

Application Event Monitoring from a Remote Host

Scenario

ServerA writes an event to the Application event log on ServerB. ServerB has a SCOM 2007 SP1 agent installed. You want to be alert to run a response based on the event being written to ServerB.

The Problem

The problem is that natively SCOM will not generate an alert or collect the event with a rule or a monitor running on ServerB when the logging computer is different from the computer on which the event is logged. In other words, if the event is logged as being from ServerA in the Application Event Log of ServerB, no alert or event collection will be triggered. This is by design for security reasons but this default behavior can be changed.

The Solution

By default SCOM does not alert on or collect events in the event log on an agent that are written from a computer other than the local computer. For example if ServerA writes an event to the event log on ServerB and ServerB has a SCOM agent installed, ServerB will not alert on or collect the event as the logging computer is not the local server, ServerB.

To allow this to occur, you must edit the XML of the Management Pack and change the `<AllowProxying>>false</AllowProxying>` value to true. This property only exists with Collection rules. See <http://technet.microsoft.com/en-us/library/dd391815.aspx> for more information.

The reason for this is that Microsoft considers the enablement of this parameter a security risk so there is no override on rules that Microsoft provides in sealed MPs or in rules created from the operations console. Therefore you need to create a custom management pack using the Authoring console or the Authoring node in the Operations Console and export the MP and edit the xml to provide this parameter `<AllowProxying>>true</AllowProxying>` on the Microsoft.Windows.EventProvider datasource.

Thanks to [Clive Eastwood](#) for this insight!

If you would like a response to an event, responses are possible with collection rules, you simply need to add a script or command response to the alert collection rule. Read on for more on this...

Environment

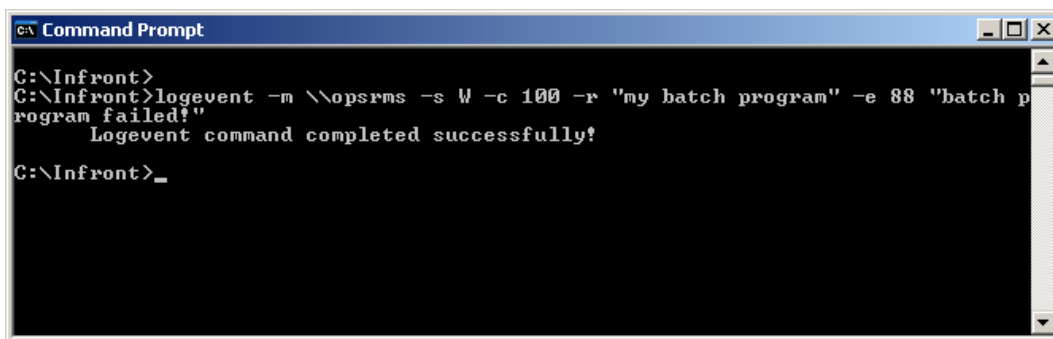
ServerA = icgbackup (Windows Server 2003, no SCOM agent)

ServerB = opsrms (SCOM RMS)

Creating the Event from the Remote Computer

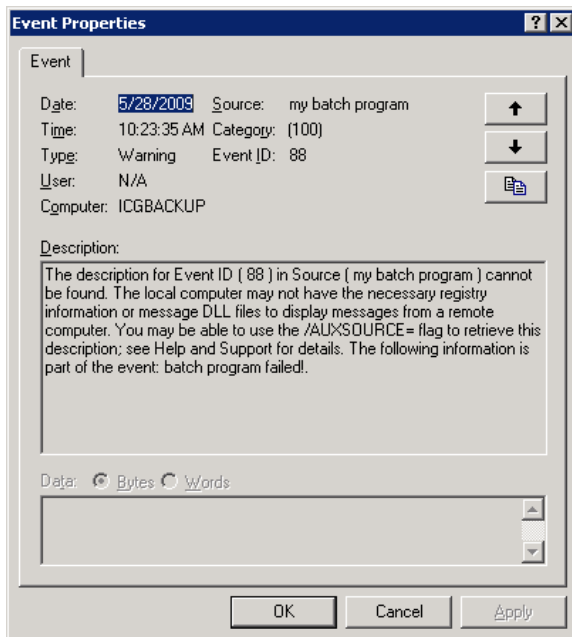
To log an event on a remote computer run the following command on icgbackup:

```
logevent -m \\opsrms -s W -c 100 -r "my batch program" -e 88 "batch program failed!"
```



```
c:\ Infront>
C:\ Infront>logevent -m \\opsrms -s W -c 100 -r "my batch program" -e 88 "batch p
program failed!"
Logevent command completed successfully!
C:\ Infront>_
```

