Inventory & Software Gathering, Detection and Deployment Methods

Description	This course is designed to provide a deep understanding of some of the more complex features within Inventory and Software Management.
	This lab assumes a basic and general understanding of the Symantec Management Platform and operating system imaging. Basic Microsoft Windows skills are recommended.

At the end of this lab, you should be able to	▪ Create a Stand-alone Inventory Package.
	▪ Configure some of the advanced Inventory options.
	▪ View Custom Inventory options.
	▪ Create Software Products.
	▪ Import software packages.
	▪ Create software Applicability Rules.
	▪ Deliver software using managed delivery policies.
	▪ Create Automation Policies.

Notes	▪ A brief presentation will introduce this lab session and discuss key concepts.
	▪ Feel free to follow the lab using the instructions on the following pages. You can optionally perform this lab at your own pace.
	▪ Be sure to ask your instructor any questions you may have.
	▪ Thank you for coming to our lab session.

Table of Contents

Lab Exercise 1: Standalone Inventory

A stand-alone inventory package is an executable file that you create from the Symantec Management Console. You run the package on target computers and gather the Inventory data on that computer. This method lets you gather inventory on the target computers that are not managed through Symantec Management Agent.

This method does not apply to the following cases:

- Older or same version of Symantec Management Agent is installed on a computer.
- Symantec Management Agent is installed on a client computer but not connected to the Notification Server computer.
- Symantec Management Agent is installed on a client computer, but is broken or not functioning.
- Symantec Management Agent is installed on a client computer, but is disabled.

If you use stand-alone packages, you must be able to report the inventory data back to the Notification Server computer. You can use different options of reporting data depending on the configuration of your network. You can create multiple packages with different options according to your needs.

Creating a Stand-alone Inventory Package

1) **Make sure the SMP, DC and Win7 Virtual Machines are powered on.**

2) **Switch to the SMP Virtual Machine.**

3) Double click on the **Symantec Management Console** icon on the desktop to launch the **Symantec Management Console.**

4) Navigate to **Settings | All Settings.**

5) Expand **Discovery and Inventory > Inventory Solution**.

6) Click on **Stand-alone Inventory Packages**.

7) On the right side of the screen press **New Package** to create a new package.
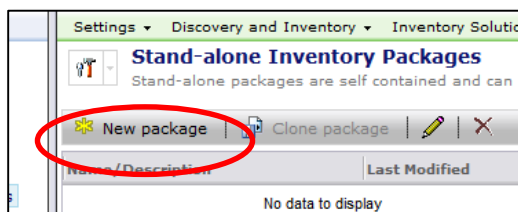

8) For the Package Name enter **My Inv Package.**

9) **Check** the following boxes:

   - ✓ Hardware and Operating System
   - ✓ Software
   - ✓ File Properties
   - ✓ Server Applications

10) Check the box to **Show progress** under "**When running on the target computer**."

11) Leave the **default Notification Server** location to send the Inventory data to.

12) Press the **Advanced button**.

13) Review the various tabs and options available to you.

14) Press **Cancel**.

15) Your package should now look like this:
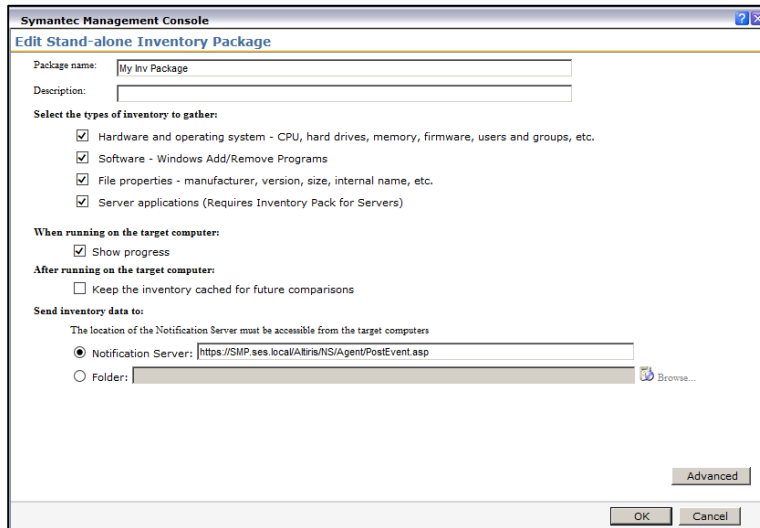
16) Press **OK.**

17) You will now be placed back at the **Stand alone Inventory Packages** page.

There are two components to this screen. The left side contains information about the names of the packages you have created. The right side of the screen display details about the selected package and also a link to download the package for distribution.

18) Click on the **package download URL** to download the package (choose the UNC path).
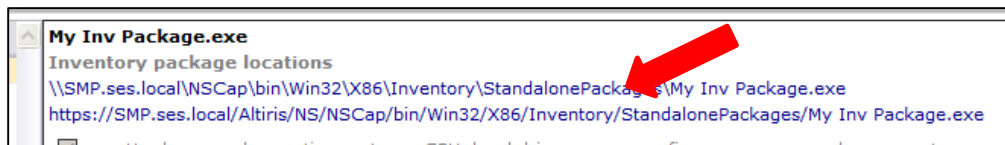
19) Select **Save As** and save the package to: **C:**

20) If you get an error, simply press the X on the window

Deploying Stand-alone Inventory Packages

1) Switch to the **Win7** virtual machine.

2) Press **Start.**

3) Type **Run** in the search box and press **Enter.**

4) Type the following command in the run box: `\\smp\c$\My Inv Package.exe`
   Press **OK.**

5) Press **Run.** The Inventory window is displayed:
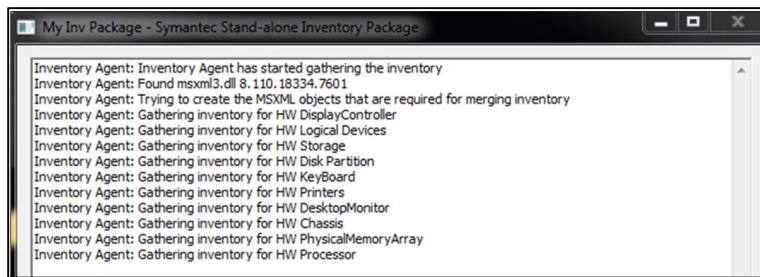
Note: This may take a few minutes to complete.

6) Press **Ok** when the inventory package finishes its scan. The operation is completed when the OK button is not greyed out.

7) No further action is required on the part of the administrator or the end user. The inventory information will be forwarded to the appropriate Notification Server and processed on schedule.

Lab Exercise 2: Advanced Inventory Configuration

Exploring Advanced Inventory Options

In most cases an administrator will want to collect as much inventory information from a client as possible. In some cases, however, there is a need to collect only a subset of the possible inventory catalog. Like all other policies in the Notification Server, Inventory Policies can be scaled down to capture only the specific details required by the administrator.

In this example we will be collecting inventory data from an ESX farm. As such we are not concerned with the hardware profiles of the machines. We need only collect software information.

1) Switch to the **SMP** virtual machine.

2) In the Symantec Management Console navigate to **Manage | Policies** in the main console menu

3) Expand the **Discovery and Inventory > Inventory** folders and note the out of the box inventory tasks are available on the left pane.

4) Right Click on the **Inventory** folder and select **New > Inventory Policy** to create a new inventory policy.
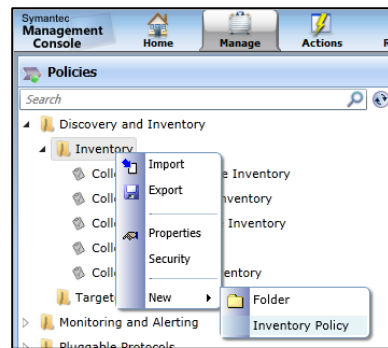
5) Name the policy **My Inventory Policy**.

6) Select the radio button labeled **Custom Schedule.**

7) Press the **Add Schedule** button.

8) Select **Scheduled Time**.

9) Leave the defaults and press **OK.**

10) Uncheck **Hardware and Operating System**.

11) Check **Software**.

12) Check **File Properties**.

13) Check **Server Applications**.

14) Press **Advanced.**

15) Under the **Data Classes** tab check the boxes for:

   ✓ Software
   ✓ Operating System
   ✓ User and Group

16) Select the **Run Options** tab.

17) <u>Check</u> the box to **Enable Verbose Client Logging**. This will provide more detailed data on the process used to gather the inventory.

18) Press **OK.**

19) In the **Applies To/Compliance** section, highlight the **SES\Administrator** line item and **delete it** (press the red X).
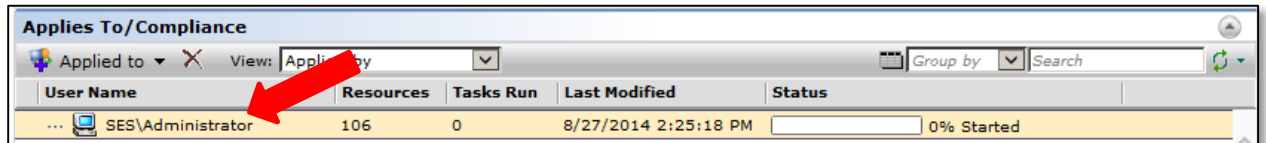
20) Enable the policy by clicking on the red orb in the upper right corner and selecting **On**.

