

FUJITSU Software

Infrastructure Manager V2.3

Infrastructure Manager for PRIMEFLEX V2.3

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

操作手順書

CA92344-2502-03
2018年12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導入手順、利用シーンに応じた操作手順を説明します。

- 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 V2.3 Infrastructure Manager for PRIMEFLEX V2.3 ユーザーズマニュアル	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、『ユーザーズマニュアル』と表記します。
FUJITSU Software Infrastructure Manager V2.3 Infrastructure Manager for PRIMEFLEX V2.3 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 V2.3 Infrastructure Manager for PRIMEFLEX V2.3 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 V2.3 Infrastructure Manager for PRIMEFLEX V2.3 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する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 V2.3 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する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 V2.3 Infrastructure Manager for PRIMEFLEX V2.3 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 V2.3 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す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 V2.3 Infrastructure Manager for PRIMEFLEX V2.3 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。
FUJITSU Software Infrastructure Manager Plug-in for Microsoft System Center Operations Manager 1.2 セットアップガイド (Windows Server 2012 R2 版)	ISM Plug-in for Microsoft System Center Operations Manager 1.2 (Windows Server 2012 R2 版)の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。

マニュアル名称	説明
FUJITSU Software Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager 1.2 セットアップガイド (Windows Server 2012 R2 版)	ISM Plug-in for Microsoft System Center Virtual Machine Manager 1.2 (Windows Server 2012 R2 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for Microsoft System Center Operations Manager 1.2 セットアップガイド (Windows Server 2016 / 2019 版)	ISM Plug-in for Microsoft System Center Operations Manager 1.2 (Windows Server 2016 / 2019 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager 1.2 セットアップガイド (Windows Server 2016 / 2019 版)	ISM Plug-in for Microsoft System Center Virtual Machine Manager 1.2 (Windows Server 2016 / 2019 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for VMware vCenter Server 1.2 セットアップガイド (vCenter Server 6.0 版)	ISM Plug-in for VMware vCenter Server 1.2 (vCenter Server 6.0 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for VMware vCenter Server Appliance 1.2 セットアップガイド (vCenter Server Appliance 6.0 版)	ISM Plug-in for VMware vCenter Server 1.2 (vCenter Server Appliance 6.0 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for VMware vCenter Server 1.2 セットアップガイド (vCenter Server 6.5/6.7 版)	ISM Plug-in for VMware vCenter Server 1.2 (vCenter Server 6.5/6.7 版) の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。
FUJITSU Software Infrastructure Manager Plug-in for VMware vCenter Server Appliance 1.2 セットアップガイド (vCenter Server Appliance 6.5/6.7 版)	ISM Plug-in for VMware vCenter Server 1.2 (vCenter Server Appliance 6.5/6.7 版) の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。
FUJITSU Software Infrastructure Manager Management Pack for VMware vRealize Operations 1.0 セットアップガイド	ISM Management Pack for VMware vRealize Operations 1.0 の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。

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、サーバやストレージなどのICT機器の統合的な管理・運用を検討される方で、かつ、ハードウェア、オペレーティングシステムおよびソフトウェアについて基礎的な知識を持つ方を対象とします。

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 7.5 (for Intel64)	RHEL 7.5	Red Hat Enterprise Linux または Linux
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	

正式名称	略称	
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)	
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 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、逆アセンブルをともなうリバースエンジニアリングを行うことはできません。

免責事項

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

登録商標について

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

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

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

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

VMware、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。

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 2018 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	2018年8月	新規作成	—	—
02	2018年10月	ISM 2.3.0.bパッチ適用による変更 新規追加	6.7 PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタを作成する (ISM 2.3.0.b以降)	—
			6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する (ISM 2.3.0.b以降)	—
		ISM 2.3.0.bパッチ適用による変更 記事を追加	2.1.1.3 KVMへISM-VAをインストールする	—
			6.8.2.2 クラスタ拡張手順	—
			6.9.2.2 クラスタ拡張手順	—
			8.2.1 GUIを利用して保守資料を採取する	保守資料の採取をキャンセルする
		手順を修正	6.5.3 ファームウェアローリングアップデートを実施する	—
		記事を追加	6.9.2.1 クラスタ拡張の動作要件	—
03	2018年12月	手順を修正	6.7.2.2クラスタ作成手順	—
			6.9.2.2クラスタ拡張手順	—
		記事を追加	6.6.3.1クラスタ作成を確認する 6.8.3.1クラスタ拡張を確認する	—

目 次

第1章 共通的操作.....	1
1.1 ヘルプ画面を表示する.....	1
1.2 画面を更新する.....	1
第2章 ISMを導入する.....	2
2.1 ISM-VAをインストールする.....	2
2.1.1 ISM-VAをインポートする.....	2
2.1.1.1 Microsoft Windows Server Hyper-VへISM-VAをインストールする.....	2
2.1.1.2 VMware vSphere HypervisorへISM-VAをインストールする.....	4
2.1.1.3 KVMへISM-VAをインストールする.....	10
2.1.2 ISM-VAをエクスポートする.....	12
2.1.2.1 Microsoft Windows Server Hyper-Vで動作するISM-VAをバックアップする.....	13
2.1.2.2 VMware vSphere Hypervisor 5.5またはVMware vSphere Hypervisor 6.0で動作するISM-VAをバックアップする.....	13
2.1.2.3 VMware vSphere Hypervisor 6.5で動作するISM-VAをバックアップする.....	13
2.1.2.4 KVMで動作するISM-VAをバックアップする.....	14
2.1.3 仮想ディスクを接続する.....	14
2.1.3.1 ISM-VA全体に対して仮想ディスクを割り当てる.....	15
2.1.3.2 ユーザーグループに対して仮想ディスクを割り当てる.....	17
2.1.4 ライセンスを登録する.....	20
2.2 データセンターを登録／削除する.....	22
2.3 フロアを登録／削除する.....	23
2.4 ラックを登録／削除する.....	23
2.5 フロア内にラックを配置する.....	24
2.6 アラーム設定をする (ISM内部のイベント).....	24
2.6.1 アクション (通知方法) を設定する.....	25
2.6.1.1 外部ホスト上に配置したスクリプトを実行する.....	25
2.6.1.2 メールを送信する.....	26
2.6.1.3 トラップ送信／転送を行う.....	26
2.6.1.4 Syslog転送を行う.....	27
2.6.2 アクション (通知方法) をテストする.....	28
2.6.3 ISM内部のイベントを対象にアラームを設定する.....	28
2.7 管理者ユーザーを登録する.....	29
2.7.1 ISMのユーザーを管理する.....	29
2.7.1.1 ユーザーを追加する.....	29
2.7.1.2 ユーザーを編集する.....	30
2.7.1.3 ユーザーを削除する.....	31
2.7.2 ユーザーグループを管理する.....	31
2.7.2.1 ユーザーグループを追加する.....	31
2.7.2.2 ユーザーグループを編集する.....	33
2.7.2.3 ユーザーグループを削除する.....	34
2.7.3 Microsoft Active DirectoryまたはLDAPと連携する.....	34
2.7.4 ノードグループを管理する.....	36
2.7.4.1 ノードグループを追加する.....	36
2.7.4.2 ノードグループを編集する.....	36
2.7.4.3 ノードグループを削除する.....	38
第3章 管理対象ノードを登録／設定／削除する.....	39
3.1 管理対象ノードを登録／削除する.....	39
3.1.1 ネットワーク内ノードを検出してノード登録する.....	39
3.1.2 ノードを直接登録する.....	43
3.1.3 ノードを削除する.....	50
3.2 ノードの設定を行う.....	50
3.2.1 アラーム設定をする (管理対象機器のイベント).....	50
3.2.1.1 アクション (通知方法) を設定する.....	50
3.2.1.2 アラーム共通設定をする.....	51
3.2.1.3 管理対象機器を対象にアラーム設定をする.....	51

3.2.2 SNMPトラップ受信設定をする.....	51
3.2.3 ログ収集スケジュールを設定する.....	52
3.3 サーバに各種設定／OSインストールをする.....	52
3.3.1 プロファイルでBIOS／iRMC／MMB／仮想IOを設定する.....	52
3.3.2 プロファイルでサーバにOSをインストールする.....	54
3.3.3 ポリシーを作成してプロファイルの作成を簡略化する.....	55
3.4 スイッチ／ストレージを設定する.....	56
3.4.1 プロファイルでスイッチ／ストレージを設定する.....	56
3.4.2 ネットワークマップからLANスイッチの設定を変更する.....	56
3.5 パスワードを変更する.....	57
3.5.1 管理対象ノードのパスワードを変更する.....	57
3.5.2 OSのパスワードを変更する.....	58
第4章 管理対象ノードの状態を確認する.....	59
4.1 ダッシュボードを操作する.....	59
4.2 ノードの位置を確認する.....	59
4.3 ノードの状態を確認する.....	60
4.4 ノードの通知情報を表示する.....	61
4.5 監視履歴をグラフ表示する.....	61
4.5.1 ノードごとに監視履歴をグラフ表示する.....	62
4.5.2 複数ノードの監視履歴をグラフ表示する.....	62
4.6 ファームウェアバージョンを確認する.....	63
4.7 ノードログを表示する.....	63
4.8 保管ログをダウンロードする.....	63
第5章 異常な管理対象ノードを特定する.....	65
5.1 異常が発生しているノードを確認する.....	65
5.2 ネットワーク上の異常箇所／影響範囲を確認する.....	65
5.3 管理対象ノードのログを収集する.....	66
第6章 対象ノードを管理／操作するその他の機能.....	67
6.1 ネットワークマップを設定する.....	67
6.2 仮想マシン／仮想リソースの情報を表示する.....	68
6.2.1 仮想化管理ソフトウェアを登録する.....	68
6.2.2 管理対象サーバ上の仮想マシンの情報を確認する.....	68
6.2.3 仮想リソースの情報を確認する.....	69
6.3 サーバのファームウェアをアップデートする.....	71
6.4 電力制御を行う.....	73
6.4.1 現在の電力制御の状態を確認する.....	74
6.4.2 ラックの電力制御設定を追加／編集する.....	74
6.4.3 ラックの電力制御ポリシーを有効化する.....	76
6.4.4 ラックの電力制御設定を削除する.....	76
6.5 ファームウェアをローリングアップデートする.....	77
6.5.1 ファームウェアローリングアップデート機能の動作要件.....	77
6.5.2 設定ファイルを編集する.....	78
6.5.3 ファームウェアローリングアップデートを実施する.....	82
6.6 PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版クラスタを作成する.....	86
6.6.1 事前準備.....	87
6.6.1.1 ADVIMの証明書を作成する.....	87
6.6.1.1.1 WinRMサービスの起動を確認する.....	87
6.6.1.1.2 WinRMサービスを設定する.....	88
6.6.1.1.3 ファイアーウォールのポートを開放する.....	91
6.6.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する.....	92
6.6.1.2 DNSへホストレコードを登録する.....	92
6.6.1.3 DHCPを設定する.....	93
6.6.1.4 OSインストール媒体のISOイメージをISM-VAへインポートする.....	93
6.6.1.5 VMware ESXiパッチをアップロードする.....	93
6.6.1.6 VMware SMIS Providerをアップロードする.....	94

6.6.1.7 プロファイルを作成する	94
6.6.1.8 設置と結線を行う	95
6.6.1.9 iRMCのIPアドレスを設定する	95
6.6.1.10 BIOSを設定する	96
6.6.1.11 ISMへノードを登録する	96
6.6.2 クラスタ作成を実行する	97
6.6.2.1 クラスタ作成の動作要件	97
6.6.2.2 クラスタ作成手順	98
6.6.3 事後処理	103
6.6.3.1 クラスタ作成を確認する	103
6.6.3.2 vCenter Serverの検知アラームを設定する	105
6.6.3.3 VMware vSphereの制限事項／注意事項	106
6.6.3.4 ServerView RAID Managerに新規クラスタを構成するサーバを登録する	106
6.6.3.5 証明書を削除する	106
6.7 PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタを作成する (ISM 2.3.0.b以降)	107
6.7.1 事前準備	107
6.7.1.1 新規クラスタを構成するサーバの証明書を作成する	107
6.7.1.2 DHCPを設定する	109
6.7.1.3 OSインストール媒体のISOイメージをISM-VAへインポートする	109
6.7.1.4 プロファイルを作成する	109
6.7.1.5 設置と結線を行う	110
6.7.1.6 iRMCのIPアドレスを設定する	110
6.7.1.7 BIOSを設定する	110
6.7.1.8 システムディスク(RAID1)を作成する	111
6.7.1.9 ISMへノードを登録する	112
6.7.2 クラスタ作成を実行する	112
6.7.2.1 クラスタ作成の動作要件	112
6.7.2.2 クラスタ作成手順	113
6.7.3 事後処理	120
6.7.3.1 クラスタ情報の取得と更新を行う	120
6.7.3.2 クラスタ作成を確認する	120
6.7.3.3 業務用仮想スイッチに登録する	121
6.7.3.4 システムボリューム名を設定する	122
6.7.3.5 新規クラスタを構成するサーバのブラウザを設定する	122
6.7.3.6 証明書を削除する	122
6.7.3.7 不要ファイルを削除する	123
6.8 PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版クラスタを拡張する	123
6.8.1 事前準備	124
6.8.1.1 ADVmの証明書を作成する	124
6.8.1.1.1 WinRMサービスの起動を確認する	124
6.8.1.1.2 WinRMサービスを設定する	125
6.8.1.1.3 ファイアーウォールのポートを開放する	128
6.8.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する	129
6.8.1.2 DNSへホストレコードを登録する	129
6.8.1.3 DHCPを設定する	130
6.8.1.4 OSインストール媒体のISOイメージをISM-VAへインポートする	130
6.8.1.5 VMware ESXiパッチをアップロードする	130
6.8.1.6 VMware SMIS Providerをアップロードする	131
6.8.1.7 プロファイルを作成する	131
6.8.1.8 クラスタ定義パラメーターの作成と編集を行う	132
6.8.1.9 設置と結線を行う	133
6.8.1.10 iRMCのIPアドレスを設定する	133
6.8.1.11 BIOSを設定する	133
6.8.1.12 ISMへノードを登録する	134
6.8.2 クラスタ拡張を実行する	134
6.8.2.1 クラスタ拡張の動作要件	134
6.8.2.2 クラスタ拡張手順	135

6.8.3 事後処理	139
6.8.3.1 クラスタ拡張を確認する	139
6.8.3.2 VMware vSphereの制限事項／注意事項	141
6.8.3.3 業務用仮想分散スイッチに登録する	141
6.8.3.4 クラスタ拡張時に追加したサーバをServerView RAID Managerに登録する	145
6.8.3.5 証明書を削除する	146
6.9 PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタを拡張する	146
6.9.1 事前準備	146
6.9.1.1 クラスタ拡張時に追加するサーバの証明書を作成する	146
6.9.1.2 DHCPを設定する	148
6.9.1.3 OSインストール媒体のISOイメージをISM-VAへインポートする	148
6.9.1.4 プロファイルを作成する	148
6.9.1.5 クラスタ定義パラメーターの作成と編集を行う	149
6.9.1.6 設置と結線を行う	149
6.9.1.7 iRMCのIPアドレスを設定する	150
6.9.1.8 BIOSを設定する	150
6.9.1.9 システムディスク(RAID1)を作成する	150
6.9.1.10 ISMへノードに登録する	151
6.9.2 クラスタ拡張を実行する	152
6.9.2.1 クラスタ拡張の動作要件	152
6.9.2.2 クラスタ拡張手順	153
6.9.3 事後処理	159
6.9.3.1 クラスタ情報の取得と更新を行う	159
6.9.3.2 クラスタ拡張を確認する	159
6.9.3.3 業務用仮想スイッチに登録する	160
6.9.3.4 システムボリューム名を設定する	161
6.9.3.5 クラスタ拡張時に追加したサーバのブラウザを設定する	161
6.9.3.6 証明書を削除する	161
6.9.3.7 不要ファイルを削除する	161
6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する (ISM 2.3.0.b以降)	162
6.10.1 クラスタ定義パラメーターをエクスポートする	162
6.10.2 クラスタ定義パラメーターをインポートする	163
6.10.3 クラスタ定義パラメーターを削除する	165
第7章 管理対象ノードのトラブルに備える	167
7.1 サーバの設定をバックアップ／リストアする	167
7.1.1 サーバの設定をバックアップする	167
7.1.2 バックアップファイルからプロファイルを作成する	167
7.1.3 バックアップファイルからポリシーを作成する	168
7.1.4 サーバの設定をインポートする	168
7.1.5 サーバの設定をリストアする	168
7.2 スイッチやストレージの設定をバックアップ／リストアする	169
7.2.1 スイッチやストレージの設定をバックアップする	169
7.2.2 スイッチやストレージの設定をエクスポートする	169
7.2.3 スイッチの設定をインポートする	169
7.2.4 スイッチの設定をリストアする	170
第8章 ISMのトラブルに備える／対処する	172
8.1 ISMをバックアップ／リストアする	172
8.1.1 ISMのバックアップ／リストアの事前準備を行う	172
8.1.2 ISMをバックアップする	173
8.1.3 ISMをリストアする	174
8.2 保守資料を採取する	175
8.2.1 GUIを利用して保守資料を採取する	175
8.2.2 コマンドを実行して保守資料を採取する	177
第9章 ISMを更新する	178
9.1 ISM-VAに修正パッチを適用する	178

9.2 ISM-VAをアップグレードする.....	179
---------------------------	-----

第1章 共通的な操作

この章では、各画面での共通する操作を説明します。

1.1 ヘルプ画面を表示する

ISMは画面ごとに、より詳しい説明のためのヘルプ画面を用意しています。表示内容の説明はヘルプ画面を参照してください。

なお、ヘルプ画面の表示方法は2つあります。操作画面に適した表示方法を選択してください。

- ・ ISMのGUIでそれぞれの画面表示中に、右上の[?]ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択
- ・ 上記以外の画面 (ウィザードなど) 表示中に、右上の[?]を選択

1.2 画面を更新する

ISMは、一部の画面を除き、画面表示の際に情報を取得します。各画面の表示中は、画面に含まれる情報を自動更新しません。最新の状態を表示したい場合は、画面を更新してください。

更新ボタン( 更新)を選択すると、情報を再取得し画面が更新されます。

第2章 ISMを導入する

この章では、ISM導入時に必要となる操作を説明します。

2.1 ISM-VAをインストールする

ISMの運用に必要な以下のハイパーバイザーでの操作について説明します。

- [2.1.1 ISM-VAをインポートする](#)
- [2.1.2 ISM-VAをエクスポートする](#)
- [2.1.3 仮想ディスクを接続する](#)

上記操作実施後、ISM-VA管理機能でライセンスを登録します。

- [2.1.4 ライセンスを登録する](#)

2.1.1 ISM-VAをインポートする

ISMソフトウェアは、「FUJITSU Software Infrastructure Manager 2.3 メディアパック」に同梱されています。

インストール先となるハイパーバイザーに応じた手順で、ISM-VAをインストールします。

ISM-VAのインストールは、ハイパーバイザーのインポートの機能を利用して行います。

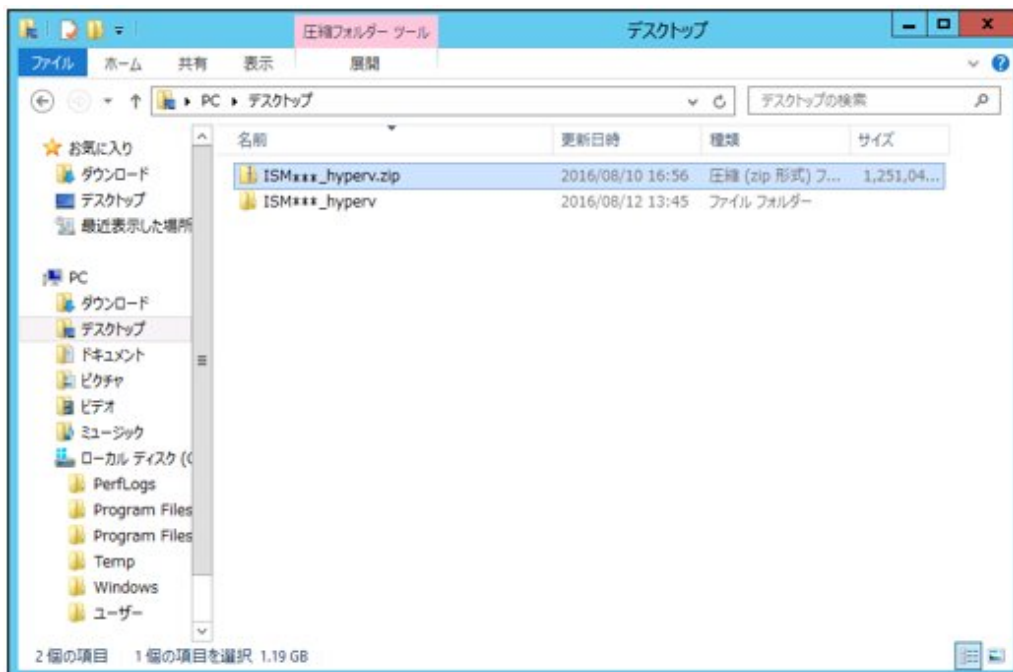
以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMへのISM-VAのインストール手順を説明します。

- [2.1.1.1 Microsoft Windows Server Hyper-VへISM-VAをインストールする](#)
- [2.1.1.2 VMware vSphere HypervisorへISM-VAをインストールする](#)
- [2.1.1.3 KVMへISM-VAをインストールする](#)

2.1.1.1 Microsoft Windows Server Hyper-VへISM-VAをインストールする

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。

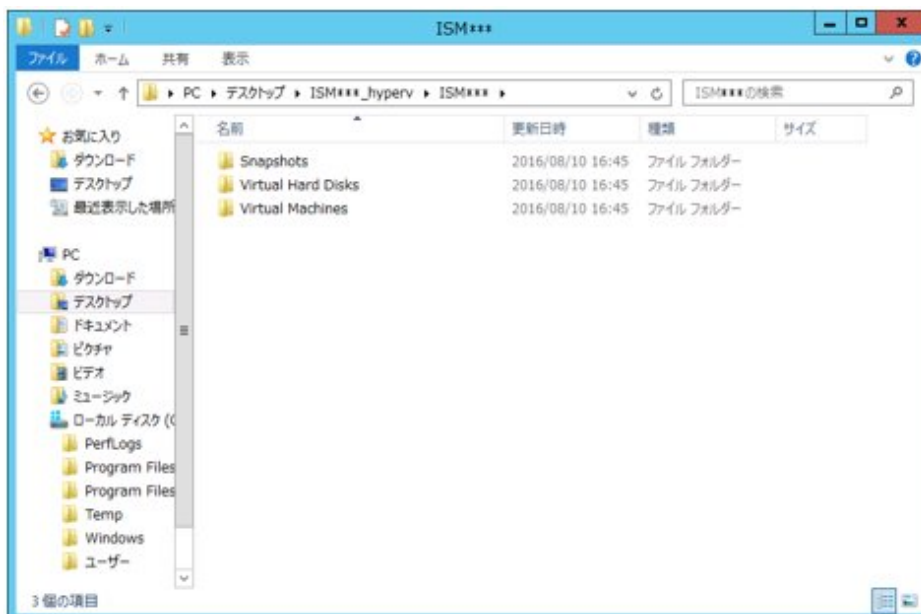


2. Hyper-Vマネージャーを起動し、Hyper-VホストであるWindowsサーバを右クリックして[仮想マシンのインポート]を選択します。

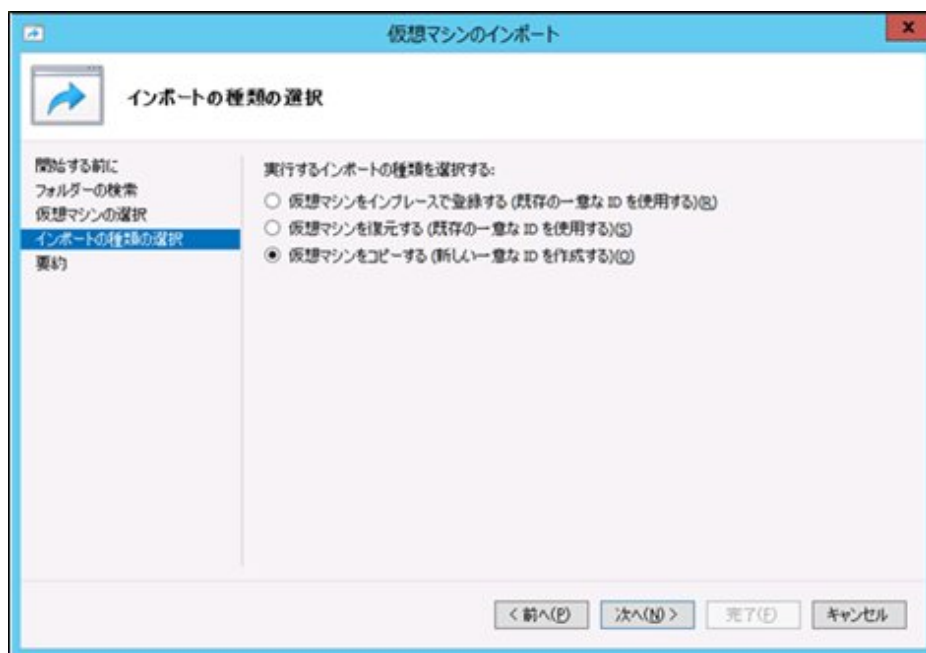


3. 「フォルダーの選択」画面で、手順1で展開したディレクトリを選択します。

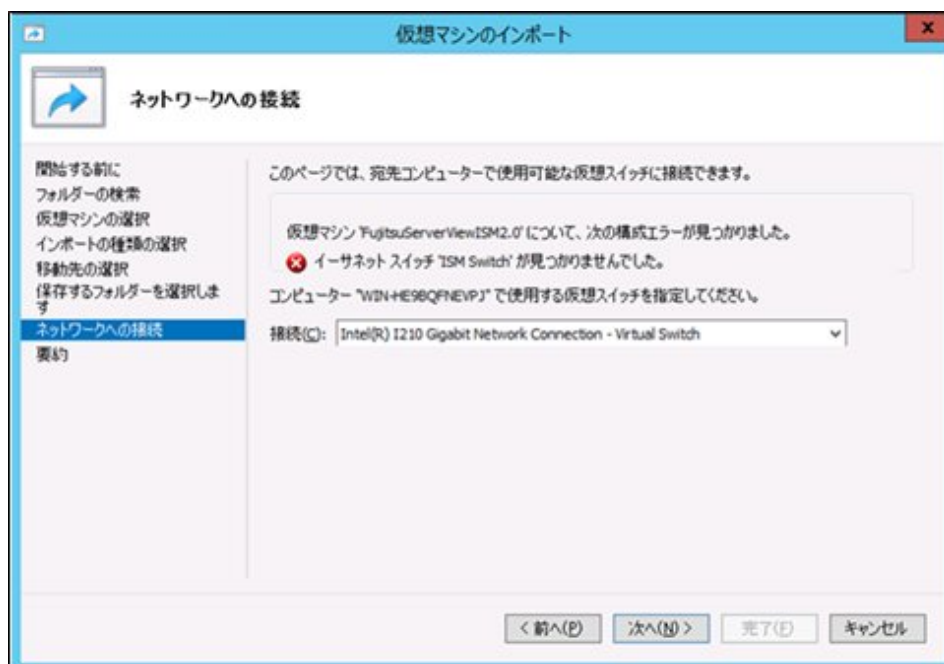
選択するディレクトリは、「Snapshots」、「Virtual Hard Disks」、「Virtual Machines」というディレクトリの親ディレクトリです。



4. 「インポートの種類を選択」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。

2.1.1.2 VMware vSphere HypervisorへISM-VAをインストールする

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。

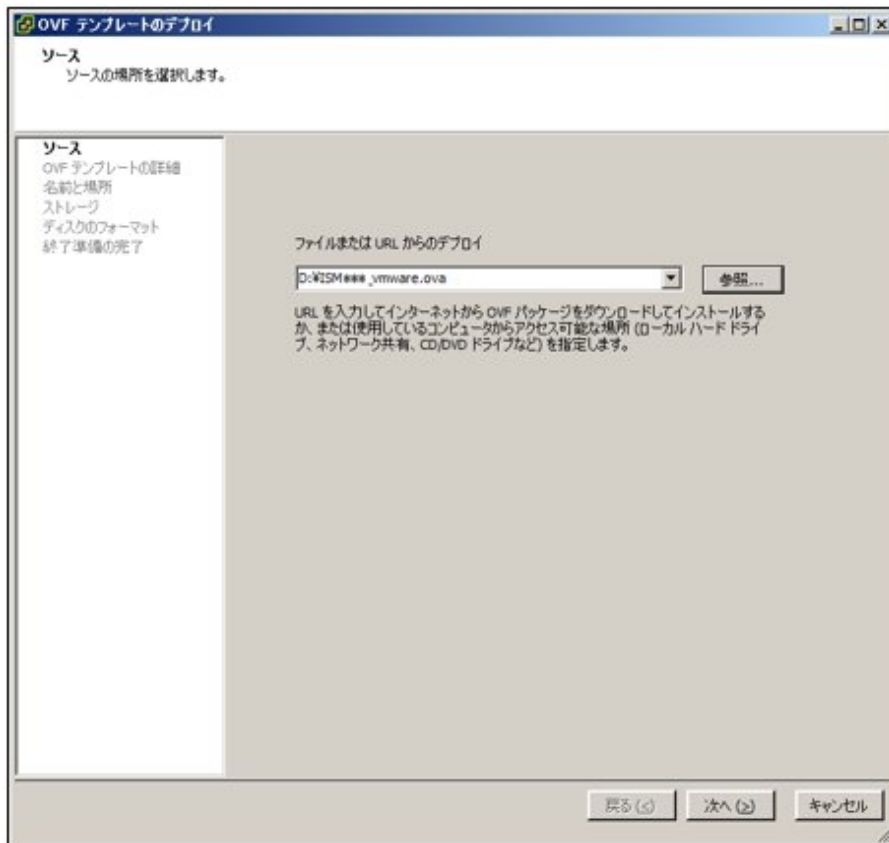
- [VMware ESXi 5.5またはVMware ESXi 6.0へインストールする](#)
- [VMware ESXi 6.5以降へインストールする](#)

VMware ESXi 5.5またはVMware ESXi 6.0へインストールする

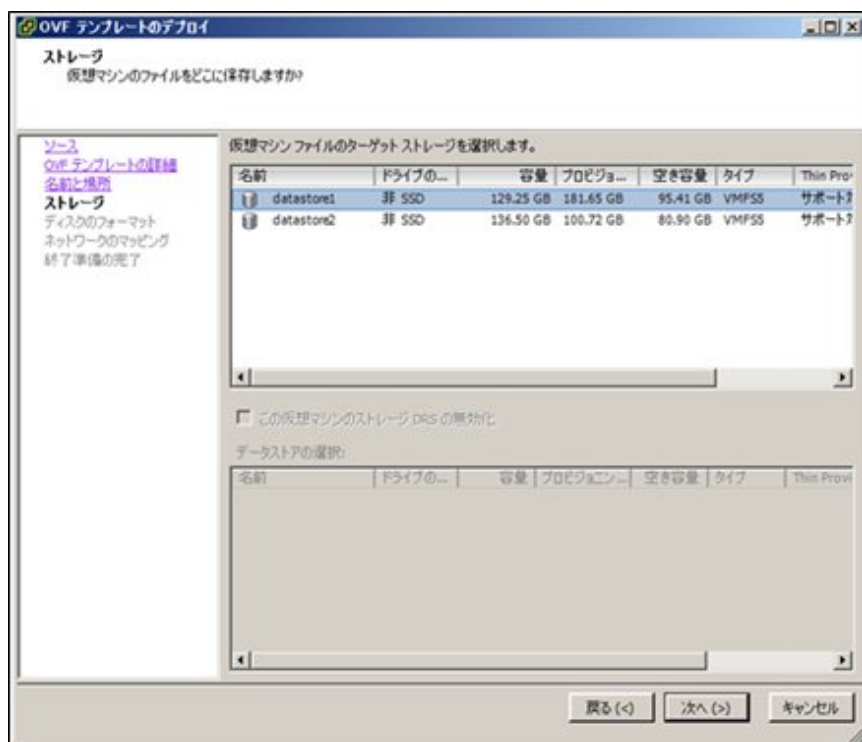
1. vSphere Clientを起動し、[ファイル]メニューから[OVFテンプレートのデプロイ]を選択します。



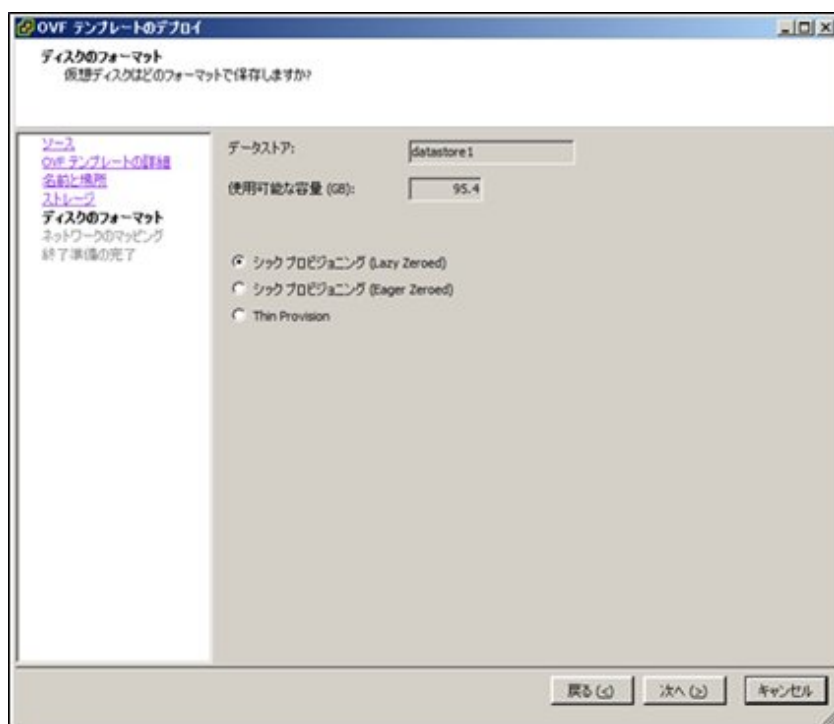
2. ソースの選択画面で、DVDメディアに含まれるovaファイルを選択し、[次へ]を選択します。



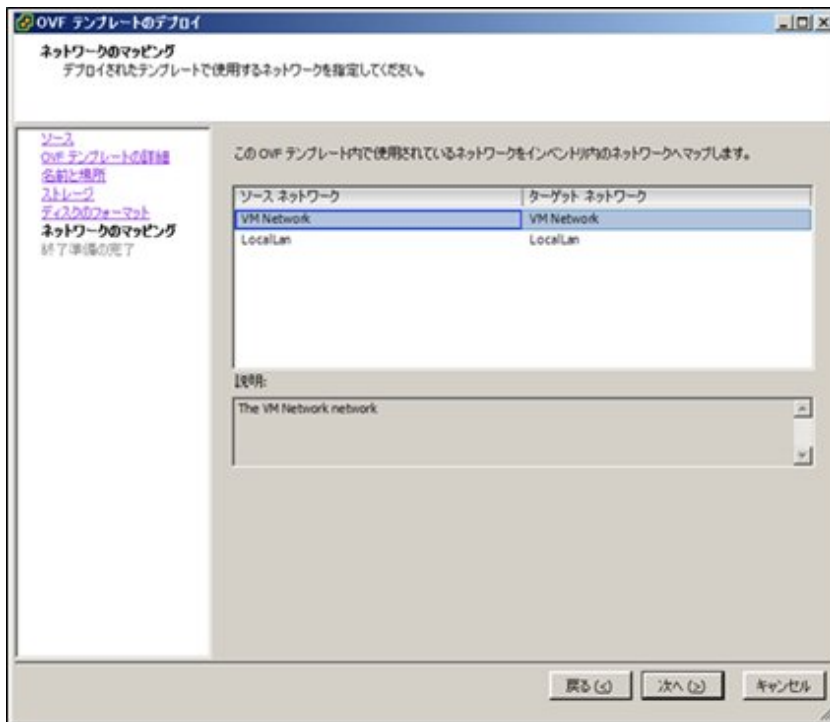
3. 「ストレージ」画面で、仮想マシンの保存場所を指定し、[次へ]を選択します。



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。



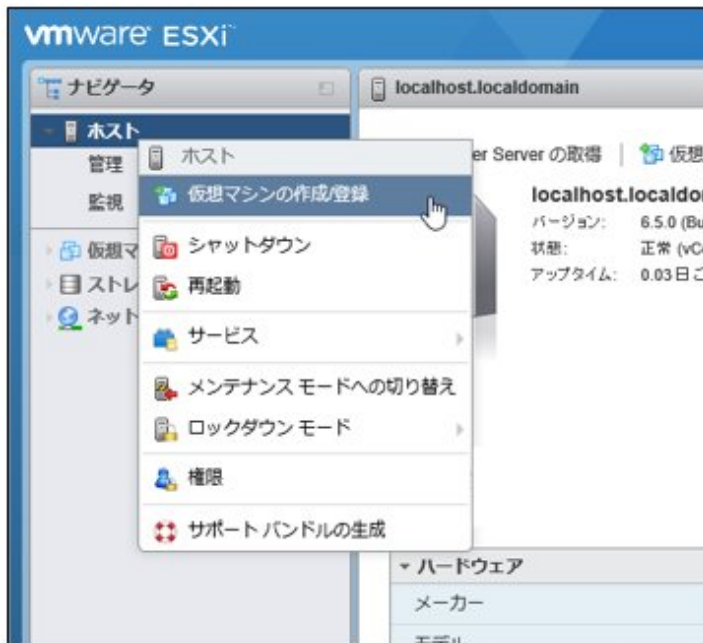
5. 「ネットワークのマッピング」画面で、ISMで使用するネットワークを選択し、[次へ]を選択します。



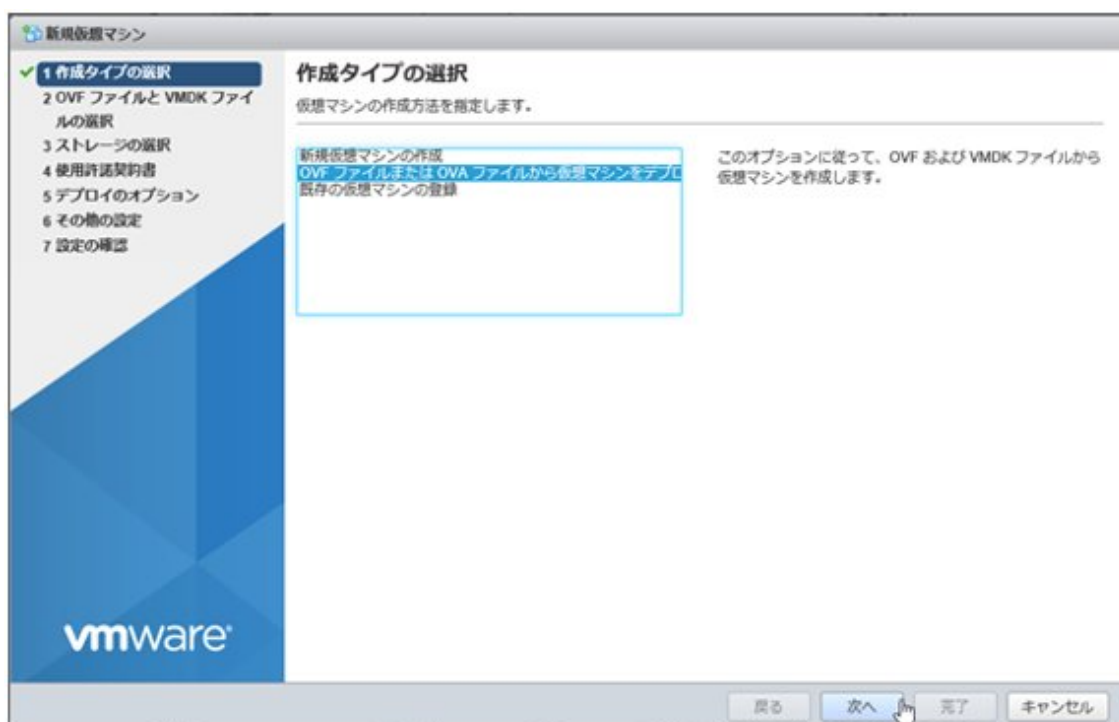
6. [完了]を選択し、OVFテンプレートのデプロイを完了させます。

VMware ESXi 6.5以降へインストールする

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。



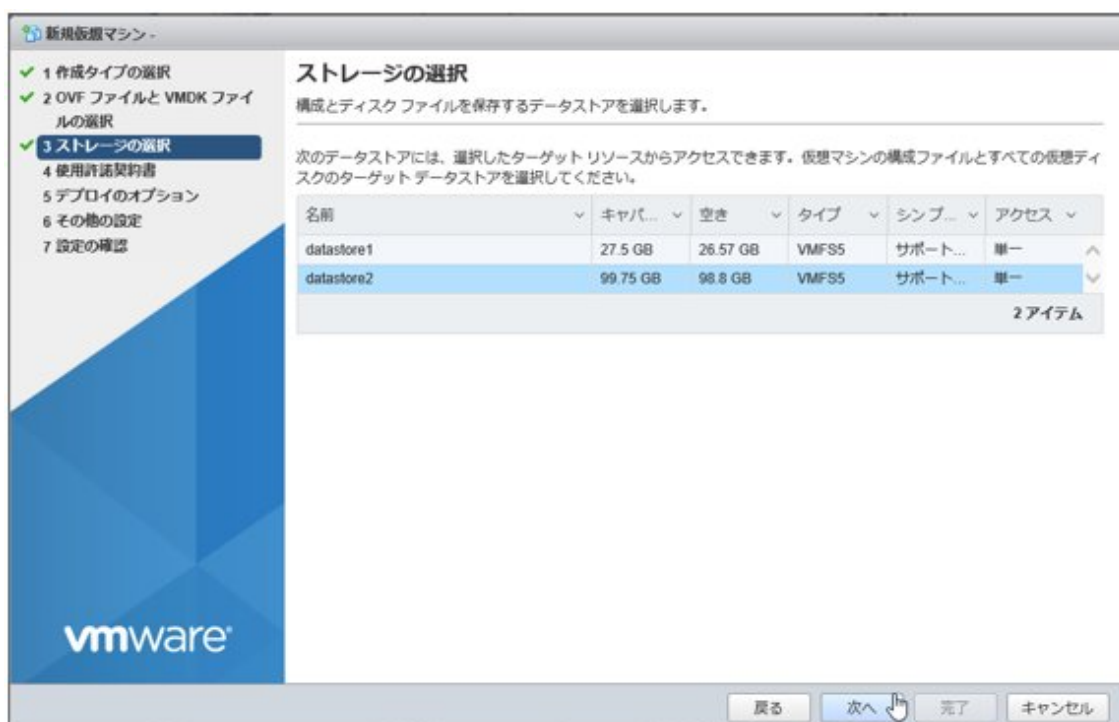
2. 「作成タイプの選択」画面で[OVFファイルまたはOVAファイルから仮想マシンをデプロイ]を選択し、[次へ]を選択します。



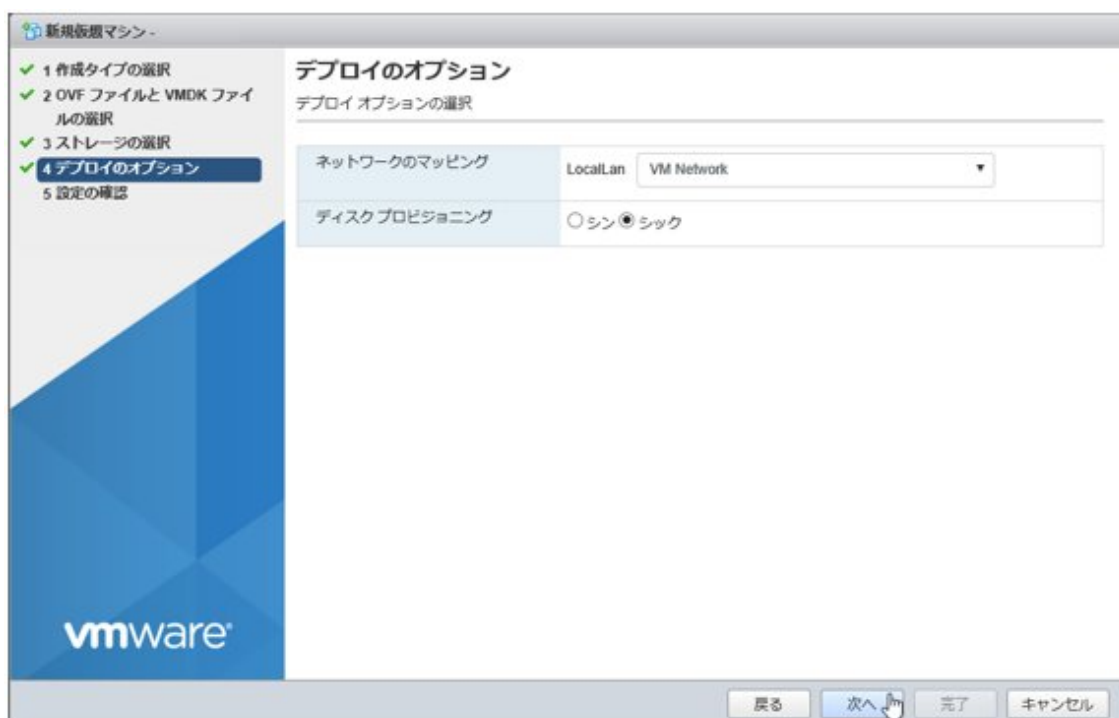
3. 「OVFファイルとVMDKファイルの選択」画面で仮想マシンに任意の名称を指定し、DVDメディアに含まれるovaファイルをデプロイ設定して、[次へ]を選択します。



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。



2.1.1.3 KVMへISM-VAをインストールする

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の版数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

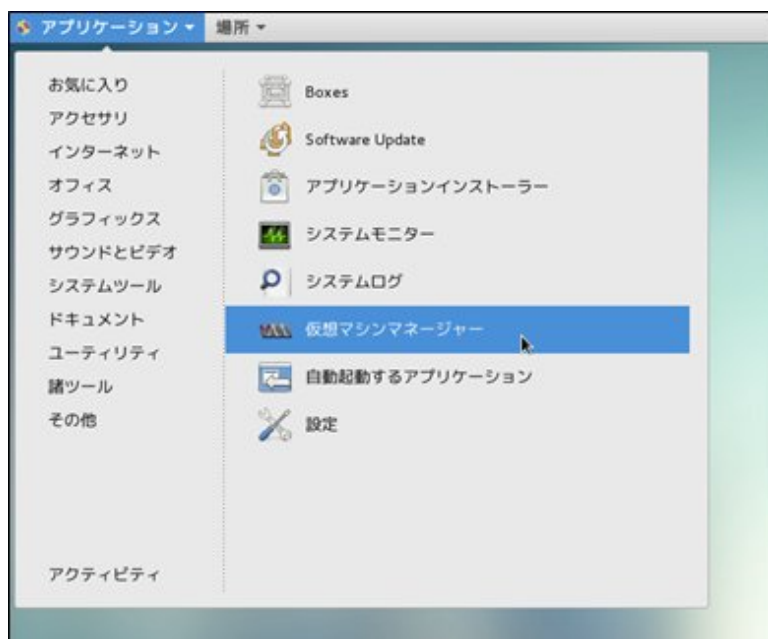
SUSE Linux Enterprise Serverにインストールする場合は、コピー前またはコピー後のxmlファイルをviなどで直接編集し、<emulator>部分を変更してください(ISM 2.3.0.b以降)。

- 変更前:<emulator>usr/libexec/qemu-kvm</emulator>
- 変更後:<emulator>usr/bin/qemu-system-x86_64</emulator>

