IBM Tivoli Endpoint Manager
Version 9.0

Virtual Endpoint Manager User's Guide

IBM

IBM Tivoli Endpoint Manager
Version 9.0

Virtual Endpoint Manager User's Guide

IBM

Contents

Chapter 1. Introduction

Use IBM Endpoint Manager Virtual Endpoint Manager to identify outdated and offline machines in a virtual environment. Virtual machines (VM) are sometimes referred to as Virtual Machine Guests. Virtual Endpoint Manager supports Virtual Machine and Host management.

Key Features

Among the key features of IBM Virtual Endpoint Manager are:

- Identification of virtual machines that have not been turned on for a long time.
- An offline virtual machine workflow where you can schedule a patch window for machines to power on, run any Tivoli Endpoint Manager Actions targeted at the machines, then power down the machines safely.
- Support of virtual machine and host management tasks such as power-on, suspend, reboot, and taking snapshots for virtual machines.
- Exposure of virtual machine guest and host relationships in ESXi through new inspectors and the Virtual Machine Guest Overview dashboard.

Supported platforms

IBM Virtual Endpoint Manager supports the following VMware products and versions:

Table 1. Supported VMware platform versions

VMware Product	Version
ESX	4.0 and 4.1
ESXi	4.0, 4.1, 5.0, and 5.1

Chapter 2. Setup

System Requirements

IBM Virtual Endpoint Manager has the following system requirements:

- IBM Endpoint Manager version 8.2 or higher must be used.
- You must subscribe to the Virtual Endpoint Manager site.
- The management extender must be installed on a system that runs Windows (Windows Vista, Server 2008, Windows 7, and Server 2008 R2). See the section on Configuring the Management Extender for more information.
- The Tivoli Endpoint Manager relay must be installed on the system with the management extender.

Components

Virtual Endpoint Manager has the following components:

Server The Endpoint Manager server is a database that communicates with the relays and the Tivoli Endpoint Manager console to manage the devices in your deployment.

**Relay** Relays are network components that distribute the download burden from the Tivoli Endpoint Manager server and compile and compress data received from clients.

Management Extenders
Management Extenders allow devices to be managed without an agent on the device. Management extenders communicate to the VMware vCenter by translating Endpoint Manager content to VMware commands that are accepted by the VMware vCenter.

Architecture

The following diagram depicts a visual representation of how Virtual Endpoint Manager is designed to work in your environment.
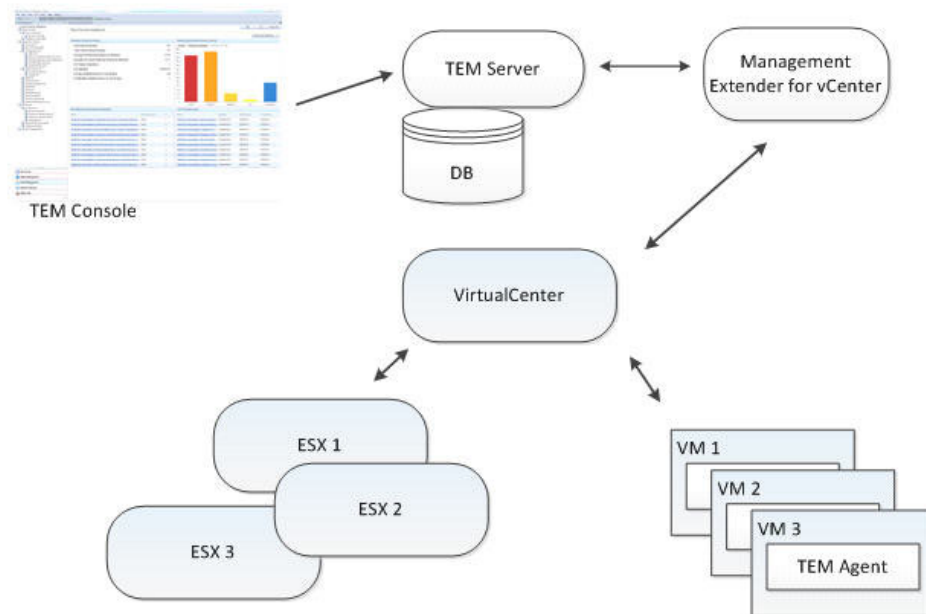
Virtual Endpoint Manager uses the standard Endpoint Manager architecture and a management extender.

A management extender is a Endpoint Manager relay that has the proxy agent installed on it along with the vSphere management extender plug-in installed and configured.

The management extender sends queries to vCenter about the virtual machines and hosts that it controls, and reports information back to the Endpoint Manager server. These reports end up as separate computer objects in the Endpoint Manager Console. Because no actual Endpoint Manager agent is installed on these computers, they are known as proxied machines. From the console, you can send commands such as power-on, power off, suspend, or take snapshots. The management extender passes the commands by communicating with vSphere through the VMware application programming interface (API).

The properties of host and virtual machine guests can be discovered with the use of the VMware API. These properties include the IP address, available memory, the BIOS versions, and number of snapshots. See the list of new properties in Appendix C, "List of actionscript commands," on page 29.

