Operations Manager 101

Antoni Hanus

Premier Field Engineer - System Center Operations Manager, MOM
US West Premier Field Engineering | Microsoft Services
San Diego, Southern California
Tel: +1 (619) 885-1089 | Email: AntoniHa@Microsoft.com

Disclaimer

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

MICROSOFT MAKES NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED HEREIN. ALL SUCH I NFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL MICROSOFT BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OF PERFORMANCE OF INFORMATION AVAILABLE HEREIN. THE INFORMATION HEREIN COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. MICROSOFT MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE SOFTWARE, PRODUCT (S) AND/OR THE PROGRAM (S) DESCRIBED HEREIN AT ANY TIME.

Revision and Signoff Sheet

Change Record

Author	Version	Change Reference	Date
Antoni Hanus	1.0	Content Created	9/14/2009
Jesse Harris	1.1	Changed Doc Format	8/24/2010

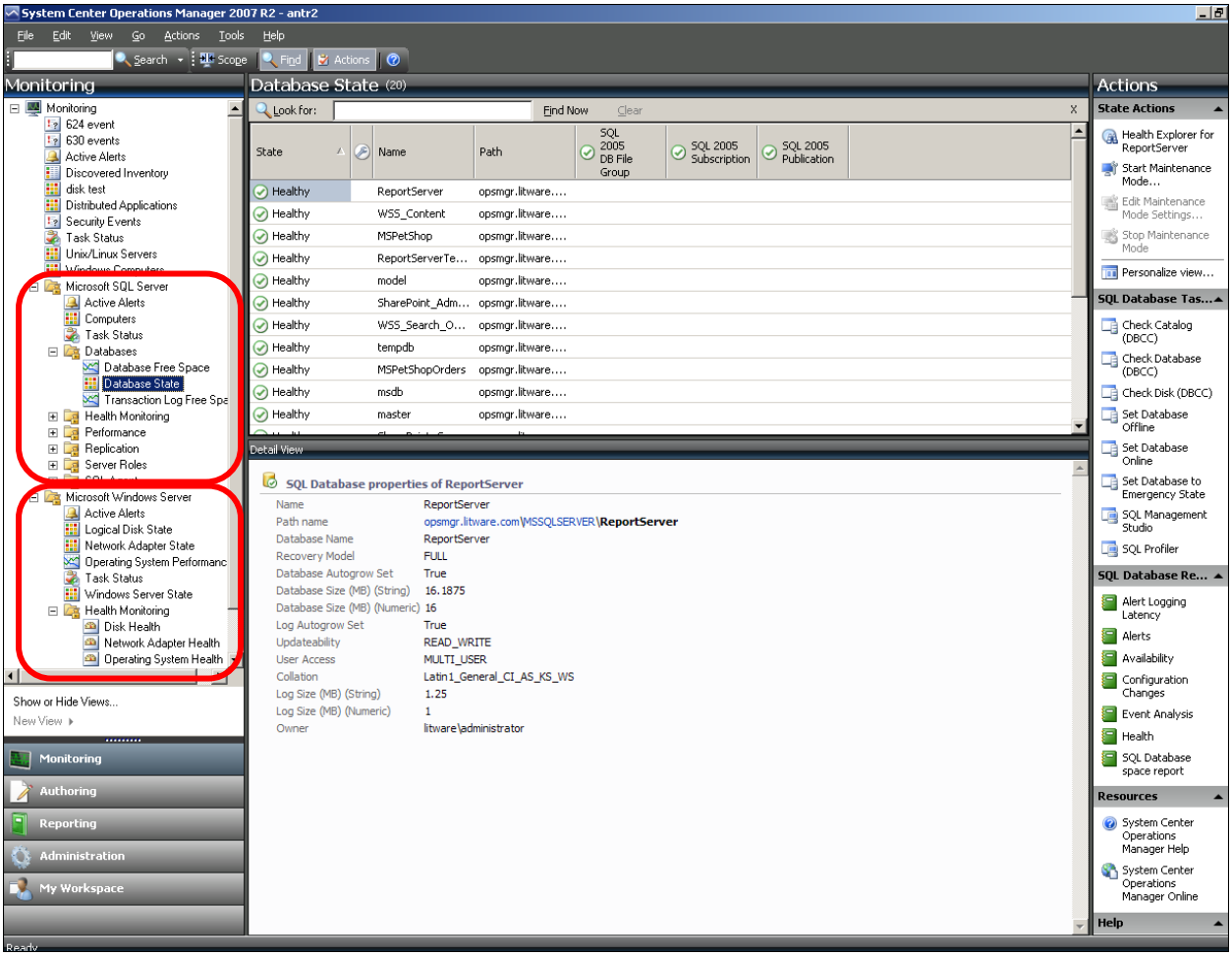
Reviewers

Name	Version approved	Position	Date

Table of Contents

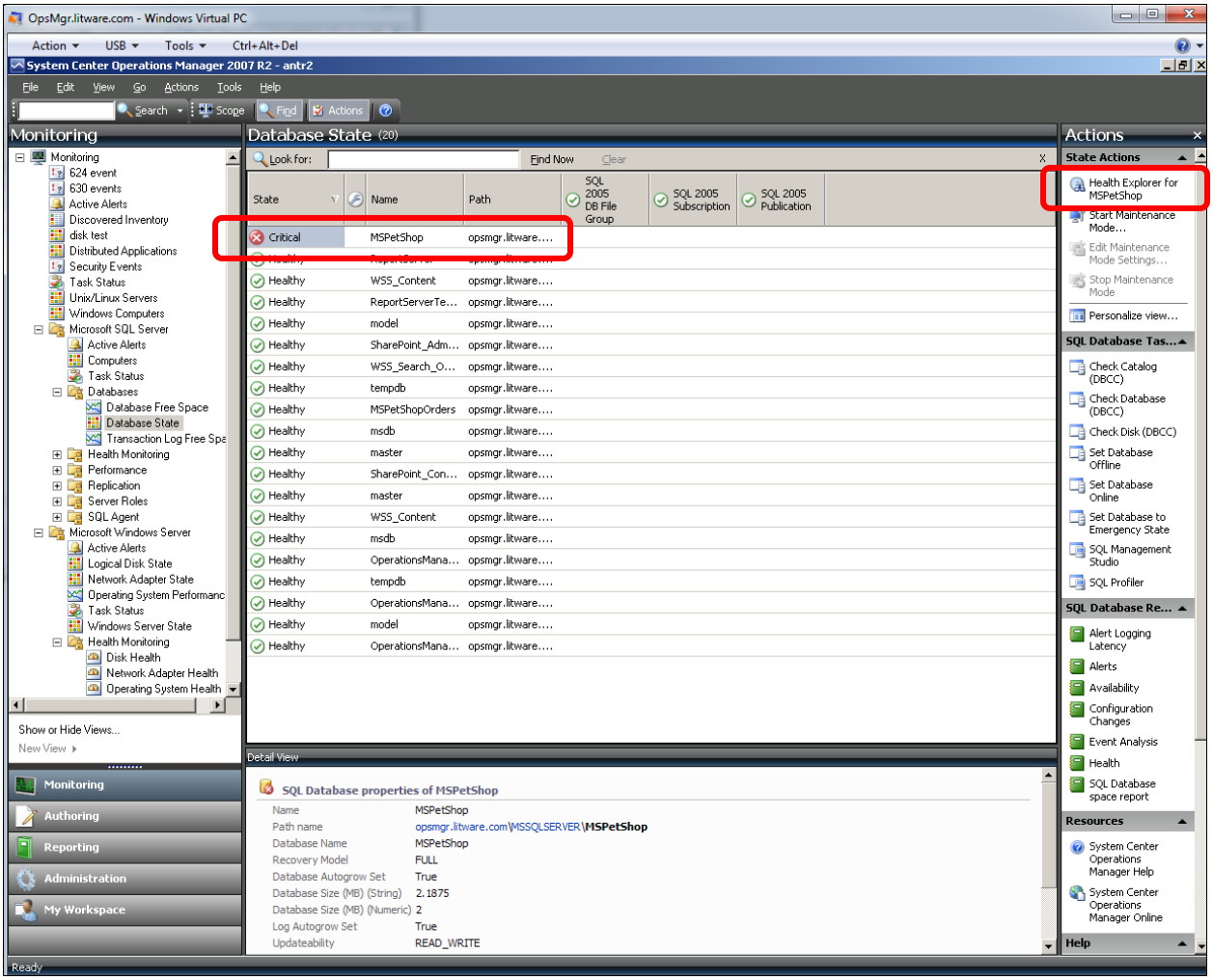
Where do I see Views / Monitoring / Alerts etc for my technology?

Open the Operator's Console, Click the Monitoring Pane and expand the folder that corresponds to the technology that you're interested in. If there is no folder for your technology, either the view is secured so that you can't see it, or (more likely) the management pack is not imported.

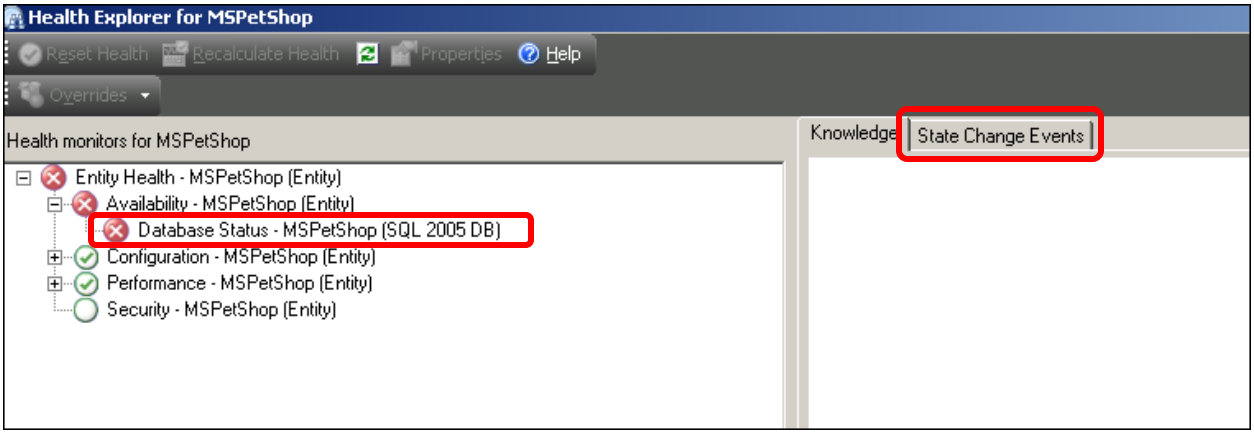


Something shows as Red. How do I figure out why it is showing as Red?

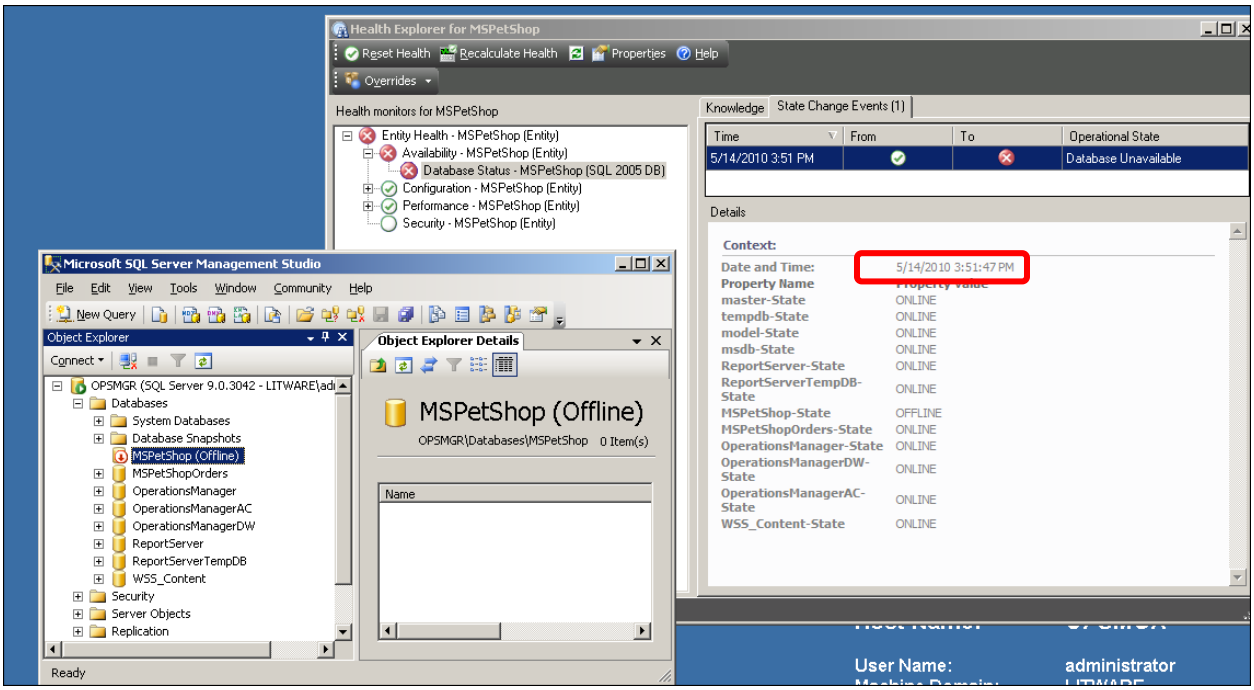
With the item in Red is Selected, click ‘Health Explorer for ….’ On the right-hand side of the console:



This will show the monitors that determine the health of the object you were looking at in the previous view. Click on the monitor that shows as Red and then click on ‘State Change Events’ :

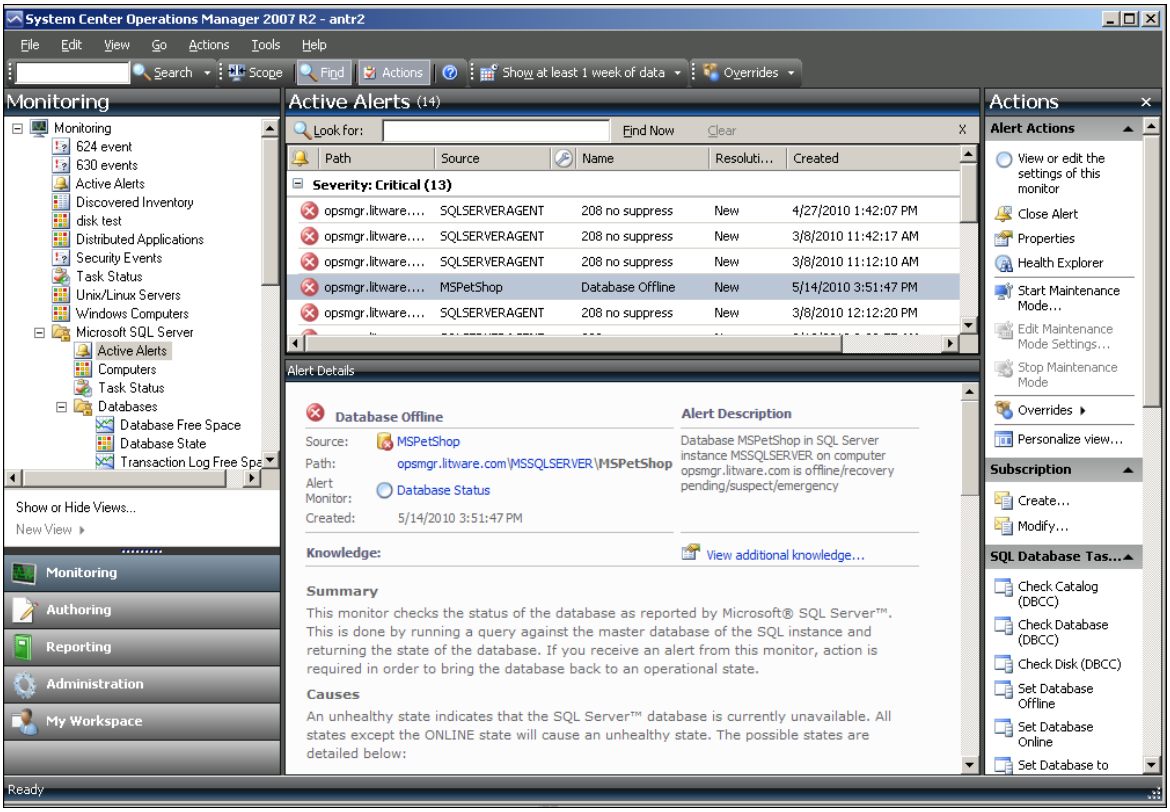


This will show when and what triggered the monitor to go into a red state:

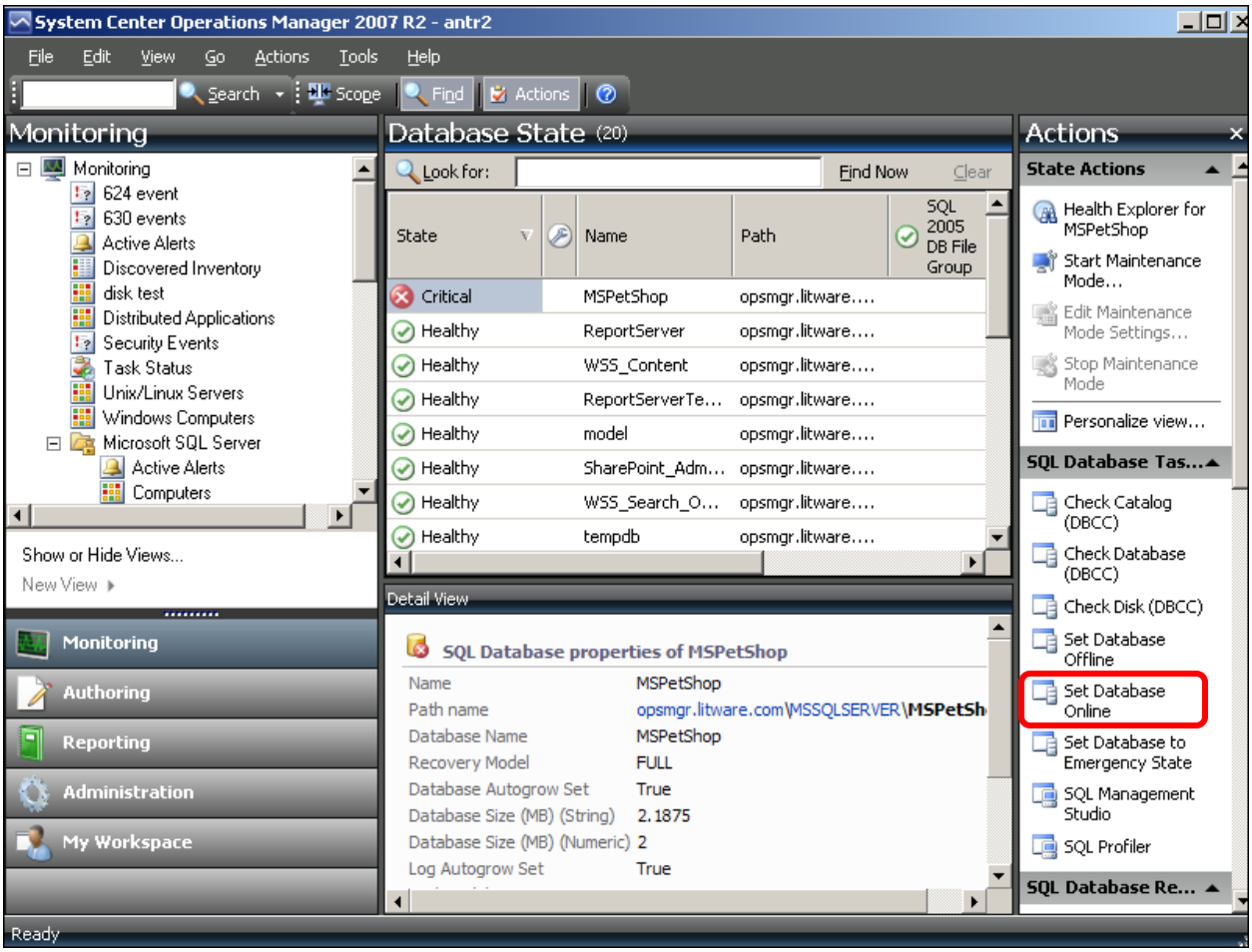


In the above example, if we look in the SQL active alerts, there is also an alert indicating this problem:

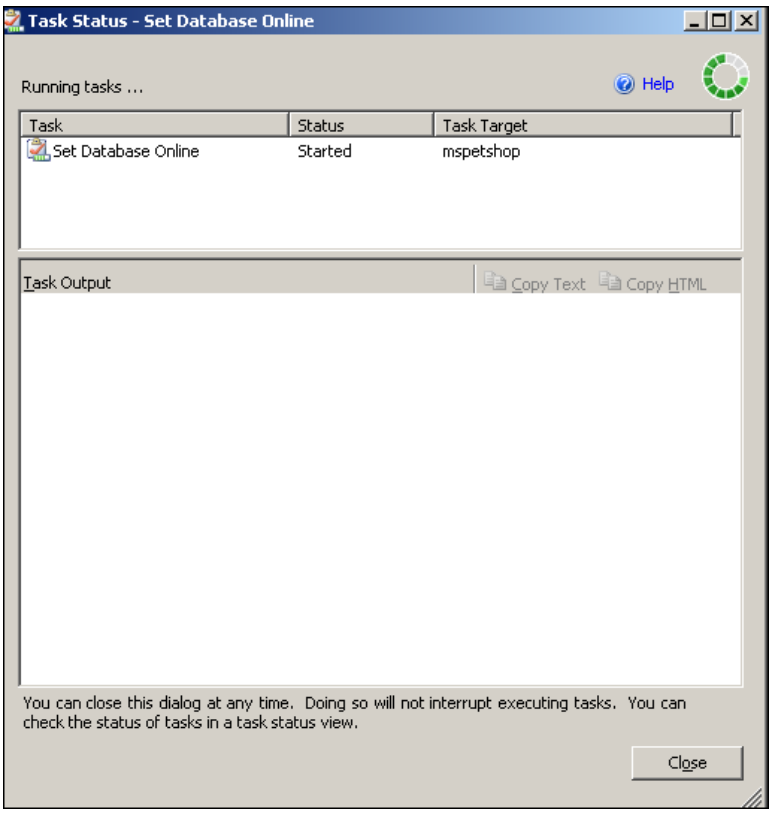
NOTE: This alert will also be visible in the top level active alerts view which displays all new alerts, regardless of the management pack that it comes from:



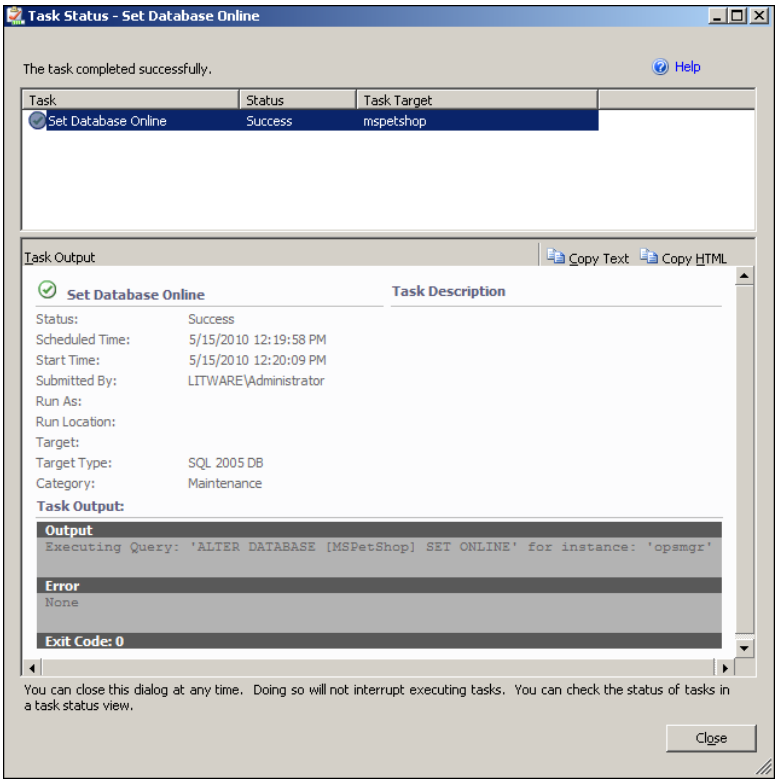
In this case, there is a task available (visible either in the alert view or state view) that will resolve the problem:



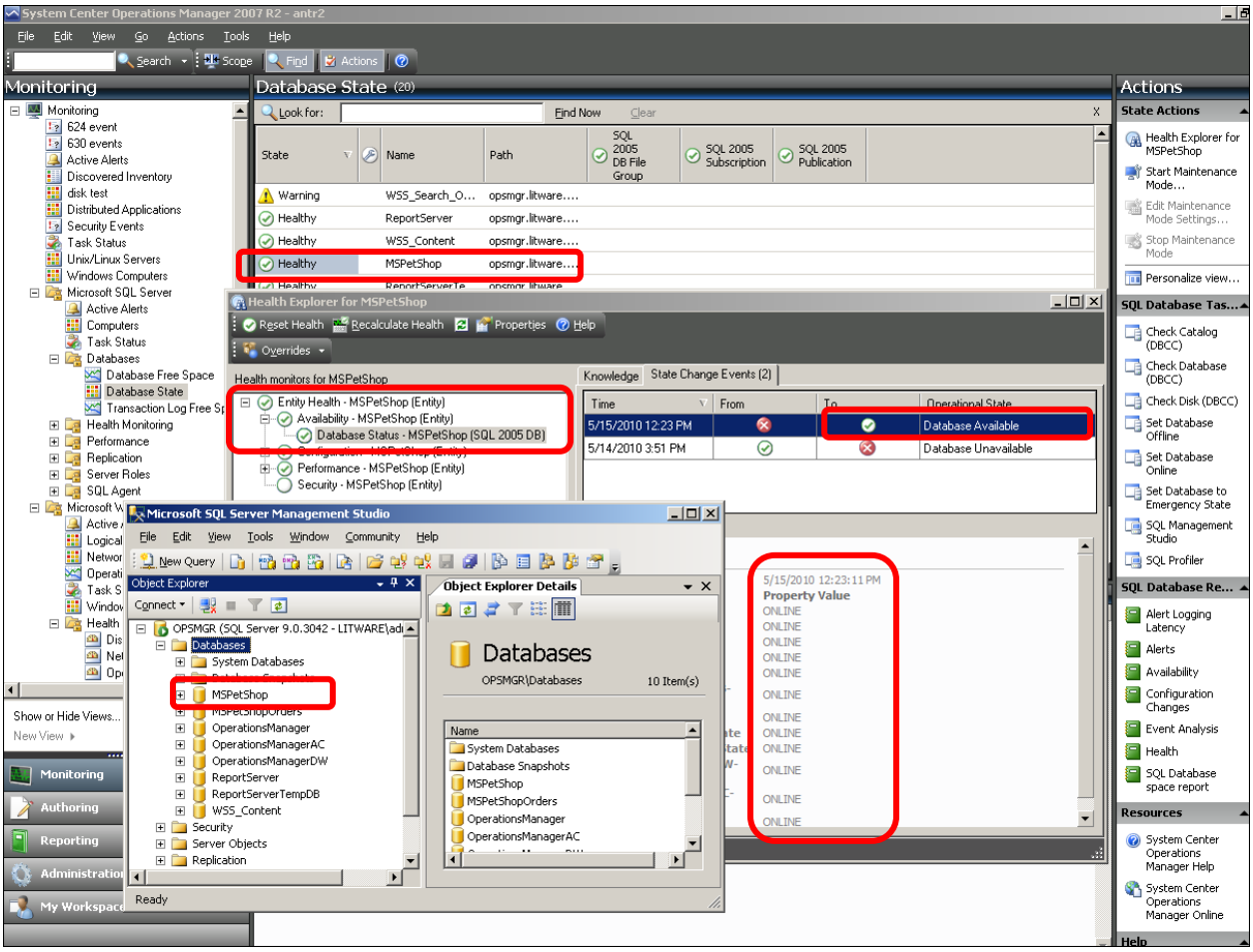
The Task will run to set the DB online:



The Task output will display if the task completed successfully:


Task Status - Set Database Online
The task completed successfully.
Help
Task
Status
Task Target
Set Database Online
Success
mspetshop
Task Output
Copy Text
Copy HTML
Set Database Online
Task Description
Status: Success
Scheduled Time: 5/15/2010 12:19:58 PM
Start Time: 5/15/2010 12:20:09 PM
Submitted By: LITWARE\Administrator
Run As:
Run Location:
Target:
Target Type: SQL 2005 DB
Category: Maintenance
Task Output:
Output
Executing Query: 'ALTER DATABASE [MSPetShop] SET ONLINE' for instance: 'opsmgr'
Error
None
Exit Code: 0
You can close this dialog at any time. Doing so will not interrupt executing tasks. You can check the status of tasks in a task status view.
Close

In SQL, the DB shows as online again, and after Operations Manager detects the online state of the DB (hourly by default), the State of the DB will change back to green in Operations Manager and the alert will get automatically resolved and disappear from the active alerts view:



How do I get more detail on what is in my Technology's Management Pack?

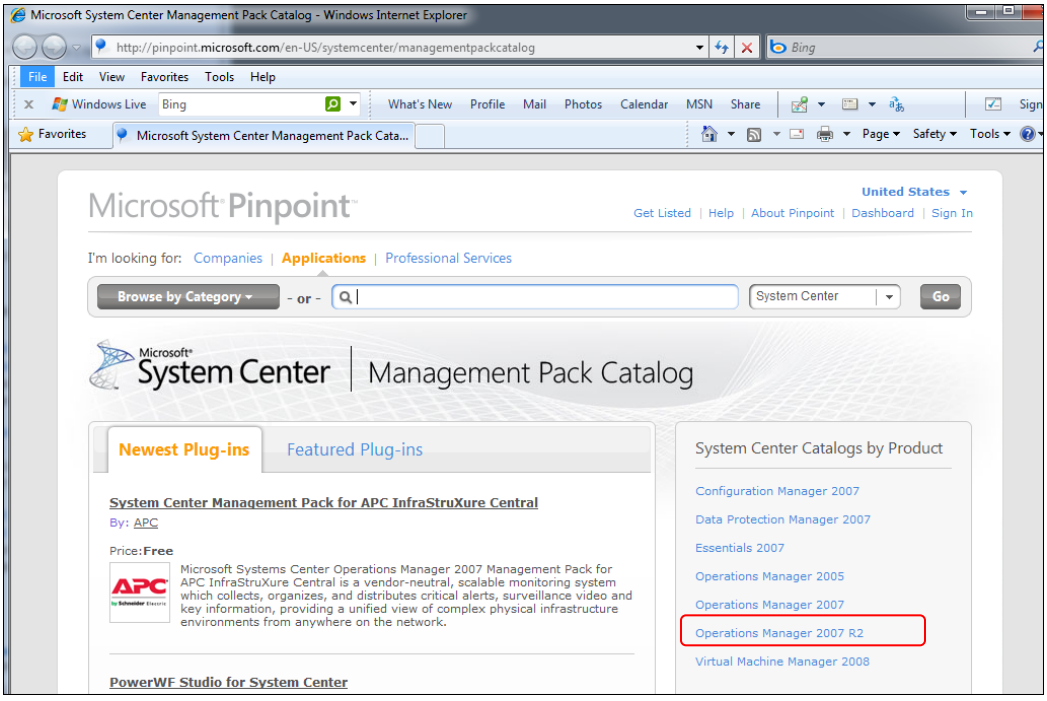
Download the Management Pack Guide:

For an Overview of the Management Pack including what it monitors, how it works, what configuration is required etc., review the Management Pack guide. Download the Management Pack guide using the following steps:

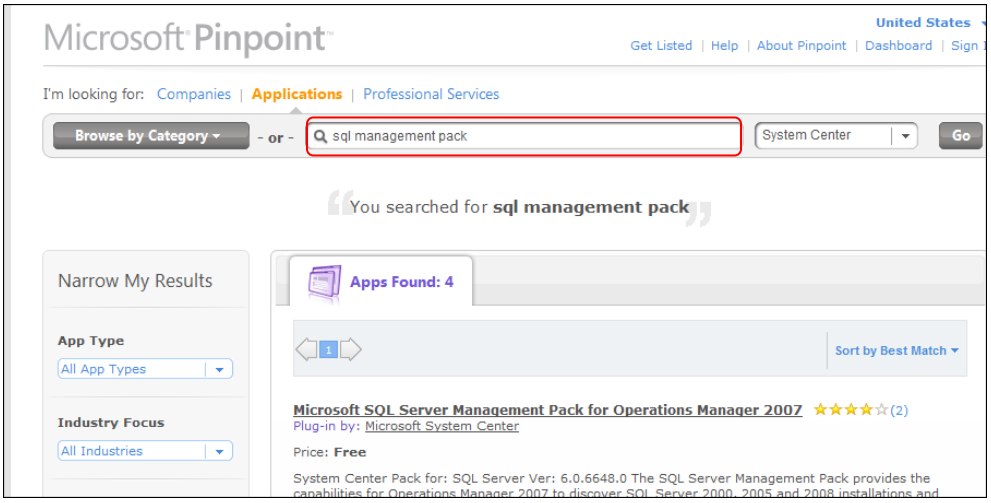
1) Go to the Management Pack catalog at:

http://pinpoint.microsoft.com/en-US/systemcenter/managementpackcatalog

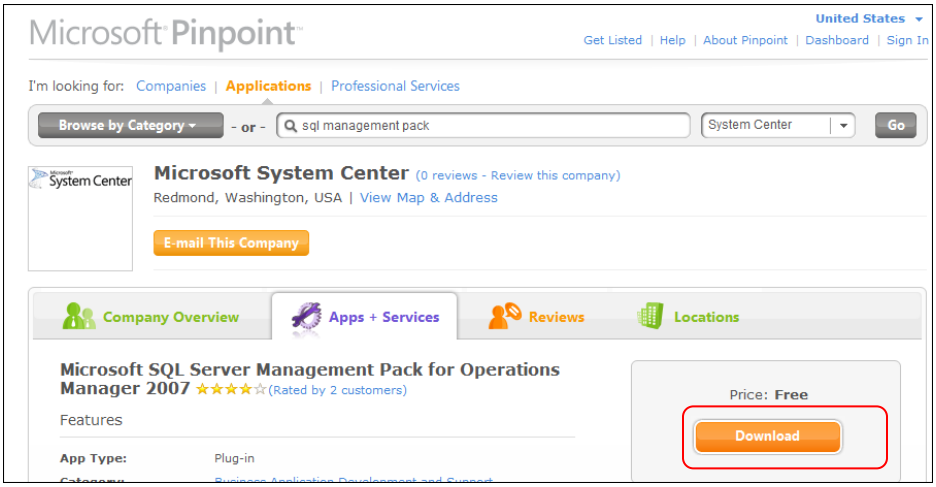
2) On the right hand side, narrow it down to the Operations Manager version you need (Operations Manager 2007 R2 is the latest version and the one that you will normally want):



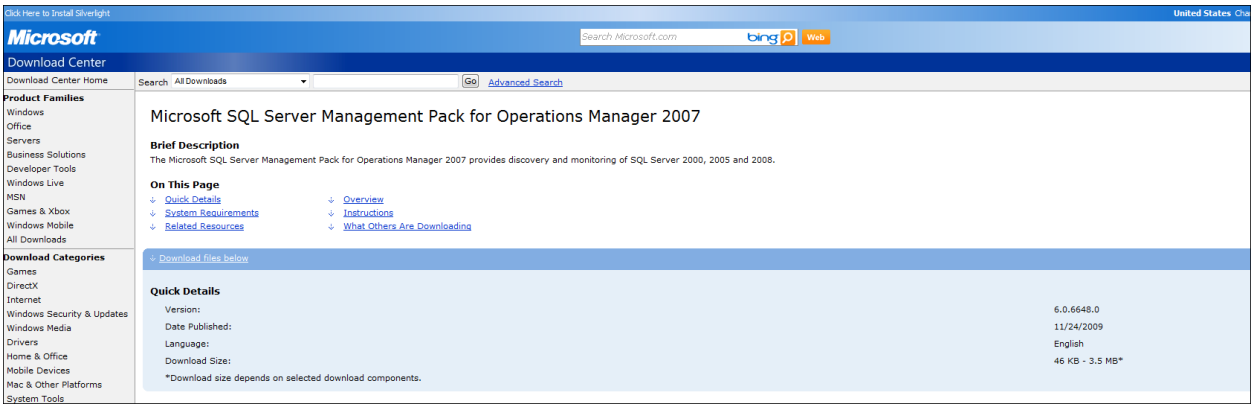
3) In the 'Search Applications' box type the name of the Management Pack that you're after, e.g. SQL Management Pack:



4) Click the Title hyperlink to take you to the pinpoint details for that Management Pack, and click the download button:



5) This will take you to the Microsoft download site to download the msi:



NOTE: you can also 'Bing' something like 'SQL 2005 management pack operations manager 2007 download' which will often take you to the same end page (shown above) much quicker.

6) Run the MSI and this will extract the files in the management pack

NOTE: It will not try to install / import the management pack. It will simply just extract the files.

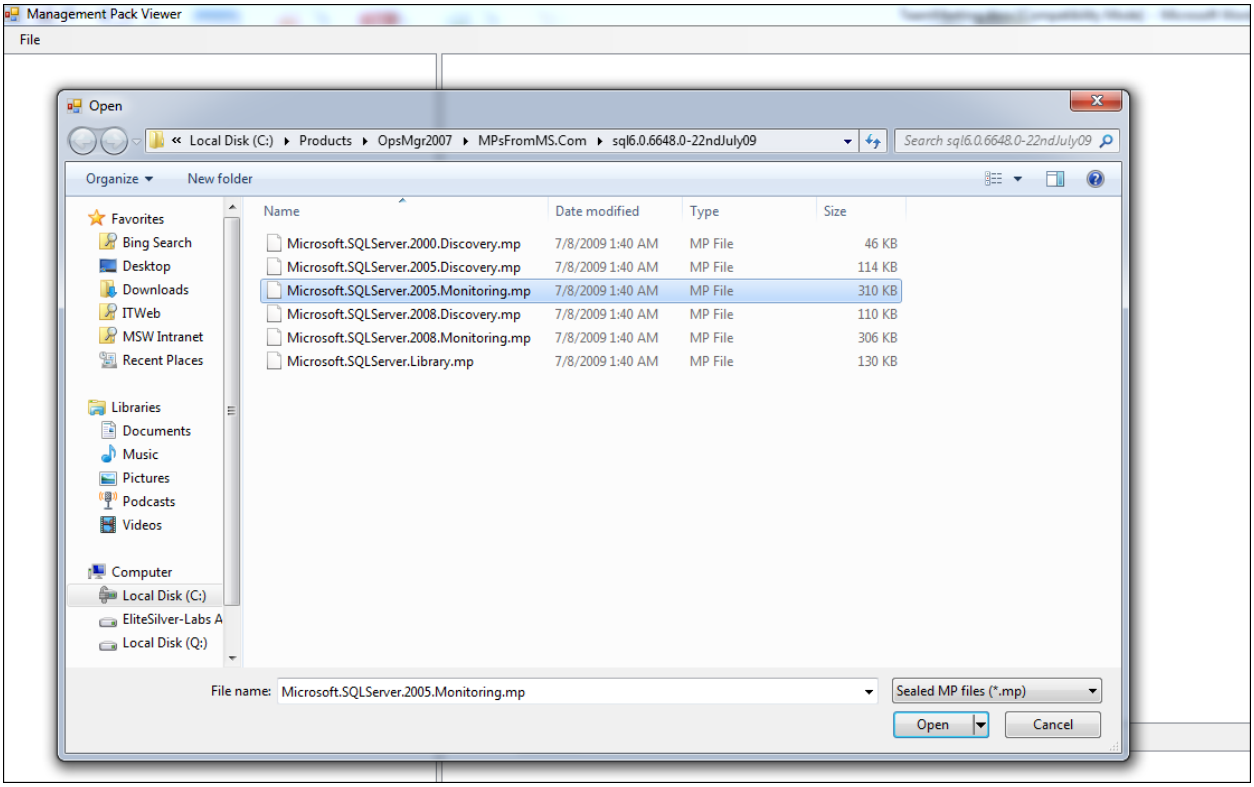
NOTE: One of the files will be a .doc guide which is the MP guide. The rest of the files (.MP extension) are the Management Pack files that need to be imported into Ops Mgr.