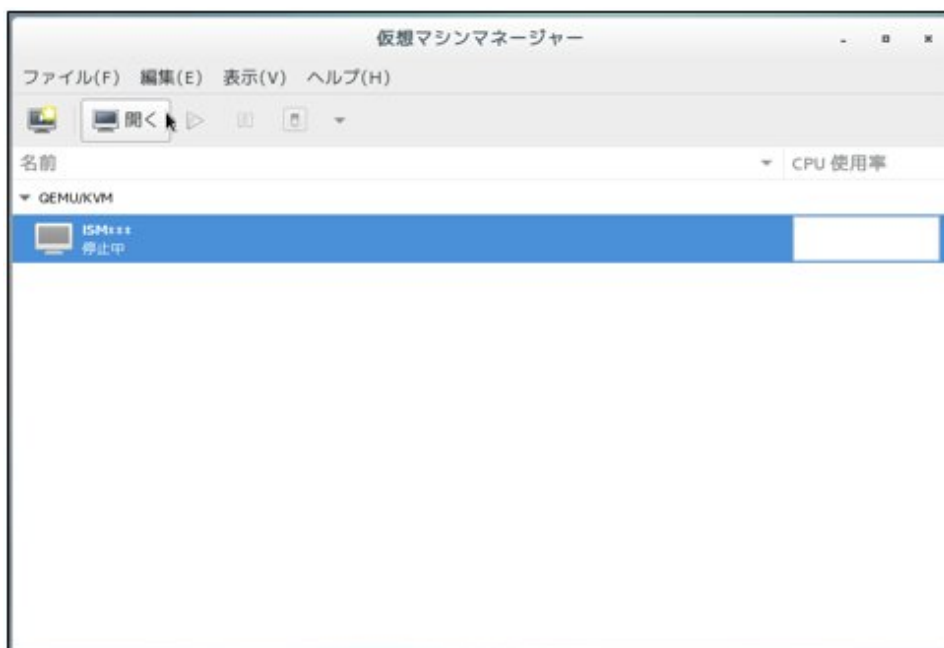
1. xmlファイルを指定してISM-VAを登録します。

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

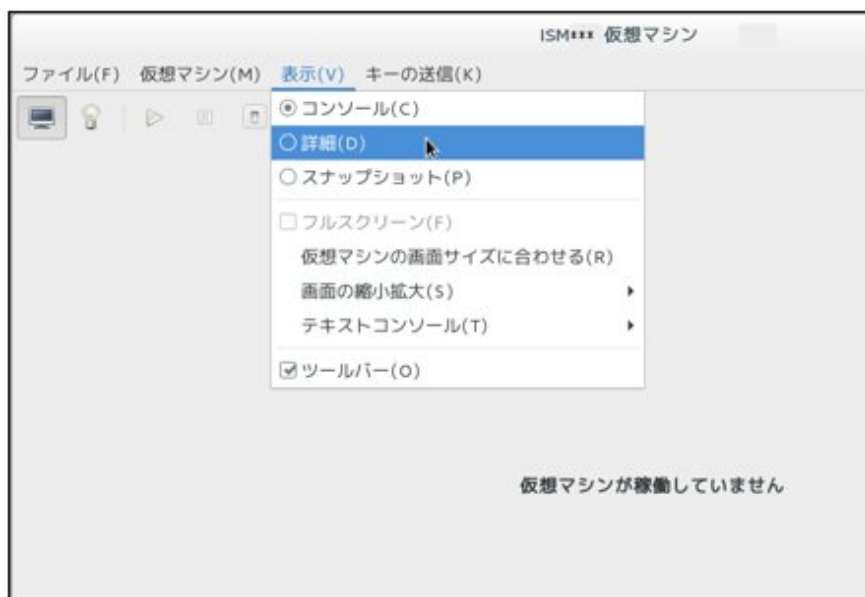
2. [仮想マシンマネージャー]を選択し、仮想マシンマネージャーを開きます。



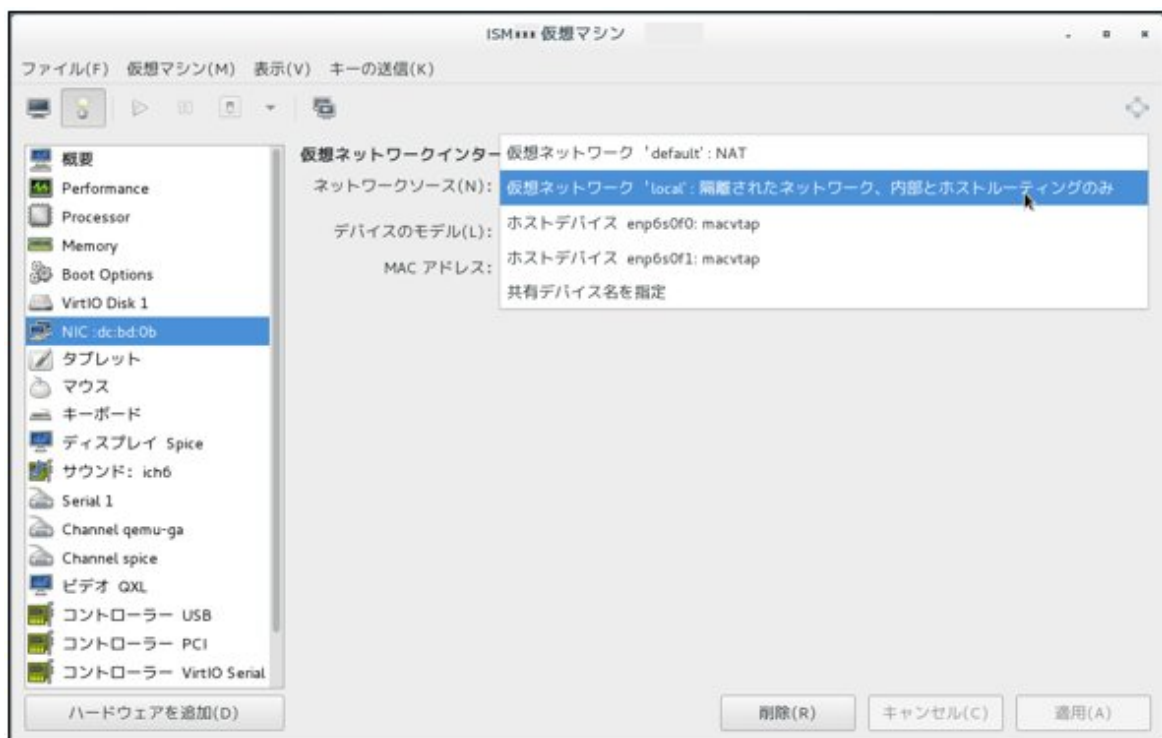
3. 仮想マシンマネージャー上でISM-VAを選択し、[開く]を選択します。



4. 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。



5. 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。



2.1.2 ISM-VAをエクスポートする

ISM-VAが動作しているハイパーバイザーに応じた手順で、ISM-VAをバックアップします。

ISM-VAのバックアップは、ハイパーバイザーのエクスポートの機能を利用して行います。

以下に、Microsoft Windows Server Hyper-V、VMware vSphere HypervisorおよびKVMでのISM-VAのバックアップ手順を説明します。

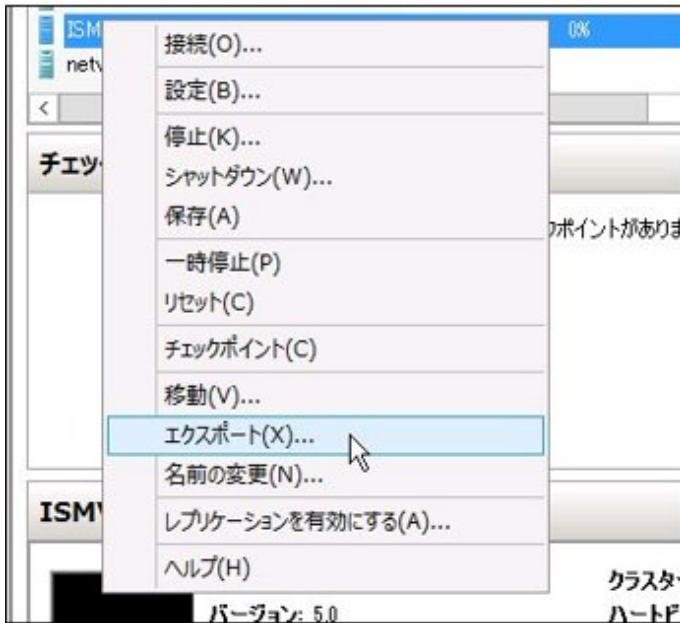


注意

ISM-VAをバックアップする前に、ISM-VAを終了してください。終了方法については、『ユーザーズマニュアル』の「4.1.2 ISM-VAの終了」を参照してください。

2.1.2.1 Microsoft Windows Server Hyper-Vで動作するISM-VAをバックアップする

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、[エクスポート]を選択します。



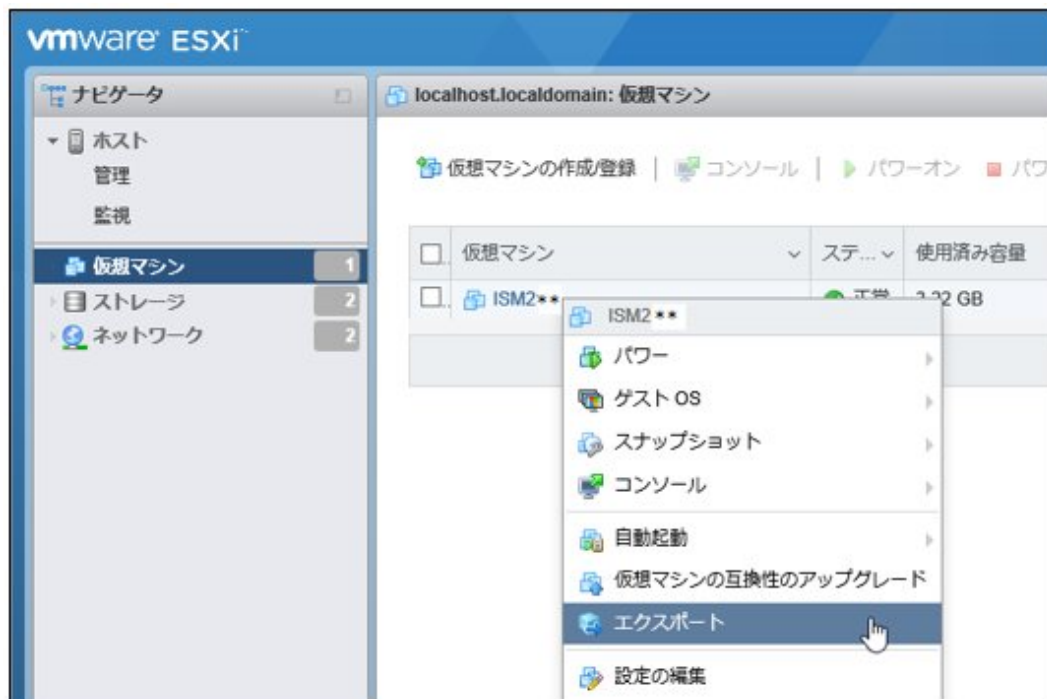
2.1.2.2 VMware vSphere Hypervisor 5.5またはVMware vSphere Hypervisor 6.0で動作するISM-VAをバックアップする

vSphere Clientで、インストールしたISM-VAを右クリックし、[ファイル]メニューから[エクスポート]-[OVFテンプレートのエクスポート]を選択します。



2.1.2.3 VMware vSphere Hypervisor 6.5で動作するISM-VAをバックアップする

vSphere Client (HTML5)でインストールしたISM-VAを右クリックし、[エクスポート]を選択します。



2.1.2.4 KVMで動作するISM-VAをバックアップする

以下の場所に格納されているKVMファイルを任意の場所にバックアップします。

- /etc/libvirt/qemu
- /var/lib/libvirt/images

2.1.3 仮想ディスクを接続する

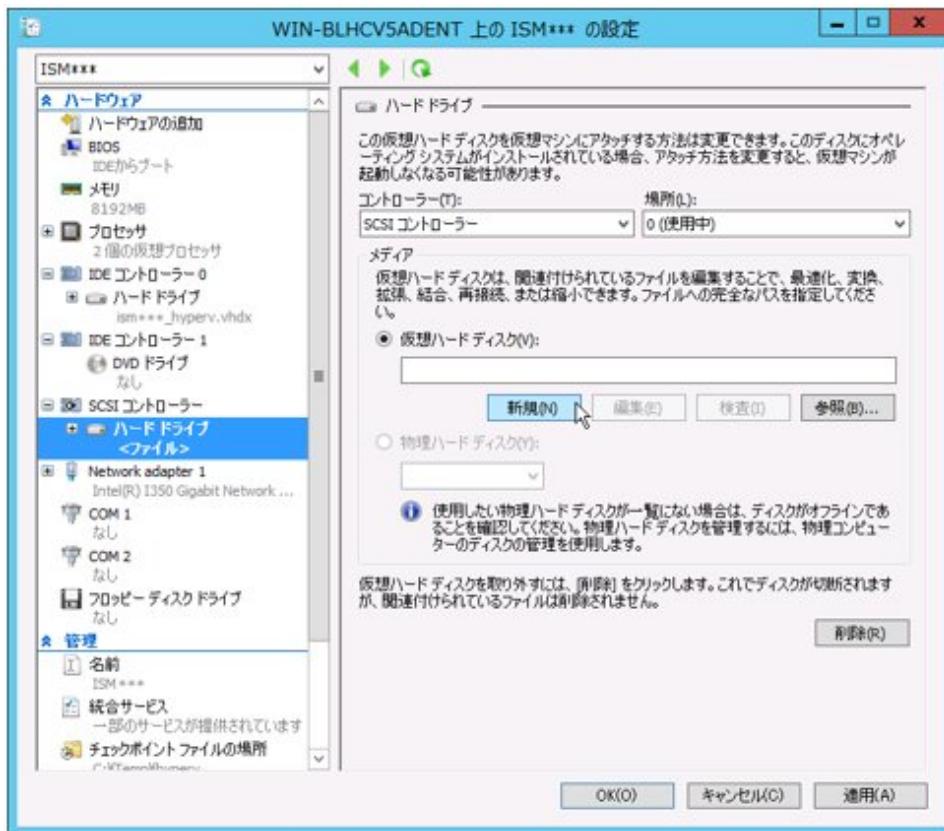
仮想ディスクは、ISM-VAのディスク容量を増設するための資源です。ログやリポジトリ、バックアップの格納には大容量のディスク資源が必要になります。また、それらの運用方法や管理対象ノードの規模などに応じて容量が異なります。大容量の資源を仮想ディスクに割り当てることにより、ISM-VAのディスク容量や負荷の影響を回避します。仮想ディスクには必要十分な容量を確保しておくことで、ログやリポジトリ、バックアップの運用を円滑に行えます。

仮想ディスクの割当ては、ISM-VA全体またはユーザーグループに対して行えます。

2.1.3.1 ISM-VA全体に対して仮想ディスクを割り当てる

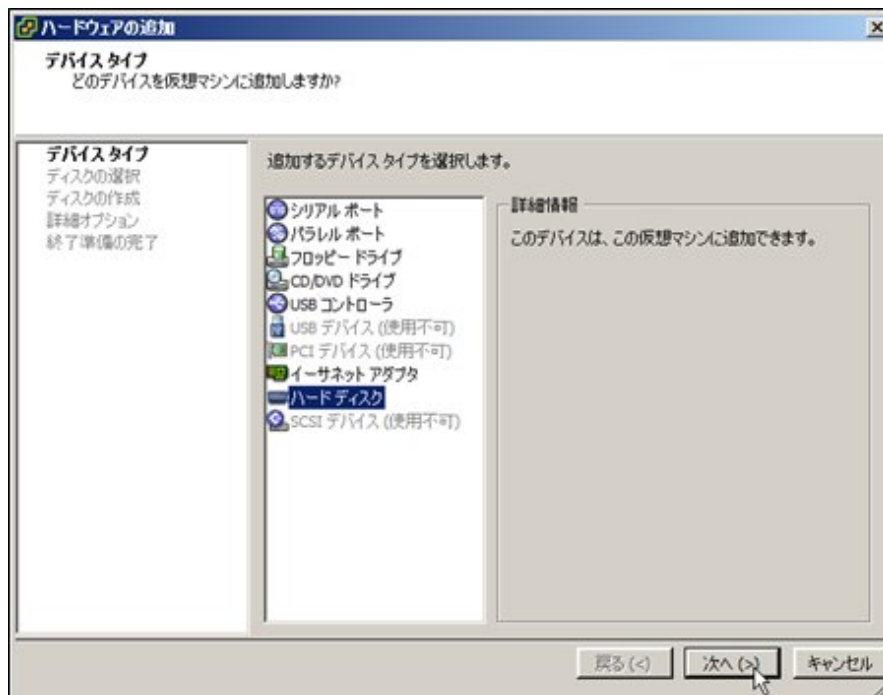
1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA(仮想マシン)に接続します。

Microsoft Windows Server Hyper-Vの場合



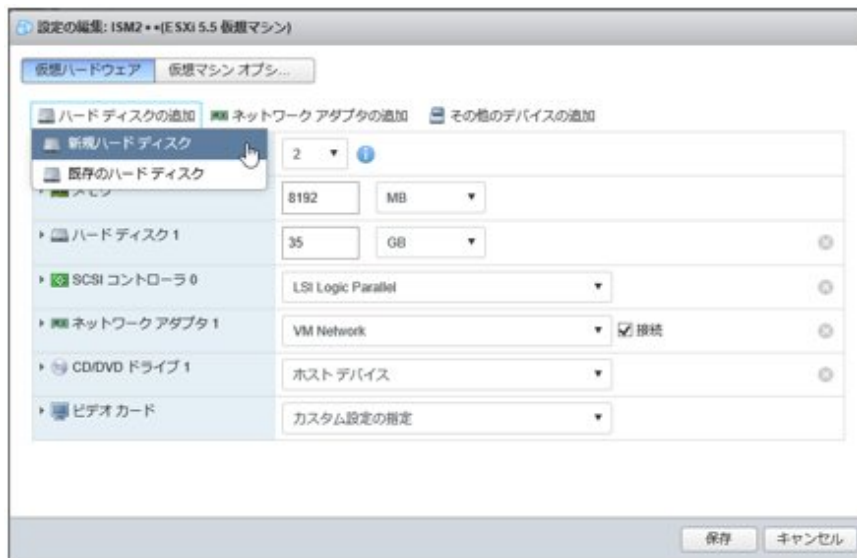
仮想ディスクは、SCSIコントローラーの配下に作成してください。

VMware vSphere Hypervisor 5.5またはVMware vSphere Hypervisor 6.0の場合



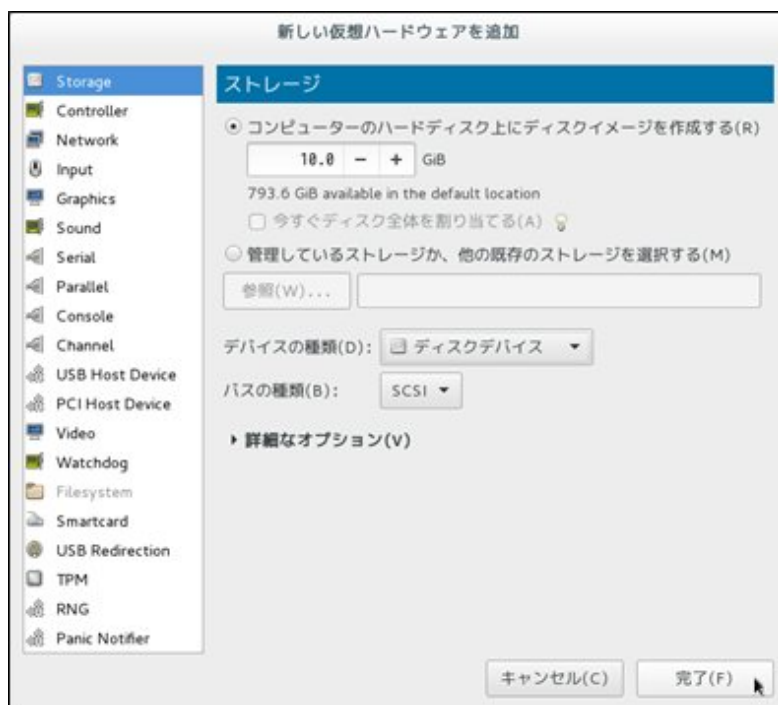
作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

VMware vSphere Hypervisor 6.5の場合



作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

KVMの場合



バスの種類は、SCSIを選択してください。

2. ISM-VA起動後、コンソールからadministratorでISM-VAにログインします。
3. 仮想ディスク割当てのため、一時的にISMサービスを停止させます。

```
# ismadm service stop ism
```

4. 手順1で追加した仮想ディスクが認識されているか確認します。

例：

```
# ismadm volume show -disk
```

ファイルシステム	サイズ	使用	残り	使用%	マウント位置
/dev/mapper/centos-root	16G	2.6G	13G	17%	/
devtmpfs	1.9G	0	1.9G	0%	/dev
tmpfs	1.9G	4.0K	1.9G	1%	/dev/shm
tmpfs	1.9G	8.5M	1.9G	1%	/run
tmpfs	1.9G	0	1.9G	0%	/sys/fs/cgroup
/dev/sda1	497M	170M	328M	35%	/boot
tmpfs	380M	0	380M	0%	/run/user/1001
/dev/sdb					(Free)

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。

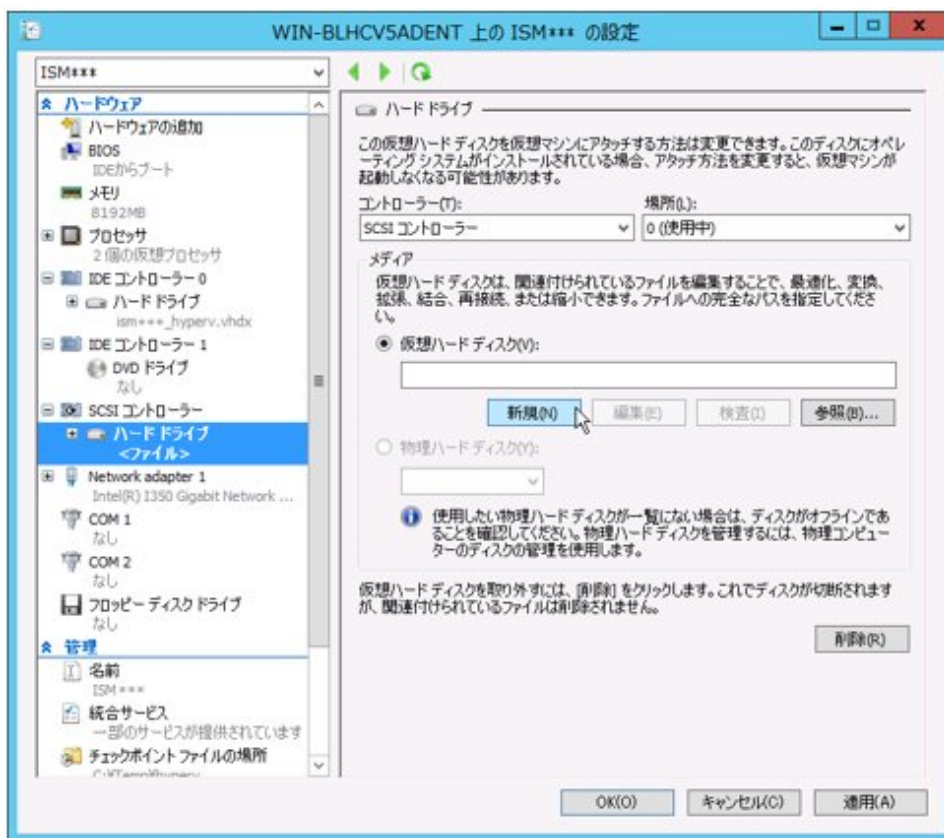
```
# ismadm power restart
```

2.1.3.2 ユーザーグループに対して仮想ディスクを割り当てる

Administratorユーザーグループを例として、仮想ディスク割当ての手順を示します。

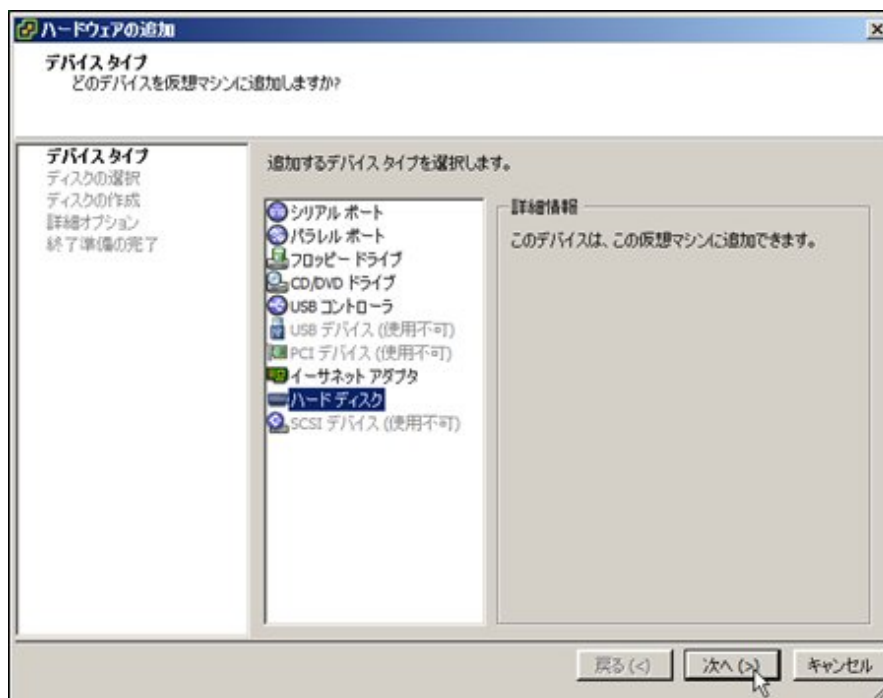
1. ISM-VA停止後、ハイパーバイザーの設定画面で仮想ディスクを作成し、ISM-VA (仮想マシン) に接続します。

Microsoft Windows Server Hyper-Vの場合



仮想ディスクは、SCSIコントローラーの配下に作成してください。

VMware vSphere Hypervisor 5.5またはVMware vSphere Hypervisor 6.0の場合



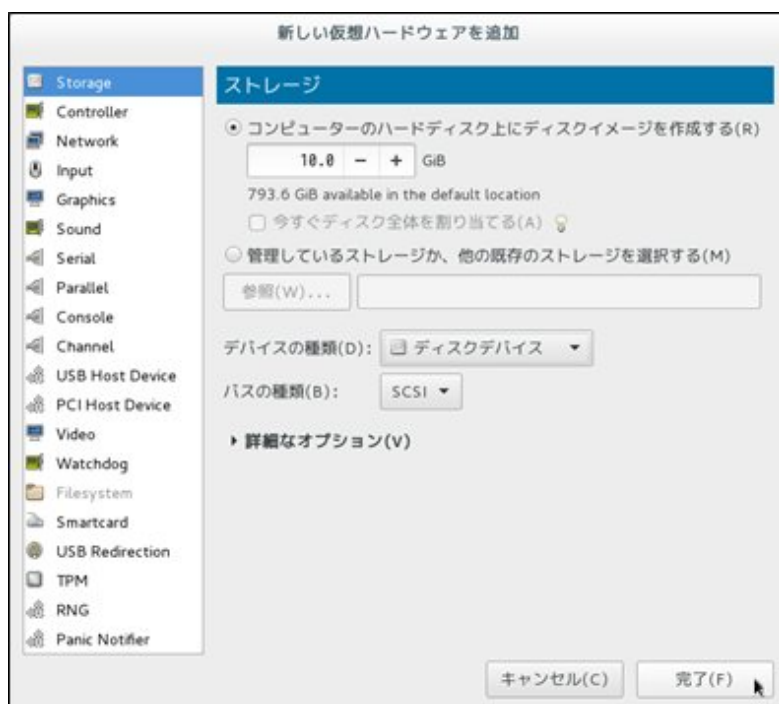
作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

VMware vSphere Hypervisor 6.5の場合



作成途中の「詳細オプション」画面にある仮想デバイスノード選択は、SCSIを選択してください。

KVMの場合



バスの種類は、SCSIを選択してください。

- 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。

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。

```

# ismadm 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。

```

# ismadm 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。

```

# ismadm volume show -disk
ファイルシステム      サイズ 使用 残り 使用% マウント位置
/dev/mapper/centos-root    16G  2.6G  13G  17% /
devtmpfs                  1.9G    0  1.9G    0% /dev
tmpfs                     1.9G  4.0K  1.9G    1% /dev/shm
tmpfs                     1.9G  8.6M  1.9G    1% /run
tmpfs                     1.9G    0  1.9G    0% /sys/fs/cgroup
/dev/sda1                 497M  170M  328M   35% /boot
tmpfs                     380M    0  380M    0% /run/user/1001
tmpfs                     380M    0  380M    0% /run/user/0
/dev/mapper/adminvol-lv    8.0G   39M  8.0G    1% 'RepositoryRoot' /Administrator

PV          VG      Fmt Attr PSize PFree
/dev/sda2  centos  lvm2 a-- 19.51g  0
/dev/sdb1  adminvol lvm2 a--  8.00g  0

```

- ISM-VAを再起動します。

```

# ismadm power restart

```

2.1.4 ライセンスを登録する

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、『ユーザーズマニュアル』の「1.1.2 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
# [Type] [Edition] [#Node] [Exp. Date] [Reg. Date] [Licensekey]
1 Server Adv. - - 2018-01-01 *****
2 Node Adv. 10 - 2018-01-01 *****
```

表2.1 コマンド出力結果の説明

項目	説明
[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。 <ul style="list-style-type: none">• 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. ISMの初期設定を実施します。

詳細は、『ユーザーズマニュアル』の「3.4.2 ISM-VAの初期設定」を参照してください。

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。

5. 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。

6. [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、『ユーザーズマニュアル』の「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。


2.2 データセンターを登録／削除する

データセンターは建屋に相当する階層です。その中に複数のフロアが存在するモデルをイメージしています。

データセンターを登録する

データセンター施設の建屋を表現する階層である「データセンター」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[管理]-[データセンター]を選択します。
「データセンターリスト」画面が表示されます。

2.  ボタンを選択します。

「データセンター / フロア / ラック登録」画面が表示されます。

3. [登録対象]で[データセンター]を選択します。

4. 設定項目を入力し、[登録]ボタンを選択します。

設定項目の説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面右上の[?]を選択

データセンターの登録を完了すると、当該のデータセンターが「データセンターリスト」画面に表示されます。

以上でデータセンター登録は完了です。

データセンターを削除する

登録されているデータセンターを削除します。

1. 「データセンターリスト」画面で、削除するデータセンターを選択します。

2. [アクション]ボタンから[データセンター削除]を選択します。
「データセンター削除」画面が表示されます。
データセンター削除時の留意事項はヘルプ画面を参照してください。
ヘルプ画面の表示方法:画面右上の[?]を選択
3. 削除するデータセンターが正しいことを確認し、[削除]ボタンを選択します。

2.3 フロアを登録／削除する


フロアは複数のラックが置かれているスペースをイメージした階層です。

ポイント

フロアビューはダッシュボードに表示させることができます。また、3Dビューではフロア単位で3Dグラフィック表示をします。

フロアを登録する

データセンター施設内のマシンルームを表現する階層である「フロア」を登録します。

1. 「データセンターリスト」画面で、 ボタンを選択します。
「データセンター/フロア/ラック登録」画面が表示されます。
2. [登録対象]で[フロア]を選択します。
3. 設定項目を入力し、[登録]ボタンを選択します。
設定項目[データセンター]には「[2.2 データセンターを登録／削除する](#)」で登録したデータセンターを指定します。
その他の設定項目の説明はヘルプ画面を参照してください。
ヘルプ画面の表示方法:画面右上の[?]を選択
フロアの登録が完了すると、当該のフロアが「データセンターリスト」画面に表示されます。
以上でフロア登録は完了です。

フロアを削除する

登録されているフロアを削除します。


1. 「データセンターリスト」画面で、削除するフロアを選択します。
2. [アクション]ボタンから[フロア削除]を選択します。
「フロア削除」画面が表示されます。
フロア削除時の留意事項はヘルプ画面を参照してください。
ヘルプ画面の表示方法:画面右上の[?]を選択
3. 削除するフロアが正しいことを確認し、[削除]ボタンを選択します。

2.4 ラックを登録／削除する

ラックは複数の管理対象機器(ノード)が搭載されているサーバラックをイメージした階層です。

ラックを登録する

フロア内のサーバラックを表現する階層である「ラック」を登録します。

1. 「データセンターリスト」画面で、 ボタンを選択します。
「データセンター/フロア/ラック登録」画面が表示されます。
2. [登録対象]で[ラック]を選択します。
3. 設定項目を入力し、[登録]ボタンを選択します。設定項目[データセンター]、[フロア]には、「[2.2 データセンターを登録／削除する](#)」、「[2.3 フロアを登録／削除する](#)」で登録したデータセンター、フロアを指定します。
その他の設定項目の説明はヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択
ラックの登録が完了すると、当該のラックが「データセンターリスト」画面に表示されます。
以上でラック登録は完了です。

ラックを削除する

登録されているラックを削除します。

1. ISMのGUIでグローバルナビゲーションメニューから[データセンター]を選択します。
「データセンターリスト」画面が表示されます。
2. 削除するラックを選択します。
3. [アクション]ボタンから[ラック削除]を選択します。
「ラック削除」画面が表示されます。
ラック削除時の留意事項はヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択
4. 削除するラックが正しいことを確認し、[削除]ボタンを選択します。

2.5 フロア内にラックを配置する

フロア内にラックを配置します。

1. 「データセンターリスト」画面で、ラックを配置するフロアを選択します。
フロアの詳細画面が表示されます。
2. [アクション]ボタンから[ラック位置設定]を選択します。
「ラック位置設定」画面が表示されます。
ラック位置の設定方法はヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択
3. [追加]ボタンを選択します。
「未配置ラック追加」画面が表示されます。
4. 追加するラックを選択し、[追加]ボタンを選択します。
5. ラックの位置を設定し、[適用]ボタンを選択します。
ラックの配置が完了すると、フロアの詳細画面にラックが表示されます。
以上でラックの配置は完了です。

2.6 アラーム設定をする(ISM内部のイベント)

アラームを設定することで、ISM内部の異常やイベントをISMが検知した際に、ISMの外部へ通知することができます。

アラーム設定を行う場合は、以下の順に行います。

1. アクション(通知方法)設定(「[2.6.1 アクション\(通知方法\)を設定する](#)」参照)

2. アクション(通知方法)のテスト(「[2.6.2 アクション\(通知方法\)をテストする](#)」参照)
3. アラーム設定(「[2.6.3 ISM内部のイベントを対象にアラームを設定する](#)」参照)

2.6.1 アクション(通知方法)を設定する

ISMの外部への通知方法を設定します。

通知の方法としては、以下の方法があります。

- ・ 外部ホスト上に配置した任意のスクリプトを実行する
- ・ メールを送信する
- ・ SNMPトラップとして、外部のSNMPマネージャーに送信／転送する
- ・ 外部Syslogサーバに、イベントのメッセージを転送／送信する

ポイント

- ・ 任意のスクリプトを実行する場合には、引数を指定できます。
- ・ メールを送信する場合には、S/MIMEによるメール本文の暗号化を選択できます。
- ・ 各画面での設定項目の入力については、ヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択

アクション(通知方法)を設定する前に事前準備が必要です。

使用するアクション(通知方法)タイプに応じて、それぞれ以下の設定を行います。

2.6.1.1 外部ホスト上に配置したスクリプトを実行する

事前設定

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	

1. 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。
2. 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して実行権限を設定してください。
3. 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、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/technical/>「補足資料」
『監視対象OS、仮想化管理ソフトウェアに対する設定』

アクション設定

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]ボタンから[追加]を選択します。
「アクション追加」画面が表示されます。
4. [アクションタイプ]に「リモートスクリプト実行」を選択します。
5. 設定項目を入力し、[適用]ボタンを選択します。
各設定項目の入力については、ヘルプ画面を参照してください。
アクションの追加が完了すると、設定したアクションが「アクションリスト」画面に表示されます。

2.6.1.2 メールを送信する

事前設定

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[SMTPサーバ]を選択します。
「SMTPサーバ設定」画面が表示されます。
3. [アクション]ボタンから[編集]を選択します。
「SMTPサーバ設定」画面が表示されます。
4. 設定項目を入力し、[適用]ボタンを選択します。
また、暗号化したメールを送信する場合は、以下の設定も行います。
5. 個人証明書を用意します。
このとき証明書がPEM形式であることと、証明書と宛先メールアドレスの対応がとれていることを確認してください。
6. FTPを使ってISM-VAへ転送します。FTPで以下にアクセスし、証明書を格納します。

`ftp://<ISM-VAのIPアドレス>/<ユーザーグループ名>/ftp/cert`
7. コンソールからadministratorでISM-VAにログインします。
8. コマンドを実行して、ISM-VAに証明書をインポートします。

```
# ismadm event import -type cert
```

コマンドを実行すると、各ユーザーがFTPに格納したすべての証明書が一括でインポートされます。

アクション設定

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]ボタンから[追加]を選択します。
「アクション追加」画面が表示されます。
4. [アクションタイプ]に「メール送信」を選択します。
5. 設定項目を入力し、[適用]ボタンを選択します。
各設定項目の入力については、ヘルプ画面を参照してください。
アクションの追加が完了すると、設定したアクションが「アクションリスト」画面に表示されます。

2.6.1.3 トラップ送信／転送を行う

事前設定

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[SNMPマネージャー]を選択します。
「SNMPマネージャーリスト」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。
「SNMPマネージャー追加」画面が表示されます。
4. 設定項目を入力し、[適用]ボタンを選択します。

アクション設定

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]ボタンから[追加]を選択します。
「アクション追加」画面が表示されます。
4. [アクションタイプ]に「トラップ送信/転送」を選択します。
5. 設定項目を入力し、[適用]ボタンを選択します。
各設定項目の入力については、ヘルプ画面を参照してください。
アクションの追加が完了すると、設定したアクションが「アクションリスト」画面に表示されます。

2.6.1.4 Syslog転送を行う

外部Syslogサーバに対して、ISMからのSyslog転送を受信できるように設定する必要があります。

外部Syslogサーバとして、以下のOSをサポートしています。

- RHEL 6、RHEL 7
- CentOS 6、CentOS 7
- SLES 11、SLES 12、SLES 15

Syslogを受信できるようにするため、外部Syslogサーバにroot権限でログインし、以下の手順で設定を変更します。ここでは、受信のために最低限必要な設定について説明します。

以下の例は、TCP 514ポートを使用してSyslog転送を実行する場合を記載しています。UDPや異なるポートを使用する場合は正しい値を設定してください。

RHEL 6、RHEL 7、CentOS 6、CentOS 7、SLES 12、SLES15の場合

1. 以下のコマンドを実行し、/etc/rsyslog.confの編集を開始します。

```
# vi /etc/rsyslog.conf
```

2. 下記内容を追記します。

```
$ModLoad imtcp
$InputTCPServerRun 514
$AllowedSender TCP, 192.168.10.10/24 ※ISMのIPアドレス
```

3. 変更完了後、以下のコマンドを実行し、rsyslogデーモンを再起動します。

ー RHEL 7、CentOS 7、SLES 12、SLES15の場合

```
# systemctl restart rsyslog
```

- ー RHEL 6、CentOS 6の場合

```
# service rsyslog restart
```

SLES 11の場合

1. 以下のコマンドを実行し、/etc/syslog-ng/syslog-ng.confの編集を開始します。

```
# vi /etc/syslog-ng/syslog-ng.conf
```

2. 下記内容を追記します。

```
source src {  
  
    (省略)  
  
    tcp(ip("0.0.0.0") port(514));    ※左行を追記、ISMのIPアドレスを使用  
}
```

3. 変更完了後、以下のコマンドを実行し、syslogデーモンを再起動します。

