Creating Automatic Inclusion Rules for Monitoring Policies

https://campus.barracuda.com/doc/99619180/

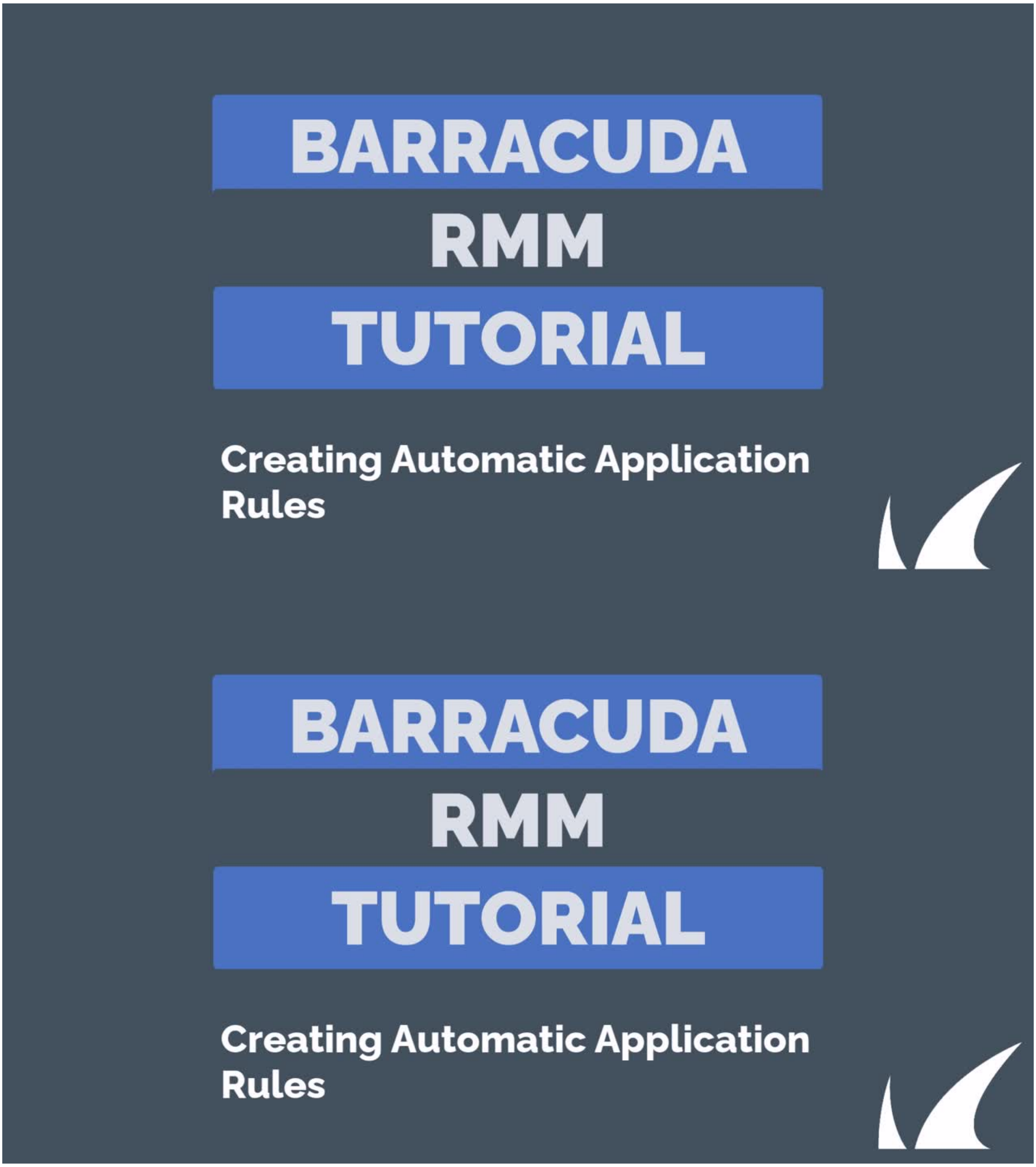
You can create automatic inclusion rules to define the criteria a device must meet to be monitored by the monitoring policy. Devices that match the inclusion rules are automatically monitored. If a device no longer meets the rule criteria, it is automatically removed from monitoring. Automatic inclusion rules only go into effect when you add the monitoring policy to a service, which is then applied to a site or group either directly or as part of a service plan. You can also associate the monitoring policy with a site or service group. For more information on creating and managing service plans, see Creating Service Plans.