7) To get more complete detail than that which is posted in the MP guide (i.e. a complete list of all rules / monitors etc. in a management pack, download and extract the MPViewer tool ZipFile from:

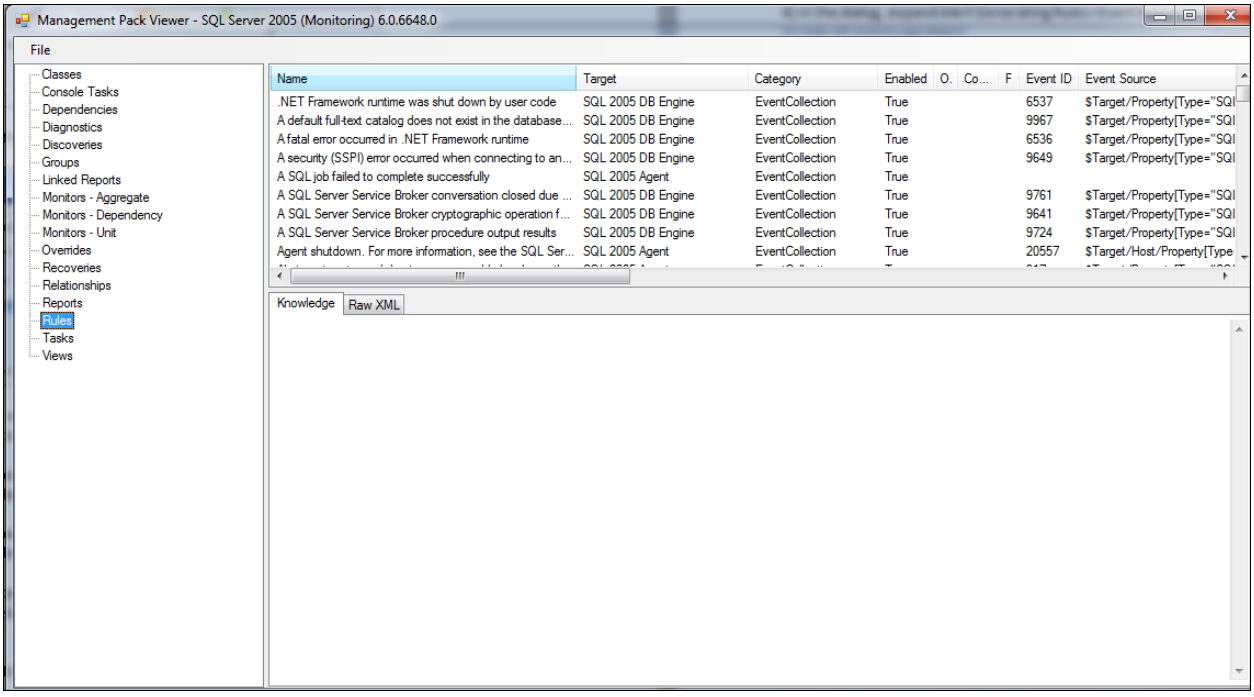
http://blogs.msdn.com/boris_yanushpolsky/archive/2008/06/25/mpviewer-1-7-now-works-with-latest-e12-mp.aspx

NOTE: MP viewer requires the Ops Mgr Operator's console (as it uses some dlls from it).

8) Open MPViewer and navigate to the extracted .mp files:



9) Click on ‘Monitors – Unit’ and / or ‘Rules’ to see the Rules and Monitors:



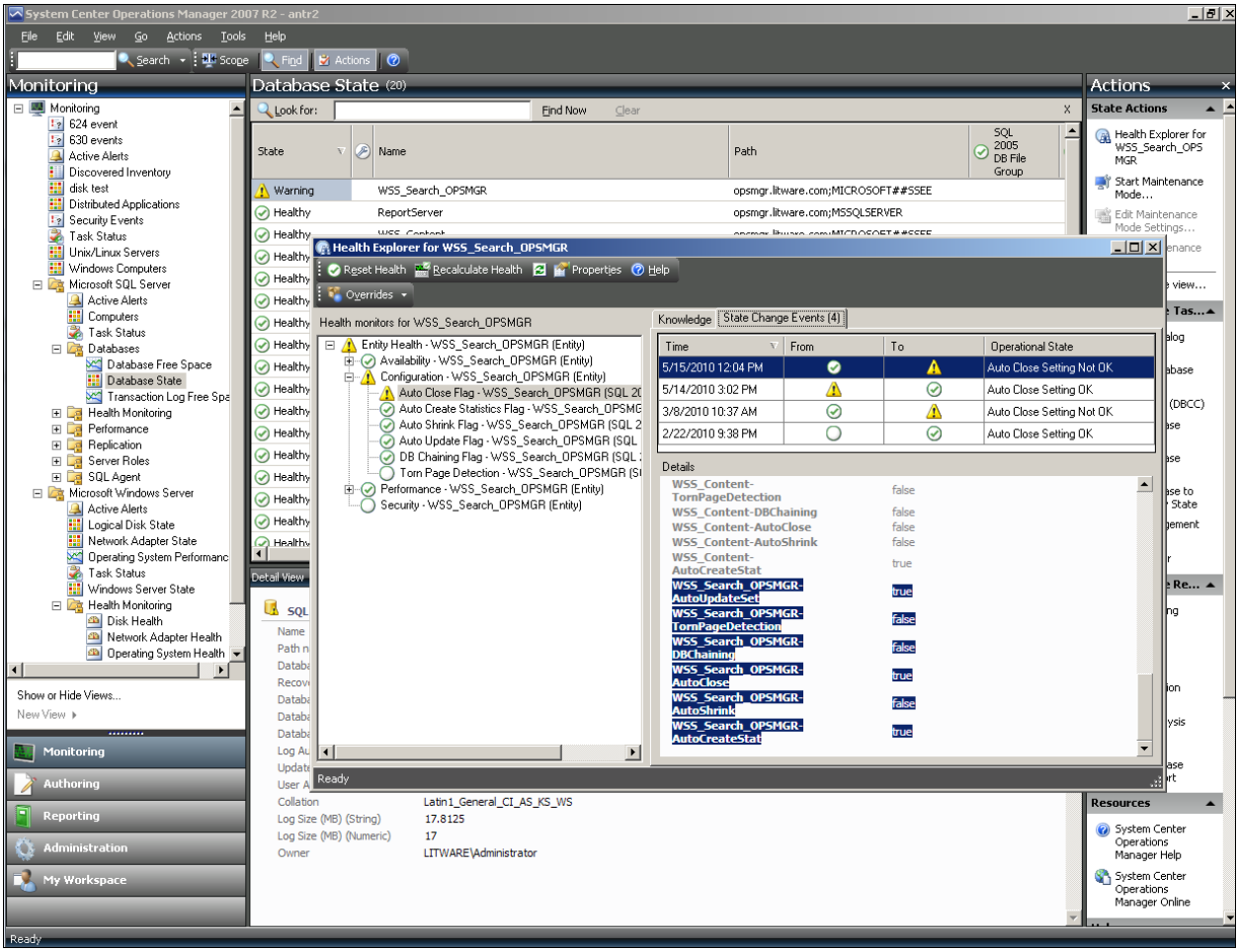
NOTE: You can also sort by Category to show all the event rules / performance rules together.

Also you can save to HTML / Excel using the pull-down file menu.

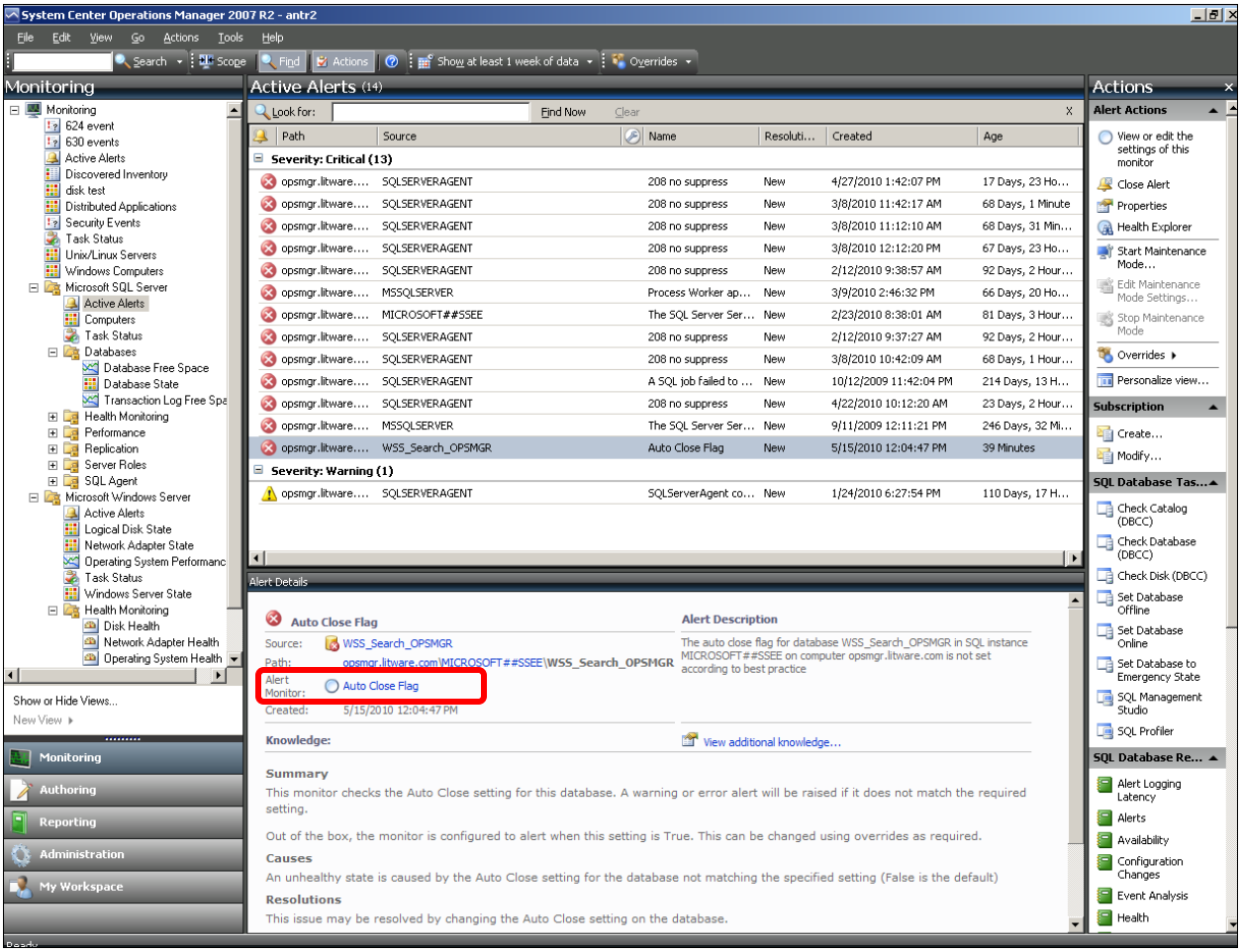
How do I disable or tune something in Ops Mgr?

All Configuration changes in Operations Manager (Enabling / Disabling / Tuning) are performed using overrides which are stored in unsealed management packs.

In the example below, this database is showing as 'Warning' because the Auto Close flag is set to True:

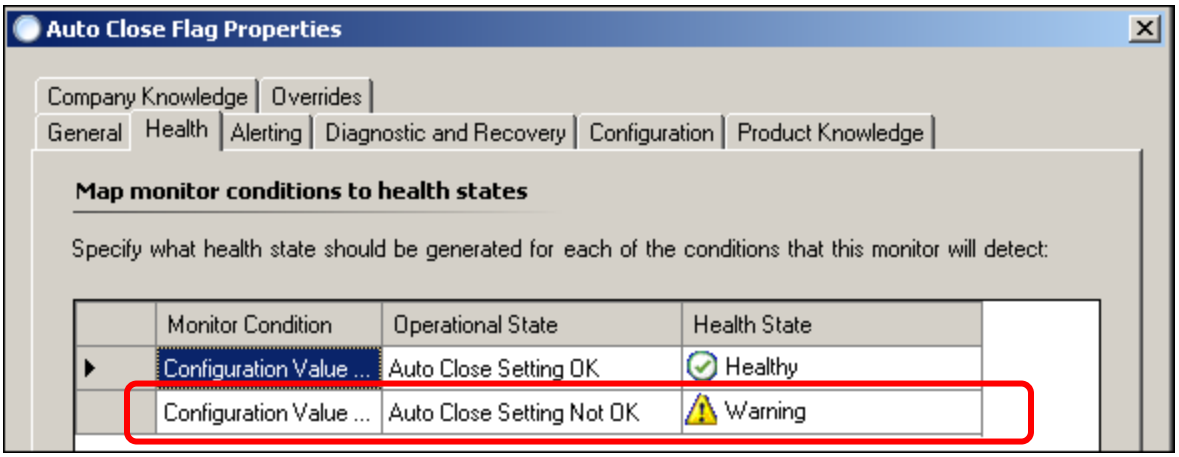


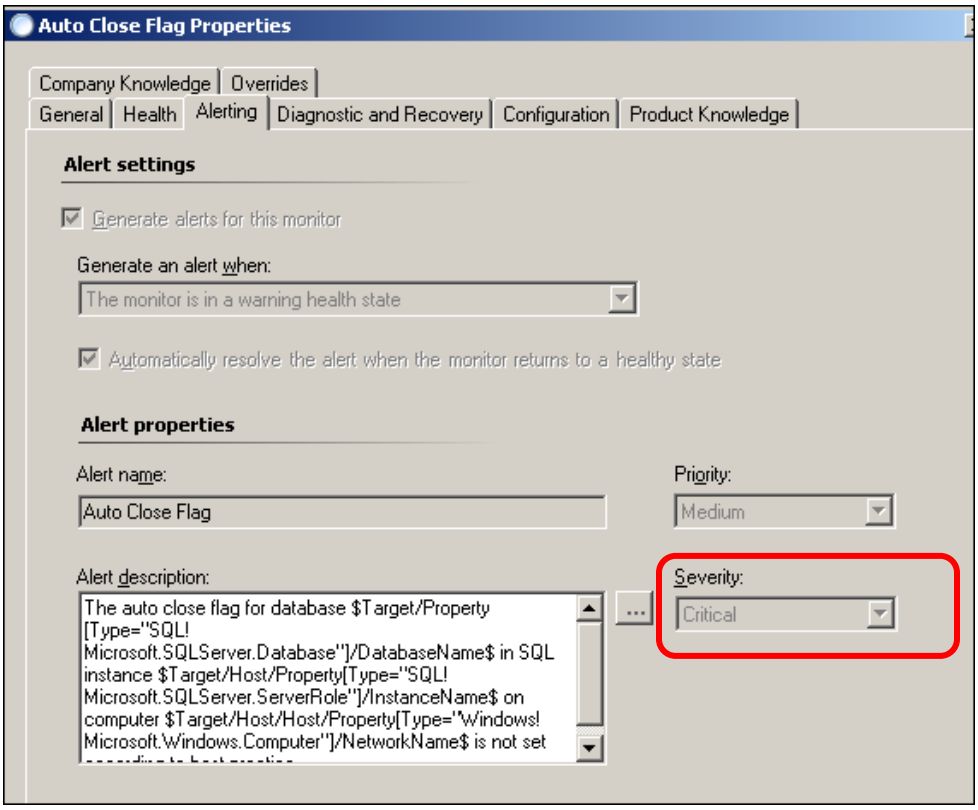
An alert is also visible both in the Active Alerts and SQL alerts views:



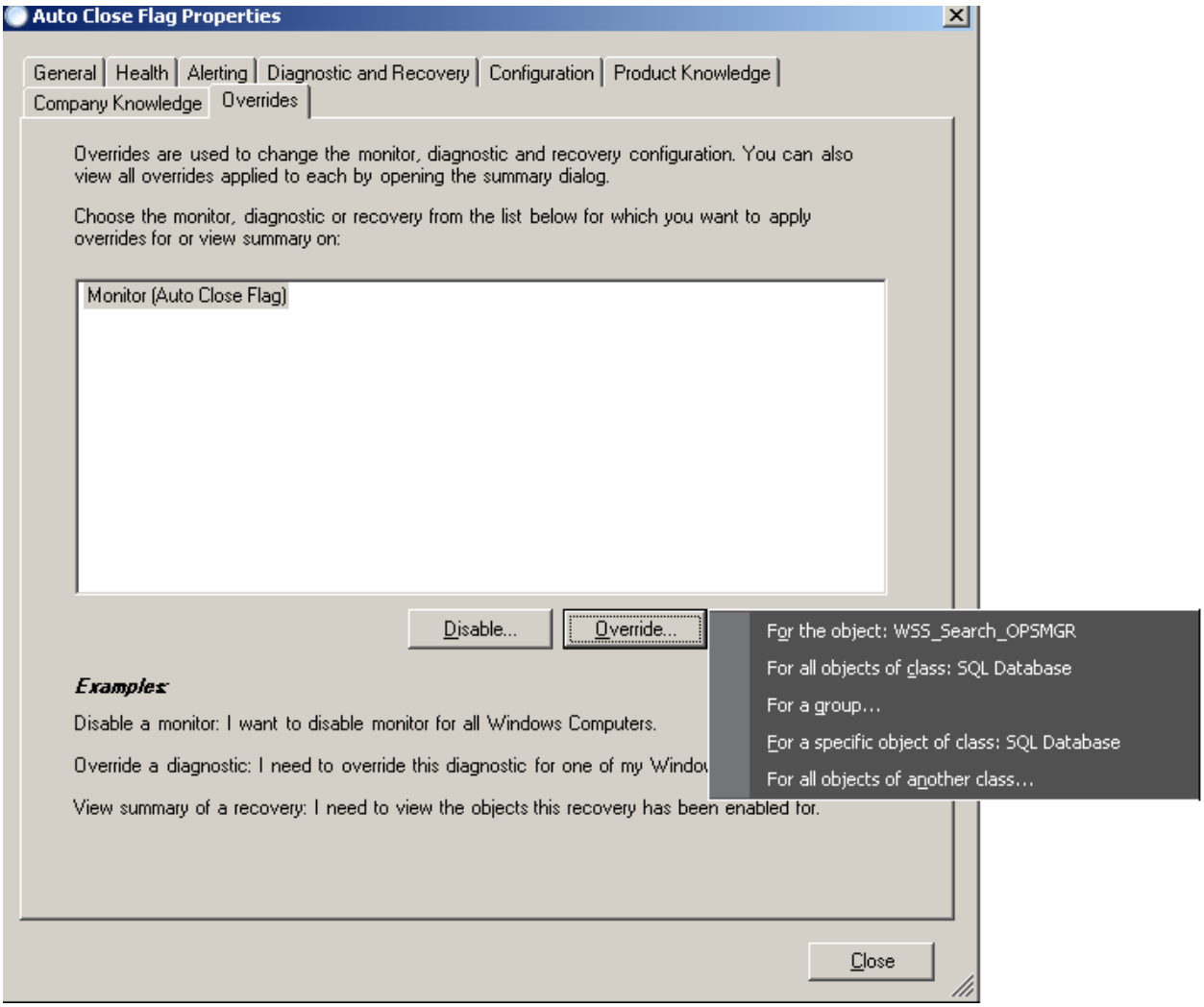
NOTE: Although the state of the object (database) shows as warning, a critical alert is raised. This is the way the monitor has been configured in the sealed SQL Management Pack:

Clicking the Alert Monitor hyperlink (red box in above screenshot) will take you to the Monitor / Rule properties:





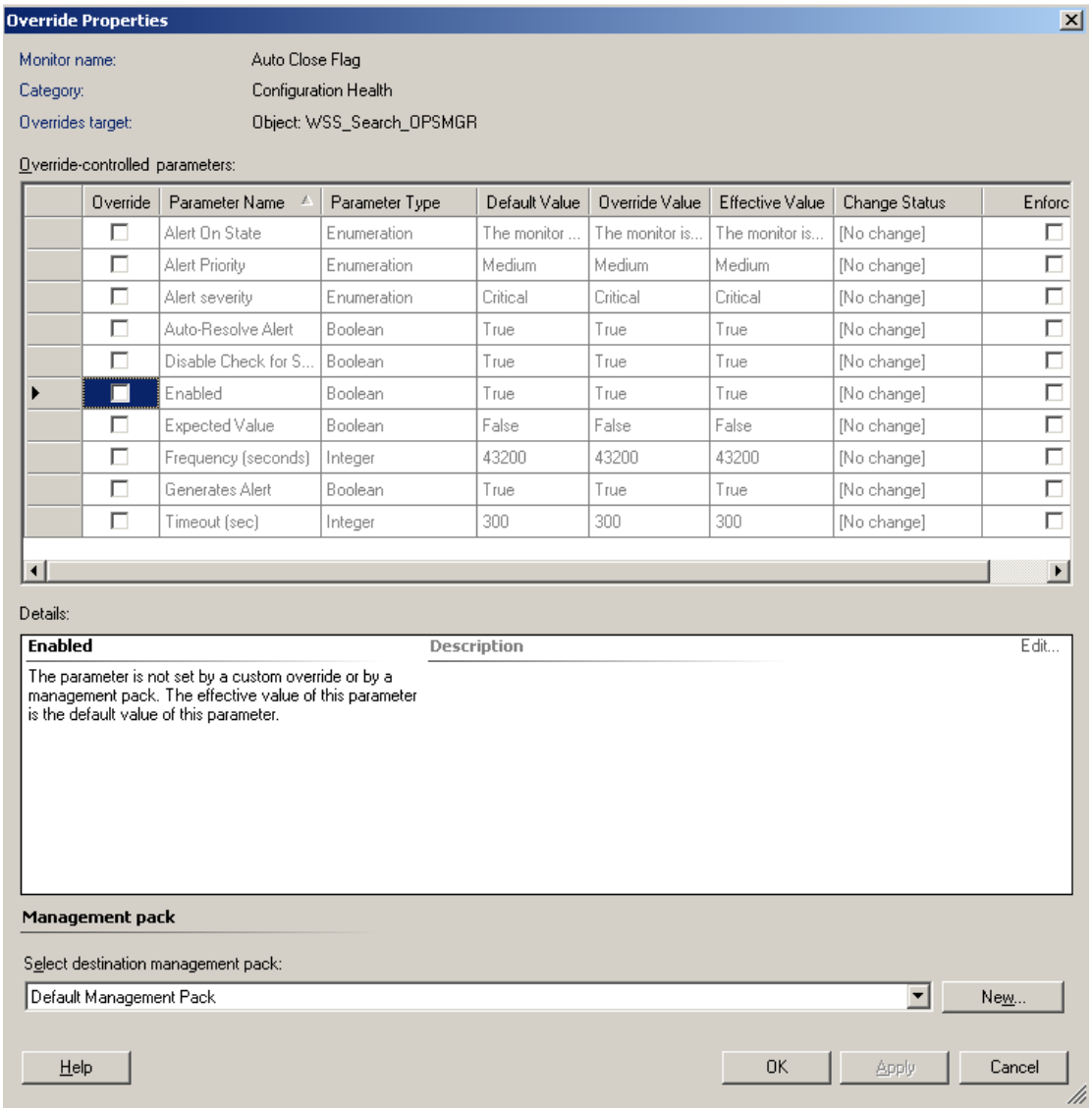
The one place where configuration changes (Enabling / Tuning / Configuration are allowed in in the Overrides tab of the rule / monitor properties:



Clicking the Override button presents a number of objects:

- For the Object: (The configuration change will apply to the one object you accessed the monitor properties through (that the alert was raised for) – in this case the one DB - WSS_Search_OPSMGR
- For all Objects of Class: This will override for every object that the Monitor is targeted to (in this case all SQL Databases that Ops Mgr has discovered – i.e. all SQL servers that have the agent installed
- For a group: You can create a group of databases in the authoring space, and then select the group to create the override against. The pre-created group
- For a specific Object of Class: Clicking this will give you a list of all SQL databases and you can pick the one that you wish to create the override (configuration change) for.
- For all objects of another Class – This option is very rarely used. Only used if relationships are involved.

Once the scope of the option is selected, you will see the same following dialog, whichever object you selected:

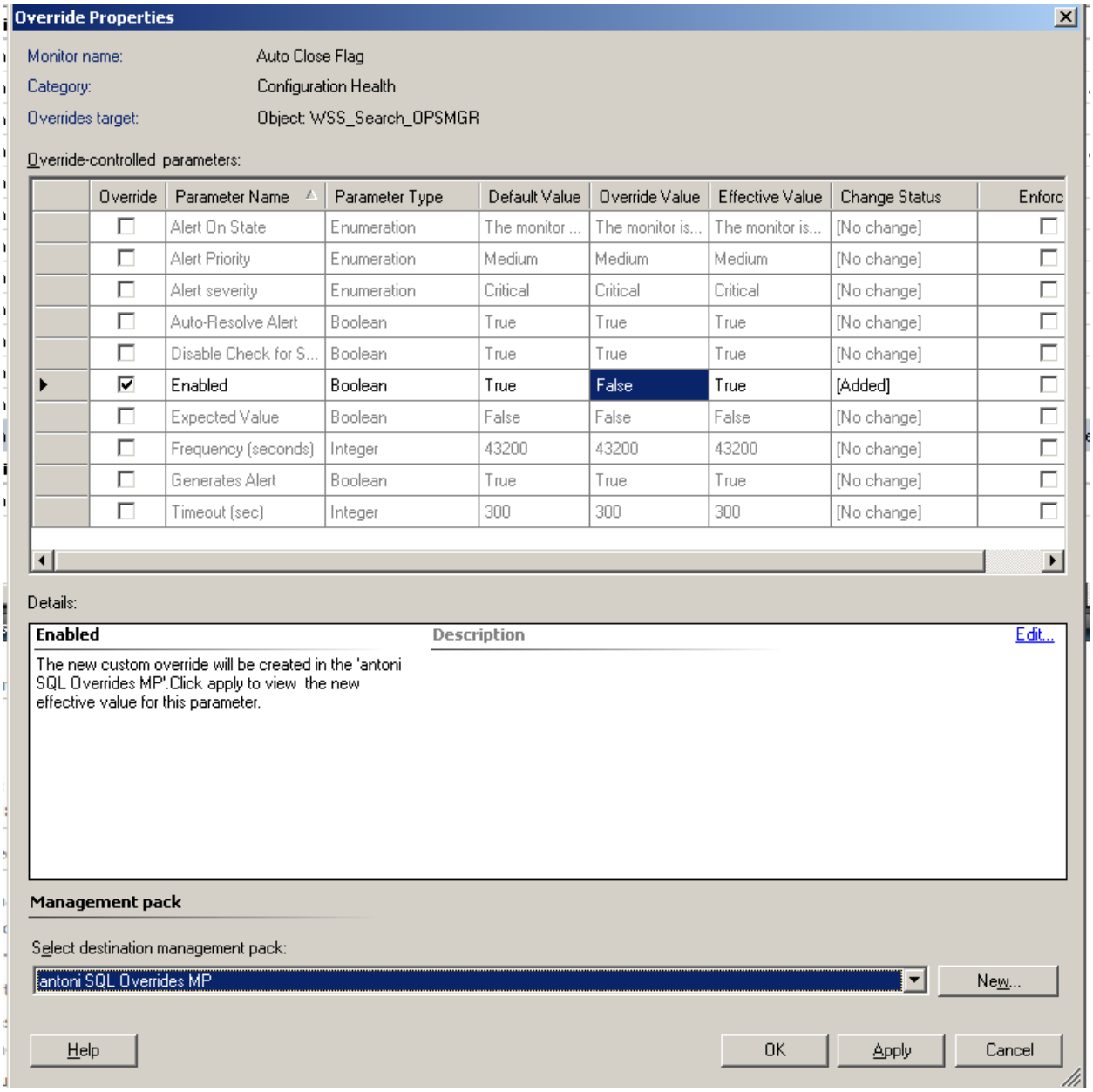


If you want to disable the rule for the object selected, place a check next to the 'Enabled' Parameter, change the Override Value to False and then Change the Management Pack from something other than the default Management Pack

NOTE: The golden rule of Ops Mgr configuration is to NEVER store anything in the default Management Pack. Best practice is to store the override in an unsealed Management Pack created for all Overrides

for your particular technology's sealed MP. So in this case you would have a [Company Name] SQL Overrides MP and that would be the appropriate place to store your overrides. If such a Management Pack does not exist, you can easily create it here, using the New button.

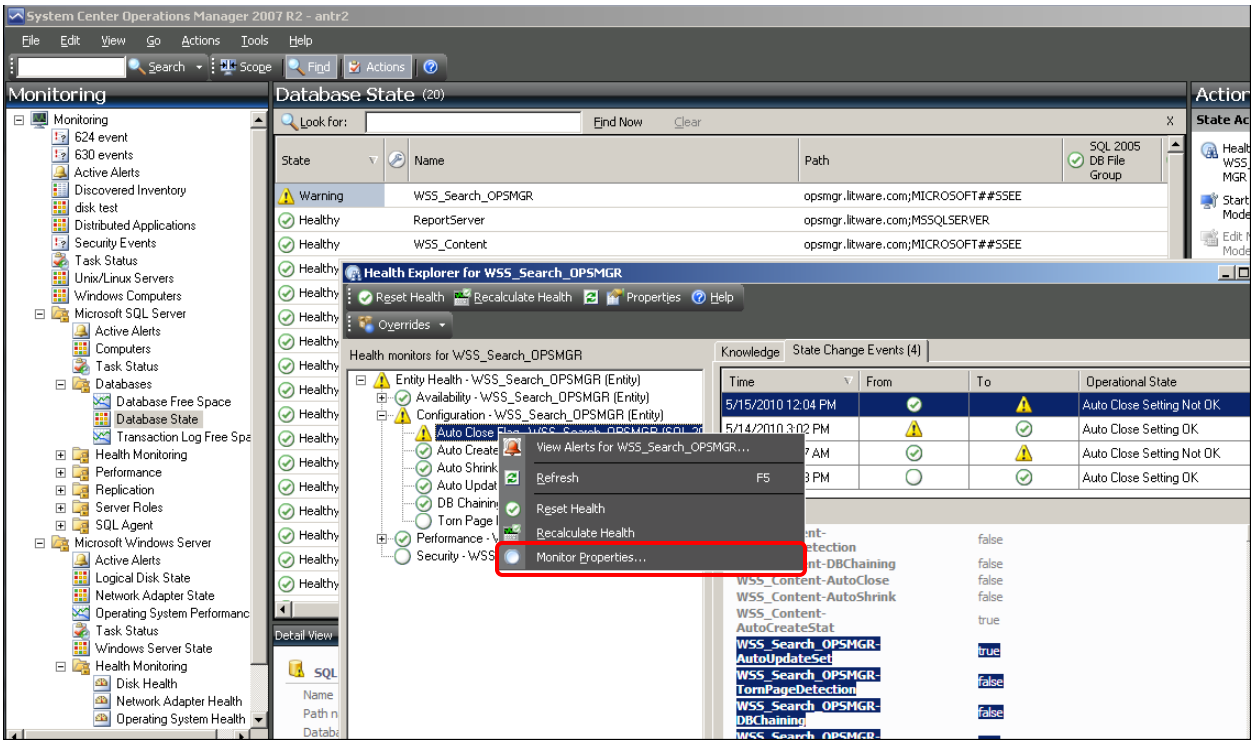
Once configured, it should look something like this to disable the monitor:



Clicking OK will complete the override and the change will be automatically sent to the agent, so that the Auto Close flag monitor gets disabled for the DB on this one SQL server.

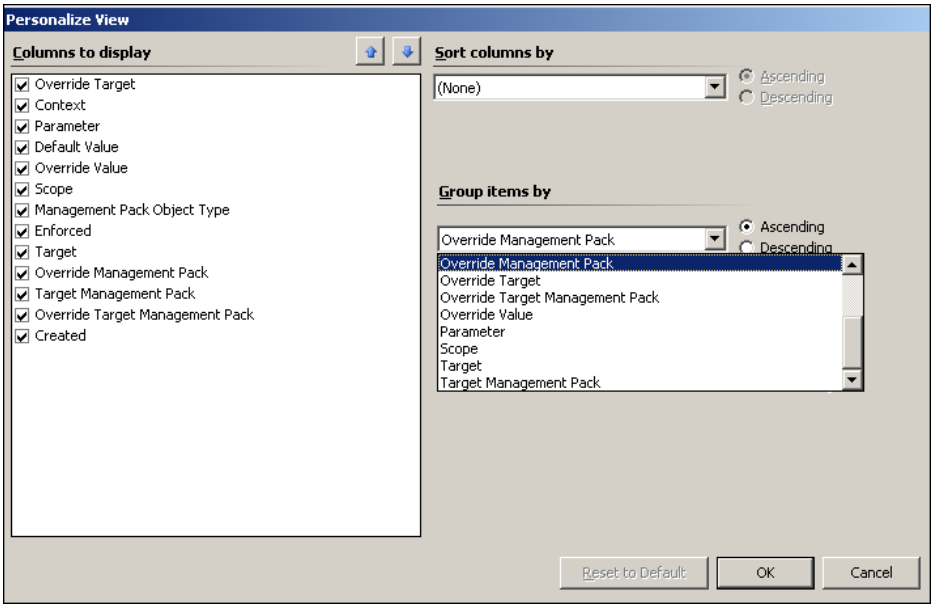
Note that the other parameters above (like frequency of the check, severity of the alert, expected value etc.) can all be overridden here also. The Management Pack Author determined what parameters are exposed as overrideable so the overrides dialog always shows the entire scope of what can be configured for a given rule or monitor.

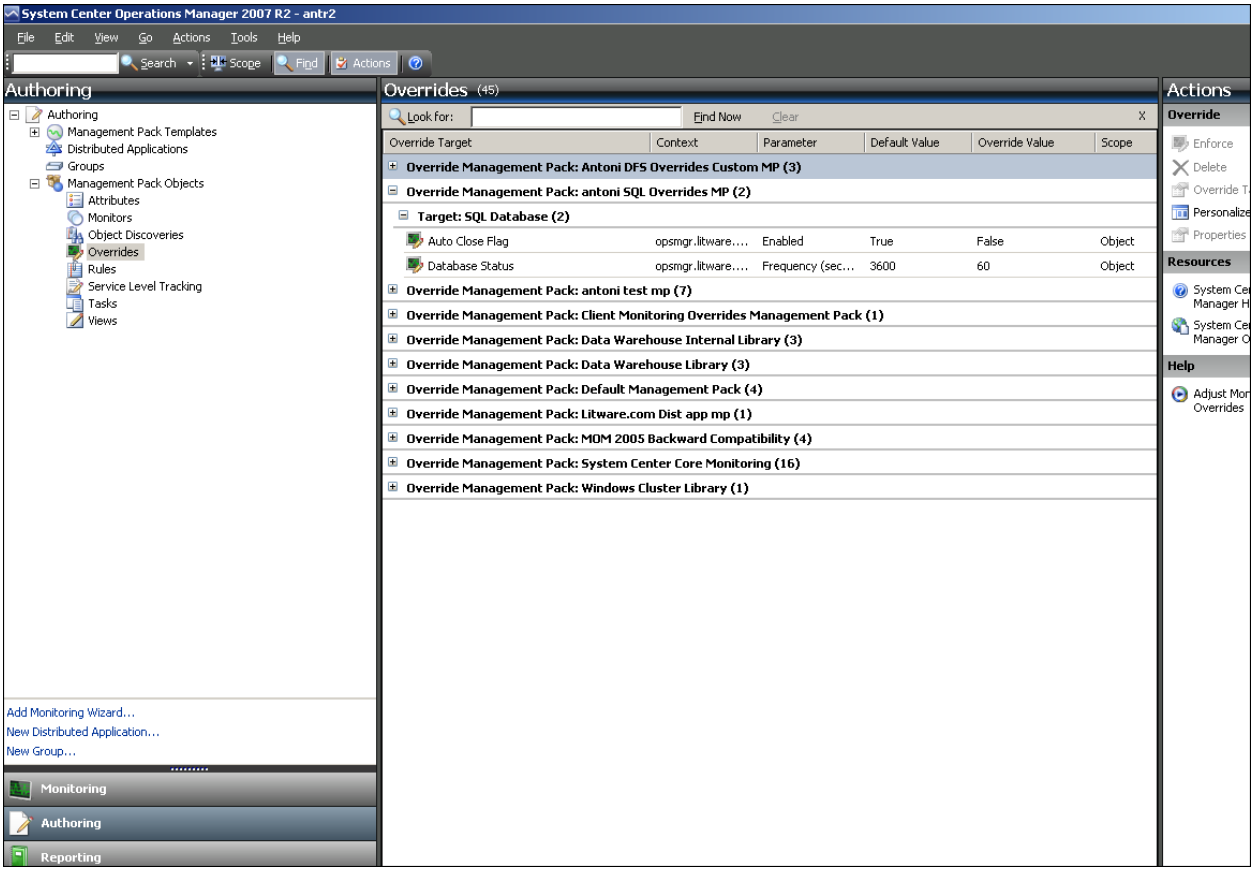
The monitor properties (and the overrides tab) can also be accessed from the health explorer view that is accessed from a state view:



Configuration changes (Overrides) can be viewed using the overrides view:

NOTE Right-click the view and use the Personalize view to Group by ‘Override Management Pack’ or ‘Override Target Management Pack’ for a more useful view:


Personalize View
Columns to display
Override Target
Context
Parameter
Default Value
Override Value
Scope
Management Pack Object Type
Enforced
Target
Override Management Pack
Target Management Pack
Override Target Management Pack
Created
Sort columns by
(None)
Ascending
Descending
Group items by
Override Management Pack
Ascending
Descending
Override Management Pack
Override Target
Override Target Management Pack
Override Value
Parameter
Scope
Target
Target Management Pack
Reset to Default
OK
Cancel


System Center Operations Manager 2007 R2 - antr2
File
Edit
View
Go
Actions
Tools
Help
Search
Scope
Find
Actions
Authoring
Authoring
Management Pack Templates
Distributed Applications
Groups
Management Pack Objects
Attributes
Monitors
Object Discoveries
Overrides
Rules
Service Level Tracking
Tasks
Views
Add Monitoring Wizard...
New Distributed Application...
New Group...
Monitoring
Authoring
Reporting
Overrides (45)
Look for:
Find Now
Clear
Override Target
Context
Parameter
Default Value
Override Value
Scope
Override Management Pack: Antoni DFS Overrides Custom MP (3)
Override Management Pack: antoni SQL Overrides MP (2)
Target: SQL Database (2)
Auto Close Flag
opsmgr.litware....
Enabled
True
False
Object
Database Status
opsmgr.litware....
Frequency (sec...
3600
60
Object
Override Management Pack: antoni test mp (7)
Override Management Pack: Client Monitoring Overrides Management Pack (1)
Override Management Pack: Data Warehouse Internal Library (3)
Override Management Pack: Data Warehouse Library (3)
Override Management Pack: Default Management Pack (4)
Override Management Pack: Litware.com Dist app mp (1)
Override Management Pack: MOM 2005 Backward Compatibility (4)
Override Management Pack: System Center Core Monitoring (16)
Override Management Pack: Windows Cluster Library (1)
Actions
Override
Enforce
Delete
Personalize
Properties
Resources
Help
Adjust Mon
Overrides

How do I create a rule to be alerted on a scenario such as a user being added to domain admins?

Go to the Authoring space

1) Launch the Operator's Console (Start>All Programs>System Center Operations Manager 2007 R2>Operations Console)

2) Click the 'Authoring' space on the bottom left hand side.

