

Partner

WMI Syslog Management of Windows AD Server

V009

2026/03/25



Copyright Declaration

N- Copyright © N-Partner Technologies Co. All Rights reserved. Without written authorization from N-Partner Technologies Co., anyone may not in any way copy, plagiarize or translate this manual. The system is keeping upgraded; therefore, N-Partner reserves the right to revise it without informing.

Registered Trademark

All company products, names and trademarks mentioned in this manual belongs to their legally registered organizations.

Contents

Preface.....	2
1. Windows 2000.....	3
1.1 Organizational Unit Settings.....	3
1.2 Group Policy Settings.....	6
1.3 Add Non-Admin Accounts.....	12
1.3.1 Add Users.....	12
1.3.2 Configure DCOM Permissions.....	15
1.3.3 Configure WMI Permissions.....	19
1.3.4 Configure Event Log Read Permissions.....	27
1.3.5 Restart the WMI Service.....	34
2. Windows 2003.....	35
2.1 Organizational Unit Settings.....	35
2.2 Group Policy Settings.....	38
2.3 Add a Non-Admin Account.....	44
2.3.1 Add Users.....	44
2.3.2 Configure DCOM Permissions.....	45
2.3.3 Configure WMI Permissions.....	49
2.3.4 Configure Event Log Read Permissions.....	58
2.3.5 Restart the WMI Service.....	65
2.4 Firewall Configuration.....	67
3. Windows 2008.....	69
3.1 Organizational Unit Settings.....	69
3.2 Group Policy Settings.....	72
3.3 Add a Non-Admin Account.....	79
3.3.1 Add Users.....	79
3.3.2 Configure DCOM Permissions.....	80
3.3.3 Configure WMI Permissions.....	84
3.3.4 Configure Event Log Read Permissions.....	92
3.3.5 Restart WMI Service.....	98
3.4 Configure Firewall.....	99
4. Windows 2012.....	101
4.1 Organizational Unit Settings.....	101
4.2 Group Policy Settings.....	104
4.3 Add a Non-Admin Account.....	110
4.3.1 Add Users.....	110
4.3.2 Configure DCOM Permissions.....	111
4.3.3 Configure WMI Permissions.....	115
4.3.4 Configure Event Log Read Permissions.....	123
4.3.5 Restart the WMI Service.....	128
4.4 Configure the Firewall.....	129
5. Windows 2016.....	130
5.1 Organizational Unit Settings.....	130
5.2 Group Policy Settings.....	133
5.3 Add a Non-Admin Account.....	140
5.3.1 Add Users.....	140
5.3.2 Configure DCOM Permissions.....	141
5.3.3 Configure WMI Permissions.....	145
5.3.4 Configure Event Log Read Permissions.....	153
5.3.5 Restart the WMI Service.....	158
5.4 Configure the Firewall.....	159
6. Windows 2019.....	160
6.1 Organizational Unit Settings.....	160
6.2 Group Policy Settings.....	163
6.3 Add a Non-Admin Account.....	170
6.3.1 Add Users.....	170
6.3.2 Configure DCOM Permissions.....	171
6.3.3 Configure WMI Permissions.....	176
6.3.4 Configure Event Log Read Permissions.....	185
6.3.5 Restart the WMI Service.....	190
6.4 Configure Firewall.....	191
7. Windows 2022.....	192
7.1 Organizational Unit Settings.....	192
7.2 Group Policy Settings.....	195
7.3 Add a Non-Admin Account.....	202
7.3.1 Add Users.....	202
7.3.2 Configure DCOM Permissions.....	203
7.3.3 Configure WMI Permissions.....	207
7.3.4 Configure Event Log Read Permissions.....	215
7.3.5 Restart the WMI Service.....	220
7.4 Configure Firewall.....	221
8. N-Reporter.....	222
8.1 For Windows 2003 or Earlier.....	223
8.2 For Windows 2008 or Later.....	229
9. Troubleshooting.....	235
9.1 Invoke-GPUUpdate Error.....	235
9.2 WMI Query Language Verification.....	237

Preface

This document introduces how to use WMI to manage the syslog of Windows AD Server for N-Reporter.

Audit Policy Recommendations: <https://docs.microsoft.com/zh-tw/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations>

Note: This document serves only as a reference for using WMI to capture log settings. It is recommended to contact the device or software manufacturer for assistance with log retrieval via WMI.

1. Windows 2000

For detailed information on setting Windows audit policies, please refer to the “audit policy recommendations link” in the preface.

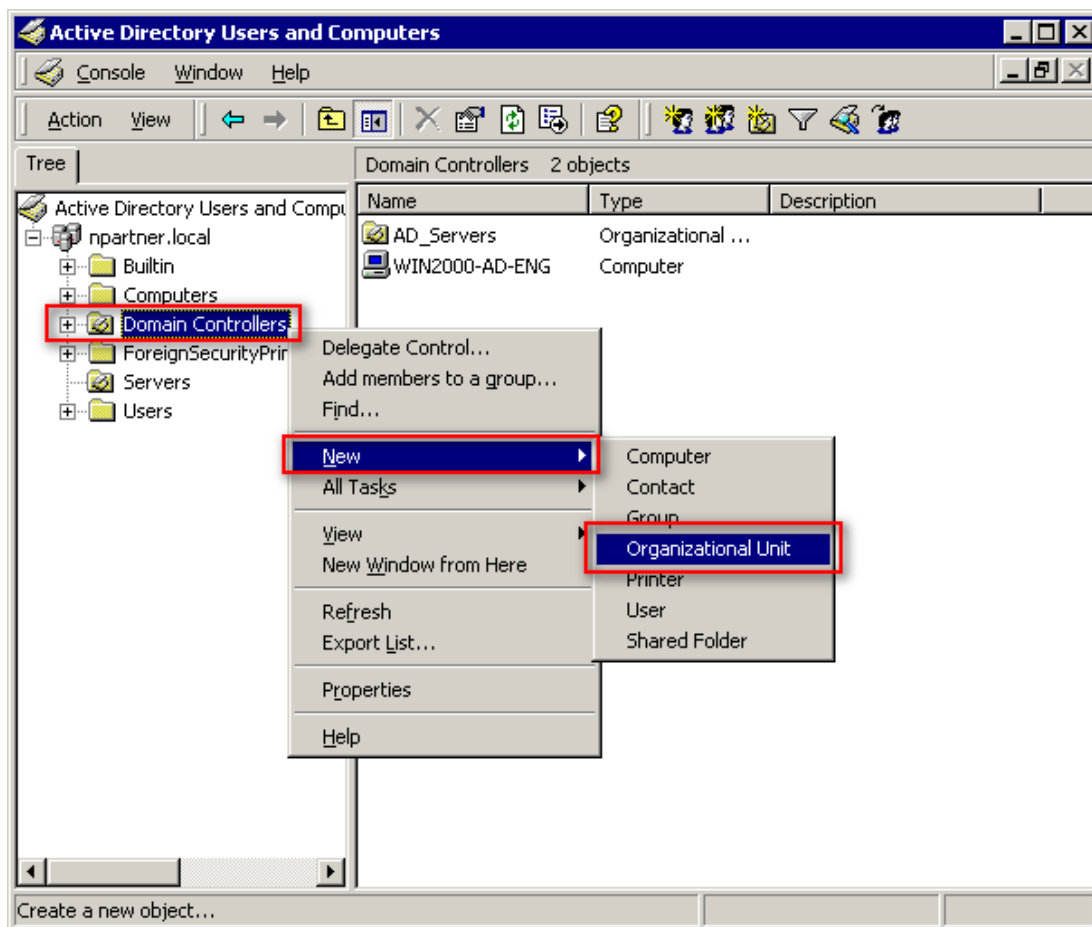
1.1 Organizational Unit Settings

(1) Click “Active Directory Users and Computers.”



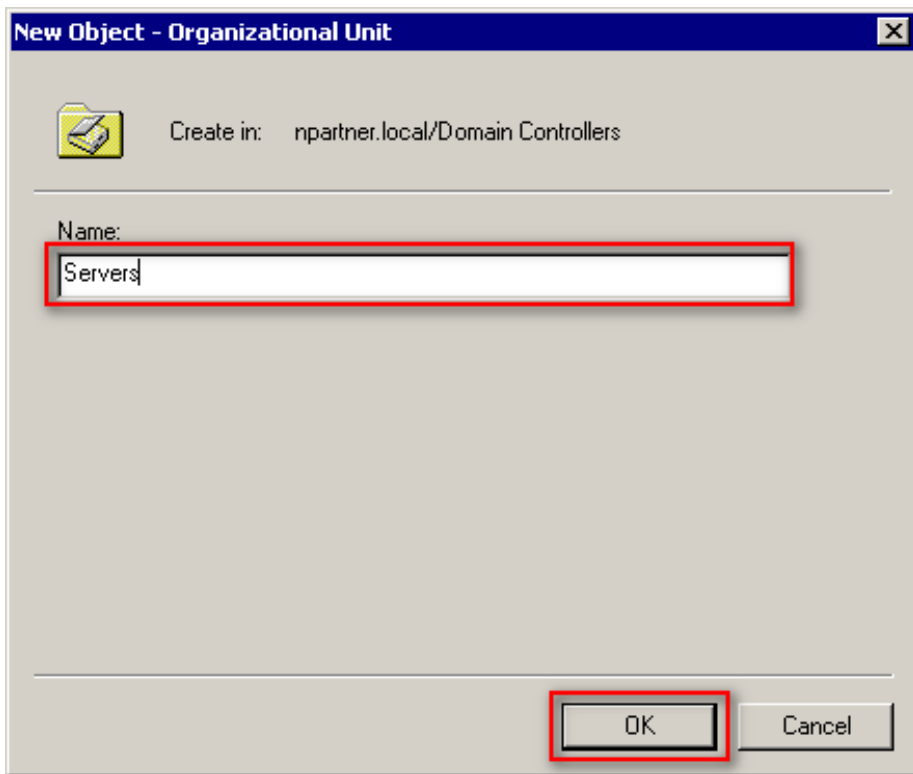
(2) Add an Organizational Unit

Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

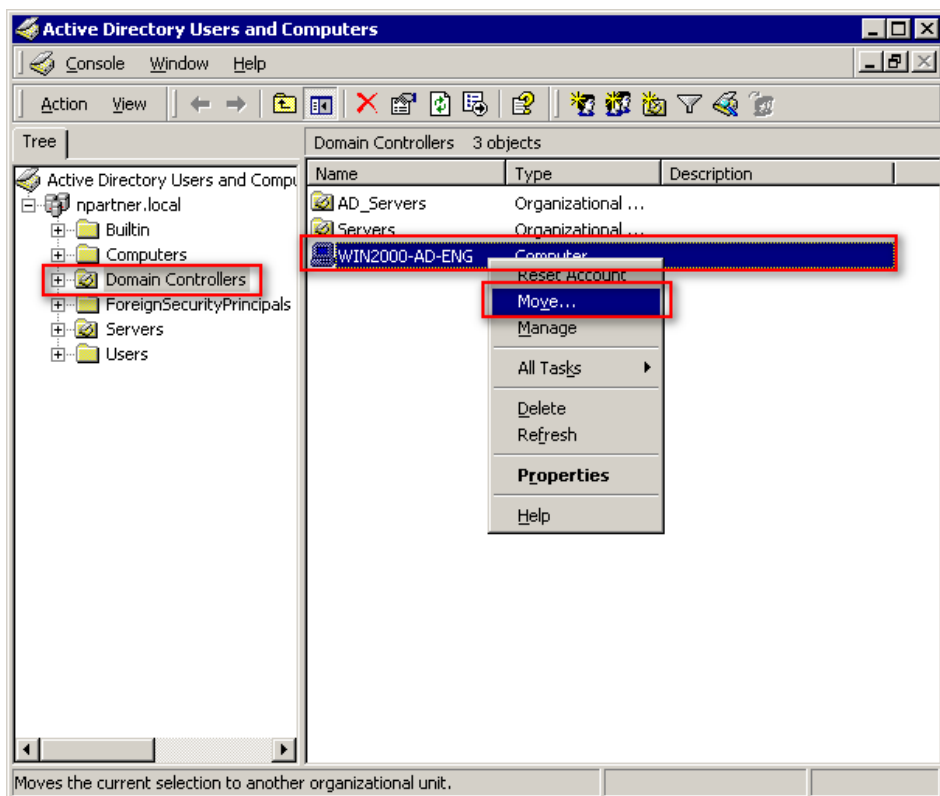
Note: Please create the organizational unit name according to the customer's environment. -> Click “OK.”



(4) Move the Server to your New Organizational Unit:

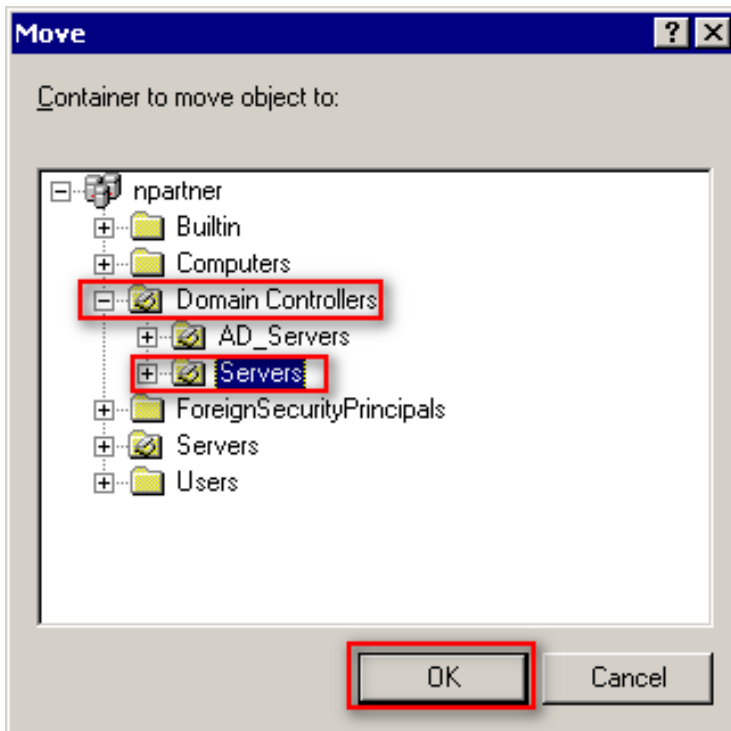
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2000-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



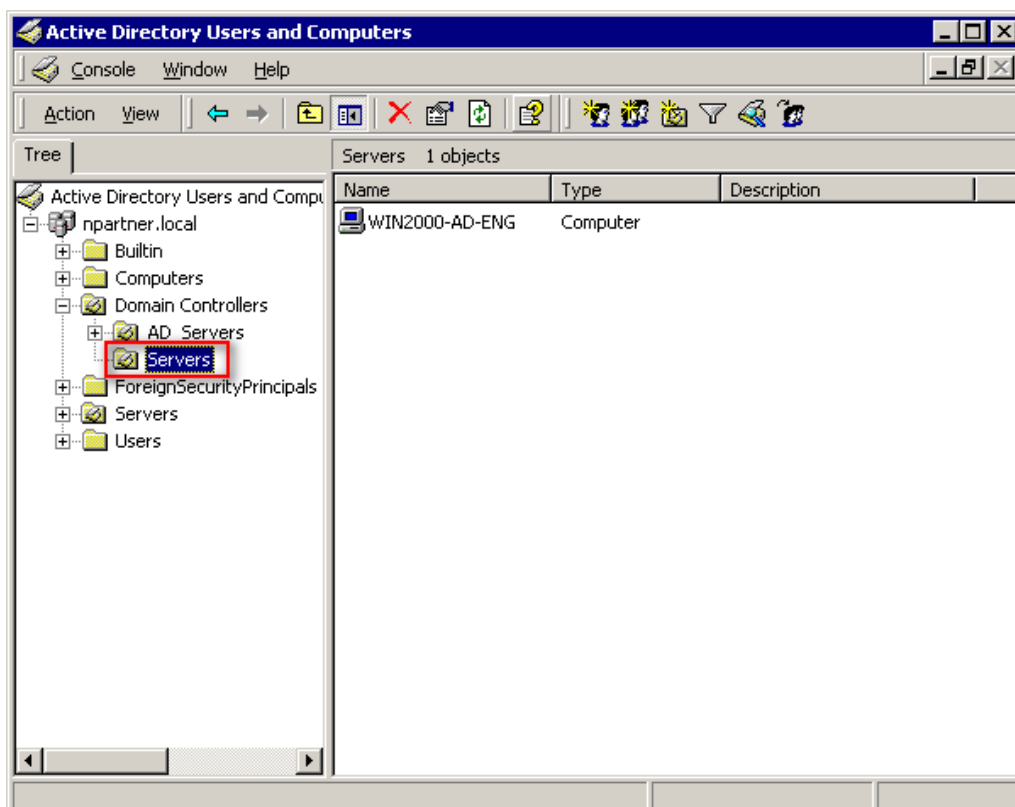
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2000-AD-ENG” server has been moved.

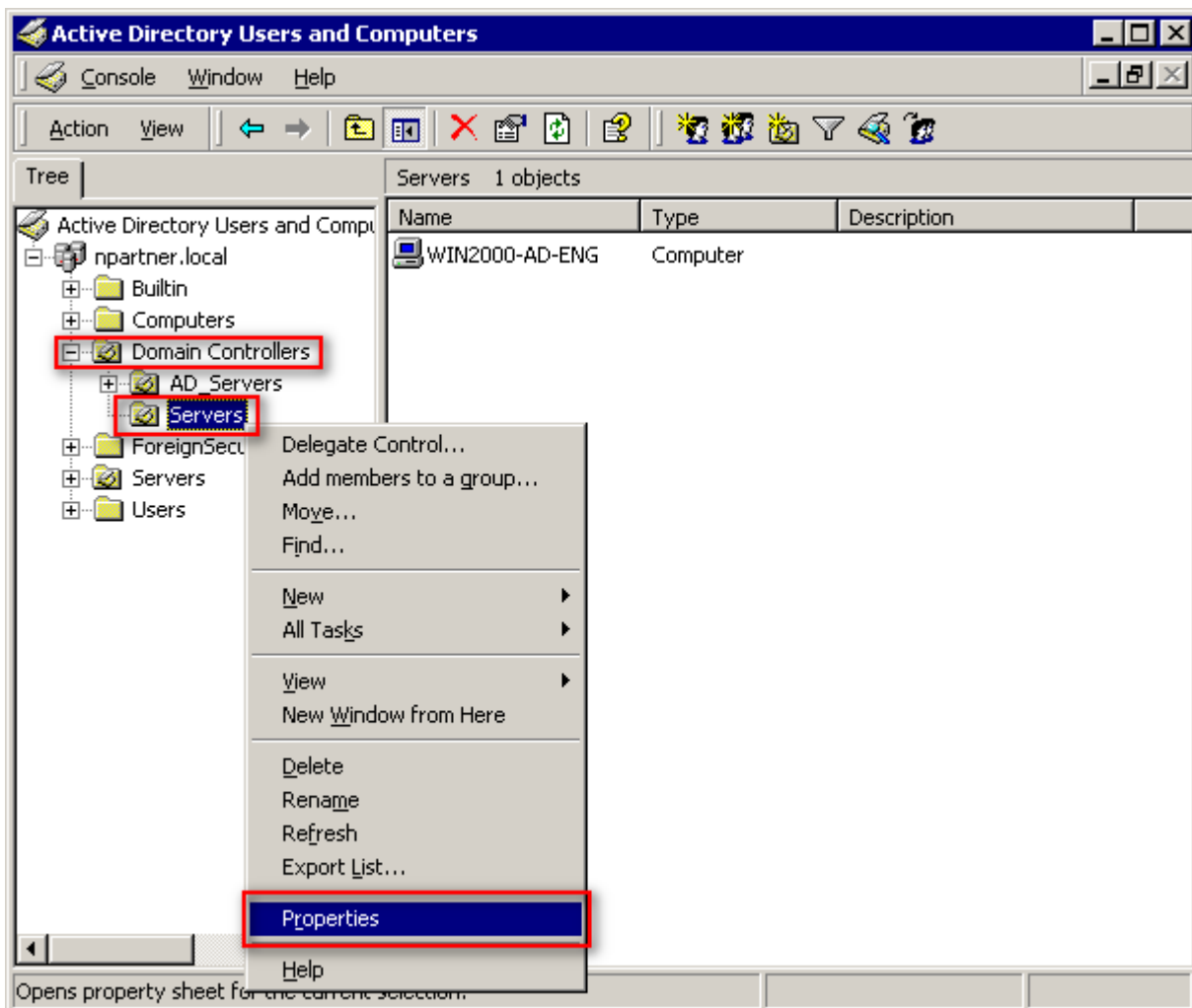


1.2 Group Policy Settings

(1) Click “Active Directory Users and Computers.”

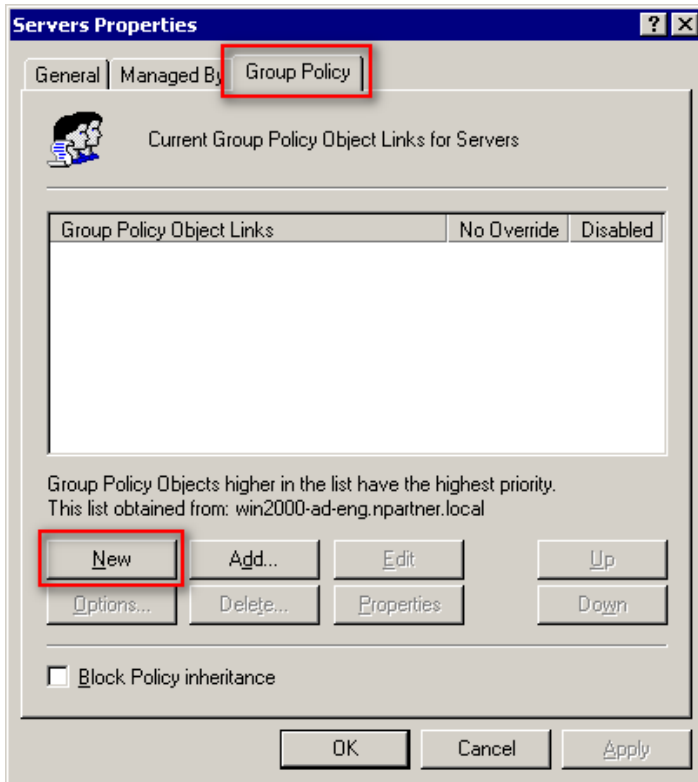


(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Properties.”



(3) Enter your Group Policy Object Name

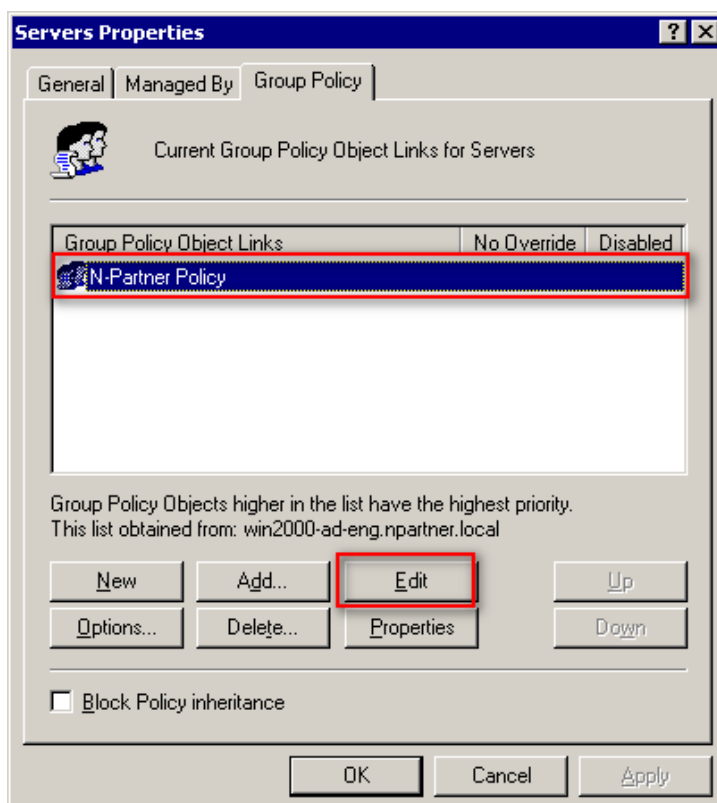
On the “Group Policy” tab, click “New.”



(4) Edit your Group Policy Object

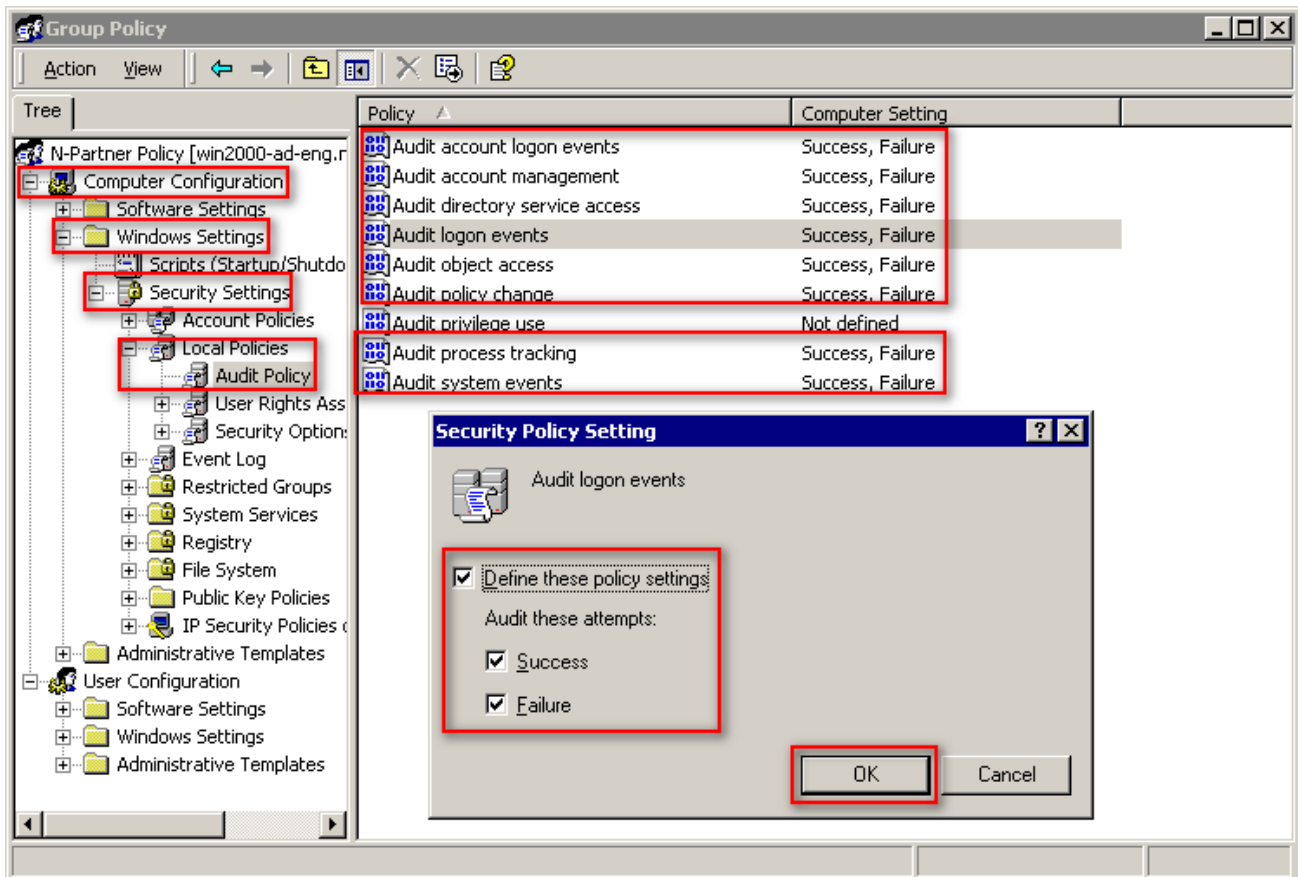
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the client's environment. Then click “Edit.”



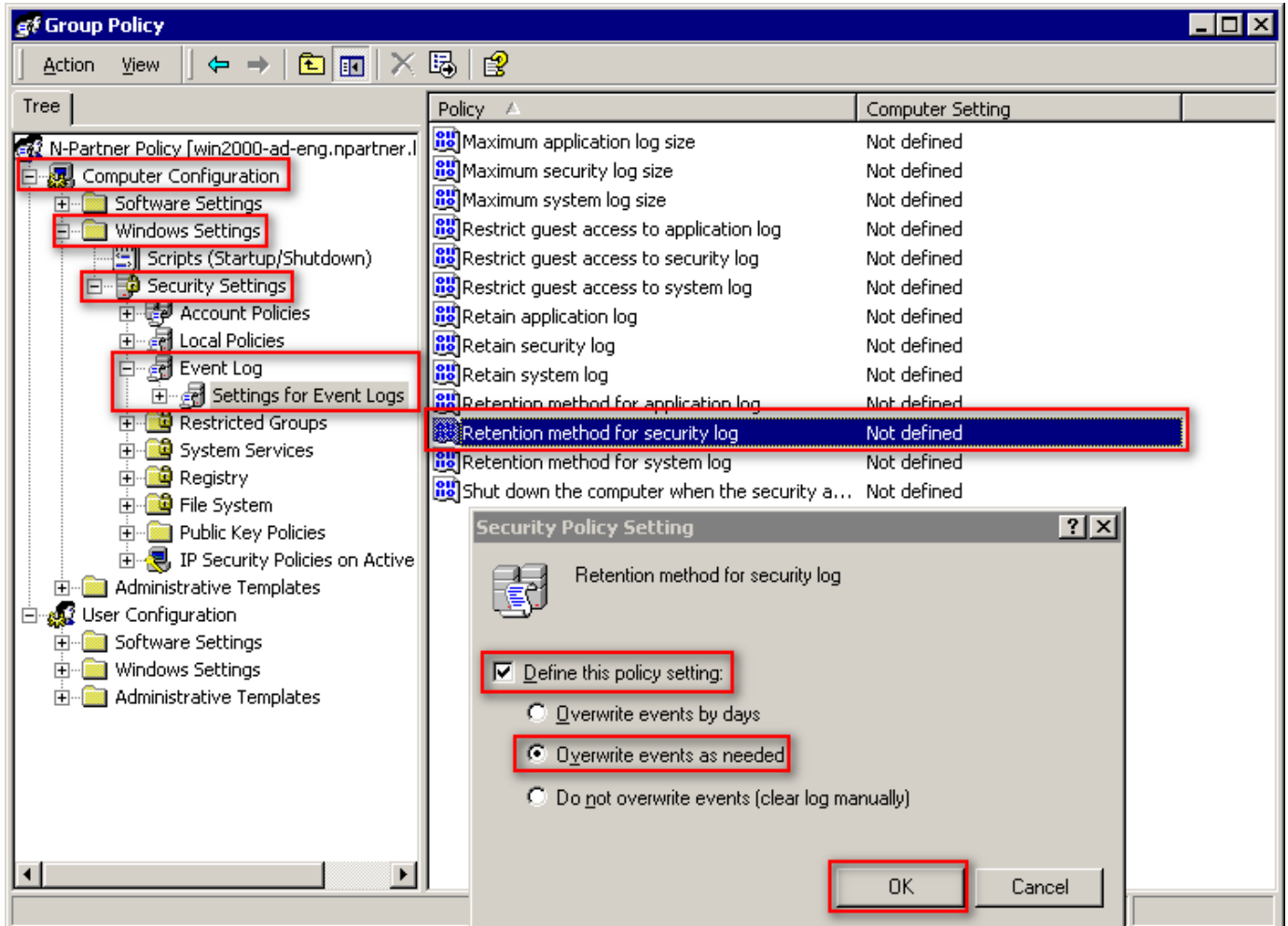
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Retention Method for Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting” -> Select “Overwrite events as needed” -> Then click “OK.”



(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click “OK.”

The screenshot displays the Group Policy console for an N-Partner Policy. The left-hand tree view shows the navigation path: Computer Configuration > Windows Settings > Security Settings > Event Log > Settings for Event Logs. The right-hand pane shows a list of policies, with 'Maximum security log size' selected and highlighted in blue. This policy is currently set to '204800 kilobytes'. A 'Security Policy Setting' dialog box is open in the foreground, showing the 'Maximum security log size' configuration. The checkbox 'Define this policy setting' is checked, and the value '204800' is entered in the text box, followed by 'kilobytes'. The 'OK' button is highlighted with a red box.

Policy	Computer Setting
Maximum application log size	Not defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not defined
Restrict guest access to application log	Not defined
Restrict guest access to security log	Not defined
Restrict guest access to system log	Not defined
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Not defined
Retention method for security log	As needed
Retention method for system log	Not defined
Shut down the computer when the security a...	Not defined

(8) Open "Command Prompt" on your Windows Server.



(9) Enter the command below to refresh group policy.

```
C:\> secedit /refreshpolicy machine_policy /enforce
```

A screenshot of a Windows Command Prompt window. The title bar reads "C:\> Command Prompt". The command prompt shows the command `secedit /refreshpolicy machine_policy /enforce` being entered. The output of the command is: `Group policy propagation from the domain has been initiated for this computer. It may take a few minutes for the propagation to complete and the new policy to take effect. Please check Application Log for errors, if any.` The prompt ends with `C:\>_`.


```
C:\>secedit /refreshpolicy machine_policy /enforce
Group policy propagation from the domain has been initiated for this computer. It
may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>_
```

1.3 Add Non-Admin Accounts

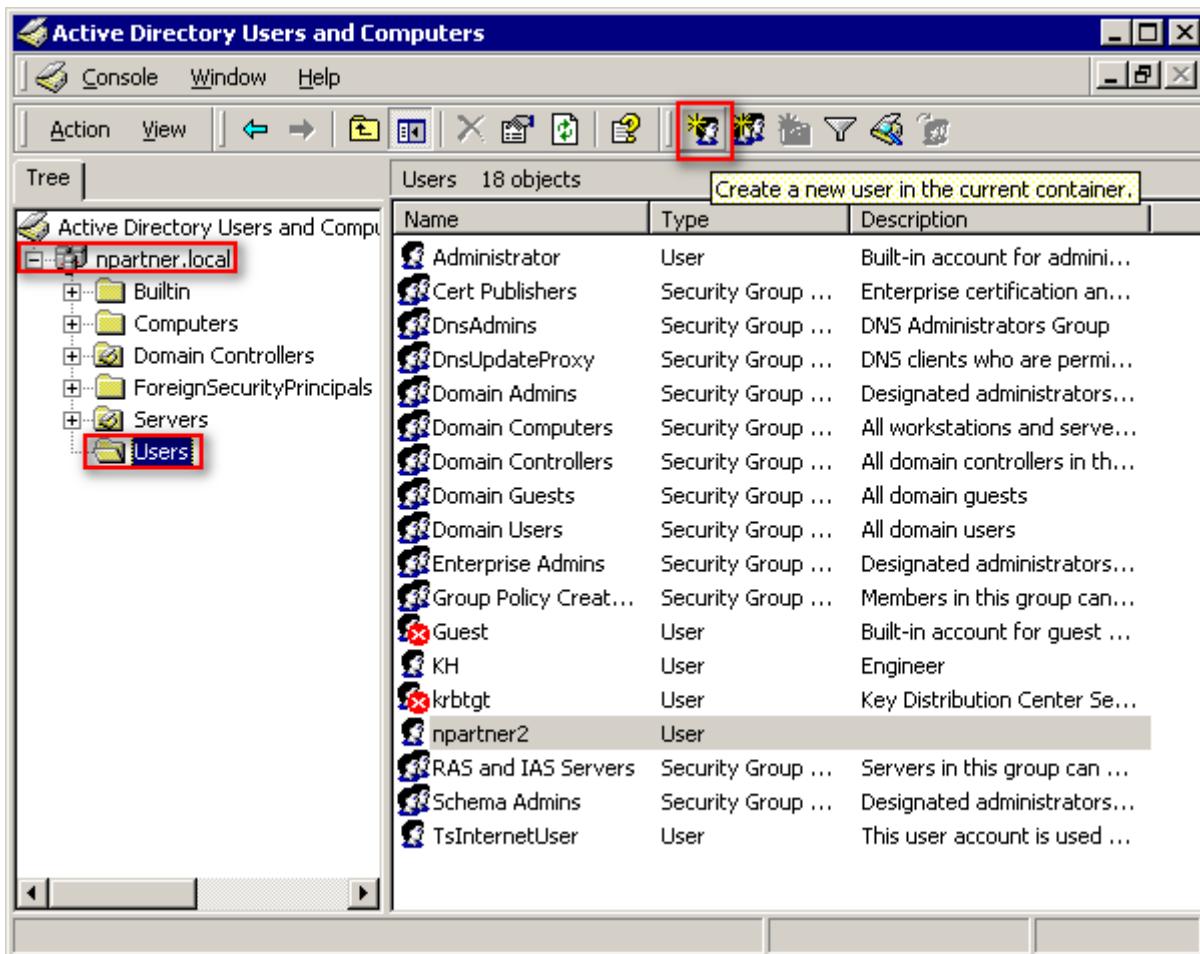
1.3.1 Add Users

(1) Open “Active Directory Users and Computers.”



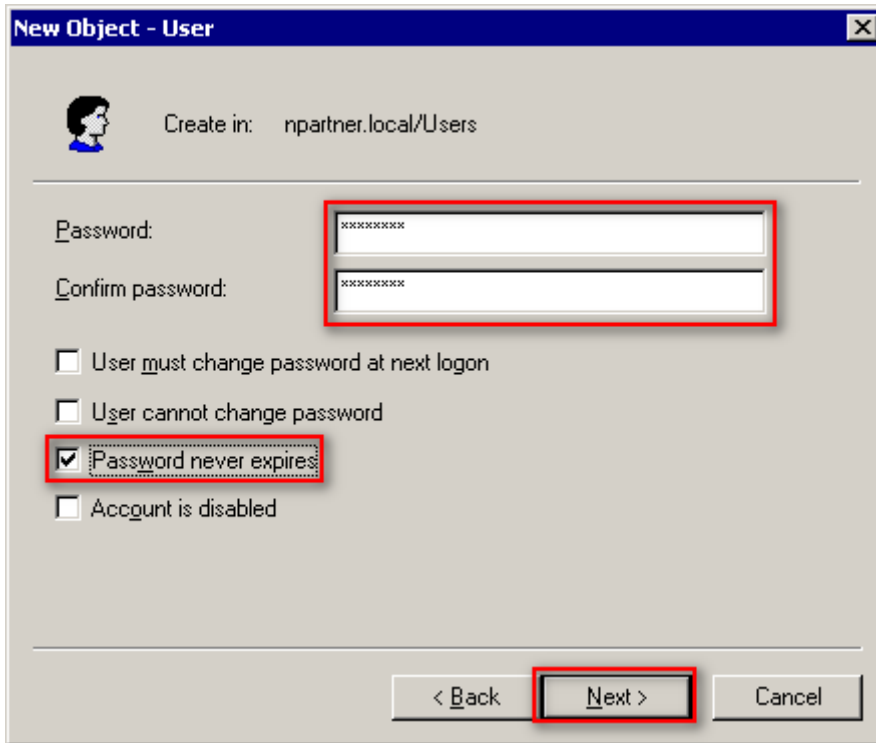
(2) In “Users” organizational unit of your domain name, click  to create a new user.

Note: Select your organizational unit according to the actual environment



(3) Enter your full name (in this example, it is “npartner”) and user logon name (in this example, it is “npartner”), then click “Next.”

(4) Enter your password and confirm the password, check “Password never expires,” then click “Next.”



New Object - User

Create in: npartner.local/Users

Password: [xxxxxxx]

Confirm password: [xxxxxxx]

User must change password at next logon

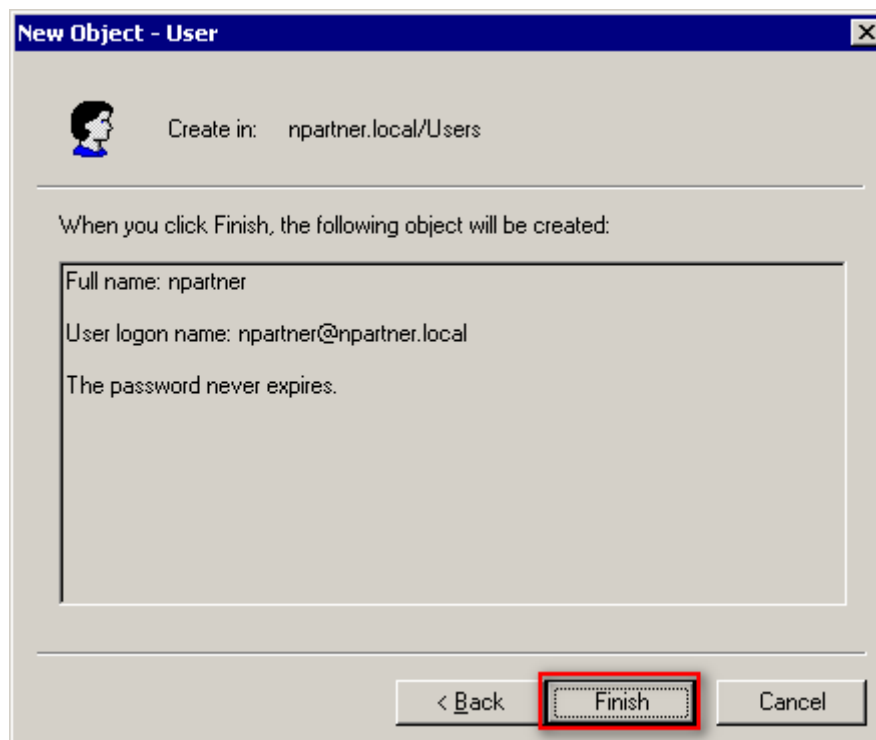
User cannot change password

Password never expires

Account is disabled

< Back **Next >** Cancel

(5) Click “Finish.”



New Object - User

Create in: npartner.local/Users

When you click Finish, the following object will be created:

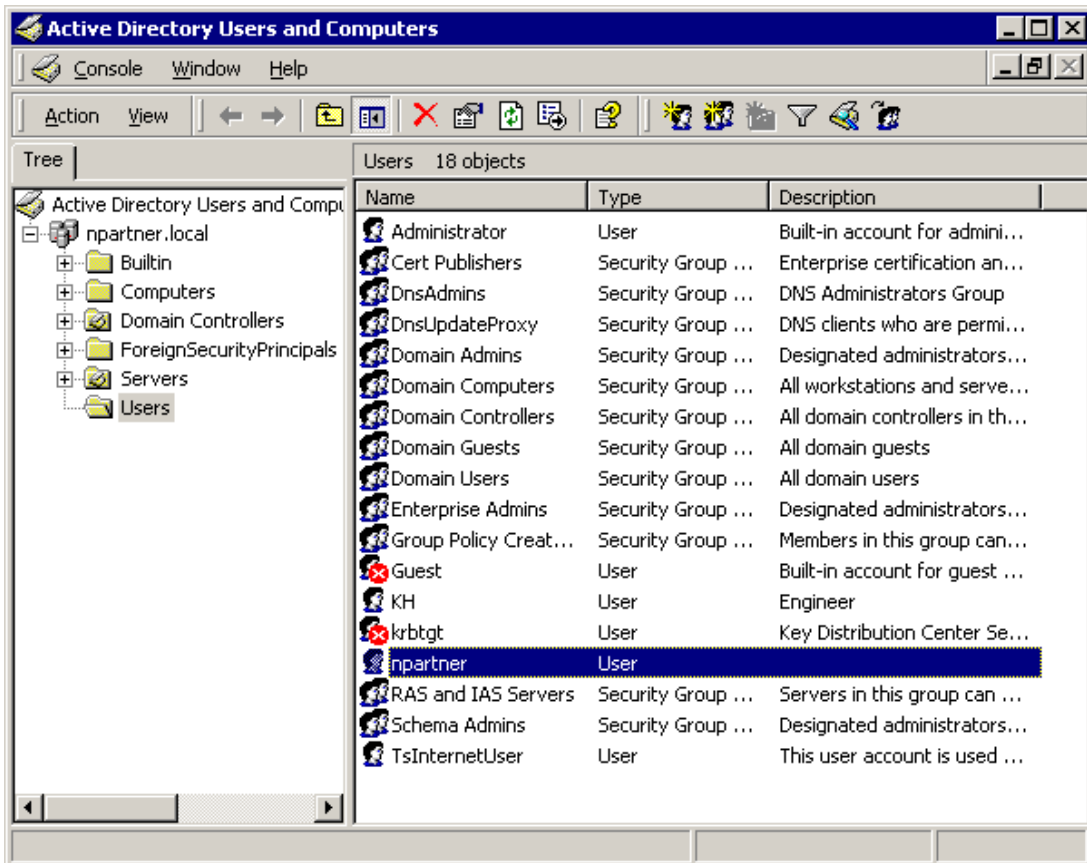
Full name: npartner

User logon name: npartner@npartner.local

The password never expires.

< Back **Finish** Cancel

(6) Check the account status.



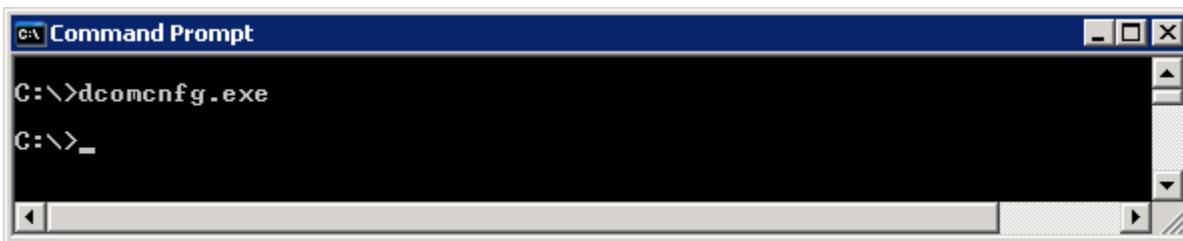
1.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”



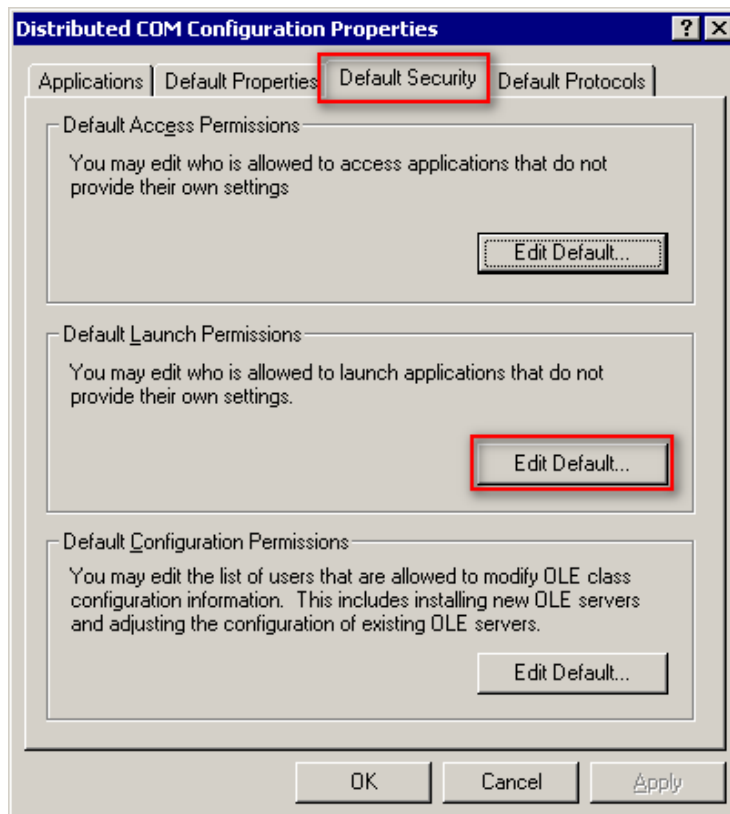
(2) Enter the command below to enable component services.

```
C:\> dcomcnfg.exe
```



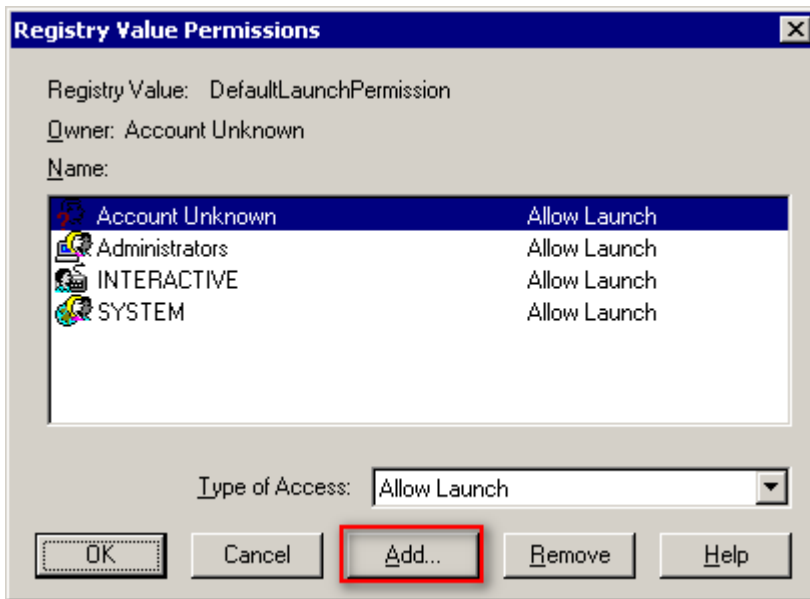
(3) Enable Default Access Permissions

Please go to the “Default Security” tab and click “Edit Default” under “Default Launch Permissions.”

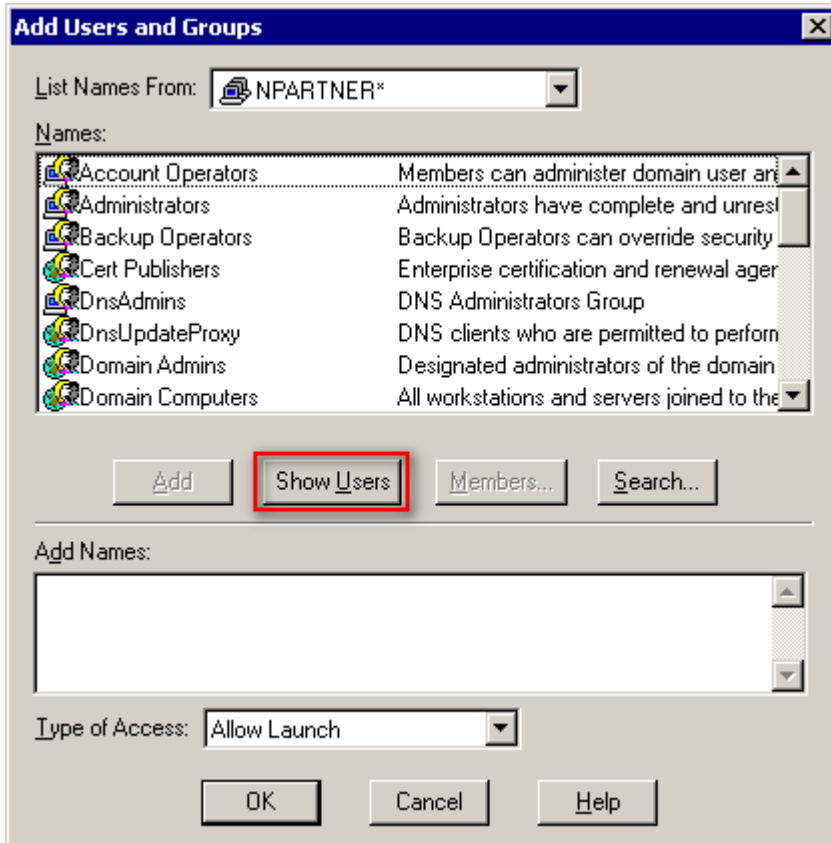


(4) Add User Permissions

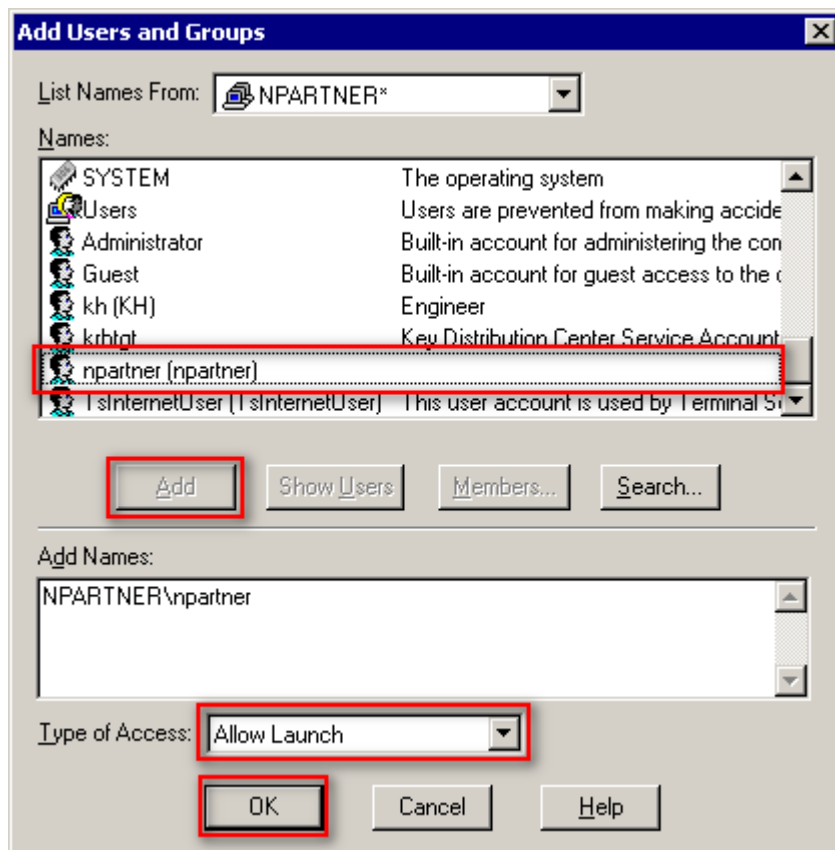
Click "Add...".