21) Press **Save Changes**.

22) At this stage the policy has been created but not applied to any computers. In the next exercises, we will create a target and apply it to this policy.

Creating User Defined Filters

Now that your inventory policy has been created, you need to apply it to the appropriate group of resources it was intended for. In this next section we will simulate creating a custom filter. We will be using the Windows 7 lab virtual machine but this process can be applied using any number of variables.

1) Navigate to **Manage | Computers**.

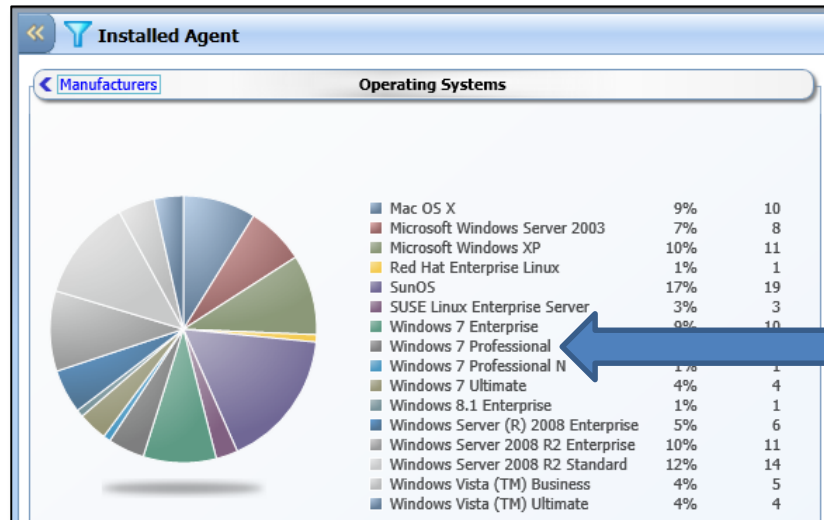2) Select the >> (double chevron) icon in the upper middle of the screen to select the **flip book**
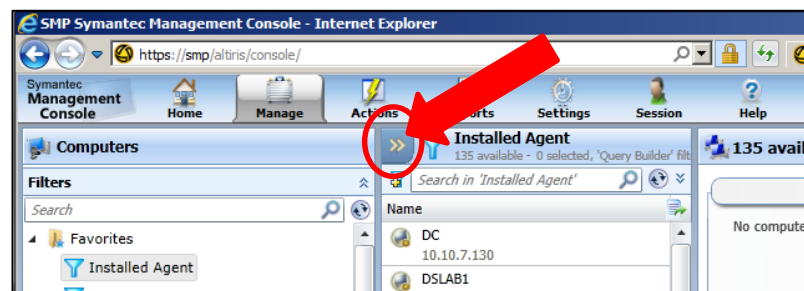
3) "Flip through" the windows by pressing the link in the right corner.
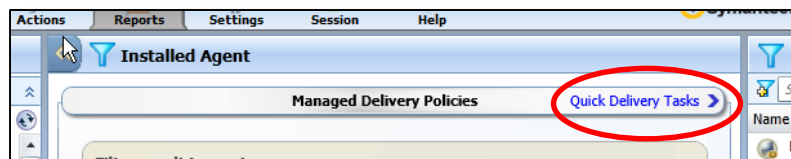
4) The next-to-the-last screen will be labeled **Operating Systems.** Stop there.

5) On the dynamic pie chart locate and select the **Windows 7 Professional** label

Note: Notice how the right hand side of the screen (*the computer list*) automatically scopes itself based on your selection.

6) Now that we have the basis of our target you may **close** (click the **>>** double chevrons) **the flip book**.

7) Your target scope has carried over and there are 5 computers with Windows 7 Professional
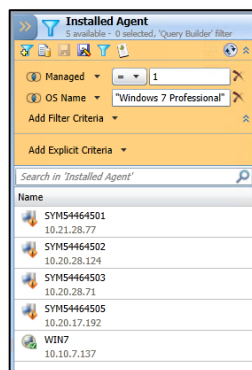
8) Now we need to filter out the objects we do not need.

9) Press the **Add Filter Criteria** button located at the bottom of the orange section.

10) Select **IP Address** from the drop down.

11) In the IP Address box type: **10.10.7.** This will only show objects with an IP address that begins with 10.10.7.

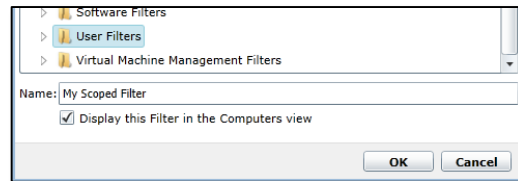12) You should now have 1 resource in view.
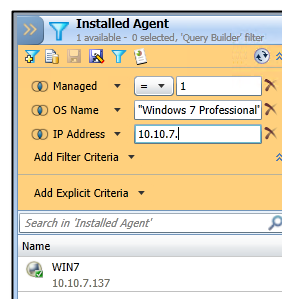
13) Press the **floppy disk** icon to save this filter.
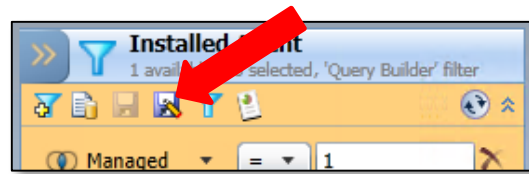
14) Name the filter **My Scoped Filter**.

15) Scroll down the list in the window and Select the **User Filters** folder.

16) Press **OK.**

Displaying User Defined Filters

By default only a certain set of filters are displayed in the Manage | Computers view. This is designed to simplify the interface. The "User Filters" folder is <u>not</u> displayed by default. In this exercise we will see how to expose the user filter folder and any additional folders that may be required.

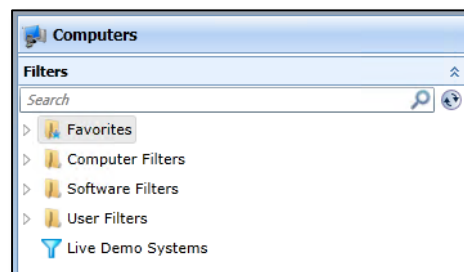1) Right click in the empty white space under the **Filters** pane.
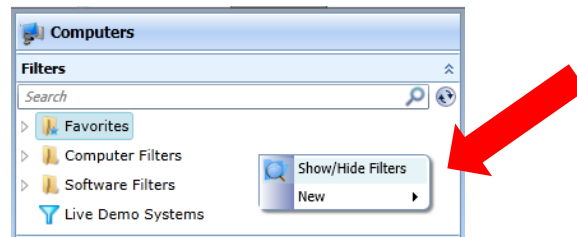
2) Select **Show/Hide** Filters.

3) Check the box for **User Filters.**

4) Press **Close.**

5) The **User Filter** folder is now available.

Creating User Defined Targets

We have learned that a filter is not an actual resource within the Notification Server; rather it is a statement that will ultimately result in a number of resources. In Notification Server terminology we call that result a Target. A target can include or exclude any number of filters, organizational groups or static resource lists. In this exercise we will create a simple target based on the previously created filter.
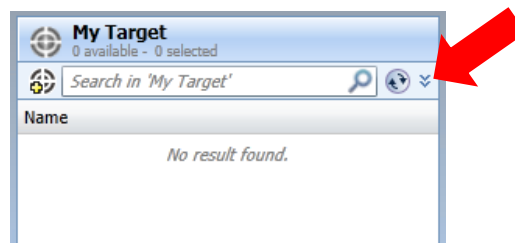
1) Right click in the empty white space under the **Targets** section.
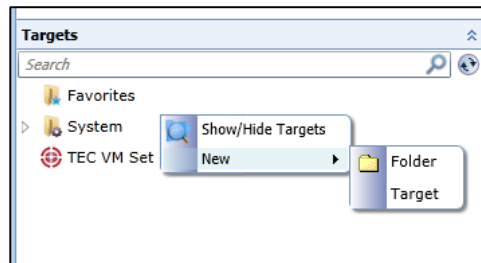
2) Select **New > Target**.

3) Name the target **My Target.**

4) Press **OK.**

5) You should now see the **My Target** object on the screen.
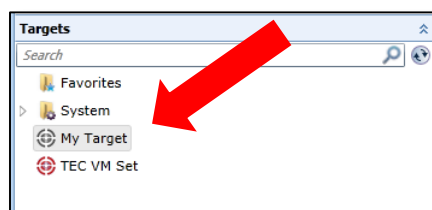
6) Select **My Target** from the list on the left pane.

7) In the middle pane, expand the target view by pressing the Double chevrons (⌄)

8) In the Orange colored area press the **Add Include/Exclude** drop down menu.

9) Select **Include** from the drop down list. The default setting is to include a filter. This can be modified to reflect a group or a list as well.

10) Click the **Select one…** link.