When the Endpoint Manager Console issues a command, it gets passed down to the management extender, which translates this action script into VMware API commands. These APIs report back success or failure, and the management extender interprets these results and pass them back up to the Endpoint Manager relay. The relay passes them back up to the Endpoint Manager Server. The status of the commands are reported back to the Endpoint Manager Console.

Configuring the Management Extender

Before you can configure the management extender, you must do the following steps:

1. Install the Endpoint Manager relay (version 8.2 or later). For more information about relays, see the IBM Endpoint Manager Operators Guide.

2. Deploy Fixlet 801: Deploy Management Extender for VMware vCenter from the Patches for ESXi site. This action appears as applicable when the TEM relay is installed.

3. Activate analysis 905: Management Extender Status.
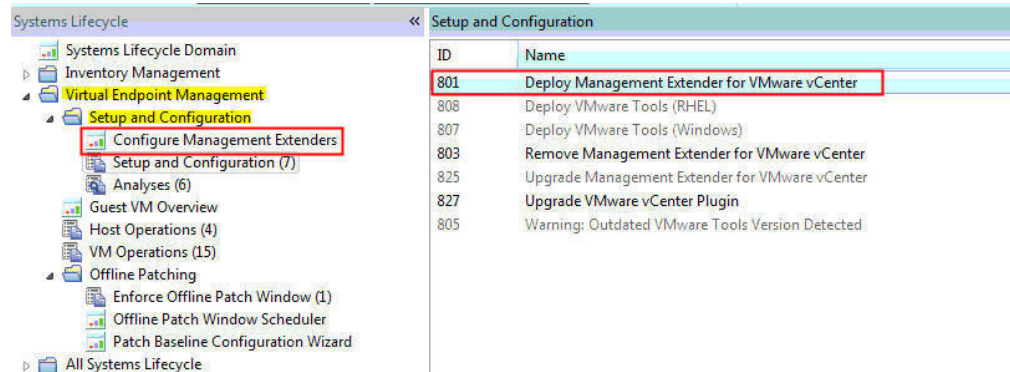
Note: The management extender uses the following ports by default: 8080 and 8443.

Using the Configure Management Extenders dashboard

To use the dashboard, navigate to **Systems Lifecycle Domain** > **Virtual Endpoint Manager** > **Setup and Configuration** > **Configure Management Extenders**. The Configure Management Extenders dashboard lists all the endpoints where you ran the Deploy Management Extender for VMware vCenter task. Select the management extender that you want to configure. Click **Configure**.

The **Configure Extender** window opens. Fill in the values for the following items in the window:

- Refresh interval minutes

  Set how often the management extender gathers data. A larger refresh cycle is highly suggested. The larger the VMware deployment is, the longer it takes to gather data.

- Server name
- Admin User
- Password

Note: By default, the windows prompts for the server name only. If you choose to do that, the URL that connected is `https://(SERVER NAME)/sdk/webService.` When the URL is not correct, you can enter your own URL by selecting the **Enter vCenter's wev service URL**.

The username and password are encrypted using the private key and public key. These keys are set during the deployment of the vCenter management extender. The public key is based on the computer name. The private key is generated during the deployment task. The username and password are then sent to the management extender, which uses the credentials to plug in to the VMware vCenter. The credentials are sent to the endpoint in an encrypted format.

You can view these credentials in the plugin-settings.ini file which is found by default in `C:\program files\bigfix enterprises\management extenders\plugin\ VMware ESXi 1\plugin.`

Note: The plugin-settings.ini file is stored in plain text.

You can configure the management extender again without removing the deployment and configuring it twice.

Chapter 3. Offline Patching Workflow

IBM Virtual Endpoint Manager follows this workflow to send patches to offline virtual machines:

1. Create offline patch windows using the Offline Patch Scheduler dashboard.
2. Enforce the Offline Patch Window task.

Note: To apply patches, the virtual machines must have an Endpoint Manager agent.

Creating offline patch windows

You can create a patch window to apply patches for outdated and offline virtual machines with the use of the Offline Patch Window Scheduler dashboard. From the dashboard, you can set the time and date when the patch window starts and ends.

When you select the **Switch VLAN** check box, you can switch to a pre-configured and quarantined VLAN from the dropdown menu.

Virtual machines that get turned on for the first time in a long while can have many unpatched vulnerabilities that leave them vulnerable to the outside world. Normally, when offline windows are set, the virtual machines that get turned on can be attacked by the outside world.
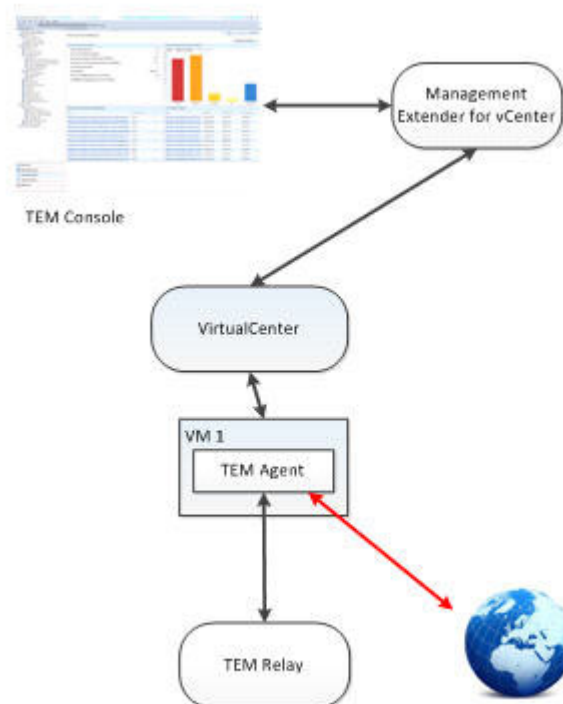
A separate VLAN can be setup and used in conjunction with the offline patch window dashboard. In this setup, the offline virtual machines are switched from a

