Securing Reporting in Operations Manager 2007

Scoping user roles to restrict report access

Michael Betts
http://www.momanswers.net

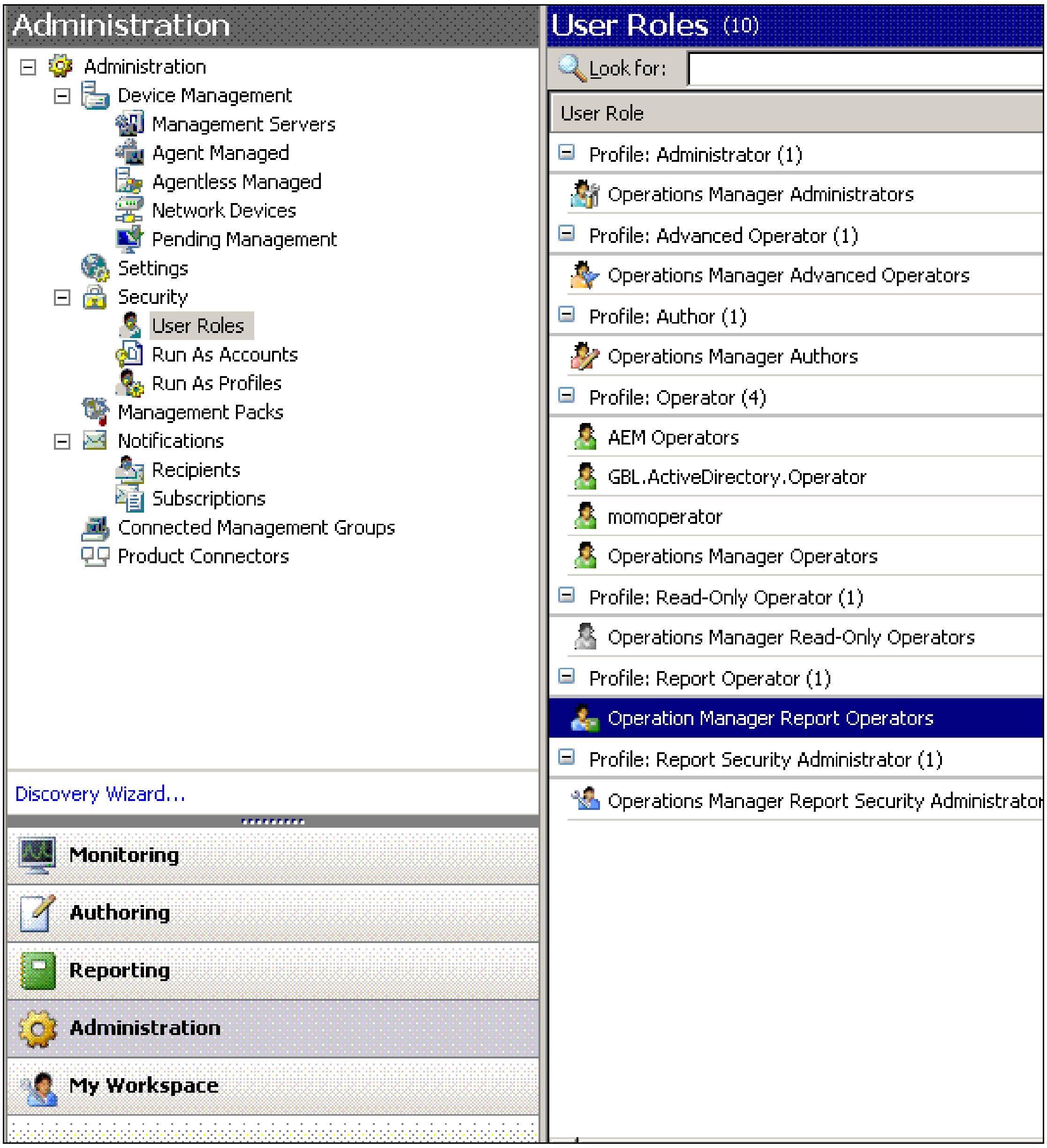
July 2007
Version 1.0

By default in OpsMgr once you are a member of the **Report Operator** role you have access to the OpsMgr **Reports**.

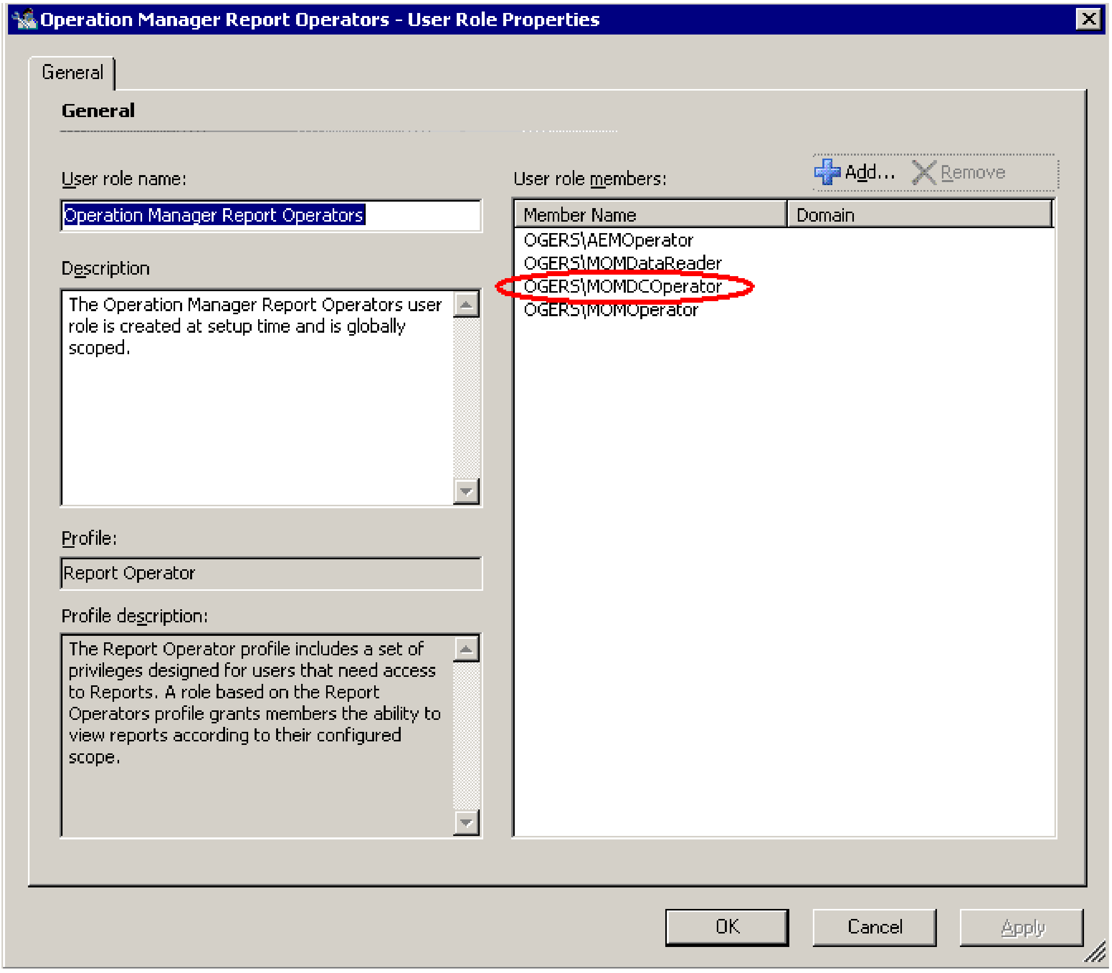
However you have access to *all* reports, which could potentially mean you have spent all that time making sure AD Operators can only see AD alerts and then the whole model collapses when they look at the Reporting utility and they can happily see what's been going on in the Exchange or SQL world.