Rules are created by first defining **AND** and **OR** statements, then by adding rules to the statements. For example, if you are creating a rule to automatically monitor all devices running on a **Windows 7** operating system, in the default **AND** group, you would specify that the **OS Name** contains "**Windows 7**".

To create a rule that specifies that the device must either have a **Windows 7** or **Windows 2008** operating system, you would change the **AND** group to an **OR** group, and then add a second rule that specifies that the **OS Name** contains "**Windows 2008**".

For more examples of automatic inclusion rules, see Automatic Inclusion Rule Examples.

Setting up Automatic Application Rules


BARRACUDA
RMM
TUTORIAL
Creating Automatic Application Rules
BARRACUDA
RMM
TUTORIAL
Creating Automatic Application Rules

Videolink:

https://campus.barracuda.com/

(13 minutes)

Planning out automatic inclusion rules

Creating automatic inclusion rules will usually be simple, but because you can put together very sophisticated rules, it's best to come up with a statement about the rule before you get started. Here are some example rule statements:

- If the device must be a firewall, the rule statement would simply be: **firewall**.
- If the chassis type must be a laptop, and the operating system must be **Windows 7**: **(Chassis type is laptop) AND (OS is Windows 7)**.
- The network service must be **HTTP** or **HTTPS**: **(HTTP) OR (HTTPS)**.
- The domain role must be a member workstation or a member server, and the operating system must be **Windows 7** or **Windows 2008**: **(Member Workstation or Member Server) AND (Windows 7 or Windows 2008)**.

To create an automatic inclusion rule for a monitoring policy

1. In Service Center, click **Configuration** > **Policies** > **Monitoring**.
2. Click the name of the monitoring policy to modify.
3. Click the **Automatic Application** tab.
4. Create the conditional statements. See Creating condition statements for a monitoring policy automatic inclusion rule .
5. Create the inclusion criteria. See Creating inclusion criteria for a monitoring policy automatic inclusion rule .
6. Preview the rule. See Previewing an Automatic Inclusion Rule .

Creating condition statements for a monitoring policy automatic inclusion rule

Set up the conditional structure of the rule by adding **AND** or **OR** statements. By default, rules include a single **AND** statement.

- Set up the conditional statements by doing any of the following:
  - To create a single **AND** statement to which you can add one or multiple rules, do nothing.
  - To create a single **OR** statement, right-click the existing **AND** statement and select **Modify**. From the **Type** list, select **Or**.
  - To add an **OR** statement below the existing **AND** statement, select the **AND** statement and click **Add**. From the Type list, select **Or**.

Creating inclusion criteria for a monitoring policy automatic inclusion rule

For each **AND** or **OR** statement, you must define at least one inclusion criteria.

1. Select the **AND** or **OR** statement to which you want to add inclusion criteria.
2. Click **Add**.
3. From the **Type** list, select **Rule**.
4. From the **Rule** list, select one of the following:

Chassis Type Filter devices according to chassis type, such as laptop, desktop, notebook, etc. Select either **Equals** or **Not Equal** from the **Operator** list, and select a chassis type from the **Value** list.
Device MAC Address Filter devices by the **MAC** address. Select either **Equals**, **Contains**, or **Starts With** from the **Operator** list, and type the **MAC** address in the **Value** box.
Device Model Filter devices by providing the device model. Select either **Equals** , **Not Equal**, **Contains** , **Not Contain** , or **Starts With** from the **Operator list** and type the device model name in the **Value box.**
Device Role Category Filters devices by device role category. As a best practice, use this rule when you are applying service plans to shared site groups; the pre-built shared site groups in Barracuda RMM are designed to be applied to the device roles defined in this rule. Select **Equals** or **Not Equal** from the **Operator** list, and then select **Network Device**, **Unknown**, **Windows Server**, or **Windows Workstation**.
Hardware Type Filters devices according to hardware type, including desktop, laptop, printer, rack mount, and others. From the **Value** list, select the hardware type.
Has Warranty Information Filter devices by whether warranty information exists. Searches for devices with both custom and vendor warranties. Supported vendors include **Acer**, **Compaq**, **Dell**, **Gateway**, **Hewlett-Packard**, **HP**, **IBM**, **Lenovo**, and **Toshiba**. Selecting this option from the **Rule** list includes all devices with warranty information.
Installed Memory (in GB) Filter devices by the installed memory. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in **GBs**.
IP Address Filter devices by the **IP** address. Select either **Equals**, **Not Equal**, **Greater Than**, **Less Than**, **Contains** or **Starts With** from the **Operator** list, then type an **IP** address in the **Value** box.
Is a Printer Filter devices to include printers. Selecting this option from the **Rule** list includes all printers.
Is a Virtual Machine Filter devices to include virtual machines. Selecting this option from the **Rule** list includes all virtual machines.
Logical Drive Size (GB) Filter devices by the logical drive size. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in **GBs**.
Manufacturer Filter devices by the manufacturer. Select **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type a manufacturer name in the **Value** box.
Network Role Filter devices by the network role, such as firewall, router, etc. Select a network role from the **Value** list.
Network Service Filter devices by standard network service ports, including commonly-used services such as **HTTP**, **SMTP**, and **POP3**. Custom ports for network services are not filtered. Select a network service from the **Value** list.
OS Family Filters devices by OS family, for example, **Android**, **iOS**, **Linux/ Unix**, and **Windows**. From the **Value** list, select an OS family.
OS Name Filter devices by the operating system name, for example, **Windows Server 2008 Standard**. Select **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an operating system name in the **Value** box.
OS SKU Filter devices by their unique operating system **SKU (Stock Keeping Unit)**. For example, **Windows 7** has several SKUs, including **Home Premium**, **Professional**, **Home**