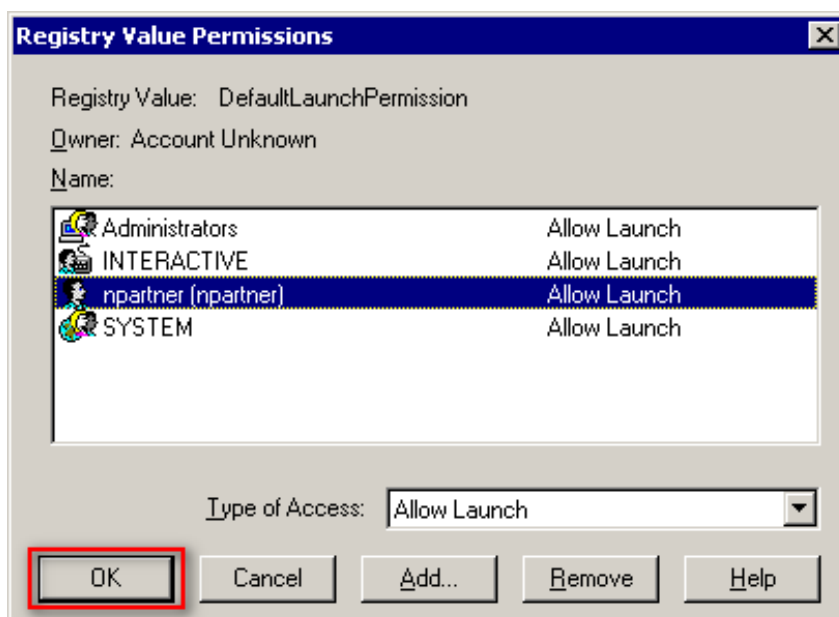
(5) Click "Show Users."



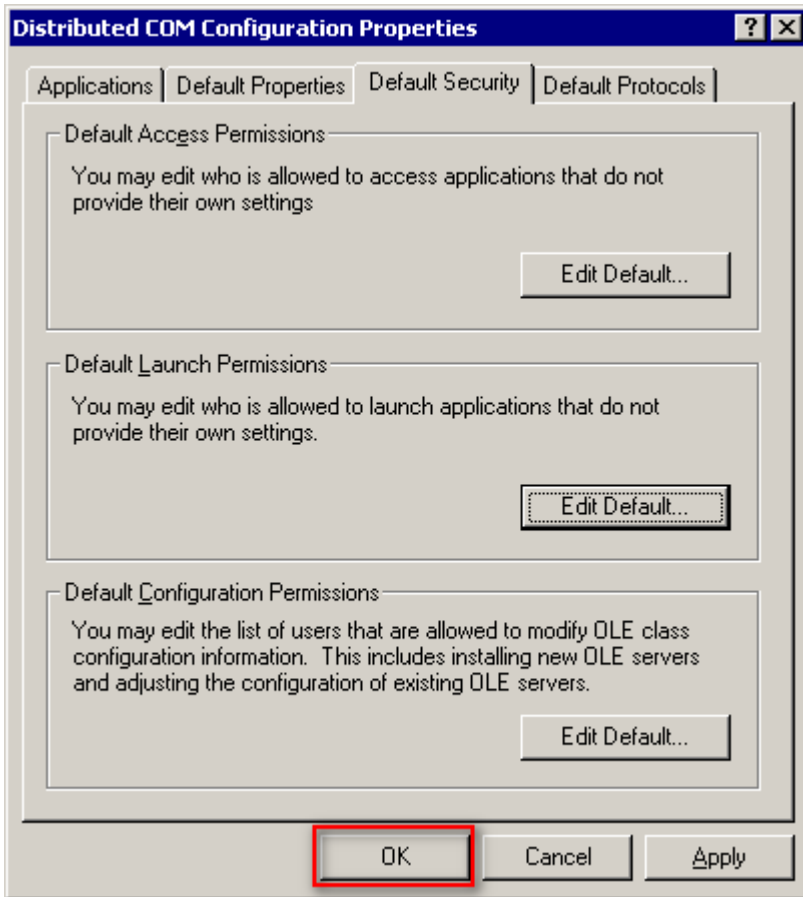
(6) Select your user account (in this example, it is “npartner”), click “Add”, set type of access to “Allow Launch,” then click “OK.”



(7) Click “OK.”



(8) Click "OK."



1.3.3 Configure WMI Permissions

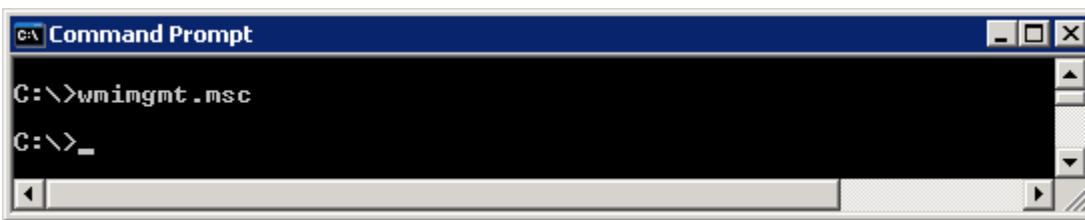
1.3.3.1 Configure Event Log Permissions

(1) Open “Command Prompt.”



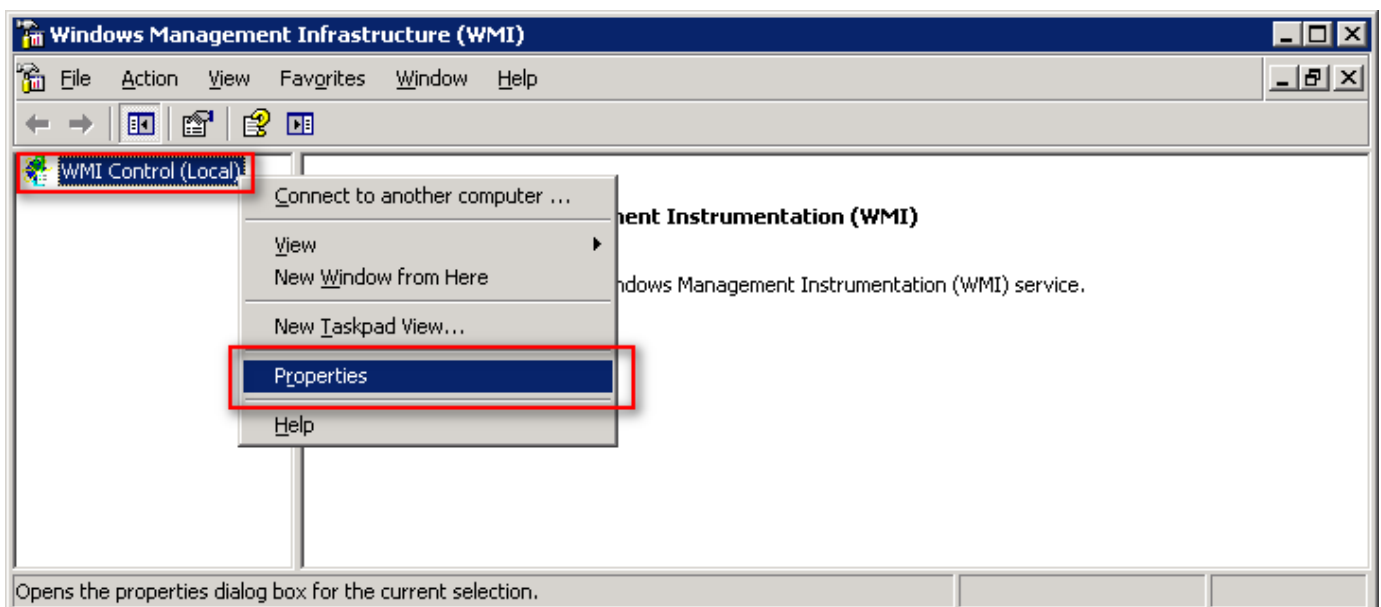
(2) Enter the command to enable WMI control service.

```
C:\> wimgmt.msc
```



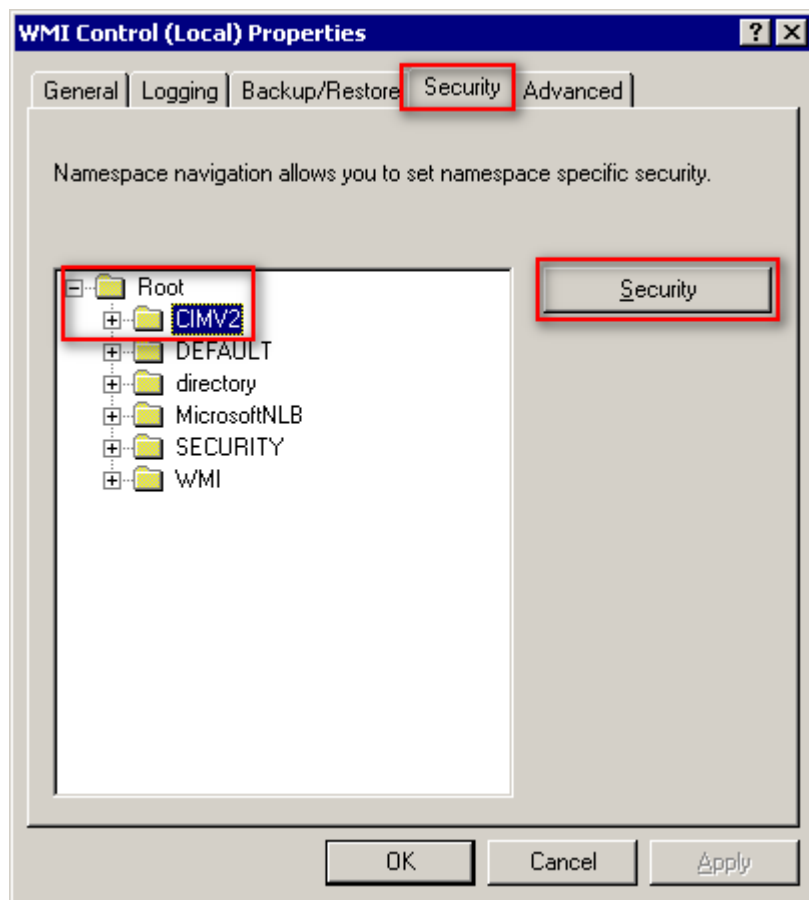
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



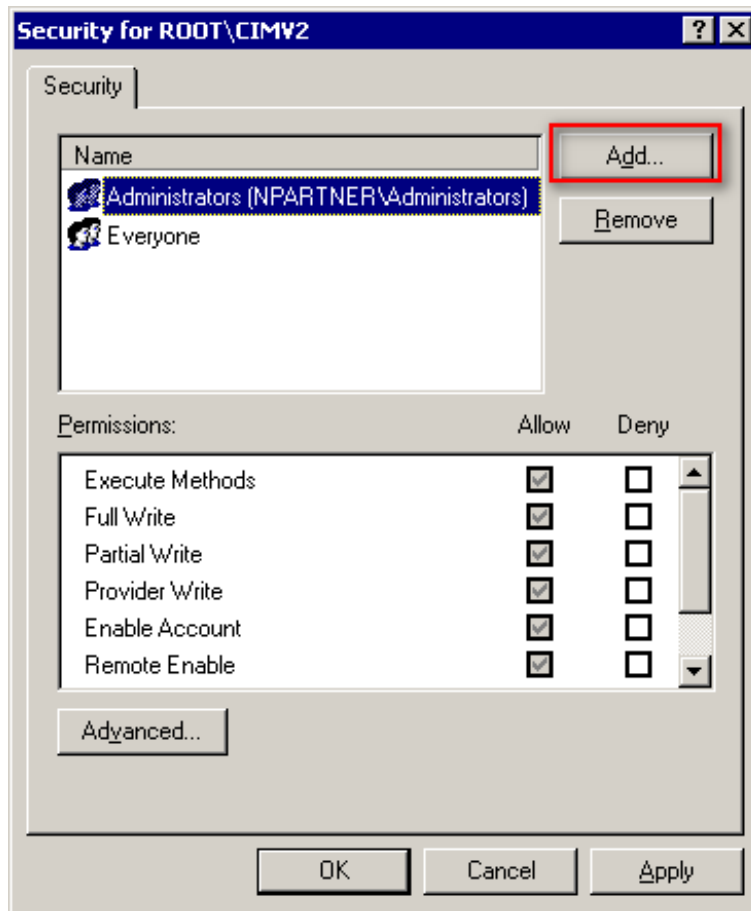
(4) Edit CIMV2 Security

On the "Security" tab, expand "Root -> CIMV2," then click "Security."



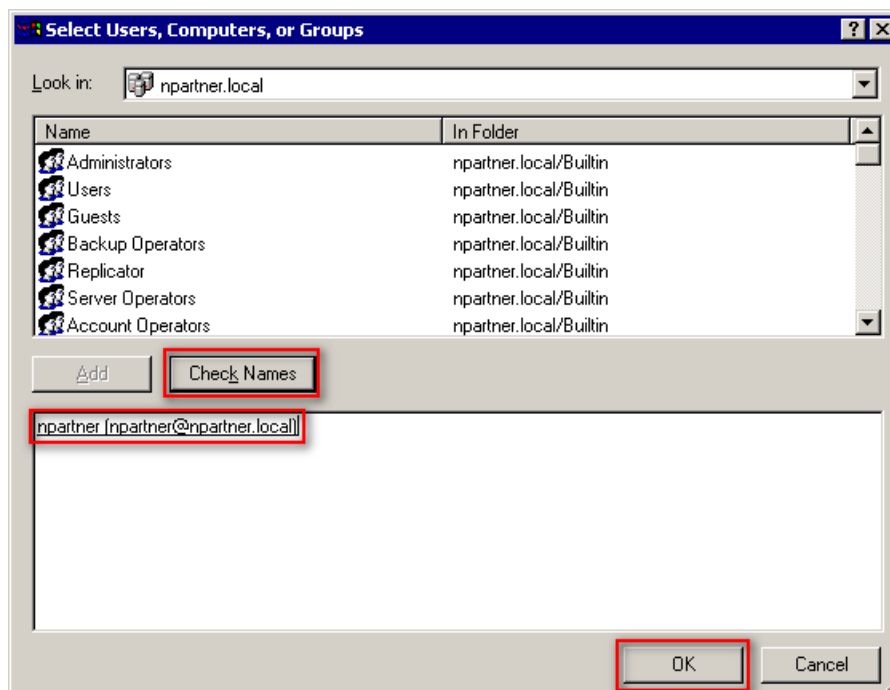
(5) Add WMI User Permissions.

Click "Add."



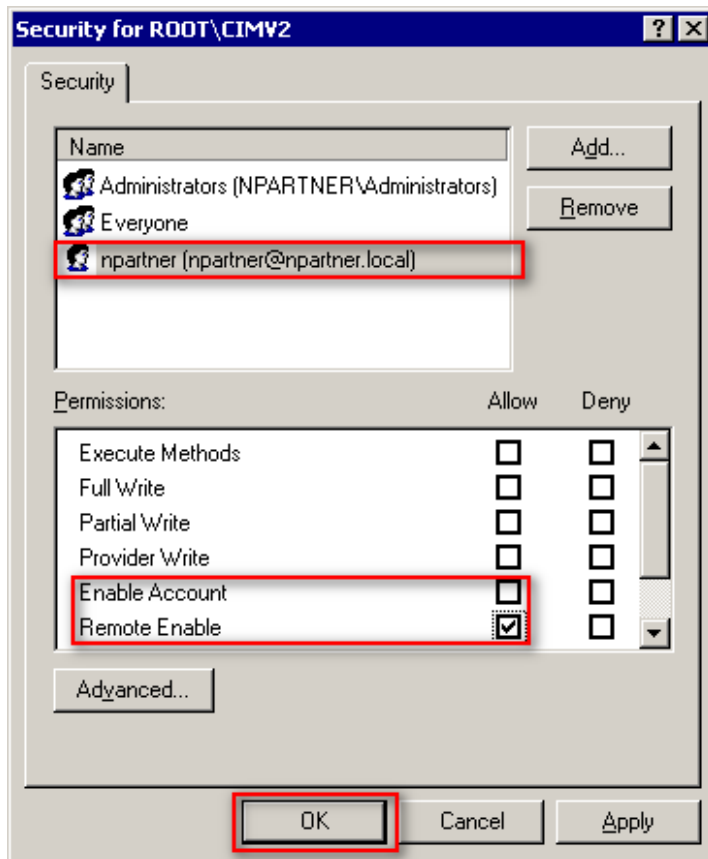
(6) Enter Your Username

Enter your username (in this example, it is "npartner") click "Check Names," then click "OK."

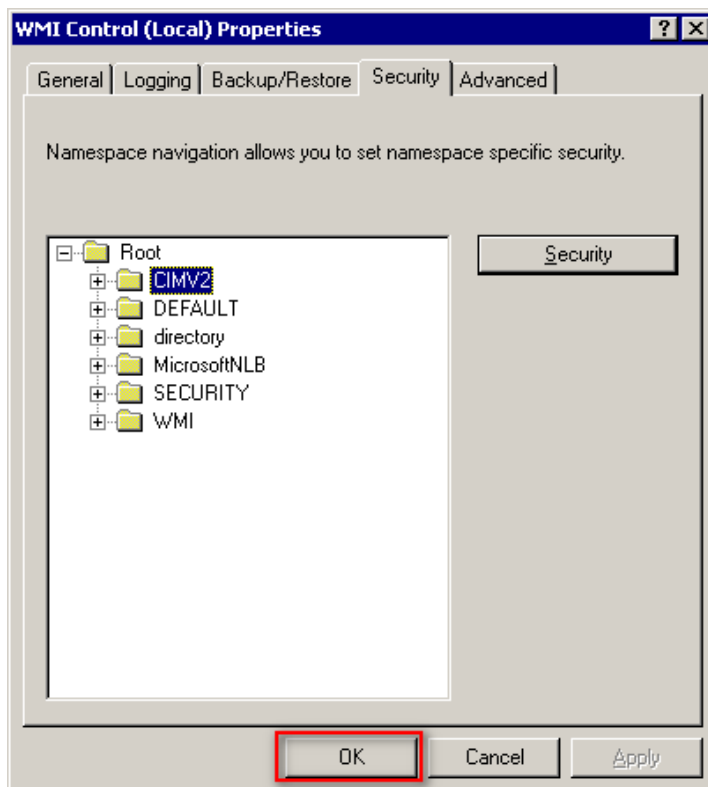


(7) Set Your User Permissions

Select your user account (in this example, it is “npartner.local”), uncheck “Enable Account,” check “Remote Enable,” then click “OK.”



(8) Click “OK.”



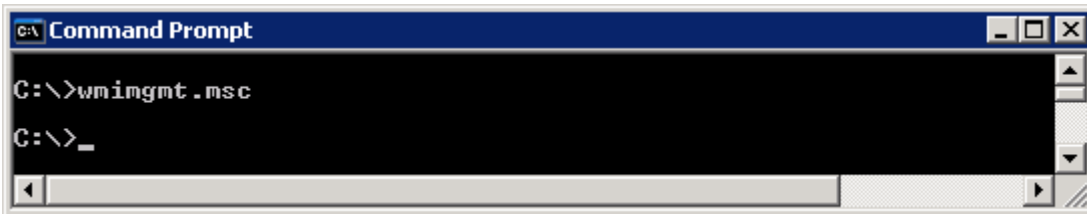
1.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”



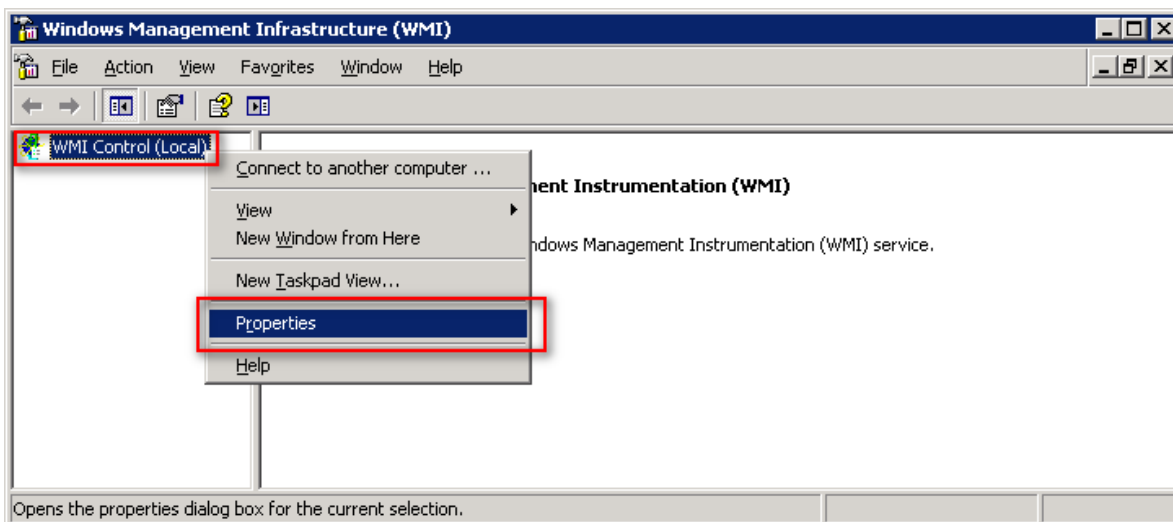
(2) Enter the command below to enable WMI Control.

```
C:\> wimgmt.msc
```



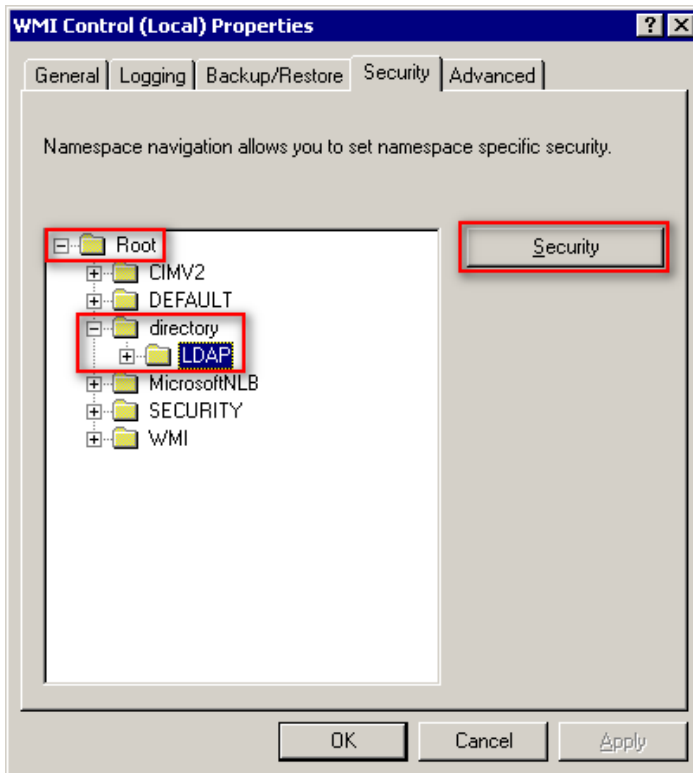
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



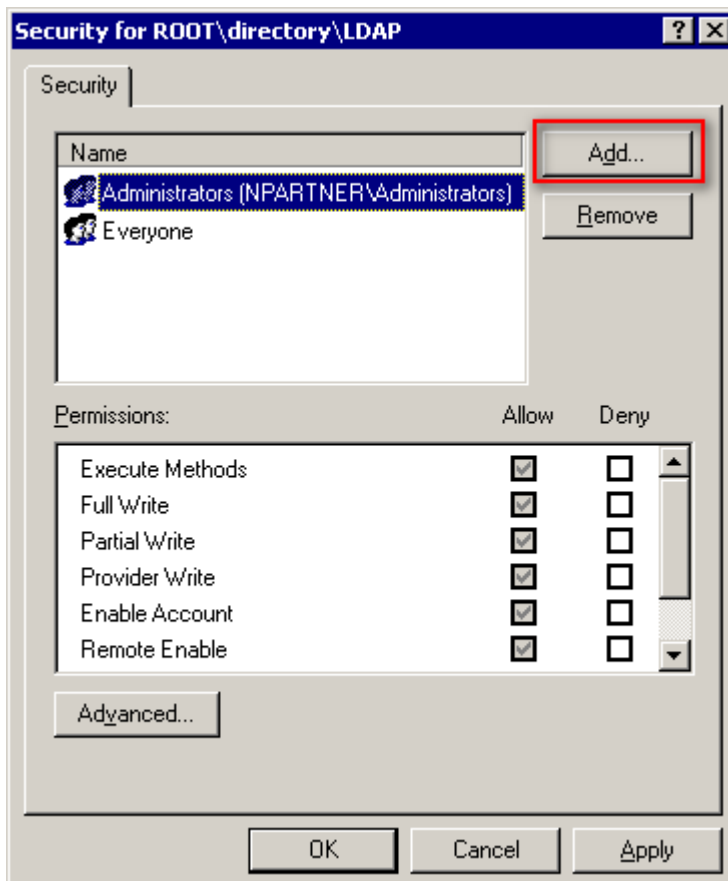
(4) Edit LDAP Security

On the "Security" tab, expand "Root"-> "directory" -> "LDAP," then click "Security."



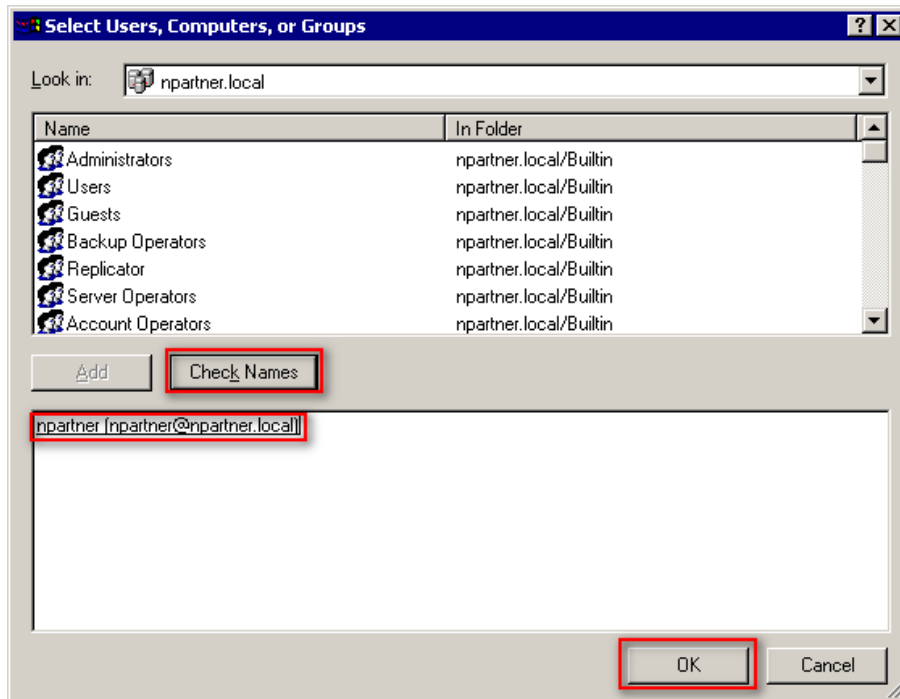
(5) Add WMI User Permissions

Click "Add."



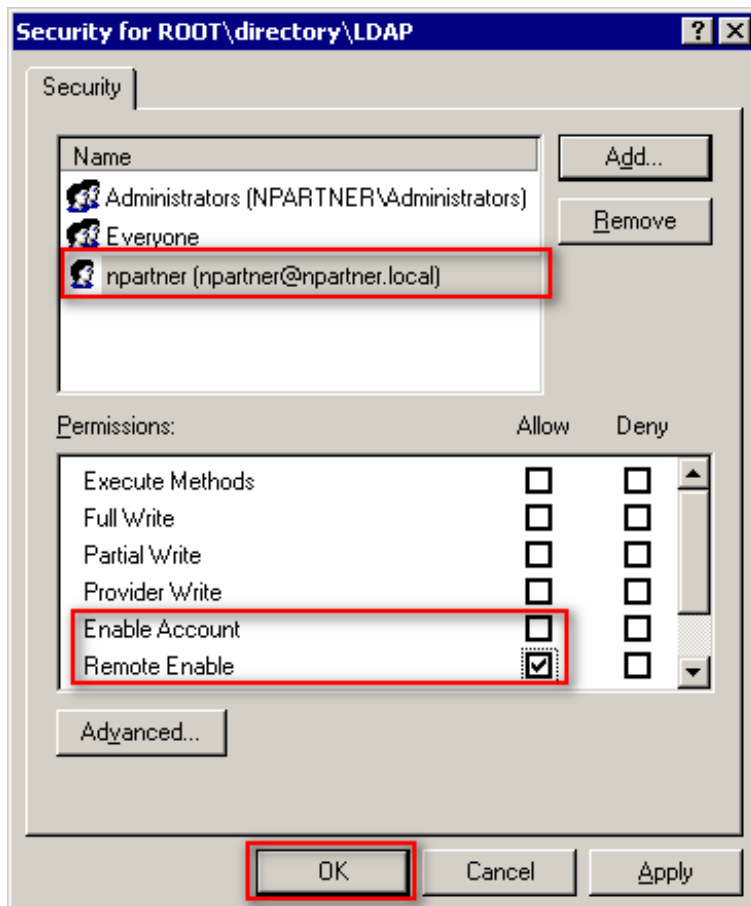
(6) Enter Your Username

Input your user account name (in this example, it is “npartner”), click “Check Names,” then click “OK.”

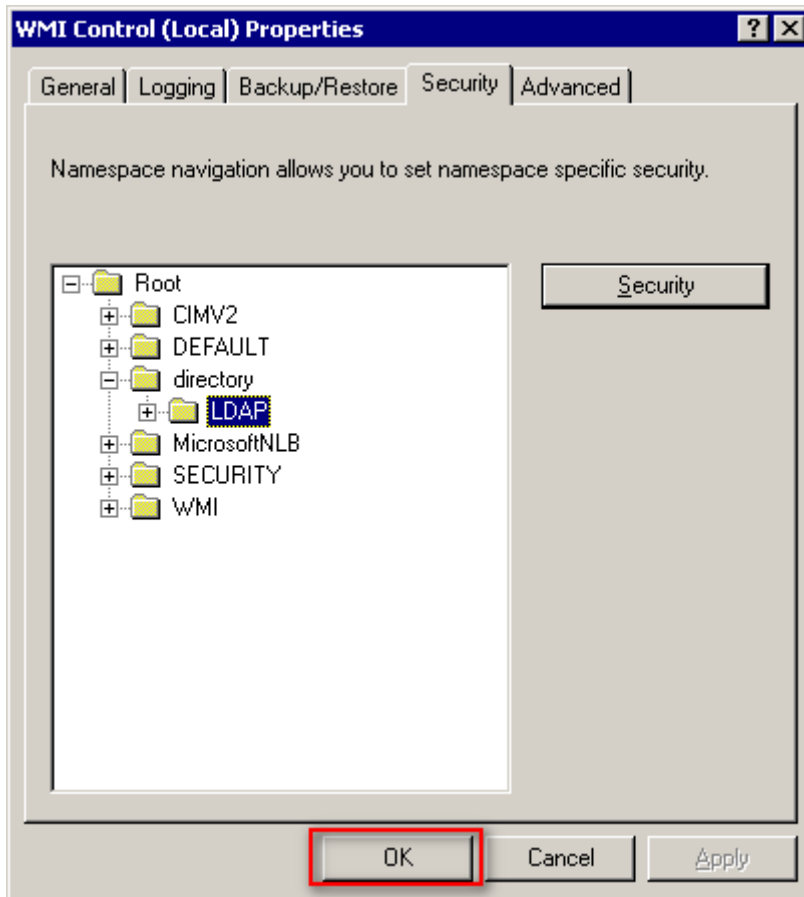


(7) Set Your User Permissions

Select your user account (in this example, it is “npartner”), **uncheck** “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Click "OK."

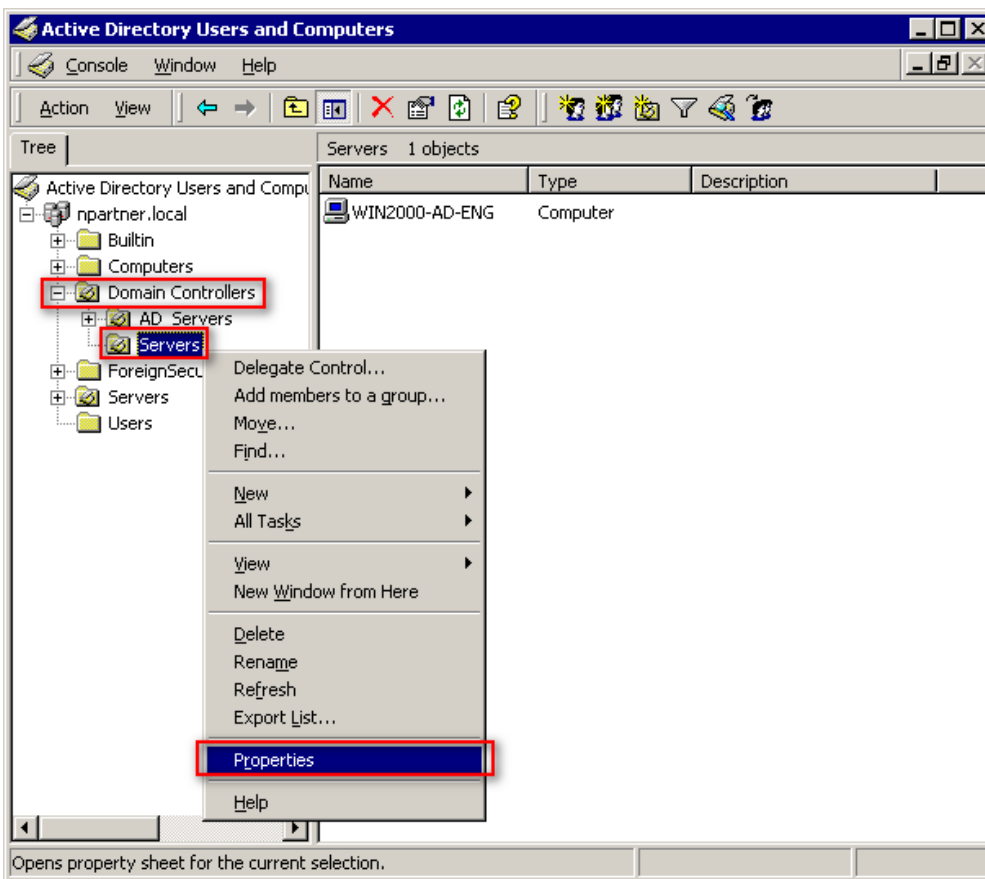


1.3.4 Configure Event Log Read Permissions

(1) Click “Active Directory Users and Computers.”

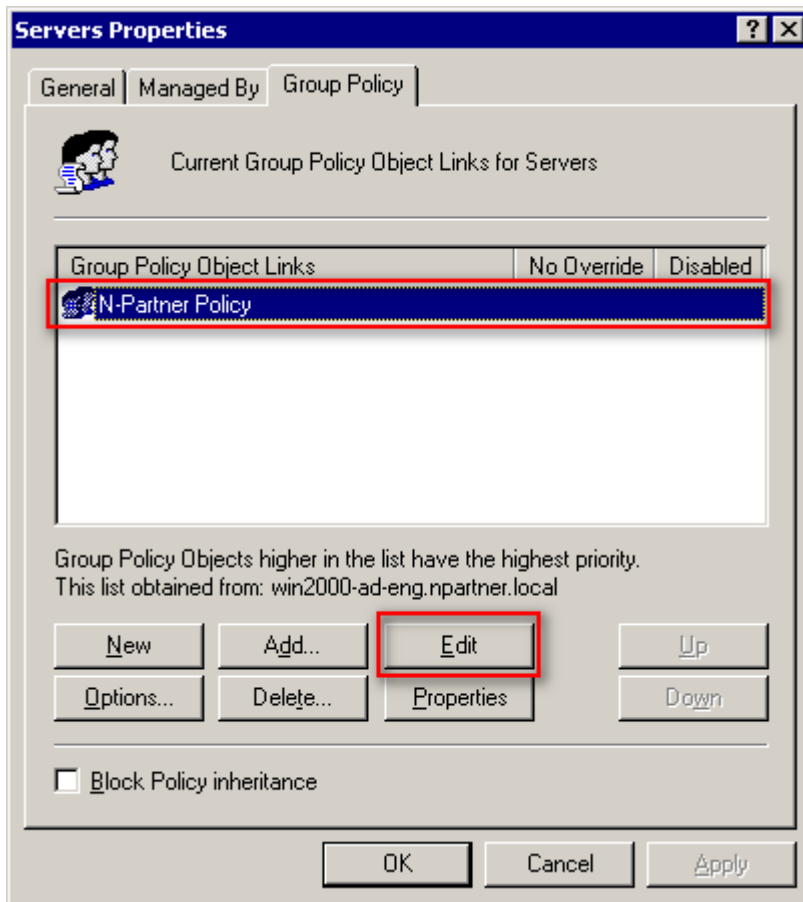


(2) In the “Servers” organizational unit of “Domain Controllers,” right-click on the “Domain Controllers” OU and select “Properties.”



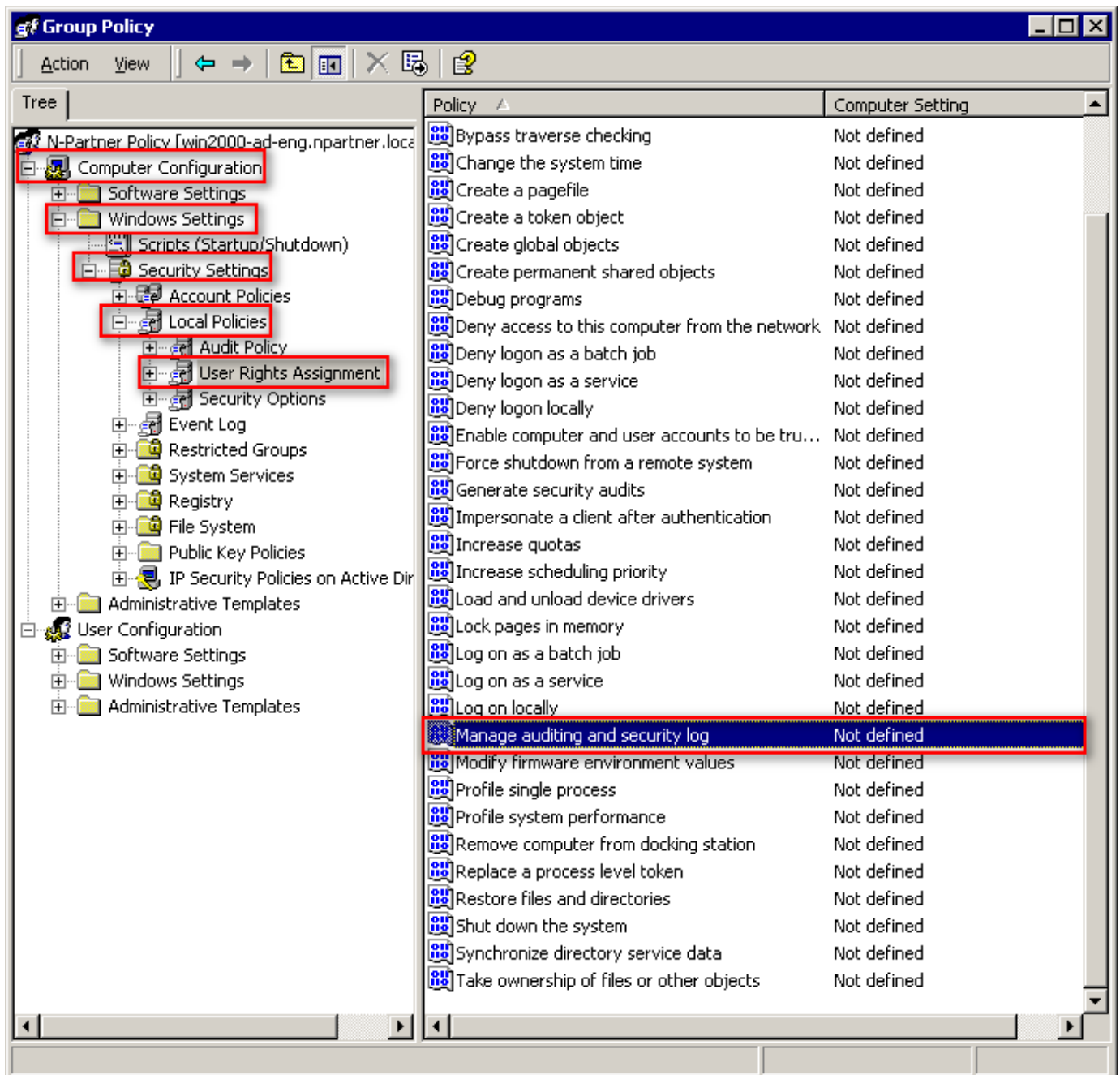
(3) Edit Group Policy Object

Select your Group Policy Object (in this example, it is “N-Partner Policy”), then click “Edit.”



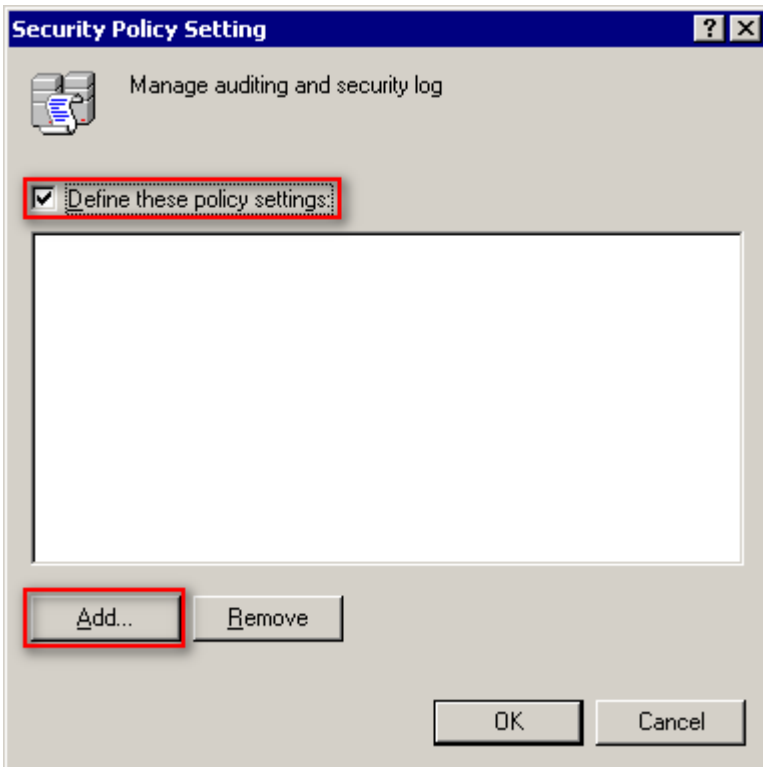
(4) Configure Audit Logs

Expand “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “User Rights Assignment,” then select “Manage Auditing and Security Log.”



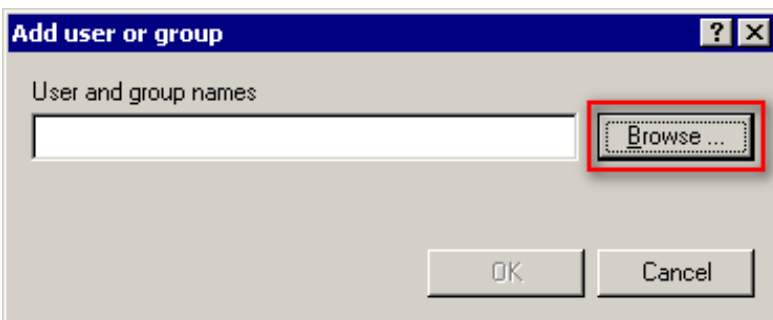
(5) Add Auditing User

Check “Define these policy settings,” then click “Add...”.



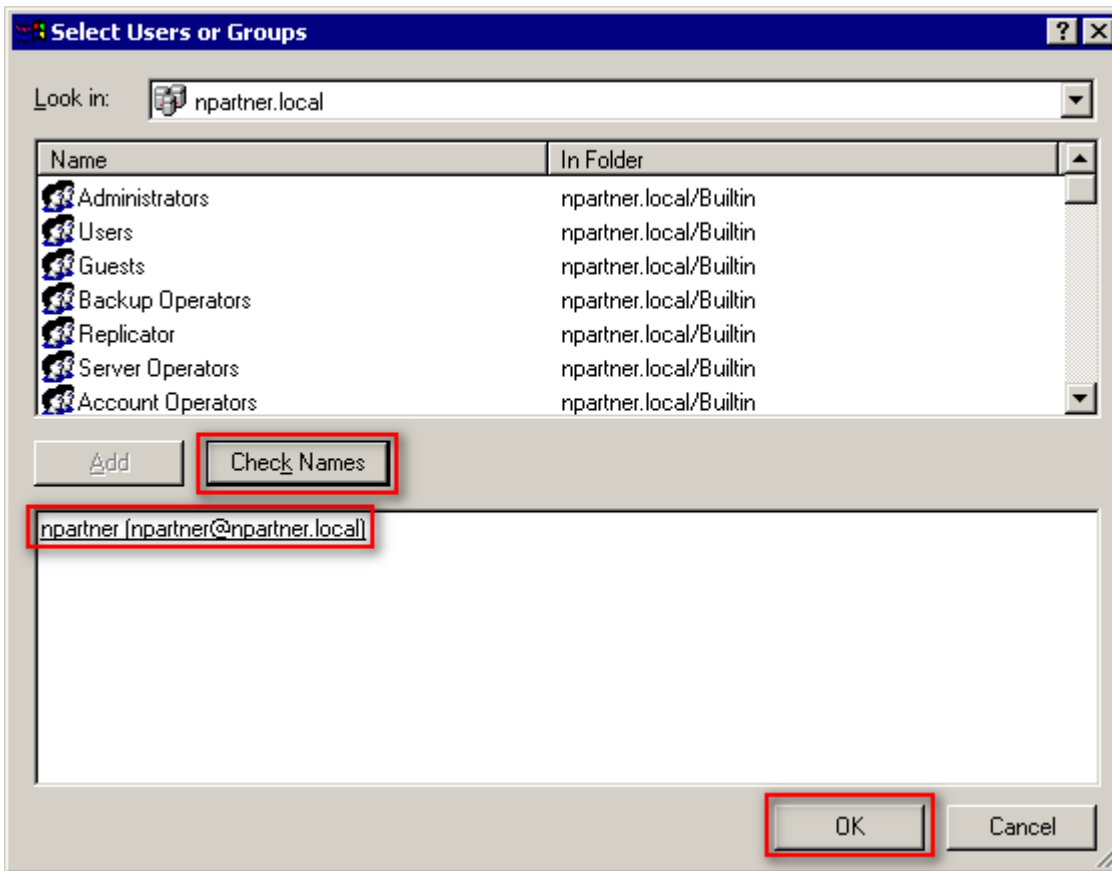
(6) Search for User

Click “Browse.”

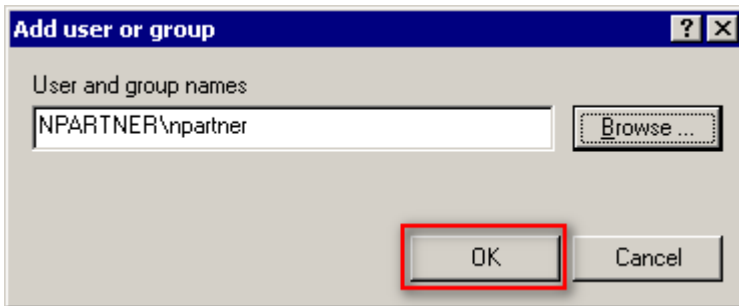


(7) Enter Your User Account

Input your user account (in this example, it is “N-Partner”), click “Check Names,” then click “OK.”

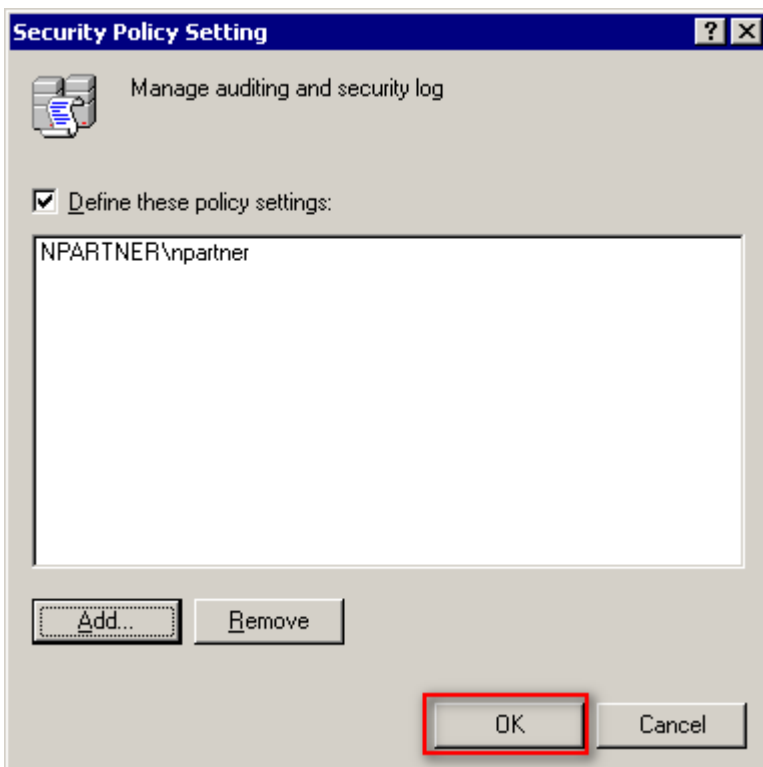


(8) Click "OK."



(9) Confirm Audit Log Settings

Click "OK."

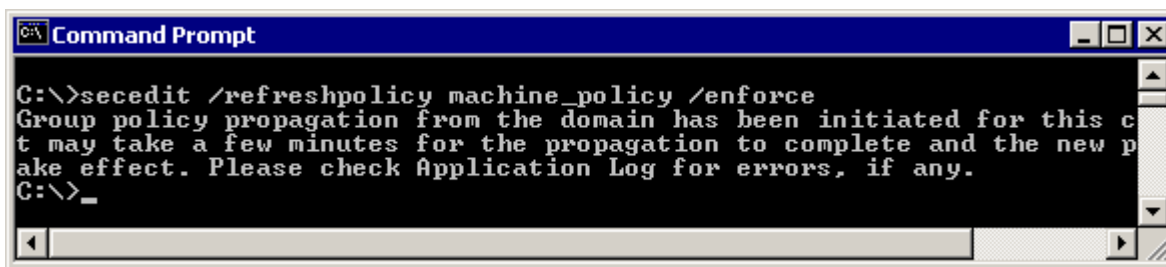


(10) Open "Command Prompt."



(11) Enter the command below to update group policy.

```
C:\> secedit /refreshpolicy machine_policy /enforce
```



```
Command Prompt
C:\>secedit /refreshpolicy machine_policy /enforce
Group policy propagation from the domain has been initiated for this computer. It may take a few minutes for the propagation to complete and the new policies will take effect. Please check Application Log for errors, if any.
C:\>_
```

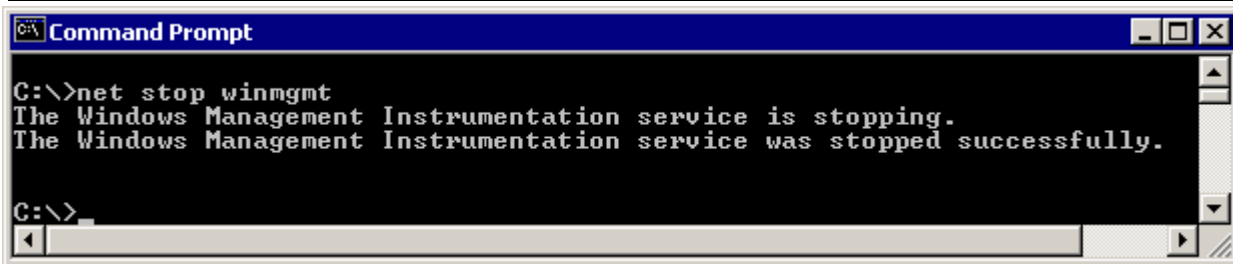
1.3.5 Restart the WMI Service

(1) Open "Command Prompt."