3) Right-click Management Pack Objects>Rules and choose 'Create a new rule'

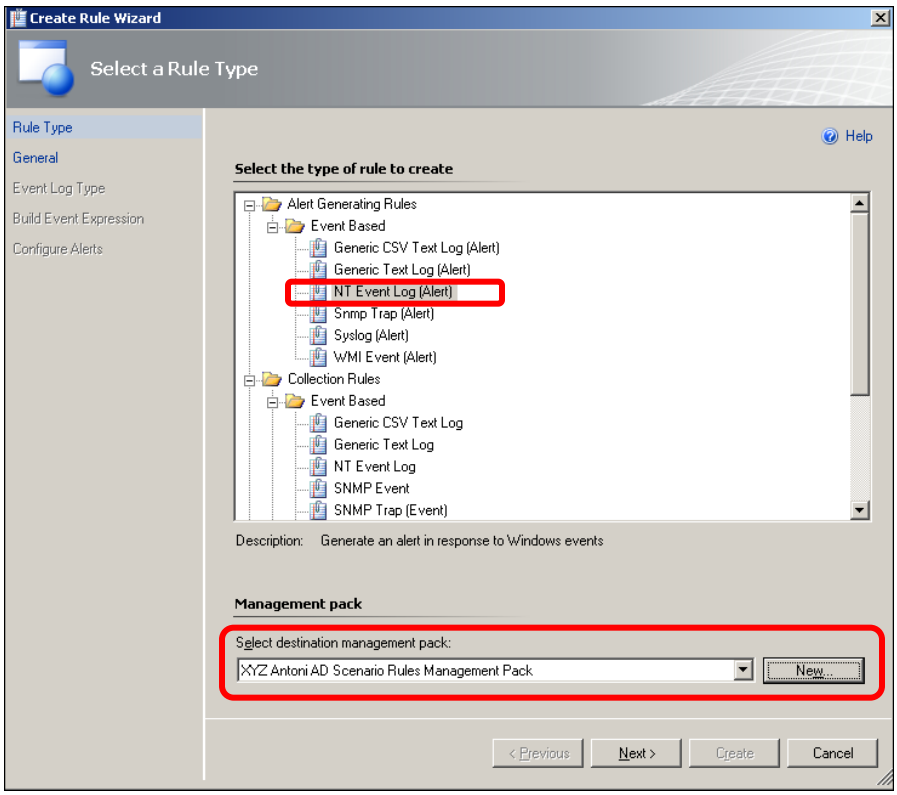
4) In the dialog, expand Alert Generating Rules>Event based

5) Click NT Event Log (Alert)

NOTE: A Golden rule of Operations Manager is to NOT store anything in the Default Management Pack. See Section M of this document for explanation why.

6) Change the Management Pack from Default Management Pack to an appropriate Management Pack. If there is an MP where all the company's custom rules and monitors are stored (or even better an MP where the organization's AD or Auditing Rules / Monitors are stored) , then select it from the dropdown. If not Create a new Management Pack by clicking the New button, give it a name, hit Next and Create)

7) With NT Event Log(Alert) and the appropriate Management Pack selected, click Next:



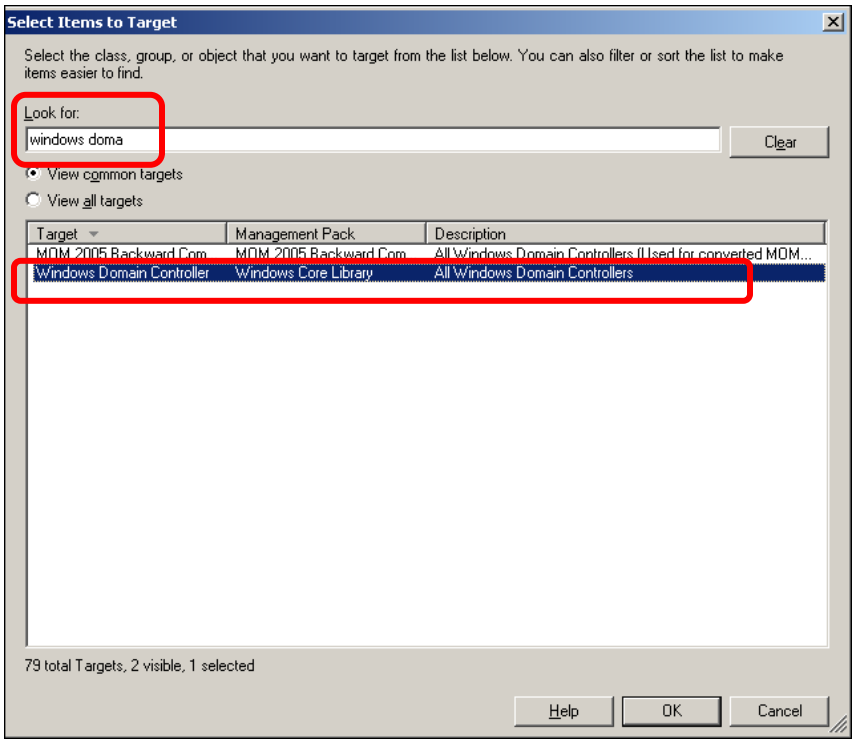
8) Give the rule a name (For Example: 'XYZ Alert generating Rule for User Added to Domain Admins 632 Event')

NOTE: It is best practice to use some form of prefix or three-letter acronym as a naming convention, to identify all of an organization's custom rules and monitors. This makes it much easier to find custom rules in the console when necessary.

9) Click the 'Select' button next to the Rule target box and choose an appropriate target such as 'Windows Domain Controller and click OK.

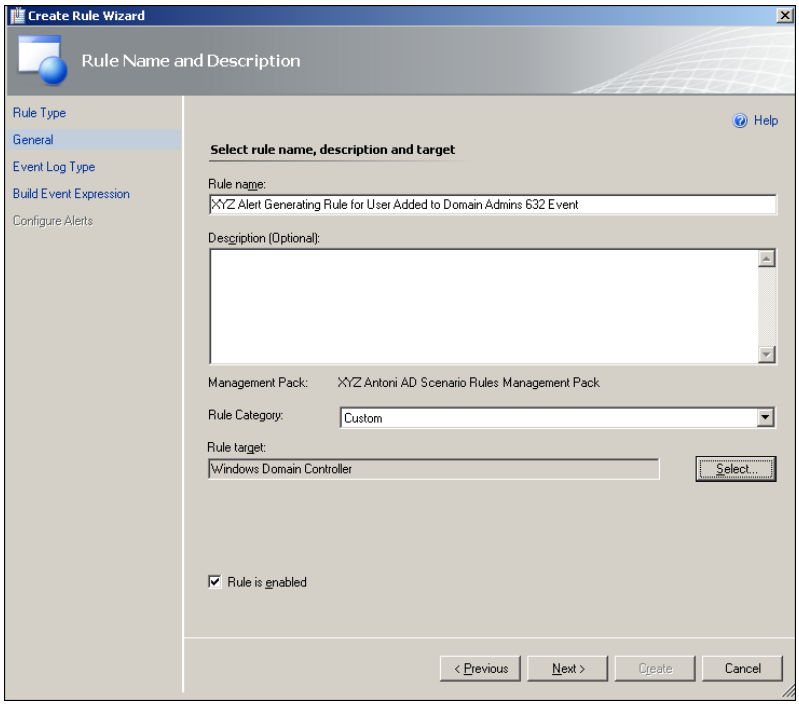
NOTE: Because the 632 event will only occur on domain controllers, it is appropriate to target the rule to the Windows domain controller object. If the event could occur on any windows computer, use 'Windows Operating System' as your target. Best practice is to be as specific as possible.

NOTE: Start typing the name of the object desired in the 'Look For' box to narrow the list down, and If the object you're after is not available, click the 'View all targets' radio button.



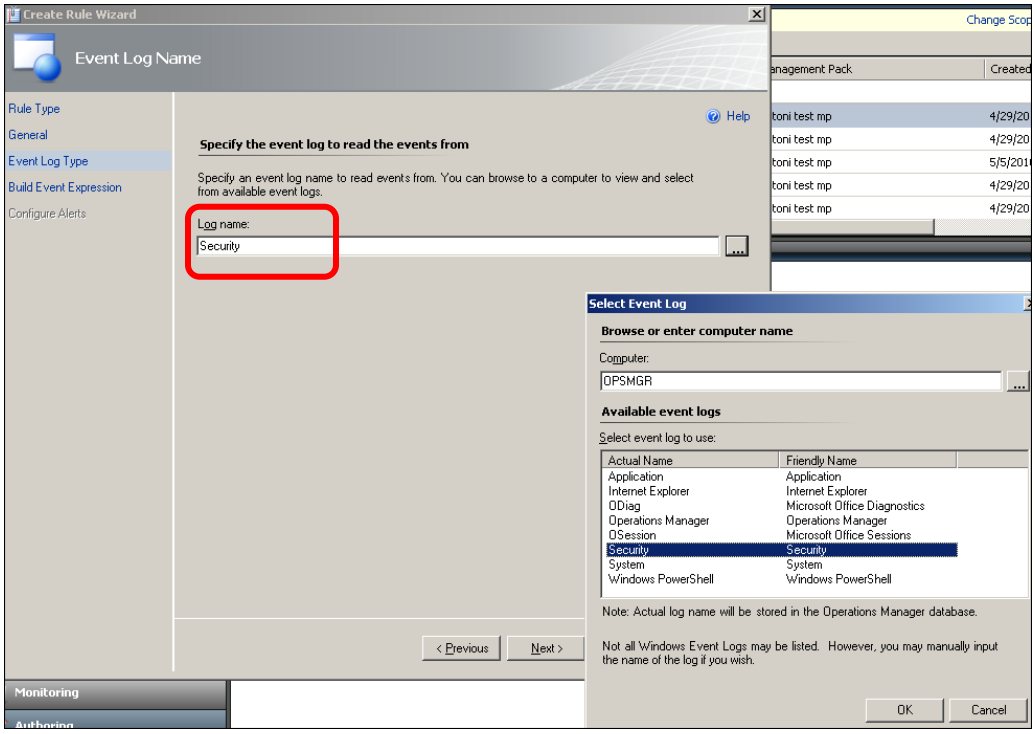
10) Leave the defaults of 'Custom' as the Category, 'Rule is enabled' checked and then click Next

NOTE: By leaving the Rule enabled, the rule will become active on every instance of the object you target the rule to (e.g. every windows computer / every windows domain controller depending on the object that you target). To target a specific instance or a subset of instanced, uncheck the 'Rule is Enable' box to disable it by default and then following the creation of the rule, Create an Override to enable for an instance or group of instances.



11) In the Event Log Name, type the word Security, or alternatively, click the 3 dots and select the Security Event Log, and click Next.

NOTE: This is nothing to do with the targeting. This is purely to make sure you get the name of the event log correct with no typos. The Rule will look in the selected event log on every object targeted (e.g. every windows computer or domain controller) that has the selected event log.



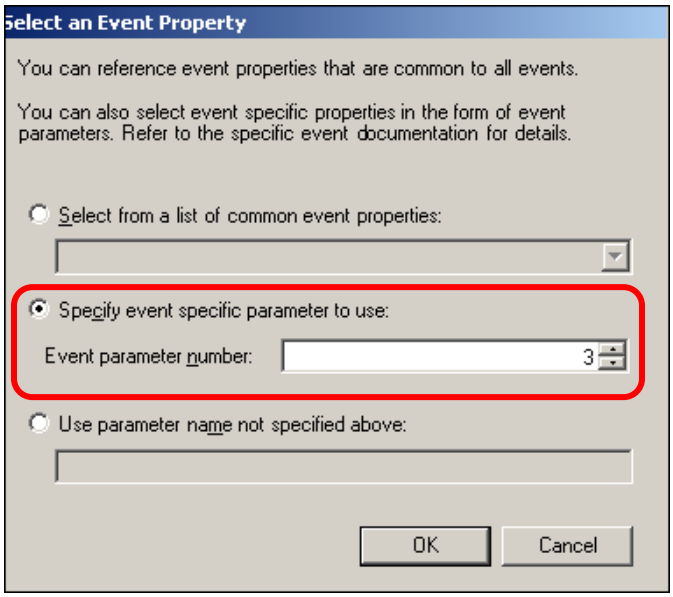
12) In the Value box on the Event ID line, type 632

NOTE: If you wish to monitor for a separate Event, simply specify the alternative Event ID here.

13) Click the grey cell next to Event Source (the second line) and click the Delete button in the UI

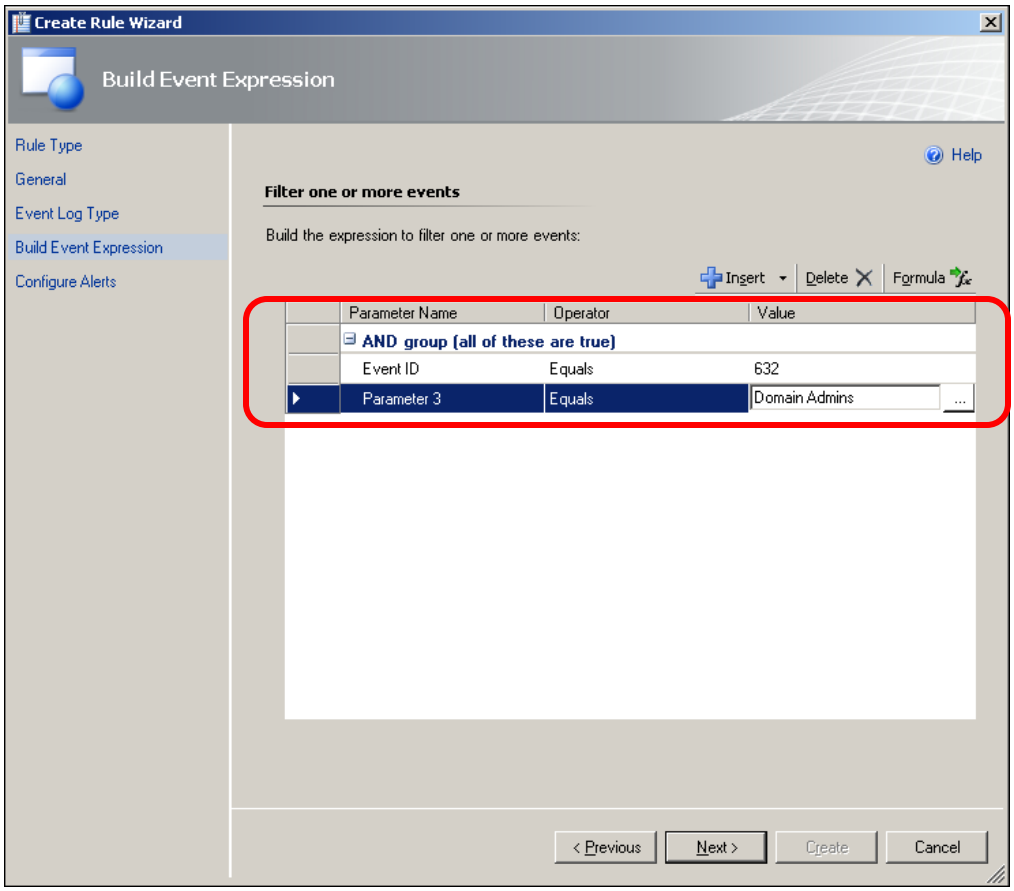
14) Click the Insert button (the main button not the drop-down section of it) and then click the 3 dots on the new line that appears

15) In the 'Select an Event Property' dialog' chose 'Specify event specific parameter to use' and change the value from 1 to 3 and click ok:



16) In the operator field on the second line choose Equals

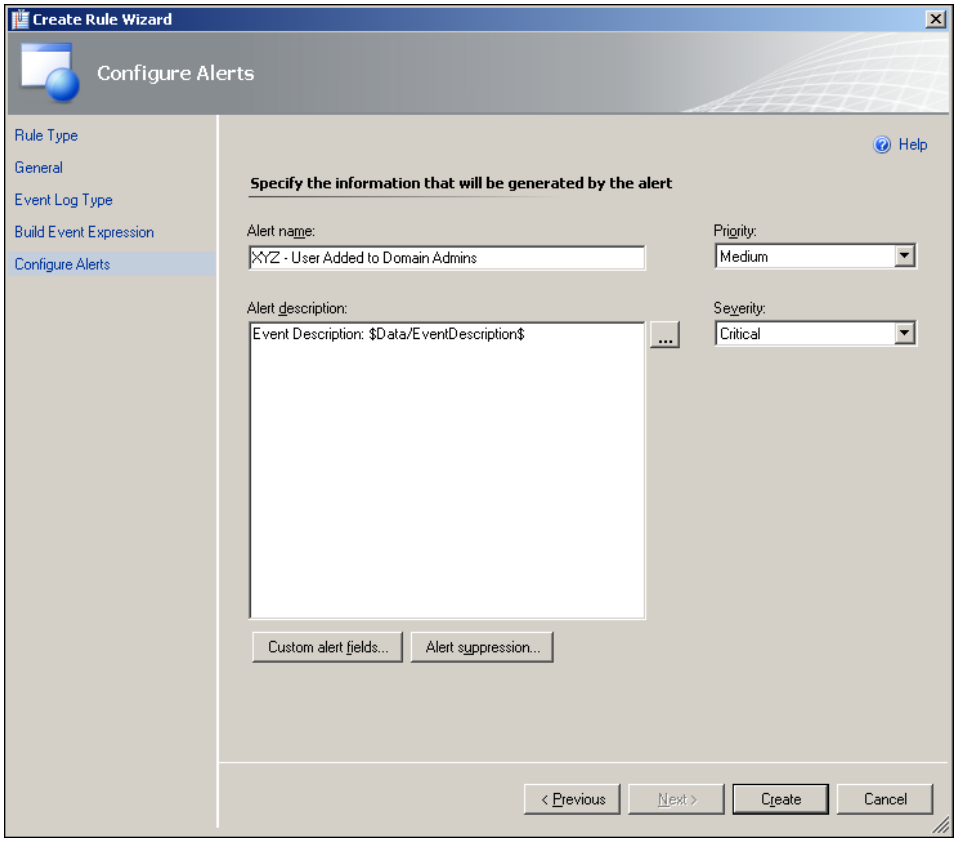
17) In the value field on the second line, type Domain Admins (Case-sensitive):



NOTE: For monitoring users added to a group other than Domain Admins, simply type the Alternative Group name in place of Domain Admins. As well as Equals, other operators such as 'contains substring' or 'Matches Regular Expression' are available.

18) Click next.

19) In Alert name either leave the rule name as the default (the rule name), or change this to a more meaningful string such as 'XYZ - User Added to Domain Admins'



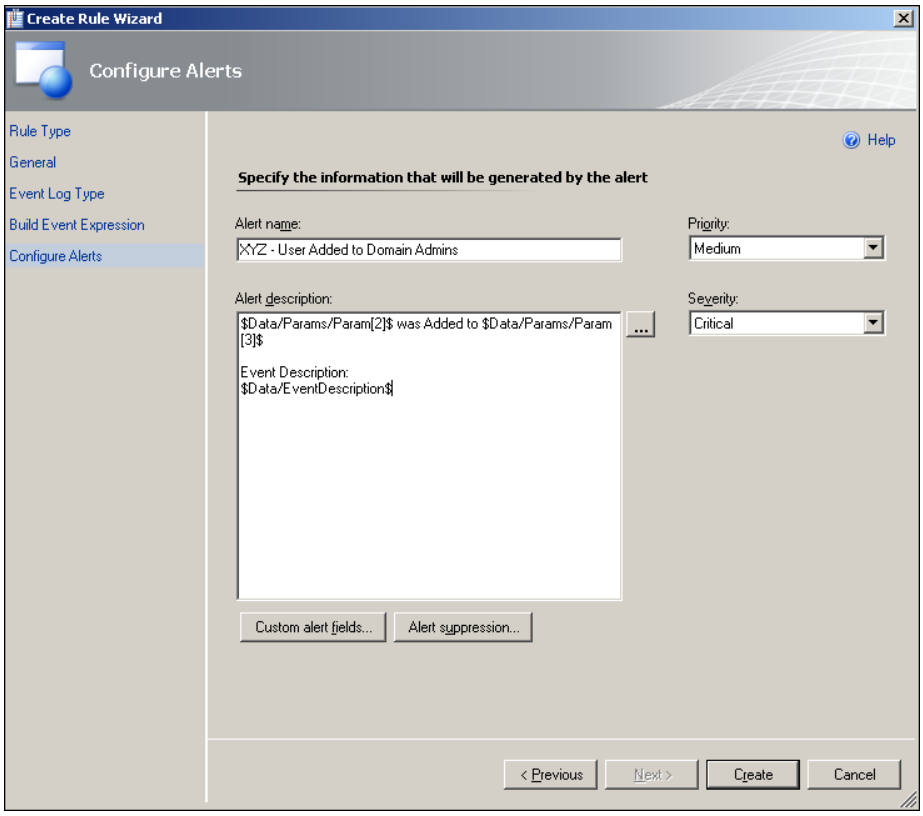
NOTE: the next step is optional. By default, only the contents of the event description will be displayed. Following the optional step below will deliver a more meaningful phrase at the top of the alert description:

Optional Step) In Alert description, click at the start of the box (before Event description) and type $Data/Params/Param[2]$ Was Added to $Data/Params/Param[3]$

and the result should look like this:

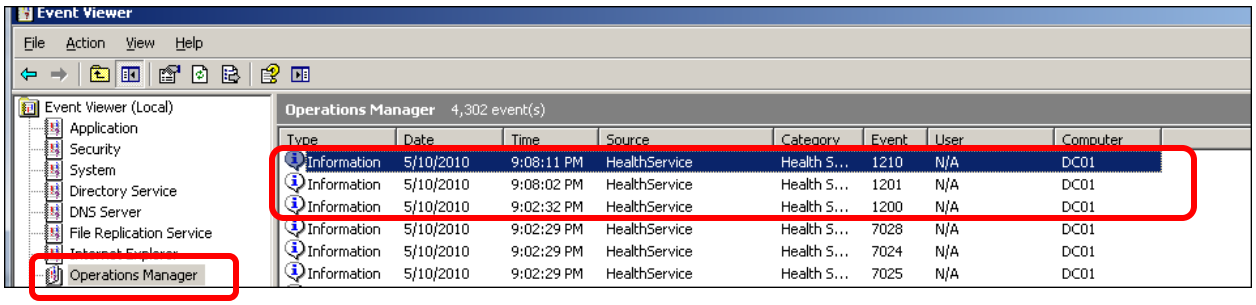
$Data/Params/Param[2]$ Was Added to $Data/Params/Param[3]$

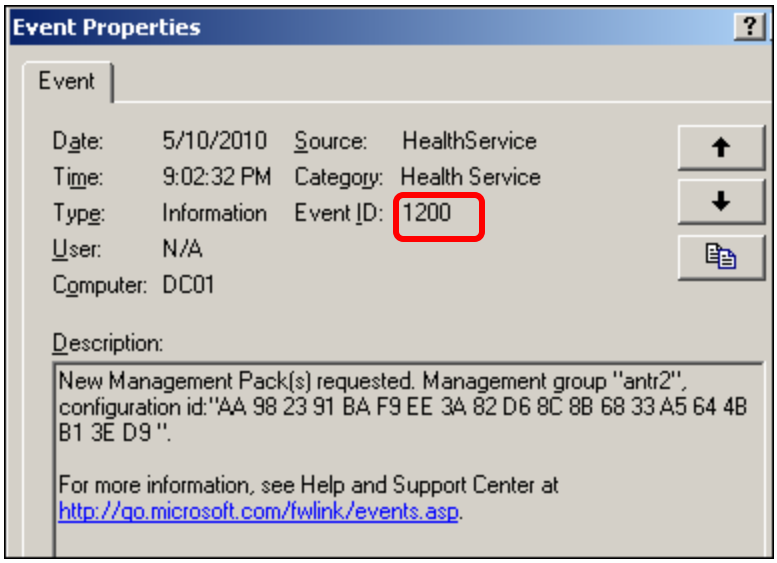
Event Description: $Data/EventDescription$

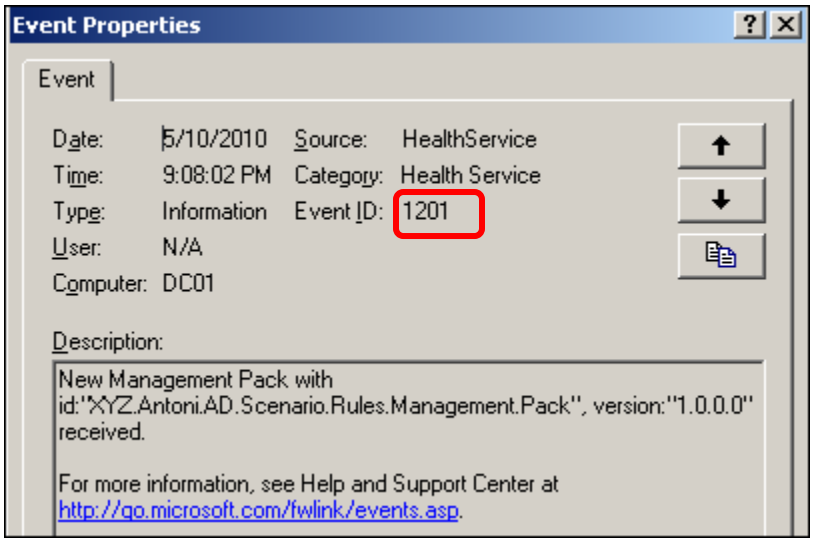


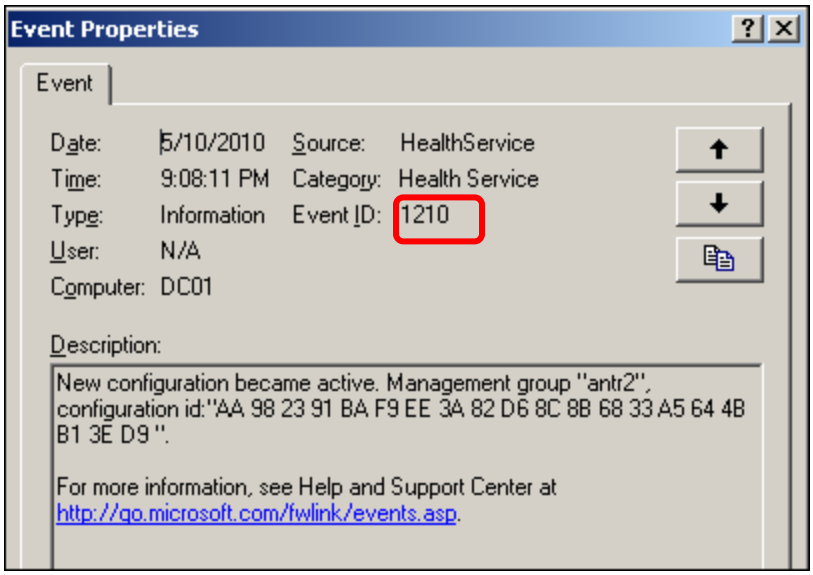
20) Change the Priority and Severity if desired, and click Create.

NOTE: Before testing the rule by adding a user to Domain Admins, ensure that the series of 1200, 1201 and 1210 events is observed in the operations manager event log on the Windows Domain Controller that you are monitoring

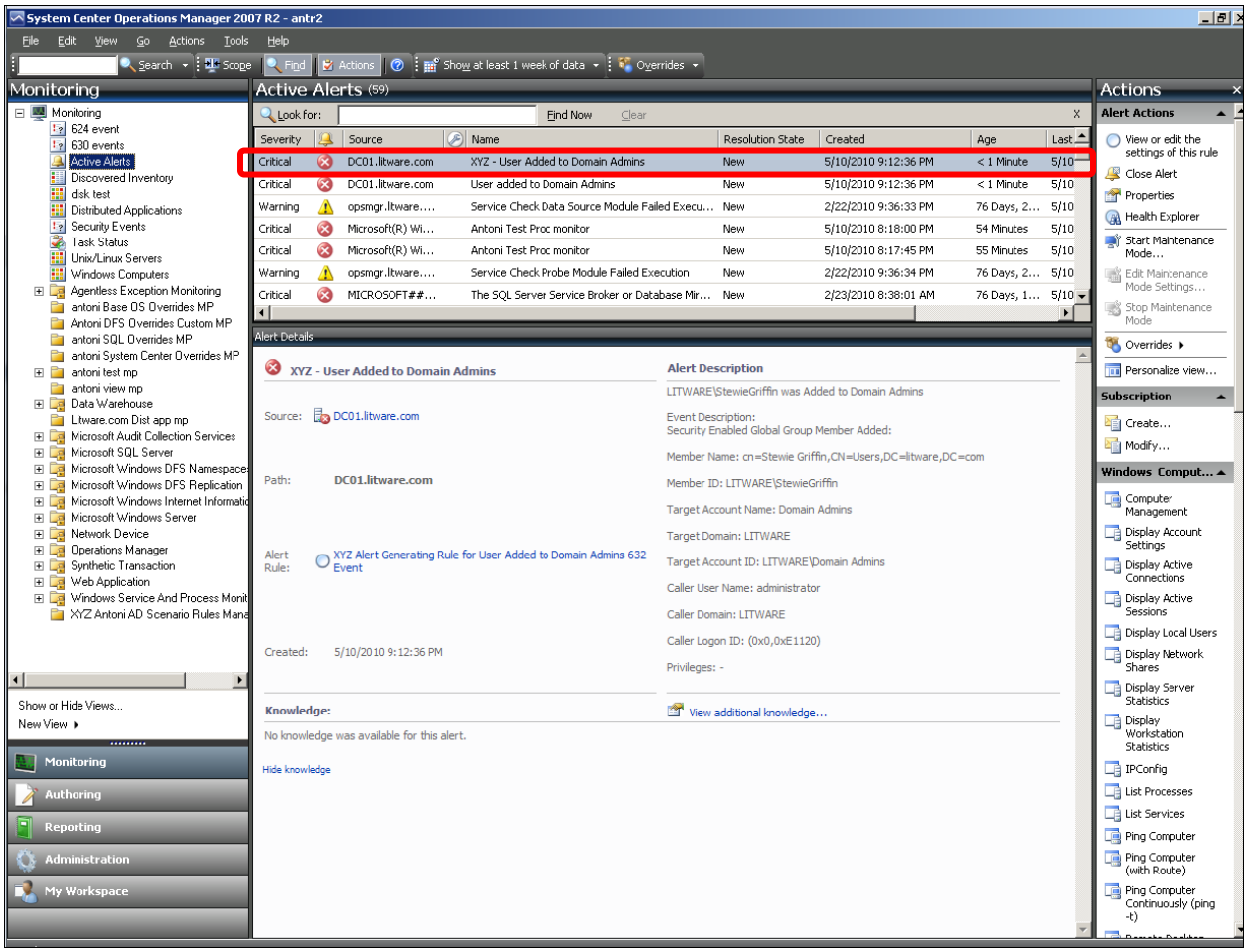



Event Properties
Event
Date: 5/10/2010 Source: HealthService
Time: 9:02:32 PM Category: Health Service
Type: Information Event ID: 1200
User: N/A
Computer: DC01
Description:
New Management Pack(s) requested. Management group "antr2", configuration id:"AA 98 23 91 BA F9 EE 3A 82 D6 8C 8B 68 33 A5 64 4B B1 3E D9 ".
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.


Event Properties
Event
Date: 5/10/2010 Source: HealthService
Time: 9:08:02 PM Category: Health Service
Type: Information Event ID: 1201
User: N/A
Computer: DC01
Description:
New Management Pack with id:"XYZ.Antoni.AD.Scenario.Rules.Management.Pack", version:"1.0.0.0" received.
For more information, see Help and Support Center at http://go.microsoft.com/fwlink/events.asp.



Now, test the rule by adding a user to domain admins on the DC, and you should see a new alert appear in the Monitoring>Active Alerts view of the Operator's console:

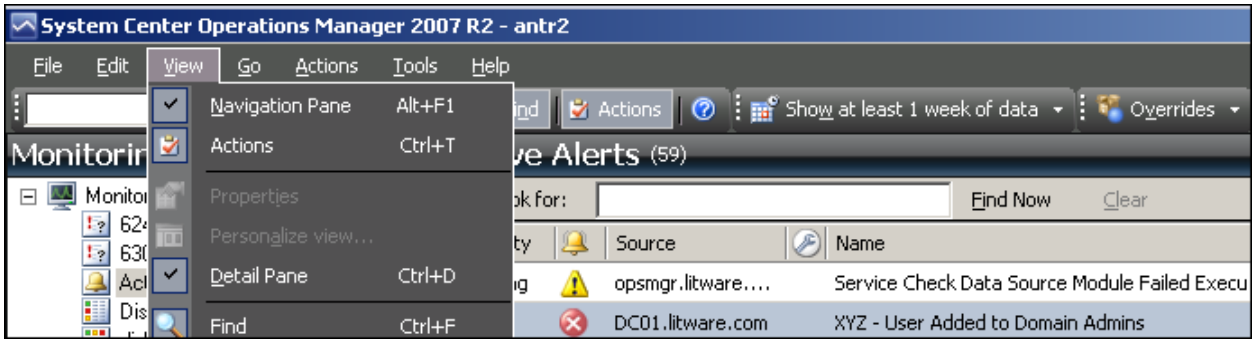


NOTE: Unless any matching subscriptions have been previously created that match the new alert, a notification email will not be sent out. In order to be notified by email when this happens, use the following steps in the next section:

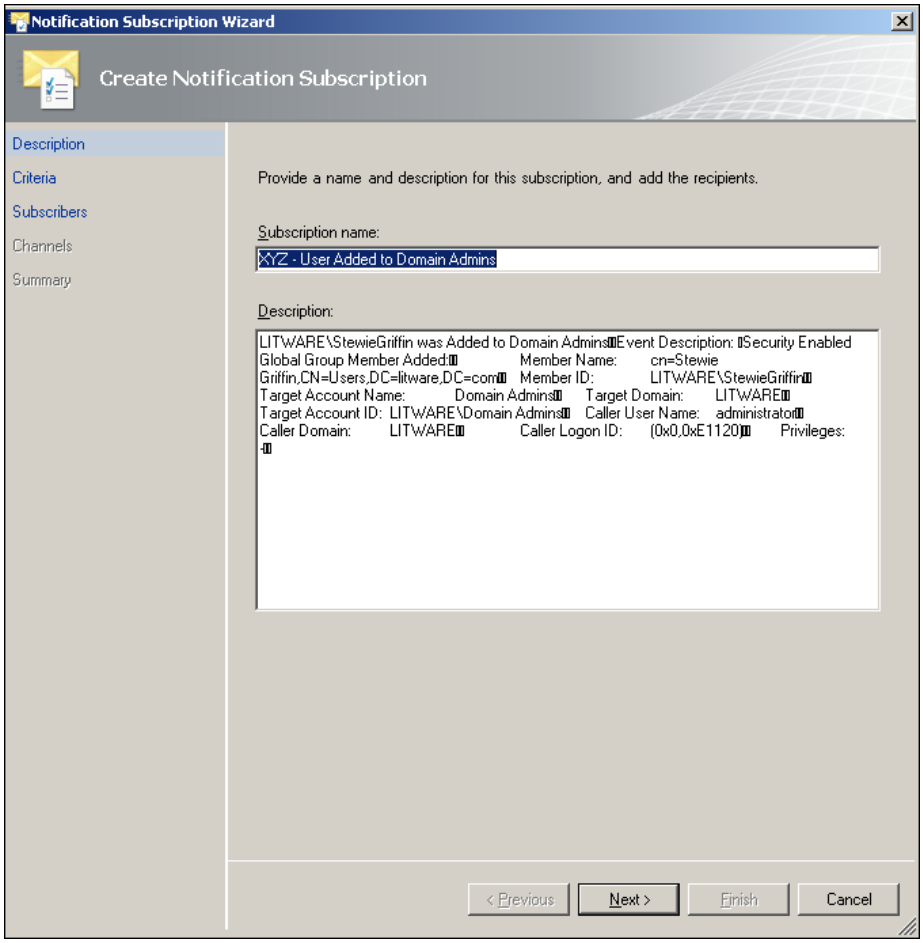
How do I create a Subscription which will notify when a given alert occurs.

1) With the Alert Selected, on the right-hand side in the Actions pane, hit the Create hyperlink underneath subscription:

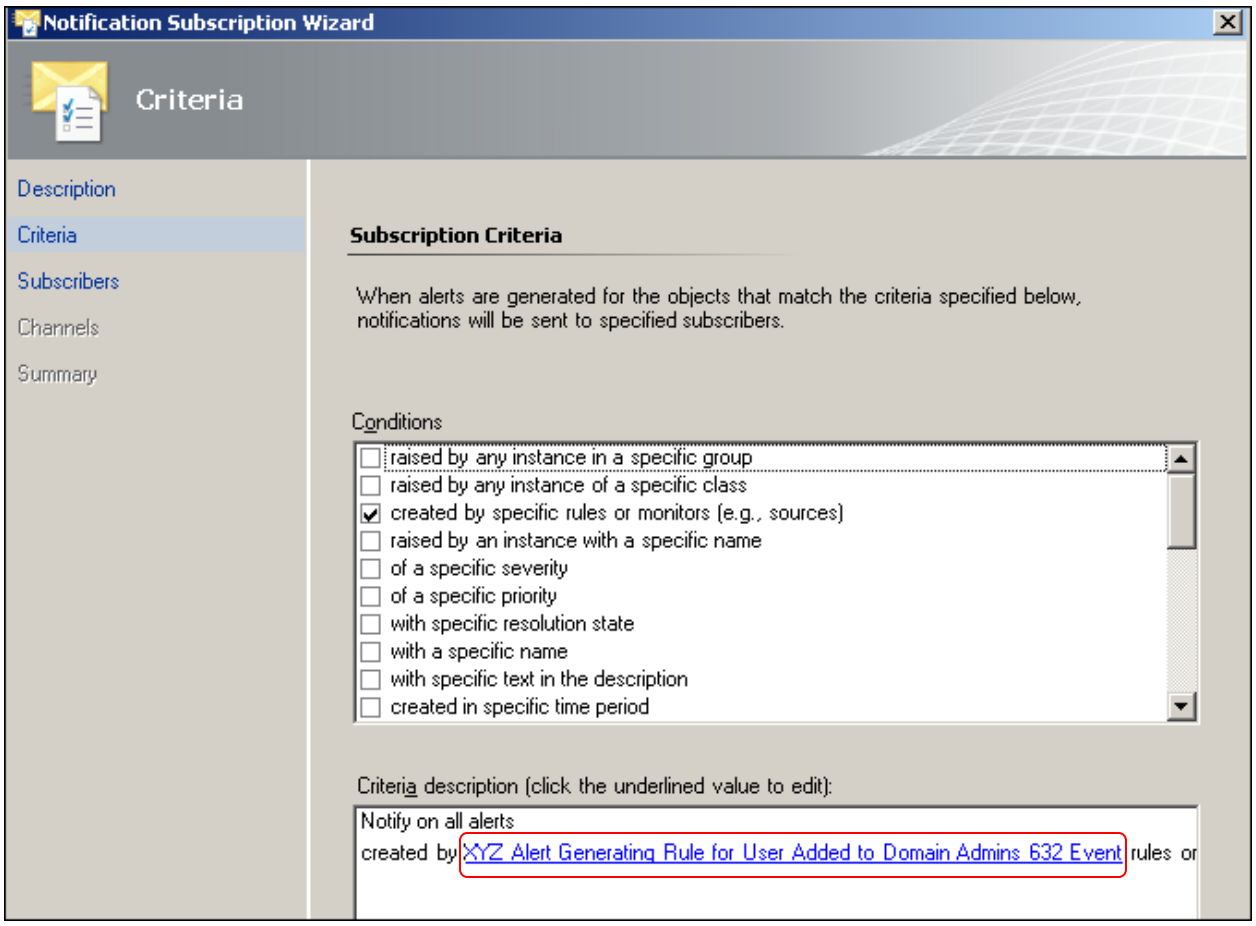
NOTE: If the Actions Pane is not visible, use the View>Actions Pull-down menu to make it visible:



2) Optionally, rename the Subscription Name and the Description or leave the defaults and click Next:

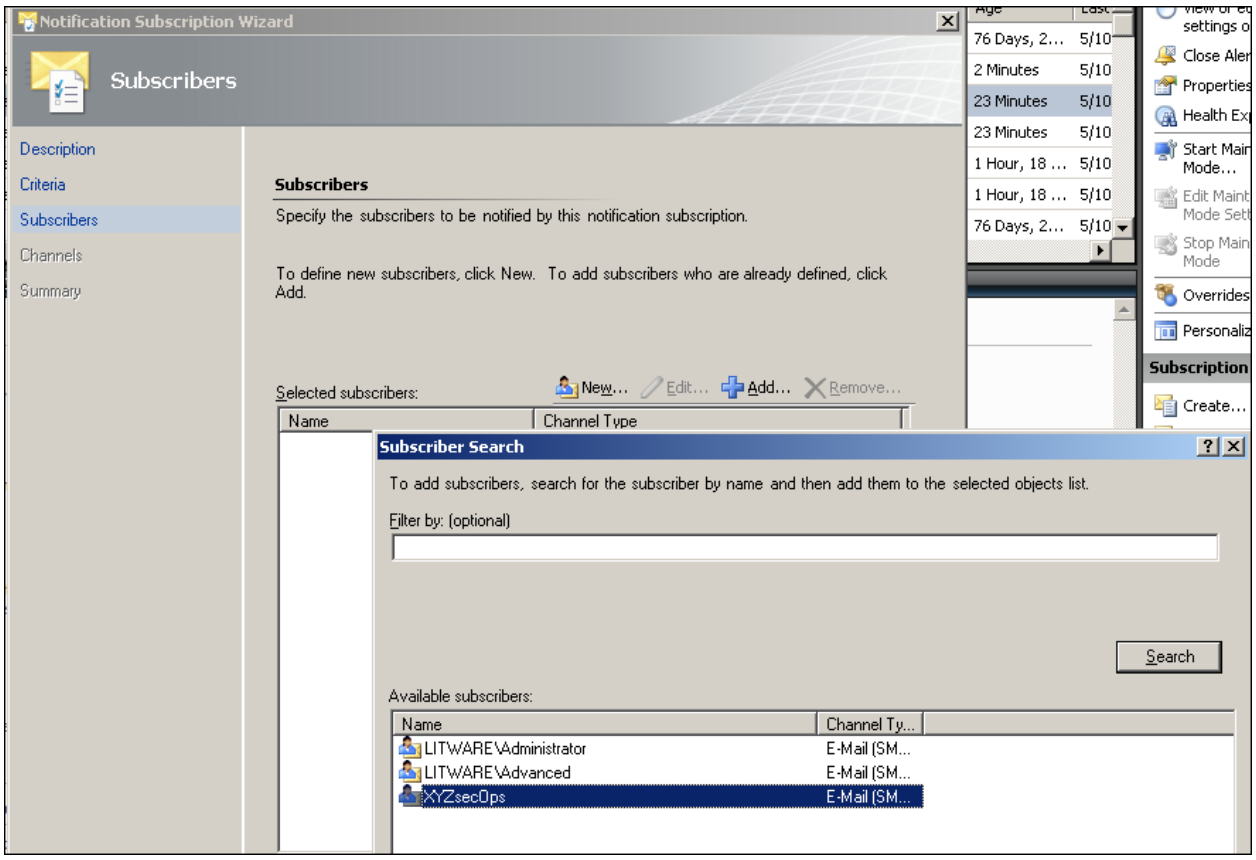


3) In criteria, leave the defaults selected and click Next:



NOTE: By clicking the hyperlink, alerts from other rules and monitors can be picked and added to the subscription.

