

**BigFix Patch
Virtual Endpoint Manager - User's Guide**



Special notice

Before using this information and the product it supports, read the information in [Notices \(on page xxxv\)](#).

Edition notice

This edition applies to BigFix version 10 and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

| | |
|----------------------------------------------------------------------------|-----------|
| Special notice..... | ii |
| Edition notice..... | iii |
| Chapter 1. Overview..... | 6 |
| Key Features..... | 6 |
| Supported platforms..... | 6 |
| Chapter 2. Setup for management extender..... | 7 |
| Site subscription..... | 7 |
| System Requirements..... | 7 |
| Components..... | 7 |
| Architecture..... | 8 |
| Managing the workload balance..... | 9 |
| Configuring the management extender..... | 10 |
| Working with multiple computer representations..... | 12 |
| Creating a custom filter..... | 13 |
| Using Roles and Operators to manage computer representations..... | 14 |
| Chapter 3. Setup for VMware plugin..... | 16 |
| Site subscription..... | 16 |
| Supported platforms..... | 16 |
| System Requirements..... | 16 |
| Components..... | 17 |
| Architecture..... | 17 |
| Managing the workload balance..... | 19 |
| Configuring the VMware plugin..... | 19 |
| Chapter 4. Migration from management extender to VMware plugin..... | 21 |
| Chapter 5. Offline Patching Workflow..... | 22 |
| Creating offline patch windows..... | 22 |
| Enforcing the Offline Patch Window task..... | 27 |
| Supersedence..... | 27 |
| Chapter 6. Virtual Machine Guest Overview..... | 28 |
| Chapter 7. Specifying virtual device computers..... | 29 |
| Chapter 8. Troubleshooting..... | 30 |

| | |
|-------------------------------------------------------|-----------|
| Appendix A. Support..... | 31 |
| Appendix B. Frequently asked questions..... | 32 |
| Appendix C. List of actionscript commands..... | 34 |
| Notices..... | XXXV |

Chapter 1. Overview

Use BigFix Virtual Endpoint Manager to identify outdated and offline machines in a virtual environment.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 BigFix 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 BigFix 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

BigFix Virtual Endpoint Manager supports the following VMware product versions:

- ESXi 7.0
- ESXi 7.0.0
- ESXi 7.0.1
- ESXi 8.0



Note:

- ESXi 6.0 was deprecated. ESXi 6.5 and ESXi 6.7 have reached its End of Life on October 15, 2022. BigFix no longer provides content or support for ESXi 6.0, ESXi 6.5, and ESXi 6.7 after the deprecation date. For more information, see <https://core.vmware.com/blog/reminder-vsphere-6567-end-general-support> and <https://kb.vmware.com/s/article/89305>.
- BigFix supersedes a bulletin Fixlet if a newer version of the vSphere Installation Bundle (VIB) that is associated with that bulletin is available. Sometimes this can happen in the same VMware patch update.

Chapter 2. Setup for management extender

This section or menu option provides instructions for installing and configuring the management extender, including the necessary prerequisite steps.



Note: The BigFix team is actively working to expand the scope of utilizing the new Plugin across a broader range of BigFix platform versions. Once this expansion is achieved, the existing VMWare VCenter Management Extender will be deprecated. For the new setup details regarding the new VMware Plugin, please refer to the [Setup for VMware plugin \(on page 16\)](#).

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by HCL, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the [BigFix Installation Guide](#).

For more information about sites, see the [BigFix Console Operator's Guide](#).

System Requirements

Ensure that you meet the necessary system requirements for the BigFix Patch for Virtual Endpoint Manager.

The requirements are as follows:

- BigFix Version 9.5.x, 10.0.x, or 11.0.x must be used.
- You must subscribe to the Patches for ESXi site.
- The management extender must be installed on a system that runs Windows (Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows 10, Server 2016, Server 2019, and Server 2022).
- The BigFix relay must be installed on the system with the management extender.
- The vCenter user must have an Administrator role to configure the management extender. Having the Administrator role enables users to retrieve host patch status and to avoid relevance issues.

Components

VMware Plugin components are individual building blocks that collectively form the plugin's functionality.

Virtual Endpoint Manager has the following components:

Server

The BigFix server is a database that communicates with the relays and the BigFix console to manage the devices in your deployment.

Relay

Relays are network components that distribute the download burden from the BigFix server and compile and compress data received from clients.