normal network to a VLAN where they can only communicate to a pre-configured Tivoli Endpoint Manager relay. In this setup, the relay can communicate to all of the clients and to the world, but the individual clients cannot communicate with the world.

The machines patch in a safe environment and at the end of a patch window, they return to their initial VLAN. To use this mode, the user needs to setup this separate network. If a VLAN is set but a targeted virtual machine does not have this VLAN configured to be one of it's network adapters, the VLAN isn't switched for that particular endpoint.
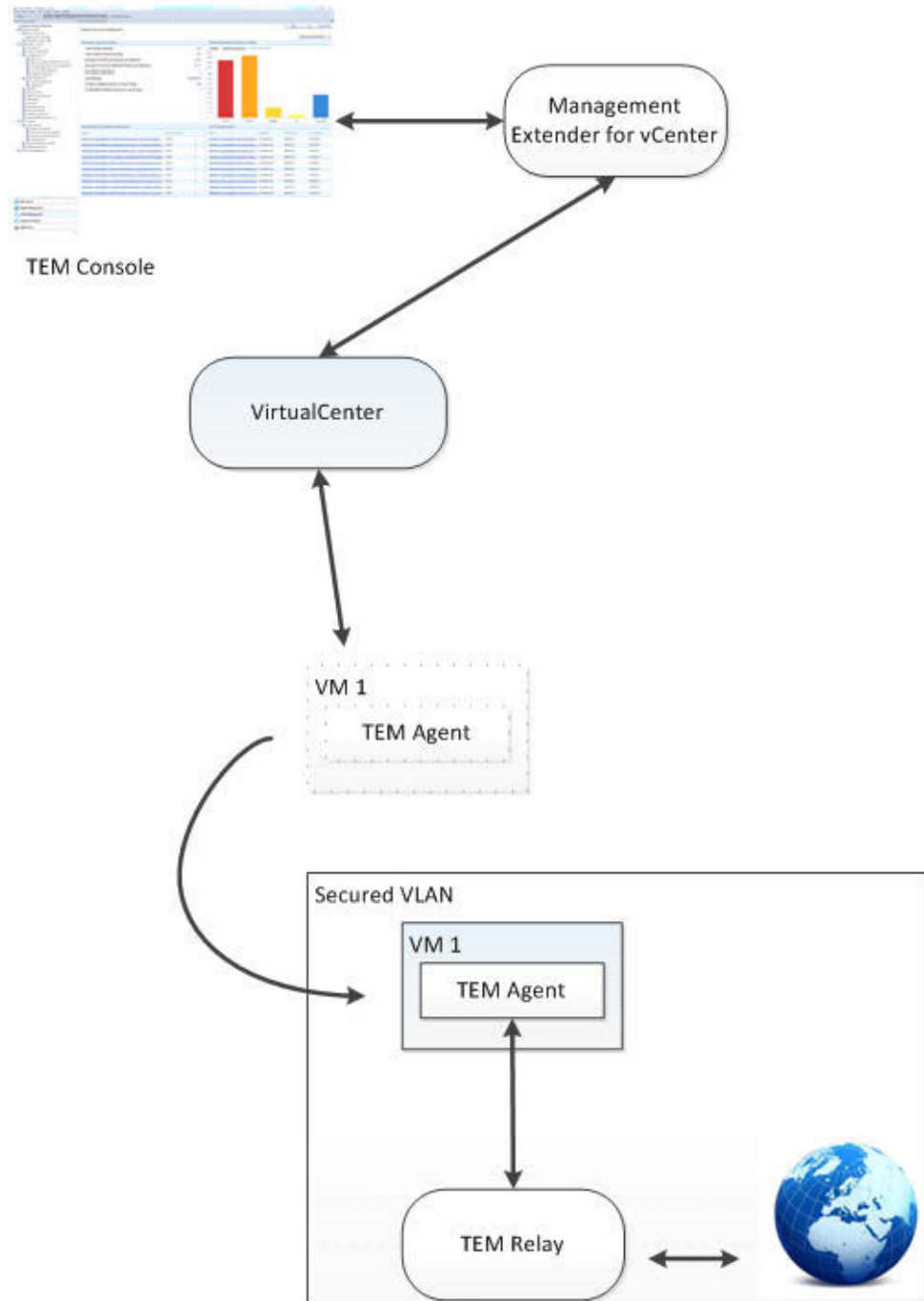
Note: You must have a VLAN configured on an adapter that lets through traffic only from port 52311.

