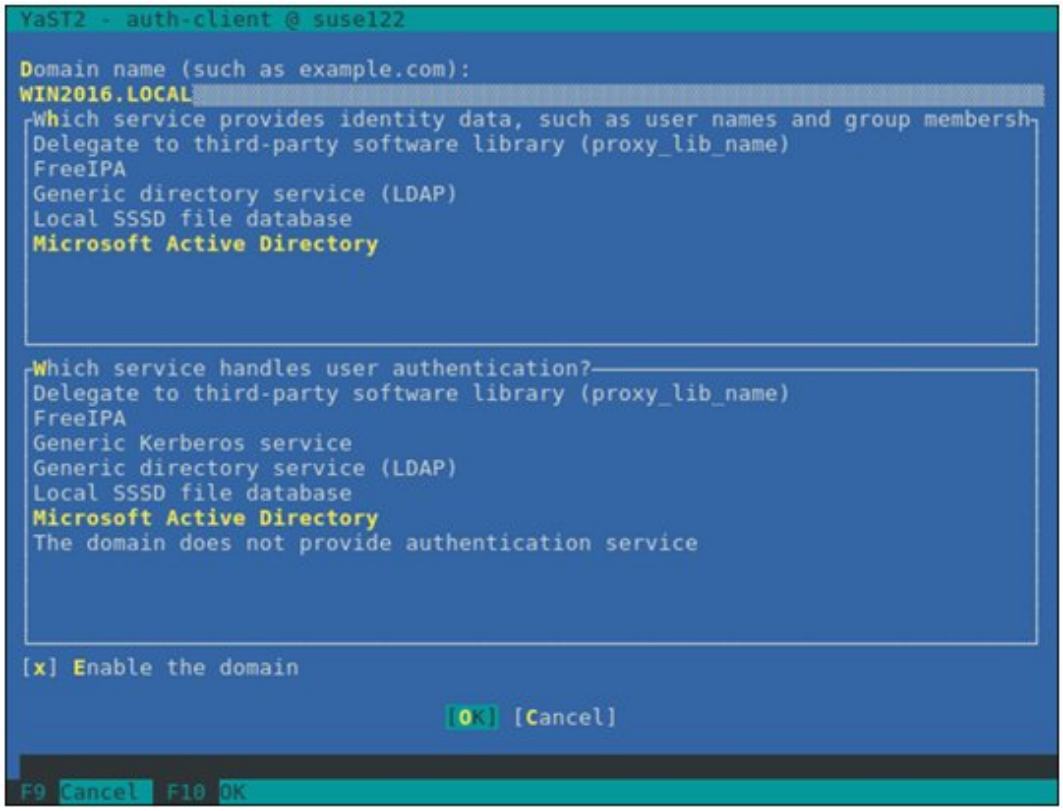
d. 以下の項目を設定してから[OK]を選択し、[Enter]キーを押します。

- Domain name
- Which service provides identity data, such as user names and group members

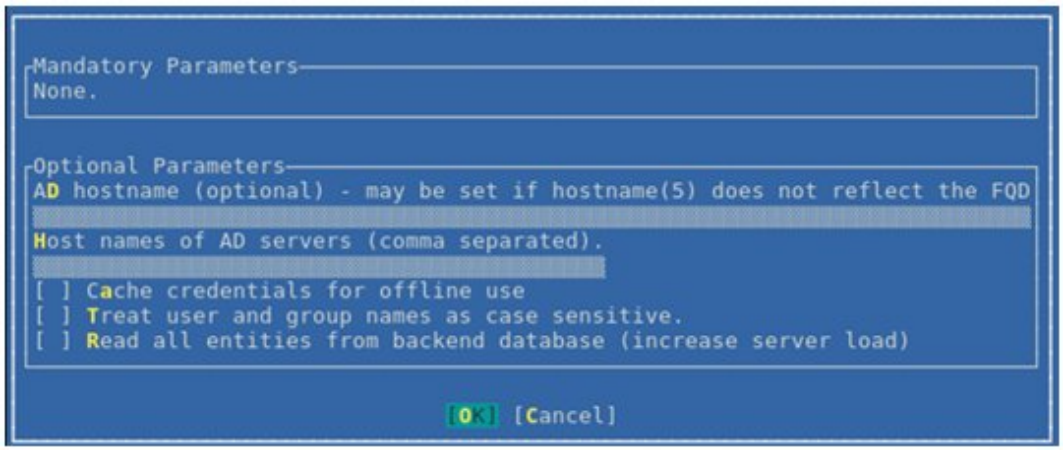
  Microsoft Active Directory
- Which service handles user authentication?

  Microsoft Active Directory

- Enable the domain



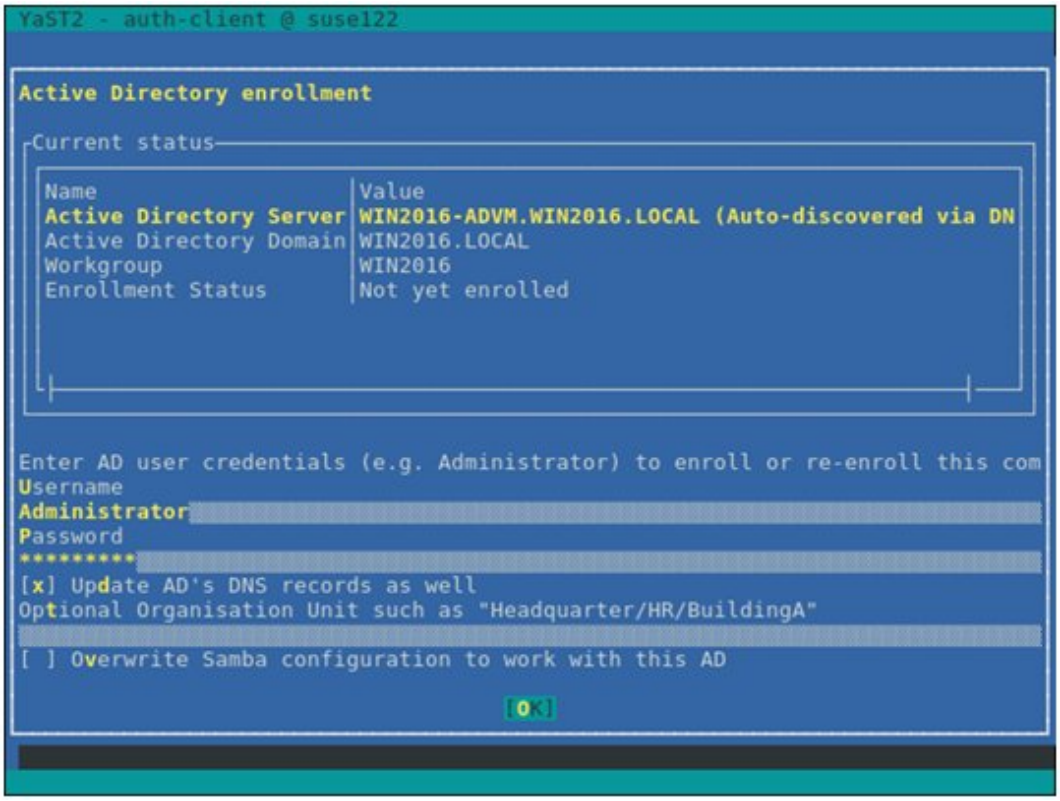
e. すべての項目を空白に設定、またはチェックを外し、[OK]を選択し、[Enter]キーを押します。



