

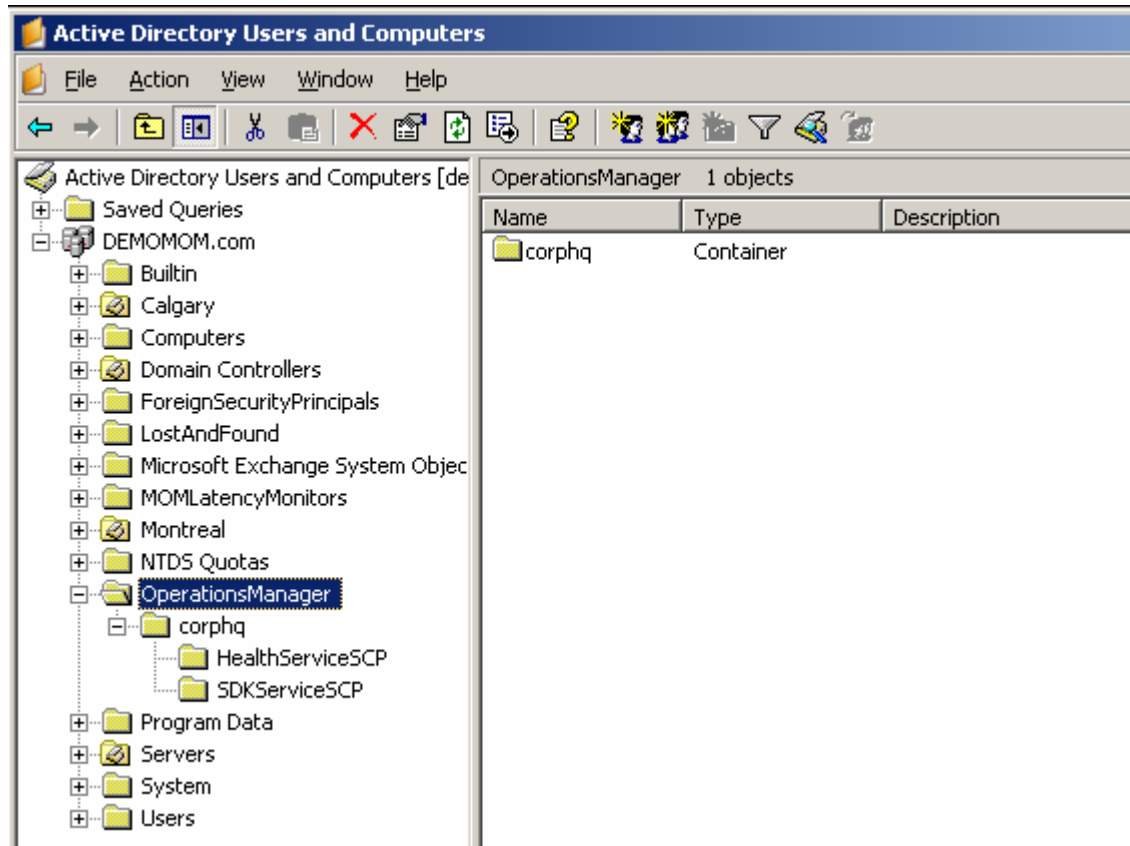
Active Directory Integration in Operations Manager 2007

MOMADAdmin.exe is a new tool included in the Support Tools folder on the Operations Manager 2007 media that allows you to prepare the Active Directory for AD Auto Agent Assignment. This tool does NOT make schema changes. It does create an Active Directory container for an Operations Manager 2007 Management Group. This container is created within the domain of the computers it manages. The purpose of this container is to assign Operations Manager administrators the rights needed to add Management Servers and assign agents to the Management Servers without the need for domain administrator credentials.

On a DC, logged on as a member of the Domain Admins group, open a CMD window and navigate to OpsMgr2007Rc2\Support Tools directory type MomADAdmin.exe <mgmtgroupname> domain\OpsMgrAdminsSecurityGroup domain\managementservername domain.

```
C:\> Command Prompt
D:\>momadadmin.exe corphq demomom\OpsMgrSecurityAdmins demomom\mom1 demomom
Microsoft System Center Operations Manager 2007 -- MOM AD Configuration Tool
(C) Copyright 2000-2006 Microsoft Corp.
Successfully Created a container for ManagementGroup corphq
Successfully added MOM1$ to demomom\OpsMgrSecurityAdmins security group
D:\>
```

The result of this command was a new container named OperationsManager with a child container named after the name of the management group and two child containers named HealthServiceSCP and SDKServiceSCP being created.



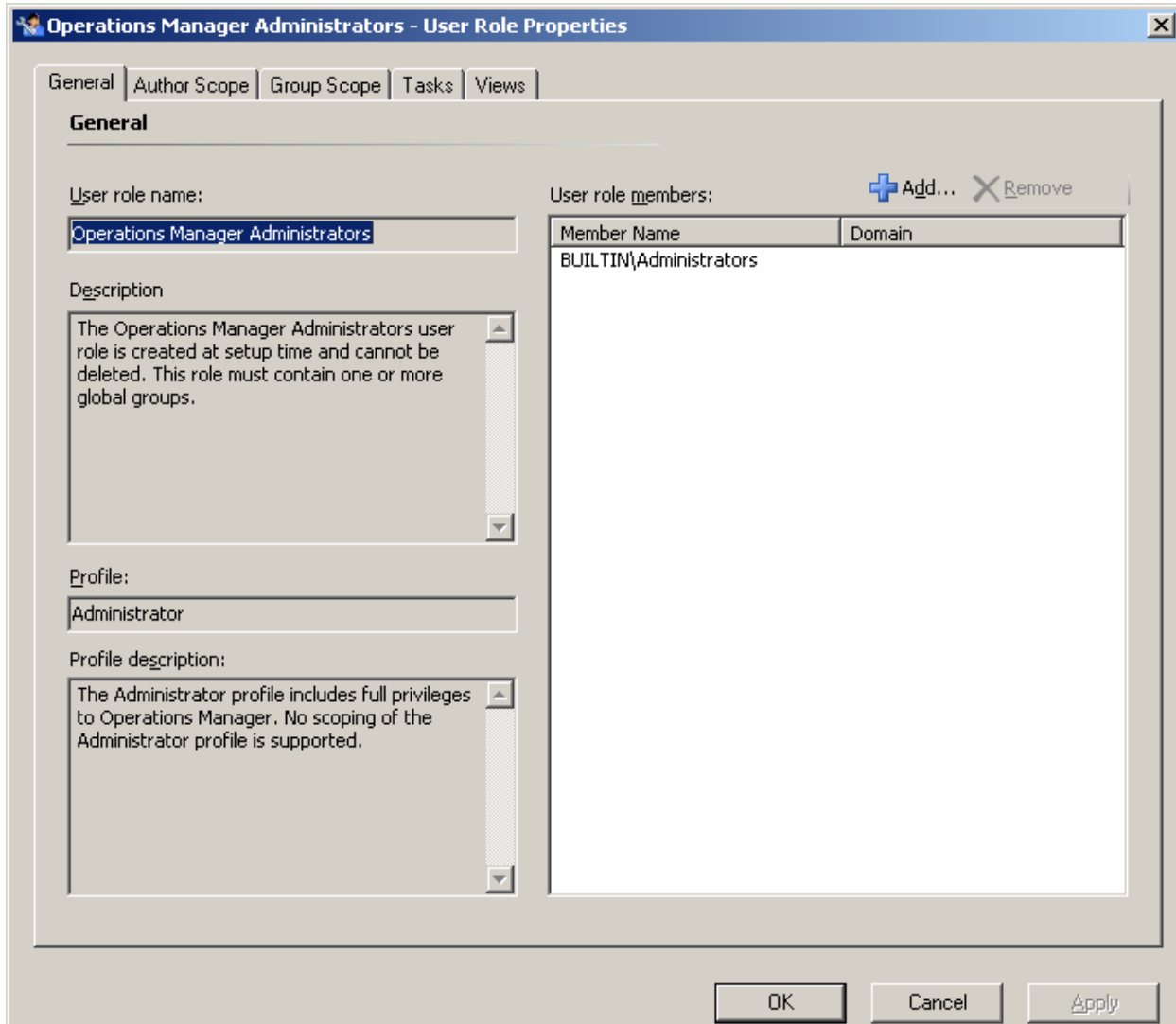
A domain local security group named mgmtgroupname_HSvcSCP_SG is also created in the MgmtGroupName container.

