IBM Endpoint Manager for Software Use Analysis
Version 9.1 (includes update 9.0.1, 9.0.1.1 and 9.0.1.2)

Managing the Infrastructure

Beta documentation

IBM Endpoint Manager for Software Use Analysis
Version 9.1 (includes update 9.0.1, 9.0.1.1 and 9.0.1.2)

Managing the Infrastructure

Beta documentation

IBM

Managing the Infrastructure Guide

This edition applies to version 9.0.1.2 of IBM Endpoint Manager for Software Use Analysis (product number 5725-F57) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Managing the infrastructure

The topics in this section provide instructions for running the scans to discover information about software and hardware in your IT infrastructure. You can manage how IBM® Endpoint Manager for Software Use Analysis handles the discovery of computers and devices on your network, view a summary of the processors in your IT infrastructure, and manage virtual machine managers.

Scalability guide

Scalability guide is intended to help system administrators plan the Software Use Analysis infrastructure and to provide recommendations for configuring the Software Use Analysis server to achieve optimal performance.

The guide explains how to:

- Divide computers into scan groups.
- Schedule software scans.
- Run data imports.

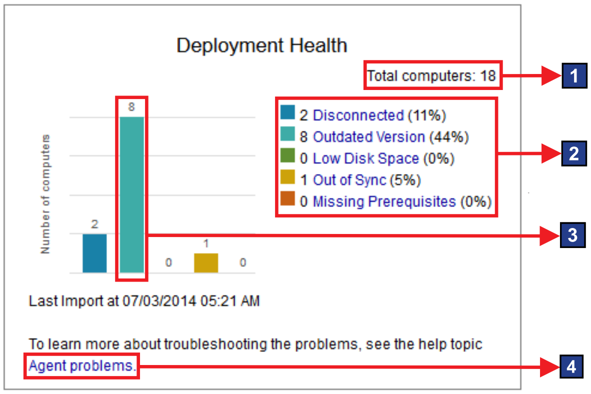
It also provides information about other actions that can be undertaken to avoid low performance. The guide is available on the Software Use Analysis wiki.

Infrastructure administrator dashboard

The dashboard provides you with a quick overview of the most important information about scans and the endpoints in your infrastructure.

Deployment Health

The widget shows whether agents are connecting to the Endpoint Manager server, their outdated versions, and the most important issues that might occur while agents are operating such as problems with disk space or missing software prerequisites.



Deployment Health

Total computers: 18

- 2 Disconnected (11%)
- 8 Outdated Version (44%)
- 0 Low Disk Space (0%)
- 1 Out of Sync (5%)
- 0 Missing Prerequisites (0%)

Last Import at 07/03/2014 05:21 AM

To learn more about troubleshooting the problems, see the help topic Agent problems.

Elements of the widget

1 The total number of computers that a user has access to view. The number of computers that a user can view is determined by the computer group access that is granted to that user.

2 Links to the detailed reports.

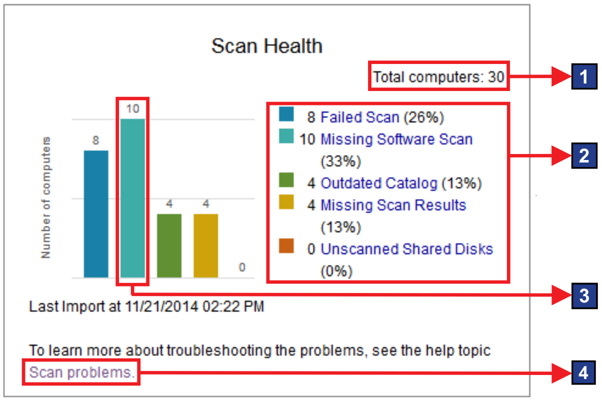
3 The number of computers with a particular status.

4 Link to information about actions that you can take to solve agent problems.

Scan Health

The widget shows the health of scans that are running in your infrastructure. You can drill down to reports for specific computers with scan problems. By sorting the columns of a report, you can quickly understand which computers are failing which specific software scan types.

Important: The Software Scan Status analysis must be enabled for the widget to show valid data. If the analysis is not activated, all computers are reported with a Failed Scan, Missing Software Scan, and Outdated Catalog.


Scan Health
Total computers: 30
Number of computers
8
10
4
4
0
🟦 8 Failed Scan (26%)
🟦 10 Missing Software Scan (33%)
🟩 4 Outdated Catalog (13%)
🟨 4 Missing Scan Results (13%)
🟧 0 Unscanned Shared Disks (0%)
1
2
3
4

Last Import at 11/21/2014 02:22 PM

To learn more about troubleshooting the problems, see the help topic Scan problems.

Elements of the widget

1 The total number of computers that a user has access to view. The number of computers that a user can view is determined by the computer group access that is granted to that user.

2 Links to detailed reports.

3 The number of computers with a particular status.

4 Link to information about scan problems.

Tip: Click **Unscanned Shared Disks** to show the computers that have shared disks that you did not enable to scan. The report also displays information about the discovered shared file systems such as the IP address of the shared disk, the mount point, and the type of shared file system.

Managing computer groups

You can set up computer groups to sort and filter inventory reports. You can also assign contracts to specific computer groups to indicate which computers are entitled to use particular software.

Before you begin

You must have the Manage Computer Groups permission to perform this task.

Procedure

1. To set up a new computer group:
   a. Click **Management** > **Computer Groups** and then, click **New**.
   b. Enter the name and description of a new group in the Create Computer Group pane.
   c. Create filters for your group parameters in the Definition section and click **Create**.
   d. To make new groups available in the component, click **Reports** > **Import Now**.
2. To modify an existing computer group:
   a. Click **Management** > **Computer Groups** and then, click the name of the computer group that you want to modify.
   b. Modify the computer group, and click **Save**.

3. To delete an existing computer group, click the name of the computer group that you want to delete, and click **Delete**.

Viewing hardware inventory

You can use the hardware inventory report to verify the completeness of hardware information and to analyze the processor value unit (PVU) capacity.

Before you begin

You must have the Manage VM Managers and Servers permission to perform this task.

Procedure

1. In the top navigation bar, click **Reports** > **Hardware Inventory**.
2. If the status of the computer is No VM Manager Data, click the name of the status. You will be redirected to the **VM Managers** panel on which you can correct the configuration of the VM manager.

Computer statuses

Agent statuses provide information about the condition of the agents in your infrastructure. To properly discover software, ensure that agents in your environment work correctly.

OK

There are no problems with the agent. No actions are required.

No Scan Data

Hardware inventory data from the capacity scan is missing. To solve the problem, schedule a capacity scan or run it manually on this computer, and upload its results.

No Host Scan Data

The agent is not installed on the host operating system. Depending on the virtualization technology, perform one of the following actions:

HP Integrity VM
Install an agent and wait until it uploads the capacity scan results or upload them manually.

Solaris Container/Zones or Logical Domains (LDOM)
Install the agent in the global zone on the control domain and in other global zones. Wait until it uploads the capacity scan results or upload them manually.

No VM Manager Data

Hardware inventory data from the server is incomplete because the VM Manager is not defined for the host operating system.

Restriction: To use VM managers, ensure that the following conditions are fulfilled:

- You have sufficient rights to collect information about the complete virtualization topology including virtual machines, hosts, clusters, and relations among them.
- The UUIDs of virtual machines and hosts are valid and in scope of the particular virtualization technology.
- Information about the number of processors, total number of cores, and processor description is available.

To solve the problem, perform one of the following actions.

- Check whether the VM Manager is connected.
- Check whether any clusters in your infrastructure are defined under the same name. In the VMware environment, it is not possible to create two clusters with the same name in the same data center. However, vCenter can manage several data centers at the same time. It means that it might control clusters with the same name defined in different data centers. Thus, if some clusters share a name, rename them to keep each name unique.
- Check whether the value of the **`computerVmManagerDetachmentPeriod`** parameter is higher than the frequency with which data is retrieved from VM Managers. The interval between consecutive retrievals of data is set in the **`vmm_polling_time_interval`** parameter and is 30 minutes by default. If the idle time after which a computer that is managed by a VM Manager is considered detached is lower, change the value of the **`computerVmManagerDetachmentPeriod`** parameter.
- Depending on the virtualization technology, perform one of the following actions:

  VMware ESX(i)
  Configure the VM manager in the user interface.

  Hyper-V or KVM
  Configure the VM manager in the user interface.

  KVM - RHEV-M
  If one or more computers have the No VM Manager Data status, even though you correctly configured the VM manager connection, perform the following actions. If the **Server ID** on the Hardware Inventory panel is in the `TLM_VM_`*`UUID_of_the_VM`* format, check whether the UUID is correctly set on the machine. If two or more virtual machines have the same UUID, manually set unique UUIDs for these machines. Note, that virtual machines can operate on different hosts.

Managing VM managers

A *virtual machine manager* is a server (for example, ESX of vCenter) that manages and monitors virtual machines that are installed in your IT infrastructure. Due to the nature of some virtualization technologies, for example VMware, scanners that are deployed on such virtualization solutions are not able to gather data about physical host computer systems. Therefore, they are not able to gather and provide information about, for example, processor types or the number of processor cores. Without this information, it is impossible to calculate the PVU, RVU, or systems capacity for a software item and maintain license compliance. You can obtain this information only when data from agents as well as VM managers are accessible. To collect data from such virtual environments, the VM Manager Tool must be used.

About this task

VM Manager Tool, which is installed automatically with the Software Use Analysis server configuration on the IBM Endpoint Manager server, is used to collect information that concerns physical and virtual machines that are installed in your IT infrastructure. The information is referred to as virtualization infrastructure capacity data and is required to calculate the processor value units (PVU), resource value units (RVU) and to maintain license compliance. For the purposes of software audit reports, you must configure all the connections to the virtual machine managers which are managing the x86 virtual machines in your infrastructure.

Default x86 PVU counting

To properly calculate the consumption of PVU subcapacity licenses, Software Use Analysis requires information about the number of processor cores that are available to virtual machines and the number of processor cores that are physically installed on the server. To retrieve this information, Software Use Analysis must connect to the hypervisor, so ensure that connections to all VM managers are properly configured. If you do not configure VM manager connections and Software Use Analysis is not able to retrieve the required information, the license usage cannot be properly counted and the calculated results might be over-counted for x86 processors.

Without hypervisor information, Software Use Analysis cannot properly identify the PVU rate for a processor that often depends on the model and type of the processor as well as the number of processors that can be installed on a physical host (the number of sockets). If Software Use Analysis cannot identify the PVU rate for a processor, it applies the PVU rate for the configuration with the highest number of sockets that is possible for the particular processor. Also, if CPU is overcommitted to virtual machines and the total virtual capacity exceeds the physical capacity, virtual capacity must be capped to physical capacity according to the pricing rules. Without the hypervisor data, Software Use Analysis cannot limit virtualization capacity to physical capacity.

Capacity data flow

In the centralized and distributed virtual machines management, the propagation of data about the infrastructure might take up to two days because of the number of intermediate hops and custom configurations.

The overall virtualization data traffic comprises:

- Configuration data that is pushed down to the endpoints
- Infrastructure data that is uploaded from the VM Manager Tool
- Capacity data that is uploaded from the Endpoint Manager clients to the Endpoint Manager and then to the Software Use Analysis server

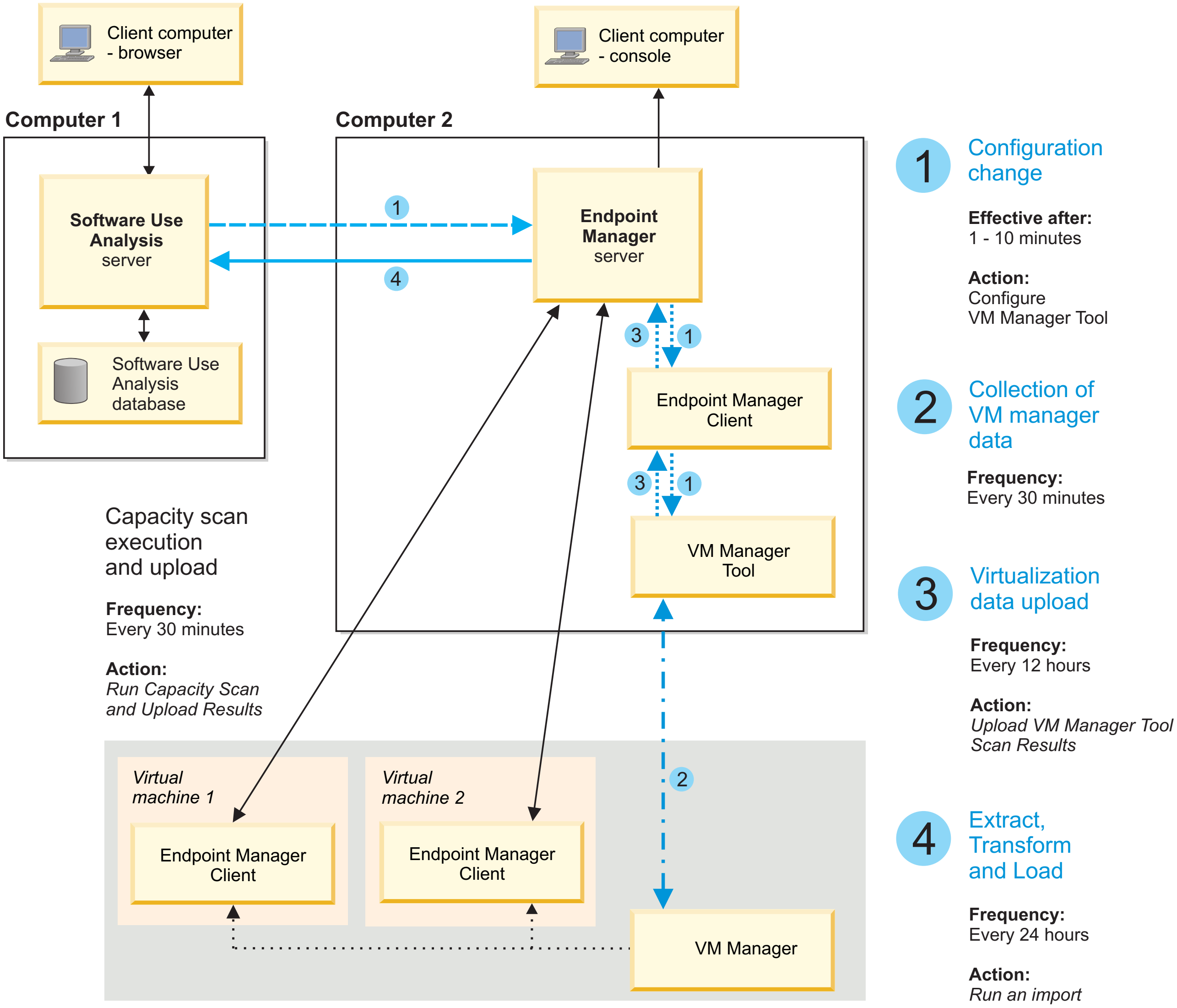
Important: It might happen that the **VM managers** panel does not display up-to-date information about your virtual systems. This delay might be caused by the fact that the data about your virtual environments and the configuration data goes through many infrastructure elements and depends on various scheduled tasks. As a result, the time that is needed for complete virtualization data to reach the product and get displayed in the interface might be long, up two days, depending on your specific configurations.

