SigmaSystemCenter 3.6 簡易構築ガイド VMware 編

SSC0306-doc-0048-1.1

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

はじめに

この文書では、「VMware vSphere」と管理ツールの「WebSAM SigmaSystemCenter 3.6 Update1」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 3.6 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（90 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（89 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。

- 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（ESXi）

- 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（ESXi）

- 予兆障害を契機に vMotion をする。

  物理サーバ（ESXi）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 vMotion 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。

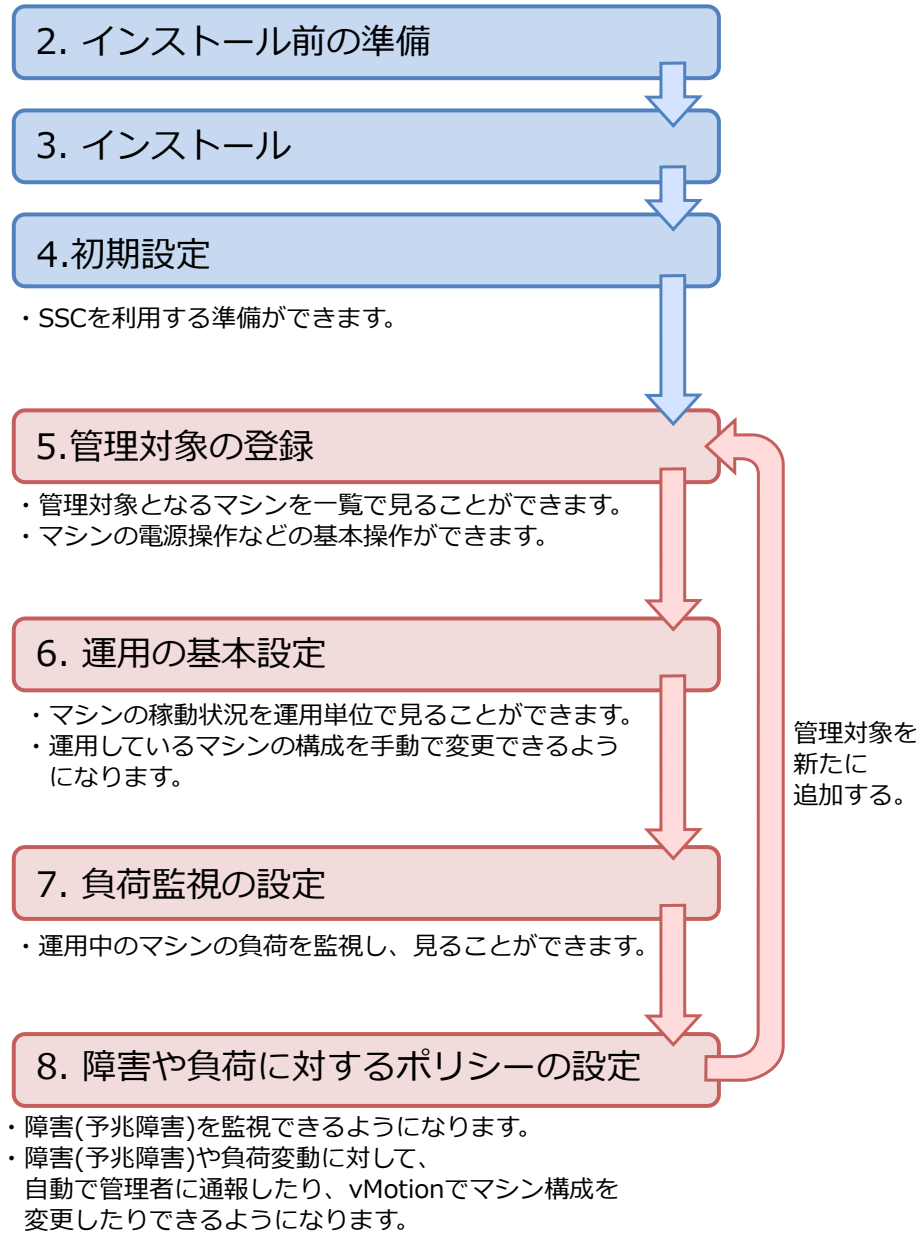


図　本ガイドでの構築の流れ

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）
    - VMware ESXi

        * ホスト名：IP アドレス(管理用ネットワーク)
            + esxi1：172.16.10.1
            + esxi2：172.16.10.2
            + esxi3：172.16.10.3
        * EXPRESSSCOPE エンジンのホスト名：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：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
    - vCenter Server
    - 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)

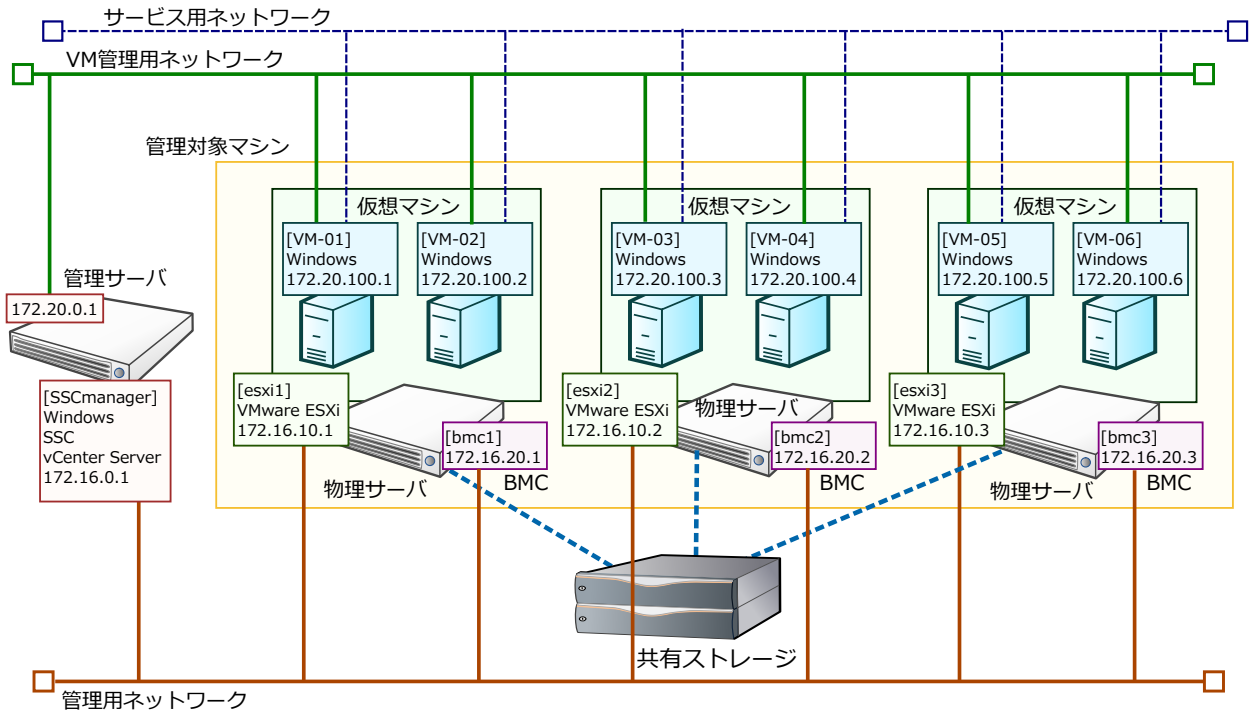


図　今回構築するシステムの構成

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」の二種類の準備があります。

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
- vCenter Server

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

SigmaSystemCenter を動作させるために、以下の Windows のコンポーネント・機能が必要です。

- .NET Framework 4.6.2 (※)
- Web サーバー (IIS)

事前に Windows の「サーバー マネージャー」を使って以下の役割と機能を追加してください。

≪管理サーバが Windows Server 2012、Winsows Server 2012 R2、Winsows Server 2016 の場合≫

- Windows に追加する役割

  Web サーバー （IIS）

  Web サーバー （IIS）にインストールする役割サービス

  - 静的なコンテンツ
  - ASP.NET
    - Windows Server 2012、Winsows Server 2012 R2 の場合は、ASP.NET 4.5 を選択
    - Windows Server 2016 の場合は、ASP.NET 4.6 を選択
  - IIS 管理コンソール
  - IIS 6 メタベース互換

Windows Server 2012、Winsows Server 2012 R2 の場合、既定の.NET Framework のバージョンは 4.5 ですが、.NET Framework 4.6.2 は、SSC のインストーラからインストールされるため、別途インストールは不要です。

Windows Server 2016 は、.NET Framework 4.6.2 は、既定でインストールされるため、別途インストールは不要です。

(※).NET Framework 4.7 も利用可能です。必要に応じて、.NET Framework 4.6.2 からアップデートして利用してください。

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

（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 は管理サーバに添付のものをあらかじめインストールしておくことでも利用できますが、SSC に添付の ESMPRO/ServerManager のバージョン(6.20)以上の ESMPRO/ServerManager をインストールしてください。

※物理サーバの機種が Express5800/D120h の場合は ESMPRO/ServerManager のバージョンは 6.22 以上が必要です。ESMPRO の下記製品サイトより、ESMPRO/ServerManager の最新のインストールモジュールを入手してインストールしてください。

http://jpn.nec.com/esmsm/index.html

[ダウンロード]→[インストールモジュール]の一覧表より、「ESMPRO/ServerManager Ver.6」の項目から入手することができます。

3.2 管理サーバの設定

3.2.1 IIS の設定

IIS の http のポート(80)を変更します。

vCenter Server は、デフォルトの設定でインストールした場合はポート(80)を使用します。一方、SSC が利用する IIS の Web サービスも、http のポート(80)を使用する設定がデフォルトなので競合しないように IIS の http のポートを変更します。

もし、vCenter Server のインストールでポート(80)を使わない設定にした場合は、この変更作業は必要ありません。

今回は、IIS10.0 の http ポートを 80 から 20080 に変更することにします。

Windows の[スタート]メニューから[Windows 管理ツール]→[インターネット インフォメーション サービス (IIS) マネージャー]をクリックします。

[インターネット インフォメーション サービス (IIS) マネージャー]画面が表示されたら、[接続]ツリービュー上で、管理サーバ名（ここでは、[SSCmanager]）→[サイト]→Web サイト名

（ここでは、[Default Web Site]）を右クリックします。メニューから[バインドの編集]をクリックします。

「サイト バインド」ダイアログが開いたら、種類の[http]を選択した状態で、[編集]をクリックします。「サイト バインドの編集」ダイアログが開いたら、[ポート]に[20080]を入力し[OK]を押せば変更が完了します。

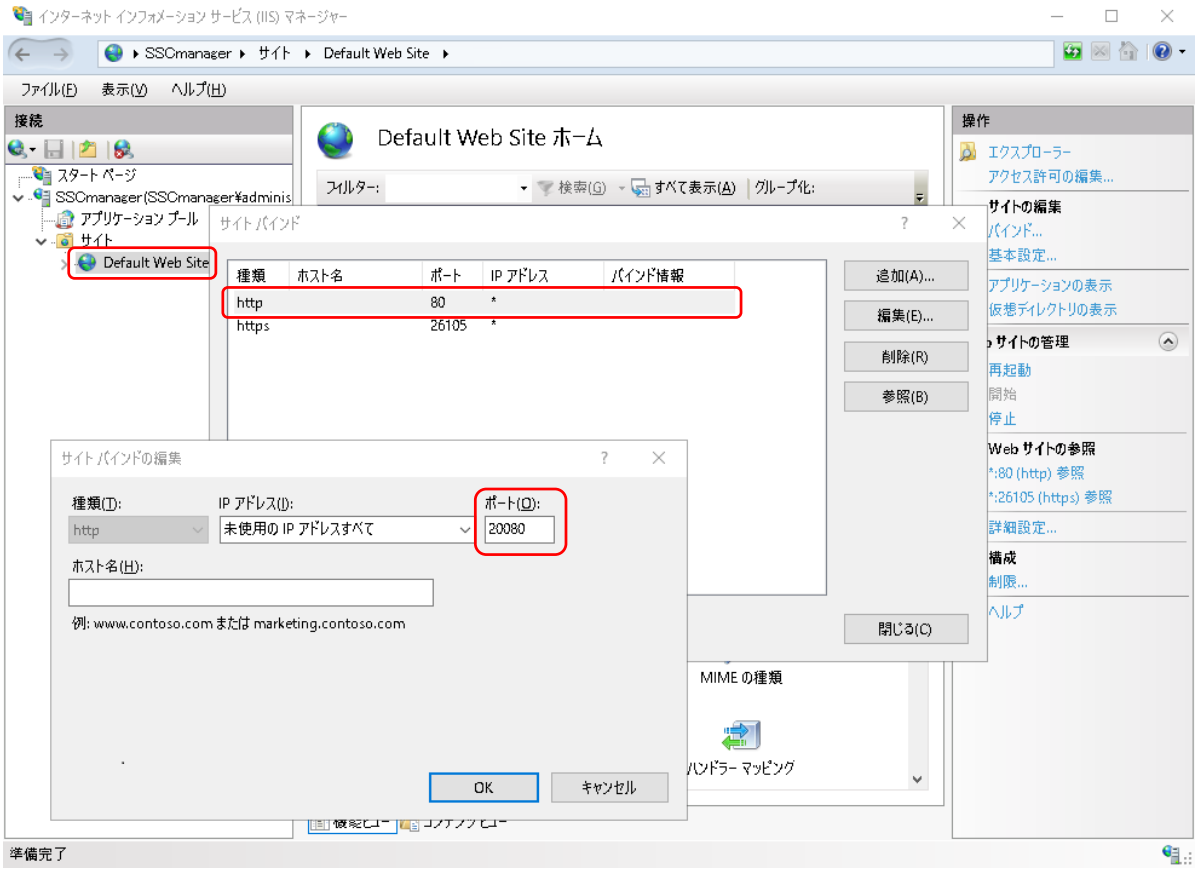


図　IIS の http ポートの変更（サイト バインドの編集）

3.2.2　SNMP Trap サービスの設定

SSC で管理対象の物理サーバのイベント（PET）を受け取るために、管理サーバで SNMP Trap の受信設定を確認します。

まず、ESMPRO/ServerManager の SNMPTrap の受信方法が Windows の SNMP Trap サービスを使用するようになっているかを確認します。

SSC 管理サーバのデスクトップ上のショートカット[ESMPRO ServerManager]をクリックします。ESMPRO/ServerManager のコンソールが起動しますので、[アラートビューア]をクリックします。アラートビューアが起動しますので、メニューから[アラート受信設定]をクリックします。

デフォルトでは、次の図のように「アラート受信設定」ダイアログの[SNMP トラップ受信設定]の枠の[SNMP トラップサービスを使用する]が選択されています。もし、選択されてい

ない場合は[SNMP トラップサービスを使用する]のラジオボタンをクリックし、[OK]をクリックします。

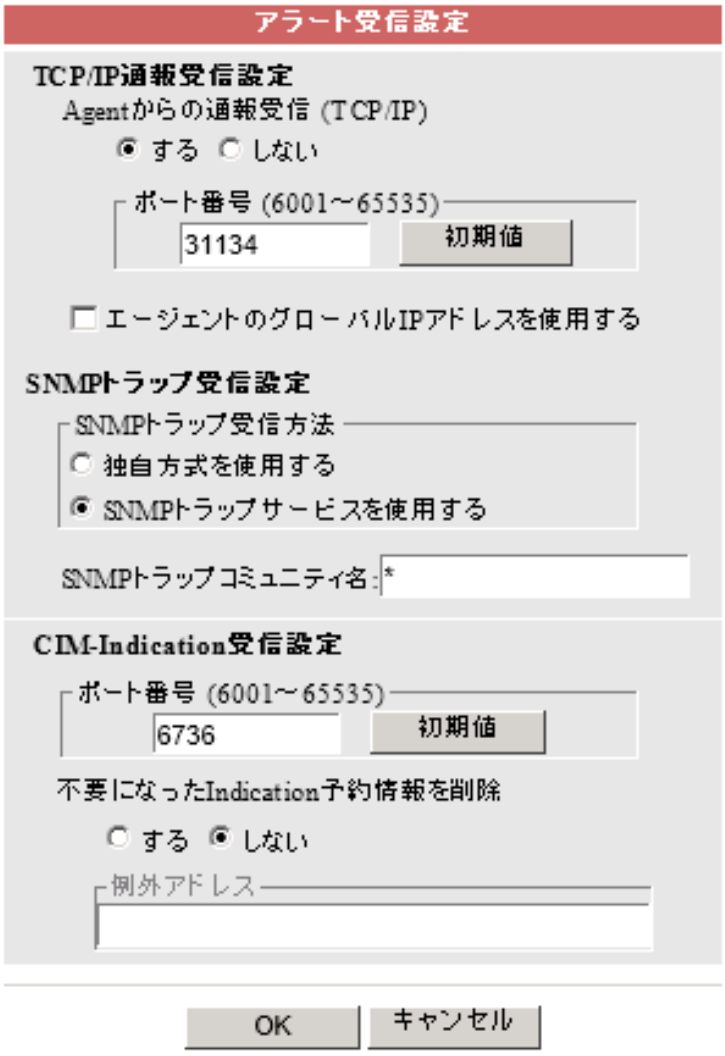


図　ESMPRO/ServerManager のアラートビューア（「アラート受信設定」ダイアログ）

次に、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。

3.2.3　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」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、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。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[接続が許可する]ようになるので、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]を選択します。

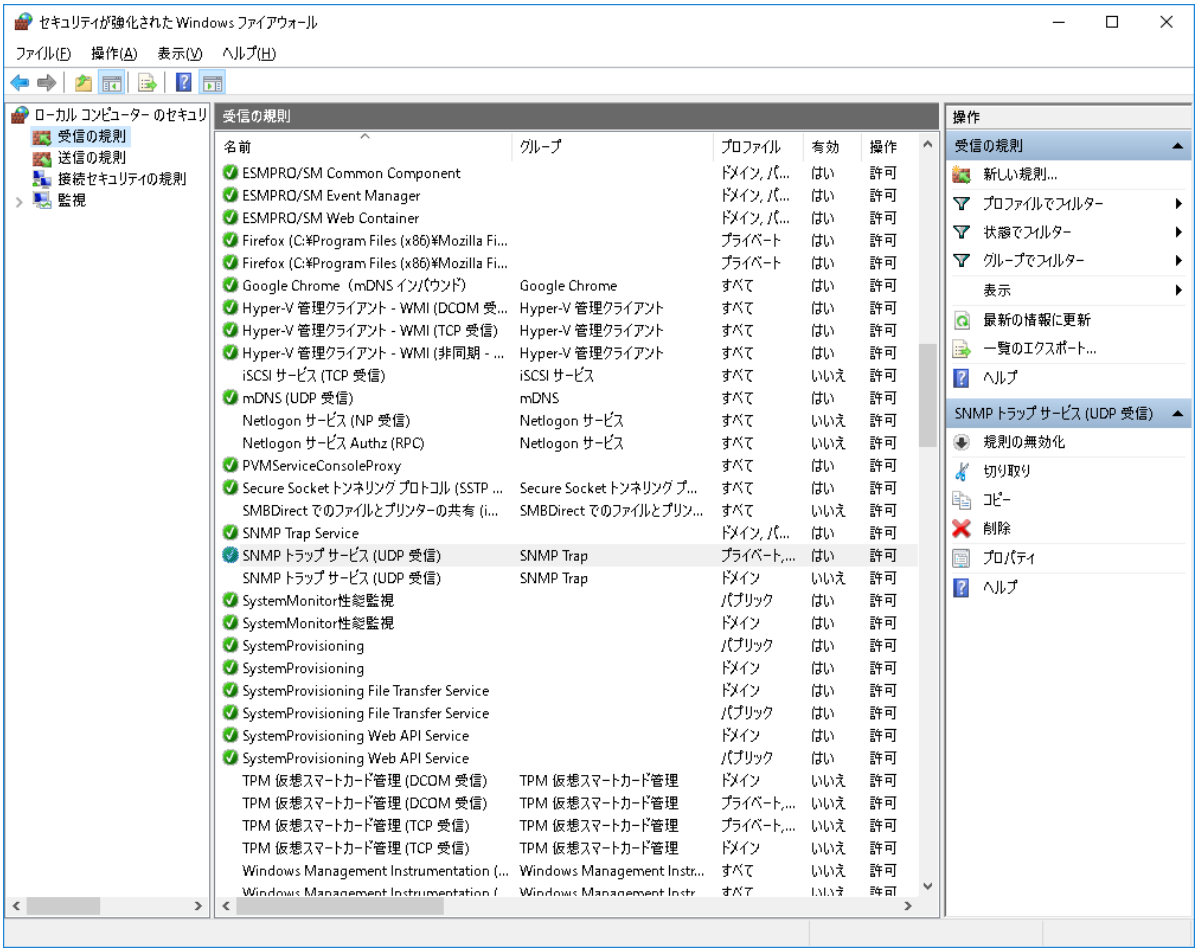


図　セキュリティが強化された Windows ファイアウォール (SNMP トラップ サービス (UDP 受信))