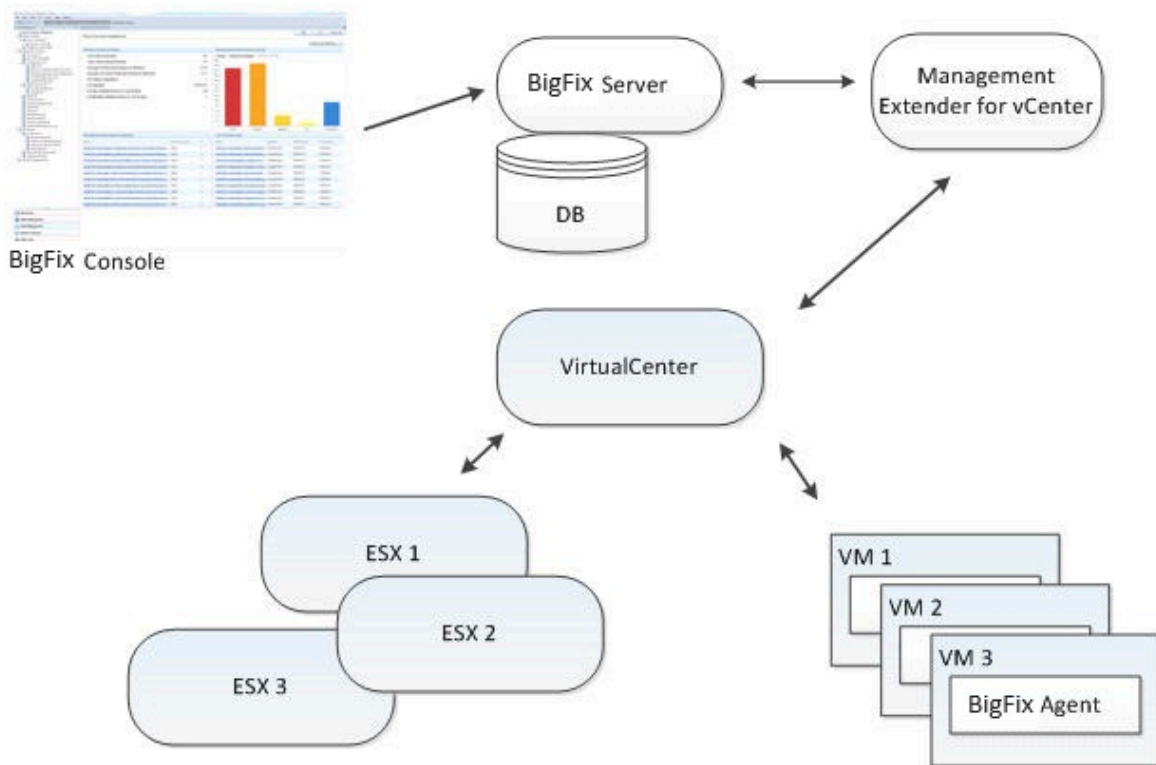
Management Extenders

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

Architecture

The VMware architecture helps in understanding and managing virtualized environment.

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 BigFix architecture and a management extender.

A management extender is a BigFix 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 BigFix server. These reports end up as separate computer objects in the BigFix Console. Because no actual BigFix 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 [List of actionsript commands \(on page 34\)](#).

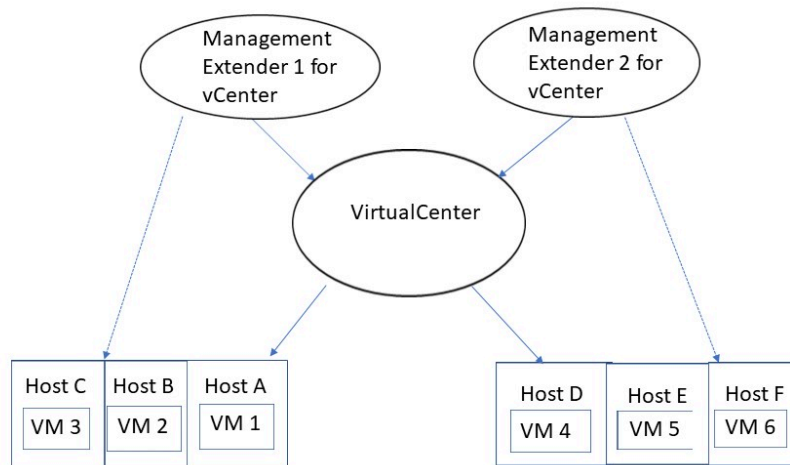
When the BigFix Console issues a command, it gets passed down to the management extender, which translates this action script into VMware API commands. These APIs report back success or failure, and the management extender interprets these results and pass them back up to the BigFix relay. The relay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

Managing the workload balance

Managing the workload balance describes how Patch for VMware ESXi is designed to work in big environments to optimize the workload balance.

The following diagram depicts a visual representation of how Virtual Endpoint Manager is designed to work in big environments to optimize the workload balance. In these environments, the same Virtual Center is managed by two or more management extenders.

