Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0

操作手順書

CA92344-5715-02
2024年11月

まえがき

本書の目的

本書では、サーバー、ストレージ、スイッチなどのICT機器やファシリティー機器（PDUなど）を統合的に管理、運用する運用管理ソフトウェアである以下のソフトウェア製品の導入手順、利用シーンに応じた操作手順を説明します。

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

製品マニュアル

マニュアル名称	説明
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 入門書	本製品を初めて使用する利用者向けのマニュアルです。 本製品の製品体系／ライセンス、利用手順の概要について説明しています。 マニュアル内では、『入門書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 解説書	本製品の機能、導入手順、操作方法を説明したマニュアルです。 本製品の全機能、全操作を把握できます。 マニュアル内では、『解説書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 操作手順書	本製品の導入手順、利用シーンに応じた操作手順を説明したマニュアルです。 マニュアル内では、『操作手順書』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 REST API リファレンスマニュアル	お客様が作成したアプリケーションと本製品を連携する際に必要なAPIの使用方法、サンプル、パラメーター情報などを説明したマニュアルです。 マニュアル内では、『REST API リファレンスマニュアル』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 メッセージ集	ISMおよびISM for PRIMEFLEX使用時に出力される各種メッセージの説明と、そのメッセージに対しての対処方法について説明しています。 マニュアル内では、『ISM メッセージ集』と表記します。
Infrastructure Manager for PRIMEFLEX V3.0.0 メッセージ集	ISM for PRIMEFLEX使用時に出力される各種メッセージの説明と、そのメッセージに対しての対処方法について説明しています。 マニュアル内では、『ISM for PRIMEFLEX メッセージ集』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 プロファイル管理機能 プロファイル設定項目集	管理対象機器のプロファイル作成の設定を行う際に選択する項目の詳細情報について説明しています。 マニュアル内では、『プロファイル管理機能 プロファイル設定項目集』と表記します。
Infrastructure Manager for PRIMEFLEX V3.0.0 クラスタ作成／拡張機能 設定値一覧	ISM for PRIMEFLEXで利用できるクラスタ作成機能、クラスタ拡張機能の自動設定内容や各機能で使用されるクラスタ定義パラメーターについて説明しています。 マニュアル内では、『ISM for PRIMEFLEX 設定値一覧』と表記します。
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 用語集	本製品を使用するうえで理解が必要な用語の定義を説明した用語集です。 マニュアル内では、『用語集』と表記します。

マニュアル名称	説明
Infrastructure Manager / Infrastructure Manager for PRIMEFLEX V3.0.0 Plug-in and Management Pack セットアップガイド	Infrastructure Manager Plug-inの以下の機能について、インストールから利用方法までと注意事項や参考情報を説明します。 ・ Infrastructure Manager Plug-in for Microsoft System Center Operations Manager ・ Infrastructure Manager Plug-in for Microsoft System Center Virtual Machine Manager ・ Infrastructure Manager Plug-in for VMware vCenter Server Appliance ・ Infrastructure Manager Plug-in for Microsoft Windows Admin Center マニュアル内では、『ISM Plug-in/MP セットアップガイド』と表記します。

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

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

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

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

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

本書の読者

このマニュアルは、サーバー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、以下の例のとおりOSを略称で記載することがあります。

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

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

用語

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

PDF表示アプリケーション（Adobe Readerなど）での操作について

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

- テキストファイルへの保存
- テキストのコピー&ペースト

高度な安全性が要求される用途への使用について

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

安全にお使いいただくために

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

改造等

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

免責事項

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

登録商標について

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

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

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

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

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

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

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

Zabbixはラトビア共和国にあるZabbix LLCの商標です。

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

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

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

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

Xenは、XenSource, Inc.の商標です。

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

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

その他の会社名と各製品名は、各社の商標、または登録商標です。

その他の各製品は、各社の著作物です。

著作権表示

改版履歴

版数	作成年月	変更内容	章・節・項	変更箇所
01	2024年9月	新規作成	―	―
02	2024年11月 ISM 3.0.0.010 パッチ適用による変更	ユーザー情報に「セッション有効時間」を追加	2.3.1.1 ユーザーを追加する	表「ユーザー情報」
		ロール毎に変更できるユーザー情報一覧に「セッション有効時間」を追加	2.3.1.2 ユーザーを編集する	手順3の表
		ETERNUS DX900 S6に関する記事の追加	2.3.4.2 ノードグループを編集する	表「ノード間で親子の繋がりが設定されるモデル」
		ノード登録時の認証確認に関する記述を追加	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	手順11
			3.1.2 ノードを直接登録する	手順4

版数	作成年月	変更内容	章・節・項	変更箇所
	2024年11月 主な構成変更や記事改善	VMwareの商標変更に伴い記述を変更	まえがき	登録商標について
		トラップ受信抑止期間の説明を改善	3.2.1.2 アラーム共通設定をする	ー
		プロファイルの適用に関する記述を追加	3.3.5 適用済みのプロファイルとハードウェア設定を比較する	[不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図しないものである場合） 「注意」
		CPU世代の確認方法を追加	6.8.2.1 vCenter ServerのVMware EVCを設定する	ー
		修正パッチ／アップグレードを適用する際のISM-VAの再起動に関する記述を追加	9.1 修正パッチ／アップグレードプログラムを適用する	ー

目　次

第1章 共通的な操作

この章では、ISMのGUI画面での共通する操作を説明します。

ポイント

ISMのGUIを起動する方法、および必要な設定については、『解説書』の「2.1.1 GUI」を参照してください。

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]-[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()を選択すると、情報を再取得し画面が更新されます。

1.3 イベントログを確認する

ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログからメッセージを確認します。

イベントログは、ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択して参照できます。

1.4 ISMで利用するファイルをISM-VAにアップロードする

ISMのGUIを使用して、ISMで利用するファイルをISM-VAにアップロードします。

1.4.1 ISM-VAにファイルをアップロードする

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[アップロード]を選択します。
3. ルートディレクトリーを一覧から選択します。
4. [アクション]ボタンから[ファイルアップロード]を選択します。

   「ファイルアップロード」画面が表示されます。

   a. ファイルタイプを選択します。

   b. ファイルタイプに「その他」を選択した場合は、アップロード先ディレクトリーを選択します。ファイルタイプに「その他」以外を選択した場合は、アップロード先は選択できません。

   c. アップロードするファイルを選択します。アップロードするファイルをISMのGUIにドラッグアンドドロップします。または、[ブラウズ]ボタンを選択して、アップロードするファイルを選択します。

      複数のファイルをアップロードする場合は、[追加]ボタンを選択し、a～cの手順を実行します。
5. [適用]ボタンを選択します。

1.4.2 ISM-VAにアップロードしたファイルを削除する

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[アップロード]を選択します。
3. ルートディレクトリーを一覧から選択します。
4. ディレクトリーのリンクを選択、または検索をして、削除するファイルを表示します。
5. 削除するファイルを選択してチェックを付けます。
6. [アクション]ボタンから[ファイル削除]を選択します。
7. 「ファイル削除」画面で、削除するファイルを確認して、[削除]ボタンを選択します。

第2章 ISM導入時に必要な設定を行う

この章では、ISM導入時に必要となる操作を説明します。

『解説書』の「第3章 導入」の各操作を完了してから実施してください。

2.1 ノードを管理するための設定をする

ISMでは、データセンター／フロア／ラック／ノードの4階層でノードを管理します。

ここでは、データセンター／フロア／ラックの登録／削除方法について説明します。

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。

2.1.1 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。

   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。

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。

2.1.2 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「2.1.1 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。

   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。

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。

2.1.3 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ーラックをイメージした階層です。

ラックを登録する

フロア内のサーバー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、「2.1.1 データセンターを登録／削除する」、「2.1.2 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。

   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。

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。

2.1.4 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。

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。

2.2 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（「2.2.1 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（「2.2.2 アクション（通知方法）をテストする」参照）
3. アラーム設定（「2.2.3 ISM内部のイベントを対象にアラームを設定する」参照）

2.2.1 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サーバーに、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。

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。

- 2.2.1.1 外部ホスト上に配置したスクリプトを実行する
- 2.2.1.2 メールを送信する
- 2.2.1.3 トラップ送信／転送を行う
- 2.2.1.4 Syslog転送を行う

2.2.1.1 外部ホスト上に配置したスクリプトを実行する

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）
Azure Stack HCI	
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ー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、『解説書』の「付録B 監視対象OS、仮想化管理ソフトウェアに対する設定」を参照してください。

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。

注意

リモートスクリプト実行では、最大実行時間（初期値：300秒）が設定されています。

設定時間内にスクリプト実行が完了しない場合は、スクリプト実行を強制終了します。

スクリプトが正常終了できる時間を設定してください。

2.2.1.2 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サーバー]を選択します。

   「SMTPサーバー設定」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サーバー設定」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。

2.2.1.3 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。

2.2.1.4 Syslog転送を行う

外部Syslogサーバーに対して、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サーバーとしてサポートしているは、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

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

Syslogを受信できるようにするため、外部Syslogサーバーに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。

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。

   ー RHEL 7、CentOS 6、CentOS 7、SLES 12、SLES 15の場合

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

   ー 上記以外の場合

```
module(load="imtcp")
input(type="imtcp" port="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 CentOS 6の場合

```
# service rsyslog restart
```

   ー 上記以外の場合

```
# systemctl restart rsyslog
```

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。

2.2.2 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。

   テスト実行時には、アクションに設定したマクロは以下の文字列に置換されます。

マクロ	置換後の文字列
$_ISM	TEST_ISM
$_TRGID	TEST_TRGID
$_TRGTYPE	TEST_TRGTYPE
$_TRG	TEST_TRG
$_IPA	TEST_IPA
$_IDN	TEST_IDN
$_MDL	TEST_MDL
$_DC	TEST_DC
$_FLR	TEST_FLR
$_RACK	TEST_RACK
$_POS	TEST_POS
$_MIB	TEST_MIB
$_SPC	TEST_SPC
$_TRP	TEST_TRP
$_SEV	TEST_SEV
$_EVT	TEST_EVT
$_MSG	TEST_MSG
$_TIM	TEST_TIM
$_TIM2	TEST_TIM2

2.2.3 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「2.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. 「5.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。

2.3 ISMのユーザーを設定する

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、『解説書』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。

2.3.1 ISMのユーザーを管理する

ユーザーを管理するための操作には、以下の4種類あります。

- 2.3.1.1 ユーザーを追加する
- 2.3.1.2 ユーザーを編集する
- 2.3.1.3 ユーザーを削除する
- 2.3.1.4 administratorユーザーを有効／無効に変更する

2.3.1.1 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。

表2.1 ユーザー情報

項目	設定内容
ユーザー名	ISM全体で、ユニークな名称を指定します。以下の名称は、使用できません。

項目	設定内容
	・ 先頭が__で始まる名称 [注] ・ administrator ・ anonymous [注] ・ svimcontent [注] [注]:ユーザー一覧画面には表示されません。
ISM連携	以下のどちらかを選択します。 ・ 連携用のユーザーとして設定しない ・ 連携用のユーザーとして設定する
パスワード	ユーザーのパスワードを指定します。
認証方式	以下のどちらかを選択します。 ・ ユーザーグループの設定に従う ・ Infrastructure Manager (ISM)
多要素認証(MFA)	以下のどちらかを選択します。 ・ ユーザーグループの設定に従う ・ 無効
ユーザーロール	以下のどれかを選択します。 ・ Administrator ・ Operator ・ Monitor ユーザーロールについては、『解説書』の「2.13.1 ユーザー管理機能」を参照してください。
説明	ユーザーの説明(コメント)を自由に指定します。
言語	日本語または英語を指定します。指定しない場合は、英語となります。
日付フォーマット	日付フォーマットを選択します。
タイムゾーン	タイムゾーンを選択します。
セッション有効時間 (ISM 3.0.0.010以降)	セキュリティーポリシーを選択するか、2～1440分の時間を入力します。

ユーザー情報設定後、そのユーザーが所属するユーザーグループを選択します。

2.3.1.2 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。
   - 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。
   - 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	○	○	○	○
ISM連携	○	×	×	×
パスワード	○	○	○	○
認証方式	○	×	○	×
多要素認証（MFA）	○	×	○	×
ユーザーロール	○	×	○	×
説明	○	○	○	○
言語	○	○	○	○
日付フォーマット	○	○	○	○
タイムゾーン	○	○	○	○
ユーザーグループ名	○	×	×	×
セッション有効時間 （ISM 3.0.0.010以降）	○	×	○	×

○：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サーバー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。
- パスワードを変更した場合、セッションが切断されてログアウトされます。

2.3.1.3 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。

2.3.1.4 administratorユーザーを有効／無効に変更する

ISMには初期状態でユーザーアカウント"administrator"が用意されています。

"administrator"を無効化することにより、GUIとコンソールのログインができなくなります。無効化状態でログインを試みると、アカウントが存在しない場合と同様のエラーとなります。

この操作ができるのは、"administrator"以外のAdministratorユーザーグループのユーザーです。

ポイント

本操作は、"administrator"ユーザー以外で、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。

以下の方法で、"administrator"ユーザーを有効／無効に変更できます。

1. ISMのGUIでグローバルナビゲーションメニューから[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。
   "administrator"ユーザーが無効の場合は、ユーザーリスト内の"administrator"ユーザーの背景がグレーになります。
3. [アクション]ボタンから[administrator有効/無効]を選択します。
   "administrator"ユーザー以外のユーザーを選択しても、有効／無効の設定はできません。
4. 認証画面で"administrator"ユーザーのパスワードを入力し、[適用]ボタンを選択します。

2.3.2 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。

- 2.3.2.1 ユーザーグループを追加する
- 2.3.2.2 ユーザーグループを編集する
- 2.3.2.3 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。

2.3.2.1 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。

表2.2 ユーザーグループ情報

項目	設定内容
ユーザーグループ名	ISM全体で、ユニークな名称を指定します。 以下の名称は、ISMで使用しているため使用できません。 ・ 先頭が__（半角アンダーバー2つ）で始まる名称 ・ Administrator ・ AbstractionLayer ・ anonymous ・ svimcontent 注意:ユーザーグループ名には、半角空白を含めないでください。半角空白を含む場合、所属するユーザーで ismadmコマンドを実行すると、ismadmコマンドの実行に失敗することがあります。
認証方式	ユーザーグループに属するユーザーの認証方式は、以下のどちらかを指定します。 ・ Infrastructure Manager (ISM)

項目	設定内容
	ユーザーの認証方式を、ISMでユーザーを追加した際のパスワードで認証します。 ・ Open LDAP / Microsoft Active Directory (LDAP) Open LDAPまたはMicrosoft Active Directoryで管理されているパスワードで認証します。
多要素認証 (MFA)	以下のどちらかを指定します。 ・ 有効 多要素認証を有効にします。ISMへログインする際に、ユーザー名とパスワードに加えて、認証コードが必要になります。 ・ 無効 多要素認証を無効にします。ISMにユーザー名とパスワードでログインできます。 [認証方式]が「Infrastructure Manager (ISM)」の場合のみ有効にできます。 [認証方式]に関わらず多要素認証を有効に設定できます。 ISM 2.8.0.010より前に作成したユーザーグループは「無効」に設定されています。
iRMCログイン/AVR	以下のどちらかを指定します。 ・ 有効 iRMCログイン/AVRの使用を有効にします。 ・ 無効 iRMCログイン/AVRの使用を無効にします。
LDAPグループ連携	[認証方式]が「Open LDAP / Microsoft Active Directory (LDAP)」のときに表示されます。 ディレクトリーサーバー上のユーザーと連携する場合に指定します。
LDAPサーバーのグループと連携する	LDAPサーバーのグループと連携するかどうかを選択します。 ・ ISMで作成したユーザーのパスワードをディレクトリーサーバーで管理する場合 本項目のチェックを外します。詳細は、「2.3.3.1 ISMで作成したユーザーのパスワードをディレクトリーサーバーで管理する」を参照してください。 ・ ディレクトリーサーバー上でユーザーとパスワードを管理する場合 本項目にチェックを付けます。また、連携するための情報を設定します。詳細は、「2.3.3.2 ディレクトリーサーバー上でユーザーとパスワードを管理する」を参照してください。
連携LDAPグループ	[LDAPサーバーのグループと連携する]が選択されているときに表示されます。 どのドメインのどのグループと連携するかを指定します。
LDAPグループユーザーのユーザーロール	[LDAPサーバーのグループと連携する]が選択されているときに表示されます。 連携するユーザーのユーザーロールを指定します。
説明	ユーザーグループの説明(コメント)を入力します。入力内容は任意です。
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。 以下のどちらかを指定します。 ・ 指定ノードグループ内 「ノードグループ名」で関連付けを行うノードグループを指定できます。 ・ 全てのノードを管理 すべてのノードを管理対象にします。

「Administrator」グループ、または、[管理対象ノード]で「指定ノードグループ内」を選択したとき、各用途のサイズ制限およびしきい値を設定できます。

表2.3 各用途のサイズ制限およびしきい値の設定

用途	サイズ制限	しきい値監視
ユーザーグループ全体	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。 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。 ・ 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 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。	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。 警告メッセージは運用ログに出力されます。
リポジトリ	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。 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。	指定できません。
保管ログ	保管ログの総容量を[最大サイズ]にMB単位で指定します。 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。 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。 [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。	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。 警告メッセージは運用ログに出力されます。
ノードログ	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。 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。 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。 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。	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。 警告メッセージは運用ログに出力されます。

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、『解説書』の「3.2.1 ディスク資源の見積り」を参照してください。

注意

- 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『解説書』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。

2.3.2.2 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。

項目	設定内容
ユーザーグループ名	ユーザーグループ名を指定します。
認証方式	認証方式を指定します。
多要素認証 (MFA)	多要素認証を指定します。
iRMCログイン/AVR	iRMCログイン/AVRの使用可否を設定します。
LDAPグループ連携	連携LDAPグループの構成とLDAPグループユーザーのユーザーロールを設定します。
説明	ユーザーグループの説明(コメント)を入力します。
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。
各用途のサイズ制限およびしきい値の設定	詳細は、「2.3.2.1 ユーザーグループを追加する」の「表2.3 各用途のサイズ制限およびしきい値の設定」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。

注意

- 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。
  - 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。
  - 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。

- ユーザーグループ名を変更する場合は、事前に以下のタスクが実行中でないことを確認してください。
  - ファームウェアデータのインポート操作
  - ファームウェアのアップデート操作
  - OSインストールファイルのインポート操作
  - プロファイルの適用
  - 手動ログ収集
  - 定期ログ収集

2.3.2.3 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。
   - 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。
   - 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。

注意

- 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。

2.3.3 Microsoft Active DirectoryまたはLDAPと連携する

ディレクトリーサーバーと連携することで、ユーザーとパスワードを一元的に管理できます。

ディレクトリーサーバーを使ったユーザーとパスワードの管理方法には、以下の2種類があります。

- ISMで作成したユーザーのパスワードを、ディレクトリーサーバーで管理する

  ISMにログインするとき、ディレクトリーサーバーで管理するパスワードを使って認証します。ISMとディレクトリーサーバーの両方に同じ名前のユーザーを作成して運用します。
- ディレクトリーサーバーでユーザーとパスワードを管理する

  ディレクトリーサーバーで管理するユーザー名と、そのパスワードを使用してISMへログインできます。ISMでユーザーを作成する必要はありません。

2.3.3.1 ISMで作成したユーザーのパスワードをディレクトリーサーバーで管理する

以下の手順で設定します。

1. ディレクトリーサーバーと連携するユーザーを、ディレクトリーサーバーに登録します。
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. ディレクトリーサーバー情報が設定されていない場合、LDAPサーバーの情報を設定します。

   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。

   b. 画面左側のメニューから[LDAPサーバー]を選択します。

   c. 「ユーザー連携」で「プライマリー」または「セカンダリー」を選択します。

   d. [アクション]ボタンから[編集]を選択します。
   「LDAPサーバー設定編集」画面が表示されます。

   e. LDAPサーバーの情報を設定します。

   設定内容については、ディレクトリーサーバーの管理者に確認してください。

項目	設定内容
ホスト名	ディレクトリーサーバー名を指定します。以下のどれかを指定します。 ・ 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	ディレクトリーサーバー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。ディレクトリーサーバーの登録内容に依存します。 例） ・ LDAPの場合：ou=Users,ou=system ・ Microsoft Active Directoryの場合：DC=company,DC=com
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。 ・ LDAPの場合：uid ・ Microsoft Active Directoryの場合：sAMAccountName
バインドDN	ディレクトリーサーバー上で、検索できるアカウントを指定します。ディレクトリーサーバーの登録内容に依存します。 例） ・ 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 またはldap_search@company.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	ディレクトリーサーバーとの接続にSSLを使用したい場合、SSL証明書を設定します。

ディレクトリーサーバーとの接続にSSLを使用したい場合、以下のように設定してください。

ー LDAPサーバー名は、ldaps://から指定してください。

ー ポート番号をSSL通信用のポート番号（例：636）を指定してください。

ー 以下のSSL証明書を設定してください。

- SSL証明書は、事前にAdministrator/ftpディレクトリーにアップロード後、設定してください。
- 設定後、アップロードしたSSL証明書は不要ですので削除してください。
- SSL証明書に記載されたURLをLDAPサーバー名に指定してください。

Microsoft Active DirectoryのSSL証明書を設定する手順例

1. [コントロールパネル] - [管理ツール] - [証明機関] を選択します。

2. 目的のサーバーを右クリックし、[プロパティ] - [全般] - [CA証明書] を選択します。
3. 証明書を確認し、[証明書の表示]を選択します。
4. 表示されたダイアログの詳細を選択し、ファイルにコピーを選択します。
5. 証明書のエクスポートウィザードで、[次へ] を選択し、「Base64 encoded X509(CER)(S)」を選択して、保存パスを指定し、[完了]を選択します。
6. 保存したファイルを、"Administrator/ftp/"のディレクトリーにアップロードします。
7. 上記のファイル名を指定します（Administrator/ftpの指定は不要です）。

4. 認証方式にMicrosoft Active DirectoryまたはLDAPを設定したユーザーグループをISMに用意します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ユーザーグループ]を選択し、ユーザーグループを追加します。

   登録する情報は以下のとおりです。

項目	設定内容
ユーザーグループ名	任意のグループ名を指定します。
認証方式	「Open LDAP / Microsoft Active Directory(LDAP)」を指定します。
LDAPグループ連携	[LDAPサーバーのグループと連携する]のチェックを外します。

   上記以外の情報については、「2.3.2.1 ユーザーグループを追加する」を参照してください。

5. 手順1でディレクトリーサーバーに登録したユーザーを、手順4で作成したISMのユーザーグループに追加します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ユーザー]を選択し、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。
ISM連携	連携用のユーザーとして使用する場合に指定します。
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。
認証方式	「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。

6. 手順5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。

   以下を指定して、ログインしてください。

   ー ユーザー名

   ISMに登録したユーザー名

   ー パスワード

   ディレクトリーサーバー上のユーザーのパスワード

注意

ディレクトリーサーバーで、バインドDNで指定したユーザーのパスワードを変更した場合、ISMの設定には反映されません。ISMのLDAPサーバーの設定で、パスワードを変更してください。

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。

連携解除後のユーザーのパスワードは、ユーザーの登録、変更操作で設定したパスワードが有効になります。

- ユーザーの連携を解除する

  以下のどちらかを行ってください。

  ー 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する

  a. 全ノードを管理するユーザーグループに属し、Administratorロールを持つユーザーでログインします。

  b. 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。

  c. 画面左のメニューから[ユーザー]を選択します。
  「ユーザーリスト」画面が表示されます。

  d. 連携を解除するユーザーを選択して、[アクション]-[編集]を選択します。

  e. 「ユーザー設定編集」画面で、ユーザーグループ名を、連携していないユーザーグループに変更します。

  ー ユーザーの認証方式を「Infrastructure Manager(ISM)」に変更する

  a. 全ノードを管理するユーザーグループに属し、Administratorロールを持つユーザーでログインします。

  b. 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。

  c. 画面左のメニューから[ユーザー]を選択します。
  「ユーザーリスト」画面が表示されます。

  d. 連携を解除するユーザーを選択して、[アクション]-[編集]を選択します。

  e. 「ユーザー設定編集」画面で、[認証方式]に「Infrastructure Manager(ISM)」を選択し、[適用]ボタンを選択します。

- ユーザーグループの連携を解除する

  1. 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。
  2. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
  3. 画面左のメニューから[ユーザーグループ]を選択します。
  「ユーザーグループリスト」画面が表示されます。
  4. LDAPグループ連携を解除するユーザーグループを選択して、[アクション]-[編集]を選択します。
  5. 「ユーザーグループ編集」画面で、[認証方式]に「Infrastructure Manager(ISM)」を選択し、[適用]ボタンを選択します。

2.3.3.2 ディレクトリーサーバー上でユーザーとパスワードを管理する

以下の手順で設定します。

1. Microsoft Active Directoryと連携するグループとユーザーを、ディレクトリーサーバーに登録します。
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. ディレクトリーサーバー情報が設定されていない場合、LDAPサーバーの情報を設定します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[LDAPサーバー]を選択します。

c. [グループ連携]で対象のLDAPサーバーを選択し、[アクション]ボタンから[編集]を選択します。

「LDAPサーバー設定編集」画面が表示されます。

d. LDAPサーバーの情報を設定します。

ユーザーアカウントとの連携は、Microsoft Active Directoryのみ対応しています。設定内容については、ディレクトリーサーバーの管理者に確認してください。

項目	設定内容
LDAPサーバー設定	ドメインの設定を有効とするか無効とするかを指定します。
CAS連携	CASの有効／無効を指定します。 ・ 有効:CASを利用する。 ・ 無効:CASを利用しない。
ホスト名	ディレクトリーサーバー名を指定します。以下のどれかを指定します。 ・ 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	ディレクトリーサーバー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。ディレクトリーサーバーの登録内容に依存します。 例） Microsoft Active Directoryの場合:DC=company,DC=com
バインドDN	ディレクトリーサーバー上で、検索できるアカウントを指定します。ディレクトリーサーバーの登録内容に依存します。 例） ・ Microsoft Active Directoryの場合:ldap_search@company.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	ディレクトリーサーバーとの接続にSSLを使用したい場合、SSL証明書を設定します。
ホスト設定	ディレクトリーサーバーの設定を有効にする場合はチェックを付けます。

ホスト名、ポート番号、SSL証明書、ホスト設定は複数指定できます。複数指定した場合、上から順にアクティブなディレクトリーサーバーとして使用します。

ディレクトリーサーバーとの接続にSSLを使用したい場合、以下のように設定してください。

ー LDAPサーバー名は、ldaps://から指定してください。

ー ポート番号をSSL通信用のポート番号（例:636）を指定してください。

ー 以下のSSL証明書を設定してください。

- SSL証明書は、事前にAdministrator/ftpディレクトリーにアップロード後、設定してください。
- 設定後、アップロードしたSSL証明書は不要ですので削除してください。
- SSL証明書に記載されたURLをLDAPサーバー名に指定してください。

Microsoft Active DirectoryのSSL証明書を設定する手順例

1. [コントロールパネル] - [管理ツール] - [証明機関] を選択します。
2. 目的のサーバーを右クリックし、[プロパティ] - [全般] - [CA証明書] を選択します。
3. 証明書を確認し、[証明書の表示]を選択します。

4. 表示されたダイアログの詳細を選択し、ファイルにコピーを選択します。
5. 証明書のエクスポートウィザードで、[次へ] を選択し、「Base64 encoded X509(CER)(S)」を選択して、保存パスを指定し、[完了]を選択します。
6. 保存したファイルを、"Administrator/ftp/"のディレクトリーにアップロードします。
7. 上記のファイル名を指定します（Administrator/ftpの指定は不要です）。

4. ディレクトリーサーバー上のグループと対応するISMのユーザーグループを作成します。
   a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
   b. 画面左側のメニューから[ユーザーグループ]を選択し、ユーザーグループを追加します。

   登録する情報は以下のとおりです。

項目	設定内容
ユーザーグループ名	任意のグループ名を指定します。
認証方式	「Open LDAP / Microsoft Active Directory(LDAP)」を指定します。
LDAPグループ連携	[LDAPサーバーのグループと連携する]にチェックを付け、以下を指定します。 ・ 連携LDAPグループ ドメイン名とそのドメインに存在するグループ名を指定します。 ・ LDAPグループユーザーのユーザーロール ユーザーロールを指定します。

   上記以外の情報については、「2.3.2.1 ユーザーグループを追加する」を参照してください。

5. 手順4で登録した「連携LDAPグループ」に所属するユーザーを使用して、以下の指定方法でISMにログインできることを確認します。

   ー ユーザー名

   ディレクトリーサーバー上のユーザー名を、「＜ユーザー名＞@＜ドメイン名＞」の形式で指定します。

   ー パスワード

   ディレクトリーサーバー上のユーザーのパスワード

   ログインするユーザーが複数のユーザーグループに所属している場合、「ログインユーザーグループ選択」画面が表示されます。ログインするユーザーグループを指定してください。

ポイント

- ディレクトリーサーバー上のユーザーでISMにログインした場合、ISM内にユーザーが作成されます。
- ディレクトリーサーバー上のユーザーを削除、またはグループから外した場合は、ISMに作成されたユーザーを削除してください。
- ドメインが異なるユーザーは、ユーザー名が同じでも、別ユーザーとして扱われます。

注意

- ディレクトリーサーバー上のユーザーとの連携は、Microsoft Active Directoryのみ対応しています。
- ディレクトリーサーバー上のユーザーと連携した場合、FTP、SSHは使用できません。
- ディレクトリーサーバー上のユーザーと同じ名前のユーザーがISMに存在した場合、ディレクトリーサーバー上のユーザーでISMにログインできません。ISMのユーザーを削除、またはユーザー名を変更してください。

- ログイン時のユーザーの指定方法によって、それぞれ以下のように扱われます。

  ー @ドメイン名を指定する場合

    Microsoft Active Directoryグループ連携のユーザー

  ー @ドメイン名を指定しない場合

    「2.3.3.1 ISMで作成したユーザーのパスワードをディレクトリーサーバーで管理する」対象のユーザー

    または、Microsoft Active DirectoryおよびLDAPと連携しないユーザー

  ドメイン名では、大文字と小文字は区別されません。

- [適用]ボタンまたは[テスト]ボタンを選択時にLDAPサーバーの設定を有効にすると、すべてのディレクトリーサーバーとの接続を確認します。
- [適用]ボタンまたは[テスト]ボタンを選択すると、ホスト設定のチェックが付いたディレクトリーサーバーとの接続を確認します。
- ディレクトリーサーバーで、バインドDNで指定したユーザーのパスワードを変更した場合、ISMの設定には反映されません。ISMのLDAPサーバーの設定で、パスワードを変更してください。

設定解除手順

ディレクトリーサーバー上のユーザーアカウント連携を解除する方法は、以下のとおりです。

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

   「ユーザーグループリスト」画面が表示されます。
4. LDAPグループ連携を解除するユーザーグループを選択して、[アクション]-[編集]を選択します。
5. 「ユーザーグループ編集」画面で、[LDAPグループ連携]-[連携LDAPグループ]の一覧から解除するLDAPグループ名の後ろの[x]を選択して削除し、[適用]ボタンを選択します。

   LDAPグループ連携をすべて解除し、ユーザーグループが不要となった場合は、ユーザーグループに所属するユーザーをすべて削除し、ユーザーグループを削除してください。

   詳細は、「2.3.1.3 ユーザーを削除する」、「2.3.2.3 ユーザーグループを削除する」を参照してください。

2.3.4 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。

- 2.3.4.1 ノードグループを追加する
- 2.3.4.2 ノードグループを編集する
- 2.3.4.3 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。

2.3.4.1 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。

2.3.4.2 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。
   - ノード割当てを解除する場合:[未割り当て]
   - 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2.4 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2.4 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 CXシャーシ	-	PRIMERGY CXサーバー	
PRIMERGY CXサーバー	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	-	
PRIMEQUEST 4000シリーズシャーシ	-	PRIMEQUEST 4000シリーズパーティション	
PRIMEQUEST 4000シリーズパーティション	PRIMEQUEST 4000シリーズシャーシ	-	
ETERNUS DX（ISM 2.9.0.030以降、ETERNUS DX900 S5を除く）	-	ドライブエンクロージャ	
ETERNUS DX900 S5（ISM 2.9.0.030以降） ETERNUS DX900 S6 (ISM 3.0.0.010以降)	-	フロントエンドエンクロージャ／コントローラーエンクロージャ／ドライブエンクロージャ	
フロントエンドエンクロージャ	ETERNUS DX900 S5 ETERNUS DX900 S6	-	
コントローラーエンクロージャ	ETERNUS DX900 S5 ETERNUS DX900 S6	-	
ドライブエンクロージャ	ETERNUS DX（ETERNUS DX900 S5, ETERNUS DX900 S6も含む）	-	
ETERNUS NR/AX/HX/AC（Ontap）クラスタ	-	ETERNUS NR/AX/HX/AC（Ontap）シャーシ	
ETERNUS NR/AX/HX/AC（Ontap）シャーシ	ETERNUS NR/AX/HX/AC（Ontap）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/AX/HX/AC（Ontap）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	-	

モデル	親ノード	子ノード	アイコン
C-Fabric	-	CFX2000シリーズ）	
CFX2000シリーズ	C-Fabric	-	

2.3.4.3 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。

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。
   - 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

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。

注意

ノード間で親子の繋がりがあるノードの親ノードが登録された場合、子ノードが自動的に登録されます。
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2.4 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。

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。

   自動検出で検出された機器は、[検出ノードリスト]に表示されます。手順8へ進みます。

   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。

   https://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。

   注意

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

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、FQDN、またはホスト名で指定します。 IPアドレスの検出範囲は、第3オクテットまで指定できます。
検出対象	以下から選択します。 ・ Server (iRMC/BMC) サーバー、PRIMEQUEST 3800Bを検出する場合に選択します。 ・ PRIMERGY 2/4/8WAY M7以降 (HTTPS) PRIMERGY M7シリーズ以降を検出する場合に選択します。 ・ PRIMERGY 2/4/8WAY M7以降, PRIMERGY RX1440/2450 M2 (HTTPS) PRIMERGY M7シリーズ以降、PRIMERGY RX1440/2450 M2を検出する場合に選択します。 ・ PRIMERGY 2/4/8WAY M7以降, PRIMERGY 1WAY M6以降, PRIMERGY RX1440/2450 M2 (HTTPS) PRIMERGY M7シリーズ以降、PRIMERGY 1WAY M6以降、PRIMERGY RX1440/2450 M2を検出する場合に選択します。 ・ PRIMERGY CX1430 M1, PRIMERGY GX, PRIMERGY RX2450 M1 (BMC + HTTPS) PRIMERGY CX1430 M1、PRIMERGY GX、またはPRIMERGY RX2450 M1 を検出する場合に選択します。 ・ PRIMERGY CX1430 M1, PRIMERGY GX (BMC + HTTPS) PRIMERGY CX1430 M1、またはPRIMERGY GX 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PRIMEQUEST 3000シリーズを検出する場合に選択します。 ・ PRIMEQUEST4000 (HTTPS) PRIMEQUEST 4000シリーズを検出する場合に選択します。 ・ Switch, Storage (SSH + SNMP) ストレージ、ネットワークスイッチを検出する場合に選択します。 ・ OntapCluster（HTTPS + SSH + SNMP) OntapClusterを検出する場合に選択します。 ・ Facility (SNMP) PDU、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)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 2/4/8WAY M7以降, PRIMERGY 1WAY M6以降, PRIMERGY RX1440/2450 M2 (HTTPS)を選択した場合

設定項目		説明
HTTPS		－
	ポート番号	HTTPSのポート番号（初期値:443）

表3.4 [検出対象]でPRIMERGY CX1430 M1, PRIMERGY GX, PRIMERGY RX2450 M1 (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3.5 [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）
	コミュニティー	SNMPのコミュニティー名

表3.6 [検出対象]でPRIMEQUEST4000 (HTTPS)を選択した場合

設定項目		説明
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3.7 [検出対象]でSwitch, Storage (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）
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）

設定項目		説明
	コミュニティー	SNMPのコミュニティー名

表3.8 [検出対象]でOntapCluster (HTTPS + SSH + SNMP)を選択した場合

設定項目		説明
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 [注]	HTTPSのポート番号（初期値:443）
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 [注]	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 [注]	SNMPのポート番号（初期値:161）
	コミュニティー	SNMPのコミュニティー名

[注]:ポート番号は変更できません。

表3.9 [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）
コミュニティー	SNMPのコミュニティー名

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3.10 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	・ 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	・ 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。 暗号化手順については、『REST API リファレンスマニュアル』の「2.4 暗号化」を参照してください。 ・ 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。

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

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

- PRIMERGY 2/4/8WAY M7以降、PRIMERGY 1WAY M6以降、PRIMERGY RX1440/2450 M2 (HTTPS)を検出する場合の記載例:

```
"IpAddress","HttpsAccount","HttpsPassword","NewHttpsPassword","HttpsPort"
"192.168.10.11","admin1","********","********",""
"192.168.10.12","admin2","********","********",""
```

- Switch, Storage (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。

   通信結果が失敗となった装置については、下記の対処内容を確認し、再度検出してください。

   通信結果のアイコン[]または[]にマウスカーソルを合わせると、ツールチップが表示されエラー内容を確認できます。

通信方法	アイコン	ツールチップ	説明／対処内容
PING		-	通信成功
		通信に失敗しました。	通信失敗 IPアドレスに誤りがないか、またはネットワークに問題がないか確認してください。
SNMP		-	通信成功
		ポートが閉塞しています。	指定した通信のポートが閉塞 ポート番号に誤りがないか確認してください。
		通信に失敗しました。	通信失敗 対象装置に異常が発生していないか、またはユーザー名、パスワード、ポート番号に誤りがないか確認してください。
		認証に失敗しました。	(SNMPv3の場合のみ) 認証失敗 ユーザー名、パスワードに誤りがないか確認してください。 装置によってはSNMPv3のユーザー名、パスワードを誤った場合に通信失敗になる可能性があります。
		通信方法が指定されていません。	ユーザー名、パスワードが未指定 以下の装置を検出する場合は指定してください。 PRIMEQUEST2000／PRIMEQUEST3000E／Switch／Storage／Facility

通信方法	アイコン	ツールチップ	説明／対処内容
		通信が実施されませんでした。	他の通信が失敗したため未実施 失敗した他の通信のツールチップを確認し、該当する対処内容を確認してください。
IPMI		-	通信成功
		ポートが閉塞しています。	指定した通信のポートが閉塞 ポート番号に誤りがないか確認してください。
		通信に失敗しました。	通信失敗 ユーザー名、パスワード、ポート番号に誤りがないか、または対象装置に異常が発生していないか確認してください。
		通信方法が指定されていません。	ユーザー名、パスワードが未指定 以下の装置を検出する場合は指定してください。 Server／PRIMERGY CX1430 M1／PRIMERGY GX／PRIMERGY LX／PRIMEQUEST2000／PRIMEQUEST3000E
		通信が実施されませんでした。	他の通信が失敗したため未実施 失敗した他の通信のツールチップを確認し、該当する対処内容を確認してください。
SSH		-	通信成功
		ポートが閉塞しています。	指定した通信のポートが閉塞 ポート番号に誤りがないか確認してください。
		通信に失敗しました。	通信失敗 ユーザー名、パスワード、ポート番号に誤りがないか、または対象装置に異常が発生していないか確認してください。
		通信方法が指定されていません。	ユーザー名、パスワードが未指定 以下の装置を検出する場合は指定してください。 PRIMEQUEST2000／PRIMEQUEST3000E／Switch／Storage
		通信が実施されませんでした。	他の通信が失敗したため未実施 失敗した他の通信のツールチップを確認し、該当する対処内容を確認してください。
HTTPS		-	通信成功
		ポートが閉塞しています。	指定した通信のポートが閉塞 ポート番号に誤りがないか確認してください。
		通信に失敗しました。	通信失敗 ポート番号に誤りがないか、または対象装置に異常が発生していないか確認してください。
		認証に失敗しました。	認証失敗 ユーザー名、パスワードに誤りがないか確認してください。
		通信方法が指定されていません。	ユーザー名、パスワードが未指定 以下の装置を検出する場合は指定してください。 Server／PRIMERGY CX1430 M1／PRIMERGY GX

通信方法	アイコン	ツールチップ	説明／対処内容
		通信が実施されませんでした。	他の通信が失敗したため未実施 失敗した他の通信のツールチップを確認し、該当する対処内容を確認してください。

8. 登録するノードのチェックボックスを選択します。
9. [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。

    ー ノード情報の入力

表3.11 ノード情報の詳細

設定項目	設定内容
ノード名	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。 /¥:*?"<>| ノード名には、初期値として以下が入力されています。 ・ 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 xxxx、yyyyに表示される文字列は、以下のとおりです。 ー 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：PDU、UPS ー yyyy ノードのシリアル番号です。検出時にノードのシリアル番号が取得できなかった場合はIPアドレスが表示されます。 ノードがOntapクラスタの場合、シリアル番号の代わりにクラスタUUIDが表示されます。
シャーシ名	PRIMERGY CXが検出された場合に、シャーシ名を入力します。 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。 /¥:*?"<>| シャーシ名には初期値として「SV_zzzz」が入力されています。 zzzzには、シャーシのシリアル番号が表示されます。検出時にシャーシのシリアル番号が取得できなかった場合はIPアドレスが表示されます。
IPアドレス	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。 []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。 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。

設定項目	設定内容
	https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/
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。

ー 通信方法の入力

通信方法の設定が必要なノードが表示されます。各ノードの[設定]を選択し、通信方法を入力してください。

11. 検出ノード登録情報の入力を完了後、[登録]ボタンを選択します。

    ISM 3.0.0.010以降では、[登録]ボタンを選択前に[認証確認]ボタンを選択すると、入力した認証情報が正しいか確認できます。

12. 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。

    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。

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

14. [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3.12 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のバージョンを選択します。
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。入力しない場合は、初期値のポート番号が設定されます。 ・ Windowsの場合：WinRMサービスのポート番号（初期値：5986） ・ Azure Stack HCIの場合：WinRMサービスのポート番号（初期値：5986） ・ Linuxの場合：SSHサービスのポート番号（初期値：22）

15. 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。

注意

以下の対象機種のノード登録時にパスワードまたはIPアドレスの変更に失敗した場合、装置側で変更後、ISMのノード詳細画面で設定してください。

- PRIMERGY M7シリーズ
- PRIMERGY 1WAY M6
- PRIMERGY RX1440 M2

- PRIMERGY RX2450 M2
- PRIMEQUEST 4000シリーズ

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。

   「ノード手動登録」ウィザードの「1.ノード情報」画面は、[ノードタイプ]と[モデル]の選択の組み合わせに応じて、[通信方法]の表示内容が異なります。

   下記表を参考に該当する[通信方法]の表示に合わせて、設定してください。

表3.13 [ノードタイプ]と[モデル]の組み合わせによる[通信方法]

ノードタイプ	モデル	[通信方法]の設定
server	PRIMERGY M7シリーズ以降、 PRIMERGY 1WAY M6以降、 PRIMERGY RX1440 M2、 PRIMERGY RX2450 M2、 PRIMEQUEST 4000シリーズ	表3.22 通信方法に[HTTPS]が表示された場合
	PRIMERGY RX/TXシリーズ（RX2450 M1以外）、 PRIMERGY CXシリーズ（CX1430 M1以外）、 PRIMEQUEST 3800B、IPCOM VX2シリーズ	表3.14 通信方法に[iRMC]が表示された場合
	PRIMERGY CX1430 M1、PRIMERGY GX、 PRIMERGY RX2450 M1	表3.15 通信方法に[BMC][HTTPS]が表示された場合
	PRIMERGY LX	表3.16 通信方法に[BMC]が表示された場合
	PRIMEQUEST 2000シリーズ、 PRIMEQUEST 3000シリーズ（PRIMEQUEST 3800B以外）	表3.17 通信方法に[MMB][SSH][SNMP]が表示された場合
	Generic Server（IPMI）	表3.16 通信方法に[BMC]が表示された場合
	Generic Server（SNMP）	表3.19 通信方法に[SNMP]が表示された場合
	Other	表3.20 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合
switch	下記モデル以外のスイッチ	表3.18 通信方法に[SSH][SNMP]が表示された場合
	Generic Switch（SNMP）	表3.19 通信方法に[SNMP]が表示された場合
	Other	表3.20 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合
	SH-E514TR1、ICX6430、Generic Switch（PING）	通信設定はありません。
storage	下記モデル以外のストレージ[注]	表3.18 通信方法に[SSH][SNMP]が表示された場合
	ETERNUS CS800 S7、Generic Storage（SNMP）[注]	表3.19 通信方法に[SNMP]が表示された場合

ノードタイプ	モデル	[通信方法]の設定
	ETERNUS AB/HBシリーズ	表3.21 通信方法に[HTTPS][SNMP]が表示された場合
	OntapCluster	表3.23 通信方法に[HTTPS][SSH][SNMP]が表示された場合
	other	表3.20 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合
	Generic Storage（PING）	通信設定はありません。
facility	下記モデル以外のファシリティー	表3.19 通信方法に[SNMP]が表示された場合
	other	表3.20 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合
	Generic Facility（PING）	通信設定はありません。
other	－	表3.20 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合

[注] ETERNUS DX900 S5の[通信方法]の設定は、ISM 2.9.0.020以前は[SNMP]、ISM 2.9.0.030以降は[SSH][SNMP]を表示します。ISM 2.9.0.020以前に登録したノードは、ISM 2.9.0.030で追加した新機能を利用できません。そのため、一度ノードを削除した上で、ISM 2.9.0.030以降で再度ノードを登録してください。

表3.14 通信方法に[iRMC]が表示された場合

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3.15 通信方法に[BMC][HTTPS]が表示された場合

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）※PRIMERGY GX2570 M5の場合は8080

表3.16 通信方法に[BMC]が表示された場合

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）

表3.17 通信方法に[MMB][SSH][SNMP]が表示された場合

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]		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）
	コミュニティー	PRIMEQUESTのSNMPコミュニティー名

[注]：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3.24 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 通信方法に[SSH][SNMP]が表示された場合

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 [注1]	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2]		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）
	コミュニティー	登録するノードのSNMPコミュニティー名

[注1]：[モデル]でCisco Catalyst switchを選択した場合に表示されます。

[注2]：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3.24 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 通信方法に[SNMP]が表示された場合

設定項目		説明
SNMP [注]		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）
	コミュニティー	登録するノードのSNMPコミュニティー名

[注]：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3.24 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 通信方法に[iRMC/BMC][HTTPS][SSH][SNMP]が表示された場合

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]		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）
	コミュニティー	登録するノードのSNMPコミュニティー名

[注]：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3.24 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 通信方法に[HTTPS][SNMP]が表示された場合

設定項目		説明
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）
SNMP [注]		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）
	コミュニティー	登録するノードのSNMPコミュニティー名

[注]：ETERNUS AB/HBシリーズはSNMPv2のみをサポートします。

表3.22 通信方法に[HTTPS]が表示された場合

設定項目		説明
iRMCのパスワードを変更する		iRMCのパスワードを工場出荷時の状態から変更していない場合は、チェックボックスをオンにします（初期値：オフ）
	現在のパスワード [注1]	iRMCの現在のパスワード
	新しいパスワード [注1]	iRMCの新しいパスワード
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 [注2]	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）

[注1]：[iRMCのパスワードを変更する]チェックボックスがオンの場合に表示されます。

[注2]：[iRMCのパスワードを変更する]チェックボックスがオンの場合は、[新しいパスワード]と同じものが表示されます。編集はできません。

表3.23 通信方法に[HTTPS][SSH][SNMP]が表示された場合

設定項目		説明
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 [注2]	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 [注2]	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：オン）
	バージョン	SNMPのバージョン
	ポート番号 [注2]	SNMPのポート番号（初期値：161）
	コミュニティー	登録するノードのSNMPコミュニティー名

[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3.24 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。

[注2]：ポート番号は変更できません。

表3.24 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（最低8文字）
	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（最低8文字）

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]-[ノード]を選択し、ノードの登録を確認します。

   ISM 3.0.0.010以降では、ノードの登録前に[認証確認]ボタンを選択すると、入力した認証情報が正しいか確認できます。

   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。

5. 「ノードリスト」画面から対象のノード名を選択し、ノードの詳細画面-[OS]タブを選択します。
6. [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3.25 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のバージョンを選択します。
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。入力しない場合は、初期値のポート番号が設定されます。 ・ Windowsの場合：WinRMサービスのポート番号（初期値：5986） ・ Azure Stack HCIの場合：WinRMサービスのポート番号（初期値：5986） ・ Linuxの場合：SSHサービスのポート番号（初期値：22）

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。

注意

以下の対象機種のノード登録時にパスワードの変更に失敗した場合、装置側で変更後、ISMのノード詳細画面で設定してください。

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

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サーバーに、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、「2.2.1 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トラップが連続して発生する状況において、トラップを受信してから指定された期間内は受信時の動作を実行しません。受信時の動作とはアラーム設定で設定されたアクションとイベントログ(運用ログ、SNMPトラップ)への記録を指します。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[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「2.対象」画面の[対象種別]でアラーム設定の対象を以下から選択します。

   ー ノード(個別)

   アラーム設定の対象とするノードを選択します。

   ー ノード(全ノード)

   すべてのノードがアラーム設定の対象になります。

   ー ノード(ノードグループ)

   アラーム設定の対象とするノードグループを選択します。選択したノードグループに所属するノードがアラーム設定の対象となります。

   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. 「5.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
  コミュニティー: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。

ポイント

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

注意

- トラップ受信設定の追加／編集／削除を行った場合、変更は即時適用されます。リクエストを受け付けてから反映されるまで、一時的にすべてのSNMPトラップを受信しない状態となります。トラップ受信設定を変更する場合は、上記事象が問題とならないことを確認したうえで行ってください。
- SNMPv3のトラップ受信を行う場合、ノードごとにSNMPトラップ受信設定が必要になります。ノード登録後、SNMPトラップ受信設定を行ってください。
- ノードに設定されている「エンジンID」を変更した場合、ノード情報取得を行い、取得した最新の「エンジンID」を再設定してください。
- 機器によっては、ノード情報取得による「エンジンID」の取得ができません。ノードの設定詳細やノード情報取得による「エンジンID」の取得についての詳細は、『解説書』の「A.2.2 ノード設定詳細」を参照してください。
- 多数のトラップを同時に受信した場合は順次処理されるため、テストトラップなどの意図したトラップや、事象発生時のトラップの受信処理が遅れることがあります。トラップ受信の対象機器の構成を見直し、1件/秒を目安にトラップ受信量を軽減してください。

MIBファイルを追加する

ISM未サポートの当社外装置、CiscoスイッチやHPサーバーなどエフサステクノロジーズ以外のベンダーから提供されているハードウェアを監視する場合、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が行われます。

ISMがサポートする機器については、当社の本製品Webサイトで『管理対象機器一覧』を参照してください。

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

除外トラップを登録する

除外トラップリストにトラップを追加することで、同一ノードからの同一トラップの受信を抑止できます。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択します。
2. [SNMPトラップ]タブでトラップ受信を抑止したいトラップを選択します。
3. [除外リストに追加]ボタンを選択します。

   除外リストに追加する内容が表示されます。
4. [適用]ボタンを選択します。

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。
   - ノードがサーバーの場合、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、サーバーの種類によっては、[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。

3.2.4 IPMI有効／無効を設定する

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

対象機種は、以下のとおりです。

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

ノード登録時のデフォルトは、IPMI無効です。IPMI有効に設定する場合、あらかじめ対象機種のiRMCでIPMIを有効化に設定（IPMI over LAN を有効にする）してください。その後、ISMでIPMI有効に設定してください。

IPMIの有効／無効は、以下の手順で設定します。

1. ISMのGUIでグローバルナビゲーションメニューから[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. 表示されるノードリストからIPMIの有効／無効を設定したいノードにチェックを付けます。
3. [アクション]ボタンから[IPMI有効/無効]を選択します。
4. 「IPMI有効/無効」画面で対象ノードを確認します。

   IPMIの設定対象外のノード（サポート外のノード）はグレー表示されます。
5. 対象ノードの[IPMIモード]を設定し、[適用]ボタンを選択します。

ポイント

- 「ノードリスト」画面から対象ノードを選択した後に表示されるノードの詳細画面の[アクション]ボタンからも[IPMI有効/無効]が選択できます。
- ノードの詳細画面の[アクション]ボタンから「IPMI有効/無効」画面を表示した場合は、[一括設定]は表示されません。

3.3 サーバーに各種設定／OSインストールをする

サーバーを初期導入する場合や、新たに増設する場合などに、複数のサーバーに対して以下の操作を一括して行うことができます。

- ハードウェア設定（BIOS、iRMC、MMB）

- OSインストール
- 仮想IOの設定
- RAIDの設定

3.3.1 プロファイルでBIOS／iRMC／MMB／仮想IO／RAID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に登録したサーバーに対して、作成したプロファイルを適用することでサーバーのBIOS／iRMC／MMB／仮想IO／RAID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、「3.3.4 ポリシーを作成してプロファイルの作成を簡略化する」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。

   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。

   【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]ボタンを選択します。

      「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] ボタンを選択します。

      「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] ボタンを選択します。

      「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。

   【ポリシーを使用しRAID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[RAIDポリシー]で、作成した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] ボタンを選択します。

      「2.詳細」画面内の[RAID]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。

【監視ポリシーを使用し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[監視ポリシー]で、[有効]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] ボタンを選択します。

「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。

【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] ボタンを選択します。

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。

6. サーバーの電源をオフにします。

7. 適用対象のプロファイルを選択します。

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。

BIOS／iRMC／MMB／仮想IO／RAID設定が完了すると、「全てのプロファイル」画面内の当該サーバーの[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。
- 「プロファイル追加」ウィザードの「1.基本情報」画面で、[モデル毎プロファイル/ポリシーを選択する] のBIOSやiRMCにチェックを付けてモデルを選択すると、モデル毎のプロファイルを作成できます。

注意

- 以下の場合、プロファイル適用した後にノードの操作が必要な場合があります。
  - ー ノードのシステムボード交換後はプロファイル適用で設定したBIOS／iRMC／MMB／仮想IO／RAIDの設定が失われます。システムボードやPCIカードなどのノードの部品を保守交換した場合は必ずPRIMERGYの電源を起動し、対象ノードのBIOS画面が表示されたことを確認してください。ノード情報取得を取得後、プロファイルを再適用してください。
  - ー モデル毎プロファイルでiRMCのIPアドレスを変更した場合、ISMに登録したノードのIPアドレスは手動で変更が必要です。変更しない場合、そのノードに対するISMの機能は使用できません。機器に対しては、サーバーの再起動後に変更したIPアドレスの設定がiRMCに反映されます。
  - ー モデル毎プロファイルには、設定項目を反映するためにiRMCの再起動が必要な設定項目が存在することがあります。iRMCのWebUI画面を確認し、指示に従いiRMCの再起動をしてください。
- iRMC設定でLDAPが有効で、ノードの詳細画面の[Web I/F URL]のプロトコルがHTTPのとき、iRMCのファームウェアバージョンによっては、BIOS／iRMC設定のプロファイル適用がエラーとなることがあります。この場合、ノードを編集して[Web I/F URL]のプロトコルをHTTPSに設定してください。ノードの編集については、『解説書』の「2.2.3 データセンター／フロア／ラック／ノードの編集」を参照してください。

- モデル毎プロファイルには、iRMC設定と同じ設定項目が存在することがあります。BIOS設定とiRMC設定の同じ設定項目で、異なる設定内容のプロファイルを適用するとiRMC設定が優先されます。

3.3.2 プロファイルでサーバーにOSをインストールする（PXEブート機能を利用する場合）

PXEブート機能を利用して、ISMに登録したサーバーに対して、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

1. OSインストールの事前環境構築として、DHCPサーバーを作成します。

   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。

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

2. 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、『解説書』の「2.13.2 リポジトリ管理機能」を参照してください。

3. 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。
4. 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。

5. [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。

6. 「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。

   設定項目の入力については、ヘルプ画面を参照してください。

   a. 「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]ボタンを選択します。

   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。

   【ポリシーを使用してOS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[OSポリシー]で、作成した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]ボタンを選択します。

      「2.詳細」画面内の[OS]タブと[OS個別情報]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。

   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. サーバーの電源をオフにします。
8. 適用対象のプロファイルを選択します。
9. [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。

10. 「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。

OSインストールが完了すると、「全てのプロファイル」画面内の当該サーバーの[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 プロファイルでサーバーにOSをインストールする(ServerView embedded Lifecycle Managementを利用する場合)

ServerView embedded Lifecycle Management機能(以降、「eLCM」と表記)を利用して、ISMに登録したサーバーに対して、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

1. 事前に対象サーバーにネットワーク環境を構築します。

   a. 対象サーバーで管理LANにネットワーク接続します。

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

   b. プロファイル管理機能でOSインストールを行うためのDHCPサーバーを準備します。

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

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

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

2. 事前に対象サーバーにeLCMの環境を構築します。

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

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

   参照手順

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

   なお、参照手順は、予告なく変更されることがあります。

3. 対象サーバーのbootable SDカードにembedded Installation Management(以降、「eIM」と表記)をダウンロードします。

   a. iRMC設定のプロファイルを利用して、eIMをダウンロードするための設定をします。設定内容については、『プロファイル管理機能プロファイル設定項目集』の「第1章 PRIMERGY・PRIMEQUEST 3000B / 4000E サーバー用プロファイルの BIOS/iRMC設定項目」を参照してください。

      設定方法については、「3.3.1 プロファイルでBIOS／iRMC／MMB／仮想IO／RAIDを設定する」を参照してください。

b. iRMC Webインターフェイスを使用して、対象サーバーのbootable SDカードにeIMをダウンロードします。

eIMのダウンロード方法については、手順1で参照したマニュアルを参照してください。

4. eLCMの情報を取得します。

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

b. 画面左側のメニューから[プロファイル適用]を選択します。

c. 対象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]ボタンを選択します。

d. [取得]ボタンを選択します。

ノード情報取得が行われます。

5. 手順3内手順aのプロファイルに、OS設定を追加します。

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

b. 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。

c. 手順3内手順aのプロファイルを選択し、[アクション]ボタンから[編集]を選択します。

「プロファイル編集」ウィザードが表示されます。

d. 「プロファイル編集」ウィザードに従い、設定項目を入力します。

以降の手順については、「3.3.2 プロファイルでサーバーにOSをインストールする（PXEブート機能を利用する場合）」の手順6以降を参照してください。

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。

3.3.4 ポリシーを作成してプロファイルの作成を簡略化する

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。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。

ここでは、以下の手順について説明します。

- 従来のポリシー作成手順
- 監視ポリシー作成手順
- 従来のポリシーから監視ポリシーを参照する手順

従来のポリシー作成手順

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[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。

－ 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。

－ OS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、「OS」を選択します。

－ RAID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、「RAID」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。

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。

ポイント

- OS設定のポリシーは、対象サーバー種別に依存することなく作成可能です。「ポリシー追加」ウィザードの「1.基本情報」画面で、「カテゴリー」に「Server-共通」を選択してください。
- 「ポリシー追加」ウィザードの「1.基本情報」画面で、[モデル毎ポリシーを選択する] にチェックを付け、BIOSまたはiRMCいずれかのポリシータイプからモデルを選択することで、モデル毎のポリシーを作成できます。モデル毎ポリシーでは設定項目をノードから取得することで、より詳細なハードウェア設定を行えます。

注意

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

監視ポリシーの作成手順

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[監視ポリシー設定]を選択します。

   「監視ポリシー」画面が表示されます。
3. [編集]ボタンを選択します。
4. [監視ポリシーを有効する]にチェックを付け、設定項目を入力してください。

   ノード登録時に監視ポリシーを使用する場合、[検出ノード登録時に監視ポリシーを適用する]にチェックを付けてください。

   設定項目の入力は、ヘルプ画面を参照してください。

   監視ポリシーの編集が完了すると、「監視ポリシー設定」画面に表示されます。

従来のポリシーから監視ポリシーを参照する手順

1. 監視ポリシー作成手順に従い、監視ポリシーを作成します。
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[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。
4. [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 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。

5. [監視ポリシー]で、[有効]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。

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。

3.3.5 適用済みのプロファイルとハードウェア設定を比較する

プロファイル適用後、ISMは一定の周期でプロファイルのベリファイを実行します。また、ユーザーが任意のタイミングでプロファイルのベリファイを実行することもできます。プロファイルのベリファイにより、適用したプロファイルの内容とノードのBIOS／iRMC設定内容が比較されます。[ベリファイステータス]が[不一致]になっている場合、該当プロファイルで差異が生じている項目を確認し、ノード設定内容の変更が意図したものかどうかを判断してください。プロファイルの内容とノードの設定内容に差異がないようにプロファイルの編集、プロファイルの再適用などを行って[ベリファイステータス]を[一致]に戻してください。

また、ISM-VA管理機能のプロファイルのベリファイ有効化／無効化設定コマンドを使用して、プロファイルのベリファイを有効化、または無効化ができます。コマンドの詳細は、『解説書』の「4.24 プロファイルのベリファイ有効化／無効化設定」を参照してください。

ここでは、以下の実行方法について説明します。

- プロファイルのベリファイの実行方法
- [ベリファイステータス]が[不一致]の場合に、差異が生じている項目の確認方法
- [不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図しないものである場合）
- [不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図したものである場合）

プロファイルのベリファイの実行方法

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

1. ISMのGUIでグローバルナビゲーションメニューから[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. プロファイルのベリファイを実行するプロファイルを選択します。
4. [アクション]ボタンから[ベリファイ実行]を選択します。

「ベリファイ実行」画面が表示されます。

5. [実行]を選択します。

プロファイルのベリファイが完了すると、「全てのプロファイル」画面内の当該プロファイルの[ベリファイステータス] 列が[一致]または[不一致]と表示されます。

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

[ベリファイステータス]が[不一致]と表示されている場合、該当プロファイルで差異が生じている項目の確認方法は、以下のとおりです。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[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. [ベリファイステータス]が[不一致]になっているプロファイル名を選択します。
4. [BIOS]タブ、または[iRMC]タブを選択します。

差異が生じている場合、「プロファイル設定に差分があります」というメッセージが表示されます。

5. メッセージ下のプルダウンボックスで「実機設定との差分」を選択します。

   差異が生じている項目が赤色で表示されます。

[不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図しないものである場合）

[ベリファイステータス]が[不一致]と表示されており、ノード設定内容の変更が意図しないものである場合、[ベリファイステータス]を[一致]に戻す方法は、以下のとおりです。

1. サーバーの電源をオフにします。ただし、ISM 3.0.0.010以降はサーバーの電源状態に依存せず実行できます。
2. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
3. 画面左側のメニューから[プロファイル設定]-[全てのプロファイル]を選択します。

   「全てのプロファイル」画面が表示されます。
4. [ベリファイステータス]を[一致]に戻すプロファイルを選択します。
5. [アクション]ボタンから[プロファイル適用/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。
6. [高度な設定を有効にする]にチェックを付けます。
7. [適用モード]で「変更がない箇所にも適用を行う」を選択します。

   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。

   プロファイル適用が完了すると、「全てのプロファイル」画面内の当該プロファイルの[ベリファイステータス]列が[一致]と表示されます。

[不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図したものである場合）

[ベリファイステータス]が[不一致]と表示されており、ノード設定内容の変更が意図したものである場合、[ベリファイステータス]を[一致]に戻す方法は、以下のとおりです。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[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. [ベリファイステータス]を[一致]に戻すプロファイルを選択します。
4. [アクション]ボタンから[編集]を選択します。
5. 「プロファイル編集」ウィザードに従い、正しい設定項目を入力します。

   プロファイルの編集が完了すると、当該のプロファイルの[ステータス]が[要再適用]と表示されます。
6. 対象のプロファイルを選択します。
7. [アクション]ボタンから[プロファイル適用/再適用]を選択します。

   「プロファイル適用」画面が表示されます。
8. [高度な設定を有効にする]にチェックを付けます。
9. [適用モード]で「プロファイルをノードに適用せず、ISM上で適用したことにする」を選択します。

   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。
10. 適用したプロファイルを選択します。
11. [アクション]ボタンから[ベリファイ実行]を選択します。

    「ベリファイ実行」画面が表示されます。
12. 「ベリファイ実行」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。

プロファイルのベリファイが完了後、当該プロファイルの[ベリファイステータス]列が[一致]と表示されることを確認してください。

[不一致] と表示されている場合は、手順3から操作し直します。

ポイント

- プロファイルのベリファイでBIOS設定を確認するには、BIOSパラメーターのバックアップファイルがサーバー上に保持されている必要があります。このため、プロファイル適用時にプロファイルのiRMC設定で[自動BIOSパラメーターバックアップ]を有効に指定してください。
- サーバーのiRMC設定で[自動BIOSパラメーターバックアップ]の項目を無効にしている場合や、項目が存在しないサーバーの場合、最新のBIOS設定でプロファイルのベリファイが実行されません。その場合、BIOSのハードウェア設定をバックアップしてから(「7.1.1 サーバーの設定をバックアップする」参照)、プロファイルのベリファイを実行してください(「プロファイルのベリファイの実行方法」参照)。サーバーのiRMC設定に[自動BIOSパラメーターバックアップ]の項目が存在するかの確認は、以下のマニュアルを参照してください。
  - 『ServerView Suite Remote Management iRMC S2/S3 - integrated Remote Management Controller』
  - 『ServerView Suite iRMC Sx Web インターフェース』(Sxには、S4以降の版数が入ります。)
- ノードがメンテナンスモードの場合、ISMによる定期的なプロファイルのベリファイは実行されません。この場合、プロファイルのベリファイは手動で実行してください。
- プロファイルのベリファイで対象外の設定項目があります。対象外の項目は、以下のとおりです。
  - iRMC設定[プロキシサーバー]-[パスワード]
  - iRMC設定[LDAP]-[認証LDAPパスワード]
- 「プロファイル適用」画面で以下両方の条件でプロファイルを適用した場合、[ベリファイステータス]は[ベリファイ失敗]になります。手動でベリファイを実行してください。
  - [適用モード]:「プロファイルをノードに適用せず、ISM上で適用したことにする」

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

注意

- iRMC設定でLDAPが有効で、ノードの詳細画面の[Web I/F URL]のプロトコルがHTTPのとき、iRMCのファームウェアバージョンによっては、プロファイルのベリファイがエラーとなることがあります。この場合、ノードを編集して[Web I/F URL]のプロトコルをHTTPSに設定してください。ノードの編集については、『解説書』の「2.2.3 データセンター／フロア／ラック／ノードの編集」を参照してください。
- サーバーの電源がオンの状態で、BIOS設定を含む[プロファイルの適用／再適用]を実施した場合、[ベリファイステータス]が[不一致]になります。[不一致]を[一致]にするには、プロファイル適用後にサーバーを再起動し、手動でベリファイ実行をしてください。詳細は、『解説書』の「2.4.2.10 プロファイルのベリファイ」を参照してください。
- モデル毎プロファイルのBIOS設定を含むプロファイルに対し[プロファイルの適用／再適用]を実施した場合、サーバーの再起動が必要となります。再起動前の状態では[ベリファイステータス]が[不一致]になります(ISM 3.0.0.010以降)。[不一致]を[一致]にするには、プロファイル適用後にサーバーを再起動し、手動でベリファイ実行をしてください。

3.3.6 検出したノードの登録時にハードウェア設定を適用する

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

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

ポイント

監視ポリシーの作成方法は、「3.3.4 ポリシーを作成してプロファイルの作成を簡略化する」を参照してください。

1. 管理対象ノードを登録します。

   「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」の手順10まで実施してください。

2. 「ノード登録」ウィザードの「4. 監視/ノードグループ/タグ」画面で、[ノード登録時に監視ポリシーを適用する]にチェックを付けます。

3. [次へ]ボタンを選択します。

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

4. 「ノード登録」ウィザードの「5. 確認」画面で、プロファイル名を確認し、[登録]ボタンを選択します。

   表示されたプロファイル名が既存のプロファイル名と重複している場合、[登録]ボタンを選択後、重複しないプロファイル名に変更され、登録されます。

   「結果」画面でプロファイル名を確認できます。

以上で、検出したノードの登録時にハードウェア設定を適用する手順は完了です。

ハードウェア設定の進行状況は、「タスク」画面から確認してください。

注意

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

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変更できます。

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。

   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. ノードの電源をオンにします。

6. 適用対象のプロファイルを選択します。

7. [アクション]ボタンから[プロファイル適用/再適用]を選択します。

   「プロファイル適用」画面が表示されます。

8. 「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。

   プロファイルの適用が完了すると、「全てのプロファイル」画面内の当該プロファイルの[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]ボタンから[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]ボタンから[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 複数のプロファイルを一括して作成しノードに割り当てる

複数のノードに同じ設定を行う場合、既存のプロファイルを参照して複数のプロファイルを一括で作成（一括参照作成）し、複数のノードに割り当てることができます。これにより、多数のプロファイルを作成し、ノードに適用する操作を簡略化できます。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]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. 参照元とするプロファイルを選択し、[アクション]ボタンから[一括参照作成/割り当て]を選択します。
「プロファイル一括参照作成/割り当て」ウィザードが表示されます。
4. 「プロファイル一括参照作成/割り当て」ウィザードに従い、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。
「プロファイル一括参照作成/割り当て」ウィザードで選択した割り当てノード数分のプロファイルが「全てのプロファイル」画面に表示されます。
続けてプロファイルを適用します。
6. 画面左側のメニューから[プロファイル適用]を選択します。
「ノードリスト」画面が表示されます。
7. プロファイルを割り当てたノードを選択し、[アクション]ボタンから[プロファイル適用/再適用]を選択します。
「プロファイル適用」画面が表示されます。
8. 「プロファイル適用」画面に従い、設定項目を入力します。

ポイント

[一括参照作成/割り当て]で作成されたプロファイル、および割り当てられたノードのステータスは、[要再適用]となります。

注意

- OSが設定されたプロファイルを参照して[一括参照作成/割り当て]を行った場合、OSのIPアドレス、コンピューター名が重複する場合があります。プロファイル適用前に、プロファイルを編集してOSのIPアドレス、コンピューター名を変更してください。
- 仮想IOが設定されたプロファイルを参照して[一括参照作成/割り当て]を行った場合、仮想アドレスが重複する場合があります。プロファイル適用前に、プロファイルを編集して仮想アドレスを変更してください。

3.6 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。

3.6.1 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。

   ポイント

   複数の管理対象ノードのパスワードを変更する場合、一括編集が利用できます。「ノードリスト」画面で対象のノードを選択後、[アクション]ボタンから[一括編集]を選択して編集してください。

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。

3.6.2 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。

   ポイント

   複数のOSのパスワードを変更する場合、一括編集が利用できます。「ノードリスト」画面で対象のノードを選択後、[アクション]ボタンから[一括編集]を選択して編集してください。

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。

3.7 サーバーのWeb画面のログインにCASベースのシングルサインオンを利用する

CAS(中央認証サービス)を利用して、ユーザー名、パスワードを指定せず、PRIMERGYサーバーのWeb画面(iRMC画面)へ自動ログイン(シングルサインオン)するための設定を行います。

3.7.1 ディレクトリーサーバーを設定する

Microsoft Active Directoryとグループ連携するように、LDAPサーバーを設定します。

詳細は、「2.3.3 Microsoft Active DirectoryまたはLDAPと連携する」を参照してください。

注意

- CASは、ディレクトリーサーバーが、Microsoft Active Directory の場合のみ使用できます。
- 証明書を登録する場合、LDAPサーバー名にフルコンピューター名を指定してください。

3.7.2 CASを設定する

ISMのログイン後、iRMC画面へのログインを可能とするため、CAS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[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[CAS設定]を選択します。

   「CAS設定」画面が表示されます。
3. [設定]ボタンを選択します。

   「CAS設定」画面が表示されます。
4. 設定項目を入力します。

   設定する情報は、以下のとおりです。

   ― CAS

   CAS機能を有効とするか無効とするかを設定します。

   ― ポート番号

   CASで使用するポート番号を設定します。

   ポート番号に、3170は指定できません。

   ― ユーザーロール

   CASを利用できるユーザーのユーザーロールを設定します。

注意

- CASが再起動後は、[設定]-[ユーザー]-[CAS設定]の「CAS状態」が正常になったあとで、再度ISMにログインしてください。

  CAS再起動のイベントをアラーム設定することで、CASの再起動を通知できます。設定方法は、「2.2 アラーム設定をする（ISM内部のイベント）」、「2.2.1.2 メールを送信する」を参照してください。
- CASを利用する場合、ISMに証明書を設定してください。証明書の設定方法は、『解説書』の「4.7 証明書設定」を参照してください。

3.7.3 CASを利用するユーザーを設定する

CASを利用できるユーザーを以下のように設定します。

1. ユーザーが属するユーザーグループの設定

   ― 管理対象ノード

   「全てのノードを管理」を設定します。

   ― 認証方式

   「Open LDAP/Microsoft Active Directory(LDAP)」を設定します。

   ユーザーグループ設定の詳細は、以下を参照してください。

   ―「2.3.2.1 ユーザーグループを追加する」

   ―「2.3.2.2 ユーザーグループを編集する」
2. ユーザーの設定

   ― ディレクトリーサーバーで行う設定

   「2.3.3.2 ディレクトリーサーバー上でユーザーとパスワードを管理する」で設定したディレクトリーサーバー（LDAPサーバー）にユーザーを設定します。

ー ISMで行うユーザー設定

a. ユーザー名

「2.3.3 Microsoft Active DirectoryまたはLDAPと連携する」で設定したディレクトリーサーバーに存在するユーザー名を設定します。

b. 認証方式

「ユーザーグループの設定に従う」を設定します。

c. ユーザーグループ

1.で設定したユーザーグループを設定します。

d. ユーザーロール

「3.7.2 CASを設定する」で設定したユーザーロールと、CASを利用可能なユーザーロールを以下に示します。

表3.26 CASを利用可能なユーザーロール

CAS設定で指定したユーザーロール	CASを利用可能なユーザーロール
Administrator	Administrator
Operator	Administrator
	Operator
Monitor	Administrator
	Operator
	Monitor

ユーザー設定の詳細は、以下を参照してください。

ー 「2.3.1.1 ユーザーを追加する」

ー 「2.3.1.2 ユーザーを編集する」

注意

設定項目[管理対象ノード]が「全てのノードを管理」以外のユーザーグループに属するユーザーは、CASを利用できません。

3.7.4 iRMCを設定する

「3.7.2 CASを設定する」設定したCASの情報を、iRMCに設定します。

CASを利用するiRMCの[設定]-[ユーザ管理]-[中央認証サービス(CAS)]で以下を設定します。

- CASサポート

  「CASを有効にする」を選択します。

- サーバー

  ISMのIPアドレスを設定します。

- ネットワークポート

  「3.7.2 CASを設定する」で設定したポート番号を設定します。

- ログインページ表示

  [ログインページを常に表示する]にチェックを付けることを推奨します。

  チェックを付けた場合の動作を示します。

  ー ISMのログイン後、iRMCのWeb画面に自動ログイン時、「ログイン」か、「CASログイン」かの選択画面が表示されます。

  - 「ログイン」を選択した場合、iRMCのユーザーアカウントを指定してログインできます。

- 「CASログイン」を選択した場合、自動ログインできます。

- Redfishロール

  [Redfishロール]の設定項目があるサーバーは、「アクセスなし」以外の項目を選択します。

  「アクセスなし」を選択すると、iRMCのWeb画面で「CASログイン」を選択した自動ログインができません。

注意

- 「ログインページを常に表示する」のチェックを外した場合、ISMにログインしないと、iRMCのWeb画面にログインできません。この場合、Webブラウザー上に手動でログイン画面のURLを入力してください。

  ログイン画面のURL例：https://＜iRMCのIPアドレス＞/login

- CAS使用時のiRMCのユーザー権限に、必要以上の権限を与えないようにしてください。

- iRMCの[設定]-[ユーザ管理]-[中央認証サービス(CAS)]-[アクセス許可の割り当て]が「LDAP 許可」の場合、iRMCの[設定]-[ユーザ管理]-[LDAP]-[アクセス設定]-[ユーザログイン検索フィルタ]に「(userPrincipalName=%s)」を設定してください。

3.7.5 ユーザー名、パスワードを指定せずにログインする

以下の手順でiRMCのWeb画面にユーザー名、パスワードを指定せずにログインします。

1. 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]-[ノード]を選択します。

   「ノードリスト」画面が表示されます。
3. ノードリストから、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。
4. ノードの詳細画面の[Web I/F URL]のURLを選択します。

   iRMCのログイン画面が表示されます。
5. 「CASログイン」を選択します。

注意

ISMにログインせずにiRMCのWeb画面で、「CASログイン」を選択すると、ISMのログイン画面が表示されます。

ISMにログイン後は、iRMCの画面は表示されません。ISMのノードの詳細画面で[Web I/F URL]のURLを選択して、iRMCの画面を表示してください。

3.8 ISMからiRMCに直接ログインする

ISMからiRMC Webインターフェイスを表示するには、ノードの詳細画面内[Web I/F URL]にiRMCのIPアドレスを登録しておき、そのURLを選択する従来の方法があります。ただし、この方法では、ログイン操作が必要です。

ここでは、iRMCへのログイン操作を行わずに、直接iRMC Webインターフェイスを表示するiRMCログインの手順について記述します。

注意

ポップアップブロックを解除する必要があります。ご使用のWebブラウザーで、ISMのURLに対してポップアップを許可してください。

3.8.1 中継ルートを設定する

中継ルートは、管理端末と監視対象ノードの間にルーターがあり、管理端末からiRMCに対するアクセスがファイアウォールで制限されている場合に設定します。

管理端末とISM-VAが同一ネットワークに存在する場合や、ファイアウォール設定がされていない場合は中継ルートを設定する必要はありません。

中継ルートの特徴については、『解説書』の「2.3.7.1 iRMCログインによるWebインターフェイス画面表示」で解説しています。

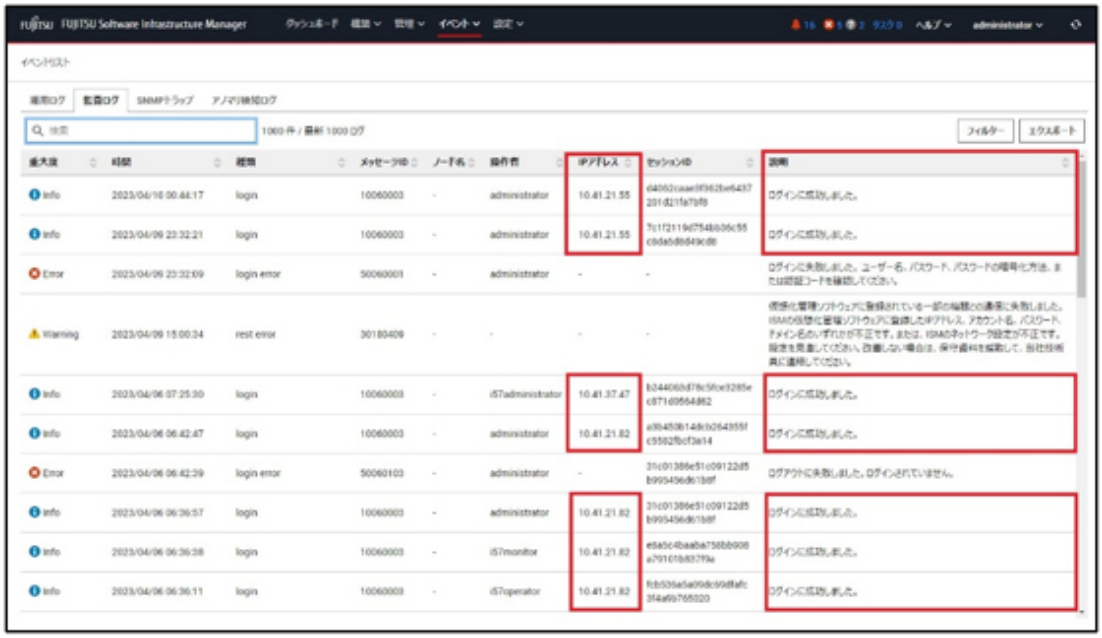
以下の手順で中継ルートを設定することで、中継ルートを経由したiRMCログインが行えます。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[ユーザー]を選択します。
2. 画面左側のメニューから[中継ルート設定]を選択します。
3. [設定]ボタンを選択します。
4. 任意の未設定の中継ルート番号に管理端末のIPアドレスを設定します。

ポイント

- 中継ルートに設定する管理端末のIPアドレスは、管理端末と監視対象ノード間にあるルーターの設定により、管理端末そのもののIPアドレスではない場合があります。以下の手順で設定すべきIPアドレスを確認できます。

  1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択します。
  2. [監査ログ]タブを選択し、[説明]が「ログインに成功しました。」の行に表示される[IPアドレス]項目のIPアドレスを確認します。



ー 複数のIPアドレスで「ログインに成功しました。」が表示される場合は、複数の管理端末からISM-VAにログインしたことがわかります。
中継ルートを設定すべき管理端末を見定めてIPアドレスを設定してください。

5. 中継ルートを設定した管理端末に、ISM-VAが発行する中継ルート用クライアント証明書をインストールします。

   中継ルート用クライアント証明書の作成からインストールの方法については、『解説書』の「4.28 中継ルート用クライアント証明書の作成」を参照してください。

3.8.2 ISMからiRMCにログインする

iRMCログインの手順を以下に記載します。
iRMCログインが可能なノードに対してのみ[ログイン]ボタンが表示されます。

注意

[ログイン]ボタン選択時に表示されるプルダウンボックスの「接続先IPアドレス」とは、いずれかのユーザーが中継ルートを使用して最後に接続したiRMCのIPアドレスを表しています。中継ルートは同時に1ユーザーしか使用できないため、他のユーザーと中継ルートを共有する場合は、他のユーザーが使用していないことを確認してから使用してください。同時に使用した場合は、先に使用していたユーザーの接続が切断され、後から使用した接続が有効になります。

iRMCログインを有効にする

ユーザーグループに対してiRMCログインを有効化します。

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. 対象のユーザーグループを選択し、[アクション]ボタンから[編集]を選択します。
4. [iRMCログイン/AVR]の項目の[有効]を選択します。

ノードリストからiRMCにログインする

ノードリストの[ログイン]ボタンを選択してiRMCログインを行います。

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]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[iRMCログイン]カラムの[ログイン]ボタンを選択します。

   中継ルートが複数設定されている場合は、[ログイン]ボタンを選択した際に、中継ルート番号がプルダウンボックスで表示されます。

   iRMC画面がWebブラウザーの別ウィンドウで表示されます。

ノードの詳細画面からiRMCにログインする

ノード詳細画面の[ログイン]ボタンを選択してiRMCログインを行います。

1. ノードの詳細画面の[iRMCログイン]項目の[ログイン]ボタンを選択します。

   中継ルートが複数設定されている場合は、[ログイン]ボタンを選択した際に、中継ルート番号がプルダウンボックスで表示されます。

   iRMC画面がWebブラウザーの別ウィンドウで表示されます。

ポイント

中継ルートの設定がある場合は、別ウィンドウでiRMC画面が表示される前に、証明書の選択を求められる場合があります。

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。

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

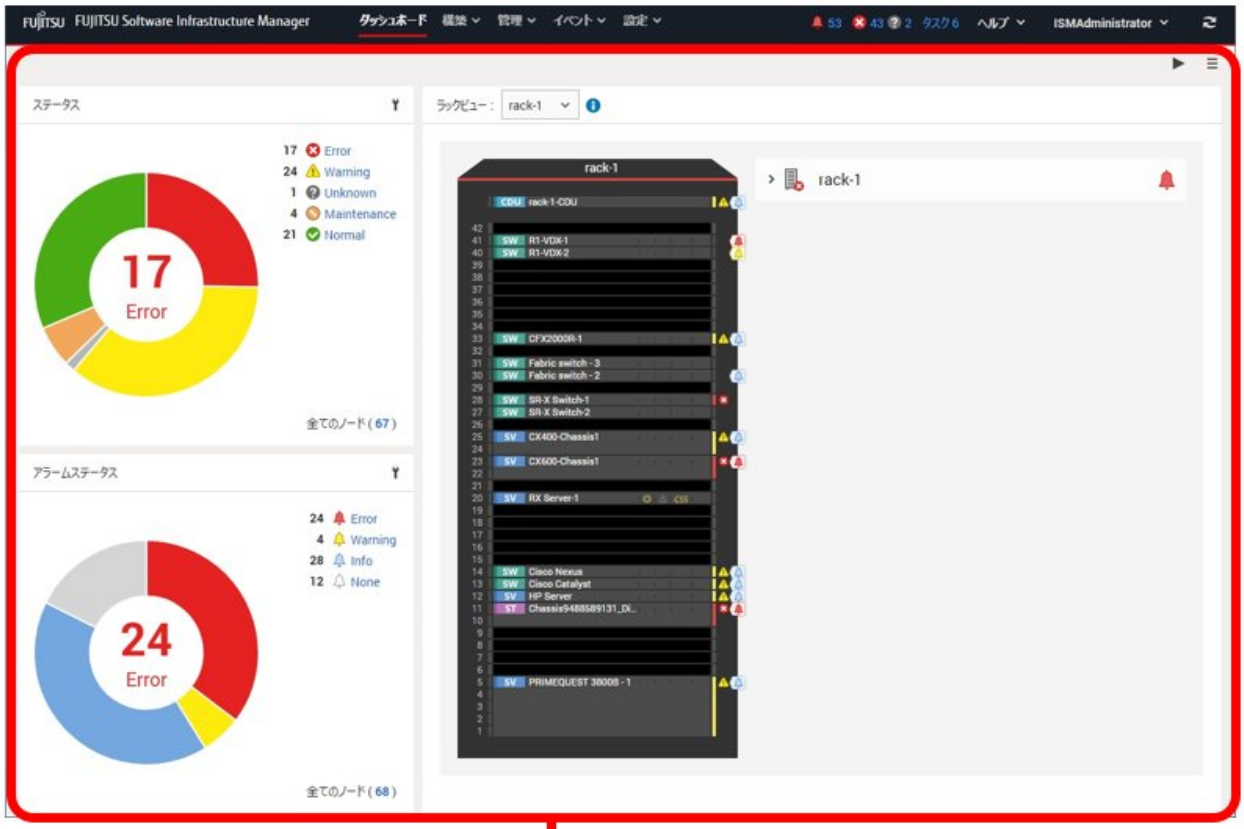
ノードの状態はダッシュボードの[ステータス]ウィジェットおよび「ノードリスト」画面で確認できます。

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。



[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。

   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

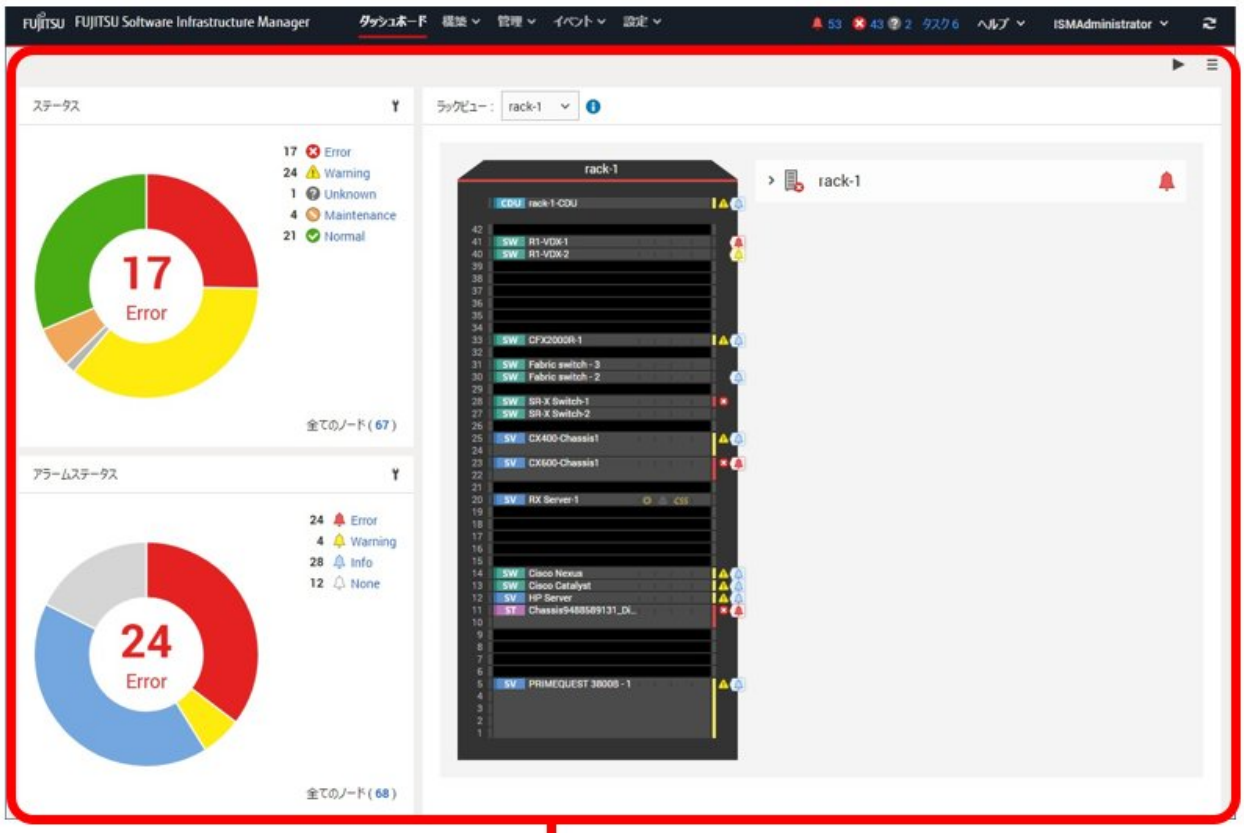
ノードのイベント発生およびノード状態はダッシュボードの[アラームステータス]ウィジェットおよび「ノードリスト」画面で確認できます。

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。



[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。

   以上でノード通知情報の表示は完了です。

4.5 ノードの電源状態を表示する

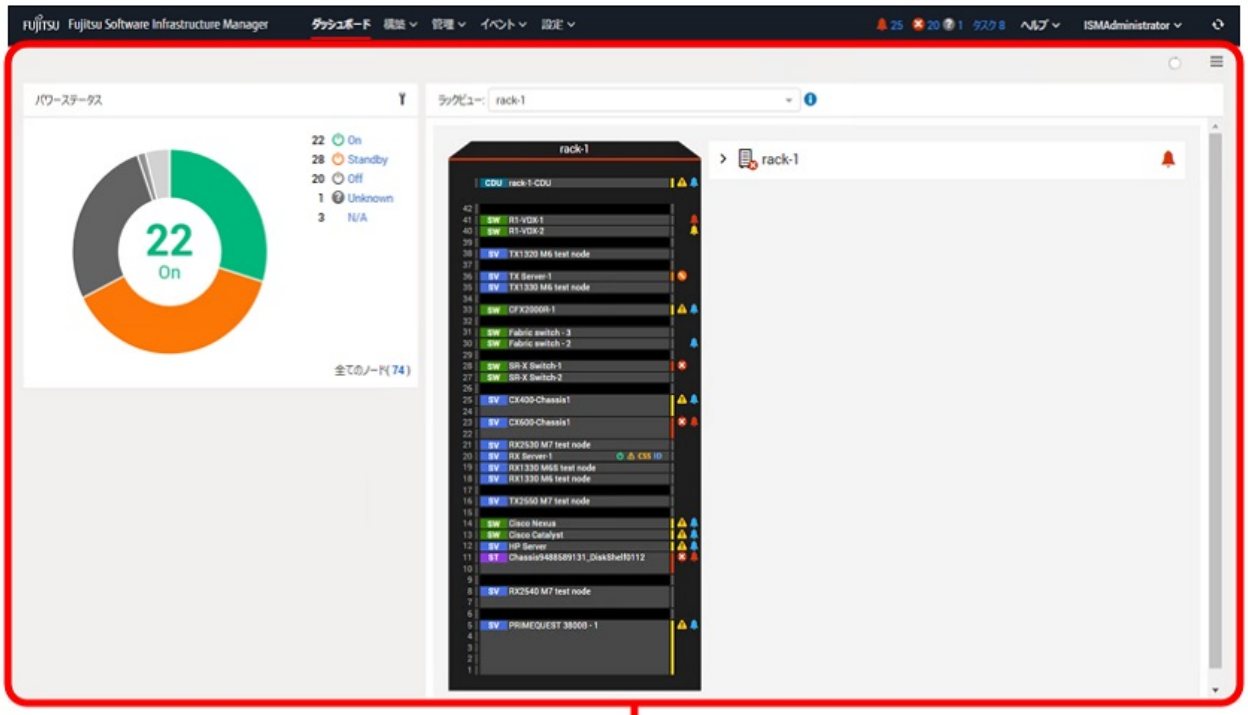
ノードの電源状態はダッシュボードの[パワーステータス]ウィジェットおよび「ノードリスト」画面で確認できます。

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. [パワーステータス]ウィジェットで電源状態を確認します。

   [パワーステータス]ウィジェットの説明はヘルプ画面を参照してください。



［ダッシュボード］画面

3. [パワーステータス]ウィジェットで、状態を確認するステータス（On、Standby、Off、Unknown、N/A）を選択します。

   当該パワー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。

   以上でノード電源状態の表示は完了です。

4.6 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。

4.6.1 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。

4.6.2 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。

4.7 ファームウェアバージョンを確認する

ISMに登録したサーバー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/ドライバー]を選択します。

   「ノードリスト」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。

   「ノードリスト」画面内の当該サーバーの[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。

   以上でサーバー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。

4.8 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。

   「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。

4.9 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にチェックを付けます。
4. [アクション]ボタンから[ダウンロードファイル作成]を選択します。

   「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。

   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。

ポイント

複数のノードを選択した場合や、複数の保管ログを選択した場合でも、ダウンロードファイルは1つのzipファイルにまとめられます。

注意

- ISMでは、ダウンロードファイルは常に1つしか保持できません。そのため、ログのダウンロード操作を連続で実行した場合、以前に作成されたダウンロードファイルは削除されます。
- ログ収集中のノードに対するダウンロードファイル作成は実行できません。ログ収集完了後にダウンロードファイル作成を実行してください。

4.10 詳細情報からノードを絞り込む

管理対象ノードの詳細情報からノードを絞り込み、特定の情報を持つノードだけを表示します。

1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
2. ⋮ ボタンを選択します。

   フィルター画面が表示されます。
3. フィルター項目を指定します。全ての項目を対象としてフィルタリングする場合は、[全ての項目]欄でフィルタリング条件を指定します。個別の項目を対象としてフィルタリングする場合は、対象の項目欄でフィルタリング条件を指定します。

   ポイント

   [ステータス]、[アラームステータス]で複数のステータスを指定した場合、OR検索が行われます。[ステータス]、[アラームステータス]以外の項目で複数の項目を指定した場合、または1つの項目にスペースで区切った複数の条件を指定した場合は、AND検索が行われます。大文字、小文字の区別は行われません。
4. [フィルター]ボタンを選択します。

   「ノードリスト」画面で、指定した項目に該当するノードが絞り込み表示されます。

   [ステータス]、[アラームステータス]、[ブート種別]がフィルタリング条件に指定されている場合、「ノードリスト」画面上部の指定されたステータスボタンまたはプルダウンボックスが選択された状態になります。

4.11 通常と異なる振る舞いをしているノードを検出する

アノマリ検知機能により通常とは異なる振る舞い(アノマリ状態)をしているサーバーを検出することができます。アノマリ検知機能は以下の手順で実施します。

- 4.11.1 アラーム、アクション設定を行う
- 4.11.2 CPU使用率予測設定を有効にする
- 4.11.3 アノマリ検知機能を開始する
- 4.11.4 現在のアノマリ検知状態を確認する
- 4.11.5 アノマリ検知イベント通知を確認する
- 4.11.6 アノマリ検知の履歴を確認する
- 4.11.7 アノマリ検知機能を停止する
- 4.11.8 CPU使用率予測設定を無効にする

4.11.1 アラーム、アクション設定を行う

アノマリ状態を検知した場合やアノマリ状態が回復した場合に通知されるイベントを外部アラームとして通知する設定を行います。外部アラームとして通知する必要がない場合、本手順は不要です。

1. アクションを設定します。

   アクションの設定手順は、「3.2.1.1 アクション（通知方法）を設定する」を参照してください。

2. アラームを追加します。

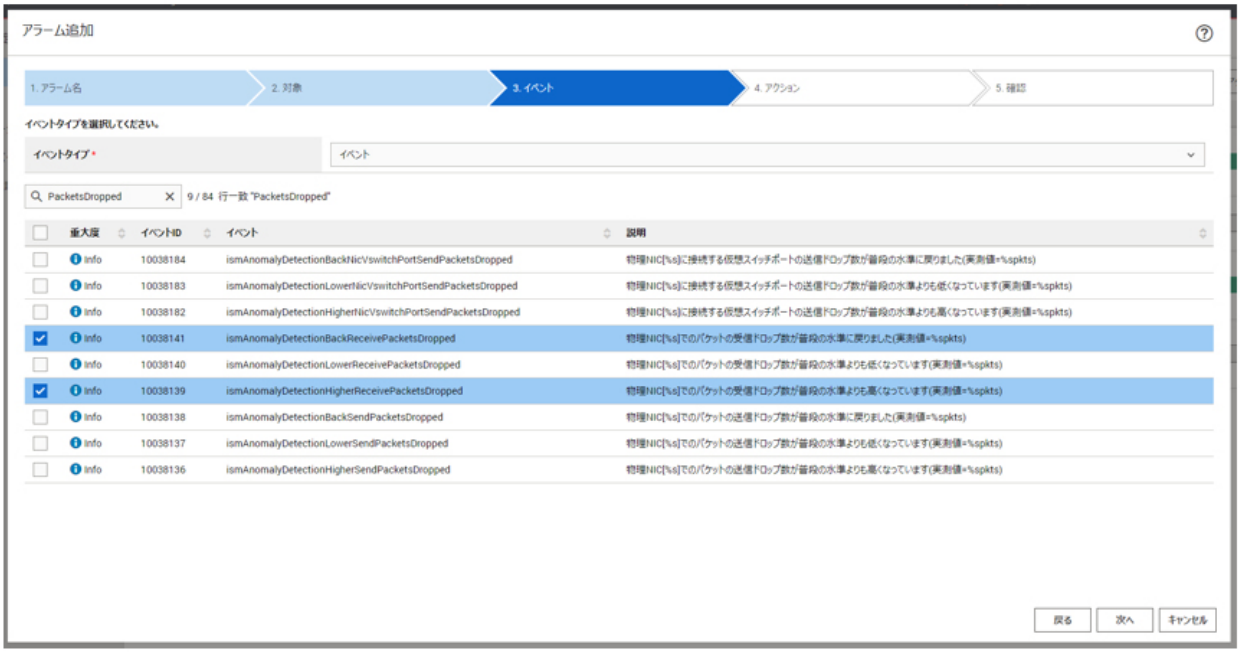
   アラームの設定手順は、「3.2.1.3 管理対象機器を対象にアラーム設定をする」を参照してください。「アラーム追加」ウィザードで以下を選択してください。

   「2.対象」では対象種別として「ノード（個別）」、「ノード（全ノード）」、または「ノード（ノードグループ）」を選択し、アラーム通知対象のサーバーを選択します。

   「3.イベント」ではイベントタイプとして「イベント」を選択し、イベントタイプが"ismAnomalyDetection"で始まるイベントIDからアラーム通知を行うイベントを選択します。

以下の例では監視項目のうち、物理NICの「パケットの受信ドロップ数（上限超過）」の検知と回復を設定しています。

図4.1 アラーム追加のイベント選択例



4.11.2 CPU使用率予測設定を有効にする

アノマリ検知として、CPU使用率の高騰の予測を行い、一定値を超える日時予測の有効／無効を設定します。予測を行わない場合、本手順は不要です。

CPU使用率予測設定は、以下の手順で有効にします。

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

   「ノードリスト」画面が表示されます。

2. [アクション]ボタンから[CPU使用率予測設定]を選択します。

   「CPU使用率予測設定」画面が表示されます。

3. [CPU使用率予測]で「有効」を選択します。

4. [適用]ボタンを選択します。

ポイント

- CPU使用率予測設定は、VMware ESXiホストのアノマリ検知を開始するすべてのノードに適用されます。先にアノマリ検知を開始し、後からCPU使用率予測設定を有効にした場合も、適用されます。

・ CPU使用率予測設定を有効にすると、予測用データが作成され予測用データの作成後、予測が行われます。
予測用データの詳細については、『解説書』の「2.3.6 アノマリ検知機能」を参照してください。

4.11.3 アノマリ検知機能を開始する

アノマリ検知機能は以下の手順で開始します。

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. 表示されるノードリストからアノマリ検知機能を開始したいノードにチェックを付けます。

3. [アクション]ボタンから[アノマリ検知開始]を選択します。

4. 「アノマリ検知開始」画面で対象ノードを確認します。

   開始対象外のノード(サポート外のノード、すでに開始されているノード)はグレー表示されます。

   図4.2「アノマリ検知開始」画面

ポイント

情報収集データを初期化する場合は、アノマリ検知を開始するときに[情報収集データ初期化]を選択します。

詳細については、『解説書』の「2.3.6.2 アノマリ検知機能の開始／停止」を参照してください。

5. [アノマリ検知の判定基準とする期間]を選択します。

6. 開始対象のノードを確認し、[はい]ボタンを選択します。

7. 「結果」画面で実行結果を確認します。

ポイント

・ 対象の1ノードでアノマリ検知機能を開始する場合は、「ノードリスト」画面から対象ノードを選択した後に表示されるノードの詳細画面の[アノマリ検知]タブで [アノマリ検知アクション]ボタンから[アノマリ検知開始]を選択します。

・ アノマリ検知を開始後、学習データを作成してから、アノマリ分析を開始します(最短2日半程度)。
また、CPU使用率予測設定が有効になっている場合は、アノマリ検知を開始してから3週間以上経過すると、予測を開始します。

注意

・ ノードの保守作業を実施する場合は、アノマリ検知機能を停止してください。保守作業による動作を普段とは異なるふるまいと判断する可能性があります。また、保守作業中の状態を普段のふるまいと学習することで精度が低下します。

・ アノマリ検知の判定基準とする期間を[31日間]と設定する場合、追加リソースが必要になります。詳細は、『解説書』の「2.3.6.1 動作要件」を参照してください。

4.11.4 現在のアノマリ検知状態を確認する

アノマリ検知機能を開始したノードは[アノマリ検知状態]が「停止」以外の状態になります。

表示されている状態に応じて必要な操作を行います。

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]を選択します。

   「ノードリスト」画面が表示されます。

2. 対象ノード名を選択し、[アノマリ検知]タブを選択します。

3. [アノマリ検知状態]の表示を確認します。

4. 表示されている状態に応じて、必要な操作を行います。

   『解説書』の「2.3.6.4 アノマリ検知状態」を参照してください。

ポイント

- 情報収集(学習データ作成)中の状態が、アノマリ検知の判定に使用する正常範囲の基準となります。情報収集(学習データ作成)中も通常の運用を行い、より実際の動作に近い情報が収集できるようにします。
- 学習データはVMware ESXiホストでは12時間ごと、Red Hat Enterprise Linuxサーバーでは24時間ごとに更新しています。アノマリ検知機能を停止せずに継続して使用することで普段のふるまいとの違いをより高い精度で判定できるようになります。

注意

仮想マシンを利用していない状態で学習すると、アノマリ検知時にその仮想マシンに対して正常値範囲が大きな値のアノマリ検知を示す場合があります。アノマリ検知結果の妥当性が疑われる場合には、再学習を実施してください。

4.11.5 アノマリ検知イベント通知を確認する

アノマリ検知機能を開始しているノードで通常とは異なる振る舞いを検知(アノマリ検知)、または通常の振る舞いに回復した場合、アノマリ検知結果のイベントが通知されます。また、該当のイベントにアラーム通知を設定している場合は、設定したアクション(メール通知など)が行われます。

アノマリ検知のイベントは、以下の手順で確認します。

1. ISMのGUIでグローバルナビゲーションメニューから[イベント]-[イベント]を選択します。

   「イベントリスト」画面が表示されます。

2. [アノマリ検知ログ]タブを選択します。

3. 通知されたイベントを確認します。

   アノマリ検知機能の開始/停止およびアノマリを検知、回復したときにイベントが通知されます。

4. 「説明」欄の「解決方法」を選択します。

   「解決方法」画面が表示されます。

   表示されている解決方法に従い、発生要因の対応を検討してください。

ポイント

対象の1ノードのアノマリ検知イベントを確認する場合は、「ノードリスト」画面から対象ノードを選択した後に表示されるノードの詳細画面の[プロパティ]タブで[アノマリ検知ログ]の件数を選択します。

4.11.6 アノマリ検知の履歴を確認する

アノマリ検知の履歴は、以下の手順で確認します。

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]-[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. 対象のノード名を選択し、[アノマリ検知]タブを選択します。

3. [履歴リスト]で表示したい期間を指定します。

   ー 任意の期間の履歴を確認する場合

   [全ての履歴を表示]チェックボックスにチェックを付け、開始日時、終了日時を選択します。

   ー 全期間で発生中のアノマリだけを表示する場合

   [全ての履歴を表示]チェックボックスのチェックを外します。

アノマリ検知結果イベントに対応するノードのアノマリ検知履歴を確認する場合

アノマリ検知イベントを確認する方法は、「4.11.5 アノマリ検知イベント通知を確認する」を参照してください。

1. イベントリストで確認したいイベントの発生時刻を記録して、ノード名を選択します。

   以下の例では、イベントの発生時刻（2021/10/7 11:08:50）を記録しておき、ノード名「RX Server-1」を選択します。

   選択したノードの詳細画面（[アノマリ検知]タブ）が表示されます。

2. 手順1で記録した時刻の入る期間を[履歴リスト]で指定します。

4.11.6.1 アノマリの発生状況を確認する

アノマリが発生したと検知された状況（測定値のグラフ）の確認は、以下の手順を実施します。

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. 対象のノード名を選択し、[アノマリ検知]タブを選択します。
3. [履歴リスト]で抑制したいアノマリにある[グラフ]ボタンを選択します。

4.11.6.2 アノマリの検知を抑制する

アノマリ検知の抑制は、以下の手順を実施します。

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. 対象のノード名を選択し、[アノマリ検知]タブを選択します。
3. [履歴リスト]で抑制したいアノマリにある[抑制]ボタンを選択します。

4.11.6.3 アノマリ検知に対する抑制を取り消す

抑制状態を取り消す場合は、以下の手順を実施します。

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. 対象のノード名を選択し、[アノマリ検知]タブを選択します。
3. [アノマリ検知アクション]ボタンから[アノマリ検知の抑制取り消し]を選択します。

注意

アノマリ検知の抑制を取り消すことで、すべての監視項目について抑制を取り消します。

4.11.7 アノマリ検知機能を停止する

アノマリ検知機能が不要となったノードは、以下の手順によりアノマリ検知機能を停止します。

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. 表示されるノードリストからアノマリ検知機能を停止したいノードにチェックを付けます。
3. [アクション]ボタンから[アノマリ検知停止]を選択します。
4. 「アノマリ検知停止」画面で対象ノードを確認します。

   停止対象外のノード(サポート外のノード、すでに停止されているノード)はグレー表示されます。
5. 停止対象のノードを確認し、[はい]ボタンを選択します。
6. 「結果」画面で実行結果を確認します。

ポイント

対象の1ノードでアノマリ検知機能を停止する場合は、「ノードリスト」画面から対象ノードを選択した後に表示されるノードの詳細画面の[アノマリ検知]タブで [アノマリ検知アクション]ボタンから[アノマリ検知停止]を選択します。

4.11.8 CPU使用率予測設定を無効にする

以下の手順によりCPU使用率予測設定を無効にします。

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

   「ノードリスト」画面が表示されます。
2. [アクション]ボタンから[CPU使用率予測設定]を選択します。

   「CPU使用率予測設定」画面が表示されます。
3. [CPU使用率予測]で「無効」を選択します。
4. [適用]ボタンを選択します。

注意

CPU使用率予測設定を無効にした場合、作成済の予測用データが削除されます。そのため、次にCPU使用率予測設定を有効にしても、新たに予測用データを作成するために予測開始には3週間の期間が必要となります。

予測用データの詳細については、『解説書』の「2.3.6 アノマリ検知機能」を参照してください。

ポイント

アノマリ検知を継続したまま、CPU使用率予測設定だけを無効にすることが可能です。

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。

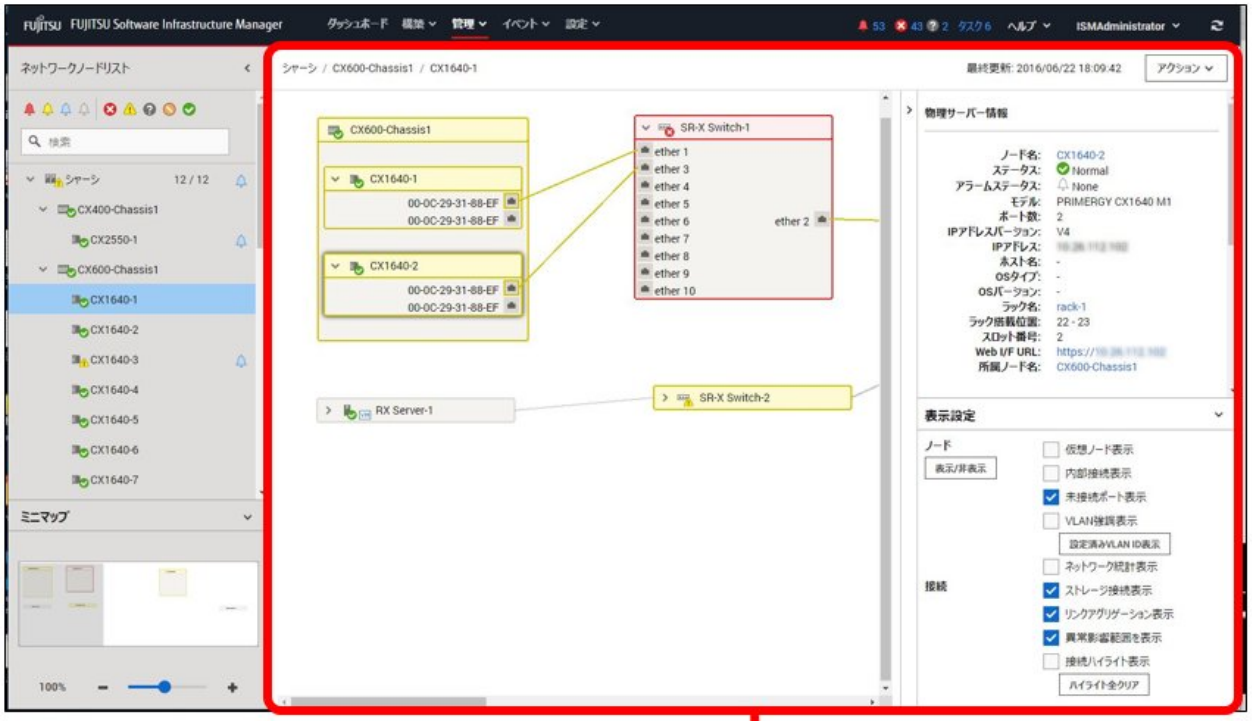
   異常が発生しているノードだけが表示されます。
3. 表示された異常ノードの情報から状況を確認します。

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、仮想ルーター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。
  - ログ収集メニューの[ログ管理]を選択します。
  - 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。
  - ノードリストの[カラム表示]から[ログ収集設定]を選択します。
  - ノードリストで対象の[ノード名]を選択し、[ログ収集設定]タブを選択します。

注意

- 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。

5.4 PRIMEFLEX for VMware vSANのクラスタに関連するログを一括収集する

PRIMEFLEX for VMware vSANのクラスタに関連するログを一括収集する操作手順を示します。

5.4.1 動作要件

vSANログ一括収集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。

・ ISM for PRIMEFLEX動作環境

　― 対象クラスタに含まれるすべてのサーバーがISMにノード登録されていること

　― 対象クラスタが仮想化管理ソフトウェアに登録されていること

　― Administratorユーザーグループの仮想ディスクに必要な空き容量があること
　必要な空き容量の目安:4ノード構成で約6Gbyte程度(vm-support、vc-supportのログサイズによっては、さらに多くの容量が必要となる場合があります。)

・ クラスタの構成・動作状況

　― vCenter Server Applianceに対してSSHによるアクセスを許可していること

・ 仮想化管理ソフトウェアの登録状況

　― 仮想化管理ソフトウェアの登録アカウント情報にローカルユーザーを使用していないこと

　― 仮想化管理ソフトウェアの登録アカウント情報に管理者権限があるユーザーを使用していること

上記の要件に合致する場合は、仮想化管理ソフトウェアから情報を取得できます。

仮想化管理ソフトウェアからの情報取得については、『解説書』の「2.13.6.2 仮想化管理ソフトウェアからの情報取得」を参照してください。

5.4.2 vSANログを一括収集する

1. コンソールからadministratorでISM-VAにログインします。
2. クラスタ名確認のコマンドを実行し、vSANログを収集したいクラスタ名を確認します。

   例:クラスタ名確認の実行結果(クラスタが3つ設定されていた場合)

```
# ismadm cluster logcollect -listcluster
Cluster List:
 TestCluster62vSanTrue            VMware
 Cluster-1                        VMware
 S2DCluster                       Hyper-V
```

   「Cluster List:」の下に＜クラスタ名＞と＜クラスタの種類＞が1行ずつ表示されます。ログを収集したいクラスタのクラスタ名(例えば「TestCluster62vSanTrue」)を確認します。

3. vSANログ一括収集の開始コマンドを実行します。

   コマンドオプションに必要な情報を設定してください。

   例:「TestCluster62vSanTrue」クラスタのvSANログを、ディレクトリー「/Administrator/ftp」にログファイル「clusterlog_20191111_TestCluster62vSanTrue.zip」として収集する場合

```
# ismadm cluster logcollect -collect -dir /Administrator/ftp -file clusterlog_20191111_TestCluster62vSanTrue.zip
```

4. コマンドプロンプトに手順2で確認したクラスタ名とzipパスワード(必要な場合)を指定します。

   例:クラスタ名を「TestCluster62vSanTrue」、zipパスワードを「Himitsu」と指定する場合

```
# ismadm cluster logcollect -collect -dir /Administrator/ftp -file clusterlog_20191111_TestCluster62vSanTrue.zip
ClusterName:                    ・・・クラスタ名
TestCluster62vSanTrue
Password:                       ・・・zipパスワード
Himitsu
```

5. メッセージを確認し、実行する場合は「Y」を入力します。

```
TestCluster62vSanTrue Collect Start?(Y/N)
Y                               ・・・実行する場合は「Y」を入力
```

6. 収集状態を確認しvSANログ一括収集が完了するのを待ちます。

   vSANログ一括収集はバックグラウンドで動作します。そのため、収集状態確認のコマンドにより「Status(vSANログの収集状態)」が「Complete」になるのを確認します。

vSANログ一括収集完了まではしばらく時間がかかります。

例:vSANログ一括収集を実施中にクラスタ「TestCluster62vSanTrue」の収集状態を確認した場合

```
# ismadm cluster logcollect -status
ClusterName:                                ・・・収集状態を確認したいクラスタ名「TestCluster62vSanTrue」を入力
TestCluster62vSanTrue
ClusterName:TestCluster62vSanTrue
Directory:/Administrator/ftp                ・・・出力先ディレクトリー名
FileName:clusterlog_20191111_TestCluster62vSanTrue.zip
Status:Collecting                           ・・・vSANログの収集状態（ここが「Complete」となるのを待ちます）
CollectStartTime:2019/11/11 12:33:40        ・・・収集開始時刻
CollectEndTime:                             ・・・収集終了時刻
CheckSum:                                   ・・・チェックサムの値
[CmsStatus]                                 ・・・CMS関連のログの収集状態
Collecting:VcSupport
Wait:RVC
[NodeStatus]                                ・・・各ノードのログの収集状態
Complete:PRIMERGY1
Collecting:PRIMERGY2
Wait:PRIMERGY3
```

例:vSANログ一括収集を一度も実施していないクラスタの収集状態を確認した場合

```
# ismadm cluster logcollect -status
ClusterName:
TestCluster62vSanTrue
'TestCluster62vSanTrue' is not collecting.      ・・・「'クラスタ名' is not collecting.」と表示
```

7. 出力されたログファイルを確認します。

   指定したディレクトリーにログファイルおよび収集結果の情報ファイルが格納されていることを確認します。収集結果は収集結果の情報ファイルにより確認できます。

   手順3の例でvSANログ一括収集を開始している場合、ディレクトリー「/Administrator/ftp」に以下のファイルが作成されます。

   - clusterlog_20191111_TestCluster62vSanTrue.zip(ログファイル)
   - clusterlog_20191111_TestCluster62vSanTrue.Result(収集結果の情報ファイル)

   例:収集結果の情報ファイル内容