So how do we put a stop to this? Well, the OpsMgr help is useful in that it has step-by-step's as to how report security is set however it does miss out an important step, so let's go through it from the start.

First up, your Report Operator has by default access to all reports. You set the Report Operator role in the User Interface Administration section:


Administration
Administration
Device Management
Management Servers
Agent Managed
Agentless Managed
Network Devices
Pending Management
Settings
Security
User Roles
Run As Accounts
Run As Profiles
Management Packs
Notifications
Recipients
Subscriptions
Connected Management Groups
Product Connectors
Discovery Wizard...
Monitoring
Authoring
Reporting
Administration
My Workspace
User Roles (10)
Look for:
User Role
Profile: Administrator (1)
Operations Manager Administrators
Profile: Advanced Operator (1)
Operations Manager Advanced Operators
Profile: Author (1)
Operations Manager Authors
Profile: Operator (4)
AEM Operators
GBL.ActiveDirectory.Operator
momoperator
Operations Manager Operators
Profile: Read-Only Operator (1)
Operations Manager Read-Only Operators
Profile: Report Operator (1)
Operation Manager Report Operators
Profile: Report Security Administrator (1)
Operations Manager Report Security Administrator

And give the membership of this according to who can view all reports:



General

User role name: Operation Manager Report Operators

Description: The Operation Manager Report Operators user role is created at setup time and is globally scoped.

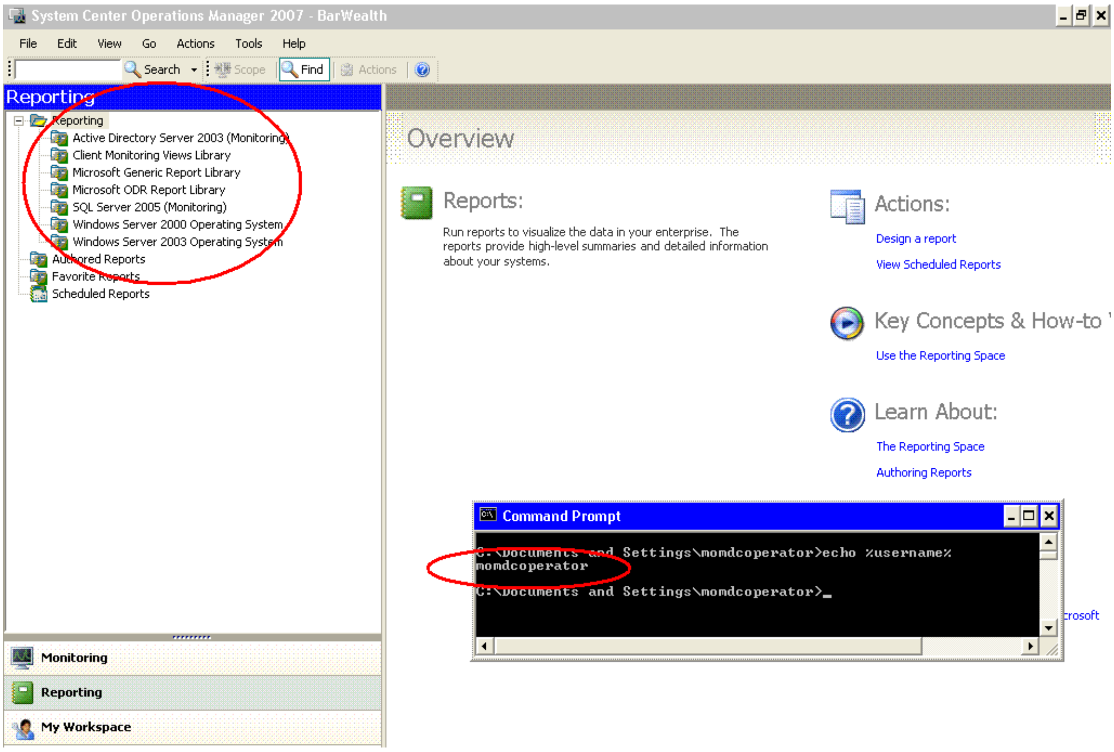
Profile: Report Operator

Profile description: The Report Operator profile includes a set of privileges designed for users that need access to Reports. A role based on the Report Operators profile grants members the ability to view reports according to their configured scope.

User role members:

Member Name	Domain
OGERS\AEMOperator	
OGERS\MOMDataReader	
OGERS\MOMDCOperator	
OGERS\MOMOperator	

This now means that the users in this group, in this case MOMDCOperator is highlighted, have access to the all reports when they log on and use the Reporting function:



Run reports to visualize the data in your enterprise. The reports provide high-level summaries and detailed information about your systems.

```
C:\Documents and Settings\momdcoperator>echo %username%
momdcoperator

C:\Documents and Settings\momdcoperator>_
```

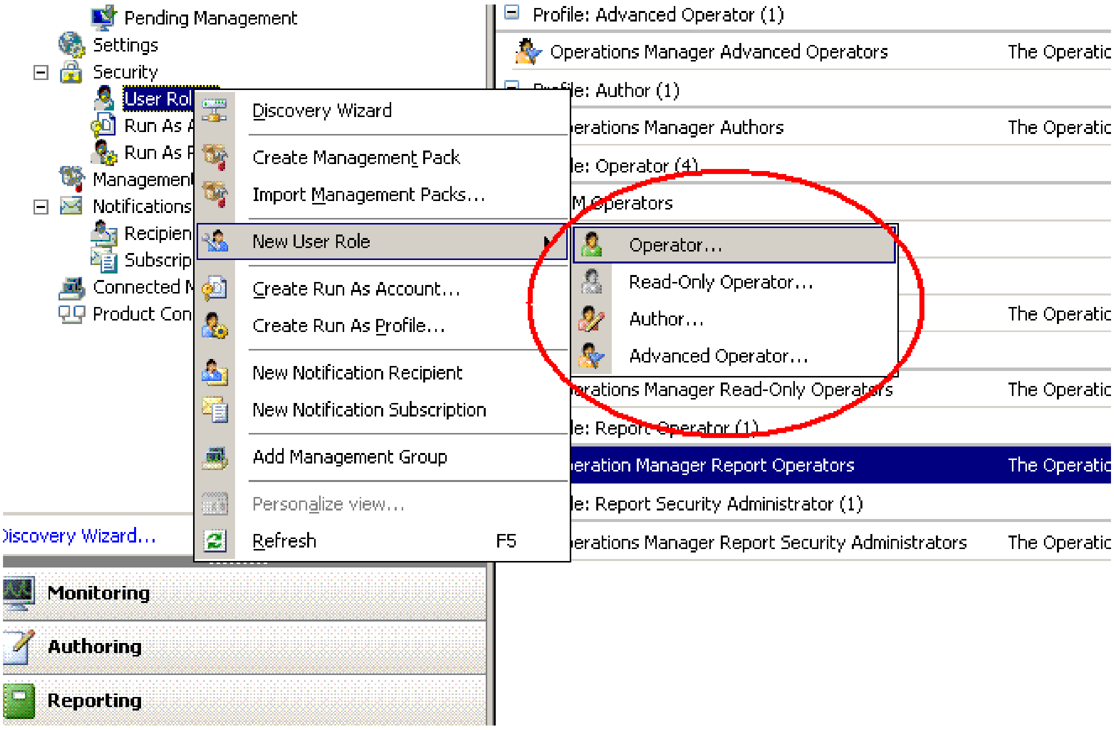
So how do we secure this so that MOMDCOperator can only see the Active Directory Reports?

