

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

Configuration Guide



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

Configuration Guide



Configuration Guide

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

© **Copyright IBM Corporation 2002, 2014.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Configuring	1
Configuring the product after installation.	1
Performing basic configuration	1
Required: Setting up a proxy exception list for environments with proxy servers	1
Setting the code page for double-byte languages	1
Setting up roles	2
Setting up users	5
Configuring mail notifications	6
Configuring the application to display inventory	6
Setting up computer properties	6
Setting up computer groups	7
Scheduling the imports of scan data	7
Adding VM managers	8
Applying important IBM updates	9
Uploading a PVU table	9
Uploading the software catalog.	10
Uploading part numbers	10
Setting up scans	11
Distribution of scans for improved performance	11
Enabling software and hardware discovery.	12
Activating the analyses	12
Setting up analysis properties	13
Installing the scanner	13
Initiating software scans	15
Uploading scan results	19
Initiating the RPM scan (deprecated)	21
Initiating the capacity scan	22

Enabling the monitoring of software usage	25
Activating the analyses	25
Excluding directories from being scanned	26
Retrieving excluded directories	26
Adding excluded directories.	27
Removing excluded directories	28
Manually excluding directories	29
Defining the scan frequency and schedule	30
Updating the fixlet site	31
Checking the version of the fixlet site.	31
Updating the content of the fixlet site on Windows	31
Updating the content of the fixlet site on Linux	32
Caching the files.	32
Configuring server settings	33
Advanced administration server settings	34
Performing optional configuration.	36
Optimizing the volume of scanned file data	36
Configuring the application usage statistics.	37
Updating scanner catalogs	38
Configuring data retention period	39
Setting the home page.	39

Notices	41
Trademarks	42

Privacy policy considerations	43
--	-----------

Configuring

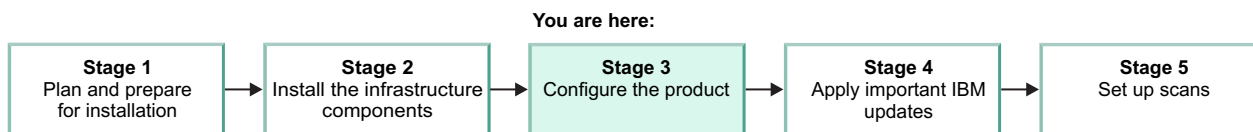


Read this guide to learn how to configure IBM® Endpoint Manager for Software Use Analysis.

Configuring the product after installation

To ensure that you take full advantage of the functions that are provided by IBM Endpoint Manager for Software Use Analysis, you must perform a set of tasks after the installation of the application.

About this task



Performing basic configuration

As an application administrator, you need to perform a few basic configurations.

Required: Setting up a proxy exception list for environments with proxy servers

If IBM Endpoint Manager server is configured to use proxy for internet connection to access fixlet sites or prefetch downloads, the Software Use Analysis catalog propagation fixlet might not work. The reason for this is that the Endpoint Manager server tries to connect to the proxy to download the catalog file for Common Inventory Technology, instead of connecting to the Software Use Analysis server directly.

For the information about how to configure the proxy exceptions on the IBM Endpoint Manager server, see the subsection *Setting a proxy connection on the server* in the topic *Setting a proxy connection*, which is available in the IBM Endpoint Manager information center.

Important: You must put on the exception list either the Software Use Analysis IP address or host name.

Setting the code page for double-byte languages

Double-byte character corruption can occur in some environments because Software Use Analysis uses the code page to transcode data. For double-byte languages such as Korean, Japanese, and Chinese, set the code page to avoid character corruption.

About this task

The `_BESClient_DeploymentEncoding_IANAName` setting of the BESClient running on the Endpoint Manager server must use the correct character set for double-byte languages. For example, for simplified Chinese the setting is CP936. One double-byte code page translation is allowed per Endpoint Manager server that is configured as a data source for Software Use Analysis.

Procedure

1. Log in to the IBM Endpoint Manager console.
2. Go to your **Subscribed Computers**, and select the computer on which you have both the Endpoint Manager server and the BESClient installed.
3. Go to **Edit Settings**, and change the `_BESClient_DeploymentEncoding_IANAName` setting to the correct encoding.
4. Stop the Software Use Analysis server.
5. Log in to the database server as a user with DB2 authority, open a DB2 command line and run the following commands:

```
db2 "connect to database database_name"
db2 "update dbo.datasources set last_sequence=cast( x'0000000000000000' as char(8) for b
db2 commit
```

6. Start the Software Use Analysis server and run a data import.

Setting up roles

You can set up roles that you assign to the users of Software Use Analysis. Each role is a collection of permissions that correlates to a list of privileges. The administrator assigns roles to each user according to the privileges the user needs to efficiently operate the application.

Before you begin



You must be an Administrator to perform this task.

Important: The Administrator role is set by default and cannot be modified.

Procedure

1. In the top navigation bar, click **Management > Roles**.
2. To add a role, click **New**.
3. Specify the name and permissions that you want the new role to have, and click **Create**.
4. Optional: To modify the role, click its name in the top pane of the Roles window.

Results

You have set up a user role. You can now create users and assign them suitable roles.

Roles:

You can create a set of roles in Software Use Analysis and assign each of them with different permissions. Then, you can assign those roles to particular users, thus making them responsible for different actions. By setting up correct roles, you

can easily establish which user has access to particular functions in Software Use Analysis. The roles can be assigned by the Administrator.

Six pre-configured roles are available in Software Use Analysis: Administrators, Auditors, Catalog Managers, Contract Managers, Software Asset Managers, and Infrastructure Administrators. Four pre-configured roles are available in : Administrators, Auditors, Software Asset Managers, and Infrastructure Administrators. Each of these roles has a different set of permissions that allow the users to perform various actions. You can edit or delete those roles, or create new ones and assign them permissions of your choice. The following table lists the pre-configured roles and their permissions.

Important: Some of the permissions are specific only for the Administrator and cannot be assigned to other users. These permissions include:

- Edit Server Configuration
- Manage Computer Properties
- Manage Data Sources
- Manage Directory Servers
- Manage Roles
- Manage User Provisioning
- Manage Users

Table 1. Pre-configured roles and permissions in Software Use Analysis

Permission	Administrator	Auditor	Catalog Manager	Contract Manager	Software Asset Manager	Infrastructure Administrator
Edit Server Configuration	✓					
Manage Catalogs	✓		✓			
Manage Computer Groups	✓					✓
Manage Computer Properties	✓					
Manage Contracts	✓			✓		
Manage Data Sources	✓					
Manage Directory Servers	✓					
Manage IBM Software Classification	✓				✓	
Manage Imports	✓				✓	✓
Manage Package Properties	✓					✓
Manage Roles	✓					
Manage Scan Configurations	✓					✓
Manage Uploads	✓		✓		✓	✓
Manage Usage Properties	✓					✓
Manage User Provisioning	✓					
Manage Users	✓					

Table 1. Pre-configured roles and permissions in Software Use Analysis (continued)

Permission	Administrator	Auditor	Catalog Manager	Contract Manager	Software Asset Manager	Infrastructure Administrator
Manage VM Managers and Servers	✓					✓
View Audit Trail	✓	✓			✓	
View Catalog Audit	✓	✓	✓		✓	
View Endpoints	✓	✓	✓	✓	✓	✓
View Hardware Inventory	✓	✓			✓	✓
View License Metrics	✓	✓			✓	
View Raw Data	✓	✓	✓	✓	✓	
View Software Catalog and Signatures	✓	✓	✓	✓	✓	

The following list describes the permissions that are available in Software Use Analysis. Find out about each of them so that you can tailor the roles to your needs.

Manage Catalogs

The user can edit catalog servers, update the catalog as well as add, modify, and delete the content of the custom software catalog.

Manage Computer Groups

The user can create, modify, and delete computer groups.

Manage Contracts

The user can create, modify, and delete contracts.

Manage IBM Software Classification

The user can reassign software instances between different products, include or exclude them in pricing calculations, and share them between more than one product.

Manage Imports

The user can schedule software scan data imports, and manually import new scan data.

Manage Scan Configurations

The user can schedule software scans.

Manage Package Properties

The user can create, edit, and delete the application properties that are used to recognize software in your infrastructure.

Manage Uploads

The user can manage the uploads of the software catalog, metric tables, and part numbers.

Manage Usage Properties

The user can create, edit, and delete the application properties that gather information about the use of software in your infrastructure.

Manage VM Managers and Servers

The user can create, edit, and delete VM managers.

View Audit Trail

The user can view the Audit Trail report that contains the history of all actions performed by users.

View Catalog Audit

The user can view information about changes to the custom software catalog.

View Endpoints

The user can view information about the installed software as well as scan, registry, and raw data from endpoints.

View Hardware Inventory

The user can view the details of the processors that are used by the software.

View License Metrics

The user can view the list of all software products that are contained in the PVU License Usage reports, the license type and usage for each product, the history of license consumption over the specified time period, and the top license consuming products.

View Raw Data

The user can view:

- Metering Data report that contains information about the use of the software items
- Unrecognized Files report that shows a ranking of the most frequently encountered files
- Scanned File Data report that provides information about all files that are detected by the software inventory tool scanner
- Package Data report that contains information about all installed packages


View Software Catalog and Signatures

The user can view the software catalog and signatures.

Setting up users

You must set up users before you can grant access to Software Use Analysis. Each user can be assigned a role that determines the permissions that the user has.

Before you begin

-  You must be an Administrator to perform this task.
- You must set up the roles that you want to assign to the specific users.

Procedure

1. In the top navigation bar, click **Management > Users**.
2. To add a user, click **New**.
3. Specify the name of the user and the role that you want to assign to that user. Select the computer group to which the user is to have access and the authentication method. Click **Create**.
4. Optional: To modify the user, click its name in the top pane of the Users window.