```
ClusterName:TestCluster62vSanTrue
Directory:/Administrator/ftp
FileName:clusterlog_20191111_TestCluster62vSanTrue.zip
Status:Complete                             ・・・収集完了
CollectStartTime:2019/11/11 12:33:40
CollectEndTime:2019/11/11 13:33:40
CheckSum:xxxxxxxxxxxxxx
[CmsStatus]                                 ・・・vc-supportおよびRVCコマンドは正常に収集
Complete:VcSupport
Complete:RVC
[NodeStatus]                                ・・・PRIMERGY1, PRIMERGY3ノードは正常に収集、PRIMERGY2ノードは収集エラー
Complete:PRIMERGY1
Error:PRIMERGY2
Complete:PRIMERGY3
```

8. ログファイルをFTPにより取得します。

9. ログファイルを削除します。

   ログファイルの取得後は、Administratorユーザーグループの仮想ディスク領域の空き容量を増やすため削除してください。

第6章 ノードを管理／操作するその他の機能

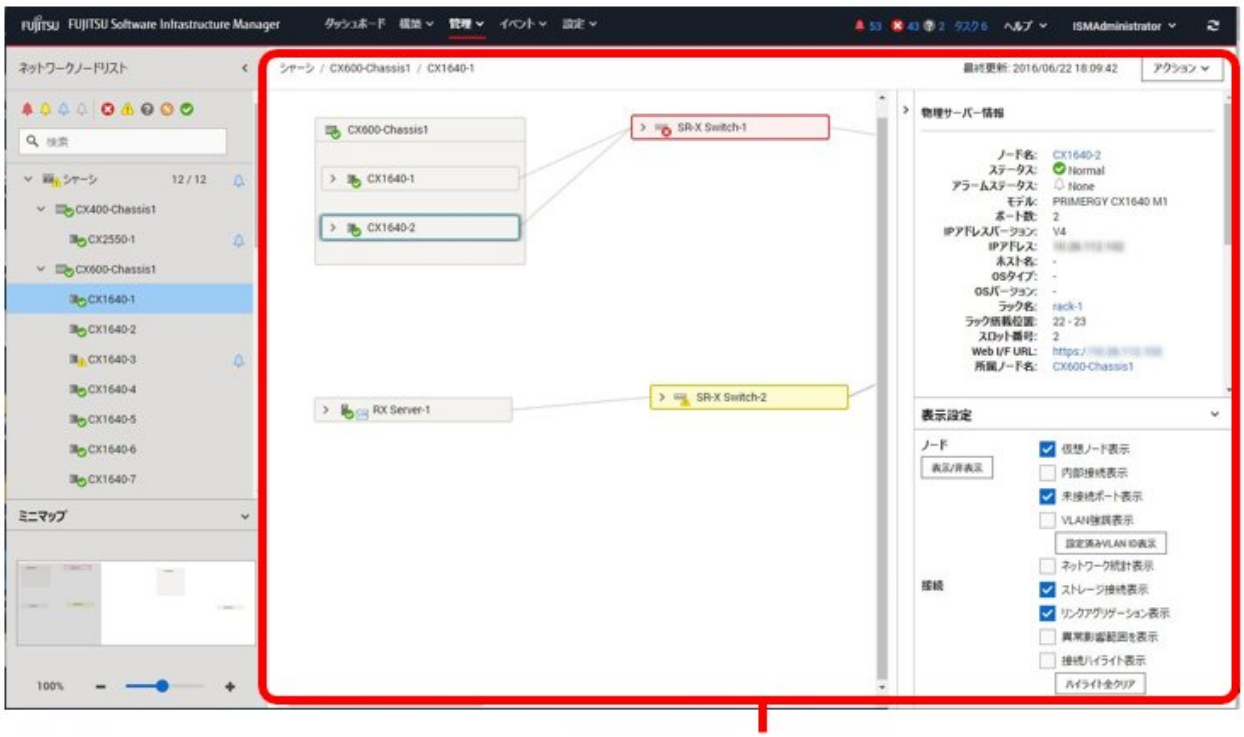
この章では、各ノードに対する様々な操作について説明します。

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は表示されません。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。



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、管理対象サーバー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。

   ー 仮想化管理ソフトウェア名

   ISM 全体で、一意な名称を設定してください。

   ー IPアドレス

   仮想化管理ソフトウェアのIPアドレスを設定してください。

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

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

   ー タイプ

   登録する仮想化管理ソフトの種類を選択してください。

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

   注意

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

   ー アカウント情報

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

   ドメイン名は大文字で記入してください。

   ポイント

   - 仮想化管理ソフトウェアの種類がOpenStackの場合、プロジェクトは登録したユーザーの主プロジェクトとなります。
   - VMware vCenter ServerとVMware ESXiのFQDNを変更した場合、仮想化管理ソフトウェアの登録削除、再登録が必要です。

   ー URL

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

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

ー ユーザーグループ

管理するユーザーグループ名を選択してください。

5. [登録]ボタンまたは[テスト]ボタンを選択します。

[登録]ボタンを選択すると、「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。

[テスト]ボタンを選択すると「仮想化管理ソフトウェアテスト」画面が表示されます。以下に「仮想化管理ソフトウェアテスト」画面での操作手順を示します。

a. 「テスト成功後、仮想化管理ソフトウェアを登録する。」または「テストだけを実行する。」を選択します。

b. [適用]ボタンを選択します。

「テスト成功後、仮想化管理ソフトウェアを登録する。」を選択した場合、テストに成功すると「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。

「テストだけを実行する。」を選択した場合、テストに成功すると「仮想化管理ソフトウェア登録」画面が表示されます。登録する場合は、[登録]ボタンを選択します。

以上で仮想化管理ソフトウェアの登録は完了です。

ポイント

[テスト]ボタンは[タイプ]で「VMware vCenter Server」、または「System Center」を選択すると有効になります。

注意

テストの完了までに時間がかかることがありますが、テストが完了するまで画面を閉じないでください。画面を閉じた場合は再度テストを実行してください。

6.2.1.1 仮想化管理ソフトウェア情報を編集する

仮想化管理ソフトウェアのパスワードやIPアドレスなどを変更した場合、ISM上の仮想化管理ソフトウェアの情報を変更する必要があります。変更しない場合、仮想リソースの情報表示でエラーになります。

仮想化管理ソフトウェア情報を編集する場合の操作方法を示します。

1. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]-[仮想化管理ソフトウェア]を選択し、表示される「仮想化管理ソフトウェアリスト」画面で、対象の仮想化管理ソフトウェアを選択します。
2. [アクション]ボタンから[編集]を選択します。
3. 情報を編集します。

項目	説明
仮想化管理ソフトウェア名	ISM全体で、一意な名称を設定します。
IPアドレス	仮想化管理ソフトウェアのIPアドレスを設定します。 Microsoft Failover Clusterの場合には、クラスタ仮想IPアドレスを設定してください。 OpenStackの場合には、コントローラーノードのIPアドレスを設定してください。
タイプ	設定されている仮想化管理ソフトウェアタイプが表示されます。 ISMに登録されている仮想化管理ソフトウェア情報のタイプは編集できません。タイプを変更する場合はISMに登録されている仮想化管理ソフトウェア情報を削除して、正しいタイプ指定し再度登録してください。
バージョン	仮想化管理ソフトウェアタイプで指定可能なバージョンを選択してください。
アカウント情報	仮想化管理ソフトウェアのドメイン名、アカウント名、パスワード、ポート番号を設定します。ドメイン名は大文字で設定してください。

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

4. [テスト]ボタンを選択します。

   [テスト]ボタンを選択すると「仮想化管理ソフトウェアテスト」画面が表示されます。以下に「仮想化管理ソフトウェアテスト」画面での操作手順を示します。

   a. 「テスト成功後、仮想化管理ソフトウェアを登録する。」を選択します。

   b. [適用]ボタンを選択します。

      テストに成功すると編集した仮想化管理ソフトウェアの情報が表示されます。

      テストに失敗した場合は、画面のメッセージに従って設定値を見直した後、[テスト]ボタンを選択してください。

以上で仮想化管理ソフトウェア情報の編集は完了です。

6.2.2 管理対象サーバー上の仮想マシンの情報を確認する

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ーが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。

   - 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、メモリー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。

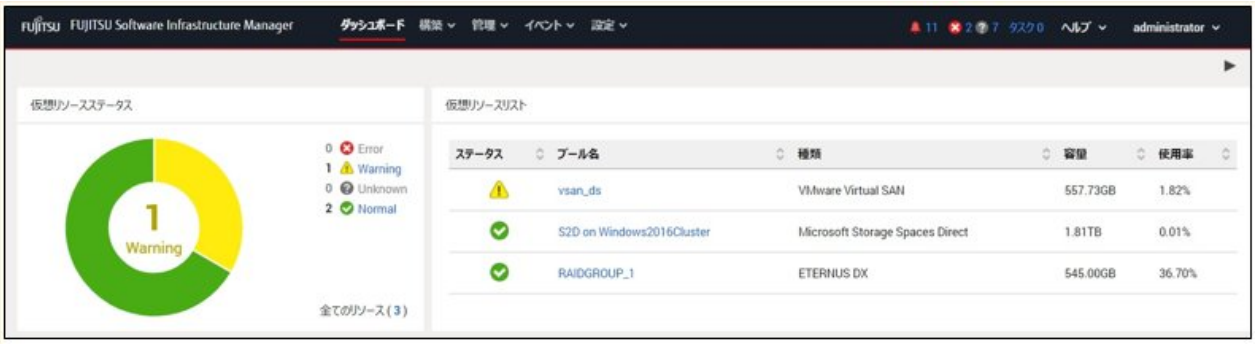
2. 画面右上部にある[☰]ボタンから[ウィジェット追加]を選択します。

   「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。

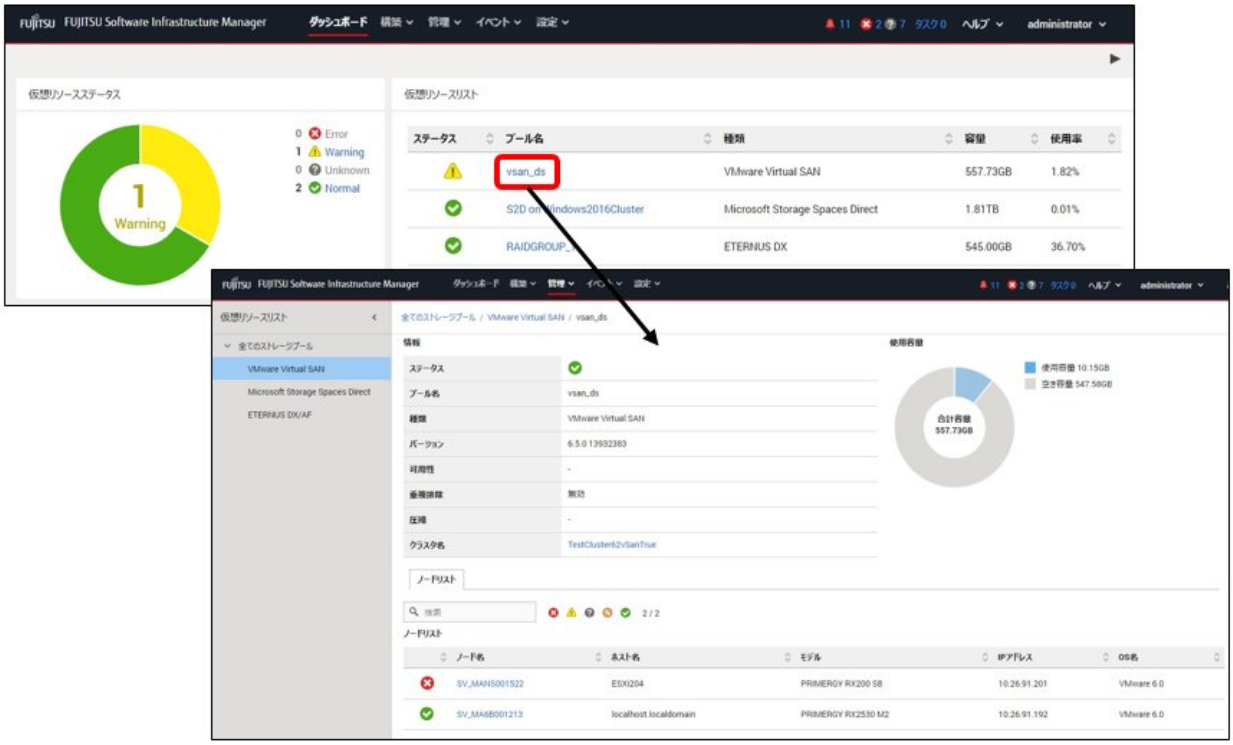


4. [仮想リソースリスト]ウィジェットで状態を確認するプール名を選択、または[仮想リソースステータス]ウィジェットで状態を確認するステータス(Error、Warning、Unknown、Normal)を選択します。

   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。

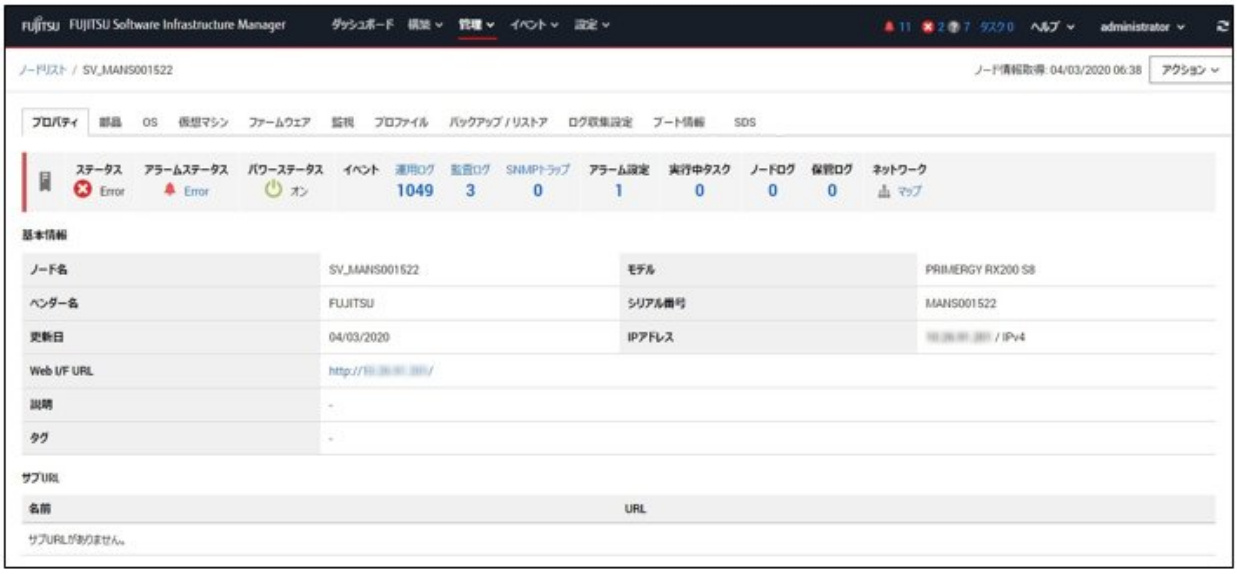


ノードの詳細画面からリソース情報を確認する

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。



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。

「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。

6.2.4 仮想マシン／vSANストレージの状態を確認する

仮想マシンが利用するvSANストレージの物理ディスクの構成と仮想ディスクに対する読み込みと書き込み遅延値およびI/O遅延ステータスが確認できます。

仮想マシン／vSANストレージの状態を表示する

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]-[仮想リソース]を選択し、「仮想リソースリスト」画面で「VMware Virtual SAN」を選択します。
2. 以下のいずれかの操作を行います。
   - ストレージプールを選択し、[アクション]ボタンから[影響分析(VMware Virtual SAN)]を選択します。
   - ストレージプールを選択してストレージプールの情報を表示します。[アクション]ボタンから[影響分析(VMware Virtual SAN)]を選択します。

   「影響分析(VMware Virtual SAN)」画面が表示されます。

仮想マシン／サーバー／vSANストレージの構成を確認する

1. 確認したい仮想マシンのドットを選択します。
2. 画面左側の構成表示エリアにて、仮想マシンが構成するvSANの物理ディスク(キャッシュディスク、キャパシティディスク)および物理ディスクを構成するサーバーを確認します。

   仮想マシンが構成するvSANの物理ディスク(キャッシュディスク、キャパシティディスク)および物理ディスクを構成するサーバーは、影響ありのドットで表示されます。
   サーバー、キャッシュディスクおよびキャパシティディスクに対してもドットを選択し、同様に確認します。

ポイント

仮想マシンのステータスは、以下のドットで表示されます。

ステータス	ISM GUIでのドットの表示	状態
Error(異常)	 (赤色)	仮想マシンのディスク遅延が発生(I/O遅延しきい値を超えている)している状態です。 ディスクの性能劣化またはデータの輻輳が考えられます。
Unknown(不明)	 (灰色)	仮想マシンのディスク遅延情報が取得できない状態です。
Normal(正常)	 (緑色)	仮想マシンは正常な状態です。

仮想マシン／サーバー／vSANストレージの情報を確認する

1. 確認したい仮想マシンのドットを選択します。
2. 画面右側の詳細情報表示エリアにて、仮想マシン名、I/O遅延ステータス、I/O遅延しきい値(ms)、書き込み遅延値(ms)、読み込み遅延値(ms)を確認します。
3. 詳細情報表示エリアを参照し、影響サーバーリストのサーバー名、影響キャッシュディスクリストのキャッシュディスク名、影響キャパシティディスクリストのキャパシティディスク名を確認します。

   影響ありドットで表示されているサーバー、キャッシュディスク、キャパシティディスクに対してもドットを選択し、同様に確認します。

   ー サーバーを選択した場合

   サーバー名、OSタイプ、影響仮想マシンリストの仮想マシン名、影響キャッシュディスクリストのキャッシュディスク名、影響キャパシティディスクリストのキャパシティディスク名を確認します。

   ー キャッシュディスクを選択した場合

   キャッシュディスク名、ディスク種別、影響サーバー名、影響仮想マシンリストの仮想マシン名、影響キャパシティディスクリストのキャパシティディスク名を確認します。

ー キャパシティディスクを選択した場合

キャパシティディスク名、ディスク種別、影響サーバー名、影響仮想マシンリストの仮想マシン名、影響キャッシュディスクリストのキャッシュディスク名を確認します。

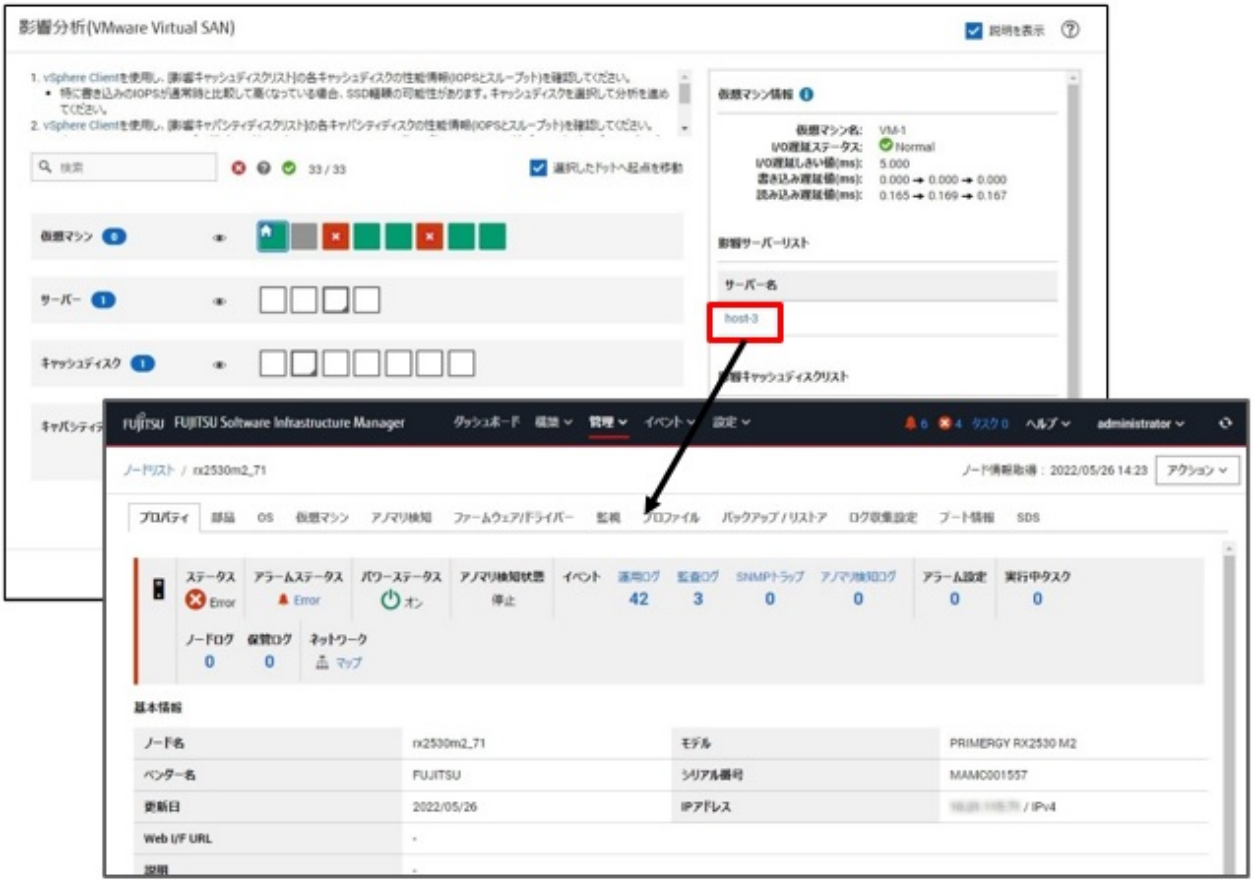
ポイント

ドットの表示数が多い時などにはドットのフィルタリングを行えます。

「フィルター」欄に条件を入力することで、表示内容をフィルタリングできます。入力された文字列に当てはまらないドットはグレーとなり選択できなくなります。

また、画面上部のステータスの絞り込みアイコンで、指定したステータスのドット表示に絞り込めます。

サーバー名にある、リンク表示の[サーバー名]を選択すると、サーバーの登録情報を確認できます。



ポイント

- 「影響分析(VMware Virtual SAN)」画面を表示した時に仮想マシンのステータスが "Error" 状態であるドットを選択し、影響があるサーバー、キャッシュディスクおよびキャパシティディスクを確認してください。
- vSphere Clientを使用し、[影響キャッシュディスクリスト]の各キャッシュディスクの性能情報(IOPSとスループット)を確認してください。

  特に書き込みのIOPSが通常と比較して高くなっている場合、SSD輻輳の可能性があります。キャッシュディスクを選択して分析を進めてください。
- vSphere Clientを使用し、[影響キャパシティディスクリスト]の各キャパシティディスクの性能情報(IOPSとスループット)を確認してください。

  特に書き込み/読み込みのIOPSが通常と比較して高くなっている場合、I/Oの集中が起こっている可能性があります。キャパシティディスクを選択して分析を進めてください。
- vSphere Clientを使用し、[影響サーバーリスト]の各サーバーの性能情報(CPU使用率とメモリ使用率)を確認してください。

  CPU使用率が90%を超えている場合、CPU競合が発生している可能性があります。サーバーを選択して分析を進めてください。

6.3 クラスタのリソース変動を予測する

リソース変動予測機能によりクラスタのリソースが不足する時期を予測できます。リソース変動予測機能は、以下の手順で実施します。

- 6.3.1 リソース変動予測を実行する
- 6.3.2 リソース変動の予測結果を表示する

6.3.1 リソース変動予測を実行する

リソース変動予測機能は、vCenter Serverから過去のvSANクラスタの稼働情報を収集し、1年後までのリソースの使用予測をグラフ化して表示します。以下の手順で実施します。

ポイント

- 事前に仮想化管理ソフトウェアがISMに登録されていて、クラスタ情報が取得されている必要があります。
- リソース変動予測の結果に対してリソースの増設を仮定し、増設に関する情報（増設日、増設台数および増設するキャパシティディスク情報、CPU、メモリー）を加えることによって、その変化をシミュレーションできます。

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]-[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. クラスタリストからリソース変動を予測するクラスタを選択します。

   [クラスタ情報]タブが表示されます。

3. [リソース変動予測]タブを選択します。

   「リソース変動予測」画面が表示されます。

4. [リソース変動予測アクション]ボタンから[リソース変動予測]を選択します。

   「リソース変動予測」ウィザードが表示されます。

5. 「リソース変動予測」ウィザードに従い、設定項目を入力します。

   設定項目の入力内容は、ヘルプ画面を参照してください。

6. 「リソース変動予測」ウィザードの[実行]ボタンを選択します。

   リソース変動予測が実行されます。
   実行結果は、[リソース変動予測]タブの「履歴リスト」に結果リストとして追加されます。

6.3.2 リソース変動の予測結果を表示する

「6.3.1 リソース変動予測を実行する」で実行した「リソース変動予測」の結果を表示させるには、以下の手順を実施します。

1. 「履歴リスト」に[結果]ボタンが表示されていることを確認します。

   ポイント

   [結果]ボタンは「リソース変動予測」の実行が正常に完了するまで表示されません。

2. [結果]ボタンを選択します。

   「リソース変動予測結果」画面が表示されます。

   [CPU]、[メモリー]、[ストレージ]のタブを選択することで、対象のリソースの予測結果を確認できます。

   結果画面については、ヘルプ画面を参照してください。

ポイント

構成変更シミュレーションを実施した場合の予測結果は、追加したディスク、CPU、メモリーを含んだキャパシティサイズで計算された使用率および使用量が表示されます。

6.4 ノードのファームウェア／ドライバーをアップデートする

ISMに登録したノードのファームウェア/ドライバーをアップデートするには、以下の方法があります。

- インポートしたファームウェアデータを利用
- ServerView embedded Lifecycle Managementを利用

注意

以降の手順内で記載しているFsas Technologies マニュアルサイトでのマニュアル参照手順は、予告なく変更されることがあります。

6.4.1 インポートしたファームウェアデータを利用してファームウェアをアップデートする

インポートしたファームウェアデータを利用して、ISMに登録したノードのファームウェアをアップデートします。

Offlineアップデートの場合は、事前準備が必要です。詳細については、『解説書』の「2.6.3 ファームウェア／ドライバーのアップデート」の「Offlineアップデートに必要な準備作業」を参照してください。

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. エフサステクノロジーズのWebサイトに公開されたファームウェアデータをダウンロードします。

   https://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してください。
4. ダウンロードしたファイルが格納されているフォルダーを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。
   a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
   b. 画面左側のメニューから[インポート]を選択します。
   c. [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。
   d. 「ファームウェアインポート」画面の[ファイル選択方式]で[ローカル]を選択します。
   e. [ファイル]の[ブラウズ]ボタンを選択し、手順4で作成したzipファイルを選択します。
   f. 「ファームウェアインポート」画面に従って、[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。
   g. 「結果」画面の左上に表示される[タスク詳細：＜タスクID＞]を選択、またはグローバルナビゲーションメニュー上部の[タスク]を選択します。

      「タスク」画面にタスクの一覧が表示されます。タスクが成功したことを確認してください。
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。
   a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
   b. 画面左側のメニューから[インポート]を選択します。
   c. 「インポート」画面で[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ます。
7. 対象ファームウェアを選択します。

   ポイント

   以下の場合は、事前にノードの詳細画面の[ファームウェア/ドライバー]タブの[PXEブートポート]で使用するポートを設定してください。

   ー サーバーのOfflineアップデート

   ー OfflineアップデートのPXEブートに使用するポートがオンボードの先頭ポート以外である
   a. 画面左側のメニューから[アップデート]を選択します。

b. 「ノードリスト」画面で[更新モード:]欄から[Onlineアップデート]または[Offlineアップデート]を選択します。

c. ファームウェアアップデートを行うファームウェアにチェックを付けます。

現行バージョンより新しいバージョンのファームウェアデータがインポートされている場合、Online最新またはOffline最新にそのファームウェアのバージョンが表示されます。現行バージョンより新しいバージョンのファームウェアデータがインポートされていない場合、ファームウェアにチェックできません。

d. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。

「ファームウェア/ドライバーアップデート」ウィザードが表示されます。

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/ドライバーアップデート」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。

ファームウェアアップデートの開始後、ISMのタスクとして登録されます。

ファームウェアアップデートの状況は「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。

注意

登録されたタスクの「タスク詳細」画面から、実行中のタスクをキャンセルできます。ただし、サブタスクのメッセージに「Updating firmware.」が表示された後は、タスクはキャンセルできません。キャンセル失敗となります。

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、対象サーバーを再起動します。

10. 対象ノード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。

a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー] を選択します。

「ノードリスト」画面が表示されます。

b. 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ます。

「ノード情報」画面が表示されます。

c. [ノード情報取得]ボタンを選択します。

ノード情報が取得され、「ノードリスト」画面の[現行バージョン]にアップデート後のバージョンが表示されます。

以上でノード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。

6.4.2 ServerView embedded Lifecycle Managementを利用してファームウェアをOfflineアップデートする

ISMに登録したノードのファームウェアを、ServerView embedded Lifecycle Management(以降、「eLCM」と表記)を利用してアップデートします。

Repository ServerまたはエフサステクノロジーズWebサイトのファームウェアデータを利用する方法と、ISMにインポートしたファームウェアデータを利用する方法があります。

6.4.2.1 Repository Serverのファームウェアデータを利用してアップデートする

エフサステクノロジーズWebサイトのファームウェアデータを利用してもアップデートできますが、ここではRepository Serverのファームウェアデータを利用する手順で説明します。

1. Repository Serverの環境を確認します。

   Repository Serverの確認方法は、下記のFsas Technologies マニュアルサイトから『ServerView Repository Server - Installation and User Guide』を参照してください。

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

   参照手順

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

2. 対象ノードにeLCMの環境を構築します。

   詳細は、下記のFsas Technologies マニュアルサイトから『ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx - Overview』(xには、最新の版数が入ります。)を参照してください。

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

   参照手順

   「製品を選択する」- [カテゴリから探す]を選択し、アップデート対象のサーバーを選択してください。
   [Server Management Controller]からダウンロードしてください。

3. 対象ノードのiRMCに、Repository Serverの情報(URL設定)を設定します。

   a. 対象ノードのiRMCにWeb ブラウザーで接続します。

   b. [設定]タブの[サービス]を選択します。

   c. [アップデートとデプロイメント]を選択します。

   d. [アップデート]項目の[リポジトリの場所]に、Repository ServerのURLを入力して[適用]ボタンを選択します。

4. ISMのGUIで対象ノードを選択します。

   a. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。

   b. 「ノードリスト」画面の[カラム表示:]欄で[ファームウェア/ドライバー]を選択します。

   c. [更新モード:]欄から[eLCM Offlineアップデート]を選択します。

   d. 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。

   e. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。

      「ファームウェア/ドライバーアップデート」ウィザードが表示されます。

5. 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/ドライバーアップデート」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。

   ファームウェアアップデートの開始後、ISMのタスクとして登録されます。

   ファームウェアアップデートの状況は「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。

ポイント

「ファームウェア/ドライバーアップデート」ウィザードの「アップデート設定」画面で[アップデート時にメンテナンスモードに設定する]を選択した場合、ファームウェアアップデートの直前でメンテナンスモードに設定され、アップデート完了後にメンテナンスモードを解除します。日時を指定してファームウェアアップデートする場合に利用してください。

> **注意**
>
> 登録されたタスクの「タスク詳細」画面から、実行中のタスクをキャンセルできます。ただし、サブタスクのメッセージに「Updating firmware. (eLCM Offline)」が表示された後は、タスクはキャンセルできません。キャンセル失敗となります。

6. 対象ノード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。
   a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
      「ノードリスト」画面が表示されます。
   b. [現行バージョン]に表示されているバージョンを確認します。

   以上でノードのファームウェアアップデートは完了です。

6.4.2.2 ISMにインポートしたファームウェアデータを利用してアップデートする

ISMに登録したノードのファームウェアを、インポートしたファームウェアデータとeLCMを利用してアップデートします。

事前準備（PCIカードをアップデートする場合）

対象ノードのPCIカードをアップデートする場合は、eLCM Offlineアップデート(SimpleUpdate)ツー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]-[ファームウェア/ドライバー]を選択します。
2. 「ファームウェアツール」画面で、eLCM Offlineアップデート(SimpleUpdate)ツールを確認します。
   eLCM Offlineアップデート(SimpleUpdate)ツールがインポートされている場合は、以降の手順は不要です。
   eLCM Offlineアップデート(SimpleUpdate)ツールがインポートされていない場合、以降の手順を実施します。
3. ServerView Suite Update DVDから、インポートするeLCM Offlineアップデート(SimpleUpdate)ツールを取り出します。
   a. ServerView Suite Update DVDの、以下のディレクトリーを参照します。
      Firmware/Tools/UpdateManagerExpress/xx.xx.xx.xx（xには、版数が入ります。）
   b. 任意のフォルダーに、"xx.xx.xx.xx"フォルダーをコピーします。
   c. コピーしたフォルダーをzip形式に圧縮します。
4. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。
5. 画面左側のメニューから[インポート]を選択します。
6. [ファームウェアツール]タブを選択します。
7. [アクション]ボタンから[インポート]を選択します。
   「ファームウェアツールインポート」画面が表示されます。
8. [ファイル選択方式]で[ローカル]を選択します。
9. [ファイル]の[ブラウズ]ボタンを選択し、手順3で作成したzipファイルを選択します。
10. [適用]ボタンを選択します。
11. インポートを行ったファームウェアツールが一覧に表示されることを確認します。

ファームウェアをアップデートする

1. 対象ノードのiRMCに、アップデートのSSL/TLS証明書有効性確認スキップを設定します。
   a. アップデート対象ノードのiRMCにWeb ブラウザーで接続します。
   b. [設定]タブの[サービス]を選択します。
   c. [アップデートとデプロイメント]を選択します。
   d. [アップデート]項目の[SSL/TLS証明書有効性確認スキップ]にチェックを付けて[適用]ボタンを選択します。

2. 対象ノードにeLCMの環境を構築します。

   詳細は、下記のFsas Technologies マニュアルサイトから『ServerView embedded Lifecycle Management (eLCM) x.x for iRMC Sx - Overview』(xには、最新の版数が入ります。)を参照してください。

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

   参照手順

   「製品を選択する」- [カテゴリから探す]を選択し、アップデート対象のサーバーを選択してください。
   [Server Management Controller]からダウンロードしてください。

3. 「6.4.1 インポートしたファームウェアデータを利用してファームウェアをアップデートする」の手順1～6を実施して、ISMにファームウェアデータをインポートします。

4. ISMのGUIで対象ファームウェアを選択します。

   a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー]を選択します。

   b. 画面左側のメニューから[アップデート]を選択します。

   c. 「ノードリスト」画面で[更新モード:]欄から[eLCM Offlineアップデート(SimpleUpdate)]を選択します。

   d. ファームウェアアップデートを行うファームウェアにチェックを付けます。

      現行バージョンより古いバージョン、またはこのアップデート方法に対応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、ファームウェアにチェックできません。

   e. [アクション]ボタンから[ファームウェア/ドライバー更新]を選択します。

      「ファームウェア/ドライバーアップデート」ウィザードが表示されます。

5. 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/ドライバーアップデート」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。

   ファームウェアアップデートの開始後、ISMのタスクとして登録されます。

   ファームウェアアップデートの状況は「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。

   なお、「アップデートを次回起動時に開始する」を指定した場合、当該タスクが正常完了すると、対象ノードにファームウェアアップデート処理が予約されます。アップデート処理は対象ノードを電源OFFした契機で動作します。対象ノードを電源ON後、ノード詳細画面から「ノード情報取得」を実行してください。

ポイント

- [アップデートを次回起動時に開始する]の実行で、ファームウェアアップデート処理を予約した後にISM-VAを再起動しないでください。

  ISM-VAを再起動した場合、ファームウェアアップデートは実施されません。

  ISM-VAを再起動した場合には、iRMC WebUIから当該ファームウェアアップデート処理をキャンセルして、予約し直してください。

- 「ファームウェア/ドライバーアップデート」ウィザードの「アップデート設定」画面で[アップデート時にメンテナンスモードに設定する]を選択した場合、ファームウェアアップデートの直前でメンテナンスモードに設定され、アップデート完了後にメンテナンスモードを解除します。日時を指定してファームウェアアップデートする場合に利用してください。

注意

登録されたタスクの「タスク詳細」画面から、実行中のタスクをキャンセルできます。ただし、サブタスクのメッセージに「Updating firmware. (eLCM Offline)」が表示された後は、タスクはキャンセルできません。キャンセル失敗となります。

6. 対象ノード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。

   a. ISMのGUIでグローバルナビゲーションメニューから[構築]-[ファームウェア/ドライバー] を選択します。

      「ノードリスト」画面が表示されます。

   b. [現行バージョン]に表示されているバージョンを確認します。

以上でノードのファームウェアアップデートは完了です。

6.4.3 ServerView embedded Lifecycle Managementを利用してファームウェア／ドライバーをOnlineアップデートする

エフサステクノロジーズWebサイトのデータを利用してもアップデートできますが、ここではRepository Serverのデータを利用する手順で説明します。

注意

- eLCM Onlineアップデートは、対象ノードのOSがWindowsの場合のみ対応しています。
- Windows用のPSP（PrimSupportPack-Win）として提供されるドライバーパッケージをアップデートできます。
- 対象ノードのOS上のServerView Agents、またはServerView Agentless Serviceが利用可能なアップデートを検出し、その結果をiRMCに通知します。ISMは、iRMCから取得した当該情報に基づいて、アップデート可能なドライバーパッケージを表示します。
- アップデート可能なドライバーパッケージにPrimSupportPack-Win/FSC_SCANが存在する場合、更新するファームウェア／ドライバーとして、当該ドライバーパッケージを選択してください。
  PrimSupportPack-Win/FSC_SCANは、対象ノード上のドライバーやソフトウェアキットの情報をスキャンし、各PSPの依存性を考慮したインストール順序を確定する特別なパッケージです。

事前準備

1. 「6.4.2.1 Repository Serverのファームウェアデータを利用してアップデートする」の手順1～3を実施して、Repository Serverと対象ノードのeLCMの環境を構築します。
2. 対象ノードにServerView PrimeUpと、ServerView AgentsまたはServerView Agentless Service（ServerView Suite製品）がインストール済みであることを確認します。

   ServerView Agents、ServerView Agentless Serviceの詳細は、下記のFsas Technologies マニュアルサイトから『ServerView-Agenten Vx.xx (Windows Server xxxx / xxxx / xxxx / xxxx)』（xには、最新の版数、対象Windows Serverバージョンが入ります。）を参照してください。

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

   参照手順

   「製品を選択する」- [製品の検索]を選択し、「Agents」と入力して、[次へ]を選択してください。
   [Documentation] - [Setup Guide]からダウンロードしてください。
3. アップデート対象ノードの電源をオンにします。

ドライバーをアップデートする

注意

- アップデート中は以下の事項を遵守してください。
  - 対象ノードの電源操作を行わない。
  - 対象ノードの再起動、リセットを行わない。
  - ISMと対象ノードの間のネットワークを切断しない。
  - 管理サーバーを再起動しない。管理サーバーの電源をオフにしない。

- ファームウェア／ドライバーのアップデート中に、リブート処理が実施されることがあります。

1. 対象ノードの一覧にファームウェア／ドライバーの情報が表示されるようにします。

   表示されている場合には、以下の手順は不要です。

   a. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。

   b. 対象ノードを選択し、[ファームウェア/ドライバー]タブを選択します。

   c. 「eLCM Online情報取得」を[有効]に変更します。

      [設定]ボタンを選択して、変更してください。

   d. [アクション]ボタンから[ノード情報取得]を選択します。

   e. ファームウェア／ドライバーの情報が一覧に表示されることを確認します。

2. [ファームウェア/ドライバーアクション]ボタンから[ファームウェア/ドライバー更新]を選択します。

   「ファームウェア/ドライバーアップデート」ウィザードが表示されます。

3. アップデート対象のファームウェア／ドライバーを選択します。

   アップデートできるファームウェア／ドライバーがある場合、[eLCM Online最新]にバージョンが表示されます。

   eLCM Onlineアップデートできるファームウェア／ドライバーがない場合、[FW/ドライバー名]欄、[eLCM Online最新]欄の両方、あるいは[eLCM Online最新]欄に「-」が表示され、アップデート対象としてチェックできません。

4. [次へ]を選択します。

5. [更新モード:]欄から[eLCM Online]を選択します。

6. [次へ]を選択して、「ファームウェア/ドライバーアップデート」ウィザードに従い、設定項目を入力して、アップデートを開始します。

   設定項目の入力は、ヘルプ画面を参照してください。

   アップデートの開始後、ISMのタスクとして登録されます。

   アップデートの状況は「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。

   注意

   登録されたタスクの「タスク詳細」画面から、実行中のタスクをキャンセルできます。ただし、サブタスクのメッセージに「Updating firmware. (eLCM Online)」が表示された後は、タスクはキャンセルできません。キャンセル失敗となります。

   以上でノードのアップデートは完了です。

6.5 電力制御を行う（ISM 3.0.0から使用できません）

本機能は、ISM 3.0.0から使用できません。

6.6 ネットワークのトラフィック状況を確認する

ネットワークマップでは、監視対象ホストで動作する仮想マシンの仮想アダプターのトラフィック状況を表示します。仮想ネットワーク パケット分析機能を利用してトラフィック状況を確認する手順について説明します。

仮想ネットワーク パケット分析機能は以下の手順で実施します。

- 6.6.1 仮想アダプターのしきい値を設定する
- 6.6.2 通知を確認する
- 6.6.3 仮想アダプターの通信量を確認する

- 6.6.4 パケット分析を開始する
- 6.6.5 パケット分析の状況を確認する
- 6.6.6 パケット分析の結果を確認する
- 6.6.7 パケット分析を終了する

注意

本機能はISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）でISMにログインが必要です。

6.6.1 仮想アダプターのしきい値を設定する

1. ISMのGUIでグローバルナビゲーションメニューから[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]ボタンから[仮想アダプターしきい値設定]を選択します。
3. 監視するノード、仮想マシンの仮想アダプターを選択します。
4. [監視設定編集]ボタンを選択します。

   ポイント

   ネットワークマップ上でノード、仮想マシン、または仮想アダプターを選択した状態で、[仮想アダプターしきい値設定]を選択した場合、対象の仮想アダプターが選択された状態になります。

5. 監視の有効/無効で「有効」を選択し、しきい値判定を有効にしたい監視項目名のしきい値を設定後に[反映]ボタンを選択します。しきい値は0.001～100までの値をパーセントで指定します。

   ポイント

   - 監視の有効/無効で監視を有効化すると仮想アダプターの監視および性能統計情報の取得を開始します。
   - 監視の有効/無効で監視を無効化すると仮想アダプターの監視および性能統計情報の取得を停止します。
   - しきい値を入力すると入力した項目のしきい値判定が有効になります。
   - しきい値をクリアするとしきい値判定が無効になります。
   - しきい値には警告しきい値と異常しきい値が設定できますが、片方のみを設定することも可能です。

注意

- 監視を有効化できる仮想アダプター数は最大1000です。ISM-VAに割り当てたリソースによる総仮想マシン数の上限を超えない範囲で設定してください。詳細は、『解説書』の「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」の「仮想ネットワークパケット分析機能を使用する場合」を参照してください。
- しきい値設定画面の上部に表示される「監視アダプター数」を確認することで、監視を有効化しているアダプター数を確認できます。

6.6.2 通知を確認する

仮想アダプターに設定したしきい値を超えるとイベントが発生します。

[イベント]の[運用ログ]に、以下のメッセージが表示されます。

イベントID	メッセージ
30030112	仮想マシン(VM名)の仮想アダプター(仮想アダプター名)の監視項目(監視項目名)が警告上限しきい値(ユーザー設定値)を超過しました(最新値=測定値)。
50030114	仮想マシン(VM名)の仮想アダプター(仮想アダプター名)の監視項目(監視項目名)が異常上限しきい値(ユーザー設定値)を超過しました(最新値=測定値)。

監視項目名には以下が設定されます。

- Transmit Error Rate(送信エラー率)
- Transmit Drop Rate(送信ドロップ率)
- Received Error Rate(受信エラー率)
- Received Drop Rate(受信ドロップ率)

6.6.3 仮想アダプターの通信量を確認する

1. 「6.6.2 通知を確認する」で通知されたイベントのノードを選択します。
2. ノードの詳細画面のネットワーク マップを選択します。
3. 通信量を確認したい仮想アダプター名を選択します。または、強調表示されている仮想アダプター名を選択します。

4. 画面の右ペインに表示されている[仮想アダプター情報]のウィンドウを下にスクロールさせ、[トラフィック情報]を確認します。
5. 情報の右側にある[グラフ]ボタンを選択することで、監視データの推移をグラフで確認できます。

ポイント

- OpenStackの場合、[仮想アダプター情報]に[プロセス情報](仮想アダプターのCPU使用率)が表示されます。
- 監視設定をした仮想アダプターを持つ仮想マシンを選択すると、[仮想マシン情報]に[CPU情報](VMのvCPUの使用率)が表示されます。vCPU IDを選択すると、[プロセス毎情報](プロセスのCPU使用率、コンテキスト情報)が表示されます。また、[物理CPUコアID]を選択すると、[物理CPU情報](物理CPU使用率)が表示されます。

図6.1 [仮想アダプター情報]のウィンドウ

6.6.4 パケット分析を開始する

トラフィックを確認しても性能低下原因が特定できなかった場合、イベントが発生している監視対象ホストに対して、パケット分析を実施します。

性能問題が発生している監視対象ホストのハイパーバイザーに対して、分析VMをデプロイします。

6.6.4.1 分析VMを入手する

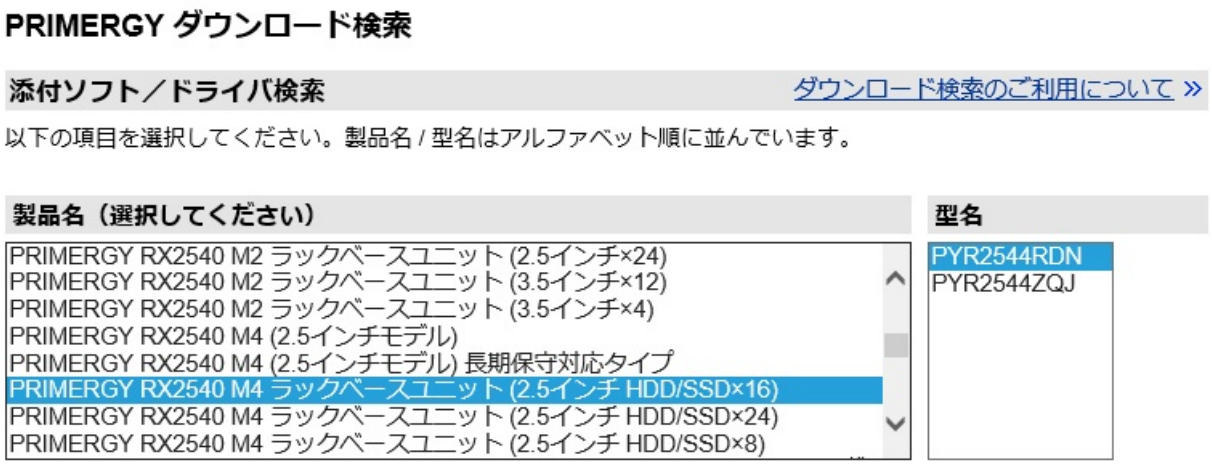
以下の手順で分析VMをダウンロードします。すでにダウンロードしている場合、本手順は不要です。

1. 「PRIMERGY ダウンロード」ページにアクセスします。

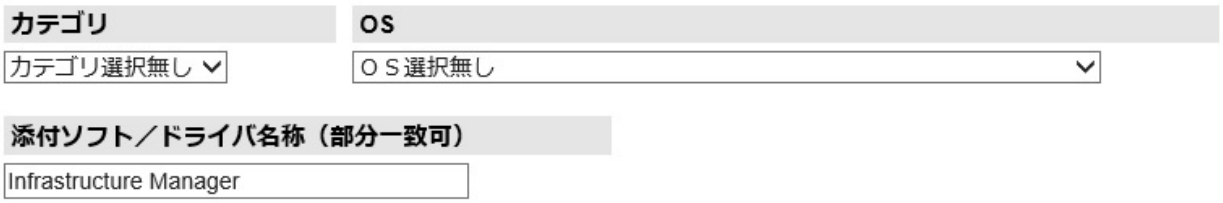
   https://www.fujitsu.com/jp/products/computing/servers/primergy/downloads/

2. ページ中段にある「ダウンロード検索」ボタンを選択します。

3. 「製品名」の欄で、ISMをインストールするサーバー（ISMの仮想マシンイメージを配置するハイパーバイザーが動作しているサーバー）の製品名を選択します（型名の選択は任意です）。



4. 「添付ソフト／ドライバ名称」の欄で、「Infrastructure Manager」と入力します。



5. 「検索開始」ボタンを選択します。
6. 検索結果の画面で、対象のCMS（クラウドマネージメントソフトウェア）と分析VMのバージョンを確認し、任意のファイルを選択します。
7. 表示されるページの記載に従って、ファイルをダウンロードします。

注意

ハイパーバイザーの種類（VMware, OpenStack）により使用するVMイメージは異なります。

6.6.4.2 分析VMをインポートする

以下の手順で分析VMイメージをISM-VAに配置します。すでにISM-VAに配置している場合、本手順は不要です。

FTPクライアント、またはファイルのアップロード機能を使用して、VMイメージをISM-VA内のファイル転送領域「/Administrator/ftp」配下に配置してください。

詳細は、『解説書』の「2.1.2 FTPアクセス」または、「1.4.1 ISM-VAにファイルをアップロードする」を参照してください。

分析VMのインポートは「6.6.4.3 分析を開始する」のパラメーター入力時に実施することもできます。この場合、ファイル名の先頭に固有の識別文字列が付与されます。

例)PKTANALYZ110_VMWARE.vmdk
インポート後のファイル名
563654e8-2f95-4c89-96b3-eece9772d179-PKTANALYZ110_VMWARE.vmdk

6.6.4.3 分析を開始する

1. 分析を実施する[仮想アダプター]を選択します。
2. 画面の右ペインに表示されているパケット分析の[分析開始]ボタンを選択します。
3. パラメーターを入力します。

表6.1 分析VM IPアドレス設定

項目	説明
IPバージョン*	IPバージョンを選択してください
DHCP*	DHCPの有効／無効を選択してください ※OpenStackの場合、IPバージョンにIPv6を選択すると自動的に有効になります
IPアドレス*	DHCPが無効の場合は指定が必須となります
プレフィックス（IPv6指定時）* サブネットマスク（IPv4指定時）*	DHCPが無効の場合は指定が必須となります
デフォルトゲートウェイ	DHCPが無効の場合は指定が必須となります ※VMwareのみ表示されます
NTPサーバーIPアドレス	NTPサーバーをIPアドレスで指定します ※時刻ずれなどを防ぐために指定することを推奨します

*：設定が必須の項目

表6.2 分析VMテプロイ設定（VMware）

項目	説明
分析VM名*	分析VM名を指定してください
分析VMイメージファイル名*	分析VMのvmdkファイルを指定してください
分析VMovfファイル名*	分析VMのovfファイルを指定してください
データストア名*	データストア名を指定してください
フォルダー名	分析VMを管理するvCenterのフォルダー名を指定してください
マネジメントポート接続先 仮想スイッチタイプ*	マネジメントポートの接続先仮想スイッチタイプ（標準仮想スイッチ/分散仮想スイッチ）を選択してください
仮想スイッチ名*	ISMと通信可能な仮想スイッチ名を指定してください
ネットワークラベル／ポートグループ*	ISMと通信可能なネットワークラベルまたはポートグループ名を指定してください

*：設定が必須の項目

表6.3 分析VMデプロイ設定（OpenStack）

項目	説明
分析VM名*	分析VM名を指定してください
分析VMイメージファイル名*	分析VMのqcow2ファイルを指定してください
セキュリティグループ*	分析VMに適用するSSHが許可されているセキュリティグループ名を指定してください
プロジェクト名*	分析対象VMが属するプロジェクト名を指定してください
ネットワーク名*	ISMと通信可能なネットワークを指定してください
Floating IPアドレス設定*	フローティングIPアドレスを使用するか選択してください
Floating IPアドレス*	フローティングIPアドレスを指定してください ※フローティングIPアドレスを使用する場合は必須です

*：設定が必須の項目

注意

- パケット分析結果を確認し、原因への対処後に状況の改善を確認できたら、処理負荷の低減およびディスク容量の節約のためパケット分析を停止することを推奨します。
- パケット分析の開始後、ノードのOSアカウント、または仮想化管理ソフトウェアの設定を削除・変更しないでください。パケット分析の情報が取得できなくなります。また、ISMから分析VMの削除ができなくなります。
- 監視対象ホストのハイパーバイザー上に分析VMをデプロイするため、あらかじめリソースを確保しておく必要があります。詳細は、『解説書』の「1.3 システム要件」を参照してください。
- 分析VMのデプロイ時に、監視対象ホスト上でパケットミラー設定が自動で実施されます。ミラーによりキャプチャしたパケットはヘッダ情報のみを解析します。また、キャプチャした情報を保存することはありません。
- パケット分析中はパケット分析で監視対象ホスト上のリソースを使用します。ノードのCPUが高負荷の場合、業務VMの性能が低下する可能性があります。本内容をご理解のうえ、ご利用願います。
- VMwareの場合、分析対象の仮想アダプターは分散仮想スイッチに接続されている必要があります。
- OpenStackの場合、分析VMに適用するセキュリティグループでは、SSHが許可されている必要があります。

6.6.5 パケット分析の状況を確認する

パケット分析の分析開始の実施状況は運用ログを確認してください。また、現在のパケット分析の状況一覧は[アクション]ボタンから[仮想ネットワーク パケット分析状況]を選択することで確認できます。

運用ログで出力される主なメッセージは以下です。

イベントID	メッセージ	対処
10030037	仮想ネットワーク分析の分析設定が完了しました(分析VM: 分析VM名)	分析開始が正常に完了しました。パケット分析結果を確認してください。
50035216	仮想ネットワーク分析のデプロイ処理中にエラーが発生しました。分析VM(分析VM名)のデプロイに失敗しました。(エラーメッセージ)	正しい入力パラメーターを指定して再実行してください。または、仮想化管理ソフトウェアの状態を確認してください。 出力される(エラーメッセージ)に従い対応してください。
50035217	仮想ネットワーク分析のデプロイ処理中にエラーが発生しました。分析VM(分析VM名)の開始設定に失敗しました。(エラーメッセージ)	正しい入力パラメーターを指定して再実行してください。または、仮想化管理ソフトウェアの状態を確認してください。 出力される(エラーメッセージ)に従い対応してください。

6.6.6 パケット分析の結果を確認する

パケット分析によるボトルネックの原因、根拠、改善案を確認します。また、パケット分析の結果を確認します。

ポイント

パケット分析の結果の確認は、パケット分析の開始から10分程度経過したあとに、[詳細確認]を選択して情報を参照してください。

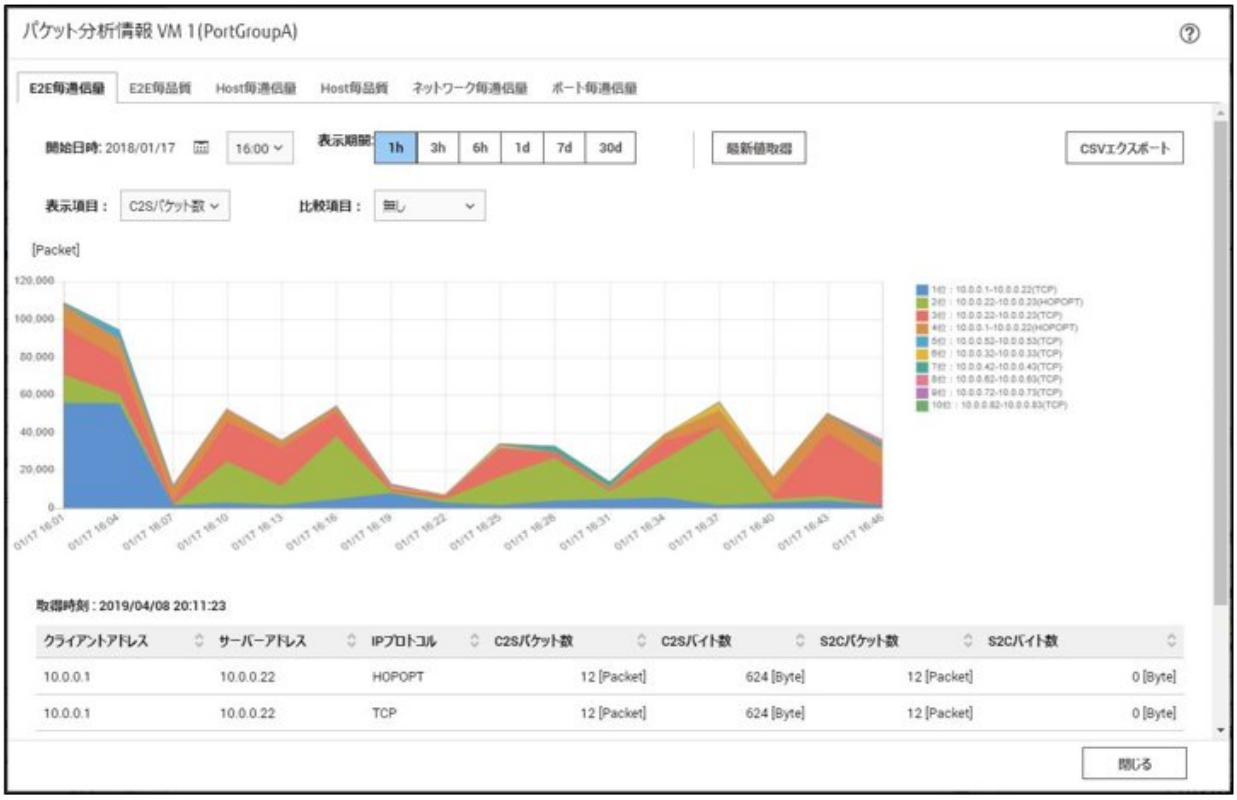
[ボトルネック分析]として以下の項目を表示します。内容を参照し、対処を検討してください。

- [分析対象期間]
- [分析対象要因情報]
- [ボトルネック分析結果](原因、根拠、改善案)

図6.2 ボトルネック分析結果

[詳細確認]を選択して、[パケット分析]の結果を確認します。

図6.3 パケット分析結果

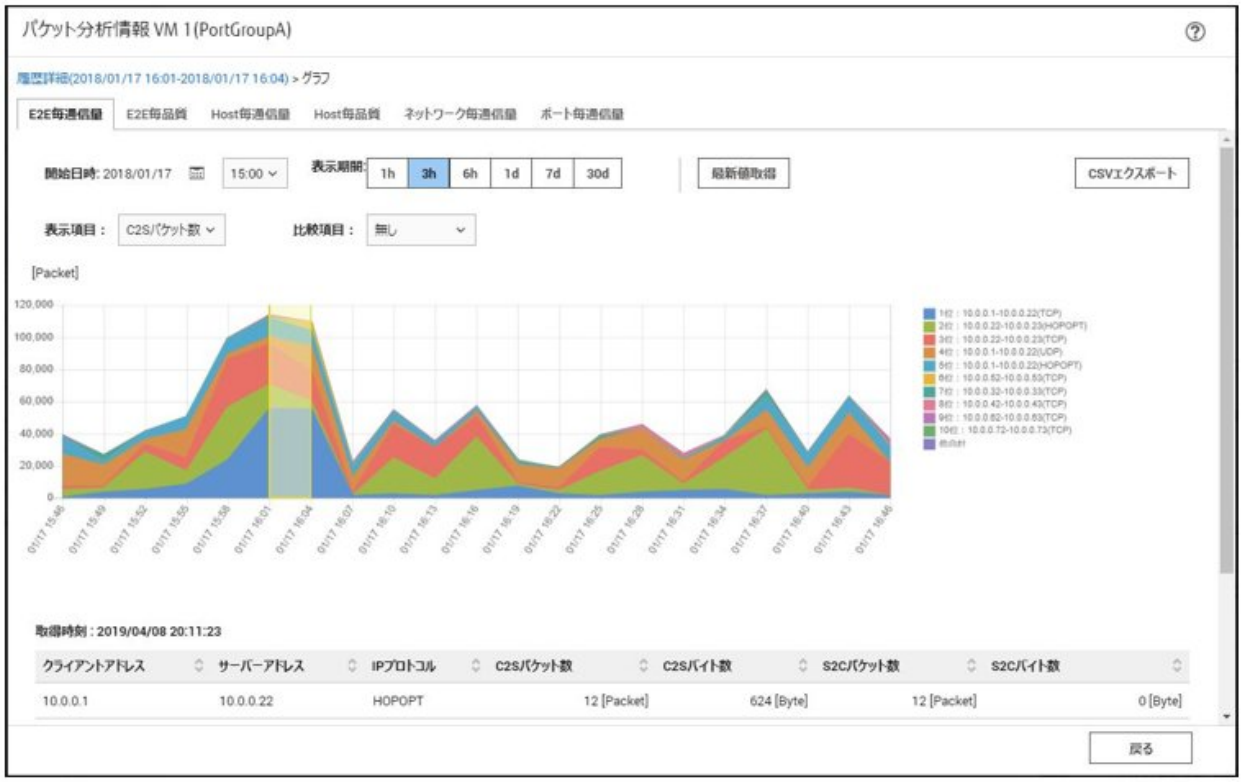


[ボトルネック分析]は[履歴表示]を選択することにより、過去のボトルネック分析結果の履歴を確認できます。

図6.4 ボトルネック分析履歴情報

[グラフ]ボタンを選択して、選択中のボトルネック分析情報の期間を含むパケット分析結果を表示します。ボトルネック分析の対象となった期間は、グラフ上で黄色の網掛けで示します。

図6.5 パケット分析結果（過去のボトルネック分析期間を含む）



6.6.7 パケット分析を終了する

パケット分析を実施している「仮想アダプター」を選択し、画面の右の[仮想アダプター情報]に表示されている[パケット分析]の [分析停止]ボタンを選択します。もしくは、[アクション]ボタンから[仮想ネットワーク パケット分析状況]を選択し、分析設定の[分析停止]ボタンを選択します。

分析VMがハイパーバイザーから削除されます。

6.7 PRIMEFLEXシステムをローリングアップデートする

PRIMEFLEX HS／PRIMEFLEX for VMware vSANの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とESXi修正パッチ、ESXiオフラインバンドル、vCSA修正パッチ、vCSAアップグレード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。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

なお、ローリングアップデート機能のファームウェアアップデートは、Offlineアップデートのみ対応しています。Offlineアップデートの詳細は、『解説書』の「2.6.3 ファームウェア／ドライバーのアップデート」を参照してください。

ローリングアップデートは、以下の作業フローで行います。

表6.4 PRIMEFLEX HS／PRIMEFLEX for VMware vSANのローリングアップデートフロー

ローリングアップデート手順		作業内容
1	事前準備	• 適用するファームウェアデータの入手 • 適用するESXi修正パッチ／オフラインバンドルファイルの入手 • 適用するvCSA修正パッチファイルまたはvCSAアップグレードファイルの入手 • 適用するファームウェアデータをISM-VAへインポート • 古いESXi修正パッチ／オフラインバンドルとESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプトの削除

ローリングアップデート手順		作業内容
		• 適用するESXi修正パッチ／オフラインバンドルファイルをISM-VAへアップロード • 適用するvCSA修正パッチファイルをデータストアへアップロード • 適用するvCSA修正パッチファイルをvCSAにマウント • 適用するvCSAアップグレードファイルをISM-VAへアップロード • ファームウェアアップデート対象ノードの選定 • 仮想マシン退避ノードの選定 • ファームウェアアップデートに必要な準備作業の実施 • ESXiの修正パッチ／オフラインバンドルの注意事項の確認と対処
2	ローリングアップデートの実行	
3	事後処理	• ファームウェアアップデート確認 • ESXiのバージョン確認 • スクリプトの実行結果確認 • vCSAのバージョン確認 • OS情報の更新 • 仮想化管理ソフトウェア情報の更新 • 適用したvCSA修正パッチファイルをvCSAからアンマウント • 既存vCSAの削除 • vCLS仮想マシンのデータストアの確認と移動 • 不要なファイルの削除 • クラスタ退避モードの解除

6.7.1 動作要件

ローリングアップデート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。

対象クラスタの動作要件

- 仮想リソース管理機能の事前設定が実施されていること

  詳細は、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

- Active Directory連携を行う構成の場合は、ADVMが最低1台以上起動していること
- ネットワーク構成はPRIMEFLEX HS／PRIMEFLEX for VMware vSAN導入サービスで構築した環境から変更していないこと
- NTPサーバーと時刻同期できていること
- 退避ノードは、以下の要件を満たすこと

  ー 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、メモリー容量など）があること

  ー 起動している仮想マシンがないこと

  ローリングアップデートでは、対象ノードを再起動するために、対象ノード上で起動している仮想マシンを退避ノードへ移行します。退避ノードが上記要件を満たしていない場合、ローリングアップデートに失敗します。

- DHCPサーバー／ルーターで払い出しするIPアドレス数が、ファームウェアのOfflineアップデート対象サーバー台数の3倍以上となるよう設定されていること

- 3台以上の正常なノードで構成されていること

  2台以下の構成ではローリングアップデート機能は使用できません。

- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること

- クラスタとノードのステータスに異常がないこと

  処理の始めにクラスタ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、ローリングアップデートは実行されません。

  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

    vCSA 6.5以前（Flash）の場合：

    1. vSphere Web ClientでvCSAにログインします。
    2. 「トップ」画面から[ホーム]タブ-[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。

    vCSA 6.7以降（HTML5）の場合：

    1. vSphere ClientでvCSAにログインします。
    2. 「トップ」画面から[ショートカット]- [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」画面のアップデート対象ノードのステータスが「Normal」であることを確認してください。

- ISMの仮想化管理ソフトウェアにPRIMEFLEXのvCSAが登録されていること

- 3台構成でローリングアップデート機能を使用する場合は、対象のクラスタに対して、以下のどちらか一方の条件満たすこと（vSphere 7.0u1以降の場合）

  ー DRS機能がオンであること

  ー DRS機能がオフであり、かつクラスタを退避モードに設定していること

  クラスタ退避モードの設定については、PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』の「vSANクラスタ停止の準備」の「クラスタを退避モードに設定します。」を参照して実施してください。

  PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4の『オペレーション＆メンテナンスガイド』入手先：

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

- VMware Distributed Resource Scheduler（以降、「DRS」と表記）機能がオンのとき、自動化レベルは、「完全自動化」に設定されていること

  自動化レベルを「完全自動化」以外に設定すると、エラー終了する可能性があります。DRS機能がオンのときは、退避ノードの準備は不要です。
  以下の手順でVMware DRSの自動化レベルを確認、設定できます。

  vCSA 6.5以前（Flash）の場合：

  1. vSphere Web ClientでvCSAにログインします。
  2. 「トップ」画面から[ホーム]タブ-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定]-[サービス]-[vSphere DRS]の[編集]からVMware DRSの自動化レベルを設定します。

  vCSA 6.7以降（HTML5）の場合：

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定 [注]]-[サービス]-[vSphere DRS]の[編集]からVMware DRSの自動化レベルを設定します。

     [注]：vCSA 7.0 U3以降の場合、[構成]と表示されます。

・ vSANデータストアに空き容量を確保すること

1台のノードをメンテナンスモードに設定しても、vSANデータストアが30%以上の空き容量を確保できる必要があります。

・ アラーム定義で健全性エラーを無効に設定すること

ローリングアップデート実行中にアップデート対象ノードを再起動するため、ESXiホストをメンテナンスモードに設定しますが、その際に以下の健全性エラーが発生する可能性があります。

ー vSAN6.5環境（VMware ESXi 6.5）～ vSAN7.0 U1環境（VMware ESXi 7.0 U1）の場合

- vSAN健全性アラーム「vSANディスクバランス」
- vSAN健全性サービスアラーム「全体的な健全性サマリ」
- vSAN健全性アラーム「クラスタの健全性」

ー vSAN7.0 U2環境（VMware ESXi 7.0 U2）の場合

- vSANクラスタアラーム「vSANディスクバランス」
- vSAN健全性サービスアラーム「全体的な健全性サマリ」
- vSANビルド推奨アラーム「vSAN ビルドの推奨事項エンジン」

ー vSAN7.0 U3環境（VMware ESXi 7.0 U3）以降の場合

- vSANクラスタアラーム「vSANディスクバランス」
- vSAN健全性サービスアラーム「全体的な健全性サマリ」
- vSAN ハードウェア互換性「vSAN HCL DB の更新状態」
- vSAN ハードウェア互換性「vSAN HCL DB の自動更新」
- vSANビルド推奨アラーム「vSAN リリース カタログの更新状態」
- vSANビルド推奨アラーム「vSAN ビルドの推奨事項エンジン」
- vSANビルド推奨アラーム「vSAN ビルドの推奨事項」(vCSA 8.0 U2以降)
- 「vSAN Support Insight」

アラーム定義で上記の健全性エラーを無効に設定してください。アラーム定義は以下から設定できます。

ー vSAN6.5環境（VMware ESXi 6.5～6.5 U3）（Flash）の場合

「トップ」画面から[インベントリ]-[ホストおよびクラスタ]の[＜vCSA名+ドメイン名＞]-[監視]-[問題]-[アラーム定義]

ー vSAN6.7環境（VMware ESXi 6.7）以降（HTML5）の場合

「トップ」画面から[インベントリ]-[ホストおよびクラスタ]の[＜vCSA名+ドメイン名＞]-[設定 [注]]-[アラーム定義]

[注]：vCSA 7.0 U3以降の場合、[構成]と表示されます。

ローリングアップデート実行完了後、必要であればアラーム定義の設定を元に戻してください。

ポイント

ー アラーム定義でこの健全性エラーを無効に設定せずに、この健全性エラーが発生するとローリングアップデート機能はエラー終了します。

ー ローリングアップデート実行完了後にアラーム定義の設定を元に戻した場合、この健全性エラーが発生する可能性があります。以下のKBを参照して対処してください。

https://kb.vmware.com/s/article/2144278?lang=ja

- vCSA 7.0 U1以降の場合、vSphereクラスタサービス(vCLS)のステータスが正常になっていること

  vSphereクラスタサービス(vCLS)のステータスは、以下の手順で確認できます。
  クラスタ退避モードの設定を行った場合、本確認手順は不要です。

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]を選択します。
  3. [名前]が[＜vCLS名＞]の[ステータス] を確認します。
     - vCSA 7.0U2以前の場合:

       ＜vCLS名＞は、"vCLS (n)" (nは数字)で表示されます。
     - vCSA 7.0U3以降の場合:

       ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"(Xは16進数)で表示されます。

     [ステータス] が「正常」であることを確認してください。
  4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

ポイント

vCSAにログインするユーザー種別によってはvSphereクラスタサービス(vCLS)が表示されない場合があります。
vSphereクラスタサービス(vCLS)関連の操作を行う際には、vCenter Single Sign-Onドメインの管理者を使用してください。

- vCSA 7.0 U1以降の場合、vCLS仮想マシンはvSANデータストア上に存在していること

  vCLS仮想マシンが配置されているデータストアは、以下の手順で確認できます。
  クラスタ退避モードの設定を行った場合、本確認手順は不要です。

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
     - vCSA 7.0U2以前の場合:

       ＜vCLS名＞は、"vCLS (n)"(nは数字)で表示されます。
     - vCSA 7.0U3以降の場合:

       ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"(Xは16進数)で表示されます。
  3. [データストア]-[名前] がvSANデータストア名であることを確認します。

     vSANデータストア名は、ISMのGUIで対象クラスタのクラスタ定義パラメーターの[クラスタ詳細情報]-[ストレージプール]タブの[ストレージプール名]で確認できます。

     vSANデータストア名ではない場合、「6.7.4.9 vCLS仮想マシンのデータストアを確認して移動する」の「vSANデータストアへの移動手順」を実施します。
  4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

対象サーバーの動作要件

- アップデート対象ノードの電源がオンになっていること

  以下の手順で確認できます。

  1. ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択し、「クラスタリスト」画面を表示します。
  2. [＜対象のクラスタ＞]-[ノードリスト]タブからアップデート対象ノードのノード名を選択し、ノードの詳細画面を表示します。
  3. [プロパティ]タブのパワーステータスで電源オンを確認します。

注意

- システムの構成やクラスタの設定などの関係で、他ノードへ移動できない仮想マシンを実行している場合、ローリングアップデートに失敗します。

  例）PRIMEFLEX for Microsoft Storage Spaces Direct構成の場合、ISM-VAは管理兼業務サーバー間でしか移動できません。

  以下のどちらかの方法で、仮想マシンの移動を回避できます。

  ー ローリングアップデートを実行する前に、他ノードへ移動できない仮想マシンを手動で停止する

  ー 他ノードへ移動できない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「ローリングアップデート」ウィザードで設定する

  ローリングアップデート実行時、アップデート対象ノードはシャットダウンされます。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、アップデート対象ノードにしないでください。

- ローリングアップデート機能は、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、その仮想マシンが起動していると、ノード再起動の際に別のノードに移動してしまいます。別のノードに移動されてライセンス違反にならないようにしてください。

  以下のどちらかの方法で、仮想マシンの移動を回避できます。

  ー ローリングアップデートを実行する前に、他ノードに移動してはいけない仮想マシンを手動で停止する

  ー 他ノードに移動してはいけない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「ローリングアップデート」ウィザードで設定する

  ローリングアップデート実行時、アップデート対象ノードはシャットダウンされます。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、かつ起動しているノードは、アップデート対象ノードにしないでください。

- PRIMEFLEX構成のADVMを使用している場合、ADVM#1およびADVM#2が実行しているノードは、同時にアップデート対象ノードにしないでください。

  ADVM#1またはADVM#2が実行しているノードは、2回に分けてローリングアップデートを実行する必要があります。

  例）2回のローリングアップデートの実行でADVM#1およびADVM#2が実行している全ノードをアップデート対象とする手順

  1. ADVM#2を手動で停止します。
  2. ADVM#1が実行しているノード以外をアップデート対象ノードに選択します。
  3. ローリングアップデートを実行します。
  4. ADVM#2を手動で起動します。
  5. ADVM#1を手動で停止します。
  6. ADVM#1が実行していたノードをアップデート対象ノードに選択します。
  7. ローリングアップデートを実行します。
  8. ADVM#1を手動で起動します。

vCSA修正パッチの適用の動作要件

- vCSAのSSHログインが有効になっていること

  SSHログインが有効かどうかの確認は、以下の手順で確認できます。

  1. VMware Appliance Managementにrootユーザーでログインします。
  2. [アクセス]-[アクセス設定]-[SSHログイン]の「有効」で確認できます。

  SSHサービスの起動は、以下の手順で設定できます。

  1. VMware Appliance Managementにrootユーザーでログインします。
  2. [アクセス]-[アクセス設定]-[編集]ボタンを選択します。
  3. 「アクセス設定の編集」画面で[SSHログインの有効化]を有効に設定して、[OK]ボタンを選択します。

- vCSA 7.0 U1以降の場合、仮想化管理ソフトウェアで使用するユーザーはvCenter Serverのシングルサインオン管理者のユーザーであること
- vCenter Server Applianceにパッチを適用する際に、vCenter Server Applianceのアップデートをまたぐ場合は、パッチを適用する前にアップデートすること

  例：vCSA 7.0にvCSA 7.0U2cのパッチを適用する場合

  次の順番でパッチを適用します。
  7.0 → 7.0U2（アップデート） → 7.0U2c（パッチ適用）（7.0 → 7.0U2cのパッチ適用はできません）

vCSAアップグレードの動作要件

- vCSAのSSHログインが有効になっていること
- DRS機能がオフになっていること
- 仮想化管理ソフトウェアで使用するユーザーはvCenter Serverのシングルサインオン管理者のユーザーであること
- 対象クラスタにvCSAが存在していること
- クラスタ定義パラメーターが作成されていること
- 使用しているvCSAの分散仮想スイッチのバージョンがサポートされていること

  以下のURLを参照して、サポート有無を確認してください。

  https://kb.vmware.com/s/article/52826?lang=ja

  サポートされていない場合、事前にアップグレードするvCSAでサポートされている分散仮想スイッチへバージョンアップをしてください。

  分散仮想スイッチのバージョンは、以下の手順で確認できます。

  vCSA 6.5以前（Flash）の場合：

  1. vSphere Web ClientでvCSAにログインします。
  2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ネットワーク]の[＜分散仮想スイッチ名＞]を選択します。
  3. [サマリ]タブ-[バージョン]を確認します。
  4. すべての分散仮想スイッチで手順2～3を実施します。

  vCSA 6.7以降（HTML5）の場合：

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[インベントリ]-[ネットワーク]の[＜分散仮想スイッチ名＞]を選択します。
  3. [サマリ]タブ-[バージョン]を確認します。
  4. すべての分散仮想スイッチで手順2～3を実施します。
- vCSAのバージョンと仮想化管理ソフトウェア情報のタイプが合っていること

ESXi修正パッチ／オフラインバンドルの適用の動作要件

- PRIMEFLEX構成のADVMを使用している場合、DRS機能がオフになっていること
- PRIMEFLEX構成のADVMを使用している場合、ADVM#1またはADVM#2が実行しているノードを退避ノードに選択すること

  退避ノードに選択したノードで実行しているADVM#1またはADVM#2は、退避ノードに選択していないADVM#1またはADVM#2が実行しているノードへ移動してください。

注意

- vSANの健全性チェックが有効になっているため、以下の警告が表示される場合があります。健全性エラーと対処方法は以下のとおりです。

  ー ハードウェア互換性の確認結果がエラー表示になっている場合は、以下のサイト（英語サイト）を参照し、HCL DB（Hardware Compatibility List Database）を最新に更新して、エラー表示が解消されることを確認してください。

  https://kb.vmware.com/kb/2109870

  以下のURLから最新のHCL DBのデータが取得できます。

  http://partnerweb.vmware.com/service/vsan/all.json

  ー パフォーマンスサービスの確認結果がエラー表示になっている場合は、パフォーマンスサービスをオンにすることで解消可能です。パフォーマンスサービスを有効にした場合、データベースの最大容量255GBを加味してキャパシティデバイスの容量を設計する必要があります。

  https://kb.vmware.com/kb/2144403

  お客様の環境でパフォーマンスサービスを使用しない運用となっている場合は、「トップ」画面から[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＞]-[サマリ]で対象警告の[緑にリセット]を選択して、警告を消すことが可能です。

  ー [ネットワーク]-[MTUチェック(パケットサイズの大きいping)]がエラーになっている場合は、誤って警告アラートが発行されている可能性があります。ネットワーク構成およびESXiホストに問題がない場合、以下を対処することで、警告アラートの抑止が可能です。

  - アラーム定義のvSAN Health アラーム「MTUチェック(パケットサイズの大きいPing)」でアラームを無効化します。
  - 「トリガーを指定する」画面で「警告」のイベントを削除します。

  ー [クラスタ]-[vSANディスクバランス]がエラーになっている場合は、「ディスクの再分散」を手動で実施することで、vSANディスクバランスを正常化できます。また、クラスタ内のキャパシティデバイスの使用率が80パーセントに達した場合、vSANはすべてのキャパシティデバイスの使用率がしきい値を下回るまで、自動的にクラスタをリバランスします。

- ローリングアップデート実行中にアップデート対象ノードを再起動するため、ESXiホストをメンテナンスモードに設定しますが、その際に以下の健全性エラーが発生する可能性があります。

  ー ディスク フォーマットのバージョン

  以下のサイトに記載されているようにESXiオフラインバンドルを適用する際、「ディスク フォーマットのバージョン」が変更される場合があります。

  https://kb.vmware.com/s/article/2148493

  アラーム定義の「ディスク フォーマットのバージョン」でアラームを無効化することで、警告アラートの抑止が可能です。

- vCSAアップグレードとESXi修正パッチ／オフラインバンドルを適用する場合、以下のURLを参照して、サポートされているバージョンの組み合わせか確認します。

  サポートされていないバージョンへのアップグレードは、環境破壊の恐れがあるため絶対にしないでください。

  https://www.vmware.com/resources/compatibility/sim/interop_matrix.php

  例）ESXi 6.7 U3では、vCSA 6.7以降が必要です。

- vCSA7.0U2以降でvCSAにログインする場合には、ローカルユーザーを使用しないでください。

6.7.2 事前準備

ローリングアップデートを行う前の準備作業について説明します。

以下の手順で事前準備してください。

6.7.2.1 適用するファームウェアデータを入手する

ファームウェアアップデートを実施する場合、ServerView Suite Update DVDが必要になります。対象のファームウェアデータが同梱されたServerView Suite Update DVDを入手してください。

入手方法は、「6.4.1 インポートしたファームウェアデータを利用してファームウェアをアップデートする」の手順2、および『解説書』の「2.13.2 リポジトリ管理機能」を参照してください。

また、サポートするファームウェアは、『解説書』の「2.12.4 ローリングアップデート機能」を参照してください。

ポイント

ServerView Suite Update DVDに同梱されていないファームウェアデータでアップデートする場合、ServerView Suite Update DVDに加え、個別ファームウェアデータが必要になります。エフサステクノロジーズのWebサイトより対象ファームウェアのASP for Linuxを入手してください。
入手方法は、「6.4.1 インポートしたファームウェアデータを利用してファームウェアをアップデートする」の手順1～4、および『解説書』の「2.13.2 リポジトリ管理機能」を参照してください。

6.7.2.2 適用するESXi修正パッチ／オフラインバンドルファイルを入手する

ESXi修正パッチ／オフラインバンドルファイルは、VMware Webサイトからダウンロードしてください。

パッチのダウンロード前に、オフラインバンドルの公開情報を確認してください。オフラインバンドルとはエフサステクノロジーズのサーバー向けにパッチ、ドライバーをまとめたものです。オフラインバンドルを利用することで、パッチとドライバーが適用された状態になります。

- 目的のパッチを同梱しているオフラインバンドルが存在する場合
  オフラインバンドルを適用してください。
- 目的のパッチバージョンまでの間にオフラインバンドルが存在する場合
  オフラインバンドルを適用してから、パッチを適用してください。

詳細は、以下のサイトを参照して、『VMware vSphere X.X ソフトウェア説明書』(Xには、バージョンが入ります。)をご確認ください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

6.7.2.3 適用するvCSA修正パッチファイルまたはvCSAアップグレードファイルを入手する

vCSA修正パッチファイルまたはvCSAアップグレードファイルは、VMware Webサイトからダウンロードしてください。

表6.5 vCSAに適用可能な種別ごとのファイル名

vCSAに適用可能な種別	ファイル名
vCSA修正パッチ	ファイル名の末尾に"-patch-FP"が付いているisoファイル 例：VMware-vCenter-Server-Appliance-<product_version>-<build_number>-patch-FP.iso
vCSAアップグレード	上記以外のisoファイル

- 例：vCSA修正パッチを使用する場合（vCSAアップグレードは使用できません。）

  vCSA6.7 Update1からvCSA6.7 Update3へのバージョンアップ

  vCSA6.7 Update1からvCSA6.7 Update2aへのバージョンアップ

  vCSA6.7からvCSA6.7 Update2aのバージョンアップ

- 例：vCSAアップグレードを使用する場合（vCSA修正パッチは使用できません。）

  vCSA6.5からvCSA6.7へのバージョンアップ

  vCSA6.5 Update1からvCSA6.7 Update2aへのバージョンアップ

6.7.2.4 適用するファームウェアデータをISM-VAへインポートする

適用するファームウェアデータをISM-VAへインポートしてください。インポートの手順は、「6.4.1 インポートしたファームウェアデータを利用してファームウェアをアップデートする」の手順5～6、および『解説書』の「2.13.2 リポジトリ管理機能」を参照してください。

また、サポートするファームウェアは、『解説書』の「2.12.4 ローリングアップデート機能」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、『解説書』の「3.7 仮想ディスクの割当て」を参照してください。

注意

- Intel LANカードは現行バージョンにeTrack-IDという識別子を表示します。

  eTrack-IDは、iRMCのWebインターフェイスで表示されるファームウェアバージョンです。

  アップデート対象を判断するため、現行バージョンとインポートしたファームウェアのバージョンを比較します。

  ー ServerView Suite Update DVD（12.19.07版以降）からインポートした場合

  表示形式：適用前のeTrack-ID-適用後のeTrack-ID（ファームウェアファイルのファームウェアバージョン）

  適用前のeTrack-IDが現行バージョンと一致した場合、アップデート対象となります。

  ー 公開サイトからダウンロードしたファームウェアをインポートした場合／ServerView Suite Update DVD（12.19.07版より前）からインポートした場合

  表示形式：（インポートしたファームウェアバージョン（eTrack-IDは含まれない））

  現行バージョンによらず、アップデート対象外となります。

- PSAS CP403i/PSAS CP400iに対するファームウェアアップデートをする場合、ServerView Suite Update DVD V13以外で対象のファームウェアが収録されているバージョンのServerView Suite Update DVDをインポートしてください。

6.7.2.5 以前に使用したスクリプトを削除する

ローリングアップデートを使用する場合には、以下の手順で古いESXiの修正パッチ／オフラインバンドルとESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプトを削除してください。

(1) 古いESXiの修正パッチを削除する

ISM-VAに対して実施してください。前回のローリングアップデート時にISM-VAにアップロードしたESXiの修正パッチを使用する場合は、本手順は不要です。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/patch
ファイル	古いESXiの修正パッチファイル

(2) 古いESXiのオフラインバンドルを削除する

ISM-VAに対して実施してください。前回のローリングアップデート時にISM-VAにアップロードしたESXiのオフラインバンドルを使用する場合は、本手順は不要です。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
ファイル	古いESXiのオフラインバンドルファイル

(3) 古いESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプトを削除する

ISM-VAに対して実施してください。前回のローリングアップデート時にISM-VAにアップロードしたESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプトを使用する場合は、本手順は不要です。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/script
ファイル	古いESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプト

6.7.2.6 適用するESXiの修正パッチ／オフラインバンドルファイルをISM-VAへアップロードする

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、ESXi修正パッチ／オフラインバンドルファイルをアップロードしてください。

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、『解説書』の「3.7 仮想ディスクの割当て」を参照してください。

表6.6 アップロードするESXiの修正パッチファイルとディレクトリー

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/patch
ファイル	ESXiの修正パッチファイル 例）ESXi650-201704001.zip

表6.7 アップロードするESXiのオフラインバンドルファイルとディレクトリー

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
ファイル	ESXiのオフラインバンドルファイル 例）VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip

注意

アップロードしたESXi修正パッチ／オフラインバンドルファイル（zipファイル）は解凍しないでください。解凍した場合には、ローリングアップデートは異常終了します。

6.7.2.7 適用するvCSA修正パッチファイルをデータストアへアップロードする

vCSA修正パッチファイルを適用する場合に必要な作業です。

以下の手順でvCSA修正パッチファイルをvCSAが起動しているホストのデータストアへアップロードしてください。

1. 以下の手順でvCSA修正パッチファイルを格納するフォルダーを作成します。

   vCSA 6.5以前（Flash）の場合：

   a. vSphere Web ClientでvCSAにログインします。

   b. 「トップ」画面から[ホーム]タブ-[ストレージ]-[vsanDatastore]-[ファイル]タブを選択します。

   c. [新規フォルダの作成]を選択して、vCSA修正パッチファイルを格納するフォルダーを作成します。

d. [＜作成したフォルダー＞]を確認します。

ポイント

フォルダーはvSphere Web Clientから、以下の2種類の名前で表示されます。

- 名前
- 分かりやすい名前

作成時に入力した名前は「分かりやすい名前」で確認できます。

それに紐づく「名前」に表示される値を記録してください。

vCSA 6.7以降（HTML5）の場合：

a. vSphere ClientでvCSAにログインします。

b. 「トップ」画面から[ショートカット]-[ストレージ]-[vsanDatastore]-[ファイル]タブを選択します。

c. [新規フォルダの作成]を選択して、vCSA修正パッチファイルを格納するフォルダーを作成します。

d. [＜作成したフォルダー＞]を確認します。

ポイント

- vCSA 6.7U3以前の場合：

  フォルダーはvSphere Clientから、以下の2種類の名前で表示されます。

  - 名前
  - 分かりやすい名前

  作成時に入力した名前は「分かりやすい名前」で確認できます。

  それに紐づく「名前」に表示される値を記録してください。

- vCSA 7.0以降の場合：

  作成後の「パス」欄に表示される値を記録してください。

2. Host Clientを使用して、vCSAが起動しているホストのESXiにログインします。
3. 「トップ」画面から[ナビゲータ]-[ストレージ]-[データストア]タブ-[vsanDatastore]を選択して、[データストアブラウザ]を選択します。

   「データストアブラウザ」画面が表示されます。
4. 手順dで確認した「名前」または「パス」と同じ値のフォルダー名を選択します。
5. [アップロード]を選択して、vCSA修正パッチファイルをアップロードします。

6.7.2.8 適用するvCSA修正パッチファイルをvCSAにマウントする

vCSA修正パッチファイルを適用する場合に必要な作業です。

以下の手順でvCSA修正パッチファイルをvCSAにマウントしてください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]-[＜vCSA名＞]-[設定]を選択します。
3. [設定]-[仮想マシンのハードウェア]-[編集]を選択します。
4. 表示された「設定の編集」画面で、[仮想ハードウェア]タブ-[CD/DVDドライブ1]-[データストアISOファイル]を選択して、[接続中]にチェックを付けます。

5. [CD/DVD ドライブ1]-[CD/DVDメディア]-[参照]を選択してvCSA修正パッチファイルをマウントします。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]-[＜vCSA名＞]-[サマリ]を選択します。
3. [サマリ]-[仮想マシンのハードウェア]-[設定の編集]を選択します。
4. 表示された「設定の編集」画面で、[仮想ハードウェア]タブ-[CD/DVD ドライブ1]-[データストアISOファイル]を選択して、[接続中]にチェックを付けます。
5. [CD/DVD ドライブ1]-[CD/DVDメディア]-[参照]を選択してvCSA修正パッチファイルをマウントします。

6.7.2.9 適用するvCSAアップグレードファイルをISM-VAへアップロードする

vCSAアップグレードファイルを適用する場合に必要な作業です。

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、vCSAアップグレードファイルをアップロードしてください。

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、『解説書』の「3.7 仮想ディスクの割当て」を参照してください。

表6.8 アップロードするvCSAアップグレードファイルとディレクトリー

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/vCSA
ファイル	vCSAアップグレードファイル 例）VMware-VCSA-all-6.7.0-10244745.iso

6.7.2.10 ファームウェアアップデートの対象ノードを選定する

対象ノードの選定は、「6.7.1 動作要件」を参照して、動作要件を満たしているノードを選定してください。

6.7.2.11 仮想マシンの退避用ノードを選定する

退避ノードの選定は、「6.7.1 動作要件」を参照して、動作要件を満たしている退避ノードを選定してください。

ポイント

PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成でDRS機能がオンの場合には、退避ノードの準備は不要です。DRS機能は、以下の手順で確認できます。

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定]-[サービス]-[vSphere DRS]で確認できます。

vCSA 6.7以降（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定 [注]]-[サービス]-[vSphere DRS]で確認できます。

   [注]：vCSA 7.0 U3以降の場合、[構成]と表示されます。

6.7.2.12 ファームウェアアップデートに必要な準備作業を実施する

ファームウェアアップデートを行う場合のみ必要になる手順です。

『解説書』の「2.6.3.1 アップデート方法」を参照し、Offlineアップデートに関する留意事項の確認と準備作業を実施してください。

ポイント

ローリングアップデート機能では、PXEブートで使用する管理LANの設定は任意です。設定しない場合、プロファイルの「管理LANネットワークポート設定」で指定したポートをPXEブート時に使用します。他のポートを使用する場合は、『解説書』の「2.6.3.1 アップデート方法」の「Offlineアップデートに必要な準備作業」を参照して設定してください。

6.7.2.13 ESXiの修正パッチ／オフラインバンドルの注意事項を確認し必要に応じて対処する

ESXiの修正パッチやオフラインバンドルには、制限事項や注意事項がある場合があります。

1. 制限留意や注意事項を確認します。

   『VMware vSphere X.X ソフトウェア説明書』(Xには、バージョンが入ります。)で注意事項の有無を確認してください。
   https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

   制限留意や注意事項がない場合は、以降の作業は不要です。

2. 制限留意や注意事項がある場合、対処を実施します。

   注意事項の内容を確認し、以下のいずれかを実施してください。

   ー 手動での対処

   注意事項の内容に従い、ローリングアップデート実行前および実行後に、手動で対処内容を実施します。

   ー スクリプトでの対処

   注意事項の対処は、スクリプトによってローリングアップデート機能の実行中に対応できます。
   注意事項の対処内容を確認し、スクリプトを作成してください。

   スクリプトの作成方法およびスクリプト例は、『解説書』の「付録G PRIMEFLEX HS／PRIMEFLEX for VMware vSANのローリングアップデートで実行するスクリプト」を参照してください。

   スクリプトを作成した場合、以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、スクリプトをアップロードしてください。

表6.9 アップロードするスクリプトとディレクトリー

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/script
ファイル	・適用前に実行するスクリプトの場合 pre_script.sh ・適用時に実行するスクリプトの場合 post01_script.sh ・適用時に実行するスクリプトの場合 post02_script.sh

ポイント

ポストスクリプト内で使用するオフラインバンドルは「6.7.2.6 適用するESXiの修正パッチ／オフラインバンドルファイルをISM-VAへアップロードする」を参照してISM-VAへアップロードしてください。オフラインバンドル以外に使用するファイルがある場合には、以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、アップロードしてください。

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/other
ファイル	その他のファイル

6.7.3 ローリングアップデートを実行する

ローリングアップデート機能を実行することで仮想化基盤にファームウェア、ESXi修正パッチ／オフラインバンドル、vCSA修正パッチ／アップグレードをローリングアップデートします。

ローリングアップデート機能を実行前に「6.7.1 動作要件」を参照して、動作要件を必ず確認してください。

ISM for PRIMEFLEXのローリングアップデート機能の実行手順について説明します。

ポイント

ローリングアップデート機能を実行する前に、以下の「仮想化管理ソフトウェアからの情報取得」と「クラスタ情報の取得と更新」を実行してください。

- 仮想化管理ソフトウェアからの情報取得を行う

  ISM GUI上に仮想化管理ソフトウェアからの情報を取得し、表示内容を最新化します。

  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. [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。

     情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10021503」のログが出力されます。

  詳細については、『解説書』の「2.13.6.2 仮想化管理ソフトウェアからの情報取得」を参照してください。

- 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。

  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ます。

  詳細については、『解説書』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。

注意

- ISM for PRIMEFLEXの他の機能が実行中にローリングアップデート機能を実行しないでください。ローリングアップデート機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

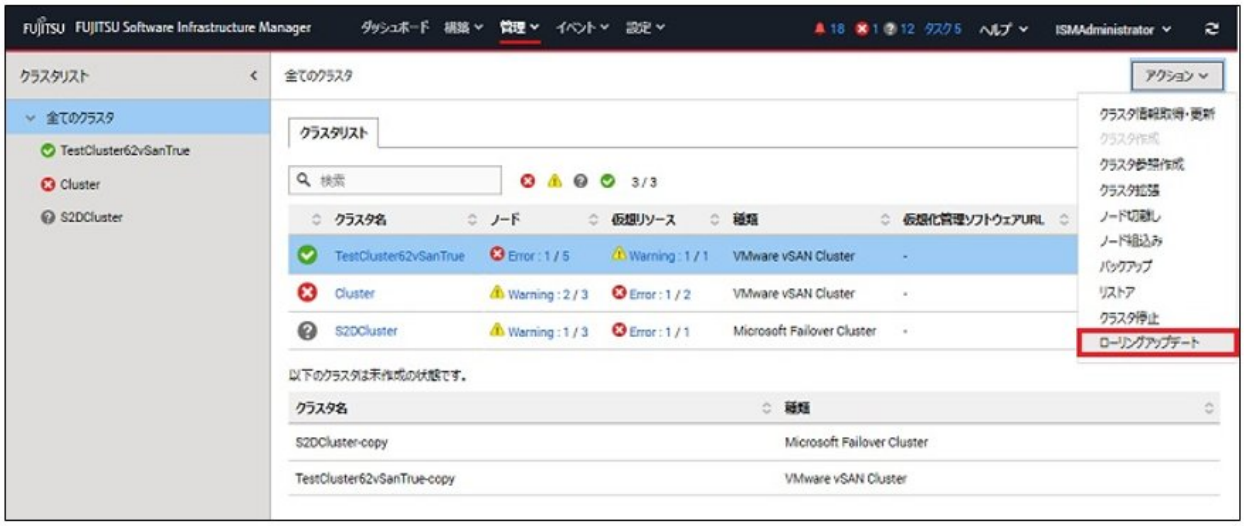
  ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

- PRIMEFLEX HS／PRIMEFLEX for VMware vSANの3台構成でローリングアップデート機能を実行中は、可用性、冗長性が低下しています。そのため、ローリングアップデート実行中ではないホストで障害が発生すると、システムが復旧できなくなる可能性があります。

1. ISM管理者（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。
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[ローリングアップデート]を選択します。

   PRIMEFLEX HS／PRIMEFLEX for VMware vSANの場合



「ローリングアップデート」ウィザードが表示されます。

以降の手順で動作オプションを選択します。

ポイント

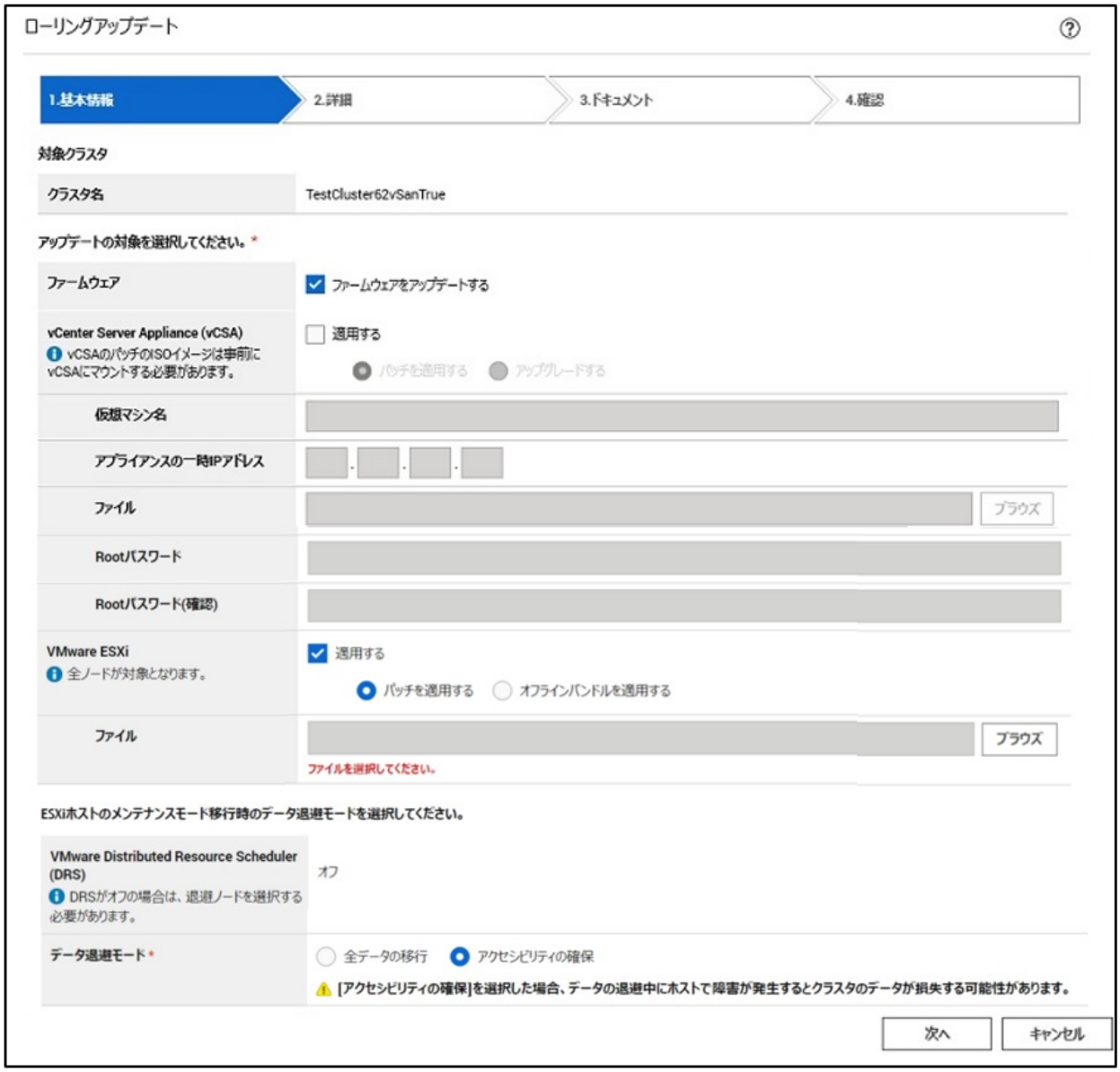
「クラスタリスト」画面のアップデートステータスが[最新ファームウェアあり]となっているクラスタのみ、ファームウェアをローリングアップデートできます。

実行条件を満たしていない場合、以下の「結果」画面が表示されます。メッセージを確認して実行条件を満たすように対処して、再実行してください。実行条件の詳細は「6.7.1 動作要件」を参照してください。

4. 「1.基本情報」画面でローリングアップデートのための基本情報を設定し、[次へ]ボタンを選択します。

   3台構成でローリングアップデート機能を実行する場合、データ退避モードは「アクセシビリティの確保」を選択してください。
   再実行の場合、再設定が不要であれば、[次へ]ボタンを選択して、手順5に進んでください。

PRIMEFLEX HS／PRIMEFLEX for VMware vSANの場合



ポイント

- アップデート対象として[VMware ESXi]を選択した場合は、すべてのノードが対象ノードとなります。システムの構成やクラスタの設定などの関係やライセンスの関係で、他ノードへ移動できない仮想マシンを実行している場合、それらの仮想マシンを手動で停止してください。
- アップデート対象として[vCenter Server Appliance (vCSA)]-[アップグレードする]を選択した場合は、以下のように入力してください。
  - 仮想マシン名は、既存vCSAの仮想マシン名を指定します。

    アップグレード後のvCSAの仮想マシン名は、＜既存vCSAの仮想マシン名＞-newとなります。
  - アプライアンスの一時IPアドレスは、既存のvCSAと同じネットワークのIPアドレスを指定します。
  - Rootパスワードは、既存vCSAのRootパスワードを指定します。

    アップグレード後のvCSAのパスワードも同じになります。

ー DRS機能がオンの場合、仮想マシンはDRS機能で移行されるためローリングアップデート後はクラスタ内の元のサーバーに戻らないことがあります。必要に応じて、ローリングアップデート機能実行完了後、仮想マシンを元のサーバーに戻してください。

注意

ー vCSAのアップグレード後はローカルアカウントユーザーが引き継がれません。「6.7.4.4 vCSAのバージョンを確認する」でローカルアカウントユーザーの追加が必要となります。

https://kb.vmware.com/s/article/78148

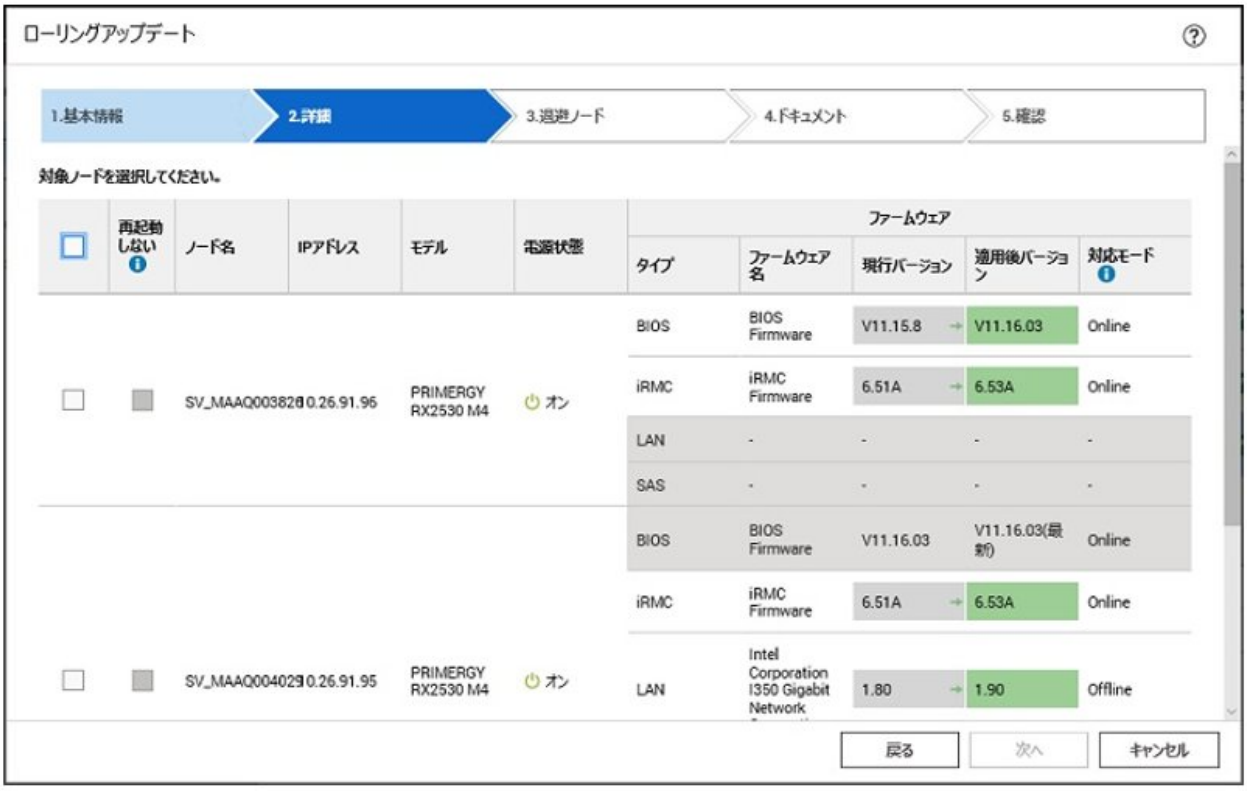
ー vCSA 7.0以前からvCSA 7.0 U1以降にアップグレードまたはパッチ適用する場合、アップデート対象は[vCenter Server Appliance (vCSA)]のみ選択し、[ファームウェア]や[VMware ESXi]を選択しないでください。

vCSA 7.0以前からvCSA 7.0 U1以降にアップグレードまたはパッチ適用すると、「6.7.4.9 vCLS仮想マシンのデータストアを確認して移動する」の手順が必要となります。

この手順を実施する前にアップデート対象に[vCenter Server Appliance (vCSA)]以外の項目が選択されていると退避ノードへのvCLS仮想マシン移行でエラーが発生し、ローリングアップデートに失敗します。

5. アップデート対象として[ファームウェア]を選択した場合に必要になる手順です。[ファームウェア]を選択しなかった場合は、手順6に進んでください。
「2.詳細」画面でファームウェアをローリングアップデートする対象ノードと[再起動しない]の有無を選択し、[次へ]ボタンを選択します。

再実行の場合、対象ノードと[再起動しない]の設定が不要であれば、[次へ]ボタンを選択して、手順6に進んでください。



注意

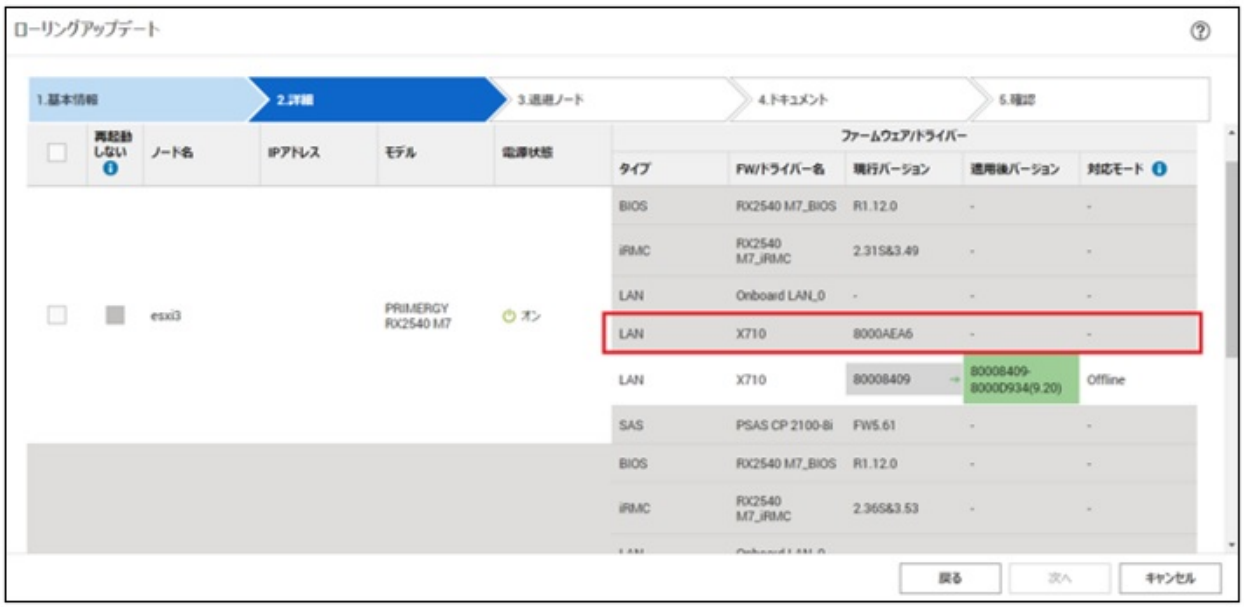
ー iRMCのファームウェアアップデートは、ノードの再起動が不要です。「2.詳細」画面で選択したファームウェアアップデート対象ノードの[再起動しない]にチェックを付けることで、再起動しない設定ができます。

ー BIOSファームウェアアップデートは、「2.詳細」画面で選択したファームウェアアップデート対象ノードの[再起動しない]のチェックを外してください。再起動できないノードがある場合は、[再起動しない]にチェックを付けて、ファームウェアのローリングアップデート実行後に手動で再起動してください。

ー 下記のIntel製カードに該当するものが2種類以上ある場合、「2.詳細」画面の[タイプ]と[FW/ドライバー名]が、一部、アップデート非対象を表すグレー表示(赤枠部)となります。ただし、ローリングアップデート自体は正常に実行されます。

[対象カード]

- PLAN EP X710-T2L 2x10GBASE-T PCIE LP
- PLAN EP X710-T2L 2x10GBASE-T OCPv3
- PLAN EP X710-DA4 2x10Gb SFP+ LP
- PLAN EP X710-DA2 2X 10G SFP OCPv3
- PLAN EP XXV710-DA2 25G 2p SFP28 LP
- PLAN EP XXV710-DA2 2p SFP28 OCP
- PLAN EP E810-XXDA2 2X 25G SFP28 PCIe LP
- PLAN EP E810-XXDA2 2X 25G SFP28 OCPv3

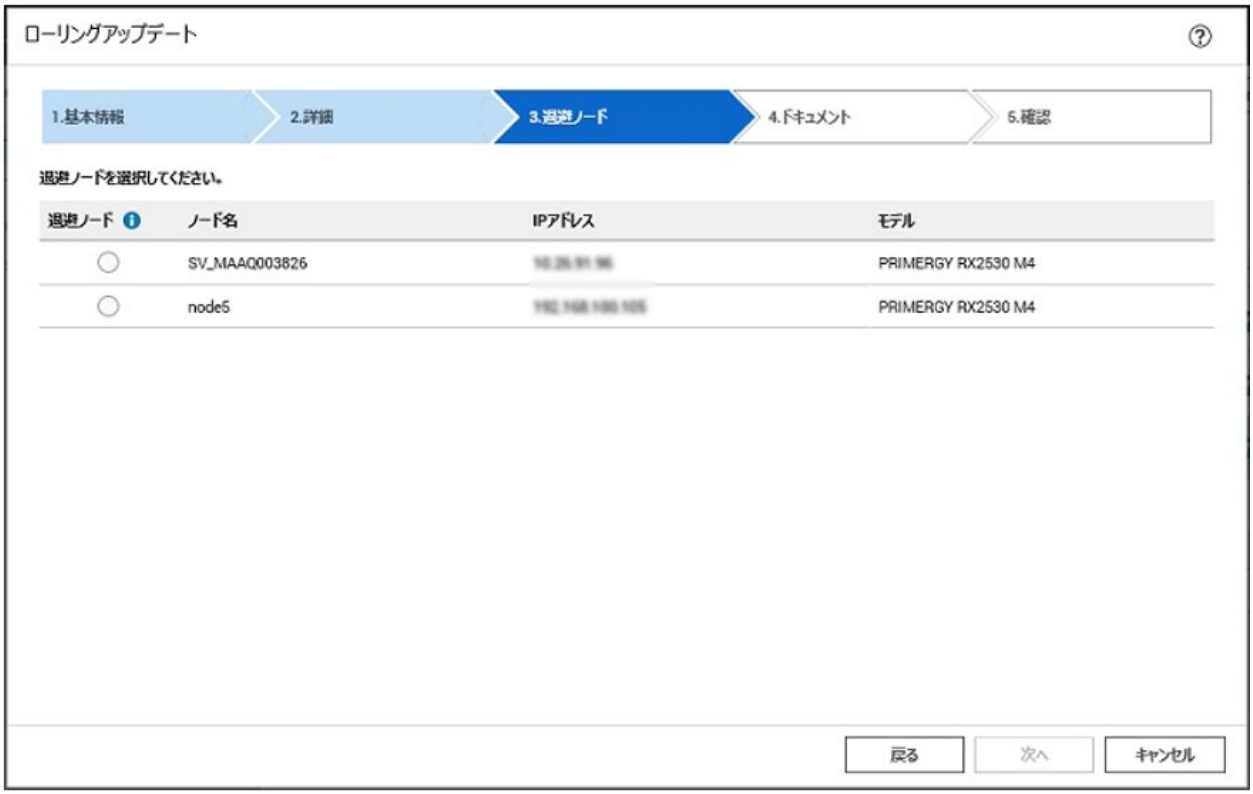


ローリングアップデートを実行後、ファームウェアアップデートの結果を確認してください。確認方法については、「6.7.4.1 ファームウェアアップデートを確認する」を参照してください。

ISMのイベントログを確認し、エラーが発生している場合、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

6. 「3.退避ノード」画面で退避ノードを選択し、[次へ]ボタンを選択します。

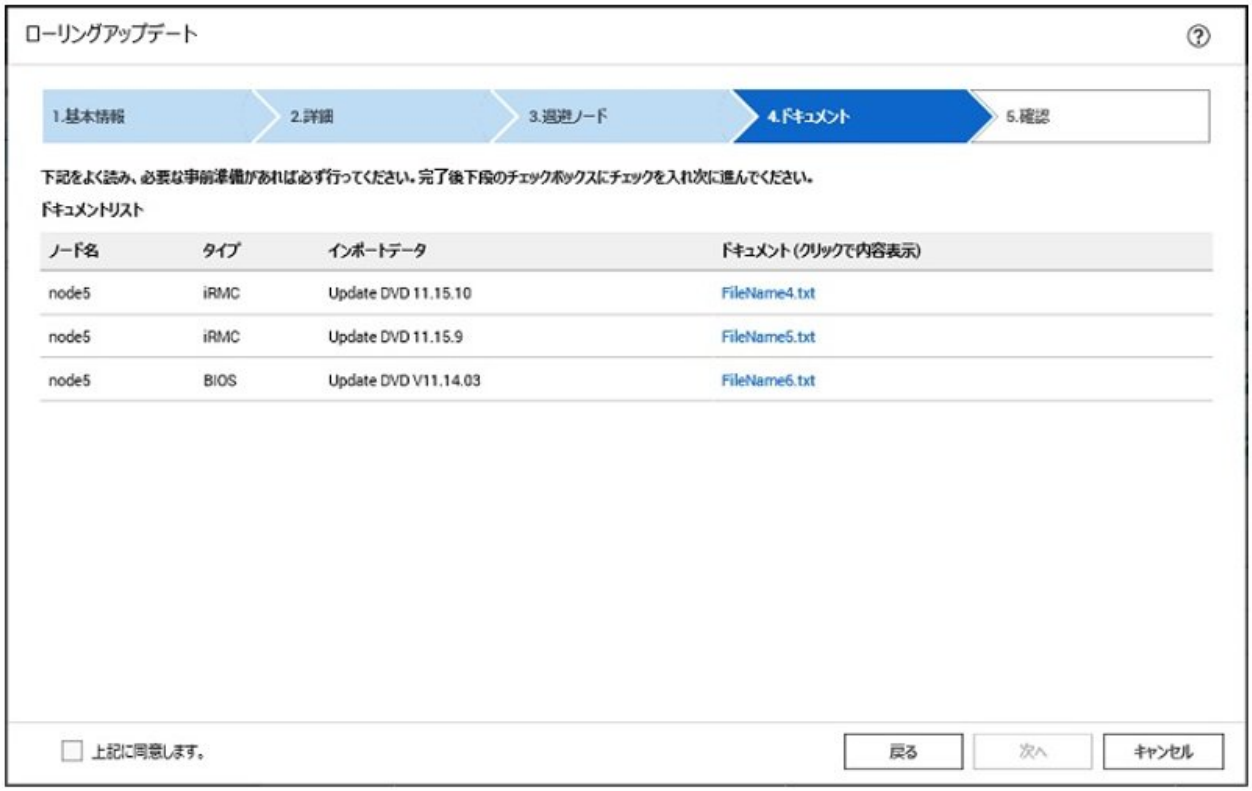
   再実行の場合、退避ノードの再選択が不要であれば、[次へ]ボタンを選択して、手順7に進んでください。



ポイント

「3.退避ノード」画面は、対象クラスタがPRIMEFLEX HS／PRIMEFLEX for VMware vSANでDRS機能がオンの場合は表示されません。手順7に進んでください。DRS機能がオンかオフかは、手順4の「1.基本情報」画面で確認できます。

7. 「3.ドキュメント」画面、または「4.ドキュメント」画面で適用するファームウェアのドキュメントを確認後、[上記に同意します。]にチェックを付け、[次へ]ボタンを選択します。

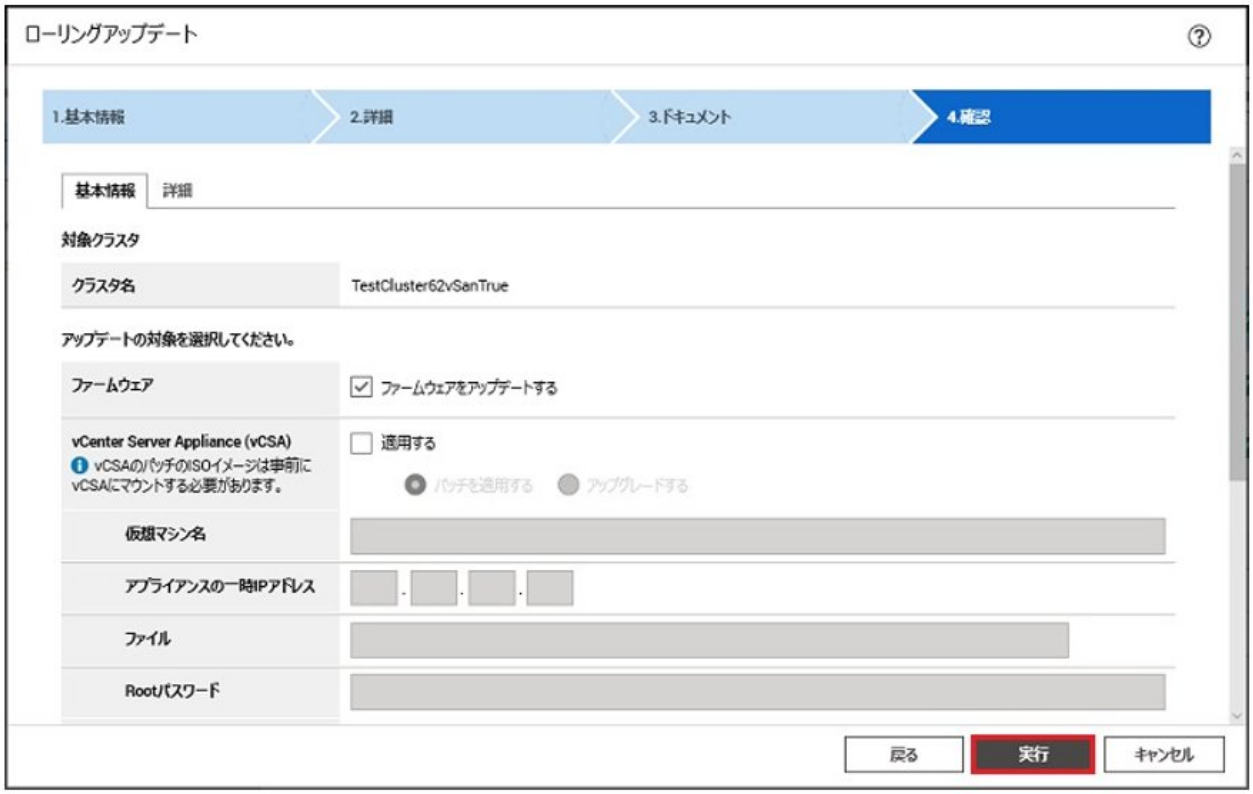


ポイント

「3.ドキュメント」画面は、対象クラスタがPRIMEFLEX HS／PRIMEFLEX for VMware vSANで「1.基本情報」のアップデート対象として[ファームウェア]を選択しない場合は表示されません。手順8に進んでください。

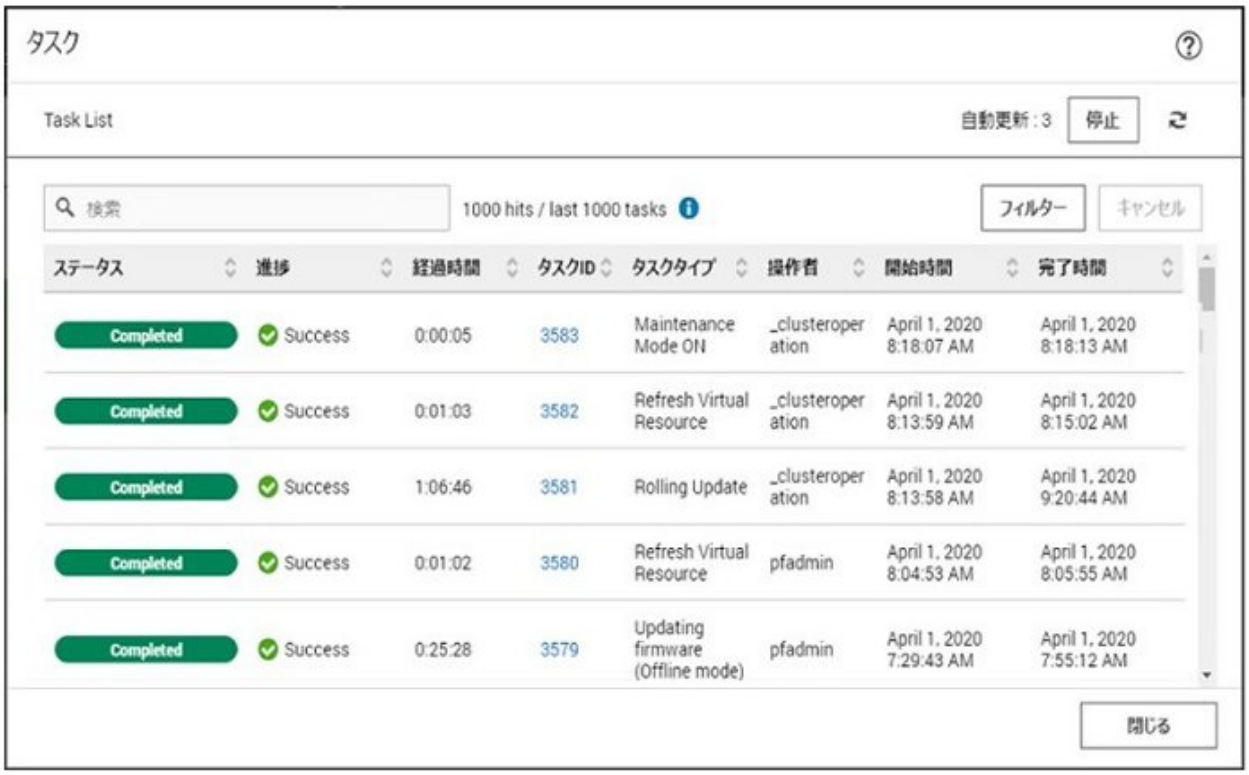
8. 「4.確認」画面、または「5.確認」画面で各設定を確認し、[実行]ボタンを選択します。

PRIMEFLEX HS／PRIMEFLEX for VMware vSANの場合



ローリングアップデートの実行は、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「Rolling Update」となっているのが、ローリングアップデートのタスクです。



ポイント

「タスク」画面のタスクリストから「Rolling Update」の[タスクID]を選択すると、「Rolling Update」の「タスク」画面が表示されます。この画面では、ローリングアップデート時にファームウェアアップデート対象ノード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。

9. 「Rolling Update」のステータスが「完了」になったことを確認します。

注意

すべての構成で共通の注意事項

- ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  問題が解決できたらローリングアップデート機能を再実行してください。

- BIOSのローリングアップデート実行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、再実行するとエラー終了します。再起動待ち状態かどうかは、以下の手順でアップデートされているか確認してください。アップデートされていない場合は、手動で再起動を実行してアップデートを完了させてください。アップデートされている場合は、対処不要です。

  1. ISM管理者（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。
  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、「クラスタリスト」画面を表示します。
  3. [＜対象のクラスタ＞]-[ノードリスト]タブから対象ノードのノード名を選択し、ノードの詳細画面を表示します。
  4. [ファームウェア/ドライバー]タブで[アクション]-[ノード情報取得]を選択します。

     ファームウェア情報が更新されます。
  5. 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ないことを確認します。

- ファームウェア管理機能のファームウェアアップデート処理がエラー終了したノードがあっても、クラスタのステータスが正常であれば、アップデートが正常に完了したノードに対しては再起動が実行され、ファームウェアが適用されます。

- ローリングアップデート機能では、ファームウェアアップデート対象ノードを再起動するように「ローリングアップデート」ウィザードで設定すると、ファームウェアアップデート後に対象ノードが再起動します。対象ノードの再起動が始まると一時的にクラスタから切断されるため、クラスタに異常が発生しますが、再起動が完了するとクラスタのステータスは正常に回復します。ローリング

アップデート機能では、再起動後にクラスタのステータスを確認しており、クラスタのステータスが正常に回復しない場合は、エラー終了します。

ただし、PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成の場合、クラスタのステータスが更新されるタイミングによっては、クラスタのステータスが異常から正常に回復するまで6時間以上かかることがあります。クラスタのステータスが正常に回復しない場合、以下の手順で再テストを実行して正常に回復することを確認してください。

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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] で再テストを実行します。

vCSA 6.7以降（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[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[注]]で再テストを実行します。

   [注]：vCSA 7.0以降の場合、[Skyline健全性]または[Skyline Health]と表示されます。

再テストを実行しても正常に回復しない場合は、保守資料を採取して、当社技術員に連絡してください。

― 以下のメッセージが表示されエラー終了した場合、ファームウェアアップデートは成功している可能性があります。

