

SigmaSystemCenter 3.8

簡易構築ガイド VMware 編

利用条件・免責事項

本書の利用条件や免責事項などについては、次のページを参照してください。

<http://jpn.nec.com/site/termsfuse.html>

目次

1. お使いになる前に.....	1
1.1 本ガイドで実現するシステム	1
1.2 構築の流れ	2
1.3 システム構成と使用機材	2
2. インストール前の準備.....	5
2.1 管理サーバの準備.....	5
2.2 管理対象（物理サーバと仮想マシン）の準備	5
3. インストール.....	7
3.1 SSC のインストール.....	7
4. 初期設定.....	8
4.1 ユーザの作成	8
4.2 ライセンスの登録.....	10
5. 基本設定(管理対象の自動登録).....	12
5.1 サブシステムの登録.....	12
5.2 リソースの登録の確認.....	15
5.2.1 仮想ビュー	15
5.2.2 リソースビュー.....	16
5.2.3 運用ビュー	17
5.2.4 増設した物理サーバや新規に作成した仮想マシンの登録について	19
5.3 リソースプールの確認.....	20
5.3.1 vCPU の単位の設定	23
5.3.2 データストアの設定	24
5.4 負荷状況の確認.....	24
5.5 手動での仮想マシンの移動(Migration(vMotion))	26
6. レポート機能の利用（負荷状況取得の設定）.....	31
6.1 レポートの作成.....	31
6.1.1 リソースプール(ESXi グループ)のレポート作成	31
6.1.2 個別の仮想マシンのレポート作成.....	34
6.2 レポートの閲覧.....	37
6.2.1 リソースプール概要のレポート	38
6.2.2 業務用仮想マシンの負荷履歴レポート	39

7. 電源操作の設定	41
7.1 物理サーバの設定	41
7.1.1 iLO (BMC) の設定	41
7.1.2 Express5800/D120h などの BMC/CMC の設定	45
7.1.3 SSC での OOB のアカウント設定	50
7.2 動作テスト(一括電源操作)	53
7.2.1 仮想マシン自動起動の設定	53
7.2.2 マシンシャットダウン	54
7.2.3 マシン起動	57
8. 予兆を含む障害対応機能の設定	60
8.1 監視・通報の基本設定	60
8.1.1 SNMP Trap サービスの設定	60
8.1.2 Windows ファイアウォールの設定	60
8.1.3 死活監視の基本設定	63
8.1.4 通報に必要な環境設定	63
8.2 負荷監視の設定	65
8.3 死活監視の設定	72
8.4 障害や負荷に対するポリシーの設定	74
8.4.1 ポリシーのインポート	75
8.4.2 仮想マシン用ポリシーの確認と適用	77
8.4.3 物理サーバ用ポリシーの確認と適用	80
8.5 動作テスト(擬似障害テスト)	85
付録 A. 運用に関する重要な情報	93
付録 B. 負荷状況取得の設定	94
B.1 物理サーバの負荷状況取得の設定	95
B.1.1 物理サーバ上の設定	96
B.1.2 ESXi の運用グループの設定	96
B.2 業務用仮想マシンの負荷状況取得の設定	97
B.2.1 ESXi 経由での負荷状況取得の設定	98
B.2.2 ゲスト OS 経由での負荷状況取得の設定	99
付録 C. SigmaSystemCenter マニュアル体系	102
付録 D. 改版履歴	104
付録 E. ライセンス情報	105
用語集	106

はじめに

この文書では、「VMware vSphere」と管理ツールの「WebSAM SigmaSystemCenter 3.8」を用いて、仮想マシンシステムを構築する手順を紹介します。SigmaSystemCenter は仮想化に対応した統合管理プラットフォームであり、物理的なサーバで動作するホストと仮想マシンを単一のコンソールから統一的に管理することが可能です。

- 対象読者と目的

「WebSAM SigmaSystemCenter 3.8 簡易構築ガイド」は、SigmaSystemCenter により仮想化サーバと仮想マシンを管理するシステムの構築、運用するために必要な最低限の知識と手順に限り説明しています。

よって、本書では SigmaSystemCenter の全ての機能、役割について説明しておらず、本書で説明する以外の機能の利用、応用については、「[付録 C. SigmaSystemCenter マニュアル体系 \(102 ページ\)](#)」で紹介のドキュメントをお読みください。

1. お使いになる前に

注

[重要] トラブルを避けるため、SigmaSystemCenter(以降、SSC と記述します)をお使いになる前に、「[付録 A. 運用に関する重要な情報 \(93 ページ\)](#)」をよくお読みください。

1.1 本ガイドで実現するシステム

本書で構築するシステムでは、以下の機能を実現することを目標とします。下記の 1 のみなど、一部の機能のみを利用することも可能です。

1. リソース使用状況、稼働状況を収集・閲覧する。

以下の対象の稼働状況を収集し、定期的にレポートを作成します。

- 業務用仮想マシン
- 物理サーバ (ESXi)

2. 電源操作を行う。

以下の対象の電源操作を可能にし、保守運用時に利用します。対象の一括電源操作も可能になります。

- 業務用仮想マシン
- 物理サーバ (ESXi)

3. 障害・負荷監視、および、障害時の自動対応を行う。

- 障害監視を行う。

以下の対象の障害を監視します。

- 業務用仮想マシン
- 物理サーバ (ESXi)

- 負荷監視を行う。

以下の対象の負荷を監視します。

- 業務用仮想マシン
- 物理サーバ (ESXi)

- 予兆障害を契機に仮想マシンを自動移動(Migration(vMotion))する。

物理サーバ (ESXi) の障害予兆を検出し、物理サーバの障害が悪化する前にその上で動作する仮想マシンを別の物理サーバへ自動移動します。

- 業務用仮想マシン

1.2 構築の流れ

本書では、以下の流れで SSC の構築を行います。図の各作業の冒頭にある数字は本書の章番号になります。

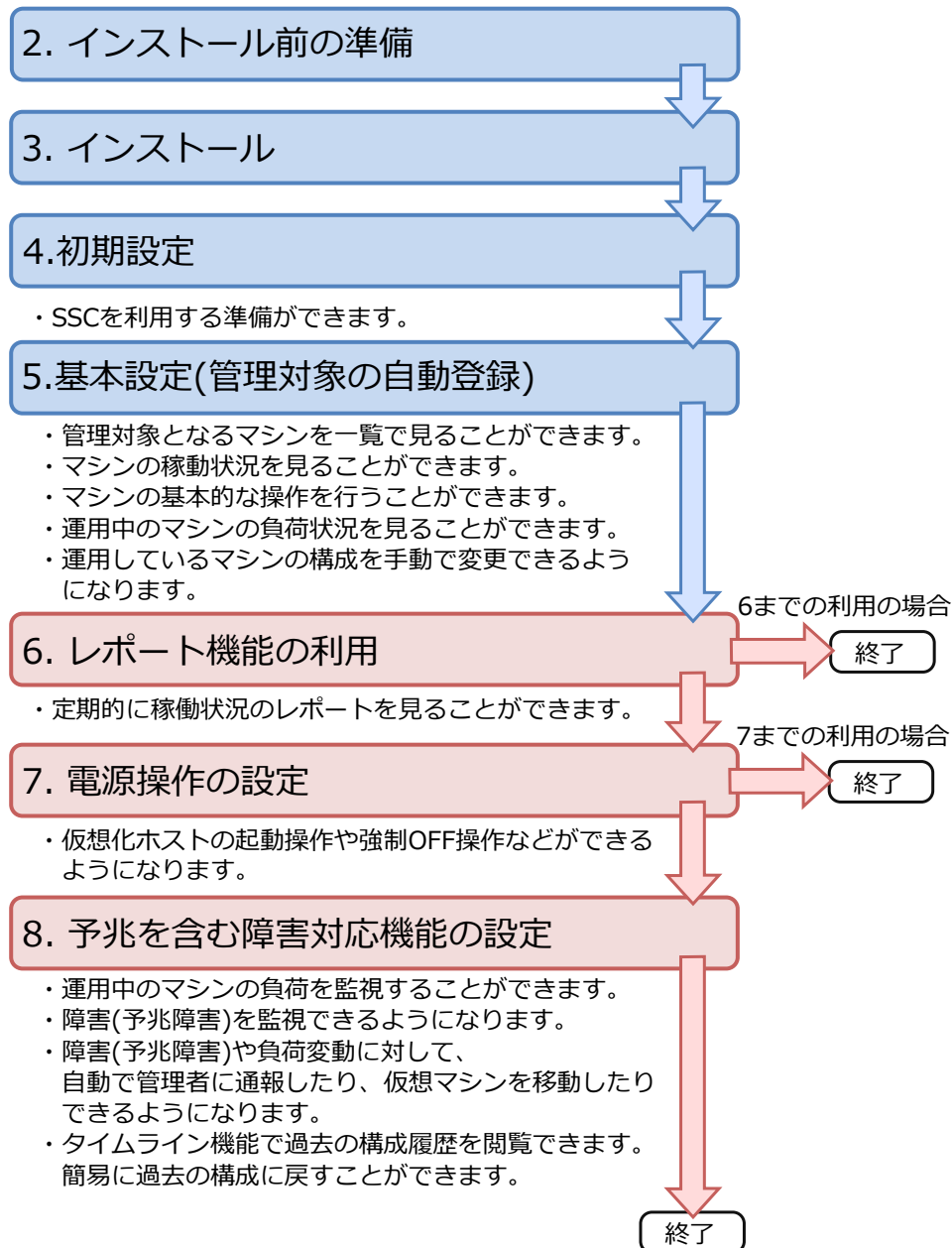


図 本ガイドでの構築の流れ

1.3 システム構成と使用機材

今回構築するシステムの構成は以下のとおりです。

- 管理対象
 - 物理サーバ (3 台)
 - * VMware ESXi
 - * ホスト名 : マシン名 : IP アドレス(管理用ネットワーク)
 - + esxi1 : esxi1.vsphere.local : 172.16.10.1
 - + esxi2 : esxi2.vsphere.local : 172.16.10.2
 - + esxi3 : esxi3.vsphere.local : 172.16.10.3
 - * BMC のホスト名 : IP アドレス(管理用ネットワーク)
 - + bmc1 : 172.16.20.1
 - + bmc2 : 172.16.20.2
 - + bmc3 : 172.16.20.3
 - 業務用仮想マシン (6 台)
 - * Windows Server 2016 Standard
 - * ホスト名(マシン名) : IP アドレス(VM 管理用ネットワーク)
 - + VM-01 : 172.20.100.1
 - + VM-02 : 172.20.100.2
 - + VM-03 : 172.20.100.3
 - + VM-04 : 172.20.100.4
 - + VM-05 : 172.20.100.5
 - + VM-06 : 172.20.100.6
 - * ※サービス用ネットワークについては説明を省略します。業務の必要に応じて設定してください。
- 管理サーバ用物理サーバ (1 台)
 - VMware ESXi
 - SigmaSystemCenter 管理サーバ(仮想マシン)
 - * Windows Server 2016 Standard
 - * SigmaSystemCenter
 - * ESMPRO/ServerManager(*1)
 - * ホスト名 : IP アドレス
 - + SSCmanager : 172.16.0.1 (管理用ネットワーク), 172.20.0.1(VM 管理用ネットワーク)
 - vCenter Server Appliance(VCSA)(仮想マシン)

- * ホスト名: vcenter.vsphere.local
- * IP アドレス : 172.16.0.2 (管理用ネットワーク)

(*1) 「8. 予兆を含む障害対応機能の設定 (60 ページ)」を利用する場合、および、対象物理サーバが Express5800/R120h、Express5800/T120h の場合、管理サーバに ESMPRO/ServerManager のインストールが必要です。

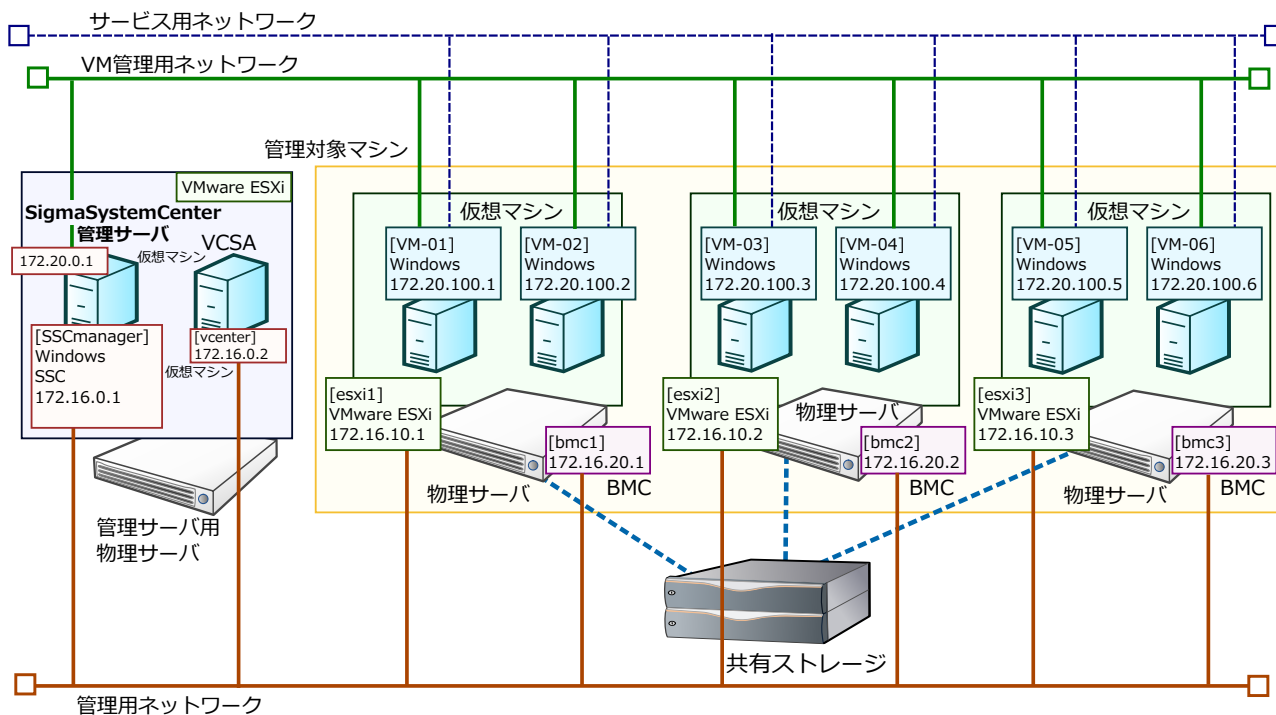


図 今回構築するシステムの構成

上記のように、3 台のラックサーバ上で 6 台の業務用の仮想マシンを運用します。仮想マシンは 7 台でも 8 台でもかまいませんが、仮想マシンの必要とするリソースが物理サーバのキャパシティを超えないようにサイジングには十分注意する必要があります。

2. インストール前の準備

SSC をインストールする前に行う準備を説明します。SSC をインストールする前の準備には、大きく分けて「管理サーバの準備」、「管理対象（物理サーバと仮想マシン）の準備」の二種類があります。

また、本ガイドでは、仮想マシンのシステムバックアップ、仮想マシンへのソフトウェア配布といった DeploymentManager(DPM)の機能の利用を想定していないため、DPM を利用するための説明は省略しています。DPM を利用する予定がある場合は、管理サーバと同一のネットワーク内に DHCP サーバを用意し、仮想マシンに DPM クライアントをインストールするなど、必要な設定を別途実施してください。

2.1 管理サーバの準備

管理サーバには、あらかじめ以下のソフトウェアをインストールしておきます。

- Windows Server

管理サーバの Windows Server については、本書では、Windows Server 2016 を使用した場合を例を中心に説明を行います。

※Windows Server 2016 以外の場合は「SigmaSystemCenter 3.8 インストレーションガイド」を参照してください。

<https://jpn.nec.com/websam/sigmasystemcenter/download.html>

Windows Server のインストール後、PowerShell の以下のコマンドを実行して後述の役割と機能を追加してください。

```
PS> Add-WindowsFeature Web-Server,Web-Static-Content,Web-Asp-Net45,Web-Mgmt-Console
```

上記コマンドより、以下の役割と機能が追加されます。

- Web サーバー (IIS)
 - 静的なコンテンツ
 - ASP.NET 4.6
 - IIS 管理コンソール

2.2 管理対象（物理サーバと仮想マシン）の準備

管理対象のラックサーバには、最初に以下の仮想化基盤ソフトウェアをインストールしておきます。

- ESXi

次に、業務で利用する仮想マシンの作成とゲスト OS のインストールを済ませておいてください。今回は仮想マシンの移動(Migration(vMotion))を利用する関係上、仮想マシンの構成ファイル群を共有ストレージ上に配置する必要があります。

3. インストール

ここでは、SSC のインストールとそれに伴う管理サーバの設定について説明します。

3.1 SSC のインストール

管理サーバに SSC のインストールメディアをセットし、インストーラ（`ManagerSetup.exe`）をダブルクリックして起動します。

すべてのコンポーネントをチェックして、[実行]をクリックしてください。あとはインストールウィザードにしたがって作業を進めます。

なお、ESMPRO/ServerManager を利用する場合、6.35 以上のバージョンをインストールしてください。SSC に添付されていない ESMPRO/ServerManager も利用可能です。

4. 初期設定

SSC の Web コンソールにアクセスします。

Web ブラウザを起動し、[http://管理サーバのホスト名または IP アドレス:ポート番号/Provisioning/Default.aspx]にアクセスしてください。

今回の場合は、http://172.16.0.1/Provisioning/Default.aspx にアクセスします。

以下の「SigmaSystemCenter ログイン」画面が表示されますので、初期アカウントとして設定されているユーザ名("admin")、パスワード("admin")を入力し、[ログイン]をクリックしてログインします。

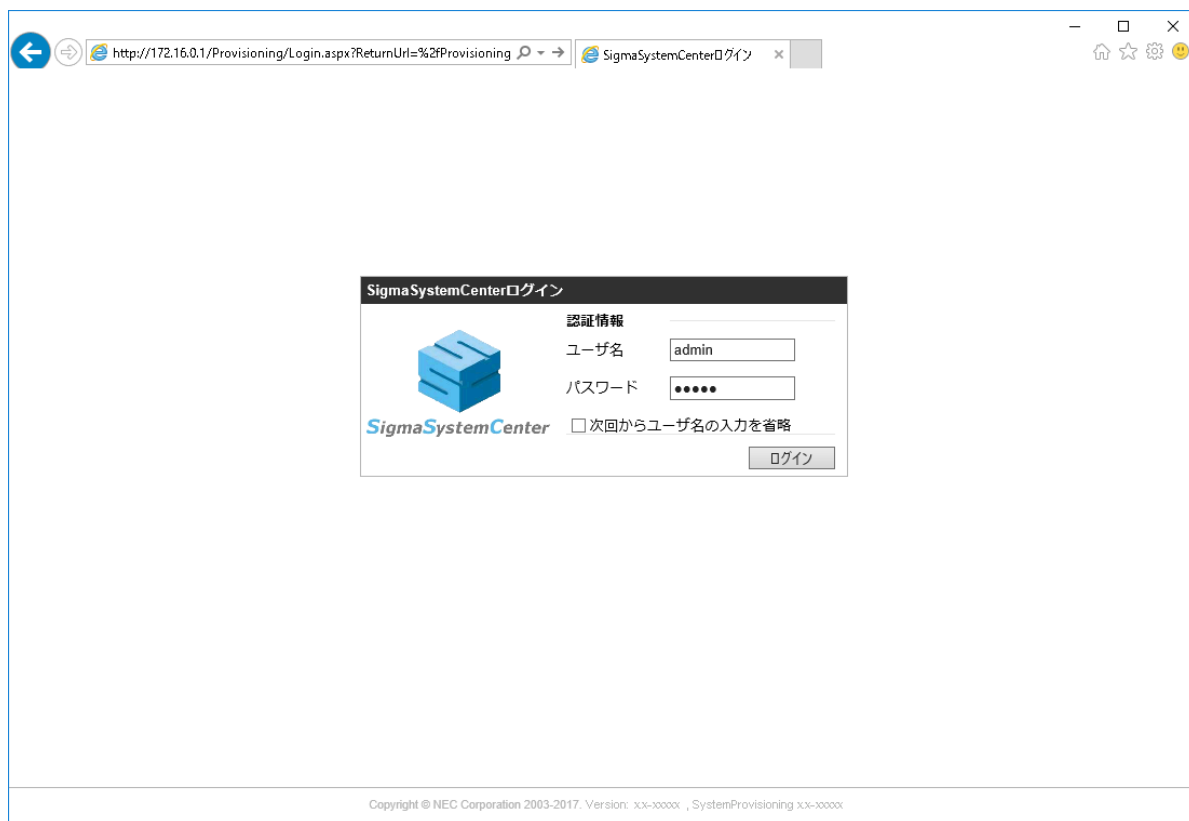


図 「SigmaSystemCenter ログイン」画面

4.1 ユーザの作成

Web コンソールが表示されたら、普段の管理で使うためのユーザを作成します。

画面右上にあるビュー切り替えリンクの中から[管理]をクリックし、[管理]ビューに移動します。

画面左側のツリービューにある[ユーザ]をクリックし、「ユーザー一覧」、「ロール一覧」の画面を表示されたら「ユーザー一覧」の枠の右上の[追加]をクリックし「ユーザ追加」画面を表示します。

[ユーザ名]、[パスワード]、[認証種別]、[ロール名]を設定し[OK]をクリックすると、ユーザが作成されます。今回は、[ユーザ名]を"sysadmin"とし、[ロール名]には[システム管理者]を選択しました。今回、作成するユーザは、LDAP を利用した認証を行わないので、[認証種別]には、[Local]を選択します。[パスワード]には任意の文字列を設定してください。

The screenshot shows the 'Add User' (ユーザ追加) screen in SigmaSystemCenter. The form fields are as follows:

- ユーザ名: sysadmin
- パスワード: [masked]
- パスワード(確認): [masked]
- 認証種別: Local
- 通報先メールアドレス: [empty]
- 説明: [empty text area]

Below the form, there are two tables:

グループ一覧

グループ	説明
[empty]	[empty]

ロール一覧

ロール名	設定対象	説明
<input checked="" type="checkbox"/> システム管理者	全リソース / システム	全ての操作・管理が可能です
<input type="checkbox"/> 参照者	全リソース / システム	各リソースへの参照のみ可能です
<input type="checkbox"/> 操作者	全リソース / システム	管理対象マシンに対する全ての操作が可能です
<input type="checkbox"/> 運用管理者	システム	運用Viewのみ表示可能です

図 「ユーザ追加」画面

[OK]をクリックすると「ユーザー一覧」、「ロール一覧」の画面に遷移し、「ユーザー一覧」に"sysadmin"が追加されていることが確認できます。

注

デフォルトの"admin"ユーザは正規のシステム管理者ユーザを追加するまでの仮のユーザであるためユーザー一覧には表示されません。また、正規のシステム管理者ユーザを追加した後、デフォルトの"admin"ユーザは無効になりログインできなくなります。



図 「ユーザー一覧」、「ロール一覧」画面（sysadmin 追加後）

ユーザが作成できたら、作成したユーザでログインしなおしてください。ログアウトするためには、画面右上の[ログアウト]をクリックします。

4.2 ライセンスの登録

ライセンス登録を行います。画面右上の[管理]をクリックし、[管理]ビューに移動します。画面左側のツリービューにある[ライセンス]をクリックし、遷移した「ライセンス」画面の一番下にある[ライセンス追加]の枠の[ライセンスキー]ラジオボタンを選択します。[ライセンスキー]のテキストボックスにライセンスキーを入力して[追加]をクリックしてください。

「PVMService を再起動しライセンスを有効化してください。」というメッセージが表示されたら、[OK]をクリックしてください。[ライセンス個別情報]に追加したライセンスキーが表示されます。



図 ライセンス登録の画面

すべてのライセンスの登録が完了したら、Windows の[スタート]メニューから[Windows 管理ツール]→[サービス] で[PVMService]を再起動してください。

5. 基本設定(管理対象の自動登録)

管理対象となるマシンを登録します。SSC では管理機能がコンポーネント化（サブシステム化）されていますので、管理対象に対応するサブシステムを SSC 本体に登録します。

今回は管理対象が VMware ESXi ですので、サブシステムとして VMware vCenter Server を先に登録します。

5.1 サブシステムの登録

SSC の[管理]ビューを開き（画面右上の[管理]をクリック）、画面左側のツリービューにある[サブシステム]をクリックします。画面右下の[設定]メニューにある[サブシステム追加]をクリックすると、「サブシステム追加」画面が表示されますので、[サブシステム種類]ドロップダウンリストで[VMware vCenter Server]を選択します。残りの項目は以下のように設定します。

- ホスト名：vCenter Server のサーバのホスト名もしくは IP アドレス
(本書では"vcenter.vsphere.local"を入力)
- ポート：vCenter Server に接続するための HTTPS ポート
(入力を省略した場合、デフォルトの"443"になります)
- URL：何も入力しないでください。
- アカウント名：vCenter Server の管理アカウント名
- パスワード：vCenter Server の管理アカウントのパスワード
- [マシンを運用グループへ自動登録する]のチェックをオン

※このチェックを行わない場合、管理対象の登録の操作を手動で行う必要がありますので、忘れずチェックを行ってください。

- [マシンの性能監視を有効にする]のチェックをオン

※このチェックを行わない場合、負荷状況の取得の設定を手動で行う必要がありますので、忘れずチェックを行ってください。

上記の項目を入力したら[OK]をクリックしてください。

The screenshot shows the 'Add Subsystem' form in the SigmaSystemCenter interface. The form includes fields for Subsystem Type, Host Name, Port, URL, Account Name, Password, and Description. Two checkboxes at the bottom are checked and highlighted with a red box: 'Automatically register machines to the operation group' and 'Enable performance monitoring for machines'. The 'OK' and 'Cancel' buttons are located at the bottom right of the form.

