Monitoring VMWare ESX Server On Microsoft System Center Operations Manager 2007

Version	2.2
Date:	10th September 2007
Writer:	Jonathan Hambrook
Email:	stockmansridge@gmail.com
Blog:	http://opsmgr.wordpress.com

Table of Contents

1 Document Overview Information

1.1 About this Document

This document contains step-by-step instructions on how to monitor VMWare ESX Servers on SCOM 2007. While I admit there are many possible ways to do this, I believe this document will demonstrate 2 of the most effective ways, allowing for greater granularity and accuracy in Alerting.

The 2 ways to monitor the VMWare ESX and the Hardware are via SNMP Traps & SysLog. The first section of this document refers to SysLog and the second to SNMP Traps.

Feedback is always welcome. Please email me at stockmansridge@gmail.com or visit my blog at http://opsmgr.wordpress.com

1.2 Decision Matrix

Alert Type	**SNMP**	**SysLog**
Server Alerts	YES	YES
Good for Alerting to Flight Desk from SCOM	YES – Will change Health State in SCOM	YES – Will change Health State in SCOM
Support Notification	YES – Email, IM or SMS	YES – Email, IM or SMS
Install Software in SC	YES – Agent to send SNMP	NO
Ease of Setup	Medium	Very
Support Management Board	YES	NO

1.3 Why monitor the VMWare ESX layer?

Monitoring the ESX layer is an important part of maintaining a VMWare environment as part of the security features are that the Operating systems that you load on the system can not interface directly with the hardware so should you have a failure of one of your systems it doesn’t effect the others. This means that just running the SCOM Agent on the clients will not report if a HDD, Power Supply or Disk has failed even with the Hardware vendors management pack.

1.4 Systems Understandings

As you may or may not know, VMWare uses its own Linux Operating System referred to as ‘ESX’. This means using the SCOM Agent is not possible as it is only compatible with Microsoft Windows Operating Systems.

There are 2 other ways of setting up monitoring of devices in SCOM, one is via the SCOM Agent and the other is via SNMP.

1.5 Limitations

These instructions are limited to VMWare ESX. You will also require hardware from a vendor that supports a Linux agent for their hardware. I know the following do:

- IBM
- HP
- DELL

You will find that as we are collecting from a SysLog and even though we configure which servers we are gathering from, you will be unable to get the Status to change from Green to Red should a SysLog Alert be generated for a particular device. This is a limitation to SCOM and how it handles SysLog Alerts. The reason for this is because the method the ESX server is added and its alive status is monitored via SNMP. To get the status to change you will need to create an SNMP Trap Monitor.

1.6 References

1.6.1 SNMP Tools

- GetIf
    - http://www.wtcs.org/snmp4tpc/getif.htm

1.6.2 MIB Sites

- MIBSearch - http://www.mibsearch.com/
- OIDView - http://www.oidview.com/mibs/detail.html
- IP Monitor SNMP Center - http://support.ipmonitor.com/snmp_center.aspx
- IP Monitor MIB OID Tree - http://support.ipmonitor.com/mibs_byoidtree.aspx
- Simple Web - http://www.simpleweb.org/ietf/mibs/

1.6.3 IBM References

- Download Agent Software
    - https://www14.software.ibm.com/webapp/iwm/web/reg/download.do?source=dmp&S_PKG=director_x_520&lang=en_US&cp=UTF-8#x12
- Which Agent to use
    - http://www-941.haw.ibm.com/collaboration/ibmwiki/pages/viewpage.action?pageId=8911
- Configuration of SNMP for IBM Director Agents
    - http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diricinfo/fqm0_t_enabling_snmp_access_and_trap_forwarding_vmware.html
- Implementing IBM Director 5.20
    - http://www.redbooks.ibm.com/abstracts/sg246188.html
- IBM Management Documentation
    - http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp

1.6.4 MOM 2005 References

- MOM 2005 Trap Information
    - http://www.momresources.org/momarticles/MOMTelecomSNMP.pdf

1.6.5 Microsoft SCOM 2007 Training Videos

- http://www.microsoft.com/winme/0701/28666/About_Monitors.asx
- http://www.microsoft.com/winme/0701/28666/Management_Packs_Demo.asx
- http://www.microsoft.com/winme/0703/28666/Add_Monitoring_Edited.asx
- http://www.microsoft.com/winme/0703/28666/Adjusting_Monitors_with_Overrides_Edit.asx
- http://www.microsoft.com/winme/0701/28666/Tasks_Demo.asx
- http://www.microsoft.com/winme/0701/28666/Views_Demo.asx
- http://www.microsoft.com/winme/0701/28666/Rules_Demo.asx
- http://www.microsoft.com/winme/0703/28666/Whats_New_for_Ops_Mgr_05_Edited.asx
- http://www.microsoft.com/winme/0701/28666/The_Monitoring_Space.asx
- http://www.microsoft.com/winme/0703/28666/Adjusting_Monitors_with_Overrides_Edit.asx
- http://www.microsoft.com/winme/0610/28666/DistributedApplicationDesigner_RTM_300k.asx

1.7 Terminology

Blog – Is short for Weblog, An online journal on a specific topic or range of topics.

OID – **O**bject **Id**entifier, A permanent number assigned to an object for storage (persistence). It is typically a long integer, such as 128 bits, that can be computed using various methods to create a unique number. It functions in a similar manner to the way a key field does in a relational database record uniquely identifies that record in a table.

MIB – **M**anagement **I**nformation **B**ase, An SNMP structure that describes the particular device being monitored

RMS – Root Management Server

SCOM – System Center Operations Manager 2007

SNMP – Simple Network Message Protocol

SNMP Trap – A notification event issued by a managed device to the network management station when a significant event (not necessarily an outage, a fault, or a security violation) occurs.

SysLog – A System Log using the defacto standard common on Linux and Network Devices. Uses UDP port 514.

VMWare – The company that produces VMWare ESX Server

VMWare ESX Server – An application that allows a single piece of hardware to run multiple Operating Systems of many flavours

2 Configuring the ESX Server

2.1 Configuring SysLog

Step	Action/Outcome	Reference
1	Login to the ESX Console using ssh – putty	
2	Edit the **#vi /etc/syslog.conf** add the following:	#vi /etc/syslog.conf
3	Edit the **#vi /etc/syslog.conf** add the following: *.* - This is a configurable option: See Appedix A	# Send All Traps to SCOM2007 *.* @SCOMRMS.COM
4	Restart the ESX SysLog service	#service syslog restart
5	Check the ESX Log File for any errors	#tail /var/log/messages

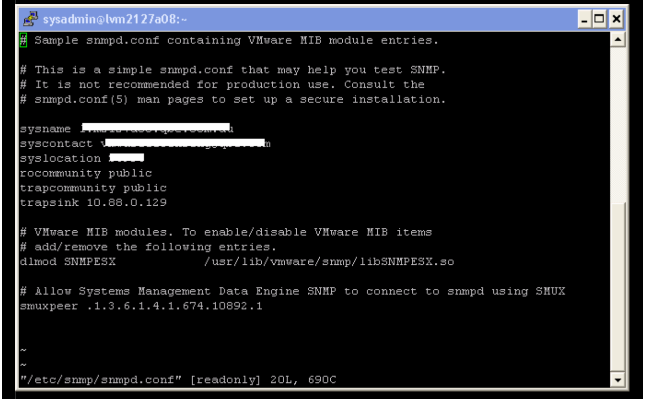
☝

See Appendix A for details of syslog.conf configurations.

2.2 Testing SysLog Configuration

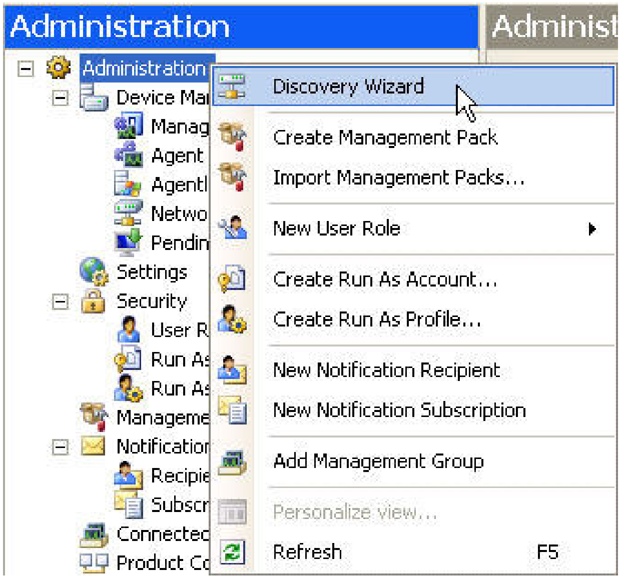
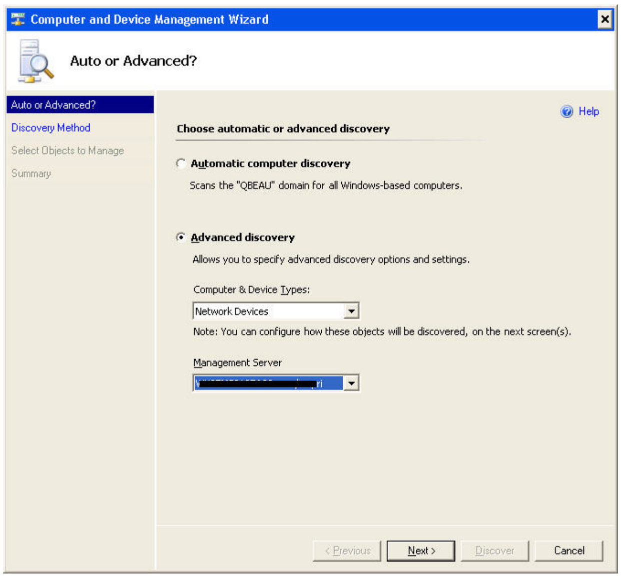
Step	Action/Outcome	Reference
1	Use ESX logger to send a test message	#logger -p ftp.warning “This is a test warning from ESX Server”
2	Check the ESX log file	#tail -f /var/log/messages
3	Check ESX firewall Settings	#esxcfg-firewall -q | grep 514
4	Allow syslog outgoing traffic	#esxcfg-firewall -o 514,udp,out,syslog
5	Check open network ports	#netstat - an Proto Local Address Foreign Address UDP 0 0 0.0.0.0:514 0.0.0.0:*

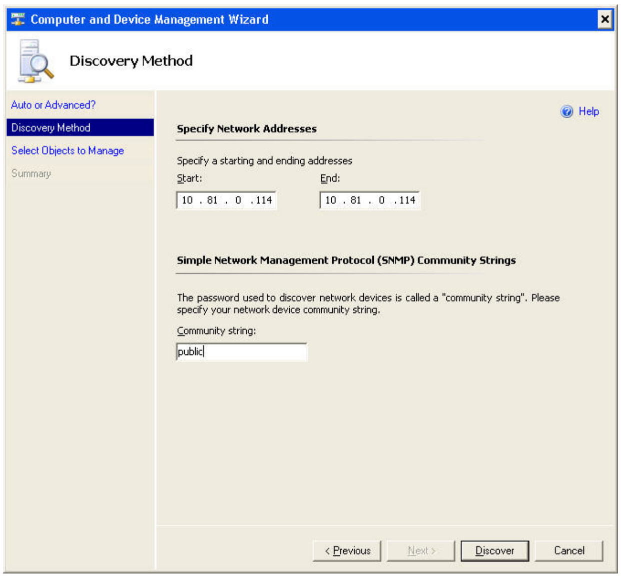
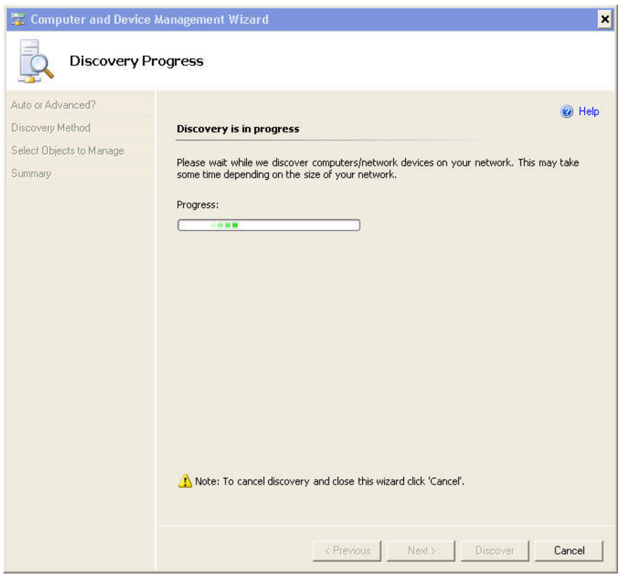
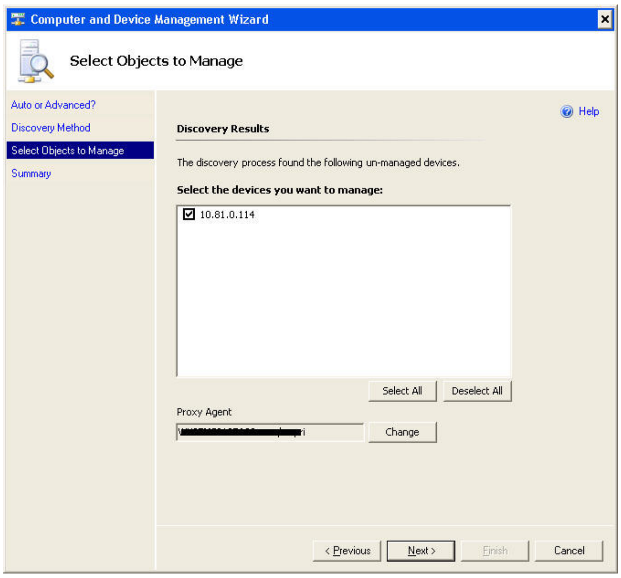
2.3 Configure SNMP Trap to be sent to RMS.

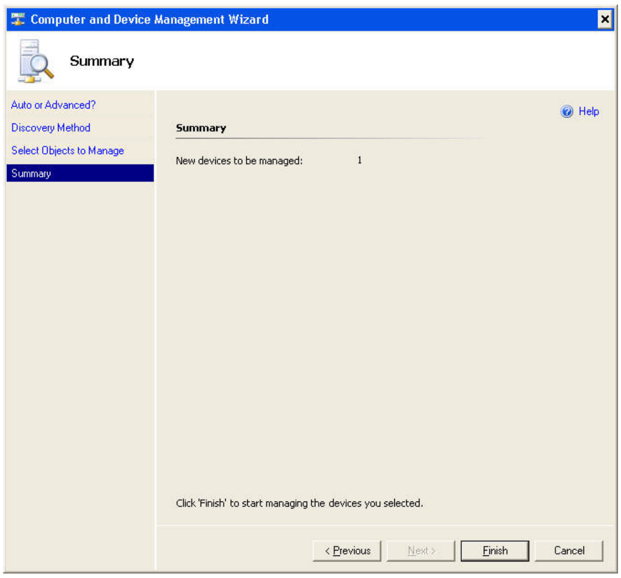
Step	Action/Outcome	Reference
1	Edit the snmpd.conf file	`#vi /etc/snmp/snmpd.conf`
2	This is where we will configure it to point to the Root Management Server as well as the community string to use. Enter the following: **trapsink 10.0.0.0** Note: You can't have duplicate entries in this file. It is suggested you configure the other parameters, sysname, syscontact, syslocation.	
3	Restart the snmpd service	`#service snmpd restart`
4	Enable snmpd to pass-through the ESX firewall	`#esxcfg-firewall -e snmpd`
5	Verify SNMP is functioning	`#snmpwalk -v 1 -c public localhost system`

```
# Sample snmpd.conf containing VMware MIB module entries.

# This is a simple snmpd.conf that may help you test SNMP.
# It is not recommended for production use. Consult the
# snmpd.conf(5) man pages to set up a secure installation.

sysname [redacted]
syscontact [redacted]
syslocation [redacted]
rocommunity public
trapcommunity public
trapsink 10.88.0.129

# VMware MIB modules. To enable/disable VMware MIB items
# add/remove the following entries.
dlmod SNMPESX            /usr/lib/vmware/snmp/libSNMPESX.so

# Allow Systems Management Data Engine SNMP to connect to snmpd using SMUX
smuxpeer .1.3.6.1.4.1.674.10892.1


~
~
"/etc/snmp/snmpd.conf" [readonly] 20L, 690C
```

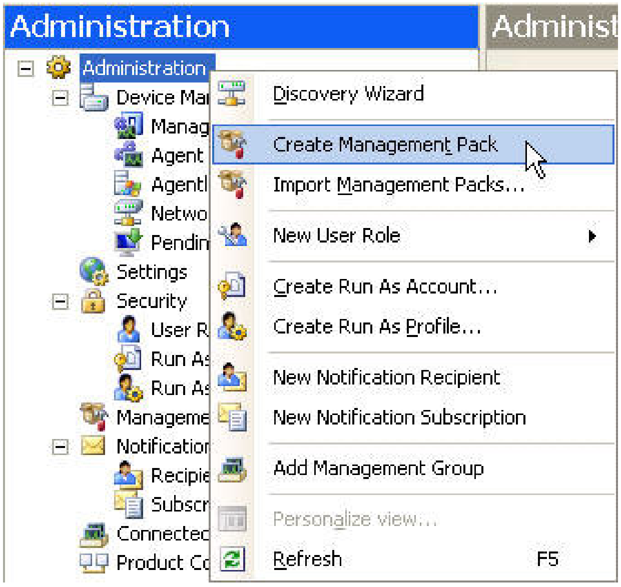
3 Discovering ESX Servers in SCOM

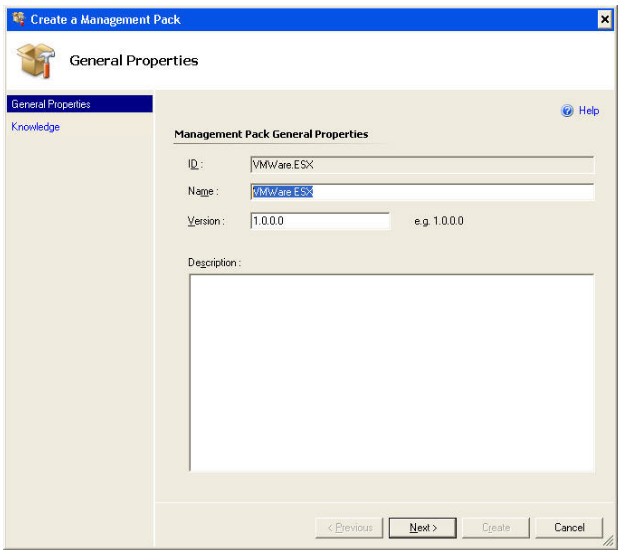
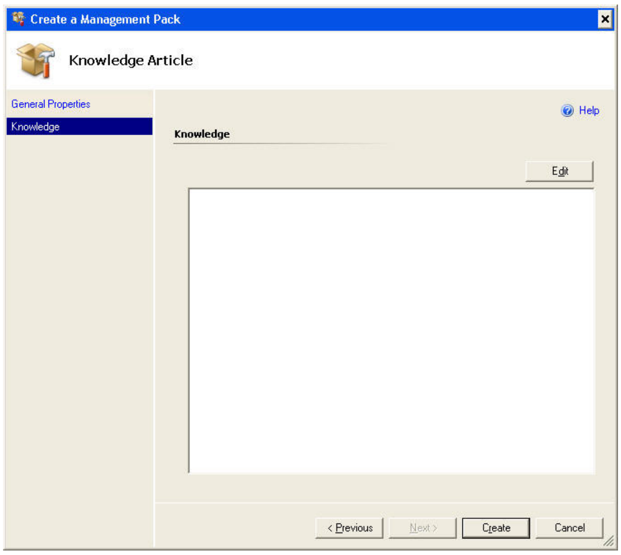
Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Administration** tab	
3	Right-click **Administration** Select **Discovery Wizard**	 Administration Administ Administration Device Ma Manag Agent Agentl Netwo Pendin Settings Security User R Run As Run As Manageme Notification Recipie Subscr Connected Product Co Discovery Wizard Create Management Pack Import Management Packs... New User Role Create Run As Account... Create Run As Profile... New Notification Recipient New Notification Subscription Add Management Group Personalize view... Refresh F5
4	Under **Advanced discovery** Select **Network Devices** Click [Next >]	Computer and Device Management Wizard Auto or Advanced? Auto or Advanced? Discovery Method Select Objects to Manage Summary Help Choose automatic or advanced discovery ○ Automatic computer discovery Scans the "QBEAU" domain for all Windows-based computers. ● Advanced discovery Allows you to specify advanced discovery options and settings. Computer & Device Types: Network Devices Note: You can configure how these objects will be discovered, on the next screen(s). Management Server: [redacted]

Step	Action/Outcome	Reference
5	Fill the **IP Address** Start: and End: fields for your ESX Server. Click Discover	 Computer and Device Management Wizard Discovery Method Auto or Advanced? Discovery Method Select Objects to Manage Summary Help **Specify Network Addresses** Specify a starting and ending addresses Start: 10 . 81 . 0 .114 End: 10 . 81 . 0 .114 **Simple Network Management Protocol (SNMP) Community Strings** The password used to discover network devices is called a "community string". Please specify your network device community string. Community string: public < Previous · Next > · Discover · Cancel
6	Please wait…	 Computer and Device Management Wizard Discovery Progress Auto or Advanced? Discovery Method Select Objects to Manage Summary Help **Discovery is in progress** Please wait while we discover computers/network devices on your network. This may take some time depending on the size of your network. Progress: ⚠ Note: To cancel discovery and close this wizard click 'Cancel'. < Previous · Next > · Discover · Cancel
7	When the device is found ☑ **- Tick** Click Next >	 Computer and Device Management Wizard Select Objects to Manage Auto or Advanced? Discovery Method Select Objects to Manage Summary Help **Discovery Results** The discovery process found the following un-managed devices. **Select the devices you want to manage:** ☑ 10.81.0.114 Select All · Deselect All Proxy Agent [redacted] Change < Previous · Next > · Finish · Cancel

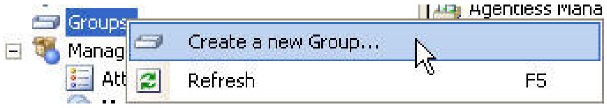
Step	Action/Outcome	Reference
8	Click Finish	 Computer and Device Management Wizard Summary Summary New devices to be managed: 1 Click 'Finish' to start managing the devices you selected. Auto or Advanced? Discovery Method Select Objects to Manage Summary Help < Previous Next > Finish Cancel

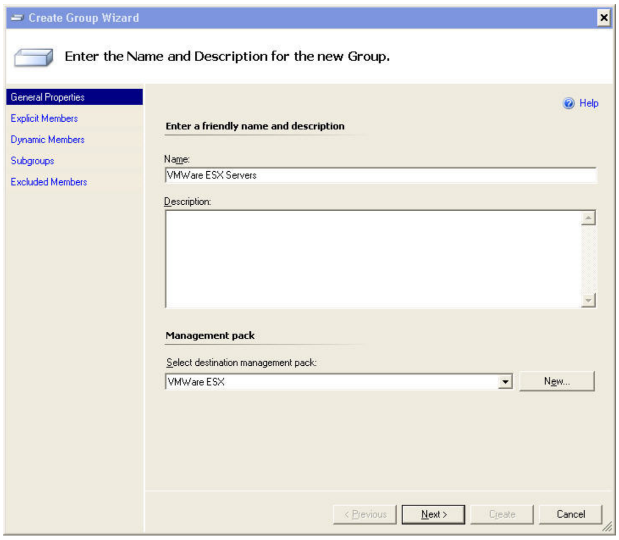
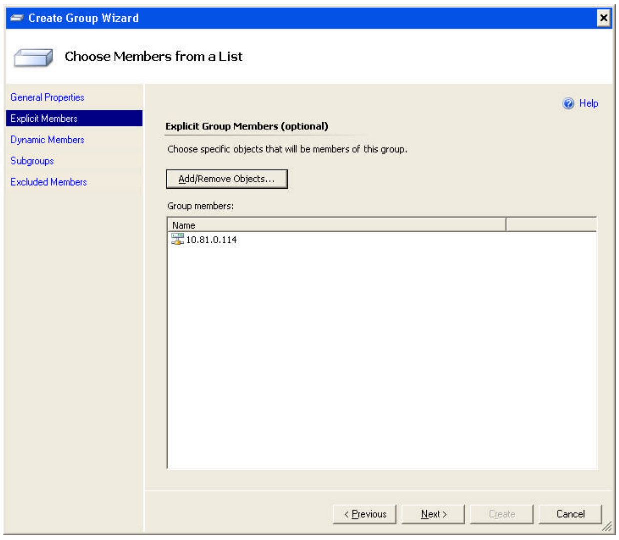
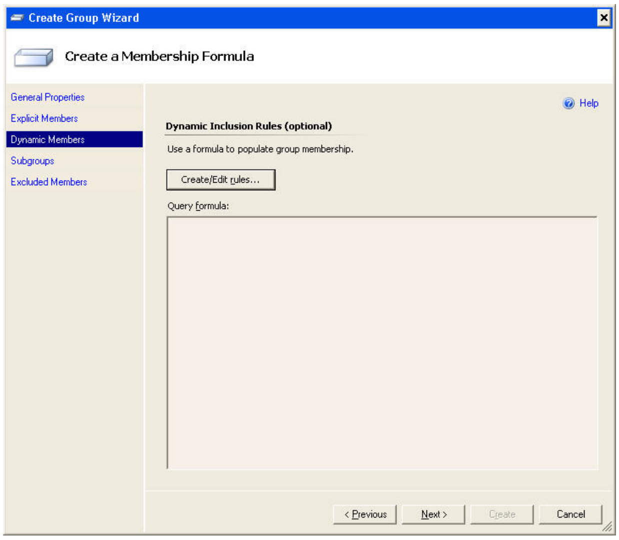
3.1 Create a Management Pack for ESX

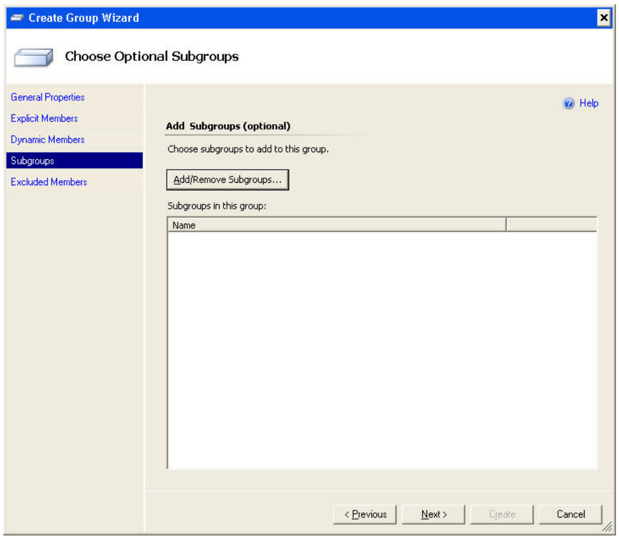
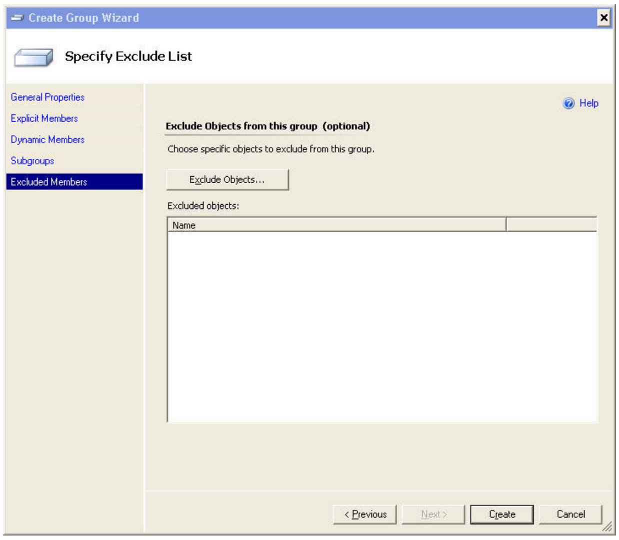
Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Administration** tab	
3	Right-click **Administration** Select **Create Management Pack**	 Administration Administ Administration Device Mai Manag Agent Agentl Netwo Pendin Settings Security User R Run As Run As Manageme Notificatior Recipie Subscr Connectec Product Cc Discovery Wizard Create Management Pack Import Management Packs... New User Role Create Run As Account... Create Run As Profile... New Notification Recipient New Notification Subscription Add Management Group Personalize view... Refresh F5

