NEC

SigmaSystemCenter 3.8
簡易構築ガイド Hyper-V 編

SSC0308-doc-0027-1.1

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/termsofuse.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. 管理対象の登録 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 14

5.2.1 仮想ビュー 14

5.2.2 リソースビュー 15

5.2.3 運用ビュー 16

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 18

5.3 リソースプールの確認 19

5.3.1 vCPU の単位の設定 22

5.3.2 データストアの設定 23

5.4 手動での仮想マシンの移動(Migration) 24

6. レポート機能の利用（負荷状況取得の設定) 29

6.1 負荷状況取得の設定 29

6.1.1 物理サーバの負荷状況取得の設定 30

6.1.2 業務用仮想マシンの負荷状況取得の設定 32

6.1.3 動作テスト 34

6.2 レポートの作成 36

6.2.1 リソースプール(物理サーバグループ)のレポート作成 37

6.2.2 個別の仮想マシンのレポート作成 40

6.3 レポートの閲覧 42
6.3.1 リソースプール概要のレポート 43
6.3.2 業務用仮想マシンの負荷履歴レポート 44

7. 電源操作の設定 46

7.1 物理サーバの設定 46
7.1.1 iLO（BMC）の設定 46
7.1.2 Express5800/D120h などの BMC/CMC の設定 50
7.1.3 SSC での OOB のアカウント設定 55

7.2 動作テスト(一括電源操作) 58
7.2.1 仮想マシン自動起動の設定 58
7.2.2 マシンシャットダウン 60
7.2.3 マシン起動 62

8. 予兆を含む障害対応機能の設定 65

8.1 監視・通報の基本設定 65
8.1.1 SNMP Trap サービスの設定 65
8.1.2 Windows ファイアウォールの設定 65
8.1.3 死活監視の基本設定 68
8.1.4 通報に必要な環境設定 68

8.2 負荷監視の設定 70

8.3 死活監視と ESMPRO/ServerManager の設定 76
8.3.1 仮想マシンの設定 76
8.3.2 死活監視と ESMPRO/ServerManager の設定 77

8.4 障害や負荷に対するポリシーの設定 79
8.4.1 ポリシーのインポート 80
8.4.2 仮想マシン用ポリシーの確認と適用 82
8.4.3 物理サーバ用ポリシーの確認と適用 85
8.4.4 物理サーバ用のポリシーの適用 89

8.5 動作テスト(擬似障害テスト) 89

付録 A. 運用に関する重要な情報 96

付録 B. SigmaSystemCenter マニュアル体系 97

付録 C. 改版履歴 99

付録 D. ライセンス情報 100

用語集 101

はじめに

この文書では、「Windows Server 2016 Hyper-V」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って説明しています。

  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 B. SigmaSystemCenter マニュアル体系（97 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（96 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、稼動状況の収集・閲覧をする。

   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（Hyper-V）

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（Hyper-V）

3. 障害・負荷監視、および、障害時の自動対処を行う。

   - 障害監視をする。

     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（Hyper-V）

   - 負荷監視をする。

     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（Hyper-V）

   - 予兆障害を契機に仮想マシンの移動(Migration)をする。

     物理サーバ（Hyper-V）の障害予兆を検出し、その上で動作する以下の仮想マシンを仮想マシンの移動(Migration)で別の物理サーバへ移動します。

     - 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。

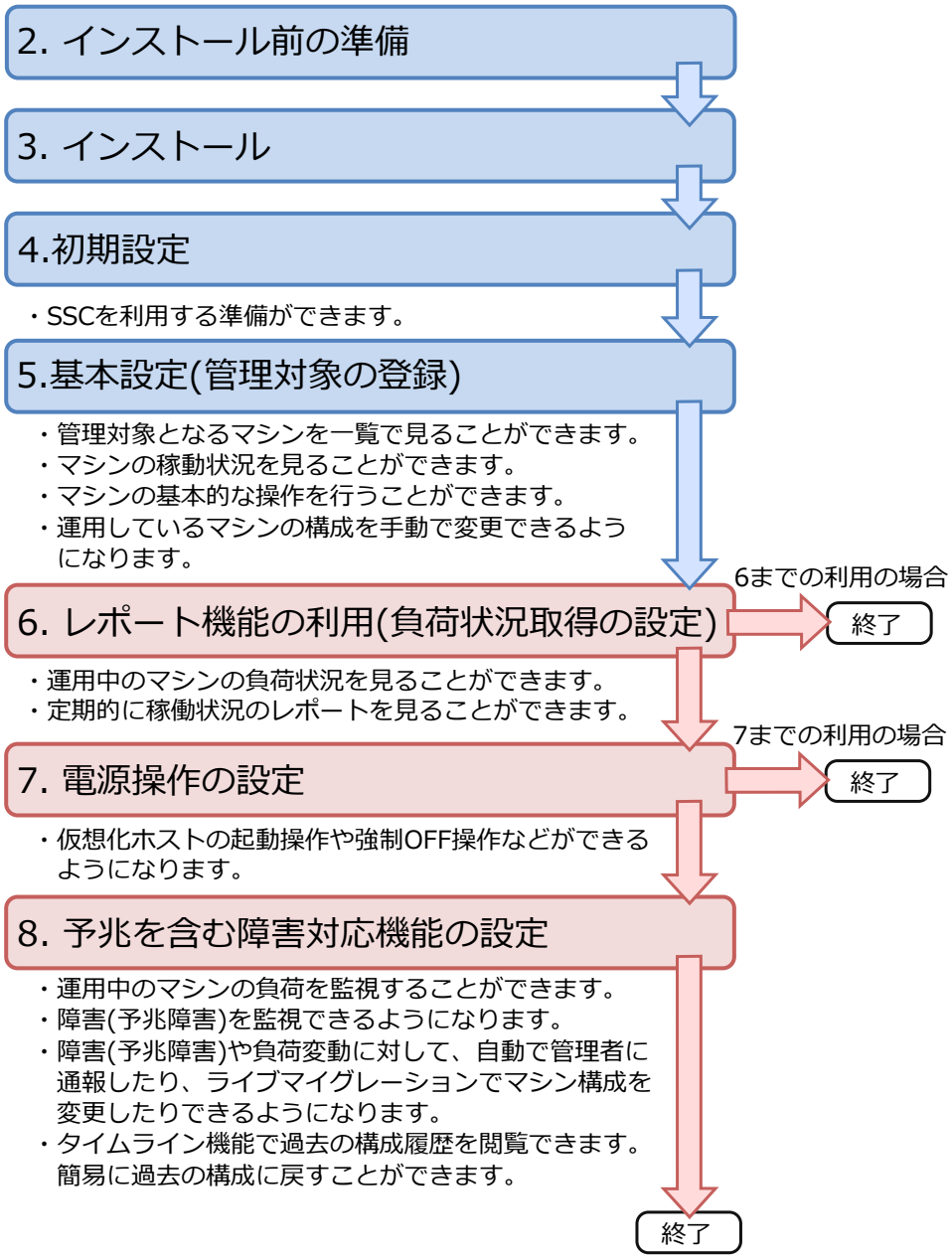


図　本ガイドでの構築の流れ

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）
    - Windows Server 2016 Hyper-V
    - ホスト名：IP アドレス(管理用ネットワーク)
      - HV01：172.16.10.1
      - HV02：172.16.10.2
      - HV03：172.16.10.3
    - 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
    - Hyper-V クラスタ
      - クラスタ名：IP アドレス(管理用ネットワーク)
        - hv-cluster.ssc-handson.net：172.16.10.10
      - クラスタノード
        - HV01、HV02、HV03
  - 業務用仮想マシン（6 台）
    - Windows Server 2016 Standard
    - ホスト名：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（1 台）
  - Windows Server 2016 Standard
  - SigmaSystemCenter
  - ESMPRO/ServerManager

- 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)

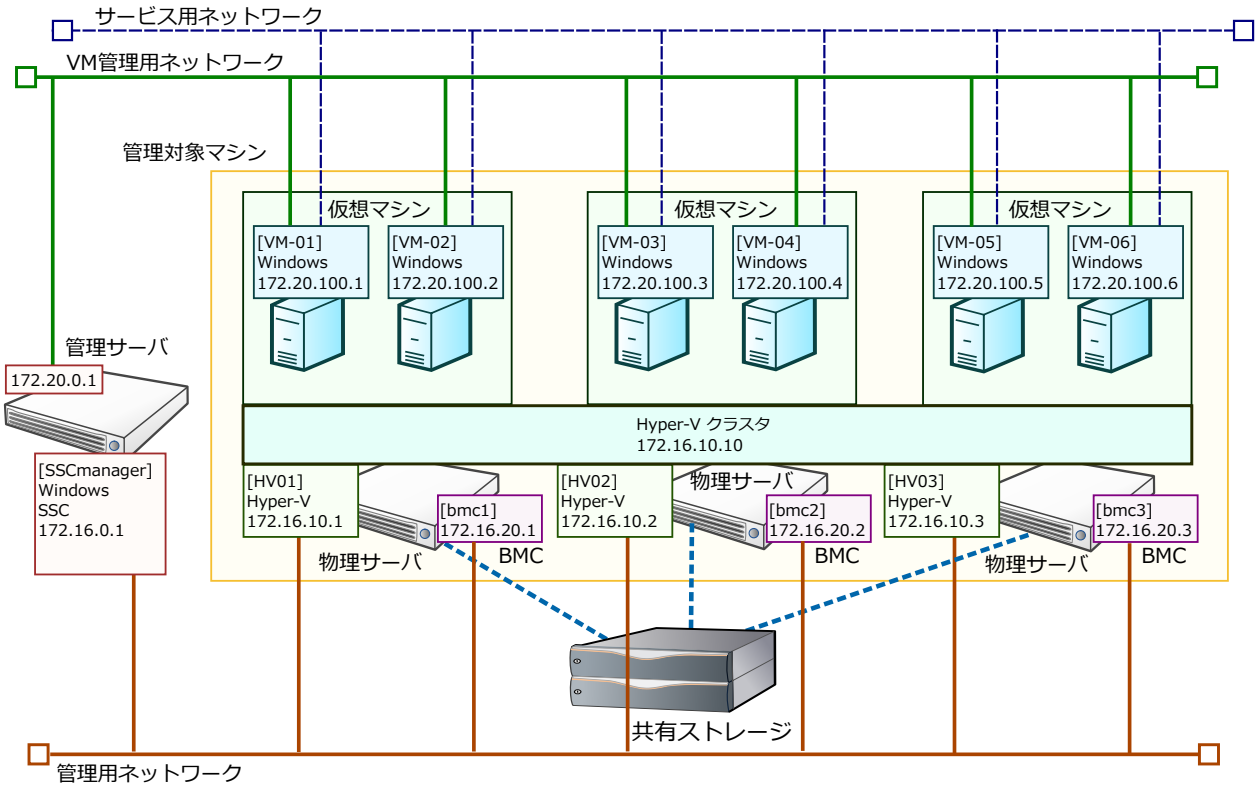


図　今回構築するシステムの構成

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 2 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(物理サーバ)には、最初に以下の順番で仮想マシンサーバとして構築しておきます。

今回は、全ての仮想マシンサーバを、フェールオーバー クラスタのノードとして追加しておいてください。物理サーバの物理的障害により Hyper-V がダウンした場合に、自動的に仮想マシンを別の仮想マシンサーバで再起動するフェールオーバーを可能にするためです。

1. Windows Server 2016 のインストール
2. 「Hyper-V」の役割を追加
3. 「フェールオーバー クラスタリング」機能を追加
4. フェールオーバー クラスタの作成

   今回の場合、[HV01]、[HV02]、[HV03]の全ての物理サーバ(仮想マシンサーバ)をノードとして追加してください。

5. ESMPRO/ServerAgentService のインストール

フェールオーバーが必要ない場合は、クラスタを用意する必要はありません。SSC でもクラスタ構成ではない Hyper-V を管理することは可能ですが、今回はそういった構成を管理する手順は説明しません。

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"Migraion"(ライブマイグレーション）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、6.24 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。

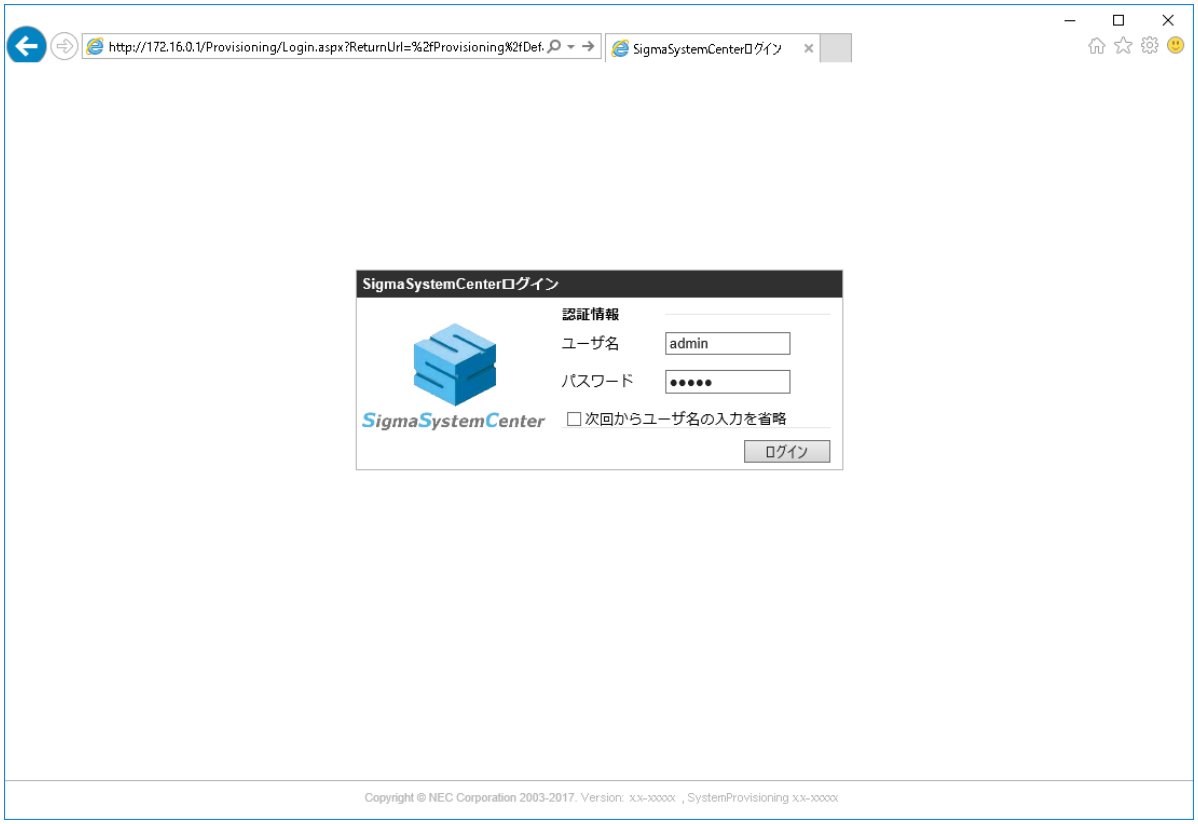


図 「SigmaSystemCenter ログイン」画面

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。

画面右上の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「ユーザ一覧」、「ロール一覧」の画面が表示されたら、「ユーザ一覧」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。

図 「ユーザ追加」画面

[OK]をクリックすると、「ユーザ一覧」、「ロール一覧」の画面に遷移し、「ユーザ一覧」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. 管理対象の登録

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 本体に先に登録しておく必要があります。

今回は管理対象がクラスタ構成の Hyper-V ですので、サブシステムとして Hyper-V Cluster を先に登録しておきます。

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）、左ペインのツリービューにある[サブシステム]をクリックします。右サイドバーの[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[Hyper-V Cluster]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： Hyper-V がインストールされたノードのクラスタ名もしくは IP アドレス

  （今回は hv-cluster.ssc-handson.net）
- ドメイン¥アカウント名： クラスタのアカウント名
- パスワード： クラスタのパスワード
- **[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。

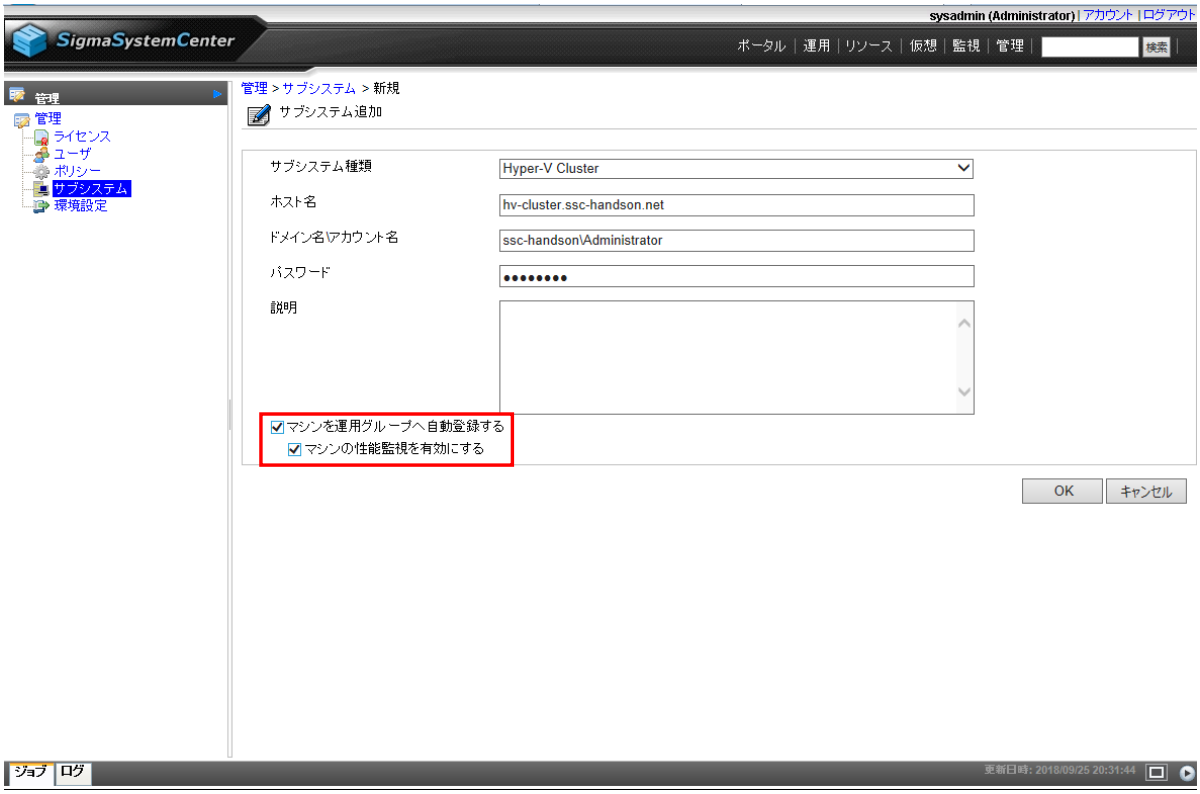


図　Hyper-V Cluster の登録

Hyper-V Cluster 登録後に「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、Microsoft Hyper-V 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）。

また、そのクラスタの各ノードである Hyper-V も自動的に検出/登録されます。

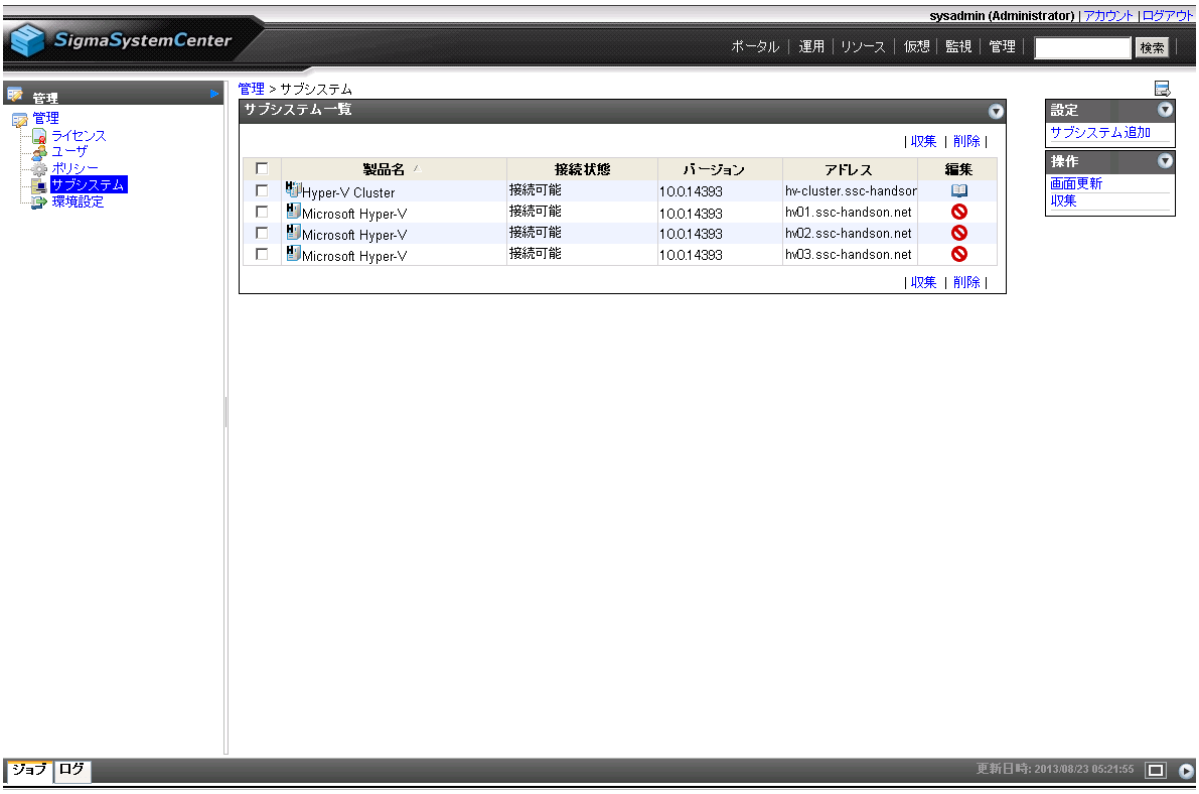


図　サブシステム一覧

なお、Hyper-V 用のサブシステムとして、「Hyper-V Cluster」のほかに「Microsoft Hyper-V」があります。「Microsoft Hyper-V」は Hyper-V Cluster でない Hyper-V 環境で使用します。