Example:

Table 1. Phases of data traffic in case of centralized virtual machine management

Number	Step	Time required
1.	Configuration data is sent to the endpoints.	10 minutes
2.	VM manager data is collected from your VM managers to the VM Manager Tool.	30 minutes
3.	VM manager data is uploaded from the VM manager tool to the Endpoint Manager server.	12 hours
4.	The current infrastructure data, both from the clients and the VM manager tool, is imported from the Endpoint Manager server to the Software Use Analysis server.	24 hours
		The total time that it takes to display virtualization data might be longer than 24 hours.

Visualization of data traffic in case of centralized virtual machine management



VM managers

A *virtual machine manager* is a particular source of data that is provided by the virtualization vendor. Use VM managers to administer virtual machines in your IT infrastructure and to access their data to calculate the processor value unit (PVU), resource value unit (RVU), or system capacity.

VM managers are used to collect information concerning virtual machines that are installed in your infrastructure. Due to the nature of some virtualization technologies, for example VMware, the scanner deployed on such virtualization solutions is not able to gather data about physical host computer systems. Therefore, they are not able to gather and provide information about, for example, processor types or the number of processor cores. Without this information, it is impossible to calculate the PVU, RVU, or system capacity for a given software and maintain license compliance. You can obtain this information only when data from the scanner as well as VM managers are accessible.

The data from virtual machine manager is collected by the VM Manager Tool that can be installed on any end point in your infrastructure. In the current version of IBM Endpoint Manager for Software Use Analysis you can use one of two possible virtual machines management approaches:

- Centralized virtual machine management, where the VM Manager Tool is automatically installed on the IBM Endpoint Manager server, and all configuration is done directly from the Software Use Analysis web user interface,
- Distributed virtual machine management, where the VM Manager Tool can be installed on any IBM Endpoint Manager endpoint, and only manual configuration in configuration files with no user interface is possible.

You can combine both approaches. It is possible to use the central VM Manager Tool that is installed on the IBM Endpoint Manager server along with other installations of theVM Manager Tool on other IBM Endpoint Manager endpoints.

VM managers can be divided according to their type:

- "VMware vSphere"
- "Microsoft Hyper-V" on page 9
- "Kernel-based Virtual Machine" on page 14

VMware vSphere

VMware vSphere is one of the virtualization technologies supported by Software Use Analysis.

Purpose

This solution consists of two products: a VMware ESX (or ESXi) hypervisor and a VMware vCenter server. Both of these components provide the API that can be used to extract information concerning virtual machines in your infrastructure. The section below shows the differences between these two varieties.

ESX or ESXi

It is an operating system that hosts virtual machines. It is enough to connect to a specific ESX if you do not use any software deployed in a clustered environment. However, if an ESX is controlled by a vCenter, it is recommended to connect a given VM manager to it via the vCenter. This is because Software Use Analysis needs data from every ESX box (every box that hosts a virtual machine where the CIT scanner is installed). If you choose a connection via ESX, you have to define all the ESX boxes separately in the VM Managers panel. If you have a vCenter deployed, you can manage all the ESX boxes via this server (it saves time and decreases the network load).

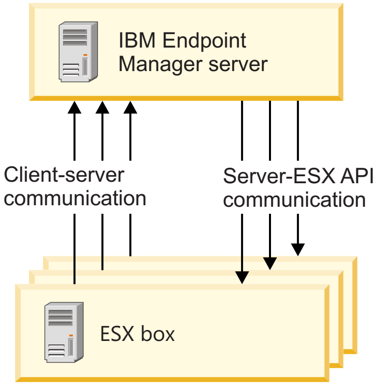
Note: Changing the Universally Unique Identifier (UUID) on ESX virtual machines may lead to overcharging because when the identifier is changed, Software Use Analysis recognizes it as a brand new virtual machine.

The default URL that is to be used (it may vary in your environment if the administrator of the ESX box has changed the configuration of the API, for example, if the HTTP protocol is used instead of the HTTPS one):

```
https://<ESX_IP_address>/sdk
```

Supported versions:

ESX	3.0, 3.5, 4.0, 4.1
ESXi	3.5, 4.0, 4.1, 5.0, 5.1, 5.5


IBM Endpoint Manager server
Client-server communication
Server-ESX API communication
ESX box

vCenter

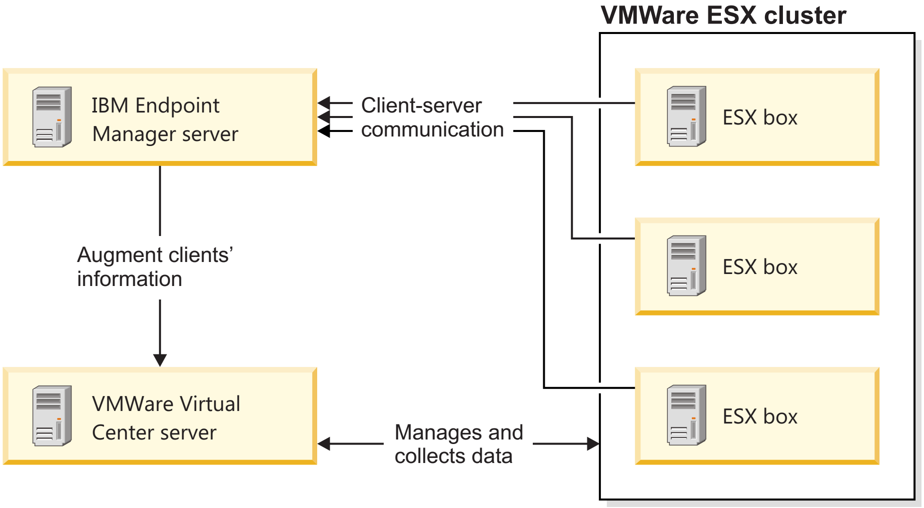
It is used for managing computer systems on which virtual machines are installed. You have to use it if your software is installed in a clustered environment. Instead of connecting to each ESX box separately, you connect to all ESX boxes via a vCenter, whose main role is to retrieve data from them. Therefore, it is beneficial to you to connect to ESX boxes through a vCenter even if you do not have a clustered environment because in this way you can reduce the network traffic.

The default URL that is to be used (it may vary in your environment if the administrator of the vCenter has changed the configuration of the API, for example, if the HTTP protocol is used instead of the HTTPS one):

```
https://<vCenter_IP_address>/sdk
```

Supported versions:

vCenter 2.0, 2.5, 4.0, 4.1, 5.0, 5.1, and 5.5


VMWare ESX cluster
IBM Endpoint Manager server
Client-server communication
ESX box
ESX box
ESX box
Augment clients' information
VMWare Virtual Center server
Manages and collects data

Verifying permissions for VMware communication:

Users must have sufficient privileges to collect all the data from the VM managers for VMWare. The user must have at least read-only rights to all VMs on which the agents are running.

Before you begin

You verify whether users have sufficient privileges in the VMware Infrastructure Client. The user must have the correct access privileges for VMs on which the endpoints are running, and for the hosts of the VMs. If a user has insufficient privileges, agents return a No VM Manager Data status.

This procedure describes how to enable read-only rights for all elements in a virtual topology. Read-access is required only to the VMs on which the endpoints are running and to hosts of these VMs. However, the easiest way to set access permissions is to configure read-only access for all elements in a virtual topology.

Procedure

1. To extend the privileges for the user, log in to VMware Infrastructure Client with a user that has administrator rights.
2. Right-click on the left bar and choose **Hosts and Clusters**.
3. Go to Permissions tab, right-click anywhere in the section, and then click **Add Permission**.
4. In the Assign Permissions panel, click **Add**, choose the user, and then click **OK**.
5. Choose Read-Only as an Assigned Role.
6. Select the **Propagate to Child Objects** check box, and click **OK**.

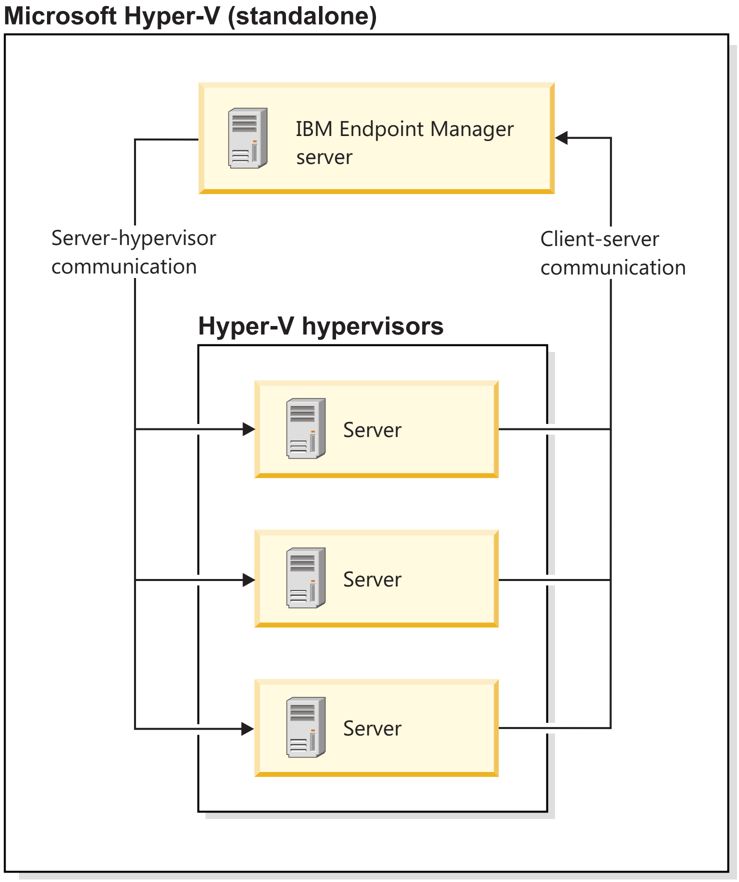
Microsoft Hyper-V

Microsoft Hyper-V is one of the virtualization technologies supported by Software Use Analysis. This solution is the successor of Microsoft Virtual Server.

Purpose

To retrieve information about the measures and virtualization structure of virtual machines that are installed in your infrastructure, it is required to define the Hyper-V hypervisors as VM managers on the Software Use Analysis server.

Hyper-V servers are able to expose required data via the WS-MAN protocol.


Microsoft Hyper-V (standalone)
IBM Endpoint Manager server
Server-hypervisor communication
Client-server communication
Hyper-V hypervisors
Server
Server
Server

Note:

By default, Windows Remote Management Service (WinRM), which provides data by using the WS-MAN protocol, is disabled for remote connections. To learn how to enable it, see "Configuring WinRM on Hyper-V hosts" on page 11.

WinRM must be configured for all members of the Hyper-V cluster.

In the case of clusters, there are two possible approaches:

1. Define all the Hyper-V servers that are a part of the cluster in the VM Managers panel (if there are any missing servers, they will have an *Incomplete definition* status).
2. If all the members of the cluster have at least one common set of credentials (for example, domain user) that has privileges to access WS-MAN interface, you can define only one computer system from the cluster as a VM manager and select the option of sharing credentials. The Software Use Analysis server will use the credentials to connect to the first Hyper-V (defined in the user interface), and then it will extract all the addresses of the rest of the cluster members and connect to them using the same credentials.

The default URL that is to be used (it may vary in your environment if the administrator of the Hyper-V hypervisor has changed the configuration of the API, for example, if the HTTP protocol is used instead of the HTTPS one):

```
https://<HYPER-V_IP_address>:<port>/wsman
```

where `<port>` refers to the port of the listener that was created for the WinRM service. The default value for HTTP listeners is 80 and for HTTPS ones is 443. To learn more, see the *Defining HTTP and HTTPS listeners* section in "Configuring WinRM on Hyper-V hosts."

Important: Different definitions of users are used for Microsoft Hyper-V, VMware, and RHEV-M:

- For Microsoft Hyper-V, the user is defined as *user_name\domain*, for example: `test\cluster.com`
- For VMware, the user is defined as *domain\user_name*, for example: `cluster.com\test`
- For RHEV-M, the user is defined as *user_name@domain*, for example: `test@cluster.com`

Supported versions:

Hyper-V R1 and R2 (either stand-alone or a part of Microsoft Server 2008)

Configuring WinRM on Hyper-V hosts:

Configure Windows Remote Management to allow the Software Use Analysis server to gather data about virtualization topology of virtual machines installed in your infrastructure.

Before you begin

- To retrieve the data that is required to properly calculate PVU, you must be logged in as a local administrator on the Hyper-V host. It is necessary because the Windows Management Instrumentation call that accesses MsCluster namespace requires an administrative account.
- Hardcoded and select-only statements are run over WinRM. The obtained data is stored in a database schema. Software Use Analysis does not modify the Hyper-V settings and does not affect it any other way.

About this task

The WinRM service is an implementation of WS-Management specification that enables cooperation between hardware and operating systems that come from different vendors. The Software Use Analysis server connects to this service defined as a VM manager and collects data regarding virtualization hierarchy. Therefore, you must perform the following procedure on each Hyper-V host in your infrastructure, including those that are part of a cluster, to ensure the WinRM service is running and configured to enable communication with the server.

