Windows Configuration Guide for Nagios plugin to Uila

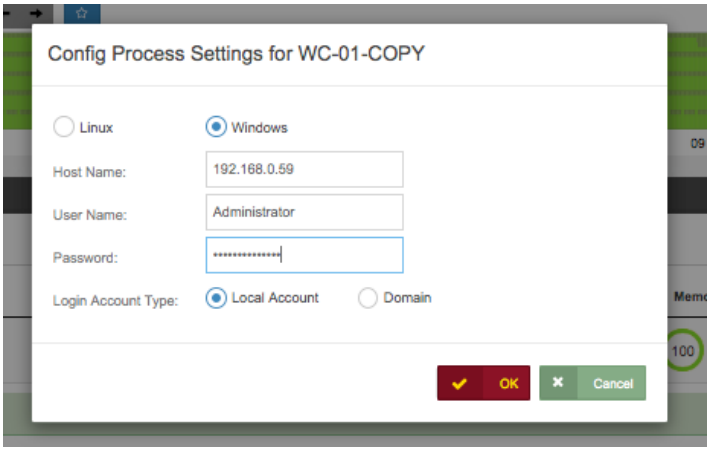
1 - Adding the Win Server 2012 as Administrator (not in domain)

2 - Adding a local account that is not the Administrator

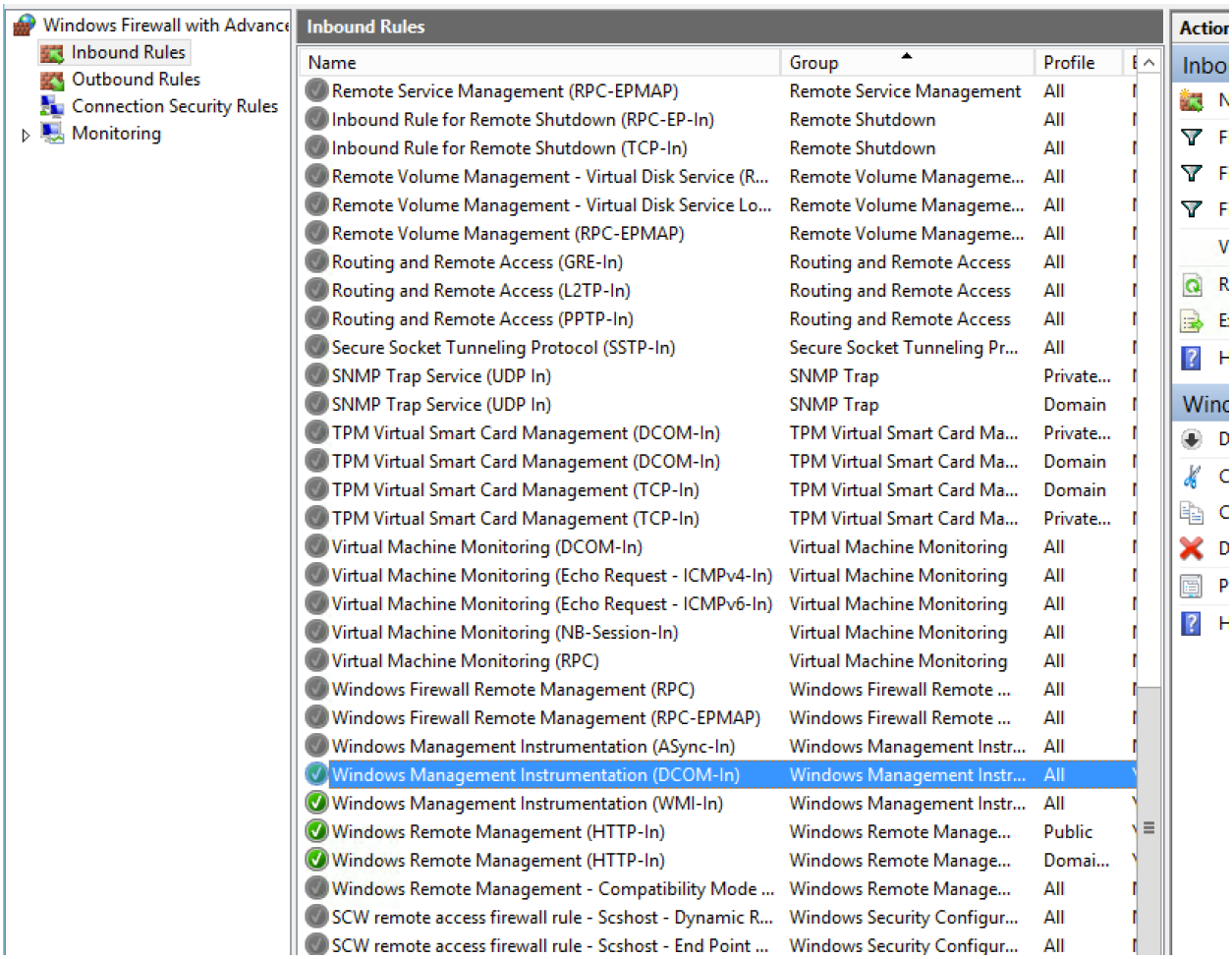
3 - Adding a host that is using a Domain Account

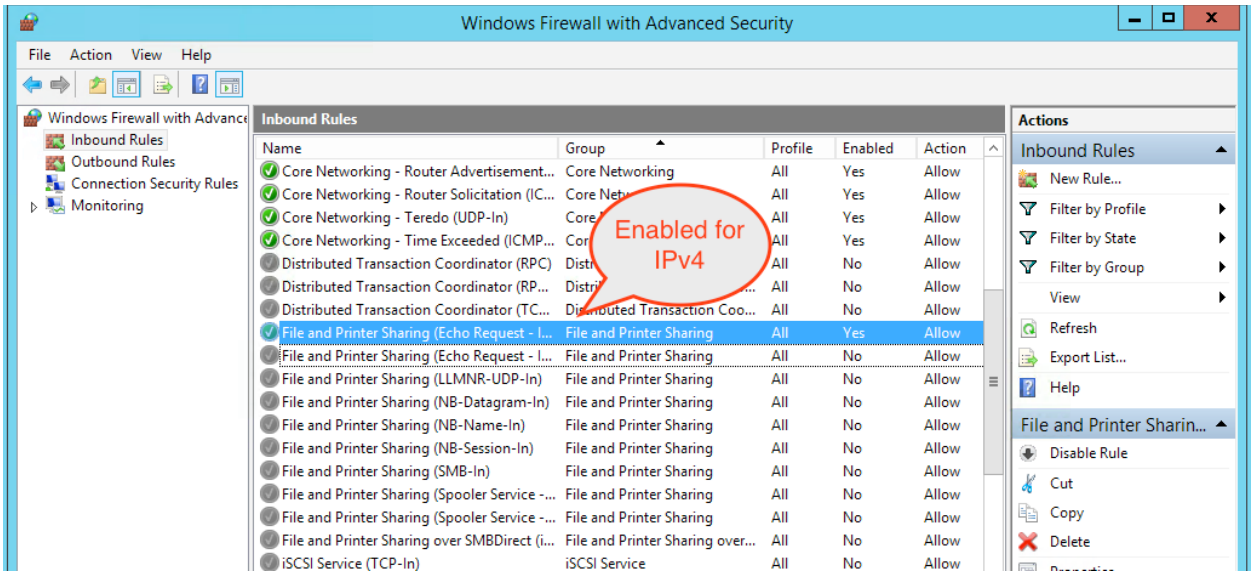
1 - Adding the Win Server 2012 as Administrator (not in domain)