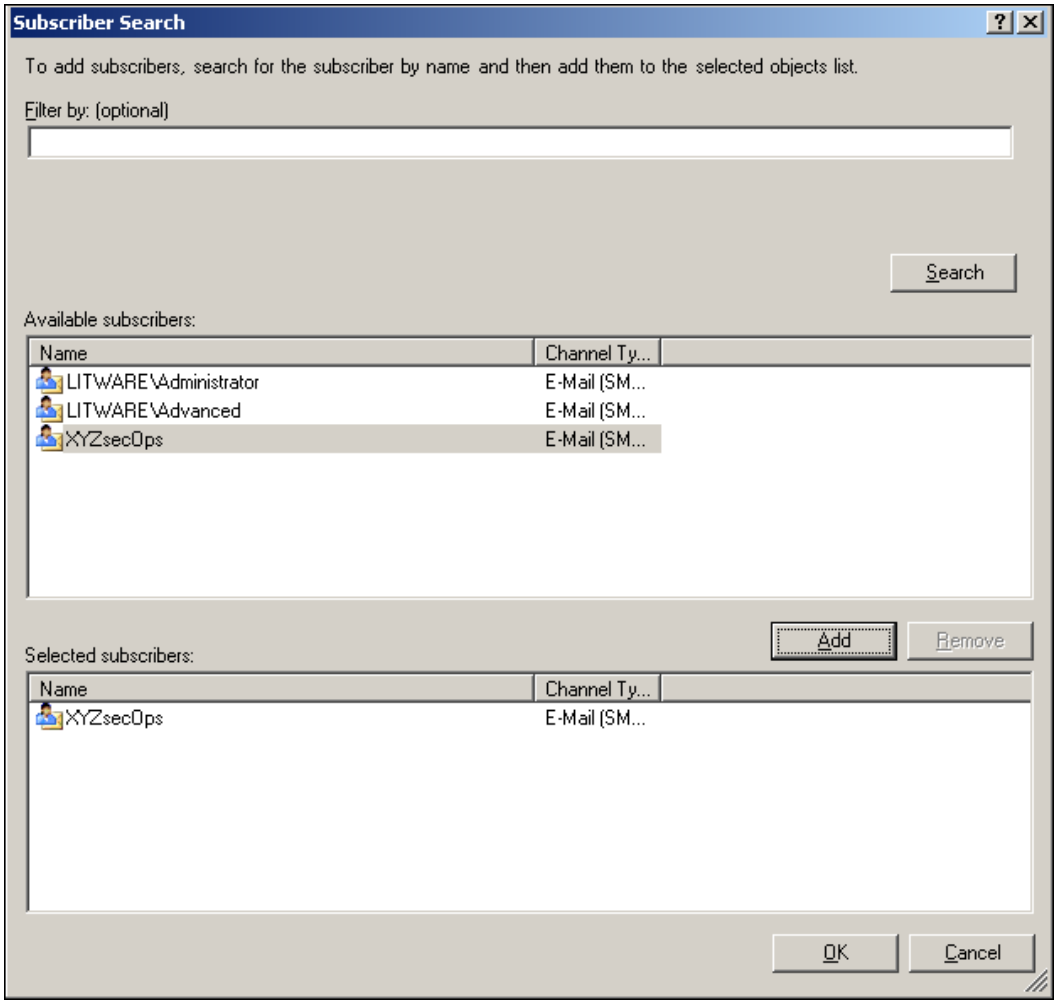
4) In the subscribers Dialog, Click Add, then click the Search button to find the available subscribers:



NOTE: If the subscriber you need is not listed, you will need to use the 'New' button in the previous dialog to create an appropriate subscriber with the desired email address.

NOTE: It is best practice to use predefined Distribution Lists as Subscribers and specify the DL in Operations manager as the deliver address, rather than specify individual email addresses

5) Click the 'Add button to add the subscriber to the list of selected subscribers and click OK:

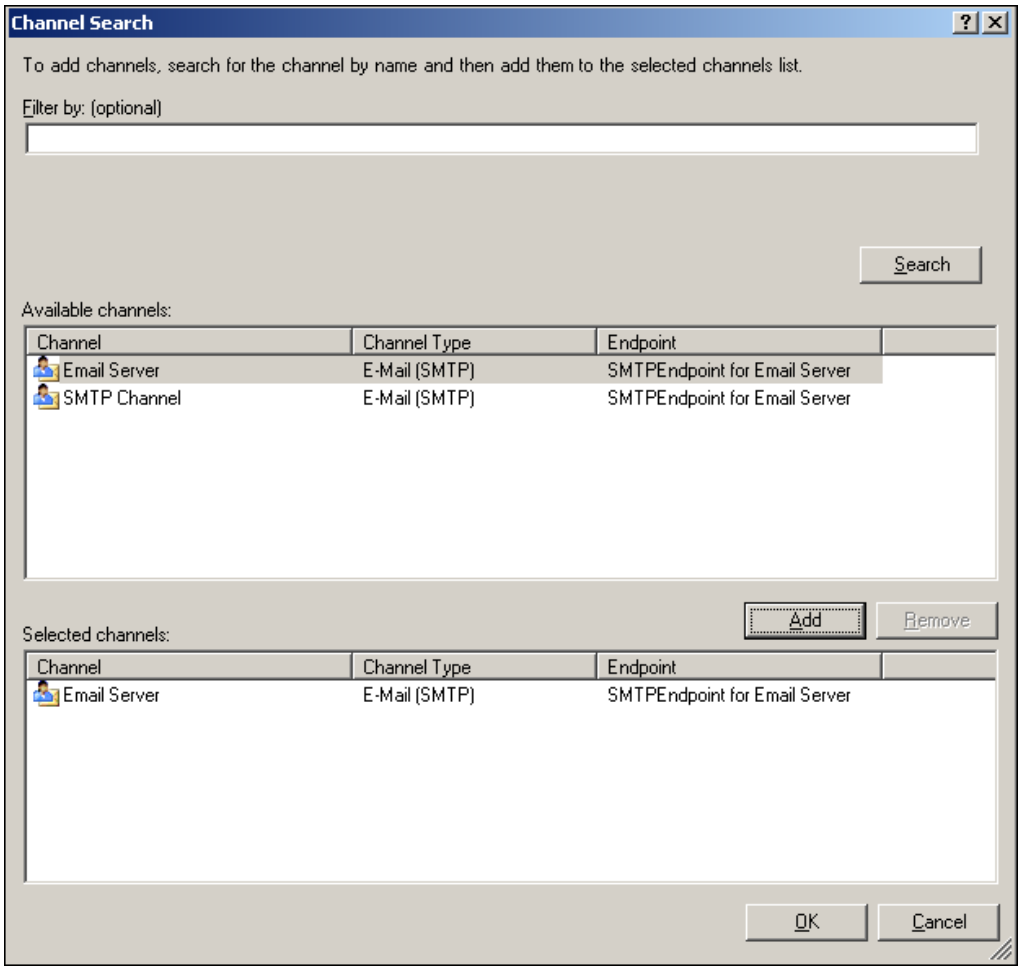


6) In the Subscribers Dialog click Next

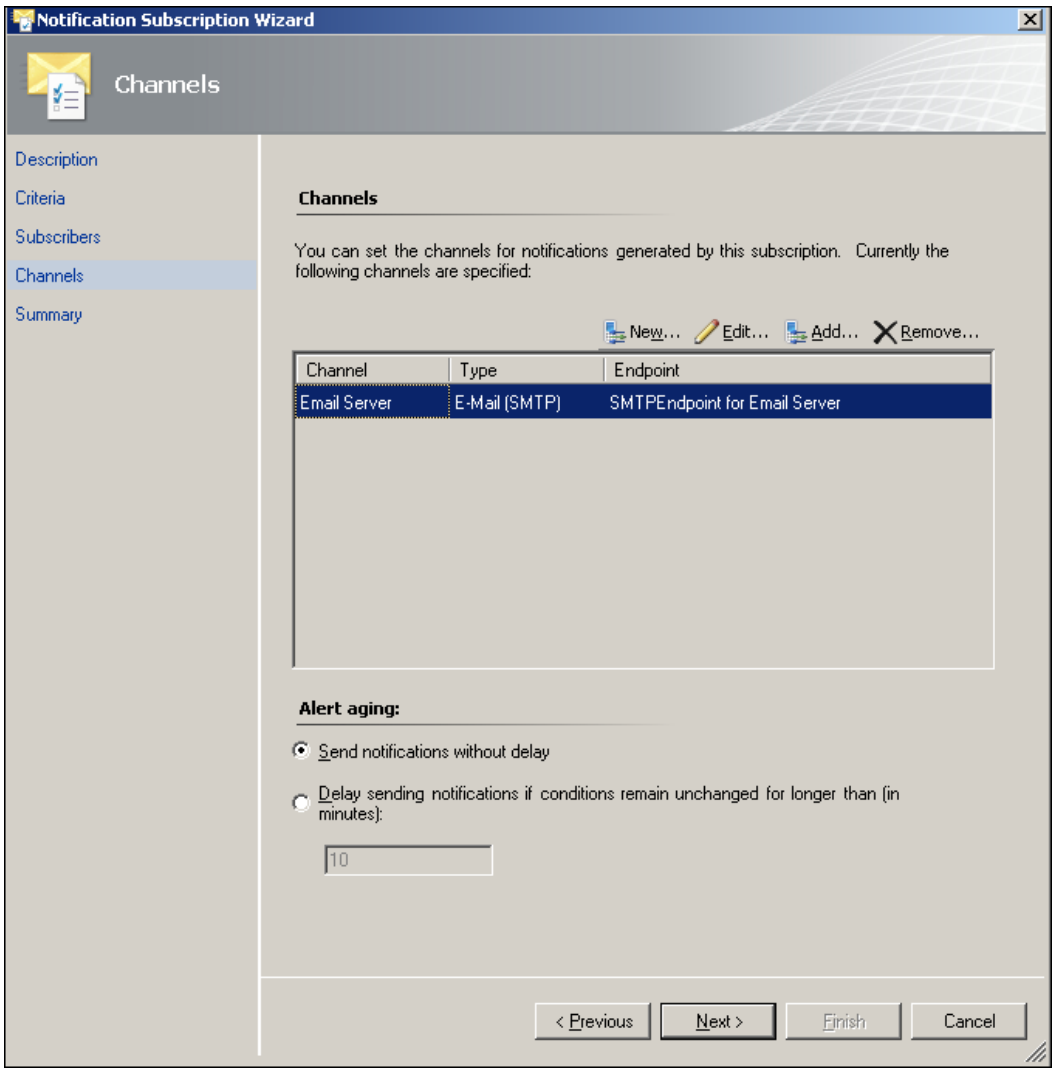
7) In the Channels dialog, click Add

8) In the Channel Search Dialog, click Search

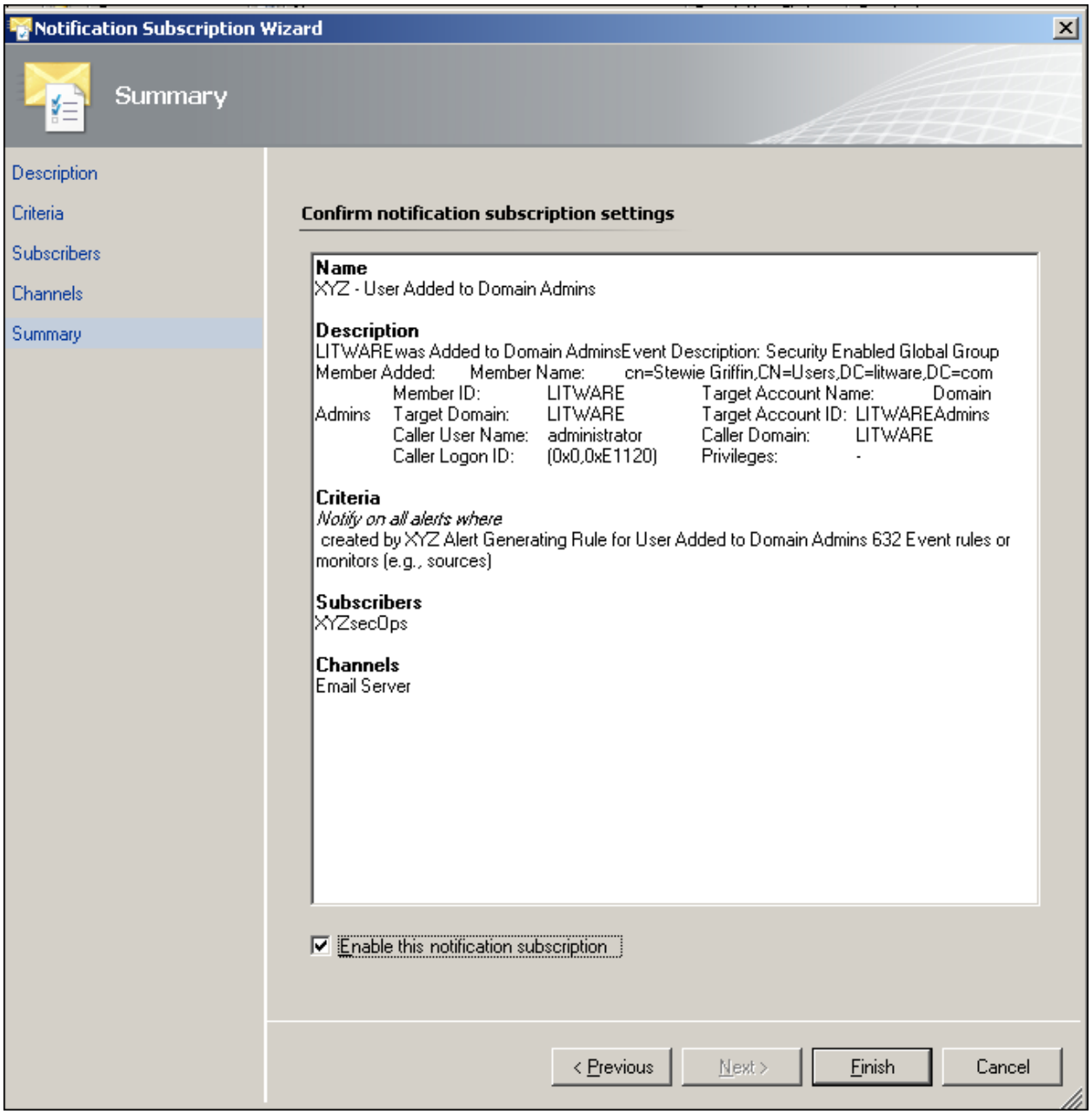
9) Select the Email Server, click Add, and click OK:



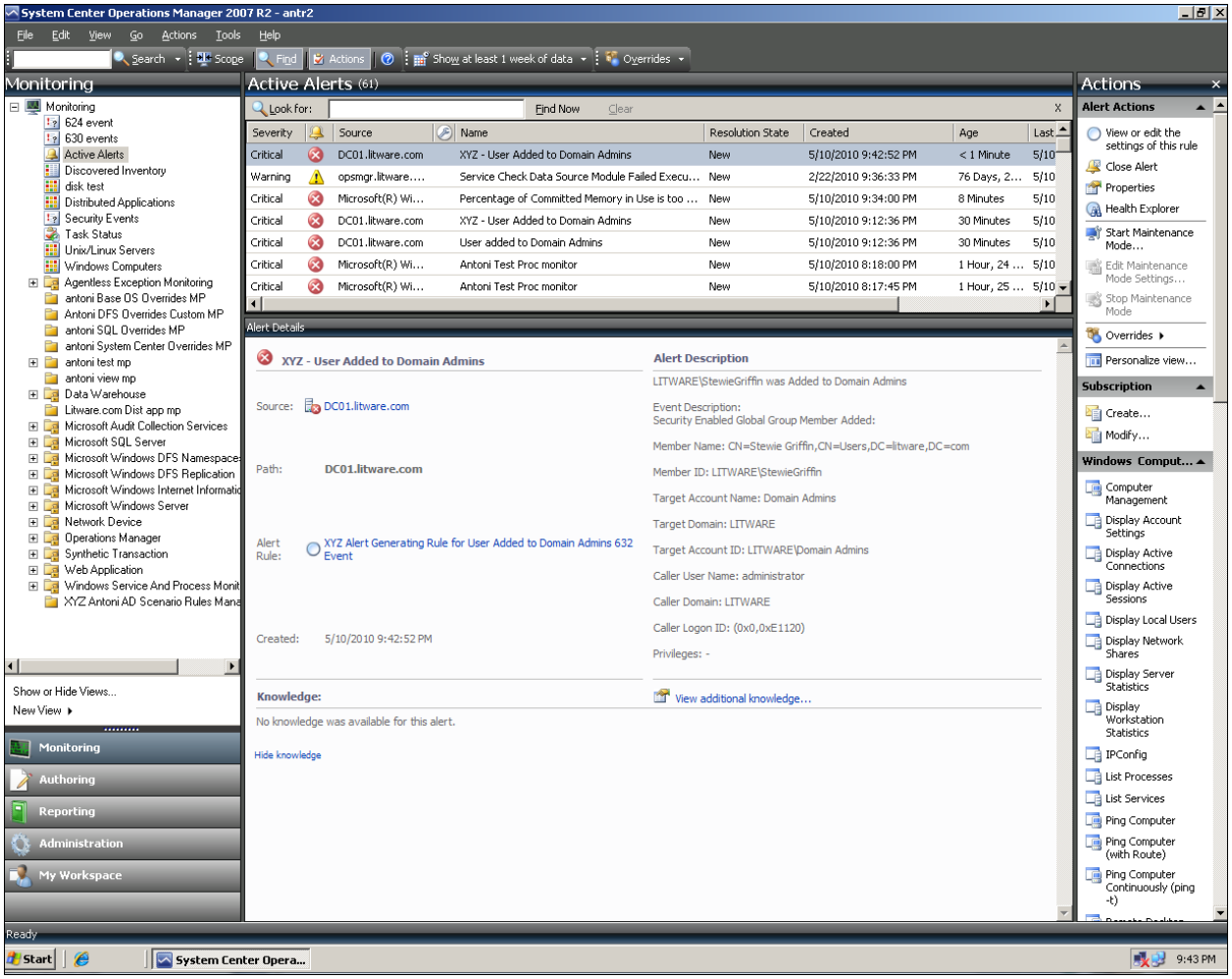
10) Leave the default setting of 'Send Notifications without delay' selected and click Next:



11) Review the Summary, leave the checkbox enabled and click Finish:



12) Test the Rule again, and this time in addition to seeing the alert in the Active Alerts View of the console, the selected subscriber should also receive an email similar to the one shown below:


System Center Operations Manager 2007 R2 - antr2
File Edit View Go Actions Tools Help
Search Scope Find Actions Show at least 1 week of data Overrides
Monitoring
Monitoring
624 event
630 events
Active Alerts
Discovered Inventory
disk test
Distributed Applications
Security Events
Task Status
Unix/Linux Servers
Windows Computers
Agentless Exception Monitoring
antoni Base OS Overrides MP
Antoni DFS Overrides Custom MP
antoni SQL Overrides MP
antoni System Center Overrides MP
antoni test mp
antoni view mp
Data Warehouse
Litware.com Dist app mp
Microsoft Audit Collection Services
Microsoft SQL Server
Microsoft Windows DFS Namespace
Microsoft Windows DFS Replication
Microsoft Windows Internet Informatic
Microsoft Windows Server
Network Device
Operations Manager
Synthetic Transaction
Web Application
Windows Service And Process Monit
XYZ Antoni AD Scenario Rules Mana
Show or Hide Views...
New View
Monitoring
Authoring
Reporting
Administration
My Workspace
Active Alerts (61)
Look for: Find Now Clear
Severity Source Name Resolution State Created Age Last
Critical DC01.litware.com XYZ - User Added to Domain Admins New 5/10/2010 9:42:52 PM < 1 Minute 5/10
Warning opsmgr.litware.... Service Check Data Source Module Failed Execu... New 2/22/2010 9:36:33 PM 76 Days, 2... 5/10
Critical Microsoft(R) Wi... Percentage of Committed Memory in Use is too ... New 5/10/2010 9:34:00 PM 8 Minutes 5/10
Critical DC01.litware.com XYZ - User Added to Domain Admins New 5/10/2010 9:12:36 PM 30 Minutes 5/10
Critical DC01.litware.com User added to Domain Admins New 5/10/2010 9:12:36 PM 30 Minutes 5/10
Critical Microsoft(R) Wi... Antoni Test Proc monitor New 5/10/2010 8:18:00 PM 1 Hour, 24 ... 5/10
Critical Microsoft(R) Wi... Antoni Test Proc monitor New 5/10/2010 8:17:45 PM 1 Hour, 25 ... 5/10
Alert Details
XYZ - User Added to Domain Admins
Source: DC01.litware.com
Path: DC01.litware.com
Alert Rule: XYZ Alert Generating Rule for User Added to Domain Admins 632 Event
Created: 5/10/2010 9:42:52 PM
Alert Description
LITWARE\StewieGriffin was Added to Domain Admins
Event Description:
Security Enabled Global Group Member Added:
Member Name: CN=Stewie Griffin,CN=Users,DC=litware,DC=com
Member ID: LITWARE\StewieGriffin
Target Account Name: Domain Admins
Target Domain: LITWARE
Target Account ID: LITWARE\Domain Admins
Caller User Name: administrator
Caller Domain: LITWARE
Caller Logon ID: (0x0,0xE1120)
Privileges: -
Knowledge:
View additional knowledge...
No knowledge was available for this alert.
Hide knowledge
Actions
Alert Actions
View or edit the settings of this rule
Close Alert
Properties
Health Explorer
Start Maintenance Mode...
Edit Maintenance Mode Settings...
Stop Maintenance Mode
Overrides
Personalize view...
Subscription
Create...
Modify...
Windows Comput...
Computer Management
Display Account Settings
Display Active Connections
Display Active Sessions
Display Local Users
Display Network Shares
Display Server Statistics
Display Workstation Statistics
IPConfig
List Processes
List Services
Ping Computer
Ping Computer (with Route)
Ping Computer Continuously (ping -t)
Ready
Start
System Center Opera...
9:43 PM

All Alert: User added to Domain Admins Resolution state: New

OM@litware.com [OM@litware.com]

Sent: Monday, May 10, 2010 9:53 PM

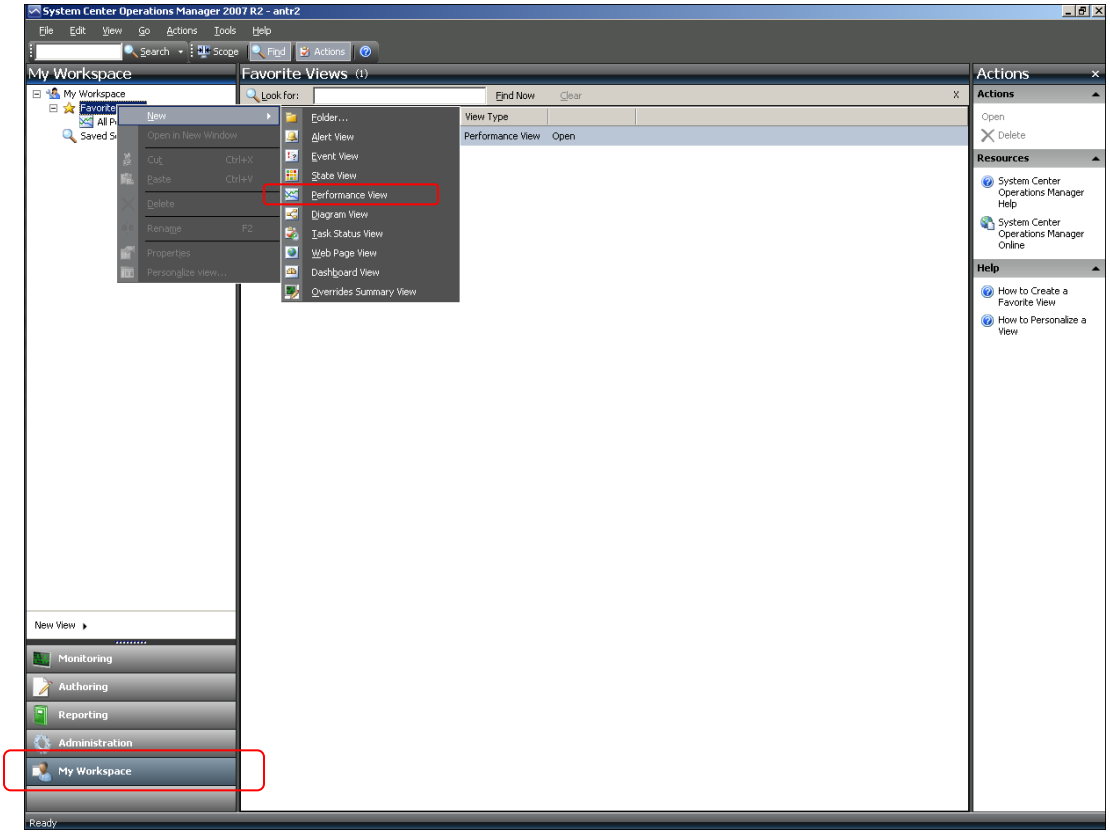
To: Administrator

```
Alert: User added to Domain Admins
Source: DC01.litware.com
Path:
Last modified by: System
Last modified time: 5/10/2010 9:42:58 PM
Alert description: LITWARE\StewieGriffin Was Added to Domain Admins
Event Description: Security Enabled Global Group Member Added:

        Member Name:    CN=Stewie Griffin,CN=Users,DC=litware,DC=com

        Member ID:      LITWARE\StewieGriffin

        Target Account Name:    Domain Admins

        Target Domain:  LITWARE

        Target Account ID:      LITWARE\Domain Admins

        Caller User Name:       administrator

        Caller Domain:  LITWARE

        Caller Logon ID:        (0x0,0xE1120)

        Privileges:     -


Alert view link: "?DisplayMode=Pivot&AlertID=%7bcd92cd2d-549c-4b7b-810f-
57aded5195a8%7d"
Notification subscription ID generating this message: {B51C0F5A-0151-
9799-4827-8DFB5BD340D9}
```

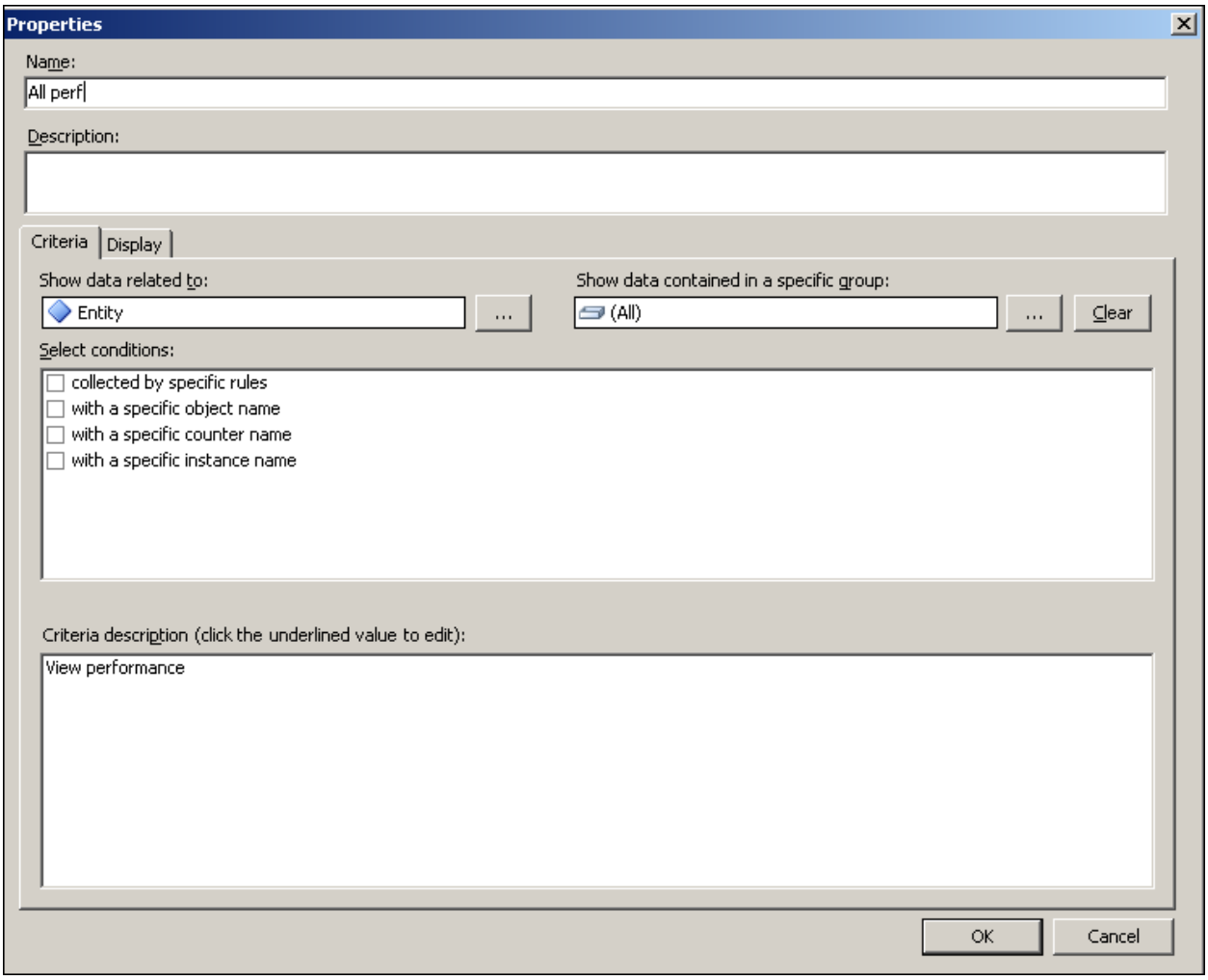
How do I know if OpsMgr is collecting a specific performance counter?

The first thing to determine is whether the performance data you need is already being collected in Operations Manager. The easiest way to do this is to create a view showing all performance counters

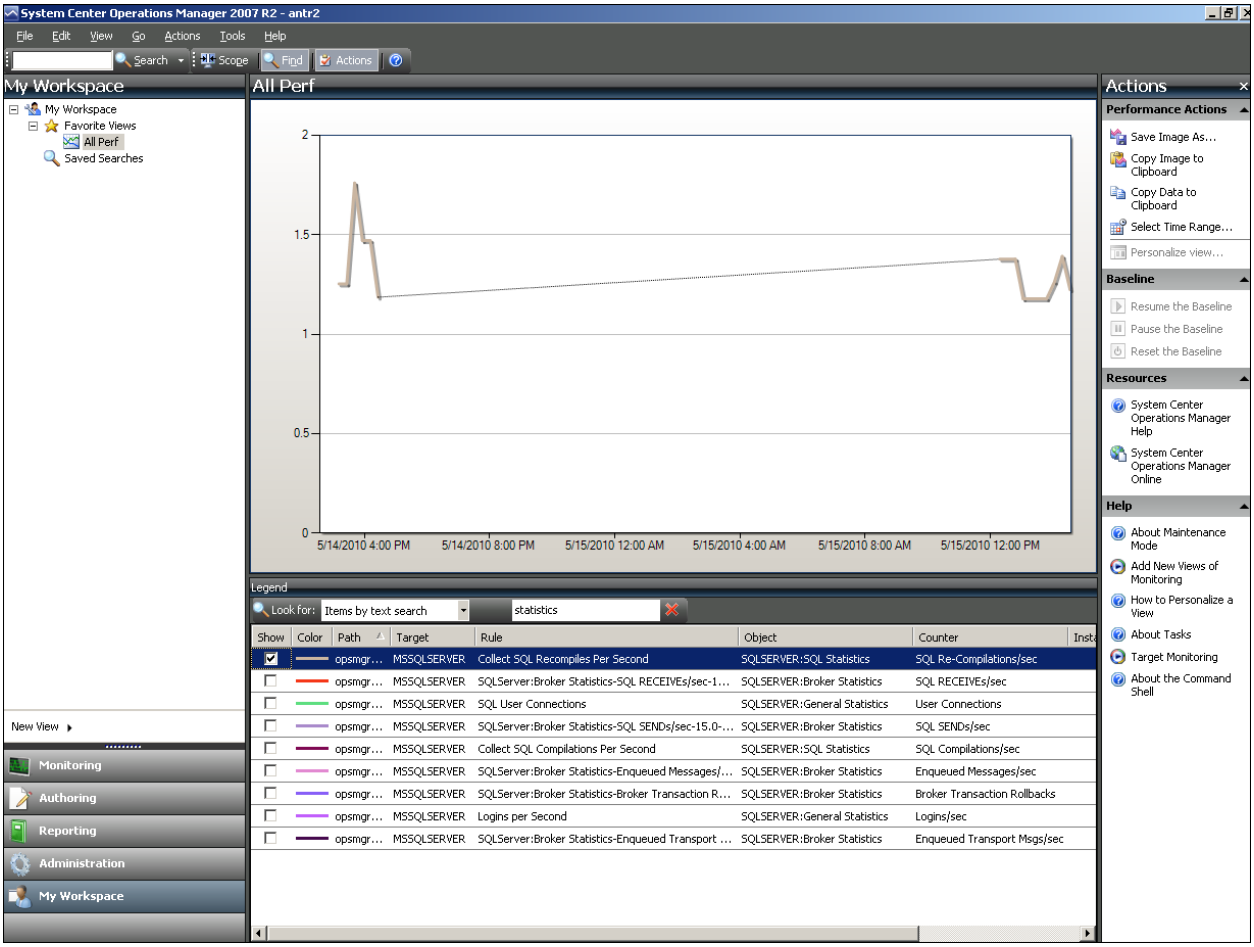
In My Workspace, Right-Click My favorites, choose New>Performance View:



Give it a name such as ‘All perf’, leave all the other default settings, and click ok to create the view:



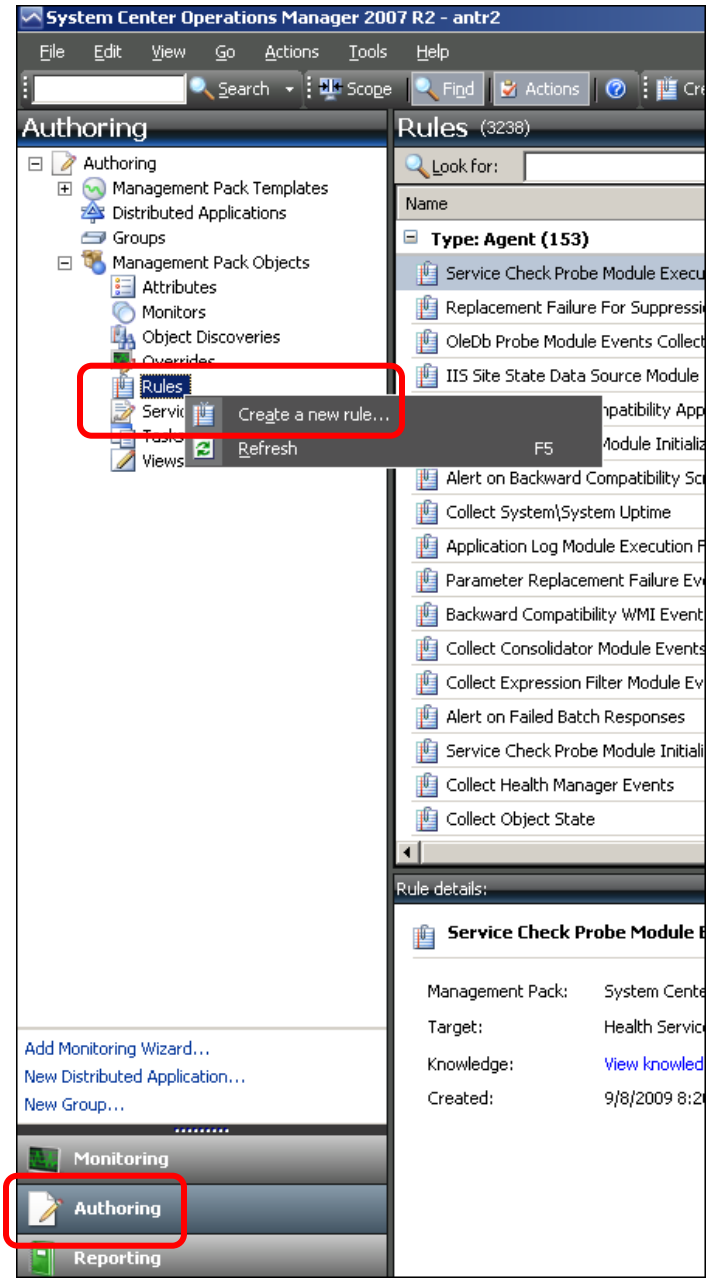
Change the “All Items’ to ‘Items by text Search’ and type part of the performance object or counter that you’re interested in. For this example, we are looking for SQLServer: SQL Statistics\Batch Requests/sec. Typing Statistics into the look for box, returns all counters / objects / rule names that have the word statistics in the title:



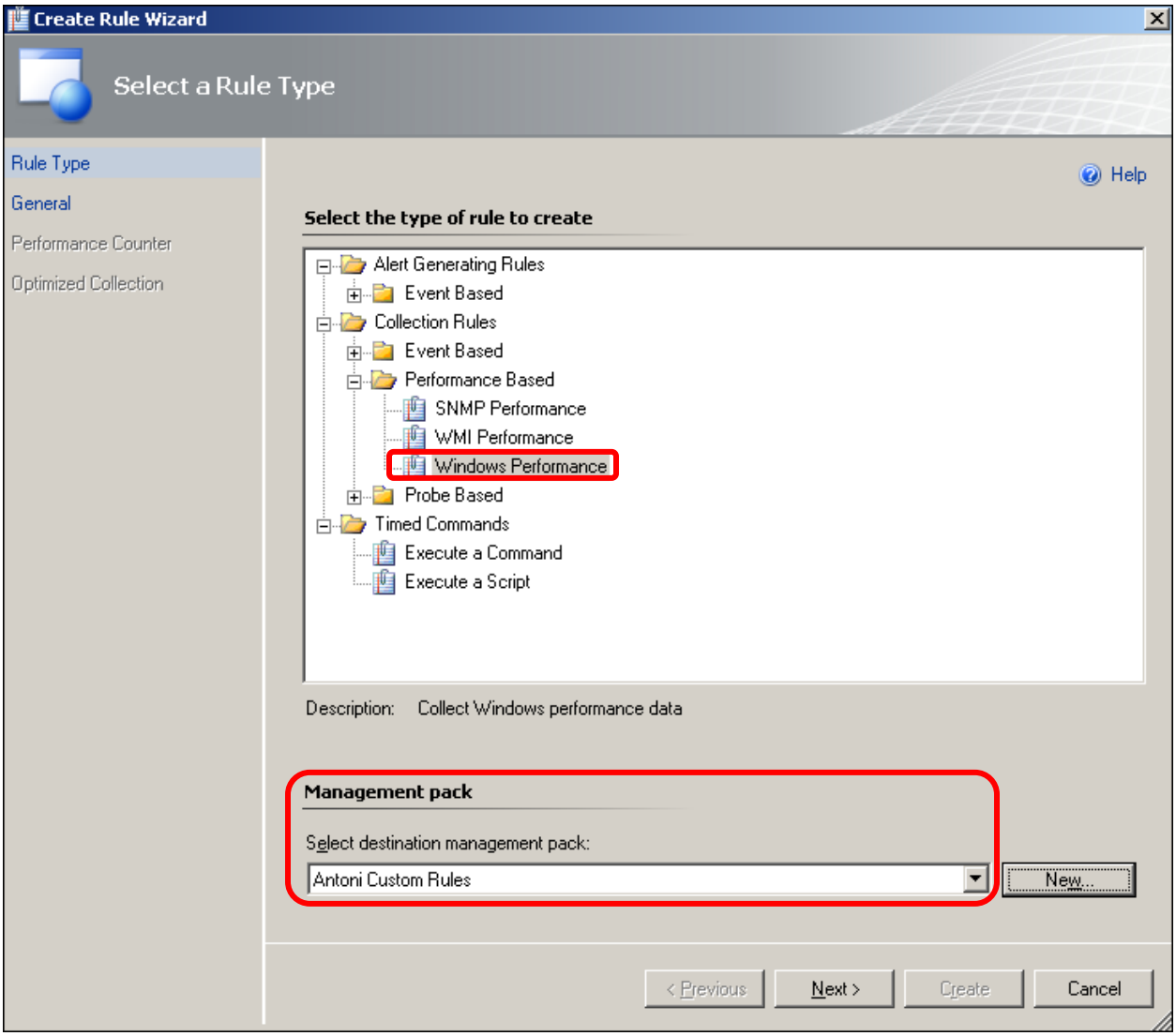
The above view shows that only the only counters collected by default for the SQL Server: SQL Statistics object are SQL Re-Compilations/Sec and SQL Compilations/Sec. This means we need to create a performance collection rule to collect the data that we want to collect and present in the above graph.