図 vCenter Server の登録

前述の[VMware vCenter Server]のサブシステムの登録を行うと、「VMware vCenter Server」と一緒にその vCenter Server で管理している ESXi、および、ESXi 上で動作する仮想マシンが自動的に検出/登録されます。

注

[マシンを運用グループへ自動登録する]のチェックをオンにして、サブシステム登録を行うと、SSC の全ビューへの登録の処理が行われるため、しばらく時間がかかります。

登録の処理完了後に「サブシステム一覧」画面の[操作]メニューで[画面更新]をクリックすると、ESXi がサブシステム一覧に表示されます（表示されていない場合は少し時間を置いて画面を更新してみてください）。



図 「サブシステム一覧」画面

もっとも、ESXi が検出されただけでは、仮想マシンの再起動(Failover)などの一部の操作を SSC から実行することができません。そこで次の追加の設定を行います。

「環境設定」の[仮想リソース]タブで、VMware ESXi 仮想マシンサーバの root パスワードの既定値を設定します。

ヒント

下記「環境設定」でのパスワードの設定は、検出した 3 台の ESXi のパスワードが共通の場合に利用できます。各 ESXi で異なるパスワードの場合は、前述の「サブシステム一覧」画面の各 ESXi の行の右端にある[編集]アイコンをクリックし、「サブシステム編集」画面で個別にパスワードを設定してください。

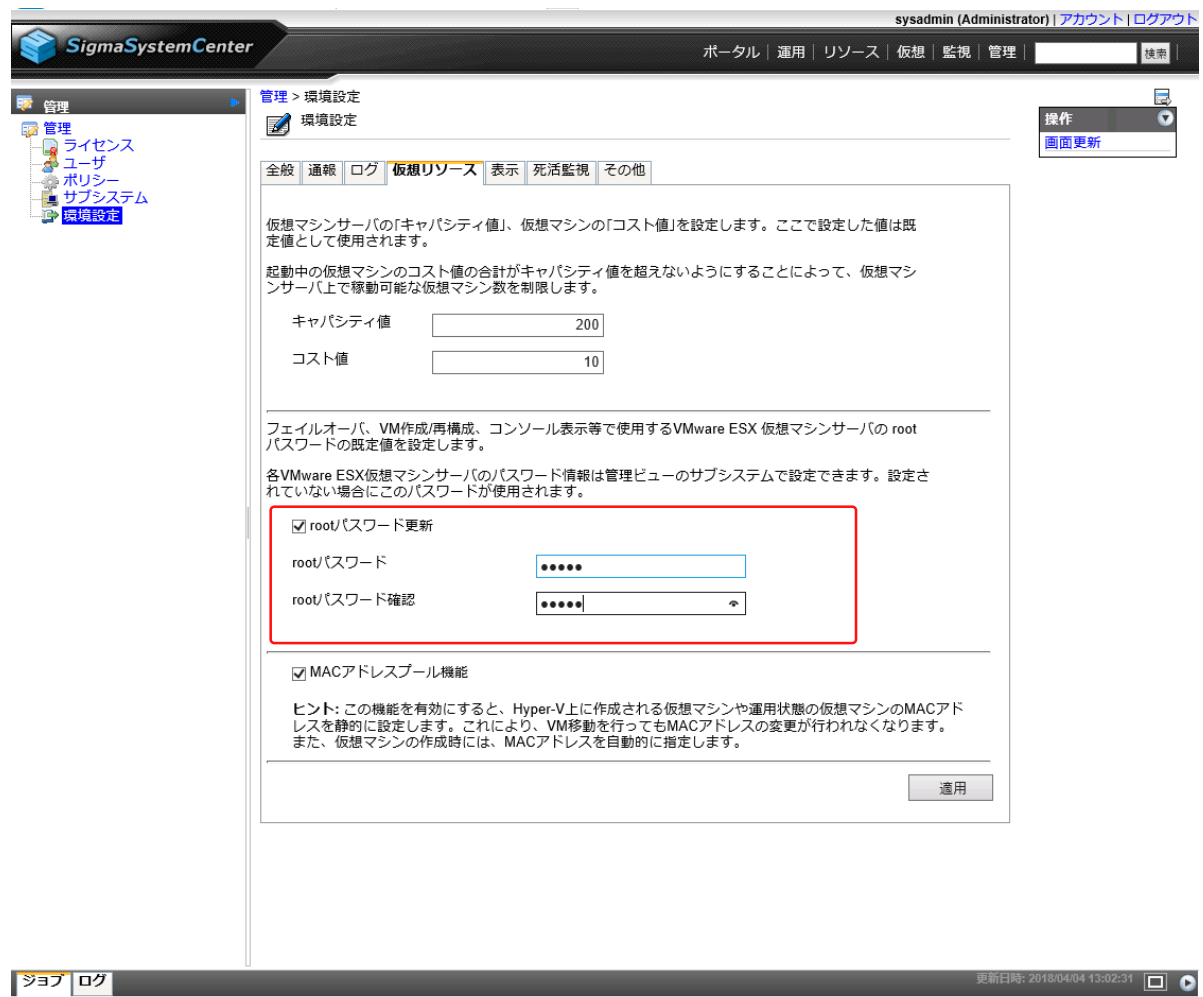


図 ESXi の追加設定

5.2 リソースの登録の確認

前節の「[5.1 サブシステムの登録 \(12 ページ\)](#)」でのサブシステムの登録時、管理対象となるマシンの SSC への登録が自動的に行われます。

登録は、[仮想]ビュー、[リソース]ビュー、[運用]ビューの3つの画面で行われます。各画面を確認していきましょう。

5.2.1 仮想ビュー

まずは、[仮想]ビューの登録について、確認します。

画面右上の[仮想]をクリックして[仮想]ビューを開きます。

左側のツリービューに、vCenter Server(vcenter.vsphere.local)に登録されている物理サーバ([esxi1.vsphere.local]、[esxi2.vsphere.local]、[esxi3.vsphere.local])、業務用仮想マシン([VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06])が、vCenter Server に登録されている構成と同じ構成で登録されていることが確認できます。



図 [仮想]ビュー

5.2.2 リソースビュー

次に、[リソース]ビューの登録について、確認します。

画面右上の[リソース]をクリックして[リソース]ビューを開いた後、ツリービューの[マシン]をクリックして「マシン一覧」画面に移動して、[リソース]ビュー上の登録内容を確認してみましょう。

vCenter Server に登録されている物理サーバ([esxi1.vsphere.local]、[esxi2.vsphere.local]、[esxi3.vsphere.local])、業務用仮想マシン([VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06])が、[マシン一覧]に次のように登録されています。

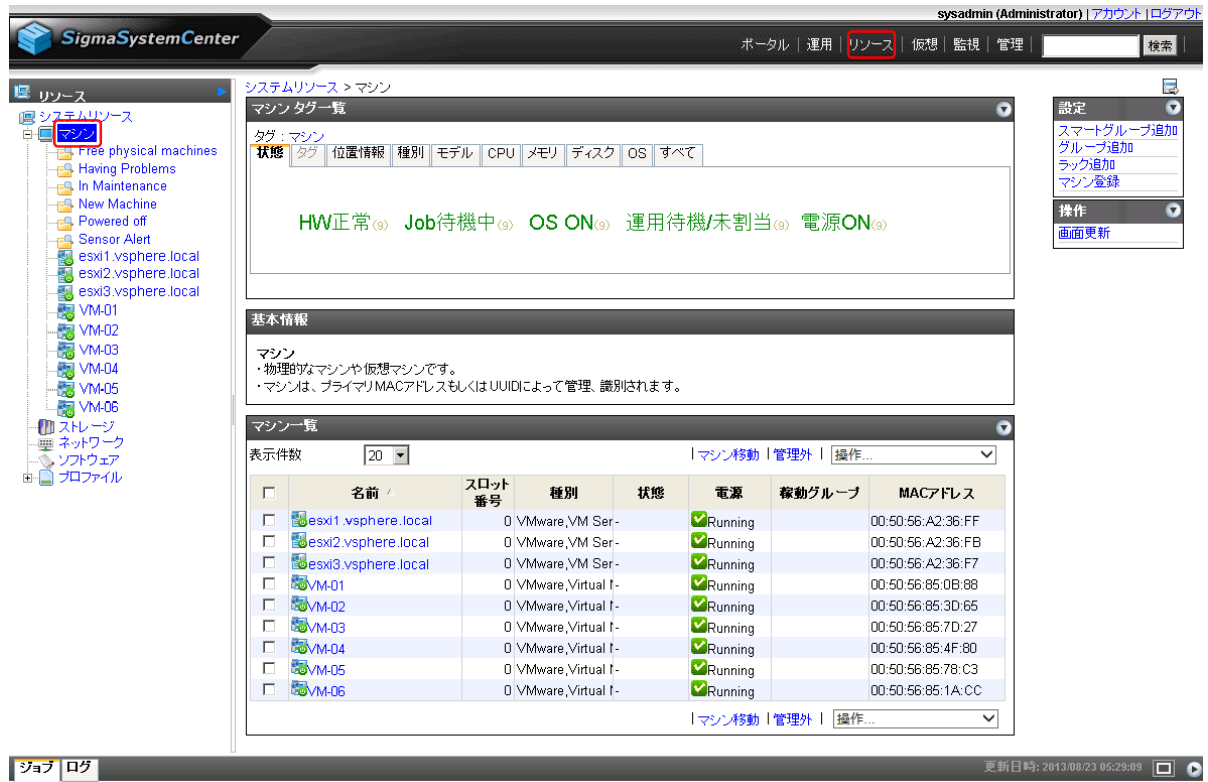


図 サブシステム登録時の「マシン一覧」画面

5.2.3 運用ビュー

次に、画面右上の[運用]をクリックして[運用]ビュー上の登録内容を確認してみましょう。

グループはシステムを構成するサーバの種類ごとに作成されます。後で設定する性能収集や「8. 予兆を含む障害対応機能の設定 (60 ページ)」を利用する場合に設定する障害監視のポリシーや負荷監視は、このグループ単位で設定することになります。

登録や利用内容をまとめると、次の表のとおりです。これらのグループやホストは自動的に作成されます。追加で必要となる設定については、後々説明します。

表 自動作成されるグループ、ホスト

サーバ		詳細		カテゴリ名 ([運用]ビュー)	グループ名 ([運用]ビュー)
ホスト名 ([運用]ビュー)	マシン名 ([リソース]ビュー、 [仮想]ビュー)	サーバの種類	OS		
esxi1	esxi1.vsphere.local	物理 (VM サーバ)	ESXi	vcenter-vsphere-local	Datacenter
esxi2	esxi2.vsphere.local				
esxi3	esxi3.vsphere.local				
VM-01	VM-01	仮想 (VM)	Windows Server	vcenter-vsphere-local	Datacenter_VM
VM-02	VM-02				
VM-03	VM-03				

サーバ		詳細		カテゴリ名 ([運用]ビュー)	グループ名 ([運用]ビュー)
ホスト名 ([運用]ビュー)	マシン名 ([リソース]ビュー、 [仮想]ビュー)	サーバの種類	OS		
VM-04	VM-04				
VM-05	VM-05				
VM-06	VM-06				

ツリービューにある物理サーバ(ESXi)のグループ名（ここでは[Datacenter]）をクリックし、グループの詳細情報画面を開くと、[ホスト一覧]に物理サーバのホスト名の一覧が次のように表示されます。



図 サブシステム登録時の Datacenter グループ(ESXi)の[ホスト一覧]

また、ツリービューにある業務用仮想マシンのグループ名（ここでは[Datacenter_VM]）をクリックし、グループの詳細情報画面を開くと、[ホスト一覧]に業務用仮想マシンのホスト名の一覧が次のように表示されます。



図 サブシステム登録時の[Datacenter_VM]グループ(VM)の[ホスト一覧]

以上でマシン登録の確認は終了です。

5.2.4 増設した物理サーバや新規に作成した仮想マシンの登録について

なお、サブシステムの登録の後に、vCenter Server への物理サーバの登録や業務用仮想マシンの作成を行った場合は、SSC に自動的に登録されませんので注意してください。

この場合は、次のように収集の操作で SSC に登録を行う作業が必要です。

ヒント

収集の操作により、SSC に登録している vCenter Server、物理サーバ、業務用仮想マシンなどの最新の情報や状態を収集し、SSC に反映することができます。

画面右上の[リソース]をクリックして[リソース]ビューを開き、ツリービューの[システムリソース]をクリックして「システムリソース」画面に移動します。

次に[操作]メニュー下の[収集]をクリックします。

収集の処理が完了した後、前述と同様に各ビューの画面に移動して、SSC に登録が反映されているか確認してください。



図 収集の操作

5.3 リソースプールの確認

SSC のリソースプールの画面では、作成可能な仮想マシンの数やシステム内のリソースの空き状況を確認することができます。

リソースプールの設定は、「5.1 サブシステムの登録 (12 ページ)」でサブシステムの登録を行った時に自動で設定されますので、既に関覧できる状態になっています。

さっそく、リソースプールの画面を確認してみましょう。

画面右上の[運用]をクリックして[運用]ビューを開いた後、ツリービューにある ESXi のグループ名（ここでは[Datacenter]）をクリックし、[リソースプール]タブをクリックするとリソースプールの情報が次のように表示されます。

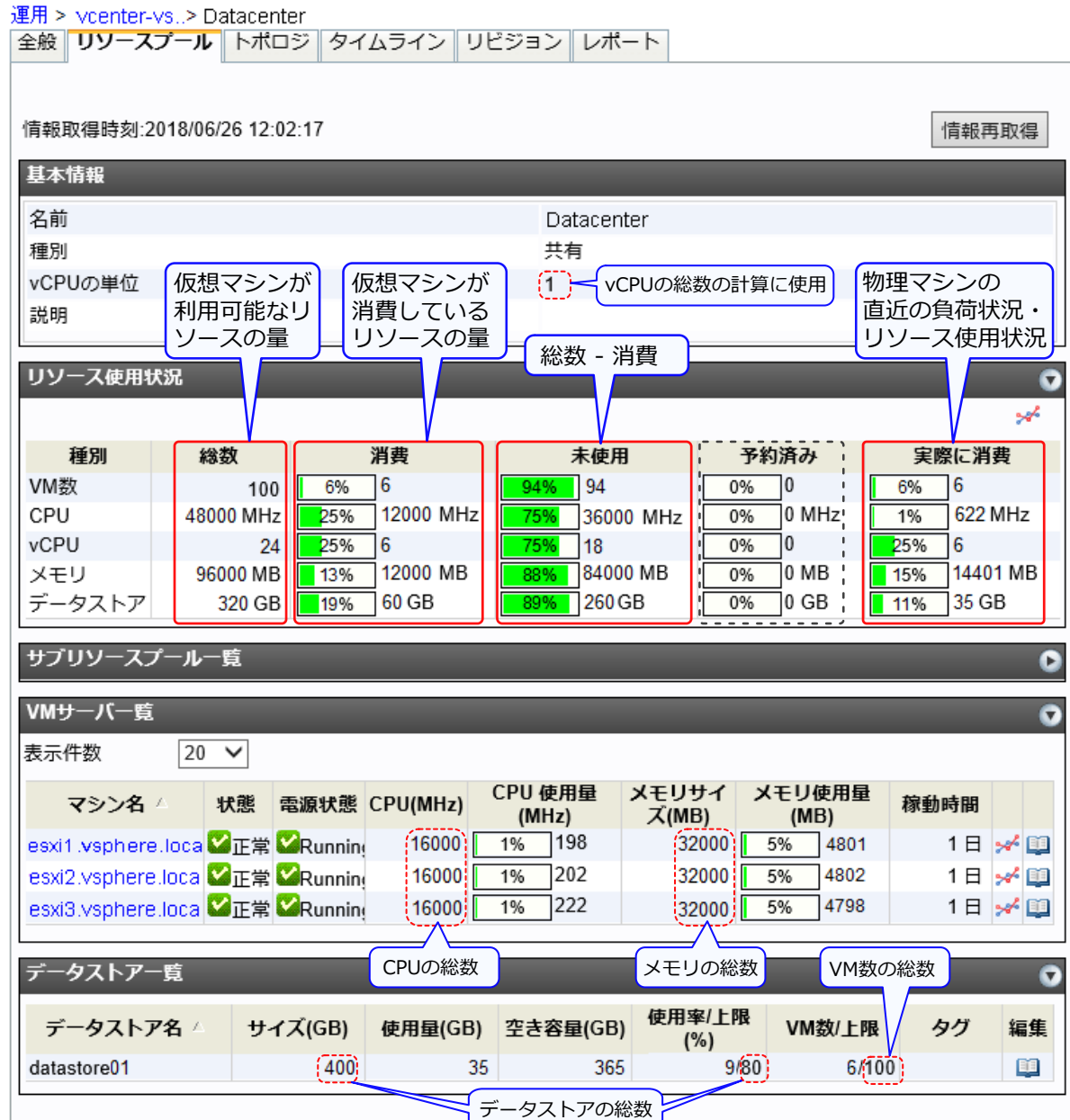


図 リソースプールの画面

上記の[リソース使用状況]の表の[vCPU]の[消費]の情報を見ると、25%と表示されています。既に6台の仮想マシンを作成していますので、この情報より、6台の仮想マシンで25%分のvCPUを消費していることがわかります。

また、[vCPU]の[未使用]の情報を見ると18と表示されていますので、この環境に仮想マシンを追加で作成する場合あと18個分のvCPUを消費できることがわかります。

このように、リソースプールの[リソース使用状況]の表により、リソースプールの全体状況を確認することができます。

仮想マシンの数、CPU、vCPU、メモリ、データストアの各行について、次の情報が表示されます。

- 総数:

仮想マシンが利用可能なリソースの量を表します。リソースプールを構成する物理マシンやデータストアの情報から自動計算されます。

- 消費:

仮想マシンが消費しているリソースの量を表します。仮想マシンに割り当てられているリソースの量から計算されます。

- 未使用:

消費可能なリソースの残量です。総数から消費の値を引いて計算されます。

- 実際に消費:

リソースプールを構成する物理マシンの実際の負荷状況やリソースの使用状況が表示されます。

- 予約済み:

今回の利用では使用しません。テナント運用のため、テナント用に払い出す予定のリソースがカウントされます。

ヒント

現在のリソースの負荷状況や使用状況を確認するには、[実際に消費]の情報を確認してください。

[消費]の情報は、仮想マシンが実際に利用可能な負荷量の上限を表します。

例えば、前述の画面の CPU について、現時点の実際の負荷状況は 622MHz しか使用されておらず使用率は 1%ですが、最大で 12000MHz(使用率は 25%)になる可能性があるということになります。

[リソース使用状況]の表の各行には、リソースの各種別の情報が以下のように表示されます。

リソースの種類別	説明
VM 数	リソースプール上の仮想マシンの数です。 上限値([総数])は、データストアに設定されている[VM 数上限]の値が参照されます。 カスタマイズ方法は「 5.3.2 データストアの設定 (24 ページ) 」を参照してください。
CPU	仮想マシンが消費する CPU の情報を、周波数単位で表示します。 上限値([総数])は、物理サーバの CPU の周波数を合計した値です。
vCPU	仮想マシンが消費する CPU の情報を、vCPU の数の単位で表示します。 上限値([総数])は、物理サーバの CPU コア数×[vCPU の単位]で計算されます。 デフォルトでは、ESXi に搭載される CPU コア 1 つにつき、仮想マシンの 1 個の vCPU として使用する前提で計算されます。 カスタマイズ方法は「 5.3.1 vCPU の単位の設定 (23 ページ) 」を参照してください。
メモリ	仮想マシンが消費するメモリの情報です。 上限値([総数])は、物理サーバのメモリ量を合計した値です。
データストア	仮想マシンが消費するデータストアの情報です。 上限値([総数])は、データストアのサイズ×データストアの[使用率上限]で計算されます。 カスタマイズ方法は「 5.3.2 データストアの設定 (24 ページ) 」を参照してください。

なお、既定値のままでもリソースプールを使用できるようになっていますが、一部の種別の[総数]について、以下のカスタマイズをすることができます。カスタマイズの設定の必要がない場合は、「5.5 手動での仮想マシンの移動(Migration(vMotion)) (26 ページ)」に進んでください。

- vCPU の単位の設定

ESXi に搭載される CPU コア 1 つにつき、仮想マシンの何個の vCPU として使用するかを設定します。

- データストアの設定(使用率上限、VM 数上限)

データストアの使用率上限、また、データストアから作成する VM 数上限を設定します。

以下、各項目について説明します。

5.3.1 vCPU の単位の設定

[リソースプール]タブの画面で、画面右上の[設定]メニュー下の[編集]をクリックし、「リソースプール編集」画面を表示します。

デフォルトでは、ESXi に搭載される CPU1 コアを 1 台の仮想マシン(1vCPU)で利用する設定となっています。CPU1 コアを複数台の仮想マシンに分割して割り当てる利用を行っている場合は、設定変更してください。

設定を変更すると[vCPU]の総数の値に反映されます。

The screenshot shows the 'Resource Pool Edit' dialog box. The 'Name' field contains 'Datacenter'. The 'Type' is set to '共有' (Shared). The 'vCPUの単位' (vCPU Unit) is set to '1コアあたりのvCPU数' (1 core per vCPU number), and the value '1' is entered in the adjacent text box. The '周波数' (Frequency) is set to 'MHz'. The '説明' (Description) field is empty. The '割り当て先' (Priority) is set to '設定なし' (Not set). The 'OK' and 'キャンセル' (Cancel) buttons are at the bottom right.

図 「リソースプール編集」画面

5.3.2 データストアの設定

[リソースプール]タブの画面で、[データストア一覧]のデータストアの行の右端にある[編集]アイコンをクリックし、「データストア編集」画面を表示します。

- [使用率上限]

仮想マシンの仮想ディスクとして使用するデータ量の上限を、データストアの使用率で設定します。データストアの容量に本設定値を掛け合わせた値が、リソースプールの[データストア]の[総数]の値として反映されます。

デフォルトは 80% です。

- [VM 数上限]

設定中のデータストアから作成する仮想マシンの数の上限を設定します。

仮想マシンで実行する業務の IO 負荷が高い場合、本設定により同じデータストア上で動作する仮想マシンを作り過ぎないように制限した値を設定することができます。

設定を変更するとリソースプールの[VM 数]の総数の値に反映されます。

デフォルトは 100 です。

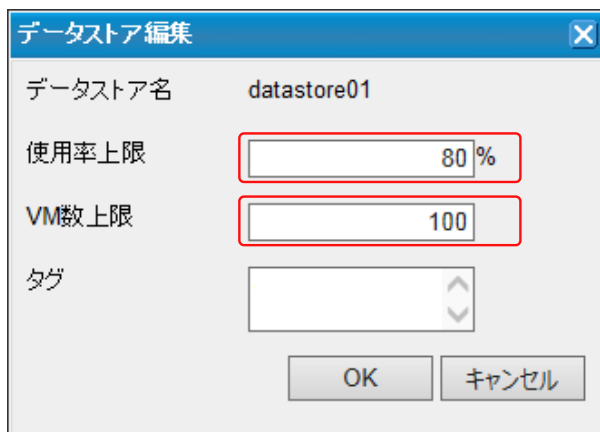


図 「データストア編集」画面

5.4 負荷状況の確認

サブシステム登録を行うと負荷状況取得設定が自動で行われます。管理対象マシン（ESXi、仮想マシン）の負荷状況を SSC の Web コンソール上で確認してみましょう。

負荷状況取得の設定のカスタマイズが必要な場合は、「[付録 B. 負荷状況取得の設定（94 ページ）](#)」を参照してください。

注

負荷状況取得設定が有効化されるには、「[5.1 サブシステムの登録（12 ページ）](#)」の設定を行ってから、デフォルトで最大 10 分程度必要となります。

まずは、物理サーバの負荷状況を確認します。

SSC の Web コンソールで負荷状況を確認するには、[運用]ビュー(画面右上の[運用])をクリック)を利用します。[運用]ビューを開いたら、ツリービューから設定対象の運用グループである[Datacenter]をクリックします。負荷状況を確認したい物理サーバを[ホスト一覧]から確認し、グラフ表示のアイコンをクリックします。



図 ホスト一覧

また、近々の負荷状況を確認するために「グラフ設定」画面で[期間]を以下のように入力します。

- 表示期間：1 時間

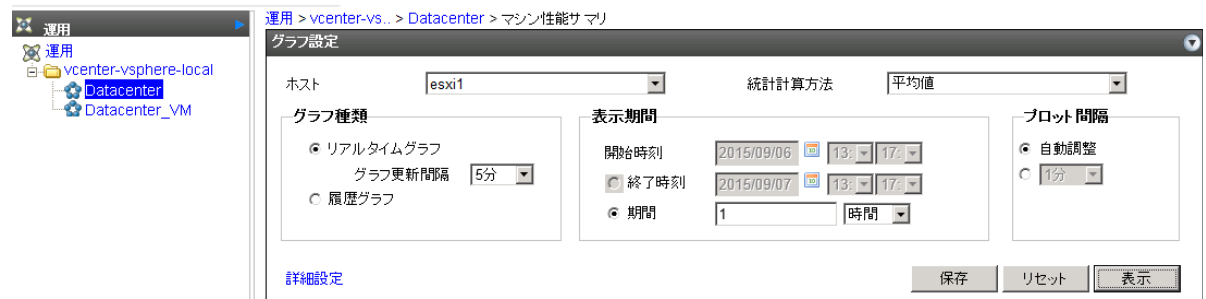


図 グラフ設定

[表示]をクリックすると、以下のように負荷状況がグラフ表示されます。[保存]をクリックすると、そのホストごとのグラフ設定を保存することもできます。

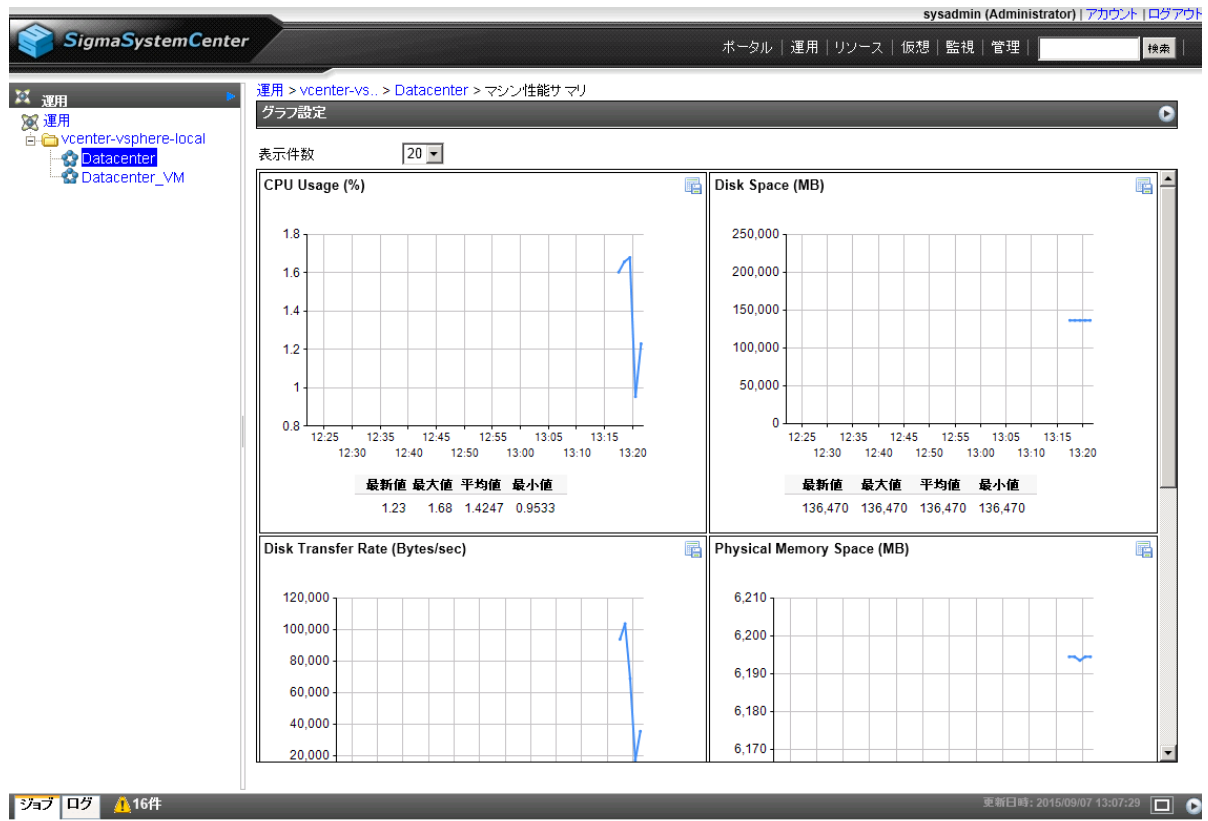


図 負荷状況

業務用仮想マシンの負荷状況についても、同様の手順で負荷状況を確認できます。

5.5 手動での仮想マシンの移動(Migration(vMotion))

以上の作業により、SSC の基本的な設定は完了です。

現在の段階でも、手動で様々な操作が SSC 上から行えます。テストを兼ねて手動での「Migration」(VMware の用語では「vMotion」)を行ってみることにしましょう。「Migration」は、仮想マシンを稼動させたままの状態での物理サーバ間の移動を行うことを指します。

注

SSC で障害時の自律運用を実現するには、「[8. 予兆を含む障害対応機能の設定 \(60 ページ\)](#)」の作業が必要です。

SSC では、仮想マシンの状態確認や手動での制御は[仮想]ビューから行います(画面右上の[仮想]をクリック)。ツリービューを確認すると、物理サーバ[esxi1.vsphere.local]上で仮想マシン([VM-01]、[VM-02])が動作しており、物理サーバ[esxi2.vsphere.local]上で仮想マシン([VM-03]、[VM-04])が動作していることが分かります。

ここでは[VM-02]を[esxi1.vsphere.local]から[esxi2.vsphere.local]に移動してみます。ちなみに仮想マシンの制御は[運用]ビューから行うこともできますが、[仮想]ビューのほうが仮想マシンの配置状況が把握しやすいのでオペレーションミスの発生を防ぎやすいでしょう。



図 [仮想]ビュー

仮想マシンを移動させるには、まずツリービュー上で当該仮想マシンが使用している物理サーバ[esxi1.vsphere.local]をクリックして選択します。次に、表示された画面を中ほどまでスクロールすると[稼動中 VM 一覧]という枠がありますので、移動させる仮想マシン[VM-02]をチェックして、右上のアクションメニューの[VM 移動]をクリックしてください。



図 移動する仮想マシンの選択

[VM 移動]をクリックすると、移動先の物理サーバと移動方法を選択する「VM 移動」画面が表示されます。[移動先データセンタ名]ではドロップダウンリストから移動先となる[esxi2.vsphere.local]が vCenter 上で属しているデータセンタを選択します。次に、移動先の[esxi2.vsphere.local]のラジオボタンをチェックします。

移動方法としては、以下の3つが用意されています。

- Migration :