Procedure

1. **Defining HTTP and HTTPS listeners.** By default, communication with the WinRM service is disabled because there are no listeners defined. To check whether there are any listeners that are currently defined, type the following command: `winrm enumerate winrm/config/listener`. If there is no output returned, there are no listeners defined.
   a. To define a default HTTP listener, type:
   ```
   winrm quickconfig
   ```

   The command starts the WinRM service and sets it to start automatically with the system start. It also creates an HTTP listener on the default port (accepting requests from any IP), it defines Internet Connection Firewall exceptions for the service, and it opens the HTTP port. Depending on the version of the WinRM service, the default HTTP port might be 80 or 5985. For more information, see Installation and Configuration for Windows Remote Management.

b. To define a listener for secure connection (HTTPS), you must have a valid certificate on the Hyper-V host with a CN that matches the host name that you are using to connect to Hyper-V. You must also create a listener with the CertificateThumbprint of that certificate. For more information, see the Microsoft documentation: http://support.microsoft.com/kb/2019527.. You might be able to create a self-signed certificate for testing purposes, however, you should consult your certificate administrator.

   Note: If an appropriate certificate was not found on the machine, the above command will not work and the following output will be returned “The certificate must have a CN matching the host name, be appropriate for Server Authentication, and not be expired, revoked, or self-signed.” If there is a need to use a self-signed certificate, you can manually generate it and create the listener by starting the following command:

   ```
   winrm create winrm/config/listener?Address=*+Transport=HTTPS
   @{Hostname="<the name of your server>";CertificateThumbprint="<certificate thumbprint>"}
   ```

   In this case you have to configure the firewall settings manually.

2. **Enabling WinRM *Negotiate* authentication scheme.** The WinRM service offers several authentication schemes to be used to authenticate the client side. The Software Use Analysis server uses *Negotiate* authentication scheme, which is enabled by default.
   a. To check the current setting of this property, type:
      ```
      winrm get winrm/config/service/auth
      ```
   b. To set the required value of this property, enter:
      ```
      winrm set winrm/config/service/auth @{Negotiate="true"}
      ```
3. **Setting WinRM *AllowUnencrypted* property.** The server requires the property to be set to "true".
   a. To check the current settings, type:
      ```
      winrm get winrm/config/service
      ```
   b. To set the required value of this property, type:
      ```
      winrm set winrm/config/service @{AllowUnencrypted="true"}
      ```

      Note: Setting this value to "true" does not mean that the sensitive data, such as user names or passwords, will be passed in an unencrypted form over the network. Only the content of the SOAP messages will be sent as a plain text. If this cannot be accepted because of security reasons, define the HTTPS listener and use the secured transport (HTTPS) while defining a VM manager in the Software Use Analysis server so that the TLS protocol will be used to encrypt all the network traffic.
4. **Verifying the listener.** After you define the HTTP or HTTPS listener, verify that you can remotely connect to the Hyper-V server.
   a. On the Hyper-V server, determine the port on which the Windows Remote Management client for the HTTP or HTTPS transport listens. Type the following command in the Windows command line:
      ```
      winrm enumerate winrm/config/listener
      ```
      - If the port number is listed in the `Port` line, the listener was properly created.

   - If you receive an error or there is no information for the transport, the listener was not created properly. Go back to step one, and define the listener again.

   b. To verify the listener, type:

   ```
   winrm enumerate winrm/config/listener /r:<transport>://
   <Hyper-V_server_name>:<port>/wsman /u:<user_id> /p:<password> /a:Negotiate
   ```

   Where

   <transport>
   Is either HTTP or HTTPS.

   <Hyper-V_server_name>
   Is the host name of the Hyper-V server. If you are using HTTPS, the host name must match the CN in the certificate.

   <port> Is the port number that you obtained in the previous step.

   <user_id>
   Is the user ID that is used to connect to the Hyper-V server.

   <password>
   Is the password that is used to connect to the Hyper-V server.

   For example:

   ```
   winrm enumerate winrm/config/listener /r:https://
   myhyperv.ibm.com:5986/wsman /u:administrator /p:abc /a:Negotiate
   ```

5. **Verifying whether the Virtual System Management service is running.** To verify that the service that provides Hyper-V management is running, go to **Administrator Tools** > **Services** on the Hyper-V server. Look for the service called Hyper-V Virtual Machine Management
   - If the service exists, but is not running, start the service.
   - If the service does not exist, the Hyper-V host was not configured properly.
6. **Verifying the MsCluster resource.** If the server is clustered, verify that you can access the MsCluster namespace. On the Hyper-V server, type the following command into the Windows command line:

   ```
   winrm enumerate wmi/root/MsCluster/*
   -dialect:"http://schemas.microsoft.com/wbem/wsman/1/WQL"
   -filter:"SELECT PrivateProperties, Type FROM MsCluster_Resource WHERE Type='Network Name' AND Flags='1'"
   ```

   If this command fails, refer to Microsoft documentation about WMI for MsCluster.
7. **Verifying remote connectivity and the server certificate.** To verify remote connectivity and the server certificate, type the following command into the Windows command line:

   Restriction: Enter the following command on the Windows command line of the Software Use Analysis server. If the server is not installed on a computer that runs on a Windows operating system, use a computer that is not the Hyper-V host and runs on Windows 2008 or higher.

   ```
   winrm set winrm/config/client @TrustedHosts={"<Hyper-V_server_name>"}
   winrm get winrm/config/client /r:<transport>://
   <Hyper-V_server_name>:<port>/wsman /u:<user_id> /p:<password> /a:Negotiate
   ```

   Where

   <transport>
   Is either HTTP or HTTPS.

   <Hyper-V_server_name>
   Is the host name of the Hyper-V server. If you are using HTTPS, the host name must match the CN in the certificate.

<port> Is the port number on which the Windows Remote Management client for the HTTP or HTTPS transport listens.

<user_id>
Is the user ID that is used to connect to the Hyper-V server.

<password>
Is the password that is used to connect to the Hyper-V server.

For example:

```
winrm set winrm/config/client @TrustedHosts={"myhyperv.ibm.com"}
winrm get winrm/config/client /r:https://
myhyperv.ibm.com:5986/wsman /u:administrator /p:abc /a:Negotiate
```

The following error is often returned when a self-signed certificate is used is:

```
WSManFault
Message = The server certificate on the destination computer (myhyperv.ibm.com:5986)
has the following errors: The SSL certificate is signed by an unknown certificate authority.
```

If you receive this error, export the self-signed certificate from the Hyper-V host, and import it on the Software Use Analysis host. For other errors, refer to Microsoft documentation for the returned error code.

Tip: For more information about Hyper-V configuration, see the following documents: Hyper-V connection fails CODVM0005E and Hyper-V configuration matrix.

Kernel-based Virtual Machine

Kernel-based Virtual Machine is one of the virtualization technologies supported by Software Use Analysis.

Purpose

Kernel-based Virtual Machine (KVM) represents the latest generation of an open source virtualization. KVM is a full virtualization solution for Linux on x86 hardware containing virtualization extensions (Intel VT or AMD-V). In the KVM architecture, each guest (virtual machine) is implemented as a regular Linux process. After you install KVM, you can run multiple guests, with each of them running a different operating system image. Each of these virtual machines has private, virtualized hardware, which includes memory, storage, graphics adapter, and a network card. This allows KVM to benefit from all the features of the Linux kernel.

Red Hat Entreprise Virtualization Manager (RHEV-M)

Red Hat Enterprise Virtualization (RHEV) is an enterprise virtualization product based on the KVM hypervisor. RHEV-M is a service running on a Red Hat Enterprise Linux server that provides interfaces for controlling the virtualization platform. It manages provisioning, connection protocols, user sessions logins and logoffs, virtual desktop pools, virtual machine images, and the high availability and clustering systems. RHEV-M provides the REST API that is used by Software Use Analysis to collect information about the whole infrastructure that is managed by RHEV-M.

The default URL that is to be used:

- For RHEV-M 3.0

  ```
  https://<RHEV-M_IP_address>:8443/api
  ```

- For RHEV-M 3.1

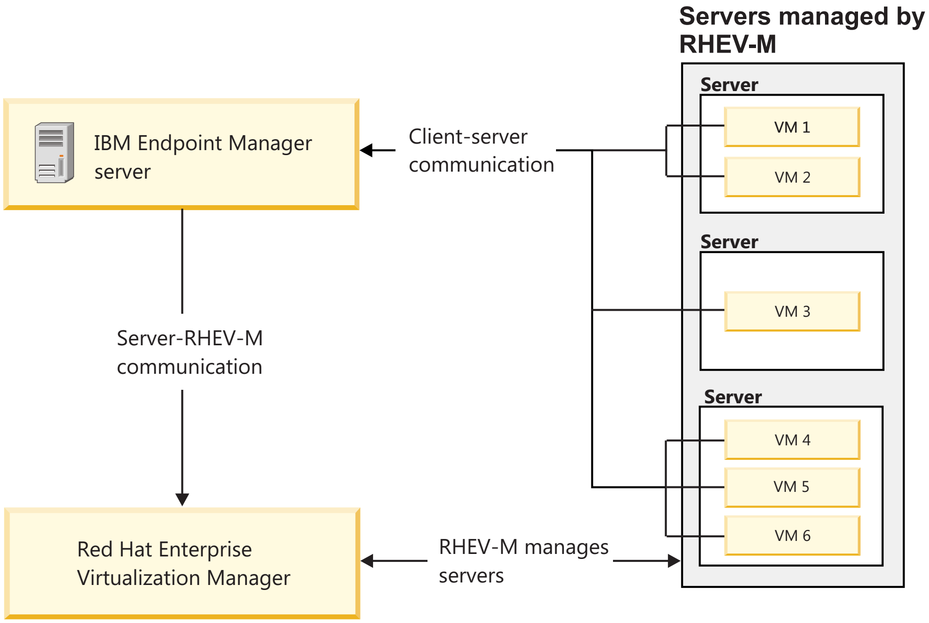
  ```
  https://<RHEV-M_IP_address>:443/api
  ```

Important: Different definitions of users are used for Microsoft Hyper-V, VMware, and RHEV-M:

- For Microsoft Hyper-V, the user is defined as *user_name*\domain, for example: `test\cluster.com`
- For VMware, the user is defined as *domain*\user_name, for example: `cluster.com\test`
- For RHEV-M, the user is defined as *user_name@domain*, for example: `test@cluster.com`

Supported versions:

Red Hat Enterprise Virtualization Manager 3.0 and 3.1


Servers managed by RHEV-M
Server
VM 1
VM 2
Server
VM 3
Server
VM 4
VM 5
VM 6
IBM Endpoint Manager server
Client-server communication
Server-RHEV-M communication
Red Hat Enterprise Virtualization Manager
RHEV-M manages servers

Important: Different definitions of users are used for Microsoft Hyper-V and VMware:

- For Microsoft Hyper-V, the user is defined as *user_name*\domain, for example: `test\cluster.com`
- For VMware, the user is defined as *domain*\user_name, for example: `cluster.com\test`

Centralized virtual machines management

Use centralized approach when the direct connection from the IBM Endpoint Manager server to all virtual machine managers is possible.

VM Manager Tool is installed and configured automatically on the Endpoint Manager server. However, as a prerequisite, you must install the Endpoint Manager client and the Web Reports on that computer. The upload of the VM Manager Tool scan results is activated during the Software Use Analysis server configuration.

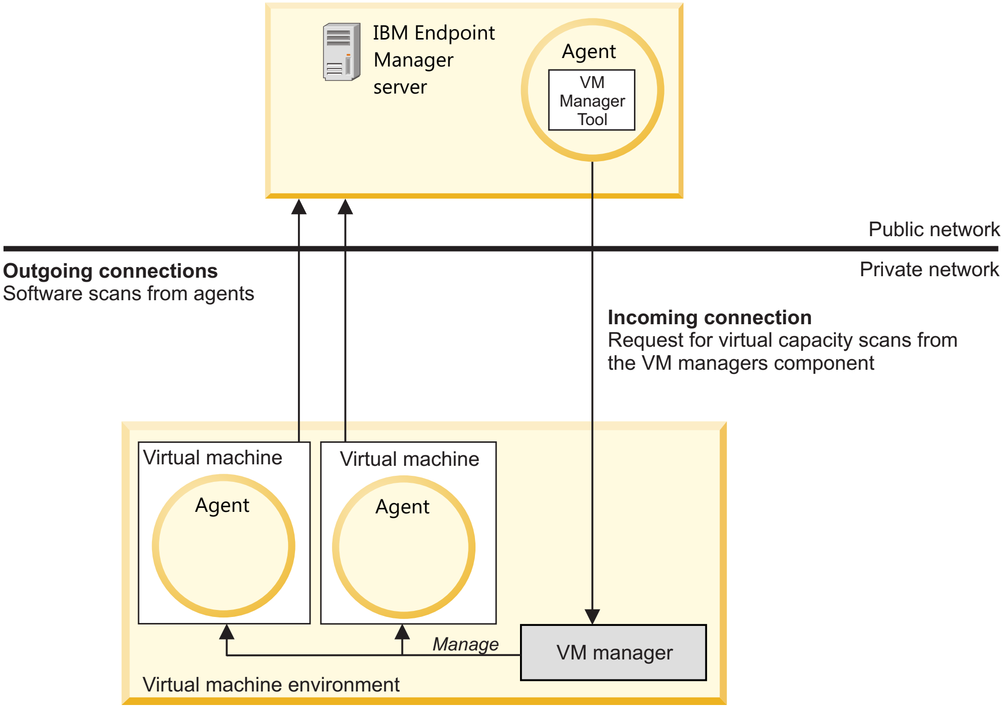
Note: If the installation of the VM Manager Tool fails, a message box is displayed which informs you that you are not able to configure a VM manager. For more information about reinstalling the tool, see Installing VM Manager Tool.

With centralized virtual machine management, you can configure the connection to your VM managers with the web User Interface. The possible operations are adding, modifying, and deleting each configuration. After you submitted a single setup record, the whole configuration is sent from the endpoint to the VM Manager Tool.

Important: You must have the Manage VM Managers and Servers permission to access the VM Managers panel.

VM managers that are in the VM Managers panel are related to the Endpoint Manager server that is defined as the primary data source on the Software Use Analysis server. If you maintain other data sources that have the VM Manager Tool installed, then the related VM managers are not visible in the panel. These VM managers can be managed with the distributed approach.

When you delete the primary data source, the next data source that you maintain becomes the primary one. In such a case, you must manually install the VM Manager Tool on that data source and then activate the upload of scan results.


IBM Endpoint Manager server
Agent
VM Manager Tool
Public network
Private network
Outgoing connections
Software scans from agents
Incoming connection
Request for virtual capacity scans from the VM managers component
Virtual machine
Agent
Virtual machine
Agent
Manage
VM manager
Virtual machine environment

Adding VM managers

You can add virtual machine managers to gather information about virtual machines that are installed in your infrastructure.