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て、hv-cluster-ssc-handson.net 下に登録されている物理サーバ([HV01]、[HV02]、[HV03])、業務用仮想マシン([VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06])が、Hyper-V クラスタ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。

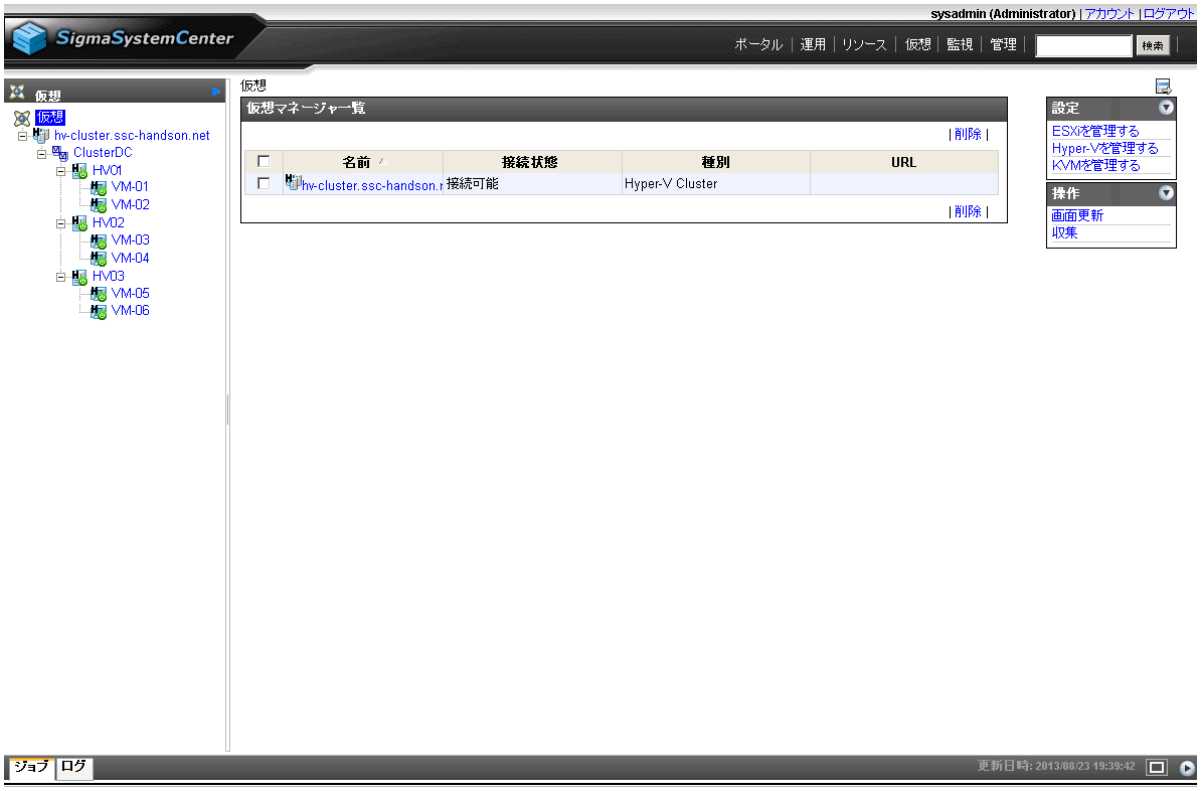


図　[仮想]ビュー

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。

Hyper-V クラスタに登録されている物理サーバ([HV01]、[HV02]、[HV03])、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。

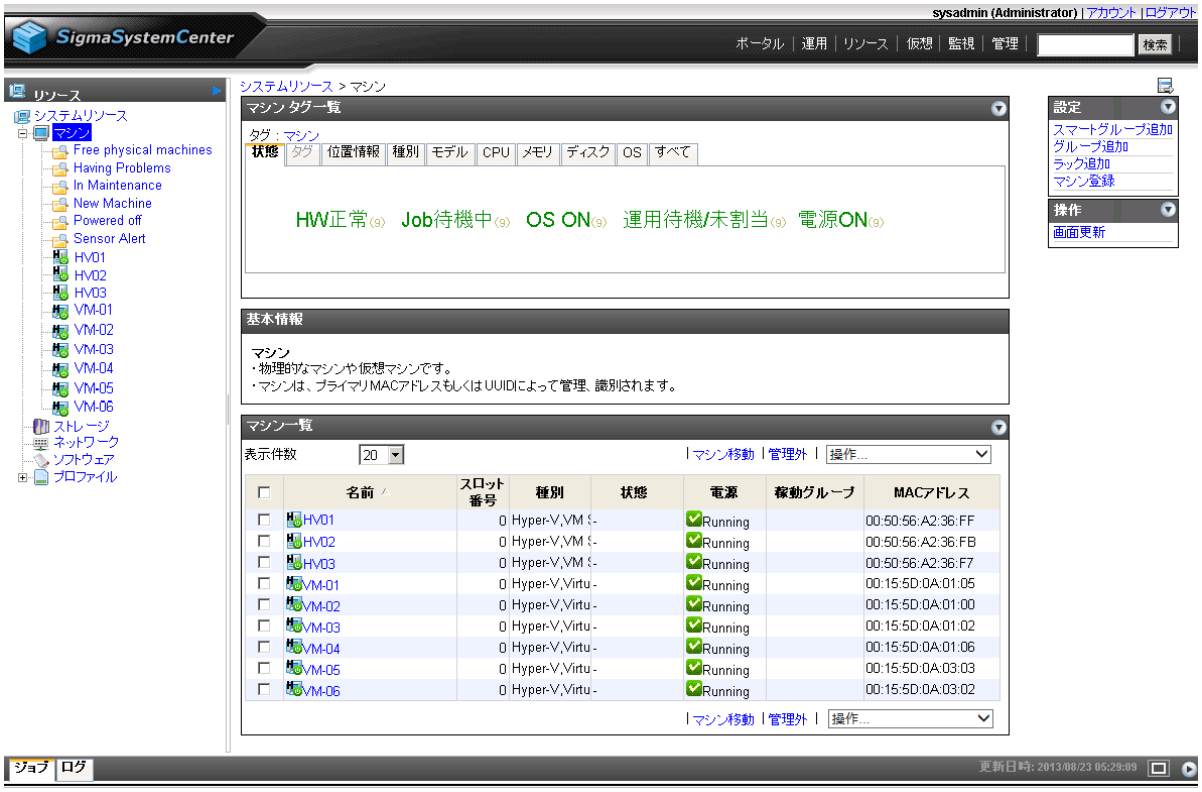


図　サブシステム登録時の「マシン一覧」画面

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（65 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		
HV01	172.16.10.1	物理（VM サーバ）	Windows Server 2016 Hyper-V	hv-cluster-ssc-handson-net	ClusterDC
HV02	172.16.10.2				
HV03	172.16.10.3				
VM-01	VM-01	仮想（VM）	Windows Server	hv-cluster-ssc-handson-net	ClusterDC_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のグループ名（ここでは[ClusterDC]）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 ClusterDC グループ(物理サーバ)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[ClusterDC_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。

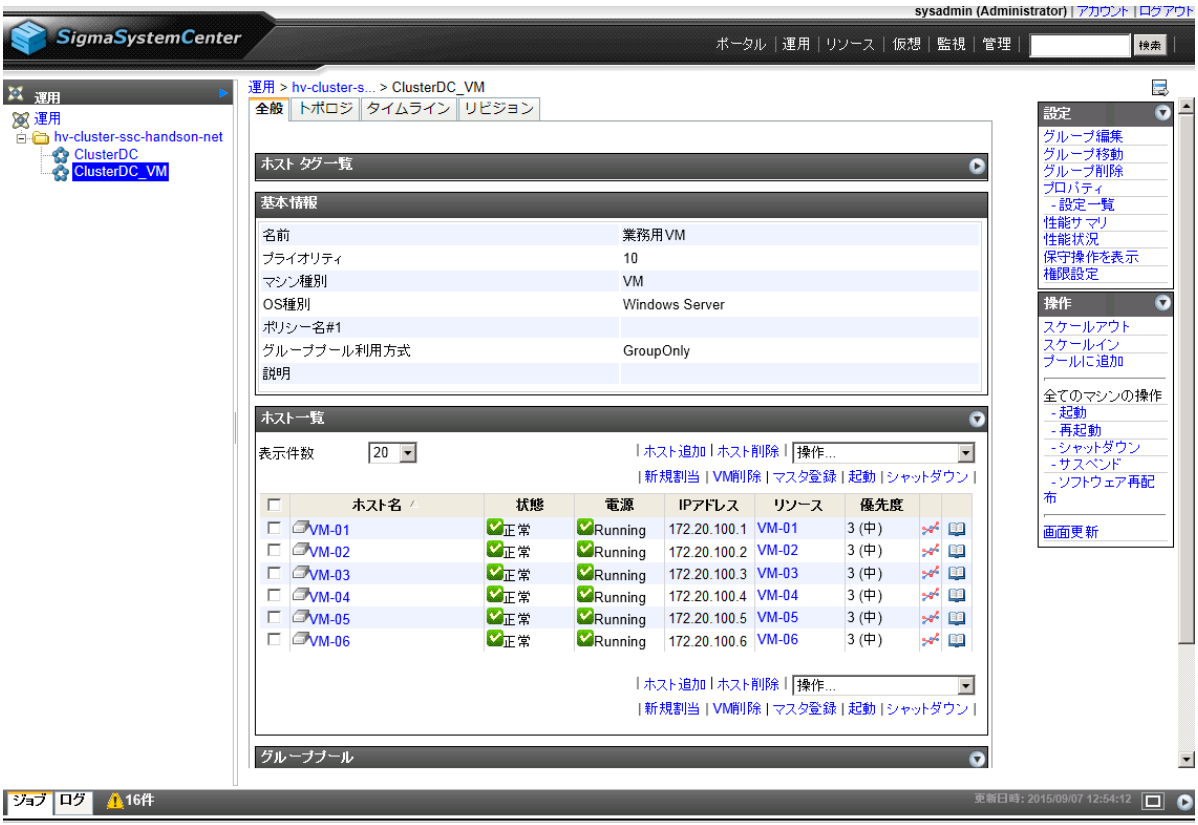


図　サブシステム登録時の[ClusterDC_VM]グループ(VM)の[ホスト一覧]

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、Hyper-V Cluster 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。

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、登録内容を確認してください。

図　収集の操作

以上で、マシン登録の確認は終了です。

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、既に閲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物理サーバのグループ名（ここでは[ClusterDC]）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。

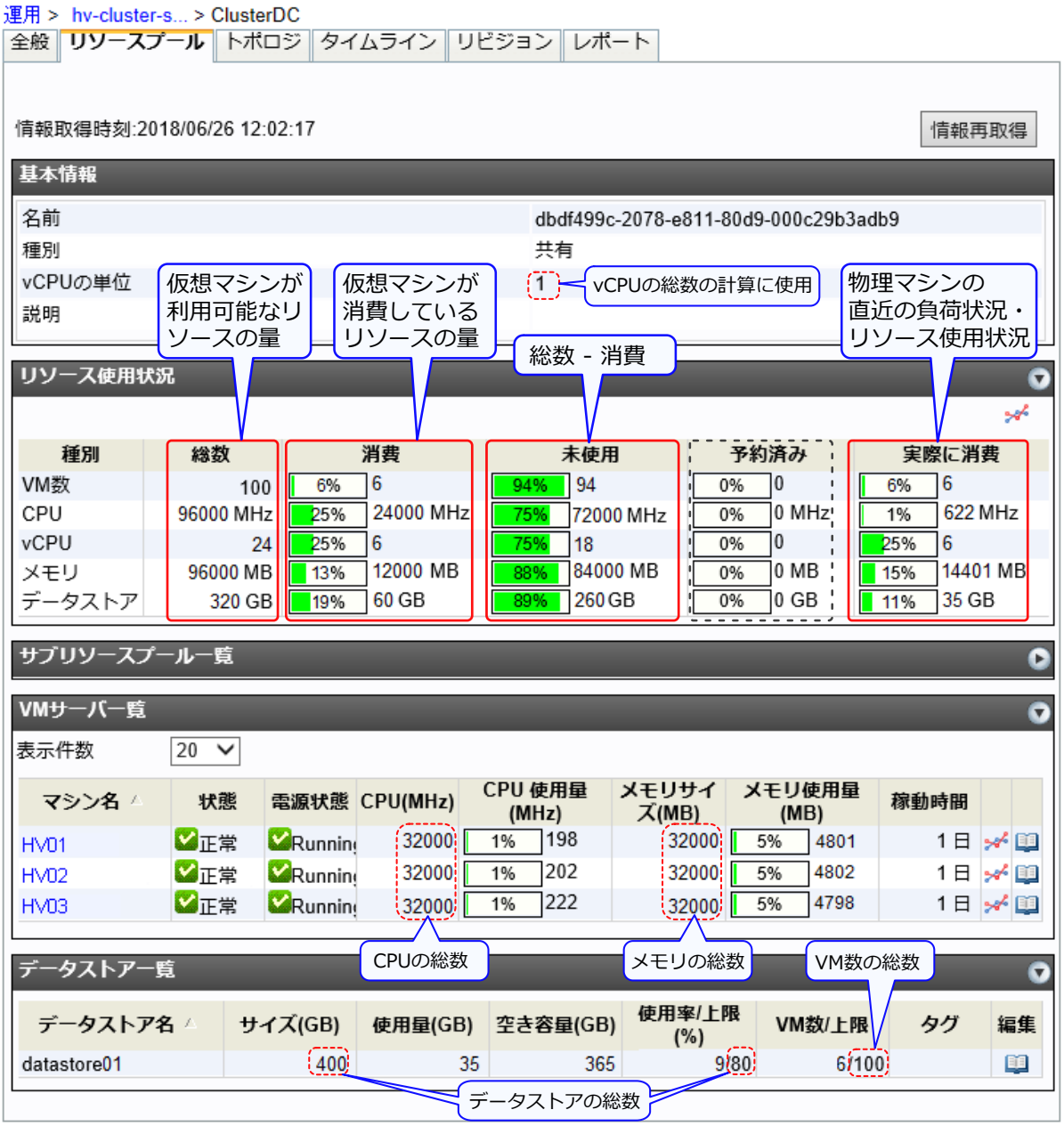


図　リソースプールの画面

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]の情報を見るとの 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。

VM 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。

- 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。

- 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。

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約 1%ですが、最大で 24000MHz(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 (23 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。 **ヒント** ハイパースレッディングが有効な環境の場合は、CPU の情報はゲスト OS 上で論理的に見える CPU のリソース量で計算されます。前述の図の場合、1 台の物理サーバに 2000MHz のコアが 8 個搭載されていて、論理的には CPU が 16 個存在することになります。そのため、1 台あたりの CPU リソースの総量は 32000MHz となります。物理サーバが 3 台の環境ですので、CPU 総数は 96000MHz となります。
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、物理サーバに搭載される 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 (22 ページ)」を参照してください。

リソースの種別	説明
	ヒント vCPU の情報は CPU コアに関係する情報のため、ハイパースレッディングの設定の影響を受けません。
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（23 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、「5.4 手動での仮想マシンの移動(Migration)（24 ページ）」に進んでください。

- vCPU の単位の設定

  物理サーバに搭載される 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、物理サーバに搭載される 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、設定変更をしてください。

設定を変更すると、[vCPU]の総数の値に反映されます。

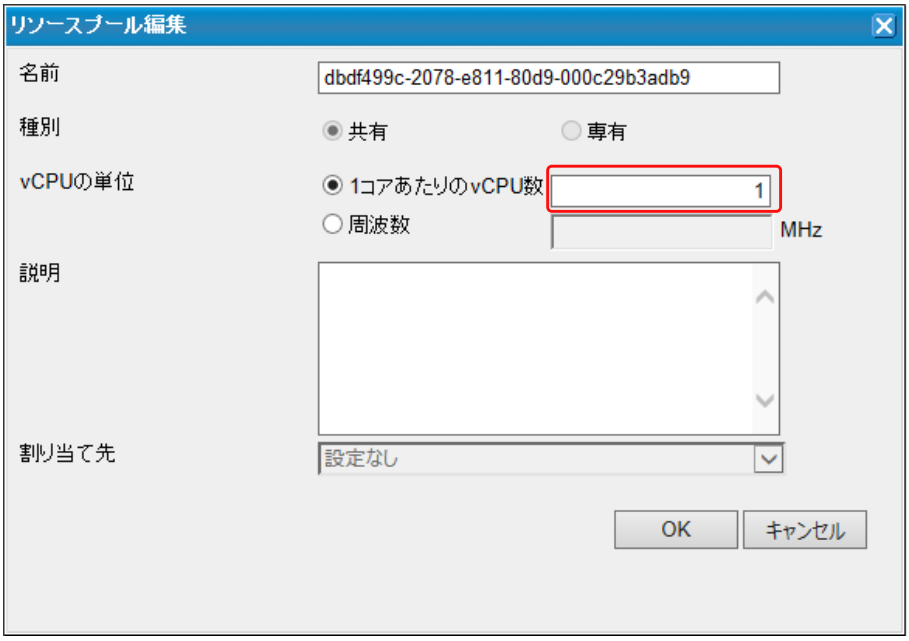


図 「リソースプール編集」画面

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の設定を、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。

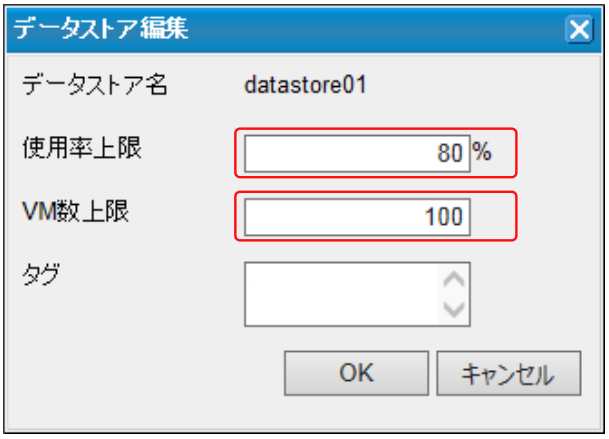


図 「データストア編集」画面

5.4 手動での仮想マシンの移動(Migration)

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、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"(Hyper-V の用語では「ライブマイグレーション」)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（65 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[HV01]上で仮想マシン([VM-01]、[VM-02])が動作しており、物理サーバ[HV02]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、仮想マシン[VM-02]を物理サーバ[HV01]から[HV02]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。

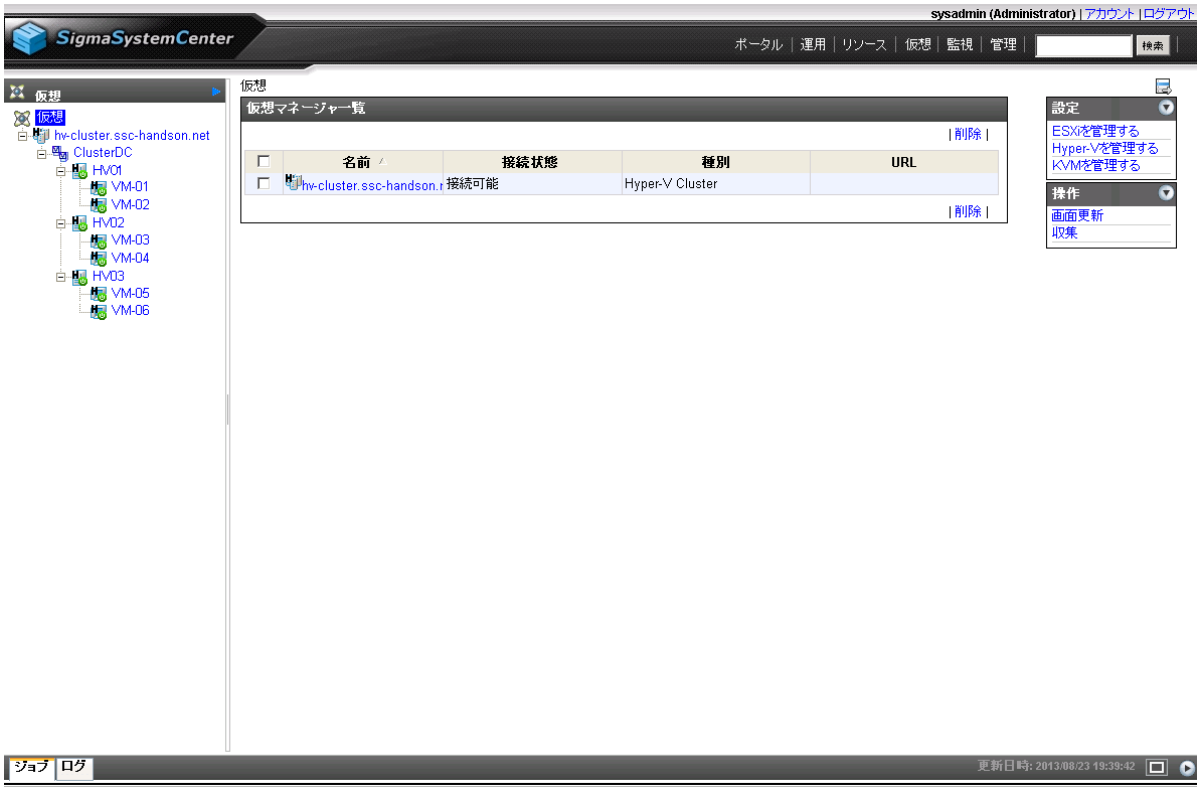


図　[仮想]ビュー

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[HV01]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]には[ClusterDC]が固定で選択されています。次に、移動先となる物理サーバ[HV02]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 2 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。Hyper-V のライブマイグレーションを利用します。

  [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。Hyper-V のストレージ ライブマイグレーションを利用します。

  [停止後に移動(Move)]をチェックした場合は、仮想マシンを停止してから仮想ストレージを移動します。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。 また、仮想マシンを移動せずにストレージだけを移動することも可能です。