稼動状態を保持したまま仮想マシンを移動します。VMware の vMotion を利用します。

[サスペンド後に移動(Quick Migration)]をチェックした場合は、移動する仮想マシンをサスペンドしてから移動を行い、移動後に仮想マシンをレジュームします。

- Storage Migration :

稼動状態を保持したまま仮想マシンと仮想ストレージを移動します。VMware の Storage vMotion を利用するため、適切な VMware のライセンスを用意してください。

[停止後に移動(Move)]をチェックした場合は、移動する仮想マシンを停止してから仮想マシンと仮想ストレージを移動します。この場合、VMware の Storage vMotion は利用しません。移動後に仮想マシンを起動したい場合には、[VM 移動後の状態]の枠の[自動起動]をチェックします。

- Failover :

仮想マシンを障害が発生した物理サーバから正常稼働中の物理サーバに移動します。仮想マシンの稼働状態は保持されず、コールドブートします(再起動したイメージになります)。

これらの移動方法のうち、Storage Migration を除いては、移動元の ESXi と移動先の ESXi で共有するストレージが必要になります。Storage Migration のみ、ローカルディスクなど共有していないストレージでも移動が可能です。

今回は、共有ストレージを利用できますので、仮想マシンを稼働させたまま移動する [Migration] をチェックします。

移動先と移動方法を選択したら [OK] をクリックします。

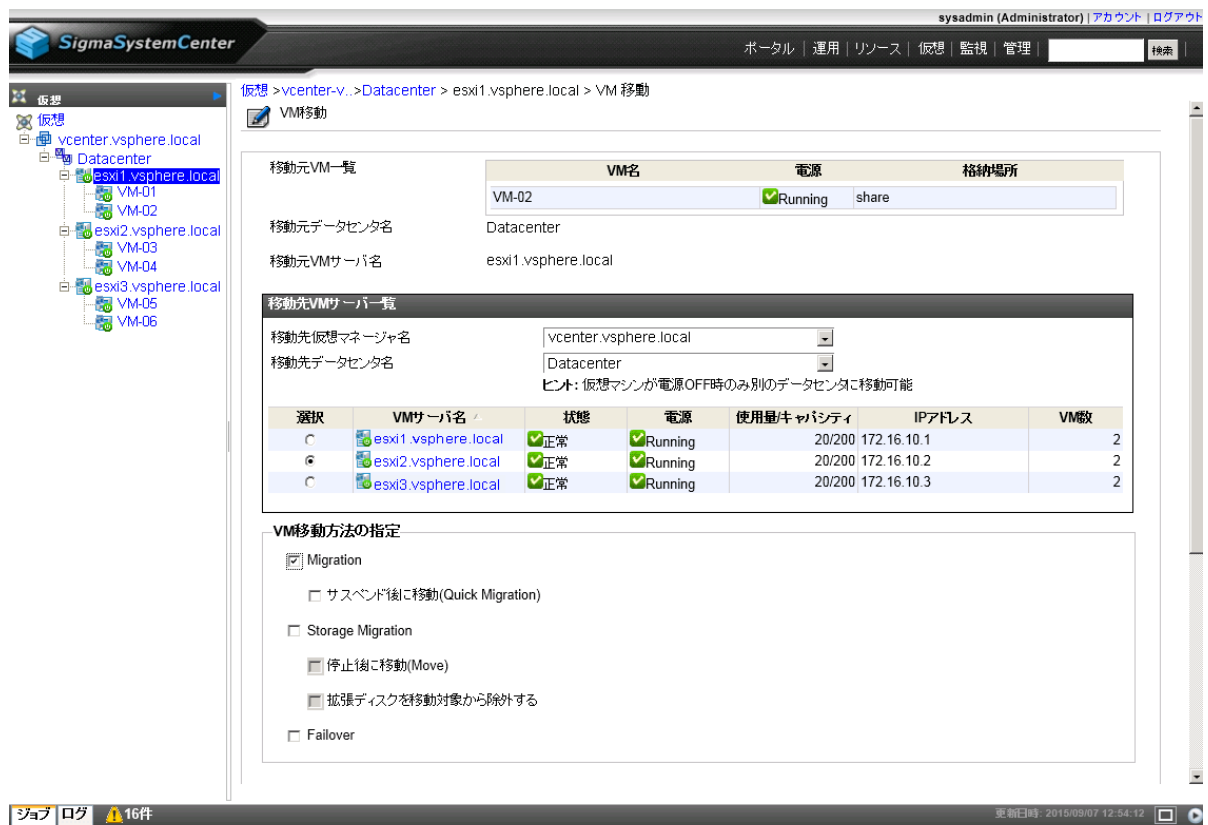


図 移動先と移動方法の選択

下記の画面は、仮想マシンを移動させたあとの[仮想]ビューです。ツリービューを見ると、[VM-02]が[esxi2.vsphere.local]に移動していることが分かります。なお、仮想マシンの移動がツリービューに反映されていない場合は[操作]メニューの[画面更新]をクリックしてみてください。

基本情報

マシン名	esxi1.vsphere.local
リソースパス	resource:/esxi1.vsphere.local
UUID	4222F6F5-90E9-E213-BF1D-9BEF0057C341
キャパシティ値	200
使用量	10
マネージャURL	vcenter.vsphere.local
製品名	VMware ESXi
バージョン	6.5.0
CPU種別	Intel(R) Xeon(R) CPU X5550 @ 2.0 GHz
プロセッサ	8 (4 Socket) x 2.0 GHz
メモリサイズ	32000MB
説明	

運用情報

ホスト名	esxi1
稼働グループ	operations:/vcenter.vsphere.local/Datacenter
サマリステータス	正常
電源状態	On
接続状態	接続可能
稼働ステータス	On
OSステータス	On
ハードウェアステータス	正常 (状態詳細)
実行ステータス	-
ポリシー状態	全て有効
メンテナンスステータス	Off
管理状態	管理中

稼働中VM一覧

VM名	コスト	状態	電源	IPアドレス	MACアドレス
VM-01	10	正常	Running	172.20.100.1	00:50:56:85:0B:88

未使用VM一覧

VM名	コスト	状態	電源	MACアドレス	管理状態
-----	-----	----	----	---------	------

図 仮想マシン移動後の[仮想]ビュー

6. レポート機能の利用（負荷状況取得の設定）

本章では、管理対象マシンのレポート表示を行うために最低限必要な設定の方法、および、レポート表示の利用方法について説明します。

6.1 レポートの作成

以上の設定でレポートの作成ができるようになりましたので、早速、レポートの作成を行ってみましょう。

レポートの作成は、レポート対象となるグループや特定のマシンを選択して行います。

以下のレポートを作成することができます。

- リソースプール(ESXi グループ)

リソースプールとして、ESXi 全体のリソース状況やグループ内の ESXi や業務用仮想マシンのリソースのレポートが閲覧できます。

- 業務用仮想マシン個別

個別の業務用仮想マシンの負荷状況のレポートが閲覧できます。

他にも種類がありますが、ここでは割愛します。詳細は、[SigmaSystemCenter 3.8 リファレンスガイドの 7.2.1. 作成可能なレポートの種類](#)を参照してください。

6.1.1 リソースプール(ESXi グループ)のレポート作成

まず、リソースプールの前月の月次レポートを作成してみましょう。リソースプールのレポートは、ESXi のグループのレポートを作成することで作成できます。

Web コンソール、ssc コマンドでの作成方法について、それぞれ説明します。

- 「(1)Web コンソールでの作成 (31 ページ)」
- 「(2)ssc コマンドでの作成 (33 ページ)」

(1)Web コンソールでの作成

レポートの作成は、[運用]ビュー（画面右上の[運用]をクリック）で行います。[運用]ビューを開いたら、ツリービューから対象のグループである[Datacenter]をクリックして、[レポート]タブをクリックします。

「レポートファイル」画面が表示されますので、[レポート作成]をクリックします。



図 「レポート作成」画面 その1

「レポート作成」画面で、以下のように期間を指定し、レポート作成を行います。(例：2018年5月の月次レポートを作成する場合)

- [期間]の単位として[ヵ月間]を選択する。
 - "1"を入力する。
- [開始時刻]のチェックを有効にする。
 - 開始時刻: 2018/05/01 00:00:00

[OK]をクリックすると、レポートファイル作成のジョブの実行が開始します。

運用 > vcenter-vs.. > Datacenter

全般 リソースプール トポロジ タイムライン リビジョン **レポート**

レポート作成

期間 ヶ月間 ▼

☒ 開始時刻

☐ 終了時刻

ヒント：開始時刻から終了時刻までのレポートを作成します。

オプション OK キャンセル

図 「レポート作成」画面 その2

レポートファイル作成のジョブ完了後、画面右下の[操作]メニュー下の[画面更新]をクリックすると、レポートファイルの一覧に新規に作成されたレポートファイルの情報が表示されます。

ファイル名のリンクをクリックすると、ダウンロードすることができます。

ダウンロードしたレポートファイルの内容については、後述の「6.2 レポートの閲覧（37ページ）」で説明します。

運用 > vcenter-vs.. > Datacenter

全般 リソースプール トポロジ タイムライン リビジョン **レポート**

レポート作成

レポートファイル

表示件数 | 削除 |

<input type="checkbox"/>	ファイル名	対象	期間	作成日時	サイズ
<input type="checkbox"/>	Datacenter_20180622_172854.xls	Datacenter	2018/05/01 00:00 - 2018/06/01 00:00	2018/06/22	163KB

| 削除 |

設定

- グループ編集
- グループ移動
- グループ削除
- リソースプール
 - 編集
 - 切り出し
 - 削除
- プロパティ
 - 設定一覧
- 性能サマリ
- 性能状況
- 保守操作を表示
- 権限設定

操作

- スケールアウト
- スケールイン
- プールに追加
- 全てのマシンの操作
 - 起動
 - 再起動
 - シャットダウン
 - ソフトウェア再配布
- 画面更新

図 レポート作成後の「レポート作成」画面

(2)ssc コマンドでの作成

次にコマンドでレポート作成を行ってみましょう。

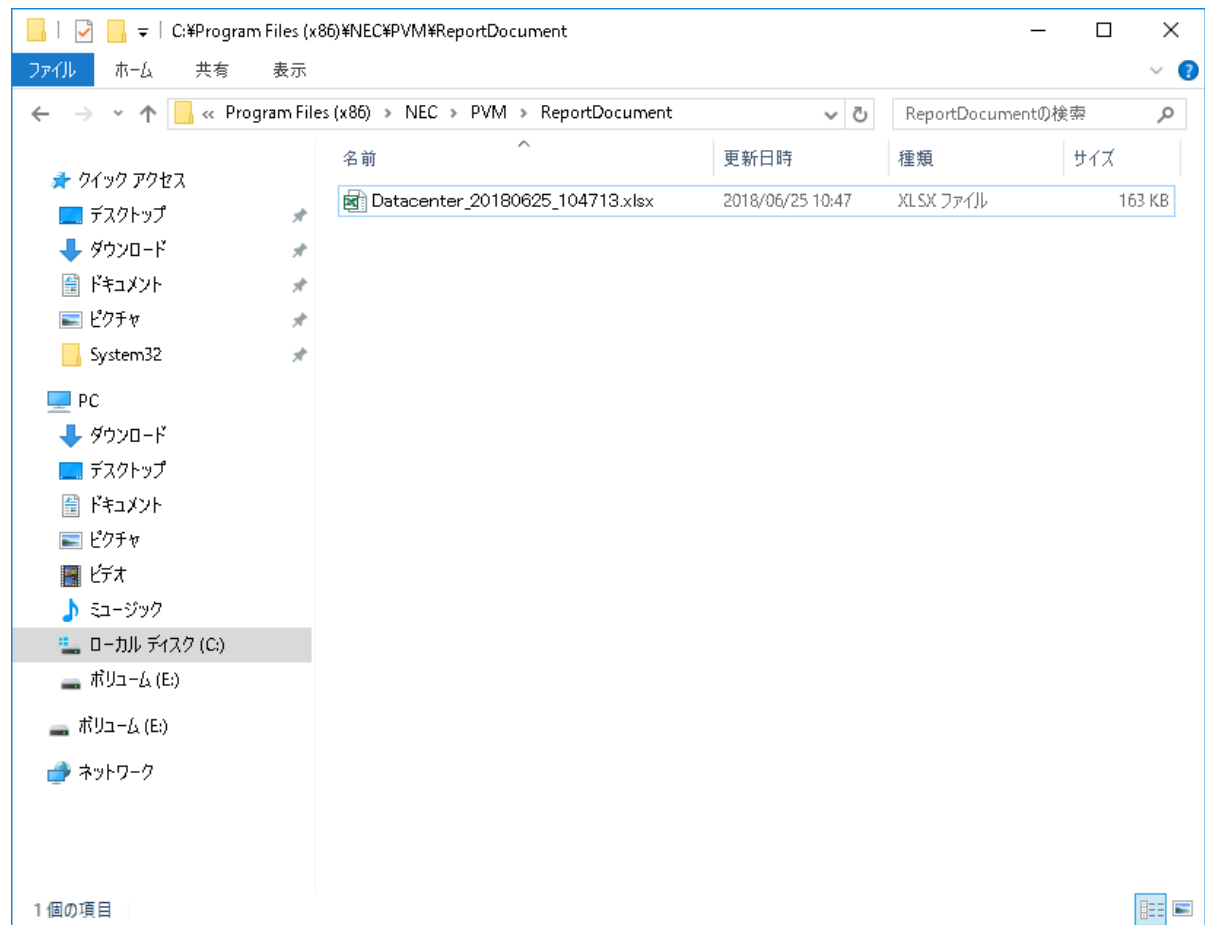
ssc コマンドでの作成も、Web コンソールと同様に、レポート対象のグループまたはホストを指定して、レポートの期間を指定することで作成できます。

SSC 管理サーバ上でコマンドプロンプトを開いて、次のコマンドを実行します。

```
>ssc create report 172-16-0-2/新規データセンター -start 2018/05/01 -end 2018/06/01
```

レポートファイルは、次のように、<SSC のインストール先フォルダ>%ReportDocument 下に作成されます。

作成したファイルの見方については、後述の「6.2 レポートの閲覧（37 ページ）」で説明します。



以上で、ESXi グループ([Datacenter]グループ)の前月の月次レポート作成の作業は完了です。

6.1.2 個別の仮想マシンのレポート作成

次に、仮想マシン VM-01 の前月の月次レポートを作成してみましょう。

Web コンソール、ssc コマンドでの作成方法について、それぞれ説明します。

- 「(1)Web コンソールでの作成（35 ページ）」
- 「(2)ssc コマンドでの作成（36 ページ）」

(1) Web コンソールでの作成

レポートの作成は、[運用]ビュー（画面右上の[運用]をクリック）で行います。[運用]ビューを開いたら、ツリービューから対象の仮想マシンのグループ[Datacenter_VM]をクリックします。

次にホスト一覧から[VM-01]をクリックして、[レポート]タブをクリックします。

「レポートファイル」画面が表示されますので、[レポート作成]をクリックします。



図 「レポート作成」画面 その1

「レポート作成」画面で、以下のように期間を指定し、レポート作成を行います。(例：2018年5月の月次レポートを作成する場合)

- [期間]
 - "1"を入力する。
 - 単位として[ヵ月間]を選択する。
- [開始時刻]のチェックを有効にする。
 - 開始時刻: 2018/05/01 00:00:00

[OK]をクリックすると、レポートファイル作成のジョブの実行が開始します。

運用 > vcenter-vs... > Datacenter_VM > VM-01

全般 リビジョン レポート

レポート作成

期間 ケ月間

☒ 開始時刻 2018/05/01 00:00

☐ 終了時刻 2019/07/03 15:38

ヒント: 開始時刻から終了時刻までのレポートを作成します。

オプション OK キャンセル

図 「レポート作成」画面 その2

レポートファイル作成のジョブ完了後、画面右下の[操作]メニュー下の[画面更新]をクリックすると、レポートファイルの一覧に新規に作成されたレポートファイルの情報が表示されます。

ファイル名のリンクをクリックすると、ダウンロードすることができます。

ダウンロードしたレポートファイルの内容については、後述の「6.2 レポートの閲覧 (37 ページ)」で説明します。

運用 > vcenter-vs... > Datacenter_VM > VM-01

全般 リビジョン レポート

レポート作成

レポートファイル

表示件数 20

ファイル名	対象	期間	作成日時	サイズ
VM-01_20180625_150527.xlsx	VM-01	2018/05/01 00:00 - 2018/06/01	2018/06/25	101KB

削除

設定

- プロパティ
- マシン性能サマリ
- 性能情報比較

操作

- 起動
- 再起動
- シャットダウン
- ソフトウェア配布
- ジョブ実行結果のリセット
- 故障状態の解除
- メンテナンス
- 画面更新

図 レポート作成後の「レポート作成」画面

(2)ssc コマンドでの作成

次にコマンドでレポート作成を行ってみましょう。

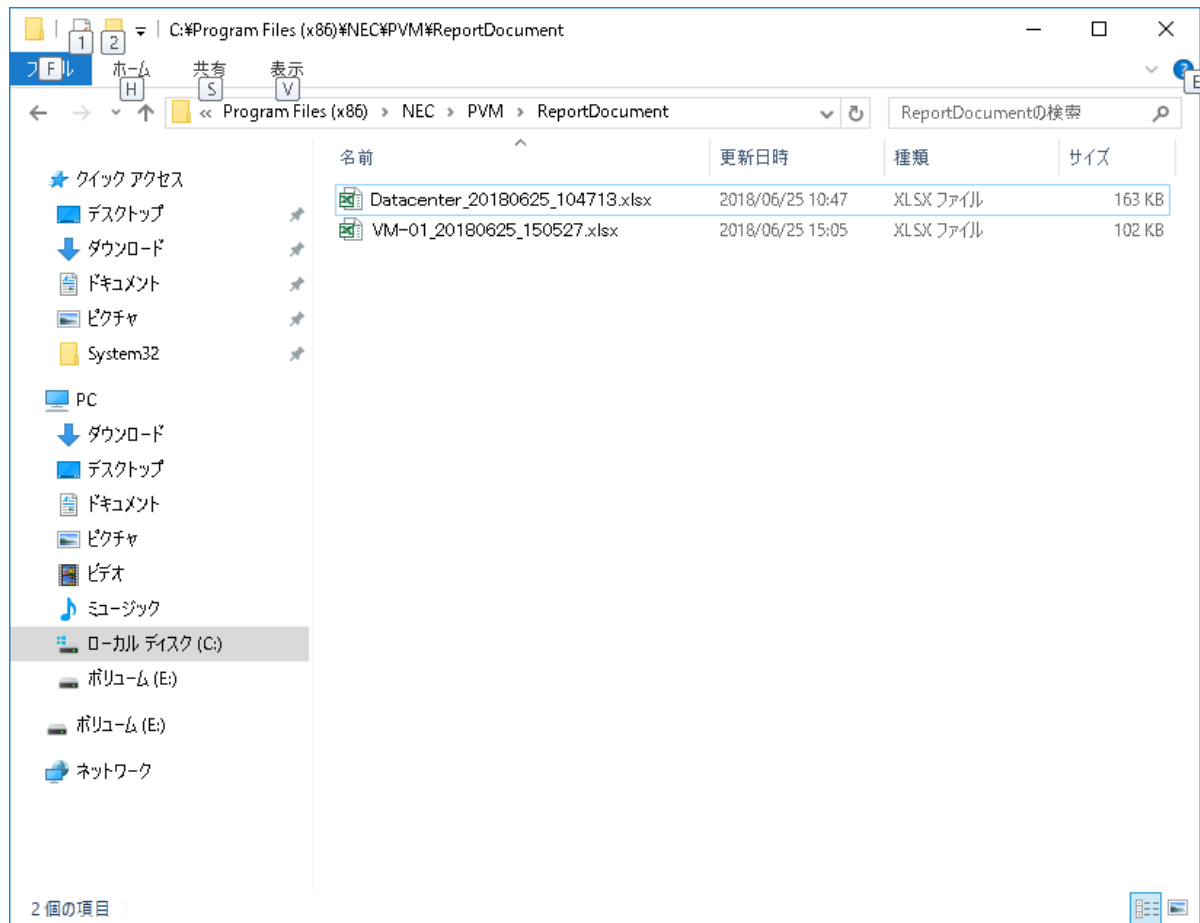
ssc コマンドでの作成も、Web コンソールと同様に、レポート対象のグループまたはホストを指定して、レポートの期間を指定することで作成できます。

SSC 管理サーバ上でコマンドプロンプトを開いて、次のコマンドを実行します。

```
>ssc create report 172-16-0-2/新規データセンター_VM/VM-01 -start 2018/05/01 -end 2018/06/01
```

レポートファイルは、次のように、<SSC のインストール先フォルダ>\ReportDocument 下に作成されます。

作成したファイルの見方については、後述の「[6.2 レポートの閲覧（37 ページ）](#)」で説明します。



以上で、仮想マシン[VM-01]の前月の月次レポート作成の作業は完了です。

6.2 レポートの閲覧

本節では、作成したレポートを Excel で閲覧してみましょう。

レポートには様々な情報が出力されますが、以下について、確認してみます。

- ・「[6.2.1 リソースプール概要のレポート（38 ページ）](#)」

「[6.1.1 リソースプール\(ESXi グループ\)のレポート作成（31 ページ）](#)」で作成したレポートより、リソースプール概要を閲覧します。

- 「6.2.2 業務用仮想マシンの負荷履歴レポート（39 ページ）」

「6.1.2 個別の仮想マシンのレポート作成（34 ページ）」で作成したレポートより、業務用仮想マシンの先月の負荷状況を閲覧します。

作成されたレポートは、その他の情報も閲覧することができます。レポートの各シートの内容については、[SigmaSystemCenter 3.8 リファレンスガイド 7.2.2. 作成可能なレポートの内容](#)の(1)仮想マシンサーバグループ、(5)仮想マシンを参照してください。

6.2.1 リソースプール概要のレポート

「6.1.1 リソースプール(ESXi グループ)のレポート作成（31 ページ）」で作成したファイルを Excel で開いて、[リソースプール概要]シートをクリックすると次の図のようなレポートが表示されます。

リソースプール概要のレポートでは、「5.3 リソースプールの確認（20 ページ）」で Web コンソール上で確認したリソースプールの情報と同じ内容を、レポートとして閲覧することができます。

その他、リソースプールを構成する ESXi の前月の負荷履歴や障害履歴などのレポートを見ることができます。以下の製品サイトのページからレポートのサンプルをダウンロードして確認してください。

- <https://jpn.nec.com/websam/sigmasystemcenter/kinoulist.html?#report>

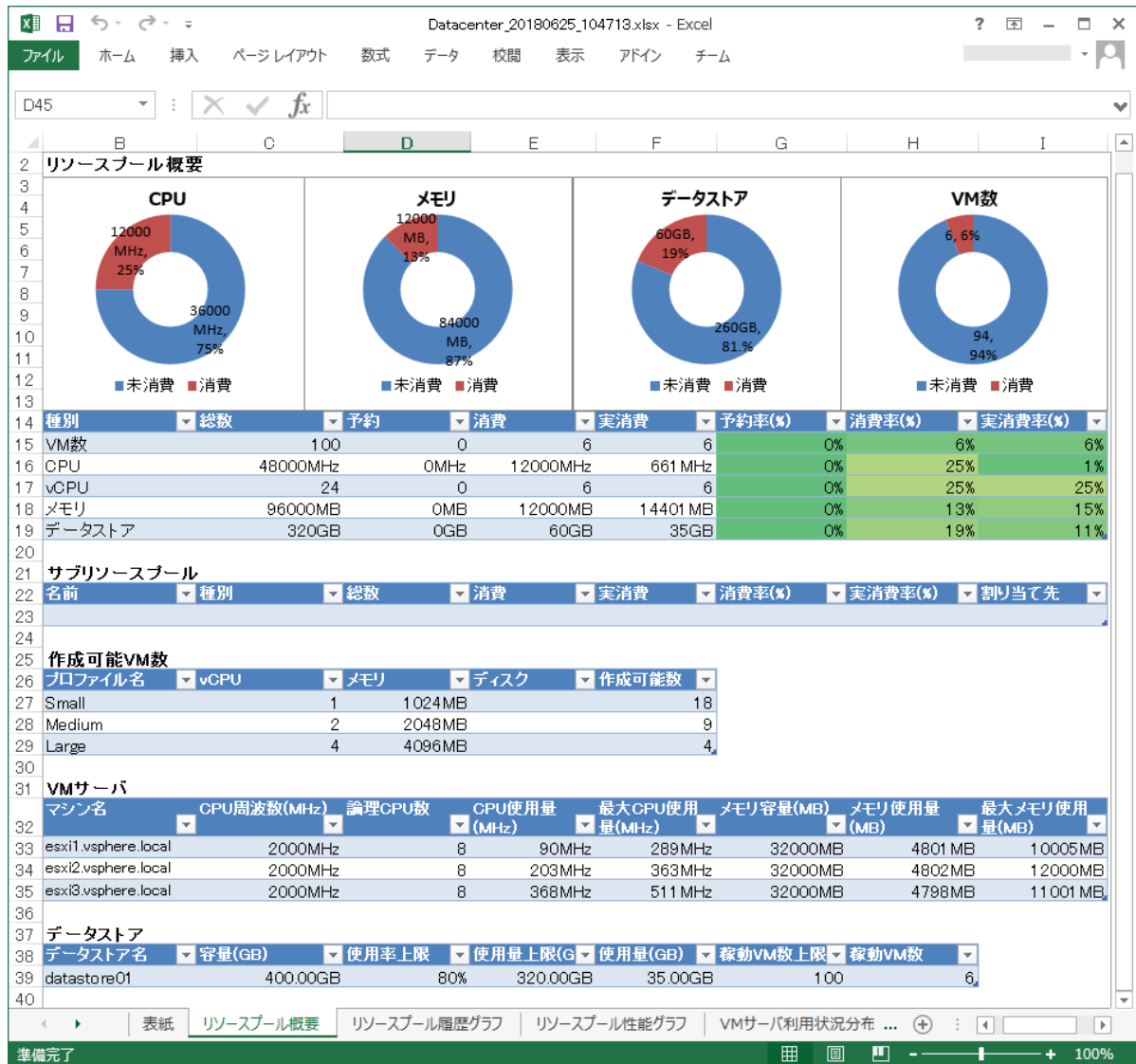


図 「リソースプール概要」のレポート表示画面

6.2.2 業務用仮想マシンの負荷履歴レポート

「6.1.2 個別の仮想マシンのレポート作成（34 ページ）」で作成したファイルを Excel で開いて、[性能グラフ]シートをクリックすると次の図のようなレポートが表示されます。

業務用仮想マシンの負荷履歴レポートでは、前月の一か月間の仮想マシンの CPU やメモリなどの負荷履歴を閲覧できます。

標準では、以下の項目の履歴がレポートに出力されます。

- CPU (MHz)
- メモリ (MB)
- ネットワーク (MBps)
- ディスク Read (IOPS)

- ディスク Write (IOPS)

上記以外にも SSC で取得できる性能情報なら、レポートのテンプレートをカスタマイズすることでレポートの表示に加えることができますので、必要な場合は製品の窓口にお問い合わせください。