How do I create a rule to collect performance data that is not already collected in a management pack, and show it in the graphs in Operations Manager?

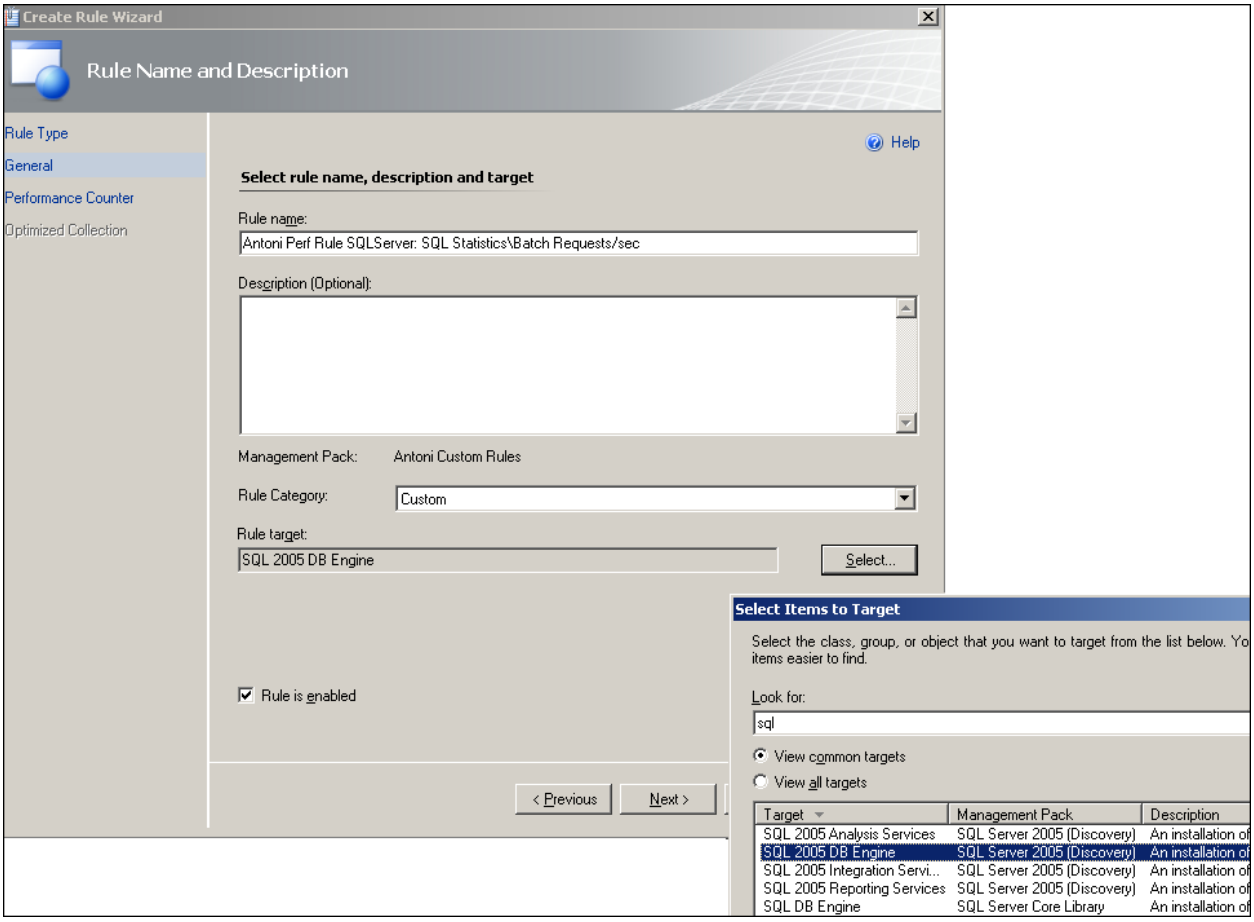
1) Navigate to the 'Authoring' Space of the console. Expand Management Pack Object and right-click Rules and choose 'Create a New Rule'



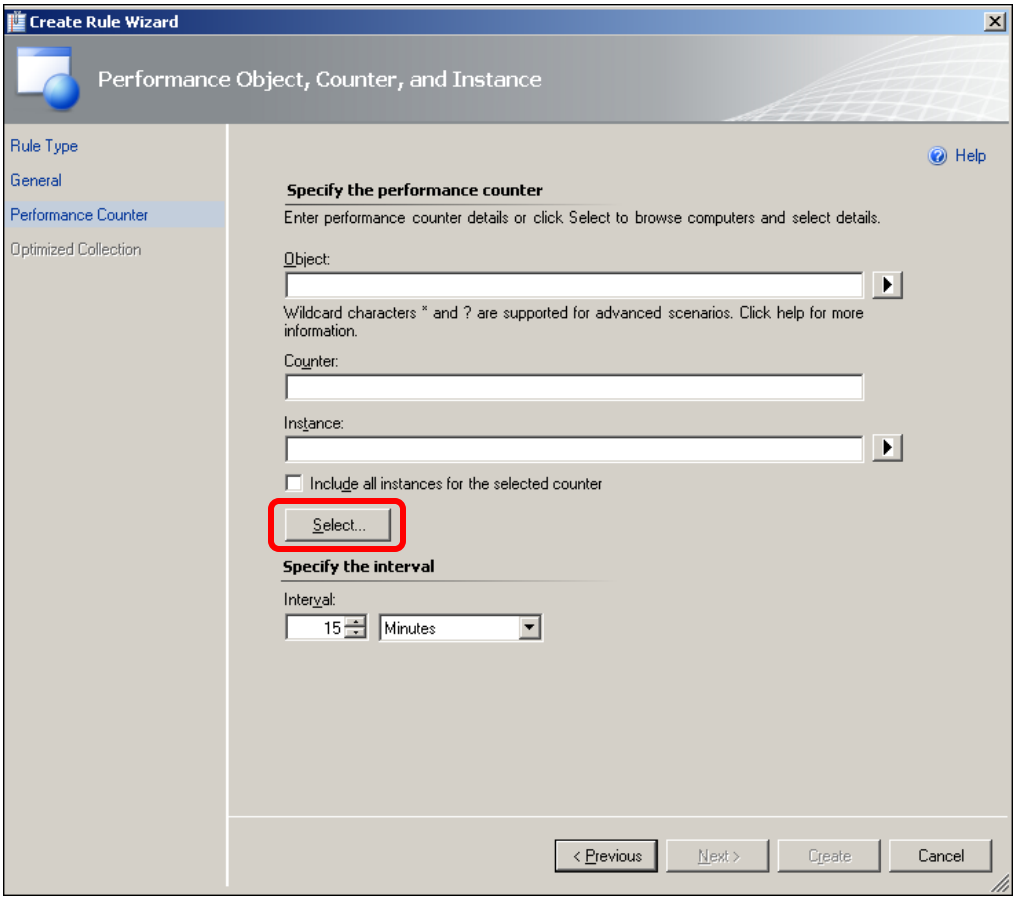
2) Select Collection Rules>Performance Based> Windows Performance, and change the management pack to something other than the Default Management Pack and click Next:



3) Give the rule a name (I recommend using a prefix to the rule name such as a 3-letter acronym of the company name as this makes it easier to find objects such as rules in the console), select a Rule Target that will be present on the computer you want to collect the performance counter from. In this case an appropriate target is SQL 2005 DB Engine, and then click Next:



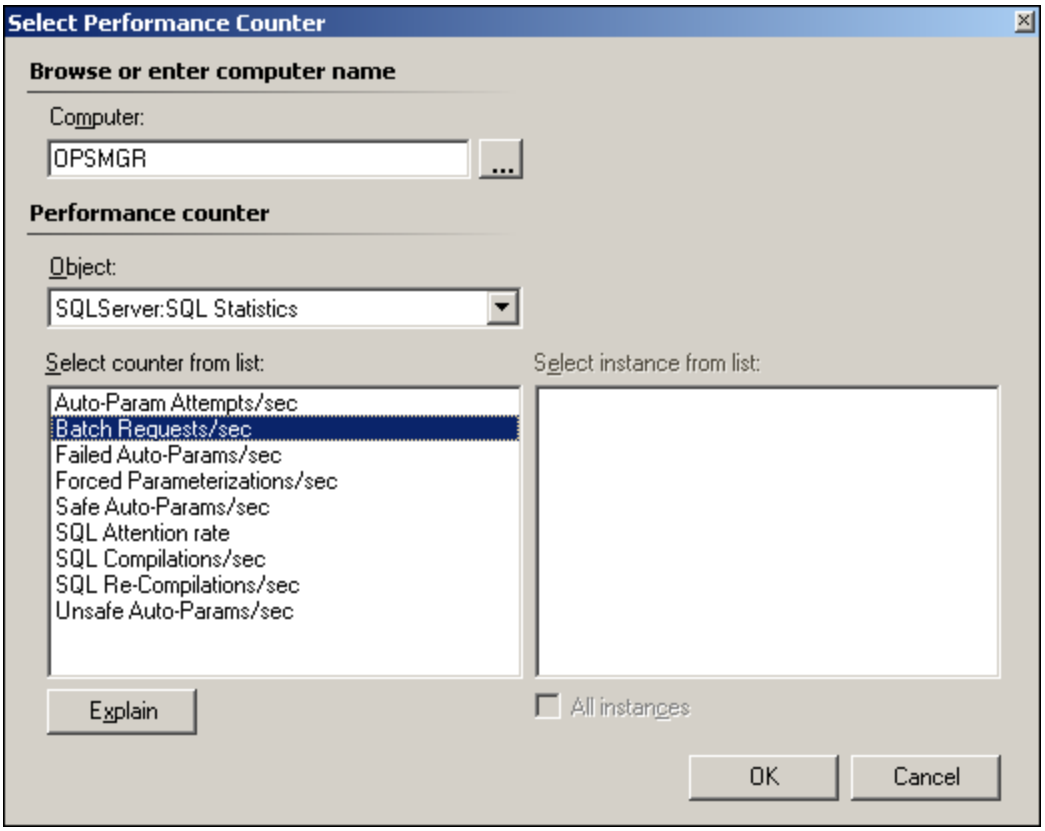
4) In the following dialog, ignore everything else and click the ‘Select’ button;



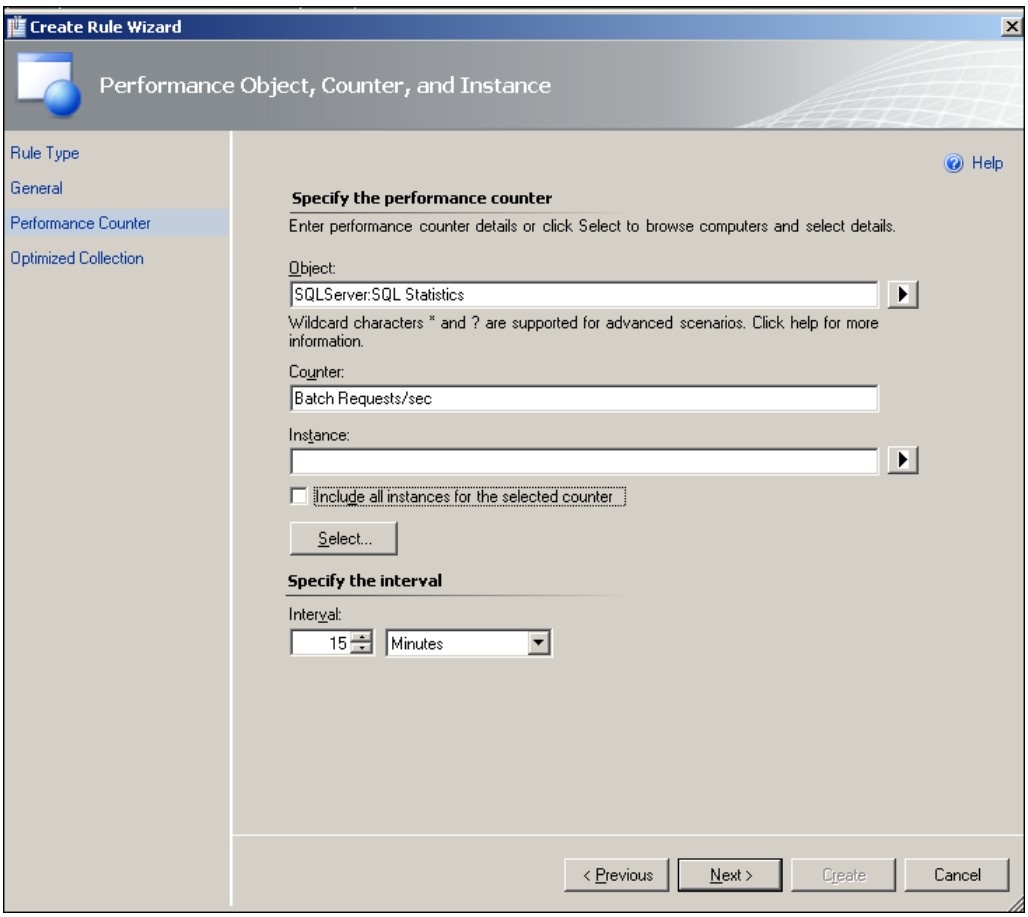
In computer, Browse to a computer that has the performance counter you need to collect and the available object and counters in the list will refresh.

NOTE: This is purely for picking the correct counter. By selecting a computer to pick the counter from, you are not saying 'I just want to target this one computer'. Because in the previous dialogs we selected SQL 2005 DB Engine, the performance counter rule will be activated on every Operations Manager agent where a SQL 2005 DB engine object and the counter picked out is found.

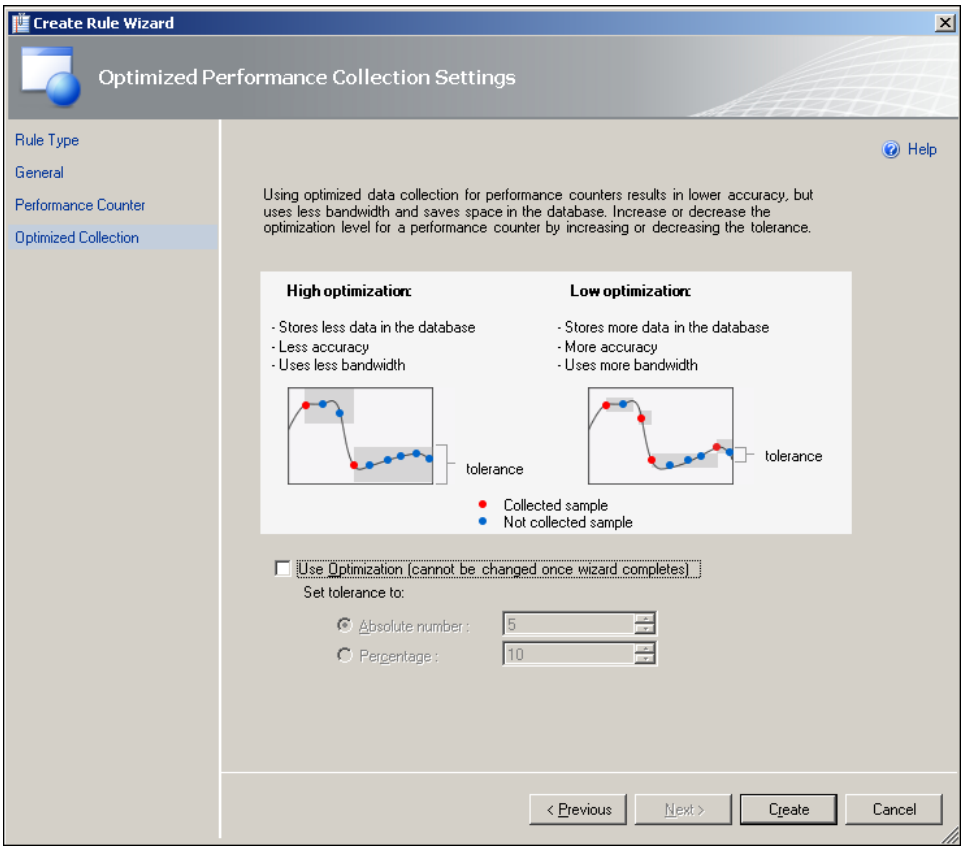
Pick the appropriate object and counter and click OK:



Configure the interval / instances as required and click Next:

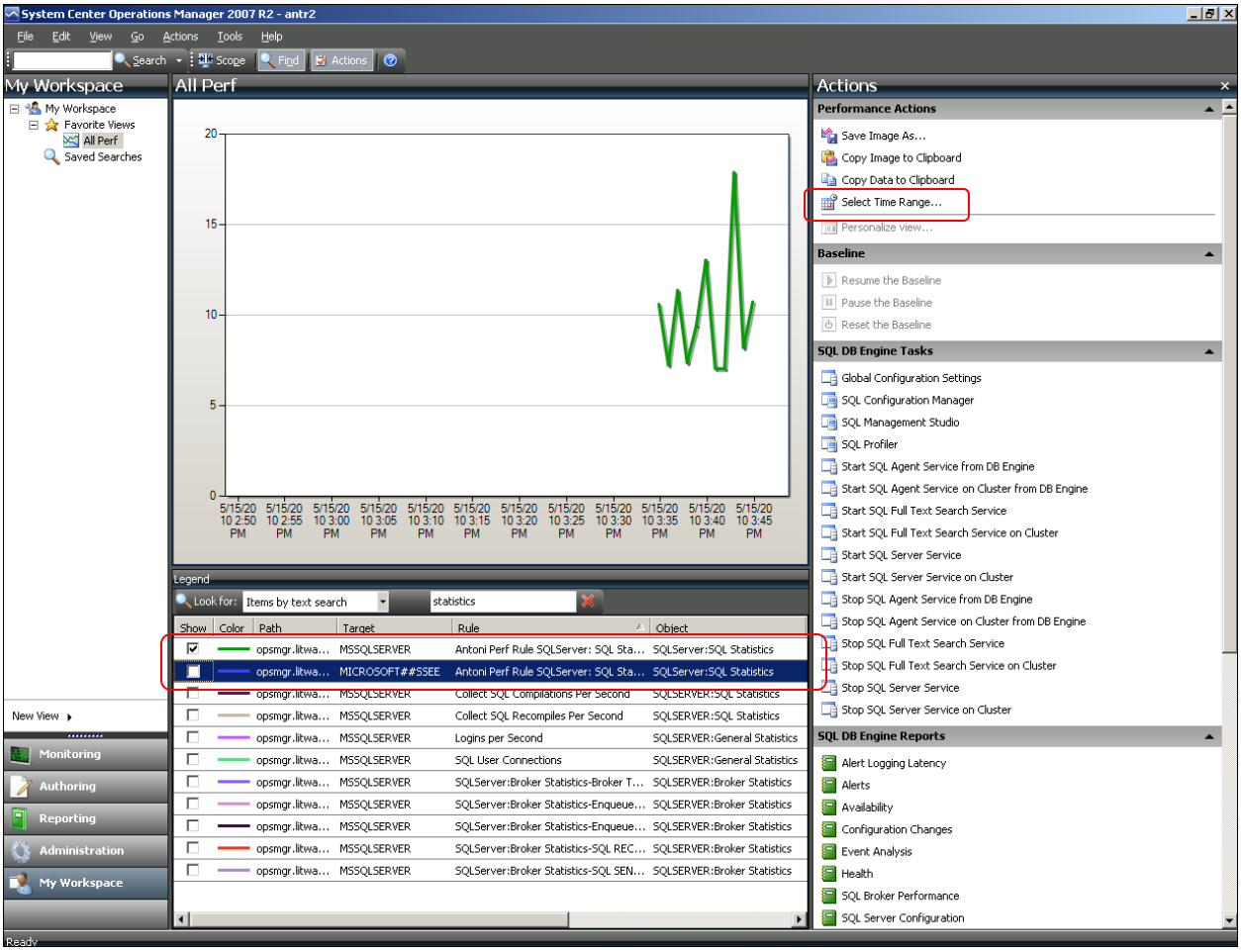


Leave the defaults in the Performance Optimization dialog, and click Create:

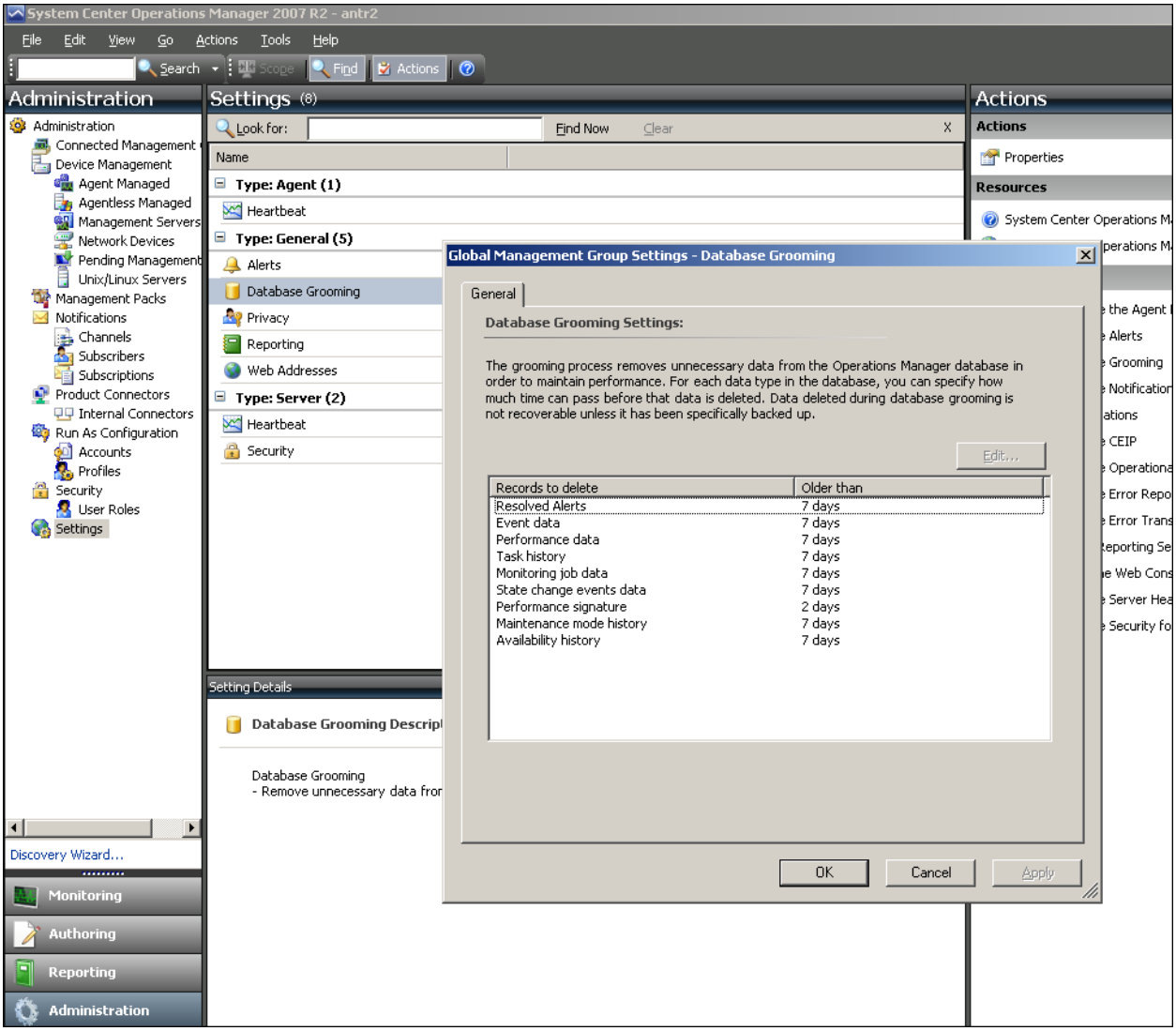


NOTE: Performance Optimization will drop samples that are within a specified range (based on absolute number or percentage) of the last sample collected. This is to reduce space in the database.

After the collection interval that you specified has past, you will see the data in the all performance view that you created. Click on the 'Show' checkbox to display the data. Note you can click on the graph to show the value of the data, or use the 'Select Time Range' option to show a more granular range:



NOTE: The data shown above will go back 7 days by default (unless the settings in Administration>Settings>Database Grooming for performance data have been changed):



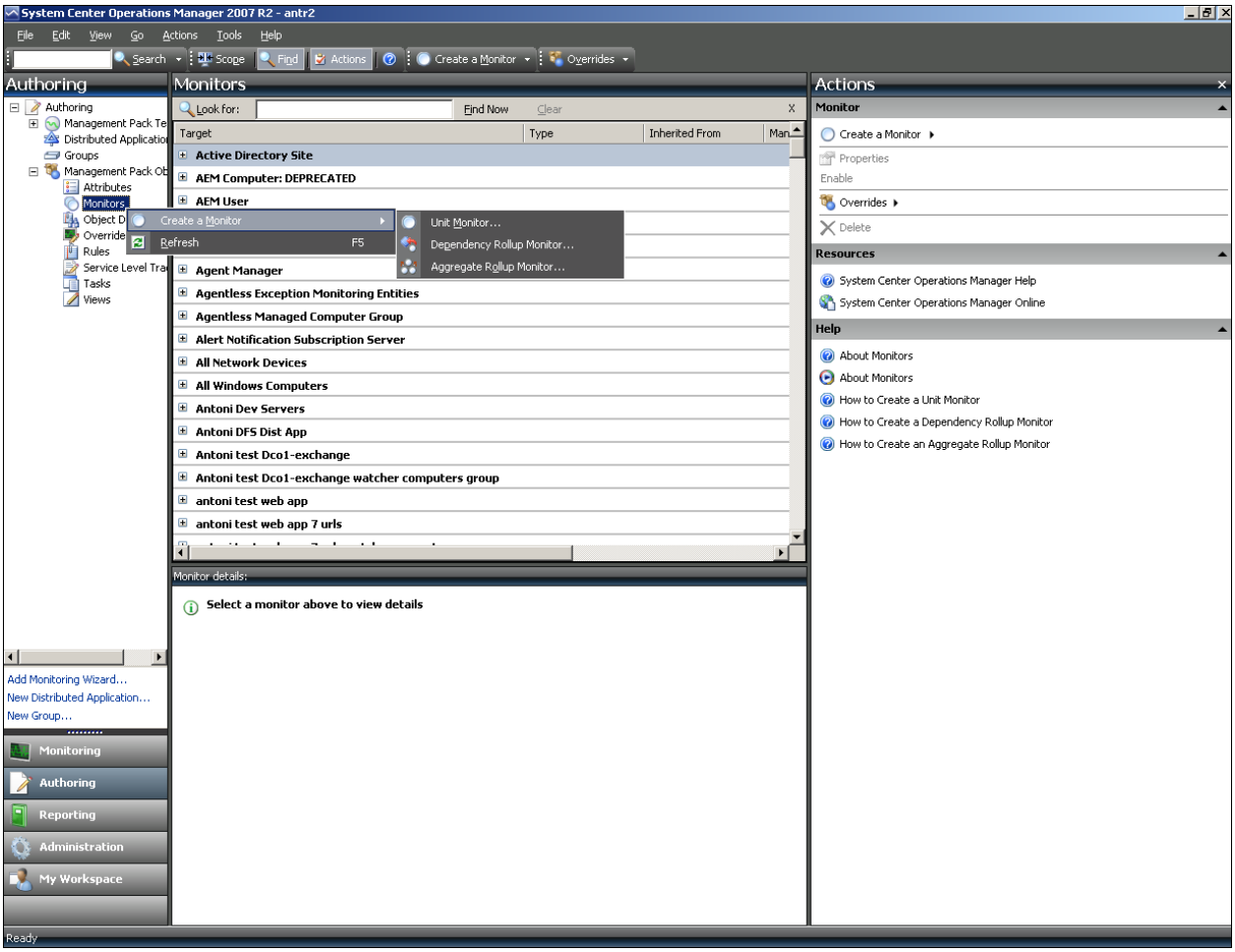
NOTE: Data older than 7 days can be shown in a report (see section X of this document). The rule by default will store the collected performance data in both the live database and the data warehouse.

How do I create a performance monitor to monitor if a performance counter sample exceeds a threshold?

Example: Create a monitor so I am alerted when CPU exceeds 80% usage on a server:

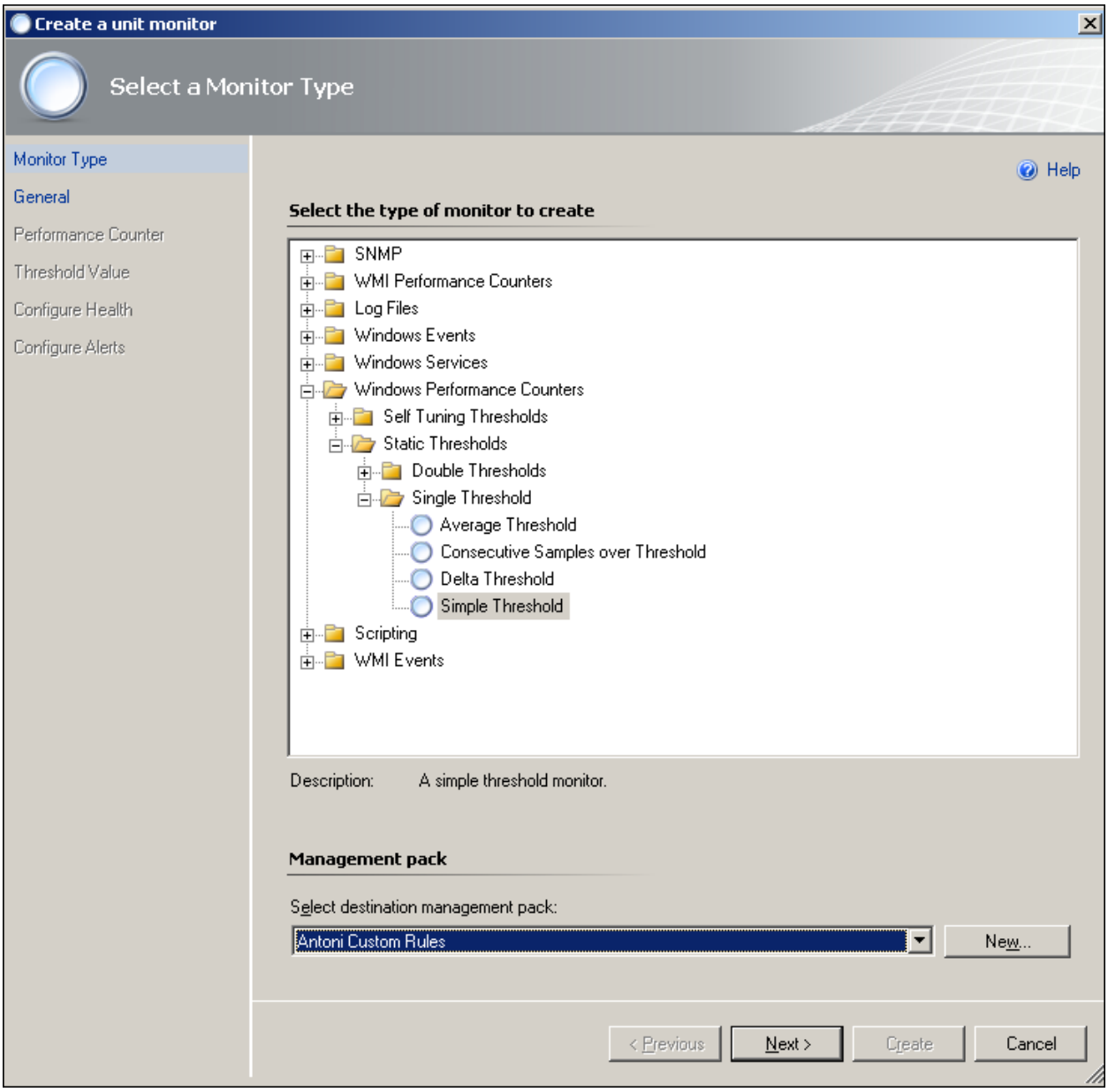
NOTE: Anything using a threshold is a monitor rather than a rule. The key difference between a monitor and a rule, is that a monitor is state-based which means it will actually change the state of an object to red (critical), yellow (warning) or green (healthy) in the state views. A rule is targeted to an object, but will not change the health state of an object.

1) Navigate to Authoring and expand Management Pack Objects. Click Monitors>Create a Monitor>Unit Monitor:



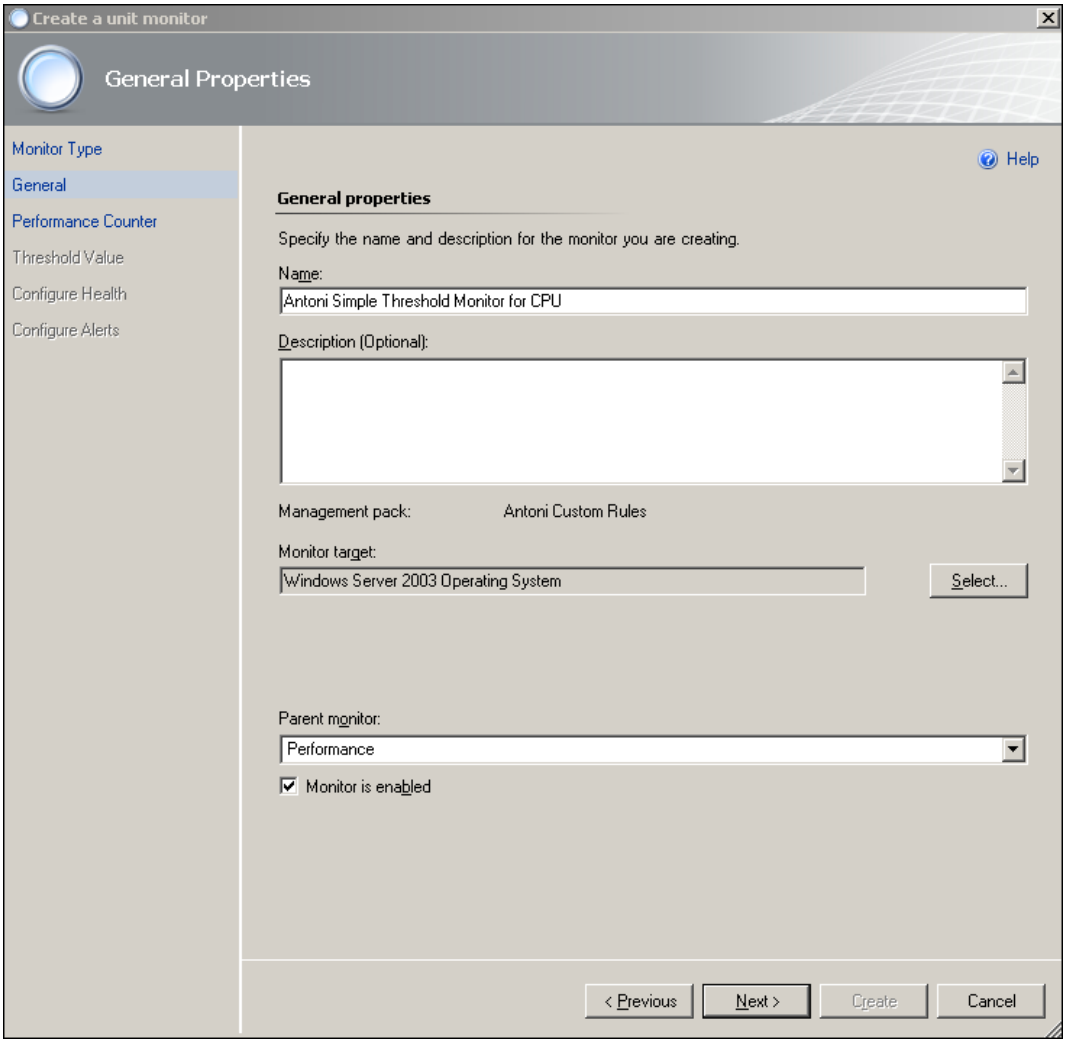
2) Navigate to Windows Performance Counters>Static Thresholds> Single Threshold>Simple Threshold and change the Management Pack so something other than the Default Management Pack, and click Next:

NOTE : This is a single threshold rather than a double threshold. A Single threshold has 2 states such as healthy and critical when the threshold is exceeded. A double threshold monitor has 3 states such as healthy, critical and warning and 2 thresholds are used to calculate which of these health states an object is in.