Step	Action/Outcome	Reference
4	Fill in the following fields: Name: **VMWare ESX** Click Next >	 Create a Management Pack General Properties General Properties Knowledge Help Management Pack General Properties Description : < Previous Next > Create Cancel ID : VMWare.ESX Name : VMWare ESX Version : 1.0.0.0 e.g. 1.0.0.0
5	Click Create	 Create a Management Pack Knowledge Article General Properties Knowledge Help Knowledge Edit < Previous Next > Create Cancel

3.2 Create Group for ESX Servers

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Groups** Select **Create a new Group…**	 Groups Manag Att Agentless Mana Create a new Group... Refresh F5

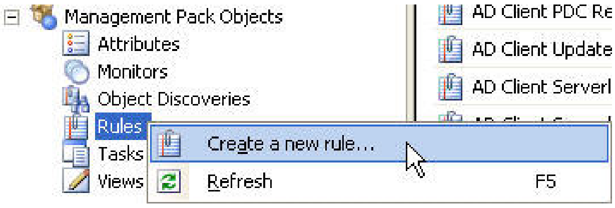
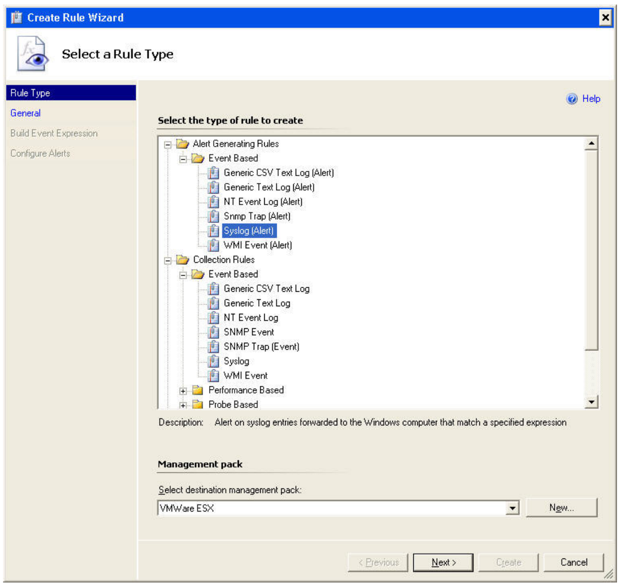
Step	Action/Outcome	Reference
4	Fill in the following fields: Name: **VMWare ESX Servers** Under Management Pack Select **VMWare ESX** Click Next >	 Create Group Wizard Enter the Name and Description for the new Group. Enter a friendly name and description Name: VMWare ESX Servers Description: Management pack Select destination management pack: VMWare ESX
5	Click Add/Remove Objects... and add your VMWare ESX Server. This will be represented by its IP Address. Click Next > Note: If you are able to create a 'Dynamic Members' rule then skip this step.	 Create Group Wizard Choose Members from a List Explicit Group Members (optional) Choose specific objects that will be members of this group. Group members: Name 10.81.0.114
6	Click Next > Note: If you are able to create a 'Dynamic Members' rule create it here. ie: if all your ESX Servers are in a group of IP's.	 Create Group Wizard Create a Membership Formula Dynamic Inclusion Rules (optional) Use a formula to populate group membership. Query formula:

Step	Action/Outcome	Reference
7	Click Next >	 Create Group Wizard Choose Optional Subgroups Add Subgroups (optional) Choose subgroups to add to this group. Subgroups in this group: General Properties Explicit Members Dynamic Members Subgroups Excluded Members Help Add/Remove Subgroups... Name < Previous Next > Create Cancel
8	Click Create	 Create Group Wizard Specify Exclude List Exclude Objects from this group (optional) Choose specific objects to exclude from this group. Excluded objects: General Properties Explicit Members Dynamic Members Subgroups Excluded Members Help Exclude Objects... Name < Previous Next > Create Cancel

4 SCOM SysLog Configuration

4.1 Create VMWare ESX SysLog Alert Rule for Hardware Monitoring

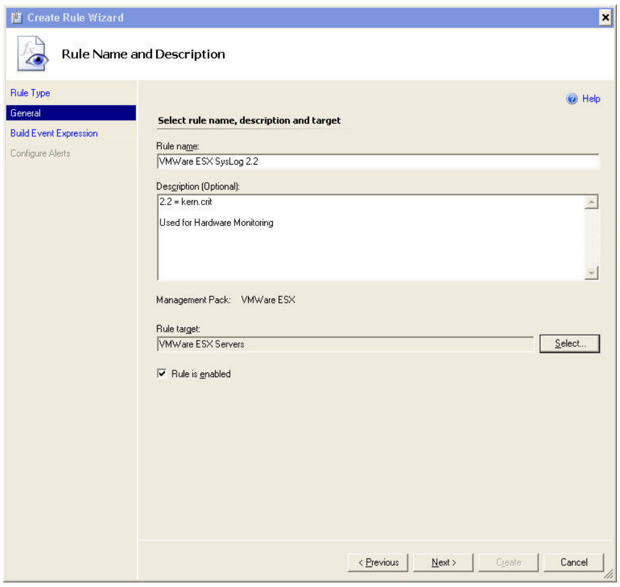
4.1.1 Example kern.crit

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Rules** Select **Create a new rule…**	 Management Pack Objects Attributes Monitors Object Discoveries Rules Tasks Views Create a new rule… Refresh F5 AD Client PDC Re AD Client Update AD Client Serverl
4	Under Alert Generating Rule\Event Based Select **Syslog (Alert)** Under Management Pack Select **VMWare ESX** Click Next > Note: Do not select Syslog under collection rules as you will not get any alerts generated.	 Create Rule Wizard Select a Rule Type Rule Type General Build Event Expression Configure Alerts Help Select the type of rule to create Alert Generating Rules Event Based Generic CSV Text Log (Alert) Generic Text Log (Alert) NT Event Log (Alert) Snmp Trap (Alert) Syslog (Alert) WMI Event (Alert) Collection Rules Event Based Generic CSV Text Log Generic Text Log NT Event Log SNMP Event SNMP Trap (Event) Syslog WMI Event Performance Based Probe Based New... < Previous Next > Create Cancel Description: Alert on syslog entries forwarded to the Windows computer that match a specified expression Management pack Select destination management pack: VMWare ESX

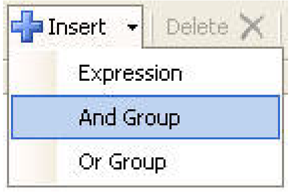
<table>
<tr><th>Step</th><th>Action/Outcome</th><th>Reference</th></tr>
<tr><td>5</td><td>Fill in the following fields:

Rule Name: <b>VMWare ESX SysLog 2.2</b>
Description: <b>2.2 = kern.crit used for Hardware Alerts</b>

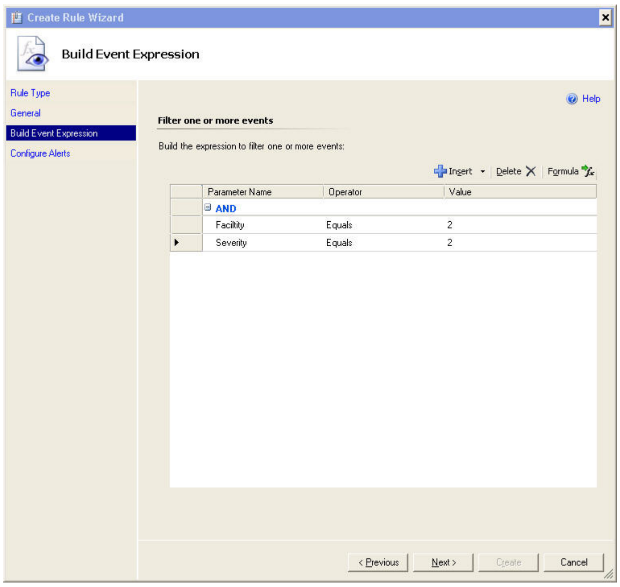
Under Rule target:
Select <b>VMWare ESX Servers</b>

Click Next ></td><td>
Create Rule Wizard
Rule Name and Description
Select rule name, description and target
Rule name: VMWare ESX SysLog 2.2
Description (Optional): 2.2 = kern.crit
Used for Hardware Monitoring
Management Pack: VMWare ESX
Rule target: VMWare ESX Servers
☑ Rule is enabled

Rule Type
General
Build Event Expression
Configure Alerts
Help
Select...
< Previous
Next >
Create
Cancel

</td></tr>
<tr><td>6</td><td>Click 

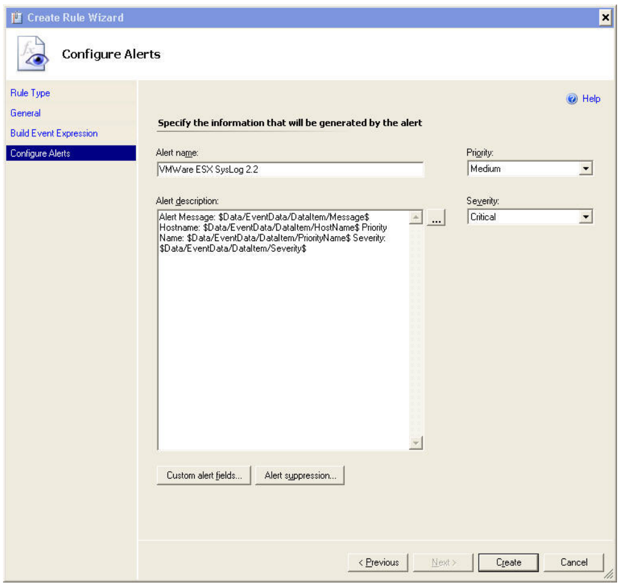
<table><tr><th>Parameter</th><th>Operator</th><th>Value</th></tr><tr><td>Severity</td><td>Equals</td><td>2</td></tr><tr><td>Facility</td><td>Equals</td><td>2</td></tr></table>
Click Next >

Note: This filter looks for the Severity and Facility parameter to equal 2 which is kern.crit where most of your hardware alerts should show up.</td><td>
Create Rule Wizard
Build Event Expression
Filter one or more events
Build the expression to filter one or more events:
<table><tr><th>Parameter Name</th><th>Operator</th><th>Value</th></tr><tr><td>AND</td><td></td><td></td></tr><tr><td>Faciltity</td><td>Equals</td><td>2</td></tr><tr><td>Severity</td><td>Equals</td><td>2</td></tr></table>

Rule Type
General
Build Event Expression
Configure Alerts
Help
Insert
Delete
Formula
< Previous
Next >
Create
Cancel

</td></tr>
<tr><td>7</td><td>Fill in the following fields:

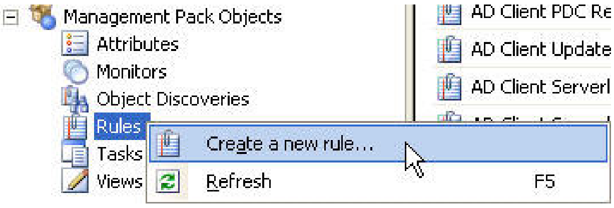
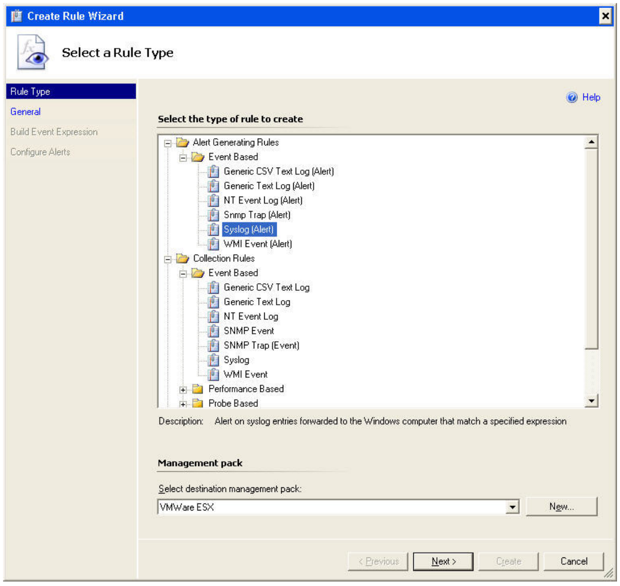
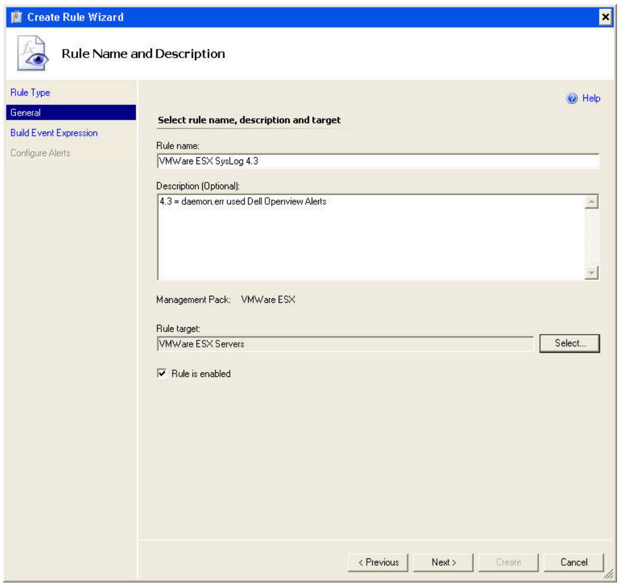
Alert Description
<b>Alert Message:
$Data/EventData/DataItem/Message$
Hostname:
$Data/EventData/DataItem/HostName$
Priority Name:
$Data/EventData/DataItem/PriorityName$
Severity:
$Data/EventData/DataItem/Severity$</b>

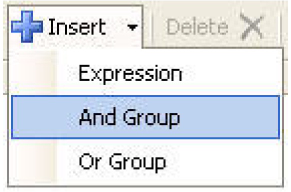
Click Create</td><td>
Create Rule Wizard
Configure Alerts
Specify the information that will be generated by the alert
Alert name: VMWare ESX SysLog 2.2
Priority: Medium
Alert description: Alert Message: $Data/EventData/DataItem/Message$ Hostname: $Data/EventData/DataItem/HostName$ Priority Name: $Data/EventData/DataItem/PriorityName$ Severity: $Data/EventData/DataItem/Severity$
Severity: Critical

Rule Type
General
Build Event Expression
Configure Alerts
Help
Custom alert fields...
Alert suppression...
< Previous
Next >
Create
Cancel

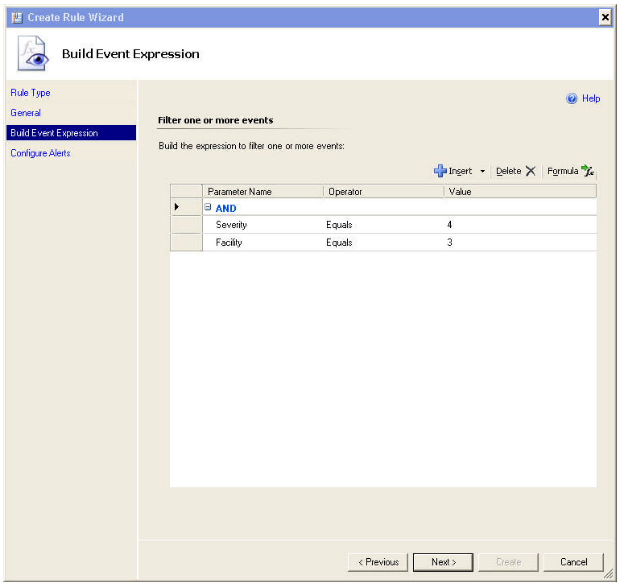
</td></tr>
</table>

4.1.2 Example daemon.err (Test with Dell Temperature Probe Trigger & Alert)

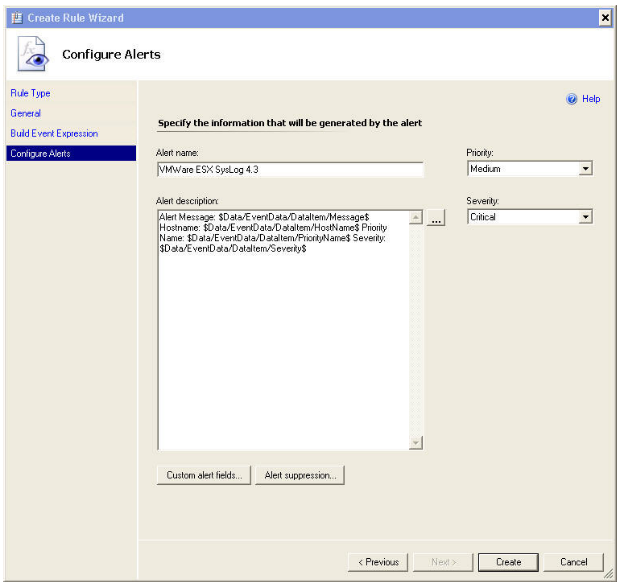
Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Rules** Select **Create a new rule…**	 Management Pack Objects Attributes Monitors Object Discoveries Rules Tasks Views Create a new rule… Refresh F5 AD Client PDC Re AD Client Update AD Client Serverl
4	Under Alert Generating Rule\Event Based Select **Syslog (Alert)** Under Management Pack Select **VMWare ESX** Click Next > Note: Do not select Syslog under 'Collection Rules' as you will not get any alerts generated.	 Create Rule Wizard Select a Rule Type Rule Type General Build Event Expression Configure Alerts Help Select the type of rule to create Alert Generating Rules Event Based Generic CSV Text Log (Alert) Generic Text Log (Alert) NT Event Log (Alert) Snmp Trap (Alert) Syslog (Alert) WMI Event (Alert) Collection Rules Event Based Generic CSV Text Log Generic Text Log NT Event Log SNMP Event SNMP Trap (Event) Syslog WMI Event Performance Based Probe Based Description: Alert on syslog entries forwarded to the Windows computer that match a specified expression Management pack Select destination management pack: VMWare ESX
5	Fill in the following fields: Rule Name: **VMWare ESX SysLog 4.3** Description: **4.3 = daemon.err used Dell Openview Alerts** Under Rule target: Select **VMWare ESX Servers** Click Next >	 Create Rule Wizard Rule Name and Description Rule Type General Build Event Expression Configure Alerts Help Select rule name, description and target Rule name: VMWare ESX SysLog 4.3 Description (Optional): 4.3 = daemon.err used Dell Openview Alerts Management Pack: VMWare ESX Rule target: VMWare ESX Servers ☑ Rule is enabled Select... < Previous Next > Create Cancel

<table>
<tr><th>Step</th><th>Action/Outcome</th><th>Reference</th></tr>
<tr><td>6</td><td>Click 

<table>
<tr><th>Parameter</th><th>Operator</th><th>Value</th></tr>
<tr><td>Severity</td><td>Equals</td><td>4</td></tr>
<tr><td>Facility</td><td>Equals</td><td>3</td></tr>
</table>
Click Next &gt;

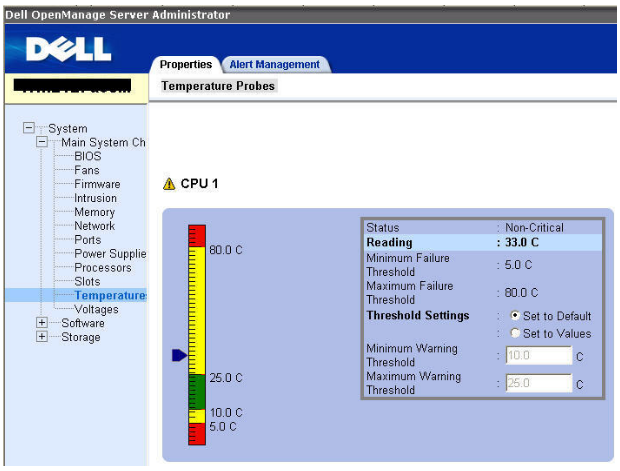
Note: This filter looks for the Severity and Facility parameter to equal 2 which is daemon.err where most of your hardware alerts should show up.</td><td>
Create Rule Wizard
Rule Type
General
Build Event Expression
Configure Alerts
Help
Insert
Delete
Formula
&lt; Previous
Next &gt;
Create
Cancel
Build Event Expression
Filter one or more events
Build the expression to filter one or more events:
Parameter Name | Operator | Value
AND
Severity | Equals | 4
Facility | Equals | 3</td></tr>
<tr><td>7</td><td>Fill in the following fields:

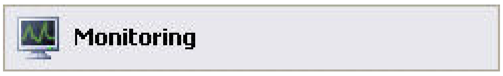
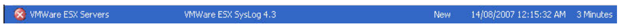
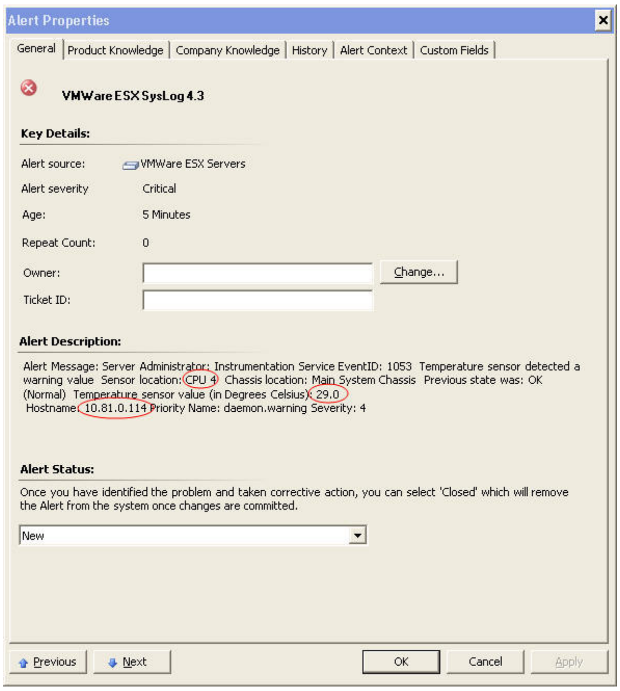
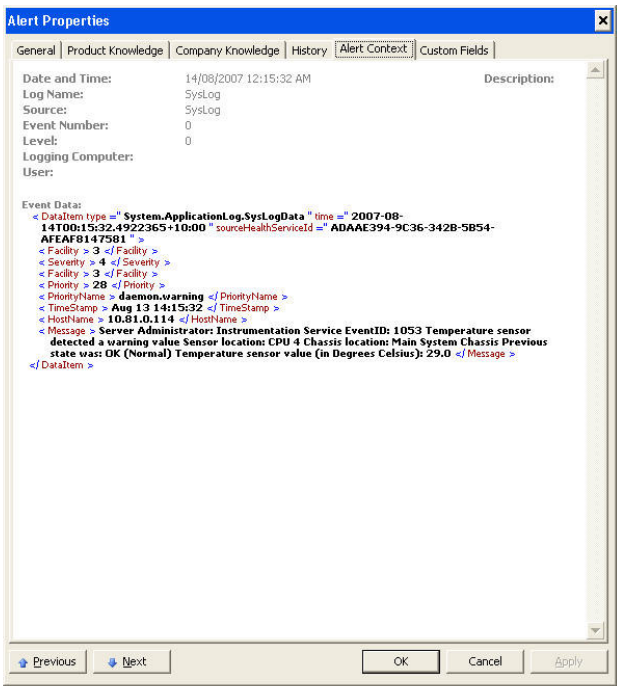
Alert Description
Alert Message: $Data/EventData/DataItem/Message$ Hostname: $Data/EventData/DataItem/HostName$ Priority Name: $Data/EventData/DataItem/PriorityName$ Severity: $Data/EventData/DataItem/Severity$

Click Create</td><td>
Create Rule Wizard
Rule Type
General
Build Event Expression
Configure Alerts
Help
Custom alert fields...
Alert suppression...
&lt; Previous
Next &gt;
Create
Cancel
Configure Alerts
Specify the information that will be generated by the alert
Alert name: VMWare ESX SysLog 4.3
Priority: Medium
Alert description: Alert Message: $Data/EventData/DataItem/Message$ Hostname: $Data/EventData/DataItem/HostName$ Priority Name: $Data/EventData/DataItem/PriorityName$ Severity: $Data/EventData/DataItem/Severity$
Severity: Critical</td></tr>
<tr><td>8</td><td>Open Dell OpenManage website

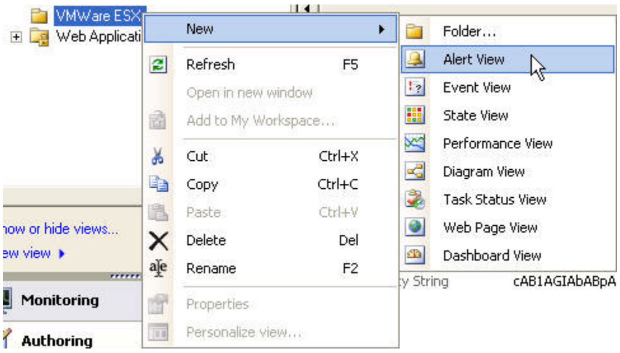
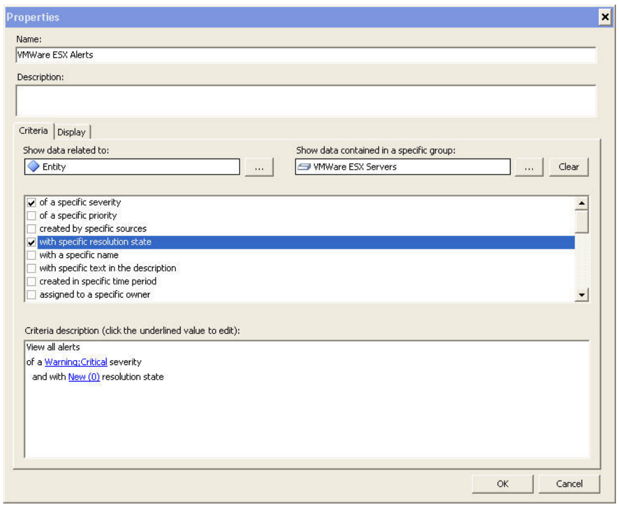
Go to Temperature and change the Maximum Warning Threshold to a value less that the Reading.