11) In the search box type: **My Scoped Filter** (Alternatively you may expand and select it from the folder tree).

12) Select the **My Scoped Filter** object

13) Press the single chevron **>** to include this filter in the target.
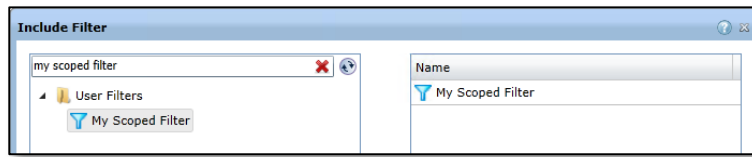
14) Press **OK.**

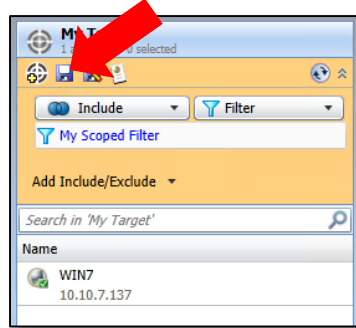15) Press the **floppy disk icon** to save the target.

16) You have successfully created a Target.

Assigning Inventory Policies to Targets

Multiple methodologies exist in the Notification Server for binding resources, policies, tasks, jobs, etc. to each other. This exercise will demonstrate the drag and drop method.

1) Select the **Policies** blade in the lower left hand corner of the screen.
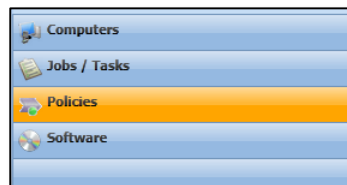
2) Navigate to **Discovery and Inventory > Inventory**.

3) Select the My **Inventory Policy**.

4) This next set of steps is completed in one fluid motion. You are going to click on the policy, drag it to the Computers blade, wait for the screen to change; and "drop" it on the My Scoped Filter that was created.

   a. Left click on and <u>hold</u> the **My Inventory Policy** object.

   b. Drag it to the **Computers** blade.
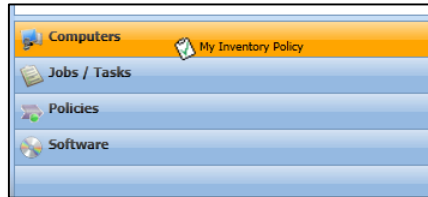
   Notice that the console changes to the Computers View

   c. While still holding the left click button move over the **My Scoped Filter** object and let go of the mouse button.
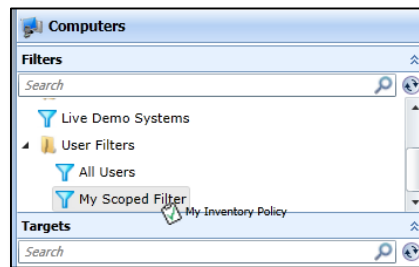
5) Notice what happens – An error window appears.
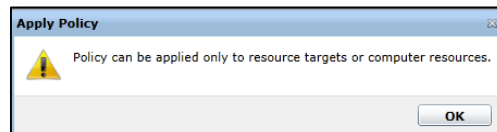
   This error occurs due to the fact that a policy can only be applied directly to a set of resources. A Filter <u>is not</u> a resource; rather it is a statement that ultimately results in a set of resources. Drag and drop functionality is resource to resource (e.g. dragging a software package on to a computer resource).

6) Press **OK.**

7) Press the **Policies** blade.

8) This time drag the policy on to the **My Target** object (instead of the My Scoped Filter object).
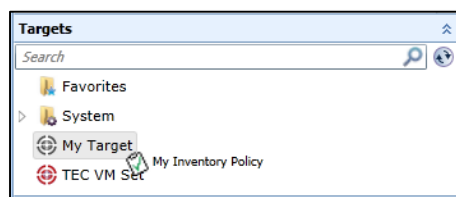
9) The operation will produce a window that verifies that you would like to complete this task.
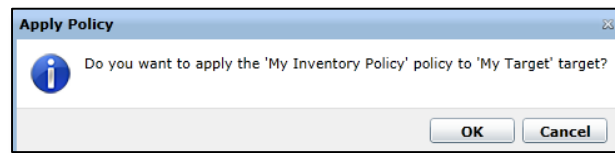
10) Press **OK.**

11) **Notice that your target has been added to the Applies to area of the policy**

12) Press **Save Changes** on the My Inventory Policy window.

13) You have successfully applied your policy to your target. This inventory policy will run on the Win7 Virtual machine sometime during this lab.

At their most basic level, policies, filters and targets are ultimately this simple. They can, however, become infinitely complex based on the number of inclusions and exclusions they contain. Think of the statement they make as a mathematical equation:
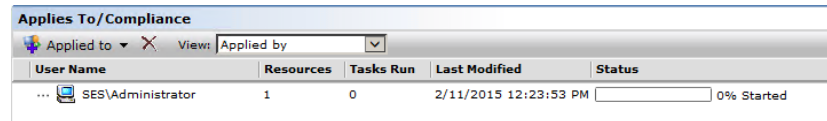
Inclusions(Filters, Organizational Groups, Lists) [–] Exclusions(Filters, Organizational Groups, Lists) = Target.

Lab Exercise 3: Complex Software Delivery Policies

Software Management Solution is a component of IT Management Suite that allows you to manage basic to advanced software implementation scenarios. It works in conjunction with portions of Inventory Solution to provide you with holistic control of your environment. We will use this exercise to create a software product out of a discovered piece of software. We will then investigate scenarios for deploying that software product in the environment.

Creating Software Products

1) In the Symantec Management Console navigate to **Manage | Software.**

   Multiple packages have been pre-loaded and detected beforehand to provide illustrative examples of what a real world environment would look like.

2) Expand the Favorites folder and select **Discovered Unreviewed Software** in the left pane.
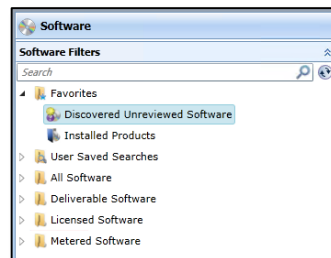
3) In the search box found in the middle pane type: **Microsoft Visio**

4) Locate and select **Microsoft Visio Viewer 2013 English x64**.

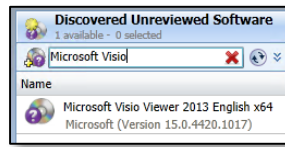5) On the right side of the screen (called the Flip Book) click the **Manage this software** link. The software product window appears.

6) For the **Name**, re-type it as **Microsoft Visio Viewer 2013 x64**.

7) In the category drop down select **Desktop Application** from the list.

8) **Review** the information on the Identify Inventory tab, and notice that there is information pre-populated and that there is 1 Installation found.
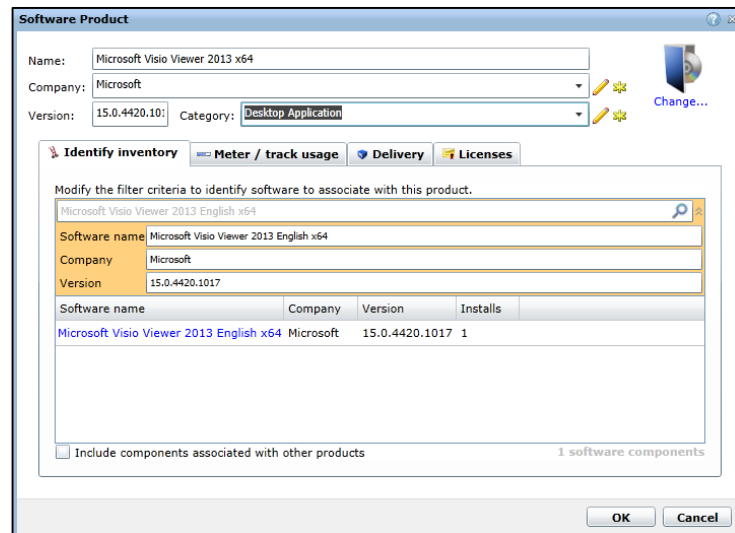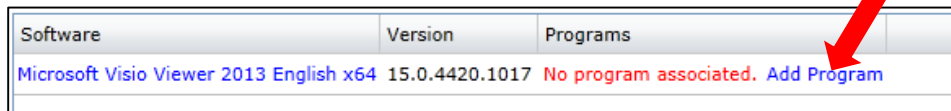
9) Select the **Meter / track usage** tab.

This option lets you perform the following tasks on your managed Windows Computers:

- Track usage of the managed software at the software product, component, and version level by enabling the software-based usage tracking option. This task is the primary method to use for the majority of software products.

- Meter the use and control the availability of applications by running predefined or custom application metering policies. Symantec recommends that you use this task only if you need to meter start, stop, and denial events for applications at the file level.

- Deny multiple applications from running by configuring the predefined Blacklisted Applications policy or running custom application metering policies.

10) Click the **Add Program** link on the Visio line item.