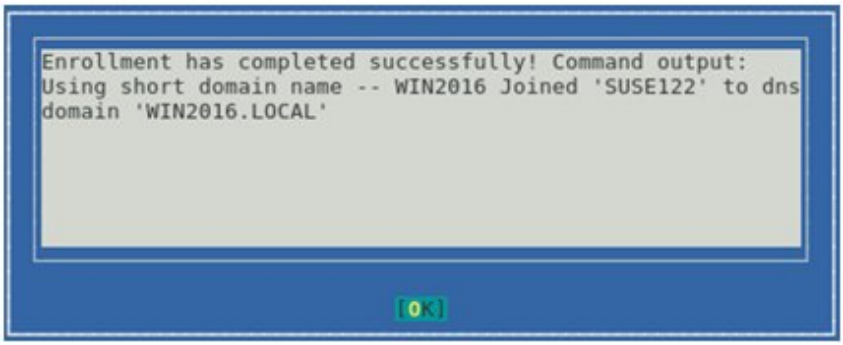
f. 以下の項目を設定してから[OK]を選択し、[Enter]キーを押します。

- Username
- Password

- Update AD's DNS records as well



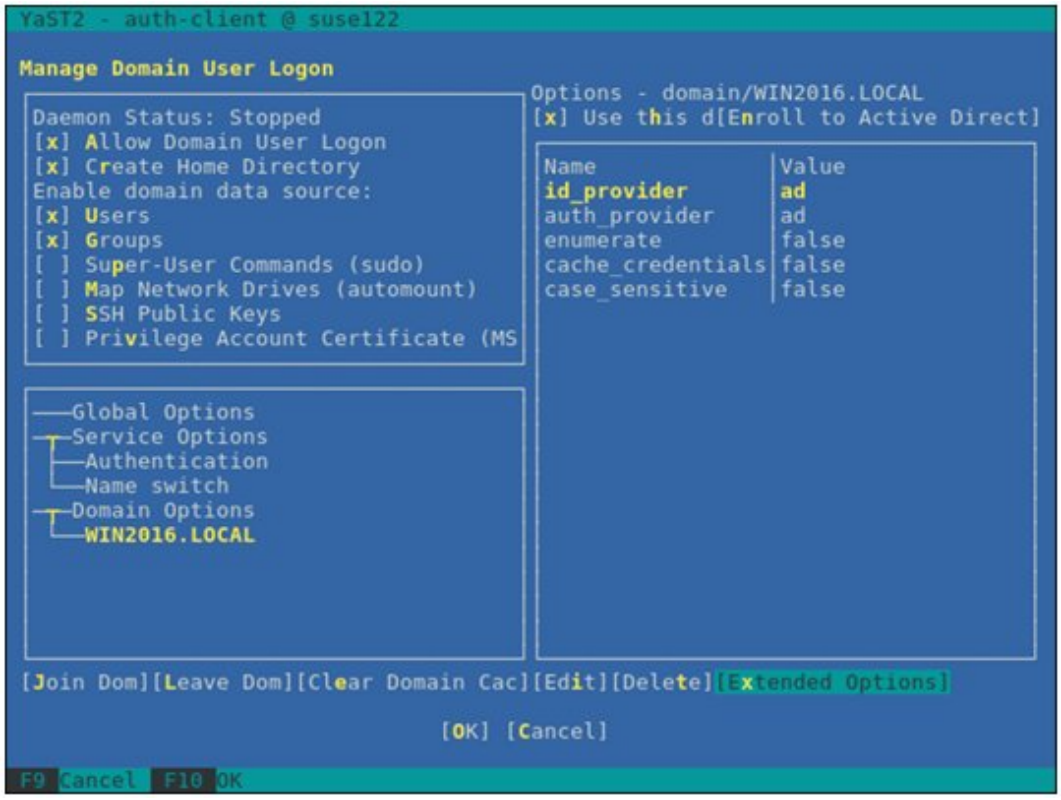
g. [OK]を選択し、[Enter]キーを押します。



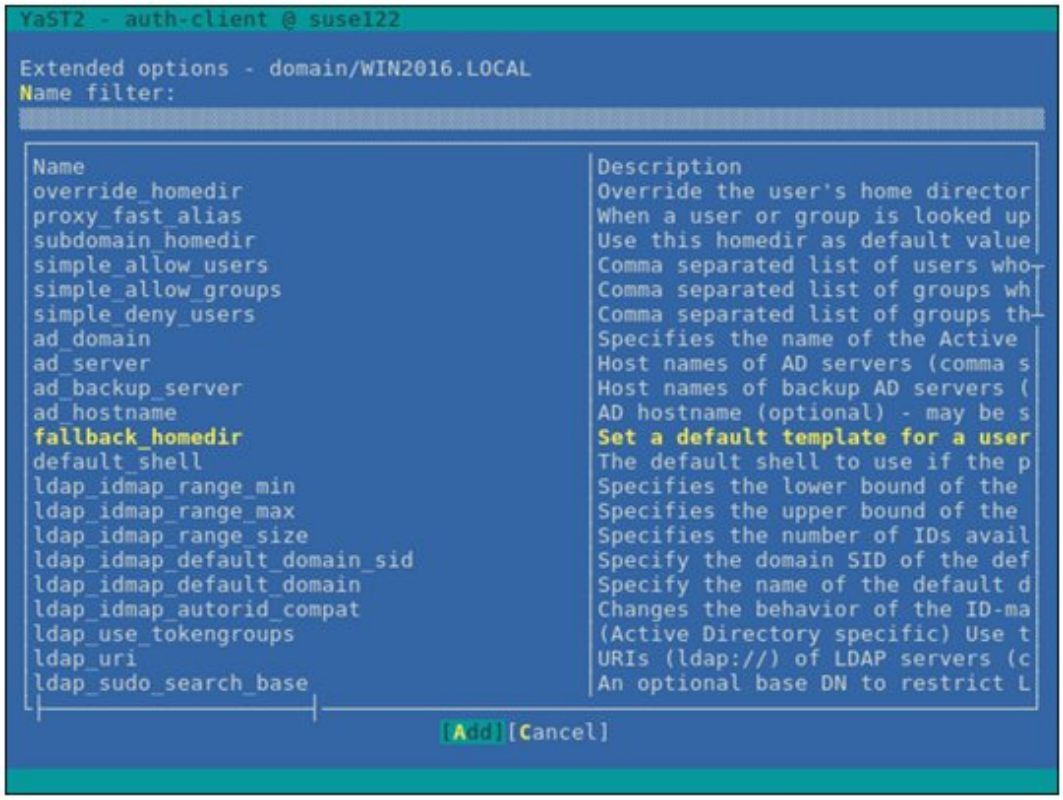
ドメインユーザーのホームディレクトリーを作成する場合は手順hに進みます。

ドメインユーザーのホームディレクトリーを作成しない場合は手順kへ進みます。

h. [Create Home Directory]を設定してから[Extended Options]を選択し、[Enter]キーを押します。

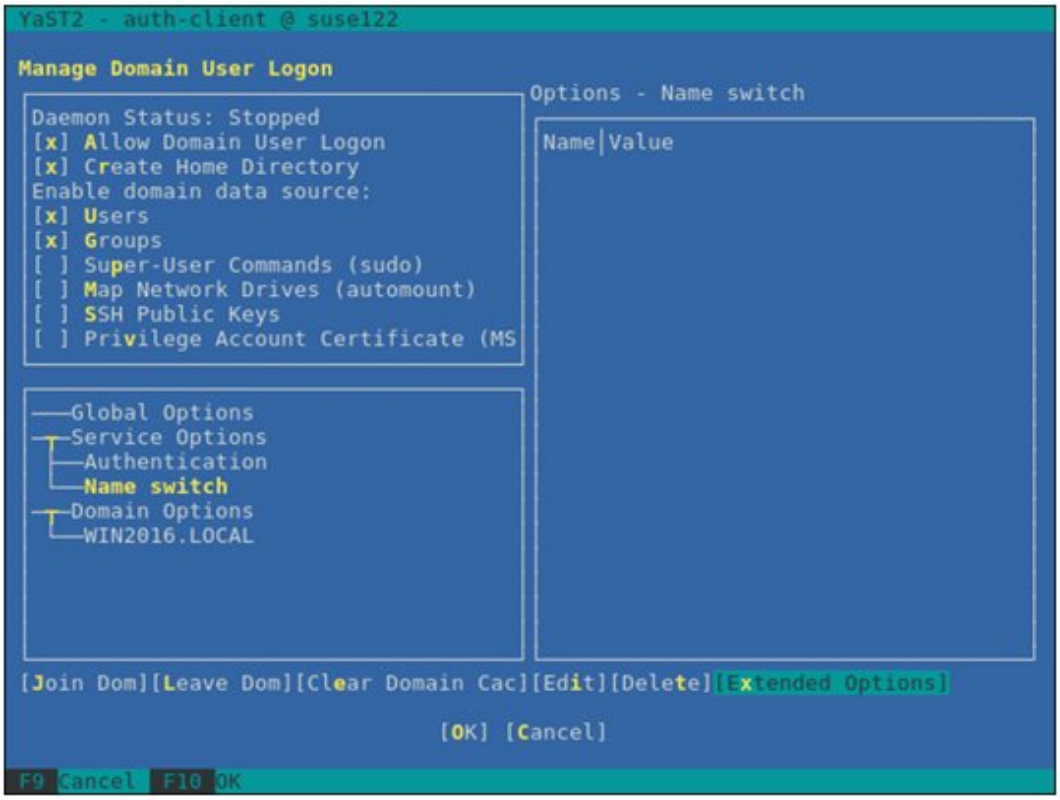


i. [fallback_homedir]を選択してから[Add]を選択し、[Enter]キーを押します。

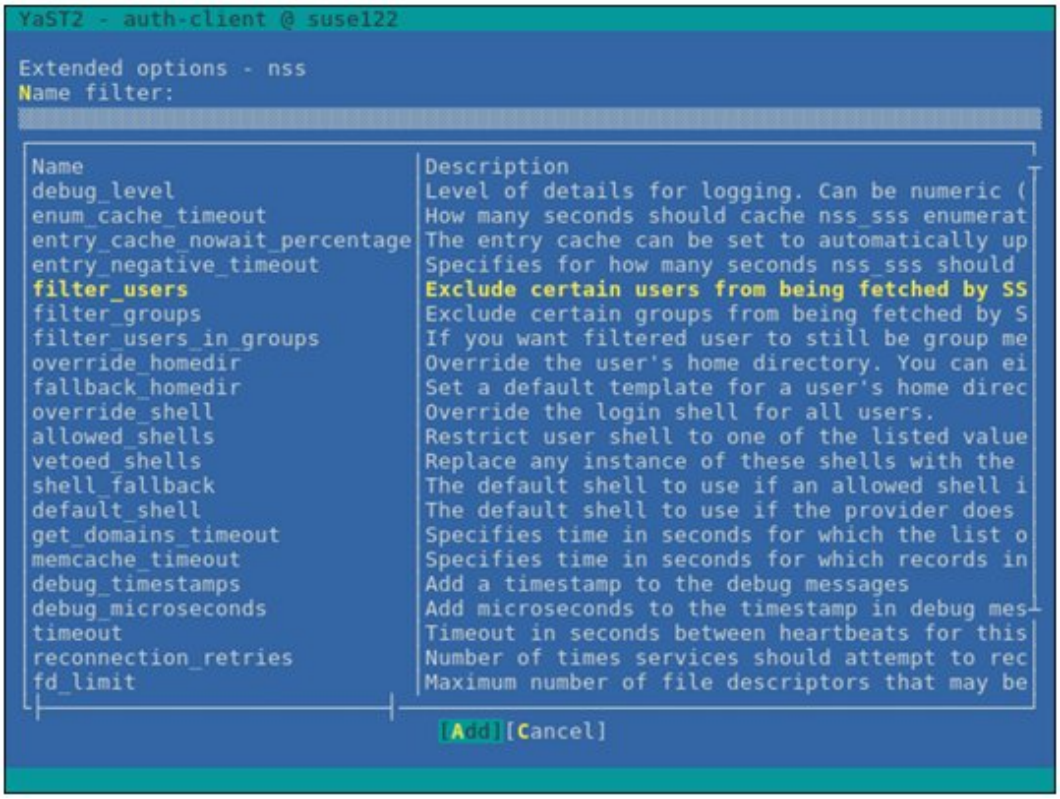


j. 「/home/%u」を入力してから[OK]を選択し、[Enter]キーを押します。

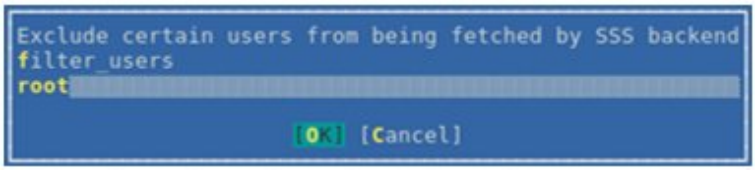
k. [Name switch]-[Extended Options]を選択し、[Enter]キーを押します。



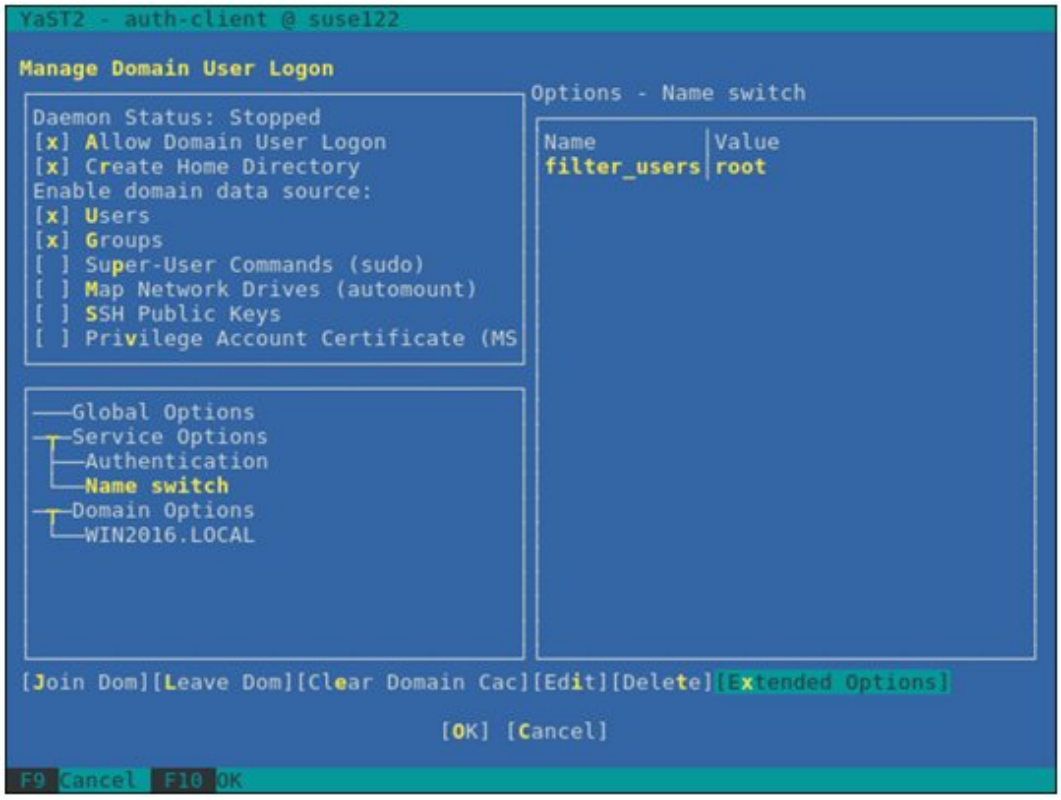
l. [filter_users]を選択してから[Add]を選択し、[Enter]キーを押します。



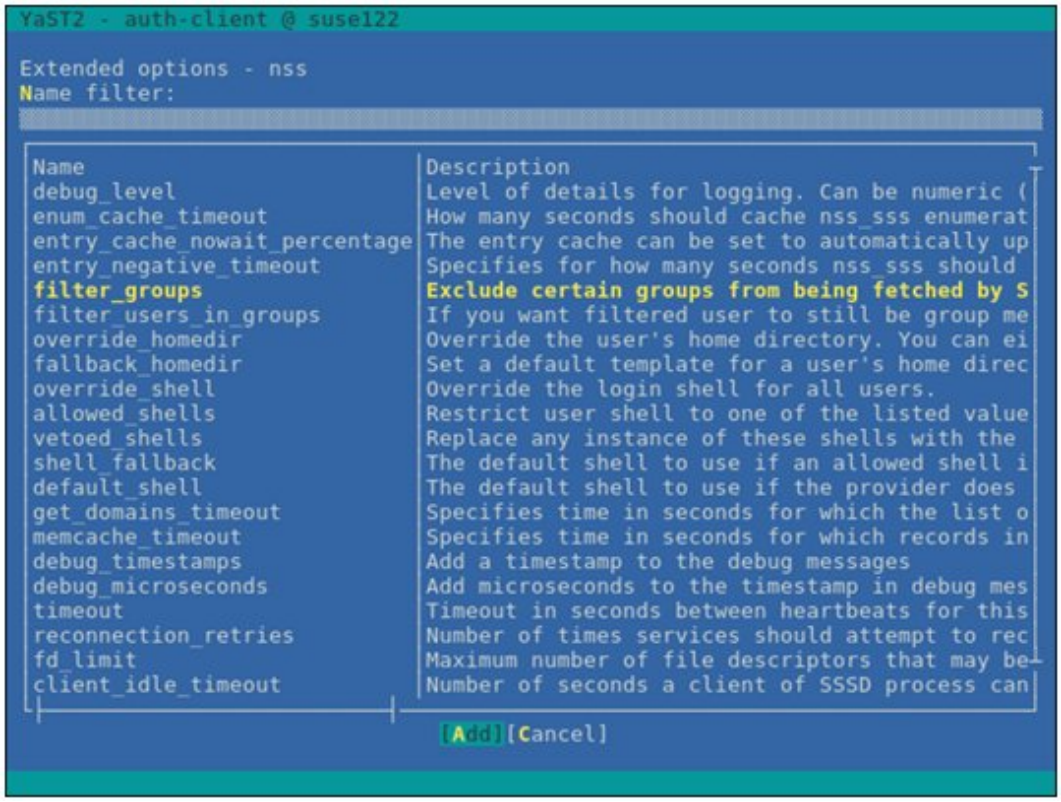
m. 「root」を入力してから[OK]を選択し、[Enter]キーを押します。



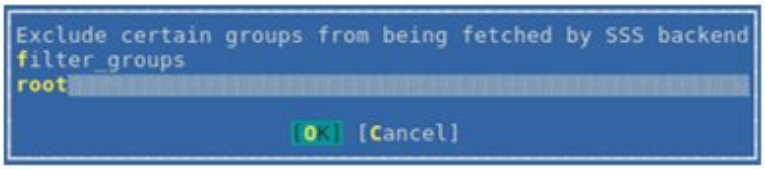
n. [Name switch]-[Extended Options]を選択し、[Enter]キーを押します。