Note: You must have quarantine VLAN setup with a Tivoli Endpoint Manager relay already installed.

You can manage the number of virtual machines that are patched in one batch when you enter a value in the **Concurrent Operations** dropdown menu. This function turns on only a maximum number of virtual machines at a time per host. The window turns off the machines when it gets through the patch baseline and turns on the next batch of virtual machines.

This function can help avoid having all the virtual machines turned on simultaneously, if, for example, you have a patch that targets several thousands of virtual machines.

The following image is an example of 5 virtual machines targeted with a concurrency value of 2 and a patch window time of 30 minutes.

Patch Window from 6PM – 7PM

Targeted: 5 VMs
Concurrent VMs: 2
Enforce Patch Window Time: 30 minutes

Window Start		Window Stop

VM #1   VM #1
VM #2
VM #3
VM #4
VM #5

6:00PM   6:30PM   7:00PM   7:30PM
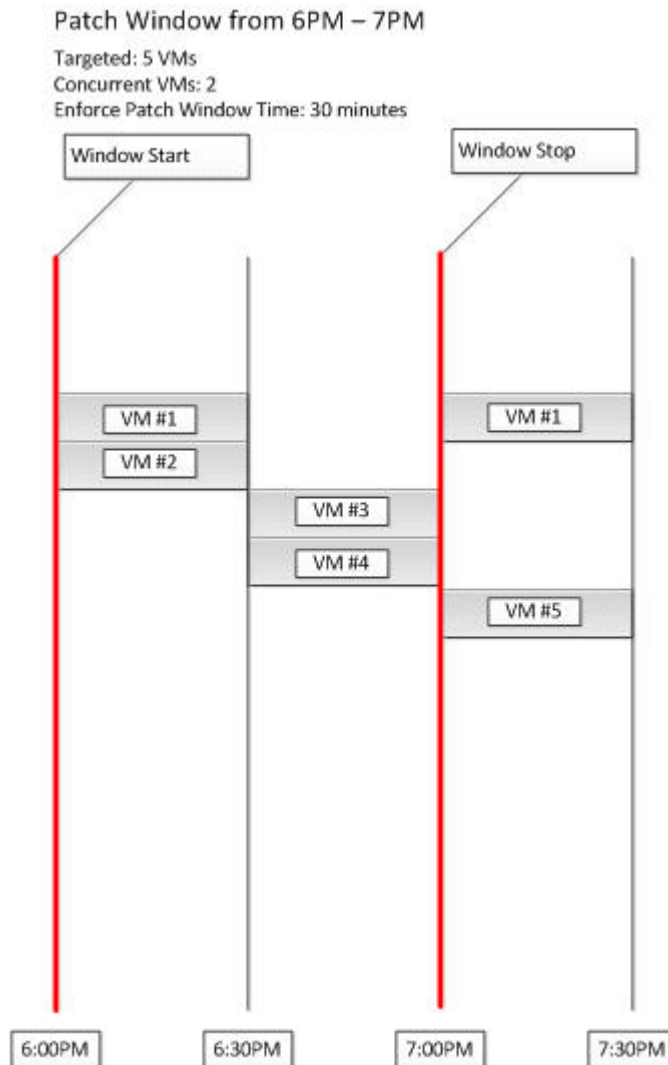
In this example shown in the image, at the beginning of the window, VM#1 and VM#2 starts up. After 30 minutes of being on, VM#1 and VM#2 turns off and #3 and #4 starts. After #3 and #4 turn off, if it's still before 7:00 p.m., VM#5 and VM#1 will start back on again. After 7:00 p.m., no new machines are turned on through this patch window, so when VM#1 and VM #5 turn off at the end of the 30 minute patch window, they won't turn on again.
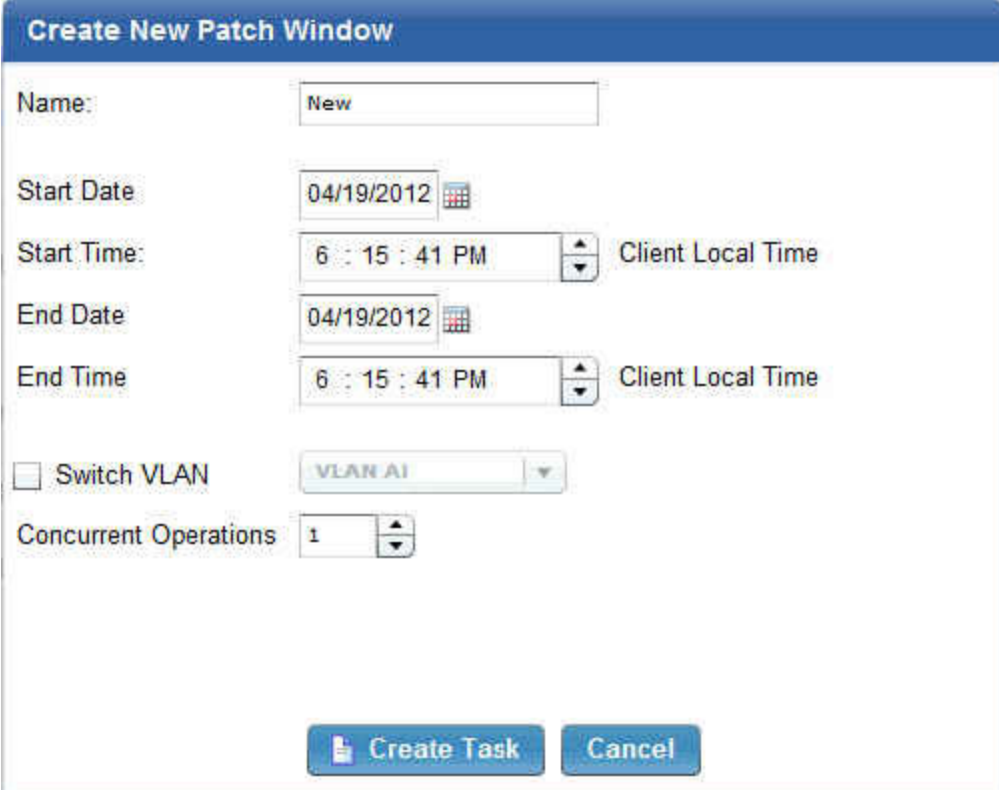
Both the Switch VLAN and Concurrent Operations functions are optional.