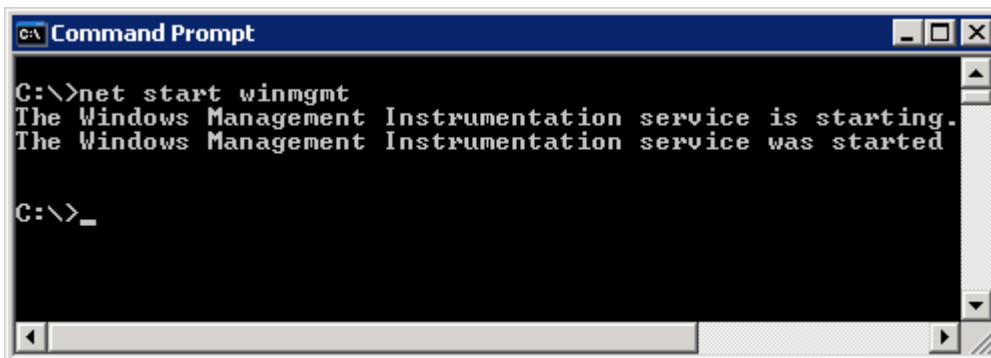
(2) Enter the command below to disable the WMI service.

```
C:\> net stop winmgmt
```



(3) Enter the command below to enable the WMI service.

```
C:\> net start winmgmt
```



2. Windows 2003

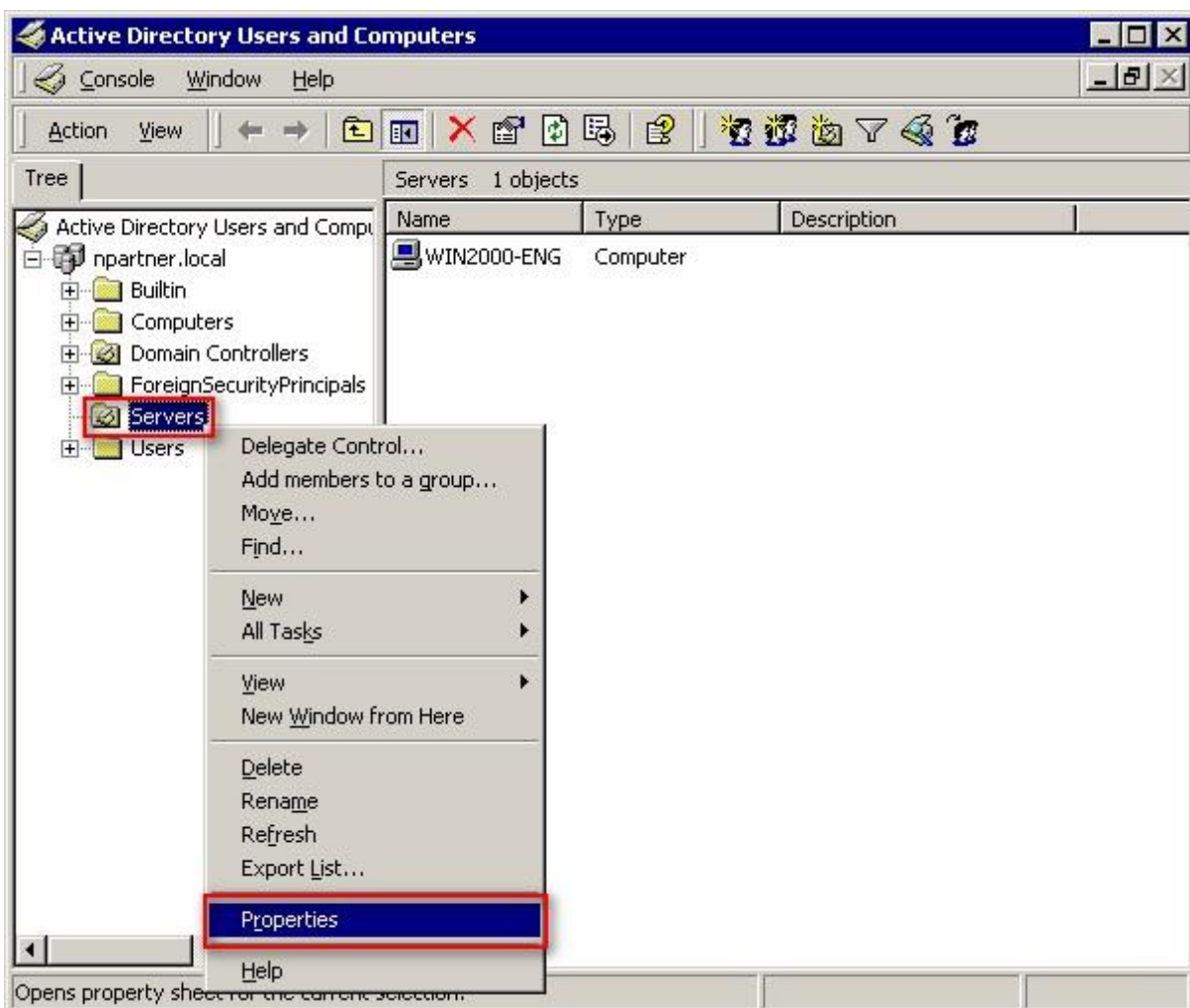
For detailed information on setting Windows audit policies, please refer to the “audit policy recommendations link” in the preface.

2.1 Organizational Unit Settings

(1) Open “Active Directory Users and Computers.”



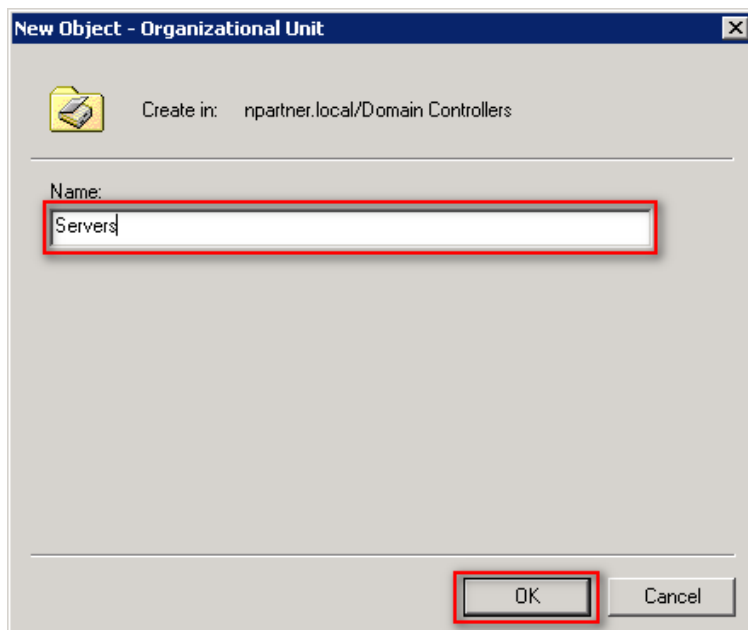
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Properties.”



(3) Name Your Group Policy Object

Enter your group policy object name (the example here is “N-Partner Policy”)

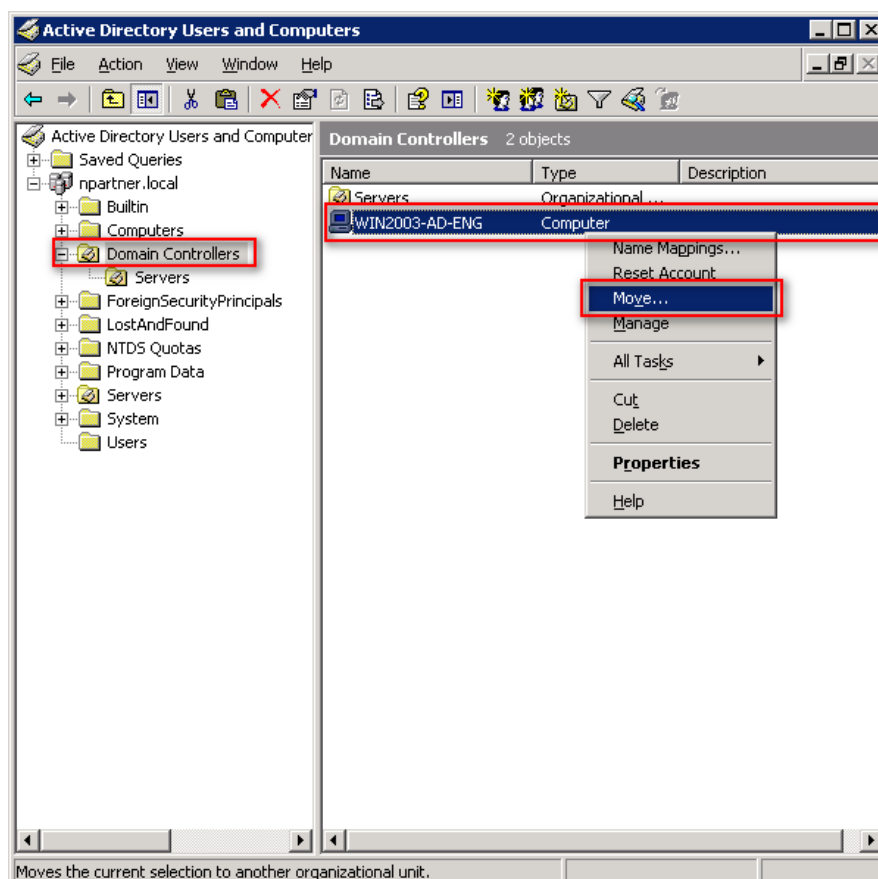
Note: Please create your group object name based on the actual environment -> Click “Edit.”



(4) Move Server to your New Organizational Unit

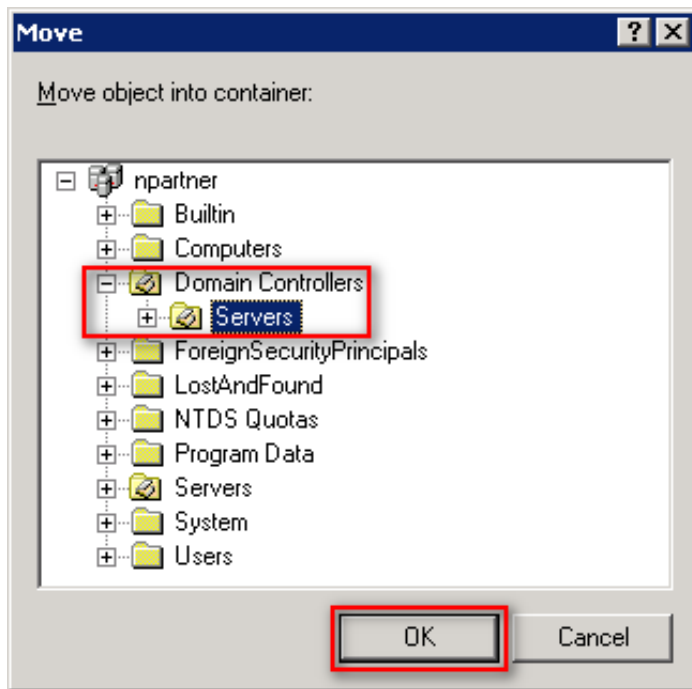
Select the “Domain Controllers” organizational unit, right-click on the “WIN2003-AD-ENG” server

(Note: select the Windows AD host according to the actual environment) and click “Move.”



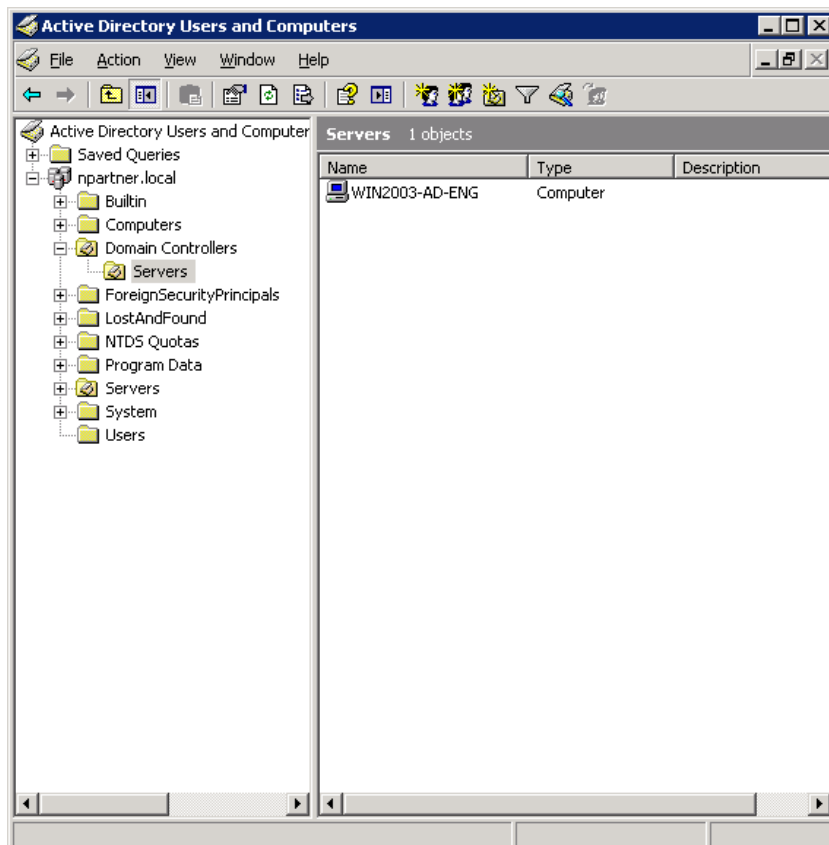
(5) Select Organizational Unit

Choose the “Servers” organizational unit under “Domain Controllers,” then click “OK.”



(6) Confirm Server Has Moved to your New Organizational Unit

Expand the “Servers” organizational unit under “Domain Controllers” and verify that the “WIN2003-AD-ENG” server has been moved.

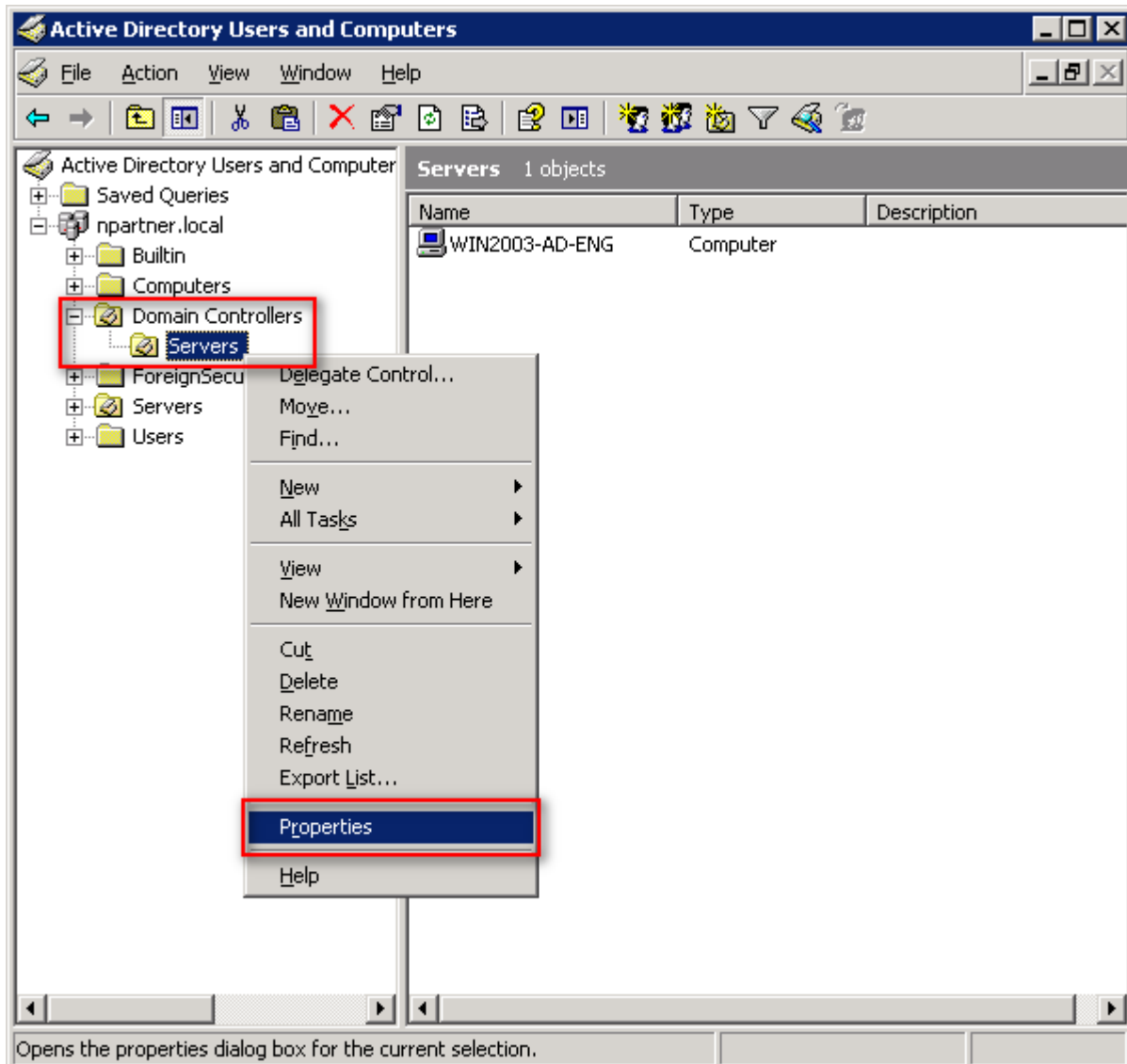


2.2 Group Policy Settings

(1) Open “Active Directory Users and Computers.”

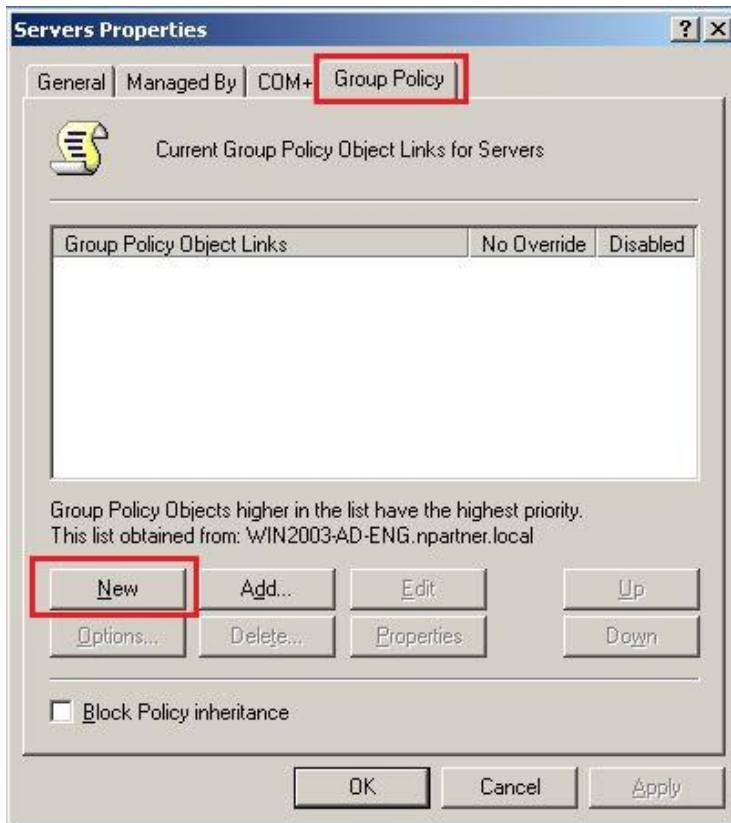


(2) Select the “Servers” organizational unit under “Domain Controllers,” right-click, and choose “Properties.”



(3) Enter your Group Policy Object Name

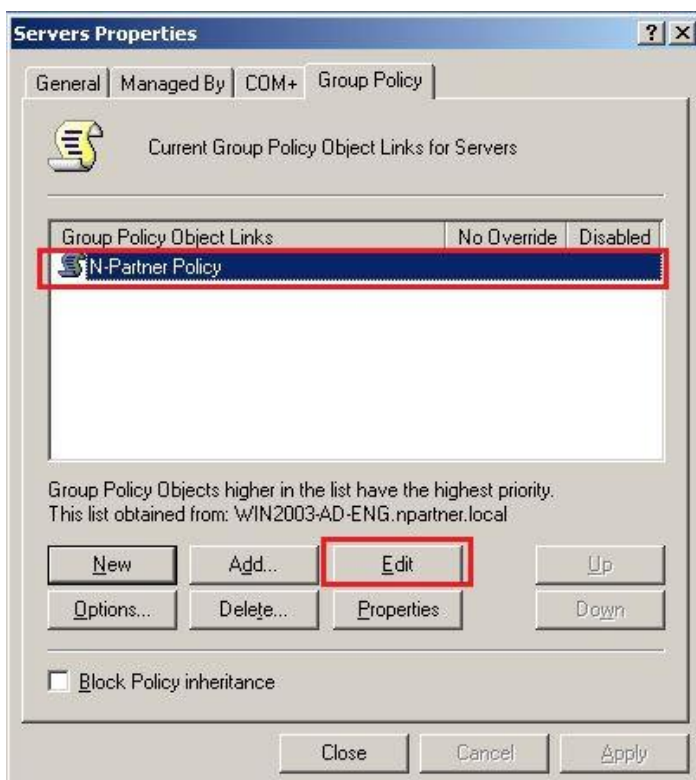
Go to the “Group Policy” tab and click “New.”



(4) Edit your Group Policy Object

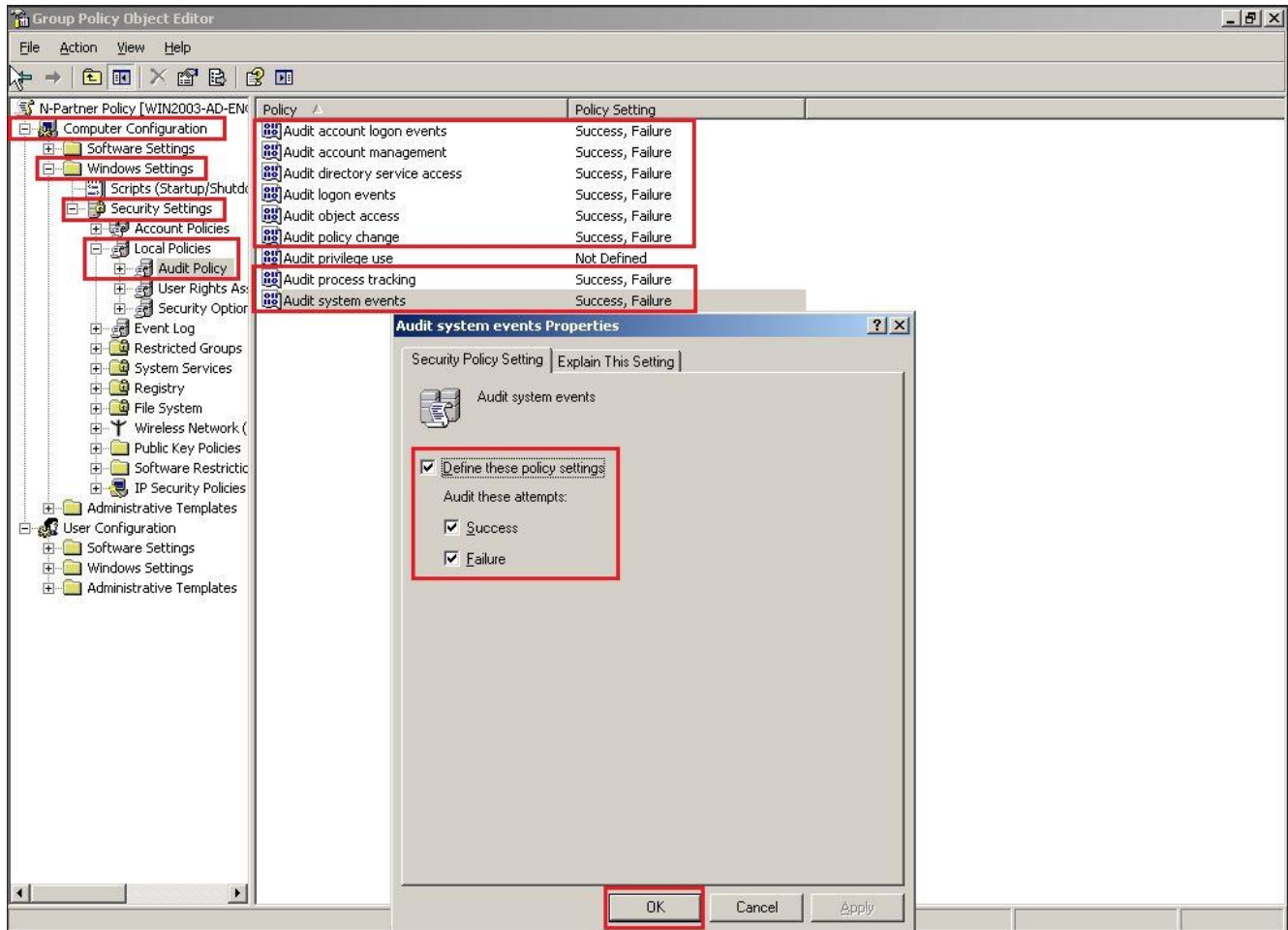
Enter the Group Policy Object name as “N-Partner Policy”

(Note: create the GPO name according to the client's environment), then click “Edit.”



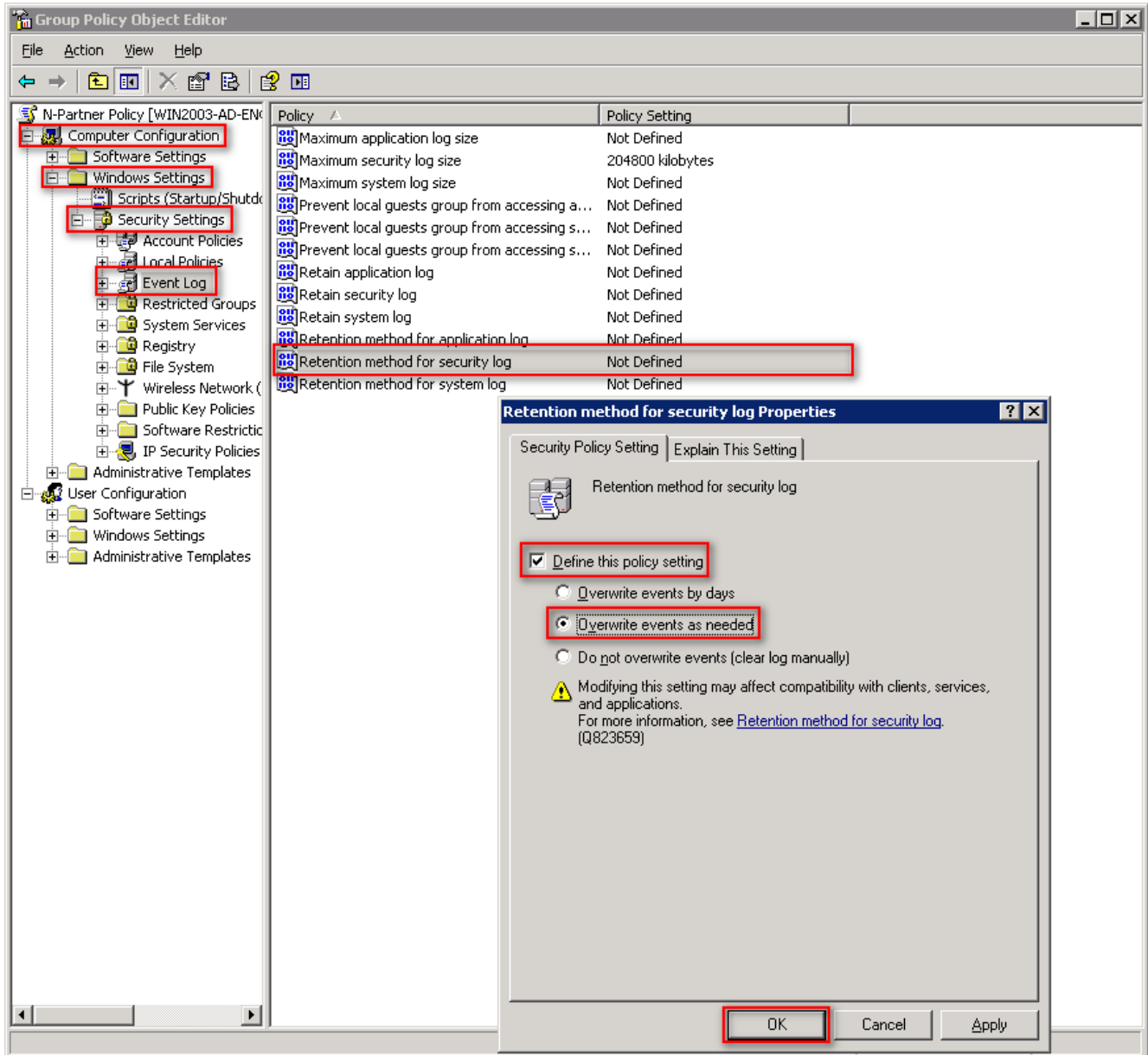
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logging: Security Log Retention Method

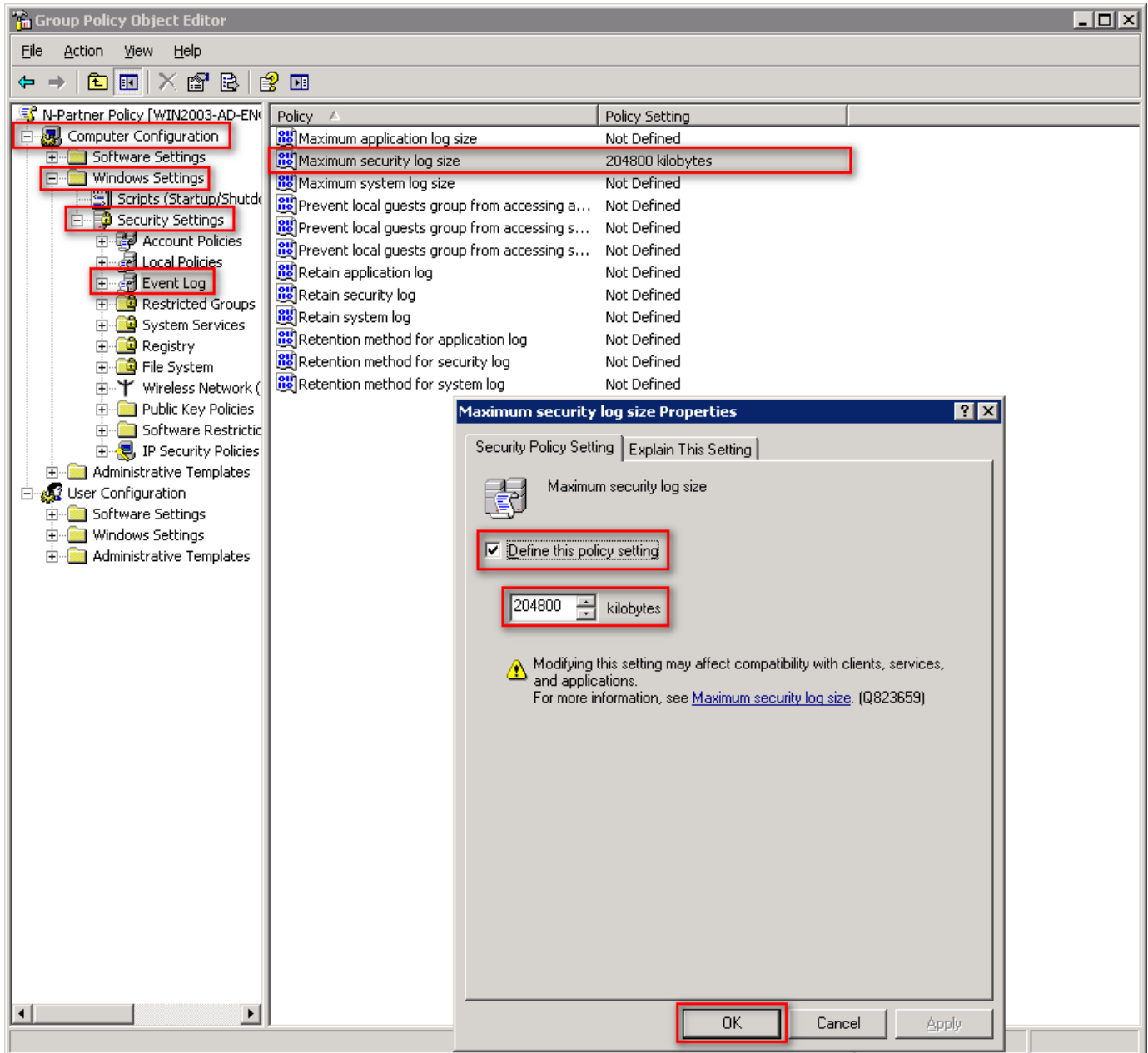
Expand “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log”, then select the “Retention Method for security method” item. Check “Define this policy setting,” select “Overwrite events as needed”, and click “OK.”



(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs” -> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment -> Click “OK.”

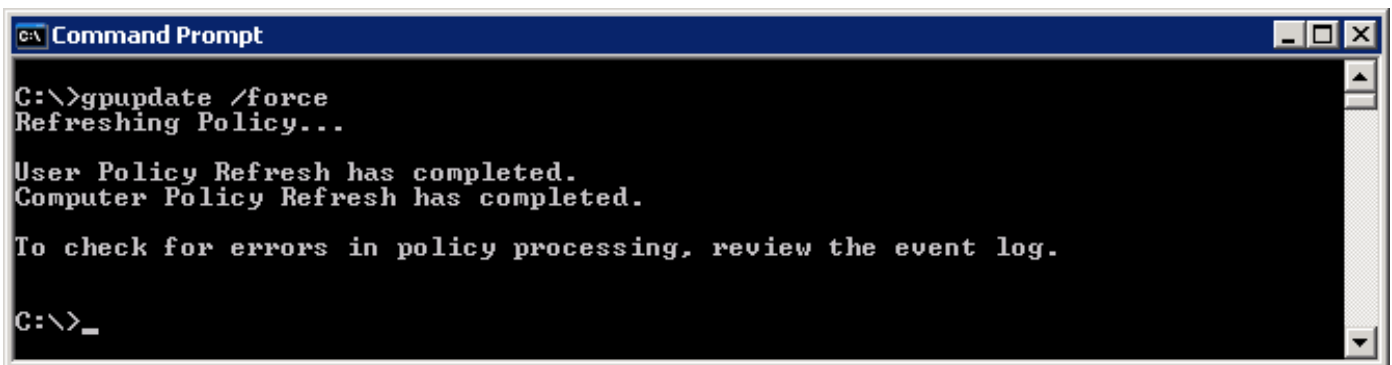


(8) Open "Command Prompt" on your Windows Server.



(9) Enter the command below to refresh group policy.

```
C:\> gpupdate /force
```



```
c:\ Command Prompt
C:\>gpupdate /force
Refreshing Policy...

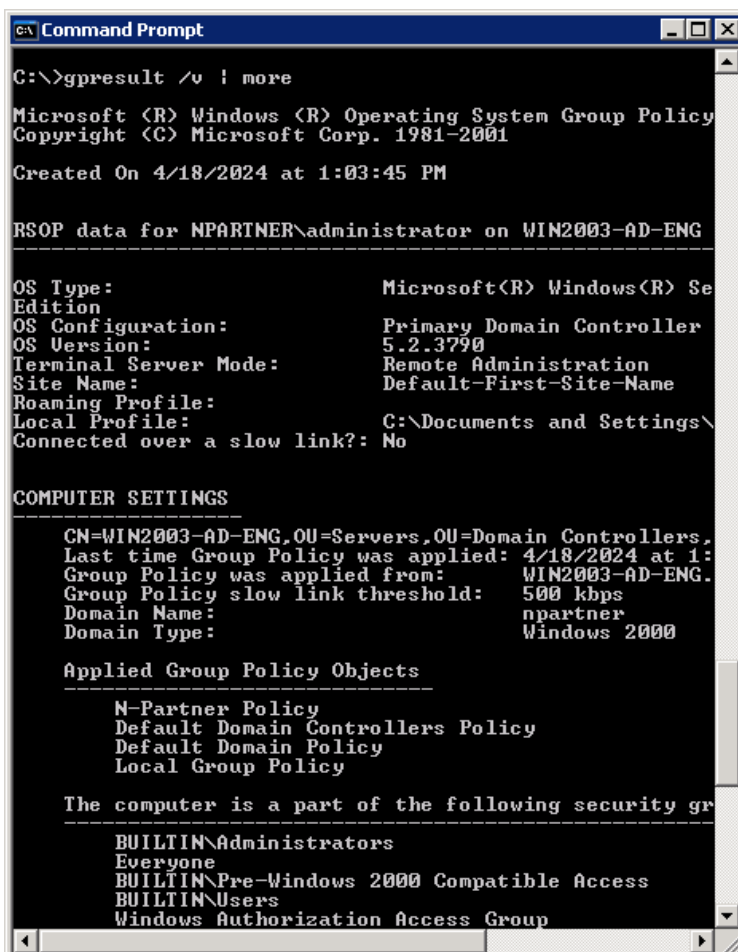
User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.

C:\>_
```

(10) Enter the command below to view the group policy application status.

```
C:\> gpresult /v
```



```
c:\ Command Prompt
C:\>gpresult /v | more
Microsoft (R) Windows (R) Operating System Group Policy
Copyright (C) Microsoft Corp. 1981-2001

Created On 4/18/2024 at 1:03:45 PM

RSOP data for NPARTNER\administrator on WIN2003-AD-ENG
-----
OS Type: Microsoft(R) Windows(R) Se
Edition
OS Configuration: Primary Domain Controller
OS Version: 5.2.3790
Terminal Server Mode: Remote Administration
Site Name: Default-First-Site-Name
Roaming Profile:
Local Profile: C:\Documents and Settings\
Connected over a slow link?: No

COMPUTER SETTINGS
-----
CN=WIN2003-AD-ENG,OU=Servers,OU=Domain Controllers,
Last time Group Policy was applied: 4/18/2024 at 1:
Group Policy was applied from: WIN2003-AD-ENG.
Group Policy slow link threshold: 500 kbps
Domain Name: npartner
Domain Type: Windows 2000

Applied Group Policy Objects
-----
N-Partner Policy
Default Domain Controllers Policy
Default Domain Policy
Local Group Policy

The computer is a part of the following security gr
-----
BUILTIN\Administrators
Everyone
BUILTIN\Pre-Windows 2000 Compatible Access
BUILTIN\Users
Windows Authorization Access Group
```

2.3 Add a Non-Admin Account

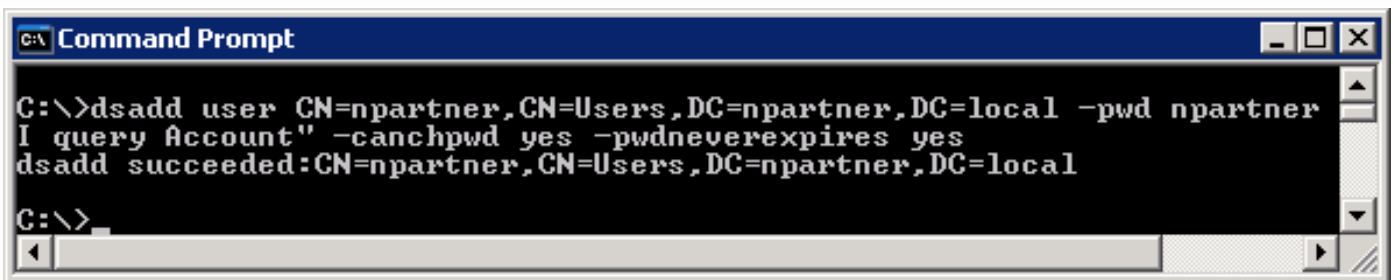
2.3.1 Add Users

(1) Open "Active Directory Users and Computers."



(2) Enter the command below to add a new account.

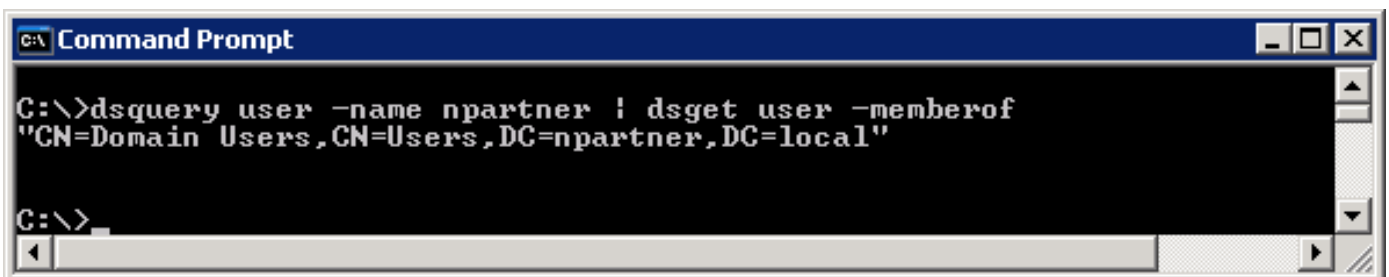
```
C:\> dsadd user CN=npartner,OU=Accounts,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command entered is: `C:\> dsadd user CN=npartner,CN=Users,DC=npartner,DC=local -pwd npartner I query Account" -canchpwd yes -pwdneverexpires yes`. The output is: `dsadd succeeded:CN=npartner,CN=Users,DC=npartner,DC=local`. The prompt is now `C:\>`.

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
C:\> dsquery user -name npartner | dsget user -memberof
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command entered is: `C:\> dsquery user -name npartner | dsget user -memberof`. The output is: `"CN=Domain Users,CN=Users,DC=npartner,DC=local"`. The prompt is now `C:\>`.

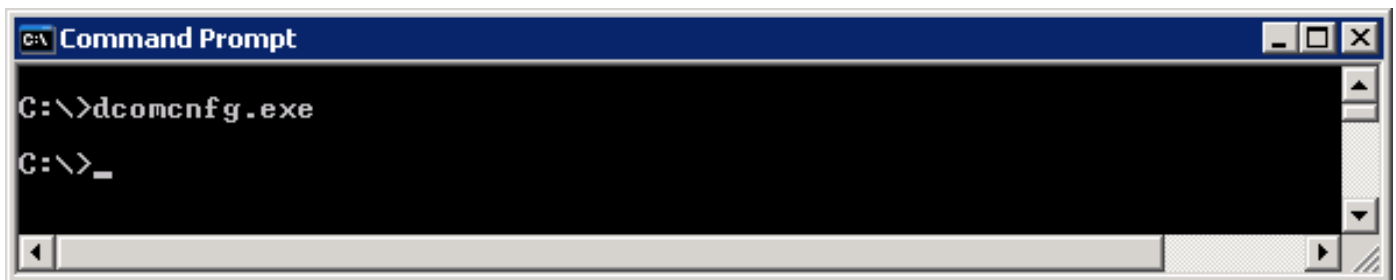
2.3.2 Configure DCOM Permissions

(1) Open "Command Prompt."



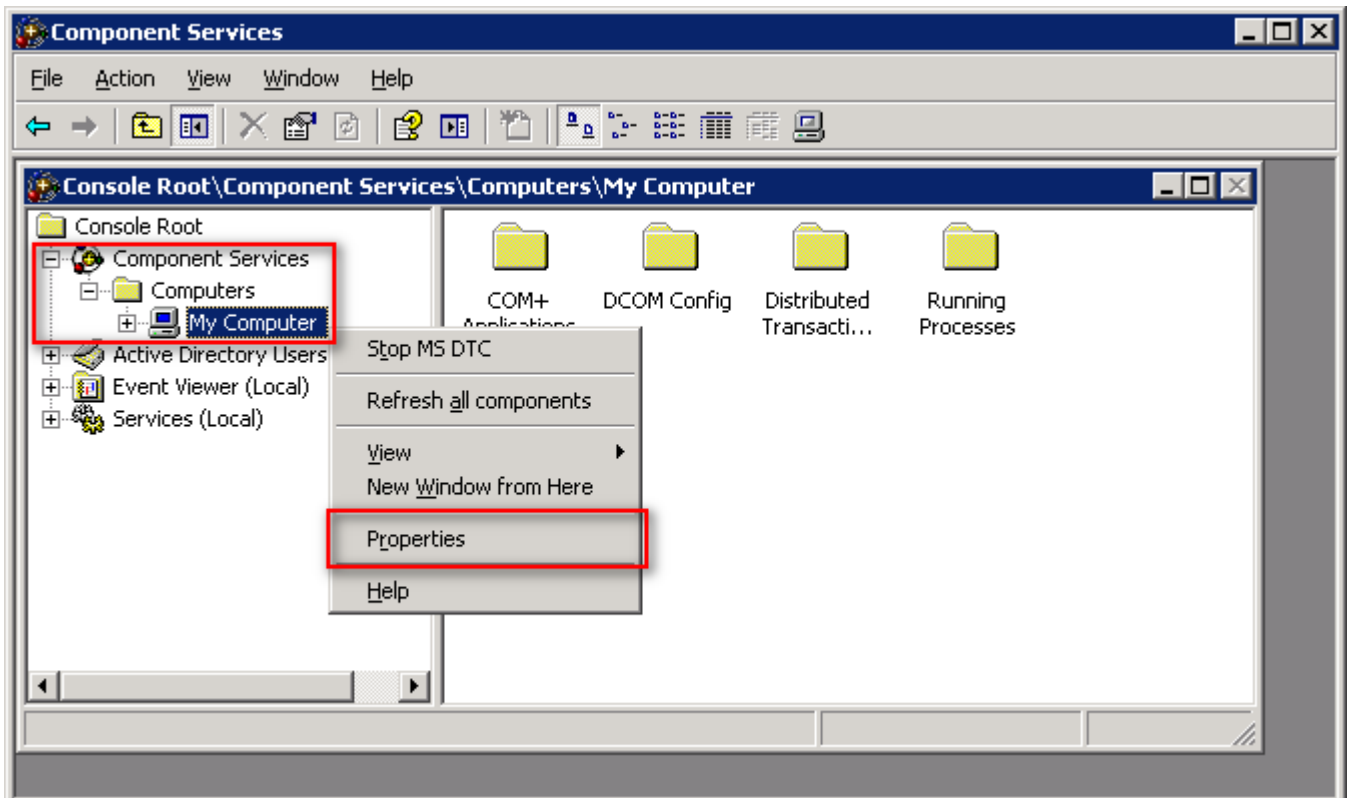
(2) Enter the command below to open component services.

```
C:\> dcomcnfg.exe
```



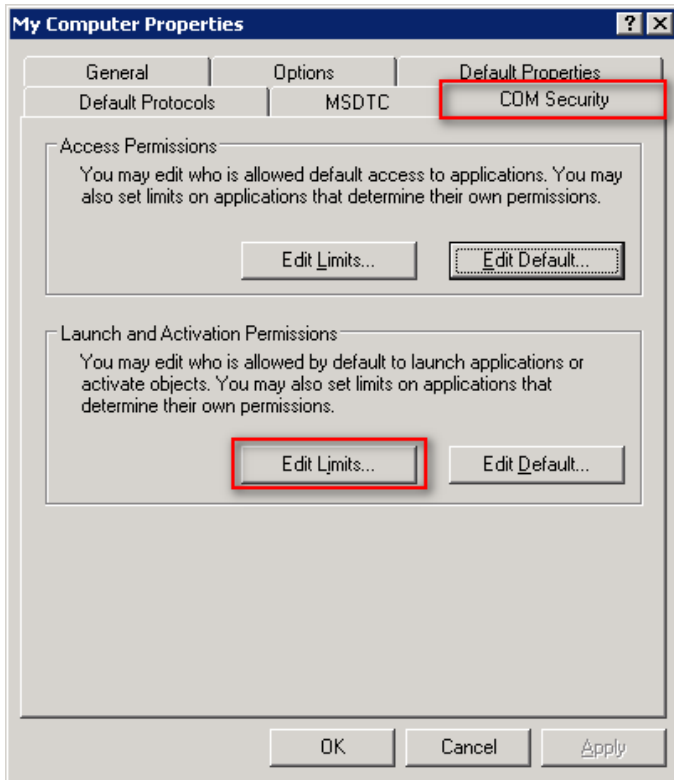
(3) Edit Computer Properties

Expand folder "Console Root" -> "Component Services" -> "Computers," right-click on "My Computer," and select "Properties."



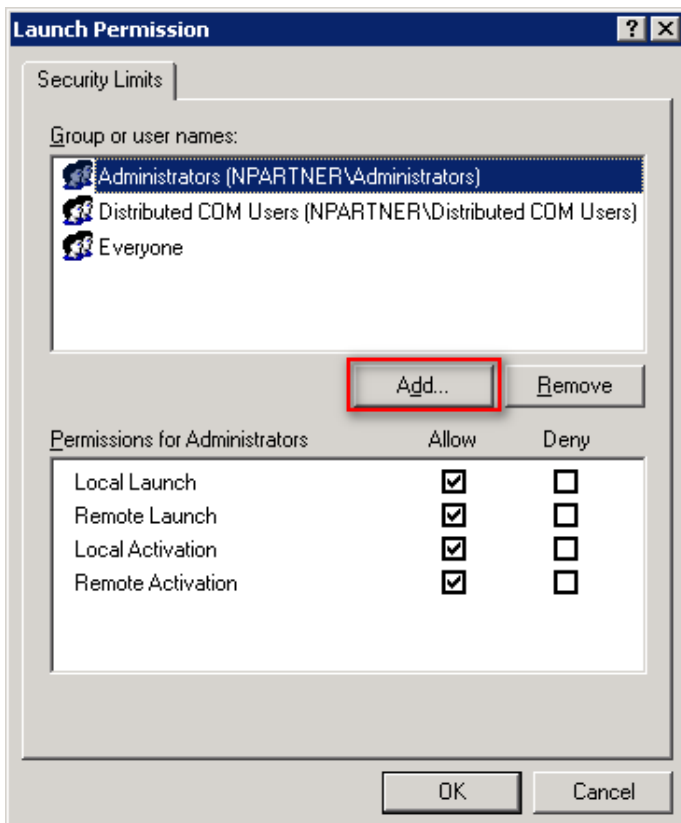
(4) Enable Permissions

Go to the “COM Security” tab, under Launch and Activation Permissions, click “Edit Limits.”



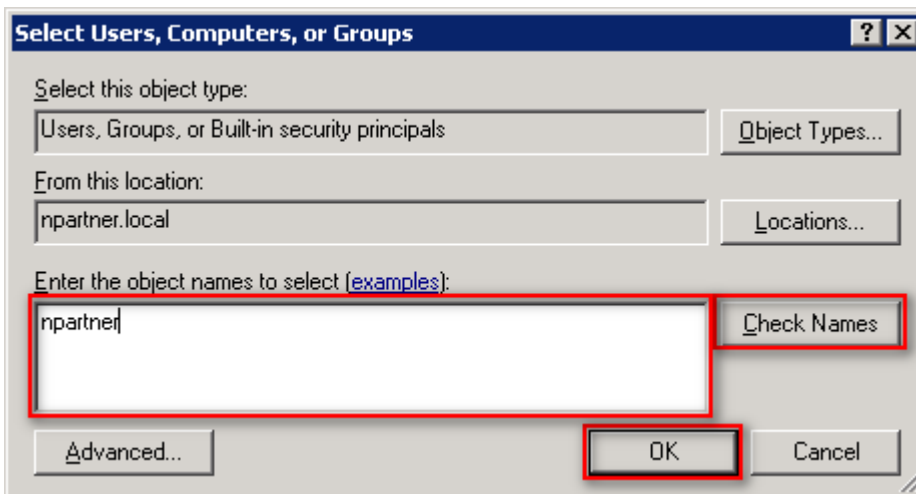
(5) Add DCOM User Permissions

Click “Add.”



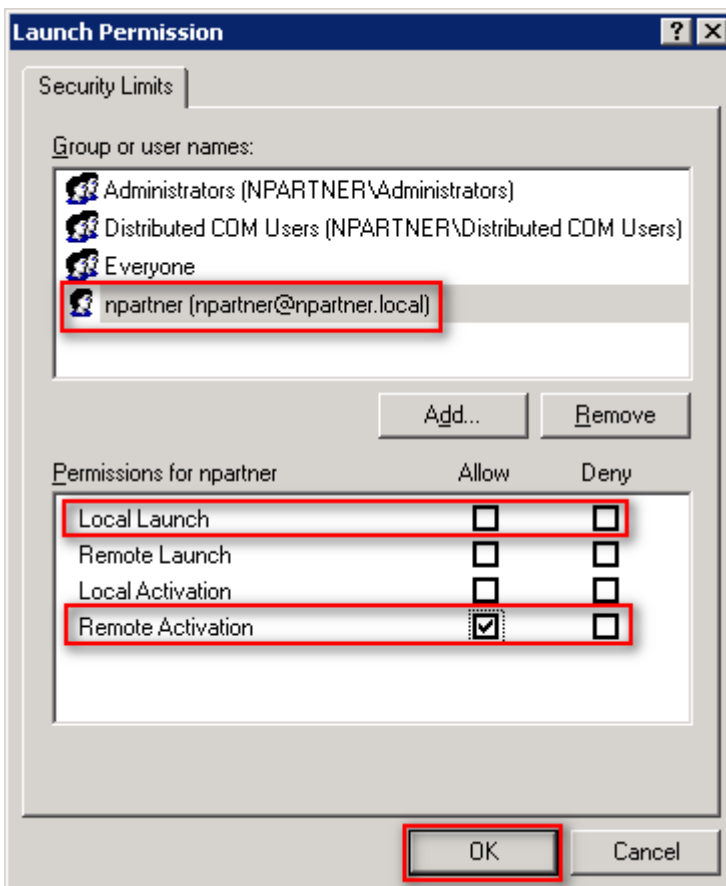
(6) Enter your Username

Input your user account: [npartner](#), click “Check Names,” then click “OK.”

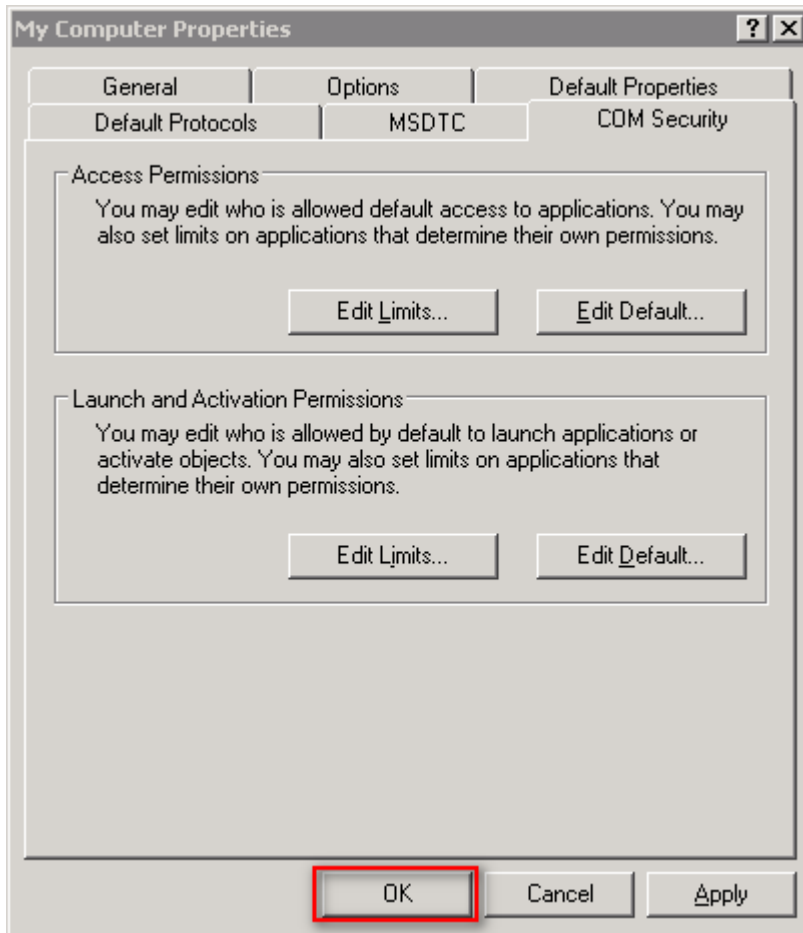


(7) Set User Permissions

Select the user account: [npartner](#), uncheck “Local Launch: Allow,” check “Remote Activation: Allow,” then click “OK.”



(8) Click "OK."



2.3.3 Configure WMI Permissions

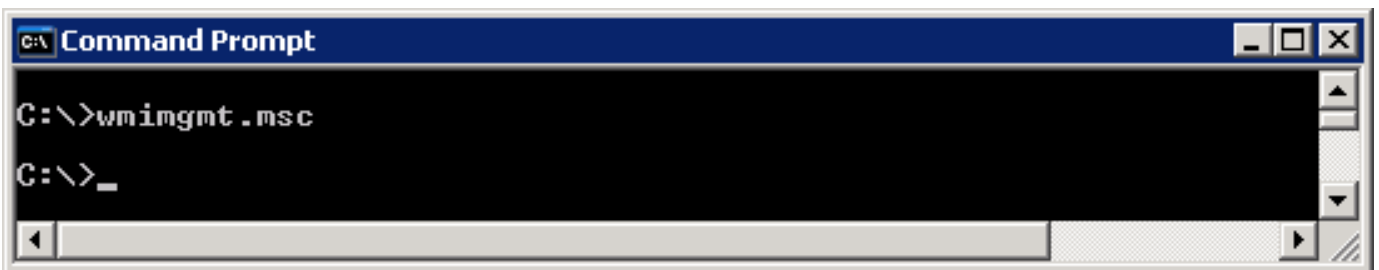
2.3.3.1 Set Event Log Permissions

(1) Open "Command Prompt."



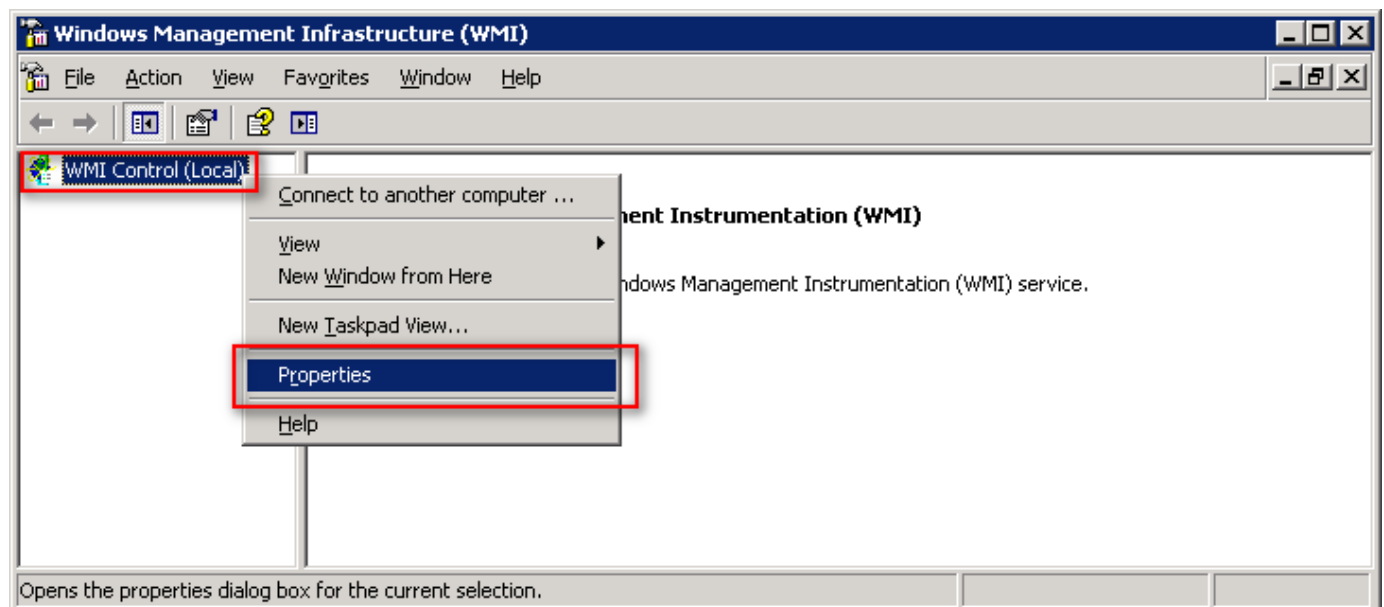
(2) Enter the command below to enable component services.