Basic, and **Enterprise**. Select either **Equals** or **Not Equal** from the **Operator** list, then select a **SKU** from the **Value** list.

The **OS SKU** rule doesn't apply to **Windows 2003** and **XP** operating systems.

OS Version Filter devices by the operating system version, which you can determine by executing the **winver** command. For example, for the **Windows 7 Enterprise** operating system, the **OS** build version is **7601**. Select either **Equals** , **Not Equal**, or **Starts With** from the **Operator** list, then type an operating system version in the **Value** box.

Responds to SNMP Filter devices by whether they respond to **Simple Network Management Protocol (SNMP)** monitors. From the **Value** list, select **True** to include devices that respond to **SNMP** monitors, or **False** to include devices that do not respond.

Responds to Specific OID Filter devices to include those that respond to a specific **SNMP** object identifier (**OID**). From the **Value** list, select an **OID** type, such as **Dell Server** or **HP Switch**.

Responds to SSH Filters devices by whether they respond to **Secure Shell (SSH)** monitors. From the **Value** list, select **True** to include devices that respond to **SSH** monitors, or **False** to include devices that do not respond.

Responds to WMI Filters devices by whether they are **WMI** enabled. From the **Value** list, select **True** to include devices are WMI enabled, or **False** to include devices that are not.

Responds to WS-MAN Filter devices by whether **WS-MAN** is enabled, which is an option for **WMI** connectivity. Select **True** or **False** from the **Value** list.

SNMP sysDesc Filter devices by the **SNMP** system description. For example, to include **Apple macOS** devices, you could enter "**Darwin**". Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an **SNMP** system description in the **Value** box.

SNMP sysObjectID Filter devices by the **SNMP system object ID**. For example, **Cisco ASA** series devices each have unique **sysObjectIDs**. To include **Cisco ASA 5505** devices, enter the **sysObjectID** for this device type (1.3.6.1.4.1.9.1.745). Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an **SNMP sysObjectID** in the **Value** box.

Software - Mac and Software - Windows Filter devices by the **Mac** or **Windows** applications that are installed. You can filter by software name, and optionally you can also filter by the software version.

1. From the **Operator** list, select either **Exists** or **Does Not Exist**.
2. Under **Software Name**, select an operator from the **Operator** list and type the software name in the **Value** box.
3. To further filter by software version, select the **Include Software Version** check box. From the **Operator** list that appears, select an operator and type a version number in the **Value** box.

System Role Filter devices by system role, for example, **File Server** or **Routing Service**. Select **Equals** or **Not Equal** from the **Operator** list, and then select a system role from the **Value** list.

Windows Service Name Filter devices by the **Windows Service Name**. To determine the **Windows Service Name**, view the device's **Properties** Page. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type a **Windows Service Name** in the **Value** box.

5. **Domain Role** Filter devices by the domain role. Select either **Equals** or **Not Equal** from the **Operator** list and select a domain role from the **Value** list, such as **Member Workstation** or **Primary Domain Controller**.
6. Click **Add**.
7. Click **Save**.

Figures