Well, in the OpsMgr help it does give you the step-by-step text on how to secure reports, under the section "How to Set Permissions on a Report Using Command Shell in Operations Manager 2007".

This page describes how the security on reports is set using the GUID's of the Roles in Operations Manager. So for example, the Operations Manager Administrators has a relating GUID within Operations Manager and if you set the security of a report to this GUID then that report will then become visible. By default all reports are visible to Operations Manager Administrator and Operations Manager Report Viewers.

There is a line of PowerShell, which we will come to in a minute, which demonstrates how to output the GUID's of all currently known MOM Roles you may have created which you can then apply to the reports. Crucially however, there is a piece of extra information you need otherwise things can become a bit unclear: You can apply security not to the GUID's of *any* roles you have created in OpsMgr but only to roles that are of the type **Report Operator**. In other words, the standard **Report Operator** has access to all reports but creating another **Operator Role**, or **Author Role** or **Advanced Operator Role** and trying to apply that GUID to the report security will have no effect: you need to create another **Report Operator Role**, populate its membership and then assign that the necessary permission.

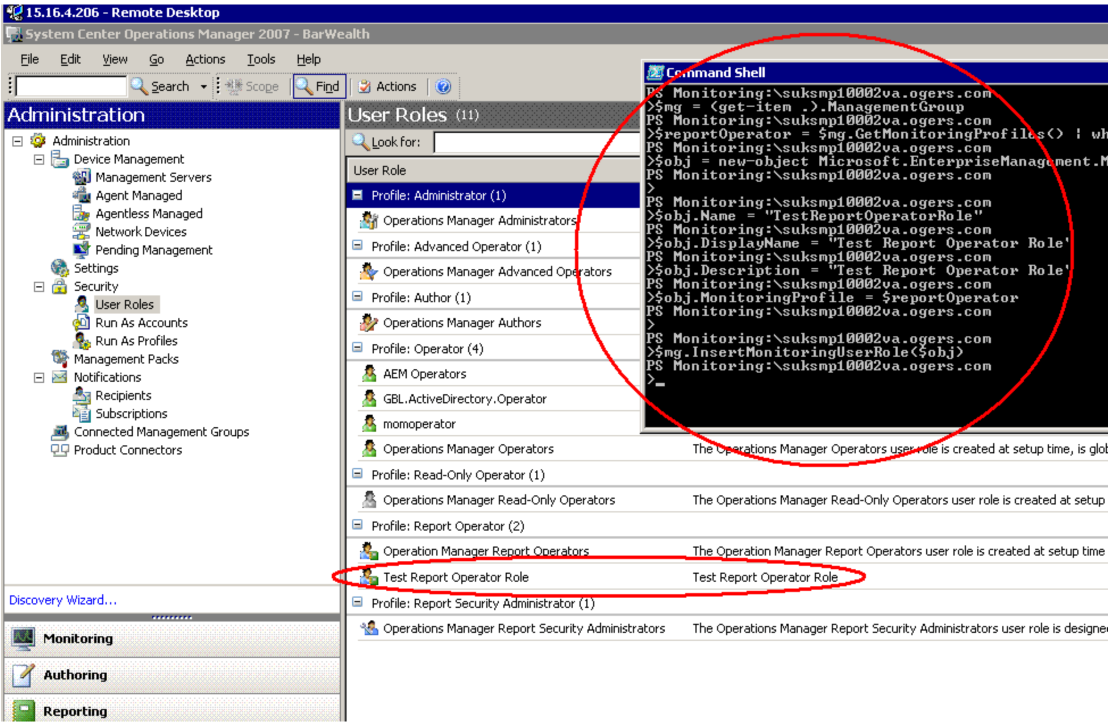
So what's so hard about that? Well, nothing, except that it's not in the GUI:



So how do we create one? Well you have to use PowerShell. The PowerShell script is as follows (many thanks to Microsoft PSS, this script is from them who responded very promptly when I raised this issue with them):

```
$mg = (get-item .).ManagementGroup
$reportOperator = $mg.GetMonitoringProfiles() | where {$_.Name -eq "ReportOperator"}
$obj = new-object
Microsoft.EnterpriseManagement.Monitoring.Security.MonitoringUserRole

$obj.Name = "TestReportOperatorRole"
$obj.DisplayName = "Test Report Operator Role"
$obj.Description = "Test Report Operator Role"
$obj.MonitoringProfile = $reportOperator

$mg.InsertMonitoringUserRole($obj)
```