A management extender is setup using a BigFix relay that has the proxy agent installed on it along with the vSphere management extender plug-in installed and configured. It enables the communication between the proxy agent and the VMware vCenter.



For each management extender you have, apply the following procedure in order to optimize the workload balance of your environment:

1. Stop the proxy agent service.
2. Clean up the contents of the `DeviceReports` folder located in the `C:\Program Files (x86)\BigFix Enterprise\Management Extender\Plugins\VMware ESXi 1\DeviceReports` directory, where:

C:\Program Files (x86)\BigFix Enterprise\Management Extender

Reflects the proxy agent installation.

3. Modify the `vcenter-plugin-settings.txt` configuration file:
 - a. Uncomment the `HOST_LIST` key and set it as follows:

```
HOST_LIST="hostA,hostB,hostC"
```

- b. Ensure that `hostA`, `hostB` and `hostC` match the ESXi host definition in Vcenter. Therefore, you cannot specify their IP address if they are registered with the Fully qualified domain name (FQDN) or otherwise.
4. Restart the proxy agent service.

After a cleanup of the environment (contents of the `DeviceReports` folder) and a restart of the proxy agent service, the management extender will handle only a subset of virtual machines (VMs), which are the ones that run on the hosts added into the `vcenter-plugin-settings.txt` configuration file.

Important note: The Fixlet 829, if executed, does not recover the `HOST_LIST` key and its content, due to the customization of the parameter, different for each installation. Therefore, it is strongly recommended that you take note of the ESXi hosts configured, if any.

Configuring the management extender

Before you can begin working with the different Virtualization features, you must configure a relay server or a root server to communicate with a specific VMware vCenter or ESX host.

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

1. Install the BigFix relay Version 9.2, 9.5, or 10.0.x.
2. Deploy Fixlet 801: Deploy Management Extender for VMware vCenter from the Patches for ESXi site. This action appears as applicable when the BigFix relay is installed.



Note: Using the Fixlet to install the Management Extender is now deprecated.

3. Activate analysis 905: Management Extender Status.

The screenshot shows the Systems Lifecycle console interface. On the left, a tree view shows the navigation path: Systems Lifecycle Domain > Virtual Endpoint Management > Setup and Configuration > Configure Management Extenders. The 'Configure Management Extenders' item is highlighted with a red box. On the right, a table titled 'Setup and Configuration' lists tasks. The first row, with ID 801 and name 'Deploy Management Extender for VMware vCenter', is highlighted with a red box.

| ID | Name |
|-----|-------------------------------------------------|
| 801 | Deploy Management Extender for VMware vCenter |
| 808 | Deploy VMware Tools (RHEL) |
| 807 | Deploy VMware Tools (Windows) |
| 803 | Remove Management Extender for VMware vCenter |
| 825 | Upgrade Management Extender for VMware vCenter |
| 827 | Upgrade VMware vCenter Plugin |
| 805 | Warning: Outdated VMware Tools Version Detected |



Note: By default, the management extender uses port 443.

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 web 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.

Working with multiple computer representations

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

For example:

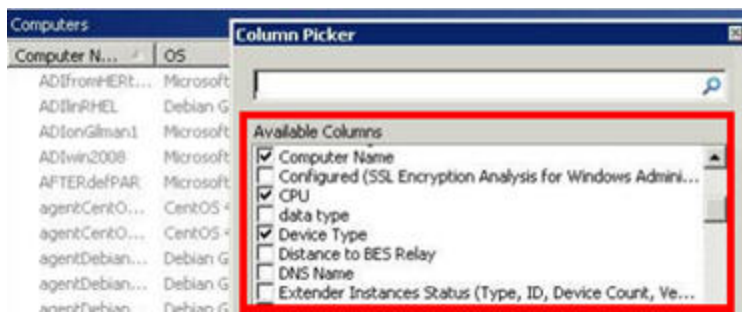
- While working within the BigFix console, some Operators manage virtual infrastructure, including managing virtualized computer processes such as creating, modifying, and powering on/off virtual machines.
- Other operators work directly with operating systems that are running on virtual machines, including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

As a result, the Computers view within the BigFix 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 the **Computers** window, right-click on any column to open the **Column Picker**. In the **Column Picker** menu, select **Device Type**.



Understanding computer representations in BigFix

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.

| Computer Name | Device Type | OS | Last Report Time |
|---------------|---------------------------------|------------------------------------------------|---------------------|
| RHEL63-1 | ESXi Hypervisor Virtual Machine | Red Hat Enterprise Linux 6 (64-bit) | 15/07/2013 14:17:19 |
| rhel63-1 | Server | Linux Red Hat Enterprise Server 6.3 (2.6.32... | 10/04/2013 13:22:44 |

Managing computer representations in BigFix

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 BigFix 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 BigFix.