After adding the host into the Critical Resources, click on the Config under Process tab to add the host:

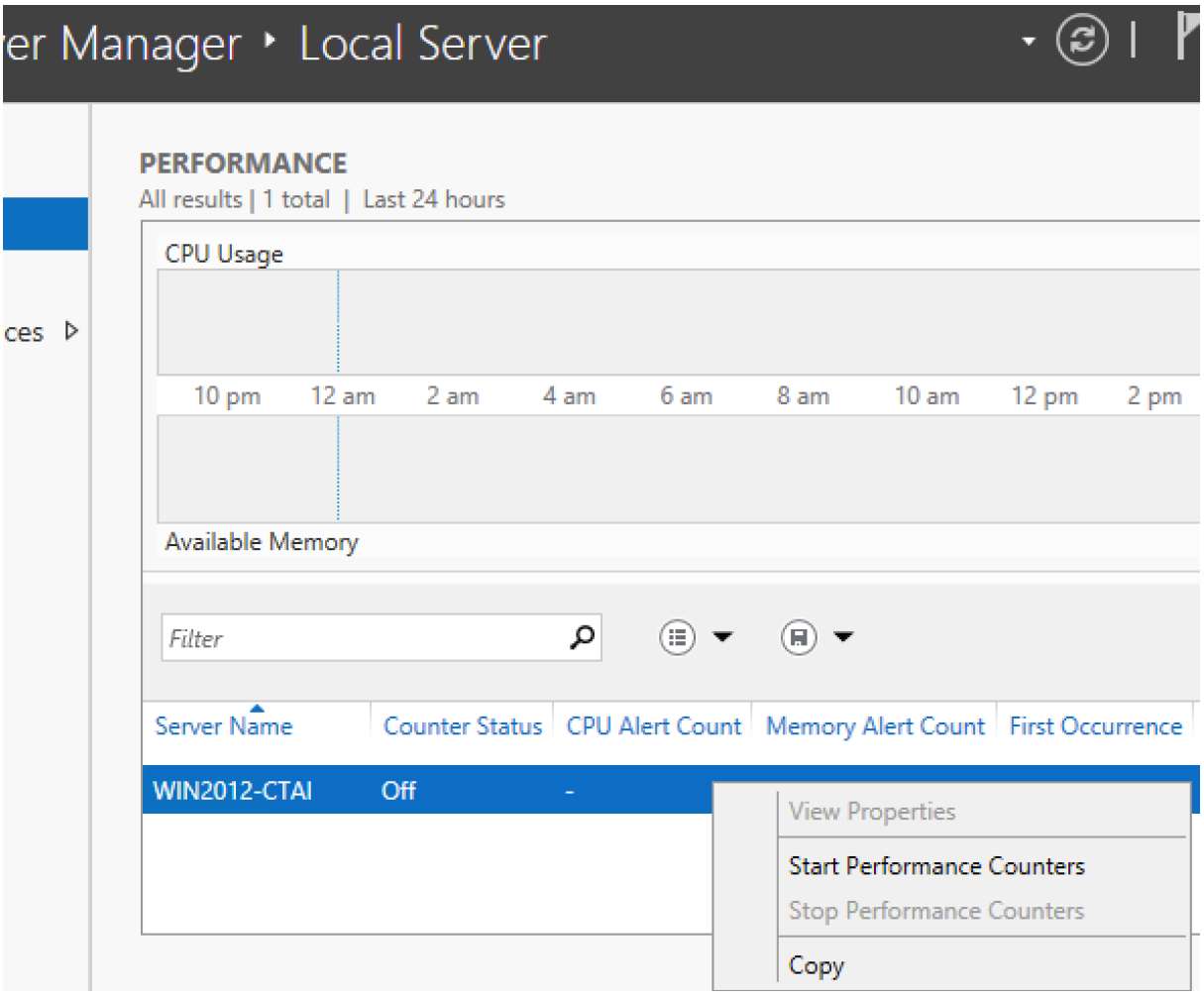


If firewall is on make sure these rules are enabled to allow DCOM and WMI access: WMI (DCOM-In), WMI (WMI-In) and IPv4 Ping (File and Printer Sharing):





Make sure that Performance Counters are being collected, in the Server Manager:



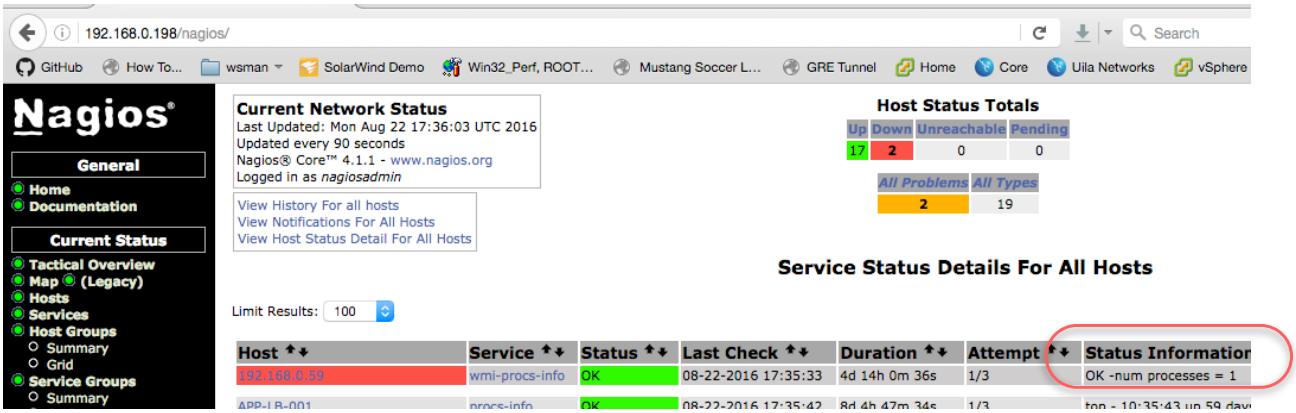
This should be enough to get the wmic to work.
To test, at the VIC goto the folder /opt/uila/VIC/bin and make a test query :

```
VIM >/usr/local/nagios/bin/wmic //192.168.0.129 -U administrator%password
"select * from win32_computersystem"
```