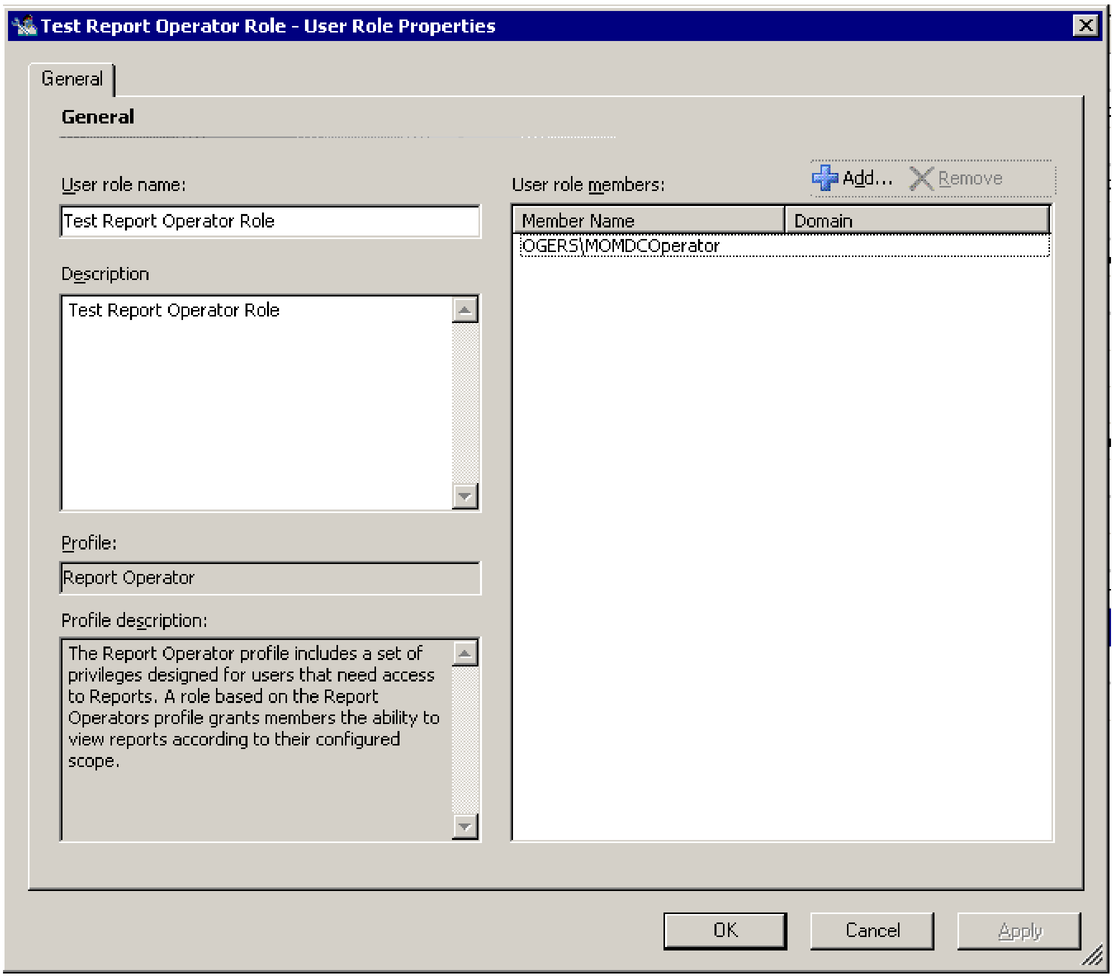
This will create a new Report Viewer role called “TestReportOperatorRole” once it is run (either run it a line at a time or save it as (for example) “CustomRole.ps1” script and run it from the PowerShell command prompt):



```
PS Monitoring:\suksmp10002va.ogers.com
>$mg = (get-item .).ManagementGroup
PS Monitoring:\suksmp10002va.ogers.com
>$reportOperator = $mg.GetMonitoringProfiles() | wh
PS Monitoring:\suksmp10002va.ogers.com
>$obj = new-object Microsoft.EnterpriseManagement.M
PS Monitoring:\suksmp10002va.ogers.com
>
PS Monitoring:\suksmp10002va.ogers.com
>$obj.Name = "TestReportOperatorRole"
PS Monitoring:\suksmp10002va.ogers.com
>$obj.DisplayName = "Test Report Operator Role"
PS Monitoring:\suksmp10002va.ogers.com
>$obj.Description = "Test Report Operator Role"
PS Monitoring:\suksmp10002va.ogers.com
>$obj.MonitoringProfile = $reportOperator
PS Monitoring:\suksmp10002va.ogers.com
>
PS Monitoring:\suksmp10002va.ogers.com
>$mg.InsertMonitoringUserRole($obj)
PS Monitoring:\suksmp10002va.ogers.com
>_
```

User Role	
Profile: Administrator (1)	
Operations Manager Administrators	
Profile: Advanced Operator (1)	
Operations Manager Advanced Operators	
Profile: Author (1)	
Operations Manager Authors	
Profile: Operator (4)	
AEM Operators	
GBL.ActiveDirectory.Operator	
momoperator	
Operations Manager Operators	The Operations Manager Operators user role is created at setup time, is glob
Profile: Read-Only Operator (1)	
Operations Manager Read-Only Operators	The Operations Manager Read-Only Operators user role is created at setup
Profile: Report Operator (2)	
Operation Manager Report Operators	The Operation Manager Report Operators user role is created at setup time
Test Report Operator Role	Test Report Operator Role
Profile: Report Security Administrator (1)	
Operations Manager Report Security Administrators	The Operations Manager Report Security Administrators user role is designe

With this new role created we can now start securing our reports. Firstly populate this group with the necessary users, in this case I am going to put my MOMDCOperator user in it:



Test Report Operator Role - User Role Properties

General

General

User role name: Test Report Operator Role

Description: Test Report Operator Role

Profile: Report Operator

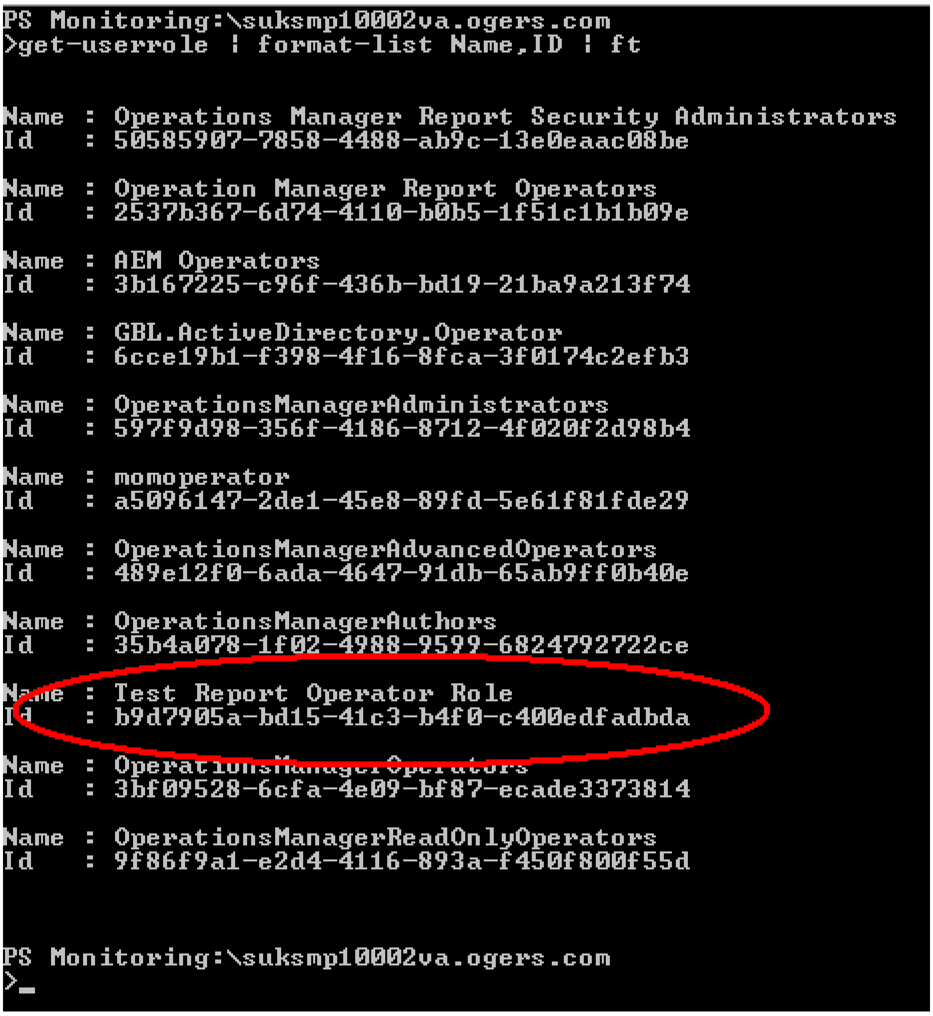
Profile description: The Report Operator profile includes a set of privileges designed for users that need access to Reports. A role based on the Report Operators profile grants members the ability to view reports according to their configured scope.