```
# service syslog restart
```

アクション設定

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]ボタンから[追加]を選択します。
「アクション追加」画面が表示されます。
4. [アクションタイプ]に「Syslog転送」を選択します。
5. 設定項目を入力し、[適用]ボタンを選択します。
各設定項目の入力については、ヘルプ画面を参照してください。
アクションの追加が完了すると、設定したアクションが「アクションリスト」画面に表示されます。

2.6.2 アクション(通知方法)をテストする

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. [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」画面が表示されます。
5. [テスト]ボタンを選択します。
アクションのテストが実行されます。
アクションが設定どおり動作したことを確認してください。

2.6.3 ISM内部のイベントを対象にアラームを設定する

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]を選択します。

3. [アクション]ボタンから[追加]を選択します。

[アラーム追加]ウィザードが表示されます。

ISM内部の異常やイベントを対象としてアラーム設定を行う場合、[アラーム追加]ウィザードの「対象」画面で、[対象種別]に「システム」を選択します。

その他の設定項目の入力については、ヘルプ画面を参照してください。

4. 「確認」画面で設定内容を確認し、[適用]ボタンを選択します。

アラームの追加が完了すると、設定したアラームが「アラームリスト」画面に表示されます。

以上でISM内部のイベントを対象にしたアラーム設定は完了です。

2.7 管理者ユーザーを登録する

ユーザーグループの種別やユーザー登録時のユーザーロールを指定することで管理者ユーザーを設定できます。

ポイント

- ユーザーグループの種別やユーザーロールの種別と各種別でのアクセス範囲や操作権限については、『ユーザーズマニュアル』の「2.13.1 ユーザー管理機能」を参照してください。
- 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。

2.7.1 ISMのユーザーを管理する

ユーザーの管理には、以下の3種類あります。

- [2.7.1.1 ユーザーを追加する](#)
- [2.7.1.2 ユーザーを編集する](#)
- [2.7.1.3 ユーザーを削除する](#)

2.7.1.1 ユーザーを追加する

ポイント

本操作は、Administratorロールを持つユーザーのみ実行できます。

以下の方法で新しくユーザーを追加します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザー]を選択します。
3. [アクション]ボタンから[追加]を選択します。

ユーザーを登録する場合に設定する情報は、以下のとおりです。

- ユーザー名
ISM全体で、ユニークな名称を指定してください。
- パスワード
- ユーザーロール
ユーザーロールについては、『ユーザーズマニュアル』の「2.13.1 ユーザー管理機能」を参照してください。
- ISM連携
以下のどちらかを選択できます。

- ー 連携用のユーザーとして設定しない
- ー 連携用のユーザーとして設定する
- ・ 認証方式

以下のどちらかを選択できます。

 - ー ユーザーグループの設定に従う
 - ー Infrastructure Manager(ISM)
- ・ 説明

ユーザーの説明(コメント)を自由に指定してください。
- ・ 言語

日本語または英語を指定してください。指定しない場合は、英語となります。
- ・ 日付フォーマット
- ・ タイムゾーン
- ・ ユーザーグループを選択してください

2.7.1.2 ユーザーを編集する

ポイント

本操作は、ユーザーグループの種別やユーザーロールの種別に応じて変更できる情報が異なります。

以下の方法でユーザーの情報を変更します。

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]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザー]を選択します。
3. 以下のどちらかを行います。
 - ー 編集したいユーザーにチェックを付け、[アクション]ボタンから[編集]を選択します。
 - ー 編集したいユーザー名を選択し、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。

変更できる情報は、以下のとおりです。

ユーザー情報	Administratorグループ		Administratorグループ以外のグループ	
	Administratorロール	Operatorロール Monitorロール	Administratorロール	Operatorロール Monitorロール
ユーザー名	○	○	○	○
パスワード	○	○	○	○
ユーザーロール	○	×	○	×
ISM連携	○	×	×	×
認証方式	○	×	○	×
説明	○	×	○	×
言語	○	○	○	○
日付フォーマット	○	○	○	○
タイムゾーン	○	○	○	○
ユーザーグループ	○	×	×	×

○:変更可能、×:変更不可能



注意

- LDAPなどと連携している場合、パスワードを変更しても、LDAPサーバのパスワードは変更されません。
- ISM連携で[連携用のユーザーとして設定する]を選択した場合、パスワードも同時に編集してください。

2.7.1.3 ユーザーを削除する



ポイント

本操作は、Administratorロールを持つユーザーのみ実行できます。

以下の方法でユーザーを削除できます。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザー]を選択します。
3. 以下のどちらかを行います。
 - 削除したいユーザーにチェックを付け、[アクション]ボタンから[削除]を選択します。
 - 削除したいユーザー名を選択し、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。

2.7.2 ユーザーグループを管理する

ユーザーグループの管理には、以下の種類があります。

- [2.7.2.1 ユーザーグループを追加する](#)
- [2.7.2.2 ユーザーグループを編集する](#)
- [2.7.2.3 ユーザーグループを削除する](#)



ポイント

本操作は、ISM管理者 (Administratorグループに属し、Administratorロールを持つユーザー) のみ実行できます。

2.7.2.1 ユーザーグループを追加する

ISM管理者が、以下の方法で新しくユーザーグループを追加します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザーグループ]を選択します。
3. [アクション]ボタンから[追加]を選択します。

ユーザーグループを追加する場合に設定する情報は、以下のとおりです。

- ユーザーグループ名
ISM全体で、ユニークな名称を指定してください。
- 認証方法
ユーザーグループに属するユーザーの認証方法は、以下のどちらかを指定します。
 - Infrastructure Manager(ISM)
 - Open LDAP / Microsoft Active Directory(LDAP)

- 説明

ユーザーグループの説明(コメント)を入力してください。入力内容は任意です。

- ディレクトリサイズ

ユーザーグループで使用するファイルの総容量の上限と警告の通知しきい値を指定できます。

用途	サイズ制限	しきい値監視
ユーザーグループ全体	<p>ユーザーグループで使用するファイルの総容量を[最大サイズ]にMB単位で指定します。</p> <p>ファイルの総容量とは、以下のデータの合計を意味します。</p> <ul style="list-style-type: none"> リポジトリ 保管ログ ノードログ FTPでISM-VAに取り込むファイル <p>実際の使用量が[最大サイズ]で指定した値を超えた場合、運用ログにエラーメッセージが出力されます。ただし、[最大サイズ]の値を超えても、リポジトリ、保管ログ、ノードログの動作には影響しません。</p>	<p>警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。</p> <p>警告メッセージは運用ログに出力されます。</p>
リポジトリ	<p>リポジトリにインポートするファイルの総容量を[最大サイズ]にMB単位で指定します。</p> <p>インポートしたファイルの総使用量が[最大サイズ]で指定した値を超えた場合、実行中のリポジトリへのインポートはエラーになり、運用ログにエラーメッセージが出力されます。</p>	指定できません。
保管ログ	<p>保管ログの総容量を[最大サイズ]にMB単位で指定します。</p> <p>保管ログの総容量が[最大サイズ]で指定した値を超えた場合、新たに発生したログは保管されなくなり、運用ログにエラーメッセージが出力されます。</p> <p>なお、[最大サイズ]を初期値の「0」のままにしておくと、発生したログは保管されず、そのたびに運用ログにエラーメッセージが出力されます。</p> <p>[最大サイズ]の値を超える前に保管されたログは、そのまま保管されます。</p>	<p>警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。</p> <p>警告メッセージは運用ログに出力されます。</p>
ノードログ	<p>ダウンロード用データとログ検索用データの総データ容量を[最大サイズ]にMB単位で指定します。</p> <p>ログ検索用データは、Administratorユーザーグループにのみ指定できます。</p> <p>ダウンロード用データ、またはログ検索用データの総データ容量のどちらかが[最大サイズ]で指定した値を超えた場合、ダウンロード用データとログ検索用データの両方が出力されなくなり、運用ログにエラーメッセージが出力されます。</p> <p>なお、ダウンロード用データ、ログ検索用データのどちらか、または両方の[最大サイズ]を初期値の「0」のままにしておくと、どちらのデータも出力されず、運用ログにエラーメッセージが出力されます。</p>	<p>ダウンロード用データの容量とログ検索用データの容量に対して、警告メッセージを出力するしきい値を[警告しきい値]に%単位で指定します。</p> <p>警告メッセージは運用ログに出力されます。</p>

リポジトリにインポートするファイルの総容量、保管ログの容量、ノードログ(ダウンロード用データ、ログ検索用データ)の容量の見積り方法については、『ユーザーズマニュアル』の「3.2.1 ディスク資源の見積り」を参照してください。

- 管理対象ノード

ノードグループを選択することで、ユーザーグループとノードグループの関連付けを行います。



- ユーザーグループに関連付けられるノードグループは1つだけです。
- ユーザーグループに所属する各ユーザーは、そのユーザーグループに関連付けられたノードグループに所属するノードだけを操作対象にできます。ユーザーグループに関連付けられていないノードグループのノードにはアクセスできません。
- ユーザーグループ作成後は、すぐに『ユーザーズマニュアル』の「3.7.2 ユーザーグループに対する仮想ディスク割当て」の手順を行ってください。
- 「全てのノードを管理」を選択した場合、Administratorグループと同様に、すべてのノードグループおよびユーザーグループにアクセスできます。ただし、リポジトリがAdministratorグループと共有されます。

2.7.2.2 ユーザーグループを編集する

ISM管理者が、以下の方法でユーザーグループの情報を編集します。

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]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザーグループ]を選択します。
3. 以下のどちらかを行います。
 - 編集したいユーザーグループにチェックを付け、[アクション]ボタンから[編集]を選択します。
 - 編集したいユーザーグループ名を選択し、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。

編集できる情報は、以下のとおりです。

- ユーザーグループ名
- 認証方法
- 説明
- システムボリューム (Administratorグループのみ)

システムボリュームの警告メッセージを出力するしきい値を[しきい値監視]に小数点2桁の%単位で指定します。警告メッセージは、運用ログとGUI画面に出力されます。

- ディレクトリサイズ

編集内容は、「2.7.2.1 ユーザーグループを追加する」の「ディレクトリサイズ」を参照してください。

- 管理対象ノード

ノードグループを選択することで、ユーザーグループとノードグループの関連付けを行います。



- Administratorグループのグループ名は、変更できません。
- ユーザーグループに関連付けられるノードグループは1つだけです。
ノードグループに関連付けられた状態のユーザーグループに、新たに別のノードグループとの関連付けを行った場合、既存のノードグループとの関連付けは解除されます。
- システムボリュームの警告メッセージについて
 - システムボリュームの使用サイズは、10分ごとにチェックされます。
 - システムボリュームの使用サイズがしきい値監視の値より大きくなった場合、警告メッセージが出力されます。
 - 一度出力された警告メッセージが解消されなかった場合、24時間ごとに同じメッセージが出力されます。

- ー 一度出力された警告メッセージが解消され、再度しきい値監視の値より大きくなった場合、同じメッセージが出力されます。
- ー 警告メッセージが出力された場合、以下の対処を行ってください。
 - リポジトリ内の不要なファイルを削除する。
 - ismadmコマンドで、システムのLVMボリュームサイズを拡張する。

2.7.2.3 ユーザーグループを削除する

ISM管理者が、以下の方法でユーザーグループを削除できます。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[ユーザーグループ]を選択します。
3. 以下のどちらかを行います。
 - ー 削除したいユーザーグループにチェックを付け、[アクション]ボタンから[削除]を選択します。
 - ー 削除したいユーザーグループ名を選択し、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。



- ・ Administratorグループは削除できません。
- ・ ユーザーが存在するユーザーグループは、削除できません。
ユーザーグループを削除する場合は、事前にユーザーを削除するか、ユーザーの所属をほかのユーザーグループへ変更してください。
- ・ ノードグループに関連付けられた状態のままユーザーグループを削除しても、ノードグループは削除されません。
- ・ ユーザーグループを削除すると、元には戻せません。
- ・ ユーザーグループに関連したデータ(リポジトリ)はすべて削除されます。

2.7.3 Microsoft Active DirectoryまたはLDAPと連携する

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。Microsoft Active DirectoryまたはLDAPと連携するには、以下の手順で設定を行います。

1. Microsoft Active DirectoryまたはLDAP (以降、「ディレクトリサーバ」と表記)と連携するユーザーを、ディレクトリサーバに登録します。
2. 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。
3. ディレクトリサーバ情報が設定されていない場合、ISMのLDAPサーバの設定で、以下の情報を設定します。
設定内容については、ディレクトリサーバの管理者に、手順1で登録した設定内容を問い合わせてください。

項目	設定内容
LDAPサーバ名	ディレクトリサーバ名を指定します。以下のどれかを指定します。 <ul style="list-style-type: none"> ・ URLまたはIPアドレス ・ ldap://<url> または ldap://<IPアドレス> ・ ldaps://<url> または ldaps://<IPアドレス>
ポート番号	ディレクトリサーバのポート番号を指定します。
ベースDN	アカウント検索用のベースDNを指定します。ディレクトリサーバの登録内容に依存します。 (例) <ul style="list-style-type: none"> ・ LDAPの場合 : ou=Users,ou=system ・ Microsoft Active Directoryの場合 : DC=company,DC=com

項目	設定内容
検索属性	アカウント検索用のアカウント属性を指定します。以下のどちらかの固定文字列を指定します。 <ul style="list-style-type: none"> LDAPの場合: uid Microsoft Active Directoryの場合: sAMAccountName
バインドDN	ディレクトリサーバ上で、検索できるアカウントを指定します。ディレクトリサーバの登録内容に依存します。 (例) <ul style="list-style-type: none"> LDAPの場合: uid=ldap_search,ou=system Microsoft Active Directoryの場合: CN=ldap_search,OU=user_group,DC=company,DC=com anonymousはサポートしていません。
パスワード	バインドDNで指定したアカウントのパスワードを指定します。
SSL証明書	ディレクトリサーバとの接続にSSLを使用したい場合、SSL証明書を設定します。

4. 認証方法にMicrosoft Active DirectoryまたはLDAPを設定したユーザーグループを用意します。

5. 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。

6. 画面左側のメニューから[ユーザー]を選択し、手順1で登録したユーザーを追加します。

登録する情報は以下のとおりです。

項目	設定内容
ユーザー名	手順1で登録したユーザー名を指定します。
パスワード	手順1のパスワードとは異なり、連携を解除した場合のパスワードを指定します。 なお、ここで指定したパスワードが、FTPでログイン時に使用するパスワードとなります。
認証方法	「ユーザーグループの設定に従う」を指定します。
ユーザーロール	ISMでのユーザーロールを指定します。
説明	自由な値を指定します。
言語	追加するユーザーで使用する言語を指定します。
日付フォーマット	追加するユーザーで使用する日付フォーマットを指定します。
タイムゾーン	追加するユーザーで使用するタイムゾーンを指定します。
ユーザーグループ名	手順4で用意したユーザーグループを指定します。

7. 手順6で登録したユーザーがログインできることを確認します。

ログインできない場合、手順3に戻ってください。

設定解除手順

連携対象のユーザーグループやユーザーの連携を解除する方法は、以下のとおりです。

・ユーザーの変更

以下のどちらかを行ってください。

- ユーザーが属するユーザーグループを、連携していないユーザーグループに変更します。ユーザーの編集で変更してください。
- ユーザーの認証方法を「Infrastructure Manager(ISM)」に変更します。

・ユーザーグループの変更

ユーザーグループの編集で、認証方法を「Infrastructure Manager(ISM)」に変更します。

上記のどちらの場合も、パスワードはユーザーの登録、変更操作で設定したパスワードが有効となります。

2.7.4 ノードグループを管理する

ノードグループの管理には、以下の種類があります。

- ・ [2.7.4.1 ノードグループを追加する](#)
- ・ [2.7.4.2 ノードグループを編集する](#)
- ・ [2.7.4.3 ノードグループを削除する](#)



ポイント


本操作は、ISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）のみ実行できます。

2.7.4.1 ノードグループを追加する

ISM管理者が、以下の方法で新しくノードグループを追加します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[ノードグループ]を選択します。
3. [アクション]ボタンから[ノードグループ追加]を選択します。

または

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]-[ノードグループ]を選択します。
2. 「ノードグループリスト」画面の  ボタンを選択します。

ノードグループを追加する場合に設定する情報は、以下のとおりです。

- ・ ノードグループ名
ISM全体で、ユニークな名称を指定してください。
- ・ 割り当てるノードを選択
所属ノードグループが[未割り当て]のノードを複数選択します。
なお、ここで割り当てなくても、あとでノードグループの編集により割り当てることができます。



注意

ノードが所属できるノードグループは1つだけです。

2.7.4.2 ノードグループを編集する

ISM管理者が、以下の方法で、ノードグループを編集します。

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]-[ユーザー]を選択します。
2. 画面左側のメニューから[ノードグループ]を選択します。
3. 以下のどちらかを行います。
 - － 編集したいノードグループにチェックを付け、[アクション]ボタンから[ノードグループ編集]を選択します。
 - － 編集したいノードグループ名を選択し、表示された情報画面で[アクション]ボタンから[ノードグループ編集]を選択します。

または

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]-[ノードグループ]を選択します。
2. 画面左側のノードグループリストからノードグループを選択し、[アクション]ボタンから[ノードグループ編集]を選択します。

ノードグループを編集する場合に設定する情報は、以下のとおりです。

- ・ ノードグループ名
ISM全体で、ユニークな名称を指定してください。
- ・ 新たに割り当てるノードを選択
所属ノードグループが[未割り当て]のノードを複数選択します。

ノードの割当てを解除または変更するには、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[管理]-[ノードグループ]を選択します。
2. 画面左側のノードグループリストからノードグループを選択します。
3. 画面右側でノードを選択し、[ノードアクション]ボタンから[ノードグループへ割り当て]を選択します。
4. 「ノードグループへの割り当て」画面で、[選択]ボタンを選択します。
5. 「ノードグループ選択」画面で以下のどちらかを選択し、[選択]ボタンを選択します。
 - ー ノード割当てを解除する場合:[未割り当て]
 - ー ノード割当てを変更する場合:[<新たに割り当てるノードグループ>]
6. 「ノードグループへの割り当て」画面で[適用]ボタンを選択します。




注意

ノード間で親子の繋がりがあるノードの場合、親ノードのみ[ノードグループへ割り当て]を実行できます。
子ノードは自動的に親ノードと同じノードグループに設定されます。

繋がりがあるノードは、ノードリスト画面でノード名の横にアイコンが表示されます。親子の繋がりが設定されるモデルについては、「[表2.2 ノード間で親子の繋がりが設定されるモデル](#)」のとおりです。

表2.2 ノード間で親子の繋がりが設定されるモデル

モデル	親ノード	子ノード	アイコン
PRIMERGY BXシャーシ	-	PRIMERGY BX サーバ BXコネクションブレード	
PRIMERGY BXサーバ	PRIMERGY BXシャーシ	-	
BXコネクションブレード	PRIMERGY BXシャーシ	-	
PRIMERGY CXシャーシ	-	PRIMERGY CXサーバ	
PRIMERGY CXサーバ	PRIMERGY CXシャーシ		
PRIMEQUEST 2000シリーズ／3000Eシリーズ	-	PRIMEQUESTパーティション	
PRIMEQUESTパーティション	PRIMEQUEST 2000シリーズ ／3000Eシリーズ	PRIMEQUEST拡張パーティ ション	
PRIMEQUEST拡張パーティション	PRIMEQUESTパーティション	-	
ETERNUS DX	-	ドライブエンクロージャ	

モデル	親ノード	子ノード	アイコン
ドライブエンクロージャ	ETERNUS DX	-	
ETERNUS NR (NetApp) クラスタ	-	ETERNUS NR (NetApp) シャーシ	
ETERNUS NR (NetApp) シャーシ	ETERNUS NR (NetApp) クラスタ	外付けディスクシェルフ	
外付けディスクシェルフ	ETERNUS NR (NetApp) シャーシ	-	
VCSファブリック	-	VDXスイッチ	
VDXスイッチ	VCSファブリック	-	
C-Fabric	-	CFX2000シリーズ/PY CB Eth Switch 10/40Gb 18/8+2 (ファブリックモード)	
CFX2000シリーズ	C-Fabric	-	
PY CB Eth Switch 10/40Gb 18/8+2 (ファブリックモード)	C-Fabric	-	

2.7.4.3 ノードグループを削除する

ISM管理者が、以下の方法で、ノードグループを削除します。

- ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
- 画面左側のメニューから[ノードグループ]を選択します。
- 以下のどちらかを行います。
 - 削除したいノードグループにチェックを付け、[アクション]ボタンから[ノードグループ削除]を選択します。
 - 削除したいノードグループ名を選択し、表示された情報画面で[アクション]ボタンから[ノードグループ削除]を選択します。

または

- ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノードグループ]を選択します。
- 画面左側のノードグループリストからノードグループを選択し、[アクション]ボタンから[ノードグループ削除]を選択します。



注意

ノードが存在するノードグループは、削除できません。ノードグループを削除する場合は、以下のどれかを行ってください。

- 事前にノードを削除する
- ノードの割当てを解除する
- ほかのノードグループに割り当てる

第3章 管理対象ノードを登録／設定／削除する

この章では、管理対象ノードの登録／削除、ノードを管理するためのアラーム設定などの各設定について説明します。

3.1 管理対象ノードを登録／削除する

ノード登録はネットワーク内に存在するノードを検出して登録する方法と、ノードの情報を直接入力して登録する方法があります。

ISMへの登録情報とノード内の登録情報が一致しない場合、ISMの機能が制限される場合があります。

3.1.1 ネットワーク内ノードを検出してノード登録する

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。

「ノード登録」画面が表示されます。

自動検出によって検出された機器は、[検出ノードリスト]に表示されます。以降の手順をスキップして手順8に進むことができます。

ポイント

自動検出の対象ノードについては、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/>

2. [アクション]ボタンから[検出]を選択します。

「検出」画面が表示されます。

3. [検出方式]を選択します。

以下のどちらかを選択します。[検出方式]での選択に応じて画面の表示内容が異なります。

ー 通常

検索対象とするIPアドレス範囲を指定して検出を実行します。手順4へ進みます。

ー CSVアップロード

検出対象を記載したCSVファイルを指定して検出を実行します。手順5へ進みます。

4. [検出方式]で「通常」を選択した場合、[IPアドレス検出範囲]と[検出対象]を設定後、検出対象ごとに必要な項目を設定します。すべて設定後に[実行]ボタンを選択します。

表3.1 検出([検出方式]で「通常」を選択した場合)

設定項目	設定内容
IPアドレス検出範囲	検索対象とする範囲をIPアドレスで指定します。
検出対象	以下から選択します。 <ul style="list-style-type: none">• Server (iRMC/BMC + HTTPS) サーバ、PRIMEQUEST 3800Bを検出する場合に選択します。• PRIMERGY CX1430 M1 (BMC + HTTPS) PRIMERGY CX1430 M1を検出する場合に選択します。• PRIMEQUEST2000, PRIMEQUEST3000E (MMB + SSH + SNMP) PRIMEQUEST 2000シリーズ、またはPRIMEQUEST 3800B以外のPRIMEQUEST3000シリーズを検出する場合に選択します。• Switch, Storage, PRIMERGY BX Chassis (SSH + SNMP) ストレージ、ネットワークスイッチ、またはPRIMERGY BXシャーシを検出する場合に選択します。• Facility (SNMP)

設定項目	設定内容
	RackCDU、PDU、またはUPSを検出する場合に選択します。

表3.2 [検出対象]でServer (iRMC/BMC + HTTPS)を選択した場合

設定項目	説明
iRMC/BMC	—
ユーザー名	iRMC/BMCのユーザー名
パスワード	iRMC/BMCのパスワード
IPMIポート番号	iRMC/BMCのポート番号(初期値:623)
HTTPSポート番号	HTTPSのポート番号(初期値:443)

表3.3 [検出対象]でPRIMERGY CX1430M1 (BMC + HTTPS)を選択した場合

設定項目	説明
BMC	—
ユーザー名	BMCのユーザー名
パスワード	BMCのパスワード
ポート番号	BMCのポート番号(初期値:623)
HTTPS	—
ユーザー名	HTTPSのユーザー名
パスワード	HTTPSのパスワード
ポート番号	HTTPSのポート番号(初期値:443)

表3.4 [検出対象]でPRIMEQUEST2000, PRIMEQUEST3000E (MMB + SSH + SNMP)を選択した場合

設定項目	説明
MMB	—
ユーザー名	MMBのユーザー名
パスワード	MMBのパスワード
ポート番号	MMBのポート番号(初期値:623)
SSH	—
ユーザー名	SSHのユーザー名
パスワード	SSHのパスワード
ポート番号	SSHのポート番号(初期値:22)
SNMP	—
バージョン	SNMPのバージョンを選択
ポート番号	SNMPのポート番号(初期値:161)
コミュニティ	SNMPのコミュニティ名

表3.5 [検出対象]でSwitch, Storage, PRIMERGY BX Chassis (SSH + SNMP)を選択した場合

設定項目	説明
SSH	—
ユーザー名	SSHのユーザー名
パスワード	SSHのパスワード
ポート番号	SSHのポート番号(初期値:22)

設定項目		説明
SNMP		—
	バージョン	SNMPのバージョンを選択
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	SNMPのコミュニティ名

表3.6 [検出対象]でFacility (SNMP)を選択した場合

設定項目		説明
バージョン		SNMPのバージョンを選択
ポート番号		SNMPのポート番号(初期値:161)
コミュニティ		SNMPのコミュニティ名

5. [検出方式]で「CSVアップロード」を選択した場合、以下の項目を設定して[実行]ボタンを選択します。
検出を実行する前に検出対象ノードの情報を記載したCSVファイルを用意する必要があります。

表3.7 検出 ([検出方式]で「CSVアップロード」を選択した場合)

設定項目	設定内容
テンプレート	CSVファイルのテンプレートをダウンロードできます。 検出対象に応じたテンプレートを選択し[ダウンロード]ボタンを選択すると、CSVテンプレートをダウンロードできます。テンプレートは複数選択可能です。
ファイル選択方式	<ul style="list-style-type: none"> ローカル ローカルに格納されているCSVファイルを指定する場合に選択します。 FTP FTPでISMに転送したCSVファイルを指定する場合に選択します。
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	<ul style="list-style-type: none"> 暗号化あり CSVファイル内に記載しているパスワードを暗号化している場合に選択します。 暗号化なし CSVファイル内に記載しているパスワードを暗号化していない場合に選択します。
検出実行後の動作	[ファイル選択方式]で「FTP」を選択した場合に指定します。 検出実行後、CSVファイルを削除する場合にチェックを付けます。

以下にCSVファイルの記載例を示します。

- ー Server (iRMC/BMC + HTTPS)を検出する場合の記載例:

```
"IpAddress", "IpmiAccount", "IpmiPassword", "IpmiPort", "HttpsAccount", "HttpsPassword", "HttpsPort"
"192.168.10.11", "admin1", "*****", "", "admin1", "*****", ""
"192.168.10.12", "admin2", "*****", "", "admin2", "*****", ""
```

- ー Switch, Storage, PRIMERGY BX Chassis (SSH + SNMP)を検出する場合の記載例:

```
"IpAddress", "SshAccount", "SshPassword", "SnmpType", "Community"
"192.168.10.21", "user1", "*****", "SnmpV1", "comm1"
"192.168.10.22", "user2", "*****", "SnmpV1", "comm2"
```

6. ノードが検出され、「ノード登録」画面の[検出ノードリスト]に表示されたことを確認します。
自動更新設定が無効に指定されていると、検出ステータスは自動更新されません。
自動更新設定の更新間隔を指定する、または更新ボタンを選択して画面を更新してください。
7. 「ノード登録」画面の[検出進捗]のステータスが[完了]と表示されたら、[検出ノードリスト]を確認します。

8. 登録するノードのチェックボックスを選択します。
9. ISM 2.3.0またはISM 2.3.0.aでは、[アクション]ボタンから[検出ノード登録]を選択します。
ISM 2.3.0.b以降では、[アクション]ボタンではなく[検出ノード登録]ボタンを選択します。
[ノード登録]ウィザードが表示されます。
10. [ノード登録]ウィザードに従い、設定項目を入力します。

設定項目の説明はヘルプ画面を参照してください。
ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

表3.8 ノード情報

設定項目	設定内容
ノード名	<p>ノード名を入力します。以下の半角記号は使用できません。 / \ : * ? " < > </p> <p>ノード名には、初期値として以下が入力されています。</p> <ul style="list-style-type: none"> • DNS名が取得できた場合:DNS名 • DNS名が取得できなかった場合:xxxx_yyyy <p>xxxx、yyyyに表示される文字列は、以下のとおりです。</p> <ul style="list-style-type: none"> — xxxx ノードタイプに応じて以下の文字列が表示されます。 serverの場合:SV switchの場合:SW storageの場合:ST facilityの場合:CDU、PDU、またはUPS — yyyy ノードのシリアルナンバーです。検出時にノードのシリアルナンバーが取得できなかった場合はIPアドレスが表示されます。
シャーシ名	<p>PRIMERGY CXが検出された場合に、シャーシ名を入力します。</p> <p>同一のシャーシに搭載されたノードが検出された場合、最も若いスロットに搭載されたノードにシャーシ名を入力します。同一シャーシ内のその他のノードでは、シャーシ名が自動で入力されます。以下の半角記号は使用できません。 / \ : * ? " < > </p> <p>シャーシ名には初期値として「SV_zzzz」が入力されています。</p> <p>zzzzには、シャーシのシリアルナンバーが表示されます。検出時にシャーシのシリアルナンバーが取得できなかった場合はIPアドレスが表示されます。</p>
IPアドレス	<p>機器のIPアドレスを変更する場合に、IPアドレスを編集します。</p> <p>[編集]ボタンを選択し、IPアドレスを入力してください。IPアドレスを編集した場合、ノード登録時に機器に対してIPアドレスの変更が行われます。</p> <p>IPアドレス設定の対象機種は、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/</p>
Web i/f URL	ノードのWeb i/fにアクセスする際のURLを入力します。
説明	説明を入力します。

検出ノードリスト項目の説明はヘルプ画面を参照してください。
ヘルプ画面の表示方法:画面表示中に、右上の[?]ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択

11. 検出ノード登録情報の入力を完了後、[登録]を選択します。

以上でノード登録は完了です。

ノード登録が完了すると、当該のノードは「ノードリスト」画面に表示されます。

対象ノードからSNMPv3でトラップ受信を行う場合、SNMPトラップ受信設定が必要です。「[SNMP設定を変更する](#)」を参照してください。

対象となるノードにOSがインストールされている場合は、以降の手順を実施します。

12. 「ノードリスト」画面から対象のノードを選択し、ノードの詳細画面-[OS]タブを選択します。

13. [OSアクション]-[OS情報編集]を選択します。

「OS情報編集」画面の設定内容は以下のとおりです。

表3.9 OS情報編集

設定項目	設定内容
OSタイプ	OSの種類を選択します。
OSバージョン	OSの版数を選択します。
OS IPアドレス	IPのバージョンを設定したあと、OS管理ポートのIPアドレスを入力してください(IPv4/IPv6形式に対応しています)。
ドメイン名	ドメイン名をFQDNで入力します。
アカウント	管理用アカウントを入力します。
パスワード	管理用アカウントのパスワードを入力します。
OS接続ポート番号	OSに接続するためのポート番号を入力します。 Windowsの場合はWinRMサービスのポート番号(初期値:5986)、Linuxの場合はSSHサービスのポート番号(初期値:22)を入力してください。入力されない場合は初期値のポート番号が設定されます。

14. OS情報の入力を完了後、[適用]を選択します。

以上でOS情報編集は完了です。OS情報編集が完了すると、当該のノードのOS情報が取得可能となります。

3.1.2 ノードを直接登録する

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。

「ノード登録」画面が表示されます。

2. [アクション]ボタンから[登録]を選択します。

[ノード手動登録]ウィザードが表示されます。

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。

設定項目の説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

[ノード手動登録]ウィザードの「1.ノード情報」画面において、[通信方法]の設定項目の説明は以下のとおりです。

表3.10 [ノードタイプ]でserver、[モデル]でPRIMERGY RX/TXシリーズ、PRIMERGY CXシリーズ(CX1430 M1以外)、PRIMERGY BXシリーズ(BX900 S2以外)、PRIMEQUEST3800B、IPCOM VX2シリーズを選択した場合

設定項目	説明
iRMC	iRMCでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
ユーザー名	iRMCのユーザー名
パスワード	iRMCユーザーのパスワード
IPMIポート番号	iRMCのポート番号(初期値:623)
HTTPSポート番号	HTTPSのポート番号(初期値:443)

表3.11 [ノードタイプ]でserver、[モデル]でPRIMERGY CX1430 M1を選択した場合

設定項目		説明
BMC		BMCでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	BMCのユーザー名
	パスワード	BMCのパスワード
	ポート番号	BMCのポート番号(初期値:623)
HTTPS		HTTPSでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード
	ポート番号	HTTPSのポート番号(初期値:443)

表3.12 [ノードタイプ]でserver、[モデル]でPRIMEQUEST 2000シリーズ、PRIMEQUEST 3800B以外のPRIMEQUEST3000シリーズを選択した場合

設定項目		説明
MMB		MMBでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	MMBのユーザー名
	パスワード	MMBのパスワード
	ポート番号	MMBのポート番号(初期値:623)
SSH		SSHでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	PRIMEQUESTのユーザー名
	パスワード	PRIMEQUESTのユーザーのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	PRIMEQUESTのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.13 [ノードタイプ]でserver、[モデル]でPRIMERGY BX900 S2を選択した場合

設定項目		説明
SSH		SSHでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	PRIMERGY BX900 S2のユーザー名
	パスワード	PRIMERGY BX900 S2のユーザーのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	PRIMERGY BX900 S2のSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.14 [ノードタイプ]でserver、[モデル]でGeneric Server(IPMI)を選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCのパスワード
	ポート番号	iRMC/BMCのポート番号(初期値:623)

表3.15 [ノードタイプ]でserver、[モデル]でGeneric Server(SNMP)を選択した場合

設定項目		説明
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	Generic Server(SNMP)のSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.16 [ノードタイプ]でserver、[モデル]でotherを選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCのパスワード
	ポート番号	iRMC/BMCのポート番号(初期値:623)
HTTPS		HTTPSでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード
	ポート番号	HTTPSのポート番号(初期値:443)
SSH		SSHでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	SSHのユーザー名
	パスワード	SSHのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	登録するノードのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.17 [ノードタイプ]でswitch、[モデル]でSH-E514TR1、ICX6430、Cisco Catalyst switch、Generic Switch(SNMP)、Generic Switch(PING)、other以外、または[ノードタイプ]でstorage、[モデル]でGeneric Storage(SNMP)、Generic Storage(PING)、other以外を選択した場合

設定項目		説明
SSH		SSHでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	switchまたはstorageのユーザー名

設定項目		説明
	パスワード	switchまたはstorageのユーザーのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	switchまたはstorageのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.18 [ノードタイプ]でswitch、[モデル]でCisco Catalyst switchを選択した場合

設定項目		説明
SSH		SSHでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	ユーザー名	SSHのユーザー名
	パスワード	SSHのパスワード
	ポート番号	SSHのポート番号(初期値:22)
	イネーブルパスワード	使用しない場合は、チェックボックスをオフにします(初期値:オン)
	パスワード	イネーブルパスワード
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	Cisco Catalyst switchのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.19 [ノードタイプ]でswitch、[モデル]でGeneric Switch (SNMP)を選択した場合

設定項目		説明
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	Generic Switch (SNMP)のSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.20 [ノードタイプ]でswitch、[モデル]でotherを選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCのパスワード
	ポート番号	iRMC/BMCのポート番号(初期値:623)
HTTPS		HTTPSでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード

設定項目		説明
	ポート番号	HTTPSのポート番号(初期値:443)
SSH		SSHでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	SSHのユーザー名
	パスワード	SSHのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	登録するノードのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.21 [ノードタイプ]でstorage、[モデル]でGeneric Storage (SNMP)を選択した場合

設定項目		説明
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします(初期値:オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	Generic Storage (SNMP) のSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.22 [ノードタイプ]でstorage、[モデル]でotherを選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCのパスワード
	ポート番号	iRMC/BMCのポート番号(初期値:623)
HTTPS		HTTPSでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード
	ポート番号	HTTPSのポート番号(初期値:443)
SSH		SSHでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	ユーザー名	SSHのユーザー名
	パスワード	SSHのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	登録するノードのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「[表3.26 SNMPのバージョンでSNMPv3を選択した場合](#)」を参照してください。

表3.23 [ノードタイプ]でfacility、[モデル]でGeneric Facility (PING)、other以外を選択した場合

設定項目		説明
SNMP [注1]		SNMPでノードにアクセスしない場合は、チェックボックスをオフにします (初期値: オン)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号 (初期値: 161)
	コミュニティ	facilityのSNMPコミュニティ名

[注1]: SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.24 [ノードタイプ]でfacility、[モデル]でotherを選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCのパスワード
	ポート番号	iRMC/BMCのポート番号 (初期値: 623)
HTTPS		HTTPSでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード
	ポート番号	HTTPSのポート番号 (初期値: 443)
SSH		SSHでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	SSHのユーザー名
	パスワード	SSHのパスワード
	ポート番号	SSHのポート番号 (初期値: 22)
SNMP [注1]		SNMPでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号 (初期値: 161)
	コミュニティ	登録するノードのSNMPコミュニティ名

[注1]: SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.25 [ノードタイプ]でotherを選択した場合

設定項目		説明
iRMC/BMC		iRMC/BMCでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	iRMC/BMCのユーザー名
	パスワード	iRMC/BMCユーザーのパスワード
	ポート番号	iRMC/BMCのポート番号 (初期値: 623)
HTTPS		HTTPSでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	HTTPSのユーザー名
	パスワード	HTTPSのパスワード
	ポート番号	HTTPSのポート番号 (初期値: 443)
SSH		SSHでノードにアクセスする場合は、チェックボックスをオンにします (初期値: オフ)
	ユーザー名	ノードのユーザー名

設定項目		説明
	パスワード	ノードのユーザーのパスワード
	ポート番号	SSHのポート番号(初期値:22)
SNMP [注1]		SNMPでノードにアクセスする場合は、チェックボックスをオンにします(初期値:オフ)
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	コミュニティ	登録するノードのSNMPコミュニティ名

[注1]:SNMPのバージョンでSNMPv1またはSNMPv2cを選択した場合の設定項目です。SNMPv3を選択した場合は、「表3.26 SNMPのバージョンでSNMPv3を選択した場合」を参照してください。

表3.26 SNMPのバージョンでSNMPv3を選択した場合

設定項目		説明
SNMP		SNMPでノードにアクセスする場合は、チェックボックスをオンにします。 SNMPでノードにアクセスしない場合は、チェックボックスをオフにします。
	バージョン	SNMPのバージョン
	ポート番号	SNMPのポート番号(初期値:161)
	エンジンID	SNMPv3のエンジンID
	コンテキスト名	SNMPv3のコンテキスト名
	ユーザー名	SNMPv3のユーザー名
	セキュリティレベル	SNMPv3のセキュリティレベル
	認証プロトコル	SNMPv3の認証プロトコル
	認証パスワード	SNMPv3の認証パスワード
	暗号化プロトコル	SNMPv3の暗号化プロトコル
	暗号化パスワード	SNMPv3の暗号化パスワード

- 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、ノードの登録を確認します。

ノード登録が完了すると、当該のノードは「ノードリスト」画面に表示されます。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

以上でノード登録は完了です。

対象となるノードにOSがインストールされている場合は、以降の手順を実施します。

- 「ノードリスト」画面から対象のノードを選択し、ノードの詳細画面-[OS]タブを選択します。

- [OSアクション]-[OS情報編集]を選択します。

「OS情報編集」画面の設定内容は、以下のとおりです。

表3.27 OS情報編集

設定項目	設定内容
OSタイプ	OSの種類を選択します。
OSバージョン	OSの版数を選択します。
OS IPアドレス	IPのバージョンを設定したあと、OS管理ポートのIPアドレスを入力してください(IPv4/IPv6形式に対応しています)。
ドメイン名	ドメイン名をFQDNで入力します。
アカウント	管理用アカウントを入力します。
パスワード	管理用アカウントのパスワードを入力します。

設定項目	設定内容
OS接続ポート番号	OSに接続するためのポート番号を入力します。 Windowsの場合はWinRMサービスのポート番号(初期値:5986)、Linuxの場合はSSHサービスのポート番号(初期値:22)を入力してください。入力されない場合は初期値のポート番号が設定されます。

7. OS情報の入力を完了後、[適用]ボタンを選択します。

以上でOS情報編集は完了です。OS情報編集が完了すると、当該のノードのOS情報が取得可能となります。

3.1.3 ノードを削除する

登録されているノードを削除します。

1. ISMのGUIでグローバルナビゲーションメニューから[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。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

2. 削除するノードを選択します。

3. [アクション]ボタンから[ノード削除]を選択します。

4. 削除するノードが正しいことを確認し、[削除]を選択します。

ノード削除が完了すると、当該のノードは「ノードリスト」画面から削除されます。

以上でノード削除は完了です。

3.2 ノードの設定を行う

ノードの各イベントを監視するための設定を行います。

3.2.1 アラーム設定をする(管理対象機器のイベント)

ISMが管理対象機器からSNMPトラップを受信した場合や、管理対象機器の異常やイベントを検知した際に、ISMの外部へ通知することができます。

アラーム設定を行う場合は、以下の順に行います。

1. アクション(通知方法)設定(「[3.2.1.1 アクション\(通知方法\)を設定する](#)」参照)

2. アラーム共通設定(「[3.2.1.2 アラーム共通設定をする](#)」参照)

3. アラーム設定(「[3.2.1.3 管理対象機器を対象にアラーム設定をする](#)」参照)

3.2.1.1 アクション(通知方法)を設定する

ISMの外部への通知方法を設定します。

通知の方法としては、以下の方法があります。

- ・ 外部ホスト上に配置した任意のスクリプトを実行する
- ・ メールを送信する
- ・ SNMPトラップとして、外部のSNMPマネージャーに送信／転送する
- ・ 外部Syslogサーバに、イベントのメッセージを転送／送信する



ポイント

管理対象機器のイベントを対象としたアラーム設定で行う、アクション設定手順は、ISM内部のイベントを対象としたアラーム設定と共通です。

詳細な設定手順は、「[2.6.1 アクション\(通知方法\)を設定する](#)」を参照してください。

3.2.1.2 アラーム共通設定をする

設定したすべてのアラームに共通の設定を行います。

アラーム共通設定には、以下があります。

- トラップ受信抑止期間

同一管理対象機器から同一のSNMPトラップを連続して受信した場合に、指定した期間内に受信した同一SNMPトラップの受信を抑止して、アクションが連続して実行されることを防ぎます。

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]-[アラーム]を選択します。

2. 画面左側のメニューから[アラーム共通設定]を選択します。

「アラーム共通設定」画面が表示されます。

3. [アクション]ボタンから[編集]を選択します。

「アラーム共通設定編集」画面が表示されます。各設定項目の入力については、ヘルプ画面を参照してください。

4. 設定項目を入力し、[適用]ボタンを選択します。

以上でアラーム共通設定は完了です。

3.2.1.3 管理対象機器を対象にアラーム設定をする

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]を選択します。

3. [アクション]ボタンから[追加]を選択します。

[アラーム追加]ウィザードが表示されます。

管理対象機器の異常やイベントを対象としてアラーム設定を行う場合、[アラーム追加]ウィザードの「対象」画面で、「対象種別」に「ノード」を選択して、アラーム設定の対象とするノードを選択します。

その他の設定項目の入力については、ヘルプ画面を参照してください。

4. 「確認」画面で設定内容を確認し、[適用]ボタンを選択します。

アラームの追加が完了すると、設定したアラームが「アラームリスト」画面に表示されます。

以上で管理対象機器のイベントを対象にしたアラーム設定は完了です。

3.2.2 SNMPトラップ受信設定をする

SNMP設定を変更する

SNMPトラップ受信設定を行います。デフォルトの受信設定は、以下のように設定されています。必要に応じて変更してください。SNMPv3でトラップ受信を行う場合、ノードごとに設定が必要になります。

- SNMPv1/v2cの場合
コミュニティ:public

- SNMPv3の場合
初期設定なし

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]を選択します。

「トラップ受信設定リスト」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、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。

MIBファイルを追加する

HPサーバ、Ciscoスイッチなど富士通以外のベンダーから提供されているハードウェアを監視する場合、MIBファイルを別途入手しISM内にインポートする必要があります。

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がある場合、対象のファイルすべてが必要になります。
2. FTPを使ってISM-VAへ転送します。FTPでftp://<ISM-VAのIPアドレス>/Administrator/ftp/mibsにアクセスし、MIBファイルをすべて格納します。
3. コンソールからadministratorでISM-VAにログインします。
4. コマンドismadm mib importを実行します。

コマンドを実行すると、FTPに格納したMIBファイルすべてについて一括でインポート処理を行います。

3.2.3 ログ収集スケジュールを設定する

ISMは設定したスケジュール(例:毎日23時)に従って、定期的にノードのログを収集して蓄積しておくことができます。ノードごとに異なる設定が可能です。また設定したスケジュール内容を任意のタイミングで実行させてログ収集することもできます。

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。
「ノードリスト」画面が表示されます。
なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。
2. ノードリストから、設定対象のノードを選択します。
3. [ログ収集設定]タブを選択します。
4. [ログ収集設定]タブ内の[ログ収集設定アクション]ボタンから[ログ収集設定編集]を選択します。
5. 設定画面内で必要な設定を入力し、[適用]ボタンを選択します。
 - － [スケジュールタイプ]を選択後、[追加]ボタンを選択してログ収集日時を指定してください。
 - － [スケジュール実行有効化]にチェックを付けてください。チェックがない場合、作成したスケジュールは実行されません。
 - － ノードがサーバの場合、ノードのOS情報を正しく設定すると、ログ収集対象として[オペレーティングシステムログ]、[ServerView Suiteログ]が選択できます。
ただし、サーバの種類によっては、[ハードウェアログ]、[ServerView Suite ログ]は選択できません。この場合、ログ収集もできません。以上の操作で、指定した日時に対象ノードのログが自動的に収集され、ISM内に蓄積されるようになります。
6. 設定した内容に従って任意のタイミングでログ収集を行う場合は、[ログ収集設定]タブ内の[ログ収集設定アクション]ボタンから[ログ収集実行]を実行します。
ログ収集が実行されます。[ログ収集実行]の作業はISMのタスクとして登録されます。グローバルナビゲーションメニュー上部の[タスク]を選択して、タスクの完了を確認してください。

3.3 サーバに各種設定／OSインストールをする

サーバを初期導入する場合や、新たに増設する場合などに、サーバに対してハードウェア設定(BIOS、iRMC、MMB)やOSインストール、仮想IOの設定を複数のサーバに対して一括して行うことができます。

3.3.1 プロファイルでBIOS／iRMC／MMB／仮想IOを設定する

プロファイルは、ノードのハードウェア設定やOSインストール時の設定をまとめたもので、ノード個別に作成します。

ISMに登録したサーバに対して、作成したプロファイルを適用することでサーバのBIOS／iRMC／MMB／仮想IOを設定します。

ポイント

ポリシーを利用して、プロファイルの作成を簡略化できます。詳細は、「[3.3.3 ポリシーを作成してプロファイルの作成を簡略化する](#)」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[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。
「全てのプロファイル」画面が表示されます。
3. [アクション]ボタンから[プロファイル追加]を選択します。
[プロファイル追加]ウィザードが表示されます。
4. [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

設定項目の入力については、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

【ポリシーを使用しBIOSを設定する場合】

- a. [プロファイル追加]ウィザードの「1.基本情報」画面内の[BIOSポリシー]で、作成したポリシー（または流用するポリシー）を選択します。
- b. 「1.基本情報」画面内のその他の設定項目を入力して、[次へ]を選択します。
「2.詳細」画面内の[BIOS]タブに、選択したポリシーの設定値が自動的に入力されます。
- c. 必要に応じてその他の項目を設定します。

【ポリシーを使用しiRMCを設定する場合】

- a. [プロファイル追加]ウィザードの「1.基本情報」画面内の[iRMCポリシー]で、作成したポリシー（または流用するポリシー）を選択します。
- b. 「1.基本情報」画面内のその他の設定項目を入力して、[次へ]を選択します。
「2.詳細」画面内の[iRMC]タブに、選択したポリシーの設定値が自動的に入力されます。
- c. 必要に応じてその他の項目を設定します。

【ポリシーを使用しMMBを設定する場合】

- a. [プロファイル追加]ウィザードの「1.基本情報」画面内の[MMBポリシー]で、作成したポリシー（または流用するポリシー）を選択します。
- b. 「1.基本情報」画面内のその他の設定項目を入力して、[次へ]を選択します。
「2.詳細」画面内の[MMB]タブに、選択したポリシーの設定値が自動的に入力されます。
- c. 必要に応じてその他の項目を設定します。

【仮想IOを設定する場合】

- a. [プロファイル追加]ウィザードの「1.基本情報」画面内の設定項目を入力して、[次へ]を選択します。
 - b. 「2.詳細」画面内の[仮想IO]タブで、[設定]を選択し、ウィザードに従って設定項目を入力します。
5. プロファイルの追加を確認します。

プロファイルの追加が完了すると、当該のプロファイルが「全てのプロファイル」画面に表示されます。

以上でプロファイル作成は完了です。続けてプロファイルを適用します。

- 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]を選択します。

「ノードリスト」画面が表示されます。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

- [カラム表示]で[プロファイル]を選択します。
- プロファイルを適用すべきノードをノードリストから選択します。
- [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。

「プロファイル適用」画面が表示されます。

- 「プロファイル適用」画面に従い、設定項目を入力します。

設定項目の入力は、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:画面右上の[?]を選択

BIOS/iRMC/MMB/仮想IO設定が完了すると、「ノードリスト」画面内の当該サーバの[ステータス]列が[適用済]と表示されます。



ポイント

事前にノードにタグを設定しておくことで、「ノードリスト」画面でタグによるノードのフィルタリングを行えます。ノードをフィルタリングすることで対象のノードを抽出しやすくなります。

3.3.2 プロファイルでサーバにOSをインストールする

ISMに登録したサーバに対して、OSをインストールします。

次のOSをインストールできます。

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware

- OSインストールの事前環境構築として、DHCPサーバを作成します。

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/technical/>

- OSインストールの事前設定として、OSイメージをリポジトリ領域にインポートします。

リポジトリの管理については、『ユーザーズマニュアル』の「2.13.2 リポジトリ管理機能」を参照してください。

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

「全てのプロファイル」画面が表示されます。

- [アクション]ボタンから[プロファイル追加]を選択します。

[プロファイル追加]ウィザードが表示されます。

- [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

設定項目の入力については、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

- [プロファイル追加]ウィザードの「1.基本情報」画面内の[OSタイプ]で、インストールするOSのタイプを選択します。

- b. 「1.基本情報」画面内のその他の設定項目を入力して、[次へ]を選択します。
- c. 「2.詳細」画面内の[OS]タブを選択し、設定項目を入力します。
- d. 「2.詳細」画面内の[OS個別情報]タブを選択し、設定項目を入力します。

プロファイルの追加が完了すると、当該のプロファイルが「全てのプロファイル」画面に表示されます。

- 7. 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。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

- 8. [カラム表示]で[プロファイル]を選択します。
- 9. プロファイルを適用すべきノードをノードリストから選択します。
- 10. [アクション]ボタンから[プロファイル適用/再適用]を選択します。
- 「プロファイル適用」画面が表示されます。
- 11. 「プロファイル適用」画面に従い、設定項目を入力します。

設定項目の入力は、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:画面右上の[?]を選択

OSインストールが完了すると、「ノードリスト」画面内の当該サーバの[ステータス]列が[適用済]と表示されます。

ポイント

.....
事前にノードにタグを設定しておくことで、「ノードリスト」画面でタグによるノードのフィルタリングを行えます。ノードをフィルタリングすることで対象のノードを抽出しやすくなります。
.....

3.3.3 ポリシーを作成してプロファイルの作成を簡略化する

ノードのハードウェア設定をテンプレート化したものをポリシーと呼びます。これにより多数のノードを管理する際に共通要素はポリシーを指定することでプロファイルへの入力を簡略化できます。このポリシーを作成します。ポリシーの作成は任意であって、プロファイル作成時に必須ではありません。

- 1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
- 2. 画面左側のメニューから[ポリシー設定]-[全てのポリシー]を選択します。
- 「全てのポリシー」画面が表示されます。
- 3. [アクション]ボタンから[ポリシー追加]を選択します。
- [ポリシー追加]ウィザードが表示されます。
 - ー BIOSのポリシーを設定する場合
 - [ポリシー追加]ウィザードの「1.基本情報」画面内の[ポリシータイプ]で、[BIOS]を選択します。
 - ー iRMCのポリシーを設定する場合
 - [ポリシー追加]ウィザードの「1.基本情報」画面内の[ポリシータイプ]で、[iRMC]を選択します。
 - ー MMBのポリシーを設定する場合
 - [ポリシー追加]ウィザードの「1.基本情報」画面内の[ポリシータイプ]で、[MMB]を選択します。

その他の設定項目は[ポリシー追加]ウィザードに従い入力します。

設定項目の入力はヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

ポリシーの追加が完了すると、当該のポリシーが「全てのポリシー」画面に表示されます。

3.4 スイッチ／ストレージを設定する

スイッチやストレージを初期導入する場合や増設する場合などに、プロファイルを利用することで、以下のような設定ができます。

- ・ スイッチ
管理者パスワードやSNMPの設定などを複数のノードに対して一括して行う
- ・ ストレージ
RAID構成やディスク構成の設定などを行う

また、ネットワークマップを利用することで、複数スイッチの複数ポートに対して、VLANやリンクアグリゲーションの設定を一括して行うことができます。

3.4.1 プロファイルでスイッチ／ストレージを設定する

ISMに登録したスイッチ／ストレージに対して、作成したプロファイルを適用することで、RAID構成やSNMP設定、アカウントなどを設定します。

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[プロファイル設定]-[全てのプロファイル]を選択します。
「全てのプロファイル」画面が表示されます。
3. [アクション]ボタンから[プロファイル追加]を選択します。
[プロファイル追加]ウィザードが表示されます。
4. [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。

RAID構成やSNMP設定、アカウントなど、各機器に応じた設定内容を入力してください。

設定項目の入力はヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

プロファイルの追加が完了すると、当該のプロファイルが「全てのプロファイル」画面に表示されます。

以上でプロファイル作成は完了です。続けてプロファイルを適用します。

5. 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。
なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

6. [カラム表示]で[プロファイル]を選択します。
7. プロファイルを適用すべきノードをノードリストから選択します。
8. [アクション]ボタンから[プロファイル適用/再適用]を選択します。
「プロファイル適用」画面が表示されます。

9. 「プロファイル適用」画面に従い、設定項目を入力します。

設定項目の入力はヘルプ画面を参照してください。

ヘルプ画面の表示方法:画面右上の[?]を選択

プロファイルの適用が完了すると、「ノードリスト」画面内の当該ノードの[ステータス]列が[適用済]と表示されます。

以上でノードへのプロファイル適用は完了です。

3.4.2 ネットワークマップからLANスイッチの設定を変更する

ネットワークマップ上で視覚的に確認しながら、LAN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を変更します。

LANスイッチのVLAN設定を変更する

ネットワークマップからLANスイッチのVLANの設定を変更します。

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]-[ネットワークマップ]を選択します。
「ネットワークマップ表示」画面が表示されます。
2. [アクション]-[VLAN一括設定]を選択し、設定の変更内容を入力します。
3. ネットワークマップ上のLANスイッチで、VLANの設定を変更したいポートを選択します。
4. 右上の[設定]を選択し、設定の変更内容を入力します。
5. 変更内容を確認し、問題なければ[登録]を選択します。
設定が変更されます。
6. 実行完了後、ネットワーク管理情報を最新化し、ネットワークマップ上で変更が適用されていることを確認します。
[VLAN設定]の作業はISMのタスクとして登録されます。グローバルナビゲーションメニュー上部の[タスク]を選択して、タスクの完了を確認してください。
以上でVLANの設定変更は完了です。

LANスイッチのリンクアグリゲーション設定を変更する

ネットワークマップからLANスイッチのリンクアグリゲーションの設定を変更します。

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]-[ネットワークマップ]を選択します。
「ネットワークマップ表示」画面が表示されます。
2. [アクション]-[リンクアグリゲーション設定]を選択します。
3. リンクアグリゲーション設定を行うノードを選択し、[追加]、[変更]、[削除]のどれかを選択します。
4. 設定の変更内容を入力し、[確認]を選択します。
5. 変更内容を確認し、問題なければ[登録]を選択します。
設定が変更されます。
6. 実行完了後、ネットワーク管理情報を最新化し、ネットワークマップ上で変更が適用されていることを確認します。
以上でリンクアグリゲーションの設定変更は完了です。

3.5 パスワードを変更する

管理対象ノード、および管理対象ノードにインストールしているOSのパスワードを変更します。

パスワードの変更は、変更対象のノードをメンテナンスモードに設定して行います。

3.5.1 管理対象ノードのパスワードを変更する

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. ノードリストから、変更対象のノード名を選択します。
ノードの詳細画面が表示されます。
3. [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。
4. 変更対象のノードのパスワードを変更します。
5. [アクション]ボタンから[編集]を選択します。
「編集」画面が表示されます。
6. 通信方法のパスワードを手順4で変更したパスワードに変更します。
パスワード以外の各設定項目は、必要に応じて変更します。
7. 変更内容を確認し、[適用]ボタンを選択します。

8. [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。

以上で管理対象ノードのパスワード変更は完了です。

3.5.2 OSのパスワードを変更する

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. ノードリストから、変更対象のノード名を選択します。
ノードの詳細画面が表示されます。
3. [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。
4. 変更対象のOSのパスワードを変更します。
5. [OS]タブを選択します。
6. [OSアクション]ボタンから[OS情報編集]を選択します。
「OS情報編集」画面が表示されます。
7. パスワードを手順4で変更したパスワードに変更します。
パスワード以外の各設定項目については、必要に応じて変更します。
8. 変更内容を確認し、[適用]ボタンを選択します。
9. [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。
以上でOSのパスワード変更は完了です。

第4章 管理対象ノードの状態を確認する

この章では、管理対象ノードやリソースのステータスやログなどの各種情報を確認する方法を説明します。

4.1 ダッシュボードを操作する

ダッシュボードは、ステータスやログなどの各種情報を表示するウィジェットを表示します。利用者の用途に合わせてウィジェットを選択し、必要となる情報を参照できます。

ダッシュボードに表示させるウィジェットの選択方法はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[?]ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択

4.2 ノードの位置を確認する

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。

また、「3Dビュー」画面では、フロア、ラックの配置、ラック内の機器搭載位置を3次元画像で確認できます。

ラックビューからノードの搭載位置を確認する

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]を選択します。
「データセンターリスト」画面が表示されます。
2. 該当のラックを選択してノードの位置を確認します。

3Dビューからノードの状態を確認する

ラックや機器の配置、およびステータスや消費電力、吸気温度を三次元表示で確認します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[3Dビュー]を選択します。
「3Dビュー」画面が表示されます。
2. 目的に応じて以下の操作を行います。
 - ー 表示するフロアを切り替える場合
 - a. 「3Dビュー」画面左上のフロアサマリのフロア表示部を選択します。
「フロア選択」画面が表示されます。
 - b. 確認したいフロアを選択し、[適用]ボタンを選択します。
フロア表示が切り替わります。
 - ー 表示情報を切り替える場合
「3Dビュー」画面右下の表示情報切替え用のボタンで表示したい情報を選択します。
3Dビューでは、以下の表示情報が確認できます。
 - ステータス
 - アラームステータス
 - 吸気温度
 - 消費電力

以上で3Dビューからのノード状態の確認は完了です。

ポイント

表示情報で消費電力ステータスを表示する場合は、事前に管理対象機器のノードの詳細画面の[監視]タブで[NodePowerConsumption]のしきい値を設定する必要があります。

4.3 ノードの状態を確認する

ノードの状態はダッシュボードの[ステータス]ウィジェットおよび「ノードリスト」画面で確認できます。

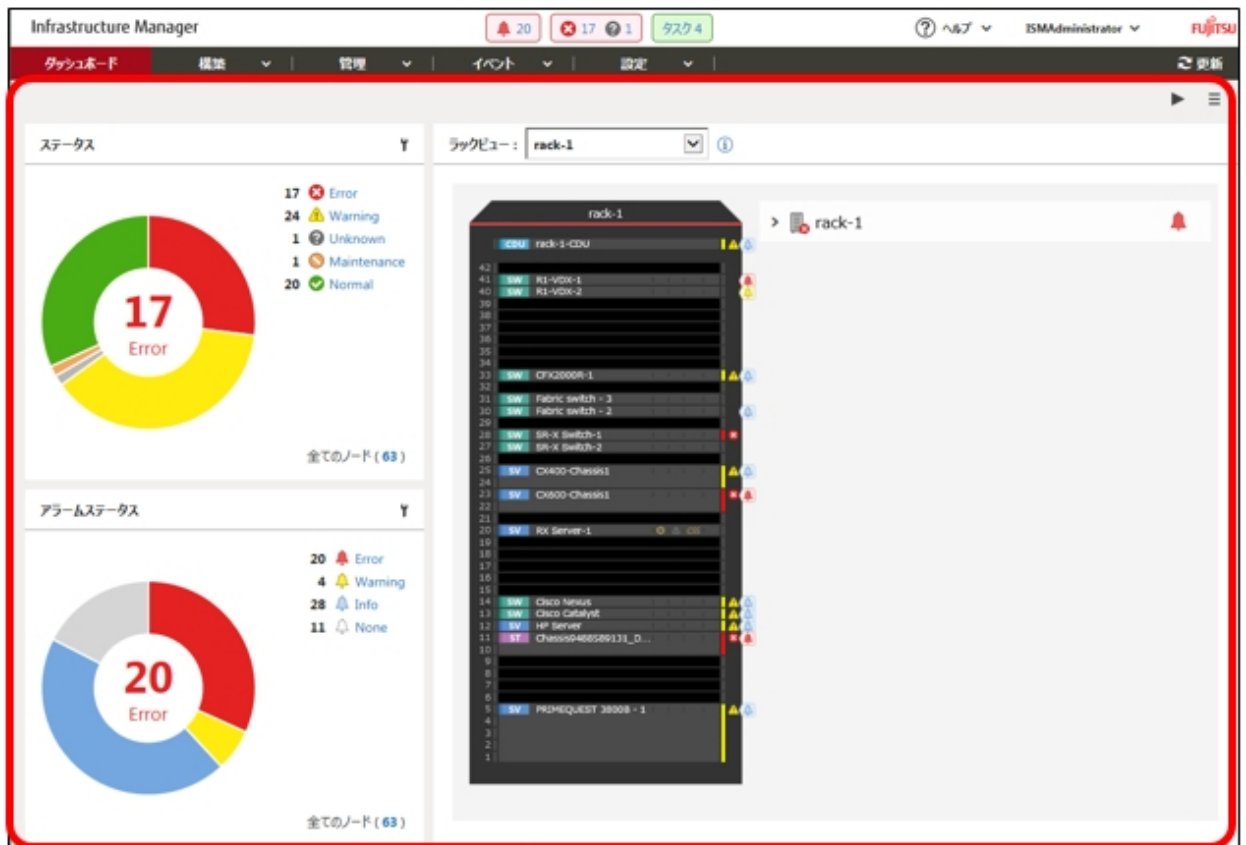
1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。

「ダッシュボード」画面が表示されます。

2. [ステータス]ウィジェットでノードの状態を確認します。

[ステータス]ウィジェットの詳細な説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択



[ダッシュボード] 画面

3. [ステータス]ウィジェットで、状態を確認するステータス(Error、Warning、Maintenance、Normal、Unknown)を選択します。

当該ステータスのノードが「ノードリスト」画面に表示されます。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

表示内容の説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択

以上でノード状態の表示は完了です。

4.4 ノードの通知情報を表示する

ノードのイベント発生およびノード状態はダッシュボードの[アラームステータス]ウィジェットおよび「ノードリスト」画面で確認できます。

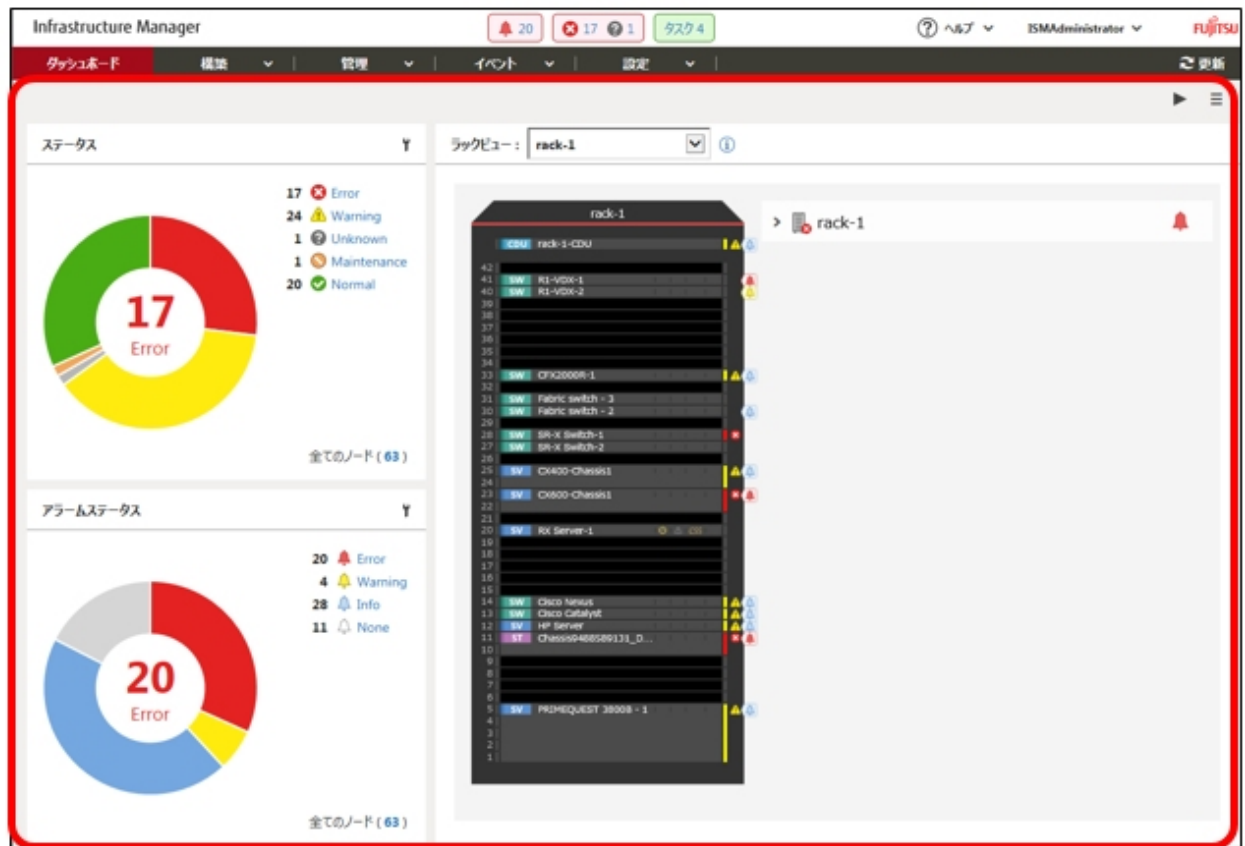
1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。

「ダッシュボード」画面が表示されます。

2. [アラームステータス]ウィジェットでアラームを確認します。

[アラームステータス]ウィジェットの説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[?]ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択



「ダッシュボード」画面

3. [アラームステータス]ウィジェットで、状態を確認するステータス(Error、Warning、Info、None)を選択します。

当該アラームステータスのノードが「ノードリスト」画面に表示されます。

なお、ISMに登録されているノード数により、ノードリストが表示されるまで時間がかかる場合があります。

表示内容の説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[?]ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択

以上でノード通知情報の表示は完了です。

4.5 監視履歴をグラフ表示する

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の[監視履歴]ウィジェットに表示する方法があります。

4.5.1 ノードごとに監視履歴をグラフ表示する

ノードごとに監視項目の履歴をグラフ表示します。

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. 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. グラフ表示する監視項目の[グラフ]ボタンを選択します。
[監視履歴グラフ]画面が表示され、グラフが表示されます。

複数のグラフを重ね合わせて表示する

[監視履歴グラフ]画面では、複数のグラフを重ね合わせて表示できます。

他の期間と比較する

[他の期間と比較]タブでは、同一監視項目の複数期間のグラフを重ね合わせて表示できます。最大5期間を追加し、6グラフを重ね合わせて表示できます。複数期間のグラフを重ねることにより、時間ごと、曜日ごとの傾向を比較して把握できます。

以下の手順で行います。

1. [他の期間と比較]タブで[表示期間追加]ボタンを選択します。
2. グラフ表示する期間を選択します。
複数のグラフが重ね合わされて表示されます。

他の項目と比較する

[他の項目と比較]タブでは、同一ノード内のほかの監視項目のグラフを重ね合わせて表示できます。最大1項目を追加し、2グラフを重ね合わせて表示できます。ほかの監視項目のグラフを重ねることにより、監視項目ごとの相関を把握できます。

以下の手順で行います。

1. [他の項目と比較]タブで[表示項目追加]ボタンを選択します。
2. 比較する項目およびグラフ表示開始日時を選択します。
複数のグラフが重ね合わされて表示されます。

4.5.2 複数ノードの監視履歴をグラフ表示する

複数ノードの監視履歴のグラフをダッシュボードに表示します。

1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。
2. [ウィジェット追加]を選択します。
3. [監視履歴]を選択して、[追加]ボタンを選択します。
4. [ウィジェット設定]ウィザードの指示に従い、ウィジェットに表示するノードおよび監視項目を選択します。
ダッシュボードに[監視履歴]ウィジェットが追加されます。

ポイント

- [監視履歴]ウィジェットを追加すると、ダッシュボード画面右上に期間指定プルダウンボックスが表示されます。このプルダウンボックスで[監視履歴]ウィジェットに表示する期間を変更できます。
- 期間指定プルダウンボックスでは、[監視履歴]ウィジェットの表示期間のみ変更できます。期間を指定しても、[監視履歴]ウィジェット以外のウィジェットは影響を受けません。

4.6 ファームウェアバージョンを確認する

ISMに登録したサーバのファームウェアバージョンを表示します。

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。
「ファームウェア」画面が表示されます。
2. 対象機器のノード名を選択し、「ノード情報」画面内の[ノード情報取得]から、ノード情報取得を行います。
ファームウェアバージョンを確認するノード数分、実施します。
「ファームウェア」画面内の当該サーバの[現行バージョン]列にファームウェアバージョンが表示されます。
以上でサーバのファームウェアバージョン確認は完了です。

ポイント

- ・ ノード情報取得は時間がかかるため、画面とは非同期で処理されます。
- ・ 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。
- ・ 事前にノードにタグを設定しておくことで、「ノードリスト」画面でタグによるノードのフィルタリングを行えます。ノードをフィルタリングすることで対象のノードを抽出しやすくなります。

4.7 ノードログを表示する

管理対象ノードから収集したログを時系列に並べて表示します。重大度、カテゴリー（ハードウェア、オペレーティングシステム）、管理対象ノードなどの条件を指定することにより、表示するログを絞り込めます。

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. 画面左側のメニューから[ノードログ検索]を選択します。
「ノードログリスト」画面が表示されます。
3. ノードログの表示を絞り込む場合は、[フィルター]ボタンを選択します。
「フィルター」画面が表示されます。
4. 「フィルター」画面にフィルタリング条件を入力し、[フィルター]ボタンを選択します。
フィルタリング条件の入力はヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択
「ノードログリスト」画面に、フィルターされたノードログが表示されます。
以上でノードログの表示は完了です。

4.8 保管ログをダウンロードする

管理対象ノードから収集した保管ログをダウンロードできます。

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]-[ログ収集]を選択します。
2. 画面左側のメニューから[ログ管理]-[保管ログ]タブを選択します。
3. 保管ログをダウンロードするノードのチェックボックスをオンにします。
4. [アクション]ボタンから[ダウンロードファイル作成]を選択します。
「ダウンロードファイル作成 (保管ログ)」画面が表示されます。
5. 設定項目を入力し、[適用]ボタンを選択します。
設定項目の入力はヘルプ画面を参照してください。
ヘルプ画面の表示方法: 画面右上の[?]を選択

ダウンロードファイルが作成されます。

6. ダウンロードファイル項目の[ダウンロード]ボタンを選択します。

手順5で作成されたダウンロードファイルがコンソールにダウンロードされます。

以上で保管ログのダウンロードは完了です。

第5章 異常な管理対象ノードを特定する

この章では、何らかの異常が発生しているノードの特定方法や、その際の保守資料の採取方法について説明します。

5.1 異常が発生しているノードを確認する

現在、異常が発生している監視対象ノードだけを表示することで、異常ノードの情報が確認しやすくなります。

ISMはノードの状態をリアルタイムに画面更新をしません。ノードの現在の状態を表示させるためには、更新ボタンを選択し画面を更新してください。

1. ISMのGUIでグローバルナビゲーションメニューから[ダッシュボード]を選択します。

2. [ステータス]ウィジェットで、の右の[Error]を選択します。

異常が発生しているノードだけが表示されます。

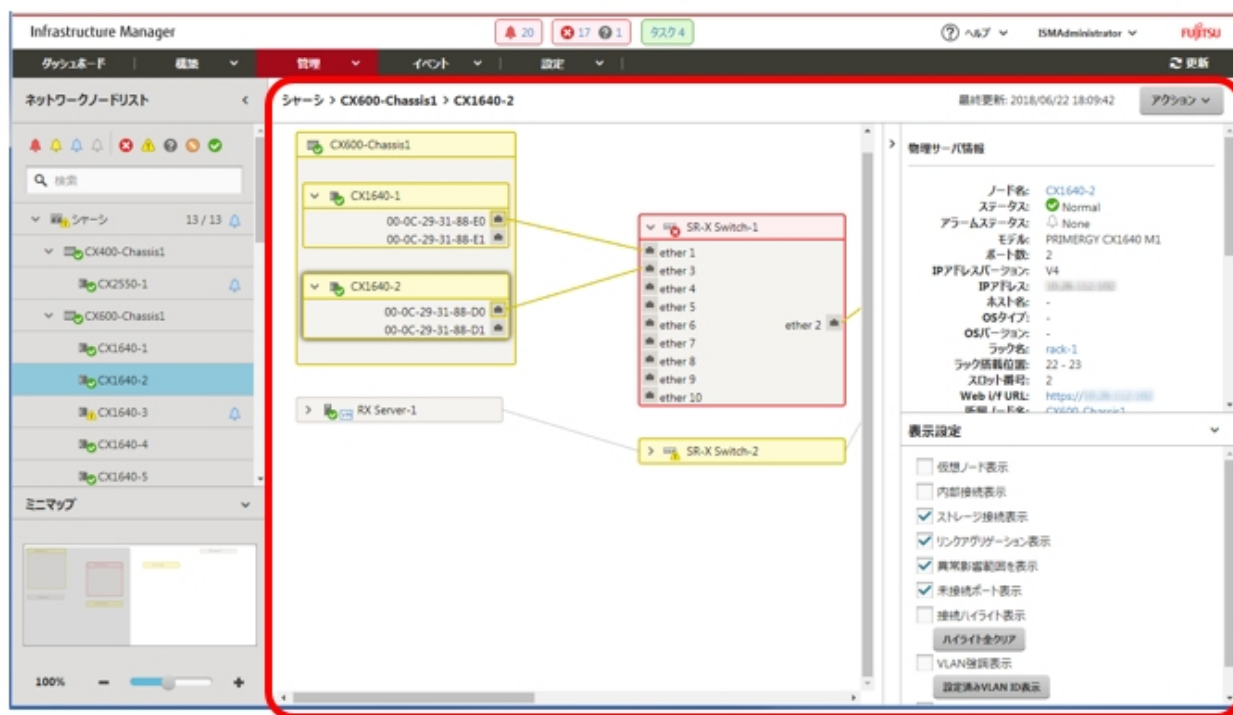
3. 表示された異常ノードの情報から状況を確認します。

5.2 ネットワーク上の異常箇所／影響範囲を確認する

ネットワーク上の異常をネットワークマップにより視覚的に表示させることで、異常箇所とその影響範囲を確認できます。

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]-[ネットワークマップ]を選択します。

「ネットワークマップ表示」画面が表示されます。



[ネットワークマップ表示]画面

異常が発生しているノードはアイコンが赤色になっています。

2. ネットワークマップ右下に表示されている表示設定パネルで[異常影響範囲を表示]にチェックを付けて、異常影響範囲を表示状態にします。

異常の影響範囲にあたる接続関係、ポートの枠またはノードの枠が黄色で表示されます。

仮想ネットワークが構築されている場合、異常の影響範囲にあたる仮想マシン、仮想スイッチ、仮想ルータおよび仮想的な接続関係についても黄色で表示されます。

以上でネットワーク上の異常箇所／影響箇所の確認は完了です。

5.3 管理対象ノードのログを収集する

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。

GUIを使ったログ収集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. ログ収集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[ログ収集実行]を選択します。
「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、[Collecting Node Log]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。



ポイント

手動ログ収集操作は、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。

- 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、以下のどちらかを行います。
 - ー ログ収集メニューの[ログ管理]を選択します。
 - ー ログ収集メニューの[ノードログ検索]を選択します。
- 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、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

- 手動ログ収集のキャンセルは、グローバルナビゲーションメニュー上部の[タスク]から行えますが、すでにログ収集が実行中の場合、ログ収集が完了するまでキャンセルは完了しません。
- 手動ログ収集を1回実行するたびに、保管ログの保有世代数が加算されます。連続して何度も実行すると、保有最大世代数の設定を超えた過去のログが削除されますので注意してください。なお、手動ログ収集がエラーとなった場合は世代数にカウントされません。
- 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、ログ削除完了後に実行されます。

第6章 対象ノードを管理／操作するその他の機能

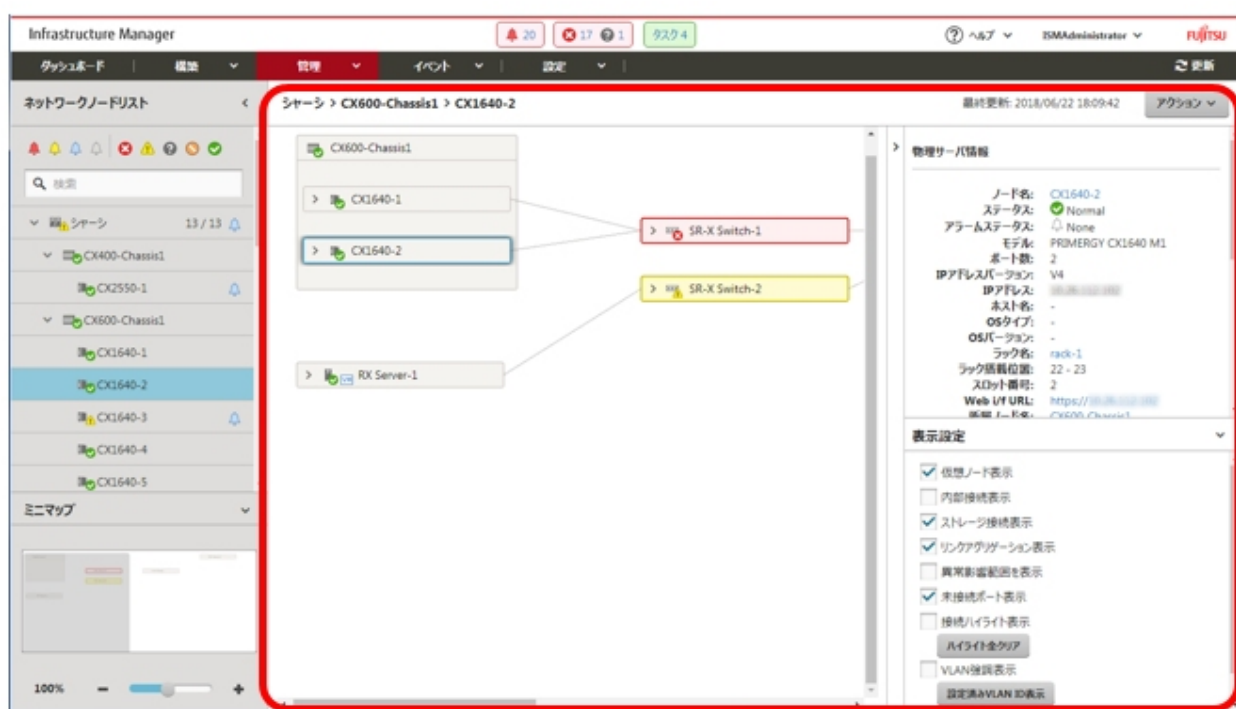
この章では、各ノードに対する様々な操作について説明します。

6.1 ネットワークマップを設定する

ネットワークマップでは、管理対象ノード間のLANケーブルの物理的な接続状態が表示されます。管理対象ノードのネットワークポートのLLDP(Link Layer Discovery Protocol)が有効の場合、管理対象ノード間の接続関係が取得され、ネットワークマップ上に接続状態が表示されます。管理対象ノードがLLDPをサポートしていない、または無効の場合、接続関係は自動的に表示されません。その場合、ユーザーが接続状態を手動で定義できます。

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。

「ネットワークマップ表示」画面が表示されます。



[ネットワークマップ表示]画面

2. [アクション]ボタンから[ネットワーク管理情報の取得]を選択し、[ネットワーク管理情報の取得]ボタンを選択します。
3. [アクション]ボタンから[手動接続編集]を選択します。
4. 接続するノードのノード名を選択します。
ネットワークポート(🔌)が表示されます。
5. 接続する2つのポートを選択し、[追加]ボタンを選択します。
設定した結線が緑になります。
6. 設定する接続の数だけ手順3～5を繰り返します。
7. 「ネットワークマップ表示」画面で、[保存]ボタンを選択します。
8. 「編集内容保存」画面で設定した接続の内容を確認し、[保存]ボタンを選択します。
設定した結線がグレーになります。

以上でネットワーク接続設定は完了です。

6.2 仮想マシン／仮想リソースの情報を表示する

仮想化管理ソフトウェアと連携することで、管理対象サーバ上で動作する仮想マシン、仮想スイッチの情報や、構成している仮想リソース（ストレージプール(クラスタ)）の情報を確認できます。

ISMで仮想マシンなどの情報や仮想リソースの情報を表示するための設定を行います。

6.2.1 仮想化管理ソフトウェアを登録する

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]を選択します。
2. 画面左側のメニューから[仮想化管理ソフトウェア]を選択します。
「仮想化管理ソフトウェアリスト」画面が表示されます。
3. [アクション]ボタンから[登録]を選択します。
「仮想化管理ソフトウェア登録」画面が表示されます。
4. 登録に必要な情報を入力します。
設定項目の入力は、ヘルプ画面を参照してください。
5. [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」画面に設定した仮想化管理ソフトウェアが表示されます。
以上で仮想化管理ソフトウェアの登録は完了です。

6.2.2 管理対象サーバ上の仮想マシンの情報を確認する

仮想マシンの情報を表示するために、仮想化管理ソフトウェアの現在の情報を取得します。



ポイント

.....
事前に管理対象サーバがISMにノード登録されていて、OS情報が設定されている必要があります。
.....

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]を選択します。
「ノードリスト」画面が表示されます。
2. 仮想化管理ソフトウェアで管理されているノードを選択します。
ノードの詳細画面が表示されます。
3. [アクション]ボタンから[ノード情報取得]を選択します。
ノード情報が取得されます。ノード情報取得が完了後、以下を実行します
4. 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。
5. 画面左側のメニューから[仮想化管理ソフトウェア]を選択します。
「仮想化管理ソフトウェアリスト」画面が表示されます。
6. 以下のどちらかの方法で情報取得を実行します。
 - － 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]ボタンを選択し、[実行]ボタンを選択します。
 - － 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ます。[アクション]ボタンから[情報取得]を選択し、[実行]ボタンを選択します。

仮想化管理ソフトウェアの情報取得の完了後、以下を実行します。

7. 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。
8. 手順3でノード情報取得を行ったノードを選択します。
ノードの詳細画面が表示されます。
9. 以下のそれぞれの手順で仮想マシンの情報を確認します。
 - ー ノード上に登録されている仮想マシンの一覧と各仮想マシンに割り当てられているCPU、メモリ情報などを確認する場合は、[仮想マシン]タブを選択します。
 - ー 仮想マシンのパワーステータスや、仮想アダプターの情報、仮想スイッチとの接続状態などを確認する場合は、[プロパティ]タブから[ネットワーク]の「マップ」を選択して、ネットワークマップを表示します。
ネットワークマップで確認したい仮想マシンを選択し、仮想マシン情報を確認します。

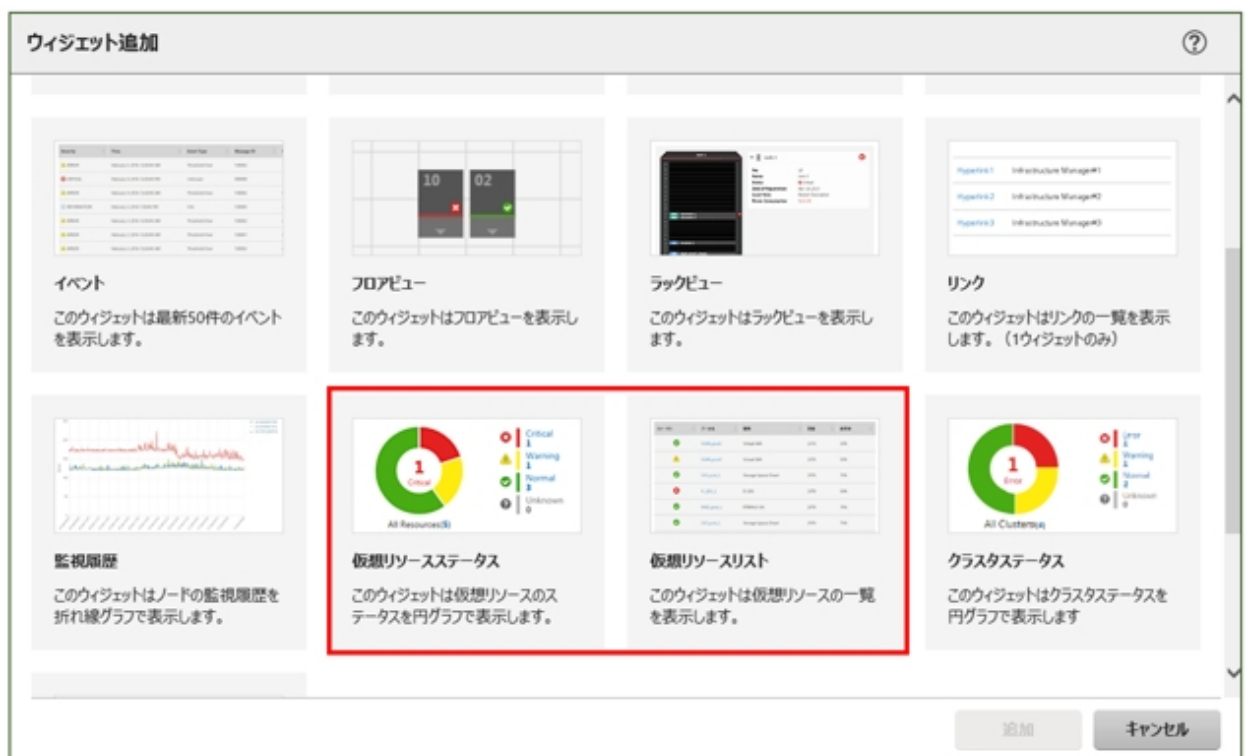
6.2.3 仮想リソースの情報を確認する

ISMダッシュボード上に、仮想リソース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リソース情報(詳細情報)を表示できます。

また、ノードの詳細画面からもリソース情報を確認できます。

ISMダッシュボードから仮想リソースの状態を確認する

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]を選択します。
「ダッシュボード」画面が表示されます。
2. 画面右上部にある[≡]ボタンから[ウィジェット追加]を選択します。
「ウィジェット追加」画面が表示されます。
「仮想リソースステータス」、「仮想リソースリスト」が仮想リソースの表示用ウィジェットです。



3. 「仮想リソースステータス」、「仮想リソースリスト」のどちらかを選択し、[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。



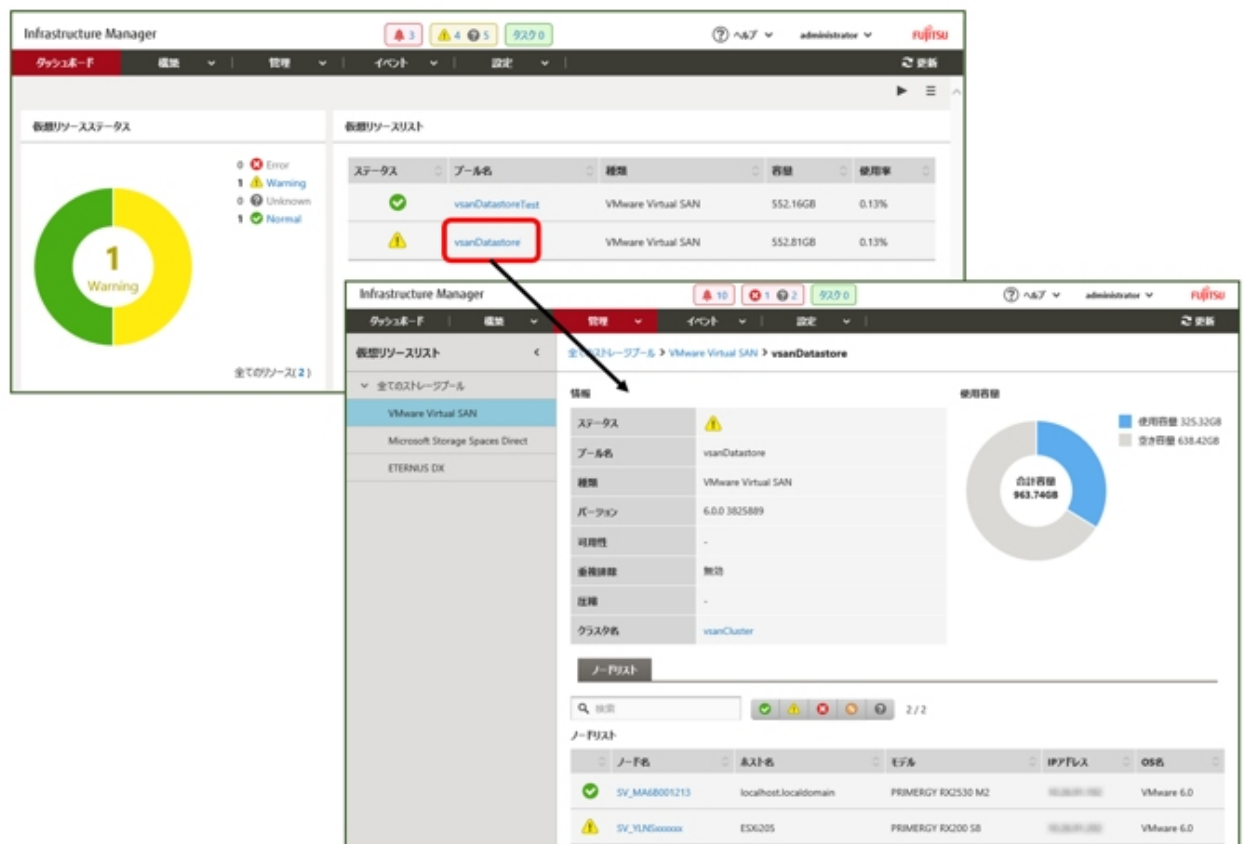
4. [仮想リソースリスト]ウィジェットで状態を確認するプール名を選択、または[仮想リソースステータス]ウィジェットで状態を確認するステータス (Error、Warning、Unknown、Normal) を選択します。

プール名を選択した場合は、プールの詳細情報が表示されます。

ステータスを選択した場合は、当該ステータスの一覧が表示されます。

表示内容の説明はヘルプ画面を参照してください。

ヘルプ画面の表示方法: 画面表示中に、右上の[ヘルプ]-[ヘルプ]-[この画面のヘルプ]を選択



ノードの詳細画面からリソース情報を確認する

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。
ノードの詳細画面が表示されます。

The screenshot shows the 'Infrastructure Manager' interface. The top navigation bar includes 'ダッシュボード', '構築', '管理' (selected), 'イベント', and '設定'. The breadcrumb trail is 'ノードリスト > ESXi228_Chassis > ESXi227'. The 'ノード情報取得: 2018/05/31 15:02' and 'アクション' buttons are visible. Below the navigation tabs, a summary row shows: ステータス (Warning), アラームステータス (Error), パワーステータス (オン), イベント (231), 運用ログ (9), 監査ログ (0), SNMPトラップ (0), アラーム設定 (0), 実行中タスク (0), ノードログ (0), 監視ログ (0), and ネットワーク (マップ). The '基本情報' section contains a table with fields: ノード名 (ESXi227), ベンダー名 (FUJITSU), 更新日 (2018/05/31), iRMC管理画面 (-), 説明 (-), and タグ (-). The 'サブURL' section shows a table with columns '名前' and 'URL', with a note 'サブURLがありません。'. The '搭載ラック情報' section shows a table with fields: データセンター (-), ラック (-), シャーシ (ESXi228_Chassis), ユニットサイズ (-), フロア (-), 搭載位置 (-), and スロット番号 (2).

2. [SDS]タブを選択します。
ノードと関連するストレージプールの情報が表示されます。

The screenshot shows the same 'Infrastructure Manager' interface, but with the 'SDS' tab selected. The breadcrumb trail remains 'ノードリスト > ESXi228_Chassis > ESXi227'. The 'SDS' tab displays a table with fields: プール名 (vSAN Datastore), 種類 (VMware Virtual SAN), バージョン (6.0.0 3825889), クラスタ名 (TestCluster65new), and クラスタの種類 (VMware vSAN Cluster).

「プール名」を選択すると、仮想リソースの詳細画面が表示されます。

6.3 サーバのファームウェアをアップデートする

ISMに登録したサーバのファームウェアをアップデートします。

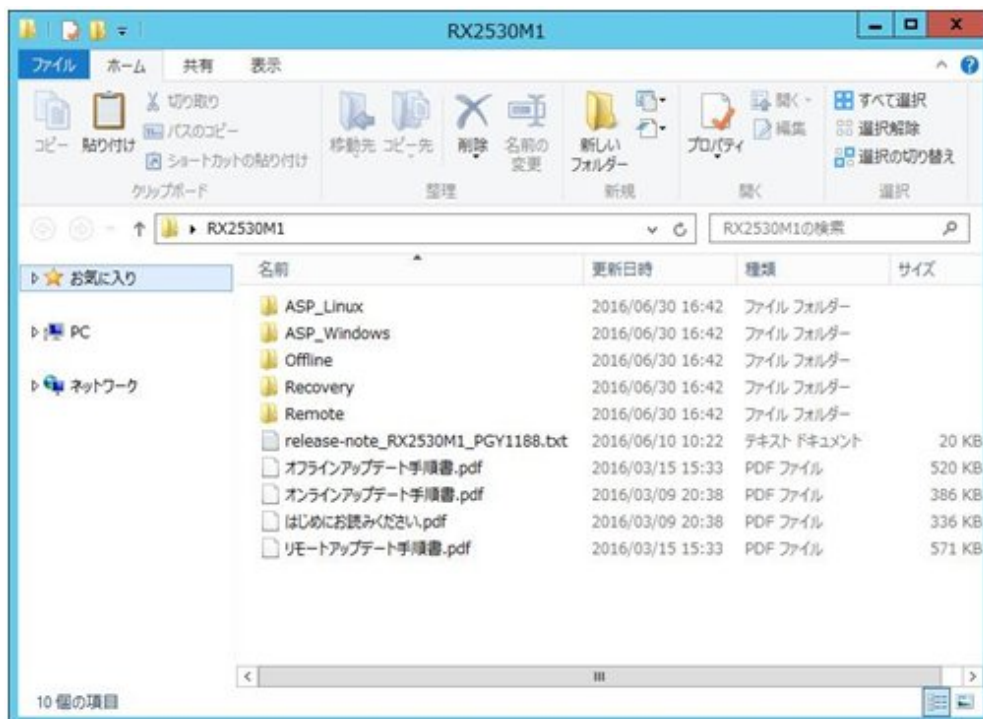
1. アップデートするファームウェアデータがインポートされていない場合は、最初にインポートを行います。インポート済みの場合は手順7へ進みます。

2. WebサイトからiRMC/BIOSのファームウェアをダウンロードします。

以下のサイトから対象モデルのファームウェアをダウンロードしてください。

<http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/>

3. 任意のフォルダーにダウンロードしたファイルを格納します。ダウンロードしたファイルが圧縮ファイルの場合は、フォルダー内で展開を行ってください。



4. ダウンロードしたファイルを格納したフォルダーをzip形式に圧縮します。

5. ファームウェアをインポートします。

ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア]選択し、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「ローカル」を選択し、画面表示に従い、[ファイル]、[種類]、[モデル]、[バージョン]を入力して[適用]ボタンを選択します。

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。

表6.1 入力バージョン

種類	モデル	バージョン入力方法
iRMC	RX100 S8,CX2550 M1など	リリースノートを参照して、iRMCのバージョンとSDRのバージョンを指定してください。
BIOS	RX100 S8,CX2550 M1など	リリースノートを参照して、BIOSバージョンを指定してください。

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。

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」画面にタスクの一覧が表示されます。

6. ファームウェアがインポートされたことを確認します。

ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア]を選択し、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」画面が表示されます。

画面右側で[ファームウェアデータ]タブを選択します。

インポートを行ったファームウェアが一覧に表示されることを確認してください。

7. 対象サーバを選択します。

「ファームウェア」画面でファームウェアアップデートを行うノードにチェックを付けます。

(現行バージョンより新しい版数のファームウェアデータがインポートされ、最新バージョン欄にそのファームウェアの版数が表示されている状態でないとチェックができないようになっています。)

[アクション]ボタンから[ファームウェア更新]を選択し、[ファームウェアアップデート]ウィザードを表示します。

8. ファームウェアアップデートを開始します。

[ファームウェアアップデート]ウィザードに従い、設定項目を入力します。

設定項目の入力は、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

ファームウェアアップデートの開始後、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。

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」画面にタスクの一覧が表示されます。

9. BIOS、PCIカードのオンラインファームウェアアップデートの場合、対象サーバを再起動します。

10. 対象サーバのファームウェアバージョンが上がったことを確認します。

ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア]を選択し、「ファームウェア」画面を表示します。

ファームウェアアップデートを行った機器のノード名を選択し、「ノード情報」画面内の[ノード情報取得]からノード情報取得を行います。

「ファームウェア」画面にアップデート後のバージョンが表示されます。

以上でサーバのファームウェアアップデートは完了です。

ポイント

.....
事前にノードにタグを設定しておくことで、「ノードリスト」画面でタグによるノードのフィルタリングを行えます。ノードをフィルタリングすることで対象のノードを抽出しやすくなります。
.....

6.4 電力制御を行う

ISMでは、消費電力の上限目標値をラックごとに設定することで、搭載された機器の消費電力を抑えることができます。

消費電力の上限目標値は、電力制御ポリシー（運用パターンに応じた定義）ごとに設定できます。

電力制御ポリシーは、2種類のカスタム定義と、スケジュール運用のための定義、最低消費電力運用（ミニマム）の定義の計4種類を切り替えて運用できます。

電力制御の運用を行うには、事前に[電力制御設定追加]（電力制御対象のノードの情報と、電力制御ポリシーの設定の定義）を行い、電力制御ポリシーを有効化する必要があります。

注意

.....
電力制御の設定は、ラックごとに管理されます。以下のタイミングには、関係するラックに対する電力制御設定（ノード電力設定、電力制御ポリシーの上限値）を見直す必要があります。
.....

- ・ ノードをラックに対して追加する
 - ・ ノードをラックから撤去する
 - ・ ノードを別のラックに移動する
-

6.4.1 現在の電力制御の状態を確認する

対象のラックに対する電力制御の状態を確認します。

1. 「データセンターリスト」画面で、電力制御設定の状態を確認するラックを選択します。
2. ラック詳細画面右上の電力制御設定ステータスの表示内容を確認します。

表6.2 電力制御設定ステータス

電力制御設定ステータス	説明
電力制御未設定	電力制御が設定されていません。
電力制御停止中	電力制御が設定されていますが、すべての電力制御ポリシーが無効となっています。 有効化するには[アクション]ボタンを選択し、[電力制御の有効/無効]を選択します。
電力制御中	電力制御が設定され、1つ以上の電力制御ポリシーが有効となっています。
電力制御更新中	電力制御の設定更新中です。
電力制御差分有	電力制御の設定後にノードの追加または削除が行われています。 追加された機器のノード電力設定を入力し、電力制御ポリシーの上限値を見直す必要があります。

6.4.2 ラックの電力制御設定を追加／編集する

対象のラックに対する電力制御の定義について登録、または編集を行います。

1. 「データセンターリスト」画面で、電力制御設定を追加、または編集するラックを選択します。
2. [アクション]ボタンから以下を選択します。
 - － 新たに電力制御設定を追加する場合:[電力制御設定追加]
 - － すでに設定されている電力制御設定を編集する場合:[電力制御設定編集]

表示内容、および設定内容は、以下のとおりです。

ラックの消費電力欄

現在の電力制御の状態値が表示されます。

表6.3 ラックの消費電力欄

項目	説明
現在のステータス	最新の電力制御設定ステータスが表示されます。
現在有効になっているポリシー	[電力制御の有効/無効]で有効状態になっている電力制御ポリシーが表示されます。
最大消費電力	現在ノード電力設定で入力されている最大消費電力の合計値が表示されます。
固定電力値	入力した固定電力の合計値(電力制御対象としない機器の最大消費電力の合計値)が表示されます。
消費電力	電力制御ができる機器(主にサーバ)と電力制御対象としない機器の最大消費電力の現在の消費電力の合計値が表示されます。

[ノード電力設定]タブ

電力制御に使用するノードごとの設定値を入力します。

表6.4 [ノード電力設定]タブ

項目	説明
ノードタイプ	ノードごとのタイプです。
ノード名	ノードごとの名称です。
固定電力	入力した最大消費電力の値を、固定値として利用します。 固定電力として扱う場合はチェックします。

項目	説明
	消費電力値が取得できない機器の場合は、自動的に有効になります。
最大消費電力	カタログスペックとしての最大消費電力値を入力します。 ノードの電力制御可能な範囲として内部計算する際に使用されます。電力制御ができない機器は、常に当該電力値が固定的に使用される前提として計算します。
消費電力	ノードから取得した現在の消費電力値が表示されます。
業務優先度	<ul style="list-style-type: none"> • Low 電力の上限に達した場合、最初に電力制御の対象とします。 • Middle Lowの機器の電力を制御しただけでは不十分な場合に、電力制御の対象とします。 • High Low、Middleの電力を制御しただけでは不十分な場合に、電力制御の対象とします。 • Critical 電力制御の対象外とします。 ただし、ミニマムポリシーが有効化された場合は、電力制御の対象とします。

[電力制御ポリシー]タブ

3種類の電力制御ポリシーについて、設定値を登録します。

消費電力の上限目標について、2種類のカスタムポリシーの上限値と、スケジュールポリシーでの上限値およびスケジュールを設定できます。

表6.5 [電力制御ポリシー]タブ

項目	説明
電力制御ポリシー	
カスタム1,2	指定した上限値の消費電力で運用します。
スケジュール	スケジュールポリシーが有効な場合、指定したスケジュール(曜日、時間帯)の間、指定した上限値の消費電力で運用します。
ミニマム	業務優先度がCriticalの機器も含め、最低限の消費電力で運用します。
表示値	
上限値	ポリシーごとの上限目標値を入力します。
固定値	電力制御対象外の機器の最大電力合計値です。
有効/無効	電力制御ポリシーの状態が表示されます。
スケジュール詳細設定	
終日	運用時間を指定しない場合にチェックします。
時間を指定する	開始時間、終了時間を設定する場合にチェックします。 <ul style="list-style-type: none"> • 開始時間 電力制御のスケジュール運用を開始する時刻を設定します。ISM-VAのタイムゾーンでの値を設定します。 • 終了時間 電力制御のスケジュール運用を終了する時刻を設定します。ISM-VAのタイムゾーンでの値を設定します。
曜日	電力制御のスケジュール運用を行う曜日をチェックします。 複数の曜日を選択できます。

注意

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が実施されますが、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。

ポイント

以下の例のように設定した場合は、ISM-VAのタイムゾーンにおける日曜日の23:00から月曜日の5:00までがスケジュールされます。

設定例:

- 開始時刻:23:00
- 終了時刻:5:00
- 曜日:日曜

6.4.3 ラックの電力制御ポリシーを有効化する

対象のラックに対する電力制御ポリシーを有効化します。

1. 「データセンターリスト」画面で、電力制御設定のポリシーを有効化するラックを選択します。
2. [アクション]ボタンから[電力制御の有効/無効]を選択します。
3. 有効化する電力制御ポリシーの行の[有効/無効]-[変更後]を[有効]に設定して、[適用]を選択します。

表示内容は、以下のとおりです。

表6.6 「電力制御の有効/無効」画面の表示内容

項目	説明
ポリシー名	電力制御ポリシーの名称です。 カスタム1、カスタム2、スケジュール、ミニマムの4種類があります。
上限値	電力制御設定で入力したポリシーごとの上限目標値です。
固定値	電力制御対象外の機器の最大電力合計値です。
有効/無効	電力制御ポリシーの状態が表示されます。

注意

- 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は最優先で実行します。その際、電力制御設定の[ノード電力設定]の業務優先度がCriticalの機器も含めて最小の消費電力に抑えるように運用します。
- ミニマム以外の複数の電力制御ポリシーが有効化された場合、消費電力の上限値が最も低いポリシーを実行します。

6.4.4 ラックの電力制御設定を削除する

対象のラックに対する電力制御の設定情報をすべて削除します。

1. 「データセンターリスト」画面で、電力制御設定を削除するラックを選択します。
2. [アクション]ボタンから[電力制御設定削除]を選択します。
3. 設定を削除するラックであることを確認し、[削除]ボタンを選択します。

6.5 ファームウェアをローリングアップデートする

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

仮想化基盤の運用開始後に、ISM for PRIMEFLEXの機能を利用してファームウェアをローリングアップデートする手順について説明します。

作業を開始する前に以下を確認してください。

- ・ 適用するファームウェアの入手
- ・ ファームウェアアップデート対象ノードの選定
- ・ 仮想マシン退避用空きノードの選定
- ・ 設定ファイル編集内容の確認

6.5.1 ファームウェアローリングアップデート機能の動作要件

すべての構成で共通の動作要件

- ・ 事前に設定ファイルを編集する必要があります。
- ・ 適用するファームウェアは、ISMに登録済みの最新ファームウェアを利用します。事前にISMへファームウェアをアップロード/インポートしてください。
- ・ BIOSおよびiRMCのOnlineアップデートのファームウェアのみ対応しています。
- ・ 仮想リソース管理機能を使用します。仮想リソースを使用するための設定は、『ユーザーズマニュアル』の「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。
- ・ 処理の始めにクラスタのステータスとノードのステータスが確認されます。異常が発生している場合には、データが保証できないため、ファームウェアローリングアップデートは実行されません。
- ・ ファームウェアローリングアップデート機能は、アップデート対象サーバ上で動作している仮想マシンを一時的に空きサーバへ移行します。アップデート対象サーバを再起動後、一時的に空きサーバへ移行した仮想マシンをアップデート対象サーバへ戻します。他ノード上の仮想マシンを移行して動作させるのに十分な資源(CPU性能、メモリ容量など)のあるサーバを空きサーバに指定してください。空きサーバは、「6.5.2 設定ファイルを編集する」の設定ファイルの「temporary_ism_node_name」オプションに指定します。
- ・ ISM-VAのworkflowサービスが起動している必要があります。

PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成のみの動作要件

- ・ ファームウェアローリングアップデートを実行する前に、クラスタとノードのステータスに異常がないか確認してください。
 - ー クラスタ
PRIMEFLEXのvCSAにvSphere Web Clientでアクセスして、[ホストおよびクラスタ]のナビゲーション内のクラスタ名に警告やエラーのアイコンがないことを確認してください。
 - ー ノード
ISMにログインして、[管理]-[ノード]の「ノードリスト」画面のステータスが「Normal」であることを確認してください。
- ・ 4台以上の正常なノードで構成してください。3台以下の構成ではファームウェアローリングアップデート機能は使用できません(強制実行オプションが有効の場合も同様です)。
- ・ ISMの仮想化管理ソフトウェアにPRIMEFLEXのvCSAが登録されている必要があります。
- ・ VMware Distributed Resource Scheduler (以降、「DRS」と表記)機能がオンのとき、VMware Host Clientでログインして、[ホーム]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSphere DRS]の[編集]からVMware DRSの自動化レベルを設定できますが、自動化レベルを「完全自動化」以外に設定すると、エラー終了してしまう可能性があります。自動化レベルは、必ず「完全自動化」に設定してください。DRS機能がオンของときは、空きサーバの準備は不要です。

PRIMEFLEX for Microsoft Storage Spaces Direct構成のみの動作要件

- ファームウェアローリングアップデートを実行する前に、クラスタとノードのステータスに異常がないか確認してください。
 - クラスタ
クラスタ代表IP(クラスタアクセスポイント)にリモートデスクトップ接続してフェイルオーバークラスタマネージャーを開き、[<クラスタ名>]のクラスイベント内に警告やエラーがないこと、[<クラスタ名>]-[記憶域]-[プール]-[<プール名>]-[仮想ディスク]の正常性状態が「正常」であることを確認してください。
 - ノード
ISMにログインして、[管理]-[ノード]の「ノードリスト」画面のステータスが「Normal」であることを確認してください。
- 仮想ディスクの「正常性の状態」が正常になっている必要があります。フェイルオーバークラスタマネージャーで[記憶域]-[プール]-[プール名]を選択し、画面下の[仮想ディスク]タブを選択すると、仮想ディスクの「正常性の状態」を確認できます。
- 3台以上の正常なノードで構成してください。2台以下の構成ではファームウェアローリングアップデート機能は使用できません(強制実行オプションが有効の場合も同様です)。
- ISMの仮想化管理ソフトウェアにPRIMEFLEXのフェイルオーバークラスタが登録されている必要があります。
- ISMの仮想化管理ソフトウェアに対象のMicrosoft Failover Clusterを登録してください。System Centerの登録も可能ですが、ファームウェアローリングアップデート機能では使用されません。
- 設定ファイルで指定するクラスタ名は、対象のMicrosoft Failover Clusterのクラスタ名を指定してください。
- 仮想マシンの移動は高可用性仮想マシンだけをサポートします。仮想マシンと仮想ハードディスクを格納する場所として共有記憶域を選択すると、高可用性仮想マシンを構成できます。

注意

- iRMCのファームウェアアップデートは、ノードの再起動が不要です。設定ファイルの動作モード(operation_mode)を「UpdateOnly」に設定することで、再起動しない設定ができます。
- BIOSファームウェアアップデートは、ノードの再起動が必要です。設定ファイルの動作モードの設定は不要です(初期値=UpdateAndReboot)。
- ネットワーク構成やVMware DRSアフィニティールールなどの関係で、他ノードへ移動できない仮想マシンを実行しているノードは、ファームウェアローリングアップデートを実施する前に、仮想マシンを手動で停止させる必要があります。
- また、VMware DRS機能がない場合、ライセンスの関係で他ノードに移動してはいけない仮想マシンが存在していたとしても、その仮想マシンはノード再起動の際に別のノードに移動してしまいます。移動を防ぐため、その仮想マシンが実行しているノードを再起動しないように設定ファイルで指定して、ライセンス違反にならないようにしてください。
- PRIMEFLEX for Microsoft Storage Spaces Direct構成では、ADVMがローカルディスク(Storage Spaces Direct外)に作成されているため、Live Migrationできません。よって、ADVMが存在するノードを再起動対象にする場合は、ADVMを事前にシャットダウンさせてください。
- PRIMEFLEX for Microsoft Storage Spaces Direct構成では、ファームウェアローリングアップデート機能の実行中にCPU Internal Error (CPU IERR)などのハードエラーが発生した場合、すべての仮想マシンがフェイルオーバーする可能性があります。

6.5.2 設定ファイルを編集する

ファームウェアローリングアップデート機能の動作を記述するXML形式の設定ファイル「fwup.conf.xml」を編集します。

設定ファイル保存先

設定ファイルは、以下に保存されています。

/Administrator/ftp/workflow/config/live/FISCRB/DAN/fwup/fwup.conf.xml

設定ファイル例

設定ファイルの参考例は、以下のとおりです。

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
Copyright FUJITSU LIMITED 2016
fwup.conf.xml

$Rev: 5392 $ ($Date:: 2016-11-02 14:22:03 +0900#$ $Author: kubo $)

firmware update configuration file
-->

<fwup_config> [注1]
  <common_config> [注1]
    <!-- <forcing>True</forcing> --> [注2]
  </common_config>

  <target_config> [注1]
    <cluster> [注1]
      <cluster_name>cluster1</cluster_name>
      <cluster_option> [注1]
        <!-- <update_all_node>True</update_all_node> --> [注2]
        <!-- <operation_mode>UpdateOnly</operation_mode> --> [注2]
      </cluster_option>

      <temporary_node>
        <temporary_ism_node_name>node4</temporary_ism_node_name>
      </temporary_node>

      <node> [注3]
        <ism_node_name>node1</ism_node_name>
        <!-- Please set to RebootNo If there is a VM not to migrate -->
        <node_type>RebootNo</node_type>
      </node>

      <node> [注3]
        <ism_node_name>node2</ism_node_name>
        <!-- Please set to RebootNo If there is a VM not to migrate -->
        <node_type>RebootNo</node_type>
      </node>

      <node> [注3]
        <ism_node_name>node3</ism_node_name>
        <node_option>
          <!-- <integrity_mode>accessibility</integrity_mode> --> [注2]
        </node_option>
      </node>

      <node> [注3]
        <ism_node_name>node4</ism_node_name>
      </node>

    <!--
      <node> [注3]
        <ism_node_name>node5</ism_node_name>
      </node>
    --> [注2]
  </cluster>
</target_config>
</fwup_config>