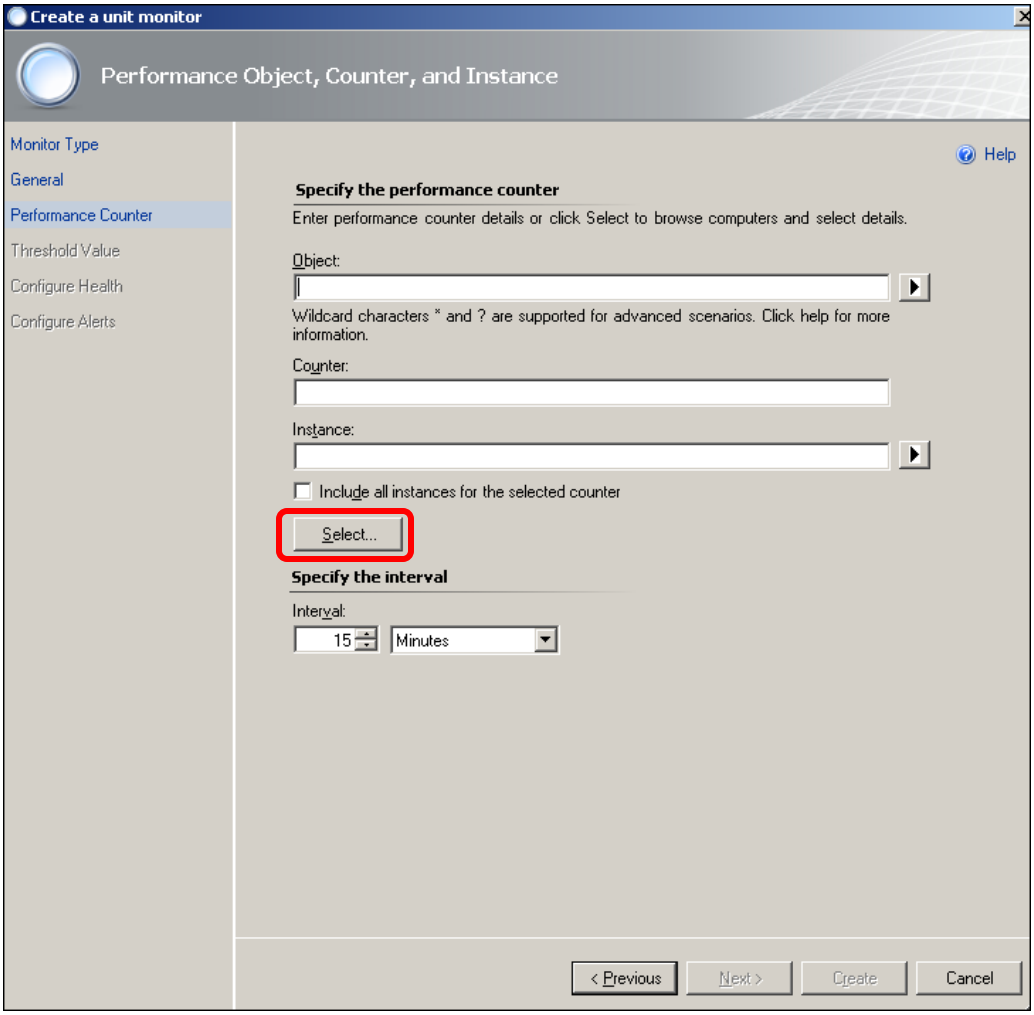


3) Give the monitor a name (For Example: 'XYZ Simple Threshold Monitor for CPU'), Select a Monitor Target that will be present on the computer you want to monitor the performance counter on. In this case an appropriate target is 'Windows Server 2003 Operating System' and then click Next:

NOTE: It is best practice to use some form of prefix or three-letter acronym as a naming convention, to identify all of an organization's custom rules and monitors. This makes it much easier to find custom rules and monitors in the console when necessary.



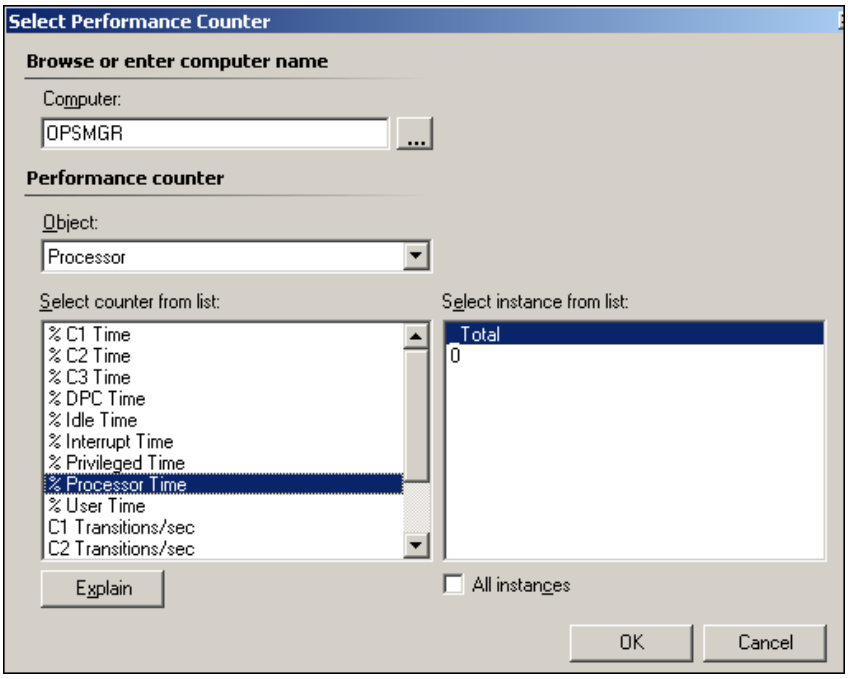
4) In the following dialog, ignore everything and click the ‘Select’ button;



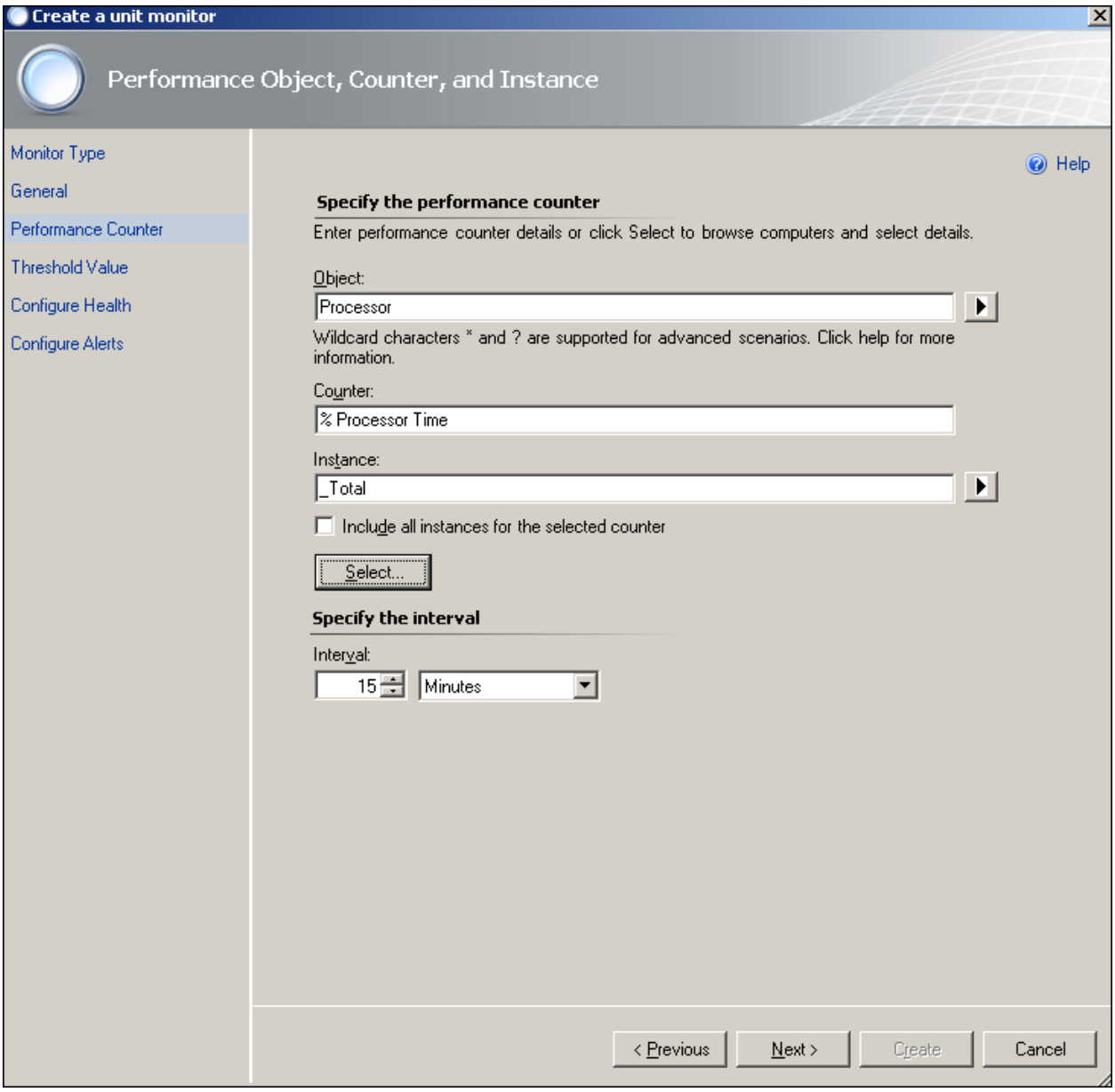
In computer, Browse to a computer that has the performance counter you need to collect and the available object and counters in the list will refresh.

NOTE: This is purely for picking the correct counter. By selecting a computer to pick the counter from, you are **not** saying 'I just want to target this one computer'. Because in the previous dialogs we selected SQL 2005 DB Engine, the performance counter rule will be activated on every Operations Manager agent where a SQL 2005 DB engine object and the counter picked out is found.

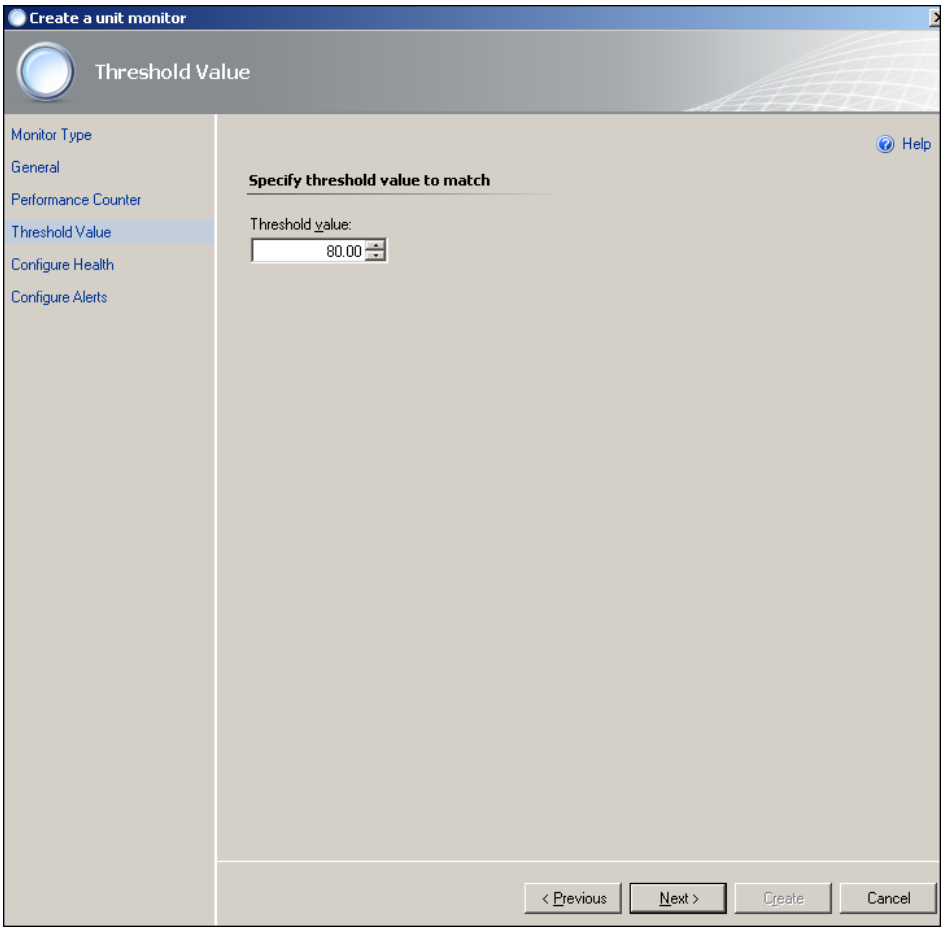
Pick the appropriate object and counter and click OK:



Configure the interval / instances as required and click Next:

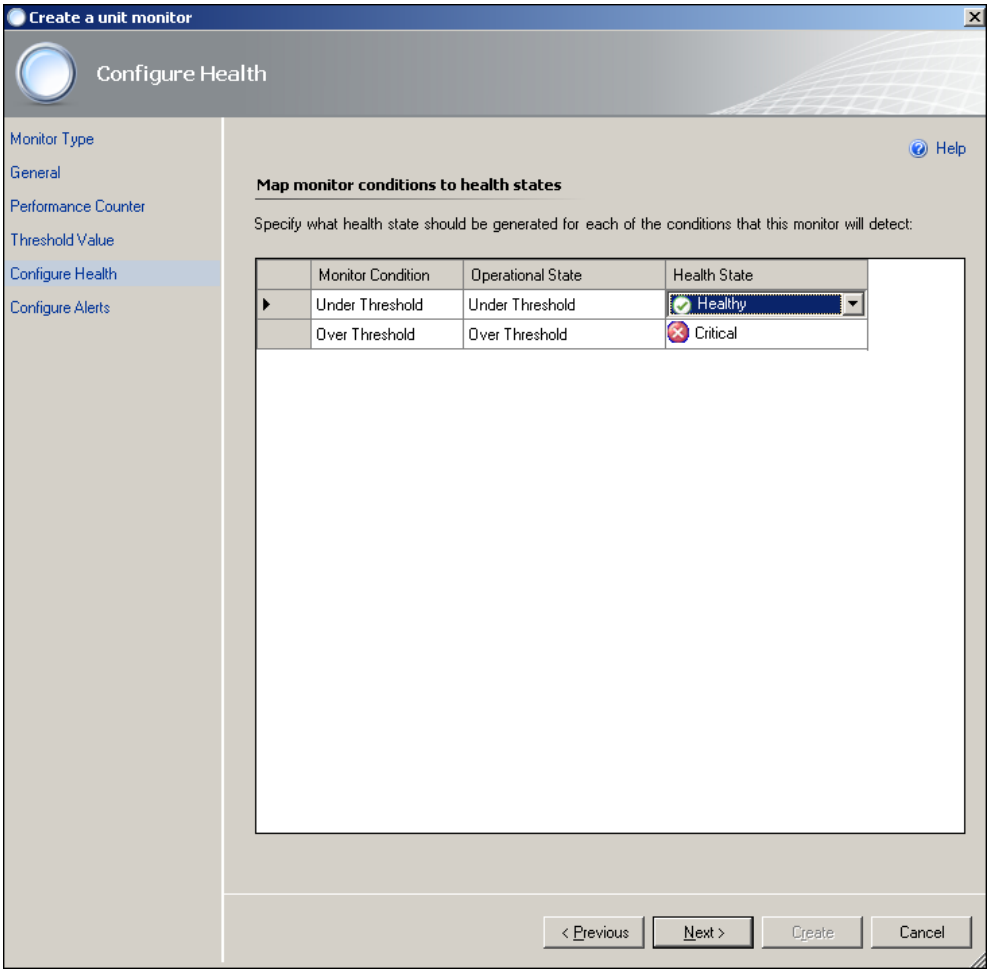


Type the desired threshold value and click Next:

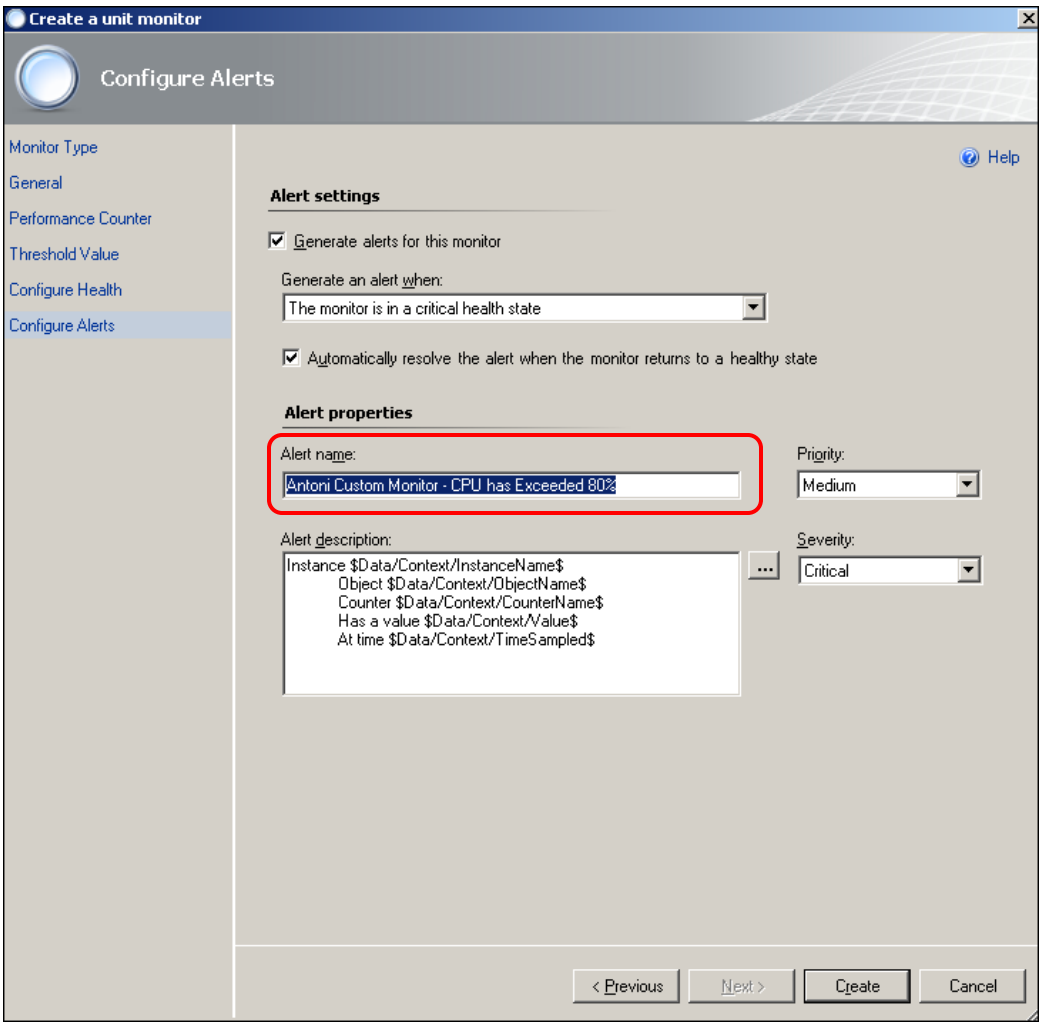


Reconfigure the states if necessary or leave the defaults and click Next:

NOTE: You may need to reverse the states for example if you were monitoring Disk Space in MB and want to change to critical if Over the threshold, and healthy if under the threshold



Place a check in the 'Generate Alerts for this Monitor' and optionally change the name to something more meaningful. Also reconfigure the other settings like severity if needed and click Create:


Create a unit monitor
Configure Alerts
Monitor Type
General
Performance Counter
Threshold Value
Configure Health
Configure Alerts
Help
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:
Antoni Custom Monitor - CPU has Exceeded 80%
Priority:
Medium
Alert description:
Instance $Data/Context/InstanceName$
Object $Data/Context/ObjectName$
Counter $Data/Context/CounterName$
Has a value $Data/Context/Value$
At time $Data/Context/TimeSampled$
Severity:
Critical
< Previous
Next >
Create
Cancel

How do I run a report for a performance counter that OpsMgr is collecting?

Note: This exercise assumes that Operations Manager 2007 reporting is already installed and that a Performance Collection Rule already exists (either in an imported management pack or created in the authoring space in a custom management pack) which is collecting the desired data.

The first step will illustrate how to create an 'All Performance' view which shows all the Performance data that is currently being collected. This only needs to be done once and is used as a reference as to which counters and rules are available.

If a new performance collection rule is created or a disabled one is enabled for the purposes of seeing the performance data in a report, the data will not be available in reports until an hour later because the data is aggregated on an hourly cycle. It is the aggregated data that is displayed in reports.

The steps below only need to be followed once to create a report. Once the report is created with all the required parameters, objects etc, it can be saved to authored reports (by publishing it) or saved to 'favorite reports' and then be executed, without having to carry out the following steps each time the report is ran.

This document uses the example of creating a performance report displaying the performance counter SQL Server: SQL Statistics and Counter –Batch Requests /Sec. This data is collected by the Rule – 'Antoni Perf Rule SQL Server: SQL Statistics\Batch Requests/Sec' which is targeted to all SQL 2005 DB Engines (Created in section H of this document).

Outline of Steps (Fully Detailed Steps Commence on Next Page)

1) Create an 'All' Performance View in My Workspace

2) Identify the rule and target name(s) for the required Performance Counter

3) Open the Generic Performance Report

4) Add the Required Chart and Series lines

5) Add an individual object to the first series line:

6) Add an individual object to any additional series lines:

7) Add the appropriate rule to the first series line

8) Add the appropriate rule to any additional series lines

9) Click OK in the settings dialog to confirm the settings.

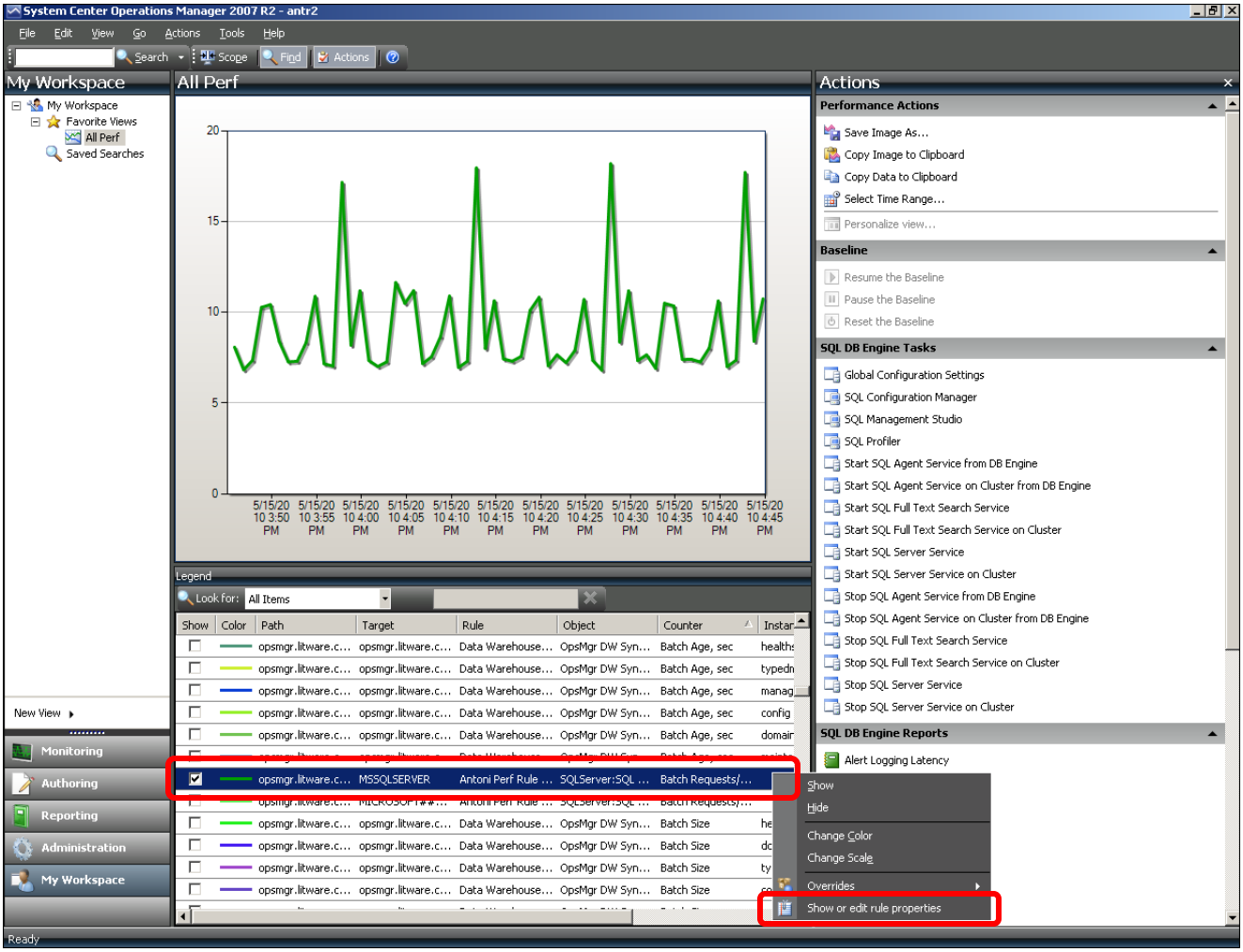
10) Change the From value to a start time in the past, for instance use a previous day in the week.

11) Click Run

Detailed Steps

1) Create an 'All' Performance View in My Workspace using the steps in Section G of this Document.

2) Identify the rule and target name(s) for the required Performance Counter:

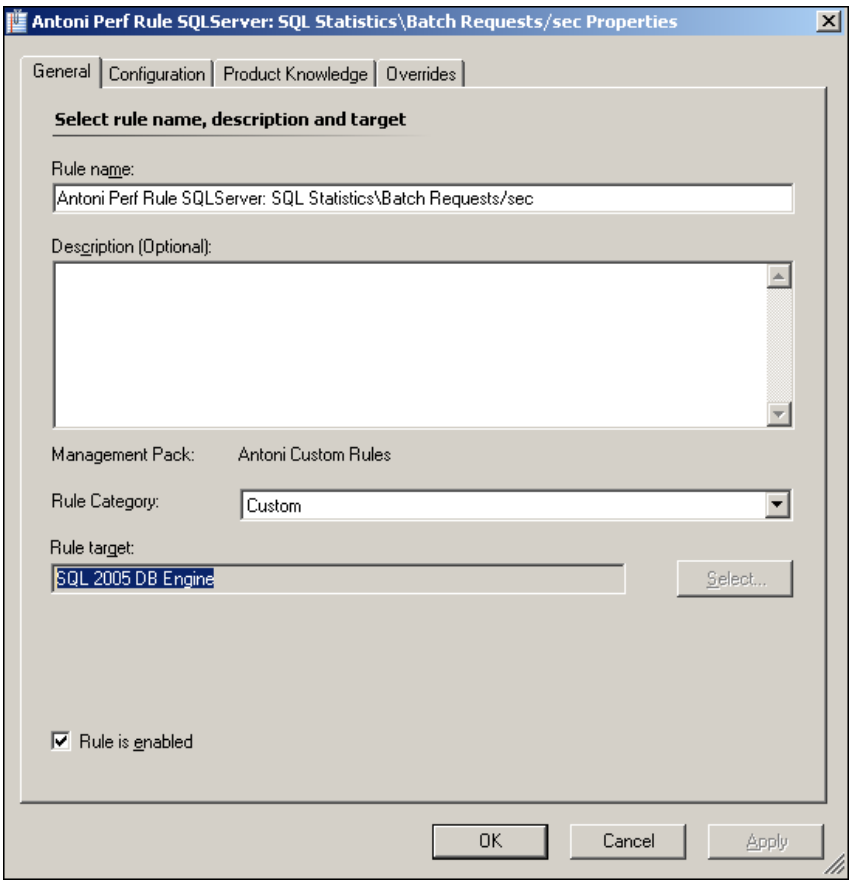


a) Sort by Counter by clicking the counter column header

b) Scroll down in the lower pane to find the Performance counter / object that you want to create a report for.

NOTE: in this example, we will use the Object SQL Server: SQL Statistics and Counter –Batch Requests /Sec

c) Right click the appropriate line and click ‘Show or Edit Rule properties’:



c) Note the 'Rule Target' and 'Rule Name' in the rule properties.

In this example:

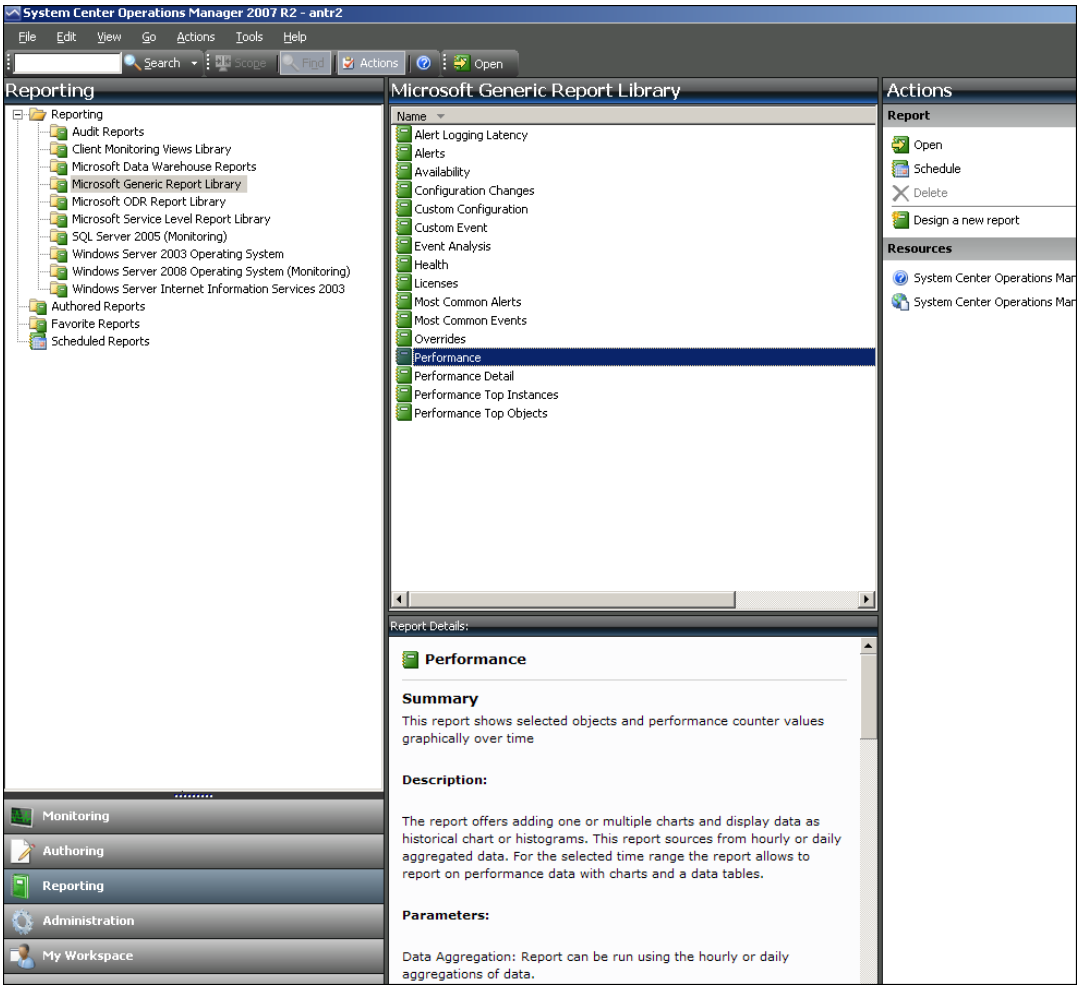
Rule Name – Antoni Perf Rule SQL Server: SQL Statistics\Batch Requests/Sec

Rule Target – SQL 2005 DB Engine:

3) Open the Generic Performance Report

a) Click the reporting space and 'Microsoft Generic Reports Library' on the left

b) Double Click 'Performance'



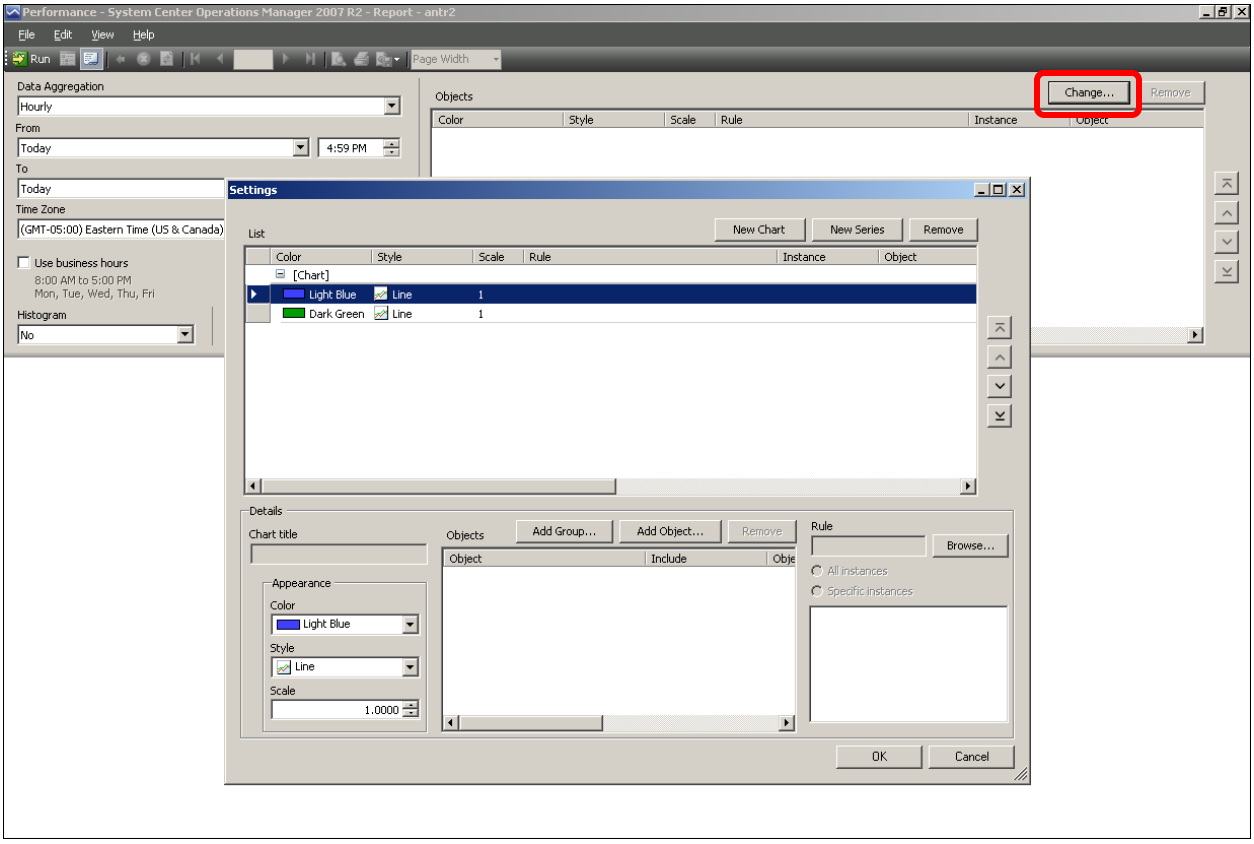
4) Add the Required Chart and Series lines

a) Click the 'Change' button near the top right of the window

b) In the settings dialog box, click the new chart button

c) Click the New Series button one or more times depending on how many datasets you would like your graph to show. If you will be adding an object such as the Batch Request/Sec for 15 different SQL 2005 DB Engines, you would need to add 15 Series lines.

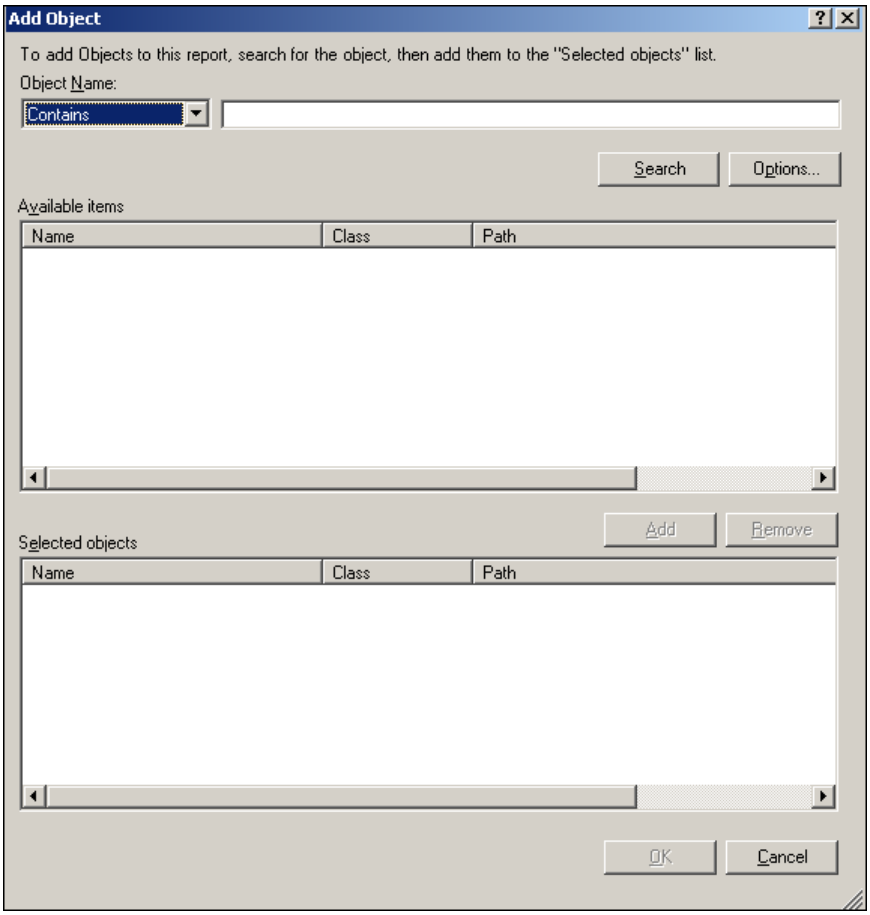
NOTE: In the example, I will add 2 SQL 2005 DB Engines (the SQL Server Instance and the SQL Express Instance), so I click New Series twice.