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. 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 BigFix 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 BigFix 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 BigFix 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 BigFix 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 BigFix Agent installed.

Chapter 3. Setup for VMware plugin

This section or menu option provides instructions for installing and configuring the VMware plugin, including the necessary prerequisite steps.

Site subscription

Sites are collections of Fixlet messages that are created internally by you, by HCL, or by vendors.

Subscribe to a site to access the Fixlet messages to patch systems in your deployment.

You can add a site subscription by using the Licensing Dashboard. For more information about subscribing to Fixlet sites, see the [BigFix Installation Guide](#).

For more information about sites, see the [BigFix Console Operator's Guide](#).

Supported platforms

BigFix Virtual Endpoint Manager supports the following VMware product versions:

- ESXi 7.0
- ESXi 7.0.0
- ESXi 7.0.1
- ESXi 8.0



Note:

- ESXi 6.0 was deprecated. ESXi 6.5 and ESXi 6.7 have reached its End of Life on October 15, 2022. BigFix no longer provides content or support for ESXi 6.0, ESXi 6.5, and ESXi 6.7 after the deprecation date. For more information, see <https://core.vmware.com/blog/reminder-vsphere-6567-end-general-support> and <https://kb.vmware.com/s/article/89305>.
- BigFix supersedes a bulletin Fixlet if a newer version of the vSphere Installation Bundle (VIB) that is associated with that bulletin is available. Sometimes this can happen in the same VMware patch update.

System Requirements

Ensure that you meet the necessary system requirements for the BigFix Patch for Virtual Endpoint Manager.

The requirements are as follows:

- BigFix Version 9.5.x, 10.0.x, or 11.0.x must be used.
- You must subscribe to the Patches for ESXi site.

- The management extender must be installed on a system that runs Windows (Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows 10, Server 2016, Server 2019, and Server 2022).
- The BigFix relay must be installed on the system with the management extender.
- The vCenter user must have an Administrator role to configure the management extender. Having the Administrator role enables users to retrieve host patch status and to avoid relevance issues.

Components

VMware Plugin components are individual building blocks that collectively form the plugin's functionality.

Virtual Endpoint Manager has the following components:

Server

The BigFix server is a database that communicates with the relays and the BigFix console to manage the devices in your deployment.

Plugin portal

For information on plugin portal, refer to The Plugin Portal.