```
50215410：ローリングアップデートの実行に失敗しました。ローリングアップデートタスクの検証処理でエラーが発生しました。
(Cluster status is abnormal; cluster name = xxxx; cluster status = YELLOW; detail code = E201003)
```

以下の手順で確認してください。ファームウェアアップデートが成功している場合は、対処不要です。

1. ISM管理者（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。
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、「クラスタリスト」画面を表示します。
3. [＜対象のクラスタ＞]-[ノードリスト]タブから対象ノードのノード名を選択し、ノードの詳細画面を表示します。
4. [ファームウェア/ドライバー]タブで[アクション]-[ノード情報取得]を選択します。

   ファームウェア情報が更新されます。
5. 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を確認します。

― 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。

― ISMのイベントログに以下のメッセージが出力される場合がありますが、無視してください。

```
仮想化管理ソフトウェア情報の取得に失敗しました。対象外または存在しない仮想化管理ソフトウェア情報が指定されました。
（メッセージID ： 50170511）
```

― ローリングアップデート機能実行中に、ISMのイベントログに以下のメッセージが出力される場合がありますが、無視してください。

```
ノード情報(OS)の再取得に失敗しました。 ESXiへのログインに失敗しました(IPアドレス=xxx.xxx.xxx.xxx,ポート番号=xxx)。
IPアドレス、ポート番号、ネットワーク設定のいずれかが不正です。 IPアドレス、ポート番号の指定が正しいことを確認してください。また、ネットワーク設定が正しいことを確認してください。
（メッセージID ： 50020385）
```

― 「タスク」画面のタスクリストで「Refresh Virtual Resource」のタスクが以下のメッセージを出力してエラーする場合がありますが、無視してください。

```
HTTPError Catched. ServerConnectionError ResponceMessage: (50975051 : An internal error that cannot be caught has occurred.)
```

― ローリングアップデートの実行に失敗した場合、その状態でクラスタ定義パラメーターの修正を行わないでください。ローリングアップデートを完了してからクラスタ定義パラメーターを修正してください。

PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成に対しての注意事項

- ESXi修正パッチ／オフラインバンドルの適用処理がエラー終了したノードがあっても、クラスタのステータスが正常であれば、パッチ／オフラインバンドルの適用が正常に完了したノードに対しては再起動が実行され、ESXi修正パッチ／オフラインバンドルが適用されます。
- ESXiの修正パッチ／オフラインバンドルを適用した場合は、vSANディスクフォーマットのバージョンを必要に応じてアップデートしてください。

  例）ESXiの修正パッチ／オフラインバンドルを適用した後にクラスタ拡張を実行する場合
- ESXiの修正パッチ／オフラインバンドルを適用し、ISMの「タスク」画面にエラーが表示された場合は、「6.7.4.2 ESXiのバージョンを確認する」と「6.7.4.3 スクリプトの実行結果を確認する」を参照して、ESXiのバージョンとスクリプトの実行結果を確認してください。

  ESXiのバージョンがESXiの修正パッチ／オフラインバンドルを適用したバージョンになっている場合、かつスクリプトの実行結果が正常な場合は、アップデート対象からESXiを外してローリングアップデート機能を再実行してください。
- vCSA修正パッチを適用またはvCSAアップグレードし、ISMの「タスク」画面にエラーが表示された場合は、「6.7.4.4 vCSAのバージョンを確認する」を参照して、vCSAのバージョンを確認してください。

  vCSAのバージョンがvCSA修正パッチを適用またはvCSAアップグレードしたバージョンになっている場合は、アップデート対象からvCSAを外してローリングアップデート機能を再実行してください。vCSA修正パッチを適用またはvCSAアップグレードを単体で実施した場合は対処不要です。
- ローリングアップデート機能では、アップデート対象ノードを再起動するため、ESXiホストをVMwareのメンテナンスモードに設定します。メンテナンスモードの設定に失敗した場合、成功するまで複数回VMwareのメンテナンスモードの設定を行います。そのため、VMwareのメンテナンスモードの設定が完了するまで8時間以上かかる場合があります。
  メンテナンスモードの設定に失敗していることは、ISMの「タスク」画面のタスクリストで「MaintenanceMode ON」のタスクに以下のエラーメッセージが出力されていることで確認できます。

```
HTTPError Catched. OperationError ResponceMessage: (50976211 : Execution failed. Execution of maintenancemodeon
is not capable under this condition. (maintenancemodeon com.vmware.vim25.Timedout Operation timed out.))
```

6.7.4 事後処理

ISM for PRIMEFLEXのローリングアップデートの事後処理について説明します。

6.7.4.1 ファームウェアアップデートを確認する

以下の手順でファームウェアアップデートを確認してください。

1. ISM管理者（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。
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]-[ファームウェア/ドライバー]を選択します。
3. 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。

   a. 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を確認します。

      [再起動しない]にチェックを付けたノード以外のすべてのファームウェアが適用されている場合、手順4に進んでください。

   b. [再起動しない]にチェックを付けたノード以外の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、『解説書』の「付録F 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。

      - 「ローリングアップデート」ウィザードから設定を変更して、ローリングアップデート機能を再実行します。
      - 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/ドライバー]を選択します。

        画面左側のメニューから[アップデート]を選択します。

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/ドライバー更新]を選択します。

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。

注意

PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成では、ローリングアップデート実行完了後にアラーム定義の設定を元に戻した場合、以下の健全性エラーが発生する可能性があります。以下のKBを参照して対処してください。

ー vSANディスクバランス

https://kb.vmware.com/s/article/2144278?lang=ja

5. 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。

6.7.4.2 ESXiのバージョンを確認する

以下の手順でESXiのバージョンを確認してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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＞]-[＜ホスト名＞]-[サマリ]を選択します。

   「ハイパーバイザー」にESXiのバージョンが表示されます。
3. 「6.7.3 ローリングアップデートを実行する」の手順4で設定したESXi修正パッチ／オフラインバンドルファイルのバージョンになっていることを確認します。

   ESXi修正パッチ／オフラインバンドルの適用に失敗している場合は、『ISM for PRIMEFLEX メッセージ集』の「3.3 ローリングアップデートエラー時の対処例」を参照して、対処してください。問題が解決しない場合は、保守資料を採取して、当社技術員に連絡してください。

   ESXi修正パッチ／オフラインバンドルの適用に成功している場合は、対処不要です。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]-[＜ホスト名＞]-[サマリ]を選択します。

   「ハイパーバイザー」にESXiのバージョンが表示されます。
3. 「6.7.3 ローリングアップデートを実行する」の手順4で設定したESXi修正パッチ／オフラインバンドルファイルのバージョンになっていることを確認します。

   ESXi修正パッチ／オフラインバンドルの適用に失敗している場合は、『ISM for PRIMEFLEX メッセージ集』の「3.3 ローリングアップデートエラー時の対処例」を参照して、対処してください。問題が解決しない場合は、保守資料を採取して、当社技術員に連絡してください。

   ESXi修正パッチ／オフラインバンドルの適用に成功している場合は、対処不要です。

注意

ESXi修正パッチ／オフラインバンドルの適用が正常に完了したにも関わらず、想定しているESXiのバージョンが確認できない場合、「ローリングアップデート」ウィザードで指定したESXiパッチファイルが誤っている可能性があります。ESXi修正パッチ／オフラインバンドルファイルの指定を確認してローリングアップデート機能を再実行してください。

6.7.4.3 スクリプトの実行結果を確認する

「6.7.2.13 ESXiの修正パッチ／オフラインバンドルの注意事項を確認し必要に応じて対処する」で作成したスクリプトの実行結果を出力したログなどで確認してください。

スクリプトの実行に成功していた場合は、ログファイルに以下のメッセージが出力されています。

適用前に実行するスクリプト（例：/scratch/log/pre_script.log）に以下のメッセージが出力されます。

```
pre_script End
```

適用時に実行するスクリプト（例：/scratch/log/post01_script.log）に以下のメッセージが出力されます。

```
post01_script End
```

適用後に実行するスクリプト（例：/scratch/log/post02_script.log）に以下のメッセージが出力されます。

```
post02_script End
```

スクリプトの実行に失敗していた場合は、スクリプトのログを確認してエラーの対処をしてください。エラーの対処後にスクリプトの内容を手動で実行して、『VMware vSphere X.X ソフトウェア説明書』（Xには、バージョンが入ります。）の注意事項の対処を完了させてください。

注意事項の対処は、以下のサイトを参照して、『VMware vSphere X.X ソフトウェア説明書』に記載されている手順を実行してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

6.7.4.4 vCSAのバージョンを確認する

以下の手順でvCSAのバージョンを確認してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCenter Serverを選択し、[サマリ]タブを選択します。

   「バージョン情報」にvCSAのバージョンが表示されます。
4. 「6.7.3 ローリングアップデートを実行する」の手順4で設定したvCSA修正パッチファイルまたはvCSAアップグレードファイルのバージョンになっていることを確認します。

   vCSA修正パッチの適用またはvCSAアップグレードに失敗している場合は、『ISM for PRIMEFLEX メッセージ集』の「3.3 ローリングアップデートエラー時の対処例」の「対処例18」と「対処例19」を参照して、対処してください。問題が解決しない場合は、保守資料を採取して、当社技術員に連絡してください。
5. vCSAアップグレードした場合、以下の手順でローカルアカウントユーザーを追加してください。
   a. vSphere Web ClientでvCSAにログインします。
   b. 「トップ」画面から[ホーム]タブ-[インベントリ]- [ホストおよびクラスタ]-[＜vCSA名＞]-[権限]を選択します。
   c. ローカルアカウントユーザーの名前を確認します。

      表示されているローカルアカウントユーザーは、実際には引き継がれてないため、以降の操作により追加してください。
   d. vCSAにrootユーザーでSSH接続します。
   e. 以下のコマンドを実行します。

      ```
      Command>localaccounts.user.add --role admin --username ＜手順cで確認したユーザー名＞ --password
      Enter password:＜パスワード＞
      Reenter password:＜パスワード＞
      Command>
      ```
   f. すべてのローカルユーザーアカウントに対して、手順5のa～eを実施してください。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCenter Serverを選択し、[サマリ]タブを選択します。

   「バージョン」にvCSAのバージョンが表示されます。
4. 「6.7.3 ローリングアップデートを実行する」の手順4で設定したvCSA修正パッチファイルまたはvCSAアップグレードファイルのバージョンになっていることを確認します。

   vCSA修正パッチの適用またはvCSAアップグレードに失敗している場合は、『ISM for PRIMEFLEX メッセージ集』の「3.3 ローリングアップデートエラー時の対処例」の「対処例18」と「対処例19」を参照して、対処してください。問題が解決しない場合は、保守資料を採取して、当社技術員に連絡してください。
5. vCSAアップグレードした場合、以下の手順でローカルアカウントユーザーを追加してください。
   a. vSphere ClientでvCSAにログインします。
   b. 「トップ」画面から[ショートカット]-[インベントリ]- [ホストおよびクラスタ]-[＜vCSA名＞]-[権限]を選択します。
   c. ローカルアカウントユーザーの名前を確認します。

      表示されているローカルアカウントユーザーは、実際には引き継がれてないため、以降の操作により追加してください。
   d. vCSAにrootユーザーでSSH接続します。
   e. 以下のコマンドを実行します。

