OpenManage Essentials を使用した仮想化環境の管理と監視

この Dell テクニカルホワイトペーパーは、VMware ESXi、VMware ESX、Microsoft Hyper-V サーバを含む仮想化環境の管理・監視方法を説明します。

OME エンジニアリングチーム

2013 年 8 月 | バージョン 1.0

目次

表

図

要旨

OpenManage Essentials (OME) は、サーバ、ストレージデバイス、プリンタ、KVM、UPS、PDU、シャーシ、ネットワークデバイス、その他のモニタリングに利用できる「一対多数」対応の管理ツールです。OME は、仮想化環境内に設置された VMware ESXi、VMware ESX、Microsoft Hyper-V、Citrix XenServer の監視と管理をサポートしており、これらのサーバ上で、検出とインベントリ、アラートの受信、システムのアップデート、OpenManage Server Administrator (OMSA) の導入を実行できます。本書は、これらのサーバを容易に管理／監視するための情報を提供します。

はじめに

本書の目的は、OpenManage Essentials を活用した、仮想化環境 (VMware ESXi、VMware ESX、Microsoft Hyper-V、Citrix XenServer) の管理・監視方法を示すことにあります。OpenManage Essentials を使用して仮想化環境を管理する主なメリットは次のとおりです。

- 「検出とインベントリ」を実行すると、サーバとその仮想マシンを含む仮想化環境の全メンバを、デバイスツリー内にグループ分けすることができます。仮想化サーバ上に作成される仮想マシンは、デバイスツリー内で、仮想化サーバのサブノードとして表示されます。

  注： Citrix XenServer の場合、仮想マシンの分類はサポートされません。
- 全種類の仮想化サーバを、1 つのコンソールからたった 1 つのタスクを実行するだけで、管理できるようになります。検出とインベントリの範囲を指定することもでき、サポートする全プロトコルを通して、すべての仮想マシンとそのホストサーバを含めることも可能です。
- VMware ESXi、VMware ESX、Microsoft Hyper-V、Citrix XenServer などのホストサーバは、1 つのタスクから、利用可能な最新パッケージを使って一括アップデートすることができます。
- ホストサーバは、OpenManage Essentials コンソールにアラートを送信するよう構成できます。OpenManage Essentials の「アラート処置」機能を構成すれば、アラートの受信時に、様々な対応措置が実行できます。
- OpenManage Essentials の検出とインベントリ機能は、ホストサーバの詳細情報だけでなく、仮想マシンの基本情報や詳細な電源ステータスも収集できます。
- デバイスツリー内では、同種類のホストサーバ同士がそれぞれ個別のグループにまとめられます。たとえば、すべての ESXi および ESX サーバは、デバイスツリー内で「VMware ESX Servers」というグループに、Hyper-V サーバは「Microsoft Virtualization」というグループに、XenServer は「Citrix XenServers」というグループにそれぞれ分類されます。XenServer 用のグループが個別に作成されるようになったのは、OpenManage Essentials バージョン 1.2 からです。v1.2 より前のバージョンでは、デバイスツリー内のサーバグループの一員として表示されるのみでした。上記のサーバはすべて、デバイスツリー内の「Servers」配下にも、重複したエントリが表示されます。

仮想化サーバ： 検出とインベントリ

仮想化したサーバの検出とインベントリは、様々なプロトコルを通して実行されます。ホストサーバとその仮想マシンを検出・インベントリする際に必要となるプロトコルは、表 1 を参照してください。ホストサーバを検出するには、SNMP プロトコルを有効にする必要があり、さらに、デバイスツリー内で仮想化サーバを正しく分類するため、その他のプロトコルが必要になる場合もあります。プロトコルを適切に構成すれば、デバイスツリー内の各ホストサーバのもとに、それぞれの仮想マシンを正しくグルーピングすることができます。