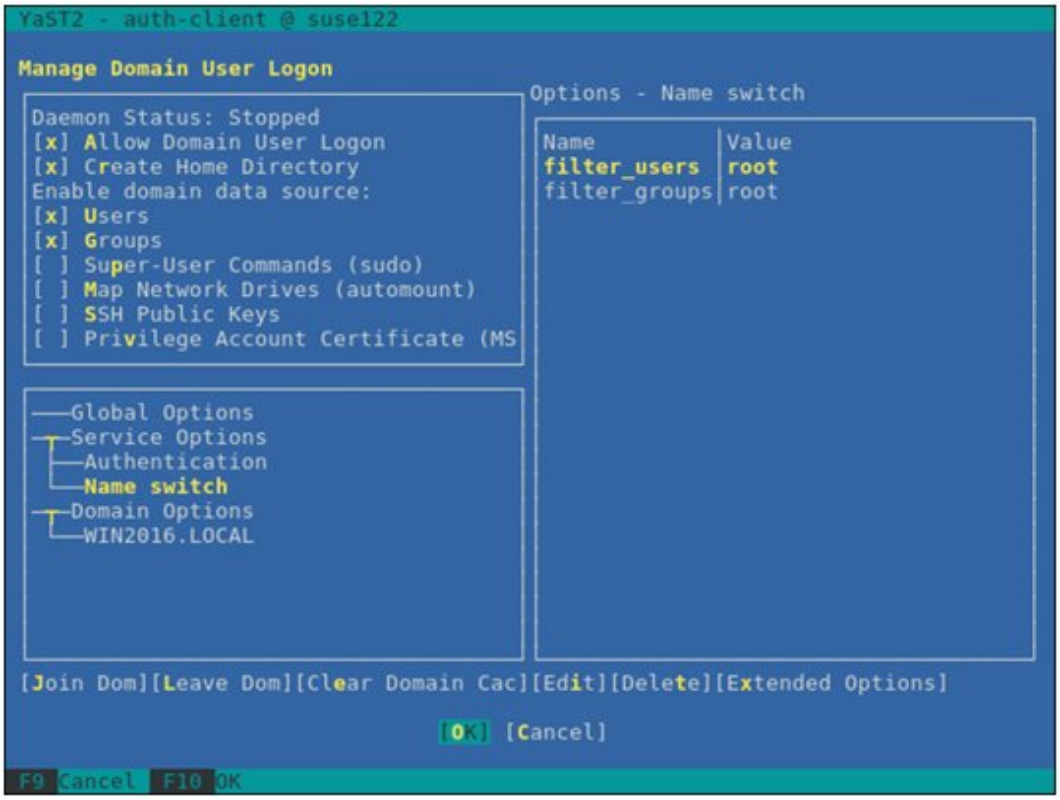
o. [filter_groups]を選択してから[Add]を選択し、[Enter]キーを押します。



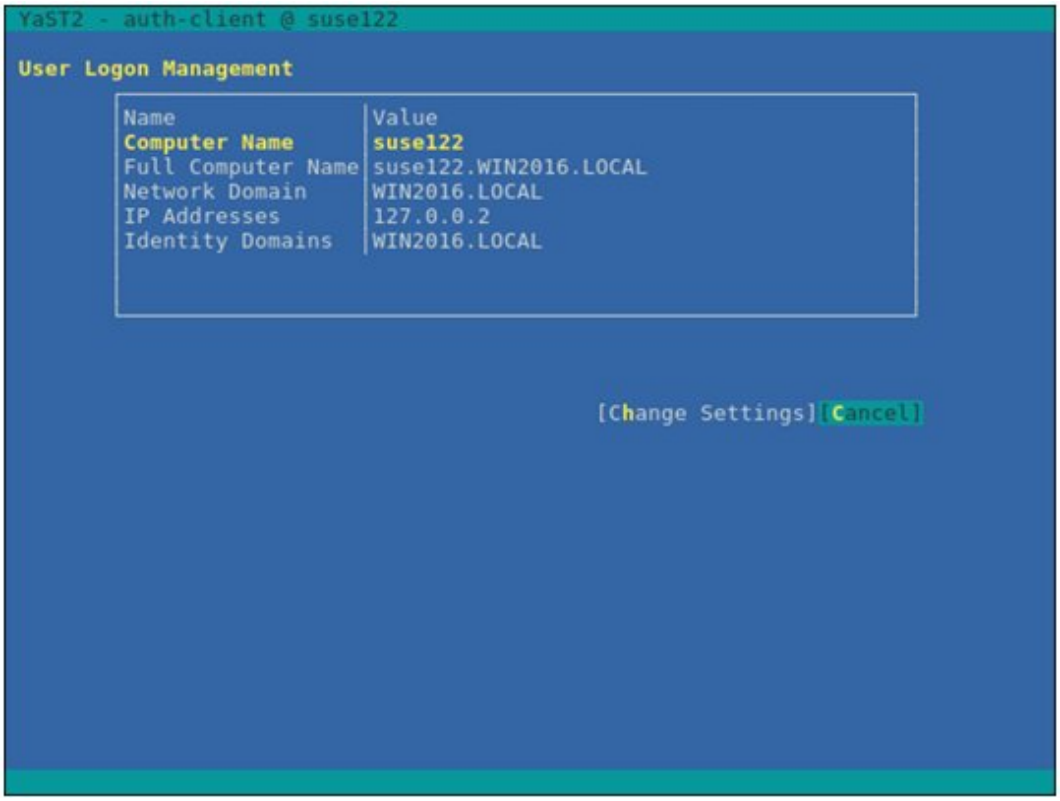
p. 「root」を入力してから[OK]を選択し、[Enter]キーを押します。



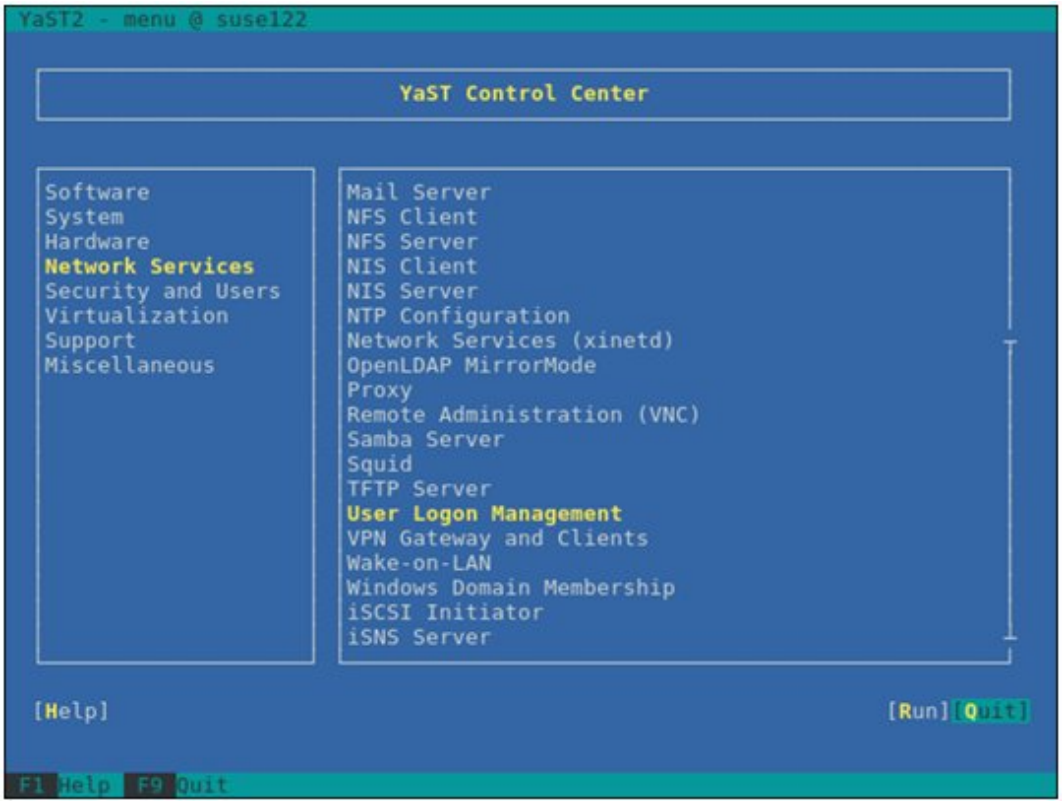
q. [OK]を選択し、[Enter]キーを押します。



r. [Cancel]を選択し、[Enter]キーを押します。



s. [Quit]を選択し、[Enter]キーを押します。



以上でSSDサービスの設定は終了です。

4. ドメインユーザーでのログイン確認

   以下のコマンドのどちらかを使用して、SSHプロトコルでのログイン確認ができます。ドメインユーザー名の表記方法については、下記のポイントを参照してください。

```
# ssh ＜ドメインユーザー名＞@＜監視対象サーバーIPアドレス＞
```

```
# ssh -l ＜ドメインユーザー名＞ ＜監視対象サーバーIPアドレス＞
```

   例:

```
# ssh administrator@192.168.30.222
```

```
# ssh 'administrator@win2016'@192.168.30.222
```

```
# ssh -l 'win2016.local¥administrator' 192.168.30.222
```

   どの方法でもログインできれば、正しく設定されています。

ポイント

ドメインユーザー名の表記方法

ドメインユーザー名の表記方法は、以下の表のようにいくつか書き方があります。なお、ドメインのオプションの設定でcase_sensitive falseとしているので、大文字・小文字は区別しません。

ドメインユーザー名の表記	表記例
ユーザー名	administrator
'ドメインプレフィックス¥ユーザー名'	'win2016¥administrator'
'ドメインプレフィックス.ドメイン名サフィックス¥ユーザー名'	'win2016.local¥administrator'
'ユーザー名@ドメインプレフィックス'	'administrator@win2016'
'ユーザー名@ドメインプレフィックス.ドメイン名サフィックス'	'administrator@win2016.local'

5. ドメインユーザーの設定

   「B.11.4 一般ユーザーアカウント使用時の設定」に従って、ドメインユーザーの設定を行ってください。

6. ISM-VAへドメイン情報の追加

   「3.4.2 ISM-VAの初期設定」を実施してください。

7. ISM-VAへDNS情報の追加

   「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

B.11.3 KVM AlmaLinuxへの設定手順(ドメインユーザー使用時)

KVM情報を取得するため、監視対象でSSSDサービスを設定する必要があります。「B.11.1 KVM Red Hat Enterprise Linuxへの設定手順(ドメインユーザー使用時)」を参照し、監視対象への設定を実施してください。

B.11.4 一般ユーザーアカウント使用時の設定

KVM情報は基本的にはrootユーザーのみで取得できます。

rootユーザー以外のユーザー(ドメインユーザーも含みます)でKVM情報を取得する場合は、監視対象Linuxサーバー上で対象ユーザーをグループlibvirtに追加する必要があります。

rootユーザーで以下を実行してください。

```
# gpasswd -a ＜ユーザー名＞ libvirt
```

ポイント

ユーザーをグループlibvirtから削除する場合は、rootユーザーで以下を実行してください。

```
# gpasswd -d <ユーザー名> libvirt
```

注意

- ユーザー名は、すべて小文字で設定してください。
- ドメインユーザーも上記コマンドでグループ追加／削除が可能です。

B.12 監視対象への設定手順（仮想化管理ソフトウェア：OpenStack）

ISMは、OpenStackに対して通信します。必要な設定は、以下のとおりです。

B.12.1 コントローラーノードへの設定手順

1. SSLモジュールのインストール

   コントローラーノードにすでにインストールされている場合は必要ありません。

   以下はyumコマンドを使用してインストールする場合の例です。

   ```
   # yum install mod_ssl
   ```

2. SSL証明書の用意

   a. HTTPS通信用のSSL証明書ファイルおよびSSL証明書キーファイルを用意します。

   SSL証明書の用意には、以下の3つの手段があります。

   - SSL証明書ファイルとSSL証明書キーファイルがすでにインストールされている場合、そのファイルを流用する
   - 認証局から発行する
   - 自己署名証明書を作成する

   ポイント

   自己署名証明書の作成方法例

   ```
   # openssl genrsa -rand /proc/uptime 2048 > server.key
   # openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM -extensions v3_req -out
   server.crt
   ```

   Common Nameには、IPアドレス、FQDNまたはホスト名を入力してください。

   注意

   - SSL証明書のバージョンはX.509 v3のみ使用可能です。以下のコマンドでVersion情報を調べることが可能です。

     ```
     # openssl x509 -text -noout -in certificate_file_path
     ```

     certificate_file_pathには、証明書ファイルのフルパスを入力してください。

   - OpenStackインストール時に自動でファイルが作成されることがありますが、X.509 v3以外で作成されている場合があります。必ずX.509 v3で作成した証明書を使用してください。

b. 用意したSSL証明書をコントローラーノードに格納します。

- SSL証明書ファイル:/etc/pki/CA/certs/
- SSL証明書キーファイル:/etc/pki/CA/private/

3. 割当てポートの決定

Proxyサーバーに割り当てるポートを決定します。

コントローラーノードでほかのサービスで使用されていないポートを選んでください。

1～1023は使用できません。

4. OpenStack環境変数設定ファイルの用意

以下の手順でダウンロードします(以下の手順は、お使いのバージョン／プラットフォームにより異なる場合があります)。

a. OpenStack Dashboardにadminユーザーでログインします。

b. 右上の[admin]アイコンを選択します。

c. 「OpenStack RC File v3」を選択し、ダウンロードします。

また、OpenStackインストール時に作成されているファイルを使用することもできます。

5. OpenStack endpoint情報の取得

以下の4種類のURL情報および2種類のバージョン情報を取得します。バージョン情報はURLの最後のvxの部分を取得してください。
また、URLは/vxの部分までを取得してください。

- Service Typeがidentity、Interfaceがpublicとなっている項目のURL、バージョン
- Service Typeがnetwork、Interfaceがpublicとなっている項目のURL
- Service Typeがimage、Interfaceがpublicとなっている項目のURL
- Service Typeがcompute、Interfaceがpublicとなっている項目のURL、バージョン