Software	Version	Programs	
Microsoft Visio Viewer 2013 English x64	15.0.4420.1017	No program associated. Add Program	

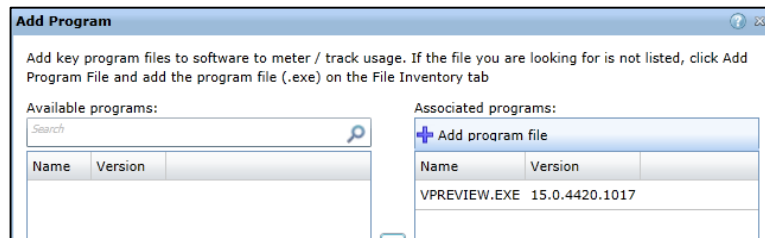11) Notice that it is already aware of the executable associated with the Visio Viewer application.

12) Select **VPREVIEW.EXE** from the list and press the **>** (chevron button) to move it to the associated programs list.

Add Program

Add key program files to software to meter / track usage. If the file you are looking for is not listed, click Add Program File and add the program file (.exe) on the File Inventory tab.
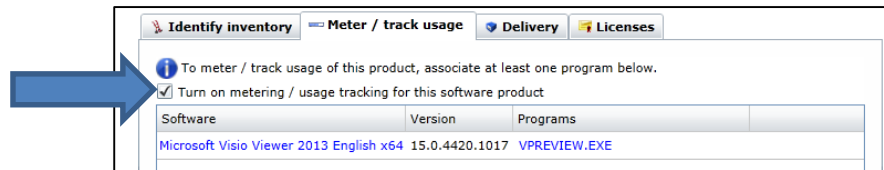
Available programs:

Search

Name	Version

Associated programs:

➕ Add program file

Name	Version
VPREVIEW.EXE	15.0.4420.1017

13) Press **OK.**

14) Make sure that the Check box to Turn on metering / usage tracking is selected

Identify inventory | **Meter / track usage** | **Delivery** | **Licenses**

ⓘ To meter / track usage of this product, associate at least one program below.

☑ Turn on metering / usage tracking for this software product

Software	Version	Programs
Microsoft Visio Viewer 2013 English x64	15.0.4420.1017	VPREVIEW.EXE

15) At this time a Visio Viewer application is not included in our Software Catalog and cannot be deployed to targeted computers. The following steps will demonstrate how we can import software into the software catalog for deployment.

16) Select the **Delivery** tab.

17) Press the **Import** button. The Import Software form loads.

   ***Press **Run** if you receive the Java Security prompt.

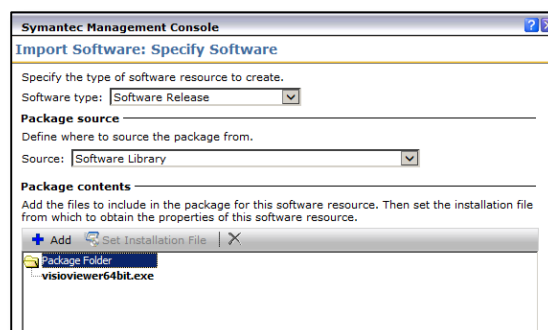18) Make sure Software Type is set to **Software Release** (default).

19) Verify that Source is set to **Software Library** (default).

20) Press **Add.**

21) Navigate to `C:\Lab Resources\SoftwareResources\WindowsSoftware`

22) Select **VisioViewer64bit.exe** from the list.

23) Press **Open**. You will now see that visioviewer64bit has been added to the package contents.

Symantec Management Console

Import Software: Specify Software

Specify the type of software resource to create.

Software type: Software Release ▾

Package source

Define where to source the package from.

Source: Software Library ▾

Package contents

Add the files to include in the package for this software resource. Then set the installation file from which to obtain the properties of this software resource.
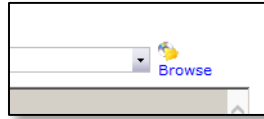
➕ Add 🔄 Set Installation File | ✕

📁 Package Folder
  visioviewer64bit.exe

24) Press **Next.** The package uploads and imports into the Software Library.

25) Select the **Update an existing software resource** radio button. It is a best practice to Update an existing package to ensure that there is only one version of it in the CMDB.

26) Press **Browse**.

27) Type **Visio Viewer 2013** in the search box.

28) Select **Microsoft Visio Viewer 2013 x64** from the list.

29) Press **OK.**

30) Press **OK** again to close the software import screen.

31) The Package view opens. Select the **Package** tab.
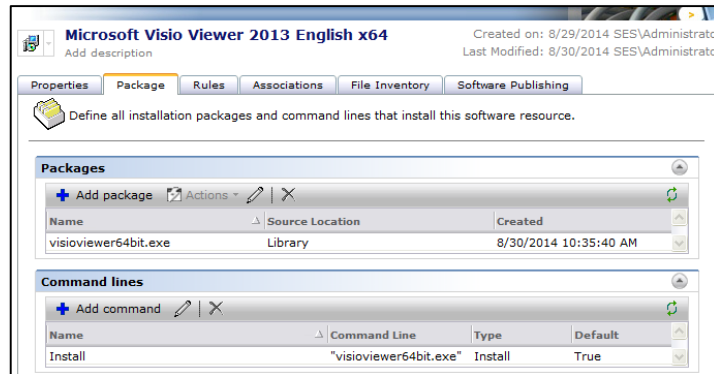
Note: A default command line is always created when a package is imported. However, unless the package is an MSI, RPM, DMG, or PKG, the default command line will likely not be sufficient. Regardless of what command lines are created Symantec recommends you test EVERY software deployment scenario BEFORE you roll it out in a production environment.

32) Highlight the **Install** command and press the pencil icon to edit it.
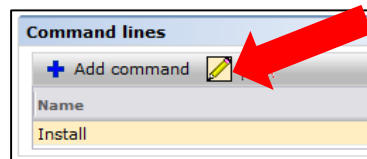
33) In the **Command Line** field append the command with the following text (after the quotes):

/passive /quiet
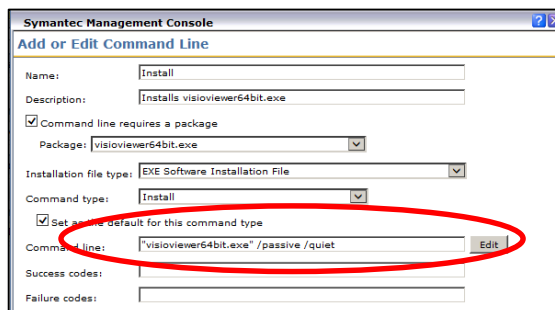
34) Press **OK.**

35) Explore the **Rules and Associations** tabs. Note how they are empty. This information is populated one of several ways. The two most common are via a package import (an MSI import will create an MSI Product Code detection rule) or after an Inventory scan has been run AND the package has been associated with a detected piece of software (the software must be installed and inventoried on at least one endpoint for this to work). We will revisit this later in the lab.

36) Press **OK** to close the Package Resource window. You are now back at the Software Product wizard.

37) Your screen should now look like this:
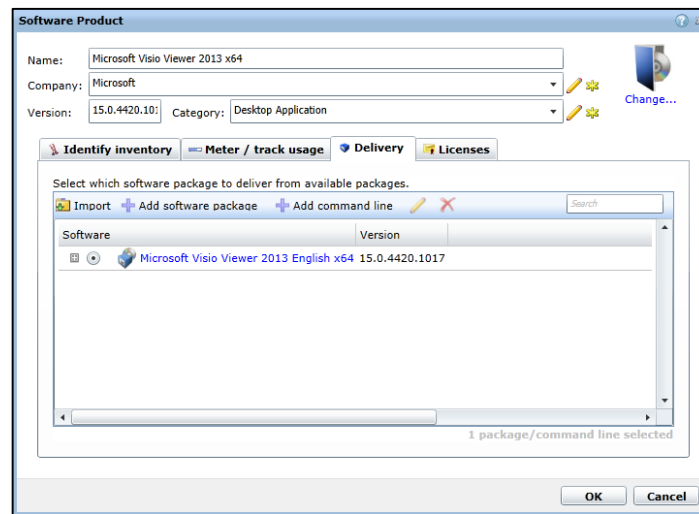
38) Press **OK** to close the Software Product wizard.

39) Expand Deliverable Software and select **Software Products** from the left pane.

40) You should now see the **Microsoft Visio Viewer 2013 x64** software product displayed in the middle pane. You have successfully created a Software Product.