```

[注1]: コメントアウトしないでください。

[注2]: <!-- -->を削除するとオプションが有効になります。コメントアウトしている場合は、「[設定ファイルで指定するオプション](#)」に記載された初期値が有効になります。


[注3]:お客様のクラスタ構成によって、<node></node>タグを追加、または削除してください。

設定ファイルで指定するオプション

設定ファイルで指定するオプションは、以下のとおりです。

ポイント

"cluster_name"以外のオプションは、コメントアウトできます。"cluster_name"は、コメントアウトしないでください。

オプション	値	説明
operation_mode*	<ul style="list-style-type: none">UpdateOnlyUpdateAndReboot (初期値)	動作モード <ul style="list-style-type: none">UpdateOnly: ファームウェアのアップデート後、再起動しません。UpdateAndReboot: ファームウェアのアップデート後、変更を有効にするため再起動します。
forcing*	<ul style="list-style-type: none">TrueFalse (初期値)	強制実行オプション <ul style="list-style-type: none">True: クラスタ内に障害が発生したノードがあっても強制実行します。False: 強制実行しません。 <p>Trueに設定した場合、ノード異常が発生してデータが保証されないケースでも、ファームウェアローリングアップデート処理が実行されます。クラスタ内に異常が発生しているノードが存在する場合は、データが失われる可能性があります。</p> <p>Falseに設定した場合、ノード異常が検出されると、ファームウェアローリングアップデート処理が中止されます。</p> <div> 注意</div> <p>クラスタ内の正常なノード数がファームウェアローリングアップデート機能の動作要件の規定値 (PRIMEFLEX HS V1.0/V1.1 / PRIMEFLEX for VMware vSAN V1版では4台以上、PRIMEFLEX for Microsoft Storage Spaces Direct版では3台以上) を満たしていない場合は、本オプションがTrueでも強制実行されません。</p>
cluster_name	クラスタ名	ファームウェアアップデート対象のクラスタ名 対象クラスタは、1つしか指定できません。 PRIMEFLEX for Microsoft Storage Spaces Direct版では、Microsoft Failover Clusterのクラスタ名を指定してください。
update_all_node*	<ul style="list-style-type: none">TrueFalse (初期値)	全ノード実行オプション <ul style="list-style-type: none">True: クラスタ内の全ノードに対して、ファームウェアアップデートが実行されます。False: <node>要素で指定したノードを対象としてファームウェアアップデートが実行されます。

オプション	値	説明
temporary_ism_node_name	ISMに登録されているノード名	ISMの[管理]-[ノード]の「ノードリスト」画面に表示される退避先ノードの「ノード名」 ISMの「ノード名」欄に登録されている値と合わせる必要があります。 PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版でVMware DRS機能なしの場合、およびPRIMEFLEX for Microsoft Storage Spaces Direct版でSCVMMなしの場合に必要なオプションです。本オプションを省略すると、アップデートが中止されます。
ism_node_name	ISMに登録されているノード名	ISMの[管理]-[ノード]の「ノードリスト」画面に表示されるファームウェアアップデート対象ノードの「ノード名」 ISMの「ノード名」欄に登録されている値と合わせる必要があります。
node_type	<ul style="list-style-type: none"> RebootNo RebootYes(初期値) 	ファームウェアアップデート対象ノードのノード種別 <ul style="list-style-type: none"> RebootNo: operation_mode=UpdateAndRebootを指定した場合に再起動しないノードを指定します。 RebootYes: operation_mode=UpdateAndRebootを指定した場合に再起動するノードを指定します。
integrity_mode*	<ul style="list-style-type: none"> accessibility copy_all(初期値) none 	メンテナンスモード移行時の退避モード <ul style="list-style-type: none"> accessibility: アクセシビリティの確保 copy_all: 全データの移行 none: データの移行なし <p>PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版でのみ有効なオプションです。PRIMEFLEX for Microsoft Storage Spaces Direct版では、本オプションは無視されます。</p>



注意

- オプション名のうしろに*があるオプションは、デフォルトでは<!-- -->でコメントアウトされています。ご使用になる際は、コメントアウトを外してご使用ください。

設定例) メンテナンスモード移行時の退避モードを「全データの移行」にしたい場合

integrity_modeに「copy_all」を指定します。

```
<node>
  <ism_node_name>node3</ism_node_name>
  <node_option>
    <integrity_mode>copy_all</integrity_mode>
  </node_option>
</node>
```

- ファームウェアアップデートの対象がiRMCだけの場合、サーバの再起動は不要です。「operation_mode」オプションを「UpdateOnly」に指定してください。「UpdateAndReboot」を指定した場合、iRMCだけのファームウェアアップデートでもサーバの再起動が実行されます。
- マニュアルに記載のないオプションは、編集不要です。

- XML形式の設定ファイルでは、<!-- -->でコメントをネストしないでください。コメントをネストさせると、エラー終了してしまいます。

設定例)コメントをネストさせた場合

```
<!--
  <node>
    <ism_node_name>hv-host4</ism_node_name>
    <node_option>
      <!-- <integrity_mode>accessibility</integrity_mode> -->
      <!-- <move_within_cluster>True</move_within_cluster> -->
    </node_option>
  </node>
-->
```

設定例)コメントをネストさせない場合

```
<!--
  <node>
    <ism_node_name>hv-host4</ism_node_name>
    <node_option>
      <integrity_mode>accessibility</integrity_mode>
      <move_within_cluster>True</move_within_cluster>
    </node_option>
  </node>
-->
```

設定ファイルの編集手順

設定ファイルの編集手順は、以下のとおりです。

1. 管理端末からFTPクライアントを使用して、administratorユーザーとしてISM-VAへログインします。
2. 設定ファイルをISM-VAから管理端末へダウンロードします。
3. 設定ファイルを編集します。
4. 管理端末からFTPクライアントを使用して、administratorユーザーとしてISM-VAへログインします。
5. 設定ファイルを再度ISM-VAへアップロードします。

ポイント

設定ファイルのダウンロードとアップロード方法は、「[8.1.3 ISMをリストアする](#)」を参照してください。

6.5.3 ファームウェアローリングアップデートを実施する

必要な事前準備が整ったら、ファームウェアローリングアップデートを実施します。

1. 適用するファームウェアを事前にISMへインポートします。
インポートの手順は、「[6.3 サーバのファームウェアをアップデートする](#)」を参照してください。
2. 「[6.5.2 設定ファイルを編集する](#)」を参照して設定ファイル編集手順を実施します。
3. Administrator権限を持ったユーザーでISMにログインします。

ポイント

Administrator権限を持ったユーザーとは

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]-[ユーザーグループ]のユーザーグループリスト画面に表示される「管理対象ノード」が「全てのノードを管理」に設定されているユーザーグループのAdministrator権限を持ったユーザーを表します。

4. [構築]-[ジョブ]を選択します。
5. ジョブリストから「Firmware Rolling Update」を選択し、表示された画面で[実行]ボタンを選択します。



6. 「ジョブの実行の確認」画面でISMのパスワードを入力し、[実行]ボタンを選択します。
ジョブが開始されます。

The screenshot shows a modal dialog titled 'ジョブの実行の確認' (Confirm Job Execution). The dialog contains the text 'Firmware Rolling Update を実行します。よろしいですか？' (Execute Firmware Rolling Update. Is it okay?). Below this, there are two input fields: 'ユーザー名' (Username) with the value 'pfadmin' and 'パスワード*' (Password*) with an empty field. At the bottom, there are two buttons: '実行' (Execute) and 'キャンセル' (Cancel).

注意

- ファームウェアローリングアップデート機能を利用する際は、ISM-VA上でworkflowサービスを起動している必要があります。
ISM-VAにSSH接続して、以下のコマンドで状態を確認してください。

```
# ismadm service status workflow
```

起動していなければ以下のコマンドを実行して起動してください。

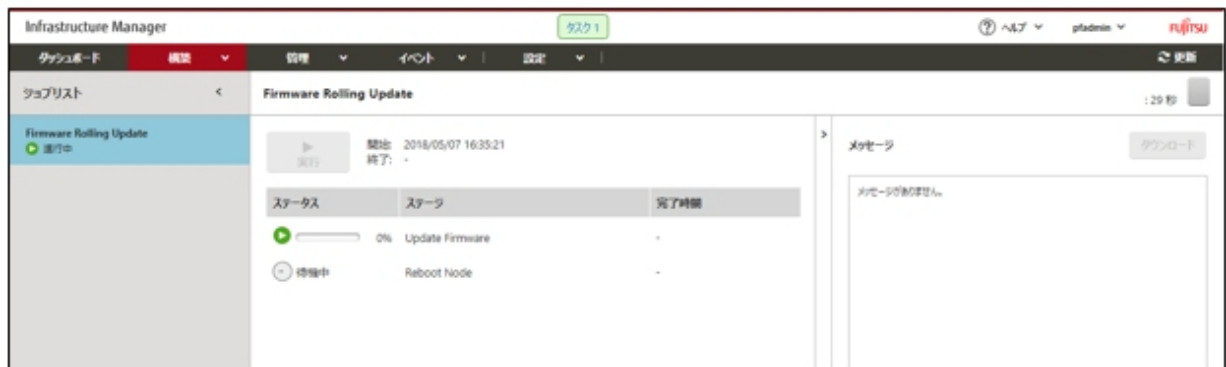
```
# ismadm service start workflow
# ismadm service enable workflow
```

- ISM-VA上でISMのサービスおよびworkflowサービスを停止しないでください。

```
# ismadm service stop ism
# ismadm service stop workflow
```

ー ジョブの実行中は途中終了できません。

ファームウェアローリングアップデート機能の実行中は、ISMの「ジョブ」画面に進捗状況が表示されます。



7. ファームウェアローリングアップデート機能が正常に完了したら、ISMの「ジョブ」画面の右側に表示されたメッセージを確認します。
ファームウェアローリングアップデート機能を実行していた時間に出力されたメッセージを確認してください。

重要度が「警告」のメッセージが出力された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して問題を解決し、必要であればジョブを再実行してください。

また、ISMの「ジョブ」画面の「ジョブリスト」欄で「Firmware Rolling Update」ジョブにエラーが表示された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して問題を解決し、ジョブを再実行してください。

「ジョブ」画面で対象ジョブを選択し、[ダウンロード]ボタンを選択すると、管理端末へログファイルをダウンロードできます。

8. 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。

表示される「タスク」画面を確認します。

- 「タスク」画面のタスクリストからタスクタイプが「Updating firmware」のタスクIDを選択します。
- サブタスクリストのタスクの結果がすべて「Success」になっていることを確認します。
すべて「Success」の場合、手順9に進んでください。
- タスクの結果が「Error」になっている場合、『ユーザーズマニュアル』の「付録Cトラブルシューティング」を参照して問題を解決します。
その後、以下のどちらかの操作を行います。
 - 設定ファイルを編集して、ジョブを再実行する。
 - 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、画面左側のメニューから[アップデート]を選択する。
表示される「ノードリスト」画面から対象のファームウェアを選択して、[アクション]ボタンから[ファームウェア更新]を選択する。

9. 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、画面左側のメニューから[アップデート]を選択します。

表示される「ノードリスト」画面を確認します。

- 表示される「ノードリスト」画面から、アップデート対象ノードの現行バージョンを確認して、ファームウェアが適用されていること確認します。
すべてのファームウェアが適用されている場合、手順10に進んでください。
- ファームウェアが適用されていない対象ノードがある場合、『ユーザーズマニュアル』の「付録Cトラブルシューティング」を参照して問題を解決します。
その後、以下のどちらかの操作を行います。
 - 設定ファイルを編集して、ジョブを再実行する。

- 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、画面左側のメニューから[アップデート]を選択する。

表示される「ノードリスト」画面から対象のファームウェアを選択して、[アクション]ボタンから[ファームウェア更新]を選択する。

- 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]を選択して表示される「クラスタリスト」画面を確認します。
クラスタの状態とクラスタを構成しているノードの状態に異常がある場合は、保守資料を採取して、当社技術員に連絡してください。
- ファームウェア (BIOS) のアップデートは、ノードの再起動が必要です。設定ファイルの動作モード (operation_mode) に「UpdateOnly」、またはファームウェアアップデート対象ノードのノード種別 (node_type) に「RebootNo」を設定している場合、任意のタイミングでノードを再起動します。
ノードの再起動が正常に完了したら、手順10を実施して「クラスタリスト」画面を確認してください。
- iRMCにログインして、システムイベントログにエラーが出力されていないことを確認します。

注意

- ファームウェアローリングアップデート機能がエラー終了した場合、問題の特定を支援する情報がログへ出力されます。問題を解決したうえで、ファームウェアローリングアップデート処理を再実行してください。
- BIOSのファームウェアローリングアップデート実施中にエラー終了した場合、対象ノードは再起動待ち状態の可能性があります。その状態で、再度ジョブを実行するとエラー終了します。再起動待ち状態かどうかの確認は、以下の画面にアップデート続行のためにシステム再起動が必要である旨のメッセージが表示されているかどうかで確認できます。メッセージが表示されている場合は、手動で再起動を実施してアップデートを完了させてください。

ー PRIMERGY M2シリーズの場合

iRMCの[BIOS]-[BIOSアップデート]の画面

ー PRIMERGY M4シリーズの場合

iRMCの[ツール]-[アップデート]-[BIOSアップデート]の画面

- ノードの再起動中でネットワーク接続不可状態のときにISMがそのノードに対して情報取得をした場合、ステータスやその他の情報が取得できずアラームが検出されることがあります。完了後、ISMの[管理]-[ノード]の「ノードリスト」画面のノードにアラーム(警告/エラー)が表示される場合は、そのノードの運用ログを確認してください。ステータスやその他の情報の取得に失敗しているログの場合は問題ありません。アラームを解除してください。
- ファームウェアローリングアップデート実施中に、ISM-VAが存在するサーバに異常が発生しISM-VAが再起動した場合、ファームウェアローリングアップデートの処理が再開できなくなることがあります。その場合は、以下の対処を実施してください。

ファイルのダウンロードとアップロード方法は、「[6.3 サーバのファームウェアをアップデートする](#)」を参照し、本環境に読み替えて実施してください。

- 管理端末からFTPクライアントを使用して、administratorでISM-VAへログインします。
- 以下の3ファイルをISM-VAから管理端末へダウンロードします。

- /Administrator/ftp/workflow/joblaunch/status_fwup.json
- /Administrator/ftp/workflow/joblaunch/progress1_fwup.json
- /Administrator/ftp/workflow/joblaunch/progress2_fwup.json

- 各ファイルの設定値を以下のように変更します。

status_fwup.jsonの場合

```
{
  "status": "",
  "startTime": "",
  "endTime": ""
}
```

progress1_fwup.json、およびprogress2_fwup.jsonの場合

```
{
  "status": "",
  "progress": 0,
  "time": ""
}
```

4. 再度ファイルをISM-VAへアップロードします。

- PRIMEFLEX for Microsoft Storage Spaces Direct版で、ファームウェアローリングアップデートの完了後、フェイルオーバークラスターマネージャーの[<クラスタ名>]のクラスタイイベント内に警告が表示される場合は、イベントIDとイベントの詳細を確認してください。以下の内容の場合は、一時的な警告のため問題ありません。右ペインの[最新のイベントの再設定]を実行してください。

イベントID	イベントの詳細
5120	クラスタの共有ボリューム'Volume1'(クラスタ仮想ディスク(Vdisk))は'STATUS_DEVICE_NOT_CONNECTED(c000009d)'が原因で一時停止状態になりました。ボリュームへのパスが再確立されるまで、すべてのI/Oは一時的にキューに登録されます。

6.6 PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版 クラスタを作成する

PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1でのクラスタ作成手順について説明します。

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ作成は、以下の作業フローで行います。

表6.7 クラスタ作成フロー

クラスタ作成手順		作業内容
1	事前準備	<ul style="list-style-type: none"> • ADVMの証明書作成 • DNSへホストレコード登録 • DHCPの設定 • OSインストール媒体のISOイメージをISM-VAへインポート • VMware ESXiパッチのアップロード • VMware SMIS Providerのアップロード • プロファイルの作成 • 設置と結線 • iRMCのIPアドレス設定 • BIOSの設定 • ISMへノード登録
2	クラスタ作成の実行	
3	事後処理	<ul style="list-style-type: none"> • 作成されたクラスタの確認 • vCenter Serverの検知アラーム設定 • VMware vSphereの制限事項／注意事項 • ServerView RAID Managerへの登録 • 証明書削除

6.6.1 事前準備

クラスタ作成を行う前の準備作業について説明します。

6.6.1.1 ADVMの証明書を作成する

本設定は、PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1専用ADVM構成時、かつクラスタ作成機能の初回使用時に必要な作業です。クラスタ拡張機能をすでに実行している場合には不要です。

クラスタ作成機能は、ISMからADVMに対してSSL暗号化通信で設定を行うため、証明書の登録が必要です。

ADVM#1とADVM#2に対して、以下の流れでSSL通信用の証明書登録と通信を許可するための設定を行ってください。

なお、SSL暗号化通信せずにクラスタ作成機能を使用することも可能です。その場合、本設定は不要です。

「6.6.1.2 DNSへホストレコードを登録する」に進んでください。



- SSL暗号化通信を使用しないでクラスタ作成機能を使用する場合は、http通信を使用するため設定パラメーター傍受などのセキュリティリスクがあります。セキュリティリスクを承知できない場合は、本手順を実施して証明書を登録してください。
- SSL暗号化通信の使用有無に応じて、クラスタ定義パラメーターの[クラスタ詳細情報]-[DNS情報]-[WinRMサービスポート番号]配下の項目を以下のとおり設定してください。

SSL暗号化通信の使用有無	設定内容	説明
SSL暗号化通信を使用する	<ul style="list-style-type: none">[通信方式]に「HTTPS」を設定[ポート番号]を入力	ADVMとのWinRM通信をSSLで行う設定にします。
SSL暗号化通信を使用しない	<ul style="list-style-type: none">[通信方式]に「HTTP」を設定[ポート番号]を入力	ADVMとのWinRM通信をSSLで行わない設定にします。

なお、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』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

- リモートデスクトップ接続時にエラーメッセージが表示されて接続できない場合、以下のURLの問題の可能性があります。リモートデスクトップの接続先にHypervisorコンソール画面から共有フォルダーを使用して最新の更新プログラムを転送し、適用してください。

<https://blogs.technet.microsoft.com/askcorejp/2018/05/02/2018-05-rollup-credssp-rdp/>

- 6.6.1.1.1 WinRMサービスの起動を確認する
- 6.6.1.1.2 WinRMサービスを設定する
- 6.6.1.1.3 ファイアウォールのポートを開放する
- 6.6.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する

6.6.1.1.1 WinRMサービスの起動を確認する

ADVM#1から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
```

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
```

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
```



注意

- WinRMサービスは、環境によって自動起動になっていない場合があります。WinRMサービスを自動起動(auto)、または遅延自動起動(delayed-auto)するように設定してください。

以下は、自動起動に設定する場合の例になります。

```
>sc config winrm start=auto
```

- ADVM#1をADVM#2に読み替えてADVM#2に対しても同様にWinRMサービスの起動確認を行ってください。

6.6.1.1.2 WinRMサービスを設定する

(1) WinRMサービスの設定

初期設定ではBasic認証が許可されていないため、「(1-1) Basic認証の許可」を行います。

https通信を使用するためBasic認証の通信は暗号化されます。

ADVM#1から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で実行されています。」と表示されている場合は、すでに設定が完了しているため、「(1-1) Basic認証の許可」に進んでください。

「WinRMは、管理用にこのコンピュータ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。」と表示されている場合は、WinRMサービスは実行されていますがリモートアクセス許可は設定されていないため、「y」を入力します。

WinRM は、管理用にこのコンピュータへのリモート 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。

(1-1) Basic認証の許可

コマンドプロンプトで以下のコマンドを実行し、WinRMサービスの設定を確認します。

```
> winrm get winrm/config
```

以下の結果を確認し、[Config]-[Client]-[Auth]-[Basic]がfalseとなっている場合、以下の手順に進んでください。trueとなっている場合は、すでに設定が完了しているため、「(2) https通信の設定」に進んでください。

```
Config
  MaxEnvelopeSizekb = 150
  MaxTimeoutms = 60000
  MaxBatchItems = 20
  MaxProviderRequests = 25
  Client
    NetworkDelaysms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
  Auth
    Basic = false
```

```
Digest = true
Kerberos = true
Negotiate = true
Certificate = true
DefaultPorts
  HTTP = 80
  HTTPS = 443
```

(以下省略)

以下のコマンドを実行します。

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

(2) 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。証明書は管理端末から作成できます。

(2-1) 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。

- .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>



- 上記ツールは管理端末にインストールしてください。
- 上記URLの.NET Framework 4.5は、証明書を作成するための管理端末の言語に合わせてダウンロードしてください。
- 上記URLのWindows Software Development Kitは、Windows 8.1およびWindows Server 2012以降の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 10以外のプラットフォームでは、Windows 10 SDKを使用する際に、Universal CRTがインストールされている必要があります (KB2999226 (<https://support.microsoft.com/ja-jp/help/2999226/update-for-universal-c-runtime-in-windows>)) を参照)。セットアップ中にエラーが発生しないようにするために、Windows SDKをインストールする前に、推奨される最新の更新プログラムとパッチをMicrosoft Updateから必ずインストールしてください。

(3) 証明書の作成

管理端末から証明書作成ツール(makecert.exe)、個人情報交換ファイル作成ツール(pvk2pfx.exe)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)

(3-1) 証明書、秘密鍵ファイルの作成

管理端末のコマンドプロンプト(管理者)から以下のコマンドを実行します。

対象ADVMのサーバ名を「192.168.10.10」、証明書の有効期間を「2018年3月30日」に設定する場合のコマンド例です。

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -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>
```

途中、証明書にセットするパスワードを2回要求されますので、間違えずに入力してください。間違えた場合は、上記コマンドを実行してやり直してください。

(3-2) サービス証明書の作成

管理端末のコマンドプロンプト(管理者)から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>
```

途中、(3-1)でセットしたパスワードを要求されますので、入力してください。



注意

ADVM#1とADVM#2の2つの証明書を作成してください。

(4) 証明書、サービス証明書の登録

管理端末で作成した証明書、サービス証明書をADVM#1へアップロードします。

証明書スナップインを起動し、(3)で作成した証明書を登録します。

1. ADVM#1でmmc.exeを実行します。
2. [ファイル] - [スナップインの追加と削除]を選択します。
3. [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。
4. 「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。
5. [OK]を選択します。

(5) SSL証明書を登録

ADVM#1の証明書スナップインから以下の手順を行ってください。

1. <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 コンピューター)] - [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、証明書のウィザードインポートを完了します。
2. <証明書のファイル名.cer>を[信頼されたルート証明機関]に登録できたことを確認します。
[コンソールルート] - [証明書(ローカル コンピューター)] - [信頼されたルート証明機関] - [証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバ名となっていること、「目的」が「サーバー認証」となっていることを確認してください。なっていない場合は(5)の手順1を再実施してください。
3. <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 コンピューター)] - [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、証明書のウィザードインポートを完了します。途中、秘密キーのパスワード要求がありますが、何も入力せず空欄のまま[次へ]ボタンを選択してください。



注意

<サービス証明書のファイル名.pfx>ファイルを選択する場合、プルダウンから指定する必要があります。

4. <サービス証明書のファイル名.pfx>を[個人]に登録できたことを確認します。
[コンソールルート] - [証明書(ローカル コンピューター)] - [個人] - [証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバ名となっていること、「目的」が「サーバー認証」となっていることを確認してください。なっていない場合は(5)の手順3を再実施してください。

(6) WinRMサービスへの証明書に記載された拇印を登録

(6-1) 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。

1. ADVM#1のコマンドプロンプトからPowerShellを起動します。
2. 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
```

(6-2) 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＞"}
```

(6-3) 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。返ってこない場合は、「(6-2) WinRMリスナーに証明書に記載された拇印を登録」からやり直してください。

```
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
```



注意

ADVM#1をADVM#2に読み替えて、「[6.6.1.1.2 WinRMサービスを設定する](#)」の(1)、(4)～(6)の手順を実施してください。

6.6.1.1.3 ファイアーウォールのポートを開放する

WinRMサービスがリクエストを受け付けられるように、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。

1. ADVM#1でWindows PowerShellを管理者権限で開きます。
2. 以下のようなコマンドを実行します。

```
>New-NetFirewallRule -DisplayName <ファイアーウォールルール名> -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort <ポート番号>
```

例) ポート番号5986を開放するルールに、「WinRM」という名前を設定します。

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort 5986
```



注意

- ・ファイアーウォールの設定は、環境(OSのバージョンなど)によって異なります。
- ・ADVM#1をADVM#2に読み替えて、ADVM#2に対しても同様に「[6.6.1.1.3 ファイアーウォールのポートを開放する](#)」を行ってください。

6.6.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する

ADVM#1から管理者権限でWindows PowerShellを開いて以下のコマンドを実行し、PowerShellスクリプトの実行ポリシーの設定を確認します。

```
> get-executionpolicy
```

コマンド結果を確認し、「RemoteSigned」となっている場合はすでに設定が完了しているため、「6.6.1.2 DNSへホストレコードを登録する」、または「6.6.1.3 DHCPを設定する」に進んでください。

「RemoteSigned」となっていない場合、以下の手順に進んでください。

1. 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



注意

ADVM#1をADVM#2に読み替えて、ADVM#2に対しても同様に「6.6.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する」を行ってください。

6.6.1.2 DNSへホストレコードを登録する

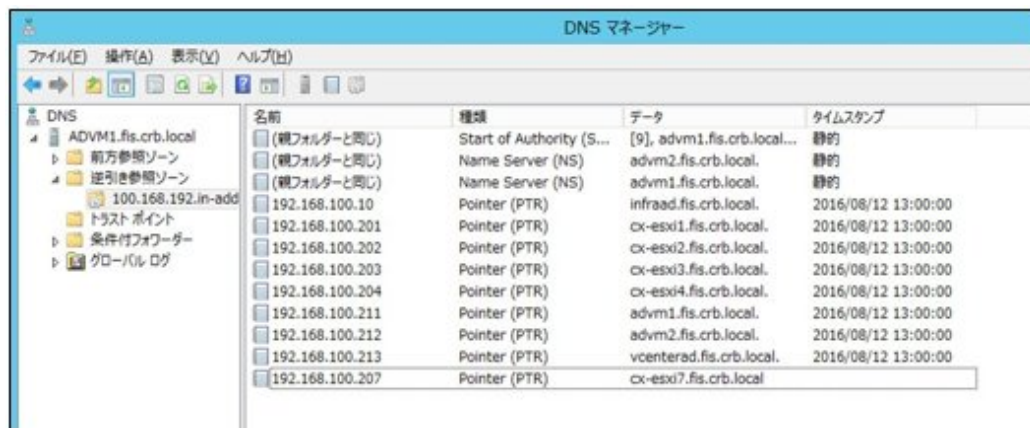
お客様環境のDNSサーバ使用時にのみ必要な作業です。クラスタ作成を実行する前にDNSの前方参照ゾーン、および逆引き参照ゾーンへ新規クラスタを構成するサーバのOSを登録して名前解決を可能にしておく必要があります。

新規クラスタを構成するすべてのサーバに対して実施してください。

図6.1 前方参照ゾーンの登録例



図6.2 逆引き参照ゾーンの登録例



6.6.1.3 DHCPを設定する

クラスタ作成機能では、プロファイル適用を使用してOSのインストール作業を実施します。プロファイル適用によるOSインストールを実行するためには、DHCPサーバが必要です。

ISM-VAは内部でDHCPサーバ機能を持っていますが、ISM-VA外部にDHCPサーバを用意して使用することもできます。内部DHCPを使用する場合は、『ユーザーズマニュアル』の「4.15 ISM-VA内部のDHCPサーバ」を参照して設定してください。

新規クラスタを構成するすべてのサーバの台数分リースできるように設定してください。



注意

- 使用するDHCPサービスが起動していることを確認してください。
- DHCPサーバが同一ネットワーク内で複数起動している場合は、正確に機能しない場合があります。使用しないDHCPサービスは必ず停止してください。
- リース期間は作業中に期限が切れないように設定してください。
- 本製品の構成では、管理ネットワークを冗長しているため、複数ポートにIPアドレスがリースされます。リースするIPアドレスが不足しないように設定してください。
- ISMが内部／外部どちらのDHCPを使用する設定になっているか確認して、お客様が使用するDHCPの設定に合わせて変更してください。変更方法は、『ユーザーズマニュアル』の「4.15.4 DHCPサーバの切替え」を参照してください。

6.6.1.4 OSインストール媒体のISOイメージをISM-VAへインポートする

ISMにServerView Suite DVD Installation (DVD 1)と、OSのインストールメディアをインポートします。

既存のものを使用する場合は、インポートは必要ありません。

インポートの操作については、『ユーザーズマニュアル』の「2.13.2 リポジトリ管理機能」を参照してください。

また、サポート版数は、『プロファイル管理機能 プロファイル設定項目集』を参照してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスク追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。

6.6.1.5 VMware ESXiパッチをアップロードする

クラスタ作成機能でESXiのパッチも適用したい場合に実施してください。ESXiパッチファイルがアップロードされた場合にパッチ適用の処理が実行されます。

既存クラスタのESXiと同じバージョンになるように、お客様環境に応じて作業してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスクの追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。



注意

- VMware ESXiパッチファイルは1つだけとします。複数アップロードした場合には、クラスタ作成は異常終了します。
- アップロードしたESXiパッチファイル(zipファイル)は解凍しないでください。解凍した場合には、クラスタ作成は異常終了します。

1. FTPでISM-VAにアクセスし、適用ファイルを以下にアップロードします。

/Administrator/ftp/kickstart/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

適用ファイルのファイル名はリネームせずにアップロードしてください。

例)

— ESXi650-201704001.zip

6.6.1.6 VMware SMIS Providerをアップロードする

クラスタ作成時に追加するサーバがPRIMERGY M4シリーズおよびVMware ESXi 6.5の場合に、必要な作業です。

VMware SMIS Providerがアップロードされた場合に適用の処理が実行されます。

VMware SMIS Providerのアップロードは、ダウンロードした圧縮ファイル(zipファイル)を解凍した中にある、オフラインバンドルを使用してください。

- ダウンロードした圧縮ファイル(zipファイル)の例:

VMware_MR_SAS_Providers-00.63.V0.05.zip

- オフラインバンドルの例:

VMW-ESX-5.5.0-Isipprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスクの追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。



注意

- VMware SMIS Providerのオフラインバンドルは1つだけとします。複数アップロードした場合には、クラスタ作成は異常終了します。
- アップロードしたVMware SMIS Providerのオフラインバンドル(zipファイル)は解凍しないでください。解凍した場合には、クラスタ作成は異常終了します。

1. FTPでISM-VAにアクセスし、適用ファイルを以下にアップロードします。

/Administrator/ftp/kickstart/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

適用ファイルのファイル名はリネームせずにアップロードしてください。

例)

— VMW-ESX-5.5.0-Isipprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

6.6.1.7 プロファイルを作成する

ISMのプロファイル管理機能を使用して、新規クラスタを構成するサーバのプロファイルを作成します。既存のプロファイルから参照作成して、プロファイルを作成してください。



注意

新規クラスタを構成するすべてのサーバに対してプロファイルを作成してください。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 参照作成元とする既存のプロファイルを選択し、[アクション]ボタンから[参照作成]を選択します。
3. 各項目を設定します。

BIOSポリシー、iRMCポリシーは新規クラスタを構成するサーバに合わせて指定します。

新規クラスタを構成するサーバが既存クラスタ環境のサーバと同じ場合には既存のものを指定します。

プロファイル作成については、「[3.3 サーバに各種設定／OSインストールをする](#)」を参照してください。



注意

- ー 以下の項目には、チェックを付けないでください。
 - [OS]タブの[ネットワーク]の[セットアップ]
 - [OS]タブの[インストール後のスクリプト実行]
 - [OS]タブの[仮想化管理ソフトへの登録]
 - [OS個別情報]タブの[DHCP]
- ー [OS]タブの[管理LANネットワークポート設定]の項目は、以下の設定をしてください。
 - [ネットワークポート指定]にチェックを付けてください。
 - [指定方法]は[MACアドレス]を選択してください。
 - [MACアドレス]は10Gbpsの通信が可能なポート拡張オプションのポート0のMACアドレスを指定してください。
- ー 以下の項目は、重複しないように設定してください。
 - [OS個別情報]タブの[IPアドレス]
 - [OS個別情報]タブの[ネットワーク]-[DHCP]-[コンピュータ名をDNSサーバから取得]-[コンピュータ名]

6.6.1.8 設置と結線を行う

新規クラスタを構成するサーバの設置と結線を行います。詳細は、新規クラスタを構成するサーバの『オペレーティングマニュアル』を参照してください。ネットワークスイッチの設定に関しては、スイッチのマニュアルを参考にして適切に設定してください。

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。新規で作成するクラスタを既存クラスタと別ネットワークに作成する場合は、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。ネットワーク構成に関しては、『ユーザーズマニュアル』の「1.4 構成」も併せて参照してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

ISMのノード登録作業時のノード検出方法に応じて以降の作業順番が異なります。

- ・ ノードを手動検出する場合
「[6.6.1.9 iRMCのIPアドレスを設定する](#)」を実施してください。
- ・ ノードを自動検出する場合
「[6.6.1.11 ISMへノードを登録する](#)」の「自動検出によるノード登録」を実施してください。

6.6.1.9 iRMCのIPアドレスを設定する

新規クラスタを構成するサーバを手動検出でISMにノード登録する場合は、iRMCに固定IPアドレスを設定してください。

新規クラスタを構成するサーバのBIOSを起動して、BIOS設定画面から固定IPアドレスを設定します。この作業を実施するためには、事前に「6.6.1.8 設置と結線を行う」の作業が必要です。また、BIOS画面表示／操作を行うために、新規クラスタを構成するサーバにディスプレイとキーボードを接続してください。

BIOSの起動と、iRMCのIPアドレス設定については、新規クラスタを構成するサーバの「BIOSセットアップユーティリティ」のマニュアルを参考にしてください。

新規クラスタを構成するすべてのサーバに対して設定してください。

また、IPアドレスの設定と同時に「6.6.1.10 BIOSを設定する」も実施してください。

新規クラスタを構成するサーバの「BIOSセットアップユーティリティ」のマニュアルは、以下のサイトから取得できます。

<http://manuals.ts.fujitsu.com/index.php?l=ja>

6.6.1.10 BIOSを設定する

BIOSの設定をします。

「6.6.1.8 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、「6.6.1.9 iRMCのIPアドレスを設定する」と一緒に本項の設定を実施してください。

「6.6.1.8 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。BIOSを起動して、BIOS設定画面で以下を設定してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

表6.8 BIOS設定

項目		設定値
Server Mgmt - iRMC LAN Parameters Configuration [注1]	iRMC IPv6 LAN Stack	Disabled
Management - iRMC LAN Parameters Configuration [注2]		

[注1]:PRIMERGY RX M4シリーズのBIOS画面に表示される項目です。

[注2]:PRIMERGY CX M4シリーズのBIOS画面に表示される項目です。

「6.6.1.8 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、引き続き「6.6.1.11 ISMへノードを登録する」の「手動検出によるノード登録」を実施してください。

「6.6.1.8 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、引き続き「6.6.2 クラスタ作成を実行する」を実施してください。

6.6.1.11 ISMへノードを登録する

ISMを使用してOSをインストールするために、新規クラスタを構成するサーバをISMに登録します。

ISMへのノード登録には手動検出機能と自動検出機能が使用できます。

新規クラスタを構成するすべてのサーバを登録してください。

ポイント

- ISMのノード登録時は、新規クラスタを構成するサーバのiRMCのユーザー名／パスワードの入力が必要です。ユーザー名／パスワードの初期設定は、それぞれ「admin/admin」です。
- ノード登録の際にノードが所属するノードグループを選択します。ノードグループは、あとからでも編集できます。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が管理できます。
- データセンター、フロアやラックの新規登録、アラーム設定は、必要に応じて設定してください。設定方法は、「第2章 ISMを導入する」を参照してください。
- ノード登録については、『ユーザーズマニュアル』の「2.2.1.2 ノードの登録」や「2.2.1.6 ノードの検出」を参照してください。

手動検出によるノード登録

手動検出によるノード登録の操作方法は、「[3.1.2 ノードを直接登録する](#)」を参照してください。

登録の際に指定するIPアドレスは、「[6.6.1.9 iRMCのIPアドレスを設定する](#)」で設定したものを指定してください。

IPアドレスの範囲を指定することで新規クラスタを構成するすべてのサーバを同時に登録できます。

引続き「[6.6.2 クラスタ作成を実行する](#)」を実施してください。

自動検出によるノード登録

自動検出によるノード登録の操作方法は、「[3.1.1 ネットワーク内ノードを検出してノード登録する](#)」を参照してください。

[ノード登録]ウィザードでiRMCの固定IPアドレスを設定してください。

引続き「[6.6.1.10 BIOSを設定する](#)」を実施してください。

6.6.2 クラスタ作成を実行する

クラスタ作成機能を実行することで仮想化基盤にクラスタを作成します。

6.6.2.1 クラスタ作成の動作要件

クラスタ作成機能を使用するには、以下の動作要件を満たす必要があります。

実行する前に以下の要件を確認してください。

- DNS、NTPが正常に動作し、利用可能なこと
- お客様環境の既存AD構成時、またはPRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1専用ADVM構成時は、ADが正常に動作し、利用可能なこと
- ISM-VAにDNSサーバの情報が登録されていること
- 既存のクラスタが正常に動作していること
- 既存のクラスタのvCSAの版数はクラスタ作成するESXiの版数と同一、またはそれより新しい版数であること
- お客様環境の既存AD構成時、ADへのコンピュータ登録がポリシーなどで制限されている場合、新規クラスタを構成するサーバを事前にADへ登録しておくこと
- ストレージのネットワークを使用する新規クラスタを構成するサーバの物理NICが10GbEであること
- ストレージのネットワークを使用する物理スイッチのポートが10GbEであること
- PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1専用ADVM構成時は、ADVM#1とADVM#2にPRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1導入サービスの以下のファイルがあること
 - c:\FISCRB\PowerShellScript\%fis_advm_ftp_put.ps1
 - c:\FISCRB\PowerShellScript\FIS_JOB_ADVM_SET_DNS_ZONE.ps1
- ISMのプロファイル管理機能で、新規クラスタを構成するサーバ用プロファイルが作成されていること
- 新規クラスタを構成するサーバの電源がオフになっていること



注意

プロファイル適用によるOSインストールが完了している状態で、クラスタ作成を再実行する場合には、以下の動作要件となります。

- 新規クラスタを構成するサーバの電源がオンになっていること

OSインストールが完了している状態かどうかの確認は、以下の手順で確認できます。

1. 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. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」のタスクIDを選択します。
3. サブタスクリストのタスクの結果がすべて「Success」になっていることを確認します。

- All Flash構成時、SSDのキャパシティデバイスは以下の条件であること
キャッシュ、キャパシティ用の2種類のSSDのうち、本数が多い方であること(SSDの本数が同じ場合、容量の大きい方であること)

6.6.2.2 クラスタ作成手順

ISM for PRIMEFLEXのクラスタ作成機能の実行手順について説明します。



注意

クラスタ作成機能を実行する前に、[ストレージへのディスクの追加]の設定を確認してください。

「手動」の場合は、クラスタ作成完了後に手動でディスクの追加作業を行ってください。

「自動」の場合は、vSANストレージへ自動でディスクが追加されます。

1. Administrator権限を持ったユーザーでISMにログインします。

ポイント

Administrator権限を持ったユーザーとは

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]-[ユーザーグループ]のユーザーグループリスト画面に表示される「管理対象ノード」が「全てのノードを管理」に設定されているユーザーグループのAdministrator権限を持ったユーザーを表します。

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]-[クラスタ]を選択します。

「クラスタリスト」画面が表示されます。

3. [アクション]ボタンから[クラスタ作成]を選択します。



[クラスタ作成]ウィザードが表示されます。

既存クラスタを参照作成する場合、既存クラスタを選択して、[アクション]ボタンから[クラスタ参照作成]を選択します。



4. 「CMS情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順5に進んでください。

クラスタ作成

?

1. CMS情報

2. クラスタ基本情報

3. クラスタ詳細情報

4. 構成ノード選択

5. ノード詳細情報

6. 確認

クラスタの種類を選択してください。

種類 *

--- クラスタの種類を選択してください。 ---

▼

次へ

キャンセル

- 99 -

5. 「クラスタ基本情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順6に進んでください。

クラスタ作成

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

仮想化管理ソフトウェア名 * VMADMIN

種類 * VMware vSAN Cluster

データセンター名 *

クラスタ名 *

ストレージ構成 * ☒ Hybrid ☐ Allflash

戻る 次へ キャンセル

6. 「クラスタ詳細情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順7に進んでください。

クラスタ作成

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

DNS NTP LDAP 機能 ネットワーク ストレージポリシー

DNS情報

ドメイン名

セカンダリDNSサーバIPアドレス ⓘ

☐ DNSレコード登録の設定を有効にする ⓘ

戻る 次へ キャンセル

7. 「構成ノード選択」画面の[選択]ボタンを選択して、表示された「対象ノードの選択」画面で、新規クラスタを構成するサーバを選択します。

再実行の場合、本手順は不要です。[次へ]ボタンを選択して、手順9に進んでください。

8. 新規クラスタを構成するサーバがプロファイル未適用の場合は、[プロファイル]の項目にある[選択]ボタンを選択して、適用対象のプロファイルを選択します。

9. 「ノード詳細情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順10に進んでください。

注意

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』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

10. 「確認」画面でパラメータを確認し、[実行]ボタンを選択します。

クラスタ作成

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

CMS 基本情報 DNS NTP LDAP 機能 ネットワーク ストレージプール 構成ノード iRMC OS vDS

種類 * VMware vSAN Cluster

仮想化管理ソフトウェア名 * VMADMIN

戻る 実行 キャンセル

クラスタ作成の実行は、ISMのタスクとして登録されます。

グローバルナビゲーションメニュー上部の[タスク]を選択して表示される「タスク」画面のタスクリストで、タスクタイプが「Cluster Creation」となっているのが、クラスタ作成のタスクです。

タスク

タスクリスト 次の自動更新まで: 9 秒 停止 更新

検索 572 / 572 (表示上限 最新 1000件) フィルター アクション

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	0:26:07	501	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:43:39
完了	Success	0:32:55	500	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:50:28
完了	Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53
完了	Success	0:00:01	498	Releasing profile	pfadmin	2018/05/02 22:57:31	2018/05/02 22:57:33
完了	Success	0:00:02	497	Releasing profile	pfadmin	2018/05/02 22:57:25	2018/05/02 22:57:27

閉じる

ポイント

「タスク」画面のタスクリストから「Cluster Creation」の[タスクID]を選択すると、「Cluster Creation」の「タスク」画面が表示されます。この画面では、新規クラスタを構成するサーバごとにサブタスクリストが表示されるので、メッセージ欄を確認することでタスクの進行状況を確認できます。

タスク

タスクリスト > 499

次の自動更新まで : 9 秒

停止

アクション ▼

更新

タスク情報

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53

サブタスクリスト

ステータス	進捗	経過時間	サブタスクID	ノード名	完了時間	メッセージ
完了	Success	1:04:21	601	node3	2018/05/03 00:21:53	Subtask complete
完了	Success	1:04:21	602	node4	2018/05/03 00:21:53	Subtask complete

閉じる

11. 「Cluster Creation」のステータスが「完了」になったことを確認します。



注意

- ISMの「タスク」画面にエラーが表示された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。問題が解決できたら再度操作を行ってください。

ISMのプロファイル管理機能によるOSインストール(Assigning profileタスク)が正常終了している場合、再実行時には新規クラスタを構成するサーバの電源はオフにしないでください。

- クラスタ作成の実行が完了しても「vSAN構成の更新」と「vSphere HA設定」の処理が実行中の場合があります。これらの処理が完了してから「6.6.3 事後処理」に進んでください。

vSphere Web Clientにアクセスして、[トップ画面]で[最近のタスク]に表示されている「vSAN構成の更新」タスクと「vSphere HA設定」タスクが完了したことを確認します。

- 新規クラスタを構成するサーバの業務用仮想ネットワークの設定は、お客様環境に応じて設定してください。
- ファームウェアローリングアップデート機能を実行中にクラスタ作成機能を実行しないでください。

6.6.3 事後処理

クラスタ作成の事後処理について説明します。

6.6.3.1 クラスタ作成を確認する

以下の手順で作成されたvSANクラスタを確認してください。

1. vSphere Web Clientにアクセスして、以下の点を確認します。

- [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]で作成したクラスタが表示されることを確認します。
- [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[物理ディスク]で新規クラスタを構成するサーバのディスクが表示されることを確認します。
- [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[健全性]で再テストを実施し、問題のないことを確認します。

パフォーマンスサービスの統計DBオブジェクトに警告が出る場合がありますが、無視してください。

ポイント

健全性エラーが存在する場合、該当エラーの詳細を確認したうえで解決してください。

vSAN6.6.1環境(VMware ESXi 6.5 Update 1)の場合、健全性エラーと対処方法は以下のとおりです。

— vSAN ディスクバラン

ディスクのプロアクティブリバランスを実施してください。

— コントローラドライバがVMwareにより認定済み

対象ホストで推奨されているSASコントローラーのドライバを適用してください。

— コントローラファームウェアがVMwareにより認定済み

対処は不要です。sas3flashコントローラーのファームウェアバージョンを取得するVIBがインストールされていないため警告が表示されます。カスタムイメージには、このVIBは含まれていないので想定内です。

— vSAN ビルドに関する推奨事項エンジンの健全性

ネットワーク接続を復旧してください。

注意

— [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[フォールトドメインおよびストレッチクラスタ]-[フォールトドメイン]で新規クラスタを構成するサーバのフォールトドメインホストを確認します。

1つのフォールトドメインに複数のホストが設定されている場合、プロファイルの[OS個別情報]-[ネットワーク]-[DHCP]-[コンピュータ名をDNSサーバから取得]-[コンピュータ名]が既存クラスタ、または新規クラスタを構成するサーバのコンピュータ名と重複していないか確認してください。確認の結果、重複している場合、『ISM for PRIMEFLEX メッセージ集』の「2.4 クラスタ作成エラー時の対処例」の「対処例23」を参照して、対処してください。

— [ストレージへのディスクの追加]の設定が「手動」になっている場合は[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[物理ディスク]で新規クラスタを構成するサーバのディスクは表示されません。

手動でディスクの追加作業を行ってください。

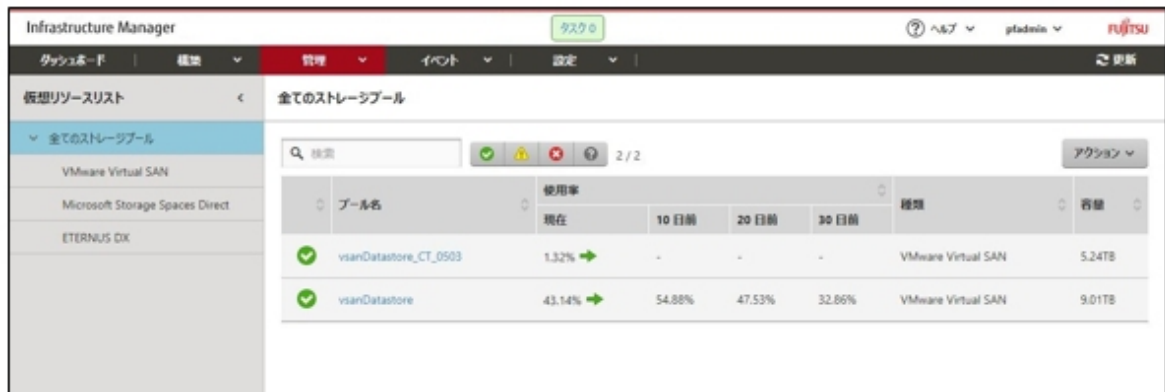
設定の確認方法は、vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSAN]-[全般]-[ストレージへのディスクの追加]を選択します。

手動でディスクを追加するには、以下の手順で設定します。新規クラスタを構成するすべてのサーバに対して実施してください。

1. vSphere Web ClientでvCSAにログインします。
2. [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[ディスク管理]を選択します。
3. 新規クラスタを構成するサーバを選択して、[新規ディスクグループの作成]を選択します。
4. 「ディスクグループの作成」画面で、「キャッシュ層として使用するディスク」と「キャパシティ層として使用するディスク」を選択して、[OK]ボタンを選択します。

タスクが完了するとディスクの追加作業が完了します。

2. ISMのGUIにアクセスして、[管理]-[仮想リソース]の「全てのストレージプール」画面で[アクション]-[仮想リソース情報の更新]を実行して更新します。更新後、対象のvSANデータストアが表示されていることを確認します。



プール名	使用率				種類	容量
	現在	10 日前	20 日前	30 日前		
vsanDatastore_CT_0503	1.32%	-	-	-	VMware Virtual SAN	5.24TB
vsanDatastore	43.14%	54.88%	47.53%	32.66%	VMware Virtual SAN	9.01TB

注意

タスクが正常に完了したに関わらず、vSANストレージが表示されない場合、またはvSANストレージ容量が想定している容量より少ない場合、以下の原因が考えられます。

- vSANネットワーク用の通信ができていない
スイッチの設定や結線を確認してください。
- [ストレージへのディスクの追加]の設定が「手動」になっている
手動でディスクの追加作業を行ってください。

設定の確認方法は、vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSAN]-[全般]-[ストレージへのディスクの追加]を選択します。

手動でディスクを追加するには、以下の手順で設定します。新規クラスタを構成するすべてのサーバに対して実施してください。

1. vSphere Web ClientでvCSAにログインします。
2. [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[ディスク管理]を選択します。
3. 新規クラスタを構成するサーバを選択して、[新規ディスクグループの作成]を選択します。
4. 「ディスクグループの作成」画面で、「キャッシュ層として使用するディスク」と「キャパシティ層として使用するディスク」を選択して、[OK]ボタンを選択します。

タスクが完了するとディスクの追加作業が完了します。

6.6.3.2 vCenter Serverの検知アラームを設定する

新規クラスタがVMware ESXi6.7の場合に必要な作業です。

vCenter Serverで検知されるアラートのうち、ハードウェアに関わるもの（ホストのハードウェアステータスやIPMIシステムイベントログ状態など）については、無効化してください。