```
C:\> wimgmt.msc
```



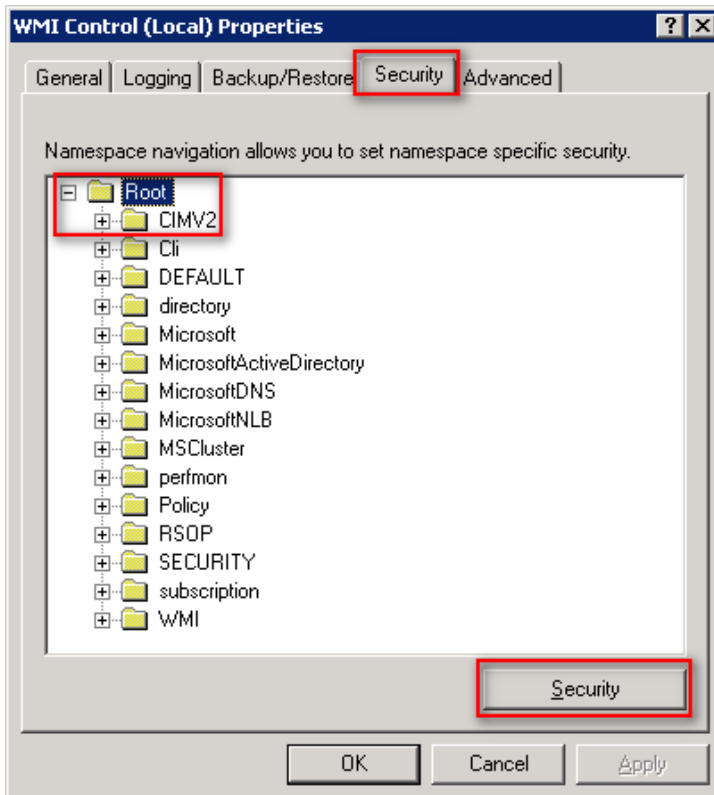
(3) Edit WMI Control

In "WMI Control (Local)," right-click and select "Properties."



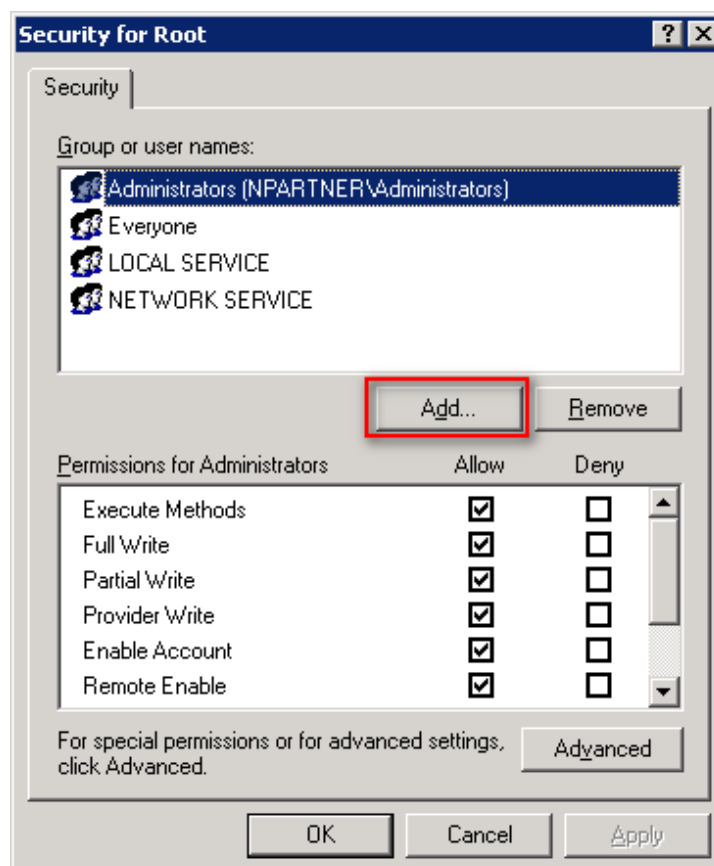
(4) Edit CIMV2 Security

On the "Security" tab, expand folder "Root" -> "CIMV2," then click "Security."



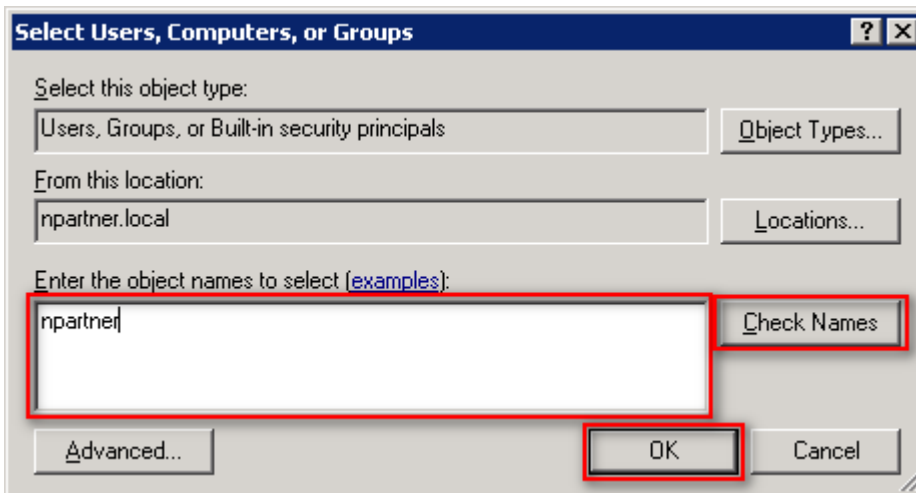
(5) Add WMI User Permissions

Click "Add."



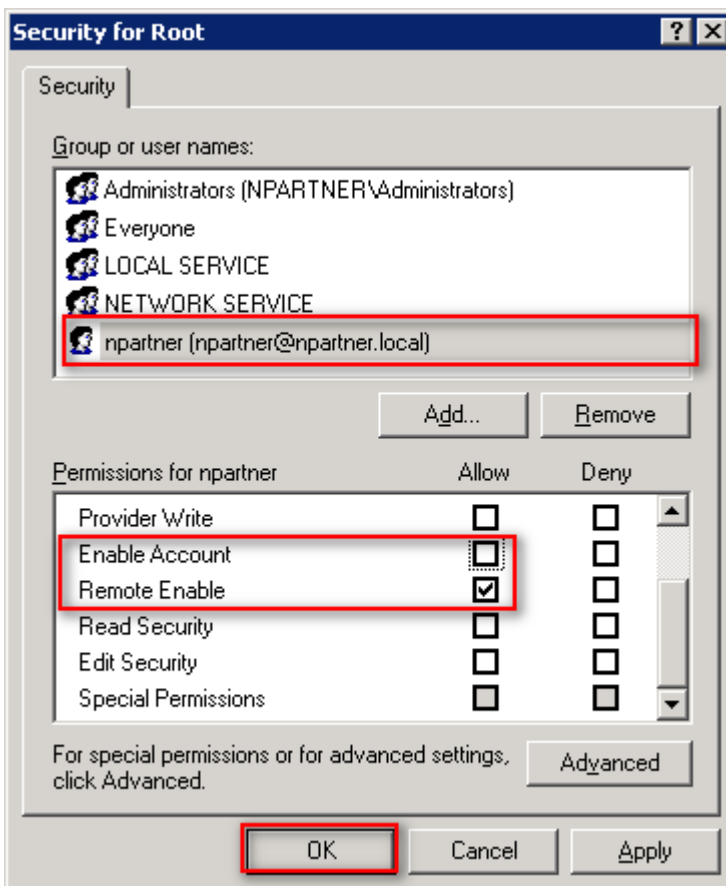
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”

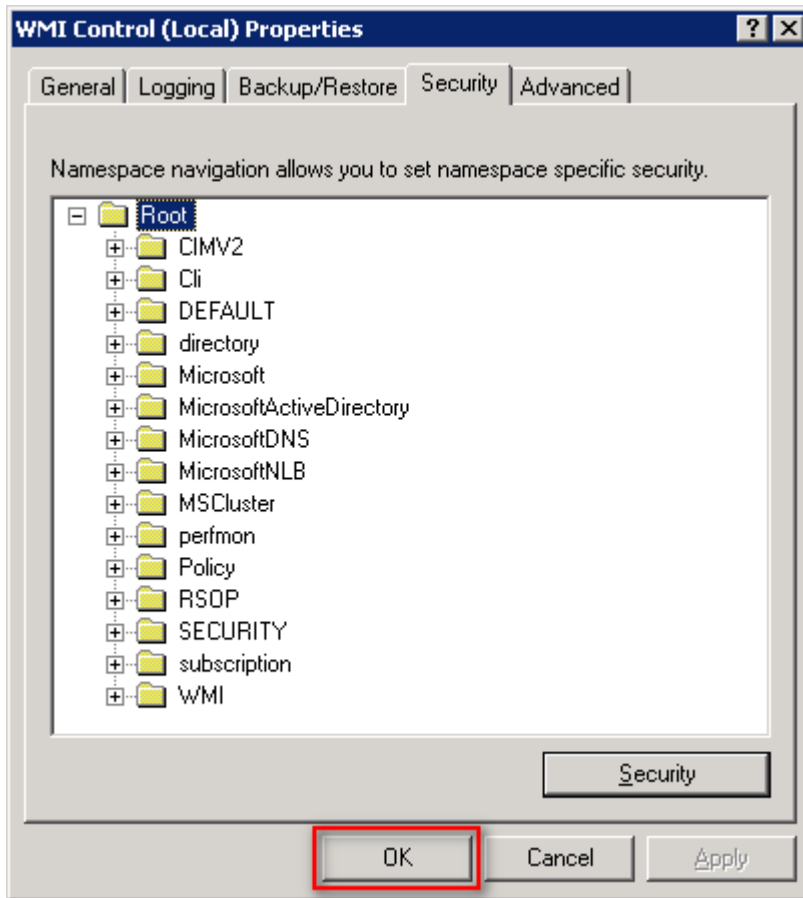


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Click "OK."



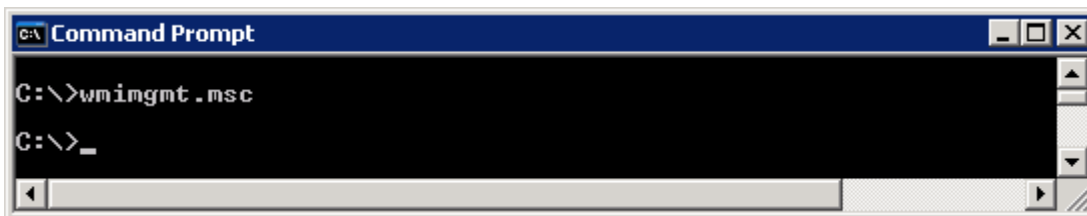
2.3.3.2 Configure Permissions for Reading User Data

(1) Open "Command Prompt."



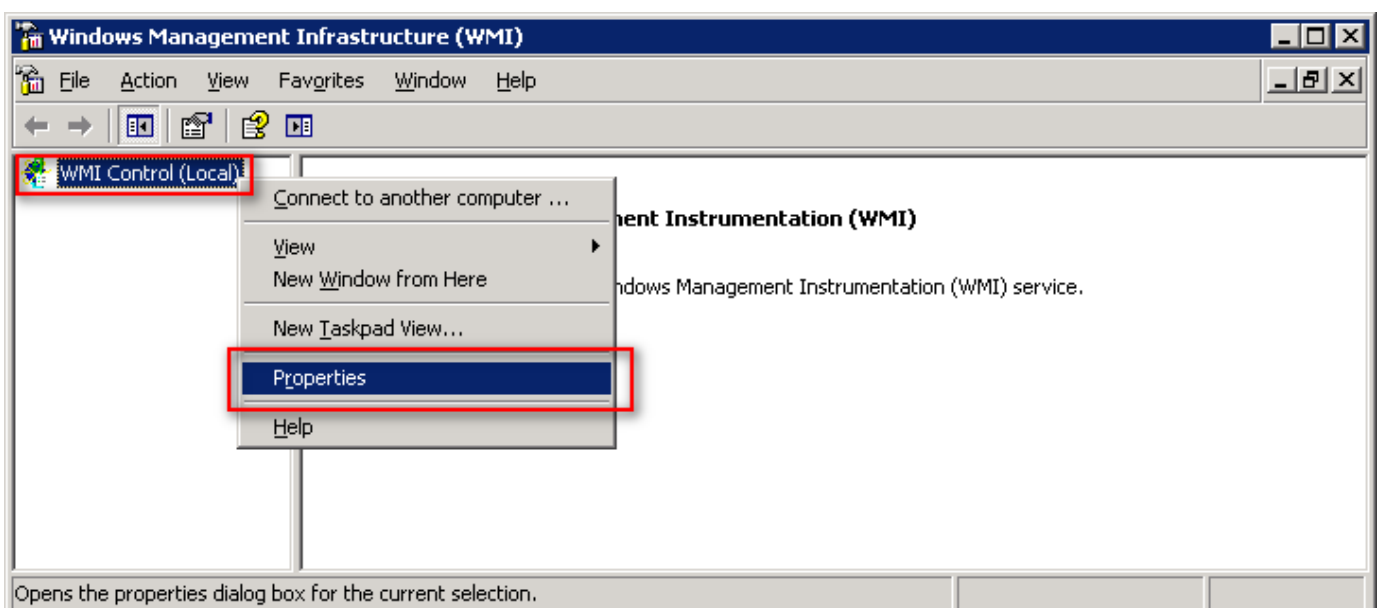
(2) Open "WMI Control."

```
C:\> wmicmgmt.msc
```



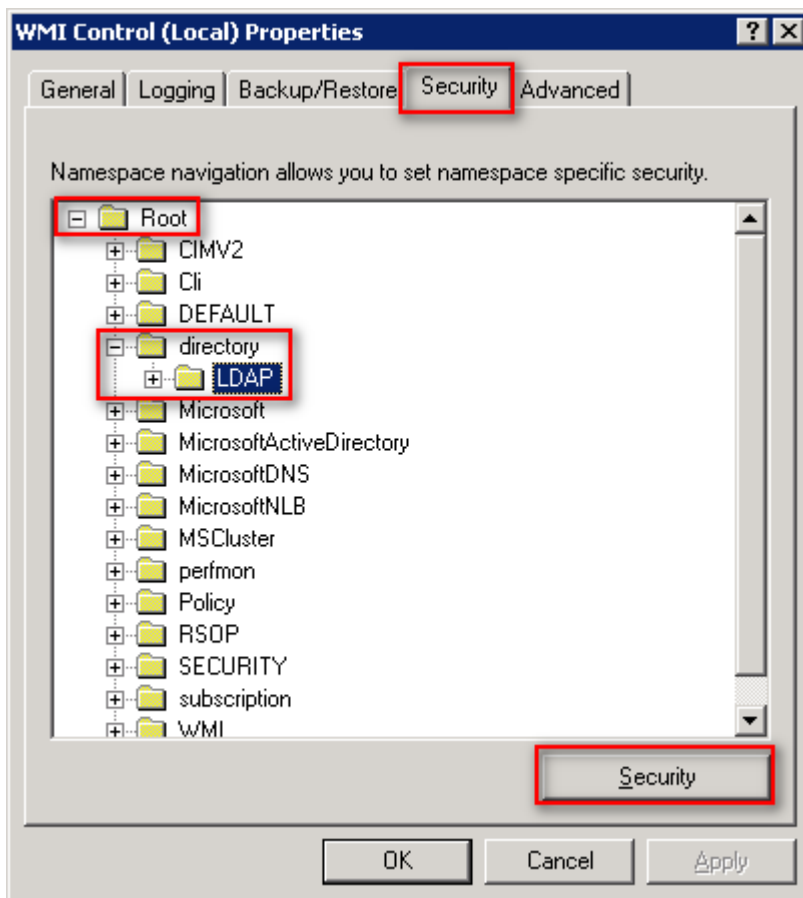
(3) Edit WMI Control

Right-click "WMI Control (Local)" → select Properties."



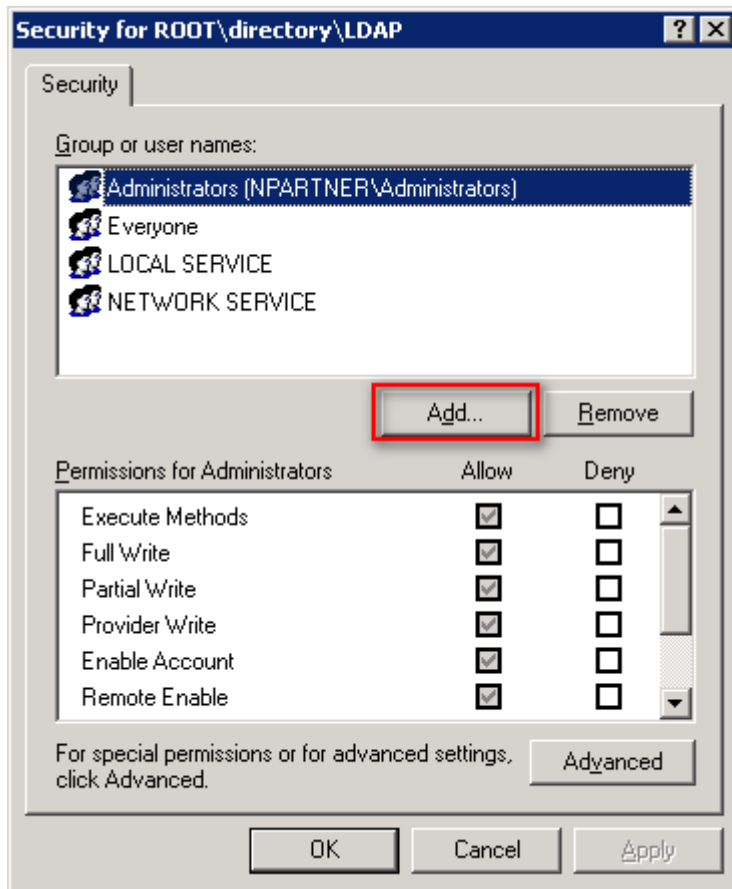
(4) Edit LDAP Security Settings

Go to the “Security tab → expand Root → directory → LDAP → click Security.”



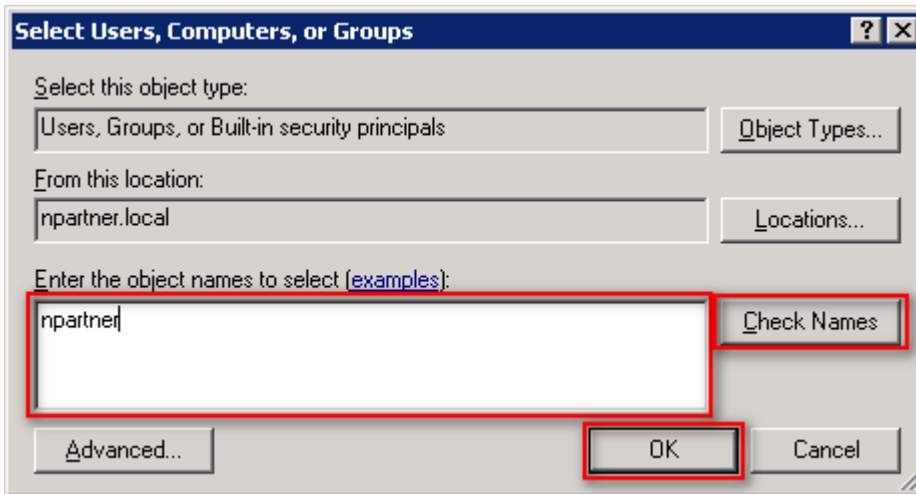
(5) Add WMI User Permissions

Click "Add."



(6) Specify the User

Enter the user account (example: **npartner**) → click Check Names → click “OK.”

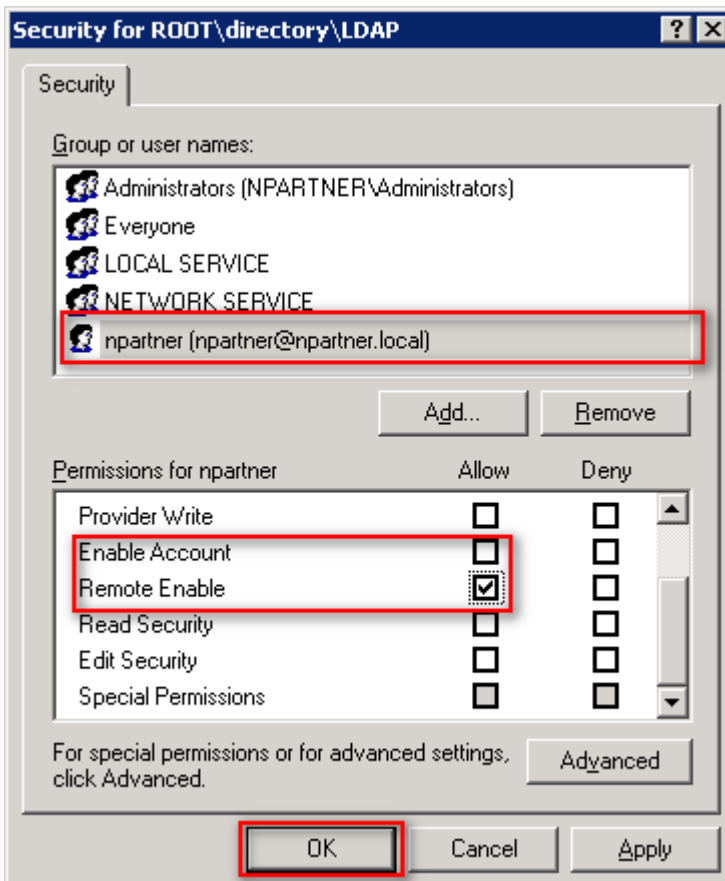


(7) Configure User Permissions

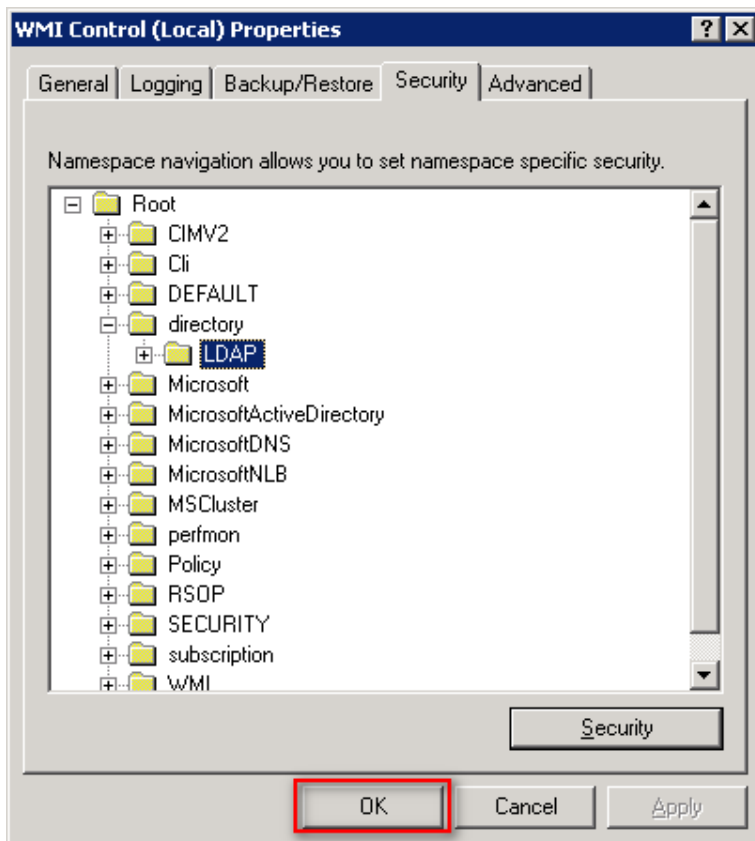
Select the user account (npartner):

- Clear Enable Account: Allow
- Select Remote Enable: Allow

Click OK.



(8) Click "OK."

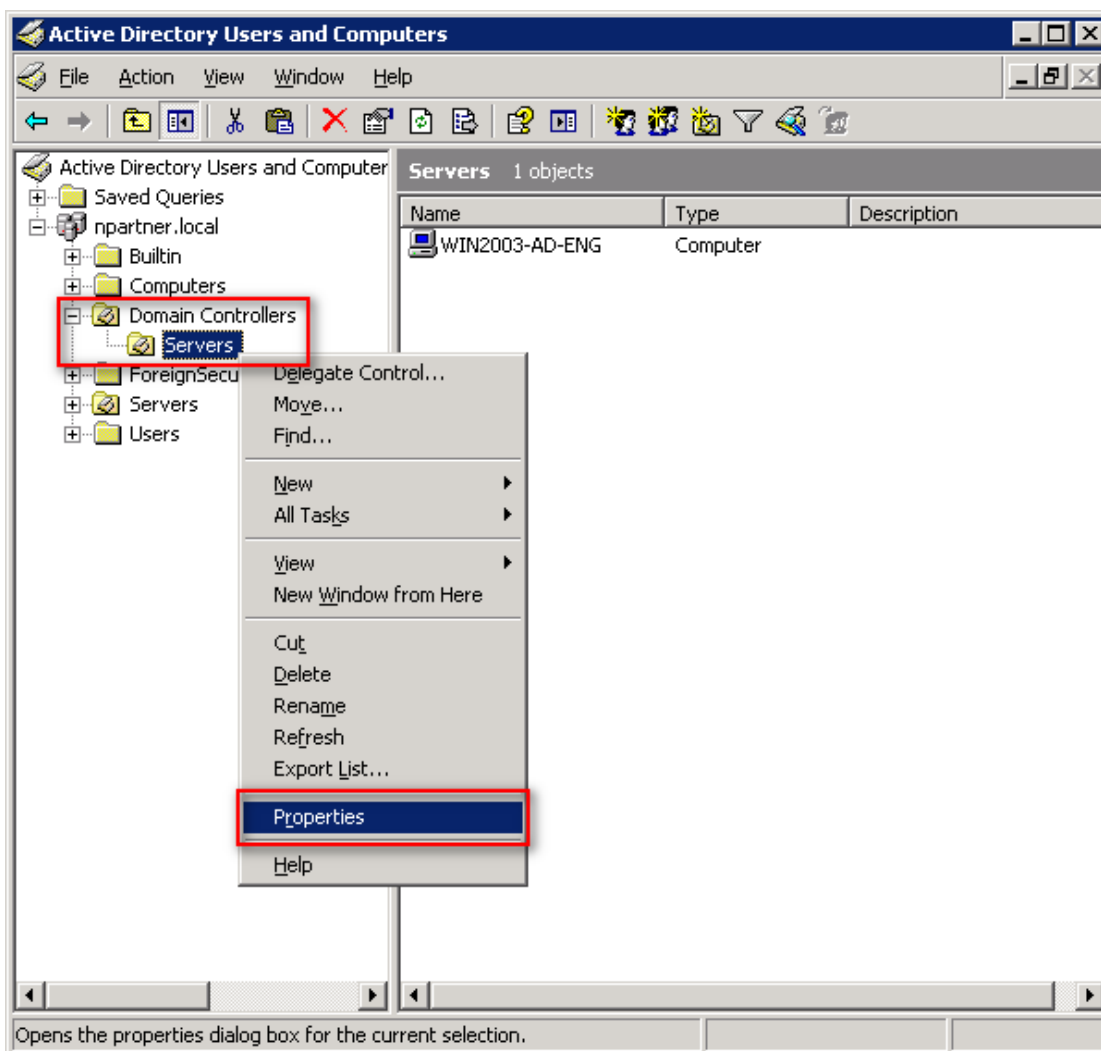


2.3.4 Configure Event Log Read Permissions

(1) Open “Active Directory Users and Computers.”



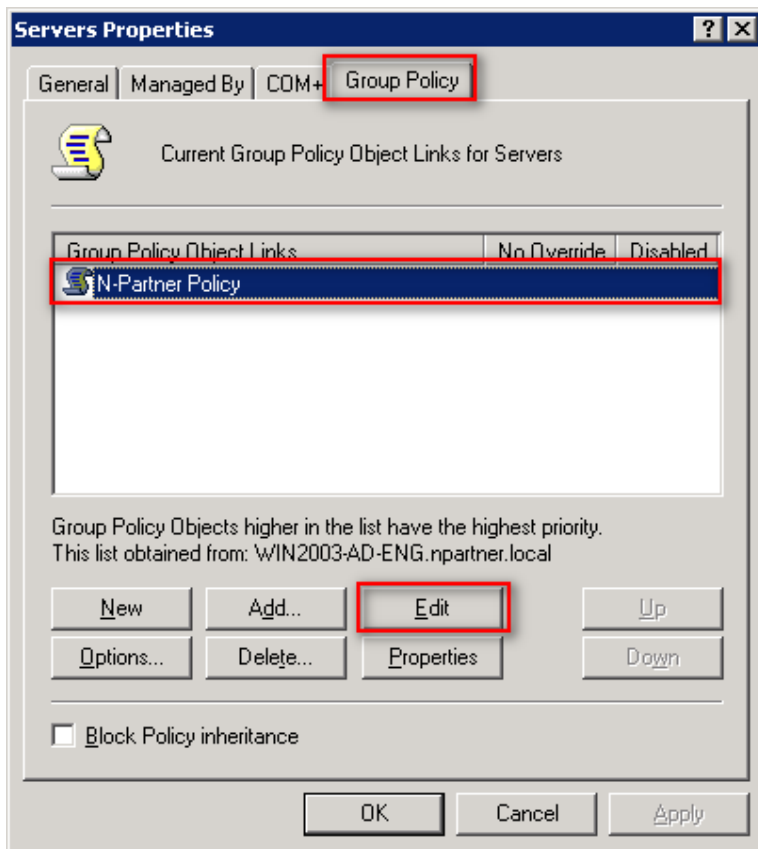
(2) Right-click the “Servers” organizational unit under Domain Controllers, then select “Properties.”




(3) Edit Your Group Policy Object

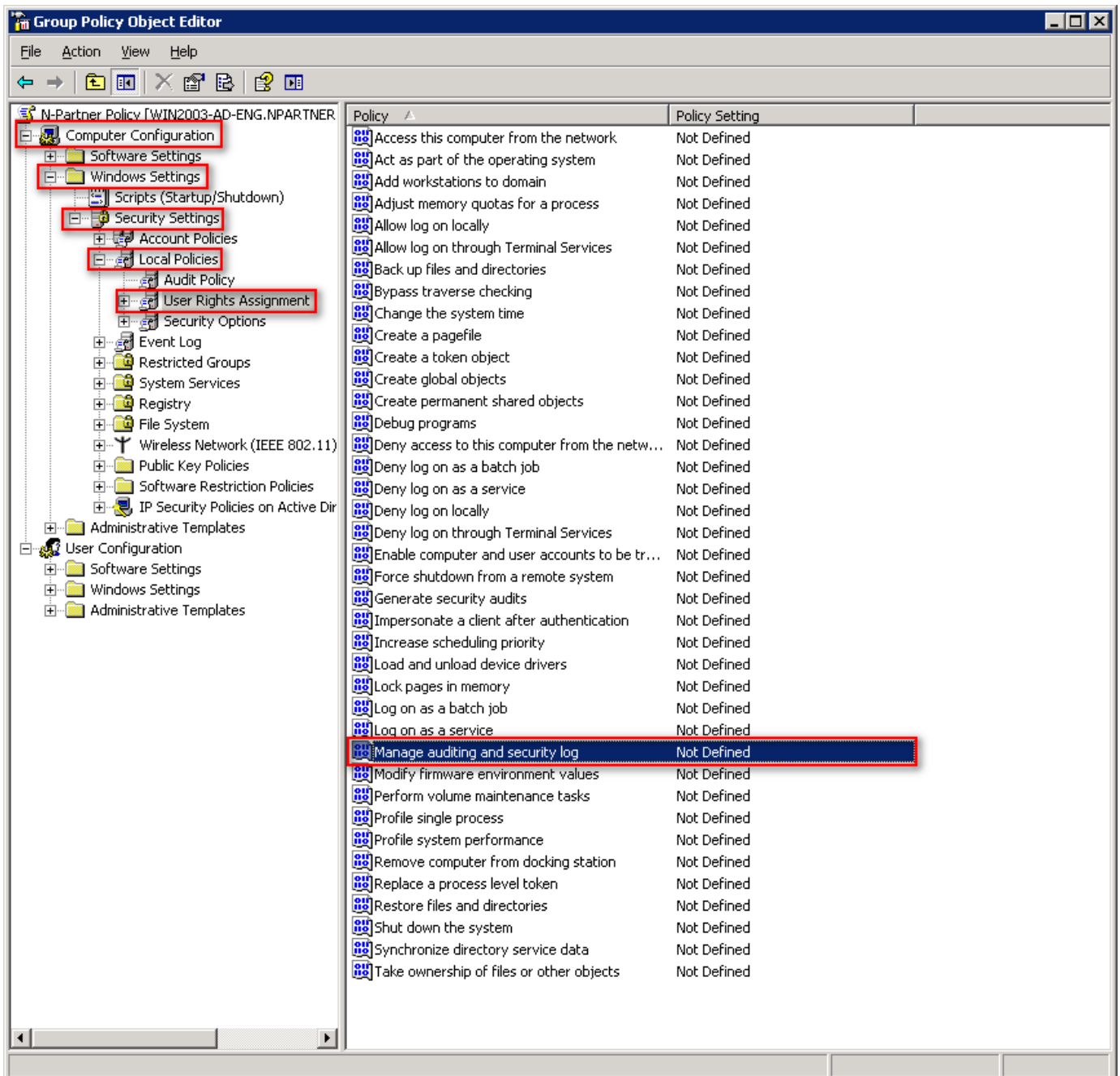
Enter your group policy object name (the example here is [N-Partner Policy](#))

Click "Edit."



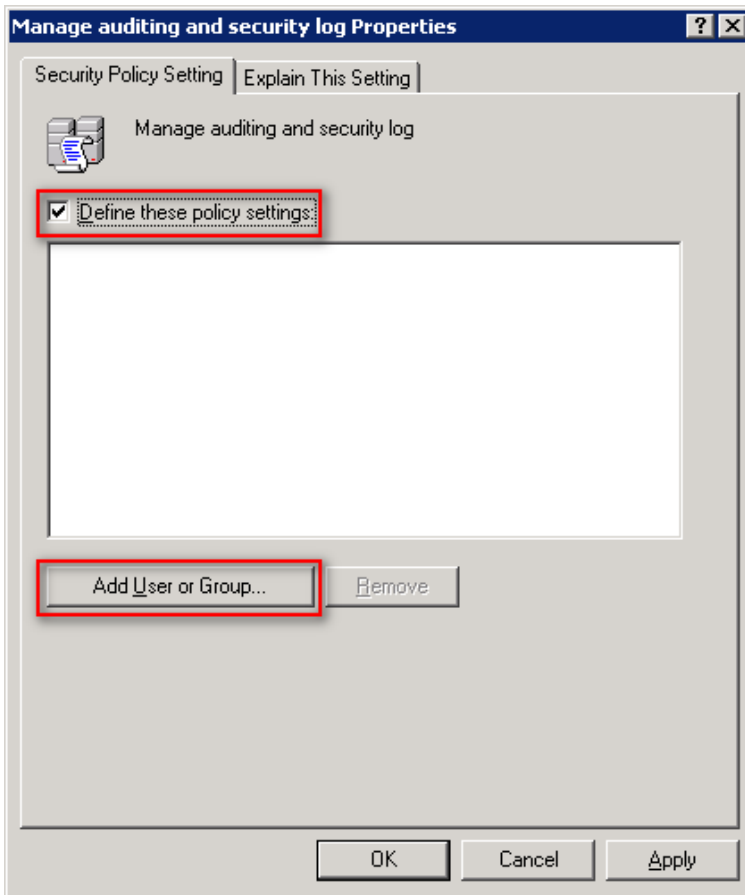
(4) Configure Logging

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “User Rights Assignment.” And click on “Manage auditing and security log,” → Click  “Properties.”



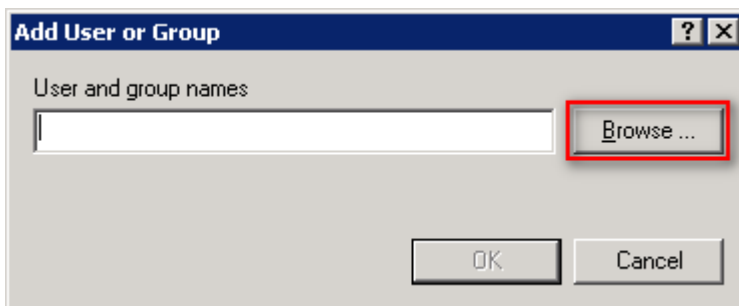
(5) Add Audit Management Users

Select “Define these policy settings, then click Add User or Group....”



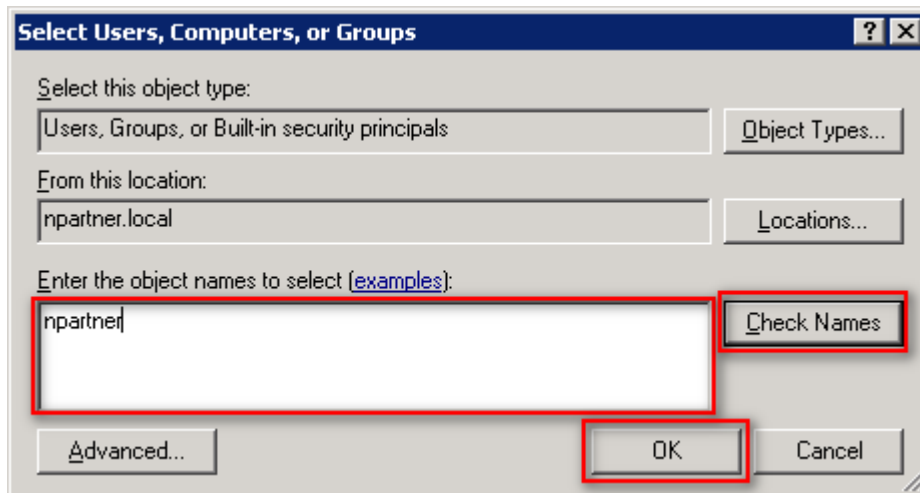
(6) Search for Users

Click “Browse.”



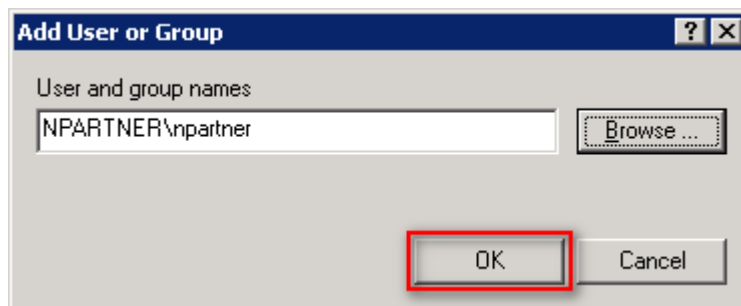
(7) Specify the User

Enter the user account (example: **npartner**) → click “Check Names” → click “OK.”



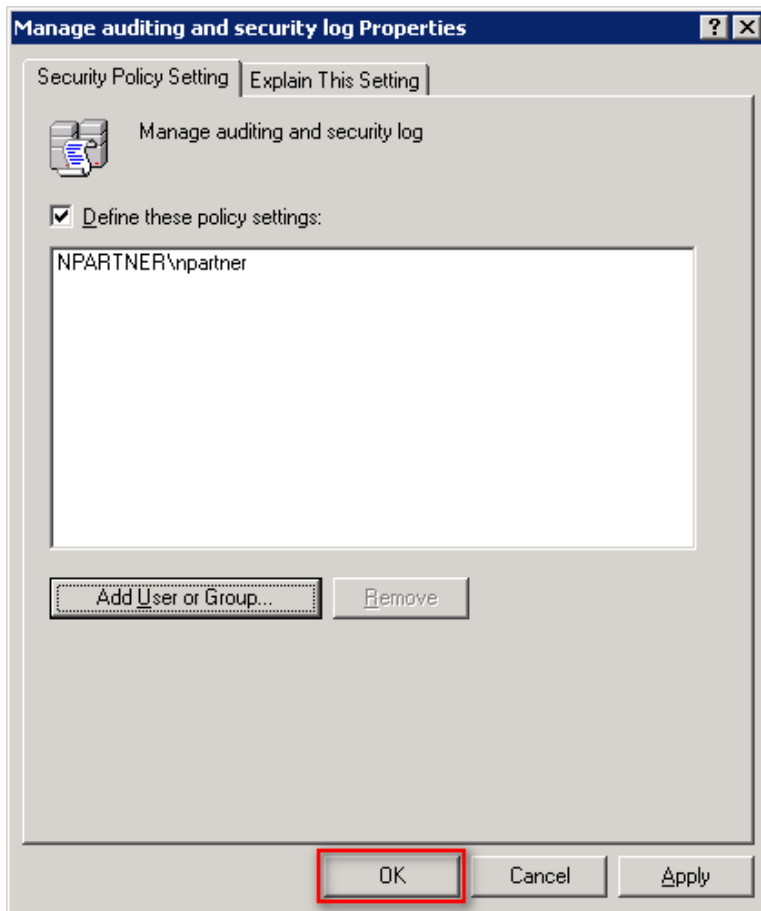
(8) Confirm the User

Click “OK.”



(9) Confirm log settings

Click "OK."

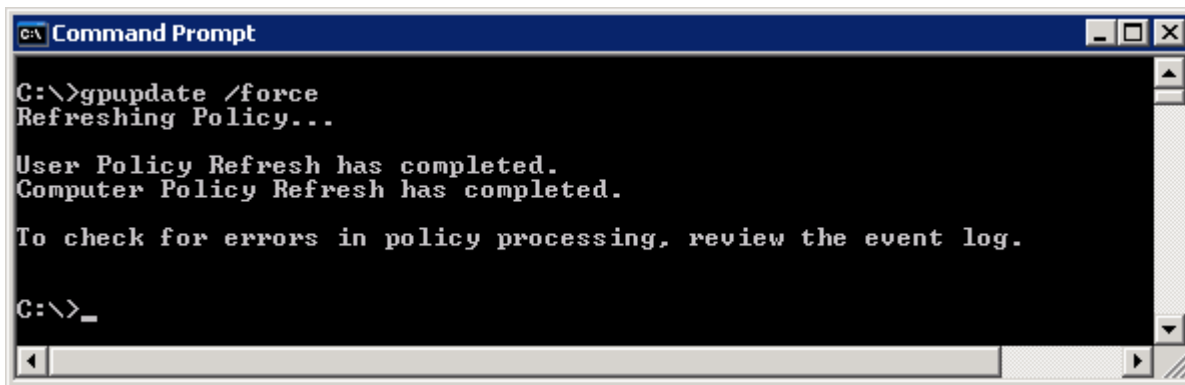


(10) Click "Command Prompt."



(11) Enter the command below to update group policy settings:

```
C:\> gpupdate /force
```



```
Command Prompt
C:\>gpupdate /force
Refreshing Policy...

User Policy Refresh has completed.
Computer Policy Refresh has completed.

To check for errors in policy processing, review the event log.

C:\>_
```

2.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”



(2) Enter the command below to disable the WMI service.

```
C:\> net stop winmgmt
```

```
C:\> net stop winmgmt
The Windows Management Instrumentation service is stopping.
The Windows Management Instrumentation service was stopped

C:\>_
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\> Command Prompt'. The command 'net stop winmgmt' has been entered and executed. The output shows two lines: 'The Windows Management Instrumentation service is stopping.' and 'The Windows Management Instrumentation service was stopped'. The prompt 'C:\>_' is visible at the bottom.

(3) Enter the command below to enable WMI service.

```
C:\> net start winmgmt
```

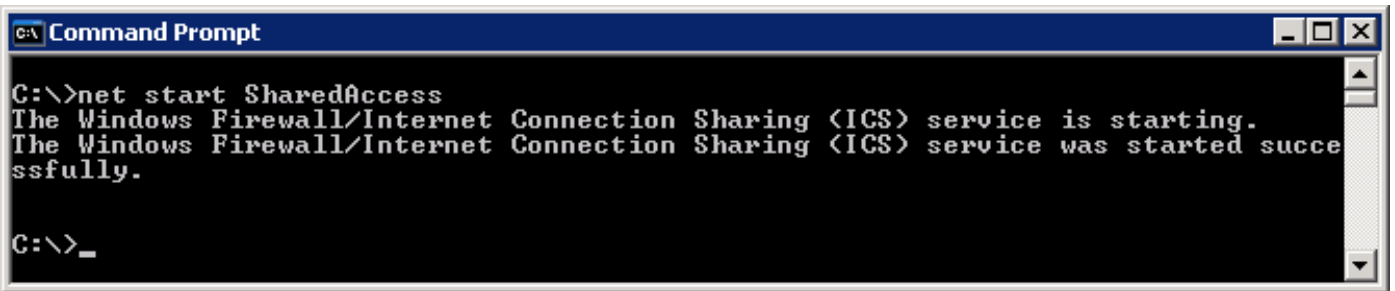
```
C:\> net start winmgmt
The Windows Management Instrumentation service is starting.
The Windows Management Instrumentation service was started

C:\>_
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\> Command Prompt'. The command 'net start winmgmt' has been entered and executed. The output shows two lines: 'The Windows Management Instrumentation service is starting.' and 'The Windows Management Instrumentation service was started'. The prompt 'C:\>_' is visible at the bottom.

(4) Enter the command below to enable the firewall service.

```
C:\> net start SharedAccess
```



```
C:\> net start SharedAccess
The Windows Firewall/Internet Connection Sharing (ICS) service is starting.
The Windows Firewall/Internet Connection Sharing (ICS) service was started successfully.

C:\> _
```

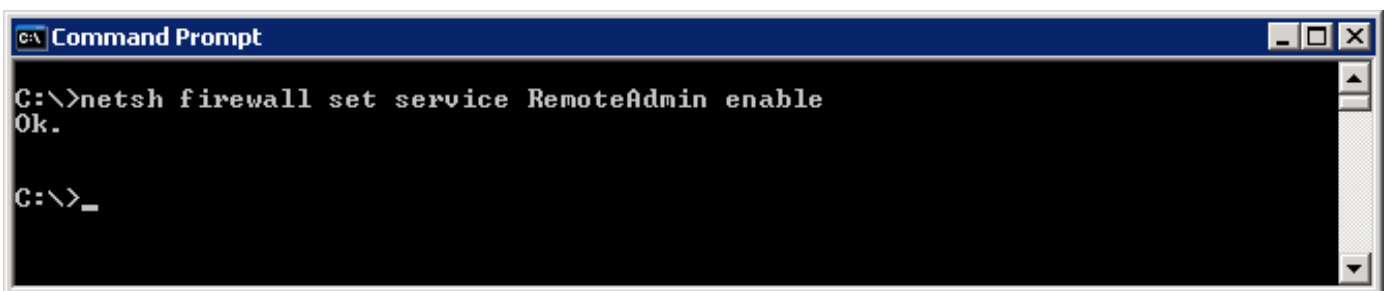
2.4 Firewall Configuration

(1) Open "Command Prompt."



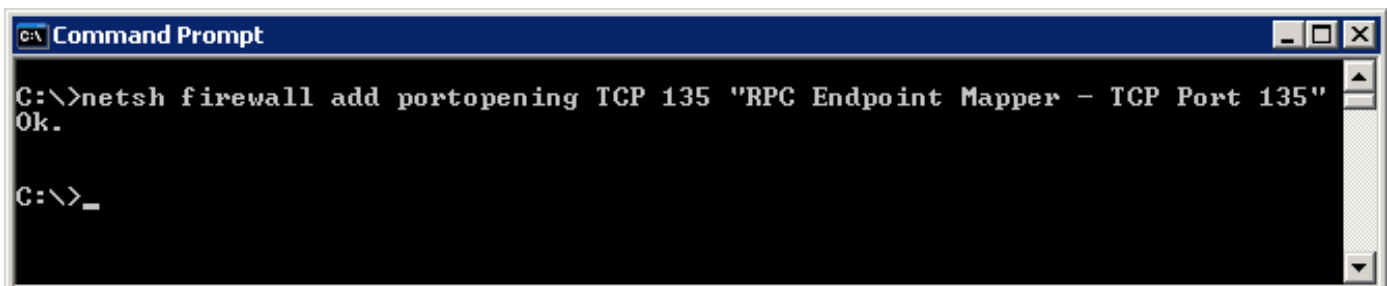
(2) Enter the command below to allow WMI traffic through the firewall.

```
C:\> netsh firewall set service RemoteAdmin enable
```



(3) Enter the command below to allow TCP Port 135 through the firewall.

```
C:\> netsh firewall add portopening TCP 135 "RPC Endpoint Mapper - TCP Port 135"
```



(4) Enter the command below to check the firewall configuration.