Configuring mail notifications

You can configure mail settings so that reports are automatically sent to the specified recipients. The option is especially useful if a person does not work with Software Use Analysis or is not familiar with the application, but needs to have access to the reports.

Before you begin



You must be an Administrator to perform this task.

Procedure

1. In the top navigation bar, click **Management > Mail Settings**.
2. Specify the SMTP server to which you want to have the email notifications sent.

Important: The SMTP port must be open for communication with Software Use Analysis.

3. Choose the port through which you want to have the email notifications sent:
 - To send email notifications through the default port, select **default**.
 - To send email notifications through the customized port, select **custom**, and specify the port that you want to use.
4. Optional: To have the email encrypted, select **Use STARTTLS**.
5. In the **IBM Endpoint Manager Analytics Server Domain**, specify the domain through which you access the Endpoint Manager server.
6. Choose the authentication method:
 - To use no authentication, click **None**.
 - To use simple authentication, click **Plain**.
 - To use login authentication, click **Login**.
 - To use a challenge-response authentication mechanism, click **CRAM-MD5**.
7. In the **From address** field, specify the address that is displayed as the sender of the email. To save the mail configuration, click **Save**.
8. Optional: To check whether you correctly configured mail settings, send a test email by clicking **Send Test Email**.

What to do next

You can now schedule reports that you want to have sent to the specified email accounts.

Configuring the application to display inventory

As an inventory administrator, you need to perform a few tasks to make the application display inventory properly.

Setting up computer properties

You can specify computer properties that are to be gathered from the computers in your infrastructure. You can then use those properties to filter data on the Computers report and to assign computers to computer groups.

Before you begin



You must be an Administrator to perform this task.

Procedure

1. To view the properties that are specified for the computers in your infrastructure, click **Management > Computer Properties**.
2. To add a property, click **New**.
3. In the Create Computer Property pane, specify the name of the property to be displayed in Software Use Analysis. Select the property from the Data Source Property list and click **Create**.

Tip: When you start typing in the property name, a list of possible values is displayed. It contains all properties whose names contain the letters that you entered in the specified order, regardless of whether the letters occur immediately one after another. For example, if you type path, the list might contain properties such as Patches Applied - Solaris, because letters p, a, t, h occur in this order in the property name.

What to do next

To have the computer property displayed, wait for the next scheduled import or run it manually. Each computer property requires that a relevant analysis is activated. After the import finishes, check the import log for warning messages that indicate that an analysis related to a particular property is not activated. For example:

```
WARN: Analysis 'Software Scan Status', bound to Computer Property  
'Status of catalog-based scan', is not activated and will not be imported.
```

If you find such a warning, activate the required analysis to have the computer property displayed.

Setting up 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 be an Administrator to perform this task.

Procedure

1. To set up a new computer group, click **Management > Computer Groups** and then, click **New**.
2. Enter the name and description of a new group in the Create Computer Group pane.
3. Create filters for your group parameters in the Definition section and click **Create**.
4. Optional: You can view the new group in the left pane of the Computer Groups window. You can also drag one group into another to make it a child or a subgroup.
5. To make new groups available in the component, click **Reports > Import Now**.

Scheduling the imports of scan data

You can schedule the imports of software and hardware scan data so that they occur regularly.

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 *(times specified in UTC +01:00)*

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.

About this task

Attention: For more information about adding VM managers in a distributed environment, see the section *Distributed virtual machine management*, which is available in the *Managing the Infrastructure* PDF guide.

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**.

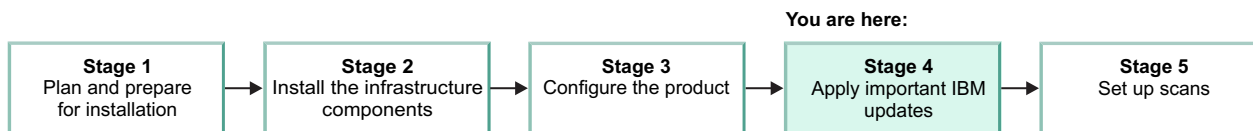
Results

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

Applying important IBM updates

After the installation, you must download the latest catalog and upload the latest PVU table. Optionally, you can import part numbers from the Passport Advantage® web site.

About this task



Uploading a PVU table

The PVU table is required to support processor-based pricing models in which charges differ according to the type of processor on which the licensed product is installed and running. In the table, a number of units are assigned to each processor type on which this type of pricing model is available.

Before you begin



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

About this task

The PVU table file is authenticated with SHA-256 to comply with the FIPS (Federal Information Processing Standards) security standards.

Update 9.0.1 Previous versions of PVU tables that are signed with SHA1 are not supported.

Procedure

1. In the top navigation bar, click **Management > Metric Table Upload**.
2. Open the IBM support website link and download a new PVU table.
3. Click **Browse**, select a file to upload, and then click **Upload**.

4. In the top navigation bar, click **Management > Data Imports** and then click **Import Now**.

Uploading the software catalog

Regularly update the software catalog and check for updates every month to keep your software inventory up-to-date. If you do not edit the content of the software catalog that is provided by IBM, update the catalog directly in Software Use Analysis.

Before you begin



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

About this task

This procedure describes how to update the software catalog directly to Software Use Analysis. Follow these steps if you do not edit the content of the software catalog or if you use the built-in catalog management functionality to create your customized catalog content. If you customize the catalog content in Software Knowledge Base Toolkit, see: Updating the software catalog in Software Knowledge Base Toolkit.

Procedure

1. Download the catalog.
2. In the navigation bar, click **Management > Catalog Upload**.
3. Click **Browse** and select the appropriate compressed file.
 - If you downloaded a compressed file that contains the software catalog, charge unit data, and the part numbers file, search for the `IBMSoftwareCatalog_canonical_2.0_form_date.zip` file.
 - If you downloaded a compressed file that contains only the software catalog in the XML format, search for the `IBMSoftwareCatalog_canonical_2.0_form_date.zip` file.
 - If you downloaded a compressed file that contains two CSV files with charge unit data and part numbers, search for the `ChargeUnits_date_dataversion_version.zip` file.

The default location of the file is `/opt/IBM/SUA/sua_catalog`.

4. To upload the file, click **Upload**.

Results

The software catalog file and the charge unit data are listed in the table. Their status is **Pending** until you import the scan data to process the new data.

Uploading part numbers

Upload and import part numbers to increase the accuracy of automated bundling of software components.

Before you begin



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

Procedure

1. Prepare the part numbers file.
2. In the top navigation bar, click **Management > Part Numbers Upload**.
3. Click **Browse** and choose the part numbers file to upload. You can upload either a csv or zip file.
4. Optional: If you want to overwrite the existing part numbers, select the Overwrite existing part numbers check box.

Note: The check box is enabled only if you have previously imported a part numbers file.

5. Click **Upload**.

When you upload the file, a new entry is created in the Upload History table. The status is Pending until you run the import.

Important: If more than one entry is Pending in the table, only the latest one will be executed during the import.

6. In the top navigation bar, click **Management > Data Imports**, and then click **Import Now**.

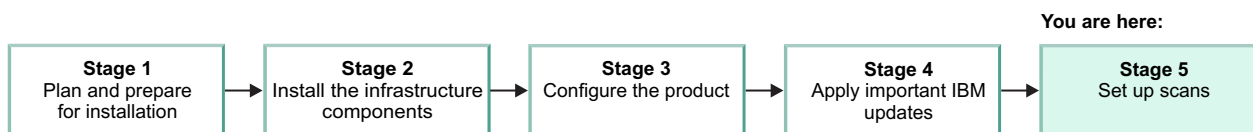
Results

The part numbers were imported to Software Use Analysis and saved in the `adm.current_part_numbers` table in the database. If you want to remove the part numbers from the server, click **Remove All Part Numbers** and then run the import. You can remove the part numbers only if you have previously imported the part numbers file to the server.

Setting up scans

You must set up scans so that data can be gathered and uploaded to IBM Endpoint Manager for Software Use Analysis.

About this task



Distribution of scans for improved performance

Performance of importing data from the Endpoint Manager server to Software Use Analysis depends on the number of scan files, usage analyses, and package analyses that are processed during a single import. By properly scheduling scans and distributing them over the computers in your infrastructure, you can reduce the length of the data import.

Use the following guidelines to improve the performance of the data import:

- After the installation of Software Use Analysis, do not install and run scanners on all computers in your infrastructure. Divide the computers into groups and start by gathering the default properties from a single computer group.
- Consider creating computer groups that are based on stability. In stable environment, scans can be run less frequently than once a week.

- Try to limit the number of computer properties that are gathered during scans.
- Schedule scans to run on different days for different computer groups. Avoid a situation in which multiple groups are scanned at the same day or the following day. It might cause that the scan and data import interfere.
- Reduce the frequency of scans. In most cases, it is sufficient to scan the infrastructure once a week, which is the default frequency. In large environments, you can disable the option to automatically run scans and initiate them only when necessary. The minimum scan frequency is once per month.
- In the initial deployment phase, or if you do not need information about software usage, disable the analysis that gathers usage data. To disable the analysis:
 1. Log in to the Endpoint Manager console.
 2. In the navigation tree, open the **IBM Endpoint Manager for Software Use Analysis v9 > IBM License Reporting (ILMT) v9 > Analyses**.
 3. In the upper-right pane, right-click **Application Usage Statistics**, and click **Deactivate**.

Enabling software and hardware discovery

To be able to discover software and hardware in your environment, you must activate the necessary analyses and install the appropriate scanners on your computers. After that, initiate software and hardware scans, and configure regular uploads of scan results.

Activating the analyses

An *analysis* is a collection of property expressions that a console operator uses to view and summarize properties of client computers across a network.