以下の手順でアラーム定義を設定してください。

1. vSphere Web Clientにアクセスして、[<vCenter Server名>]-[監視]-[問題]-[アラーム定義]-[<対象アラーム定義>]-[編集]を選択します。
2. 表示された編集画面で、[このアラームを有効にする]のチェックを外します。

対象アラーム定義

設定対象のアラーム定義は、以下のとおりです。

- ホストのプロセッサ ステータス

- ホストのメモリ ステータス
- ホストのハードウェアファン ステータス
- ホストのハードウェア電圧
- ホストのハードウェア温度ステータス
- ホストのハードウェアの電源状態
- ホストのハードウェア システム ボード ステータス
- ホストのバッテリーステータス
- ほかのホストのハードウェア オブジェクトのステータス
- ホストの IPMI システム イベント ログの状態
- ホストのベースボード管理コントローラーのステータス

6.6.3.3 VMware vSphereの制限事項／注意事項

以下のサイトを参照して『VMware vSphere ソフトウェア説明書 (PRIMERGY)』を熟読し、お客様の環境に該当する制限事項に対処してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

<http://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/>

6.6.3.4 ServerView RAID Managerに新規クラスタを構成するサーバを登録する

SSDの寿命監視をするために、ServerView RAID Managerに新規クラスタを構成するサーバを登録します。

本作業は、構成に応じて以下で実施します。

構成	実施箇所
PRIMEFLEX構成のADVMを使用している構成時	ADVM#1
PRIMEFLEX構成のADVMを使用していない構成時	お客様環境のServerView RAID Managerをインストールしたサーバ

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ます。

```
>cd "C:\Program Files\Fujitsu\ServerView Suite\RAID Manager\bin"
```

2. 新規クラスタを構成するすべてのサーバの台数分、以下のコマンドを実行します。

```
>amCLI -e 21/0 add_server name=<新規クラスタを構成するサーバESXiのIPアドレス> port=5989 username=root password=<rootのパスワード>
```

3. 以下のコマンドを実行して新規クラスタを構成するすべてのサーバが登録されていることを確認します。

```
>amCLI -e 21/0 show_server_list
```

4. サーバーマネージャーで[ツール]-[サービス]をクリックします。
5. [ServerView RAID Manager]を右クリックし、[再起動]をクリックします。
6. ServerView RAID Managerにログインして左ツリーの[ホスト]を選択すると、すべてのサーバが表示されます。
すべてのサーバの状態が正常であることを確認します。

6.6.3.5 証明書を削除する

「6.6.1.1 ADVMの証明書を作成する」で作成した証明書は、登録後は不要です。



注意

「6.6.1.1 ADVmの証明書を作成する」でADVm#1とADVm#2にアップロードした証明書はセキュリティリスクが生じます。セキュリティリスクが承知できない場合は、削除してください。

6.7 PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタを作成する(ISM 2.3.0.b以降)

PRIMEFLEX for Microsoft Storage Spaces Directでのクラスタ作成手順について説明します。

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。



ポイント

PRIMEFLEX for Microsoft Storage Spaces Direct版でのクラスタ作成は、ISM 2.3.0.b以降で使用できます。

クラスタ作成は、以下の作業フローで行います。

表6.9 クラスタ作成フロー

クラスタ作成手順		作業内容
1	事前準備	<ul style="list-style-type: none">新規クラスタを構成するサーバの証明書作成DHCPの設定OSインストール媒体のISOイメージをISM-VAへインポートプロファイルの作成設置と結線iRMCのIPアドレス設定BIOSの設定システムディスク(RAID1)の作成ISMへノード登録
2	クラスタ作成の実行	
3	事後処理	<ul style="list-style-type: none">クラスタ情報の取得と更新クラスタ作成確認業務用仮想スイッチへの登録システムボリューム名の設定ブラウザの設定証明書削除不要ファイルの削除

6.7.1 事前準備

クラスタ作成を行う前の準備作業について説明します。

6.7.1.1 新規クラスタを構成するサーバの証明書を作成する

クラスタ作成機能は、新規クラスタを構成するサーバに対してISMからSSL暗号化通信で設定を行うため、証明書の作成と登録が必要です。

(1) 証明書の作成

管理端末から証明書作成ツール(makecert.exe)、個人情報交換ファイル作成ツール(pvk2pfx.exe)を使用し、以下の3つのファイルを作成します。

- ー CERファイル(証明書)
- ー PVKファイル(秘密鍵ファイル)
- ー PFXファイル(サービス証明書)

(1-1) 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。

- .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>



- 上記ツールは管理端末にインストールしてください。
- 上記URLの.NET Framework 4.5は、証明書を作成するための管理端末の言語に合わせてダウンロードしてください。
- 上記URLのWindows Software Development Kitは、Windows 8.1およびWindows Server 2012以降の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 10以外のプラットフォームでは、Windows 10 SDKを使用する際に、Universal CRTがインストールされている必要があります (KB2999226 (<https://support.microsoft.com/ja-jp/help/2999226/update-for-universal-c-runtime-in-windows>)) を参照)。セットアップ中のエラーを回避するために、Windows SDKをインストールする前に、推奨される最新の更新プログラムとパッチをMicrosoft Updateから必ずインストールしてください。

(1-2) 証明書、秘密鍵ファイルの作成

管理端末のコマンドプロンプト(管理者)から以下のコマンドを実行します。

新規クラスタを構成するサーバ名を「192.168.10.10」、証明書の有効期間を「2018年3月30日」に設定する場合のコマンド例です。

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -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>
```

途中、証明書にセットするパスワードを2回要求されますので、間違えずに入力してください。間違えた場合は、上記コマンドを実行してやり直してください。

(1-3) サービス証明書の作成

管理端末のコマンドプロンプト(管理者)から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>
```

途中、(1-2)でセットしたパスワードを要求されますので、入力してください。



- ー 新規クラスタを構成するすべてのサーバに対して証明書を作成してください。
 - ー 証明書のファイル名は、「ISMのプロファイルに設定するコンピュータ名」を指定してください。
- 例)
- hv-host4.cer

- hv-host4.pfx

(2) 証明書の登録

証明書の登録は、OSインストール時にOS設定スクリプトで実行されます。

(1)で作成した証明書は、FTPでISM-VAにアクセスして以下にアップロードしてください。

/Administrator/ftp/postscript_ClusterOperation/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

6.7.1.2 DHCPを設定する

クラスタ作成機能ではプロファイル適用を使用してOSのインストール作業を実施します。プロファイル適用によるOSインストールを実行するためには、DHCPサーバが必要です。

ISM-VAは内部でDHCPサーバ機能を持っていますが、ISM-VA外部にDHCPサーバを用意して使用することもできます。内部DHCPを使用する場合は、『ユーザーズマニュアル』の「[4.15 ISM-VA内部のDHCPサーバ](#)」を参照して設定してください。

新規クラスタを構成するすべてのサーバの台数分リースできるように設定してください。



注意

- 使用するDHCPサービスが起動していることを確認してください。
- DHCPサーバが同一ネットワーク内で複数起動している場合は、正確に機能しない場合があります。使用しないDHCPサービスは必ず停止してください。
- リース期間は作業中に期限が切れないように設定してください。
- 本製品の構成では、管理ネットワークを冗長しているため、複数ポートにIPアドレスがリースされます。リースするIPアドレスが不足しないように設定してください。
- ISMが内部／外部どちらのDHCPを使用する設定になっているか確認して、お客様が使用するDHCPの設定に合わせて変更してください。変更方法は、『ユーザーズマニュアル』の「[4.15.4 DHCPサーバの切替え](#)」を参照してください。

6.7.1.3 OSインストール媒体のISOイメージをISM-VAへインポートする

ISMにServerView Suite DVD Installation (DVD 1)と、OSのインストールメディアをインポートします。

既存のものを使用する場合は、インポートの必要はありません。

インポートの操作については、『ユーザーズマニュアル』の「[2.13.2 リポジトリ管理機能](#)」を参照してください。

また、サポート版数は、『プロファイル管理機能プロファイル設定項目集』を参照してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスク追加方法は、『ユーザーズマニュアル』の「[3.7 仮想ディスクの割当て](#)」を参照してください。

6.7.1.4 プロファイルを作成する

ISMのプロファイル管理機能を使用して、新規クラスタを構成するサーバのプロファイルを作成します。既存のプロファイルから参照作成して、プロファイルを作成してください。



注意

新規クラスタを構成するすべてのサーバに対してプロファイルを作成してください。

- ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
- 参照作成元とする既存のプロファイルを選択し、[アクション]ボタンから[参照作成]を選択します。

3. 各項目を設定します。

BIOSポリシー、iRMCポリシーは新規クラスタを構成するサーバに合わせて指定します。

新規クラスタを構成するサーバが既存クラスタ環境のサーバと同じ場合には既存のものを指定します。

プロファイル作成については、「[3.3 サーバに各種設定／OSインストールをする](#)」を参照してください。

注意

- ー 以下の項目には、チェックを付けないでください。
 - [OS]タブの[インストール後のスクリプト実行]
 - [OS個別情報]タブの[DHCP]
- ー 以下の項目は、重複しないように設定してください。
 - [OS個別情報]タブの[コンピュータ名]
 - [OS個別情報]タブの[ネットワーク]-[DHCP]-[IPアドレス]

6.7.1.5 設置と結線を行う

新規クラスタを構成するサーバの設置と結線を行います。詳細は、新規クラスタを構成するサーバの『オペレーティングマニュアル』を参照してください。ネットワークスイッチの設定に関しては、スイッチのマニュアルを参考にして適切に設定してください。

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。新規で作成するクラスタを既存クラスタと別ネットワークに作成する場合は、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。ネットワーク構成に関しては、『ユーザーズマニュアル』の「1.4 構成」も併せて参照してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

ISMのノード登録作業時のノード検出方法に応じて以降の作業順番が異なります。

- ・ ノードを手動検出する場合
「[6.7.1.6 iRMCのIPアドレスを設定する](#)」を実施してください。
- ・ ノードを自動検出する場合
「[6.7.1.9 ISMへノードを登録する](#)」の「自動検出によるノード登録」を実施してください。

6.7.1.6 iRMCのIPアドレスを設定する

新規クラスタを構成するサーバを手動検出でISMにノード登録する場合は、iRMCに固定IPアドレスを設定してください。

新規クラスタを構成するサーバのBIOSを起動して、BIOS設定画面から固定IPアドレスを設定します。この作業を実施するためには、事前に「[6.7.1.5 設置と結線を行う](#)」の作業が必要です。また、BIOS画面表示／操作を行うために、新規クラスタを構成するサーバにディスプレイとキーボードを接続してください。

BIOSの起動と、iRMCのIPアドレス設定については、新規クラスタを構成するサーバの「BIOSセットアップユーティリティ」のマニュアルを参考にしてください。

新規クラスタを構成するすべてのサーバに対して設定してください。

また、IPアドレスの設定と同時に「[6.7.1.7 BIOSを設定する](#)」も実施してください。

新規クラスタを構成するサーバの「BIOSセットアップユーティリティ」のマニュアルは、以下のサイトから取得できます。

<http://manuals.ts.fujitsu.com/index.php?l=ja>

6.7.1.7 BIOSを設定する

BIOSの設定をします。

「[6.7.1.5 設置と結線を行う](#)」で「ノードを手動検出する場合」を選択している場合は、「[6.7.1.6 iRMCのIPアドレスを設定する](#)」と一緒に本項の設定を実施してください。

「6.7.1.5 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。BIOSを起動して、BIOS設定画面で以下を設定してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

表6.10 BIOS設定

項目		設定値
Main	System Date	ローカル日時
	System Time	ローカル日時
Advanced - Network Stack Configuration	Network Stack	Enabled
	IPv4 PXE Support	Enabled
	IPv6 PXE Support	Disabled
Security - Security Boot Configuration	Secure Boot Control	Enabled
Server Mgmt - iRMC LAN Parameters Configuration	IP Configuration	Use static configuration
	iRMC IPv6 LAN Stack	Disabled



注意

BIOSの設定が完了したら、BIOS画面の[Save & Exit]タブの「Save Changes and Exit」を実施し、それから数分後に電源を停止してください。

引続き「6.7.1.8 システムディスク(RAID1)を作成する」を実施してください。

6.7.1.8 システムディスク(RAID1)を作成する

PRIMERGYのUEFI画面で、システムディスクとして使用するロジカルディスク(HDD2本をRAID1で構築)を作成します。新規クラスタを構成するすべてのサーバに対して実施してください。

1. iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。新規クラスタを構成するサーバの電源をONにします。ビデオリダイレクションのメニューから、[電源(Power)] - [電源投入(Power ON)]を選択します。
2. BIOS (UEFI) 起動画面で[F2]キーを押します。
UEFIのセットアップ画面が表示されます。
3. [Advanced]タブを選択し、「LSI SAS3 MPT Controller SAS3008」を選択して[Enter]キーを押します。
4. 「LSI SAS3 MPT Controller X.XX.XX.XX」を選択し、[Enter]キーを押します。
5. 「Controller Management」を選択し、[Enter]キーを押します。
6. 「Create Configuration」を選択し、[Enter]キーを押します。
7. 「Select RAID level」で「RAID 1」を選択し、「Select Physical Disks」を選択して[Enter]キーを押します。
8. 「Select Interface Type」で用意したシステムディスクのタイプを選択します。
9. 「Select Media Type」でシステムディスクのメディア(HDD)を選択します。
「Select Media Type」に表示されたディスクの中からお客様が購入されたOSブート用のシステムディスクを2本選択します。
10. システムディスクとするディスク2本を「Enabled」に変更し、「Apply Changes」を選択して[Enter]キーを押します。
11. 確認画面が表示されますので、「Confirm」を「Enabled」に変更後、「Yes」を選択して[Enter]キーを押します。
12. 「Operation completed successfully」で「OK」を選択し、[Enter]キーを押します。
13. [Esc]キーを複数回押し、「Exit Without Saving」で「Yes」を選択し、[Enter]キーを押します。
14. サーバの電源をオフにします。ビデオリダイレクションのメニューから、[電源(Power)] - [電源切断(Immediate Power Off)]を選択します。

「[6.7.1.5 設置と結線を行う](#)」で「ノードを手動検出する場合」を選択している場合は、引き続き「[6.7.1.9 ISMへノードを登録する](#)」の「手動検出によるノード登録」を実施してください。

「[6.7.1.5 設置と結線を行う](#)」で「ノードを自動検出する場合」を選択している場合は、引き続き「[6.7.2 クラスタ作成を実行する](#)」を実施してください。

6.7.1.9 ISMへノードを登録する

ISMを使用してOSをインストールするために、新規クラスタを構成するサーバをISMに登録します。

ISMへのノード登録には手動検出機能と自動検出機能が使用できます。

新規クラスタを構成するすべてのサーバを登録してください。



ポイント

- ISMのノード登録時は、新規クラスタを構成するサーバのiRMCのユーザー名／パスワードの入力が必要です。ユーザー名／パスワードの初期設定は、それぞれ「admin/admin」です。
- ノード登録の際にノードが所属するノードグループを選択します。ノードグループは、あとからでも編集できます。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が管理できます。
- データセンター、フロアやラックの新規登録、アラーム設定は、必要に応じて設定してください。設定方法は、「[第2章 ISMを導入する](#)」を参照してください。
- ノード登録については、『ユーザーズマニュアル』の「2.2.1.2 ノードの登録」や「2.2.1.6 ノードの検出」を参照してください。

手動検出によるノード登録

手動検出によるノード登録の操作方法は、「[3.1.2 ノードを直接登録する](#)」を参照してください。

登録の際に指定するIPアドレスは、「[6.7.1.6 iRMCのIPアドレスを設定する](#)」で設定したものを指定してください。

IPアドレスの範囲を指定することで新規クラスタを構成するすべてのサーバを同時に登録できます。

引き続き「[6.7.2 クラスタ作成を実行する](#)」を実施してください。

自動検出によるノード登録

自動検出によるノード登録の操作方法は、「[3.1.1 ネットワーク内ノードを検出してノード登録する](#)」を参照してください。

[ノード登録]ウィザードでiRMCの固定IPアドレスを設定してください。

引き続き「[6.7.1.7 BIOSを設定する](#)」を実施してください。

6.7.2 クラスタ作成を実行する

クラスタ作成機能を実行することで仮想化基盤にクラスタを作成します。

6.7.2.1 クラスタ作成の動作要件

クラスタ作成機能を使用するには、以下の動作要件を満たす必要があります。

- 実行する前に以下の要件を確認してください。
 - AD、DNS、NTPが正常に動作し、利用可能なこと
 - ISM-VAにDNSサーバの情報が登録されていること
 - クラスタが正常に動作していること
 - お客様環境の既存AD構成時、ADへのコンピュータ登録がポリシーなどで制限されている場合、新規クラスタを構成するサーバを事前にADへ登録しておくこと
 - 新規クラスタを構成するサーバにIntel、またはMellanoxのEthernetアダプターが装着されていること

- Ethernetアダプターは10G以上で通信できること
- 新規クラスタを構成するサーバのBIOS設定値が、「6.7.1.7 BIOSを設定する」どおりに設定されていること
- PRIMEFLEX for Microsoft Storage Spaces Directのデバイス構成が、以下のとおりになっていること

デバイス	初期値	用途
PCIカード1 (Port1)、PCIカード2 (Port1)	vSwitch0	業務 (Service) LAN
PCIカード1 (Port0)、PCIカード2 (Port0)	vSwitch1	管理 (Management) LAN Storage_1 LAN、Storage_2 LAN (フェイルオーバークラスタのハートビート、ライブマイグレーション用)

- ISMのプロファイル管理機能で、新規クラスタを構成するサーバ用プロファイルが作成されていること
- 新規クラスタを構成するサーバの電源がオフになっていること

注意

.....
 プロファイル適用によるOSインストールが完了している状態で、クラスタ作成を再実行する場合には、以下の動作要件となります。

- 新規クラスタを構成するサーバの電源がオンになっていること

OSインストールが完了している状態かどうかの確認は、以下の手順で確認できます。

1. 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. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」のタスクIDを選択します。
 3. サブタスクリストのタスクの結果がすべて「Success」になっていることを確認します。
-

- PRIMEFLEX for Microsoft Storage Spaces Direct専用ADVM構成時は、ADVM#1とADVM#2にPRIMEFLEX for Microsoft Storage Spaces Direct導入サービスの以下のファイルがあること
 - c:\FISCRB\PowerShellScript\fis_advm_ftp_put.ps1
 - c:\FISCRB\PowerShellScript\FIS_JOB_ADVM_RECEIVE_FILES.ps1
- ・ 2ノードでクラスタを作成した場合はクォーラムが必要です。

6.7.2.2 クラスタ作成手順

ISM for PRIMEFLEXのクラスタ作成機能の実行手順について説明します。

1. Administrator権限を持ったユーザーでISMにログインします。

ポイント

Administrator権限を持ったユーザーとは

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]-[ユーザーグループ]のユーザーグループリスト画面に表示される「管理対象ノード」が「全てのノードを管理」に設定されているユーザーグループのAdministrator権限を持ったユーザーを表します。

.....

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]-[クラスタ]を選択します。
 「クラスタリスト」画面が表示されます。

3. [アクション]ボタンから[クラスタ作成]を選択します。



[クラスタ作成]ウィザードが表示されます。

既存クラスタを参照作成する場合、既存クラスタを選択して、[アクション]ボタンから[クラスタ参照作成]を選択します。



4. 「CMS情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順5に進んでください。

5. 「クラスタ基本情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順6に進んでください。

クラスタ作成

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

仮想化管理ソフトウェア名 * PRMSPC

種類 * Microsoft Failover Cluster

クラスタ名 *

構成ノード数 * ☐ 2ノード ☒ 3ノード以上

戻る 次へ キャンセル

6. 「クラスタ詳細情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順7に進んでください。

クラスタ作成

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

DNS LDAP ネットワーク ストレージルール

DNS設定

セカンダリDNSサーバIPアドレス

戻る 次へ キャンセル

7. 「構成ノード選択」画面の[選択]ボタンを選択して、表示された「対象ノードの選択」画面で、新規クラスタを構成するサーバを選択します。

再実行の場合、本手順は不要です。[次へ]ボタンを選択して、手順9に進んでください。

8. 新規クラスタを構成するサーバがプロファイル未適用の場合は、[プロファイル]の項目にある[選択]ボタンを選択して、適用対象のプロファイルを選択します。
9. 「ノード詳細情報」画面の各種パラメーターを入力します。

再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順10に進んでください。

注意

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』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

10. 「確認」画面でパラメータを確認し、[実行]ボタンを選択します。

クラスタ作成の実行は、ISMのタスクとして登録されます。

グローバルナビゲーションメニュー上部の[タスク]を選択して表示される「タスク」画面のタスクリストで、タスクタイプが「Cluster Creation」となっているのが、クラスタ作成のタスクです。

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	0:26:07	501	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:43:39
完了	Success	0:32:55	500	Assigning profile	pfadmin	2018/05/02 23:17:32	2018/05/02 23:50:28
完了	Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53
完了	Success	0:00:01	498	Releasing profile	pfadmin	2018/05/02 22:57:31	2018/05/02 22:57:33
完了	Success	0:00:02	497	Releasing profile	pfadmin	2018/05/02 22:57:25	2018/05/02 22:57:27

11. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」の[タスクID]を選択します。



注意

PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタ作成では、タスク実行中、ライセンス条項に承諾する必要があります。

また、システムを安定稼働させるために、最新のWindowsの更新プログラムを適用してください。

以降の手順12～25は、プロファイル適用の完了後180分以内に作業を実施してください。時間が過ぎるとISMのイベントログに以下のメッセージが出力されてクラスタ作成がタイムアウトで異常終了しますので、ご注意ください。

50215309 : Subtask error : クラスタ作成に失敗しました。クラスタ作成タスクの設定処理でエラーが発生しました。(The task type setting process retried out; task type = Cluster Creation; id = 20; task item set name = OS Installation; task item name = Wait Hyperv OS Boot; detail code = E010205)

クラスタ作成がタイムアウトで異常終了した場合、手順25まで実施後、クラスタ作成機能を再実行してください。

手順12～25を実施中にクラスタ作成機能がタイムアウトによる異常終了をしても、そのまま続けて手順25まで実施してください。

ポイント

「タスク」画面のタスクリストから「Cluster Creation」の[タスクID]を選択すると、「Cluster Creation」の「タスク」画面が表示されます。この画面では、新規クラスタを構成するサーバごとにサブタスクリストが表示されるので、メッセージ欄を確認することでタスクの進行状況を確認できます。



タスク							
タスクリスト > 499							
次の自動更新まで: 9 秒							
タスク情報							
ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	1:04:21	499	Cluster Creation	pfadmin	2018/05/02 23:17:31	2018/05/03 00:21:53
サブタスクリスト							
ステータス	進捗	経過時間	サブタスクID	ノード名	完了時間	メッセージ	
完了	Success	1:04:21	601	node3	2018/05/03 00:21:53	Subtask complete	
完了	Success	1:04:21	602	node4	2018/05/03 00:21:53	Subtask complete	

- 「タスク」画面で「Assigning profile」タスクのステータスが「完了」になったら、新規クラスタを構成するサーバのiRMCの画面を表示し、ログインして、ビデオリダイレクション(Video Redirection)を選択します。

セキュリティ警告が表示された場合は、「リスクを受け入れて、このアプリケーションを実行します」にチェックを付け[実行]ボタンを選択します。

ビデオリダイレクションの画面(サーバの画面)が表示されます。

- 「プロダクトキーを入力してください」という画面が表示されたら、インストールメディアのプロダクトキーを入力し、[次へ]を選択します。

注意

OSインストールメディアによっては、表示されない場合もあります。

- ライセンス条項画面で[承諾する]ボタンを選択します。
- [キーボード]タブの[Ctrl+Alt+Del]を選択して、Administrator権限を持ったユーザーでログインします。

ServerView Installation Managerのスク립トが実行されます。

注意

ビデオリダイレクションの画面で、ServerView Installation Manager画面の[Restart system]ボタンを選択、またはWindowsを再起動しないでください。

Windowsの更新プログラムとMellanox LANドライバの適用ができなくなります。

- 新規クラスタを構成するサーバのWindows OSに対して、Administrator権限を持ったユーザーでリモートデスクトップにアクセスします。

注意

リモートデスクトップ接続時にエラーメッセージが表示されて接続できない場合、以下のURLの問題の可能性があります。リモートデスクトップの接続先にビデオリダイレクションの画面から共有フォルダーを使用して最新の更新プログラムを転送し、適用してください。

<https://blogs.technet.microsoft.com/askcorejp/2018/05/02/2018-05-rollup-credssp-rdp/>

17. 新規クラスタを構成するサーバに最新のWindowsの更新プログラムを転送します。
18. 新規クラスタを構成するサーバにMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、Mellanox LANドライバを転送します。

Mellanox LANドライバは、以下のサイトからドライバパッケージをダウンロードしてください。

<http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/>

Mellanox LANドライバが適用済みの場合は、本手順は不要です。手順19に進んでください。

ポイント

Mellanox LANドライバは、[コントロールパネル]-[プログラム]-[プログラムと機能]-[プログラムのアンインストールまたは変更]に「MLNX_WinOF2」がインストールされていることで確認できます。

注意

Mellanox LANカードをご利用の場合は、手順20でMellanox LANカードのドライバをインストールしてください。

19. 新規クラスタを構成するサーバに転送したWindowsの更新プログラムを適用します。
20. 新規クラスタを構成するサーバにMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、転送したMellanox LANドライバを適用します。

Mellanox LANドライバが適用済みの場合は、本手順は不要です。手順21に進んでください。
21. Windowsの更新プログラムの適用が完了すると、再起動の確認画面が表示されます。[閉じる]ボタンを選択してからリモートデスクトップを閉じて、ビデオリダイレクションの画面に戻ります。

画面がロックされていた場合は、Administrator権限を持ったユーザーでログインし直します。
22. サーバーマネージャーが最前面になっていた場合は、最小化してServerView Installation Manager画面を表示します。
23. ServerView Installation Manager画面で[Restart system]ボタンを選択します。

サインアウト画面が表示されて、再起動されます。
24. 再起動後、Administrator権限を持ったユーザーでログインします。
25. 新規クラスタを構成するサーバに転送したWindowsの更新プログラムとMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、転送したMellanox LANドライバを削除します。
26. 新規クラスタを構成するすべてのサーバで手順12～25を実施します。
27. 「Cluster Creation」のステータスが「完了」になったことを確認します。

注意

- ISMの「タスク」画面にエラーが表示された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。問題が解決できたら再度操作を行ってください。

ISMのプロファイル管理機能によるOSインストール (Assigning profileタスク) が正常終了している場合、再実行時には新規クラスタを構成するサーバの電源はオフにしないでください。

- 新規クラスタを構成するサーバの業務用仮想ネットワークの設定は、お客様環境に応じて設定してください。

- ・ ファームウェアローリングアップデート機能を実行中にクラスタ作成機能を実行しないでください。

6.7.3 事後処理

クラスタ作成の事後処理について説明します。

6.7.3.1 クラスタ情報の取得と更新を行う

新規クラスタをクラスタ管理機能で監視するための設定を行ってください。その後、クラスタ情報の取得と更新を行ってください。

(1) Active Directoryへのサービスプリンシパル名を追加する

新規クラスタのサービスプリンシパル名 (SPN) を Active Directory に登録します。

1. 以下のコマンドを実行し、新規クラスタのサービスプリンシパル名 (SPN) を Active Directory に登録します。

```
>setspn -A HOST/<監視対象クラスタ IP アドレス> <監視対象クラスタ名>
```

2. 以下のコマンドを実行し、監視対象クラスタのサービスプリンシパル名が Active Directory に登録されたことを確認します。

```
>setspn -L <監視対象クラスタ名>
```

(2) Active DirectoryへKerberos委任を構成する

新規クラスタを構成するすべてのサーバと新規クラスタのKerberos委任をActive Directory に構成します。

1. Active Directory サーバにログインします。
2. サーバマネージャを開きます。
3. [ツール]ボタンから[Active Directory ユーザーとコンピュータ]を選択します。
4. ドメインを展開し、[コンピュータ]フォルダーを展開します。
5. 画面右側で、<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。
6. [委任]タブで、[任意のサービスへ委任でこのコンピュータを信頼する]にチェックが付いていることを確認します。
7. [OK]ボタンを選択し、すべてのクラスタノードおよびクラスタに対して手順5～6を実施します。

(3) クラスタ情報の取得と更新を行う

ISM GUI上に仮想化基盤の情報を取得し、表示内容を最新化します。

詳細については、『ユーザーズマニュアル』の「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。

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]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
2. [アクション]ボタンから[クラスタ情報取得・更新]を選択します。
3. クラスタ情報の更新が「完了」となったことを確認し、しばらく待ってからISM GUIの画面更新(画面右上の更新ボタンを選択)をします。
4. 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]を選択します。
5. [<対象のクラスタ>]-[クラスタ定義パラメーター]タブにクラスタ定義パラメーターが表示されていることを確認します。
クラスタ定義パラメーターが表示されない場合、しばらく待ってからISM GUIの画面更新(画面右上の更新ボタンを選択)を表示されるまで繰り返し行ってください。

6.7.3.2 クラスタ作成を確認する

以下の手順でPRIMEFLEX for Microsoft Storage Spaces Directへのクラスタ作成を確認してください。

1. フェイルオーバークラスタマネージャーにアクセスして、[<クラスタ名>]-[ノード]で作成したクラスタが表示されていることを確認します。以下の点を確認します。

- ー [<クラスタ名>]のクラスタイイベント内に警告やエラーがないこと
- ー [<クラスタ名>]-[ノード]-[<ノード名>]の状態が「稼働中」であること
- ー [<クラスタ名>]-[記憶域]-[プール]-[<プール名>]-[物理ディスク]のすべてのディスクにおいて、正常性状態が「正常」であること

注意

上記の点を確認できない場合は、保守資料を採取して、当社技術員に連絡してください。

2. ISMのGUIにアクセスして、[管理]-[仮想リソース]の「ストレージプール」画面で[アクション]-[仮想リソース情報の更新]を実行して更新します。更新後、対象の記憶域プールが表示されていることを確認します。

プール名	使用率				種類	容量
	現在	10 日前	20 日前	30 日前		
vsanDatastore	66.24%	67.00%	64.18%	54.63%	VMware Virtual SAN	9.01TB
S2D on cluster-S2D	0.00%	-	-	-	Microsoft Storage Spaces Direct	4.55TB

注意

- ー タスクが正常に完了したにも関わらず、記憶域プールが表示されない場合、PRIMEFLEX for Microsoft Storage Spaces Direct ネットワーク用の通信ができていない可能性があります。スイッチの設定や結線を確認してください。
- ー タスクの完了後、フェイルオーバークラスタマネージャーの[<クラスタ名>]のクラスタイイベント内に警告が表示される場合は、イベントIDとイベントの詳細を確認してください。以下の内容の場合は、一時的な警告のため問題ありません。右ペインの[最新のイベントの再設定]を実行してください。

イベントID	イベントの詳細
5120	クラスタの共有ボリューム'Volume1'('クラスタ仮想ディスク(Vdisk)')は'STATUS_DEVICE_NOT_CONNECTED(c000009d)'が原因で一時停止状態になりました。ボリュームへのパスが再確立されるまで、すべてのI/Oは一時的にキューに登録されます。

6.7.3.3 業務用仮想スイッチに登録する

新規クラスタを構成するすべてのサーバに対して実施してください。

Serviceアダプターを設定します。管理者権限でコマンドプロンプトからPowerShellを開いて、以下のコマンドを実行します。

```
>Add-VMNetworkAdapter -SwitchName vSwitch0 -Name "Service" -ManagementOS
>Set-VMNetworkAdapterVlan -VMNetworkAdapterName "Service" -VlanId <VLAN ID> -Access -ManagementOS [注1]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -PhysicalNetAdapterName "Slot <スロット番号> ポート 2" [注2]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -PhysicalNetAdapterName "Slot <スロット番号> ポート 2" [注3]
```

[注1]: <VLAN ID>には、業務LANのVLAN IDを指定します。

[注2]: <スロット番号>には、Serviceアダプターに設定する1枚目のPCIカードのネットワークアダプター名のスロット番号を指定します。

[注3]: <スロット番号>には、Serviceアダプターに設定する2枚目のPCIカードのネットワークアダプター名のスロット番号を指定します。

ポイント

スロット番号が不明な場合は、以下のコマンドで確認できます。

```
> Get-NetAdapterHardwareInfo | select Name, InterfaceDescription, Slot, Function | Sort-Object Name
```

コマンド出力例:

Name	InterfaceDescription	Slot	Function
Onboard Flexible LOM ポート 1	Intel (rainbow) Ethernet Connection X722 for 10GBASE-T		0
Onboard Flexible LOM ポート 2	Intel (rainbow) Ethernet Connection X722 for 10GBASE-T #2		1
Onboard LAN ポート 1	Intel (rainbow) I350 Gigabit Network Connection #2		0
Onboard LAN ポート 2	Intel (rainbow) I350 Gigabit Network Connection		1
Slot 03 ポート 1	Intel (R) Ethernet Converged Network Adapter X550-T2 #4	3	0
Slot 03 ポート 2	Intel (R) Ethernet Converged Network Adapter X550-T2 #2	3	1
Slot 07 ポート 1	Intel (R) Ethernet Converged Network Adapter X550-T2	7	0
Slot 07 ポート 2	Intel (R) Ethernet Converged Network Adapter X550-T2 #3	7	1

6.7.3.4 システムボリューム名を設定する

新規クラスタを構成するすべてのサーバに対して実施してください。

システムボリューム名を、以下の手順で「system」に設定してください。

1. 新規クラスタを構成するホストにログインします。
2. エクスプローラーを起動し、Cドライブを選択して右クリックし、[名前の変更]を選択します。
3. ドライブの名前に「system」と入力します。
4. すべてのホストに対して、手順1～3を実施します。

6.7.3.5 新規クラスタを構成するサーバのブラウザを設定する

ServerView RAID ManagerでSSDの寿命監視をするために、新規クラスタを構成するサーバのブラウザを設定します。

『FUJITSU Software ServerView Suite ServerView RAID Manager』の「2.2.1 クライアント/ブラウザ設定」を参照し、新規クラスタを構成するサーバのWebブラウザを設定してください。

6.7.3.6 証明書を削除する

「6.7.1.1 新規クラスタを構成するサーバの証明書を作成する」で作成した証明書は、新規クラスタを構成するサーバへOSインストール時に転送され登録されます。以下の手順で証明書を削除してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

1. 新規クラスタを構成するサーバのWindows OSに対してリモートデスクトップでアクセスします。
2. エクスプローラーを開き、以下のファイルを削除します。
 - C:\¥PostInstall¥UserApplication¥postscript_ClusterOperation¥<証明書のファイル名.cer>
 - C:\¥PostInstall¥UserApplication¥postscript_ClusterOperation¥<サービス証明書のファイル名.pfx>
 - C:\¥DeploymentRepository¥Add-on¥UserApplication¥postscript_ClusterOperation¥<証明書のファイル名.cer>
 - C:\¥DeploymentRepository¥Add-on¥UserApplication¥postscript_ClusterOperation¥<サービス証明書のファイル名.pfx>



注意

「6.7.1.1 新規クラスタを構成するサーバの証明書を作成する」でISM-VAにアップロードした証明書はセキュリティリスクが生じます。セキュリティリスクが承知できない場合は、削除してください。

6.7.3.7 不要ファイルを削除する

クラスタ作成の完了後は、以下の手順で不要なファイルを削除してください。

新規クラスタを構成するすべてのサーバに対して実施してください。

1. 新規クラスタを構成するサーバのWindows OSに対してリモートデスクトップでアクセスします。
2. エクスプローラーを開き、以下のディレクトリ配下のファイルとディレクトリをすべて削除します。
 - C:\PostInstall\UserApplication\postscript_ClusterOperation
 - C:\FISCRB\PowershellScript
 - C:\FISCRB\log

6.8 PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1版 クラスタを拡張する

PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1でのクラスタ拡張手順について説明します。

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ拡張は、以下の作業フローで行います。

表6.11 拡張フロー

クラスタ拡張手順		作業内容
1	事前準備	<ul style="list-style-type: none"> • ADVMの証明書作成 • DNSへホストレコード登録 • DHCPの設定 • OSインストール媒体のISOイメージをISM-VAへインポート • VMware ESXiパッチのアップロード • VMware SMIS Providerのアップロード • プロファイルの作成 • クラスタ定義パラメーターの作成と編集 • 設置と結線 • iRMCのIPアドレス設定 • BIOSの設定 • ISMへノード登録
2	クラスタ拡張の実行	
3	事後処理	<ul style="list-style-type: none"> • クラスタ拡張確認 • VMware vSphereの制限事項／注意事項 • 業務用仮想分散スイッチへの登録 • ServerView RAID Managerへの登録 • 証明書削除

6.8.1 事前準備

クラスタ拡張を行う前の準備作業について説明します。

6.8.1.1 ADVMの証明書を作成する

本設定は、PRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1専用ADVM構成時、かつクラスタ拡張機能の初回使用時に必要な作業です。

クラスタ拡張機能は、ISMからADVMに対してSSL暗号化通信で設定を行うため、証明書の登録が必要です。

ADVM#1とADVM#2に対して、以下の流れでSSL通信用の証明書登録と通信を許可するための設定を行ってください。

なお、SSL暗号化通信せずにクラスタ拡張機能を使用することも可能です。その場合、本設定は不要です。「[6.8.1.2 DNSへホストレコードを登録する](#)」に進んでください。



注意

- SSL暗号化通信を使用しないでクラスタ拡張機能を使用する場合は、http通信を使用するため設定パラメーター傍受などのセキュリティリスクがあります。セキュリティリスクを承知できない場合は、本手順を実施して証明書を登録してください。
- SSL暗号化通信の使用有無に応じた設定は、以下のとおりです。

ー SSL暗号化通信を使用する

クラスタ定義パラメーターの[クラスタ]-[DNS情報]-[WinRMサービス(SSL)ポート番号]を入力して、ADVMとのWinRM通信をSSLで行う設定にしてください。

ー SSL暗号化通信を使用しない

クラスタ定義パラメーターの[クラスタ]-[DNS情報]-[WinRMサービスポート番号]を入力して、ADVMとのWinRM通信をSSLで行わない設定にしてください。

クラスタ定義パラメーターの詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

- リモートデスクトップ接続時にエラーメッセージが表示されて接続できない場合、以下のURLの問題の可能性があります。リモートデスクトップの接続先にHypervisorコンソール画面から共有フォルダーを使用して最新の更新プログラムを転送し、適用してください。

<https://blogs.technet.microsoft.com/askcorejp/2018/05/02/2018-05-rollup-credssp-rdp/>

- [6.8.1.1.1 WinRMサービスの起動を確認する](#)
- [6.8.1.1.2 WinRMサービスを設定する](#)
- [6.8.1.1.3 ファイアーウォールのポートを開放する](#)
- [6.8.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する](#)

6.8.1.1.1 WinRMサービスの起動を確認する

ADVM#1から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
```

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	

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
```



注意

- WinRMサービスは、環境によって自動起動になっていない場合があります。WinRMサービスを自動起動(auto)、または遅延自動起動(delayed-auto)するように設定してください。

以下は、自動起動に設定する場合の例になります。

```
>sc config winrm start=auto
```

- ADVM#1をADVM#2に読み替えてADVM#2に対しても同様にWinRMサービスの起動確認を行ってください。

6.8.1.1.2 WinRMサービスを設定する

(1) WinRMサービスの設定

初期設定ではBasic認証が許可されていないため、「(1-1) Basic認証の許可」を行います。

https通信を使用するためBasic認証の通信は暗号化されます。

ADVM#1から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で実行されています。」と表示されている場合は、すでに設定が完了しているため、「(1-1) Basic認証の許可」に進んでください。

「WinRMは、管理用にこのコンピュータ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。」と表示されている場合は、WinRMサービスは実行されていますがリモートアクセス許可は設定されていないため、「y」を入力します。

WinRM は、管理用にこのコンピュータへのリモート 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。

(1-1) Basic認証の許可

コマンドプロンプトで以下のコマンドを実行し、WinRMサービスの設定を確認します。

```
> winrm get winrm/config
```

以下の結果を確認し、[Config]-[Client]-[Auth]-[Basic]がfalseとなっている場合、以下の手順に進んでください。trueとなっている場合は、すでに設定が完了しているため、「(2) https通信の設定」に進んでください。

```
Config
  MaxEnvelopeSizekb = 150
  MaxTimeoutms = 60000
  MaxBatchItems = 20
  MaxProviderRequests = 25
  Client
    NetworkDelays = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
  Auth
    Basic = false
    Digest = true
```

```
Kerberos = true
Negotiate = true
Certificate = true
DefaultPorts
  HTTP = 80
  HTTPS = 443
(以下省略)
```

以下のコマンドを実行します。

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

(2) 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。証明書は管理端末から作成できます。

(2-1) 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。

- .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>



- 上記ツールは管理端末にインストールしてください。
- 上記URLの.NET Framework 4.5は、証明書を作成するための管理端末の言語に合わせてダウンロードしてください。
- 上記URLのWindows Software Development Kitは、Windows 8.1およびWindows Server 2012以降の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 10以外のプラットフォームでは、Windows 10 SDKを使用する際に、Universal CRTがインストールされている必要があります (KB2999226 (<https://support.microsoft.com/ja-jp/help/2999226/update-for-universal-c-runtime-in-windows>)) を参照)。セットアップ中にエラーが発生しないようにするために、Windows SDKをインストールする前に、推奨される最新の更新プログラムとパッチをMicrosoft Updateから必ずインストールしてください。

(3) 証明書の作成

管理端末から証明書作成ツール (makecert.exe)、個人情報交換ファイル作成ツール (pvk2pfx.exe) 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)

(3-1) 証明書、秘密鍵ファイルの作成

管理端末のコマンドプロンプト (管理者) から以下のコマンドを実行します。

対象ADVMのサーバ名を「192.168.10.10」、証明書の有効期間を「2018年3月30日」に設定する場合のコマンド例です。

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -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>
```

途中、証明書にセットするパスワードを2回要求されますので、間違えずに入力してください。間違えた場合は、上記コマンドを実行してやり直してください。

(3-2) サービス証明書の作成

管理端末のコマンドプロンプト (管理者) から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>
```

途中、(3-1)でセットしたパスワードを要求されますので、入力してください。



注意

ADVM#1とADVM#2の2つの証明書を作成してください。

(4) 証明書、サービス証明書の登録

管理端末で作成した証明書、サービス証明書をADVM#1へアップロードします。

証明書スナップインを起動し、(3)で作成した証明書を登録します。

1. ADVM#1でmmc.exeを実行します。
2. [ファイル] - [スナップインの追加と削除]を選択します。
3. [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。
4. 「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。
5. [OK]を選択します。

(5) SSL証明書を登録

ADVM#1の証明書スナップインから以下の手順を行ってください。

1. <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 コンピューター)] - [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、証明書のウィザードインポートを完了します。
2. <証明書のファイル名.cer>を[信頼されたルート証明機関]に登録できたことを確認します。
[コンソールルート] - [証明書(ローカル コンピューター)] - [信頼されたルート証明機関] - [証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバ名となっていること、「目的」が「サーバー認証」となっていることを確認してください。なっていない場合は(5)の手順1を再実施してください。
3. <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 コンピューター)] - [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、証明書のウィザードインポートを完了します。途中、秘密キーのパスワード要求がありますが、何も入力せず空欄のまま[次へ]ボタンを選択してください。



注意

<サービス証明書のファイル名.pfx>ファイルを選択する場合、プルダウンから指定する必要があります。

4. <サービス証明書のファイル名.pfx>を[個人]に登録できたことを確認します。
[コンソールルート] - [証明書(ローカル コンピューター)] - [個人] - [証明書]の順に選択し、「発行先」と「発行者」がCNに指定したサーバ名となっていること、「目的」が「サーバー認証」となっていることを確認してください。なっていない場合は(5)の手順3を再実施してください。

(6) WinRMサービスへの証明書に記載された拇印を登録

(6-1) 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。

1. ADVM#1のコマンドプロンプトからPowerShellを起動します。
2. 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
```

(6-2) 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＞"}
```

(6-3) 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。返ってこない場合は、「(6-2) WinRMリスナーに証明書に記載された拇印を登録」からやり直してください。

```
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
```



注意

ADVM#1をADVM#2に読み替えて、「[6.8.1.1.2 WinRMサービスを設定する](#)」の(1)、(4)～(6)の手順を実施してください。

6.8.1.1.3 ファイアーウォールのポートを開放する

WinRMサービスがリクエストを受け付けられるように、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。

1. ADVM#1でWindows PowerShellを管理者権限で開きます。
2. 以下のようなコマンドを実行します。

```
>New-NetFirewallRule -DisplayName <ファイアーウォールルール名> -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort <ポート番号>
```

例) ポート番号5986を開放するルールに、「WinRM」という名前を設定します。

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort 5986
```



注意

- ・ファイアーウォールの設定は、環境(OSのバージョンなど)によって異なります。
- ・ADVM#1をADVM#2に読み替えて、ADVM#2に対しても同様に「[6.8.1.1.3 ファイアーウォールのポートを開放する](#)」を行ってください。

6.8.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する

ADVM#1から管理者権限でWindows PowerShellを開いて以下のコマンドを実行し、PowerShellスクリプトの実行ポリシーの設定を確認します。

