

FUJITSU Software

Infrastructure Manager V2.4

Infrastructure Manager for PRIMEFLEX V2.4

A horizontal band featuring a red abstract graphic with flowing, curved lines and bright light flares, creating a sense of motion and energy.

解説書

CA92344-2697-03
2019年5月

まえがき

本書の目的

本書では、サーバ、ストレージ、スイッチなどのICT機器やファシリティ機器(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。

- FUJITSU Software Infrastructure Manager (以降、「ISM」と表記)
- FUJITSU Software 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
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.4 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。
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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
FUJITSU Software Infrastructure Manager V2.4 Infrastructure Manager for PRIMEFLEX V2.4 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 - Infrastructure Manager Plug-in for VMware vCenter Server Appliance - Infrastructure Manager Management Pack for VMware vRealize Operations - Infrastructure Manager Plug-in for VMware vRealize Orchestrator 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。

<http://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。

<http://jp.fujitsu.com/platform/server/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、以下のとおり略称で記載することがあります。

正式名称	略称	
Microsoft® Windows Server® 2019 Datacenter	Windows Server 2019 Datacenter	Windows Server 2019
Microsoft® Windows Server® 2019 Standard	Windows Server 2019 Standard	
Microsoft® Windows Server® 2019 Essentials	Windows Server 2019 Essentials	
Microsoft® Windows Server® 2016 Datacenter	Windows Server 2016 Datacenter	Windows Server 2016
Microsoft® Windows Server® 2016 Standard	Windows Server 2016 Standard	
Microsoft® Windows Server® 2016 Essentials	Windows Server 2016 Essentials	
Microsoft® Windows Server® 2012 R2 Datacenter	Windows Server 2012 R2 Datacenter	Windows Server 2012 R2
Microsoft® Windows Server® 2012 R2 Standard	Windows Server 2012 R2 Standard	
Microsoft® Windows Server® 2012 R2 Essentials	Windows Server 2012 R2 Essentials	
Microsoft® Windows Server® 2012 Datacenter	Windows Server 2012 Datacenter	Windows Server 2012
Microsoft® Windows Server® 2012 Standard	Windows Server 2012 Standard	
Microsoft® Windows Server® 2012 Essentials	Windows Server 2012 Essentials	
Microsoft® Windows Server® 2008 R2 Datacenter	Windows Server 2008 R2 Datacenter	Windows Server 2008 R2
Microsoft® Windows Server® 2008 R2 Enterprise	Windows Server 2008 R2 Enterprise	
Microsoft® Windows Server® 2008 R2 Standard	Windows Server 2008 R2 Standard	
Red Hat Enterprise Linux 8.0 (for Intel64)	RHEL 8.0	Red Hat Enterprise Linux または Linux
Red Hat Enterprise Linux 7.6 (for Intel64)	RHEL 7.6	
Red Hat Enterprise Linux 7.5 (for Intel64)	RHEL 7.5	
Red Hat Enterprise Linux 7.4 (for Intel64)	RHEL 7.4	
Red Hat Enterprise Linux 7.3 (for Intel64)	RHEL 7.3	
Red Hat Enterprise Linux 7.2 (for Intel64)	RHEL 7.2	
Red Hat Enterprise Linux 7.1 (for Intel64)	RHEL 7.1	
Red Hat Enterprise Linux 6.10 (for Intel64)	RHEL 6.10(Intel64)	
Red Hat Enterprise Linux 6.10 (for x86)	RHEL 6.10(x86)	
Red Hat Enterprise Linux 6.9 (for Intel64)	RHEL 6.9(Intel64)	
Red Hat Enterprise Linux 6.9 (for x86)	RHEL 6.9(x86)	

正式名称	略称	
Red Hat Enterprise Linux 6.8 (for Intel64)	RHEL 6.8(Intel64)	
Red Hat Enterprise Linux 6.8 (for x86)	RHEL 6.8(x86)	
Red Hat Enterprise Linux 6.7 (for Intel64)	RHEL 6.7(Intel64)	
Red Hat Enterprise Linux 6.7 (for x86)	RHEL 6.7(x86)	
Red Hat Enterprise Linux 6.6 (for Intel64)	RHEL 6.6(Intel64)	
Red Hat Enterprise Linux 6.6 (for x86)	RHEL 6.6(x86)	
SUSE Linux Enterprise Server 15 (for AMD64 & Intel64)	SUSE 15(AMD64) SUSE 15(Intel64) または SLES 15(AMD64) SLES 15(Intel64)	SUSE Linux Enterprise Server または Linux
SUSE Linux Enterprise Server 12 SP4 (for AMD64 & Intel64)	SUSE 12 SP4(AMD64) SUSE 12 SP4(Intel64) または SLES 12 SP4(AMD64) SLES 12 SP4(Intel64)	
SUSE Linux Enterprise Server 12 SP3 (for AMD64 & Intel64)	SUSE 12 SP3(AMD64) SUSE 12 SP3(Intel64) または SLES 12 SP3(AMD64) SLES 12 SP3(Intel64)	
SUSE Linux Enterprise Server 12 SP2 (for AMD64 & Intel64)	SUSE 12 SP2(AMD64) SUSE 12 SP2(Intel64) または SLES 12 SP2(AMD64) SLES 12 SP2(Intel64)	
SUSE Linux Enterprise Server 12 SP1 (for AMD64 & Intel64)	SUSE 12 SP1(AMD64) SUSE 12 SP1(Intel64) または SLES 12 SP1(AMD64) SLES 12 SP1(Intel64)	
SUSE Linux Enterprise Server 12 (for AMD64 & Intel64)	SUSE 12(AMD64) SUSE 12(Intel64) または SLES 12(AMD64) SLES 12(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for AMD64 & Intel64)	SUSE 11 SP4(AMD64) SUSE 11 SP4(Intel64) または SLES 11 SP4(AMD64) SLES 11 SP4(Intel64)	
SUSE Linux Enterprise Server 11 SP4 (for x86)	SUSE 11 SP4(x86) または SLES 11 SP4(x86)	
VMware® vSphere™ ESXi 6.7	VMware ESXi 6.7	VMware ESXi
VMware® vSphere™ ESXi 6.5	VMware ESXi 6.5	
VMware® vSphere™ ESXi 6.0	VMware ESXi 6.0	
VMware® vSphere™ ESXi 5.5	VMware ESXi 5.5	

正式名称	略称
VMware Virtual SAN	vSAN

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。

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富士通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、逆アセンブルをとま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、VMwareロゴ、VMware ESXi、VMware SMPおよびVMotionはVMware,Inc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。

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。

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

Copyright 2019 FUJITSU LIMITED

本書を無断で複製・転載することを禁止します。

改版履歴

版数	提供年月	変更内容	章・節・項	変更箇所
01	2019年2月	新規作成	—	—
02	2019年4月 ISM 2.4.0.b パッチ適用 による変更	FQDNでのノード検出と結果表示に関する記事を追記	2.2.1.6 ノードの検出	—
		UPnP／Redfishによる自動検出の際の要件について表を追記	2.2.1.6 ノードの検出	自動検出実行「注意」
		管理対象ノードのAIS Gateway との連携に関する記事を追記	2.2.2 データセンター／フロア／ラック／ノードの確認	—
		OS設定のポリシーに関するポイントを新規作成	2.4.2 プロファイルとポリシー	ポリシーの作成
		アップデート時のスクリプト実行の記事を新規作成	2.6.2.3 アップデート時のスクリプト実行	—
		仮想ネットワーク ボトルネック分析機能の記事を新規作成	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	—
		ファームウェア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に種別とアップデート方法を追記	2.12.4 ファームウェアローリングアップデート機能	—
		Offlineアップデートサブタスクの処理一覧を追記	2.12.4.2 タスク一覧	—
		コマンド出力結果の説明に動作モードを追加	3.5 ライセンスの登録	表「コマンド出力結果の説明」
		コマンド出力結果の説明に動作モードを追加	4.8 ライセンス設定	表「コマンド出力結果の説明」
	2019年4月 主な構成変更や記事改善	『入門書』へ一部の記事を移動	第1章	—
		他製品との連携に関する記事を新規作成	1.4 他製品との連携	—
		分析VMが動作するホストに必要なリソース量を修正	2.11.2 分析VMの確認	—
		監視対象OS、仮想化管理ソフトウェアの設定に関する記事を新規作成	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	—
03	2019年5月 ISM 2.4.0.c パッチ適用 による変更	PRIMERGY GX2580 M5のログ取得に関する記事を追記	2.5.1 収集可能なログの種類	—
			付録A ノードを管理・運用するための環境設定詳細 ・ A.3.2 ログ管理機能利用時のディスク消費量の目安	—
		サポートする仮想化管理ソフトウェアに関する記事を追記	2.13.6 仮想化管理ソフトウェア管理機能	—
		サポートOSに Red Hat Enterprise Linux 8.x を追加	・ B.1.1 監視対象OSごとに必要な設定	—

版数	提供年月	変更内容	章・節・項	変更箇所
			• B.3.1 sshサービスの起動確認	
		Red Hat Enterprise Linux 8.0でのドメインユーザー使用時の手順を追記	• B.9.1 KVM Red Hat Enterprise Linuxへの設定手順(ドメインユーザー使用時)	手順10の「注意」
		PRIMERGY M5シリーズに関する記事とPRIMEFLEX for VMware vSANに関する記事を追記	• D.1.1 追加可能な後継機サーバ • D.1.2 ネットワーク構成 • D.2.1 事前準備	—
	2019年5月 主な構成変更や記事改善	ドメインユーザーアカウントの設定手順を修正	• B.2.5 ドメインユーザーアカウント使用時の設定	—
		LANポートの指定に関する注意事項を追記	• 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	「注意」

目 次

第1章 Infrastructure Managerの概要	1
1.1 主な機能概要	1
1.1.1 ノード管理機能の概要	1
1.1.2 モニタリング機能の概要	1
1.1.3 プロファイル管理機能の概要	1
1.1.4 ログ管理機能の概要	1
1.1.5 ファームウェア管理機能の概要	2
1.1.6 ネットワーク管理機能の概要	2
1.1.7 仮想リソース管理機能の概要	2
1.1.8 仮想ネットワークパケット分析機能の概要	3
1.1.9 ISM for PRIMEFLEXの機能概要	3
1.2 構成	4
1.3 システム要件	6
1.3.1 ISM-VAを動作させるハイパーバイザーの要件	6
1.3.2 管理端末のシステム要件	6
1.3.3 ISMの運用に必要なサービス要件	8
1.3.4 ISM for PRIMEFLEXの動作要件	9
1.4 他製品との連携	10
第2章 ISMの機能	12
2.1 ユーザーインターフェース	12
2.1.1 GUI	12
2.1.2 FTPアクセス	15
2.1.3 コンソールアクセス	17
2.1.4 REST API	17
2.2 ノード管理機能	17
2.2.1 データセンター／フロア／ラック／ノードの登録	17
2.2.1.1 データセンター／フロア／ラックの登録	18
2.2.1.2 ノードの登録	18
2.2.1.3 ノード情報の管理	19
2.2.1.4 ノードのラック搭載位置情報の管理	20
2.2.1.5 ノードのOS情報の登録	20
2.2.1.6 ノードの検出	21
2.2.1.7 ノードへのタグ付け	28
2.2.2 データセンター／フロア／ラック／ノードの確認	29
2.2.3 データセンター／フロア／ラック／ノードの編集	31
2.2.4 データセンター／フロア／ラック／ノードの削除	31
2.3 モニタリング機能	32
2.3.1 監視項目／しきい値の設定	33
2.3.2 ネットワーク統計情報監視	33
2.3.3 アクション設定	34
2.3.4 アラーム設定の登録	37
2.3.5 監視履歴グラフ表示	40
2.4 プロファイル管理機能	40
2.4.1 プロファイルの利用方法	41
2.4.2 プロファイルとポリシー	43
2.4.2.1 ポリシーグループ／ポリシーの作成	44
2.4.2.2 プロファイルグループ／プロファイルの作成	44
2.4.2.3 プロファイルの適用	45
2.4.2.4 プロファイルの編集と再適用	45
2.4.2.5 プロファイルの適用解除と削除	46
2.4.2.6 プロファイルのエクスポート／インポート	47
2.4.2.7 プロファイルグループの編集／削除	48
2.4.2.8 ポリシーグループの編集／削除	48
2.4.2.9 プロファイル適用時の動作指定	48

2.4.3 OSインストールの設定	49
2.4.4 仮想IO管理機能	49
2.4.5 プール管理機能	52
2.4.6 ブート情報の確認	53
2.5 ログ管理機能	54
2.5.1 収集可能なログの種類	55
2.5.2 ログ保有期間の設定	57
2.5.3 ログ収集対象と収集日時の設定	57
2.5.4 ログ収集の動作	59
2.5.5 ノードログの検索	61
2.5.6 ノードログのダウンロード	61
2.5.7 保管ログのダウンロード	63
2.5.8 ノードログの削除	64
2.5.9 保管ログの削除	65
2.6 ファームウェア管理機能	65
2.6.1 ノードのファームウェアバージョンの確認	66
2.6.2 ファームウェアのアップデート	66
2.6.2.1 ファームウェアアップデート方法	67
2.6.2.2 アップデート時の動作	68
2.6.2.3 アップデート時のスクリプト実行 (ISM 2.4.0.b 以降)	69
2.6.2.4 ファームウェアアップデートの実施	71
2.6.3 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	73
2.6.4 ジョブ管理	74
2.6.5 ファームウェアベースライン	74
2.6.5.1 ファームウェアベースライン定義の作成	75
2.6.5.2 ファームウェアベースライン定義の割当て	76
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	76
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	77
2.6.5.5 ファームウェアベースライン定義の編集	77
2.6.5.6 ファームウェアベースライン定義の削除	77
2.7 ネットワーク管理機能	78
2.7.1 ネットワーク接続情報の表示	79
2.7.2 ネットワーク管理情報の更新	80
2.7.3 ネットワーク接続の変化情報の確認	81
2.7.4 ネットワーク接続の変化情報の基準設定	81
2.7.5 ネットワーク統計情報の表示	82
2.7.6 VLAN、リンクアグリゲーション設定の確認	82
2.7.7 VLAN設定の変更	83
2.7.8 リンクアグリゲーション設定の変更	84
2.7.9 手動でのネットワーク接続情報の設定	84
2.8 電力制御機能	85
2.8.1 電力制御設定の追加／編集	85
2.8.2 電力制御の有効／無効	86
2.9 仮想リソース管理機能	86
2.9.1 サポート対象の仮想リソース	87
2.9.2 仮想リソース管理GUI	88
2.9.3 仮想リソース管理の操作	89
2.9.3.1 ストレージプールの使用状況の監視	90
2.9.3.2 ストレージプールの異常の特定	93
2.9.3.3 仮想リソース情報の更新	97
2.10 ハードウェア設定バックアップ／リストア機能	98
2.10.1 ハードウェア設定のバックアップ	98
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	99
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	99
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	100
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	100
2.10.6 ハードウェア設定のリストア	101

2.10.7 ハードウェア設定バックアップファイルの削除.....	101
2.11 仮想ネットワーク パケット分析機能.....	102
2.11.1 サポート対象.....	102
2.11.2 分析VMの確認.....	102
2.11.3 仮想ネットワーク パケット分析機能の表示項目.....	103
2.11.4 仮想ネットワーク パケット分析機能の機能差.....	103
2.11.5 仮想ネットワーク パケット分析機能の動作.....	104
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 (ISM 2.4.0.b 以降).....	104
2.12 ISM for PRIMEFLEXの機能.....	105
2.12.1 クラスタ管理機能.....	105
2.12.1.1 クラスタ管理GUI.....	106
2.12.1.2 クラスタ管理機能のサポート対象.....	115
2.12.1.3 クラスタ情報の取得と更新.....	116
2.12.1.4 クラスタの管理／監視.....	117
2.12.1.5 PRIMEFLEX for Microsoft Storage Spaces Direct 仮想ディスクの監視.....	119
2.12.2 クラスタ作成機能.....	120
2.12.2.1 自動設定項目.....	121
2.12.2.2 プロファイル管理機能との連携.....	124
2.12.2.3 クラスタ定義パラメーター.....	125
2.12.2.4 タスク一覧.....	125
2.12.3 クラスタ拡張機能.....	126
2.12.3.1 自動設定項目.....	127
2.12.3.2 プロファイル管理機能との連携.....	129
2.12.3.3 クラスタ定義パラメーター.....	130
2.12.3.4 タスク一覧.....	131
2.12.4 ファームウェアローリングアップデート機能.....	131
2.12.4.1 ファームウェア管理機能との連携.....	133
2.12.4.2 タスク一覧.....	134
2.13 ISM運用基盤の機能.....	135
2.13.1 ユーザー管理機能.....	136
2.13.2 リポジトリ管理機能.....	143
2.13.2.1 ファームウェアデータの保存と削除.....	143
2.13.2.2 OSインストールファイルの保存と削除.....	148
2.13.2.3 ServerView Suite DVDの保存と削除.....	149
2.13.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入.....	150
2.13.4 タスク管理.....	151
2.13.5 ISM-VA管理機能.....	151
2.13.5.1 ISM-VA管理機能のコマンド一覧.....	152
2.13.6 仮想化管理ソフトウェア管理機能.....	155
2.13.6.1 仮想化管理ソフトウェアの登録.....	155
2.13.6.2 仮想化管理ソフトウェアからの情報取得.....	156
2.13.6.3 仮想化管理ソフトウェアの編集.....	157
2.13.6.4 仮想化管理ソフトウェアの削除.....	158
2.13.7 共有ディレクトリ管理機能.....	158
2.13.7.1 共有ディレクトリの追加.....	158
2.13.7.2 共有ディレクトリの編集.....	159
2.13.7.3 共有ディレクトリの削除.....	159
2.13.7.4 共有ディレクトリのマウント.....	160
2.13.7.5 共有ディレクトリのマウント解除.....	160
2.13.8 ISM連携管理機能.....	160
2.13.8.1 他ISMのステータス情報のリンク表示.....	160
2.13.8.2 他ISMのリンク用の証明書管理.....	161
2.13.9 他ソフトウェア連携機能.....	162
2.13.9.1 Deep Security連携の事前準備.....	163
2.13.9.2 Deep Securityへの連携手順.....	165
第3章 ISMの導入.....	168

3.1 ISM導入の流れ.....	168
3.2 ISMの導入設計.....	169
3.2.1 ディスク資源の見積り.....	169
3.2.1.1 ログ保存容量の見積り.....	171
3.2.1.2 リポジトリの必要容量の見積り.....	171
3.2.1.3 ノード管理データ容量の見積り.....	172
3.2.1.4 障害調査ログ容量の見積り.....	172
3.2.1.5 保守資料容量の見積り.....	172
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.....	172
3.2.2 ネットワークの設計.....	172
3.2.3 ノード名の設定.....	173
3.2.4 ユーザーの設計.....	173
3.3 ISM-VAのインストール.....	174
3.3.1 Microsoft Windows Server Hyper-Vへのインストール.....	174
3.3.2 VMware vSphere Hypervisorへのインストール.....	174
3.3.3 KVMへのインストール.....	175
3.4 ISM-VAの環境設定.....	176
3.4.1 ISM-VAの初回起動.....	176
3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(初回).....	176
3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(初回).....	177
3.4.1.3 KVMで動作するISM-VAの場合(初回).....	180
3.4.2 ISM-VAの初期設定.....	180
3.4.2.1 基本設定メニューを使用した初期設定.....	180
3.4.2.2 ismadmコマンドを使用した初期設定.....	181
3.5 ライセンスの登録.....	184
3.6 ユーザーの登録.....	186
3.7 仮想ディスクの割当て.....	186
3.7.1 ISM-VA全体に対する仮想ディスク割当て.....	186
3.7.2 ユーザーグループに対する仮想ディスク割当て.....	187
3.8 仮想リソース管理機能の事前設定.....	188
3.9 クラスタ管理機能の事前設定.....	189
3.9.1 vSANの事前設定.....	189
3.9.2 PRIMEFLEX for Microsoft Storage Spaces Directの事前設定.....	191
3.9.3 ISMへの事前設定.....	192
第4章 ISMの操作.....	195
4.1 ISMの起動と終了.....	195
4.1.1 ISM-VAの起動.....	195
4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合(導入後).....	195
4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(導入後).....	196
4.1.1.3 KVMで動作するISM-VAの場合(導入後).....	199
4.1.2 ISM-VAの終了.....	199
4.1.3 ISM-VAの再起動.....	200
4.1.4 ISMのサービス起動と停止.....	200
4.2 ISM-VA基本設定メニュー.....	200
4.3 ISM公開サービスポートの変更.....	203
4.4 ISM-VAのバックアップとリストア.....	203
4.4.1 ハイパーバイザーによるISM-VAのバックアップ／リストア.....	204
4.4.2 ISM-VA管理コマンドによるISMのバックアップ／リストア.....	204
4.4.2.1 ISMバックアップ.....	208
4.4.2.2 ISMリストア.....	209
4.4.2.3 バックアップファイル一覧表示.....	209
4.5 保守資料の採取.....	210
4.5.1 ISM／ISM-VAの保守資料.....	210
4.5.1.1 障害調査ログ切替え.....	211
4.5.1.2 障害調査ログレベル切替え.....	211
4.5.1.3 coreファイル採取ディレクトリの指定.....	212

4.5.1.4 ISMの保守資料の採取方法	212
4.5.2 ISM for PRIMEFLEXの保守資料	212
4.5.2.1 クラスタ作成機能のログ	213
4.5.2.2 クラスタ拡張機能のログ	213
4.5.2.3 クラスタ管理機能のログ	214
4.5.2.4 ファームウェアローリングアップデート機能のログ	214
4.6 仮想ディスクの管理	214
4.6.1 仮想ディスクの割当て解除	214
4.6.2 ISM-VA全体に対する仮想ディスクの追加割当て	215
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	215
4.7 証明書設定	216
4.7.1 SSLサーバ証明書配置	216
4.7.2 SSLサーバ証明書表示	217
4.7.3 SSLサーバ証明書出力	217
4.7.4 SSLサーバ自己署名証明書作成	217
4.7.5 CA証明書のダウンロード	218
4.8 ライセンス設定	218
4.9 ネットワーク設定	219
4.10 アラーム通知設定	220
4.11 ISM-VAサービス制御	220
4.12 システム情報の表示	221
4.13 ホスト名変更	222
4.14 プラグイン操作	222
4.14.1 プラグイン適用	222
4.14.2 プラグイン表示	223
4.14.3 プラグイン削除	223
4.15 ISM-VA内部のDHCPサーバ	224
4.15.1 ISM-VA内部のDHCPサーバの設定	224
4.15.2 ISM-VA内部のDHCPサービスの操作	225
4.15.3 ISM-VA内部のDHCPサーバ情報の確認	226
4.15.4 DHCPサーバの切替え	226
4.16 MIBファイル設定	226
4.17 修正パッチ適用	227
4.18 ISM-VAのアップグレード	228
4.19 ISM-VAの統計情報表示	228
4.19.1 統計情報の概要表示	229
4.19.2 統計情報の詳細表示	229
4.19.3 リアルタイムの情報表示	230
4.19.4 統計情報ファイル出力	230
4.20 SSL/TLSプロトコルのバージョンの変更	231
4.21 他ソフトウェア連携設定	231
4.22 GUIを使用したファイルアップロード	232
第5章 ノードの保守	233
5.1 メンテナンスモード	233
5.2 エラー発生時の調査方法	234
付録A ノードを管理・運用するための環境設定詳細	235
A.1 ISMの動作環境設定	235
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	235
A.1.2 仮想リソース管理機能の事前設定	236
A.1.3 ETERNUS DX/AFドライブエンクロージャの表示	240
A.1.4 MIBファイルのインポートに関する注意	240
A.2 管理対象ノードの設定詳細	241
A.2.1 使用ポート番号一覧	241
A.2.2 ノード設定詳細	244
A.3 ノードの運用に関するその他の情報	247
A.3.1 ファームウェアアップデート時間の目安	248

A.3.2 ログ管理機能利用時のディスク消費量の目安	249
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	252
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	252
B.1.1 監視対象OSごとに必要な設定	252
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	252
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	253
B.2 監視対象への設定手順 (OS: Windows)	253
B.2.1 WinRMサービスの起動確認	254
B.2.2 WinRMサービスの設定	254
B.2.3 ファイアウォールのポート開放	257
B.2.4 Windows PowerShellの実行ポリシー変更	257
B.2.5 ドメインユーザーアカウント使用時の設定	258
B.3 監視対象への設定手順 (OS: Red Hat Enterprise Linux)	259
B.3.1 sshサービスの起動確認	259
B.3.2 ドメインユーザーアカウント使用時の設定	260
B.3.3 一般ユーザーアカウント使用時の設定	260
B.3.4 ユーザーアカウント共通の設定	261
B.4 監視対象への設定手順 (OS: SUSE Linux Enterprise Server)	261
B.4.1 sshサービスの起動確認	262
B.4.2 ファイアウォールのポート開放	262
B.4.3 ドメインユーザーアカウント使用時の設定	265
B.4.4 一般ユーザーアカウント使用時の設定	266
B.4.5 ユーザーアカウント共通の設定	266
B.5 監視対象への設定手順 (OS: VMware ESXi)	267
B.5.1 ドメインユーザーアカウント使用時の設定	267
B.6 監視対象への設定手順 (仮想化管理ソフトウェア: vCenter Server)	267
B.6.1 ISM-VAへDNS情報の追加	267
B.6.2 ドメインユーザーアカウント使用時の設定	267
B.7 監視対象への設定手順 (仮想化管理ソフトウェア: Microsoft Failover Cluster)	268
B.7.1 ドメインユーザーアカウント使用時の設定	268
B.8 監視対象への設定手順 (仮想化管理ソフトウェア: Microsoft System Center)	268
B.9 監視対象への設定手順 (仮想化管理ソフトウェア: KVM)	268
B.9.1 KVM Red Hat Enterprise Linuxへの設定手順 (ドメインユーザー使用時)	269
B.9.2 KVM SUSE Linux Enterprise Serverへの設定手順 (ドメインユーザー使用時)	274
B.9.3 一般ユーザーアカウント使用時の設定	287
B.10 監視対象への設定手順 (仮想化管理ソフトウェア: IPCOM)	288
B.10.1 仮想マシン情報取得コマンド実行権限設定手順	288
B.11 監視対象への設定手順 (仮想化管理ソフトウェア: OpenStack)	288
B.11.1 コントローラーノードへの設定手順	288
B.11.2 仮想ネットワーク分析機能使用時の設定	293
付録C ISM-VAのアンインストール	295
付録D 後継機種のクラスタ拡張	298
D.1 後継機種のクラスタ拡張の要件	298
D.1.1 追加可能な後継機種サーバ	298
D.1.2 ネットワーク構成	299
D.1.3 ハードウェア要件	301
D.1.4 ソフトウェア要件	303
D.2 後継機種のクラスタ拡張	305
D.2.1 事前準備	305
D.2.2 ISM for PRIMEFLEXによるクラスタ拡張	306
付録E トラブルシューティング	307

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 ノード管理機能の概要

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 モニタリング機能の概要

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。

1.1.3 プロファイル管理機能の概要

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)にOSをインストール
- ・ 管理対象ノード(サーバ)に仮想MACアドレス／仮想WWNの割当て、サーバ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 ログ管理機能の概要

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の概要

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

ファーム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の概要

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の概要

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。

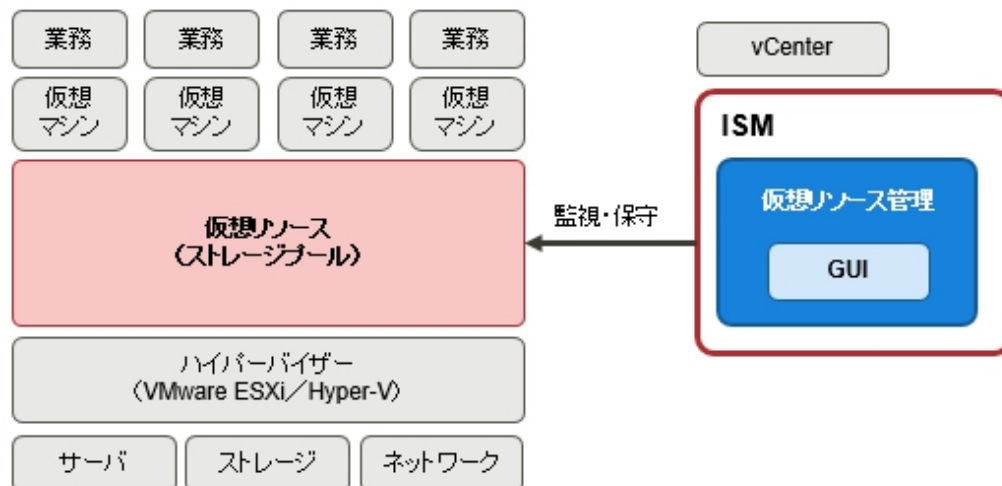
仮想リソース管理機能は、ストレージプールの状態や使用率を表示してストレージプールを管理する機能です。

- ・ 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、リソースの使用率が見える化し、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 パケット分析機能の概要

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、問題箇所を特定を支援します。

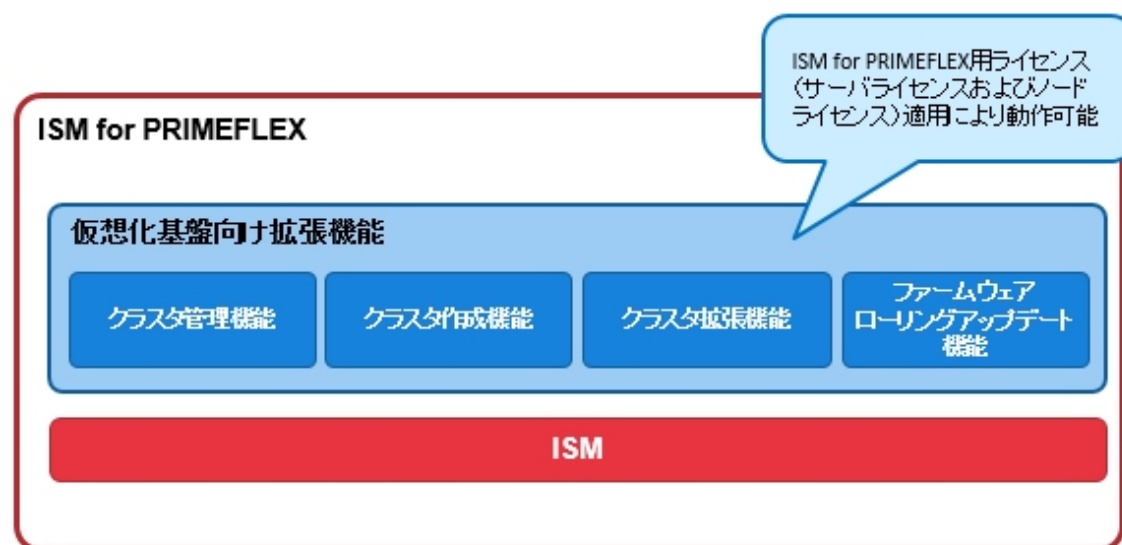
仮想ネットワークパケット分析機能の詳細については、「[2.11 仮想ネットワークパケット分析機能](#)」を参照してください。

1.1.9 ISM for PRIMEFLEXの機能概要

ISM for PRIMEFLEX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、クラスタ管理機能、クラスタ作成機能、クラスタ拡張機能、およびファームウェアローリングアップデート機能を提供します。

ISM for PRIMEFLEXは、垂直統合型仮想化基盤 FUJITSU Integrated System PRIMEFLEX HS、PRIMEFLEX for VMware vSAN、PRIMEFLEX for Microsoft Storage Spaces Directの環境に導入されるインフラ管理ソフトウェアです。

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。

仮想化基盤向け拡張機能	機能概要
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を追加する作業を自動化します。
ファームウェア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に対して、業務を停止することなく、ファームウェアを自動アップデートします。

ISM for PRIMEFLEXの機能詳細については、「[2.12 ISM for PRIMEFLEXの機能](#)」を参照してください。

ポイント

- ・クラスタ管理機能は、クラスタ単位でのリソース管理が可能です。
- ・クラスタ作成機能は、「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。
- ・クラスタ拡張機能は、「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。
- ・ファームウェアローリングアップデート機能は、「ファームウェアローリングアップデート」ウィザードを使用してファームウェアをアップデートできます。

注意

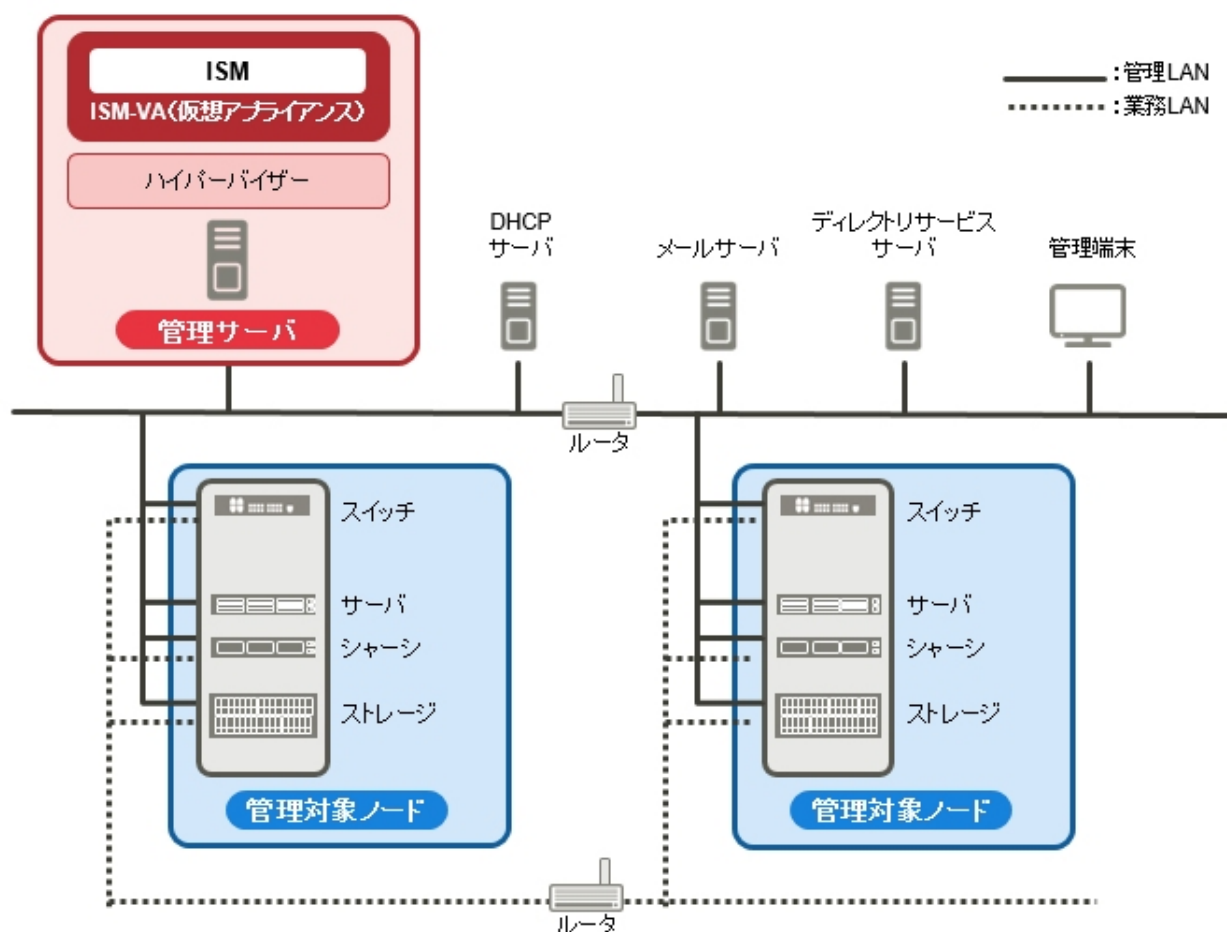
ISM for PRIMEFLEXでは、電力制御機能は使用できません。

1.2 構成

ISMは、原則的に管理対象となるサーバとは別に用意したサーバ上で動作します。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を「管理サーバ」と呼びます。管理サーバとノード間は、LANで接続します。

ISMのネットワークインターフェースは、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。

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。管理サーバは接続しません。
管理サーバ	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。
	ストレージ	

機器および機能		説明
	サーバ (管理対象サーバ)	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)を動作させるハイパーバイザーの要件は以下のとおりです。

項目	説明
CPUコア数	2コア以上[注1][注5]
メモリ容量	8GB以上[注1][注5]
空きディスク容量	35GB以上[注2][注3][注4][注5]
ネットワーク	1Gbps以上
ハイパーバイザー	Hyper-Vの役割が含まれるWindows Server 2012/2012 R2/2016/2019 VMware ESXi 5.5/6.0/6.5/6.7 KVMがインストールされているRed Hat Enterprise Linux 7.2/7.3/7.4/7.5/7.6 KVMがインストールされているSUSE Linux Enterprise Server 12 SP3/15

[注1]: 管理するノード数に応じて、必要なコア数およびメモリ容量が異なります。

ノード数	CPUコア数	メモリ容量
1～100	2	8GB
101～400	4	8GB
401～1000	8	12GB

[注2]: 約100ノードを監視するのに必要最低限のディスク容量です。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。

[注3]: ISM-VAをバックアップする場合は、管理サーバにISM-VAと同等以上の空きディスク容量が必要です。

[注4]: ISM-VA導入時に固定的に割り当てる必要があります。

[注5]: 仮想ネットワークパケット分析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以下のリソースが追加で必要となります。

追加CPUコア数	追加メモリ容量	追加ディスク容量
2コア以上	8GB以上	60GB以上

1.3.2 管理端末のシステム要件

GUI(ブラウザ)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、Windows 10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、Windows 10タブレット:1280×768ピクセル以上 ISM GUIを表示するブラウザ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	- パソコン、サーバ、Windows 10タブレット: - Internet Explorer 11以降 「3Dビュー」画面を表示するためには、更新バージョン:11.0.15以降が適用されている必要があります。 - Microsoft Edge 25以降 - Mozilla Firefox 38以降 - Google Chrome 43以降 - Androidタブレット:Google Chrome 43以降 - iPad:Safari8以降
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	デバイス			
	パソコン、サーバ	Windows 10タブレット	Androidタブレット	iPad
Microsoft Internet Explorer	○[注1] [注4]	○[注1] [注2] [注4]	－	－
Microsoft Edge	○[注4]	○[注2] [注4]	－	－
Mozilla Firefox	○[注4]	○[注2] [注4]	－	－
Google Chrome	○[注4]	○[注4]	○[注4]	－
Safari	－	－	－	○[注3] [注4]

[注1]:ポップアップブロックが有効な場合、GUIのヘルプが表示されません。ヘルプが表示されない場合、[インターネットオプション]-[プライバシー]-[ポップアップブロック]-[設定]-[許可するWebサイトのアドレス]にGUIを表示するときのURLを追加してください。

[注2]:「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3]:デバイスの制限によりファイルを保存できません。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。

[注4]: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
空きディスク容量	8GB以上

項目	説明
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

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 (SMTPサーバ)	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、メールサーバが必要です。 [イベント]-[アラーム]-[SMTPサーバ]で設定します。  注意 ISMに登録できるメールサーバは1つだけです。
ディレクトリサーバ	以下の用途で使用する場合に、ディレクトリサーバが必要です。 - 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サービスは、以下の2種類です。 - OpenLDAP - Microsoft Active Directory 構築したサーバを、[設定]-[ユーザー]-[LDAPサーバ設定]で登録します。  注意 - ISMにはプライマリ、セカンダリの2つのLDAPサーバを登録できます。 - 監視対象ノードがディレクトリ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	以下の場合に、DHCPサーバが必要です。 - プロファイル管理機能でOSインストールを行う場合 - 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)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サーバを別途準備する代わりに、ISM-VAに含まれているDHCPサーバ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」を参照してください。
DNSサーバ	以下の用途で使用する場合に、DNSサーバが必要です。 - ISMにホスト名でアクセスしたい場合 - LDAP連携などISMの各種サーバ設定でFQDNを使う場合

項目	説明
	DNSサーバをISMに設定する方法は、「4.9 ネットワーク設定」の「DNSサーバ追加」を参照してください。  ポイント • DNSサーバを使用せずに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サーバを使用しない場合、LDAP連携などISMの各種サーバ設定は、すべてIPアドレスで設定してください。
NTPサーバ	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に同期させる場合に、NTPサーバが必要です。 NTPサーバを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サーバ追加削除」を参照してください。
Proxyサーバ	管理クライアントからProxyサーバを経由してISMへアクセスする場合に、Proxyサーバが必要です。  注意 監視対象ノードとISM間は、Proxyサーバを経由して接続することはできません。
ルータ	ISMのネットワークインターフェースは、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。

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 サーバライセンス V2
 - Infrastructure Manager Advanced Edition for PRIMEFLEX ノードライセンス V2
- 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:「[2.12.1.2 クラスタ管理機能のサポート対象](#)」
- 事前設定要件:「[3.9 クラスタ管理機能の事前設定](#)」

クラスタ作成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「6.7.2.1 クラスタ作成の動作要件」
- ・ PRIMEFLEX for Microsoft Storage Spaces Directの要件:『操作手順書』の「6.8.2.1 クラスタ作成の動作要件」

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「6.9.2.1 クラスタ拡張の動作要件」
- ・ PRIMEFLEX for Microsoft Storage Spaces Directの要件:『操作手順書』の「6.10.2.1 クラスタ拡張の動作要件」

ファームウェア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。

- ・ 留意事項、前提条件:『操作手順書』の「6.6.2.1 ファームウェアローリングアップデートの動作要件」

ISM for PRIMEFLEX V2.4のサポート製品

ISM for PRIMEFLEX V2.4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。

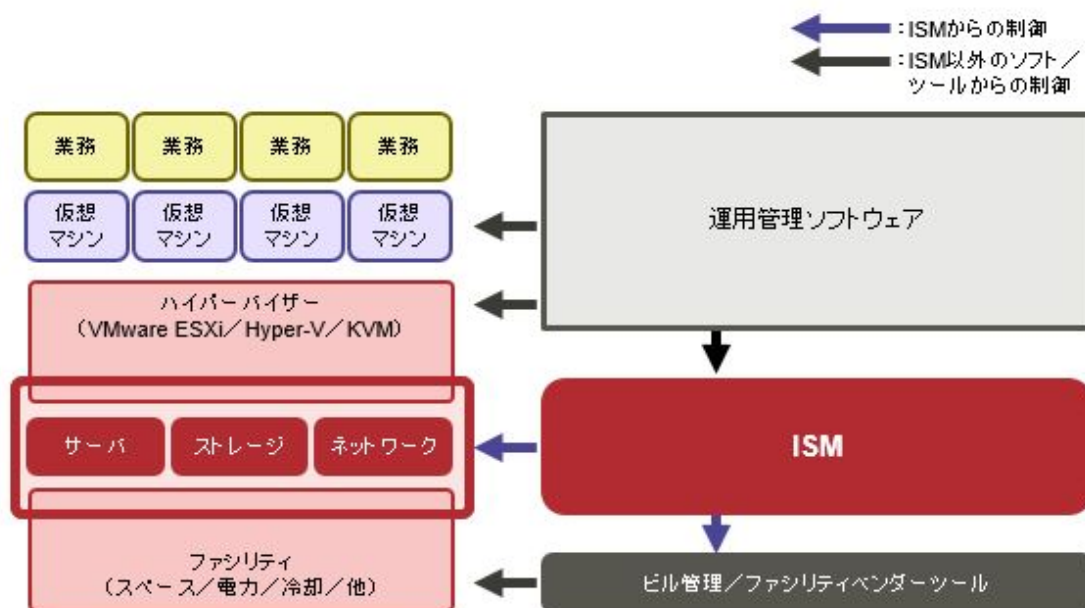
<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/>

1.4 他製品との連携

ISMは、サーバ、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ウェアからの連携
- ・ 総合サーバセキュリティ「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
- VMware vCenter Server Appliance
- VMware vRealize Operations
- VMware vRealize Orchestrator

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
- Infrastructure Manager Plug-in for VMware vCenter Server Appliance
- Infrastructure Manager Management Pack for VMware vRealize Operations
- Infrastructure Manager Management Pack for VMware vRealize Orchestrator

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、「[2.13.9 他ソフトウェア連携機能](#)」を参照してください。

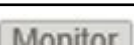
第2章 ISMの機能

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、「[2.13.1 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		
	Operatorロール		
	Monitorロール		
Administratorグループ以外	Administratorロール		
	Operatorロール		
	Monitorロール		

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)



- ー 上記の表示の場合、以下のユーザー属性を持つユーザーが操作を実行できます。
 - 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
- 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ース

ISMのユーザーインターフェースについて説明します。

ISMは、ユーザーインターフェー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ース
- ・ 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ース
- ・ 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ース
- ・ 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ース

2.1.1 GUI

ISMではWebブラウザで動作するGUIを提供します。

ポイント

- 使用するブラウザでCookieおよびJavaScriptを有効にする必要があります。
 - Firefoxを使用する場合、サーバ証明書をブラウザに登録する設定が必要です。
 1. Firefoxを起動します。メニューから[オプション]を選択します。
 2. [詳細]を選択し、[証明書]を選択します。
 3. [証明書を表示]を選択します。
 4. [サーバ証明書]タブの[例外を追加]を選択します。
 5. [URL]に「https://<ISMサーバIPアドレス>または<ISMサーバFQDN名>:25566/」を入力し、[証明書を取得]を選択します。
 6. [次回以降にもこの例外を有効にする]にチェックが入っ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。
 - Internet Explorerを使用する場合、以下の設定が必要です。
 1. Internet Explorerを起動します。メニューから[ツール]-[インターネットオプション]を選択します。
 2. [セキュリティ]タブで[レベルのカスタマイズ]ボタンを選択し、以下の項目で[有効にする]を選択して[OK]ボタンを選択します。
 - [ActiveX コントロールとプラグイン]配下の[ActiveX コントロールとプラグインの実行]
 - [ActiveX コントロールとプラグイン]配下の[スクリプトを実行しても安全だとマークされているActiveXコントロールのスクリプトの実行]
 - [ダウンロード]配下の[ファイルのダウンロード]
 - [ダウンロード]配下の[フォントのダウンロード]
 3. [詳細設定]タブで[マルチメディア]配下の[Webページのアニメーションを再生する]にチェックを付け、[OK]ボタンを選択します。
 - Internet Explorer 11で「3Dビュー」画面を表示するには、Microsoftのサポート技術情報(以下「KB」)2991001が適用されている必要があります。「3Dビュー」画面とは、フロア、ラックの配置、ラック内の機器搭載位置を3次元画像で表示するGUIです。

<https://support.microsoft.com/ja-jp/kb/2991001>

「3Dビュー」画面でラックが表示されない場合、KB 2991001が含まれるマイクロソフトセキュリティ情報 MS14-051を適用してください。詳細については、以下のWebサイトを参照してください。

<https://technet.microsoft.com/ja-jp/library/security/MS14-051>
 - 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などによっては、WebGL機能(ブラウザで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。
- Webブラウザに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。

ISM GUIを起動する方法は以下のとおりです。

1. ブラウザを起動し、以下のURLを入力します。

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

2. ログイン画面が表示されますので、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。

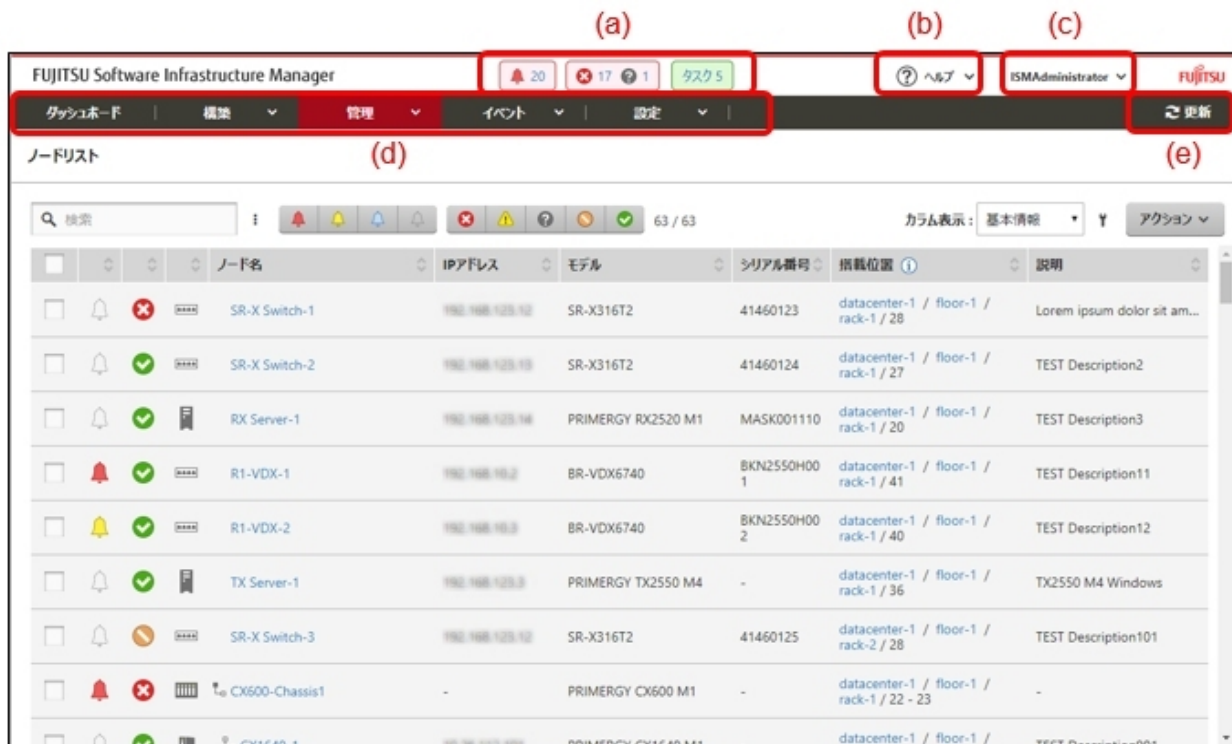
3. 内容を確認し、[上記内容を確認しました]にチェックを入れます。
4. [同意する]ボタンを選択します。

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

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。

(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。

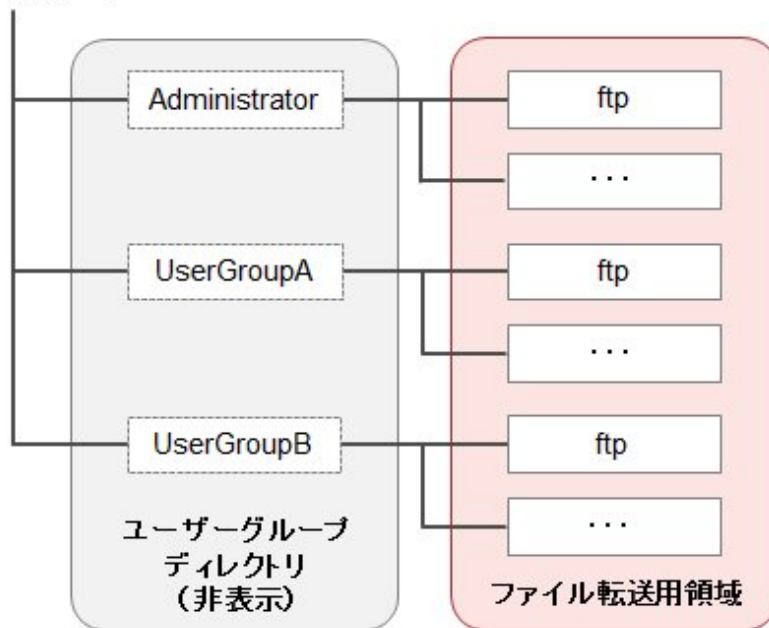


注意

- 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「2.7.2 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>ディレクトリ配下の「ftp」ディレクトリ配下を使用してください。
- 既存ディレクトリの変更／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。
- Microsoft Active DirectoryまたはLDAP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構成

ftpログインルート



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。

「[2.13.1 ユーザー管理機能](#)」で説明する、Administratorロールを持つユーザーのみ使用可能です。

使用可能なコマンドは、「[2.13.5.1 ISM-VA管理機能のコマンド一覧](#)」を参照してください。



[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。

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。

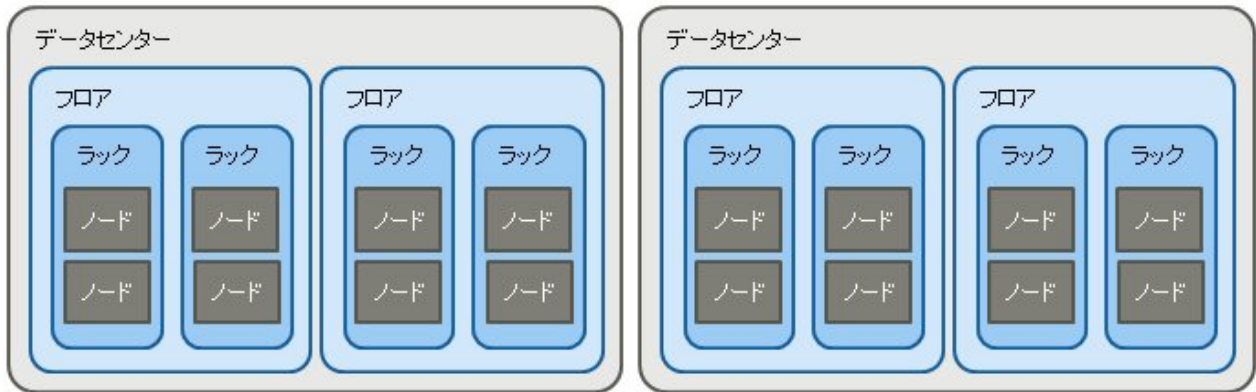
- ・ [2.2.1 データセンター／フロア／ラック／ノードの登録](#)
- ・ [2.2.2 データセンター／フロア／ラック／ノードの確認](#)
- ・ [2.2.3 データセンター／フロア／ラック／ノードの編集](#)
- ・ [2.2.4 データセンター／フロア／ラック／ノードの削除](#)