Using the Offline Patch Window Scheduler dashboard

To create a patch window using the Offline Patch Window Scheduler dashboard, select **System Lifecyle** from the console. From the navigation tree, select **Virtual Endpoint Management** > **Offline Patching** > **Offline Patch Window Scheduler.**

The dashboard opens. Click *Create New Patch Window*. Enter information for the following fields:
- Name
- Start Date
- Start Time
- End Date
- End Time

You have the option to click *Switch VLAN*. Select the VLAN from the dropdown menu. You can also select the number of concurrent operations that will be executed.

Note: Setting *Switch VLAN* and *Concurrent Operations* are optional steps.
Click *Create Task*. At the end of the patch window, the plug-in suspends or powers

off any remaining virtual machines depending on the initial conditions of the virtual machines.

Enforcing the Offline Patch Window task

After the patch window schedule has been set, the second part of the offline patching workflow involves enforcing the Offline Patch Window task. To do this, from the console, navigate to the **Systems Lifecycle Domain**. From the navigation tree, navigate to **Virtual Endpoint Management** > **Offline Patching** > **Enforce Offline Patch Window.**

The Offline Patch Window task executes the schedule of the power down of a machine, based on what value is set. The client checks if the Tivoli Endpoint Manager actions are running. The client waits until all the actions are complete before the machine turns off. When the proxy agent sees the machine is off, the proxy agent will move to the next machine on the list.
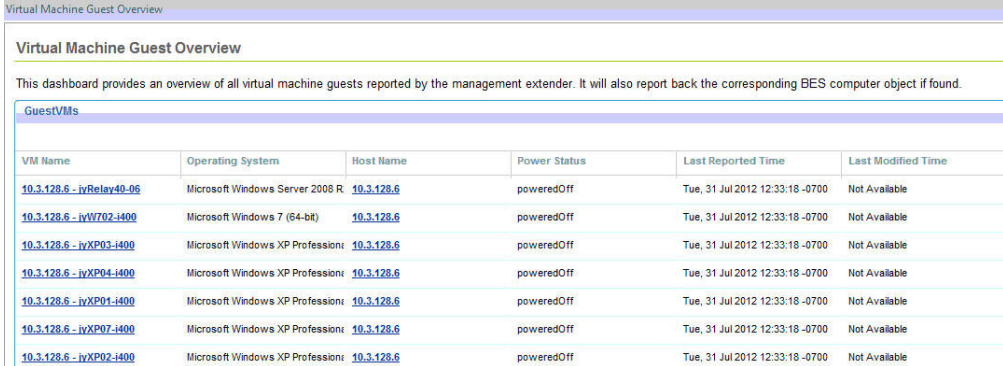
Note: The targets of the Offline Patch Window task are the proxied machines that were part of the patch windows when the Offline Patch Window Scheduler dashboard is discussed in the "Creating offline patch windows" on page 7 section.

Chapter 4. Virtual Machine Guest Overview

The Virtual Machine Guest Overview dashboard lists the virtual machine objects reported by the management extender through the VMware API. The dashboard correlates the virtual machine object with the Endpoint Manager object. From the list, you can view which machines have the Endpoint Manager agents deployed in it.

Note: Before you use the Virtual Machine Guest Overview dashboard, you must activate the following analyses: Virtual Guest Information, Virtual Machine Guest Information - Virtual Machines with Tivoli Endpoint Manager Client, and Virtual Machine Host Information.

Select the **All Systems domain** in the console. From the navigation tree, click **Virtual Endpoint Management** > **Setup and Configuration** > **Guest VM Overview**.

Virtual Machine Guest Overview

Virtual Machine Guest Overview

This dashboard provides an overview of all virtual machine guests reported by the management extender. It will also report back the corresponding BES computer object if found.