これらの移動方法の Storage Migration を除いては、移動元の Hyper-V ホストと移動先の Hyper-V ホスト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、仮想マシンを稼動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。

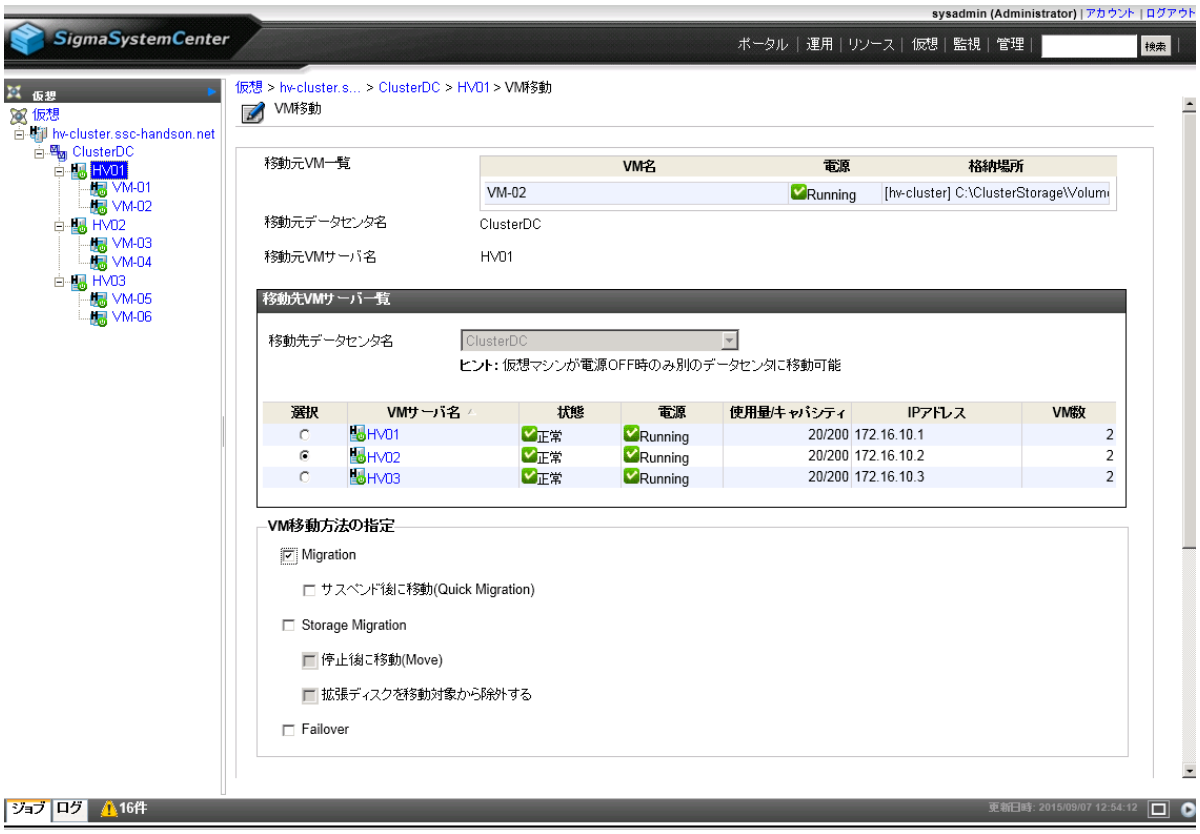


図　移動先と移動方法の選択

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、仮想マシン[VM-02]が物理サーバ[HV02]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、F5 キーで全画面を更新してみてください。

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 負荷状況取得の設定

ここからは、管理対象マシンのレポート表示を行うために必要な負荷状況の取得の設定を行います。

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。

なお、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（70 ページ)」で説明します。

監視プロファイルは、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。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。

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。今回は、レポート表示用にデフォルトで用意されている以下の監視プロファイルを使用します。下記監視プロファイルは、「5.1 サブシステムの登録（12 ページ)」でサブシステム登録時に自動で設定されます。

- 物理サーバグループ: [Builtin](For Report)VMServer Monitoring Profile (5min)
- 業務 VM グループ:[Builtin](For Report)VM Monitoring Profile[VM OS] (5min)

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。

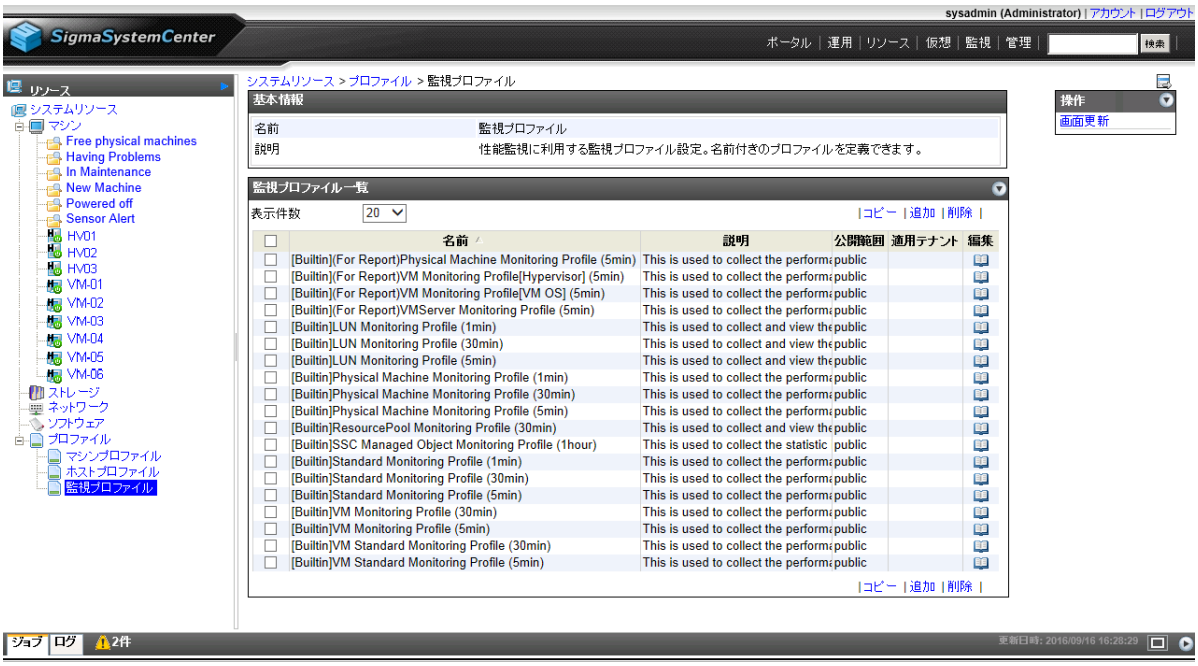


図　監視プロファイル一覧

6.1.1　物理サーバの負荷状況取得の設定

物理サーバの負荷監視に必要な設定について説明します。

(1)物理サーバ上の設定

使用する監視プロファイル[Builtin](For Report)VMServer Monitoring Profile (5min)は、物理サーバに直接アクセスして情報を取得します。

物理サーバにアクセスするには、十分な権限(Administrators グループなど)を持ったアカウントが物理サーバ上に準備されている必要があります。既定の設定では「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に使用したクラスタのアカウントが使用されますので、クラスタのアカウントを物理サーバの Administrators グループに所属させるようにしてください。

また、負荷状況を取得するための管理サーバから物理サーバへの通信を確保するために、物理サーバの OS 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。物理サーバ[HV01]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。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）

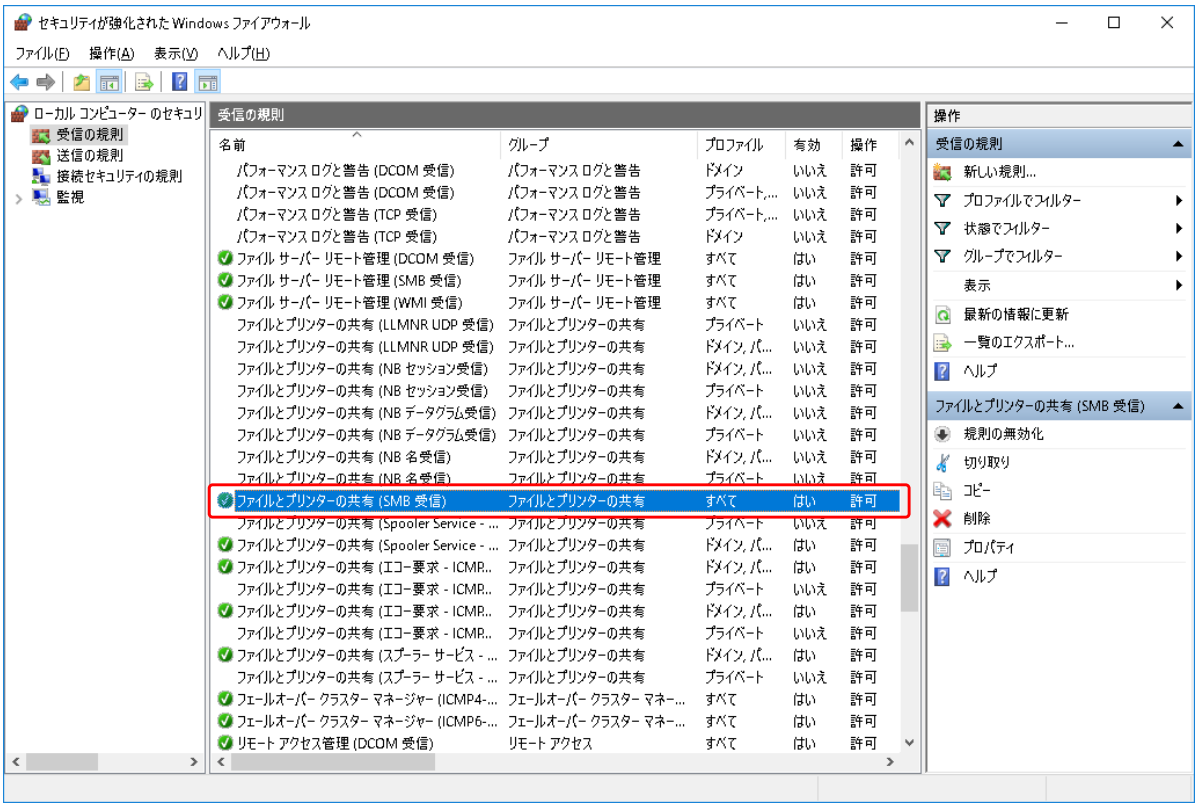


図　セキュリティが強化された Windows ファイアウォール

物理サーバ[HV02]、[HV03]についても、同様の設定を行います。

(2)物理サーバの運用グループの設定

物理サーバの負荷状況取得設定については、「5.1　サブシステムの登録（12 ページ）」でサブシステムを登録する時に自動的に行われます。SSC の Web コンソール上で確認してみましょう。

[運用]ビュー（画面右上の[運用]をクリック）を表示し、ツリービューから設定対象の運用グループである[CluseterDC]をクリックします。次に、[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]タブの各項目が、以下のようになっていることを確認します。

ヒント

アカウントは、既定ではサブシステム登録時に指定したクラスタのアカウントが使用されます。クラスタのアカウント以外のアカウントを使用する場合は、下記のアカウントとパスワードの項目に設定してください。

また、物理サーバごとにアカウントの設定が異なる場合は、「ホスト設定」の[性能監視]タブにて、物理サーバごとにアカウントとパスワードの項目を設定してください。

- 性能データ収集設定：チェック(変更しません)
- プロファイル名：[Builtin](For Report)VMServer Monitoring Profile (5min)(変更しません)

- IP アドレス：127.0.0.(変更しません)
- ポート番号：26200(変更しません)
- アカウント：設定なし(変更しません)
- パスワード：設定なし(変更しません)

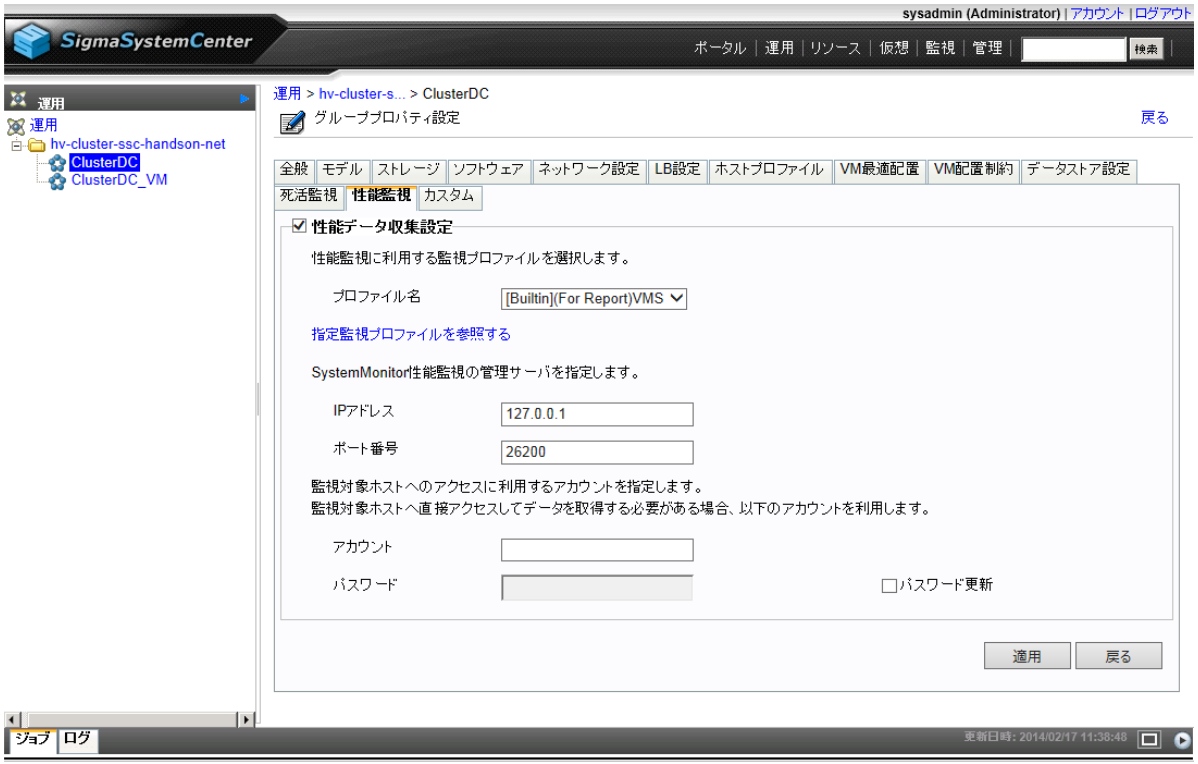


図　[ClusterDC]グループの[性能監視]タブ

6.1.2　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。

(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[VM OS] (5min) は、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。）

負荷状況を取得するための管理サーバからゲスト OS への通信を確保するために、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。仮想マシン[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。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）

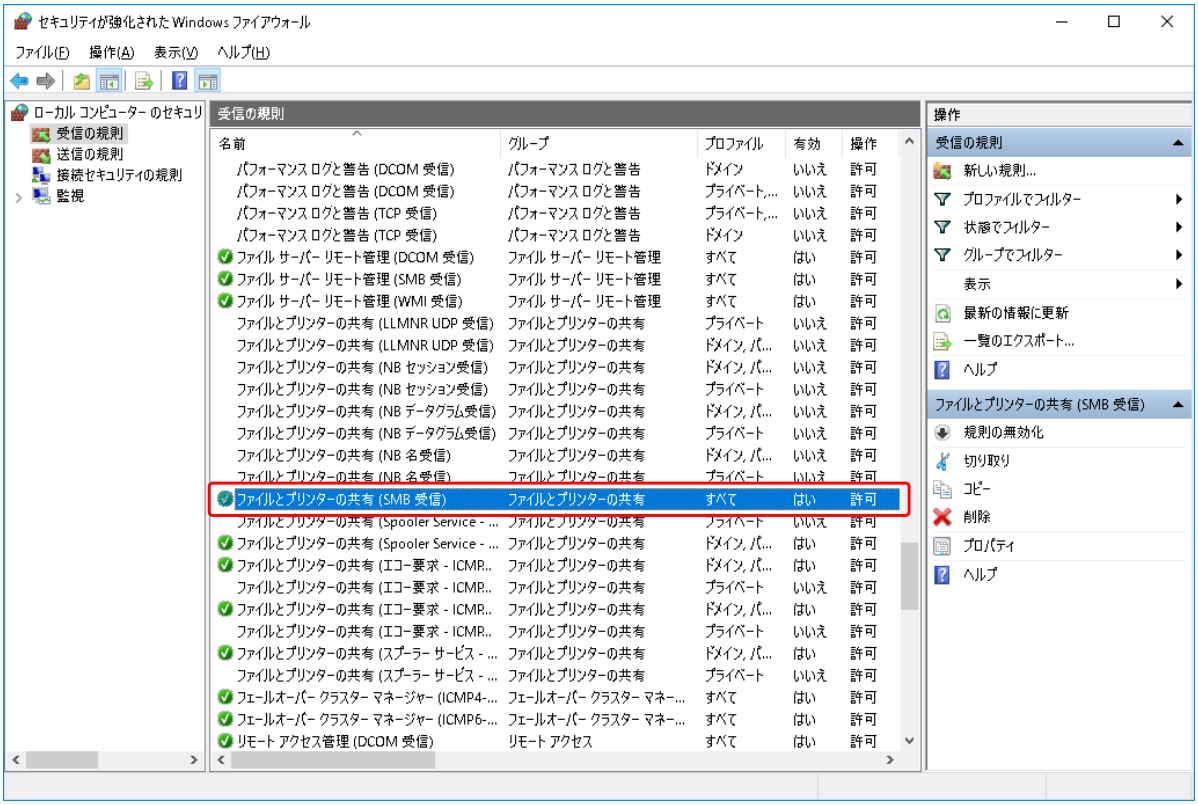


図　セキュリティが強化された Windows ファイアウォール

仮想マシン[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

業務用仮想マシンの負荷状況取得に必要な設定は、アカウントとパスワード以外は「5.1　サブシステムの登録（12 ページ）」でサブシステムを登録する時に自動的に行われます。

下記では、自動的に行われた設定の確認と、アカウントとパスワードの設定を行います。

[運用]ビュー（画面右上の[運用]をクリック）を表示し、ツリービューから設定対象の運用グループである[ClusterDC_VM]をクリックします。

次に、[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。

監視プロファイルなどの設定は既に設定済の状態ですので、アカウントとパスワードを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(変更しません)

- プロファイル名：[Builtin](For Report)VM Monitoring Profile[VM OS] (5min)(変更しません)
- 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

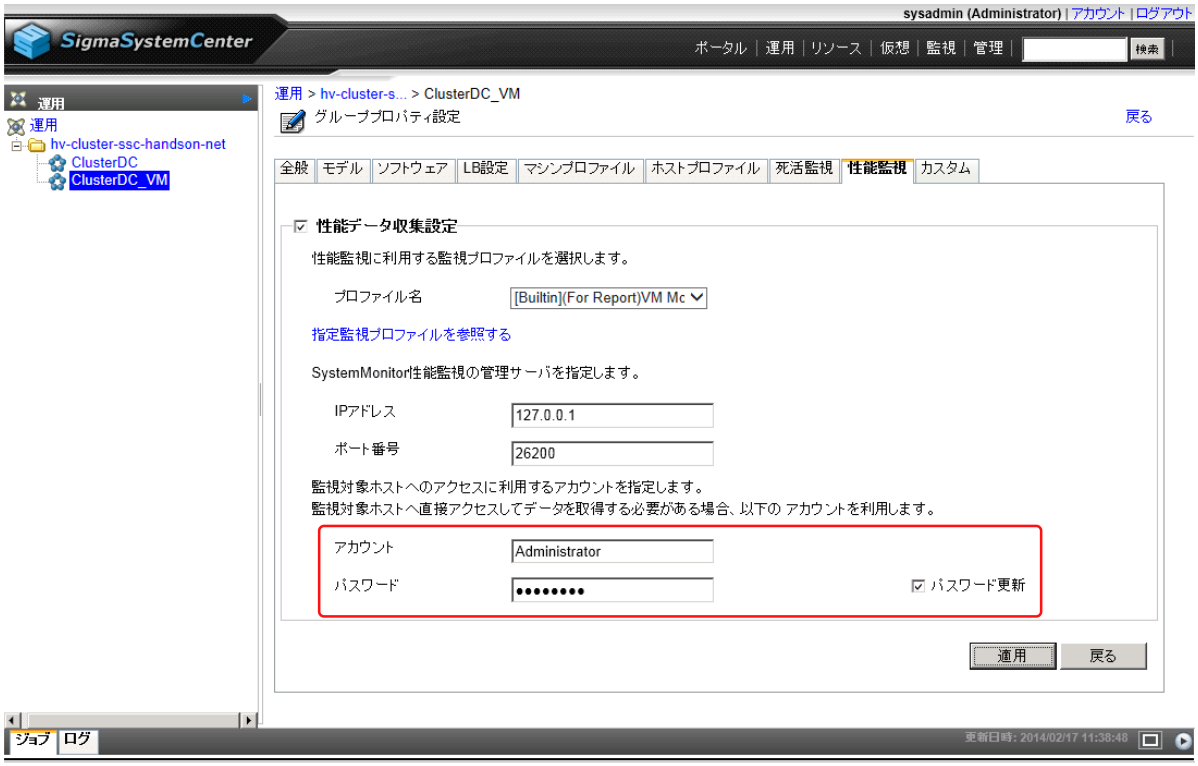


図　[ClusterDC_VM]グループの[性能監視]タブ

6.1.3　動作テスト

では実際に、管理対象マシン（物理サーバ、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。

注

負荷状況取得設定が有効化されるには、「6.1.1　物理サーバの負荷状況取得の設定（30 ページ）」と「6.1.2　業務用仮想マシンの負荷状況取得の設定（32 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[ClusterDC]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

[グラフ設定]が開きますので、近々の負荷状況を確認するために、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。