Before you begin

-  You must be a Master Operator to perform this task.

Procedure

1. In the left navigation bar of the Endpoint Manager console, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Analyses**.
2. In the upper-right pane, select the analyses that collect information needed in your environment. Right-click to display a list of options, and select **Activate**. The following analyses can be activated:
 - **Capacity Configuration for Linux on z/VM**
 - **Environment Information**
 - **Installed UNIX Packages**
 - **Installed Windows Applications**
 - **Scanner Information**
 - **Scanner Trace Settings**
 - **Shared Disk Information**
 - **Software Scan Status**
 - **VM Manager Information**

Tip: To learn how each analysis affects your deployment, click the analysis and view a description in the work area that opens.

Results

When an analysis is activated, its status changes in the **List Panel**. Now you can view and analyze the computers that you targeted.

Setting up analysis properties

Analysis properties are used to recognize software and gather information about its usage. Analysis properties are set by default in Software Use Analysis. You can also set up your own properties that you want to use to gather information from the endpoints.

Before you begin



You must have the Manage Usage and Package Properties permission to perform this task.

Procedure



1. In the top navigation, click **Management > Usage Properties**.
2. To add an application usage property, click **New**.
3. In the Create Application Usage Property pane, specify the name of the property. From the list of available properties, choose the data source property that you want to use to discover software that is installed in your infrastructure, its use or other properties, and click **Create**.

Installing the scanner

The scanner is installed from the Endpoint Manager console. You must install it so that you can run the software scans which collect information about file signatures on the endpoints and detect complex software signatures. The scanner is also used for a capacity scan that gathers hardware information about the endpoints to calculate the license usage.

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.

-  You must be a Master Operator to perform this task.
- Ensure that the Endpoint Manager client is installed and running on the target endpoint.
- Subscribe the target endpoints to the **IBM Endpoint Manager for Software Use Analysis v9** site.
-  Ensure that the following libraries are installed on the target endpoint: `libstdc++.so.5` or `libstdc++.so.6`.

Procedure

1. Log in to 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 **Install Scanner**, and then in the lower pane, click **Take Action**.

Fixlets and Tasks			
Name	Source Sev...	Applicab...	Category
Edit Scanner Trace Settings	Low	8 / 13	Troubleshooting
Initiate Scanner Diagnostic Tool	Low	8 / 13	Troubleshooting
Initiate Software Scan	High	12 / 13	Scanner
Install Scanner	High	1 / 13	Scanner
Install VM Manager Tool	Low	9 / 13	VM Managers
Remove Targeting Exception	Low	0 / 13	Configuration

Task: Install Scanner						
Take Action	Edit	Copy	Export	Hide Locally	Hide Globally	Remove

- Select the name of the computer on which you want to install the scanner, and click **OK**.

Tip: You can click the **Action Script** tab to view or modify the script.

Target	Execution	Users	Messages	Offer	Post-Action	Applicability	Success Criteria	Action Script																									
Target:																																	
<input checked="" type="radio"/> Select devices <input type="radio"/> Dynamically target by property <input type="radio"/> Enter device names																																	
<div style="border: 1px solid gray; padding: 5px;"> > Applicable Computers (4) <table border="1" style="float: right; margin-left: 10px;"> <thead> <tr> <th>Computer Na...</th> <th>OS</th> <th>CPU</th> <th>Last Report Ti...</th> <th>Loa</th> </tr> </thead> <tbody> <tr> <td>NC91281112...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431260...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 13:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> </tbody> </table> </div>									Computer Na...	OS	CPU	Last Report Ti...	Loa	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
Computer Na...	OS	CPU	Last Report Ti...	Loa																													
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																													

The scanner has several configurations that define its operation. The default configuration specifies, for example, which files and directories are examined during software scans.

- Optional: You can view information about the installed scanner in the **Scanner Information** analysis.

Analyses				
Status	Name	Applicable Computer C...	Activated By	Time Activated
Activated Globally	Scanner Trace Settings	9	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Installed UNIX Packages	9	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Software Scan Status	13	IEMAdmin	2014-06-12 14:23:29
Activated Globally	Scanner Information	13	IEMAdmin	2014-06-12 15:30:51
Not Activated	Capacity Configuration for Linux on z/VM	0		

Analysis: Scanner Information																				
Activate	Deactivate	Edit	Export	Hide Locally	Hide Globally	Remove														
Description	Details	Results	Applicable Computers (13)																	
<div style="border: 1px solid gray; padding: 5px;"> > Applicable Computers (13) <table border="1" style="float: right; margin-left: 10px;"> <thead> <tr> <th>Computer Na...</th> <th>Libraries Prere...</th> <th>Scanner Version</th> <th>Scanner Exploi...</th> <th>Scanner Install ...</th> </tr> </thead> <tbody> <tr> <td>NC046213</td> <td>True</td> <td>2.7.0.2039</td> <td>SUA:</td> <td>C:\Program Fil...</td> </tr> <tr> <td>NC047005</td> <td>True</td> <td>2.7.0.2039</td> <td>SUA:</td> <td>C:\Program Fil...</td> </tr> </tbody> </table> </div>						Computer Na...	Libraries Prere...	Scanner Version	Scanner Exploi...	Scanner Install ...	NC046213	True	2.7.0.2039	SUA:	C:\Program Fil...	NC047005	True	2.7.0.2039	SUA:	C:\Program Fil...
Computer Na...	Libraries Prere...	Scanner Version	Scanner Exploi...	Scanner Install ...																
NC046213	True	2.7.0.2039	SUA:	C:\Program Fil...																
NC047005	True	2.7.0.2039	SUA:	C:\Program Fil...																

What to do next

After you install the scanner, run an import. Then, run the software scans.

Manually excluding directories:

After you install the scanner, you can specify which directories are to be excluded from scanning during the raw scan of the file system.

You specify those directories by adding paths to the `exclude_path.txt` file that is in the `<BES Client>LMT/CIT` directory. Each path must be added on a separate line. The file already contains some entries depending on the operating system. You can remove the content of the file which means that no paths are excluded from the scan. However, if you delete the whole file, it will be recreated with the default content before the next software scan.

Unless you exclude specific paths, all the following drives are included in the scan:

- **UNIX** All local drives and other drives, such as floppy disk, CD-ROM, and DVD.

Note: Remote drives are not scanned.

- **Windows** All local drives.

Specify paths according to the following syntax:

`drive:path`

Important: When you specify a path delimiter, you must use a forward slash (/) instead of a backslash (\). For example, `C:/Program Files`.

- drive** Specifies the drive. Asterisks (*) and question marks (?) are supported. This variable is optional on UNIX.
- path** Specifies the path. Asterisks (*) and question marks (?) are supported. This variable also supports the following CSIDL values on Windows:

```
%CSIDL_WINDOWS%
%CSIDL_PROGRAM_FILES%
%CSIDL_COMMON_DESKTOPDIRECTORY%
%CSIDL_COMMON_STARTMENU%
%CSIDL_COMMON_STARTMENU%
%CSIDL_COMMON_STARTUP%
%CSIDL_COMMON_PROGRAMS%
```

Important: The above CSIDL values already have a drive specified. If you use them, omit the *drive* variable.

You can refer to the following examples when specifying your paths.

- Excludes the System Volume Information folder on any local drive:
`?:/System Volume Information`
- Excludes the System32 folder on the local drive that is specified in the CSIDL value:
`%CSIDL_WINDOWS%/System32`


Initiating software scans

Software scans collect information about files with particular extensions, package data, and software identification tags to evaluate whether particular software exists on the target endpoints. They also gather information about the running processes

to measure software usage. By default, software scans are scheduled to run regularly but you can specify the exact days and times of the scans, or modify their start and end dates.

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.

-  You must be a Master Operator to perform this task.
- If the **Initiate Software Scan** task is not applicable on an endpoint, see: *Server operation problems* in the Troubleshooting guide.
- If you store backups of software directories on your endpoints, they might be reported as separate software instances resulting in false discoveries and incorrect license consumption. To avoid this problem, either exclude the backups from scanning or compress them with a data compressor, such as zip or rar.

About this task

The scanner can search for different types of information to determine whether software is installed on the target endpoints and UNIX shared disks or to measure its usage.

Catalog-based scan

In this type of scan, the Endpoint Manager server creates scanner catalogs that are sent to the endpoints. Based on those catalogs, the scanner discovers exact matches and sends its findings to the server. The scanner catalogs do not include signatures that can be found based on the list of file extensions nor entries that are irrelevant for a particular operating system.

File system scan

In this type of scan, the scanner uses a list of file extensions to check whether any files with those extensions exist on the endpoints. Then, it returns the findings to the Endpoint Manager server where the discovered files are compared with the software catalog. If a particular file matches an entry in the catalog, the software is discovered.

Package data scan

In this type of scan, the scanner searches the system registry to gather information about Windows and UNIX packages that are installed on the endpoints. Then, it returns the findings to the Endpoint Manager server where the discovered packages are compared with the software catalog. If a particular package matches an entry in the catalog, the software is discovered.

Update 9.0.1.1 Application usage statistics

In this type of scan, the scanner gathers information about processes that are running on the target endpoints. Then, it returns the findings to the Endpoint Manager server where the data is translated into usage statistics.

Remember: By default, the usage scan is scheduled to run weekly to avoid performance issues. If you want to collect software usage on a daily basis, run the usage scan daily.

Software identification tags scan

In this type of scan, the scanner searches for software identification tags

that are delivered with software products. Then, it returns the findings to the Endpoint Manager server where the tags are processed. Based on the information that they contain, the software is discovered.