GuestVMs

VM Name	Operating System	Host Name	Power Status	Last Reported Time	Last Modified Time
10.3.128.6 - jyRelay40-06	Microsoft Windows Server 2008 R	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyW702-i400	Microsoft Windows 7 (64-bit)	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyXP03-i400	Microsoft Windows XP Profession:	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyXP04-i400	Microsoft Windows XP Profession:	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyXP01-i400	Microsoft Windows XP Profession:	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyXP07-i400	Microsoft Windows XP Profession:	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available
10.3.128.6 - jyXP02-i400	Microsoft Windows XP Profession:	10.3.128.6	poweredOff	Tue, 31 Jul 2012 12:33:18 -0700	Not Available

Chapter 5. Specifying virtual device computers

You must create a custom site or have an existing external site in the IBM Endpoint Manager console that you want to use.

You can use the Computer Subscriptions feature in Sites to limit the computer subscriptions to ESXi Hypervisors or ESXi Hypervisor Virtual Machines only. For more information on Sites, and how to create a Custom Site, see the IBM Endpoint Manager Information Center:

* http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/index.jsp?topic=
  %2Fcom.ibm.tem.doc_9.0%2FPlatform%2FConsole
  %2Fc_creating_custom_sites.html
* http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/index.jsp?topic=
  %2Fcom.ibm.tem.doc_9.0%2FPlatform%2FConsole%2Fc_restricting_readers.html

1. In the IBM Endpoint Manager console, navigate to **All Contents** domain and select **Sites**.
2. Select the Site of which you want to manage the computer representations and in the **Site** window, select the **Computer Subscriptions** tab.
3. In the **The following computers will be subscribed to:** area, select "Computers which match the condition below".
4. From the lists, select **Relevance Expression is true** and click **Edit Relevance**.
5. Add the following relevance to filter the computer representations: `in proxy agent context` and click **OK**.
6. Click the + button if you want to add more relevance expressions.
7. Add the following relevance to filter the computer representations: `((data type = "ESXi Hypervisor") or (data type = "ESXi Hypervisor Virtual Machine"))`
8. Click **OK**.

You can now see your filtered list of computer representations in the **Subscribed Computers** section of your custom site.

Chapter 6. Working with multiple computer representations

You can use the IBM Endpoint Manager console to perform do a number of different actions on virtualized computers.

For example:

- While working within the Endpoint Manager console, some Operators manage virtual infrastructure, including managing virtualized computer processes such as creating, modifying, and powering on/off virtual machines.
- Other operators work directly with operating systems that are running on virtual machines, including performing actions on the operating system such as patching and software installation.

As a result, the Computers view within the Endpoint Manager console displays multiple views of the same virtualized computer.

You can manage multiple computer representations by creating custom filters or by using Roles and Operators.

Selecting device types

In the **All Content** domain, go to **Computers** and in theComputers window, right-click on any column to open the **Column Picker**. In the **Column Picker** menu, select **Device Type**.
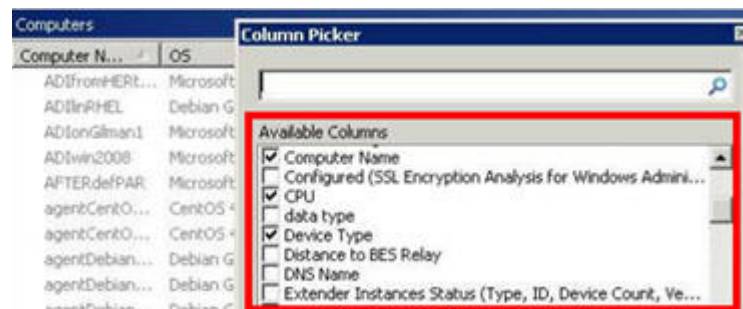
Understanding computer representations in IBM Endpoint Manager

In the following image, the computers RHEL63-1 and rhel63-1 are two representations of the same computer.

- Computer rhel63-1 with the icon is the Operating System representation (used for performing actions on the operating system such as patching, software install). The Device type is either Laptop or Server.
- Computer RHEL63-1 is the virtual infrastructure representation (used for managing virtualized computer processes such as creating, modifying, powering on/off virtual machines). The Device type is either ESXi Hypervisor or ESX Hypervisor virtual machine.

Managing computer representations in IBM Endpoint Manager

To ensure that the endpoint management administrators only work with the computer representations that they manage, you can create custom filters or assign Device Type-specific Roles to each Operator. Their Computer view then contains only the computer representations that they must manage.

Creating a custom filter

Use the custom filter to manage the virtualized computer representations that are displayed in the Computer view. Repeat this process to create filters for each representation that you want to view.

1. In the IBM Endpoint Manager console, navigate to the **All Content** domain.
2. Right-click on **Custom Filter** and select **Create Custom Filter**.
3. In the **Create Filter** dialog box, enter a name for your new filter in the Name field. For this example, use the name "ESXi Hypervisors".
4. In **Visibility**, select **Available to all operators**.
5. In the **Include** list, select **Computers**.
6. In the **with** list select **all of the following properties**.
7. From the first properties list, select **Device type**.
8. Select **contains** and enter ESXi Hypervisors.
9. Select the **+** symbol to add another filter.
10. From the properties list select **Device type**, then select **does not contain** and enter Virtual Machines.
11. Click Create to create your new custom filter.