以下のコマンドをコントローラーノード上で実行します。

```
source ＜OpenStack環境変数設定ファイル＞; unset OS_SERVICE_TOKEN;  export OS_PASSWORD=＜OpenStack_PASSWORD＞;
openstack endpoint list
```

例:

```
source keystonerc_admin; unset OS_SERVICE_TOKEN;  export OS_PASSWORD=password; openstack endpoint list
```

出力結果例:

```
+----------------------------------+-----------+--------------+--------------+---------+-----------
+-----------------------------------------------+
| ID                               | Region    | Service Name | Service Type | Enabled | Interface |
URL                                            |
+----------------------------------+-----------+--------------+--------------+---------+-----------
+-----------------------------------------------+
| 01d7dd66d19947d5870acec413876ba2 | RegionOne | keystone     | identity     | True    | public    | http://
192.168.30.86:5000/v3                          |
| 04005c8d71a544e596b9e40083fa7206 | RegionOne | placement    | placement    | True    | internal  | http://
192.168.30.86:8778/placement                   |
| 0797675ff3c64da58a57a4988ec44a2b | RegionOne | cinderv2     | volumev2     | True    | admin     | http://
192.168.30.86:8776/v2/%(tenant_id)s            |
| 09ae73e20c004030ae04a7f5d8bf048a | RegionOne | placement    | placement    | True    | admin     | http://
192.168.30.86:8778/placement                   |
| 12d9cbc0b1de4bf5a63d6819ec274685 | RegionOne | swift        | object-store | True    | internal  | http://
192.168.30.86:8080/v1/AUTH_%(tenant_id)s       |
| 201c7c5ecef54c0691c043eafe6087ae | RegionOne | neutron      | network      | True    | admin     | http://
192.168.30.86:9696                            |
| 32920d76f674494d9a9dd98e06c9e229 | RegionOne | gnocchi      | metric       | True    | internal  | http://
192.168.30.86:8041                            |
```

```
| 3ff445febbee434aafc70c964dc3dbdc | RegionOne | ceilometer   | metering     | True    | internal  | http://
192.168.30.86:8777                |
| 42f8a5c483ef43f18e736b622c2d5cf8 | RegionOne | cinderv2     | volumev2     | True    | internal  | http://
192.168.30.86:8776/v2/%(tenant_id)s      |
| 4aba919df7f947bbaf7a19918fadd01e | RegionOne | swift        | object-store | True    | admin     | http://
192.168.30.86:8080/v1/AUTH_%(tenant_id)s |
| 4b8c976fe4e742018b0fd4177dcae429 | RegionOne | cinderv3     | volumev3     | True    | admin     | http://
192.168.30.86:8776/v3/%(tenant_id)s      |
| 5b61335921c247689906b1bf390a45e7 | RegionOne | cinderv2     | volumev2     | True    | public    | http://
192.168.30.86:8776/v2/%(tenant_id)s      |
| 676ec9c2044947fea66b15f6168465de | RegionOne | gnocchi      | metric       | True    | admin     | http://
192.168.30.86:8041                |
| 6855184db088496baabb85f5a70021f4 | RegionOne | aodh         | alarming     | True    | internal  | http://
192.168.30.86:8042                |
| 8944c76fb0784089b1f7f56c94388530 | RegionOne | nova         | compute      | True    | public    | http://
192.168.30.86:8774/v2.1/%(tenant_id)s    |
| 930030ede13049439e2933665e91a3b4 | RegionOne | cinderv3     | volumev3     | True    | public    | http://
192.168.30.86:8776/v3/%(tenant_id)s      |
| 9503ad1f5e754993838fa53fd5d58690 | RegionOne | nova         | compute      | True    | admin     | http://
192.168.30.86:8774/v2.1/%(tenant_id)s    |
| 9541b01381404c4cb200dcbeea0168c4 | RegionOne | keystone     | identity     | True    | admin     | http://
192.168.30.86:35357/v3            |
| 98f00b9d75564ba29e92ccd5fdccb376 | RegionOne | keystone     | identity     | True    | internal  | http://
192.168.30.86:5000/v3             |
| 9ae897c5ae704d9aa142b7b61c728468 | RegionOne | aodh         | alarming     | True    | admin     | http://
192.168.30.86:8042                |
| 9bdc57b0a32e40148e2a049ba9211e8b | RegionOne | placement    | placement    | True    | public    | http://
192.168.30.86:8778/placement      |
| b0ea3c01f909451bafb57ccc2e5a6e32 | RegionOne | glance       | image        | True    | admin     | http://
192.168.30.86:9292                |
| b75f5ae0fc8644fc9859ef37d4a4afc5 | RegionOne | ceilometer   | metering     | True    | public    | http://
192.168.30.86:8777                |
| b7de11ad749b4d0f9b593446794c355c | RegionOne | swift        | object-store | True    | public    | http://
192.168.30.86:8080/v1/AUTH_%(tenant_id)s |
| b82ce3bd754a46289838cdc4ec17fd0f | RegionOne | cinder       | volume       | True    | public    | http://
192.168.30.86:8776/v1/%(tenant_id)s      |
| be3d757e64a945f8b0cdf784f0167ff8 | RegionOne | neutron      | network      | True    | internal  | http://
192.168.30.86:9696                |
| c70161c0b104474f8f1d15fee74b222f | RegionOne | gnocchi      | metric       | True    | public    | http://
192.168.30.86:8041                |
| c89faf6e8b9d4b3f9823d1a7e490e45b | RegionOne | cinder       | volume       | True    | internal  | http://
192.168.30.86:8776/v1/%(tenant_id)s      |
| cbd56dff0a5d4fe4b1a705e820115fd6 | RegionOne | ceilometer   | metering     | True    | admin     | http://
192.168.30.86:8777                |
| dab0b8fa23c943a787803e0fd5e00450 | RegionOne | nova         | compute      | True    | internal  | http://
192.168.30.86:8774/v2.1/%(tenant_id)s    |
| dbaf3b9d826d49ec8955623bf57cd7ec | RegionOne | neutron      | network      | True    | public    | http://
192.168.30.86:9696                |
| e2fff591156f4176a13aad68c7e0e000 | RegionOne | glance       | image        | True    | internal  | http://
192.168.30.86:9292                |
| ecda799534b144e7a48dbe8c4e99836a | RegionOne | cinderv3     | volumev3     | True    | internal  | http://
192.168.30.86:8776/v3/%(tenant_id)s      |
| f9052dd300904e8c80fca87fdb8bc2a1 | RegionOne | glance       | image        | True    | public    | http://
192.168.30.86:9292                |
| fa9b861b2e14423baba72aa08bf2953d | RegionOne | aodh         | alarming     | True    | public    | http://
192.168.30.86:8042                |
| fd768ee6e3844bd982e27b6cd3501c5b | RegionOne | cinder       | volume       | True    | admin     | http://
192.168.30.86:8776/v1/%(tenant_id)s      |
+----------------------------------+-----------+--------------+--------------+---------+-----------
+-------------------------------------------+
```

取得例:

Service Type	URL	バージョン
identity	http://192.168.30.86:5000/v3	v3
network	http://192.168.30.86:9696	-
image	http://192.168.30.86:9292	-
compute	http://192.168.30.86:8774/v2.1	v2.1

6. バージョン情報付きのOpenStack endpoint情報の取得

networkとimageについて、curlコマンドでバージョン情報付きURLおよびURLのバージョンを取得します。

バージョン情報はURLの最後のvxの部分を取得してください。

結果が複数件ある場合、statusがCURRENTのhrefキーを使用してください。

ー networkの場合

以下のコマンドを実行してください。

```
# curl -k ＜networkのurl＞
```

例:

```
# curl -k "http://192.168.30.86:9696"
```

出力結果例:

```
{"versions": [{"status": "CURRENT", "id": "v2.0", "links": [{"href": "http://192.168.30.86:9696/v2.0/", "rel":
"self"}]}]}
```

取得例:

Service Type	URL	バージョン
network	http://192.168.30.86:9696/v2.0	v2.0

ー imageの場合

以下のコマンドを実行してください。

```
# curl -k ＜imageのurl＞
```

例:

```
# curl -k "http://192.168.30.86:9292"
```

出力結果例:

```
{"versions": [{"status": "CURRENT", "id": "v2.5", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "SUPPORTED", "id": "v2.4", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "SUPPORTED", "id": "v2.3", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "SUPPORTED", "id": "v2.2", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "SUPPORTED", "id": "v2.1", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "SUPPORTED", "id": "v2.0", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel":
"self"}]}, {"status": "DEPRECATED", "id": "v1.1", "links": [{"href": "http://192.168.30.86:9292/v1/", "rel":
"self"}]}, {"status": "DEPRECATED", "id": "v1.0", "links": [{"href": "http://192.168.30.86:9292/v1/", "rel":
"self"}]}]}
```

取得例:

Service Type	URL	バージョン
image	http://192.168.30.86: 9292/v2	v2

7. Apache SSL設定の変更

a. 下記例を参考に任意の名称で設定ファイルを作成します。

ただし、拡張子は「.conf」である必要があります。

```
Listen ＜手順3で決定したポート番号＞
<VirtualHost *:＜手順3で決定したポート番号＞>
    ServerName ＜コントローラーノードのIPアドレス、FQDNまたはホスト名＞
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile    ＜SSL証明書ファイルのフルパス＞
    SSLCertificateKeyFile ＜SSL証明書キーファイルのフルパス＞
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass  ＜手順5で取得したidentityのURL＞
        Header set x-openstack-api-version ＜手順5で取得したidentityのバージョン＞
    </Location>
    <Location /network>
        ProxyPass  ＜手順5で取得したnetworkのURL＞
        Header set x-openstack-api-version ＜手順6で取得したnetworkのバージョン＞
    </Location>
    <Location /compute>
        ProxyPass  ＜手順5で取得したcomputeのURL＞
        Header set x-openstack-api-version ＜手順5で取得したcomputeのバージョン＞
    </Location>
    <Location /image>
        ProxyPass  ＜手順5で取得したimageのURL＞
        Header set x-openstack-api-version ＜手順6で取得したimageのバージョン＞
    </Location>
</Virtualhost>
```

例:

```
Listen 5001
<VirtualHost *:5001>
    ServerName 192.168.30.86
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile    /etc/pki/CA/certs/server.crt
    SSLCertificateKeyFile /etc/pki/CA/private/server.key
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass  http://localhost:5000/v3
        Header set x-openstack-api-version v3
    </Location>
    <Location /network>
        ProxyPass  http://localhost:9696/v2.0
        Header set x-openstack-api-version v2.0
    </Location>
    <Location /compute>
        ProxyPass  http://localhost:8774/v2.1
        Header set x-openstack-api-version v2.1
    </Location>
```

```
    <Location /image>
        ProxyPass  http://localhost:9292/v2
        Header set x-openstack-api-version v2
    </Location>
</Virtualhost>
```

b. Apache SSL設定ファイルを格納します。

以下に格納してください。

```
/etc/httpd/conf.d/
```

c. Apache設定を再読み込みします。

ターミナルで以下のコマンドをrootユーザーで実行してください。

```
systemctl reload httpd
```

8. ファイアウォールの設定

以下のコマンドを使用して設定したポートを許可してください。

― ポート許可状況確認コマンド

```
iptables -nL --line-numbers
```

― ポート開放コマンド

```
iptables -I INPUT 1 -p tcp --dport ＜port＞ -s ＜ISMのIPアドレス＞ -j ACCEPT
```

ポート開放コマンド例:

```
iptables -I INPUT 1 -p tcp --dport 5001 -s 192.168.0.101 -j ACCEPT
```

― 設定保存コマンド

```
/sbin/service iptables save
```

― ポート閉鎖コマンド

```
iptables -D INPUT ＜No＞
```

ポート閉鎖コマンド例:

```
iptables -D INPUT 1
```

B.12.2 仮想ネットワーク分析機能使用時の設定

1.「/etc/nova/nova.conf」の編集

a. /etc/nova/nova.confファイルを開きます。

```
# vi /etc/nova/nova.conf
```

b. 以下の2項目をそれぞれ1行で追加します。

キー	値
scheduler_available_filters	任意
scheduler_default_filters	SameHostFilter

例:

```
scheduler_available_filters = nova.scheduler.filters.all_filters
scheduler_default_filters =
```

```
SameHostFilter,RetryFilter,AvailabilityZoneFilter,RamFilter,DiskFilter,ComputeFilter,ComputeCapabilitiesFilter,ImagePropertiesFilter,ServerGroupAntiAffinityFilter,ServerGroupAffinityFilter
```

2. novaサービスの再起動

   コントローラーノードで以下のコマンドを実行します。

   コマンドはすべて1行で記述してください。

```
for service in api consoleauth conductor scheduler novncproxy; do  systemctl restart openstack-nova-$service; done
```

B.13 監視対象への設定手順(仮想化管理ソフトウェア:IPCOM)

ISMは、IPCOMに対して通信します。必要な設定は、以下のとおりです。

B.13.1 仮想マシン情報取得コマンド実行権限設定手順

adminユーザーでIPCOMの仮想情報を取得する場合は、監視対象IPCOMサーバー上でadminユーザーをグループlibvirtに追加し、仮想マシン情報取得コマンド実行権限を与える必要があります。

adminユーザーで以下を実行してください。

```
# sudo gpasswd -a admin libvirt
```

ポイント

adminユーザーをグループlibvirtから削除する場合は、adminユーザーで以下を実行してください。

```
# sudo gpasswd -d admin libvirt
```

B.14 監視対象への設定手順(仮想化管理ソフトウェア:Microsoft Failover Cluster (Azure Stack HCI))