```
C:\> netsh firewall show config
```

```
Command Prompt
C:\>netsh firewall show config

Domain profile configuration:
-----
Operational mode           = Disable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Standard profile configuration (current):
-----
Operational mode           = Enable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Service configuration for Standard profile:
Mode      Customized  Name
-----
Enable   No          Remote Desktop
Enable   No          Remote Administration

Port configuration for Standard profile:
Port      Protocol  Mode      Name
-----
135       TCP       Enable    RPC Endpoint Mapper - TCP Port 135
3389      TCP       Enable    Remote Desktop

Log configuration:
-----
File location      = C:\WINDOWS\pf\firewall.log
Max file size     = 4096 KB
Dropped packets   = Disable
Connections       = Disable

Local Area Connection firewall configuration:
-----
Operational mode           = Enable

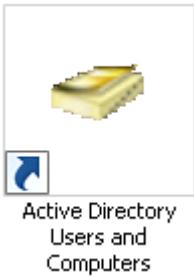
C:\>
```

3. Windows 2008

For detailed information on setting Windows audit policies, please refer to the [“audit policy recommendations link”](#) in the preface.

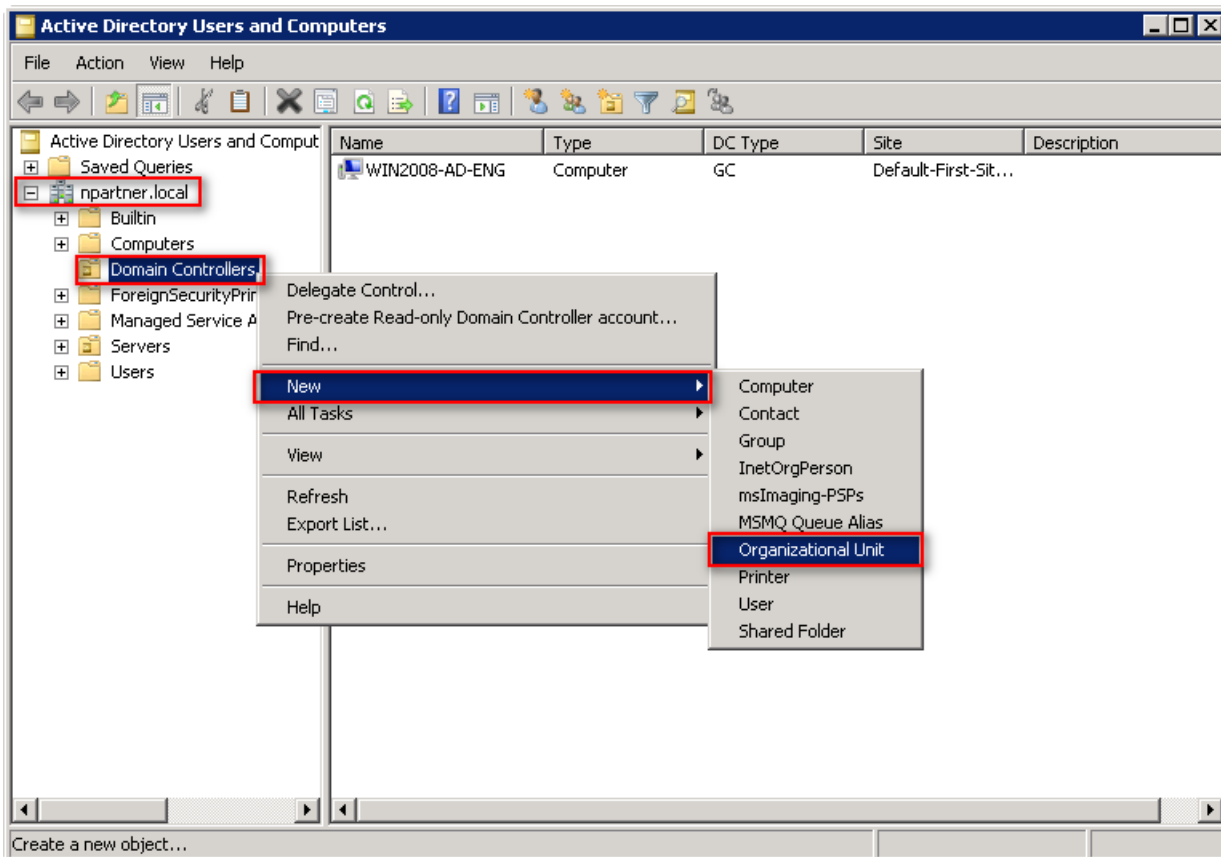
3.1 Organizational Unit Settings

(1) Open “Active Directory Users and Computers.”



(2) Add an Organizational Unit

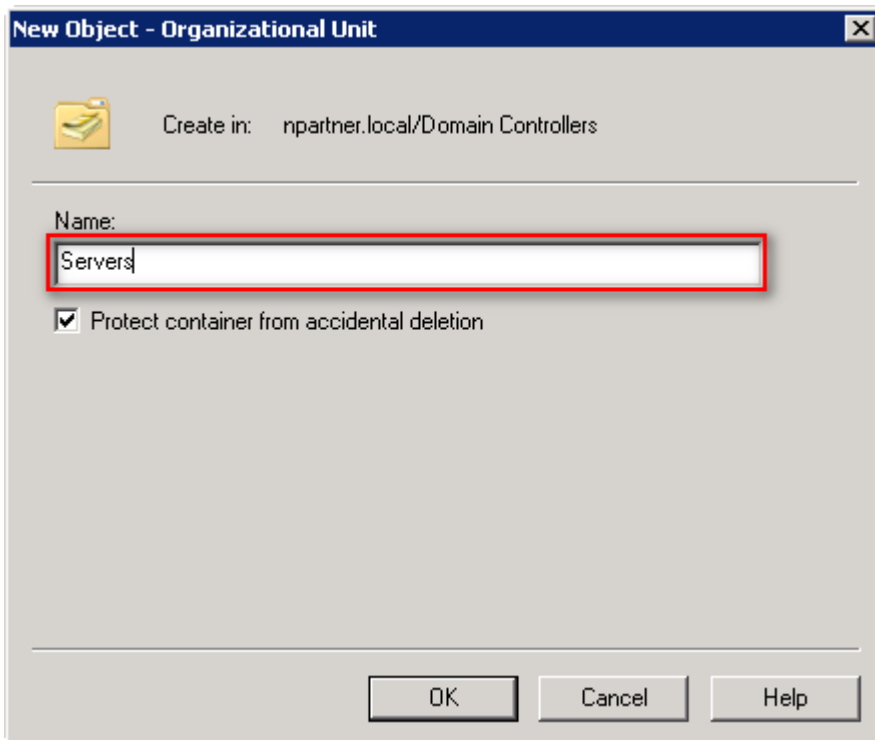
Right-click on “Domain Controllers,” select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit’s name according to the actual environment.

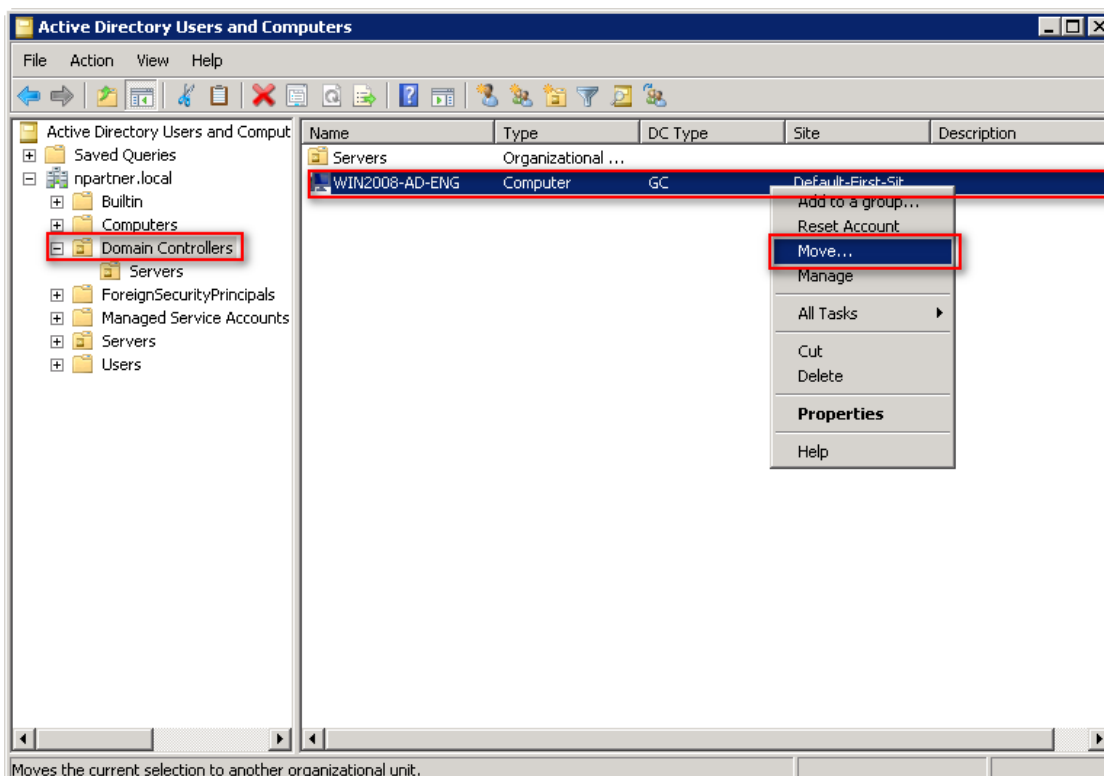
-> Click “OK.”



(4) Move the Server to your New Organizational Unit:

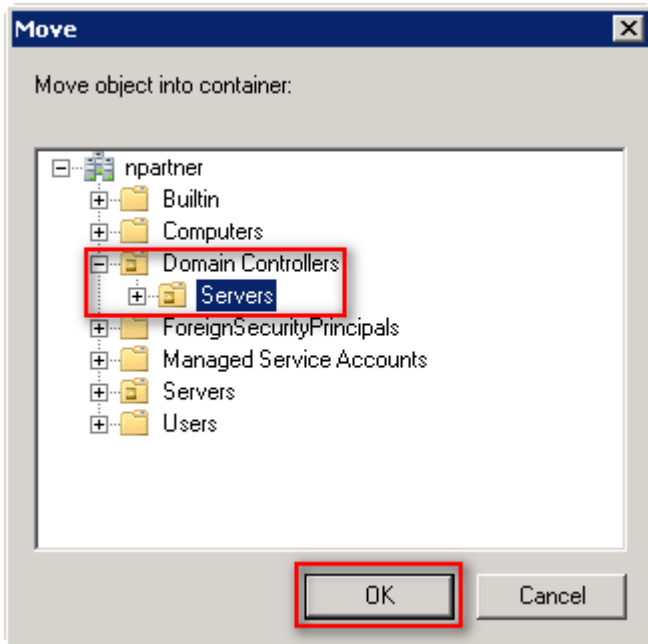
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2008-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



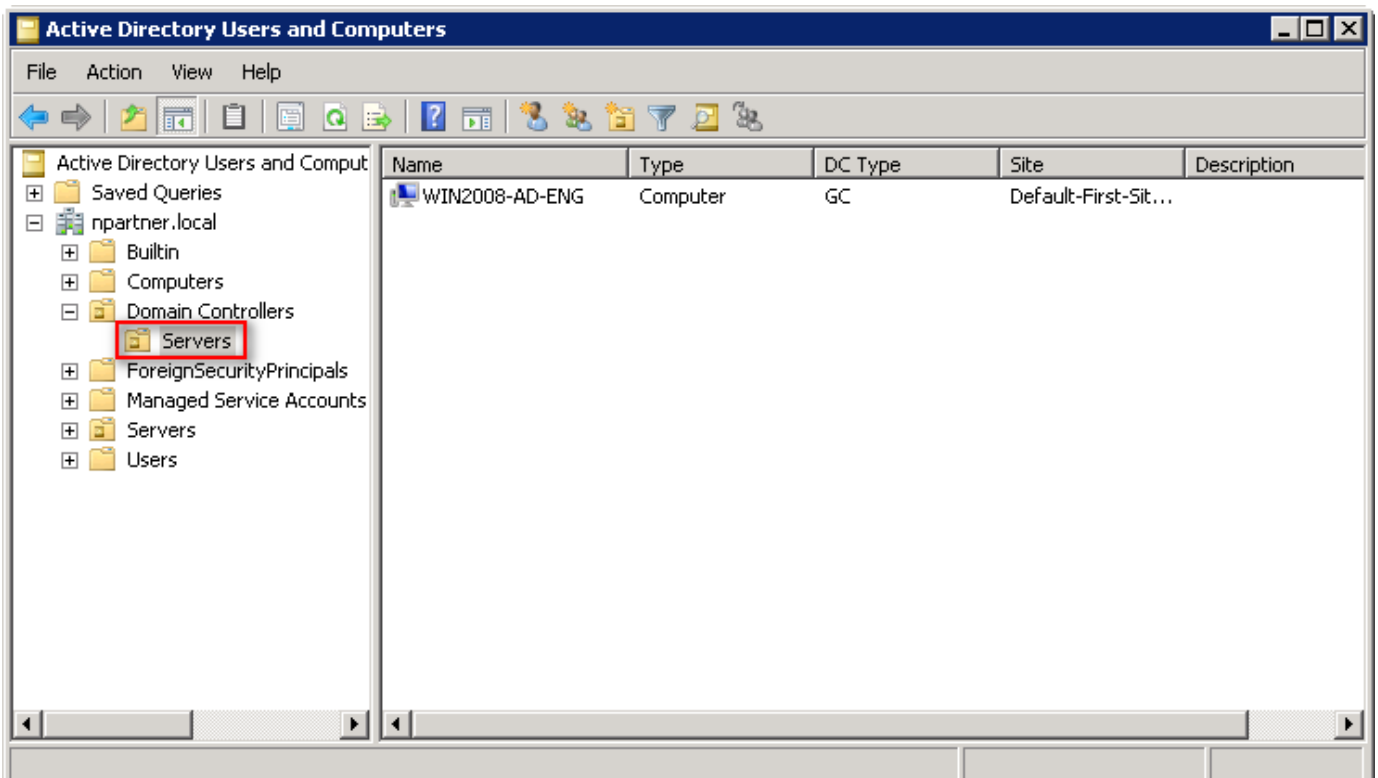
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



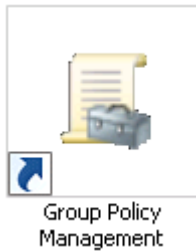
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2008-AD-ENG” server has been moved.

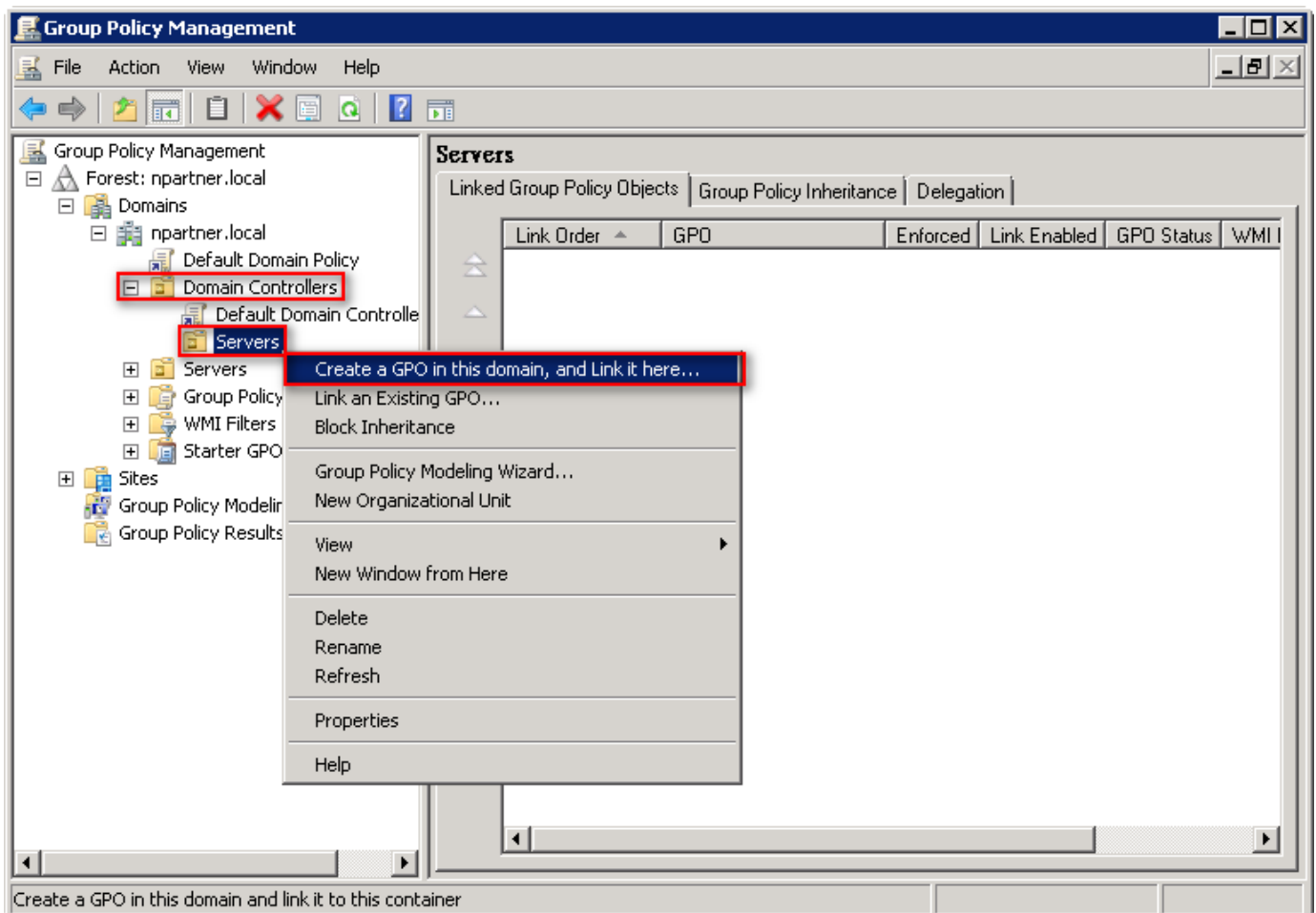


3.2 Group Policy Settings

(1) Open “Group Policy Management.”



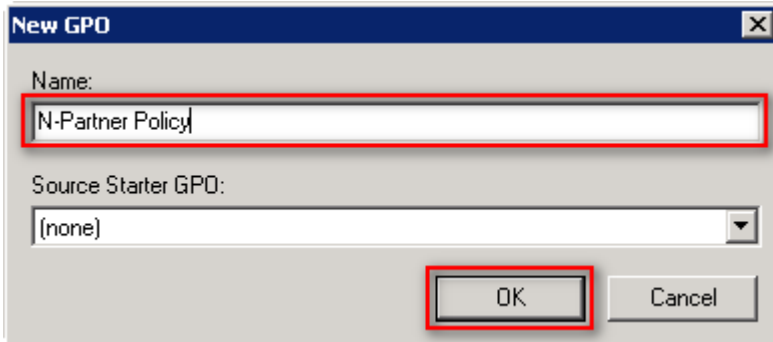
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(3) Edit your Group Policy Object

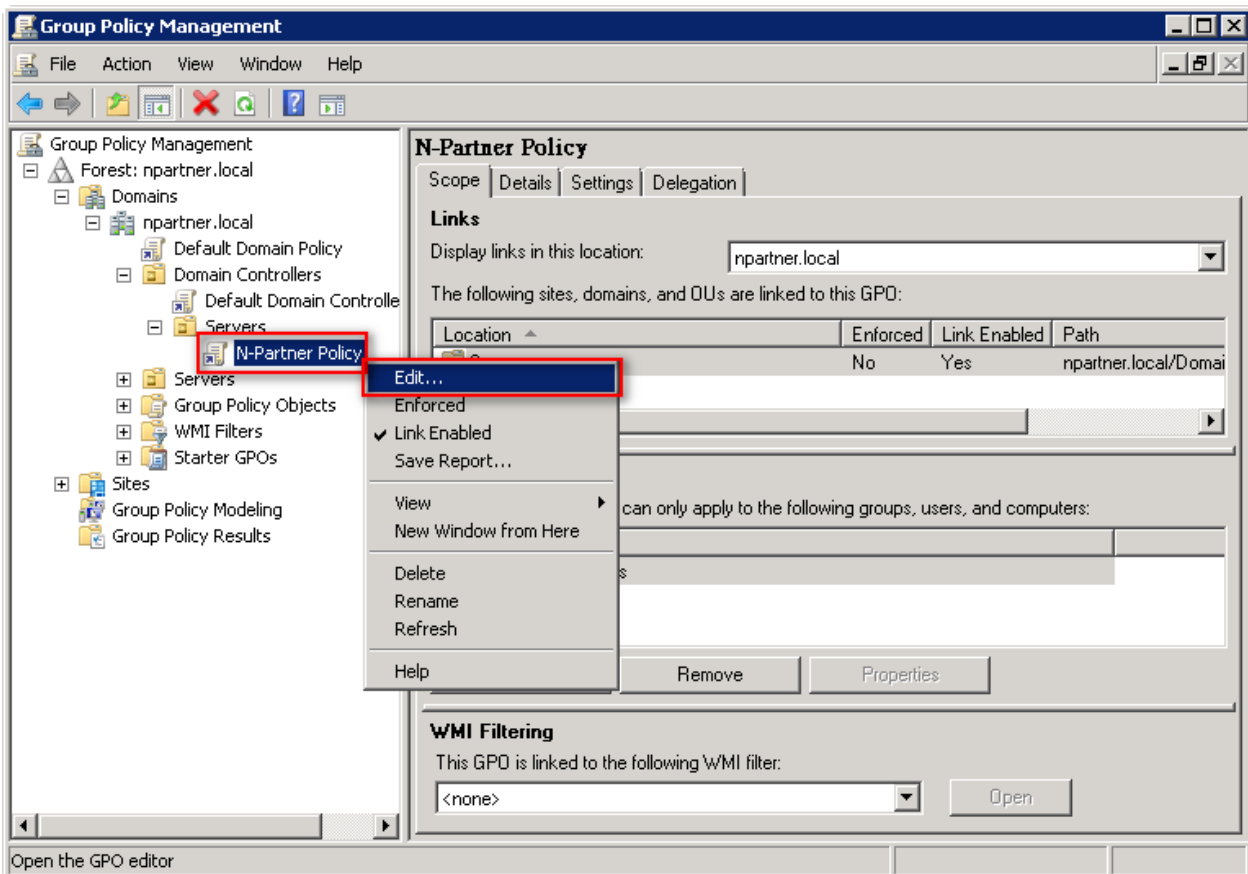
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. Then click “Edit.”



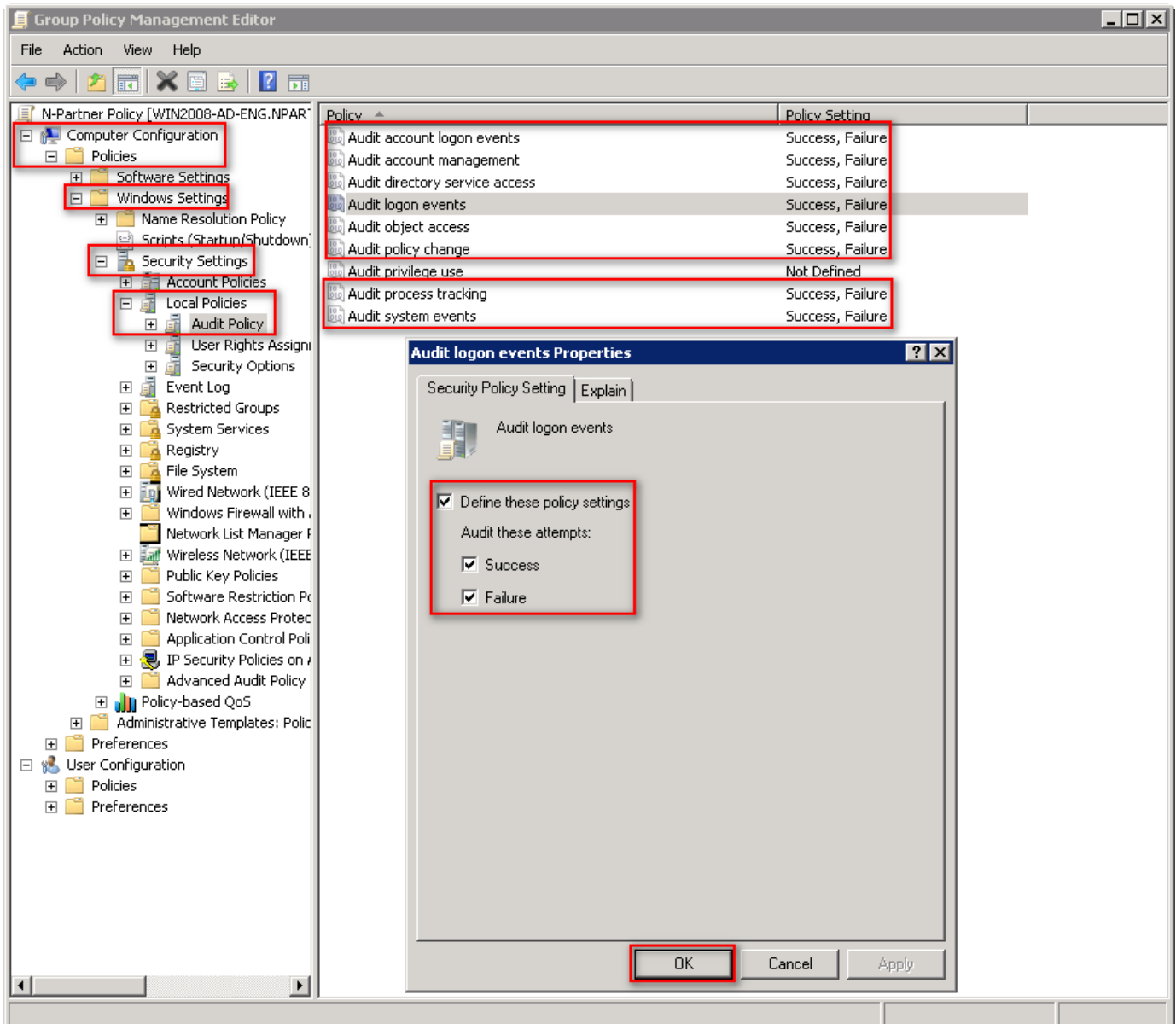
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click “OK.”

The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows the tree structure: Computer Configuration > Windows Settings > Security Settings > Event Log. The right-hand pane lists various policies, with 'Maximum security log size' selected and highlighted. A 'Maximum security log size Properties' dialog box is open in the foreground, showing the 'Define this policy setting' checkbox checked and the value '204800 kilobytes' entered in the text field. The 'OK' button is also highlighted.

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

(7) Event Logs: Retention Method for Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting” -> Select “Overwrite events as needed” -> Then click “OK.”

The screenshot shows the Group Policy Management Editor interface. The left-hand tree view is expanded to show the path: Computer Configuration > Windows Settings > Security Settings > Event Log. The right-hand pane displays a list of policies, with 'Retention method for security log' selected and highlighted in red. Below this, the 'Retention method for security log Properties' dialog box is open. In this dialog, the 'Define this policy setting' checkbox is checked, and the 'Overwrite events as needed' radio button is selected. The 'OK' button at the bottom of the dialog is also highlighted in red.

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Retention method for security log Properties

Security Policy Setting | Explain

Retention method for security log

Define this policy setting

Overwrite events by days

Overwrite events as needed

Do not overwrite events (clear log manually)

Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see [Retention method for security log](#). (Q823659)

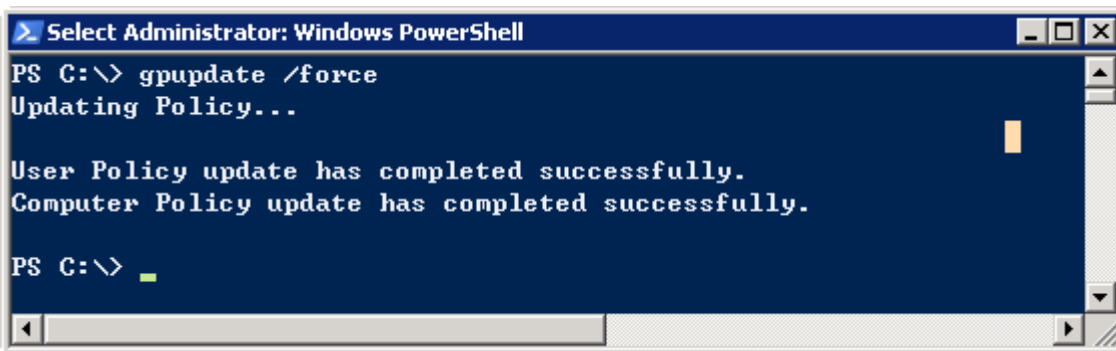
OK Cancel Apply

(8) Open "Windows PowerShell."



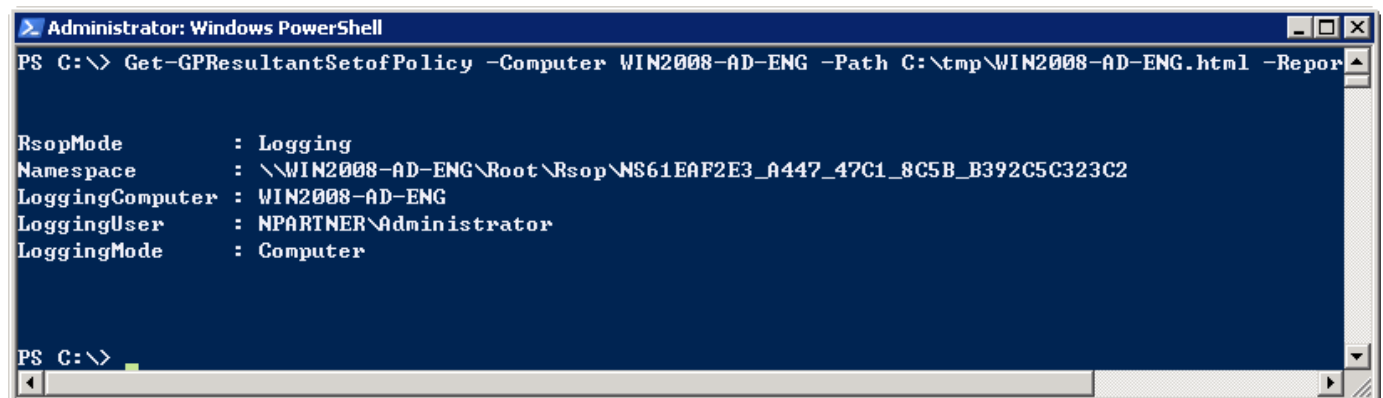
(9) Enter the command below to refresh group policy.

```
PS C:\> gpupdate /force
```



(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008-AD-ENG -Path C:\tmp\WIN2008-AD-ENG.html -ReportType html
```



For the red text , please enter the Windows AD server name and the folder path/file name.

(11) Open the report and verify that your Windows AD server is applying the N-Partner Policy Group Policy.

The screenshot shows a web browser window titled "NPARTNER\WIN2008-AD-ENG - Internet Explorer". The address bar shows "C:\tmp\WIN2008-AD-ENG.html". The main content area is titled "Security Settings" and contains a table of policies and their settings. The table is organized into several sections:

Policy	Setting	Winning GPO
Account Policies/Password Policy		
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
Account Policies/Account Lockout Policy		
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
Account Policies/Kerberos Policy		
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy
Local Policies/Audit Policy		
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit directory service access	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit policy change	Success, Failure	N-Partner Policy
Audit process tracking	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
Local Policies/User Rights Assignment		
Access this computer from the network	Everyone, Administrators, Authenticated Users, ENTERPRISE DOMAIN	Default Domain Controllers Policy

3.3 Add a Non-Admin Account

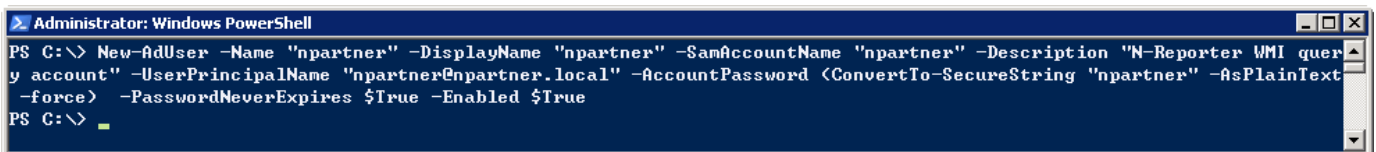
3.3.1 Add Users

(1) Open "Windows PowerShell."



(2) Enter the command below to add a new account.

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

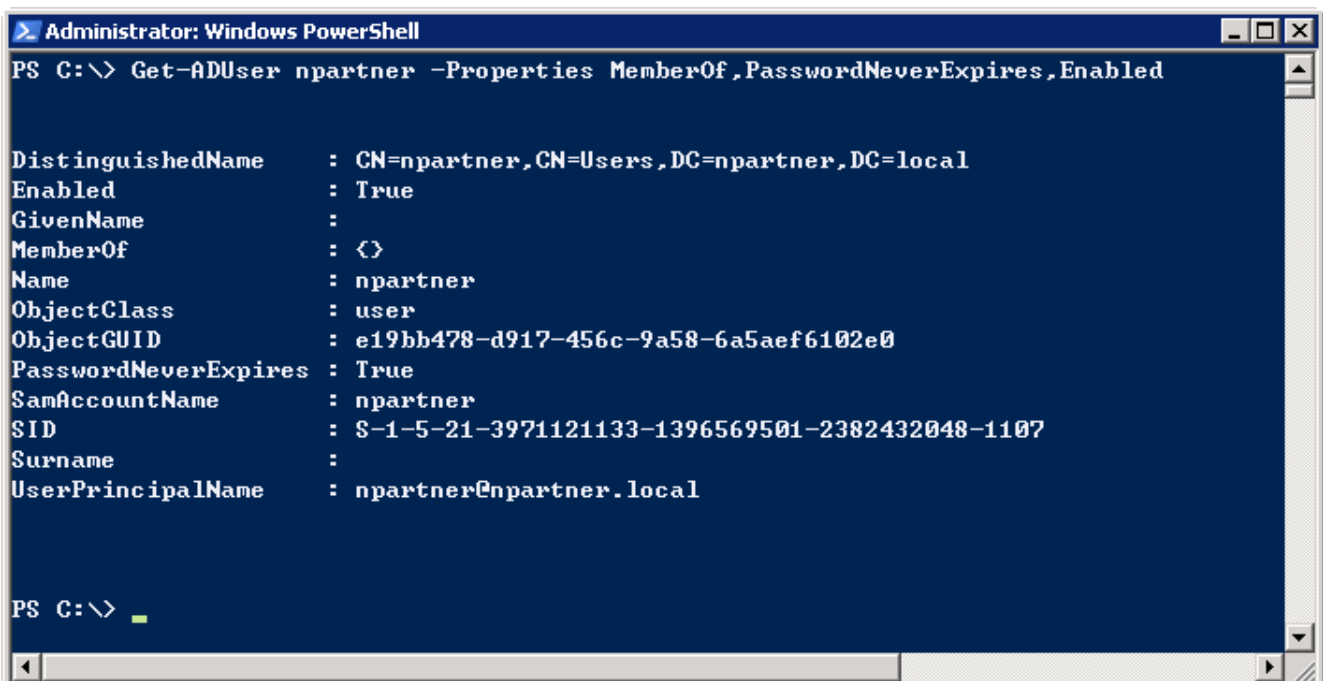
A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the New-AdUser command with the following output:

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True
PS C:\> _
```

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the Get-ADUser command with the following output:

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName              :
MemberOf               : {}
Name                   : npartner
ObjectClass            : user
ObjectGUID             : e19bb478-d917-456c-9a58-6a5aef6102e0
PasswordNeverExpires   : True
SamAccountName         : npartner
SID                    : S-1-5-21-3971121133-1396569501-2382432048-1107
Surname                :
UserPrincipalName      : npartner@npartner.local

PS C:\> _
```

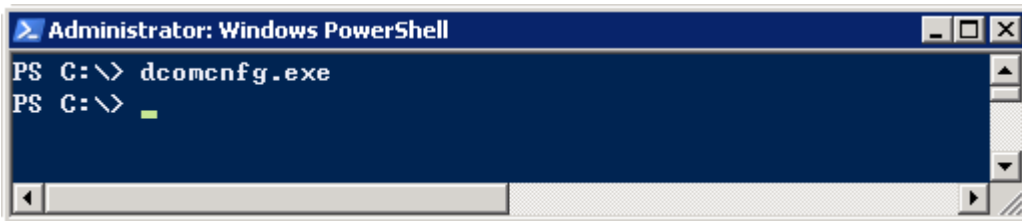
3.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”



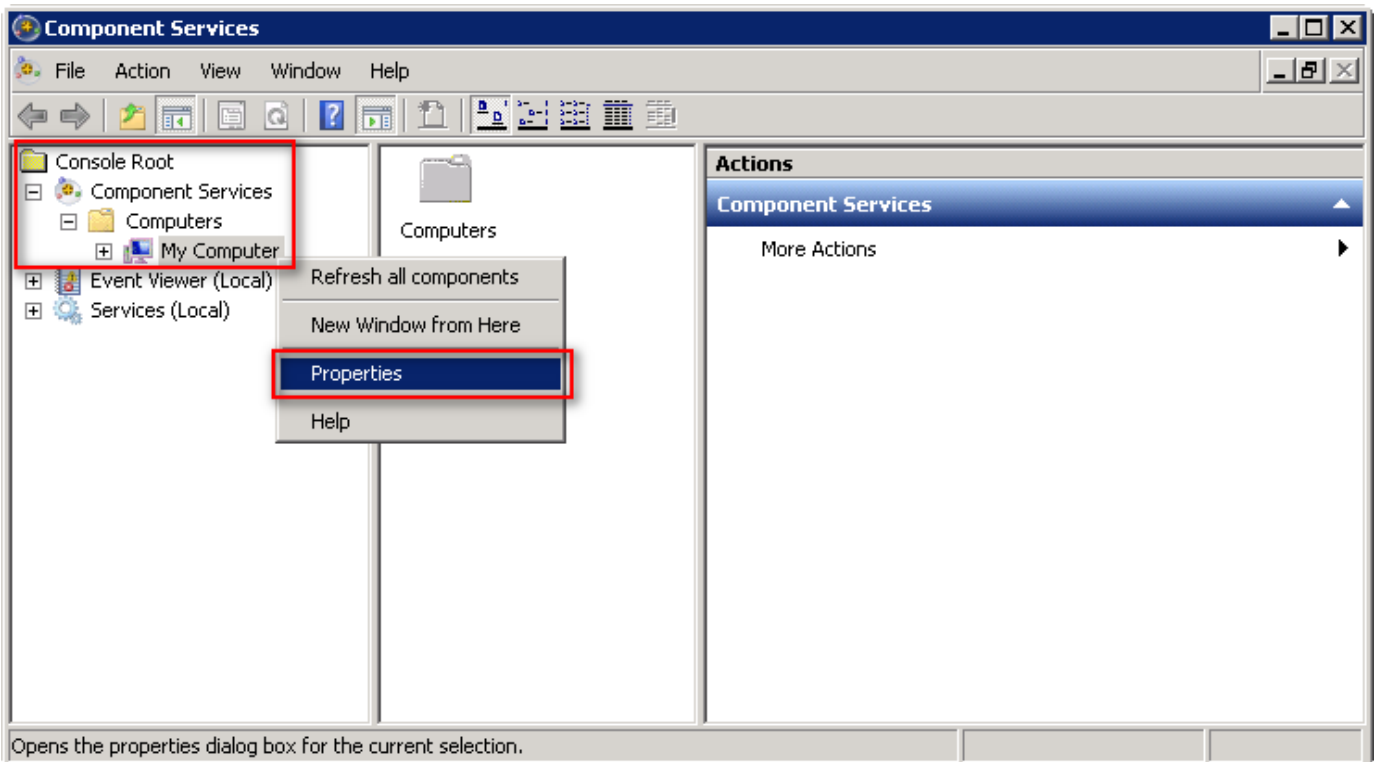
(2) Enter the command below to open component services.

```
PS C:\> dcomcnfg.exe
```



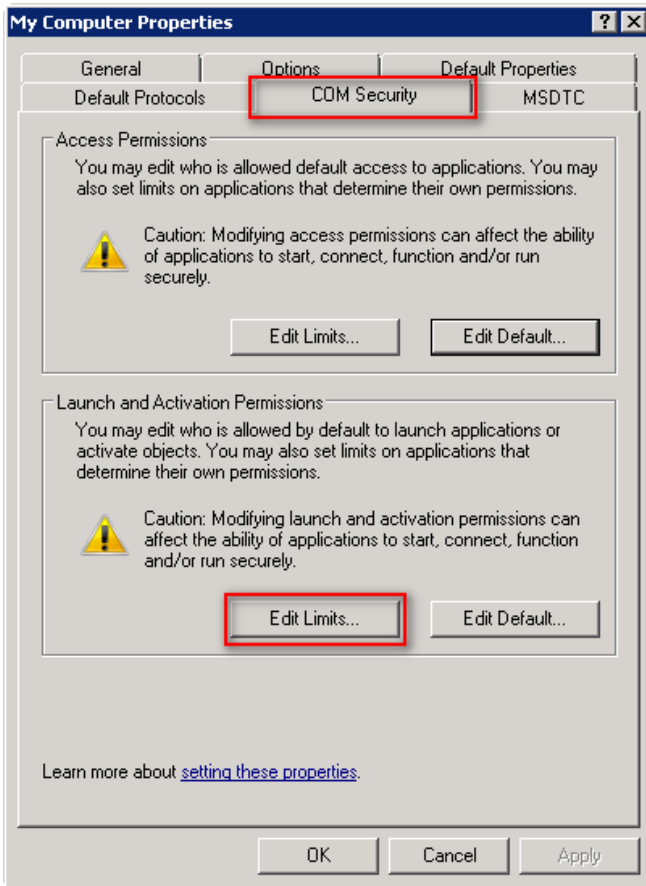
(3) Edit Computer Properties

Expand folder “Console Root” -> “Component Services” -> “Computers,” right-click on “My Computer,” and select “Properties.”



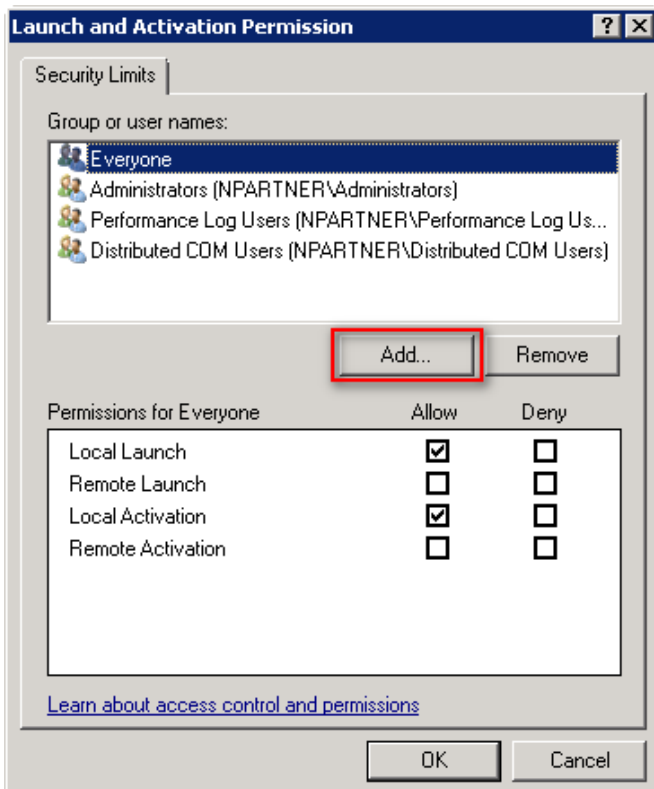
(4) Enable Permissions

Go to the “COM Security” tab, under Launch and Activation Permissions, click “Edit Limits.”



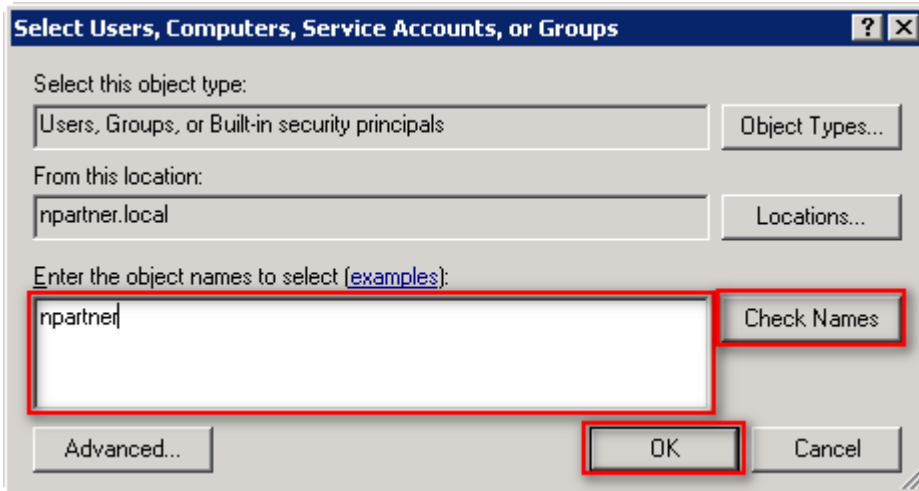
(5) Add DCOM User Permissions

Click “Add.”



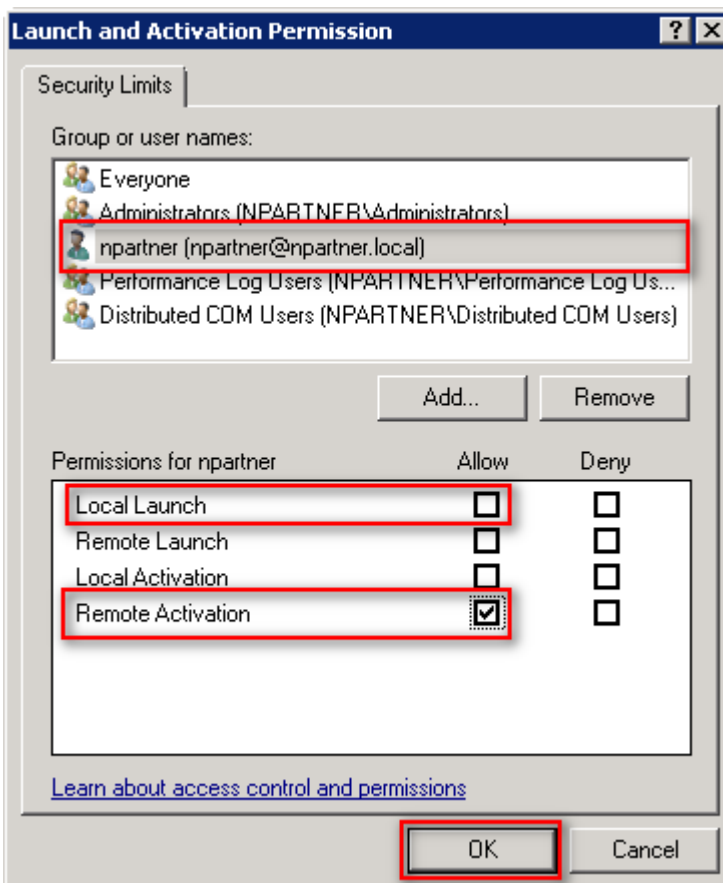
(6) Enter your Username

Input your user account: `npartner`, click “Check Names,” then click “OK.”

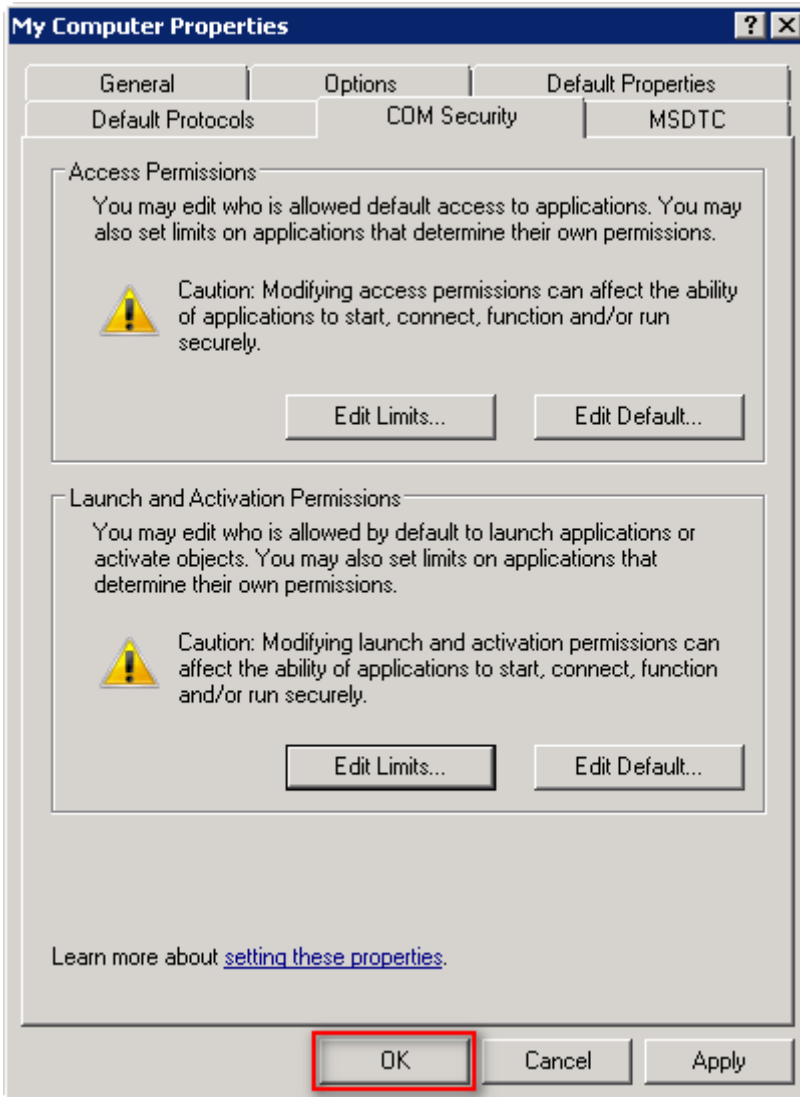


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Local Launch: Allow,” check “Remote Activation: Allow,” then click “OK.”



(8) Click "OK."



3.3.3 Configure WMI Permissions

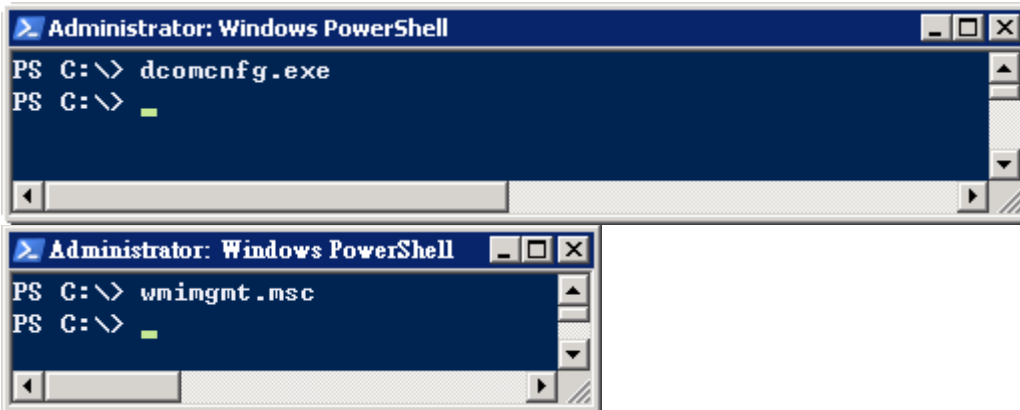
3.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”




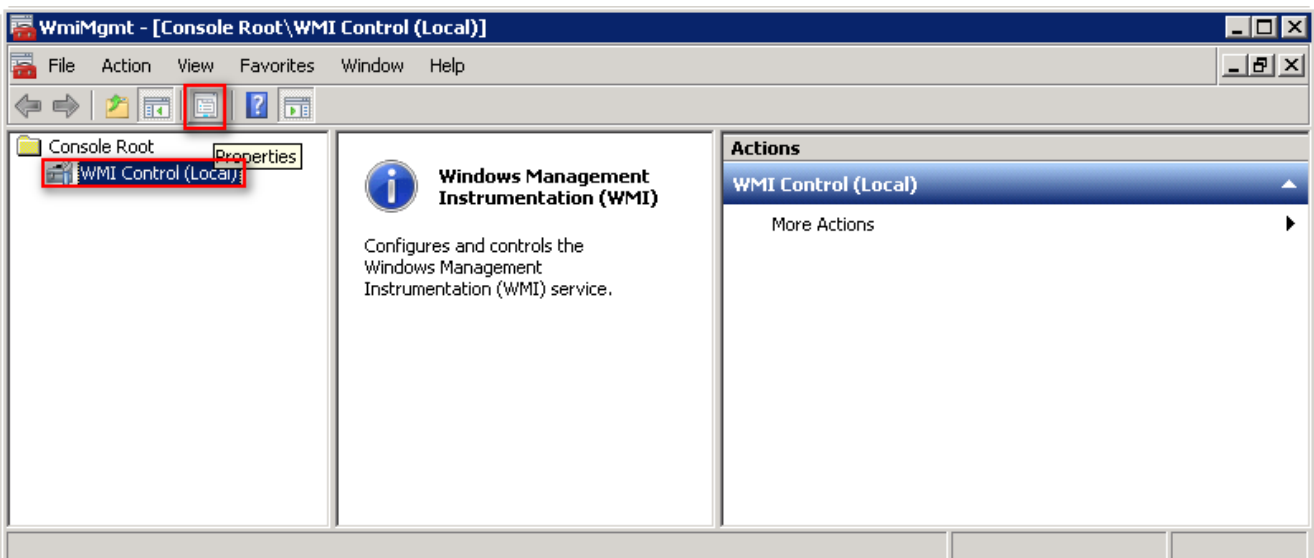
(2) Enter the command below to enable WMI control.

```
PS C:\> wmicmgmt.msc
```



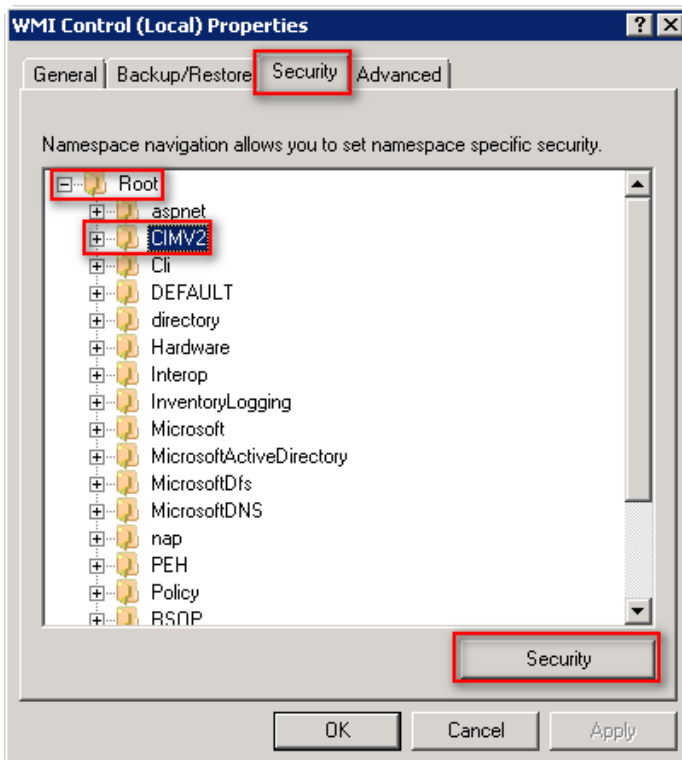
(3) Edit WMI Control

In “WMI Control (Local),” click  (Properties).