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



以下の操作を行います。

- [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

実行できるユーザー

Administratorグループ	その他のグループ
<input checked="" type="button" value="Admin"/> Operator Monitor	Admin Operator Monitor

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で一意的な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

実行できるユーザー

Administratorグループ	その他のグループ
<input checked="" type="button" value="Admin"/> Operator Monitor	Admin Operator Monitor

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で一意的な名前を設定する。
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。

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。

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]を選択します。
2. [アクション]ボタンから[登録]を選択します。
3. 「ノード手動登録」ウィザードに従い、設定項目を入力します。
 - ー ノード名
ISM全体で、一意な名称を設定してください。
 - ー ノードタイプ
登録するノードの種類を選択してください。
 - ー モデル
ノードのモデル名を選択してください。サポート外の機種を登録する場合は、モデル名を入力してください。
 - ー IPアドレス
ノードのIPアドレスを設定してください。
 - ー Web i/f URL
ノードのWeb管理画面にアクセスするためのURLを設定してください。
 - ー 説明
ノードの説明(コメント)を自由に設定してください。
4. ノードのアカウント情報を入力します。
5. ノードのラック搭載位置情報を入力します。
6. ノードが所属するノードグループを選択します。
ノードグループを設定しない場合、ノードはノードグループ未割当てとなります。未割当てのノードは、Administratorグループのユーザーのみ管理できます。
7. ノードに設定するタグ情報を指定します。
8. 登録を実行します。



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。

2.2.1.3 ノード情報の管理

	Administratorグループ	その他のグループ
実行できるユーザー	Admin Operator Monitor	Admin Operator Monitor

「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収集します。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。



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サーバブレード、コネクシオ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。

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。

注意

- サーバ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。

操作例を示します。

- 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、[OS]タブを選択します。
- [OSアクション]ボタンから[OS情報編集]を選択します。
- 必要な情報を入力し、適用します。
- [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。
- 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

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。

対象ノードによっ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。

<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/servviewism/environment/>

ポイント

ISM-VAにDNSサーバのIPアドレスが設定されている場合、検出されたノードのFQDN名を取得します。

FQDN名が取得された場合、検出されたノードの登録時にノード名の初期値として入力されます。

DNSサーバのIPアドレス設定については、「[4.2 ISM-VA基本設定メニュー](#)」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
 - ー 検出設定を入力して手動検出実行
 - ー 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

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、またはFQDN名を設定します (FQDN名はISM 2.4.0.b以降)。
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。

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

- ー [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。
- ー [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。
- ー [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、またはFQDN名) (FQDN名はISM 2.4.0.b以降)
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
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

項目名	説明
	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 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	－	－	◎	－	－	－
HttpsPort	－	－	○	－	－	－
SnmpType	－	－	－	◎	◎	◎
SnmpPort	－	－	－	○	○	○
Community	－	－	－	◎	◎	－
V3Account	－	－	－	－	－	◎
V3SecLevel	－	－	－	－	－	◎
V3AuthProtocol	－	－	－	－	－	○[注1]
V3AuthPassword	－	－	－	－	－	○[注1]
V3PrivProtocol	－	－	－	－	－	○[注2]

項目名	アカウント種別					
	IPMI	SSH	HTTPS	SNMP		
				V1	V2	V3
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な項目の設定値は、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。



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。



- 検出ノード情報は、同じセッション内でのみ有効です。
- 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スイッチまたはPRIMERGY BX Ethernet Switch/IBP 10Gbit/s 18/8+2 SBAX3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。

検出したノードの登録

手動検出によって検出されたノードを登録する際の操作例を示します。

1. 検出されたノードを確認します。
2. 検出されたノードの中から登録するノードを選択します。[検出ノード登録]ボタンを選択します。
3. ノード名、シャーシ名、Web i/f URL、説明など、登録に必要な情報を入力します。

機器に設定されているIPアドレスを変更するには、IPアドレス欄にある[編集]ボタンを選択して設定します。設定した場合、ノード登録時に機器に対してIPアドレス設定操作が実行されます。

4. ノードのラック搭載位置情報を設定します。
5. ノードグループ情報を設定します。
6. 登録を実行します。

ノードのアカウント情報には、ノード検出時にノードへのアクセスに成功したアカウント情報が登録されます。登録されるアカウントは、[検出ノードリスト]の[成功した通信]カラムに表示されます。

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、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。

<http://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。設定変更項目はありません。

注意

UPnP/Redfishによる自動検出を行うためには、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
PRIMERGYサーバ PRIMEQUEST	SSDP機能
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

- ー 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。

検出したノードの登録

自動検出によって検出されたノードを登録する際の操作例を示します。

1. 検出されたノードを確認します。
2. 検出されたノードの中から登録するノードを選択します。[検出ノード登録]ボタンを選択します。
3. ノード名、シャーシ名、Web i/f URL、説明など、登録に必要な情報を入力します。また、ISMに登録するIPアドレスを指定します。
自動検出機能では、対象機器に設定されているIPv4とIPv6それぞれのIPアドレスが検出される場合があります。ISMに登録するIPアドレスを指定してください。
機器のIPアドレスを変更する場合、設定するIPアドレスバージョンを選択し、[編集]ボタンを選択して設定します。
設定した場合、ノード登録時に機器に対してIPアドレスが設定されます。
4. 通信方法を設定します。
自動検出によって検出されたノードが表示されます。各ノードの通信方法を設定してください。機器のIPアドレスを変更する場合、通信方法の設定が必須です。
5. ノードのラック搭載位置情報を設定します。
6. ノードグループ情報およびタグ情報を設定します。
7. 登録を実行します。



注意

- ー 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。
- ー 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 PRIMEQUEST 3000B	機器がDHCP設定の場合のみ変更できます。機器に固定IPアドレスを設定している場合は、IPアドレスを変更せずに登録を実行してください。
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、登録を実行してください。

- ー 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。

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。

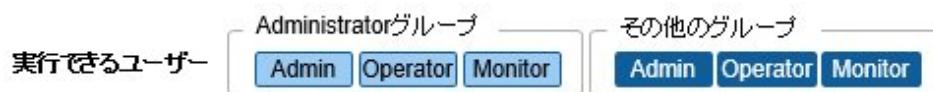
1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. 対象ノード名を選択し、[プロパティ]タブを表示します。
3. [アクション]ボタンから[編集]を選択します。
4. タグ情報を編集します。
5. [適用]を実行し、編集内容を反映します。

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



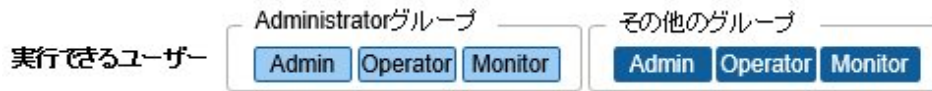
タグを指定してノードをフィルタリングする際の操作例を示します。

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。

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)のWebURLを選択することでWeb画面を表示できます。

- Microsoft Active Directory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 (ISM 2.4.0.b 以降)



管理対象ノード (PRIMERGYサーバのみ) 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。
 - ー 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

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

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

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

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。
5. [適用]を実行し、編集内容を反映します。

2.2.4 データセンター／フロア／ラック／ノードの削除

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

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。

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。

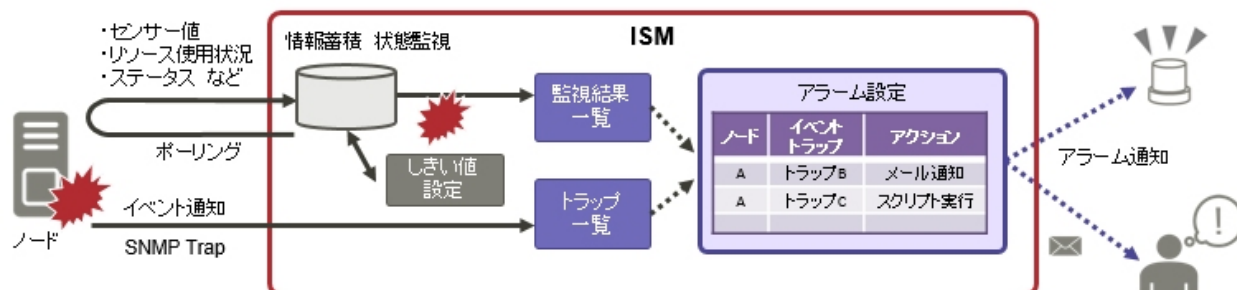
2.3 モニタリング機能

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



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／しきい値の設定
- 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 アラーム設定の登録
- 2.3.5 監視履歴グラフ表示

2.3.1 監視項目／しきい値の設定

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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。
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。

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。
平均消費電力／平均吸気温度	消費電力、吸気温度の3分ごとの平均値を監視します。電力制御機能が有効で、電力制御設定の対象となっているノードのみ監視可能です。

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。

2.3.2 ネットワーク統計情報監視

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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[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

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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。転送の場合、以下の転送タイプを選択できます。 - 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。 - 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「2.6 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 機器により表示形式が異なります。 1Uサーバが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	○	○
\$_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

- 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]-[アラーム]を選択します。

- 画面左側のメニューから[アクション]を選択し、「アクションリスト」画面を表示します。
- 画面右側の[アクション]ボタンから[追加]を選択し、アクションを追加します。

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

実行するスクリプトファイルは、外部ホスト上に配置しておく必要があります。

使用できる外部ホストのOSと実行できるスクリプトファイルは、以下のとおりです。

OS	スクリプトファイル(拡張子)
Windows	バッチファイル (bat)
Red Hat Enterprise Linux	シェルスクリプト (sh)
SUSE Linux Enterprise Server	シェルスクリプト (sh)

- アクション設定に使用するスクリプトファイルを用意します。
- 外部ホストのOSの任意ディレクトリにスクリプトファイルを配置します。
シェルスクリプトの場合は、設定するユーザーに対する実行権限を設定してください。
- 外部ホストのOSに監視対象OSに対する設定と同様の設定を行います。
この設定は、ISMから外部ホストにアクセスし、スクリプトファイルを実行するために必要です。
設定手順については、「[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。



リモートスクリプト実行では、最大実行時間(初期値:300秒)が設定されています。
設定時間内にスクリプト実行が完了しない場合は、スクリプト実行を強制終了します。
スクリプトが正常終了できる時間を設定してください。

メール送信

メール送信するためには、SMTPサーバの情報を登録しておく必要があります。

- 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]-[アラーム]を選択します。
- 画面左側のメニューから[SMTPサーバ]を選択し、「SMTPサーバ設定」画面を表示します。
- 画面右側の[アクション]ボタンから[編集]を選択し、SMTPサーバ情報を登録します。

また、メール送信はS-MIMEによるメッセージの暗号化が可能です。その場合、暗号化に使用するユーザー証明書をISM-VA上にインポートしておく必要があります。

- アクション設定に使用する個人証明書をを用意します。
- ISM-VAに証明書ファイルを転送します。
この際、証明書はPEMエンコード形式である必要があります。
- ISM-VA管理機能から証明書の登録コマンドを実行します。
詳細は、「[アラーム通知メール用証明書登録](#)」を参照してください。

トラップ送信／転送

SNMPトラップを送信／転送する場合、送信／転送先のSNMPマネージャーを登録する必要があります。

- 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]-[アラーム]を選択します。
- 画面左側のメニューから[SNMPマネージャー]を選択し、「SNMPマネージャー設定」画面を表示します。
- 画面右側の[アクション]ボタンから[追加]を選択し、SNMPマネージャー情報を登録します。

アクションのテスト実行手順

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[アラーム]を選択します。
2. 画面左側のメニューから[アクション]を選択します。
「アクションリスト」画面が表示されます。
3. 「アクションリスト」からテストを実行するアクションを選択します。
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。
「アクションテスト」画面を表示されます。
5. 画面右側の[テスト]ボタンを選択し、アクションのテストを実行します。

テスト実行時には、アクション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
\$_ISM	TEST_ISM
\$_TRGID	TEST_TRGID
\$_TRGTYPE	TEST_TRGTYPE
\$_TRG	TEST_TRG
\$_IPA	TEST_IPA
\$_IDN	TEST_IDN
\$_MDL	TEST_MDL
\$_DC	TEST_DC
\$_FLR	TEST_FLR
\$_RACK	TEST_RACK
\$_POS	TEST_POS
\$_MIB	TEST_MIB
\$_SPC	TEST_SPC
\$_TRP	TEST_TRP
\$_SEV	TEST_SEV
\$_EVT	TEST_EVT
\$_MSG	TEST_MSG
\$_TIM	TEST_TIM
\$_TIM2	TEST_TIM2

2.3.4 アラーム設定の登録

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

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

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]-[アラーム]を選択します。
2. 画面左側のメニューから[アラーム]を選択し、「アラームリスト」画面を表示します。

3. 画面右側の[アクション]ボタンから[追加]を選択し、アラームを追加します。

ISM自身のイベント(例: DVDのインポート完了)に関しては、[対象種別]で「システム」を選択してください。

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わります。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。[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。

- 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ます。
- [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。

トラップ受信設定

	Administratorグループ	その他のグループ
実行できるユーザー	☒ Admin ☐ Operator ☐ Monitor	☐ Admin ☐ Operator ☐ Monitor

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

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[トラップ受信]を選択し、「トラップ受信設定リスト」画面を表示します。
3. 画面右側の[アクション]ボタンから[追加]を選択し、トラップ受信設定を追加します。
4. 設定を行うSNMPバージョンを選択し、必要な情報を入力します。

SNMPv3のトラップ受信設定を行う場合、受信対象ノードを選択して、「エンジンID」を設定してください。

ポイント

ノード情報取得を行うことでトラップ受信設定画面に最新の「エンジンID」が表示されます。

注意

- トラップ受信設定の追加／編集／削除を行った場合、変更は即時適用されます。リクエストを受け付けてから反映されるまで、一時的にすべてのSNMPトラップを受信しない状態となります。トラップ受信設定を変更する場合は、上記事象が問題とならないことを確認したうえで行ってください。
- SNMPv3のトラップ受信を行う場合、ノードごとにSNMPトラップ受信設定が必要になります。ノード登録後、SNMPトラップ受信設定を行ってください。
- ノードに設定されている「エンジンID」を変更した場合、ノード情報取得を行い、取得した最新の「エンジンID」を再設定してください。
- 機器によっては、ノード情報取得による「エンジンID」の取得ができません。ノードの設定詳細やノード情報取得による「エンジンID」の取得についての詳細は、「[A.2.2 ノード設定詳細](#)」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。

- ・ 当社外装置から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

- ・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.1.4 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「[4.5 監視履歴をグラフ表示する](#)」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、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、およびその設定可能項目を以下に示します。

表2.1 プロファイル管理機能の対象ノードおよび設定可能項目

ノード種別	対象ノード(例)	設定可能項目
サーバ	PRIMERGY RX PRIMERGY TX PRIMERGY BX PRIMERGY CX	・ BIOS設定 ・ iRMC設定 ・ OSインストール ・ 仮想IO設定
	PRIMEQUEST 2000-Partition	・ MMB設定 ・ OSインストール
	PRIMEQUEST 3000E-Partition	・ MMB設定 ・ OSインストール ・ 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インストール
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 (NetApp)	・ 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 OSインストールの設定](#)
- ・ [2.4.4 仮想IO管理機能](#)
- ・ [2.4.5 プール管理機能](#)
- ・ [2.4.6 ブート情報の確認](#)

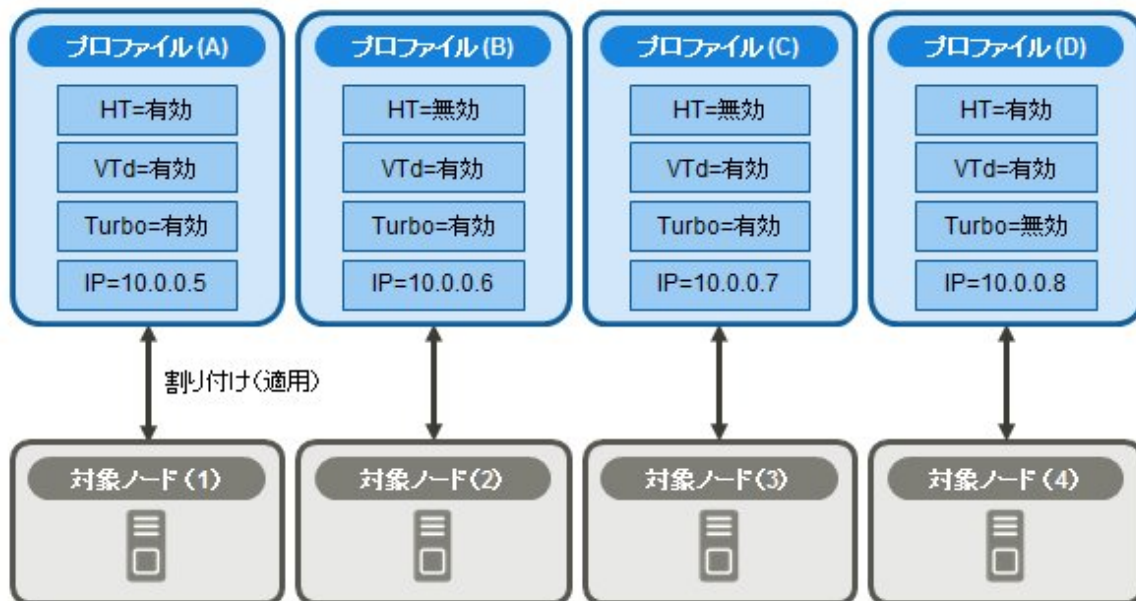
2.4.1 プロファイルの利用方法

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。

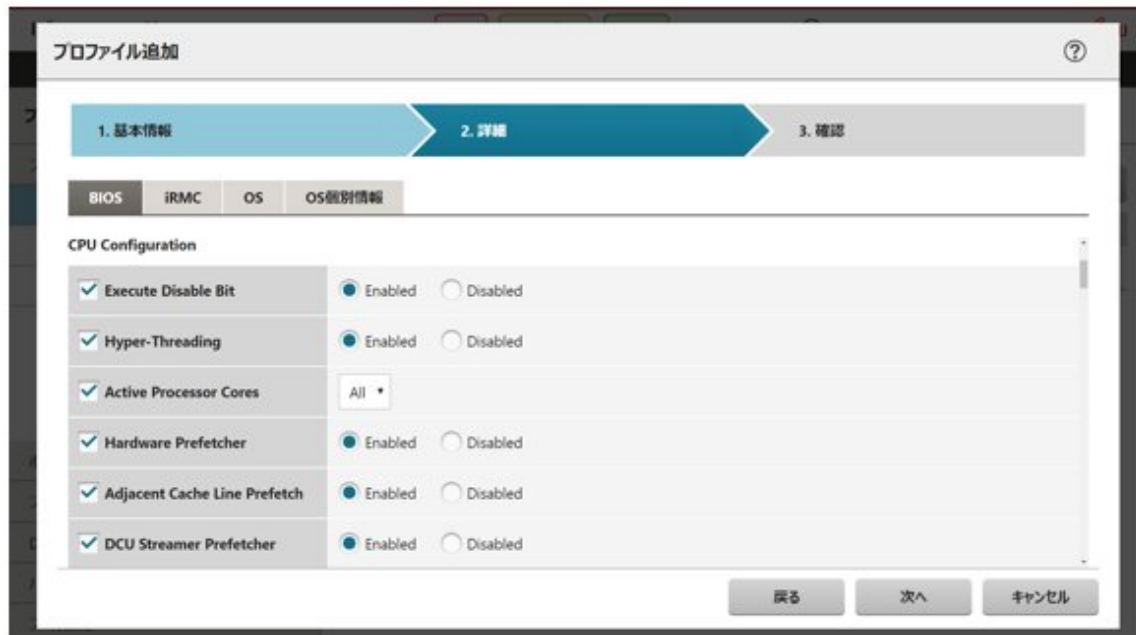
図2.4 プロファイルと管理対象のノードの関係



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2.5 「プロファイル作成」画面例 (GUI)



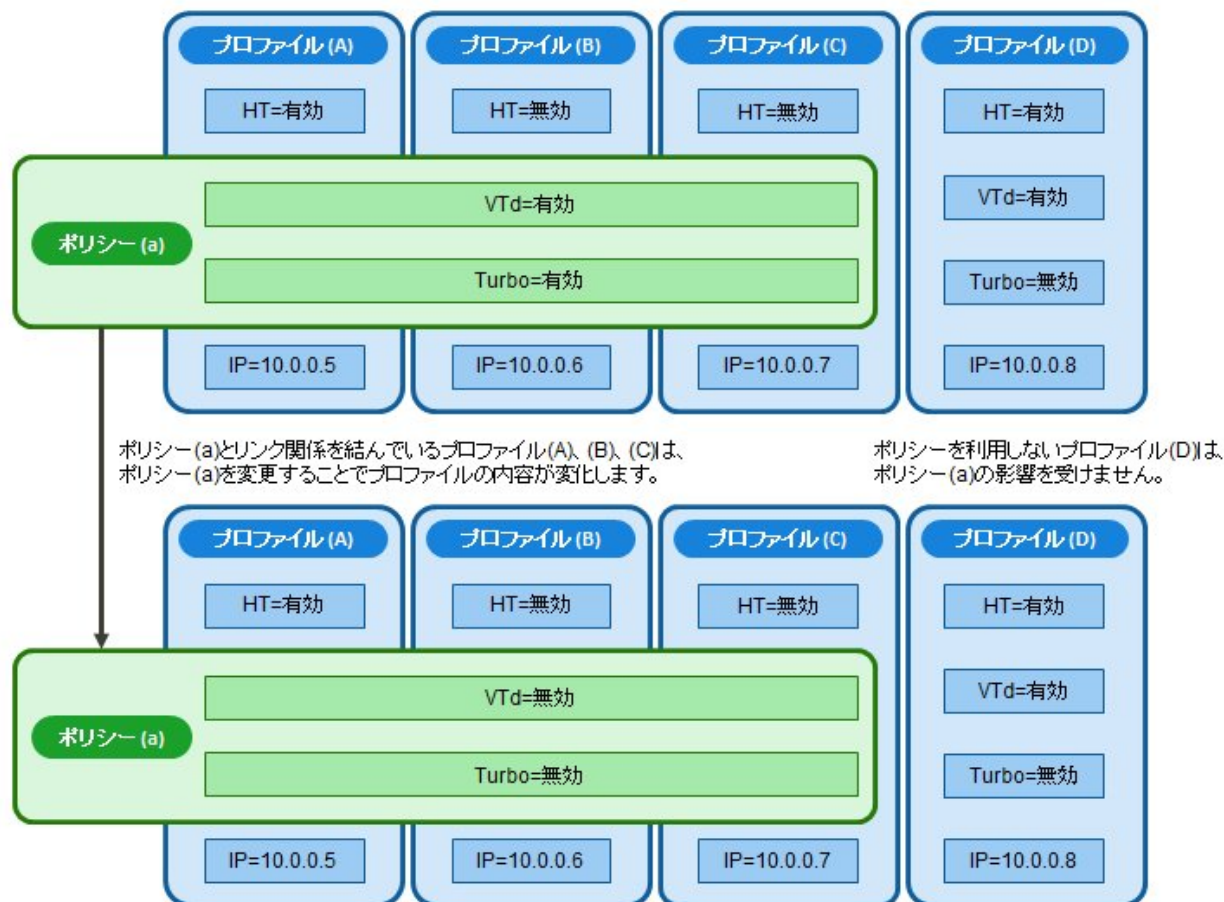
2.4.2 プロファイルとポリシー

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。

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2.6 プロファイルとポリシーの関係



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、サーバに対するOS設定、BIOS設定、iRMC設定、またはMMB設定に利用できます。

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、画面左側のメニューから[ポリシー設定]を選択します。
2. 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

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、画面左側のメニューから[ポリシー設定]を選択します。
2. 画面左側のツリー部からポリシー作成先を選択します。[アクション]ボタンから[ポリシー追加]を選択します。
3. 「ポリシー追加」ウィザードに従い、設定項目を入力します。

ポリシーの設定項目のうち、プロファイルに反映する設定項目は、「ポリシー追加」ウィザードの[2.詳細]で、チェックボックスにチェックを付けたうえで設定値を選択します。チェックボックスにチェックを付けない設定項目は、ポリシーの設定がプロファイルに反映されません。

ポイント

OS設定のポリシーは、対象サーバ種別に依存することなく作成可能です。「ポリシー追加」ウィザードの[1.基本情報]で、「カテゴリー」に「Server-共通」を選択してください(ISM 2.4.0.b以降)。

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

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作成先を選択します。[アクション]ボタンから[プロファイル追加]を選択します。

3. 「プロファイル追加」ウィザードに従い、設定項目を入力します。

プロファイルの設定項目のうち、ノードに反映する設定項目は、「プロファイル追加」ウィザードの[2.詳細]で、チェックボックスにチェックを付けたうえで設定値を選択します。チェックボックスにチェックを付けない設定項目は、プロファイルをノードに適用しても、プロファイルの設定がノードに反映されません。

2.4.2.3 プロファイルの適用

	Administratorグループ	その他のグループ
実行できるユーザー	☒ Admin ☒ Operator ☐ Monitor	☒ Admin ☒ Operator ☐ Monitor



- ・ 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。
- ・ OSインストールを行うためには、事前に必要な設定とファイルの準備が必要です。以下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](#)」

1. プロファイル適用の対象ノードがサーバの場合は、プロファイル適用前にサーバの電源をオフにします。サーバ以外の場合は、電源をオンにします。
2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
3. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。
4. プロファイル適用対象ノードにチェックを付けます。[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、「[2.13.4 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

	Administratorグループ	その他のグループ
実行できるユーザー	☒ Admin ☒ Operator ☐ Monitor	☒ Admin ☒ Operator ☐ Monitor

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. 画面左側のツリー部からプロファイル編集先を選択して、右側の一覧からプロファイルを選択します。
3. [アクション]ボタンから[編集]を選択し、プロファイルを編集します。
4. プロファイル適用の対象ノードがサーバの場合は、プロファイル適用前にサーバの電源をオフにします。サーバ以外の場合は、電源をオンにします。
5. 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。

6. 「ノードリスト」画面の[カラム表示]欄で[プロファイル]を選択します。
7. 対象のノードを選択し、[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。

ノード設定とプロファイルの一致確認

1. ISMのGUIでグローバルナビゲーションメニューから[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[プロファイル]を選択します。
ノードの設定とプロファイルが不一致となっているノードは、[ステータス]に[要再適用]と表示されます。
ノードの設定とプロファイルが一致しているノードは、[ステータス]に[適用済]と表示されます。
ノードの設定とサーバのOSの設定のプロファイルのみ不一致となっているノードは、[ステータス]に[適用済み(差分あり)]と表示されます。



- プロファイル管理機能を使用せずに直接ノードの設定を変更した場合、ISM画面に表示される適用済みプロファイルの内容とノードの状態が不一致となります。
- [ステータス]が[適用済み(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



以下の場合に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、「[2.13.1 ユーザー管理機能](#)」を参照してください。

プロファイルの適用解除

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[プロファイル]を選択します。
3. プロファイル適用済みノードにチェックを付け、[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

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削除先を選択して、右側の一覧からプロファイルを選択します。
3. [アクション]ボタンから[削除]を選択します。
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



プロファイルを別のISMで流用したい場合や、適用したプロファイルをISM外(管理端末)に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. エクスポート対象のプロファイルを選択します。
3. [アクション]ボタンから[エクスポート]を選択します。
4. 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。
 - ー 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。
 - ー FTP
ISM-VAのFTPサーバ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、任意の暗号化キーを指定することが必須となっています。
-

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、画面左側のメニューから[ポリシー設定]を選択します。
2. 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。
3. [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、画面左側のメニューから[ポリシー設定]を選択します。
2. 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。
3. [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

通常、プロファイルは新規でノードに適用するか、適用済みの状態でプロファイルを変更したあとに再適用します。ただし、適用／再適用のGUI操作途中に、「プロファイル適用」画面で[高度な設定を有効にする]にチェックを付けることで、プロファイル適用時の動作条件(適用モード)を変更できます。また、サーバの場合は、適用する範囲を機能グループ(BIOS、iRMC、MMB、OS、仮想IO)ごとに指定できます。

指定可能な動作条件(適用モード)は、以下のとおりです。

- ・「変更がない箇所にも適用を行う」

プロファイル適用状態で、ノードとプロファイル内容が一致している場合でも、ノードに対して設定を上書きします。
ただし、OSは再適用できません。

- ・「電源オン状態でプロファイルを適用する」

サーバにプロファイルを適用する場合、通常は対象ノードの電源をオフにした状態で適用を行う必要がありますが、本動作を選択すると、対象ノードが電源オンの状態でもプロファイル適用が可能です。

以下の点に注意してください。

- BIOS設定、iRMC設定、MMB設定の一部はサーバを再起動するまで変更が反映されません。
プロファイル適用が完了したあと、任意のタイミングで再起動してください。
 - OS設定または仮想IO設定が適用対象の場合は、本モードは選択できません。
 - iRMC S5を搭載したサーバの場合は、本モードでBIOS設定のプロファイルを適用できません。
 - iRMC S4を搭載したサーバでiRMCファームウェアバージョンが9.xxF以降の場合は、本モードでBIOS設定のプロファイルを適用できません。本モードでBIOS設定のプロファイルを適用したい場合、iRMCファームウェアバージョンを8.xxFにしてください。
- ・「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」
- ISMの管理上はプロファイル適用を完了させますが、ノードに対する変更は行いません。そのため、適用後にノードの状態とISM管理状態に差異が発生する場合があります。

2.4.3 OSインストールの設定

OSインストール時に必要な準備作業

- ・ 事前にOSインストール媒体およびServerView Suite 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。
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。
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、「[2.13.2 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ブート機能を利用します。管理LANからPXEブートが可能のように、ネットワーク接続および対象サーバの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インストールの注意事項

ネットワーク環境や対象サーバの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

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ディレクトリ配下にスクリプト用の任意のディレクトリを作成し、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と実行するスクリプトファイル名を指定します。

2.4.4 仮想IO管理機能

仮想IO管理機能は、LAN、FC (Fibre Channel) のI/Oパラメーター (MACとWWN) を仮想化する機能です。

- ・ LANコントローラーのMACアドレスの代わりに仮想MACアドレスを使用できます。
- ・ FCコントローラーのWWNの代わりに仮想WWNを使用できます。

- ・ 仮想MACアドレス、仮想WWN、ネットワーク経路の割当て、およびネットワークブートのI/Oパラメーターをプロファイルとして保持できます。

ポイント

仮想MACアドレスや仮想WWNは、ISMで管理するノード全体またはノードグループ単位に一意である必要があります。このため、仮想MACアドレスや仮想WWNなどの仮想IOを設定したプロファイルは、複数のノードに適用できません。

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 3000Eパーティションの場合、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 3000Eパーティションの場合、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。各設定方法については、以下の参照先を確認してください。

<http://www.fujitsu.com/jp/products/computing/servers/primequest/products/3000/catalog/manual/3000/>

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 3000Eパーティションの場合、BIOSのCSM設定を無効にしてください。
- ・ PRIMEQUEST 3000Eパーティションの場合、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 3000Eパーティションの場合、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。

MACアドレス、WWNの仮想化

サーバの仮想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、プロファイルを適用することによって仮想IO管理機能を使用可能にします。管理対象サーバや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管理機能を使用した管理対象サーバ、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2.7 仮想IO管理機能を使用した管理対象サーバの交換

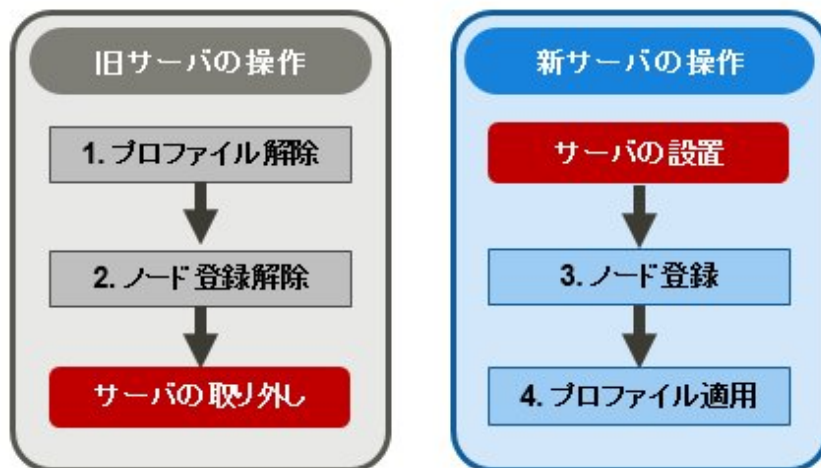
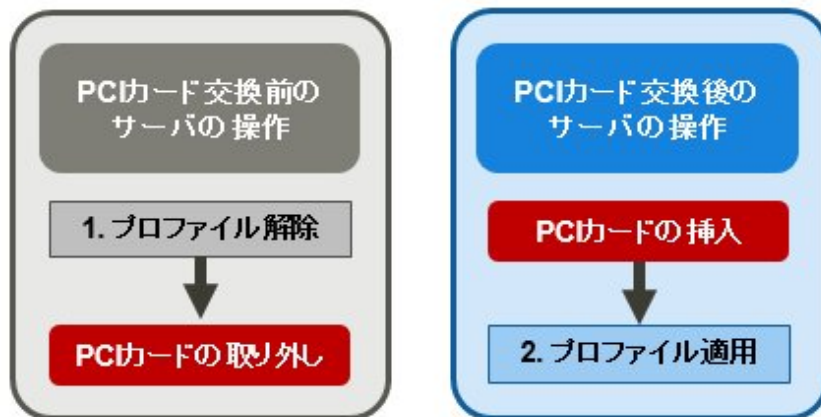


図2.8 仮想IO管理機能を使用したPCIカードの交換



仮想IOのiRMC AC電源OFFリカバリ

iRMCの電力が喪失(すべての電源ケーブルの切断、またはデータセンターでの電力喪失)したとき、iRMCは仮想IO設定を失います。AC電源が復帰し、iRMCが再びブートされたとき、仮想IO設定を再適用します。

仮想IOのiRMC AC電源OFFリカバリに必要な準備作業

事前にサーバのSNMPトラップ送信先にISMのIPアドレスを設定しておく必要があります。

注意

- この処理が動作するには、ISMとiRMCがアクセス可能であることが必要です。
- 仮想IOのiRMC AC電源OFFリカバリは、PRIMERGYの場合のみ有効です。

PRIMEQUEST 3000E パーティションの場合は、装置側のパーティションのiRMCアカウントを再設定してから、手動でプロファイルを再適用してください。

ポイント

iRMCは、ISMから仮想IO設定の再適用が完了するまでの一定時間、仮想IO設定の再適用を促すSNMPトラップを定期的にISMに送信します。この処理は、iRMCユーザーインターフェースまたはBIOSインターフェースで仮想IOの管理状態を無効にすることで中断できます。

仮想IOの再設定に成功した場合でも、エラーメッセージが出力されることがあります。仮想IOの再設定がされているか、確認してください。

リカバリ機能による再適用が実施されない場合は、プロファイルの再適用を実施してください。

2.4.5 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管理機能において、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。

ー プールタイプ

設定するプールの種類を選択します。

ー 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。

ー 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

	Administratorグループ	その他のグループ
実行できるユーザー	Admin Operator Monitor	Admin Operator Monitor

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

	Administratorグループ	その他のグループ
実行できるユーザー	Admin Operator Monitor	Admin Operator Monitor

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。



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

	Administratorグループ	その他のグループ
実行できるユーザー	Admin Operator Monitor	Admin Operator Monitor

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。

2.4.6 ブート情報の確認

	Administratorグループ	その他のグループ
実行できるユーザー	Admin Operator Monitor	Admin Operator Monitor

仮想IO管理機能で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。

2.5 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。

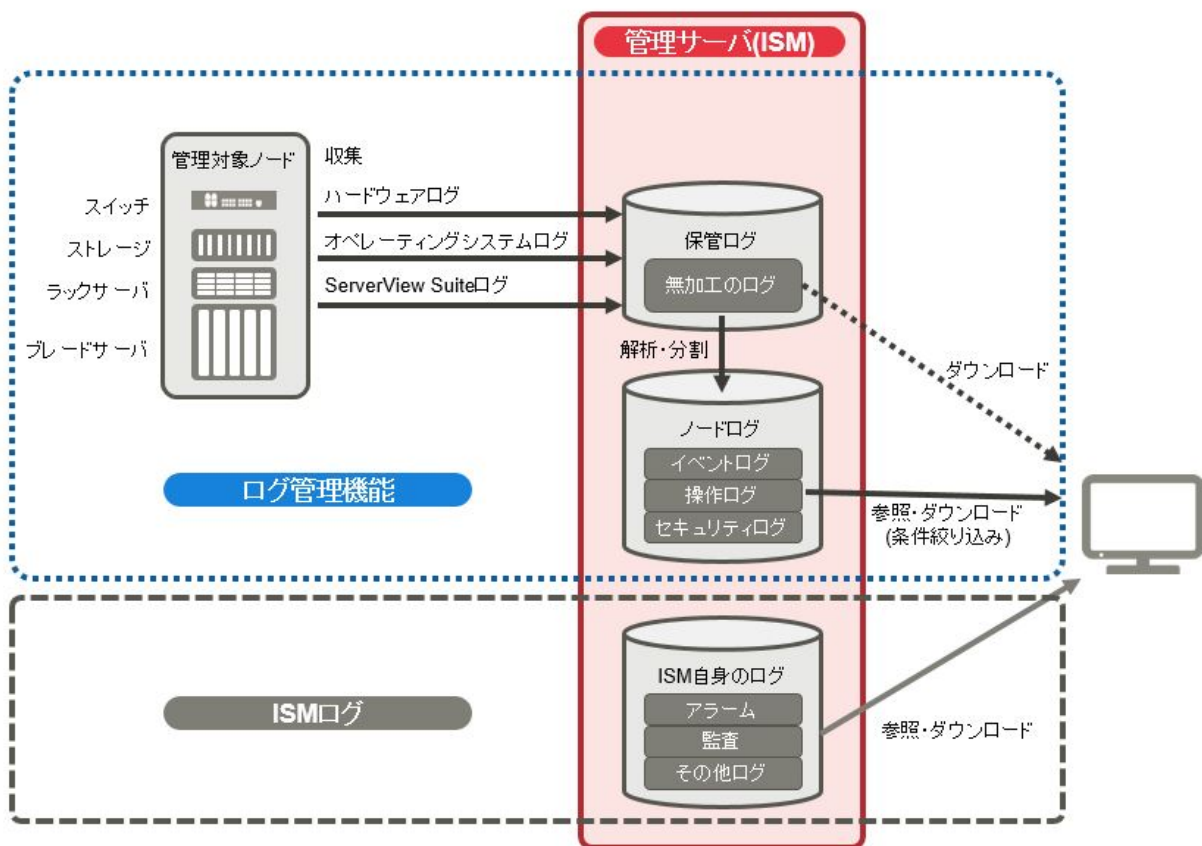
その設定に従ってノードから収集したログデータのひとかたまりを「保管ログ」と呼びます。

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2.9 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](#)
- [2.5.2 ログ保有期間の設定](#)
- [2.5.3 ログ収集対象と収集日時の設定](#)
- [2.5.4 ログ収集の動作](#)
- [2.5.5 ノードログの検索](#)
- [2.5.6 ノードログのダウンロード](#)
- [2.5.7 保管ログのダウンロード](#)
- [2.5.8 ノードログの削除](#)
- [2.5.9 保管ログの削除](#)

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。

<http://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	PRIMERGY (CX1430 M1、GX2580 M5 (ISM 2.4.0.c 以降)を除く)	SEL System Report (iRMC S4以降を搭載したサーバ)	SEL
	PRIMEQUEST 3000B		
	IPCOM VX2		
	PRIMERGY CX1430 M1、PRIMERGY GX2580 M5 (ISM 2.4.0.c 以降)	SEL (バイナリ)	なし
シャーシ	PRIMERGY BX	show Log/MgmtBlade LogMgmtBladeAllコマンドの出力結果 set SystemInfo/Dump Started=trueコマンドの出力結果	show Log/MgmtBlade LogMgmtBladeAll コマンドの出力結果
	PRIMEQUEST 3000E	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 /mroot/etc/logディレクトリ配下の各種 ファイル	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
コネクション ブレード	Ethernet Switch	show tech-supportコマンドの出力結果	show logging buffered、または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)
	Fibre Channel Switch	supportshowコマンドの出力結果 supportsaveコマンドで作成される各種ファイル	supportshowコマンドの出力結果
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		
	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)

オペレーティングシステムログ

管理対象サーバ上で動作している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	—



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

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

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

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

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「毎週〇曜日の〇時〇分」のように指定します。また、「毎月の第△〇曜日の〇時〇分」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。
 - ー 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。
 - ー 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。

- ー 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)
- ー 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。

- ・ 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「2.7.2 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。 「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。 - ー 保管ログの場合

条件	動作
	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 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)保存領域が設定容量(xxMB)に達しました。 「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

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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. [フィルター]ボタンを選択します。
4. 「フィルター」画面で条件を入力し、[フィルター]ボタンを選択します。
入力した条件に合致したログが表示されます。

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

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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>¥<ログ種別>

<カテゴリ>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。

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]-[保管ログ]タブを選択します。
3. ダウンロードする保管ログ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。

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ダウンロード操作が行えます。この場合は、ダウンロードするファイルにチェックを付けます。

5. ダウンロード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 Archive 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

- ・ 保管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や、複数の保管ログ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

- ・ 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

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
- ・ 管理対象ノードのファームウェアをアップデート
- ・ 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

ファームウェア管理機能の対象ノードは以下のとおりです。

- ・ サーバおよび搭載される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。

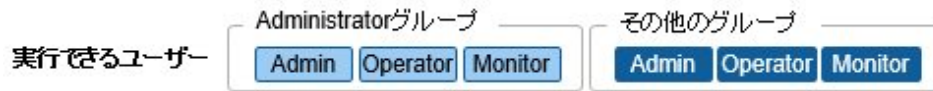
<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/>

ここでは、以下について説明します。

- ・ [2.6.1 ノードのファームウェアバージョンの確認](#)

- [2.6.2 ファームウェアのアップデート](#)
- [2.6.3 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](#)
- [2.6.4 ジョブ管理](#)
- [2.6.5 ファームウェアベースライン](#)

2.6.1 ノードの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]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 ファームウェアのアップデート

以下について説明します。

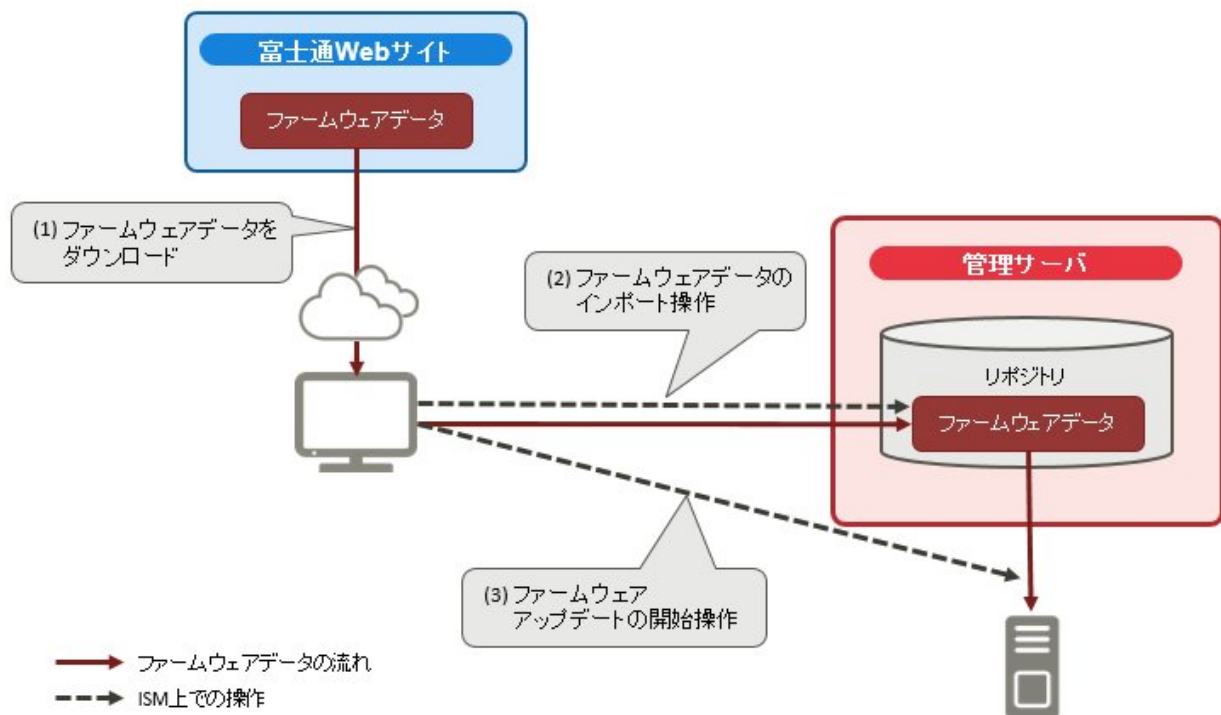
- [2.6.2.1 ファームウェアアップデート方法](#)
- [2.6.2.2 アップデート時の動作](#)
- [2.6.2.4 ファームウェアアップデートの実施](#)

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富士通の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は、「[2.13.2 リポジトリ管理機能](#)」を参照してください。

図2.10 ファームウェア管理機能のイメージ



2.6.2.1 ファームウェアアップデート方法

ファームウェア管理機能では、「Onlineアップデート」と「Offlineアップデート」の2種類のファームウェアアップデート方法が使用できます。

Onlineアップデート

ファームウェアアップデートを行う装置の電源がオンの状態で行うアップデート方法です。サーバの場合は、電源がオフの状態でもOnlineアップデートを実行できます。

ファームウェアアップデートの対象がサーバ(BIOS/iRMC/搭載PCIカード/PRIMEQUEST本体ファームウェア)、スイッチ、ストレージ、PRIMERGY BXシャーシ(MMB)の場合に使用できます。

Offlineアップデート

ファームウェアアップデートを行う装置の電源がオフの状態で行うアップデート方法です。

ファームウェアアップデートの対象がサーバ(BIOS/iRMC/搭載PCIカード/PRIMEQUEST本体ファームウェア)の場合に使用できます。

Offlineアップデートを行う際は、事前にサーバの電源をオフにしてください。

Offlineアップデートに必要な準備作業

サーバ(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 DVDおよび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。

ServerView Suite DVDのISOイメージをインポートする場合は、システムのLVMボリュームサイズを拡張してください。ServerView Suite DVDのISOイメージをISM上に一度インポートしている場合、再度インポートする必要はありません(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、「[2.13.2 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]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。



「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、機器によっ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。

<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/>

2.6.2.2 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2.2 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 (iRMC)	サーバの電源がオン／オフどちらの状態でもアップデートが可能です。
サーバ (BIOS)	サーバの電源がオン／オフどちらの状態でもアップデートが可能です。 - 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 (PRIMEQUEST本体ファームウェア)	サーバの電源がオンの状態でアップデートが可能です。
サーバ (搭載PCIカード)	サーバで、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、PY CB Eth Switch 10/40Gb 18/8+2以外)	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。

種別	アップデート時およびアップデート後の動作
ストレージ	
スイッチ (CFX、PY CB Eth Switch 10/40Gb 18/8+2)	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。
PRIMERGY BXシャーシ (MMB)	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。

表2.3 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 (iRMC)	サーバの電源がオフの状態でアップデートが可能です。
サーバ (BIOS)	ファームウェアアップデート中はサーバ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。アップデート設定の画面で「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。
サーバ (搭載PCIカード)	
サーバ (PRIMEQUEST本体ファームウェア)	サーバの電源がオフの状態でアップデートが可能です。 ファームウェアアップデート中はサーバ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。

2.6.2.3 アップデート時のスクリプト実行 (ISM 2.4.0.b 以降)

対象ノードのファームウェア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	ファームウェアアップデート対象ノードのノードID
\$_TRG	ファームウェアアップデート対象ノードのノード名
\$_IPA	ファームウェアアップデート対象ノードのIPアドレス
\$_MDL	ファームウェアアップデート対象ノードのモデル名
\$_OSIP	ファームウェアアップデート対象ノードのOSのIPアドレス
\$_OSTYPE	ファームウェア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

ファームウェア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時に必要な準備作業

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]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

- ・ファームウェア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の実行からファームウェア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、ファームウェア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。
- ・ファームウェアアップデートのスクリプト設定画面で「ファームウェア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、ファームウェア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るても、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ファームウェア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]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

2.6.2.4 ファームウェアアップデートの実施



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。
 - － 管理サーバを再起動しない。管理サーバ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、「[2.13.2 リポジトリ管理機能](#)」を参照してください。
- ・ 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。
- ・ ETERNUS DX/AFのファームウェアアップデートを行う際は、Maintainerのロールを持つアカウント情報がISMに登録されている必要があります。
- ・ 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のOS情報がISMに登録されている必要があります。
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。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
- ・ サーバに搭載される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、「[2.13.3 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、現行バージョン欄と最新バージョン欄に表示されるバージョンのフォーマットが異なります。
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。
<http://software.fujitsu.com/jp/serverviewism/environment/>
- ・ Ciscoスイッチ(Catalyst, Nexus)は、現行バージョンと最新バージョンの比較を行いません。
現行バージョンと最新バージョンの値が異なる場合、アップデート対象となります。

- 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。
- Onlineアップデートを使用したサーバ搭載のPCIカードおよびサーバの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。

- サーバ搭載の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。
- 電源オンの状態でサーバの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。
- 電源オフの状態でサーバの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。

- 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。

-
- 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]を選択します。
 - 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。
ノード名を選択し、[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。
 - アップデートを行うノードの「現行バージョン」と「最新バージョン」を確認します。
 - 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[ファームウェア更新]を選択します。
 - 画面表示に従い、操作を実行します。
 - 日時を指定してファームウェアアップデートする場合
[ファームウェア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[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。
 - [ファームウェアアップデートをすぐに開始する]を選択して実行した場合
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。
 - 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行えます。
 - 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]を選択します。
 - 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]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]タブを選択します。
- 日時を指定してファームウェアアップデートするには、事前にworkflowサービスを起動しておく必要があります。「[4.11 ISM-VAサービス制御](#)」を参照して、「内部サービス個別有効化設定」および「内部サービス個別起動」を行ってください。
- アップデート設定の画面で「ファームウェア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、ファームウェア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。日時を指定してファームウェアアップデートする場合に利用してください。

2.6.3 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サーバから、対象サーバのiRMC Webインターフェー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

- 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]を選択します。
- 画面左側のメニューから[アップデート]を選択します。
- ドキュメントを確認したいノードの[現行バージョン]欄、または[最新バージョン]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。
- [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。

- 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。
- ノードリストで対象の[ノード名]を選択し、[ファームウェア]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

- 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]を選択します。
- 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。
- 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]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。
 - ー ノードリストの[カラム表示]から[ファームウェア]を選択します。
 - ー 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]タブを選択します。
 3. [アクション]ボタンから[ファームウェア更新]を選択します。
- 以降の手順は上記と同様です。
-

2.6.4 ジョブ管理

日時を指定してファームウェア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。

.....