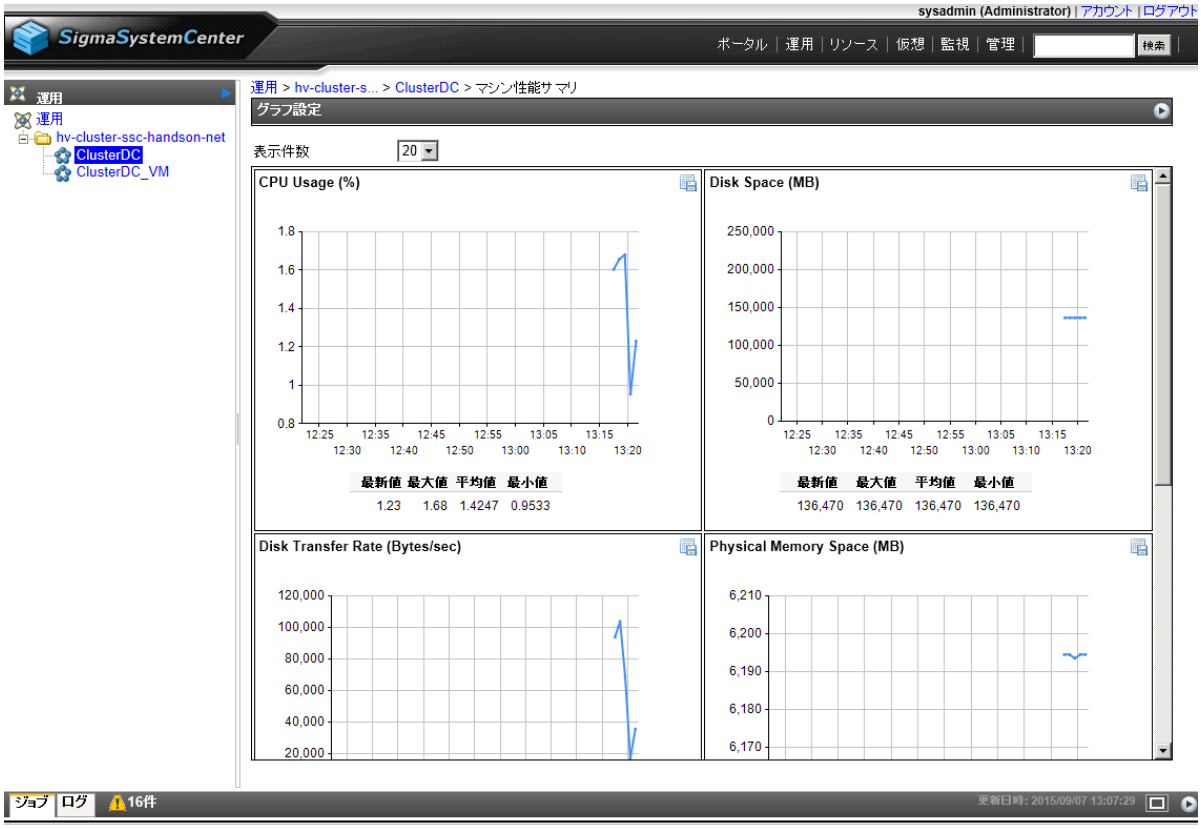


図　負荷状況

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。

6.2　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(物理サーバグループ)

  リソースプールとして、物理サーバ全体のリソース状況や、グループ内の物理サーバ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。

6.2.1 リソースプール(物理サーバグループ)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、物理サーバ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（37 ページ）」
- 「(2)ssc コマンドでの作成（39 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[ClusterDC]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。

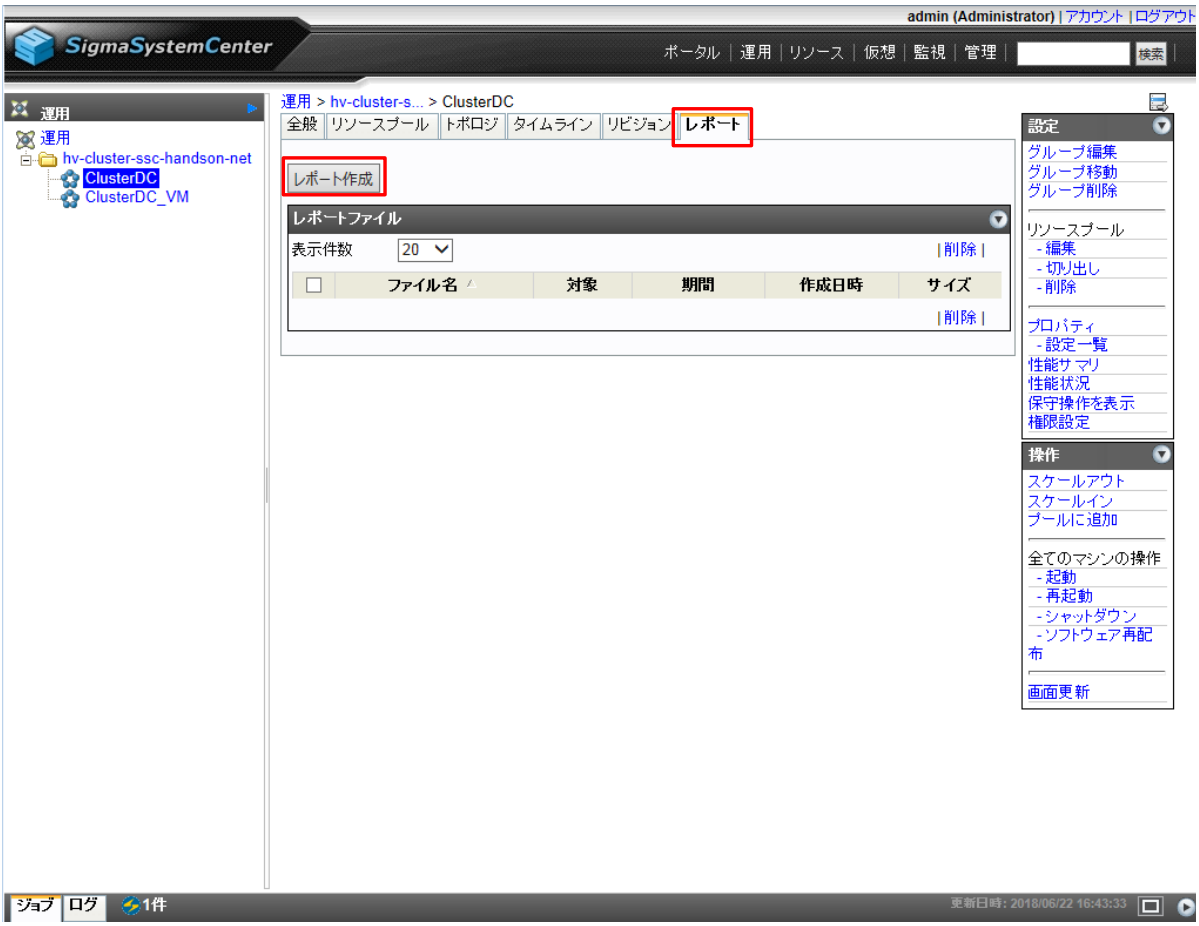


図 「レポート作成」画面 その 1

「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 月とする場合)

- [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。

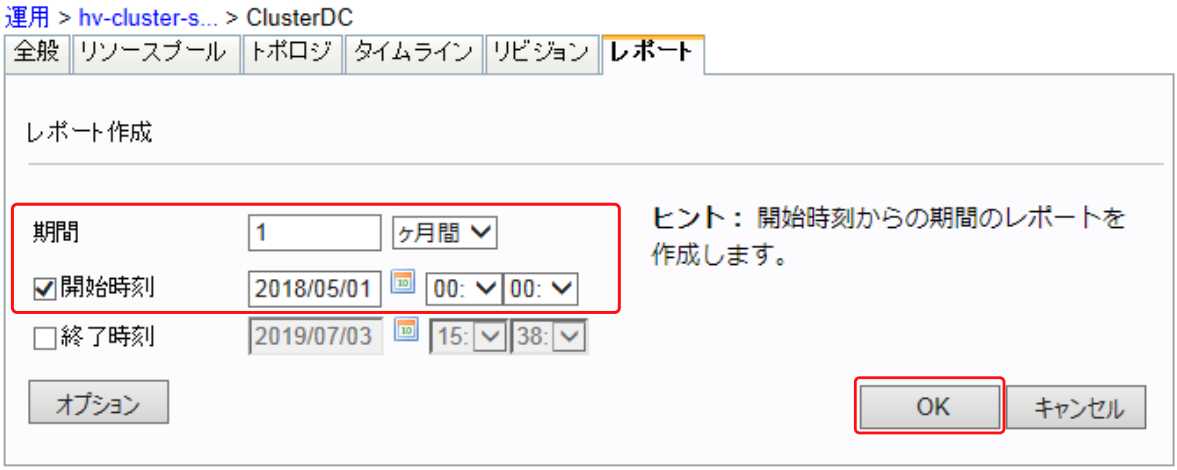


図 「レポート作成」画面 その 2

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「6.3 レポートの閲覧（42ページ）」で説明します。

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。

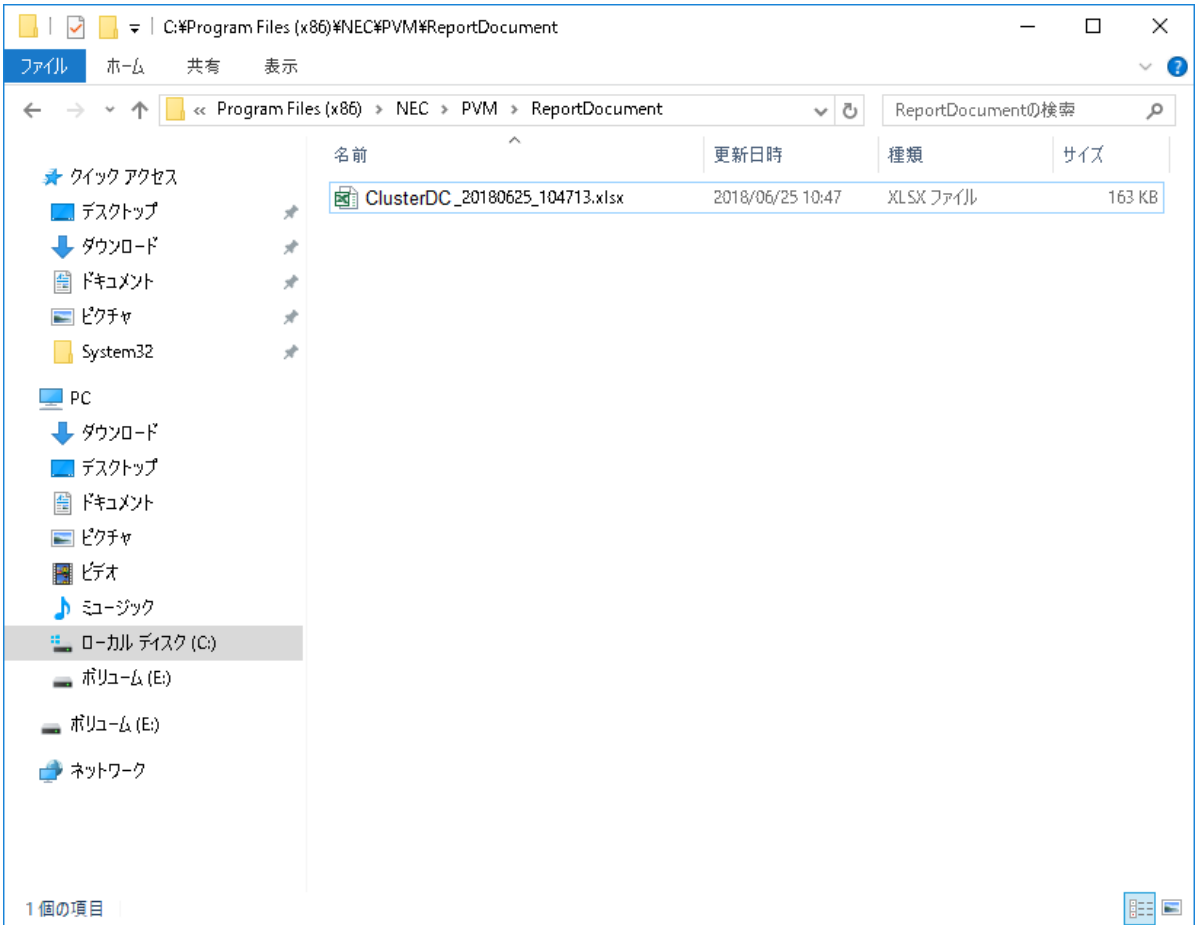
ssc コマンドでの作成も、Web コンソールと同様に、レポート対象のグループまたはホストを指定して、レポートの期間を指定することで作成できます。

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 hv-cluster.ssc-handson.net/ClusterDC -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「6.3　レポートの閲覧（42 ページ）」で説明します。



以上で、物理サーバグループ([ClusterDC]グループ)の前月の月次レポート作成の作業は完了です。

6.2.2 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（40 ページ）」
- 「(2)ssc コマンドでの作成（42 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[ClusterDC_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]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。

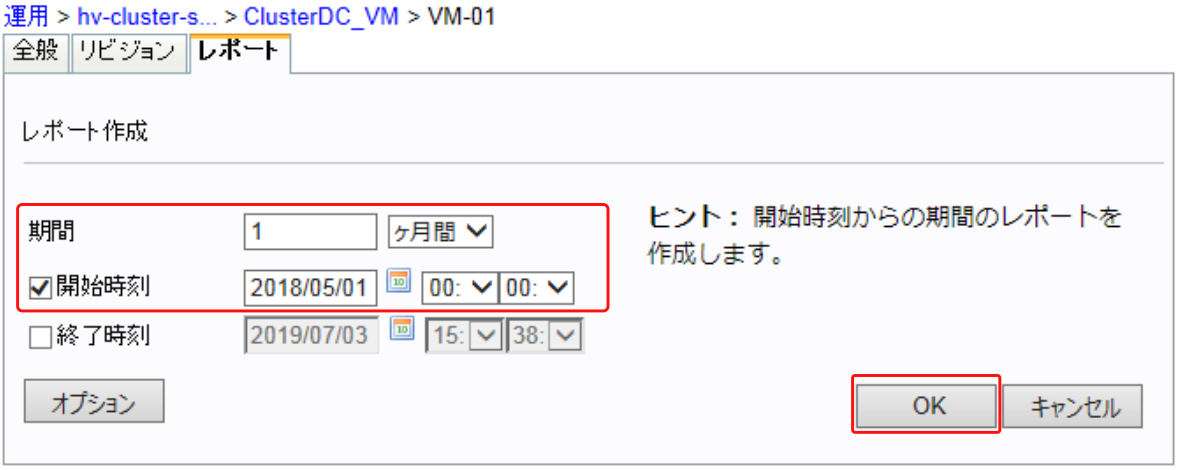


図 「レポート作成」画面 その 2

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「6.3 レポートの閲覧（42ページ）」で説明します。

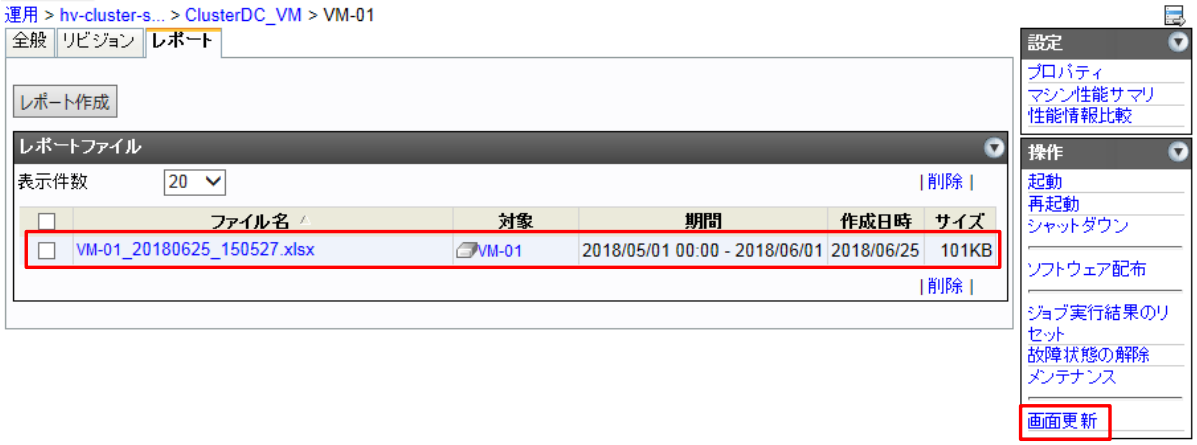


図 レポート作成後の「レポート作成」画面

(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。

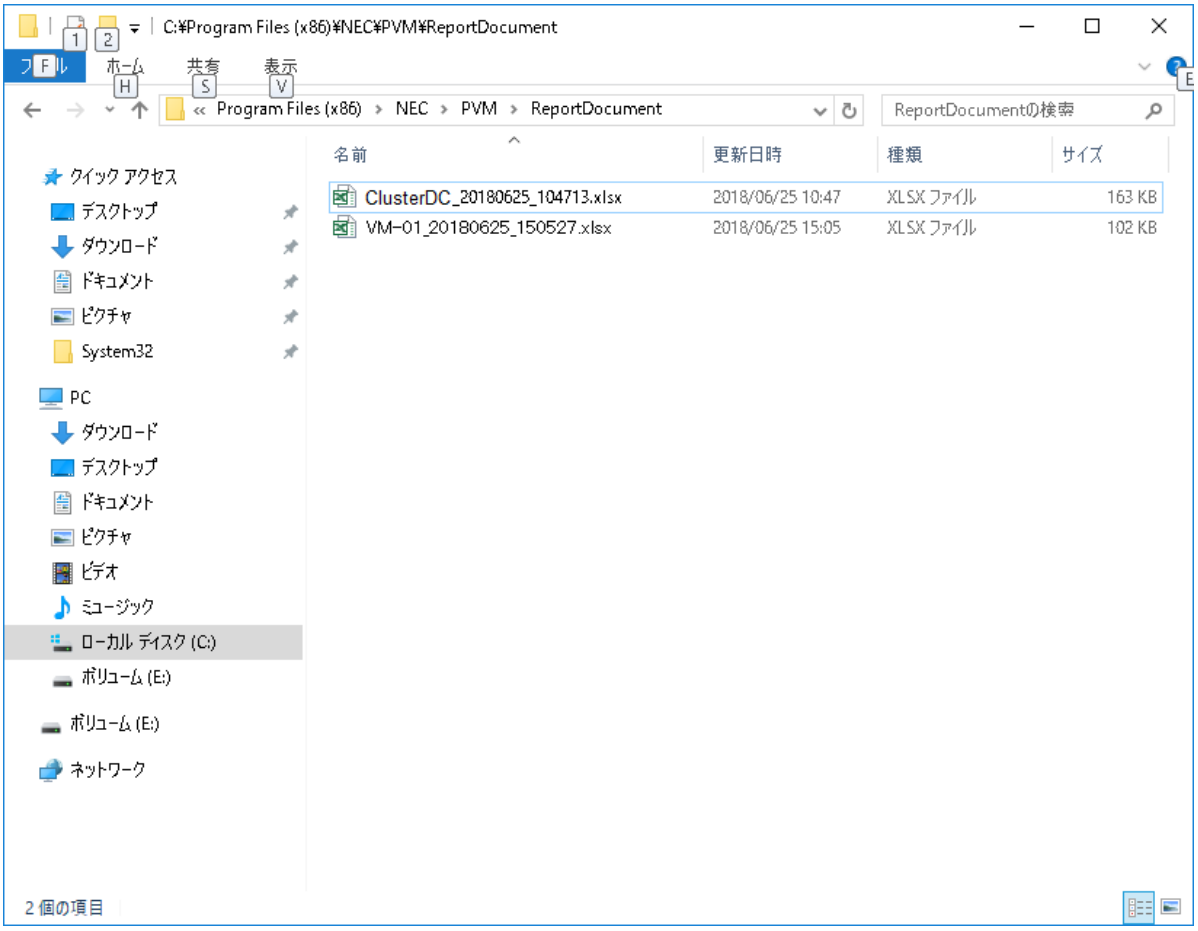
ssc コマンドでの作成も、Web コンソールと同様にレポート対象のグループまたはホストを指定して、レポートの期間を指定することで作成できます。

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 hv-cluster.ssc-handson.net/ClusterDC_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「6.3　レポートの閲覧（42 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。

6.3　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ます。

- 「6.3.1 リソースプール概要のレポート（43 ページ）」

  「6.2.1 リソースプール(物理サーバグループ)のレポート作成（37 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。

- 「6.3.2 業務用仮想マシンの負荷履歴レポート（44 ページ）」

  「6.2.2 個別の仮想マシンのレポート作成（40 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の 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。

6.3.1 リソースプール概要のレポート

「6.2.1 リソースプール(物理サーバグループ)のレポート作成（37 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（19 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。