ISMは、Microsoft Failover Cluster (Azure Stack HCI)に対して通信します。必要な設定は、以下のとおりです。

B.14.1 ドメインユーザーアカウント使用時の設定

1. クラスタを構成する各ホストへのWinRM設定

   Microsoft Failover Cluster(Azure Stack HCI)から情報を取得するためには、クラスタを構成する各ホストへの設定が完了している必要があります。「B.7 監視対象への設定手順(OS:Azure Stack HCI)」を参照し、各ホストへの設定を実施してください。

2. Active Directoryへの SPNの追加

   ドメインユーザーアカウントを使用しAzure Stack HCIの監視をする際には、監視対象クラスタのサービスプリンシパル名(SPN)を正しくActive Directoryに登録する必要があります。以下の手順を実行し、監視対象クラスタのサービスプリンシパル名を登録してください。

```
> setspn -S HTTP/<監視対象クラスタIP> <監視対象クラスタ名>
```

ポイント

確認方法

```
> setspn -L <監視対象クラスタ名>
```

コマンド実行結果に以下が出力されていれば、正しく登録されています。

```
HTTP/<監視対象クラスタIP>
```

3. ISM-VAへドメイン情報の追加

   ドメインユーザーアカウントでの監視を行う際には、「3.4.2 ISM-VAの初期設定」を実施してください。

4. ISM-VAへDNS情報の追加

   ドメインユーザーアカウントでの監視を行う際には、「4.9 ネットワーク設定」の「DNSサーバー追加」を行い、ISM-VAにDNSサーバーを登録してください。

5. Active Directoryへ Kerberos委任の構成

   a. Active Directory サーバーにログオンします。

   b. サーバーマネージャーを開きます。

   c. [ツール]ボタンから[Active Directoryユーザーとコンピューター]を選択します。

   d. ドメインを展開し、[コンピューター]フォルダーを展開します。

   e. 右側ウィンドウで、クラスタノード名またはクラスタ名を右クリックし、[プロパティ]を選択します。

   f. [委任]タブで、[任意のサービスへ委任でこのコンピューターを信頼する]にチェックを付けます。

   g. [OK]を選択し、すべてのクラスタノードおよびクラスタに対して手順e～fを実施します。

付録C　ISM-VAのアンインストール

ISM-VAのインストール先に応じてアンインストールします。

以下に各アンインストール手順を説明します。

- Microsoft Windows Server Hyper-Vからのアンインストール
- VMware vSphere Hypervisor 6.5以降からのアンインストール
- KVMからのアンインストール
- Nutanix AHVからのアンインストール

Microsoft Windows Server Hyper-Vからのアンインストール

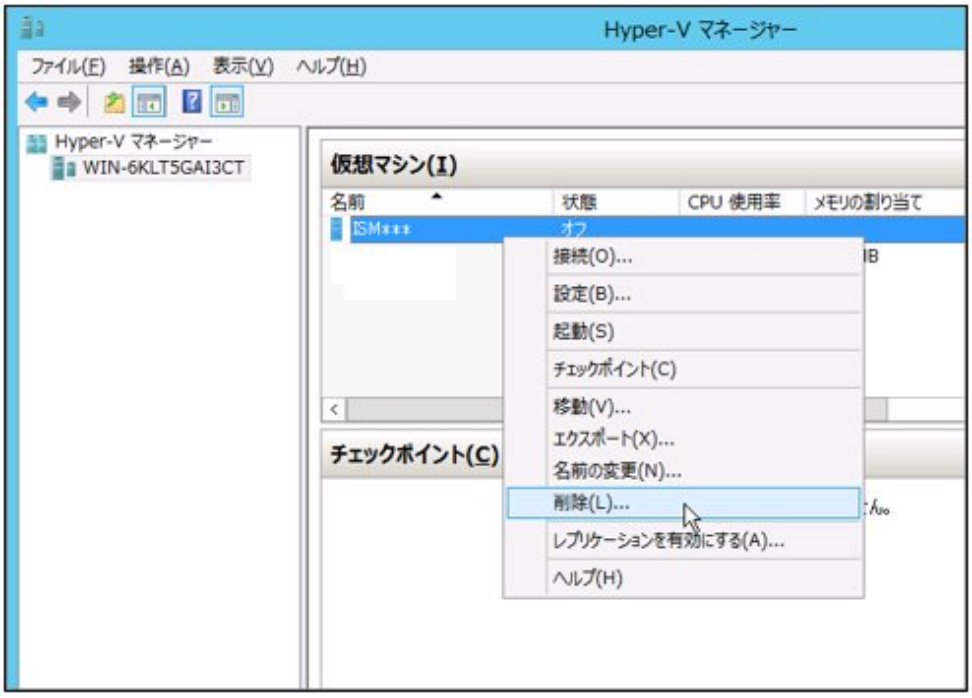
1. ISM-VAを停止します。

   詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. Hyper-Vマネージャーを起動し、インストールしたISM-VAを右クリックして[設定]を選択します。

   ISM-VAに割り当てられている仮想ハードディスクの格納場所とファイル名が表示されるので、メモしてください。

3. Hyper-Vマネージャー上で、インストールしたISM-VAを右クリックして[削除]を選択します。



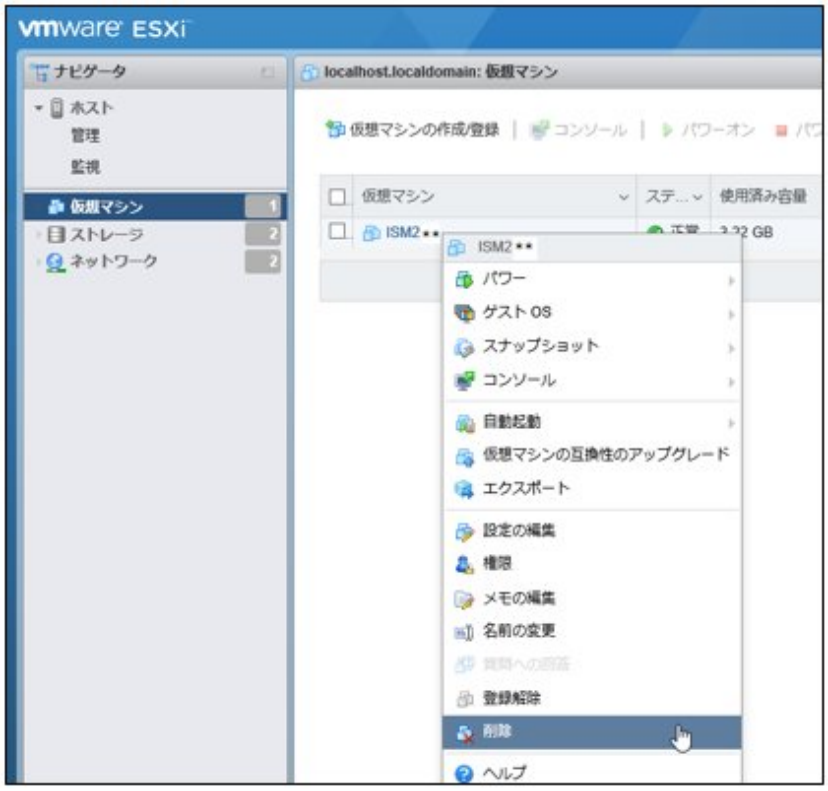
4. 手順2で記録した仮想ハードディスクを、エクスプローラーで削除します。

VMware vSphere Hypervisor 6.5以降からのアンインストール

1. ISM-VAを停止します。

   詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. vSphere Client（HTML5）を起動し、インストールしたISM-VAを右クリックして[削除]を選択します。



KVMからのアンインストール

1. ISM-VAを停止します。

   詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

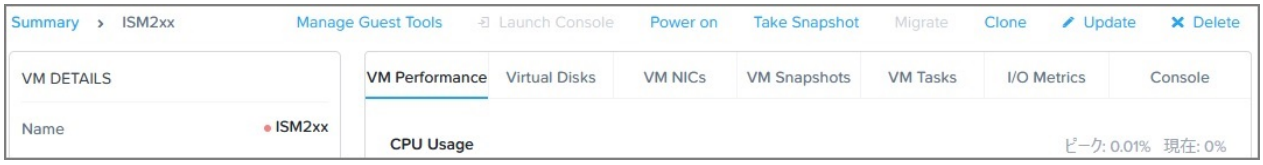
2. 仮想マシンマネージャーを起動し、インストールしたISM-VAを右クリックして[削除]を選択します。

Nutanix AHVからのアンインストール

1. ISM-VAを停止します。

   詳しくは、「4.1.2 ISM-VAの終了」を参照してください。

2. NutanixのPRISMで、[仮想マシン]画面の[テーブル]表示を選択します。



3. ISM-VAの仮想マシンを選択し、[Delete]を選択して削除します。
4. NutanixのPRISMで、[設定]メニュー - [イメージ設定]を選択します。表示された画面でISM-VAのイメージを削除します。

付録D　PRIMEFLEX HS／PRIMEFLEX for VMware vSANのクラスタ作成およびクラスタ拡張の要件

ハイパーコンバージドインフラストラクチャー（HCI）製品であるPRIMEFLEXは、購入時のサーバーと同世代のサーバーに加え、後継機種となるサーバーを追加可能です。

D.1　追加可能なサーバー

購入時のサーバー機種に対して、追加可能なサーバーの機種については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/

D.2　ADVM構成へのクラスタ作成およびクラスタ拡張

PRIMEFLEX HS、およびPRIMEFLEX for VMware vSANのADVMが稼働する構成において、追加したサーバーをADVMで管理する場合は、下記のKBを参照し、ADVMの機能レベルをサポートしているバージョンのESXi／vCSAを適用する必要があります。

なお、PRIMEFLEX HS 1.0のADVMの機能レベルは、「Windows Server 2012R」です。PRIMEFLEX HS 1.1、およびPRIMEFLEX for VMware vSANのADVMの機能レベルは、「Windows Server 2016」です。

- vCenter Server

  https://kb.vmware.com/s/article/2071592

- ESXi

  https://kb.vmware.com/s/article/2113023

また、将来的にESXi／vCSAのActive Directoryによるユーザー管理が非サポートとなる可能性があります。

Active Directoryによる管理をサポートしないバージョンのESXi／vCSAを使用し、クラスタ拡張を行う場合は、Active Directoryによるユーザー管理からローカルアカウント管理に変更が必要です。

D.3　ネットワーク構成

サーバーを追加するにあたり、管理LAN／vMotion LAN／vSAN LANの物理／論理ネットワーク構成は、購入時のサーバーに合わせてください。

既存サーバーとクラスタ拡張時に追加するサーバーのネットワークインターフェイス（10GBase／10GBase-T、25GBase／25GBase-T）は同一ポートを選択してください。

既存サーバーとクラスタ拡張時に追加するサーバーの物理ネットワーク構成は、以下となります。管理LAN／vMotion LAN／vSAN LANで使用しない、追加搭載されたLANカードは除きます。

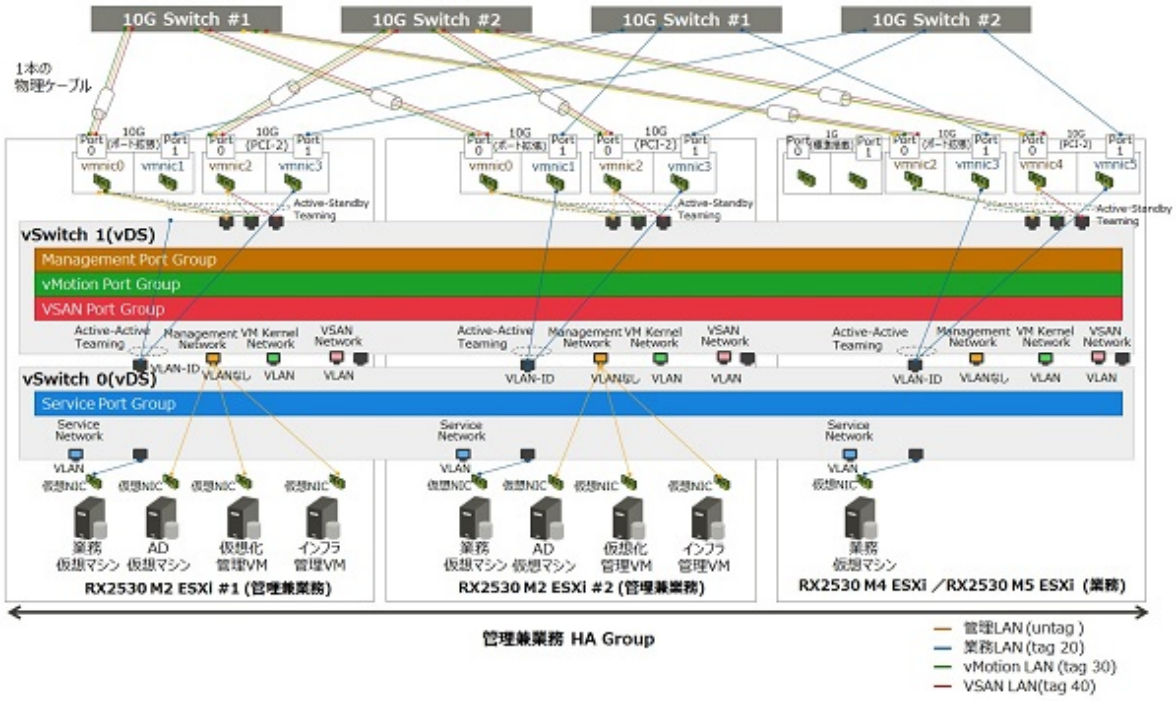
表D.1 PRIMEFLEX HSのネットワーク構成

項目	既存サーバーとネットワーク構成		クラスタ拡張時に追加するサーバーとネットワーク構成	
サーバー機種	PRIMERGY RX2530 M2 PRIMERGY RX2540 M2	PRIMERGY CX2550 M2	PRIMERGY RX2530 M2 PRIMERGY RX2540 M2 PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY RX2530 M5 PRIMERGY RX2540 M5	PRIMERGY CX2550 M2 PRIMERGY CX2560 M4 PRIMERGY CX2560 M5
ネットワーク構成	・ ポート拡張オプション 10G x2ポート ・ PCI 10G x2ポート	・ ポート拡張オプション 1G x2ポート ・ PCI 10G x2ポート	・ ポート拡張オプション 10G x2ポート ・ PCI 10G x2ポート	・ ポート拡張オプション 10G x2ポート ・ PCI 1G x2ポート