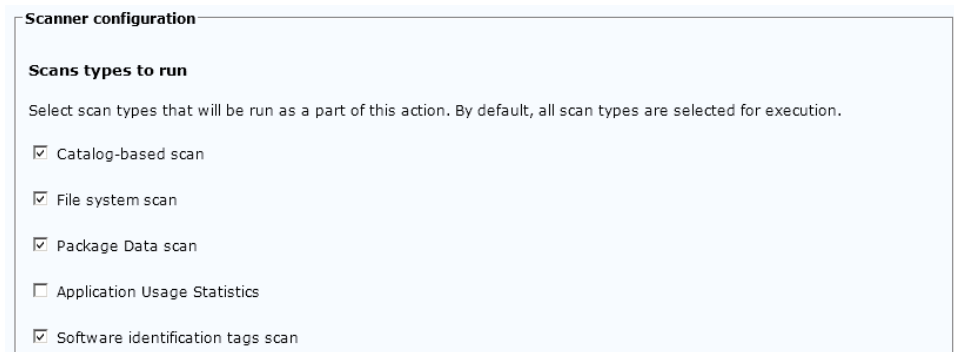
Update 9.0.1.2 Scan remote shared disks

This option enables the scanning of UNIX shared disks. By default, only local drives are scanned.

Tip: Generally, all types of scans should be run regularly. However, you can choose to run different types of scans at different times or distribute the scan schedule over the computers in your environment to improve the performance of the import process.

Procedure

1. Log in to the Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
3. Select **Initiate Software Scan**.
4. In the lower pane, select the types of scans that you want to initiate.



The screenshot shows a configuration window titled "Scanner configuration". Under the heading "Scans types to run", there is a sub-heading "Select scan types that will be run as a part of this action. By default, all scan types are selected for execution." Below this, there are five checkboxes: "Catalog-based scan" (checked), "File system scan" (checked), "Package Data scan" (checked), "Application Usage Statistics" (unchecked), and "Software identification tags scan" (checked).

5. Optional: If you want to scan shared file systems, select **Scan remote shared disks**. For more information, see the topic *Scanning remote shared file systems* in the *Managing the infrastructure* guide.



The screenshot shows a configuration window titled "File system scan settings". It contains a sub-heading "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." Below this, there is one checked checkbox: "Scan remote shared disks."

6. Optional: If you want to limit the amount of the processor resources that the scanner consumes, select **Initiate the software scan with CPU threshold**. Specify the consumption limit that is in the range 5 - 100. The higher value you specify, the higher is the consumption limit. For example, if you specify 75, scanner processes use up to 75% of the processing power of the target computer.

Important: If you provide a non-integer value or a value that is out of the range, the action fails.

CPU threshold

Initiate the software scan with CPU threshold

CPU threshold value: (range 5-100)

- To start the scan, click **Take Action**.

Fixlets and Tasks

Name	Source Sev...	Applicab...	Category
Edit Capacity Configuration for Linux on z...	Low	0 / 13	Configuration
Edit Scanner Trace Settings	Low	9 / 13	Troubleshooting
Initiate Scanner Diagnostic Tool	Low	9 / 13	Troubleshooting
Initiate Software Scan	High	13 / 13	Scanner
Install Scanner	High	0 / 13	Scanner
Install VM Manager Tool	Low	9 / 13	VM Managers

Task: Initiate Software Scan

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

- To select a subset of computers on which you want to initiate the scans, open the **Target** tab, and then click the computer that you want to scan.

Target

Execution | Users | Messages | Offer | Post-Action | Applicability | Success Criteria | Action Script

Target:

Select devices
 Dynamically target by property
 Enter device names

Applicable Computers (4)

Computer Na...	OS	CPU	Last Report Ti...	Loc
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

- Optional: By default, the scans are scheduled to run regularly. If you want to specify the dates and frequency of the scans, open the **Execution** tab. Specify the details, and click **OK**.

Tip: It is best to run the scans every week. In large deployments, it is better to target individual computer groups at different times.

Target	Execution	Users	Messages	Offer	Post-Action	Applicability	Success Criteria	Action Script
Constraints								
<input type="checkbox"/>	Starts on	2014-06-12	at	15:27:03	client local time			
<input type="checkbox"/>	Ends on	2014-06-14	at	15:27:03	client local time			
<input type="checkbox"/>	Run between	01:00:00	and	02:59:00	client local time			
<input type="checkbox"/>	Run only on	Sun Mon Tue Wed Thu Fri Sat			client local time			
<input type="checkbox"/>	Run only when	Active Directory Path	matches					
Behavior								
<input checked="" type="checkbox"/>	On failure, retry	3	times					
	<input checked="" type="radio"/> Wait	30 minutes	between attempts					
	<input type="radio"/> Wait until computer has rebooted							
<input checked="" type="checkbox"/>	Reapply this action							
	<input type="radio"/> whenever it becomes relevant again							
	<input checked="" type="radio"/> while relevant, waiting	7 days	between reapplications					
<input type="checkbox"/>	Limit to	3	reapplications					
<input type="checkbox"/>	Start client downloads before constraints are satisfied							
<input type="checkbox"/>	Stagger action start times over	5	minutes to reduce network load					

What to do next

1. Upload scan results to the Endpoint Manager console.
2. Run the capacity scan to gather hardware information.

Uploading scan results

Scan results are uploaded to the Endpoint Manager server by the **Upload Software Scan Results** task. By default, the task is scheduled to run on a regular basis. To ensure that inventory data is kept current, upload and scan tasks must be on a similar schedule.

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.

-  You must be a Master Operator to perform this task.

Procedure

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

Fixlets and Tasks			
Name	Source Sev...	Applicab...	Category
Uninstall VM Manager Tool	Low	1 / 13	VM Managers
Unset DSD Mode	Low	0 / 13	Configuration
Upgrade to IBM License Metric Tool 9.0	High	0 / 13	Deployment
Upload Scanner Diagnostic Data	Low	0 / 13	Troubleshooting
Upload Software Scan Results	High	7 / 13	Scanner
Upload VM Manager Tool Scan Results	Low	1 / 13	VM Managers

Task: Upload Software Scan Results

Note: The size of a single compressed scan result cannot exceed 1 MB.

- To select a subset of computers from which you want to upload the results, open the **Target** tab, and then click the computer.

Target	Execution	Users	Messages	Offer	Post-Action	Applicability	Success Criteria	Action Script																									
Target: <ul style="list-style-type: none"> <input checked="" type="radio"/> Select devices <input type="radio"/> Dynamically target by property <input type="radio"/> Enter device names 																																	
Applicable Computers (4) <table border="1"> <thead> <tr> <th>Computer Na...</th> <th>OS</th> <th>CPU</th> <th>Last Report Ti...</th> <th>Loc</th> </tr> </thead> <tbody> <tr> <td>NC91281112...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431260...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 13:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> </tbody> </table>									Computer Na...	OS	CPU	Last Report Ti...	Loc	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
Computer Na...	OS	CPU	Last Report Ti...	Loc																													
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																													

- Optional: To specify the frequency of uploading scan results, open the **Execution** tab. By default, the task runs when the new results are available.

Target	Execution	Users	Messages	Offer	Post-Action	Applicability	Success Criteria	Action Script
Constraints <ul style="list-style-type: none"> <input type="checkbox"/> Starts on: 2014-06-16 at 09:55:14 client local time <input type="checkbox"/> Ends on: 2014-06-18 at 09:55:14 client local time <input type="checkbox"/> Run between: 01:00:00 and 02:59:00 client local time <input type="checkbox"/> Run only on: Sun Mon Tue Wed Thu Fri Sat client local time <input type="checkbox"/> Run only when: Active Directory Path matches 								
Behavior <ul style="list-style-type: none"> <input checked="" type="checkbox"/> On failure, retry: 3 times <ul style="list-style-type: none"> <input type="radio"/> Wait: 1 hour between attempts <input checked="" type="radio"/> Wait until computer has rebooted <input checked="" type="checkbox"/> Reapply this action <ul style="list-style-type: none"> <input checked="" type="radio"/> whenever it becomes relevant again <input type="radio"/> while relevant, waiting: 15 minutes between reapplications <input type="checkbox"/> Limit to: 3 reapplications <input type="checkbox"/> Start client downloads before constraints are satisfied <input type="checkbox"/> Stagger action start times over: 5 minutes to reduce network load 								

- Click OK.

Initiating the RPM scan (deprecated)

The RPM scan collects information about the installed RPM packages on the UNIX systems.

Before you begin



You must be a Master Operator to perform this task.

About this task

The **Run RPM Scan and Upload Results** fixlet is a legacy fixlet that is available only in older versions of the **IBM Endpoint Manager for Software Use Analysis v9** action site. In the newer version of the action site, information about the installed RPM packages is gathered by the **Initiate Software Scan** fixlet. If you have an older version of the action site, update it.

Procedure

- Log on to the Endpoint Manager console.
- In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
- Select **Run RPM Scan and Upload Results**, and then in the lower pane, click **Take Action**.

Fixlets and Tasks			
Name	Source Sev...	Applicab...	Category
Download IBM License Metric Tool	High	4 / 13	Deployment
Initiate Software Scan	High	13 / 13	Scanner
Run Capacity Scan and Upload Results	High	1 / 13	Scanner
Run RPM Scan and Upload Results	High	9 / 13	Scanner
Add Targeting Exception	Low	13 / 13	Configuration
Edit Scanner Trace Settings	Low	9 / 13	Troubleshooting

Task: Run RPM Scan and Upload Results

Take Action
 Edit
 Copy
 Export
 Hide Locally
 Hide Globally
 Remove

- To select a subset of computers on which you want to initiate the scan, open the **Target** tab, and then click the computer that you want to scan.