そのほか、リソースプールを構成する物理サーバ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

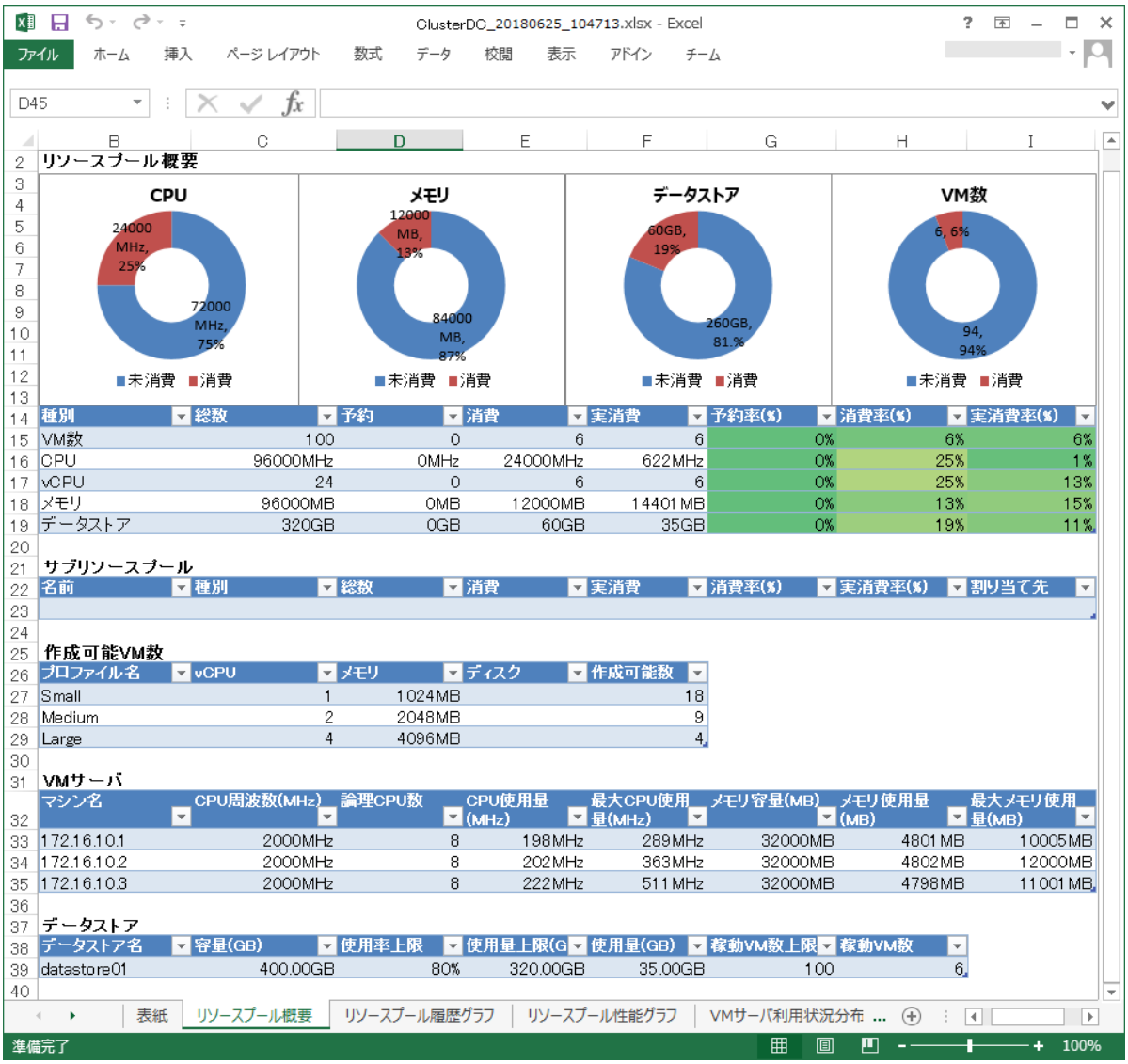


図 「リソースプール概要」のレポート表示画面

6.3.2 業務用仮想マシンの負荷履歴レポート

「6.2.2 個別の仮想マシンのレポート作成（40 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/sigmasystemcenter/kinoulist.html?#report

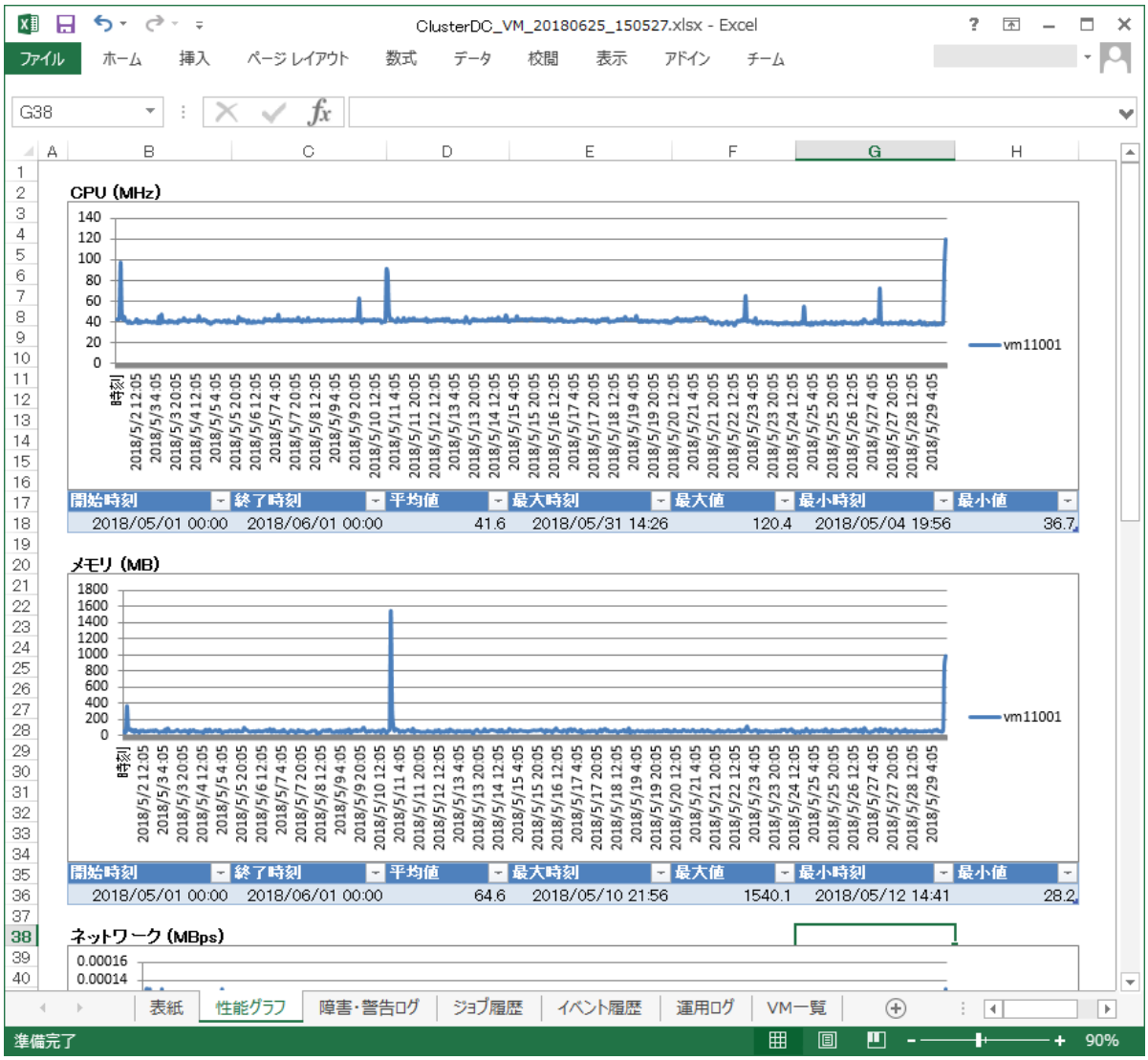


図 「性能グラフ」のレポート表示画面

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[HV01]、[HV02]、[HV03]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[HV01]、[HV02]、[HV03]の電源制御や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（46 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（50 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（55 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[HV01]の iLO（BMC）の管理 LAN の設定を行います。[HV01]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。

図　iLO 5 の管理 LAN の設定

◇<u>ローカルユーザアカウントの作成</u>

次に、物理サーバ[HV01]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
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 SSC
ログイン名 SSC
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

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
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
新しいパスワードを入力します。
****
新しいユーザー情報:
新しいユーザー名 SSC
ログイン名 SSC
パスワード
入力するにはEnterキーを押してください
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 のローカルユーザアカウントの作成

◇**IPMI 通信の有効化**

次に、物理サーバ[HV01]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。

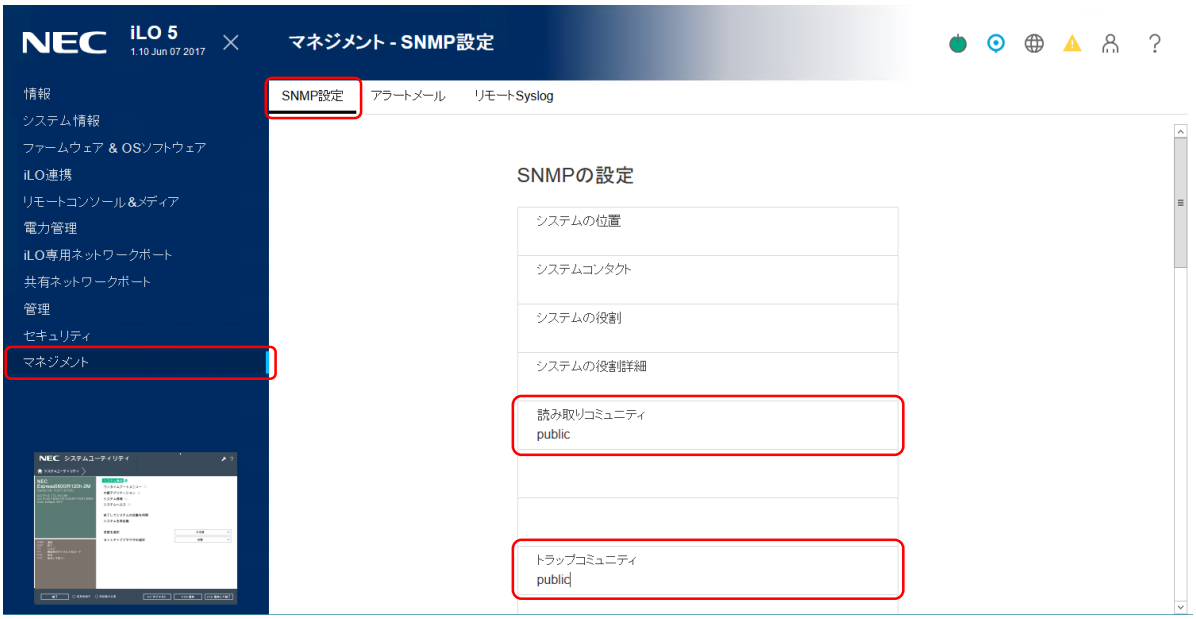


図　iLO 5 の SNMP の設定

物理サーバ[HV02]、[HV03]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[HV01]の BMC の管理 LAN の設定を行います。[HV01]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。

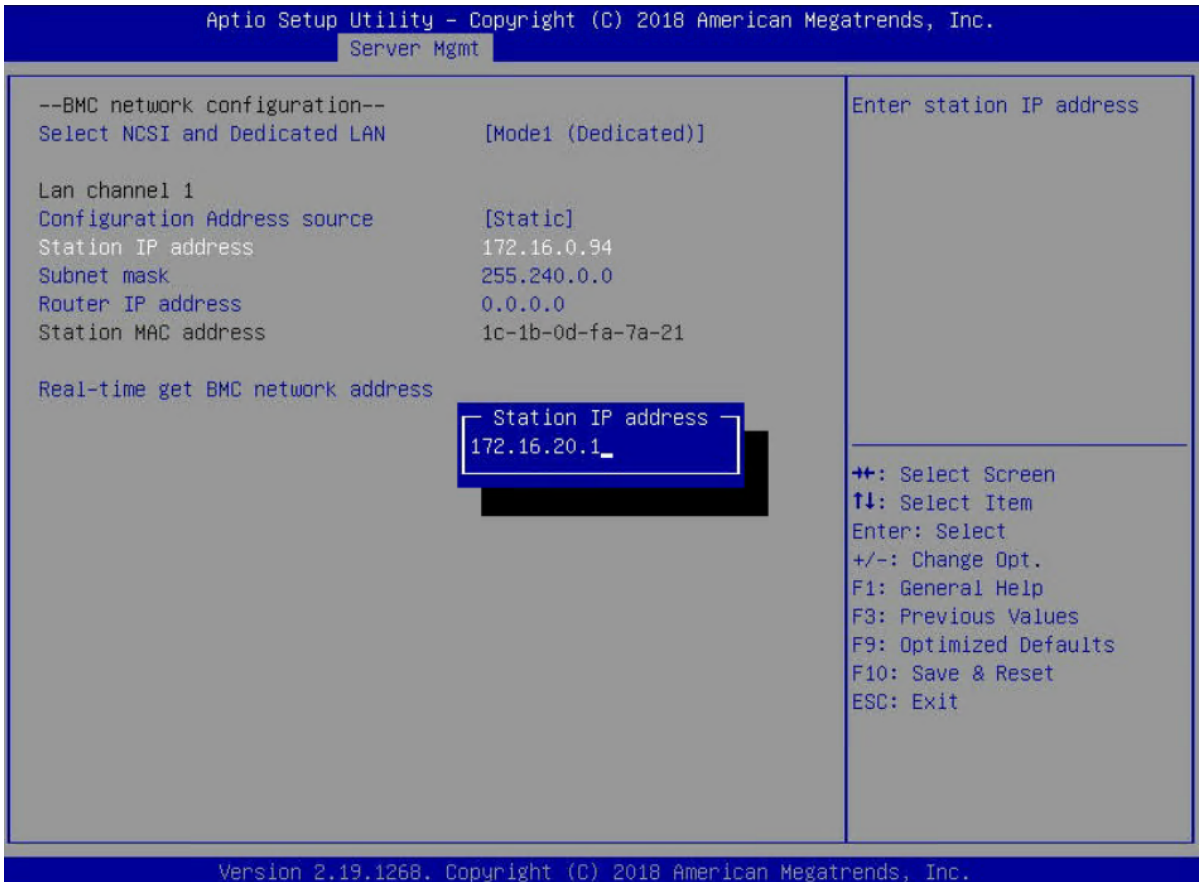


図　マネージメント LAN 設定

◇<u>管理者権限のあるユーザーの作成</u>

次に、物理サーバ[HV01]の BMC のリモートマネジメントで、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. 左ペインのメニューから、[EMS]→[設定]→[ユーザー]をクリックします。
2. メインペイン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。

図　ユーザーの選択

3. メインペイン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. メインペイン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

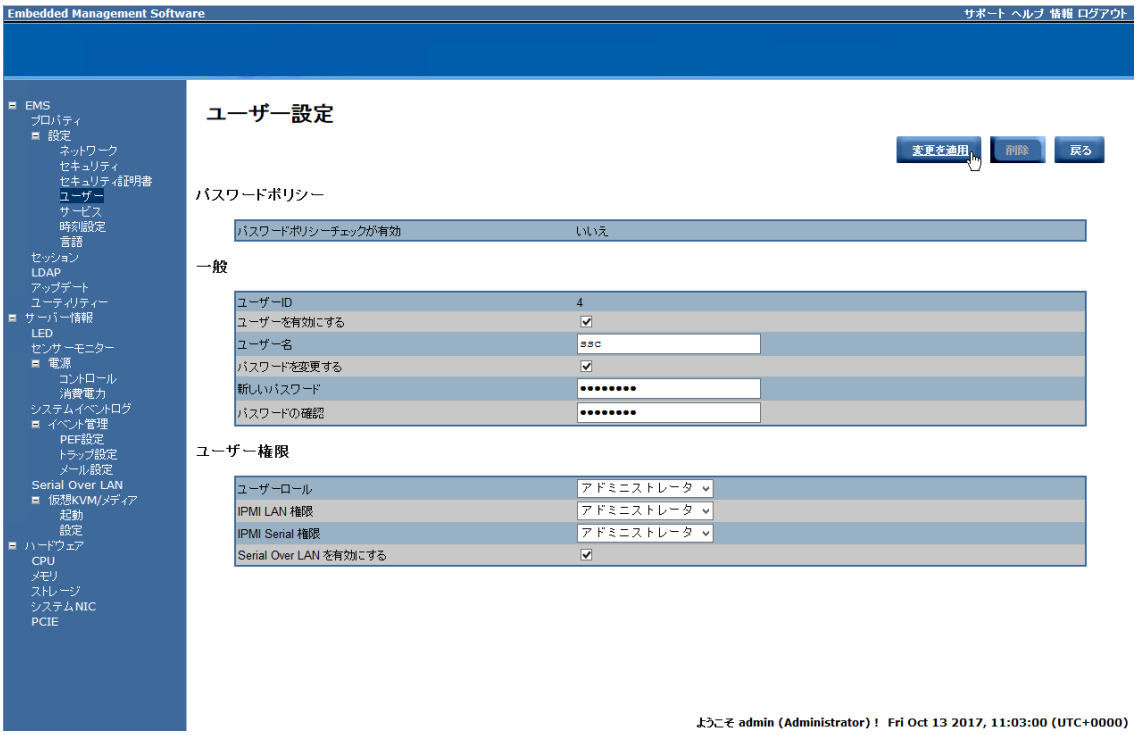


図　ユーザーの追加

5. メインペイン右上の[変更を適用]をクリックします。

◇<u>トラップ設定</u>

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。

1. 左ペインのメニューから、[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。

2. メインペインの 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

3. メインペイン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

4. メインペイン右上の[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。

1. 左ペインのメニューから、[サーバー情報]→[イベント管理]→[PEF 設定]をクリックします。
2. メインペイン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

3. メインペイン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

4. メインペイン右上の[変更を適用]をクリックします。

図　PEF 設定

物理サーバ[HV02]、[HV03]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[HV01]、[HV02]、[HV03]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[HV01]（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、"sscadmin"）
- 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（46 ページ）」/「7.1.2　Express5800/D120h などの BMC/CMC の設定（50 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 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[HV01]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、[HV02]と[HV03]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、Hyper-V クラスタ下のデータセンターを選択して、データセンター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の変更が必要です。

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[ClusterDC]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。

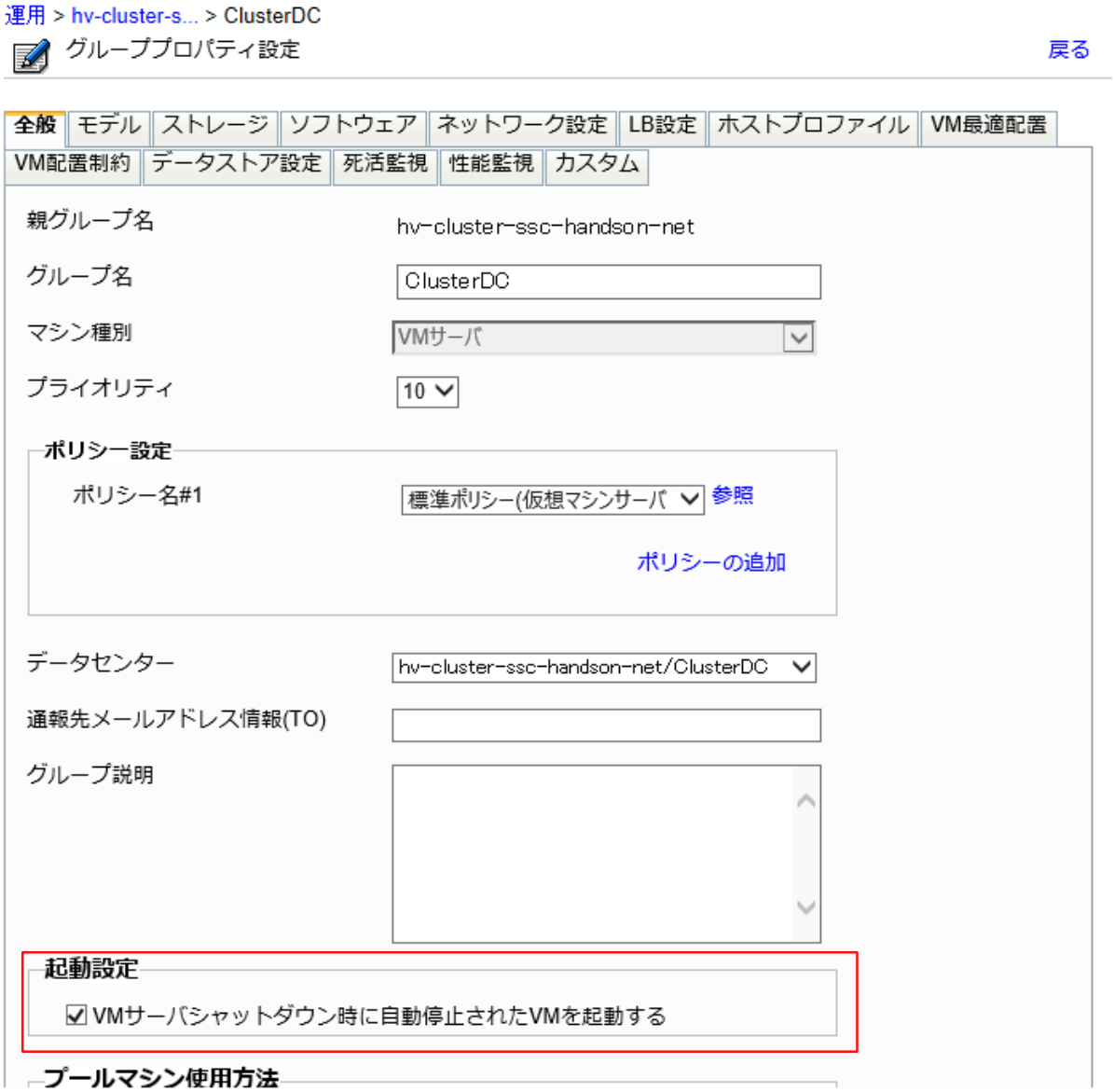


図 「グループプロパティ設定」画面の[全般]タブ

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[ClusterDC]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、[ClusterDC]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)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。

[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。

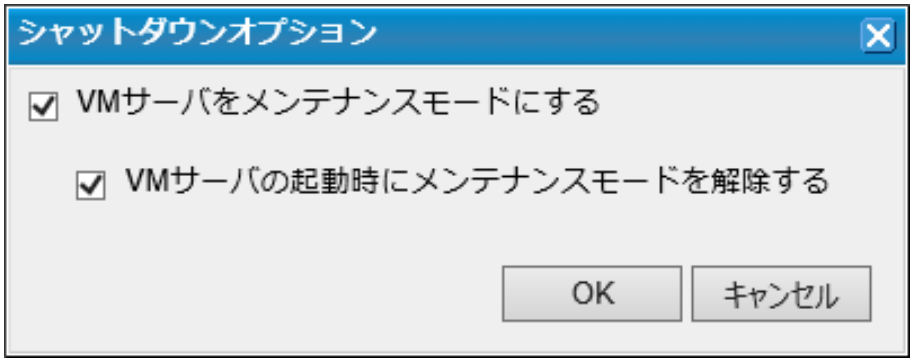


図 「シャットダウンオプション」画面

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。

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[ClusterDC]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、[ClusterDC]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（58 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 SimgaSystemCenter 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 2 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。