表 1. ホストサーバと仮想マシンの検出をサポートするプロトコル

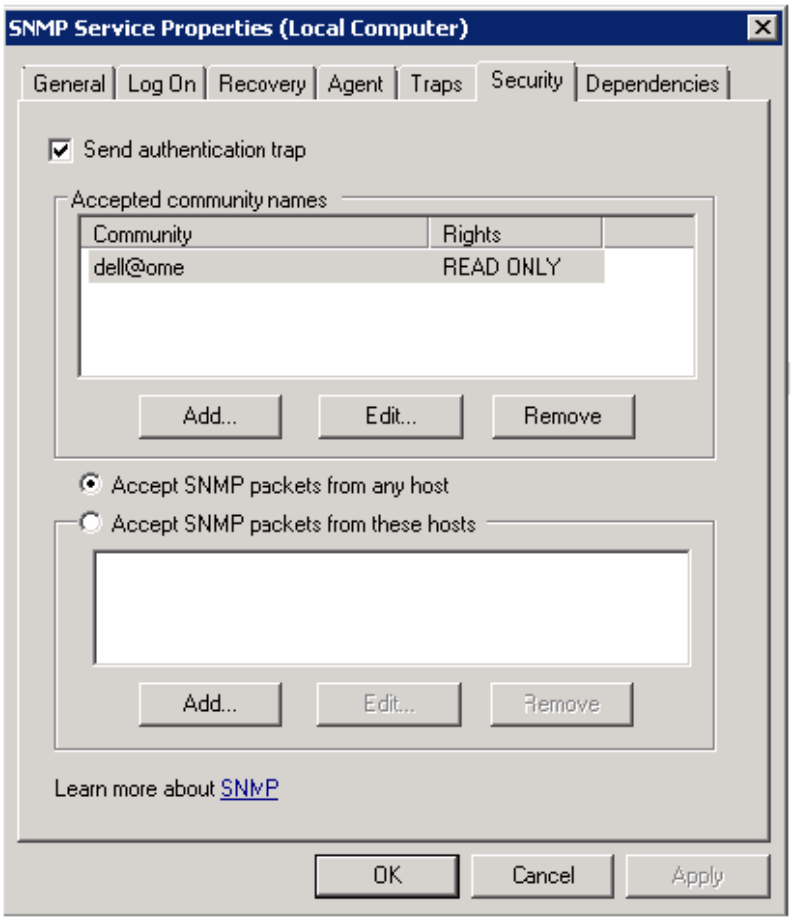
ホストサーバ	検出、インベントリ、ホストサーバと仮想マシンとの対応付けに必要なプロトコル	仮想マシンの検出とインベントリに必要なプロトコル
Citrix XenServer	SNMP	–
Microsoft Hyper-V	WMI	SNMP
VMware ESX	SNMP	SNMP
VMware ESXi	SNMP+WSMAN	SNMP

Microsoft Hyper-V の SNMP 構成

Microsoft Hyper-V サーバで SNMP を有効にするには、以下を実行します。

1. [スタート]→[ファイル名を指定して実行] を選択し、「`services.msc`」と入力して [OK] を押します。
2. [SNMP サービス] を右クリックし、[プロパティ] を選択します。
3. [セキュリティ] タブを選択し、コミュニティストリングを入力します (図 1)。

図 1. Microsoft Hyper-V の SNMP コミュニティストリング設定例



VMware ESX と Citrix XenServer の SNMP 構成

VMware ESX または Citrix XenServer で SNMP を有効にするには、**/etc/snmp/snmpd.conf** ファイルに「**rocommunity <community>**」(<community> には適切なコミュニティストリングを入力) を追加した後、**service snmpd restart** コマンドを使用して、snmp サービスを再起動します。

ESXi ホストの SNMP 構成

ESXi ホスト上で SNMP を有効にするには、PuTTY を使って ESXi コンソールにログインした後、以下を実行します。

1. まず、ESX ファイアウォールを開きます。

   ```
   esxcfg-firewall -e snmpd
   ```

2. 次に、SNMP を構成します。

   ```
   vicfg-snmp.pl –server <server>–username <user> –password <pass> -p <port>
   vicfg-snmp.pl –server <server>–username <user> –password <pass> -c <community>
   ```

   このとき、<community> には SNMP コミュニティストリングが入ります。

3. SNMP サービスを有効にします。

   ```
   vicfg-snmp.pl –server <server>–username <user> –password <pass> –enable
   ```