負荷履歴以外のその他のレポートについては、以下の製品サイトのページからレポートのサンプルをダウンロードして確認してください。

- <https://jpn.nec.com/websam/sigmatasystemcenter/kinoulist.html?#report>

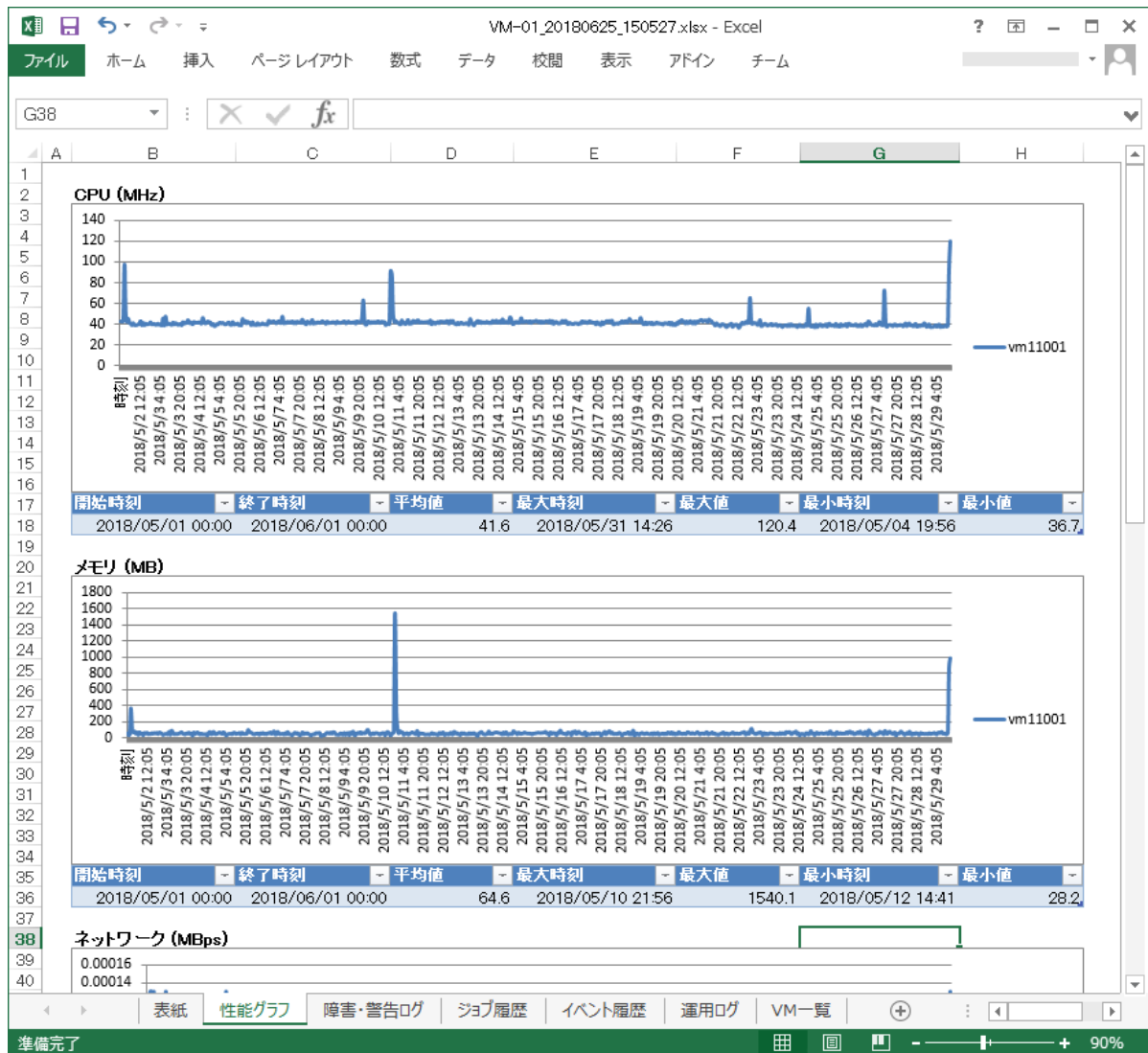


図 「性能グラフ」のレポート表示画面

7. 電源操作の設定

ここまでの作業で、管理対象リソースを SSC に登録することができました。

次に、物理サーバである[esxi1.vsphere.local]、[esxi2.vsphere.local]、[esxi3.vsphere.local]の起動操作、強制 OFF 操作、センサ情報の取得を可能にするための設定を行います。

現時点でも、物理サーバのシャットダウン操作や仮想マシンの電源操作全般が実行可能ですが、本章の設定により、一通りの電源操作が可能となります。

また、SSC では、個々の電源操作に加えて、以下の付加機能を利用することができます。ここでは、設定後に動作テストとして、下記の一括電源操作で電源操作が利用可能になっているかを確認してみましょう。

- 管理対象全体の一括電源操作
- 複数同時操作時における電源操作順の優先度や依存関係の指定

7.1 物理サーバの設定

物理サーバである[esxi1.vsphere.local]、[esxi2.vsphere.local]、[esxi3.vsphere.local]の起動操作、強制 OFF 操作、センサ情報の取得を可能にするための設定を行います。

SSC が「Out-of-Band (OOB) Management を利用するための設定」として、物理サーバの BMC または iLO にリモートログインするための以下の設定を行います。

1. 管理対象の物理サーバの BMC の設定を行う。

※機種別に設定方法が異なります。

- Express5800/R120h などに搭載される iLO については、「[7.1.1 iLO \(BMC\) の設定 \(41 ページ\)](#)」を参照。
- Express5800/D120h などに搭載される BMC については、「[7.1.2 Express5800/D120h などの BMC/CMC の設定 \(45 ページ\)](#)」を参照。

2. SSC 上で、管理対象の OOB アカウント設定を行う。

「[7.1.3 SSC での OOB のアカウント設定 \(50 ページ\)](#)」を参照。

7.1.1 iLO (BMC) の設定

◇管理 LAN の設定

まず、物理サーバ[esxi1.vsphere.local]の iLO (BMC) の管理 LAN の設定を行います。
[esxi1.vsphere.local]の iLO の IP アドレスは"172.16.20.1"を設定します(「[1.3 システム構成と使用機材 \(2 ページ\)](#)」参照)。手順については、「iLO 5 ユーザーズガイド」の「2. iLO セットアップ」を参照して、管理 LAN を設定してください。

NEC システム構成

システムユーティリティ > システム構成 > BMC構成ユーティリティ > ネットワークオプション

NEC Express5800/R120h-2M
 Server SN: SerialNum.0AC
 iLO IPv4: 172.16.20.1
 iLO IPv6: FE80::9640:C9FF:FE1E:06B8
 User Default: OFF

ネットワークオプション

MACアドレス: 94:40:C9:1E:06:B8

ネットワークインターフェイス: オン

送信速度自動選択: オン

VLAN有効: オフ

DHCP有効: オフ

DNS名: BMCSerialNum-0A

IPアドレス: 172.16.20.1

サブネットマスク: 255.240.0.0

ゲートウェイIPアドレス: 172.16.0.1

Enter: 選択
 ESC: 終了
 F1: ヘルプ
 F7: デフォルトをロード
 F10: 保存
 F12: 保存して終了

終了 変更保留中 再起動が必要 F7: デフォルト F10: 保存 F12: 保存して終了

図 iLO 5 の管理 LAN の設定

◇ローカルユーザアカウントの作成

次に、[esxil.vsphere.local]の iLO（BMC）で管理者権限のあるユーザを作成します。手順については、「iLO 5 ユーザーズガイド」の「2. iLO セットアップ」を参照して、ローカルユーザアカウントを作成してください。

ここでは、仮に[ユーザ名]を"ssc"、[パスワード]を"sscadmin"に設定したとします。

NEC システム構成

More Forms > BMC構成ユーティリティ > ユーザー管理 > ユーザーの追加

NEC Express5800/R120h-2M
Server SN: SerialNum.0AC
iLO IPv4: 172.16.20.1
iLO IPv6: FE80::9640:C9FF:FE1E:06B8
User Default: OFF

Enter: 選択
ESC: 終了
F1: ヘルプ
F7: デフォルトをロード
F10: 保存
F12: 保存して終了

ユーザーの追加

新しいユーザーのBMCの権限:

ユーザーアカウント管理	はい
リモートコンソールアクセス	はい
仮想電源およびリセット	はい
仮想メディア	はい
設定の構成	はい
ホストBIOS	はい
ホストNIC	はい
ホストストレージ	はい

新しいユーザー情報:

新しいユーザー名:

ログイン名:

☒ 変更保留中
☐ 再起動が必要

NEC システム構成

More Forms > BMC構成ユーティリティ > ユーザー管理 > ユーザーの追加

NEC Express5800/R120h-2M
Server SN: SerialNum.0AC
iLO IPv4: 172.16.20.1
iLO IPv6: FE80::9640:C9FF:FE1E:06B8
User Default: OFF

Enter: 選択
ESC: 終了
F1: ヘルプ
F7: デフォルトをロード
F10: 保存
F12: 保存して終了

ユーザーの追加

新しいユーザーのBMCの権限:

ユーザーアカウント管理	はい
リモートコンソールアクセス	はい
仮想電源およびリセット	はい
仮想メディア	はい
設定の構成	はい
ホストBIOS	はい
ホストNIC	はい
ホストストレージ	はい

新しいユーザー情報:

新しいユーザー名:

ログイン名:

パスワード:

入力するにはEnterキーを押してください

☒ 変更保留中
☐ 再起動が必要

図 iLO 5 のローカルユーザアカウントの作成

◇IPMI 通信の有効化

次に、[esxi1.vsphere.local]の iLO（BMC）で IPMI 通信を有効にします。手順については、「iLO 5 ユーザーズガイド」の「14. iLO のセキュリティ機能の使用」を参照して、IPMI/DCMI アクセスオプションを[有効]に設定し、[適用]をクリックします。



図 iLO 5 の IPMI 通信の有効化

◇SNMP の設定

続いて、iLO（BMC）で、管理サーバである SSCmanager(172.16.0.1)へ SNMP アラートを行うための設定をします。手順については、「iLO 5 ユーザーズガイド」の「15. iLO マネージメント設定の構成」を参照して、SNMP の設定を行ってください。

1. 以下の設定を行います。

項目名	設定値
読み取りコミュニティ	public
トラップコミュニティ	public
SNMP アラートの送信先	172.16.0.1

2. [適用]をクリックします。

NEC iLO 5 1.10 Jun 07 2017 マネジメント - SNMP設定

情報 システム情報 ファームウェア & OSソフトウェア iLO連携 リモートコンソール&メディア 電力管理 iLO専用ネットワークポート 共有ネットワークポート 管理 セキュリティ マネジメント

SNMP設定 アラートメール リモートSyslog

SNMPの設定

システムの位置

システムコンタクト

システムの役割

システムの役割詳細

読み取りコミュニティ
public

トラップコミュニティ
public

トラップコミュニティ
public

SNMPアラートの送信先
172.16.0.1

SNMPポート
161

適用

図 iLO 5 の SNMP の設定

他の物理サーバ[esxi2.vsphere.local]と[esxi3.vsphere.local]についても、同様に設定します。

7.1.2 Express5800/D120h などの BMC/CMC の設定

◇管理 LAN の設定

まず、物理サーバ [esxi1.vsphere.local] の BMC の管理 LAN の設定を行います。
[esxi1.vsphere.local] の BMC の IP アドレスは "172.16.20.1" を設定します(「1.3 システム構成と使用機材 (2 ページ)」参照)。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「2. サーバ側の設定」を参照して、マネージメント LAN 設定を行ってください。

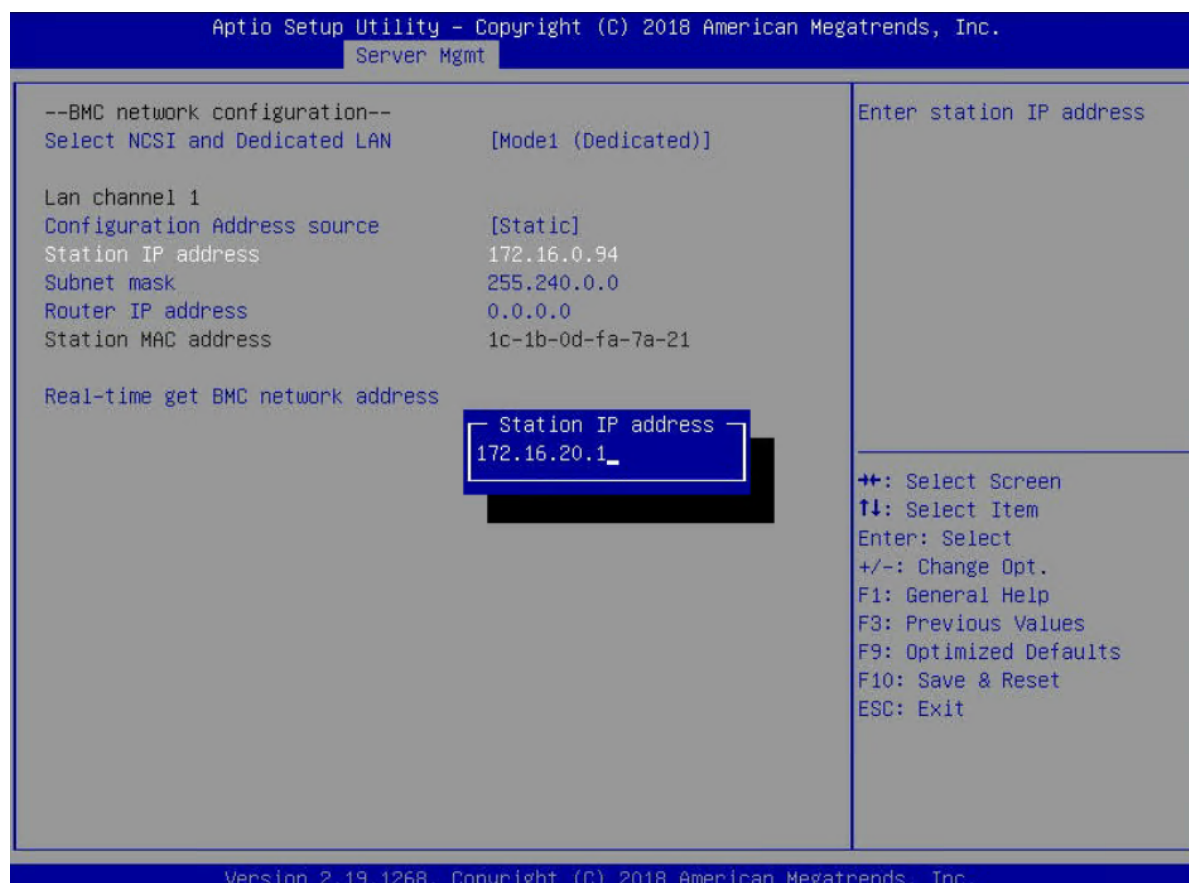


図 マネージメント LAN 設定

◇管理者権限のあるユーザーの作成

次に、[esxi1.vsphere.local]の BMC のリモートマネージメントで管理者権限のあるユーザーを作成します。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネージメントの使い方」を参照して、ユーザーを作成してください。

ここでは、仮に[ユーザ名]を"ssc"、[パスワード]を"sscadmin"に設定したとします。

1. 画面左側のメニューから[EMS]→[設定]→[ユーザー]をクリックします。
2. メインの画面のユーザーリストで任意の[ユーザー ID]をクリックします。

Embedded Management Software サポート ヘルプ 情報 ログアウト

- EMS
 - プロパティ
 - 設定
 - ネットワーク
 - セキュリティ
 - セキュリティ証明書
 - ユーザー
 - サービス
 - 時刻設定
 - 言語
 - セッション
 - LDAP
 - アップデイト
 - ユーティリティ
- サーバー情報
 - LED
 - センサーモニター
 - 電源
 - コントロール
 - 消費電力
 - システムイベントログ
 - イベント管理
 - PEF設定
 - トラップ設定
 - メール設定
 - Serial Over LAN
 - 仮想KVM/メディア
 - 起動
 - 設定
- ハードウェア
 - CPU
 - メモリ
 - ストレージ
 - システムNIC
 - PCIe

ユーザー

変更を適用
更新

特定のユーザーを設定するには、ユーザーIDをクリックします。パスワードポリシーチェックを有効にすると、ユーザー設定を更新する際にパスワード強度がチェックされます。

☐ パスワードポリシーチェックを有効にする

ユーザーID	状態	ユーザー名	ユーザーロール	IPMI LAN 権限	IPMI Serial 権限	Serial Over LAN
1	無効	なし	なし	アドミニストレータ	アドミニストレータ	有効
2	有効	admin	アドミニストレータ	アドミニストレータ	アドミニストレータ	有効
3	有効	ADMIN	アドミニストレータ	アドミニストレータ	アドミニストレータ	有効
4	無効	なし	なし	なし	なし	無効
5	無効	なし	なし	なし	なし	無効
6	無効	なし	なし	なし	なし	無効
7	無効	なし	なし	なし	なし	無効
8	無効	なし	なし	なし	なし	無効
9	無効	なし	なし	なし	なし	無効
10	無効	なし	なし	なし	なし	無効
11	無効	なし	なし	なし	なし	無効
12	無効	なし	なし	なし	なし	無効
13	無効	なし	なし	なし	なし	無効
14	無効	なし	なし	なし	なし	無効
15	無効	なし	なし	なし	なし	無効
16	無効	なし	なし	なし	なし	無効

ようこそ admin (Administrator) ! Fri Oct 13 2017, 11:00:35 (UTC+0000)

図 ユーザーの選択

3. メインの画面の一般セクションで以下の設定を行います。

項目名	設定値
ユーザーを有効にする	チェック
ユーザー名	ssc
パスワードを変更する	チェック
新しいパスワード	"sscadmin"
パスワードの確認	"sscadmin"

4. メインの画面のユーザー権限セクションで以下の設定を行います。

項目名	設定値
ユーザーロール	アドミニストレータ
IPMI LAN 権限	アドミニストレータ
IPMI Serial 権限	アドミニストレータ
Serial Over LAN を有効にする	チェック



図 ユーザーの追加

5. メインの画面右上の[変更を適用]をクリックします。

◇ トラップ設定

続いて、BMC のリモートマネジメントで、管理サーバである SSCmanager(172.16.0.1)へ SNMP アラートを行うための設定をします。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネジメントの使い方」を参照してください。今回は、IP 通報先リストの IP 通報先 1 を使うことにします。

- 画面左側のメニューから[サーバー情報]→[イベント管理]→[トラップ設定]をクリックします。
- メインの画面の IP 通報先リストセクションで以下の設定を行います。

項目名	設定値
有効	チェック
IPv4/IPv6	該当する IP を選択
IP アドレス	172.16.0.1

- メインの画面のコミュニティ名セクションで以下の設定を行います。

項目名	設定値
コミュニティ名	public

- メインの画面右上の[変更を適用]をクリックします。



図 トラップ設定

◇PEF 設定

続いて、BMC のリモートマネジメントで、プラットフォームイベントフィルタの設定をします。手順については、「BMC/CMC 管理コンソール ユーザーズガイド」の「5. リモートマネジメントの使い方」を参照してください。ハードウェアに関連するすべてのイベントが届くように、全てのフィルタで[PET の生成]にチェックを入れます。

- 画面左側のメニューから[サーバー情報]→[イベント管理]→[PEF 設定]をクリックします。
- メインの画面のプラットフォームイベントフィルタ (PEF) アクショングローバル制御リストで以下の設定を行います。

項目名	設定値
アクション名	[PET の生成]をチェック

- メインの画面のプラットフォームイベントフィルタ (PEF) リストセクションで以下の設定を行います。

項目名	設定値
通報有効	チェック
フィルタ名	全てのフィルタについて、[PET の生成]をチェック

- メインの画面右上の[変更を適用]をクリックします。

Embedded Management Software

サポート ヘルプ 情報 ログアウト

EMS

- プロパティ
- 設定
 - ネットワーク
 - セキュリティ
 - セキュリティ証明書
 - ユーザー
 - サービス
 - 時刻設定
 - 言語
 - セッション
 - LDAP
 - アップデート
 - ユーティリティ
- サーバー情報
 - LED
 - センサーモニター
 - 電源
 - コントロール
 - 消費電力
 - システムイベントログ
 - イベント管理
 - PEF設定
 - トラップ設定
 - メール設定
 - Serial Over LAN
 - 仮想KVM/メディア
 - 起動
 - 設定
- ハードウェア
 - CPU
 - メモリ
 - ストレージ
 - システムNIC
 - PCIe

PEF設定

プラットフォームイベントフィルタ (PEF) アクショングローバル制御リスト

アクション名
<input checked="" type="checkbox"/> リポート
<input checked="" type="checkbox"/> パワーサイクル
<input checked="" type="checkbox"/> 電源オフ
<input checked="" type="checkbox"/> PETの生成

プラットフォームイベントフィルタ (PEF) リスト

☒ 通報有効 ⓘ 注: (PEF通報とメール通報の両方を有効または無効にします)。

フィルタ名	なし	リポート	パワーサイクル	電源オフ	PETの生成
Threshold Type, Temperature Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Threshold Type, Temperature Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Threshold Type, Voltage Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Threshold Type, Voltage Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Threshold Type, Fan Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Threshold Type, Fan Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Chassis Intrusion Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Processor Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Processor Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Power Supply Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Power Supply Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Memory Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Memory Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Critical Interrupt Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Sensor-specific Type, Watchdog 2 Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

ようこそ admin (Administrator) ! Fri Oct 13 2017, 11:41:36 (UTC+0000)

図 PEF 設定

他の物理サーバ[esxi2.vsphere.local]と[esxi3.vsphere.local]についても、同様に設定します。

7.1.3 SSC での OOB のアカウント設定

SSC では、物理サーバの BMC または iLO にログインするために、[リソース]ビューで [esxi1.vsphere.local]、[esxi2.vsphere.local]、[esxi3.vsphere.local]のそれぞれの OOB アカウントを設定します。

まず画面右上の[リソース]をクリックして[リソース]ビューを開きます。ツリービューから設定対象の物理サーバである[esxi1.vsphere.local]（ここでは、[マシン]配下）をクリックすると、下の画面のようにマシンの詳細情報が表示されます。



図 マシンの詳細

リソースの設定を編集するには、[設定]メニューにある[プロパティ]をクリックして「マシンプロパティ設定」画面を開きます。

マシンの設定項目は、複数のタブに分類されています。OOB アカウントを設定するには、[アカウント情報]タブをクリックします。[アカウント一覧]の枠の右上の[追加]をクリックすると、「アカウント追加」画面が表示されます。

さらに、「アカウント追加」画面の[プロトコル一覧]の枠の右上の[追加]をクリックすると、下の画面のように[プロトコル]追加の枠が表示されます。

各項目は、以下のように入力します。

- ・ アカウントタイプ : OOB
- ・ ユーザ名 : 物理サーバの BMC(※)のユーザ名を入力 (今回は、"ssc")
- ・ パスワード : 物理サーバの BMC(※)のパスワードを入力 (今回は、"ssadmin")
- ・ 接続先 : 物理サーバの BMC(※)の管理 LAN のホスト名、または、IP アドレス(今回は、"172.16.20.1")
- ・ オフラインマシンのアカウントでも登録する。: チェックしない
- ・ [プロトコル追加]の枠の IPMI : チェックする
- ・ [プロトコル追加]の枠の[監視を有効にする] : チェックする

※BMC の設定については、機種に応じて、「7.1.1 iLO (BMC) の設定 (41 ページ)」 / 「7.1.2 Express5800/D120h などの BMC/CMC の設定 (45 ページ)」を参照してください。



図 OOB アカウントの追加

上記を全て入力した状態で [プロトコル追加] の枠の左下の [OK] をクリックすると、[プロトコル一覧] の枠に [IPMI] が追加されます。続いて、右下の [OK] をクリックします。

以下の画面は、OOB アカウント追加後の [アカウント情報] タブです。[アカウント一覧] の枠に [OOB] が追加され、[接続状態] が [接続可能] となっていれば SSC が管理対象の物理サーバの BMC にログインできたことを示しています。



図 OOB アカウント追加後の「マシンプロパティ設定」([アカウント情報]タブ)

以上で物理サーバの[esxi1.vsphere.local]の OOB アカウントが設定できました。同様の手順を繰り返して、[esxi2.vsphere.local]と[esxi3.vsphere.local]も設定してください。

7.2 動作テスト(一括電源操作)

電源操作ができるようになりましたので、実際に電源操作のテストを行ってみましょう。

テストでは、vCenter Server 下の Datacenter を選択して、Datacenter 下の全ての物理マシン・仮想マシンを一括して電源操作を行う以下の操作を行います。

- マシンシャットダウン
- マシン起動

7.2.1 仮想マシン自動起動の設定

まず、デフォルトでは、一括操作で物理サーバを起動した時に仮想マシンが自動で起動しないようになっていますので、仮想マシンを自動起動できるように次の設定変更が必要です。


1. [運用]ビュー（画面右上の[運用]をクリック）を開いて、ツリービューから設定対象の運用グループである[Datacenter]をクリックします。
2. 画面右上の[設定]メニュー下の[プロパティ]をクリックして、「グループプロパティ設定」画面の[全般]タブを表示します。

3. 以下の設定変更を行います。

- ・[VM サーバシャットダウン時に自動停止された VM を起動する]のチェックをオン
- 物理サーバのシャットダウンを実行する際、起動中の仮想マシンは物理サーバのシャットダウン前にシャットダウンが行われますが、上記設定により、次回物理サーバが起動した時に、仮想マシンも自動的に起動されます。

※物理サーバシャットダウン時に起動していなかった仮想マシンは、自動起動されません。

運用 > vcenter-vs.. > Datacenter

 グループプロパティ設定

[戻る](#)

全般	モデル	ストレージ	ソフトウェア	ネットワーク設定	LB設定	ホストプロファイル	VM最適配置
<div>VM配置制約 データストア設定 死活監視 性能監視 カスタム</div> <div> <p>親グループ名 vcenter-vmware-local</p> <p>グループ名 <input type="text" value="Datacenter"/></p> <p>マシン種別 <input type="text" value="VMサーバ"/></p> <p>プライオリティ <input type="text" value="10"/></p> <div> <p>ポリシー設定</p> <p>ポリシー名#1 <input type="text" value="標準ポリシー(仮想マシンサーバ)"/> 参照</p> <p>ポリシーの追加</p> </div> <p>データセンター <input type="text" value="vcenter.vsphere.local/Datacenter"/></p> <p>通報先メールアドレス情報(TO) <input type="text"/></p> <p>グループ説明 <div><div></div></div></p> <div> <p>起動設定</p> <p><input checked="" type="checkbox"/> VMサーバシャットダウン時に自動停止されたVMを起動する</p> </div> <p>グループマシン使用方法</p> </div>							

図 「グループプロパティ設定」画面の[全般]タブ

7.2.2 マシンシャットダウン

準備ができましたので、一括シャットダウンを行ってみましょう。

一括電源操作は[仮想]ビューから行います（画面右上の[仮想]をクリック）。

次に、ツリービュー上で一括操作の単位となる[Datacenter]をクリックします。

画面右側の[操作]メニュー下の[マシンシャットダウン]をクリックすると、[Datacenter]下の物理サーバ、仮想マシンの一括シャットダウン操作が開始します。



図 [マシンシャットダウン]操作

「シャットダウンオプション」ダイアログが表示されますので、次の設定を行います。

- [VM サーバをメンテナンスモードにする]のチェックをオンにする。
 - [VM サーバの起動時にメンテナンスモードを解除する]のチェックをオンにする。

ヒント

メンテナンスモードは、保守中のマシンなど、SSC による自動の仮想マシンの移動 (Migration(vMotion))などを抑止したい時に設定してください。

メンテナンスモードを設定したマシンに対しては、SSC は自動の処理を実行しなくなります。

また、上記の設定では、SSC だけでなく、vCenter Server 上でもメンテナンスモードに切り替わります。

[OK]をクリックすると、実際のシャットダウン操作が開始します。

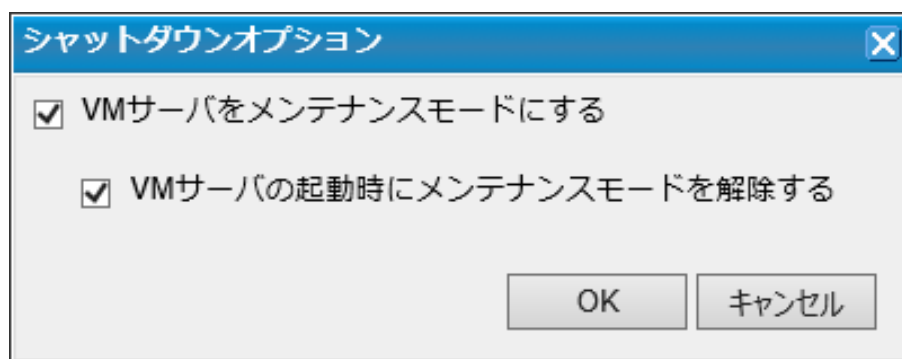


図 「シャットダウンオプション」画面

シャットダウン処理中、画面は次のように表示されます。画面下側のジョブウィンドウにシャットダウンジョブの進捗状況が表示されます。

VMサーバー一覧

VMサーバ名	状態	電源	接続状態	使用量/キャパシティ	IPアドレス	VM数
esxi1.vsphere.local	処理中	Running	接続可能	20/200	172.16.10.1	2
esxi2.vsphere.local	処理中	Running	接続可能	20/200	172.16.10.2	2
esxi3.vsphere.local	処理中	Running	接続可能	20/200	172.16.10.3	2

ジョブ

進捗	ジョブ名	実行者	開始日時	終了日時
24%	マシンのシャットダウン (esxi1.vsphere.local)	admin	2018/07/11 17:16:49	
24%	マシンのシャットダウン (esxi2.vsphere.local)	admin	2018/07/11 17:16:49	
24%	マシンのシャットダウン (esxi3.vsphere.local)	admin	2018/07/11 17:16:49	
0%	マシンを停止する	admin	2018/07/11 17:16:48	
Success	マシンの起動	admin	2018/07/11 17:05:10	2018/07/11 17:08:41