User role members:

Member Name	Domain
OGERS\MOMDCOperator	

Then use the necessary PowerShell cmdlet to pull back all the current GUIDS:

```
Get-userrole | format-List Name, ID
```

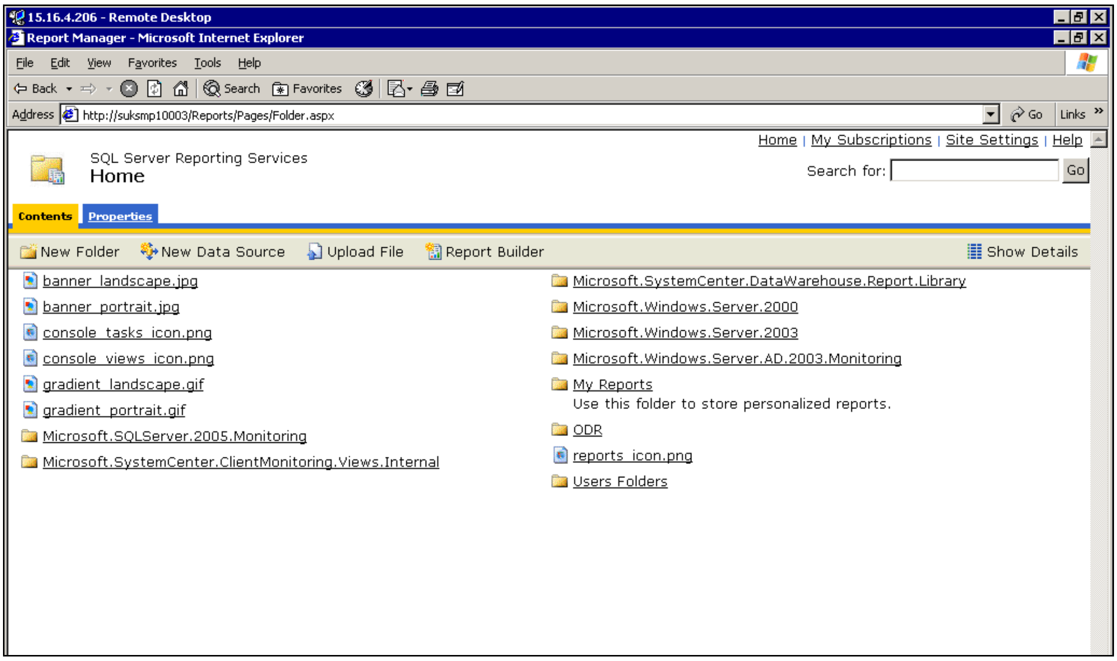


```
PS Monitoring:\suksmp10002va.ogers.com
>get-userrole | format-list Name,ID | ft


Name : Operations Manager Report Security Administrators
Id   : 50585907-7858-4488-ab9c-13e0eaac08be

Name : Operation Manager Report Operators
Id   : 2537b367-6d74-4110-b0b5-1f51c1b1b09e

Name : AEM Operators
Id   : 3b167225-c96f-436b-bd19-21ba9a213f74

Name : GBL.ActiveDirectory.Operator
Id   : 6cce19b1-f398-4f16-8fca-3f0174c2efb3

Name : OperationsManagerAdministrators
Id   : 597f9d98-356f-4186-8712-4f020f2d98b4

Name : momoperator
Id   : a5096147-2de1-45e8-89fd-5e61f81fde29

Name : OperationsManagerAdvancedOperators
Id   : 489e12f0-6ada-4647-91db-65ab9ff0b40e

Name : OperationsManagerAuthors
Id   : 35b4a078-1f02-4988-9599-6824792722ce

Name : Test Report Operator Role
Id   : b9d7905a-bd15-41c3-b4f0-c400edfadbda

Name : OperationsManagerOperators
Id   : 3bf09528-6cfa-4e09-bf87-ecade3373814

Name : OperationsManagerReadOnlyOperators
Id   : 9f86f9a1-e2d4-4116-893a-f450f800f55d



PS Monitoring:\suksmp10002va.ogers.com
>_
```

Now we are nearly there. Next we need to get to the **SQL Reporting Services** box itself and go and look at the reports. Type in the URL:

http://<RSName>/Reports

(Where <RSName> is the Reporting Server computer name.)


15.16.4.206 - Remote Desktop
Report Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Home | My Subscriptions | Site Settings | Help
Search for: Go
Contents Properties
New Folder New Data Source Upload File Report Builder Show Details

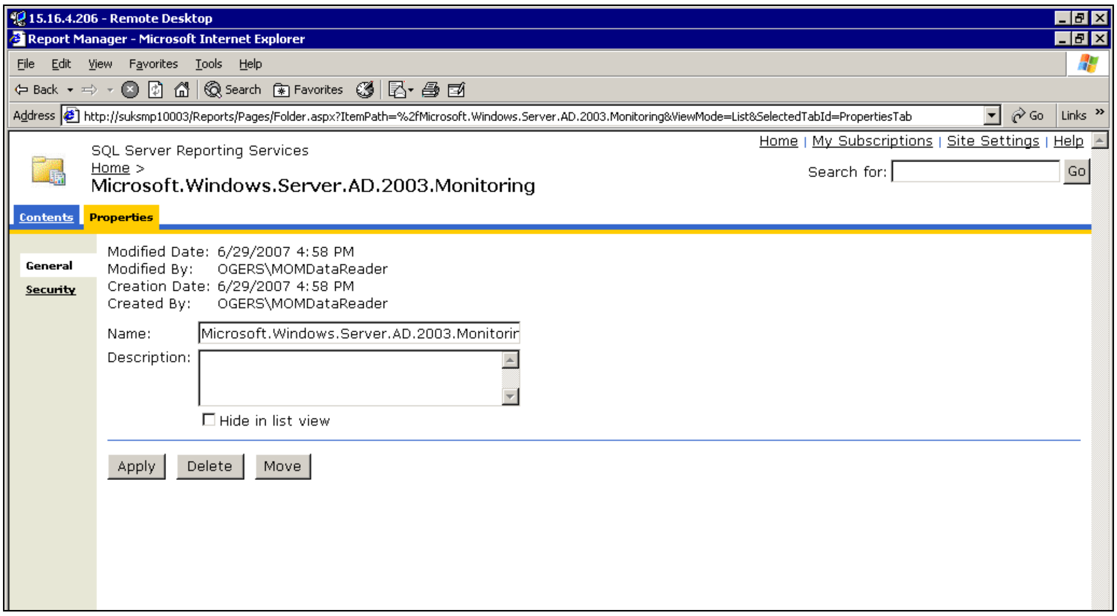
Address: http://suksmp10003/Reports/Pages/Folder.aspx

SQL Server Reporting Services
Home

- banner_landscape.jpg
- banner_portrait.jpg
- console_tasks_icon.png
- console_views_icon.png
- gradient_landscape.gif
- gradient_portrait.gif
- Microsoft.SQLServer.2005.Monitoring
- Microsoft.SystemCenter.ClientMonitoring.Views.Internal
- Microsoft.SystemCenter.DataWarehouse.Report.Library
- Microsoft.Windows.Server.2000
- Microsoft.Windows.Server.2003
- Microsoft.Windows.Server.AD.2003.Monitoring
- My Reports
  Use this folder to store personalized reports.
- ODR
- reports_icon.png
- Users Folders

Next select the **Report Category** you are interested in, such as **Microsoft.Windows.Server.AD.2003.Monitoring** and select **Properties**.