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]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します。今回は[プライベート]を選択します。
- 名前
  - 任意の名前を入力します。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。

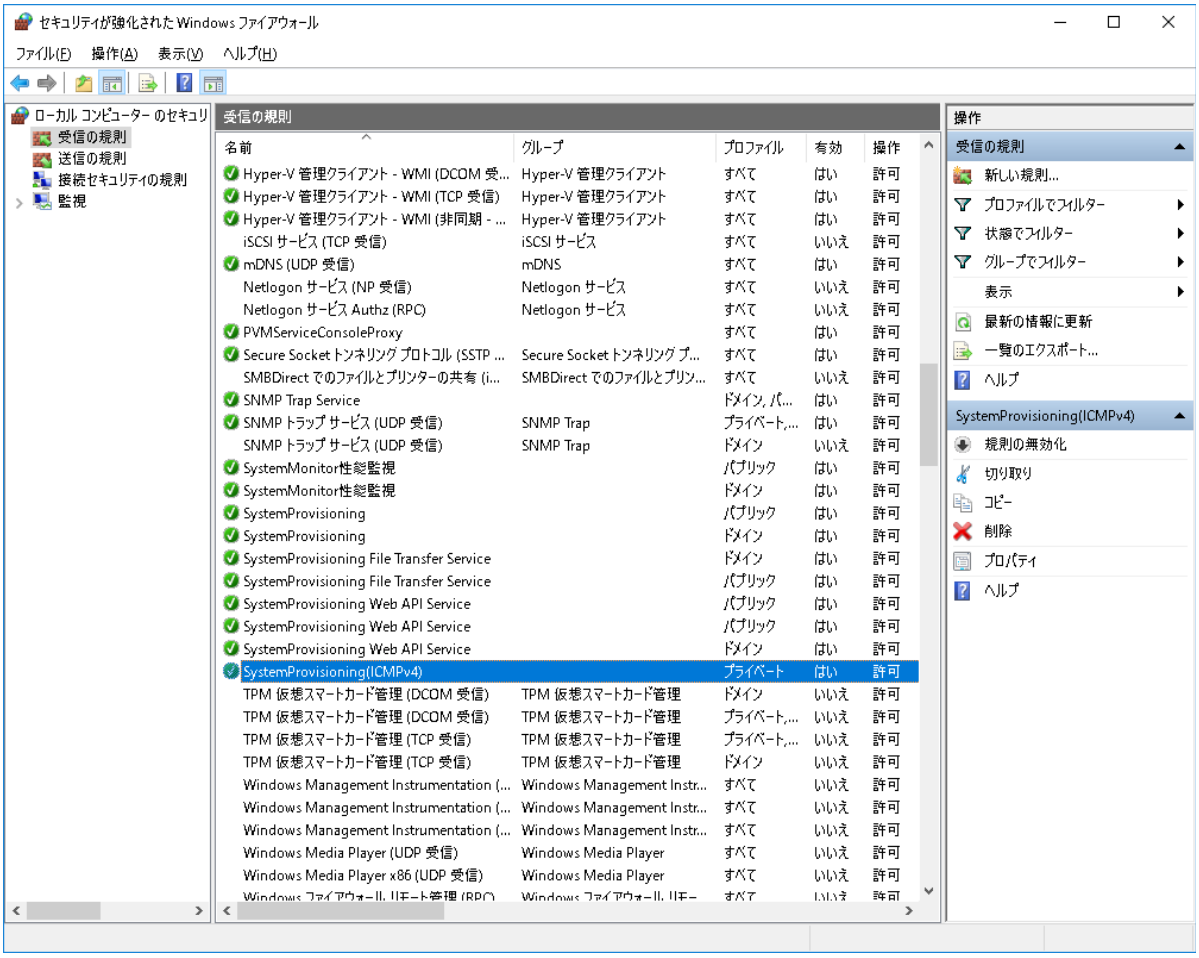


図　セキュリティが強化された Windows ファイアウォール（SystemProvisioning(ICMPv4)）

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。

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://172.16.0.1:20080/Provisioning/Default.aspx にアクセスします。

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。

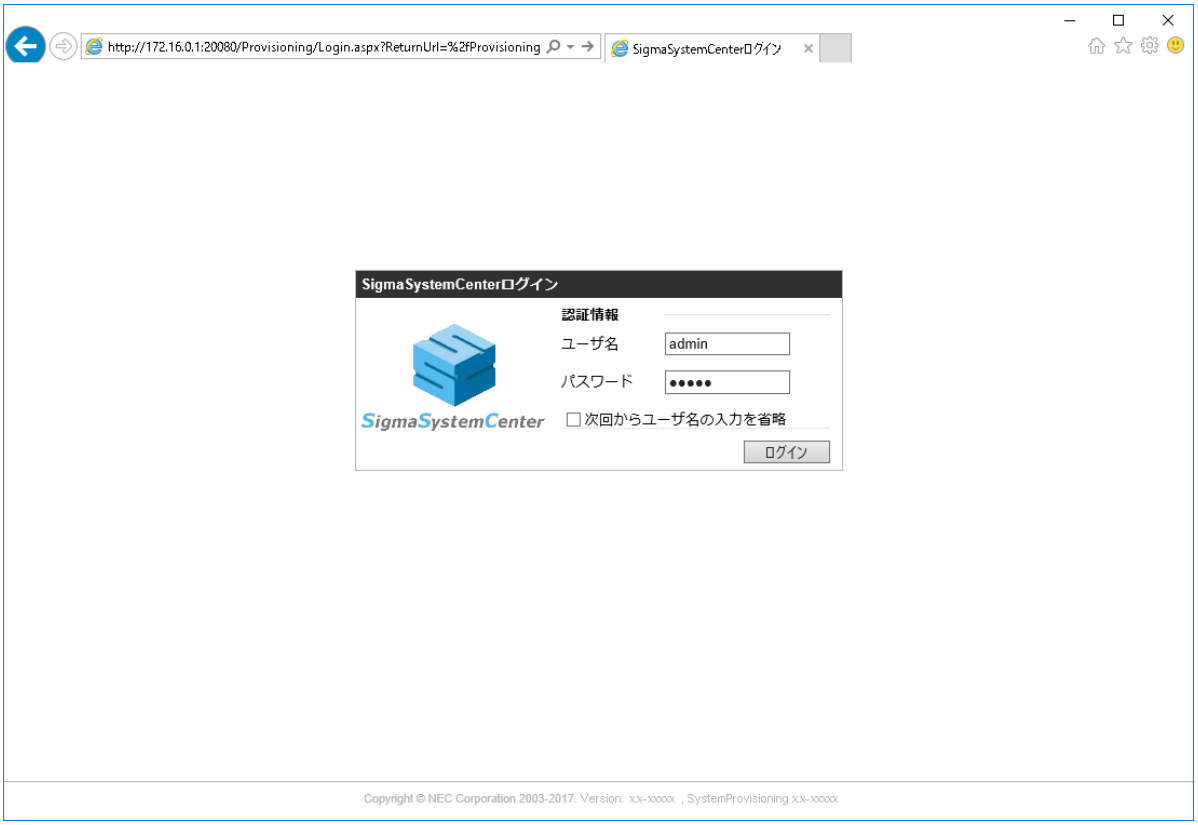


図 「SigmaSystemCenter ログイン」画面

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。

画面の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、「ユーザ一覧」、「ロール一覧」の画面を表示されたら「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]を設定し[OK]を押せば、ユーザが[作成されます。今回は、[ユーザ名]を[sysadmin]とし、[ロール]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]を押すと「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。

「PVM サービスを再起動し、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

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。

4.3　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のかだけを別に設定します。

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するので、[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]を押してください。

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。

4.4 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。

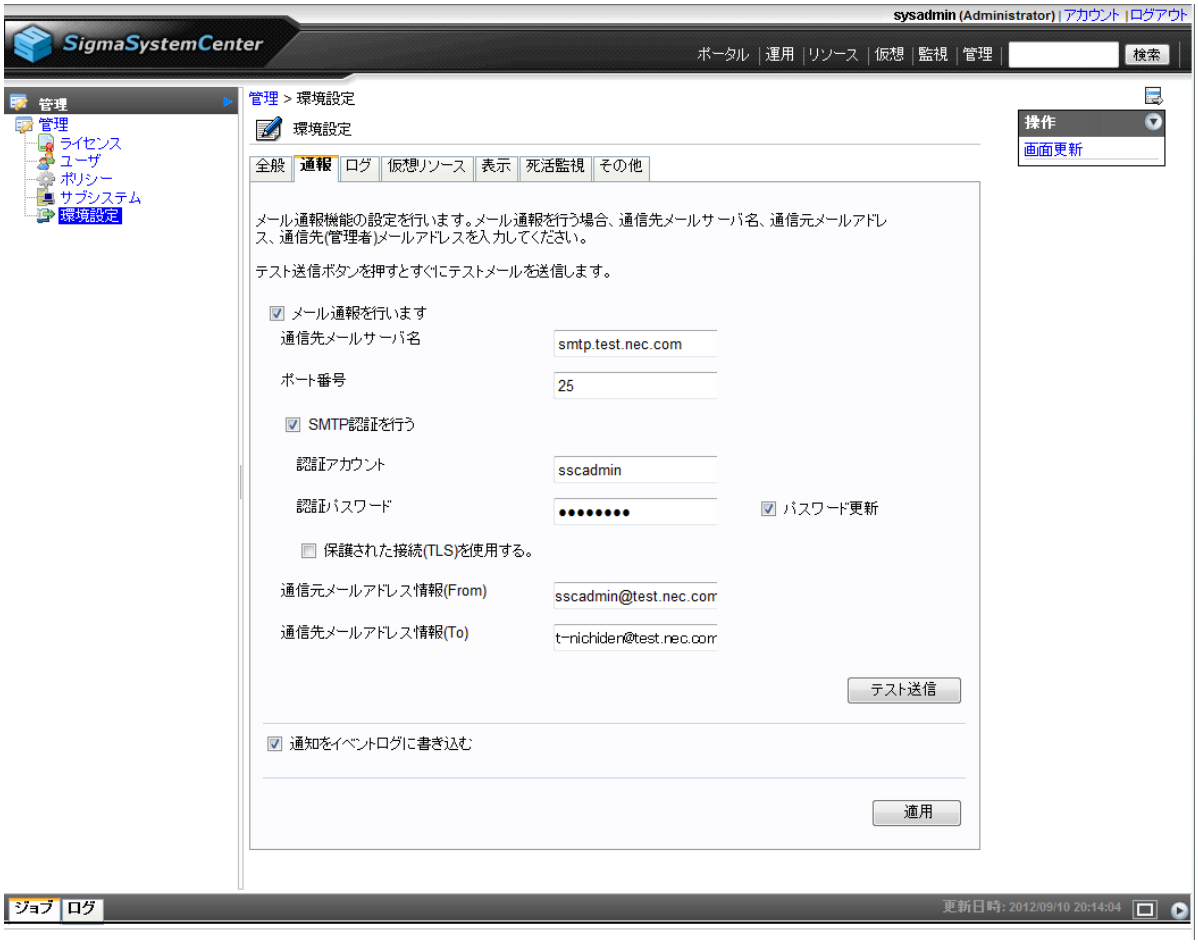


図 「環境設定」画面（[通報]タブ）

まず、[メール通報を行います]の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）
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	―

設定項目	説明	入力例
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]を押す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]を押して、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。

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）されているので、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 VMware ESXi ですので、サブシステムとして VMware vCenter Server 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]をクリックすると下の画面が表示されるので、[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 がインストールしてあるサーバのホスト名もしくは IP アドレス
- 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

上記の項目を入力したら[OK]をクリックしてください。

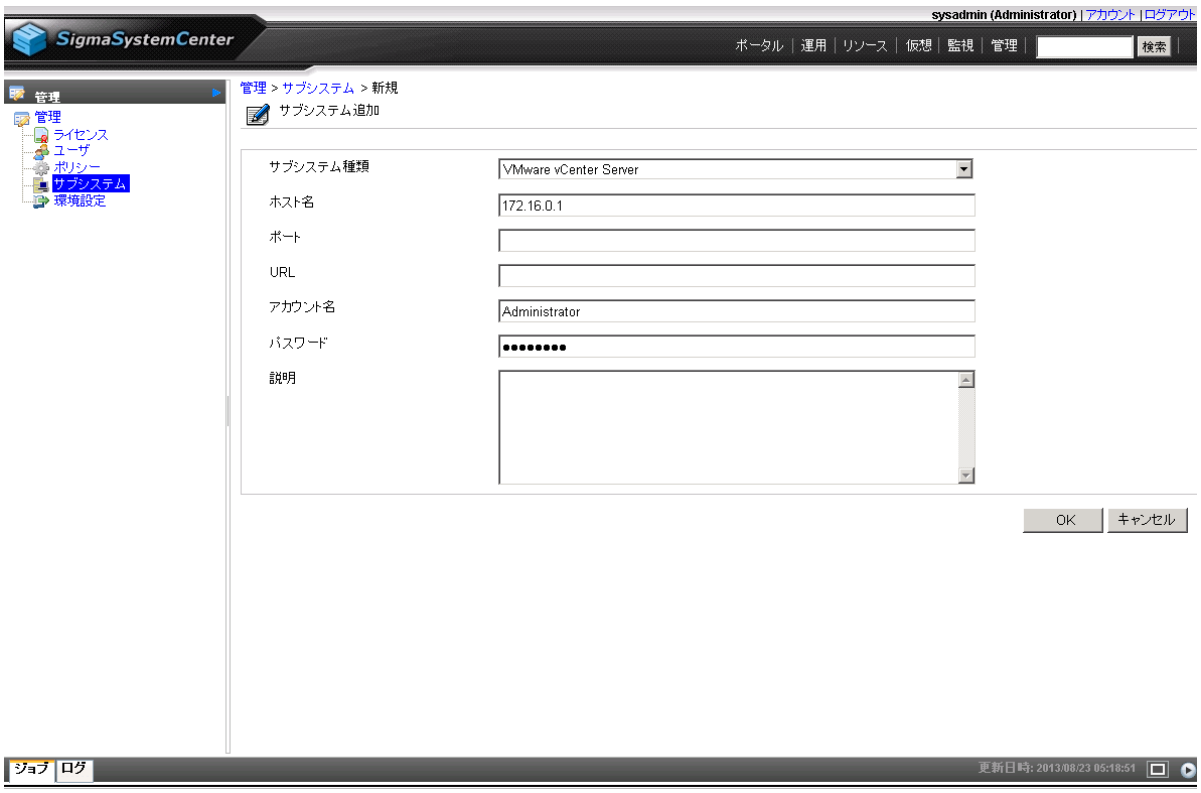


図　vCenter Server の登録

さて、SSC のサブシステムには VMware 用の「VMware vCenter Server」のほかに「VMware ESXi」があります。ただし、こちらは vCenter Server を登録するとその vCenter Server で管理している ESXi が自動的に検出/登録されるので、手動で登録する必要はありません。vCenter Server 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、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)。

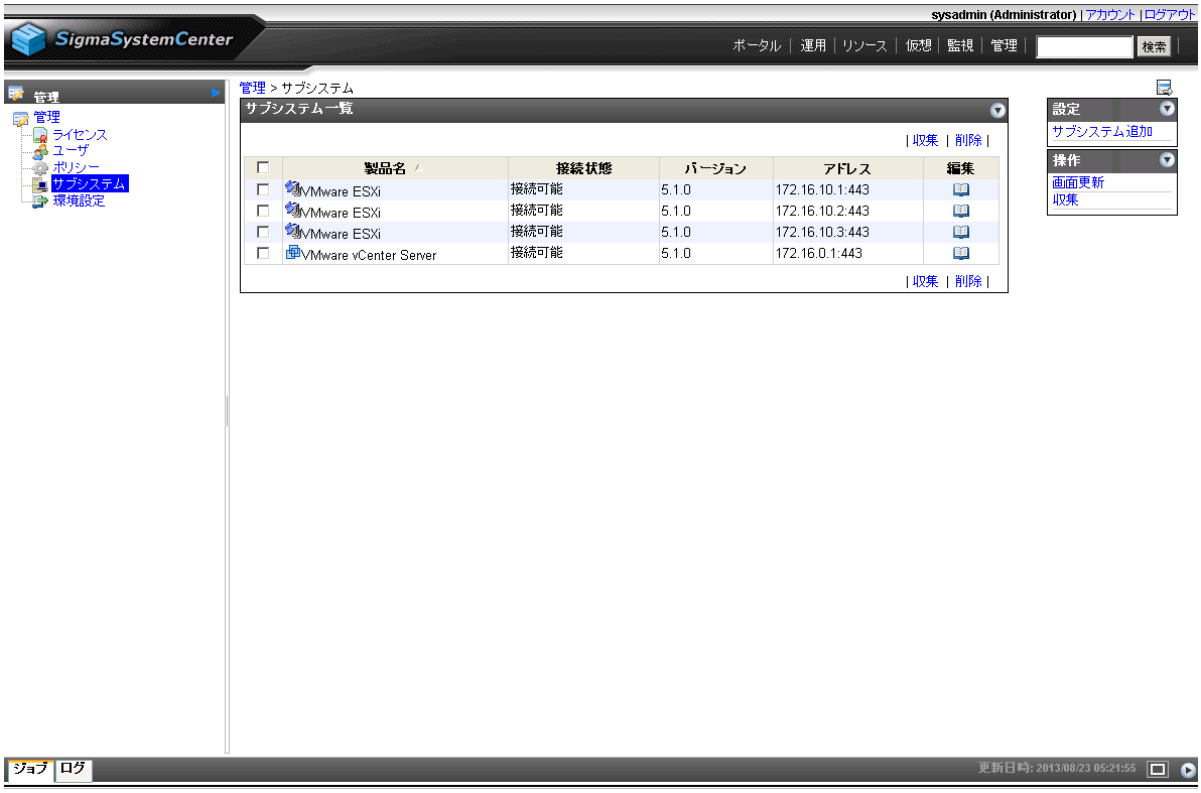


図　サブシステム一覧

もっとも、ESXi が検出されただけでは、Failover、VM 作成/再作成などの操作を SSC から実行することができません。そこで追加の設定を行います。[サブシステム一覧]の VMware ESXi の右端にある[編集]アイコンをクリックして下の画面を開いてください。[ホスト名]および[ポート]には自動検出された値が設定されているので、[アカウント名]に管理者アカウントの[root]を入力し、[パスワード更新]をチェックして[パスワード]に root のパスワードを入力して[OK]をクリックします。今回は物理サーバが 3 台なので、3 台それぞれで追加の設定を行います。