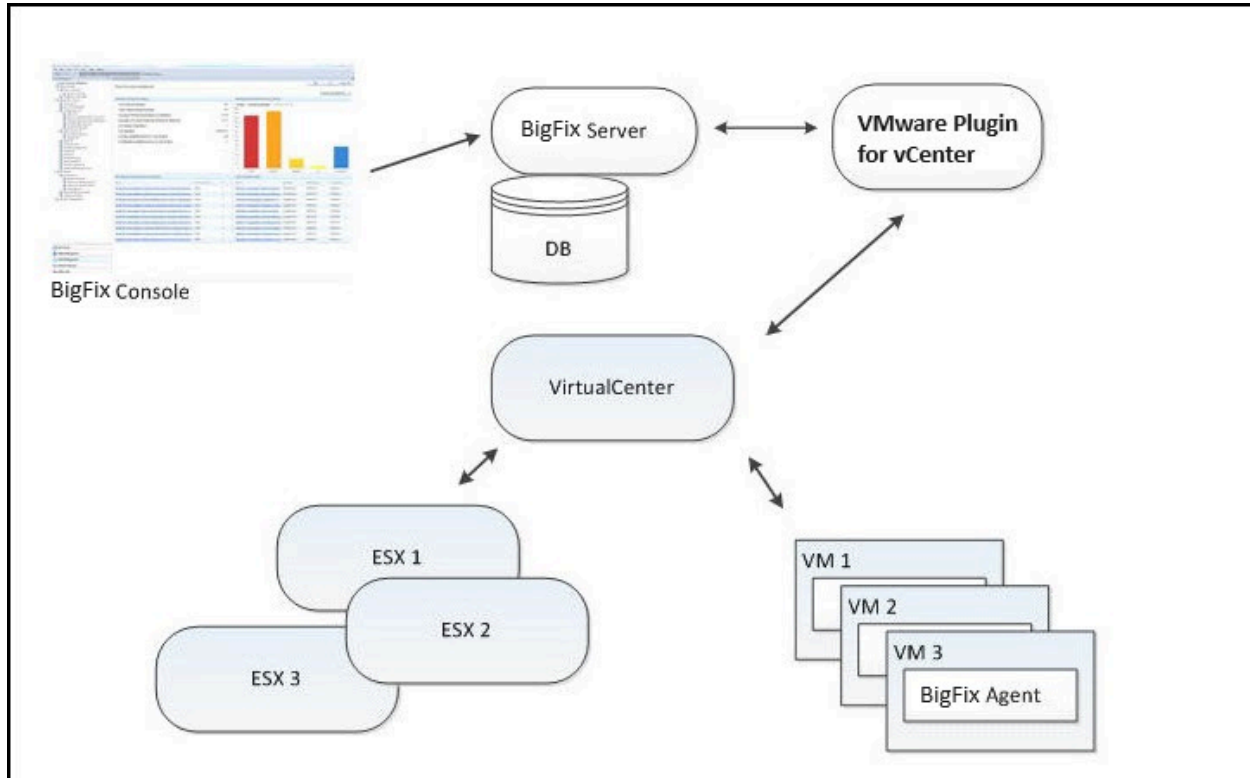
VMware plugin

VMware plugin allow devices to be managed without an agent on the device. VMware plugin communicate to the VMware vCenter by translating BigFix content to VMware commands that are accepted by the VMware vCenter.

Architecture

The VMware architecture helps in understanding and managing virtualized environment.

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 BigFix architecture and a VMware plugin.

A VMware plugin is a BigFix client that has the plugin portal installed on it along with the vSphere management extender plug-in installed and configured.

The VMware plugin sends queries to vCenter about the virtual machines and hosts that it controls, and reports information back to the BigFix server. These reports end up as separate computer objects in the BigFix console. Because no actual BigFix 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 VMware plugin 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 [List of actionscript commands \(on page 34\)](#).

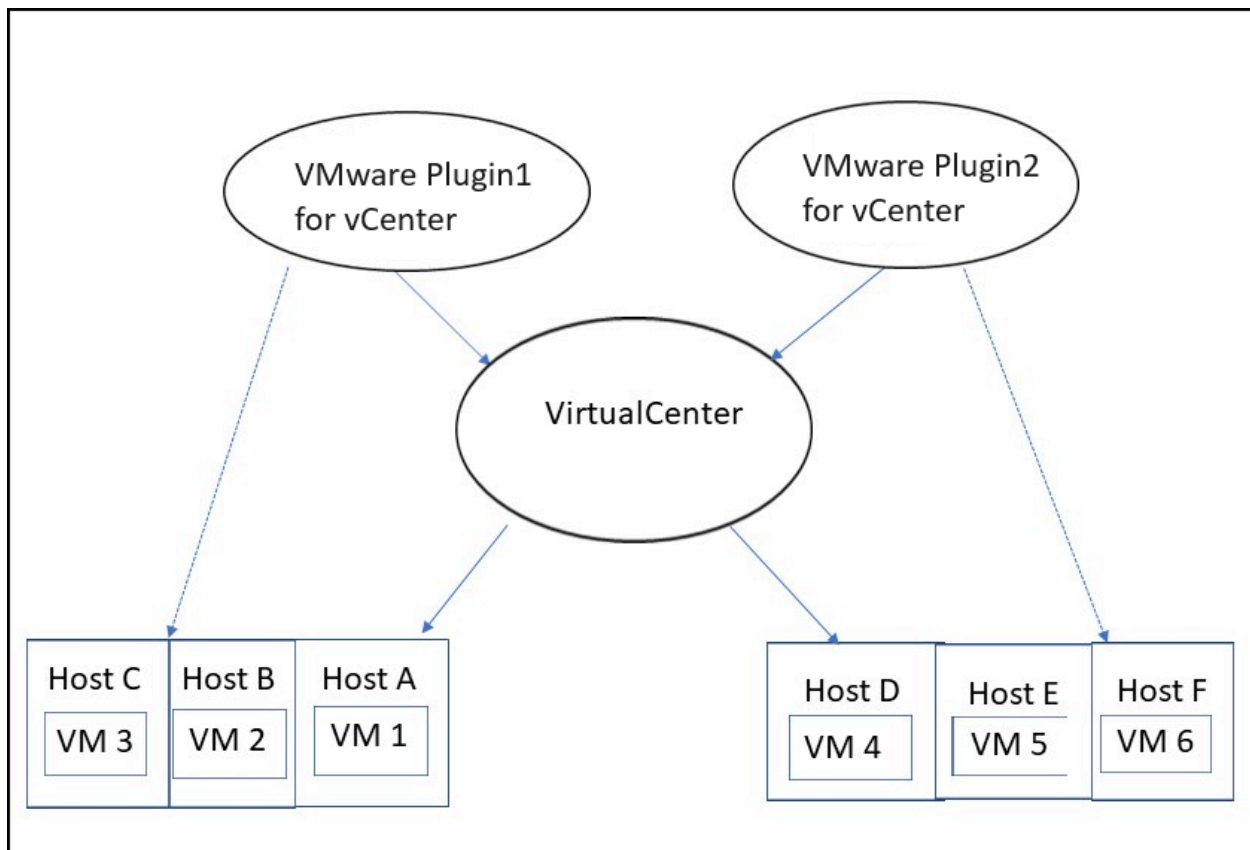
When the BigFix console issues a command, it gets passed down to the VMware plugin, which translates this action script into VMware API commands. These APIs report back success or failure, and the VMware plugin interprets these results and pass them back up to the BigFix client. The client passes them back up to the BigFix server. The status of the commands are reported back to the BigFix console.