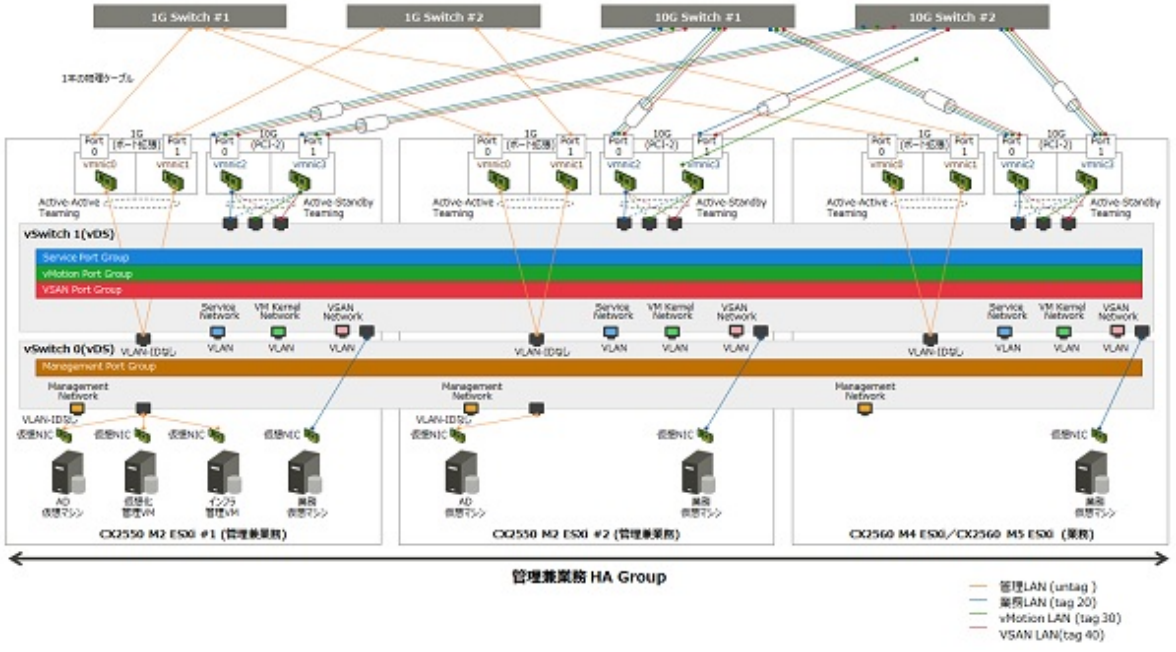
表D.2 PRIMEFLEX for VMware vSANのネットワーク構成

項目	既存サーバーとネットワーク構成	クラスタ拡張時に追加するサーバーとネットワーク構成
サーバー機種	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY CX2560 M4	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY CX2560 M4 PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX2530 M6 PRIMERGY RX2540 M6
	PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX4770 M5	PRIMERGY RX2530 M5 PRIMERGY RX2540 M5 PRIMERGY CX2560 M5 PRIMERGY RX4770 M5 PRIMERGY RX2530 M6 PRIMERGY RX2540 M6 PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
	PRIMERGY RX2530 M6 PRIMERGY RX2540 M6	PRIMERGY RX2530 M6 PRIMERGY RX2540 M6 PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
	PRIMERGY RX2530 M7 PRIMERGY RX2540 M7	PRIMERGY RX2530 M7 PRIMERGY RX2540 M7
ネットワーク構成	・ ポート拡張オプション 10G/25G x2ポート ・ PCI 10G/25G x2ポート	・ ポート拡張オプション 10G/25G x2ポート ・ PCI 10G/25G x2ポート

図D.1 PRIMEFLEX HSのPRIMERGY RX2530 M2環境へPRIMERGY RX2530 M4／PRIMERGY RX2530 M5を追加する場合のネットワーク構成



図D.2 PRIMEFLEX HSのPRIMERGY CX2550 M2環境へPRIMERGY CX2560 M4／PRIMERGY CX2560 M5を追加する場合のネットワーク構成



D.4 ハードウェア要件

SDSでは、既存サーバーと同等構成のハードウェアでサーバーを追加することが推奨されています。しかし、既存サーバーとクラスタ拡張時に追加するサーバーの世代が異なっていると、同等の構成にできない場合があります。

ここでは、既存サーバーに対するクラスタ拡張時に追加するサーバーのハードウェア構成の選択方針について説明します。

既存サーバーとクラスタ拡張時に追加するサーバーで関連性があるオプションは、以下のとおりです。新規クラスタを構成するサーバーの場合も同様です。

- ベースユニット
- CPU
- メモリー
- HDD
- SSD
- オンボードLAN（Flexible LOMなど）
- SASコントローラーカード
- オプションカード（搭載必須LANカード）

注意

- 関連性があるオプションは、下記に記載している方針に従い、選択することを推奨します。この方針に合わないオプションを選択した場合、性能に影響が出る可能性があります。クラスタ拡張時に追加するサーバーの推奨構成は、コンフィグレータにより確認できます。
- 関連性がないオプションは、各サーバーの搭載条件、およびお客様環境に応じて選択してください。

各オプションの詳細は、以下のとおりです。

D.4.1 ベースユニット

「D.1 追加可能なサーバー」に記載されたサーバー機種を追加可能です。

D.4.2 CPU

既存サーバーとクラスタ拡張時に追加するサーバーで搭載可能なCPU世代が異なるため、クラスタ拡張時に追加するサーバーに搭載するCPUは、既存サーバーに搭載されたCPUと同等以上のCPUを搭載することを推奨します。

同等以上のCPUとは、コア数、およびクロック数がともに既存サーバーに搭載されたCPU以上とします。

CPUの個数は既存サーバーと同じとします。

既存サーバーに搭載されているCPUによっては、クラスタ拡張時に追加するサーバーに搭載可能な同等以上のCPUが存在しない場合があります。その場合、既存サーバーとはクラスタを分けて運用することを推奨します。

同等ではないCPUが搭載されたサーバーを同じクラスタに追加した場合、仮想マシンや仮想マシンコンポーネントの配置先によって、仮想マシンのスループットに影響を及ぼす可能性があります。

D.4.3 メモリー

クラスタ拡張時に追加するサーバーに搭載するメモリーは、既存サーバー1ノード当たりの搭載メモリーの総容量以上となるように搭載します。

既存サーバーと同じ型名のメモリーが手配可能な場合、同じ型名で、同じ個数を搭載することを推奨します。

同じ型名のメモリーが存在しない場合、メモリー1個当たりの容量や搭載個数については追加先と異なっていても問題ありません。

D.4.4 HDD（キャパシティ）

クラスタ拡張時に追加するサーバーに搭載するHDDは、既存サーバーと同じ型名のHDDが手配可能な場合は、同じ型名で、同じ個数を搭載することを推奨します。

既存サーバーと同じ型名のHDDが、クラスタ拡張時に追加するサーバーでサポートされていない場合は、同等以上の性能を持つHDDを使用し、ディスク容量が既存サーバー以上となるように搭載します。

クラスタ拡張時に追加するサーバーに搭載するHDDは、すべて同じ型名としてください。新規クラスタを構成するサーバーの場合も同様です。

同等以上の性能を持つHDDは、以下の条件を満たすHDDとします。条件を満たすHDDが複数存在する場合は、「回転数」がクラスタ拡張時に追加するサーバーに近いHDDを選択します。

項目	条件
HDD種別（ニアラインSAS、SASなど）	既存サーバーと同じ
回転数（rpm）	既存サーバーと同等以上
セクターサイズ	既存サーバーと同じ

HDD1台当たりのディスク容量と搭載数については、クラスタ拡張時に追加するサーバー当たりのディスク容量が既存サーバー以上となるように搭載します。

HDD搭載パターンとしては、以下の構成があります。

条件を満たすHDD搭載パターンが複数存在する場合、構成1 > 構成2 = 構成3 > 構成4の順で推奨します。

なお、SDSとしてのHDD搭載数の条件は満たす必要があります。

構成	項目	
	ディスク容量（HDD1台当たり）	搭載数
構成1	既存サーバーと同じ	既存サーバーと同じ台数
構成2	既存サーバーより容量が多い、かつ最も容量が少ないHDD	既存サーバーと同じ台数
構成3	既存サーバーより容量が少ない、かつ最も容量が多いHDD	サーバー当たりのキャパシティ容量が既存サーバー以上となる最小の個数 （既存サーバーより多い台数）
構成4	既存サーバーより容量が多い、かつ最も容量が少ないHDD	サーバー当たりのキャパシティ容量が既存サーバー以上となる最小の個数 （既存サーバーより少ない台数）

以下にHDDの搭載例を示します。

例1：

既存サーバー（vSAN）のHDD構成：900GB x 4台

- クラスタ拡張時に追加するサーバーのディスクが400GB、900GB、1TB、2TBの場合は、構成1の900GB x 4台になります。
- クラスタ拡張時に追加するサーバーのディスクが400GB、1TB、2TBの場合は、構成2の1TB x 4台になります。
- クラスタ拡張時に追加するサーバーのディスクが400GB、600GBの場合は、構成3の600GB x 6台になります。
- クラスタ拡張時に追加するサーバーのディスクが2TBの場合は、構成4の2TB x 2台になります。

例2：

既存サーバー（vSAN）のHDD構成：600GB x 2台

- クラスタ拡張時に追加するサーバーのディスクが400GB、1.2TBの場合は、構成3の400GB x 3台（HDD搭載数は2台以上なので、1.2TB x 1台は不可）になります。

D.4.5 SSD（キャッシュ／キャパシティ）

クラスタ拡張時に追加するサーバーに搭載するSSDは、既存サーバーと同じ型名のSSDが手配可能な場合は、同じ型名で、同じ個数を搭載することを推奨します。

既存サーバーと同じ型名のSSDが、クラスタ拡張時に追加するサーバーでサポートされていない場合は、同等以上の性能を持つSSDを使用し、ディスク容量が既存サーバー以上となるように搭載します。

製品クラスについては、既存サーバーと同じものを推奨しますが、お客様環境に合わせて変更可能です。

クラスタ拡張時に追加するサーバーに搭載するSSDは、すべて同じ型名としてください。新規クラスタを構成するサーバーの場合も同様です。

同等以上の性能を持つSSDは、以下の条件を満たすSSDとします。

項目	条件
データ転送速度（SAS 12Gbpsなど）	既存サーバーと同じ
記録方式（MLCなど）	既存サーバーと同じ

SSD1台当たりのディスク容量と搭載数については、クラスタ拡張時に追加するサーバー当たりのディスク容量が既存サーバー以上となるように搭載します。

搭載パターンとしては、以下の構成があります。

条件を満たすSSD搭載パターンが複数存在する場合、構成1 > 構成2 = 構成3 > 構成4の順で推奨します。

なお、各SDSとしてのSSD搭載数の条件は満たす必要があります。

構成	項目		
	ディスク容量（SSD1台当たり）	搭載数	製品クラス （書込み保証値）
構成1	既存サーバーと同じ	既存サーバーと同じ台数	既存サーバーと同数を推奨
構成2	既存サーバーより容量が多い、かつ最も容量が少ないSSD	既存サーバーと同じ台数	
構成3	既存サーバー未満、かつ最も容量が多いSSD	サーバー当たりのキャパシティ容量が既存サーバー以上となる個数 （既存サーバーより多い台数）	
構成4	既存サーバーより容量が多い、かつ最も容量が少ないSSD	サーバー当たりのキャパシティ容量が既存サーバー以上となる最小の個数 （既存サーバーより少ない台数）	

D.4.6 オンボードLAN（Flexible LOMなど）

「D.3 ネットワーク構成」に記載された通信速度／ポート数を持つオプションを選択してください。

D.4.7 SASコントローラーカード

各世代のサーバーで選択可能なvSAN接続用のSASコントローラーカードを選択します。

SASコントローラーカードには、導入するESXi／vSANのバージョンをサポートするファームウェアの適用が必要となります。

必要に応じて、SASコントローラーカードのファームウェアをアップデートしてください。

vSANのバージョンとファームウェアのバージョンの対応関係については、下記サイトを参照してください。

Certified PRIMERGY Components for VMware Virtual SAN（VMware Virtual SAN認証コンポーネント一覧）

https://jp.fujitsu.com/platform/server/primergy/software/vmware/support/

また、SASコントローラーカードのファームウェアとドライバーバージョンの組合せで、vSAN Ready Node認証を取得しているため、ファームウェアのアップデートに伴い、ドライバーのアップデートも必要となります。

ファームウェア／ドライバーバージョンについては、ノード間で不一致でも構いません。ただし、性能への影響、障害対応などの点から最新バージョンへのアップデートを推奨します。