The computer account of the root management server and the group 'OpsMgrSecurityAdmins' specified in the MOMADAdmin.exe command are both granted Read access to the managementgroupname container in AD.

The domain local security group named mgmtgroupname_HSvcSCP_SG is granted Read permission on the HealthServiceSCP container but on this container the 'OpsMgrSecurityAdmins' specified in the MOMADAdmin.exe command is granted Full Control.

The 'OpsMgrSecurityAdmins' specified in the MOMADAdmin.exe command is granted only Read permission on the SDKService SCP container as is the root management server computer account. The mgmtgroupname_HSvcSCP_SG domain local group isn't defined in the DACL.

Finally, we must add the security group 'OpsMgrSecurityAdmins' as a member of the Operations Manager Administrators role for the Management Group. To do this navigate to the Administration node and expand Security and select User Roles. Right click the Operations Manager Administrators role and select Properties.



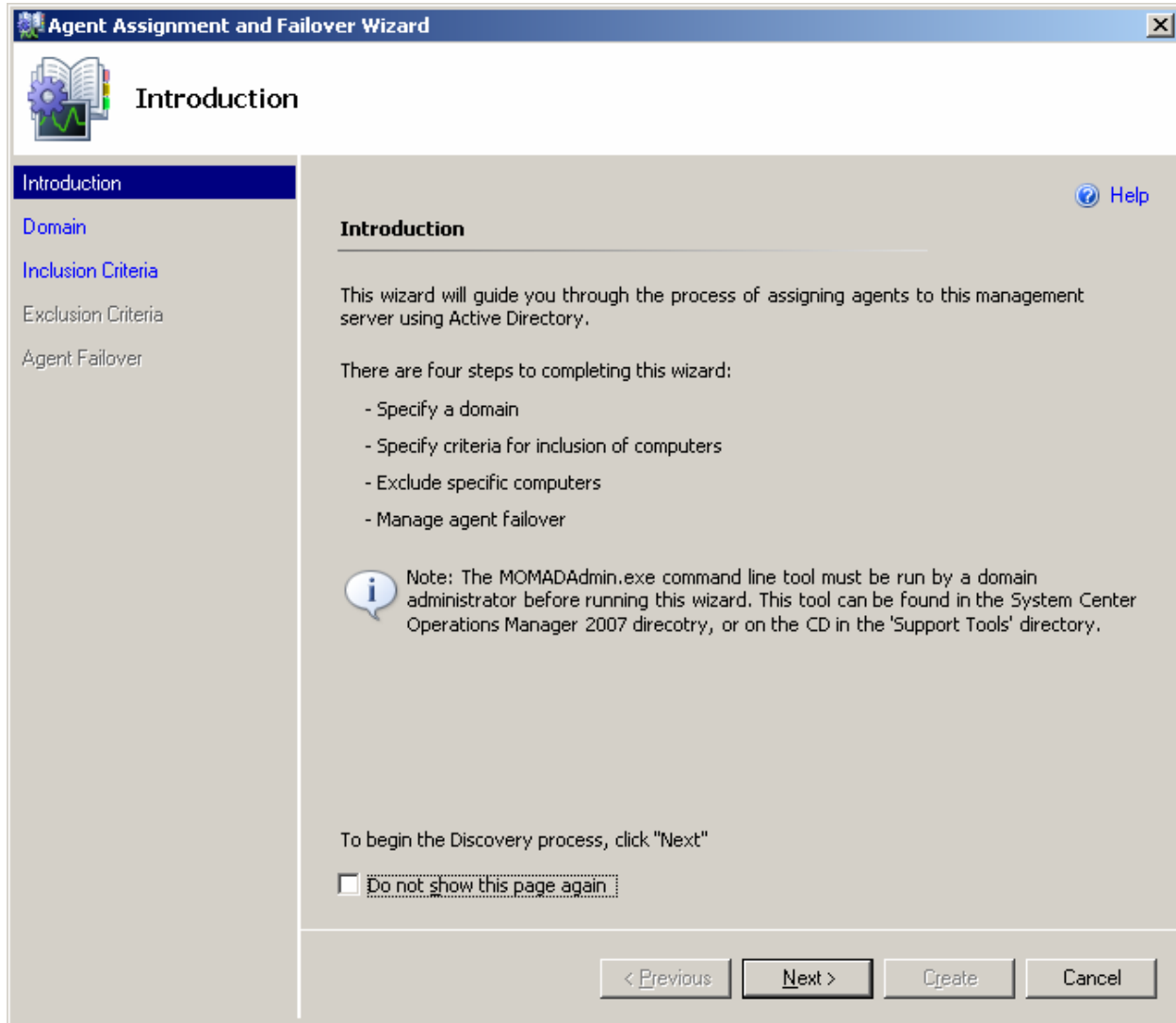
Click Add and add in 'OpsMgrSecurityAdmins' and click OK. Click OK again.