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。

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。

<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serveviewism/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
- 2.6.5.2 ファームウェアベースライン定義の割当て
- 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
- 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
- 2.6.5.5 ファームウェアベースライン定義の編集
- 2.6.5.6 ファームウェアベースライン定義の削除

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、2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

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]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。

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]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。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を利用して作成することを推奨します。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。
- ・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、「[2.13.2.1 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。

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]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

- ・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]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。

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]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]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]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

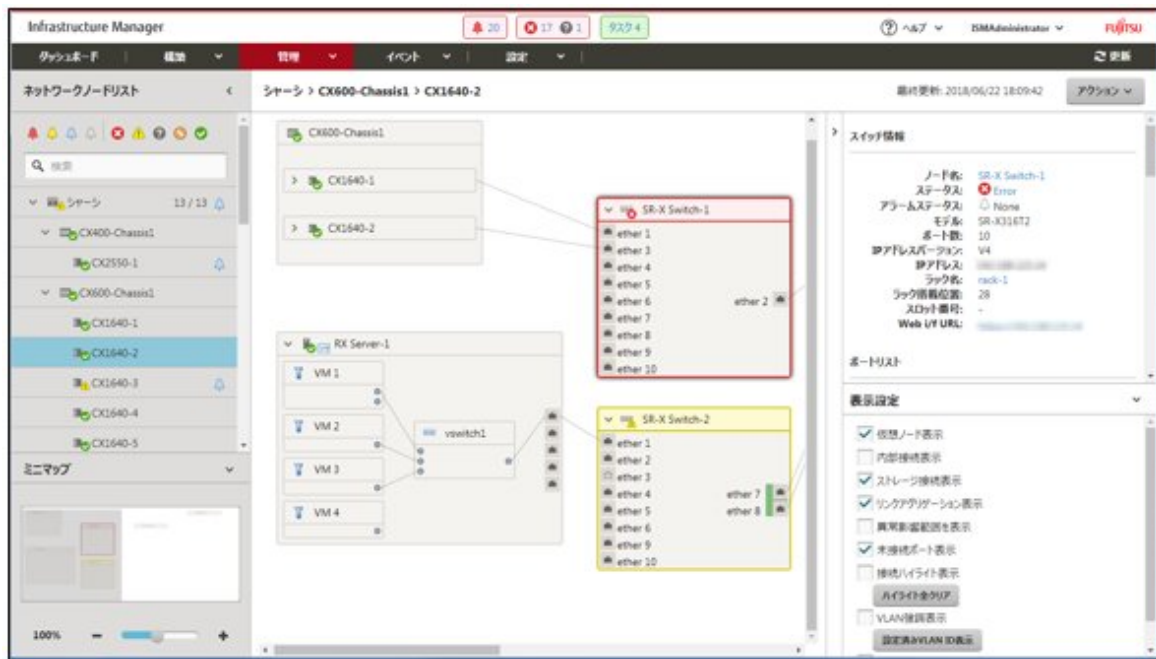
ファームウェアベースライン定義を削除すると、ファームウェアベースライン定義の割当てが解除されます。

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

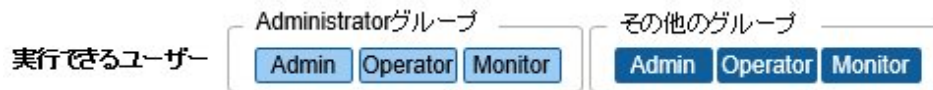
図2.11 ネットワークマップ



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、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、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。

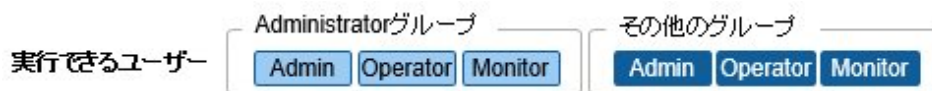
ポイント

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。

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「[2.13.6 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。

- 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。
- [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。
- [ネットワーク管理情報の取得]ボタンを選択します。

注意

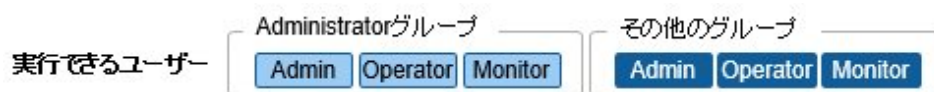
ネットワーク管理情報の更新中に、ネットワーク接続情報の取得および各ノードへの設定はできません。情報更新の完了後に操作してください。

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が表示されます。

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



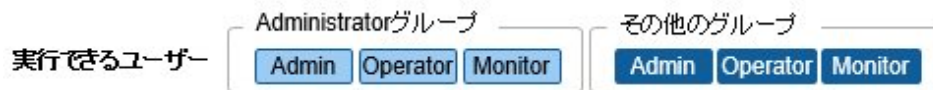
ネットワークスイッチのポートの各種統計情報(トラフィックなど)をネットワークマップ上で視覚的に確認できます。

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。

ー 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。

ー 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

	Administratorグループ	その他のグループ
実行できるユーザー	☒ Admin ☒ Operator ☐ Monitor	☒ Admin ☒ Operator ☐ Monitor

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、「[2.13.4 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よっ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よって予約済みの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

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

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よっ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よって設定可能な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マ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。マルチシャーマ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。
- ・ マルチシャーマ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よって異なります。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

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

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

ラックに搭載した機器に対して、設定した消費電力の上限値に抑えるように電力制御を行います。

事前に、ラックに対して、ノードごとの制御情報と電力制御ポリシーの設定情報を登録し、電力制御ポリシーを有効化することで電力制御の運用を開始します。

ポイント

電力制御ポリシーは、以下の4種類があります。

- ・ カスタム1、カスタム2
通常運用の電力制御ポリシーです。2種類を切り替えて運用できます。
- ・ スケジュール
指定した曜日／時間帯だけ有効となるポリシーです。
- ・ ミニマム
消費電力が最小限となるように制御します。

注意

ISM for PRIMEFLEXでは、電力制御機能は使用できません。

2.8.1 電力制御設定の追加／編集

	Administratorグループ	その他のグループ
実行できるユーザー	☒ Admin ☐ Operator ☐ Monitor	☐ Admin ☐ Operator ☐ Monitor

ノード電力設定

ノードごとの電力情報、業務の優先度を設定します。

業務の優先度の低いノードから電力制御が実行されます。

消費電力値が取得可能な機器の場合、電力制御ステータスが[電力制御停止中]または[電力制御中]の状態で、現在の消費電力値を確認できます。

電力制御ができないノードの場合、最大消費電力の値を固定値として換算します。

電力制御ポリシー

ポリシーごとの消費電力の上限値を設定します。

スケジュールポリシーについては、運用スケジュールを設定します。

2.8.2 電力制御の有効／無効

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

電力制御ポリシーの有効、無効を切り替えます。

ポイント

それぞれの電力制御ポリシーは、独立して有効化できますが、ミニマムが設定されている場合、ミニマムを最優先で実行します。ミニマム以外のポリシーが複数有効化された場合、消費電力の上限値が最も低いポリシーを実行します。

注意

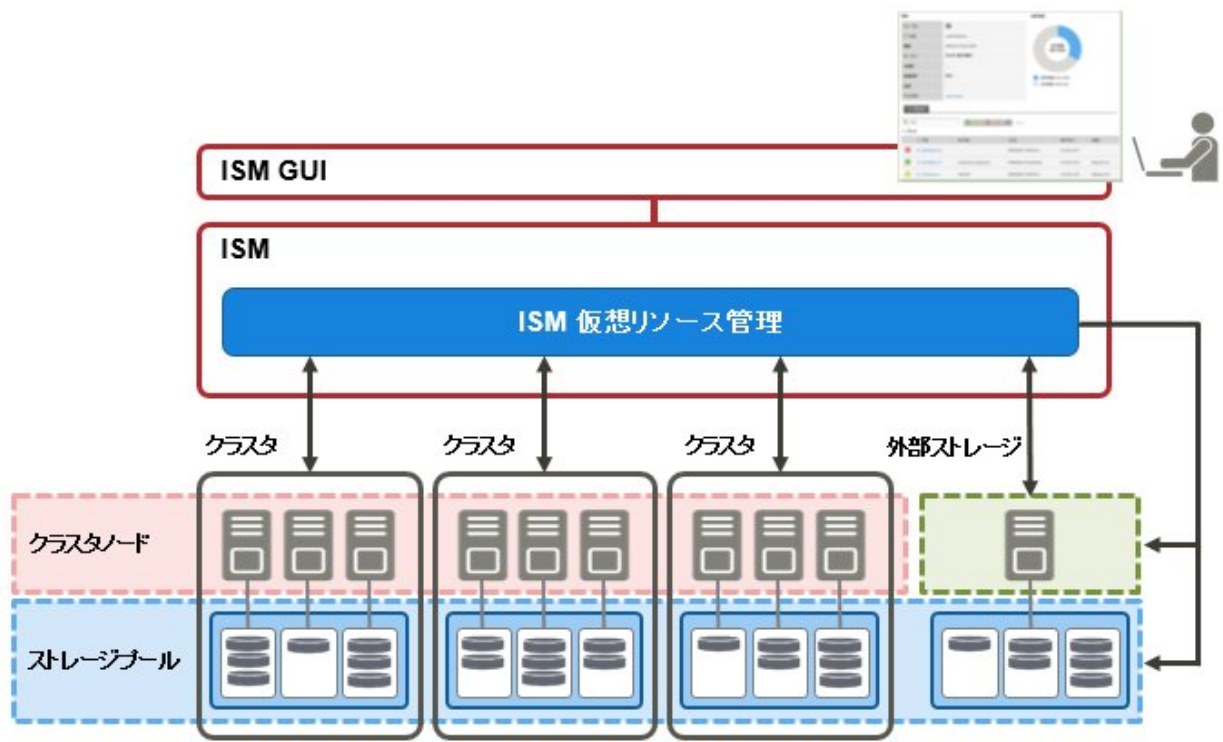
- 電力制御設定を実施済みのラックに対してノードを追加した場合、そのラックの電力制御設定を変更する必要があります。設定を変更しない場合、ラック当たりの消費電力が設定した上限値より大きくなります。
ノードを削除した場合も、そのラックの電力制御設定の上限値を見直すことを推奨します。
ノードを移動した場合は、移動前と移動後のラックそれぞれに対して対処を行う必要があります。
- 上限値は電力制御目標の値です。通常、上限値よりも消費電力が低くなるよう余裕をもって制御を実施します。ただし、上限値が低く設定されている場合は消費電力を超過することもあります。
- PRIMERGY RX／TX S7シリーズをご使用の場合は、ポリシーの上限値に対して、PRIMERGY RX／TX S7シリーズの最小電力値を合計した値よりも大きい数値を指定してください。
機器の最小電力値は、iRMC Webインターフェースの[電力制御]-[現在の消費電力]-[現在の全体消費電力]欄で確認できます。
- ISM-VAの日付／時間を過去の日時に変更すると、「ラック詳細」画面の[ラック情報]に表示される消費電力の値、およびノードの詳細画面の[監視]タブに表示される平均消費電力、平均吸気温度の値が正しく表示されなくなります。
ISM-VAの日付／時間が変更した時刻を経過すると正しく表示されるようになります。

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2.12 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、「[A.1.2 仮想リソース管理機能の事前設定](#)」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、以下のとおりです。

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、以下のとおりです。

凡例：○＝サポート対象、－＝サポート対象外

ソフトウェア環境 (SDS)			ハイパーバイザー	仮想化管理ソフトウェア	サポート有無
VMware vSAN	5.x		VMware ESXi 5.x	vCenter Server Appliance 5.x	－
	6.x	6.2	VMware ESXi 6.0 Update2	vCenter Server Appliance 6.0 Update2	○
		6.5	VMware ESXi 6.5	vCenter Server Appliance 6.5	○
		6.6	VMware ESXi 6.5[注1]	vCenter Server Appliance 6.5[注1]	○
		6.6.1	VMware ESXi 6.5 Update1	vCenter Server Appliance 6.5 Update1	○
		6.6.1 U2	VMware ESXi 6.5 Update2	vCenter Server Appliance 6.5 Update2	○
		6.7	VMware ESXi 6.7	vCenter Server Appliance 6.7	○
		上記以外			－
Microsoft Storage Spaces		Windows Server 2012 Hyper-V	Microsoft Failover Cluster	－	

ソフトウェア環境 (SDS)	ハイパーバイザー	仮想化管理ソフトウェア	サポート有無
		Microsoft System Center 2012	—
Microsoft Storage Spaces Direct	Windows Server 2016 Hyper-V	Microsoft Failover Cluster	○
		Microsoft System Center 2016	—
	Windows Server 2019 Hyper-V	Microsoft Failover Cluster	○
		Microsoft System Center 2019	—

[注1]: VMware vSAN 6.6は、VMware ESXi 6.5d以上、およびvCenter Server Appliance 6.5d以上が必要です。



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、「[A.1.2 仮想リソース管理機能の事前設定](#)」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機器の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。

<http://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。

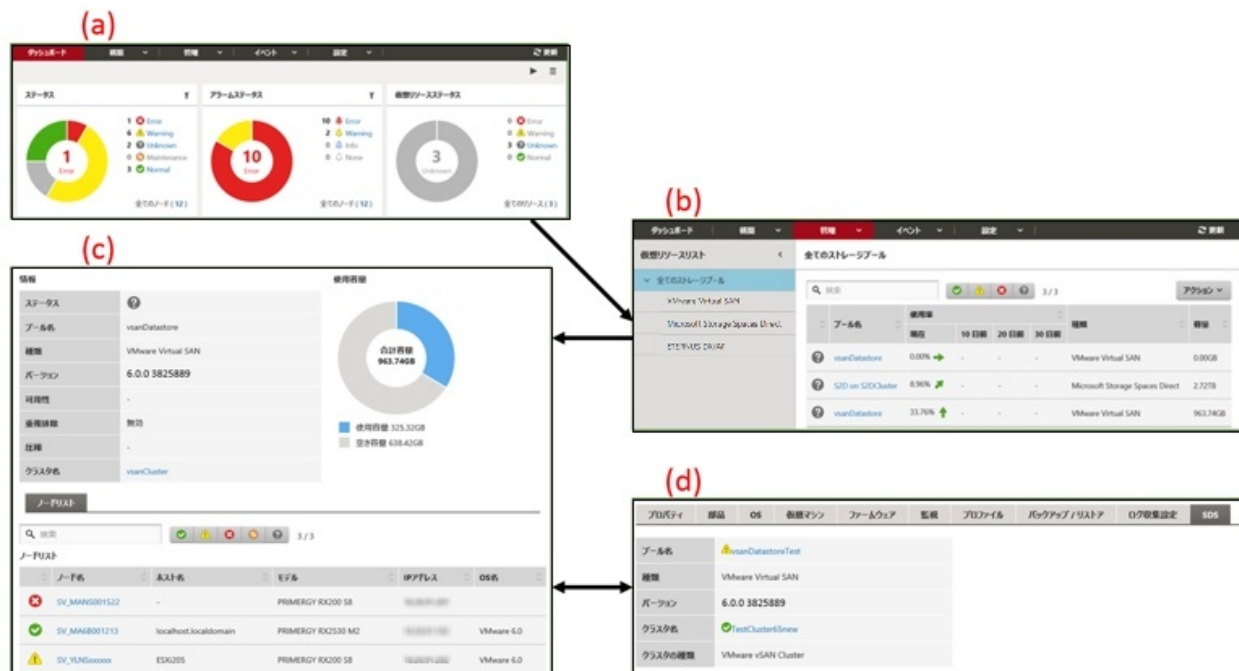
シン・プロビジョニングプールの参照および管理については、ETERNUS Web GUIを使用してください。

2.9.2 仮想リソース管理GUI

仮想リソース管理機能は、管理GUIを備えています。

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2.13 仮想リソース管理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、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

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

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>

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。

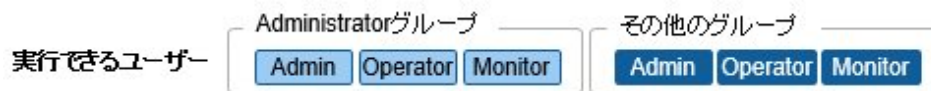
- ・ [2.9.3.1 ストレージプールの使用状況の監視](#)
- ・ [2.9.3.2 ストレージプールの異常の特定](#)
- ・ [2.9.3.3 仮想リソース情報の更新](#)

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、「[2.13.6 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。
－ 「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。

仮想リソースリスト					
ステータス	プール名	種類	容量	使用率	
✓	vSANDatastore-1	VMware Virtual SAN	22.01TB	57.32%	
⚠	vSANDatastore-2	VMware Virtual SAN	13.96TB	21.92%	
✓	StoragePool-1	Microsoft Storage Spaces Direct	11.23TB	19.87%	
✗	vSANDatastore-3	VMware Virtual SAN	2.82TB	91.92%	
✓	raidgrp-1	ETERNUS DX	27.38TB	71.31%	

- － 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。

全てのストレージプール							
検索		5 / 5				アクション	
プール名	使用率	現在	10 日前	20 日前	30 日前	種類	容量
✓ vSANDatastore-1	57.32%	→	55.02%	50.01%	49.02%	VMware Virtual SAN	22.01TB
⚠ vSANDatastore-2	21.92%	↗	15.11%	11.23%	9.83%	VMware Virtual SAN	13.96TB
✓ StoragePool-1	19.87%	→	16.02%	8.02%	-	Microsoft Storage Spaces Direct	11.23TB
✗ vSANDatastore-3	91.92%	↑	-	-	-	VMware Virtual SAN	2.82TB
✓ raidgrp-1	71.31%	↗	63.31%	58.99%	56.00%	ETERNUS DX	27.38TB

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。

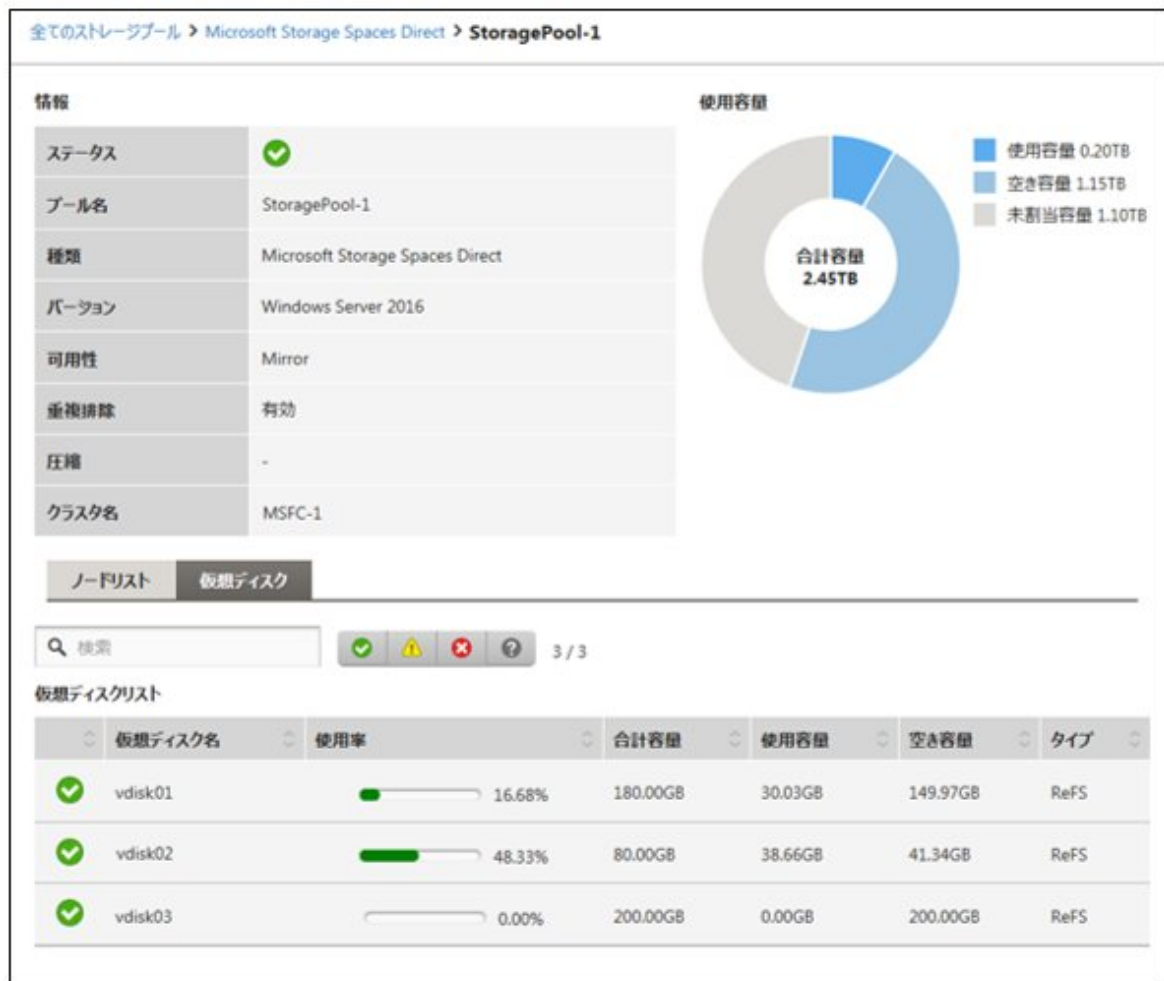
横向き: 使用率が横ばい、微増(使用率が5%未満の増加)、または減少

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。

- 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。
- 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。
- 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。

- 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。

ノードヘ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。

- 一 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



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。

プール名	使用率				種類	容量
	現在	10 日前	20 日前	30 日前		
vsanData	0.00% →	-	-	-	VMware Virtual SAN	0.00GB
S2D on S2DC	8.96% ↗	-	-	-	Microsoft Storage Spaces Direct	2.72TB
vsanDi	33.76% ↑	-	-	-	VMware Virtual SAN	963.74GB
S2DCenter	8.96% ↗	-	-	-	Microsoft Storage Spaces Direct	2.72TB
vsanDatastore	33.76% ↑	-	-	-	VMware Virtual SAN	963.74GB

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みます。

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。

仮想リソースリスト

全てのストレージプール > VMware Virtual SAN > vsanDatastore

▼ 全てのストレージプール

- VMware Virtual SAN
- Microsoft Storage Spaces Direct
- EXTENSIVE DRIFT

情報

ステータス	⚠
プール名	vsanDatastore
種類	VMware Virtual SAN
バージョン	6.0.0 3825889
可用性	-
重複検出	無効
圧縮	-
クラスタ名	vsanCluster

使用容量

使用容量 325.32GB
空き容量 638.42GB
合計容量 963.74GB

ノードリスト

検索

3 / 3

ノード名	ホスト名	モデル	IPアドレス	OS名
✖ SV_MAN5001522	-	PRIMERGY RX200 S8	192.168.1.101	
✔ SV_MAG8001213	localhost.localdomain	PRIMERGY RX2530 M2	192.168.1.102	VMware 6.0
⚠ SV_YUN5000000	ESX0205	PRIMERGY RX200 S8	192.168.1.103	VMware 6.0

(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。



↓

仮想リソースステータス						
全てのストレージプール						
プール名	使用率	現在	10 日前	20 日前	30 日前	種類
vsanData	0.00%	↑	-	-	-	VMware Virtual SAN
S2D on S2DC	8.96%	↓	-	-	-	Microsoft Storage Spaces Direct
vsanD	33.76%	↑	-	-	-	VMware Virtual SAN
S2DCenter	8.96%	↓	-	-	-	Microsoft Storage Spaces Direct
vsanDatastore	33.76%	↑	-	-	-	VMware Virtual SAN

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 • Microsoft Storage Spaces Direct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 • 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

ステータス異常が発生した層	状態
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、各ストレージプール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VMware vCenter Server 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。

- 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。
- VMware vCenter Server 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。
- 「ホストおよびクラスタ」で、手順1で確認したクラスタ名を選択します。
- [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。

- VMware vCenter Server 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。
- [監視]タブから[Virtual SAN]-[健全性]を選択し、表示されるVirtual SANの健全性画面で[再テスト]を選択して、「失敗」となっていたテスト結果が「パス」に変わったことを確認します。
- [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。
- 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。

Microsoft Storage Spaces Directの場合

ISM GUIおよび管理サーバ上のサーバマネージャーから、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。

- 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. 管理サーバ上でサーバ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. 管理サーバ上でサーバ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

実行できるユーザー

Administratorグループ

Admin Operator Monitor

その他のグループ

Admin Operator Monitor

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。



P 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、仮想リソースの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。

なお、更新処理はISMのタスクに登録されます。

表示情報が古いままの場合、ISM GUIの「タスク」画面からタスクタイプが「Refresh Virtual Resource」のタスクが「完了」になっているか確認してください。

ステータス	進捗	結果	タスクID	タスクタイプ	操作者	登録時間	完了時間
完了	1 / 1	Success	1	Refresh Virtual Resource	administrator	2017/05/15 22:55:21	2017/05/15 22:55:21

- ・ 仮想リソース情報は、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)。
 - ー すべての仮想リソース情報は、毎日ローカルタイムのAM0:00に自動更新されます。
 - ー 仮想リソースのステータスは、3分おきに自動更新されます。

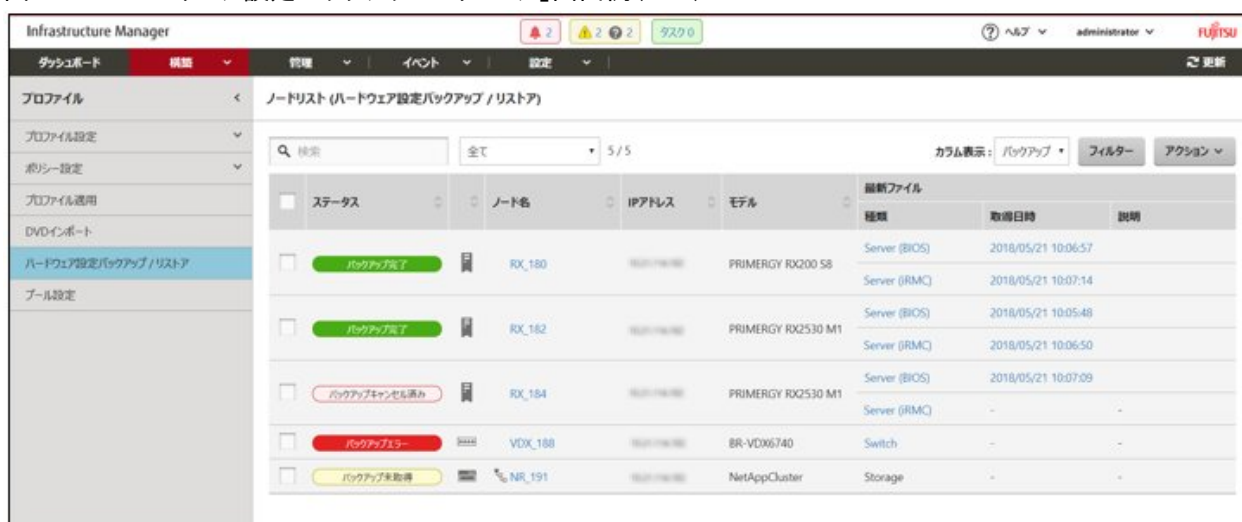
2.10 ハードウェア設定バックアップ／リストア機能

本機能は、ハードウェアの設定を吸い上げて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やPRIMEQUEST 3000BのBIOS／iRMCの設定
- ・ ETERNUS NR (NetApp) のストレージの設定
- ・ 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へインポートし、インポートしたBIOS／iRMC設定のファイルをPRIMERGYやPRIMEQUEST 3000Bへ、スイッチ設定のファイルをVDXへ反映できます。

図2.14 「ハードウェア設定バックアップ / リストア」画面例 (GUI)



P 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の電源をオフにする必要があります。
- ・ ストレージ設定、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



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。

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]-[プロフィール]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. ノードを選択します。[アクション]ボタンから[ハードウェア設定バックアップ]を選択します。
「ハードウェア設定バックアップ」画面が表示されます。
4. 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の電源をオフにし、[サーバ電源状態取得]ボタンを選択して、パワーステータスが「Off」になったことを確認します。
5. 設定をバックアップする[Server (BIOS)]、[Server (iRMC)]、[Storage]、[Switch]にチェックを付けて、[実行]ボタンを選択します。

ポイント

複数のノードとハードウェア設定を選択して、バックアップできます。

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。

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. ノードを選択します。[アクション]ボタンから[エクスポート(バックアップ)]を選択します。
4. 画面表示に従い、ファイルを選択して、[実行]ボタンを選択します。

ポイント

複数のノードとハードウェア設定を選択して、エクスポートできます。

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

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をプロファイルに変換して追加します。

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. ノードを選択します。[アクション]ボタンから[バックアップからプロファイル追加]を選択します。
4. 「バックアップからプロファイル追加」ウィザードに従い、設定項目を入力します。

ポイント

- ・ 複数のノードを選択して、プロファイル追加できます。
- ・ PRIMERGY / PRIMEQUEST 3000Bサーバのバックアップでのみ使用できます。

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

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をポリシーに変換して追加します。

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. ノードを選択します。[アクション]ボタンから[バックアップからポリシー追加]を選択します。
4. 「バックアップからポリシー追加」ウィザードに従い、設定項目を入力します。

ポイント

- ・ 複数のノードを選択して、ポリシー追加できます。
- ・ PRIMERGY / PRIMEQUEST 3000Bサーバのバックアップでのみ使用できます。

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

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

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。

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. ノードを選択します。[アクション]ボタンから[インポート]を選択します。
4. [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
ローカルにあるバックアップファイルをインポートします。
 - ー FTP
ISM-VAのFTPサーバからバックアップ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」のディレクトリ配下にバックアップ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。
5. [ファイル]でインポート対象のバックアップファイルを指定し、[実行]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。
- ・ 複数のノードを選択して、インポートできます。

注意

ETERNUS NR (NetApp) のバックアップファイルはインポートできません。

2.10.6 ハードウェア設定のリストア

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のハードウェア設定をノードへ反映します。

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. 「ノードリスト」画面の[カラム表示]欄で[リストア]を選択します。
4. ノードを選択します。[アクション]ボタンから[ハードウェア設定リストア]を選択します。
5. 画面表示に従い、ファイルを選択して、[実行]ボタンを選択します。

ポイント

複数のノードを選択して、リストアできます。

注意

- ETERNUS NR (NetApp) のバックアップファイルはリストアできません。
- VDXのリストアでは、設定項目を初期化してからリストアしてください。初期化されていない項目は、バックアップの内容が反映されないことがあります。
VDXでは、リストアできない設定項目があります。リストアできない設定項目を以下に示します。

- ライセンス情報
- 動作モード
- シャーシ / ホスト名
- パスワード
- 管理用ポート
- NTP サーバの設定
- 日時設定 (clock set コマンド)

リストア後に設定内容を確認し、必要に応じて設定してください。

2.10.7 ハードウェア設定バックアップファイルの削除

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。

2.11.1 サポート対象

本機能がサポートするハイパーバイザー、仮想化管理ソフトウェアは、以下のとおりです。

項目		ハイパーバイザー	仮想化管理ソフトウェア
VMware	5.x	VMware ESXi 5.5	vCenter Server 5.5
			vCenter Server Appliance 5.5
	6.x	VMware ESXi 6.0	vCenter Server 6.0
			vCenter Server Appliance 6.0
		VMware ESXi 6.5	vCenter Server 6.5
			vCenter Server Appliance 6.5
		VMware ESXi 6.7	vCenter Server 6.7
			vCenter Server Appliance 6.7
Redhat	7.x	Redhat Enterprise Linux 7.2 (KVM) [注1]	OpenStack
		Redhat Enterprise Linux 7.3 (KVM)	
		Redhat Enterprise Linux 7.4 (KVM)	
		Redhat Enterprise Linux 7.5 (KVM)	
		Redhat Enterprise Linux 7.6 (KVM)	

[注1] 分析VMを使用した通信量および通信品質情報の表示はサポート対象外です。

注意

- 仮想ネットワークアダプターを監視するにあたり、あらかじめ対象のハイパーバイザー、仮想化管理ソフトウェアに設定が必要な場合があります。
- OpenStackでの動作実績については当社技術員へお問合せください。

2.11.2 分析VMの確認

本機能がサポートするISMバージョンと分析VMバージョンは以下のとおりです。

ISMバージョン	Infrastructure Manager 分析VM for KVM	Infrastructure Manager 分析VM for VMware
ISM 2.4.0以降	V1.1.1	V1.1.0

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が必要となります。

追加CPUコア数	追加メモリ容量	追加ディスク容量
2コア以上	8GB以上	40GB以上

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ヶ月以内です。

表2.4 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。
仮想ネットワークアダプターのCPU使用率[注1]	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1]	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1]: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2.5 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

VMwareとKVMにおける仮想ネットワーク パケット分析機能の機能差は以下のとおりです。

サポート機能	表示項目	VMware	KVM
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。



注意

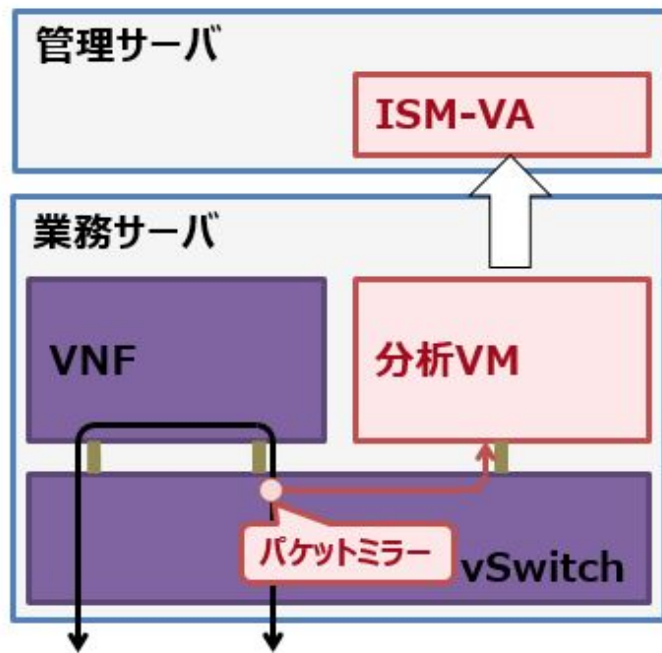
- Xenは利用できません。

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 パケット分析機能は、通信性能の低下が発生しているハイパーバイザーに対して、分析VMを手動でデプロイすることで、その分析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。取得対象は以下項目です。

- ・ 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2.15 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（ISM 2.4.0.b 以降）

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2.6 (OpenStack)ボトルネック分析によって表示される要因

要因	説明
パケット転送プロセスの過負荷	パケット転送プロセスの負荷が高いため、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の負荷が高いため、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。
パケット転送プロセスのリソース競合	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。

要因	説明
仮想アダプターのバッファ不足	仮想アダプターのパケットキューのバッファ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。
VMのバッファ不足	分析対象VMのパケットキューのバッファ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。

表2.7 (VMware)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 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。

- [2.12.1 クラスタ管理機能](#)
- [2.12.2 クラスタ作成機能](#)
- [2.12.3 クラスタ拡張機能](#)
- [2.12.4 ファームウェアローリングアップデート機能](#)



注意

- ISM for PRIMEFLEXでは、ISMの電力制御機能は使用できません。

2.12.1 クラスタ管理機能

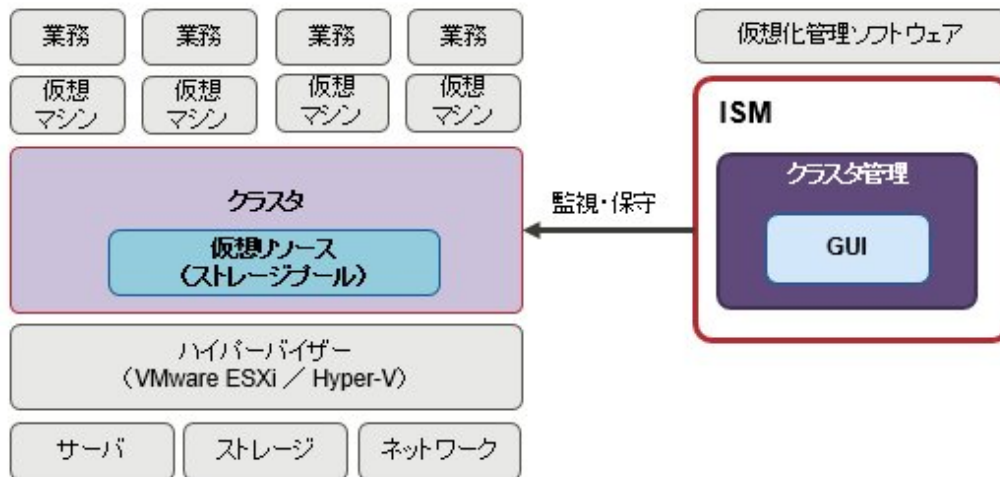
ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ管理機能は、ISMと連携してクラスタを管理でき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、「[2.12.1.2 クラスタ管理機能のサポート対象](#)」を参照してください。

図2.16 クラスタ管理機能の概要



クラスタ管理機能は、ISM GUIと連動したクラスタ管理のための各種GUIを提供し、以下のような機能を備えます。

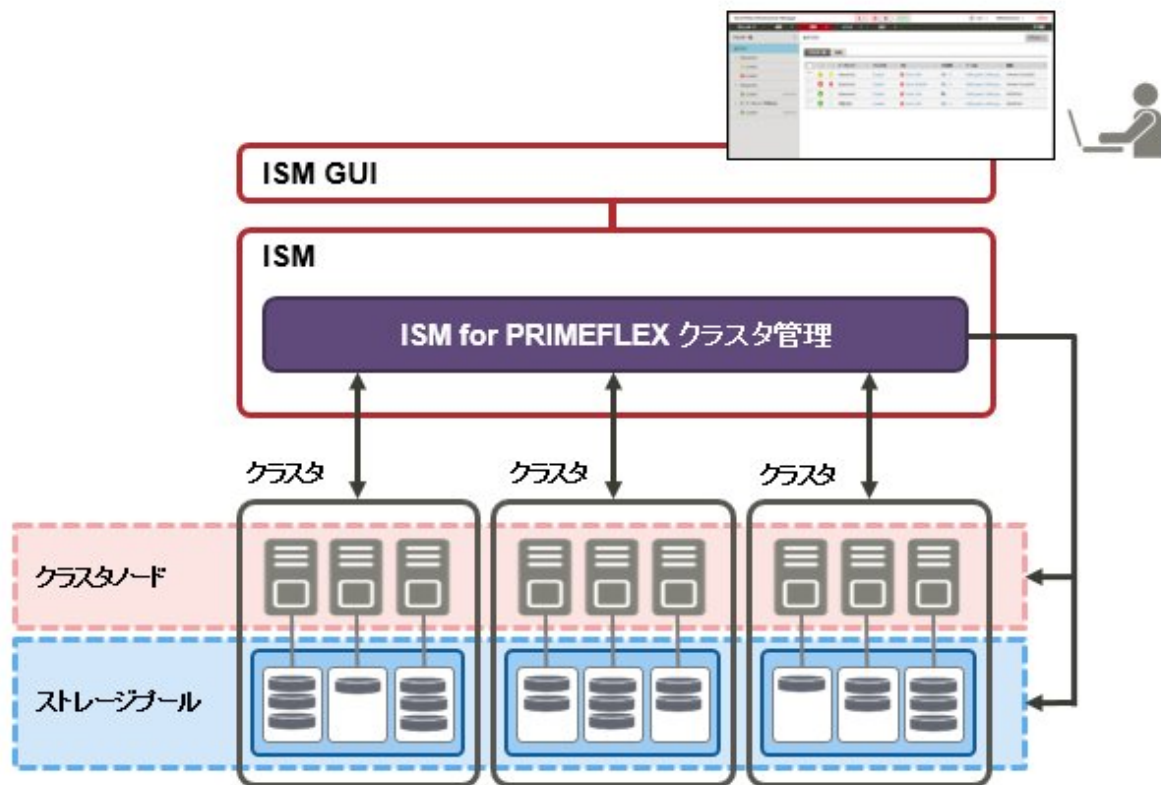
- クラスタの一覧表示と、クラスタの状態などのサマリ表示
- クラスタの詳細情報の表示
クラスタの構成情報について、以下のような情報を表示します。
 - ー クラスタのノード情報
 - ー クラスタ上の仮想リソースの情報
 - ー クラスタ作成およびクラスタ拡張のパラメーター設定情報
- ダッシュボードからのクラスタ監視を可能とするウィジェット

2.12.1.1 クラスタ管理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2.17 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。

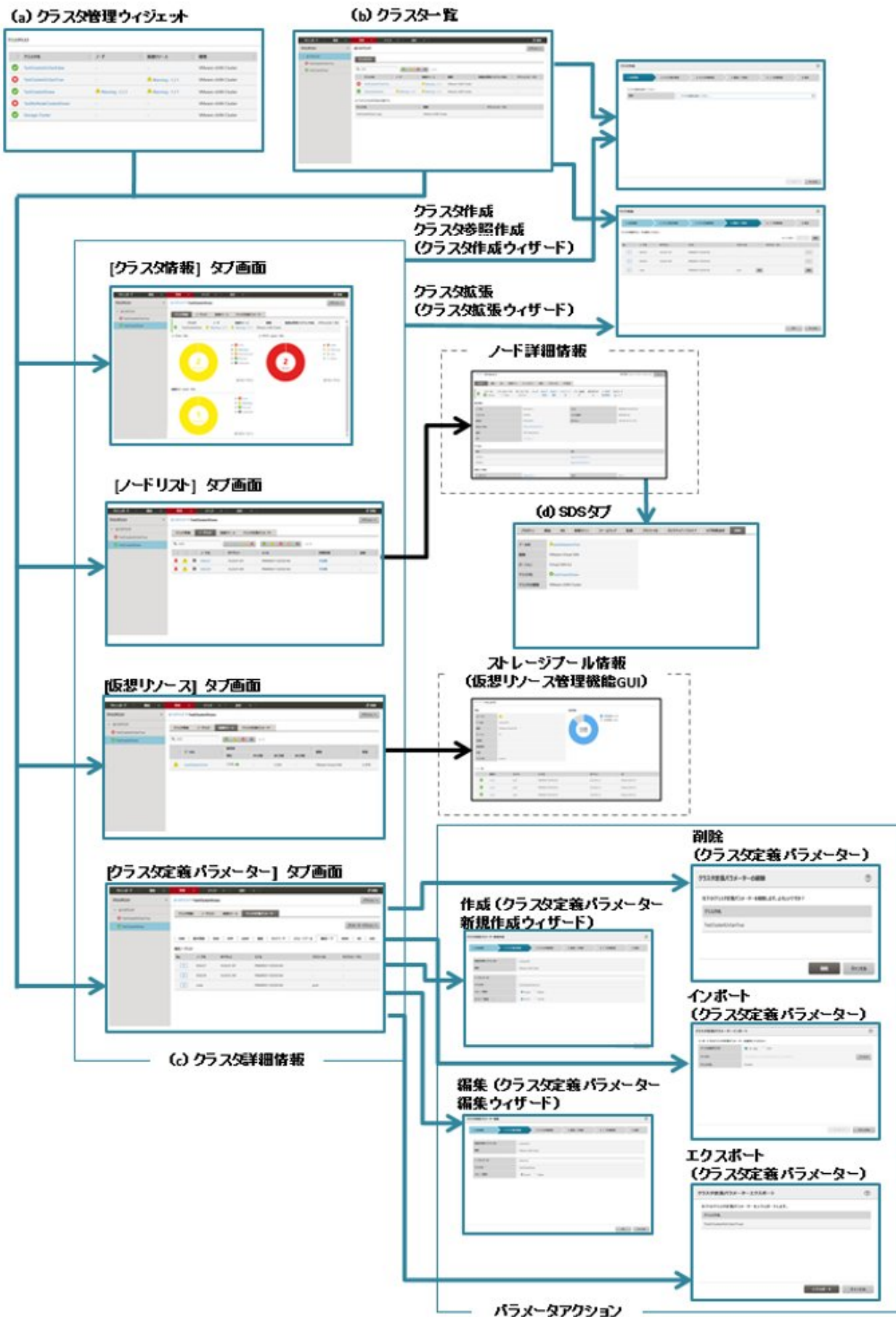
クラスタ管理GUI(図2.18 クラスタ管理GUI中の(a)～(d))でクラスタに関する各種情報を表示します。

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GUIについては、「2.9.2 仮想リソース管理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2.18 クラスタ管理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) クラスタ一覧

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、ノードに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GUIの内容について、以下に説明します。

クラスタ一覧画面

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、クラスタ一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2.19 クラスタ一覧画面



クラスタの詳細画面 (タブ表示画面)

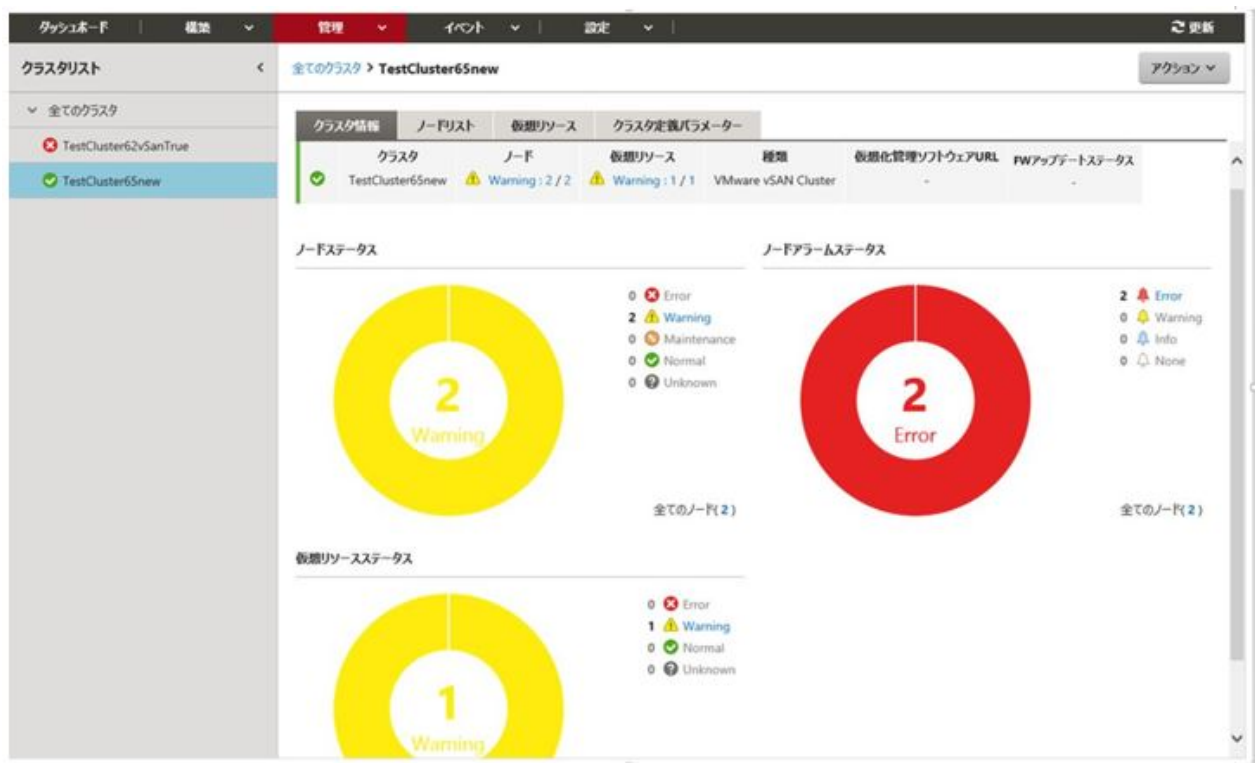
クラスタ一覧画面のクラスタ名を選択するとクラスタの詳細画面が表示され、クラスタおよびクラスタを構成する各要素の情報を確認できます。

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。

The screenshot shows the vSphere Web Client interface for a cluster named 'TestCluster65New'. The left sidebar lists clusters, with 'TestCluster65New' selected. The main area has tabs for 'Cluster Information', 'Node List', 'Virtual Resources', and 'Cluster Configuration Parameters'. The 'Node List' tab is active, showing a table of nodes. The table has columns: Node Name, IP Address, Model, Storage Location, and Description. There are two nodes listed: ESX6227 and ESX6229, both with a status of 'Warning' (yellow icon) and 'Storage Location' of '未搭載' (Not Installed).