D.4.8 オプションカード（搭載必須LANカード）

「D.3 ネットワーク構成」で記載したように、クラスタ拡張時に追加するサーバーを既存サーバーと同じネットワーク構成にするために搭載するLANカードです。その要件を満たすLANカードを選択してください。

ネットワークインターフェイス（10GBase／10GBase-T、25GBase／25GBase-T）は、既存サーバーと同じにしてください。

D.4.9 上記以外のオプション

上記以外のオプションについては、クラスタ拡張時に追加するサーバーとは関連がないため、各PRIMEFLEXの要件やお客様の要件に応じて選択可能です。

D.5 ソフトウェア要件

D.5.1 ソフトウェアバージョン

クラスタ拡張時に追加するサーバーと既存サーバーは、同じバージョンのソフトウェアを導入する必要があります。

既存サーバーに導入されているソフトウェアが、クラスタ拡張時に追加するサーバーをサポートしていない場合は、サーバーを追加する前に、既存サーバーのソフトウェアをアップデートしてください。新規クラスタを構成するサーバーの場合も同様です。

各PRIMEFLEXに導入されているソフトウェアのアップデート方針は、以下のとおりです。

ソフトウェア名	導入場所	バージョン
ESXi	• クラスタ拡張時に追加するサーバー • 既存サーバー	既存サーバーおよびクラスタ拡張時に追加するサーバーで、ともにサポートされているバージョンを導入してください。 既存サーバー、クラスタ拡張時に追加するサーバーともに同じバージョン(ビルド番号を含む)にしてください。
vSAN	• クラスタ拡張時に追加するサーバー • 既存サーバー	既存サーバーおよびクラスタ拡張時に追加するサーバーで、ともにサポートされているバージョンを導入してください。 既存サーバー、クラスタ拡張時に追加するサーバーともに同じバージョン(ビルド番号を含む)にしてください。
vCenter Server(vCSA)	仮想化管理VM	ESXiと同等か、より新しいバージョンを導入してください。
Windows Server(ADVM)	ADVM	購入時のバージョンを導入してください。
ISM for PRIMEFLEX	インフラ管理VM	既存サーバーおよびクラスタ拡張時に追加するサーバーのESXi/vSANをサポートするバージョンを導入してください。
ServerView RAID Manager	ADVM	既存サーバーおよびクラスタ拡張時に追加するサーバーのESXiをサポートするバージョンを導入してください。
ServerView Suite DVD	インフラ管理VM	ServerView Suite DVDをISM for PRIMEFLEXにインポートしてください。 なお、インポートするServerView Suite DVDに同梱されているServerView Installation Managerが以下の要件を満たしていることを確認してください。 • クラスタ拡張時に追加するサーバーに導入するカスタムイメージ版数をサポートしていること

D.5.2 ソフトウェア版数確認

クラスタ拡張先となるvSANクラスタのESXiホストに導入されているESXiのバージョンを確認します。

以下のサイトに公開されている『VMware ESXiサポート版数一覧表(PRIMERGY機種別)』を参照し、確認したESXiのバージョンがクラスタ拡張時に追加するサーバーでサポートされているかを確認します。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/support/

サポートされていない場合、ソフトウェアのアップデートが必要となります。クラスタ拡張時に追加するサーバーでサポートされているESXiのバージョンを確認し、アップデートするESXiのバージョンを決定してください。

クラスタ拡張時に使用するESXiのバージョンを決定したら、そのESXiバージョンをサポートする以下のソフトウェアのバージョンを確認します。新規クラスタを構成するサーバーの場合も同様です。

- PRIMERGYのファームウェア
- vCSAのバージョン

- ISM for PRIMEFLEXのバージョン
- RAID Managerのバージョン
- ServerView Installationのバージョンと、それを同梱するServerView Suite DVDのバージョン

D.5.3 SASコントローラーカードのファームウェア確認

SASコントローラーカードのファームウェアのバージョンが、「D.5.2 ソフトウェア版数確認」で決定したESXiのバージョンをサポートしていることを確認します。

以下のサイトに公開されている『Certified PRIMERGY Components for VMware Virtual SAN（VMware Virtual SAN認証コンポーネント一覧）』を参照してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/support/

ESXiのバージョンとvSANバージョンの対応関係は以下を参照してください。

https://kb.vmware.com/s/article/2150753

SASコントローラーカードのファームウェアをアップデートした場合、ドライバーもアップデートが必要なことがあります。

以下のサイトに公開されている『VMware vSphereソフトウェア説明書（PRIMERGY）』を参照してください。

参照するソフトウェア説明書は、ご使用のESXiのバージョンに対応したドキュメントを参照してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/support/

D.6 管理VMのサイジング

追加するサーバーの台数に応じて、インフラ管理VM、仮想化管理VM、ADVMのリソースが不足する場合があります。

各VMのリソースが不足する場合、物理／仮想リソースを追加してください。

リソース増加のためにサーバーを追加する場合であっても、事前にISM-VAやvCSAにリソースを確保する必要があります。

管理兼業務サーバーの物理リソースが不足する場合は、管理兼業務サーバーに物理メモリー／ディスクを追加してください。

登録ノード数に対し必要なリソース量、およびリソース量の変更手順については、各ソフトウェアのマニュアルを参照してください。

各モデルにおける工場出荷時の管理VMのリソース量と登録可能ノード数は、以下のとおりです。

モデル名	管理VM名／ソフトウェア名	リソース量			登録可能ノード数
		CPU	メモリー	ディスク	
PRIMEFLEX HS V1.0	インフラ管理VM （ISM for PRIMEFLEX）	4vCPU	16GB	136GB	400ノード
	仮想化管理VM （vCenter Server Appliance）	2vCPU	10GB	120GB	ホスト：10台 仮想マシン：100台
PRIMEFLEX HS V1.1	インフラ管理VM （ISM for PRIMEFLEX）	4vCPU	16GB	136GB	400ノード
	仮想化管理VM（Small選択時） （vCenter Server Appliance）	4vCPU	16GB	290GB	ホスト：100台 仮想マシン：1000台
PRIMEFLEX for VMware vSAN	インフラ管理VM （ISM for PRIMEFLEX）	4vCPU	16GB	100GB	400ノード
	仮想化管理VM（Small選択時） （vCenter Server Appliance）	4vCPU	16GB	290GB	ホスト：100台 仮想マシン：1000台

付録E　トラブルシューティング

ISMの動作がエラーになる場合や、期待した動作にならない場合の主な原因と対処について説明します。

現象：IPアドレスの編集を行ってノード登録を行った場合、登録時に「手動検出したノードの登録に失敗しました。IPアドレスが変更できません。指定されたIPアドレスは既に存在します。」のエラーが表示される。

原因／対処

IPアドレスの編集を行ってノード登録を行う場合、変更後のIPアドレスにpingを行い、応答がないことを確認してから実施してください。

iRMC S3世代のPRIMERGYは、IPアドレス変更後の数分間、変更前と変更後の両方のIPアドレスに対してpingが成功する場合があります。

現象：正常に使用できていたISMでGUIへのログインに「セッションタイムアウト」で失敗し、ISM-VAを再起動しても現象が変わらない。
ハイパーバイザのコンソール画面には、以下のようなメッセージが出力されている。

```
[55490.269659] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.272852] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.275983] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.277488] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.278907] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.280367] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.281844] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.284837] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.286288] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.287727] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.289073] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.290441] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.291716] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
[55490.294744] XFS (dm-0): Corruption detected. Unmount and run xfs_repair
[55490.296176] ffff8801ecb6e000: 42 4d 41 50 00 00 00 82 00 00 00 00 00 7a 2e fc  BMAP.........z..
[55490.297620] ffff8801ecb6e010: ff ff ff ff ff ff ff ff 00 00 00 00 03 a5 20 00  .............. .
[55490.299035] ffff8801ecb6e020: 00 00 10 a1 ae 80 00 80 00 00 00 00 03 a6 20 00  .............. .
[55490.300401] ffff8801ecb6e030: 00 00 10 a1 c5 80 00 30 00 00 00 00 03 a6 80 00  .......0........
[55490.301766] XFS (dm-0): Internal error xfs_bmap_read_extents(1) at line 1321 of file fs/xfs/libxfs/xfs_bmap.c.
Caller xfs_iread_extents+0x75/0xd0 [xfs]
```

原因／対処

- ISM-VAの仮想ディスクが破損しているためISMが正常に動作していません。

  仮想ディスクの破損は、物理的なハードの異常や、ISM-VAを動作させているサーバーまたはISM-VAが強制的に停止された場合に起こることがあります。

- バックアップ済みのISM-VAがある場合は、バックアップ済みのISM-VAをリストアして使用してください。
  バックアップしていない場合は、新規にインストールしてください。

現象：以下の機能において、ファイルのインポート操作の実施時に、ファイル選択画面で「サーバーとの通信に失敗しました。」のエラーが表示される。

- [構築]-[プロファイル]-[アクション]-[インポート]-[ブラウズ]ボタン
- [構築]-[ファームウェア/ドライバー]-画面左側のメニューから[インポート]を選択し、[インポートデータリスト]タブ-[アクション]-[DVDインポート]-[ブラウズ]ボタン
- [構築]-[ファームウェア/ドライバー]-画面左側のメニューから[インポート]を選択し、[インポートデータリスト]タブ-[アクション]-[ファームウェアインポート]-[ブラウズ]ボタン

- [構築]-[ファームウェア/ドライバー]-画面左側のメニューから[インポート]を選択し、[SeverView Suite]タブ-[アクション]-[DVDインポート]-[ブラウズ]ボタン

原因／対処

- 使用者が所属しているユーザーグループのFTPフォルダー配下のファイルについて、ファイル名にUTF-8でない文字コードが含まれていないか確認してください。
- ISMとクライアントの通信状態を確認してください。

現象：ノードの状態確認、制御に失敗する。

原因／対処

- 対象ノードとISM間のネットワークが正しく動作していることを確認してください。
- 電源ケーブルが対象装置に接続されているか、電源が供給されているかを確認してください。
- ISMに登録されているIPアドレスと、対象装置（またはOS）のIPアドレスが一致しているか確認してください。特にIPアドレスを変更した場合は、ISMの登録情報の変更忘れがないか確認してください。
- ISMに登録されているユーザーアカウントと、対象装置（またはOS）のユーザーアカウントが一致しているか確認してください。特にパスワードを変更した場合は、ISMの登録情報の変更忘れがないか確認してください。
- ISMで操作対象ノードに対して、ISMの別の機能を利用中でないことを確認してください（ファームウェアアップデート中にプロファイル適用を開始するなど）。

現象：Microsoft Active DirectoryをLDAPサーバー設定で登録すると失敗する。

原因／対処

大量のユーザー情報（例えば1000件以上）を登録しているActive Directoryを登録する場合、Active Directoryの「MaxPageSize」という環境変数が、登録ユーザー情報数に応じた値になっているか確認してください。

現象：GUIを使用したISMの修正パッチまたはアップグレードプログラム適用開始後、GUI画面に以下のメッセージが表示され適用が失敗する。また、GUIからログインできなくなる。

```
修正パッチ／アップグレードプログラムの適用が失敗しました。
ERROR:50980030:Update failed () (Elapsed: xx:xx:xx)
```

原因／対処

- ディスク容量不足のため修正パッチまたはアップグレードプログラムの適用に失敗しています。
- ISM-VAを再起動することにより適用前の状態で使用できるようになります。
- ISMの修正パッチまたはアップグレードプログラム適用時は、ISM-VAのシステム領域に以下のサイズの空き容量を確保したうえで適用してください。

  修正パッチ：3.5GB以上

  アップグレードプログラム：5.5GB以上

ファームウェア管理機能

現象：ファームウェアのアップデート操作を行う際に、アップデートするファームウェアが指定できない。

原因／対処

- ファームウェアデータは、事前にインポートして取り込んでおく必要があります。インポートしていない場合は、最初にインポートを実行してください。
- 個別ファームウェアのインポートの際、指定したファームウェア種別、モデル名などが間違っていると、指定したノードに対応するファームウェアとして表示されません。リポジトリ画面で情報を確認してください。間違いがある場合は、一度リポジトリから削除したあとに、正しい情報でインポートを実行してください。

- ファームウェアのバージョンを下げることができないため、ノードの現行バージョンより古いファームウェアは、最新バージョン欄に表示されません。ノードの現行バージョンと、インポートしたファームウェアのバージョンを確認してください。

現象：PCIカードのOnlineアップデートに失敗する。

原因／対処

Onlineアップデートの場合、PCIカードのファームウェアの動作は、PCIカードが搭載されているサーバーのOSに依存します。ファームウェアデータ添付のドキュメント、または入手元を参照し、ファームウェアがサーバーのOSに対応しているか確認してください。

ファームウェアがサーバーのOSに対応していない場合は、Offlineアップデートを使用してください。

現象：リリースノート内の文字が正常に表示されない

原因／対処

ご利用のブラウザーのエンコードの設定によって、リリースノートの表示が正常に行われない場合があります。エンコードの設定を確認してください。

現象：ETERNUS DX/AFモデルのファームウェアアップデートに失敗する。

原因／対処

「Update モード実施可能」な条件を満たしていない可能性があります。

ファームウェアデータと共に提供されている、留意事項のpdfファイルの「ファームウェアアップデート実行可否バージョンマトリクス」を参照して、ご利用の環境が「Update モード実施可能」な条件を満たしているか確認してください。