Managing the workload balance

Managing the workload balance describes how Patch for VMware ESXi is designed to work in big environments to optimize the workload balance.

The following diagram depicts a visual representation of how Virtual Endpoint Manager is designed to work in big environments to optimize the workload balance. In these environments, the same Virtual Center is managed by two or more VMware plugin.

A VMware plugin is setup using a BigFix client that has the plugin portal installed on it along with the vSphere management extender plug-in installed and configured. It enables the communication between the plugin portal and the VMware vCenter.



To verify and configure the installation of the VMware plugin, please refer to the following links:

1. Verifying the cloud plugin installation
2. Configuring cloud plugins

Configuring the VMware plugin

Before you can begin working with the different Virtualization features, you must configure a VMware plugin.

Before you can configure the VMware plugin, you must do the following steps:

1. Install the BigFix Agent with plugin portal version 10.0.2 or higher.
2. Deploy and configure the BigFix plugin for VMware Discovery for VMware vCenter from the BES support site.
This action appears as applicable when the plugin portal is installed.



Note: For version 11.x onwards, ensure that BigFix plugin portal version 11.0.0 or higher is installed.

To configure, fill in the values for the following items in the window:

- Account Label
- vCenter Server
- User name and Password

Task: Install BigFix Plugin for VMware Discovery - version X.XX.X

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (2)

Description

Install BigFix Plugin for VMware Discovery - version X.XX.X
Installs and configures the BigFix plugin for discovering VMware resources.

Note: This Task will become relevant only on computers where the BigFix Plugin Portal Version 10/11

Enter values for the following parameters:

Account Label:

vCenter Server:

User Name:

Password:

Confirm Password:

For more information on VMware plugin, refer to [Installing cloud plugins](#).

3. Activate analysis 4516: VMware plugin setting.

Chapter 4. Migration from management extender to VMware plugin

This section provides instructions on migrating from the Management Extender to the new VMware plugin for existing setups.

Follow the steps below to migrate from the management extender to VMware plugin:

1. Run the Task 803: Remove Management Extender for VMware vCenter located under "Virtual Endpoint Management site". After completion of this step, the plugin folder and its contents will be removed.
2. Run the Task 1795: Uninstall BigFix Proxy Agent within the BES Support site. This action will uninstall the BigFix Proxy Agent, and also remove the management extender folder and its contents.
3. Follow the steps under [Setup for VMware plugin \(on page 16\)](#), to install and configure the new VMware plugin.

Chapter 5. Offline Patching Workflow

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:

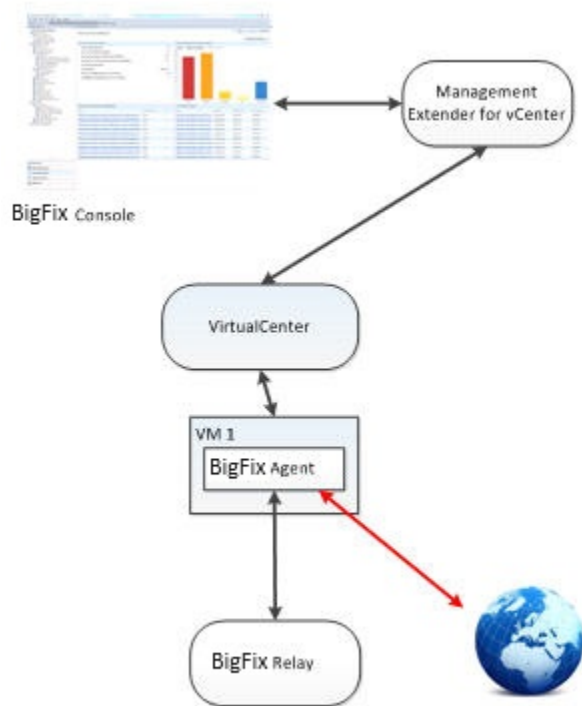
- To apply patches, the virtual machines must have a BigFix agent.
- Currently, this feature is supported by the Management Extender only. However, VMware plugin support is planned for the future.