Maximum Warning Threshold: **25.0**

Click **Apply Changes**</td><td>
Dell OpenManage Server Administrator
DELL
Properties
Alert Management
System
Main System Ch
BIOS
Fans
Firmware
Intrusion
Memory
Network
Ports
Power Supplie
Processors
Slots
Temperature
Voltages
Software
Storage
80.0 C
25.0 C
10.0 C
5.0 C
[redacted]
Temperature Probes
CPU 1
Status : Non-Critical
Reading : 33.0 C
Minimum Failure Threshold : 5.0 C
Maximum Failure Threshold : 80.0 C
Threshold Settings : ● Set to Default
: ○ Set to Values
Minimum Warning Threshold : 10.0 C
Maximum Warning Threshold : 25.0 C</td></tr>
<tr><td>9</td><td>Open the **System Center Operations Manager Console**</td><td>
</td></tr>
</table>

Step	Action/Outcome	Reference
10	Click on the **Monitoring** tab	 Monitoring
11	Select **Active Alerts** You should see an alert in the Active Alerts View	 VMWare ESX Servers · VMWare ESX SysLog 4.3 · New · 14/08/2007 12:15:32 AM · 3 Minutes
12	Double-click the active **VMWare ESX 4.3 Alert** !! Note the Alert Description	 Alert Properties General | Product Knowledge | Company Knowledge | History | Alert Context | Custom Fields VMWare ESX SysLog 4.3 **Key Details:** Alert source: VMWare ESX Servers Alert severity: Critical Age: 5 Minutes Repeat Count: 0 Owner: [Change...] Ticket ID: **Alert Description:** Alert Message: Server Administrator: Instrumentation Service EventID: 1053 Temperature sensor detected a warning value Sensor location: CPU 4 Chassis location: Main System Chassis Previous state was: OK (Normal) Temperature sensor value (in Degrees Celsius): 29.0 Hostname: 10.81.0.114 Priority Name: daemon.warning Severity: 4 **Alert Status:** Once you have identified the problem and taken corrective action, you can select 'Closed' which will remove the Alert from the system once changes are committed. New Previous · Next · OK · Cancel · Apply
13	Select the **Alert Context** tab !! Note the Event Data	 Alert Properties General | Product Knowledge | Company Knowledge | History | Alert Context | Custom Fields Date and Time: 14/08/2007 12:15:32 AM Description: Log Name: SysLog Source: SysLog Event Number: 0 Level: 0 Logging Computer: User: Event Data: < DataItem type =" System.ApplicationLog.SysLogData " time =" 2007-08-14T00:15:32.4922365+10:00 " sourceHealthServiceId =" ADAAE394-9C36-342B-5B54-AFEAF8147581 " > < Facility > 3 </ Facility > < Severity > 4 </ Severity > < Facility > 3 </ Facility > < Priority > 28 </ Priority > < PriorityName > daemon.warning </ PriorityName > < TimeStamp > Aug 13 14:15:32 </ TimeStamp > < HostName > 10.81.0.114 </ HostName > < Message > Server Administrator: Instrumentation Service EventID: 1053 Temperature sensor detected a warning value Sensor location: CPU 4 Chassis location: Main System Chassis Previous state was: OK (Normal) Temperature sensor value (in Degrees Celsius): 29.0 </ Message > </ DataItem > Previous · Next · OK · Cancel · Apply

4.2 Create VMWare ESX Alerts (Alert View)

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Monitoring** tab	
3	In the Navigation Pane Right-click **VMWare ESX** Select **New** Select **Alert View**	 VMWare ESX Web Applicati New Refresh F5 Open in new window Add to My Workspace… Cut Ctrl+X Copy Ctrl+C Paste Ctrl+V Delete Del Rename F2 Properties Personalize view… Folder… Alert View Event View State View Performance View Diagram View Task Status View Web Page View Dashboard View ow or hide views… ew view Monitoring Authoring y String cAB1AGIAbABpA
4	Fill in the following Fields: Name: **VMWare ESX Alerts** Show data contained in a specific group: **VMWare ESX Servers** Tick ☑ **of a specific severity** Click specific Tick ☑ **Warning** Tick ☑ **Critical** Click OK Tick ☑ **with specific resolution state** Click specific Tick ☑ **New (0)** Click OK Click OK	Properties Name: VMWare ESX Alerts Description: Criteria | Display Show data related to: Entity Show data contained in a specific group: VMWare ESX Servers ☑ of a specific severity ☐ of a specific priority ☐ created by specific sources ☑ with specific resolution state ☐ with a specific name ☐ with specific text in the description ☐ created in specific time period ☐ assigned to a specific owner Criteria description (click the underlined value to edit): View all alerts of a Warning;Critical severity and with New (0) resolution state OK Cancel

5 SCOM SNMP Configurations

This section will be written differently as this is where I will endeavour to, as the saying goes, "Teach you to fish instead of giving you the fish". I am writing this section this way because depending on your Hardware Vendor etc you will be using different data and the screens could look different to the examples I will use. However, I hope to demonstrate the techniques required to create a monitor.

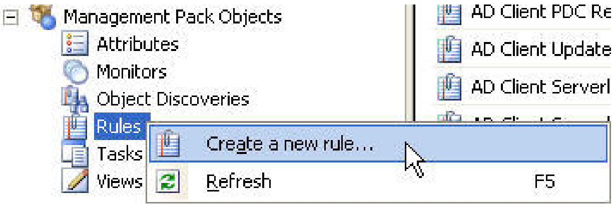
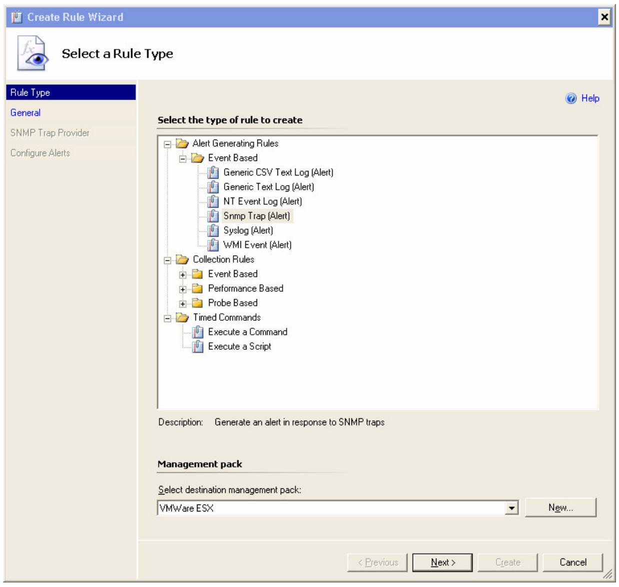
To understand this process you will need to understand a little about SNMP and OID's. First we will be setting up a capture for all Traps from a specific device and MIB OID. Second, we will use the data gained to create a Monitor for a specific requirement.

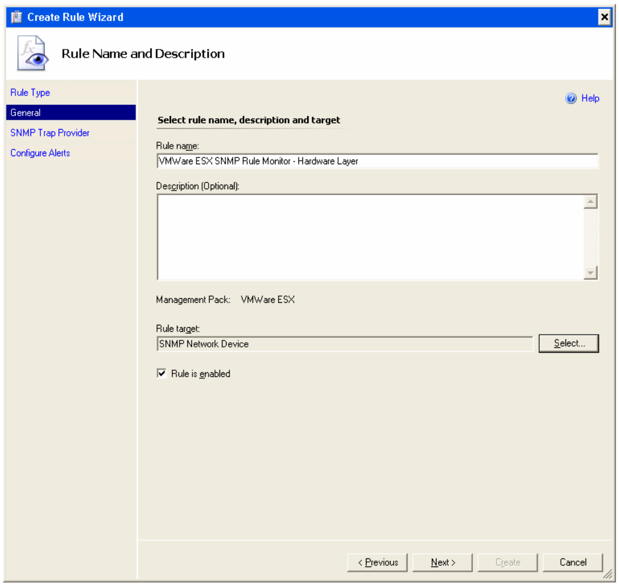
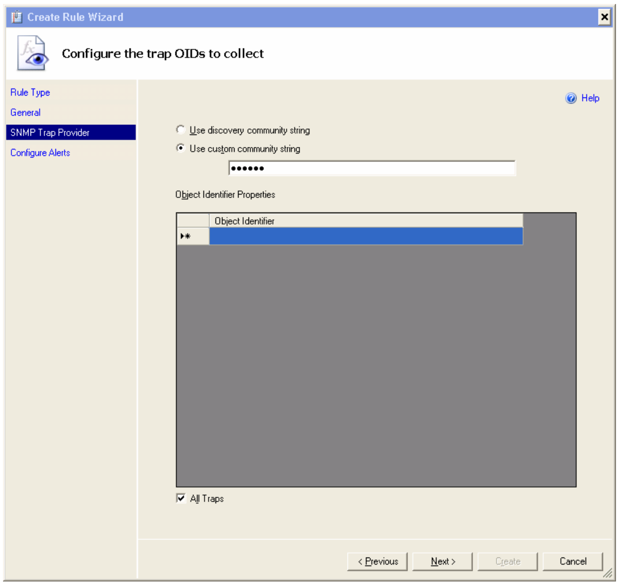
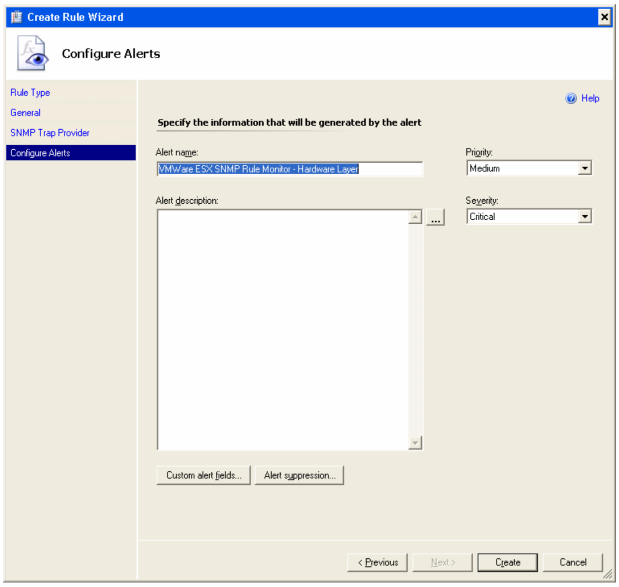
5.1 Create 'Trap Rule' to capture Events from the hardware layer

We need to create a Trap Rule to find out the OID of the Hardware layer being used. In this example I am using Dell Hardware.

You can also find out MIB OID info from the following sites: (More can be found in Chapter 1.6.2)

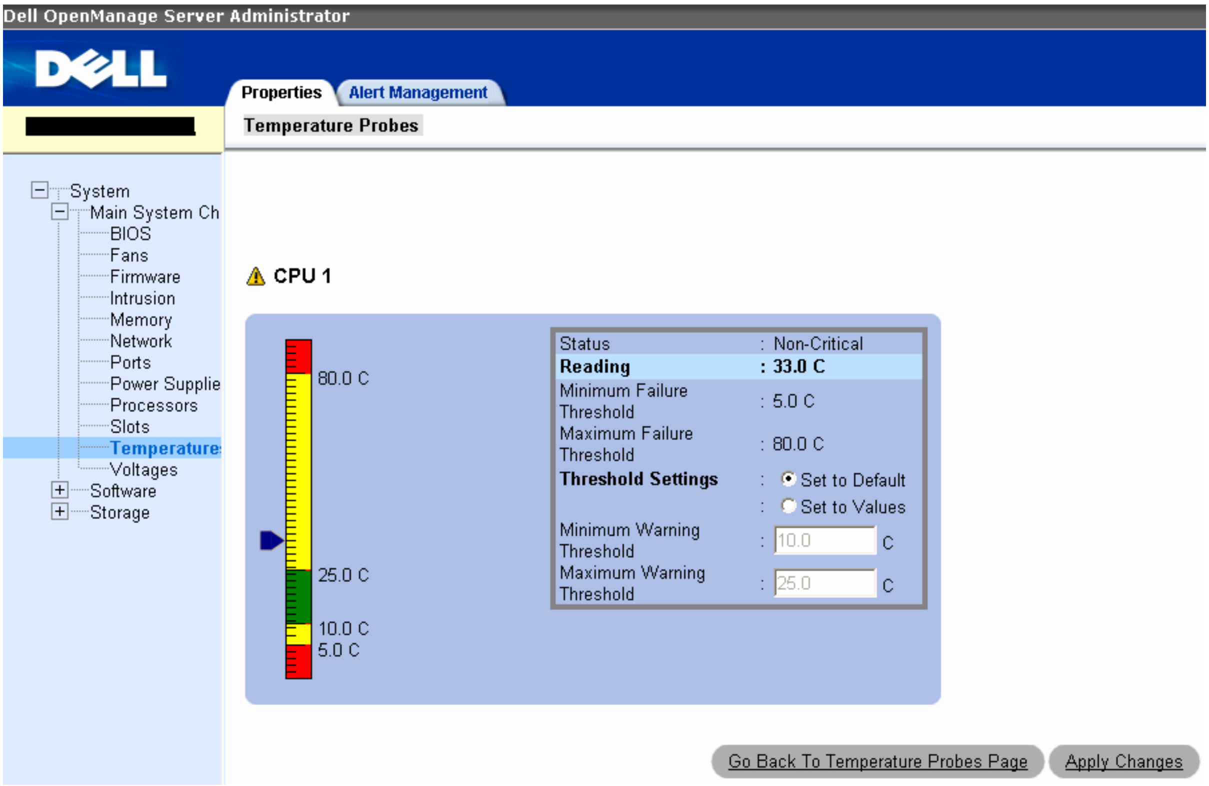
- http://www.oidview.com/mibs/detail.html
- http://support.ipmonitor.com/mibs_byoidtree.aspx

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Rules** Select **Create a new rule…**	 Management Pack Objects Attributes Monitors Object Discoveries Rules Tasks Views AD Client PDC Re AD Client Update AD Client Serverl Create a new rule… Refresh F5
4	Under Alert Generating Rule\Event Based Select **Snmp Trap (Alert)** Under Management Pack Select **VMWare ESX** Click Next > Note: Do not select Syslog under collection rules as you will not get any alerts generated.	 Create Rule Wizard Select a Rule Type Rule Type General SNMP Trap Provider Configure Alerts Help Select the type of rule to create Alert Generating Rules Event Based Generic CSV Text Log (Alert) Generic Text Log (Alert) NT Event Log (Alert) Snmp Trap (Alert) Syslog (Alert) WMI Event (Alert) Collection Rules Event Based Performance Based Probe Based Timed Commands Execute a Command Execute a Script Management pack New... < Previous Next > Create Cancel Description: Generate an alert in response to SNMP traps Select destination management pack: VMWare ESX

Step	Action/Outcome	Reference
5	Fill in the following fields: Rule Name: **VMWare ESX SNMP Rule Monitor - Hardware Layer** Under Monitor target: Select **SNMP Network Device** Click Next > Note: You must select SNMP Network Device for this type of rule to work.	 Create Rule Wizard Rule Name and Description Select rule name, description and target Rule name: VMWare ESX SNMP Rule Monitor - Hardware Layer Description (Optional): Management Pack: VMWare ESX Rule target: SNMP Network Device ☑ Rule is enabled Rule Type General SNMP Trap Provider Configure Alerts Help Select... < Previous Next > Create Cancel
6	Select **Use custom community string** Type **public** (or what ever you have setup in your ESX snmpd.conf file) Tick ☑ **All Traps** Click Next >	 Create Rule Wizard Configure the trap OIDs to collect ○ Use discovery community string ● Use custom community string •••••• Object Identifier Properties Object Identifier ☑ All Traps Rule Type General SNMP Trap Provider Configure Alerts Help < Previous Next > Create Cancel
7	Click Create	 Create Rule Wizard Configure Alerts Specify the information that will be generated by the alert Alert name: VMWare ESX SNMP Rule Monitor - Hardware Layer Priority: Medium Alert description: Severity: Critical Rule Type General SNMP Trap Provider Configure Alerts Help Custom alert fields... Alert suppression... < Previous Next > Create Cancel

- To test we will now generate two Hardware alerts. To demonstrate I will change the Temperature setting of the CPU through **Dell OpenManage**. Secondly, I will remove a physical Hard Disk.

- First we will change the Threshold Settings of a CPU to be beneath the current temperature reading. This will now generate an SNMP Trap that SCOM will receive.



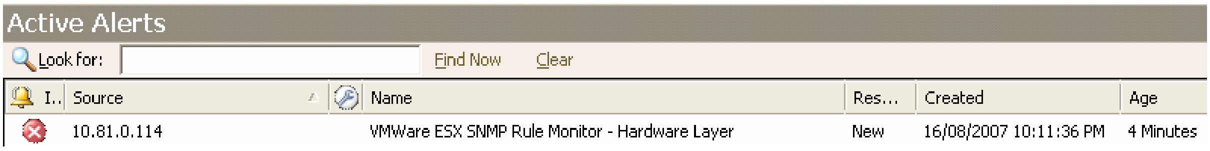
[redacted]

Temperature Probes

CPU 1

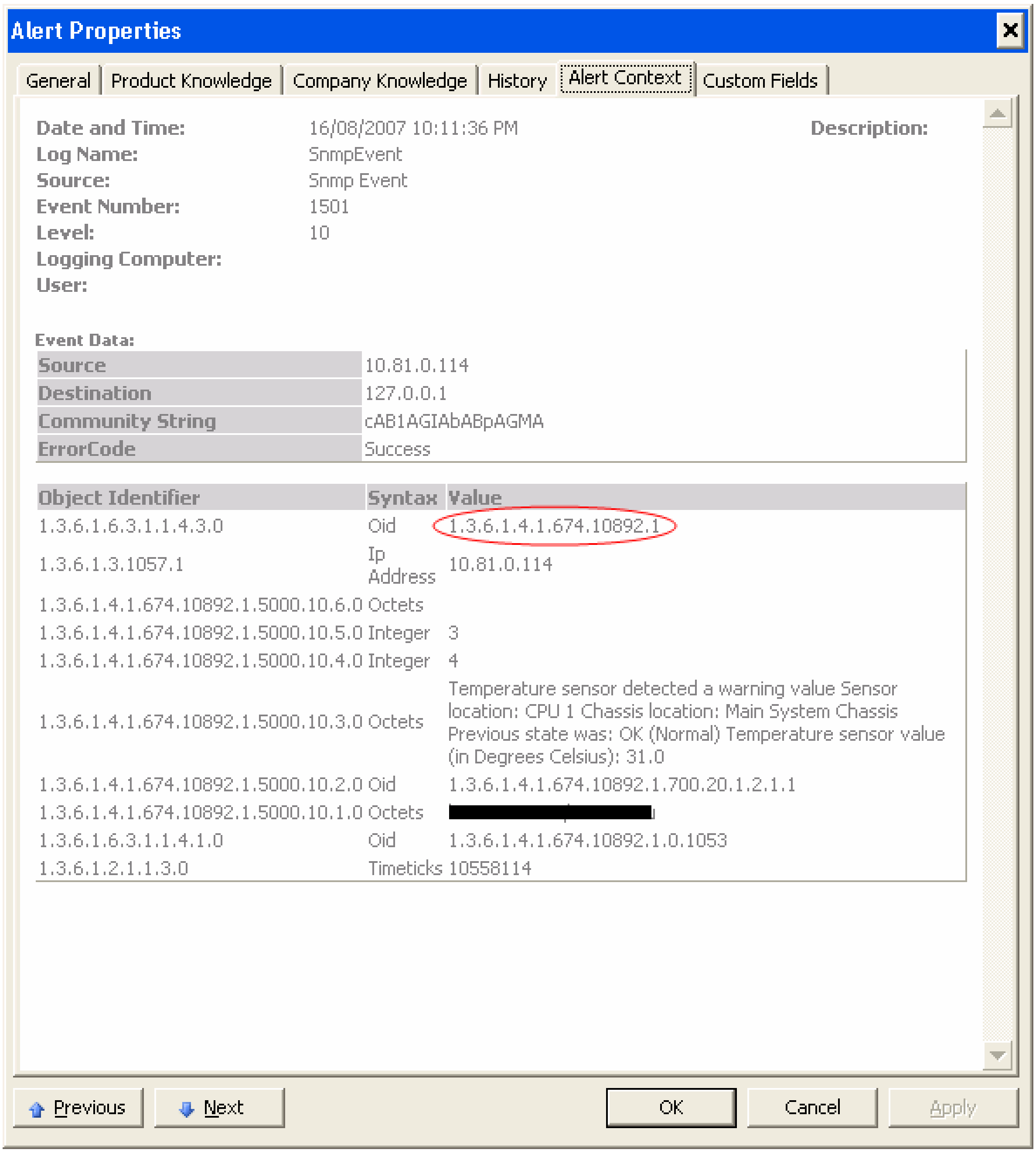
Status	:	Non-Critical
Reading	:	**33.0 C**
Minimum Failure Threshold	:	5.0 C
Maximum Failure Threshold	:	80.0 C
Threshold Settings	:	● Set to Default
	:	○ Set to Values
Minimum Warning Threshold	:	10.0 C
Maximum Warning Threshold	:	25.0 C

- If you open the Operations Manager Console and look in Active Alerts and you will see the **VMWare ESX SNMP Rule Monitor – Hardware Layer** alert.



I..	Source	Name	Res...	Created	Age
⊗	10.81.0.114	VMWare ESX SNMP Rule Monitor - Hardware Layer	New	16/08/2007 10:11:36 PM	4 Minutes

- Double click on the alert and click on the Alert Context tab, and you will see the OID for the Dell Server. The first parameter of the SNMP trap is the OID, 1.3.6.1.4.1.674.10892.1 this represents the Hardware Layer. The 764 of the number indicated that OID is from a DELL MIB. See Appendix B for more.



Date and Time: 16/08/2007 10:11:36 PM

Log Name: SnmpEvent

Source: Snmp Event

Event Number: 1501

Level: 10

Logging Computer:

User:

Description:

Event Data:

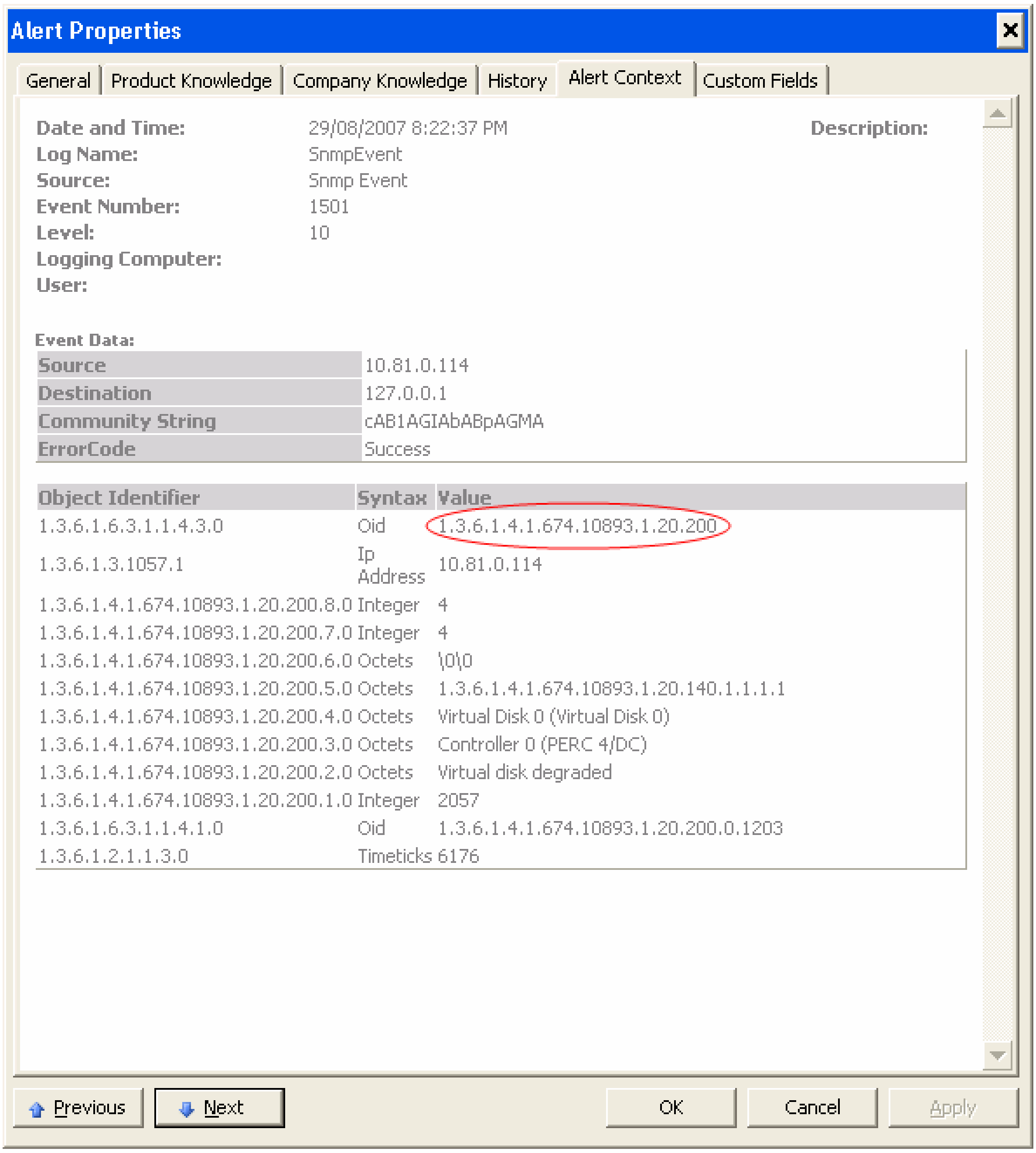
Source	10.81.0.114
Destination	127.0.0.1
Community String	cAB1AGIAbABpAGMA
ErrorCode	Success

Object Identifier	Syntax	Value
1.3.6.1.6.3.1.1.4.3.0	Oid	1.3.6.1.4.1.674.10892.1
1.3.6.1.3.1057.1	Ip Address	10.81.0.114
1.3.6.1.4.1.674.10892.1.5000.10.6.0	Octets	
1.3.6.1.4.1.674.10892.1.5000.10.5.0	Integer	3
1.3.6.1.4.1.674.10892.1.5000.10.4.0	Integer	4
1.3.6.1.4.1.674.10892.1.5000.10.3.0	Octets	Temperature sensor detected a warning value Sensor location: CPU 1 Chassis location: Main System Chassis Previous state was: OK (Normal) Temperature sensor value (in Degrees Celsius): 31.0
1.3.6.1.4.1.674.10892.1.5000.10.2.0	Oid	1.3.6.1.4.1.674.10892.1.700.20.1.2.1.1
1.3.6.1.4.1.674.10892.1.5000.10.1.0	Octets	[redacted]
1.3.6.1.6.3.1.1.4.1.0	Oid	1.3.6.1.4.1.674.10892.1.0.1053
1.3.6.1.2.1.1.3.0	Timeticks	10558114

- To prove this point and provide another example, this time I will remove a Hard Disk. I received 2 alerts:

- First is one to show the Virtual Disk is degraded, note that it uses a different MIB and the structure of the alert is different. This is not always the case and is dependent on how your hardware vendors structure their MIB's which is why its important to do this type of discovery and testing for your particular hardware.

- Now is a good time to point out that the first 2 rows of the content are the same, row 1 is the OID and row 2 is the IP Address. We will use this as a base for when we are creating our Monitors.