Define Auto Agent Assignment settings in Active Directory

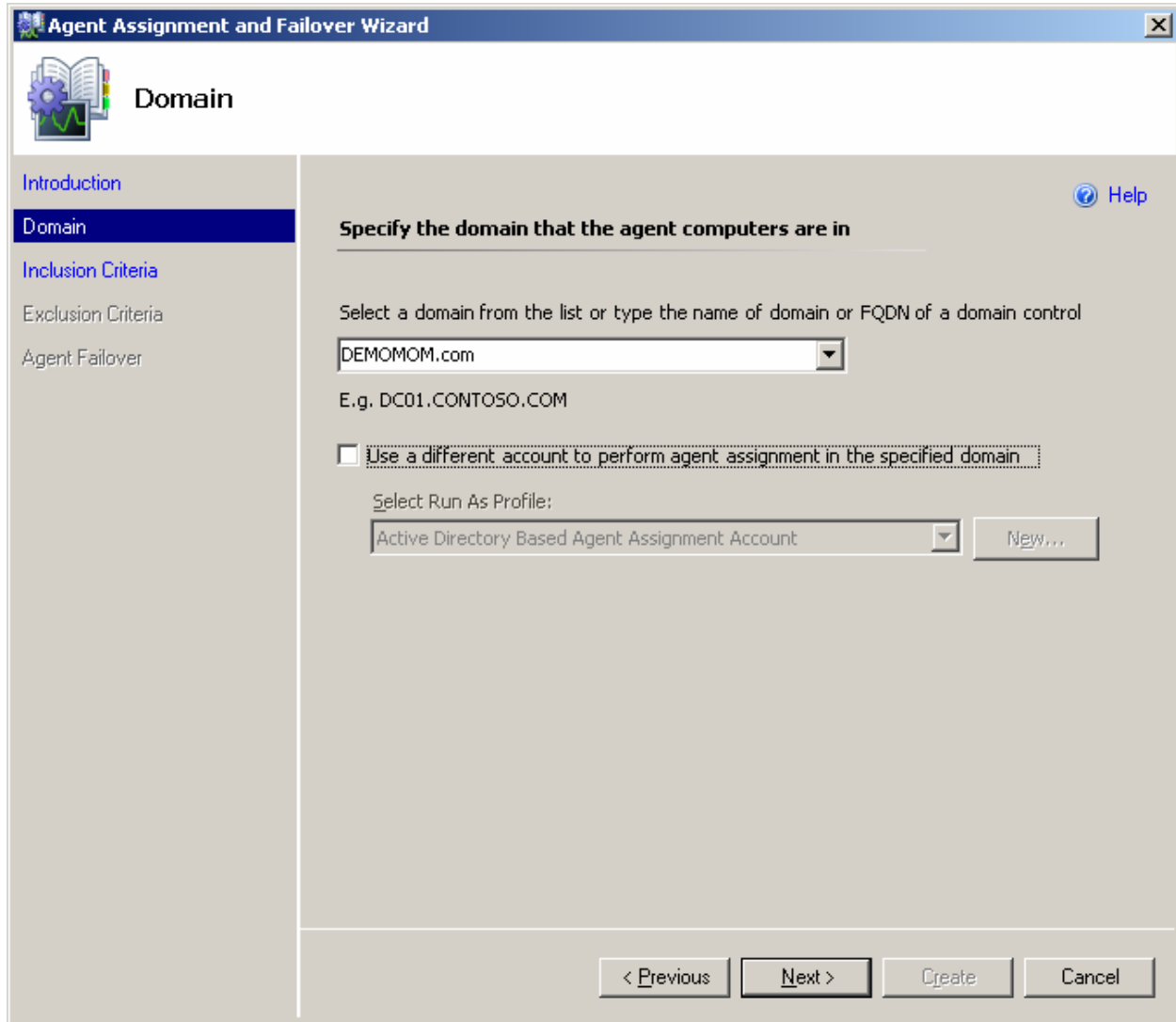
A new feature in Operations Manager 2007 allows you to define agent assignment settings in Active Directory. This allows you to define the agent managed computers and the management servers that will monitor them. To configure this, navigate to the Administration node and under Device Management select Management Servers. Right click on a Management Server and select Properties. Click Add on the Auto Agent Assignment tab.

Notice the note that the MOMADAdmin.exe tool must be run by a member of the Domain Administrators group before running this wizard.

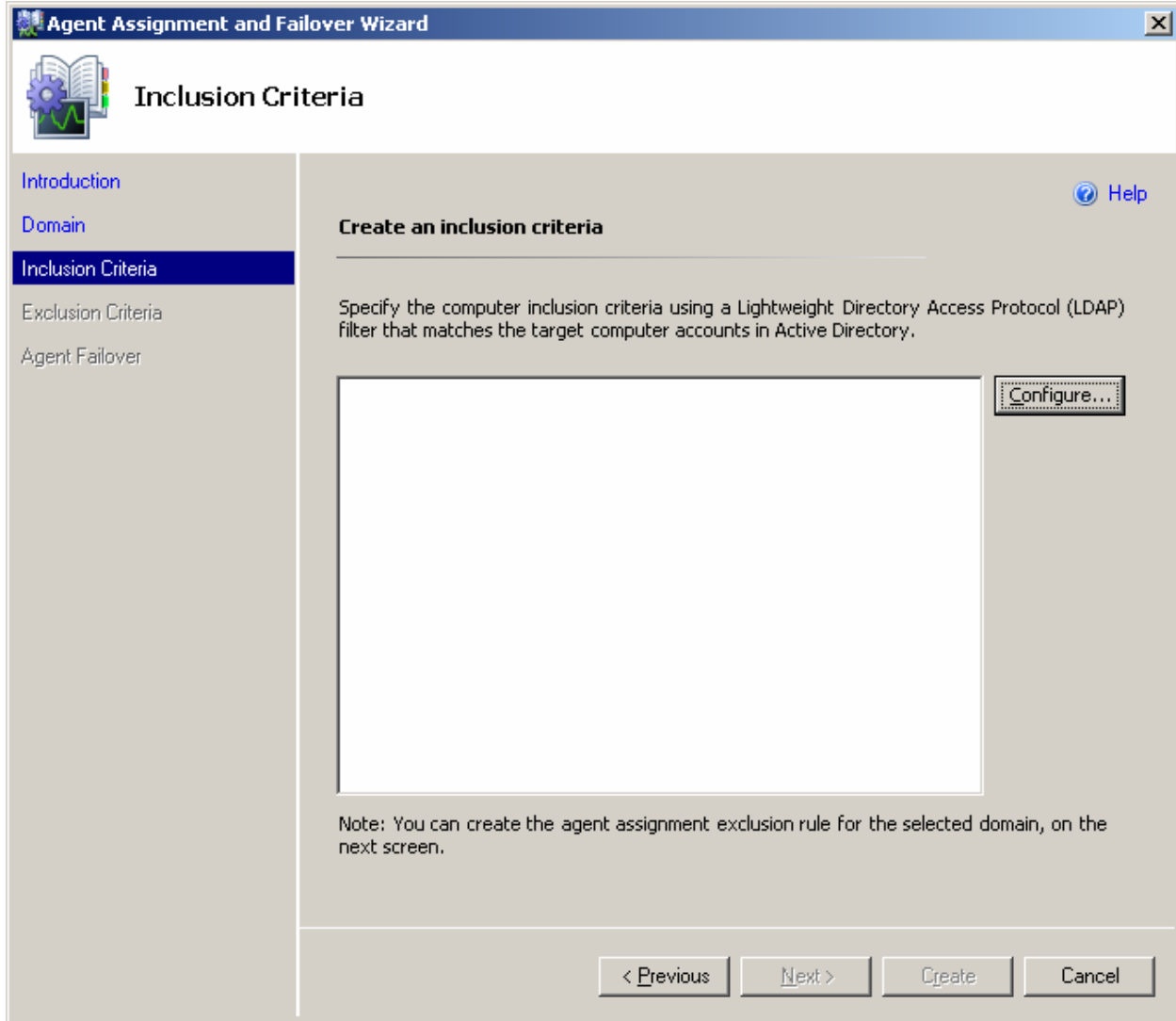
Click **Next** on the Introduction page.