ノード名	IPアドレス	モデル	搭載位置	説明
ESX6227	10.10.10.10	PRIMERGY CX2550 M2	未搭載	-
ESX6229	10.10.10.10	PRIMERGY CX2550 M2	未搭載	-

[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、仮想リソース管理GUIのストレージプールの情報画面が表示されます。

仮想リソース管理GUIの説明については、「[2.9.2 仮想リソース管理GUI](#)」、または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

クラスタの作成、およびクラスタへサーバ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]
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。

— 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。

— 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。

— 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。

— 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。

— 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、「[2.12.1.3 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

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、「[2.12.2 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

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、「[2.12.2 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

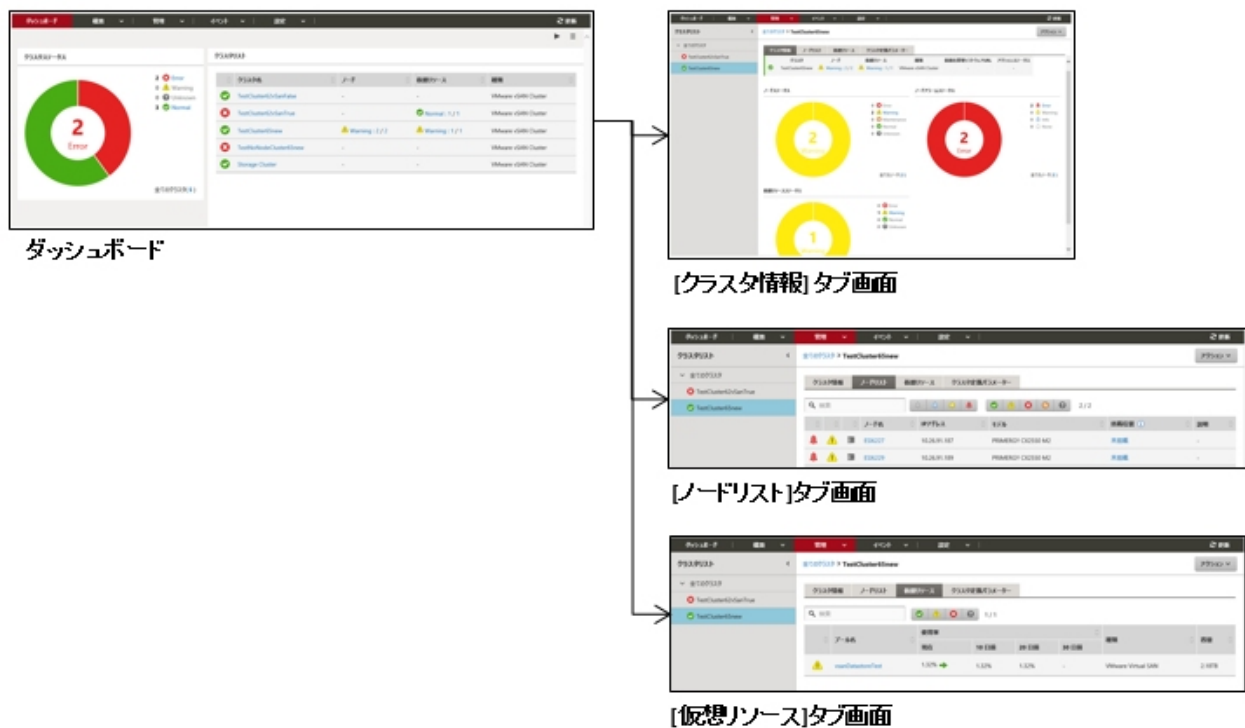
本メニューを選択すると、「クラスタ拡張」ウィザードが起動されます。ウィザードに従ってクラスタへサーバを追加します。

詳細については、「[2.12.3 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2.20 ダッシュボードとの連携



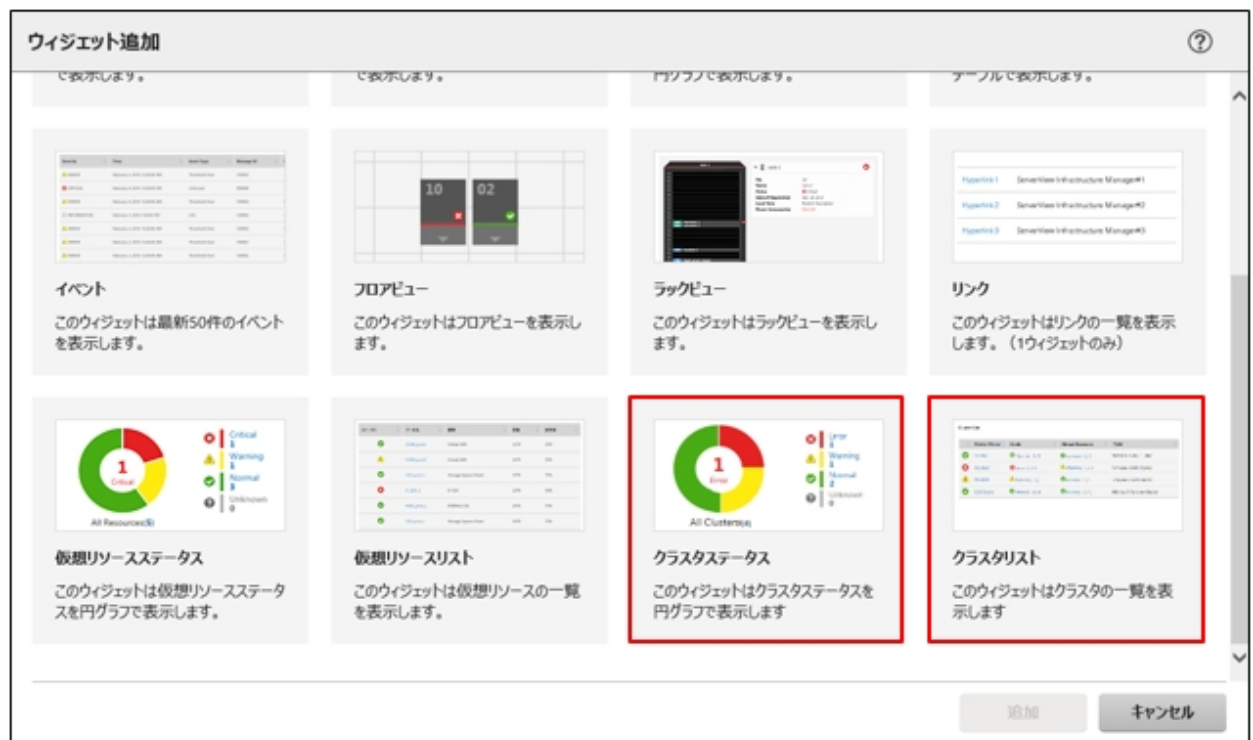
ISMのダッシュボードにウィジェットを追加する方法は以下のとおりです。

1. 上部にある[≡]から[ウィジェット追加]を選択します。

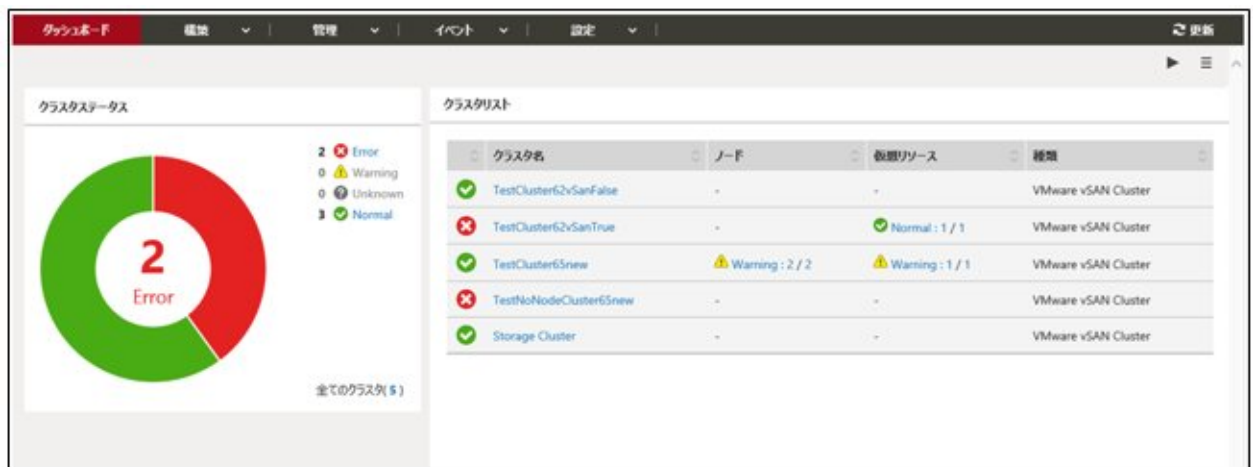


ウィジェット追加メニューが表示されます。

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。

プロパティ	部品	OS	仮想マシン	ファームウェア	監視	プロファイル	バックアップ/リストア	ログ収集設定	SDS
プール名	vsanDatastoreTest								
種類	VMware Virtual SAN								
バージョン	6.0.0 3825889								
クラスタ名	TestCluster65new								
クラスタの種類	VMware vSAN Cluster								

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GUI](#)」を参照してください。

2.12.1.2 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
- Microsoft Failover Cluster

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。

vSANクラスタ環境の要件は、以下のとおりです。

項目	要件
ハイパーバイザー	• VMware ESXi 6.0 Update 2 • VMware ESXi 6.5 • VMware ESXi 6.5 Update 1 • VMware ESXi 6.7
仮想化管理ソフトウェア	• vCenter Server Appliance 6.0 Update 2 • vCenter Server Appliance 6.5 • vCenter Server Appliance 6.7
SDS	• VMware Virtual SAN 6.2 • VMware Virtual SAN 6.5 • VMware Virtual SAN 6.6 • VMware Virtual SAN 6.6.1

Microsoft Failover Cluster

Microsoft Failover Clusterは、Windows Serverが導入された複数のサーバから構成されるシステムです。

クラスタ管理機能はWindows Server OSからクラスタに関する情報を取得し、ISM GUIへ反映します。

クラスタ上では、各サーバに搭載される物理ストレージを集約して、仮想ストレージであるStorage Spaces Directの「記憶域プール」が構成されます。記憶域プールの監視はISMから実施できます。

Microsoft Failover Cluster環境の要件は、以下のとおりです。

項目	要件
OS	- Windows Server 2016 - Windows Server 2019
役割と機能	クラスタノードに、以下の役割と機能がインストール済みであること - Hyper-V - Microsoft Failover Cluster
ハイパーバイザー	Hyper-V
SDS	Microsoft Storage Spaces Direct
その他	- ISMからのOSおよびクラスタの監視が可能であること - クラスタノードにおいて、CredSSP認証が有効であること



注意

Microsoft Failover Clusterの場合は以下が必要です。

- 各ノードに対して、ISMからのOS監視を有効にするための事前設定
- フェイルオーバークラスタに対して、ISMからの監視を有効にするための事前設定
- 各ノードにおいて、CredSSP認証が有効であること

設定方法については、「[3.9.2 PRIMEFLEX for Microsoft Storage Spaces Directの事前設定](#)」を参照してください。

監視対象OSに対する設定手順については、「[B.2 監視対象への設定手順\(OS:Windows\)](#)」、「[B.7 監視対象への設定手順\(仮想化管理ソフトウェア:Microsoft Failover Cluster\)](#)」を参照してください。

2.12.1.3 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、「[2.12.1.1 クラスタ管理GUI](#)」を参照してください。



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、クラスタの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。
- クラスタ情報の更新はISMのタスクに登録されます。

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、タスクタイプが「Refresh Virtual Resource」のタスクを確認します。

ステータス	進捗	結果	タスクID	タスクタイプ	操作者	登録時間	完了時間
完了	1 / 1	Success	1	Refresh Virtual Resource	administrator	2017/05/15 22:55:21	2017/05/15 22:55:21

タスクのステータスが「完了」になるまでは、表示の更新は完了していません。

タスクのステータスが「完了」となったことを確認してから、ISM GUIの画面更新(画面右上の更新ボタンを選択)をしてください。

- GUI上の情報は、毎日ローカルタイムのAM0:00に自動更新されます。
- GUIに表示されるクラスタのステータスは、3分おきに自動更新されます。

2.12.1.4 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

クラスタの監視

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。

The screenshot shows the 'クラスタリスト' (Cluster List) page. On the left is a sidebar with a search bar and a list of clusters: 'TestCluster62vSanTrue' (with a red error icon) and 'TestCluster65new' (with a green checkmark icon). The main area is titled '全てのクラスタ' (All Clusters) and contains a table with the following columns: 'クラスタ名' (Cluster Name), 'ノード' (Node), '仮想リソース' (Virtual Resources), '種類' (Type), '仮想化管理ソフトウェアURL' (Virtualization Management Software URL), and 'アクションステータス' (Action Status). The table lists two clusters: 'TestCluster62vSanTrue' (VMware vSAN Cluster) with a red error icon and 'TestCluster65new' (VMware vSAN Cluster) with a green checkmark icon. The '仮想リソース' column shows 'Normal : 1 / 1' for the first cluster and 'Warning : 2 / 2' for the second cluster.

クラスタ名	ノード	仮想リソース	種類	仮想化管理ソフトウェアURL	アクションステータス
TestCluster62vSanTrue	-	Normal : 1 / 1	VMware vSAN Cluster	-	-
TestCluster65new	Warning : 2 / 2	Warning : 1 / 1	VMware vSAN Cluster	-	-

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」画面では、ノードおよび仮想リソースについて、異常を示す数が表示されます。

クラスタリスト

<

全てのクラスタ

▼ 全てのクラスタ

TestCluster62vSanTrue

TestCluster65new

全てのクラスタ

クラスタリスト

検索

2 / 2

クラスタ名	ノード	仮想リソース	種類	仮想化管理ソフトウェアURL	アクションステータス
TestCluster62vSanTrue	-	Normal : 1 / 1	VMware vSAN Cluster	-	-
TestCluster65new	Warning : 2 / 2	Warning : 1 / 1	VMware vSAN Cluster	-	-

異常を示す数は、以下の書式で表示されます。

[異常ステータスにある管理対象の数] / [管理対象の総数]

[異常ステータスにある管理対象の数]は、最も重要度の高いステータスにある対象の数を示します。

異常ステータスの重要度については、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。 「クラスタリスト」画面では、「—」と表示されます。

「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、「[2.12.1.1 クラスタ管理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、「[2.12.1.1 クラスタ管理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。

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。

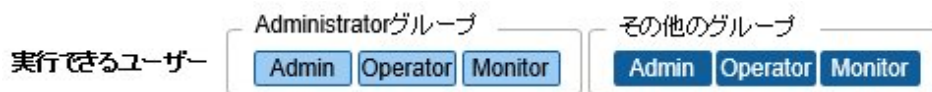
ストレージプールの状態、およびストレージの使用率などが表示されます。

画面内容については、「[2.12.1.1 クラスタ管理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GUIの詳細画面へ遷移し、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。

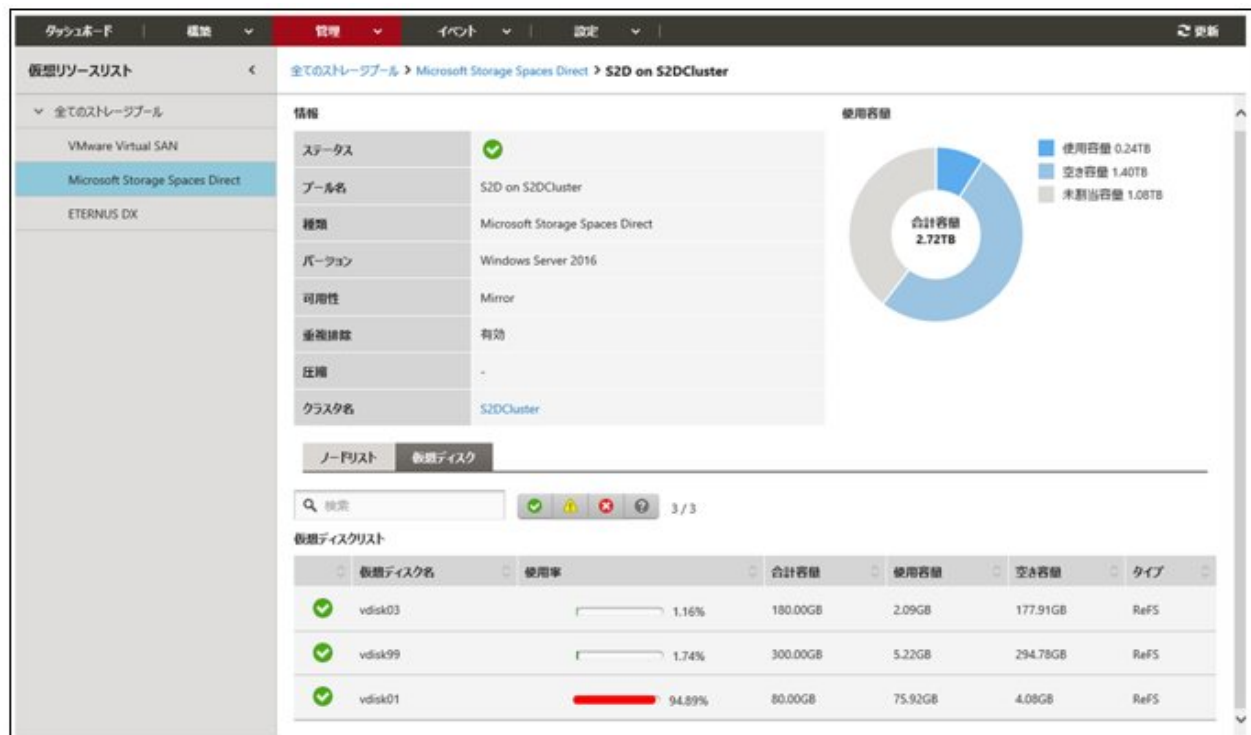
2.12.1.5 PRIMEFLEX for Microsoft Storage Spaces Direct 仮想ディスクの監視



仮想リソース管理GUIで対象のプール名を選択すると、詳細情報画面が表示され、[使用容量]で使用中の容量および空き容量を確認できます。

仮想リソース管理GUIの利用方法については、「[2.9 仮想リソース管理機能](#)」を参照してください。

PRIMEFLEX for 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。



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。

- ・ 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。
- ・ 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。
- ・ 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。

2.12.2 クラスタ作成機能

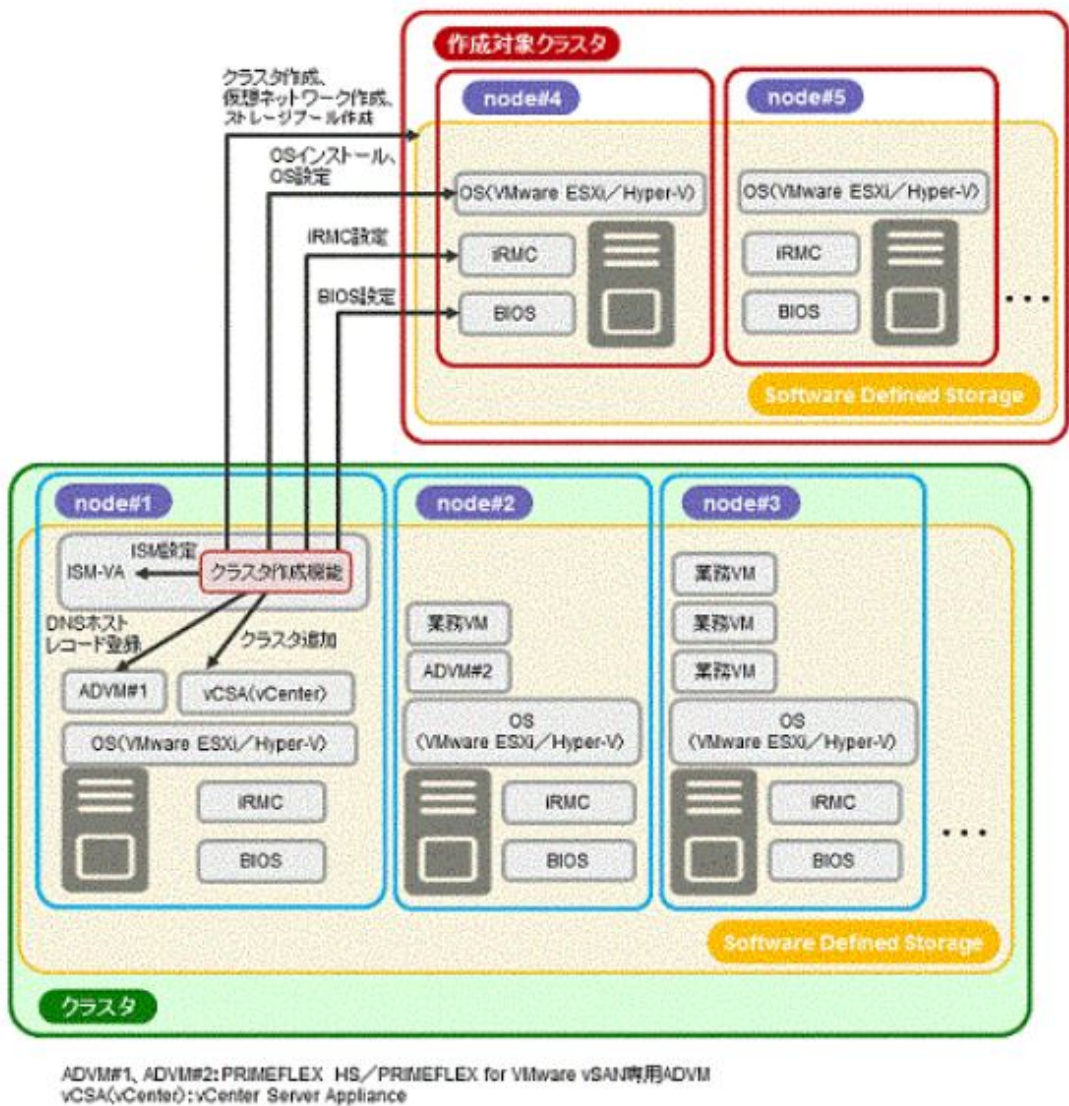
ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ作成機能は、PRIMEFLEX HS／PRIMEFLEX for VMware vSANおよびPRIMEFLEX for Microsoft Storage Spaces Direct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を新規クラスタ環境に追加

図2.21 クラスタ作成機能の概要



2.12.2.1 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2.8 PRIMEFLEX for VMware vSANの自動設定項目一覧

自動設定項目	説明
OSインストール	- 新規クラスタを構成するサーバのOSインストール - 新規クラスタを構成するサーバのシステム日時の設定 - 新規クラスタを構成するサーバのOSパッチの適用
DNSホストレコード登録	新規クラスタを構成するサーバの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)
OS設定	- ESXiシェルの有効化と起動 - SSHサービスの有効化と起動 - 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)

自動設定項目	説明
	• ixgbendライバの有効化 (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) • ローカル管理ユーザーの追加 • ホスト名をFQDNに設定 • SSL v3の有効化 • IPv6の無効化 • セカンダリDNSサーバのIPアドレスの設定 • DNSサフィックスの設定 • NTPサーバのIPアドレスの設定 • NTPクライアントのファイアーウォールの設定 • NTPクライアントサービスの実行 • ホストの電源管理を高パフォーマンスに設定 • OSの再起動 • 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 • 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 • Management NetworkへNICの設定 • 新規クラスタを構成するサーバのESXiのActive Directory認証設定 (PRIMEFLEX構成のADVM、またはお客様環境のADサーバを使用したActive Directory連携を行わない構成時は設定しない) • ESXiシェルの無効化と停止 • SSHサービスの無効化と停止
iRMC設定	• ローカルユーザー (pflocaladmin) の作成 • adminユーザーのパスワード変更 • 新規クラスタを構成するサーバのiRMCのActive Directory認証設定 (PRIMEFLEX構成のADVM、またはお客様環境のADサーバを使用したActive Directory連携を行わない構成時は設定しない) • 新規クラスタを構成するサーバのiRMCのリセット
クラスタへのサーバ追加	• 新規クラスタを構成するサーバを管理用分散仮想スイッチへ登録 • 新規クラスタを構成するサーバを業務用分散仮想スイッチへ登録 • 分散仮想スイッチの設定 • SSDのキャパシティデバイスの設定 (All Flash環境時) • 新規クラスタを構成するサーバをクラスタに追加
ISM設定	• 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 • ISMに登録されているiRMCのWebインターフェースURLの変更 • 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
クラスタ作成	• クラスタの作成
仮想ネットワーク作成	• 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 • NIOCの有効化

自動設定項目	説明
	・ポートグループの作成と設定 ・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
ストレージプール作成	・vSANの有効化 ・デデュープおよび圧縮の設定
仮想リソース更新	・クラスタ情報の更新

表2.9 PRIMEFLEX for Microsoft Storage Spaces Directの自動設定項目一覧

自動設定項目	説明
OSインストール	・新規クラスタを構成するサーバのOSインストール
OS設定	・リモート接続機能の有効化 ・Basic認証の有効化 ・CredSSP認証の有効化 ・事前準備で用意したルート証明(cerファイル)、個人証明(pfxファイル)の登録 ・httpsリスナーの設定 ・httpsリスナー用ポートの開放 ・ローカルユーザー(pflocaladmin)の作成 ・新規クラスタを構成するサーバへの設定 － Hyper-Vのインストール － MACアドレス範囲の設定 － Windows Server バックアップのインストール － フェイルオーバークラスタのインストール － 仮想スイッチの作成 － VMネットワークアダプターの作成 － VMネットワークアダプターのVLAN設定 － 管理LANネットワークアダプターの切替え － IPv6の無効化 － 優先DNSサーバの設定 － 代替DNSサーバの設定 － Intel、Mellanox LANドライバのSR/IOVの無効化 － Intel、Mellanox LANドライバのVMQの有効化 － 管理LAN用ポートのVMQ設定 － 業務LAN用ポートのVMQ設定 － Intel、Mellanox LANドライバのQoSの無効化
iRMCの設定	・ローカルユーザー(pflocaladmin)の作成 ・adminユーザーのパスワード変更 ・新規クラスタを構成するサーバのiRMCのActive Directory認証設定 ・新規クラスタを構成するサーバのiRMCのリセット
クラスタへのサーバ追加	・新規クラスタを構成するサーバをフェイルオーバークラスタに追加

自動設定項目	説明
ISMの設定	- 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 - ISMに登録されているiRMCのWebインターフェースURLの変更 - ISMに登録されているOSのアカウントの変更 - 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
クラスタ作成	- クラスタの検証 - クラスタの作成
仮想ネットワーク作成	クラスタネットワークの設定
ストレージプール作成	- Storage Spaces Directの有効化 - ジャーナル用仮想ディスクの設定 - ストレージティアの設定
仮想リソース更新	新規クラスタのCMS情報を追加

2.12.2.2 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

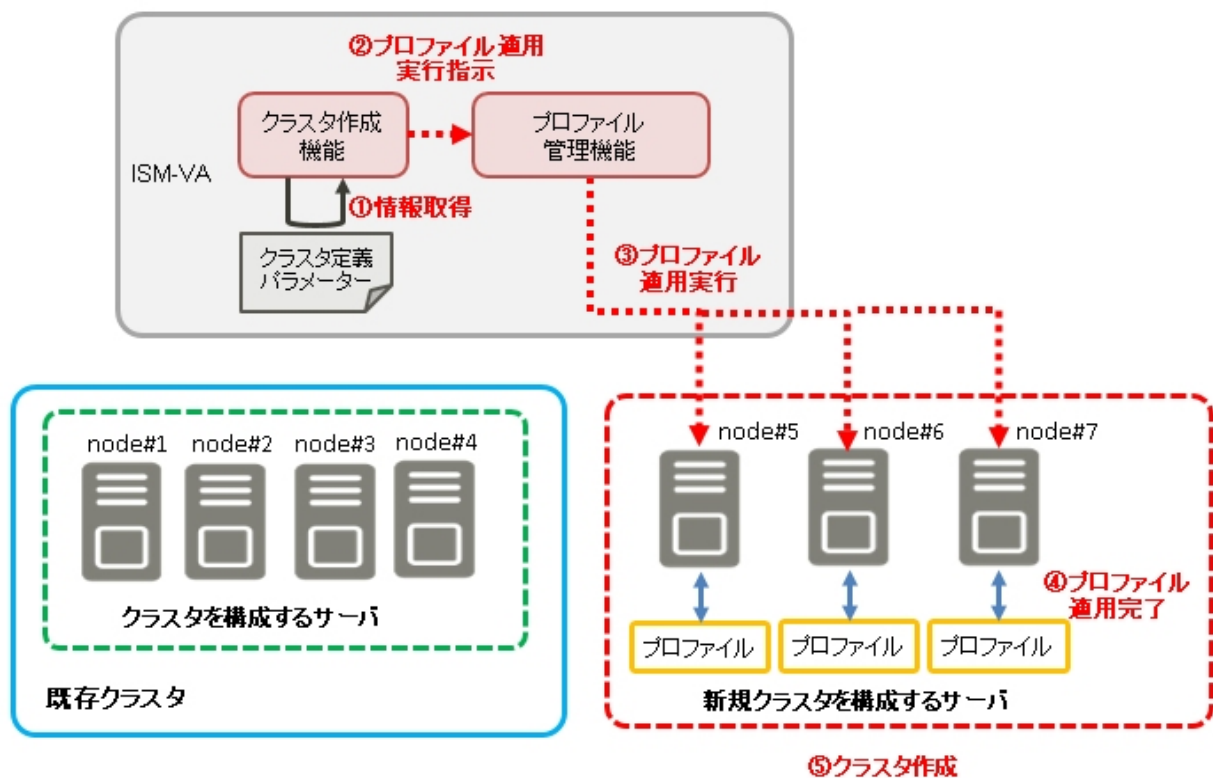
OS設定スクリプトとは、クラスタ作成機能の処理中に、ISMから新規クラスタを構成するサーバのOSに接続するために必要な設定を実行するスクリプトです。

注意

- クラスタ作成を実行する前に、事前にプロファイルを作成してください。
- インストール後のスクリプト実行機能で使用するOS設定スクリプトは、クラスタ作成機能実行時に自動で指定されます。プロファイル作成時に、「インストール後のスクリプト実行」の項目には何も指定しないでください。指定した場合は、クラスタ作成実行時にOS設定スクリプトで上書きされます。

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2.22 クラスタ作成機能とプロファイル管理機能の連携



2.12.2.3 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「6.11 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。



注意

クラスタ定義パラメーターをインポートして使用する場合は、クラスタ定義パラメーターの編集が必要です。

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。

2.12.2.4 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2.10 PRIMEFLEX for VMware vSANのサブタスクの処理一覧

処理名	実施内容
Prep Check	クラスタ作成の実行条件をチェックします。

処理名	実施内容
OS Installation	新規クラスタを構成するサーバのOSをインストールします。
DNS Settings	新規クラスタを構成するサーバの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のiRMC設定とISMの設定を行います。
OS Settings	新規クラスタを構成するサーバの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のOS設定(事後設定)を行います。

実施内容は、「[表2.8 PRIMEFLEX for VMware vSANの自動設定項目一覧](#)」を参照してください。

表2.11 PRIMEFLEX for Microsoft Storage Spaces Directのサブタスクの処理一覧

処理名	実施内容
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のOSをインストールします。
iRMC Settings	新規クラスタを構成するサーバのiRMC設定とISMの設定を行います。
OS Settings	新規クラスタを構成するサーバのOS設定を行います。
Cluster Settings	新規クラスタを構成するサーバのクラスタ設定を行います。
Ism Settings	新規クラスタを構成するサーバの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。
Kerberos Delegation	新規クラスタのKerberos委任の構成を行います。
Storage Pool Creation	新規クラスタのストレージプールを作成します。
ResourceList Registration	新規クラスタ情報を更新します。

実施内容は、「[表2.9 PRIMEFLEX for Microsoft Storage Spaces Directの自動設定項目一覧](#)」を参照してください。

2.12.3 クラスタ拡張機能

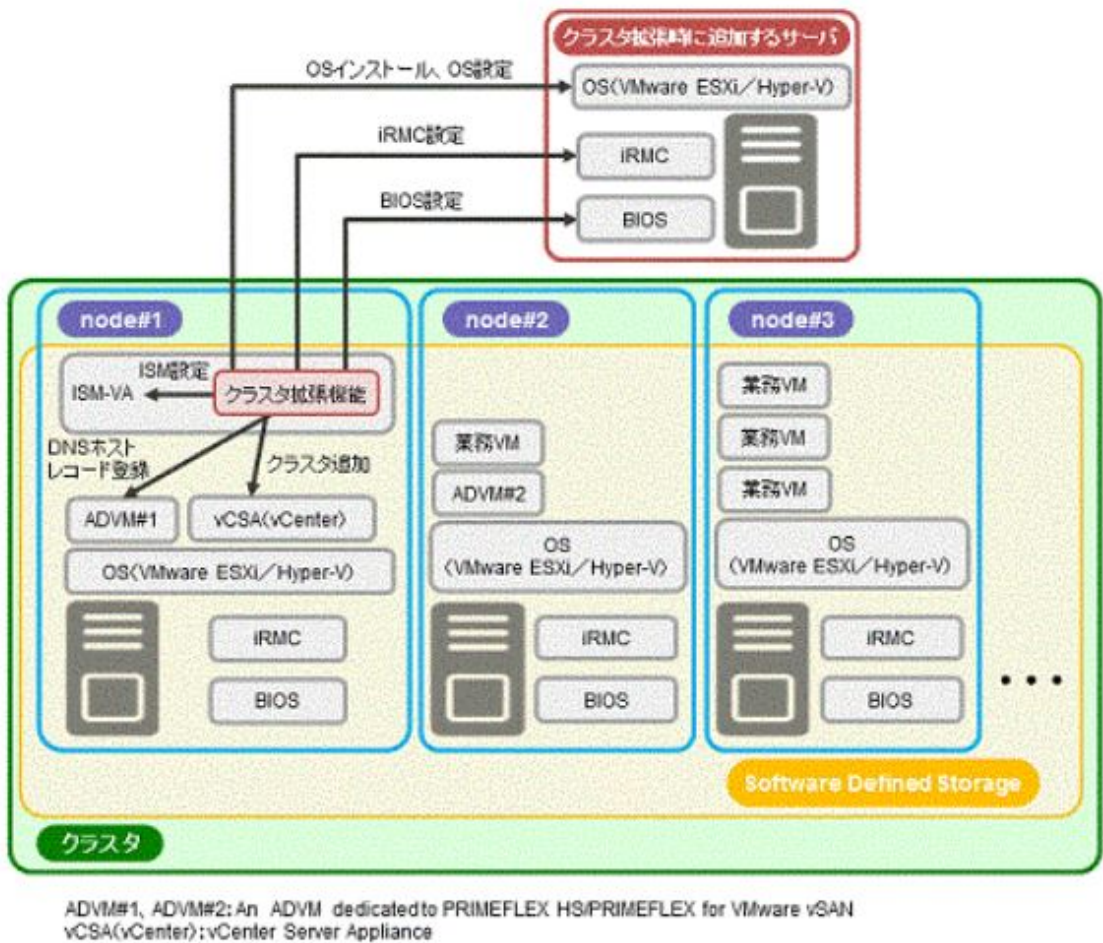
ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ拡張機能は、VMware vSANやMicrosoft Storage Spaces Directのストレージリソースが枯渇した際に、PRIMEFLEX HS／PRIMEFLEX for VMware vSANおよびPRIMEFLEX for Microsoft Storage Spaces Directの仮想化基盤環境に対して、新規にサーバ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を既存のクラスタ環境に追加

図2.23 クラスタ拡張機能の概要



2.12.3.1 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2.12 PRIMEFLEX HS／PRIMEFLEX for VMware vSANの自動設定項目一覧

自動設定項目	説明
OSインストール	- クラスタ拡張時に追加するサーバのOSインストール - クラスタ拡張時に追加するサーバのシステム日時の設定 - クラスタ拡張時に追加するサーバのOSパッチの適用
DNSホストレコード登録	クラスタ拡張時に追加するサーバの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)
OS設定	- ESXiシェルの有効化と起動 - SSHサービスの有効化と起動 - 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) - ixgbeドライバの有効化 (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) - ローカル管理ユーザーの追加 - ホスト名をFQDNに設定

自動設定項目	説明
	• SSL v3の有効化 • IPv6の無効化 • セカンダリDNSサーバのIPアドレスの設定 • DNSサフィックスの設定 • NTPサーバのIPアドレスの設定 • NTPクライアントのファイアーウォールの設定 • NTPクライアントサービスの実行 • ホストの電源管理を高パフォーマンスに設定 • OSの再起動 • 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 • 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 • Management NetworkへNICの設定 • クラスタ拡張時に追加するサーバのESXiのActive Directory認証設定(PRIMEFLEX構成のADVМ、またはお客様環境のADサーバを使用したActive Directory連携を行わない構成時は設定しない)
iRMC設定	• ローカルユーザー(pflocaladmin)の作成 • adminユーザーのパスワード変更 • クラスタ拡張時に追加するサーバのiRMCのActive Directory認証設定(PRIMEFLEX構成のADVМ、またはお客様環境のADサーバを使用したActive Directory連携を行わない構成時は設定しない) • クラスタ拡張時に追加するサーバのiRMCのリセット
クラスタへのサーバ追加	• クラスタ拡張時に追加するサーバを管理用分散仮想スイッチへ登録 • クラスタ拡張時に追加するサーバを業務用分散仮想スイッチへ登録 • 分散仮想スイッチの設定 • SSDのキャパシティデバイス設定(All Flash環境時) • クラスタ拡張時に追加するサーバをクラスタに追加
ISMの設定	• 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 • ISMに登録されているiRMCのWebインターフェースURLの変更 • 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

表2.13 PRIMEFLEX for Microsoft Storage Spaces Directの自動設定項目一覧

自動設定項目	説明
OSインストール	• クラスタ拡張時に追加するサーバのOSインストール
OS設定	• リモート接続機能の有効化 • Basic認証の有効化 • CredSSP認証の有効化 • 事前準備で用意したルート証明(cerファイル)、個人証明(pfxファイル)の登録 • httpsリスナーの設定

自動設定項目	説明
	- httpsリスナー用ポートの開放 - ローカルユーザー (pflocaladmin) の作成 - クラスタ拡張時に追加するサーバへの設定 - Hyper-Vのインストール - MACアドレス範囲の設定 - Windows Server バックアップのインストール - フェイルオーバークラスタのインストール - 仮想スイッチの作成 - VMネットワークアダプターの作成 - VMネットワークアダプターのVLAN設定 - 管理LANネットワークアダプターの切替え - IPv6の無効化 - 優先DNSサーバの設定 - 代替DNSサーバの設定 - Intel、Mellanox LANドライバのVMQの有効化 - Intel、Mellanox LANドライバのSR/IOVの無効化 - 管理LAN用ポートのVMQ設定 - 業務LAN用ポートのVMQ設定 - Intel、Mellanox LANドライバのQoSの無効化
iRMCの設定	- ローカルユーザー (pflocaladmin) の作成 - adminユーザーパスワードの変更 - クラスタ拡張時に追加するサーバのiRMCのActive Directory認証設定
クラスタへのサーバ追加	クラスタ拡張時に追加するサーバをフェイルオーバークラスタに追加
ISMの設定	- 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 - ISMに登録されているiRMCのWebインターフェースURLの変更 - ISMに登録されているOSのアカウントの変更 - 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

2.12.3.2 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

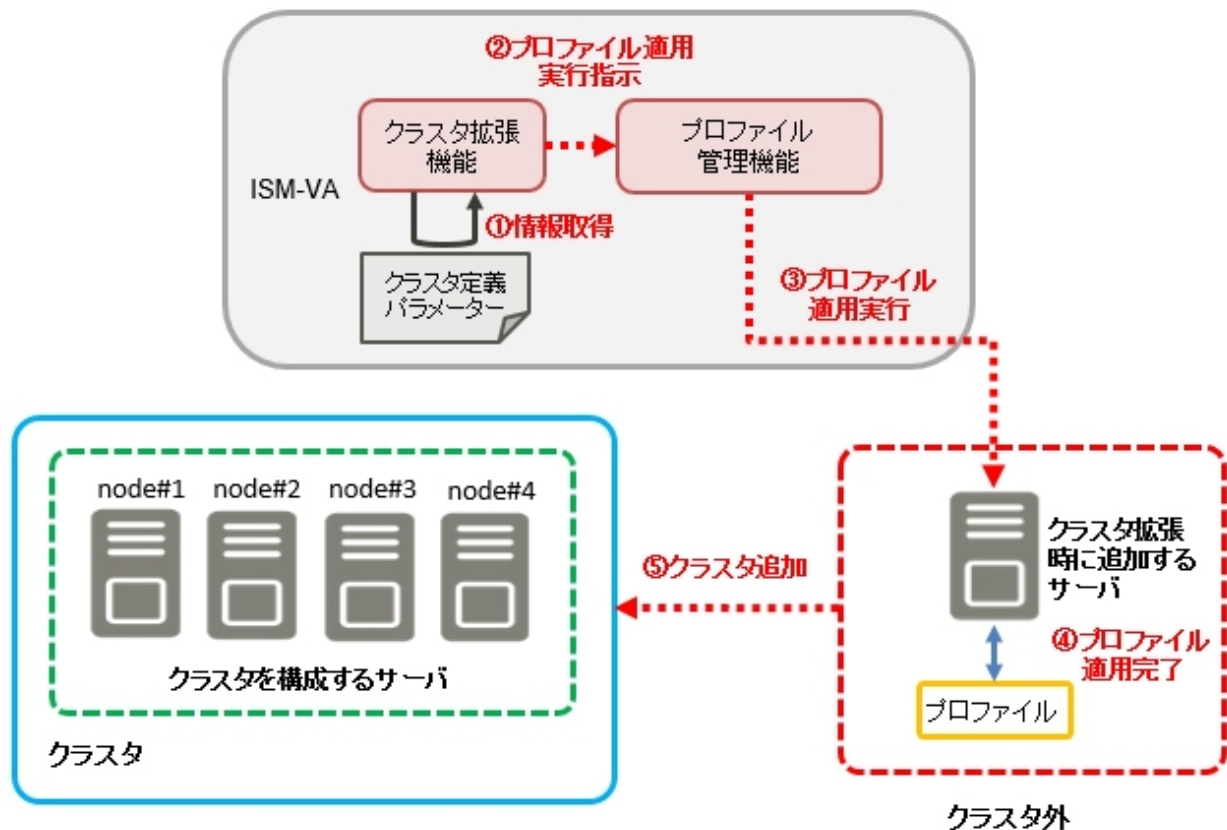
OS設定スクリプトとは、クラスタ拡張機能の処理中に、ISMからクラスタ拡張時に追加するサーバのOSに接続するために必要な設定を実行するスクリプトです。

注意

- ・ クラスタ拡張を実行する前に、事前にプロファイルを作成してください。
- ・ インストール後のスクリプト実行機能で使用するOS設定スクリプトは、クラスタ拡張機能実行時に自動で指定されます。プロファイル作成時に、「インストール後のスクリプト実行」の項目には何も指定しないでください。指定した場合は、クラスタ拡張実行時にOS設定スクリプトで上書きされます。

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2.24 クラスタ拡張機能とプロファイル管理機能の連携



2.12.3.3 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「6.11 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。

注意

クラスタ定義パラメーターをインポートして使用する場合は、クラスタ定義パラメーターの編集が必要です。

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。

2.12.3.4 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2.14 PRIMEFLEX HS／PRIMEFLEX for VMware vSANのサブタスクの処理一覧

処理名	実施内容
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のOSをインストールします。
DNS Settings	クラスタ拡張時に追加するサーバの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のOS設定(事後設定)を行います。

実施内容は、「表2.12 PRIMEFLEX HS／PRIMEFLEX for VMware vSANの自動設定項目一覧」を参照してください。

表2.15 PRIMEFLEX for Microsoft Storage Spaces Directのサブタスクの処理一覧

処理名	実施内容
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のOSをインストールします。
iRMC Settings	クラスタ拡張時に追加するサーバの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のISMの設定を行います。

実施内容は、「表2.13 PRIMEFLEX for Microsoft Storage Spaces Directの自動設定項目一覧」を参照してください。

2.12.4 ファームウェアローリングアップデート機能

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

ファームウェア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仮想マシンのvMotion (PRIMEFLEX HS／PRIMEFLEX for VMware vSAN)、またはLive Migration (PRIMEFLEX for Microsoft Storage Spaces Direct)を活用して、業務を停止することなくファームウェアのアップデートを行う機能です。

本機能は、ISMのファームウェア管理機能と連携して、クラスタを構成するすべてのサーバに対してファームウェアをアップデートすることで、お客様の作業を削減します。



注意

ファームウェアローリングアップデート機能を実行する前に、仮想マシン退避用のサーバを対象のクラスタの中から選択する必要があります。

ファームウェア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
サーバ (iRMC)	Onlineアップデート
	Offlineアップデート (ISM 2.4.0.b 以降)
サーバ (BIOS)	Onlineアップデート
	Offlineアップデート (ISM 2.4.0.b 以降)
サーバ (LAN/CNAカード) [注1]	Offlineアップデート (ISM 2.4.0.b 以降)

[注1]: PRIMEFLEX HS／PRIMEFLEX for VMware vSANおよびPRIMEFLEX for Microsoft Storage Spaces DirectでサポートしているLAN/CNAカードが対象です。

LAN/CNA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。

<http://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/>



注意

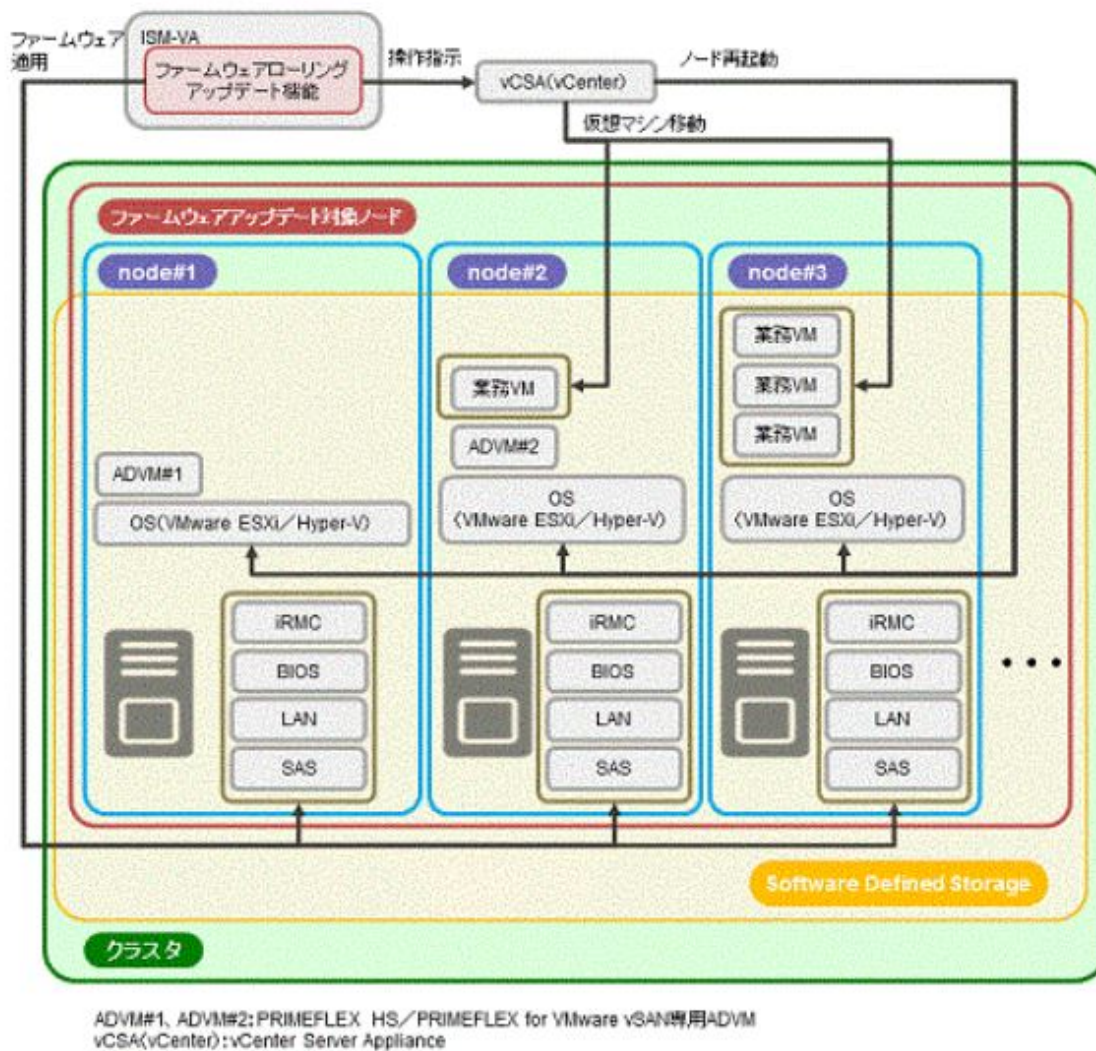
.....

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。

ISM 2.4.0.b 以降では、OnlineアップデートとOfflineアップデートのファームウェアデータがインポートされている場合は、Onlineアップデートのファームウェアが適用されます。UpdateDVDにOnlineとOfflineのファームウェアデータがどちらも含まれている場合は、Onlineアップデートが優先されます。

.....

図2.25 ファームウェアローリングアップデート機能の概要



2.12.4.1 ファームウェア管理機能との連携

ファームウェア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。

ISM 2.4.0.b以降では、OnlineアップデートとOfflineアップデートのファームウェアデータがインポートされている場合は、Onlineアップデートのファームウェアが適用されます。

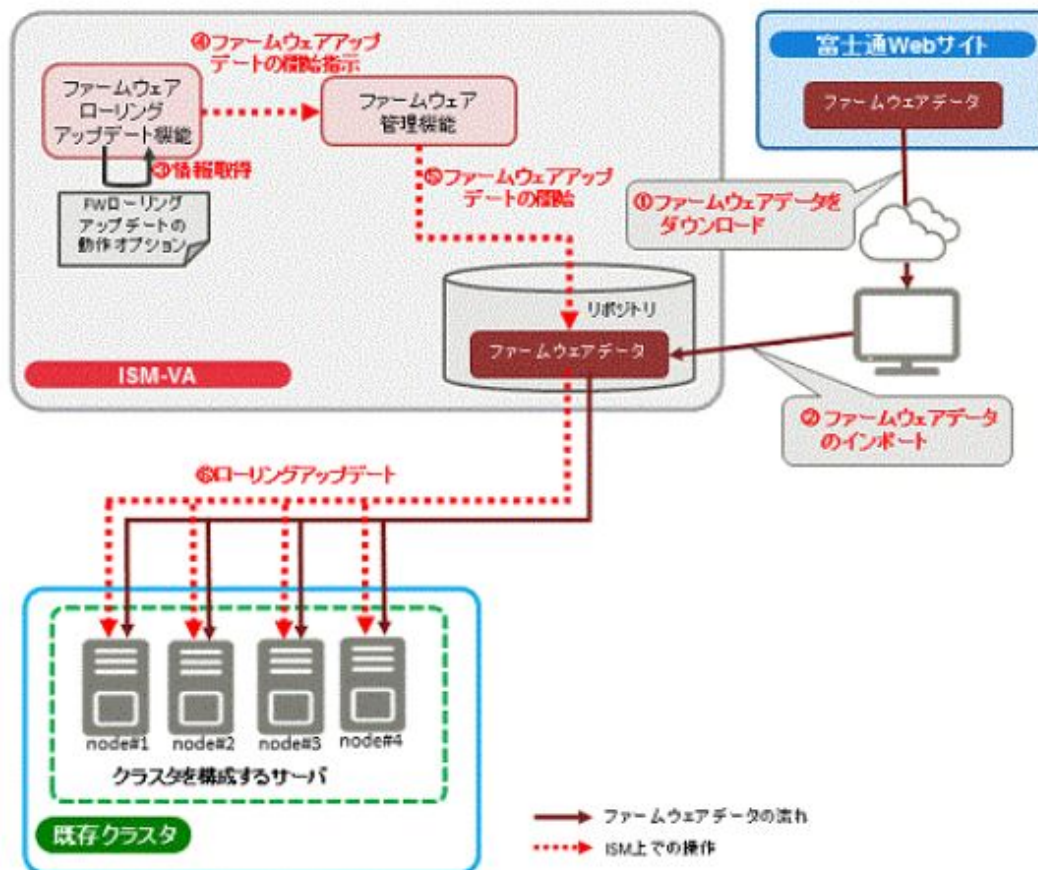


注意

- ファームウェアローリングアップデート機能を実行する前に、ファームウェアデータをISMにインポートしてください。
ファームウェアデータのインポートについては、「[2.13.2 リポジトリ管理機能](#)」を参照してください。
- ファームウェア管理機能のファームウェアアップデート処理がエラー終了したノードがあっても、アップデートが正常に完了したノードに対しては再起動が実行され、ファームウェアが適用されます。

以下にファームウェア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2.26 ファームウェア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



2.12.4.2 タスク一覧

ファームウェアローリングアップデート機能は、「FWローリングアップデート」ウィザードから実行できます。ファームウェア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。ファームウェアローリングアップデート機能のタスク名は「Firmware Rolling Update」です。タスク一覧からタスクタイプが「Firmware 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、ファームウェアアップデート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2.16 Online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
Firmware Rolling Update (ファームウェア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と再起動を行います)	1. Prep Check 2. Migrate VM to Another Node & Set Maintenance Mode 3. Migrate VM to Another Node & Set Maintenance Mode 4. Update Firmware (online) 5. Shutdown Node 6. Boot Node	1. ファームウェアローリングアップデートの実行条件をチェックします 2. 対象ノード上で稼働しているVMを回避ノードへ移動します [注1] 3. ノードをメンテナンスモードに設定します 4. ファームウェアデータをOnlineで適用します 5. ノードをシャットダウンします

処理名	設定項目名	設定項目内容
	7. Unset Maintenance Mode & Migrate VM to Target Node 8. Unset Maintenance Mode & Migrate VM to Target Node 9. Post Check	6. ノードを起動します 7. ノードのメンテナンスモードを解除します 8. 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] 9. ファームウェア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。

表2.17 Offlineアップデートサブタスクの処理一覧 (ISM 2.4.0.b 以降)

処理名	設定項目名	設定項目内容
Firmware Rolling Update (ファームウェア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と再起動を行います)	1. Prep Check 2. Migrate VM to Another Node & Set Maintenance Mode 3. Migrate VM to Another Node & Set Maintenance Mode 4. Shutdown Node 5. Update Firmware (offline) 6. Boot Node 7. Unset Maintenance Mode & Migrate VM to Target Node 8. Unset Maintenance Mode & Migrate VM to Target Node 9. Post Check	1. ファームウェアローリングアップデートの実行条件をチェックします 2. 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] 3. ノードをメンテナンスモードに設定します 4. ノードをシャットダウンします 5. ファームウェアデータをOfflineで適用します 6. ノードを起動します 7. ノードのメンテナンスモードを解除します 8. 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] 9. ファームウェア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。

2.13 ISM運用基盤の機能

ISMの運用基盤となる各機能について説明します。

- ・ [2.13.1 ユーザー管理機能](#)
- ・ [2.13.2 リポジトリ管理機能](#)
- ・ [2.13.3 Emulex OneCommand Manager CLI、Qlogic QConvergeConsole CLIの導入](#)
- ・ [2.13.4 タスク管理](#)
- ・ [2.13.5 ISM-VA管理機能](#)

- ・ [2.13.6 仮想化管理ソフトウェア管理機能](#)
- ・ [2.13.7 共有ディレクトリ管理機能](#)
- ・ [2.13.8 ISM連携管理機能](#)
- ・ [2.13.9 他ソフトウェア連携機能](#)

2.13.1 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2.27 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](#)
- ・ [ISM初期設定後の必要なユーザーの作成](#)
- ・ [ユーザー管理機能の操作](#)
- ・ [Microsoft Active DirectoryまたはLDAPとの連携](#)

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、ユーザーロールによっ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。
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		
	Operatorロール		
	Monitorロール		
その他のグループ (Administratorグループ以外)	Administratorロール		
	Operatorロール		
	Monitorロール		

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)



ー 上記の表示の場合、以下のユーザー属性を持つユーザーが操作を実行できます。

- 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

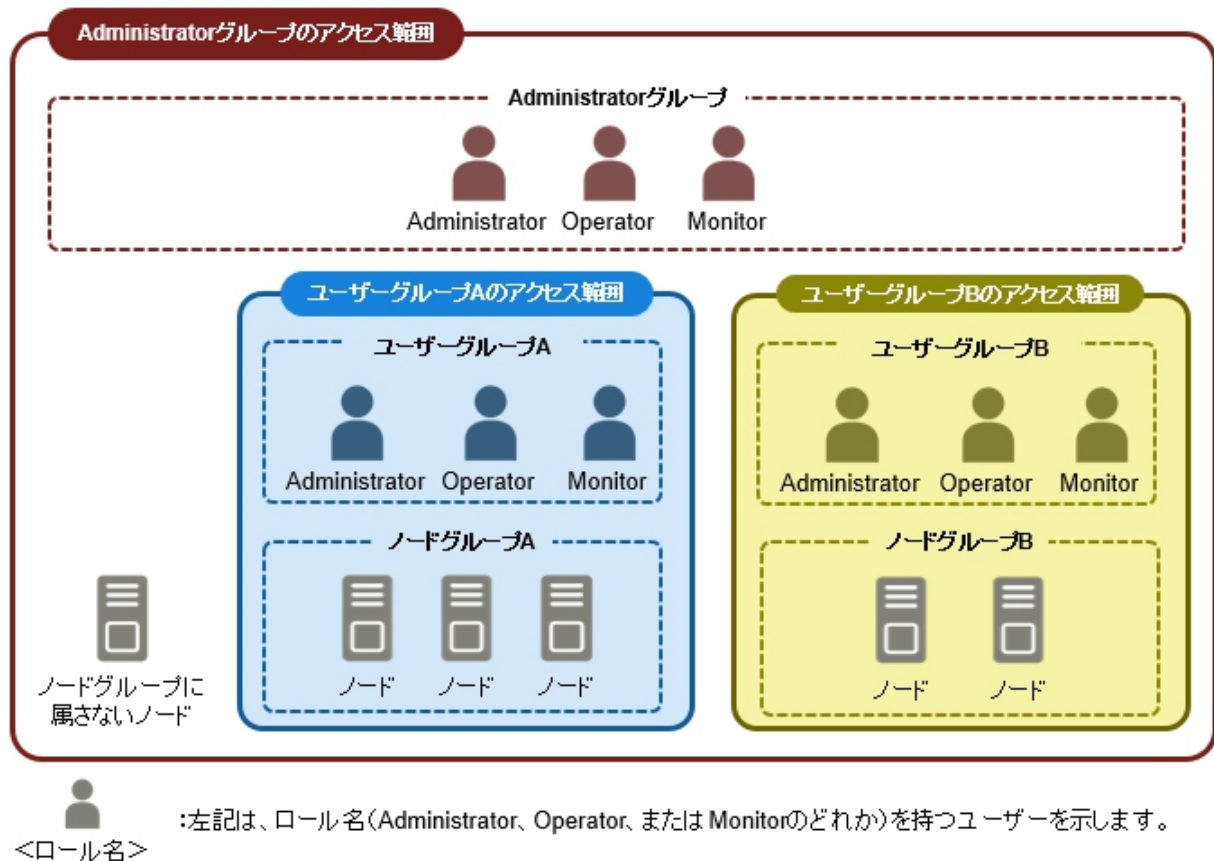
- グレーアイコンで示される、Monitorロールを持つユーザーは、機能を実行できません。