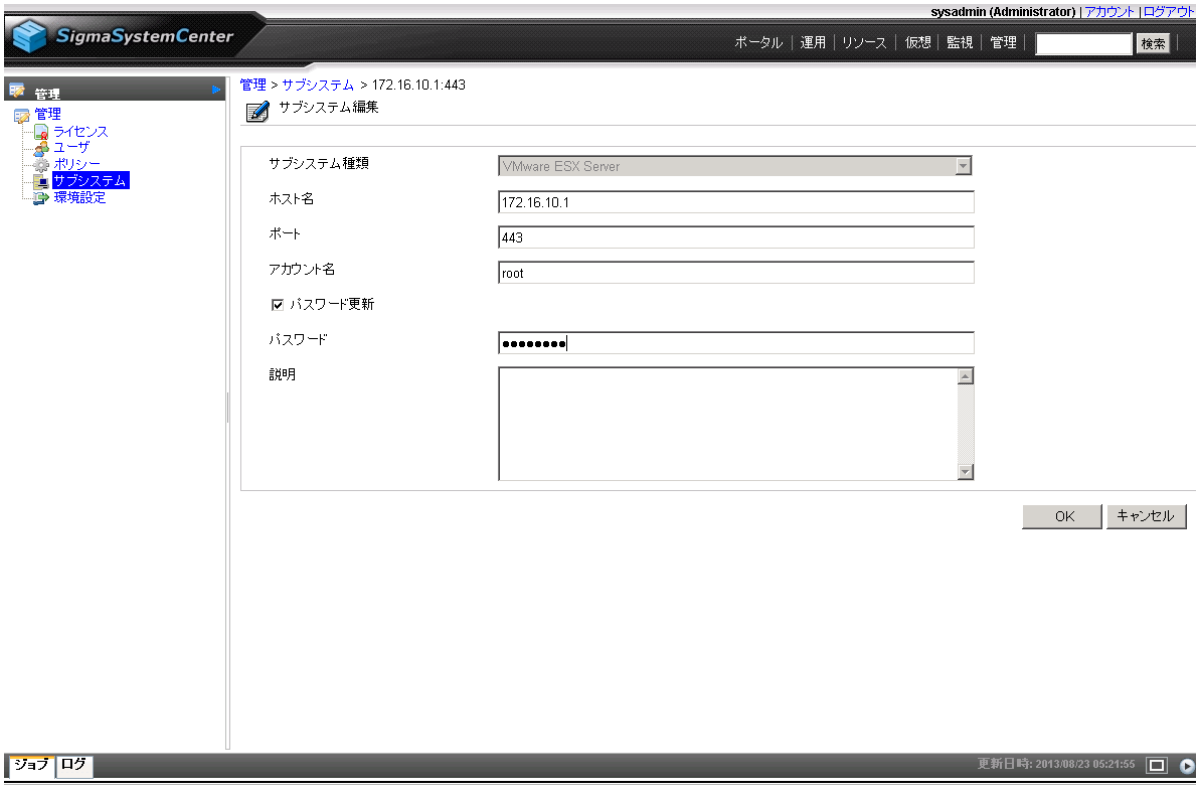


図　ESXi の追加設定

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（20 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 への登録も行われます。

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、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[172.16.10.1](esxi1)、[172.16.10.2](esxi2)、[172.16.10.3](esxi3)、業務用仮想マシン[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]が次のように登録されています。

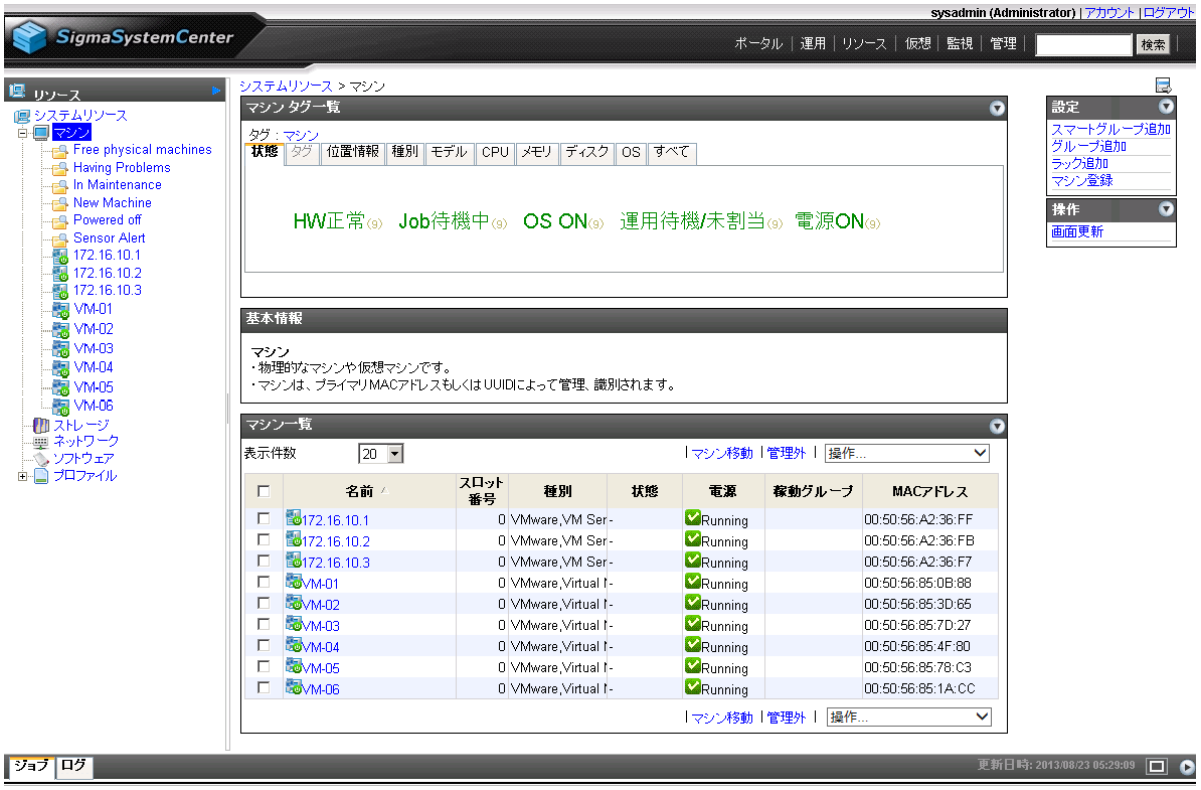


図　マシン登録後の[マシン一覧]

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。

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「マシン一覧」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　物理サーバの設定

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「172.16.10.1」(esxi1)と「172.16.10.3」(esxi2)、「172.16.10.3」(esxi3)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(EXPRESSSCOPE エンジンや iLO など)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。
   - 従来の EXPRESSSCOPE エンジンについては、「5.3.1　EXPRESSSCOPE エンジン（BMC）の設定（26 ページ）」を参照
   - Express5800/R120h などに搭載される iLO については、「5.3.2　iLO（BMC）の設定（27 ページ）」を参照
   - Express5800/D120h などに搭載される BMC については、「5.3.3　Express5800/D120h などの BMC/CMC の設定（31 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。「5.3.4　SSC での OOB のアカウント設定（36 ページ）」を参照。

5.3.1 EXPRESSSCOPE エンジン（BMC）の設定

◇管理 LAN の設定

まず、「172.16.10.1」(esxi1)となるサーバの EXPRESSSCOPE エンジン（BMC）の管理 LAN の設定を行います。手順については、「EXPRESSSCOPE エンジン 3 ユーザーズガイド」の「2. 本体装置側の設定」を参照して、管理 LAN を設定してください。

◇管理者権限のあるユーザの作成

次に、「172.16.10.1」(esxi1)となるサーバの EXPRESSSCOPE エンジン（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、「EXPRESSSCOPE エンジン 3 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、「ユーザ管理」画面で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。

図　EXPRESSSCOPE エンジン 3 のアカウントの設定

◇PET 通報の設定

続いて、EXPRESSSCOPE エンジン（BMC）で、管理サーバである SSCmanager(172.16.0.1)へ PET 通報を行うための設定をします。今回は、通報先の設定枠の 1 次通報先を使うことにします。

1. [設定] タブをクリックします。
2. 左のメニューツリーから[BMC]→[通報]→[SNMP 通報] をクリックします。

3. 中央メインペイン下の[編集] をクリックして、以下の設定を行います。

項目名	設定値
通報	有効
コンピュータ名	esxi1
コミュニティ名	public
通報手順	全ての通報先
通報応答確認	無効
1 次通報先－通報先 IP アドレス	チェックの上、172.16.0.1
2 次通報先－通報先 IP アドレス	他のアプリケーションに合わせて任意
3 次通報先－通報先 IP アドレス	他のアプリケーションに合わせて任意
通報レベル	異常、警告、情報

4. メインペイン下の[適用]をクリックします。

図　EXPRESSSCOPE エンジン 3 の SNMP(PET)通報の設定

[172.16.10.2」(esxi2)と[172.16.10.3」(esxi3)となるサーバについても、同様に設定します。

5.3.2 iLO（BMC）の設定

◇管理 LAN の設定

まず、「172.16.10.1」(esxi1)となるサーバの iLO（BMC）の管理 LAN の設定を行います。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、管理 LAN を設定してください。

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、「172.16.10.1」(esxi1)となるサーバの 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: 7CE712P3GU
iLO IPv4: 172.16.10.1
iLO IPv6: FE80::FE15:B4FF:FE97:8890
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
リモートコンソールアクセス
仮想電源およびリセット
仮想メディア
設定の構成
ホストBIOS
ホストNIC
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
ssc
Enter: 選択
ESC: 終了
F1: ヘルプ
F7: 製造時の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

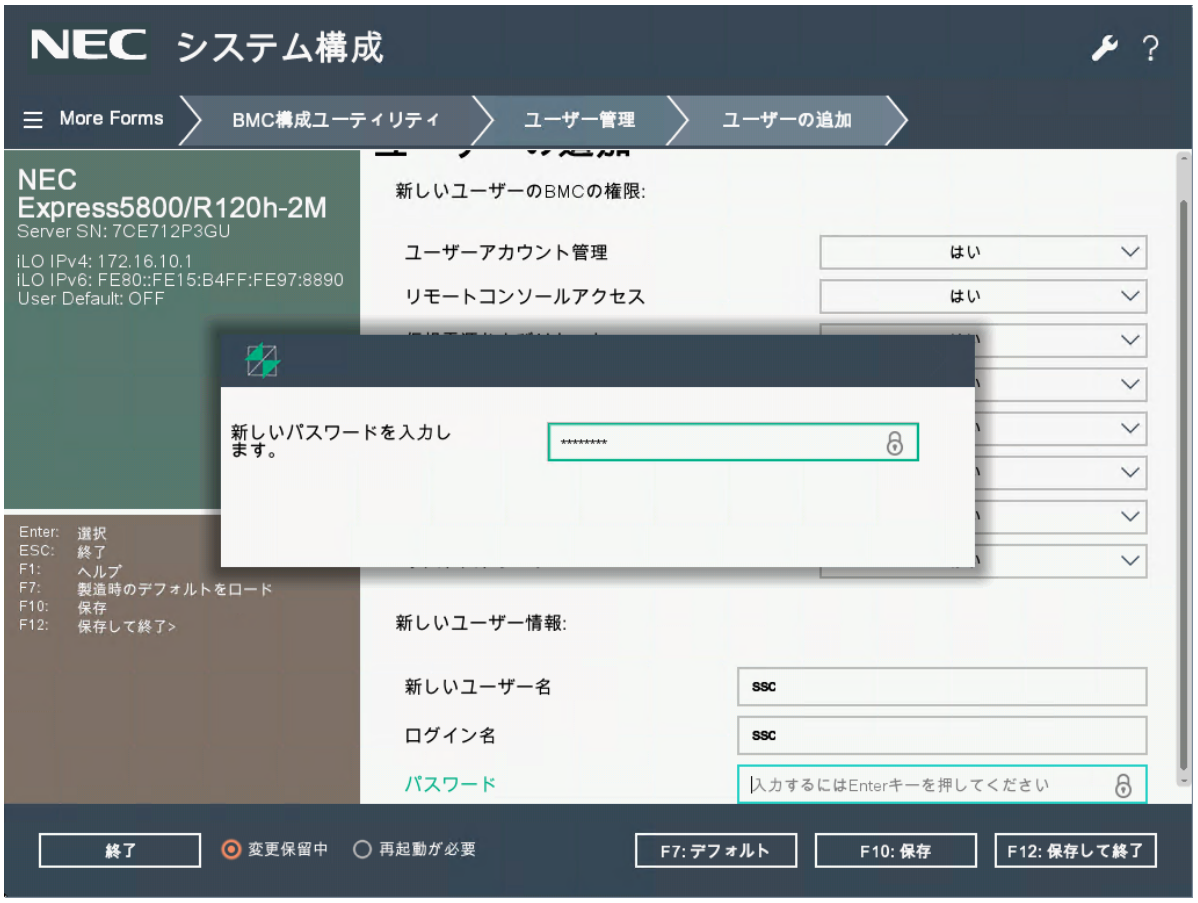

NEC システム構成
More Forms
BMC構成ユーティリティ
ユーザー管理
ユーザーの追加
NEC Express5800/R120h-2M
Server SN: 7CE712P3GU
iLO IPv4: 172.16.10.1
iLO IPv6: FE80::FE15:B4FF:FE97:8890
User Default: OFF
新しいユーザーのBMCの権限:
ユーザーアカウント管理
リモートコンソールアクセス
はい
新しいパスワードを入力します。
****
新しいユーザー情報:
新しいユーザー名
ログイン名
パスワード
ssc
入力するにはEnterキーを押してください
Enter: 選択
ESC: 終了
F1: ヘルプ
F7: 製造時の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、「172.16.10.1」(esxi1)となるサーバの 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 の設定をします。

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。

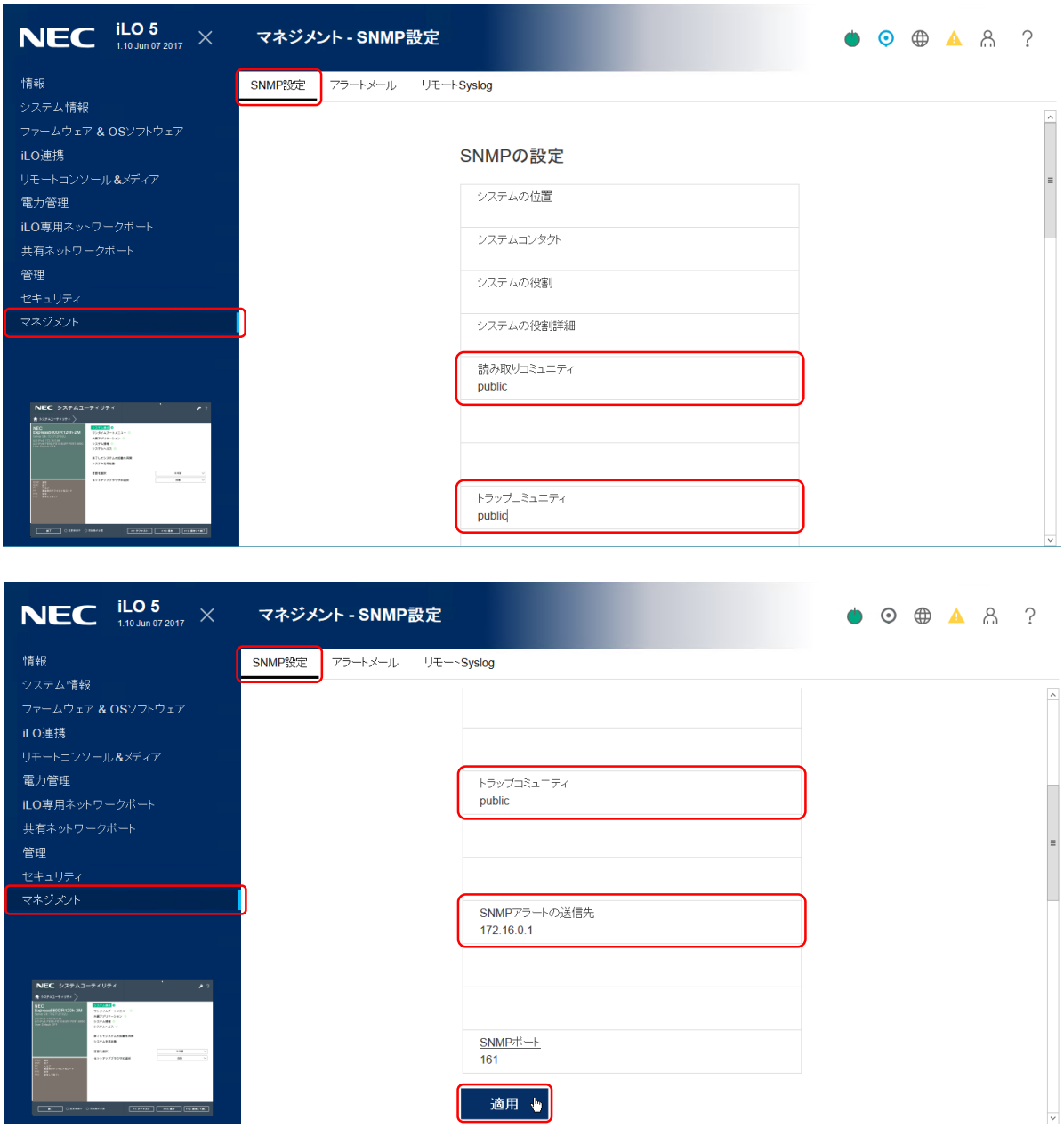


図　iLO 5 の SNMP の設定

[172.16.10.2」(esxi2)と[172.16.10.3」(esxi3)となるサーバについても、同様に設定します。

5.3.3　Express5800/D120h などの BMC/CMC の設定

◇管理 LAN の設定

まず、「172.16.10.1」(esxi1)となるサーバの BMC の管理 LAN の設定を行います。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「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。