Target	Execution	Users	Messages	Offer	Post-Action	Applicability	Success Criteria	Action Script																									
Target:																																	
<input checked="" type="radio"/> Select devices <input type="radio"/> Dynamically target by property <input type="radio"/> Enter device names																																	
<div style="border: 1px solid gray; padding: 5px;"> <p>Applicable Computers (4)</p> <table border="1"> <thead> <tr> <th>Computer Na...</th> <th>OS</th> <th>CPU</th> <th>Last Report Ti...</th> <th>Loc</th> </tr> </thead> <tbody> <tr> <td>NC91281112...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431260...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 13:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> <tr> <td>NC91431261...</td> <td>Linux Red Hat ...</td> <td>2400 MHz Xeon</td> <td>2014-06-12 14:...</td> <td>No</td> </tr> </tbody> </table> </div>									Computer Na...	OS	CPU	Last Report Ti...	Loc	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
Computer Na...	OS	CPU	Last Report Ti...	Loc																													
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																													

- Optional: By default, the scan runs on a regular basis. If you want to specify the dates and frequency of the scan, open the **Execution** tab. Specify the details, and click **OK**.

Tip: It is best to run the scans every week. In large deployments, it is better to target individual subsets of computers at different times.

The screenshot shows a configuration window with several tabs: Target, Execution, Users, Messages, Offer, Post-Action, Applicability, Success Criteria, and Action Script. The 'Constraints' section includes options for 'Starts on', 'Ends on', 'Run between', 'Run only on', and 'Run only when'. The 'Behavior' section, highlighted with a red box, includes options for 'On failure, retry' (3 times, Wait 10 minutes), 'Reapply this action' (while relevant, waiting 7 days), 'Limit to' (3 reapplications), 'Start client downloads before constraints are satisfied', and 'Stagger action start times over' (5 minutes).

6. When the scan completes successfully, it automatically uploads the scan results to the server.
7. You can view the collected data in the **Installed UNIX Packages** analysis. To read multiple results returned by the analysis, double-click on the results for the endpoint.

The screenshot shows the 'Analyses' window with a search bar and a table of scan results. The 'Installed UNIX Packages' analysis is selected, and its results are shown in a sub-window. The sub-window shows a table with columns for 'Computer Na...' and 'Installed Unix ...'.

Status	Name	Applicable Computer C...	Activated By	Time Activated
Activated Globally	VM Manager Information	1	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Installed Windows Applications	4	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Scanner Trace Settings	9	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Installed UNIX Packages	9	IEMAdmin	2014-06-12 15:30:51
Activated Globally	Software Scan Status	13	IEMAdmin	2014-06-12 14:23:29
Activated Globally	Scanner Information	13	IEMAdmin	2014-06-12 15:30:51

Computer Na...	Installed Unix ...
NC91431261...	<multiple resu...
NC91431261...	<multiple resu...
NC91431260...	<multiple resu...

Initiating the capacity scan

The capacity scan gathers hardware information about your endpoints, which is required to properly calculate the license consumption.

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.

-  You must be a Master Operator to perform this task.

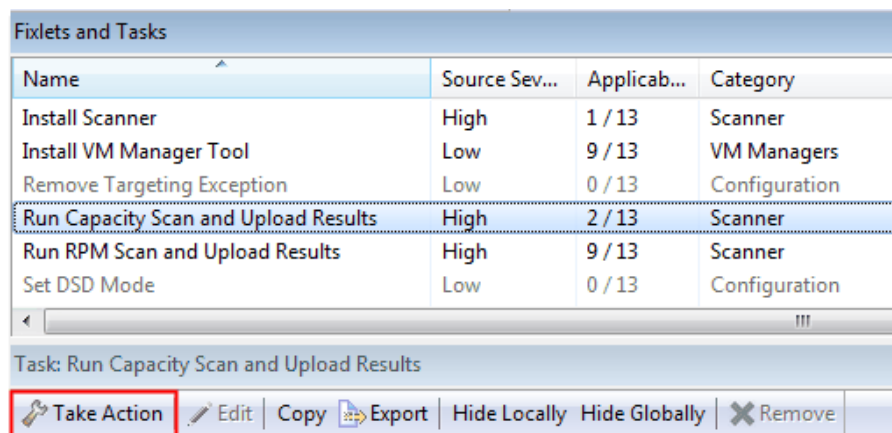
About this task

The capacity scan reports the system type (physical or virtual) and details of the physical processor. If applicable, it also collects information about the guest operating system and logical partitions.

The scan runs every 30 minutes and its schedule cannot be changed. Such a high frequency is required to always gather current results for virtual machines whose capacity can change depending on the assigned resources. This data must be accurate to ensure that PVU and RVU MAPC consumption is properly calculated. Despite the high frequency, the scan does not take long to complete and has minimal impact on your processor usage. Moreover, results that did not change since the last scan are not uploaded to the server.

Procedure

1. Log on to the Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
3. Select **Run Capacity Scan and Upload Results**, and then in the lower pane, click **Take Action**.

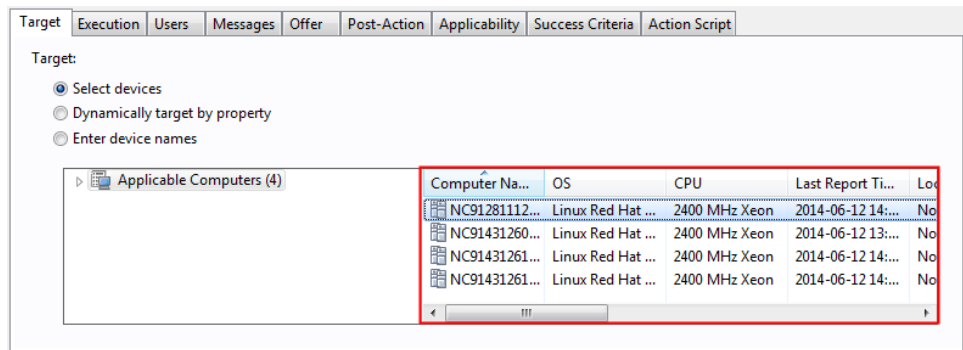


Name	Source Sev...	Applicab...	Category
Install Scanner	High	1 / 13	Scanner
Install VM Manager Tool	Low	9 / 13	VM Managers
Remove Targeting Exception	Low	0 / 13	Configuration
Run Capacity Scan and Upload Results	High	2 / 13	Scanner
Run RPM Scan and Upload Results	High	9 / 13	Scanner
Set DSD Mode	Low	0 / 13	Configuration

Task: Run Capacity Scan and Upload Results

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

4. To select a subset of computers on which you want to initiate the scan, open the **Target** tab, and then click the computer that you want to scan.



- When the scan completes successfully, it automatically uploads the scan results to the server.

Creating the capacity configuration for Linux on z/VM:

To properly calculate subcapacity values for Linux on z/VM, run a fixlet that creates a file with manually entered capacity values and places it on the target computer.

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.

About this task

The **Create Capacity Configuration for Linux on z/VM** fixlet is relevant on computers where manual configuration is required. If you have a computer where Linux is installed on z/VM and the fixlet is not relevant on that computer, your virtualization supports automatic capacity configuration. In such a case, you do not have to perform any manual actions to calculate the capacity values. The automatic capacity configuration is supported on System z10 E64 (type 2097) mainframes with z/VM 6.3 that supports the Store Hypervisor Information (STHYI) instruction.

Procedure

- Log on to the Endpoint Manager console.
- In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
- Select **Create Capacity Configuration for Linux on z/VM** and specify the following values:
 - Machine Type
 - Processor Type
 - Shared Pool Capacity
 - System Active Processors
- After you specify the required values, click **Take Action** to run the task.
- To select the computers for which you want to create the capacity configuration, open the **Target** tab, and then click the computer.
- Optional: If you want to edit or delete the capacity configuration, use the **Edit Capacity Configuration for Linux on z/VM** or **Delete Capacity Configuration for Linux on z/VM** task.

Setting the DSD mode:

If your computer runs the Solaris operating system and is in the DSD domain, you must set the DSD mode so that the PVU data can be correctly calculated.

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.

Procedure

1. Log on to the Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
3. Select **Set DSD Mode** and then in the lower pane, click **Take Action**.
4. To select the computers for which you want to set the DSD mode, open the **Target** tab, and then click the computer.
5. Optional: If you want to remove the DSD mode, use the **Unset DSD Mode** task.

Enabling the monitoring of software usage

To monitor software usage, activate the appropriate analyses and set up their properties.

Activating the analyses

An *analysis* is a collection of property expressions that a console operator uses to view and summarize properties of client computers across a network. After activating the analysis, you must also add two settings to each computer from which you want to collect the data.

Procedure

1. In the left navigation bar of the Endpoint Manager console, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Analyses**.
2. In the upper-right pane, select the **Application Usage Statistics** analysis. Right-click to display a list of options and select **Activate**.

Tip: To learn how the analysis affects your deployment, click the analysis and view a description in the work area that opens.

3. In the left navigation bar, click **Computers**.
4. Right-click on a computer from which you want to collect the application usage statistics and click **Edit Computer Settings**.
5. Click **Add** to add a setting:
 - a. Specify the setting name as `_BESClient_UsageManager_EnableAppUsageSummary` and the value as 1.
 - b. Click **OK**.
6. Click **Add** to add another setting:
 - a. Specify the setting name as `_BESClient_UsageManager_EnableAppUsageSummaryApps` and the value as `-:noapp:` .
 - b. Click **OK**.

Results

When the analysis is activated, its status changes in the **List Panel**. Now you can view and analyze the computers that you targeted.