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るだけで、実行できる操作は同じです。

図2.27 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

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

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 ($1 \leq n \leq 24$)	「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	1～32(バイト) (推奨値:8(バイト))	
使用文字種類	- 限定しない(推奨値) - 数字、小文字、大文字、特殊文字のうち最低n種類使用する ($2 \leq n \leq 4$)	
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。

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

—すでに作成されているユーザーについて、ISM 2.0.0.dパッチ以前のバージョンからISM V2.4へアップデートした場合の注意事項を以下に示します。

- パスワードの有効期限は、パッチを適用したときから計算されます。
- ユーザーパスワードポリシーは、以下のように設定されます。
 - パスワードの長さ:1(バイト)
 - 使用文字種類:限定しない
 - ユーザー名と同じパスワード:許可する
 - 有効期限:無期限
 - 期限超過後のアクション:警告メッセージのみ出す

- 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えると、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	2～60(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。
アカウントロックしきい値	6～256(回) (初期値:6(回))	ログインを連続して失敗し、一定時間ログインが禁止される際のしきい値となる回数です。
アカウントロック期間	1～1440(分) (初期値:30(分))	ログインを連続して失敗後、一定時間ログインが禁止される際の時間です。



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。

- ー ログインが成功した場合
- ー 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

ISM初期設定後の必要なユーザーの作成



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。

ユーザーの作成は、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。
詳細は、『操作手順書』の「2.7.4.1 ノードグループを追加する」を参照してください。
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)。
詳細は、『操作手順書』の「2.7.4.2 ノードグループを編集する」を参照してください。
4. ユーザーグループを作成します。
詳細は、『操作手順書』の「2.7.2.1 ユーザーグループを追加する」を参照してください。
5. ユーザーグループに所属するユーザーを登録します。
詳細は、『操作手順書』の「2.7.1.1 ユーザーを追加する」を参照してください。

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LDAPと連携
- ノードグループを管理

ユーザー管理機能では、操作ユーザーにより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、SVS 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

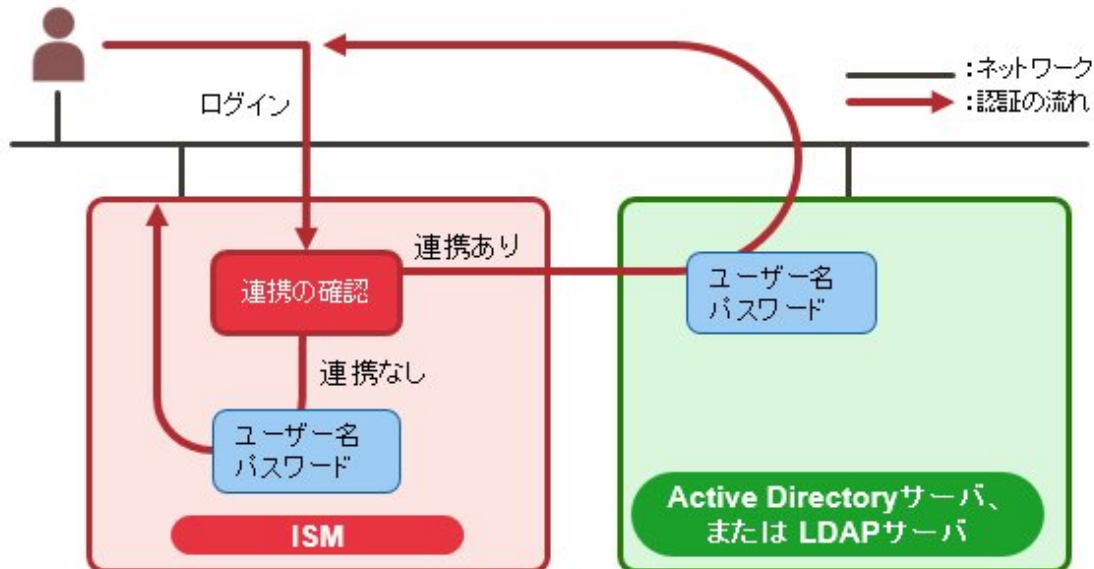
ユーザーグループ名を変更する場合は、事前に以下のタスクが実行中でないことを確認してください。

- 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

Microsoft Active DirectoryまたはLDAPとの連携

Microsoft Active DirectoryまたはLDAP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2.28 ISMとMicrosoft Active Directory／LDAPとの連携イメージ



1. ユーザーがログインします。
 - ユーザーが連携対象であった場合
Microsoft Active DirectoryまたはLDAPで認証を行います。
 - ユーザーが連携対象でない場合
ISMで認証を行います。

注意

- administratorユーザーは、Microsoft Active DirectoryまたはLDAP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LDAPと連携できません。
- Microsoft Active Directory名またはLDAPサーバ名にFQDN名を指定する場合、事前にDNSサーバをISMに設定する必要があります。
- [設定]-[ユーザー]-[LDAPサーバ設定]で指定した内容で、ディレクトリサーバと接続できない場合、ディレクトリサーバ情報はエラーとなって設定できません。
- ディレクトリサーバは、プライマリーとセカンダリの2つ指定できます。2つ指定した場合、現在使用中のサーバと応答できなくなったときは、もう一方のサーバを使用します。
- 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ディレクトリにアップロード後、指定してください。
 - 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サーバ名に指定してください。
- ディレクトリサーバとの接続に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。

ー SSL証明書を設定してください。

- ・ ディレクトリサーバで、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サーバの設定で、パスワードを変更してください。

2.13.2 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。



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 リポジトリの必要容量の見積り
- ・ 3.7 仮想ディスクの割当て
- ・ 『操作手順書』の「2.7.2 ユーザーグループを管理する」

2.13.2.1 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。
- ・ 富士通の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よっ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 (11.15.09版以降) [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 http://azby.fmworld.net/app/customer/driversearch/ia/drviaindex http://support.ts.fujitsu.com/globalflash/ManagementController/
PRIMERGY本体 BIOS	BIOS	ServerView Suite Update DVD (11.15.09版以降) [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

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
		http://azby.fmworld.net/app/customer/driversearch/ia/drviaindex http://support.ts.fujitsu.com/globalflash/SystemBoard/
PCIカード	FC	ServerView Suite Update DVD (11.15.09版以降) [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 http://support.ts.fujitsu.com/globalflash/FibreChannelController/
	CNA	ServerView Suite Update DVD (11.15.09版以降) [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 http://support.ts.fujitsu.com/globalflash/LanController/
	SAS	ServerView Suite Update DVD (11.15.09版以降) [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 http://support.ts.fujitsu.com/globalflash/ScsiController/
	RAID	ServerView Suite Update DVD (11.15.09版以降) [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 http://support.ts.fujitsu.com/globalflash/ScsiController/
	LAN	ServerView Suite Update DVD (11.15.09版以降) [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 http://support.ts.fujitsu.com/globalflash/LanController/
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 http://www.fujitsu.com/jp/products/computing/servers/primequest/download/
PRIMERGY BXシャーシ (MMB)	MMB	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 http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ http://support.ts.fujitsu.com/globalflash/BladeSystem/
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 http://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 http://eservice.fujitsu.com/supportdesk/ [注3]
	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 http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/
	LAN Switch (PY CB Eth Switch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 http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/ http://support.ts.fujitsu.com/globalflash/BladeSystem/
	LAN Switch (Cisco Systems Nexus シリーズ、Cisco Systems Catalystシ リーズ)	富士通の担当営業/SE、またはサポートに連絡して入手してください。
	FC Switch	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 http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/
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 http://eservice.fujitsu.com/supportdesk/ [注3]

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
		http://www.fujitsu.com/jp/products/computing/storage/download/ [注4]

[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。

<http://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/ドライバ名称(部分一致可)」欄に「Update DVD」と入力して検索してください。ISMは、11.15.09版以降のServerView Suite Update DVDに対応しています。

[注2]: SupportDesk-Webについては、以下のURLを参照してください。

<http://eservice.fujitsu.com/supportdesk/>

インポートの手順は「富士通の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」を参照してください。

[注3]: ご利用にはSupportDesk契約が必要です。

[注4]: ご利用には「富士通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

- 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]を選択します。
- 画面左側のメニューから[インポート]を選択します。
- [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。
- [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
共有ディレクトリから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をマウントしておく必要があります。
共有ディレクトリの設定、マウント方法の詳細は、「[2.13.7 共有ディレクトリ管理機能](#)」を参照してください。
- [ファイル]でISOイメージを指定します。
- [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サーバに転送したファイルはインポートが完了したあととは不要です。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」を選択した場合、[共有ディレクトリ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とのマウントを解除します。

富士通の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

- 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]を選択します。
- 画面左側のメニューから[インポート]を選択します。
- [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。
- [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。
- [ファイル]でインポート対象を指定します。
- [種類]でファームウェアの種類を選択します。
- [モデル]でファームウェアのモデルを選択します。
- [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, S5を搭載したサーバ) ・ PRIMEQUEST 3800B
BIOS	・ PRIMERGY (iRMC S3, S4, S5を搭載したサーバ) ・ PRIMEQUEST 3800B [注1]

[注1]: 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。

種類	モデル	バージョン
iRMC	RX100 S8、CX2550 M1、BX920 S4、TX2550 M4、PRIMEQUEST 3800Bなど	iRMCとSDRのバージョン[注1]
BIOS	RX100 S8、CX2550 M1、BX920 S4、TX2550 M4、PRIMEQUEST 3800Bなど	BIOSのバージョン[注1]
MMB	BX900 S2	ファームウェアのバージョン[注1]
PRIMEQUEST	PRIMEQUEST 2400S3など	本体ファームウェアのバージョン[注1]
FC	LPe1250、LPe12002、MC-FC82E	BIOSとFWのバージョン[注2]
	LPe1250、LPe12002以外のLPeXXX、MC-FC162E	ファームウェアのバージョン[注2]
	QLEXXX	BIOSのバージョン[注2]

種類	モデル	バージョン
CNA	OCe10102、OCe14102、MC-CNA112E	ファームウェアのバージョン[注1]
SAS	PSAS CP200i、PSAS CP400i、PSAS CP400e	ファームウェアのバージョン[注1]
RAID	PRAID CP400i、PRAID EP420e、PY SAS RAID Mezz Card 6Gbなど	ファームウェアのバージョン[注1]
LAN	MCX415、MCX416など	ファームウェアのバージョン[注1]
LAN Switch	SR-Xモデル	基本ソフトウェアのバージョン[注1]
	VDXモデル	ファームウェアのバージョン[注1]
	CFXモデル	ファームウェアのバージョン[注1]
	PY CB Eth Switch/IBP 1Gb 36/12	ファームウェアのバージョン[注1]
	PY CB Eth Switch/IBP 10Gb 18/8	ファームウェアのバージョン[注1]
	PY CB Eth Switch 10/40Gb 18/8+2	ファームウェアのバージョン[注1]
	Cisco Systems Nexusシリーズ	NX-OSのバージョン[注1]
	Cisco Systems Catalystシリーズ	IOSのバージョン[注1]
FC Switch	Brocade FC Switch	基本ソフトウェアのバージョン[注2]
ETERNUS DX/AF	ETERNUS DX/AFモデル	ファームウェアのバージョン[注1]

[注1]: バージョンについては、リリースノートを参照してください。

[注2]: 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。

ポイント

- [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を格納したフォルダーを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。
ファームウェアデータがZIP圧縮された状態で提供されている場合、一度ZIPファイルを展開します。展開時に作成されたフォルダーを再度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サーバにファームウェアデータ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。
ファームウェアデータがZIP圧縮された状態で提供されている場合、ZIPファイルを展開します。展開時に作成されたフォルダーをISM-VAに転送し、インポートしてください。
- ISM-VAのFTPサーバ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ず、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力し、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」を選択します。
3. [ファームウェア名]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]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。
 - ー 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。
 - ー 富士通の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。

2.13.2.2 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の場合は富士通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。
 - 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

共有ディレクトリから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をマウントしておく必要があります。

共有ディレクトリの設定、マウント方法の詳細は、「[2.13.7 共有ディレクトリ管理機能](#)」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」を選択した場合、[共有ディレクトリ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。

- 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。
- 画面左側のメニューから[DVDインポート]を選択します。
- 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。
- 画面表示に従い、操作を実行します。

2.13.2.3 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、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。

- ServerView Suite DVDのISOイメージを用意します。
- ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
- 画面左側のメニューから[DVDインポート]を選択します。
- [アクション]ボタンから[DVDインポート]を選択します。
- [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

共有ディレクトリから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をマウントしておく必要があります。

共有ディレクトリの設定、マウント方法の詳細は、「[2.13.7 共有ディレクトリ管理機能](#)」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」を選択した場合、[共有ディレクトリ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。

- 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。
- 画面左側のメニューから[DVDインポート]を選択します。
- 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。
- 画面表示に従い、操作を実行します。

2.13.3 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。

<http://software.fujitsu.com/jp/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/ドライバ名称(部分一致可)の欄に「OCManager」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/>

2.13.4 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
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

「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。

2.13.5 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管理機能で利用できるコマンドについては、「[2.13.5.1 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の各種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 ・ デバッグフラグ切替え

2.13.5.1 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

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サーバ追加	ismadm time add-ntpserver
NTPサーバ削除	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

機能	コマンド
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サーバ証明書配置	ismadm sslcert set
SSLサーバ証明書表示	ismadm sslcert show
SSLサーバ証明書出力	ismadm sslcert export
SSLサーバ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

機能	コマンド
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
ホスト名変更	ismadm system modify
障害調査ログ切替え	ismadm system set-debug-flag
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設定

機能	コマンド
採取ディレクトリ表示	ismadm system core-dir-show
採取ディレクトリ設定	ismadm system core-dir-set
採取ディレクトリ解除	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有効状態表示	ismadm security show-tls
SSL/TLS有効化設定	ismadm security enable-tls

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



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。

2.13.6 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 5.5
- VMware vCenter Server 6.0
- VMware vCenter Server 6.5
- VMware vCenter Server 6.7
- Microsoft System Center 2012
- Microsoft System Center 2012R2
- Microsoft System Center 2016
- Microsoft System Center 2019 (ISM 2.4.0.c 以降)
- Microsoft Failover Cluster (Windows Server 2012) [注1]
- Microsoft Failover Cluster (Windows Server 2012R2) [注1]
- Microsoft Failover Cluster (Windows Server 2016) [注1]
- Microsoft Failover Cluster (Windows Server 2019) [注1]
- KVM (Red Hat Enterprise Linux)
- KVM (SUSE Linux Enterprise)
- IPCOM OS 1.x
- OpenStack (Red Hat Enterprise Linux)

[注1]: 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。

2.13.6.1 仮想化管理ソフトウェアの登録



新しく仮想化管理ソフトウェアを登録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。

ー 仮想化管理ソフトウェア名

ISM 全体で、一意な名称を設定してください。

ー IPアドレス

仮想化管理ソフトウェアのIPアドレスを設定してください。

Microsoft Failover Clusterの場合には、クラスタ仮想IPアドレスを登録してください。

OpenStackの場合には、コントローラーノードのIPアドレスを登録してください。

ー タイプ

登録する仮想化管理ソフトの種類を選択してください。

Microsoft Failover Clusterの場合には、Windows Serverのバージョンも指定してください。



注意

Microsoft Failover Clusterを指定した場合は、[アカウント情報]にドメイン名を必ず設定してください。

ー アカウント情報

仮想化管理ソフトウェアのドメイン名、アカウント名、パスワードを設定してください。

ドメイン名は大文字で記入してください。



ポイント

仮想化管理ソフトウェアの種類がOpenStackの場合、プロジェクトは登録したユーザーの主プロジェクトとなります。

ー URL

仮想化管理ソフトウェアのWeb管理画面にアクセスするためのURLを設定してください。

[タイプ]にWeb管理機能を提供する仮想化管理ソフトウェアを指定した場合は、Web管理画面にアクセスするためのURLを設定してください。

ー ユーザーグループ

管理するユーザーグループ名を選択してください。

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。

2.13.6.2 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。

- ・ 仮想ルータ情報

仮想化管理ソフトウェアから取得した仮想ルータ情報は、「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には以下の手順を実行してください。

1. 仮想化管理ソフトウェアで管理されているノードのノード情報を取得します。
2. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択します。
3. 以下のどちらかの方法で情報を取得します。
 - － すべての仮想化管理ソフトウェアから情報を取得する場合は、[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。
 - － 取得対象を限定する場合は、対象の仮想化管理ソフトウェアを選択し、[アクション]ボタンから[情報取得]-[実行]を選択します。

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。

2.13.6.3 仮想化管理ソフトウェアの編集

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

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[編集]を選択します。
3. 情報を編集します。

項目	説明
仮想化管理ソフトウェア名	ISM全体で、一意な名称を設定します。
IPアドレス	仮想化管理ソフトウェアのIPアドレスを設定します。 Microsoft Failover Clusterの場合には、クラスタ仮想IPアドレスを設定してください。 OpenStackの場合には、コントローラーノードのIPアドレスを設定してください。
アカウント情報	仮想化管理ソフトウェアのドメイン名、アカウント名、パスワード、ポート番号を設定します。 ドメイン名は大文字で設定してください。

項目	説明
URL	仮想化管理ソフトウェアがWeb管理機能を提供している場合、Web管理画面にアクセスするためのURLを設定します。
ユーザーグループ名	管理するユーザーグループ名を選択します。

4. [登録]を実行し、情報の内容を反映します。

2.13.6.4 仮想化管理ソフトウェアの削除

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

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。

2.13.7 共有ディレクトリ管理機能

DVDインポートで使用する共有ディレクトリを追加します。

2.13.7.1 共有ディレクトリの追加

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

新しく共有ディレクトリ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]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。
共有ディレクトリパス	共有ディレクトリのパスを設定します。
種類	共有ディレクトリタイプを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。

「共有ディレクトリリスト」画面に追加した共有ディレクトリが表示されます。



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情報を追加できます。

- ・ 指定した共有ディレクトリ情報で、共有ディレクトリをマウントできない場合はエラーとなります。

2.13.7.2 共有ディレクトリの編集

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

ISMに登録されている共有ディレクトリ情報を編集する場合の操作方法を示します。

- 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]-[共有ディレクトリ]を選択します。
- 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。
- 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。
共有ディレクトリパス	共有ディレクトリのパスを設定します。
種類	共有ディレクトリタイプを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	共有ディレクトリのパスワードを設定します。

- [登録]を選択し、情報の内容を反映します。



注意

共有ディレクトリがマウント中の場合は、編集できません。

2.13.7.3 共有ディレクトリの削除

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

ISMに登録されている共有ディレクトリを削除する場合の操作方法を示します。

- 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]-[共有ディレクトリ]を選択します。
- 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。
- [削除]を選択します。



注意

共有ディレクトリがマウント中の場合は、削除できません。

2.13.7.4 共有ディレクトリのマウント



ISMに登録されている共有ディレクトリ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]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の権限について、以下に示します。
 - 読み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

2.13.7.5 共有ディレクトリのマウント解除



マウントされた共有ディレクトリ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]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。

2.13.8 ISM連携管理機能

2.13.8.1 他ISMのステータス情報のリンク表示

ISMで、他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。

リンク			Y
Tokyo DC	 3  1  5	Tokyo	
Kawasaki DC	 2  2	Kawasaki	

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。

- 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。
 - 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。
 - 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
- 表示したい他ISMのCA証明書を登録します。
 詳細は、「[2.13.8.2 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。
- GUIのダッシュボードに[リンク]を追加します。
 - ISMのGUIでグローバルナビゲーションメニューから[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。
 - 上部にある[≡]から[ウィジェット追加]を選択します。
 - 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。
 - [≡]から[レイアウト変更]を選択します。
 - [レイアウト変更中]の[保存]を選択します。
 - ダッシュボードに表示される[リンク]の[Y]を選択します。
 - 「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。

2.13.8.2 他ISMのリンク用の証明書管理

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

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。
 - ー 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。
 - ー 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。

2.13.9 他ソフトウェア連携機能

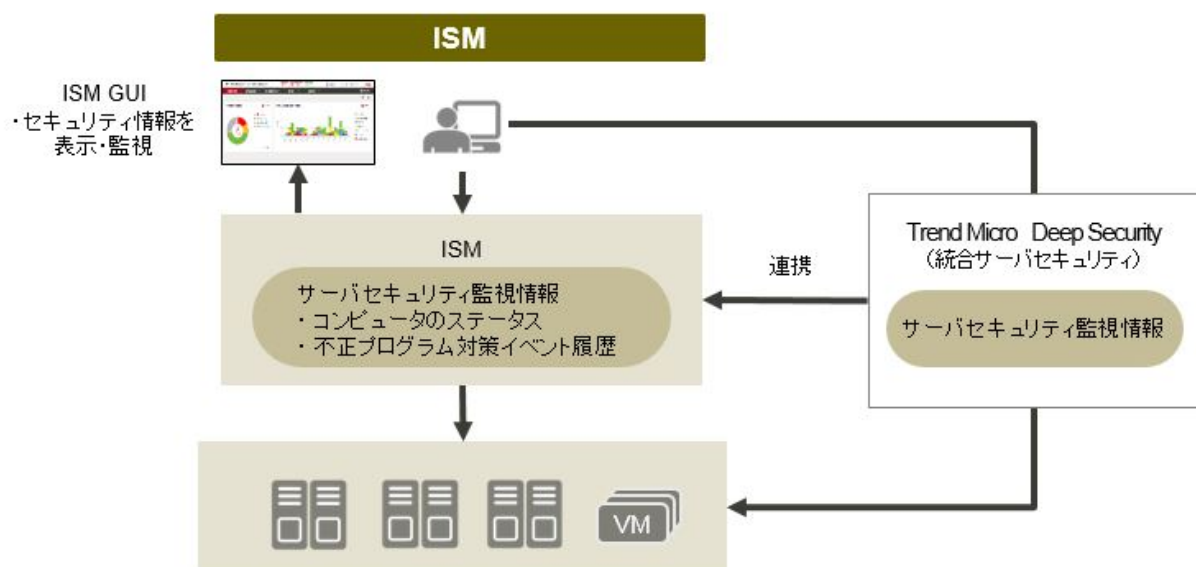
ISMから他のソフトウェアへ連携し、ソフトウェアが管理する情報をISM GUIのダッシュボード画面にウィジェットで表示できます。

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2.29 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2.30 Deep Security連携ウィジェット



2.13.9.1 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Web 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。

P ポイント

Webブラウザ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ブラウザでDeep Security ManagerのWeb GUIを表示し、以下の手順でエクスポートします。

ー Internet Explorerの場合

1. アドレス横の鍵のアイコンを選択し、「証明書の表示」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 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「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。他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「2.8 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) の種類によっ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
```

2.13.9.2 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。

9. 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。 「 2.13.9.1 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。 「 2.13.9.1 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。 「 2.13.9.1 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。 <code>https://<Deep Security ManagerのIPアドレス>:<Deep Security Managerのポート番号></code> 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 Managerの画面が表示される。	ブラウザの[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 ISMの導入

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。

- ・ vSANモデルを構築する場合
『FUJITSU 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」
- ・ S2Dモデルを構築する場合
『FUJITSU Integrated System PRIMEFLEX for Microsoft Storage Spaces Direct 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」

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
- ・ ノード名の設定
- ・ ユーザーの設定

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、「[2.13.6 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) 仮想リソース管理機能の事前設定

「[3.8 仮想リソース管理機能の事前設定](#)」を参照してください。

(9) クラスタ管理機能の事前設定

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。

設定方法については、「[3.9 クラスタ管理機能の事前設定](#)」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 ノード名の設定](#)
- [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 リポジトリの必要容量の見積り 」	○[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 リポジトリの必要容量の見積り 」	○	—
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	○	—

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
		「3.2.1.3 ノード管理データ容量の見積り」		
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 「4.4.2 ISM-VA管理コマンドによるISMのバックアップ／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]

[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。

3.2.1.2 リポジトリの必要容量の見積り

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UpdateDVDの数に応じて異なりますが、通常は10GB以上が使用されます。下表を参照して必要な容量を見積ってください。

用途	操作	必要容量
ファームウェアデータの格納	UpdateDVDのインポート	UpdateDVD1枚当たり7GB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
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	
	ネットワーク統計情報を監視しない場合	ネットワーク統計情報を監視する場合
100ノード以下	20GB	25GB
400ノード以下	80GB	100GB
1000ノード以下	200GB	250GB

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、「[4.5.1.2 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、「[4.5.1.2 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

3.2.2 ネットワークの設計

ISMがサーバを管理するには、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. 「4.4 ISM-VAのバックアップとリストア」の手順に従いバックアップ
4. バックアップしたISM-VAを、「インポート機能によるISM-VAのリストア」の手順に従い本番環境のハイパーバイザーにリストア



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ー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ースは、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。

3.2.3 ノード名の設定

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、「2.13.1 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、FUJITSU Software 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。

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zipファイル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を選択します。
選択するディレクトリは、「Snapshots」、「Virtual Hard Disks」、「Virtual Machines」というディレクトリの親ディレクトリです。
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。

3.3.2 VMware vSphere Hypervisorへのインストール

DVDメディアに含まれるovaファイルを使用してインストールします。

VMware ESXiのバージョンによっ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。

- [VMware ESXi 5.5またはVMware ESXi 6.0へのインストール](#)
- [VMware ESXi 6.5以降へのインストール](#)

VMware ESXi 5.5またはVMware ESXi 6.0へのインストール

1. vSphere Clientを起動し、[ファイル]メニューから[OVFテンプレートのデプロイ]を選択します。
2. ソースの選択画面で、DVDメディアに含まれるovaファイルを選択し、[次へ]を選択します。
3. 「ストレージ」画面で、仮想マシンの保存場所を指定し、[次へ]を選択します。
4. 「ディスクのフォーマット」画面で、[シックプロビジョニング(Lazy Zeroed)]または[シックプロビジョニング(Eager Zeroed)]を選択し、[次へ]を選択します。
5. 「ネットワークのマッピング」画面で、ISMで使用するネットワークを選択し、[次へ]を選択します。
6. [完了]を選択し、OVFテンプレートのデプロイを完了させます。

VMware ESXi 6.5以降へのインストール

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ova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。

3.3.3 KVMへのインストール

DVDメディアに含まれるtar.gzファイルを使用してインストールします。

1. KVMホストの任意のディレクトリに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/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。

```
# cp ISM<Version>.xml /etc/libvirt/qemu
```

ポイント

SUSE Linux Enterprise Serverにインストールする場合は、コピー前またはコピー後のxmlファイルをviなどで直接編集し、<emulator>部分を変更してください。

変更前

```
<emulator>/usr/libexec/qemu-kvm</emulator>
```

変更後

```
<emulator>/usr/bin/qemu-system-x86_64</emulator>
```

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. [仮想マシンマネージャー]を選択し、仮想マシンマネージャーを開きます。
5. 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。
6. 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仮想マシンの詳細画面で[NIC]を選択し、ISM-VAを接続する仮想ネットワークまたはホストデバイスを選択して、[適用]を選択します。

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

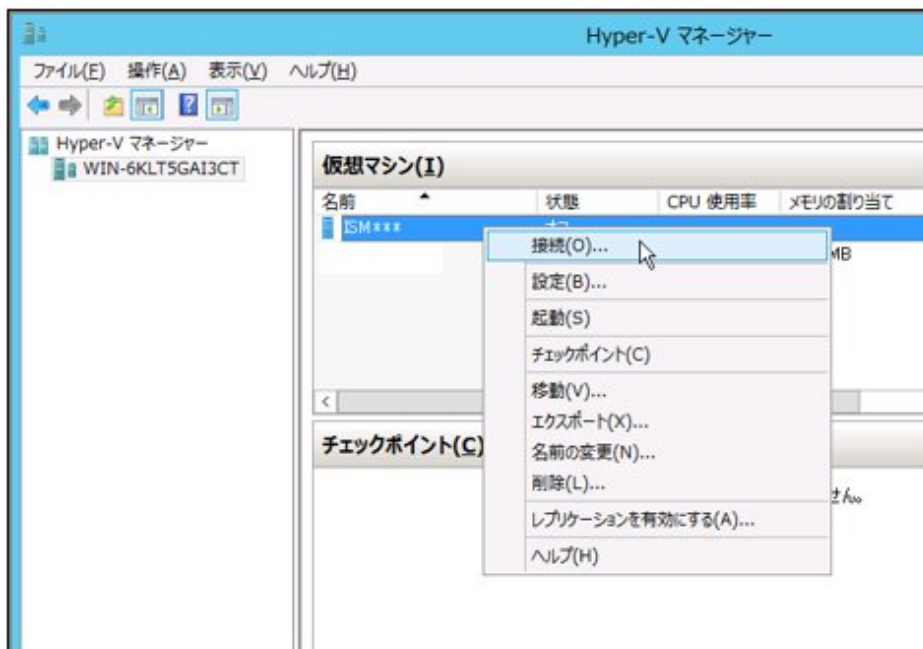
インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

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。

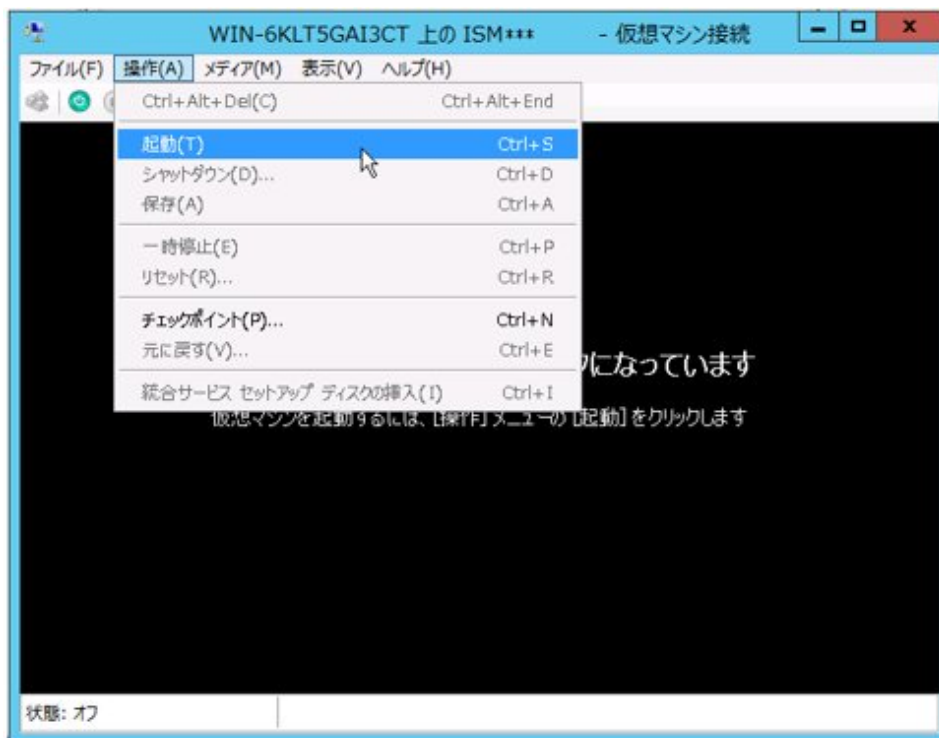
- [3.4.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合 \(初回\)](#)
- [3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合 \(初回\)](#)
- [3.4.1.3 KVMで動作するISM-VAの場合 \(初回\)](#)

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。



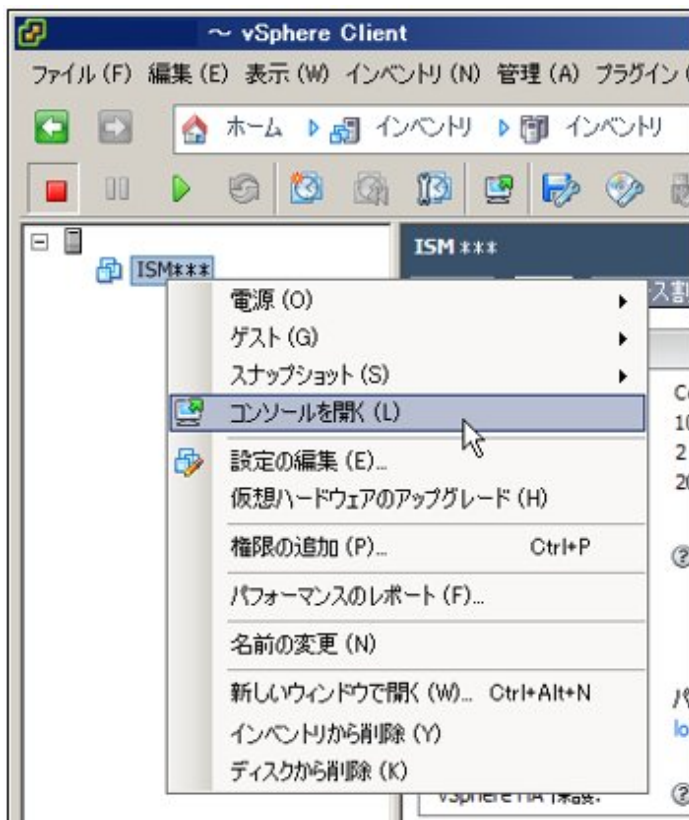
3.4.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(初回)

VMware ESXiのバージョンによっ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。

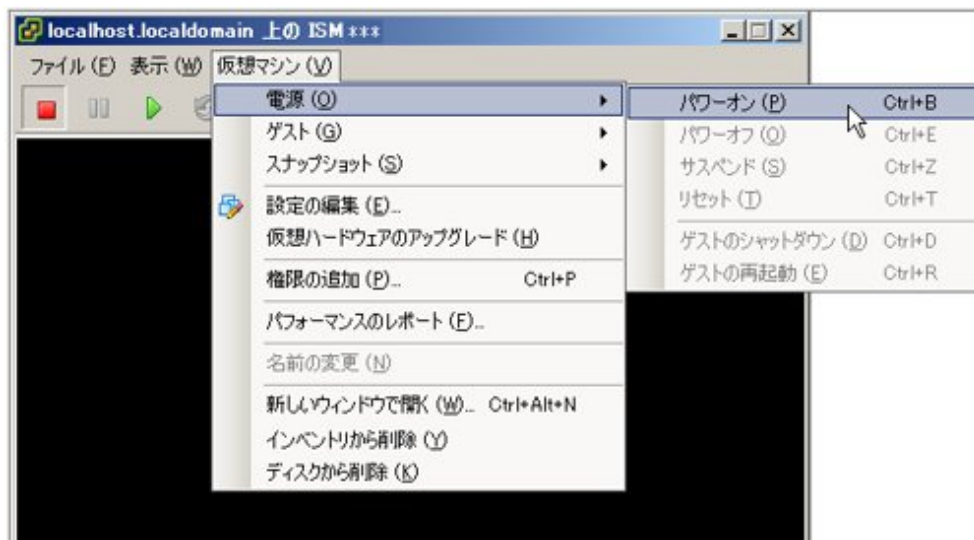
- [VMware ESXi 5.5またはVMware ESXi 6.0の場合](#)
- [VMware ESXi 6.5以降の場合](#)

VMware ESXi 5.5またはVMware ESXi 6.0の場合

1. vSphere Clientで、インストールしたISM-VAを右クリックし、[コンソールを開く]を選択します。

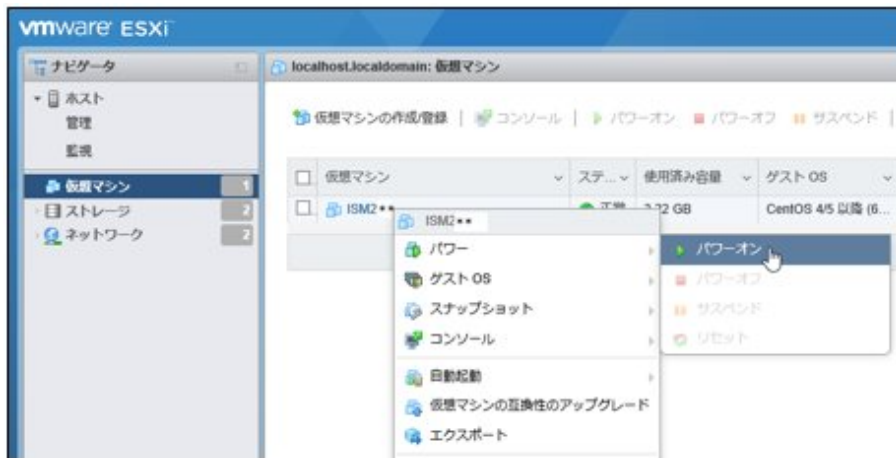


2. 「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。

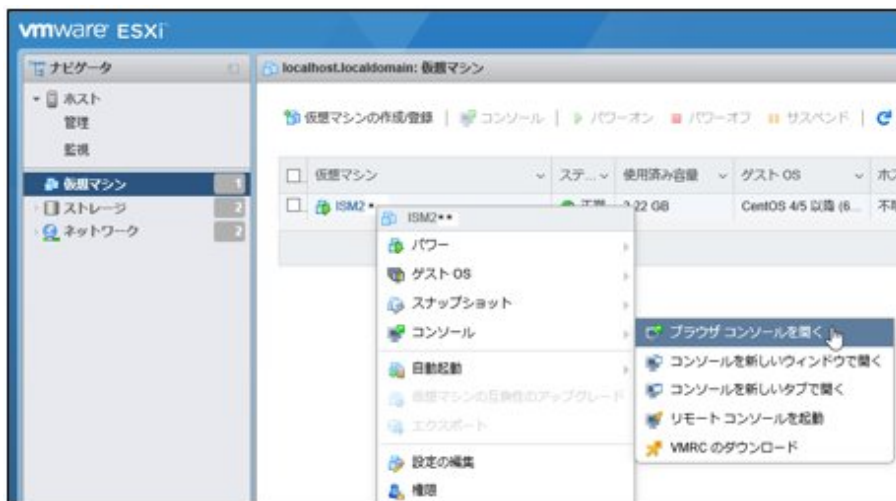


VMware ESXi 6.5以降の場合

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。



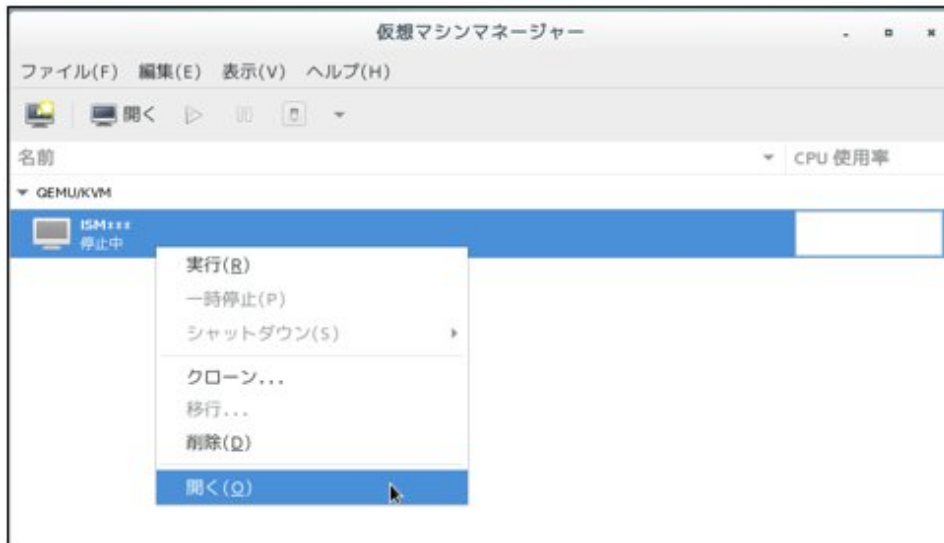
ポイント

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 5.5/6.0/6.5/6.7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)

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。



3.4.2 ISM-VAの初期設定

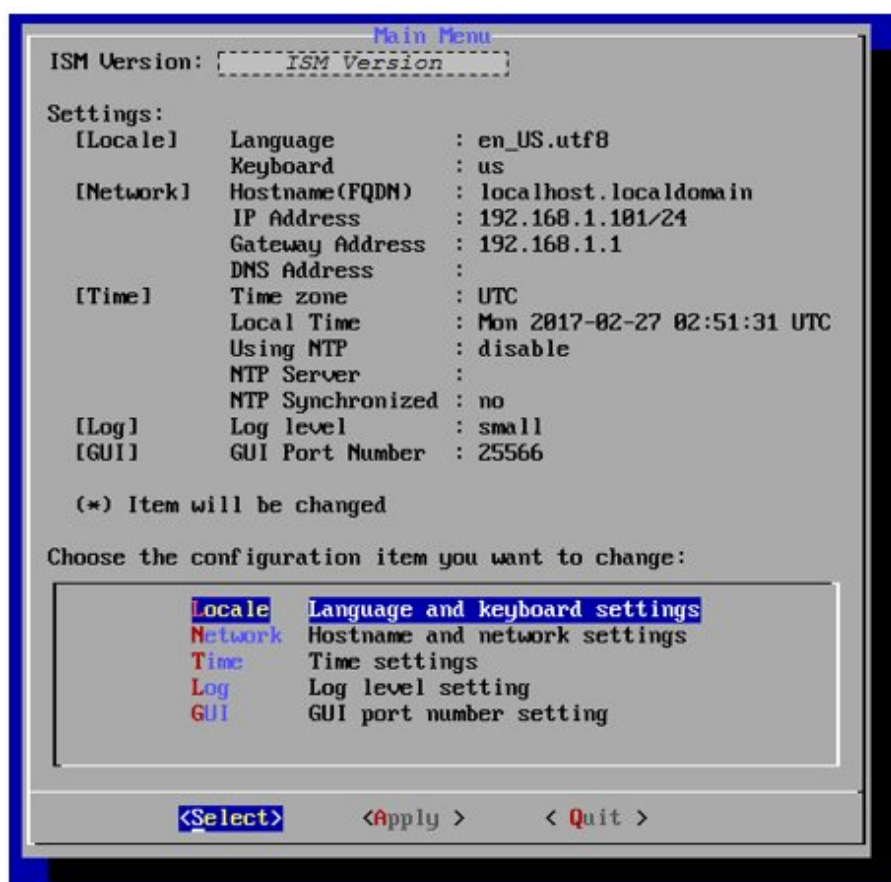
ISM-VA起動後、コンソールの基本設定メニューまたはismadmコマンドを使用して、ISM-VAの基本的な設定を行います。

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
```

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
- 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>

# 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ので、「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。

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3.1 キーマップ一覧

言語名	キーマップ名
日本語	jp

言語名	キーマップ名
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
```

ー 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
```

ー NTPサーバ追加／削除

NTPサーバ追加

```
# ismadm time add-ntpserver <NTPサーバ>
```

NTPサーバ削除

```
# ismadm time del-ntpserver <NTPサーバ>
```

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。

- ー 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
```

- ー ドメイン設定情報を表示する

```
# ismadm kerberos show
```

- ー 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。

- ー 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。ISMでは、サーバ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。

- ・ サーバライセンス

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のライセンスの種類についての詳細は、『入門書』の「1.2 商品体系とライセンス」を参照してください。

ライセンスの登録は、コンソールから登録する方法と、Webブラウザで動作するGUIから登録する方法の2通りあります。

コンソールから登録する方法

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]	[Exp. Date]	[Reg. Date]	[Licensekey]
1	Server	Adv.	-	-	2018-01-01	*****=
2	Node	Adv.	10	-	2018-01-01	*****=

表3.2 コマンド出力結果の説明

項目	説明
[Operation Mode]	動作モード (ISM 2.4.0.b 以降) • Essential • Advanced • Advanced for PRIMEFLEX
[Type]	サーバ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。
[Exp.Date]	ライセンスの有効期限が表示されます。無期限の場合は常に“-”が表示されます。
[Reg.Date]	ライセンスを登録した日時が表示されます。
[Licensekey]	登録済みライセンスキーの文字列が表示されます。

4. ISM-VAを再起動します。

```
# ismadm power restart
```

Webブラウザで動作するGUIから登録する方法

ライセンスを初めて登録する場合

1. 「[3.4.2 ISM-VAの初期設定](#)」を実施します。
2. ISM-VAを再起動します。
3. Webブラウザで動作するGUIを起動します。
4. GUIからadministratorでログインします。
「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。
5. 内容を確認し、[上記内容を確認しました]にチェックを入れます。
6. [同意する]ボタンを選択します。
7. ライセンスキーを以下の方法で登録します。
 - a. 入力フィールドに、ライセンスキーを指定します。
 - b. [適用]ボタンを選択します。
 - c. 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。
 - d. 手順a～cを繰り返し、すべてのライセンスを登録後、[閉じる]ボタンを選択します。

ポイント

[登録済みライセンス]ボタンを選択すると、登録済みのライセンスが一覧表示されます。

8. [ISM-VA再起動]ボタンを選択して、ISM-VAを再起動します。

ノードライセンスを追加で登録する場合

GUIからadministratorでログインし、以下の方法で新しくライセンスを登録します。

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]を選択します。
2. 画面左側のメニューから[ライセンス]を選択します。
「ライセンスリスト」画面が表示されます。
3. [登録]ボタンを選択します。
4. ライセンスキーを以下の方法で登録します。
 - 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指定後、[適用]ボタンを選択します。



注意

GUIからはライセンスの削除はできません。ライセンスの削除は、コンソールから行ってください。詳細は、「[4.8 ライセンス設定](#)」のライセンス削除を参照してください。

3.6 ユーザーの登録

ISMの運用に必要なユーザーを登録します。

ユーザーの登録方法については、「[2.13.1 ユーザー管理機能](#)」を参照してください。

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よっ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によって、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。



ポイント

仮想ディスクの作成方法や接続方法の詳細な手順は、『操作手順書』を参照してください。

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。
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。
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)

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。

- 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
```

- 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

- 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。

- 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。
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。
- ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
- 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
```

- 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)

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。

- 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。

```

# isadm volume add -vol adminvol -disk /dev/sdb
Logical volume "/dev/mapper/adminvol-lv" created.

```

- 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。

```

# isadm volume mount -vol adminvol -gdir /Administrator

```

- 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。

```

# isadm 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

```

- ISM-VAを再起動します。

```

# isadm power restart

```

3.8 仮想リソース管理機能の事前設定

仮想化基盤の運用監視は、仮想リソース管理機能を使用して行えます。

仮想リソースの管理／監視は、ISM GUIの仮想リソースの各管理画面から行えます。

なお、仮想リソース管理GUIの内容および表示項目の説明などについては、ISMのオンラインヘルプを参照してください。



注意

- 仮想リソース管理機能の事前設定については、「[A.1.2 仮想リソース管理機能の事前設定](#)」を参照してください。
- PRIMEFLEX for Microsoft Storage Spaces Directの事前設定の場合、クラスタに対しても「[B.7.1 ドメインユーザーアカウント使用時の設定](#)」の手順5を実施してください。

3.9 クラスタ管理機能の事前設定

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。

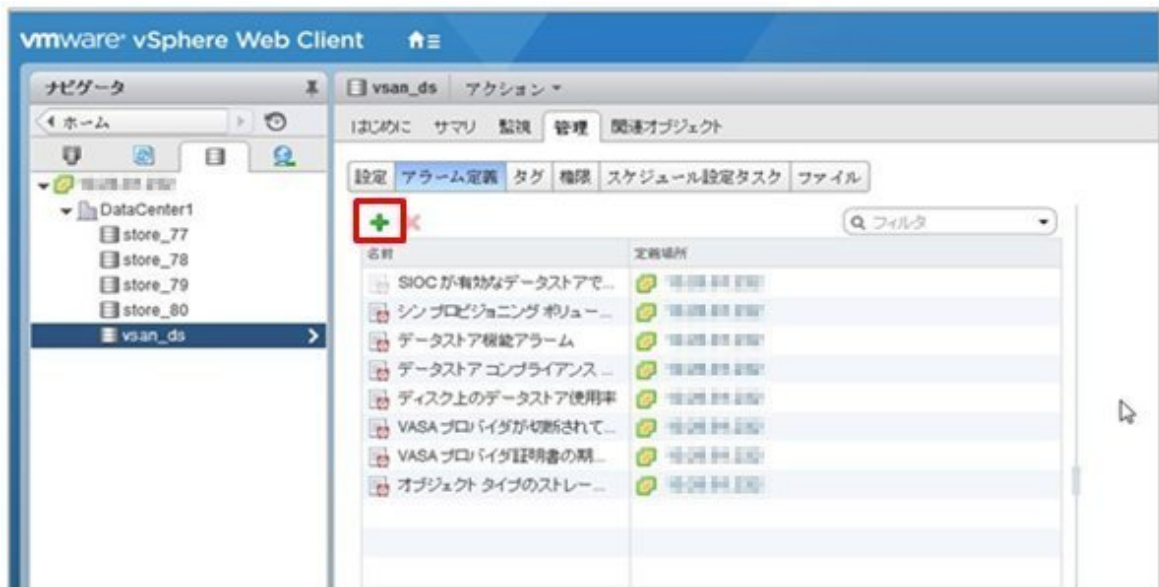
3.9.1 vSANの事前設定

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。vSANのアラーム定義の追加方法について説明します。

1. vSphere Web Client画面を表示し、[ホーム]-[ナビゲータ]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[管理]タブから[アラーム定義]を選択（vCenter Server Appliance 6.0 Update 2の場合）、または[監視]タブから[問題]-[アラーム定義]を選択（vCenter Server Appliance 6.5またはvCenter Server Appliance 6.7の場合）して[+]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。

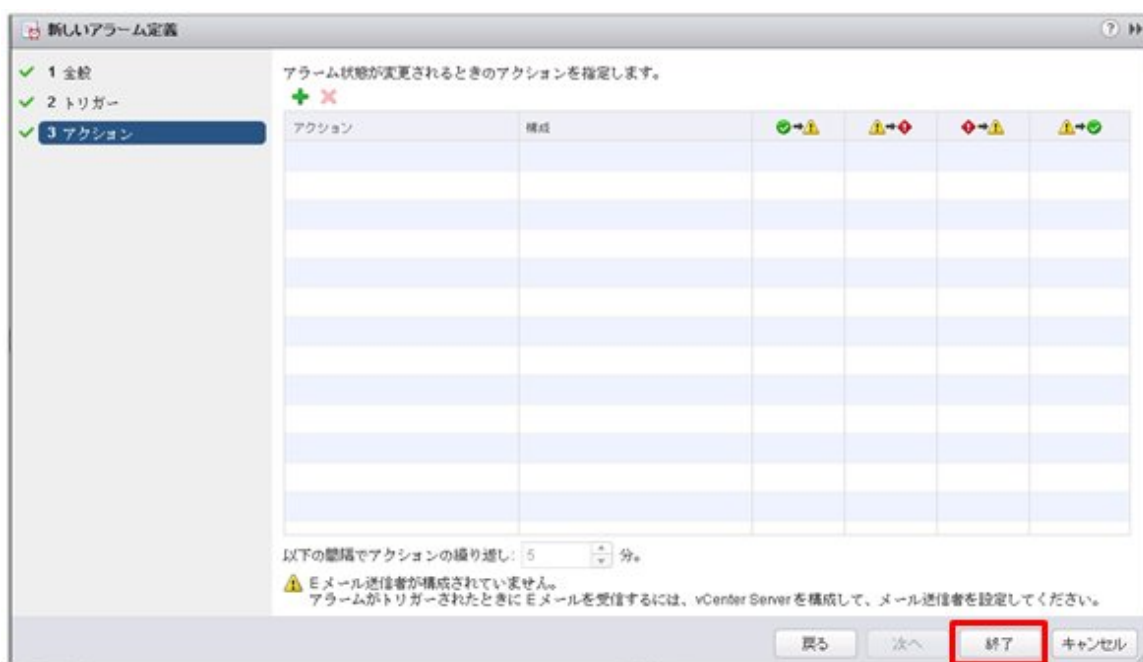


項目	入力内容
アラーム名	ホスト間ネットワークの断線
説明	ホスト間のネットワークが断線した場合のアラーム

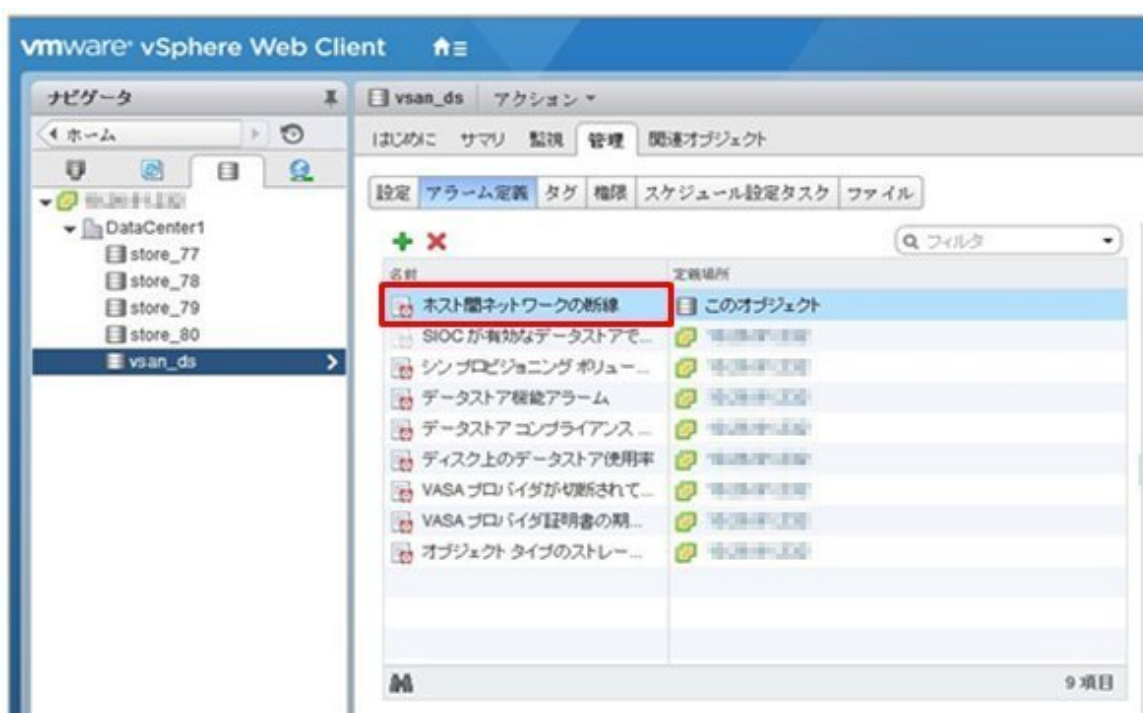
3. 以下の画面で[+]を選択し、各項目を下表のように設定して、[次へ]ボタンを選択します。

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
警告条件	なし
重大条件	切断状態

4. アクションは設定不要です。[終了]ボタン(または[完了]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。



3.9.2 PRIMEFLEX for Microsoft Storage Spaces Directの事前設定

PRIMEFLEX for Microsoft Storage Spaces Directの運用管理を行うために、ISM-VAに対してOS監視の設定、および記憶域プールを構成するすべてのノードに対してCredSSP認証の有効化が必要です。以下の手順で実施してください。

ISMからのWindows OS監視設定

ISMからWindows OSを監視するための設定を行います。

設定手順については、「[B.2 監視対象への設定手順\(OS:Windows\)](#)」、「[B.7 監視対象への設定手順\(仮想化管理ソフトウェア:Microsoft Failover Cluster\)](#)」を参照してください。



- PRIMEFLEX for Microsoft Storage Spaces Directの運用管理には、ドメインユーザーアカウントを使用します。ドメインユーザーアカウント使用時の手順も含め、すべて実施してください。
- 「[B.7.1 ドメインユーザーアカウント使用時の設定](#)」の手順5の設定では、クラスタに対しても実施してください。

ノードへのCredSSP認証有効化設定

記憶域プールを構成するすべてのノードに対してCredSSP認証の有効化を設定します。

記憶域プールを構成するノードは、サーバーマネージャーまたはフェイルオーバークラスタマネージャーから確認できます。



本設定を行わない場合、PRIMEFLEX for Microsoft Storage Spaces Directに対して仮想リソース管理機能が利用できません。

以下にノードに対してのCredSSP認証有効化設定の手順を示します。

- ISM管理者(Administratorグループに属し、Administratorロールを持つユーザー)でノードにログインし、管理者権限でPowerShellを起動します。
- 以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role client -DelegateComputer <対象ノード（フルコンピュータ）名>
```