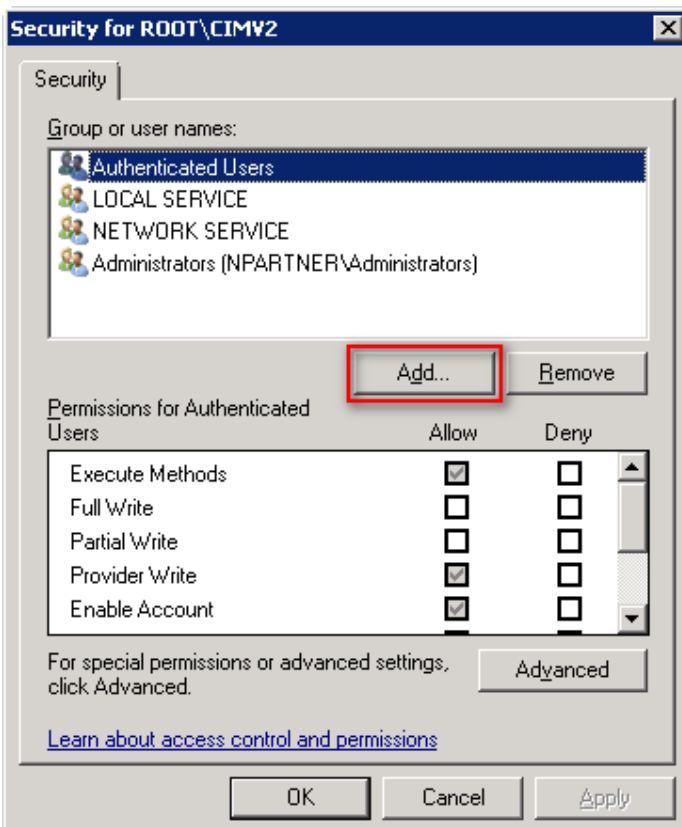
(4) Edit CIMV2 Security

On the “Security” tab, expand folder “Root” -> “CIMV2,” then click “Security.”



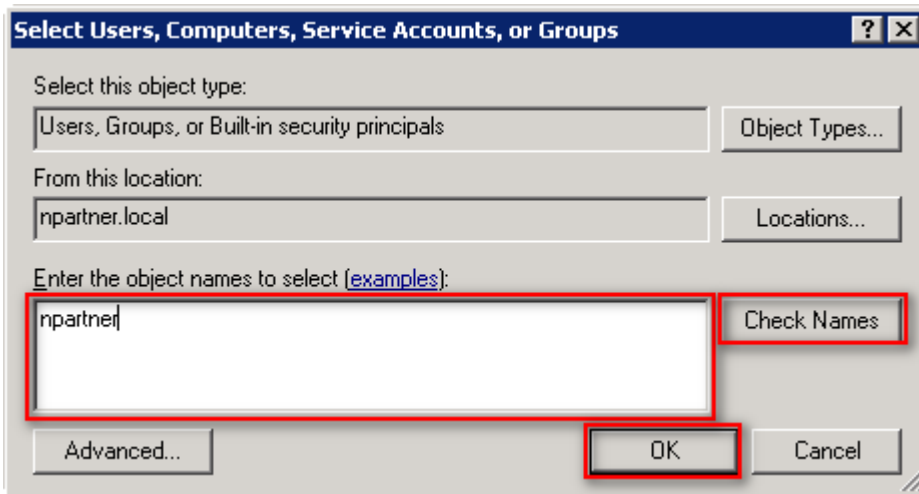
(5) Add WMI User Permissions

Click “Add.”



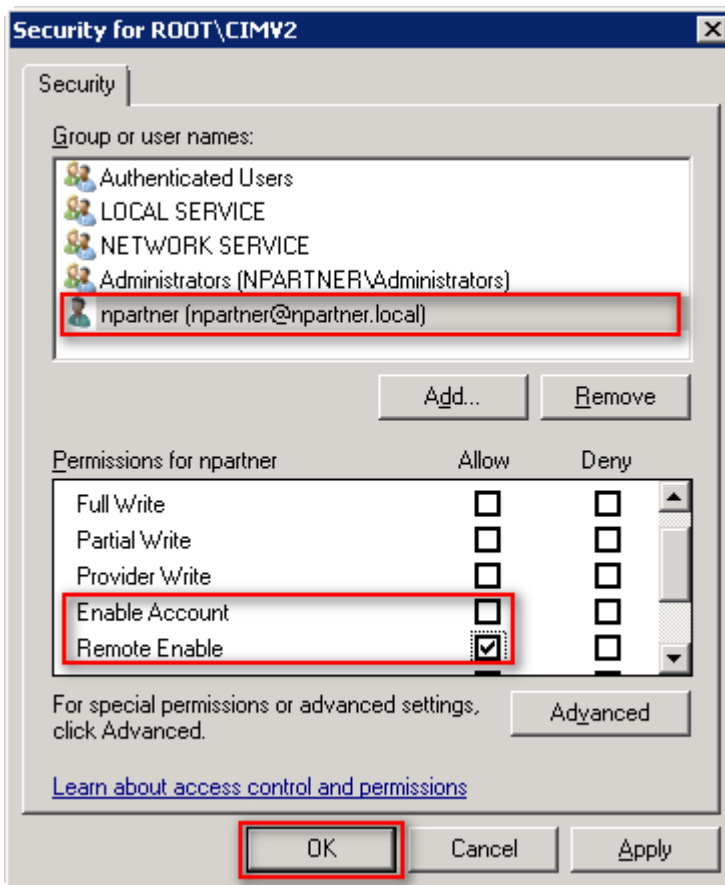
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”

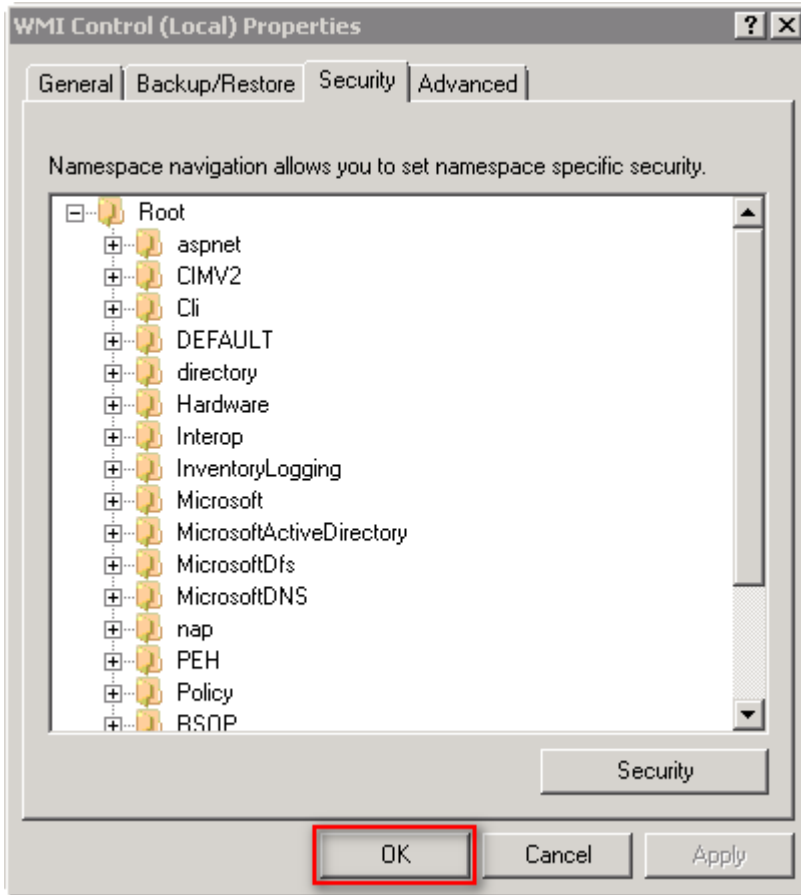


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Click "OK."



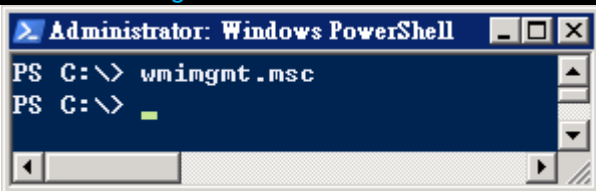
3.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”



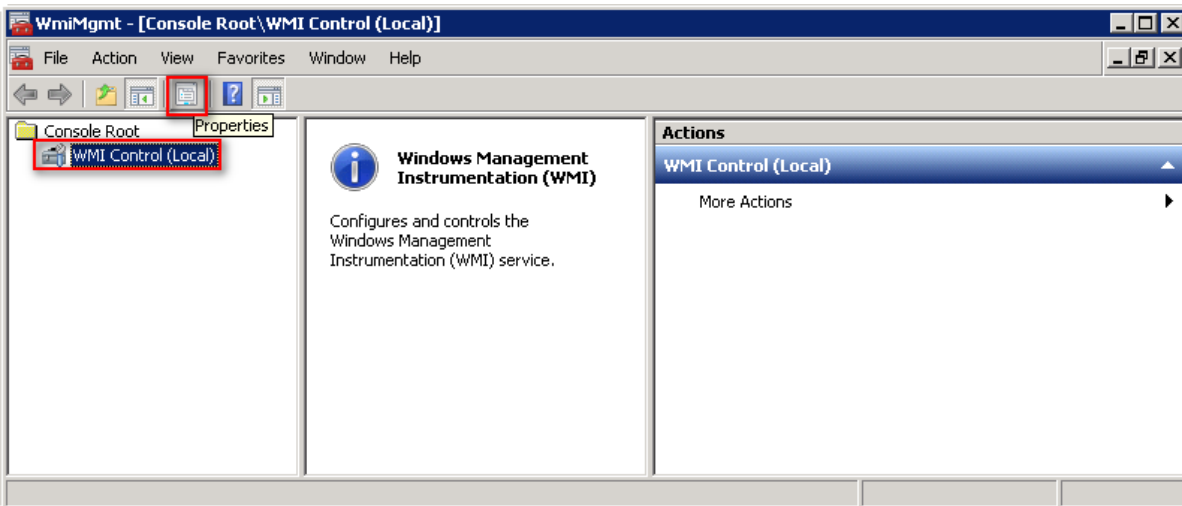
(2) Enter the command below to open component services.

```
PS C:\> wmicgmt.msc
```



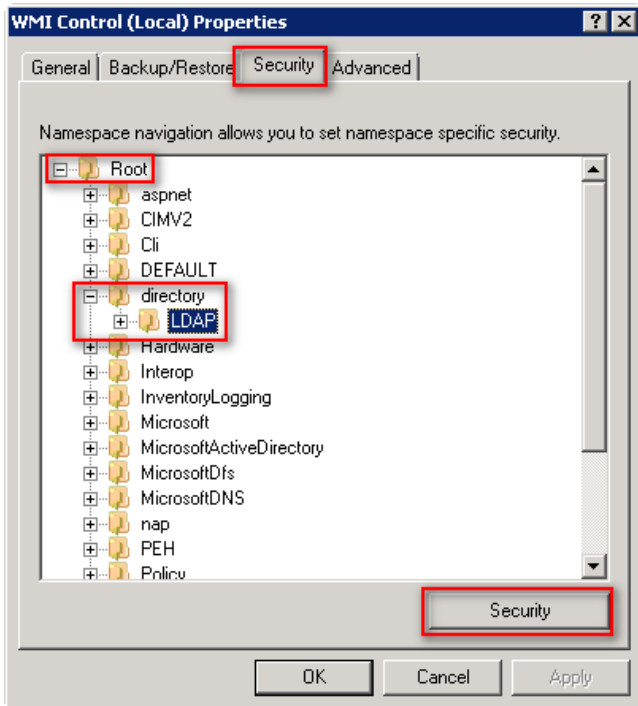
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select  (Properties).



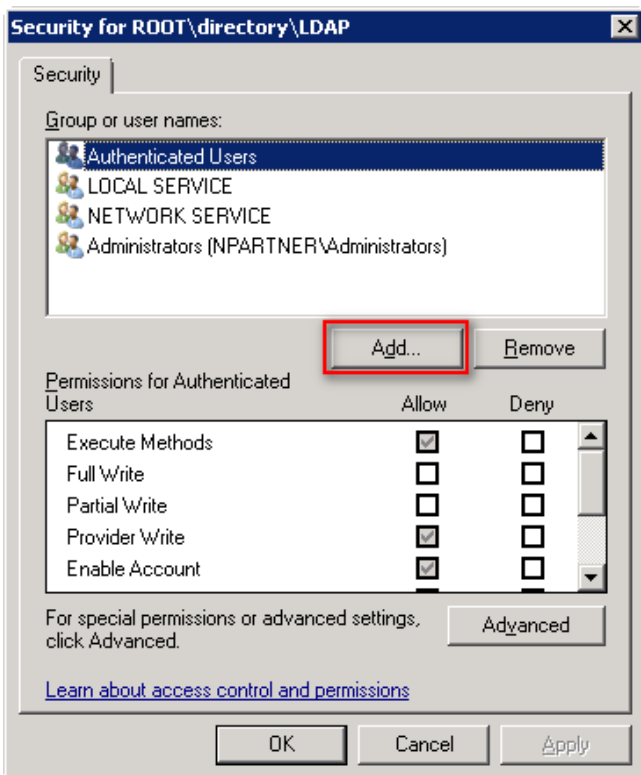
(4) Edit LDAP Security

On the "Security" tab, expand "Root"-> "directory" -> "LDAP," then click "Security."



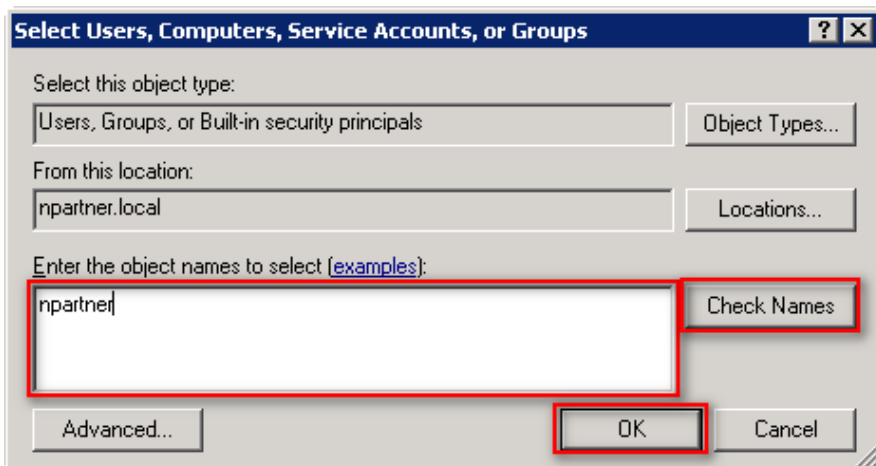
(5) Add WMI User Permissions

Click "Add."



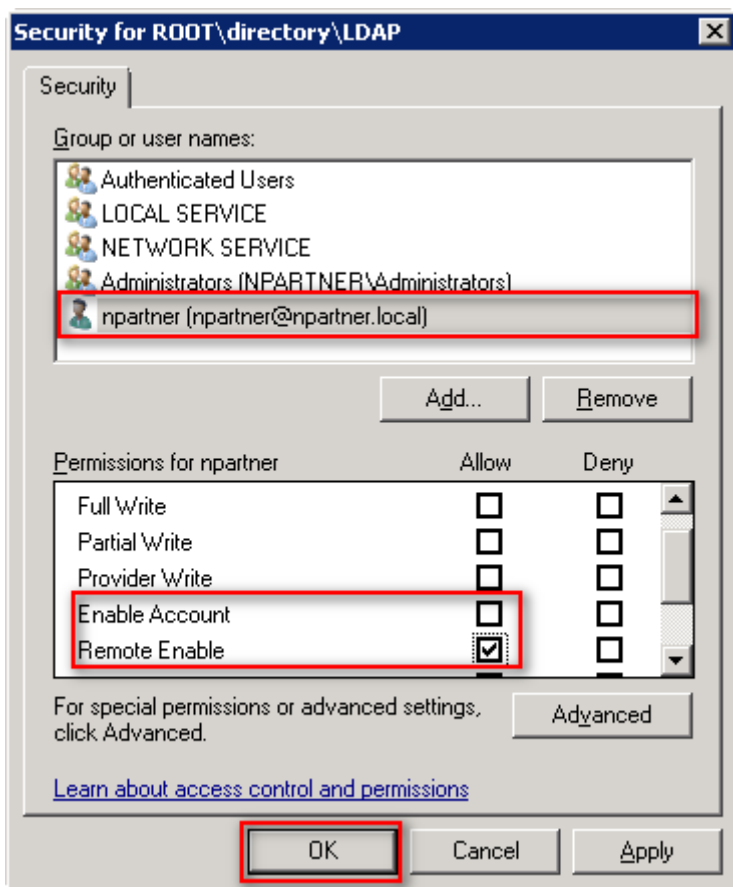
(6) Enter Your Username

Input your user account name (in this example, it is “npartner”), click “Check Names,” then click “OK.”

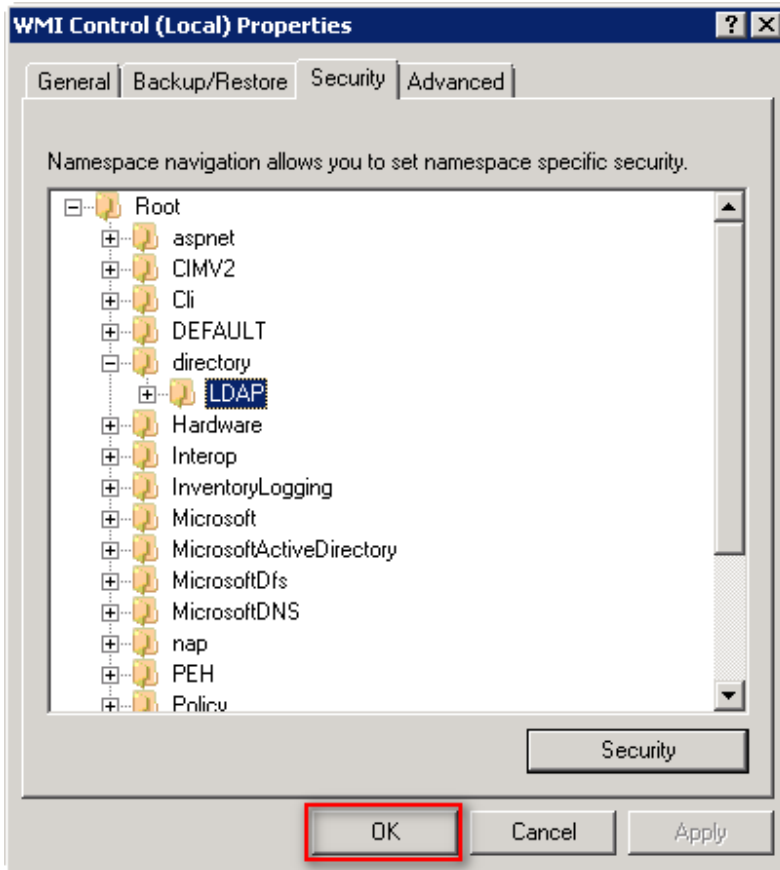


(7) Set Your User Permissions

Select your user account (in this example, it is “npartner”), **uncheck** “Enable Account: Allow,” **check** “Remote Enable: Allow,” then click “OK.”

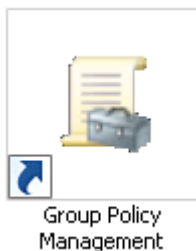


(8) Click "OK."



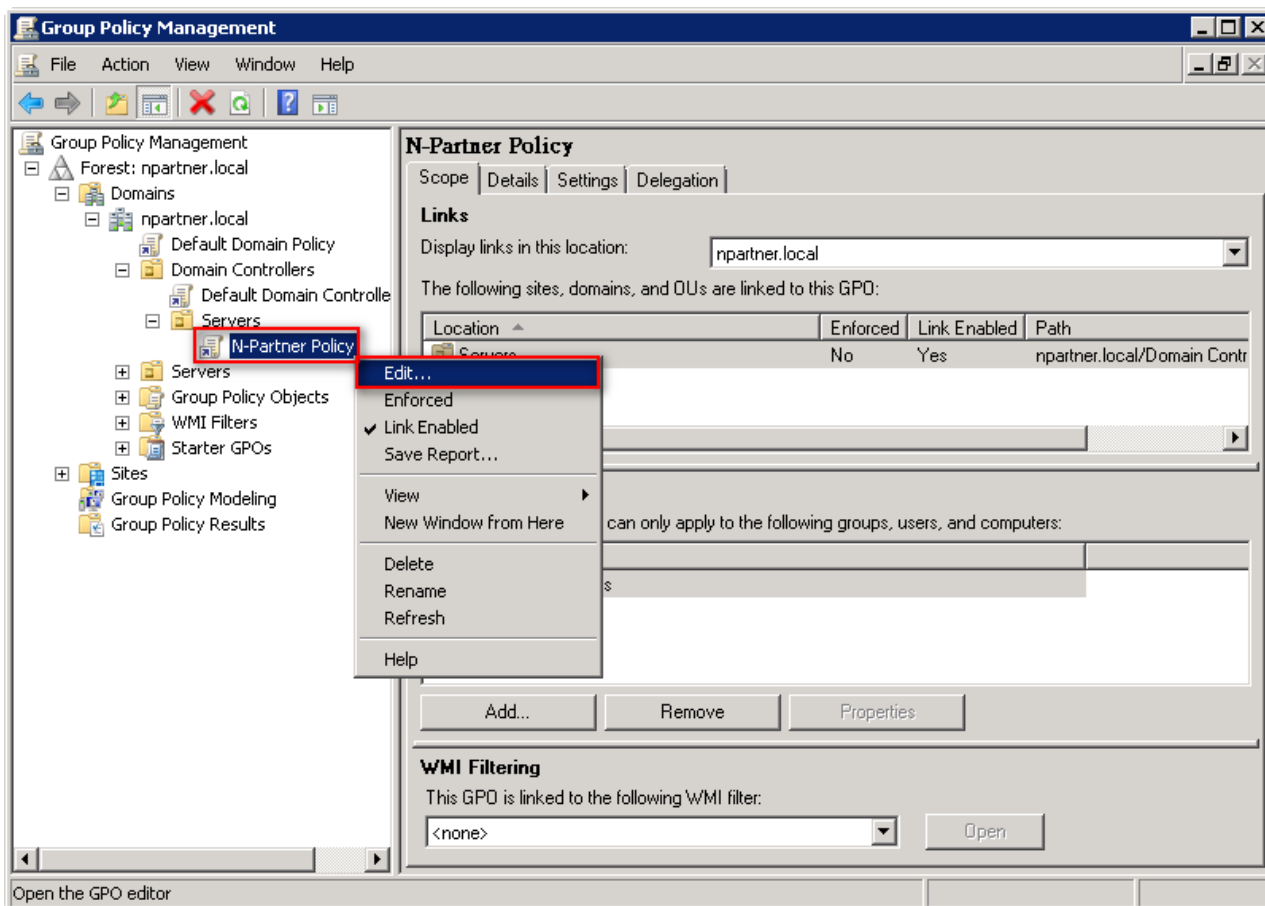
3.3.4 Configure Event Log read permissions

(1) Open Group Policy Management



(2) Edit the Group Policy Object

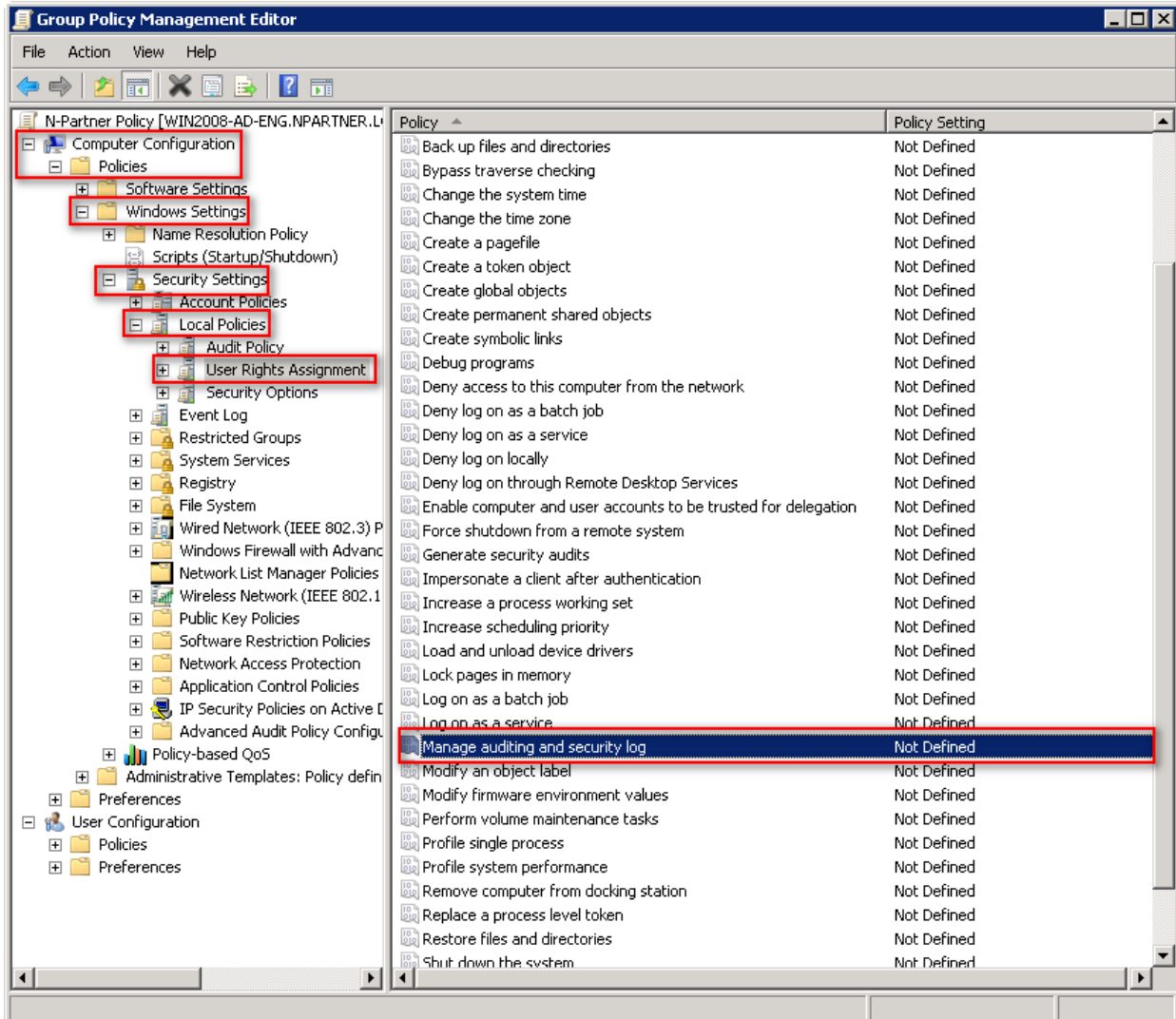
In the “N-Partner Policy” Group Policy Object, right-click and select “Edit.”



(3) Configure Log Settings

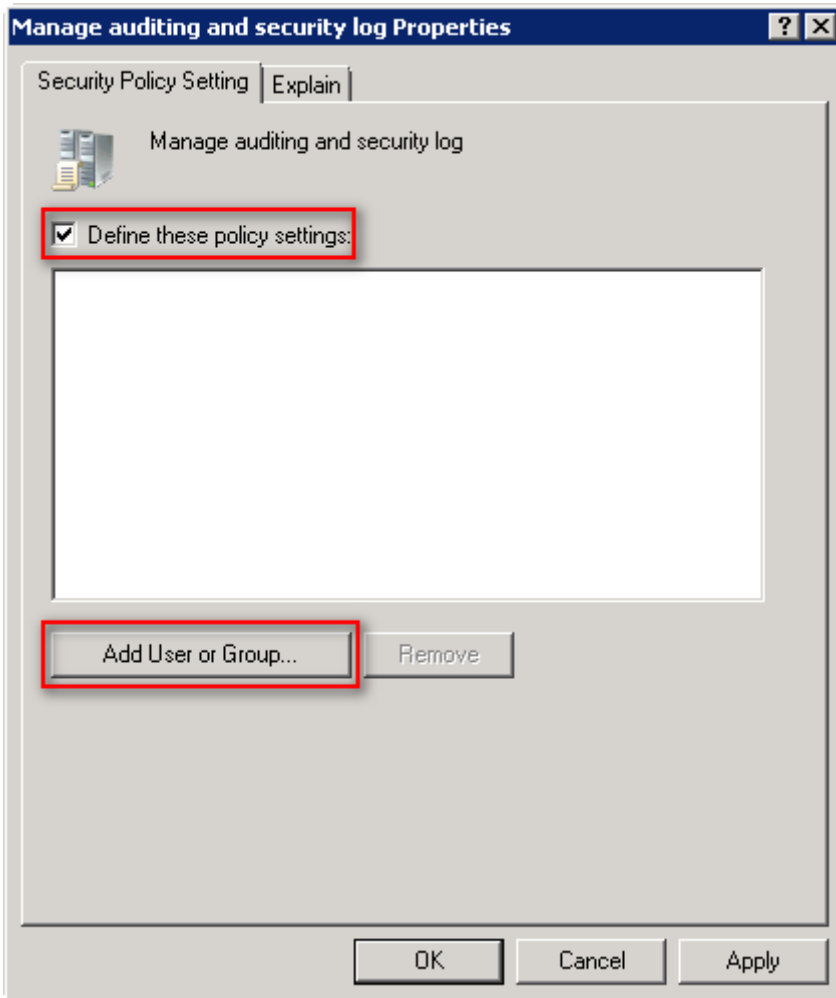
Click “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

Select “Manage auditing and security log,” then click “Properties.”



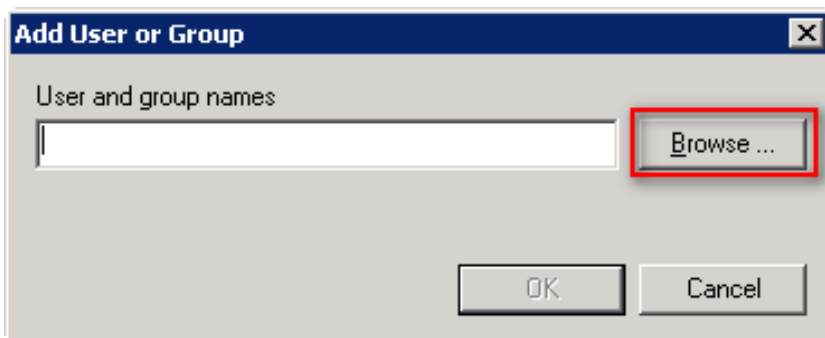
(4) Add Audit Management User

Check “Define these policy settings,” then click “Add User or Group...”.



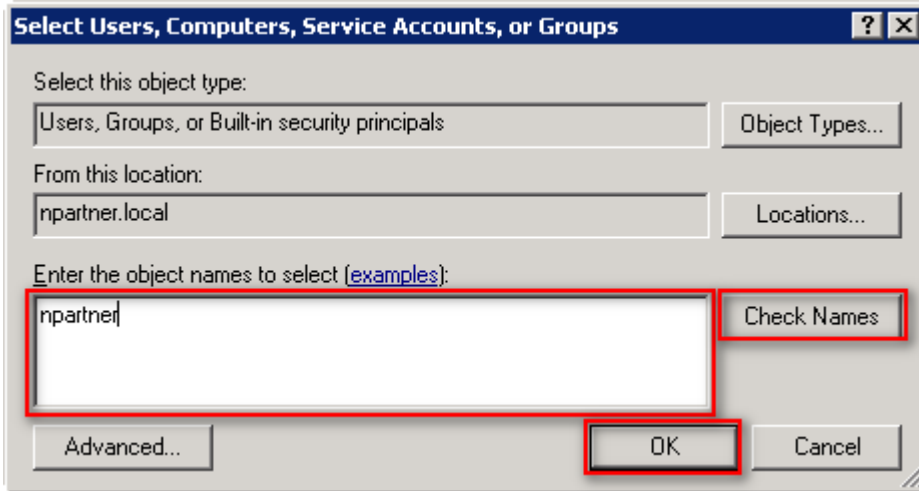
(5) Search for User

Click “Browse.”



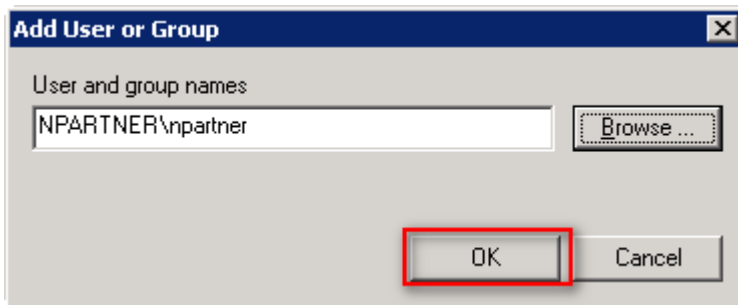
(6) Enter User

Enter the user account: npartner → click “Check Names” → click “OK.”



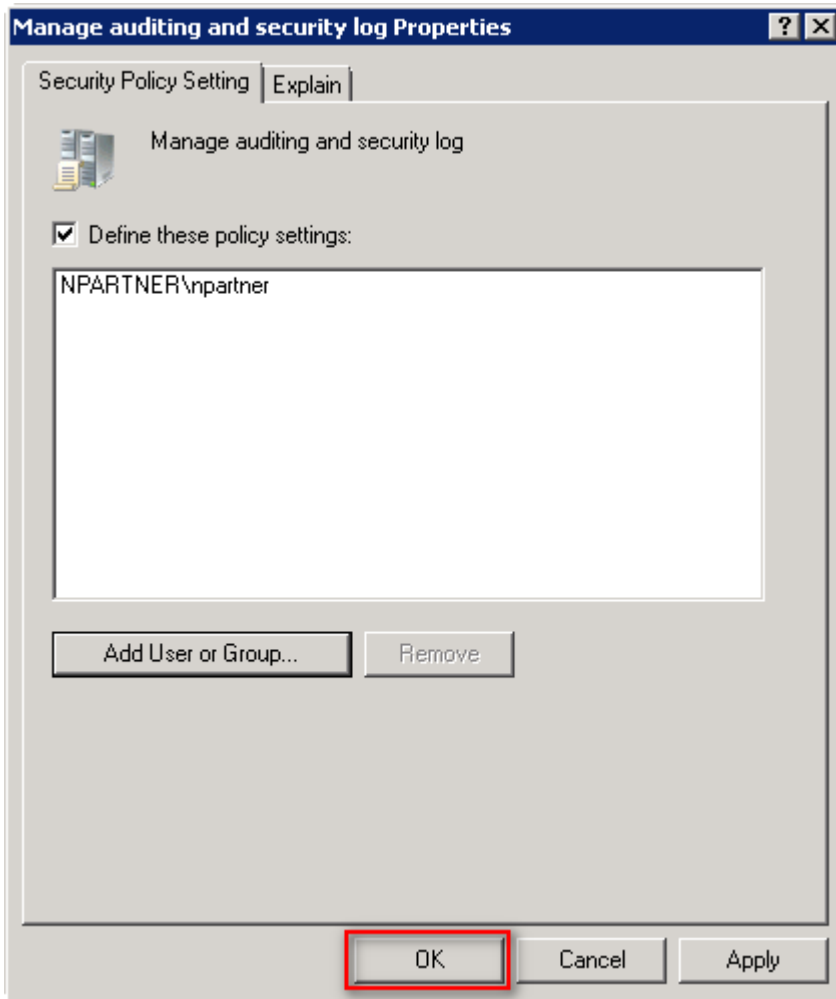
(7) Confirm User

Click “OK.”



(8) Confirm Log Settings

Click "OK."

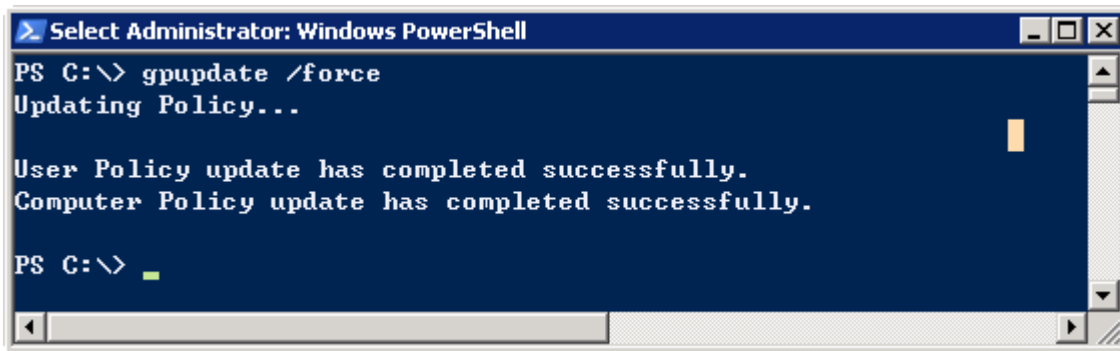


(9) Open "Windows PowerShell."



(10) Enter the command below to update group policy settings:

```
PS C:\> gpupdate /force
```



```
Select Administrator: Windows PowerShell
PS C:\> gpupdate /force
Updating Policy...

User Policy update has completed successfully.
Computer Policy update has completed successfully.

PS C:\> █
```

3.3.5 Restart WMI Service

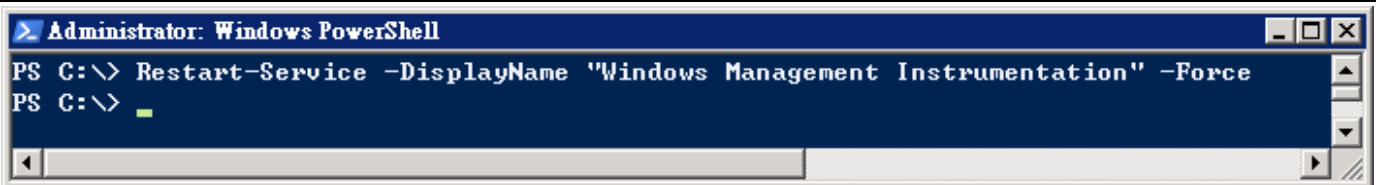
(1) Click “Windows PowerShell.”



(2) Restart WMI Service

Run the following command to restart the WMI service:

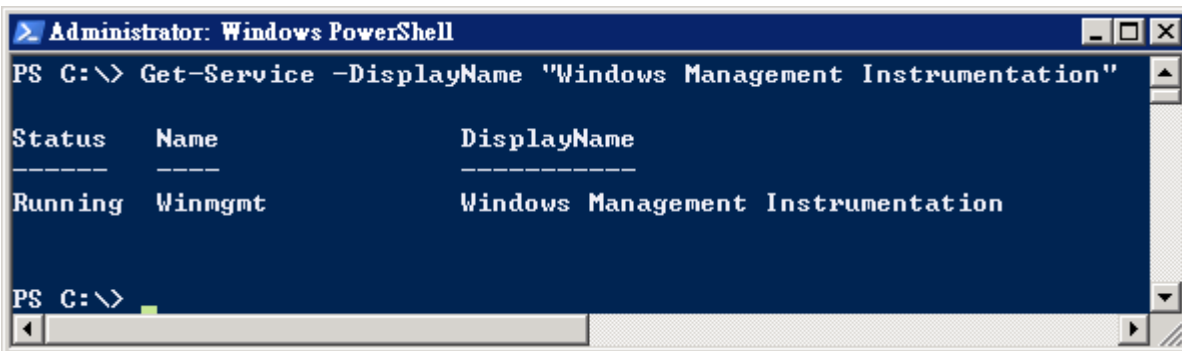
```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) Check WMI Service Status

Verify the status of the WMI service:

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



3.4 Configure Firewall

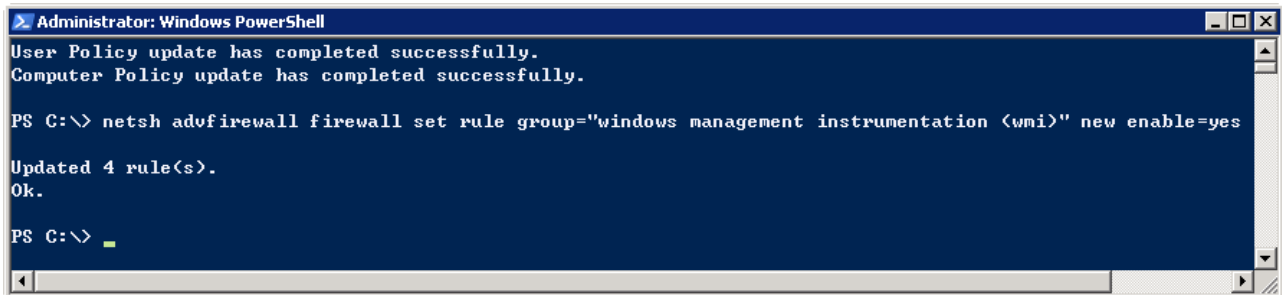
(1) Open "Windows PowerShell."



(2) Allow WMI Through the Firewall

Enable the Windows Management Instrumentation (WMI) firewall rule group:

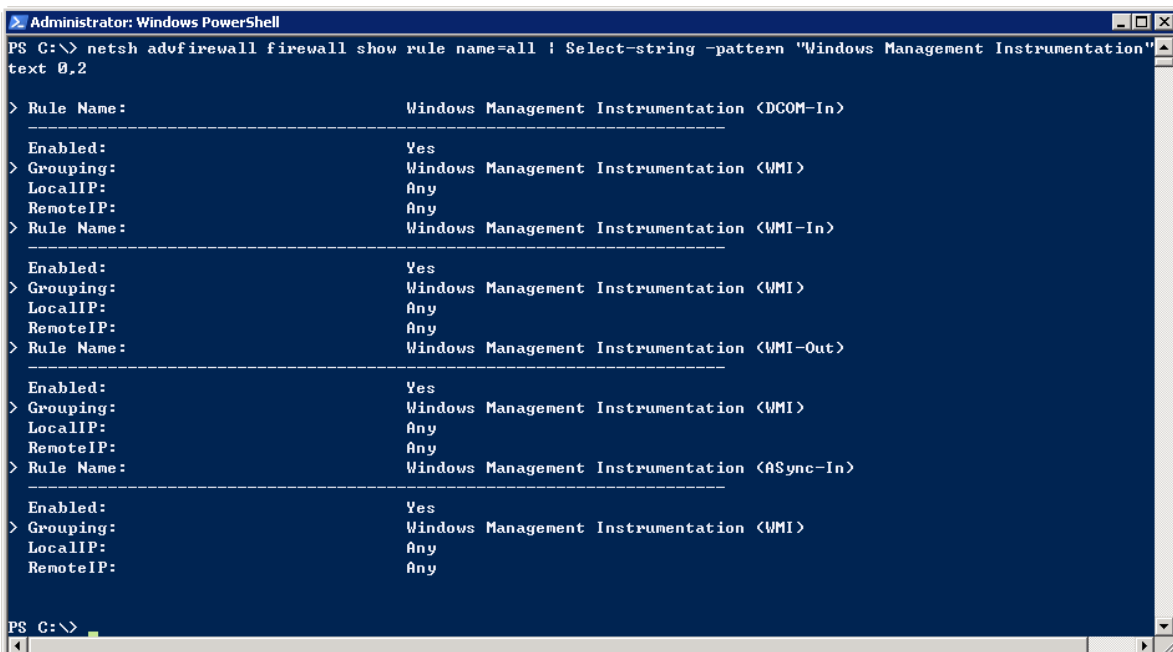
```
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```



(3) Check WMI Firewall Rule Status

View the current WMI firewall rule status:

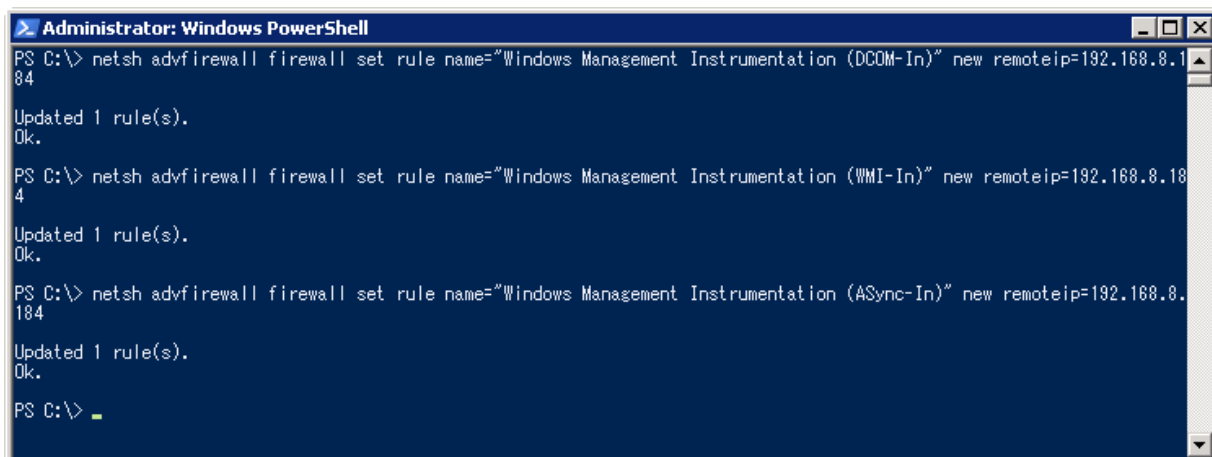
```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```



(4) Configure Firewall to Allow Only N-Reporter IP to Query WMI

Restrict WMI access so that only the N-Reporter IP address is allowed:

```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)"
new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new
remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)"
new remoteip=192.168.8.184
```



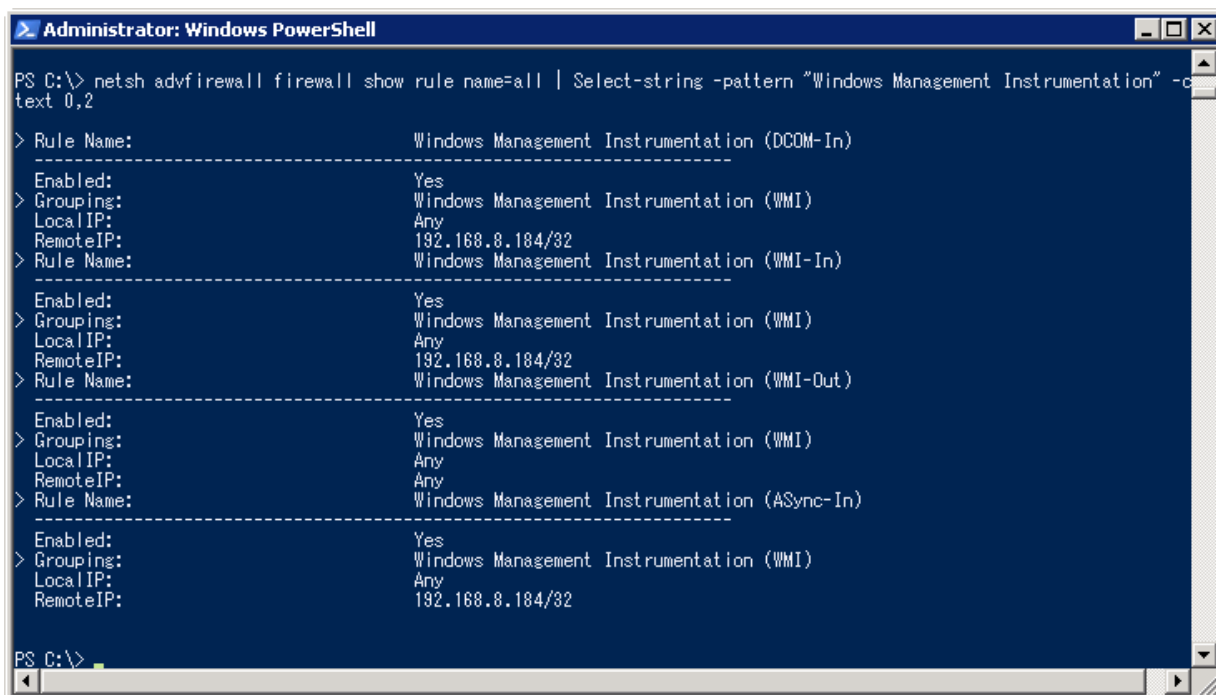
```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
Updated 1 rule(s).
Ok.
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
Updated 1 rule(s).
Ok.
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)" new remoteip=192.168.8.184
Updated 1 rule(s).
Ok.
PS C:\> _
```

Note: Replace the IP address in red text with the N-Reporter IP address.

(5) Check WMI Firewall Configuration Status

Verify the updated WMI firewall rule settings:

```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management
Instrumentation" -context 0,2
```



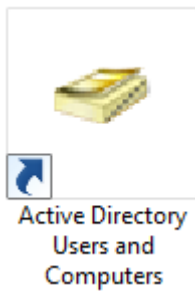
```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -c
text 0,2
> Rule Name: Windows Management Instrumentation (DCOM-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
LocalIP: Any
RemoteIP: 192.168.8.184/32
> Rule Name: Windows Management Instrumentation (WMI-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
LocalIP: Any
RemoteIP: 192.168.8.184/32
> Rule Name: Windows Management Instrumentation (WMI-Out)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
LocalIP: Any
RemoteIP: 192.168.8.184/32
> Rule Name: Windows Management Instrumentation (ASync-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
LocalIP: Any
RemoteIP: 192.168.8.184/32
PS C:\> _
```

4. Windows 2012

For detailed information on setting Windows audit policies, please refer to the “audit policy recommendations link” in the preface.

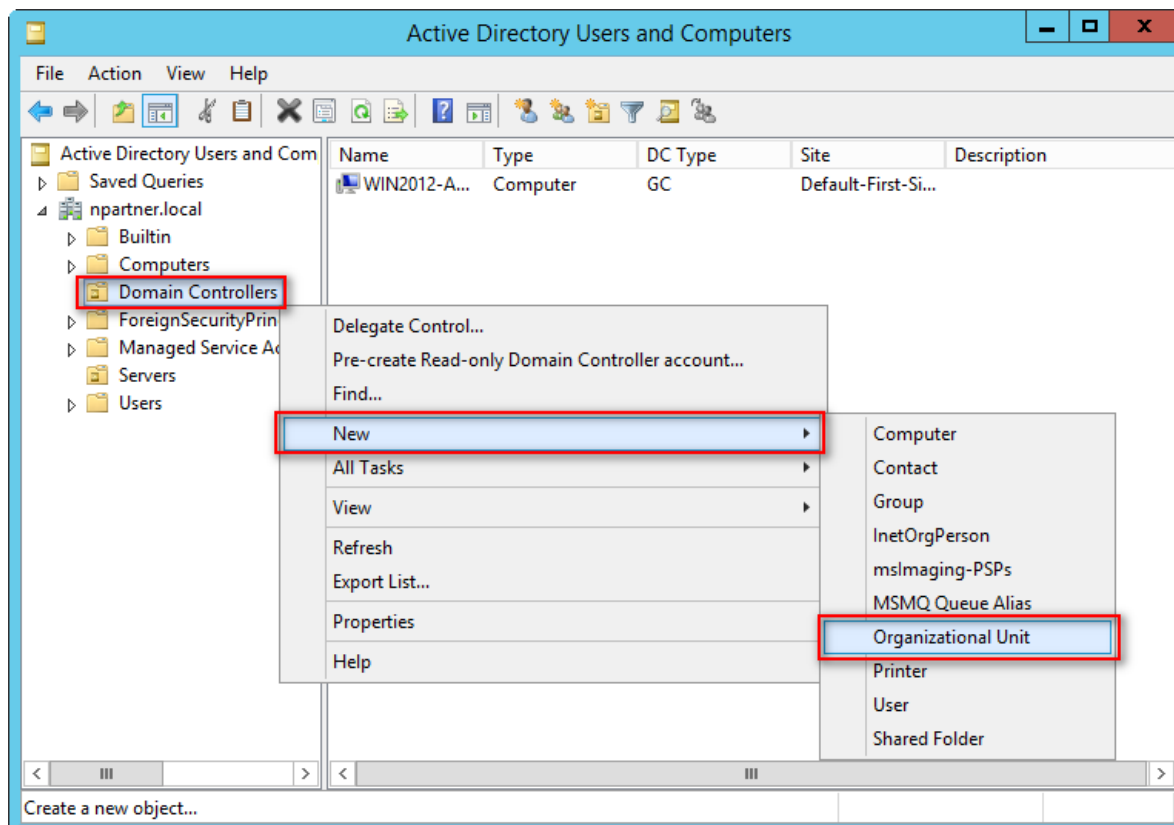
4.1 Organizational Unit Settings

(1) Open “Active Directory Users and Computers.”



(2) Add an Organizational Unit

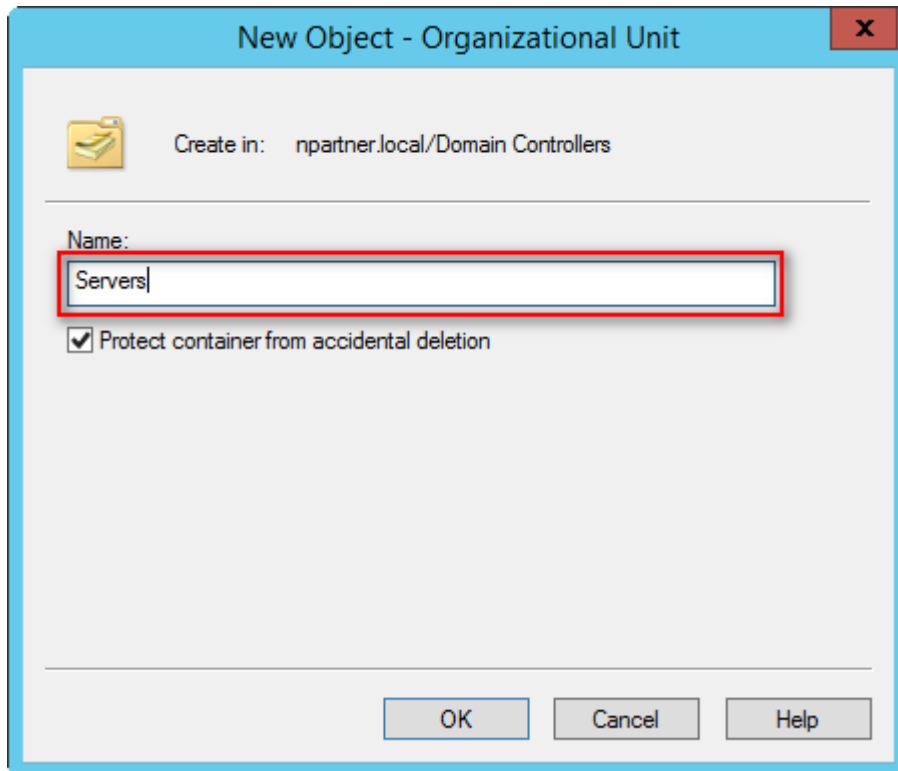
Right-click on “Domain Controllers,” select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit name according to the actual environment.

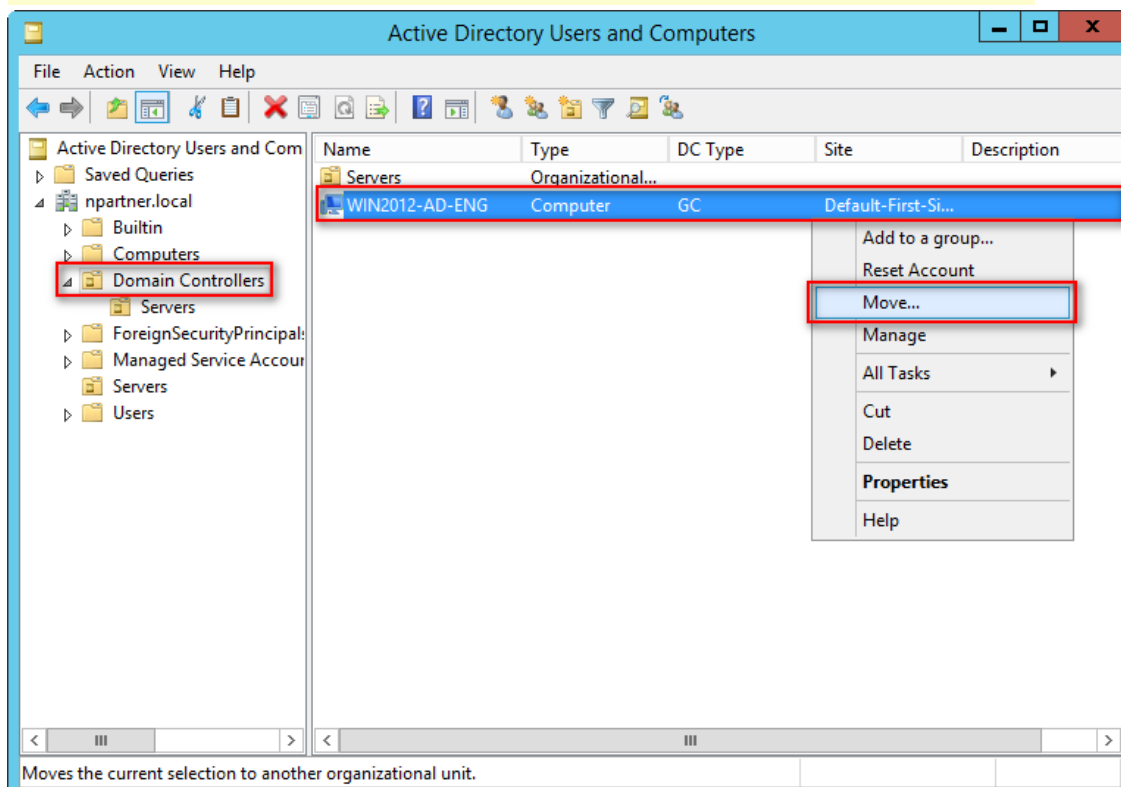
-> Click “OK.”



(4) Move the Server to your New Organizational Unit:

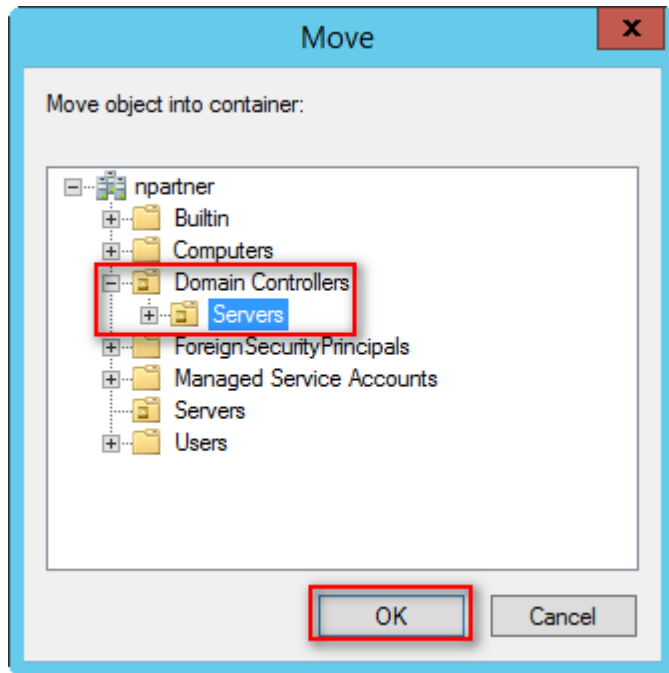
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2012-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



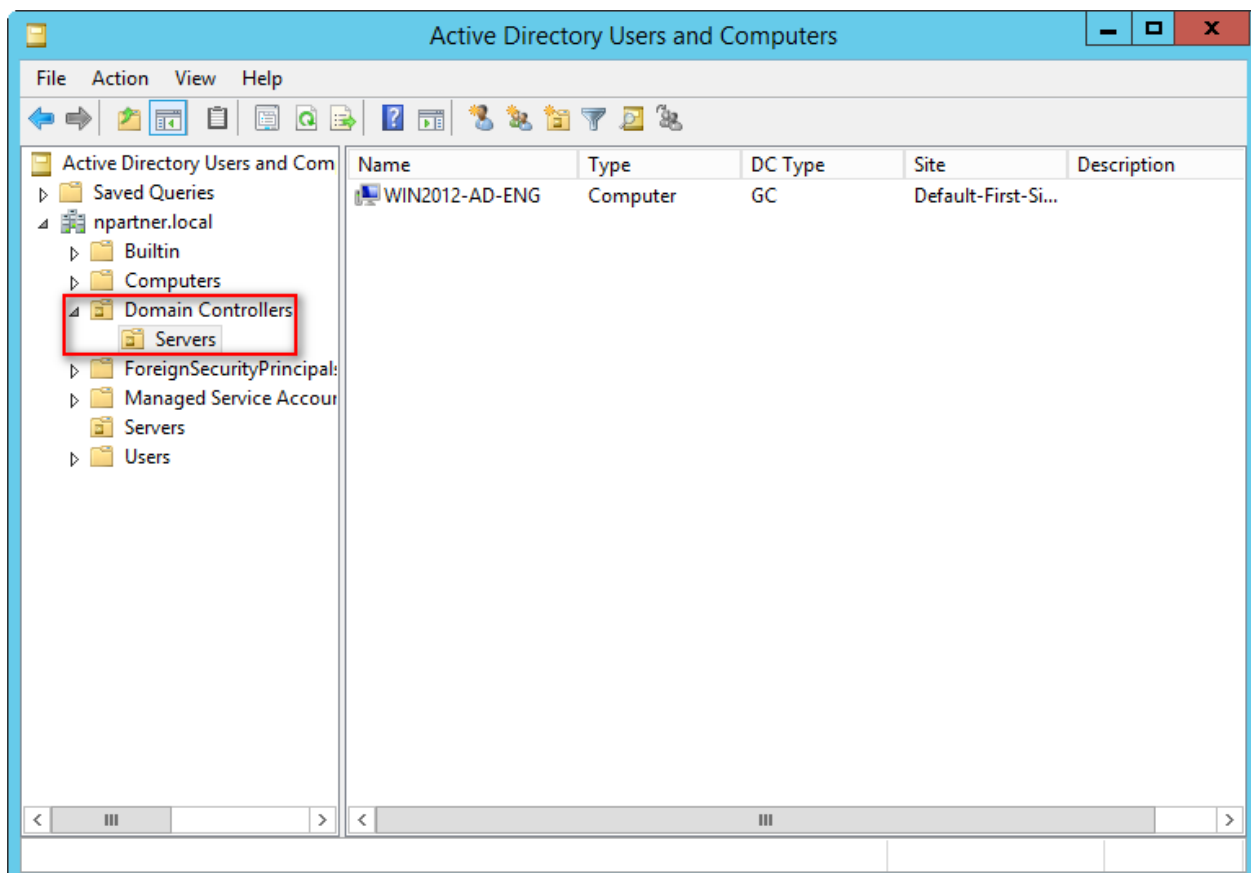
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



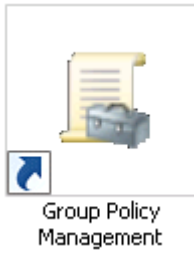
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2012-AD-ENG” server has been moved.

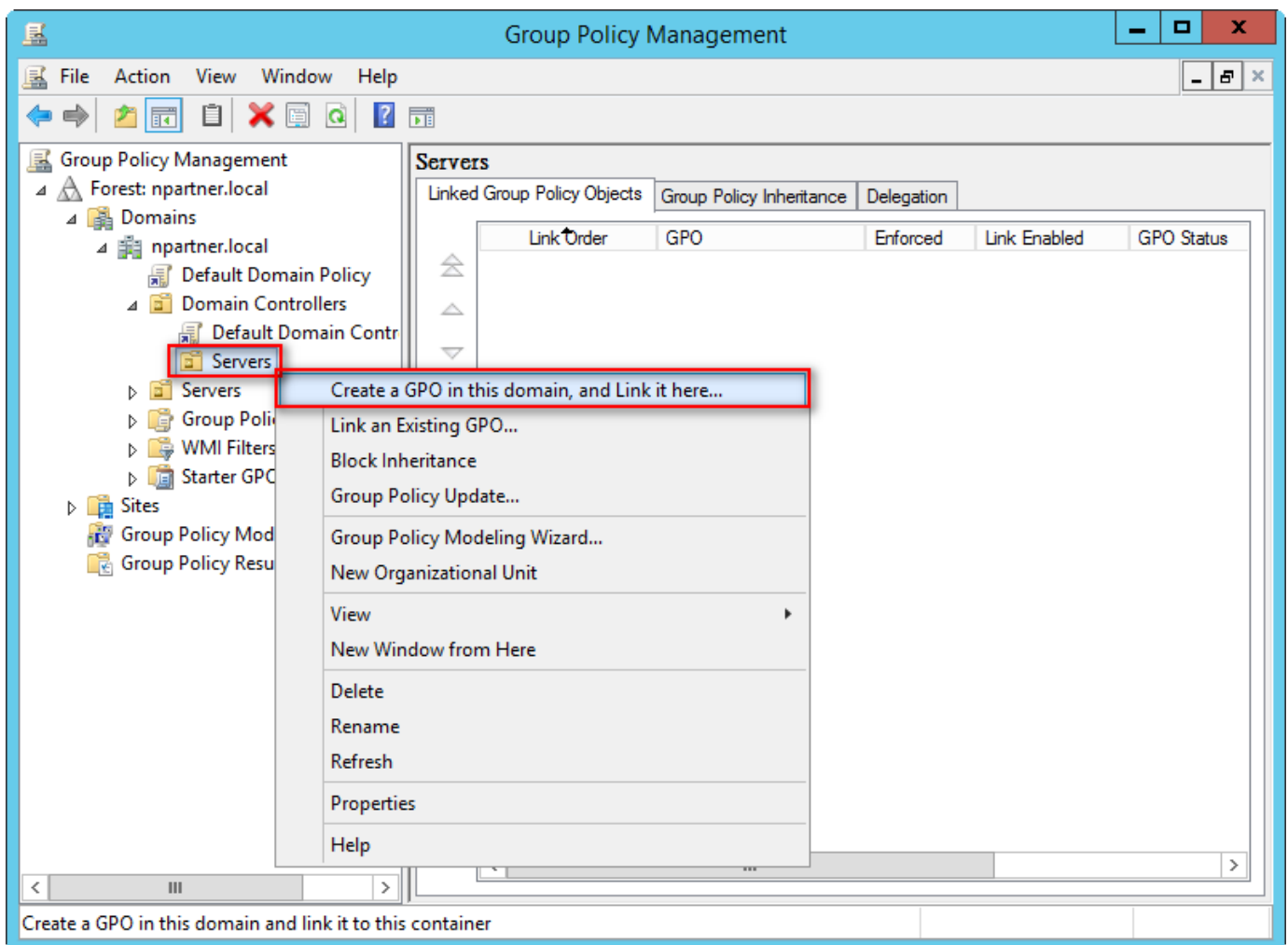


4.2 Group Policy Settings

(1) Click “Group Policy Management.”



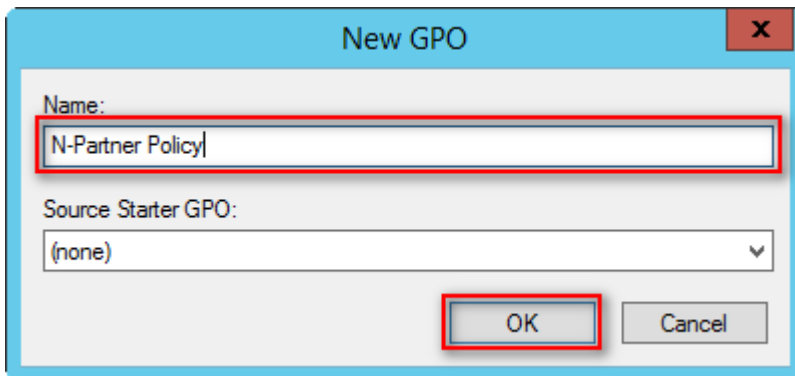
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(3) Enter your Group Policy Object Name

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

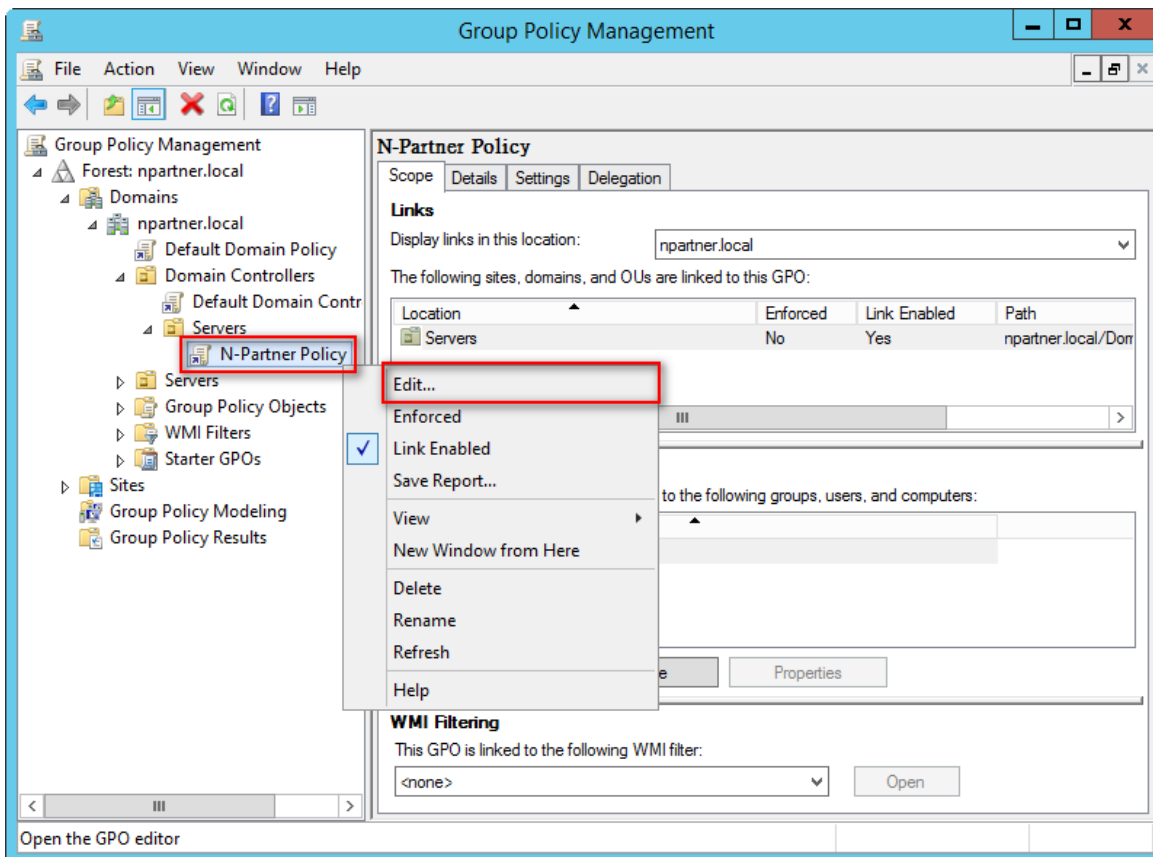
Note: Create your GPO name according to the client's environment. Then click “OK.”



(4) Edit your Group Policy Object

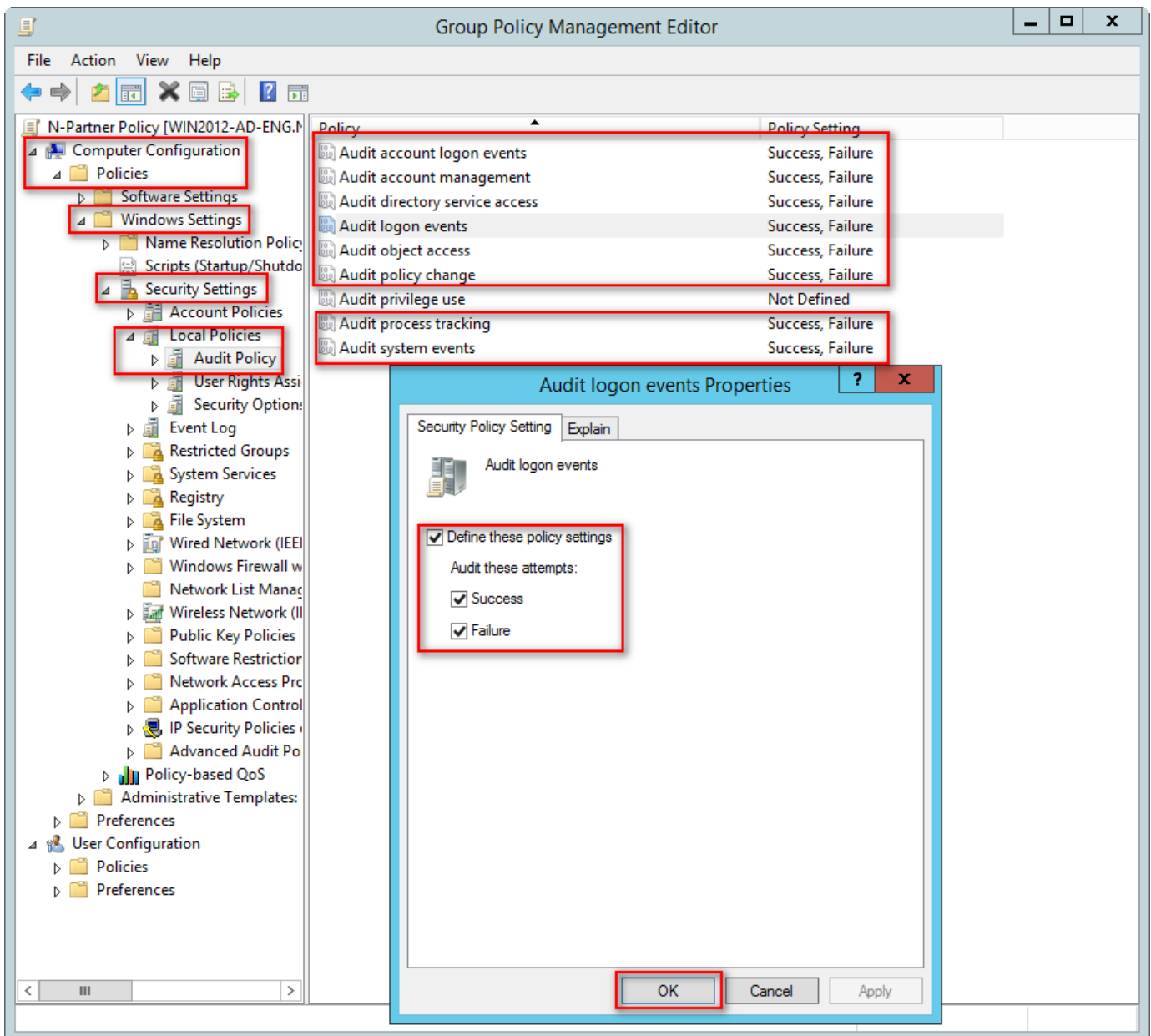
In your group policy object, (in this example, it is “N-Partner Policy”)

right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

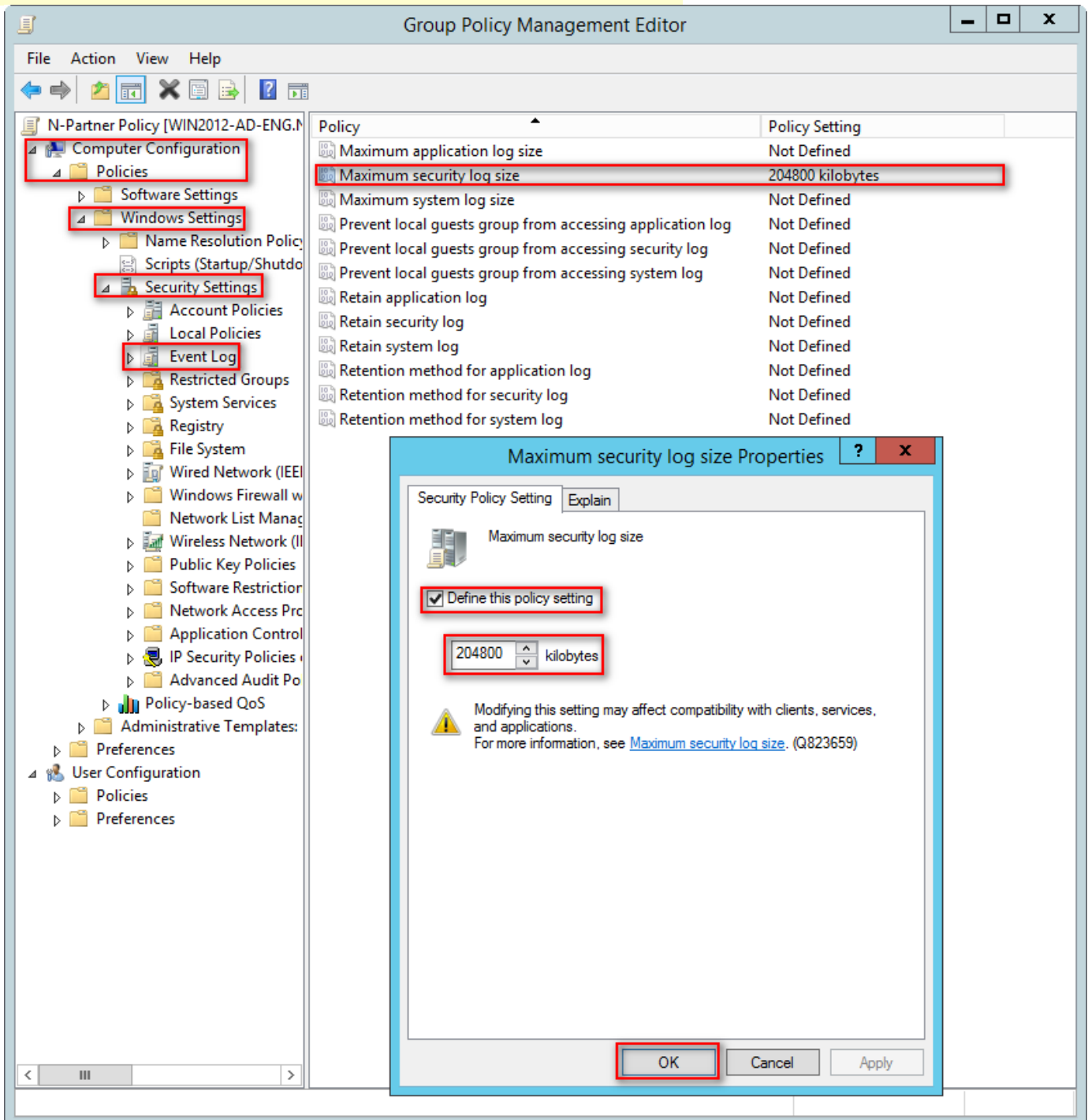
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Maximum Size of Security Log

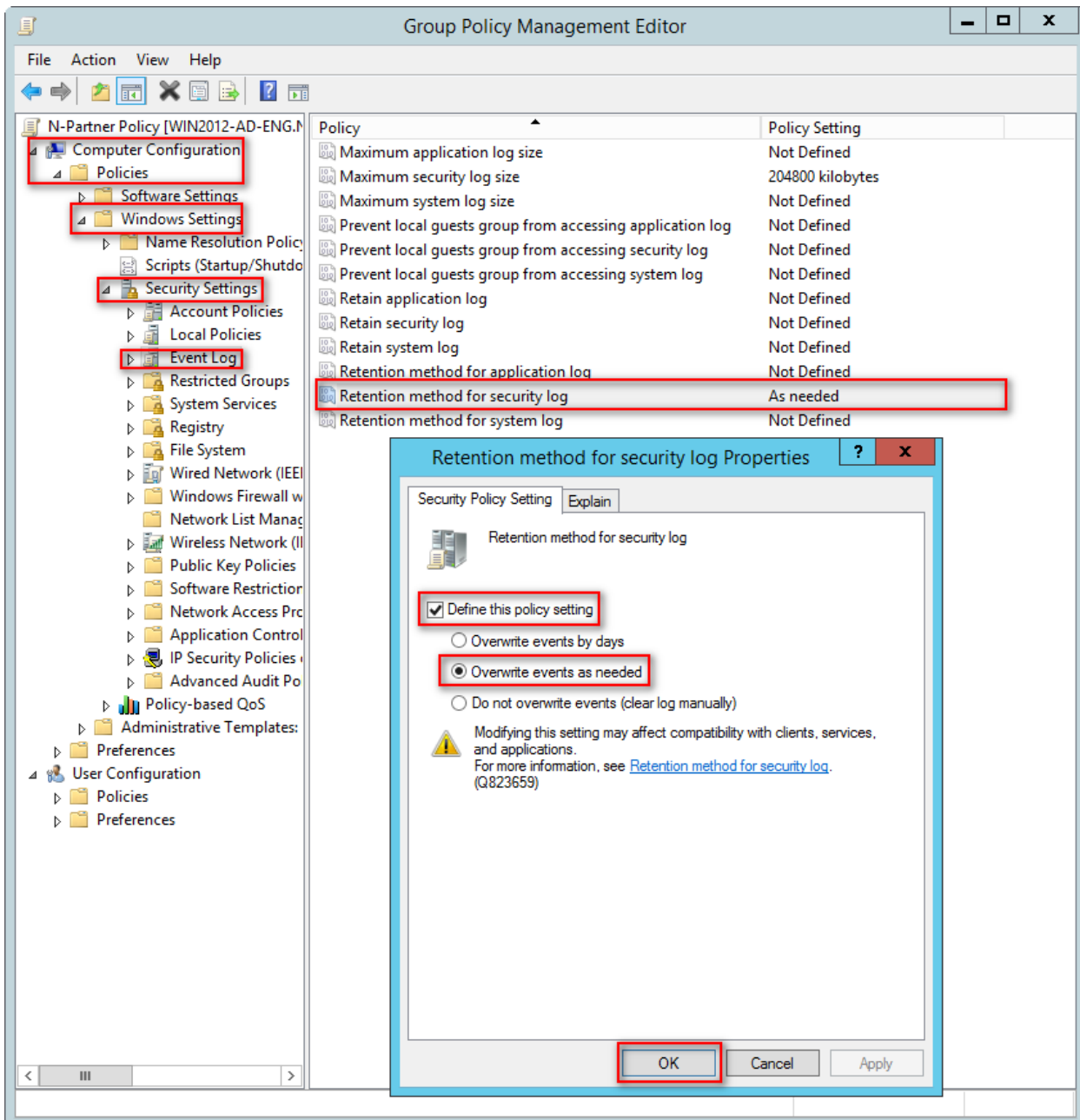
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click “OK.”



(7) Event Logs: Retention Method for Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”

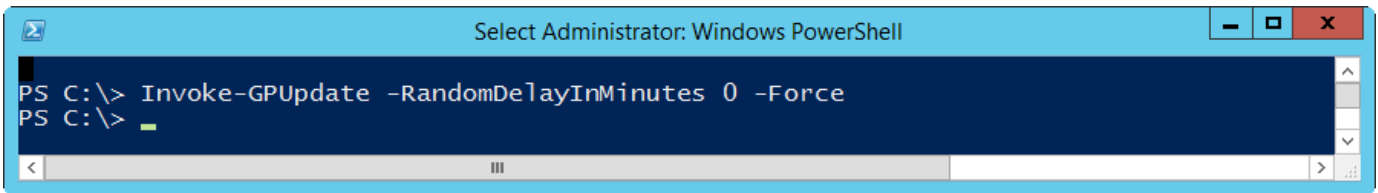


(8) Open “Windows PowerShell.”



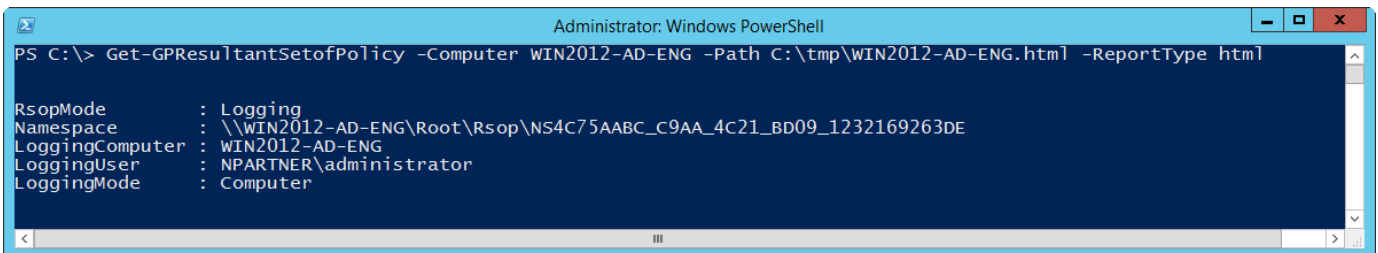
(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
```



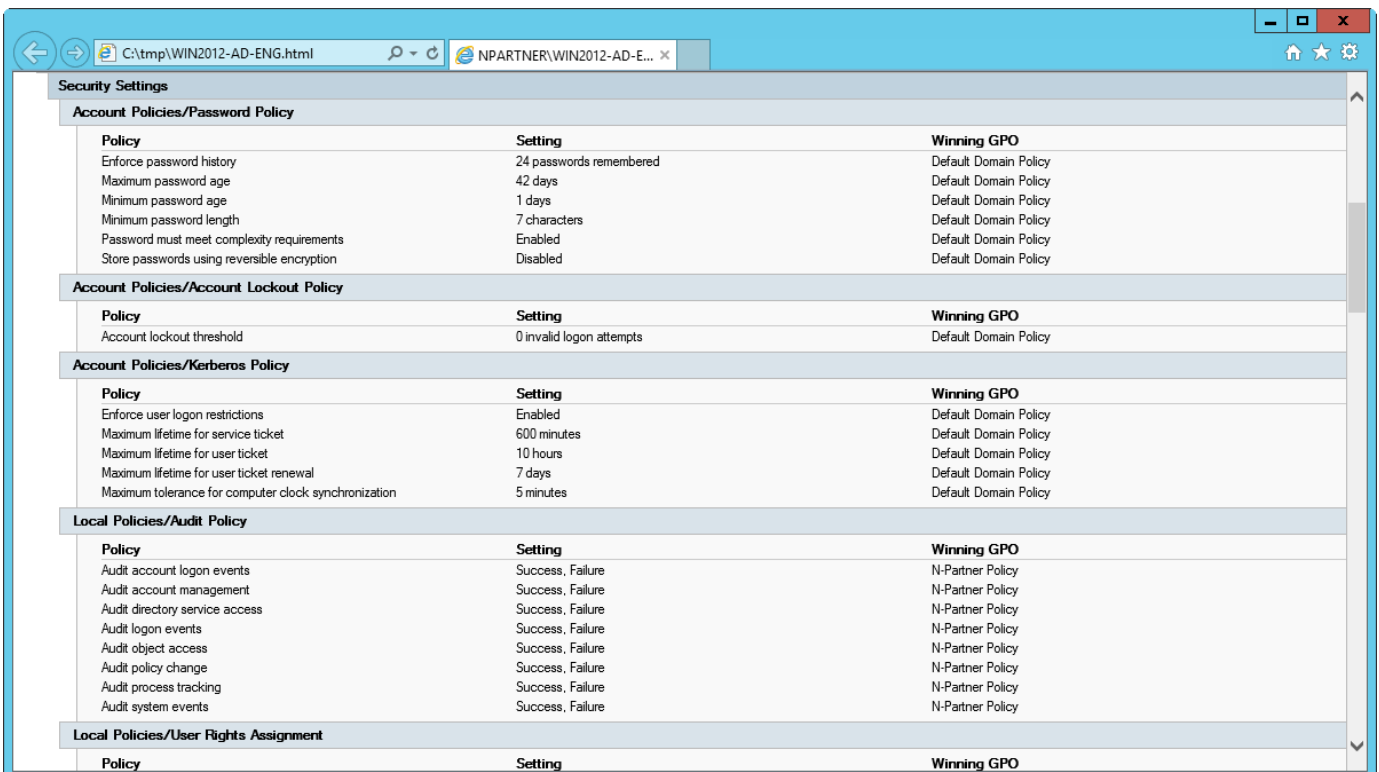
(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-AD-ENG -Path C:\tmp\WIN2012-AD-ENG.html -ReportType html
```



For the red text, please enter the Windows AD server name and the folder path/file name.

(11) Open the report and verify that the Windows AD server is applying the N-Partner Policy Group Policy.



4.3 Add a Non-Admin Account

4.3.1 Add Users

(1) Open "Windows PowerShell."



(2) Enter the command below to add a new account.

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command: `PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True`. The command is followed by a prompt `PS C:\> -`.

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command: `PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled`. The output is: `DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled : True
GivenName :
MemberOf : {}
Name : npartner
ObjectClass : user
ObjectGUID : 95571959-fad6-41d9-9e28-0ea76bd1d6f2
PasswordNeverExpires : True
SamAccountName : npartner
SID : S-1-5-21-634504633-3093900228-1641980093-1110
Surname :
UserPrincipalName : npartner@npartner.local`

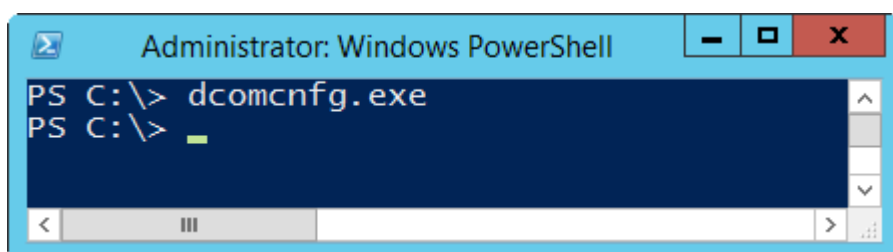
4.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”



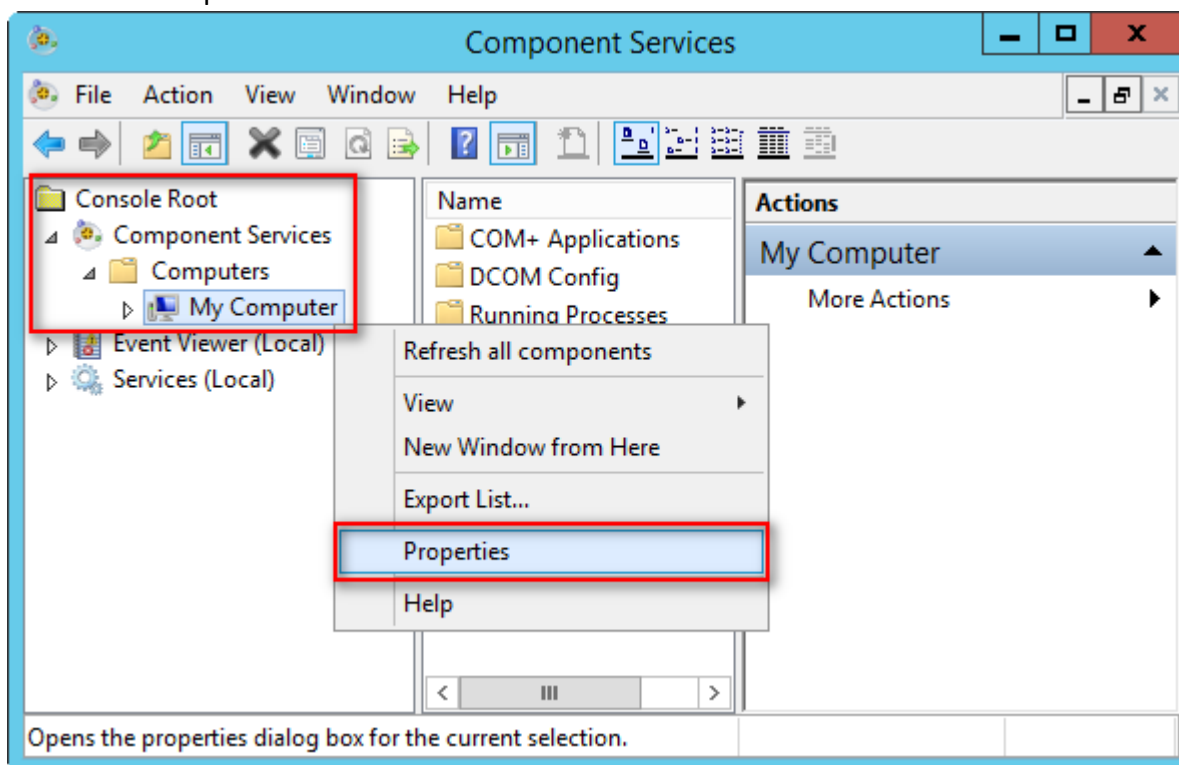
(2) Enter the command below to open component services.

```
PS C:\> dcomcnfg.exe
```



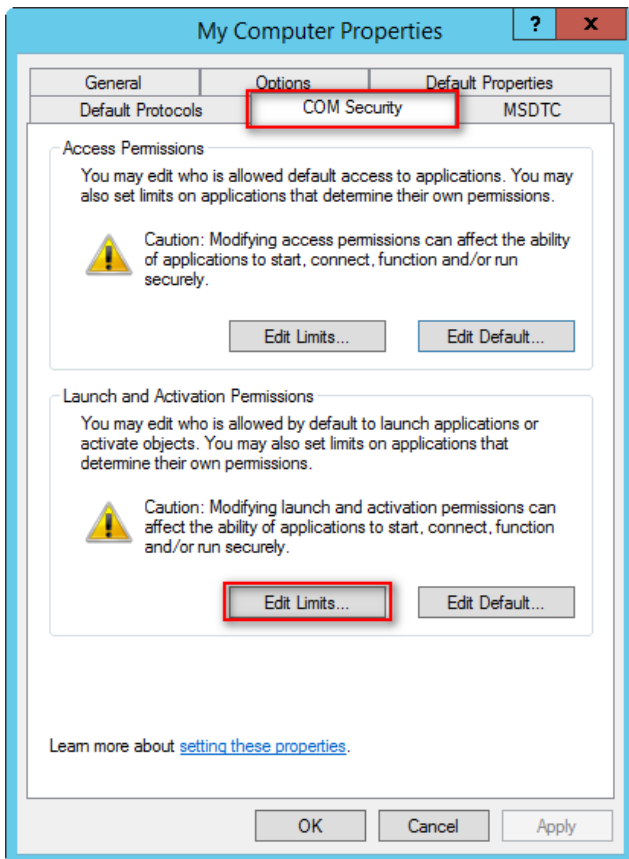
(3) Edit Computer Properties

Expand folder “Console Root” -> “Component Services” -> “Computers,” right-click on “My Computer,” and select “Properties.”



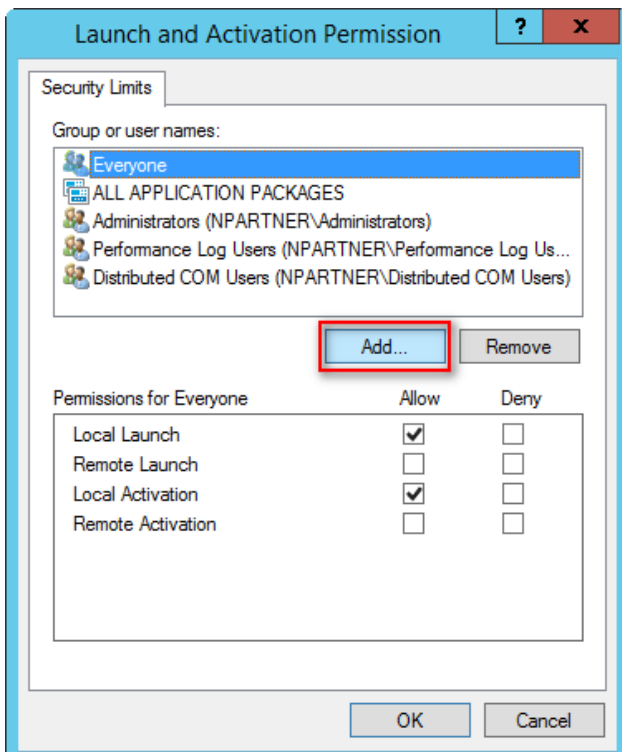
(4) Enable Permissions

Go to the “COM Security” tab, under Launch and Activation Permissions, click “Edit Limits.”



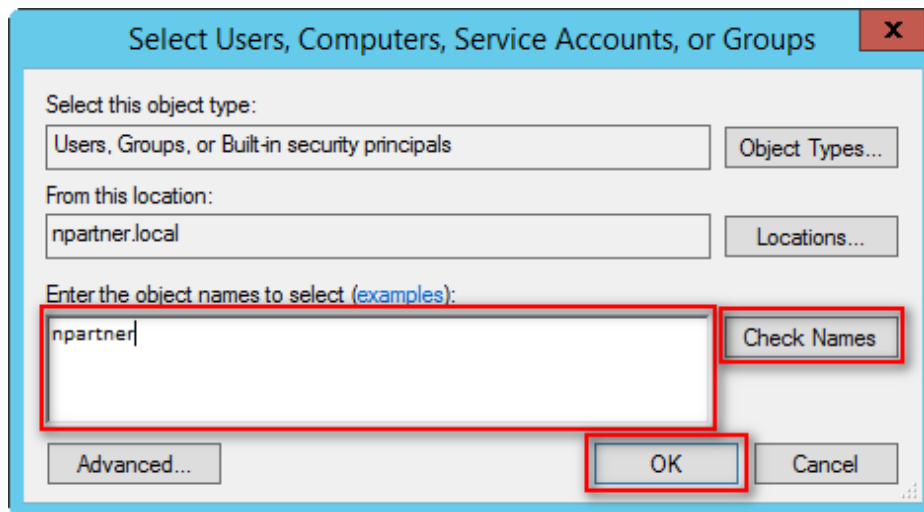
(5) Add DCOM User Permissions

Click “Add.”



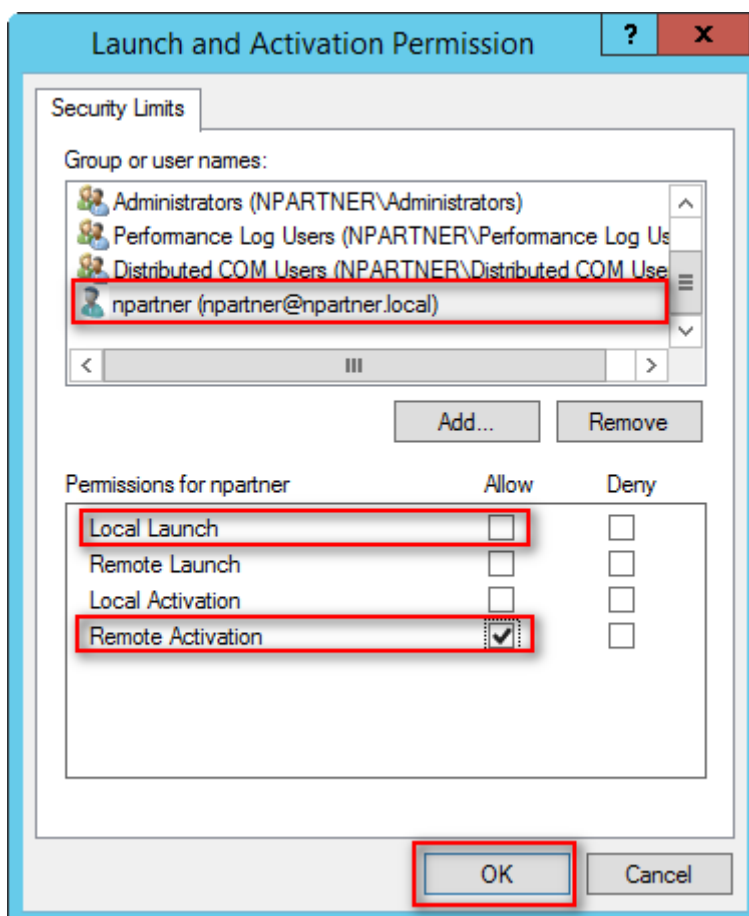
(6) Enter your Username

Input your user account: `npartner`, click “Check Names,” then click “OK.”

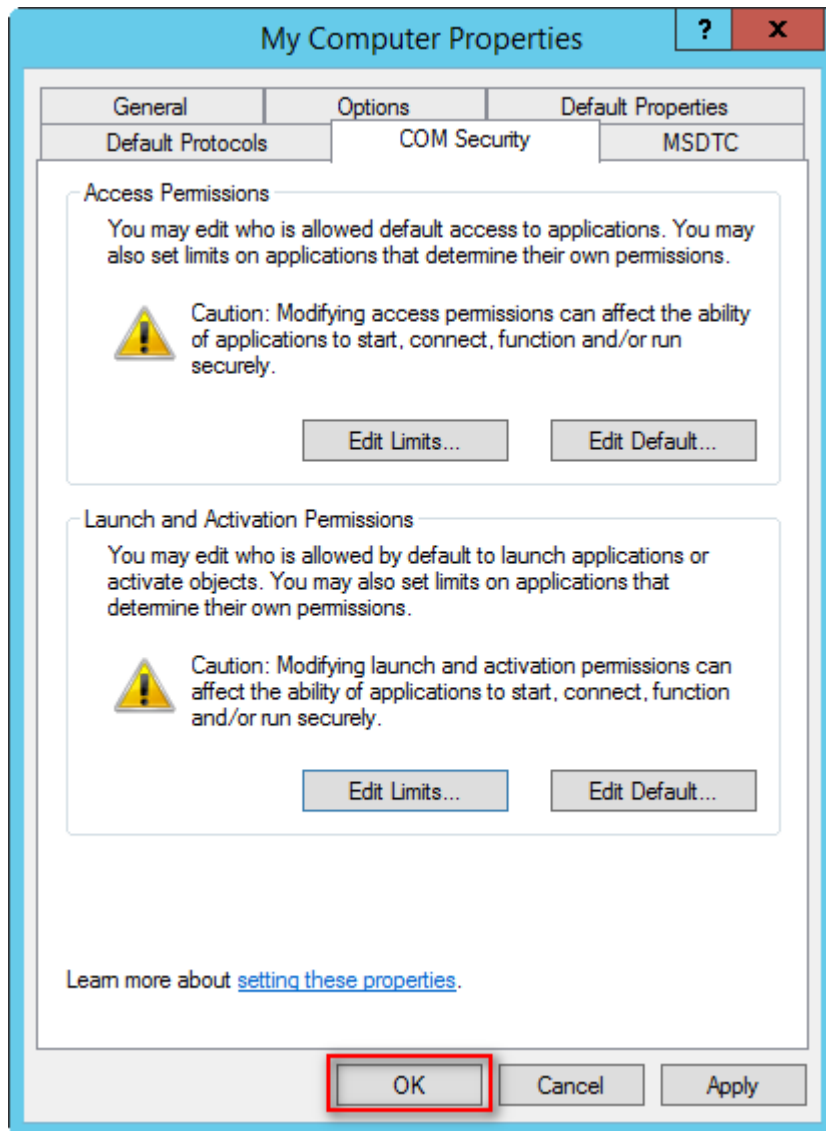


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Local Launch: Allow,” check “Remote Activation: Allow,” then click “OK.”



(8) Click "OK."



4.3.3 Configure WMI Permissions

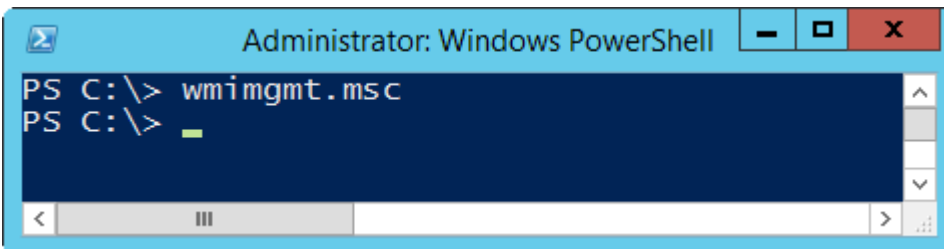
4.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”



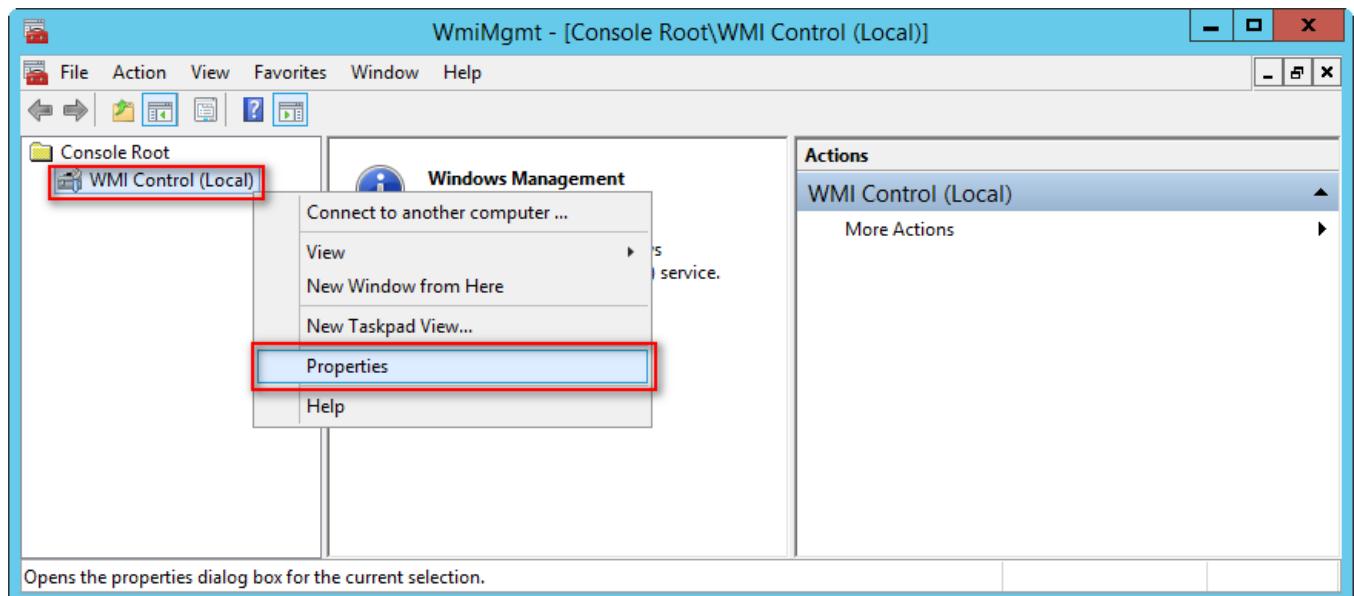
(2) Enter the command below to enable component services.