図 マシンシャットダウン中の画面

操作が完了すると、画面は次のように表示されます。



図 マシンシャットダウン完了時の画面

以上で、[マシンシャットダウン]操作は完了です。

7.2.3 マシン起動

次に、一括起動操作で、先ほどシャットダウンした各マシンを起動してみましょう。

[仮想]ビュー（画面右上の[仮想]をクリック）から、ツリービュー上で一括操作の単位となる[Datacenter]をクリックした画面から、画面右側の[操作]メニュー下の[マシン起動]をクリックすると、[Datacenter]下の物理サーバ、仮想マシンの一括起動操作が開始します。

操作確認のダイアログが表示されますので、[OK]をクリックすると、実際の起動操作が開始します。



図 [マシン起動]操作

操作が完了すると、画面は次のように表示されます。

操作実行前に物理サーバ(ESXi)に設定されていたメンテナンスモードは、マシンシャットダウン時の「シャットダウンオプション」画面で[VM サーバの起動時にメンテナンスモードを解除する]のチェックをオンに指定していたため、自動的に解除されます。

また、各物理サーバ上の仮想マシンについては、物理サーバのシャットダウン前は起動していたので、「7.2.1 仮想マシン自動起動の設定 (53 ページ)」での[VM サーバシャットダウン時に自動停止された VM を起動する]のチェックオンの指定により、自動的に起動されます。



図 マシン起動完了時の画面

以上で、電源操作のテストは完了です。

8. 予兆を含む障害対応機能の設定

ここからは、障害発生や負荷変動を検出するための監視の設定と、障害発生・負荷変動に応じて仮想マシンを制御するための設定の方法について、説明します。

最後に、擬似的に障害のイベントを発生させて動作を確認します。

8.1 監視・通報の基本設定

管理サーバの OS や SSC の環境設定について、監視や通報のために基本的な設定を行います。

- SNMP Trap サービスの設定
- Windows ファイアウォールの設定
- 死活監視の基本設定
- 通報に必要な環境設定

8.1.1 SNMP Trap サービスの設定

OS 起動時に Windows の SNMP Trap サービスが自動的に起動するように設定します。

Windows の[スタート]メニューから[Windows 管理ツール]→[サービス]をクリックします。「サービス」が開いたら、[SNMP Trap]サービスの[スタートアップの種類]を[自動]に設定します。

8.1.2 Windows ファイアウォールの設定

SSC が管理対象と通信できるように、Windows ファイアウォールに接続を許可する設定を行います。SSC のインストーラでは、Windows ファイアウォールに最低限の接続許可設定を行いますが、管理内容によっては設定を追加しておく必要があります。

今回、物理サーバからの障害通報の受信と仮想マシンの死活監視のために、Windows ファイアウォールの設定を追加します。

まず、障害通報の受信のために SNMP Trap を受信できるようにします。

Windows の[スタート]メニューから[Windows 管理ツール]→[セキュリティが強化された Windows ファイアウォール]をクリックします。「セキュリティが強化された Windows ファイアウォール」画面が開いたら、[受信の規則]をクリックして規則の一覧を表示します。

デフォルトでは、次の画面のように一覧の中にはプロファイルの異なる二つの[SNMP トラップ サービス (UDP 受信)]があります。使用する管理用ネットワークに適したプロファイルの[SNMP トラップ サービス (UDP 受信)]を選択し、[操作]メニューから[規則の有効化]をクリックします。どちらのプロファイルの規則も、デフォルトでは[接続を許可する]よう

に設定されていますので、これで **SNMP Trap** を受信できるようになります。今回は、[プライベート、パブリック]のプロファイルを選択します。

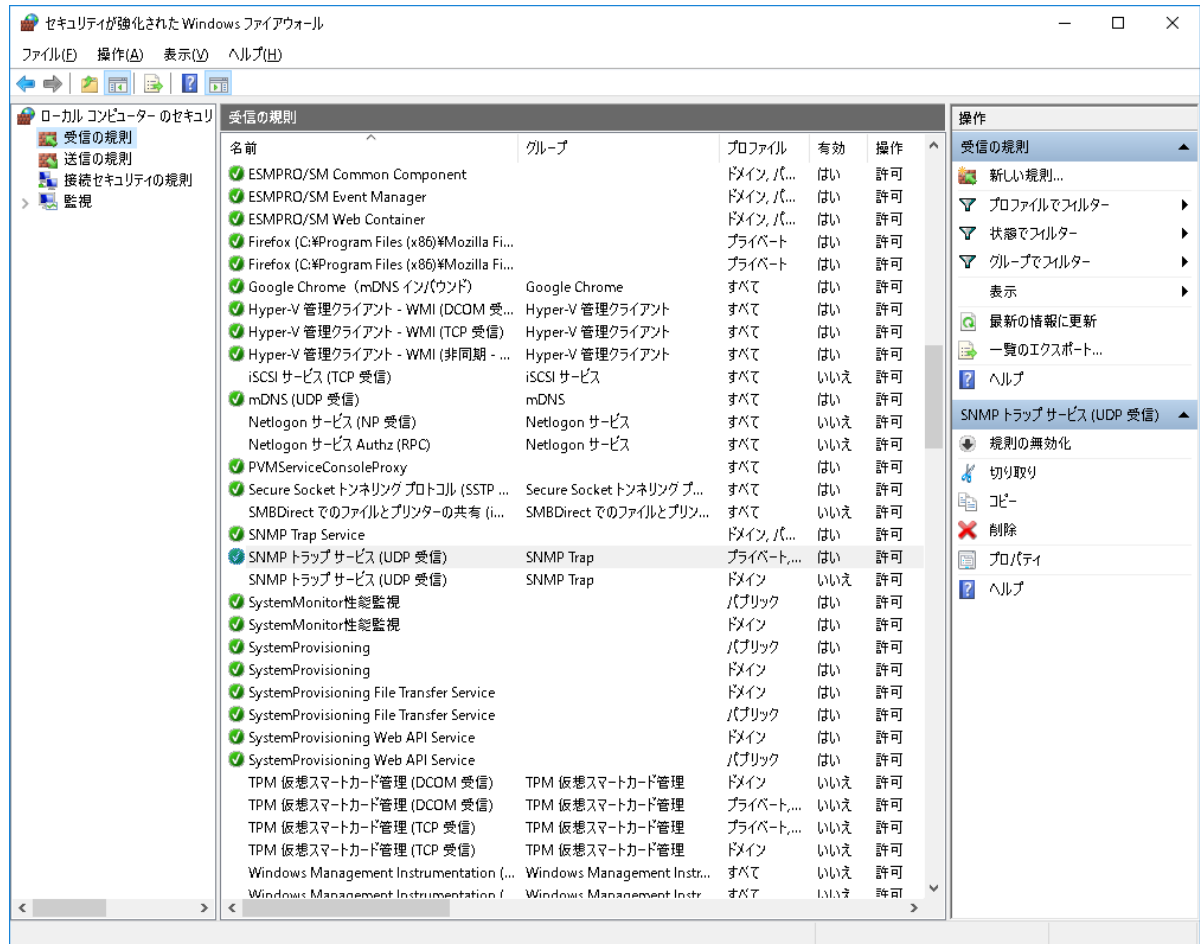


図 セキュリティが強化された Windows ファイアウォール (SNMP トラップ サービス (UDP 受信))

次に、死活監視 (Ping 監視) のために ICMP Echo Reply を受信できるようにします。

「セキュリティが強化された Windows ファイアウォール」画面の[受信の規則]をクリックして規則の一覧を表示します。[操作]メニューから[新しい規則]をクリックします。

「新規の受信の規則ウィザード」ダイアログが開いたら、各ステップで次のように規則を作成します。

- 規則の種類
 - [カスタム]ラジオボタンを選択
- プログラム
 - [このプログラムのパス]を選択
 - パス入力欄に"%ProgramFiles% (x86)\%NEC\PVM\bin\PVMServiceProc.exe"を入力
- プロトコルおよびポート

- [プロトコルの種類]で[ICMPv4]を選択
- スコープ
 - [この規則を適用するローカル IP アドレスを選択してください。]で、[任意の IP アドレス]を選択（デフォルト）
 - [この規則を適用するリモート IP アドレスを選択してください。]で、[任意の IP アドレス]を選択（デフォルト）
- 操作
 - [接続を許可する]を選択（デフォルト）
- プロファイル
 - 管理用ネットワークに適したプロファイルを選択(今回は[プライベート]を選択します)
- 名前
 - 任意の名前を入力(今回は"SystemProvisioning(ICMPv4)"と入力します)

[受信の規則]の一覧に[名前]が[SystemProvisioning(ICMPv4)]で、[プロトコル]が[ICMPv4]の規則が追加されたことを確認します。

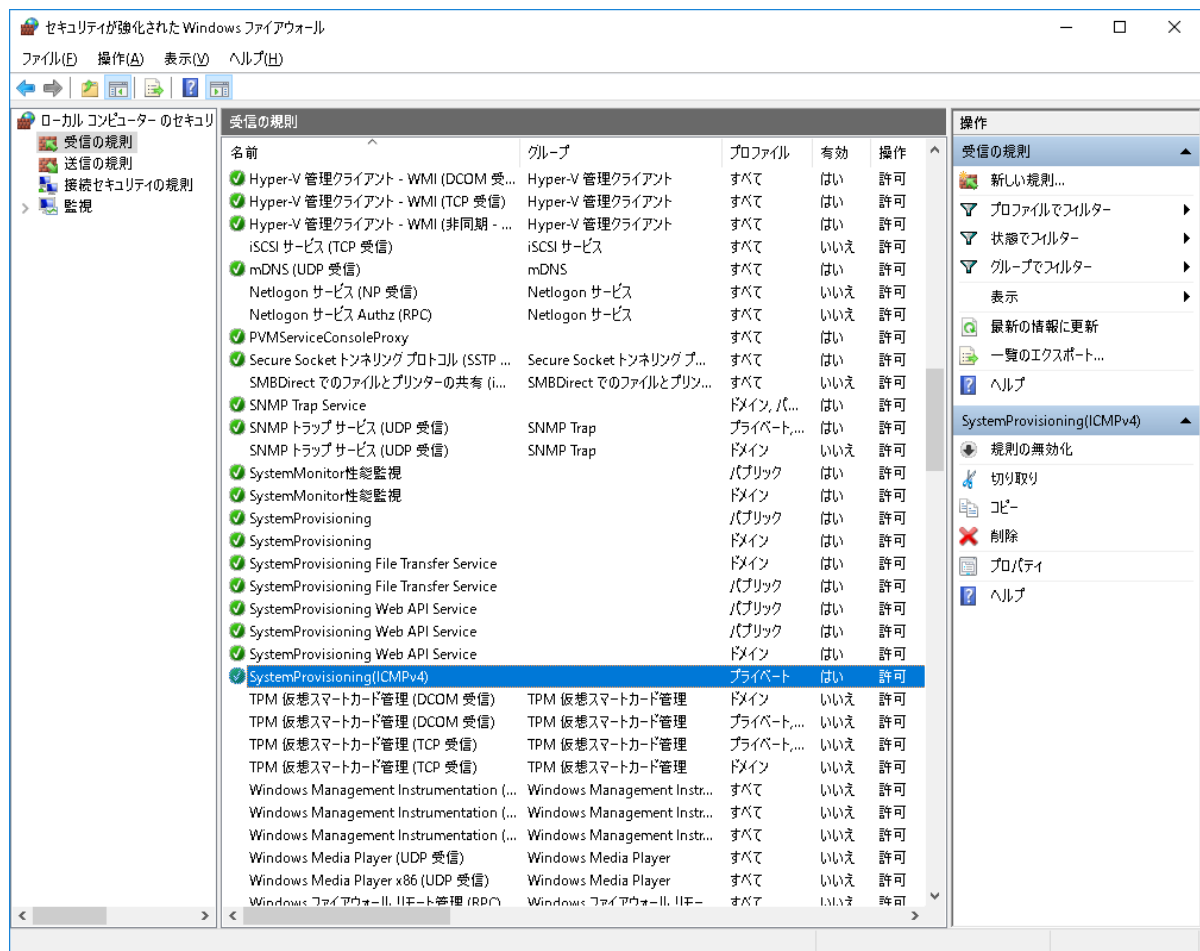


図 セキュリティが強化された Windows ファイアウォール (SystemProvisioning(ICMPv4))

以上の設定が完了したら、管理サーバを再起動してください。

8.1.3 死活監視の基本設定

SSC で死活監視を行う場合は、全体としてどの死活監視を有効にするのか、こういった間隔で実行するのかなどの基本の設定をしておきます。その上でそれぞれの管理対象ではどの死活監視を利用するかを別に設定します。

基本設定を行うために[管理]ビュー（画面右上の[管理]をクリック）を開きます。[管理]ビューが開いたらツリービューにある[環境設定]をクリックして「環境設定」画面を開き、[死活監視]タブをクリックします。

今回は仮想マシンも死活監視の対象としますので、[監視対象モデル種別]の枠の[VM]チェックボックスをチェックし、右下の[適用]をクリックしてください。



図 「環境設定」画面（[死活監視]タブ）

他の設定項目については、死活監視により機能停止イベントなどを過剰に検出する場合など、ネットワークや、サーバの性能に応じて調整します。

今回はそのままの値で使用し、問題がある場合のみ調整してください。

8.1.4 通報に必要な環境設定

次に、障害や負荷といった事象が発生した際に通報を行うための設定を行っておきます。

通報には、メール通報とイベントログ出力の二種類があります。デフォルトではイベントログ出力のみが有効なので、メール通報は実行されません。今回はメール通報も行うように設定します。

メール通報の環境設定は[管理]ビュー（画面右上の[管理]をクリック）で行います。[管理]ビューを開いたらツリービューにある[環境設定]をクリックし「環境設定」画面を開き、[通報]タブをクリックします。



図 「環境設定」画面（[通報]タブ）

まず、[メール通報を行います]チェックボックスをチェックし、入力欄を有効にします。その後、メールを送信するためのメールサーバ（SMTP）、通報先メールアドレス、送信元メールアドレスを設定します。

各項目は次のように設定します。

表 メール通報の設定（入力例）

設定項目	説明	入力例
メール通報を行います	メール通報を有効にする場合はチェック	—
通信先メールサーバ名	通報メールを送信するためのメールサーバ (SMTP)	"smtp.test.nec.com"
ポート番号	[通信先メールサーバ]が使用しているポート番号	"25"（デフォルト）

設定項目	説明	入力例
SMTP 認証を行う	[通信先メールサーバ]が SMTP 認証を行っている場合はチェック	-
認証アカウント	SMTP 認証で使用するアカウント名	"sscadmin"
認証パスワード	SMTP 認証で使用するパスワード ([パスワード更新]をチェックして入力)	表示されません
保護された接続(TLS)を使用する。	[通信先メールサーバ]に 暗号化(TLS)接続する場合はチェック	—
通信元メールアドレス (From)	通報メールの送信元となるメールアドレス (必須)	"sscadmin@test.nec.com"
通信先メールアドレス (To)	通報メールの送信先となるメールアドレス (必須)	"t-nichiden@test.nec.com"

メール通報に必要な項目を入力したら、実際に送信できるかのテストを行います。右下の[テスト送信]をクリックすると通信先メールアドレスへテストメールが送信されます。テストメールを受信して問題がないことを確認します。

テストで問題がないことを確認したら、右下の[適用]をクリックして、設定内容を保存します。

なお、[通報]タブの下の[通知をイベントログに書き込む]チェックボックスは、管理サーバの Windows のイベントログへの出力を有効にします。デフォルトではチェック(有効)になっており、今回も出力することとします。

8.2 負荷監視の設定

ここからは管理対象マシンの負荷状況を監視するために必要な設定を行います。

今回説明する負荷監視の設定は、先に仮想マシンの負荷状況の取得の設定の変更が必要です。

仮想マシンの負荷状況の取得の設定は、デフォルトでは下記 ESXi 経由の監視プロファイルが設定されますが、ここでは、業務視点のメモリの情報を監視するために、後者(ゲスト OS 経由)の設定を行った場合を説明しますので設定変更が必要です。「[B.2.2 ゲスト OS 経由での負荷状況取得の設定 \(99 ページ\)](#)」を参考に監視プロファイルの設定変更を行ってください。

負荷状況の取得の設定については「[付録 B. 負荷状況取得の設定 \(94 ページ\)](#)」を参照してください。

- ESXi 経由([Builtin](For Report)VM Monitoring Profile[Hypervisor])
 - 「[B.2.1 ESXi 経由での負荷状況取得の設定 \(98 ページ\)](#)」
- ゲスト OS 経由([Builtin](For Report)VM Monitoring Profile[VM OS])
 - 「[B.2.2 ゲスト OS 経由での負荷状況取得の設定 \(99 ページ\)](#)」

ゲスト OS 経由の監視プロファイル[Builtin](For Report)VM Monitoring Profile[VM OS](5min)の以下の性能情報に閾値の設定を行ってみましょう。

- CPU Usage (%)
- Physical Memory Space Ratio (%)

まず、[リソース]ビュー（画面右上の[リソース]をクリック）を開き、ツリービューから[監視プロファイル]を選択します。「監視プロファイル一覧」画面に用意されている監視プロファイルの一覧が表示されます。

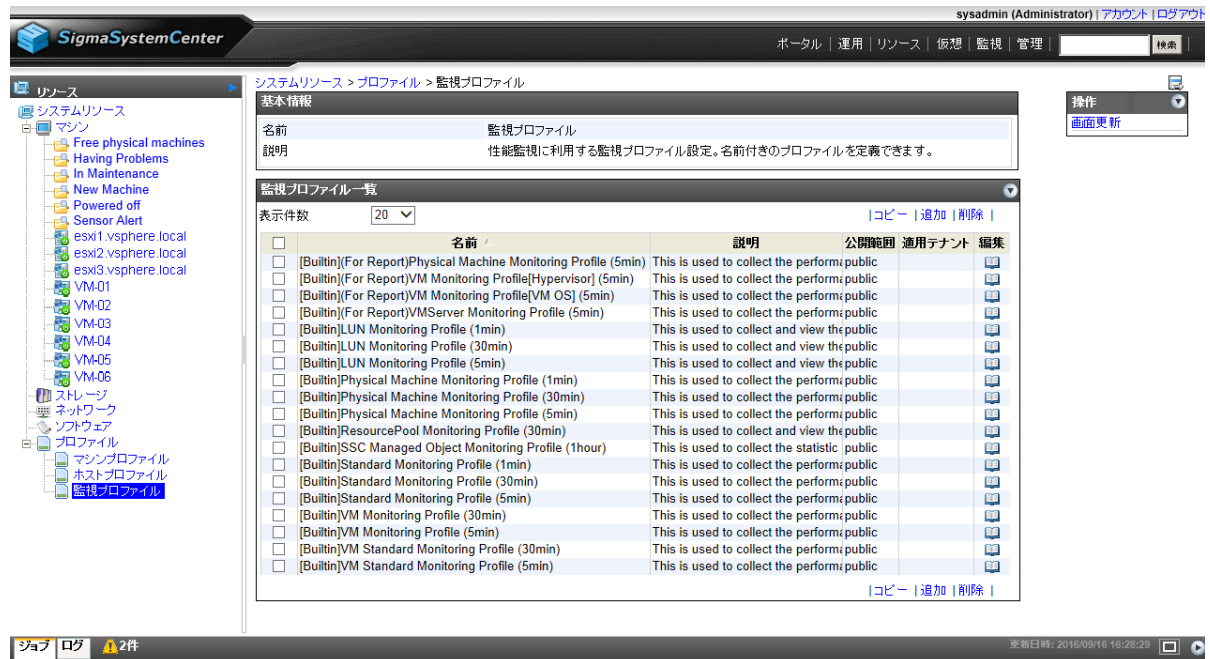


図 監視プロファイル一覧

[監視プロファイル一覧]から、監視プロファイル[Builtin](For Report)VM Monitoring Profile[VM OS](5min)の行の右端にある[編集]アイコンをクリックすると、「監視プロファイル編集」画面が表示されます。



図 監視プロファイル編集

ここからは、個々の性能情報の設定を行います。

まず、CPU 使用率が閾値に達した際に通報するための設定を行います。

CPU 使用率を表す CPU Usage (%) の設定を変更するために、CPU Usage (%) の行の右端にある[編集]アイコンをクリックして、「性能情報設定」画面を表示します。



図 CPU Usage (%) の「性能情報設定」

CPU Usage (%) の閾値監視の設定を追加するには、「閾値監視情報一覧」画面の[追加]をクリックします。クリックすると、以下の「閾値監視設定」画面が開きます。CPU Usage (%) が 80%に達する状況が、10 分間続いた場合に通報する場合は、以下のように設定します。

- 有効にする：チェックする（変更しません）
- 性能情報：CPU Usage (%)
- 監視種類：上限異常値監視（変更しません）
- 監視対象種類：マシン（変更しません）
- 統計計算方法：平均値（変更しません）
- 閾値：80
- 超過通報：上限異常超過
- 回復通報：上限異常回復
- 超過時間：10（分）
- 再通報する：チェックする（変更しません）

閾値監視設定

☒ 有効にする

性能情報: CPU Usage (%)

監視種類: 上限異常値監視

監視対象種類: マシン

統計計算方法: 平均値

閾値: 80

超過通報: 上限異常超過

回復通報: 上限異常回復

超過時間: 10 分 ☒ 再通報する

OK キャンセル

図 CPU Usage (%) の「閾値監視設定」

[OK]をクリックすると、閾値監視情報一覧に設定が追加されます。

sysadmin (Administrator) | アカウント | ログアウト

ポータル | 運用 | リソース | 仮想 | 監視 | 管理 | 検索

システムリソース > プロファイル > 監視プロファイル > 編集

性能情報一覧

性能情報	収集間隔	編集
<input type="checkbox"/> CPU Usage (%)	5 分	
<input type="checkbox"/> Disk Read Count (IO/sec)	5 分	
<input type="checkbox"/> Disk Read Transfer Rate (Bytes/sec)	5 分	
<input type="checkbox"/> Disk Space (MB)	5 分	
<input type="checkbox"/> Disk Space Ratio (%)	5 分	
<input type="checkbox"/> Disk Write Count (IO/sec)	5 分	
<input type="checkbox"/> Disk Write Transfer Rate (Bytes/sec)	5 分	
<input type="checkbox"/> Network Packet Transfer Rate (Bytes/sec)	5 分	
<input type="checkbox"/> Physical Memory Space (MB)	5 分	
<input type="checkbox"/> Physical Memory Space Ratio (%)	5 分	

OK キャンセル

性能情報設定

リソース: CPU

性能情報: CPU Usage (%)

収集間隔: 1 分

閾値監視情報一覧

監視種類	監視対象種類	統計計算方法	閾値	監視状態	編集
<input type="checkbox"/> 上限異常値監視	マシン	平均値	80	有効	

OK キャンセル

ジョブ ログ

更新日時: 2013/08/23 19:41:29

図 性能監視情報一覧

[OK]をクリックすると、性能情報設定が閉じます。

次に、メモリの空き容量割合について、データを収集し、閾値に達した際に通報するための設定を実施します。メモリの空き容量割合を表す Physical Memory Space Ratio (%) は、監視

プロファイル [Builtin]Standard Monitoring Profile に含まれていないため、新たに追加する必要があります。「性能情報一覧」画面で[追加]をクリックして、表示された「性能情報設定」画面に、以下のような設定を行います。

- ・ リソース : Memory
- ・ 性能情報 : Physical Memory Space Ratio (%)
- ・ 収集間隔 : 1 分 (変更しません)



図 Physical Memory Space Ratio (%) 性能情報設定

次に、Physical Memory Space Ratio (%) の閾値監視の設定を追加するために、「閾値監視情報一覧」画面の[追加]をクリックします。クリックすると、「閾値監視設定」画面が開きます。メモリの空き容量割合が 10%に達する状況が、30 分間続いた場合に通報する場合は、以下のように設定します。

- ・ 有効にする : チェックする (変更しません)
- ・ 性能情報 : Physical Memory Space Ratio (%)
- ・ 監視種類 : 下限異常値監視
- ・ 監視対象種類 : マシン (変更しません)
- ・ 統計計算方法 : 平均値 (変更しません)
- ・ 閾値 : 10
- ・ 超過通報 : 下限異常超過

- 回復通報：下限異常回復
- 超過時間：30（分）
- 再通報する：チェックする（変更しません）

The screenshot shows a dialog box titled '閾値監視設定' (Threshold Monitoring Settings) with a close button (X) in the top right corner. The dialog is for configuring monitoring for 'Physical Memory Space Ratio (%)'. It includes a checkbox '有効にする' (Enable) which is checked. Below this, there are several settings:

性能情報	Physical Memory Space Ratio (%)
監視種類	下限異常値監視
監視対象種類	マシン
統計計算方法	平均値
閾値	10
超過通報	下限異常超過
回復通報	下限異常回復
超過時間	30 分

At the bottom right, there is a checkbox '再通報する' (Report again) which is checked. At the bottom center, there are two buttons: 'OK' and 'キャンセル' (Cancel).