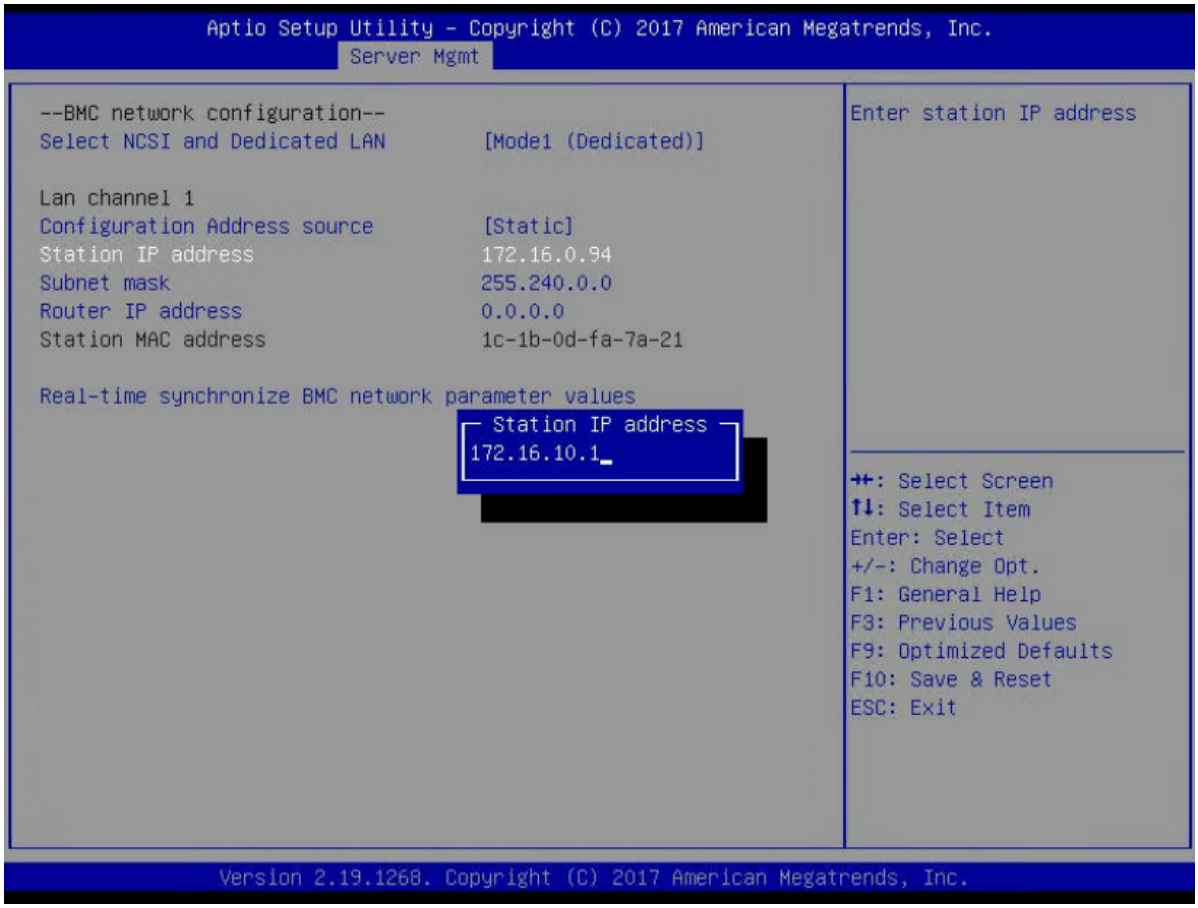


図　マネージメント LAN 設定

◇管理者権限のあるユーザーの作成

次に、「172.16.10.1」(esxi1)となるサーバの 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

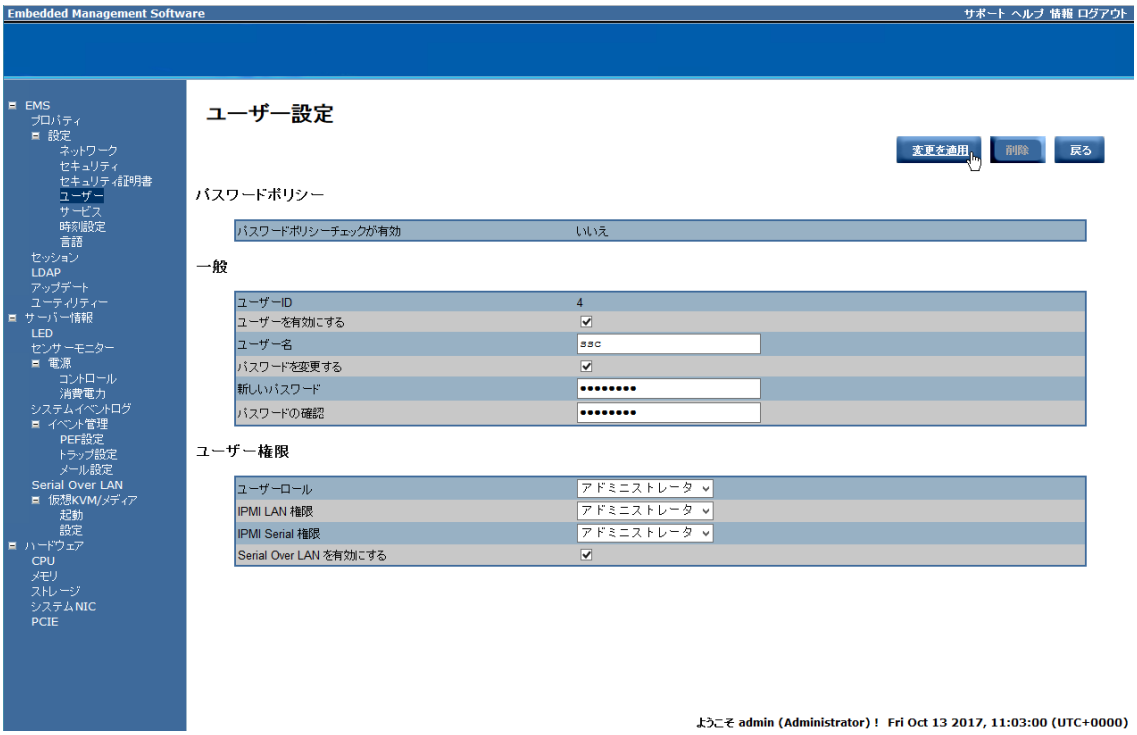


図　ユーザーの追加

◇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」を参照します。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」を参照します。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

[172.16.10.2」(esxi2)と[172.16.10.3」(esxi3)となるサーバについても、同様に設定します。

5.3.4　SSC での OOB のアカウント設定

SSC では、物理サーバの BMC(EXPRESSSCOPE エンジンや iLO など)にログインするために、[リソース]ビューで「172.16.10.1」(esxi1)と「172.16.10.2」(esxi2)、[172.16.10.3」(esxi3)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[172.16.10.1](esxi1)（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、「5.3.1 EXPRESSSCOPE エンジン（BMC）の設定（26 ページ）」/「5.3.2 iLO（BMC）の設定（27 ページ）」/「5.3.3 Express5800/D120h などの BMC/CMC の設定（31 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]を押します。

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「172.16.10.1」(esxi1)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、「172.16.10.2」(esxi2)と「172.16.10.3」(esxi3)も設定してください。

6. 運用の基本設定

ここからは、登録したリソースをどのような用途でどのように利用するのかといった運用に関する設定を行います。このような設定は[運用]ビュー（画面右上の[運用]をクリック）で行います。

6.1 運用グループの作成

[運用]ビューで最初に行う作業は“グループ”の追加です。

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します。また、後で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に設定することになるので、障害監視や負荷監視の内容に応じてグループを分けて作るようにします。

今回のシステムでは、次の表のように同じ考え方や要素で管理するサーバをひとかたまりのグループとしており、物理サーバのグループ「ESXi」と業務用仮想マシンのグループ「業務用 VM」を作成することにします。同じ仮想マシン（VM）でも OS や業務が違う場合は、障害監視と負荷監視の内容を別にするためにもグループを分けるようにします。

表　グループの設計例

サーバ	グループを設計する際の考え方				グループ
	物理サーバか？ 仮想サーバか？	OS は何か？	障害発生時にどのように対応するか？	負荷を 監視するか？	
172.16.10.1 (esxi1)	物理（VM サーバ）	ESXi	障害（予兆）対応	監視する	ESXi
172.16.10.2 (esxi2)	物理（VM サーバ）	ESXi	障害（予兆）対応	監視する	
172.16.10.3 (esxi3)	物理（VM サーバ）	ESXi	障害（予兆）対応	監視する	
VM-01	仮想（VM）	Windows Server	障害対応（通報）	監視する	業務用 VM
VM-02	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-03	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-04	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-05	仮想（VM）	Windows Server	障害対応（通報）	監視する	
VM-06	仮想（VM）	Windows Server	障害対応（通報）	監視する	

[運用]ビューの[設定]メニューにある[グループ追加]をクリックし、下の画面を開きます。[名前]にグループ名を入力し、[マシン種別]のドロップダウンリストから当該グループで稼動させるマシンのマシン種別を選び、[OS 種別]のドロップダウンリストから当該グループで利用する OS を選んで[OK]をクリックします。

ESXi のマシン種別は VM サーバなので、[ESXi]グループの[マシン種別]は[VM サーバ]を選び、ESXi は Linux ベースなので、[ESXi]グループの[OS 種別]は[Linux]を選びます。

業務用仮想マシンのマシン種別は VM なので、[業務用 VM]グループの[マシン種別]は[VM]を選び、今回構築する業務用仮想マシンの OS は Windows Server なので、[業務用 VM]グループの[OS 種別]は[Windows Server]にします。

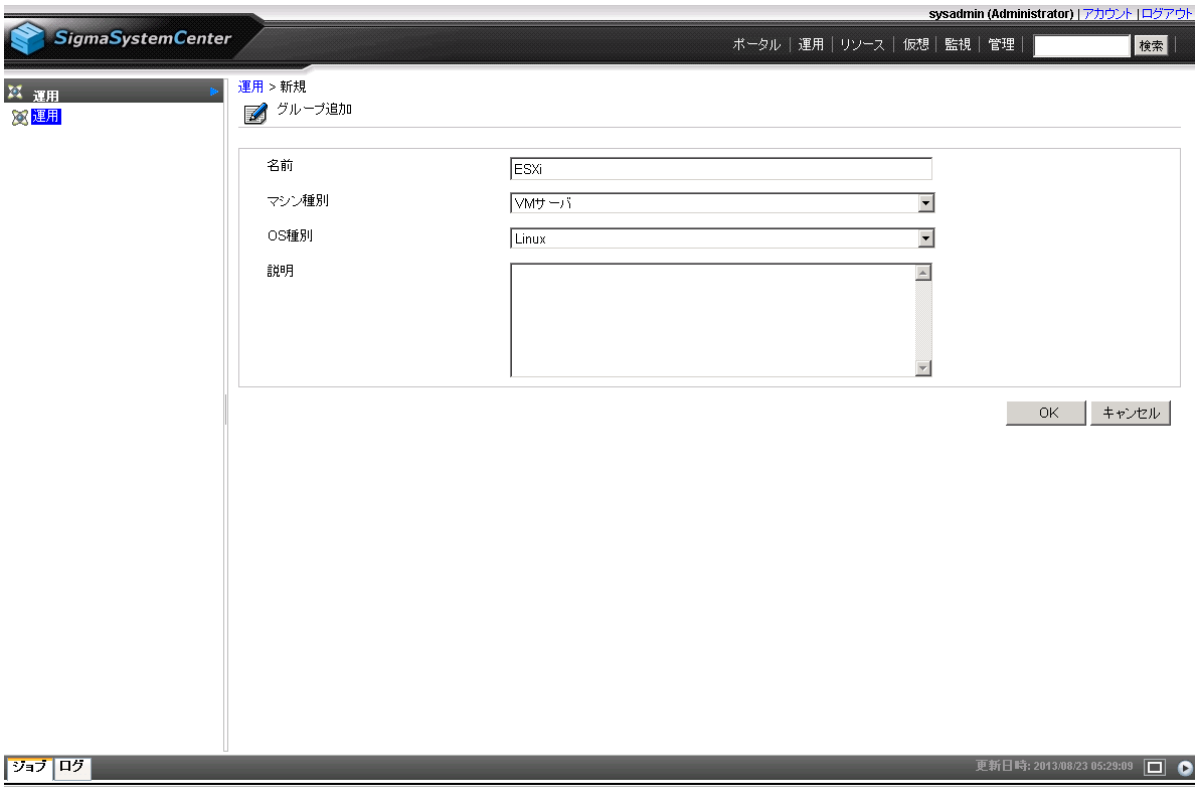


図　グループの追加

グループ追加後の[運用]ビュー（テナント/カテゴリ/グループ一覧）です。

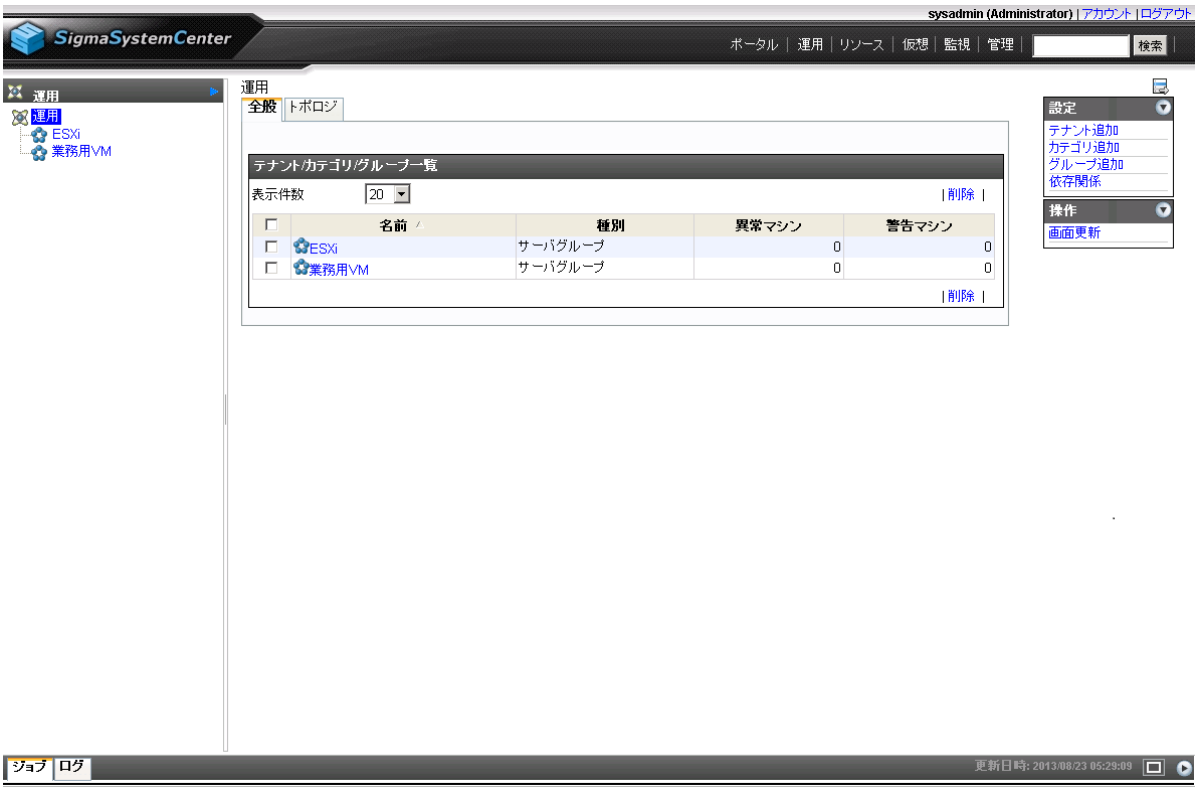


図　テナント／カテゴリ／グループ一覧

6.1.1　物理サーバグループへのホストの追加

次に、“ホスト”の追加を行います。

“ホスト”は、実体のマシンに対して SSC でどのような運用・管理を行うかの定義の枠になります。

ホストを追加するには、ツリービューにあるグループ名（ここでは[ESXi]）をクリックし、下の画面のようにグループの詳細情報画面を開きます。

図　グループの詳細情報

中央の[ホスト一覧]枠内メニューの[ホスト追加]をクリックし、「ホスト追加」画面を開きます。ここでは物理サーバのホスト「172.16.10.1」(esxi1)について設定します。IP アドレスには、管理 LAN 接続する際の IP アドレスを入力してください。

- 複数ホストを作成する：チェックしない
- ホスト名： esxi1
- タグ： 設定しない
- ネットワークを設定：チェックする
- IP アドレス：172.16.10.1
- サブネットマスク：255.255.0.0
- デフォルトゲートウェイ：172.16.0.254
- 管理用 IP アドレスにする：チェックする

下の画面のように、「ホスト追加」画面へ入力したら、[OK]をクリックします。

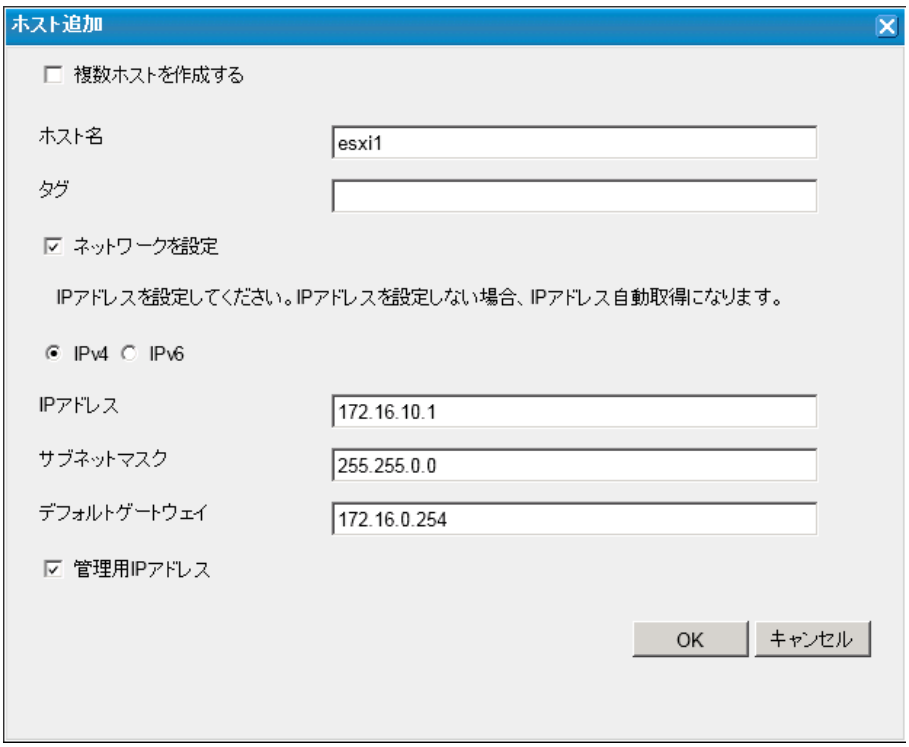


図　ホスト追加

図　ESXi グループのホスト一覧（esxi1 追加後）

ホスト追加後の[ESXi]グループの詳細情報の画面です。[ホスト一覧]に追加したホスト[esxi1]が表示されています。この時点では、まだ実体となる物理サーバを割り当てていないので、状態には[定義のみ]と表示されます。

以上で物理サーバのホスト「esxi1」が設定できました。同様の手順を繰り返して、「esxi2」と「esxi3」も設定してください。下は esxi2 と esxi3 設定後のホスト一覧です。

図　ESXi グループのホスト一覧

6.1.2　仮想マシングループへのホストの追加

続けて仮想マシンのグループ「業務用 VM」にもホストを追加します。手順は物理サーバグループ「ESXi」のときと同様に、「ホスト追加」を実施します。ホスト追加と IP アドレス設定の方法は物理サーバのときとまったく同じです。下は業務用 VM の 6 台の仮想マシン[VM-01]、[VM-02]、[VM-03]、[VM-04]、[VM-05]、[VM-06]にそれぞれ IP アドレスを設定した状態のホスト一覧です。

図　VM グループのホスト一覧

6.1.3　マスタマシンの登録

ここまでの作業で、システムを構成するサーバの定義を SigmaSystemCenter（SSC）に追加することができました。次はこのサーバの定義にリソースを割り当てます。まずは ESXi グループのホストにリソースを割り当ててみましょう。[運用]ビューのツリービューで ESXi グループをクリックすると、グループの情報が表示されます。[ホスト一覧]の枠のリソースを割り当てるホスト（ここでは「esxi1」）のチェックボックスをチェックし、枠内メニューの[マスタ登録]をクリックしてください。

図　マスタマシン登録

すると、割り当てるマシンが属しているプールを選択する画面が表示されます。今回は、[共通プールから選択]のラジオボタンをチェックして[次へ]をクリックします。

図　プールの選択

次に、割り当てるマシンを選択する画面が表示されます。ここには登録済みのリソースの中から、運用グループで選択しているマシン種別に適合するものだけがリストアップされます。割り当てるマシンのラジオボタンをチェックして[次へ]をクリックします。