41) Notice that the Icon for Visio Viewer is the default icon. If you would like to have a company logo or product icon for this product, complete the following steps:

    a. Double click on the **Microsoft Visio Viewer 2013 x64** software product in the middle pane.

    b. Select the "**Change…**" link under the icon on the top right corner

    c. Browse to `C:\Lab Resources\Inventory Solution\Visio Viewer.png`

    d. Press **Open**. Notice that the icon changed.

    e. Press **OK**

**NOTE:** Many manufacturer icons are included and can be found and selected by browsing to:

C:\Program Files\Altiris\ActivityCenter\Web\ClientBin\img\product
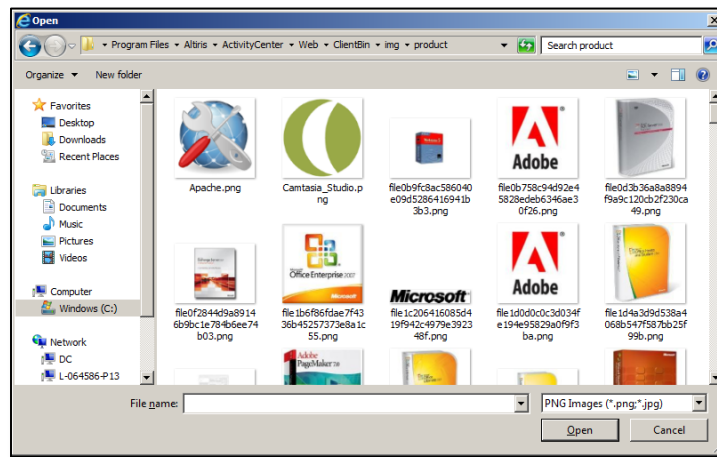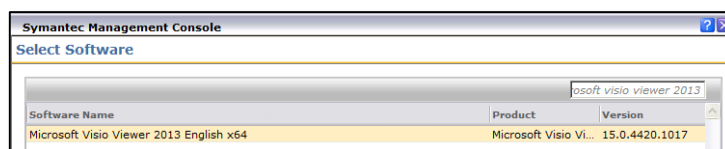
Creating Software Detection Rules

Software detection rules are the basis for advanced software management. They utilize a set of IF, THEN statements and Boolean arguments to determine whether or not a piece of software is installed on an endpoint. The most straightforward way of detecting software is to look for an MSI product code, look in Add/Remove Programs or look for a specific file. Any, all and a few more additional rules may be used to detect software all at the same time. This would ensure a granular account of software resources in the environment.

1) Navigate to **Manage | Software**.

2) In the left pane, expand **Deliverable Software** and select **Software Releases.**

3) Locate and select the **Microsoft Visio Viewer 2013 English x64** software package.

4) Double click on the **Microsoft Visio Viewer 2013 English x64** software package to edit the software resource.

5) Select the **Rules** tab.

6) In the **Detection Rule** section press * **New.**
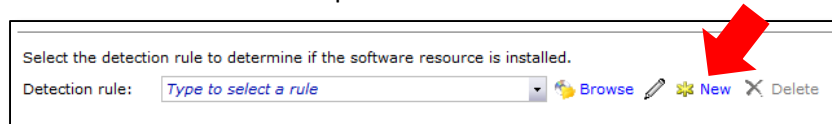
Understand that these detection rules can end up being quite complex. It is always recommended to keep them as simple as possible. If a Registry Key will accurately detect a product then there is no need to add an additional statement for Add/Remove Programs.

7) Name the rule **My Detection Rule**.

8) Press the **+** sign to create a new rule expression.

9) Select **Smart Rule > Software File Expression**.

10) Click the **Select a Software Resource** link to browse the software catalog.

11) Type **Microsoft Visio Viewer 2013** in the search bar.

12) Locate and select **Microsoft Visio Viewer 2013 English x64**.

13) Press **OK.**

14) Your screen should now look like this:
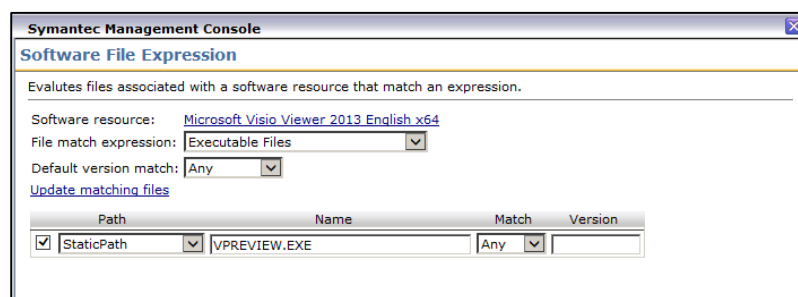
15) Press **OK.**

16) Press **OK** to close the Create Rule form. You have successfully created a Detection Rule.

17) IMPORTANT: Leave the Package Resource Editor open for the next exercise!

Software Dependencies & Applicability Rules

Software dependencies & applicability rules are the pieces of logic that allow you to deploy one software policy to thousands of computers without having to worry about whether or not the appropriate prerequisites exist on the end point. They are not designed to be a "lazy way" of deploying software to the masses, rather they are built it check points to make sure mistakes are avoided.

A Software Dependency is a piece of logic that check the endpoint for a value or set of values and then returns a status. If the status is negative (the dependency is not met) then the rule fails and the software is not installed. In some cases, dependences can be applied "on demand" if they are not met (e.g. deploying the required Java client if it is not on the endpoint).

An Applicability Rule is almost identical in structure but serves a different purpose. Where a dependency rule validates *if* a software package has all of the necessary components an Applicability Rule validates if the software *can* be installed at all (e.g. this software package applies to 32-bit systems only).

There are many cases where the same logic could be used in either place. The ultimate decision boils down to remediation. Software Dependencies can be remediated. Applicability Rules (by nature) cannot be.

Creating a Basic Applicability Rule

1) While still in the Software Package Resource Editor press the ***New** button located next to **Applicability Rule.**
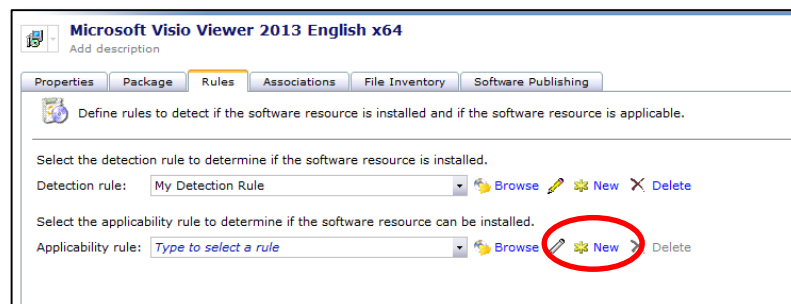
2) Name the rule **My Applicability Rule**.

3) Press the + button to add a new Expression.

4) Select **Operators > Not**.

5) Select the **Not** operator on the left pane.

6) Press the **+** button to add a new expression.

7) Select **Standard Rule > 64-bit Windows Installed**.
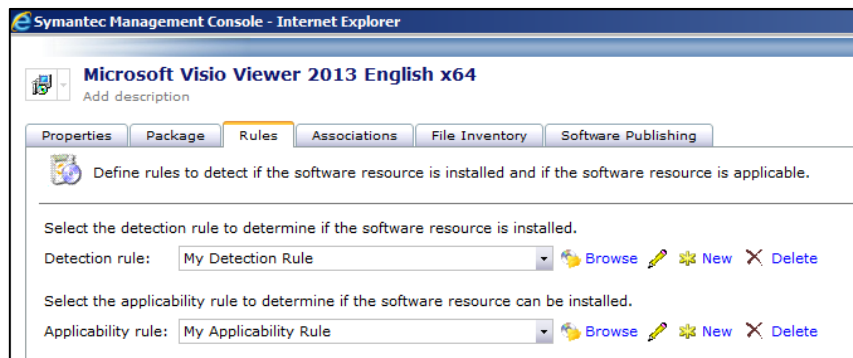
8) Press **OK.**

9) Your rule should now look like this:
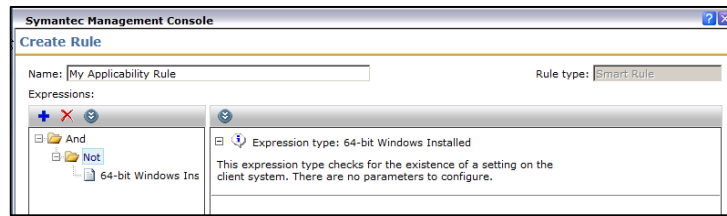
> **Note:** Pay close attention to the rule logic. The statement reads "And Not 64-bit Windows Installed." In plain English; do not execute on x64 based systems.

10) Press **OK.**

11) Your screen will now look like this:

12) Press **Ok** to close the Package Resource Editor.

Using Advanced Delivery Policies to Deploy Software

Now that we have created a Software Product with install command and some logic rules, it is time to test the deployment of this software product.

1) Switch to the **Win7** virtual machine.

2) Open the **Symantec Management Agent** by double clicking the icon in the taskbar.
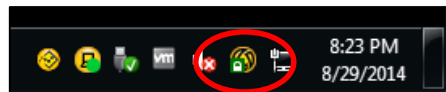
3) **Press the Software Delivery Tab**. Leave this window open for now. We will be switching back and forth to the SMP virtual machine to watch the software policy be deployed.

4) Switch to the **SMP** virtual machine.

5) Navigate to **Manage | Software** if it is not already open.

6) Expand the **Deliverable Software** folder and select **Software Products** from the left pane.

7) Right click on **Microsoft Visio Viewer 2013 x64**.

8) Select **Actions > Managed Software Delivery**.

9) Review the defaults and press **Next.**

10) In the **Select Destinations** screen press the **Apply to** button.

11) Select **Quick Apply**.

12) In the search box, type **My Target**.