You should now have this screen:


15.16.4.206 - Remote Desktop
Report Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go Links
Home | My Subscriptions | Site Settings | Help
Search for: Go
Contents Properties
General
Security
Apply Delete Move

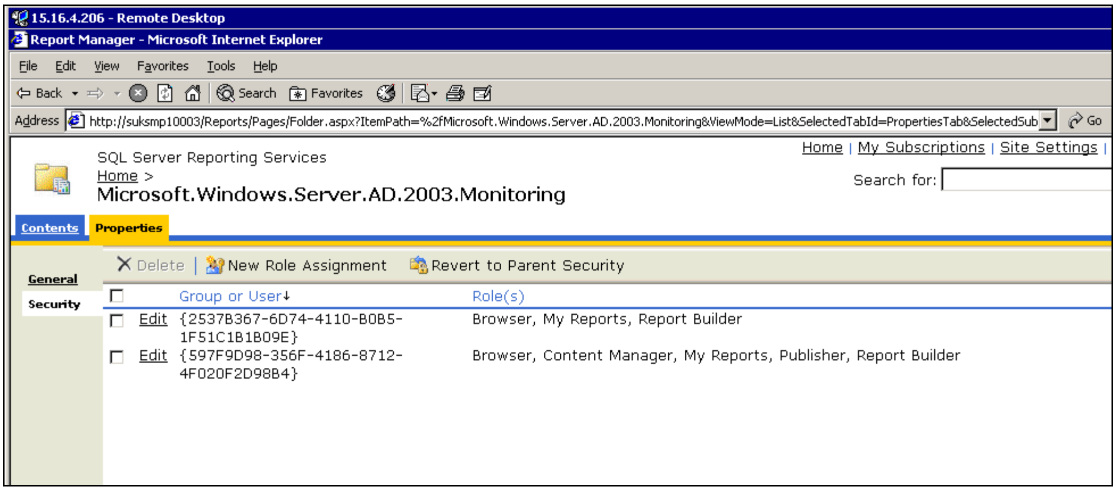
Address: http://suksmp10003/Reports/Pages/Folder.aspx?ItemPath=%2fMicrosoft.Windows.Server.AD.2003.Monitoring&ViewMode=List&SelectedTabId=PropertiesTab

SQL Server Reporting Services
Home >
Microsoft.Windows.Server.AD.2003.Monitoring

Modified Date: 6/29/2007 4:58 PM
Modified By: OGERS\MOMDataReader
Creation Date: 6/29/2007 4:58 PM
Created By: OGERS\MOMDataReader

Name: Microsoft.Windows.Server.AD.2003.Monitorir
Description:
☐ Hide in list view

If you select **Security** you can see the security on the folder and if you examine the GUID list that the PowerShell command returned you will identify the two GUID’s as the one for **Operations Manager Administrators** and the one for **Operations Manager Report Viewers**:


15.16.4.206 - Remote Desktop
Report Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://suksmp10003/Reports/Pages/Folder.aspx?ItemPath=%2fMicrosoft.Windows.Server.AD.2003.Monitoring&ViewMode=List&SelectedTabId=PropertiesTab&SelectedSub
Home | My Subscriptions | Site Settings
Search for:
SQL Server Reporting Services
Home >
Contents
Properties
General
Security
Delete
New Role Assignment
Revert to Parent Security

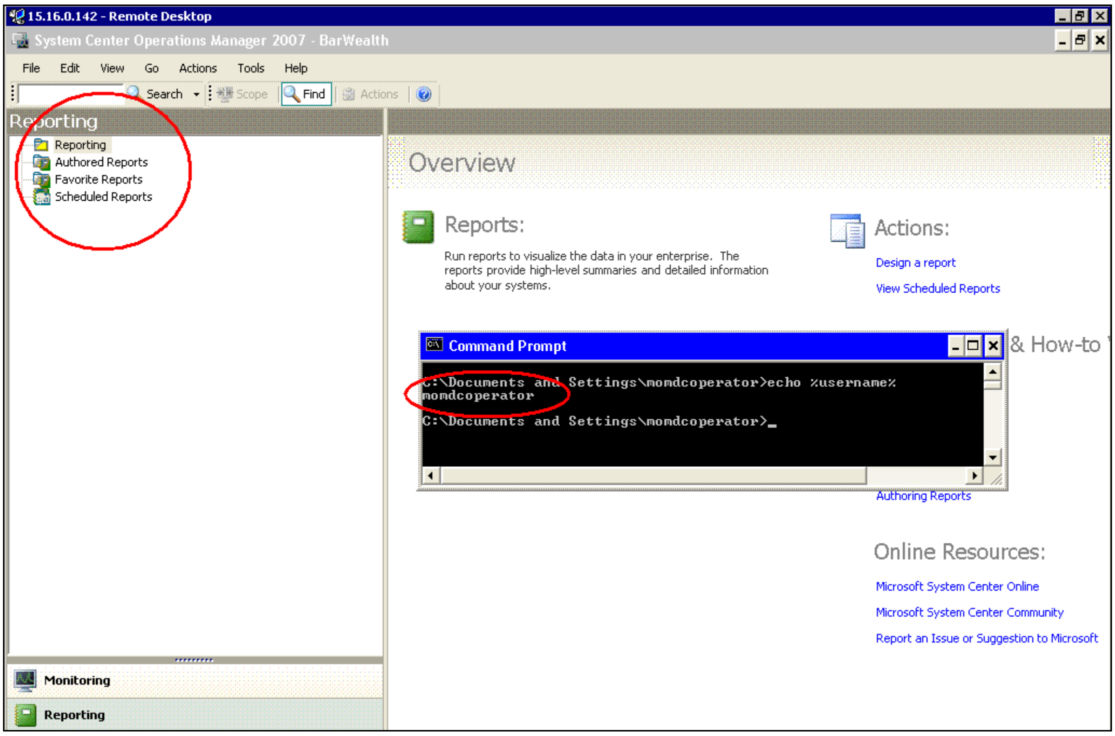
Microsoft.Windows.Server.AD.2003.Monitoring

□		Group or User↓	Role(s)
□	Edit	{2537B367-6D74-4110-B0B5-1F51C1B1B09E}	Browser, My Reports, Report Builder
□	Edit	{597F9D98-356F-4186-8712-4F020F2D98B4}	Browser, Content Manager, My Reports, Publisher, Report Builder

Now it isn't just possible to remove Report Viewers from the root of all reports, you get an **access denied** when you try and launch the reporting in that case. So in this situation, the most sensible way to do it is now to go through all the folders you want one hidden one at a time and remove the GUID that represents the **Operations Manager Report Operators** role (use the PowerShell command mentioned earlier to see what that GUID is).

This is done simply by selecting the GUID and clicking Delete.