現象：Offlineアップデートが失敗する。

原因／対処

- Offlineアップデートを使用するには、ServerView Suite Update DVDがインポートされている必要があります。ServerView Suite Update DVDがインポートされているか確認してください。
- PXEブートを動作させるための環境設定に問題がある可能性があります。以下を確認してください。
  - DHCPサーバーが適切なIPアドレスをリースできるか
  - ノードのBIOS設定でPXE機能が無効になっていないか
  - ノードのオンボードLANまたはLANカードとISMが接続されているか、など

プロファイル管理機能

現象：PRIMERGYサーバーに対するプロファイル適用／再適用／適用解除がエラーになる。

原因／対処

プロファイル適用操作時に、対象ノードの電源がオンになっています。PRIMERGYへのプロファイル適用操作は、電源をオフにした状態で実行してください。

現象：スイッチ、ストレージに対するプロファイル適用／再適用／適用解除がエラーになる。

原因／対処

ISM以外からSSHやWeb経由で対象ノードに接続している状態のときは、ISMから設定を実行するとエラーになる場合があります。ISMからノードを操作する際は、外部からの接続をログアウトしてください。

現象：プロファイル管理機能でOSインストールがエラーになる。

原因／対処

- インストール対象のOSインストールメディアがインポートされていません。インストールするOSのインストールメディアをインポートしてからプロファイル適用を実行してください。
- インストール対象ノードとOS種別に対応したServerView Suite DVDがインポートされていません。インストール対象ノードとOS種別をサポートしたServerView Suite DVDをインポートしてからプロファイル適用を実行してください。プロファイル内で使用する

ServerView Suite DVDバージョンの指定がない場合は、インポートされた最新のDVDが使用されます。旧機種、旧OSの場合には、使用するDVDバージョンをプロファイル内で設定してください。

- PXEブートを動作させるための環境設定に問題がある可能性があります。以下を確認してください。
  - DHCPサーバーが適切なIPアドレスをリースできるか
  - ノードのBIOS設定でPXE機能が無効になっていないか
  - ノードのオンボードLANまたはLANカードとISMが接続されているか、など

現象：エクスポートしたプロファイル／ポリシーをインポートするとエラーになる。

原因／対処

エクスポート元のISMに、そのままインポートすると、同一名の既存プロファイル／ポリシーが存在するためエラーとなります。インポートするファイル内の「ProfileName」を編集して、プロファイル名／ポリシー名を変更してください。

ネットワーク管理機能

現象：ネットワークマップに接続情報が表示されない。

原因／対処

ISMが接続情報を自動的に取得して表示するためには、各ノードのLLDP機能を有効にする必要があります。ノードの取扱説明書などを参照して、LLDPを有効にしてください。LLDP機能を持たないノードの場合は、ISM画面の手動接続定義で接続情報を入力してください。

現象：ネットワークマップの表示情報が古い、また正しい情報が表示されない。

原因／対処

- ネットワークマップに表示される内容は、GUI画面上で[ネットワーク管理情報の取得]を最後に実行した時点の情報となります。[ネットワーク管理情報の取得]を実行してください。
- ノードのポート状態などが変更された場合は、[ノード情報取得]を実行後に、[ネットワーク管理情報の取得]を実行してください。

現象：ネットワークマップに仮想スイッチ、仮想マシンの接続関係が表示されない、または表示内容に誤りがある。

原因／対処

仮想スイッチ、仮想マシンの接続関係を表示するためには、管理対象ノードを管理している仮想化管理ソフトウェア、および管理対象ノードのOS情報をISMに登録しておく必要があります。

仮想化管理ソフトウェア情報、および管理対象ノードのOS情報が正しく登録されているかを確認してください。

現象：VLAN設定の変更に失敗する。

原因／対処

- 設定対象のネットワークスイッチがISMからアクセス可能である必要があります。ネットワークスイッチが正常に動作し、ISMからアクセス可能になっていることを確認してください。
- ネットワークスイッチの機種によっては予約済みのVLAN IDがあります。変更するVLAN IDが設定対象のネットワークスイッチの予約済みVLAN IDでないことを確認してください。

現象：リンクアグリゲーション設定の変更に失敗する。

原因／対処

- 設定対象のネットワークスイッチがISMからアクセス可能である必要があります。ネットワークスイッチが正常に動作し、ISMからアクセス可能になっていることを確認してください。
- ネットワークスイッチの機種に応じて設定可能なLAG名や動作モードが異なります。LAG名や動作モードについて設定可能であることを装置仕様で確認してください。

ログ管理機能

現象：ノードのログが収集されない、ノードのログ収集に失敗する。

原因／対処

- 通信状態などによる影響でログ収集に失敗した場合、時間をおいて再度実行してください。
- ノードを新規に登録した時点では、ログ収集は行われない状態になっています。[ログ収集設定]でログ収集スケジュールを設定してください。
- ノードの詳細画面の[ログ収集設定]タブ内で、ステータスが「対象外」となっていて、ログ収集用のアクションボタンが表示されない場合は、ノードがログ収集対象外の機器か、ノード登録直後で機器情報が未取得の状態です。ログ収集対象ノードの場合は、数分待ったあとに画面を更新してください。
- ログ収集時に指定するログ種類の[対象]を確認してください。スケジュール設定の場合は、[スケジュール実行有効化]にチェックが付いていることを確認してください。
- GUI画面から[ログ収集実行]を実行するとログが収集できるが、スケジュール設定してもログが収集できていない場合は、スケジュール実行のタイミングでノードの電源がオフになっているなどが考えられます。スケジュールの内容を確認してください。
- ログファイルの総容量がユーザーグループ設定に設定された上限（サイズ制限）設定値を超えると、新たなログは保管されません。グローバルナビゲーションメニューの[イベント]-[イベント]の[運用ログ]タブを確認し、ログ収集のタイミングで以下のどれかが記録されている場合は、収集済みのログを一部削除してファイル容量を減らしてください。
  - 「ノード(<ノード名>)のログ収集中に、ユーザーグループ(<ユーザーグループ名>)の保管ログ保存領域が設定容量(xxMB)に達しました。」
  - 「ノード(<ノード名>)のログ収集中に、ユーザーグループ(<ユーザーグループ名>)のノードログ(ダウンロード用データ)保存領域が設定容量(xxMB)に達しました。」
  - 「ノード(<ノード名>)のログ収集中に、ノードログ（ログ検索用データ）保存領域が設定容量(xxMB)に達しました。」

現象：ノードのログ収集の設定ができない。

原因／対処

ノードのステータスが「対象外」となっている場合は、ノードがログ収集のサポート対象であるか確認してください。サポート対象で「対象外」となっている場合は、ISMがノード情報を取得できていないことがあるので、ノードとのネットワーク接続やノードプロパティの設定を確認したあと、[ノード情報取得]を実行してください。

現象：ノードのログ収集で、「オペレーティングシステム」、「ServerView Suite」が指定できない。

原因／対処

- 対象ノードのOS情報が登録されていないか、ISMがノードのOS情報を未取得の場合は指定できません。OS情報を登録後に[ノード情報取得]を実行してください。
- OSの種類によっては、「ServerView Suite」は取得対象外のため指定できません。

Nutanix AHV上でのISM-VAの動作

現象：ISM-VAのIPアドレスを変更した場合、NutanixのPRISMに変更前と変更後のIPアドレスが表示される。

原因／対処

Nutanixの仕様により、ISM-VAのIPアドレス変更から約24時間の間はPRISMに変更前と変更後のIPアドレスが表示されます。ISM-VAに設定されているIPアドレスを確認するためには、ismadmコマンドまたはismsetupコマンドを使用してください。ISMの動作に影響はありません。

付録F　PRIMEFLEX HS／PRIMEFLEX for VMware vSANのローリングアップデートで実行するスクリプト

ESXiの修正パッチやオフラインバンドルには制限事項や注意事項がある場合があります。詳細は、以下のサイトを参照して『VMware vSphere ソフトウェア説明書（PRIMERGY）』の注意事項をご確認ください。注意事項の対処は、スクリプトを作成することでローリングアップデート機能の実行中に対応できます。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

注意事項の対処は、スクリプトによってローリングアップデート機能の実行中に対応できます。必要に応じてスクリプトを作成してください。スクリプトは、以下の3つのタイミングで実行が可能です。

- ESXiの修正パッチ／オフラインバンドル適用前
- ESXiの修正パッチ／オフラインバンドル適用時
- ESXiの修正パッチ／オフラインバンドル適用後

注意

- ESXiの修正パッチ／オフラインバンドル適用時とは適用コマンド実行直後のことであり、ESXiの再起動前になります。

  ESXiの修正パッチ／オフラインバンドル適用後とは適用コマンドを実行して、ESXiの再起動も実行した後になります。
- スクリプトは規定時間（720秒）以内で終了しないとローリングアップデートに失敗します。ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

実行するスクリプト名は固定です。以下の実行するタイミングごとにスクリプト名は異なります。

スクリプト名 [注]	実行するタイミング
pre_script.sh	ESXiの修正パッチ／オフラインバンドル適用前に実行する
post01_script.sh	ESXiの修正パッチ／オフラインバンドル適用時に実行する
post02_script.sh	ESXiの修正パッチ／オフラインバンドル適用後に実行する

[注]：スクリプトの形式はシェル（bash）のみサポートしています。

ポイント

- 「exit 1」でスクリプトを終了することでエラー検出できます。
- 事後処理でスクリプトの実行結果を確認できるように、ESXi上にログをファイル出力するなどの処理を入れてください。

適用前に実行するスクリプトの作成例

ESXiをパッチ適用する際に必要な以下の処理を実行するスクリプトをそれぞれ作成しています。

- ツールの削除
- ドライバーの削除
- ドライバーの設定変更

「ツールの削除」のスクリプト例

```
#!/usr/bin/sh

### Tool removal ###
echo "Tool removal Start" >> /scratch/log/pre_script.log
```

```
toolName=`(esxcli software vib list | grep storcli)`
if [ $? = 0 ]; then
    echo ${toolName} >> /scratch/log/pre_script.log
    toolName=`(echo ${toolName} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ${toolName}"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Tool removal End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

「ドライバーの削除」のスクリプト例

```
#!/usr/bin/sh

### Driver removal ###
echo "Driver removal Start" >> /scratch/log/pre_script.log
driver1=`(esxcli software vib list | grep "OEM.500")`
if [ $? = 0 ]; then
    echo ${driver1} >> /scratch/log/pre_script.log
    driver1Name=`(echo ${driver1} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ¥"${driverName1}¥""
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver removal End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

「ドライバーの設定変更」のスクリプト例

```
#!/usr/bin/sh

### Driver settings ###
echo "Driver settings Start" >> /scratch/log/pre_script.log
driver2=`(esxcli system module list | grep lsi_mr3)`
if [ $? = 0 ]; then
    echo ${driver2} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_mr3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
driver3=`(esxcli system module list | grep lsi_msgpt3)`
if [ $? = 0 ]; then
    echo ${driver3} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_msgpt3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
```

```
echo "Driver settings End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

適用時に実行するスクリプトの作成例

ここではESXi 6.7の運用と保守の注意事項に対する対処を実行するスクリプトを作成しています。

v470-1のカスタムイメージで構築したESXiに、パッチ「ESXi670-201905001」以降を適用する際のInboxドライバーの置換を実施するスクリプトです。

```
#!/usr/bin/sh

#### parameter settings ####
EffectiveValue='VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip -n lsi-mr3 -n lsi-msgpt3'

### Execution command ###
cmd="esxcli software vib install --dry-run -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

echo "post01_script End" >> /scratch/log/post01_script.log
exit 0
```

適用後に実行するスクリプトの作成例

ESXiの修正パッチ／オフラインバンドル適用後の制限事項／注意事項に対する以下の対処を実行するスクリプトをそれぞれ作成しています。

- 電力管理設定に関する留意事項
- igbnドライバーの更新について
- テンポラリ領域の設定

「電力管理設定に関する留意事項」のスクリプト例

```
#!/usr/bin/sh

#### parameter settings ####
PowerValue="High Performance"

### Execution command ###
# Power Policy
echo "Power Policy Start" >> /scratch/log/post02_script.log
CurrentValue=`esxcli system settings advanced list --option=/Power/CpuPolicy | grep '   String Value: High Performance'`
if [ $? != 0 ]; then
    cmd='esxcli system settings advanced set --option=/Power/CpuPolicy --string-value="High Performance"'
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
```

```
echo "Power Policy End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

「igbnドライバーの更新について」のスクリプト例

```
#!/usr/bin/sh

#### parameter settings ####
DriverFile="＜適用するドライバーファイル名＞"

### Execution command ###
# Update Driver
echo "Update Driver Start" >> /scratch/log/post02_script.log
cmd="esxcli software vib install -d /var/tmp/RollingUpdatePatch/${DriverFile}"
echo ${cmd} >> /scratch/log/post02_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi
echo "Update Driver End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

「テンポラリ領域の設定」のスクリプト例

```
#!/usr/bin/sh

#### parameter settings ####
TemporaryName="scratch"

### Execution command ###
# Temporary
echo "Temporary Start" >> /scratch/log/post02_script.log
TmpSetting=`(vim-cmd hostsvc/advopt/view ScratchConfig.ConfiguredScratchLocation | grep "value")`
TmpDir=`(echo ${TmpSetting} | cut -f 2 -d '"')`
if [ ${#TmpDir} = 0 ]; then
    cmd="mkdir /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
    cmd="vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Temporary End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

ポイント

スクリプトの1行目には、以下の記述をする必要があります。

```
#!/usr/bin/sh
```

注意

作成するスクリプトには、対象ノードを再起動する処理は入れないでください。スクリプト実行の後には必ず再起動が実行されます。