Before you begin

You must have the Manage VM Managers and Servers permission to perform this task.

Procedure

1. In the top navigation bar, click **Management** > **VM Managers**.
2. To create a VM manager, click **New**.

3. From the drop-down list, choose the type of the VM manager.

   Note: If you choose Microsoft Hyper-V, you can select the option to **Share credentials with other hosts in the same cluster**.
4. Enter the URL of the VM manager that you want to add.

   Important: You can enter either a full URL, its part, a host name, or an IP address. If you enter the host name, or IP address, the full address of the VM manager is built based on the selected type of the VM manager and protocol (if specified). The HTTPS protocol is used by default.
5. Enter your user name and password.

   Important: Different definitions of users are used for Microsoft Hyper-V, VMware, and RHEV-M:
   - For Microsoft Hyper-V, the user is defined as *user_name\domain*, for example: `test\cluster.com`
   - For VMware, the user is defined as *domain\user_name*, for example: `cluster.com\test`
   - For RHEV-M, the user is defined as *user_name@domain*, for example: `test@cluster.com`
6. Click **Create**.

Results

After a successful configuration, all configuration entries are sent to the VM Manager Tool.

Changing VM managers

Modify the settings of the VM manager by changing its URL or user credentials. You can also to resume a given VM manager if it was suspended due to incorrectly specified credentials or password expiration.

Before you begin

You must have the Manage VM Managers and Servers permission to perform this task.

Procedure

1. In the top navigation bar, click **Management** > **VM Managers**.
2. Click the VM manager that you want to change, or resume.
3. Change the manager type, URL, or user credentials of the VM manager.
4. To confirm the changes, click **Save**.

   Note: If you choose Microsoft Hyper-V, you will be able to select the option to share credentials with other hosts in the same cluster.

Results

After the successful change of configuration parameters of the VM manager, all configuration entries are sent to the VM Manager Tool.

Deleting VM managers

You can remove the VM managers from the list so that the server can connect to collect the data.

Before you begin

You must have the Manage VM Managers and Servers permission to perform this task.

Procedure

1. In the top navigation bar, click **Management** > **VM Managers**.
2. Click the VM manager that you want to remove from the list and then click **Delete**.
3. To confirm your decision, click **Delete**.

   Restriction: You can only delete a single VM manager at a time.

Results

After the successful removal of the VM manager, all configuration entries and records are sent to the VM Manager Tool.

Testing connections to VM managers

You can test the connection to verify that the communication between the VM manager and the Software Use Analysis server is successful.

Before you begin

You must have the Manage VM Managers and Servers permission to perform this task.

About this task

When you test the connection, the Software Use Analysis server sends an action request to perform this task to the VM Manager Tool that is installed on the IBM Endpoint Manager server. When the request is submitted, the VM manager changes its status to **Testing the connection**.

Important: If you start the import during the process, the status of the VM manager is overwritten by the status that is received from the VM Manager Tool. Also, the status is set to **Pending** if the VM manager definition is modified. In such cases, repeat the connection test.

When you modify settings of the VM manager, the new information is saved and used during the connection test.

Procedure

1. In the top navigation bar, click **Management** > **VM Managers**.
2. Select the VM manager for which you want to test the connection.
3. Click **Test Connection**.

Results

A request to test the connection is submitted. It might take a few minutes for the Software Use Analysis server to receive the response. By default, the minimum time is 1 minute.

Important: Refresh the VM Managers panel to see the updated status. The status is changed either to **Connection test successful** or **Connection test failed**.

VM manager statuses

You can check the status of the last server operation on a VM manager in the VM Managers report view.

Information about the status of a VM manager is displayed in the **Operation status** column.

Tip: If you encounter any problems with VM managers, you can check the VM Manager Tool log files that are in the `<BES Client>\LMT\VMMAN\logs` directory.

VM manager statuses

OK
A VM manager is working properly.

Pending
A VM manager was not contacted to access its data yet. The status might be displayed after the VM manager is created or after its definition is modified.

Inactive
Data from a VM manager was not retrieved for a longer time. The status is displayed when the maximum allowed inactivity of a VM manager is exceeded.

Connection failed
Connecting to a VM manager failed and the data was not retrieved. Check the VM Manager Tool log files to determine the cause.

Hard timeout - suspended
Connecting to a VM manager failed because the provided URL is invalid or the configuration is incorrect. Provide a valid URL or reconfigure the VM manager to reestablish the connection. The status then changes to **Pending**.

Invalid credentials - attempting
Connecting to a VM manager failed because the credentials are incorrect or the password expired. It might also be the case that the administrator of a VM manager did not grant access for a given user. More attempts are made to check it. If the limit of attempts is exceeded, the status changes to **Invalid credentials – suspended**.

Invalid credentials - suspended
The connection to a VM manager is suspended because the invalid credentials might lead to blocking the account. Correct the credentials of a VM manager to resume the operation.

Duplicated address

The address of a VM manager is duplicated. The first address remains active and the status is displayed for the remaining ones. Delete the extra VM manager to ensure that data is gathered only once. The duplicated addresses might occur only within a particular VM manager type.

Unknown problem

The problem does not fall into other categories. Check the VM Manager Tool log files to determine the cause.

Testing the connection

A request to test the connection is submitted. It might take a few minutes for the Software Use Analysis server to receive the response. By default, the minimal waiting time is 1 minute. Refresh the VM manager panel to see the updated status. It can change either to **Connection test was successful** or **Connection test failed**.

Connection test was successful

The connection test for a VM manager completed successfully.

Connection test failed

The connection test for a VM manager failed. Check the VM Manager Tool log files to determine the cause.

Distributed virtual machines management

Centralized virtual machines management is the preferred approach to managing your virtual infrastructure. However, if a connection between your virtual machine manager and the IBM Endpoint Manager server is not possible, if you want to balance the network traffic between multiple VM Manager Tools, or apply the UUID-based virtual machine filtering, then choose the distributed approach and install the VM Manager Tool.

Restriction:

- In the distributed approach, the VM Manager Tool can be installed only on a computer on which the IBM Endpoint Manager client is already deployed.
- Centralized virtual machines management is the preferred method to manage virtual machines in your infrastructure.

Note: The data from the virtual topology provider can be correctly gathered by VM Manager Tools only when the direct connection from the VM Manager Tool to the virtual topology provider, for example VMware vCenter Server or KVM RHEV-M, can be established.

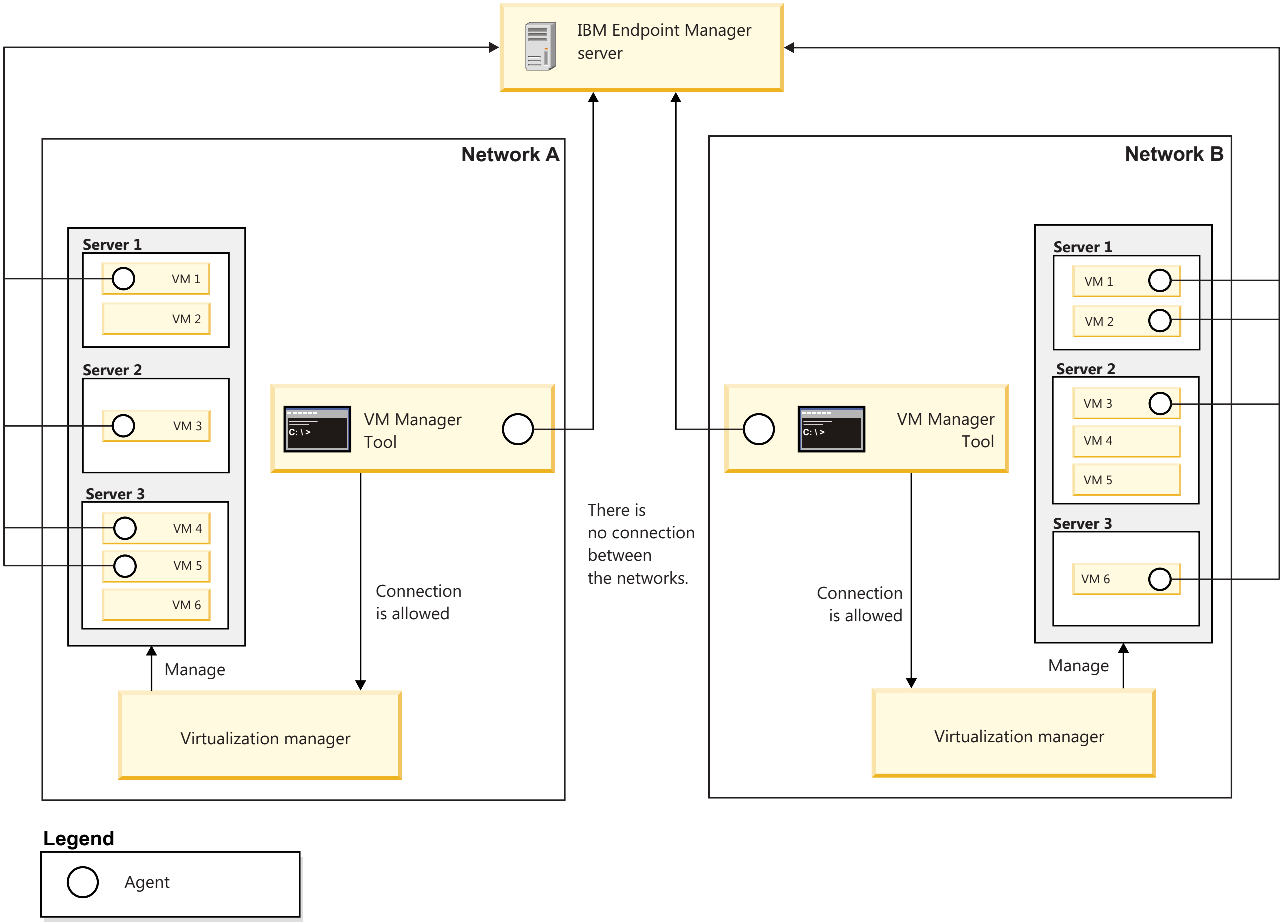
Deployment scenarios

Use the scattered approach if the direct connection between your virtual machine manager and the IBM Endpoint Manager server is not possible, if you want to balance the network traffic between multiple VM Manager Tools, or if you want to apply the UUID-based virtual machine filtering.

Scenario 1: At least one virtual machine manager is running in a separated network from which direct connection to the IBM Endpoint Manager server computer is not possible.

If you decide to use this solution instead of the functionality that is built into the centralized approach, you must choose at least one computer in each of your private networks on which the virtual agents are deployed. In a large virtual environment, you can install more than one VM Manager Tool within one network zone to balance the network traffic load.

Figure 1. Typical implementation



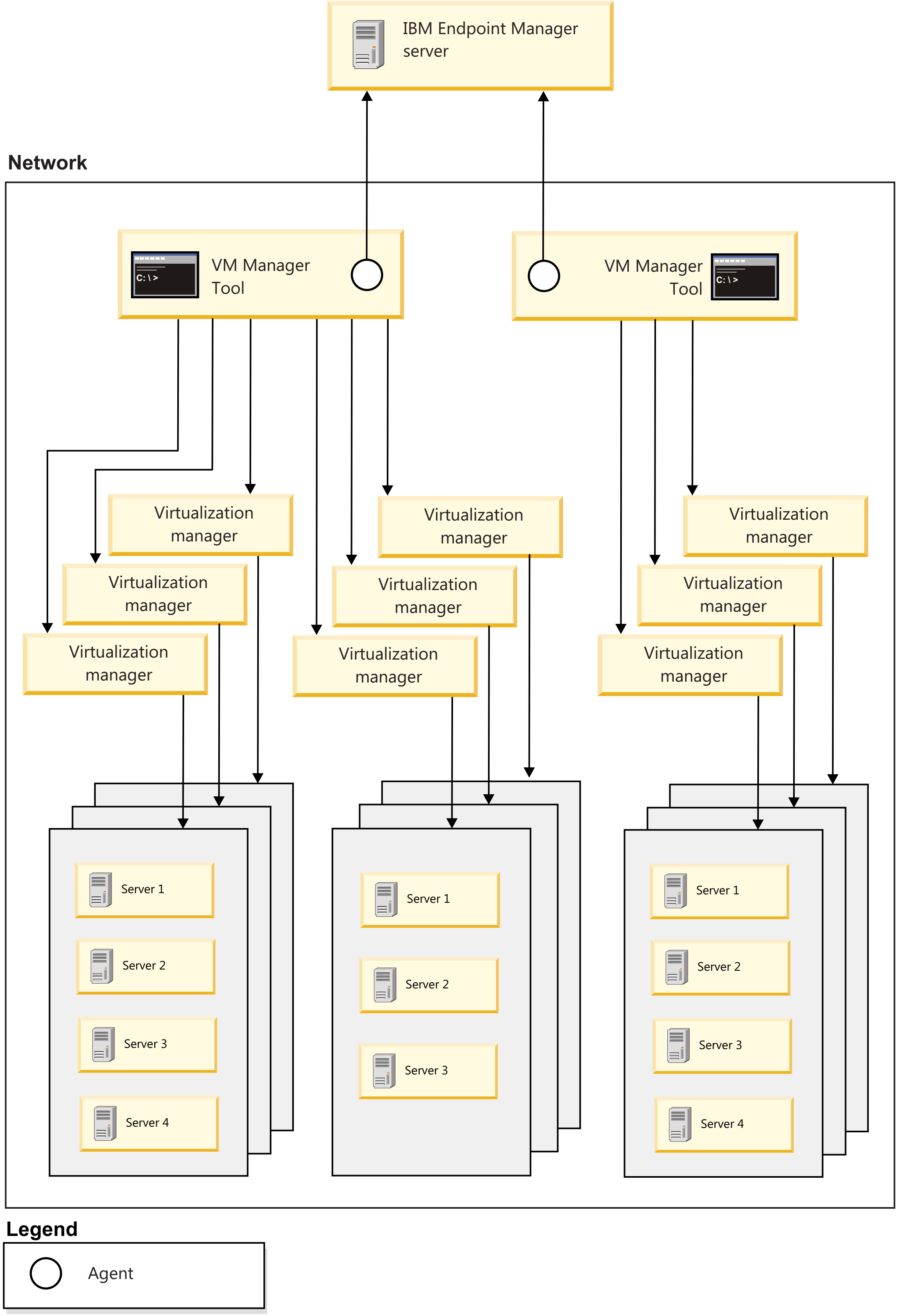
To install the VM Manager Tool, you need more disk space and hardware resources so it is a good idea to choose less busy or non-production computers.