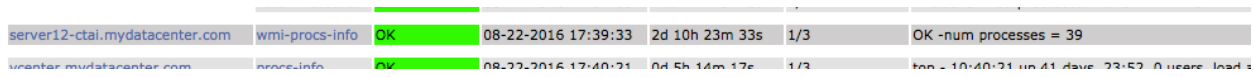
If the connection is working, you should get something like this:

```
CLASS: Win32_ComputerSystem
AdminPasswordStatus|AutomaticManagedPagefile|AutomaticResetBootOption|
AutomaticResetCapability|BootOptionOnLimit|BootOptionOnWatchDog|
BootROMSupported|BootupState|Caption|ChassisBootupState|CreationClassName|
CurrentTimeZone|DaylightInEffect|Description|DNSHostName|Domain|DomainRole|
EnableDaylightSavingsTime|FrontPanelResetStatus|HypervisorPresent|
InfraredSupported|InitialLoadInfo|InstallDate|KeyboardPasswordStatus|
LastLoadInfo|Manufacturer|Model|Name|NameFormat|NetworkServerModeEnabled|
NumberOfLogicalProcessors|NumberOfProcessors|OEMLogoBitmap|OEMStringArray|
PartOfDomain|PauseAfterReset|PCSystemType|PCSystemTypeEx|
PowerManagementCapabilities|PowerManagementSupported|PowerOnPasswordStatus|
PowerState|PowerSupplyState|PrimaryOwnerContact|PrimaryOwnerName|
ResetCapability|ResetCount|ResetLimit|Roles|Status|SupportContactDescription|
SystemStartupDelay|SystemStartupOptions|SystemStartupSetting|SystemType|
ThermalState|TotalPhysicalMemory|UserName|WakeUpType|Workgroup
3|True|True|True|0|0|True|Normal boot|WIN2012-CTAI|3|
Win32_ComputerSystem|-420|True|AT/AT COMPATIBLE|WIN2012-CTAI|
mydatacenter.com|3|True|3|True|False|NULL|(null)|3|(null)|Microsoft
Corporation|Virtual Machine|WIN2012-CTAI|(null)|True|1|1|NULL|([MS_VM_CERT/
SHA1/9b80ca0d5dd061ec9da4e494f4c3fd1196270c22],
00000000000000000000000000000000,To be filed by MSFT)|True|3932100000|1|1|
NULL|False|3|0|3|(null)|Windows User|1|-1|-1|
(LM_Workstation,LM_Server,NT,Server_NT)|OK|NULL|0|NULL|0|x64-based PC|1|
2147012608|(null)|6|(null)
```

If the configuration is not correct, you would see this in the Nagios Page:



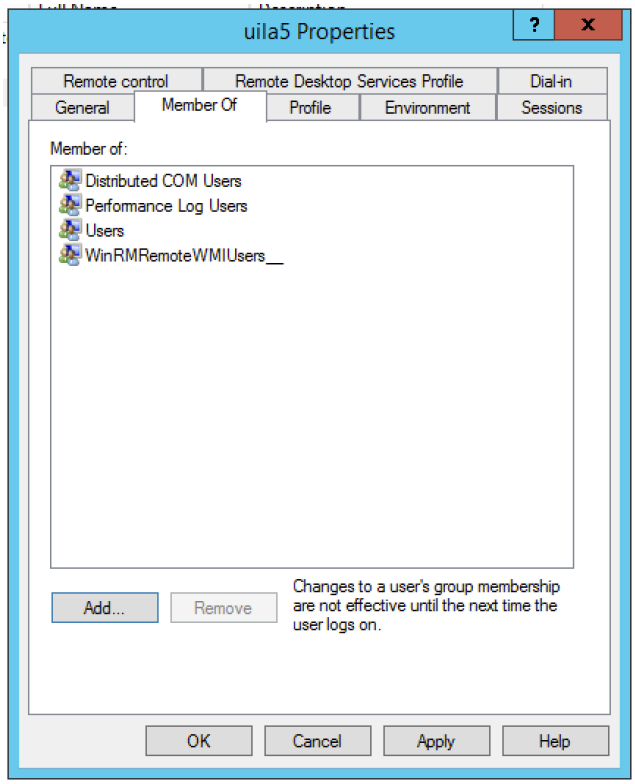
If successful, you should see the number of processes running:



2- Adding a local account that is not the Administrator

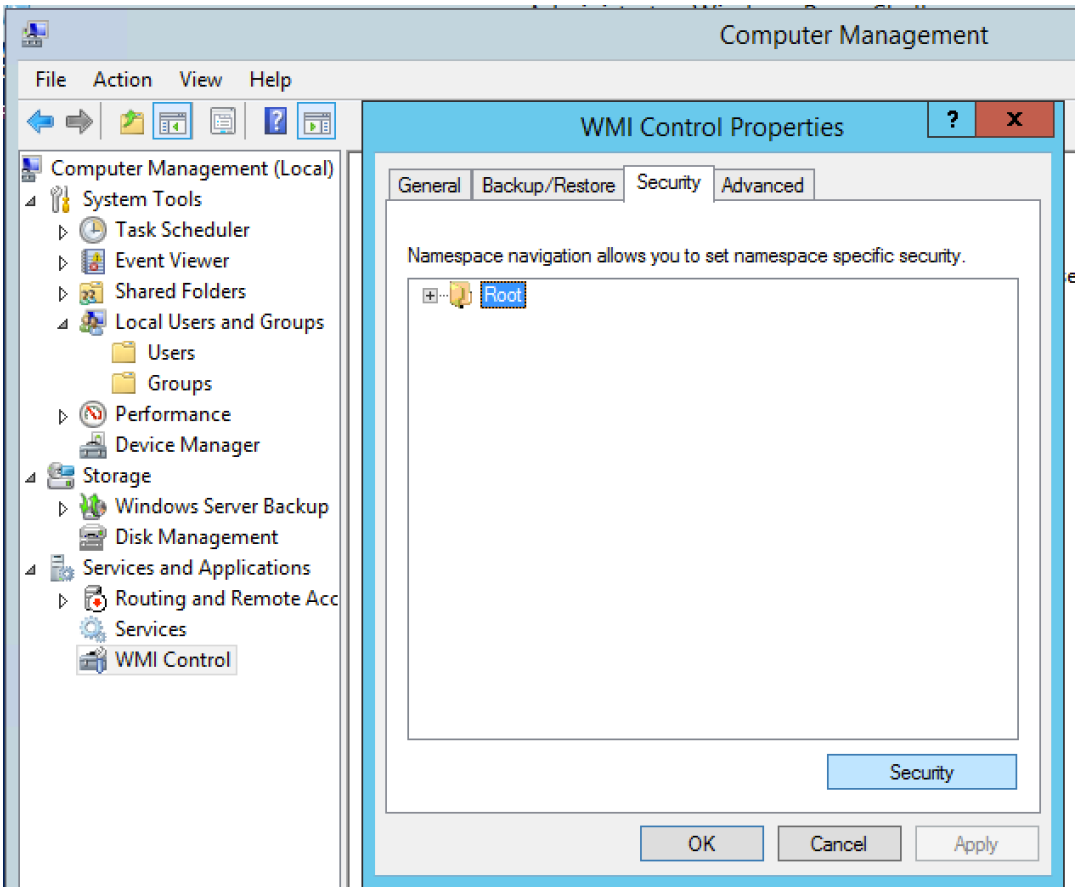
All previous settings from above needs to be complete as well to open the ports and making sure the Performance Counters are enabled.