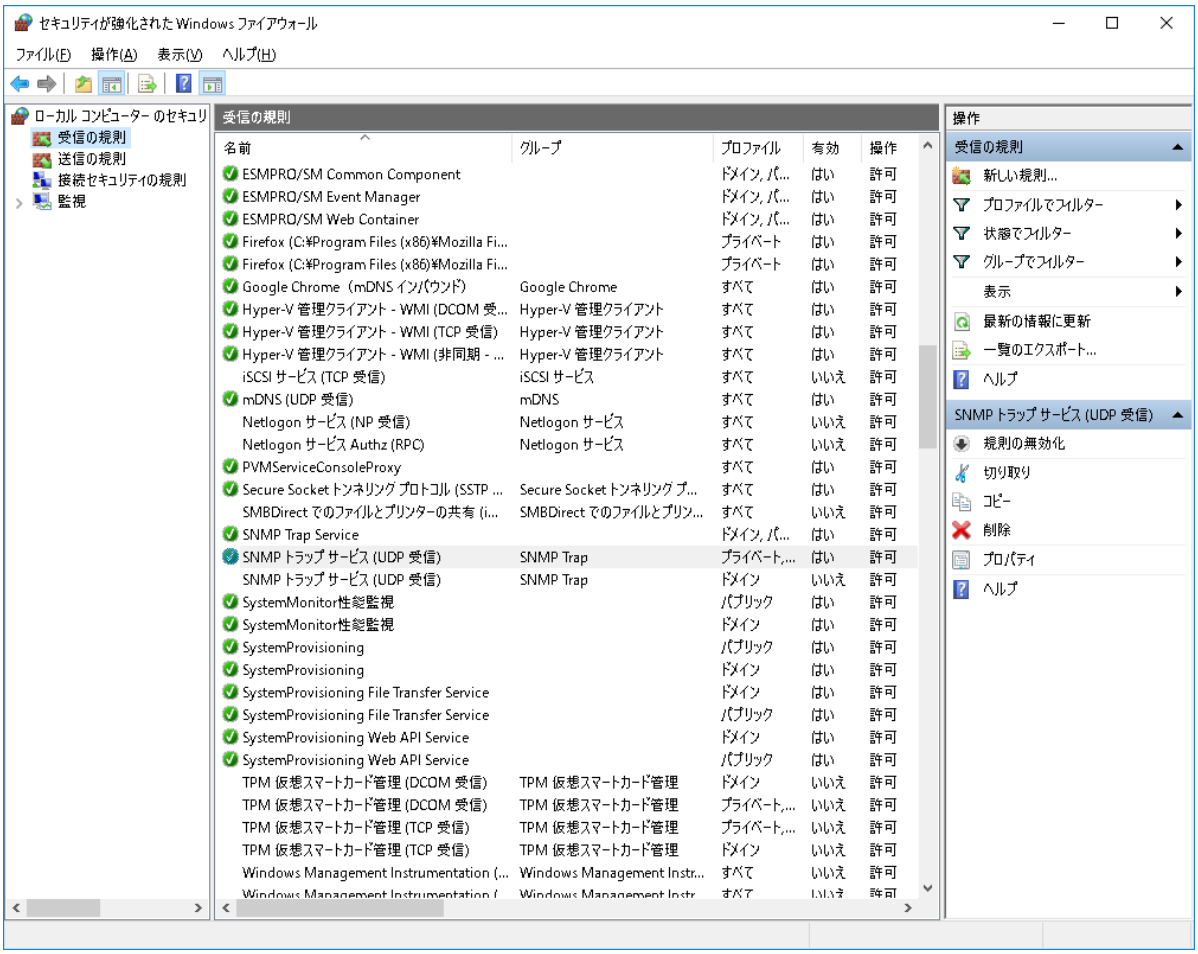


図　セキュリティが強化された Windows ファイアウォール（SNMP トラップ サービス (UDP 受信)）

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)]、[プロトコル]が[ICMPv4]の規則が追加されたことを確認します。

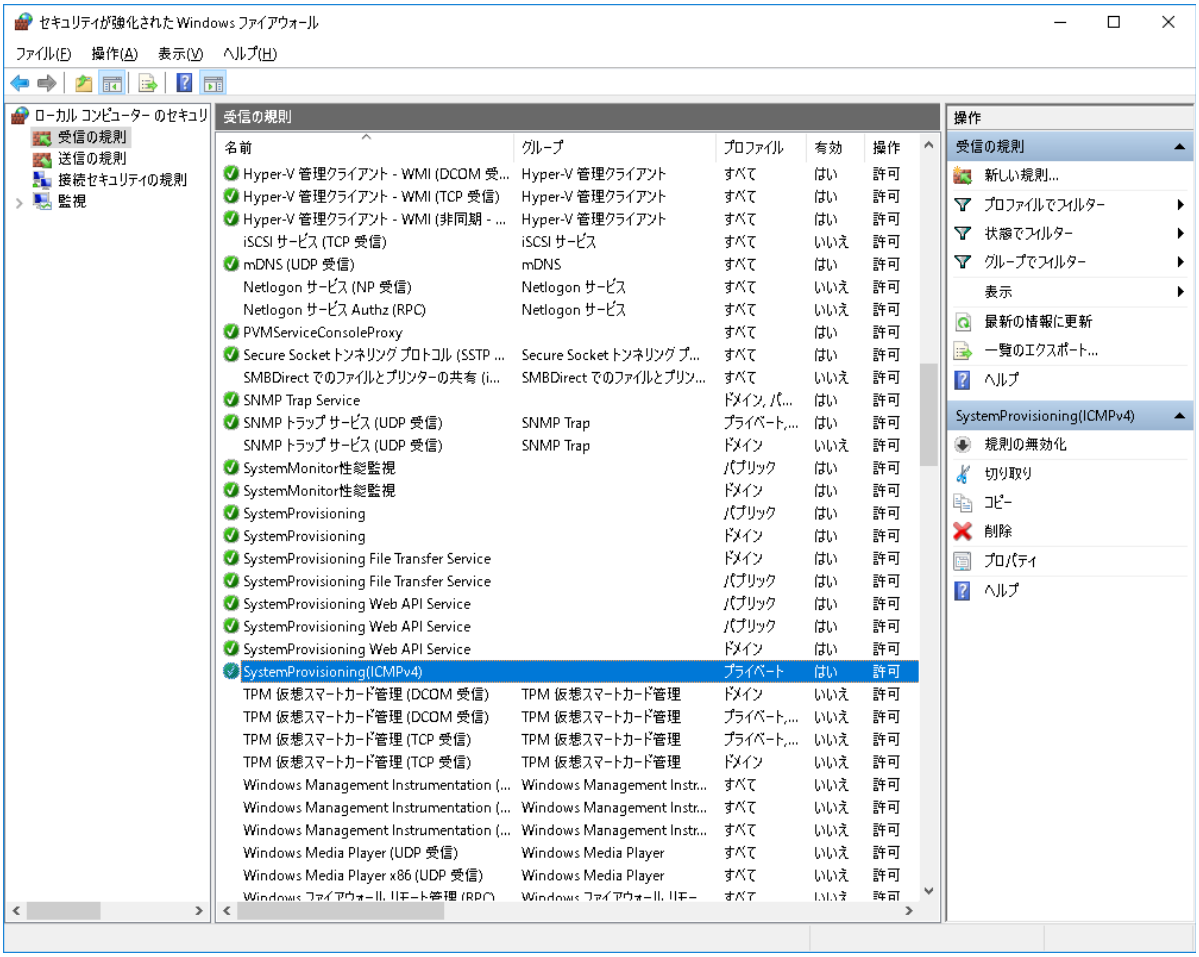


図　セキュリティが強化された Windows ファイアウォール（SystemProvisioning(ICMPv4)）

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、ど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 2 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]をクリックして「環境設定」画面を開き、[通報]タブをクリックします。

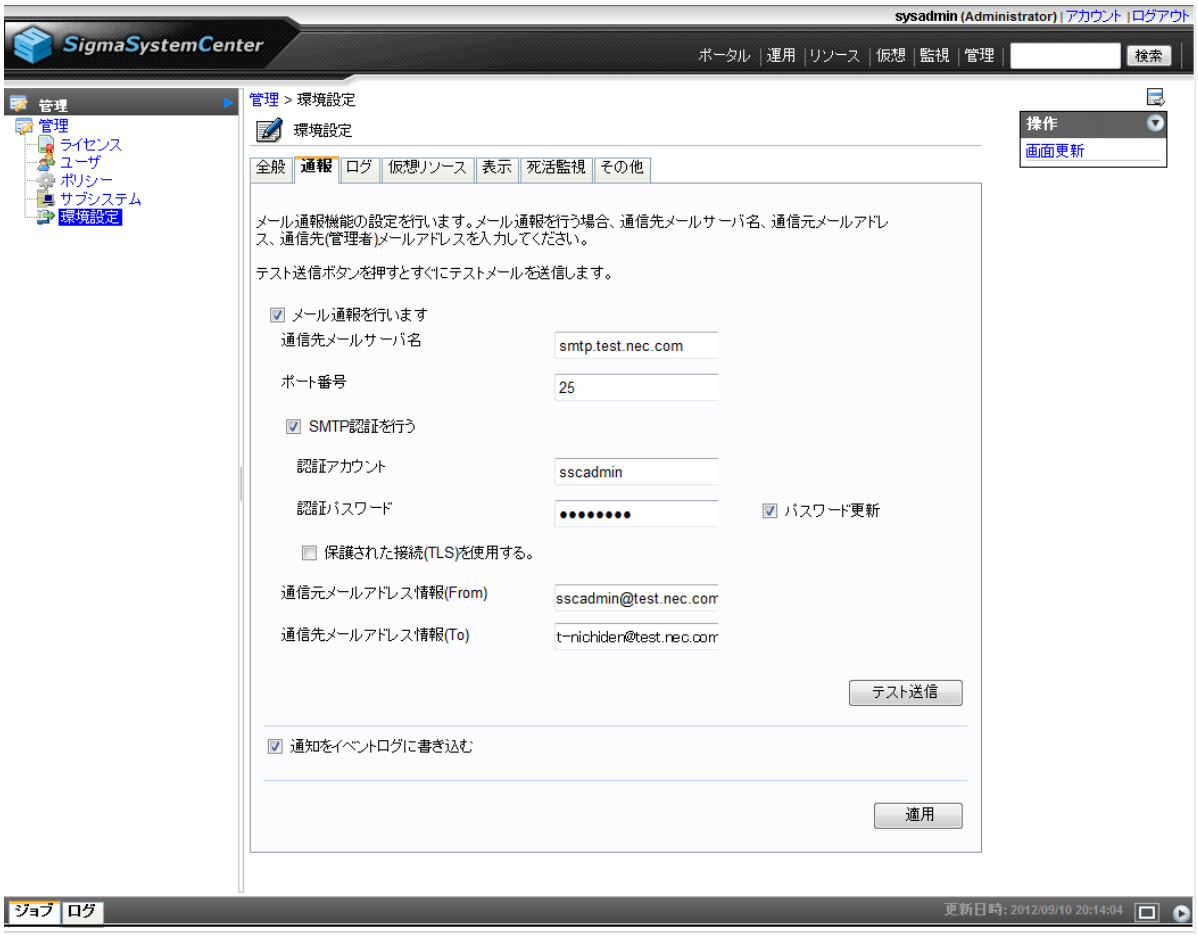


図 「環境設定」画面（[通報]タブ）

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	ー
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。

6 章で仮想マシンの負荷状況の取得方法(「6.1.2 業務用仮想マシンの負荷状況取得の設定(32 ページ)」参照)について説明しましたが、本章では仮想マシンに負荷監視を行う方法について説明します。

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。

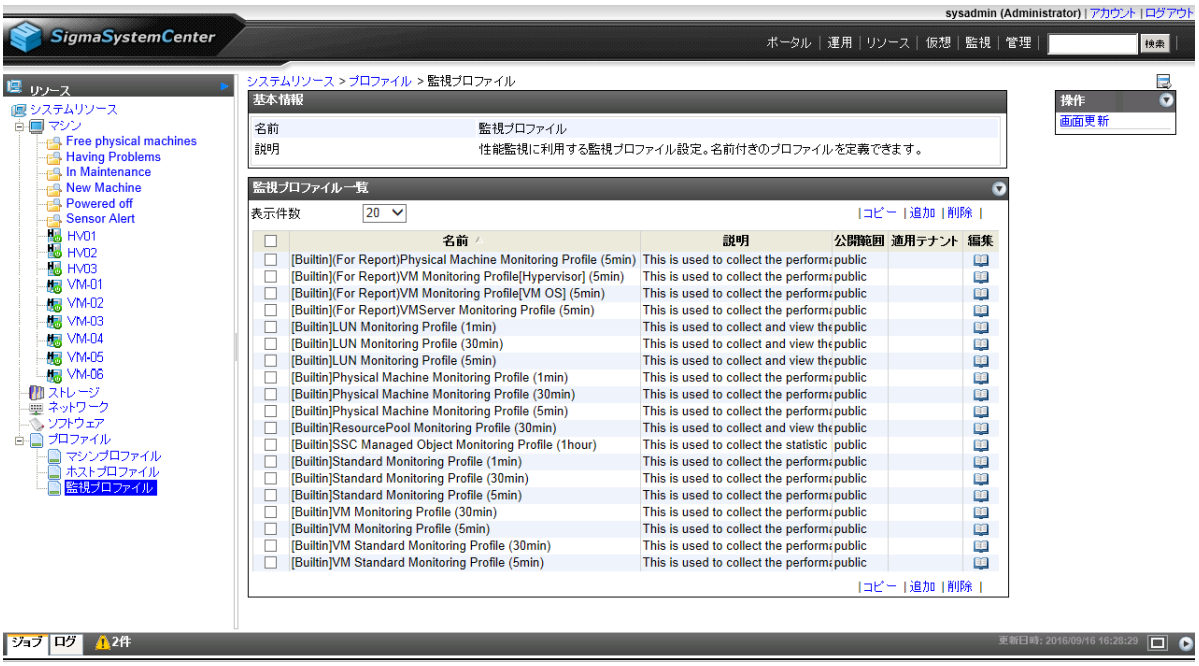


図　監視プロファイル一覧

[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。

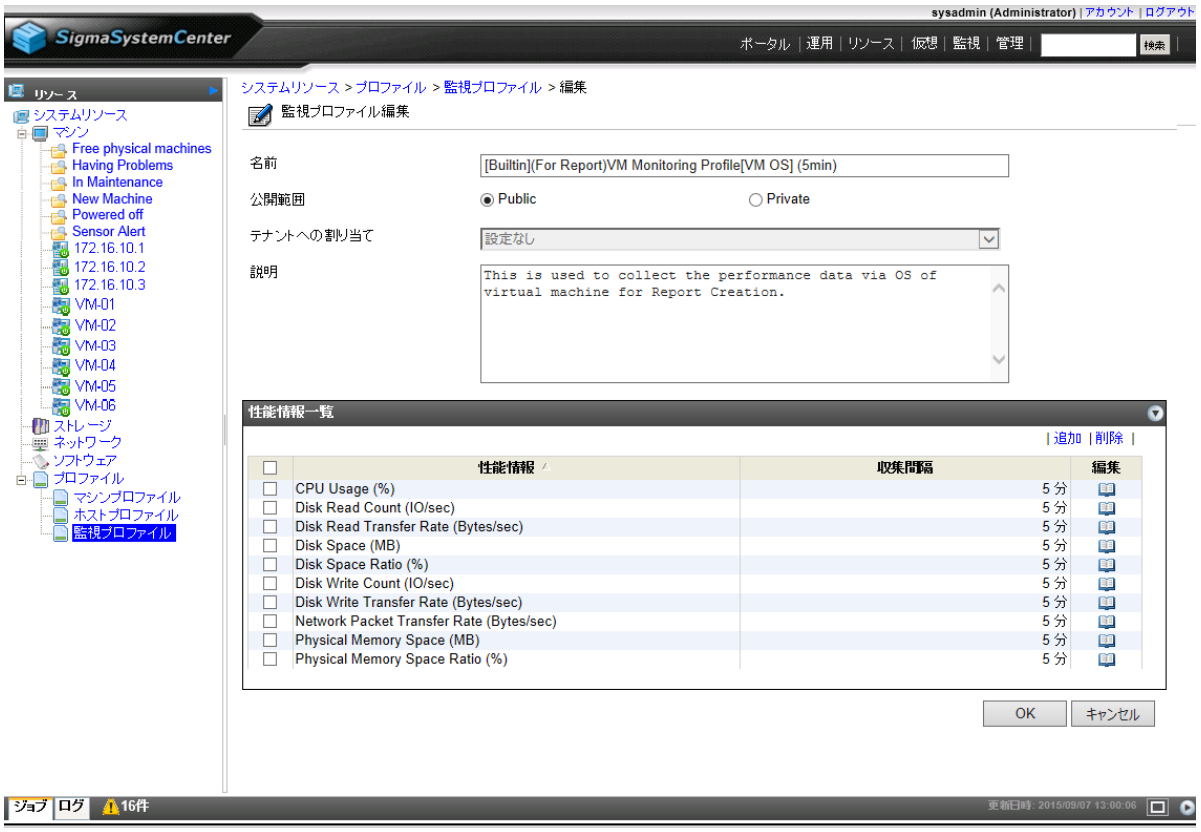


図　監視プロファイル編集

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 (%) について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）

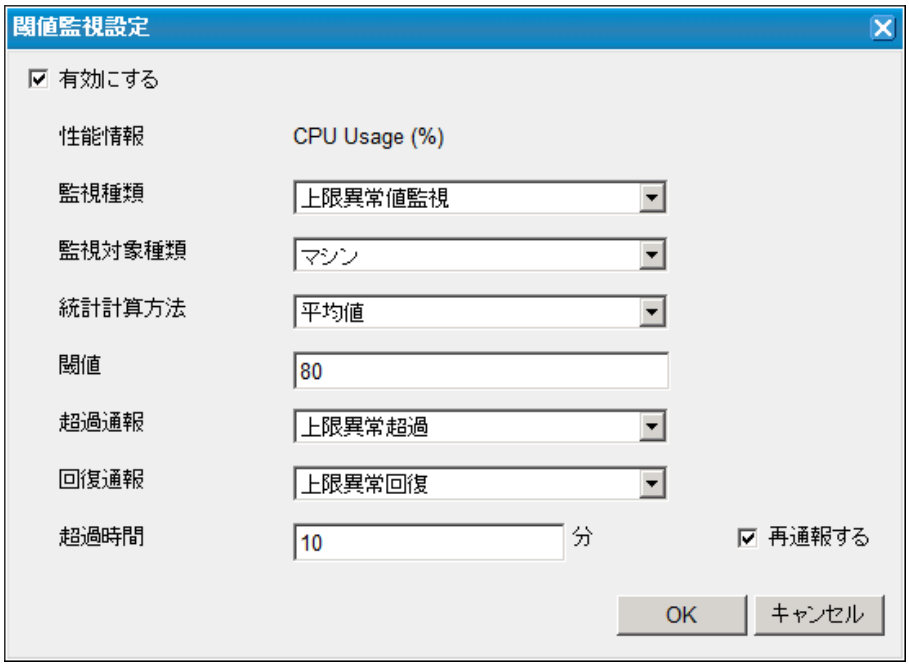


図　CPU Usage (%) の「閾値監視設定」

[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。

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 (%) についての設定を変更するために、Physical Memory Space Ratio (%) 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　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）

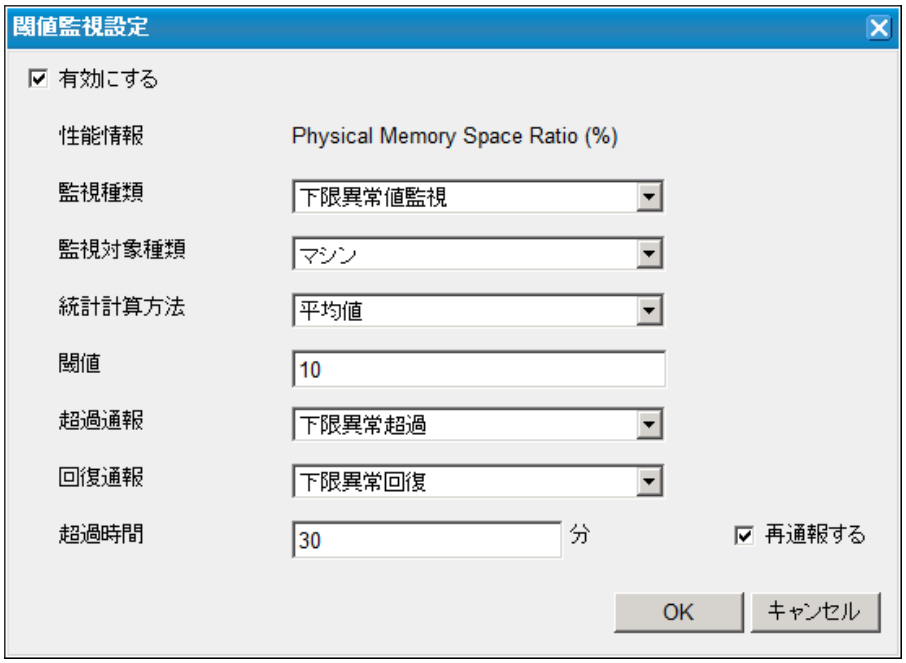


図　Physical Memory Space Ratio (%) 性能監視設定

[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。

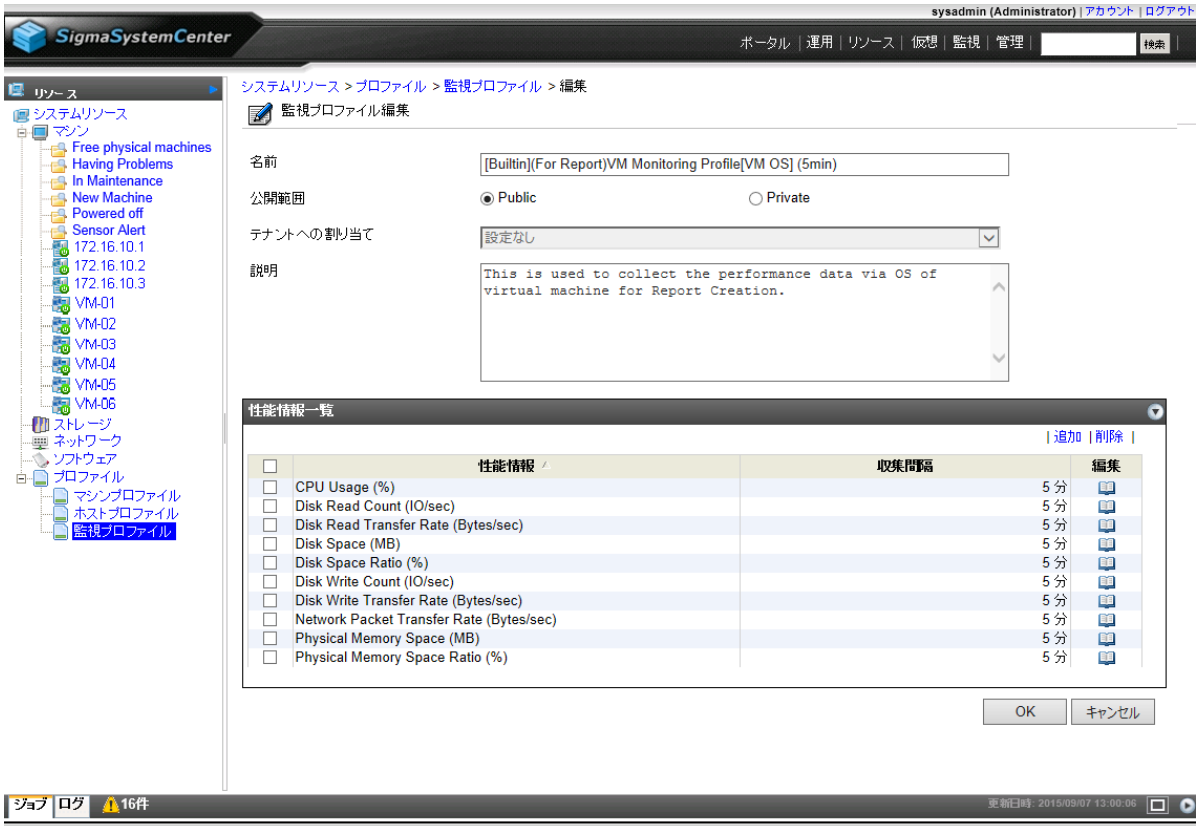


図　性能情報一覧

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 死活監視と ESMPRO/ServerManager の設定