To use your custom filter, navigate to **Custom Filter** in the **All Contents** domain and select **ESXi Hypervisors**. In the **Custom Filter: ESXi Hypervisors**, the custom filter displays computers with the Device Type of ESXi Hypervisor only.

Using Roles and Operators to manage computer representations

You can also use Roles and Operators to manage computer representations in IBM Endpoint Manager.

Here is an example of a procedure that demonstrates how Roles can be assigned to different Operators. The vCenter administrator Role has the ability to provision virtual infrastructure. The vCenter user Role has the ability to power on/power off, take snapshots etc, and the General role can, for example, patch and update the operating systems of computers.

Creating a VMware vCenter Admin Operator

1. 1.Open the **All Content** domain.
2. In the **All Content** domain, navigate to **Roles**.
3. In the **Roles** window, right-click and select **Create Role**.
4. In the **Create Role...** window, enter a name for your new role. For example VcenterAdmin
5. Select the **Computer Assignments** tab in the **Role:** window and click **Add**.
6. Navigate to **All Computers** > **By Retrieved Properties** > **By Device Type**.
7. Select all types that begin with ESXi and click **OK**.
8. In the **All Content** domain, select **Operators**.

9. In the **Operators** window, right-click and select **Create Local Operator**.
10. In the **Create Local Operator** window, enter a name and password for the new Operator and click **OK**.
11. In the **Console Operator:** window, select the **Assigned Roles** tab and click **Assign Role**.
12. In the **Assign Role to User** window, select the role which you just created and click **OK**.
13. In the **Console Operator:** window, click **Save Changes**.
14. Exit the IBM Endpoint Manager console and log in as the new Operator.

You can view and work with all virtual ESXi virtual machines and hypervisors.

Creating an operator for vCenter users

1. Open the **All Content** domain.
2. In the **All Content** domain, go to **Roles**.In the Roles window, right-click and select **Create Role...**.
3. In the **Create Role** window, enter a name for your new Role. For example: vCenterUser.
4. Select the **Computer Assignments** tab in the Role: window and click **Add**.
5. Navigate to **All Computers** > **By Retrieved Properties** > **By Device Type**. Select **ESXi Hypervisor Virtual Machine** and click **OK**.
6. In the **Create Role** window, click **Save Changes**.
7. In the **All Content** domain, select **Operators**.
8. In the Operators window, right-click and select **Create Local Operator**.
9. In the **Create Local Operator** window, enter a name and password for the new operator. For example vCenterUser.
10. In the **Console Operator:** window, select the **Assigned Roles** tab and click **Assign Role**.
11. In the **Assign Role to User** window, select the Role which you just created and click **OK**.
12. In the **Console Operator:** window, click **Save Changes**.
13. Exit the IBM Endpoint Manager console and log in as the new Operator.

You can view and work with ESXi Hypervisor Virtual Machines only.

Creating a general operator

1. In the IBM Endpoint Manager console, open the **All Content** domain.
2. In the **All Content** domain, go to **Roles**.
3. In the Roles window, right-click and select **Create Role...**.
4. In the **Create Role** window, enter a name for your new role. For example, GeneralUser.
5. Select the **Computer Assignments** tab in the "Role:" window and click **Add**.
6. Go to **All Computers** > **By Retrieved Properties** > **By Device Type**. Select all non-virtual computers (Laptops, Servers, and others) and click **OK**.
7. In the **All Content**, select **Operators**.
8. In the Operators window, right-click and select **Create Local Operator**.
9. In the "Create Local Operator" window, enter a name and password for the new Operator.

10. In the **Console Operator:** window, select the **Assigned Roles** tab and click **Assign Role**.
11. In the "Assign Role to User" window, select the role that you created and click **OK**.
12. In the Console Operator: window, click **Save Changes**.
13. Exit the IBM Endpoint Manager console and log in as the new Operator.

In the Computers view in the **All Content** domain, you cannot view any ESXi Virtual Machine or Hypervisors, only computers. You can now take action on any computer with the IBM Endpoint Manager Agent installed.

Chapter 7. Troubleshooting

See the following files to help you during troubleshooting.

Settings file location

- The value of the refresh interval of the machine reports is set in the Configure Management Extenders dashboard. To view where this value is stored, go to: `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\VMware ESXi\settings.json` The default value is set at 15. The suggested value for the refresh interval must be at least be 5. Larger requirements may require a bigger value. The maximum value is 100.
- To view the credentials to logon to VMware vCenter, go to: `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\VMware ESXi\plugin\plugin-settings.ini`.

Note: The `plugin-settings.ini` file is in plain text.

Log files location

- To view the proxy agent log, go to `C:\Program Files\BigFix Enterprise\Management Extender\__Logs\ProxyAgent.log`.
- To view the management extender plug-in log, go to `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\Vmware ESXi 1\Logs`.

Inspectors file format

Inspectors are designed to interrogate the software, firmware, and hardware of each of the client computers on the network using relevance. The inspectors that Virtual Endpoint Manager uses are defined in the `ESX.inpectors` file. These inspectors can be plugged in to the relevance and get information back to the servers.