Excluding directories from being scanned

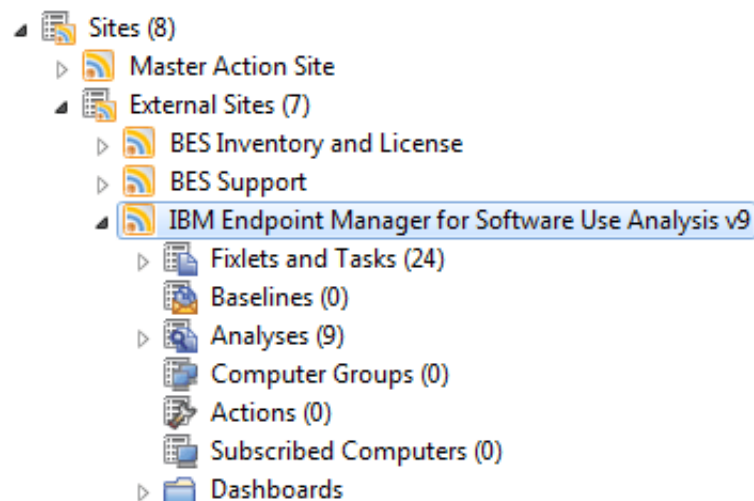
Excluding some directories from scanning is useful if the directories are large and contain no information that is important to the software inventory. By excluding them, you can speed up the scanning process. You can add directories or remove them from the list by using tasks in the IBM Endpoint Manager console. You can also manually add them to the scanner files on particular endpoints.

Retrieving excluded directories

The list of all directories that are excluded from scanning can be retrieved by activating an analysis in the IBM Endpoint Manager console.

Procedure

1. Log in to the IBM Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9**, and then click **Analyses**.



3. Select the **Excluded Directories** analysis, right-click on it, and then click **Activate**. The analysis is activated and starts retrieving the list of directories.
4. To view the excluded directories, click the **Results** tab. Directories are divided according to endpoints. You can view the directories in three ways:
 - All directories printed on separate lines are listed in the **Excluded Directories** column. If an entry says <multiple results>, hover over it to view the complete list.
 - All directories printed on one line and separated with a semicolon (;) are listed in the **Excluded Directories (semicolon separated)** column.
 - You can also double-click on <multiple results> to view the summary. All directories are listed in the **Excluded Directories** entry.

Computer Name	Operating System	Excluded Directories	Excluded Directories (semicolon separated)
NC040203	Win2008R2 6.1.7600	<multiple results>	%CSIDL_WINDOWS%/SNtServicePackUninst...
NC043019	Linux Red Hat Enterp...	<multiple results>	*/eznim;*/tmp;/proc
NC043024	Win2008R2 6.1.7600	<multiple results>	%CSIDL_WINDOWS%/SNtServicePackUninst...
NC9128110031	Linux Red Hat Enterp...	<multiple results>	*/eznim;*/tmp;/proc;?;/tomek
NC9143126242	Win2008 6.0.6002	<multiple results>	%CSIDL_WINDOWS%/SNtServicePackUninst...

Results

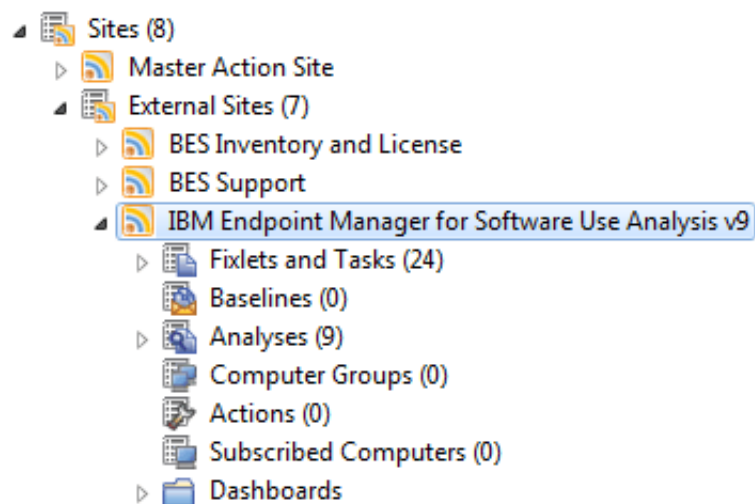
You retrieved the list of all directories that are excluded from scanning. Whenever you add or remove a directory from the list, you can use this analysis to verify if the operation succeeded.

Adding excluded directories

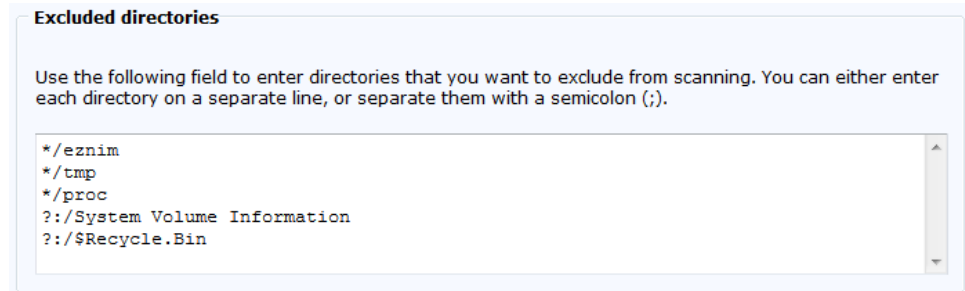
To exclude a directory from being scanned, add it to the list, and then run the task against the chosen endpoints.

Procedure

1. Log in to the IBM Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9**, and then click **Fixlets and Tasks**.



3. Select the **Add Excluded Directories** task.
4. Specify which directories are to be excluded from scanning.



5. Click **Take Action** and select endpoints for which you want to apply the changes.

Results

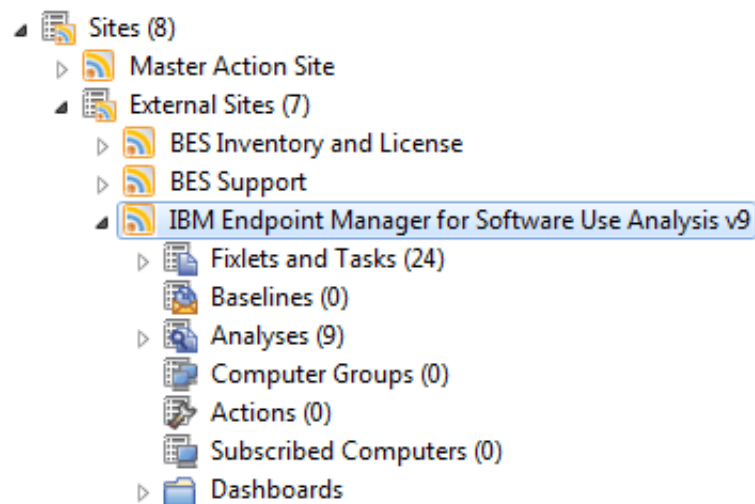
You added new entries to the list of directories that are excluded from scanning.

Removing excluded directories

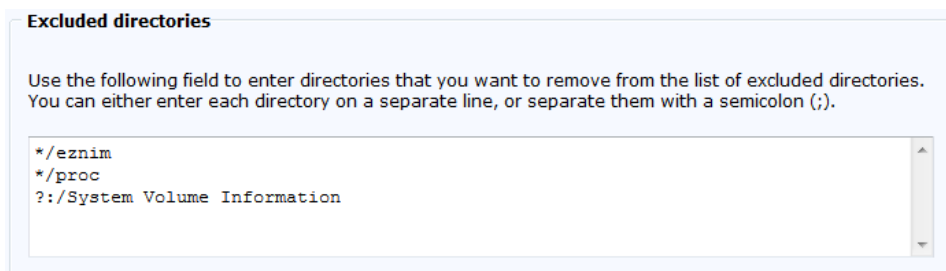
To include a directory back in the software scan, add it to the list, and then run the task against the chosen endpoints.

Procedure

1. Log in to the IBM Endpoint Manager console.
2. In the navigation tree, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9**, and then click **Fixlets and Tasks**.



3. Select the **Remove Excluded Directories** task.
4. Specify which directories are to be removed from the list of excluded directories.



5. Click **Take Action** and select endpoints for which you want to apply the changes.

Results

You removed the entries from the list of directories that are excluded from scanning. Those directories are now scanned during the software scan.

Manually excluding directories

After you install the scanner, you can specify which directories are to be excluded from scanning during the raw scan of the file system.

You specify those directories by adding paths to the `exclude_path.txt` file that is in the `<BES Client>LMT/CIT` directory. Each path must be added on a separate line. The file already contains some entries depending on the operating system. You can remove the content of the file which means that no paths are excluded from the scan. However, if you delete the whole file, it will be recreated with the default content before the next software scan.

Unless you exclude specific paths, all the following drives are included in the scan:

- **UNIX** All local drives and other drives, such as floppy disk, CD-ROM, and DVD.

Note: Remote drives are not scanned.

- **Windows** All local drives.

Specify paths according to the following syntax:

`drive:path`

Important: When you specify a path delimiter, you must use a forward slash (/) instead of a backslash (\). For example, `C:/Program Files`.

drive Specifies the drive. Asterisks (*) and question marks (?) are supported. This variable is optional on UNIX.

path Specifies the path. Asterisks (*) and question marks (?) are supported. This variable also supports the following CSIDL values on Windows:

```
%CSIDL_WINDOWS%
%CSIDL_PROGRAM_FILES%
%CSIDL_COMMON_DESKTOPDIRECTORY%
%CSIDL_COMMON_STARTMENU%
%CSIDL_COMMON_STARTMENU%
%CSIDL_COMMON_STARTUP%
%CSIDL_COMMON_PROGRAMS%
```

Important: The above CSIDL values already have a drive specified. If you use them, omit the *drive* variable.

You can refer to the following examples when specifying your paths.

- Excludes the System Volume Information folder on any local drive:
?:/System Volume Information
- Excludes the System32 folder on the local drive that is specified in the CSIDL value:
%CSIDL_WINDOWS%/System32

Defining the scan frequency and schedule

You can set the scan frequency and schedule for each data source in your environment in the Scan Configurations window. Use the Scan Configurations window as an alternative to using the IBM Endpoint Manager console to manage scan scheduling.