Date and Time: 29/08/2007 8:22:37 PM
Log Name: SnmpEvent
Source: Snmp Event
Event Number: 1501
Level: 10
Logging Computer:
User:

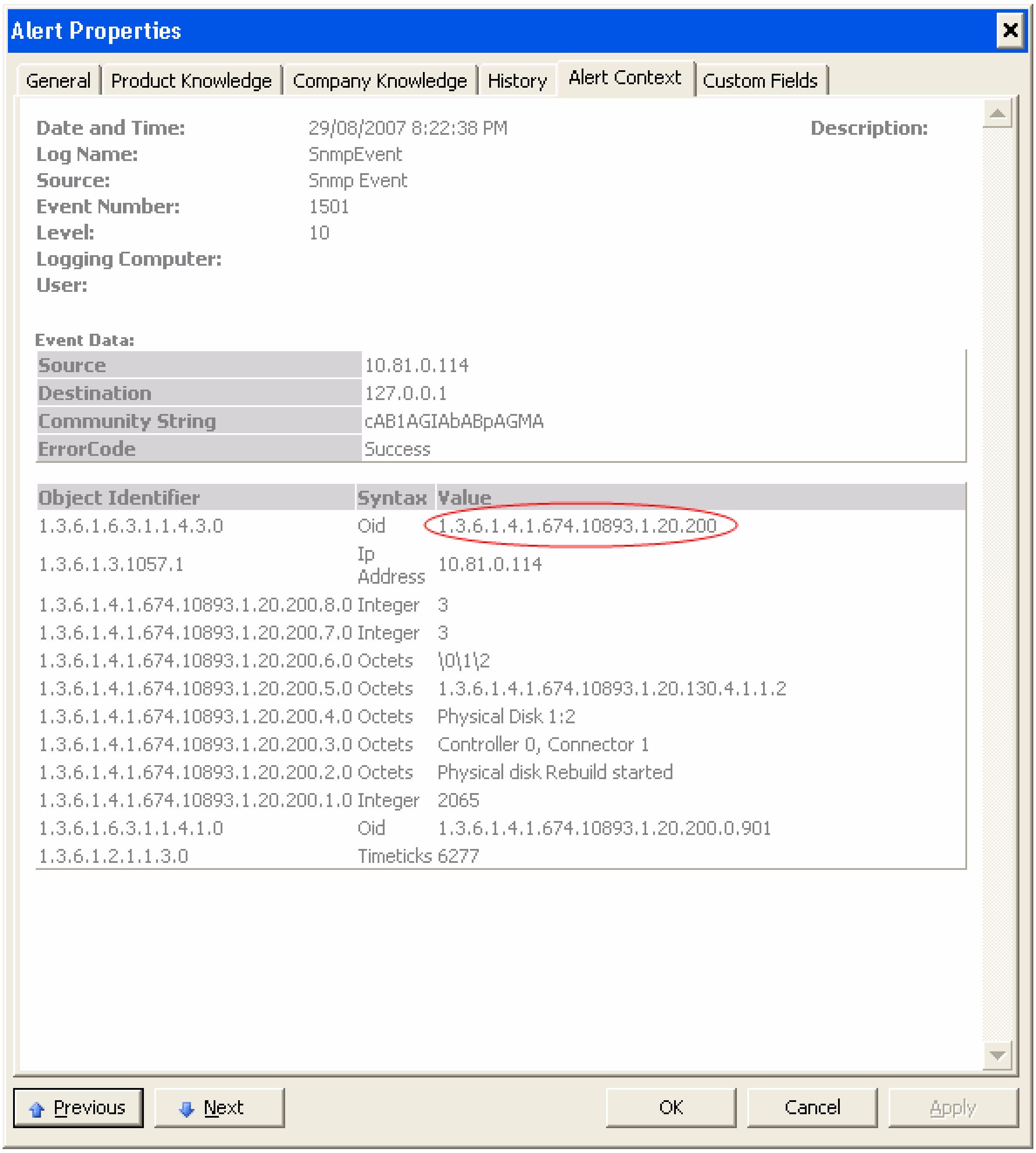
Description:

Event Data:

Source	10.81.0.114
Destination	127.0.0.1
Community String	cAB1AGIAbABpAGMA
ErrorCode	Success

Object Identifier	Syntax	Value
1.3.6.1.6.3.1.1.4.3.0	Oid	1.3.6.1.4.1.674.10893.1.20.200
1.3.6.1.3.1057.1	Ip Address	10.81.0.114
1.3.6.1.4.1.674.10893.1.20.200.8.0	Integer	4
1.3.6.1.4.1.674.10893.1.20.200.7.0	Integer	4
1.3.6.1.4.1.674.10893.1.20.200.6.0	Octets	\0\0
1.3.6.1.4.1.674.10893.1.20.200.5.0	Octets	1.3.6.1.4.1.674.10893.1.20.140.1.1.1.1
1.3.6.1.4.1.674.10893.1.20.200.4.0	Octets	Virtual Disk 0 (Virtual Disk 0)
1.3.6.1.4.1.674.10893.1.20.200.3.0	Octets	Controller 0 (PERC 4/DC)
1.3.6.1.4.1.674.10893.1.20.200.2.0	Octets	Virtual disk degraded
1.3.6.1.4.1.674.10893.1.20.200.1.0	Integer	2057
1.3.6.1.6.3.1.1.4.1.0	Oid	1.3.6.1.4.1.674.10893.1.20.200.0.1203
1.3.6.1.2.1.1.3.0	Timeticks	6176

- Second, you will see that the Rebuild has started, again note the OID.



Date and Time: 29/08/2007 8:22:38 PM
Log Name: SnmpEvent
Source: Snmp Event
Event Number: 1501
Level: 10
Logging Computer:
User:
Description:

Event Data:

Source	10.81.0.114
Destination	127.0.0.1
Community String	cAB1AGIAbABpAGMA
ErrorCode	Success

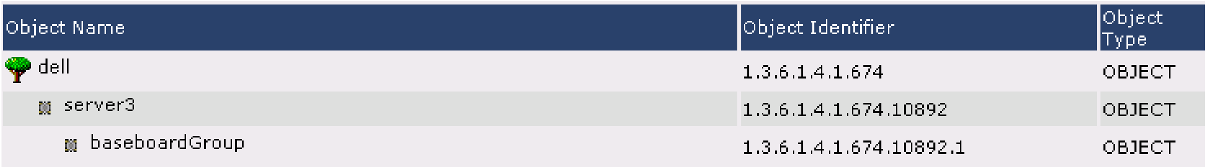
Object Identifier	Syntax	Value
1.3.6.1.6.3.1.1.4.3.0	Oid	1.3.6.1.4.1.674.10893.1.20.200
1.3.6.1.3.1057.1	Ip Address	10.81.0.114
1.3.6.1.4.1.674.10893.1.20.200.8.0	Integer	3
1.3.6.1.4.1.674.10893.1.20.200.7.0	Integer	3
1.3.6.1.4.1.674.10893.1.20.200.6.0	Octets	\0\1\2
1.3.6.1.4.1.674.10893.1.20.200.5.0	Octets	1.3.6.1.4.1.674.10893.1.20.130.4.1.1.2
1.3.6.1.4.1.674.10893.1.20.200.4.0	Octets	Physical Disk 1:2
1.3.6.1.4.1.674.10893.1.20.200.3.0	Octets	Controller 0, Connector 1
1.3.6.1.4.1.674.10893.1.20.200.2.0	Octets	Physical disk Rebuild started
1.3.6.1.4.1.674.10893.1.20.200.1.0	Integer	2065
1.3.6.1.6.3.1.1.4.1.0	Oid	1.3.6.1.4.1.674.10893.1.20.200.0.901
1.3.6.1.2.1.1.3.0	Timeticks	6277

☝

See Appendix B for a list of Common Enterprise OID's.

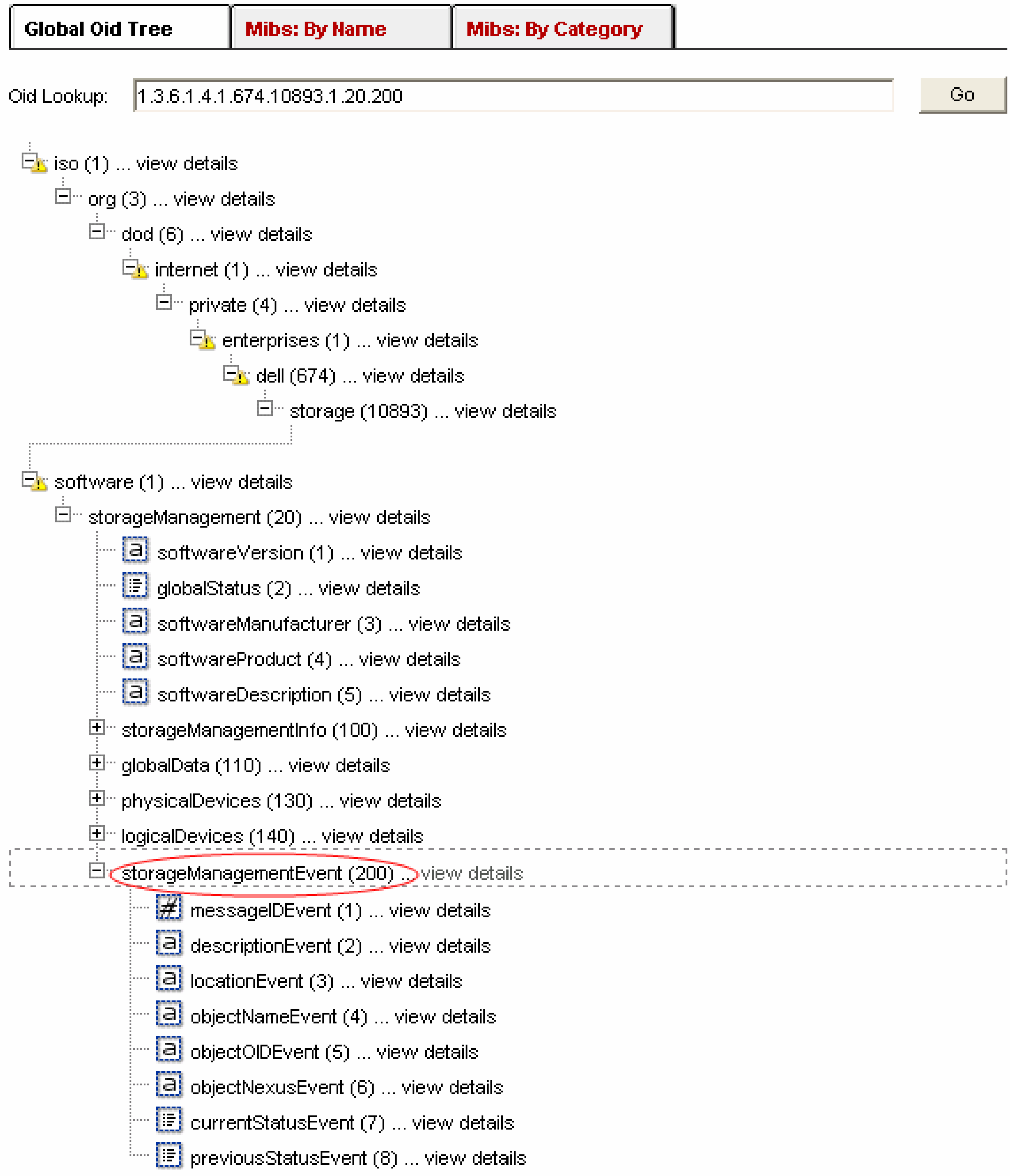
- You can now find out exactly what these OID's are by using sites listed in Chapter 1.6.2.
- Here are the details of the 2 OID's I have received from 2 different sites.

OID produced by Temperature.



Object Name	Object Identifier	Object Type
dell	1.3.6.1.4.1.674	OBJECT
server3	1.3.6.1.4.1.674.10892	OBJECT
baseboardGroup	1.3.6.1.4.1.674.10892.1	OBJECT

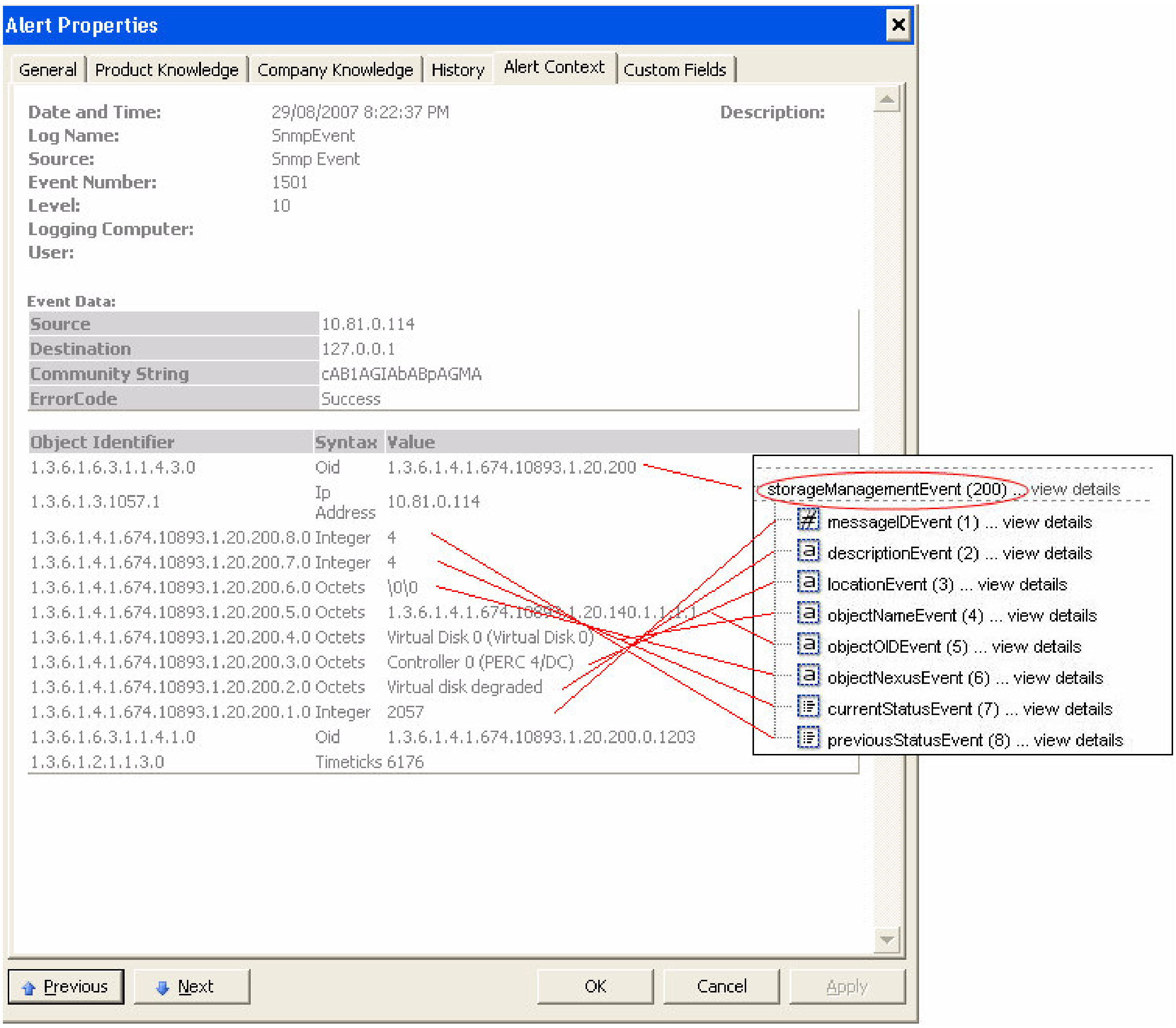
OID produced by Hard Disk failure



Oid Lookup: 1.3.6.1.4.1.674.10893.1.20.200

```
iso (1) ... view details
    org (3) ... view details
        dod (6) ... view details
            internet (1) ... view details
                private (4) ... view details
                    enterprises (1) ... view details
                        dell (674) ... view details
                            storage (10893) ... view details
software (1) ... view details
    storageManagement (20) ... view details
        softwareVersion (1) ... view details
        globalStatus (2) ... view details
        softwareManufacturer (3) ... view details
        softwareProduct (4) ... view details
        softwareDescription (5) ... view details
        storageManagementInfo (100) ... view details
        globalData (110) ... view details
        physicalDevices (130) ... view details
        logicalDevices (140) ... view details
        storageManagementEvent (200) ... view details
            messageIDEvent (1) ... view details
            descriptionEvent (2) ... view details
            locationEvent (3) ... view details
            objectNameEvent (4) ... view details
            objectOIDEvent (5) ... view details
            objectNexusEvent (6) ... view details
            currentStatusEvent (7) ... view details
            previousStatusEvent (8) ... view details
```

- If we take this information and overlay it with our alert you can see from the below images how the OID data relates to the Alert generated in SCOM.



Date and Time: 29/08/2007 8:22:37 PM

Log Name: SnmpEvent

Source: Snmp Event

Event Number: 1501

Level: 10

Logging Computer:

User:

Description:

Event Data:

Source	10.81.0.114
Destination	127.0.0.1
Community String	cAB1AGIAbABpAGMA
ErrorCode	Success

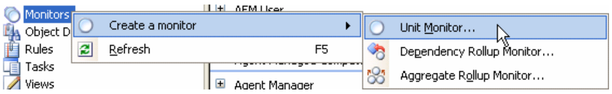
Object Identifier	Syntax	Value
1.3.6.1.6.3.1.1.4.3.0	Oid	1.3.6.1.4.1.674.10893.1.20.200
1.3.6.1.3.1057.1	Ip Address	10.81.0.114
1.3.6.1.4.1.674.10893.1.20.200.8.0	Integer	4
1.3.6.1.4.1.674.10893.1.20.200.7.0	Integer	4
1.3.6.1.4.1.674.10893.1.20.200.6.0	Octets	\0\0
1.3.6.1.4.1.674.10893.1.20.200.5.0	Octets	1.3.6.1.4.1.674.10893.1.20.140.1.1.1.1
1.3.6.1.4.1.674.10893.1.20.200.4.0	Octets	Virtual Disk 0 (Virtual Disk 0)
1.3.6.1.4.1.674.10893.1.20.200.3.0	Octets	Controller 0 (PERC 4/DC)
1.3.6.1.4.1.674.10893.1.20.200.2.0	Octets	Virtual disk degraded
1.3.6.1.4.1.674.10893.1.20.200.1.0	Integer	2057
1.3.6.1.6.3.1.1.4.1.0	Oid	1.3.6.1.4.1.674.10893.1.20.200.0.1203
1.3.6.1.2.1.1.3.0	Timeticks	6176

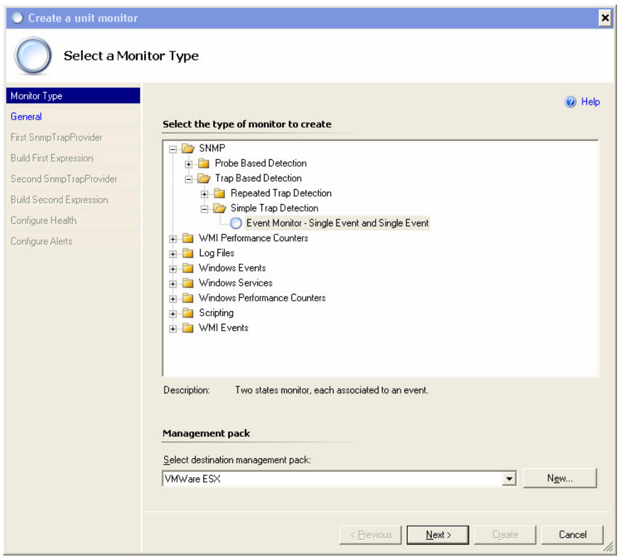
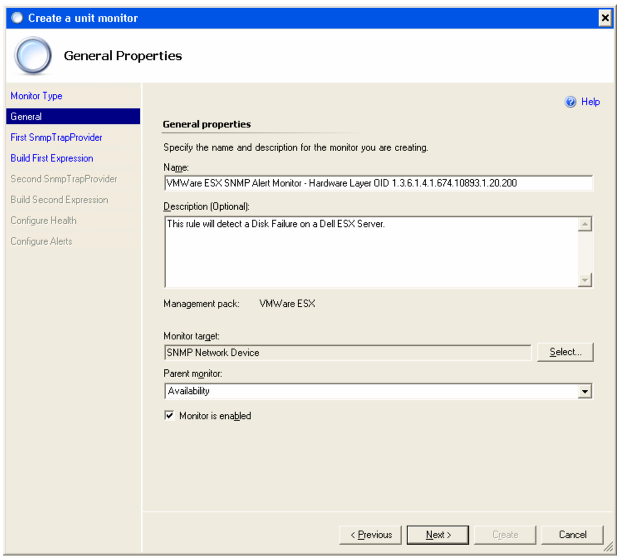
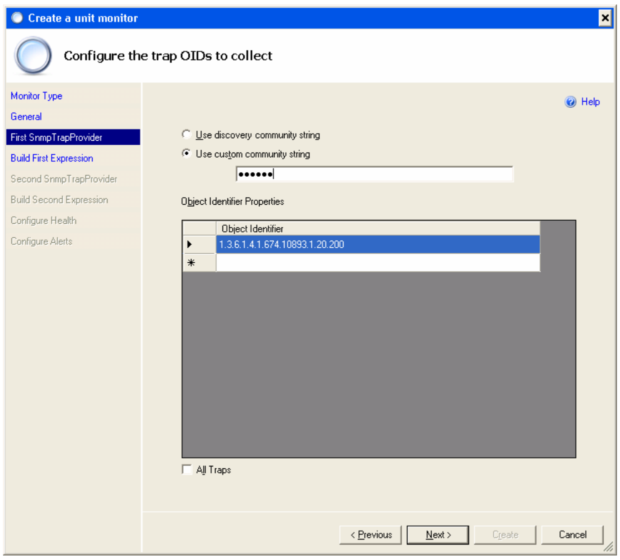
storageManagementEvent (200) ... view details
- messageIDEvent (1) ... view details
- descriptionEvent (2) ... view details
- locationEvent (3) ... view details
- objectNameEvent (4) ... view details
- objectOIDEvent (5) ... view details
- objectNexusEvent (6) ... view details
- currentStatusEvent (7) ... view details
- previousStatusEvent (8) ... view details

- Knowing this information allows us to prepare for the creation of a Monitor and to build an Expression for the Hardware Layer.

5.2 Create a 'Trap Monitor' for Alerting

- Now we will create a monitor, however you can create as many as you require to give you as much or as little information you desire.

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Monitors** Select **Create a monitor** Select **Unit Monitor…**	 Monitors Object D Rules Tasks Views Create a monitor Refresh F5 AEM User Agent Manager Unit Monitor… Dependency Rollup Monitor… Aggregate Rollup Monitor…

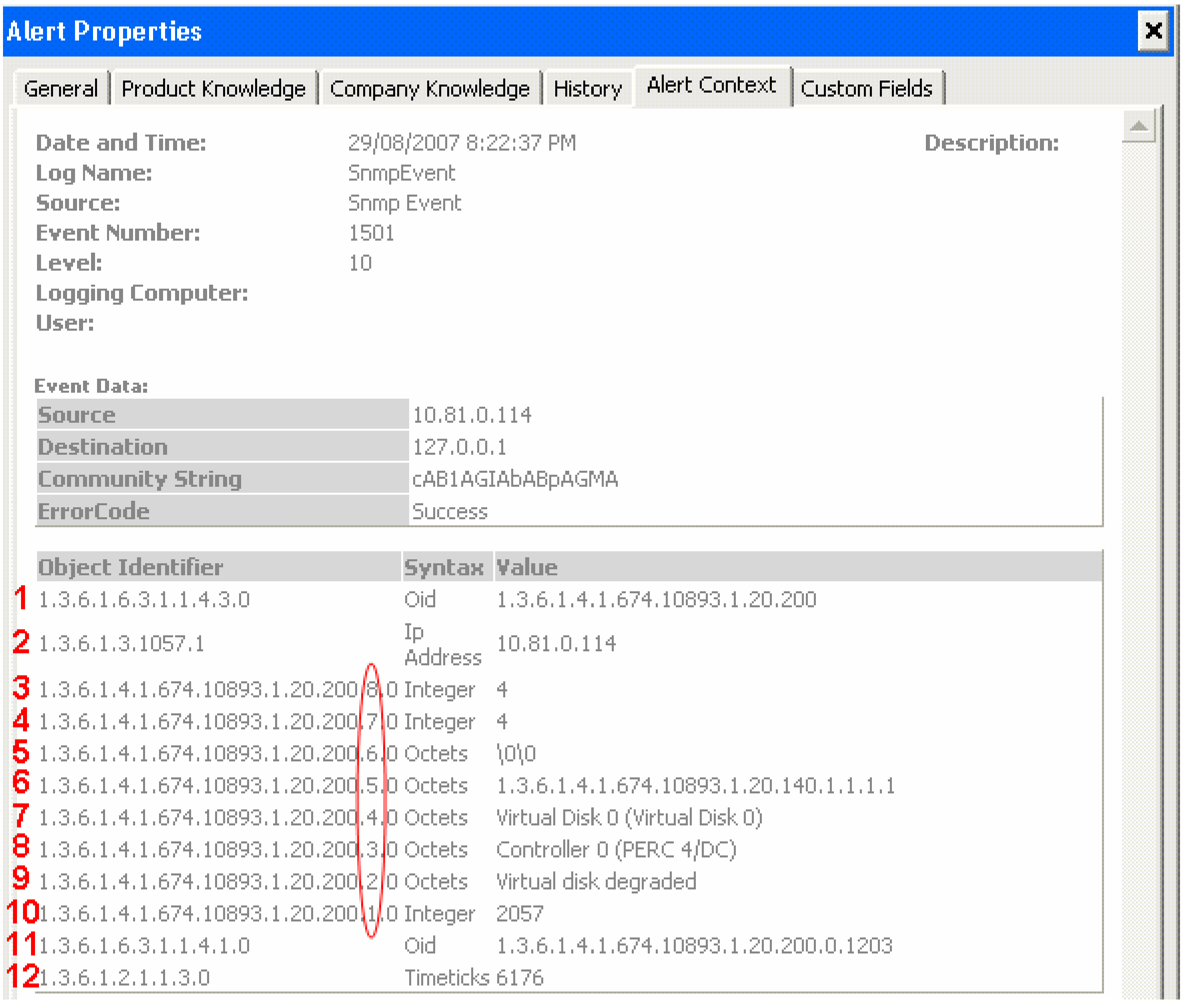
Step	Action/Outcome	Reference
4	Expand SNMP + Trap Based Detection + Simple Trap Detection Select **Event Monitor – Single Event and Single Event** Under Management Pack Select **VMWare ESX** Click Next >	 Create a unit monitor Select a Monitor Type Select the type of monitor to create SNMP Probe Based Detection Trap Based Detection Repeated Trap Detection Simple Trap Detection Event Monitor - Single Event and Single Event WMI Performance Counters Log Files Windows Events Windows Services Windows Performance Counters Scripting WMI Events Description: Two states monitor, each associated to an event. Management pack Select destination management pack: VMWare ESX
5	Fill in the following fields: Name: **VMWare ESX SNMP Alert Monitor - Hardware Layer OID 1.3.6.1.4.1.674.10893.1.20.200** Monitor target: Select **SNMP Network Device** Parent Monitor: Select **Availability** Click Next > Note: You must select SNMP Network Device for this type of monitor to work.	 Create a unit monitor General Properties General properties Specify the name and description for the monitor you are creating. Name: VMWare ESX SNMP Alert Monitor - Hardware Layer OID 1.3.6.1.4.1.674.10893.1.20.200 Description (Optional): This rule will detect a Disk Failure on a Dell ESX Server. Management pack: VMWare ESX Monitor target: SNMP Network Device Parent monitor: Availability ☑ Monitor is enabled
6	Select **Use custom community string** Type **public** (or what ever you have configured in your ESX snmpd.conf file) Under Object Identifier Properties Type **1.3.6.1.4.1.674.10893.1.20.200** Click Next > Note: This is the OID we just generated and collected after removing a Hard Disk.	 Create a unit monitor Configure the trap OIDs to collect ○ Use discovery community string ● Use custom community string •••••• Object Identifier Properties Object Identifier: 1.3.6.1.4.1.674.10893.1.20.200 □ All Traps

- At this point I will try to provide an understanding of how to come up with the required Parameter Name, Operator and Value you require for the next step.

- The **Parameter Name** field for SNMP refers to the line of data received in an SNMP Event or Alert. For SNMP the Parameter Name will be:

  /DataItem/SnmpVarBinds/SnmpVarBind[X]/Value

  Where X equals the row of interest in the Alert.



Date and Time:	29/08/2007 8:22:37 PM	**Description:**
Log Name:	SnmpEvent	
Source:	Snmp Event	
Event Number:	1501	
Level:	10	
Logging Computer:		
User:		

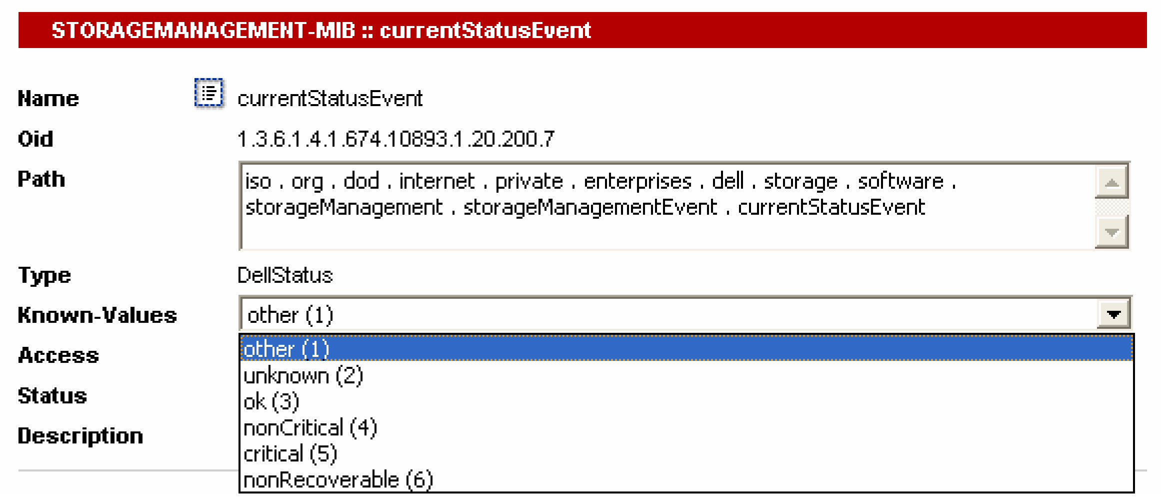
Event Data:

Source	10.81.0.114
Destination	127.0.0.1
Community String	cAB1AGIAbABpAGMA
ErrorCode	Success

	Object Identifier	**Syntax**	**Value**
1	1.3.6.1.6.3.1.1.4.3.0	Oid	1.3.6.1.4.1.674.10893.1.20.200
2	1.3.6.1.3.1057.1	Ip Address	10.81.0.114
3	1.3.6.1.4.1.674.10893.1.20.200.8.0	Integer	4
4	1.3.6.1.4.1.674.10893.1.20.200.7.0	Integer	4
5	1.3.6.1.4.1.674.10893.1.20.200.6.0	Octets	\0\0
6	1.3.6.1.4.1.674.10893.1.20.200.5.0	Octets	1.3.6.1.4.1.674.10893.1.20.140.1.1.1.1
7	1.3.6.1.4.1.674.10893.1.20.200.4.0	Octets	Virtual Disk 0 (Virtual Disk 0)
8	1.3.6.1.4.1.674.10893.1.20.200.3.0	Octets	Controller 0 (PERC 4/DC)
9	1.3.6.1.4.1.674.10893.1.20.200.2.0	Octets	Virtual disk degraded
10	1.3.6.1.4.1.674.10893.1.20.200.1.0	Integer	2057
11	1.3.6.1.6.3.1.1.4.1.0	Oid	1.3.6.1.4.1.674.10893.1.20.200.0.1203
12	1.3.6.1.2.1.1.3.0	Timeticks	6176

NOTE: The issue with how SCOM handles this information is a little backwards, as you can see the next octet after the base OID runs from high to low. Ie: .200.8 is on line 3 and .200.7 is on line 4. Unfortunately all Trap can have as many or as little octets thus making Expressions harder to compile.