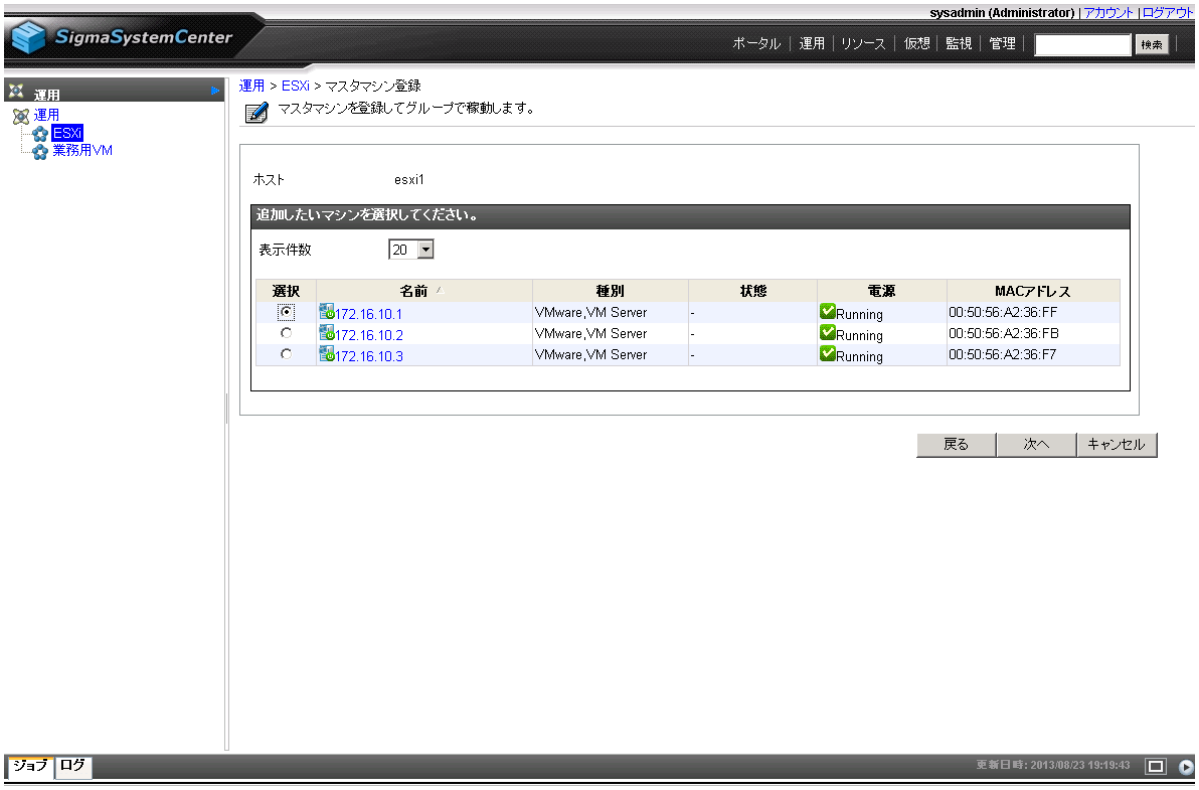


図　割り当てマシンの選択

マスタマシン登録の確認画面が表示されるので、間違ったマシンを選択していないことを確認してから[完了]をクリックしてください。

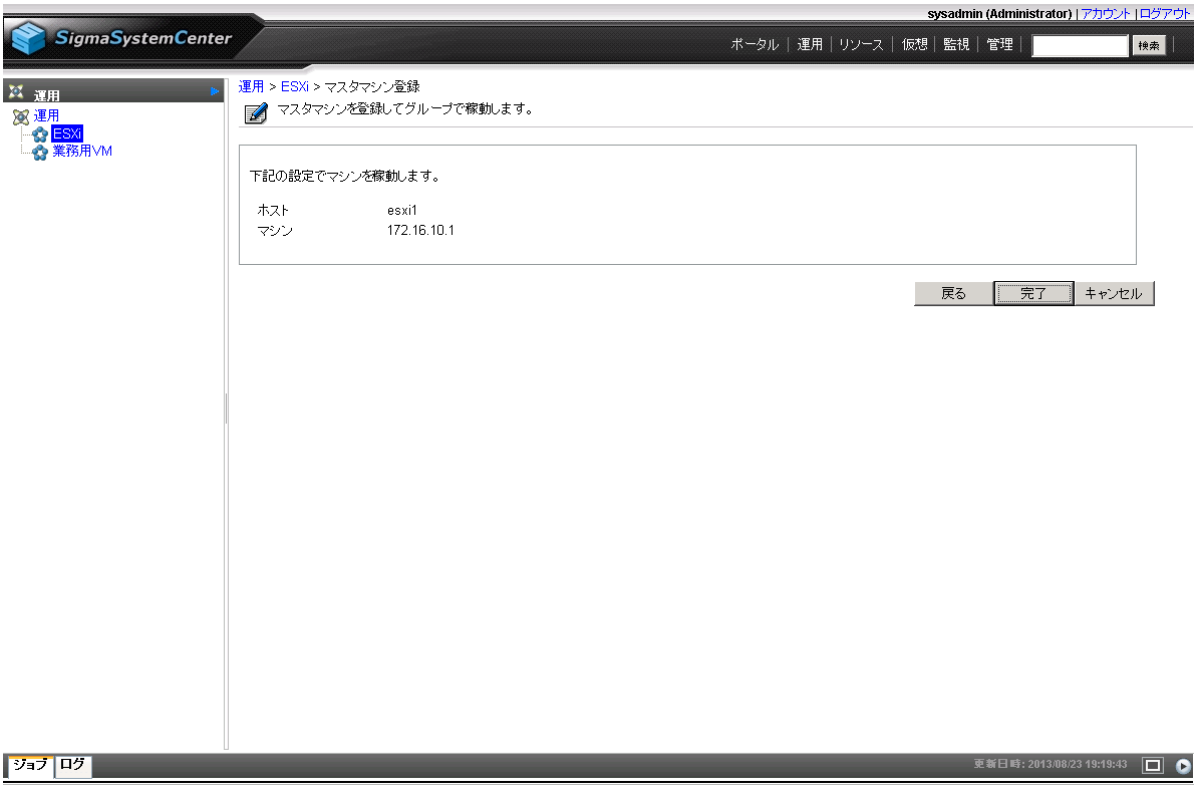


図　割り当てマシンの確認

「グループの情報」画面に戻るので、同じ手順で 2 台目の物理サーバホスト「esxi2」と「esxi3」にもマスタマシンを登録します。下は、3 台の物理サーバにマスタマシンを登録した状態です。

図　マスタマシン登録後のグループ情報（ESXi）

業務用仮想マシンのホスト定義にも物理サーバと同じようにしてマスタマシンを登録します。下は、6 台の仮想マシンにマスタマシンを登録した状態です。

図　マスタマシン登録後のグループ情報（VM）

6.2　手動での Migration（vMotion）

以上の作業により、システム構成定義と管理対象の物理サーバ（リソース）の対応関係が SSC に設定されました。目標の自律運用を実現するには運用ポリシーを作成して適用する必要がありますが、この段階でも手動での制御は SSC 上から行えます。そこで、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物理サーバ間の移動を行うことを指します。

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[172.16.10.1](esxi1)上で仮想マシン[VM-01]、[VM-02]が動作しており、物理サーバ[172.16.10.1](esxi2)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 172.16.10.1(esxi1)から 172.16.10.2(esxi2)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[172.16.10.1](esxi1)をクリックして選択します。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]という枠があるので、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「172.16.10.2」(esxi2)が vCenter 上で属しているデータセンタを選択します。次に、移動先となる[172.16.10.2](esxi2)のラジオボタンをチェックします。

一方、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 VM をサスペンドしてから移動を行い、移動後に VM 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 VM 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。さらに、移動後に VM 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動中の物理サーバに移動します。仮想マシンの稼動状態は保持されず、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 Storage Migration の[停止後に移動(Move)]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[停止後に移動(Move)]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、共有ストレージを利用できるので、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[172.16.10.2](esxi2)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。

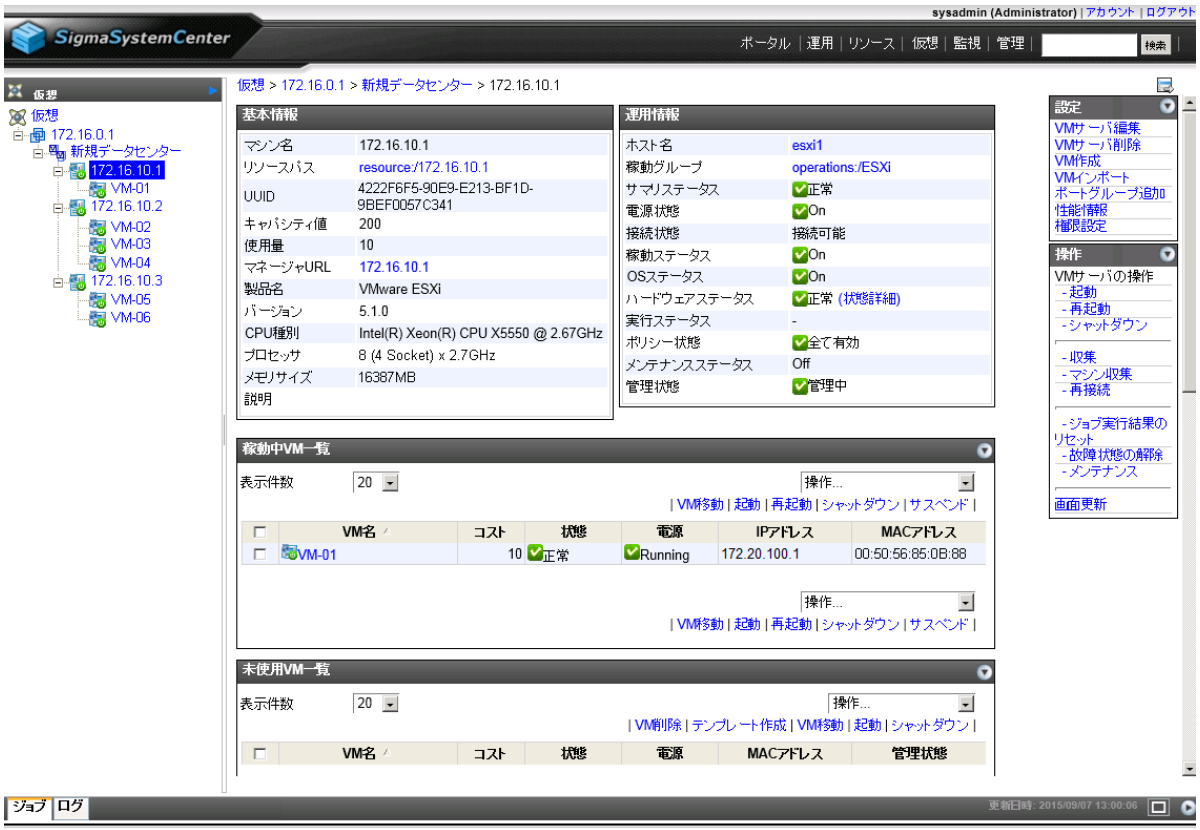


図　仮想マシン移動後の[仮想]ビュー

7. 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。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。本章では、管理対象マシン（物理サーバ(ESXi)、仮想マシン）の負荷状況を取得し、SSC の Web コンソール上で確認するための手順について説明します。

7.1 監視プロファイルの設定

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監視を実施する場合、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、負荷監視が可能となります。

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、デフォルトで用意されている監視プロファイル [Builtin]Standard Monitoring Profile (1min) をベースにして新規の監視プロファイル Standard Monitoring Profile for ConstructionGuide を作成する手順について説明します。

[Builtin]Standard Monitoring Profile (1min) は、4 つの性能情報について、1 分間隔で性能データを収集する監視プロファイルです。今回利用する監視プロファイル　Standard Monitoring Profile for ConstructionGuide は、[Builtin]Standard Monitoring Profile (1min) をベースに、監視する項目として メモリの空き容量割合を追加して、CPU 使用率とメモリの空き容量割合の閾値監視を有効にしたものです。

表　監視プロファイル比較

性能情報	説明	[Builtin]Standard Monitoring Profile		Standard Monitoring Profile for ConstructionGuide	
		データ収集	閾値監視	データ収集	閾値監視
CPU Usage (%)	CPU 使用率です。プロセッサの処理状況を示すために、ビジー時間を指定収集間隔内の平均割合としてパーセントで取得します。	有効	無効	有効	有効
Disk Space (MB)	ディスク空き容量です。ディスクドライブ上の利用可能な空き領域をメガバイト数で取得します。	有効	無効	有効	無効
Disk Transger Rate (Bytes/sec)	ディスク転送速度です。書き込みまたは読み取り操作中にディスク間でバイトが転送される速度を取得します。	有効	無効	有効	無効
Physical Memory Space (MB)	メモリ空き容量です。割り当て可能な物理メモリのサイズをメガバイト数で取得します。	有効	無効	有効	無効
Physical Memory	物理メモリの合計サイズに対する、割り当て可能なサイズの割合をパーセントで取得します。Physical Memory Space	無効	ー	有効	有効

性能情報	説明	[Builtin]Standard Monitoring Profile		Standard Monitoring Profile for ConstructionGuide	
		データ収集	閾値監視	データ収集	閾値監視
Space Ratio (%)	(MB) /メモリの合計サイズ×100 によって、計算する数値です。				

監視プロファイルの設定は[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。

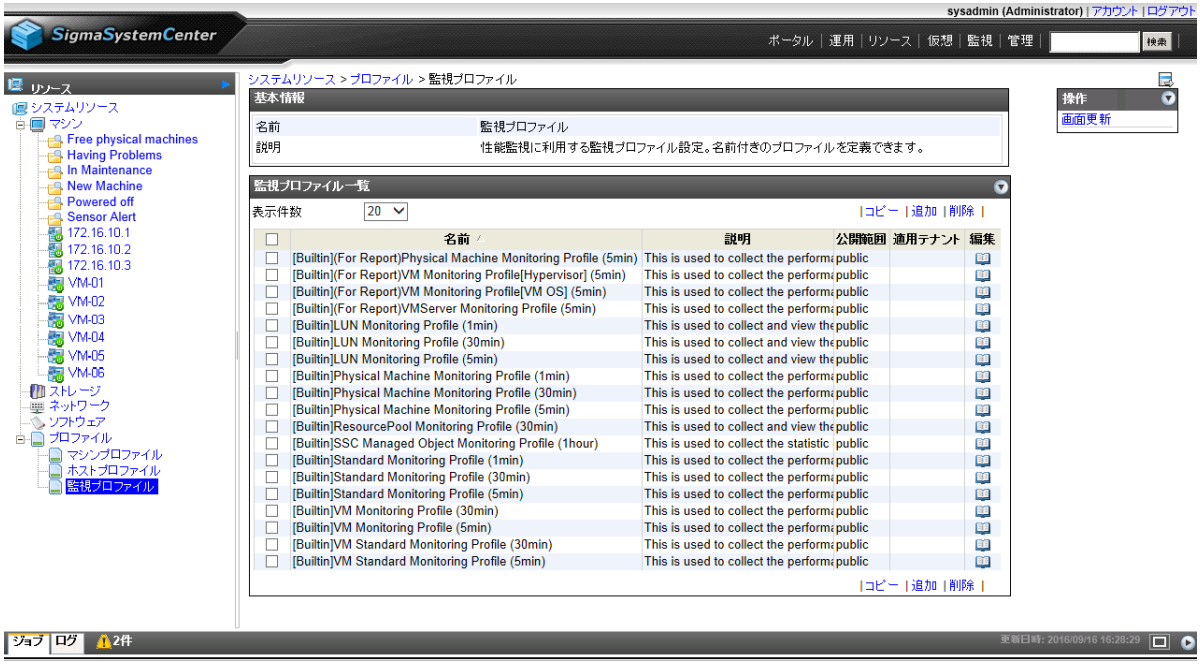


図　監視プロファイル一覧

[Builtin]Standard Monitoring Profile (1min) をチェックして、[コピー]をクリックします。コピー完了後、[Builtin]Standard Monitoring Profile (1min)[2] という名前の監視プロファイルが新たに追加されます。

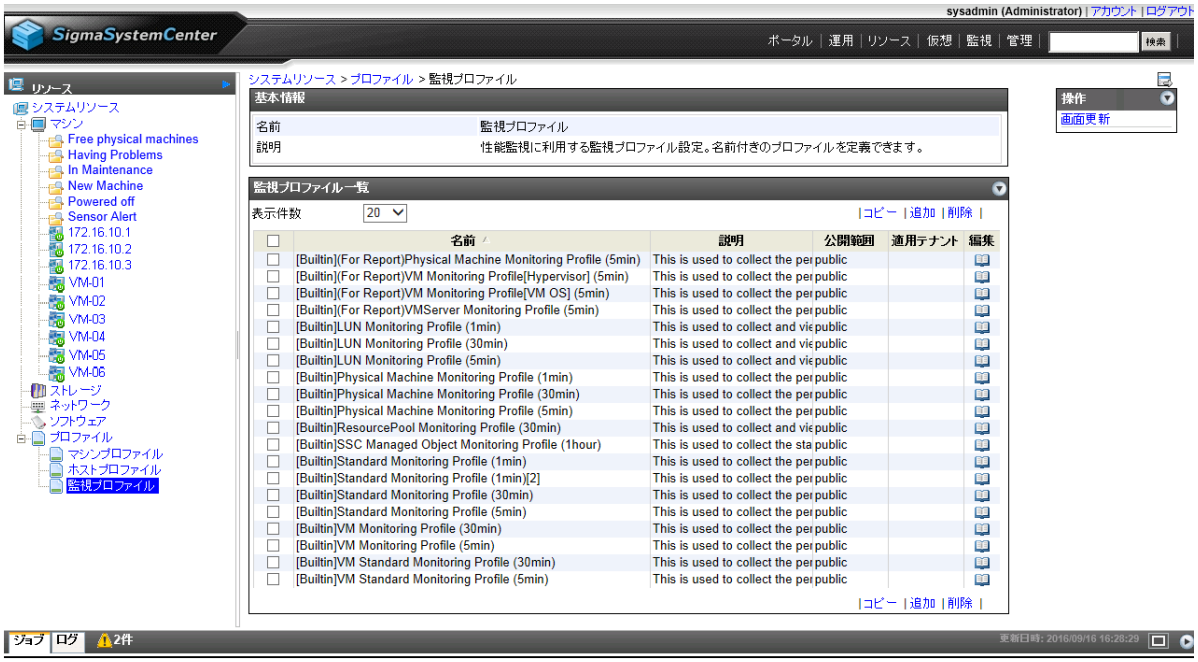


図　コピー実施後の監視プロファイル一覧

コピーした監視プロファイルを編集します。[Builtin]Standard Monitoring Profile (1min)[2] の[編集]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ので、プロファイル名として [Standard Monitoring Profile for ConstructionGuide]　と入力します。