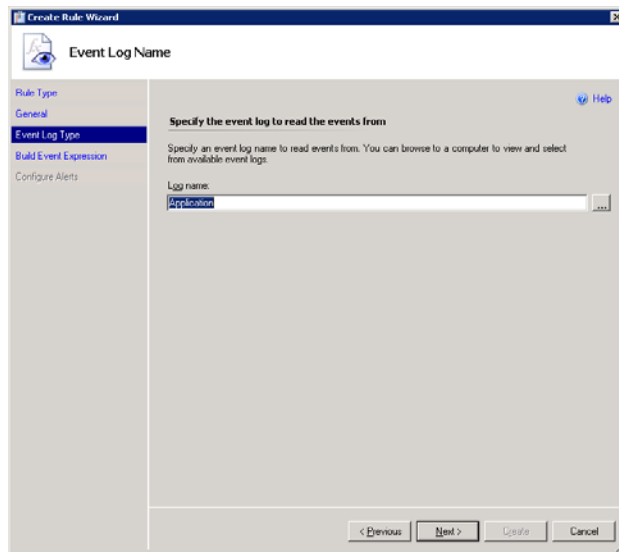
Confirm the event is in the Application Event Log on the remote computer opsrms.



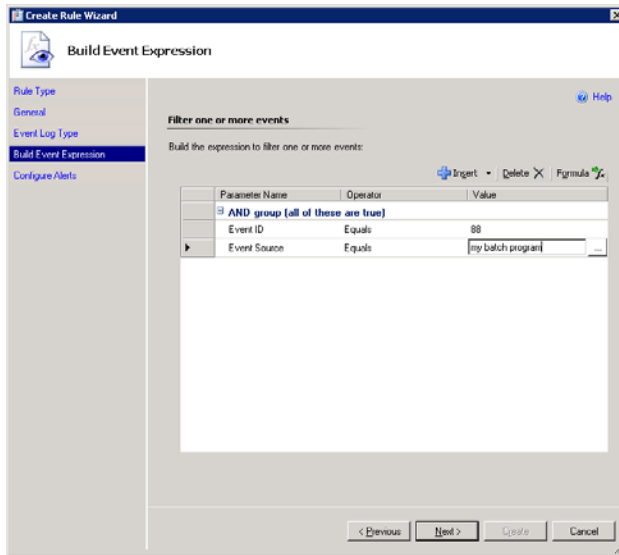
Create a Collection Rule for this Event

To create a Collection rule for this event:

1. Open the Operations console. Select the Authoring node. Expand Management Pack Objects. Right click on **Rules** and select **Create a new rule**.
2. In the Create Rule Wizard under Collection Rules, expand Event Based and select **NT Event Log (Alert)**. Select the **TestMP** to store the new rule and click **Next**.
3. On the General page, type **Test Rule** as the rule name. Change the rule category to **Collection**. Click the **Select** button and target the rule to **Windows Server 2003 Operating System**. Clear the **rule is enabled** check box. Click **Next**.
4. Leave Application log selected and click **Next**.