Scenario 2: You want to balance the network traffic between multiple VM manager tools

Use this kind of the distributed approach solution when you want to balance the network traffic between multiple VM Manager Tools. Successful load balancing optimizes resource use, maximizes throughput, minimizes response time, and avoids overload.

Using multiple components with load balancing instead of a single component may increase reliability through redundancy. Load balancing is usually provided by dedicated software or hardware, such as a multilayer switch or a Domain Name System server Process.

Figure 2. Load-balancing example



Scenario 3: UUID-based virtual machine filtering

The purpose of filtering based on universally unique identifier (UUID) is to select only those virtual machines whose capacity and topology data is to be included in a final report. The VM manager has the function of matching UUIDs of selected guests. To stay compliant, all the necessary virtual machines units must be included in the report. When you enable UUID-based filtering all of the non-selected guests, empty hosts and clusters are removed.

Installing the VM Manager Tool

In centralized virtual machine management, the VM Manager Tool is automatically installed and configured on the IBM Endpoint Manager server. If the installation of the VM Manager Tool fails, or you use distributed virtual machine management, you must install the VM Manager Tool manually.

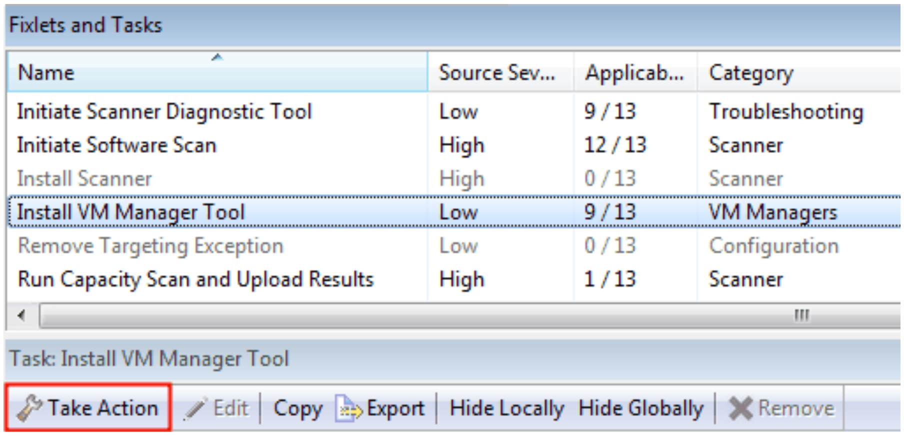
Before you begin

Important: If you see any discrepancies between the fixlets in your site and the fixlets described in the documentation, check the version of your fixlet site and update it if necessary.

- Review software requirements and other considerations
- Ensure that the IBM Endpoint Manager client is installed on the target endpoint.
- You must install and start Web Reports on your IBM Endpoint Manager server.
- Subscribe the target endpoint to the **IBM Endpoint Manager for Software Use Analysis v9** site.

Procedure

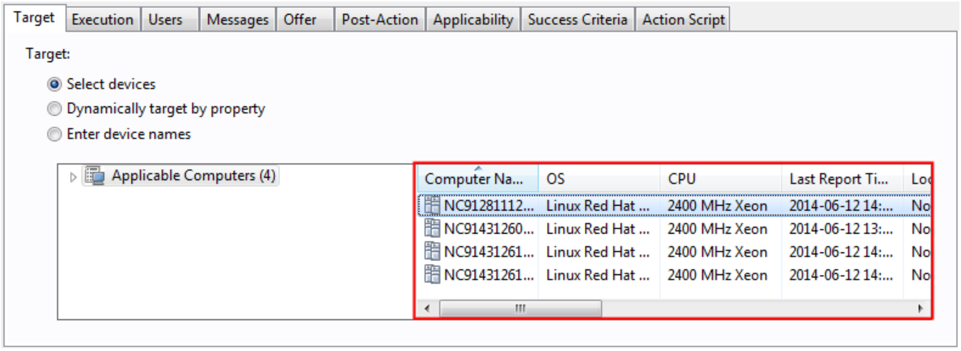
1. Log in to IBM Endpoint Manager console.
2. In the navigation tree, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.
3. In the upper right pane, select **Install VM Manager Tool**, and then in the lower pane, click **Take Action**.



Name	Source Sev...	Applicab...	Category
Initiate Scanner Diagnostic Tool	Low	9 / 13	Troubleshooting
Initiate Software Scan	High	12 / 13	Scanner
Install Scanner	High	0 / 13	Scanner
Install VM Manager Tool	Low	9 / 13	VM Managers
Remove Targeting Exception	Low	0 / 13	Configuration
Run Capacity Scan and Upload Results	High	1 / 13	Scanner

4. To select a computer on which you want to install the VM Manager Tool, click the **Target** tab, and then click the computer name. Then, click **OK**.

   Important: Select only a computer on which the IBM Endpoint Manager server is installed.



Target:

● Select devices
○ Dynamically target by property
○ Enter device names

Applicable Computers (4)

Computer Na...	OS	CPU	Last Report Ti...	Lo
NC91281112...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No
NC91431260...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 13:...	No
NC91431261...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No
NC91431261...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No

What to do next

When the installation of the VM Manager Tool is complete, you must upload the VM Manager Tool scan results.

VM Manager Tool installation requirements:

Ensure that you fulfill all software requirements to install the VM Manager Tool.

Supported operating systems

Table 2. Requirements for installing VM Manager Tool.

Operating system	Version	Software requirements
Linux	Red Hat Enterprise Linux for Intel/AMD x86 (32 and 64-bit) **versions 5 and 6**	`unzip` `glibc library` 2.4 or higher
	Red Hat Linux Desktop for Intel/AMD x86 (32 and 64-bit) **versions 5 and 6**	
	SUSE Linux Enterprise Server for Intel/AMD x86 (32 and 64-bit) **versions 10 and 11**	
	SUSE Linux Enterprise Desktop for Intel/AMD x86 (32 and 64-bit) **versions 10 and 11**	
Windows	**Server 2012** Standard and Datacenter (64-bit)	
	Server 2008 R2 Standard, Enterprise and Datacenter (64-bit)	
	Server 2008 Standard and Enterprise (32 and 64-bit)	
	Server 2003 R2 (32 and 64-bit)	
	Server 2003 Datacenter, Enterprise and Standard Edition (32 and 64-bit)	
	8 Ultimate, Professional (32 and 64-bit)	
	7 Ultimate, Enterprise and Professional (32 and 64-bit)	
	Vista Ultimate, Enterprise and Business (32 and 64-bit)	

Required free disk space

The VM Manager Tool requires **250 MB** of disk space.

Other requirements

Web Reports must be installed and running on the IBM Endpoint Manager server when the VM managers function is running.

Uploading the VM Manager Tool scan results

Upload the VM Manager Tool scan results to calculate processor value unit (PVU) and resource value unit (RVU) capacity, and to maintain license compliance for the purposes of software audit reports.

Before you begin

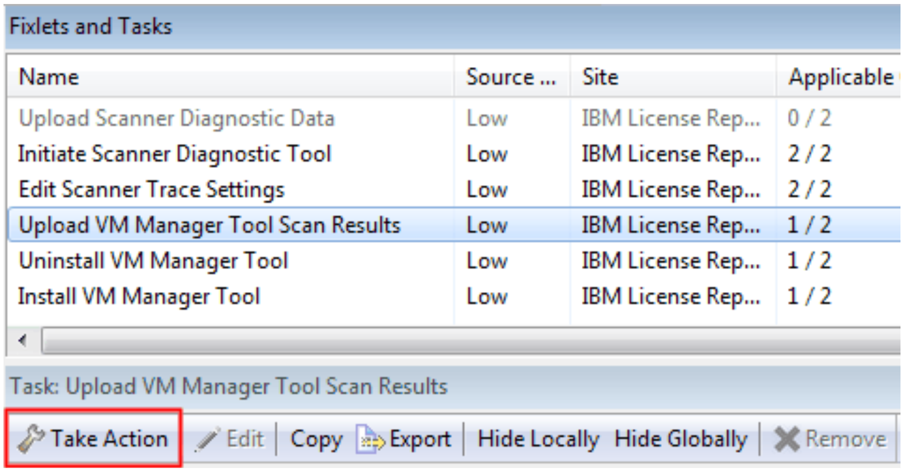
Important: If you see any discrepancies between the fixlets in your site and the fixlets described in the documentation, check the version of your fixlet site and update it if necessary.

- Ensure that the VM Manager Tool is installed.
- Ensure that the IBM Endpoint Manager client is installed on the target endpoint.
- Subscribe the target endpoint to the **IBM Endpoint Manager for Software Use Analysis v9** site.

Note: Uploading of a scan of the VM Manager Tool that is installed on IBM Endpoint Manager server using the centralized approach is scheduled automatically. If the tool was not installed automatically during Software Use Analysis first initialization, you must manually activate the upload of data after manual tool installation.

Procedure

1. Log in to IBM Endpoint Manager console.
2. In the navigation bar, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.
3. In the upper right pane, select **Upload VM Manager Tool Scan Results**, and then in the lower pane, click **Take Action**.



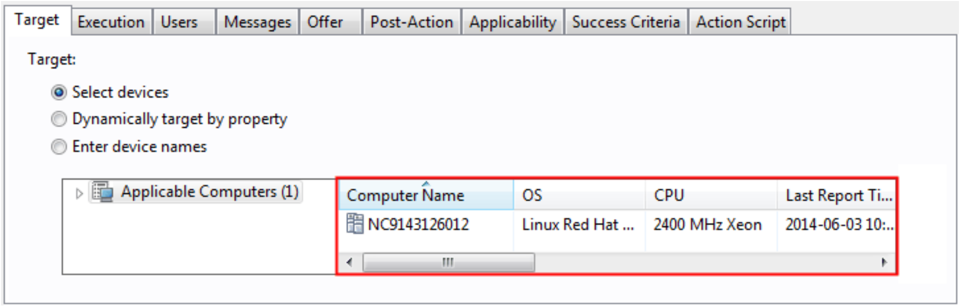
Fixlets and Tasks

Name	Source ...	Site	Applicable
Upload Scanner Diagnostic Data	Low	IBM License Rep...	0 / 2
Initiate Scanner Diagnostic Tool	Low	IBM License Rep...	2 / 2
Edit Scanner Trace Settings	Low	IBM License Rep...	2 / 2
Upload VM Manager Tool Scan Results	Low	IBM License Rep...	1 / 2
Uninstall VM Manager Tool	Low	IBM License Rep...	1 / 2
Install VM Manager Tool	Low	IBM License Rep...	1 / 2

Task: Upload VM Manager Tool Scan Results

4. To select a computer from which you want to upload VM Manager Tool scan results, click the **Target** tab, and then click the computer. Then, click **OK**.

   Important: The only applicable computer should be the computer on which the IBM Endpoint Manager server is installed.



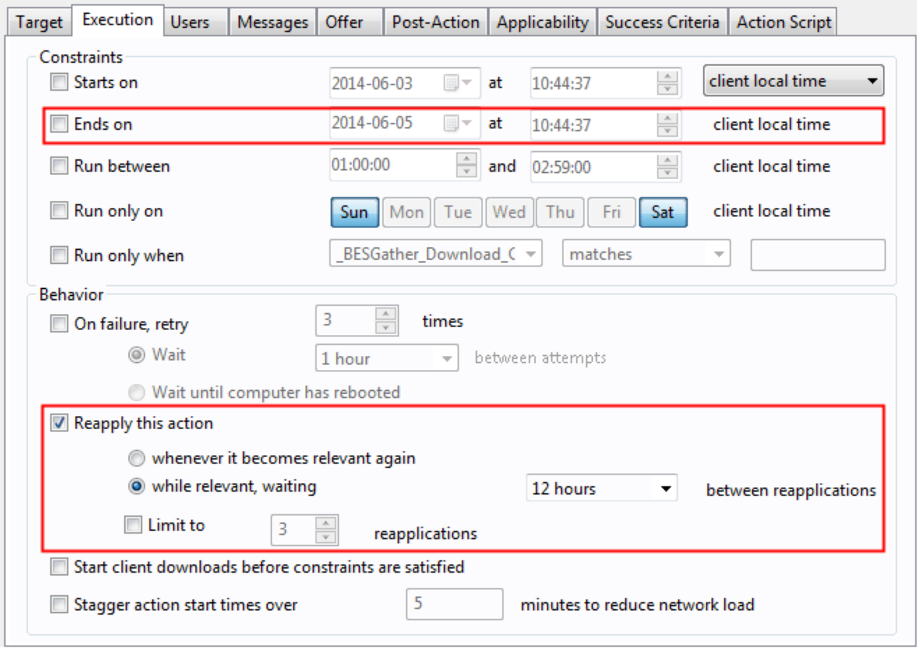
Target:

● Select devices
○ Dynamically target by property
○ Enter device names

Applicable Computers (1)

Computer Name	OS	CPU	Last Report Ti...
NC9143126012	Linux Red Hat ...	2400 MHz Xeon	2014-06-03 10:...

5. Click the **Execution** tab to schedule regular uploads of the scan results:
   a. Clear the **Ends on** check box so that the action does not have the end date.
   b. Select the **Reapply this action** check box and set the **while relevant, waiting** option to 12 hours.
   c. Clear the **Limit to 3 reapplications** check box.



Constraints

□ Starts on 2014-06-03 at 10:44:37 client local time
□ Ends on 2014-06-05 at 10:44:37 client local time
□ Run between 01:00:00 and 02:59:00 client local time
□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time
□ Run only when _BESGather_Download_(matches

Behavior

□ On failure, retry 3 times
● Wait 1 hour between attempts
○ Wait until computer has rebooted
☑ Reapply this action
○ whenever it becomes relevant again
● while relevant, waiting 12 hours between reapplications
□ Limit to 3 reapplications
□ Start client downloads before constraints are satisfied
□ Stagger action start times over 5 minutes to reduce network load

Adding VM managers

Add a connection to a VM manager to retrieve the virtual capacity scan data. You configure a connection to a single VM manager by creating and editing its configuration file in which you specify the web address of the VM manager, its type, and the user name and password that are used to access it.

Procedure

1. Navigate to the `<BES Client>\LMT\VMMAN\config` directory.
2. Create a VM manager configuration file by copying the `vmmconf_template.properties` file and renaming it, for example, to `vmmconf_VM1.properties`.