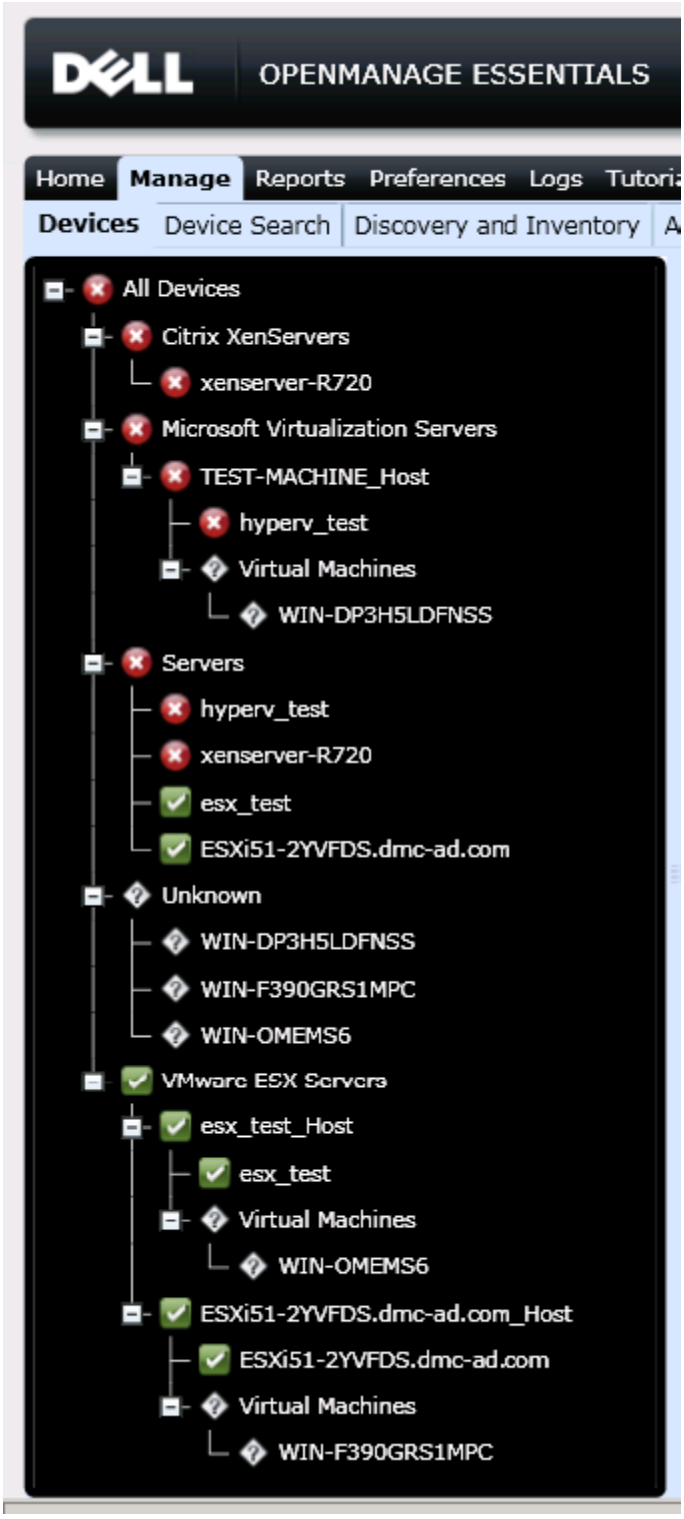
これで SNMP がオンになり、ホストを確認できるはずです。

ESXi 上での詳細な SNMP 構成方法は、英語版ホワイトペーパー『How to setup and configure ESXi 5 for use in OpenManage Essentials』 (http://en.community.dell.com/techcenter/extras/m/white_papers/20071085.aspx) を参照してください。

デバイスツリー内に、ホストサーバとその仮想マシンを分類する方法

図 2 は、検出とインベントリの実行後、デバイスツリー内にホストサーバ (ESXi、ESX、Hyper-V、XenServer) とその仮想マシンがグループ化された画面例です。

図 2. デバイスツリー内に分類されたホストサーバとその仮想マシン



仮想化サーバ： アラートの受信

ホストサーバとその仮想マシンは、OpenManage Essentials コンソールにアラート／トラップを送信するよう構成できます。これらのアラートから、以下のように様々な組み込みアクション (処置) が実行可能です。

- アプリケーションの起動： このアラート処置は、特定のアラートを受信したときに、アプリケーションを実行することができます。
- 電子メール： このアラート処置は、OpenManage Essentials が受信したアラートを指定の電子メールアドレスに転送します。
- 無視： システム管理者がアラートを一切受信したくないときは、この機能を使ってアラートを無視できます。デフォルトでは、DefaultDuplicateAlertFilter (既定重複アラートフィルタ) が有効になっているため、15 秒以内に同じアラートを受信すると、2 回目のアラートは無視されます。
- トラップの転送： OpenManage Essentials は、アラートを別の OME コンソールや、その他のコンソール (Microsoft SCOM、Dell-DMC など) に送信するよう構成できます。これらのアラートは、受信したままのフォーマットで転送することも、OpenManage Essentials コンソールからアラート送信する時と同じフォーマットに整えて転送することもできます。

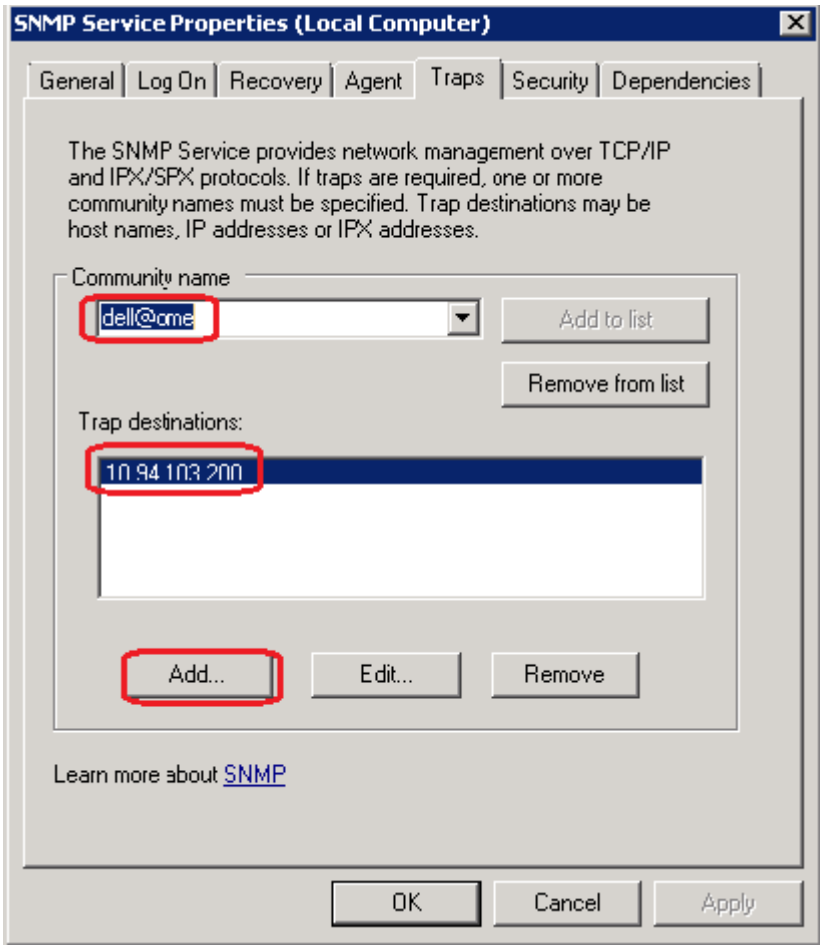
  トラップ転送の詳細は、英語版ホワイトペーパー『Forwarding Dell Hardware Alerts in a Tiered Monitoring Environment』(http://en.community.dell.com/techcenter/extras/m/white_papers/20278428.aspx) を参照してください。