図 Physical Memory Space Ratio (%) 性能監視設定

[OK]をクリックすると、CPU Usage (%) の設定時と同様、閾値監視情報一覧に設定が追加されます。

さらに、性能情報設定の[OK]をクリックし、「監視プロファイル編集」の画面に戻ります。

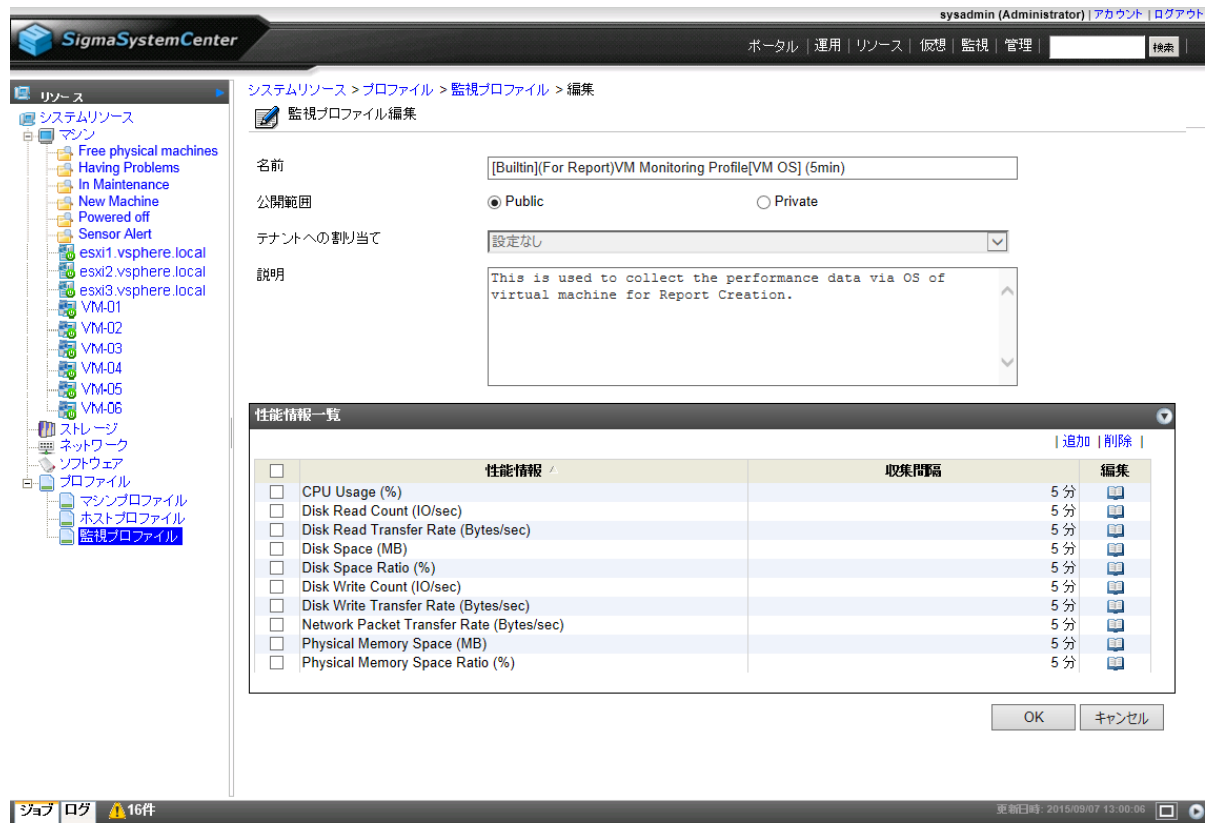


図 性能情報一覧

最後に、[OK]をクリックして、以上で閾値の設定は完了です。

8.3 死活監視の設定

死活監視を行うには、「[8.1.3 死活監視の基本設定 \(63 ページ\)](#)」で説明した共通の基本設定を行った上で、それぞれのグループ、または、ホストへの設定を行います。

今回は、グループの単位で死活監視の設定を行います。

グループ単位の死活監視の設定を行うには、[運用]ビュー（画面右上の[運用]をクリック）を開きます。

まずは、仮想マシンの死活監視の設定のため、[Datacenter_VM]グループの設定を行うことにします。[Datacenter_VM]グループに適用する[仮想マシン用ポリシー](後述の「[8.4.2 仮想マシン用ポリシーの確認と適用 \(77 ページ\)](#)」参照)では、Ping 監視、ポート監視のイベント（ターゲットアクセス不可）に対処するようになっています。

今回、[Datacenter_VM]グループの仮想マシンでは Web サーバが動作しているものとして、Port 監視では 80 を監視します。

Ping 監視、ポート監視の設定は次のように行います。

1. ツリービューにある[Datacenter_VM]グループをクリック
2. [設定]メニューの[プロパティ]をクリック

3. 「グループプロパティ設定」画面が開いたら[死活監視]タブをクリック
4. [死活監視機能を有効にする]チェックボックスをチェック
5. [Ping 監視]チェックボックスをチェック
6. [Port 監視]チェックボックスをチェックし、[監視ポート]に"80"を入力
7. 右下の[適用]をクリックする



図 [Datacenter_VM]グループの「グループプロパティ設定」画面（[死活監視]タブ）

次に物理サーバの死活監視について説明します。

[Datacenter]グループ(ESXi)の物理サーバに適用する[仮想マシンサーバ用ポリシー(VMware)](後述の「[8.4.3 物理サーバ用ポリシーの確認と適用 \(80 ページ\)](#)」参照)では、vCenter Server を利用した死活監視のイベント（VMS アクセス不可）に対処するようになっています。

vCenter Server では、[Datacenter]グループ(ESXi)の物理サーバに対する死活監視はデフォルトで有効になっていますので、設定変更は必要ありません。

また、設定変更は不要ですが、デフォルトでは[Datacenter]グループ(ESXi)の「グループプロパティ設定」画面の[死活監視]タブは以下のようになっています。

注

[ESMPRO/SM にマシンを登録する]チェックボックスのチェックは、有効になっていますが、本設定は使用されませんので注意してください。

ESMPRO/ServerManager に管理対象マシンを登録したい場合は、ESMPRO/ServerManager の画面から行う必要があります。

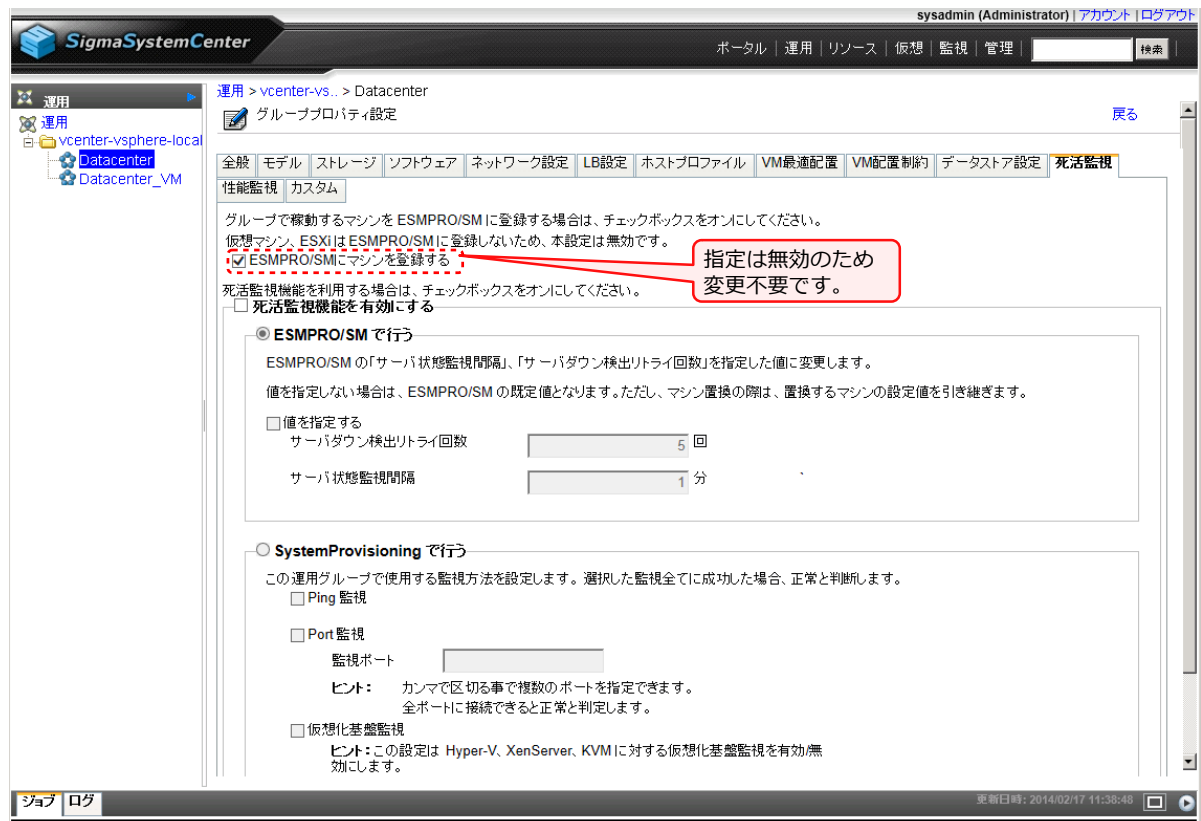


図 [Datacenter]グループ(ESXi)の「グループプロパティ設定」画面（[死活監視]タブ）

8.4 障害や負荷に対するポリシーの設定

ここからは障害発生時や負荷変動に応じて仮想マシンを制御するためのポリシーの設定を行います。このポリシーは「あるイベントが発生した際にどのようなアクションを実行するか」というルールの集まりです。

例えば、「障害を示すイベントが発生した場合は、対象のサーバに故障マークを設定し通報を行う。」といった動作もポリシーで設定します。

ポリシーの設定は[管理]ビュー（画面右上の[管理]をクリック）で行います。[管理]ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。



図 ポリシー一覧

上記「ポリシー一覧」画面のように、ポリシー一覧にはあらかじめ4種類のポリシーが用意されています。これらの標準ポリシーはそのまま使用することもできますが、システムに合わせてテンプレートから作成したものを使用することもできます。

また、あらかじめシステムに合わせて作られたポリシーをインポートして利用することもできます。

本ガイドで想定するシステム向けには、Web サイトに仮想マシン用のポリシーと物理サーバ用のポリシーが用意されているため、今回はこれらをインポートして利用します。

8.4.1 ポリシーのインポート

製品 Web サイトの以下のファイルをダウンロードします。

- 簡易構築ガイド用ポリシーファイル(VMware)

管理サーバの任意のフォルダに以下のファイルを解凍します。今回は、<C:\temp>に保存したとします。

- vm_policy.xml : 仮想マシン用ポリシー
- esxi_policy.xml : 物理サーバ（仮想マシンサーバ）用ポリシー

まず、仮想マシン用のポリシーファイルである[vm_policy.xml]をインポートします。

Windows の[スタート]メニューから[Windows システムツール]→[コマンドプロンプト]をクリックします。コマンドプロンプトが起動したら、次のように ssc コマンドを実行してください。

```
> ssc import policy "C:\temp\vm_policy.xml"
```

実行後に[実行終了 コード：0]が表示されれば、インポートが完了しています。

同様に、物理サーバ用の[esxi_policy.xml]もインポートしてください。

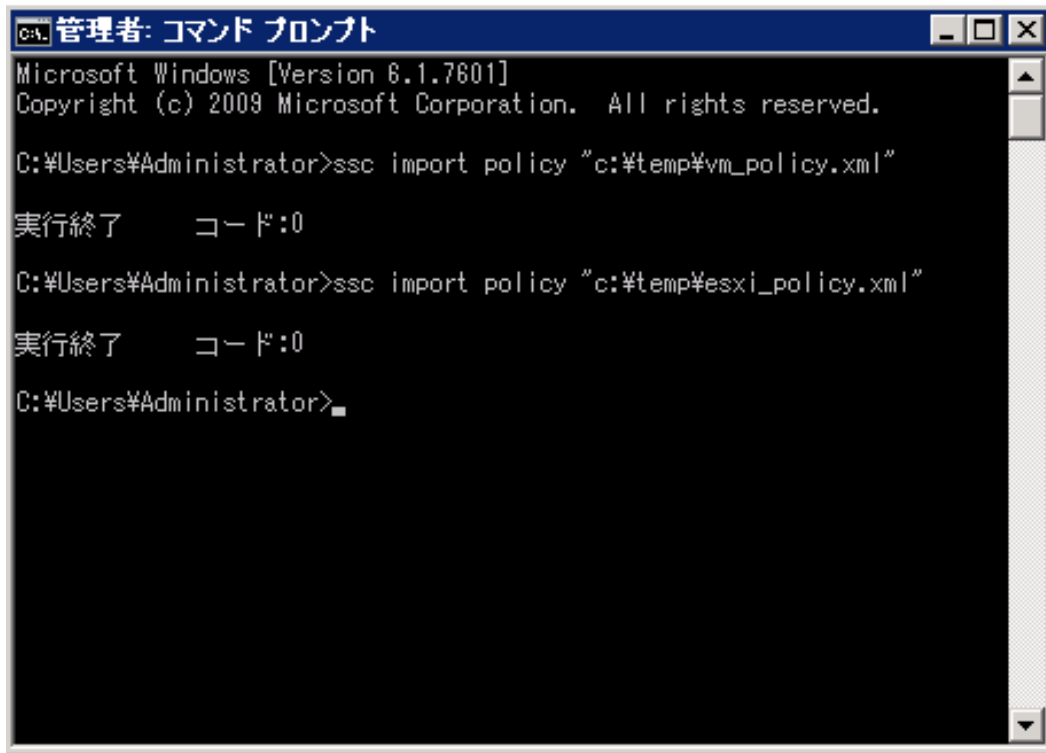


図 ssc コマンドによるポリシーのインポート（インポート実行後）

二つのポリシーのインポートが完了したら SSC の Web コンソールに戻り、「ポリシー一覧」画面の[操作]メニューの[画面更新]をクリックしてください。

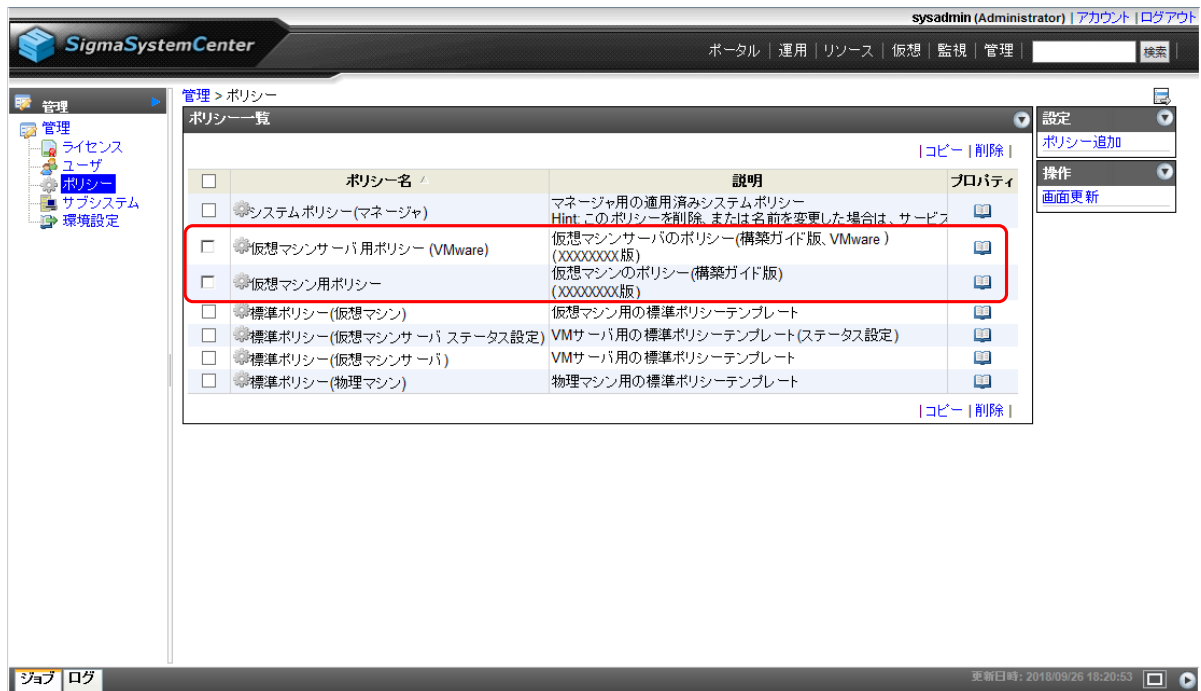


図 「ポリシー一覧」(インポート後)

「ポリシー一覧」画面に「仮想マシンサーバ用ポリシー(VMware)」と「仮想マシン用ポリシー」が表示されます。

8.4.2 仮想マシン用ポリシーの確認と適用

次に、仮想マシン用のグループ ([Datacenter_VM]グループ) に、先ほどインポートした仮想マシン用のポリシーを適用します。

(1)仮想マシン用のポリシーの確認

ポリシーを適用する前にどのようなルールが定義されているのかを確認しておきましょう。
[管理]ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。

仮想マシン用にインポートしたポリシーは、[仮想マシン用ポリシー]です。[仮想マシン用ポリシー]の[プロパティ]アイコンをクリックして「ポリシープロパティ設定」画面を開き[ポリシー規則]タブをクリックします。

[ポリシー規則一覧]の枠の[状態]が[有効]になっているイベントに注目します。

[仮想マシン用ポリシー]では大まかに次の考えに基づいた設定がデフォルトとなっています。

- 仮想マシンが停止している可能性がある場合

対処として、故障マーク設定と通報、イベントログ出力を行います。

「ターゲットアクセス不可」、「マシン停止」が該当します。

- ・ 仮想マシンの負荷が設定した閾値を上回った（下回った）場合

対処として、通報、イベントログ出力を行います。

「CPU 使用率（%）異常（回復）」、「メモリ空き容量割合（%）異常（回復）」が該当します。

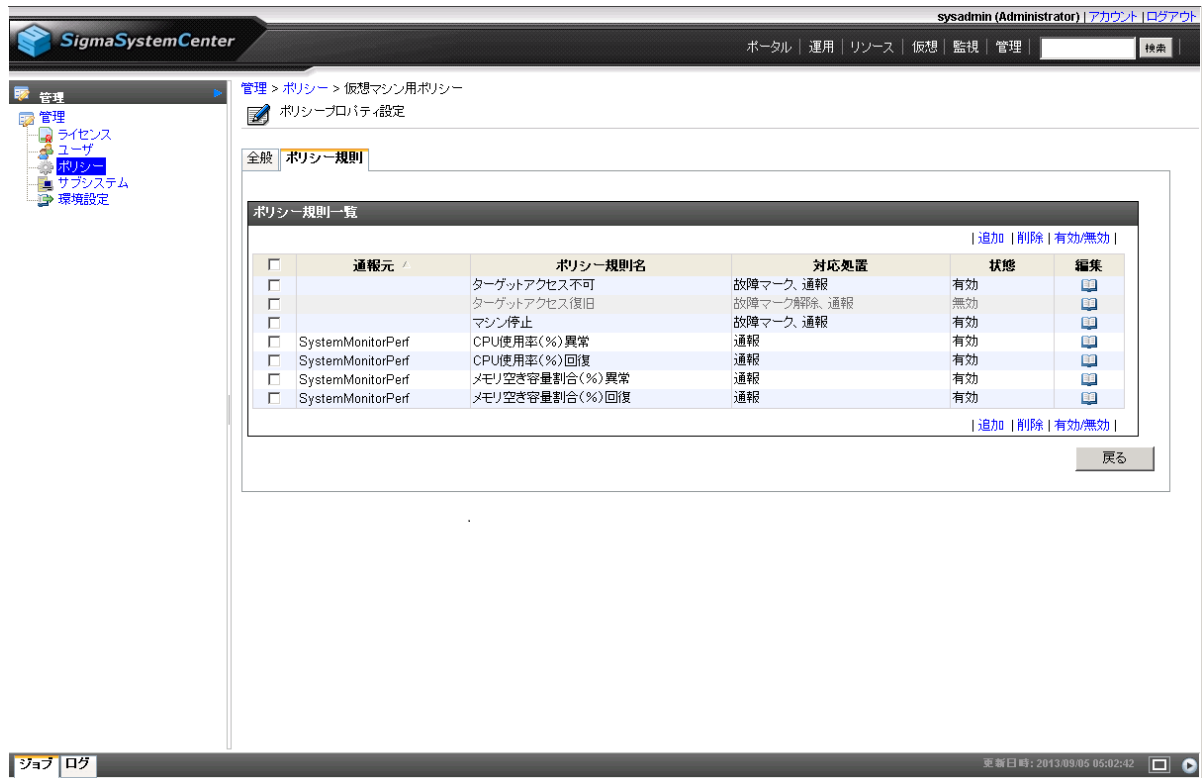


図 「ポリシープロパティ設定」画面（[ポリシー規則]タブ）

次に、イベントが発生した際に実行する対応処置の詳細を確認します。

「ターゲットアクセス不可」では Ping 監視とポート監視によって仮想マシンの死活監視を行っています。「ターゲットアクセス不可」イベントの列の[編集]アイコンをクリックすると、「ポリシー規則設定（編集）」画面が表示されます。

この画面（ポリシー規則設定（編集））では、監視するイベントの情報とそのイベントが発生した際に実行する処理（アクション）を確認、設定することができます。

画面上ではイベントを定義し、そのイベントに対し、画面下にある[イベントに対するアクション]の枠内で実行するアクションを設定します。

デフォルトでは、1 番目のアクションとして[通報/ E-mail 通報、イベントログ出力]、2 番目のアクションとして[マシン設定/ ステータス設定 故障]が設定されていることが確認できます。

上記の設定より、仮想マシンが Ping 監視、ポート監視で反応がない場合には、「通報/ E-mail 通報、イベントログ出力を行い、故障マークを設定する。」という動作を行うことが分かります。

今回はデフォルト設定を利用しますので、何も変更せずに画面下の[戻る]をクリックします。



図 対応処置詳細設定（編集）

(2)仮想マシン用のポリシーの適用

[運用]ビューで作成したグループ単位にポリシーを適用するため、[運用]ビューの「グループプロパティ設定」画面で適用作業を行います。

まず、[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]にポリシーを適用するために、[Datacenter_VM]グループに先ほどインポートした[仮想マシン用ポリシー]を適用することになります。手順は以下のとおりです。

1. 画面右上の[運用]をクリック
2. ツリービューで対象グループ（ここでは[Datacenter_VM]）をクリック
3. [設定]メニューの[プロパティ]をクリック
4. [全般]タブをクリック
5. [ポリシー名#1]のドロップダウンリストで適用するポリシー（ここでは[仮想マシン用ポリシー]）を選択
6. 右下の[適用]をクリック後、[戻る]をクリック

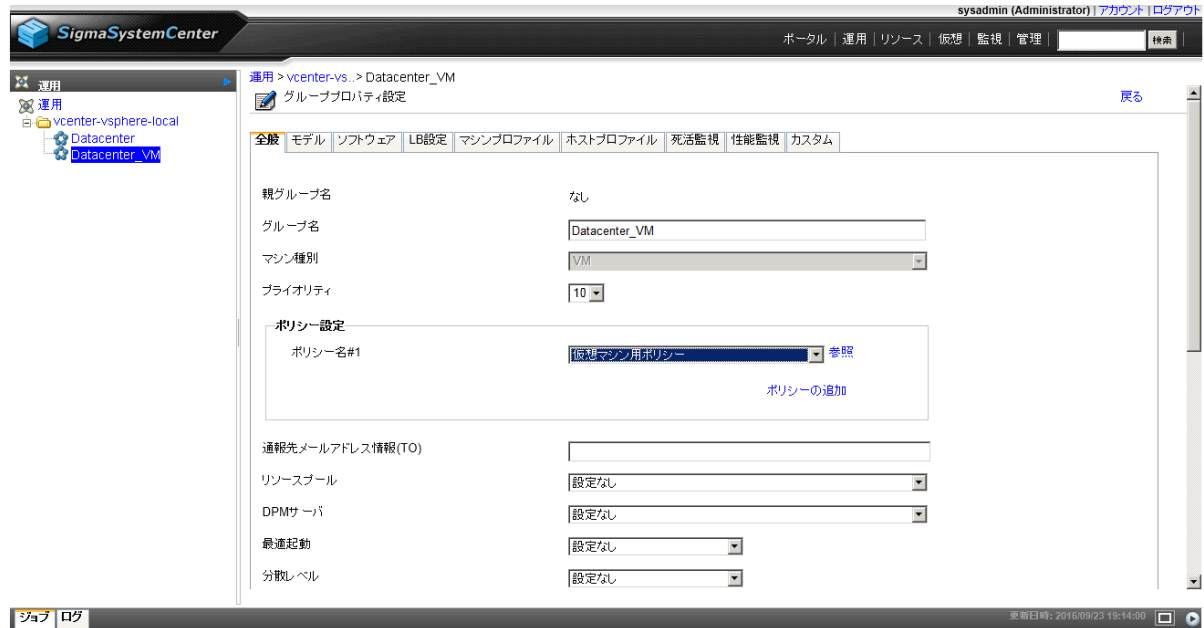


図 仮想マシン用ポリシーの適用

以上で仮想マシンへのポリシー適用は終了です。

8.4.3 物理サーバ用ポリシーの確認と適用

仮想マシンの次は、物理サーバである ESXi 用のポリシーを用意します。物理サーバのグループ（[Datacenter]グループ）にも仮想マシン用ポリシーと同様に、先ほどインポートしたポリシーを適用します。

(1)物理サーバ用のポリシーの確認

仮想マシン用と同様に、ポリシーを適用する前にどのようなルールが定義されているのかを確認します。[管理]ビューを開いたらツリービューにある[ポリシー]をクリックし、[ポリシー一覧]を表示させます。

物理サーバである ESXi 用にインポートしたポリシーは、[仮想マシンサーバ用ポリシー (VMware)]です。[仮想マシンサーバ用ポリシー (VMware)]の[プロパティ]アイコンをクリックして「ポリシープロパティ設定」画面を開き[ポリシー規則]タブをクリックします。

[ポリシー規則一覧]の枠の[状態]が[有効]になっているイベントに注目します。

[仮想マシンサーバ用ポリシー (VMware)]では大まかに次の考えに基づいた設定がデフォルトとなっています。

- ・ イベント発生時点、ESXi が機能停止している可能性が高い障害

対処として、故障マーク設定、通報、イベントログ出力を行った上で、ESXi が停止していない可能性もあるため、ESXi と仮想マシンをシャットダウン（できない場合は強制停止）します。その後、別の ESXi で仮想マシンの再起動（Failover）を行います。

「VMS アクセス不可」、「ファン/冷却装置異常(復旧不能)」、「電圧異常(復旧不能)」、「筐体温度異常(復旧不能)」が該当します。

- イベント発生時点、ESXi が機能停止している障害

対処として、故障マーク設定、通報、イベントログ出力を行った上で、他の ESXi へ仮想マシンを移動し、再起動 (Failover) を行います。

「CPU 温度異常」が該当します。

- イベント発生時点、ESXi は稼働しているが、その後、致命的な障害に陥る可能性がある障害

対処として、故障マーク設定、通報、イベントログ出力を行った上で、他の ESXi へ仮想マシンの移動を行います。まず、移動(Migration(vMotion))により仮想マシンを稼働させたままの移動を試し、移動(Migration)できない場合には続けて再起動 (Failover) を試します。

その後、障害イベントが発生した ESXi を停止させます。

「予兆：〇〇」が該当します。

- イベント発生時点、ストレージに異常がある場合

対処として、故障マーク設定、通報、イベントログ出力を行った上で、他の ESXi へ仮想マシンの移動を行います。まず、移動(Migration(vMotion))により仮想マシンを稼働させたままの移動を試し、移動(Migration)できない場合には、ESXi と仮想マシンをシャットダウン（できない場合は強制停止）し、仮想マシンの再起動 (Failover) を行います。

「ハードディスク障害」が該当します。

- イベント発生時点、ストレージパスの冗長性について低下・喪失がある場合

対処として、故障マーク設定、通報、イベントログ出力のみ行います。障害箇所によっては複数経路でイベントが発生し、状況が複雑になる可能性があります。そのため、単純に仮想マシンを移動する対処では、有効な対処を実行できない可能性が考えられます。また、前述の「予兆：〇〇」のイベントとは異なり、冗長性の低下・喪失が直ちに全パス障害としてストレージパスの接続障害につながる可能性が低いことが考えられます。これらを考慮して、ストレージパスの冗長性の障害については通知の対処のみとします。

「ストレージパス冗長性喪失」、「ストレージパス冗長性低下」が該当します。

ヒント

環境によっては、対処を実施した方がよい場合もあります。必要に応じて以下の設定を行ってください。FC スイッチがなく、ストレージとマシンが直結している環境のような場合は、前述のような懸念がないため、対処を実施しておくことで有効な場合が考えられます。

「ストレージパス冗長性喪失」、「ストレージパス冗長性低下」の「ポリシー規則設定(編集)」画面にて、[イベントに対するアクション]に[VMS 操作/稼働中の VM を移動(Migration, Failover)]のアクションを追加してください。

- イベント発生時点、ハードウェア自身の機能により縮退動作している場合
 対処として、故障マークを設定、通報、イベントログ出力を行います。
 「CPU 障害」、「メモリ縮退障害」が該当します。
- イベント発生時点、経過を観察する判断になる障害、効果的な対応処置がない障害
 対処として、故障マークを設定、通報、イベントログ出力を行います。
 「メモリ障害」が該当します。
- ESXi の負荷が設定した閾値を上回った（下回った）場合
 対処として、通報、イベントログ出力を行います。
 「CPU 使用率（%）異常（回復）」、「メモリ空き容量割合（%）異常（回復）」が該当します。

注

vCenter 上で vSphere HA を利用する設定をしている ESXi に対しては、SSC から、ESXi の停止/強制停止、仮想マシンの再起動（Failover）のアクションが動作しないようにしてください。障害発生時に双方の復旧処理が競合し、意図しない動作となる可能性があります。

上記のアクションを動作させないようにするためには、次のいずれかの方法があります。

- [運用]ビューのグループのプロパティのポリシー設定で、ESXi の停止/強制停止、仮想マシンの再起動（Failover）のアクションを含むポリシーを設定しない。
- ポリシー規則一覧で、ESXi の停止/強制停止、仮想マシンの再起動（Failover）のアクションを含むポリシー規則を無効に設定する。
- ポリシー規則の設定のアクションの一覧から、ESXi の停止/強制停止、仮想マシンの再起動（Failover）が行われるアクションを削除する。

また、仮想マシンの再起動(Failover)の失敗した後に仮想マシンの移動(Migration)を行うアクションを、仮想マシンの移動(Migration)のみを行うアクションに、以下のように変更する。

- [VMS 操作/ 稼働中の VM を移動(Migration, Failover)] → [VMS 操作/ 稼働中の VM を移動(Migration)]
- [VMS 操作/ 全 VM を移動(Migration, Failover)] → [VMS 操作/ 全 VM を移動(Migration)]