Before you begin



You must be an Administrator or an Infrastructure Administrator to perform this task.

About this task

Each row in the Scan Configurations window shows the schedule and status of the Initiate Software Scan action. This action is applied to the All Computers group. Updates to the scan configuration are recorded in the Audit trail report.

Procedure

1. Click **Management > Scan Configurations** and select the data source that you want to change scan settings for.

A scan configuration for a data source can have one of three statuses:

Active The scan schedule is active. When a scan schedule is active the Initiate Software Scan action is run according to the schedule defined in the Scan Configurations window.

Stopped

The scan schedule is inactive. You can define a new schedule in the Scan Configurations window.

Server unavailable

The scan schedule cannot be displayed and set because either the IBM Endpoint Manager server or the Web Reports server is not responding.

2. To specify the scan frequency, select a new frequency from the **Frequency** list.
3. To specify the scan scheduled start time, enter a new start date and time in the **Requested Start Date** field.

Note: Due to any network latency, the time on the server can be several minutes different from the requested start time that is specified in the Scan Configurations window.

4. Click **Save**.

Updating the fixlet site

The content of the Software Use Analysis fixlet site can be periodically modified. New fixlets, tasks, and analyses can be added. The existing ones can be changed or might become obsolete due to functionality changes. If the Endpoint Manager server is installed on a computer with the Internet access, the Software Use Analysis fixlet site is updated automatically whenever the updates are available. However, if the server is installed on a computer without the Internet access, you must update the fixlet site manually. Start by checking whether the fixlet site that you are currently using is up-to-date. If a newer version of the fixlet site exists, download the site content by using the Airgap tool. Then, cache the files on the Endpoint Manager server by using the BES Download Cacher.

Checking the version of the fixlet site

Compare the current version of the fixlet site with the latest version that was published. If a newer version is available, update the content of your fixlet site.

Procedure

1. To check what is the latest version of the fixlet site, open the <http://sync.bigfix.com/cgi-bin/bfgather/ibmforsua> site, and look for the Version line.
2. To check what is the current version of the fixlet site that you are using, open the Endpoint Manager console and click the name of the fixlet site. The version of the site is displayed on the **Details** tab.

What to do next

If a newer version of the fixlet site is available, update the content of your fixlet site.

Updating the content of the fixlet site on Windows

If the Endpoint Manager server is installed on a Windows computer without the Internet access, use the Airgap tool to download the content of the fixlet site to a Windows computer with the Internet access.

Before you begin

You need a Windows computer with the Internet access.

Procedure

1. Open the directory where the Endpoint Manager server is installed and run the `BESAirgapTool.exe` file. When prompted, save the file to a new folder, for example `Airgap`. An airgap request file is created.
2. Copy all the created files to a Windows computer with the Internet access.
3. On the computer with the Internet access, run the `BESAirgapTool.exe`. The airgap request file is changed into a response file.
4. Copy the `AirgapResponse` file to the Endpoint Manager server and place it in the directory that you created in step 1.
5. Run `BESAirgapTool.exe`. The airgap response is loaded to the Endpoint Manager server.

What to do next

Cache the files and move them to the Endpoint Manager server.

Updating the content of the fixlet site on Linux

If the Endpoint Manager server is installed on a Linux computer without the Internet access, use the Airgap tool to download the content of the fixlet site to a Windows computer with the Internet access.

Before you begin

- You need a Windows computer with the Internet access.
- Download the Airgap tool to the Windows computer with the Internet access. The tool is available on the Utilities page on the Endpoint Manager wiki.

Procedure

1. Open the command line and enter the following commands to run the Airgap tool:

```
cd /opt/BESServer/bin
./Airgap.sh -run
```

The `airgap.tar` file is created. It contains the `airgap` request file.

2. Extract the file by using the following command:

```
tar xvf airgap.tar
```
3. Copy the extracted `AirgapRequest.xml` file to the Windows computer and place it in the folder that contains the downloaded `BESAirgapTool.exe` file.
4. On the Windows computer, run the `BESAirgapTool.exe`. The `airgap` request file is changed into the `airgap` response file.
5. Copy the `AirgapResponse` file to the Endpoint Manager server and place it in the `/opt/BESServer/bin` directory.
6. Run the Airgap tool again to upload the `AirgapResponse` file to Endpoint Manager.

```
cd /opt/BESServer/bin
./Airgap.sh -run
```

Wait a few minutes for the Endpoint Manager console to refresh.

What to do next

Cache the files and move them to the Endpoint Manager server.

Caching the files

Typically, all fixlets, tasks, and analyses download the required files from the Internet. However, in a separated network, the files must first be cached and then moved to the Endpoint Manager server so that they are always available to fixlets.

Before you begin

- You need a Windows computer with the Internet access.
- Download the BES Download Cacher to the Windows computer with the Internet access. The tool is available on the Utilities page on the Endpoint Manager wiki.

Procedure

1. Go to the following location on the computer where the Endpoint Manager server is installed: *Installation_dir*\BES Server\wwwrootbes\bfsites.
2. Copy the IBM Endpoint Manager for Software Use Analysis.efxm file to the Windows computer with the Internet access and place it in the C:\IEM directory.
3. On the Windows computer, go to the C:\IEM directory and create a folder that is called downloads.

Tip: Do not clean the contents of this folder. Next time, when you run the Download Cacher only the files that were changed since the last download will be updated. The process will last shorter than if you downloaded the entire content every time.

4. Run the BES Download Cacher by running the following command:

```
BESDownloadCacher.exe -m "C:\IEM\IBM Endpoint Manager for Software Use Analysis.efxm"  
-x C:\IEM\downloads
```

The BES Download Cacher downloads 1 GB of required files.

5. Optional: The default cache size is enough if you use only the **IBM Endpoint Manager for Software Use Analysis v9** fixlet site. However, if you plan to run fixlets from other sites, such as **BES Support**, increase the cache size so that the IBM Endpoint Manager server does not try to delete any files:
 - a. In the left navigation bar of the Endpoint Manager console, click **Computers** and select your Endpoint Manager server from the list.
 - b. Right-click the server and then click **Edit Computer Settings**.
 - c. Increase the value of the `_BESgather_Download_CacheLimitMB` setting. If the setting is not on the list, add it and specify the value in MB.

Tip: The size depends on each fixlet site, however you might need to increase it to at least a couple of gigabytes.

6. Copy the contents of the downloads folder into the following directory on the Endpoint Manager server:

Installation_dir\BES Server\wwwrootbes\bfmirror\downloads\sha1

Results

The cached files are automatically delivered to the Endpoint Manager relays and clients every time you run a fixlet that requires those files. Use both the Airgap tool and the BES Download Cacher periodically to ensure that the content of your fixlet site is always up-to-date.

What to do next

Fixlets that were initiated from your old fixlet site are still saved as actions and continue to run using the old content. After you update the site, delete the old actions and then rerun the corresponding fixlets from the updated site. In the navigation tree of the Endpoint Manager console, click **Actions**, and delete all actions that originated from your fixlet site.

Configuring server settings

You can change the settings of the Software Use Analysis server by using the REST API queries.

About this task

For the list of administration server settings that you can change, see: “Advanced administration server settings.”

Procedure

- To check the current value of all server parameters, use the following REST API query.

```
GET http://server_host_name:port_number/api/sam/configs?token=token
```

For example:

```
GET http://localhost:9988/api/sam/configs?
token=7adc3efb175e2bc0f4484bdd2efca54a8fa04623&
```

- To check the current value of a single parameter, use the following REST API query.

```
GET http://server_host_name:port_number/api/sam/configs?token=token&
name=parameter_name
```

Where *token* is a unique user authentication identifier, and *parameter_name* is the name of the parameter whose value you want to check. For example:

```
GET http://localhost:9988/api/sam/configs?
token=7adc3efb175e2bc0f4484bdd2efca54a8fa04623&
name=maxVMManagerInactivity
```

- To change the value of a parameter, use the following REST API query.

```
PUT http://server_host_name:port_number/rest/configs?token=token&
name=parameter_name&value=parameter_value
```

Where *token* is a unique user authentication identifier, and *parameter_name* is the name of the parameter whose value you want to change and *value* is the new value. For example:

```
PUT http://localhost:9988/api/sam/configs?
token=7adc3efb175e2bc0f4484bdd2efca54a8fa04623&
name=maxVMManagerInactivity&value=10
```

Advanced administration server settings

Refer to the list of administration server parameters that can be configured to tune the product to your needs.

Restriction: The parameters whose names begin with **vmman** can be configured from the server only if you are using the centralized virtual machine management. Otherwise, you must edit VM manager configuration files to change the parameters.

Table 2. Configuration parameters of the administration server

Parameter	Units	Default	Minimum	Maximum
	Description			
<code>calculateLicenseUsageForIncompleteComputers</code>	Boolean (true/false)	True		
	Specifies how PVU consumption on x86 virtual machines that have incomplete data is counted. If set to true, PVU consumption is counted based on the number of PVUs on the host. In this case, the reported PVU consumption might be higher than the real value, but configuration of VM managers is not required. If set to false, the reported PVU consumption is 0, and VM managers must be configured.			