Attention: Each time you create a VM manager configuration file, use the `vmmconf_template.properties` file as a template. Do not copy and edit configuration files that you previously created for a different VM manager. After you run the configuration file for the first time, an ID is generated for a VM manager. Each ID must be unique. When you copy and edit an existing configuration file, the ID is duplicated.

3. Edit the file and specify the following parameters:

   vmm_url
   Specify the web address of the VM manager. You can specify either a full URL or only the host name or IP address, for example, `http://192.0.2.0/wsman`.

   vmm_type
   Specify the type of the VM manager. The possible values are `VMWARE_V_SPHERE`, `MICROSOFT_HYPER_V`, or `KVM_RHEV_M`.

   vmm_login
   Specify the user name that is used to access the VM manager.

   vmm_password
   Specify the password that is used to access the VM manager. The password is encrypted and saved when you load the configuration files.

4. Save the configuration file.
5. Repeat the procedure for each new connection to a VM manager.
6. By default, the VM Manager Tool is installed and run as a system service. Use the **`-reloadconfig`** command to load a new configuration file and make it visible to the VM Manager Tool.

VM Manager Tool

VM Manager Tool is used to collect information that concerns physical and virtual machines that are installed in your IT infrastructure. The information is referred to as virtualization infrastructure capacity data and is required to calculate the processor value units (PVU), resource value units (RVU) and to maintain license compliance. It is needed for the purposes of software audit reports.

VM Manager Tool is installed automatically within the Software Use Analysis server configuration. It is installed on the IBM Endpoint Manager server. You must have the Endpoint Manager client installed on that computer.

Note: Information that is contained in this section is useful only for the distributed virtual machines management. In case of the centralized approach, the VM Manager Tool is installed and configured automatically. If you are using only the centralized approach, refer to this section for problem determination purposes.

Installing the VM Manager Tool

In centralized virtual machine management, the VM Manager Tool is automatically installed and configured on the IBM Endpoint Manager server. If the installation of the VM Manager Tool fails, or you use distributed virtual machine management, you must install the VM Manager Tool manually.

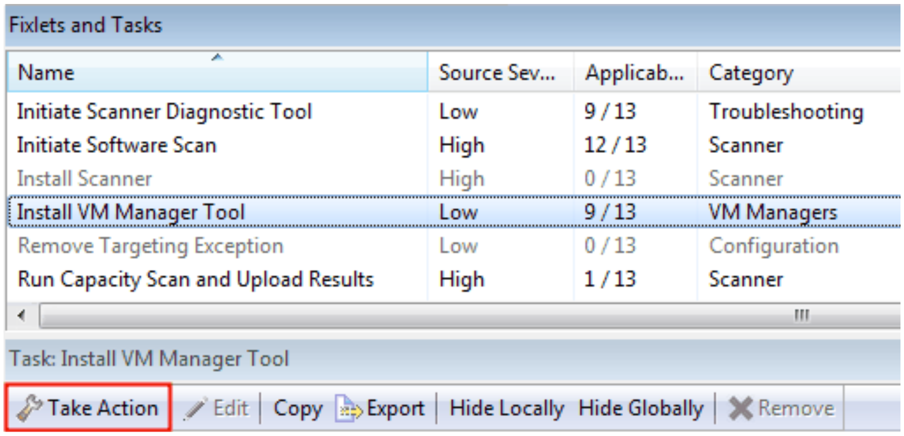
Before you begin

Important: If you see any discrepancies between the fixlets in your site and the fixlets described in the documentation, check the version of your fixlet site and update it if necessary.

- Review software requirements and other considerations
- Ensure that the IBM Endpoint Manager client is installed on the target endpoint.
- You must install and start Web Reports on your IBM Endpoint Manager server.
- Subscribe the target endpoint to the **IBM Endpoint Manager for Software Use Analysis v9** site.

Procedure

1. Log in to IBM Endpoint Manager console.
2. In the navigation tree, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.
3. In the upper right pane, select **Install VM Manager Tool**, and then in the lower pane, click **Take Action**.



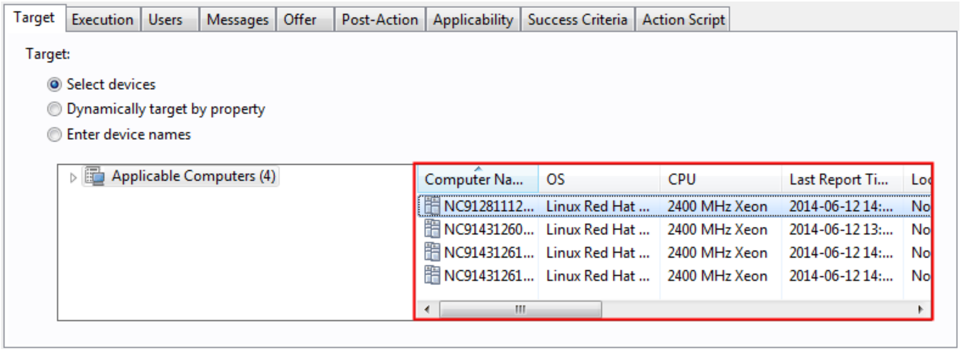
Fixlets and Tasks

Name	Source Sev...	Applicab...	Category
Initiate Scanner Diagnostic Tool	Low	9 / 13	Troubleshooting
Initiate Software Scan	High	12 / 13	Scanner
Install Scanner	High	0 / 13	Scanner
Install VM Manager Tool	Low	9 / 13	VM Managers
Remove Targeting Exception	Low	0 / 13	Configuration
Run Capacity Scan and Upload Results	High	1 / 13	Scanner

Task: Install VM Manager Tool

4. To select a computer on which you want to install the VM Manager Tool, click the **Target** tab, and then click the computer name. Then, click **OK**.

   Important: Select only a computer on which the IBM Endpoint Manager server is installed.



Target:

● Select devices
○ Dynamically target by property
○ Enter device names

Applicable Computers (4)

Computer Na...	OS	CPU	Last Report Ti...	Lo
NC91281112...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No
NC91431260...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 13:...	No
NC91431261...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No
NC91431261...	Linux Red Hat ...	2400 MHz Xeon	2014-06-12 14:...	No

What to do next

When the installation of the VM Manager Tool is complete, you must upload the VM Manager Tool scan results.

VM Manager Tool installation requirements:

Ensure that you fulfill all software requirements to install the VM Manager Tool.

Supported operating systems

Table 3. Requirements for installing VM Manager Tool.

Operating system	Version	Software requirements
Linux	Red Hat Enterprise Linux for Intel/AMD x86 (32 and 64-bit) **versions 5 and 6**	`unzip` `glibc library` 2.4 or higher
	Red Hat Linux Desktop for Intel/AMD x86 (32 and 64-bit) **versions 5 and 6**	
	SUSE Linux Enterprise Server for Intel/AMD x86 (32 and 64-bit) **versions 10 and 11**	
	SUSE Linux Enterprise Desktop for Intel/AMD x86 (32 and 64-bit) **versions 10 and 11**	
Windows	**Server 2012** Standard and Datacenter (64-bit)	
	Server 2008 R2 Standard, Enterprise and Datacenter (64-bit)	
	Server 2008 Standard and Enterprise (32 and 64-bit)	
	Server 2003 R2 (32 and 64-bit)	
	Server 2003 Datacenter, Enterprise and Standard Edition (32 and 64-bit)	
	8 Ultimate, Professional (32 and 64-bit)	
	7 Ultimate, Enterprise and Professional (32 and 64-bit)	
	Vista Ultimate, Enterprise and Business (32 and 64-bit)	

Required free disk space

The VM Manager Tool requires **250 MB** of disk space.

Other requirements

Web Reports must be installed and running on the IBM Endpoint Manager server when the VM managers function is running.

Checking the VM Manager Tool version details

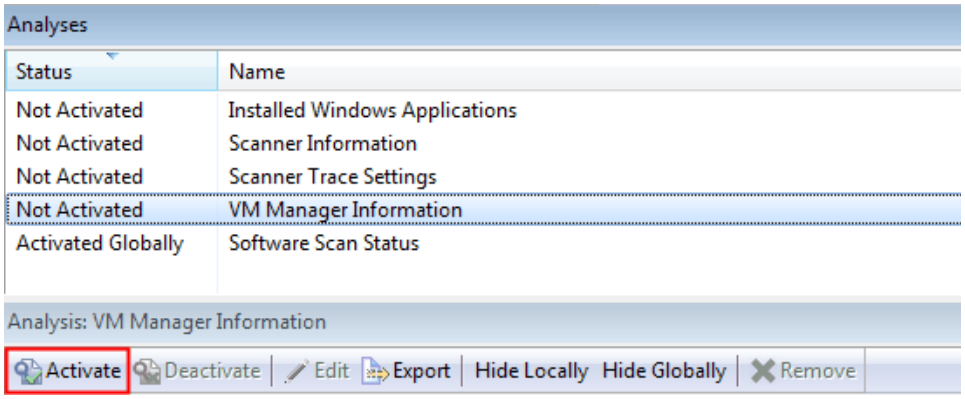
Activate the **VM Manager Information** analysis to retrieve data about the installed version of the VM Manager Tool. You can use the analysis to quickly confirm the successful installation of the tool.

About this task

The **VM Manager Information** analysis returns information for two properties, `VMMAN_Tool_Version` that specifies the installed version of the VM Manager Tool, and `Build_Version` that shows the details of the build. If the VM Manager Tool is not installed on the target endpoint, the analysis reports this information.

Procedure

1. Log in to IBM Endpoint Manager console.
2. In the navigation bar, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Analyses**.
3. In the upper-right pane, select **VM Manager Information**, and then in the lower pane, click **Activate**.



Analyses

Status	Name
Not Activated	Installed Windows Applications
Not Activated	Scanner Information
Not Activated	Scanner Trace Settings
Not Activated	VM Manager Information
Activated Globally	Software Scan Status

Analysis: VM Manager Information

4. After you activate the analysis, go to the Results tab. The information about the version and the build is available next to the name of the applicable computer.

Uploading the VM Manager Tool scan results

Upload the VM Manager Tool scan results to calculate processor value unit (PVU) and resource value unit (RVU) capacity, and to maintain license compliance for the purposes of software audit reports.

Before you begin

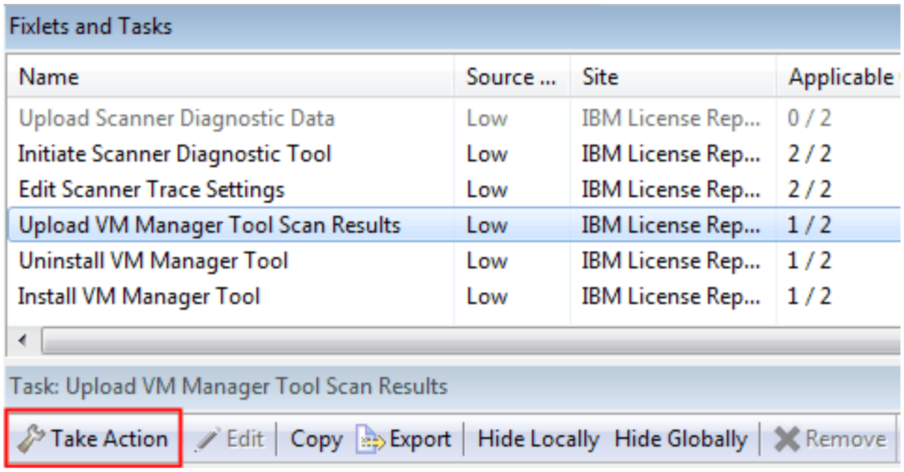
Important: If you see any discrepancies between the fixlets in your site and the fixlets described in the documentation, check the version of your fixlet site and update it if necessary.

- Ensure that the VM Manager Tool is installed.
- Ensure that the IBM Endpoint Manager client is installed on the target endpoint.
- Subscribe the target endpoint to the **IBM Endpoint Manager for Software Use Analysis v9** site.

Note: Uploading of a scan of the VM Manager Tool that is installed on IBM Endpoint Manager server using the centralized approach is scheduled automatically. If the tool was not installed automatically during Software Use Analysis first initialization, you must manually activate the upload of data after manual tool installation.

Procedure

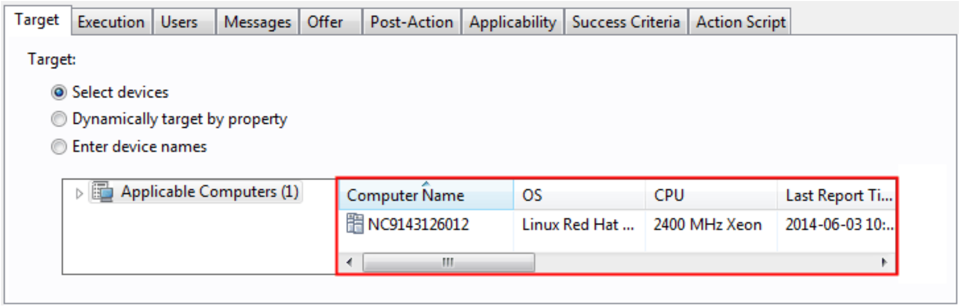
1. Log in to IBM Endpoint Manager console.
2. In the navigation bar, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.
3. In the upper right pane, select **Upload VM Manager Tool Scan Results**, and then in the lower pane, click **Take Action**.



Name	Source ...	Site	Applicable
Upload Scanner Diagnostic Data	Low	IBM License Rep...	0 / 2
Initiate Scanner Diagnostic Tool	Low	IBM License Rep...	2 / 2
Edit Scanner Trace Settings	Low	IBM License Rep...	2 / 2
Upload VM Manager Tool Scan Results	Low	IBM License Rep...	1 / 2
Uninstall VM Manager Tool	Low	IBM License Rep...	1 / 2
Install VM Manager Tool	Low	IBM License Rep...	1 / 2

4. To select a computer from which you want to upload VM Manager Tool scan results, click the **Target** tab, and then click the computer. Then, click **OK**.

   Important: The only applicable computer should be the computer on which the IBM Endpoint Manager server is installed.