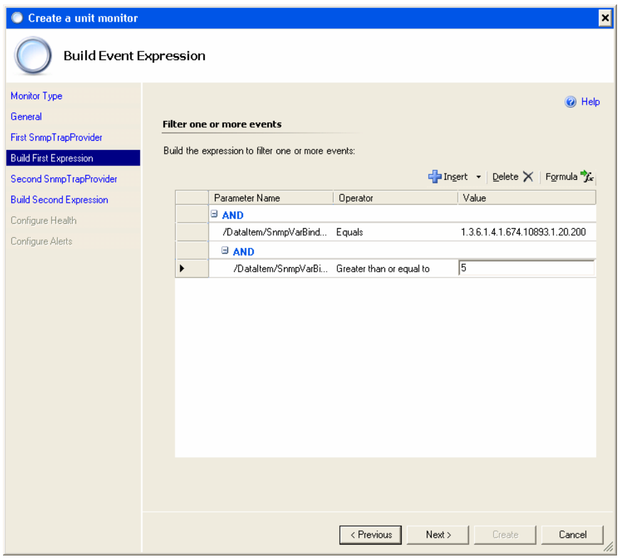
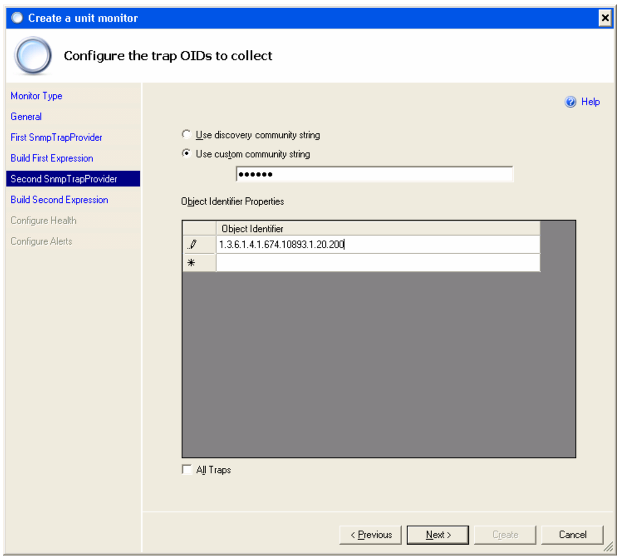
- From one of the many website that have a list of all the MIB I found what the data for the currentStatusEvent field was.



STORAGEMANAGEMENT-MIB :: currentStatusEvent

Name	currentStatusEvent
Oid	1.3.6.1.4.1.674.10893.1.20.200.7
Path	iso . org . dod . internet . private . enterprises . dell . storage . software . storageManagement . storageManagementEvent . currentStatusEvent
Type	DellStatus
Known-Values	other (1)
Access	
Status	
Description	

other (1)
unknown (2)
ok (3)
nonCritical (4)
critical (5)
nonRecoverable (6)

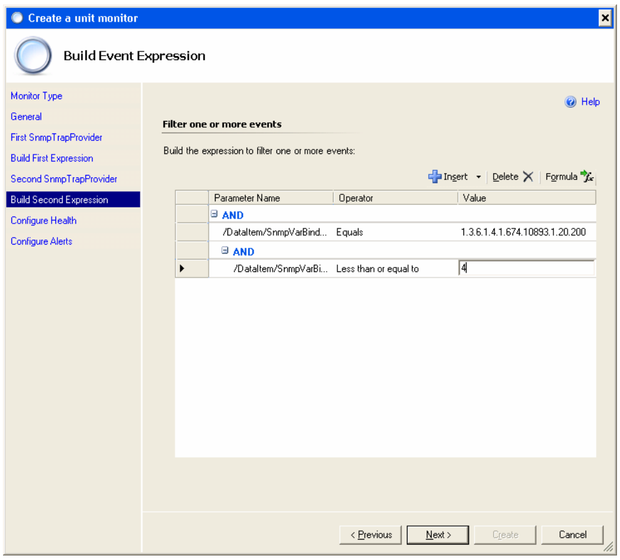
7	To continue we will need to create an Expression. See **Appendix C** for more Expression examples. Click Next >	 Create a unit monitor Build Event Expression Filter one or more events Build the expression to filter one or more events: Parameter Name / Operator / Value AND /DataItem/SnmpVarBind... Equals 1.3.6.1.4.1.674.10893.1.20.200 AND /DataItem/SnmpVarBi... Greater than or equal to 5
8	Select **Use custom community string** Type **public** (or what ever you have setup in your ESX snmpd.conf file) Under Object Identifier Properties Type **1.3.6.1.4.1.674.10893.1.20.200** Click Next > Note: This is the OID we just generated and collected from the 'Hardware Rule'.	 Create a unit monitor Configure the trap OIDs to collect ○ Use discovery community string ● Use custom community string •••••• Object Identifier Properties Object Identifier 1.3.6.1.4.1.674.10893.1.20.200 □ All Traps

9

To continue we will need to create an Expression.

☝
See
Appendix C
for more
Expression
examples.

Click Next >



Create a unit monitor

Build Event Expression

Filter one or more events

Build the expression to filter one or more events:

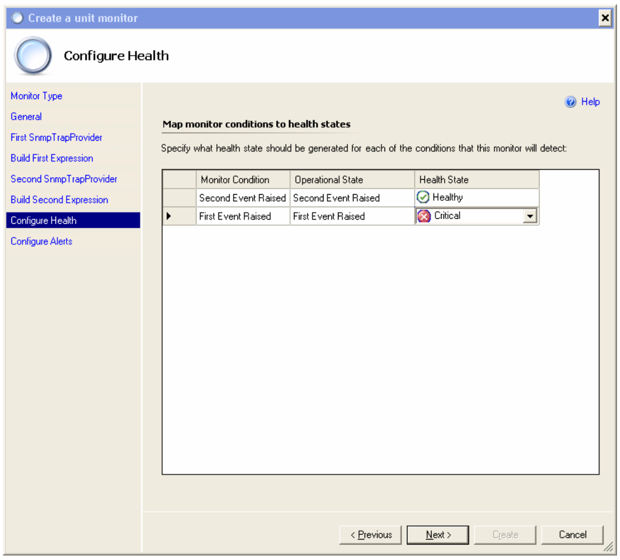
Parameter Name	Operator	Value
⊟ AND		
/DataItem/SnmpVarBind...	Equals	1.3.6.1.4.1.674.10893.1.20.200
⊟ AND		
/DataItem/SnmpVarBi...	Less than or equal to	4

10

This is where we will now specify that if the 1st Expression conditions are met to set the alert to Critical and if the 2nd Expression conditions are met to set the alert back to Healthy.

Change **First Event Raised** Health State to **Critical**

Click Next >



Create a unit monitor

Configure Health

Map monitor conditions to health states

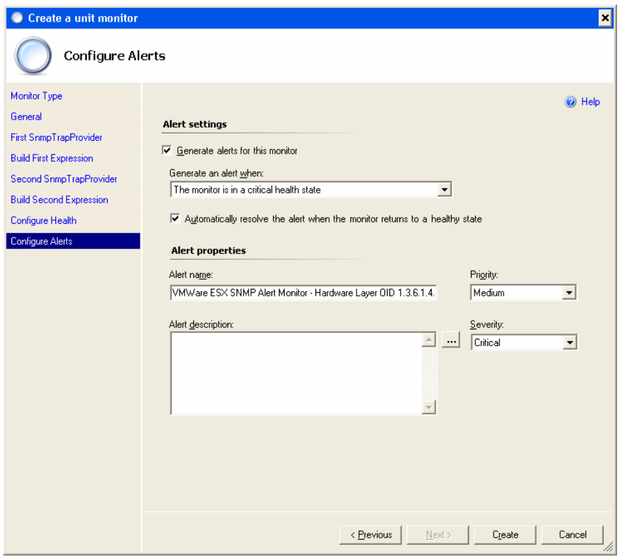
Specify what health state should be generated for each of the conditions that this monitor will detect:

Monitor Condition	Operational State	Health State
Second Event Raised	Second Event Raised	✓ Healthy
First Event Raised	First Event Raised	☒ Critical

11

Tick ☑ **Generate Alerts for this monitor**

Click Create



Create a unit monitor

Configure Alerts

Alert settings

☑ Generate alerts for this monitor

Generate an alert when: The monitor is in a critical health state

☑ Automatically resolve the alert when the monitor returns to a healthy state

Alert properties

Alert name: VMWare ESX SNMP Alert Monitor - Hardware Layer OID 1.3.6.1.4.

Priority: Medium

Alert description:

Severity: Critical

- For steps 7 & 9 you will need to create your own Expression and from the information provided I hope I have shown the method finding out how to figure this out.

☝

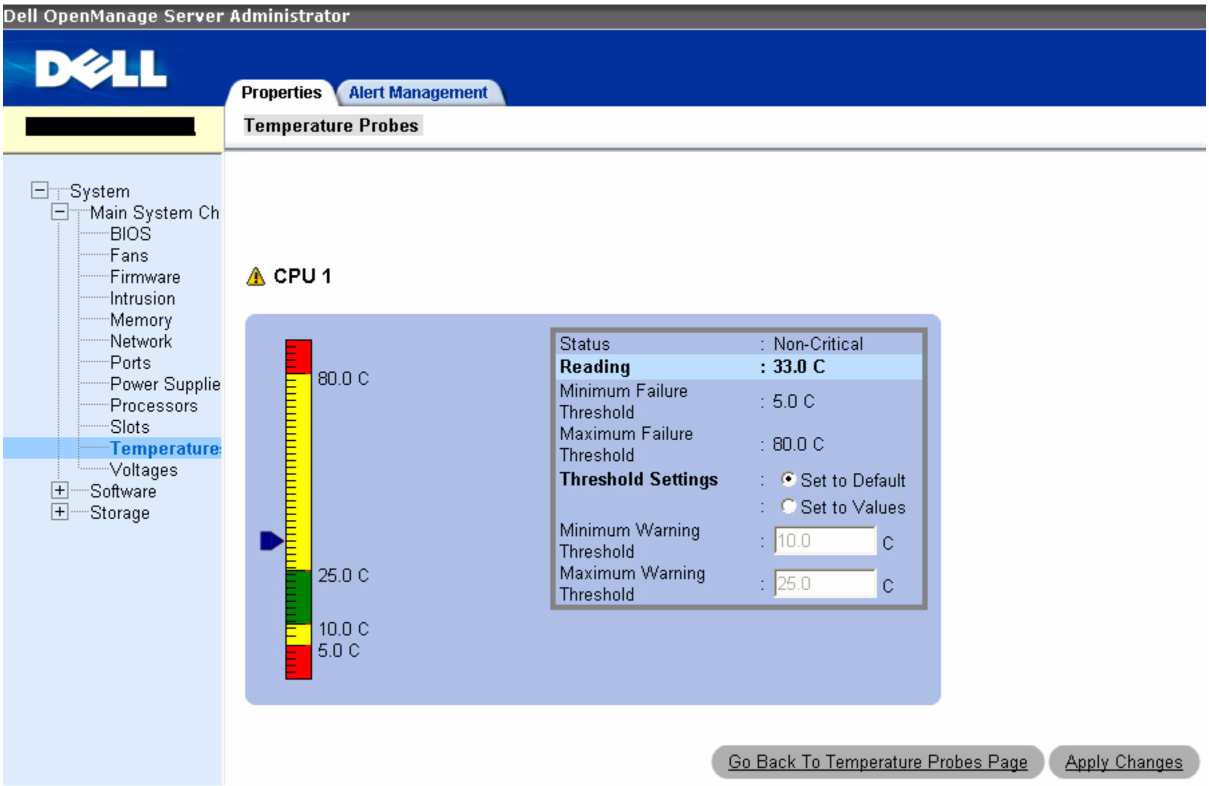
See Appendix C for more Expression examples.

- You can now test this Alert by doing the same test as in Chapter 5.1.

- Here I will generate a Hardware alert again, I have created a couple of monitors for each of the OID's I expect to receive. To prove this monitor is working I will change the Temperature setting of the CPU through **Dell OpenManage**.

- I would suggest that you clear out the old alerts from the Active Alerts view for easy identification and testing.

- Change the Threshold Settings of a CPU to be beneath the current temperature reading. This will now generate an SNMP Trap that SCOM will receive.

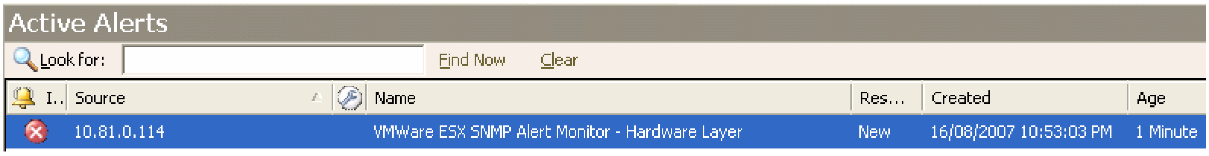


Temperature Probes

CPU 1

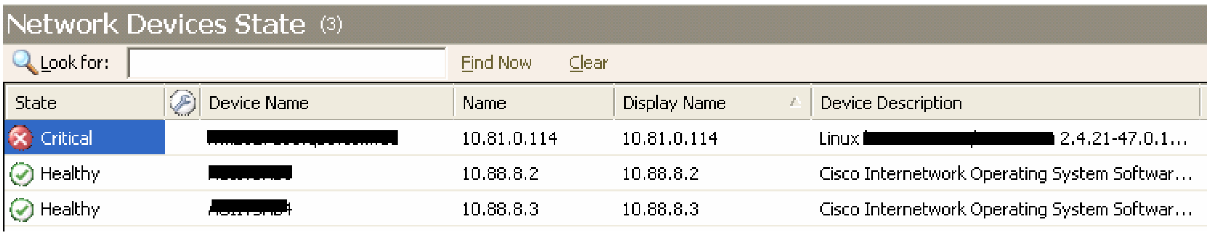
Status	: Non-Critical
Reading	**: 33.0 C**
Minimum Failure Threshold	: 5.0 C
Maximum Failure Threshold	: 80.0 C
Threshold Settings	: ● Set to Default
	: ○ Set to Values
Minimum Warning Threshold	: 10.0 C
Maximum Warning Threshold	: 25.0 C

- Open the Operations Manager Console and look in Active Alerts and you will the **VMWare ESX SNMP Alert Monitor – Hardware Layer** alert.



I..	Source		Name	Res...	Created	Age
☒	10.81.0.114		VMWare ESX SNMP Alert Monitor - Hardware Layer	New	16/08/2007 10:53:03 PM	1 Minute

- Since we now have a monitor functioning you can now select the **Network Device State** and see that the state of that device has changed from Healthy to Critical.



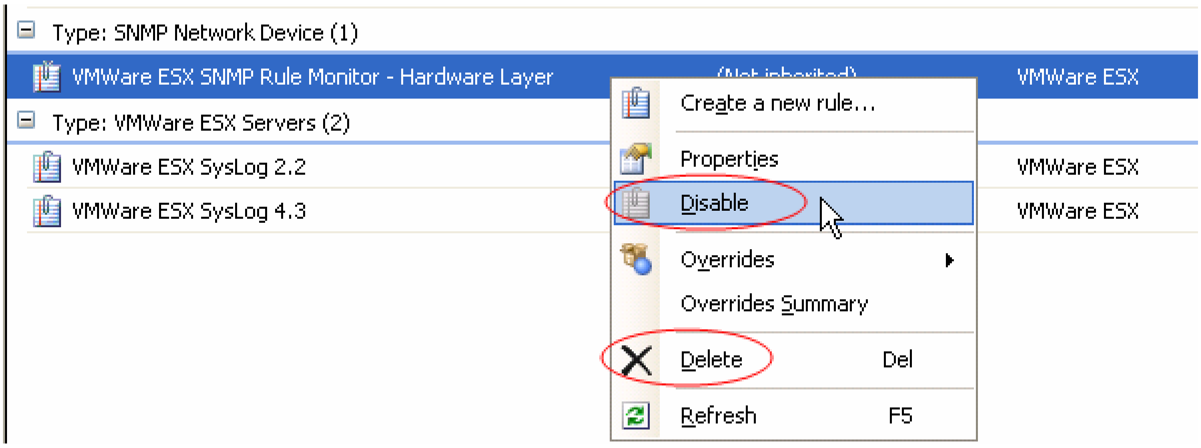
Network Devices State (3)

Look for: Find Now Clear

State		Device Name	Name	Display Name	Device Description
Critical		[redacted]	10.81.0.114	10.81.0.114	Linux [redacted] 2.4.21-47.0.1...
Healthy		[redacted]	10.88.8.2	10.88.8.2	Cisco Internetwork Operating System Softwar...
Healthy		[redacted]	10.88.8.3	10.88.8.3	Cisco Internetwork Operating System Softwar...

5.3 Disable the Trap Rule

To reduce the number of alerts when a Hardware Trap is sent we can now either delete or disable the Hardware Rule alert. Search the rule for ESX, highlight **VMWare ESX SNMP Rule Monitor – Hardware Layer** and select either **Disable** or **Delete**.



Type: SNMP Network Device (1)

VMWare ESX SNMP Rule Monitor - Hardware Layer	(Not inherited)	VMWare ESX

Type: VMWare ESX Servers (2)

VMWare ESX SysLog 2.2	VMWare ESX
VMWare ESX SysLog 4.3	VMWare ESX

6 Configure usability

Having completed the Alerting setup now we need to create some views that will make Administration easy.

6.1 Create Views

I believe most environments would benefit from 3 main Views.

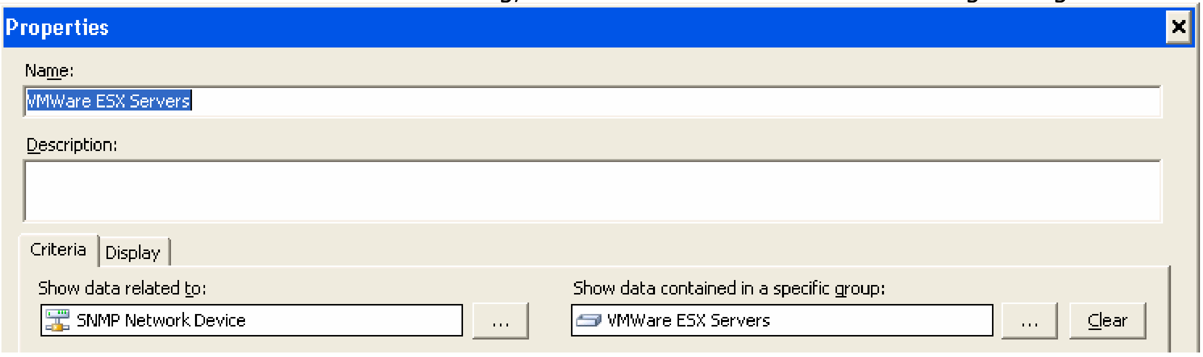
1. VMWare ESX Alerts – Used by System Administrators of your ESX Environment
2. VMWare ESX Servers – This will allow you to view the Status of all your ESX Servers.
3. VMWare ESX Environment – A diagrammatic view of your ESX servers.

Earlier we already created the VMWare ESX Alerts view.

6.1.1 VMWare ESX Servers (State View)

I find the following settings work well:

Under the VMWare ESX folder in Monitoring, Create a State View with the following settings:

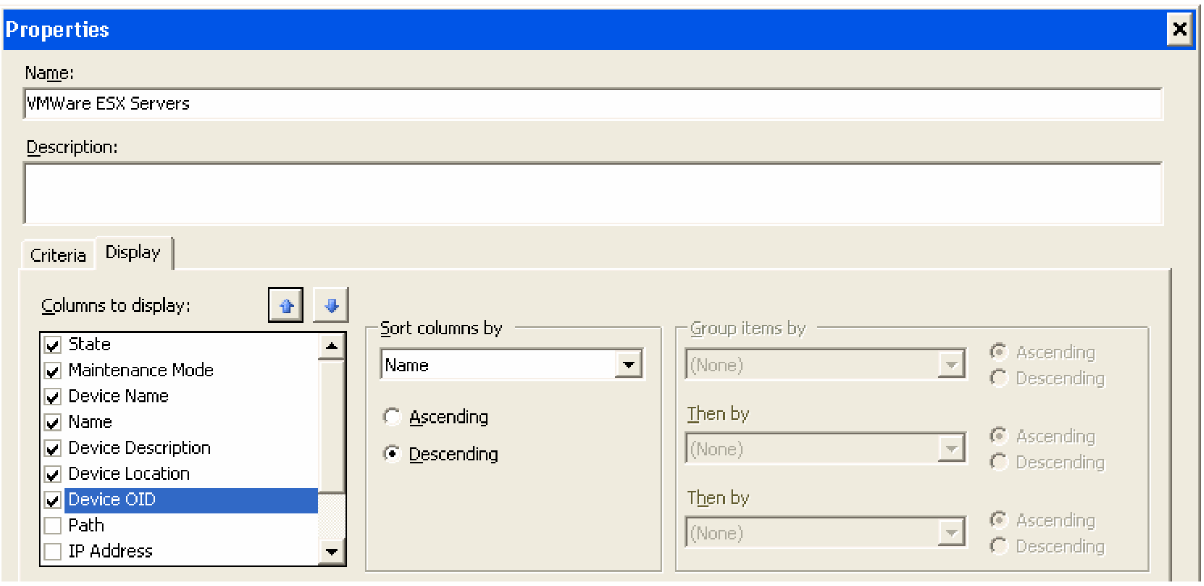


Name: VMWare ESX Servers

Description:

Show data related to: SNMP Network Device

Show data contained in a specific group: VMWare ESX Servers



Name: VMWare ESX Servers

Description:

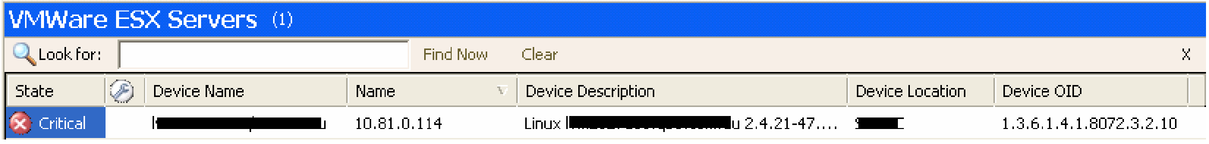
Columns to display:

☑ State
☑ Maintenance Mode
☑ Device Name
☑ Name
☑ Device Description
☑ Device Location
☑ Device OID
□ Path
□ IP Address

Sort columns by: Name
○ Ascending
● Descending

Group items by: (None) ● Ascending ○ Descending
Then by: (None) ● Ascending ○ Descending
Then by: (None) ● Ascending ○ Descending

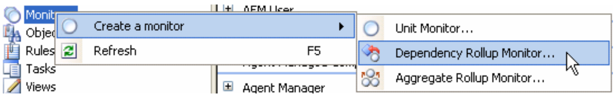
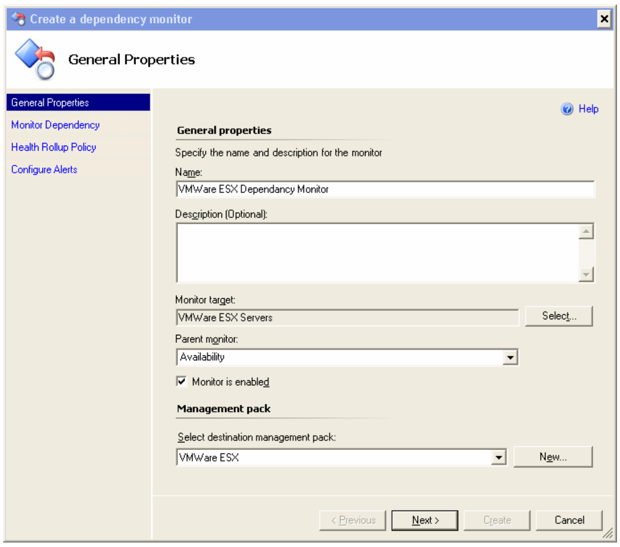
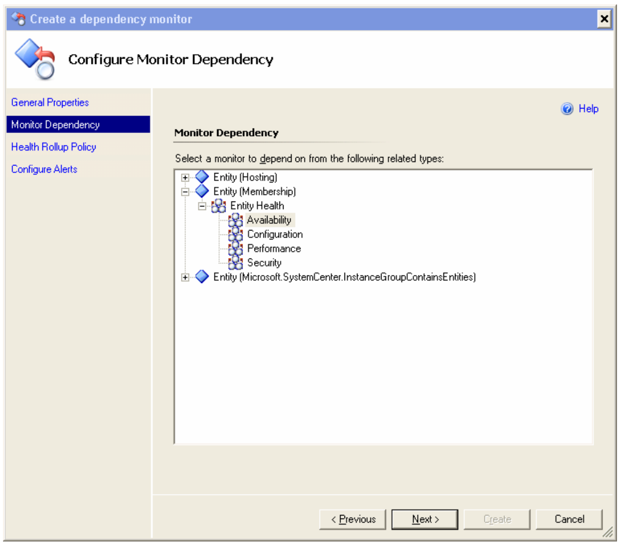
Your Display will look like this:

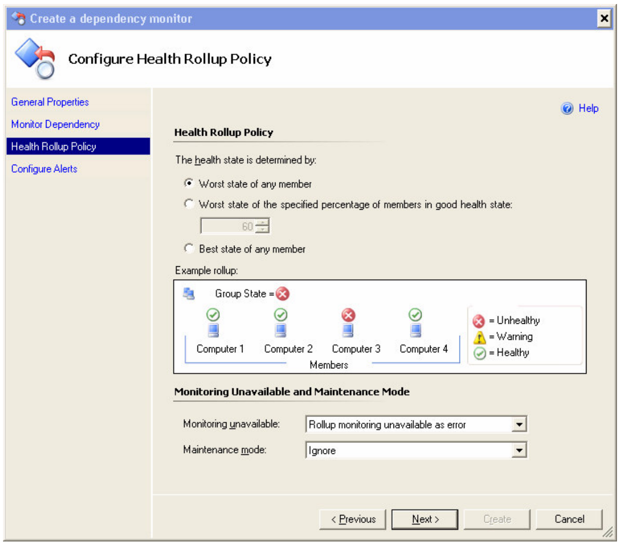
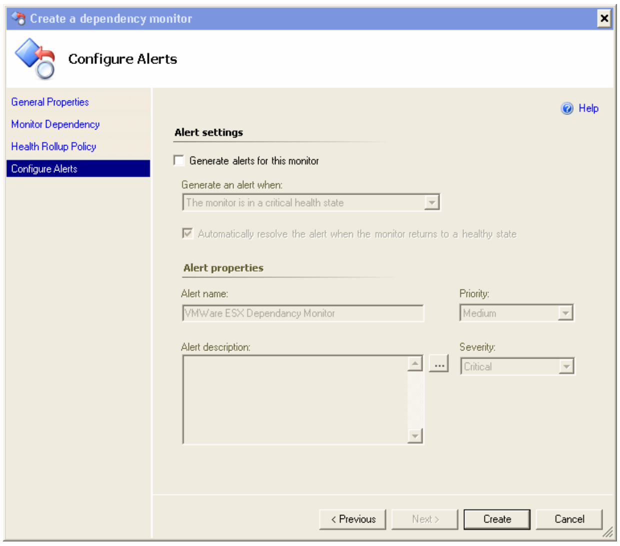


State		Device Name	Name	Device Description	Device Location	Device OID
Critical		[redacted]	10.81.0.114	Linux [redacted]u 2.4.21-47....	[redacted]	1.3.6.1.4.1.8072.3.2.10

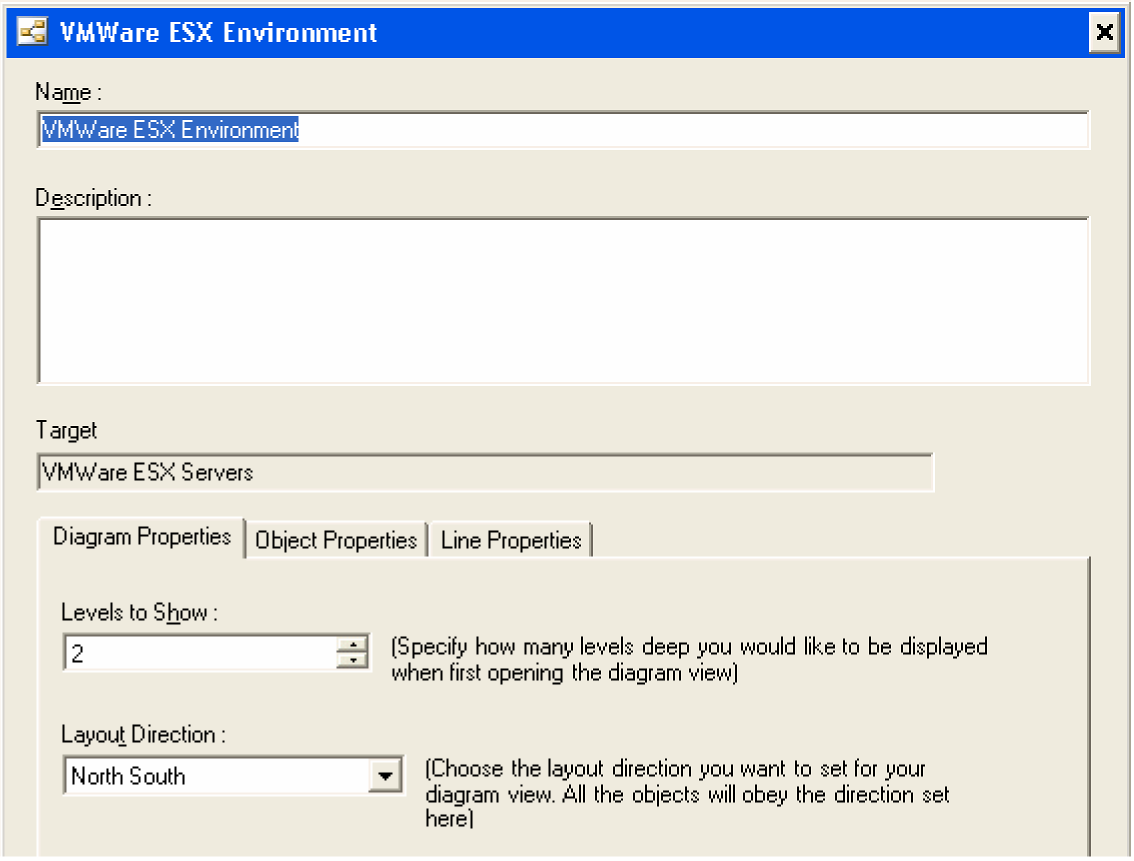
6.1.2 VMWare ESX Environment (Diagram View)

If you would like to view or break down your environment into a nice single icon or group of icons to show the health of your environment then this chapter should help with that.