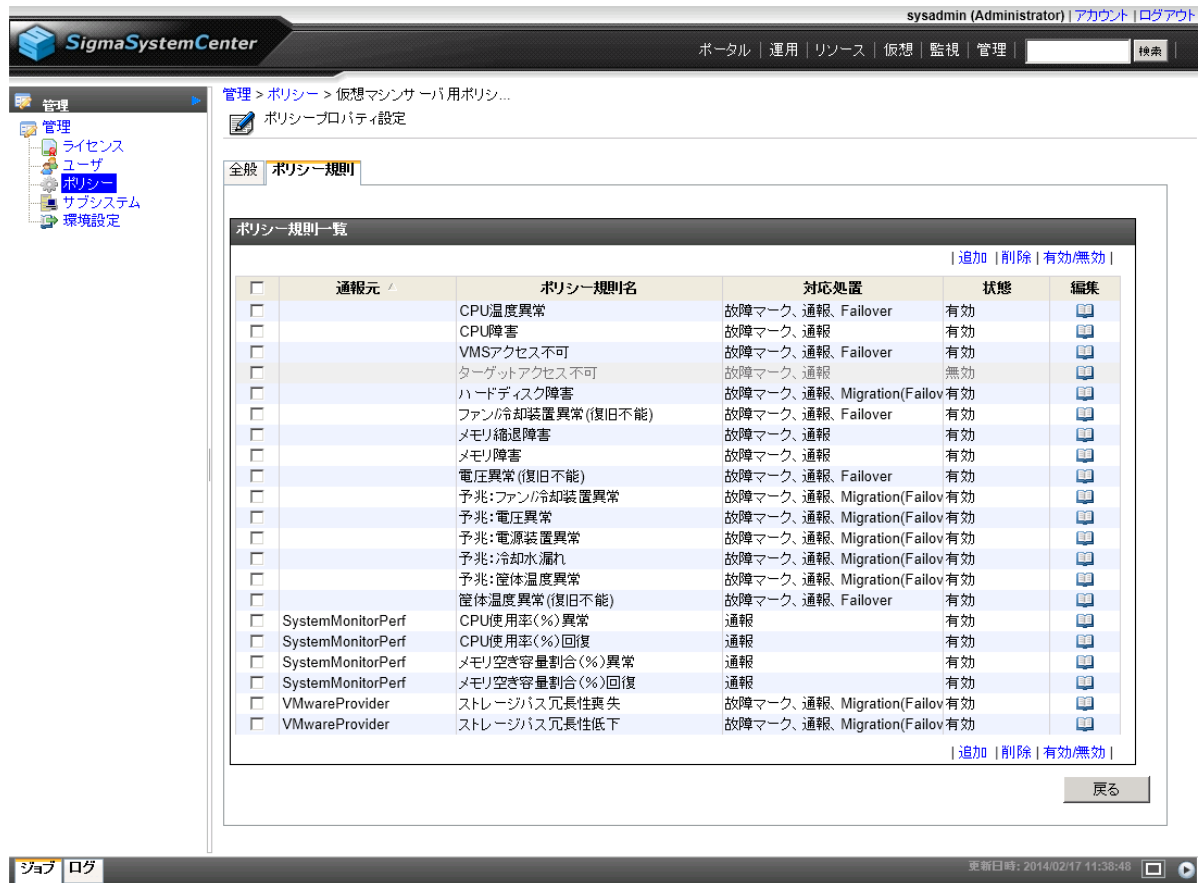


図 仮想マシンサーバ用ポリシー(VMware)の[ポリシー規則]タブ

(2)故障状態の物理サーバの制約と故障状態の解除

物理サーバ(ESXi)に障害が発生すると、先ほどのポリシーが動作して、故障マークが設定された物理サーバ(ESXi)は、下の図のように[ハードウェアステータス]に[故障]と表示されます。



図 障害発生後の物理サーバの詳細情報 ([リソース]ビュー)

故障状態になった ESXi では、仮想マシンを新たに起動できないように SSC の動作が制限されます。故障状態になった ESXi は、移動(Migration(vMotion))や再起動(Failover)による仮想マシンの移動先とすることもできません。

まず、ESXi で発生した障害を解消する必要がありますが、さらに、故障状態を解除して、ESXi を通常の運用で利用できるようにする必要があります。

SSC で故障状態を解除するためには、次の操作を行います。

1. 画面右上の[リソース]をクリックします。
2. [リソース]ビューが表示されたら、ツリービューで、故障マークがついている ESXi をクリックします。
3. ESXi の詳細画面が表示されたら、中央の[マシンステータス情報]の枠の[ハードウェアステータス]の[(状態詳細)]をクリックします。
4. 状態詳細画面が表示されたら、[状態一覧]の枠の[状態]が[正常]以外のステータス名のチェックボックスをチェックし、右上の[リセット(正常)]をクリックします。
5. 再び、ツリービューで、故障マークがついている ESXi をクリックします。
6. 左側の[操作]メニューの[故障状態の解除]をクリックします。

SSC では自動的に故障状態を解除するポリシーを設定することもできますが、管理者が ESXi に問題ないことを実際に確認した上で、手動で故障状態を解除することをお勧めします。

(3)物理サーバ用のポリシーの適用

次に、仮想マシンと同様に[運用]ビューの「グループプロパティ設定」画面でポリシーの適用作業を行います。

[esxi1]、[esxi2]にポリシーを適用するために、[Datacenter]グループに先ほどインポートした[仮想マシンサーバ用ポリシー(VMware)]を適用することにします。手順は以下のとおりです。

1. 画面右上の[運用]をクリックします。
2. ツリービューで対象グループ（ここでは[Datacenter]）をクリックします。
3. [設定]メニューの[プロパティ]をクリックします。
4. [全般]タブをクリックします。
5. [ポリシー名#1]のドロップダウンリストで適用するポリシー、ここでは[仮想マシンサーバ用ポリシー(VMware)]を選択します。
6. [適用]をクリック後、[戻る]をクリックします。



図 物理サーバへのポリシー適用

8.5 動作テスト(擬似障害テスト)

ポリシーを適用したところで、動作テストを行ってみます。今回は物理サーバ[esxi1]に擬似的なストレージ障害を発生させることで、[仮想マシンサーバ用ポリシー(VMware)]の[ハードディスク障害]イベントへの対応処置をテストします。

「ハードディスク障害」イベントの対応処置は、故障マーク設定、通報、イベントログ出力、そして、仮想マシンの他の ESXi への移動(Migration)です。テストでは、SSC の Web コンソー

ルで擬似障害を発生させた物理サーバ[esxi1]に故障マークが付き、[esxi1]上の仮想マシンが他の ESXi に移動されることを確認します。

注

「8.4.3 物理サーバ用ポリシーの確認と適用 (80 ページ)」では、上記の仮想マシンの他の ESXi への移動(Migration)が失敗した場合は、物理サーバ[esxi1]と仮想マシンをシャットダウン（できない場合は強制停止）し、仮想マシンの再起動（Failover）を行うことも説明しましたが、今回のテストでは、ハードディスク障害発生後も物理サーバ[esxi1]が停止しておらず、移動(Migration)が成功する状況を想定したテストを実施します。

より深刻な状況については、擬似的に簡易に障害状況を作り出して実施することが難しいため、説明を省略します。

まず、Web サイトから[擬似イベント発生ツール]の圧縮ファイルをダウンロードし、管理サーバの任意のフォルダに解凍・保存します。今回は、<C:¥temp>に保存したとします。

Windows の[スタート]メニューから[Windows システムツール]→[コマンドプロンプト]をクリックします。コマンドプロンプトが起動したら、次のようにカレントディレクトリを<C:¥temp>に移動します。

```
> cd ¥temp
```

次に、<C:¥temp>内に保存した[擬似イベント発生ツール(sendevent.exe)]を次のように実行します。

```
> ssc sendevent VMwareProvider "Storage path is all down" -group  
vcenter-vsphere-local¥Datacenter esxi1 -message "Storage path is all down"
```

障害がどのように見えるか確認しましょう。

まず、画面右上の[運用]をクリックし、[運用]ビューを開きます。ツリービューの[Datacenter]グループに故障マーク(赤い×アイコン)が付いているのが確認できますので、[Datacenter]グループをクリックします。

[全般]タブの[ホスト一覧]の枠を見ると、[esxi1]が[故障]状態であることが分かります。



図 障害発生時の[運用]ビュー

[ホスト一覧]の枠の[esxi1]のリソース[esxi1.vsphere.local]をクリックし、リソースの状態を確認してみます。

下の図のように[リソース]ビューでリソース[esxi1.vsphere.local]の状態が表示されます。[マシンステータス情報]の枠を見ると、やはり[故障]であることが分かります。



図 障害発生時の[リソース]ビュー

さらに、[運用情報]の枠の[仮想パス]の[virtual:/vcenter.vsphere.local/Datacenter/esxi1.vsphere.local]をクリックし、[仮想]ビューを確認してみます。

下の図のように、[仮想]ビューのツリービュー上でも[esxi1.vsphere.local]に故障マークが表示され、故障状態にあることが分かります。さらに、各 ESXi のツリーを展開すると、[esxi1.vsphere.local]の配下にあった[VM-01]が別の ESXi の配下に移動していることが分かります。

ちなみに、擬似障害の投入直後の仮想マシンの移動が完了していない場合、[esxi1.vsphere.local]の配下に[VM-01]が残っていることがあります。その場合は、しばらく時間をおいてから右側[操作]メニューの[画面更新]をクリックし、仮想マシンが移動したことを確認してください。

また、各 ESXi で稼動している仮想マシンの一覧は、中央の[稼動中 VM 一覧]の枠でも見ることができます。



図 障害発生時の[仮想]ビュー

次に、[esxi1.vsphere.local]の[運用情報]の枠の[ハードウェアステータス]の[(状態詳細)]をクリックしてみます。

[esxi1.vsphere.local]の[状態詳細]が表示され、[状態一覧]の枠の[ストレージ接続性]の状態が[故障]となっていることが分かります。



図 [esxi1.vsphere.local]の状態一覧の画面

テストの確認が終了しましたので、最後に、[仮想]ビューで故障状態を解除し、[esxi1.vsphere.local]の配下に戻すために[VM-01]と[VM-02]を移動します。

ツリービューの[esxi1.vsphere.local]をクリックし、[esxi1.vsphere.local]を選択状態にします。左の[操作]メニューから[故障状態の解除]をクリックすると、故障状態がクリアされ、ステータスが[正常]に変わります。

次に、[esxi1.vsphere.local]の配下への仮想マシンの移動(Migration(vMotion))を行います。

「5.5 手動での仮想マシンの移動(Migration(vMotion)) (26 ページ)」に記載の方法でも可能ですが、今回は、タイムライン機能を利用して行ってみましょう。

タイムライン機能では、運用グループ内のマシンの状態や仮想マシンの配置に関する過去からの経過の情報がわかりやすく表示されます。

今回のテストでの障害の発生タイミングや障害前後の仮想マシンの配置も、簡単に確認することができます。また、過去の仮想マシンの配置に1度の操作で簡単に元に戻すことが可能です。

まず、[運用]ビューのツリービューにある[Datacenter]をクリックした後、[タイムライン]タブをクリックして、タイムライン画面を表示します。

今回のテストにおける変更の履歴を確認するために、画面の上側にあるタイムラインの表示部でマウスのスクロールボタン（ホイール）によるスクロールを行ったり、[拡大]のアイコンをクリックしたりして、表示期間を拡大して次の画面のように表示します。

前述で説明しました[esxi1.vsphere.local]に対して、[故障状態の解除]を実行した後の状態が表示されています。

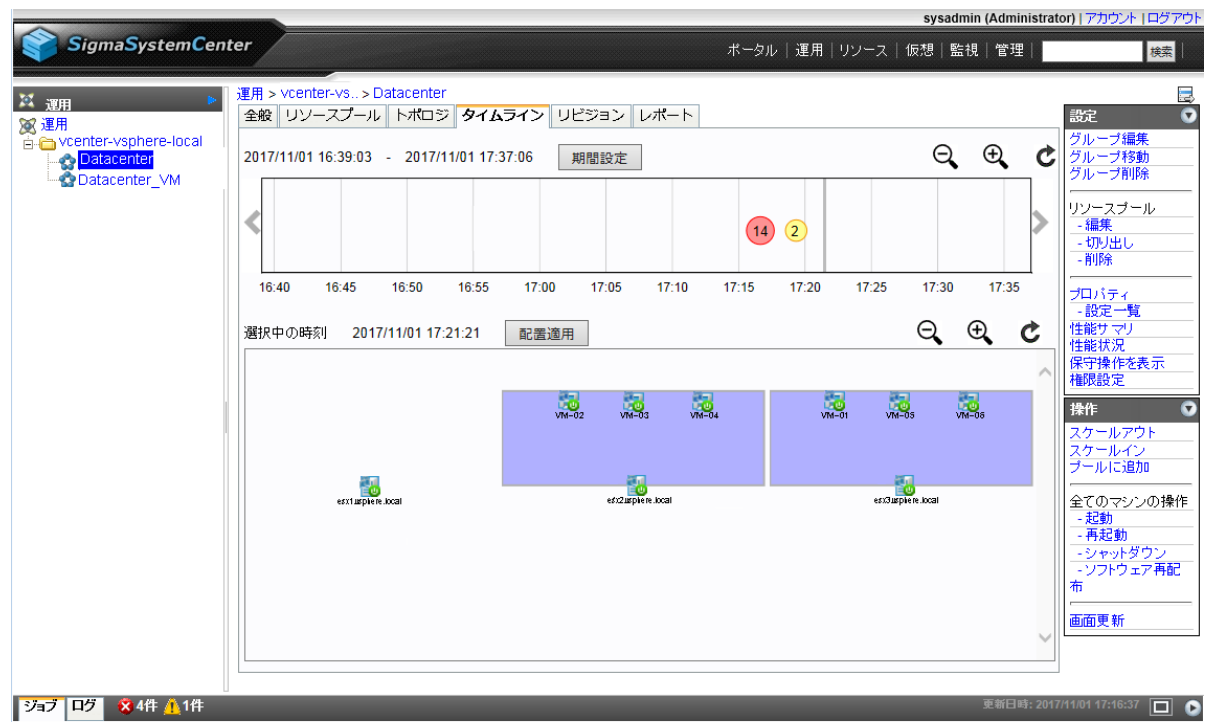


図 [esxi1.vsphere.local]の故障状態を解除した後の仮想マシンの配置

履歴の詳細は、以下のように確認することができます。

- 前述の図中に表示されている数字が 14 の赤丸には、擬似障害のイベントや仮想マシンの移動などの対応処置による状態変更が含まれます。

赤丸にマウスカーソルをあわせて右クリックすると次の履歴の一覧が表示されます。

状態履歴一覧				
履歴数		14 (異常:[2],警告:[1])		
詳細	イベント(ジョブ)	発生日時	マシン	メッセージ
14	RE378301	2017/11/01 17:16:21		Storage path is all down
	RE378301	2017/11/01 17:16:21	esxi1.vsphere.local	Storage path is all down
	RE378301 (00194-01)	2017/11/01 17:16:21	esxi1.vsphere.local	マシン設定/ステータス設定故障
	RE378301 (00194-01)	2017/11/01 17:16:21	VM-01	マシン設定/ステータス設定故障
	RE378301 (00194-01)	2017/11/01 17:16:21	VM-02	マシン設定/ステータス設定故障
	RE378301 (00194-02)	2017/11/01 17:16:25	esxi1.vsphere.local	VMS操作/全VMを移動(Migration)
	RE378301 (00194-02)	2017/11/01 17:16:26	esxi1.vsphere.local	VMS操作/全VMを移動(Migration)

- 前述の図中に表示されている数字が 2 の黄丸には、[esxi1.vsphere.local]の故障状態解除による状態変更が含まれます。

黄丸にマウスカーソルをあわせて右クリックすると次の履歴の一覧が表示されます。

状態履歴一覧				
履歴数		2 (異常:[0],警告:[1])		
詳細	イベント(ジョブ)	発生日時	マシン	メッセージ
2	UC378323	2017/11/01 17:19:20	esxi1.vsphere.local	故障状態の解除
	UC378323	2017/11/01 17:19:20	esxi1.vsphere.local	故障状態の解除
	UC378323	2017/11/01 17:19:20	esxi1.vsphere.local	故障状態の解除

次に、タイムラインの表示部上で数字が 14 の赤丸より前の日時をクリックすると、次の画面のように擬似障害テストを実施する前の[Datacenter]グループの仮想マシンの配置が表示されます。

この画面から、次の操作を行うと擬似障害テスト実施前の仮想マシンの配置に戻すことができます。

- [配置適用]をクリック
- 移動確認のダイアログが表示されたら、[OK]をクリック

仮想マシンが移動する時間をしばらく待ち、[仮想]ビュー上のツリービューなどで[esxi1.vsphere.local]に[VM-01]と[VM-02]が移動したことを確認します。仮想マシンの移動がツリービューに反映されていない場合は[操作]メニューの[画面更新]をクリックしてみてください。



図 擬似障害テスト前の仮想マシンの配置

付録 A. 運用に関する重要な情報

仮想マシンサーバと仮想マシンの操作

以下のような仮想マシンサーバと仮想マシンについての操作は SSC で実施し、vCenter Server や仮想マシンサーバ、および仮想マシン上の OS から直接実施しないでください。

- 電源の On/Off
- ハイパーバイザーや OS のシャットダウン

上記の操作を SSC 外で行った場合、以下の影響があります。

- 仮想マシンサーバや仮想マシンの実際の状態と SSC の収集した状態との間にずれが生じる場合がある。

さらに、SSC からこの状態のずれが生じている仮想マシンサーバや仮想マシンの操作を行った場合、その操作が失敗することもあります。

実際のマシンの状態と SSC の収集した状態との間にずれが生じた場合や、ずれが原因で操作が失敗した場合は、「マシンの状態のずれを解消する」の対処を行ってください。

- 死活監視のイベントにより、SSC が障害と認識し、ポリシーの処理が動作してしまう。

SSC が認識していない状態でマシンの停止が行われた場合、死活監視のイベントが発生し、ポリシーで設定されているイベントに対応する処理が動作してしまいます。

ポリシーの影響がでないように操作するためには、事前に SSC 上で対象マシンについてメンテナンスモードの設定をしておく必要があります。

マシンの状態のずれを解消する

仮想マシンサーバや仮想マシンの実際の状態と SSC の収集した状態との間にずれを解消するには、以下のように[仮想]ビューで仮想マシンサーバの状態の収集を行います。

- 画面右上の[仮想]をクリック

ツリービューで、ずれが生じている仮想マシンサーバ (ESXi)、または、ずれが生じている仮想マシンが稼動している仮想マシンサーバ (ESXi) を選択

- [操作]メニューの[収集]をクリック

マシンの状態のずれが原因で SSC の操作が失敗していた場合は、マシンの状態の収集を行った後でもう一度失敗した操作を行います。

付録 B. 負荷状況取得の設定

管理対象マシンの負荷状況の取得の設定について説明します。

SSC は管理対象マシンの負荷状況を時系列のグラフとして Web コンソール上に表示し、閾値によって監視することができます。また、レポート表示のために取得した負荷状況のデータを蓄積することができます。

ここでは負荷データの取得の設定の説明のみ行います。閾値による監視の設定方法については、「[8.2 負荷監視の設定 \(65 ページ\)](#)」で説明します。

管理対象マシンの負荷状況の取得を行う場合、監視プロファイルを準備して、運用グループに割り当てることで、負荷状況閲覧が可能となります。

監視プロファイルとは、性能情報の監視項目、監視間隔、閾値などの設定を含む、性能監視設定のセットです。

SSC では、一般的な監視項目が既に設定済みの監視プロファイルをあらかじめ用意しています。

本書の利用方法の場合、以下の監視プロファイルが各グループに自動で設定されます（「[5.1 サブシステムの登録 \(12 ページ\)](#)」を参照）が、本節では、明示的に手動で設定する場合の設定方法について説明します。

- ESXi グループ: [Builtin](For Report)VM Server Monitoring Profile (5min)
- 業務 VM グループ: [Builtin](For Report)VM Monitoring Profile[Hypervisor] (5min)

ヒント

仮想マシンで使用する上記の[Builtin](For Report)VM Monitoring Profile[Hypervisor] (5min)は、負荷情報を取得対象の仮想マシンが動作する ESXi から取得します。

その他、仮想マシン上のゲスト OS から取得する[Builtin](For Report)VM Monitoring Profile[VM OS] (5min)があります。

ESXi 経由でもゲスト OS 経由でも基本的に同様の性能データを取得できますが、それぞれ視点が異なるため、若干取得できる情報の傾向が異なります。

- ESXi 経由([Builtin](For Report)VM Monitoring Profile[Hypervisor])

ESXi の視点で ESXi が仮想マシンに割り当てたリソースの情報が取得できます。また、ESXi 経由でまとめてデータを取得することができるため、比較的低負荷で処理を行うことができます。管理するマシンが多い大規模な環境では処理負荷が少ない本プロファイルの利用を推奨します。

また、ゲスト OS 経由の場合、仮想マシン単位で設定を行う必要がありますが、本プロファイルの場合、ESXi の設定のみで簡易に設定することが可能です。

[VMware vCenter Server]のサブシステムで[マシンを運用グループへ自動登録する]と[マシンの性能監視を有効にする]のチェックをオンにした場合、本プロファイルが自動設定されます。

- ゲスト OS 経由([Builtin](For Report)VM Monitoring Profile[VM OS])

ゲスト OS の視点でゲスト OS 上の使用リソースの情報が取得できます。特に、空きメモリ容量の情報について、業務アプリケーションの使用状況を正確に確認したい場合は本プロファイルを利用してください。

アカウントやファイアウォールの設定など監視プロファイル以外の設定が別途必要です。

ゲスト OS 経由で取得する方法については、「[B.2.2 ゲスト OS 経由での負荷状況取得の設定 \(99 ページ\)](#)」を参照してください。

監視プロファイルの一覧の確認は、[リソース]ビュー（画面右上の[リソース]をクリック）で行います。[リソース]ビューを開いたら、ツリービューから[監視プロファイル]を選択します。用意されている監視プロファイルの一覧が表示されます。

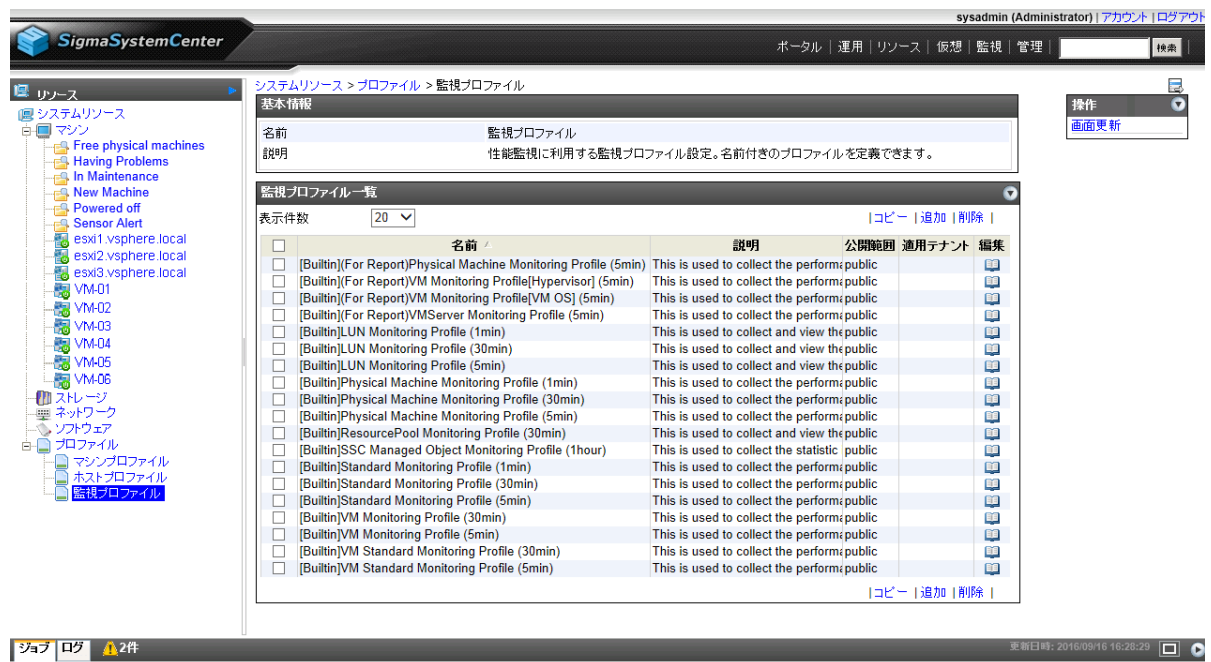


図 監視プロファイル一覧

B.1 物理サーバの負荷状況取得の設定

物理サーバ（ESXi）の負荷監視に必要な設定について説明します。

ヒント

[VMware vCenter Server]のサブシステムで[マシンを運用グループへ自動登録する]と[マシンの性能監視を有効にする]のチェックをオンにした場合、以下の設定が自動で登録されます。

- 性能データ収集設定：チェックする
- プロファイル名：[Builtin](For Report)VM Server Monitoring Profile (5min)
- IP アドレス：127.0.0.1
- ポート番号：26200

アカウントとパスワードの設定は、以下の設定が記載の優先順で使用されます。本節の説明の[性能監視]タブの画面で設定されている場合は[性能監視]タブの設定が使用されます。

- 「環境設定」の[仮想リソース]タブの root パスワード設定
- 「サブシステム一覧」画面の各 ESXi の個別の root パスワード設定

B.1.1 物理サーバ上の設定

SSC では、ESXi の負荷状況を取得するために、ESXi に直接アクセスして情報を取得します。ESXi にアクセスするには、十分な権限を持ったアカウントが ESXi 上に準備されている必要があります。負荷状況を取得するためのアカウントとして root を利用できますので、ESXi に対して追加の設定は不要です。

B.1.2 ESXi の運用グループの設定

SSC が ESXi の負荷状況を取得するための設定を[運用]ビュー（画面右上の[運用]をクリック）で行います。[運用]ビューを開いたら、ツリービューから設定対象の運用グループである[Datacenter]をクリックします。ESXi の性能監視設定を行うには、[設定]メニューにある[プロパティ]をクリックして「グループプロパティ設定」画面を開き、[性能監視]タブに移動します。[性能監視]タブの各項目は、以下のように入力し、[適用]をクリックします。

- 性能データ収集設定：チェックする
- プロファイル名：[Builtin](For Report)VMServer Monitoring Profile (5min)
- IP アドレス：127.0.0.1（変更しません）
- ポート番号：26200（変更しません）
- アカウント：root
- パスワード更新：チェックする
- パスワード：ESXi の root のパスワード

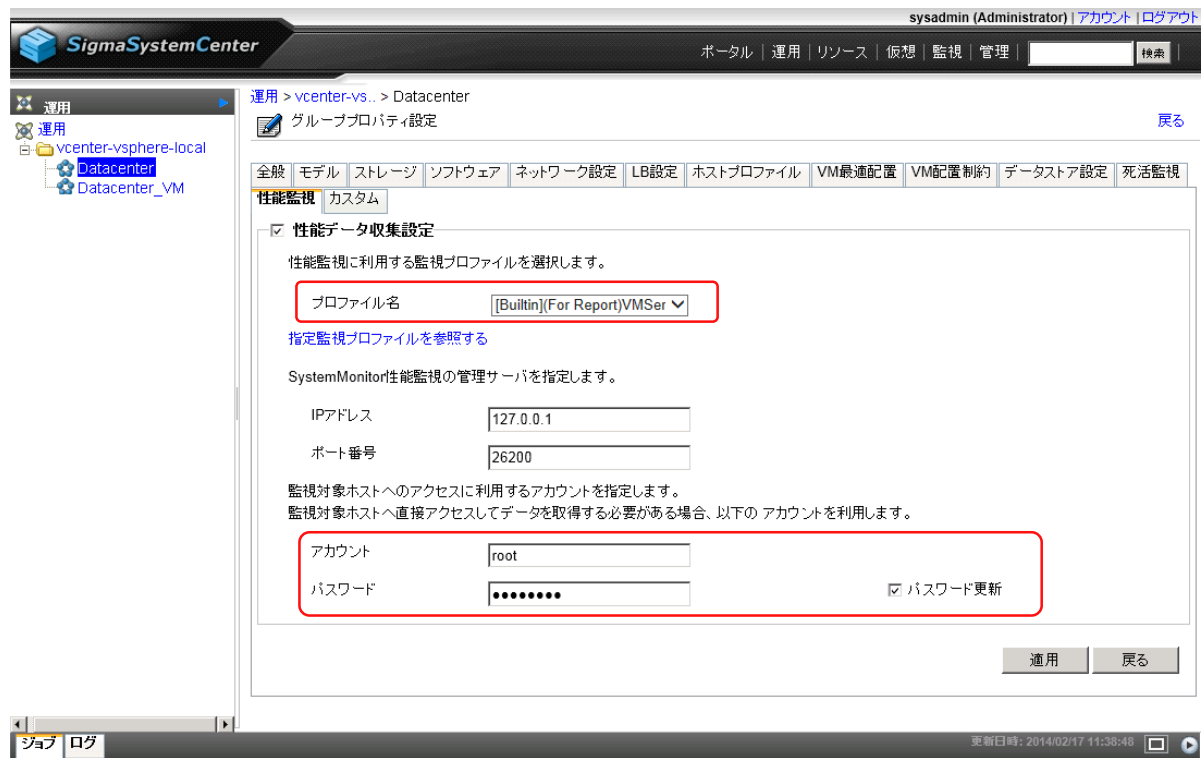


図 [Datacenter]グループの[性能監視]タブ

B.2 業務用仮想マシンの負荷状況取得の設定

業務用仮想マシンの負荷状況取得に必要な設定について説明します。

- ESXi 経由での負荷状況取得の設定(デフォルト)
- ゲスト OS 経由での負荷状況取得の設定

ヒント

[VMware vCenter Server]のサブシステムで[マシンを運用グループへ自動登録する]と[マシンの性能監視を有効にする]のチェックをオンにした場合、以下の設定が自動で登録されます。