Target:

● Select devices

○ Dynamically target by property

○ Enter device names

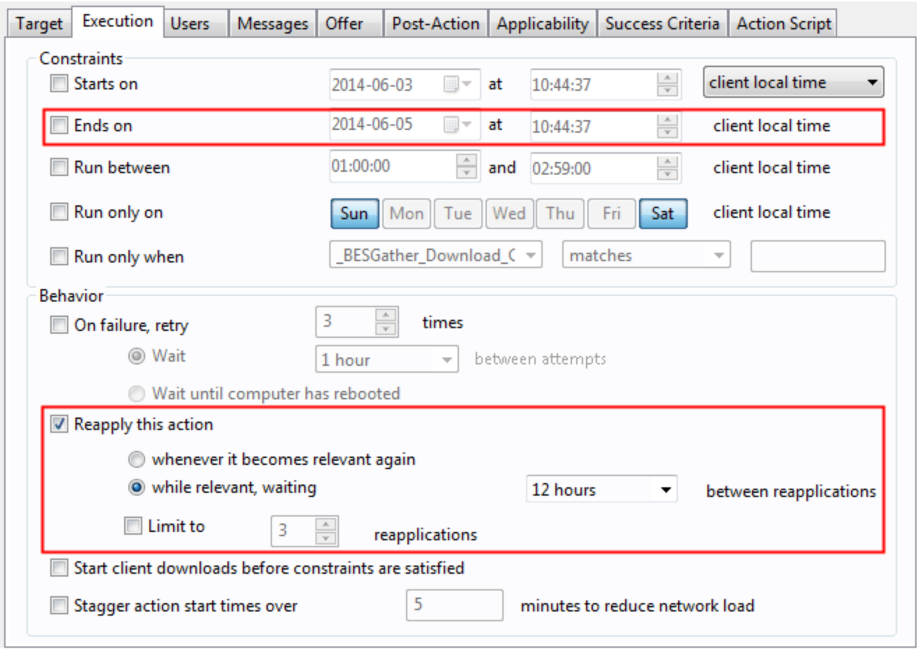
Computer Name	OS	CPU	Last Report Ti...
NC9143126012	Linux Red Hat ...	2400 MHz Xeon	2014-06-03 10:...

5. Click the **Execution** tab to schedule regular uploads of the scan results:

   a. Clear the **Ends on** check box so that the action does not have the end date.

   b. Select the **Reapply this action** check box and set the **while relevant, waiting** option to 12 hours.

   c. Clear the **Limit to 3 reapplications** check box.



Constraints

□ Starts on 2014-06-03 at 10:44:37 client local time

□ Ends on 2014-06-05 at 10:44:37 client local time

□ Run between 01:00:00 and 02:59:00 client local time

□ Run only on Sun Mon Tue Wed Thu Fri Sat client local time

□ Run only when _BESGather_Download_C matches

Behavior

□ On failure, retry 3 times

○ Wait 1 hour between attempts

○ Wait until computer has rebooted

☑ Reapply this action

○ whenever it becomes relevant again

● while relevant, waiting 12 hours between reapplications

□ Limit to 3 reapplications

□ Start client downloads before constraints are satisfied

□ Stagger action start times over 5 minutes to reduce network load

Configuring VM Manager Tool

You can modify the global settings of the VM Manager Tool, settings of a single VM manager, or the log settings.

Global configuration:

You can configure the main configuration settings (global scope) of the VM Manager Tool by editing the `vmmainconf.properties` file that is stored in the `<BES Client>\LMT\VMMAN\config` directory.

Important: The following content applies only to the distributed virtual machines management. For the centralized approach, any changes to the configuration files are overwritten during the next action performed on the VM managers.

Table 4. Global configuration parameters

Parameter	Unit	Default	Minimum	Maximum
vmm_polling_time_interval Specifies the interval between the consecutive retrievals of data from VM managers.	Minutes	30	30	10080 (1 week)
vmm_connection_timeout Specifies the time after which the connection with a VM manager is ended.	Seconds	90	10	3600 (1 hour)
vmm_thread_pool_size Specifies the number of threads in thread pool that is used for connections to VM managers.	Number	10	1	50
vmm_data_transfer_period Determines how often the scan data is transferred to the agent to be uploaded to the server if subsequent scans have the same results.	Minutes	720	0	10080

Table 4. Global configuration parameters (continued)

Parameter	Unit	Default	Minimum	Maximum
`check_vm_managers_uniqueness` Distinguishes unique VM managers from duplicates.	Boolean (true/false)	True		
`uuid_filtering_enabled` Enables UUID filtering.	Boolean (true/false)	False		
`vmm_rmi_ssl_port` Specifies the number of the port that connects to the server when you enter the *reload configuration* and *stop* commands.	Number	25001		
`vmm_max_subsequent_login_failures` Specifies the maximum number of failed attempts of logging in to the VM manager.	Number	3	0	100

VM manager configuration:

You can configure VM manager settings by editing the VM manager configuration files. Each file represents a separate VM manager and includes its connection settings. All of the configuration files are read when you start the VM Manager Tool. The administrator of the VM Manager Tool must create a configuration file for each VM manager connection to be configured. The accepted mask of the VM manager configuration file is `vmconf_`*`vm_manager_name`*`.properties`, where *vm_manager_name* is the name of the VM manager that is configured by the file.

Important: The following content applies only to the distributed virtual machines management. For the centralized approach, any changes to the configuration files are overwritten during the next action performed on the VM managers.

Table 5. VM manager configuration parameters

	Unit	Default	Minimum	Maximum
Parameter	**Description**			
vmm_url	Web address (URL)			
	Specifies the web address of the VM manager. You can provide either a full URL, a partial URL, or only a host name or IP address. In the second case, the full address of the VM manager is built based on the selected type of the VM manager and protocol (if specified). Https protocol is used by default. If you specify only the addresses, the defaults are used: • https://*virtualcenter*/sdk for VMWARE_V_SPHERE • https://*hyper-v*/wsman for MICROSOFT_HYPER_V • https://*rhev-m:8443*/api for KVM_RHEV_M If you do not specify the complete URL but only a protocol, or a port, or a context path, the URL is built based on the following defaults: • VMWARE_V_SPHERE - default protocol https, port 443 (for https) or 80 (for http), context path - sdk • KVM_RHEV_M - default protocol https, port 8443 (for https) or 8080 (for http), context path - api • MICROSOFT_HYPER_V - default protocol https, port 443 (for https) or 80 (for http), context path - wsman If the URL contains the name of a VM manager, the name is resolved to an IP address. However, the full URL, including a port number, is used by the server to identify the VM manager. Each VM manager must have a different web address, that is, only one entry is allowed for a particular URL. If two or more configuration files duplicate the URL address, only the first file is treated as valid. The remaining files are ignored.			
vmm_type	Characters			
	Specifies the type of VM manager. The possible values are: • VMWARE_V_SPHERE • MICROSOFT_HYPER_V • KVM_RHEV_M			
vmm_login	Characters			
	Specifies the user name that is used to access the VM manager.			
vmm_password	Characters			
	Specifies the password that is used to access the VM manager. A password that is entered in plain text is immediately encrypted and saved while the configuration files are loaded.			
vmm_max_subsequent_login_failures	Integer	3	0	100
	Specifies the maximum number of failed attempts of logging in to the VM manager. If you set the value of this parameter to 0, an unlimited number of attempts is allowed. If the specified number of failed attempts is exceeded, the VM Manager Tool does not connect to this VM manager and the parameter *vmm_communication_locked* is set to *true*.			

Table 5. VM manager configuration parameters (continued)

Parameter	Unit	Default	Minimum	Maximum
	Description			
vmm_communication_locked	True/false	False		
	Indicates whether the connection to the VM manager is locked. The possible values are: **true** Disables the connection to the VM manager but keeps the configuration file. If the number of failed logging attempts that is specified in the **vmm_max_subsequent_login_failures** parameter is exceeded, the value of the **vmm_communication_locked** parameter is automatically set to `true`. **false** Unlocks communication with the VM manager and resets the count of the subsequent failed logging attempts.			
vmm_get_cluster_info_with_shared_credentials	True/false	False		
	Indicates whether the same credentials can be used to connect to every host in the same cluster. You can use this parameter only for Microsoft Hyper-V. The possible values are: **true** Uses the same credentials to get information about all other hosts in the same cluster. **false** Set when credentials for every host in the cluster are different. Each host in the same Hyper-V cluster requires a separate configuration file.			

Log files:

You can gather the log files to determine the problems that are related to the VM Manager Tool. You can also change the log settings.

The log files for the VM Manager Tool are in the following directories:

- Trace log files: `<BES Client>\LMT\VMMAN\logs`
- Installation log files: `<BES Client>\LMT\VMMAN\logs\install`

You can also gather the complete set of logs by running the **-retrievedebugdata** command in VM Manager Tool.

Log settings

You can change the log settings by editing the `log4j.properties` file. The following parameters are the most useful:

- **log4j.appender.mylogger.maxFileSize** specifies the maximum size of a log file

  Default value = 1000 KB
- **log4j.appender.mylogger.MaxBackupIndex** specifies the maximum number of log files

  Default value = 10

UUID-based virtual machine filtering:

The purpose of filtering based on universally unique identifier (UUID) is to select only those virtual machines whose capacity and topology data is to be included in a final report. VM manager has the function of matching UUIDs of selected guests. To stay compliant, enough virtual machines units must be included in the report. When you enable UUID-based filtering, all of the non-selected guests, empty hosts and clusters are removed.

Important: The UUID-based filtering can be enabled only for the distributed virtual machines management.

Enabling UUID-based virtual machine filtering:

The `uuid_filtering_enabled` parameter is set by default to `false`. You must set it to `true` before you can select virtual machines to be included in a final report.

Procedure

1. To enable filtering of UUIDs of selected guests, go to the `<BES Client>\LMT\VMMAN\config` directory, and open the `vmmainconf.properties` file.
2. Set the `uuid_filtering_enabled` property to `true`.

What to do next

You can disable filtering by setting the `uuid_filtering_enabled` property to `false`.

Selecting virtual machines for UUID-based filtering:

You can select guests whose data is to be included in the generated report by putting their UUIDs in the `vmmfilterconf.properties` file.

Procedure

1. Optional: Obtain the list of virtual machines UUIDs by running the `select distinct uuid from ADM.VIRTUAL_VM_UUID` SQL query. For more information, see the topic Obtaining the list of virtual machine UUIDs.
2. In the `<BES Client>\LMT\VMMAN\config` directory, open the `vmmfilterconf.properties` file.
3. Add the UUIDs for the guests that you want to include in your report. During filter matching, the VM manager removes any white space characters and hyphens (-). All letters are also converted to uppercase.

Example

All of these entries are valid:

- `5030a6eb-485a-35b5-0fa0-a8bc4a459c9d`
- `564da050-7b20-8754-b578-e8437da8653e`
- `564D1E0d4C0CE65B8A54203D7E032D2B`

What to do next

Run the following command to load the list of UUIDs that you configured:

- Linux **`vmman.sh -reloadconfig`**
- Windows **`vmman.bat -reloadconfig`**

Obtaining the list of virtual machine UUIDs:

You can use the list of virtual machine UUIDs that are currently connected to the Software Use Analysis server to select guests for data retrieval. This data can be included in the generated report.

About this task

You can find all of the virtual machine UUIDs that are currently connected to the Software Use Analysis server in the `ADM.VIRTUAL_VM_UUID` table in the SUADB database. You can extract the complete list of UUIDs and then remove those UUIDs that should not be included in the report.

Procedure

1. Log in as `tlmsrv` user or a user with the DBADM access to the database.
2. To obtain the list of virtual machines UUIDs, enter the following commands in the system command line:
   ```
   db2 connect to SUADB
   db2 "select distinct uuid from ADM.VIRTUAL_VM_UUID" >out.txt
   ```
   Note: The default name for the database is `SUADB`. Change it if you named your database differently.

Results

The list is now stored in the `out.txt` file.

What to do next

Remove the unnecessary UUIDs from the `out.txt` file and copy the remaining UUIDs to the `vmmfilterconf.properties` file.

Running the VM Manager Tool

You can use the VM Manager Tool to retrieve data about the virtualization infrastructure capacity. The data is then transferred to the Software Use Analysis server and merged with software scan data that is gathered from the IBM Endpoint Manager clients that are installed in the virtualization environment.

About this task

To see a list of options that you can use while you run the VM Manager Tool, see: Command-line options for VM Manager Tool.

Procedure

To run the VM Manager Tool, use the following scripts.

Note: The Administrator or root privileges are required if you want to **`install`**, **`remove`**, or **`run`** the VM Manager Tool.

- Windows `vmman.bat`
- Linux `vmman.sh`

Command-line options for the VM Manager Tool:

You can use different options of the VM Manager Tool to encrypt your password, test connection, and reload the configuration.

The following table provides a list of command-line options that you can use when you run the VM Manager Tool. If you run the application without specifying any options, the help screen is displayed by default.

Option	Description	Example
`-help`	Displays the help screen. It is the default option when no other option is specified.	
`-install`	Installs VM Manager Tool as a system service. **Important:** You must have the administrative or root privileges to use this option. Windows The installation logs are in the directory: `<BES Client>\LMT\VMMAN\logs\install`.	Linux `vmman.sh -install` Windows `vmman.bat -install`
`-passwd passwordString -config` *`file_path`*	Encrypts a password for the VM manager that is defined in the file that is specified in the *config* parameter.	Linux `vmman.sh -passwd newPassword -config ./config/vmconf_vmmanager3.properties` Windows `vmman.bat -passwd newPassword -config config\vmconf_vmmanager3.properties`
`-reloadconfig`	Reloads all configuration files and updates the parameters in the memory of VM Manager Tool. You can use this option only if VM Manager Tool runs as a system service. **Tip:** Use this option each time a new VM manager connection is defined to load the newly created configuration.	Linux `vmman.sh -reloadconfig` Windows `vmman.bat -reloadconfig`
`-remove`	Removes VM Manager Tool from the service registry. **Important:** You must have the administrative or root privileges to use this option. Windows The removal logs are in the directory: `<BES Client>\LMT\VMMAN\logs\install`.	Linux `vmman.sh -remove` Windows `vmman.bat -remove`
`-retrievedebugdata`	Collects debug information from all defined VM Managers and stores it in the `debugData.zip` file that is in the main the VM Manager Tool directory. The collected information includes: • Configuration files • Log files • Network communication log files • Data collected from VM Managers • Status of all VM Managers	Linux `vmman.sh -retrievedebugdata` Windows `vmman.bat -retrievedebugdata`
`-run`	Starts the VM Manager Tool in service mode. In this mode, data is collected for all defined VM managers repeatedly at the interval that is set in the **`vmm_polling_time_interval`** parameter. To use this option, you must install VM Manager Tool as a system service. **Important:** Windows You must have the administrative privileges to use this option.	Linux `vmman.sh -run` Windows `vmman.bat -run`

Option	Description	Example
-runonce [-config *file_path*]	Collects data from all defined VM managers once and exits the VM Manager Tool. To collect data from a particular VM manager, use the -config *file_path* option, where *file_path* is a full or relative path to the configuration file of the VM manager that you want to collect data from.	Linux vmman.sh -runonce -config ./config/vmconf_vmmanager1.properties Windows vmman.bat -runonce -config config\vmconf_vmmanager1.properties
-status [-config *file_path*]	Displays the operation status for all VM managers. If the file path is specified, the operation status for the particular VM manager is displayed. To see the information about all the operation statuses, refer to the topic VM Manager Tool statuses.	Linux vmman.sh -status -config ./config/vmconf_vmmanager4.properties Windows vmman.bat -status -config config\vmconf_vmmanager4.properties
-stop	Stops VM Manager Tool that was started as a system service.	Linux vmman.sh -stop Windows vmman.bat -stop
-testconnection [-config *file_path*]	Tests connections to all defined VM managers. To collect data from a particular VM manager, use the -config *file_path* option, where *file_path* is a full or relative path to the configuration file of the VM manager that you want to collect data from.	Linux vmman.sh -testconnection -config ./config/vmconf_vmmanager2.properties Windows vmman.bat -testconnection -config config\vmconf_vmmanager2.properties

Uninstalling the VM Manager Tool

Follow the procedure to uninstall the VM Manager Tool from the endpoints and to delete all the related settings and folders. Uninstallation of the VM Manager Tool is also required if you want to reinstall the tool.