Microsoft Hyper-V サーバでトラップ転送先を設定する方法

Microsoft Hyper-V サーバで SNMP を有効にするには、以下を実行します。

1. [スタート]→[ファイル名を指定して実行] を選択し、「services.msc」と入力して [OK] を押します。
2. [SNMP サービス] を右クリックし、[プロパティ] を選択します。
3. [**トラップ**] タブを選択し、コミュニティストリングを入力します (図 3)。

図 3. Microsoft Hyper-V サーバで、トラップの宛先を設定した例



VMware ESX と Citrix XenServer でトラップ転送先を構成する方法

VMware ESX サーバか Citrix XenServer でトラップ転送先を指定するには、**/etc/snmp/snmpd.conf** ファイルに「**trapsink <detination_IP> <community>**」を追加します。このとき、<destination_IP> には、宛先となる OpenManage Essentials サーバの IP アドレスが、また、<community> には、その SNMP コミュニティストリングがそれぞれ入ります。

Windows または Linux を稼働するリモートサーバを対象に SNMP とトラップ転送先を構成するには、「http://en.community.dell.com/techcenter/extras/m/white_papers/20097170.aspx」(英語サイト) を参照してください。

VMware ESXi でトラップ転送先を設定する方法

VMware ESXi サーバでトラップ転送先を指定するには、次のコマンドを実行します。

```
vicfg-snmp.pl –server <server>–username <user> –password <pass> -t
<destination>@<port>/<community>
```

このとき <destination> には宛先の IP アドレスかホスト名が、また、<port> には通信に使用予定のポートが、さらに、<community> には SNMP コミュニティストリングがそれぞれ入ります。

上記のいずれかのコマンドを実行すると、「Failed : A general system error occurred: Load persistent store failed」というエラーメッセージが出ることがあります。この場合、**/etc/vmware/snmp.xml** ファイルが破損しているか、タグの不備が原因として考えられます。この問題を修正するには、次の手順を実行してください。

1. 次のコマンドを使用して、/etc/vmware/snmp.xml ファイルの名前を snmp.xml.old (または、他の一意の名前) に変更します

   ```
   mv snmp.xml snmp.xml.old
   ```

2. 次のコマンドを使用して、新しい snmp.xml ファイルを作成します。

   ```
   vi /etc/vmware/snmp.xml
   ```

3. その新しい snmp.xml ファイルに次の内容をコピー＆ペーストします。

   ```
   <config>
   <snmpSettings>
   <communities>public</communities>
   <enable>true</enable>
   </snmpSettings>
   </config>
   ```

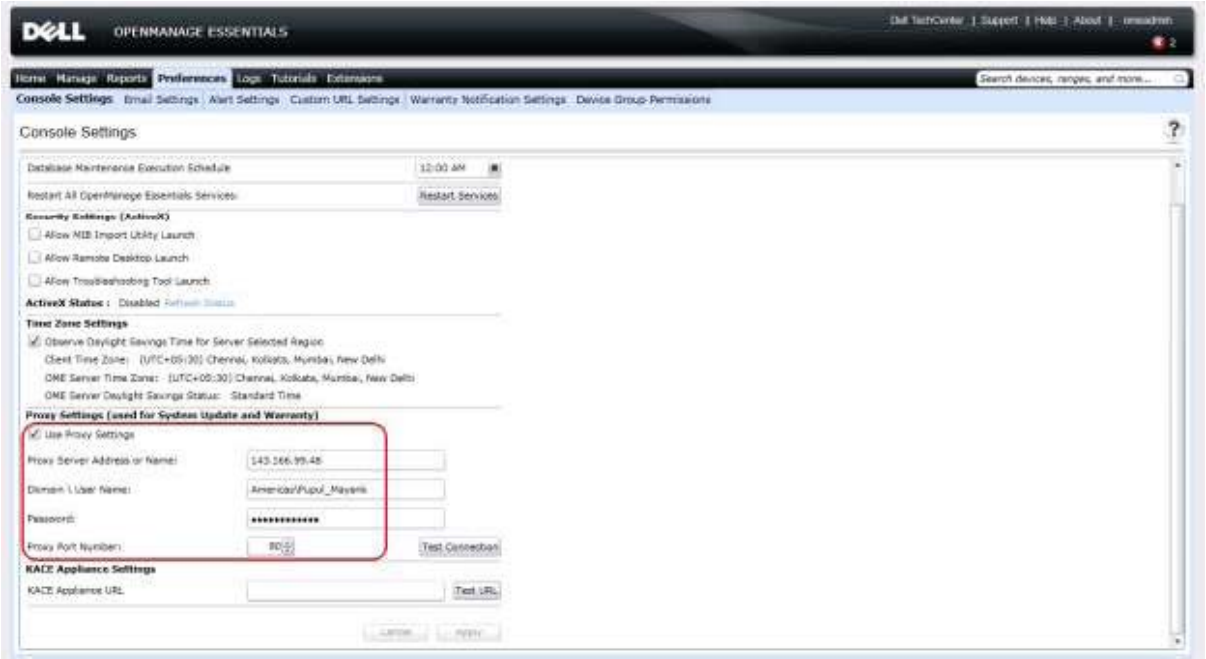
テキストの前後に余計な改行や空白が入らないよう注意してください。このファイルを保存したら、「**./sbin/services.sh restart**」コマンドを使用して VMware サービスを再始動します。