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Authoring** tab	
3	Right-click **Monitors** Select **Create a monitor** Select **Dependency Rollup Monitor**	 Monit Objec Rules Tasks Views AEM User Agent Manager Create a monitor Refresh F5 Unit Monitor… Dependency Rollup Monitor… Aggregate Rollup Monitor…
4	Fill in the following fields: Name: **VMWare ESX Dependency Monitor** Under Monitor target: Select **VMWare ESX Servers** Under Parent Monitor: Select **Availability** Under Management Pack: Select **VMWare ESX** Click Next > Note: You must select SNMP Network Device for this type of monitor to work.	 Create a dependency monitor General Properties General Properties Monitor Dependency Health Rollup Policy Configure Alerts Help General properties Specify the name and description for the monitor Name: VMWare ESX Dependancy Monitor Description (Optional): Monitor target: VMWare ESX Servers Select... Parent monitor: Availability ☑ Monitor is enabled Management pack Select destination management pack: VMWare ESX New... < Previous Next > Create Cancel
5	Expand Entity (Membership) + Entity Health Select **Availability** Click Next >	 Create a dependency monitor Configure Monitor Dependency General Properties Monitor Dependency Health Rollup Policy Configure Alerts Help Monitor Dependency Select a monitor to depend on from the following related types: Entity (Hosting) Entity (Membership) Entity Health Availability Configuration Performance Security Entity (Microsoft.SystemCenter.InstanceGroupContainsEntities) < Previous Next > Create Cancel

Step	Action/Outcome	Reference
6	Select the appropriate setting for your situation. Click Next >	 Create a dependency monitor Configure Health Rollup Policy Health Rollup Policy The health state is determined by: ● Worst state of any member ○ Worst state of the specified percentage of members in good health state: 60 ○ Best state of any member Example rollup: Group State = ✗ Computer 1 ✓, Computer 2 ✓, Computer 3 ✗, Computer 4 ✓ (Members) ✗ = Unhealthy, ⚠ = Warning, ✓ = Healthy Monitoring Unavailable and Maintenance Mode Monitoring unavailable: Rollup monitoring unavailable as error Maintenance mode: Ignore
7	Click Create	 Create a dependency monitor Configure Alerts Alert settings □ Generate alerts for this monitor Generate an alert when: The monitor is in a critical health state ☑ Automatically resolve the alert when the monitor returns to a healthy state Alert properties Alert name: VMWare ESX Dependancy Monitor Priority: Medium Alert description: Severity: Critical

Under the VMWare ESX folder in Monitoring, Create a Diagram View with the following settings:



VMWare ESX Environment

Name : VMWare ESX Environment

Description :

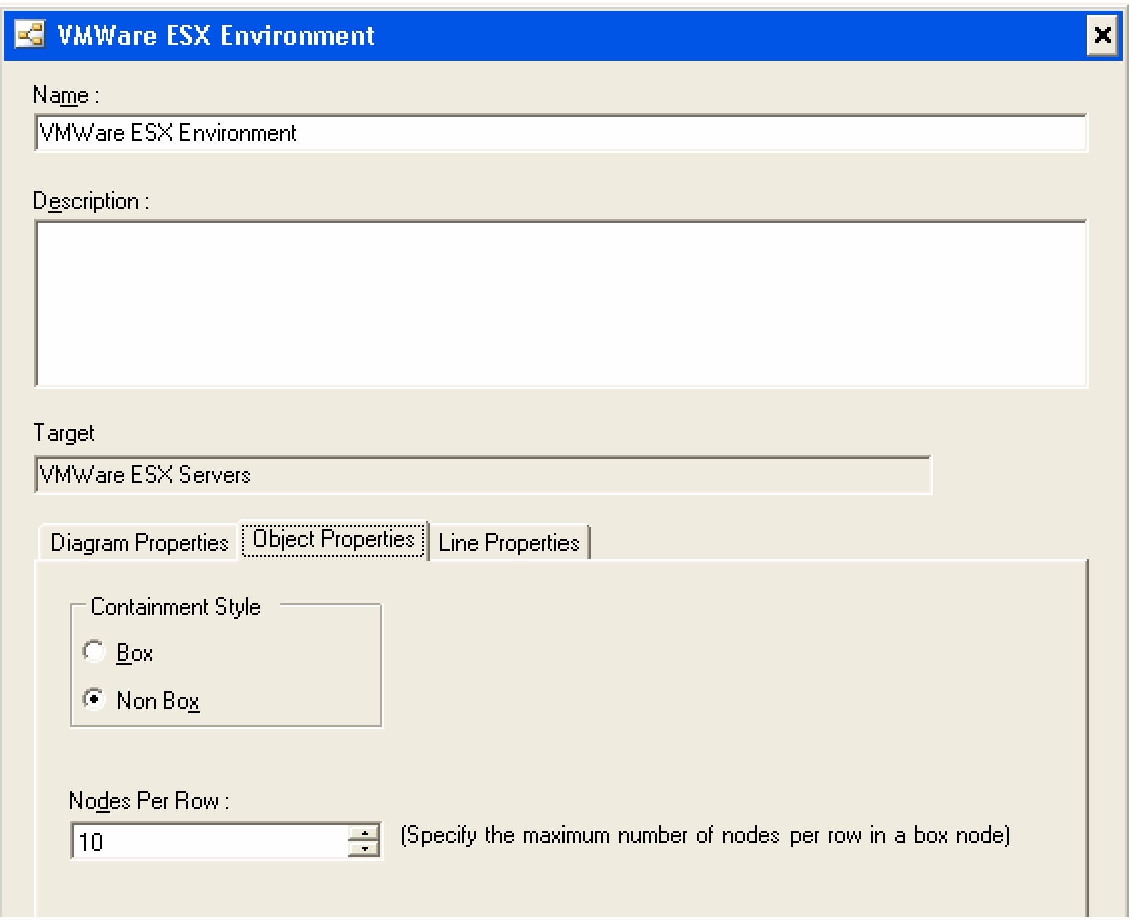
Target: VMWare ESX Servers

Levels to Show : 2

(Specify how many levels deep you would like to be displayed when first opening the diagram view)

Layout Direction : North South

(Choose the layout direction you want to set for your diagram view. All the objects will obey the direction set here)



VMWare ESX Environment

Name : VMWare ESX Environment

Description :

Target: VMWare ESX Servers

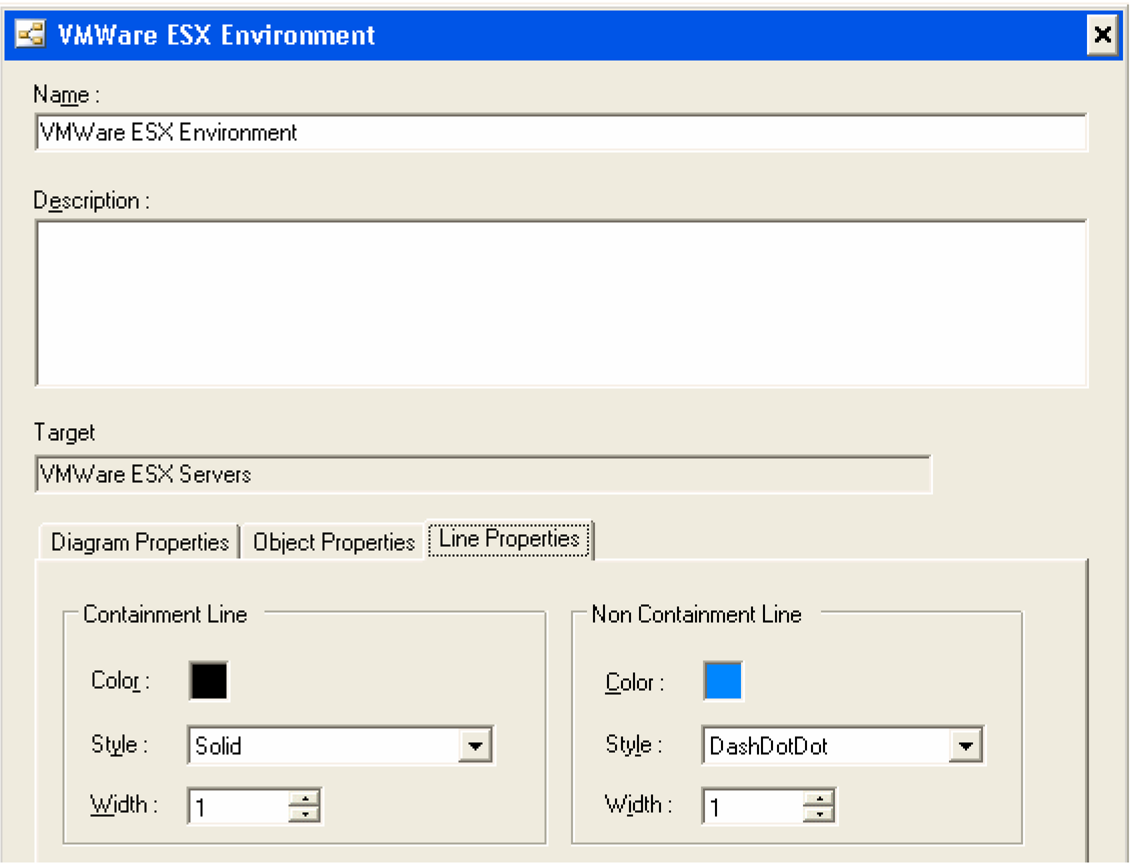
Containment Style

○ Box

● Non Box

Nodes Per Row : 10

(Specify the maximum number of nodes per row in a box node)



VMWare ESX Environment

Name : VMWare ESX Environment

Description :

Target: VMWare ESX Servers

Containment Line

Color : ■

Style : Solid

Width : 1

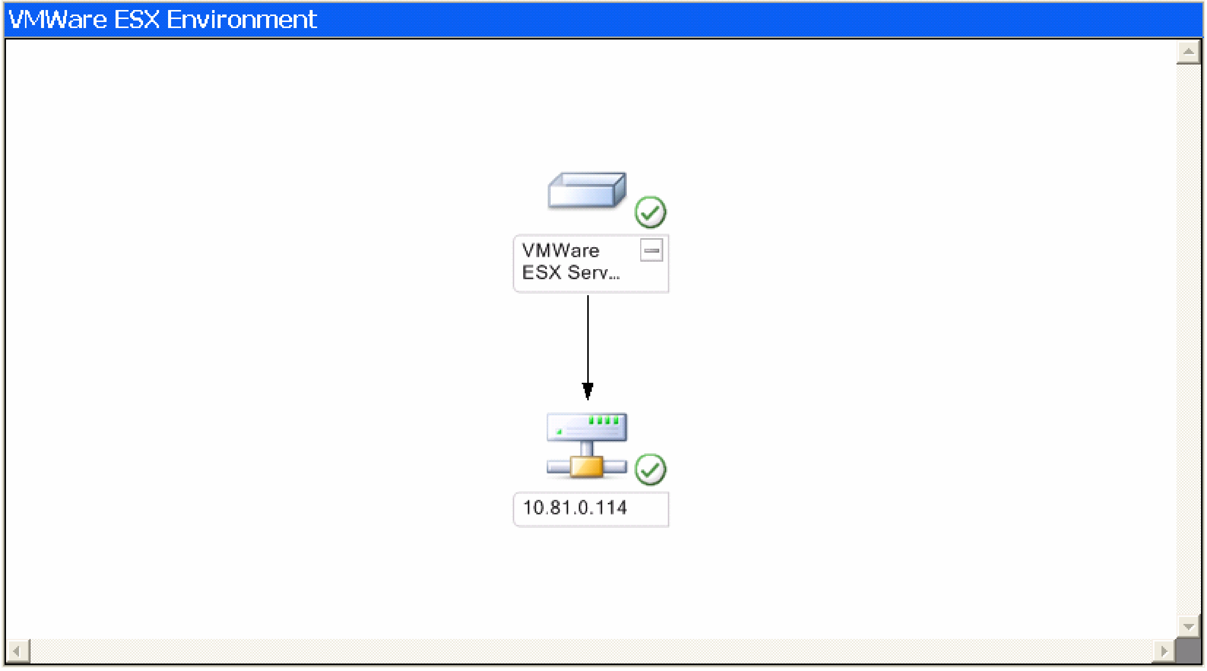
Non Containment Line

Color : 🟦

Style : DashDotDot

Width : 1

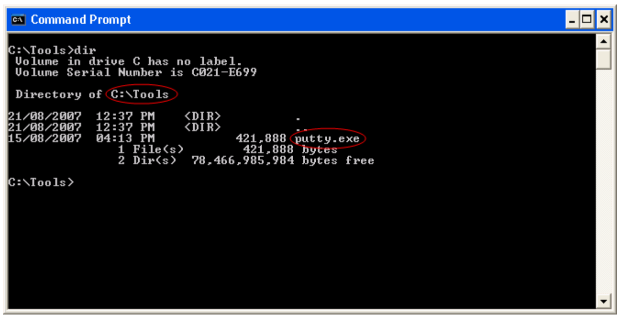
Your Display will look like this:



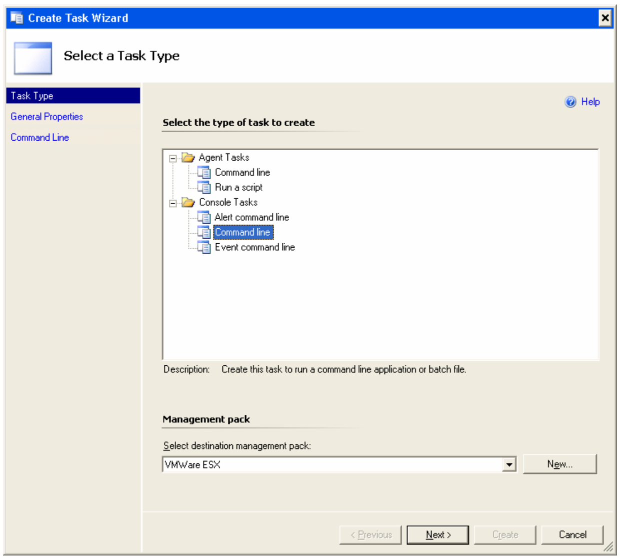
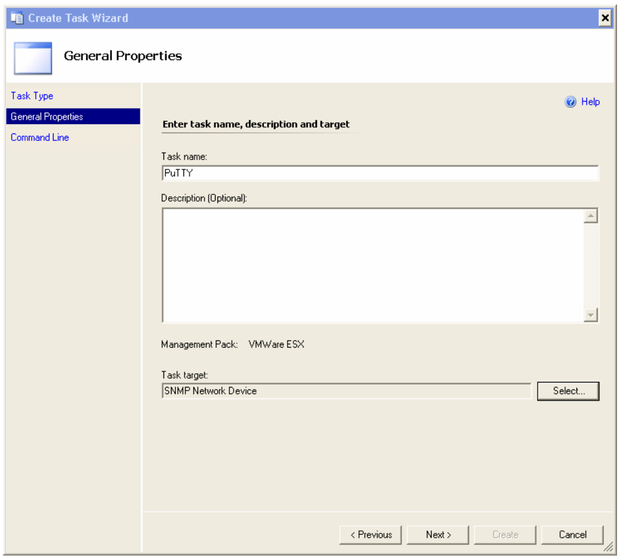
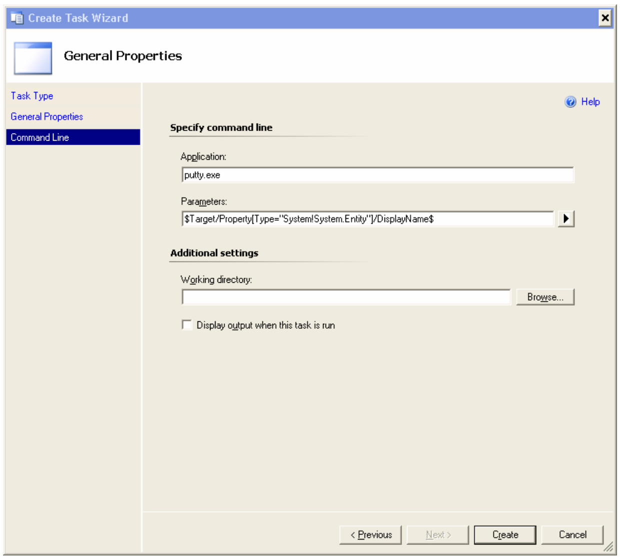
6.2 Create Tasks

6.2.1 Create task to run 'PuTTY'

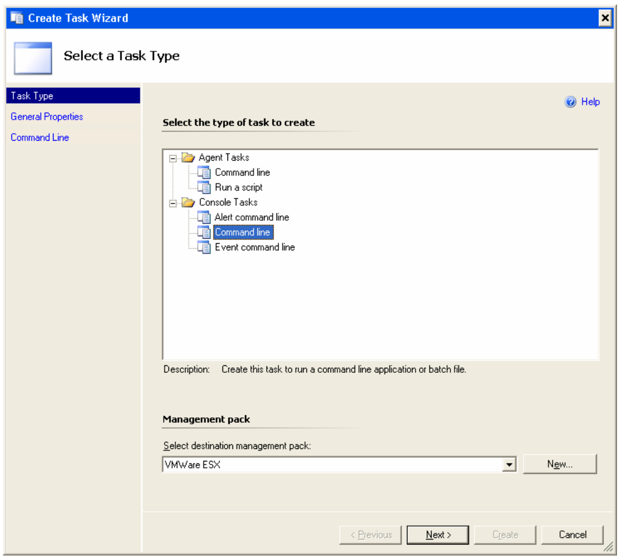
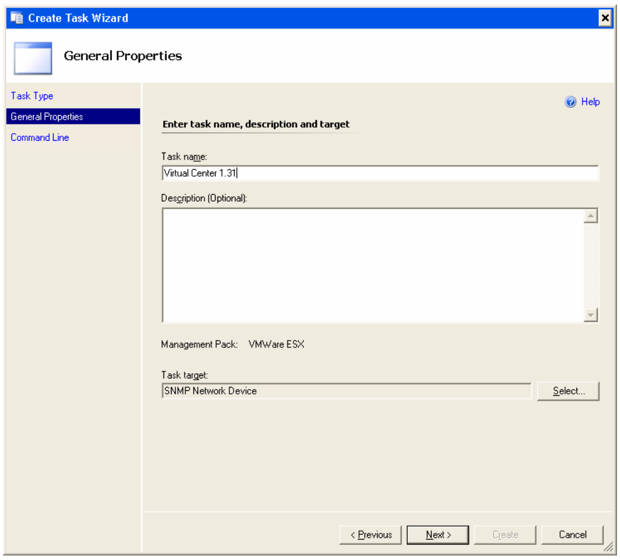
Step	Action/Outcome	Reference

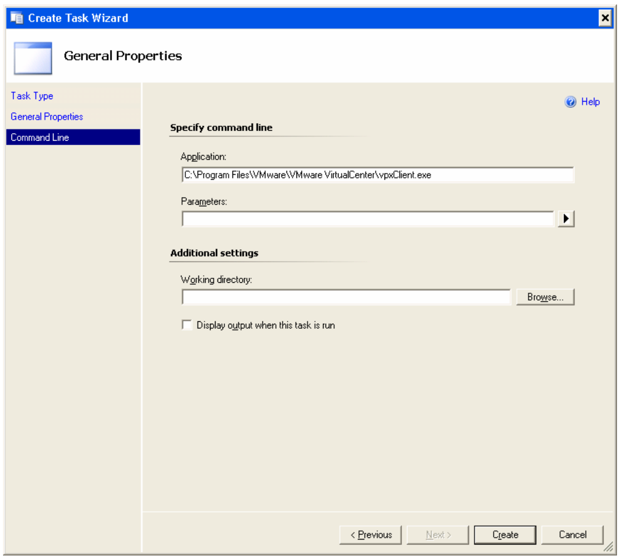
1	Download and copy a copy of the PuTTY application to a directory of your choice.
	For these instructions I have copied a copy to **C:\Tools** on the machine that runs the Operations Console
		 Command Prompt
		`C:\Tools>dir`
		` Volume in drive C has no label.`
		` Volume Serial Number is C021-E699`
		` Directory of C:\Tools`
		`21/08/2007  12:37 PM    <DIR>          .`
		`21/08/2007  12:37 PM    <DIR>          ..`
		`15/08/2007  04:13 PM           421,888 putty.exe`
		`               1 File(s)        421,888 bytes`
		`               2 Dir(s)  78,466,985,984 bytes free`
		`C:\Tools>`

2	Open the **System Center Operations Manager Console**	
3	Click on the **Authoring** tab	

Step	Action/Outcome	Reference
4	Under Console Tasks Select **Command Line** Click Next >	 Create Task Wizard Select a Task Type Task Type General Properties Command Line Help **Select the type of task to create** Agent Tasks Command line Run a script Console Tasks Alert command line Command line Event command line Description: Create this task to run a command line application or batch file. **Management pack** Select destination management pack: VMWare ESX New... < Previous Next > Create Cancel
5	Fill in the following fields: Task name: **PuTTY** Under Monitor target: Select **SNMP Network Device** Click Next >	 Create Task Wizard General Properties Task Type General Properties Command Line Help **Enter task name, description and target** Task name: PuTTY Description (Optional): Management Pack: VMWare ESX Task target: SNMP Network Device Select... < Previous Next > Create Cancel
6	Fill in the following fields: Application: **putty.exe** Parameters: **$Target/Property[Type="System!System.Entity"]/DisplayName$** Tick ☑ **Display output when task is run** Click Create Note: If you just put the name of the .exe file in the Application field the .exe file must reside in directory specified in the the OS's 'PATH' statement. You can also put the full path in this field.	 Create Task Wizard General Properties Task Type General Properties Command Line Help **Specify command line** Application: putty.exe Parameters: $Target/Property[Type="System!System.Entity"]/DisplayName$ **Additional settings** Working directory: Browse... □ Display output when this task is run < Previous Next > Create Cancel

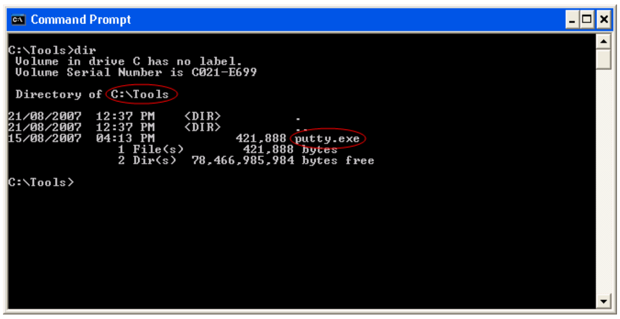
6.2.2 Create task to run 'Virtual Center 1.31'

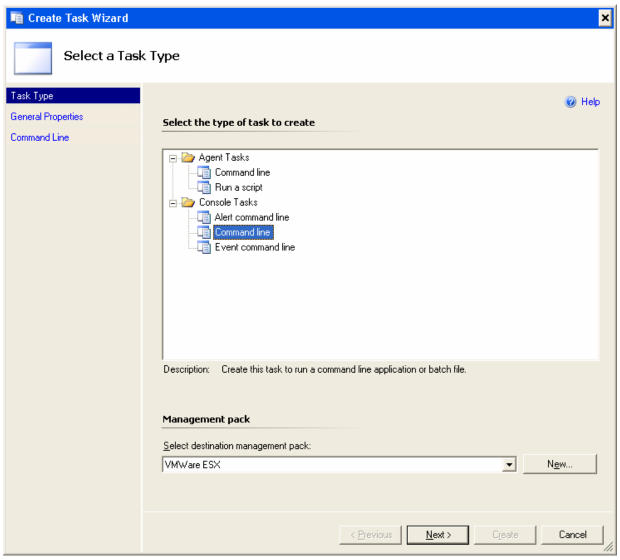
Step	Action/Outcome	Reference
1	Install Virtual Center on the machines that will be used to monitor your Virtual Center environment.	
2	Open the **System Center Operations Manager Console**	 Operations Console
3	Click on the **Authoring** tab	 Authoring
4	Under Console Tasks Select **Command Line** Click Next >	 Create Task Wizard Select a Task Type Select the type of task to create Agent Tasks Command line Run a script Console Tasks Alert command line Command line Event command line Description: Create this task to run a command line application or batch file. Management pack Select destination management pack: VMWare ESX Task Type General Properties Command Line Help New... < Previous Next > Create Cancel
5	Fill in the following fields: Task name: **Virtual Center 1.31** Under Monitor target: Select **SNMP Network Device** Click Next >	 Create Task Wizard General Properties Enter task name, description and target Task name: Virtual Center 1.31 Description (Optional): Management Pack: VMWare ESX Task target: SNMP Network Device Task Type General Properties Command Line Help Select... < Previous Next > Create Cancel