To see the `ESX.inpectors` file, go to `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\Vmware ESXi 1\Inspectors\ESX.inspectors`.

Note: The paths indicated in this section are for 32-bit operating systems. In a 32-bit operating system, the path is `C:\Program Files\BigFix Enterprise`. In a 64-bit operating system, the path is `C:\Program Files (x86)\BigFix Enterprise`.

Appendix A. Support

For more information about this product, see the following resources:

- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Appendix B. Frequently asked questions

Why are some things not showing up on my console?

Check to make sure that your management configure is configured properly and has the correct credentials to your vCenter machine. By default, the location of this file is at: `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\VMware ESXi 1\plugin\plugin-settings.ini`. For 64-bit systems, it is found in `C:\Program Files (x86)\BigFix Enterprise\Management Extender\Plugins\VMware ESXi 1\plugin\plugin-settings.ini`).

I've set up an offline patch window but I'm seeing unusual behavior. What might be wrong?

Check to see that a TEM agent is installed on each of the machines targeted by the offline patch window. Check to see if you have multiple actions in the action history of the 'Enforce Offline Patch Window task' affecting the same endpoints.

What should I configure to have a running offline window?

Check that you have the following items setup:
- The TEM agent is installed on each of the machines targeted by the offline patch window.
- A patch window is set through the offline patch window dashboard.
- The Enforce Offline Patch window task is set as a policy action.

My virtual machines are no longer powering on during a patch window. What happened?

Check to see if you are at the maximum number of concurrent running machines. That setting can be found by default in this directory: `C:\Program Files\BigFix Enterprise\Management Extender\Plugins\VMware ESXi 1\Patch Windows\(name of patch window)\(host - operations.txt)`. For 64-bit systems, it is found in `C:\Program Files (x86)\BigFix Enterprise\Management Extender\Plugins\VMware ESXi 1\Patch Windows\(name of patch window)\(host - operations.txt)`. The number inside represents the number of concurrently running virtual machines per host. If the number is at the limit that was initially set, consider setting a higher concurrent virtual machine number.

Can I have more than one offline window at a time targeted at the same endpoint?

Yes, you can have more than one offline window at a time targeted at the same endpoint.

Does the offline patch window scheduler workflow work for more than just patch content?

Yes, it does. You can run any TEM action from any site via this offline workflow.

Why can't I apply any ESXi patches?

The Patches for ESXi content is audit only. In order to remediate ESXi issues, use the VMware Update Manager or download and apply patches manually from the VMware website.

Why is it that I cannot install an agent on ESXi?

This is a restriction that VMware introduced in their ESXi hypervisors.

Can I install the management extender on a non windows machine?

Currently, the proxy agent can only be installed on Windows-based machines.

Can I run the IBM Endpoint Manager for Mobile Management Extender alongside the vCenter Management Extender?

Yes, you can run both management extenders.

What is the difference between proxied machines and normal machines on the TEM Console?I

Normal machines have a full TEM agent installed on them, with the full standard set of inspectors and actions. Instead of a full TEM agent, proxied machines use APIs to pull back information about devices and feed that information into the console as a computer report. Proxied machines have a more limited set of inspectors and actions.

Will having proxied machines affect my machine count?

Yes. Proxied machines will also count as normal machines on licensing. Talk with your sales representative to figure out how to adjust the license agreement to accommodate your virtual infrastructure.

Why are some fields different between what a proxied VM reports and what the TEM agent reports?

The vCenter plug-in grabs data directly from the VMware APIs and then translates them into TEM properties. However, because a lot of these fields are set by the user, sometimes they can mismatch what gets reported in the TEM Agent. For example, it is possible to set the Guest Operating System version to be something very different from what is actually installed on virtual machine.

What kind of best practices or highly suggested settings do you have for this management extender?

The device refresh interval should be at least 5 minutes. On a medium to large size deployment, this refresh interval time should be set to 15 minutes or beyond. The Enforce Management Extender policy action should be set to however long it takes to run a substantial amount of TEM actions before it is forced to power down. The maximum time limit that can be set is an hour long.

What kind of machine should the Management Extender be?

For medium to larger size deployments, the main limiting factor is most likely going to be the CPU. As long as it is something running quad cores, the machine should be able to handle all of the management extender tasks.

If I revert a snapshot, can I expect a different computer report on the console?

No, it will be the same computer report on the TEM Console.

Appendix C. List of actionscript commands

These are the new actionscript commands:

- Power on
- Power off soft
- Power off hard
- Create snapshot (takes in a parameter for the snapshot name to be created)
- Revert snapshot (takes in a parameter for the snapshot name to be reverted)
- Go to snapshot (takes in a parameter for the snapshot name to go to)
- Rename snapshot (takes in a parameter for the target snapshot to rename and the new snapshot name)
- Remove snapshot (takes in a parameter for the snapshot name to remove)
- Remove all snapshots
- Suspend hard
- Suspend soft
- Reset
- Restart
- Shutdown host
- Enter maintenance mode
- Exit maintenance mode
- Reboot host
- Change VLAN (takes in a parameter for the VLAN to be changed)

Notices

This information was developed for products and services offered in the U.S.A.

IBM® may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the "Web at Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

IBM ®

Printed in USA