13) Select **My Target** from the list and press >.
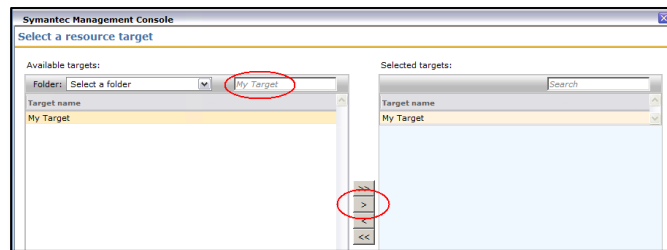
14) Press **OK**.

15) Press **Next.**

16) In the **Choose when to check compliance** section press **Add Schedule.**

17) Select **Schedule Window**.

18) Set the Schedule Window to check every **5 Minutes.**

19) Press the **No repeat** link.

20) Select **Day** from the drop down.

21) Press **OK**

22) Your window should look like this:
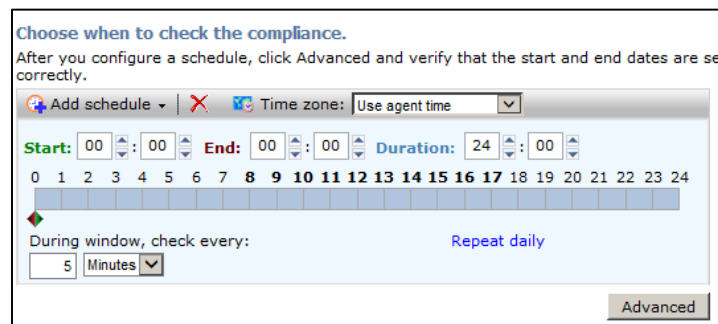
23) Press **Next** to continue the wizard.

24) Press **Deliver Software**.

25) Switch to the **Win7** virtual machine. In a few moments the policy will be delivered.

26) To speed the process up you can press the **Update Configuration** button at the top of the agent window.

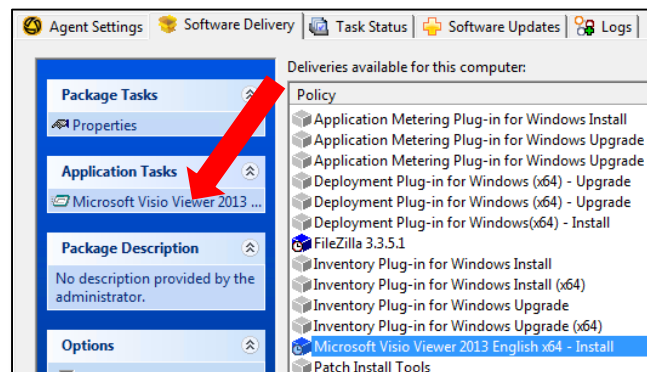27) You will see the software policy in the **Software Delivery** tab.

28) Select Microsoft Visio Viewer 2013 English x64 – Install from the list.
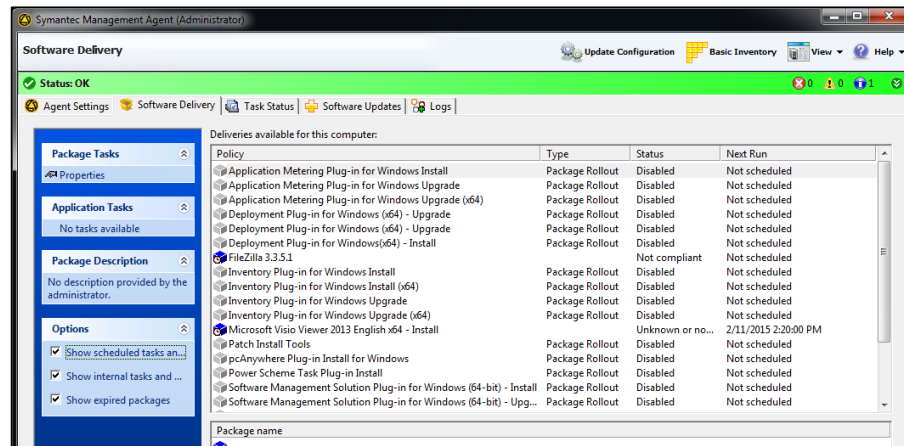
29) After a few minutes have passed you will see the four step process for the policy attempting to install the package in the bottom half of the Software Delivery window. This process will:

- Check to see if package has been downloaded.

- Run Applicability Rule to see if package *can* be installed*.

- If Applicability Rule passes then download package.

- Execute command line to install package.

30) To speed up the process, under **Application Tasks** on the left, select the "**Microsoft Visio Viewer 2013…**" link. This will execute the policy immediately.


31) As you can see from the screenshot below our policy stopped at step 2.

This is because the "only install on x64 base systems" Applicability Rule failed. This process demonstrated how rules can affect the way a policy behaves.

Removing the Applicability Rule from the Policy

1) Switch to the **SMP** virtual machine.

2) Navigate to **Manage | Software** if it is not already open.

3) Select **Deliverable Software > Software Releases** from the navigation pane.

4) Double click on the icon for **Microsoft Visio Viewer 2013 English x64.** The Package Resource Editor opens.

5) Select the **Rules** tab.

6) Locate the Applicability Rule **My Applicability Rule** and press the **Delete** link.
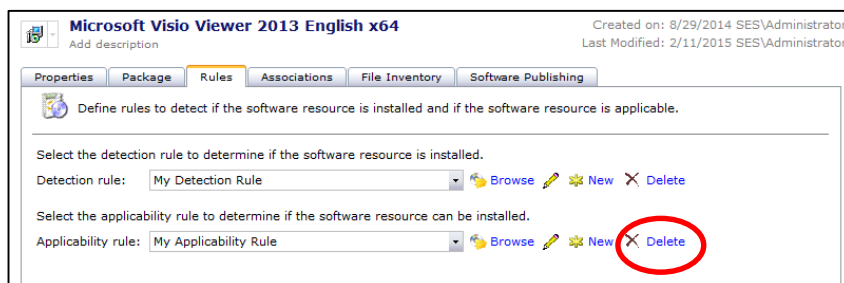
7) Press **OK** to confirm the delete.

8) Press **OK** to close the Package Resource Editor.

9) Switch to the **Win7** virtual machine.

10) Now that the package rules have been updated it is only a matter of time before the client checks in to the Notification Server and updates its policy information. This should take less than 5 minutes (Or press the Update Configuration button in the Symantec Management Agent on Win7).

    Note: Nothing will happen at this point. No matter how long you wait. Can anyone guess why? Hint: there is a clue in the statement for question 10. Your instructor will explain.

11) Note the absence of the Applicability Rule check:

12) Once you see a **Success** message displayed next to the **Execute Install Command**

13) In Windows, open **Control Panel | Programs | Uninstall a program** to validate that the Visio Viewer has been successfully installed.

Lab Exercise 4: Automation Policies

Automation Policies allow an administrator to automate reoccurring tasks within the Notification Server. They can be as simple as assigning a user to a location based on computer name or as complex as automatically assigning contracts to locations based on the amount of software installed in a particular location. For this exercise we are going to demonstrate how a computer resource can be moved into an Organizational Group based on the computers IP Schema found by Inventory Solution.

Creating an Automation Policy

1) On the **SMP** virtual machine open the **Symantec Management Console**.

2) Navigate to **Manage | Organizational Views and Groups** in the console main menu

3) Right click on the **Organizational View** folder on the left pane and select **New > Organizational View**

4) Name the new view **Machines by Subnet**

5) Right click on the **Machines by Subnet** organizational view on the left pane and select **New > Organizational Group**

6) Name the new group **Subnet: 10.10.7.x**

7) Select the view **Subnet: 10.10.7.x** group**.** Notice that there are no resources in the Group.
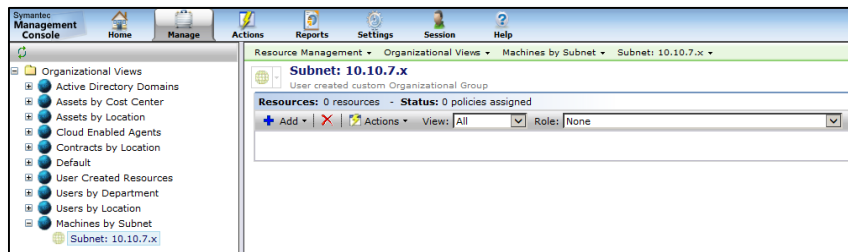
8) Navigate to **Manage | Policies**.

9) Select the **Automation Policies** link on the left pane

10) Create a new policy by pressing the **New policy** button on the right pane.

11) Name the policy **My Automation Policy**.

12) Set the schedule to **Repeat every 5 minutes** starting today.
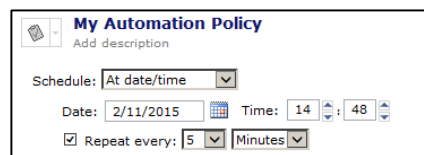
13) In the Data Source drop down select **Raw SQL Query.** Notice you can choose a report or Resource Query if you wish. Most users choose a custom report that was previously created.