ESXi を OpenManage Essentials 用に構成する詳細な手順は、英語版ホワイトペーパー『How to setup and configure ESXi 5 for use in OpenManage Essentials』(http://en.community.dell.com/techcenter/extras/m/white_papers/20071085.aspx) を参照してください。OpenManage Essentials で管理する ESXi のセットアップ情報は、OpenManage Essentials 内の [チュートリアル] セクションからも参照できます。

仮想化サーバ： システムアップデート

OpenManage Essentials は、すべての仮想化ホストサーバのアップデートに活用できます。アップデートをサポートするのは、VMware ESX および ESXi、Citrix XenServer、Microsoft Hyper-V を稼働するサーバです。実際、これらの全ホストサーバが、たった 1 つのタスクから一括アップデートできます。OpenManage Essentials が単一のタスクでアップデートできる台数は、最大 30 サーバです。Microsoft Hyper-V、Citrix XenServer、VMware ESX を稼働するサーバは、OMSA を使用するか、iDRAC を使用することでアップデートできるため、このどちらかの方法が選択可能です。一方、VMware ESXi のアップデート方法は、iDRAC 経由に限定されます。サーバ上でシステムのアップデートを実行する前に、まず、最新版のカタログをダウンロードしてください。カタログの取得源には、SUU、RM、FTP などがあります。FTP カタログをダウンロードするときは、インターネット接続が必要です。管理サーバをプロキシサーバ経由でインターネットに接続する場合は、図 4 のようにプロキシを設定してください。

図 4. OpenManage Essentials の [プリファランス] ページから設定したプロキシ例



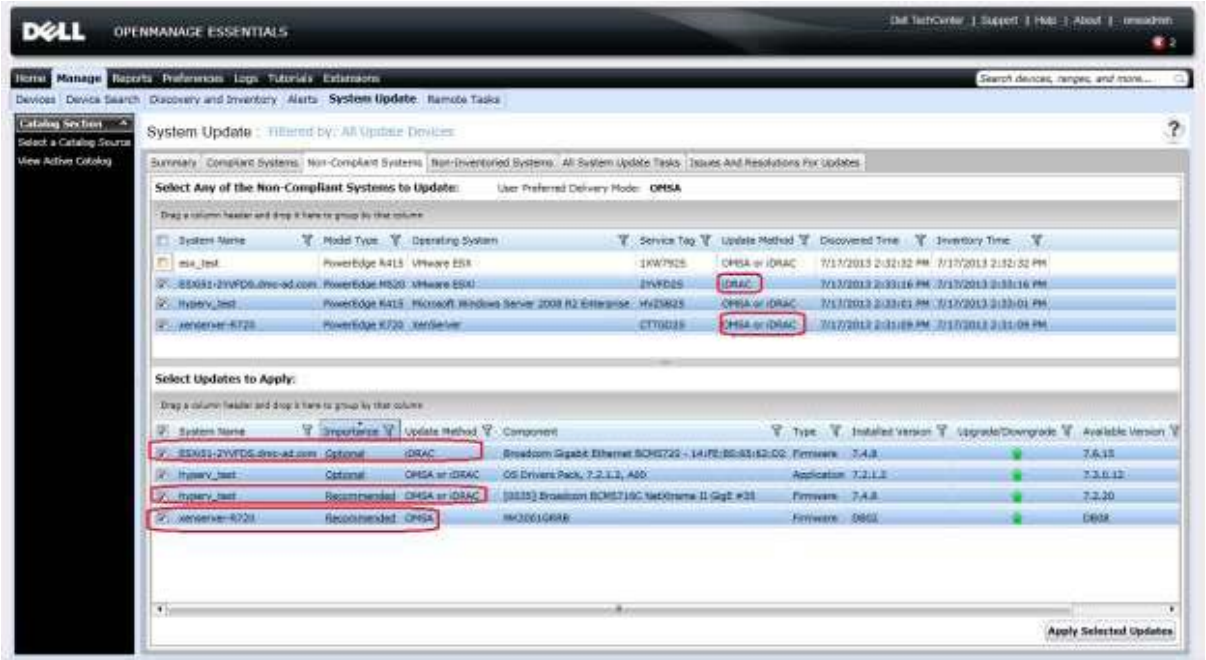
iDRAC 経由のシステムアップデートは、iDRAC6 以降でしかサポートされません。iDRAC を使用してシステムをアップデートするには、まず、WSMAN プロトコルを通してサーバ内の iDRAC を検出およびインベントリする必要があります。サーバの RAC も検出された場合、デバイスツリーの RAC 下にも、同じサーバ名のエントリが重複して現れるはずです。