```
> get-executionpolicy
```

コマンド結果を確認し、「RemoteSigned」となっている場合はすでに設定が完了しているため、「6.8.1.2 DNSへホストレコードを登録する」、または「6.8.1.3 DHCPを設定する」に進んでください。

「RemoteSigned」となっていない場合、以下の手順に進んでください。

1. 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



注意

ADVM#1をADVM#2に読み替えて、ADVM#2に対しても同様に「6.8.1.1.4 Windows PowerShellスクリプトの実行ポリシーを変更する」を行ってください。

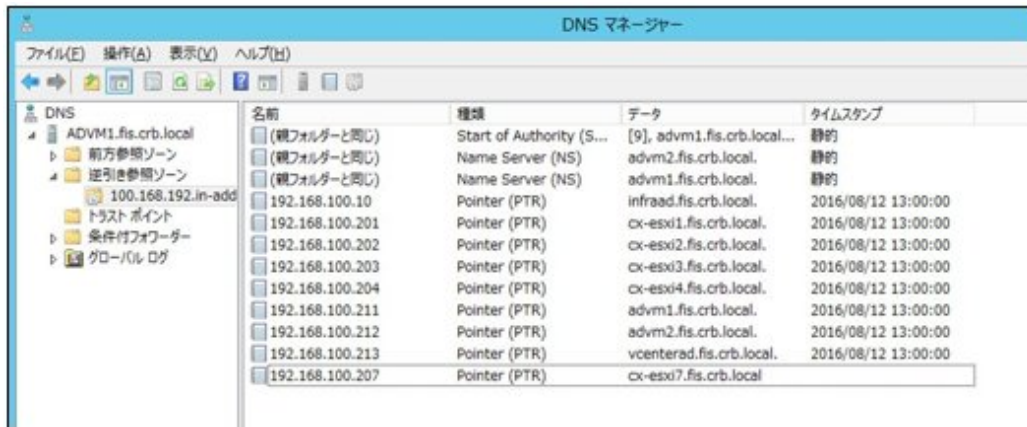
6.8.1.2 DNSへホストレコードを登録する

お客様環境のDNSサーバ使用時にのみ必要な作業です。OSインストールを実行する前にDNSの前方参照ゾーン、および逆引き参照ゾーンへクラスタ拡張時に追加するサーバのOSを登録して名前解決を可能にしておく必要があります。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

図6.3 前方参照ゾーンの登録例

図6.4 逆引き参照ゾーンの登録例



6.8.1.3 DHCPを設定する

クラスタ拡張機能ではプロファイル適用を使用してOSのインストール作業を実施します。プロファイル適用によるOSインストールを実行するためには、DHCPサーバが必要です。

ISM-VAは内部でDHCPサーバ機能を持っていますが、ISM-VA外部にDHCPサーバを用意して使用することもできます。内部DHCPを使用する場合は、『ユーザーズマニュアル』の「4.15 ISM-VA内部のDHCPサーバ」を参照して設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、複数台分リースできるように設定してください。



注意

- 使用するDHCPサービスが起動していることを確認してください。
- DHCPサーバが同一ネットワーク内で複数起動している場合は、正確に機能しない場合があります。使用しないDHCPサービスは必ず停止してください。
- リース期間は作業中に期限が切れないように設定してください。
- 本製品の構成では、管理ネットワークを冗長しているため、複数ポートにIPアドレスがリースされます。リースするIPアドレスが不足しないように設定してください。
- ISMが内部／外部どちらのDHCPを使用する設定になっているか確認して、お客様が使用するDHCPの設定に合わせて変更してください。変更方法は、『ユーザーズマニュアル』の「4.15.4 DHCPサーバの切替え」を参照してください。

6.8.1.4 OSインストール媒体のISOイメージをISM-VAへインポートする

ISMにServerView Suite DVD Installation (DVD 1)と、OSのインストールメディアをインポートします。

既存のものを使用する場合は、インポートは必要ありません。

インポートの操作については、『ユーザーズマニュアル』の「2.13.2 リポジトリ管理機能」を参照してください。

また、サポート版数は、『プロファイル管理機能 プロファイル設定項目集』を参照してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスク追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。

6.8.1.5 VMware ESXiパッチをアップロードする

クラスタ拡張機能でESXiのパッチも適用したい場合に実施してください。ESXiパッチファイルがアップロードされた場合にパッチ適用の処理が実行されます。

既存クラスタのESXiと同じバージョンになるように、お客様環境に応じて作業してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスクの追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。



注意

- VMware ESXiパッチファイルは1つだけとします。複数アップロードした場合には、クラスタ拡張は異常終了します。
- アップロードしたESXiパッチファイル(zipファイル)は解凍しないでください。解凍した場合には、クラスタ拡張は異常終了します。

1. FTPでISM-VAにアクセスし、適用ファイルを以下にアップロードします。

/Administrator/ftp/kickstart/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

適用ファイルのファイル名はリネームせずにアップロードしてください。

例)

— ESXi650-201704001.zip

6.8.1.6 VMware SMIS Providerをアップロードする

クラスタ拡張時に追加するサーバがPRIMERGY M4シリーズおよびVMware ESXi 6.5の場合に、必要な作業です。

VMware SMIS Providerがアップロードされた場合に適用の処理が実行されます。

VMware SMIS Providerのアップロードは、ダウンロードした圧縮ファイル(zipファイル)を解凍した中にある、オフラインバンドルを使用してください。

- ダウンロードした圧縮ファイル(zipファイル)の例:

VMware_MR_SAS_Providers-00.63.V0.05.zip

- オフラインバンドルの例:

VMW-ESX-5.5.0-Isipprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスクの追加方法は、『ユーザーズマニュアル』の「3.7 仮想ディスクの割当て」を参照してください。



注意

- VMware SMIS Providerのオフラインバンドルは1つだけとします。複数アップロードした場合には、クラスタ拡張は異常終了します。
- アップロードしたVMware SMIS Providerのオフラインバンドル(zipファイル)は解凍しないでください。解凍した場合には、クラスタ拡張は異常終了します。

1. FTPでISM-VAにアクセスし、適用ファイルを以下にアップロードします。

/Administrator/ftp/kickstart/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

適用ファイルのファイル名はリネームせずにアップロードしてください。

例)

— VMW-ESX-5.5.0-Isipprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

6.8.1.7 プロファイルを作成する

ISMのプロファイル管理機能を使用して、クラスタ拡張時に追加するサーバのプロファイルを作成します。既存のプロファイルから参照作成して、プロファイルを作成してください。



注意

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対してプロファイルを作成してください。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 参照作成元とする既存のプロファイルを選択し、[アクション]ボタンから[参照作成]を選択します。
3. 各項目を設定します。

BIOSポリシー、iRMCポリシーは既存のものを指定します。

プロファイル作成については、「[3.3 サーバに各種設定／OSインストールをする](#)」を参照してください。



注意

- ー 以下の項目には、チェックを付けないでください。
 - [OS]タブの[ネットワーク]の[セットアップ]
 - [OS]タブの[インストール後のスクリプト実行]
 - [OS]タブの[仮想化管理ソフトへの登録]
 - [OS個別情報]タブの[DHCP]
- ー PRIMERGY M2シリーズの場合、以下の項目には、チェックを付けないでください。
 - [OS]タブの[ネットワークポート指定]
- ー PRIMERGY M4シリーズの場合、[OS]タブの[管理LANネットワークポート設定]の項目は、以下の設定をしてください。
 - [ネットワークポート指定]にチェックを付けてください。
 - [指定方法]は[MACアドレス]を選択してください。
 - [MACアドレス]は10Gbpsの通信が可能なポート拡張オプションのポート0のMACアドレスを指定してください。
- ー 以下の項目は、重複しないように設定してください。
 - [OS個別情報]タブの[IPアドレス]
 - [OS個別情報]タブの[ネットワーク]-[DHCP]-[コンピュータ名をDNSサーバから取得]-[コンピュータ名]

6.8.1.8 クラスタ定義パラメーターの作成と編集を行う

ISMのGUIを使用して、必要に応じてクラスタ定義パラメーターの作成と編集を行います。

拡張するクラスタに対してクラスタ定義パラメーターを作成してください。拡張するクラスタが複数ある場合は、すべてのクラスタに対して作成してください。クラスタ拡張時に追加するサーバのクラスタ定義パラメーターの作成は不要です。クラスタ拡張を実行する時に設定します。

クラスタ定義パラメーターがすでに作成されている場合は、内容を確認してください。内容の変更が必要な場合は、編集してください。

ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]-[＜対象のクラスタ＞]-[クラスタ定義パラメーター]タブを選択します。

- ・ 新規に作成する場合
[パラメーターアクション]ボタンから[作成]を選択します。
- ・ 既存のパラメーターを編集する場合
[パラメーターアクション]ボタンから[編集]を選択します。



ポイント

- ・ クラスタ定義パラメーターの作成と編集の操作については、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の詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第3章 クラスタ定義パラメーターの設定値一覧」を参照してください。

6.8.1.9 設置と結線を行う

クラスタ拡張時に追加するサーバの設置と結線を行います。詳細は、クラスタ拡張時に追加するサーバの『オペレーティングマニュアル』を参照してください。ネットワークスイッチの設定に関しては、スイッチのマニュアルを参考にして適切に設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

ISMのノード登録作業時のノード検出方法に応じて以降の作業順番が異なります。

- ・ ノードを手動検出する場合
「6.8.1.10 iRMCのIPアドレスを設定する」を実施してください。
- ・ ノードを自動検出する場合
「6.8.1.12 ISMへノードを登録する」の「自動検出によるノード登録」を実施してください。

6.8.1.10 iRMCのIPアドレスを設定する

クラスタ拡張時に追加するサーバを手動検出でISMにノード登録する場合は、iRMCに固定IPアドレスを設定してください。

クラスタ拡張時に追加するサーバのBIOSを起動して、BIOS設定画面から固定IPアドレスを設定します。この作業を実施するためには、事前に「6.8.1.9 設置と結線を行う」の作業が必要です。また、BIOS画面表示／操作を行うために、クラスタ拡張時に追加するサーバにディスプレイとキーボードを接続してください。

BIOSの起動とiRMCのIPアドレス設定については、クラスタ拡張時に追加するサーバの「BIOSセットアップユーティリティ」のマニュアルを参考してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して設定してください。

また、IPアドレスの設定と同時に「6.8.1.11 BIOSを設定する」も実施してください。

クラスタ拡張時に追加するサーバの「BIOSセットアップユーティリティ」のマニュアルは、以下のサイトから取得できます。

<http://manuals.ts.fujitsu.com/index.php?l=ja>

6.8.1.11 BIOSを設定する

BIOSの設定をします。

「6.8.1.9 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、「6.8.1.10 iRMCのIPアドレスを設定する」と一緒に本項の設定を実施してください。

「6.8.1.9 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。BIOSを起動して、BIOS設定画面で以下を設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

表6.12 BIOS設定

項目		設定値
Server Mgmt - iRMC LAN Parameters Configuration [注1]	iRMC IPv6 LAN Stack	Disabled
Management - iRMC LAN Parameters Configuration [注2]		

[注1]: PRIMERGY RX M4シリーズのBIOS画面に表示される項目です。

[注2]: PRIMERGY CX M4シリーズのBIOS画面に表示される項目です。

「6.8.1.9 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、引き続き「6.8.1.12 ISMへノードを登録する」の「手動検出によるノード登録」を実施してください。

「6.8.1.9 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、引き続き「6.8.2 クラスタ拡張を実行する」を実施してください。

6.8.1.12 ISMへノードを登録する

ISMを使用してOSをインストールするために、クラスタ拡張時に追加するサーバをISMに登録します。

ISMへのノード登録には手動検出機能と自動検出機能が使用できます。クラスタ拡張時に追加するすべてのサーバを登録してください。

ポイント

- ISMのノード登録時は、クラスタ拡張時に追加するサーバのiRMCのユーザー名／パスワードの入力が必要です。ユーザー名／パスワードの初期設定は、それぞれ「admin/admin」です。
- ノード登録の際にノードが所属するノードグループを選択します。ノードグループは、あとからでも編集できます。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が管理できます。
- データセンター、フロアやラックの新規登録、アラーム設定は、必要に応じて設定してください。設定方法は、「第2章 ISMを導入する」を参照してください。
- ノード登録については、『ユーザーズマニュアル』の「2.2.1.2 ノードの登録」や「2.2.1.6 ノードの検出」を参照してください。

手動検出によるノード登録

手動検出によるノード登録の操作方法は、「3.1.2 ノードを直接登録する」を参照してください。

登録の際に指定するIPアドレスは、「6.8.1.10 iRMCのIPアドレスを設定する」で設定したものを指定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、IPアドレスの範囲を指定することで複数台を同時に登録できます。

引続き「6.8.2 クラスタ拡張を実行する」を実施してください。

自動検出によるノード登録

自動検出によるノード登録の操作方法は、「3.1.1 ネットワーク内ノードを検出してノード登録する」を参照してください。

[ノード登録]ウィザードでiRMCの固定IPアドレスを設定してください。

引続き「6.8.1.11 BIOSを設定する」を実施してください。

6.8.2 クラスタ拡張を実行する

クラスタ拡張機能を実行することで仮想化基盤のクラスタを拡張します。

6.8.2.1 クラスタ拡張の動作要件

クラスタ拡張機能を使用するには、以下の動作要件を満たす必要があります。

- 実行する前に以下の要件を確認してください。
 - DNS、NTPが正常に動作し、利用可能なこと
 - お客様環境の既存AD構成時、またはPRIMEFLEX HS V1.0/V1.1／PRIMEFLEX for VMware vSAN V1専用ADVM構成時は、ADが正常に動作し、利用可能なこと
 - ISM-VAにDNSサーバの情報が登録されていること
 - クラスタが正常に動作していること
 - お客様環境の既存AD構成時、ADへのコンピュータ登録がポリシーなどで制限されている場合、クラスタ拡張時に追加するサーバを事前にADへ登録しておくこと
 - クラスタ拡張時に追加するサーバがストレージのネットワークを使用する場合、そのサーバの物理NICが10GbEであること
 - ストレージのネットワークを使用する物理スイッチのポートが10GbEであること
 - [ストレージへのディスクの追加]の設定を確認すること
- 「自動」の場合、vSANストレージへ自動でディスクが追加されます。

「手動」の場合、拡張完了後に手動でディスクの追加作業を行ってください。

設定の確認方法は、vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSAN]-[全般]-[ストレージへのディスクの追加]を選択します。

- ー All Flash構成の環境で[デデュープおよび圧縮]を有効に設定している場合、[ストレージへのディスクの追加]を「手動」に設定すること

[ストレージへのディスクの追加]を「自動」に設定していると、クラスタ拡張機能実行後に「vSANクラスタ構成の一貫性」のvSANの健全性エラーが発生する可能性があります。
- ー PRIMEFLEX HS V1.0/V1.1 / PRIMEFLEX for VMware vSAN V1専用ADVM構成時は、ADVM#1とADVM#2にPRIMEFLEX HS V1.0/V1.1 / PRIMEFLEX for VMware vSAN V1導入サービスの以下のファイルがあること
 - c:\FISCRB\PowerShellScript\fis_advm_ftp_put.ps1
 - c:\FISCRB\PowerShellScript\FIS_JOB_ADVM_SET_DNS_ZONE.ps1
- ー ISMのプロファイル管理機能で、クラスタ拡張時に追加するサーバ用プロファイルが作成されていること
- ー クラスタ定義パラメーターが設定されていること

詳細は、「[6.8.1.8 クラスタ定義パラメーターの作成と編集を行う](#)」を参照してください。
- ー クラスタ拡張時に追加するサーバの電源がオフになっていること

注意

プロファイル適用によるOSインストールが完了している状態で、クラスタ拡張を再実行する場合には、以下の動作要件となります。

- クラスタ拡張時に追加するサーバの電源がオンになっていること

OSインストールが完了している状態かどうかの確認は、以下の手順で確認できます。

1. 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. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」のタスクIDを選択します。
3. サブタスクリストのタスクの結果がすべて「Success」になっていることを確認します。

- ー All Flash構成時、SSDのキャパシティデバイスは以下の条件であること

PRIMEFLEX HS V1.0/V1.1: サイズが160～210GB、320～420GB以外であること

PRIMEFLEX for VMware vSAN V1: キャッシュ、キャパシティ用の2種類のSSDのうち、本数が多い方であること (SSDの本数が同じ場合、容量の大きい方であること)
- ・ 現在のvSANストレージ容量を確認しておいてください。確認方法については、「[6.8.3.1 クラスタ拡張を確認する](#)」を参照してください。
- ・ クラスタ拡張機能を使用するためには、クラスタ拡張対象のクラスタに対して、仮想リソース管理機能の設定が必要です。

仮想リソース管理機能の設定については、『ユーザーズマニュアル』の「3.9 クラスタ管理機能の事前設定」を参照してください。

6.8.2.2 クラスタ拡張手順

ISM for PRIMEFLEXのクラスタ拡張機能の実行手順について説明します。

1. Administrator権限を持ったユーザーでISMにログインします。

ポイント

Administrator権限を持ったユーザーとは

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]-[ユーザーグループ]のユーザーグループリスト画面に表示される「管理対象ノード」が「全てのノードを管理」に設定されているユーザーグループのAdministrator権限を持ったユーザーを表します。

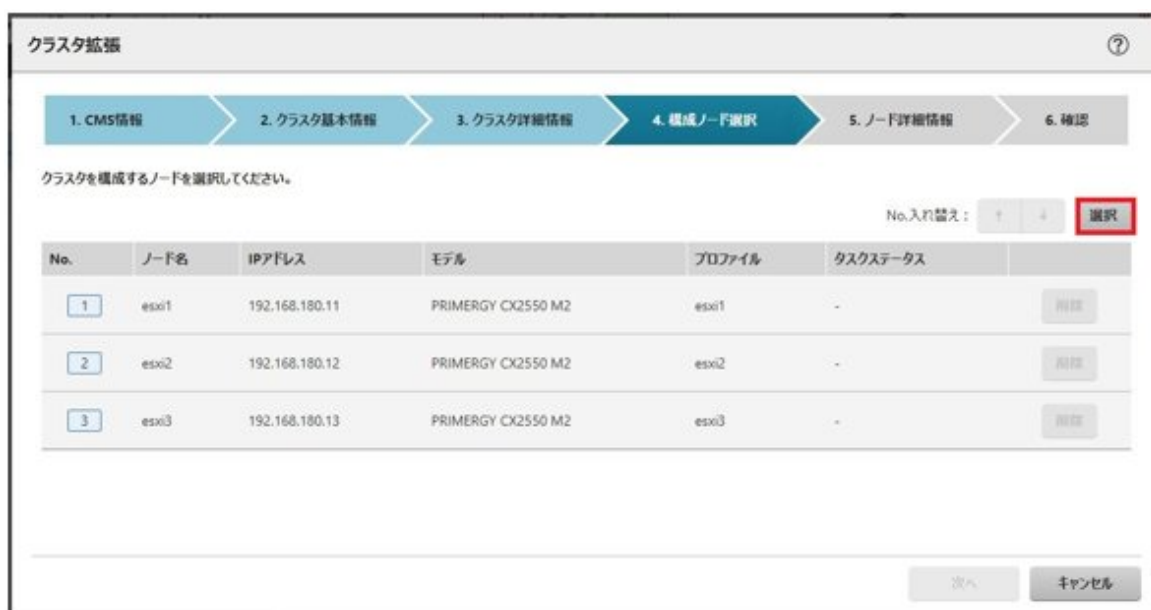
- ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
- [<対象のクラスタ>]を選択して、[アクション]ボタンから[クラスタ拡張]を選択します。



[クラスタ拡張]ウィザードが表示されます。

- 「構成ノード選択」画面の[選択]ボタンを選択して、表示された「対象ノードの選択」画面で、クラスタ拡張時に追加するサーバを選択します。

再実行の場合、本手順は不要です。[次へ]ボタンを選択して、手順6に進んでください。



- クラスタ拡張時に追加するサーバがプロファイル未適用の場合は、[プロファイル]の項目にある[選択]ボタンを選択して、適用対象のプロファイルを選択します。

6. 「ノード詳細情報」画面でクラスタ拡張時に追加するサーバの各種パラメーターを入力します。
- 再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順7に進んでください。

注意

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』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

7. 「確認」画面でパラメーターを確認し、[実行]ボタンを選択します。

ISM 2.3.0.a以前の場合

ISM 2.3.0.b以降の場合

クラスタ拡張

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

☐ 1 の値を増設対象のノードにも適用

IRMC OS vDS

IRMC設定情報を入力してください。

No.	ノード名	ローカルユーザー設定	管理ユーザー
1	esxi1	adminユーザー	管理ユーザー
		パスワード	ユーザー名 *
			pflocaladmin
		パスワード(確認)	パスワード *
			パスワード(確認) *

戻る 次へ キャンセル

クラスタ拡張の実行は、ISMのタスクとして登録されます。

グローバルナビゲーションメニュー 上部の[タスク]を選択して表示される「タスク」画面のタスクリストで、タスクタイプが「Cluster Expansion」となっているのが、クラスタ拡張のタスクです。

タスク

タスクリスト 次の自動更新まで: 9 秒 停止 更新

検索 572 / 572 (表示上限 最新 1000件) フィルター アクション

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	0:32:21	489	Assigning profile	pfadmin	2018/04/21 19:43:26	2018/04/21 20:15:48
完了	Success	0:57:14	488	Cluster Expansion	pfadmin	2018/04/21 19:43:26	2018/04/21 20:40:41
完了	Success	0:00:01	487	Releasing profile	pfadmin	2018/04/21 19:42:13	2018/04/21 19:42:14
完了	Success	0:32:51	486	Assigning profile	pfadmin	2018/04/21 19:02:44	2018/04/21 19:35:35
キャンセル完了	Success	-	485	Cluster Expansion	pfadmin	2018/04/21 19:02:43	2018/04/21 19:36:52

閉じる

P ポイント

「タスク」画面のタスクリストから「Cluster Expansion」の[タスクID]を選択すると、「Cluster Expansion」の「タスク」画面が表示されます。この画面では、クラスタ拡張時に追加するサーバごとにサブタスクリストが表示されるので、メッセージ欄を確認することでタスクの進行状況を確認できます。

タスク

タスクリスト > 488

次の自動更新まで: 9 秒

停止 アクション ▼ 更新

タスク情報

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
完了	Success	0:57:14	488	Cluster Expansion	pfadmin	2018/04/21 19:43:26	2018/04/21 20:40:41

サブタスクリスト

ステータス	進捗	経過時間	サブタスクID	ノード名	完了時間	メッセージ
完了	Success	0:57:14	575	node4	2018/04/21 20:40:41	Subtask complete

閉じる

8. 「Cluster Expansion」のステータスが「完了」になったことを確認します。



注意

- ISMの「タスク」画面にエラーが表示された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。問題が解決できたら再度操作を行ってください。

ISMのプロファイル管理機能によるOSインストール (Assigning profileタスク) が正常終了している場合、再実行時にはクラスタ拡張時に追加するサーバの電源はオフにしないでください。

- クラスタ拡張時に追加するサーバの業務用仮想ネットワークの設定は、お客様環境に応じて設定してください。
- ファームウェアローリングアップデート機能を実行中にクラスタ拡張機能を実行しないでください。

6.8.3 事後処理

クラスタ拡張の事後処理について説明します。

6.8.3.1 クラスタ拡張を確認する

以下の手順でvSANへのクラスタ拡張を確認してください。

- vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[物理ディスク]でクラスタ拡張時に追加したサーバのディスクが表示されることを確認します。

[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[健全性]で再テストを実施し、問題のないことを確認します。

パフォーマンスサービスの統計DBオブジェクトに警告が出る場合がありますが、無視してください。



ポイント

健全性エラーが存在する場合、該当エラーの詳細を確認したうえで解決してください。

vSAN6.6.1環境 (VMware ESXi 6.5 Update 1) の場合、健全性エラーと対処方法は以下のとおりです。

ー vSAN ディスクバラン

ディスクのプロアクティブリバランスを実施してください。

- ー コントローラドライバがVMwareにより認定済み
対象ホストで推奨されているSASコントローラーのドライバを適用してください。
- ー コントローラファームウェアがVMwareにより認定済み
対処は不要です。sas3flashコントローラーのファームウェアバージョンを取得するVIBがインストールされていないため警告が表示されます。カスタムイメージには、このVIBは含まれていないので想定内です。
- ー vSAN ビルドに関する推奨事項エンジンの健全性
ネットワーク接続を復旧してください。

注意

- ー [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[フォールトドメインおよびストレッチクラスタ]-[フォールトドメイン]でクラスタ拡張時に追加するサーバのフォールトドメインホストを確認します。
1つのフォールトドメインに複数のホストが設定されている場合、プロファイルの[OS個別情報]-[ネットワーク]-[DHCP]-[コンピュータ名をDNSサーバから取得]-[コンピュータ名]が既存クラスタを構成するサーバのコンピュータ名と重複していないか確認してください。確認の結果、重複している場合、『ISM for PRIMEFLEX メッセージ集』の「3.14 クラスタ拡張エラー時の対処例」の「対処例19」を参照して、対処してください。
 - ー [ストレージへのディスクの追加]の設定が「手動」になっている場合は[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[監視]-[vSAN]-[物理ディスク]でクラスタ拡張時に追加したサーバのディスクは表示されません。
手動でディスクの追加作業を行ってください。
設定の確認方法は、vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSAN]-[全般]-[ストレージへのディスクの追加]を選択します。
手動でディスクを追加するには、以下の手順で設定します。クラスタ拡張時に追加するすべてのサーバに対して実施してください。
 1. vSphere Web ClientでvCSAにログインします。
 2. [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[ディスク管理]を選択します。
 3. クラスタ拡張時に追加するサーバを選択して、[新規ディスクグループの作成]を選択します。
 4. 「ディスクグループの作成」画面で、「キャッシュ層として使用するディスク」と「キャパシティ層として使用するディスク」を選択して、[OK]ボタンを選択します。
 タスクが完了するとディスクの追加作業が完了します。
2. ISMのGUIにアクセスして、[管理]-[仮想リソース]の「全てのストレージプール」画面で[アクション]-[仮想リソース情報の更新]を実行して更新します。更新後、対象のvSANデータストアの[容量]が増加していることを確認します。

プール名	使用率	10 日前	20 日前	30 日前	種類	容量
vsanDatastore	68.59% ↑	-	-	-	VMware Virtual SAN	9.01TB

注意

タスクが正常に完了したにも関わらず、事前に確認したvSANストレージの容量から増加していない場合、以下が考えられます。

- ー vSANネットワーク用の通信ができていない
スイッチの設定や結線を確認してください。
- ー [ストレージへのディスクの追加]の設定が「手動」になっている
手動でディスクの追加作業を行ってください。

設定の確認方法は、vSphere Web Clientにアクセスして、[トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[vSAN]-[全般]-[ストレージへのディスクの追加]を選択します。

手動でディスクを追加するには、以下の手順で設定します。クラスタ拡張時に追加するすべてのサーバに対して実施してください。

1. vSphere Web ClientでvCSAにログインします。
2. [トップ画面]-[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]の[<クラスタ名>]-[設定]-[ディスク管理]を選択します。
3. クラスタ拡張時に追加するサーバを選択して、[新規ディスクグループの作成]を選択します。
4. 「ディスクグループの作成」画面で、「キャッシュ層として使用するディスク」と「キャパシティ層として使用するディスク」を選択して、[OK]ボタンを選択します。

タスクが完了するとディスクの追加作業が完了します。

拡張されていることを確認するため、現在のvSANストレージ容量を確認しておいてください。

6.8.3.2 VMware vSphereの制限事項／注意事項

以下のサイトを参照して『VMware vSphere ソフトウェア説明書 (PRIMERGY)』を熟読し、お客様の環境に該当する制限事項に対処してください。

クラスタ拡張時に追加するすべてのサーバに対して実施してください。

<http://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/>

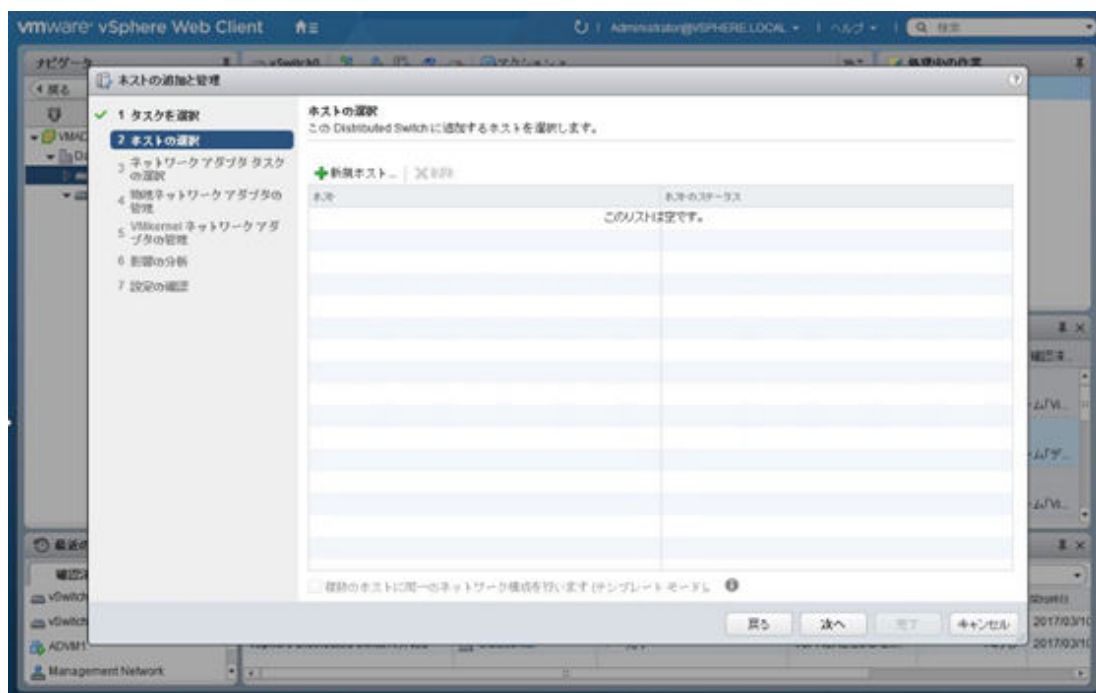
6.8.3.3 業務用仮想分散スイッチに登録する

本手順は、PRIMEFLEX HS V1.0/V1.1版のPRIMERGY RXシリーズ、およびPRIMEFLEX for VMware vSAN V1版のPRIMERGY CX/RXシリーズで構成された環境の場合に必要な手順です。ISM for PRIMEFLEX V2.2.0.c.1以降の場合は、本手順は不要です。

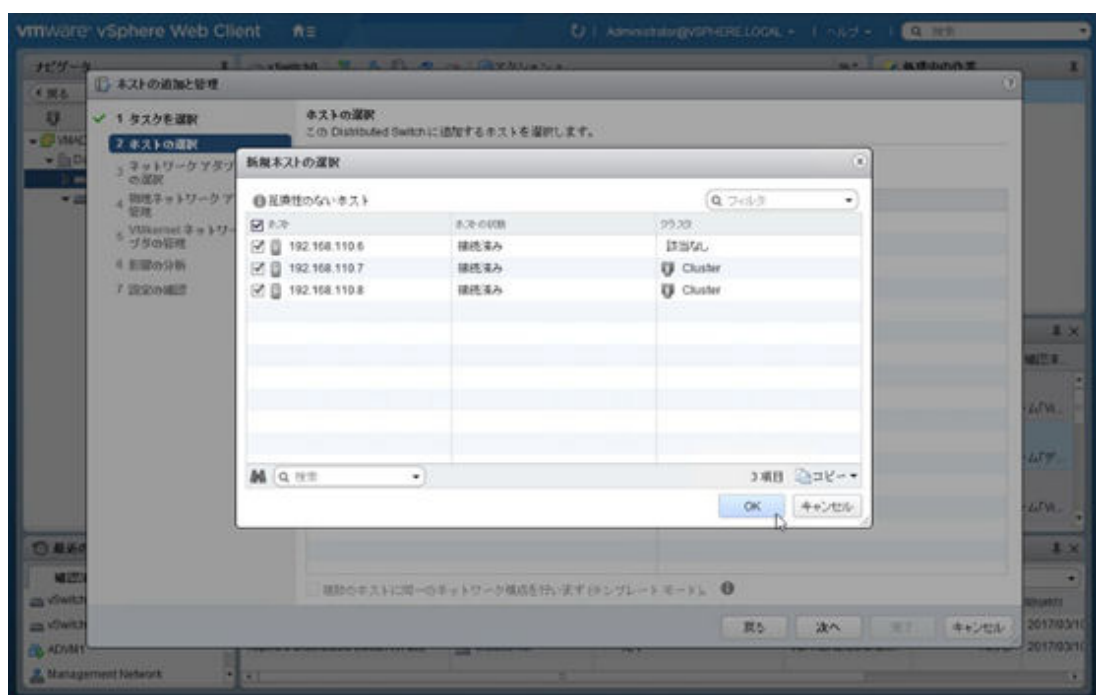
クラスタ拡張時に追加するすべてのサーバに対して実施してください。

1. vSphere Web ClientでvCSAにログインします。
2. ホーム画面内より[ネットワーク]を選択後、業務用のvDS(仮想分散スイッチ)を右クリックしてから、[ホストの追加と管理]を選択します。
3. 「タスクを選択」画面で、[ホストの追加]を選択し、[次へ]を選択します。

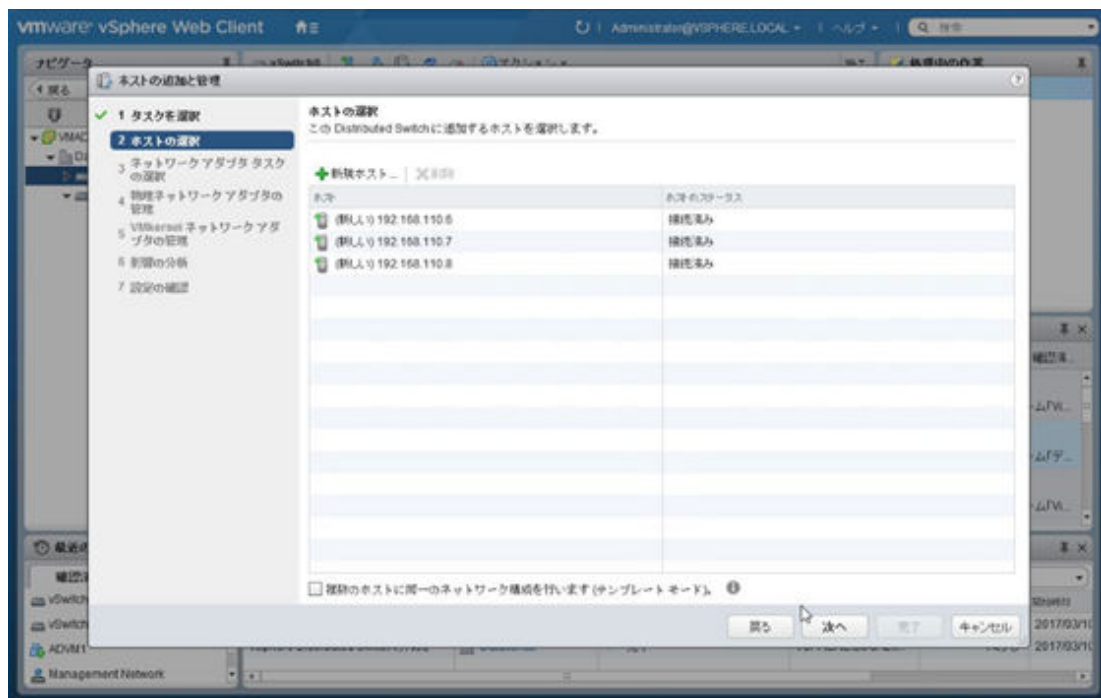
4. 「ホストの選択」画面で、[新規ホスト]を選択します。



5. 「新規ホストの選択」画面で、クラスタ拡張時に追加するサーバすべてにチェックを付けて、[OK]ボタンを選択します。



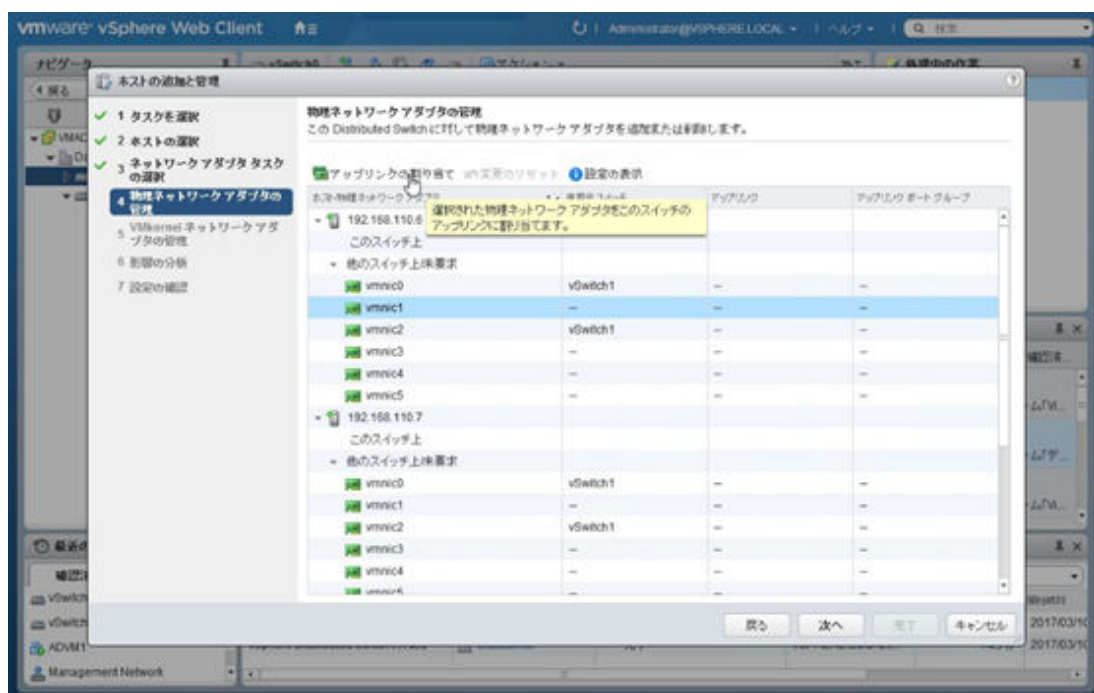
6. 「ホストの選択」画面に、クラスタ拡張時に追加するサーバがすべて表示されたことを確認し、[次へ]ボタンを選択します。



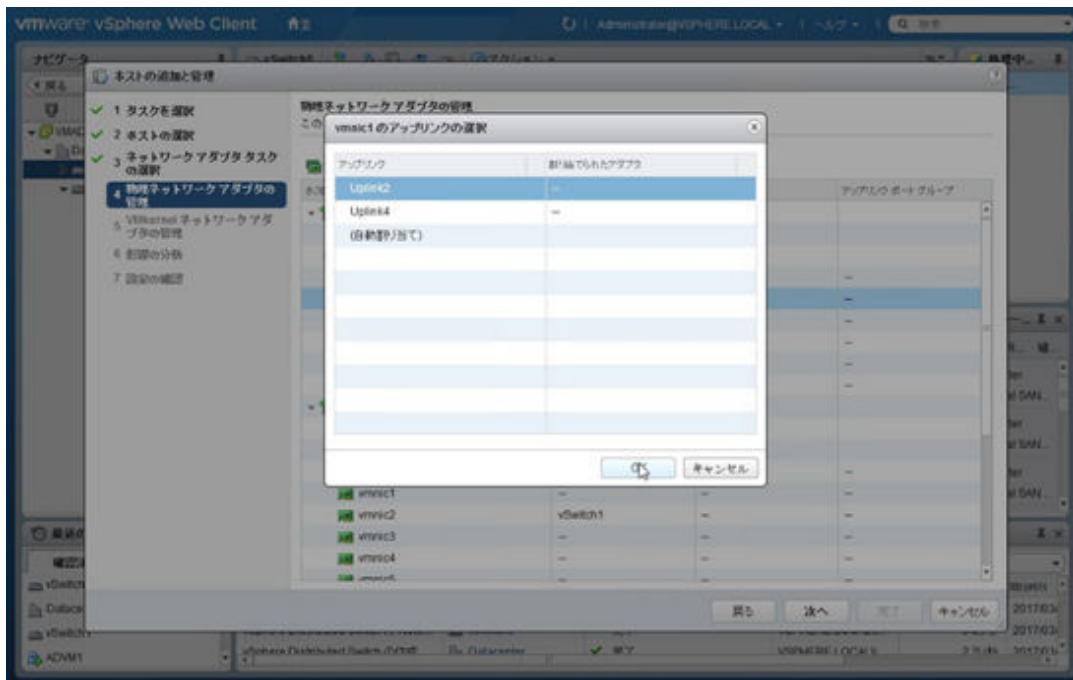
7. 「ネットワークアダプタタスクの選択」画面で、[次へ]ボタンを選択します。
 8. クラスタ拡張時に追加するサーバのうち1つを選び、その配下から業務系ポート#1として設定するvmnicを選択します。

項目	設定値
業務系ポート#1のvmnic	管理系ポート#1のvmnic番号+1 例: 管理系ポート#1がvmnic0の場合、vmnic1

9. [アップリンクの割り当て]を選択します。



10. 「vmnicのアップリンクの選択」画面で、「Uplink2」を選択し、[OK]ボタンを選択します。



11. 手順8と同じサーバの配下から、業務系ポート#2として設定するvmnicを選択します。

項目	設定値
業務系ポート#2のvmnic	管理系ポート#2のvmnic番号+1 例: 管理系ポート#2がvmnic2の場合、vmnic3

12. [アップリンクの割り当て]を選択します。
13. 「vmnicのアップリンクの選択」画面で、「Uplink4」を選択し、[OK]ボタンを選択します。
14. クラスタ拡張時に追加するすべてのサーバに対して、手順8～13を繰り返します。

6.8.3.5 証明書を削除する

「6.8.1.1 ADVmの証明書を作成する」で作成した証明書は、登録後は不要です。



「6.8.1.1 ADVmの証明書を作成する」でADV#1とADV#2にアップロードした証明書はセキュリティリスクが生じます。セキュリティリスクが承知できない場合は、削除してください。

6.9 PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタを拡張する

PRIMEFLEX for Microsoft Storage Spaces Directでのクラスタ拡張手順について説明します。

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

クラスタ拡張は、以下の作業フローで行います。

表6.13 拡張フロー

クラスタ拡張手順		作業内容
1	事前準備	<ul style="list-style-type: none">・ クラスタ拡張時に追加するサーバの証明書作成・ DHCPの設定・ OSインストール媒体のISOイメージをISM-VAへインポート・ プロファイルの作成・ クラスタ定義パラメーターの作成と編集・ 設置と結線・ iRMCのIPアドレス設定・ BIOSの設定・ システムディスク(RAID1)の作成・ ISMへノード登録
2	クラスタ拡張の実行	
3	事後処理	<ul style="list-style-type: none">・ クラスタ情報の取得と更新・ クラスタ拡張確認・ 業務用仮想スイッチへの登録・ システムボリューム名の設定・ ブラウザの設定・ 証明書削除・ 不要ファイルの削除

6.9.1 事前準備

クラスタ拡張を行う前の準備作業について説明します。

6.9.1.1 クラスタ拡張時に追加するサーバの証明書を作成する

クラスタ拡張機能は、クラスタ拡張時に追加するサーバに対してISMからSSL暗号化通信で設定を行うため、証明書の作成と登録が必要です。

(1) 証明書の作成

管理端末から証明書作成ツール(makecert.exe)、個人情報交換ファイル作成ツール(pvk2pfx.exe)を使用し、以下の3つのファイルを作成します。

- ー CERファイル(証明書)
- ー PVKファイル(秘密鍵ファイル)
- ー PFXファイル(サービス証明書)

(1-1) 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。

- .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>



- 上記ツールは管理端末にインストールしてください。
- 上記URLの.NET Framework 4.5は、証明書を作成するための管理端末の言語に合わせてダウンロードしてください。
- 上記URLのWindows Software Development Kitは、Windows 8.1およびWindows Server 2012以降の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 10以外のプラットフォームでは、Windows 10 SDKを使用する際に、Universal CRTがインストールされている必要があります (KB2999226 (<https://support.microsoft.com/ja-jp/help/2999226/update-for-universal-c-runtime-in-windows>)) を参照)。セットアップ中にエラーが発生しないようにするために、Windows SDKをインストールする前に、推奨される最新の更新プログラムとパッチをMicrosoft Updateから必ずインストールしてください。

(1-2) 証明書、秘密鍵ファイルの作成

管理端末のコマンドプロンプト(管理者)から以下のコマンドを実行します。

クラスタ拡張時に追加するサーバ名を「192.168.10.10」、証明書の有効期間を「2018年3月30日」に設定する場合のコマンド例です。

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2018 -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>
```

途中、証明書にセットするパスワードを2回要求されますので、間違えずに入力してください。間違えた場合は、上記コマンドを実行してやり直してください。

(1-3) サービス証明書の作成

管理端末のコマンドプロンプト(管理者)から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>
```

途中、(1-2)でセットしたパスワードを要求されますので、入力してください。



- ー クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して証明書を作成してください。
- ー 証明書のファイル名は、「ISMのプロファイルに設定するコンピュータ名」を指定してください。

例)

- hv-host4.cer

- hv-host4.pfx

(2) 証明書の登録

証明書の登録は、OSインストール時にOS設定スクリプトで実行されます。

(1)で作成した証明書は、FTPでISM-VAにアクセスして以下にアップロードしてください。

/Administrator/ftp/postscript_ClusterOperation/

FTP接続の方法は、「[8.1.3 ISMをリストアする](#)」の手順3を参照し、本環境に読み替えて実施してください。

6.9.1.2 DHCPを設定する

クラスタ拡張機能ではプロファイル適用を使用してOSのインストール作業を実施します。プロファイル適用によるOSインストールを実行するためには、DHCPサーバが必要です。

ISM-VAは内部でDHCPサーバ機能を持っていますが、ISM-VA外部にDHCPサーバを用意して使用することもできます。内部DHCPを使用する場合は、『ユーザーズマニュアル』の「[4.15 ISM-VA内部のDHCPサーバ](#)」を参照して設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、複数台分リースできるように設定してください。



注意

- 使用するDHCPサービスが起動していることを確認してください。
- DHCPサーバが同一ネットワーク内で複数起動している場合は、正確に機能しない場合があります。使用しないDHCPサービスは必ず停止してください。
- リース期間は作業中に期限が切れないように設定してください。
- 本製品の構成では、管理ネットワークを冗長しているため、複数ポートにIPアドレスがリースされます。リースするIPアドレスが不足しないように設定してください。
- ISMが内部／外部どちらのDHCPを使用する設定になっているか確認して、お客様が使用するDHCPの設定に合わせて変更してください。変更方法は、『ユーザーズマニュアル』の「[4.15.4 DHCPサーバの切替え](#)」を参照してください。

6.9.1.3 OSインストール媒体のISOイメージをISM-VAへインポートする

ISMにServerView Suite DVD Installation (DVD 1)と、OSのインストールメディアをインポートします。

既存のものを使用する場合は、インポートの必要はありません。

インポートの操作については、『ユーザーズマニュアル』の「[2.13.2 リポジトリ管理機能](#)」を参照してください。

また、サポート版数は、『プロファイル管理機能 プロファイル設定項目集』を参照してください。

必要に応じてISM-VAの仮想ディスクを追加してください。仮想ディスク追加方法は、『ユーザーズマニュアル』の「[3.7 仮想ディスクの割当て](#)」を参照してください。

6.9.1.4 プロファイルを作成する

ISMのプロファイル管理機能を使用して、クラスタ拡張時に追加するサーバのプロファイルを作成します。既存のプロファイルから参照作成して、プロファイルを作成してください。



注意

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対してプロファイルを作成してください。

- ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
- 参照作成元とする既存のプロファイルを選択し、[アクション]ボタンから[参照作成]を選択します。

3. 各項目を設定します。

BIOSポリシー、iRMCポリシーは既存のものを指定します。

プロファイル作成については、「[3.3 サーバに各種設定／OSインストールをする](#)」を参照してください。

注意

- ー 以下の項目には、チェックを付けないでください。
 - [OS]タブの[インストール後のスクリプト実行]
 - [OS個別情報]タブの[DHCP]
- ー 以下の項目は、重複しないように設定してください。
 - [OS個別情報]タブの[コンピュータ名]
 - [OS個別情報]タブの[ネットワーク]-[DHCP]-[IPアドレス]

6.9.1.5 クラスタ定義パラメーターの作成と編集を行う

ISMのGUIを使用して、必要に応じてクラスタ定義パラメーターの作成と編集を行います。

拡張するクラスタに対してクラスタ定義パラメーターを作成してください。拡張するクラスタが複数ある場合は、すべてのクラスタに対して作成してください。クラスタ拡張時に追加するサーバのクラスタ定義パラメーターの作成は不要です。クラスタ拡張を実行する時に設定します。

クラスタ定義パラメーターがすでに作成されている場合は、内容を確認してください。内容の変更が必要な場合は、編集してください。

ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]-[<対象のクラスタ>]-[クラスタ定義パラメーター]タブを選択します。

- ・ 新規に作成する場合
[パラメーターアクション]ボタンから[作成]を選択します。
- ・ 既存のパラメーターを編集する場合
[パラメーターアクション]ボタンから[編集]を選択します。

ポイント

- ・ クラスタ定義パラメーターの作成と編集の操作については、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の詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

6.9.1.6 設置と結線を行う

クラスタ拡張時に追加するサーバの設置と結線を行います。詳細は、クラスタ拡張時に追加するサーバの『オペレーティングマニュアル』を参照してください。ネットワークスイッチの設定に関しては、スイッチのマニュアルを参考にして適切に設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

ISMのノード登録作業時のノード検出方法に応じて以降の作業順番が異なります。

- ・ ノードを手動検出する場合
「[6.9.1.7 iRMCのIPアドレスを設定する](#)」を実施してください。
- ・ ノードを自動検出する場合
「[6.9.1.10 ISMへノードを登録する](#)」の「自動検出によるノード登録」を実施してください。

6.9.1.7 iRMCのIPアドレスを設定する

クラスタ拡張時に追加するサーバを手動検出でISMにノード登録する場合は、iRMCに固定IPアドレスを設定してください。

クラスタ拡張時に追加するサーバのBIOSを起動して、BIOS設定画面から固定IPアドレスを設定します。この作業を実施するためには、事前に「6.9.1.6 設置と結線を行う」の作業が必要です。また、BIOS画面表示／操作を行うために、クラスタ拡張時に追加するサーバにディスプレイとキーボードを接続してください。

BIOSの起動と、iRMCのIPアドレス設定については、クラスタ拡張時に追加するサーバの「BIOSセットアップユーティリティ」のマニュアルを参考にしてください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して設定してください。

また、IPアドレスの設定と同時に「6.9.1.8 BIOSを設定する」も実施してください。

クラスタ拡張時に追加するサーバの「BIOSセットアップユーティリティ」のマニュアルは、以下のサイトから取得できます。

<http://manuals.ts.fujitsu.com/index.php?l=ja>

6.9.1.8 BIOSを設定する

BIOSの設定をします。

「6.9.1.6 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、「6.9.1.7 iRMCのIPアドレスを設定する」と一緒に本項の設定を実施してください。

「6.9.1.6 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。BIOSを起動して、BIOS設定画面で以下を設定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

表6.14 BIOS設定

項目		設定値
Main	System Date	ローカル日時
	System Time	ローカル日時
Advanced - Network Stack Configuration	Network Stack	Enabled
	IPv4 PXE Support	Enabled
	IPv6 PXE Support	Disabled
Security - Security Boot Configuration	Secure Boot Control	Enabled
Server Mgmt - iRMC LAN Parameters Configuration	IP Configuration	Use static configuration
	iRMC IPv6 LAN Stack	Disabled



注意

BIOSの設定が完了したら、BIOS画面の[Save & Exit]タブの「Save Changes and Exit」を実施し、それから数分後に電源を停止してください。

引続き「6.9.1.9 システムディスク(RAID1)を作成する」を実施してください。

6.9.1.9 システムディスク(RAID1)を作成する

PRIMERGYのUEFI画面で、システムディスクとして使用するロジカルディスク(HDD2本をRAID1で構築)を作成します。

クラスタ拡張時に追加するサーバが複数台ある場合は、クラスタ拡張時に追加するすべてのサーバに対して実施してください。

1. iRMCのビデオリダイレクション機能を使用して、リモートでBIOSの設定が可能です。クラスタ拡張時に追加するサーバの電源をONにします。ビデオリダイレクションのメニューから、[電源(Power)] - [電源投入(Power ON)]を選択します。
2. BIOS (UEFI) 起動画面で[F2]キーを押します。

UEFIのセットアップ画面が表示されます。

3. [Advanced]タブを選択し、「LSI SAS3 MPT Controller SAS3008」を選択して[Enter]キーを押します。
4. 「LSI SAS3 MPT Controller X.XX.XX.XX」を選択し、[Enter]キーを押します。
5. 「Controller Management」を選択し、[Enter]キーを押します。
6. 「Create Configuration」を選択し、[Enter]キーを押します。
7. 「Select RAID level」で「RAID 1」を選択し、「Select Physical Disks」を選択して[Enter]キーを押します。
8. 「Select Interface Type」で用意したシステムディスクのタイプを選択します。
9. 「Select Media Type」でシステムディスクのメディア (HDD) を選択します。
「Select Media Type」に表示されたディスクの中からお客様が購入されたOSブート用のシステムディスクを2本選択します。
10. システムディスクとするディスク2本を「Enabled」に変更し、「Apply Changes」を選択して[Enter]キーを押します。
11. 確認画面が表示されますので、「Confirm」を「Enabled」に変更後、「Yes」を選択して[Enter]キーを押します。
12. 「Operation completed successfully」で「OK」を選択し、[Enter]キーを押します。
13. [Esc]キーを複数回押し、「Exit Without Saving」で「Yes」を選択し、[Enter]キーを押します。
14. サーバの電源をオフにします。ビデオリダイレクションのメニューから、[電源(Power)] - [電源切断(Immediate Power Off)]を選択します。

「6.9.1.6 設置と結線を行う」で「ノードを手動検出する場合」を選択している場合は、引き続き「6.9.1.10 ISMへノードを登録する」の「手動検出によるノード登録」を実施してください。

「6.9.1.6 設置と結線を行う」で「ノードを自動検出する場合」を選択している場合は、引き続き「6.9.2 クラスタ拡張を実行する」を実施してください。

6.9.1.10 ISMへノードを登録する

ISMを使用してOSをインストールするために、クラスタ拡張時に追加するサーバをISMに登録します。

ISMへのノード登録には手動検出機能と自動検出機能が使用できます。クラスタ拡張時に追加するすべてのサーバを登録してください。

ポイント

- ISMのノード登録時は、クラスタ拡張時に追加するサーバのiRMCのユーザー名／パスワードの入力が必要です。ユーザー名／パスワードの初期設定は、それぞれ「admin/admin」です。
- ノード登録の際にノードが所属するノードグループを選択します。ノードグループは、あとからでも編集できます。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が管理できます。
- データセンター、フロアやラックの新規登録、アラーム設定は、必要に応じて設定してください。設定方法は、「第2章 ISMを導入する」を参照してください。
- ノード登録については、『ユーザーズマニュアル』の「2.2.1.2 ノードの登録」や「2.2.1.6 ノードの検出」を参照してください。

手動検出によるノード登録

手動検出によるノード登録の操作方法は、「3.1.2 ノードを直接登録する」を参照してください。

登録の際に指定するIPアドレスは、「6.9.1.7 iRMCのIPアドレスを設定する」で設定したものを指定してください。

クラスタ拡張時に追加するサーバが複数台ある場合は、IPアドレスの範囲を指定することで複数台を同時に登録できます。

引き続き「6.9.2 クラスタ拡張を実行する」を実施してください。

自動検出によるノード登録

自動検出によるノード登録の操作方法は、「3.1.1 ネットワーク内ノードを検出してノード登録する」を参照してください。

[ノード登録]ウィザードでiRMCの固定IPアドレスを設定してください。

引き続き「6.9.1.8 BIOSを設定する」を実施してください。

6.9.2 クラスタ拡張を実行する

クラスタ拡張機能を実行することで仮想化基盤のクラスタを拡張します。

6.9.2.1 クラスタ拡張の動作要件

クラスタ拡張機能を使用するには、以下の動作要件を満たす必要があります。

- ・ 実行する前に以下の要件を確認してください。
 - － AD、DNS、NTPが正常に動作し、利用可能なこと
 - － ISM-VAにDNSサーバの情報が登録されていること
 - － クラスタが正常に動作していること
 - － お客様環境の既存AD構成時、ADへのコンピュータ登録がポリシーなどで制限されている場合、クラスタ拡張時に追加するサーバを事前にADへ登録しておくこと
 - － クラスタ拡張時に追加するサーバにIntel、またはMellanoxのEthernetアダプターが装着されていること
 - － Ethernetアダプターは10G以上で通信できること
 - － クラスタ拡張時に追加するサーバのBIOS設定値が「[6.9.1.8 BIOSを設定する](#)」どおりに設定されていること
 - － PRIMEFLEX for Microsoft Storage Spaces Directの仮想ネットワークの構成が以下のとおりになっていること

設定項目	設定値
Switch Embedded Teaming	vSwitch0
	vSwitch1
Virtual Network Adapter	<ul style="list-style-type: none">• vEthernet (Management)• vEthernet (Storage_1)• vEthernet (Storage_2)

PRIMEFLEX for Microsoft Storage Spaces Directの仮想ネットワークの構成は、以下の手順で確認できます。

1. クラスタ代表IP(クラスタアクセスポイント)にリモートデスクトップ接続します。
2. 管理者権限でコマンドプロンプトからPowerShellを開いて、以下の2つのコマンドを実行します。