- 性能データ収集設定：チェックする
- プロファイル名：[Builtin](For Report)VM Monitoring Profile[Hypervisor] (5min)
- IP アドレス：127.0.0.1
- ポート番号：26200

アカウントとパスワードの設定は、以下の設定が記載の優先順で使用されます。本節の説明の[性能監視]タブの画面で設定されている場合は[性能監視]タブの設定が使用されます。

- 「環境設定」の[仮想リソース]タブの root パスワード設定
- 「サブシステム一覧」画面の各 ESXi の個別の root パスワード設定

※監視プロファイルの指定を ESXi 経由([Builtin](For Report)VM Monitoring Profile[Hypervisor])からゲスト OS 経由([Builtin](For Report)VM Monitoring Profile[VM OS])に変更した場合は上記の root パスワード設定は使用されません。

B.2.1 ESXi 経由での負荷状況取得の設定

本節では、仮想マシンの負荷状況について、ESXi 経由での負荷状況取得の設定の方法を説明します。

(1)仮想マシン上の設定

使用する監視プロファイル[Builtin](For Report)VM Monitoring Profile[Hypervisor] (5min) は、ゲスト OS の負荷状況を取得するために、仮想マシンが動作する ESXi にアクセスして情報を取得します。そのため、仮想マシンの設定は不要です。

(2)業務用仮想マシンの運用グループの設定

SSC が Windows サーバの負荷状況を取得するための設定を[運用]ビュー（画面右上の[運用]をクリック）で行います。[運用]ビューを開いたら、ツリービューから設定対象の運用グループである[Datacenter_VM]をクリックします。業務用仮想マシンの性能監視設定を行うには、[設定]メニューにある[プロパティ]をクリックしてグループの「プロパティ設定」画面を開き、[性能監視]タブに移動します。[性能監視]タブの各項目は、以下のように入力し、[適用]をクリックします。

- 性能データ収集設定：チェックする
- プロファイル名：[Builtin](For Report)VM Monitoring Profile[Hypervisor] (5min)
- IP アドレス：127.0.0.1（変更しません）
- ポート番号：26200（変更しません）
- アカウント：(設定しません)
- パスワード更新：チェックしない(設定しません)

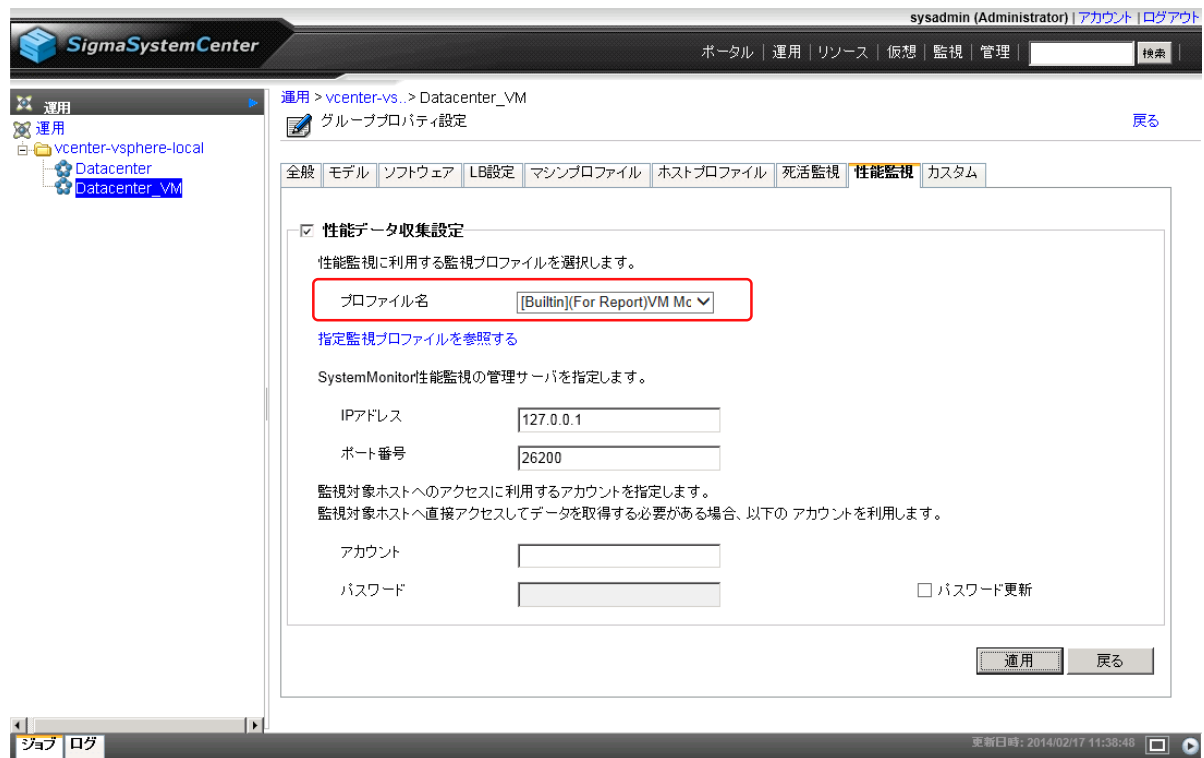


図 [Datacenter_VM]グループの[性能監視]タブ

B.2.2 ゲスト OS 経由での負荷状況取得の設定

本節では、仮想マシンの負荷状況について、ゲスト OS 経由での負荷状況取得の設定の方法を説明します。

(1)仮想マシン上の設定

SSC では、ゲスト OS（Windows Server 2016）の負荷状況を取得するために、ゲスト OS に直接アクセスして情報を取得します。仮想マシン上で動作しているゲスト OS にアクセスするには、十分な権限を持ったアカウントがゲスト OS 上に準備されている必要があります。Windows サーバから負荷状況を取得するためのアカウントとして Administrator を利用できますので、Administrator アカウントが有効であれば Windows サーバに対してアカウントの追加は不要です。（デフォルトでは Administrator アカウントは有効です。）

また、ゲスト OS の負荷状況を取得するためには、管理サーバからゲスト OS へ通信できるようにゲスト OS 上の Windows ファイアウォールの設定を変更する必要があります。[VM-01]に管理者権限を持つアカウントでログオンしてください。

ログオン後、Windows の[スタート]メニューから[Windows 管理ツール]→[セキュリティが強化された Windows ファイアウォール]をクリックします。左のツリーで[受信の規則]を選択し、以下の規則について、接続を許可します。

- ファイルとプリンターの共有（SMB 受信）

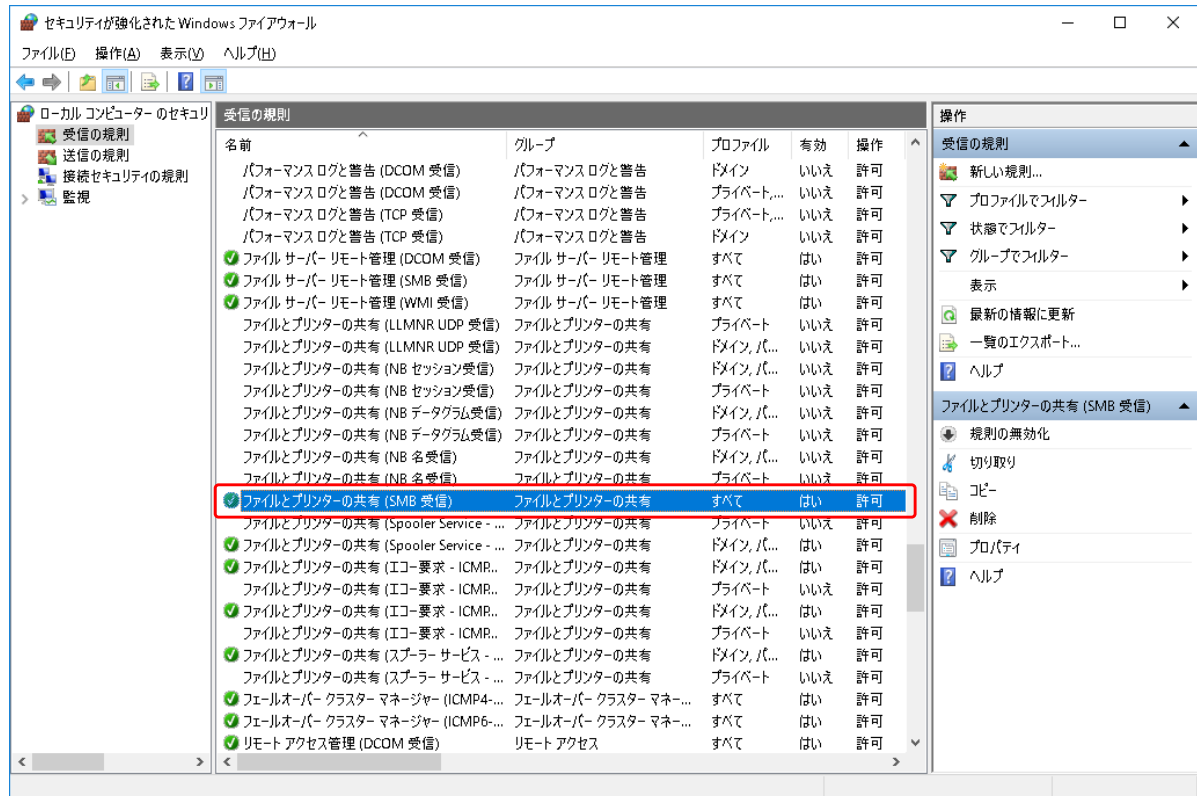


図 セキュリティが強化された Windows ファイアウォール

[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]についても同様の設定を行います。

(2)業務用仮想マシンの運用グループの設定

SSC が Windows サーバの負荷状況を取得するための設定を[運用]ビュー（画面右上の[運用]をクリック）で行います。[運用]ビューを開いたら、ツリービューから設定対象の運用グループである[Datacenter_VM]をクリックします。業務用仮想マシンの性能監視設定を行うには、[設定]メニューにある[プロパティ]をクリックしてグループの「プロパティ設定」画面を開き、[性能監視]タブに移動します。[性能監視]タブの各項目は、以下のように入力し、[適用]をクリックします。

- 性能データ収集設定：チェックする
- プロファイル名：[Builtin](For Report)VM Monitoring Profile[VM OS] (5min)
- IP アドレス："127.0.0.1"（変更しません）
- ポート番号："26200"（変更しません）
- アカウント："Administrator"
- パスワード更新：チェックする
- パスワード：Windows サーバの Administrator のパスワード

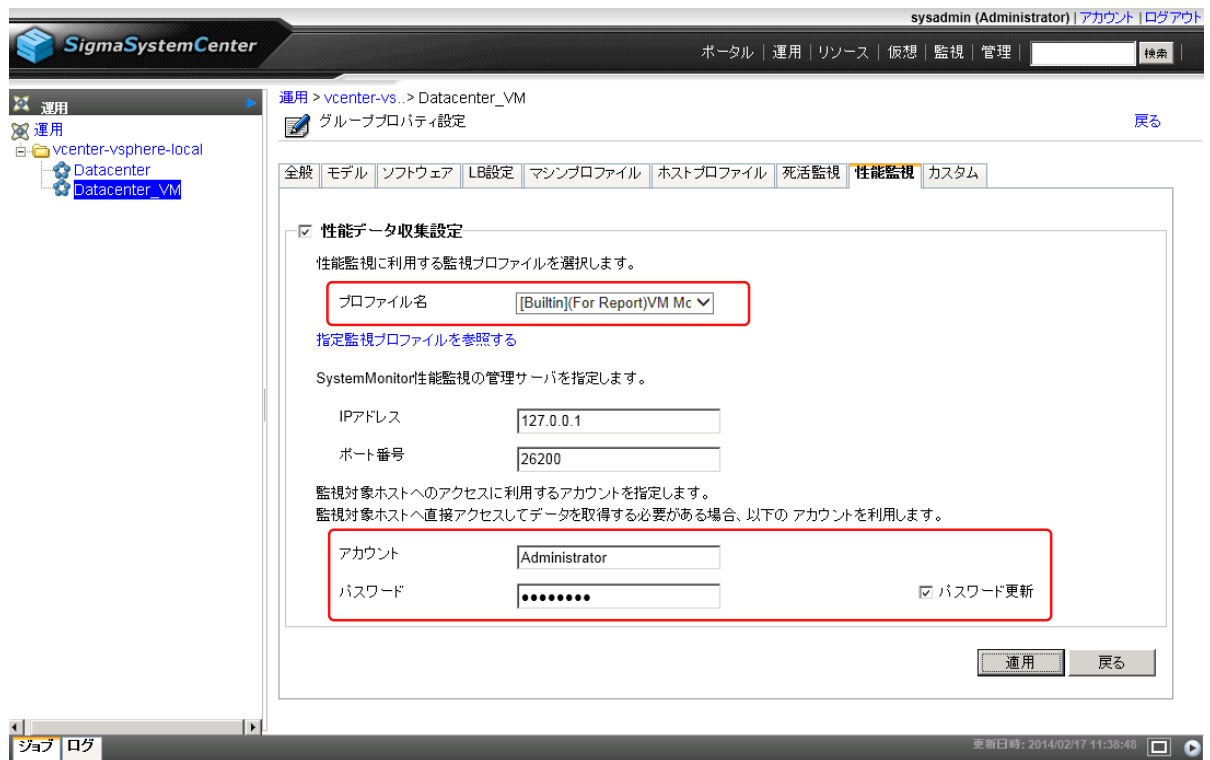


図 [Datacenter_VM]グループの[性能監視]タブ

付録 C. SigmaSystemCenter マニュアル体系

SigmaSystemCenter のマニュアルは、各製品、およびコンポーネントごとに以下のように構成されています。

また、本書内では、各マニュアルは「本書での呼び方」の名称で記載します。

製品 / コンポーネント名	マニュアル名		本書での呼び方
WebSAM SigmaSystemCenter 3.8	WebSAM SigmaSystemCenter 3.8 ファーストステップガイド		SigmaSystemCenter ファーストステップガイド
	WebSAM SigmaSystemCenter 3.8 インストレーションガイド		SigmaSystemCenter インストレーションガイド
	WebSAM SigmaSystemCenter 3.8 コンフィグレーションガイド		SigmaSystemCenter コンフィグレーションガイド
	WebSAM SigmaSystemCenter 3.8 リファレンスガイド	-	SigmaSystemCenter リファレンスガイド
		データ編	SigmaSystemCenter リファレンスガイド データ編
		注意事項、トラブルシューティング編	SigmaSystemCenter リファレンスガイド 注意事項、トラブルシューティング編
		Web コンソール編	SigmaSystemCenter リファレンスガイド Web コンソール編
SystemMonitor 性能監視 5.12	SystemMonitor 性能監視 5.12 ユーザーズガイド		SystemMonitor 性能監視 ユーザーズガイド

ヒント

SigmaSystemCenter のすべての最新のマニュアルは、以下の URL から入手できます。

<https://jpn.nec.com/websam/sigmasystemcenter/index.html>

→ 「ダウンロード」

SigmaSystemCenter の製品概要、インストール、設定、運用、保守に関する情報は、以下の4つのマニュアルに含みます。各マニュアルの役割を以下に示します。

「SigmaSystemCenter ファーストステップガイド」

SigmaSystemCenter を使用するユーザを対象読者とし、製品概要、システム設計方法、動作環境などについて記載します。

「SigmaSystemCenter インストレーションガイド」

SigmaSystemCenter のインストール、アップグレードインストール、およびアンインストールを行うシステム管理者を対象読者とし、それぞれの方法について説明します。

「SigmaSystemCenter コンフィグレーションガイド」

インストール後の設定全般を行うシステム管理者と、その後の運用・保守を行うシステム管理者を対象読者とし、インストール後の設定から運用に関する操作手順を実際の流れに則して説明します。また、保守の操作についても説明します。

「SigmaSystemCenter リファレンスガイド」

SigmaSystemCenter の管理者を対象読者とし、「SigmaSystemCenter インストレーションガイド」、および「SigmaSystemCenter コンフィグレーションガイド」を補完する役割を持ちます。

SigmaSystemCenter リファレンスガイドは、以下の 4 冊で構成されています。

- 「SigmaSystemCenter リファレンスガイド」
SigmaSystemCenter の機能説明などを記載します。
- 「SigmaSystemCenter リファレンスガイド データ編」
SigmaSystemCenter のメンテナンス関連情報などを記載します。
- 「SigmaSystemCenter リファレンスガイド 注意事項、トラブルシューティング編」
SigmaSystemCenter の注意事項、およびトラブルシューティング情報などを記載します。
- 「SigmaSystemCenter リファレンスガイド Web コンソール編」
SigmaSystemCenter の操作画面一覧、および操作方法などを記載します。

付録 D. 改版履歴

版数	年月	改版内容
第 1 版	2019.08	新規作成
第 1.1 版	2019.12	「7.1. 物理サーバの設定」の説明を修正

付録 E. ライセンス情報

本製品には、一部、オープンソースソフトウェアが含まれています。当該ソフトウェアのライセンス条件の詳細につきましては、以下に同梱されているファイルを参照してください。また、GPL / LGPL に基づきソースコードを開示しています。当該オープンソースソフトウェアの複製、改変、頒布を希望される方は、お問い合わせください。

<SigmaSystemCenter インストール DVD>¥doc¥OSS

- PXE Software Copyright (C) 1997 - 2000 Intel Corporation.
- 本製品には、Microsoft Corporation が無償で配布している Microsoft SQL Server Express を含んでいます。使用許諾に同意したうえで利用してください。著作権、所有権の詳細につきましては、以下の LICENSE ファイルを参照してください。

<Microsoft SQL Server Express をインストールしたフォルダ>¥License Terms

- Some icons used in this program are based on Silk Icons released by Mark James under a Creative Commons Attribution 2.5 License. Visit <http://www.famfamfam.com/lab/icons/silk/> for more details.
- This product includes software developed by Routrek Networks, Inc.
- This product includes NM Library from NetApp, Inc. Copyright 2005 - 2010 NetApp, Inc. All rights reserved.

用語集

英数字

BMC

"Baseboard Management Controller (ベースボードマネジメントコントローラ)" の略です。

CMC

"Chassis Management Controller" の略です。

サーバに搭載されている、システムの状態や OS に依存することなく、ファン、電源とノードの監視機能を提供する IPMI 仕様に準拠した管理用コントローラです。標準で筐体 ボード上に組み込まれています。

DHCP サーバ

DHCP とは、"Dynamic Host Configuration Protocol" の略です。DHCP サーバとは、ネットワークにおいて、コンピュータに動的に IP アドレスを割り当てるための機能を実装したサーバです。DHCP クライアントからの要求により、あらかじめ用意した IP アドレス、サブネットマスク、ドメイン名などの情報を割り当てます。

DPM

"DeploymentManager" の略です。SystemProvisioning からの指示により、管理対象マシンへ OS、アプリケーション、パッチなどのソフトウェアの配布、更新やマシンの起動、停止を行います。

ESMPRO/ServerManager,ESMPRO/ServerAgentService

Express5800 シリーズに標準添付のマシン管理ソフトウェアです。SigmaSystemCenter は、管理対象マシンが物理サーバの場合に ESMPRO/ServerManager を介してマシンを監視します。

ESXi

スタンドアロン環境で仮想マシンを実現できる VMware 社の製品です。

vCenter Server を介して管理することも、SystemProvisioning から直接管理することもできます。SystemProvisioning から直接管理される ESXi を "スタンドアロン ESXi" と呼びます。また、ESXi の管理・運用形態について、vCenter Server を使用した運用を "vCenter Server 環境での運用"、SystemProvisioning から直接管理する運用を "スタンドアロン環境での運用" と呼びます。

IIS

"Internet Information Services" の略で、Microsoft 社が提供するインターネットサーバ用ソフトウェアです。

iLO

"Integrated Lights-Out" の略で、システムボードに内蔵されているリモートサーバ管理プロセッサです。

標準インターフェース仕様の IPMI2.0 に準拠してリモートの場所からサーバを監視および制御できます。

iLO は BMC として機能します。

iLO は Express5800/R120h-2M, R120h-1M 以降のサーバマネージメントチップ iLO 搭載モデルの NEC 製のサーバに搭載されました。

IPMI

"Intelligent Platform Management Interface (インテリジェントプラットフォームマネジメントインターフェース)" の略です。装置に対して、センサ情報の取得、電源操作、装置のログを取得するインターフェースを提供します。

Migration

Migration は、共有ディスク上に存在する仮想マシンを別の仮想マシンサーバに移動します。仮想マシンの電源がオンの場合、稼動状態のままライブマイグレーションします (Hot Migration)。仮想マシンの電源がオフの場合は、電源オフの状態のまま移動します (Cold Migration)。電源オンの状態の仮想マシンをサスペンド状態にして移動させる方法は、Quick Migration と呼びます。

OOB

"Out-of-Band (アウトオブバンド)" の略です。ハードウェア上で動作しているソフトウェアとの通信ではなく、直接ハードウェアに対して管理、操作を行う管理方法です。

PET

"Platform Event Trap" の略です。

BIOS やハードウェアで発生したイベントを、SNMP トラップを利用して BMC などから直接通報するものです。

RMCP/RMCP+

"Remote Management Control Protocol (リモートマネージメントコントロールプロトコル)" の略です。IPMI の命令をリモートからネットワークを介して実行するプロトコルです。UDP を使います。

SNMP Trap (SNMP トラップ)

SNMP (Simple Network Management Protocol、簡易ネットワーク管理プロトコル) における通信で、SNMP エージェントがイベントをマネージャに通知することです。

SQL Server

Microsoft 社が提供している、リレーショナルデータベースを構築・運用するための管理ソフトウェアです。SigmaSystemCenter は、システムの構成情報を格納するデータベースとして SQL Server を使用します。

SystemMonitor 性能監視

マシンリソースの使用状況などを監視する SigmaSystemCenter のコンポーネントです。性能障害発生時には SystemProvisioning に通報することも可能です。

SystemProvisioning

SigmaSystemCenter の中核となるコンポーネントです。管理対象マシンの構築、構成情報の管理、構成変更、マシン障害時の自律復旧などを行います。

SSC

SigmaSystemCenter の略称です。

SSC 小規模仮想化運用パック

仮想化ホスト 3 台までの小規模仮想化環境を管理するために必要なライセンスをパックにして提供する製品です。VMware 環境、Hyper-V 環境の管理が可能です。

vCenter Server

複数の ESX、およびその上に構成された仮想マシンを統合管理するための VMware 社の製品です。

VM

"Virtual Machine" の略です。仮想マシンと同じです。「仮想マシン」の項を参照してください。

VMS

"Virtual Machine Server" の略です。仮想マシンサーバと同じです。「仮想マシンサーバ」の項を参照してください。

VM サーバ

仮想マシンサーバを指します。

vSphere Client

仮想マシン、および仮想マシンのリソースとホストの作成、管理、監視を行うユーザインターフェースを備えた VMware 社の製品です。

Web コンソール

Web コンソールには、SigmaSystemCenter の Web コンソールと DPM の Web コンソールの 2 種類があります。本書で、Web コンソールと記載している場合、SigmaSystemCenter の Web コンソールを指します。SigmaSystemCenter の Web コンソールは、ブラウザから SigmaSystemCenter の設定や運用を行うものです。DPM の Web コンソールは、ブラウザから DPM サーバを操作するものです。

か

仮想マシン

仮想マシンサーバ上に仮想的に実現されたマシンを指します。

仮想マシンサーバ

仮想マシンを実現するためのサーバを指します。

SigmaSystemCenter では、VMware ESXi、Citrix XenServer、Microsoft Hyper-V、Red Hat KVM を管理対象とすることができます。

稼動

SigmaSystemCenter でホストにマシンを割り当て、グループに登録した状態を指します。

監視対象マシン

SystemMonitor 性能監視により監視されているマシンです。

管理サーバ

SystemProvisioning がインストールされたサーバです。

管理対象マシン

SystemProvisioning で管理対象とするマシンです。

共有ディスク

複数のマシンで共有できるディスクボリュームを指します。

グループ

SystemProvisioning は、運用時にマシンをグループ単位で管理します。グループ管理により、マシン管理の負担を軽減し、運用コストを削減することができます。このような同じ用途で使用するマシンの集合を運用グループと呼びます。SystemProvisioning で、"グループ" という場合、"運用グループ" を指します。

また、SystemProvisioning では、管理対象マシンをリソースとして管理します。Web コンソールの [リソース] ビューでは、管理対象マシンを分類表示するためのグループを作成することができます。こちらは、"リソースグループ" と呼びます。

さ

閾値

SigmaSystemCenter に含まれる ESMPRO や SystemMonitor 性能監視などの監視製品は、管理対象のデータと閾値を比較して、異常 / 正常状態を判断しています。

スタンドアロン ESXi

VMware vCenter Server を使用しないで、SystemProvisioning から直接管理される ESXi を指します。

スマートグループ

管理対象マシンの検索条件を保持する論理的なグループです。検索条件に合致する管理対象マシンが検索できます。

また、電源状態など、逐次変化するステータス情報を検索条件として設定することもできます。

た

タグクラウド

管理対象マシンの様々な情報を "タグ" として分類・集計し、管理対象マシン全体の情報を "タグの集合" として視覚的に表示する機能です。

また、"タグ" を選択することで、そのタグに分類されたマシンのみを絞り込むことができます。

データセンタ

仮想マシンサーバを束ねる役割を持ちます。

vCenter Server 環境を管理する場合には、vCenter Server のデータセンタと対応しています。vCenter Server のクラスタは、SigmaSystemCenter ではデータセンタと同等に扱います。

は

復旧処理設定

イベントが発生した際に行う復旧処理を定めた設定です。

SystemProvisioning では、ポリシーと呼びます。

配布ソフトウェア

SigmaSystemCenter では、マシン移動や置換などの構成変更の際に使用する設定を配布ソフトウェアと呼びます。以下の 3 種類があります。

- シナリオ
- テンプレート
- ローカルスクリプト

パワーサイクル

いったん、マシンの電源をオフにした後、再度、オンにする操作です。

物理マシン

実体を持つハードウェアマシンの総称です。本書では物理サーバと記載しています。

物理マシンは、一般マシン、および仮想マシンサーバを含みます。

プライマリ NIC

SystemProvisioning 管理対象マシンの管理に使用するネットワークに接続する NIC です。WakeOnLAN により起動する設定を行った NIC です。

ポリシー

"マシンで障害が発生した場合、どのような処理を自動実行するのか" といった障害時の復旧処理設定を指します。SystemProvisioning では、ESMPRO/ServerManager、vCenter Server など

の仮想マシン基盤、Out-of-Band Management 管理機能、および SystemMonitor 性能監視が検出したマシンの障害に対し、復旧処理を設定できます。

ま

マシン

SigmaSystemCenter で管理できる物理マシン / 仮想マシンの総称です。

メンテナンスモード

マシンのメンテナンス作業中など、障害通報を無視したいときに使用するモードです。メンテナンスモードに設定したマシンで障害が発生しても、ポリシーによる復旧処理は行いません。

ら

ローカルスクリプト機能

.bat 形式の実行可能ファイル (ローカルスクリプトと呼びます。) を SigmaSystemCenter 管理サーバ上で実行する機能です。管理対象マシンの追加や用途変更、置換などを行う際に、システム構成や環境に依存した特定の処理を管理サーバ上で行いたい場合に使用します。

SigmaSystemCenter 3.8
簡易構築ガイド VMware 編

SSC0308-doc-0026-1.1

2019 年 12 月 1.1 版 発行

© NEC Corporation 2012 - 2019