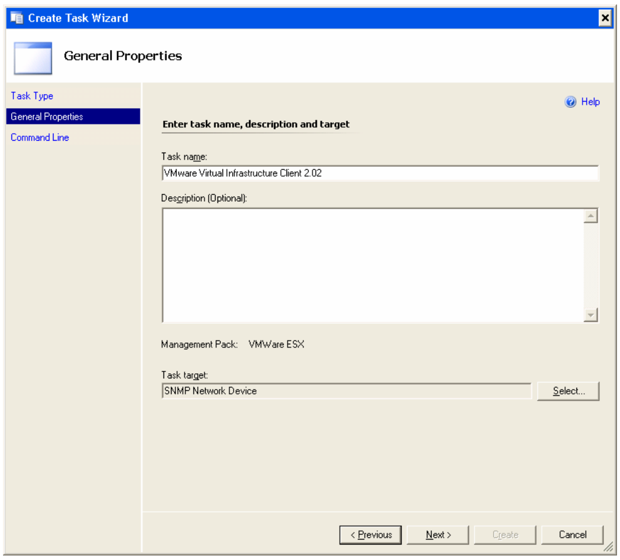
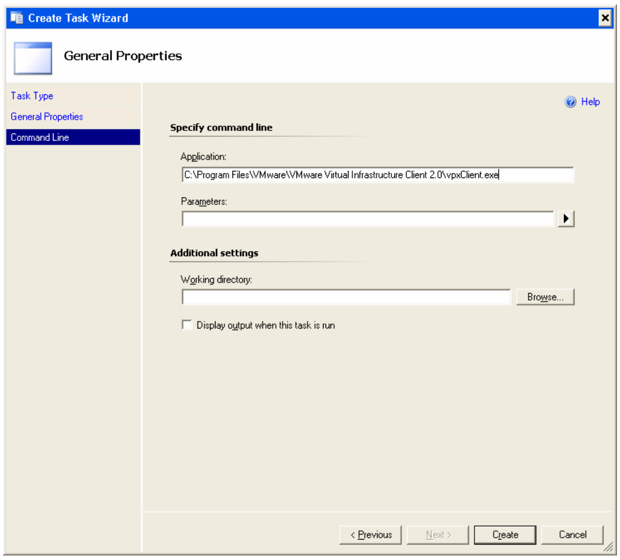
Step	Action/Outcome	Reference
6	Fill in the following fields: Application: **C:\Program Files\VMware\VMware VirtualCenter\vpxClient.exe** Click Create	 Create Task Wizard General Properties Task Type General Properties Command Line Help **Specify command line** Application: C:\Program Files\VMware\VMware VirtualCenter\vpxClient.exe Parameters: **Additional settings** Working directory: Browse... ☐ Display output when this task is run < Previous Next > Create Cancel

6.2.3 Create task to run 'Virtual Center 2.02'

Step	Action/Outcome	Reference

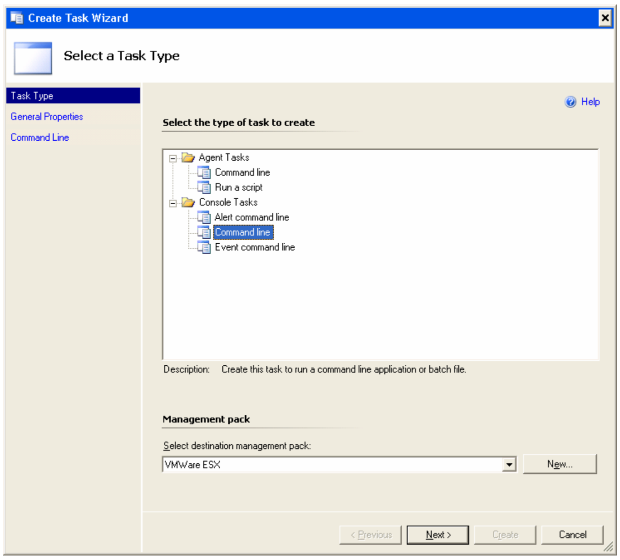
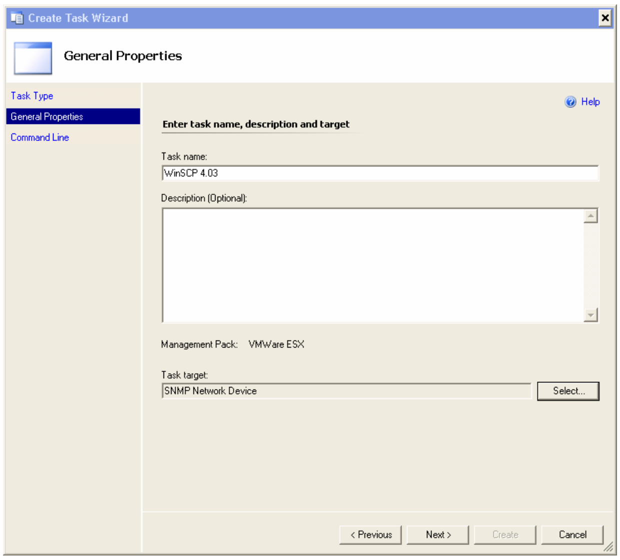
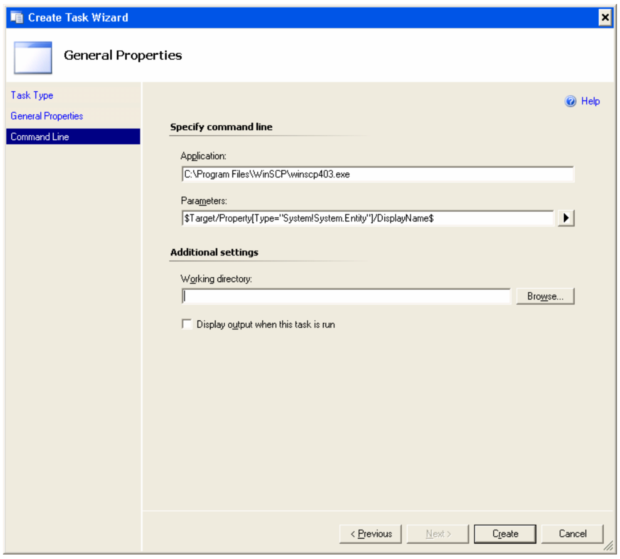
1	Download and copy a copy of the PuTTY application to a directory of your choice.
	For these instructions I have copied a copy to **C:\Tools** on the machine that runs the Operations Console
		
		Command Prompt
		`C:\Tools>dir`
		` Volume in drive C has no label.`
		` Volume Serial Number is C021-E699`
		` Directory of C:\Tools`
		`21/08/2007  12:37 PM    <DIR>          .`
		`21/08/2007  12:37 PM    <DIR>          ..`
		`15/08/2007  04:13 PM           421,888 putty.exe`
		`               1 File(s)        421,888 bytes`
		`               2 Dir(s)  78,466,985,984 bytes free`
		`C:\Tools>`

2	Open the **System Center Operations Manager Console**	 Operations Console
3	Click on the **Authoring** tab	 Authoring
4	Under Console Tasks Select **Command Line** Click Next >	 Create Task Wizard Select a Task Type Task Type General Properties Command Line Help **Select the type of task to create** Agent Tasks Command line Run a script Console Tasks Alert command line Command line Event command line Description: Create this task to run a command line application or batch file. **Management pack** Select destination management pack: VMWare ESX New... < Previous Next > Create Cancel

Step	Action/Outcome	Reference
5	Fill in the following fields: Task name: **VMware Virtual Infrastructure Client 2.02** Under Monitor target: Select **SNMP Network Device** Click Next >	 Create Task Wizard General Properties Task Type General Properties Command Line Help **Enter task name, description and target** Task name: VMware Virtual Infrastructure Client 2.02 Description (Optional): Management Pack: VMWare ESX Task target: SNMP Network Device Select... < Previous Next > Create Cancel
6	Fill in the following fields: Application: **C:\Program Files\VMware\VMware Virtual Infrastructure Client 2.0\vpxClient.exe** Click Create	 Create Task Wizard General Properties Task Type General Properties Command Line Help **Specify command line** Application: C:\Program Files\VMware\VMware Virtual Infrastructure Client 2.0\vpxClient.exe Parameters: **Additional settings** Working directory: Browse... □ Display output when this task is run < Previous Next > Create Cancel

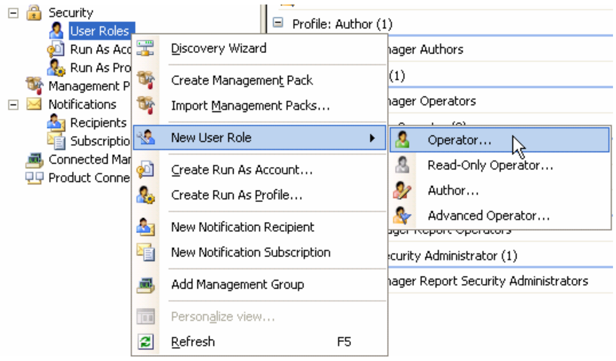
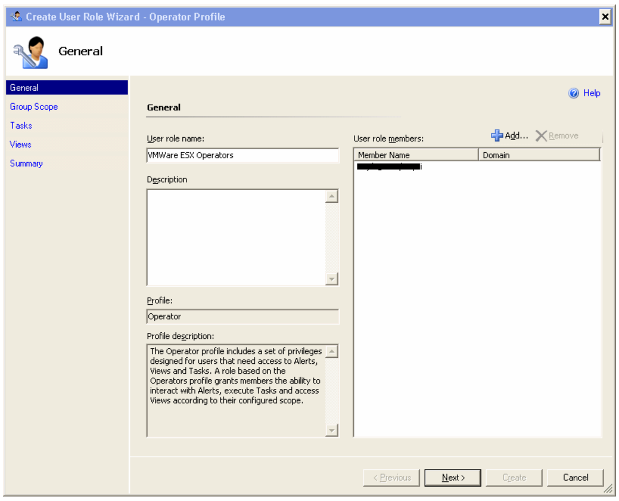
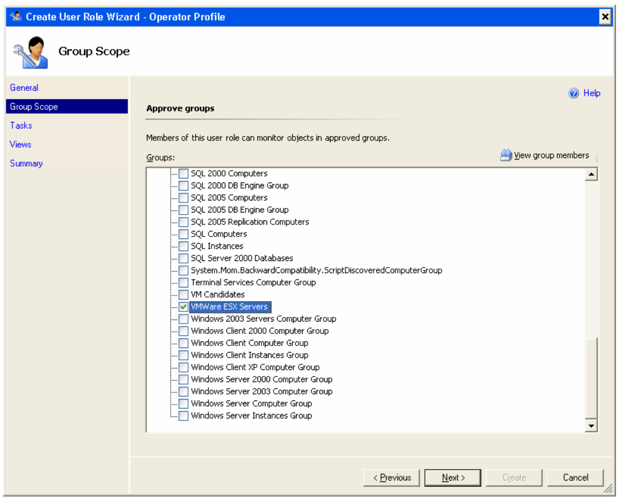
6.2.4 Create task to run 'WinSCP 4.03'

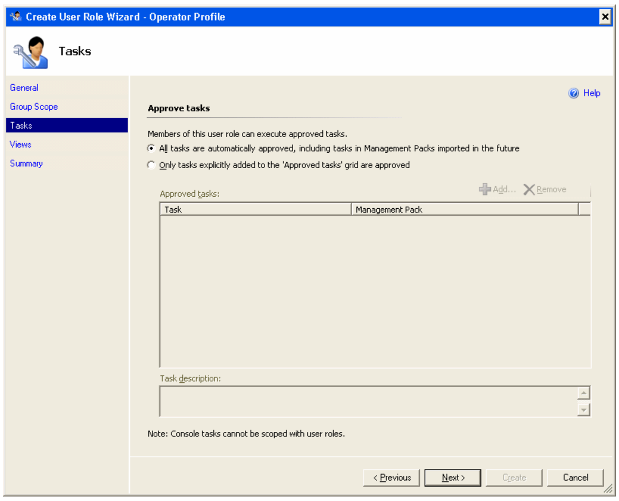
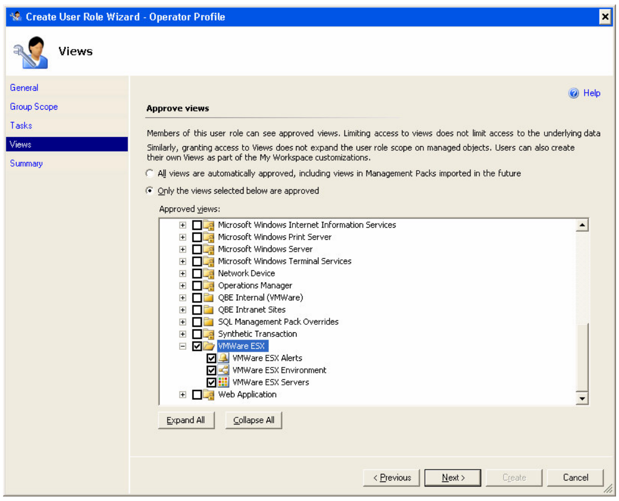
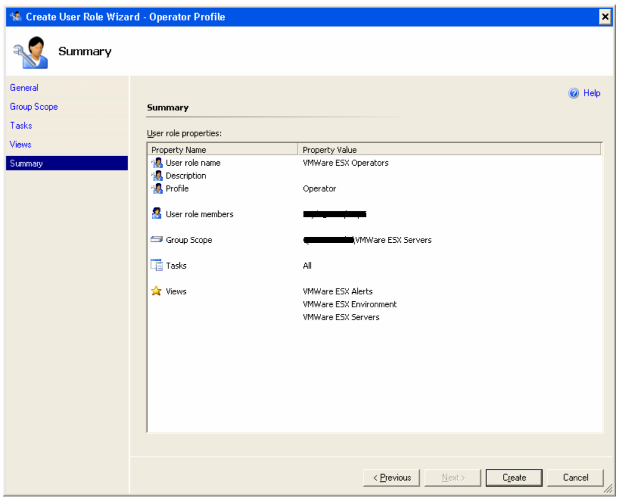
Step	Action/Outcome	Reference
1	Download and copy WinSCP to a directory of your choice. For these instructions I have copied a copy to **C:\Program Files\WinSCP** on the machine that runs the Operations Console	
2	Open the **System Center Operations Manager Console**	 Operations Console
3	Click on the **Authoring** tab	 Authoring

Step	Action/Outcome	Reference
4	Under Console Tasks Select **Command Line** Click Next >	 Create Task Wizard Select a Task Type Select the type of task to create Agent Tasks Command line Run a script Console Tasks Alert command line Command line Event command line Description: Create this task to run a command line application or batch file. Management pack Select destination management pack: VMWare ESX Task Type General Properties Command Line Help New... < Previous Next > Create Cancel
5	Fill in the following fields: Task name: **WinSCP 4.03** Under Monitor target: Select **SNMP Network Device** Click Next >	 Create Task Wizard General Properties Enter task name, description and target Task name: WinSCP 4.03 Description (Optional): Management Pack: VMWare ESX Task target: SNMP Network Device Task Type General Properties Command Line Help Select... < Previous Next > Create Cancel
6	Fill in the following fields: Application: **C:\Program Files\WinSCP\winscp403.exe** Parameters: **$Target/Property[Type="System!System.Entity"]/DisplayName$** Click Create	 Create Task Wizard General Properties Specify command line Application: C:\Program Files\WinSCP\winscp403.exe Parameters: $Target/Property[Type="System!System.Entity"]/DisplayName$ Additional settings Working directory: ☐ Display output when this task is run Task Type General Properties Command Line Help Browse... < Previous Next > Create Cancel

6.3 Create Alerting

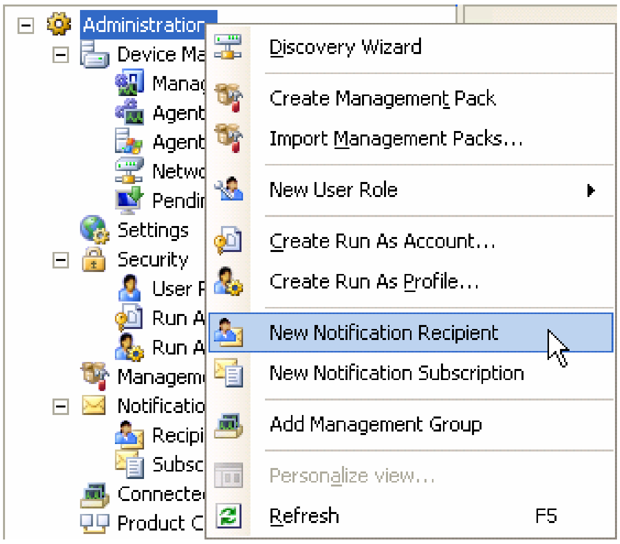
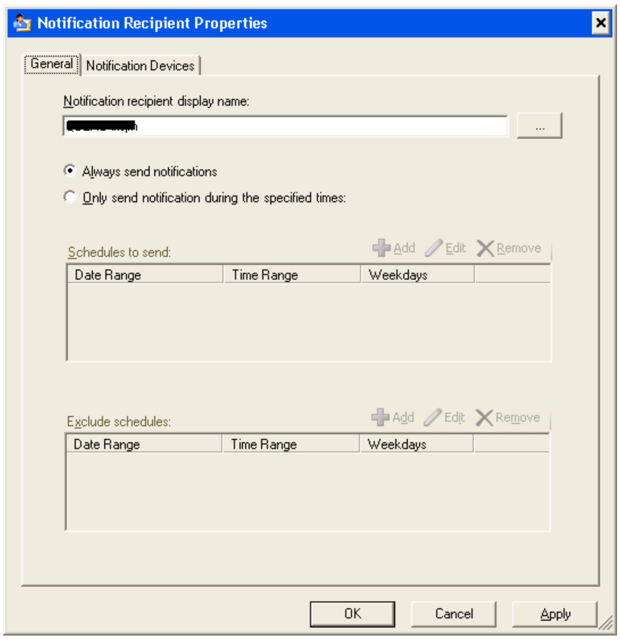
6.3.1 Create User Role – "VMWare ESX Operators"

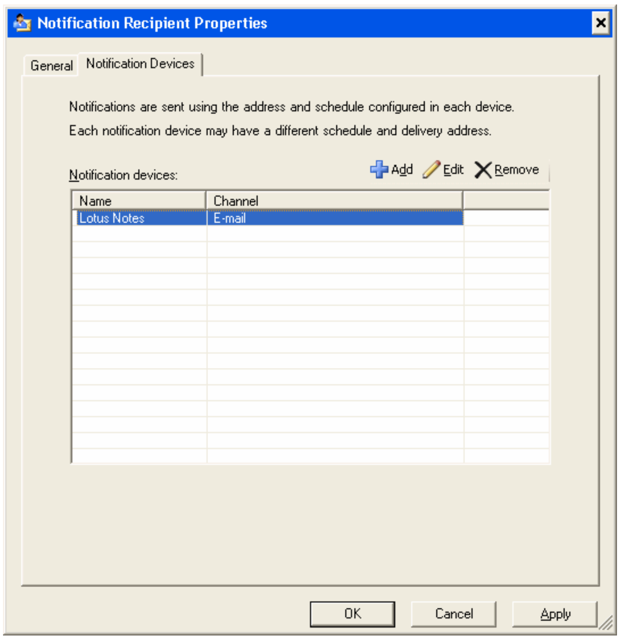
Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Administration** tab	
3	Right-click **Administration** Select **New User Role** Select **Operator…**	 Security User Roles Run As Acc Run As Pro Management P Notifications Recipients Subscriptio Connected Mar Product Conne Profile: Author (1) ager Authors (1) ager Operators curity Administrator (1) ager Report Security Administrators Discovery Wizard Create Management Pack Import Management Packs… New User Role Create Run As Account… Create Run As Profile… New Notification Recipient New Notification Subscription Add Management Group Personalize view… Refresh F5 Operator… Read-Only Operator… Author… Advanced Operator…
4	Fill in the following fields: User role name: **VMWare ESX Operators** Click Add… and select all users required from your Active Directory Click Next >	 Create User Role Wizard - Operator Profile General User role name: VMWare ESX Operators Description Profile: Operator Profile description: The Operator profile includes a set of privileges designed for users that need access to Alerts, Views and Tasks. A role based on the Operators profile grants members the ability to interact with Alerts, execute Tasks and access Views according to their configured scope. User role members: Member Name | Domain [redacted] General Group Scope Tasks Views Summary Help Add… Remove < Previous Next > Create Cancel
5	De-Select the first tick box (Management Group) Select only: **VMWare ESX Servers** Click Next >	 Create User Role Wizard - Operator Profile Group Scope Approve groups Members of this user role can monitor objects in approved groups. Groups: □ SQL 2000 Computers □ SQL 2000 DB Engine Group □ SQL 2005 Computers □ SQL 2005 DB Engine Group □ SQL 2005 Replication Computers □ SQL Computers □ SQL Instances □ SQL Server 2000 Databases □ System.Mom.BackwardCompatibility.ScriptDiscoveredComputerGroup □ Terminal Services Computer Group □ VM Candidates ☑ VMWare ESX Servers □ Windows 2003 Servers Computer Group □ Windows Client 2000 Computer Group □ Windows Client Computer Group □ Windows Client Instances Group □ Windows Client XP Computer Group □ Windows Server 2000 Computer Group □ Windows Server 2003 Computer Group □ Windows Server Computer Group □ Windows Server Instances Group General Group Scope Tasks Views Summary Help View group members < Previous Next > Create Cancel

Step	Action/Outcome	Reference
6	You have the option to allow any users to only have access to PuTTY or any other application individually. If you leave the default they will have access to all Task that are in the Management Pack. If you completed the previous chapter this will include PuTTY. Click Next >	 Create User Role Wizard - Operator Profile Tasks General / Group Scope / Tasks / Views / Summary Approve tasks Members of this user role can execute approved tasks. ● All tasks are automatically approved, including tasks in Management Packs imported in the future ○ Only tasks explicitly added to the 'Approved tasks' grid are approved Approved tasks: Add... Remove Task | Management Pack Task description: Note: Console tasks cannot be scoped with user roles. < Previous Next > Create Cancel
7	De-Select all Tick ☑ **VMWare ESX** Click Next >	 Create User Role Wizard - Operator Profile Views General / Group Scope / Tasks / Views / Summary Approve views Members of this user role can see approved views. Limiting access to views does not limit access to the underlying data Similarly, granting access to Views does not expand the user role scope on managed objects. Users can also create their own Views as part of the My Workspace customizations. ○ All views are automatically approved, including views in Management Packs imported in the future ● Only the views selected below are approved Approved views: □ Microsoft Windows Internet Information Services □ Microsoft Windows Print Server □ Microsoft Windows Server □ Microsoft Windows Terminal Services □ Network Device □ Operations Manager □ QBE Internal (VMWare) □ QBE Intranet Sites □ SQL Management Pack Overrides □ Synthetic Transaction ☑ VMWare ESX ☑ VMWare ESX Alerts ☑ VMWare ESX Environment ☑ VMWare ESX Servers □ Web Application Expand All Collapse All < Previous Next > Create Cancel
8	Click Create	 Create User Role Wizard - Operator Profile Summary General / Group Scope / Tasks / Views / Summary Summary User role properties: Property Name: Property Value User role name: VMWare ESX Operators Description: Profile: Operator User role members: [redacted] Group Scope: [redacted]VMWare ESX Servers Tasks: All Views: VMWare ESX Alerts, VMWare ESX Environment, VMWare ESX Servers < Previous Next > Create Cancel

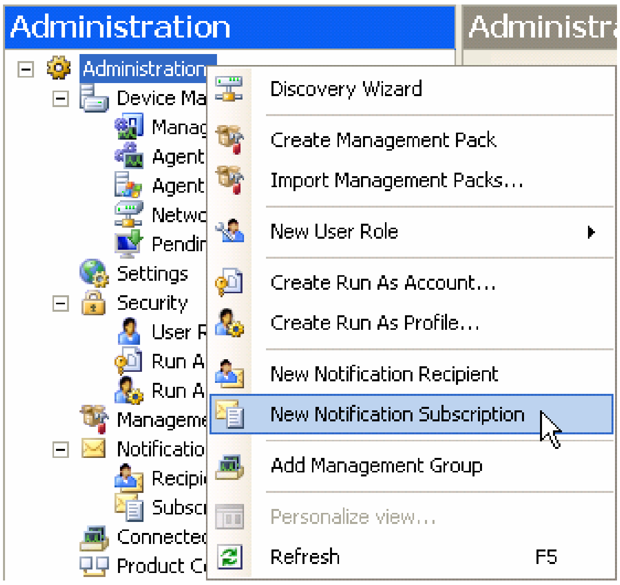
6.3.2 Create a Recipient

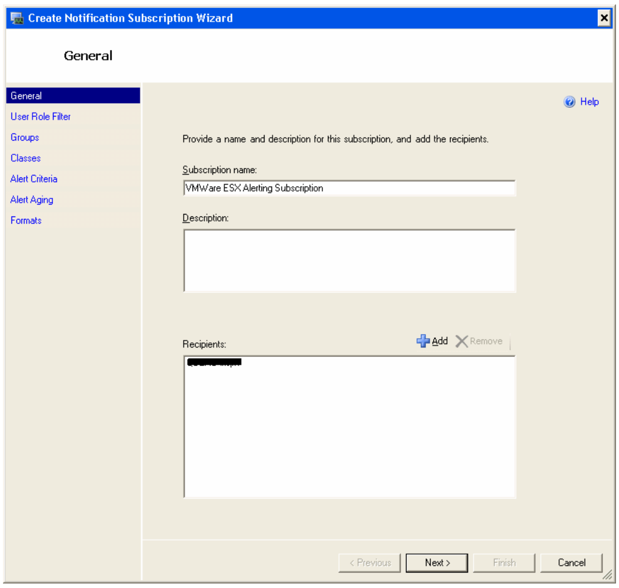
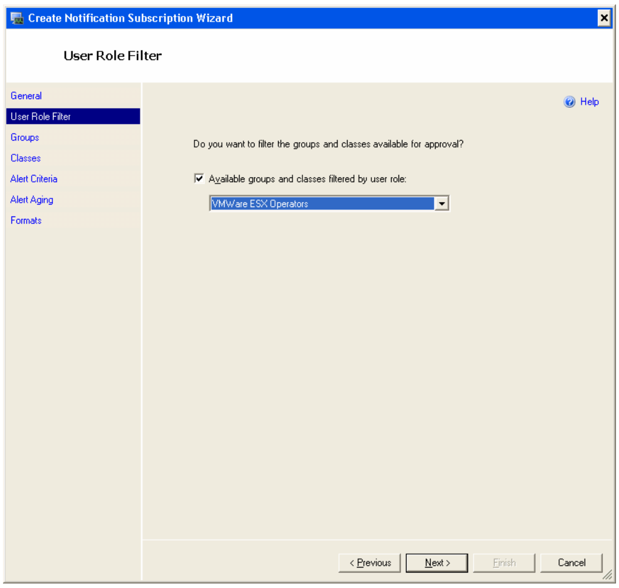
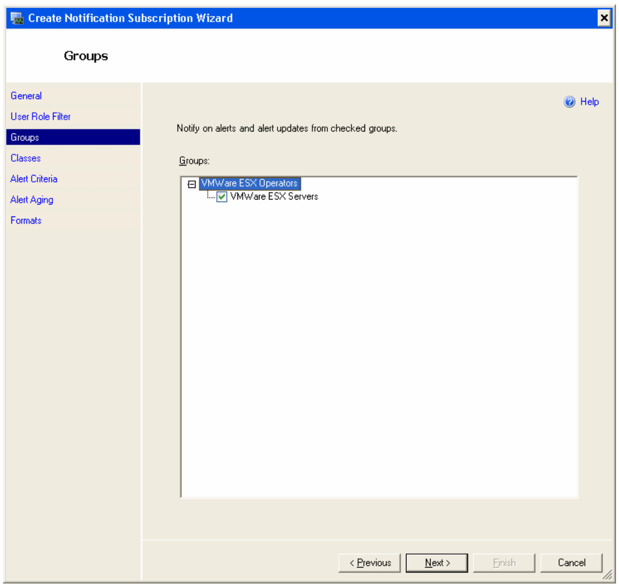
If you haven't already got a Recipient setup, the you will need to create one.