```
>Get-VMSwitchTeam
```

```
>Get-NetAdapter
```

3. 「Name」に設定値が出力されることを確認します。

- － PRIMEFLEX for Microsoft Storage Spaces Directのデバイス構成が以下のとおりになっていること

デバイス	初期値	用途
PCIカード1 (Port1)、PCIカード2 (Port1)	vSwitch0	業務 (Production) LAN
PCIカード1 (Port0)、PCIカード2 (Port0)	vSwitch1	管理 (Management) LAN Storage_1 LAN、Storage_2 LAN (フェイルオーバークラスタのハートビート、ライブマイグレーション用)

PRIMEFLEX for Microsoft Storage Spaces Directのデバイス構成は、以下の手順で確認できます。

1. クラスタ代表IP(クラスタアクセスポイント)にリモートデスクトップ接続します。

2. 管理者権限でコマンドプロンプトからPowerShellを開いて、以下のコマンドを実行します。

```
>Get-VMSwitchTeam
```

3. 「Name」と「NetAdapterInterfaceDescription」がデバイス構成になっていることを確認します。

- ー 仮想ディスクの「正常性の状態」が正常になっていること

仮想ディスクの「正常性の状態」は、以下の手順で確認できます。

1. クラスタ代表IP(クラスタアクセスポイント)にリモートデスクトップ接続します。
2. 管理者権限でコマンドプロンプトからPowerShellを開いて、以下のコマンドを実行します。

```
>Get-Virtualdisk
```

3. 「HealthStatus」が"Healthy"になっていることを確認します。

- ー ISMのプロファイル管理機能で、クラスタ拡張時に追加するサーバ用プロファイルが作成されていること
- ー クラスタ定義パラメーターが設定されていること
詳細は、「[6.9.1.5 クラスタ定義パラメーターの作成と編集を行う](#)」を参照してください。
- ー クラスタ拡張時に追加するサーバの電源がオフになっていること

注意

プロファイル適用によるOSインストールが完了している状態で、クラスタ拡張を再実行する場合には、以下の動作要件となります。

- クラスタ拡張時に追加するサーバの電源がオンになっていること

OSインストールが完了している状態かどうかの確認は、以下の手順で確認できます。

1. 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. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」のタスクIDを選択します。
3. サブタスクリストのタスクの結果がすべて「Success」になっていることを確認します。

- ・ 現在のPRIMEFLEX for Microsoft Storage Spaces Directストレージ容量を確認しておいてください。確認方法については、「[6.9.3.2 クラスタ拡張を確認する](#)」を参照してください。
- ・ クラスタ拡張機能を使用するためには、対象のクラスタに対して、仮想リソース管理機能の設定が必要です。
仮想リソース管理機能の設定については、『ユーザーズマニュアル』の「3.9 クラスタ管理機能の事前設定」を参照してください。

6.9.2.2 クラスタ拡張手順

ISM for PRIMEFLEXのクラスタ拡張機能の実行手順について説明します。

1. Administrator権限を持ったユーザーでISMにログインします。

ポイント

Administrator権限を持ったユーザーとは

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]-[ユーザーグループ]のユーザーグループリスト画面に表示される「管理対象ノード」が「全てのノードを管理」に設定されているユーザーグループのAdministrator権限を持ったユーザーを表します。

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]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。

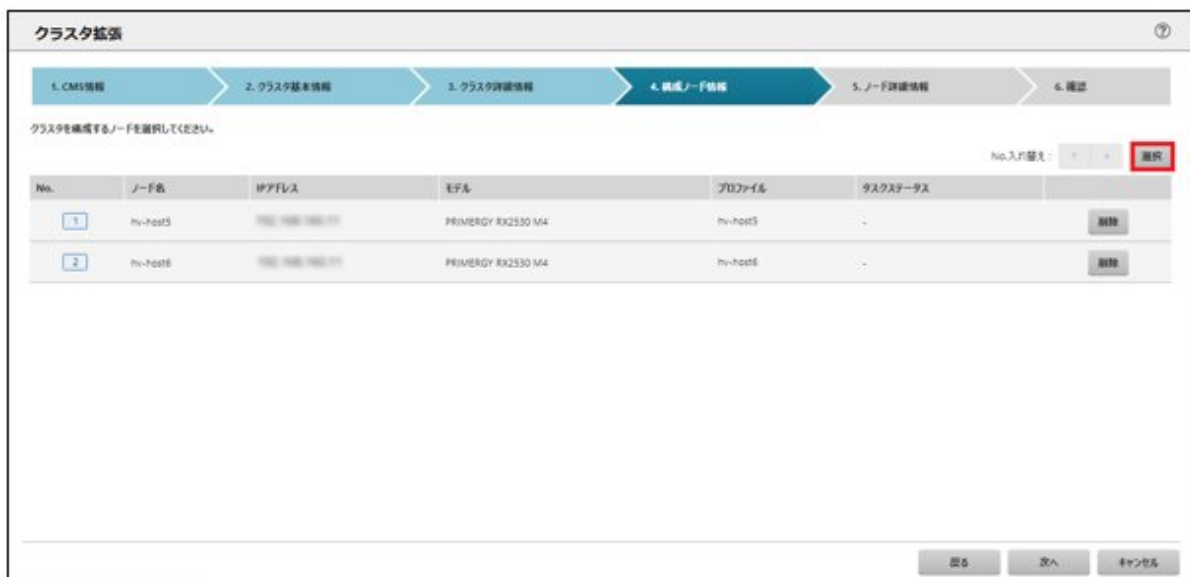
3. [対象のクラスタ]を選択して、[アクション]ボタンから[クラスタ拡張]を選択します。



[クラスタ拡張]ウィザードが表示されます。

4. 「構成ノード情報」画面の[選択]ボタンを選択して、表示された「対象ノードの選択」画面で、クラスタ拡張時に追加するサーバを選択します。

再実行の場合、本手順は不要です。[次へ]ボタンを選択して、手順6に進んでください。



5. クラスタ拡張時に追加するサーバがプロファイル未適用の場合は、[プロファイル]の項目にある[選択]ボタンを選択して、適用対象のプロファイルを選択します。

6. 「ノード詳細情報」画面でクラスタ拡張時に追加するサーバの各種パラメーターを入力します。
- 再実行の場合、パラメーターの再入力が必要であれば、[次へ]ボタンを選択して、手順7に進んでください。

注意

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』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

7. 「確認」画面でパラメーターを確認し、[実行]ボタンを選択します。

ISM 2.3.0.a以前の場合

ISM 2.3.0.b以降の場合

クラスタ拡張

1. CMS情報 2. クラスタ基本情報 3. クラスタ詳細情報 4. 構成ノード選択 5. ノード詳細情報 6. 確認

基本情報 DNS LDAP ネットワーク ストレージプール 構成ノード iSCSI OS 仮想スイッチ

クラスタ名: Cluster-S2D

戻る 実行 キャンセル

クラスタ拡張の実行は、ISMのタスクとして登録されます。

グローバルナビゲーションメニュー 上部の[タスク]を選択して表示される「タスク」画面のタスクリストで、タスクタイプが「Cluster Expansion」となっているのが、クラスタ拡張のタスクです。

タスク

タスクリスト 自動更新が設定されていません 開始 更新

検索 8 / 8 (表示上限 最新 1000件) フィルター アクション

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
進行中	1 / 300	0:00:20	8	Assigning profile	pfadmin	2018/05/21 18:11:39	-
進行中	1 / 24	0:00:21	7	Cluster Expansion	pfadmin	2018/05/21 18:11:38	-
完了	Success	0:00:58	6	Refresh Virtual Resource	administrator	2018/05/20 13:39:21	2018/05/20 13:40:20
完了	Success	0:00:34	5	Refresh Virtual Resource	administrator	2018/05/20 13:39:16	2018/05/20 13:39:51
完了	Success	0:00:27	4	Refresh Virtual Resource	administrator	2018/05/20 13:29:37	2018/05/20 13:30:05
完了	Success	1:24:50	3	Assigning profile	administrator	2018/05/19 17:12:10	2018/05/19 18:37:00
完了	Success	0:01:46	2	Importing OS DVD	administrator	2018/05/19 16:57:04	2018/05/19 16:58:50

閉じる

8. 「タスク」画面のタスクリストからタスクタイプが「Assigning profile」の[タスクID]を選択します。

注意

PRIMEFLEX for Microsoft Storage Spaces Direct版クラスタ拡張では、タスク実行中、ライセンス条項に承諾する必要があります。
また、システムを安定稼働させるために、最新のWindowsの更新プログラムを適用してください。

以降の手順9～22は、プロファイル適用の完了後180分以内に作業を実施してください。時間が過ぎるとISMのイベントログに以下のメッセージが出力されてクラスタ拡張がタイムアウトで異常終了しますので、ご注意ください。

50215109 : Subtask error : Failed to add server. An error occurred during the setting process of the Cluster Expansion task. (The task type setting process retried out; task type = Cluster Expansion; id = 20; task item set name = OS Installation; task item name = Wait Hyperv OS Boot; detail code = E010205)

クラスタ拡張がタイムアウトで異常終了した場合、手順22まで実施後、クラスタ拡張機能を再実行してください。

手順9～22を実施中にクラスタ拡張機能がタイムアウトによる異常終了をしても、そのまま続けて手順22まで実施してください。

ポイント

「タスク」画面のタスクリストから「Cluster Expansion」の[タスクID]を選択すると、「Cluster Expansion」の「タスク」画面が表示されます。この画面では、クラスタ拡張時に追加するサーバごとにサブタスクリストが表示されるので、メッセージ欄を確認することでタスクの進行状況を確認できます。

タスク

タスクリスト > 8

次の自動更新まで: 8 秒

停止

アクション ▼

更新

タスク情報

ステータス	進捗	経過時間	タスクID	タスクタイプ	操作者	開始時間	完了時間
進行中	<div><div></div></div> 201 / 300	0:03:36	8	Assigning profile	pfadmin	2018/05/21 18:11:39	-

サブタスクリスト

ステータス	進捗	経過時間	サブタスクID	ノード名	完了時間	メッセージ
完了	<div><div></div></div> Success	0:03:11	10	hv-host3	2018/05/21 18:14:51	Assigning profile(BIOS) was completed.
完了	<div><div></div></div> Success	0:03:25	11	hv-host3	2018/05/21 18:15:05	Assigning profile(iRMC/MMIO) was completed.
進行中	<div><div></div></div> 1 / 100	0:03:35	12	hv-host3	-	-

閉じる

- 「タスク」画面で「Assigning profile」タスクのステータスが「完了」になったら、クラスタ拡張時に追加するサーバのiRMCの画面を表示し、ログインして、ビデオリダイレクション(Video Redirection)を選択します。

セキュリティ警告が表示された場合は、「リスクを受け入れて、このアプリケーションを実行します」にチェックを付け[実行]ボタンを選択します。

ビデオリダイレクションの画面(サーバの画面)が表示されます。

- ライセンス条項画面で[承諾する]ボタンを選択します。
- 「プロダクトキーを入力してください」という画面が表示されたら、インストールメディアのプロダクトキーを入力し、[次へ]を選択します。

注意

OSインストールメディアによっては、表示されない場合もあります。

- [キーボード]タブの[Ctrl+Alt+Del]を選択して、Administrator権限を持ったユーザーでログインします。

ServerView Installation Managerのスクリプトが実行されます。

注意

ビデオリダイレクションの画面で、ServerView Installation Manager画面の[Restart system]ボタンを選択、またはWindowsを再起動しないでください。

Windowsの更新プログラムとMellanox LANドライバの適用ができなくなります。

13. クラスタ拡張時に追加するサーバのWindows OSに対して、Administrator権限を持ったユーザーでリモートデスクトップにアクセスします。

注意

リモートデスクトップ接続時にエラーメッセージが表示されて接続できない場合、以下のURLの問題の可能性があります。リモートデスクトップの接続先にビデオリダイレクションの画面から共有フォルダーを使用して最新の更新プログラムを転送し、適用してください。

<https://blogs.technet.microsoft.com/askcorejp/2018/05/02/2018-05-rollup-credssp-rdp/>

14. クラスタ拡張時に追加するサーバに既存クラスタと同等のWindowsの更新プログラムを転送します。
15. クラスタ拡張時に追加するサーバにMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、Mellanox LANドライバを転送します。

Mellanox LANドライバは、以下のサイトからドライバパッケージをダウンロードしてください。

<http://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/>

Mellanox LANドライバが適用済みの場合は、本手順は不要です。手順16に進んでください。

ポイント

Mellanox LANドライバは、[コントロールパネル]-[プログラム]-[プログラムと機能]-[プログラムのアンインストールまたは変更]に「MLNX_WinOF2」がインストールされていることで確認できます。

注意

Mellanox LANカードをご利用の場合は、手順17でMellanox LANカードのドライバをインストールしてください。

16. クラスタ拡張時に追加するサーバに転送したWindowsの更新プログラムを適用します。
17. クラスタ拡張時に追加するサーバにMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、転送したMellanox LANドライバを適用します。

Mellanox LANドライバが適用済みの場合は、本手順は不要です。手順18に進んでください。
18. Windowsの更新プログラムの適用が完了すると、再起動の確認画面が表示されます。[閉じる]ボタンを選択してからリモートデスクトップを閉じて、ビデオリダイレクションの画面に戻ります。

画面がロックされていた場合は、Administrator権限を持ったユーザーでログインし直します。
19. サーバーマネージャーが最前面になっていた場合は、最小化してServerView Installation Manager画面を表示します。
20. ServerView Installation Manager画面で[Restart system]ボタンを選択します。

サインアウト画面が表示されて、再起動されます。
21. 再起動後、Administrator権限を持ったユーザーでログインします。
22. クラスタ拡張時に追加するサーバに転送したWindowsの更新プログラムとMellanox LANカードをご利用の場合、かつ構築に使用されるSVIMの版数が12.08.04未満の場合には、転送したMellanox LANドライバを削除します。
23. クラスタ拡張時に追加するすべてのサーバで手順9～22を実施します。
24. 「Cluster Expansion」のステータスが「完了」になったことを確認します。



注意

- ISMの「タスク」画面にエラーが表示された場合は、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。問題が解決できたら再度操作を行ってください。
- ISMのプロファイル管理機能によるOSインストール(Assigning profileタスク)が正常終了している場合、再実行時にはクラスタ拡張時に追加するサーバの電源はオフにしないでください。
- クラスタ拡張時に追加するサーバの業務用仮想ネットワークの設定は、お客様環境に応じて設定してください。
- ファームウェアローリングアップデート機能を実行中にクラスタ拡張機能を実行しないでください。

6.9.3 事後処理

クラスタ拡張の事後処理について説明します。

6.9.3.1 クラスタ情報の取得と更新を行う

クラスタ拡張時に追加するサーバをクラスタ管理機能で監視するための設定を行ってください。その後、クラスタ情報の取得と更新を行ってください。

(1) Active DirectoryへKerberos委任を構成する

クラスタ拡張時に追加するすべてのサーバのKerberos委任をActive Directory に構成します。

- Active Directory サーバにログインします。
- サーバマネージャを開きます。
- [ツール]ボタンから[Active Directory ユーザーとコンピュータ]を選択します。
- ドメインを展開し、[コンピュータ]フォルダーを展開します。
- 画面右側で、<クラスタノード名>を右クリックし、[プロパティ]を選択します。
- [委任]タブで、[任意のサービスへ委任でこのコンピュータを信頼する]にチェックが付いていることを確認します。
- [OK]ボタンを選択し、すべてのクラスタノードに対して手順5～6を実施します。

(2) クラスタ情報の取得と更新を行う

ISM GUI上に仮想化基盤の情報を取得し、表示内容を最新化します。

詳細については、『ユーザーズマニュアル』の「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。

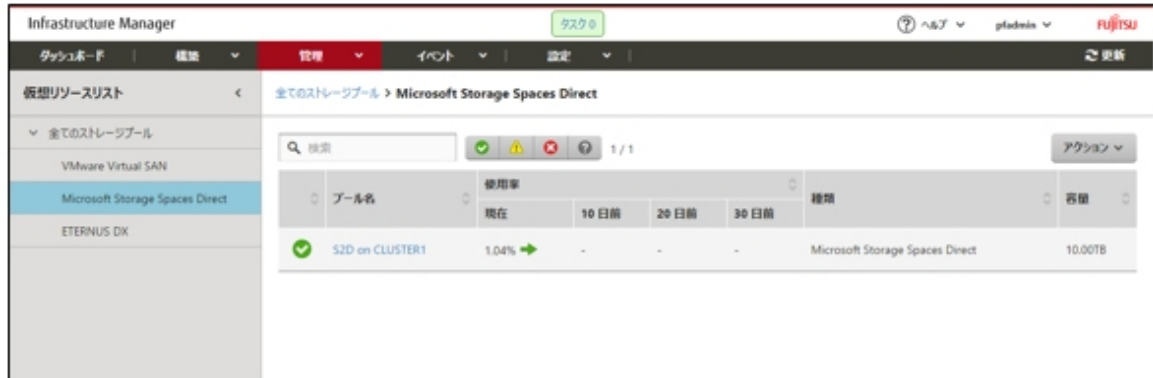
- ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
- [アクション]ボタンから[クラスタ情報取得・更新]を選択します。
- クラスタ情報の更新が「完了」となったことを確認し、しばらく待ってからISM GUIの画面更新(画面右上の更新ボタンを選択)をします。

6.9.3.2 クラスタ拡張を確認する

以下の手順でPRIMEFLEX for Microsoft Storage Spaces Directへのクラスタ拡張を確認してください。

- フェイルオーバークラスタマネージャにアクセスして、<クラスタ名>-[ノード]でクラスタ拡張時に追加したサーバのノードが表示されていることを確認します。以下の点を確認します。
 - <クラスタ名>のクラスタイベント内に警告やエラーがないこと
 - <クラスタ名>-[ノード]-<ノード名>の状態が「稼働中」であること
 - <クラスタ名>-[記憶域]-[プール]-<プール名>-[仮想ディスク]の正常性状態が「正常」であること

- ー [＜クラスタ名＞]-[記憶域]-[プール]-[＜プール名＞]-[物理ディスク]のすべてのディスクにおいて、正常性状態が「正常」であること
2. ISMのGUIにアクセスして、[管理]-[仮想リソース]の「ストレージプール」画面で[アクション]-[仮想リソース情報の更新]を実行して更新します。
- 更新後、対象の記憶域プールの[容量]が増加していることを確認します。



注意

- ー タスクが正常に完了したにも関わらず、事前に確認した記憶域プールの容量から増加していない場合、PRIMEFLEX for Microsoft Storage Spaces Directネットワーク用の通信ができていない可能性があります。スイッチの設定や結線を確認してください。
- 拡張されていることを確認するため、現在の記憶域プールの容量を確認しておいてください。
- ー タスクの完了後、フェイルオーバークラスターマネージャの[＜クラスタ名＞]のクラスタイイベント内に警告が表示される場合は、イベントIDとイベントの詳細を確認してください。以下の内容の場合は、一時的な警告のため問題ありません。右ペインの[最新のイベントの再設定]を実行してください。

イベントID	イベントの詳細
5120	クラスタの共有ボリューム'Volume1'('クラスタ仮想ディスク(Vdisk)')は'STATUS_DEVICE_NOT_CONNECTED(c000009d)'が原因で一時停止状態になりました。ボリュームへのパスが再確立されるまで、すべてのI/Oは一時的にキューに登録されます。

6.9.3.3 業務用仮想スイッチに登録する

クラスタ拡張時に追加したすべてのサーバに対して実施してください。

Serviceアダプターを設定します。管理者権限でコマンドプロンプトからPowerShellを開いて、以下のコマンドを実行します。

```
>Add-VMNetworkAdapter -SwitchName vSwitch0 -Name "Service" -ManagementOS
>Set-VMNetworkAdapterVlan -VMNetworkAdapterName "Service" -VlanId <VLAN ID> -Access -ManagementOS [注1]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -PhysicalNetAdapterName "Slot <スロット番号> ポート 2" [注2]
>Set-VMNetworkAdapterTeamMapping -VMNetworkAdapterName "Service" -ManagementOS -PhysicalNetAdapterName "Slot <スロット番号> ポート 2" [注3]
```

[注1]: <VLAN ID>には、業務LANのVLAN IDを指定します。

[注2]: <スロット番号>には、Serviceアダプターに設定する1枚目のPCIカードのネットワークアダプター名のスロット番号を指定します。

[注3]: <スロット番号>には、Serviceアダプターに設定する2枚目のPCIカードのネットワークアダプター名のスロット番号を指定します。

ポイント

スロット番号が不明な場合は、以下のコマンドで確認できます。

```
> Get-NetAdapterHardwareInfo | select Name, InterfaceDescription, Slot, Function | Sort-Object Name
```

コマンド出力例:

Name	InterfaceDescription	Slot	Function
Onboard Flexible LOM ポート 1	Intel (rainbow) Ethernet Connection X722 for 10GBASE-T		0
Onboard Flexible LOM ポート 2	Intel (rainbow) Ethernet Connection X722 for 10GBASE-T #2		1
Onboard LAN ポート 1	Intel (rainbow) I350 Gigabit Network Connection #2		0
Onboard LAN ポート 2	Intel (rainbow) I350 Gigabit Network Connection		1
Slot 03 ポート 1	Intel (R) Ethernet Converged Network Adapter X550-T2 #4	3	0
Slot 03 ポート 2	Intel (R) Ethernet Converged Network Adapter X550-T2 #2	3	1
Slot 07 ポート 1	Intel (R) Ethernet Converged Network Adapter X550-T2	7	0
Slot 07 ポート 2	Intel (R) Ethernet Converged Network Adapter X550-T2 #3	7	1

6.9.3.4 システムボリューム名を設定する

クラスタ拡張時に追加したすべてのサーバに対して実施してください。

システムボリューム名を、以下の手順で「system」に設定してください。

1. クラスタ拡張時に追加したホストにログインします。
2. エクスプローラーを起動し、Cドライブを選択して右クリックし、[名前の変更]を選択します。
3. ドライブの名前に「system」と入力します。
4. すべてのホストに対して、手順1～3を実施します。

6.9.3.5 クラスタ拡張時に追加したサーバのブラウザを設定する

ServerView RAID ManagerでSSDの寿命監視をするために、クラスタ拡張時に追加したサーバのブラウザを設定します。

『FUJITSU Software ServerView Suite ServerView RAID Manager』の「2.2.1 クライアント/ブラウザ設定」を参照し、クラスタ拡張時に追加したサーバのWebブラウザを設定してください。

6.9.3.6 証明書を削除する

「6.9.1.1 クラスタ拡張時に追加するサーバの証明書を作成する」で作成した証明書は、クラスタ拡張時に追加したサーバへOSインストール時に転送され登録されます。以下の手順で証明書を削除してください。

クラスタ拡張時に追加したすべてのサーバに対して実施してください。

1. クラスタ拡張時に追加したサーバのWindows OSに対してリモートデスクトップでアクセスします。
2. エクスプローラーを開き、以下のファイルを削除します。
 - C:\¥PostInstall¥UserApplication¥powerscript_ClusterOperation¥<証明書のファイル名.cer>
 - C:\¥PostInstall¥UserApplication¥powerscript_ClusterOperation¥<サービス証明書のファイル名.pfx>
 - C:\¥DeploymentRepository¥Add-on¥UserApplication¥powerscript_ClusterOperation¥<証明書のファイル名.cer>
 - C:\¥DeploymentRepository¥Add-on¥UserApplication¥powerscript_ClusterOperation¥<サービス証明書のファイル名.pfx>



注意

「6.9.1.1 クラスタ拡張時に追加するサーバの証明書を作成する」でISM-VAにアップロードした証明書はセキュリティリスクが生じます。セキュリティリスクが承知できない場合は、削除してください。

6.9.3.7 不要ファイルを削除する

クラスタ拡張の完了後は、以下の手順で不要なファイルを削除してください。

クラスタ拡張時に追加したすべてのサーバに対して実施してください。

1. クラスタ拡張時に追加したサーバのWindows OSに対してリモートデスクトップでアクセスします。
2. エクスプローラーを開き、以下のディレクトリ配下のファイルとディレクトリをすべて削除します。
 - － C:\¥PostInstall¥UserApplication¥postscript_ClusterOperation
 - － C:\¥FISCRB¥PowershellScript
 - － C:\¥FISCRB¥log

6.10 クラスタ定義パラメーターをエクスポート／インポート／削除する(ISM 2.3.0.b以降)

クラスタ定義パラメーターをエクスポート／インポート／削除する手順について説明します。

ISM for PRIMEFLEX用ライセンスのみ使用できる機能です。

ポイント

クラスタ定義パラメーターのエクスポート／インポート／削除は、ISM 2.3.0.b以降で操作できます。

6.10.1 クラスタ定義パラメーターをエクスポートする

クラスタ定義パラメーターをエクスポートする手順について説明します。

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します。

1. Administrator権限を持ったユーザーでISMにログインします。
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]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
3. エクスポート対象の[<対象のクラスタ>]-[クラスタ定義パラメーター]タブを選択します。
4. [パラメーターアクション]ボタンから[エクスポート]を選択します。



5. [エクスポート]ボタンを選択します。



エクスポートが完了すると結果の画面が表示されます。

6. [ダウンロードURL]に表示されたリンクを選択してファイルをダウンロードします。



6.10.2 クラスタ定義パラメーターをインポートする

クラスタ定義パラメーターをインポートする手順について説明します。

JSON形式で記述されたテキストファイルをクラスタ定義パラメーターとしてインポートします。



注意

インポート対象のクラスタにクラスタ定義パラメーターがすでに作成されている場合は、インポートできません。事前にクラスタ定義パラメーターを削除してください。

ポイント

ISM-VAのFTPサーバに配置したファイルは、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。

1. Administrator権限を持ったユーザーでISMにログインします。
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]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
3. インポート対象の[<対象のクラスタ>]-[クラスタ定義パラメーター]タブを選択します。
4. [パラメーターアクション]ボタンから[インポート]を選択します。



5. [ファイル選択方式]でファイルの選択方式を選択し、[ファイル]でインポート対象のファイルを指定します。



The screenshot shows the 'クラスタ定義パラメーターインポート' (Cluster Definition Parameter Import) dialog box. It contains the following fields and controls:

- インポートするクラスタ定義パラメーターの情報を入力してください。** (Please enter information about the cluster definition parameters to import.)
- ファイル選択方式 *** (File Selection Method *): Radio buttons for ☒ ローカル (Local) and ☐ FTP.
- ファイル *** (File *): A text input field with the placeholder 'ファイルをここにドラッグ & ドロップしてください' (Drag & drop the file here) and a 'ブラウズ' (Browse) button.
- クラスタ名** (Cluster Name): A text input field containing 'ClusterTest'.
- At the bottom right, there are two buttons: 'インポート' (Import) and 'キャンセル' (Cancel).

6. [インポート]ボタンを選択します。

クラスタ定義パラメーターインポート

?

インポートするクラスタ定義パラメーターの情報を入力してください。

ファイル選択方式 *

☒ ローカル ☐ FTP

ファイル *

Cluster4.json X

ブラウズ

クラスタ名

ClusterTest

インポート

キャンセル

注意

クラスタ定義パラメーターは、インポート後に編集が必要です。

以下の手順でクラスタ定義パラメーターを編集してください。

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]-[クラスタ]を選択します。
2. [<対象のクラスタ>]-[クラスタ定義パラメーター]タブを選択します。
3. [パラメーターアクション]ボタンから[編集]を選択します。

パスワードなどお客様環境に応じて設定するパラメーターは未指定のため、必要に応じて設定値を変更してください。

クラスタ定義パラメーターの詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第3章クラスタ定義パラメーターの設定値一覧」を参照してください。

ポイント

ISM-VAのFTPサーバに配置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。

6.10.3 クラスタ定義パラメーターを削除する

クラスタ定義パラメーターを削除する手順について説明します。

1. Administrator権限を持ったユーザーでISMにログインします。
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]-[クラスタ]を選択します。
「クラスタリスト」画面が表示されます。
3. 削除対象の [<対象のクラスタ>]-[クラスタ定義パラメーター]タブを選択します。

4. [パラメーターアクション]ボタンから[削除]を選択します。



5. [削除]ボタンを選択します。



ポイント

.....
インポート対象のクラスタにすでにクラスター定義パラメーターが作成されている場合は、インポートできません。上記操作で既存のクラスター定義パラメーターを削除するとインポートできるようになります。
.....

第7章 管理対象ノードのトラブルに備える

この章では、管理対象のノードに発生するトラブルに備えて実施する事前操作や、トラブル発生時の対処について説明します。

7.1 サーバの設定をバックアップ／リストアする

7.1.1 サーバの設定をバックアップする

ISMに登録したサーバのハードウェア設定 (BIOS、iRMC) を採取してファイルとして保存します。また、保存したファイルをエクスポートできます。

バックアップ手順

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]-[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. ノードを選択して、[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)]、または[Server (iRMC)]にチェックを付けて、[実行]ボタンを選択します。

エクスポート手順

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]-[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. ノードを選択して、[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。
「バックアップファイルエクスポート」画面が表示されます。
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

バックアップ、エクスポートは、複数のノードとハードウェア設定を選択できます。

7.1.2 バックアップファイルからプロファイルを作成する

「7.1.1 サーバの設定をバックアップする」で保存したハードウェア設定ファイルから、プロファイルを作成します。

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. ノードを選択して、[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。

設定項目の入力は、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

ポイント

複数のハードウェア設定を選択してプロファイルを作成できます。

7.1.3 バックアップファイルからポリシーを作成する

「7.1.1 サーバの設定をバックアップする」で保存したハードウェア設定ファイルから、ポリシーを作成します。

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. ノードを選択して、[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。

設定項目の入力は、ヘルプ画面を参照してください。

ヘルプ画面の表示方法:ウィザード画面右上の[?]を選択

ポイント

複数のハードウェア設定を選択してポリシーを作成できます。

7.1.4 サーバの設定をインポートする

「7.1.1 サーバの設定をバックアップする」でエクスポートしたノードのハードウェア設定ファイル、またはiRMCから採取したハードウェア設定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. ノードを選択して、[アクション]ボタンから[インポート]を選択します。

「バックアップファイルインポート」画面が表示されます。

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。

事前に、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、『ユーザーズマニュアル』の「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]ボタンを選択します。

インポートが実行されます。

ポイント

複数のノードを選択してインポートできます。

7.1.5 サーバの設定をリストアする

「7.1.1 サーバの設定をバックアップする」で保存したハードウェア設定ファイル、または「7.1.4 サーバの設定をインポートする」でインポートしたファイルを、ISMに登録したサーバに対してリストアします。

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. ノードを選択して、[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。
「ハードウェア設定リストア」画面が表示されます。
5. BIOSのハードウェア設定をリストアする場合は、リストア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。
6. 画面表示に従い、ファイルを選択して、[確認]ボタンを選択します。
7. 設定を確認し、「上記内容を確認しました。」にチェックを付けて[実行]ボタンを選択します。

ポイント

複数のノードを選択してリストアできます。

7.2 スイッチやストレージの設定をバックアップ／リストアする

7.2.1 スイッチやストレージの設定をバックアップする

ISMに登録したスイッチ、ストレージの設定を採取してファイルとして保存します。また、保存したファイルをエクスポートできます。

1. バックアップ前にハードウェアの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[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[ハードウェア設定バックアップ / リストア]を選択します。
4. ノードを選択して、[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。
5. 設定をバックアップする[Switch]、[Storage]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。

7.2.2 スイッチやストレージの設定をエクスポートする

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. ノードを選択して、[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。
「バックアップファイルエクスポート」画面が表示されます。
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。

7.2.3 スイッチの設定をインポートする

「7.2.2 スイッチやストレージの設定をエクスポートする」でエクスポートしたスイッチのハードウェア設定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. ノードを選択して、[アクション]ボタンから[インポート]を選択します。
「バックアップファイルインポート」画面が表示されます。
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。
事前に、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、『ユーザーズマニュアル』の「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]ボタンを選択します。
インポートが実行されます。

ポイント

複数のノードを選択してインポートできます。

7.2.4 スイッチの設定をリストアする

「7.2.1 スイッチやストレージの設定をバックアップする」で保存したスイッチのハードウェア設定ファイル、または「7.2.3 スイッチの設定をインポートする」でインポートしたファイルを、ISMに登録したスイッチに対してリストアします。

1. リストア前にハードウェアの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[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[ハードウェア設定バックアップ / リストア]を選択します。
4. 「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。
5. ノードを選択して、[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。
「ハードウェア設定リストア」画面が表示されます。
6. 画面表示に従い、ファイルを選択して、[確認]ボタンを選択します。
7. 設定を確認し、「上記内容を確認しました。」にチェックを付けて[実行]ボタンを選択します。

ポイント

複数のノードを選択してリストアできます。

注意

ExtremeSwitching VDX (以降VDXと表記) (Brocade 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については、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は、以下のとおりです。

- ・ 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。



第8章 ISMのトラブルに備える／対処する

この章では、ISM全体に対してのトラブルに備えて実施する事前操作や、トラブル発生時の対処について説明します。

8.1 ISMをバックアップ／リストアする

ISMのバックアップ／リストアの手順を説明します。

この手順は、ハイパーバイザーを使用したバックアップとは異なり、稼働中のISM-VAの電源を停止することなくバックアップができます。また、バックアップ対象を限定しているため、短い時間でバックアップができます。

ISMのバックアップ／リストアの手順は、以下のとおりです。

1. 事前準備として、リストア先として使用するISM-VAをバックアップします。

「[8.1.1 ISMのバックアップ／リストアの事前準備を行う](#)」を参照してください。



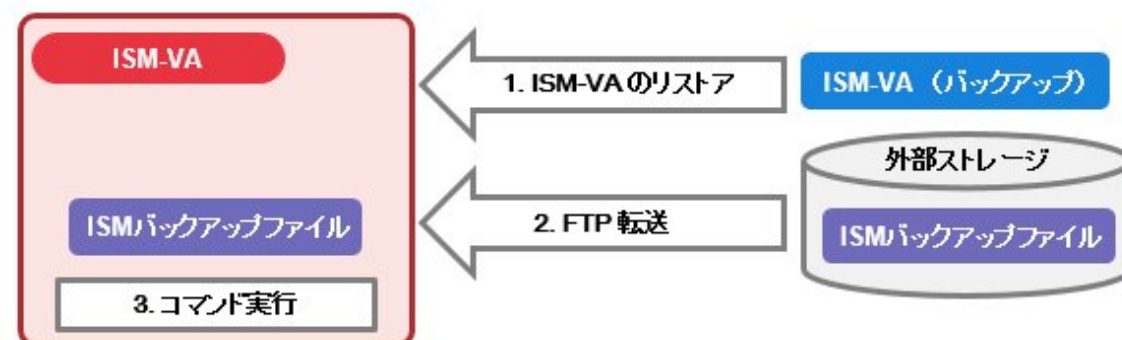
2. 日々の運用でISMをバックアップします。

「[8.1.2 ISMをバックアップする](#)」を参照してください。



3. リストアが必要な状況が発生した場合にISMをリストアします。

「[8.1.3 ISMをリストアする](#)」を参照してください。



8.1.1 ISMのバックアップ／リストアの事前準備を行う

ISMのバックアップファイルのリストア先として使用するISM-VAをバックアップします。

バックアップは、利用するISM-VAのバージョンで行ってください。

ISM-VAのバックアップ手順は、「[2.1.2 ISM-VAをエクスポートする](#)」を参照してください。



注意

ISM-VAのバックアップは、以下の作業後に必ず行ってください。

- ISMの導入時
- ISMのアップグレード時
- ISMの修正パッチ適用時

8.1.2 ISMをバックアップする

ISM-VAの設定情報やノード管理データなどのバックアップ対象ファイルを収集して、ISMのバックアップファイルを作成します。



注意

- 以下の場合は、バックアップを実行できません。
 - ISMのバックアップに必要な空きディスク容量がISM-VAにない場合
リポジトリ、保管ログ、ノードログなどを削除するか、システムの仮想ディスクの割当てを行ってください。
 - ISMのサービスが停止している場合
ISMのサービスを起動してください。
 - プロファイル適用、ファームウェアアップデートなどのタスクが動作している場合
タスクの完了を待つか、タスクをキャンセルしてください。
- ISMのバックアップ実行中は、ISMの全サービス(ノード管理やノード監視など)が停止します。バックアップ終了時、自動的にISMの全サービスが再起動されます。
- GUI操作、REST API、スケジュールによるバックアップの実行は未サポートです。

1. コンソールからadministratorでISM-VAにログインします。
2. ISMバックアップコマンドを実行します。

```
# ismadm system backup
```

ISMバックアップコマンド実行例:

```
# ismadm system backup
[System Information]
  Version : 2.3.0.x (S20180220-01)

[Disk Space Available]
  System      : 30000MB

[Disk Space Required]
  System      : 2400MB

Start backup process? [y/n]:
```

コマンド実行後に、バックアップの確認画面が表示されます。

3. 「y」を入力して、バックアップを開始します。
バックアップ完了後、ISMのバックアップファイル名が表示されます。

ISMのバックアップファイル名の表示例:

```
ism backup end.
Output file: /Administrator/ftp/ism2.3.0.x-backup-20180801120000.tar.gz
```

ISMのバックアップファイル名:ism<バージョン>-backup-<バックアップ日時>.tar.gz

4. 作成されたISMのバックアップファイルをダウンロードします。

FTPで「ftp://<ISM-VAのIPアドレス>/Administrator/ftp」にアクセスし、ISMのバックアップファイルをダウンロードします。



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。

8.1.3 ISMをリストアする

「8.1.2 ISMをバックアップする」で作成したISMのバックアップファイルを、「8.1.1 ISMのバックアップ／リストアの事前準備を行う」でバックアップしたISM-VAに対してリストアします。



- 以下の場合は、ISMのリストアを実行できません。
 - ISMのバックアップファイルとリストア先のISM-VAのバージョンが異なる場合
ISM-VAのリストアでは、ISMのバックアップファイルと同じバージョンのISM-VAのバックアップをリストアしてください。
 - ISMのリストアに必要な空きディスク容量がリストア先のISM-VAにない場合
リポジトリ、保管ログ、ノードログなどを削除するか、システムの仮想ディスクの割当てを行ってください。
- GUI操作、REST API、スケジュールによるリストアの実行は未サポートです。

1. 「8.1.1 ISMのバックアップ／リストアの事前準備を行う」でバックアップしたISM-VAをリストアします。

ISMのバックアップファイルを作成したISM-VAのバックアップをリストアしてください。

リストアしたISM-VAをISMのリストア先として使用します。

ISM-VAのリストア手順は、「2.1.1 ISM-VAをインポートする」を参照してください。

2. 「8.1.2 ISMをバックアップする」で作成したISMバックアップファイルを用意します。
3. FTPを使用して、リストア先のISM-VAへ転送します。FTPで「ftp://<リストア先のISM-VAのIPアドレス>/Administrator/ftp」にアクセスし、手順2で用意したISMバックアップファイルを格納します。
4. コンソールからadministratorでリストア先のISM-VAにログインします。
5. ISMリストアコマンドを実行します。

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

ISMリストアコマンド実行例:

```
# ismadm system restore -file ism2.3.0.x-backup-20180801120000.tar.gz
[System Information]
  Version : 2.3.0.x (S20180220-01)

[Backup File Information]
  Version : 2.3.0.x (S20180220-01)

[Disk Space Available]
  System      : 30000MB

[Disk Space Required]
  System      : 2400MB

Start restore process? [y/n]:
```

コマンド実行後に、リストアの確認画面が表示されます。

6. 「y」を入力して、リストアを開始します。

7. リストア完了後、以下のコマンドを実行してISM-VAを再起動します。

```
# ismadm power restart
```

8. 仮想ディスクの割当てを行います。

ポイント

ISMのリストア後、すべてのユーザーグループの仮想ディスクの割当てが解除されています。また、システムの仮想ディスクの割当ては、ISM-VAのバックアップ時の状態となっています。

仮想ディスクの割当て状態を確認し、必要に応じてシステムおよびユーザーグループの仮想ディスクの割当てを新規割当ての手順で行ってください。仮想ディスクの割当て手順は、「[2.1.3 仮想ディスクを接続する](#)」を参照してください。

9. 仮想ディスクを割当て後、ISM-VAを再起動します。
10. 電力制御の設定を行います。

ポイント

ISMのリストア後、各ラックに対する電力制御機能が無効化されています。

ラックの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、「[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。

11. ISMのリストア時にリポジトリ、保管ログ、およびノードログは削除されています。必要に応じて、リポジトリのインポート、ログの収集を実施します。

8.2 保守資料を採取する

ISMの保守資料を採取するには、ISMのGUIを使用する方法とコマンドを使用する方法があります。

8.2.1 GUIを利用して保守資料を採取する

ISM GUIへログインし、以下の方法で保守資料を採取およびダウンロードします。

ポイント

本操作は、ISM管理者 (Administratorグループに属し、Administratorロールを持つユーザー) のみ実行できます。

保守資料を新規に採取する

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[保守資料]を選択します。
「保守資料」画面が表示されます。
3. [アクション]ボタンから[採取]を選択します。
4. 表示された画面で、以下のどちらかの採取モードを選択し、[実行]ボタンを選択します。
 - ー 全て:障害調査ログ/ISM-VA オペレーティングシステムログ/データベース情報の一括採取
 - ー 一部:障害調査ログのみの採取



保守資料の一括採取には数時間かかり、大容量の空きディスク容量が必要です。詳細は、『ユーザーズマニュアル』の「3.2.1.5 保守資料容量の見積り」を参照してください。

採取が開始され、[ステータス]の列に採取の進行状況が表示されます。進行状況の表示を更新するには、画面の更新を実施してください。

また、進行状況は「タスク」画面でも確認できます。タスクタイプは「Collecting Maintenance Data」です。

採取が完了するとステータスのアイコンが「完了」となり、ダウンロード可能になります。

保守資料をダウンロードする

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[保守資料]を選択します。
「保守資料」画面が表示されます。
3. 採取したい保守資料の[ダウンロード]ボタンを選択します。
4. ブラウザのダウンロード確認に従って、保守資料をダウンロードします。

保守資料を削除する

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[保守資料]を選択します。
「保守資料」画面が表示されます。
3. 削除したい保守資料にチェックを付け、[アクション]ボタンから[削除]を選択します。
削除対象のファイル名が表示されます。
4. ファイル名を確認し、[実行]ボタンを選択します。

保守資料の採取をキャンセルする

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[保守資料]を選択します。
「保守資料」画面が表示されます。
3. 採取中の保守資料にチェックを付け、[アクション]ボタンから[キャンセル]を選択します。
採取中の保守資料は、[ステータス]列に進行状況が表示されています。
4. 表示される確認画面で、[はい]ボタンを選択します。

ISM 2.3.0では、キャンセル後、[ステータス]列には「失敗」と表示されます。

ISM 2.3.0.b以降では、キャンセルされた保守資料は削除されます。



- ・ ISM GUIの「保守資料」画面から採取された保守資料は、以下のディレクトリに保持され、このディレクトリ配下の保守資料だけが表示されます。

保守資料格納ディレクトリ: /Administrator/transfer

ISM-VAのFTP送受信ディレクトリ/Administrator/ftpに保持されている保守資料は、「保守資料」画面には表示されません。

- ・ 保守資料は、5世代分まで保持されます。5世代を超えると作成日時の古いものから自動的に削除されます。
- ・ 保守資料は、採取後5週間が経過すると自動的に削除されます。

- ・ 仮想リソース管理機能の保守資料としてvCenterからvc-supportログを採取します。詳細は、以下のURL (英語ページ) の「To collect ESX/ESXi and vCenter Server diagnostic data」の手順を参照してください。

https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

上記URLに記載されたログ収集の手順6で、ログ収集対象のESXiホストとして、問題が発生しているvSANクラスタのESXiホストをすべて選択してください。

8.2.2 コマンドを実行して保守資料を採取する

ISM-VAのコマンドを使用して、ISMの保守資料を採取します。

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. ISMの保守資料を採取します。

ISMやISM-VAの誤動作を調査するときの実施例

ー 障害調査ログのみの採取

```
# ismadm system snap -dir /Administrator/ftp
snap start
Your snap has been generated and saved in:
/Administrator/ftp/ismsnap-20160618175323.tar.gz
```

ー 障害調査ログ／ISM-VA オペレーティングシステムログ／データベース情報の一括採取

```
# ismadm system snap -dir /Administrator/ftp -full
snap start
Your snap has been generated and saved in:
/Administrator/ftp/ismsnap-20160618175808.tar.gz
```

ポイント

-dirは出力先の指定です。『ユーザーズマニュアル』の「2.1.2 FTPアクセス」に記述されているファイル転送領域を指定することにより、FTPアクセスで採取した保守資料を取り出せます。

注意

保守資料の一括採取には数時間かかり、大容量の空きディスク容量が必要です。詳細は、『ユーザーズマニュアル』の「3.2.1.5 保守資料容量の見積り」を参照してください。

3. 採取した保守資料をダウンロードします。

採取コマンド実行時に出力先とファイル名が表示されますので、管理端末からadministratorでFTPアクセスし、ダウンロードします。

注意

- ・ 保守資料格納ディレクトリに作成された保守資料は、最新の5ファイルが保存されます。不要になった保守資料は、FTPクライアントソフトウェアなどを使用して手動で削除してください。
- ・ 仮想リソース管理機能の保守資料としてvCenterからvc-supportログを採取します。詳細は、以下のURL (英語ページ) の「To collect ESX/ESXi and vCenter Server diagnostic data」の手順を参照してください。

https://kb.vmware.com/selfservice/search.do?cmd=displayKC&docType=kc&docTypeID=DT_KB_1_1&externalId=2032892

上記URLに記載されたログ収集の手順6で、ログ収集対象のESXiホストとして、問題が発生しているvSANクラスタのESXiホストをすべて選択してください。

第9章 ISMを更新する

この章では、ISM-VAに対しての修正パッチ適用やISM-VAのアップグレードなど、ISMを更新する方法について説明します。

9.1 ISM-VAに修正パッチを適用する

ISM-VAに修正パッチを適用する際は、以下の手順で行います。

ここでは、ISM-VAの"/Administrator/ftp" へ修正ファイル (ISM230x_S20180901-01.tar.gz) を転送して、修正パッチを適用する場合の手順を説明します。



注意

- 修正パッチを適用する際は、一時的にISMサービスを停止してください。
- 修正パッチを適用後、ISM-VAを再起動してください。
- 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、「[2.1.2 ISM-VAをエクスポートする](#)」を参照してください。

1. administratorユーザーでFTP接続して、修正ファイルをISM-VAへ転送します。

「ftp://<ISM-VAのIPアドレス>/Administrator/ftp」にアクセスし、修正ファイルを格納します。



注意

修正ファイルをFTP転送する際は、バイナリモードで転送してください。

2. administratorユーザーでSSH接続して、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サービスを停止します。

```
# ismadm service stop ism
```

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/ISM230x_S20180901-01.tar.gz
```

以下が表示されたら、修正パッチの適用は終了です。

```
Complete!
=====
Update finished successfully.
Please restart ISM-VA.
=====
```

5. 修正パッチが適用されていることを確認します。

```
# ismadm system show
```

コマンド出力結果の [ISM Version] が修正パッチの版数になっていることを確認します。

例)

```
ISM Version      : 2.3.0.x (S20180901-01)
```

6. 修正パッチを適用後、ISM-VAを再起動します。

```
# ismadm power restart
```

以上でISM-VAに修正パッチを適用する手順は完了です。

9.2 ISM-VAをアップグレードする

ISMをV2.0/V2.1/V2.2からV2.3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]メニューをご確認ください。

SupportDesk-Webについては、『ユーザーズマニュアル』の「1.6 ISMの保守／更新について」を参照してください。



注意

- ・ V1.0～V1.5のバージョンからV2.3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を申し込んでください。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。
- ・ アップグレードをする前に、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、「[2.1.2 ISM-VAをエクスポートする](#)」を参照してください。

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。

1. FTPでアップグレードファイルをISM-VAへ転送します。

FTPで「ftp://<リストア先のISM-VAのIPアドレス>/Administrator/ftp」にアクセスし、アップグレードファイルを格納します。

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。

FTPでの転送方法は、『ユーザーズマニュアル』の「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。

```
# ismadm service stop ism
```

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/ISM230_S2018xxxx-0X.tar.gz
```

5. アップグレード後、ISM-VAを再起動します。

```
# ismadm power restart
```