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.

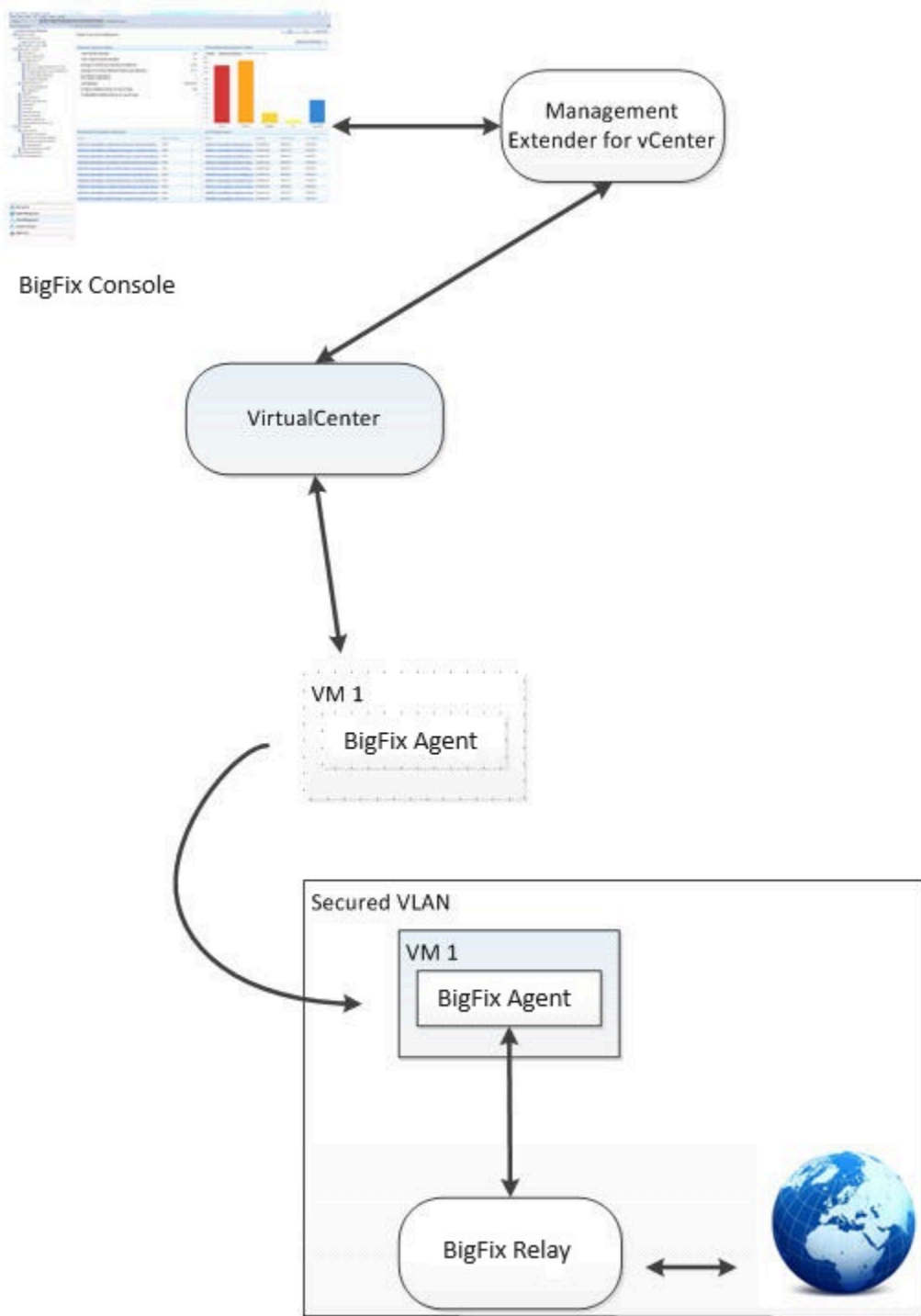
When you select the **Switch VLAN** check box, you can switch to a pre-configured and quarantined VLAN from the dropdown menu.


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 BigFix 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 its network adapters, the VLAN isn't switched for that particular endpoint.