死活監視を行うには、「8.1.3 死活監視の基本設定（68 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。

8.3.1 仮想マシンの設定

まずは、仮想マシンの死活監視の設定のため、[ClusterDC_VM]グループの設定を行うことにします。[ClusterDC_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（82 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、[ClusterDC_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[ClusterDC_VM]グループをクリックします。
2. [設定]メニューの[プロパティ]をクリックします。
3. 「グループプロパティ設定」画面が開いたら、[死活監視]タブをクリックします。
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します。
5. [Ping 監視]チェックボックスをチェックします。
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"を入力します。
7. 右下の[適用]をクリックします。

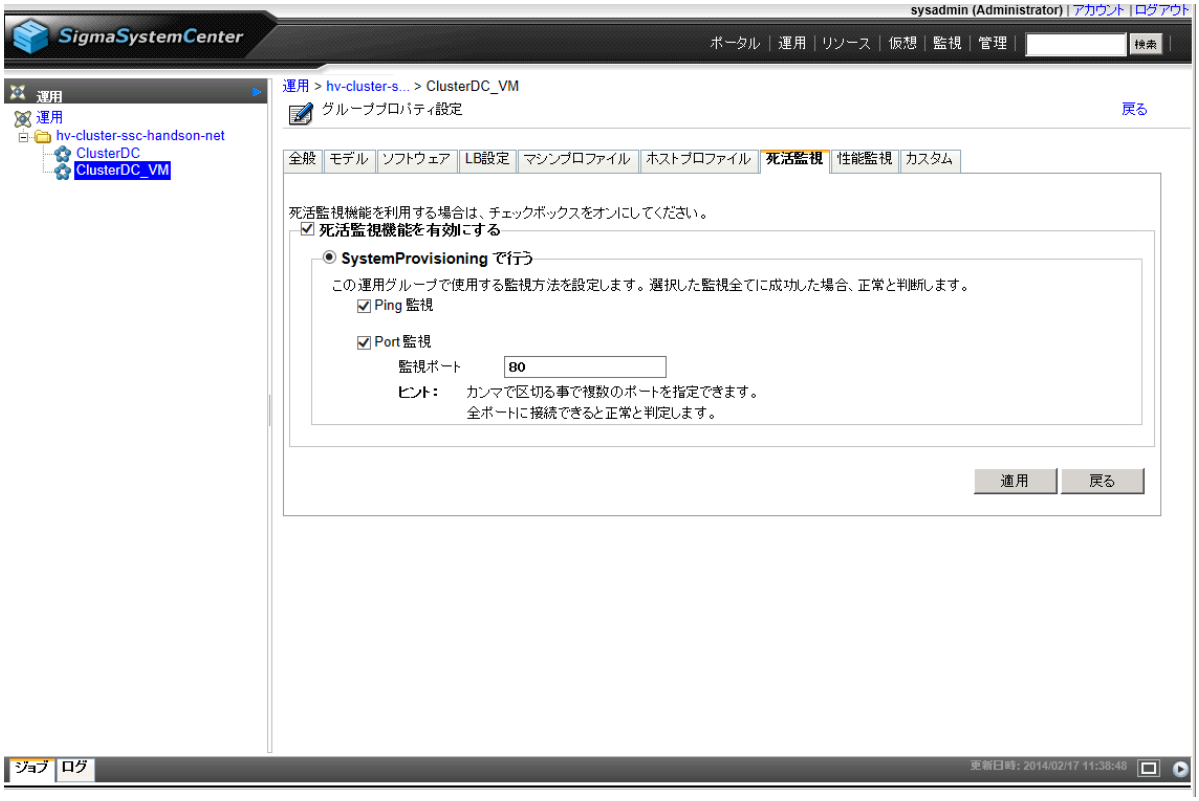


図　[ClusterDC_VM]グループの「グループプロパティ設定」画面（[死活監視]タブ）

8.3.2　死活監視と ESMPRO/ServerManager の設定

次に、物理サーバの死活監視、および ESMPRO/ServerManager の設定について説明します。

[ClusterDC]グループの物理サーバについては、後述(「8.4.3　物理サーバ用ポリシーの確認と適用（85 ページ）」を参照）にて適用する[仮想マシンサーバ用ポリシー(Hyper-V)]で、Windows Server Failover Cluster を利用した死活監視のイベント（クラスタノード停止）に対処するようになっています。

そのため、ESMPRO/ServerManager の死活監視については、利用する必要はありません。

しかし、ディスク障害監視などの監視は、ESMPRO/ServerManager を利用する必要があります。これらの監視を行うためには、SSC で管理しているマシンを ESMPRO/ServerManager へ登録する必要がありますので、以下に登録方法について説明します。

次の手順で、[ClusterDC]グループの物理サーバを ESMPRO/ServerManager に登録してください。

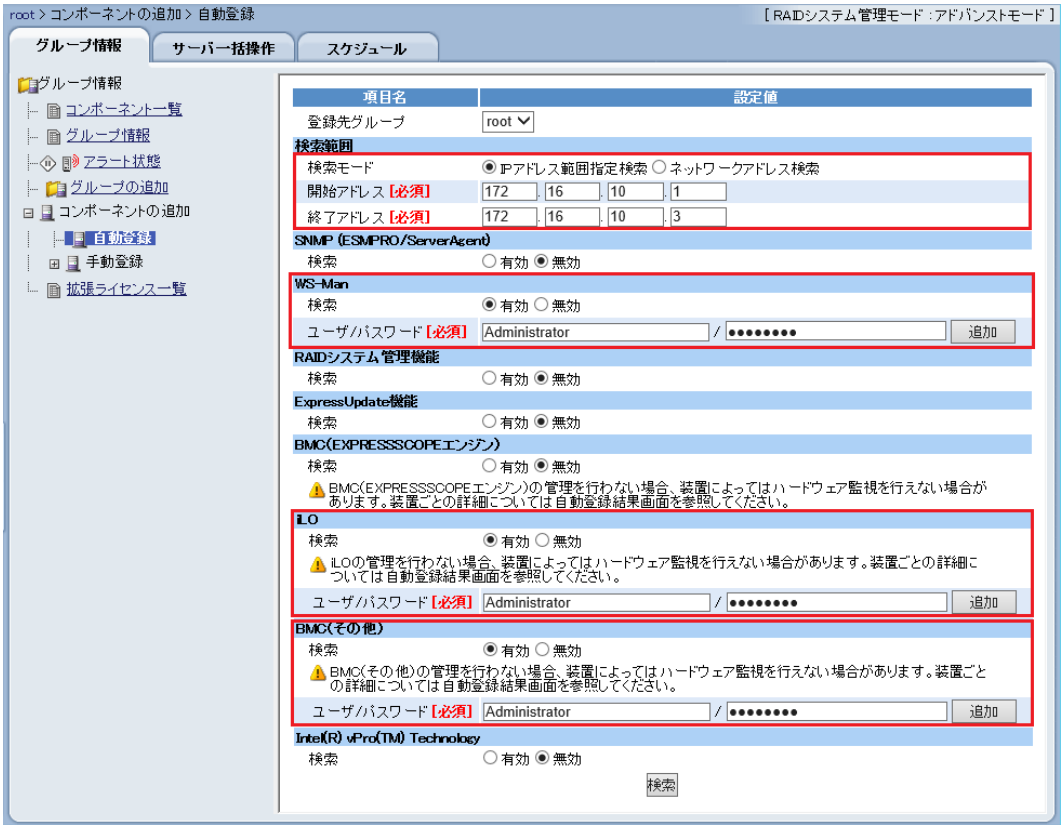
※登録対象の管理対象マシンに、ESMPRO/ServerAgentService がインストールされている前提です。

1. ESMPRO/ServerManager の WebGUI にログインします。
2. [グループ情報] タブの[コンポーネントの追加] － [自動登録] を選択します。
3. IP アドレス範囲指定検索で、各物理サーバの IP アドレスを含む範囲を指定します。

また、[WS-Man]の設定を行い、[iLO] または [BMC(その他)] の設定を有効にします。

- [検索範囲]
  - [開始アドレス]: 172.16.10.1
  - [終了アドレス]: 172.16.10.3
- [WS-Man]の[有効]ラジオボタンを選択
  - [ユーザ/パスワード]には、各物理サーバの WindowsOS の管理者権限のアカウントの設定を行います。
- [iLO](Express5800/R120h,T120h など)、または、[BMC(その他)](Express5800/D120h など) のいずれかの[有効]ラジオボタンを選択
  - [iLO]を選択した場合は、[ユーザ/パスワード]には、各物理サーバの iLO のアカウントの設定を行います。
  - [BMC(その他)]を選択した場合は、[ユーザ/パスワード]には、各物理サーバの BMC のアカウントの設定を行います。

4. 必要に応じて各項目の設定を行い、[検索] をクリックします。
5. 検索結果は、[登録されたコンポーネント] - [設定タブ] - [接続設定]で確認することができます。手順 3.で有効にした各管理機能が、登録<有効>になっていることを確認してください。



注

なお、設定変更は不要ですが、デフォルトでは[ClusterDC]グループの「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。

[ESMPRO/SM にマシンを登録する]と[死活監視を有効にする]チェックボックスのチェックは、サブシステムの設定に[マシンを運用グループへ自動登録する]のチェックがある場合、有効になり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、前述の通り、ESMPRO/ServerManager の画面から行う必要があります。

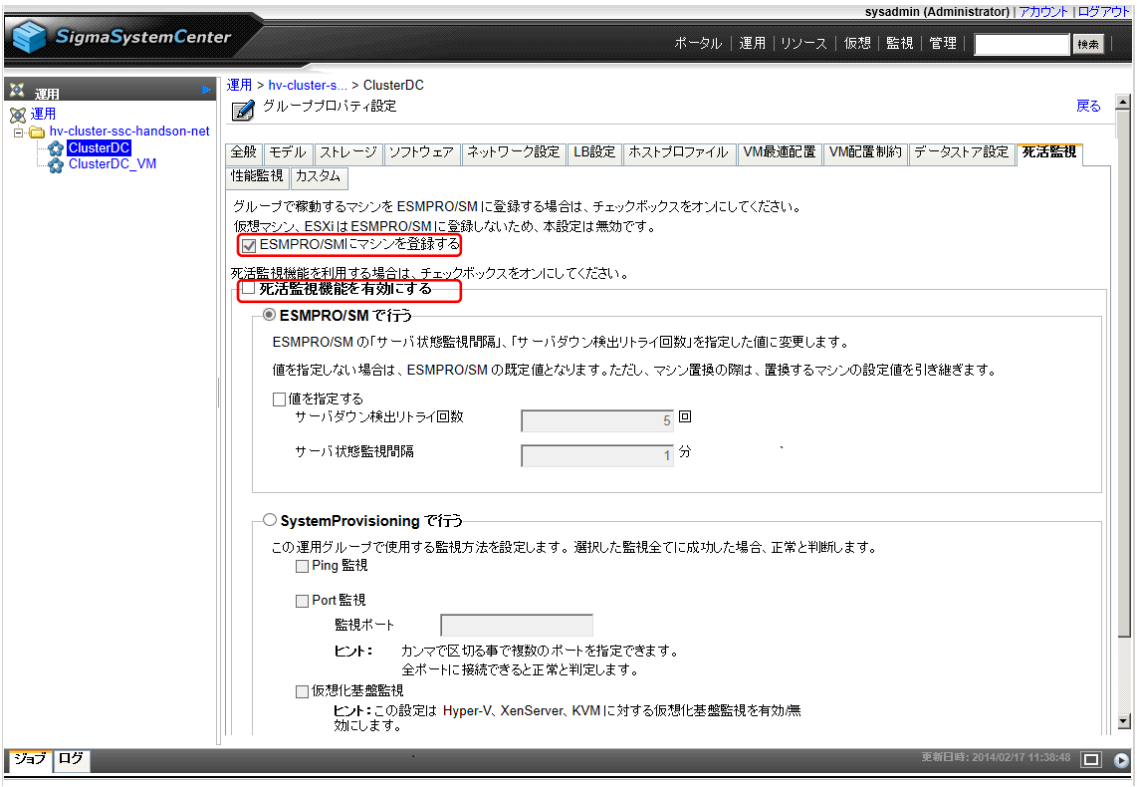


図 [ClusterDC]グループの「グループプロパティ設定」画面（[死活監視]タブ）

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(Hyper-V)

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
- hvcluster_policy.xml ：物理サーバ（Hyper-V ホスト）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[hvcluster_policy.xml]もインポートしてください。

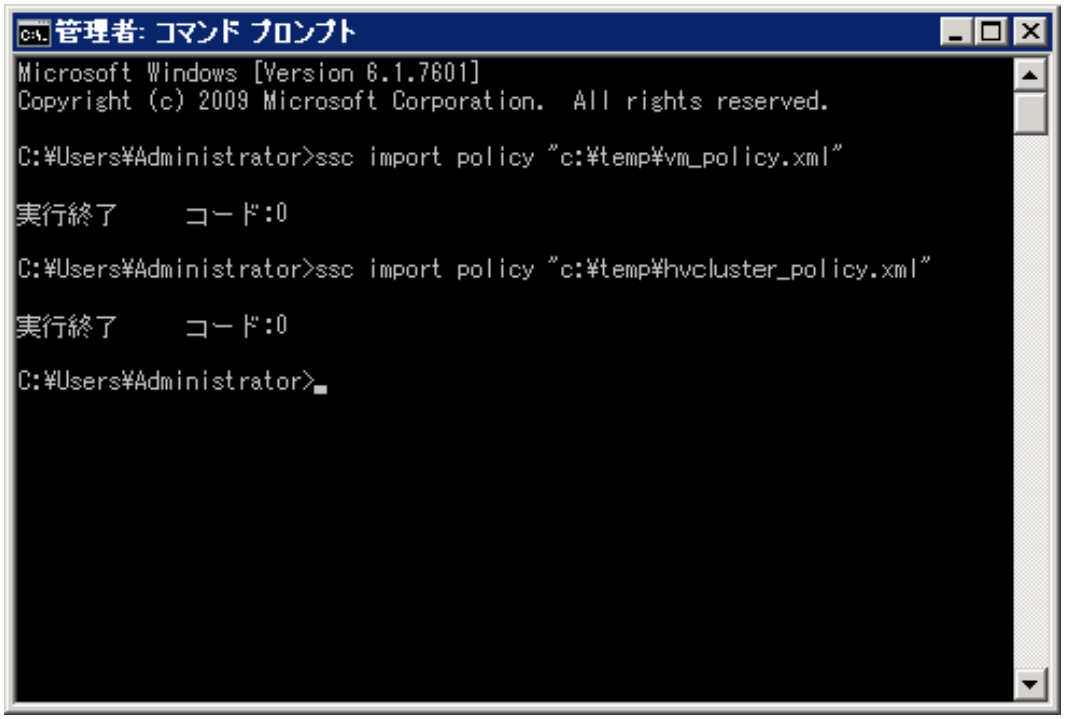


図　ssc コマンドによるポリシーのインポート（インポート実行後）

2 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。

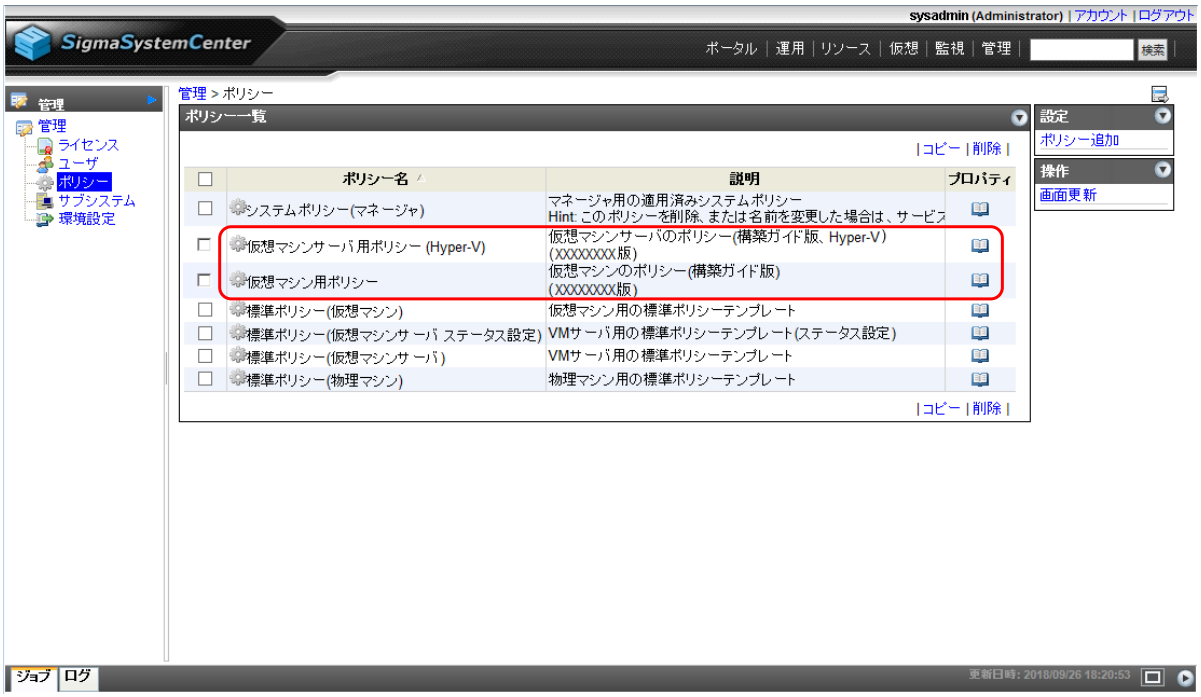


図　ポリシー一覧（インポート後）

ポリシー一覧に、「仮想マシンサーバ用ポリシー(Hyper-V)」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（[ClusterDC_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。