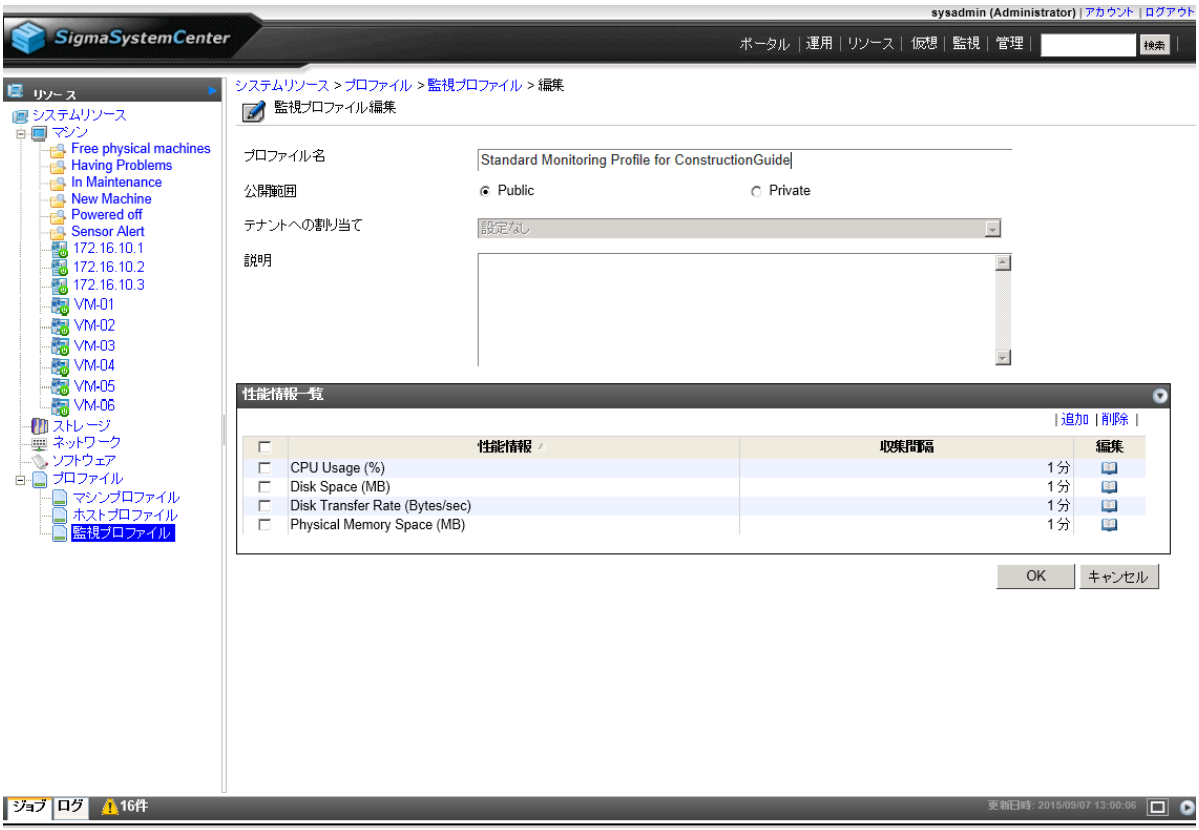


図　監視プロファイル編集

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[編集]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ので、「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。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）

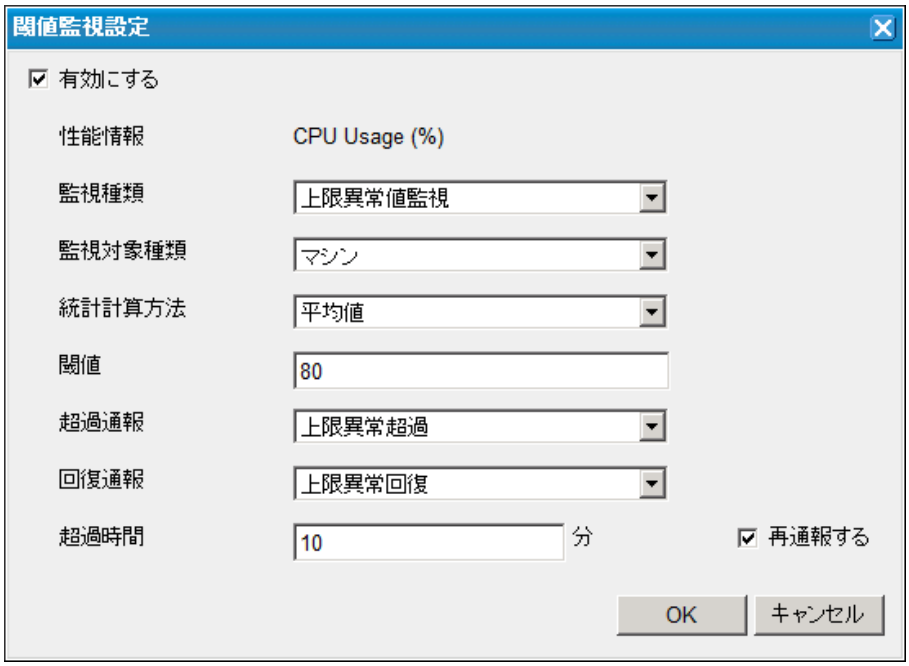


図　CPU Usage (%) の「閾値監視設定」

[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 (%) 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）

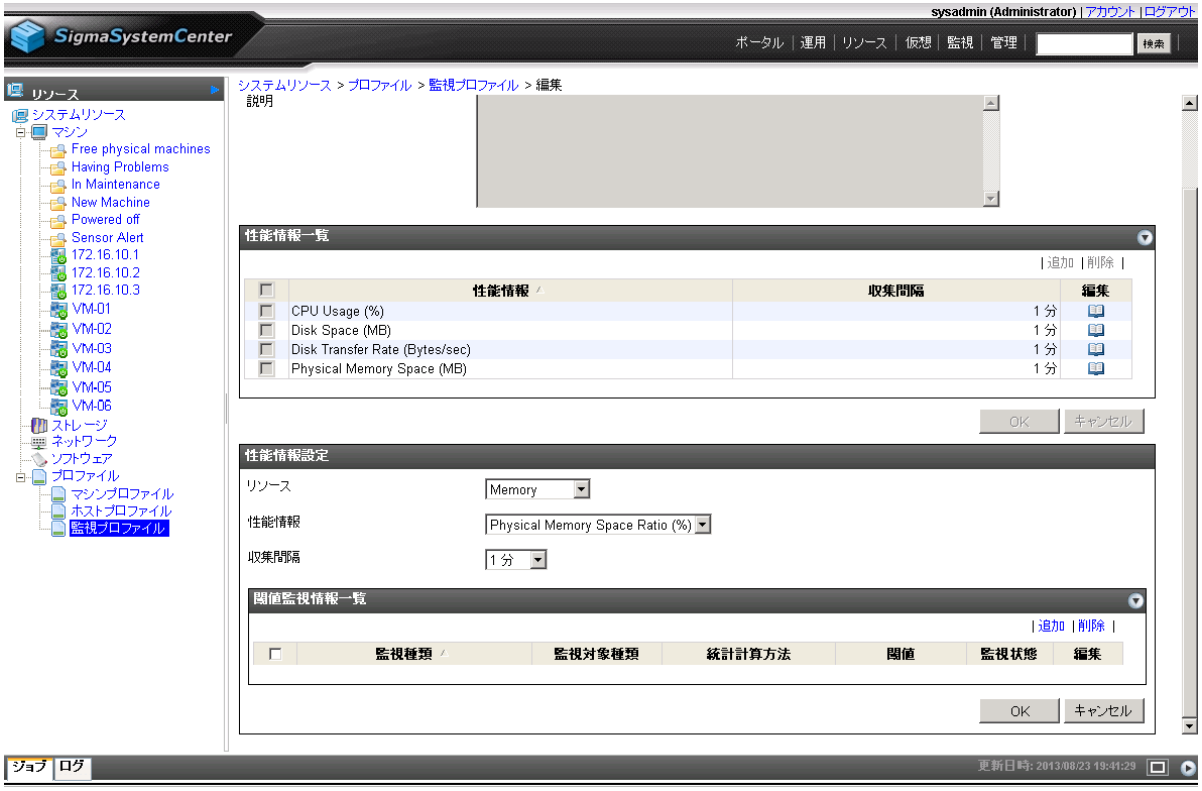


図　Physical Memory Space Ratio (%) 性能情報設定

Physical Memory Space Ratio (%) の閾値監視の設定を追加するので、「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）

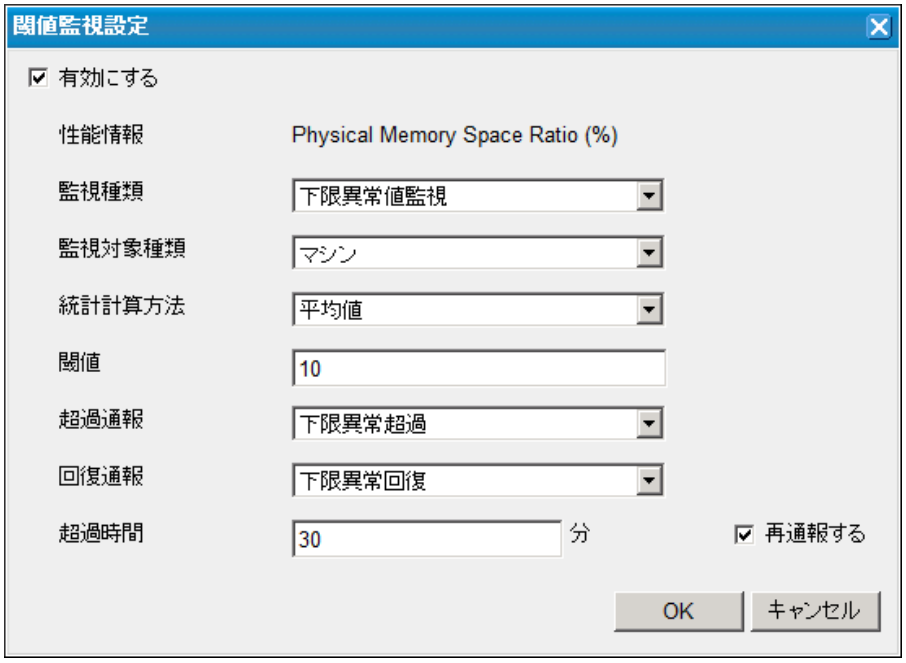


図　Physical Memory Space Ratio (%) 性能監視設定

[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。

性能情報設定の[OK]をクリックすると、性能情報一覧に設定が追加されます。

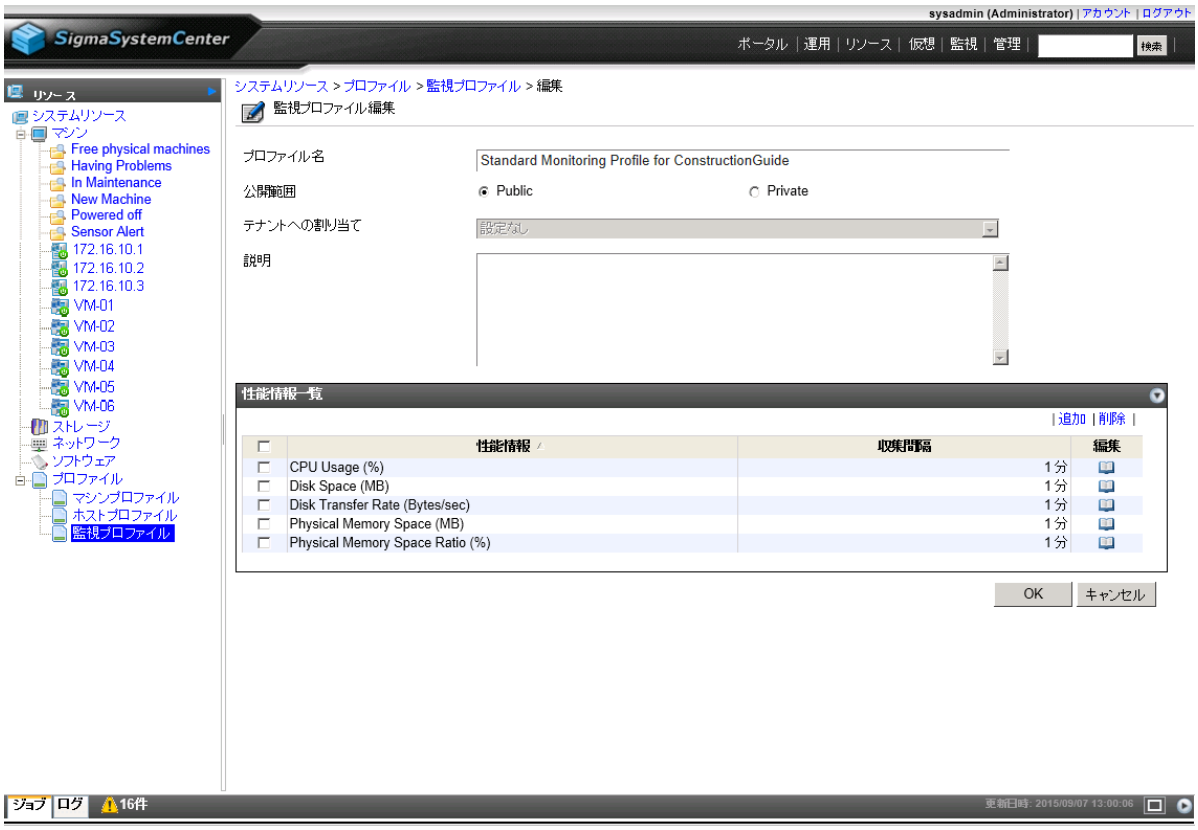


図　性能情報一覧

[OK]をクリックすると、監視プロファイル一覧が表示されます。監視プロファイルの名前が Standard Monitoring Profile for ConstructionGuide に更新されていることを確認します。

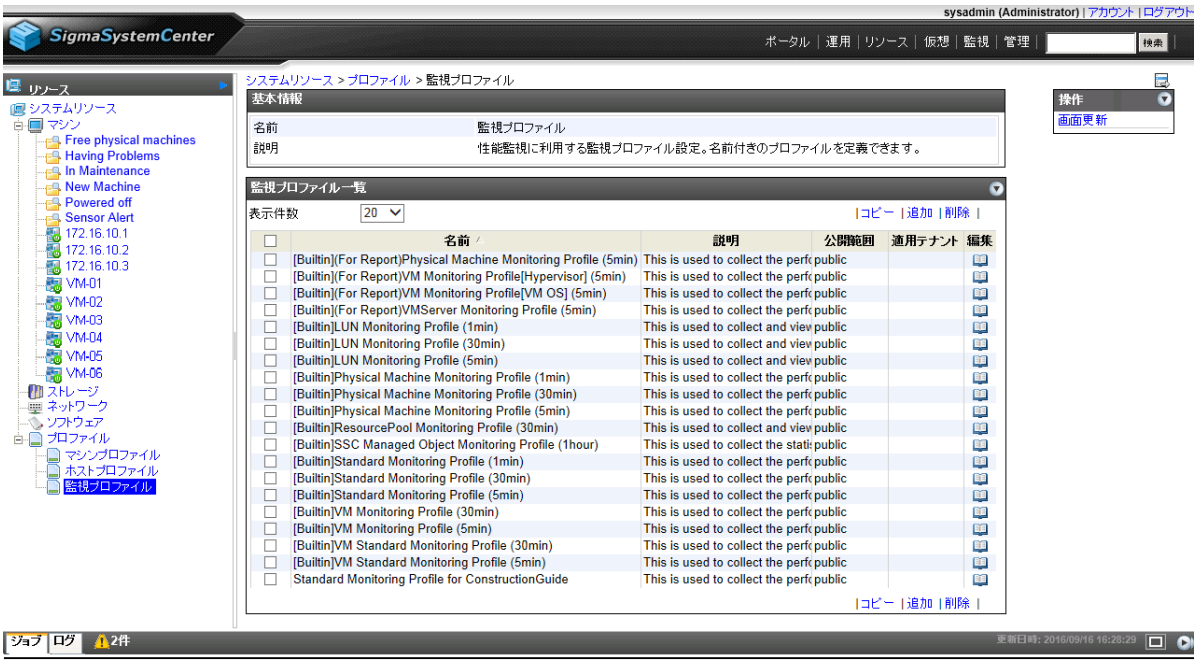


図　監視プロファイル一覧

これで、監視プロファイルの準備は完了です。

7.2 物理サーバの負荷監視の設定

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。

7.2.1 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。

7.2.2 ESXi 用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[ESXi]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：Standard Monitoring Profile for ConstructionGuide
- 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　グループの[性能監視]タブ

7.3　業務用 VM の負荷監視の設定

業務用 VM の負荷監視に必要な設定について説明します。

7.3.1　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。）

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。[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）

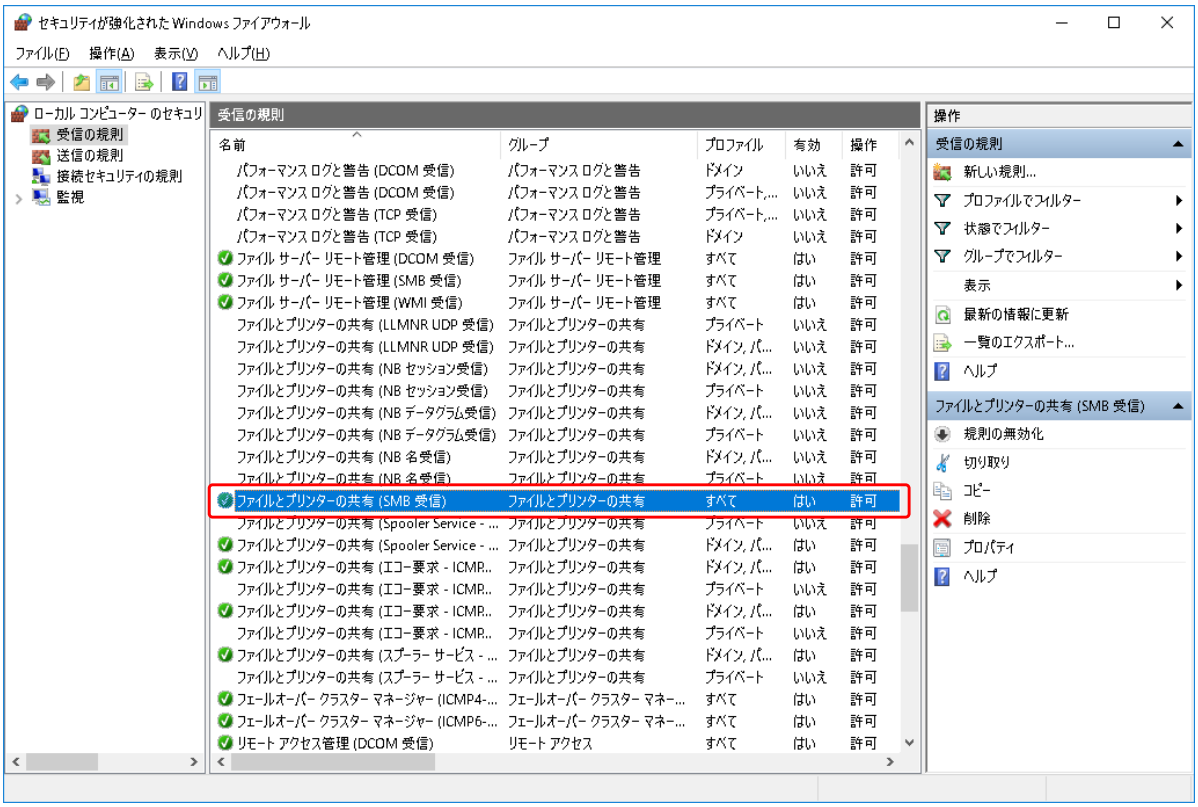


図　セキュリティが強化された Windows ファイアウォール

[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。

7.3.2　VM 用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[業務用 VM]をクリックします。業務用 VM 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：Standard Monitoring Profile for ConstructionGuide
- 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