5. Type **88** in the Event ID value. Type **my batch program** in the Event Source value. Click **Next**.

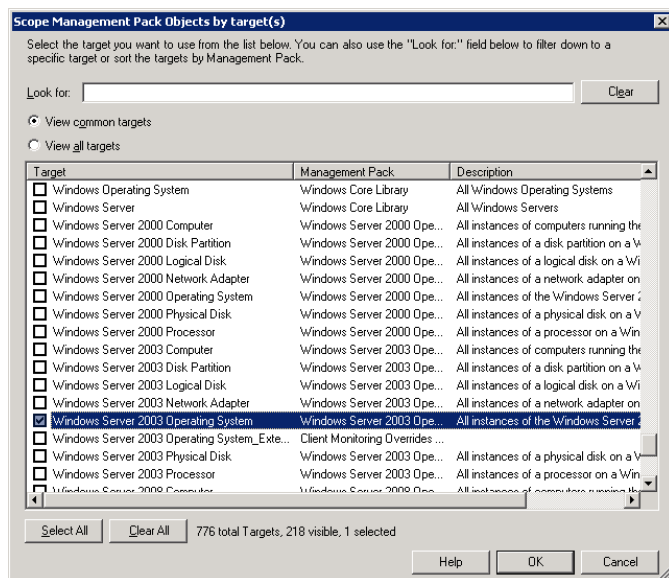


6. Click **Create**.

Enabling the Rule through an Override

Note: This is not necessary, you can enable the rule natively but creating the rule disabled and enabling it through an override during testing is a best practice.

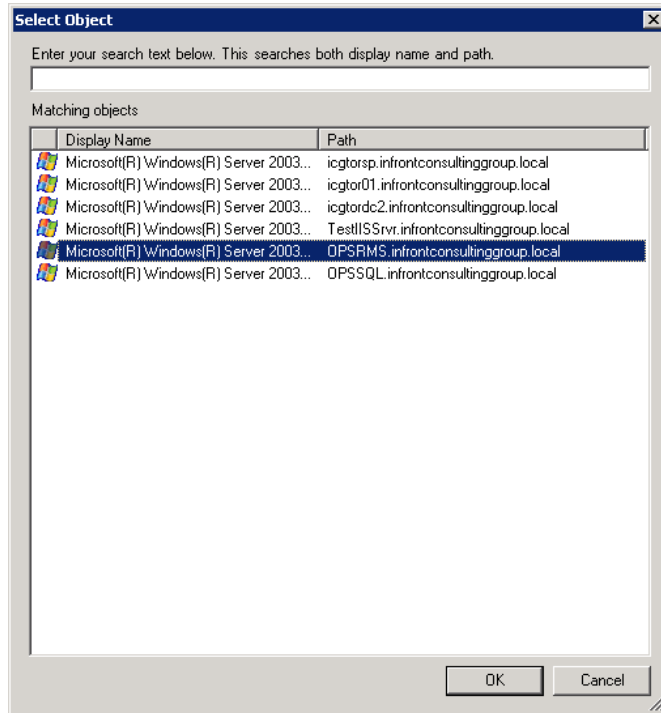
In the Authoring node of the Operations Console, change the scope to Windows Server 2003 Operating System as this is the object class that you targeted the rule to.



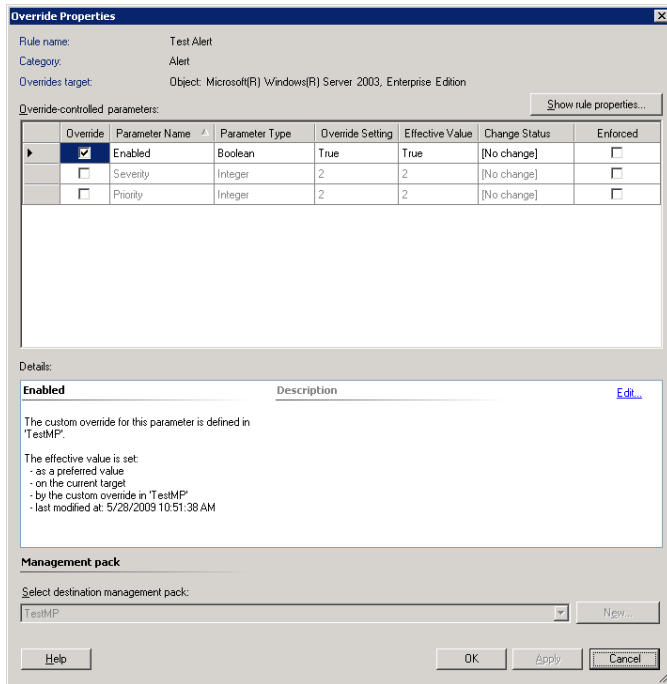
Scroll through the list of rules to locate the rule you created named Test Alert.