```
Command>localaccounts.user.add --role admin --username ＜手順cで確認したユーザー名＞ --password
Enter password:＜パスワード＞
Reenter password:＜パスワード＞
Command>
```

   f. すべてのローカルユーザーアカウントに対して、手順5のa～eを実施してください。

ポイント

- vCSA 7.0U2以降はパスワードポリシーが変更されているため、以前お使いのパスワードが使用できない場合があります。その場合、別のパスワードに変更してローカルアカウントユーザーを追加してください。
- vSphere Web Client／vSphere Clientのサポート対象のWebブラウザーをご確認ください。
  - vCSA 6.5

    https://docs.vmware.com/jp/VMware-vSphere/6.5/com.vmware.vsphere.upgrade.doc/GUID-F6D456D7-C559-439D-8F34-4FCF533B7B42.html
  - vCSA 6.7

    https://docs.vmware.com/jp/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-EC80836B-BE02-4CB2-9F40-15928AFB6E20.html
  - vCSA 7.0

    https://docs.vmware.com/jp/VMware-vSphere/7.0/com.vmware.vcenter.install.doc/GUID-EC80836B-BE02-4CB2-9F40-15928AFB6E20.html

6.7.4.5 OS情報の更新を行う

ESXiオフラインバンドルの適用を行った場合に必要な作業です。

以下の手順でOS情報の更新を行ってください。

ISM GUI上でOS情報を更新し、表示内容を最新化します。

詳細については、『解説書』の「2.2.1.5 ノードのOS情報の登録」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]-[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、[OS]タブを選択します。

3. [OSアクション]ボタンから[OS情報編集]を選択します。

   [OSバージョン]に「Auto」を選択している場合、手順4は不要です。手順5に進んでください。

4. [OSバージョン]の情報を入力し、適用します。

5. [アクション]ボタンから[ノード情報取得]を選択します。

   ノード情報取得が完了すると、[イベント]-[イベント]-[運用ログ]にメッセージID「10020303」のログが出力されます。

6. [更新]ボタンを選択して、[OS]タブの表示を更新します。

7. [OS]タブ画面から[OSからの取得情報]の[版数]を確認して、「6.7.3 ローリングアップデートを実行する」の手順4で設定したESXi修正パッチ／オフラインバンドルファイルのバージョンになっていることを確認します。

   ESXi修正パッチ／オフラインバンドルの適用に失敗している場合は、『ISM for PRIMEFLEX メッセージ集』の「3.3 ローリングアップデートエラー時の対処例」を参照して、対処してください。問題が解決しない場合は、保守資料を採取して、当社技術員に連絡してください。

   ESXi修正パッチ／オフラインバンドルの適用に成功している場合は、対処不要です。

6.7.4.6 仮想化管理ソフトウェア情報の更新を行う

vCSAアップグレードを行った場合に必要な作業です。

以下の手順で仮想化管理ソフトウェア情報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[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. vCSAアップグレードを行った仮想化管理ソフトウェアを選択し、[アクション]ボタンから[編集]を選択します。

4. 「仮想化管理ソフトウェア編集」画面で、vCSAアップグレードを行った仮想化管理ソフトウェアのバージョンに更新して、パスワードを入力します。

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」画面が表示されます。編集した仮想化管理ソフトウェアの[タイプ]が更新されて表示されます。

6.7.4.7 適用したvCSA修正パッチファイルをvCSAからアンマウントする

vCSA修正パッチファイルを適用した場合に必要な作業です。

以下の手順でvCSA修正パッチファイルをvCSAにからアンマウントしてください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。

2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]-[＜vCSA名＞]-[設定]を選択します。

3. [設定]-[仮想マシンのハードウェア]-[編集]を選択します。

4. 表示された「設定の編集」画面で、[仮想ハードウェア]タブ-[CD/DVDドライブ1]-[データストアISOファイル]を選択して、[接続中]のチェックを外します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。

2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]-[＜vCSA名＞]-[設定]を選択します。

3. [サマリ]-[仮想マシンのハードウェア]-[設定の編集]を選択します。
4. 表示された「設定の編集」画面で、[仮想ハードウェア]タブ-[CD/DVDドライブ1]-[データストアISOファイル]を選択して、[接続中]のチェックを外します。
5. 手順4でアンマウントされない場合、vCSAを再起動します。

6.7.4.8 既存のvCSAを削除する

vCSAアップグレードを行ったあと、必要に応じて既存のvCSAを削除します。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[ディスクから削除]を選択します。
4. 「削除の確認」画面で、[はい]ボタンを選択します。
5. [最近のタスク]に表示されるタスク名[仮想マシンの削除]のステータスが「完了」となることを確認します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[ディスクから削除]を選択します。
4. 「削除の確認」画面で、[はい]ボタンを選択します。
5. [最近のタスク]に表示されるタスク名[仮想マシンの削除]のステータスが「完了」となることを確認します。

6.7.4.9 vCLS仮想マシンのデータストアを確認して移動する

vCSA 7.0 U1以降にアップデートまたはパッチ適用を行った場合に必要な作業です。

vCSAを7.0 U1以降へアップデートまたはパッチ適用するとvSphereクラスタサービス（vCLS）が有効になり、vCLS仮想マシンがクラスタに作成されます。vCLS仮想マシンは、クラスタに最大で3台作成されます。

このvCLS仮想マシンがローカルデータストアに作成された場合は、vSANデータストアへ移動する必要があります。

すべての対象クラスタで実施してください。

ポイント

vCSAにログインするユーザー種別によってはvSphereクラスタサービス（vCLS）が表示されない場合があります。
vSphereクラスタサービス（vCLS）関連の操作を行う際には、vCenter Single Sign-Onドメインの管理者を使用してください。

vCLS仮想マシンが配置されているデータストアの確認手順

vCLS仮想マシンが配置されているデータストアを確認します。

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
   - vCSA 7.0U2以前の場合：

     ＜vCLS名＞は、"vCLS (n)"（nは数字）で表示されます。
   - vCSA 7.0U3以降の場合：

     ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"（Xは16進数）で表示されます。

3. [データストア]-[名前] がvSANデータストア名であることを確認します。

   vSANデータストア名は、ISMのGUIで対象クラスタのクラスタ定義パラメーターの[クラスタ詳細情報]-[ストレージプール]タブの[ストレージプール名]で確認できます。

   vSANデータストア名ではない場合、「vSANデータストアへの移動手順」を実施します。

4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

vSANデータストアへの移動手順

vCLS仮想マシンをvSANデータストアへ移動します。

vCSA 7.0U2以前の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
3. [アクション]-[移行]を選択します。

   確認画面が表示されます。

4. 確認画面で[はい]を選択します。

   「移行」画面が表示されます。

5. [1 移行タイプの選択]で「ストレージのみ変更します」を選択して、[NEXT]ボタンを選択します。
6. [2 ストレージの選択]でvSANデータストアを選択して、[NEXT]ボタンを選択します。

   vSANデータストアは、[タイプ]の「vSAN」で確認できます。

7. [3 設定の確認]で設定内容を確認して、[FINISH]ボタンを選択します。

vCSA 7.0U3以降の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]を選択します。
3. [構成]-[vSphere クラスタ サービス]-[データストア]-[追加]を選択します。

   データストアの追加画面が表示されます。

4. データストアの追加画面でvSANデータストアを選択して、[追加]を選択します。

6.7.4.10 不要なファイルを削除する

ローリングアップデートの完了後は、以下の手順で不要なファイルを削除してください。

(1)ESXiの修正パッチを削除する

ISM-VAに対して実施してください。

1. ISM管理者(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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/patch
ファイル名	「6.7.2.6 適用するESXiの修正パッチ／オフラインバンドルファイルをISM-VAへアップロードする」のESXiの修正パッチファイル

(2)ESXiのオフラインバンドルを削除する

ISM-VAに対して実施してください。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/offlinebundle
ファイル名	「6.7.2.6 適用するESXiの修正パッチ／オフラインバンドルファイルをISM-VAへアップロードする」のESXiのオフラインバンドルファイル

（3）ESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプトを削除する

ISM-VAに対して実施してください。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/script
ファイル名	「6.7.2.13 ESXiの修正パッチ／オフラインバンドルの注意事項を確認し必要に応じて対処する」のESXiの修正パッチ／オフラインバンドル適用前後で実行するスクリプト

6.7.4.11 不一致となっているプロファイルのベリファイステータスを一致させる（iRMC S5のファームウェア版数を3.37P以降にアップデートした場合）

ローリングアップデートでiRMC S5のファームウェア版数を3.37P以降にアップデートした場合、プロファイルの内容とノードの設定内容に差異が生じるため、プロファイルのベリファイステータスが不一致となります。

「3.3.5 適用済みのプロファイルとハードウェア設定を比較する」の「[不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図したものである場合）」を参照してください。

なお、プロファイル編集時は、『ISM for PRIMEFLEX 設定値一覧』の「4.5.3 詳細 - [iRMC]タブ」を参照してください。

6.7.4.12 クラスタ退避モードを解除する

クラスタの退避モードを設定した場合に必要な操作です。

要件が以下を満たす場合、ローリングアップデート機能を実施する前にクラスタの退避モードを設定しています。

- PRIMEFLEX HS／PRIMEFLEX for VMware vSAN構成
- 3台のノード構成
- DRS機能がオフ

クラスタ退避モードを設定したクラスタは、必ず退避モードを解除してください。

クラスタ退避モードの解除手順については、PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』の「vSANクラスタの起動」の「クラスタの退避モードを解除します。」を参照して実施してください。

PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4の『オペレーション＆メンテナンスガイド』入手先：

https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

6.8 PRIMEFLEX HS／PRIMEFLEX for VMware vSANのリソースを増やす

PRIMEFLEX HS／PRIMEFLEX for VMware vSANのリソースを増やすために、クラスタ作成機能またはクラスタ拡張機能を実行します。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

新規クラスタを構成するサーバーまたはクラスタ拡張時に追加するサーバーを以降、「対象サーバー」と表記します。

クラスタ作成またはクラスタ拡張は、以下の作業フローで行います。

表6.10 クラスタ作成またはクラスタ拡張フロー

クラスタ作成またはクラスタ拡張手順		作業内容
1	事前準備	• vCenter ServerのVMware EVC設定 • ADVMの証明書作成 • DNSへホストレコード登録 • DHCPの設定 • ServerView Suite DVDに同梱されるServerView Installation ManagerとOSインストール媒体のISOイメージをISM-VAへインポート • 古いVMware ESXiパッチとVMware ESXiパッチ適用前後で実行するスクリプトの削除 • VMware ESXiパッチのアップロード • VMware ESXiパッチ適用前後で実行するスクリプトの作成 • 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 • ストレージデバイスの確認 • 設置と結線 • iRMCのIPアドレス設定 • BIOSの設定 • ネットワーク表示の確認 • ISMへノード登録
2	クラスタ作成の実行またはクラスタ拡張の実行	
3	事後処理	• リソースの確認 • スクリプトの実行結果確認 • VMware vSphereの制限事項／注意事項 • vCLS仮想マシンのデータストアの確認と移動 • ServerView RAID Managerへの登録 • 不要なファイルの削除 • VMware EVCモードの設定の確認

6.8.1 動作要件

クラスタ作成機能または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。

- クラスタ作成／クラスタ拡張で共通の動作要件
- クラスタ作成の動作要件
- クラスタ拡張の動作要件

クラスタ作成／クラスタ拡張で共通の動作要件

既存クラスタの動作要件

- PRIMEFLEX for VMware vSANのクラスタであること
- DNS、NTPが正常に動作し、利用可能なこと
- NTPサーバーと時刻同期できていること
- お客様環境の既存AD構成時、またはPRIMEFLEX HS／PRIMEFLEX for VMware vSAN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サーバー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
- お客様環境の既存AD構成時、ADへのコンピューター登録がポリシーなどで制限されている場合、対象サーバーを事前にADへ登録しておくこと
- PRIMEFLEX HS／PRIMEFLEX for VMware vSAN専用ADVM構成時は、ADVM#1とADVM#2にPRIMEFLEX HS／PRIMEFLEX for VMware vSAN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
- vCenter上の以下のネットワーク構成は、PRIMEFLEX HS／PRIMEFLEX for VMware vSAN導入サービスで構築した環境から変更しないこと（変更すると、クラスタ作成／拡張機能の動作に影響します）
  - 管理用分散仮想スイッチ
  - 業務用分散仮想スイッチの名前とアップリンクポート

  分散仮想スイッチ名の確認は、vSphere Clientでインベントリを選択し、表示されたインベントリツリーからネットワークを選択してください。PRIMEFLEX HS／PRIMEFLEX for VMware vSAN導入サービスで構築後の分散仮想スイッチは、vCenter上で以下の名前で表示されます。
  - 管理用分散仮想スイッチ：vSwitch1（PRIMEFLEX HSモデルのPRIMERGY CXシリーズの場合 vSwitch0と表示）
  - 業務用分散仮想スイッチ：vSwitch0（PRIMEFLEX HSモデルのPRIMERGY CXシリーズの場合 vSwitch1と表示）
- Active Directoryドメイン名にNetBIOSドメイン名を使用していないこと
- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること

対象サーバーの動作要件

- ストレージのネットワークを使用する対象サーバーの物理NICが10GbEまたは25GbE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または25GbEであること
- 対象サーバーの電源がオフになっていること

  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、クラスタ作成または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。
  - 対象サーバー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. ISMのGUIでグローバルナビゲーションメニュー上部の[タスク]を選択します。
  2. 「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。
- ストレージ構成が環境に応じた構成であること

  詳細は、「6.8.2.12 搭載したストレージデバイスを確認する」を参照してください。

- 対象サーバーはOS情報が登録されていないこと

  OS情報が登録されている場合、対象ノードの選択から除外されます。

- ISMのプロファイル管理機能で、対象サーバー用プロファイルが作成されていること
- プロファイルで指定する対象サーバーのコンピューター名は、ISMが管理するすべてのノードのコンピューター名と重複していないこと

  コンピューター名の重複確認は、以下の条件で比較します。

  ー 大文字小文字を区別しない

  ー ドメイン名は含めない

- プロファイルで指定する対象サーバーのOSのIPアドレスは、ISMが管理するすべてのノードのOSのIPアドレスと重複していないこと
- 対象サーバーはプロファイル適用されていないこと

  プロファイル適用が完了している場合、対象ノードの選択から除外されます。

- 「クラスタ作成」ウィザードまたは「クラスタ定義パラメーター新規作成」ウィザードの「3.クラスタ詳細情報」画面で[機能]タブ-[vSAN設定]-[ストレージへのディスクの追加]は、「手動」であること
- Hybrid構成時、「クラスタ作成」ウィザードまたは「クラスタ定義パラメーター新規作成」ウィザードの「3.クラスタ詳細情報」画面で[機能]タブ-[vSAN設定]-[デデューブおよび圧縮]は、「無効」であること
- 管理用ネットワークポートグループのIPv4アドレスはプロファイル設定値([詳細]- [OS個別情報]タブ-[ネットワーク]-[DHCP]-[IPアドレス])と同じであること
- iRMC上でネットワーク情報が表示されること

  詳細は、「6.8.2.16 ネットワーク表示を確認する」を参照してください。

クラスタ作成の動作要件

既存クラスタの動作要件

- 既存のクラスタが1つ以上あること
- 既存のクラスタでvCSAのバージョンがクラスタ作成するESXiのバージョンと同一、またはそれより新しいバージョンであること

対象サーバーの動作要件

- 対象サーバー機種は同一であること
- 対象サーバーは3台以上であること
- 「クラスタ作成」ウィザードの「2.クラスタ基本情報」画面で[クラスタ名]は、15文字以内であること
- 「クラスタ作成」ウィザードの「3.クラスタ詳細情報」画面で[ストレージプール]タブ-[ストレージプール名]が既存クラスタの[ストレージプール名]と重複していないこと
- 「クラスタ作成」ウィザードの「3.クラスタ詳細情報」画面で[ネットワーク]タブ-[ポートグループ名]は、新規のvDS作成時、既存クラスタの[ポートグループ名]と重複していないこと
- 既存クラスタのvDS名と同じvDS名を指定した場合、既存クラスタのvDSのvmnicがLAG(Link Aggregation)設定されていないこと
- 既存クラスタのvDS名と同じvDS名を指定した場合、既存クラスタを構成するサーバーのvmnicが各vDSに2個ずつ存在すること
- 新規クラスタを構成するサーバーでVMware ESXiのインストールメディアはすべて同じであること
- VMware ESXiのパッチを適用する場合は、VMware ESXiのパッチのバージョンとVMware ESXiのインストールメディアのバージョンが同じであること

  また、VMware ESXiのパッチのビルド番号は、VMware ESXiのインストールメディアのビルド番号より新しいこと

- vCSAのバージョンとVMware ESXiのバージョンがサポートされていること

  クラスタ作成機能がサポートする製品に関する最新の情報は、当社の本製品Webサイトを参照してください。

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

クラスタ拡張の動作要件

既存クラスタの動作要件

- 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。

  詳細は、「6.8.2.11 クラスタ定義パラメーターの作成と編集を行う」の「注意」を参照してください。

- クラスタ拡張対象の既存クラスタに対して、クラスタ管理機能の事前設定が実施されていること

  クラスタ管理機能の設定については、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

- クラスタ拡張対象の既存クラスタのVMware ESXiはすべて同じバージョンのビルド番号であること

- クラスタ拡張対象の既存クラスタのvSAN ディスク フォーマットはすべて同じバージョンであること

  以下の手順で確認できます。

  vCSA 6.5以前（Flash）の場合：

  1. vSphere Web ClientでvCSAにログインします。
  2. 「トップ」画面から[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]で対象サーバーのディスクが表示されます。

  vCSA 6.7以降（HTML5）の場合：

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[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]で対象サーバーのディスクが表示されます。

  vCSA 7.0U3以降の場合：

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]- [構成]-[vSAN]-[ディスク管理]の[＜ホスト名＞]-[ディスクの表示]で[ディスクフォーマットのバージョン]にカーソルを合わせることで表示されます。

- 「ディスク フォーマットのバージョン」のvSANの健全性エラーが発生していないこと

  以下の手順で確認できます。

  vCSA 6.5以前（Flash）の場合：

  1. vSphere Web ClientでvCSAにログインします。
  2. 「トップ」画面から[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] で再テストを実行します。

  vCSA 6.7以降（HTML5）の場合：

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[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 [注]]で再テストを実行します。

     [注]：vCSA 7.0以降の場合、[Skyline健全性]または[Skyline Health]と表示されます。

- 既存クラスタのvDSのvmnicがLAG（Link Aggregation）設定されていないこと

  以下の手順で確認できます。

  vCSA 6.5以前（Flash）の場合：

  1. vSphere Web ClientでvCSAにログインします。

2. 「トップ」画面から[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＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[仮想スイッチ]-[vDS]にLAGの設定がないことを確認します。

vCSA 6.7以降（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[仮想スイッチ]-[vDS]にLAGの設定がないことを確認します。

- 既存クラスタを構成するサーバーのvmnicが各vDSに2個ずつ存在すること

以下の手順で確認できます。

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[仮想スイッチ]-[vDS]にvmnicの設定が2個ずつ存在することを確認します。

vCSA 6.7以降（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[仮想スイッチ]-[vDS]にvmnicの設定が2個ずつ存在することを確認します。

- 既存クラスタを構成するサーバーのVMkernelアダプタのvSAN（vMotion）トラフィックのデバイスがvmk1（vmk2）であること

以下の手順で確認できます。

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[Vmkernelアダプタ]-[vmk1（vmk2）]がvSAN（vMotion）の設定であることを確認します。

vCSA 6.7以降（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]-[＜ホスト名＞]-[構成]-[ネットワーク]-[Vmkernelアダプタ]-[vmk1（vmk2）]がvSAN（vMotion）の設定であることを確認します。

- vCSA 7.0 U1以降の場合、vSphereクラスタサービス（vCLS）のステータスが正常であること

vSphereクラスタサービス（vCLS）のステータスは、以下の手順で確認できます。

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]を選択します。
3. [名前]が[＜vCLS名＞]の[ステータス] を確認します。
   - vCSA 7.0U2以前の場合：

     ＜vCLS名＞は、"vCLS (n)"（nは数字）で表示されます。
   - vCSA 7.0U3以降の場合：

     ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"（Xは16進数）で表示されます。

   [ステータス] が「正常」であることを確認してください。
4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

ポイント

vCSAにログインするユーザー種別によってはvSphereクラスタサービス(vCLS)が表示されない場合があります。
vSphereクラスタサービス(vCLS)関連の操作を行う際には、vCenter Single Sign-Onドメインの管理者を使用してください。

- vCSA 7.0 U1以降の場合、vCLS仮想マシンはvSANデータストア上に存在していること

  vCLS仮想マシンが配置されているデータストアは、以下の手順で確認できます。

  1. vSphere ClientでvCSAにログインします。
  2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
     - vCSA 7.0U2以前の場合:

       ＜vCLS名＞は、"vCLS (n)"(nは数字)で表示されます。

     - vCSA 7.0U3以降の場合:

       ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"(Xは16進数)で表示されます。
  3. [データストア]-[名前] がvSANデータストア名であることを確認します。

     vSANデータストア名は、ISMのGUIで対象クラスタのクラスタ定義パラメーターの[クラスタ詳細情報]-[ストレージプール]タブの[ストレージプール名]で確認できます。

     vSANデータストア名ではない場合、「6.8.4.4 vCLS仮想マシンのデータストアを確認して移動する」の「vSANデータストアへの移動手順」を実施します。
  4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

対象サーバーの動作要件

- 対象サーバーは、既存クラスタで構成されるサーバーに対して、同一または後継機種であること

  詳細については、当社の本製品Webサイトで『管理対象機器一覧』([ISM for PRIMEFLEX_詳細]シート)を参照してください。
  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/
- 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、「6.8.2.11 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。
- VMware ESXiのパッチはクラスタ拡張対象の既存クラスタのVMware ESXiと同じバージョンのビルド番号であること
- VMware ESXiのインストールメディアは以下であること
  - 対象サーバーが複数台ある場合は、VMware ESXiのインストールメディアはすべて同じであること
  - VMware ESXiのパッチを適用しない場合は、クラスタ拡張対象の既存クラスタのVMware ESXiと同じバージョンのビルド番号であること
  - VMware ESXiのパッチを適用する場合は、クラスタ拡張対象の既存クラスタのVMware ESXiと同じバージョンであること

ポイント

- クラスタ拡張の実行後にリソースが増えているか確認が必要です。クラスタ拡張を実行前に現在の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、「6.8.4.1 リソースを確認する」を参照してください。
- VMware ESXiのバージョンとビルド番号、vSAN ディスク フォーマット バージョンは、以下のURLを参照して、サポート有無を確認してください。

  https://kb.vmware.com/s/article/2150753

注意

vCSA7.0U2以降でvCSAにログインする場合には、ローカルユーザーを使用しないでください。

6.8.2 事前準備

クラスタ作成またはクラスタ拡張を行う前の準備作業について説明します。

6.8.2.1 vCenter ServerのVMware EVCを設定する

本設定は、クラスタ拡張機能を使用する場合に必要な作業です。クラスタ作成機能を使用する場合には不要です。

PRIMEFLEXに後継機種となるサーバーもしくは同一機種で異なる世代のCPUが搭載されているサーバーを追加するために必要な作業です。

CPU世代の確認方法

1. Webブラウザーで各サーバーのiRMCのIPアドレスを入力します。
2. ユーザー名／パスワードを入力後、[ログイン]を選択してログインします。
3. [システム]-[システムボード]を選択し、[CPU]の項目を開きます。
4. [CPUモデル]に記載された数字4桁の左から2桁目がCPU世代を示します。各サーバーで数字が異なる場合は、設定が必要です。

   例:
   Intel(R) Xeon(R) Platinum 8480+の場合、4桁の数字の左から2桁目が"4"のためSapphire Rapids
   Intel(R) Xeon(R) Silver 4514Yの場合、4桁の数字の左から2桁目が"5"のためEmerald Rapids

VMwareのEVC（Enhanced vMotion Compatibility）機能を使用すると、クラスタ内のホスト全体でvMotionの互換性を維持できるようになります。

注意

- クラスタを構成するサーバーがすべて同一のときでも、VMware EVCモードを設定するには、vSANクラスタ上の仮想マシンの停止が必要な場合があります。

  PRIMEFLEX構成のADVMを停止が必要な場合は、ドメインユーザー以外の管理者権限でVMware EVCモードを設定してください。
- 以下のURLを参照して、使用しているvCSAおよびESXiのバージョンで、設定するCPU世代がサポートされているかを確認します。

  サポートされていない場合、事前に該当のCPU世代がサポートされているvCSAおよびESXiへバージョンアップをしてください。

  https://kb.vmware.com/s/article/1003212

  https://kb.vmware.com/s/article/1005764

  例）PRIMERGY M2シリーズ(Intel(R)「Broadwell」Generation)では、vCSA 6.5以降およびESXi 6.5以降が必要です。

以下の手順でVMware EVCを設定してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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]-[設定]-[VMware EVC]-[編集]を選択します。
3. 表示されたEVCモードの変更画面で、[EVCモードの選択]で[Intel(R) ホスト用にEVCを有効化]にチェックを付け、[VMware EVCモード]を選択します。

表6.11 VMware EVCモードの設定

お客様のPRIMEFLEX環境で最も旧世代のサーバー	設定値
PRIMERGY M2シリーズ	Intel(R)「Broadwell」Generation
PRIMERGY M4シリーズ	Intel(R)「Skylake」Generation
PRIMERGY M5シリーズ	Intel(R)「Cascade Lake」Generation
PRIMERGY M6シリーズ	Intel(R)「Ice Lake」Generation
PRIMERGY M7シリーズ	Intel(R)「Sapphire Rapids」Generation

4. [OK]ボタンを選択します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定]-[設定]-[VMware EVC]-[編集]を選択します。
3. 表示されたEVCモードの変更画面で、[EVCモードの選択]で[Intel(R) ホスト用にEVCを有効化]にチェックを付け、[VMware EVCモード]を選択します。

表6.12 VMware EVCモードの設定

お客様のPRIMEFLEX環境で最も旧世代のサーバー	設定値
PRIMERGY M2シリーズ	Intel(R)「Broadwell」Generation
PRIMERGY M4シリーズ	Intel(R)「Skylake」Generation
PRIMERGY M5シリーズ	Intel(R)「Cascade Lake」Generation
PRIMERGY M6シリーズ	Intel(R)「Ice Lake」Generation
PRIMERGY M7シリーズ	Intel(R)「Sapphire Rapids」Generation

4. [OK]ボタンを選択します。

vCSA 7.0U3以降の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[構成]-[設定]-[VMware EVC]-[編集]を選択します。
3. 表示されたEVCモードの変更画面で、[Intel(R) ホスト用にEVCを有効化]にチェックを付け、[CPUモード]を選択します。

表6.13 VMware EVCモードの設定

お客様のPRIMEFLEX環境で最も旧世代のサーバー	設定値
PRIMERGY M2シリーズ	Intel(R)「Broadwell」Generation
PRIMERGY M4シリーズ	Intel(R)「Skylake」Generation
PRIMERGY M5シリーズ	Intel(R)「Cascade Lake」Generation
PRIMERGY M6シリーズ	Intel(R)「Ice Lake」Generation
PRIMERGY M7シリーズ	Intel(R)「Sapphire Rapids」Generation

4. [OK]ボタンを選択します。

6.8.2.2 ADVMの証明書を作成する

本設定は、クラスタ作成機能またはクラスタ拡張機能において、PRIMEFLEX HS／PRIMEFLEX for VMware vSAN専用ADVM構成時に必要な作業です。初回に一度だけ実施してください。お客様環境のADをご使用の場合やActiveDirectory連携を行わない場合は不要です。

クラスタ作成機能または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作成機能または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。
「6.8.2.3 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作成機能または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	• [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	• [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に記載されている問題が原因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://support.microsoft.com/ja-jp/help/4093492/credssp-updates-for-cve-2018-0886-march-13-2018

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

6.8.2.2.1 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
```

再度、上記の確認コマンドを実行し、STATEがRUNNINGになっていることを確認します。

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。

6.8.2.2.2 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、「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ー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、「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ーへのリモート アクセスを許可するように設定されていません。」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ーへのリモート アクセスを許可するように設定されていません。
次の変更を行う必要があります:

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成してください。
変更しますか [y/n]? y
```

以下のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成しました。
```

再度、上記のコマンドを実行し、「WinRM サービスは、既にこのコンピューターで実行されています。」と表示されることを確認します。

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
        NetworkDelayms = 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"}
```

再度、上記の確認コマンドを実行し、[Config]-[Client]-[Auth] -[Basic]がtrueとなっていることを確認します。

(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。

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

注意

- 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。
- 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)

ADVM#1とADVM#2の2つの証明書を作成してください。

(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。

```
>makecert.exe -r -pe -n "CN=<ADVM#1のサーバー名>" -e <証明書の有効期限(mm/dd/yyyy)> -eku 1.3.6.1.5.5.7.3.1 -ss My -sr localMachine -sky exchange <ADVM#1のコンピューター名>.cer -sv <秘密鍵のファイル名>.pvk
```

以下は対象ADVM#1のサーバー名を「192.168.10.10」、証明書の有効期間を「2018年3月30日」、ADVM#1のコンピューター名と秘密鍵のファイル名を「ADVM1」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 ADVM1.cer -sv ADVM1.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。

以下のコマンドを実行して、＜ADVM#1のコンピューター名＞.cerと＜秘密鍵のファイル名＞.pvkの作成を確認します。

```
>dir
```

(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 <ADVM#1のコンピューター名>.cer -pfx <ADVM#1のコンピューター名>.pfx
```

以下は秘密鍵のファイル名とADVM#1のコンピューター名を「ADVM1」に設定する場合のコマンド例です。

実行例:

```
>pvk2pfx.exe -pvk ADVM1.pvk -spc ADVM1.cer -pfx ADVM1.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。

以下のコマンドを実行して、＜ADVM#1のコンピューター名＞.pfxの作成を確認します。

```
>dir
```

(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]を選択します。
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. ＜ADVM#1のコンピューター名＞.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、＜ADVM#1のコンピューター名＞.cerファイルを選択し、「証明書のインポートウィザード」画面を完了します。

2. ＜ADVM#1のコンピューター名＞.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に指定したサーバー名となっていること、「目的」が「サーバー認証」となっていることを確認してください。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. ＜ADVM#1のコンピューター名＞.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、＜ADVM#1のコンピューター名＞.pfxファイルを選択し、「証明書のインポートウィザード」画面を完了します。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

   ＜ADVM#1のコンピューター名＞.pfxファイルを選択する場合、プルダウンボックスから指定する必要があります。

4. ＜ADVM#1のコンピューター名＞.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に指定したサーバー名となっていること、「目的」が「サーバー認証」となっていることを確認してください。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、「6.8.2.2.2 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。

6.8.2.2.3 ファイア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
```

3. 以下のコマンドを実行して、ファイアウォールの設定を確認します。

```
Show-NetFirewallRule | ?{$_.LocalPort -match <ポート番号>}
```

例:ポート番号5986のファイアウォールの設定を確認します。

```
Show-NetFirewallRule | ?{$_.LocalPort -match 5986}
```

以下のようなコマンド結果が返ってくれば、ファイアウォールのポート開放ができています。

```
$_ | Get-NetFirewallPortFilter
Protocol : TCP
LocalPort : 5986
RemotePort : Any
IcmpType : Any
DynamicTarget : Any

$_ | Get-NetFirewallPortFilter
Protocol : TCP
LocalPort : 5986
RemotePort : Any
IcmpType : Any
DynamicTarget : Any
```

注意

- ファイアウォールの設定は、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「6.8.2.2.3 ファイアウォールのポートを開放する」を行ってください。

6.8.2.2.4 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、「6.8.2.3 DNSへホストレコードを登録する」、または「6.8.2.4 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
```

3. 再度、上記の確認コマンドを実行し、「RemoteSigned」となっていることを確認します。

注意

ADVM#1をADVM#2に読み替えて、ADVM#2に対しても同様に「6.8.2.2.4 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。

6.8.2.3 DNSへホストレコードを登録する

お客様環境のDNSサーバー使用時にのみ必要な作業です。クラスタ作成またはクラスタ拡張を実行する前にDNSの前方参照ゾーン、および逆引き参照ゾーンへ対象サーバーの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。

すべての対象サーバーに対して実施してください。

図6.6 前方参照ゾーンの登録例

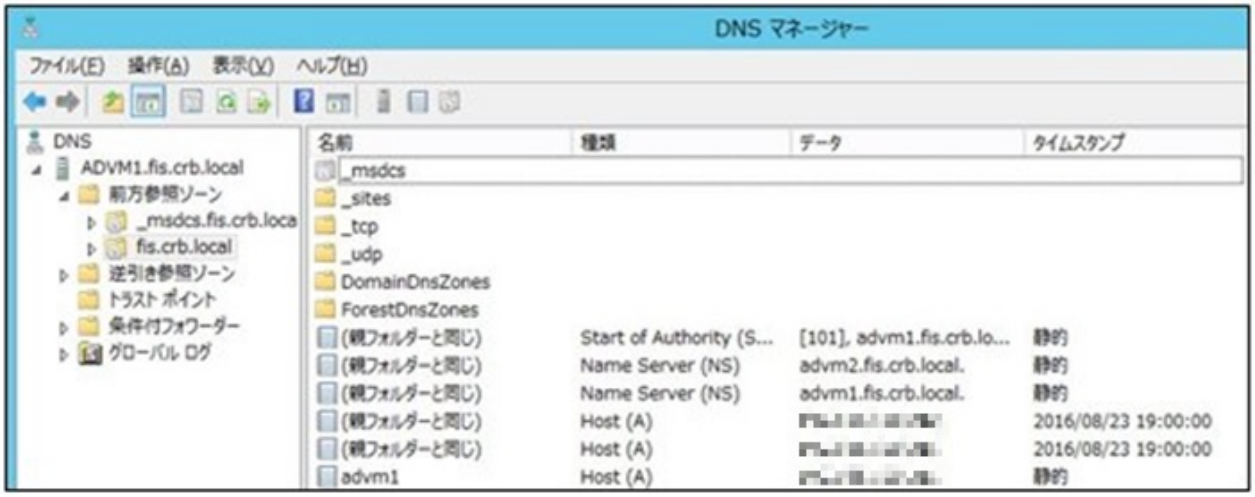
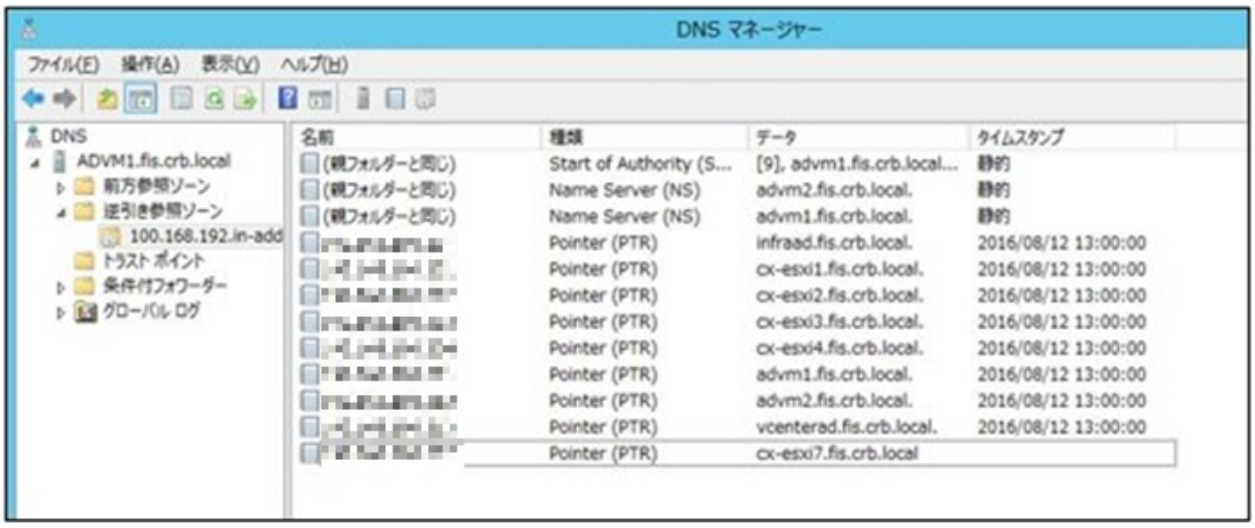


図6.7 逆引き参照ゾーンの登録例



6.8.2.4 DHCPを設定する

クラスタ作成機能または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サーバーが必要です。

ISM-VAは内部でDHCPサーバー機能を持っていますが、ISM-VA外部にDHCPサーバー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、『解説書』の「4.15 ISM-VA内部のDHCPサーバー」を参照して設定してください。

すべての対象サーバー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サーバー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、2つのポートに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1ノード当たり2つ分のIPアドレスを設定してください。
- 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、『解説書』の「4.15.4 DHCPサーバーの切替え」を参照してください。

6.8.2.5 ServerView Suite DVDに同梱されるServerView Installation ManagerとOSのインストールメディアをISM-VAへインポートする

ServerView Suite DVDに同梱されるServerView Installation Manager（以降、「SVIM」と表記）とOSのインストールメディアの2つをISMにインポートします。

- ServerView Installation Managerのインポート

  対象サーバーに対応したServerView Installation Managerをインポートしてください。

- OSのインストールメディアのインポート

  既存クラスタのVMware ESXiと同じバージョンのOSのインストールメディアをインポートしてください。

インポートの操作については、『解説書』の「2.13.2 リポジトリ管理機能」を参照してください。

また、サポートバージョンは、『プロファイル管理機能 プロファイル設定項目集』の「3.2 VMware ESXi用プロファイル」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、『解説書』の「3.7 仮想ディスクの割当て」を参照してください。

注意

- クラスタ拡張機能を使用する場合、OSのインストールメディアは以下のものをインポートします。異なるものをインポートした場合には、クラスタ拡張は異常終了します。

  ー VMware ESXiのパッチを適用しない場合は、既存クラスタのVMware ESXiと同じバージョンのビルド番号

  ー VMware ESXiのパッチを適用する場合は、既存クラスタのVMware ESXiと同じバージョン

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

6.8.2.6 以前に使用したスクリプトを削除する

クラスタ作成またはクラスタ拡張を使用する場合には、以下の手順で古いVMware ESXiパッチとVMware ESXiパッチ適用前後で実行するスクリプトを削除してください。

(1) 古いVMware ESXiパッチを削除する

ISM-VAに対して実施してください。前回のクラスタ作成またはクラスタ拡張時にISM-VAにアップロードしたVMware ESXiパッチを使用する場合は、本手順は不要です。

1. ISM管理者（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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/kickstart
ファイル	古いVMware ESXiパッチファイル

(2)古いVMware ESXiパッチ適用前後で実行するスクリプトを削除する

ISM-VAに対して実施してください。前回のクラスタ作成またはクラスタ拡張時にISM-VAにアップロードしたVMware ESXiパッチ適用前後で実行するスクリプトを使用する場合は、本手順は不要です。

1. ISM管理者(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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/script
ファイル	古いVMware ESXiパッチ適用前後で実行するスクリプト

6.8.2.7 VMware ESXiパッチをアップロードする

クラスタ作成機能またはクラスタ拡張機能でVMware ESXiのパッチも適用したい場合に実施してください。VMware 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。

クラスタ拡張機能を使用する場合は、既存クラスタのVMware ESXiと同じバージョンのビルド番号になるように、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、『解説書』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、クラスタ作成またはクラスタ拡張は異常終了します。
- アップロードしたVMware 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、クラスタ作成またはクラスタ拡張は異常終了します。

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、VMware ESXiパッチファイルをアップロードしてください。

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	クラスタ管理用ファイル
アップロード先ディレクトリー	Administrator/ftp/kickstart
ファイル	VMware ESXiパッチファイル [注] 例)ESXi650-201704001.zip

[注]:VMware ESXiパッチ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。

6.8.2.8 VMware ESXiパッチ適用前後で実行するスクリプトを必要に応じて作成する

VMware ESXiの修正パッチには制限事項や注意事項がある場合があります。
以下のサイトを参照して、『VMware vSphere X.X ソフトウェア説明書』(Xには、バージョンが入ります。)で注意事項を確認してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

注意事項の対処は、スクリプトによってクラスタ作成またはクラスタ拡張機能の実行中に対応できます。なお、スクリプトは必須ではありません。

スクリプトは、以下の3つのタイミングで実行が可能です。

- VMware ESXiのパッチ適用前
- VMware ESXiのパッチ適用時
- VMware ESXiのパッチ適用後

注意

- VMware ESXiのパッチ適用時とは適用コマンド実行直後のことであり、ESXiの再起動前になります。

  VMware ESXiのパッチ適用後とは適用コマンドを実行して、ESXiの再起動も実行した後になります。
- スクリプトは規定時間(720秒)以内で終了しないとクラスタ作成またはクラスタ拡張に失敗します。ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

実行するスクリプト名は固定です。以下の実行するタイミングごとにスクリプト名は異なります。

スクリプト名 [注]	実行するタイミング
pre_script.sh	VMware ESXiのパッチ適用前に実行する
post01_script.sh	VMware ESXiのパッチ適用時に実行する
post02_script.sh	VMware ESXiのパッチ適用後に実行する

[注]:スクリプトの形式はシェル(bash)のみサポートしています。

ポイント

- 「exit 1」でスクリプトを終了することでエラー検出できます。
- 事後処理でスクリプトの実行結果を確認できるように、ESXi上にログをファイル出力するなどの処理を入れてください。
- クラスタ作成機能またはクラスタ拡張機能のタスクでエラー終了した場合、クラスタ作成またはクラスタ拡張の再実行が必要になります。スクリプトは再実行してもエラー終了しないように作成してください。以下の作成例では、再実行してもエラー終了しないようにしています。

以下のサンプルを参照してスクリプトを作成してください。

VMware ESXiのパッチ適用前に実行するスクリプトの作成例

ESXiをパッチ適用する際に必要な以下の処理を実行するスクリプトを作成しています。

- ツールの削除
- ドライバーの削除
- ドライバーの設定変更

```
#!/usr/bin/sh

### Tool removal ###
echo "Tool removal Start" >> /scratch/log/pre_script.log
toolName=`(esxcli software vib list | grep storcli)`
if [ $? = 0 ]; then
    echo ${toolName} >> /scratch/log/pre_script.log
    toolName=`(echo ${toolName} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ${toolName}"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
```

```
        exit 1
    fi
fi
echo "Tool removal End" >> /scratch/log/pre_script.log

### Driver removal ###
echo "Driver removal Start" >> /scratch/log/pre_script.log
driver1=`(esxcli software vib list | grep "OEM.500")`
if [ $? = 0 ]; then
    echo ${driver1} >> /scratch/log/pre_script.log
    driver1Name=`(echo ${driver1} | cut -f 1 -d ' ')`
    cmd="esxcli software vib remove -n ¥"${driverName1}¥""
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver removal End" >> /scratch/log/pre_script.log

### Driver settings ###
echo "Driver settings Start" >> /scratch/log/pre_script.log
driver2=`(esxcli system module list | grep lsi_mr3)`
if [ $? = 0 ]; then
    echo ${driver2} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_mr3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
driver3=`(esxcli system module list | grep lsi_msgpt3)`
if [ $? = 0 ]; then
    echo ${driver3} >> /scratch/log/pre_script.log
    cmd="esxcli system module set -e true -m lsi_msgpt3"
    echo ${cmd} >> /scratch/log/pre_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Driver settings End" >> /scratch/log/pre_script.log

echo "pre_script End" >> /scratch/log/pre_script.log
exit 0
```

VMware ESXiのパッチ適用時に実行するスクリプトの作成例

ここではESXi 6.7の運用と保守の注意事項に対する対処を実行するスクリプトを作成しています。

ー v470-1のカスタムイメージで構築したESXiに、パッチ「ESXi670-201905001」以降を適用する際のInboxドライバーの置換を実施するスクリプトです。

```
#!/usr/bin/sh

#### parameter settings ####
EffectiveValue='VMware-ESXi-6.7.0-13473784-Fujitsu-v470-1-offline_bundle.zip -n lsi-mr3 -n lsi-msgpt3'

### Execution command ###
cmd="esxcli software vib install --dry-run -d /var/tmp/SvrExpScriptDir/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
```

```
    exit 1
fi

cmd="esxcli software vib install -d /var/tmp/SvrExpScriptDir/${EffectiveValue}"
echo ${cmd} >> /scratch/log/post01_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi

echo "post01_script End" >> /scratch/log/post01_script.log
exit 0
```

VMware ESXiのパッチ適用後に実行するスクリプトの作成例

ESXiのパッチ適用後の制限事項／注意事項に対する以下の対処を実行するスクリプトを作成しています。

- 電力管理設定に関する留意事項
- igbnドライバーの更新について
- テンポラリ領域の設定

```
#!/usr/bin/sh

#### parameter settings ####
PowerValue="High Performance"
DriverFile="＜適用するドライバーファイル名＞"
TemporaryName="scratch"
### Execution command ###
# Power Policy
echo "Power Policy Start" >> /scratch/log/post02_script.log
CurrentValue=`esxcli system settings advanced list --option=/Power/CpuPolicy | grep '   String Value: High
Performance'`
if [ $? != 0 ]; then
    cmd='esxcli system settings advanced set --option=/Power/CpuPolicy --string-value="High Performance"'
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Power Policy End" >> /scratch/log/post02_script.log

# Update Driver
echo "Update Driver Start" >> /scratch/log/post02_script.log
cmd="esxcli software vib install -d /var/tmp/SvrExpScriptDir/${DriverFile}"
echo ${cmd} >> /scratch/log/post02_script.log
eval ${cmd}
if [ $? != 0 ]; then
    exit 1
fi
echo "Update Driver End" >> /scratch/log/post02_script.log

# Temporary
echo "Temporary Start" >> /scratch/log/post02_script.log
TmpSetting=`(vim-cmd hostsvc/advopt/view ScratchConfig.ConfiguredScratchLocation | grep "value")`
TmpDir=`(echo ${TmpSetting} | cut -f 2 -d '"')`
if [ ${#TmpDir} = 0 ]; then
    cmd="mkdir /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
```

```
    cmd="vim-cmd hostsvc/advopt/update ScratchConfig.ConfiguredScratchLocation string /var/tmp/${TemporaryName}"
    echo ${cmd} >> /scratch/log/post02_script.log
    eval ${cmd}
    if [ $? != 0 ]; then
        exit 1
    fi
fi
echo "Temporary End" >> /scratch/log/post02_script.log

echo "post02_script End" >> /scratch/log/post02_script.log
exit 0
```

ポイント

スクリプトの1行目には、以下の記述をする必要があります。

