SCOM - Creating alerts based on Event Description

It's been a while since my last post, so I thought that I would try and make this one count. I am trying my best to play around with SCOM as much as possible, but am finding it hard to find the time to do so.

For this post I am going to be filtering alerts in SCOM by the Event Description, this is not best practice as this will add additional overhead to the SCOM agent, but in some cases this is the best solution to the problem.

The first thing that I am going to need to do is create an alert in SCOM that we can use to filter on. Lets do that.

- Open the authoring console and create a blank MP
    - I am calling mine Richard.Alert.Test
- Create a new Windows Event Alerting rule and give it a name
    - Mine will be called Richard.Alert.Test.FilterTestAlert
    - Target this rule at Windows.Server.Computer
    - For the category, select Alert (to keep things uniform).
    - Click Next
- For the Event Log Name page complete the following:
    - For the Log Name, select "Operations Manager"
    - Click Next
- For the Build Event Expression page complete the following:
    - EventID = 12345
    - Click Insert, Select "Use parameter name not specified above" and for the value enter in "EventDescription", click OK to close the dialog
    - For the Operator select "Contains"
    - For the value, enter in "Hello World"
    - Click Next to continue
- On the Configur Alerts page complete the following:
    - Enter in an Alert Name
    - For the event description, leave this as is (for now – you can change this later)
    - If needs be, change the Priority, Severity and Suppression for the alert
    - Click Finish to complete the creation of the alert.

For testing purposes you should disable this rule explicitly and target it at your test server (I am not going to be doing this).

The next stage of this would be to import the MP into SCOM and test this guy out. The first thing I am going to do is create a test alert on my server that will not satisfy the alerting rule.

Using the following VBScript I generate the below alert on my serve, check SCOM to see that nothing comes through.

```
Set oAPI                        = CreateObject("MOM.ScriptAPI")
eventDescription     = "This will not alert in SCOM"
scriptName                      = "TestAlert.vbs"
eventID                                 = 12345
Call oAPI.LogScriptEvent(scriptName, eventID, 1, eventDescription)
```

Now that I see filtering is working, the next step is to add the text “Hello World” to the alert and see if anything comes into SCOM. To do this I modify my alert VBScript to look something like the below and run this on my server.

```
Set oAPI                        = CreateObject("MOM.ScriptAPI")
eventDescription     = "Hello World, I should appear in SCOM"
scriptName                      = "TestAlert.vbs"
eventID                                 = 12345
Call oAPI.LogScriptEvent(scriptName, eventID, 1, eventDescription)
```

The rule is working :)

You could take this a step further and allow the rule to filter on Regular expressions, not contains etc if you need to.

You can grab the completed Management Pack from here.