Right click on the Test Alert rule and select **Overrides** | **Override the rule** | **For a specific object of type: Windows Server 2003 Operating System**.

Select the **Opsrms** server in the list and click **OK**. This is the server that you want to enable the rule on.



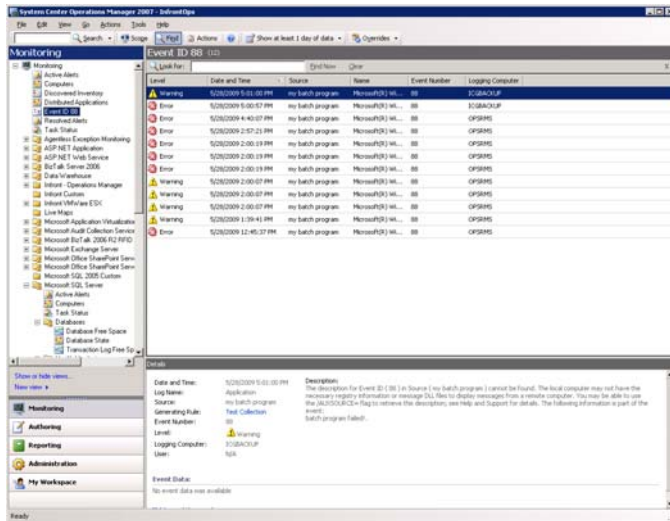
Place a check mark to the left of the **Enabled** property. Change False to **True** and click **Apply**. Click **OK**.



The rule is now enabled.

Export and Modify the XML

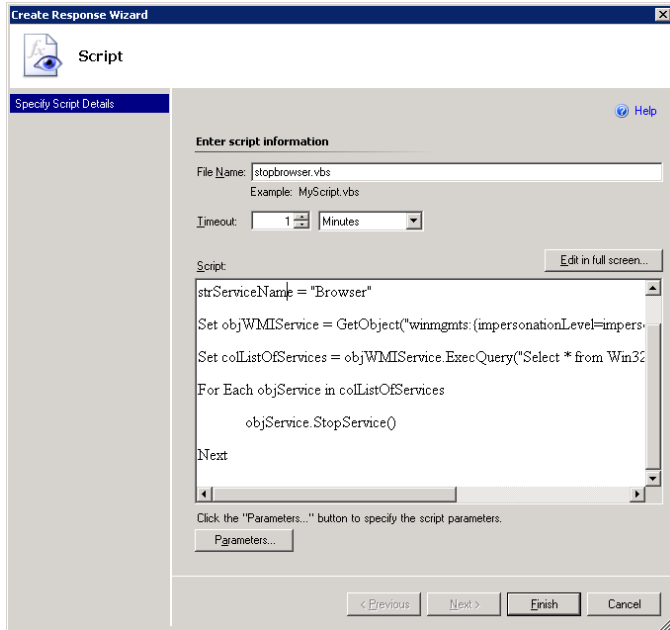
In order to get the collection rule to collect an event written to the opsrms (ServerB) server from igbackup (ServerA) you need to modify the MP's XML. By default the collection rule does work until you edit the XML and change the default `<AllowProxying>>false</AllowProxying>` to `<AllowProxying>>true</AllowProxying>`. After making this change, increment the version of the MP and save it to disk. Then import the new version into Operations Manager. Once the updated rule has been received and you rerun the remote creation of the event, you can see below that the event written from another computer igbackup is captured.



This is part one of a two part solution as the second request is to have a response run. To do this we will have to modify the Event Collection rule.

In the Authoring node of the Operations Console, locate the Collection rule and open the Properties of the rule. Select the Configuration tab and click **Add** at the bottom right in the Responses section.

Select Run Script. Enter a script name and enter the script code.



Running the logevent command from icgbackup now successfully logs an event to opsrms in the Application log and the event collection rule picks it up and the new script response now runs and stops the browser service.