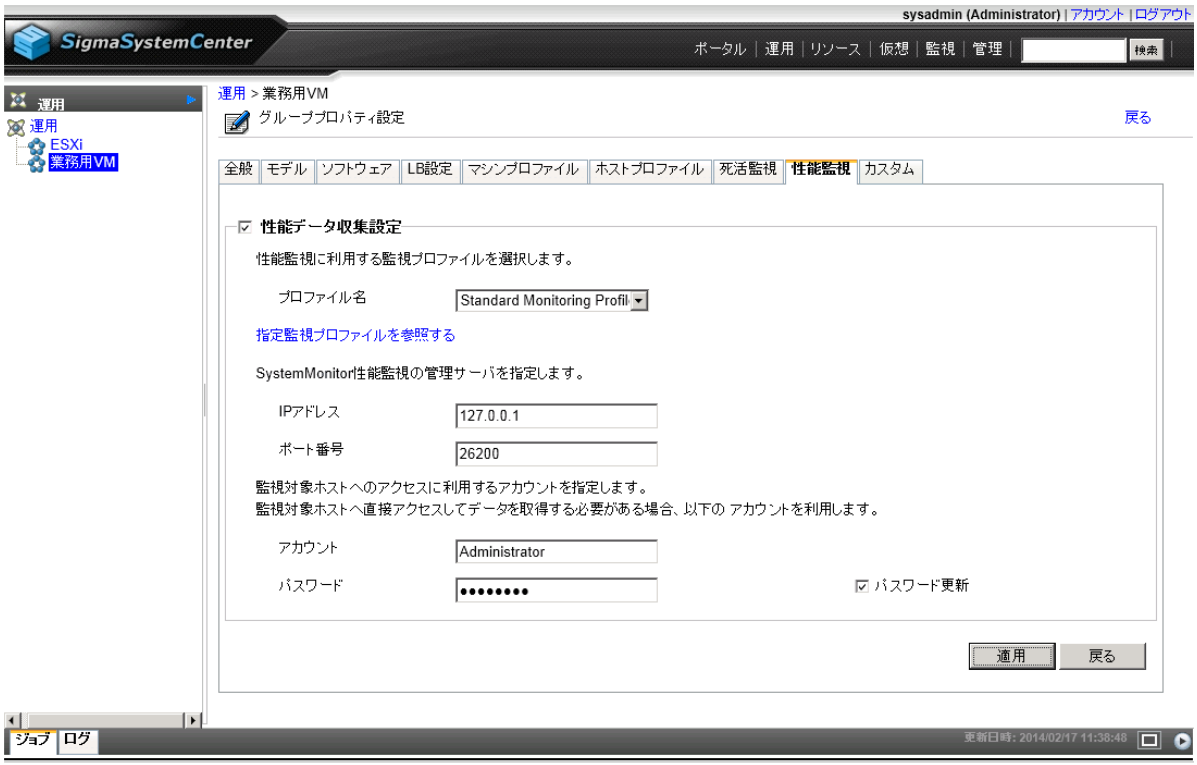


図　グループの[性能監視]タブ

7.4　動作テスト

では実際に、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。

注

負荷監視設定が有効化されるには、既述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[ESXi]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。

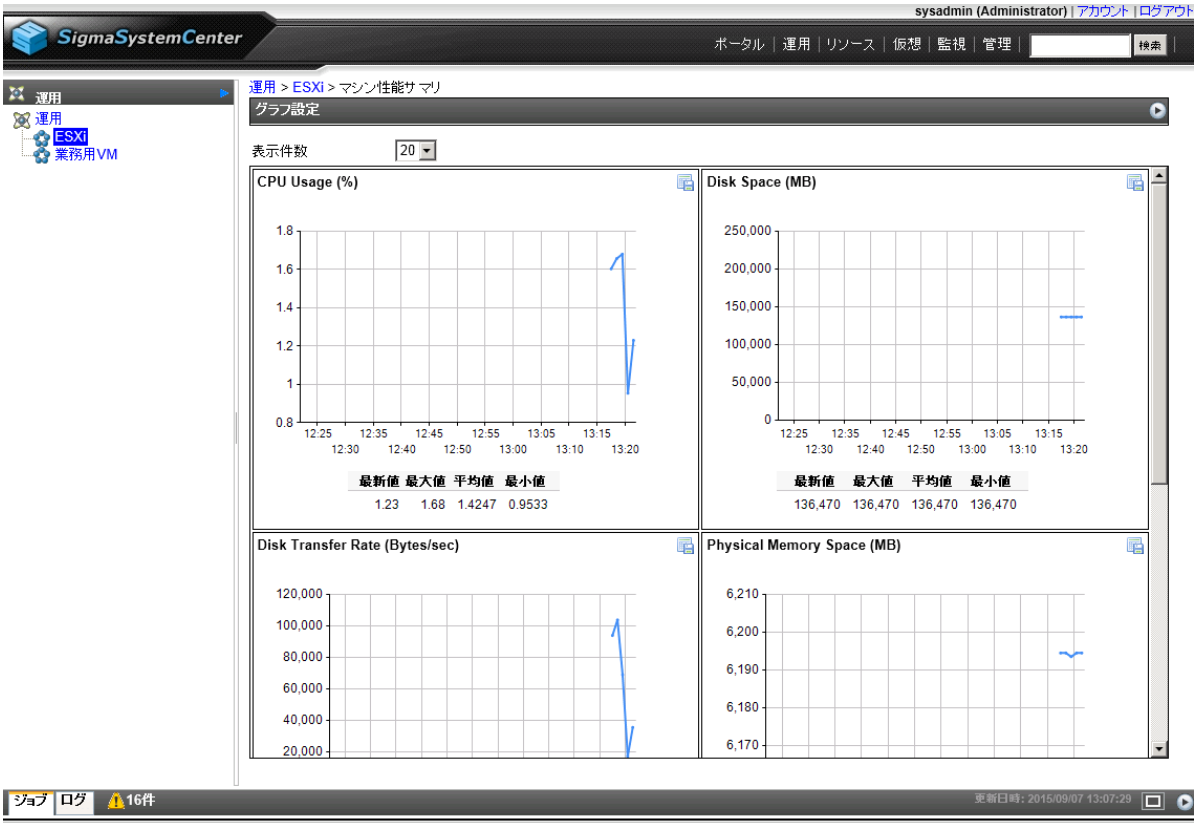


図　負荷状況

業務用 VM 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。

8. 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

ご覧のように、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うこともできますが、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うこともできます。

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ので、今回はこれらをインポートして利用します。

8.1 ポリシーのインポート

Web サイトから以下のファイルをダウンロードし、管理サーバの適当なフォルダに保存します。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。

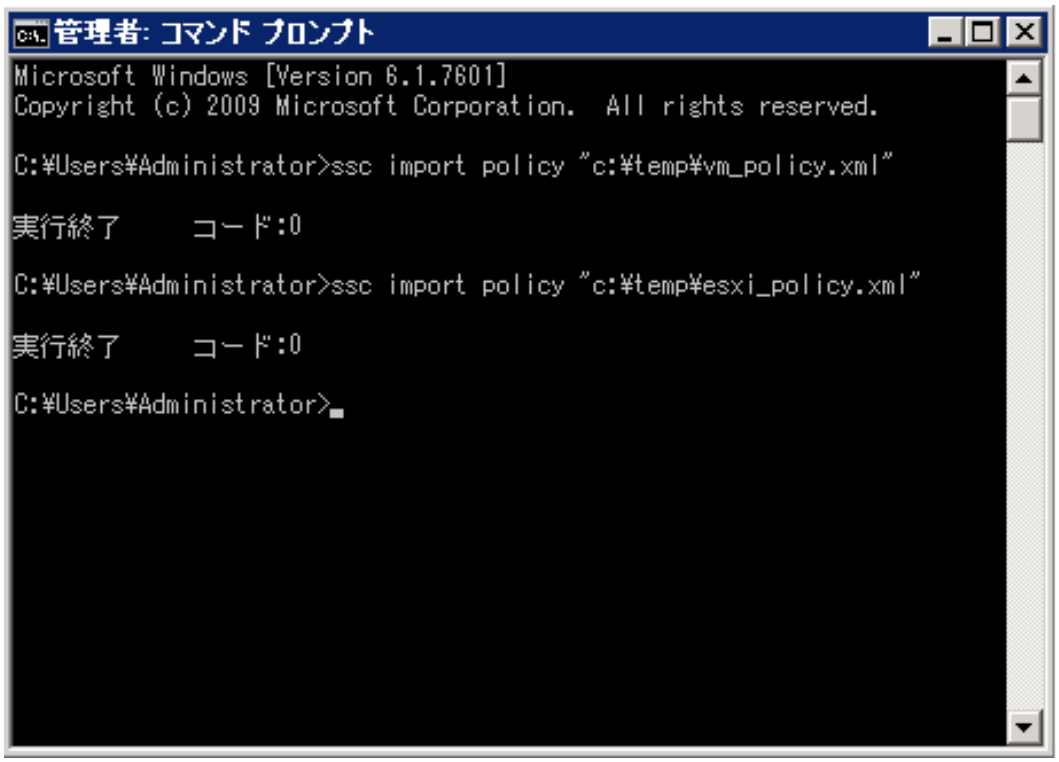


図　ssc コマンドによるポリシーのインポート（インポート実行後）

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。

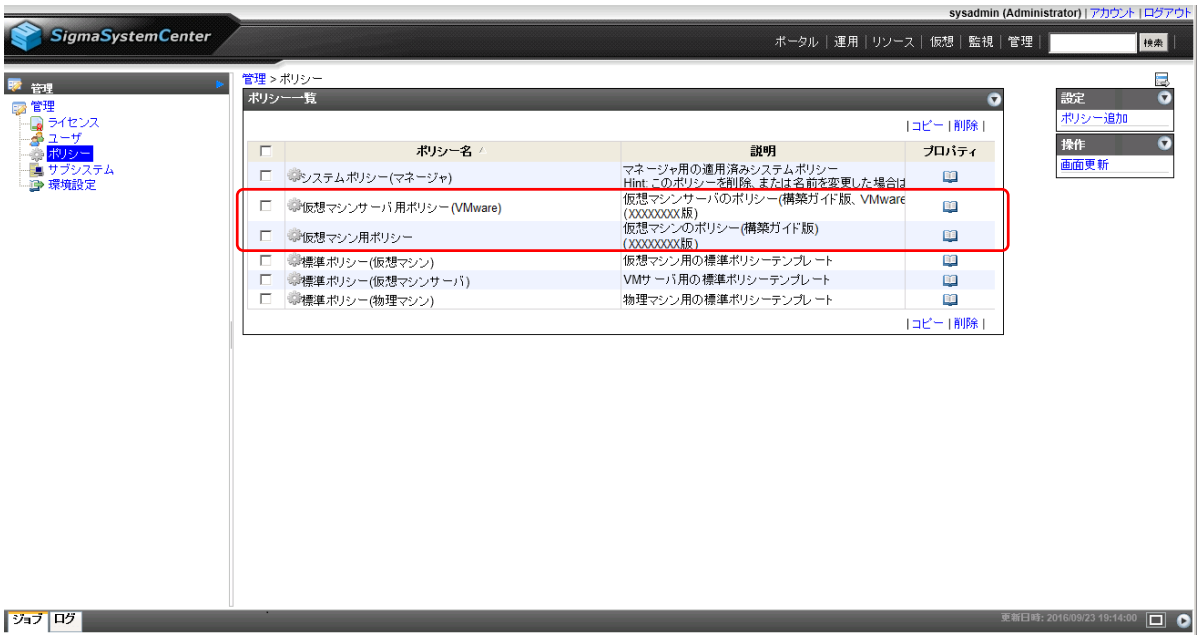


図 「ポリシー一覧」(インポート後)

「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。

8.2 仮想マシン用ポリシーの確認と適用

「6. 運用の基本設定 (40 ページ)」で設計したように仮想マシン用のグループ(業務用 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することにします。

8.2.1 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。

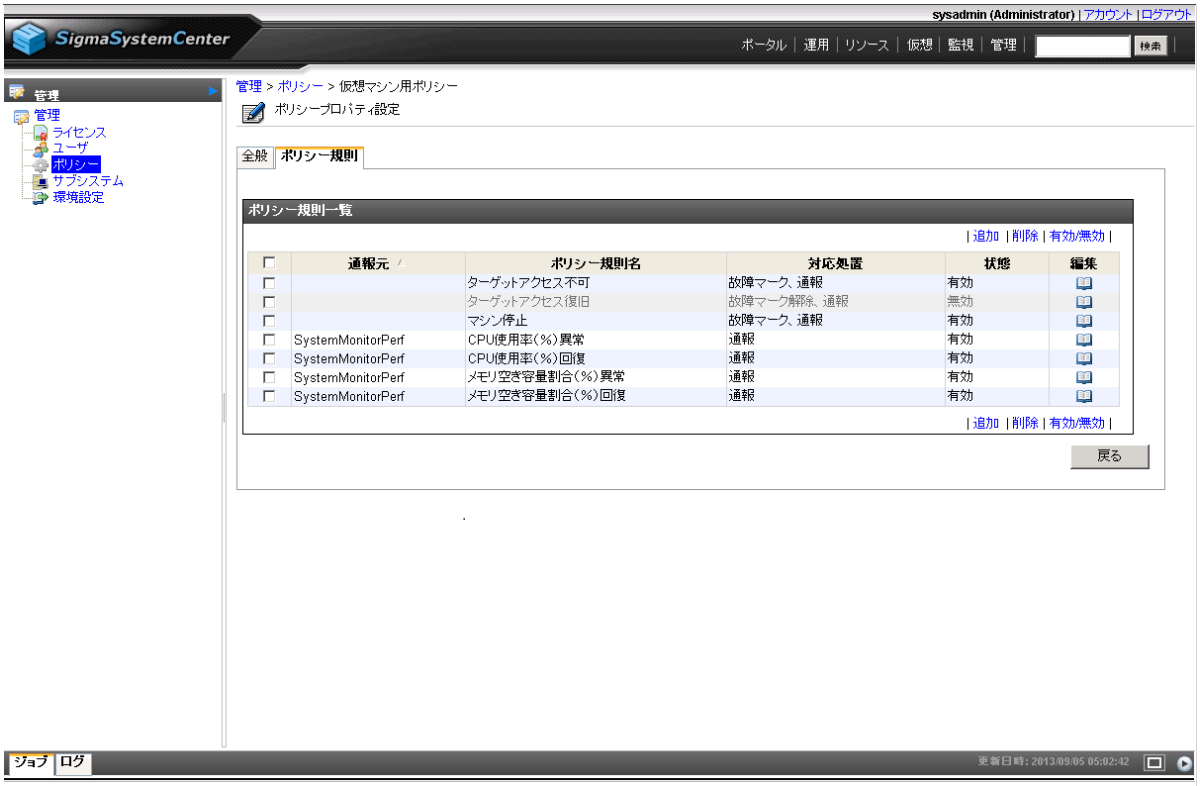


図 「ポリシープロパティ設定」画面（[ポリシー規則]タブ）

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。

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するので、何も変更せずに画面下の[戻る]をクリックします。

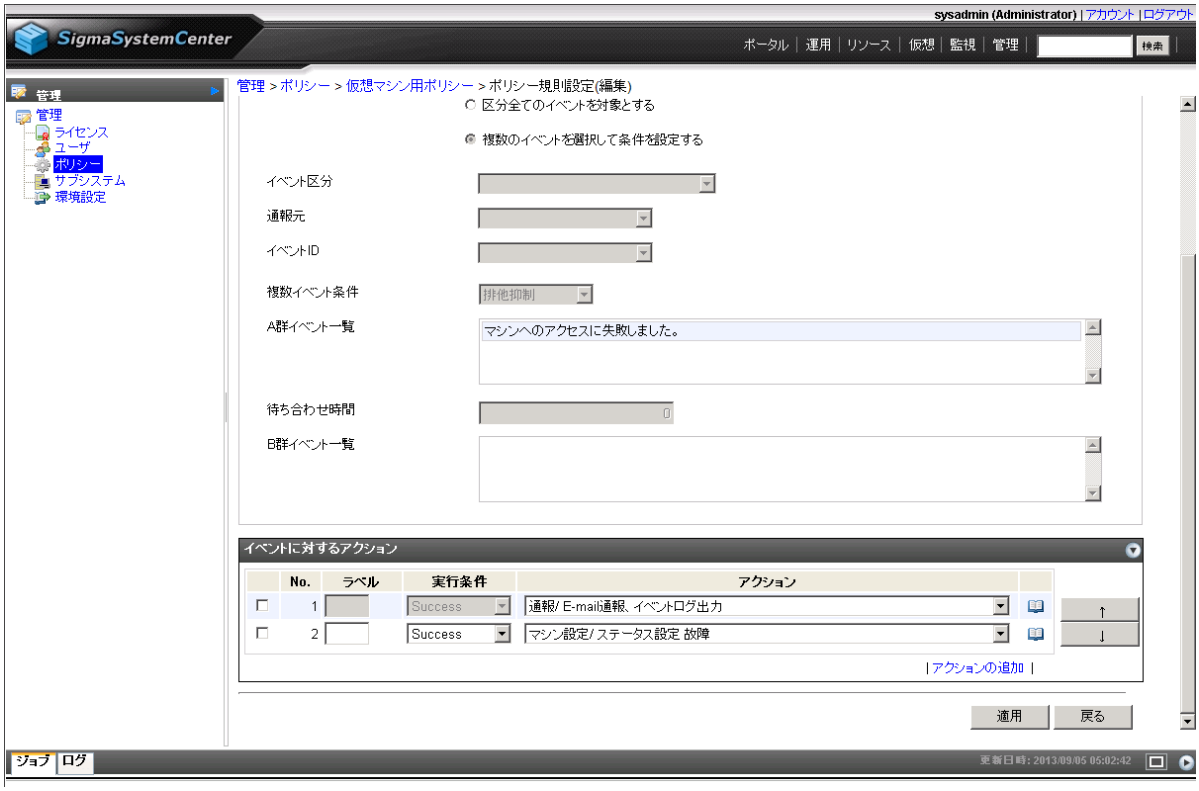


図　対応処置詳細設定（編集）

8.2.2　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、[業務用 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]を適用することにします。手順は以下のとおりです。

- 画面右上の[運用]をクリック
- ツリービューで対象グループ（ここでは[業務用 VM]）をクリック
- [設定]メニューの[プロパティ]をクリック
- [全般]タブをクリック
- [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
- 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。

8.3　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（ESXi 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。

8.3.1　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 VM 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 VM 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 VM 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、他の ESXi へ VM の移動を行います。まず、Migration（vMotion）により VM を稼動させたままの移動を試し、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：○○」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 VM の移動を行います。まず、Migration（vMotion）により VM を稼動させたままの移動を試し、Migration できない場合には、ESXi と VM をシャットダウン（できない場合は強制停止）し、VM 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 VM 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：○○」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。

- 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。

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、VM 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。

1. [運用]ビューのグループのプロパティのポリシー設定で停止、ESXi の停止/強制停止、VM の再起動（Failover）のアクションのアクションを含むポリシーを設定しない。
2. ポリシー規則一覧で ESXi の停止/強制停止、VM 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。
3. ポリシー規則の設定のイベントに対するアクションから ESXi の停止/強制停止、VM の再起動（Failover）のアクションを削除する。

   また、ポリシー規則の設定のイベントに対するアクションに Migraion が失敗した場合、再起動(Failover)を行うアクションがある場合は、Migraion のみを行うアクションに変更する。