Click **Next**.

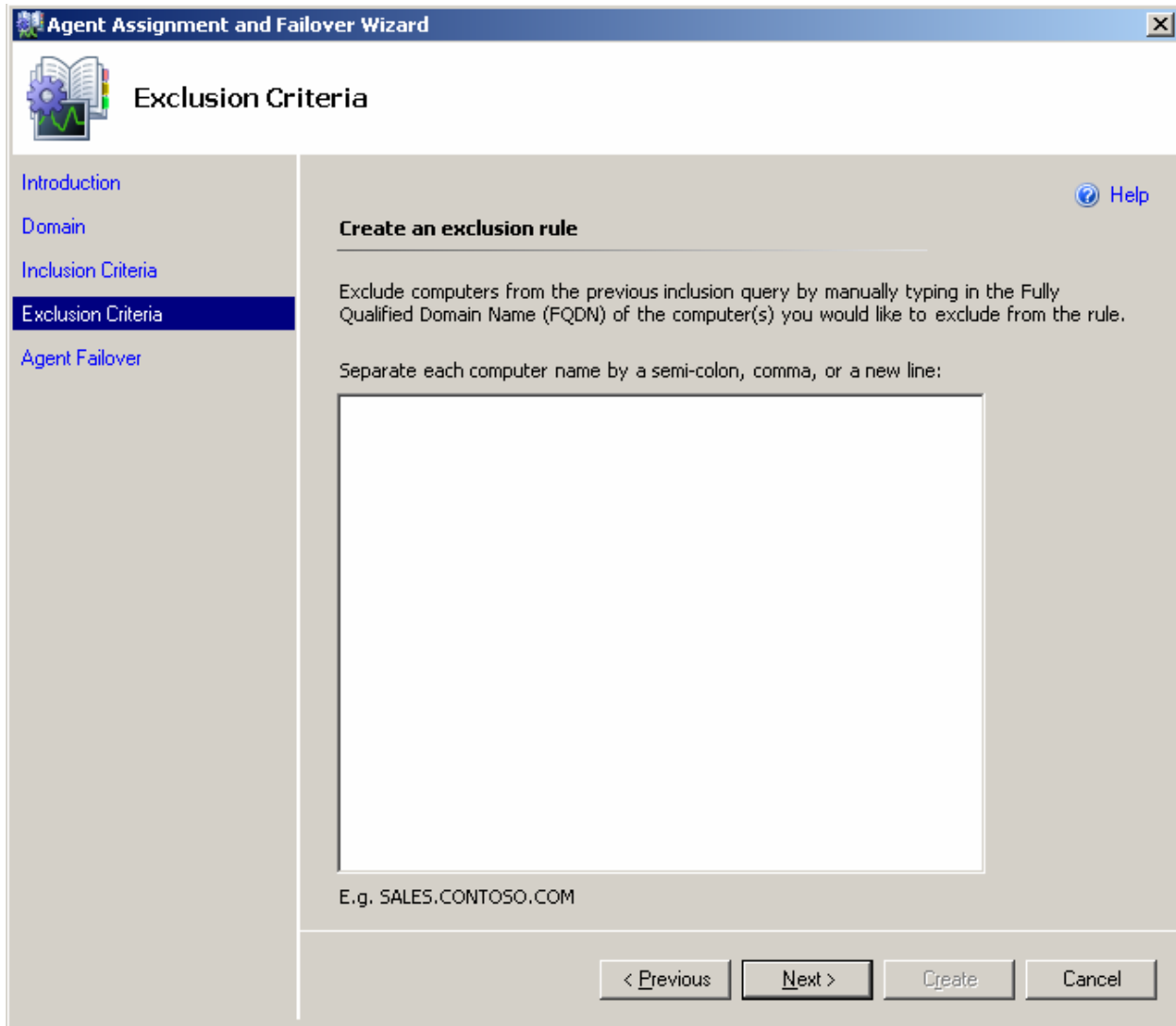


Click **Configure** on the Inclusion Criteria page.