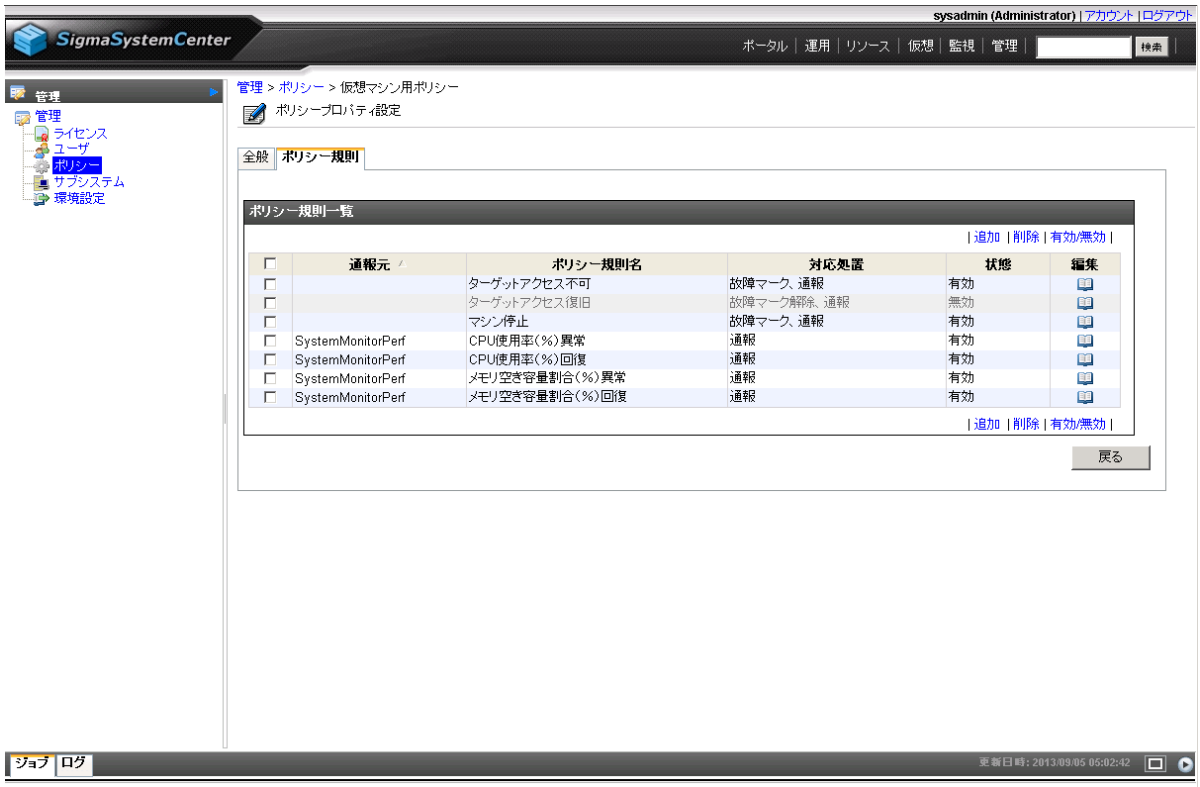


図 「ポリシープロパティ設定」画面（[ポリシー規則]タブ）

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。

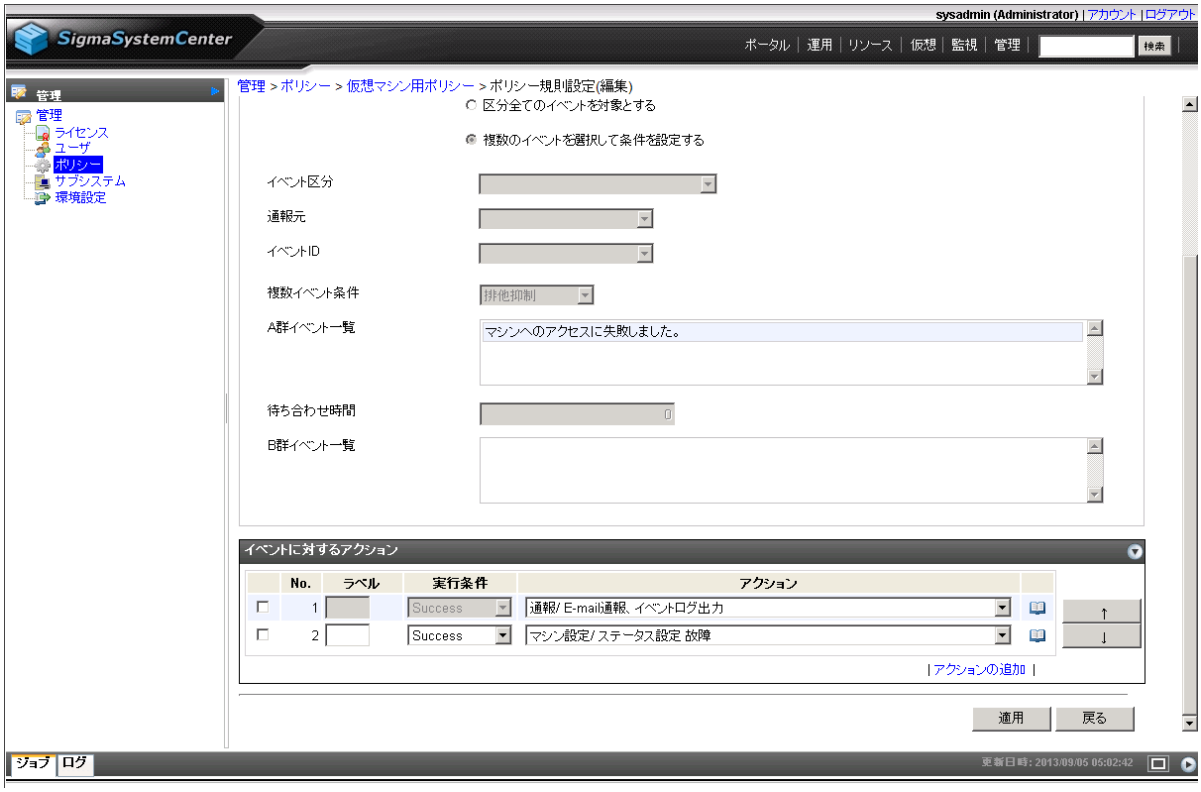


図　対応処置詳細設定（編集）

(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、[ClusterDC_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[ClusterDC_VM]）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[仮想マシン用ポリシー]）を選択します。
6. 右下の[適用]をクリック後、[戻る]をクリックします。

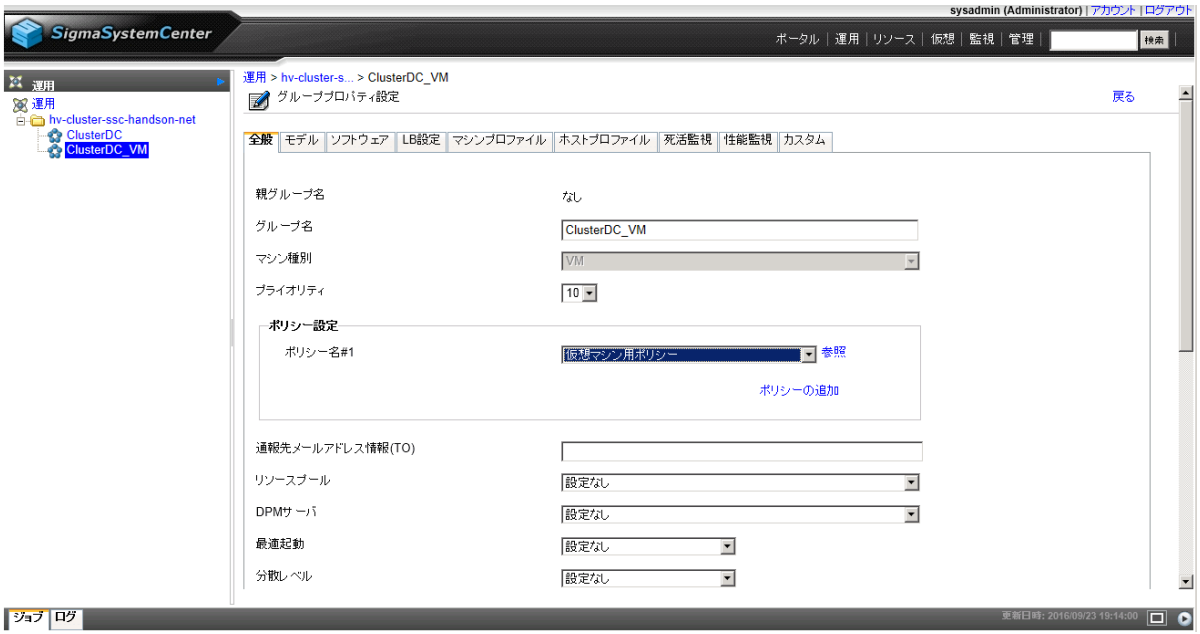


図　仮想マシン用ポリシーの適用

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 Hyper-V ホスト用のポリシーを用意します。物理サーバのグループ（ClusterDC 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 Hyper-V ホスト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(Hyper-V)]です。[仮想マシンサーバ用ポリシー(Hyper-V)]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、[監視イベント]タブをクリックします。

[イベントに対する対応処置一覧]の枠の[イベント状態]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(Hyper-V)]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。

- <u>イベント発生時点、Hyper-V ホストが機能停止している可能性が高い障害</u>

  対処として、故障マーク設定、通報、イベントログ出力を行います。

他の仮想化ホストへの仮想マシンの移動と再起動は、Windows Server Failover Cluster によって実行されます。

「CPU 温度異常」、「クラスタノード停止」が該当します。

- イベント発生時点、Hyper-V ホストは稼動しているが、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、仮想マシンの移動(Migration(ライブマイグレーション))により他の Hyper-V ホストへ仮想マシンを稼動させたままの移動を行います。

  仮想マシンの移動処理前または処理中に障害が進行しホストダウンに至った場合には、上の「イベント発生時点、Hyper-V ホストが機能停止している可能性が高い障害」として、Windows Server Failover Cluster によって移動と再起動の対処が実施されます。

  「予兆：○○」が該当します。

- イベント発生時点、ディスクに異常がある場合

  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、仮想マシンの移動(Migration(ライブマイグレーション))により他の Hyper-V ホストへ仮想マシンを稼動させたままの移動を行います。

  仮想マシンの移動処理前または処理中に障害が進行しホストダウンに至った場合には、上の「イベント発生時点、Hyper-V ホストが機能停止している可能性が高い障害」として、Windows Server Failover Cluster によって移動と再起動の対処が実施されます。

  「ディスク障害(ESMPRO 警告)」が該当します。

- 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。

  「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。

  「CPU 障害」、「メモリ障害」、「ネットワークインタフェース障害」が該当します。

- Hyper-V ホストの負荷が設定したしきい値を上回った（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。

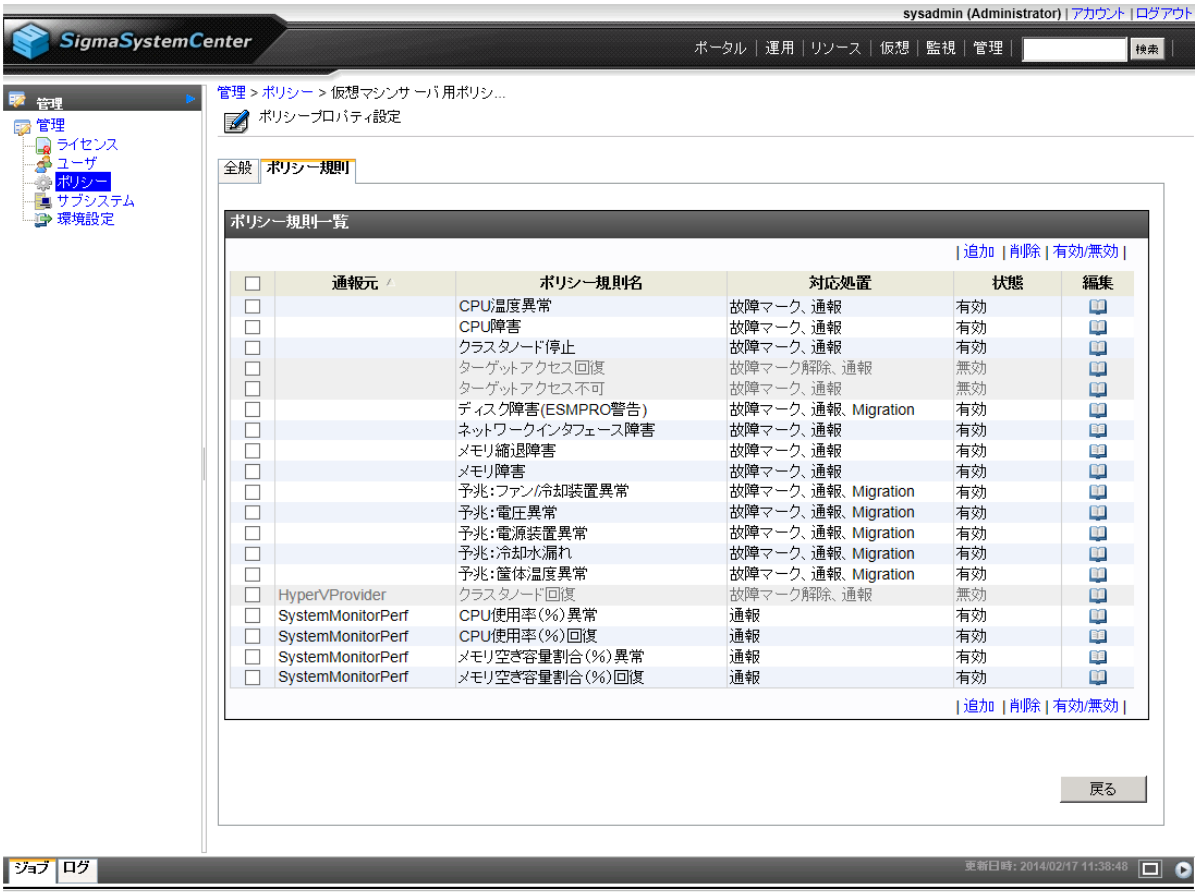


図　仮想マシンサーバ用ポリシー(Hyper-V)の[ポリシー規則]タブ

(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である Hyper-V ホストは、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 Hyper-V ホストでは、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 Hyper-V ホストは、仮想マシンの移動(Migration(ライブマイグレーション))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、Hyper-V ホストの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、Hyper-V ホスト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状態を解除したい Hyper-V ホストをクリックします。
3. Hyper-V ホスト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、故障状態を解除したい Hyper-V ホストをクリックします。
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、基本的には管理者が Hyper-V ホストに問題ないことを確認し、手動で故障状態を解除することをお勧めします。

8.4.4 物理サーバ用のポリシーの適用

監視イベントを確認したところで、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物理サーバに行います。

物理サーバ[HV01]、[HV02]、[HV03]にポリシーを適用するために、[Hyper-V]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(Hyper-V)]を適用します。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「Hyper-V」）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]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(Hyper-V)」）を選択します。
6. [適用]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、ひとまず動作テストを行ってみます。今回は物理サーバ[HV01]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(Hyper-V)]の[ディスク障害(ESMPRO 警告)]イベントへの対応処置をテストします。

「8.4.3 物理サーバ用ポリシーの確認と適用（85 ページ）」で説明したとおり、[ディスク障害(ESMPRO 警告)]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 Hyper-V ホストへの移動です。テストでは、SSC の GUI で擬似障

害を発生させた物理サーバ[HV01]に故障マークが付き、[HV01]上の仮想マシンが他のHyper-V ホストに移動されることを確認します。

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。

```
> sendevent localhost SystemMonitorEvent "ESMSTORAGESERVICE[0X800403E9]"
 test hv-cluster-ssc-handson-net¥ClusterDC HV01
```

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[ClusterDC]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、[ClusterDC]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、物理サーバ[HV01]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[Hyper-V]のリソース[HV01]をクリックし、リソースの状態を確認します。

下の図のように、[リソース]ビューでリソース[HV01]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:/hv-cluster.ssc-handson.net/ClusterDC/HV01]をクリックし、[仮想]ビューを確認します。

下の図のように、[仮想]ビューのツリービュー上でも物理サーバ[HV01]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 Hyper-V ホストのツリーを展開すると、物理サーバ[HV01]の配下にあった仮想マシン[VM-01]と[VM-02]が、別の Hyper-V 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、物理サーバ[HV01]の配下に仮想マシン[VM-01]と[VM-02]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、F5 キーで全画面を更新し、仮想マシンが移動したことを確認してください。

また、各 Hyper-V 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、物理サーバ[HV01]の[運用情報]の枠の[ハードウェアステータス]の[(状態詳細)]をクリックします。

[HV01]の[状態詳細]が表示され、[状態一覧]の枠の[ディスク(要交換)]の状態が[故障]となっていることが分かります。

図　[HV01]の状態一覧画面

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、物理サーバ[HV01]の配下に戻すために仮想マシン[VM-01]と[VM-02]を移動します。

ツリービューの[HV01]をクリックし、[HV01]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、物理サーバ[HV01]の配下への仮想マシンの移動を行います。

「5.4 手動での仮想マシンの移動(Migration)（24 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 VM 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 VM 配置も、簡単に確認することができます。また、過去の VM 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[Hyper-V]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なったり、[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。

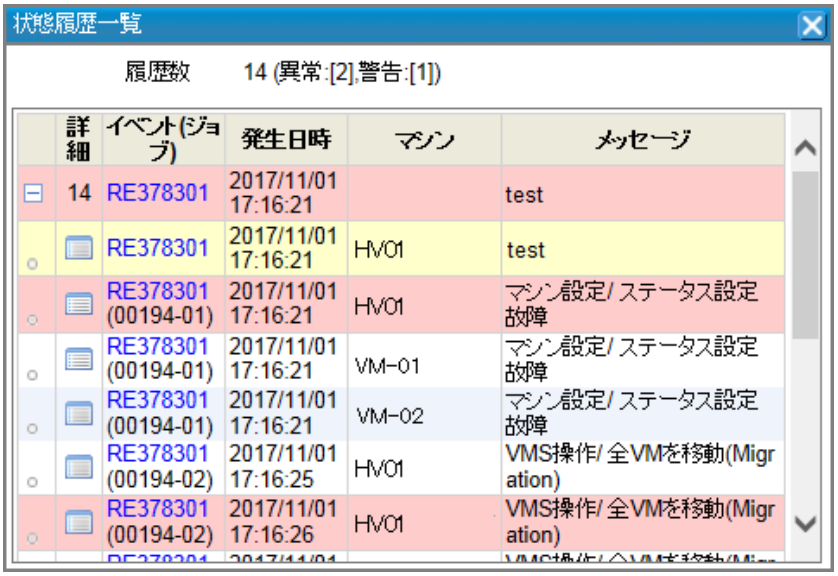
前述で説明しました物理サーバ[HV01]に対して、[故障状態の解除]を実行した後の状態が表示されています。

図　物理サーバ[HV01]の故障状態を解除した後の VM 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。



- 前述の図中に表示されている数字が 2 の黄丸には、物理サーバ[HV01]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。

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 Hyper-V グループの VM 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 VM 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、物理サーバ[HV01]に仮想マシン[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、F5 キーで全画面を更新してみてください。

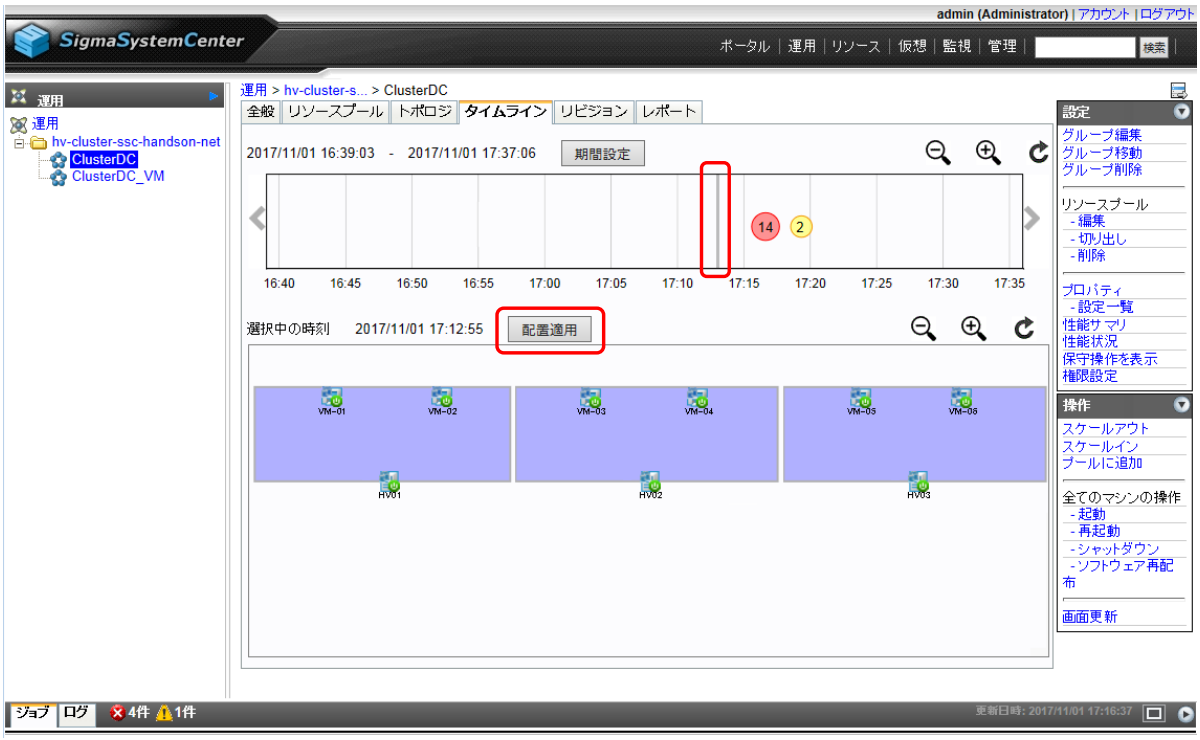


図　擬似障害テスト前の VM 配置

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、Hyper-V マネージャー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

  （※：Windows Server Failover Cluster による動作は問題ありません。）

上記の操作を行った場合、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。

  仮想マシンについて、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、故障マーク設定、通報、イベントログ出力などの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の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（Hyepr-V ホスト）、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（Hyepr-V ホスト）を選択します。

- [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.　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 C.　改版履歴

版数	年月	改版内容
第 1 版	2019.10	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 D.　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 (ベースボードマネー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。

CSV（Cluster Shared Volumes）

Windows Server 2008 R2 以降で Hyper-V のために実装された複数のサーバから同時にアクセスできるファイルシステムです。

Live Migration を行う場合、使用することが推奨されている機能になります。

DataCenter

仮想マシンサーバを束ねる役割を持ちます。Hyper-V クラスタ環境を管理する場合には、クラスタ登録時に 1 つのみ作成され、追加も削除もできません。

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マシンの場合に ESMPRO/ServerManager を介してマシンを監視します。

Hyper-V

Microsoft 社の仮想化技術を指します。Windows Server 2008 以降の一部のエディションに標準で組み込まれています。

Hyper-V クラスタ

クラスタ化された Hyper-V を表します。

Hyper-V マネージャー

Microsoft 社の標準の Hyper-V 管理コンソールです。

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ー管理プロセッサーです。

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ー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ー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。

MSFC(Microsoft Failover Cluster)

Windows Server OS に標準で入っているクラスタリングソフトウェアです。本書では、本機能を利用する前提で説明します。

WSFC(Windows Server Failover Cluster)と表記されることが多いです。

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。

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。

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。

WSFC(Windows Server Failover Cluster)

Windows Server OS に標準で入っているクラスタリングソフトウェアです。本書では、本機能を利用する前提で説明します。

MSFC(Microsoft Failover Cluster)と表記される場合もあります。

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。

Hyper-V クラスタ環境を管理する場合には、クラスタ登録時に 1 つのみ作成され、追加も削除もできません。

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、マシン稼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。

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 Hyper-V 編

SSC0308-doc-0027-1.1

2019 年 12 月 1.1 版 発行

© NEC Corporation 2013 - 2019