ドメイン内のすべてのフルコンピュータ名の指定には、ワイルドカード(*)を使用できます。

実行例:

```
Enable-WSManCredSSP -Role client -DelegateComputer *.pfdomain.local
```

CredSSP認証を有効にするかどうかを確認する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。

- 続いて以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role server
```

CredSSP認証を有効にするかどうかを確認する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。

- CredSSP認証の有効化の設定は、以下のコマンドで確認できます。

```
Get-WSManCredSSP
```

以下のようなコマンド結果が表示されれば、CredSSP認証の有効化を設定できています。

例:

```
このコンピューターは、次のターゲットに対する新しい資格情報の委任を許可するよう構成されています:  
wsman/*.pfdomain.local  
このコンピューターは、リモート クライアント コンピューターから資格情報を受け取るように構成されています。
```

3.9.3 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、「[2.13.6 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

- PRIMEFLEX for Microsoft Storage Spaces Directの場合、IPアドレスにはクラスタ代表IPアドレスを設定します。
 - タイプは以下を指定します。
 - vSANの場合
VMware vCenter Server 6.0、6.5、または 6.7
 - PRIMEFLEX for Microsoft Storage Spaces Directの場合
Microsoft Failover Cluster (Windows Server 2016 または Windows Server 2019)
 - 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。

注意

PRIMEFLEX for Microsoft Storage Spaces Directの場合は、「[3.9.2 PRIMEFLEX for Microsoft Storage Spaces Directの事前設定](#)」を先に実施してください。

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。
 - 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: 6.0、6.5、または 6.7
 - Storage Spaces Directの場合
OSタイプ: Windows Server
OSバージョン: 2016または2019
 - OS IPアドレスを入力します。
 - 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。



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 ISMの操作

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

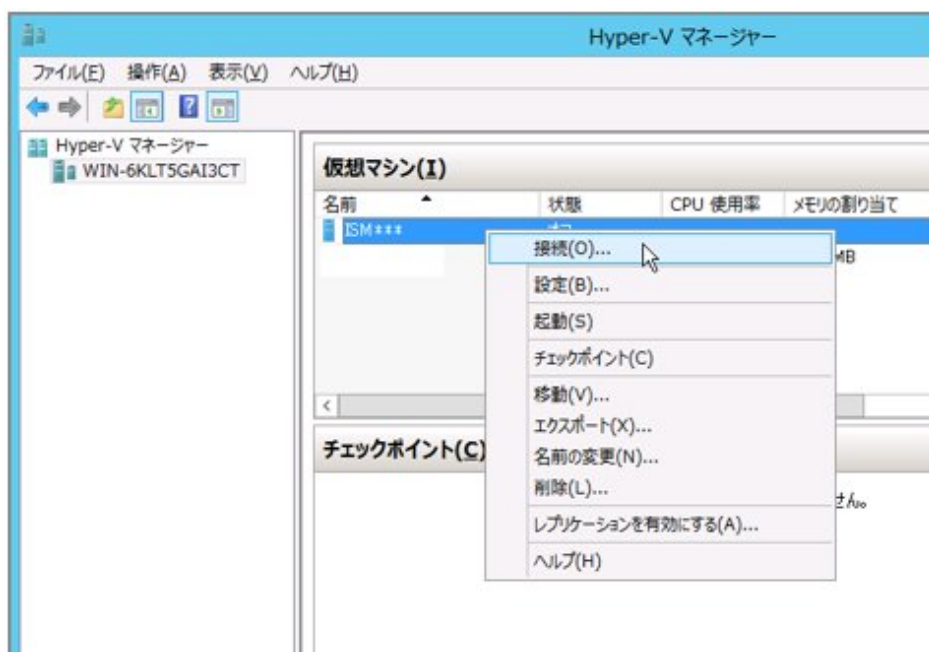
インストール先のハイパーバイザーの機能を使用して、ISM-VAを起動します。管理者権限を持つホストOSのユーザーでISM-VAを起動します。

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。

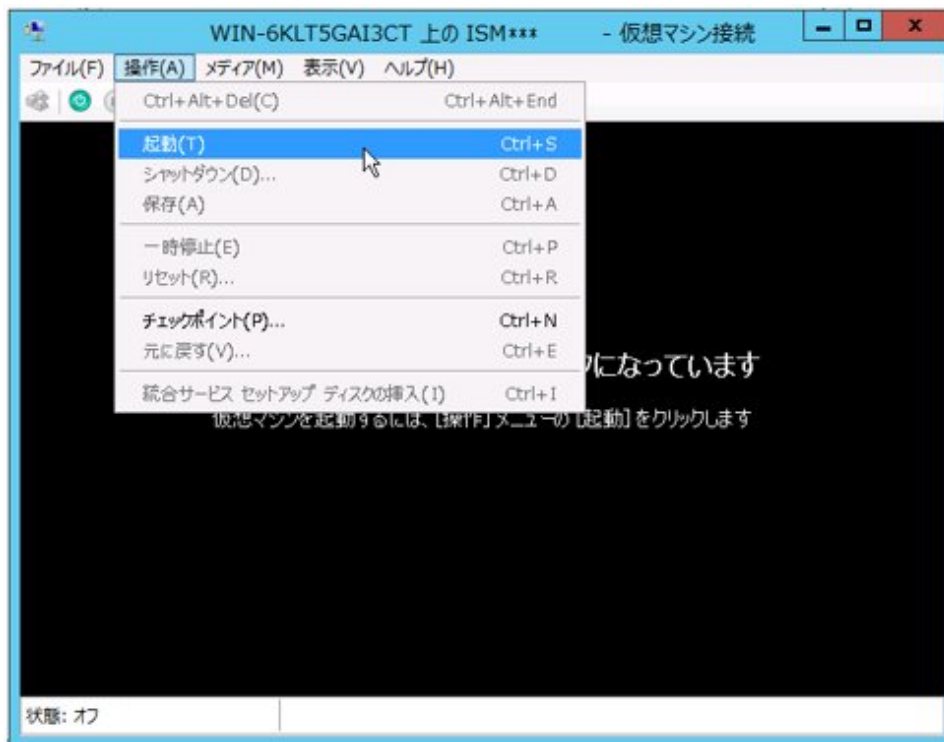
- 4.1.1.1 Microsoft Windows Server Hyper-Vで動作するISM-VAの場合 (導入後)
- 4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合 (導入後)
- 4.1.1.3 KVMで動作するISM-VAの場合 (導入後)

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。



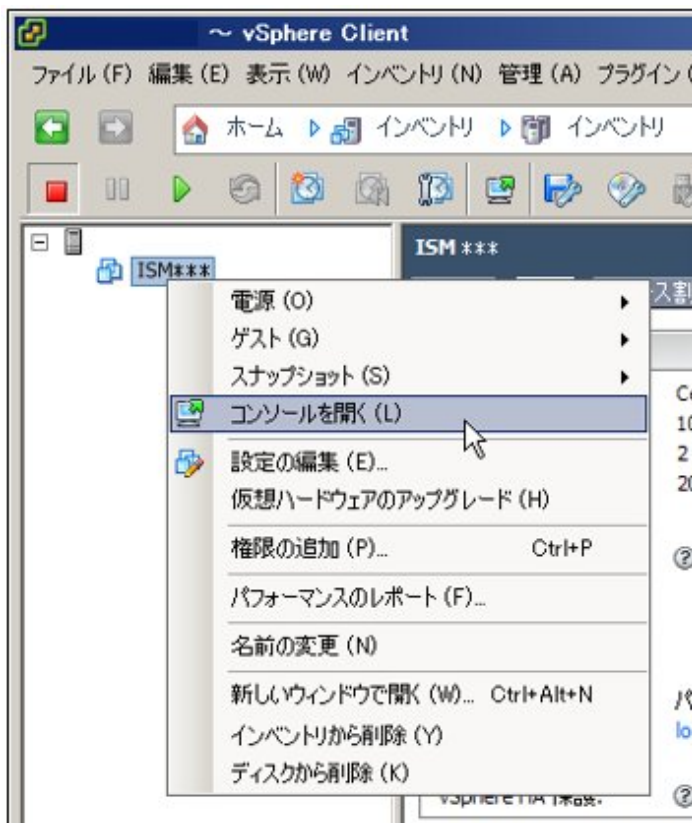
4.1.1.2 VMware vSphere Hypervisorで動作するISM-VAの場合(導入後)

VMware ESXiのバージョンによっ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。

- [VMware ESXi 5.5またはVMware ESXi 6.0の場合](#)
- [VMware ESXi 6.5以降の場合](#)

VMware ESXi 5.5またはVMware ESXi 6.0の場合

1. vSphere Clientで、インストールしたISM-VAを右クリックし、[コンソールを開く]を選択します。

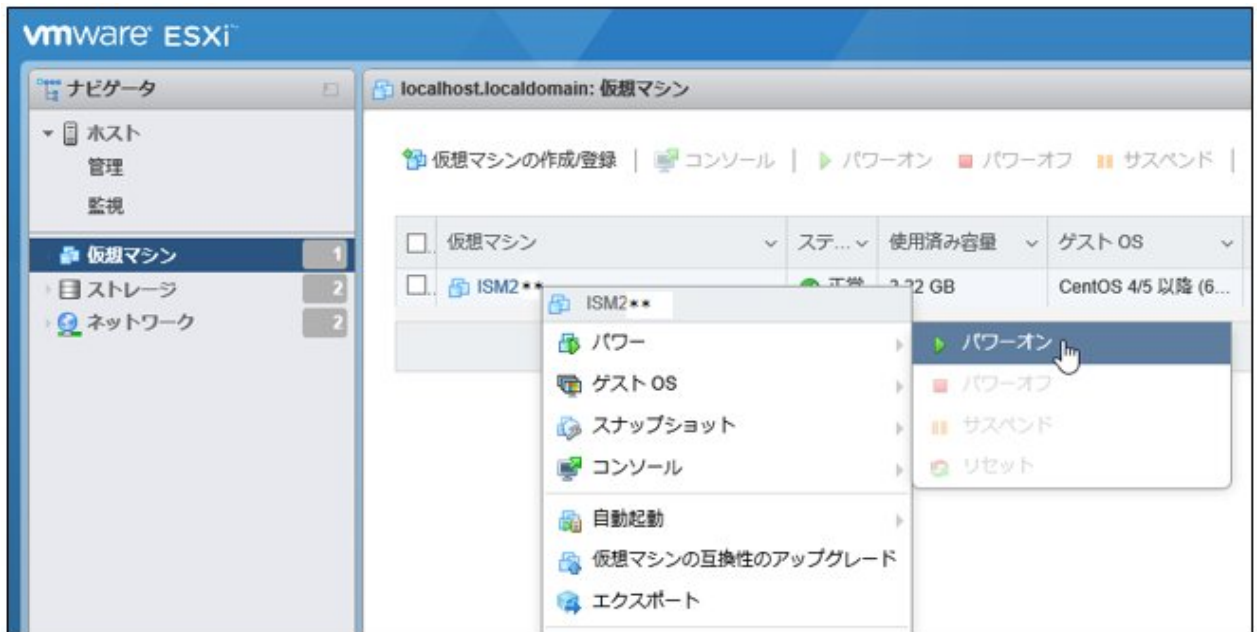


2. 「コンソール」画面の[仮想マシン]メニューから[電源]-[パワーオン]を選択し、ISM-VAを起動します。

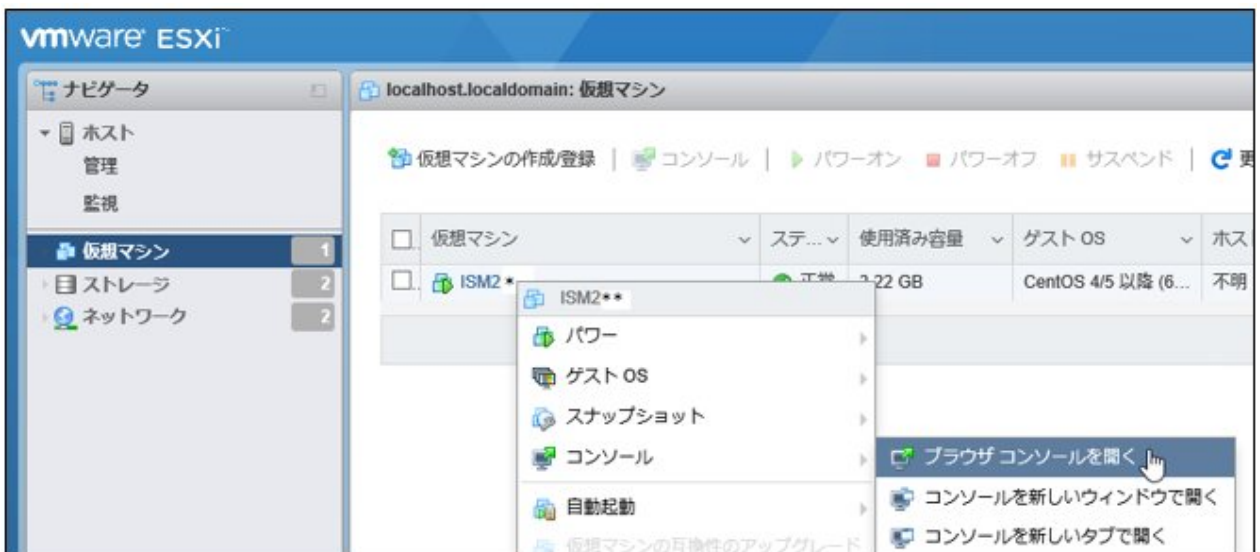


VMware ESXi 6.5以降の場合

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)

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。



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。

4.1.2 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。



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
```

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。

The image shows a terminal window titled "Main Menu". At the top, it displays "ISM Version: ISM Version". Below this, a "Settings:" section lists various configurations: [Locale] Language: en_US.utf8, Keyboard: us; [Network] Hostname(FQDN): localhost.localdomain, IP Address: 192.168.1.101/24, Gateway Address: 192.168.1.1, DNS Address: ; [Time] Time zone: UTC, Local Time: Mon 2017-02-27 02:51:31 UTC, Using NTP: disable, NTP Server: , NTP Synchronized: no; [Log] Log level: small; [GUI] GUI Port Number: 25566. A note states "(*) Item will be changed". Below the settings, it asks "Choose the configuration item you want to change:" and lists five options: Locale (Language and keyboard settings), Network (Hostname and network settings), Time (Time settings), Log (Log level setting), and GUI (GUI port number setting). At the bottom, there are three buttons: <Select>, <Apply>, and <Quit>.

```
Main Menu
ISM Version: ISM Version

Settings:
[Locale]  Language      : en_US.utf8
         Keyboard      : us
[Network] Hostname(FQDN) : localhost.localdomain
         IP Address    : 192.168.1.101/24
         Gateway Address : 192.168.1.1
         DNS Address    :
[Time]   Time zone     : UTC
         Local Time     : Mon 2017-02-27 02:51:31 UTC
         Using NTP      : disable
         NTP Server     :
         NTP Synchronized : no
[Log]    Log level     : small
[GUI]    GUI Port Number : 25566

(*) Item will be changed

Choose the configuration item you want to change:

Locale  Language and keyboard settings
Network Hostname and network settings
Time    Time settings
Log     Log level setting
GUI     GUI port number setting

<Select>  <Apply>  <Quit>
```

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。

The image shows a terminal window titled "You made the following changes:". It lists the changes made: Language: en_US.utf8 -> ja_JP.utf8, Keyboard: us -> jp, Hostname(FQDN): localhost.localdomain -> localhost2.localdomain, IP Address: 192.168.1.101/24 -> 192.168.1.102/24, Gateway: 192.168.1.1 -> 192.168.1.10, DNS: -> 192.168.1.20, Time zone: UTC -> Asia/Tokyo, and Log level: small -> medium. At the bottom, there are two buttons: <Execute> and <Cancel>.

```
You made the following changes:

Language: en_US.utf8 -> ja_JP.utf8
Keyboard: us -> jp
Hostname(FQDN): localhost.localdomain ->
localhost2.localdomain
IP Address: 192.168.1.101/24 -> 192.168.1.102/24
Gateway: 192.168.1.1 -> 192.168.1.10
DNS: -> 192.168.1.20
Time zone: UTC -> Asia/Tokyo
Log level: small -> medium

<Execute>  <Cancel>
```

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-VAのバックアップとリストア

バックアップ／リストアは、以下の方法があります。

- ・ [ハイパーバイザーによるISM-VAのバックアップ／リストア](#)
- ・ [ISM-VA管理コマンドによるISMのバックアップ／リストア](#)



注意

ISM-VAをバックアップ／リストアするときには、以下の点に注意してください。

- ・ バックアップはISM-VAを停止した状態で行ってください。
- ・ バックアップ採取以降にISMの運用で変更した内容は、リストア後に反映する必要があります。
- ・ ISMで以下の連携がある場合、それぞれの管理サーバ(管理VM)も同時にバックアップ／リストアをする必要があるかを判断してください。
 - ー ドメインユーザーとISMのユーザーが連携している場合
 - ー ISMに仮想化管理ソフトウェアの情報を登録している場合

- ・ バックアップソフトを使用する場合、バックアップソフトが提供する以下の機能を使用したバックアップ／リストアはサポートしません。
 - － 仮想マシン (ISM-VA) にエージェントを必要とする機能
 - － ファイル単位の復元

4.4.1 ハイパーバイザーによるISM-VAのバックアップ／リストア



ISM-VAをバックアップ／リストアする前に、ISM-VAを終了してください。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。

エクスポート機能によるISM-VAのバックアップ

ハイパーバイザーのエクスポート機能を使用して、ISM-VA全体をバックアップできます。

ハイパーバイザーをエクスポートする詳細な手順は、『操作手順書』を参照してください。

インポート機能によるISM-VAのリストア

エクスポートしたファイルを「[3.3 ISM-VAのインストール](#)」の手順でインポートすることにより、ISM-VAをリストアします。

4.4.2 ISM-VA管理コマンドによるISMのバックアップ／リストア

ISM-VA管理コマンドを使用して、一部の情報のみを持つバックアップファイルを作成します。

ハイパーバイザーを使用したバックアップ機能とは異なり、稼働中のISM-VAの電源を停止することなくバックアップできます。バックアップ対象を限定しているため短時間で実施でき、外部ストレージに必要となるディスク容量も少なくなります。ただし、リストア完了後に一部の環境設定やDVDインポートなどを再度実施する必要があります。



ISMのバックアップ／リストア前に必要なディスク容量を見積ってください。必要となる容量の目安は、「[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](#)」を参照してください。

ISMのバックアップ対象については、以下の表を参照してください。

凡例：○＝バックアップ可、×＝バックアップ不可

対象	バックアップ可否
ISM-VAの設定情報 (ISM-VA基本設定メニューの設定項目)	○
ノードの管理データ	○
ノードグループの管理データ	○
アカウントの管理データ	○
ユーザーグループの管理データ	○
運用ログ、監査ログ、SNMPトラップ	○
プロファイル	○
電力制御設定[注1]	○
仮想ディスクの割当て情報[注2]	×
リポジット[注3]	×
保管ログ、ノードログ[注3]	×
「/＜ユーザーグループ名＞/ftp」のディレクトリに転送したファイル[注4]	×

対象	バックアップ可否
ファームウェアベースライン定義[注3]	×

[注1]:電力制御設定はバックアップされますが、電力制御は無効化されます。ISMのリストア後に電力制御を行う場合は、電力制御ポリシーを有効にしてください。電力制御ポリシーを有効にする手順は、『操作手順書』の「6.4.3 ラックの電力制御ポリシーを有効化する」を参照してください。

[注2]:ISMをリストアしたあとの仮想ディスクの割当て状態は、以下のとおりです。ISMをリストアしたあと、必要に応じて仮想ディスクの割当てを行ってください。

- ・ ISM-VA全体に割り当てた仮想ディスクの状態は、ISM-VAのバックアップ時の状態になります。
- ・ すべてのユーザーグループに対する仮想ディスクの割当てが解除されています。

[注3]:リポトリ、保管ログ、ノードログ、およびファームウェアベースライン定義は、リストア実行時に削除されます。リストア後に再度リポトリのインポート、ログの収集、およびファームウェアベースライン定義の作成を実施してください。

[注4]:転送したファイルは、リストア実行時に削除されます。ただし、プロファイル管理機能で[インストール後のスクリプト実行]の項目に指定したスクリプトファイルは、バックアップされます。

ISMのバックアップファイルのリストアは、特定のリストア先 (ISM-VAのバックアップ) に対してのみ行うことができます。

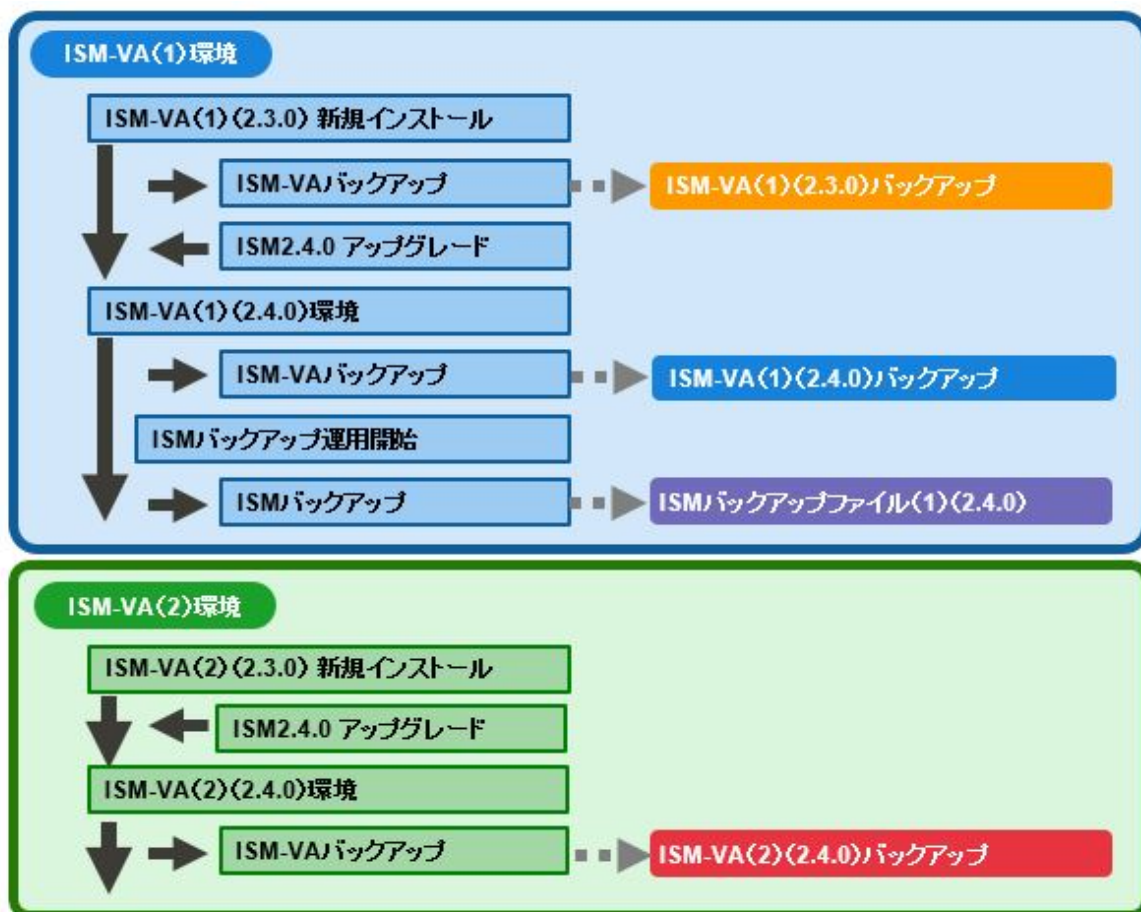
リストア先として使用できるISM-VAの条件は、以下のとおりです。下記以外のISM-VAに対するリストアは未サポートです。

- ・ ISMのバックアップを開始する前にISM-VAをバックアップし、それをリストアした環境であること
- ・ リストア先として使用するISM-VAのバックアップのバージョンと、ISMのバックアップファイルのバージョンが同じであること

以下に例を示します。

ISM-VA(1)(2.4.0)でバックアップしたISMバックアップファイル(1)(2.4.0)のリストア可否について説明します。

ISMバックアップファイル(1)(2.4.0)と各ISM-VAバックアップは、以下の流れで取得したものとします。



ISMバックアップファイル(1)(2.4.0)のリストア可否は以下のとおりです。

凡例: ○=リストア可、×=リストア不可

ISM-VAの環境	リストア先のISM-VA	リストア可否
ISM-VA(1)	ISM-VA(1)(2.4.0)のバックアップをリストアした環境	○[注1]
	ISM-VA(1)(2.3.0)のバックアップをリストアした環境	×[注2]
	ISM-VA(1)(2.3.0)のバックアップをリストア後、ISM 2.4.0にアップグレードした環境	×[注2]
ISM-VA(2)	ISM-VA(2)(2.4.0)のバックアップをリストアした環境	×[注3]

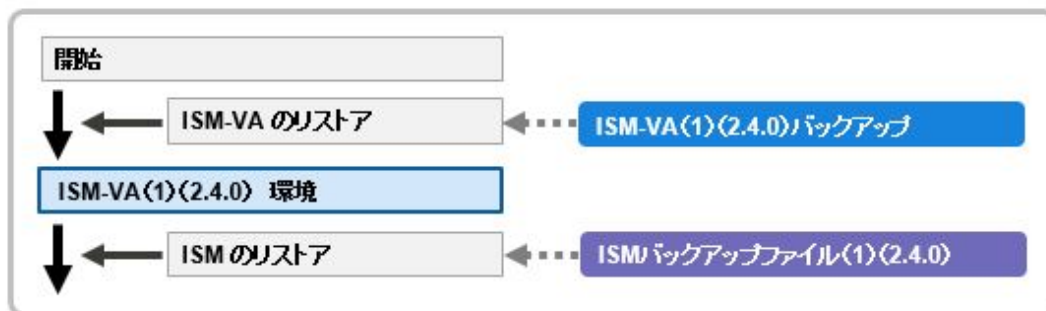
[注1]: 詳細は、「ISM-VA(1)(2.4.0)のバックアップをリストアした環境へのISMのリストア」を参照してください。

[注2]: 詳細は、「ISM-VA(1)(2.3.0)のバックアップをリストアした環境へのISMのリストア」を参照してください。

[注3]: 詳細は、「ISM-VA(2)(2.4.0)のバックアップをリストアした環境へのISMのリストア」を参照してください。

ISM-VA(1)(2.4.0)のバックアップをリストアした環境へのISMのリストア

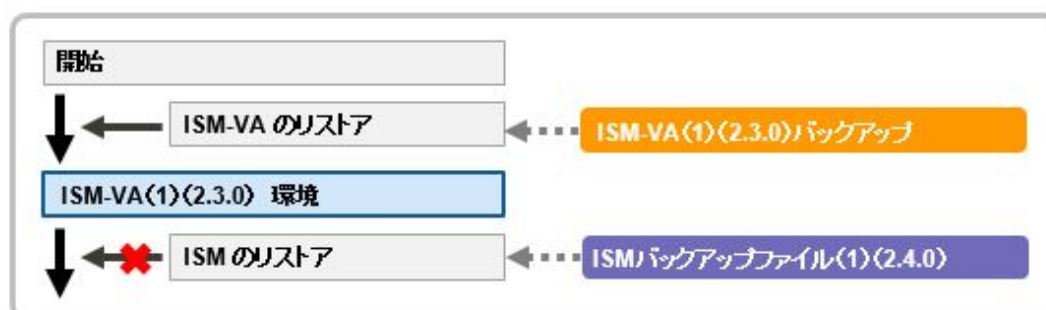
ISM-VA(1)(2.4.0)のバックアップをリストアした環境に対してISMのバックアップファイル(1)(2.4.0)をリストアできます。



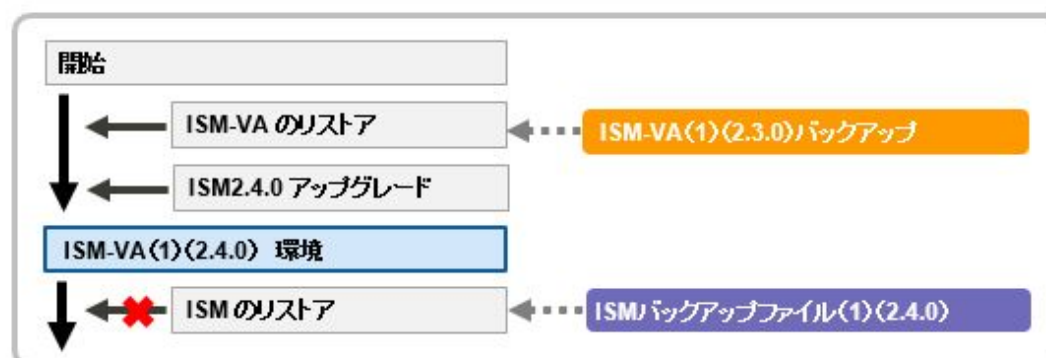
ISM-VA(1)(2.3.0)のバックアップをリストアした環境へのISMのリストア

ISM-VA(1)(2.3.0)のバックアップをリストアした環境に対するISMのバックアップファイル(1)(2.4.0)のリストアは未サポートです。

ISMのバックアップファイルと異なるバージョンのISM-VAのバックアップをリストアした環境に対するISMのリストアは未サポートです。



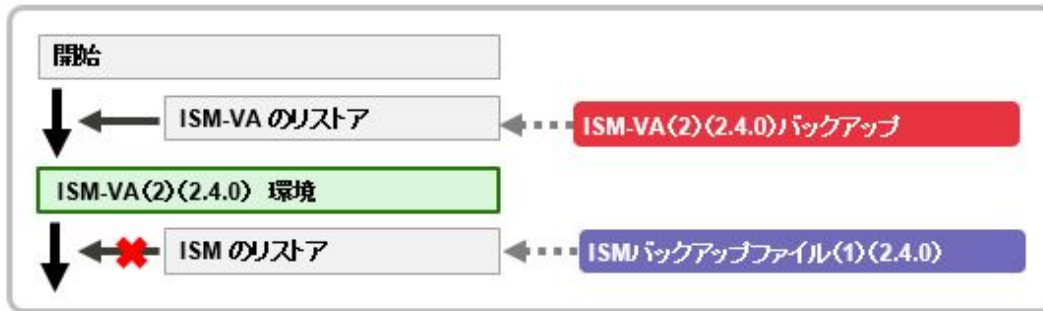
また、ISM-VA(1)(2.3.0)のバックアップをリストア後、ISM 2.4.0にアップグレードした環境に対するリストアも同様に未サポートです。



ISM-VA(2)(2.4.0)のバックアップをリストアした環境へのISMのリストア

ISM-VA(2)(2.4.0)のバックアップをリストアした環境に対するISMのバックアップファイル(1)(2.4.0)のリストアは未サポートです。

ISMのバックアップファイルを作成したISM-VAと異なるISM-VAのバックアップをリストアした環境に対するISMのリストアは未サポートです。



詳細な手順については、『操作手順書』を参照してください。

4.4.2.1 ISMバックアップ

ISMバックアップコマンドは以下のとおりです。

```
# ismadm system backup
```

以下に、ISMバックアップコマンドの実行例を示します。

コマンドを実行すると、空きディスク容量とISMバックアップに必要なディスク容量が表示されます。

十分な空き容量があることを確認し、「Start backup process? [y/n]:」に「y」を入力して[Enter]キーを押します。ISMバックアップを中止するときは、「n」を入力して[Enter]キーを押します。



注意

空き容量が不足している状態でバックアップを実行するとエラーになります。

ISMバックアップコマンド実行例: (※部以降の文言は、実際の画面には表示されません。)

```
# ismadm system backup
[System Information]
Version : 2.4.0 (S2019xxxx-xx) ※動作中のISM-VAのバージョン

[Disk Space Available]
System      : 27000MB          ※System (ISM-VA全体[注1]) の空きディスク容量
/Administrator : 17000MB      ※/Administratorリポジトリの空きディスク容量

[Disk Space Required]
System      : 1200MB          ※バックアップ実行のためSystem (ISM-VA全体[注1]) に必要なディスク容量
/Administrator : 1200MB      ※バックアップ実行のため/Administratorリポジトリに必要なディスク容量

Start backup process? [y/n]:   ※バックアップ実行／中止選択

      (バックアップ処理実行表示)

Output file: /Administrator/ftp/ism<ISMバージョン>-backup-<バックアップ日時>.tar.gz ※バックアップファイル名
```

[注1]:仮想ディスクが割り当てられていないユーザーグループリポジトリも含まれます。

バックアップファイルは、「/Administrator/ftp」配下に出力されますので、FTPで取り出すことができます。



注意

バックアップファイルをFTP転送する際は、バイナリモードで転送してください。

ポイント

空き容量が不足している場合は、以下の対応を行ってください。

- Systemが不足している場合は、「4.6.2 ISM-VA全体に対する仮想ディスクの追加割当て」に従い、仮想ディスクを追加してください。
- 「/Administrator」が不足している場合は、不要ファイルを削除するか、「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」に従い、「/Administrator」に追加の仮想ディスクを割り当ててください。

4.4.2.2 ISMリストア

あらかじめ、ISMリストアするバックアップファイルを「/Administrator/ftp」に用意しておきます。

ISMリストアで指定可能なバックアップファイルは、「4.4.2.3 バックアップファイル一覧表示」で確認できます。

ISMリストアコマンドは以下のとおりです。＜バックアップファイル名＞には、「/Administrator/ftp」に格納されているバックアップファイルを指定します。

```
# ismadm system restore -file <バックアップファイル名>
```

以下に、ISMリストアコマンドの実行例を示します。

コマンドを実行すると、ISM-VAのバージョンとバックアップファイルのバージョン、および空きディスク容量とISMリストアに必要なディスク容量が表示されます。

ISM-VAとバックアップファイルの両方のバージョンが同じで、十分な空き容量があることを確認し、「Start restore process? [y/n]:」に「y」を入力して[Enter]キーを押します。ISMリストアを中止するときは、「n」を入力して[Enter]キーを押します。

ISMリストアコマンド実行例: (※部以降の文言は、実際の画面には表示されません。)

```
# ismadm system restore -file ism2.4.0-backup-20190202102723.tar.gz
[System Information]
  Version : 2.4.0 (S2019xxxx-xx)      ※動作中のISM-VAのバージョン

[Backup File Information]
  Version : 2.4.0 (S2019xxxx-xx)      ※指定されたバックアップファイルのバージョン

[Disk Space Available]
  System      : 45000MB                ※System (ISM-VA全体) の空きディスク容量

[Disk Space Required]
  System      : 2400MB                 ※リストア実行のためSystem (ISM-VA全体) に必要なディスク容量

Start restore process? [y/n]:          ※リストア実行／中止選択
```

注意

- バックアップファイルをFTP転送する際は、バイナリモードで転送してください。
- ismadm system restoreコマンドを実行後は、ISM-VAの再起動が必要です。詳細な手順については、『操作手順書』を参照してください。

4.4.2.3 バックアップファイル一覧表示

「/Administrator/ftp」配下に格納されているバックアップファイル一覧を表示します。

```
# ismadm system backup -list
```

または

```
# ismadm system restore -list
```

バックアップファイル一覧表示コマンド実行例: (※部以降の文言は、実際の画面には表示されません。)

```
# ismadm system backup -list
[System Information]
  Version : 2.4.0 (S2019xxxx-xx)    ※動作中のISM-VAのバージョン

[Disk Space Available]
  System      : 45000MB              ※System (ISM-VA全体) の空きディスク容量

[Backup Files]
-----
  DIRECTORY   : /Administrator/ftp          ※バックアップファイル格納ディレクトリ
  FILE NAME    : ism2.4.0-backup-20190202102723.tar.gz  ※バックアップファイル名
  FILE SIZE    : 200MB                      ※バックアップファイルサイズ
  BACKUP SIZE  : 1200MB                     ※バックアップされたISM-VA情報のサイズ
  BACKUP DATE  : 2019-02-02 10:27:23         ※バックアップの日付／時間
  VERSION      : 2.4.0 (S2019xxxx-xx)       ※バックアップされたISM-VAのバージョン
-----
  DIRECTORY   : /Administrator/ftp
  FILE NAME    : ism2.4.0-backup-20190201151041.tar.gz
  FILE SIZE    : 150MB
  BACKUP SIZE  : 1000MB
  BACKUP DATE  : 2019-02-01 15:10:41
  VERSION      : 2.4.0 (S2019xxxx-xx)
```

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 ISM／ISM-VAの保守資料

ISM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	調査担当者	保守資料
ISMやISM-VAの誤動作を調査	当社技術員	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。

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に提供します。



- 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。
- コマンド実行時、ハイパーバイザーのコンソールに以下のメッセージが表示される場合がありますが、問題はありません。

```
blk_update_request: I/O error, dev fd0, sector 0
```

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。

- 4.5.1.1 障害調査ログ切替え
- 4.5.1.2 障害調査ログレベル切替え
- 4.5.1.3 coreファイル採取ディレクトリの指定
- 4.5.1.4 ISMの保守資料の採取方法

4.5.1.1 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
```

4.5.1.2 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。

4.5.1.3 coreファイル採取ディレクトリの指定

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の場所と、使用されているディレクトリサイズが表示されます。

採取ディレクトリの場所が未設定の場合は、「Default Internal Directory」と表示されます。

ー 採取ディレクトリ設定

```
# ismadm system core-dir-set -dir <ディレクトリ>
```

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を作成し、そのディレクトリ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 採取ディレクトリ解除

```
# ismadm system core-dir-reset
```

採取ディレクトリを未設定状態に戻します。

4.5.1.4 ISMの保守資料の採取方法

ISMの保守資料の採取方法には、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。

4.5.2 ISM for PRIMEFLEXの保守資料

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。

4.5.2.1 クラスタ作成機能のログ

クラスタ作成機能のログは、以下のとおりです。

保守資料	取得方法
クラスタ作成機能のログ	ISM-VAコマンドを使用して採取できます。 詳細は、「 4.5.1.4 ISMの保守資料の採取方法 」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	- PRIMEFLEX for VMware vSAN V1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 (容量の目安:約30KB) - PRIMEFLEX for Microsoft Storage Spaces Direct版 Hyper-Vホスト上の以下の場所より取得してください。 C:\FISCRB\Log\post_script.log (容量の目安:約30KB)
Windows Server上で実行したPowerShellスクリプトの実行ログ	Windows Server上の以下の場所より取得してください。 - PRIMEFLEX for Microsoft Storage Spaces Direct版の新規クラスタを構成するサーバ - PRIMEFLEX for VMware vSAN V1版DNSサーバ 以下の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

4.5.2.2 クラスタ拡張機能のログ

クラスタ拡張機能のログは、以下のとおりです。

保守資料	取得方法
クラスタ拡張機能のログ	ISM-VAコマンドを使用して採取できます。 詳細は、「 4.5.1.4 ISMの保守資料の採取方法 」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	- PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1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 (容量の目安:約30KB) - PRIMEFLEX for Microsoft Storage Spaces Direct版 Hyper-Vホスト上の以下の場所より取得してください。 C:\FISCRB\Log\post_script.log (容量の目安:約30KB)
Windows Server上で実行したPowerShellスクリプトの実行ログ	Windows Server上の以下の場所より取得してください。 - PRIMEFLEX for Microsoft Storage Spaces Direct版のクラスタ拡張時に追加するサーバ - PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版 DNSサーバ

保守資料	取得方法
	以下の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

4.5.2.3 クラスタ管理機能のログ

クラスタ管理機能のログは、以下のとおりです。

保守資料	取得方法
クラスタ管理機能のログ	ISM-VAコマンドを使用して採取できます。 詳細は、「4.5.1.4 ISMの保守資料の採取方法」を参照してください。
vSANのログ	vCenterからvc-supportログを採取します。 詳細は、「4.5.1.4 ISMの保守資料の採取方法」を参照してください。

4.5.2.4 ファームウェアローリングアップデート機能のログ

ファームウェアローリングアップデート機能のログは、以下のとおりです。

保守資料	取得方法
ファームウェアローリングアップデート機能のログ	ISM-VAコマンドを使用して採取できます。 詳細は、「4.5.1.4 ISMの保守資料の採取方法」を参照してください。

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、usrgrp1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)

PV          VG          Fmt Attr PSize PFree
/dev/sda2  centos      lvm2 a-- 19.51g  0
/dev/sdb1  usrgrp1vol  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)

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ブラウザに設定する、SSLサーバ証明書の管理ができます。

4.7.1 SSLサーバ証明書配置

セキュリティを考慮して認証機関などで発行されたSSLサーバ証明書を使用する場合、以下の手順で設定できます。

1. SSLサーバ証明書をISM-VAへ転送します。

転送先:/Administrator/ftp

GUIでの転送方法は、「[4.22 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サーバ証明書を配置します。

転送した「key」ファイルと「cert」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 -cert /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サーバ証明書は、opensslコマンドがインストールされたLinuxサーバ上で、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サーバ証明書表示

ISM-VAに設定されているSSLサーバ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サーバ証明書表示コマンドを実行します。

```
# ismadm sslcert show
```

4.7.3 SSLサーバ証明書出力

ISM-VAに設定されているSSLサーバ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サーバ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 SSLサーバ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、SSLサーバ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. SSLサーバ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

SSLサーバ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>

Internet Explorerや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、ブラウザに応じて以下を選択してください。

- ・ Internet Explorerの場合:[テキストファイル(*.txt)]
- ・ Google Chromeの場合:[すべてのファイル]

実行例:curlコマンドがインストールされたLinuxサーバ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] [Exp. Date] [Reg. Date] [Licensekey]
1 Server Adv. - - 2018-01-01 *****==
2 Node Adv. 10 - 2018-01-01 *****==
```

表4.1 コマンド出力結果の説明

項目	説明
[Operation Mode]	動作モード (ISM 2.4.0.b 以降) ・ Essential ・ Advanced ・ Advanced for PRIMEFLEX
[Type]	サーバ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

項目	説明
	・ 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。
[Exp.Date]	ライセンスの有効期限が表示されます。無期限の場合は常に "-" 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。
[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>
```

注意

ライセンスの登録／削除後は、ISM-VAの再起動が必要です。

ポイント

ライセンスの登録、および種別を含む表示内容の確認は、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。

4.9 ネットワーク設定

ネットワークの設定／表示を行います。

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サーバ追加

```
# ismadm network modify <LANデバイス名> +ipv4.dns <DNSサーバ>
```

実行例:

```
# ismadm network modify eth0 +ipv4.dns 192.168.1.2
```

- ー DNSサーバ削除

```
# ismadm network modify <LANデバイス名> -ipv4.dns <DNSサーバ>
```

実行例:

```
# ismadm network modify eth0 -ipv4.dns 192.168.1.2
```

- 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。

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、「[4.22 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。

- － ISM-VA再起動

```
ismadm power restart
```

- － ISM-VA停止

```
ismadm power stop
```

- － 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 <サービス名>
```

実行例:FTPサーバの個別起動

```
# ismadm service start vsftpd
```

- － 内部サービス個別停止

```
ismadm service stop <サービス名>
```

実行例:FTPサーバの個別停止

```
# ismadm service stop vsftpd
```

- － 内部サービス個別再起動

```
ismadm service restart <サービス名>
```

実行例:FTPサーバの個別再起動

```
# ismadm service restart vsftpd
```

- － 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サーバの個別ステータス表示

```
# ismadm service status vsftpd
```

- － 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サーバの個別有効化設定

```
# ismadm service enable vsftpd
```

- － 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]:
```



- ホスト名は小文字で入力してください。
- 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。



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、「[4.22 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
```

5. プラグイン適用後、ISM-VAを再起動します。

```
# ismadm power restart
```

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。
3. プラグイン削除後、ISM-VAを再起動します。

```
# ismadm power restart
```

4.15 ISM-VA内部のDHCPサーバ

ISM-VA内部のDHCPサービスを起動することで、ISM-VAをDHCPサーバとして使用できます。

DHCPサーバは、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サーバの切替え](#)」で示されている手順により、どちらのDHCPサーバを使用するかを指定します。)

外部のDHCPサーバ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サーバの設定

ISM-VA内部のDHCPサーバの設定をします。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 configuration ? (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、「[4.22 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 dhcprsv set -file <confファイル>
```

実行例:

```
# ismadm dhcprsv 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

```
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

- ISM-VA内部のDHCPサービスを起動する前に、DHCPサーバの設定を行ってください。
DHCPサーバの設定方法は、「[4.15.1 ISM-VA内部のDHCPサーバの設定](#)」を参照してください。
- DHCPサーバが起動状態設定で「(dead)」状態になっている場合は、「[4.15.3 ISM-VA内部のDHCPサーバ情報の確認](#)」の「DHCPサーバメッセージ表示」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サーバ情報の確認

ISM-VA内部のDHCPサーバの情報を表示します。

現在設定されているDHCPサーバの内容の表示、DHCPサーバ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サーバの内容を表示

```
# ismadm dhcpd show-conf
```

- DHCPサーバのメッセージ表示

```
# ismadm dhcpd 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 dhcpd 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 dhcpd 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 dhcpd export-sample -dir /Administrator/ftp
```

4.15.4 DHCPサーバの切替え

プロファイル管理機能でDHCPサーバを使用する場合に、ISM-VA内部のDHCPサーバを使用するか、外部のDHCPサーバ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 dhcpd show-mode
```

コマンド出力

```
DHCP mode: local    : Profile機能はISM内部のDHCPサーバを使用します。
DHCP mode: remote  : Profile機能は外部のDHCPサーバを使用します。
```

- 設定の切替え

- ISM-VA内部のDHCPサーバを使用してプロファイル適用を行うように設定

```
# ismadm dhcpd set-mode local
```

- 外部のDHCPサーバを使用してプロファイル適用を行うように設定

```
# ismadm dhcpd 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、「[4.22 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-VAをバックアップしてください。

ISM-VAのバックアップ方法は、『操作手順書』の「[2.1.2 ISM-VAをエクスポートする](#)」を参照してください。

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、「[4.22 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>
```

実行例:

```
# ismadm system patch-add -file /Administrator/ftp/SVISM_V200S20160606-02.tar.gz
```

5. 修正パッチ適用後、ISM-VAを再起動します。

```
# ismadm power restart
```

4.18 ISM-VAのアップグレード

ISMをV2.0/V2.1/V2.2/V2.3からV2.4にアップグレードするためには、アップグレードプログラム(DVD媒体、アップグレードファイル)の入手が必要です。入手方法については、SupportDesk-Webの製品ページの[アップグレード]メニューを参照してください。

SupportDesk-Webについては、『入門書』の「ISMの保守」を参照してください。



注意

V1.0～V1.5からV2.4へのアップグレードをご希望の場合も、SupportDesk-Webを参照してアップグレードの申込みをしてください。アップグレード方法については、当社技術員にご相談ください。

アップグレードファイル入手後、以下の手順でアップグレードを実施してください。



注意

アップグレードする前に、ISM-VAをバックアップしてください。

ISM-VAのバックアップ方法は、『操作手順書』の「2.1.2 ISM-VAをエクスポートする」を参照してください。

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、「4.22 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名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名>
```

実行例:

```
# ismadm system upgrade -file /Administrator/ftp/ISM240_S2019xxxx-0X.tar.gz
```

5. アップグレード後、ISM-VAを再起動します。

```
# ismadm power restart
```

4.19 ISM-VAの統計情報表示

ISM-VAのCPU使用率/メモリ使用率/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量(MB)
MEM-avg	平均メモリ使用率(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
HOURL	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量(MB)
MEM-avg	平均メモリ使用率(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
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量(MB)
MEM-avg	平均メモリ使用率(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。

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。

```
# 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利用可能になります。



- ・ 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は、以下のとおりです。

SSLv3, TLSv1, TLSv1.1, TLSv1.2

- ・ コマンド実行後に再起動が必要です。
- ・ デフォルトでは、以下が設定されています。

ISMの環境	利用可能なSSL/TLSバージョン
ISM 2.3.0より前からアップデート／アップグレード	SSLv3, TLSv1, TLSv1.1, TLSv1.2
ISM 2.3.0以降で利用を開始	TLSv1.2