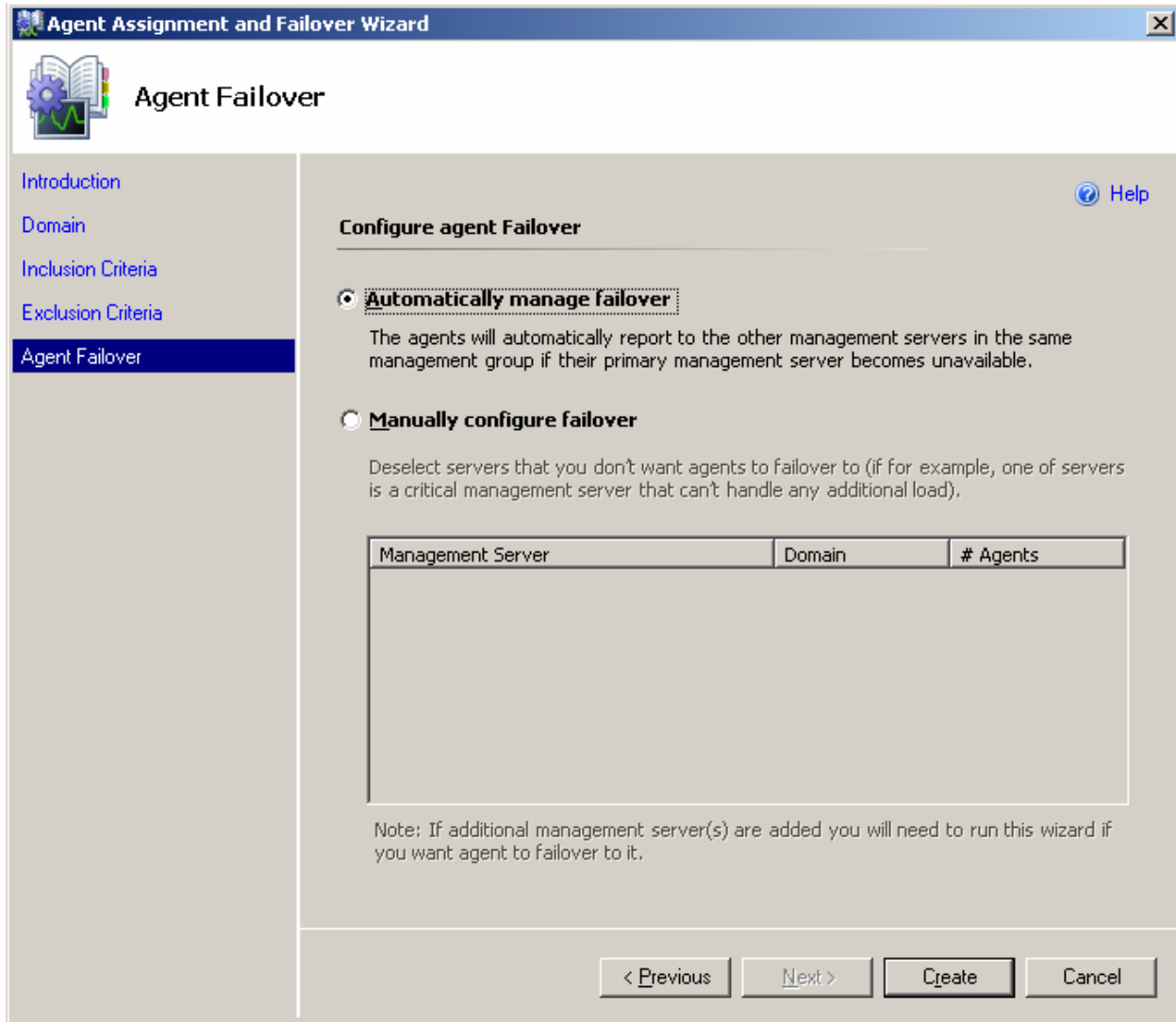


Define your LDAP query such as `(&(sAMAccountType=805306369)(objectCategory=computer)(operatingSystemVersion=5*))` to look for any computer where the operating system version starts with 5. This will include all Windows 2000 through Windows Server 2003 R2 systems as well as XP systems. Click **Next**.

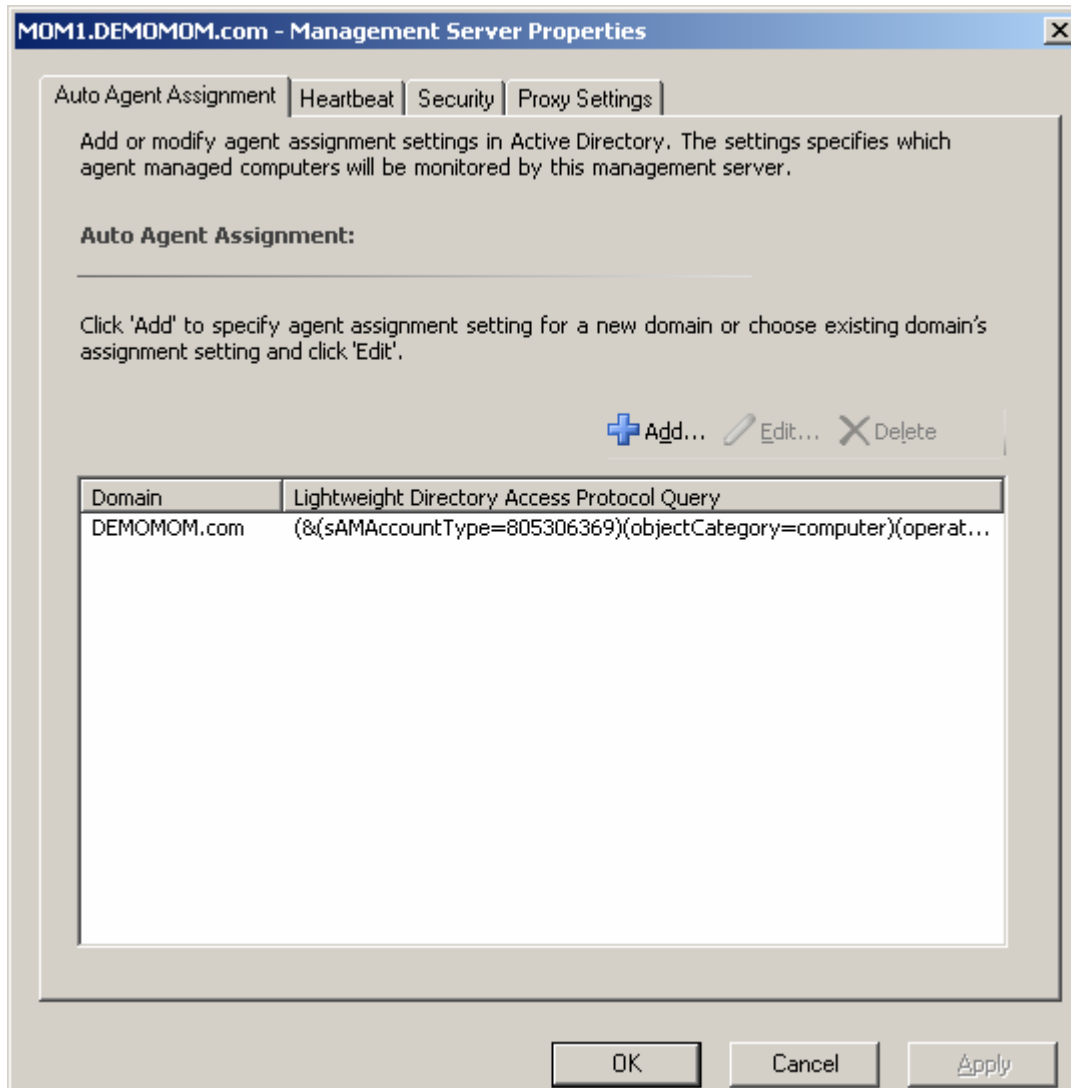
Click **Next** on the Exclusion rule page.



Determine your automatic failover settings and click **Create**.