14) Press **Edit Query**.

15) Type the following query into the blank area:

```
SELECT _ResourceGuid
FROM Inv_AeX_AC_TCPIP
WHERE [IP Address] Like '10.10.7.%'
```

16) This query simply returns the GUID of any computer that has an IP address in the 10.10.7.x subnet range

17) Select the **Results** tab.

18) You should now see the GUID's of 4 computers who have an IP Address that starts with 10.10.7.

19) Press **OK.**

20) Under **Evaluation Rule** choose **Run for non-empty data** from the drop down.

21) Press **select a job or task**.

22) Expand **System Jobs and Tasks > Notification Server > Automation Policy Tasks**.

23) Select **Assign to Organizational Group**. This step simply selects the task you wish to run in the Automation Policy – it is not configured here – it is a read only task.
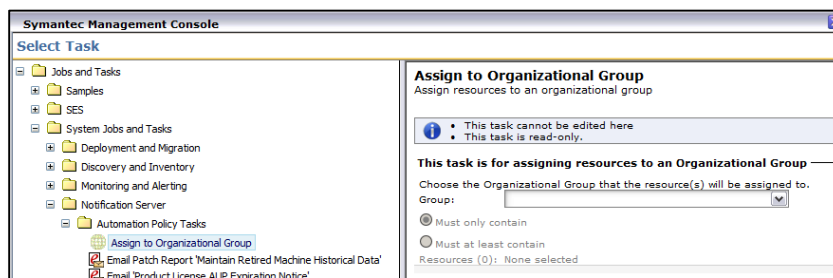
24) Press **OK**

25) Press **Edit Input Parameters.** This is where we enter the parameters that are needed by the previously selected task. We will need to know the Organizational Group we want to send the resources to.

26) In the Organizational Group drop down, select **[Custom]** then on the right dropdown, choose **Machines by Subnet > Subnet: 10.10.7.x**
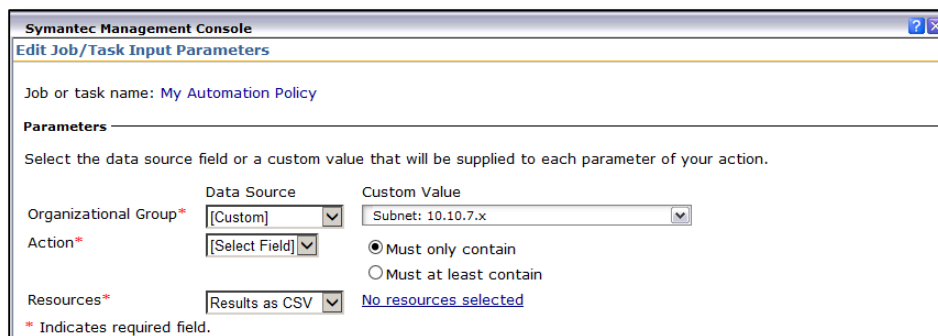
27) In the Resources drop down, select **Results as CSV.** This will ensure that the GUID's are compatible to the task (text instead of another format).

28) Press **OK.**

29) Press **Save Changes** to save the automation policy.

30) Press **Test Automation Policy** to verify the automation policy is working.

31) Navigate to **Manage | Organizational Views and Groups** in the main console menu.

32) Expand **Machines by Subnet > Subnet: 10.10.7.x** on the left pane.

33) Verify that our 4 resources have been moved to the organizational group. This automation policy is set to run every 5 minutes and will add any new resources to this group if they are part of the 10.10.7.x subnet.

Lab Exercise 5: Custom Inventory

Custom Inventory is designed to extend the functionality of Inventory Solution by allowing an administrator to collect data points outside of what is included by default with Inventory Solution. First, a custom data class is created to store your information in the database. Then some methodology for collecting the data point (typically a script of sorts) is executed on the endpoint(s) to gather the data. Once the data is on the Notification Server it is managed like any other piece of information.

Collecting Custom Inventory

1) **Switch to the SMP Virtual Machine**

2) Open the Symantec Management Console if it is not already open.

3) Select **Manage | Computers**

4) Select **All Computers** under the **Computer Views and Groups** view on the left pane

5) Find **SMP** in the list and double-click on it. The Resource Manager will open.

6) Select **View > Inventory** on the top menu

7) In the middle pane, expand the **Data Classes > Inventory** folder

8) Look for a folder called **Custom** - You will notice that it does not exist. This is where custom inventory data will be stored.

9) Close the **Resource Manager** window.

10) Navigate to **Manage | Jobs and Tasks**.

11) Expand the **Samples > Discovery and Inventory > Inventory Samples > Custom** folder

12) Select **Custom Inventory – Processor** from the list.

13) Notice that this is just a **Run Script** task rebranded as a custom inventory.
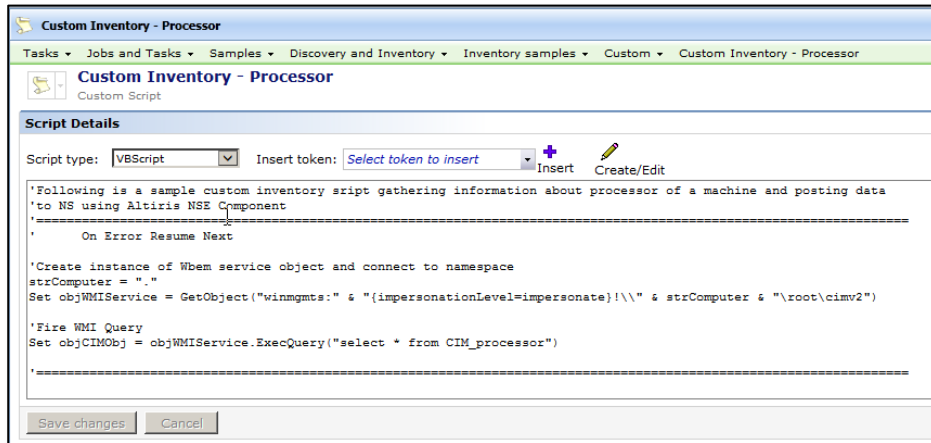
You can see that the script type is set to **VBscript.** You can choose a multitude of programming languages to feed data into the CMDB. You can read and research further information on the VBscript programming language on the internet.

14) Select the **Quick Run** under **Task Status**, type **SMP** and from the drop-down menu, select SMP as the resource you want to run this on.
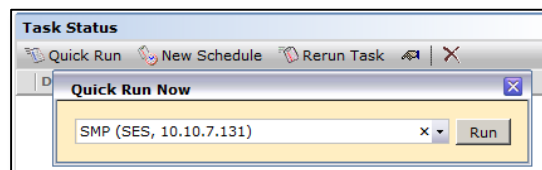
15) Press **Run**.

16) It should only take a few seconds for this task to run.

17) Double click on the **Symantec Management Agent** in the system tray.

18) Select the **Task tab** and notice that the **Custom Inventory – Processor** task ran.

19) In the console main menu Select **Manage | Computers**.

20) Select **All Computers** under the Computer Views and Groups view on the left pane.

21) Find **SMP** in the list and double-click on it. The Resource Manager will open.

22) Select **View > Inventory** on the top menu.

23) In the middle pane, expand the **Data Classes > Inventory** folder.

24) You will now notice that there is now a custom folder and inventory data in this data class called **Processor Extension**.

25) Close the Resource Manager window.

Creating a Custom Inventory Task

In this example the Administrator is tasked with tracking the service state of the Print Spooler service on a target group of computers. In order to complete this task, the following must be accomplished:

- Create a Custom Data Class through the Manage Custom Data Classes item

- Create a Custom Task VBScript that collects the data from a computer resource and places it in the created Custom Data Class
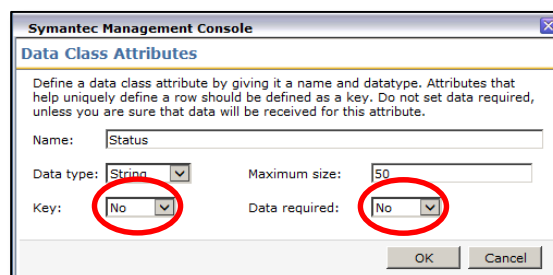
Creating the Custom Data Class (Table/Fields)

To get this data into the CMDB we will need to create a custom data class for inventory to place the collected data into.

1) Open the **Symantec Management Console**.

2) Select **Settings | All Settings**.

3) Expand **Settings > Discovery & Inventory > Inventory Solution**.

4) Select **Manage Custom Data Classes**.
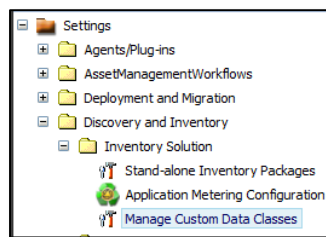
5) Press the **New Data Class** button in the middle pane.

6) Name it **Monitor Spooler Service**.

7) Press **OK**.

8) Make sure the **Monitor Spooler Service** data class is selected.

9) Press the **+ Add Attribute** button on the right pane.

10) Type **Status** in the **Name** field.

11) Ensure that you select NO to Key, and NO to required like the following:

12) Press **OK**.