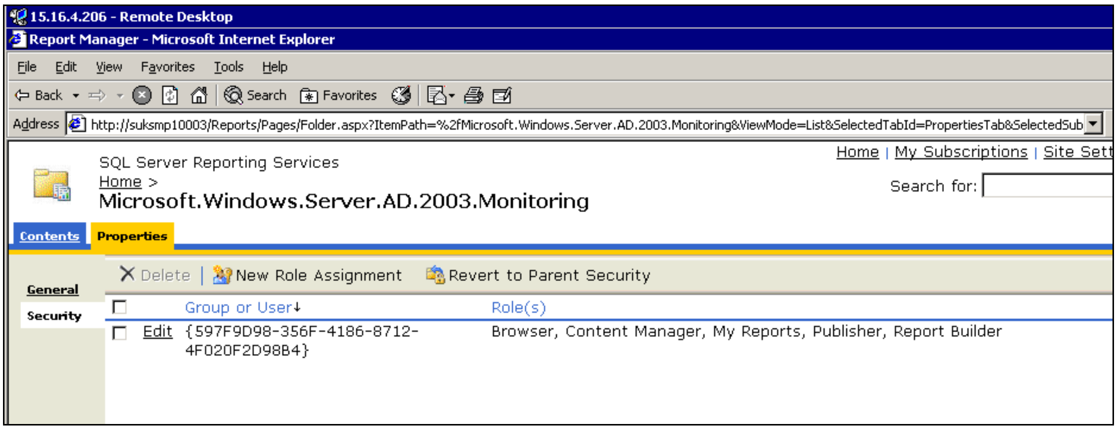
Once I have removed it from all my reports the reporting screen now looks like this for the MOMDCOperator User:



Run reports to visualize the data in your enterprise. The reports provide high-level summaries and detailed information about your systems.

```
C:\Documents and Settings\momdcoperator>echo %username%
momdcoperator

C:\Documents and Settings\momdcoperator>_
```

Now we need to go into the Report Server again, select the **Microsoft.Windows.Server.AD.2003.Monitoring** report folder again, go into the **Properties** and it is currently now set to only the GUID of **MOM Administrators**:



15.16.4.206 - Remote Desktop

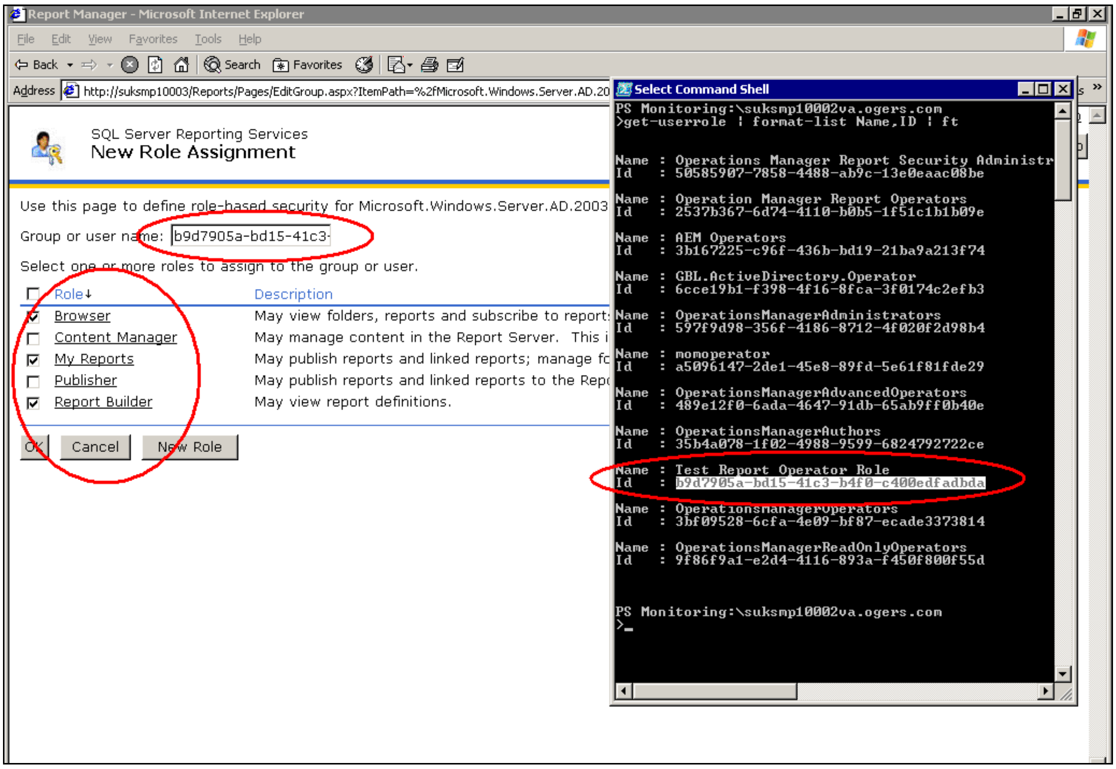
Report Manager - Microsoft Internet Explorer

Address http://suksmp10003/Reports/Pages/Folder.aspx?ItemPath=%2fMicrosoft.Windows.Server.AD.2003.Monitoring&ViewMode=List&SelectedTabId=PropertiesTab&SelectedSub

SQL Server Reporting Services
Home >
Microsoft.Windows.Server.AD.2003.Monitoring

		Group or User	Role(s)
□	Edit	{597F9D98-356F-4186-8712-4F020F2D98B4}	Browser, Content Manager, My Reports, Publisher, Report Builder

Now we add the GUID for the new **Test Report Operator Role** by adding the GUID in by selecting **New Role Assignment** and giving them the **Browser, My Reports** and **Report Builder** permissions:



Report Manager - Microsoft Internet Explorer

Address http://suksmp10003/Reports/Pages/EditGroup.aspx?ItemPath=%2fMicrosoft.Windows.Server.AD.20

SQL Server Reporting Services
New Role Assignment

Use this page to define role-based security for Microsoft.Windows.Server.AD.2003

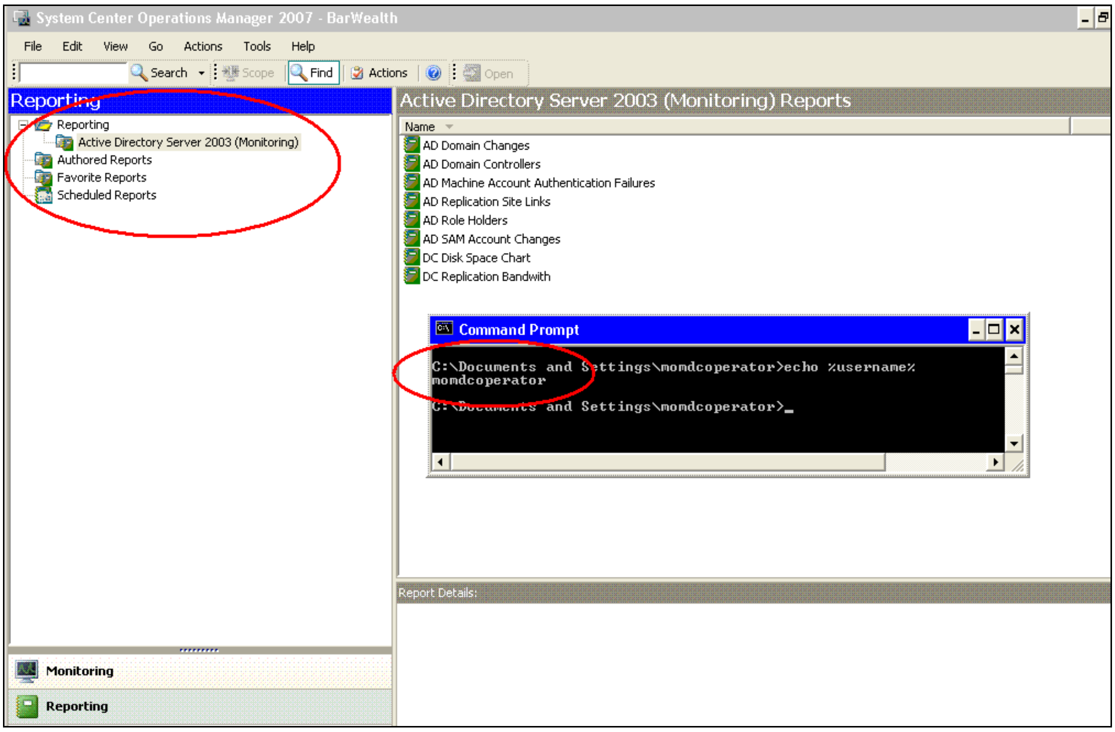
Group or user name: b9d7905a-bd15-41c3-

Select one or more roles to assign to the group or user.