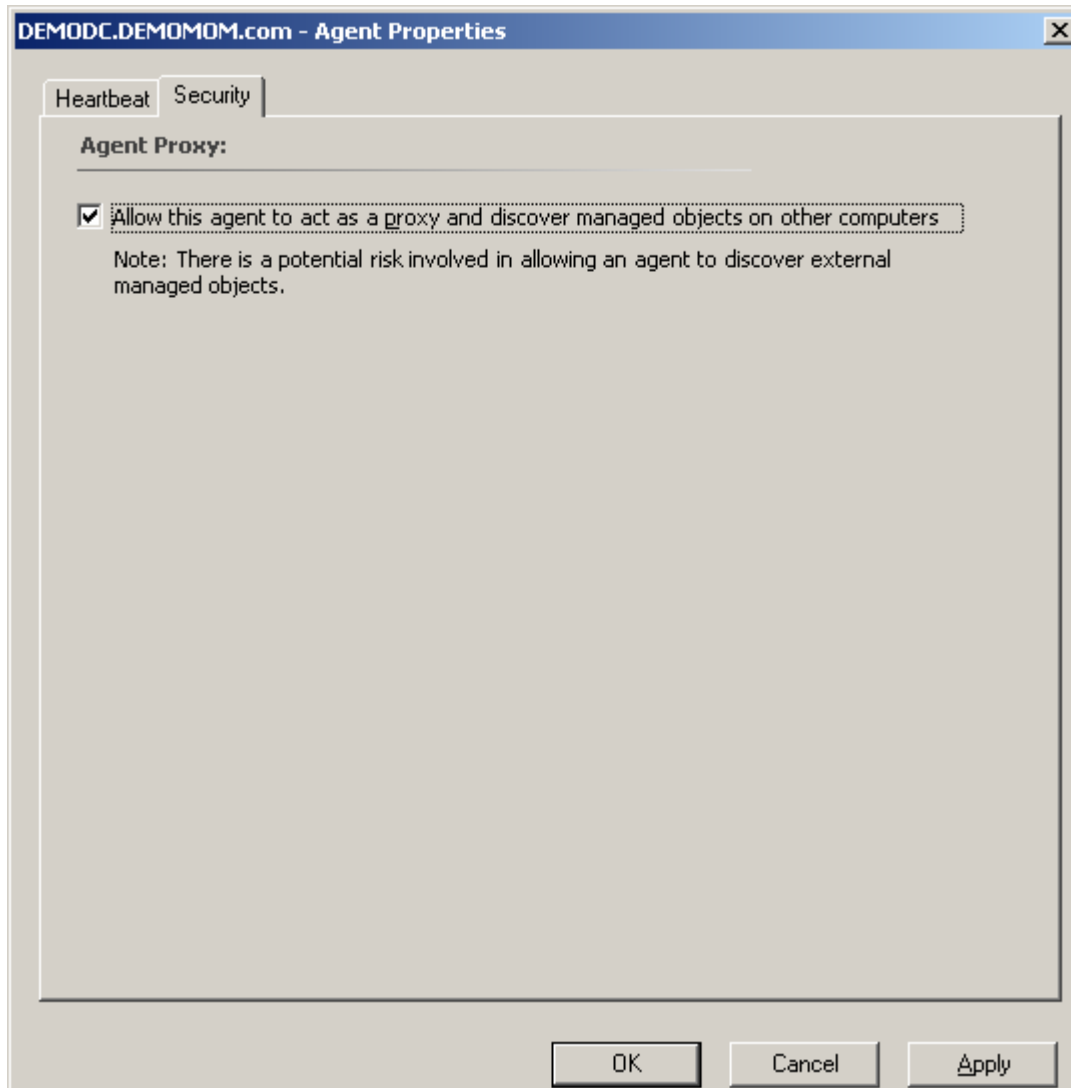
Click **OK** on the Agent Auto Assignment page.



Enabling Agent Proxying

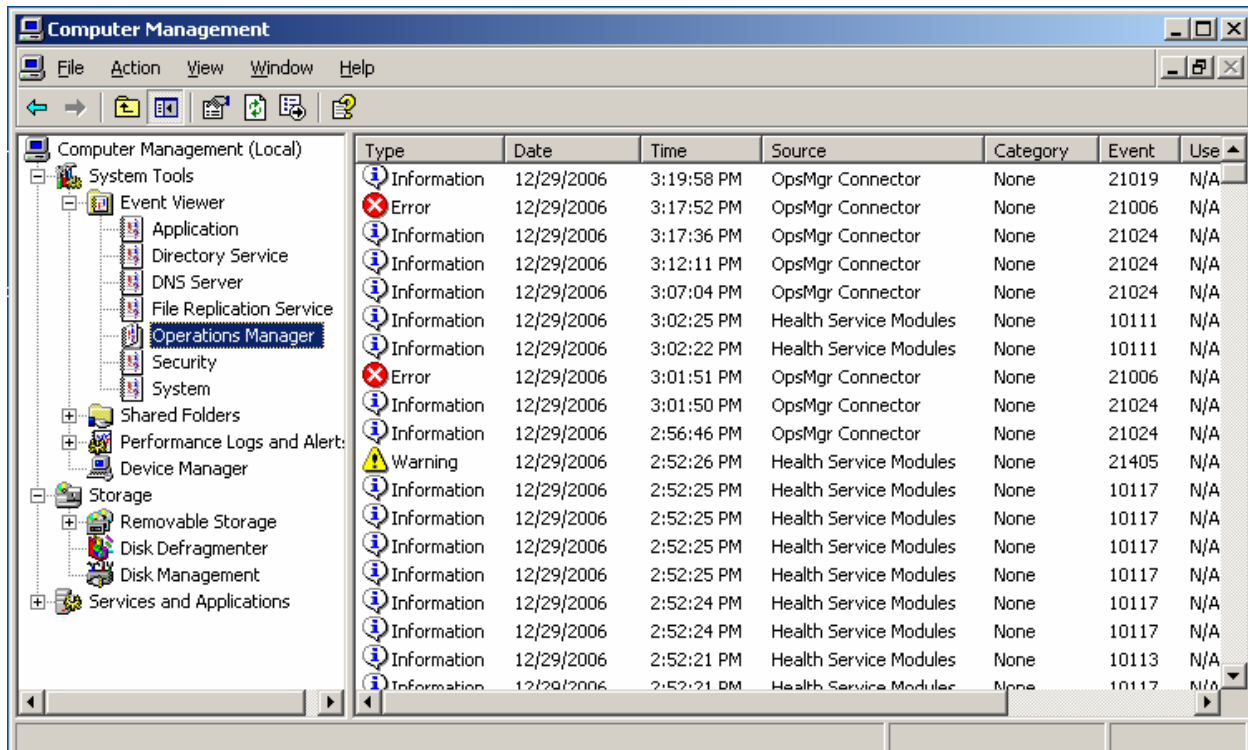
Agent proxying must be enabled for all Domain Controllers and Exchange Servers. This is because discovery data is submitted by the DCs which reference objects that are not 'owned' by the Health Service on the DC. Exchange Topology discovery requires that Agent Proxying be enabled on all Exchange Servers.

To enable agent proxying, navigate to the Administration node and under Device Management select Agent Managed. Right click on the DC or multiple DCs and select Properties. Select the Security tab and enable **Allow this agent to act as a proxy and discover managed objects on other computers** and click OK.