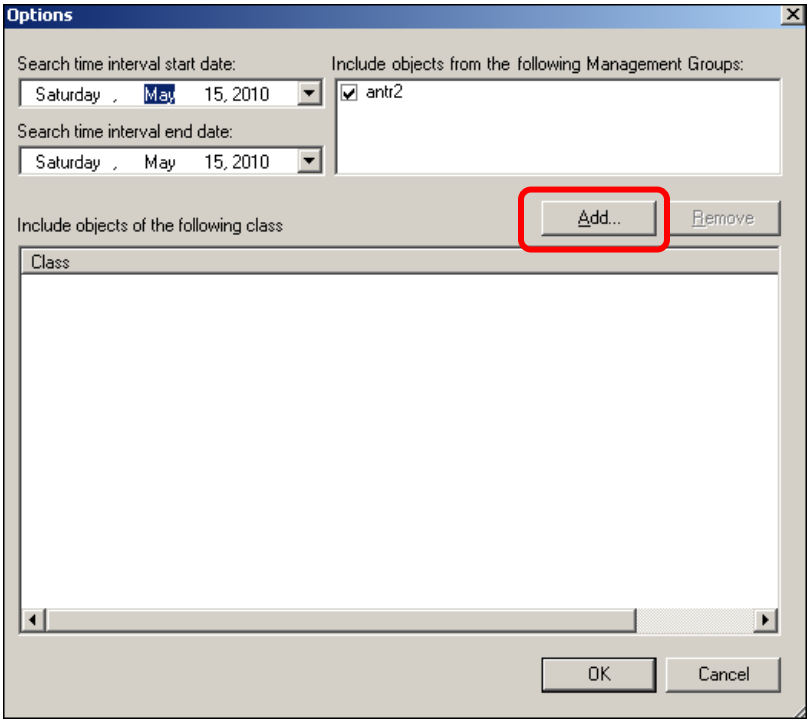
5) Add an individual object to the first series line:

a) Click on the first series and click Add Object

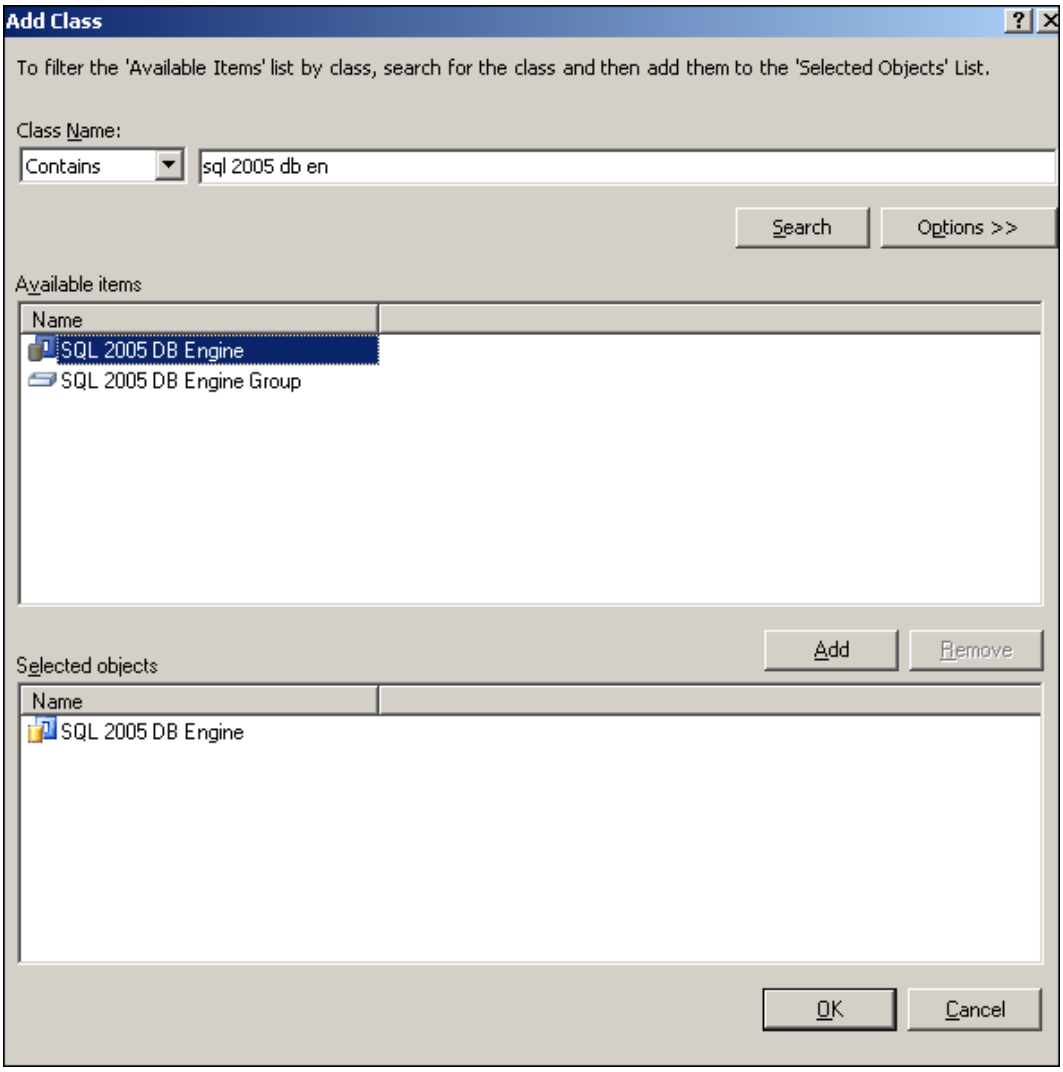
b) Click the Options button:



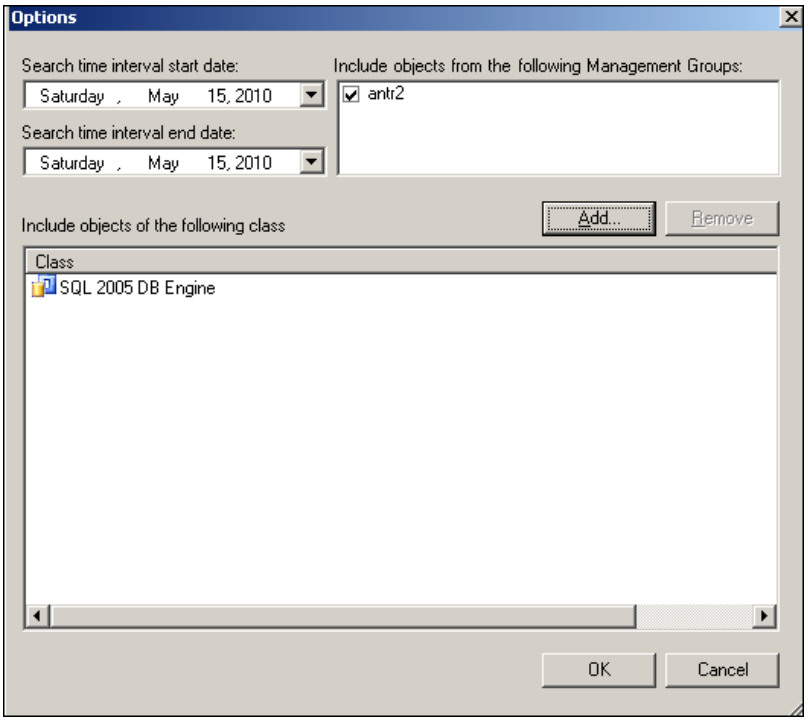
c) Click the Add button:



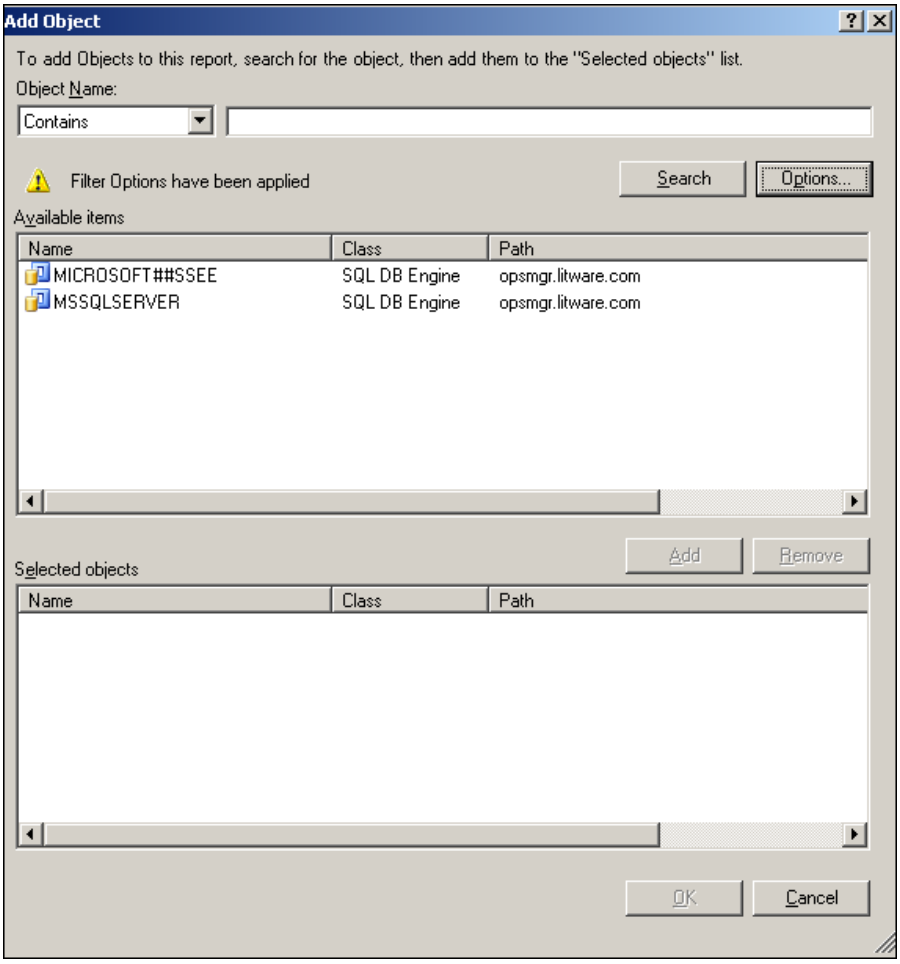
d) Type in all or part of the class name that you noted in Step 2, Search for it and add the exact class then click OK:



e) Click Ok in the Options dialog:

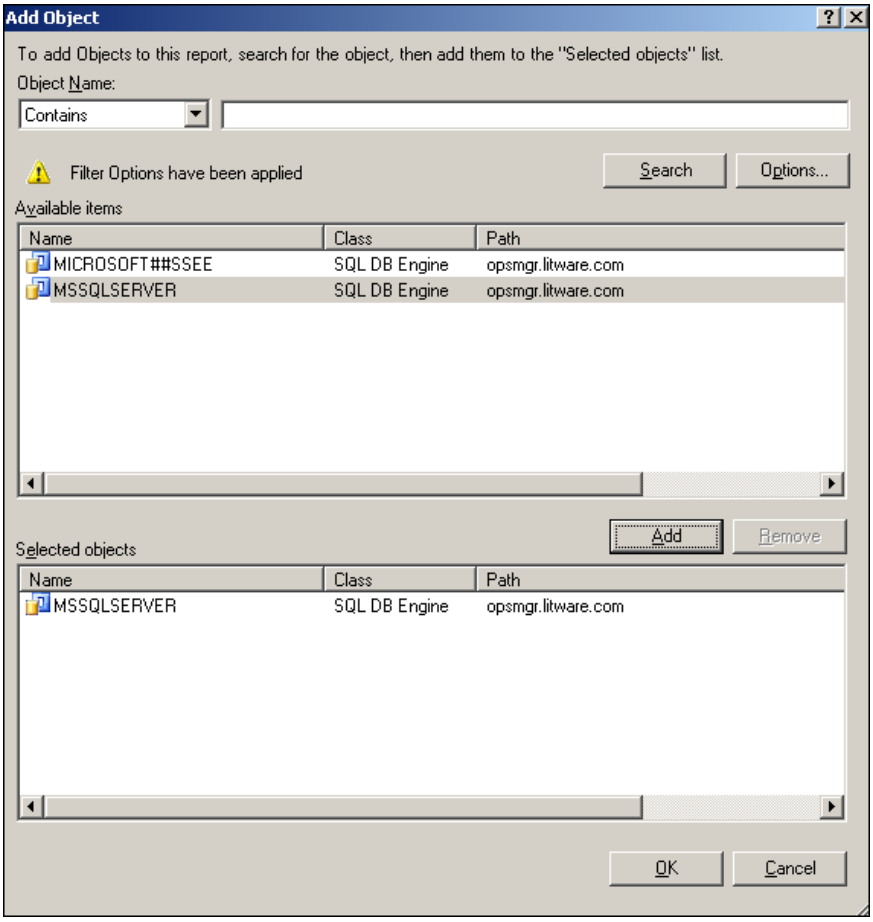


f) With the Filter applied, click Search and all instances of the selected object should be returned:



g) Pick ONE instance of the Objects, Add click OK

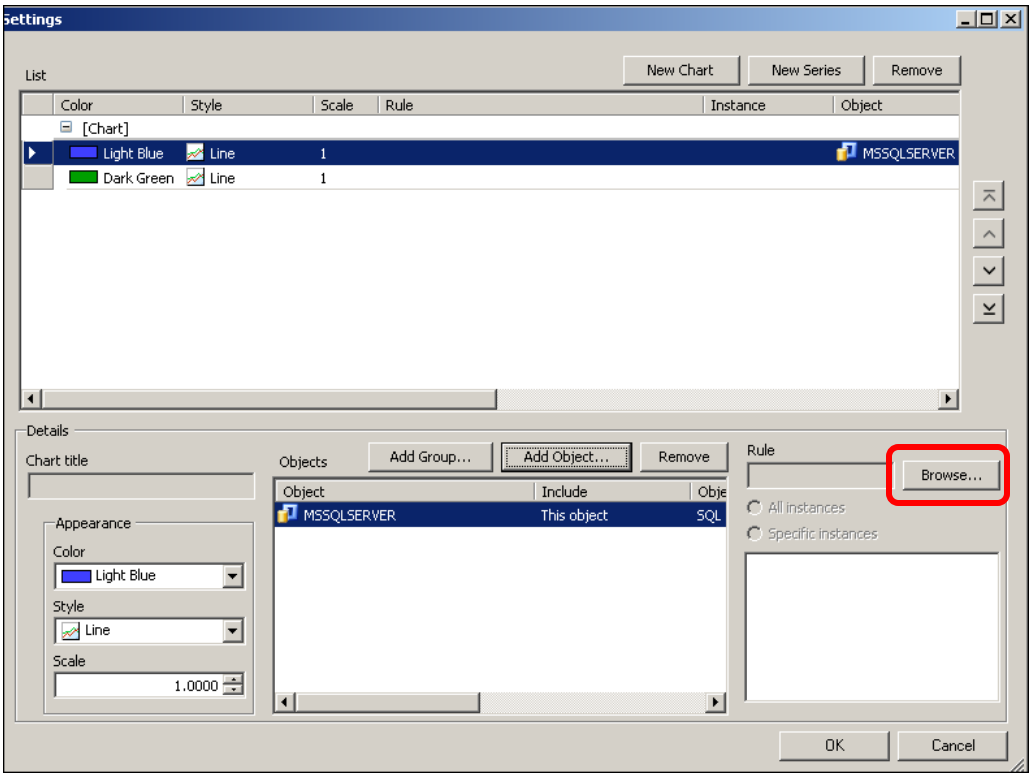
NOTE: Do not pick multiple instances. If you wish to add more than 2 instances (for instance 10 SQL Servers) you will need to add 10 series lines (using the new series button) and then add an individual instance to each series using steps Xx, Xx and X:



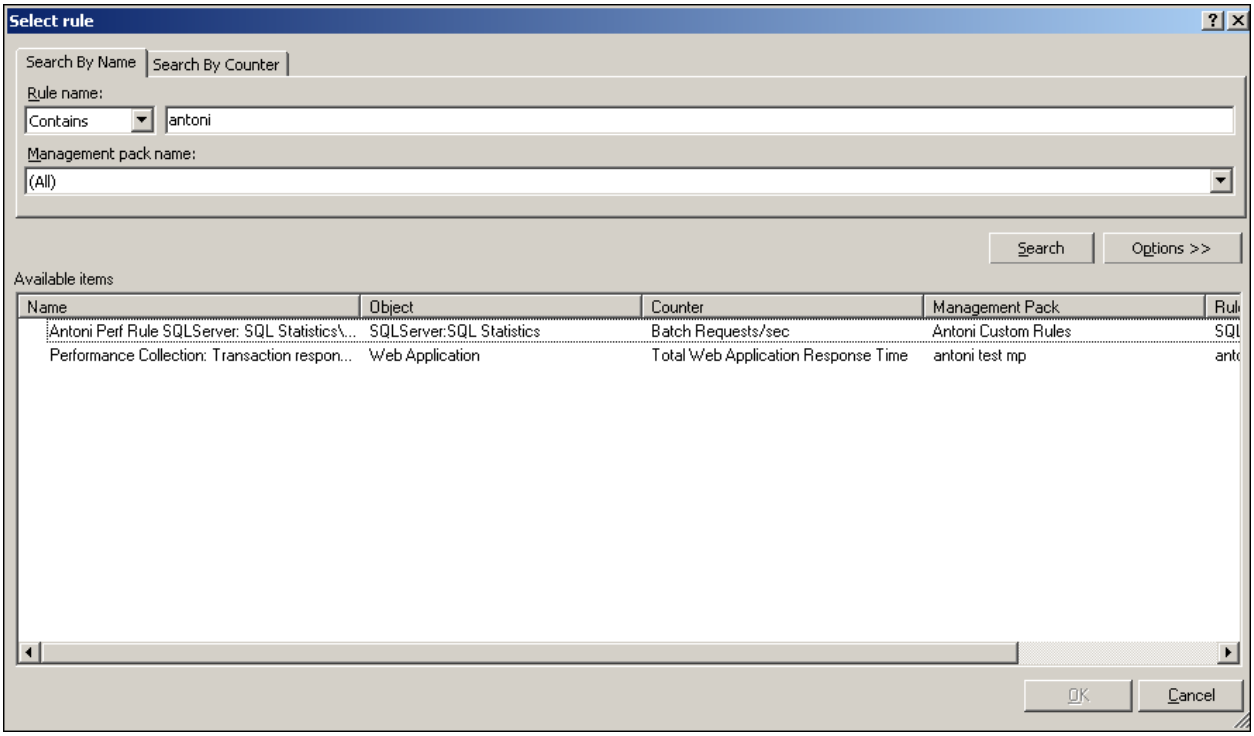
7) Add the appropriate rule to the first series line

a) If not already selected, click the first series line that was added under the chart header

b) Click the Browse button next to Rule on the right-hand side of the Settings Dialog:



c) Leave the default 'Search by Name' Selected and in the search box, type part or the entire rule name noted in step 2 and click search:

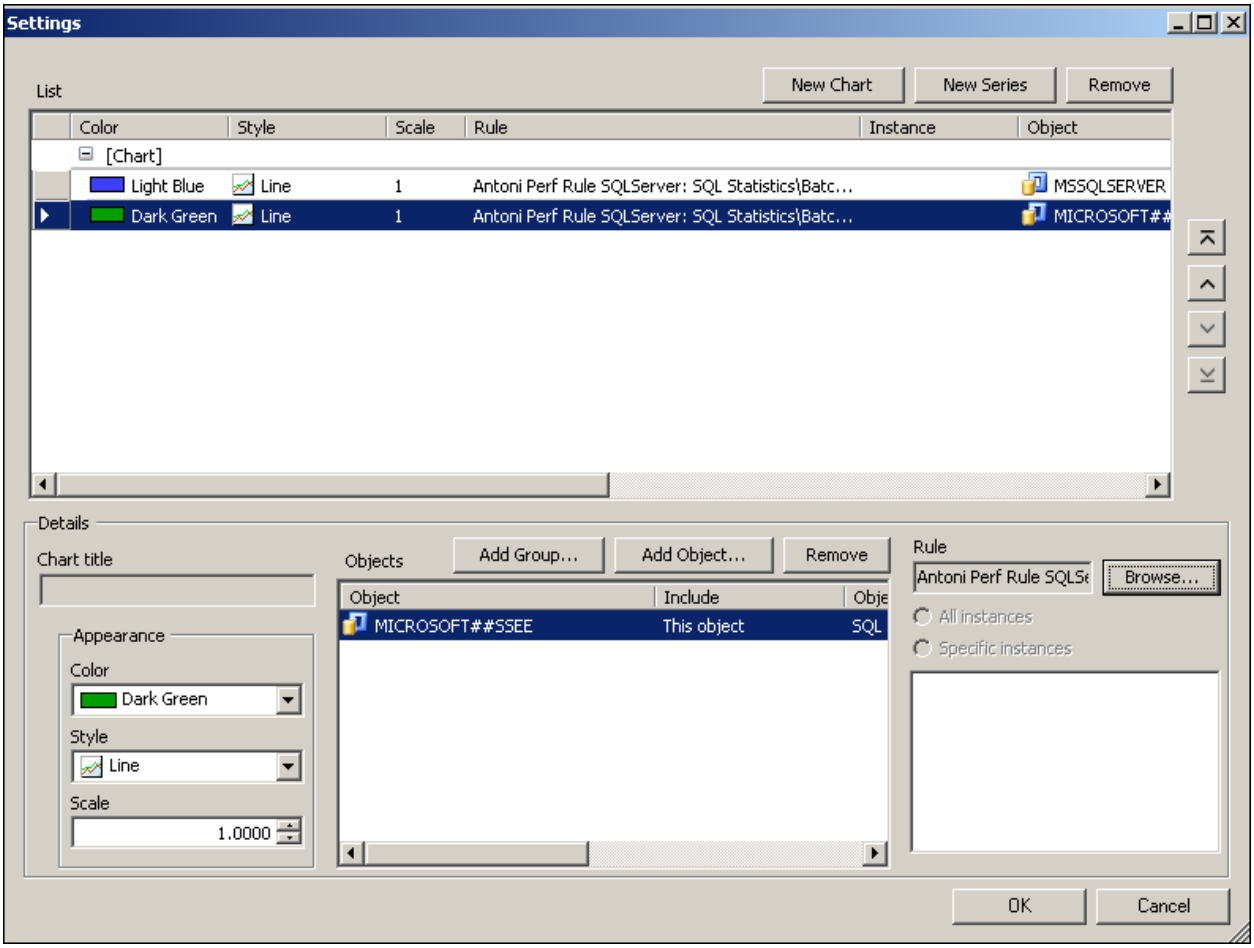


Select the appropriate rule and click OK.

Click the next series without a rule or object assigned.

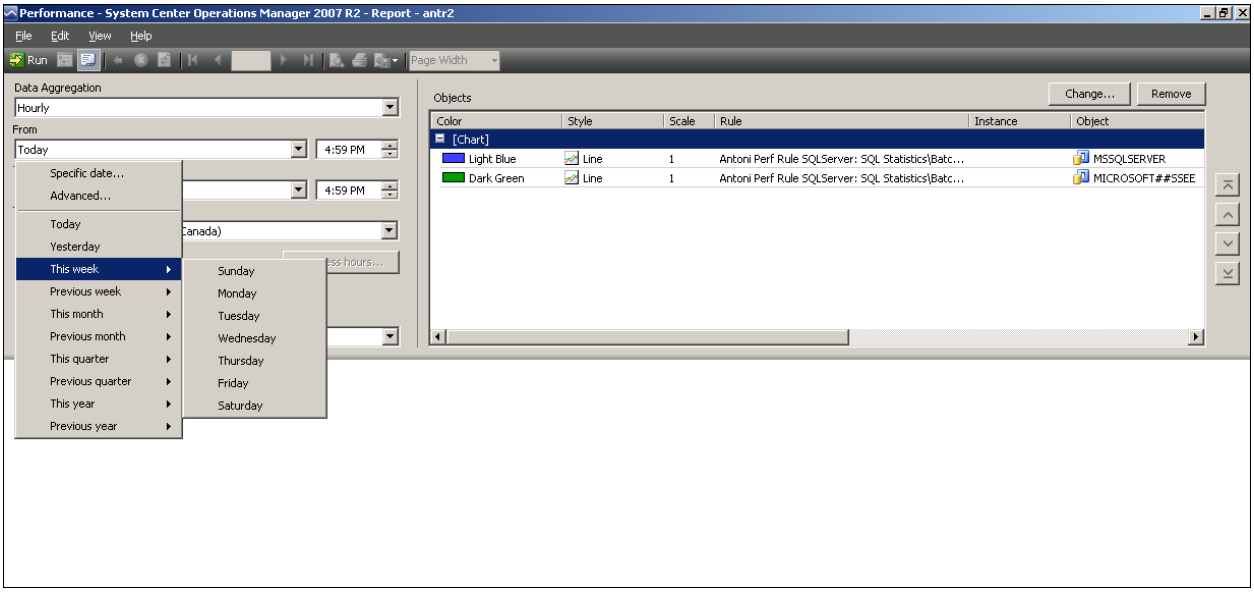
Repeat 6 and 7 for the next object you wish to add. When finished it should look something like this:

NOTE: although the rule name is cached and you will not need to search for it if using the same rule, you will need to search for the object type again, apply the filter, search for instances and then add the instance.



8) Click OK in the settings dialog to confirm the settings.

9) Change the From value to a start time in the past, for instance use a previous day in the week.


Performance - System Center Operations Manager 2007 R2 - Report - antr2
File
Edit
View
Help
Run
Page Width
Data Aggregation
Hourly
From
Today
4:59 PM
4:59 PM
Specific date...
Advanced...
Today
Yesterday
This week
Previous week
This month
Previous month
This quarter
Previous quarter
This year
Previous year
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Objects
Change...
Remove
Color
Style
Scale
Rule
Instance
Object
[Chart]
Light Blue
Line
1
Antoni Perf Rule SQLServer: SQL Statistics\Batc...
MSSQLSERVER
Dark Green
Line
1
Antoni Perf Rule SQLServer: SQL Statistics\Batc...
MICROSOFT##SSEE

11) Click Run

This was the report output using my example:

TIPS:

1) You can click the 'Show or Hide Parameter button' to bring back the parameters and modify the report settings. Access the settings dialog using the Change button.

2) Once the report appears, you can use the File menu to perform one of the following options which will remember the way in which you configured the report, allowing it to be re-ran by simply double clicking it:

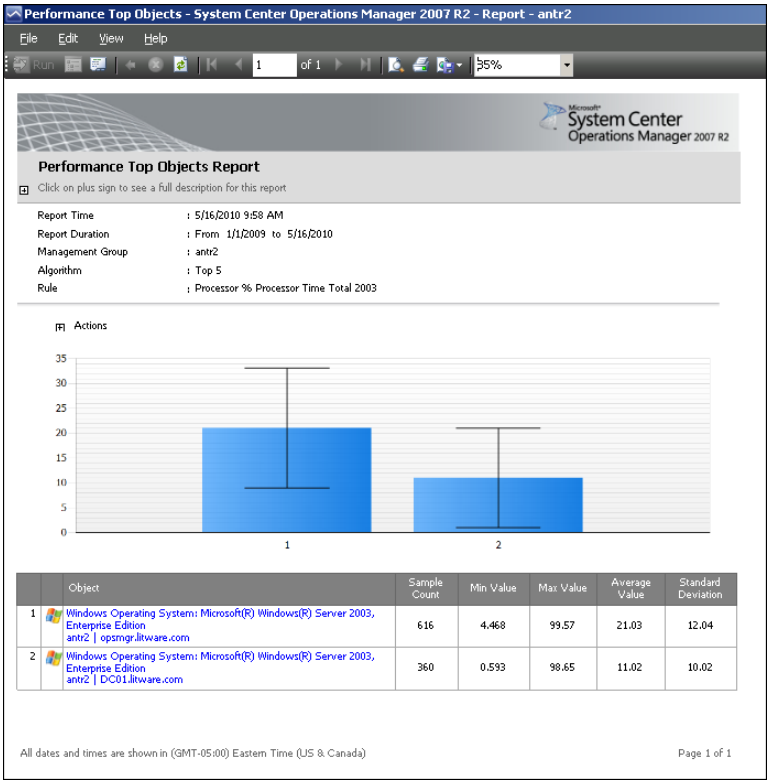
Save to favorites – This will save the report to the ‘Favorite Reports’ node which is user-profile specific so the report will only be seen by the user who publishes it

Publish – This will save the report to the ‘Authored Reports’ node which is user-profile specific so the report will only be seen by the user who publishes it
Save to Management Pack – Will allow you to specify an existing management pack or create a new one to store the report in. This will create a new Folder under the reporting tree in the reporting space.

How Do I Generate a Top ‘n’ Performance Report?

The Top ‘n’ reports are very powerful in that they can display the top ‘n’ server for CPU usage, memory or any performance counter being collected by Operations Manager and stored in the warehouse.

Instructions:
1) Open the Performance Top Objects Report
2) Click the reporting space and 'Microsoft Generic Reports Library' on the left
3) Double Click 'Performance Top Objects’
4) Click the Browse button next to ‘Rule’ and pick out the appropriate rule (if required this can be determined from the view created in Section G of this document)
5) Search for the appropriate rule name (e.g. for a report showing top ‘n’ objects for CPU usage, type processor and click ‘Search’.
6) Choose the appropriate rule such as Processor % Processor Time Total 2003 and click ok.
7) Change the From and To fields to the desired timeframe.
8) Change the Algorithm from top N to Bottom N if appropriate for the counter being collected (e.g. if running against % free space, Bottom N may be more appropriate)
9) Change the ‘n’ to the appropriate number. By default this is 5 and will therefore show the top 5 / bottom 5 objects.
10) Click the Run button



How do I know what parameters are available in an event to monitor off?

High-Level Steps (Detailed Steps follow):

1) Create an Event collection rule to collect the event
2) Create an Event View in Operations Manager for collecting the Events (optional).
3) Query the DB to find which the table the events are being stored in, and then query the appropriate table to get the event parameters.

Task 1 – Create an Event Collection Rule for the event you're interested in, using the following steps

NOTE: An Event Collection Rule will only store the events in the Operations Manger database, making them accessible via event views. It will not generate an alert when an event occurs – for the purpose of generating an alert (from which email notification can be configured) use an Alert-generating rule.

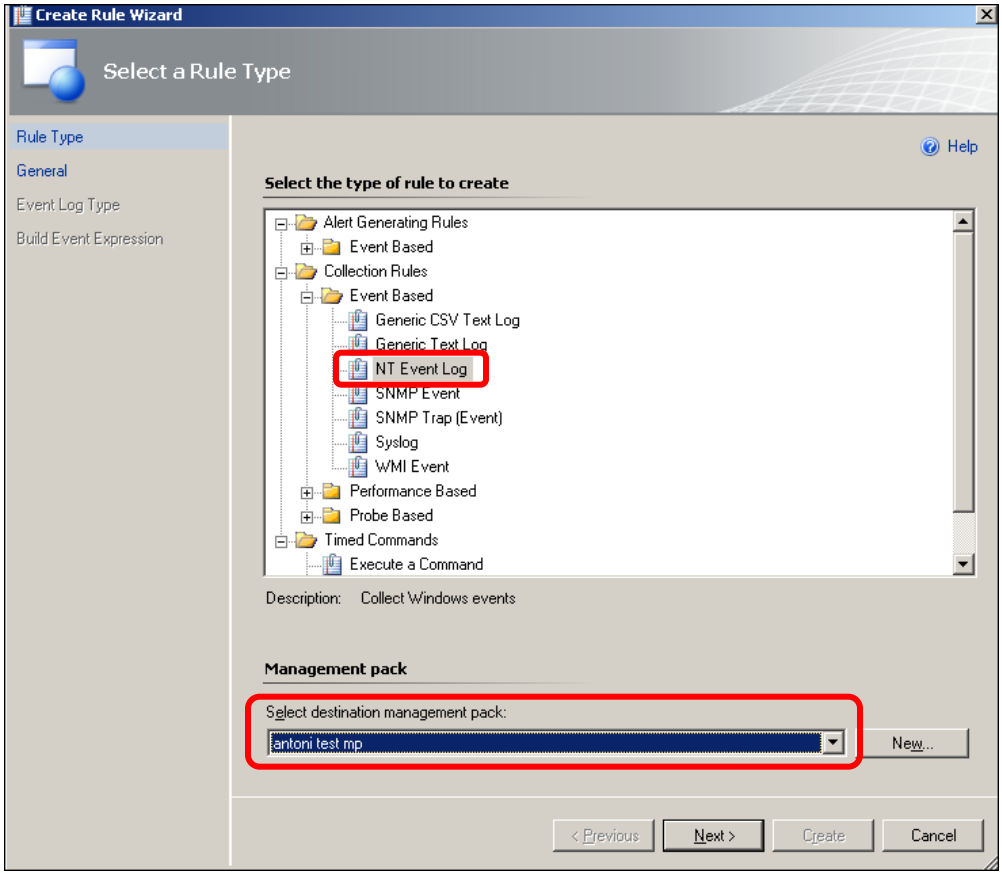
Go to the Authoring space

1) Launch the Operator's Console (Start>All Programs>System Center Operations Manager 2007 R2>Operations Console)
2) Click the 'Authoring' space on the bottom left hand side.
3) Right-click Management Pack Objects>Rules and choose 'Create a new rule'
4) In the dialog, expand Collection Rules>Event based
5) Click 'NT Event Log'

NOTE: A Golden rule of Operations Manager is to NOT store anything in the Default Management Pack. See Section M of this document for explanation why.

6) Change the Management Pack from Default Management Pack to an appropriate Management Pack. If there is an MP where all the company's test rules and monitors are stored, then select it from the dropdown. If not Create a new Management Pack by clicking the New button, give it a name, hit Next and Create)

7) With NT Event Log and the appropriate Management Pack selected, click Next:



8) Give the rule a name (For Example: 'XYZ Event Collection Rule for 632 events')

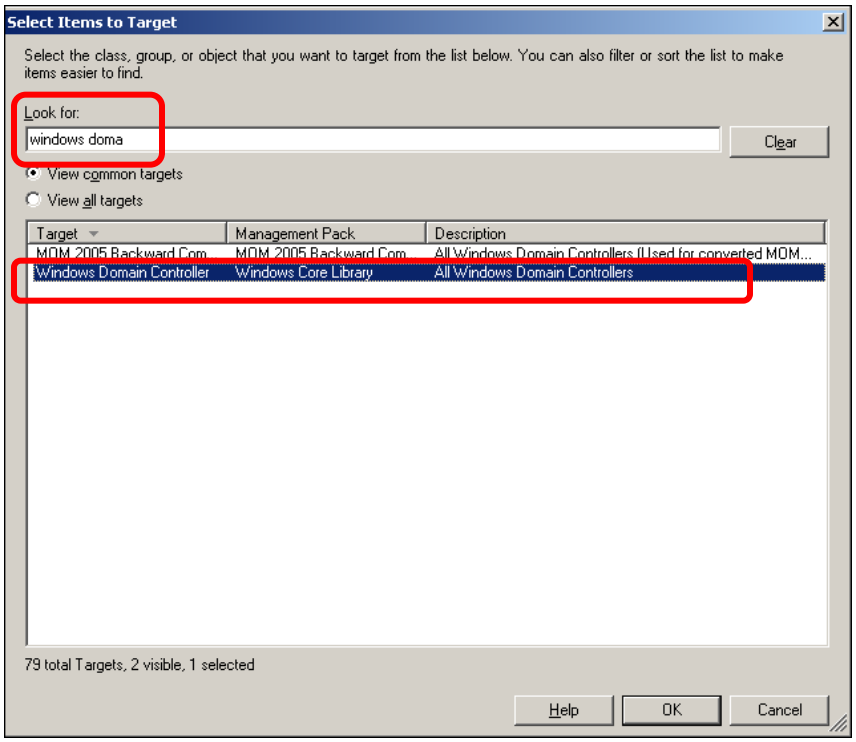
NOTE: It is best practice to use some form of prefix or three-letter acronym as a naming convention, to identify all of an organization's custom rules and monitors. This makes it much easier to find custom rules in the console when necessary.

9) Click the 'Select' button next to the Rule target box and choose an appropriate target such as 'Windows Domain Controller and click OK.

NOTE: Because the 632 event will only occur on domain controllers, it is appropriate to target the rule to the Windows domain controller object. If the event could occur on any windows computer, use

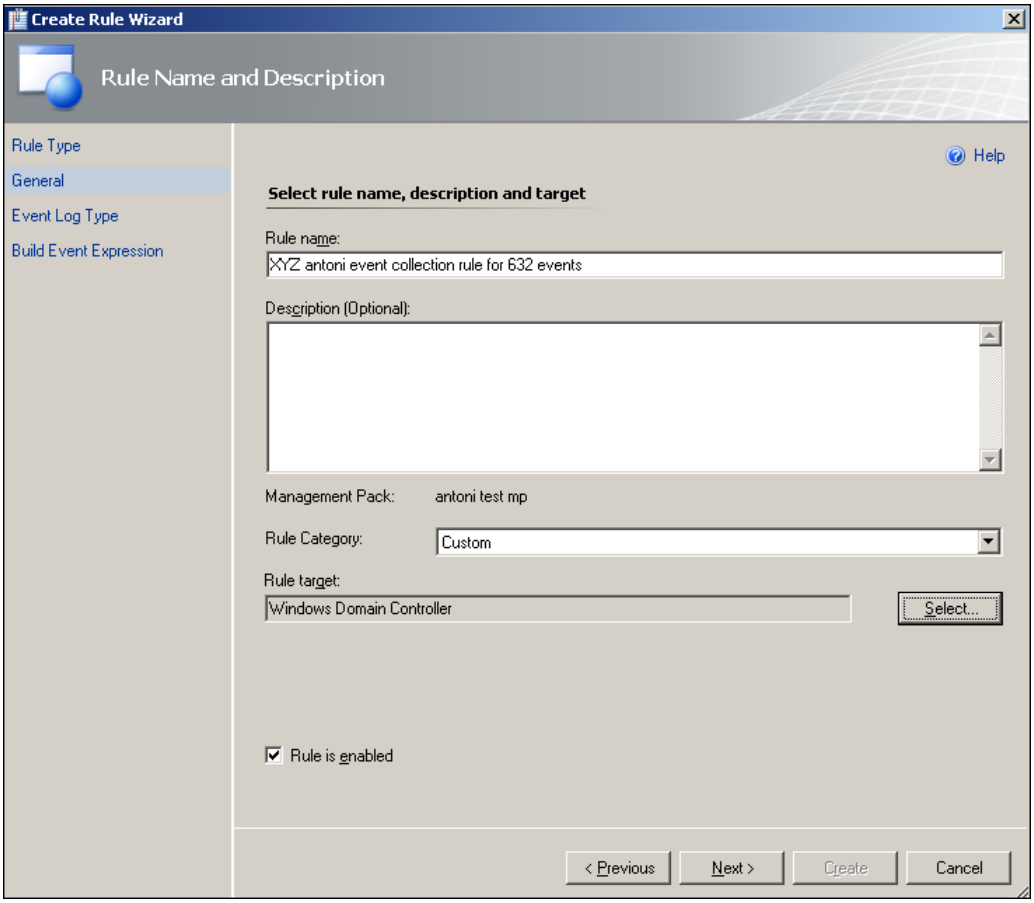
'Windows Operating System' ,'Windows Server 2003 Operating System' or 'Windows Server 2008 Operating System' as your target. Best practice is to be as specific as possible.

NOTE: Start typing the name of the object desired in the 'Look For' box to narrow the list down, and If the object you're after is not available, click the 'View all targets' radio button.



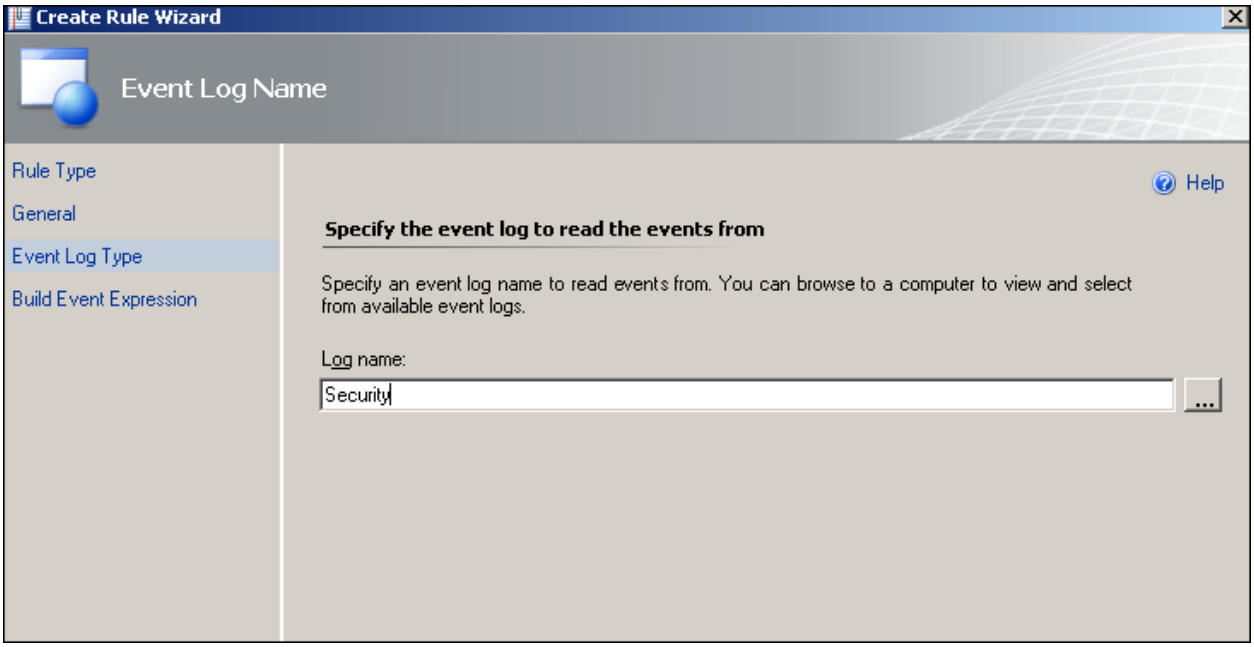
10) Leave the defaults of 'Custom' as the Category, 'Rule is enabled' checked and then click Next

NOTE: By leaving the Rule enabled, the rule will become active on every instance of the object you target the rule to (e.g. every windows computer / every windows domain controller depending on the object that you target). To target a specific instance or a subset of instanced, uncheck the 'Rule is Enable' box to disable it by default and then following the creation of the rule, Create an Override to enable for an instance or group of instances.