13) Your managed custom data classes should look like the following now:
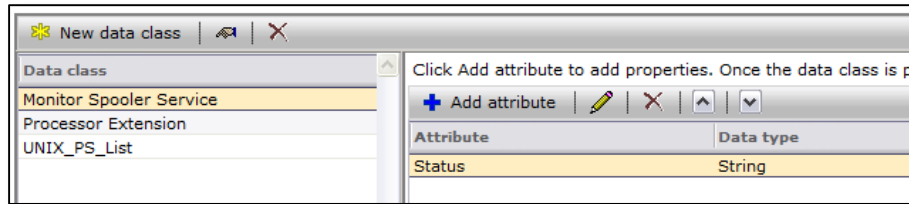
14) Press **Save Changes**

15) You have now made a data class for the custom Inventory script to populate.

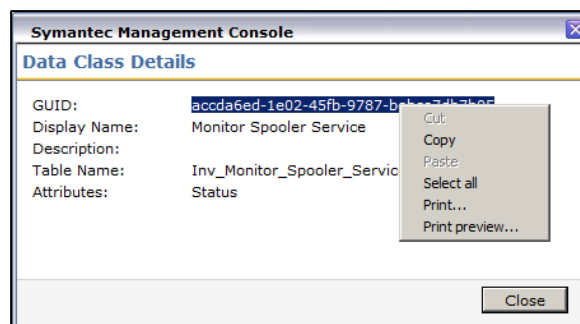## *Creating the Custom Inventory Script*

Now we need to create an initial VBScript Task that will be executed on a computer resource. But before we do that you will need to configure a pre-made script that has been written and modify it so it now collects data and places it in the data class we just created.

This script was created by taking the base script in the Processor Extension example provided in the default installation of the Symantec Management Platform.

1) In Windows Explorer, browse to: `C:\Lab Resources\Inventory Solution\Check Service Example`

2) Double-click **Checkspooler.txt** to open it in Notepad.

3) Look for the line with **("{XXX}")** in the script. It will need to be updated with the GUID of the dataclass we just created.

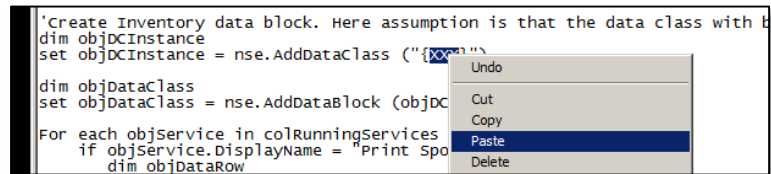4) In the console, make sure **Monitor Spooler Service** is selected and press the **Properties** button.
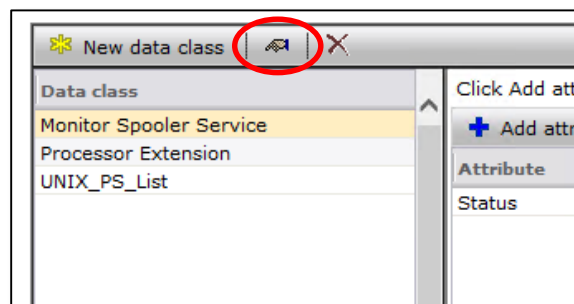
5) Highlight the GUID, right-click it and select **copy**.


6) Press **Close**.

7) Return to the **Checkspooler.txt** file and replace the **XXX** letters with the copied GUID. Make sure there are no spaces between the { and }.


8) Save the script, but keep it open.

Creating the Custom Inventory Task

1) You are ready to create the task and associate a schedule to it to collect this information.

2) From the Symantec Management Console select **Manage | Jobs & Tasks**.

3) Expand the **Samples > Discovery & Inventory Inventory Samples > Custom** folders.

4) Right Click on the **Custom** folder and select **New Task**. The Create New Task window appears.

5) Scroll down the list in the left pane and near the bottom, select **Run Script**.

6) Name the task **Monitor Spooler Service**.

7) Select **VBScript** for the **Script Type**.

8) Return to the **Checkspooler.txt** and copy the contents of the file.

9) Return to the **Monitor Spooler Service** task and **Paste** the contents into the blank area.
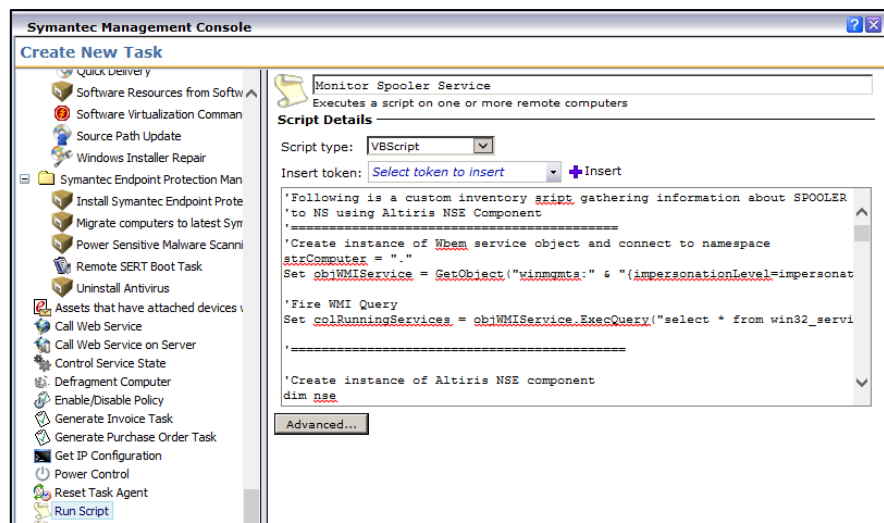
10) Press **OK**

11) Once you have finished saving your Task, it should look something like the following:
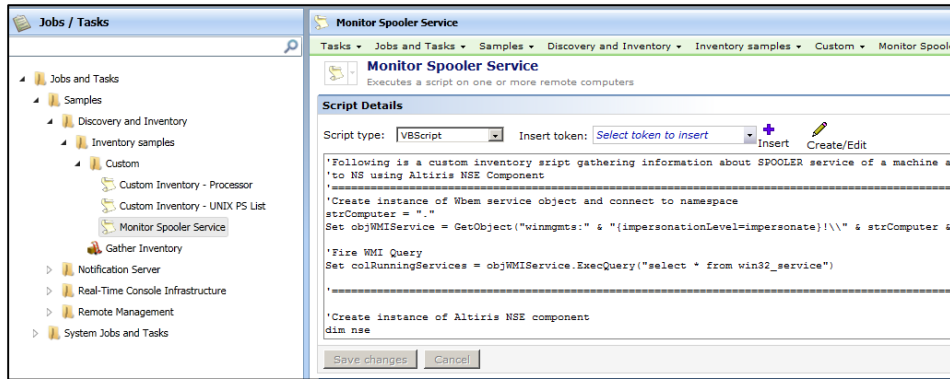
12) Open a Command Prompt and type `net stop spooler` then press enter.

13) The following will appear indicating that your command executed correctly

    ```
    The Print Spooler service is stopping.

    The Print Spooler service was stopped successfully.
    ```

14) Perform a quick run to run the task against the SMP virutual machine by selecting the **Quick Run** button under **Task Status** and selecting **SMP** as the Resource you want to run this on.
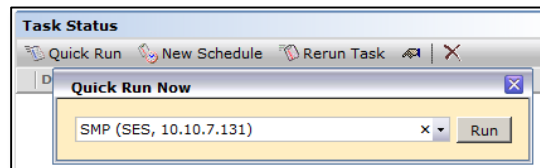
15) Press the **Run** button. It should only take a few seconds for this task to run.

16) Double click on the **Symantec Management Agent** in the system tray.

17) Select the **Task tab** and notice that the **Monitor Spooler Service** task ran.

18) In the console main menu, select **Manage | Computers**

19) Select **All Computers** under the Computer Views and Groups view on the left pane

20) Find **SMP** in the list and Double Click on it. The Resource Manager will open

21) Select **View > Inventory** on the top menu

22) In the middle pane, expand the **Data Classes > Inventory > Custom** folder

23) Select the **Monitor Spooler Service** data class and note that the status indicates **Stopped**.

Scheduling the Custom Inventory Task

Once you have verified that everything is working you can now schedule the script for daily/hourly runs an a targeted group of computers. In this case the Administrator has been asked to target all Windows Servers.

1) Return to the console and select **Manage | Jobs and Tasks**

2) Highlight the **Monitor Spooler Service** task

3) On the right pane, select the **New Schedule** button on the bottom of the pane.

4) In the New Schedule Window select the **Schedule** radio button and select **At date/time** in the drop-down.

5) Check the **Repeat every** box and select **30 Minutes**.

6) In the **Selected Devices** area, press the **Add** dropdown list and select **Target**.

7) Press the **Open** button and search for and select **All Windows Servers**.

8) Press **OK**.

9) Press **OK**.

10) Press **Schedule**.

This has demonstrated to you how to create a custom inventory in a windows environment and provide a mechanism for collecting custom inventory from a machine and viewing that information

----END OF LAB----