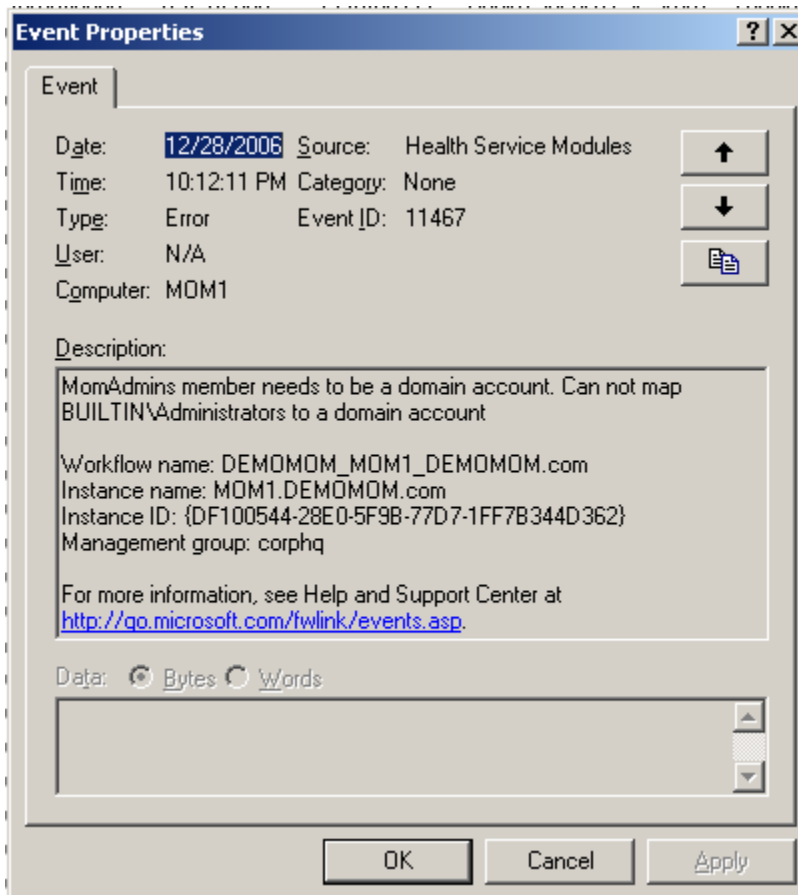
New Event Log

On every system that has an Operations Manager agent installed, as well as on the server hosting the Operations Manager database and the server acting as the Management Server a new Event Log called Operations Manager is created.

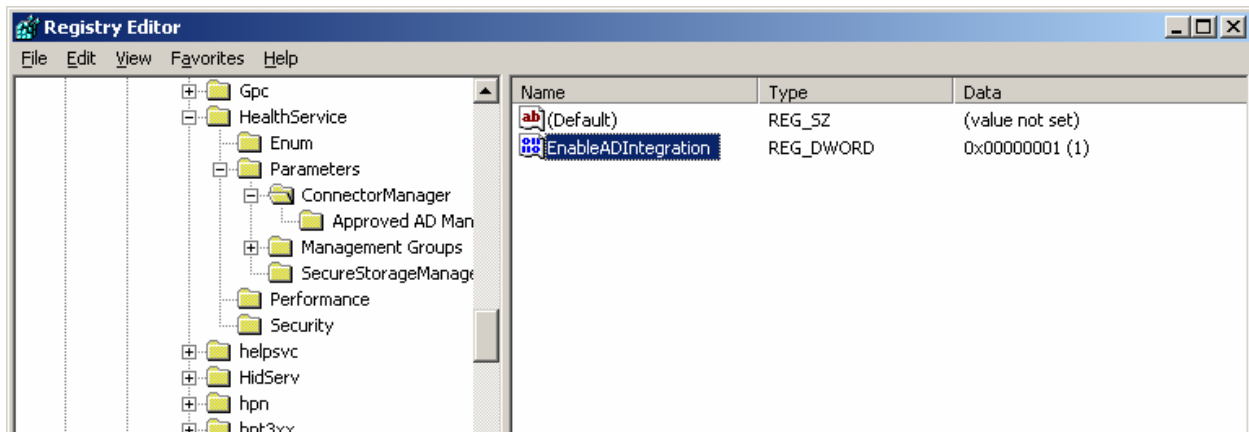
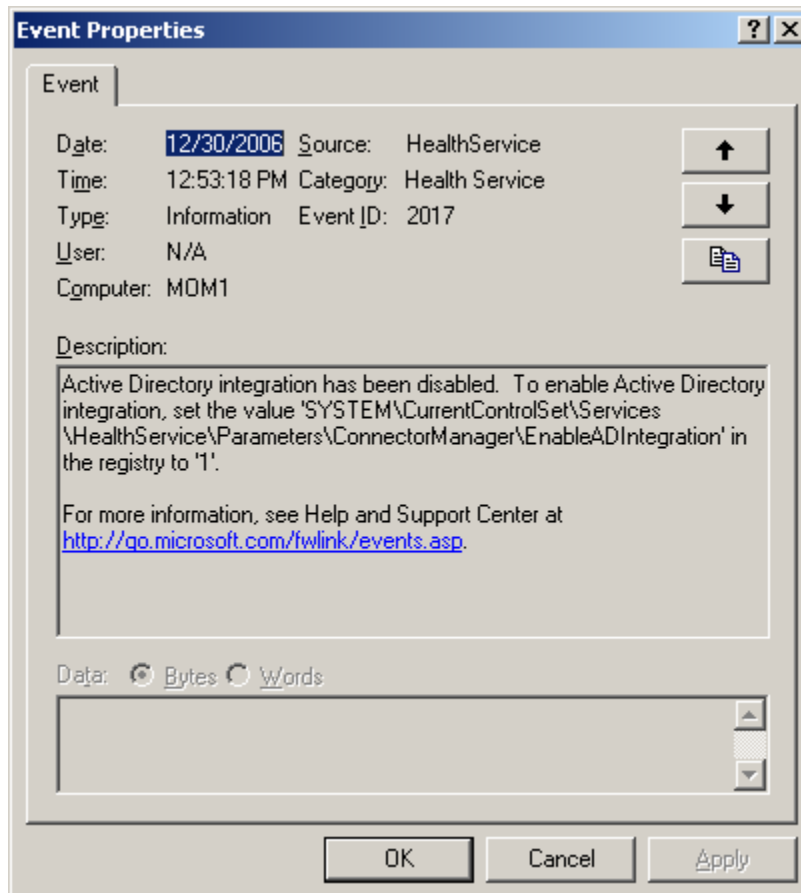


Wow, this was a chore! For AD integration to work, I needed to perform a bunch of steps that weren't in the docs including raise my domain level to Windows 2000 native from the default Windows 2000 mixed but I didn't see this mentioned anywhere in the docs. Did I miss something or does this need to be added to the docs? This was a change I made after receiving an error message in the Operations Manager event log with Event ID 21010 from source Health Service is the Health Service isn't able to connect to Active Directory.