Add a user to the windows host and make sure it is a member of the 'WinRMRemoteWMIUsers__', 'Distributed COM Users', and 'Performance Log Users' groups.

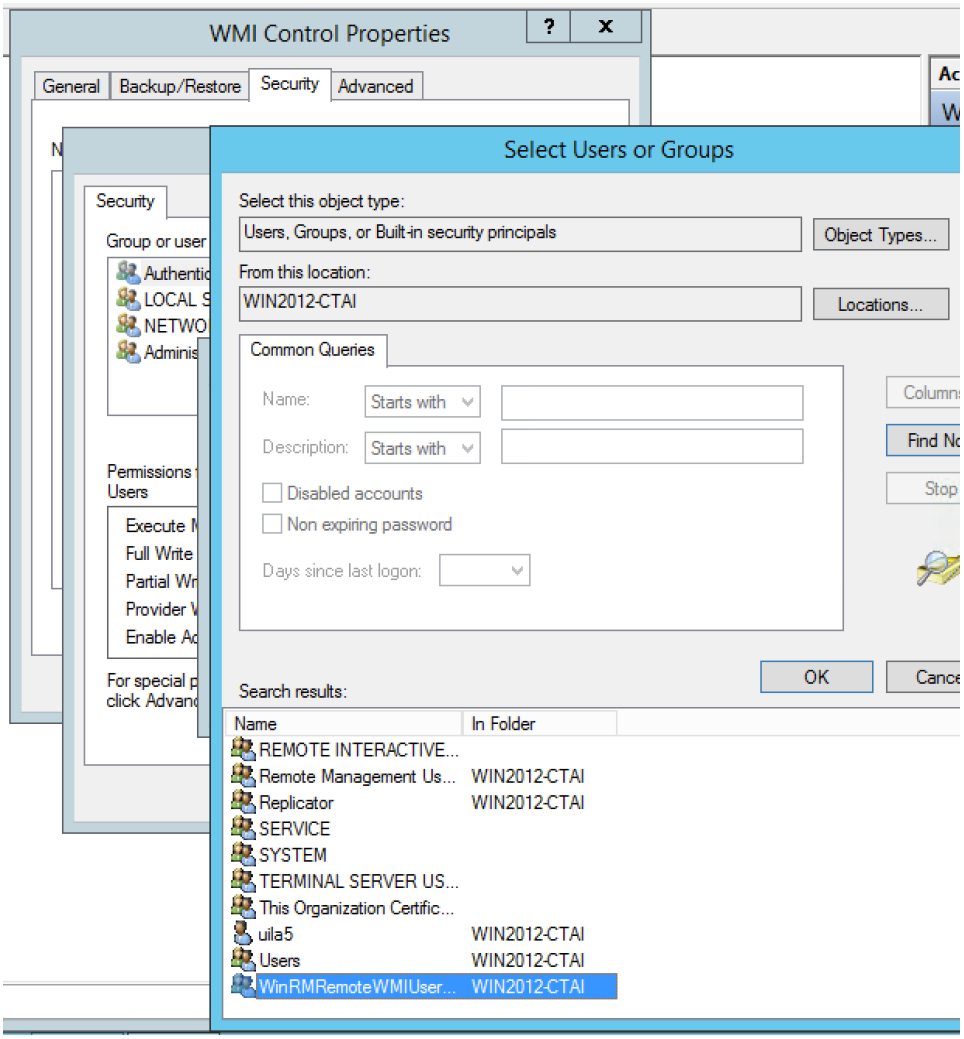


This will allow this user access to DCOM and performance log access. But not WMI access as we need to set what classes are available to that user.

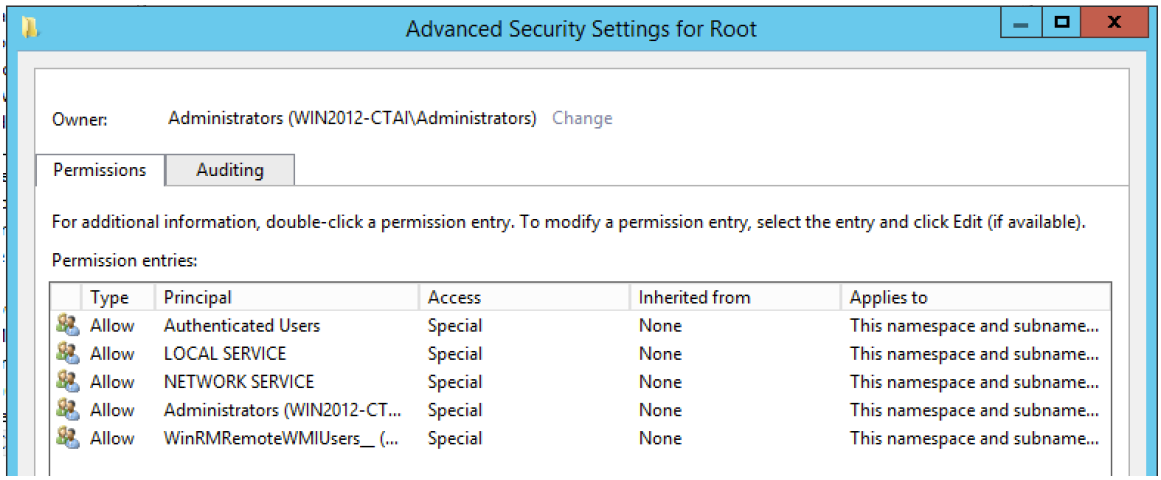
To give access to all the classes of the WMI counters, right click Computer Manager >> Services and Applications >> WMI Control and select Properties.
Then select the Security tab and select the Root namespace, and select the Security button:



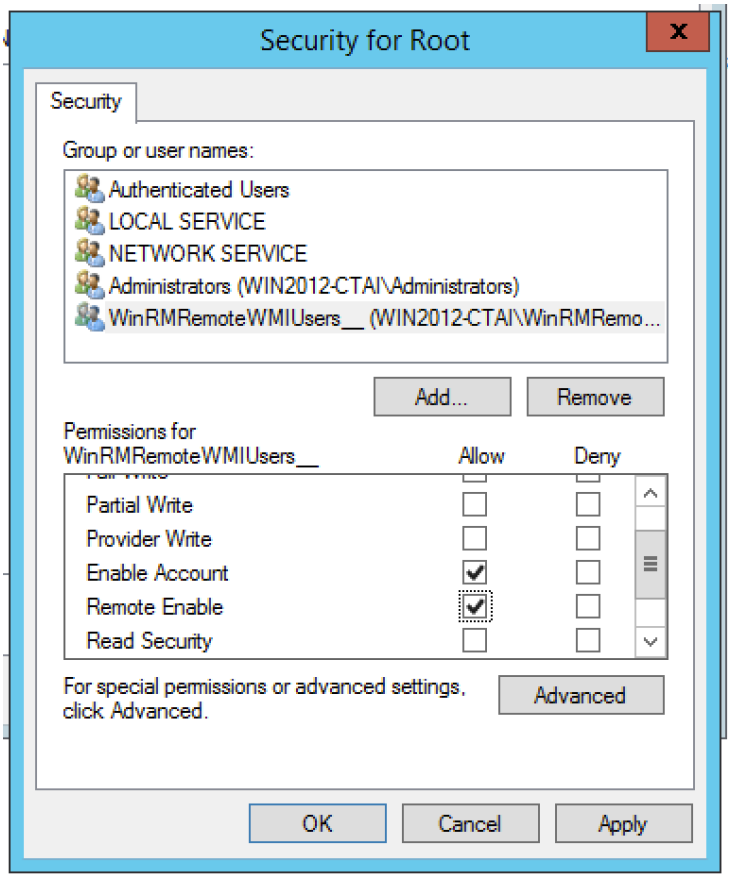
We need to add the WinRMWMIUsers__ group into this list:



Make sure the Remote Enable is checked for this and subsequent namespaces:



The permissions should look like this:

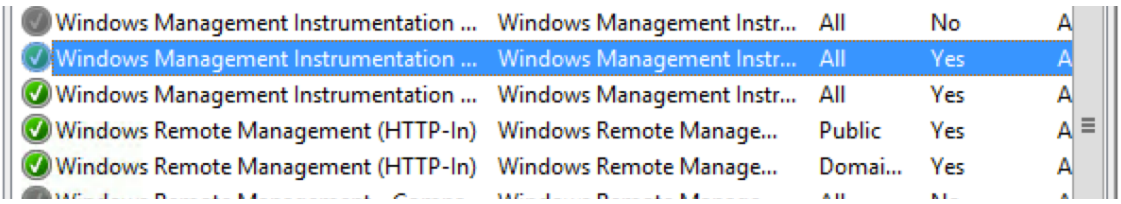


This will be enough for the user to login using the test:

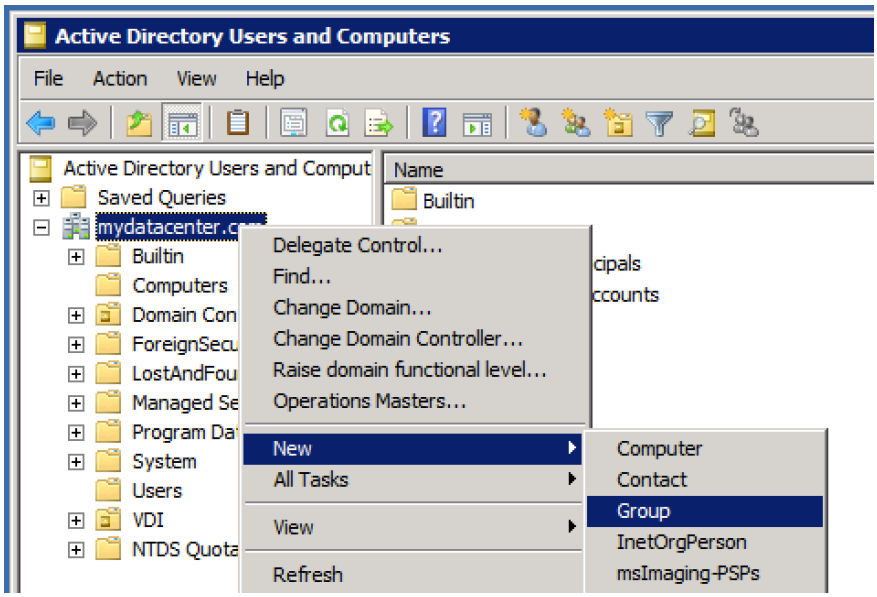
```
VIM >/usr/local/nagios/bin/wmic //192.168.0.129 -U uila5%password "select * from win32_computersystem”
```

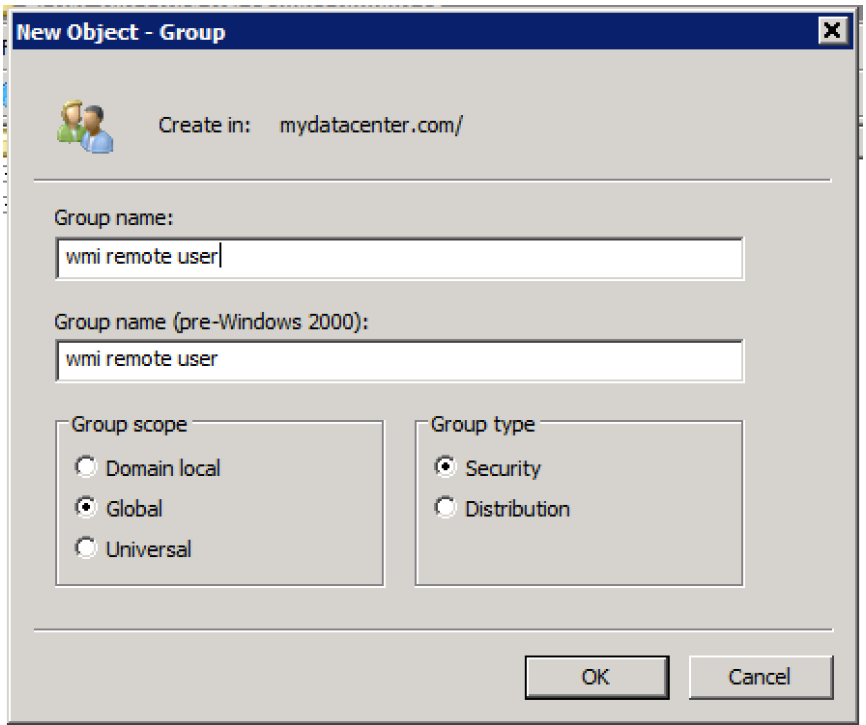
3 - Adding a host that is using a Domain Account

Make sure the firewall is open for Ping, DCOM and WMI as before.