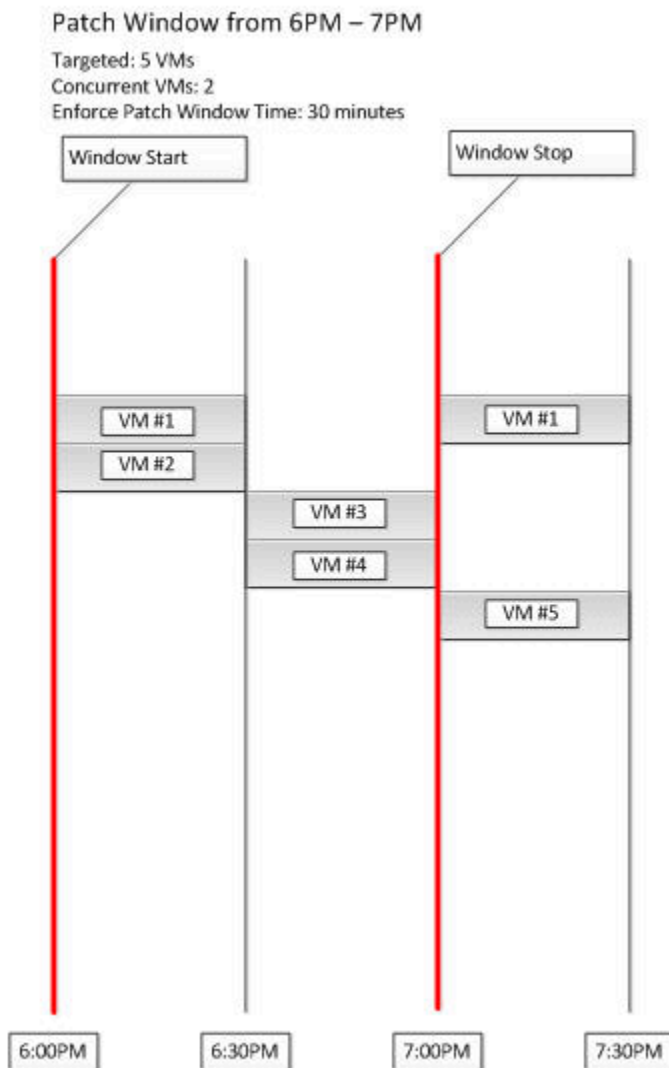
 **Note:** You must have a VLAN configured on an adapter that lets through traffic only from port 52311.

 **Note:** You must have quarantine VLAN setup with a BigFix 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** drop-down 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.



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 Lifecycle** 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

Create New Patch Window

Name:

Start Date:

Start Time: Client Local Time

End Date:

End Time: Client Local Time

Switch VLAN

Concurrent Operations:

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 BigFix 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 \(on page 22\)](#) section.

Supersedence

Please refer to Supersedence for Non-Windows to know more about the supersedence.

Chapter 6. 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 BigFix object. From the list, you can view which machines have the BigFix 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 BigFix 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 - iyRelay40-06 | Microsoft Windows Server 2008 R | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |
| 10.3.128.6 - iyW702-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 - iyXP03-i400 | Microsoft Windows XP Profession: | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |
| 10.3.128.6 - iyXP04-i400 | Microsoft Windows XP Profession: | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |
| 10.3.128.6 - iyXP01-i400 | Microsoft Windows XP Profession: | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |
| 10.3.128.6 - iyXP07-i400 | Microsoft Windows XP Profession: | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |
| 10.3.128.6 - iyXP02-i400 | Microsoft Windows XP Profession: | 10.3.128.6 | poweredOff | Tue, 31 Jul 2012 12:33:18 -0700 | Not Available |

Chapter 7. Specifying virtual device computers

You must create a custom site or have an existing external site in the BigFix 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 BigFix Platform Knowledge Center topic:

[Creating Custom Sites](#)

1. In the BigFix 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: `((device type = "ESXi Hypervisor") or (device 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 8. 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.inspectors` file. These inspectors can be plugged in to the relevance and get information back to the servers.

To see the `ESX.inspectors` 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:

- [BigFix Support Portal](#)
- [BigFix Developer](#)
- [BigFix Playlist on YouTube](#)
- [BigFix Tech Advisors channel on YouTube](#)
- [BigFix Forum](#)

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 BigFix 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 BigFix 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 BigFix 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 BigFix 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?!

Normal machines have a full BigFix agent installed on them, with the full standard set of inspectors and actions. Instead of a full BigFix 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 BigFix properties. However, because a lot of these fields are set by the user, sometimes they can mismatch what gets reported in the BigFix 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 BigFix 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 BigFix 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 US.

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

HCL 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:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. 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 jurisdictions 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. HCL 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-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide 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:

HCL

330 Potrero Ave.

Sunnyvale, CA 94085

USA

Attention: Office of the General Counsel

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 HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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

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

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 actual people or business enterprises 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 HCL, 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. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:

© (your company name) (year).

Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

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

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

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

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

HCL MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.