Another common event that appears after Operations Manager installation and MOMAdmin configuration is Event ID 11467 from source Health Service Modules indicating that a MOMAdmins member needs to be a domain account. This error will be generated every 60 minutes in the Operations Manager event log on the MOM Management Server until configured correctly. I guess I was logged on as the local Administrator when I installed it so the only member was the BUILTIN\Administrators group.



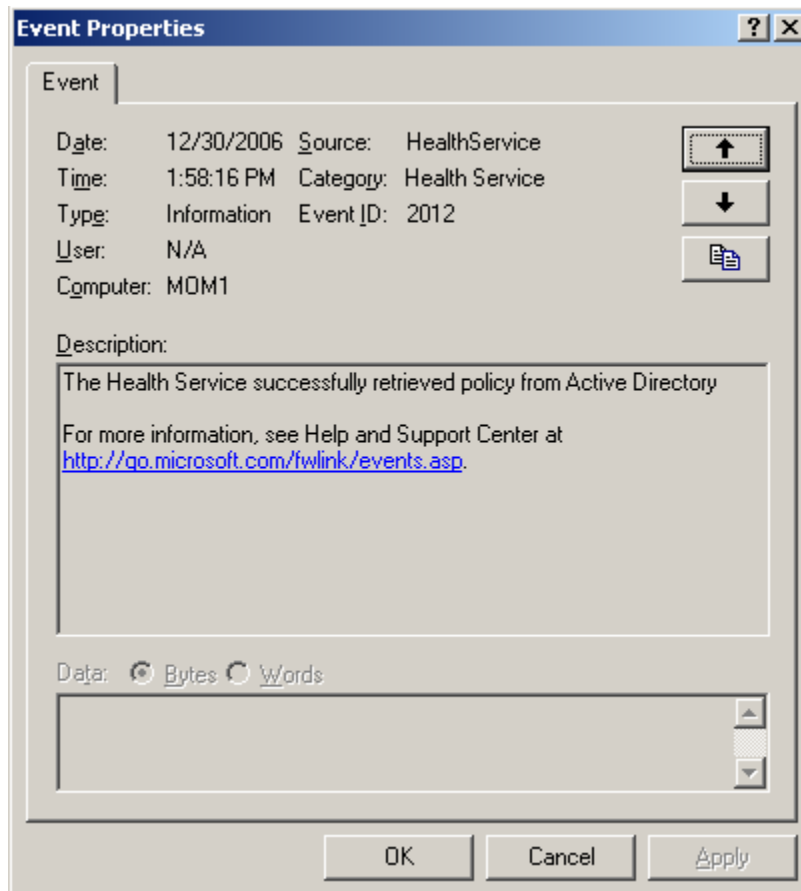
Then another error occurred even though the group was added to the MOMAdmins role but no users were in the group other than the Mgmt Server computer account\$. To correct this, I added the domain account da_roy which was an ordinary user but after an hour the alert didn't go away. Then I restarted the SDK service and the Config Service on the Mgmt Server. After restarting the Health Service on the management server, Event ID 2017 from source Health service was logged indicating that the AD integration has been disabled and in order to enable it you have to set the value EnableADIntegration to 1 in HKLM\System\CurrentControlSet\Services\HealthService\Parameters\ConnectorManager\EnableADIntegration.



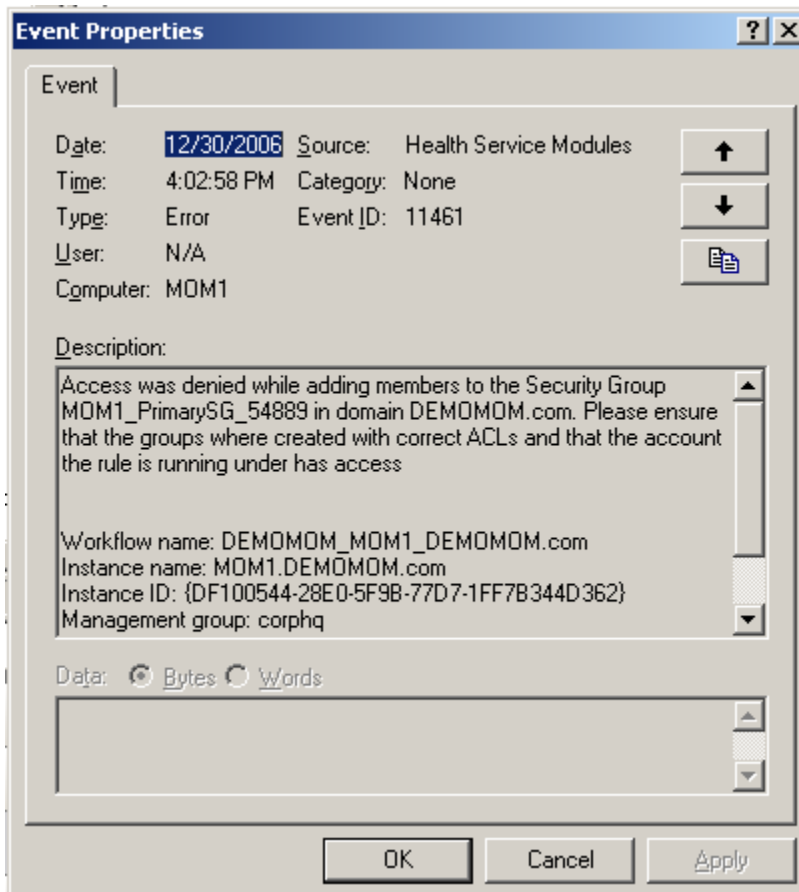
Next I found that event with ID 11467 continues to appear when BUILTIN\Administrators is a member of the MOMAdmins role. Removed that group and the event stopped.

Oh, don't forget to restart the OpsMgr config and SDK services after every change.

Finally success indicated by Event ID 2012 being logged indicating that the Health Service successfully retrieved policy from AD.



Well, not yet actually. I had to then add a user to the domain global security group OpsMgrSecurityAdmins named da_rory that was an ordinary user. Then I had to grant OpsMgrSecurityAdmins Write, Create All Child Objects, Delete All Child Objects, and Add/Remove self as a member on the DACL of the MOM1_SecondarySG_54889 domain local group created in the <mgmt group name> container. Then I granted OpsMgrSecurityAdmins Write, Create All Child Objects, Delete All Child Objects, and Add/Remove self as a member on the DACL of the MOM1_PrimarySG_54889 domain local group created in the <mgmt group name> container. Granting those permissions results in the groups being visible in the <mgmtgroupname> container and allowed for the creation of the MgmtServer_SCP container.



That's it!

Have fun, learn Ops Mgr 2007!