□	Role	Description
☑	Browser	May view folders, reports and subscribe to report
□	Content Manager	May manage content in the Report Server. This i
☑	My Reports	May publish reports and linked reports; manage fc
□	Publisher	May publish reports and linked reports to the Repo
☑	Report Builder	May view report definitions.

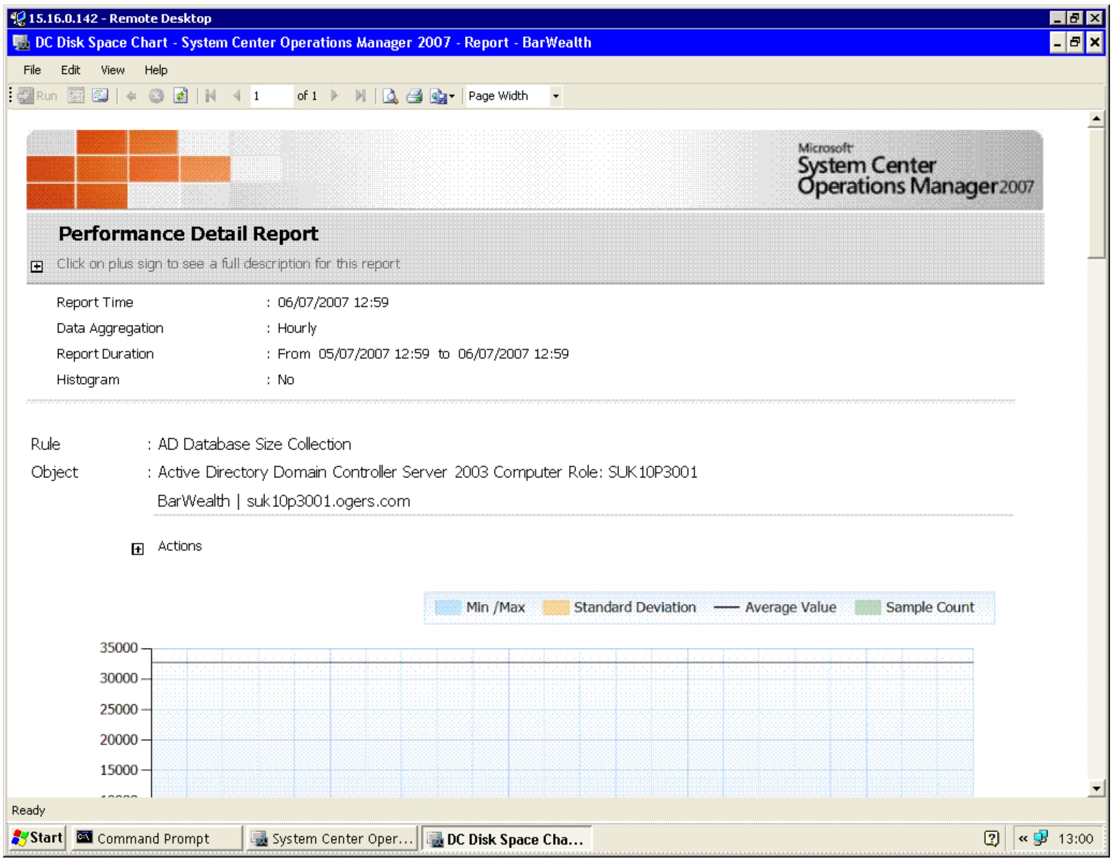
```
PS Monitoring:\suksmp10002va.ogers.com
>get-userrole | format-list Name,ID | ft


Name : Operations Manager Report Security Administr
Id   : 50585907-7858-4488-ab9c-13e0eaac08be

Name : Operation Manager Report Operators
Id   : 2537b367-6d74-4110-b0b5-1f51c1b1b09e

Name : AEM Operators
Id   : 3b167225-c96f-436b-bd19-21ba9a213f74

Name : GBL.ActiveDirectory.Operator
Id   : 6cce19b1-f398-4f16-8fca-3f0174c2efb3

Name : OperationsManagerAdministrators
Id   : 597f9d98-356f-4186-8712-4f020f2d98b4

Name : momoperator
Id   : a5096147-2de1-45e8-89fd-5e61f81fde29

Name : OperationsManagerAdvancedOperators
Id   : 489e12f0-6ada-4647-91db-65ab9ff0b40e

Name : OperationsManagerAuthors
Id   : 35b4a078-1f02-4988-9599-6824792722ce

Name : Test Report Operator Role
Id   : b9d7905a-bd15-41c3-b4f0-c400edfadbda

Name : OperationsManagerOperators
Id   : 3bf09528-6cfa-4e09-bf87-ecade3373814

Name : OperationsManagerReadOnlyOperators
Id   : 9f86f9a1-e2d4-4116-893a-f450f800f55d



PS Monitoring:\suksmp10002va.ogers.com
>_
```

And now when the **MOMDCOperator** user logs on and goes into reporting, all they can see is reports relevant to them:


System Center Operations Manager 2007 - BarWealth
File Edit View Go Actions Tools Help
Search Scope Find Actions Open
Reporting
Reporting
Active Directory Server 2003 (Monitoring)
Authored Reports
Favorite Reports
Scheduled Reports
Active Directory Server 2003 (Monitoring) Reports
Name
AD Domain Changes
AD Domain Controllers
AD Machine Account Authentication Failures
AD Replication Site Links
AD Role Holders
AD SAM Account Changes
DC Disk Space Chart
DC Replication Bandwith
Command Prompt
Report Details:
Monitoring
Reporting

```
C:\Documents and Settings\momdcoperator>echo %username%
momdcoperator

C:\Documents and Settings\momdcoperator>_
```

And the reports now run:


15.16.0.142 - Remote Desktop
DC Disk Space Chart - System Center Operations Manager 2007 - Report - BarWealth
File Edit View Help
Run 1 of 1 Page Width
Microsoft System Center Operations Manager 2007

Performance Detail Report

Click on plus sign to see a full description for this report

Report Time : 06/07/2007 12:59
Data Aggregation : Hourly
Report Duration : From 05/07/2007 12:59 to 06/07/2007 12:59
Histogram : No

Rule : AD Database Size Collection
Object : Active Directory Domain Controller Server 2003 Computer Role: SUK10P3001
BarWealth | suk10p3001.ogers.com

From now on whenever you add a new Management Pack in you need to make sure you remove the **Report Operators** role and create a new role that is of type **Report**

Operators using the PowerShell script earlier then permission this new role against that report.