11) In the Event Log Name, type the word Security, or alternatively, click the 3 dots and select the Security Event Log, and click Next:

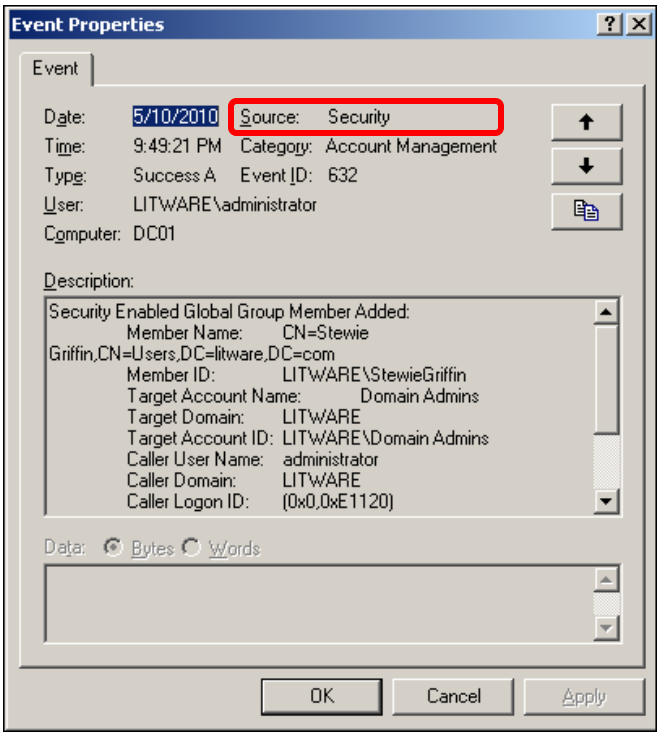
NOTE: This is nothing to do with the targeting. This is purely to make sure you get the name of the event log correct with no typos. The Rule will look in the selected event log on every object targeted (e.g. every windows computer or domain controller) that has the selected event log.



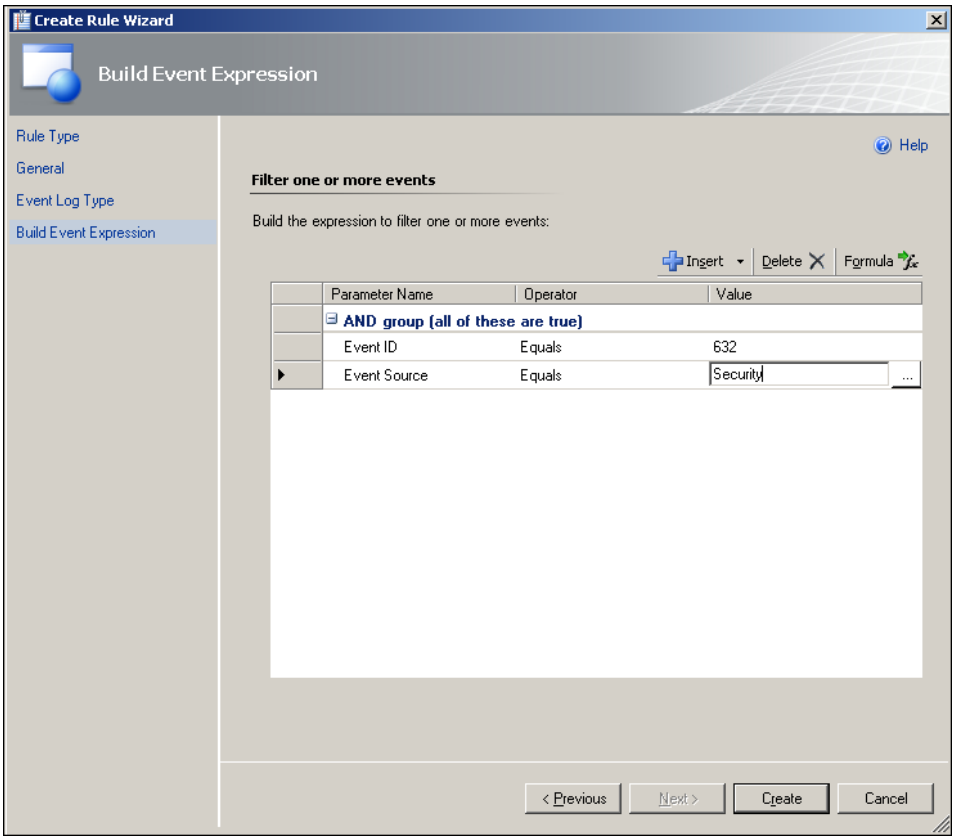
12) In the Value box on the Event ID line, type 632

NOTE: If you wish to collect a different Event, simply specify the alternative Event ID here.

13) In the box underneath, type the Event Source as it appears in the event. In the case of the 632 event, the Event Source is Security:



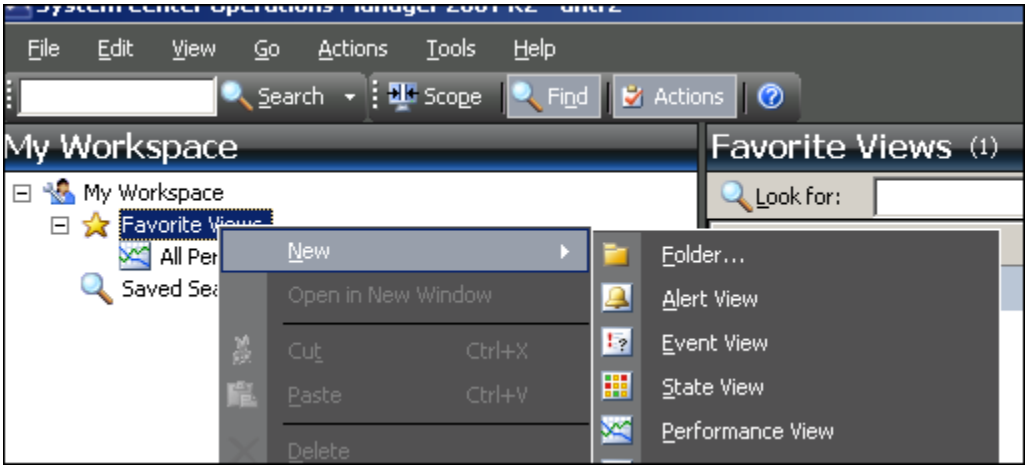
14) Click Create:



Task 2 (Optional) – Create an Event View in Operations Manager for collecting the Events.

1) In the Operator's console, Click the My Workspace space.

2) Right click Favorite Views, and choose New>Event View:

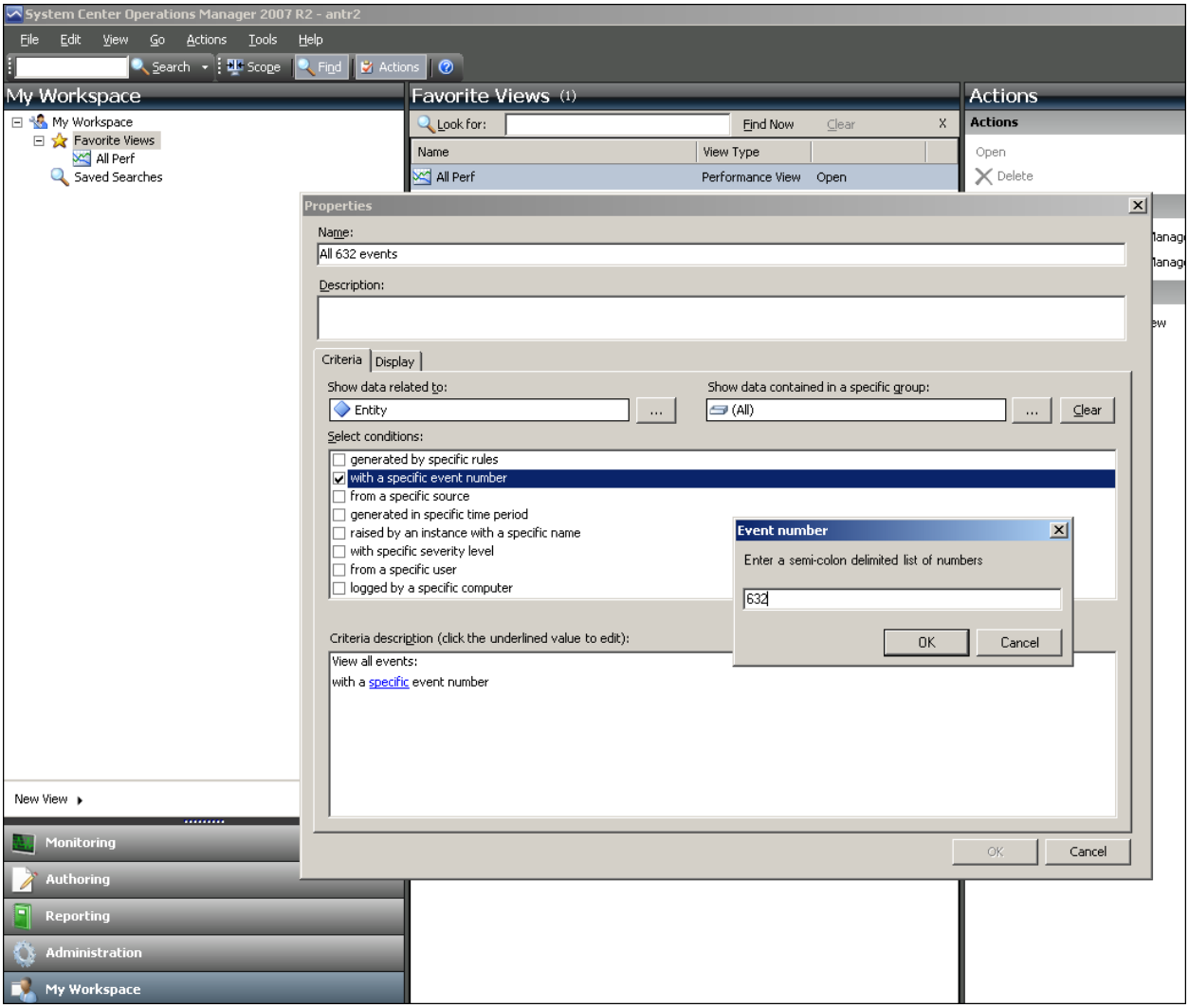


3) Give the view a name. In our case, a name like 'All 632 events' is relevant.

4) Place a check in the 'with a specific event number' criteria

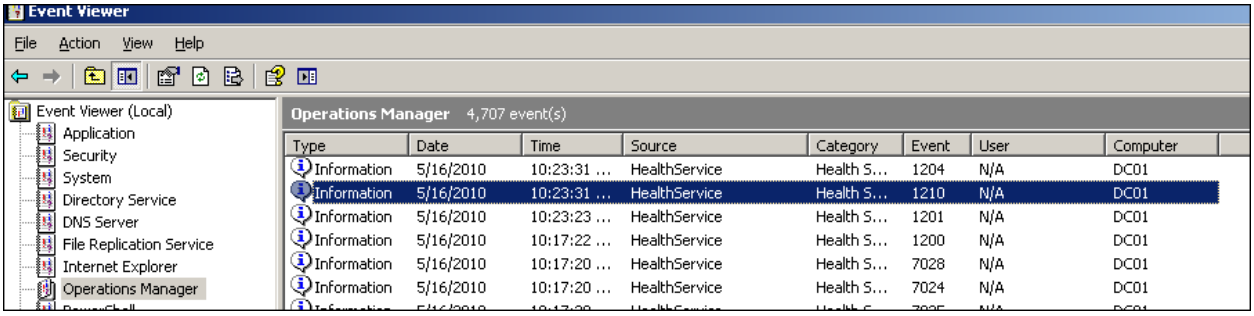
5) Click the 'specific' hyperlink that appears in the criteria description box.

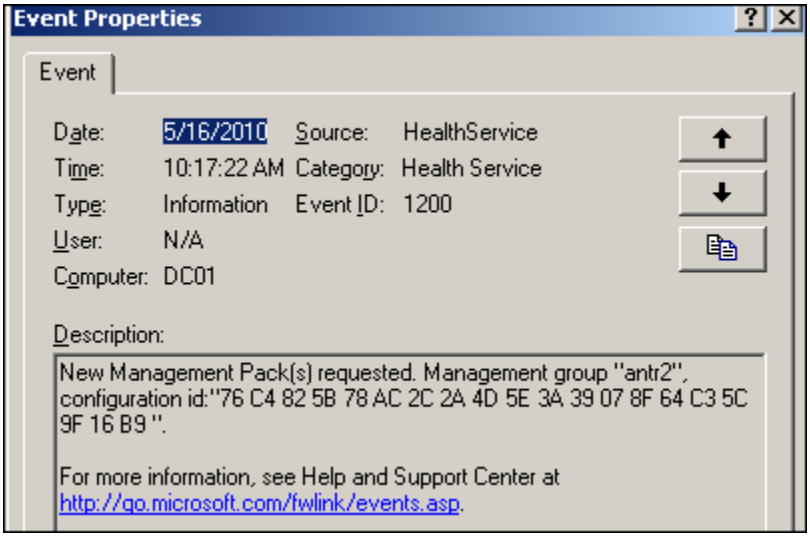
6) Type the event ID that you want to display (in our case 632) and click OK:

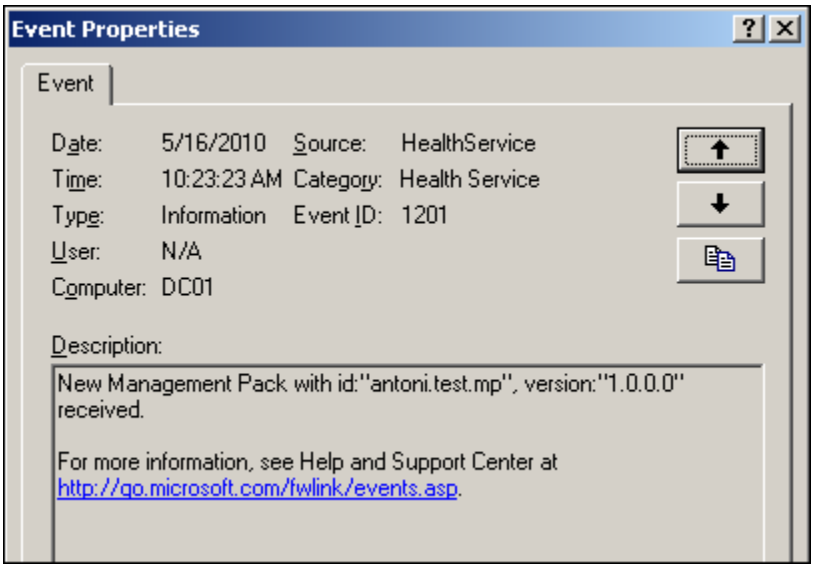


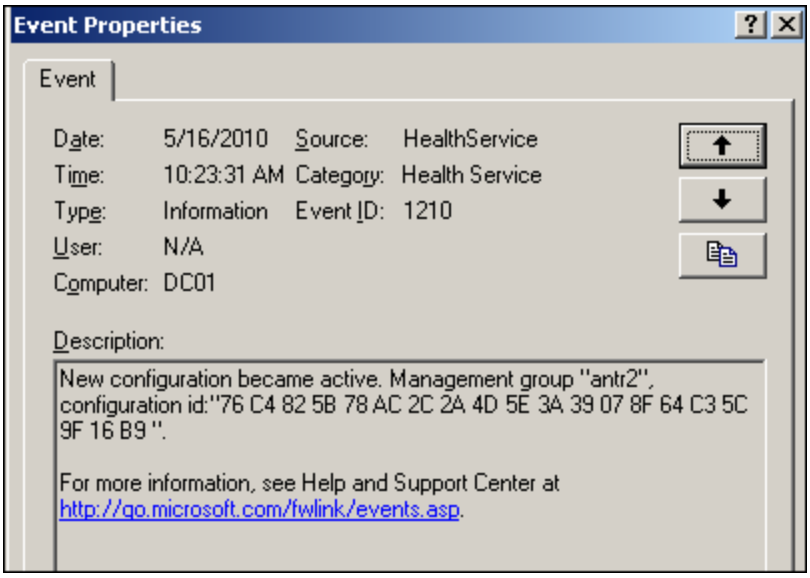
7) Click OK in the Properties dialog

8) Verify that the new rule makes it down to the computer on which you intend the event to be collected from by looking for a series of 1200, 1201 and 1210 events In the Operations Manager event log (The 1201 event should show the name of the management pack that you created the rule in):

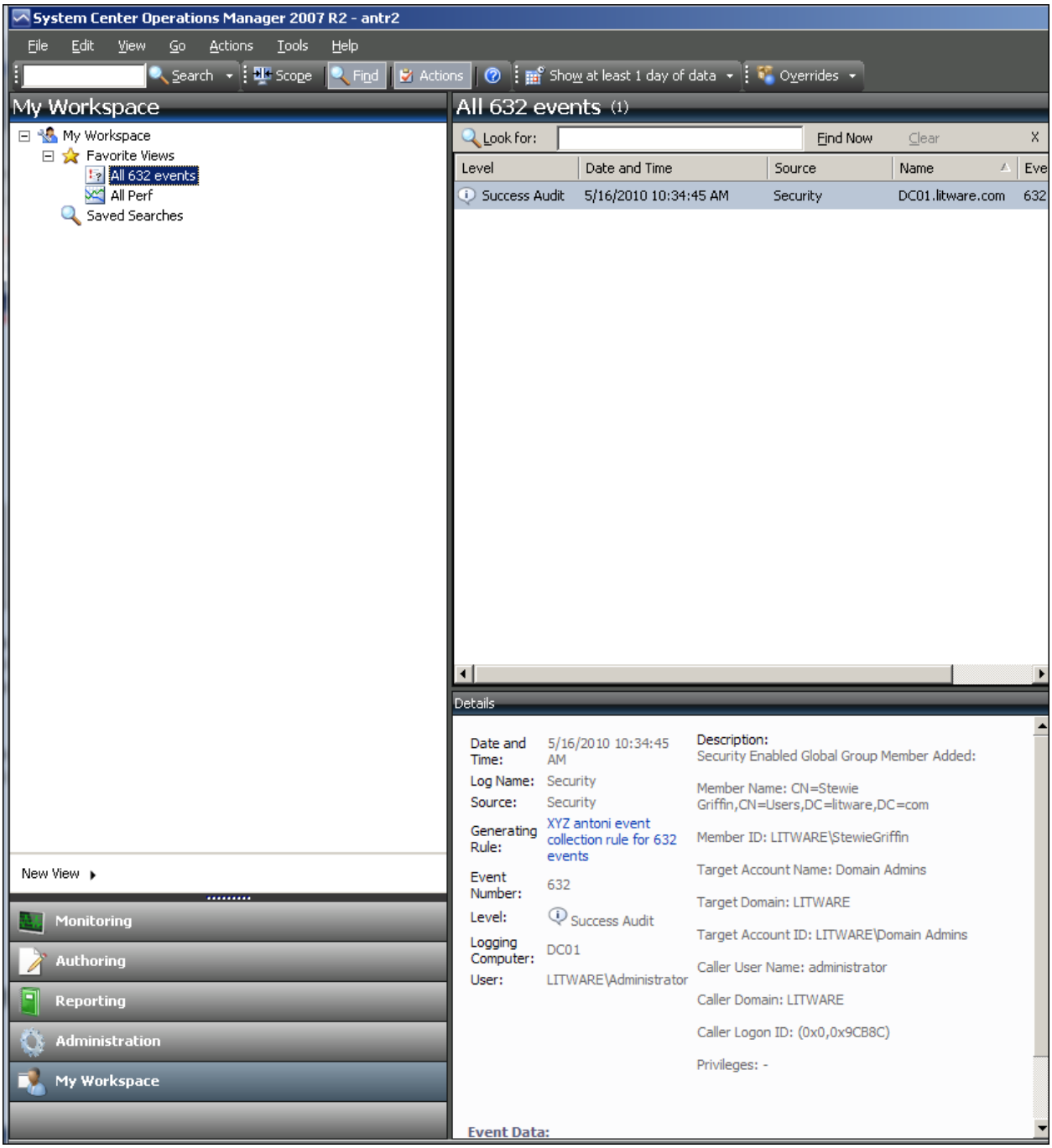

Event Viewer
File Action View Help
Event Viewer (Local)
Application
Security
System
Directory Service
DNS Server
File Replication Service
Internet Explorer
Operations Manager
Operations Manager 4,707 event(s)
Type Date Time Source Category Event User Computer
Information 5/16/2010 10:23:31 ... HealthService Health S... 1204 N/A DC01
Information 5/16/2010 10:23:31 ... HealthService Health S... 1210 N/A DC01
Information 5/16/2010 10:23:23 ... HealthService Health S... 1201 N/A DC01
Information 5/16/2010 10:17:22 ... HealthService Health S... 1200 N/A DC01
Information 5/16/2010 10:17:20 ... HealthService Health S... 7028 N/A DC01
Information 5/16/2010 10:17:20 ... HealthService Health S... 7024 N/A DC01


Event Properties
Event
Date: 5/16/2010 Source: HealthService
Time: 10:17:22 AM Category: Health Service
Type: Information Event ID: 1200
User: N/A
Computer: DC01
Description:
New Management Pack(s) requested. Management group "antr2", configuration id:"76 C4 82 5B 78 AC 2C 2A 4D 5E 3A 39 07 8F 64 C3 5C 9F 16 B9 ".
For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.


Event Properties
Event
Date: 5/16/2010 Source: HealthService
Time: 10:23:23 AM Category: Health Service
Type: Information Event ID: 1201
User: N/A
Computer: DC01
Description:
New Management Pack with id:"antoni.test.mp", version:"1.0.0.0" received.
For more information, see Help and Support Center at
http://go.microsoft.com/fwlink/events.asp.



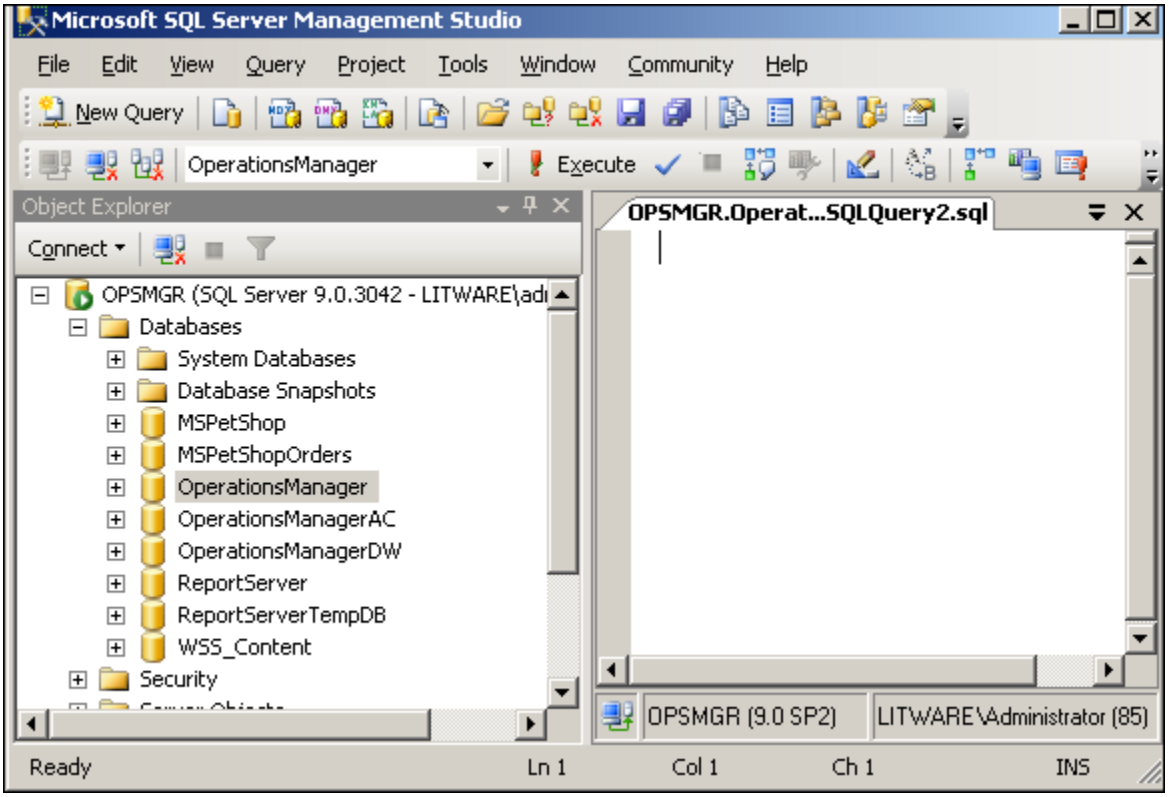
9) Repro the scenario so that an event is generated on the computer and collected in operations Manager. In this example we added a user to domain admins and then saw the following event:



Task 3 – Query the DB to find which the table the events are being stored in and then query the appropriate table to get the event parameters.

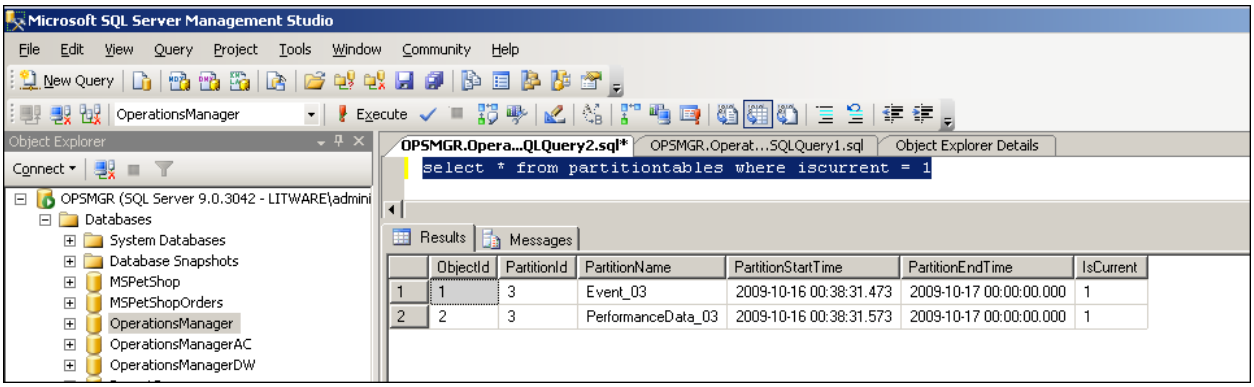
1) Open SQL Management Studio, Connect to the SQL Server hosting the OperationsManager Database (this is the live operational DB where all the data presented in the Operator's console is stored)

2) Click the 'New Query' button and change the DB dropdown from 'Master' to 'OperationsManager'



3) Type and execute the following Query:

Select * from PartitionTables where iscurrent = 1

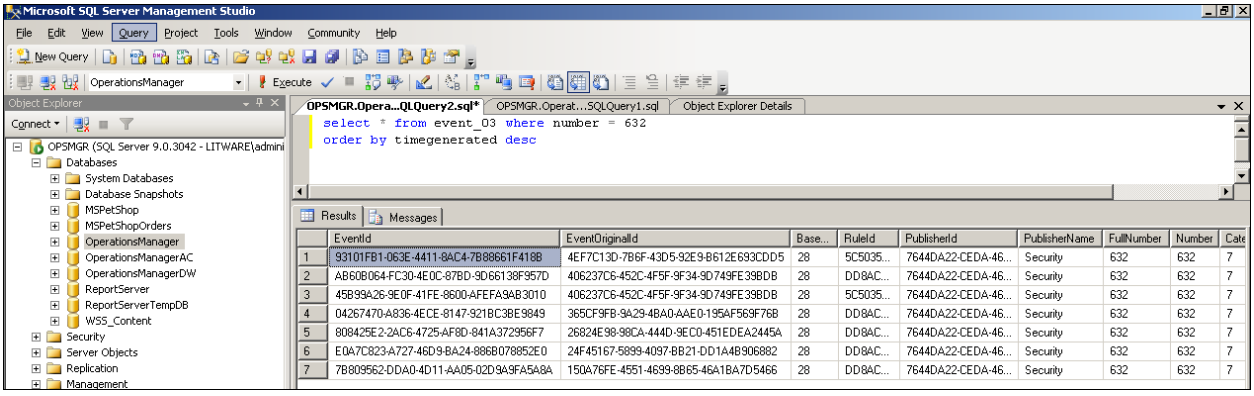


4) Note the name of the Event table listed, in the above example it is Event_03.

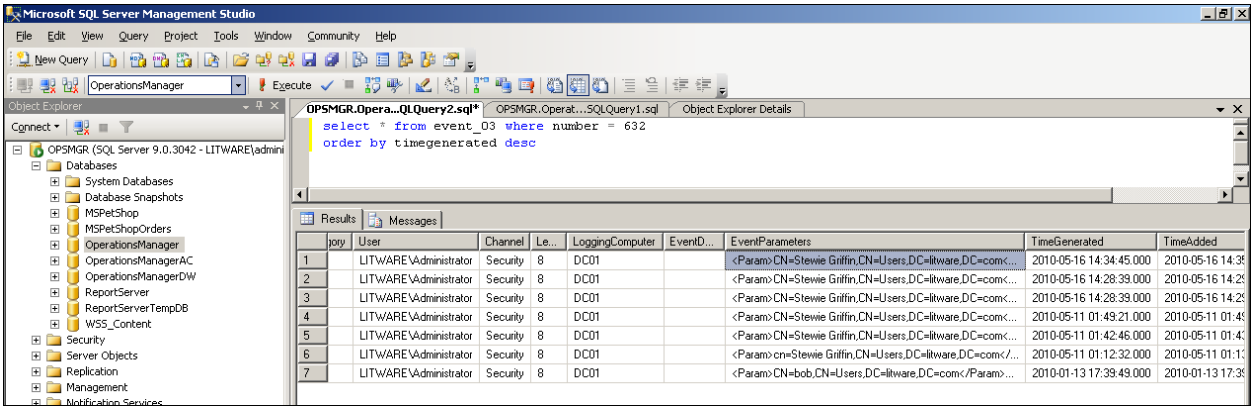
NOTE: This is the table that OperationsManager is writing all its collected event data to today. Tomorrow it will be writing Event_04, and then Event_05 the next day and so on. The tables are structured in this manner for more effective grooming.

5) Type and execute the following query (replacing Event_03) with the event table name returned by the previous query:

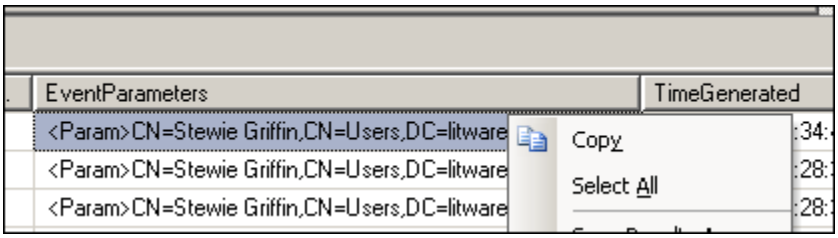
Select * from event_03 where number = 632 order by timegenerated desc



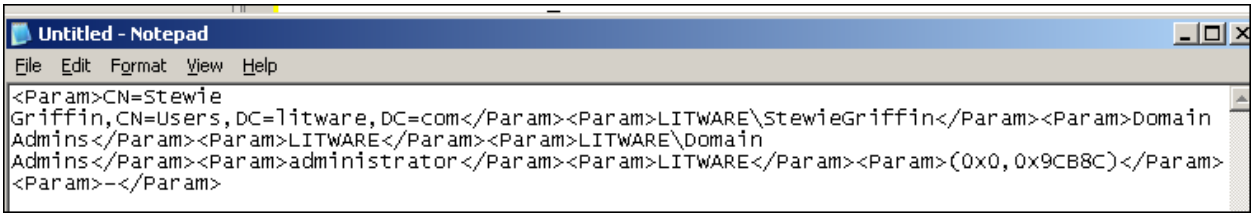
6) The most recently collected event will be shown at the top. In the results, scroll across to the EventParameters field:



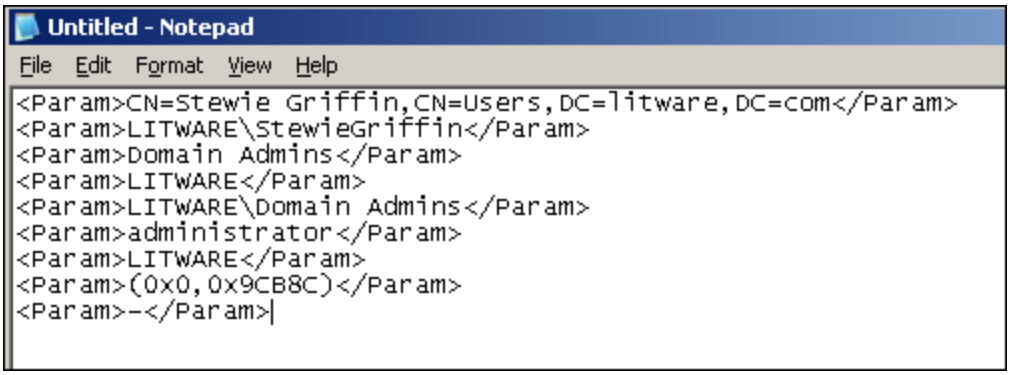
7) Click the EventParameters field and copy out the contents:



8) Open notepad and paste the contents there:



9) Rearrange the contents of the notepad file, so a parameter is shown on each line:



The above is a numerically ordered list of parameters. So for instance:

Parameter 1 is the distinguished username

Parameter 2 is the Username

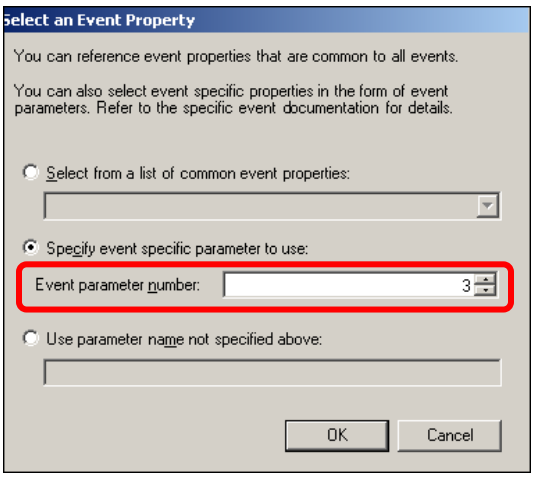
Parameter 3 is the Group name that the user was added to

Parameter 4 in the Domain Name

Parameter 5 is the Domain\Group Name

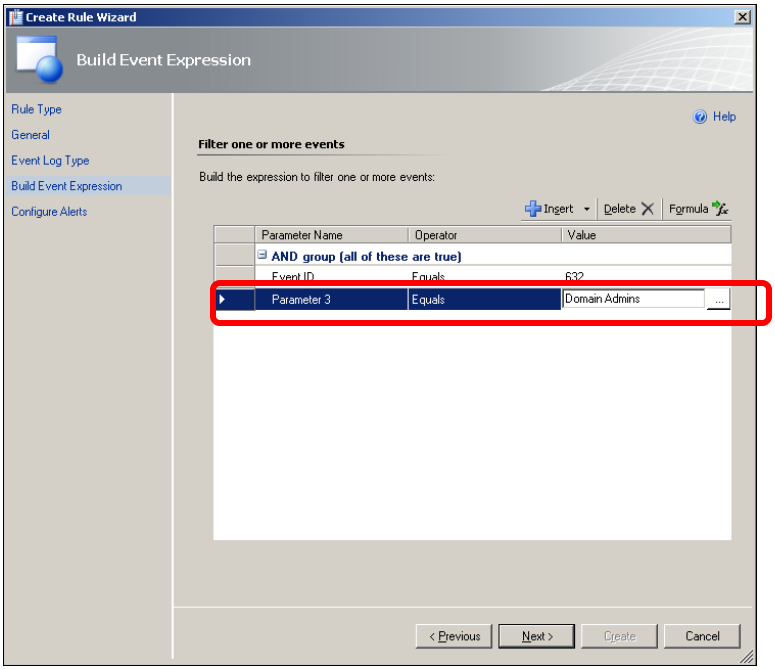
Parameter 6 is the user that made the change.

In Operations Manager, these parameters can be used to create a more granular event collection rule or alert generating rule as outlined in Section E of this document:



16) In the operator field on the second line choose Equals

17) In the value field on the second line, type Domain Admins (Case-sensitive):



Appendix - Best Practices:

Management Pack / Override Best Practice:

First of all, the golden rule is please, please, please do not store anything (including overrides) in the default management pack.

Another important best practice is to use a naming convention. So whenever you create a new management pack, rule, monitor, group or anything, I would recommend that you always prefix it with something like HRS.

This makes it a lot easier to find anything that you've created in the console.

An MP that you download from microsoft.com like AD / Exchange / SQL are all sealed management packs. This means that you cannot change their contents in any way. If you look at the 'Monitoring' view in the console and the folders, you will see a lot of them have padlocks next to them and you will not be able to right-click and create new views within the folders, because they are sealed MPs. Likewise if you click on an alert and then click rule or monitor properties in the lower alert details pane, in the rule or monitor properties, you will see that all the fields are grayed out and you cannot change anything here.

So the only way you can customize a rule or a monitor such as whether it is enabled or disabled, or a threshold for example, is by creating an override in an Unsealed Custom Management Pack.

When you go to override, you will see the 'Default Management Pack' as the option and if you click the dropdown, it will show other available unsealed MPs and also gives you the option to create a new one.

Our recommended best practice is that for each sealed MP (let's say you have SQL, AD and Exchange), is that you have an unsealed MP, so in this example you would also have a MyCompany Custom SQL MP, MyCompany Custom AD MP, MyCompany Custom Exchange MP and if you are overriding a rule in the sealed SQL MP, you store the override in the MyCompany Custom SQL MP.

The reason for this and also the reason you don't store anything in the default MP, is that when you create an override, you create a dependency between the sealed MP and the unsealed MP.

So let's say you didn't know this best practice and had stored all your overrides (for SQL sealed MP, AD Sealed MP, Exchange Sealed MP etc) in the default MP. If you then tried to remove one of those sealed

MPs (let's say SQL for example) from the console, it will prevent you from doing so, as it will say that you have dependencies in the default management pack. In order to resolve this, you would need to remove all the SQL overrides from the default MP before you can remove the sealed SQL MP. Another way of resolving it, would be to delete the default management pack, but this is not recommended because if you do that, you lose the top level views under monitoring. You can get them back, but for this reason, we suggest that you don't get into the situation where you need to delete the default MP, if you can avoid it.

If you have followed best practice and have all your SQL overrides in your MyCompany Custom SQL MP, that means if you needed to remove the sealed SQL MP one day, then the only MP you need to remove first (that will have all dependent overrides) is the MyCompany Custom SQL MP, and you don't have to go anywhere near the default MP or any other management pack.

One tip here too, when you right click an alert to override the rule / monitor, and you see the flash out menu to either 'disable / enable' or override, NEVER use the disable / enable flash out menu as this will create an override to enable / disable and store it in the default management pack without giving you the choice of which MP you'd like to store it in. So always use the 'override' flash-out menu instead (even if you are just enabling ' disabling) as this will allow you to control the MP the override is stored in. Or alternatively, go into the rule / monitor properties and use the overrides tab there.