```
#!/usr/bin/sh
```

注意

作成するスクリプトには、対象ノードを再起動する処理は入れないでください。スクリプト実行の後には必ず再起動が実行されます。

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、スクリプトをアップロードしてください。

表6.14 アップロードするスクリプトとディレクトリー

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/script
ファイル	• 適用前に実行するスクリプトの場合 pre_script.sh • 適用時に実行するスクリプトの場合 post01_script.sh • 適用時に実行するスクリプトの場合 post02_script.sh

ポイント

ポストスクリプト内で使用するオフラインバンドルは「6.8.2.7 VMware ESXiパッチをアップロードする」を参照してISM-VAへアップロードしてください。オフラインバンドル以外に使用するファイルがある場合には、以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、アップロードしてください。

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/ESXi/other
ファイル	その他のファイル

6.8.2.9 VMware SMIS Providerをアップロードする

対象サーバーが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-lsiprovider-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、『解説書』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、クラスタ作成また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、クラスタ作成またはクラスタ拡張は異常終了します。

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、VMware SMIS Providerのオフラインバンドルをアップロードしてください。

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	クラスタ管理用ファイル
アップロード先ディレクトリー	Administrator/ftp/kickstart
ファイル	VMware SMIS Providerのオフラインバンドル [注] 例）VMW-ESX-5.5.0-lsiprovider-500.04.V0.63-0005-offline_bundle-5240997.zip

[注]：VMware SMIS Providerのオフラインバンド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。

6.8.2.10 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、対象サーバーのプロファイルを作成します。

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

プロファイルの設定値の詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第4章 プロファイルの設定値一覧」を参照してください。

- クラスタ作成機能を使用する場合

  対象サーバーが既存クラスタ環境のサーバーと同じ場合には、既存のプロファイルから参照作成してください。
  対象サーバーが既存クラスタ環境のサーバーと異なる場合には、新規作成してください。

- クラスタ拡張機能を使用する場合

  ― 対象サーバーが既存クラスタ環境のサーバーと同じ場合には、既存のプロファイルから参照作成してください。
  後継機種となるサーバーを追加する場合には、新規作成してください。

  ― 対象サーバーが既存クラスタ環境のサーバーと同じ場合には、既存のプロファイル、ポリシーから参照作成し、プロファイルの再適用をしてください。「3.3.5 適用済みのプロファイルとハードウェア設定を比較する」の「[不一致]になっている[ベリファイステータス]を[一致]に戻す方法（ノード設定内容の変更が意図したものである場合）」を参照してください。

ー 既存クラスタ環境のESXiがアップデートしている場合には、導入予定の版数のインストールメディアを指定したOSポリシーを作成したうえで、プロファイルを新規作成してください。
作成手順は、「3.3 サーバーに各種設定／OSインストールをする」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. 新規作成の場合は、[アクション]ボタンから[プロファイル追加]を選択します。
参照作成の場合は、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。

ポイント

『解説書』の「2.4.4 OSインストールの設定」を参照して、OSインストール時に必要な準備作業を行ってください。

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]

  VM標準ネットワークを使用しないため、本項目の設定は不要です。

- [OS]タブの[仮想化管理ソフトへの登録]

  既存クラスタの仮想化管理ソフトウェアを使用するため、本項目の設定は不要です。

- [OS個別情報]タブの[DHCP]

  管理LANのIPアドレスは固定IPアドレスを使用するため、本項目の設定は不要です。

ー 以下の項目には、チェックが付いていても問題ありません。

クラスタ作成機能、またはクラスタ拡張機能が自動で設定するためです。

- [OS]タブの[インストール後のスクリプト実行]

  OSポリシーで本項目を指定している場合、以下の設定になっていることを確認してください。値が異なる場合、クラスタ作成機能またはクラスタ拡張機能がエラー終了します。

  ・[OS]タブの[インストール後のスクリプト実行]：有効

  ・[OS]タブの[スクリプト格納ディレクトリ]：kickstart

  ・[OS]タブの[実行するスクリプト]：ESXi_Setting.sh

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]-[コンピューター名をDNSサーバーから取得]-[コンピューター名]

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。本項目はオンボードLANが複数あり、管理LANに使用するネットワークポートを特定するために必要な設定です。

- [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以上の通信が可能なポートのMACアドレスを指定してください。

  なお、PRIMERGY M6シリーズ／PRIMERGY M7シリーズの場合、PCIカード上のポートのMACアドレスを指定してください。

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。本項目はオンボードLANが1つであり、管理LANに使用するネットワークポートを特定する必要がないため、設定は不要です。

- [OS]タブの[ネットワークポート指定]

ー クラスタ拡張機能を使用する場合、以下の項目には、「6.8.2.5 ServerView Suite DVDに同梱されるServerView Installation ManagerとOSのインストールメディアをISM-VAへインポートする」でインポートしたものを指定してください。異なるものを指定した場合には、クラスタ拡張は異常終了します。

- [OS]タブの[インストール指定]-[インストールメディア]

ー クラスタ作成機能またはクラスタ拡張機能がサポートする製品に関する最新の情報は、当社の本製品Webサイトを参照してください。

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

6.8.2.11 クラスタ定義パラメーターの作成と編集を行う

本設定は、クラスタ拡張機能を使用する場合に必要な作業です。クラスタ作成機能を使用する場合には不要です。

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ーのクラスタ定義パラメーターを作成する必要はありません。クラスタ拡張を実行するときに設定します。

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。
- ISMのアップグレード後にクラスタ定義パラメーターが指定されていない設定項目がある場合は、クラスタ定義パラメーターを編集してください。また、ISMのGUIでは自動入力の項目があります。設定値が正しいことを確認してください。

注意

- クラスタ定義パラメーターがすでに以下の内容で作成されている場合は、変更が必要です。クラスタ定義パラメーターを編集してください。
  デデュープおよび圧縮はストレージ構成がAll-Flashの場合に有効な設定です。

設定項目	現在の設定値	変更後の設定値
クラスタ詳細情報-[機能]タブ-[vSAN設定]-[ストレージへのディスクの追加]	自動	手動
クラスタ詳細情報-[機能]タブ-[vSAN設定]-[デデュープおよび圧縮] [注]	有効	無効

[注]:ストレージ構成がHybridの場合に変更してください。ストレージ構成がAll-Flashの場合には変更不要です。

クラスタ定義パラメーターを変更した場合、以下の手順で対象クラスタの設定を変更してください。
また、ストレージへのディスクの追加とデデュープおよび圧縮の変更は、同時に実施が可能です。

ー ストレージへのディスクの追加を「自動」から「手動」に変更した場合の対象クラスタへの設定手順
vCSA 6.7以降では設定不要です。

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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]-[vSANがオンになっています]-[編集]を選択します。

   「vSAN設定の編集」画面が表示されます。
3. [ストレージへのディスクの追加]を「手動」に設定して、[OK]ボタンを選択します。

ー デデュープおよび圧縮を「有効」から「無効」に変更した場合の対象クラスタへの設定手順

vCSA 6.5以前（Flash）の場合：

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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]-[vSANがオンになっています]-[編集]を選択します。

   「vSAN設定の編集」画面が表示されます。
3. [サービス]-[デデュープおよび圧縮]を「無効」に設定して、[OK]ボタンを選択します。

vCSA 6.7 ～ vCSA 7.0 U1（HTML5）の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[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]-[サービス]-[デデュープおよび圧縮]-[編集]を選択します。

   「vSANサービス」画面が表示されます。
3. [サービス]-[デデュープおよび圧縮]を「無効」に設定して、[適用]ボタンを選択します。

vCSA 7.0 U2以降の場合：

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-「ホストおよびクラスタ」の[＜クラスタ名＞]-[設定 [注]]-[vSAN]-[サービス]-[データサービス]-[編集]を選択します。

   「vSANサービス」画面が表示されます。

   [注]：vCSA 7.0 U3以降の場合、[構成]と表示されます。
3. [容量効率]を「なし」に設定して、[適用]ボタンを選択します。

・ ローリングアップデート機能が実行中またはエラー終了していた場合は、クラスタ定義パラメーターの作成と編集を行わないでください。クラスタ定義パラメーターの作成と編集に失敗します。

6.8.2.12 搭載したストレージデバイスを確認する

対象サーバーに搭載したストレージデバイスを確認します。環境に応じて、搭載したストレージデバイスがストレージ構成の動作要件を満たしているか確認してください。

・ PRIMEFLEX HSの場合：

ー お使いのストレージ構成に対応した要件を満たしていること

ストレージ構成	ディスクグループごとの構成	
	種類	本数
Hybrid	キャッシュデバイス：SSD	1本
	キャパシティデバイス：HDD	最大7本
All Flash	キャッシュデバイス：SSD	1本

ストレージ構成	ディスクグループごとの構成	
	種類	本数
	キャパシティデバイス:SSD [注]	最大7本

[注]:ディスク容量が160～210GB以外、320～420GB以外であること

ー 最大ディスクグループ数は以下であること

機種	最大ディスクグループ数
PRIMERGY RX2530 M2	2
PRIMERGY RX2540 M2	4
PRIMERGY CX2550 M2	1

・ PRIMEFLEX for VMware vSANの場合:

ー お使いのストレージ構成に対応した要件を満たしていること

ストレージ構成	ディスクグループごとの構成		SASコントローラカードごとの構成
	種類	本数	
Hybrid	キャッシュデバイス:SSD	1本	SSD1本以上、HDD本数はSSDの本数以上であること
	キャパシティデバイス:HDD	最大7本	
All Flash	キャッシュデバイス:SSD	1本	キャッシュ、キャパシティ用の2種類のSSDのディスク容量が2種類または1種類であること ・ ディスク容量が2種類の場合 キャッシュデバイスはディスク容量が2種類のSSDのうち、本数が少ない方(SSDの本数が同じとき、ディスク容量の小さい方)であること ・ ディスク容量が1種類の場合 キャッシュデバイスは1つのSSDがキャッシュ用のSSDであること
	キャパシティデバイス:SSD	最大7本	

ー キャッシュデバイスは5本以内であること

ー 最大ディスクグループ数は以下であること

機種	最大ディスクグループ数
PRIMERGY RX2530 M4	3
PRIMERGY RX2540 M4	5
PRIMERGY CX2560 M4	2
PRIMERGY RX2530 M5	3
PRIMERGY RX2540 M5	5
PRIMERGY CX2560 M5	2
PRIMERGY RX4770 M5	4
PRIMERGY RX2530 M6	4
PRIMERGY RX2540 M6	5
PRIMERGY RX2530 M7	5
PRIMERGY RX2540 M7	5

6.8.2.13 設置と結線を行う

対象サーバーの設置と結線を行います。詳細は、対象サーバーの『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。

ポイント

ISMのネットワークインターフェイスは、1つだけ定義できます。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、ルーターを設定し、各ネットワーク間で通信可能な状態にしてください。ネットワーク構成に関しては、『解説書』の「1.2 構成」も併せて参照してください。

すべての対象サーバー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

  以下の手順で作業を実施してください。

  1. 「6.8.2.14 iRMCのIPアドレスを設定する」
  2. 「6.8.2.15 BIOSを設定する」
  3. 「6.8.2.17 ISMへノードを登録する」の「手動検出によるノード登録」
  4. 「6.8.3 クラスタ作成またはクラスタ拡張を実行する」

- ノードを自動検出する場合

  以下の手順で作業を実施してください。

  1. 「6.8.2.17 ISMへノードを登録する」の「自動検出によるノード登録」
  2. 「6.8.2.15 BIOSを設定する」
  3. 「6.8.3 クラスタ作成またはクラスタ拡張を実行する」

6.8.2.14 iRMCのIPアドレスを設定する

対象サーバーを手動検出で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。

対象サーバーの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「6.8.2.13 設置と結線を行う」の作業が必要です。また、「BIOS設定」画面で表示／操作を行うために、対象サーバー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、対象サーバーの「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。

すべての対象サーバー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「6.8.2.15 BIOSを設定する」も実施してください。

対象サーバーの「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。

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

上記サイトで「製品を選択する」- [カテゴリから探す]を選択し、カテゴリ:[Fujitsu Server PRIMERGY] - グループ:[＜対象サーバーのグループ＞] - 製品:[＜対象サーバー＞]を選択してください。
[Systemboard]からダウンロードしてください。

なお、参照手順は、予告なく変更されることがあります。

6.8.2.15 BIOSを設定する

BIOSの設定手順について説明します。

ISMのノード登録作業時のノード検出方法が手動検出の場合は、「6.8.2.14 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。

ISMのノード登録作業時のノード検出方法が自動検出の場合は、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。

1. 「6.8.2.16 ネットワーク表示を確認する」の手順1、2を参照し、対象サーバーの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。

   ビデオリダイレクションの画面(サーバーの画面)が表示されます。

   ポイント

   ビデオリダイレクションの画面(サーバーの画面)が表示されない場合

   iRMCログイン後、[設定]タブ - [AVR(Advanced Video Redirection)]- [KVMリダイレクションタイプ]を確認し、「HTML5 Viewer」になっていることを確認してください。「JViewer(JAVA)」となっている場合は、「HTML5 Viewer」を選択し、[適用]ボタンを選択してから再度ビデオリダイレクションを選択してください。

2. 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 Server)またはパワーサイクル(Power Cycle)]を選択します。

   実施確認のダイアログに対しては、[はい]を選択します。
   正常実行のダイアログに対しては、[OK]を選択します。

3. 起動中に[F2]キーを押し、BIOSを起動して、「BIOS設定」画面で以下を設定してください。

すべての対象サーバーに対して実施してください。

表6.15 BIOS設定(PRIMERGY CX M4、CX M5シリーズの場合)

項目		設定値
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [注]	Power Technology	Custom
	Enhanced Speedstep	Disabled
	Turbomode	Disabled
	Override OS Energy Performance	Enabled
	CPU C1E Support	Disabled
	CPU C6 Report	Disabled
	Package C State limit	C0
Configuration - UEFI Network Stack Configuration [注]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[注]:ISMのプロファイル設定値([詳細]-[BIOS]タブ)に指定している場合には、設定不要です。

表6.16 BIOS設定(PRIMERGY RX M4、RX M5シリーズの場合)

項目		設定値
Server Mgmt - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Advanced - CPU Configuration [注]	Override OS Energy Performance	Enabled
	Energy Performance	Performance
	Package C State Limit	C0
Advanced - Network Stack Configuration [注]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[注]:ISMのプロファイル設定値([詳細]-[BIOS]タブ)に指定している場合には、設定不要です。

表6.17 BIOS設定（PRIMERGY RX M6シリーズの場合）

項目		設定値
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [注]	Enhanced Speedstep	Disabled
	Turbomode	Disabled
	Energy Performance	Performance
	Override OS Energy Performance	Enabled
	CPU C1E Support	Disabled
	CPU C6 Report	Disabled
	Package C State limit	C0
Configuration - UEFI Network Stack Configuration [注]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[注]：ISMのプロファイル設定値（[詳細]-[BIOS]タブ）に指定している場合には、設定不要です。

表6.18 BIOS設定（PRIMERGY RX M7シリーズの場合）

項目		設定値
Management - iRMC LAN Parameters Configuration	iRMC IPv6 LAN Stack	Disabled
Configuration - CPU Configuration [注]	Enhanced Speedstep	Enabled
	Turbomode	Enabled
	Energy Performance	Performance
	Override OS Energy Performance	Enabled
	CPU C1E Support	Enabled
	CPU C6 Report	Enabled
	Package C State limit	C0
Configuration - UEFI Network Stack Configuration [注]	Network Stack	Enabled
	IPv6 PXE Support	Disabled

[注]：ISMのプロファイル設定値（[詳細]-[BIOS]タブ）に指定している場合には、設定不要です。

注意

BIOSの設定が完了したら、「BIOS設定」画面の[Save & Exit]タブの「Save Changes and Exit」または「Commit setting and Exit」を実行し、再度BIOS設定画面が表示されたことを確認してから電源を停止してください。

ISMのノード登録作業時のノード検出方法が手動検出の場合は、引続き「6.8.2.17 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。

ISMのノード登録作業時のノード検出方法が自動検出の場合は、引続き「6.8.3 クラスタ作成またはクラスタ拡張を実行する」を実施してください。

6.8.2.16 ネットワーク表示を確認する

対象の全サーバーに対して、iRMC Web Serverで「ネットワーク」が表示されることを確認します。

iRMC S4の場合

1. Webブラウザーで各サーバーのiRMCのIPアドレスを入力します。

2. ユーザー名／パスワードを入力後、[ログイン]を選択してログインします。

   ユーザー名／パスワードの初期設定は、それぞれ「admin／admin」です。

3. 左ツリーの[システム情報]-[ネットワーク一覧]を選択します。

   「イーサネットポート」欄にネットワークの一覧が表示された場合は問題ありません。

4. 手順3でネットワーク一覧の表示を確認できなかった場合、該当サーバーの電源をONにしてBIOS処理の完了を確認します。その後、電源をOFFにします。

5. 再度ネットワークの表示を確認します。

6. 全サーバーのiRMCに対して、上記手順を実施します。

iRMC S5の場合

1. Webブラウザーで各サーバーのiRMCのIPアドレスを入力します。

2. ユーザー名／パスワードを入力後、[ログイン]を選択してログインします。

   ユーザー名／パスワードの初期設定は、それぞれ「admin／admin」です。

3. [システム]タブを選択し、「ネットワーク」を選択します。

   右側ペインの「ネットワーク」から「イーサネットポート」（iRMC2.20P以降では「ネットワークアダプタ」と表記）を展開してネットワークの一覧が表示された場合は問題ありません。

4. 手順3でネットワーク一覧の表示を確認できなかった場合、該当サーバーの電源をONにしてBIOS処理の完了を確認します。その後、電源をOFFにします。

5. 再度ネットワークの表示を確認します。

6. 全サーバーのiRMCに対して、上記手順を実施します。

iRMC S6の場合

1. Webブラウザーで各サーバーのiRMCのIPアドレスを入力します。

2. ユーザー名／パスワードを入力後、[ログイン]を選択してログインします。

   ユーザー名／パスワードの初期設定は、それぞれ「admin／＜変更後パスワード [注]＞」です。
   [注]：iRMCの初回ログイン時に、工場出荷時パスワード（装置に付帯するタグに記載）から変更を促され、変更したパスワード

3. [システム]タブを選択し、「ネットワーク」を選択します。

   右側ペインの「ネットワーク」から「ネットワークアダプタ」を展開してネットワークの一覧が表示された場合は問題ありません。

4. 手順3でネットワーク一覧の表示を確認できなかった場合、該当サーバーの電源をONにしてBIOS処理の完了を確認します。その後、電源をOFFにします。

5. 再度ネットワークの表示を確認します。

6. 全サーバーのiRMCに対して、上記手順を実施します。

6.8.2.17 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、対象サーバーを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。

すべての対象サーバーを登録してください。

ポイント

- ISMのノード登録時は、対象サーバーの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。iRMC S6の場合では、それぞれ「admin／＜変更後パスワード [注]＞」です。
  [注]：iRMCの初回ログイン時に、工場出荷時パスワード（装置に付帯するタグに記載）から変更を促され、変更したパスワード

- 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導入時に必要な設定を行う」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。

「ノード手動登録」ウィザードでiRMCの固定IPアドレスを設定してください。

登録の際に指定するIPアドレスは、「6.8.2.14 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。

引続き「6.8.3 クラスタ作成または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。

IPアドレスの範囲を指定することですべての対象サーバーを同時に登録できます。

引続き「6.8.2.15 BIOSを設定する」を実施してください。

6.8.3 クラスタ作成またはクラスタ拡張を実行する

クラスタ作成機能またはクラスタ拡張機能を実行してPRIMEFLEX HS／PRIMEFLEX for VMware vSANのリソースを増やします。

クラスタ作成機能またはクラスタ拡張機能を実行前に「6.8.1 動作要件」を参照して、動作要件を必ず確認してください。

- 6.8.3.1 クラスタ作成手順
- 6.8.3.2 クラスタ拡張手順

6.8.3.1 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

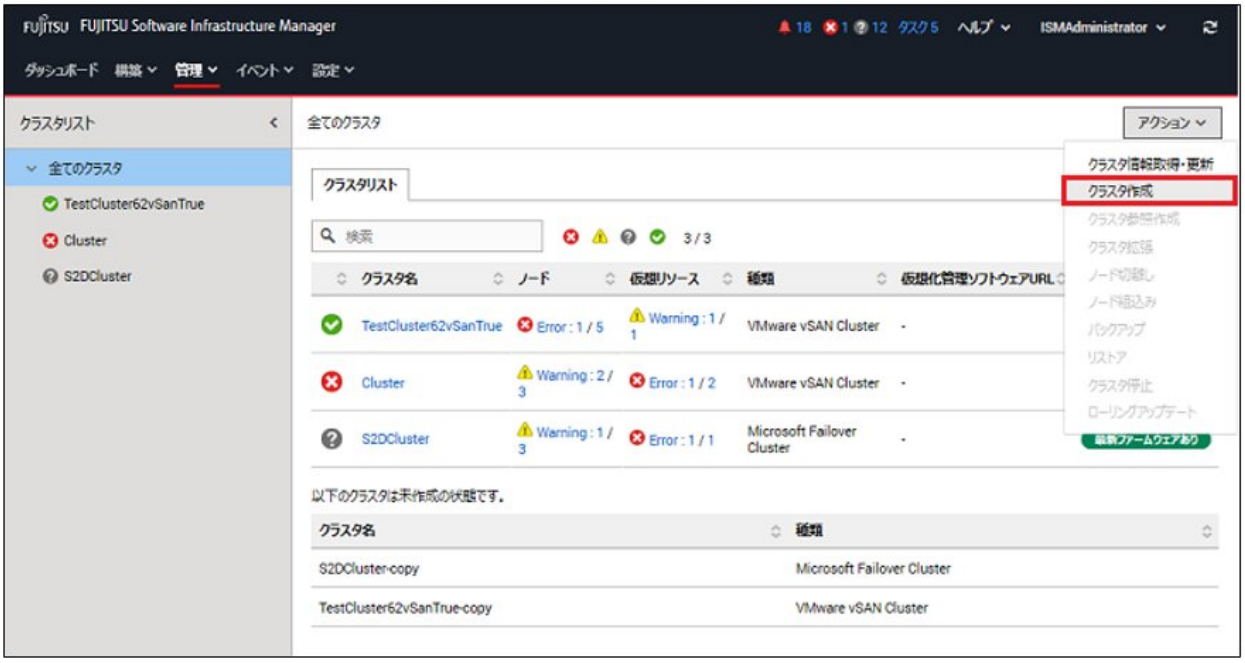
ISM for PRIMEFLEXの他の機能が実行中にクラスタ作成機能を実行しないでください。クラスタ作成機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

1. ISM管理者（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。
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。

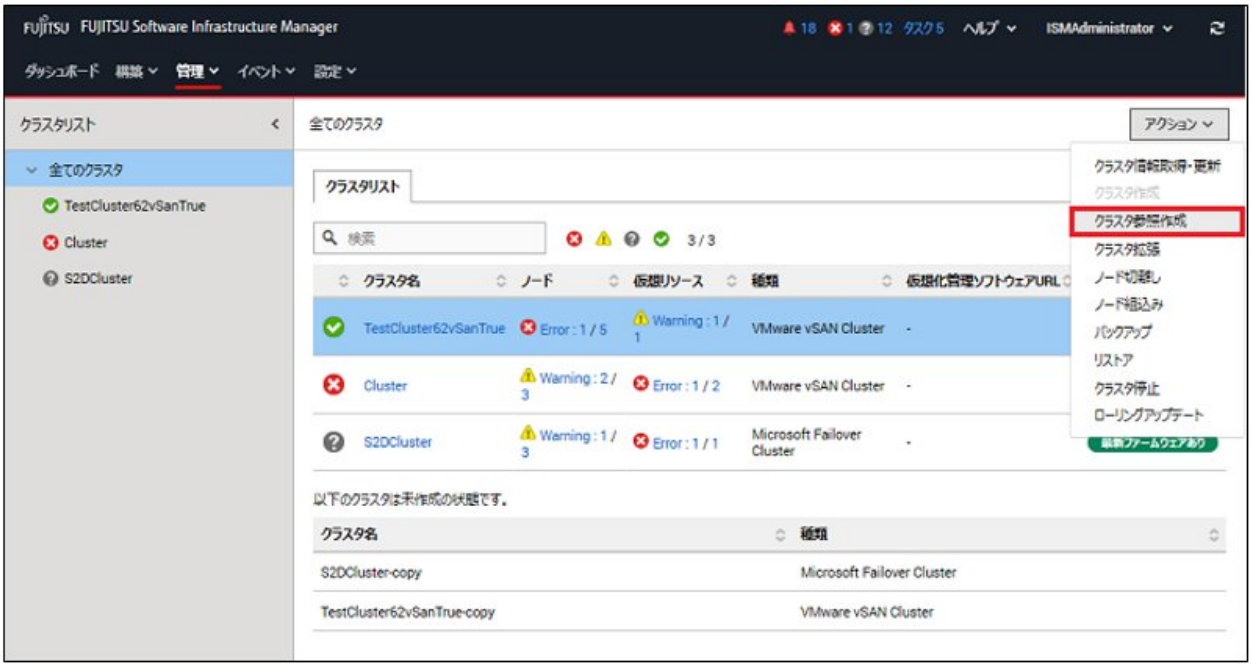
   「クラスタリスト」画面が表示されます。

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。

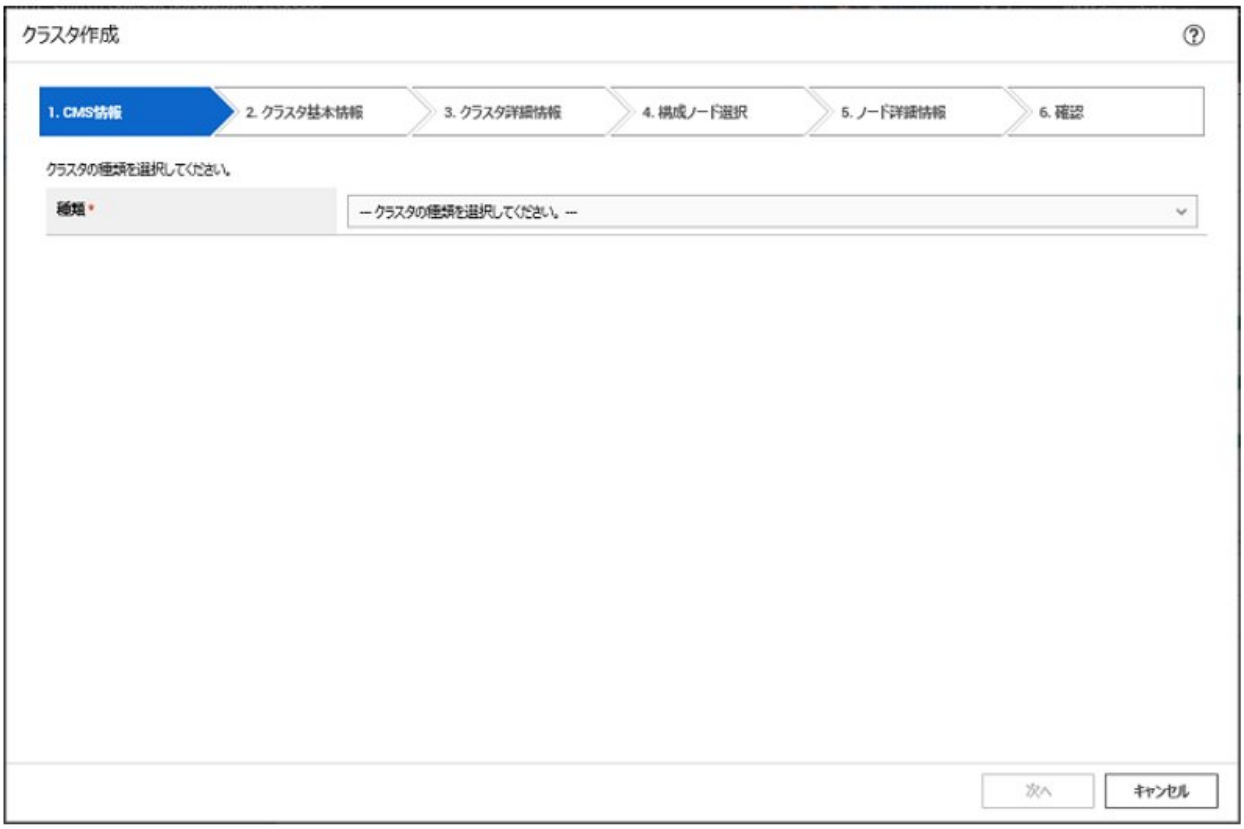


注意

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。

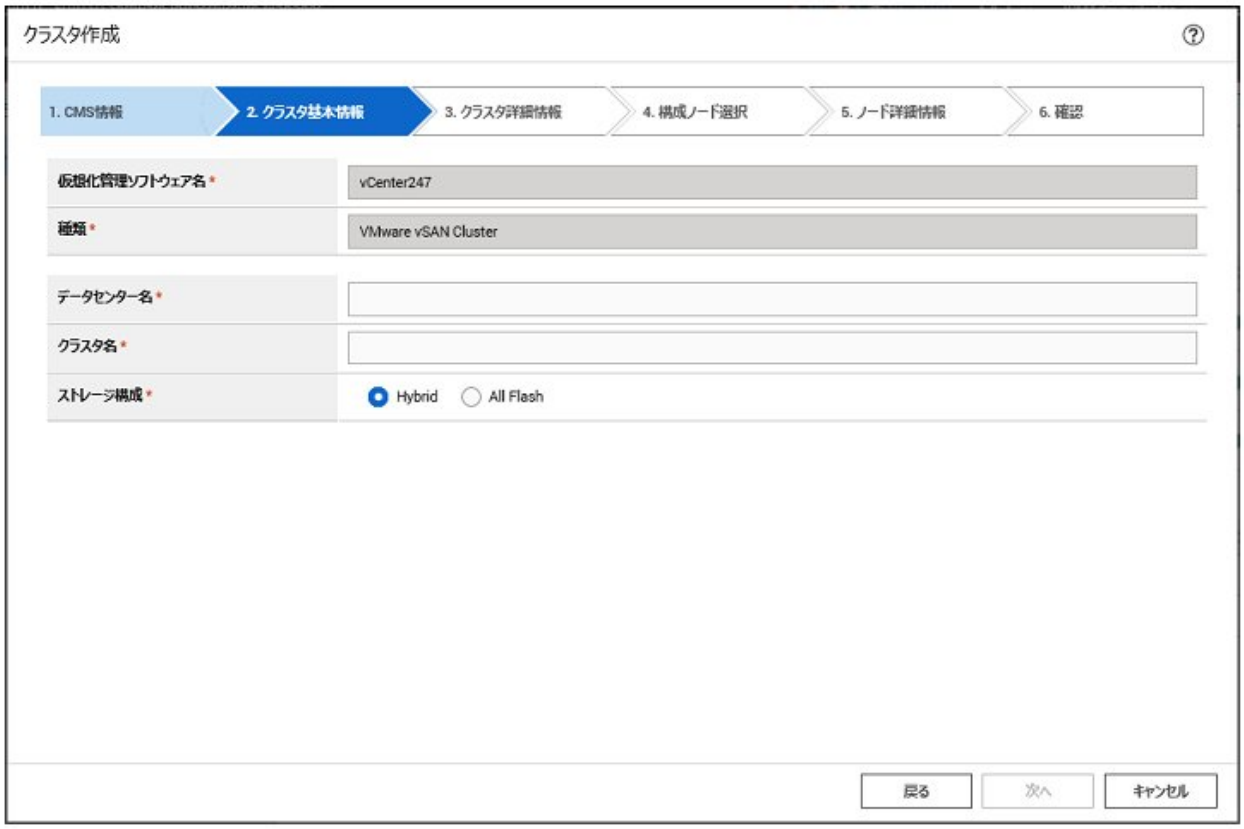
4. 「1. CMS情報」画面の各種パラメーターを入力し、[次へ]ボタンを選択します。

   エラーにより停止したクラスタ作成機能を再実行する場合、パラメーターの再入力が不要であれば、[次へ]ボタンを選択して、手順5に進んでください。



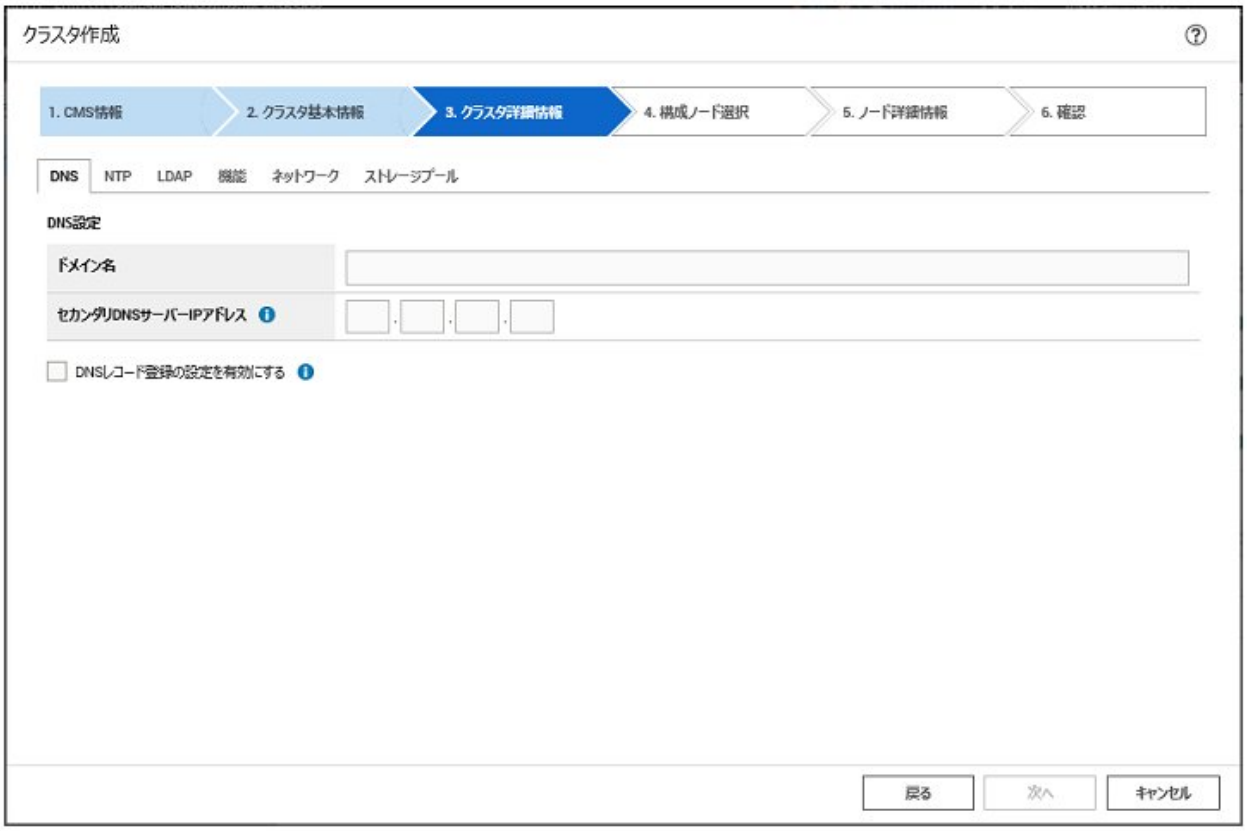
5. 「2.クラスタ基本情報」画面の各種パラメーターを入力し、[次へ]ボタンを選択します。

   エラーにより停止したクラスタ作成機能を再実行する場合、パラメーターの再入力が不要であれば、[次へ]ボタンを選択して、手順6に進んでください。

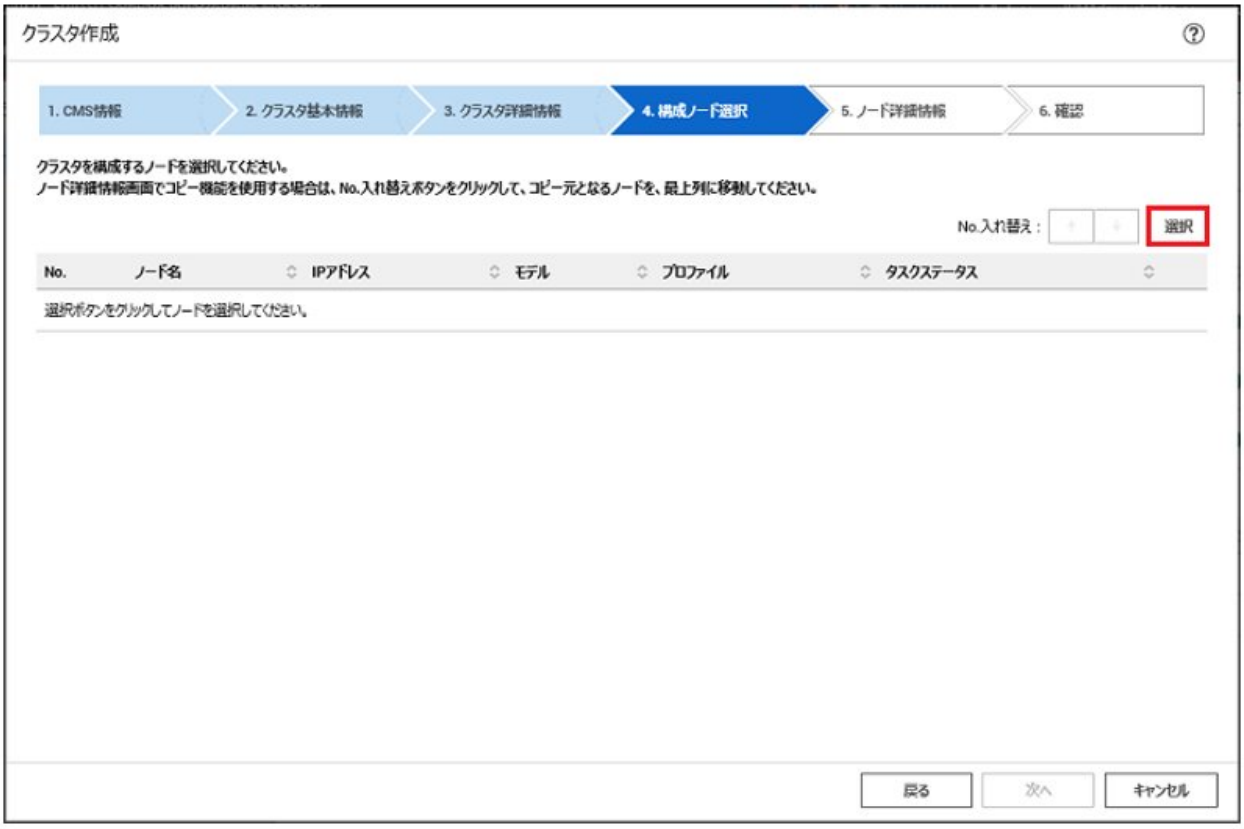


6. 「3.クラスタ詳細情報」画面の各種パラメーターを入力し、[次へ]ボタンを選択します。

   エラーにより停止したクラスタ作成機能を再実行する場合、パラメーターの再入力が不要であれば、[次へ]ボタンを選択して、手順7に進んでください。



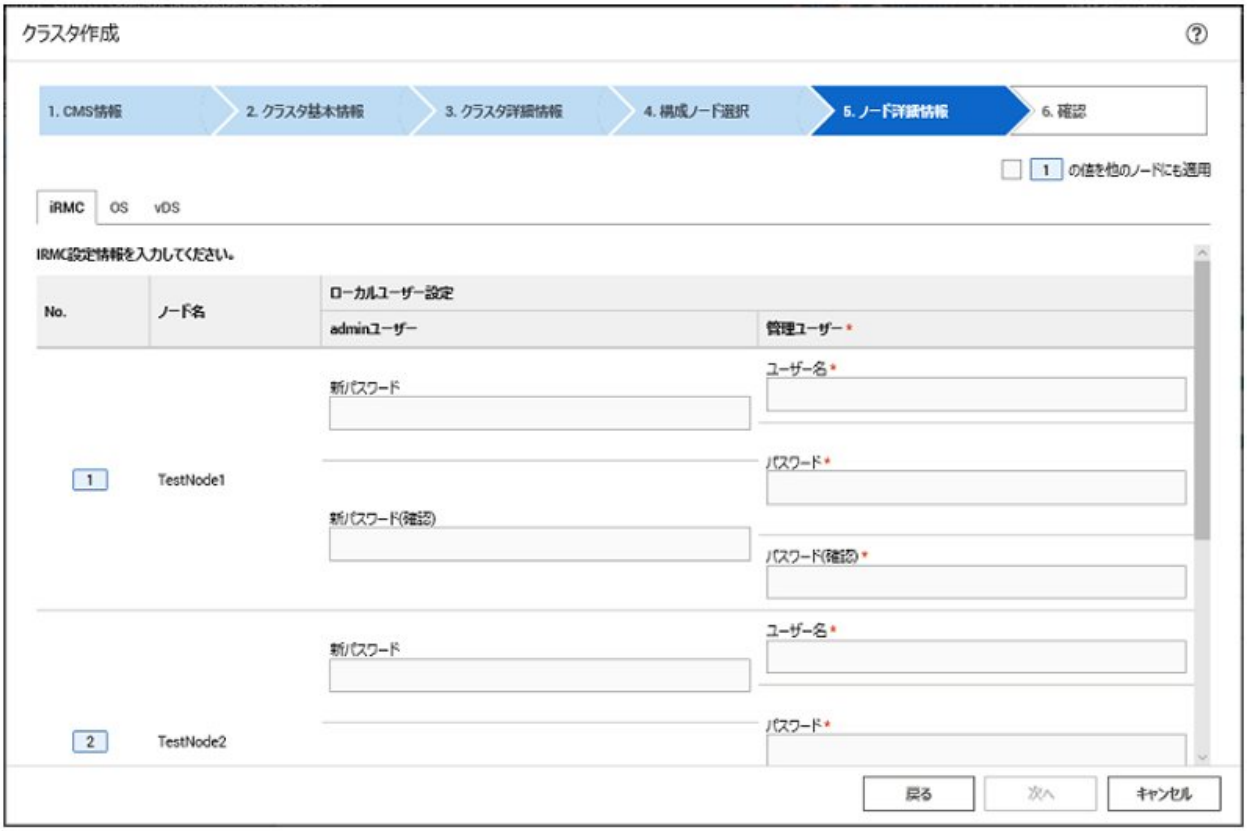
7. 「4.構成ノード選択」画面の[選択]ボタンを選択して、表示された「対象ノードの選択」画面で、対象サーバーを選択します。
   エラーにより停止したクラスタ作成機能を再実行する場合、本手順は不要です。[次へ]ボタンを選択して、手順9に進んでください。



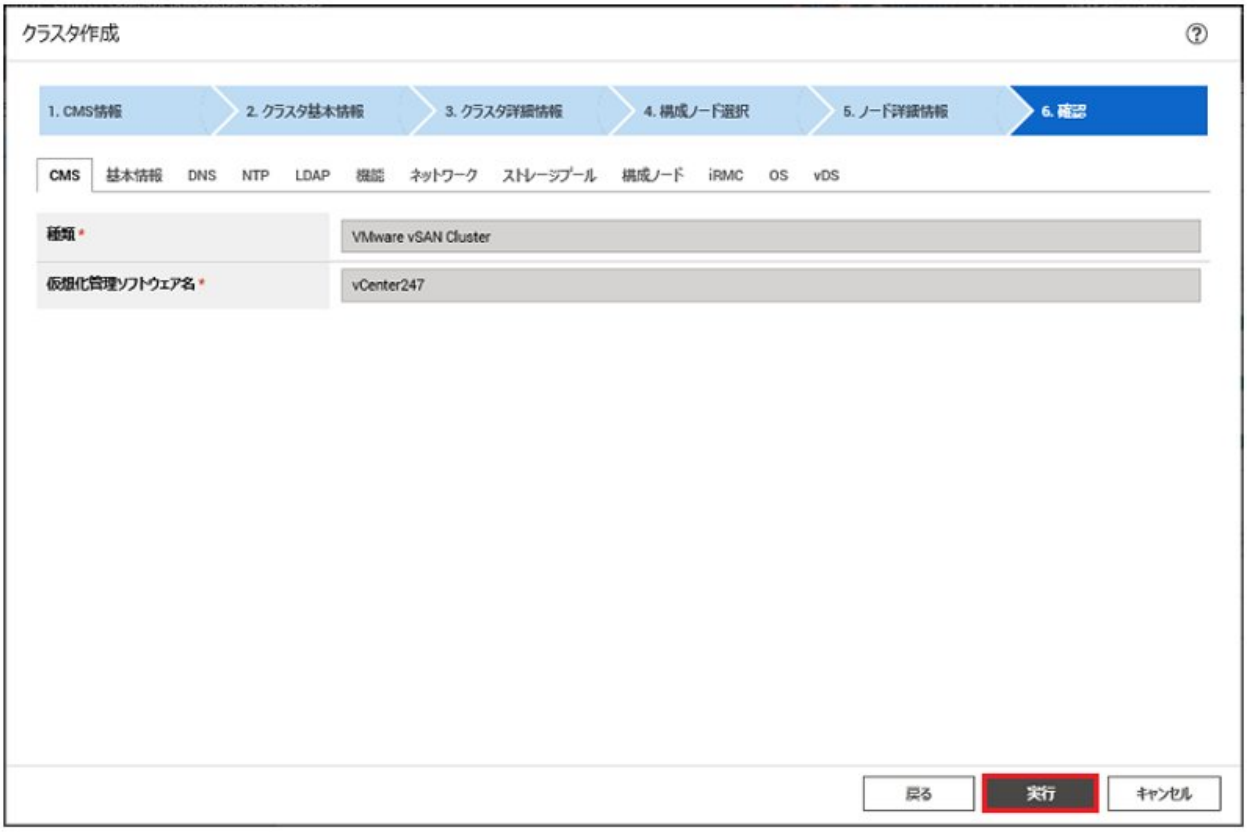
8. 対象サーバーがプロファイル未適用の場合は、[プロファイル]の項目にある[選択]ボタンを選択し、適用対象のプロファイルを選択して[次へ]ボタンを選択します。

9. 「5.ノード詳細情報」画面の各種パラメーターを入力し、[次へ]ボタンを選択します。

   エラーにより停止したクラスタ作成機能を再実行する場合、パラメーターの再入力が不要であれば、[次へ]ボタンを選択して、手順10に進んでください。



10. 「6.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。



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。

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、対象サーバー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。

11. 「Cluster Creation」のステータスが「完了」になったことを確認します。
12. 「vSAN構成の更新」と「vSphere HA設定」の処理が完了したことを確認します。

    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「6.8.4 事後処理」に進んでください。

    vCSA 6.5以前（Flash）の場合：

    vSphere Web ClientでvCSAにログインして、「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。

    vCSA 6.7以降（HTML5）の場合：

    vSphere ClientでvCSAにログインして、「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

注意

- ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  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、再実行時には対象サーバーの電源はオフにしないでください。

- 対象サーバー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。
- VMware ESXiパッチ適用前後で実行するスクリプトを作成し、ISMの「タスク」画面にエラーが表示された場合は、「6.8.4.2 スクリプトの実行結果を確認する」を参照して、スクリプトの実行結果を確認してください。

  また、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

6.8.3.2 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。

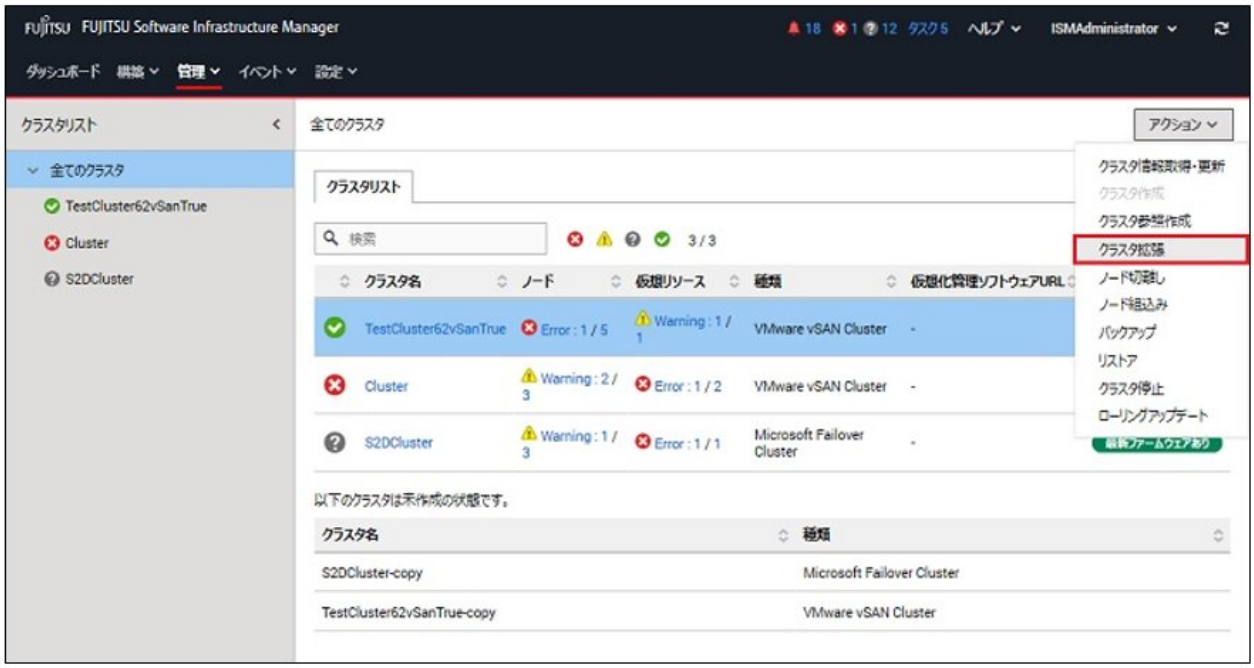
注意

ISM for PRIMEFLEXの他の機能が実行中にクラスタ拡張機能を実行しないでください。クラスタ拡張機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

1. ISM管理者（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。
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。

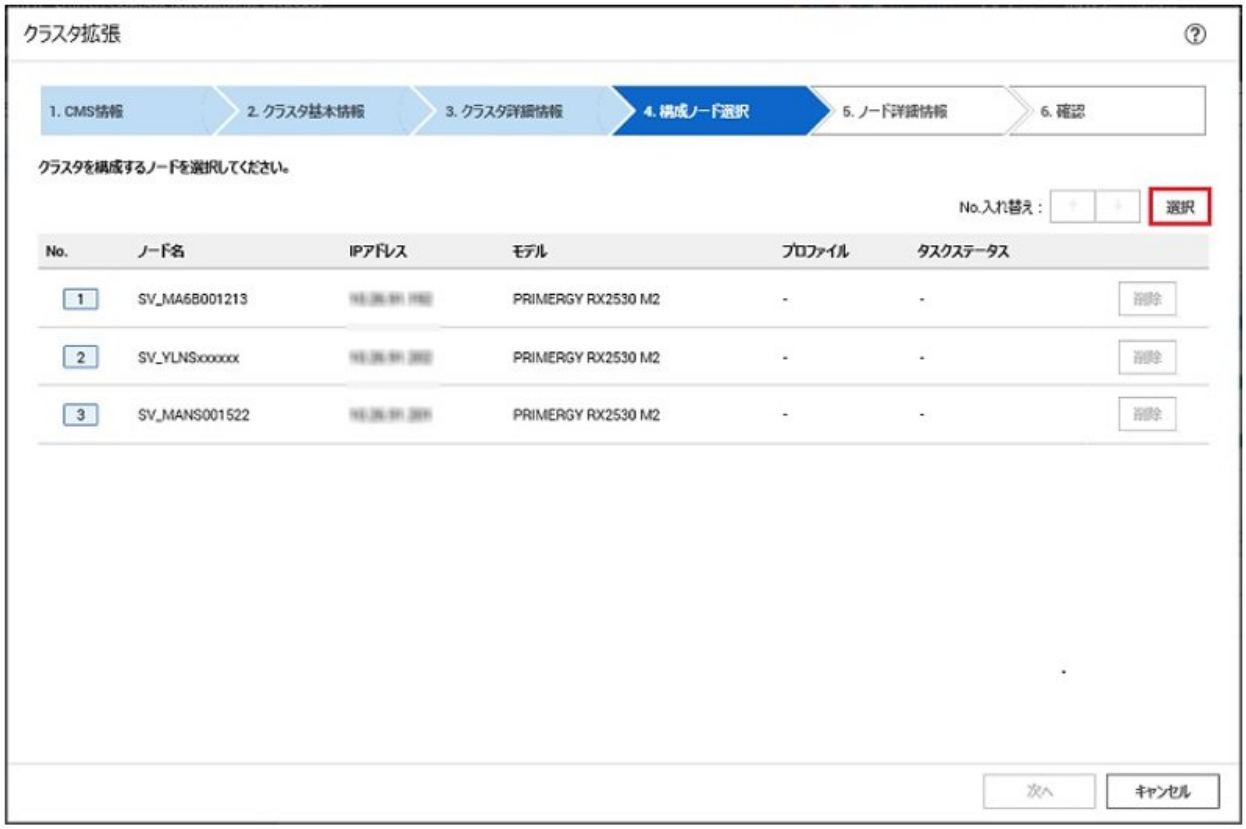
   「クラスタリスト」画面が表示されます。
3. [＜対象のクラスタ＞]を選択して、[アクション]ボタンから[クラスタ拡張]を選択します。



「クラスタ拡張」ウィザードが表示されます。

4. 「4.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、対象サーバーを選択します。

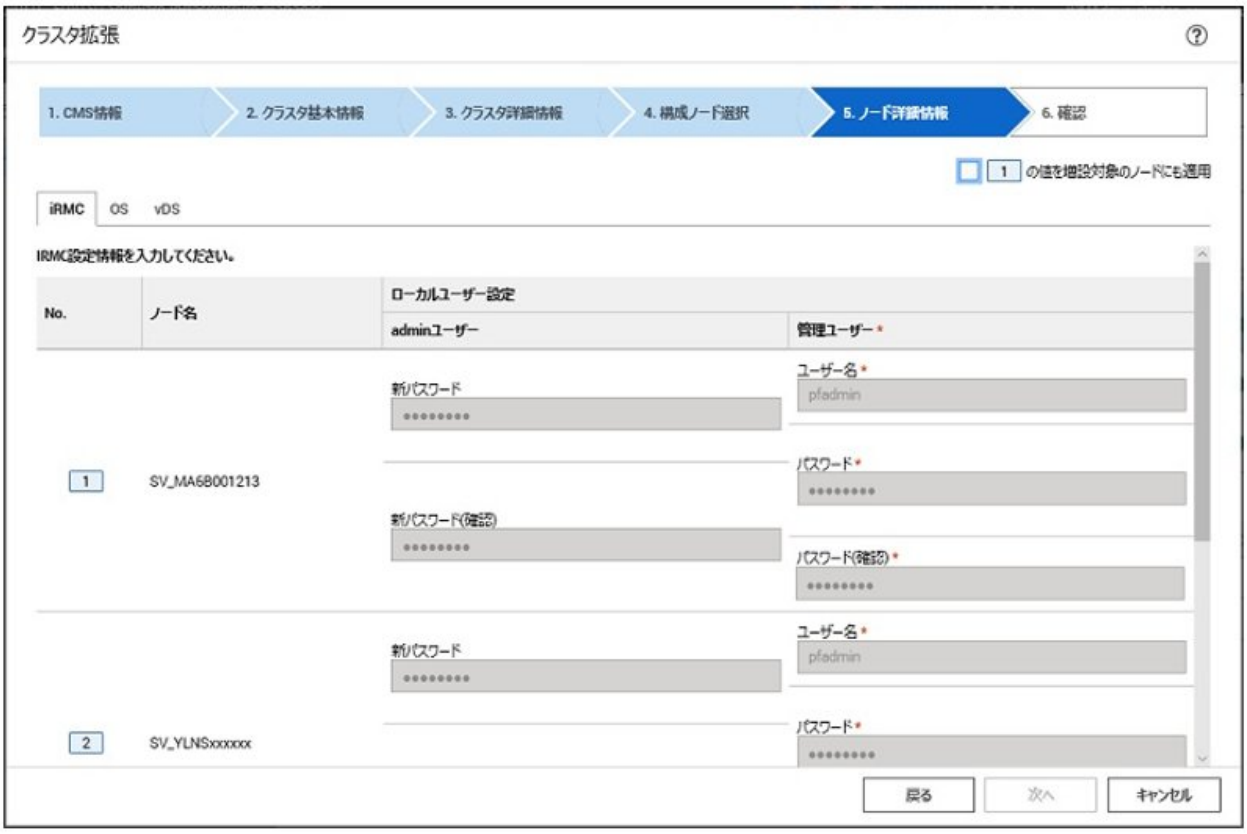
   エラーにより停止したクラスタ拡張機能を再実行する場合、本手順は不要です。[次へ]ボタンを選択して、手順6に進んでください。



5. 対象サーバー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、適用対象のプロファイルを選択して[次へ]ボタンを選択します。

6. 「5.ノード詳細情報」画面で対象サーバーの各種パラメーターを入力し、[次へ]ボタンを選択します。

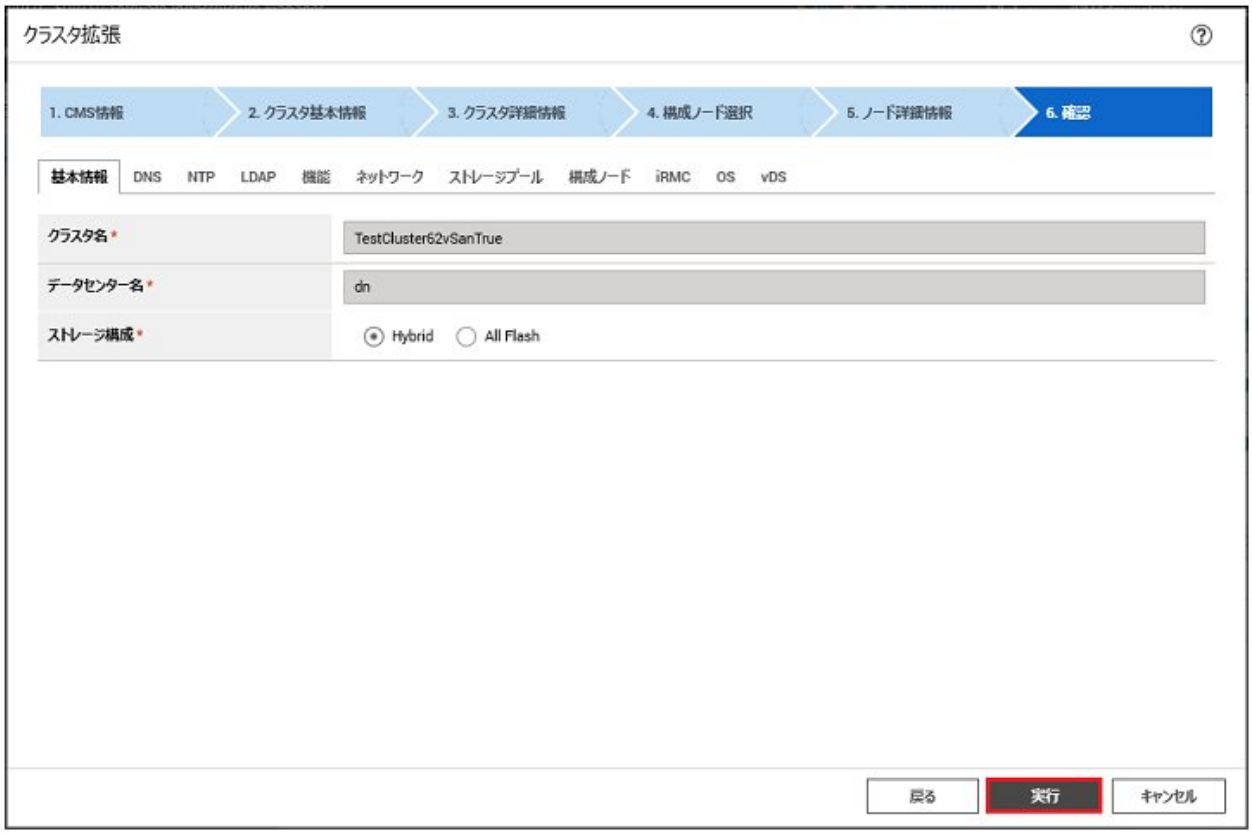
   エラーにより停止したクラスタ拡張機能を再実行する場合、パラメーターの再入力が不要であれば、[次へ]ボタンを選択して、手順7に進んでください。



注意

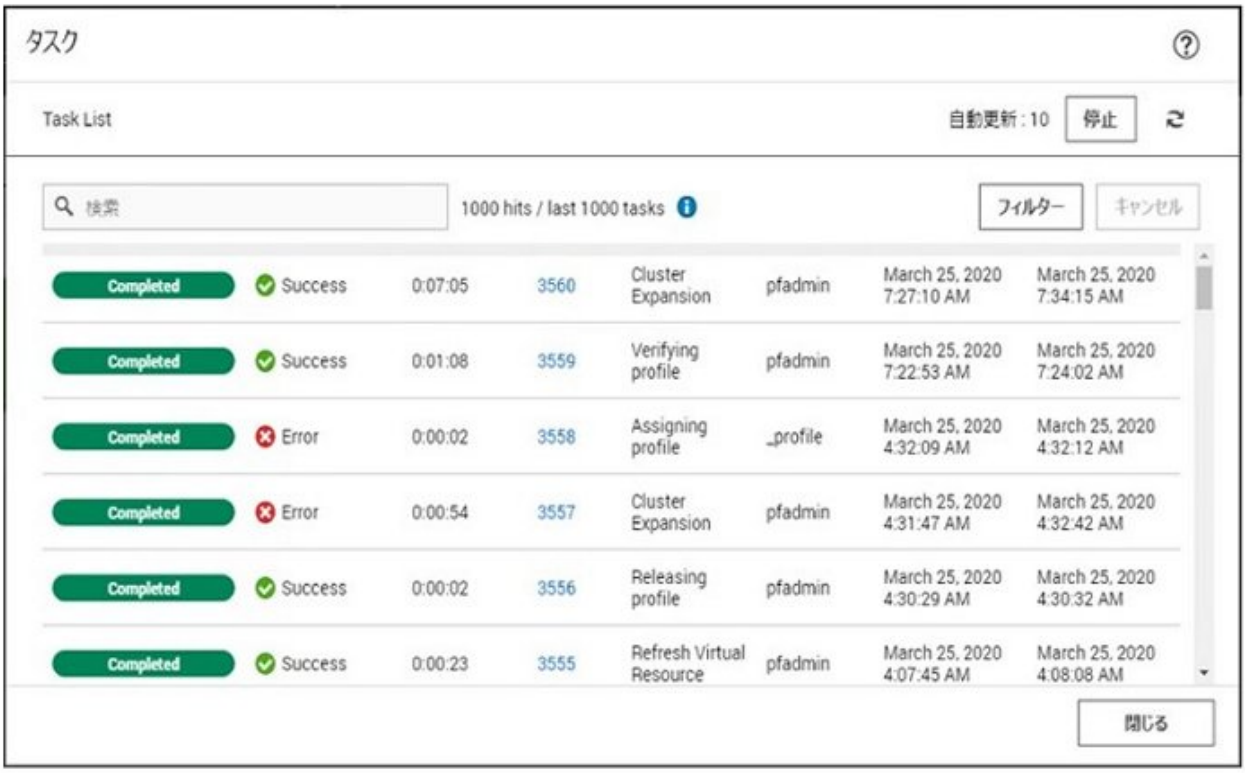
クラスタ定義パラメーターの詳細については、『ISM for PRIMEFLEX 設定値一覧』の「第3章 クラスタ定義パラメーターの設定値一覧」を参照してください。

7. 「6.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。



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。



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、対象サーバー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。

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のイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  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、再実行時には対象サーバーの電源はオフにしないでください。

- 対象サーバー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。
- VMware ESXiパッチ適用前後で実行するスクリプトを作成し、ISMの「タスク」画面にエラーが表示された場合は、「6.8.4.2 スクリプトの実行結果を確認する」を参照して、スクリプトの実行結果を確認してください。

  また、『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

6.8.4 事後処理

クラスタ作成またはクラスタ拡張の事後処理について説明します。

6.8.4.1 リソースを確認する

以下の手順でvSANクラスタを確認してください。

1. 以下の点を確認します。

   vCSA 6.5以前（Flash）の場合：

   vSphere Web ClientでvCSAにログインして、以下を確認します。

   ー 「トップ」画面から[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

   ー 「トップ」画面から[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]で対象サーバーのディスクが表示されること

   ー 「トップ」画面から[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]で再テストを実行し、問題のないこと

   vCSA 6.7以降（HTML5）の場合：

   vSphere ClientでvCSAにログインして、以下を確認します。

   ー 「トップ」画面から[ショートカット]-[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

   ー 「トップ」画面から[ショートカット]-[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]で対象サーバーのディスクが表示されること

     vCSA 7.0U3以降の場合は、以下の表示結果を確認してください。

     「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[構成]-[vSAN]-[ディスク管理]表示後、対象サーバーを選択して、[ディスクの表示]を表示。

   ー 「トップ」画面から[ショートカット]-[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]-[Skyline健全性]または[Skyline Health]で再テストを実行し、問題のないこと

   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表示され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。

vSAN6.7U3環境（VMware ESXi 6.7 Update 3）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 ディスクバランス

  ディスクのプロアクティブリバランスを実行してください。

  vCSA 7.0以降の場合は、自動リバランスの設定を実行してください。

ー コントローラドライバーが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ー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（VMware Infrastructure Bundle）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

vCSA 6.5以前（Flash）の場合：

「トップ」画面から[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]-[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]で対象サーバーのフォールトドメインホストを確認します。

vCSA 6.7以降（HTML5）の場合：

「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定 [注]]-[vSAN]-[フォールトドメイン]-[フォールトドメイン]で対象サーバーのフォールトドメインホストを確認します。

[注]:vCSA 7.0 U3以降の場合、[構成]と表示されます。

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]-[コンピューター名をDNSサーバーから取得]-[コンピューター名]が既存クラスタ、または対象サーバーのコンピューター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、以下を参照して、対処してください。

- クラスタ作成の場合

  『ISM for PRIMEFLEX メッセージ集』の「3.2 クラスタ作成エラー時の対処例」の「対処例23」

- クラスタ拡張の場合

  『ISM for PRIMEFLEX メッセージ集』の「3.1 クラスタ拡張エラー時の対処例」の「対処例19」

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]-[仮想リソース]を選択します。

   「全てのストレージプール」画面が表示されます。

3. [アクション]ボタンから[仮想リソース情報の更新]を選択します。

   情報が更新されます。

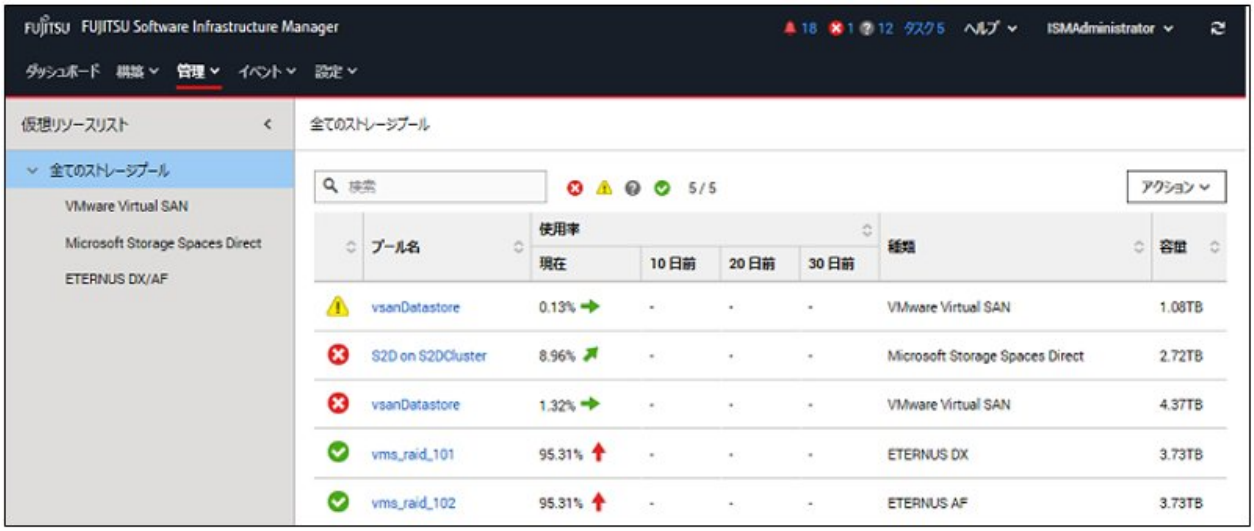
4. 情報更新後、以下を確認します。

   - クラスタ作成の場合

     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。

   - クラスタ拡張の場合

     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。



注意

クラスタ作成またはクラスタ拡張のタスクが正常に完了したにも関わらず、以下の現象が発生することがあります。

- vSANストレージが表示されない
- vSANストレージ容量が想定している容量より少ない
- 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

上記の場合、vSANネットワーク用の通信ができていないことが原因として考えられます。スイッチの設定や結線を確認してください。

6.8.4.2 スクリプトの実行結果を確認する

「6.8.2.8 VMware ESXiパッチ適用前後で実行するスクリプトを必要に応じて作成する」で作成したスクリプトの実行結果を出力したログなどで確認してください。

スクリプトの実行に成功していた場合は、ログファイルに以下のメッセージが出力されています。

VMware ESXiのパッチ適用前に実行するスクリプト(例:/scratch/log/pre_script.log)に以下のメッセージが出力されます。

```
pre_script End
```

VMware ESXiのパッチ適用時に実行するスクリプト(例:/scratch/log/post01_script.log)に以下のメッセージが出力されます。

```
post01_script End
```

VMware ESXiのパッチ適用後に実行するスクリプト(例:/scratch/log/post02_script.log)に以下のメッセージが出力されます。

```
post02_script End
```

スクリプトの実行に失敗していた場合は、スクリプトのログを確認してエラーの対処をしてください。エラーの対処後にスクリプトの内容を手動で実行して、『VMware vSphere X.X ソフトウェア説明書』(Xには、バージョンが入ります。)の注意事項の対処を完了させてください。

注意事項の対処は、以下のサイトを参照して、『VMware vSphere X.X ソフトウェア説明書』に記載されている手順を実行してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

6.8.4.3 VMware vSphereの制限事項／注意事項

以下のサイトを参照して、『VMware vSphere X.X ソフトウェア説明書』(Xには、バージョンが入ります。)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。

すべての対象サーバーに対して実施してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/

6.8.4.4 vCLS仮想マシンのデータストアを確認して移動する

vCSA 7.0 U1以降でクラスタ作成を行った場合に必要な作業です。

vCSAを7.0 U1以降でクラスタを作成するとvSphereクラスタサービス(vCLS)が有効になり、クラスタにvCLS仮想マシンが作成されます。
vCLS仮想マシンは、クラスタに最大で3台作成されます。

このvCLS仮想マシンがローカルデータストアに作成された場合は、vSANデータストアへ移動する必要があります。

対象クラスタで実施してください。

ポイント

vCSAにログインするユーザー種別によってはvSphereクラスタサービス(vCLS)が表示されない場合があります。
vSphereクラスタサービス(vCLS)関連の操作を行う際には、vCenter Single Sign-Onドメインの管理者を使用してください。

vCLS仮想マシンが配置されているデータストアの確認手順

vCLS仮想マシンが配置されているデータストアを確認します。

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
   - vCSA 7.0U2以前の場合:

     ＜vCLS名＞は、"vCLS (n)"(nは数字)で表示されます。
   - vCSA 7.0U3以降の場合:

     ＜vCLS名＞は、"vCLS-XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX"(Xは16進数)で表示されます。
3. [データストア]-[名前] がvSANデータストア名であることを確認します。

   vSANデータストア名は、ISMのGUIで対象クラスタのクラスタ定義パラメーターの[クラスタ詳細情報]-[ストレージプール]タブの[ストレージプール名]で確認できます。

vSANデータストア名ではない場合、「vSANデータストアへの移動手順」を実施します。

4. すべてのvCLS仮想マシンに対して、手順2～3を実施します。

vSANデータストアへの移動手順

vCLS仮想マシンをvSANデータストアへ移動します。

vCSA 7.0U2以前の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[仮想マシン]-[仮想マシン]-[＜vCLS名＞]を選択します。
3. [アクション]-[移行]を選択します。

   確認画面が表示されます。
4. 確認画面で[はい]を選択します。

   「移行」画面が表示されます。
5. [1 移行タイプの選択]で「ストレージのみ変更します」を選択して、[NEXT]ボタンを選択します。
6. [2 ストレージの選択]でvSANデータストアを選択して、[NEXT]ボタンを選択します。

   vSANデータストアは、[タイプ]の「vSAN」で確認できます。
7. [3 設定の確認]で設定内容を確認して、[FINISH]ボタンを選択します。

vCSA 7.0U3以降の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[ホストおよびクラスタ]の[＜クラスタ名＞]を選択します。
3. [構成]-[vSphere クラスタ サービス]-[データストア]-[追加]を選択します。

   データストアの追加画面が表示されます。
4. データストアの追加画面でvSANデータストアを選択して、[追加]を選択します。

6.8.4.5 ServerView RAID Managerに対象サーバーを登録する

SSDの寿命監視をするために、ServerView RAID Managerに対象サーバーを登録します。

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ー

また、対象サーバーでSASコントローラカード（CP400i、CP403i、CP503i）を使用している場合に必要な作業です。

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. すべての対象サーバーの台数分、以下のコマンドを実行します。

```
>amCLI -e 21/0 add_server name=＜対象サーバー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すべての対象サーバー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]を選択します。
5. [ServerView RAID Manager]を右クリックし、[再起動]を選択します。

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、すべてのサーバーが表示されます。

   すべてのサーバーの状態が正常であることを確認します。

6.8.4.6 不要なファイルを削除する

クラスタ作成または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。

(1)証明書の削除

「6.8.2.2 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

「6.8.2.2 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。

(2)ISM-VAの不要なファイルの削除

ISM-VAに対して実施してください。

1. ISM管理者(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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/kickstart
ファイル名	・「6.8.2.7 VMware ESXiパッチをアップロードする」のVMware ESXiパッチファイル ・「6.8.2.9 VMware SMIS Providerをアップロードする」のVMware SMIS Providerのオフラインバンドル

(3)VMware ESXiパッチ適用前後で実行するスクリプトを削除する

ISM-VAに対して実施してください。

1. ISM管理者(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。
2. 以下の項目を確認しながら、「1.4.2 ISM-VAにアップロードしたファイルを削除する」を参照して、不要なファイルを削除してください。

項目	値
ルートディレクトリー	Administrator/ftp
ディレクトリー名	Administrator/ftp/ClusterOperation/ESXi/script
ファイル名	「6.8.2.8 VMware ESXiパッチ適用前後で実行するスクリプトを必要に応じて作成する」のVMware ESXiパッチ適用前後で実行するスクリプト

6.8.4.7 VMware EVCモードの設定を確認する

クラスタ拡張機能を行った場合に必要な作業です。クラスタ作成機能を行った場合には不要です。

VMware EVCモードが設定されていることを確認してください。

確認手順は、「6.8.2.1 vCenter ServerのVMware EVCを設定する」を参照してください。

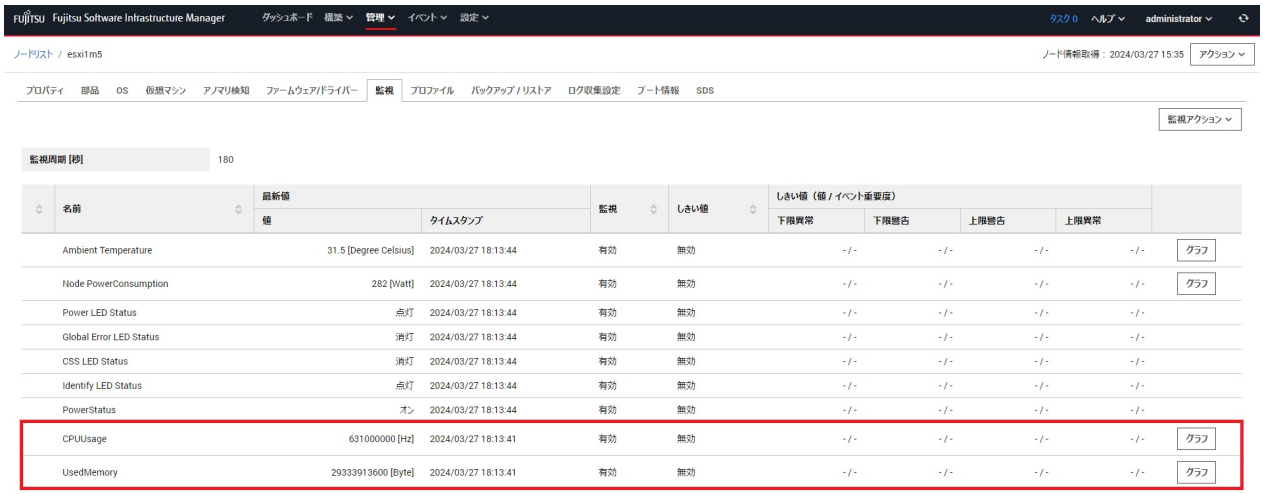
設定されていない場合は、vCSAをvSANクラスタ外へ移行し、vSANクラスタ上の仮想マシンをすべて停止してから、「6.8.2.1 vCenter ServerのVMware EVCを設定する」を参照して、VMware EVCモードを設定してください。

6.8.4.8 対象サーバーに監視項目設定を行う

クラスタ作成またはクラスタ拡張を行った各ノードに対して行う作業です。

ノードの監視項目として[CPUUsage]と[UsedMemory]を設定します。

1. ISM管理者（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。
2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。
「ノードリスト」画面が表示されます。
3. ノードリストから設定対象のノードを選択します。
4. [監視]タブ内の[監視アクション]ボタンから[追加]を設定します。
5. [監視項目追加]画面で監視項目名[CPUUsage]を選択し、[次へ]ボタン選択します。
既に監視項目として[CPUUsage]が追加されている場合、[監視項目追加]画面に[CPUUsage]は表示されません。
その場合、手順7に進んでください。
6. 表示された画面で、[監視項目の設定内容]と[しきい値（値 / イベント重要度）]に対して任意の設定値を入力し、[追加]ボタンを選択します。
7. [監視]タブ内の[監視アクション]ボタンから[追加]を設定します。
8. [監視項目追加]画面で監視項目名[UsedMemory]を選択し、[次へ]ボタン選択します。
既に監視項目として[UsedMemory]が追加されている場合、[監視項目追加]画面に[UsedMemory]は表示されません。
その場合、手順10に進んでください。
9. 表示された画面で、[監視項目の設定内容]と[しきい値（値 / イベント重要度）]に対して任意の設定値を入力し、[追加]ボタンを選択します。
10. 対象ノードの[監視]タブ画面に[CPUUsage]と[UsedMemory]が表示されることを確認します。



11. クラスタ作成またはクラスタ拡張を行った全てのノードに対して手順1～10を実施します。

6.9 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

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の動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

6.9.1 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。

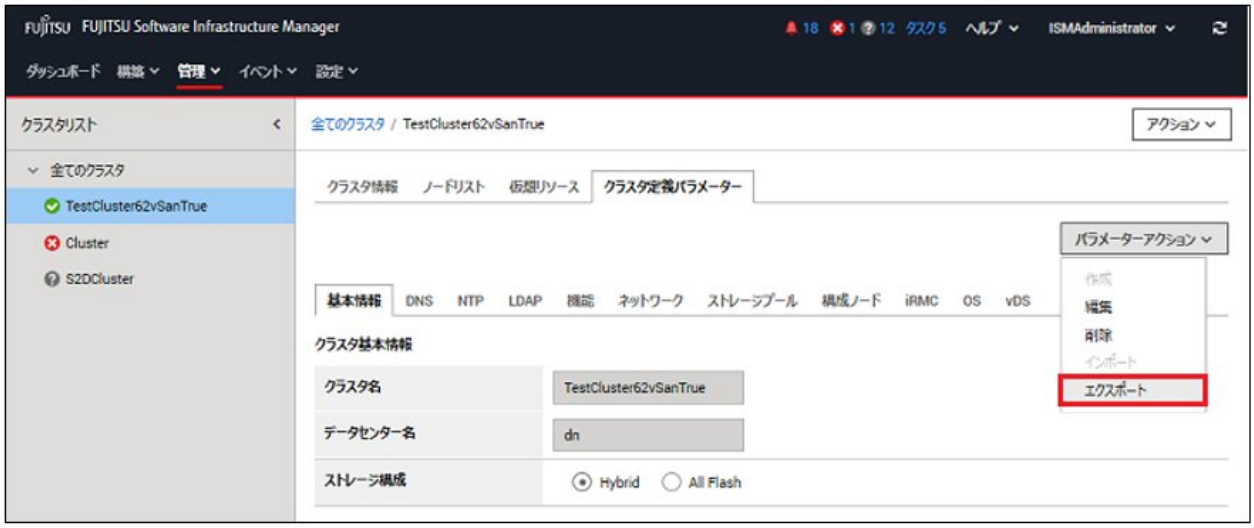
1. ISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）でISMにログインします。