Before you begin

Important: If you see any discrepancies between the fixlets in your site and the fixlets described in the documentation, check the version of your fixlet site and update it if necessary.

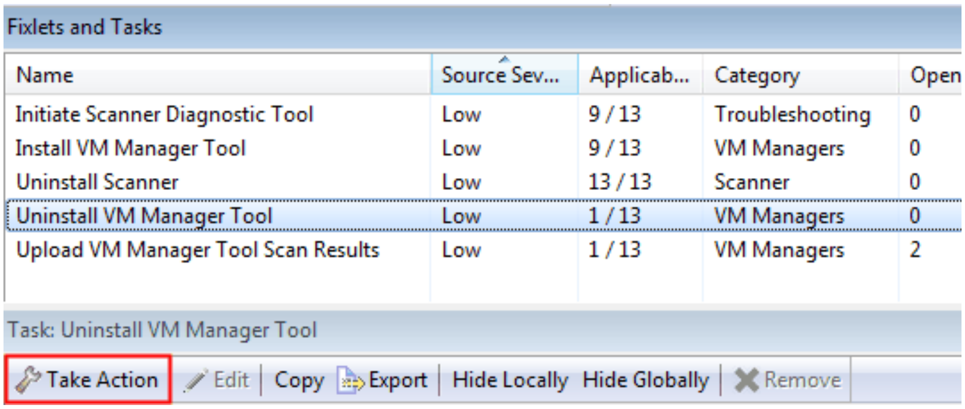
- Ensure that the IBM Endpoint Manager server and client are installed on the target endpoint.
- Subscribe the target endpoint to the **IBM Endpoint Manager for Software Use Analysis v9** site.

Note: If the target endpoint is not on the list of applicable computers in the IBM Endpoint Manager console, it means that the task is non-relevant for this endpoint. The reason for it could be that the tool is not installed. Additionally, a non-relevant task could mean that the console does not have up-to-date information. To refresh the endpoint status, perform the following steps:

1. Access the subscribed computers: in the left tree click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Subscribed Computers**.
2. Right-click the endpoint on the list of computers, click **Send refresh**, and then wait for the task to show the new status.

Procedure

1. On the navigation bar of the IBM Endpoint Manager console, click **Sites** > **External** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.
2. In the upper-right pane, select **Uninstall VM Manager Tool**, and then in the lower pane, click **Take Action**.



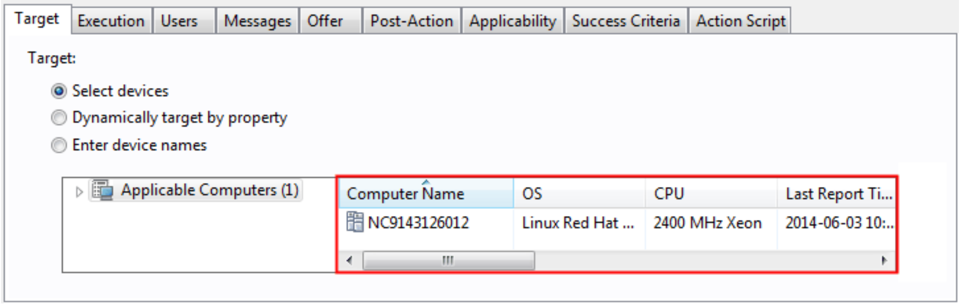
Fixlets and Tasks

Name	Source Sev...	Applicab...	Category	Open
Initiate Scanner Diagnostic Tool	Low	9 / 13	Troubleshooting	0
Install VM Manager Tool	Low	9 / 13	VM Managers	0
Uninstall Scanner	Low	13 / 13	Scanner	0
Uninstall VM Manager Tool	Low	1 / 13	VM Managers	0
Upload VM Manager Tool Scan Results	Low	1 / 13	VM Managers	2

Task: Uninstall VM Manager Tool

3. Select the computer on which you want to run the task, and click **OK**.

   Important: The only applicable computer should be the computer on which the IBM Endpoint Manager server is installed.



Target:

● Select devices

○ Dynamically target by property

○ Enter device names

Applicable Computers (1)

Computer Name	OS	CPU	Last Report Ti...
NC9143126012	Linux Red Hat ...	2400 MHz Xeon	2014-06-03 10:...

Scanning remote shared file systems

By default, shared file systems are not scanned by the Endpoint Manager agent. To scan a shared file system, you must select the **Scan remote shared disks** option while configuring a software scan.

About this task

Important: The following two types of shared file systems can be scanned: UNIX Network File System (NFS) and Windows Common Internet File System (CIFS).

To obtain complete information about the shared disks and the software that is installed on them, perform the following tasks:

Procedure

1. Run the task **Discover Remote Shared Disks** to identify the remote shared disks in your environment.
   a. Log in to the Endpoint Manager console.

b. In the navigation tree, click **Sites** > **External Sites** > **IBM Endpoint Manager for Software Use Analysis v9** > **Fixlets and Tasks**.

c. In the right section of the window, select the relevant computers and click **OK**.

2. Activate the **Shared Disk Information** analysis, which gathers remote shared disk information that was retrieved by the Discover Remote Shared Disks task. It also gathers the settings that identify the computers whose remote shared drives are scanned. By default, the following information is collected:
   - Computer name
   - Type of file system
   - Shared disk IP address
   - Mount point
3. Exclude unsupported file systems from scanning:

   a. In **Analyses**, open the **Shared Disk Information** analysis and click the Results tab to recognize file systems that must be excluded from scanning.

   b. In **Fixlets and Tasks**, open the **Add Excluded Directories** task and specify directories or mount points of unsupported file systems. For more information about excluding the directories, see *Excluding directories from being scanned* in *Configuring*.

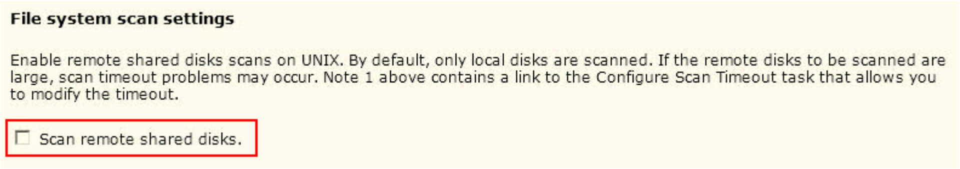
   Tip: A mount point is a directory that is at the top of the file system hierarchy. You can verify whether a directory is a mount point by checking the output of the `mount` or `mountpoint` commands.

   c. Run the **Add Excluded Directories** task against all endpoints that use the unsupported file systems.
4. Stop the current software scans.

   a. In the navigation tree of the console, click **Actions**.

   b. In the upper right pane, find the **Initiate Software Scan** action.

   c. In the lower pane, click **Stop**.
5. Open the **Initiate Software Scan** fixlet and select the option to scan remote shared disks.



File system scan settings

Enable remote shared disks scans on UNIX. By default, only local disks are scanned. If the remote disks to be scanned are large, scan timeout problems may occur. Note 1 above contains a link to the Configure Scan Timeout task that allows you to modify the timeout.

☐ Scan remote shared disks.

For more information, see the *Initiating software scans* topic in the *Managing the Infrastructure* guide.

If you have software that is installed on a shared disk, you must select one computer for the Software Use Analysis to scan the shared disk.

Note:

- Software scans can decrease the performance of a shared disk. If more clients are configured to scan a shared disk, performance of the disk might decrease drastically and the scanning might take a long time. It is then recommended to schedule the clients to scan the shared disk at different times, for example you might want to spread the scanning across many days of the week.
- If the remote disks to be scanned are large, scan timeout problems might occur.

Restriction: Automounted remote disks will be scanned only if they are mounted during a scan.

Importing software scan data

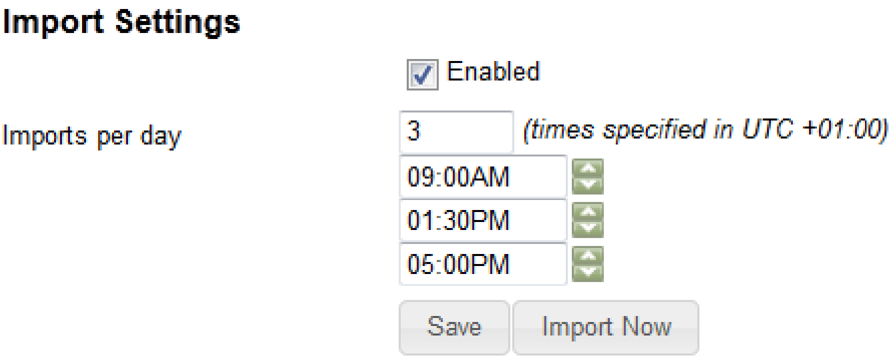
The inventory results are stored on your Endpoint Manager server. To import software scan data, the software catalog and other settings that changed since the last update, you must extract the data from Endpoint Manager server and load it into Software Use Analysis.

Before you begin

You must have the Manage Imports permission to perform this task.

Procedure

1. In the navigation bar, click **Management** > **Data Imports**.
2. To import software scan data, the software catalog and other settings that changed since the last update, click **Import Now**.
3. To schedule regular imports, select the **Enabled** check box, specify the number of daily imports and their hours, and click **Save**.



Import Settings

☑ Enabled

Imports per day: 3 *(times specified in UTC +01:00)*

09:00AM

01:30PM

05:00PM

Configuring catalog servers

Software Knowledge Base Toolkit can serve as a catalog server. Before the first import, you can optionally define the location of your software catalog server, so that Software Use Analysis can automatically gather catalog updates from that server.

Before you begin

- You must have the Manage Catalogs permission to perform this task.
- You must have Tivoli® Software Knowledge Base Toolkit installed in your infrastructure.

About this task

Configure the catalog server before the first import of the software catalog. Otherwise, assistance of the IBM support will be needed to reconcile catalog versions.

Update 9.0.1.2 Starting from application update 9.0.1.2, you can configure the catalog server at any point of time.

Procedure

1. In the top navigation bar, click **Management** > **Catalog Servers**. The default Software Knowledge Base Toolkit host and port number are specified in the table.
2. To change the default settings, click the row in the table with the `localhost:12344` server data, modify the data, and click **Save**.
3. To verify that the connection is configured correctly, click **Check Connection**.

Results

You have configured your catalog server. The most recent publication is now automatically pulled in from that catalog server during the import. Note that the software catalog must be published in Software Knowledge Base Toolkit for the automated catalog update to be possible.

Starting the server

To start the server, you must run the `SUAserver` script. If the server does not start after running the script, start the DB2® instance and then rerun the script.

Before you begin

You must be the user who installed Software Use Analysis or have root privileges to perform this task.

Procedure

1. Run the following command to start the server:

   ```
   /etc/init.d/wlpserver start
   ```

   Update 9.0.1 :

   ```
   /etc/init.d/SUAserver start
   ```

2. Optional: If the server does not start after running the script, start your DB2 instance and then restart the server:
   a. Log on to the computer where DB2 is installed. You must be a DB2 instance owner.
   b. Type **`db2start`** at the command line. The DB2 instance starts.

Stopping the server

You can stop the Software Use Analysis server by running the `SUAserver` script.

Before you begin

You must be the user who installed Software Use Analysis or have root privileges to perform this task.

Procedure

1. Run the following command to stop the server:

   ```
   /etc/init.d/wlpserver stop
   ```

   Update 9.0.1 :

```
/etc/init.d/SUAserver stop
```

2. Optional: After stopping the server, you can also stop the DB2 instance:
   a. Log on to the computer where DB2 is installed. You must be a DB2 instance owner.
   b. Type **db2stop** at the command line. The DB2 instance starts.

Updating the database password

You can update the database user password when needed, for example if the password is changed and users cannot log in to IBM Endpoint Manager for Software Use Analysis.

Before you begin

Before you can run the security utility you must set the JAVA_HOME environment variable, for example `export JAVA_HOME=`*install_dir*`/jre/jre`.

Procedure

1. Log in to the server where IBM Endpoint Manager for Software Use Analysis is installed.
2. Run the following command and enter the new password for the database user.

   ```
   install_dir/wlp/bin/securityUtility encode
   ```

   The password is returned as an encrypted string.
3. Edit the following configuration files, and enter the new encrypted password.
   - *install_dir*/wlp/usr/servers/server1/server.xml

     Copy the new encrypted password to **password**, for example:

     ```
     properties.db2.jcc databaseName="SUADB" driverType="4"
     enableExtendedIndicators="2" password="{xor}Bq141231"
     portNumber="50000" serverName="localhost" user="db2inst1"
     ```

     Be sure to keep the double quotation marks around the encrypted value for the password.
   - *install_dir*/wlp/usr/servers/server1/config/database.yml

     Copy the new encrypted password to **encrypted_password**.
4. Restart the IBM Endpoint Manager for Software Use Analysis server.

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 79758 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 information 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.

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.

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.

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.

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.

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

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

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

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

Privacy policy considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

Printed in USA