検出とインベントリが適切に実行され、アップデートの必要なコンポーネントがサーバ内に見つかると、それらが [システムアップデート] タブ内の [非対応システム] にリストアップされます。一方、最新アップデートが適用されているサーバは、[システムアップデート] タブ内の [対応システム] にリストアップされます

システム管理者は、[**システムアップデート**] ページの [**詳細設定**] オプションを選択すると、アップデート方法として、iDRAC か OMSA (OpenManage Server Administrator) のどちらかが選択できます。ここで選択した内容が、デフォルトのシステムアップデート方法として保存されます。仮に、OMSA でしかアップデートできないシステムのデフォルトアップデート方法が iDRAC に設定されていた場合でも、OpenManage Essentials は、OMSA を使用してシステムをアップデートすることができます (逆も同様)。サーバが規定のプロトコル経由で検出され、そのサーバの iDRAC が WSMAN プロトコル経由で検出された場合、図 5 のように、[非対応システム] にはアップデート方法として OMSA か iDRAC が表示され、アップデートの適用時にはデフォルトのシステムアップデート方法が使用されます。図 5 からわかるとおり、VMware ESXi は、iDRAC を使用したアップデート方法しかサポートしません。

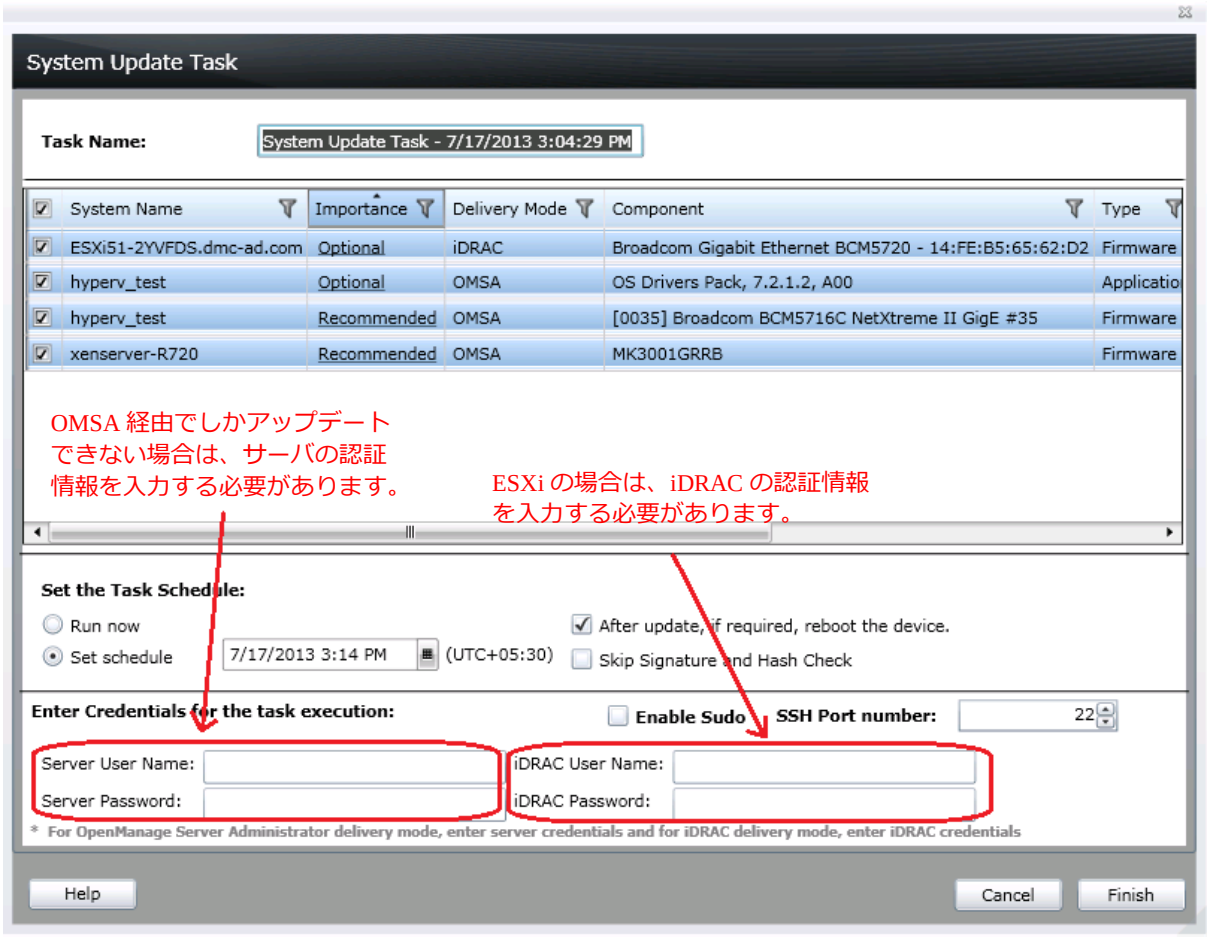
iDRAC からはアップデートできないコンポーネントの場合、そのサーバが検出およびインベントリされていれば、OMSA を通してそれらのコンポーネントをアップデートできます (図 5)。