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。

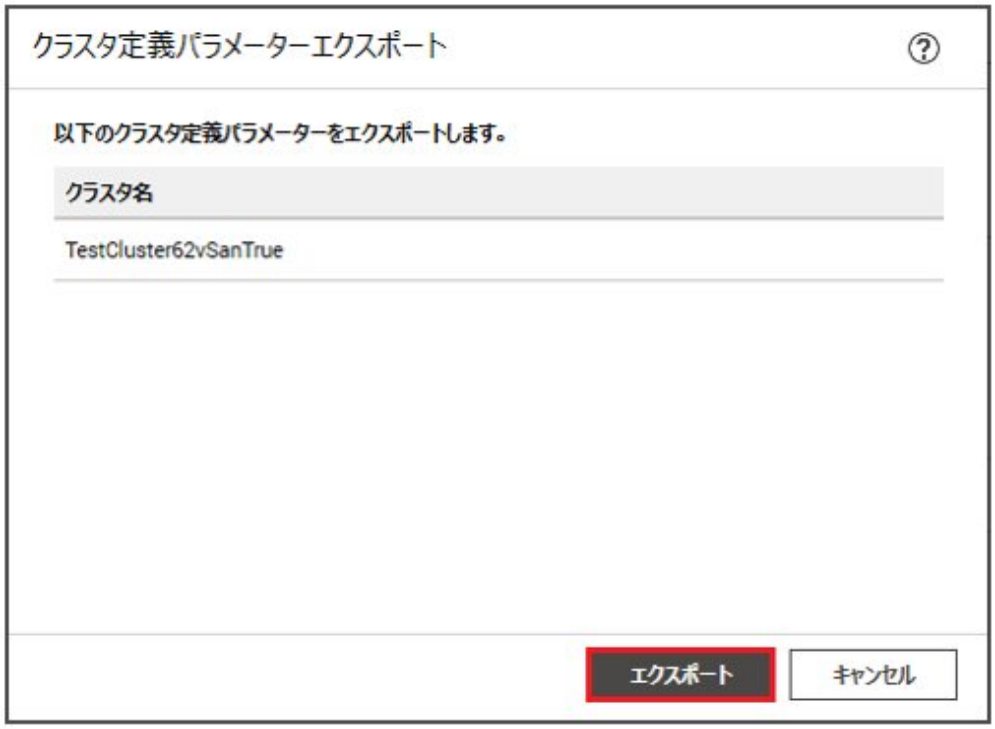
   「クラスタリスト」画面が表示されます。

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。

ファイルのダウンロードが完了したら、クラスタ定義パラメーターのエクスポートは完了です。

6.9.2 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

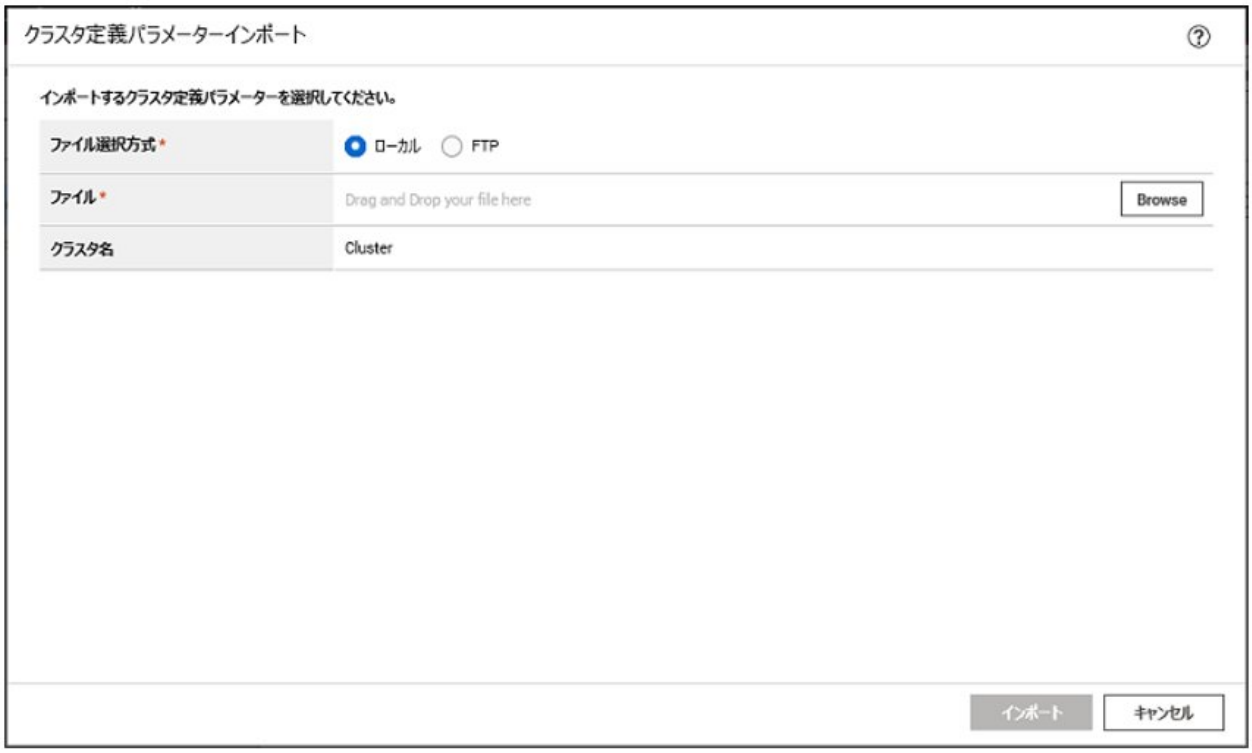
- インポート対象のクラスタにクラスタ定義パラメーターがすでに作成されている場合は、インポートできません。事前にクラスタ定義パラメーターを削除してください。
- インポート先として使用できるISM-VAの条件は、以下のとおりです。以下以外のISM-VAに対するインポートは未サポートです。
  - ー クラスタ定義パラメーターをエクスポートした環境であること
  - ー クラスタを構成するノードのノード情報やプロファイルを削除／再登録していない環境であること

1. ISM管理者（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。
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。

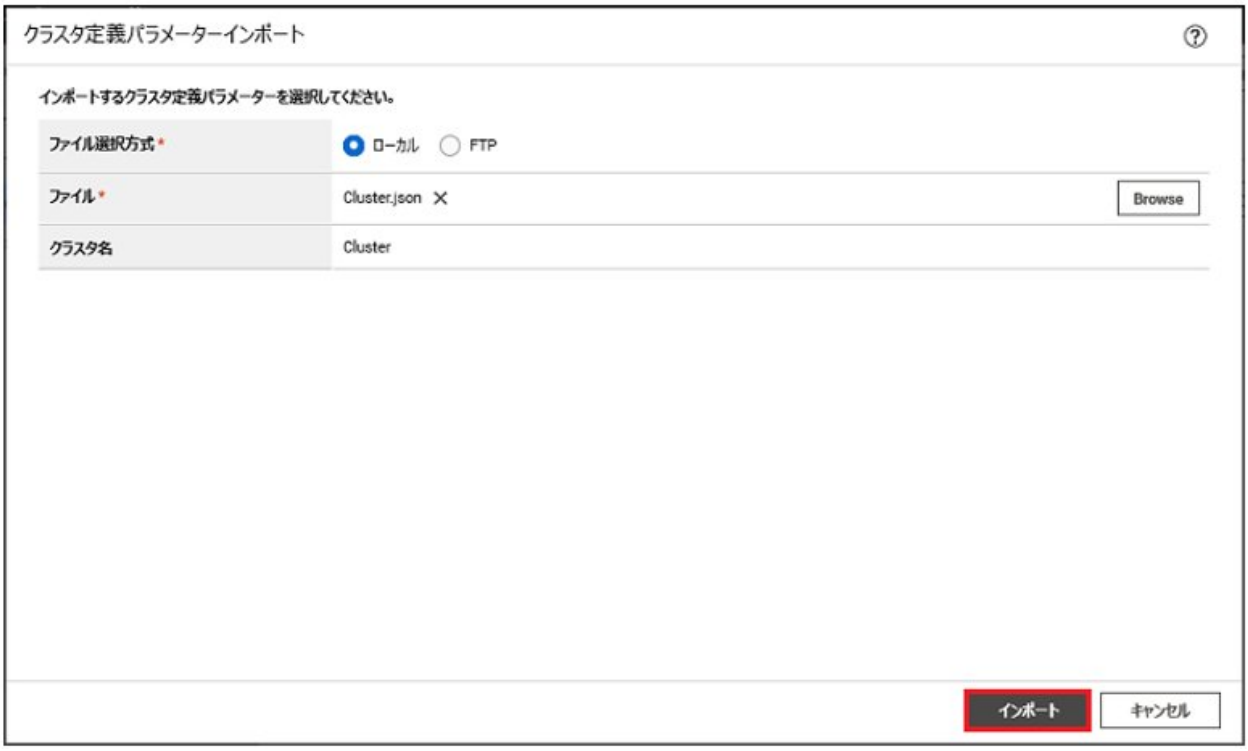
   「クラスタリスト」画面が表示されます。
3. インポート対象の[＜対象のクラスタ＞]-[クラスタ定義パラメーター]タブを選択します。

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。



6. [インポート]ボタンを選択します。



7. 「クラスタリスト」画面でインポート対象の[＜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。クラスタ定義パラメーターが表示されたら、クラスタ定義パラメーターのインポートは完了です。

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。

   パスワードはエクスポートされません。設定値を入力してください。

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。

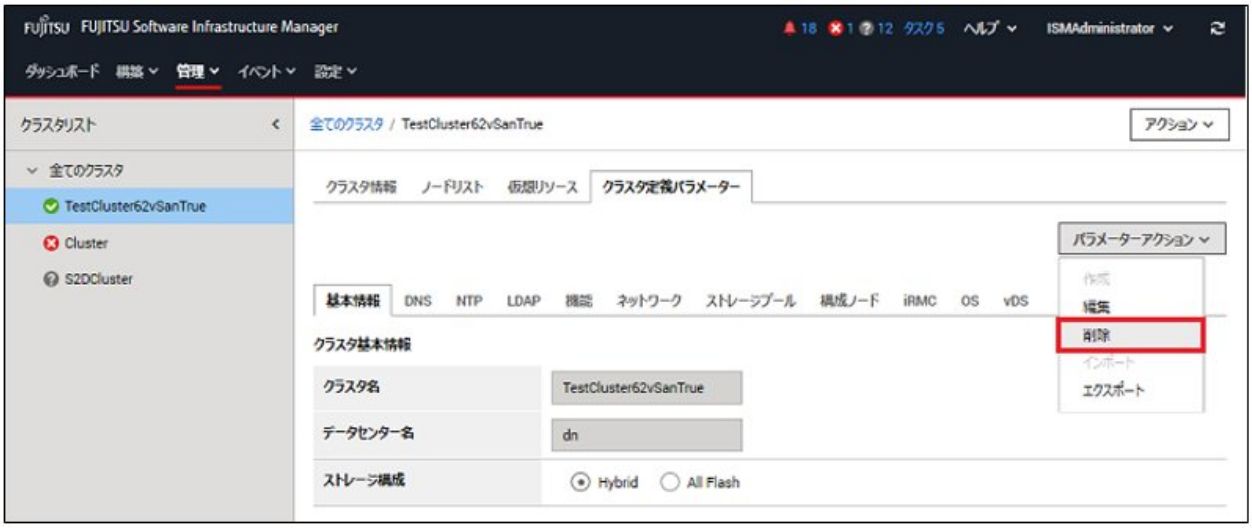
6.9.3 クラスタ定義パラメーターを削除する

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. ISM管理者（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。
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。

6. 「クラスタリスト」画面で削除対象の[＜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。「クラスタ定義パラメーターが未作成の状態です。」が表示されたら、クラスタ定義パラメーターの削除は完了です。

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。

6.10 クラスタを構成するノードを保守する

PRIMEFLEX for VMware vSANのノード再起動を伴う保守作業を行うために、ノード切離し機能またはノード組込み機能を実行します。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

ノード切離し／組込み機能は、以下の作業フローで行います。

表6.19 クラスタを構成するノードの保守フロー

クラスタを構成するノードの保守手順		作業内容
1	事前準備	仮想マシンを保守対象外サーバーへ移行

クラスタを構成するノードの保守手順		作業内容
2	ノード切離しの実行	
3	保守作業	拡張ボードの交換などの保守作業を実施
4	ノード組込みの実行	
5	事後処理	仮想マシンを保守対象サーバーへ移行

6.10.1 動作要件

ノード切離し／組込み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。

ノード切離し／組込みで共通の動作要件

対象クラスタの動作要件

- PRIMEFLEX for VMware vSANのクラスタであること
- 保守対象サーバーのクラスタが仮想化管理ソフトウェアに登録されていること
- 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、「6.8.2.11 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。
- ノード切離し／組込み対象のクラスタに対して、クラスタ管理機能の事前設定が実施されていること

  クラスタ管理機能の設定については、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。
- クラスタ情報の表示内容が最新化されていること

  詳細については、『解説書』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。
- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること
- 4台以上の正常なノードで構成されていること

  3台以下の構成ではノード切離し／組込み機能は使用できません。

対象サーバーの動作要件

- 保守対象サーバーがISMにノード登録されていること

ノード切離しの動作要件

対象クラスタの動作要件

- ノード切離しを行うクラスタ内で、電源オフ状態のサーバーが1台以下であること

対象サーバーの動作要件

- 保守対象サーバー上のすべての仮想マシンは、他のサーバーへ移行されていること

  （vSphere 7.0 Update 1以降の場合、vCLS 仮想マシンも含めて移行されていること）

6.10.2 事前準備

クラスタを構成するノードの保守を行う前の準備作業について説明します。

6.10.2.1 仮想マシンを保守対象外サーバーに移行する

DRS機能の設定状態に応じて、行う操作が異なります。

6.10.2.1.1 DRS機能がオンの場合

DRS機能がオンの場合は、保守対象サーバー上の仮想マシンを自動で移行させるため、仮想マシンの移行操作は不要です。
ただし、vSphere DRSの自動化レベルが「完全自動化」に設定されている必要があります。以下の手順でvSphere DRSの自動化レベルを確認してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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]を選択し、vSphere DRSの自動化レベルが「完全自動化」であることを確認します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]の[＜クラスタ名＞]-[設定]を選択し、vSphere DRSの自動化レベルが「完全自動化」であることを確認します。
3. vSphere 7.0 Update 1以降の場合、vSphere DRSの動作に必要なvSphere クラスタサービスの動作状況を確認します。

   「ホストおよびクラスタ」画面から[＜クラスタ名＞]-[サマリ]を選択し、[Cluster Services]の[Cluster Service health]の値が「Healthy」であることを確認します。

6.10.2.1.2 DRS機能がオフの場合

DRS機能がオフの場合は、以下の手順で仮想マシンを移行してください。

保守対象サーバーで動作するすべての仮想マシンに対して実施してください。
vSphere 7.0 Update 1以降の場合、vCLS 仮想マシンについても以下の手順で移行してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、保守対象サーバーで動作する仮想マシンがあるか確認します。
4. 動作する仮想マシンがある場合、保守対象サーバー名、保守対象サーバーで動作する仮想マシン名をすべて記録します。
5. 動作する仮想マシンを選択し、[＜仮想マシン名＞]-[移行]を選択します。
6. 「移行タイプの選択」画面で、[コンピューティング リソースのみ変更します]を選択し、[次へ]ボタンを選択します。
7. 「コンピューティングリソースの選択」画面で[ホスト]を選択し、保守対象サーバーで動作する仮想マシンの移行先サーバーを選択し、[次へ]ボタンを選択します。
8. 「ネットワークの選択」画面で仮想マシンの移行先ネットワークを選択し、[次へ]ボタンを選択します。
9. 「vMotionの優先順位の選択」画面で、vMotionのスケジュールを選択し、[次へ]ボタンを選択します。
10. 「設定の確認」画面で、表示されている内容を確認し、[完了]ボタンを選択します。
11. [最近のタスク]に表示されるタスク名[仮想マシンの再配置]のステータスが「完了」となることを確認します。
12. 保守対象サーバーで動作する仮想マシンがなくなるまで、手順4～手順10を繰り返します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、保守対象サーバーで動作する仮想マシンがあるか確認します。
4. 動作する仮想マシンがある場合、保守対象サーバー名、保守対象サーバーで動作する仮想マシン名をすべて記録します。

5. 動作する仮想マシンを選択し、[＜仮想マシン名＞]-[移行]を選択します。
6. 「移行タイプの選択」画面で、[コンピューティング リソースのみ変更します]を選択し、[NEXT]ボタンを選択します。
7. 「コンピューティング リソースの選択」画面で[ホスト]を選択し、保守対象サーバーで動作する仮想マシンの移行先サーバーを選択し、[NEXT]ボタンを選択します。
8. 「ネットワークの選択」画面で仮想マシンの移行先ネットワークを選択し、[NEXT]ボタンを選択します。
9. 「vMotionの優先順位の選択」画面で、vMotionのスケジュールを選択し、[NEXT]ボタンを選択します。
10. 「設定の確認」画面で、表示されている内容を確認し、[FINISH]ボタンを選択します。
11. [最近のタスク]に表示されるタスク名[仮想マシンの再配置]のステータスが「完了」となることを確認します。
12. 保守対象サーバーで動作する仮想マシンがなくなるまで、手順4～手順10を繰り返します。

6.10.3 ノード切離しまたはノード組込みを実行する

ノード切離し／組込み機能を実行して、PRIMEFLEX for VMware vSANのノードの切離しまたは組込みを行います。

ノード切離し／組込み機能を実行前に「6.10.1 動作要件」を参照して、動作要件を必ず確認してください。

- 6.10.3.1 ノード切離し手順
- 6.10.3.2 ノード組込み手順

6.10.3.1 ノード切離し手順

ISM for PRIMEFLEXのノード切離し機能の実行手順について説明します。

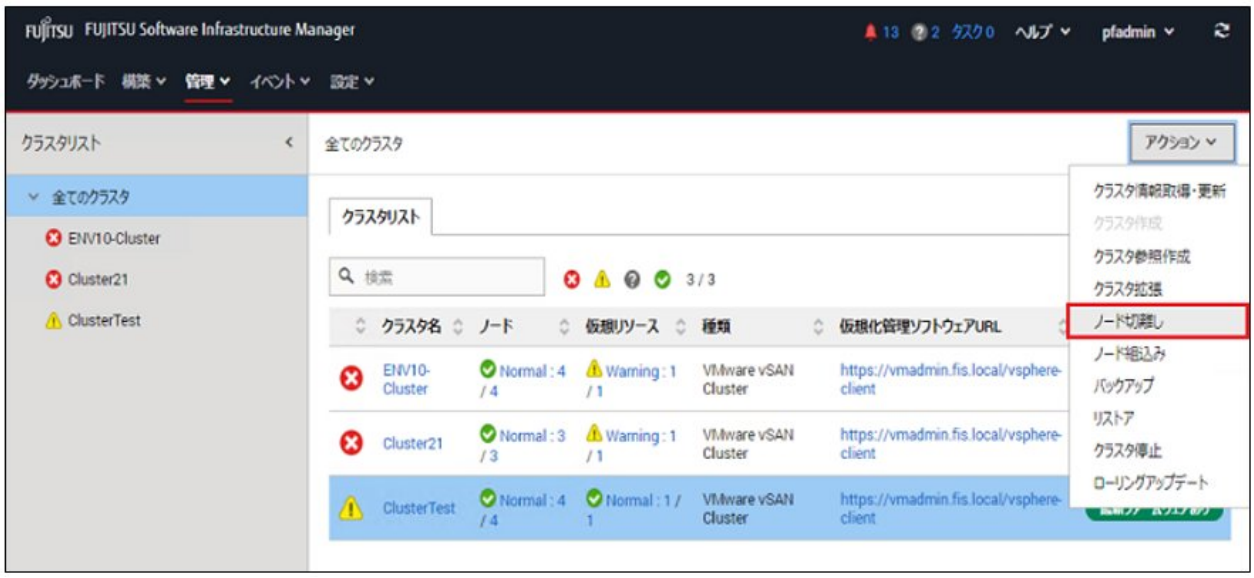
注意

ISM for PRIMEFLEXの他の機能が実行中にノード切離し機能を実行しないでください。ノード切離し機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

1. ISM管理者（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。
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[ノード切離し]を選択します。



4. 「ノード切離し」画面で対象クラスタを確認します。

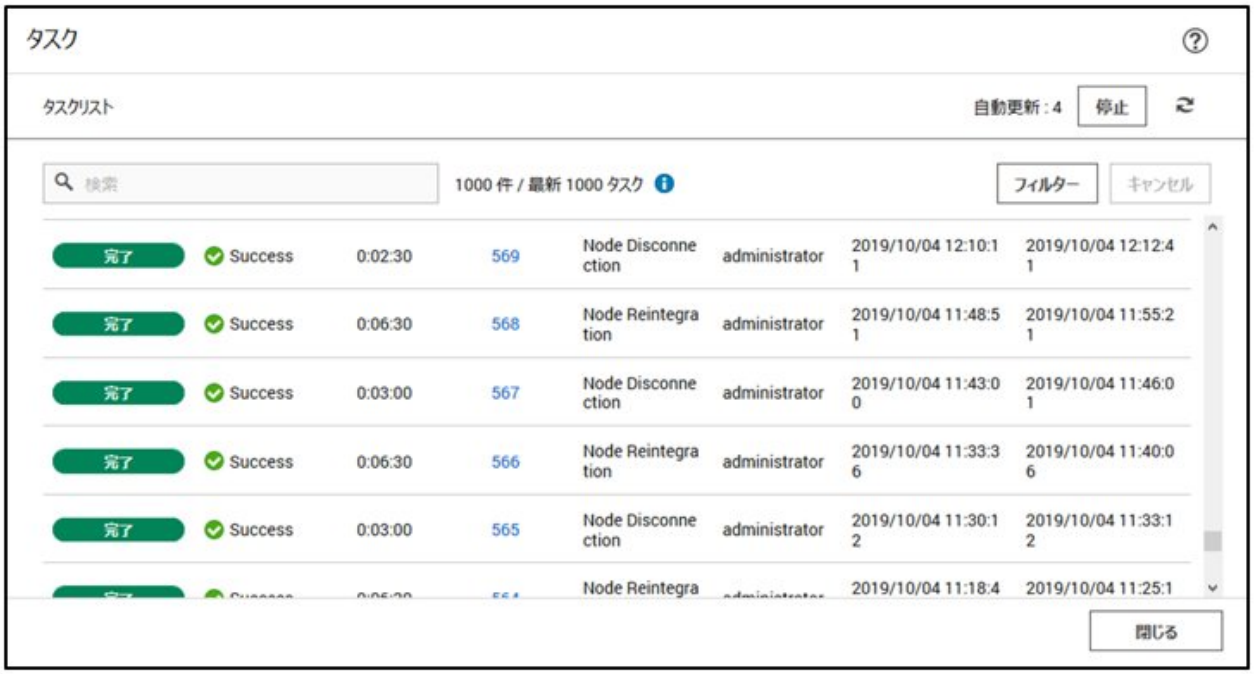
5. ノード切離しの対象サーバーを選択して、[実行]ボタンを選択します。

ポイント

データ退避モードに「全データの移行」を選択して実行した場合、ノードのすべてのデータを別のノードに移行します。このため、ノード上のデータ量によって操作に要する時間が長くなることがあります。

ノード切離しの実行は、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「Node Disconnection」となっているのが、ノード切離しのタスクです。



ポイント

「タスク」画面のタスクリストから「Node Disconnection」の[タスクID]を選択すると、「Node Disconnection」の「タスク」画面が表示されます。この画面では、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。

6. 「Node Disconnection」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のイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  問題が解決できたら再度操作を行ってください。

- vCSA 6.7u2環境の場合、ノード切離し機能実行後に以下の健全性エラーが発生する可能性があります。この健全性エラーの対処は不要です。保守対象サーバーに対してノード組込み機能実行後に自動で健全性エラーは解消されます。

  ー vSAN 健全性アラーム「vCenter Server から切断されたホスト」

  ー ホストの接続と電源状態

6.10.3.2 ノード組込み手順

ISM for PRIMEFLEXのノード組込み機能の実行手順について説明します。

注意

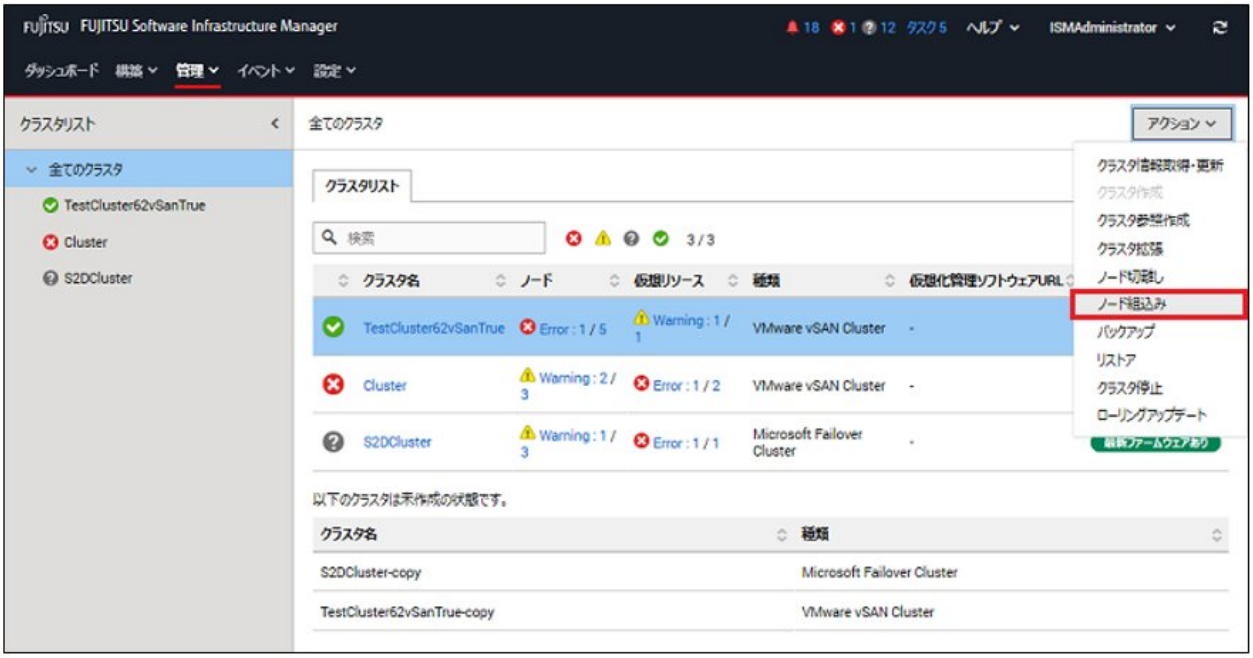
ISM for PRIMEFLEXの他の機能が実行中にノード組込み機能を実行しないでください。ノード組込み機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

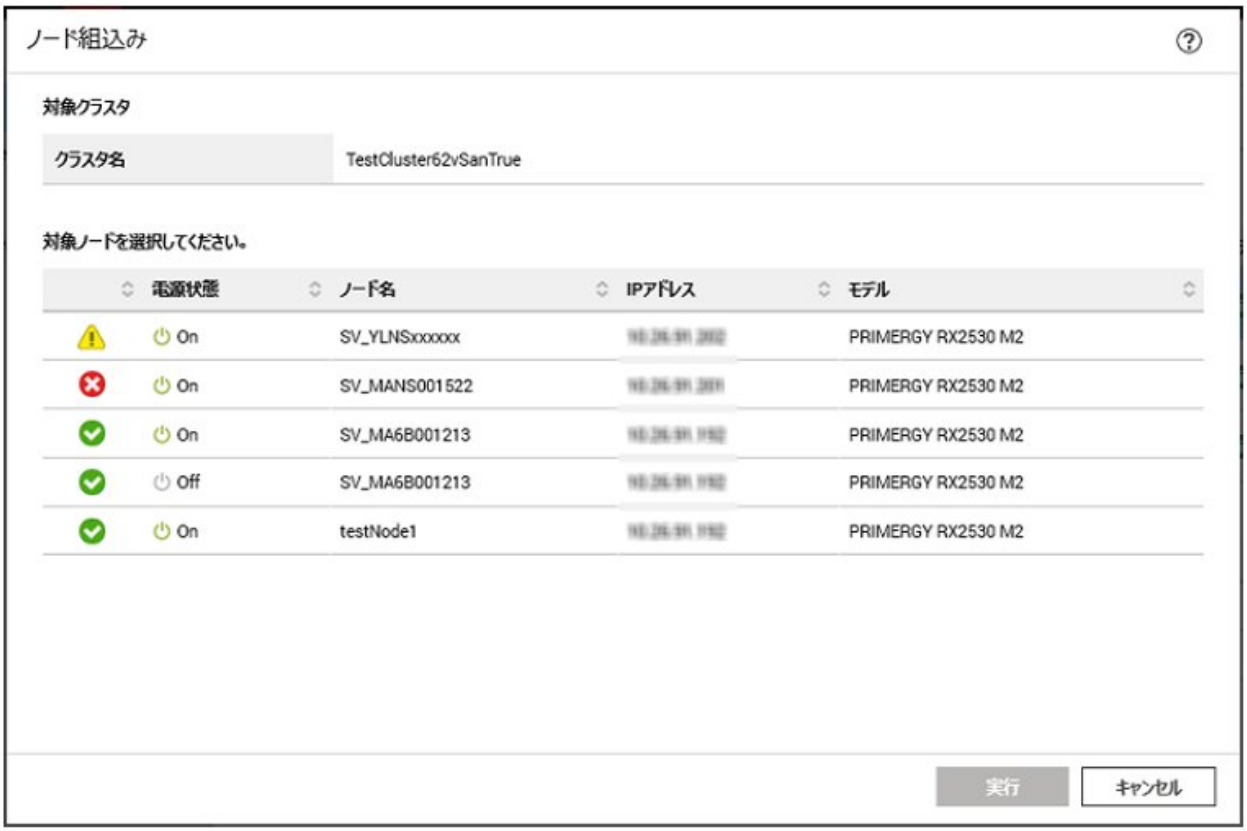
1. ISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）でISMにログインします。
2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択します。

   「クラスタリスト」画面が表示されます。

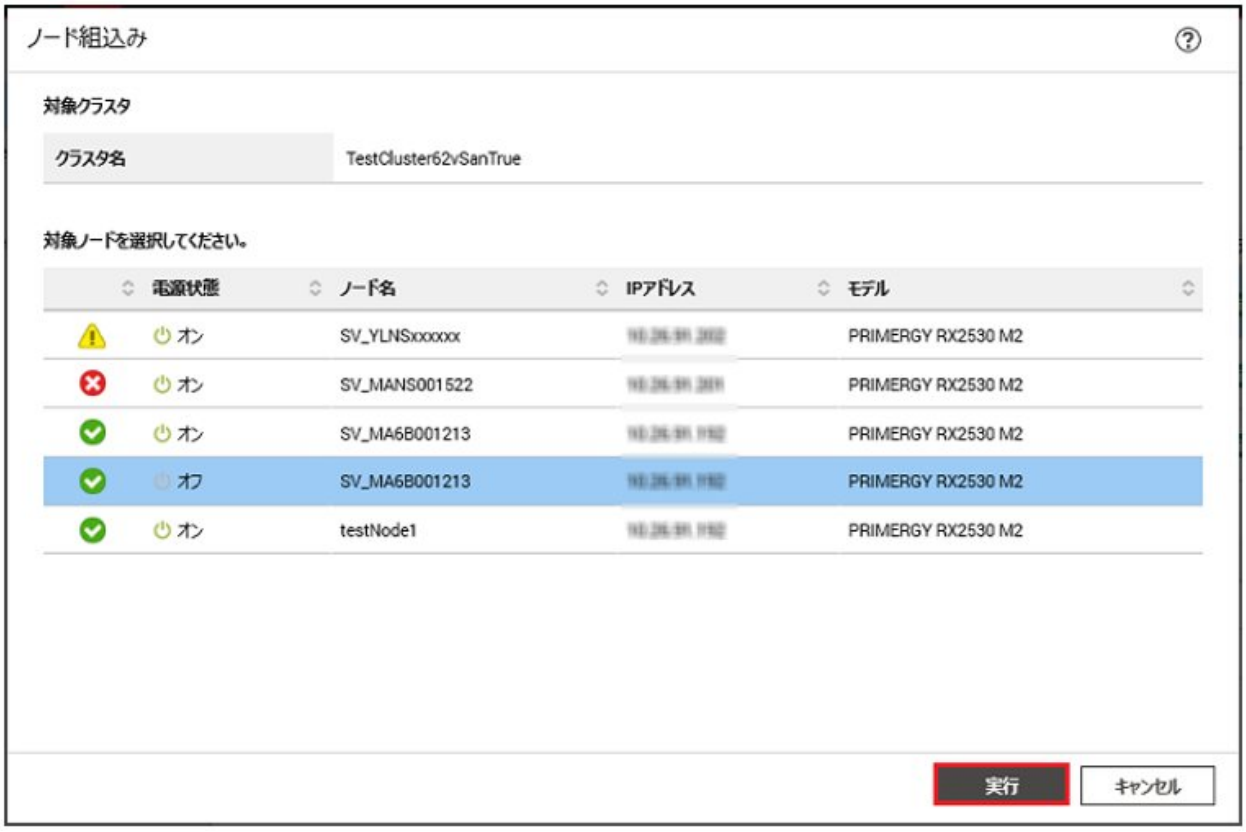
3. [＜対象のクラスタ＞]を選択して、[アクション]ボタンから[ノード組込み]を選択します。



4. 「ノード組込み」画面で対象クラスタを確認します。

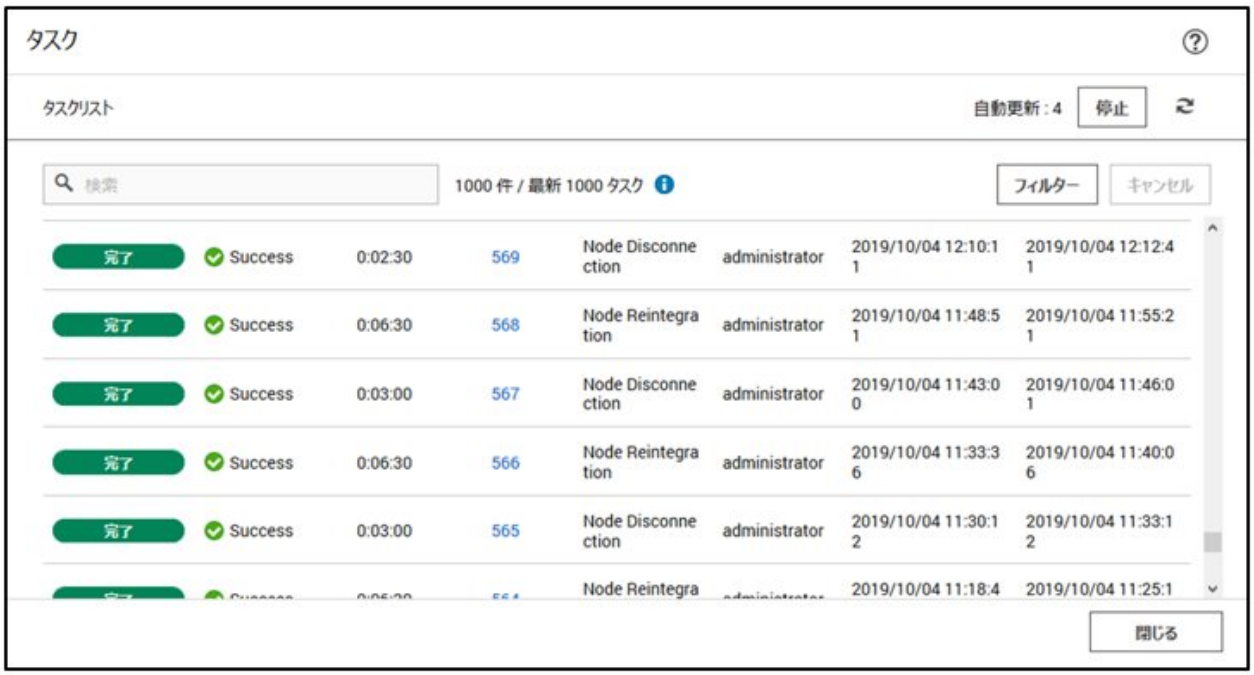


5. ノード組込みの対象サーバーを選択して、[実行]ボタンを選択します。



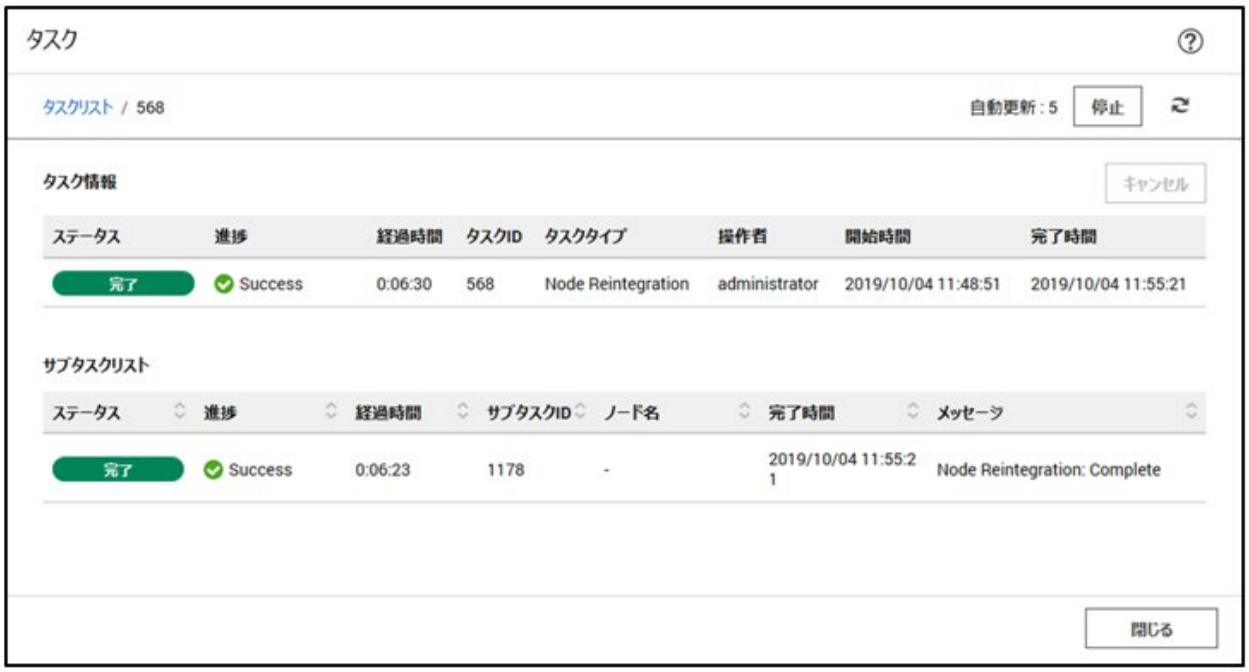
ノード組込みの実行は、ISMのタスクとして登録されます。

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「Node Reintegration」となっているのが、ノード組込みのタスクです。



ポイント

「タスク」画面のタスクリストから「Node Reintegration」の[タスクID]を選択すると、「Node Reintegration」の「タスク」画面が表示されます。この画面では、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。



6. 「Node Reintegration」のステータスが「完了」になったことを確認します。

ポイント

ISMからタスクのキャンセルを実行した場合やISMの「タスク」画面にエラーが表示された場合、ノード組込みの実行前の状態に戻すために、VMwareのメンテナンスモードの設定が行われることがあります。この際に、指定されるデータ退避モードは「アクセシビリティの確保」です。

注意

ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

問題が解決できたら再度操作を行ってください。

6.10.4 事後処理

クラスタを構成するノードの保守の事後処理について説明します。

6.10.4.1 仮想マシンを保守対象のサーバーに移行する

保守を行ったあと、事前準備で保守対象外サーバーに移行した仮想マシンを保守対象サーバーに戻します。

保守対象外サーバーへ移行したすべての仮想マシンに対して実施してください。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。

3. 表示された画面で、「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した仮想マシンを選択し、[＜仮想マシン名＞]-[移行]を選択します。
4. 「移行タイプの選択」画面で、[コンピューティング リソースのみ変更します]を選択し、[次へ]ボタンを選択します。
5. 「コンピューティング リソースの選択」画面でクラスタを展開し、「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した保守対象サーバーを選択し、[次へ]ボタンを選択します。
6. 「ネットワークの選択」画面で仮想マシンの移行先ネットワークを選択し、[次へ]ボタンを選択します。
7. 「vMotionの優先順位の選択」画面で、vMotionのスケジュールを選択し、[次へ]ボタンを選択します。
8. 「設定の確認」画面で、表示されている内容を確認し、[完了]ボタンを選択します。
9. [最近のタスク]に表示されるタスク名[仮想マシンの再配置]のステータスが「完了」となることを確認します。
10. 「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した仮想マシンがなくなるまで、手順2～手順8を繰り返します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した仮想マシンを選択し、[＜仮想マシン名＞]-[移行]を選択します。
4. 「移行タイプの選択」画面で、[コンピューティング リソースのみ変更します]を選択し、[次へ]ボタンを選択します。
5. 「コンピューティング リソースの選択」画面で[ホスト]を選択し、「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した保守対象サーバーを選択し、[次へ]ボタンを選択します。
6. 「ネットワークの選択」画面で仮想マシンの移行先ネットワークを選択し、[次へ]ボタンを選択します。
7. 「vMotionの優先順位の選択」画面で、vMotionのスケジュールを選択し、[次へ]ボタンを選択します。
8. 「設定の確認」画面で、表示されている内容を確認し、[完了]ボタンを選択します。
9. [最近のタスク]に表示されるタスク名[仮想マシンの再配置]のステータスが「完了」となることを確認します。
10. 「6.10.2.1 仮想マシンを保守対象外サーバーに移行する」で記録した仮想マシンがなくなるまで、手順2～手順8を繰り返します。

6.11 クラスタを構成するノードまたはvCSAをバックアップする

PRIMEFLEX for VMware vSANの障害発生時のシステム復旧のために、バックアップ機能を実行します。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

バックアップ機能は、以下の作業フローで行います。

表6.20 クラスタを構成するノードまたはvCSAのバックアップフロー

クラスタを構成するノードまたはvCSAのバックアップ手順		作業内容
1	事前準備	バックアップを格納するサーバーの準備
2	バックアップの実行	
3	事後処理	TSM-SSHサービスの起動

6.11.1 動作要件

バックアップ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。

- バックアップ格納先サーバーのディスク空き容量が確保されていること

  バックアップに必要なディスク空き容量の目安は以下です。

－ VMware ESXiをバックアップする場合

VMware ESXi 1台につき0.05MB以上

－ vCenter Server Applianceをバックアップする場合

1GB + 分散仮想スイッチ1台につき1MB以上

対象クラスタの動作要件

- PRIMEFLEX for VMware vSANのクラスタであること
- バックアップ対象サーバーのクラスタが仮想化管理ソフトウェアに登録されていること
- 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、「6.8.2.11 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。
- バックアップ対象サーバーのクラスタに対して、クラスタ管理機能の事前設定が実施されていること

  クラスタ管理機能の設定については、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。
- クラスタ情報の表示内容が最新化されていること

  詳細については、『解説書』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。
- PRIMEFLEX for VMware vSANは以下の版数であること
  - － VMware ESXi v6.7 Update1以降
  - － VMware vCenter Server Appliance v6.7 Update1以降
- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること
- バックアップ対象サーバーのクラスタが正常に動作していること
- バックアップ対象のvCenter Serverが起動していること
- vCSAをバックアップする場合は、ISMの「仮想化管理ソフトウェアリスト」画面に登録されているvCenterで、vCSAの仮想マシンが管理されていること

対象サーバーの動作要件

- バックアップ対象サーバーがISMにノード登録されていること
- バックアップ対象のサーバーが起動し、正常に動作していること

6.11.2 事前準備

クラスタを構成するノードまたはvCSAのバックアップを行う前の準備作業について説明します。

6.11.2.1 バックアップを格納するサーバーを準備する

1. バックアップ格納先サーバーを用意し、サーバー上でSMB/CIFSの共有フォルダーを設定します。

   以下は、バックアップ格納先サーバー（Windows Server 2019）で共有フォルダーを設定する例です。

   a. バックアップ格納先サーバーでバックアップを格納するフォルダーを作成します。

   b. フォルダーを右クリックして、[プロパティ]を選択します。

   c. [共有]タブから[共有]を選択します。

   d. バックアップ格納先サーバーのユーザーの中から、共有するユーザーを選択して[共有]を選択します。

   e. 「ネットワークの探索とファイル共有」ウィンドウが表示された場合、パブリックネットワークの探索とファイル共有の設定に対し、お客様の環境に応じて「はい」／「いいえ」のいずれかを選択します。

   f. [閉じる]を選択します。

2. バックアップ格納先サーバーをPRIMEFLEX for VMware vSANの管理LANネットワークに接続します。

6.11.3 バックアップを実行する

バックアップ機能を実行して、PRIMEFLEX for VMware vSANのノードまたはvCSAのバックアップを行います。

バックアップ機能を実行前に「6.11.1 動作要件」を参照して、動作要件を必ず確認してください。

注意

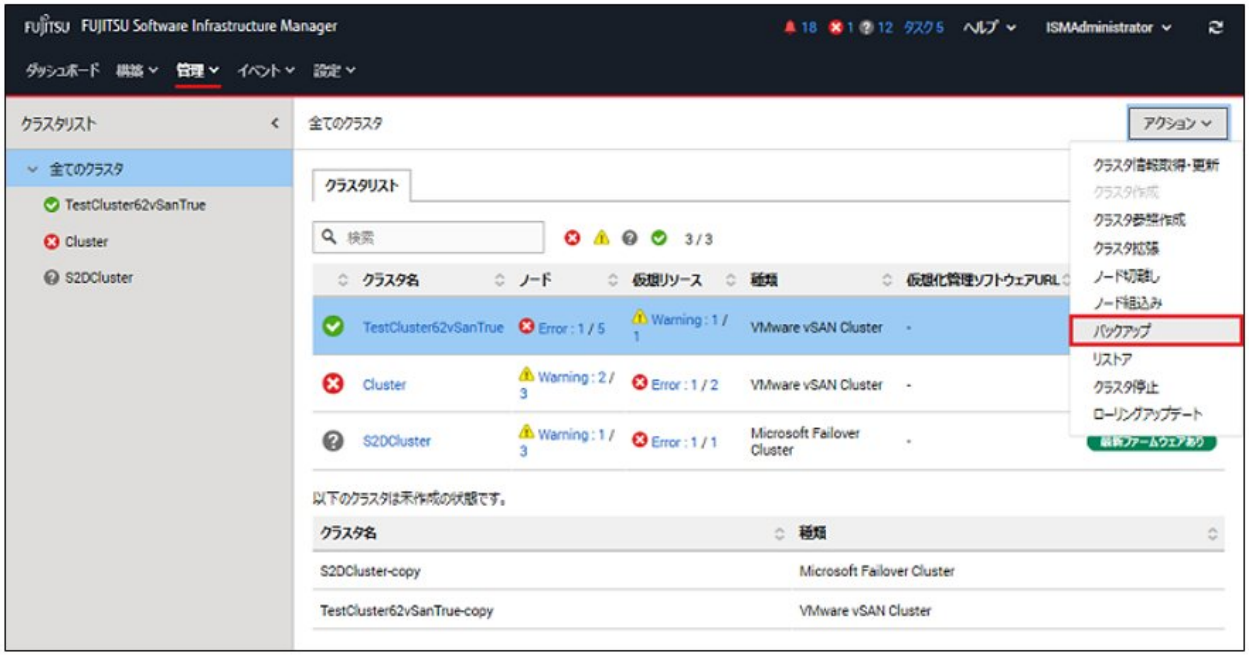
- ISM for PRIMEFLEXの他の機能が実行中にバックアップ機能を実行しないでください。バックアップ機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。

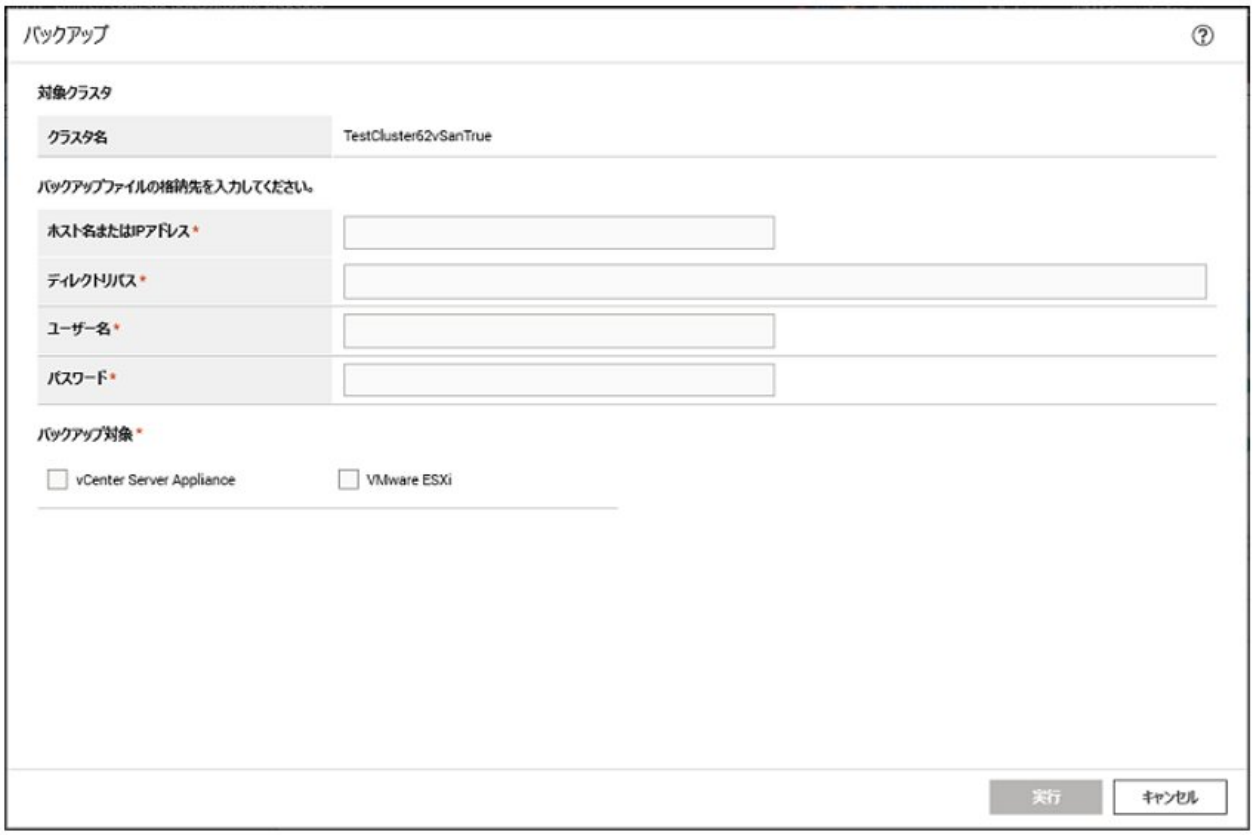
- バックアップ機能実行時、ISM for PRIMEFLEX は対象ノードのTSM-SSHサービスを停止させます。バックアップ機能実行前に、サービスの起動状態を確認してください。サービスが起動している場合は、バックアップ機能実行後に手動で起動し直してください。

1. ISM管理者（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。
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[バックアップ]を選択します。



4. 「バックアップ」画面で対象クラスタを確認します。

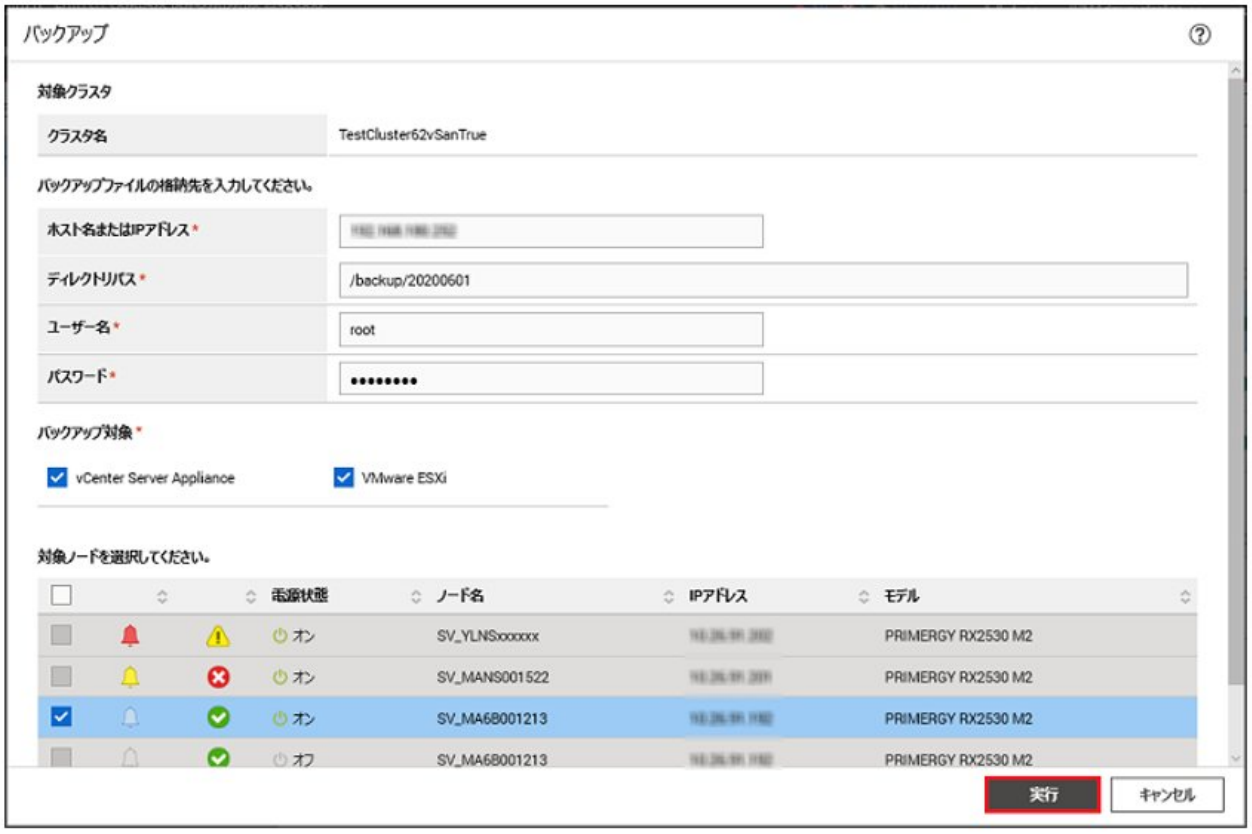


5. バックアップ対象と対象ノードを選択して、各種パラメーターを入力し、[実行]ボタンを選択します。

ポイント

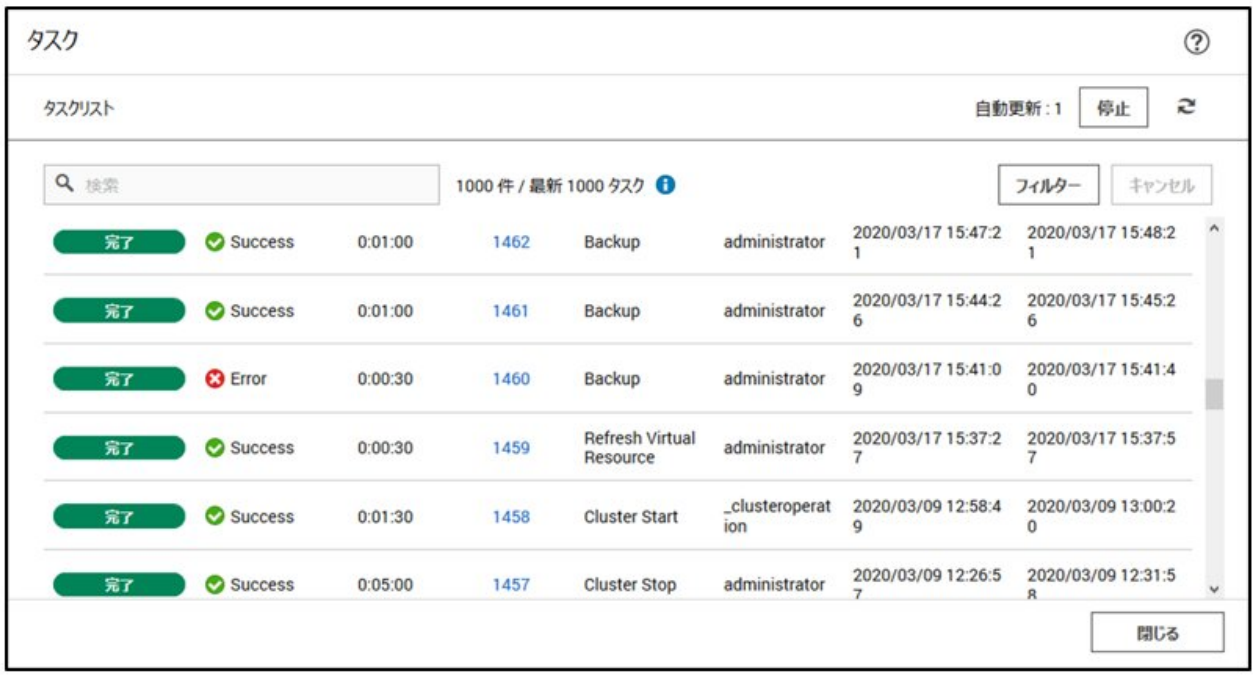
ドメインのユーザーを指定する場合は、ユーザー名に以下の書式で入力します。

<ドメイン名>¥<ユーザー名>、または <ユーザー名>@<ドメイン名>



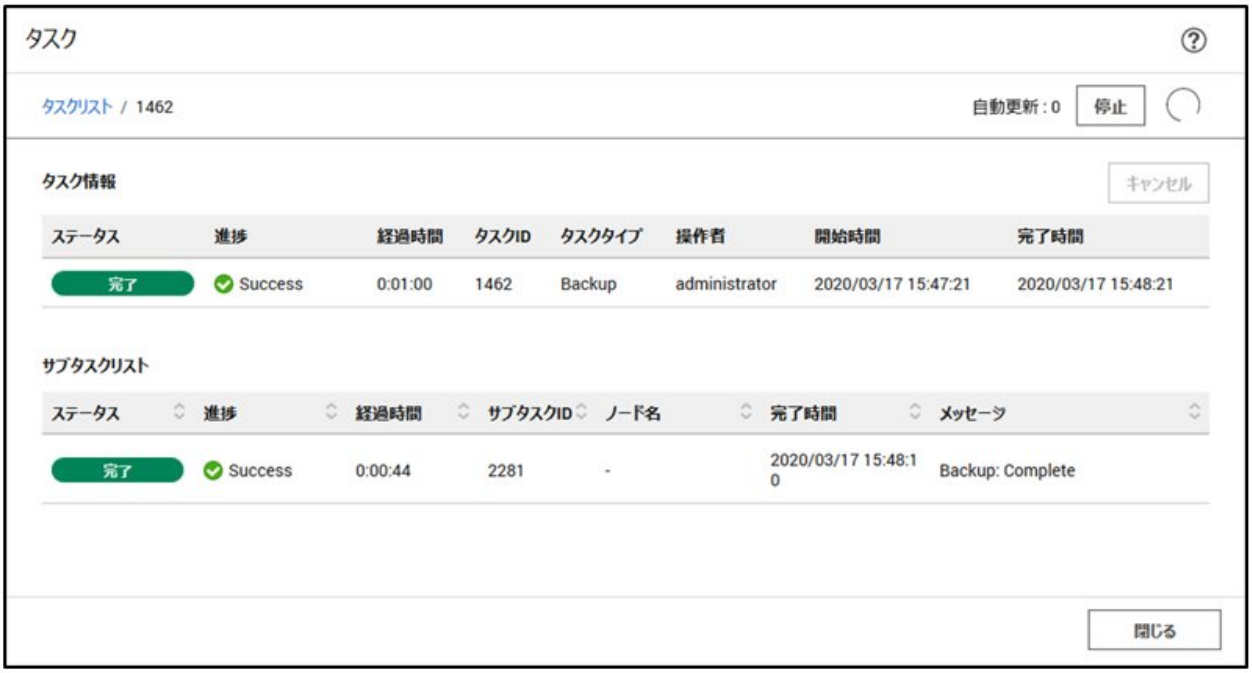
バックアップの実行は、ISMのタスクとして登録されます。

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「Backup」となっているのが、バックアップのタスクです。



ポイント

「タスク」画面のタスクリストから「Backup」の[タスクID]を選択すると、「Backup」の「タスク」画面が表示されます。この画面では、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。



6. 「Backup」のステータスが「完了」になったことを確認します。
7. バックアップ格納サーバーにバックアップが作成されたことを確認します。フォルダー形式は以下です。

フォルダー	説明
＜日時＞_＜ISMタスクID＞	ルートフォルダー ＜日時＞の形式はUTC時刻を「YYYYMMDD_hhmmss（年月日時分秒）」で設定します
vcsa_＜vCSAのIPアドレス＞	vCSAのバックアップの親フォルダー
va	vCSAのバックアップフォルダー [注]
vds	vDSのバックアップフォルダー
esxi_＜ESXiのIPアドレス＞	ESXiのバックアップフォルダー

[注]:ISM独自のバックアップファイルとして、"va"フォルダー内に以下のファイルを作成します。

以下のファイルは、ISMを使用したvCSAのリストアでのみ使用します。

ファイル:

pfx_vcsa_disk.json

注意

- ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  問題が解決できたら再度操作を行ってください。

- 以下の構成を変更した場合、再度バックアップを行ってください。リストアを実行する際に以下の構成が変更されている場合、エラー終了します。
  - 分散仮想スイッチと分散ポートグループの設定
  - vCSAのユーザー名とパスワード
  - ESXiのユーザー名とパスワード

6.11.4 事後処理

クラスタを構成するノードまたはvCSAのバックアップ事後処理について説明します。

6.11.4.1 TSM-SSHサービスを起動する

バックアップ機能実行後、バックアップ対象ノードのTSM-SSHサービスは停止しています。バックアップ機能実行前にサービスが起動していた場合は、必要に応じてサービスを起動し直してください。サービスの起動手順については、PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』の「ESXiホストのESXi Shell(TSM)とSSH(TSM-SSH)のサービスを有効にします」を参照してください。

PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』入手先:

- PRIMEFLEX HSV1.0/V1.1、PRIMEFLEX for VMware vSAN V1

  当社担当営業までお問い合わせください。

- PRIMEFLEX for VMware vSAN V2、PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

入手できない場合には当社担当営業までお問い合わせください。

6.12 クラスタを構成するvCSAをリストアする

PRIMEFLEX for VMware vSANの障害発生時のシステム復旧のために、リストア機能を実行します。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

リストア機能は、以下の作業フローで行います。

表6.21 クラスタを構成するvCSAのリストアフロー

クラスタを構成するvCSAのリストア手順		作業内容
1	事前準備	• バックアップを格納しているサーバーの準備 • vCSAインストーラーファイルをISM-VAへアップロード
2	リストアの実行	
3	事後処理	• vCSAのポートグループ変更 • 既存vCSAの削除 • TSM-SSHサービスの起動

6.12.1 動作要件

リストア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。

ISM 2.5.0.030以前で採取されたバックアップをリストアする場合は、以下の条件も必要です。

- vCenter Serverをアップグレードしている場合、その際にストレージサイズをデフォルトで指定していること
- vCenter Serverを過去に手動でリストアしている場合、その際にストレージサイズをデフォルトで指定していること
- vCenter Serverのディスク容量を拡張していないこと

バックアップがISM 2.5.0.030以前で採取された場合は、バックアップフォルダーに以下のファイルが存在しません。

ファイル:

＜バックアップフォルダー＞¥vcsa_＜vCSAのIPアドレス＞¥va¥pfx_vcsa_disk.json

例:

20200203_004120_1353¥vcsa_192.168.120.1¥va¥pfx_vcsa_disk.json

ストレージサイズにデフォルト以外を指定している場合や、ディスク容量を拡張している場合は、PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』を参照し、手動でのリストアを行ってください。

手動でのリストアでは、SMB/CIFSプロトコルを用いたバックアップファイルの読み込みがサポートされていません。このため、SMB/CIFSプロトコル以外のプロトコルを用いてバックアップファイルの読み込みを行ってください。

PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』入手先:

- PRIMEFLEX HSV1.0/V1.1、PRIMEFLEX for VMware vSAN V1

  当社担当営業までお問い合わせください。

- PRIMEFLEX for VMware vSAN V2、PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

入手できない場合には当社担当営業までお問い合わせください。

対象クラスタの動作要件

- PRIMEFLEX for VMware vSANのクラスタであること
- リストア対象サーバーのクラスタが仮想化管理ソフトウェアに登録されていること
- 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、「6.8.2.11 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。

- リストア対象サーバーのクラスタに対して、クラスタ管理機能の事前設定が実施されていること

  クラスタ管理機能の設定については、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

- クラスタ情報の表示内容が最新化されていること

  詳細については、『解説書』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。

- PRIMEFLEX for VMware vSANは以下の版数であること
  - VMware ESXi v6.7 Update1以降
  - VMware vCenter Server Appliance v6.7 Update1以降
- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること
- vCenter Serverが削除または停止しており、vCenter ServerのIPアドレスを使用したサーバーが存在しないこと
- vCenter ServerのFQDNがDNSサーバーで名前解決できること
- 管理用分散仮想スイッチのNIC(vmnic)が冗長構成であること

対象サーバーの動作要件

- リストア対象サーバーがISMにノード登録されていること

6.12.2 事前準備

クラスタを構成するvCSAのリストアを行う前の準備作業について説明します。

6.12.2.1 バックアップを格納したサーバーを準備する

1. バックアップを格納したサーバーを用意し、サーバー上でSMB/CIFSの共有フォルダーを設定します。
2. バックアップを格納したサーバーをPRIMEFLEX for VMware vSANの管理LANネットワークに接続します。

6.12.2.2 vCSAインストーラーファイルをISM-VAへアップロードする

vCSAインストーラーファイルは、VMware Webサイトからダウンロードしてください。

以下の項目を確認しながら、「1.4.1 ISM-VAにファイルをアップロードする」を参照して、vCSAインストーラーファイルをアップロードしてください。

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、『解説書』の「3.7 仮想ディスクの割当て」を参照してください。