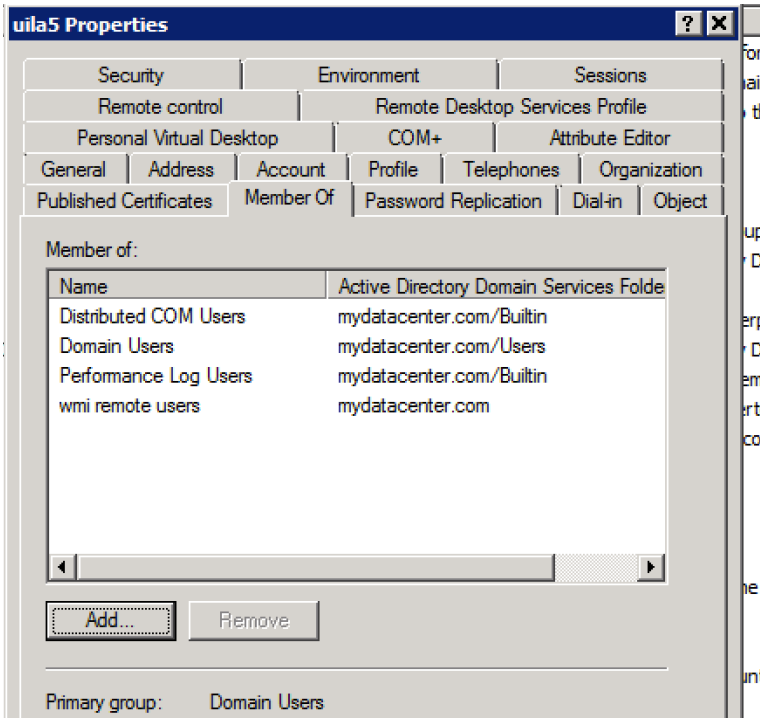


At the AD, the user account (i.e. Uila5) will need to be in a new group that can be given permissions to the WMI classes. So we can create a new group on the AD:

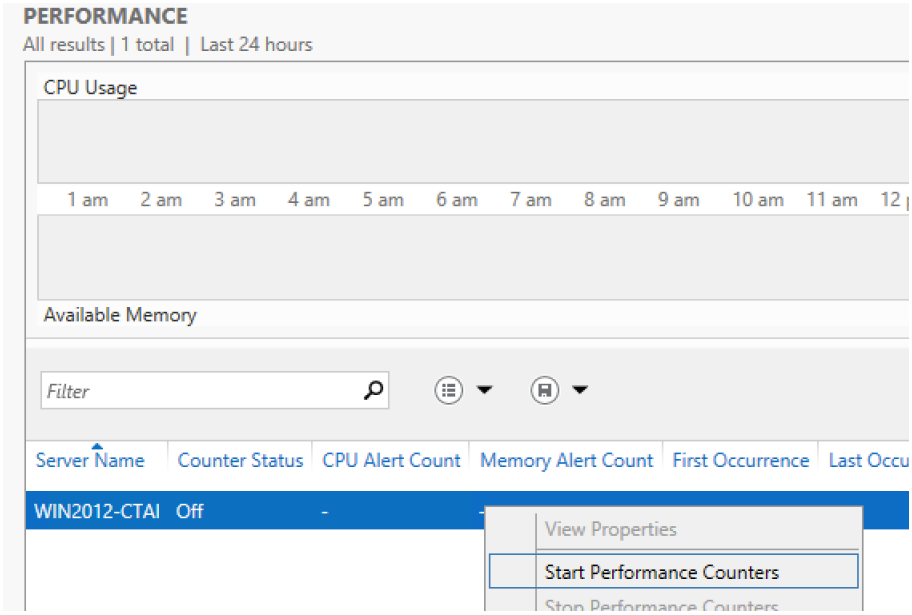




Make sure the user account on the AD is a member of following groups:
Distributed COM Users, Performance Log Users, and a new group called ‘wmi remote users’.

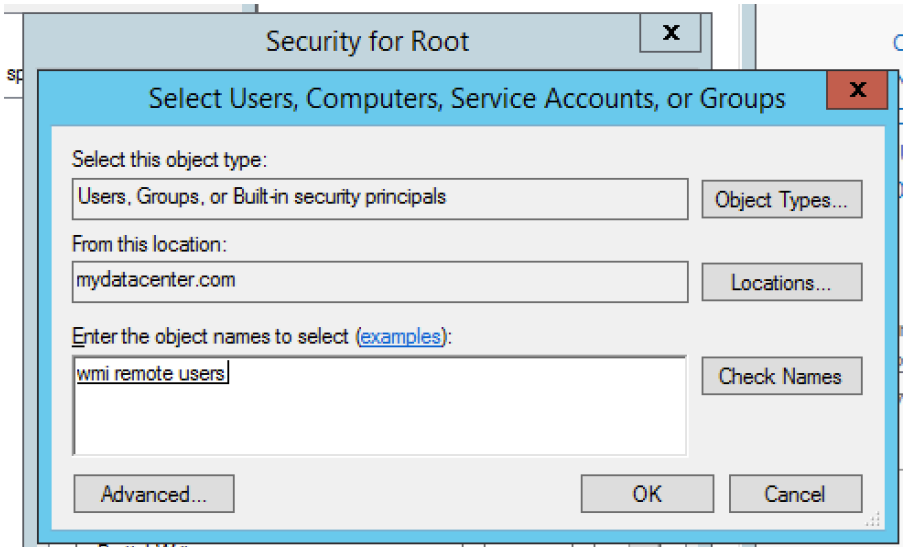


At the monitoring host, make sure to enable the performance counters that we will be querying for:

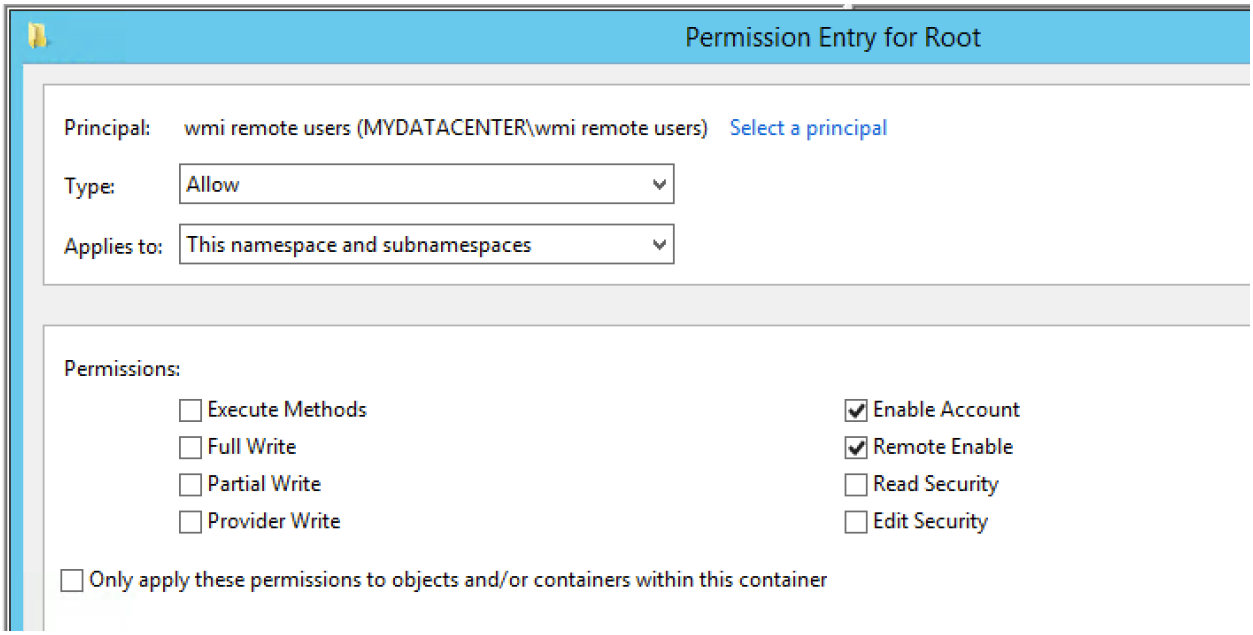


This can take 15 -30 minutes before counters will be available, so start this early.

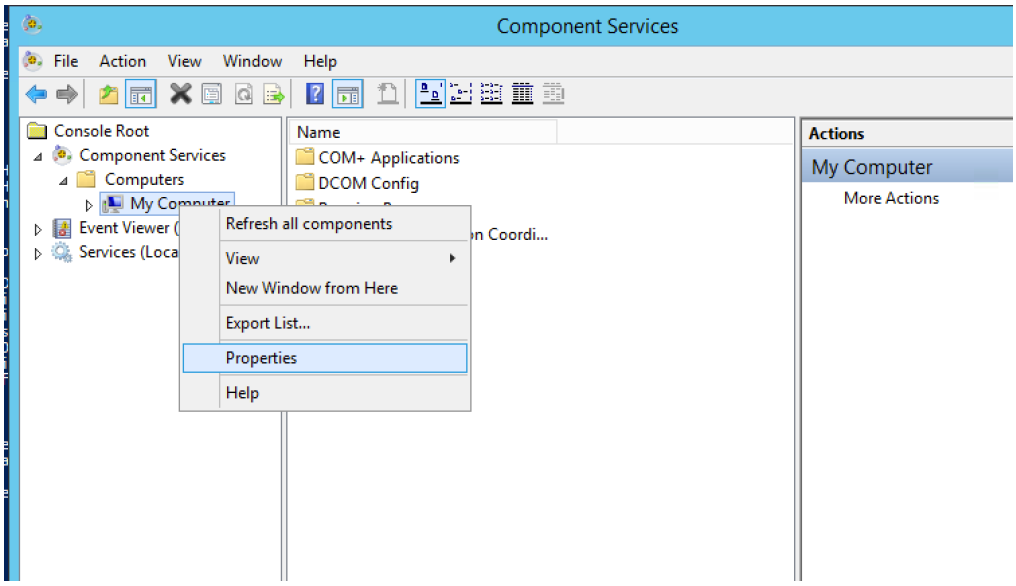
On the monitoring host, run ‘wmimgmt’ from the powershell and right click the ‘WMI Control’ and select Properties. Select ‘Root’ then ‘Security’ and add the group we created before:



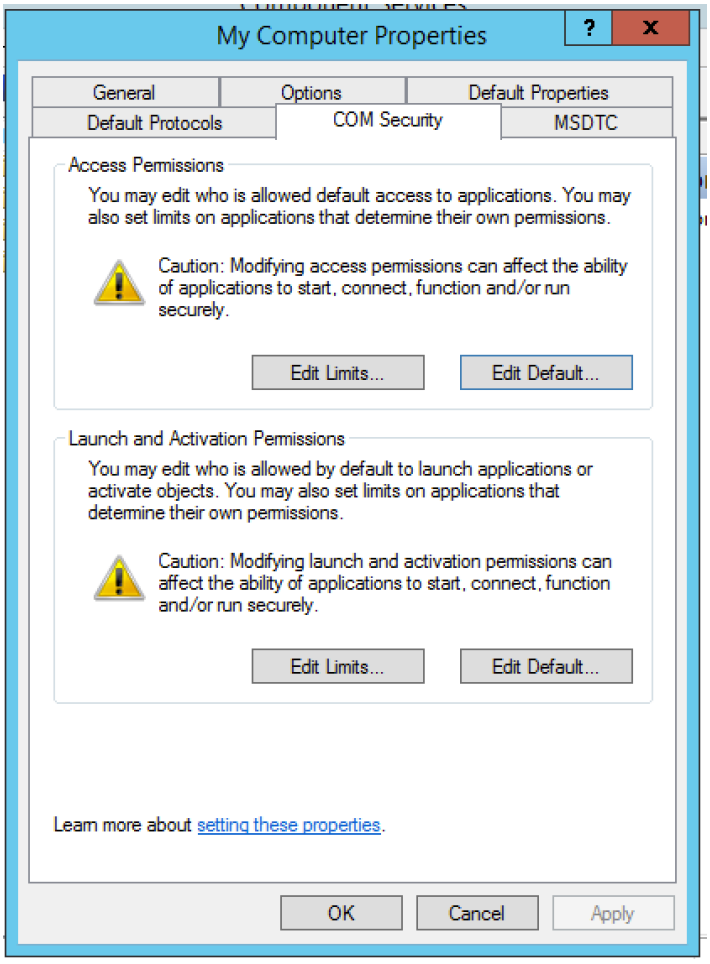
Then select ‘Advanced’ to change its permissions to the NameSpace and Subsequent Namespaces and “Remote Enable”:



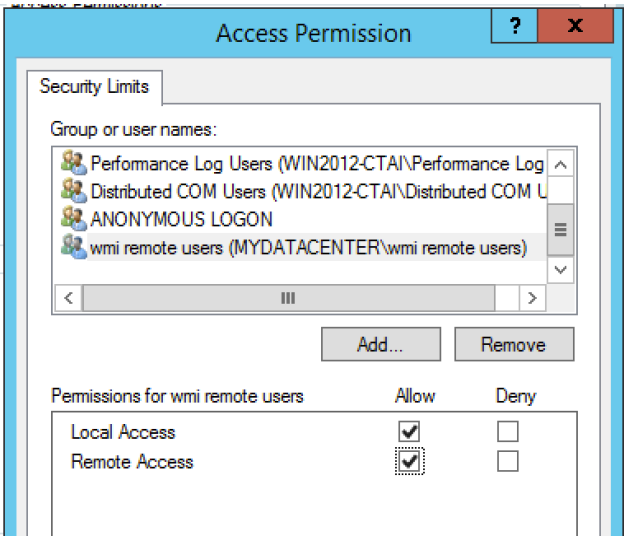
We need to give this group access to the DCOM. Run ‘dcomcnfg’ from a powershell and select the Component Services >> Computers >> My Computer. Right click to bring up the properties:

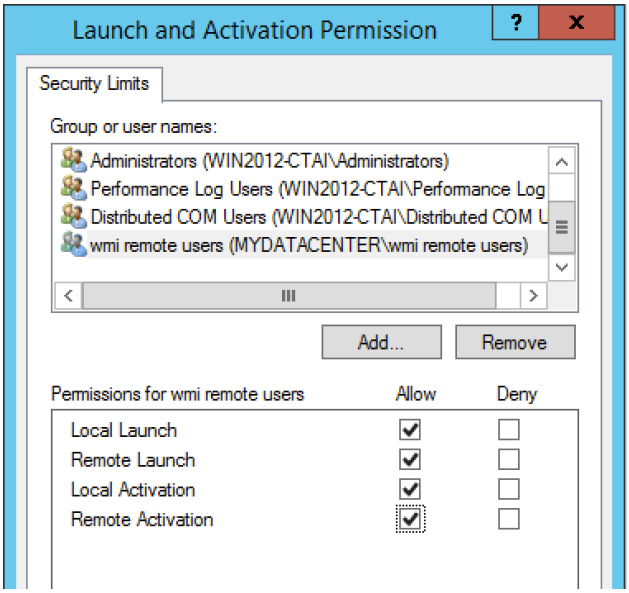


Select the COM Security tab:

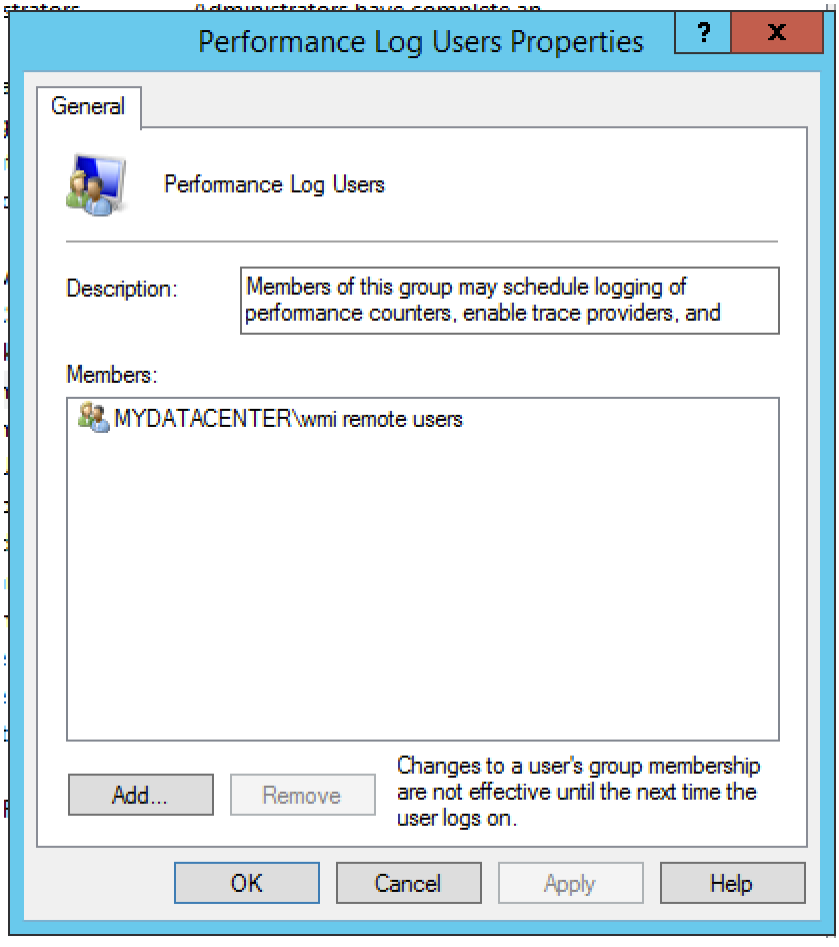


Add the group we created to the 2 Edit Limits and enable the following options:





Add the group to the local Performance Logs. At the host, run “lusrmgr” and select the Group - ‘Performance Log Users’ and add the group we created:



Running the test program. Make sure to add the Domain/User%password :

```
VIM >/usr/local/nagios/bin/wmic //192.168.0.129 -U mydatacenter.com/
uila5%password "select * from win32_computersystem"
```

```
CLASS: Win32_ComputerSystem
AdminPasswordStatus|AutomaticManagedPagefile|AutomaticResetBootOption|
AutomaticResetCapability|BootOptionOnLimit|BootOptionOnWatchDog|
BootROMSupported|BootupState|Caption|ChassisBootupState|CreationClassName|
CurrentTimeZone|DaylightInEffect|Description|DNSHostName|Domain|DomainRole|
EnableDaylightSavingsTime|FrontPanelResetStatus|HypervisorPresent|
InfraredSupported|InitialLoadInfo|InstallDate|KeyboardPasswordStatus|
LastLoadInfo|Manufacturer|Model|Name|NameFormat|NetworkServerModeEnabled|
NumberOfLogicalProcessors|NumberOfProcessors|OEMLogoBitmap|OEMStringArray|
PartOfDomain|PauseAfterReset|PCSystemType|PCSystemTypeEx|
PowerManagementCapabilities|PowerManagementSupported|PowerOnPasswordStatus|
PowerState|PowerSupplyState|PrimaryOwnerContact|PrimaryOwnerName|
ResetCapability|ResetCount|ResetLimit|Roles|Status|SupportContactDescription|
SystemStartupDelay|SystemStartupOptions|SystemStartupSetting|SystemType|
ThermalState|TotalPhysicalMemory|UserName|WakeUpType|Workgroup
3|True|True|True|0|0|True|Normal boot|WIN2012-CTAI|3|
Win32_ComputerSystem|-420|True|AT/AT COMPATIBLE|WIN2012-CTAI|
mydatacenter.com|3|True|3|True|False|NULL|(null)|3|(null)|Microsoft
Corporation|Virtual Machine|WIN2012-CTAI|(null)|True|1|1|NULL|([MS_VM_CERT/
SHA1/9b80ca0d5dd061ec9da4e494f4c3fd1196270c22],
0000000000000000000000000000000000,To be filed by MSFT)|True|3932100000|1|1|
NULL|False|3|0|3|(null)|Windows User|1|-1|-1|
(LM_Workstation,LM_Server,NT,Server_NT)|OK|NULL|0|NULL|0|x64-based PC|1|
2147012608|(null)|6|(null)
```

This will test the counter Nagios will be reading:

```
VIM >/usr/local/nagios/bin/wmic //192.168.0.129 -U mydatacenter.com/
uila5%password "select IDProcess,Name,PercentProcessorTime,WorkingSetPrivate
from Win32_PerfFormattedData_PerfProc_Process where Name != '_Total' and Name
!= 'Idle'" | tail -n +4 | tr '|' ':'
```