図 5. 仮想化サーバのアップデート方法



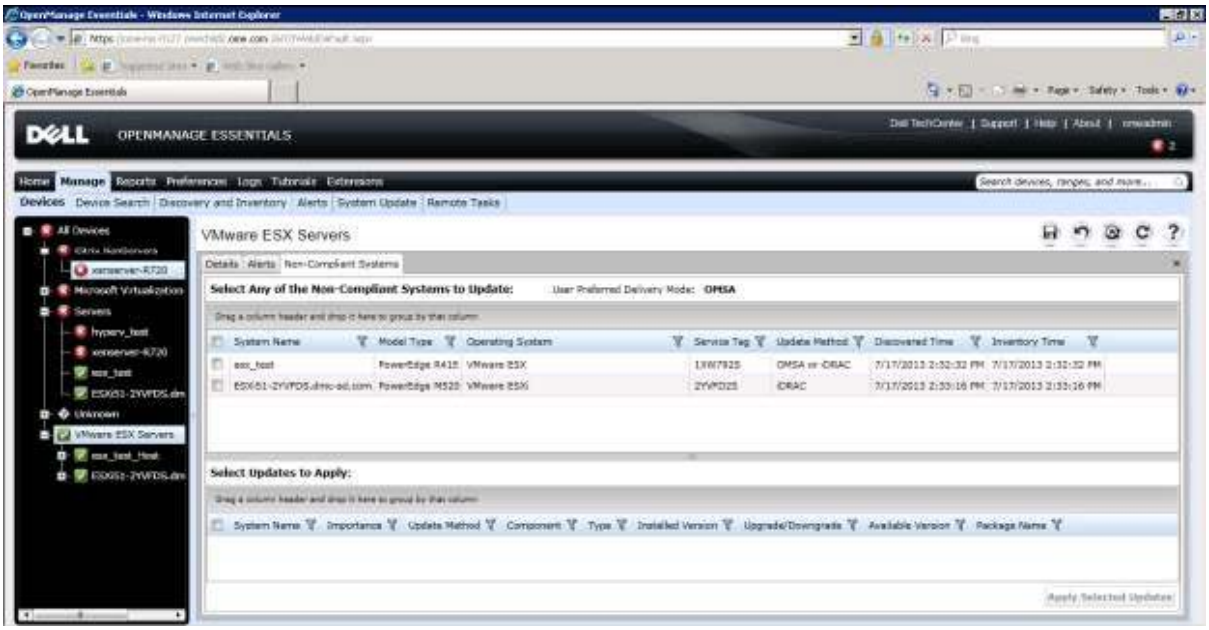
iDRAC 経由でのみアップデートできるシステムは、システムアップデートタスクを作成するときに、iDRAC の認証情報を入力する必要があります。この件は、OMSA 経由のシステムアップデートタスクにも当てはまります。そのため、1 つのタスクに OMSA 経由でのみアップデートできるサーバと、iDRAC 経由でのみアップデートできるサーバが含まれる場合は、両システムの認証情報を入力する必要があります。たとえば、WMI プロトコルから Microsoft Hyper-V サーバが検出およびインベントリされ、WSMAN プロトコルから VMware ESXi とその iDRAC が検出およびインベントリされたとします。次に、システムアップデートタスクを作成し、この両サーバを選択した場合は、Hyper-V サーバの認証情報と、ESXi の iDRAC の認証情報が必要です (図 6)。

図 6. システムアップデートタスクの作成時に入力する認証情報



既にカタログがインポート済みの場合は、ホストサーバをデバイスツリーから最新パッケージに直接アップデートすることも可能です。直接アップデートするには、デバイスツリー内から、目的のサーバが分類されているグループ (例： VMware ESX Servers) を選択します。図 8 の画面例では、右ペイン内の [非対応システム] タブに、上記の手順でアップデートできるシステムが表示されています。

図 7. [デバイス] ページから実行するホストサーバのアップデート



仮想化サーバ： OMSA の導入

OpenManage Essentials を使用すると、VMware ESX や Microsoft Hyper-V を含む仮想化ホストサーバ上に OMSA を導入できます。これらのサポート対象サーバ上には、64 ビット版と 32 ビット版の両 OMSA バージョンが導入可能です。