項目	値
ルートディレクトリー	Administrator/ftp
ファイルタイプ	その他
アップロード先ディレクトリー	Administrator/ftp/ClusterOperation/vCSA
ファイル	vCSAインストーラーファイル [注] 例：VMware-VCSA-all-6.7.0-10244745.iso

[注]：vCSAインストーラーファイルはバックアップ時のvCSAバージョンと同一のものをアップロードしてください。

6.12.3 リストアを実行する

リストア機能を実行して、PRIMEFLEX for VMware vSANのvCSAのリストアを行います。

リストア機能を実行前に「6.12.1 動作要件」を参照して、動作要件を必ず確認してください。

注意

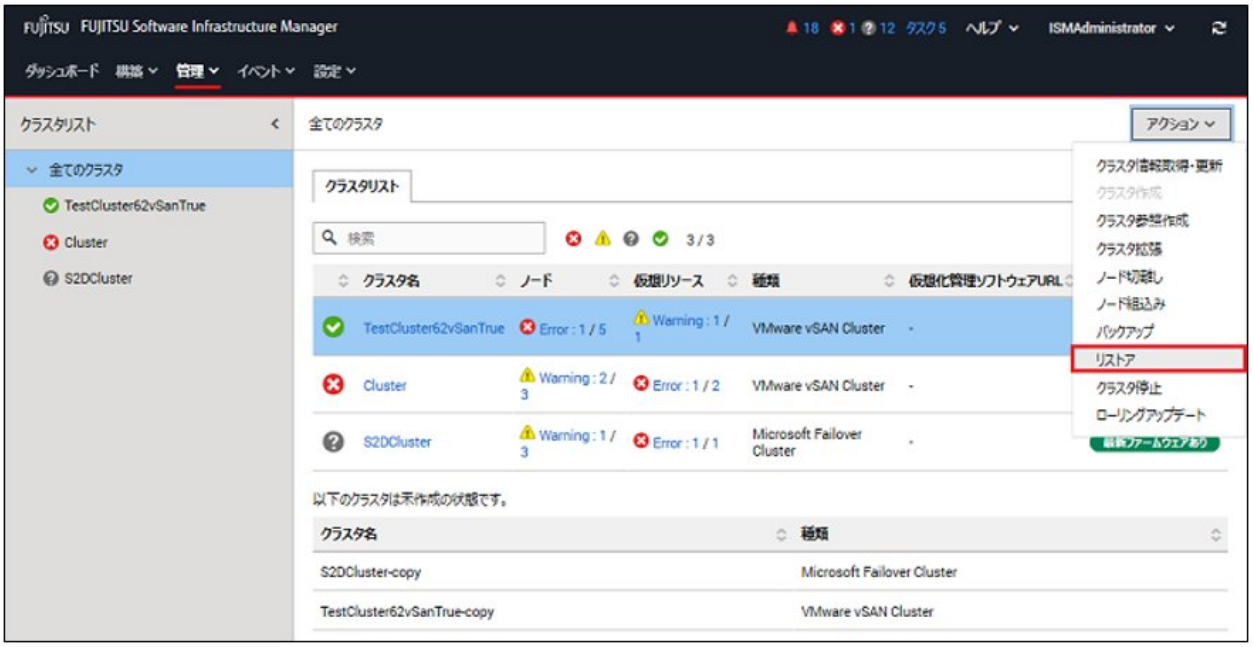
- ISM for PRIMEFLEXの他の機能が実行中にリストア機能を実行しないでください。リストア機能に失敗します。ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

  ISM for PRIMEFLEXの機能は、『解説書』の「2.12 ISM for PRIMEFLEXの機能」を参照してください。
- リストア機能実行時、ISM for PRIMEFLEX はリストア対象ノードのTSM-SSHサービスを停止させます。リストア機能実行前に、サービスの起動状態を確認してください。サービスが起動している場合には、リストア機能実行後に手動で起動し直してください。

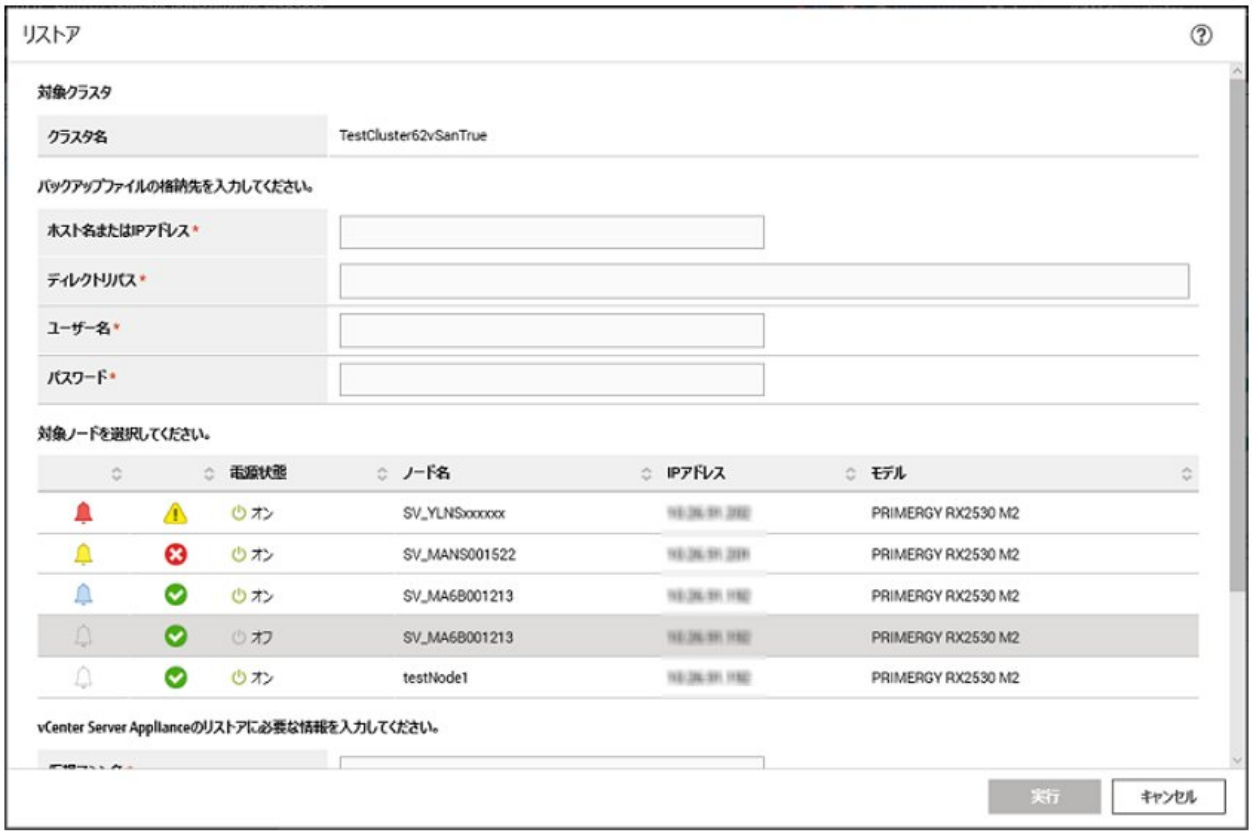
1. ISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）でISMにログインします。
2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択します。

   「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[リストア]を選択します。



4. 「リストア」画面で対象クラスタを確認します。



5. 対象ノードを選択して、各種パラメーターを入力し、[実行]ボタンを選択します。

ポイント

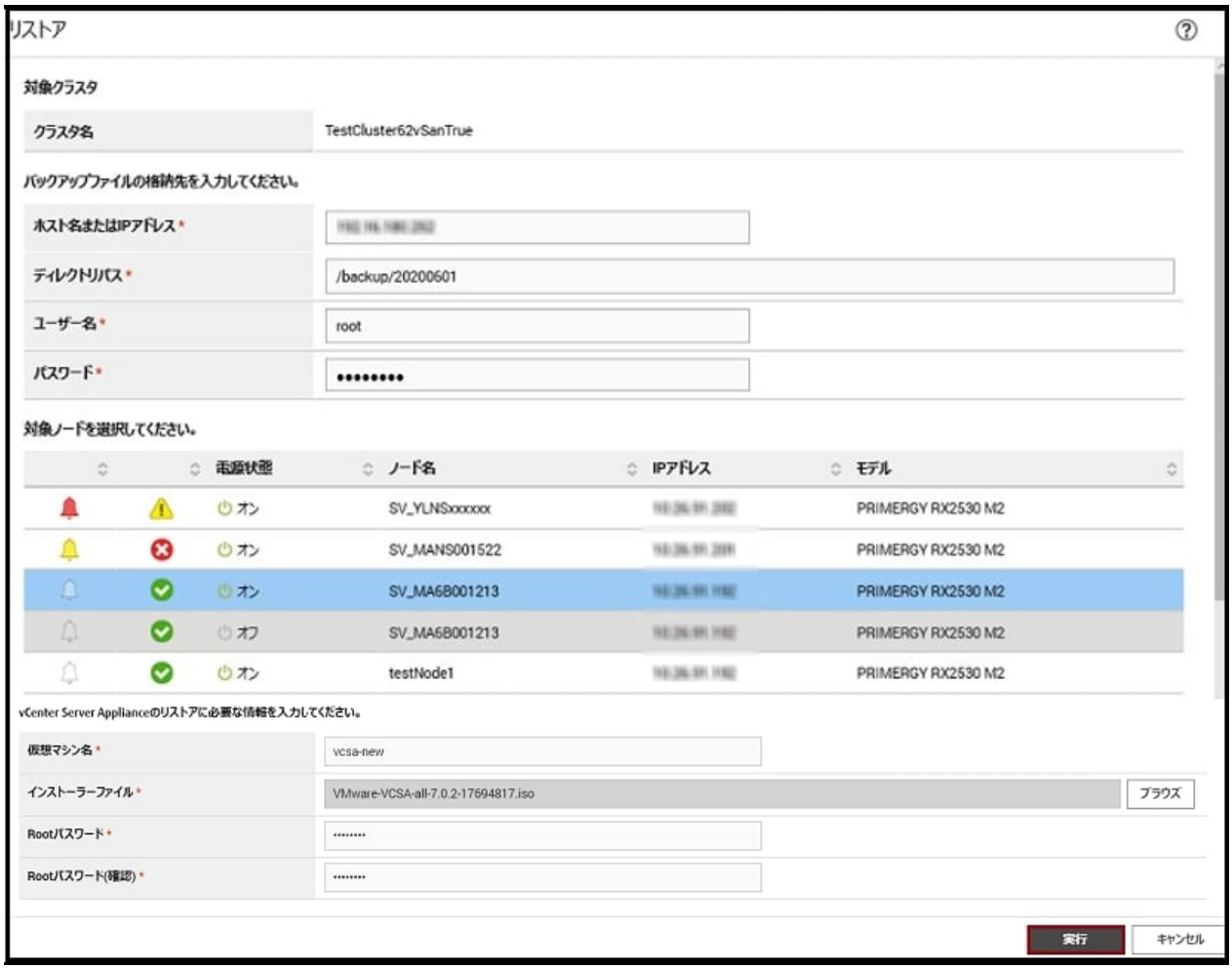
- バックアップファイルの [ディレクトリパス] は、ISM for PRIMEFLEXのバックアップ機能で作成された以下のバックアップ格納フォルダーのルートフォルダーを入力します。

  バックアップ格納フォルダー/＜日時＞_＜ISMタスクID＞

- ドメインのユーザーを指定する場合は、[ユーザー名] に以下の書式で入力します。

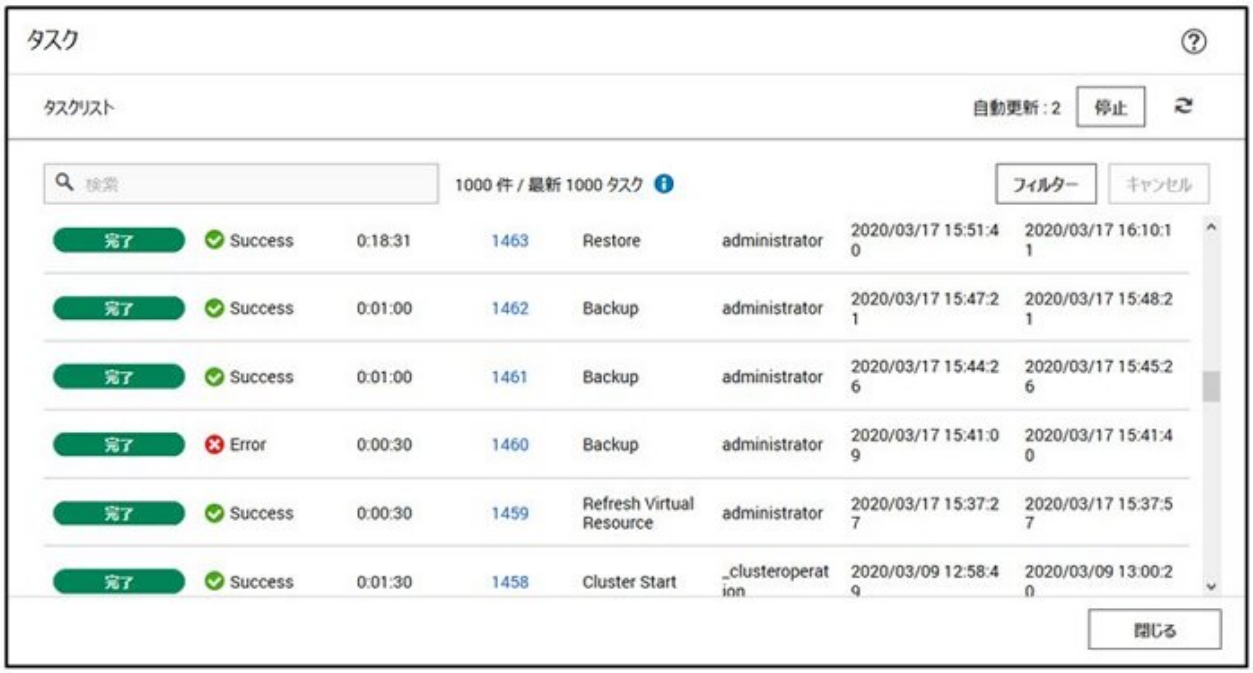
  ＜ドメイン名＞¥＜ユーザー名＞、または＜ユーザー名＞@＜ドメイン名＞

- [仮想マシン名] は、他の仮想マシンと重複しない名前を入力します。



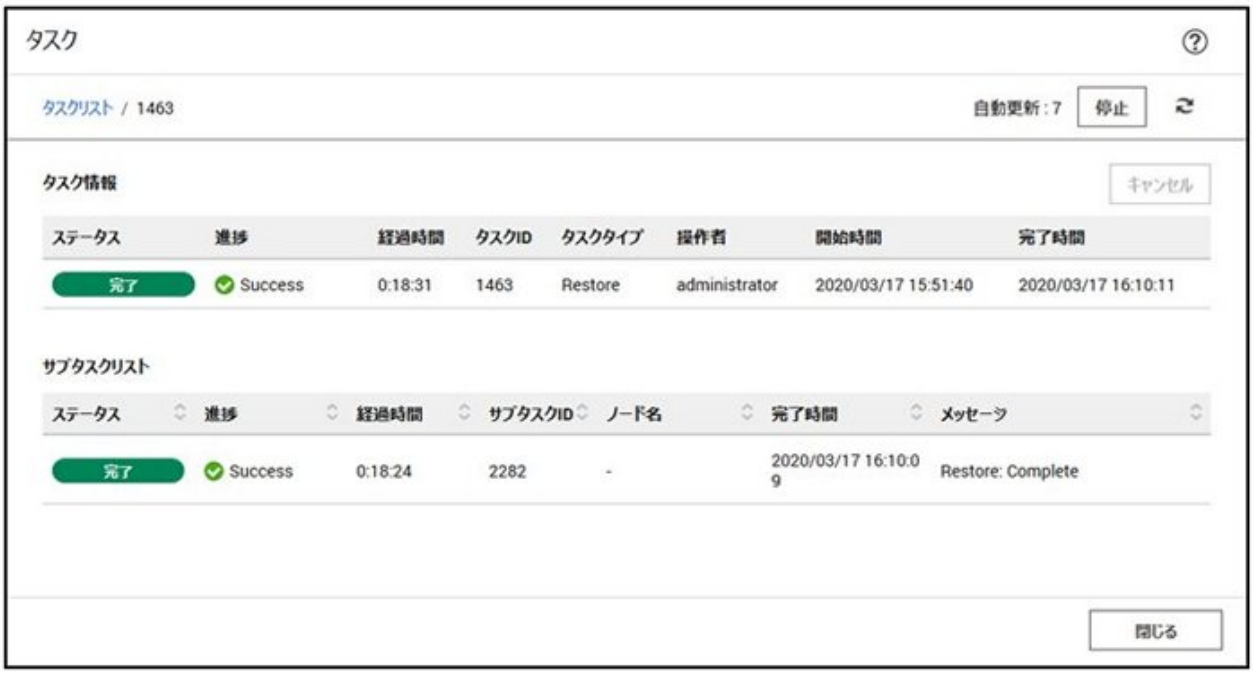
リストアの実行は、ISMのタスクとして登録されます。

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「Restore」となっているのが、リストアのタスクです。



ポイント

「タスク」画面のタスクリストから「Restore」の[タスクID]を選択すると、「Restore」の「タスク」画面が表示されます。この画面では、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。



6. 「Restore」のステータスが「完了」になったことを確認します。

ポイント

サブタスクのメッセージに「Info: Please change the port group of the vCSA」が含まれている場合は、事後手順として「6.12.4.1 vCSAのポートグループを変更する」を実行してください。

注意

サブタスクのメッセージに以下の内容が含まれる場合、リストア後のvCSAは、vSANのデフォルトのストレージポリシーが適用された状態となっています。vCSAにストレージポリシーを適用し直す必要があります。

```
[Warning]: The storage policy for management VMs is not applied. Log in to vCSA with vSphere Client and apply the storage policy for management VMs.
```

以下の手順を実行してください。なお、手順を実施するにあたり『Integrated System PRIMEFLEX for VMware vSAN デザインガイド』が必要です。

PRIMEFLEX for VMware vSAN の『デザインガイド』入手先:

- PRIMEFLEX for VMware vSAN V1

  当社担当営業までお問い合わせください。

- PRIMEFLEX for VMware vSAN V2、PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

入手できない場合には当社担当営業までお問い合わせください。

vCSA 6.5以前(Flash)の場合:

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[操作およびポリシー]-[仮想マシンストレージポリシー]を選択します。
3. [仮想マシンストレージポリシーの作成]を選択します。
4. 以下を参照して、管理仮想マシンのストレージポリシーの設定値を入力します。

   『Integrated System PRIMEFLEX for VMware vSAN デザインガイド』ー「ストレージポリシー」

   ポリシー構造の設定値では、[ストレージポリシーでのルールセットの使用]-[vSAN]を設定します。
5. [完了]ボタンを選択し、仮想マシンストレージポリシーを作成します。
6. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]-[<vCSA名>]-[設定]-[ポリシー]-[仮想マシン ストレージポリシーの編集]の順に選択します。
7. 仮想マシンストレージポリシーのプルダウンメニューから、手順5で作成したストレージポリシーを選択します。
8. [OK]ボタンを選択し、変更を適用します。

vCSA 6.7以降(HTML5)の場合:

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[監視]-[仮想マシンストレージポリシー]を選択します。
3. 「仮想マシンストレージポリシー」-[作成]を選択します。
4. 以下を参照して、管理仮想マシンのストレージポリシーの設定値を入力します。

   『Integrated System PRIMEFLEX for VMware vSAN デザインガイド』ー「ストレージポリシー」

   ポリシー構造の設定値では、[データストア固有のルール]-[「vSAN」ストレージでルールを有効化]を設定します。
5. [完了]ボタンを選択し、仮想マシンストレージポリシーを作成します。

6. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]-[＜vCSA名＞]-[構成]-[ポリシー]-[仮想マシン ストレージポリシーの編集]の順に選択します。
7. 仮想マシンストレージポリシーのプルダウンメニューから、手順5で作成したストレージポリシーを選択します。
8. [OK]ボタンを選択し、変更を適用します。

注意

ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。イベントログで確認したメッセージは『ISM for PRIMEFLEX メッセージ集』を参照して対処してください。

問題が解決できたら再度操作を行ってください。

6.12.4 事後処理

vCSAのリストアの事後処理について説明します。

6.12.4.1 vCSAのポートグループを変更する

必要に応じてvCSAを管理仮想マシン用のポートグループに接続します。

リストア完了後のサブタスクのメッセージに「Info: Please change the port group of the vCSA」が含まれている場合、リストア後のvCSAはESXiのVMkernel用のポートグループに接続された状態です。
このため、以下の手順を実行して、vCSAを管理仮想マシン用のポートグループに接続します。
管理仮想マシン用のポートグループ名のデフォルトは、「Management Port Group」です。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[設定の編集]を選択します。
4. [仮想ハードウェア]タブの[ネットワーク アダプタ1]の値を管理仮想マシン用のポートグループに変更します。
5. [OK]ボタンを選択し、変更を適用します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[設定の編集]を選択します。
4. [仮想ハードウェア]タブの[ネットワーク アダプタ1]の値を管理仮想マシン用のポートグループに変更します。
5. [OK]ボタンを選択し、変更を適用します。

6.12.4.2 既存のvCSAを削除する

リストアを行ったあと、必要に応じて既存のvCSAを削除します。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[ディスクから削除]を選択します。
4. 「削除の確認」画面で、[はい]ボタンを選択します。

5. [最近のタスク]に表示されるタスク名[仮想マシンの削除]のステータスが「完了」となることを確認します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、vCSAの仮想マシンを選択し、[＜仮想マシン名＞]-[ディスクから削除]を選択します。
4. 「削除の確認」画面で、[はい]ボタンを選択します。
5. [最近のタスク]に表示されるタスク名[仮想マシンの削除]のステータスが「完了」となることを確認します。

6.12.4.3 TSM-SSHサービスを起動する

リストア機能実行後、リストア対象ノードのTSM-SSHサービスは停止しています。リストア機能実行前にサービスが起動していた場合は、必要に応じてサービスを起動し直してください。サービスの起動手順については、PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』の「ESXiホストのESXi Shell(TSM)とSSH(TSM-SSH)のサービスを有効にします」を参照してください。

PRIMEFLEX for VMware vSANの『オペレーション＆メンテナンスガイド』入手先：

- PRIMEFLEX HSV1.0/V1.1、PRIMEFLEX for VMware vSAN V1

  当社担当営業までお問い合わせください。

- PRIMEFLEX for VMware vSAN V2、PRIMEFLEX for VMware vSAN V3、PRIMEFLEX for VMware vSAN V4

  https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

入手できない場合には当社担当営業までお問い合わせください。

6.13 クラスタを停止する

PRIMEFLEX for VMware vSANのクラスタの停止を行うために、クラスタ停止機能を実行します。

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

本機能で停止したクラスタを起動するためには、クラスタ起動コマンドを使用します。
クラスタ起動コマンドの入手方法は『解説書』の「2.12.8 クラスタ停止機能」を参照してください。

クラスタ停止機能の実行前に「6.13.1 動作要件」を参照し、動作要件を必ず確認してください。

クラスタ停止機能は、以下の作業フローで行います。

表6.22 クラスタの停止フロー

クラスタの停止手順		作業内容
1	事前準備	・ クラスタの事前設定 ・ vSAN健全性テストの実施 ・ ISMクラスタ情報の取得・更新 ・ 業務用仮想マシンの停止
2	クラスタ停止の実行	
3	事後処理	・ 電源状態の確認

6.13.1 動作要件

クラスタ停止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。

- PRIMEFLEX for VMware vSANのクラスタであること
- ISM for PRIMEFLEX動作環境
  - 対象クラスタに含まれるすべてのサーバーがISMにノード登録されていること

- 対象クラスタが仮想化管理ソフトウェアに登録されていること

・ クラスタの構成・動作状況

- 対象クラスタのステータスが正常であること
- 動作中のクラスタが対象クラスタ以外に存在する場合、ISM-VAとvCSAは対象クラスタに存在しないこと
  動作中のクラスタが対象クラスタのみの場合、ISM-VAとvCSAは対象クラスタに存在してもよい。
- 対象クラスタ上のすべてのサーバーが起動しており、サーバーはISMおよびESXiのメンテナンスモードでないこと
- クラスタ定義パラメーターが作成されていること
- 仮想リソース管理機能の事前設定が実施されていること

  詳細は、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

・ 仮想化管理ソフトウェアの登録状況

- 仮想化管理ソフトウェアの登録アカウント情報に、vCenter Single Sign-Onドメインの管理者を使用していること

6.13.2 事前準備

クラスタの停止を行う前の準備作業について説明します。

6.13.2.1 クラスタの事前設定を行う

クラスタ管理機能の事前設定を行ってください。

詳細は、『解説書』の「3.8 仮想リソース／クラスタを管理するための事前設定」を参照してください。

6.13.2.2 クラスタのvSAN健全性テストを行う

クラスタのvSAN健全性のテストを行います。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[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]を選択します。
3. [vSANの健全性]に表示されている[テスト結果]で、「失敗」のものについて対処を行います。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[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 [注]]を選択します。
3. [健全性 [注]]に赤で表示されている項目について対処を行います。

[注]：vCSA 7.0以降の場合、[Skyline健全性]または[Skyline Health]と表示されます。

6.13.2.3 ISMクラスタ情報の取得・更新を行う

クラスタ情報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[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ます。

6.13.2.4 業務用仮想マシンを停止する

停止対象のクラスタで動作するすべての業務用仮想マシンを停止します。

vSphere 7.0 Update 1以降の場合、vCLS 仮想マシンの停止は、ISMにより自動で行われます。そのため、本手順で停止する必要はありません。

vCSA 6.5以前（Flash）の場合

1. vSphere Web ClientでvCSAにログインします。
2. 「トップ」画面から[ホーム]タブ-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、停止対象のクラスタに起動状態の仮想マシンがあるか確認します。
4. 起動状態の仮想マシンを選択し、[＜仮想マシン名＞]-[電源]-[ゲストOSのシャットダウン]を選択します。
5. 「ゲストのシャットダウンの確認」画面で[はい]ボタンを選択します。
6. [最近のタスク]に表示されるタスク名[ゲストOSのシャットダウンの開始]のステータスが「完了」となることを確認します。
7. 起動状態の仮想マシンがなくなるまで、手順4～手順6を繰り返します。

vCSA 6.7以降（HTML5）の場合

1. vSphere ClientでvCSAにログインします。
2. 「トップ」画面から[ショートカット]-[インベントリ]-[ホストおよびクラスタ]を選択します。
3. 表示された画面で、停止対象のクラスタに起動状態の仮想マシンがあるか確認します。
4. 起動状態の仮想マシンを選択し、[＜仮想マシン名＞]-[電源]-[ゲストOSのシャットダウン]を選択します。
5. 「ゲストのシャットダウンの確認」画面で[はい]ボタンを選択します。
6. [最近のタスク]に表示されるタスク名[ゲストOSのシャットダウンの開始]のステータスが「完了」となることを確認します。
7. 起動状態の仮想マシンがなくなるまで、手順4～手順6を繰り返します。

6.13.3 クラスタ停止を実行する

クラスタ停止機能を実行して、PRIMEFLEX for VMware vSANのクラスタ停止を行います。

「6.13.1 動作要件」および「6.13.2 事前準備」を参照して、動作要件の確認と事前準備を実施してください。

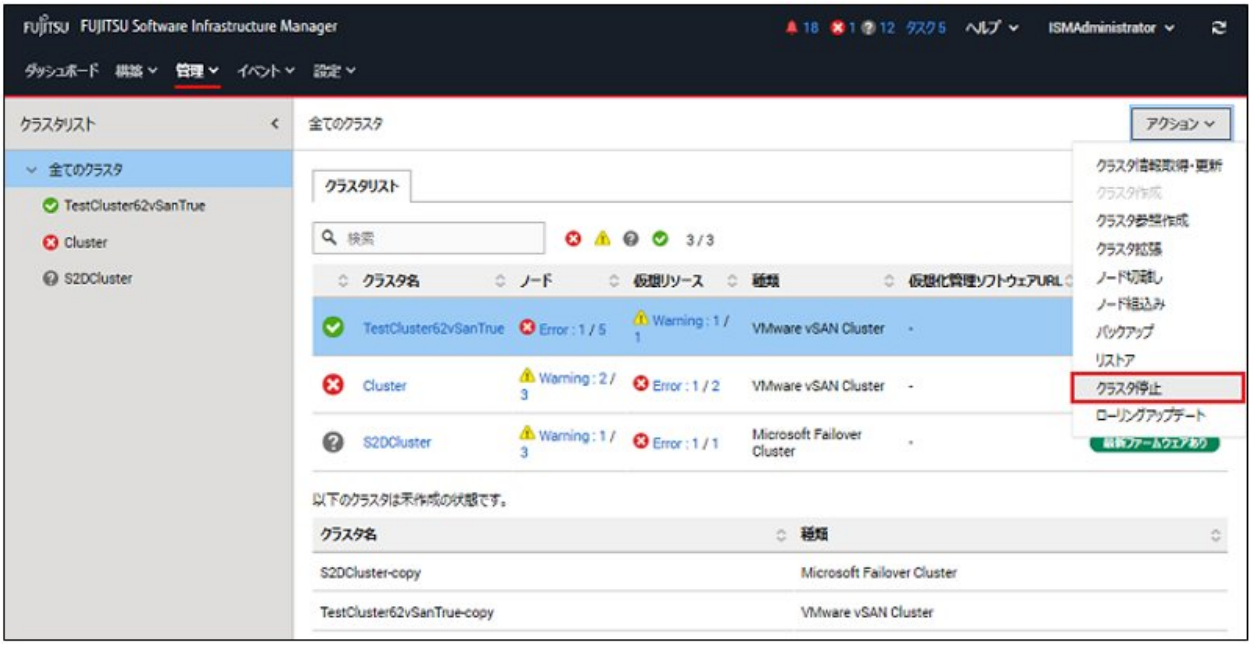
注意

ISM for PRIMEFLEXの他の機能が実行中にクラスタ停止機能を実行しないでください。クラスタ停止機能に失敗します。

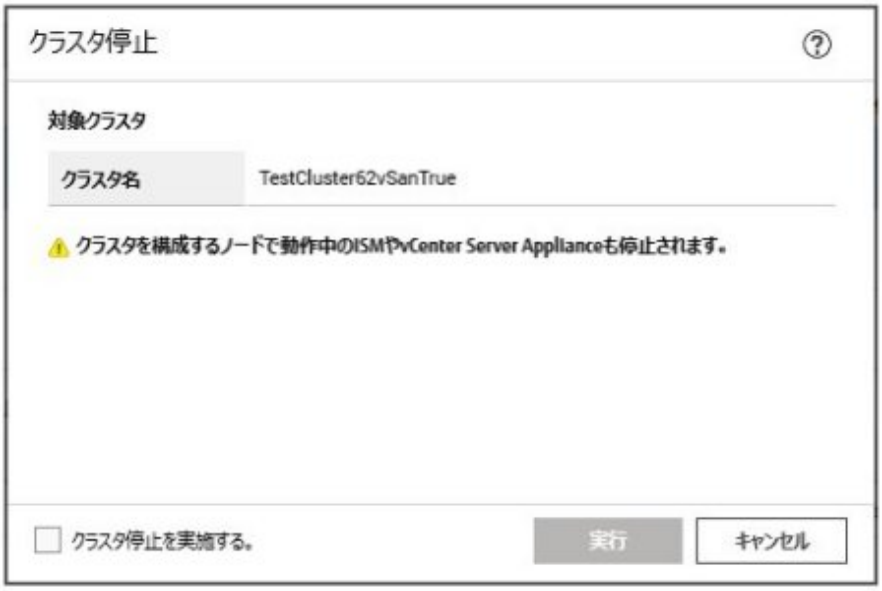
1. ISM管理者（Administratorグループに属し、Administratorロールを持つユーザー）でISMにログインします。
2. ISMのGUIでグローバルナビゲーションメニューから[管理]-[クラスタ]を選択します。

   「クラスタリスト」画面が表示されます。

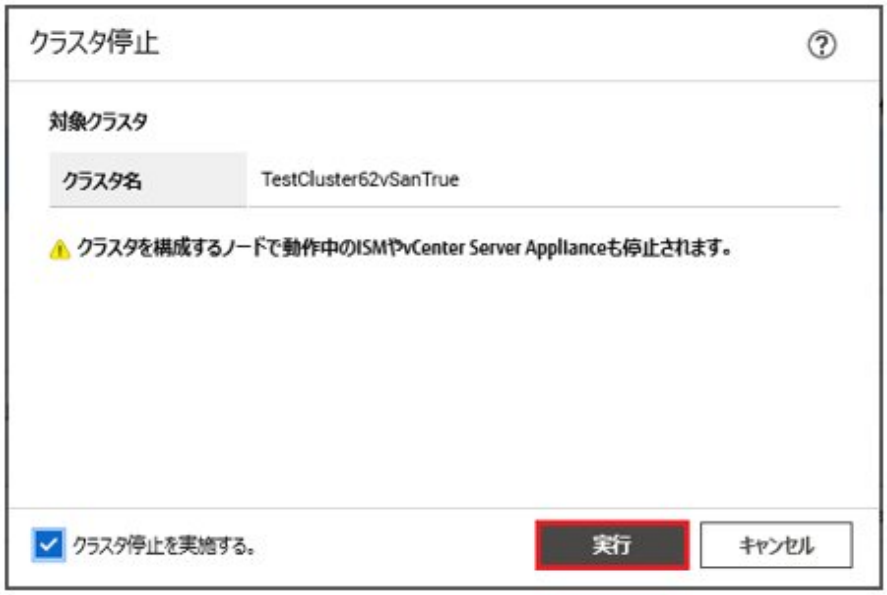
3. [＜対象のクラスタ＞]を選択して、[アクション]ボタンから[クラスタ停止]を選択します。



4. 「クラスタ停止」画面で対象クラスタを確認します。

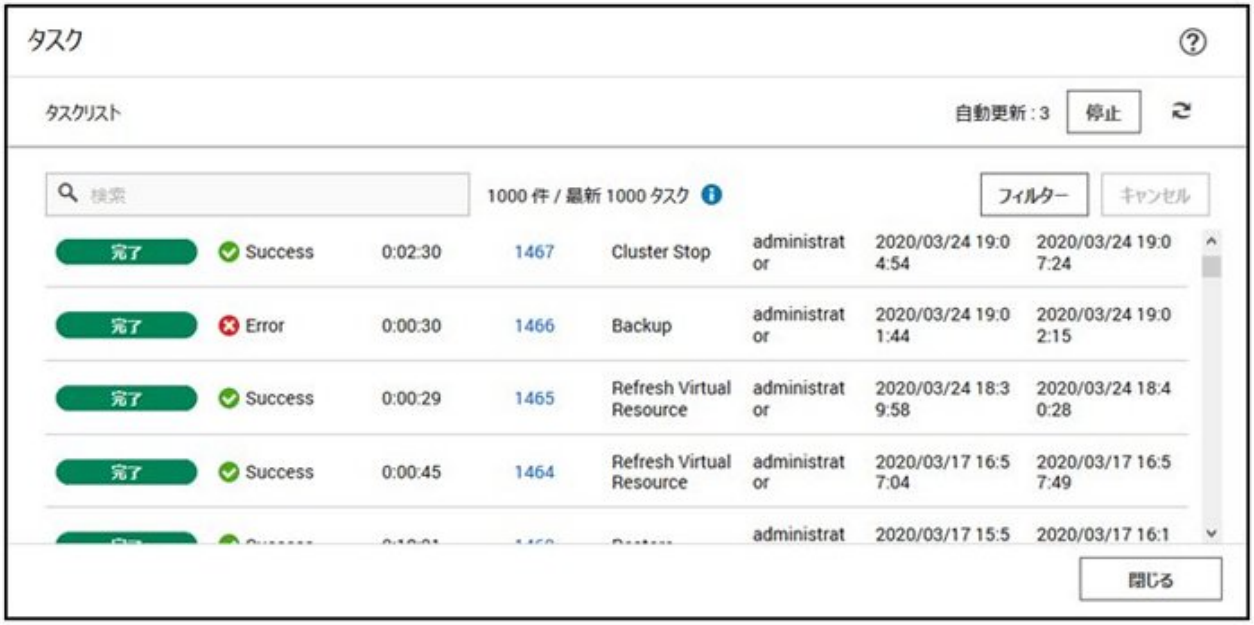


5. 「クラスタ停止を実行する」にチェックを付け、[実行]ボタンを選択します。



クラスタ停止の実行は、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 Stop」となっているのがクラスタ停止のタスクです。



ポイント

「タスク」画面のタスクリストから「Cluster Stop」の[タスクID]を選択すると、「Cluster Stop」の「タスク」画面が表示されます。この画面では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。

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

注意

- 停止させるクラスタ上にISM-VAが存在している場合は、クラスタ停止処理の進行に伴い、ISM-VAも停止します。その結果、GUI画面の更新が停止しISM-VAへのネットワーク接続が切断されますが、正常な動作です。ISM-VAが存在しない場合は、ネットワーク接続が切断することなくタスクは「完了」まで進みます。
- ISMの「タスク」画面にエラーが表示された場合は、ISMのイベントログを確認してください。問題が解決できたら再度操作を行ってください。

6.13.4 事後処理

クラスタの停止の事後処理について説明します。

6.13.4.1 電源状態を確認する

タスクの完了後、クラスタのすべてのサーバーについて電源ランプが停止状態になっていることを目視で確認します。タスクの完了からすべてのサーバーの電源切断まで10分程度かかる場合があります。

6.14 PRIMEFLEXの世代管理情報の表示／切り替えをする

PRIMEFLEXの世代管理情報の表示／切り替えをする手順について説明します。
世代管理情報とは、ISM内で保持する以下の情報を指します。

- PRIMEFLEXの仮想化基盤構築機能やクラスタ作成機能で構築したPRIMEFLEXの世代（登録世代）
- ノードがPRIMEFLEXに参加した契機（登録契機）
- ISMの世代切替機能を実行した後の世代（切替世代）

ISMの動作モードがAdvanced for PRIMEFLEXの場合のみ使用できる機能です。

PRIMEFLEXの世代とは、PRIMEFLEXのモデル名を指します（例：PRIMEFLEX HS、PRIMEFLEX for VMware vSAN V1、PRIMEFLEX for VMware vSAN V2）。

PRIMEFLEX の世代の切り替えとは、後継機種のサーバーの増設と古い世代のサーバーをすべて減設したうえで、PRIMEFLEX の世代を後継モデルの世代に移行することです。

複数世代のサーバーが混在する場合、世代は最も古い世代のサーバーに対応したものとなります(例:世代切り替えを未実施の状態でM4／M5サーバーが混在したシステムの場合、世代は PRIMEFLEX for VMware vSAN V1 となります)。

なお、世代切り替えを実施する場合は、PRIMEFLEX専用SupportDesk契約が必要となります。
詳細は、『サーバー増設／世代切り替えガイド』を参照してください。

https://eservice.fujitsu.com/supportdesk/sdk/sdk?sv=156&lang=JA&mode=2

6.14.1 動作要件

世代の切り替えを使用するには、以下の動作要件を満たす必要があります。

- PRIMEFLEX for VMware vSANのクラスタであること
- 後継機種のサーバーの増設と古い世代のサーバーをすべて減設したうえで実施すること

  PRIMEFLEX for VMware vSANのクラスタが複数ある場合、後継機種のサーバーを増設し、すべてのクラスタにおいて古い世代のサーバーをすべて減設したうえで実施すること

6.14.2 PRIMEFLEXの世代管理情報を表示する

PRIMEFLEXの世代管理情報を表示する手順について説明します。

1. 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. [＜対象のクラスタ＞]を選択します。

   [登録世代]、[切替世代]にVx(xは数字)という形式でPRIMEFLEXの世代が表示されます。

   世代切り替えが実施されていない場合、[切替世代]には「-」が表示されます。

   世代切り替えについては、「6.14.3 PRIMEFLEXの世代管理情報を切り替える」を参照してください。

4. [ノードリスト]タブを選択します。

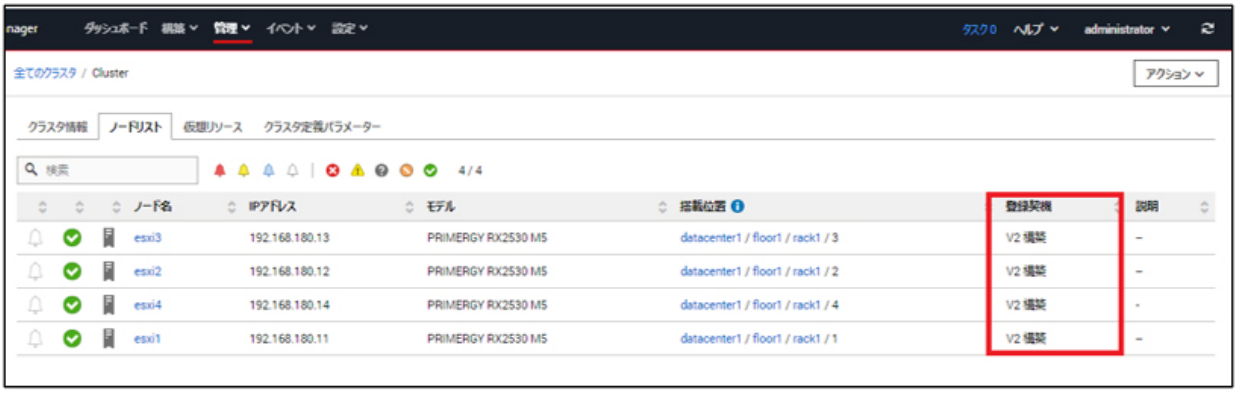
   [登録契機]にVx(xは数字)という形式でPRIMEFLEXの世代が表示されます。

   Vxに続けて、ノードが登録された契機の以下の文言が表示されます。

   ― 構築:仮想化基盤構築機能によるノード登録

   ― クラスタ作成:クラスタ作成機能によるノード登録

ー クラスタ拡張:クラスタ拡張機能によるノード登録



6.14.3 PRIMEFLEXの世代管理情報を切り替える

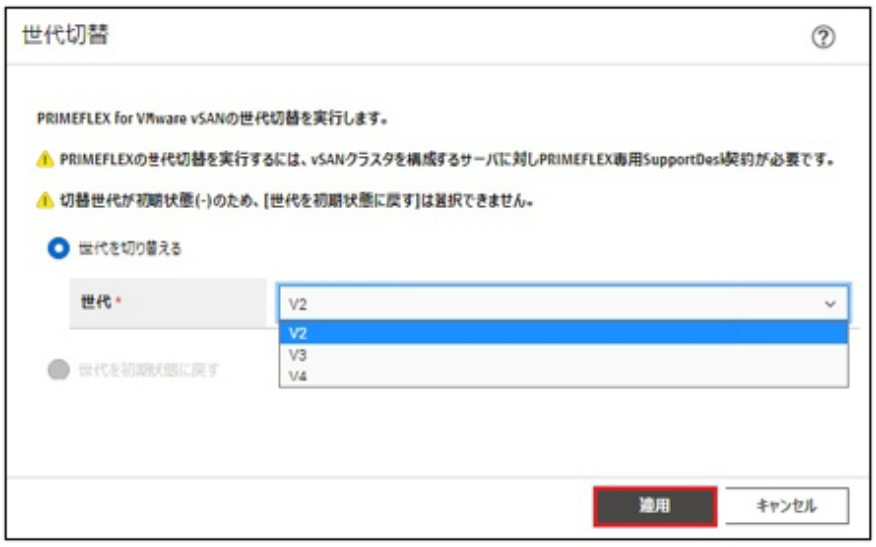
PRIMEFLEXの世代管理情報を切り替える手順について説明します。

1. ISM管理者(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。
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[世代切替]を選択します。

4. 世代を選択し、[適用]ボタンを選択します。

   [世代を切り替える]を選択し、[世代]のリストから世代を選択します。



ポイント

「切替可能な世代はありません。最新の世代です。」と表示される場合は、[閉じる]ボタンを選択し終了してください。

5. [切替世代]が更新されたことを確認します。

注意

- 世代切替結果がエラー表示になっている場合は、[閉じる]ボタンを選択し、動作要件を満たすことを確認してください。その後、手順4を再実行する、もしくは[キャンセル]ボタンを選択して終了してください。

- PRIMEFLEX for VMware vSANのクラスタが複数ある場合、いずれかのクラスタを選択し、[アクション]ボタンから[世代切替]を選択してください。すべてのクラスタで切替世代が更新されます。

6.14.4 PRIMEFLEXの世代管理情報を初期化する

PRIMEFLEXの世代管理情報を初期化する手順について説明します。

1. ISM管理者（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。
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。
3. [＜対象のクラスタ＞] を選択して、[アクション]ボタンから[世代切替]を選択します。

4. [世代を初期状態に戻す]を選択し、[適用]ボタンを選択します。

5. 確認画面で[はい]を選択します。
6. [切替世代]が初期状態(-)に変更されていることを確認します。

6.15 ISMからiRMCのAVR画面を直接表示する

ISMからiRMCのAVR(Advanced Video Redirection:ビデオリダイレクション)(以降「AVR画面」と表記)を表示するには、ノードの詳細画面内[Web I/F URL]にiRMCのIPアドレスを登録しておき、Webインターフェイスを開いてからWebインターフェイスを操作してAVR画面表示する従来の方法があります。ただし、この方法はログイン操作が必要です。

ここでは、iRMCへのログイン操作を行わずに、直接AVR画面を表示する手順について記述します。

AVRの詳細情報については、当社のWebサイトの「AVRの起動手順と動作確認情報」を参照してください。

https://jp.fujitsu.com/platform/server/primergy/products/note/

注意

- ポップアップブロックを解除する必要があります。ご使用のWebブラウザーで、ISMのURLに対してポップアップを許可してください。
- 本機能はiRMCログインをサポートしていないPRIMERGYには使用できません。

  iRMCログインのサポート状況については、当社の本製品Webサイトを参照してください。

  https://www.fujitsu.com/jp/products/software/infrastructure-software/infrastructure-software/serverviewism/environment/
- 中継ルートを経由したAVRの画面表示は、未サポートです。

ポイント

AVRを利用するには、iRMCのライセンスの購入（製品名 リモートマネジメントコントローラアップグレード）が必要です。

6.15.1 ISMからAVR画面を直接表示する

ISMから直接AVR画面を表示する手順について以下に記述します。

AVR画面表示が可能なノードに対してのみ、以下に説明する[開始]ボタンが表示されます。

AVR画面表示を有効にする

ユーザーグループに対してAVR画面表示を有効化します。

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. 対象のユーザーグループを選択し、[アクション]ボタンから[編集]を選択します。
4. [iRMCログイン/AVR]の項目の[有効]を選択します。

ノードリストからAVR画面を表示する

ノードリストの[開始]ボタンを選択してAVR画面を表示します。

1. ISMのGUIでグローバルナビゲーションメニューから[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[AVR]カラムの[開始]ボタンを選択します。

   AVR画面が別ウィンドウで表示されます。

ノードの詳細画面からAVR画面を表示する

ノード詳細画面の[開始]ボタンを選択してAVR画面を表示します。

1. ノードの詳細画面の[AVR]項目の[開始]ボタンを選択します。

   AVR画面が別ウィンドウで表示されます。

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 サーバーの設定をバックアップ／リストアする

ISMに登録したサーバーのハードウェア設定をファイルに保存することにより、ハードウェア設定のリストアやプロファイルの追加、他のISMにエクスポートやインポートできます。

7.1.1 サーバーの設定をバックアップする

ISMに登録したサーバー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ーの電源をオフにし、[サーバー電源状態取得]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。

注意

iRMC設定でLDAPが有効で、ノードの詳細画面の[Web I/F URL]のプロトコルがHTTPのとき、iRMCのファームウェアバージョンによっては、ハードウェア設定のバックアップがエラーとなることがあります。この場合、ノードを編集して[Web I/F URL]のプロトコルをHTTPSに設定してください。ノードの編集については、『解説書』の「2.2.3 データセンター／フロア／ラック／ノードの編集」を参照してください。

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 サーバー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。

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。
- PRIMERGY／PRIMEQUEST 3000B／PRIMEQUEST 4000シリーズサーバーのバックアップでのみ使用できます。

注意

- モデル毎プロファイルは、バックアップから追加できません。
- iRMC設定の[プロキシサーバー]-[パスワード]の項目は設定されません。バックアップからプロファイルを追加したあと、手動で設定してください。

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 サーバー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。

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。
- PRIMERGY／PRIMEQUEST 3000B／PRIMEQUEST 4000シリーズサーバーのバックアップでのみ使用できます。

注意

- モデル毎ポリシーは、バックアップから追加できません。
- iRMC設定の[プロキシサーバー]-[パスワード]の項目は設定されません。バックアップからポリシーを追加したあと、手動で設定してください。

7.1.4 サーバーの設定をインポートする

「7.1.1 サーバー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。

   ― 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。

   ― FTP

     ISM-VAのFTPサーバー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」のディレクトリー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、『解説書』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。
- ISM-VAのFTPサーバーに転送したファイルはインポートが完了したあとは不要です。FTPのコマンドを使用して削除してください。

7.1.5 サーバーの設定をリストアする

「7.1.1 サーバー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 サーバー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に登録したサーバー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ーの電源をオフにし、[サーバー電源状態取得]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。

注意

- VDXのリストアでは、設定項目を初期化してからリストアしてください。初期化されていない項目は、バックアップの内容が反映されないことがあります。

  VDXでは、以下のようにリストアできない設定項目があります。

  ― ライセンス情報

  ― 動作モード

  ― シャーシ／ホスト名

  ― パスワード

  ― 管理用ポート

－ NTP サーバーの設定

－ 日時設定（clock set コマンド）

リストア後に設定内容を確認し、リストアできなかった項目は装置側で設定してください。

- iRMC設定でLDAPが有効で、ノードの詳細画面の[Web I/F URL]のプロトコルがHTTPのとき、iRMCのファームウェアバージョンによっては、ハードウェア設定のリストアがエラーとなることがあります。この場合、ノードを編集して[Web I/F URL]のプロトコルをHTTPSに設定してください。ノードの編集については、『解説書』の「2.2.3 データセンター／フロア／ラック／ノードの編集」を参照してください。

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

ISMに登録したスイッチやストレージの設定をファイルに保存することにより、ハードウェア設定のリストア、他のISMにエクスポートやインポートできます。

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

「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」で保存したファイルをエクスポートします。

1. ISMのGUIでグローバルナビゲーションメニューから[構築]-[プロファイル]を選択します。
2. 画面左側のメニューから[ハードウェア設定バックアップ / リストア]を選択します。
3. ノードを選択して、[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サーバー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」のディレクトリー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、『解説書』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

ISMに登録したスイッチに対して、すでにあるハードウェア設定ファイルをリストアします。リストアできるファイルは、以下のとおりです。

- 「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
- 「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

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サーバーの設定
- 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

トラブルによるISMの設定データの破損や誤操作による設定データの消失などに備えて、ISMの設定値およびノード登録データなどを退避しておき、必要に応じて復元します。

以下にISMのバックアップ／リストアの手順を説明します。

注意

- ISMのバックアップは同一版数のISMにリストアします。異なる版数にはリストアできません。
- ISMのバックアップにはISM-VA内に十分な空き容量が必要です。必要な容量については、『解説書』の「3.2.1.6 ISMバックアップ／リストアに必要な容量の見積り」で解説しています。
- 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。
- 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。

8.1.1 ISMをバックアップする

ISMの設定情報やノード管理データなどをISMのバックアップファイルとして作成します。

8.1.1.1 GUIを利用してISMをバックアップする

ISM GUIへログインし、以下の方法でバックアップを実行およびバックアップファイルを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。

バックアップを実行する

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[バックアップ]を選択します。
3. [アクション]ボタンから[バックアップ]を選択します。
4. 画面の内容を確認し、[上記内容を確認しました。]チェックボックスにチェックを付け、[はい]ボタンを選択します。
5. 「バックアップ確認」画面に従いパスワードを入力し、[確認]ボタンを選択します。
6. バックアップが完了するまで待ちます。

   バックアップが完了後、ログイン画面に移動してください。

7. ログイン後、バックアップが完了したことを確認します。
    a. ISMのGUIでグローバルナビゲーションメニューから[設定]-[全般]を選択します。
    b. 画面左側のメニューから[バックアップ]を選択します。
    c. バックアップファイルリストにバックアップファイルが作成されたことを確認します。

バックアップファイル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[バックアップ]を選択します。
3. 対象のバックアップファイルの[ダウンロード]ボタンを選択してダウンロードを実行します。

バックアップファイルを削除する

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[バックアップ]を選択します。
3. 削除したいバックアップファイルにチェックを付け、[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。

注意

ISM GUIの「バックアップ」画面から実行され、作成されたバックアップファイルは、以下のディレクトリーに保持され、このディレクトリー配下のバックアップファイルだけが表示されます。

バックアップファイル格納ディレクトリー:/Administrator/transfer/webbackup

8.1.1.2 コマンドを実行してISMをバックアップする

ISM にコンソールからログインしてバックアップする手順です。以下の方法でバックアップを実行およびバックアップファイルをダウンロードします。

バックアップを実行する

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 : 3.0.0.x (S2024xxxx-xx)

[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: ism3.0.0.x-backup-20240601120000.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

バックアップファイルをダウンロードする

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。

注意

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

8.1.2 ISMをリストアする

「8.1.1 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から復元します。

8.1.2.1 GUIを利用してISMをリストアする

ISM GUIへログインし、以下の方法でリストアを実行します。

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。

リストアを実行する

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[リストア]を選択します。

   現在のISMのバージョンが表示されます。
3. [リストア]ボタンを選択します。
4. 「リストア用バックアップファイルアップロード」画面に従い管理端末のバックアップファイルを選択し、[適用]ボタンを選択します。
5. 画面の内容を確認し、[上記内容を確認しました。]チェックボックスにチェックを付け、[はい]ボタンを選択します。
6. 「リストア確認」画面に従いパスワードを入力し、[確認]ボタンを選択します。
7. リストアが完了するまで待ちます。

   リストアが完了後、ログイン画面に移動してください。
8. ログイン後、画面にポップアップ表示されるメッセージでリストアされたことを確認します。

8.1.2.2 コマンドを実行してISMをリストアする

ISMにコンソールからログインし、以下の方法でリストアを実行します。

バックアップファイルはあらかじめ、FTPで「ftp://＜ISM-VAのIPアドレス＞/Administrator/ftp」にアップロードします。

リストアを実行する

1. 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。

2. 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 ism3.0.0.x-backup-20240601120000.tar.gz
[System Information]
  Version : 3.0.0.x (S2024xxxx-xx)

[Backup File Information]
  Version : 3.0.0.x (S2024xxxx-xx)

[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。

3. 「y」を入力して、リストアを開始します。

リストア完了後、以下のメッセージが表示されます。

```
You need to reboot the system to use.
It will take several minutes to complete.
Immediately reboots the system.  [y/n]:
```

4. 「y」を入力して、ISM-VAを再起動します。

8.1.3 リストア後の設定をする

以下の設定値は、ISMバックアップ／リストアで復元されません。必要に応じて設定してください。

- 仮想ディスクの割当て

  仮想ディスクの割当て状態を確認し、必要に応じて実施してください。

- リポジトリ

  必要に応じて、リポジトリにコンテンツを再インポートしてください。

- 保管ログ、ノードログ

  保管ログ、ノードログは初期化状態となっています。

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。

ポイント

以下の機能の保守資料採取については、『解説書』の「4.5.1 必要な保守資料」を参照してください。

- 仮想リソース管理機能
- クラスタ管理機能
- クラスタ作成機能
- クラスタ拡張機能

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、以下を選択し、[実行]ボタンを選択します。

   ー 採取対象

   - 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
   - 一部：障害調査ログのみの採取

   ー 採取期間

   - 全期間
   - 指定期間：開始日付と終了日付を指定

   ### 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、『解説書』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. ブラウザー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。

   キャンセルされた保守資料は削除されます。

注意

- 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ーに保持され、このディレクトリー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ー:/Administrator/transfer

  ISM-VAのFTP送受信ディレクトリー/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。

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

   ― 障害調査ログのみを採取する場合(期間指定なし)

```
# ismadm system snap -dir /Administrator/ftp
snap start
Your snap has been generated and saved in:
  /Administrator/ftp/ismsnap-20220110175323.zip
```

   ― 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をする場合(期間指定なし)

```
# ismadm system snap -dir /Administrator/ftp -full
snap start
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220110175808-full.zip
```

   ― 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／アノマリ検知機能および仮想ネットワークパケット分析機能で収集された統計情報を一括採取する場合(期間指定必須)

   採取期間(2022年5月18日～2022年5月19日)を指定して収集する場合

```
# ismadm system snap -dir /Administrator/ftp -full -extstats -from 20220518 -to 20220519
snap start
```

```
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220519072513-20220518-20220519-full-extstats.zip
```

ー 採取期間(2021年12月10日～2022年1月10日)を指定して障害調査ログのみを採取する場合

```
# ismadm system snap -dir /Administrator/ftp -from 20211210 -to 20220110
snap start
Your snap has been generated and saved in:
  /Administrator/ftp/ismsnap-20220110175323-20211210-20220110.zip
```

ー 採取期間(2021年12月10日～2022年1月10日)を指定して障害調査ログ／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をする場合

```
# ismadm system snap -dir /Administrator/ftp -full -from 20211210 -to 20220110
snap start
Your snap has been generated and saved in:
 /Administrator/ftp/ismsnap-20220110175808-20211210-20220110-full.zip
```

ポイント

ー -dirは出力先の指定です。『解説書』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。

ー 採取する保守資料の期間を指定する場合は、「-from」および「-to」オプションを追加して採取開始日と採取終了日を指定してください。指定する日付は「YYYYMMDD」形式で指定してください。採取する保守資料の期間を指定した場合はファイル名に採取開始日と採取終了日が追加されます。採取開始日と採取終了日はISM-VAに設定されているタイムゾーンを元に設定されます。

なお、期間を指定しない場合は、全期間を対象として保守資料を採取します。

注意

ー 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、『解説書』の「3.2.1.5 保守資料容量の見積り」を参照してください。

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

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

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ー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。保存された保守資料は自動削除されないため、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。

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 修正パッチ／アップグレードプログラムを適用する

ISMに修正パッチ／アップグレードプログラムを適用します。

ポイント

ISMの修正パッチ、アップグレードプログラムを入手する場合は、SupportDesk-Webからダウンロードしてください(SupportDesk契約が必要です)。

SupportDesk-Webについては、以下のURLを参照してください。

https://eservice.fujitsu.com/supportdesk/

注意

- 修正パッチ／アップグレードプログラムを適用する前に、ISMが動作しているハイパーバイザーでバックアップ(エクスポート)してください。
- システムをアップデートするためにISM-VAのディスク容量を使用します。必要なディスク容量は、『解説書』の「1.3.1 ISM-VAを動作させるハイパーバイザーの要件」の「修正パッチまたはアップグレード適用後のシステムアップデート」を参照してください。
- 修正パッチ／アップグレードプログラムを適用する際、ISM-VAが再起動されます。プロファイル適用やファームウェアアップデートなどのタスクがすべて完了してから適用してください。

1. 修正パッチまたはアップグレード適用時に必要となるディスク容量を確認します。

   修正パッチ適用の場合

   a. コンソールからadministratorでISM-VAにログインし、以下のコマンドを実行します。

   ```
   # apply-update
   ```

   以下のいずれかのメッセージが表示されます。

   (表示例3)が表示された場合、以降の手順 b ～ dの作業は不要です。

   (表示例1)

   ```
   Ready to start System update.

   Number of total node logs: 75416
   Disk size required for system updates: 31.1MB
   Size of available space: 20.8MB
   Not Enough hard disk space for system update without deleting Node Log.
   If system update without deleting Node Log, after selection “0: Cancel System Update” please free at least an
   additional 31.1MB of disk space on ‘/’.
   If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the menu below.

   1: System Update (Delete Node Log)
   0: Cancel System Update
   Please select one of the mode:
   ```

ポイント

メッセージ内に"Disk size required for system updates"が表示されている場合、システムアップデート時にディスク容量不足によりノードログを削除する必要があります。
過去のノードログを保管しておきたい場合、以下のいずれかを実施してください。

- "Size of available space"(現在の空きディスク容量)に表示されている容量を確認し、"Disk size required for system updates"に表示されている容量分まで、容量を確保する。
- 『解説書』の「2.5.6 ノードログのダウンロード」を参照して、事前にノードログをダウンロードする。

(表示例2)

```
Ready to start System update

Number of total node logs: 27364
Time of System update depends on the number of Node log.
If you do not need the node logs, please select "1: System Update (Delete Node Log)" from the menu below.
"Delete Node Log" contributes to shortening of System upgrade.

1: System Update (Delete Node Log)
2: System Update (Node Log Undeleted)
0: Cancel System Update
Please select one of the mode:
```

(表示例3)

```
Your system is up to date.
```

b. "Number of total node logs"の行の数値(ISMに登録されている全ノードのノードログ件数)を確認します。

c. 「0: Cancel System Update」を選択しメッセージ表示を終了します。

d. 以下の計算式で必要なディスク容量を算出します。

＜手順bで確認した値＞ × 500Byte

アップグレード適用の場合

a. ISMのGUIでグローバルナビゲーションメニューから[管理]-[ノード]を選択します。

b. 「ノードリスト」画面でノード名を選択します。

c. ノードの詳細画面で[プロパティ]タブを選択し、「ノードログ」に表示されているノードログ件数を確認します。

d. ISMに登録されている全ノードのノードログ件数を合計し、以下の計算式で必要なディスク容量を算出します。

＜全ノードのノードログ件数＞ × 500Byte

2. コンソールからadministratorでISM-VAにログインし、システム領域(ISM-VA全体)とAdministratorユーザーグループの空きディスク容量を確認します。

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

システム領域(ISM-VA全体)の空きディスク容量は、マウント位置が「/」の行の「残り」を参照してください。

Administratorユーザーグループに仮想ディスクを割当てている場合は、Administratorユーザーグループの空きディスク容量も確認してください。

Administratorユーザーグループの空きディスク容量は、マウント位置が「'RepositoryRoot'/Administrator」の「残り」を参照してください。

3. 修正パッチまたはアップグレード適用に必要なディスクを追加します。

手順1で算出されたディスク容量と修正パッチファイルまたはアップグレードファイルのサイズを元に、適用するために必要なディスク容量を確認します。

ー Administratorユーザーグループに仮想ディスクを割当てていない場合

システム領域（ISM-VA全体）に必要な空き容量：

「手順1 で算出された容量」と「修正パッチファイルまたはアップグレードファイルサイズの6倍程度の容量」の合計

ー Administratorユーザーグループに仮想ディスクを割当てている場合

- システム領域（ISM-VA全体）に必要な空き容量：

  「修正パッチファイルまたはアップグレードファイルサイズの3倍程度の容量」

- Administratorユーザーグループに必要な空き容量：

  「手順1 で算出された容量」と「修正パッチファイルまたはアップグレードファイルサイズの3倍程度の容量」の合計

空き容量が不足している場合は、システム領域（ISM-VA全体）とAdministratorユーザーグループそれぞれに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、『解説書』の「3.7 仮想ディスクの割当て」および「4.6 仮想ディスクの管理」を参照してください。

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[修正パッチ／アップグレードプログラム]を選択します。

   現在のISMのバージョンが表示されます。
6. [ISMを更新する]ボタンを選択します。
7. 「修正パッチ／アップグレードプログラム」画面に従い設定項目を入力し、[確認]ボタンを選択します。
8. 表示内容を確認し、[はい]ボタンを選択します。
   修正パッチ／アップグレードが適用されます。適用の最中にISM-VAが再起動されます。
9. 修正パッチの適用またはアップグレードが完了するまで待ちます。

   修正パッチの適用またはアップグレードの完了後、キャッシュをクリアし、ログイン画面に移動してください。
10. ログイン後、修正パッチまたはアップグレードが適用されたことを確認します。

    ISMのGUIでグローバルナビゲーションメニューから[ヘルプ]-[ISMについて]を選択します。
    選択したバージョンが表示されていることを確認します。