4.21 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、「[4.22 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のIPアドレスまたはFQDN>
```

4.22 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「2.8 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の新規作成、名称変更、および削除

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が定期的に行う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。

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。
- ・ 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。

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、サーバまたは搭載IOカードのOfflineアップデートを実行する。

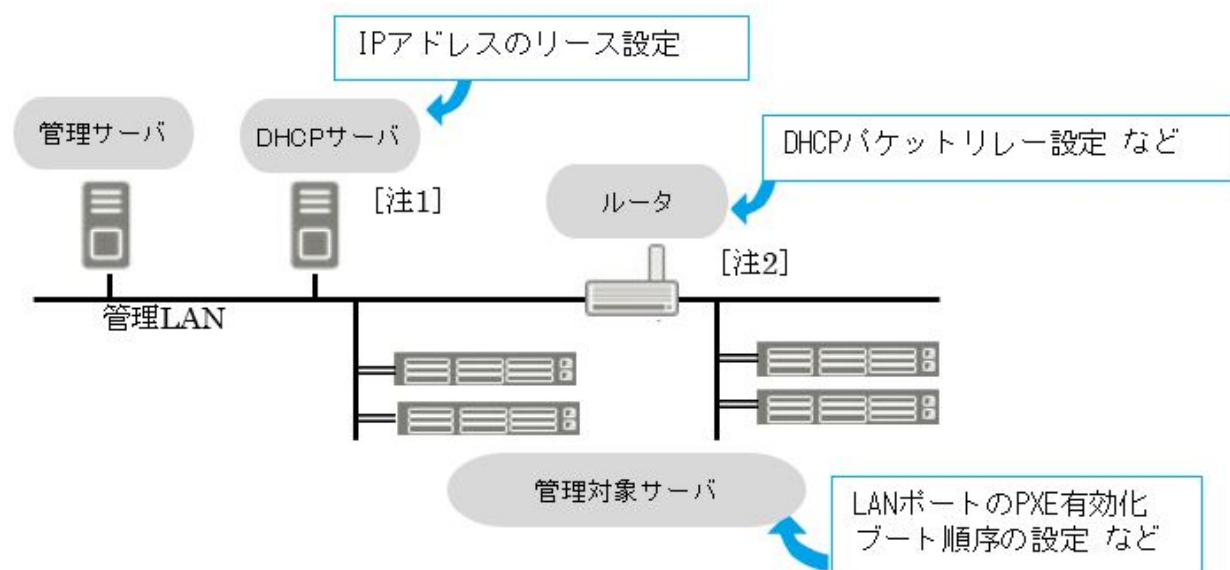
PXEブートを正しく動作させるためには、事前に管理対象サーバ(ノード)およびネットワーク構成について適切な準備が必要です。ここではPXEブートに必要な作業について情報を提供します。

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サーバを用意する代わりに、ISM-VA(管理サーバ)内のDHCPサーバ機能の使用も可能です。

外部のDHCPサーバと管理サーバ内部のDHCPサーバ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、ルータは不要です。

必要な準備作業

管理対象サーバ

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。
- 複数のネットワークポートでPXEブートを有効にしている場合は、BIOSのブート順設定を確認し、ISMがPXEブートに使用するLANポートがネットワークポートの中で最も高い優先度になるように設定してください。
- 使用するLANポートの指定を「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/ルータ

ISM-VA内のDHCP機能を有効にするか、管理サーバと同じネットワークセグメント内でDHCPサーバを動作させ、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)

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 仮想リソース管理機能の事前設定

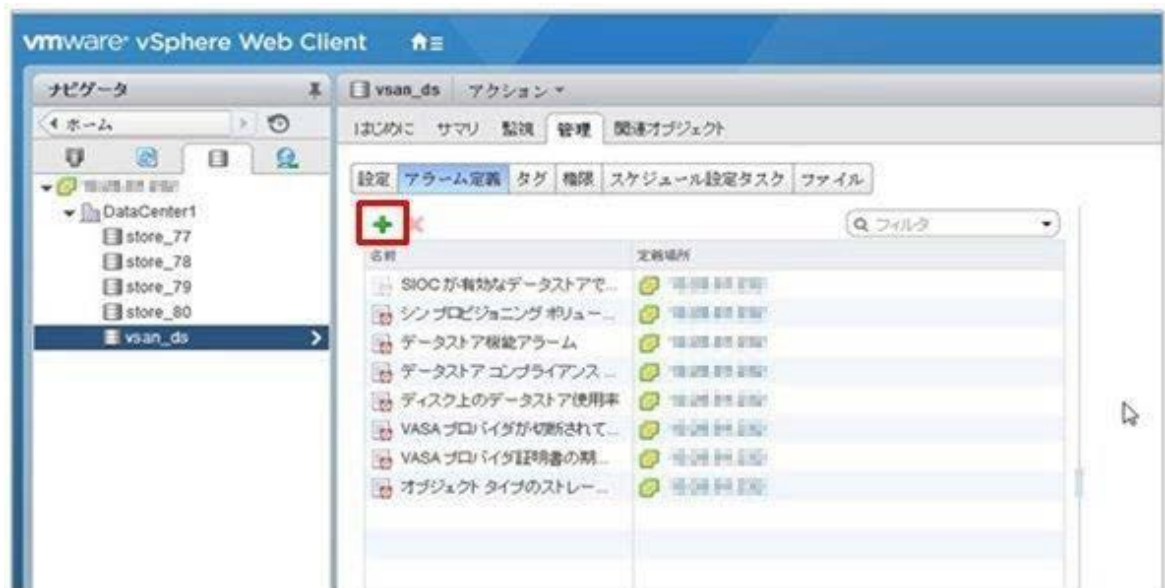
仮想リソース管理機能を使用することで、仮想化基盤の運用監視ができます。ここでは仮想リソース管理機能に必要な事前設定の情報を提供します。

VMware vSANの事前設定

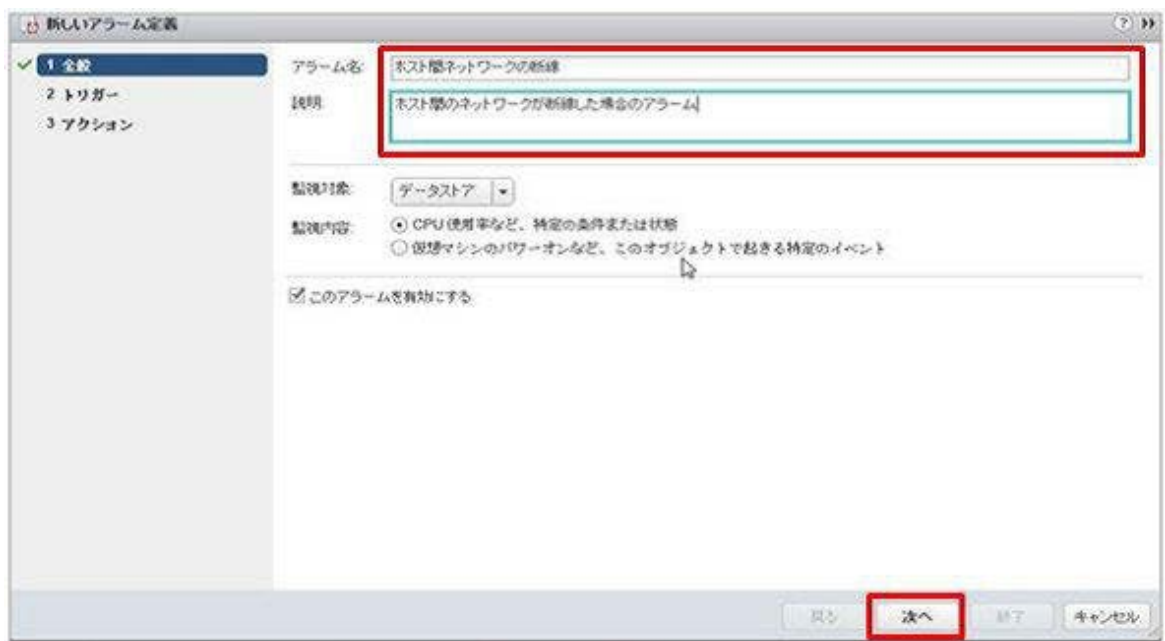
VMware vSANのホスト間のネットワーク断線によるvSANデータストアの異常を検出できるようにするため、アラーム定義を行います。vSANのアラーム定義の追加方法について説明します。

1. vSphere Web Client画面を表示します。[ホーム]からストレージビュータブを選択し、表示されたデータストアから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」の例)。

表示された画面右側の[管理]タブ(vCenter Server Appliance 6.5の場合は[監視]タブから[問題]を選択)から[アラーム定義]を選択して[+]を選択します。



2. ウィザード画面で「アラーム名」と「説明」に下表のように入力し[次へ]ボタンを選択します。



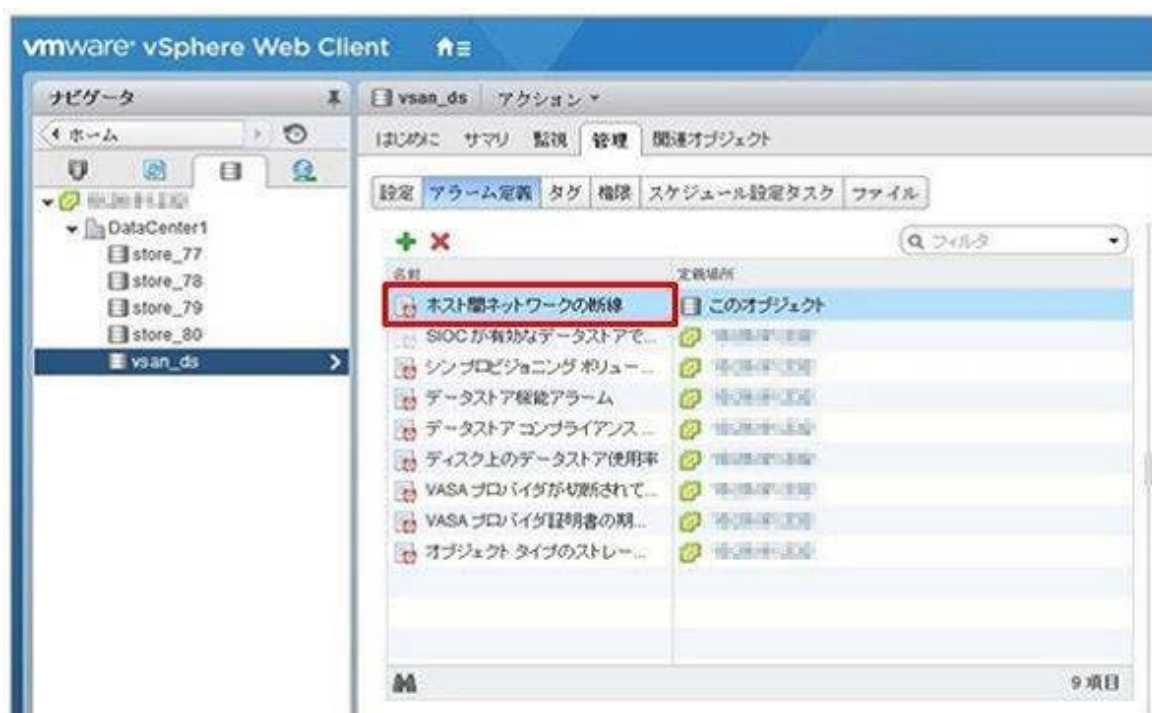
項目	入力内容
アラーム名	ホスト間ネットワークの断線
説明	ホスト間のネットワークが断線した場合のアラーム

3. 以下の画面で[+]を選択し、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
警告条件	なし
重大条件	切断状態

4. アクションは設定不要です。[終了]ボタン(または[完了]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。



Storage Spaces Directの事前設定

Microsoft Storage Spaces Directの運用管理を行うために、ISM-VAに対してOS監視の設定、および記憶域プールを構成するすべてのノードに対して、CredSSP認証の有効化が必要です。以下の手順で実施してください。

ISM-VAへの設定

ISMからOSを監視するための設定を行います。設定方法については、「[B.2 監視対象への設定手順\(OS:Windows\)](#)」を参照してください。

ノードへの設定

記憶域プールを構成するすべてのノードに対してCredSSP認証の有効化を設定します。



本設定を行わない場合、Storage Spaces Direct に対して仮想リソース管理機能が利用できません。

また、記憶域プールを構成するノードは、サーバマネージャーまたはフェイルオーバークラスタマネージャーから確認できます。

1. ノードにドメイン管理者権限のユーザーでログインし、PowerShellを起動します。
2. 以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role client -DelegateComputer <対象ノード（コンピュータ）名>
```

ドメイン内のすべてのコンピュータ名の指定には、ワイルドカード(*)を使用できます。

例)

```
Enable-WSManCredSSP -Role client -DelegateComputer *.fujitsu.local
```

3. 続いて以下のコマンドを実行します。

```
Enable-WSManCredSSP -Role server
```

A.1.3 ETERNUS DX/AF ドライブエンクロージャの表示

ISMは、ETERNUS DX/AF のコントローラーエンクロージャに接続されているドライブエンクロージャをノードとして管理します。
ここではドライブ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。

ドライブエンクロージャの登録

ドライブエンクロージャは、以下の手順によって自動的に ISM にノード登録されます。

1. ドライブエンクロージャが接続されている ETERNUS DX/AF のコントローラーエンクロージャを ISM にノード登録します。
2. コントローラーエンクロージャのノード情報取得が完了すると、ドライブエンクロージャがノードリストに表示されます。

ドライブエンクロージャのノード詳細情報

ISMでは、ドライブエンクロージャのノード詳細情報はコントローラーエンクロージャのノード詳細情報に表示します。

ドライブエンクロージャのステータス

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。

ドライブエンクロージャの削除

ドライブエンクロージャは、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あとに、コントローラーエンクロージャのノード情報取得が実行された場合
- ISM からコントローラーエンクロージャのノードを削除した場合

A.1.4 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	ブ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)



- --#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、あるいは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.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する必要があります。

表A.1 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
PRIMERGY (RX/BX/CX/TX) PRIMEQUEST 3000B IPCOM VX2 (PRIMERGY CX1430 M1を除く)	ノード情報取得	IPMI / HTTPS	623 / 443
	自動検出	SSDP	1900
	モニタリング	IPMI	623
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	IPMI / TFTP	623 / 69
	ログ収集	IPMI / SSH / HTTPS	623 / 22 / 443
	プロファイル適用(全般)	IPMI	623
		HTTP	80
		HTTPS	443

対象機器	機能	プロトコル	使用ポート
	プロファイル適用 (OSインストール時のみ)	FTP	21
		DHCP	67
		TFTP	69
		SMB	445
		PXE	4011
		独自	9213
PRIMERGY CX1430 M1	ノード情報取得	IPMI / HTTPS	623 / 443
	モニタリング	IPMI	623
	ファームウェアアップデート		
PRIMERGY BX シャーシ (MMB)	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP / SSH	161 / 22
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	SNMP / SSH / TFTP	161 / 22 69
	ログ収集	SSH	22
PRIMEQUEST 2000Type3 PRIMEQUEST 3000E	ノード情報取得	SNMP / IPMI	161 / 623
	モニタリング	SNMP / IPMI	161 / 623
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	IPMI	623
ETERNUS DX/AF	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	FTP / SSH	21 / 22
	プロファイル適用	SSH	22
ETERNUS NR (NetApp)	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP / HTTPS	161 / 443
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	-	-
	ログ収集	SSH / HTTPS	22 / 443
	プロファイル適用	-	-
SR-X	ノード情報取得	SNMP / SSH	161 / 22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
イーサネットスイッチ	ノード情報取得	SNMP / SSH	161 / 22

対象機器	機能	プロトコル	使用ポート
(10GBASE-T 48+6 / 10GBASE 48+6)	自動検出	SSDP	1900
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
VDX	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
Catalyst 3750-X Nexus 5000 Series Arista 7000 Family	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
CFX2000F/R PRIMERGY スイッチブレード/コンバージド ファブリックスイッチブレード(10Gbps 18/8+2)	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / SSH	21 / 22
	ログ収集	SSH	22
	プロファイル適用	SSH	22
PRIMERGY BX スイッチブレード(1Gbps/ 10Gbps)	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	FTP / TFTP SSH	21 / 69 22
	ログ収集	SSH	22
PRIMERGY BX LANパススルー ブレード	ノード情報取得	SNMP	161
	モニタリング		(通信先はMMB)
	トラップ受信	SNMP (Trap)	162
Brocade FCスイッチ	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
PRIMERGY BX FCスイッチブレード	ノード情報取得	SSH	22
	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162
	ファームウェアアップデート	SSH	22
	ログ収集	SSH	22
Asetek Rack CDU /	ノード情報取得	SNMP	161

対象機器	機能	プロトコル	使用ポート
Schneider Electric Metered Rack Mount PDU / Schneider Electric Smart-UPS	モニタリング	SNMP	161
	トラップ受信	SNMP (Trap)	162

表A.2 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
Windows	OS情報取得	WSMAN	5986
	モニタリング	WSMAN	5986
	ファームウェアアップデート	-	-
	ログ収集	WSMAN	5986
Linux	OS情報取得	SSH	22
	モニタリング	SSH	22
	ファームウェアアップデート	SSH	22
	ログ収集	SSH	22
VMware ESXi	OS情報取得	vSphere API / CIM	443 / 5989
	モニタリング	vSphere API	443
	ファームウェアアップデート	-	-
	ログ収集	REST	443

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.3 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) (CX1430 M1を除く)	○	-	-	- [注4]
PRIMERGY CX1430 M1	○	-	-	○
PRIMEQUEST 2000Type3	○	○	○	-
PRIMEQUEST 3000E	○	○	○	-
PRIMEQUEST 3000B	○	-	-	- [注4]
ETERNUS DX/AF	-	○	○	-
ETERNUS NR	-	○	○	-
SR-X	-	○	○	-

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
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	-	○	○	-
Cisco Nexus	-	○	○	-
Arista 7000 Family	-	○	-	-
PRIMERGY BX シャーシ (MMB)	-	○	○	-
PRIMERGY BX サーバブレード	○	-	-	-
PRIMERGY BX スイッチブレード(1Gbps/10Gbps)	-	○	○	-
PRIMERGY BX LANパススルーブレード	-	-	- [注3]	-
PRIMERGY BX FCスイッチブレード	-	○	○	-
PRIMERGY スwitchブレード / コン バージドファブリックスイッチブレード (10Gbps 18/8+2)	-	○	○	-
CFX2000F/R	-	○	○	-
AsetekRackCDU	-	-	○	-
SchneiderElectric Metered RackMountPDU	-	-	○	-
SchneiderElectric Smart-UPS	-	-	○	-

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。

<http://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、コミュニティ名の入力が必要ですが、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することができます。

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世代のサーバにて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カードについての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。変更は以下のように行います。

1. [ユーザ管理] - [iRMC S4ユーザ管理] - [IPMI権限/許可] - [Redfish Enabled] をチェック。
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。

【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。
- AGモードを無効にしてください。

【Arista 7000 Family】

LLDP設定を有効にしてください。

【ETERNUS DX/AF】

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ご使用ください。

(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。)

【PRIMEQUEST 2000 Type3、PRIMEQUEST 3000E】

- 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ご使用ください。
- 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ご使用ください。その際PrivilegeはAdminまたはCEである必要があります。

【PRIMERGY BX】

- スイッチブレード: LLDP設定を有効にしてください。
- ファイバーチャネルスイッチブレード: SW-MIBを有効にしてください。

実行例)

```
snmpconfig --enable mibCapability -mib_name SW-MIB
```

- シャーシの電源がOFFの場合、MMBから情報が取得できません。それにより、サーバブレード、コネクショブレードとの関係性が一時的に解除されて見えます。電源がON状態になってからシャーシを選択し、[アクション] - [ノード情報取得]の操作を実施してください。

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、以下の機器では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す。

表A.4 対応機器

ノード	エンジンIDの自動入力
PRIMERGY(RX/CX/TX)	○
PRIMEQUEST 2000Type3	-

ノード	エンジンIDの自動入力
PRIMEQUEST 3000E	○
PRIMEQUEST 3000B	○
ETERNUS DX/AF	○
ETERNUS NR	-
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	○
PRIMERGY BXシャーシ (MMB)	-
PRIMERGY BX サーバブレード	○
PRIMERGY BX スイッチブレード(1Gbps/10Gbps)	○ [注1]
PRIMERGY BX LANパススルーブレード	-
PRIMERGY BX FCスイッチブレード	○
PRIMERGY スwitchブレード / コンバージドファブリック スイッチブレード(10Gbps 18/8+2)	○ [注1][注2]
CFX2000F/R	○ [注1][注2]
AsetekRackCDU	-
SchneiderElectricMetered RackMountPDU	-
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。

- ・ PRIMERGY BXスイッチブレード(10Gbps)
- ・ PRIMERGY スwitchブレード / コンバージドファブリックスイッチブレード(10Gbps 18/8+2)
- ・ 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。



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.5 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 10～20分	
	Offlineアップデート 15～30分	ファームウェアを適用後、サーバ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 1～2分	ファームウェアを適用するためにサーバの電源オフ・オン操作の時間が別途必要。
	Offlineアップデート 15～30分	ファームウェアを適用後、サーバ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。
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の電源オフ・オン操作の時間が別途必要。
PRIMEQUEST 2000シリーズ、3000シリーズ の本体ファームウェアアップデート	70～130分	
PRIMERGY BX900S2 MMB	10～20分	左記はMMB 1枚当たりの時間。
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	
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	
LAN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	
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	
FC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	
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 5～15分	ファームウェア適用でサーバの電源オフ・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 15～20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。



- ・ 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

【保管ログの容量】

表A.6 1ノードあたりの1世代の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY	1KB

ログ収集ターゲット			容量の目安
		PRIMERGY GX2580 M5 (ISM 2.4.0.c 以降)	10KB
		PRIMEQUEST 3000B	1KB
		IPCOM VX2	1KB
	Chassis	PRIMERGY BX	100KB
		PRIMEQUEST 3000E	50KB
	Connection	Ethernet Switch	100KB
	Blade	Fibre Channel Switch	10MB
		Switch	SR-X
	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		1MB
	Storage	ETERNUS DX/AF	10MB
		ETERNUS NR (NetApp) Cluster	100KB
		ETERNUS NR (NetApp) Chassis	500MB
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		

【ノードログ(ダウンロード用データ)の容量】

表A.7 1ノードあたりの30日間分の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY (CX1430 M1、GX2580 M5 (ISM 2.4.0.c 以降)を除く)	50KB
		PRIMEQUEST 3000B	50KB
		IPCOM VX2	50KB
	Chassis	PRIMERGY BX	50KB
		PRIMEQUEST 3000E	50KB
	Connection	Ethernet Switch	100KB
	Blade	Fibre Channel Switch	50KB
	Switch	SR-X	100KB

ログ収集ターゲット			容量の目安
		CFX	100KB
		イーサネットスイッチ (10GBASE-T 48+6 / 10GBASE 48+6)	150KB
		VDX	100KB
		Cisco Catalyst	50KB
		Cisco Nexus	50KB
	Storage	ETERNUS DX/AF	100KB
		ETERNUS NR (NetApp) Cluster	200KB
オペレーティング システム	Windows		1MB
	Linux		1MB
	VMware ESXi		4MB
	IPCOM OS		1MB

【ノードログ(検索用データ)の容量】

表A.8 1ノードあたりの30日間分の目安

ログ収集ターゲット			容量の目安
ハードウェア	Server	PRIMERGY (CX1430 M1、GX2580 M5 (ISM 2.4.0.c 以降)を除く)	500KB
		PRIMEQUEST 3000B	500KB
		IPCOM VX2	500KB
	Chassis	PRIMERGY BX	500KB
		PRIMEQUEST 3000E	500KB
	Connection	Ethernet Switch	1MB
	Blade	Fibre Channel Switch	500KB
	Switch	SR-X	1MB
		CFX	1MB
		イーサネットスイッチ 10GBASE-T 48+6 / 10GBASE 48+6)	1MB
		VDX	1MB
		Cisco Catalyst	500KB
		Cisco Nexus	500KB
	Storage	ETERNUS DX/AF	1MB
		ETERNUS NR (NetApp) Cluster	2MB
オペレーティング システム	Windows		15MB
	Linux		15MB
	VMware ESXi		50MB
	IPCOM OS		15MB

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
Red Hat Enterprise Linux	6.x	○	－	×	－	－	○
	7.x	○	－	×	－	－	○
	8.x	○	－	×	－	－	○
SUSE Linux Enterprise Server	11	○	－	○	－	－	○
	12	○	－	○	－	－	○
	15	○	－	○	－	－	○
Windows Server	2008 R2	－	○	○	○	○	○
	2012	－	○	○	○	○	○
	2012 R2	－	○	○	○	○	○
	2016	－	○	○	○	○	○
	2019	－	○	○	○	○	○
VMware ESXi	5.x	－	－	－	－	－	○
	6.x	－	－	－	－	－	○

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\(OS:VMware ESXi\)](#)

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	5.5以降	－	－	－	○	－
	6.x以降	－	－	－	○	－

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
Microsoft Failover Cluster	Windows Server 2012以降	—	○	○	○	○
Microsoft System Center	2012以降	—	○	○	○	○
KVM Red Hat		○	—	—	○	○
KVM SUSE Linux Enterprise		○	—	—	○	○
OpenStack		「 B.11 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				

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.6 監視対象への設定手順 \(仮想化管理ソフトウェア: vCenter Server\)](#)
- [B.7 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.8 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.9 監視対象への設定手順 \(仮想化管理ソフトウェア: KVM\)](#)
- [B.10 監視対象への設定手順 \(仮想化管理ソフトウェア: IPCOM\)](#)
- [B.11 監視対象への設定手順 \(仮想化管理ソフトウェア: OpenStack\)](#)

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使用率の性能監視のために、対象サーバの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。

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 ファイアー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。」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 (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-10-sdk>



- 上記 URL の Windows Software Development Kit は、Windows 7 SP1 または Windows 8.1、および Windows Server 2012 R2 または Windows Server 2016 の OS に対応しています。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/bfskty3\(v=vs.80\).aspx](https://msdn.microsoft.com/ja-jp/library/bfskty3(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](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、対象サーバのサーバ名を "192.168.10.10"、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](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。

- 対象サーバでmmc.exeを実行します。
- [ファイル]-[スナップインの追加と削除]を選択します。
- [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。
- 「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。
- [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。

- [コンソールルート]-[証明書(ローカルコンピュータ)]-[信頼されたルート証明機関]を右クリックします。
- [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。
- [コンソールルート]-[証明書(ローカルコンピュータ)]-[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に指定したサーバ名となっていること、[目的]が「サーバ認証」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。

- [コンソールルート]-[証明書(ローカルコンピュータ)]-[個人]を右クリックします。
- [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。
- [コンソールルート]-[証明書(ローカルコンピュータ)]-[個人]-[証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバ名となっていること、[目的]が「サーバ認証」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。

- コマンドプロンプトからPowerShellを起動します。
- 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 2008 R2の場合

以下のようなコマンドを実行します。

```
>netsh advfirewall firewall add rule name=＜ファイアウォールルール名＞ enable=yes localip=any remoteip=any protocol=tcp  
localport=＜ポート番号＞ remoteport=any edge=no dir=in profile=domain,private,public action=allow
```

例:ポート番号5986を解放するルールに、"WinRM"という名前を設定します。

```
>netsh advfirewall firewall add rule name=WinRM enable=yes localip=any remoteip=any protocol=tcp localport=5986  
remoteport=any edge=no dir=in profile=domain,private,public action=allow
```

Windows Server 2012 / 2012R2 / 2016 /2019の場合

コマンドプロンプトからPowerShellを開き、以下のような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を解放するルールに、"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、対象サーバの環境によって異なります。

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 -A WSMAN/<監視対象ホスト名> <監視対象ホスト名>
```

```
>setspn -A 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、監視対象サーバのサービスプリンシパル名を登録してください。

```
>setspn -A HOST/<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 HOST/<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サーバ追加」を行い、ISM-VAにDNSサーバ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では、Red Hat Enterprise Linuxがインストールされている対象サーバと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 ドメインユーザーアカウント使用時の設定](#)
- [B.3.3 一般ユーザーアカウント使用時の設定](#)
- [B.3.4 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のバージョンによって、コマンドが異なります。

Red Hat Enterprise Linux 6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。

```
#chkconfig --list 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。

```
sshd          0:off  1:off  2:off  3:off  4:off  5:off  6:off
```

2. 対象サーバのランレベルに対応する番号の項目がoffになっている場合は、以下のコマンドを実行してsshdを自動起動するようにします。

```
#chkconfig sshd on
```

対象サーバの次回起動時から、sshdが自動起動します。

3. sshdを起動します

```
#/etc/init.d/sshd start
```

Red Hat Enterprise Linux 7 / 8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 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サーバ追加」を行い、ISM-VAにDNSサーバ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

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の収集を行います。

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ウェア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.3.3 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.3.4 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.3.3 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では、SUSE Linux Enterprise Serverがインストールされている対象サーバと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](#)
- ・ [B.4.2 ファイアウォールのポート開放](#)
- ・ [B.4.3 ドメインユーザーアカウント使用時の設定](#)

- ・ [B.4.4 一般ユーザーアカウント使用時の設定](#)
- ・ [B.4.5 ユーザーアカウント共通の設定](#)

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のバージョンによって、コマンドが異なります。

SUSE Linux Enterprise Server 11

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。

```
#chkconfig --list 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。

```
sshd          0:off  1:off  2:off  3:off  4:off  5:off  6:off
```

2. 対象サーバのランレベルに対応する番号の項目がoffになっている場合は、以下のコマンドを実行してsshdを自動起動するようにします。

```
#chkconfig sshd on
```

対象サーバの次回起動時から、sshdが自動起動します。

3. sshdを起動します。

```
#/etc/init.d/sshd start
```

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 ファイアーウォールのポート開放

ファイアーウォールを有効にしている場合、ファイアー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のファイアーウォールは、デフォルトでsshのポートを閉じています。

ファイアーウォールの設定は、対象サーバの環境によって異なります。

SUSE Linux Enterprise Server 11 / 12

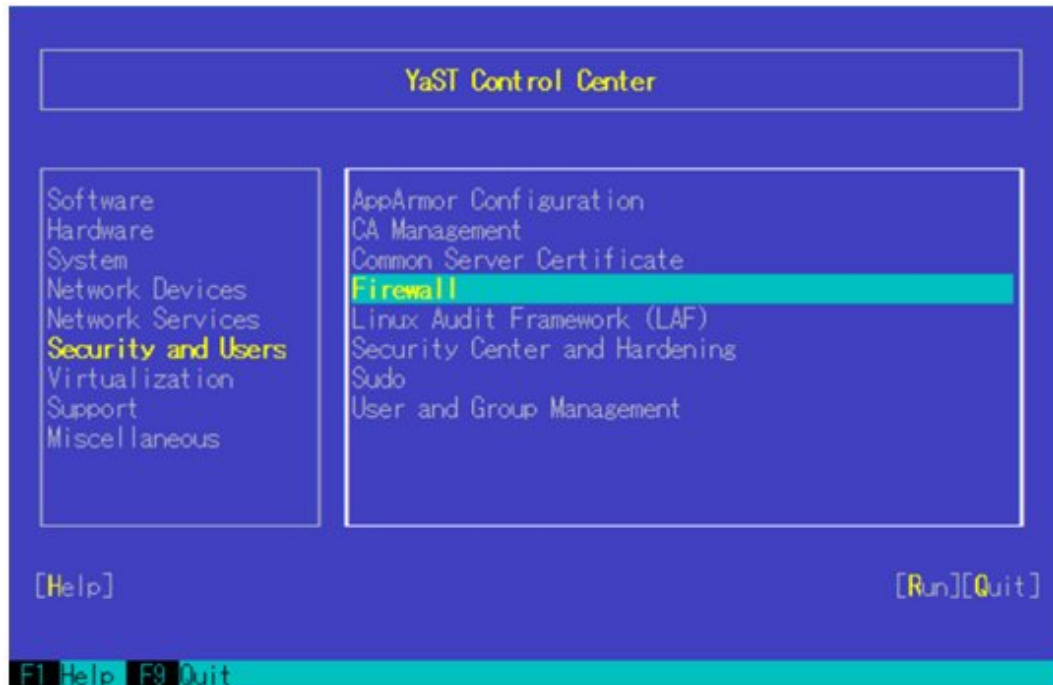
以下は、YaSTを使用した場合のファイアーウォールの設定例です。

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]キーを組み合わせで選択します。

2. [Security and Users]-[Firewall]を選択し、[Enter]キーを押します。

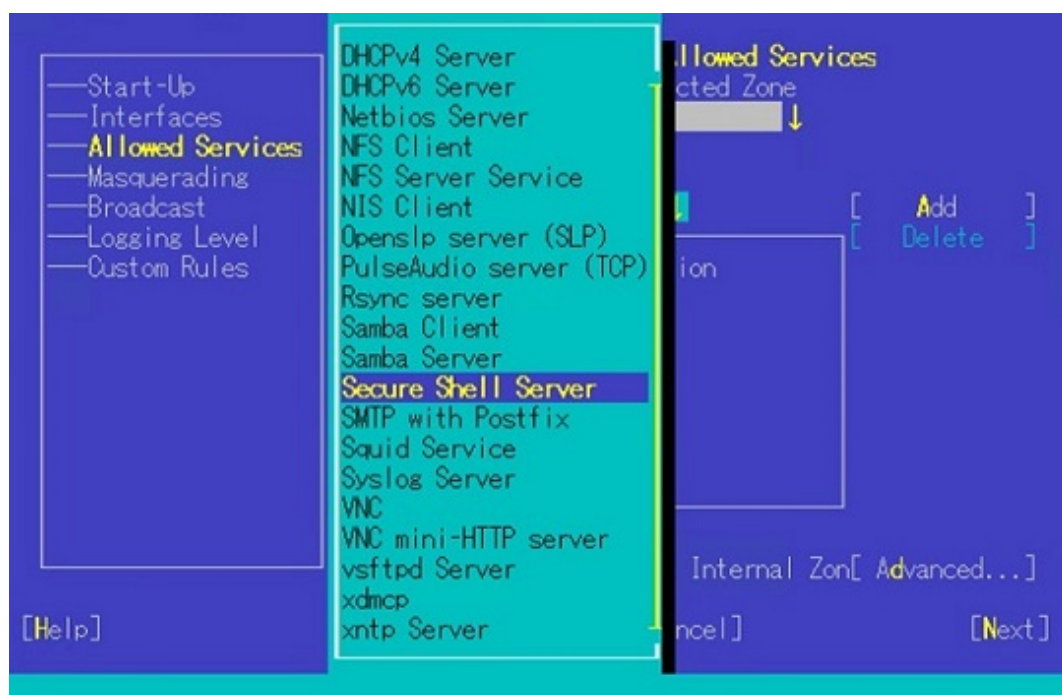


3. 「Start-Up」画面から、[Service Start]の状態を「Enable Firewall Automatic Starting」にします。



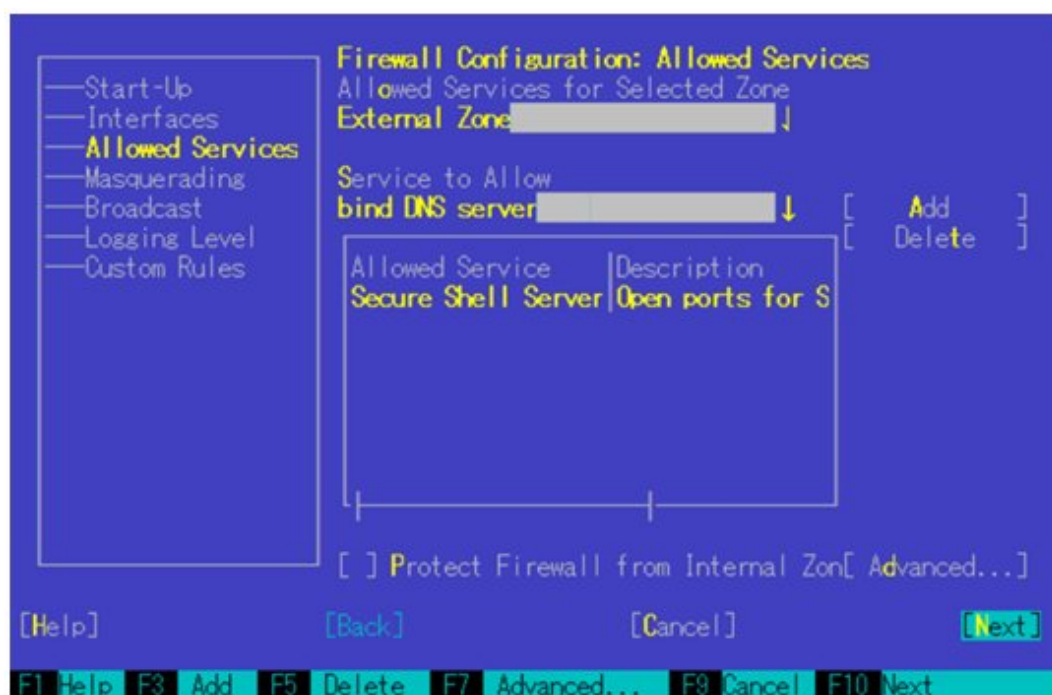
4. [Allowed Services]-[Service to Allow]へ移動し、下矢印のキーを押します。

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、ファイアー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ー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をする場合、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サーバ追加」を行い、ISM-VAにDNSサーバ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の収集を行います。

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ウェア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:VMware ESXi)

ISMでは、VMware ESXiがインストールされている対象サーバと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.5.1 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サーバ追加」を行い、ISM-VAにDNSサーバを登録してください。

B.6 監視対象への設定手順(仮想化管理ソフトウェア:vCenter Server)

B.6.1 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サーバ追加」を行い、ISM-VAにDNSサーバを登録してください。

B.6.2 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.5 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.7 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.7.1 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 -A HOST/<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。

```
HST/<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サーバ追加」を行い、ISM-VAにDNSサーバを登録してください。

5. Active DirectoryへKerberos委任の構成

- a. Active Directory サーバにログオンします。
- b. サーバマネージャを開きます。
- 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.8 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.9 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.9.1 KVM Red Hat Enterprise Linuxへの設定手順\(ドメインユーザー使用時\)](#)
- [B.9.2 KVM SUSE Linux Enterprise Serverへの設定手順\(ドメインユーザー使用時\)](#)

B.9.1 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
```

注意

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のIPアドレスを設定します。

admin_serverには、Kerberos管理サーバのFQDNを設定します。

通常、kdcとadmin_serverは、DNSサーバとActive Directoryサーバと同じサーバです。

- 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
```



注意

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
```



注意

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/sss/sss.conf」の作成

- a. 「/etc/sss/sss.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/sss/sss.conf
```

例:

```
[sss]
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を自動作成する場合、「/etc/sss/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/sss/sssd.conf」のパーミッションの変更

「/etc/sss/sssd.conf」のパーミッションを600に変更します。

```
# chmod 600 /etc/sss/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サーバのIPアドレス設定

- a. 以下のコマンドで、DNSサーバのIPアドレスを設定し、インターフェースを再起動します。

```
# nmcli connection modify <インターフェース名> ipv4.dns <DNSサーバのIPアドレス>
# systemctl restart NetworkManager
```

- b. インターフェース名を調べるには、以下のコマンドを実行します。

- Red Hat Enterprise Linux 6以下の場合

```
# ifconfig
```

- Red Hat Enterprise Linux 7以上の場合

```
# 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
```



Red Hat Enterprise Linux 8.0 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/sss/sss.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IPアドレス>
```

```
# ssh -l <ドメインユーザー名> <監視対象サーバ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/sss/sss.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.9.3 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サーバ追加」を行い、ISM-VAにDNSサーバを登録してください。

B.9.2 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

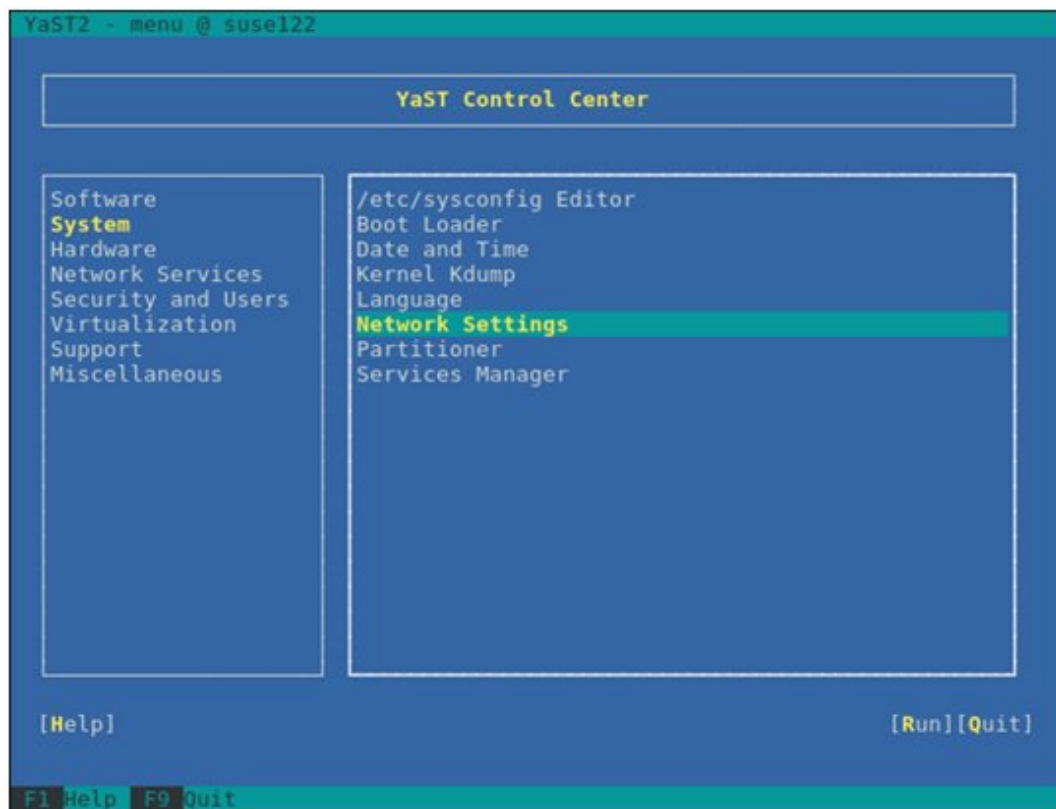
ターミナルよりrootユーザーで以下のコマンドを実行します。

```
# yast
```

yast内での項目の選択は、矢印キーと[Tab]キーを組み合わせで選択します。

2. ホスト名／DNSの設定

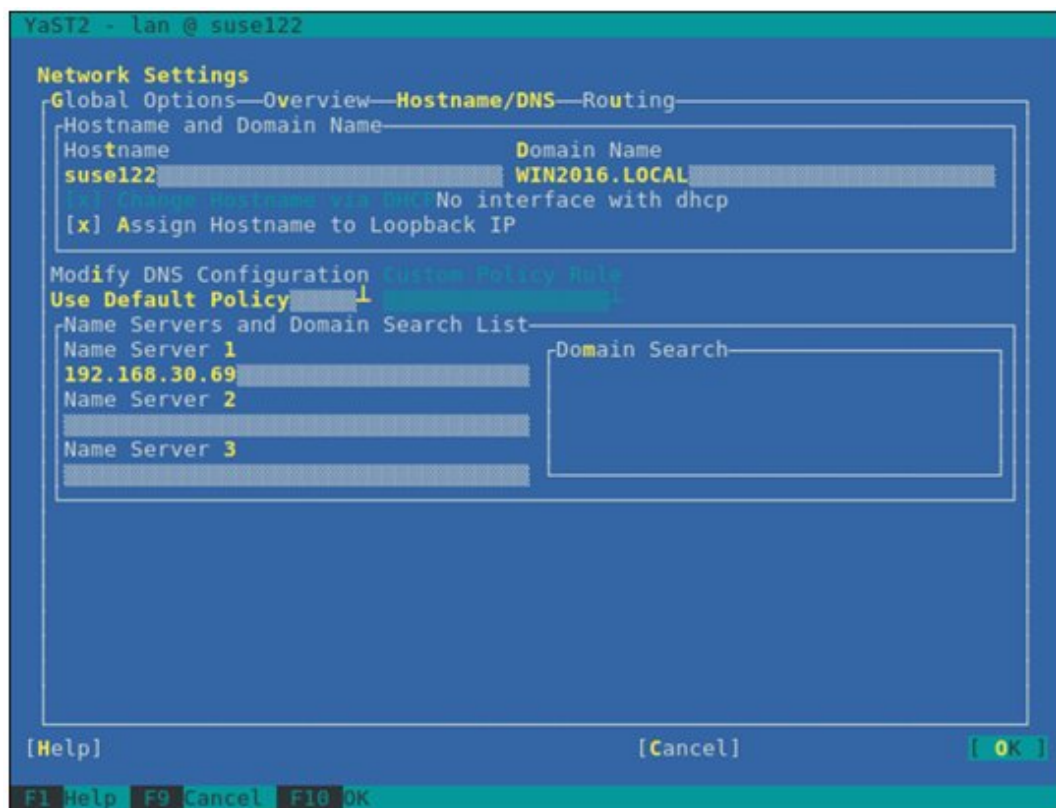
- a. [System]-[Network Settings]を選択し、[Enter]キーを押します。



- 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。

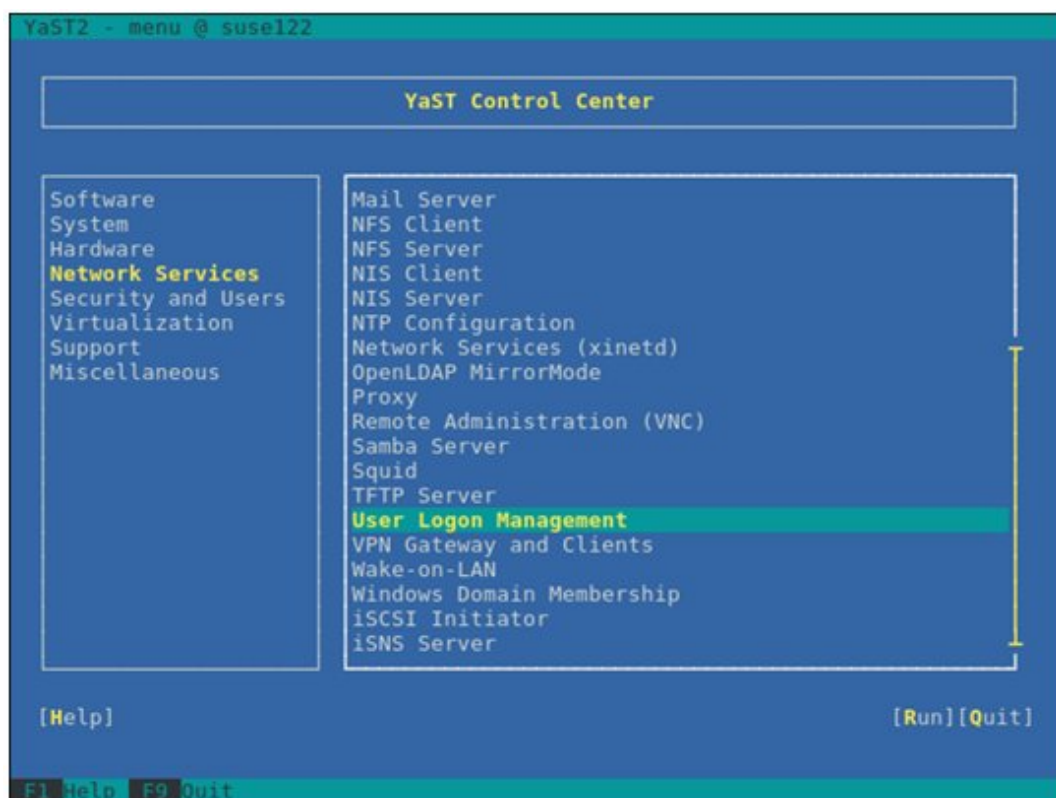
- Hostname
- Domain Name
- Assign Hostname to Loopback IP

- Name Server 1

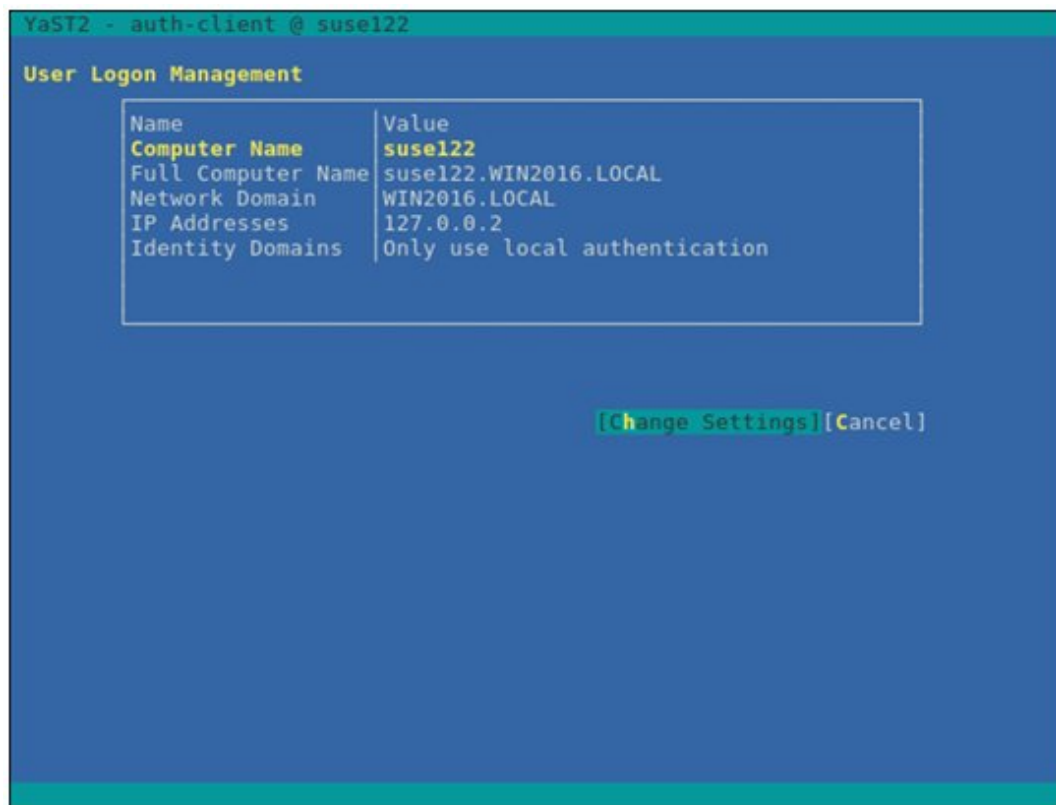


3. SSSDサービスの設定

- [Network Services]-[User Logon Management]を選択し、[Enter]キーを押します。



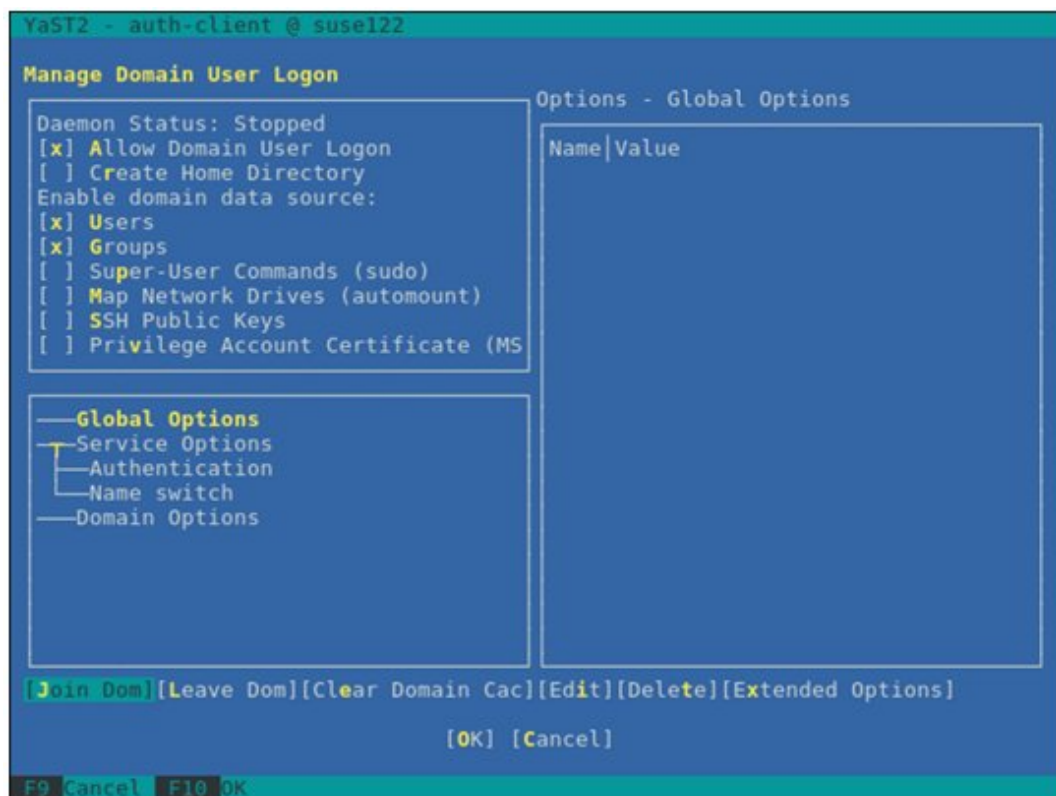
b. [Change Settings]を選択し、[Enter]キーを押します。



c. 以下の項目にチェックを入れ、[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

```

YaST2 - auth-client @ susel22

Domain name (such as example.com):
WIN2016.LOCAL
Which service provides identity data, such as user names and group membersh-
Delegate to third-party software library (proxy_lib_name)
FreeIPA
Generic directory service (LDAP)
Local SSSD file database
Microsoft Active Directory

Which service handles user authentication?—
Delegate to third-party software library (proxy_lib_name)
FreeIPA
Generic Kerberos service
Generic directory service (LDAP)
Local SSSD file database
Microsoft Active Directory
The domain does not provide authentication service

[x] Enable the domain

[OK] [Cancel]

F9 Cancel F10 OK