Table 2. Configuration parameters of the administration server (continued)

Parameter	Units	Default	Minimum	Maximum
computerVmManagerDetachmentPeriod	Days	7	1	90
	Specifies the maximum idle time after which a computer that is managed by a VM manager is considered detached. After that time, the data that is sent by an agent is not augmented by the data that is retrieved from the VM manager. The computer status changes into <i>No VM Manager Data</i> .			
csvReportSeparator	Character	Comma (,)		
	Specifies the character that is used as a line separator during the creation of CSV files.			
maxWaitingForVMData	Days	7	1	30
	Specifies the maximum age of capacity data of a virtualization infrastructure that is gathered by the VM Manager Tool scan. Data that is older than the specified age is discarded during the retrieval and storage process and is not included in the aggregation process.			
maxVMManagerInactivity	Days	3	1	90
	Specifies the maximum time after which a VM manager is considered inactive if no new data is received by the server.			
numberOfImportThreads	Number	0	0	32
	Specifies the number of threads that are used to process capacity scan data and VM manager scan data during the import of data from the Endpoint Manager server. Tip: In environments with over 10000 endpoints that are running on high-performance machines, it can be beneficial to increase the number of threads to speed up the import.			
storeHwDataForAllVMManagerNodes	Boolean (true/false)	False		
	Specifies whether information about nodes and clusters that is retrieved from VM managers is stored in the database, regardless of whether an agent is running on any virtual machine on such nodes or clusters.			
tempPathForGeneratedFiles	Path	Period (.)		
	Specifies the path to the folder where temporary application files, such as the CSV file during generation, are stored.			
vmManagerPostprocessGuestEnabled	Boolean (true/false)	True		
	Specifies whether data about incomplete virtualization hierarchy is removed when new data is uploaded from VM managers. If set to <i>true</i> , incomplete topology data is removed on condition that the VM manager is configured within 24 hours since the first incomplete scan. If set to <i>false</i> , incomplete topology data remains on the server and might be shown on reports.			
vmman_check_uniqueness_enabled	Boolean (true/false)	True		
	Distinguishes unique VM managers from duplicates.			
vmman_connection_time_out	Seconds	90	10	3600 (1 hour)
	Specifies the time after which the connection with a VM manager is ended.			
vmman_max_subsequent_login_failures	Number	3	0	100
	Specifies the maximum number of failed attempts of logging in to the VM manager.			
vmman_thread_pool_size	Number	10	1	50
	Specifies the number of threads in thread pool that is used for connections to VM managers.			

Table 2. Configuration parameters of the administration server (continued)

Parameter	Units	Default	Minimum	Maximum
vmman_pooling_time_interval	Description			
	Minutes	30	30	10080 (1 week)
vmman_transfer_period	Specifies the interval between the consecutive retrievals of data from VM managers.			
	Minutes	720	30	10080 (1 week)
vmman_uuid_filtering_enabled	Determines how often scan data is transferred to the agent to be uploaded to the server if subsequent scans have the same results.			
	Boolean (true/false)	False		
Enables UUID filtering of VM managers.				

Performing optional configuration

You can perform optional configuration tasks to further customize the application.

Optimizing the volume of scanned file data

The Scanned File Data report provides information about files with particular extensions that were discovered on the computers in your infrastructure. The information is typically used for creating custom software signatures. To optimize the volume of the monitored data, narrow down the list of file extensions that are collected to only those extensions that are typically used for creating signatures. It reduces the workload on the Software Use Analysis server and improves the application performance.

About this task

If you are upgrading to application update 9.0.1.2, a configuration panel on which you can automatically optimize the volume of scanned file data is displayed. The following procedure describes manual steps that you can perform if you skipped the automatic configuration.

Procedure

1. Stop the Software Use Analysis server by running the following command:

```
/etc/init.d/SUAserver stop
```
2. To optimize the volume of the scanned file data, remove extensions that are not typically used for creating signatures from the following files. The files are in the `<SUA_install_dir>\wlp\usr\servers\server1\apps\tema.war\WEB-INF\domains\sam\config` directory.

Note: Do not remove extensions that you used for creating custom signatures. If you remove a particular extension and want to create a signature that is based on a file with that extensions later on, add the extension back to the appropriate file.

- In the `file_names_all.txt` file, leave the following extension:

```
\.ear$
```
- In the `file_names_unix.txt` file, leave the following extensions:

```
\.sh$
\.bin$
\.pl$
\.ear$
```

```
\.SH$
\.BIN$
\.PL$
\.EAR$
```

- In the `file_names_win.txt` file, leave the following extensions:

```
\.exe$
\.sys$
\.com$
\.ear$
\.ocx$
```

3. Start the Software Use Analysis server by running the following command:
`/etc/init.d/SUAserver start`
4. Optional: If a new software catalog is available, upload it.
5. Wait for the scheduled import or run it manually. During this import, performance might be lower because the software catalog is reimported.
6. Wait for the scheduled software scan. Alternatively, if you have infrequent software scans, stop the current scan and start a new one. It will allow you for using the optimized list of file extensions in a shorter time.
 - a. Log in to the Endpoint Manager console and in the left navigation tree, click **Actions**.
 - b. In the upper-right pane, click **Initiate Software Scan** and then click **Stop**.
 - c. Initiate a new software scan.
7. Wait for the scheduled import or run it manually. From now on, the optimized list of file extensions is used.

Configuring the application usage statistics

The default behavior of the software scan can be changed to collect the software usage information from all endpoints in your environment on a daily basis.

Before you begin

Note: Changing the default behavior increases the amount of data that is collected from your endpoints and results in longer data imports. This procedure is not recommended, especially for large environments. Before you proceed, ensure that you need this type of information to be collected from your environment.

About this task

Due to changes that were introduced in Software Use Analysis application update 9.0.1, the software usage information is no longer collected from all your endpoints on daily basis but is now aligned with the software scans schedule. This means that your endpoints must complete software scans before usage data is collected from them. This behavior shortens each data import and limits the amount of data that is collected from your environment, however it can be changed to resemble the configuration of the base Software Use Analysis 9.1 version.

Procedure

1. Log in to the IBM Endpoint Manager console.
2. In the left navigation bar, click **Sites > External Sites > IBM Endpoint Manager for Software Use Analysis v9 > Fixlets and Tasks**.
3. Select the **Initiate Software Scan** task.

4. In the Scanner configuration section, select only the **Application Usage Statistics** check box so that the changes are made specifically for this type of scan.
5. Click **Take Action** and then specify the applicable computers and the schedule for collecting the results:
 - a. In the Target tab, select the **Dynamically target by property** check box, and then select **All Computers**.
 - b. In the Execution tab, select **Reapply this action**, and set the **while relevant, waiting** option to 1 day.
 - c. Click **OK**.

Results

You changed the default settings for the Application Usage Statistics type of software scan. The software usage information is now collected daily from all endpoints in your environment.

Updating scanner catalogs

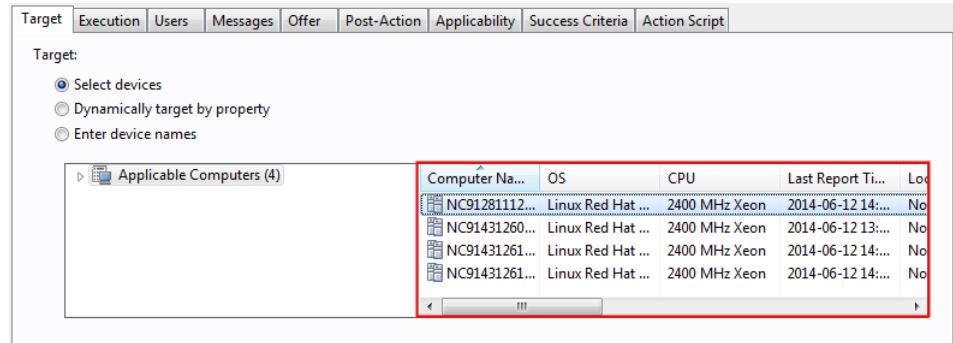
The scanner catalogs are used by the scanner to discover software on the endpoints. The catalogs are automatically updated after each import of the IBM software catalog. Use this procedure only if the automatic update of the scanner catalogs fails.

Before you begin

- Before you update the scanner catalogs manually, try to determine why the automatic update failed. For more information, see *Server operation problems*.
- Ensure that the Software Use Analysis server is visible to your Endpoint Manager server.
- If Secure Socket Layer (SSL) is enabled in Software Use Analysis, all updates are also downloaded through SSL. The Endpoint Manager server must recognize SSL certificates of Software Use Analysis as valid.

Procedure

1. Log in to Software Use Analysis.
2. **Import** the software catalog.
3. In the top navigation bar, click **Management > Catalog Upload**.
4. To download the fixlet file to your computer, click **Catalog Download Fixlet**. Choose the location where you want to save the `catalog_download.bes` file, and click **Save**.
5. Copy the file to the computer where the Endpoint Manager console is installed.
6. Log on to the Endpoint Manager console.
7. To import the fixlet, click **File > Import**.
8. Open the directory where you store the `catalog_download.bes` file, select the file, and click **Open**. The file is imported.
9. In the left pane, click **Sites > Master Action Site > Fixlets and Tasks**. A list of available fixlets opens in the upper right pane.
10. To run the fixlet on the endpoints, select **Catalog Download (SUA)**, and click **Take Action**.
11. Select the computers on which you want to run the fixlet, and click **OK**.



What to do next

You imported the scanner catalogs to the endpoints in your infrastructure. To gather inventory data from the endpoint, you must now **initiate software scans**.

Configuring data retention period

You can specify the period after which historical data from previous imports is removed from Software Use Analysis.

Procedure

1. In the top navigation bar, click **Management > Server Settings**.
2. To configure the data retention period, select the **Discard data older than** check box.

Data Retention

Discard data older than

Days

3. Specify the period after which data is to be removed, and click **Save**.

Setting the home page

If you use a particular report or panel frequently, you can set it as Software Use Analysis home page.

Procedure

- To set a new home page:
 1. Open the report or panel that you want to set as the home page.
 2. In the upper-right corner, expand the user name menu, and click **Set as home page**.
- To return to the default home page:
 1. Expand the user name menu and click **Profile**.
 2. Click **Clear** under the Home page field.

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.

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, Windows, Windows NT, and the Windows logo 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