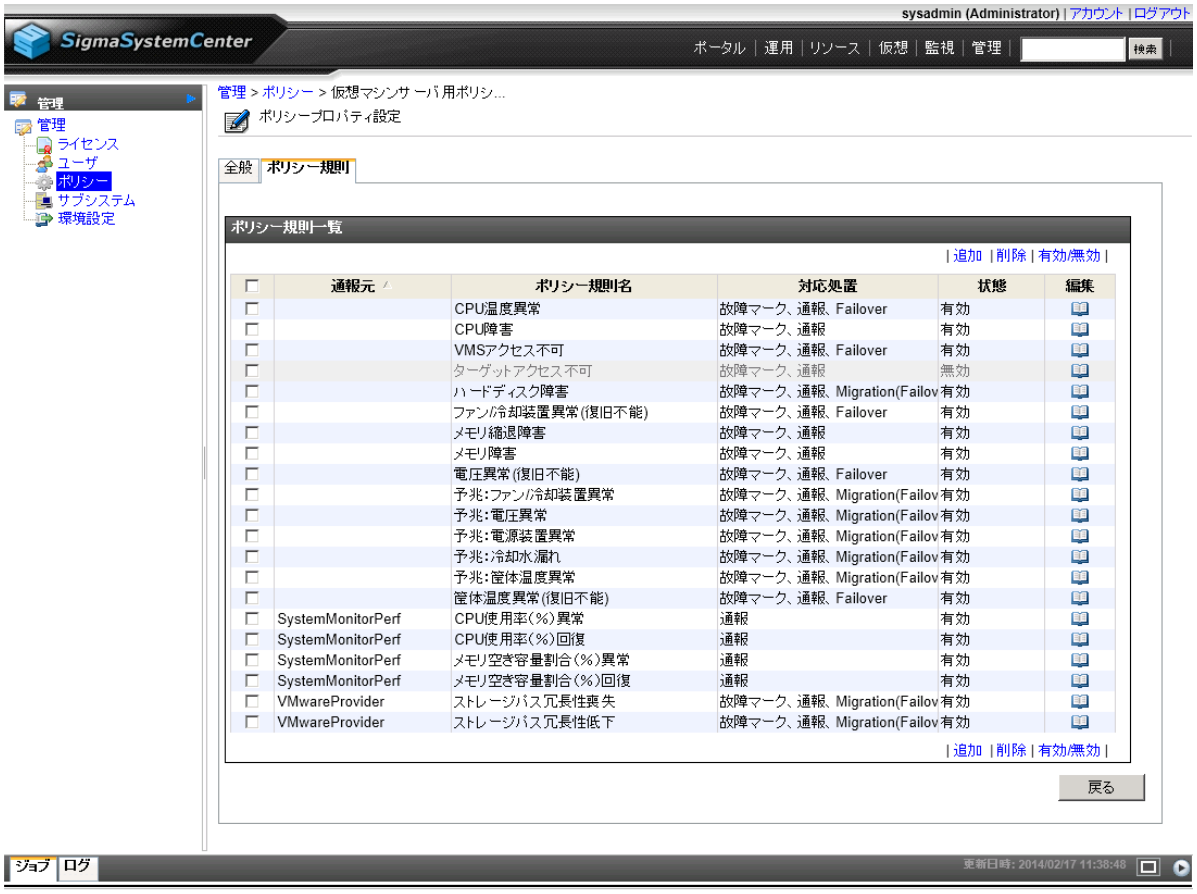


図　仮想マシンサーバ用ポリシー(VMware)の[ポリシー規則]タブ

8.3.2 故障状態の物理サーバの制約と故障状態の解除

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 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 を Migration（vMotion）や 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ことは当然のことですが、さらに、故障状態を解除することで 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、次の操作をおこないます。

- 画面右上の[リソース]をクリック
- [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
- 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
- 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
- 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
- 左側の[操作]メニューの[故障状態の解除]をクリック

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。

8.3.3 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行います。

[esxi1]、[esxi2]にポリシーを適用するために、[ESXi]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。

- 画面右上の[運用]をクリック
- ツリービューで対象グループ（ここでは[ESXi]）をクリック
- [設定]メニューの[プロパティ]をクリック
- [全般]タブをクリック
- [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(VMwar)]を選択
- [適用]をクリック後、[戻る]をクリック

図　物理サーバへのポリシー適用

8.4 死活監視の設定

死活監視を行うには、「4.3　死活監視の基本設定（16 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、「6.1 運用グループの作成（40 ページ）」で作成したグループの単位で死活監視の設定を行います。

8.4.1 グループ単位の死活監視の設定

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、[業務用 VM]グループの設定を行うことにします。業務用 VM に先ほど適用した[仮想マシン用ポリシー]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、業務用 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。次の手順で、Ping 監視、ポート監視を行うように設定します。

- ツリービューにある[業務用 VM]グループをクリック
- [設定]メニューの[プロパティ]をクリック
- 「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
- [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
- [Ping 監視]チェックボックスをチェック
- [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
- 右下の[適用]を押す

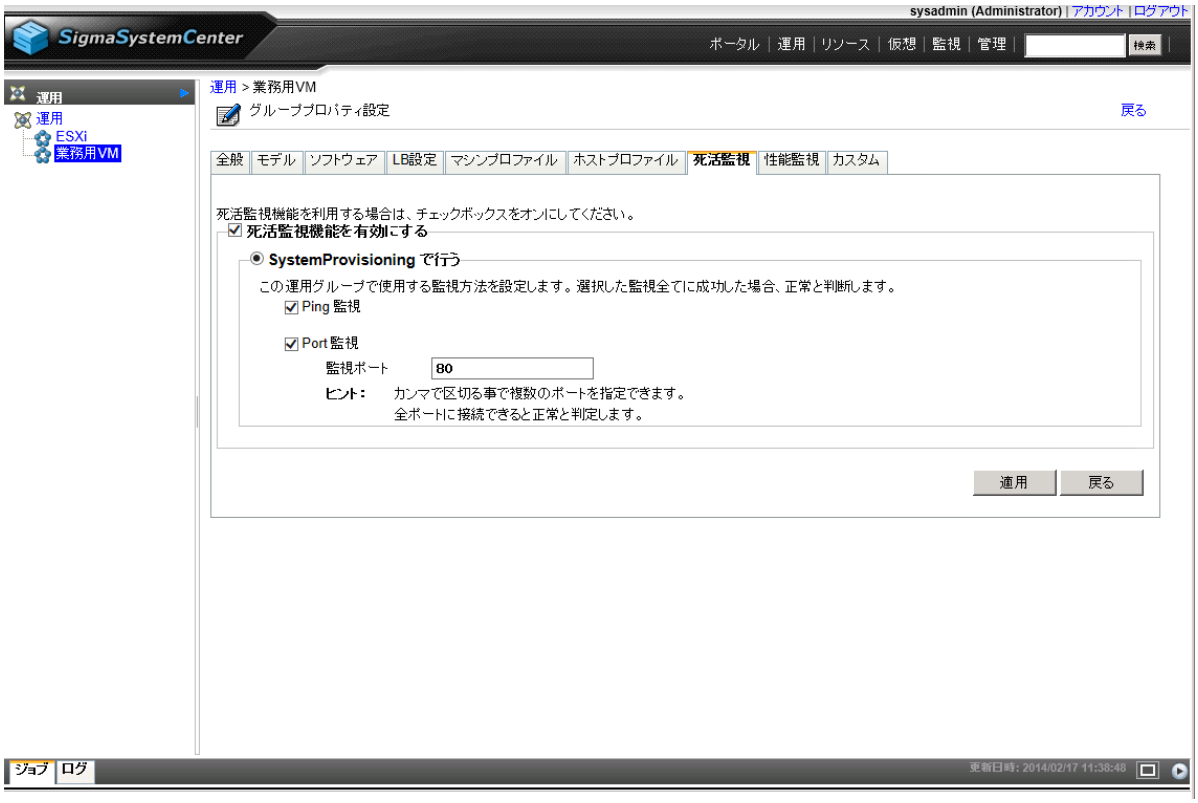


図 「グループプロパティ設定」画面（[死活監視]タブ）、Ping 監視、Port 監視の設定

ESXi グループの物理マシンに先ほど適用した[仮想マシンサーバ用ポリシー(VMware)]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。

ESXi グループの物理マシンについては、ESMPRO による死活監視を行わないので、次の手順で ESMPRO による監視を無効にします。

- ツリービューにある[ESXi]グループをクリック
- [設定]メニューの[プロパティ]をクリック
- 「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
- [ESMPRO/SM にマシンを登録する]チェックボックスのチェックを外す
- [死活監視機能を有効にする]チェックボックスのチェックを外す
- 右下の[適用]を押す

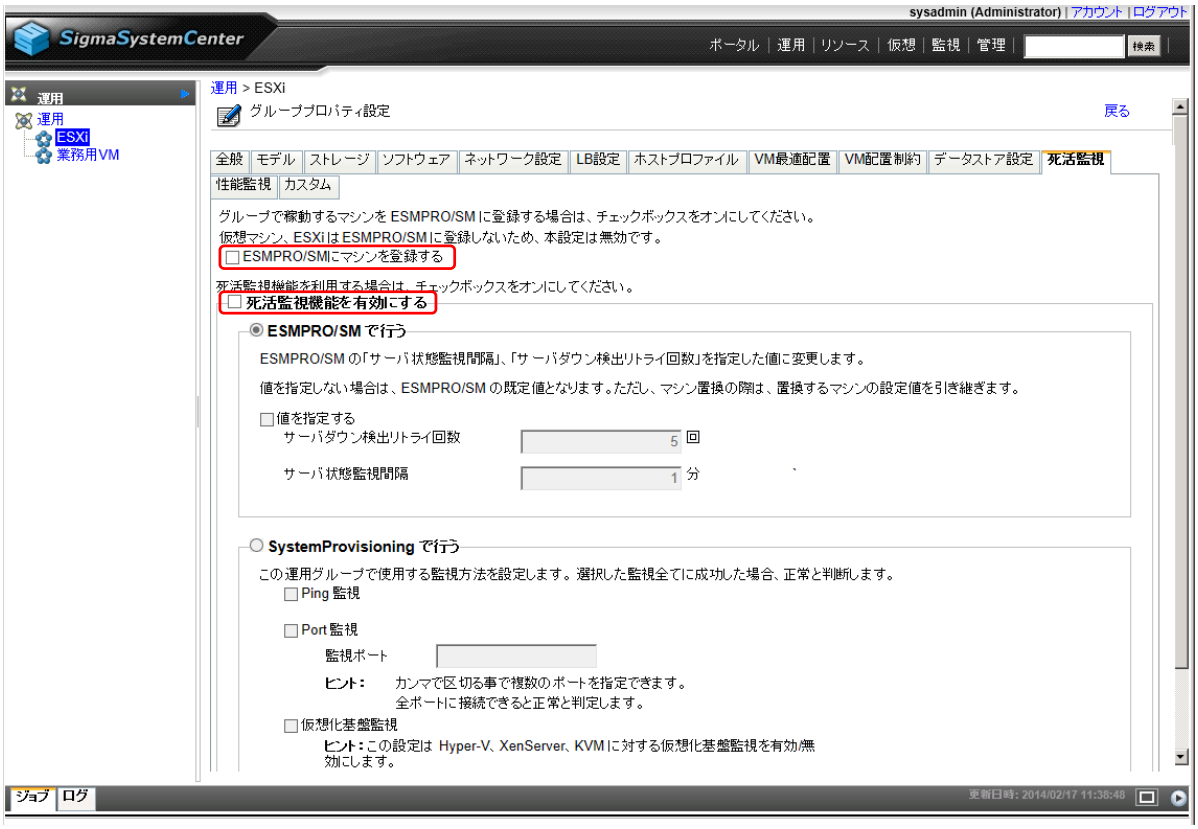


図 「グループプロパティ設定」画面（[死活監視]タブ）

8.5 動作テスト

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[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、VM 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

「8.3.1　物理サーバ用のポリシーの確認（75 ページ）」では、上記の VM の他の ESXi への移動(Migration)が失敗した場合は、物理サーバ[esxi1]と VM をシャットダウン（できない場合は強制停止）し、VM 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、管理サーバの適当なフォルダに解凍・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 VMwareProvider "Storage path is all down"
"Storage path is all down" ESXi esxi1
```

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[ESXi]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るので、[ESXi]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[172.16.10.1]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[172.16.10.1]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:/172.16.0.1/新規データセンター/172.16.10.1]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[172.16.10.1]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、[172.16.10.1]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 VM の移動が完了していない場合、[172.16.10.1]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、VM 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 VM 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、[172.16.10.1]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。

[172.16.10.1]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　[172.16.10.1]の状態一覧の画面

最後に、テストの確認が終わったら、[仮想]ビューで故障状態を解除し、[172.16.10.1]の配下に[VM-01]と[VM-02]を移動しておきます。

ツリービューの[172.16.10.1]をクリックし、[172.16.10.1]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、[172.16.10.1]の配下への VM の移動を行います。

「6.2 手動での Migration（vMotion）（51 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 配置を簡単に確認することができます。また、過去の VM 配置に 1 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[ESXi]をクリック後、[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が確認できるように、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みると次の画面の表示のようになります。

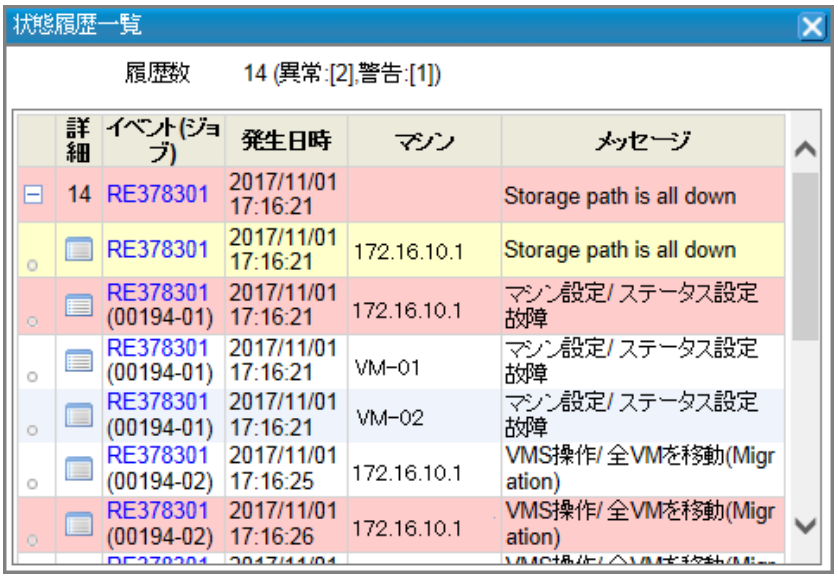
前述で説明しました[172.16.10.1]に対して、[故障状態の解除]を実行した後の状態が表示されています。

図 [172.16.10.1]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。

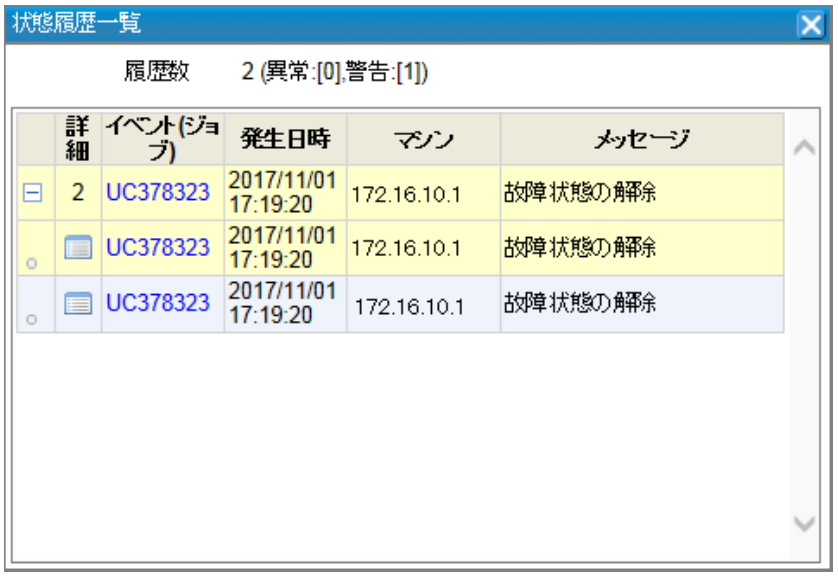
- 前述の図中に表示されている数字が 14 の赤丸には、擬似障害のイベントや VM 移動などの対応処置による状態変更が含まれます。

  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、[172.16.10.1]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 ESXi 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

VM 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[172.16.10.1](esxi1)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。

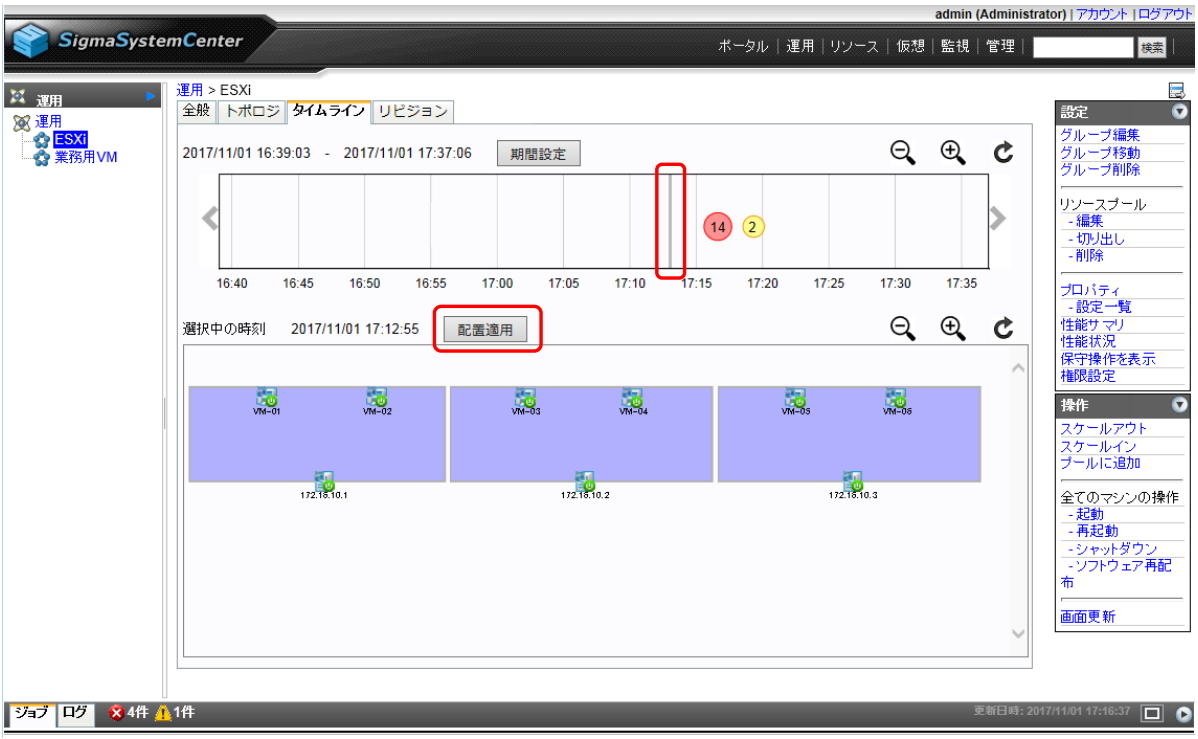


図　擬似障害テスト前の VM 配置

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、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. 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 3.6	WebSAM SigmaSystemCenter 3.6 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 3.6 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 3.6 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 3.6 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 5.10	SystemMonitor 性能監視 5.10 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。

http://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	2017.12	新規作成
第 1.1 版	2018.1	「8.3.1. 物理サーバ用のポリシーの確認」、「8.5. 動作テスト」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。

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。

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。

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。

マスタマシン

作成元とするマシン 1 台を構築し、そのマシンのイメージを他のマシンにクローニング (複製) することにより、複数のマシンを同じ構成で作成することができます。この作成元となるマシンをマスタマシンと呼びます。

マスタ VM

仮想マシンを作成するためのテンプレートの作成元とする仮想マシンです。

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。

論理マシン

SigmaSystemCenter は、ハードウェアの機能によって MAC アドレスや WWN、UUID などを仮想化したマシンを論理マシンとして扱います。論理マシンは、もともと装置に設定された ID を持つ物理マシンと関連付けて管理します。

SigmaSystemCenter 3.6 簡易構築ガイド VMware 編

SSC0306-doc-0048-1.1

2018 年 1 月 1.1 版 発行