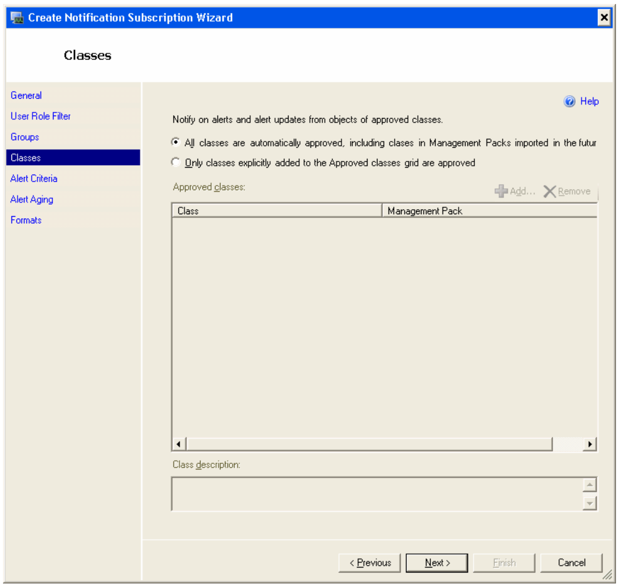
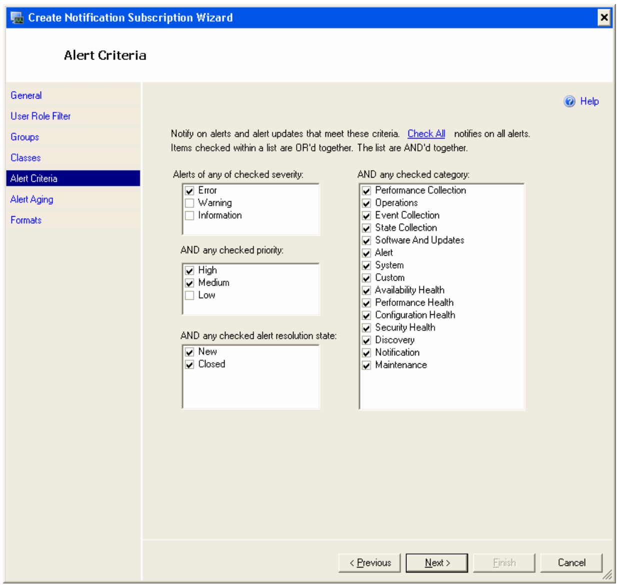
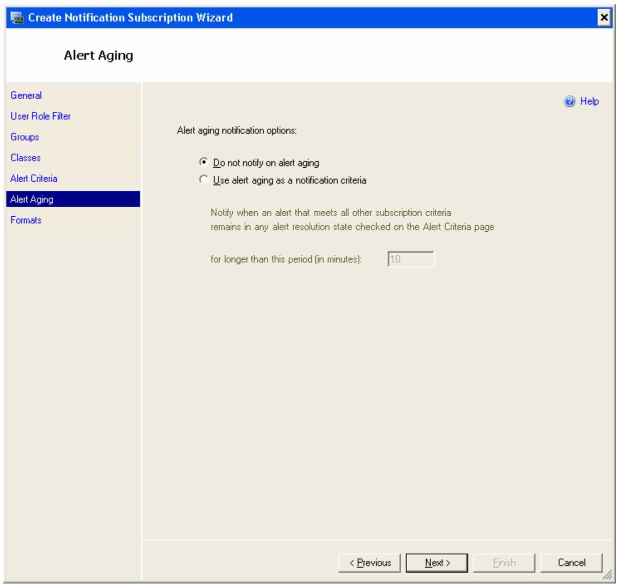
Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Administration** tab	
3	Right-click **Administration** Select **New Notification Recipient**	 Administration Device Ma Manag Agent Agent Netwo Pendir Settings Security User R Run A Run A Managem Notificatio Recipi Subsc Connecte Product C Discovery Wizard Create Management Pack Import Management Packs... New User Role Create Run As Account... Create Run As Profile... New Notification Recipient New Notification Subscription Add Management Group Personalize view... Refresh F5
4	In the **General** Tab Select the username of the recipient And the notification times	Notification Recipient Properties General | Notification Devices Notification recipient display name: [redacted] ... ● Always send notifications ○ Only send notification during the specified times: Schedules to send: Add Edit Remove Date Range | Time Range | Weekdays Exclude schedules: Add Edit Remove Date Range | Time Range | Weekdays OK Cancel Apply

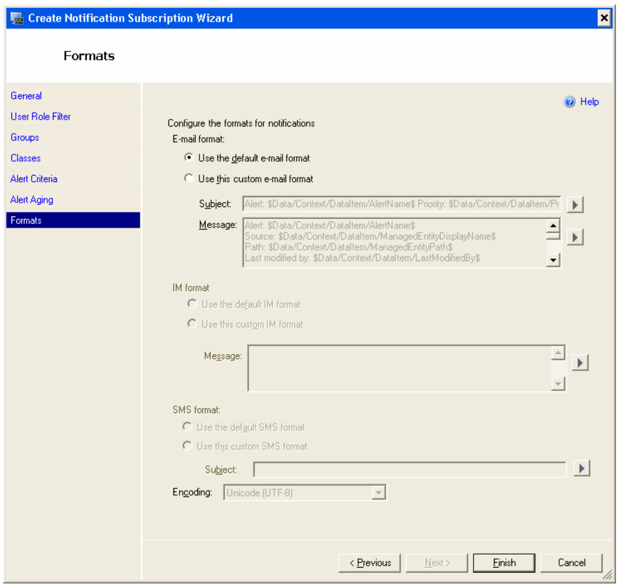
Step	Action/Outcome	Reference
5	In the **Notification Devices** Tab Click Add... and fill in the appropriate settings. Click OK	 Notification Recipient Properties General | Notification Devices Notifications are sent using the address and schedule configured in each device. Each notification device may have a different schedule and delivery address. Notification devices: Add Edit Remove Name: Lotus Notes — Channel: E-mail OK Cancel Apply

6.3.3 Create a Subscription

Step	Action/Outcome	Reference
1	Open the **System Center Operations Manager Console**	
2	Click on the **Administration** tab	
3	Right-click **Administration** Select **New Notification Subscription**	 Administration Administra Administration Device Ma Manag Agent Agent Netwo Pendir Settings Security User R Run A Run A Manageme Notificatio Recipi Subscr Connected Product C Discovery Wizard Create Management Pack Import Management Packs... New User Role Create Run As Account... Create Run As Profile... New Notification Recipient New Notification Subscription Add Management Group Personalize view... Refresh F5

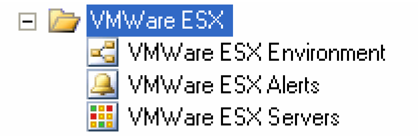
Step	Action/Outcome	Reference
4	Fill in the following fields: Subscription name: **VMWare ESX Alerting Subscription** Click Add… and select the appropriate user/s. Click Next >	 Create Notification Subscription Wizard General Provide a name and description for this subscription, and add the recipients. Subscription name: VMWare ESX Alerting Subscription Description: Recipients: [redacted]
5	If you are working in a locked down environment then I would suggest you Tick ☑ **VMWare ESX Operators** Click Next >	 Create Notification Subscription Wizard User Role Filter Do you want to filter the groups and classes available for approval? ☑ Available groups and classes filtered by user role: VMWare ESX Operators
6	Tick ☑ **VMWare ESX Servers** Click Next >	 Create Notification Subscription Wizard Groups Notify on alerts and alert updates from checked groups. Groups: VMWare ESX Operators ☑ VMWare ESX Servers

Step	Action/Outcome	Reference
7	Depending on your environment you may like to select additional classes. Click Next >	 Create Notification Subscription Wizard Classes General User Role Filter Groups Classes Alert Criteria Alert Aging Formats Help Add... Remove Class Management Pack < Previous Next > Finish Cancel Notify on alerts and alert updates from objects of approved classes. ● All classes are automatically approved, including classes in Management Packs imported in the futur ○ Only classes explicitly added to the Approved classes grid are approved Approved classes: Class description:
8	This step is specific to your requirements, if unsure leave the default and you can come back and fine tune later. Click Next >	 Create Notification Subscription Wizard Alert Criteria General User Role Filter Groups Classes Alert Criteria Alert Aging Formats Help < Previous Next > Finish Cancel Notify on alerts and alert updates that meet these criteria. Check All notifies on all alerts. Items checked within a list are OR'd together. The list are AND'd together. Alerts of any of checked severity: ☑ Error ☐ Warning ☐ Information AND any checked priority: ☑ High ☑ Medium ☐ Low AND any checked alert resolution state: ☑ New ☑ Closed AND any checked category: ☑ Performance Collection ☑ Operations ☑ Event Collection ☑ State Collection ☑ Software And Updates ☑ Alert ☑ System ☑ Custom ☑ Availability Health ☑ Performance Health ☑ Configuration Health ☑ Security Health ☑ Discovery ☑ Notification ☑ Maintenance
9	If you want to be alerted repeatedly as the alert gets older the you can change this setting. Click Next >	 Create Notification Subscription Wizard Alert Aging General User Role Filter Groups Classes Alert Criteria Alert Aging Formats Help < Previous Next > Finish Cancel Alert aging notification options: ● Do not notify on alert aging ○ Use alert aging as a notification criteria Notify when an alert that meets all other subscription criteria remains in any alert resolution state checked on the Alert Criteria page for longer than this period (in minutes): 10

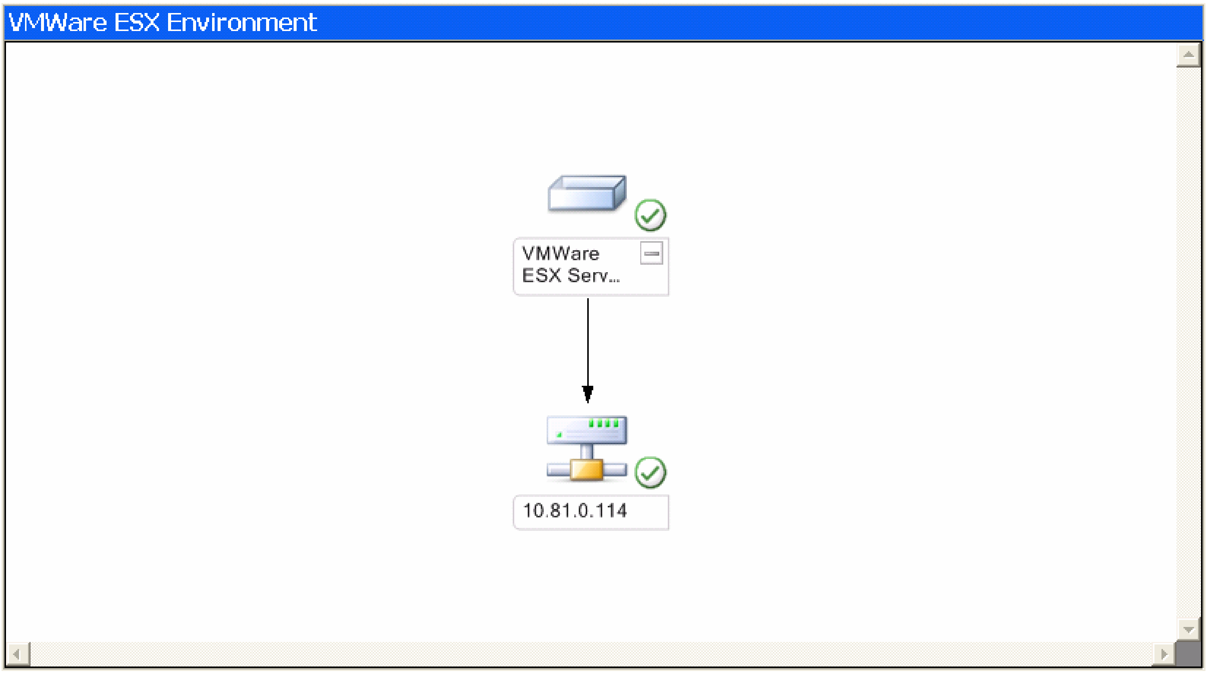
Step	Action/Outcome	Reference
10	Depending on how you would like your alerts (email, IM or SMS) to appear, you can change them here. Click Finish	Create Notification Subscription Wizard Formats Configure the formats for notifications E-mail format: ● Use the default e-mail format ○ Use this custom e-mail format Subject: Alert: $Data/Context/DataItem/AlertName$ Priority: $Data/Context/DataItem/Pr Message: Alert: $Data/Context/DataItem/AlertName$ Source: $Data/Context/DataItem/ManagedEntityDisplayName$ Path: $Data/Context/DataItem/ManagedEntityPath$ Last modified by: $Data/Context/DataItem/LastModifiedBy$ IM format ○ Use the default IM format ○ Use this custom IM format Message: SMS format: ○ Use the default SMS format ○ Use this custom SMS format Subject: Encoding: Unicode (UTF-8) General User Role Filter Groups Classes Alert Criteria Alert Aging Formats Help < Previous Next > Finish Cancel

7 What the operators will see in SCOM

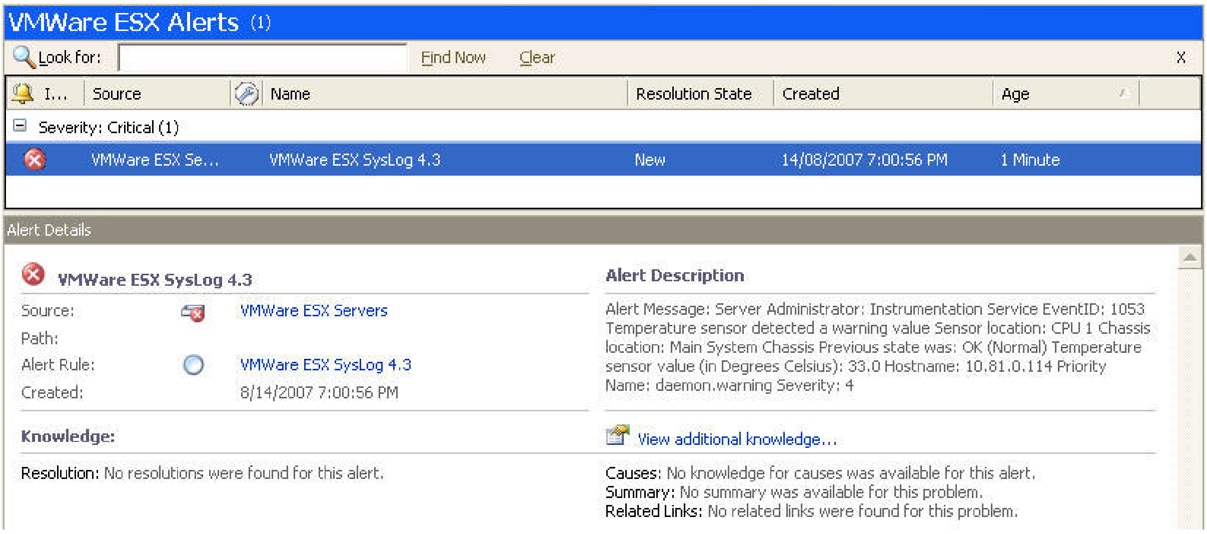
7.1 Example of the VMWare Management Pack Views



7.2 Example of the 'VMWare ESX Environment' View



7.3 Example of the 'VMWare ESX Alerts' View with Alert



I...	Source	Name	Resolution State	Created	Age
Severity: Critical (1)					
✕	VMWare ESX Se...	VMWare ESX SysLog 4.3	New	14/08/2007 7:00:56 PM	1 Minute

Alert Details

VMWare ESX SysLog 4.3

Source:	VMWare ESX Servers
Path:	
Alert Rule:	VMWare ESX SysLog 4.3
Created:	8/14/2007 7:00:56 PM

Alert Description

Alert Message: Server Administrator: Instrumentation Service EventID: 1053 Temperature sensor detected a warning value Sensor location: CPU 1 Chassis location: Main System Chassis Previous state was: OK (Normal) Temperature sensor value (in Degrees Celsius): 33.0 Hostname: 10.81.0.114 Priority Name: daemon.warning Severity: 4

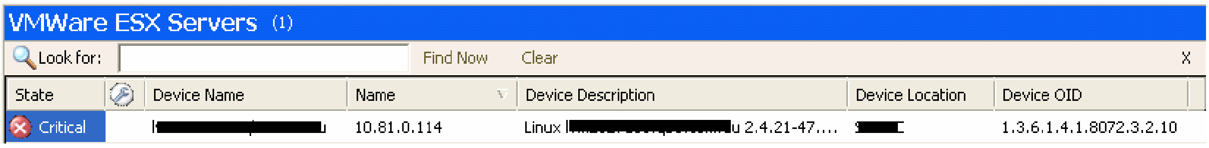
Knowledge:

View additional knowledge...

Resolution: No resolutions were found for this alert.

Causes: No knowledge for causes was available for this alert.
Summary: No summary was available for this problem.
Related Links: No related links were found for this problem.

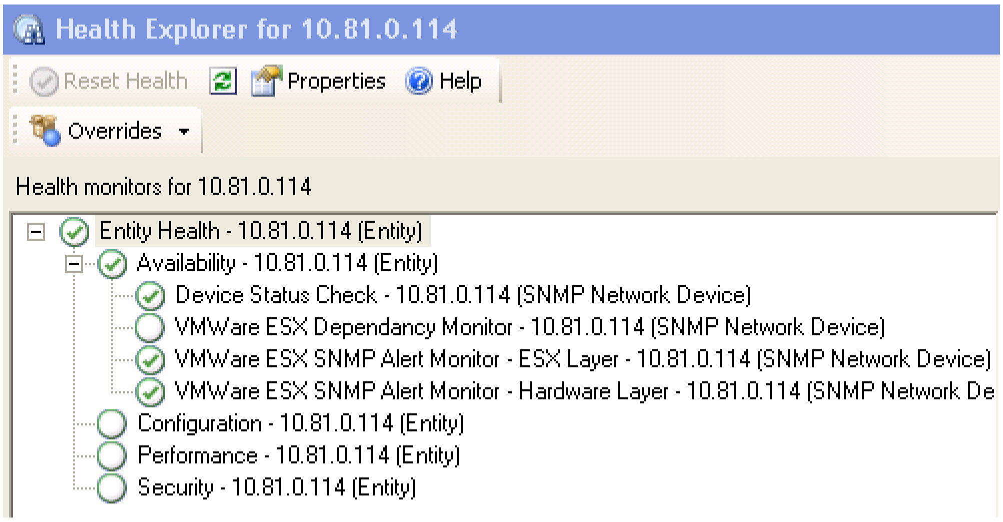
7.4 Example of the ‘VMWare ESX Servers’ View



VMWare ESX Servers (1)

State		Device Name	Name	Device Description	Device Location	Device OID
Critical		[redacted]	10.81.0.114	Linux [redacted] 2.4.21-47....	[redacted]	1.3.6.1.4.1.8072.3.2.10

7.5 Example of the Health Explorer View for an ESX Server

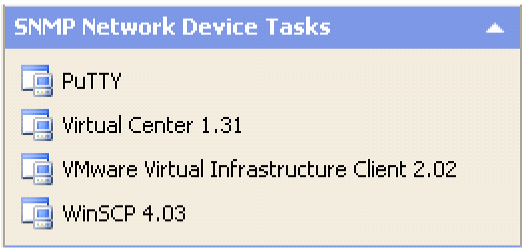


Health Explorer for 10.81.0.114

Health monitors for 10.81.0.114

- ✓ Entity Health - 10.81.0.114 (Entity)
  - ✓ Availability - 10.81.0.114 (Entity)
    - ✓ Device Status Check - 10.81.0.114 (SNMP Network Device)
    - ○ VMWare ESX Dependancy Monitor - 10.81.0.114 (SNMP Network Device)
    - ✓ VMWare ESX SNMP Alert Monitor - ESX Layer - 10.81.0.114 (SNMP Network Device)
    - ✓ VMWare ESX SNMP Alert Monitor - Hardware Layer - 10.81.0.114 (SNMP Network De
  - ○ Configuration - 10.81.0.114 (Entity)
  - ○ Performance - 10.81.0.114 (Entity)
  - ○ Security - 10.81.0.114 (Entity)

7.6 Example of the SNMP Tasks when you have selected an ESX Server



SNMP Network Device Tasks

- PuTTY
- Virtual Center 1.31
- VMware Virtual Infrastructure Client 2.02
- WinSCP 4.03

8 Creating Virtual Center Alerts in the Event Log

This chapter is a supplement and while I will not go in to much detail I will highlight the steps that you can use to add Virtual Center Alerts in to the Event Log.

1. Create a vbs script and save it as VCtoEventviewer.vbs

```
' Takes alerts from VirtualCenter and puts them in the EventLog
Const LogName = "Application"
EventID = WScript.Arguments.Item(0)
Source = WScript.Arguments.Item(1)
Description = WScript.Arguments.Item(2)

Set WshShell=WScript.CreateObject("WScript.Shell")
strCommand="eventcreate /T Warning /ID "& EventID & " /L "&LogName&" /SO "& _

Chr(34) & Source& Chr(34)& " /D " & Chr(34) & Description & Chr(34)
WshShell.Run strCommand
```

All this script does is take 3 parameters, and creates a Warning event to the Application Event Log, the parameters are:

1. Event id, number between 1 and 1000.
2. Event Title
3. Event Description

2. Copy the script to a folder on your Virtual Center Server. (C:\scripts\VCtoEventviewer.vbs)

3. You can pass parameters to the script from VirtualCenter, In this example I have chosen {alarmName} {newStatus} and {eventDescription} as the most appropriate

4. There are other parameters that can be passed to the script, but the above seems to work well. Other parameters:

{eventDescription}
{targetName}
{alarmName}
{triggeringSummary}
{declaringSummary}
{oldStatus}
{newStatus}
{target}

To configure: In VirtualCenter select an Alert, i.e. ESX Host Connection Status; Select Actions, and add an action of Run Script, and enter the following script command to run:

cscript c:\scripts\VCtoEventviewer.vbs 700 "{alarmName} {newStatus}" "{eventDescription}"

This will then call the vbs script and log events in the event log, it seems to work for all alerts. The only thing I suggest changing is the event ID for each alert.

5. Now you can create a Rule or Monitor in SCOM and capture the Eventlog of the Virtual Center Server and alert as appropriate.

9 Appendix A – SysLog Facility & Severity Reference

. referrers to **Facility.Severity**

If you specify 2.4 then you will be forwarding all alerts from kern with a warning or lower alert eg: Warning, err, crit, alert and emerg.

*** represents ALL.**

Facility reference:

Facility	SCOM Representation	Description
user	1	Generated by user processes. This is the default facility; messages not fitting any of the other listed categories here are classified as facility user.
kern	2	Generated by the system kernel
mail	3	Generated by the email system
daemon	4	Generated by system daemons, such as ftpd.
auth	5	Generated by authorisation programs login, su, getty.
lpr	6	Generated by the printing system
news	7	Generated by Usenet News system
uccp	8	Generated by UUCP system
cron	9	Generated by cron and at
local0-7		Generated by up to eight locally defined categories numbered 0 through 7
mark		Generated by syslog itself for time stamping logs

Severity reference:

Severity	SCOM Representation	Description
emerg	0	The most severe messages that prevent continuation of operation, such as immediate system shutdown.
alert	1	System conditions require immediate attention (for example corrupt system database, insufficient disk space, run out of file descriptors, etc)
crit	2	Most serious system/application malfunctioning, such as failing hardware (hard device errors) or software. Usually non-recoverable.
err	3	Mostly correctable errors, for example errors other than hard device errors. Continuation of the operation is possible. Usually all err conditions are automatically recoverable.
warning	4	Warning messages
notice	5	Notices requiring attention at a later time. Non-error conditions that might require special handling. Difference between warning is not clear.
info	6	Informational Messages
debug	7	Messages for debugging purposes
none	8	Messages are not sent from the indicated facility to the selected file.

10 Appendix B – Common Enterprise MIB Numbers

Company	Enterprise MIB String	Enterprise ID
IBM	1.3.6.1.4.1.	2
Hewlett Packard	1.3.6.1.4.1.	11
DELL	1.3.6.1.4.1.	674
Linux	1.3.6.1.4.1.	2021
VMWare	1.3.6.1.4.1.	6876
Net-SNMP	1.3.6.1.4.1.	8072

11 Appendix C – Expression Examples for Guidance

11.1 Example 1

This example refers to the exact error in the form of the OID. Note the first line ensures that you have a base OID so that the rule doesn't apply across the board to all SNMP Traps.

1st Expression

Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[6]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200.140.1.1.1.1

2nd Expression

Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[6]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200.130.4.1.1.2

11.2 Example 2

This example shows that you can look for specific wording in an error, again you will need to use a base OID to keep the Monitor specific.

1st Expression

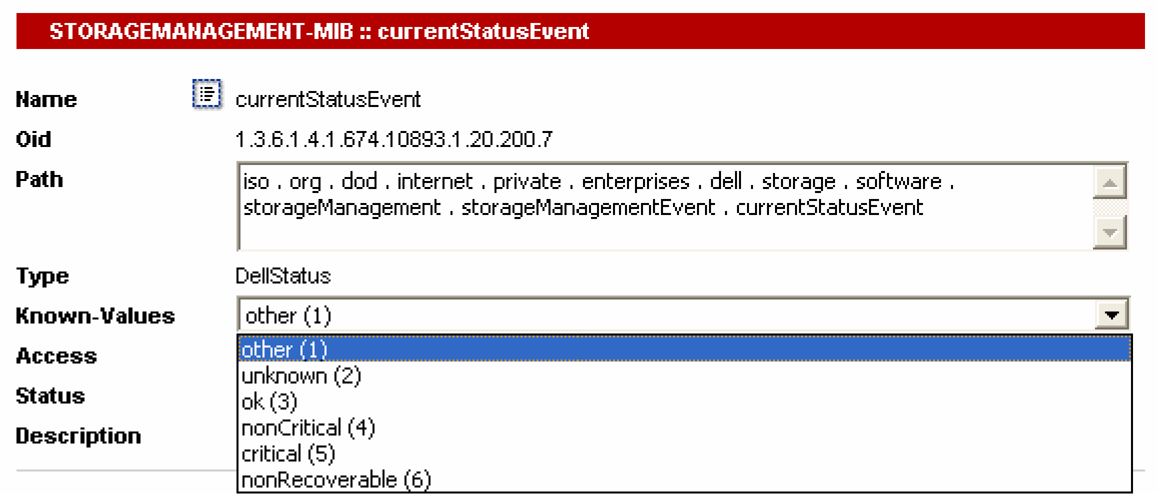
Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[9]/Value	Contains	disk degraded

2nd Expression

Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[9]/Value	Contains	disk Rebuild complete

11.3 Example 3

This example shows how we can use a field dedicated to a current status to base the alert on. From one of the many websites that have a list of all the MIB I found what the data for the 'currentStatusEvent' field was.



STORAGEMANAGEMENT-MIB :: currentStatusEvent

Name: currentStatusEvent

Oid: 1.3.6.1.4.1.674.10893.1.20.200.7

Path: iso . org . dod . internet . private . enterprises . dell . storage . software . storageManagement . storageManagementEvent . currentStatusEvent

Type: DellStatus

Known-Values: other (1)

other (1)
unknown (2)
ok (3)
nonCritical (4)
critical (5)
nonRecoverable (6)

Access

Status

Description

1st Expression

Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[4]/Value	Greater than or equals to	5

2nd Expression

Parameter Name	Operator	Value
/DataItem/SnmpVarBinds/SnmpVarBind[1]/Value	Equals	1.3.6.1.4.1.674.10893.1.20.200
/DataItem/SnmpVarBinds/SnmpVarBind[4]/Value	Less than or equal to	4