注： Citrix XenServer と VMware ESX では、OMSA の導入をサポートしていません。

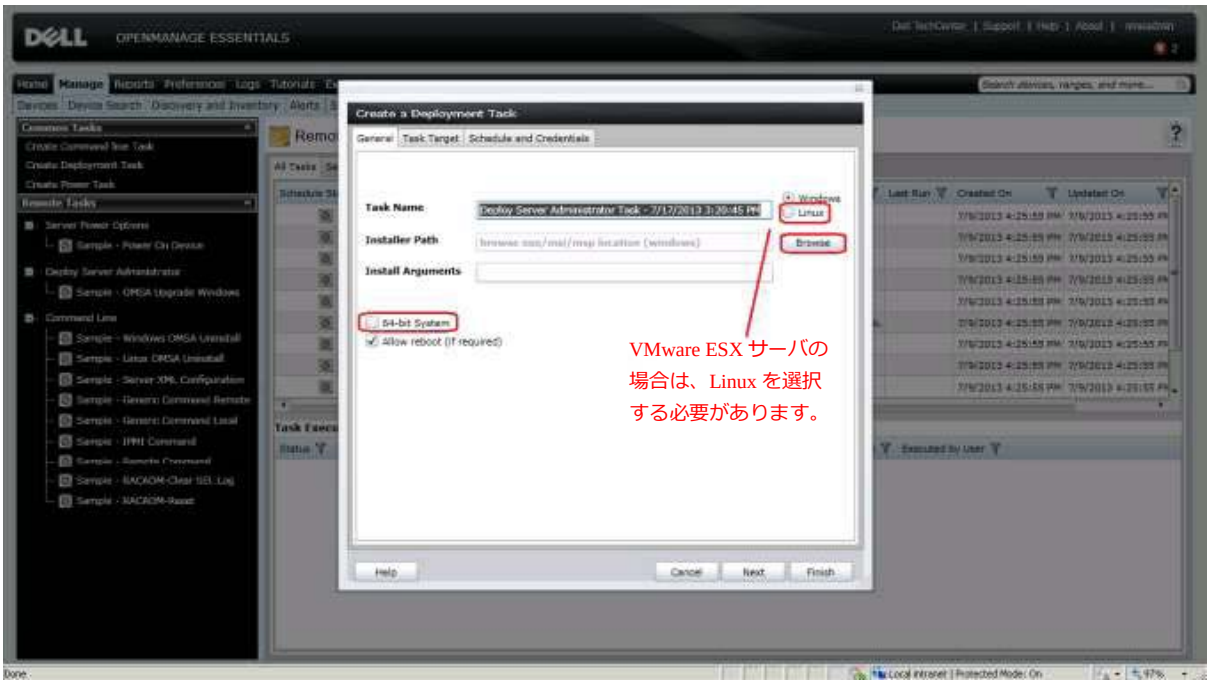
OMSA を導入するには、まず、導入先となるホストサーバを検出してください。既に旧バージョンの OMSA がインストールされているサーバは、デバイスツリー内に正しく分類されるはずです。OpenManage Essentials では、旧バージョンの OMSA を新バージョンにアップデートすることもできます。

OMSA の導入タスクを作成するには、次の手順に従います。

1. [**リモートタスク**] から [**導入タスクの作成**] をクリックします。
2. 図 8 のようなポップアップ画面が現れるので、[参照] ボタンを押して、OMSA パッケージへのパスを指定します。VMware ESX サーバの場合は、「**Linux**」オプションを選択してください。オプションで、インストールの引数を指定することもできます。引数を指定すると、ターゲットサーバに OMSA をインストールするとき、特定のコンポーネントを選択することができます。詳細は、英語版ホワイトペーパー『Deploying OpenManage Server Administrator using OpenManage Essentials』(http://en.community.dell.com/techcenter/extras/m/white_papers/20069180.aspx) を参照してください。
3. [次へ] を押します。OMSA の導入先として、ホストターゲットを指定します。OMSA が既にインストールされている場合は、[**サーバ**] の下に表示され、その他の場合は、[**不明**] の下に表示されます。

4. [**次へ**] を押し、ホストサーバの認証情報を入力します。OMSA 導入タスクを直ちに実行したいときは、[**今すぐ実行**] を選択します。デフォルトでは、現時点から 10 分後にタスクを実行するスケジュールが組まれます。スケジュールを更新することで、後日、指定の日時にタスクを実行することもできます。

図 8. OMSA の導入



まとめ

OpenManage Essentials (OME) は、仮想化環境の管理・監視に活用できます。OME は柔軟なため、1 つのタスクを作成し、そこから仮想化環境全体を一括管理することも、また、ホストサーバごとに個々の管理タスクを作成することもできます。OpenManage Essentials バージョン 1.2 では、デバイスツリー内で、Citrix XenServer が独立したグループとして表示されるようになりました。これにより、XenServer サーバ群をサブグループとして区別できるので、管理が一層容易になります。