```

- 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。

```

Mandatory Parameters—
None.

Optional Parameters—
AD hostname (optional) - may be set if hostname(5) does not reflect the FQD
Host names of AD servers (comma separated).
[ ] Cache credentials for offline use
[ ] Treat user and group names as case sensitive.
[ ] Read all entities from backend database (increase server load)

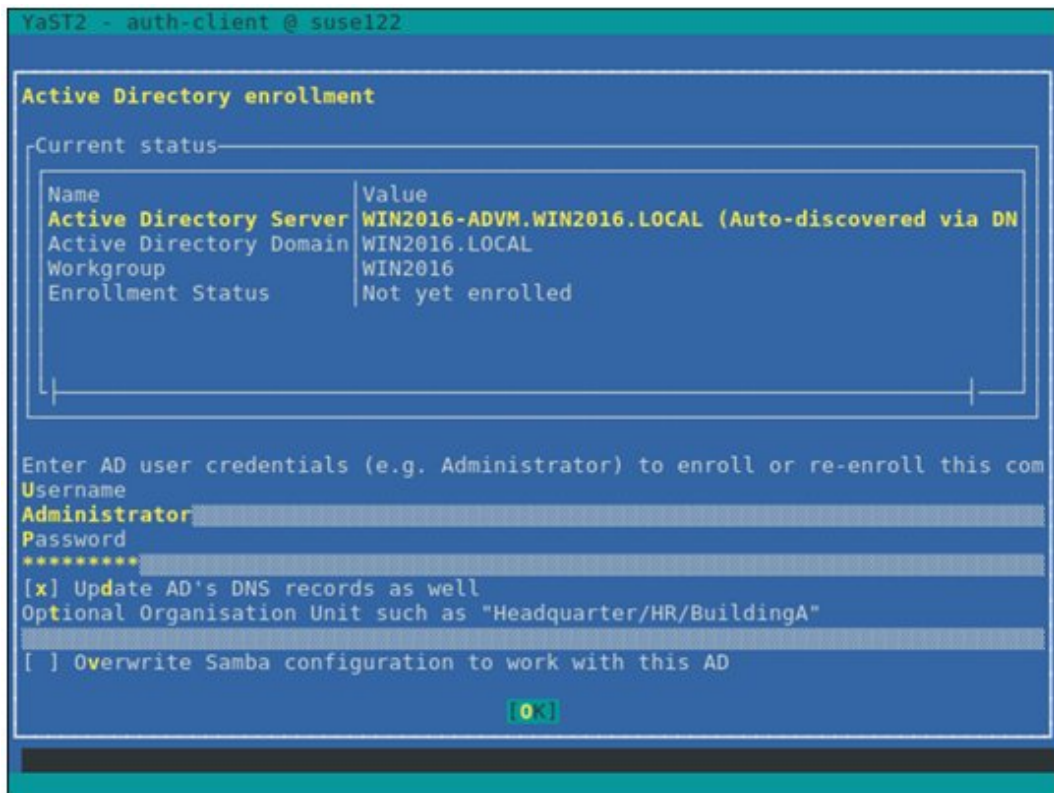
[OK] [Cancel]

```

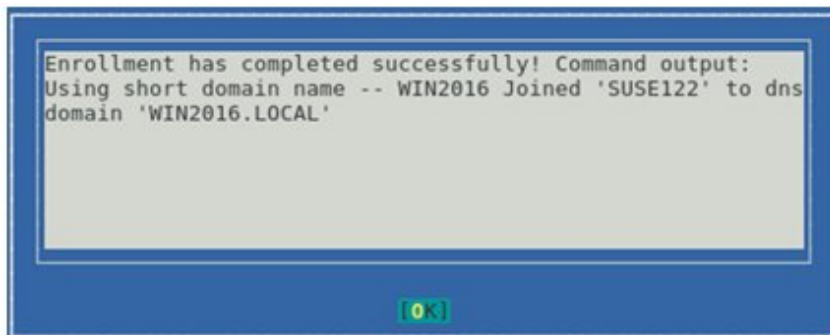
- f. 以下の項目を設定してから[OK]を選択し、[Enter]キーを押します。

- 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。

```
YaST2 - auth-client @ suse122

Manage Domain User Logon

Daemon Status: Stopped
[x] Allow Domain User Logon
[x] Create Home Directory
Enable domain data source:
[x] Users
[x] Groups
[ ] Super-User Commands (sudo)
[ ] Map Network Drives (automount)
[ ] SSH Public Keys
[ ] Privilege Account Certificate (MS

Options - domain/WIN2016.LOCAL
[x] Use this d[Enroll to Active Direct]

Name      Value
id_provider  ad
auth_provider ad
enumerate   false
cache_credentials false
case_sensitive false

--Global Options
--Service Options
--Authentication
--Name switch
--Domain Options
--WIN2016.LOCAL

[Join Dom][Leave Dom][Clear Domain Cac][Edit][Delete][Extended Options]

[OK] [Cancel]

F9 Cancel F10 OK
```

- i. [fallback_homedir]を選択してから[Add]を選択し、[Enter]キーを押します。

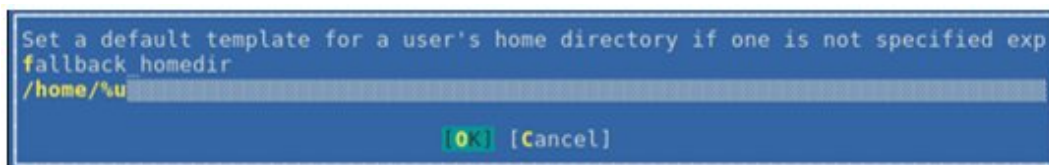
```
YaST2 - auth-client @ suse122

Extended options - domain/WIN2016.LOCAL
Name filter:

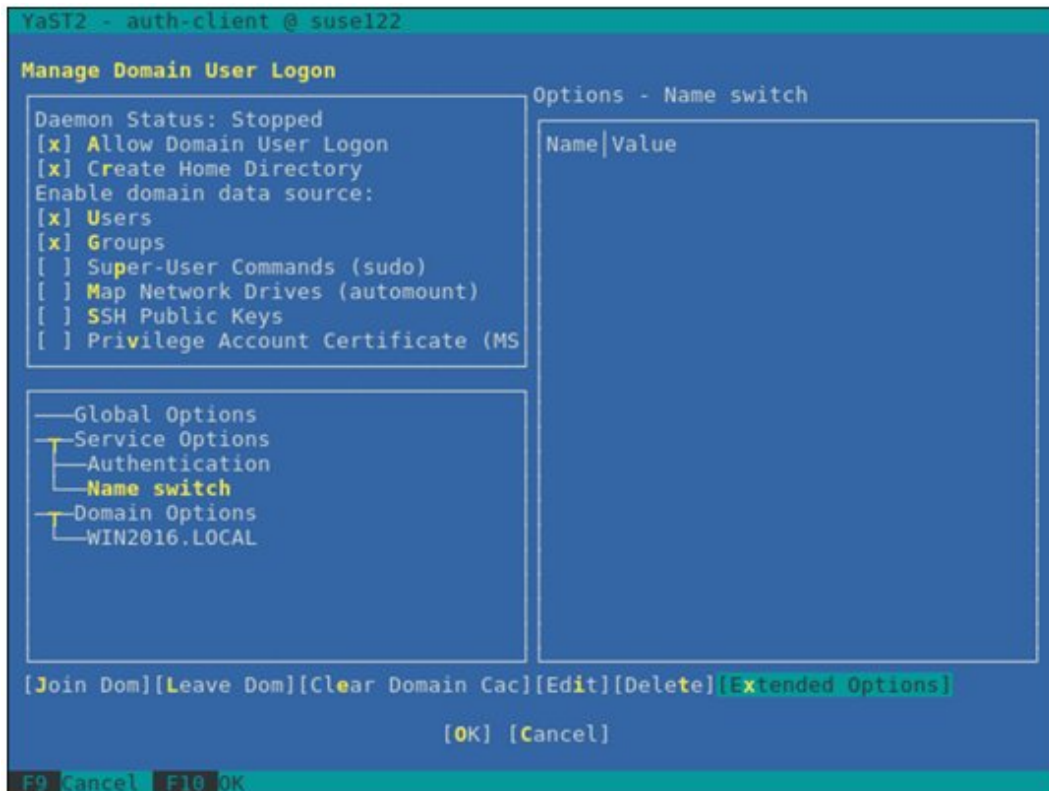
Name      Description
override_homedir Override the user's home director
proxy_fast_alias When a user or group is looked up
subdomain_homedir Use this homedir as default value
simple_allow_users Comma separated list of users who
simple_allow_groups Comma separated list of groups wh
simple_deny_users Comma separated list of groups th
ad_domain Specifies the name of the Active
ad_server Host names of AD servers (comma s
ad_backup_server Host names of backup AD servers (
ad_hostname AD hostname (optional) - may be s
fallback_homedir Set a default template for a user
default_shell The default shell to use if the p
ldap_idmap_range_min Specifies the lower bound of the
ldap_idmap_range_max Specifies the upper bound of the
ldap_idmap_range_size Specifies the number of IDs avail
ldap_idmap_default_domain_sid Specify the domain SID of the def
ldap_idmap_default_domain Specify the name of the default d
ldap_idmap_autorid_compat Changes the behavior of the ID-ma
ldap_use_tokengroups (Active Directory specific) Use t
ldap_uri URIs (ldap://) of LDAP servers (c
ldap_sudo_search_base An optional base DN to restrict L

[Add] [Cancel]
```

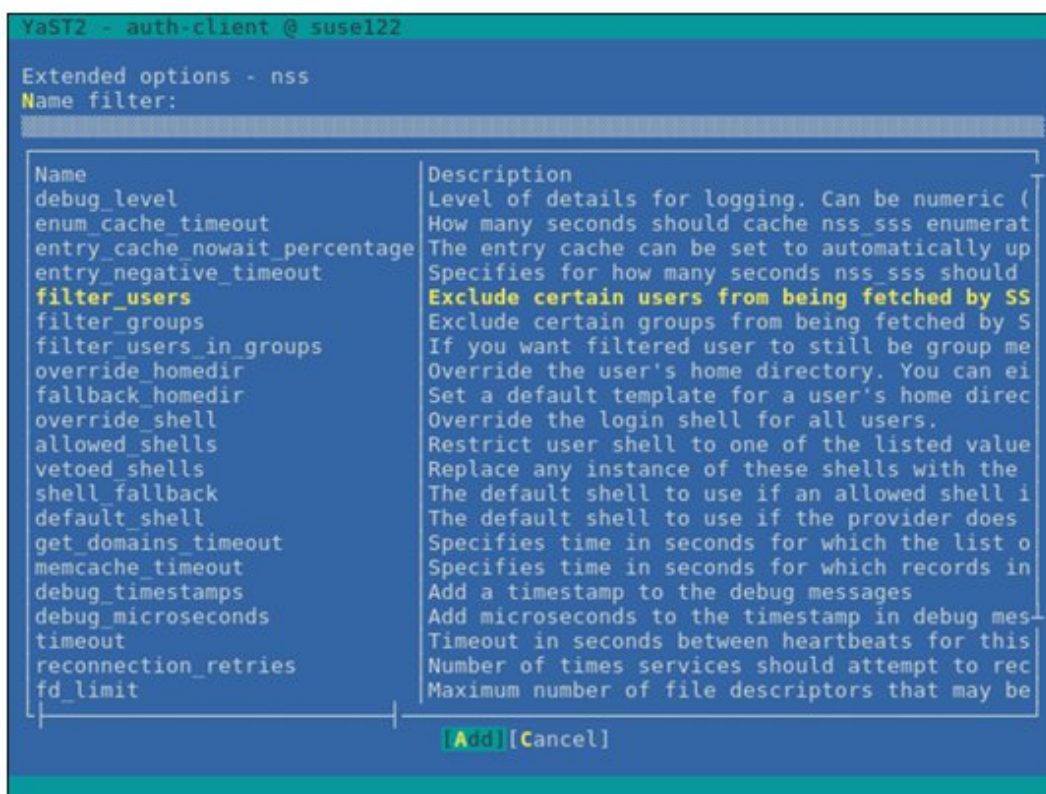
j. 「/home/%u」を入力してから[OK]を選択し、[Enter]キーを押します。



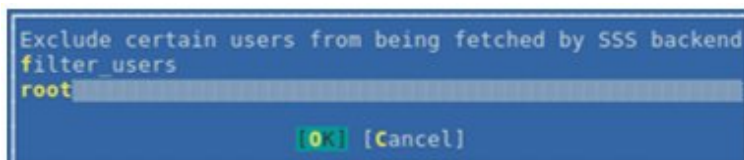
k. [Name switch]-[Extended Options]を選択し、[Enter]キーを押します。



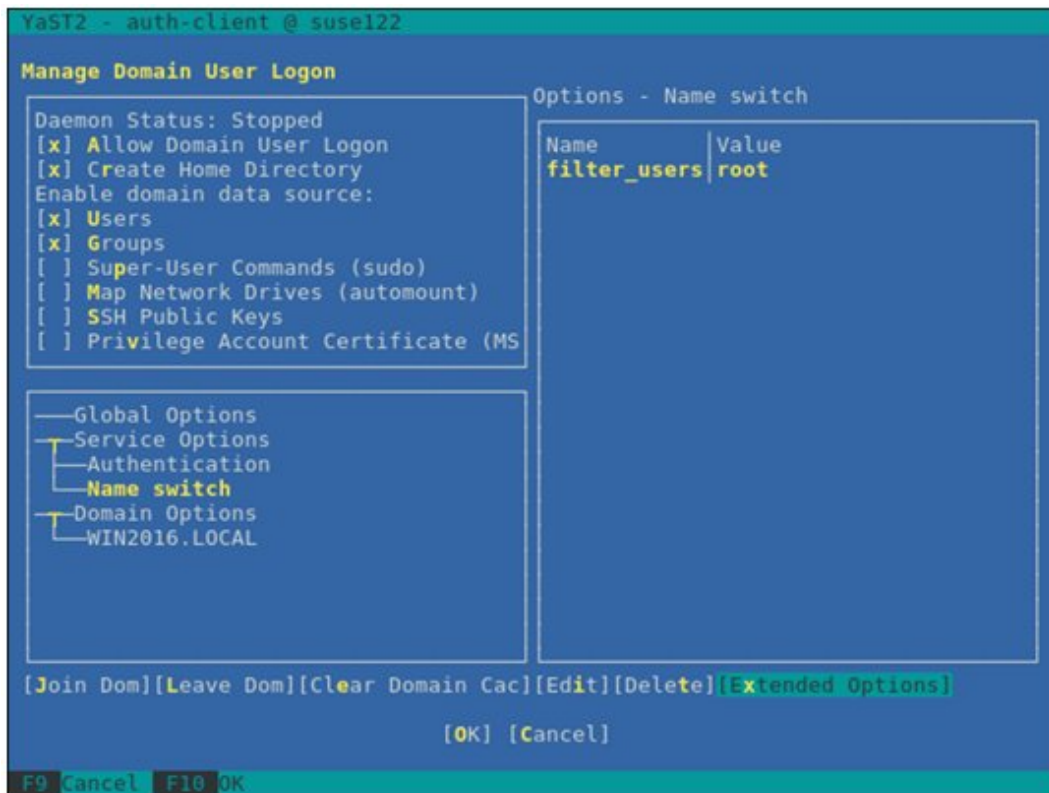
- l. [filter_users]を選択してから[Add]を選択し、[Enter]キーを押します。



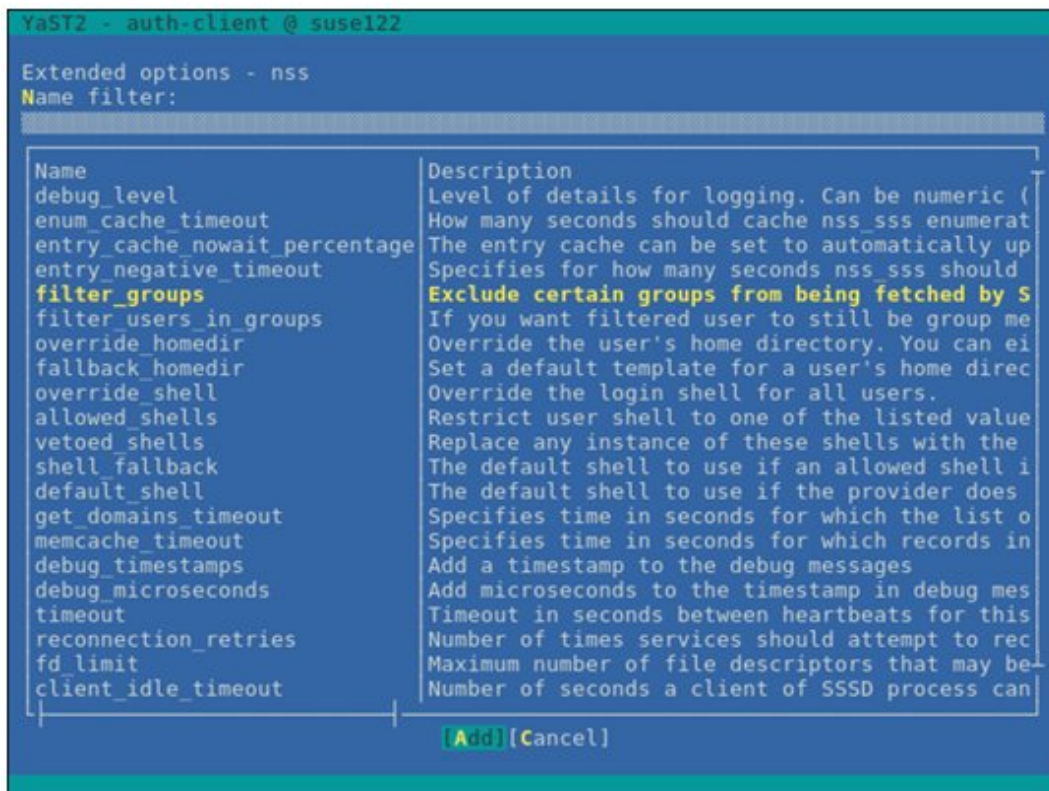
- m. 「root」を入力してから[OK]を選択し、[Enter]キーを押します。



- 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。

```
Exclude certain groups from being fetched by SSS backend
filter_groups
root
[OK] [Cancel]
```

- q. [OK]を選択し、[Enter]キーを押します。

```
YaST2 - auth-client @ suse122

Manage Domain User Logon

Daemon Status: Stopped
[x] Allow Domain User Logon
[x] Create Home Directory
Enable domain data source:
[x] Users
[x] Groups
[ ] Super-User Commands (sudo)
[ ] Map Network Drives (automount)
[ ] SSH Public Keys
[ ] Privilege Account Certificate (MS

Options - Name switch

Name | Value
filter_users | root
filter_groups | root

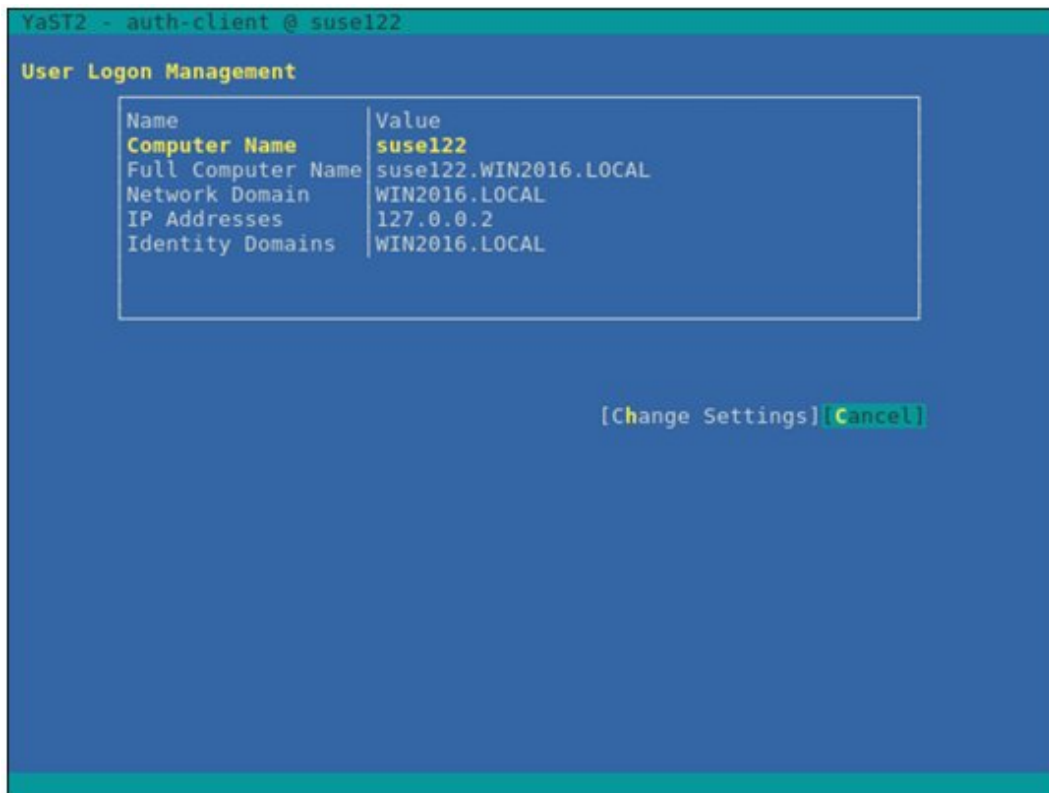
Global Options
Service Options
Authentication
Name switch
Domain Options
WIN2016.LOCAL

[Join Dom][Leave Dom][Clear Domain Cac][Edit][Delete][Extended Options]

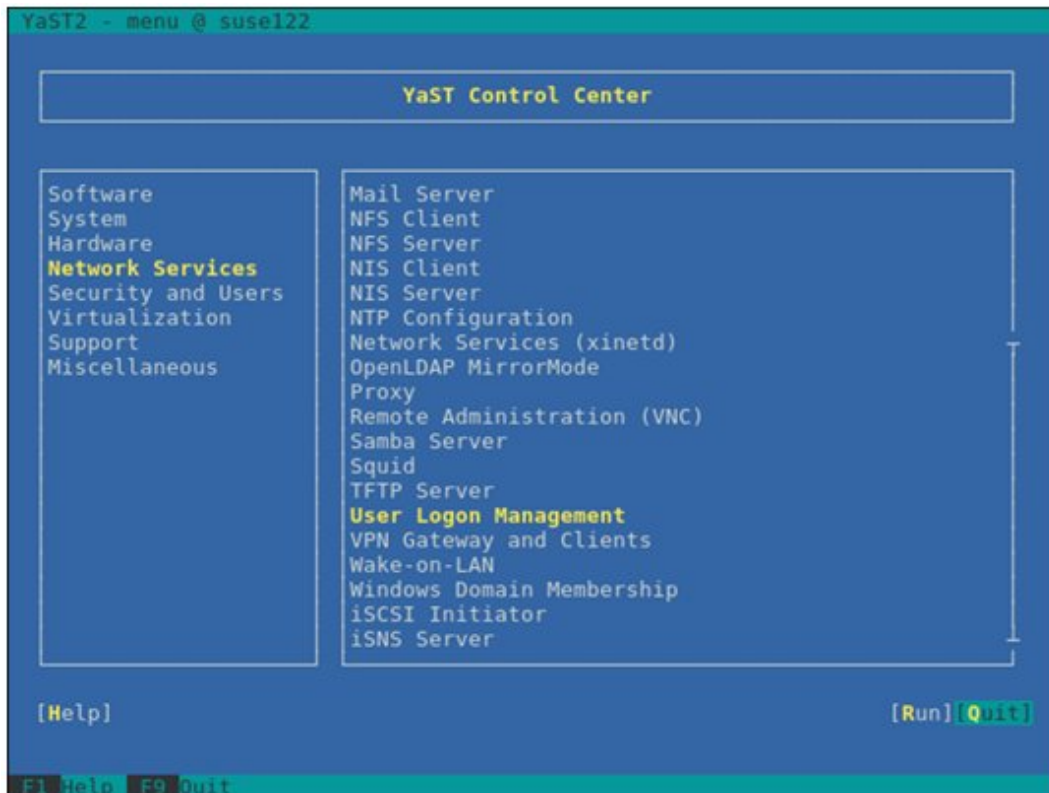
[OK] [Cancel]

F9 Cancel F10 OK
```

- 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IPアドレス>
```

```
# ssh -l <ドメインユーザー名> <監視対象サーバ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.9.3 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サーバ追加」を行い、ISM-VAにDNSサーバを登録してください。

B.9.3 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.10 監視対象への設定手順(仮想化管理ソフトウェア:IPCOM)

B.10.1 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.11 監視対象への設定手順(仮想化管理ソフトウェア:OpenStack)

B.11.1 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
- 自己証明書を作成する



ポイント

自己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情報を調べる事が可能です。

```
# 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他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"}]}]}
```

```

"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

- 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.11.2 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
```

付録C ISM-VAのアンインストール

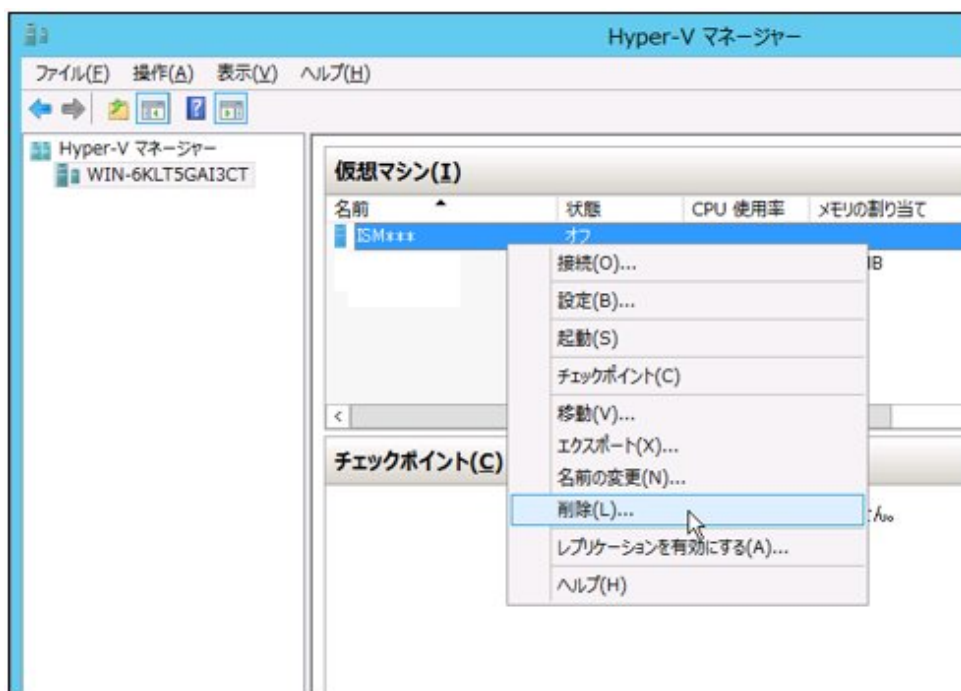
ISM-VAのインストール先に応じてアンインストールします。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMからの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 5.5、またはVMware vSphere Hypervisor 6.0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](#)

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。

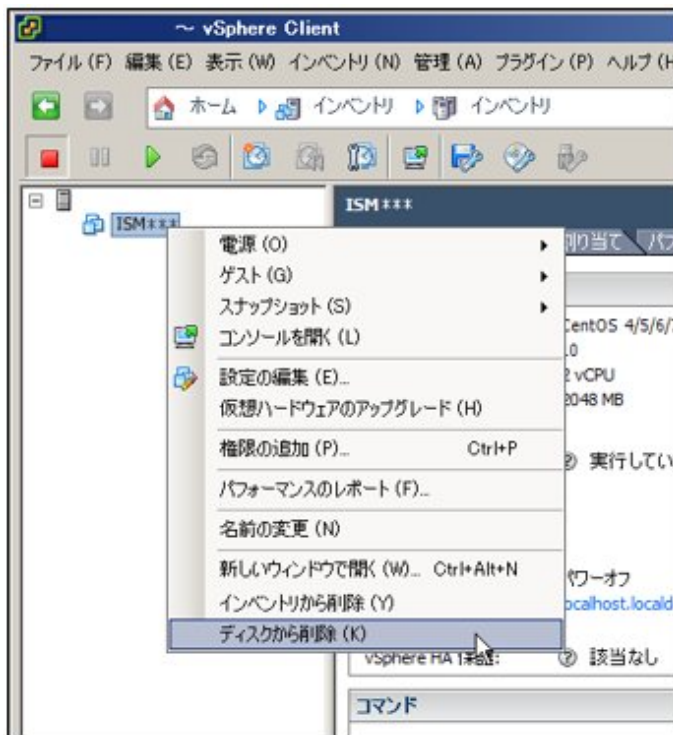


4. 手順2で記録した仮想ハードディスクを、エクスプローラーで削除します。

VMware vSphere Hypervisor 5.5、またはVMware vSphere Hypervisor 6.0からのアンインストール

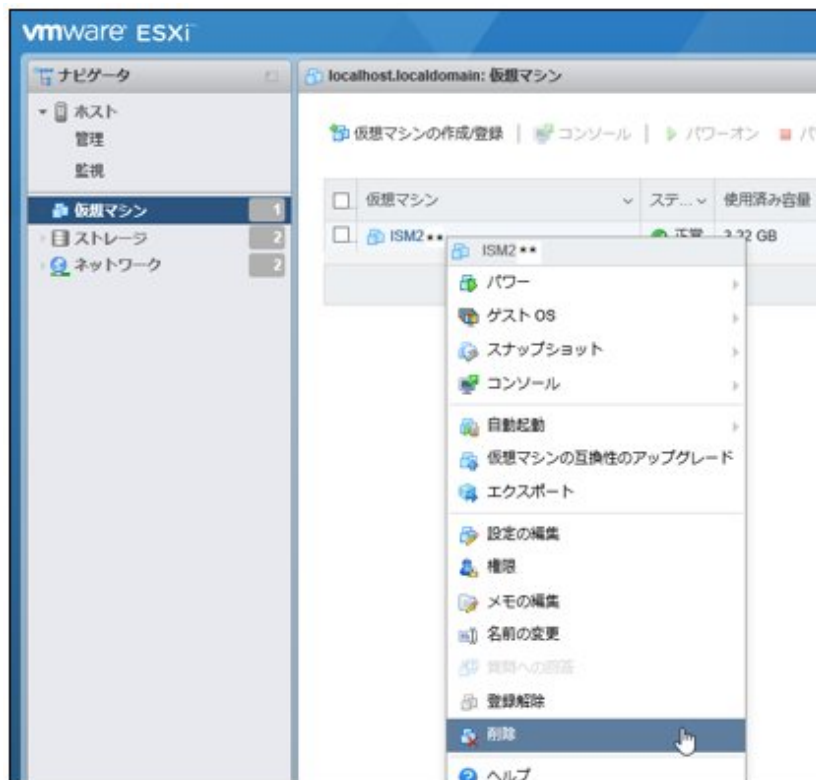
1. ISM-VAを停止します。
詳しくは、「[4.1.2 ISM-VAの終了](#)」を参照してください。

2. vSphere Clientを起動し、インストールしたISM-VAを右クリックして[ディスクから削除]を選択します。



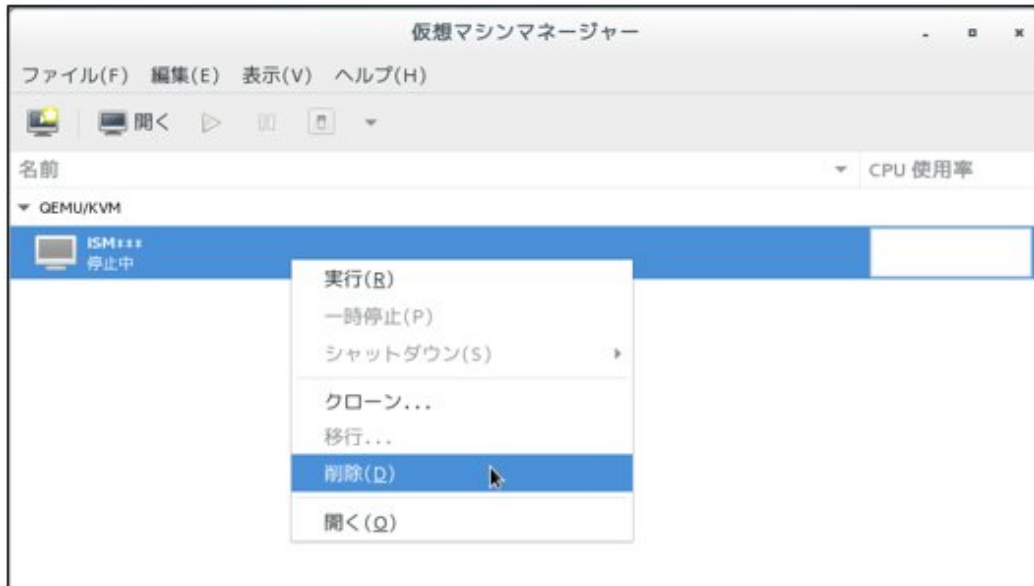
VMware vSphere Hypervisor 6.5以降からのアンインストール

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。



付録D 後継機種のクラスタ拡張

この章では、PRIMEFLEXに後継機種となるサーバを追加する方法について説明します。

D.1 後継機種の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、購入時のサーバと同世代のサーバに加え、後継機種となるサーバを追加可能です。



PRIMERGY M5シリーズはISM 2.4.0.c 以降で使用できます。

D.1.1 追加可能な後継機種サーバ

各PRIMEFLEXに対して、追加可能なサーバの世代は以下のとおりです。

PRIMEFLEXモデル名	クラスタ拡張時に追加するサーバの世代		
	PRIMERGY M2シリーズ	PRIMERGY M4シリーズ	PRIMERGY M5シリーズ
PRIMEFLEX HS V1.0	購入時と同じサーバ世代で追加可能です。	購入時のサーバの後継機種であるため、追加可能です。	購入時のサーバの後継機種であるため、追加可能です。
PRIMEFLEX HS V1.1			
PRIMEFLEX for VMware vSAN	追加できません。	購入時と同じサーバ世代で追加可能です。	購入時のサーバの後継機種であるため、追加可能です。

購入時のサーバ機種に対して、追加可能なサーバの機種は以下のとおりです。

vSANを使用したモデルは、購入時のサーバの後継機種により追加してください。

表D.1 PRIMEFLEX HSの後継機種

購入時のサーバ機種	クラスタ拡張時に追加するサーバの機種		
	PRIMERGY RX2530 M4 PRIMERGY RX2530 M5	PRIMERGY RX2540 M4 PRIMERGY RX2540 M5	PRIMERGY CX2560 M4 PRIMERGY CX2560 M5
PRIMERGY RX2530 M2	購入時のサーバの後継機種であるため、ISM for PRIMEFLEXにより追加可能です。	追加できません。	追加できません。
PRIMERGY RX2540 M2	追加できません。	購入時のサーバの後継機種であるため、ISM for PRIMEFLEXにより追加可能です。	追加できません。
PRIMERGY CX2550 M2	追加できません。	追加できません。	購入時のサーバの後継機種であるため、ISM for PRIMEFLEXにより追加可能です。

表D.2 PRIMEFLEX for VMware vSANの後継機種

購入時のサーバ機種	クラスタ拡張時に追加するサーバの機種		
	PRIMERGY RX2530 M5	PRIMERGY RX2540 M5	PRIMERGY CX2560 M5
PRIMERGY RX2530 M4	購入時のサーバの後継機種であるため、ISM for	追加できません。	追加できません。

購入時のサーバ機種	クラスタ拡張時に追加するサーバの機種		
	PRIMERGY RX2530 M5	PRIMERGY RX2540 M5	PRIMERGY CX2560 M5
	PRIMEFLEXにより追加可能です。		
PRIMERGY RX2540 M4	追加できません。	購入時のサーバの後継機種であるため、ISM for PRIMEFLEXにより追加可能です。	追加できません。
PRIMERGY CX2560 M4	追加できません。	追加できません。	購入時のサーバの後継機種であるため、ISM for PRIMEFLEXにより追加可能です。

D.1.2 ネットワーク構成

後継機種サーバを追加するにあたり、物理／論理ネットワーク構成を購入時のサーバに合わせる必要があります。

既存サーバ(PRIMERGY RX2530 M2／PRIMERGY RX2540 M2)のネットワークインターフェースは、10GBase-T、10GBaseが選択可能であるため、クラスタ拡張時に追加するサーバ(PRIMERGY RX2530 M4／PRIMERGY RX2540 M4／PRIMERGY RX2530 M5／PRIMERGY RX2540 M5)のポート拡張オプション、およびPCIカードは同じポートを選択してください。

既存サーバ(PRIMERGY CX2550 M2)のネットワークインターフェースは、1GBase-T、10GBaseが選択可能であるため、クラスタ拡張時に追加するサーバ(PRIMERGY CX2560 M4／PRIMERGY CX2560 M5)のポート拡張オプション、およびPCIカードは同じポートを選択してください。

既存サーバ(PRIMERGY RX2530 M4／PRIMERGY RX2540 M4)のネットワークインターフェースは、ポート拡張オプション、およびPCIカードが選択可能であるため、クラスタ拡張時に追加するサーバ(PRIMERGY RX2530 M5／PRIMERGY RX2540 M5)のポート拡張オプション、およびPCIカードは同じポートを選択してください。

既存サーバ(PRIMERGY CX2560 M4)のネットワークインターフェースは、ポート拡張オプション、およびPCIカードが選択可能であるため、クラスタ拡張時に追加するサーバ(PRIMERGY CX2560 M5)のポート拡張オプション、およびPCIカードは同じポートを選択してください。

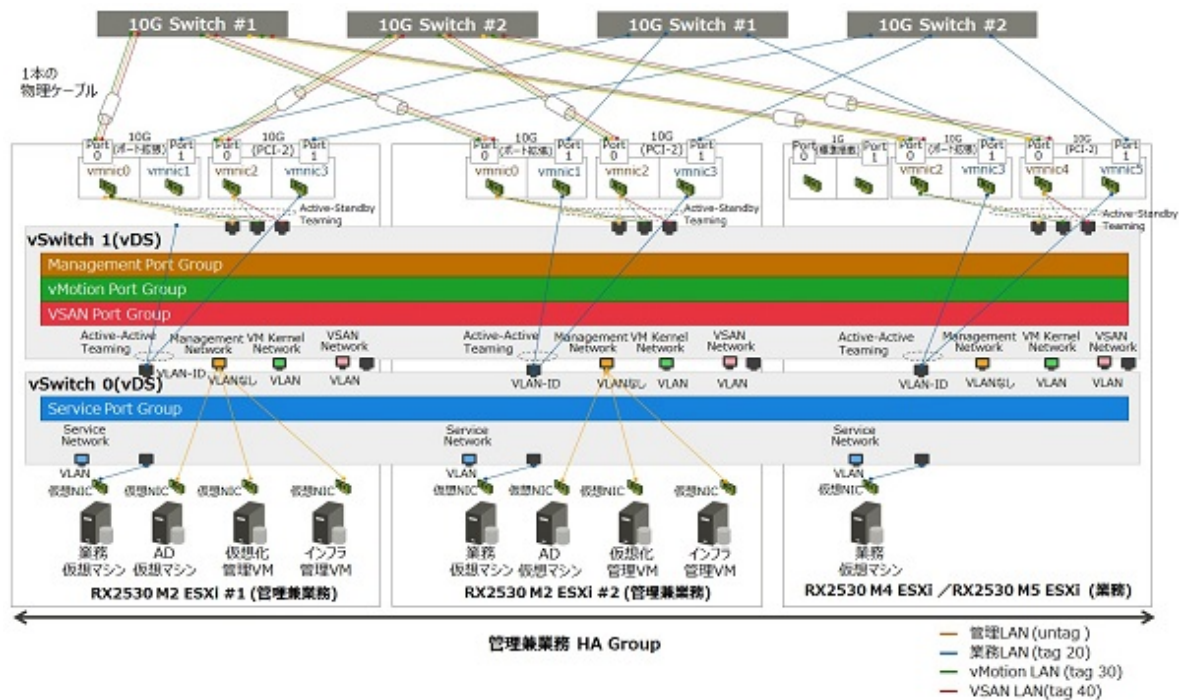
表D.3 PRIMEFLEX HSのネットワーク構成

項目	既存サーバとネットワーク構成		クラスタ拡張時に追加するサーバとネットワーク構成	
サーバ機種	PRIMERGY RX2530 M2 PRIMERGY RX2540 M2	PRIMERGY CX2550 M2	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4 PRIMERGY RX2530 M5 PRIMERGY RX2540 M5	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	- Onboard 1G 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	- Onboard 1G x1ポート - ポート拡張オプション 1G x2ポート - PCI 10G x2ポート

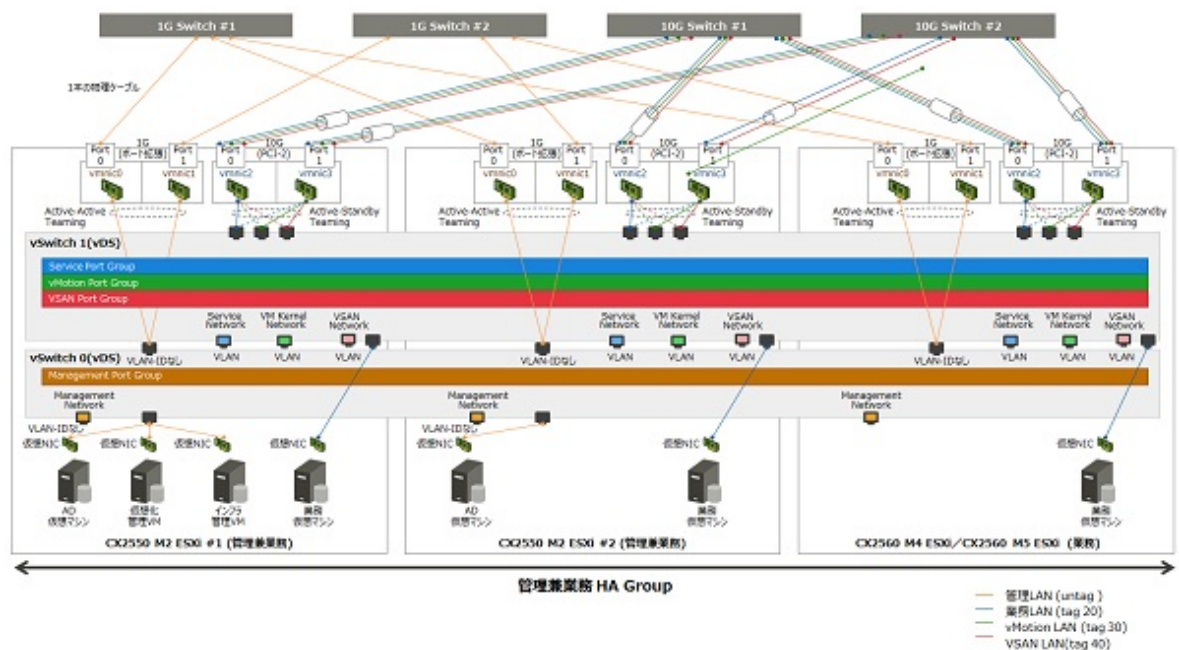
表D.4 PRIMEFLEX for VMware vSANのネットワーク構成

項目	既存サーバとネットワーク構成		クラスタ拡張時に追加するサーバとネットワーク構成	
サーバ機種	PRIMERGY RX2530 M4 PRIMERGY RX2540 M4	PRIMERGY CX2560 M4	PRIMERGY RX2530 M5 PRIMERGY RX2540 M5	PRIMERGY CX2560 M5
ネットワーク構成	- Onboard 1G 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	- Onboard 1G x1ポート - ポート拡張オプション 1G x2ポート - PCI 10G x2ポート	- Onboard 1G 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	- Onboard 1G x1ポート - ポート拡張オプション 1G x2ポート - PCI 10G 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



PRIMEFLEX for VMware vSANへPRIMERGY M5シリーズを追加するためのネットワーク構成は、PRIMERGY M4シリーズを追加する場合と同じです。

D.1.3 ハードウェア要件

SDSでは、既存サーバと同等構成のハードウェアでサーバを追加することが推奨されています。しかし、既存サーバとクラスタ拡張時に追加するサーバ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、既存サーバに対するクラスタ拡張時に追加するサーバのハードウェア構成の選択方針について説明します。

既存サーバとクラスタ拡張時に追加するサーバで関連性があるオプションは、以下のとおりです。

- ベースユニット
- CPU
- メモリ
- HDD
- SSD
- オンボードLAN (Flexible LOM)
- 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の推奨の構成は、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。

ベースユニット

「[D.1.1 追加可能な後継機種サーバ](#)」に記載されたサーバ機種を追加可能です。

CPU

既存サーバとクラスタ拡張時に追加するサーバで搭載可能なCPU世代が異なるため、クラスタ拡張時に追加するサーバに搭載するCPUは、既存サーバに搭載された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に搭載されたCPU以上とします。

CPUの個数は既存サーバと同じとします。

既存サーバに搭載されている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。

メモリ

クラスタ拡張時に追加するサーバに搭載するメモリは、既存サーバ1ノード当たりの搭載メモリの総容量以上となるように搭載します。

既存サーバと同じ型名のメモリが手配可能な場合、同じ型名で、同じ個数を搭載することを推奨します。

同じ型名のメモリが存在しない場合、メモリ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も問題ありません。

HDD(キャパシティ)

クラスタ拡張時に追加するサーバに搭載するHDDは、既存サーバと同じ型名の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。

既存サーバと同じ型名のHDDが、クラスタ拡張時に追加するサーバ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に搭載するHDDは、すべて同じ型名としてください。

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)	既存サーバと同じ
回転数(rpm)	既存サーバと同等以上
セクターサイズ	既存サーバと同じ

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当たりのディスク容量が既存サーバ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	既存サーバと同じ	既存サーバと同じ台数
構成2	既存サーバより容量が多い、かつ最も容量が少ないHDD	既存サーバと同じ台数
構成3	既存サーバより容量が少ない、かつ最も容量が多いHDD	サーバ当たりのキャパシティ容量が既存サーバ以上となる最小の個数(既存サーバより多い台数)
構成4	既存サーバより容量が多い、かつ最も容量が少ないHDD	サーバ当たりのキャパシティ容量が既存サーバ以上となる最小の個数(既存サーバより少ない台数)

以下にHDDの搭載例を示します。

例1:

既存サーバ(vSAN)のHDD構成:900GB x 4台

- ・ クラスタ拡張時に追加するサーバのディスクが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(vSAN)のHDD構成:600GB x 2台

- ・ クラスタ拡張時に追加するサーバのディスクが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。

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に搭載するSSDは、既存サーバと同じ型名の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。

既存サーバと同じ型名のSSDが、クラスタ拡張時に追加するサーバ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に搭載するSSDは、すべて同じ型名としてください。

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)	既存サーバと同じ
記録方式 (MLCなど)	既存サーバと同じ

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当たりのディスク容量が既存サーバ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	既存サーバと同じ	既存サーバと同じ台数	既存サーバと同数を推奨
構成2	既存サーバより容量が多い、かつ最も容量が少ないSSD	既存サーバと同じ台数	
構成3	既存サーバ未満、かつ最も容量が多いSSD	サーバ当たりのキャパシティ容量が既存サーバ以上となる個数 (既存サーバより多い台数)	
構成4	既存サーバより容量が多い、かつ最も容量が少ないSSD	サーバ当たりのキャパシティ容量が既存サーバ以上となる最小の個数 (既存サーバより少ない台数)	

オンボードLAN (Flexible LOMなど)

「[D.1.2 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。

SASコントローラカード

既存サーバと同じ型名が選択可能な場合は、同じ型名を選択します。

同じ型名が存在しない場合は、既存サーバに搭載されているカードの後継品を選択してください。

オプションカード (搭載必須LANカード)

クラスタ拡張時に追加するサーバを既存サーバ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。

「[D.1.2 ネットワーク構成](#)」に記載された要件を満たす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ース (10GBase/10GBase-T) は、既存サーバと同じにしてください。

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、各PRIMEFLEXの要件、およびお客様環境に応じて選択可能です。

D.1.4 ソフトウェア要件

クラスタ拡張時に追加するサーバと既存サーバは、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。

ソフトウェアバージョン

既存サーバ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をサポートしていない場合は、サーバを追加する前に、既存サーバのソフトウェアをアップデートしてください。

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。

表D.5 アップデート方針(vSANの場合)

ソフトウェア名	導入場所	バージョン
VMware vSphere	クラスタ拡張時に追加するサーバ 既存サーバ	既存サーバおよびクラスタ拡張時に追加するサーバで、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、クラスタ拡張時に追加するサーバ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 既存サーバ	既存サーバおよびクラスタ拡張時に追加するサーバで、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、クラスタ拡張時に追加するサーバ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	VMware vSphere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	既存サーバおよびクラスタ拡張時に追加するサーバのVMware vSphere／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	既存サーバおよびクラスタ拡張時に追加するサーバのVMware vSphereをサポートするバージョンを導入してください。

手配品

クラスタ拡張時に追加するサーバ用に手配すべきソフトウェア製品について説明します。

vSANモデルで手配が必要なソフトウェア製品は、以下のとおりです。

ソフトウェア製品	既存サーバとの関連性	選択
VMware vSphereライセンス	あり	必須
vSANライセンス	あり	必須
vCenter Serverライセンス	なし	任意
Windows Serverライセンス	なし	任意
ISM for PRIMEFLEXメディアパック	なし	不要
ISM for PRIMEFLEXサーバライセンス	なし	不要
ISM for PRIMEFLEXノードライセンス	なし	必須

各ソフトウェア製品の詳細は、以下のとおりです。

- VMware vSphereライセンス

既存サーバに導入されているライセンスと同じ(エディション、サポートレベル[平日|24H])ライセンスを手配してください。サポート年数については、お客様の要件に応じて変更可能です。

- vSANライセンス

既存サーバに導入されているライセンスと同じ(エディション、サポートレベル[平日|24H])ライセンスを手配してください。サポート年数については、お客様の要件に応じて変更可能です。

- vCenter Serverライセンス

既存サーバの構成と関連がありません。2個以上のvCenter Serverを導入する場合は手配してください。

- Windows Serverライセンス

既存サーバの構成と関連がありません。必要に応じて手配してください。

- ISM for PRIMEFLEXメディアパック

クラスタ拡張時に追加するサーバに対してISM for PRIMEFLEXのメディアパックの追加手配は不要です。

- ISM for PRIMEFLEXサーバライセンス

クラスタ拡張時に追加するサーバに対してISM for PRIMEFLEXのサーバライセンスの追加手配は不要です。

- ISM for PRIMEFLEXノードライセンス

既存サーバの構成と関連がありません。クラスタ拡張時に追加するサーバ台数分のノードライセンスを手配してください。

D.2 後継機種のクラスタ拡張

後継機種のクラスタ拡張は、以下の作業フローで行います。

表D.6 後継機種のクラスタ拡張フロー

クラスタ拡張手順		作業内容
1	事前準備	- 管理VMのサイジング - ソフトウェア、ファームウェアのアップデート - CPUの互換性に関する設定
2	ISM for PRIMEFLEXによるクラスタ拡張	クラスタ拡張の実行

D.2.1 事前準備

クラスタ拡張を実施する前に行う作業について説明します。

管理VMのサイジング

追加するサーバの台数に応じて、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。

管理兼業務サーバの物理リソースが不足する場合は、管理兼業務サーバに物理メモリ／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	ディスク	
PRIMEFLEX HS V1.0	インフラ管理VM (ISM for PRIMEFLEX)	4vCPU	8GB	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	8GB	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 V1	インフラ管理VM (ISM for PRIMEFLEX)	4vCPU	8GB	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

ソフトウェア、ファームウェアのアップデート

クラスタ拡張時に追加するサーバおよび既存サーバのハイパーバイザーバージョン、パッチバージョンが同一になるよう、必要に応じて以下をアップデートします。

アップデート手順については、各ソフトウェアのマニュアルを参照してください。

- PRIMERGYのファームウェア
- ハイパーバイザーのバージョン、パッチバージョン
- vCSAのバージョン(vSANの場合)
- ISM for PRIMEFLEXのバージョン
- RAID Managerのバージョン(vSANの場合)

CPUの互換性に関する設定

CPUの世代が異なるサーバ間でライブマイグレーションをするには、各モデルで設定が必要です。

VMwareでプロセッサ世代の異なるホスト間でライブマイグレーションをするには、クラスタに対してEVC (Enhanced vMotion Compatibility) を設定する必要があります。有効にした場合、vMotionの互換性に影響を与えるCPUの機能がマスクされるため、アプリケーションによっては予期しない動作をすることがあります。

詳細、および設定方法については、以下のサイトの「vCenter Serverおよびホスト管理」を参照してください。

<https://docs.vmware.com/jp/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-651-host-management-guide.pdf>

EVC機能を有効にする際、EVCに設定するCPUレベルよりも高いレベルで仮想マシンが起動している場合、設定したレベルに合わせなければ、EVCを有効にしているクラスタ上のホスト間でvMotionが行えません。

仮想マシンのCPUレベルは、仮想マシンの起動時にホストから取得するCPU情報に含まれます。そのため、高いCPUレベルで起動している場合、仮想マシンを再起動する必要があります。

現在、稼働している仮想マシンのCPUレベルと同等のレベルでEVCを設定する場合は、仮想マシンを停止せずにEVCを有効にできます。

D.2.2 ISM for PRIMEFLEXによるクラスタ拡張

ISM for PRIMEFLEXによるクラスタ拡張については、以下を参照してください。

- 『操作手順書』の「6.9 PRIMEFLEX HS／PRIMEFLEX for VMware vSANのクラスタを拡張する」

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: 検出したノードの登録に失敗する

原因／対処

検出したノードのシリアル番号を確認してください。すでにノード登録されている場合にはノードを削除してから登録してください。

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]-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]-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]-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:Internet Explorer 11を使用している場合に、ファイルのダウンロードが失敗する。

原因／対処

Internet Explorerの設定によりファイルのダウンロードが失敗します。以下の設定を変更してください。

[インターネットオプション]-[セキュリティ]タブで[レベルのカスタマイズ]ボタンを選択し、[ダウンロード]-[ファイルのダウンロード]を[有効にする]に変更。

現象:Microsoft Active DirectoryをLDAPサーバ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。

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 DVDおよびServerView Suite Update DVDがインポートされている必要があります。ServerView Suite DVDおよび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よって設定可能な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。