```
PS C:\> wmicmgmt.msc
```



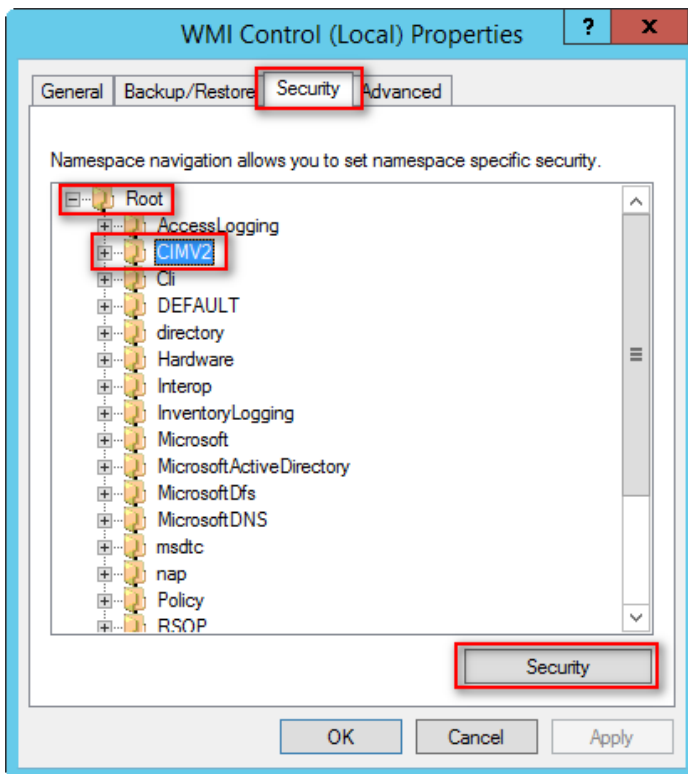
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



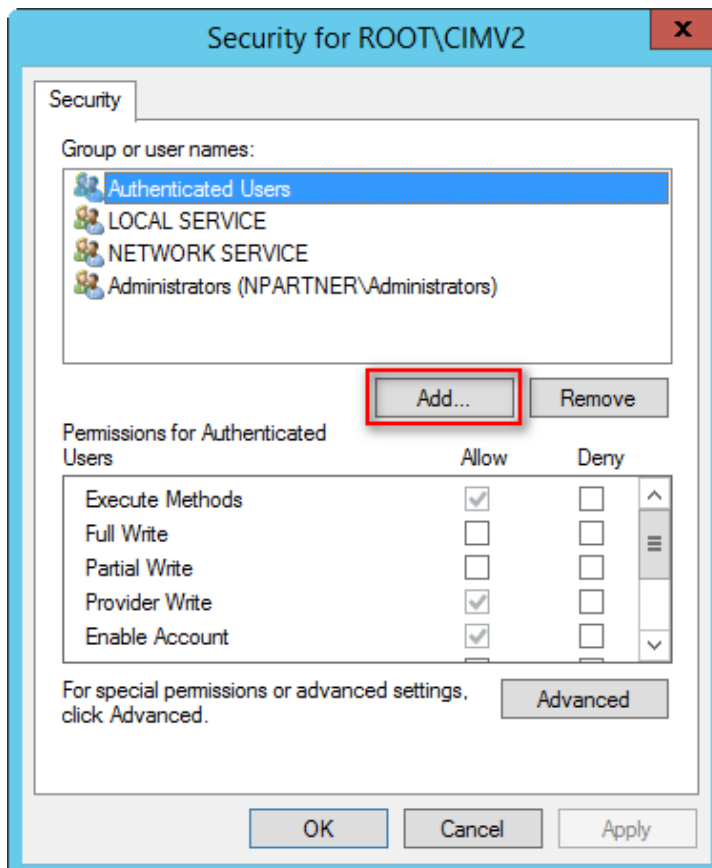
(4) Edit CIMV2 Security

On the “Security” tab, expand folder “Root” -> “CIMV2,” then click “Security.”



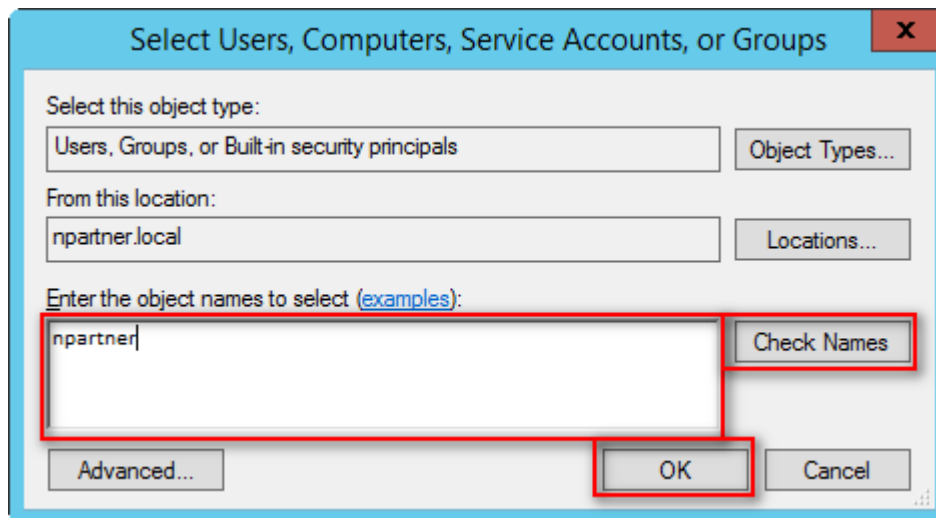
(5) Add WMI User Permissions

Click “Add.”



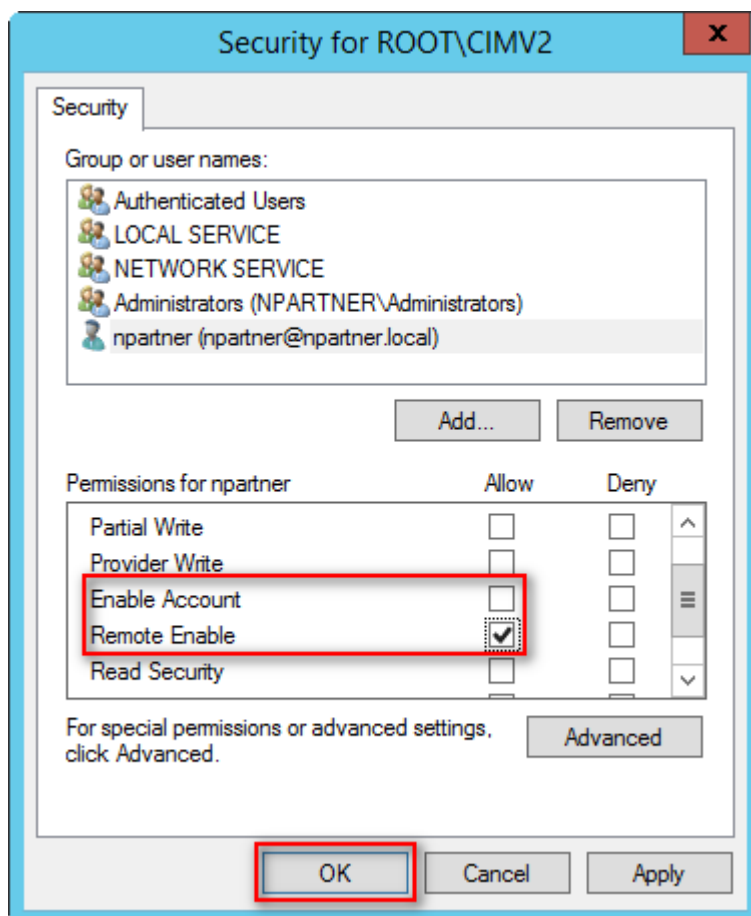
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”

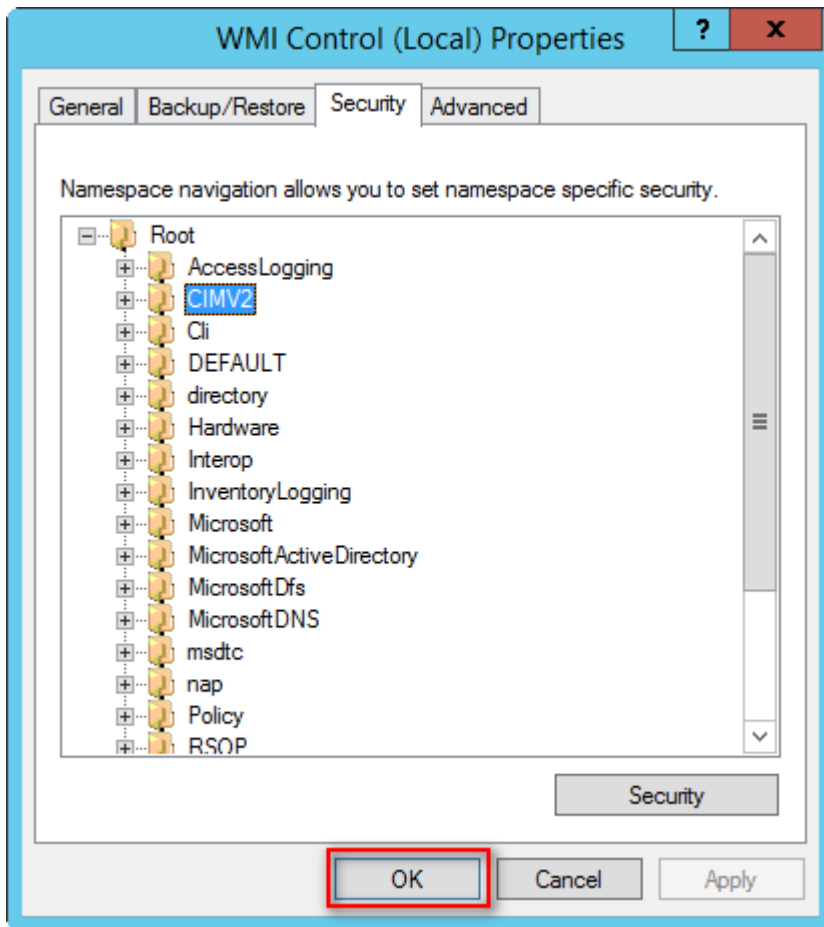


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Click "OK."



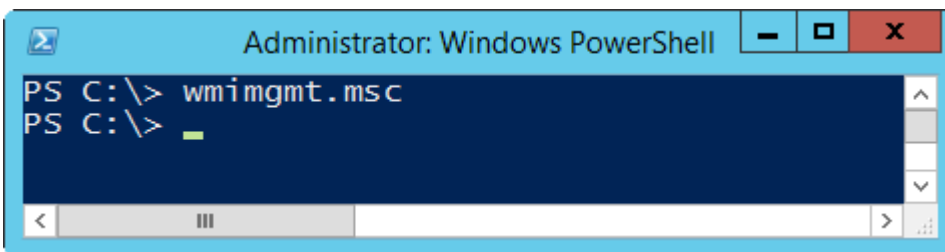
4.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”



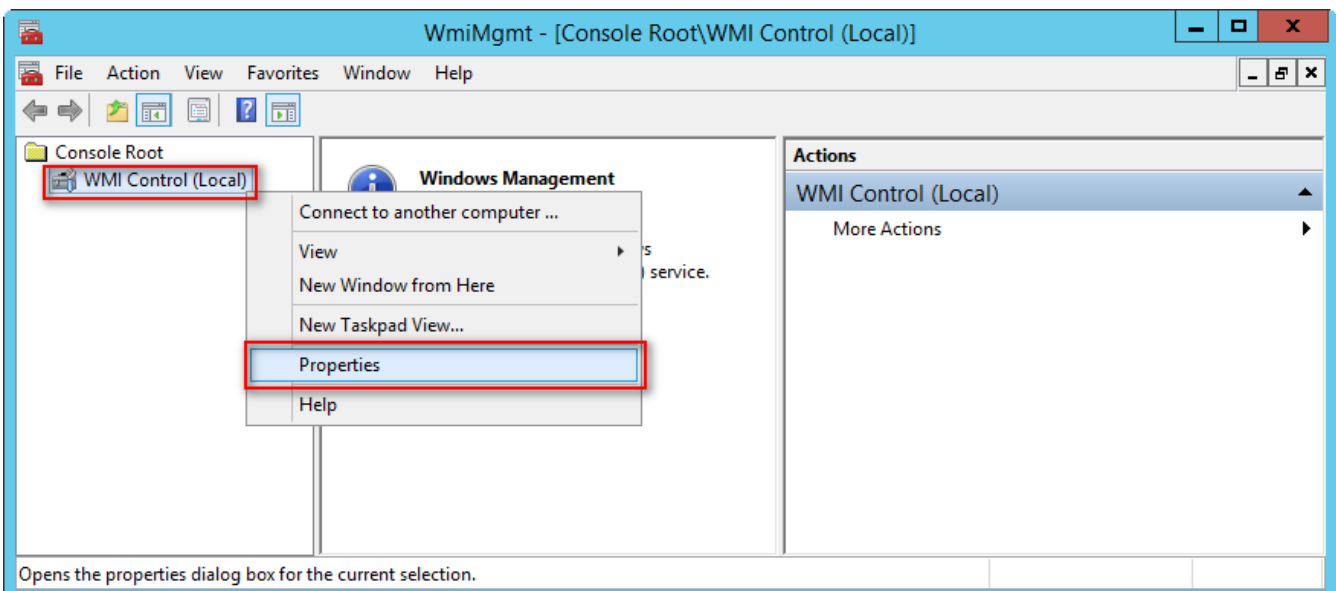
(2) Enter the command below to enable WMI Control.

```
PS C:\> wmicmgmt.msc
```



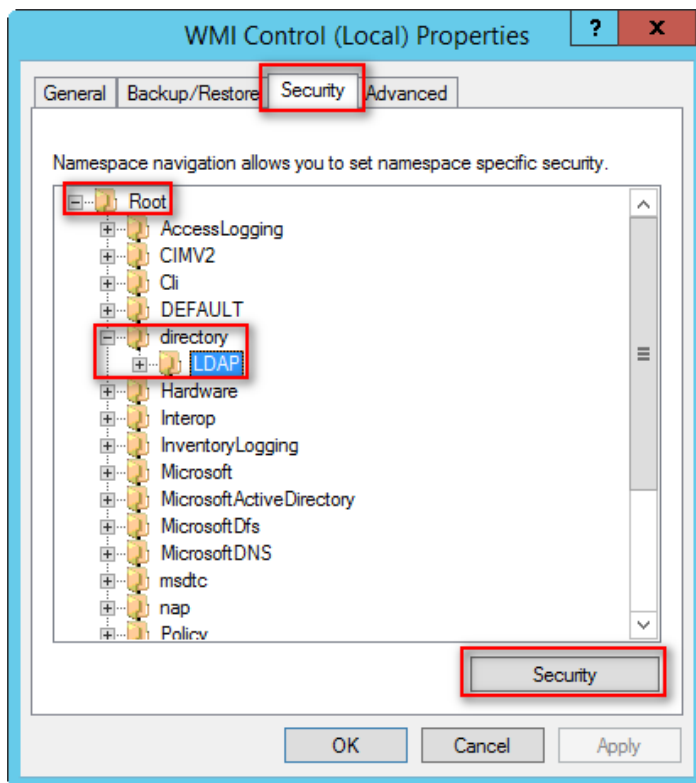
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



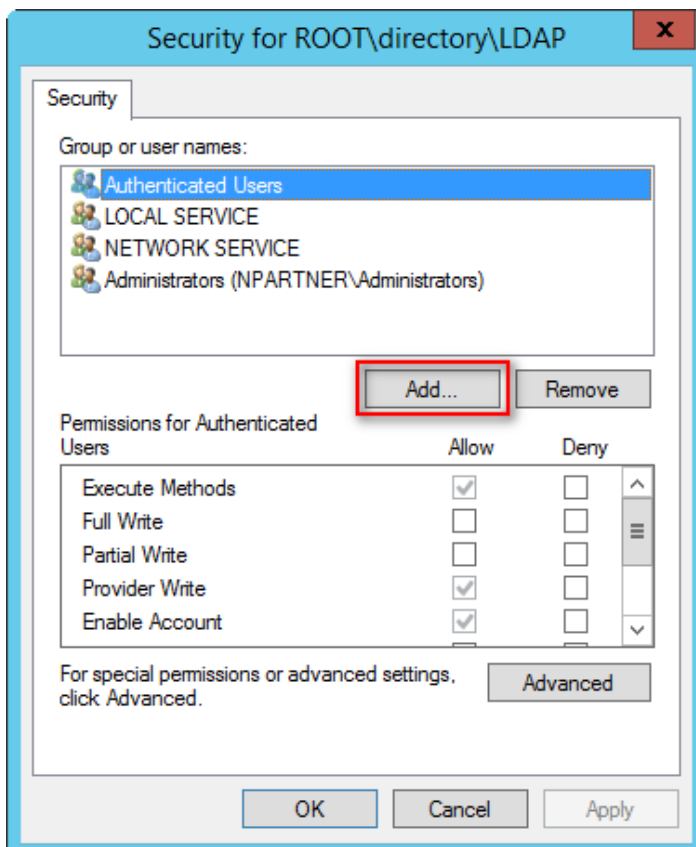
(4) Edit LDAP Security

On the "Security" tab, expand "Root"-> "directory" -> "LDAP," then click "Security."



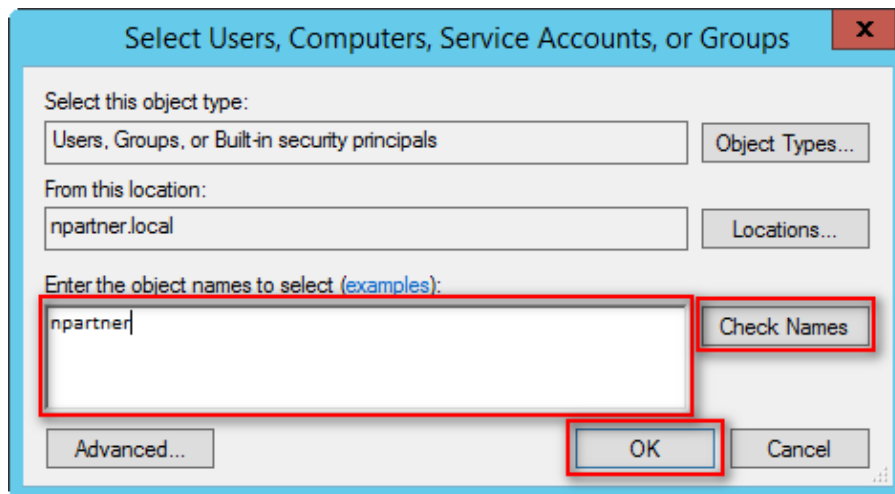
(5) Add WMI User Permissions

Click "Add."



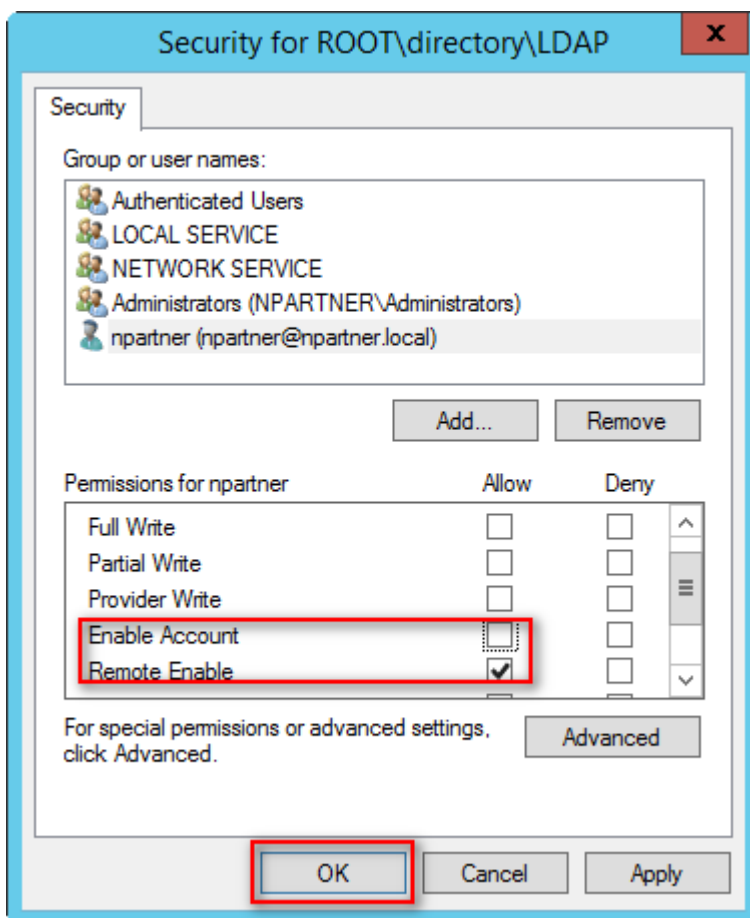
(6) Enter Your Username

Input your user account name (in this example, it is “npartner”), click “Check Names,” then click “OK.”

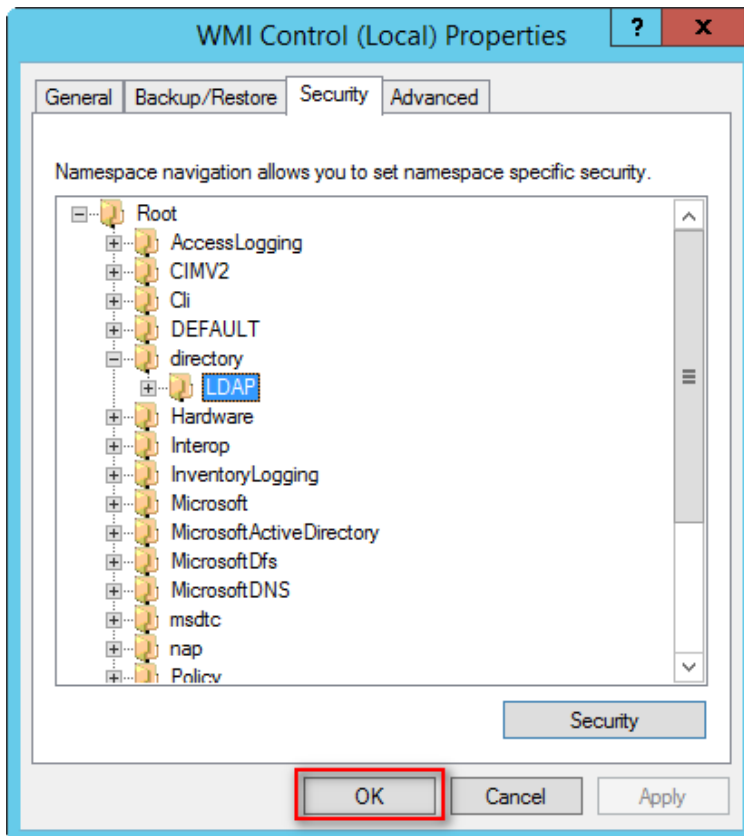


(7) Set Your User Permissions

Select your user account (in this example, it is “npartner”), uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”

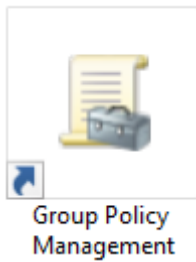


(8) Click "OK."



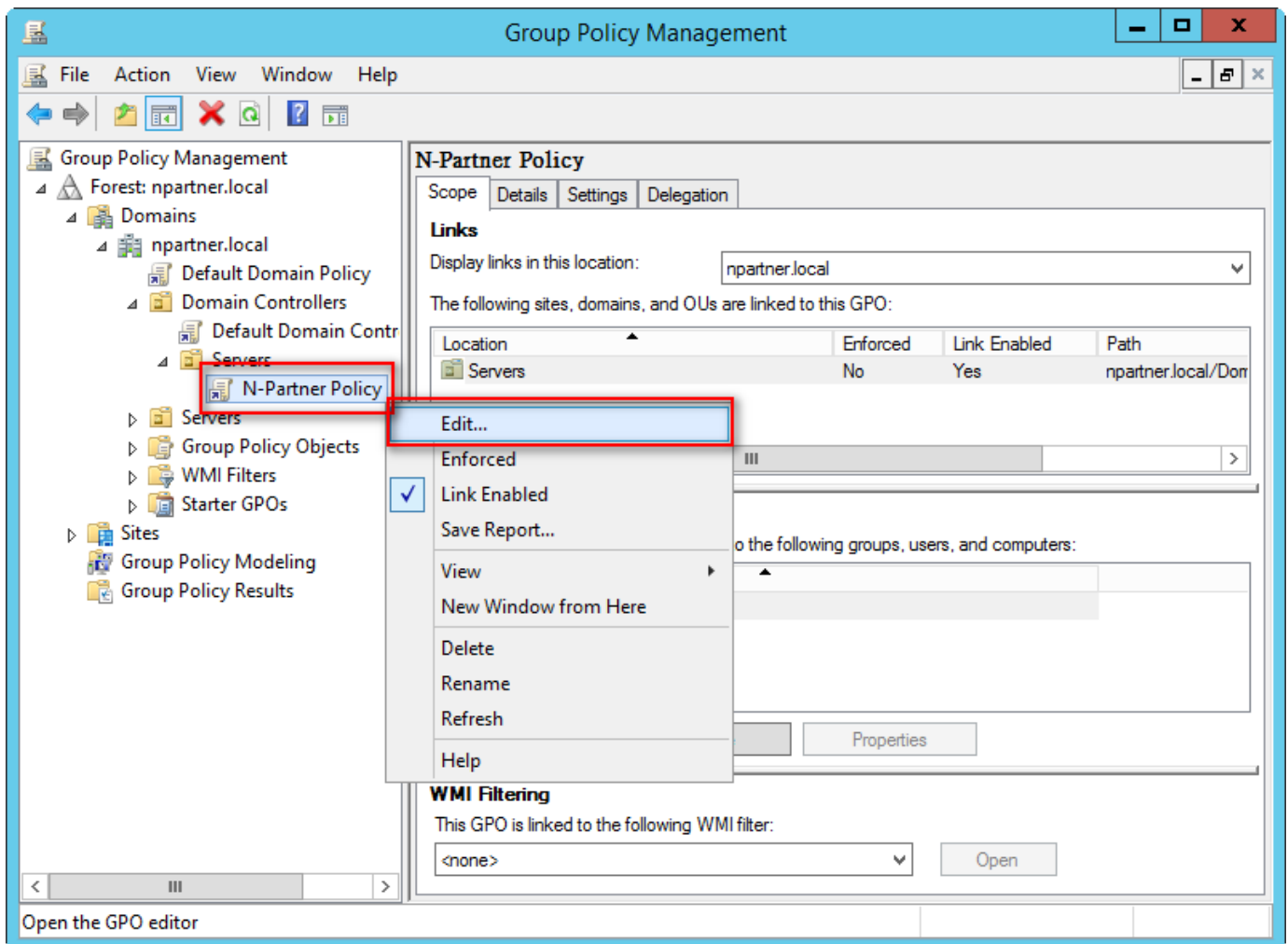
4.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object

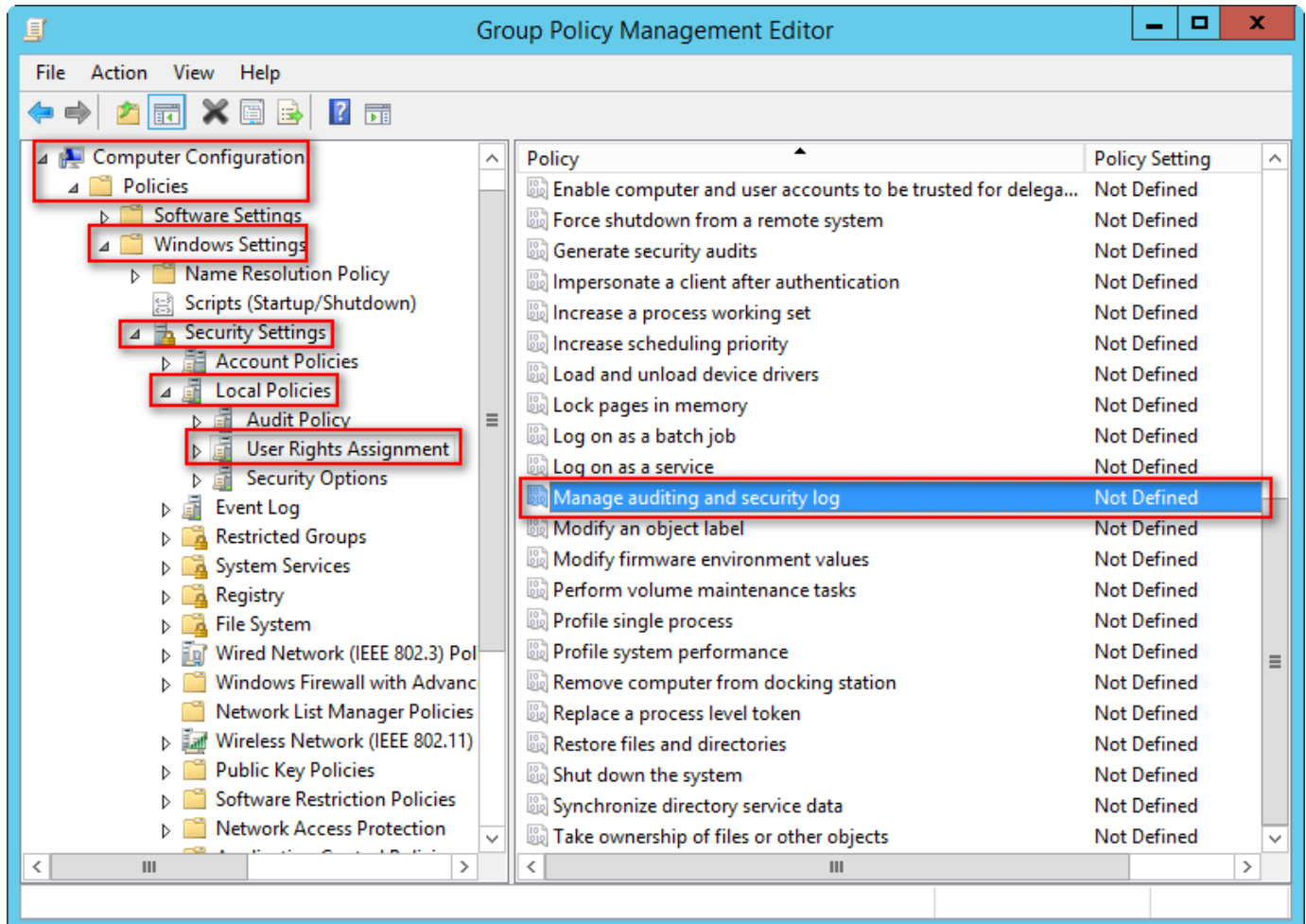
In the “N-Partner Policy” Group Policy Object, right-click and select “Edit.”



(3) Configure Log Settings

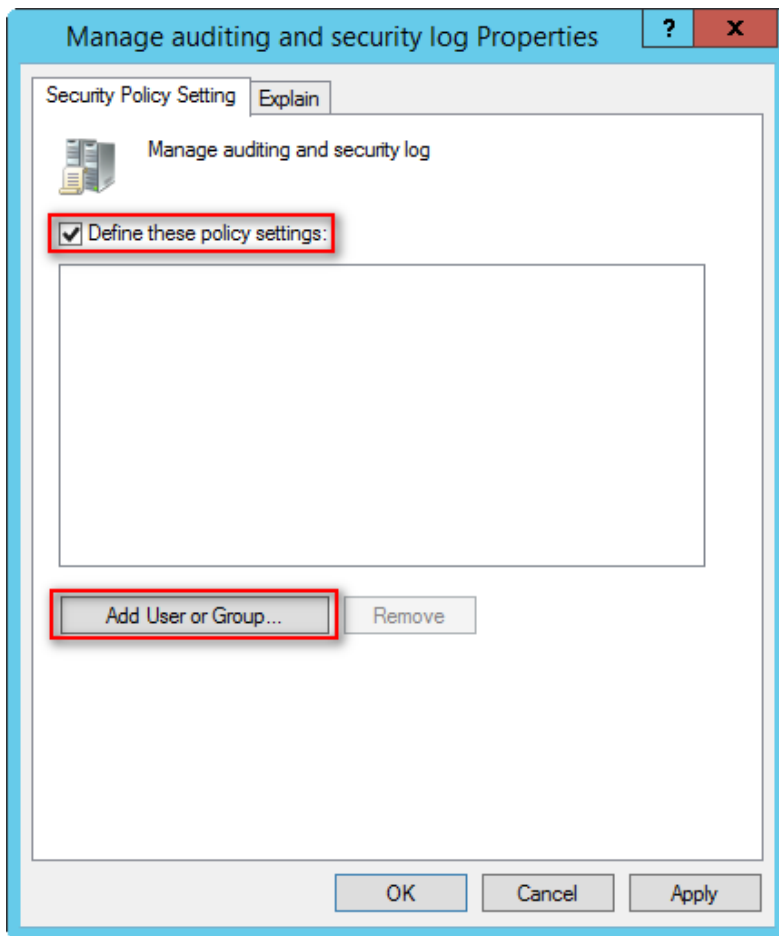
“Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “User Rights Assignment”

Select “Manage auditing and security log,” then click “Properties”.



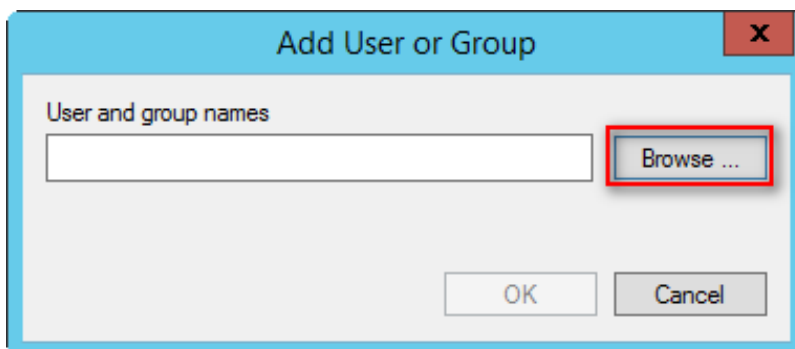
(4) Add Audit Management Users

Select “Define these policy settings,” then click “Add User or Group...”



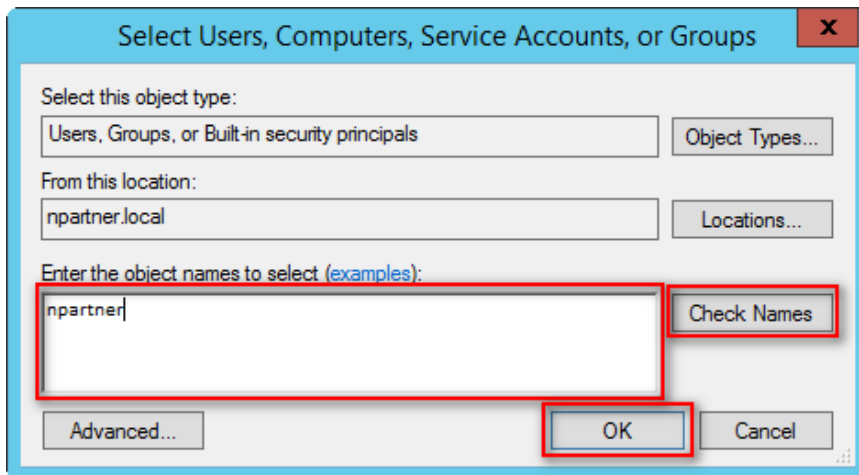
(5) Search for Users

Click “Browse.”



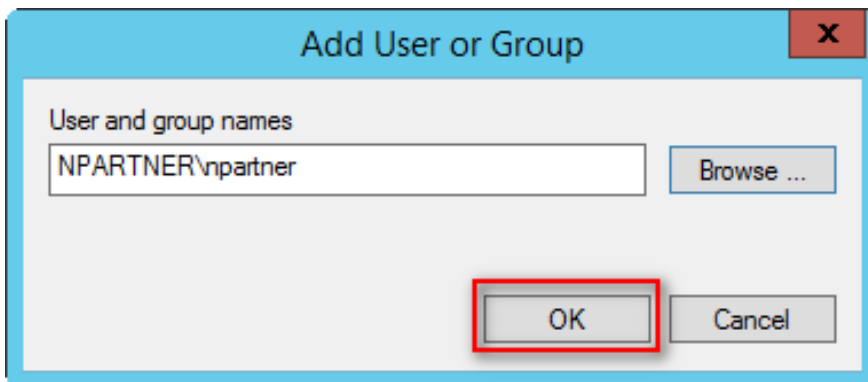
(6) Enter the User

Enter the user account (example: npartner) → click “Check Names” → click “OK.”



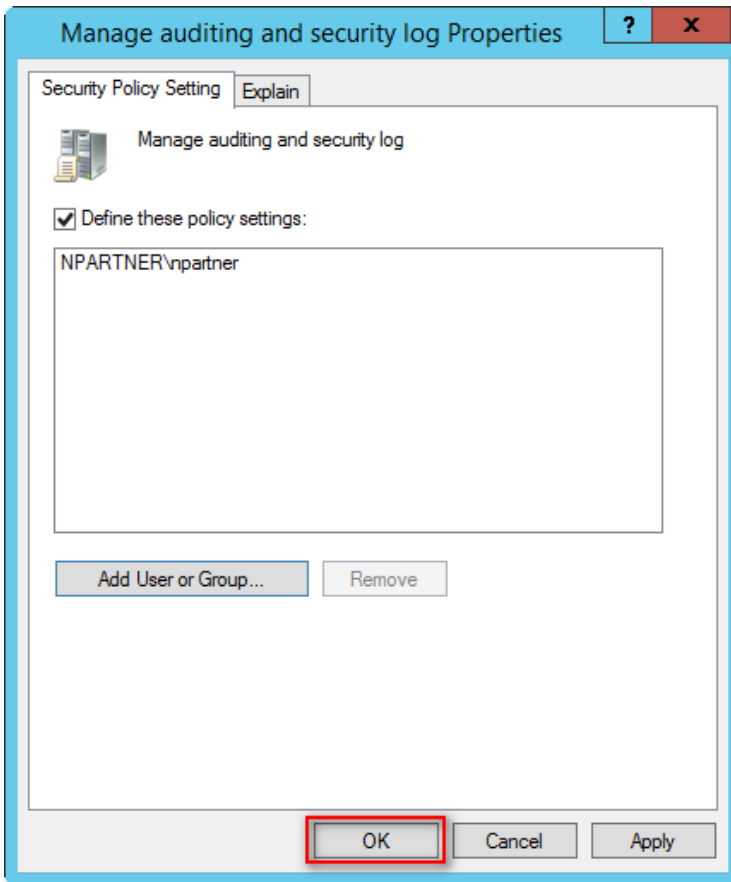
(7) Confirm the User

Click “OK.”



(8) Confirm Logging Settings

Click "OK" to apply the configuration.

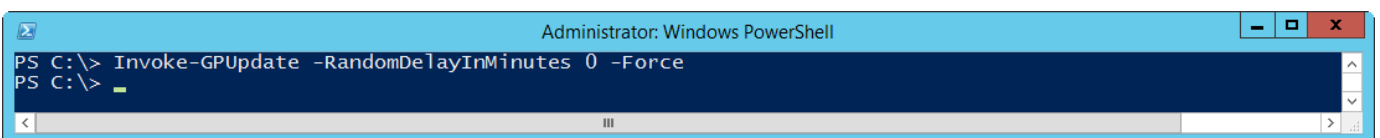


(9) Click "Windows PowerShell."



(10) Enter the command to update group policy:

```
PS C:\> Invoke-GPUUpdate -RandomDelayInMinutes 0 -Force
```



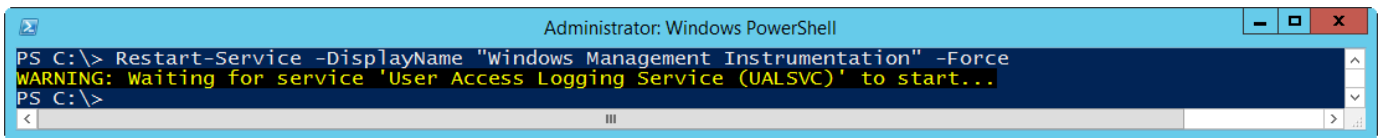
4.3.5 Restart the WMI Service

(1) Click “Windows PowerShell.”



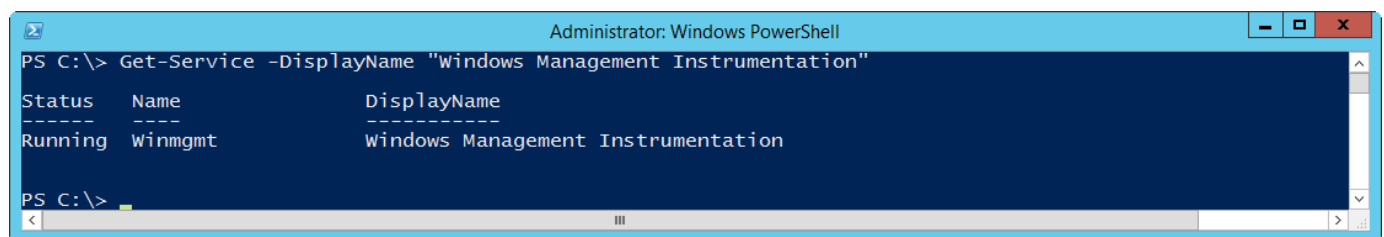
(2) Enter the command below to restart the WMI service:

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) Enter the command below to Verify the WMI service status:

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



4.4 Configure the Firewall

(1) Open "Windows PowerShell."



(2) Enter the command below to configure the firewall to allow only the N-Reporter IP to query WMI:

```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```

A screenshot of an Administrator Windows PowerShell window. The command entered is `Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True`. The prompt shows the command has been executed successfully, with a cursor on the next line.

```
Administrator: Windows PowerShell
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
PS C:\> _
```

Enter the N-Reporter system IP address in the red text.

(3) Enter the command below to verify the WMI firewall rule status:

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```

A screenshot of an Administrator Windows PowerShell window showing the output of the `Get-NetFirewallRule` command. The output is a table with columns: Name, DisplayName, DisplayGroup, RemoteAddress, Enabled, Direction, and Action. The table lists three rules for the 'Windows Management Instrumentation (WMI)' display group, all of which are enabled and allow inbound traffic from the IP address 192.168.8.184.

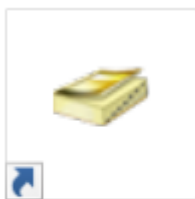
```
Administrator: Windows PowerShell
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound | Format-Table -Property Name,DisplayName,DisplayGroup,@{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},Enabled,Direction,Action
Name                DisplayName          DisplayGroup        RemoteAddress      Enabled            Direction           Action
-----                -
WMI-RPCSS-In-TCP    Windows Manag...    Windows Manag...    192.168.8.184      True              Inbound             Allow
WMI-WINMGMT-In...   Windows Manag...    Windows Manag...    192.168.8.184      True              Inbound             Allow
WMI-ASYNC-In-TCP    Windows Manag...    Windows Manag...    192.168.8.184      True              Inbound             Allow
PS C:\> _
```

5. Windows 2016

For detailed information on setting Windows audit policies, please refer to the [“audit policy recommendations link”](#) in the preface.

5.1 Organizational Unit Settings

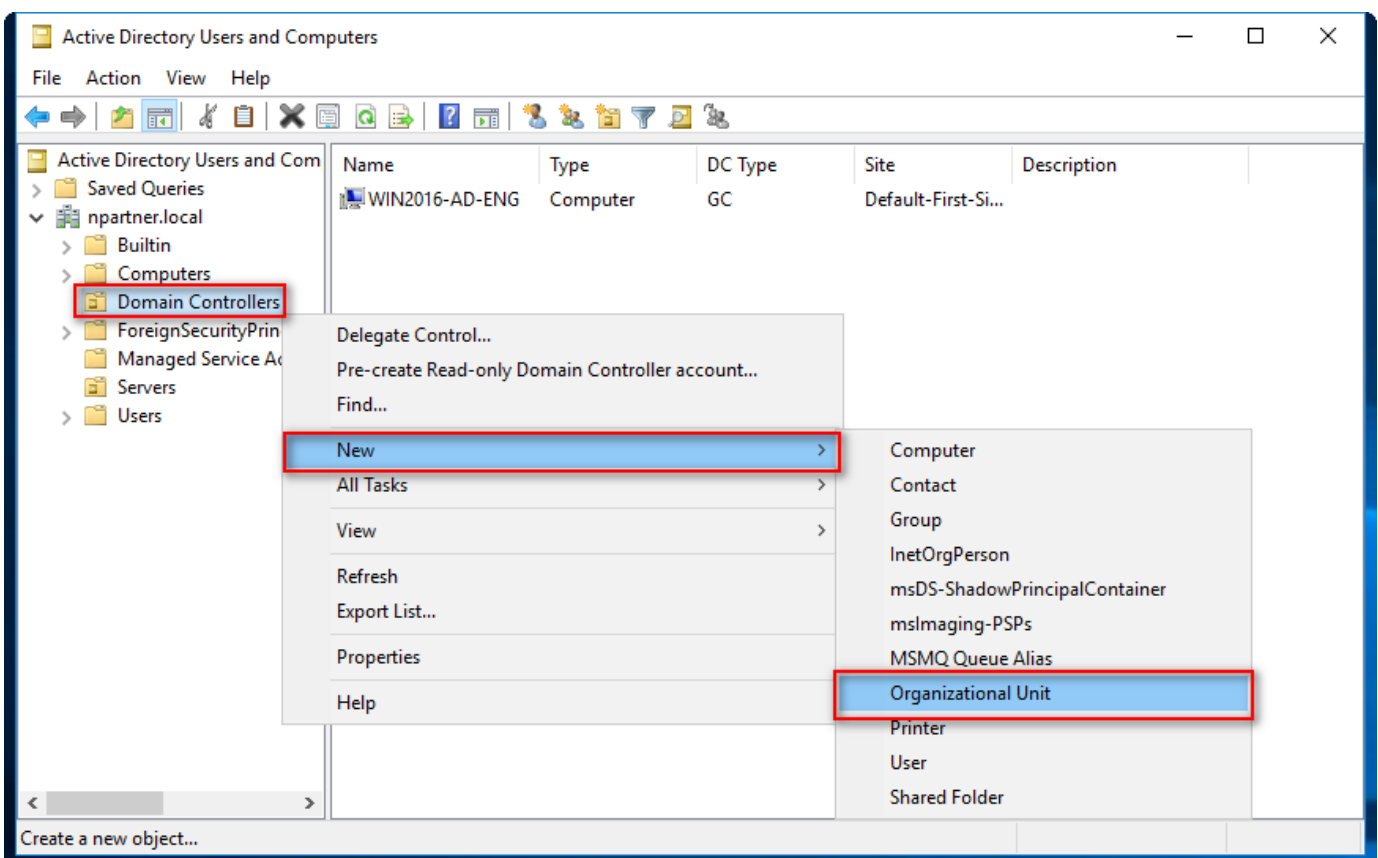
(1) Open “Active Directory Users and Computers.”



Active Directory
Users and
Computers

(2) Add an Organizational Unit

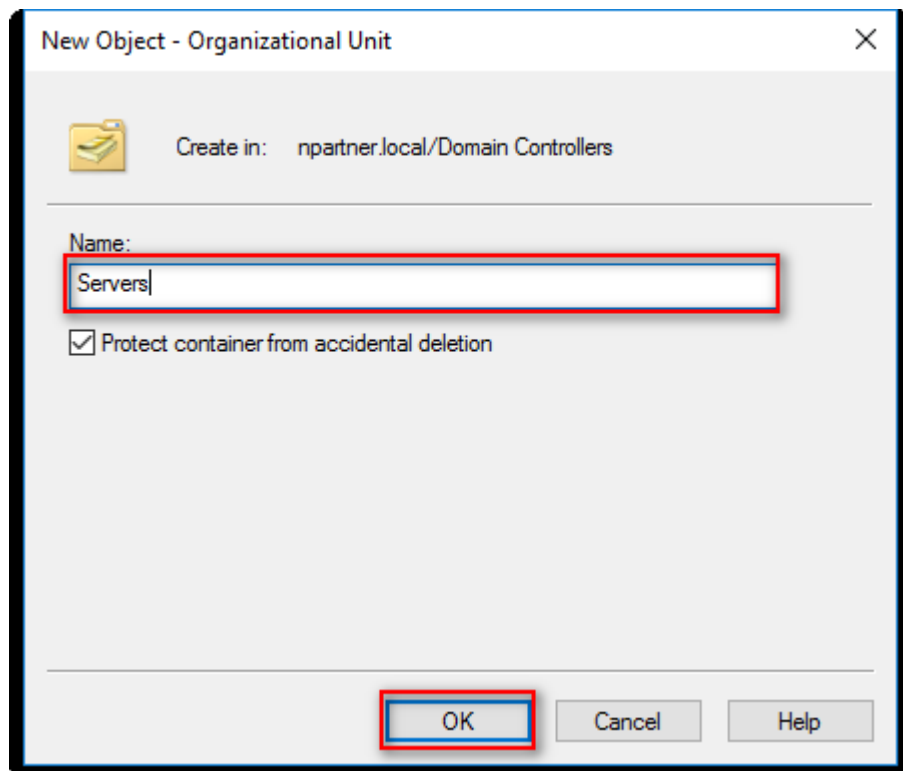
Right-click on “Domain Controllers,” select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

Note: Please create the organizational unit’s name according to the actual environment.

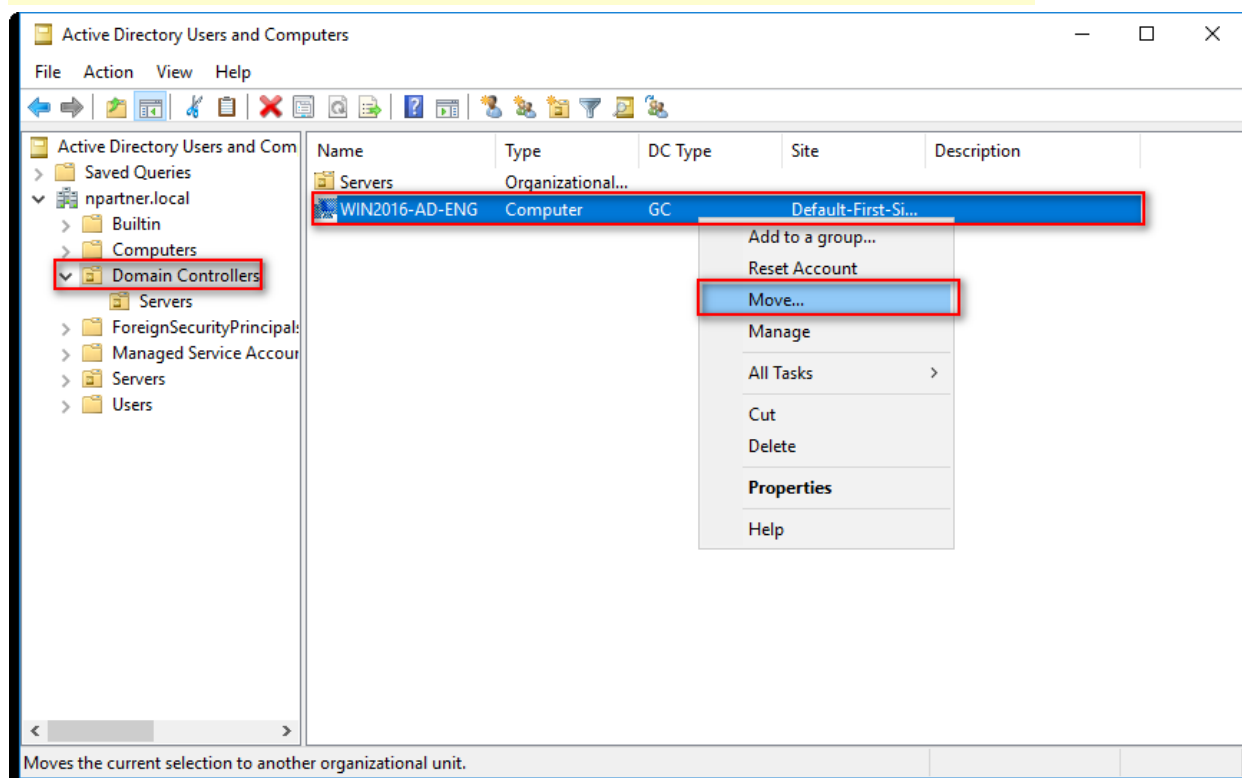
-> Click “OK.”



(4) Move the Server to your New Organizational Unit:

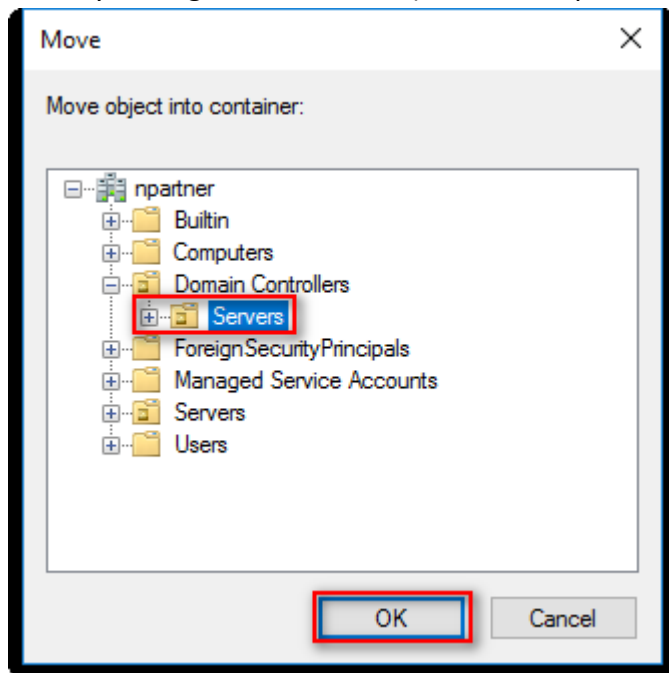
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2016-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



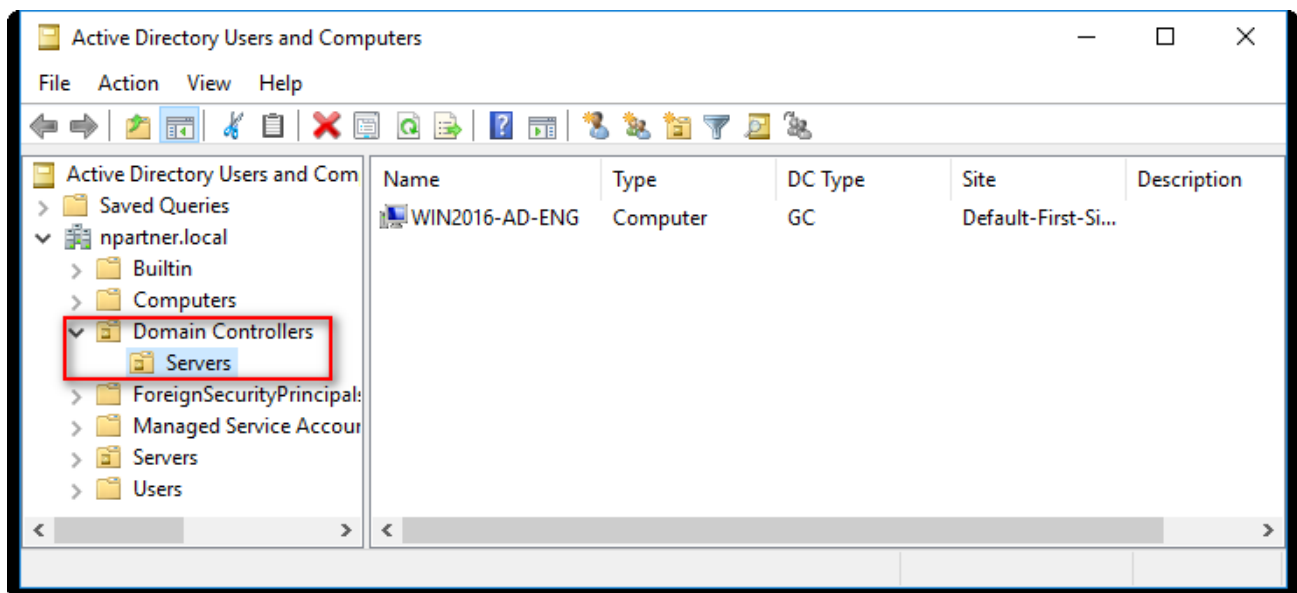
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



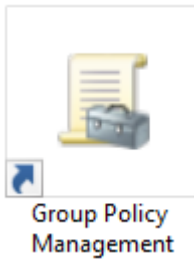
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2016-AD-ENG” server has been moved.

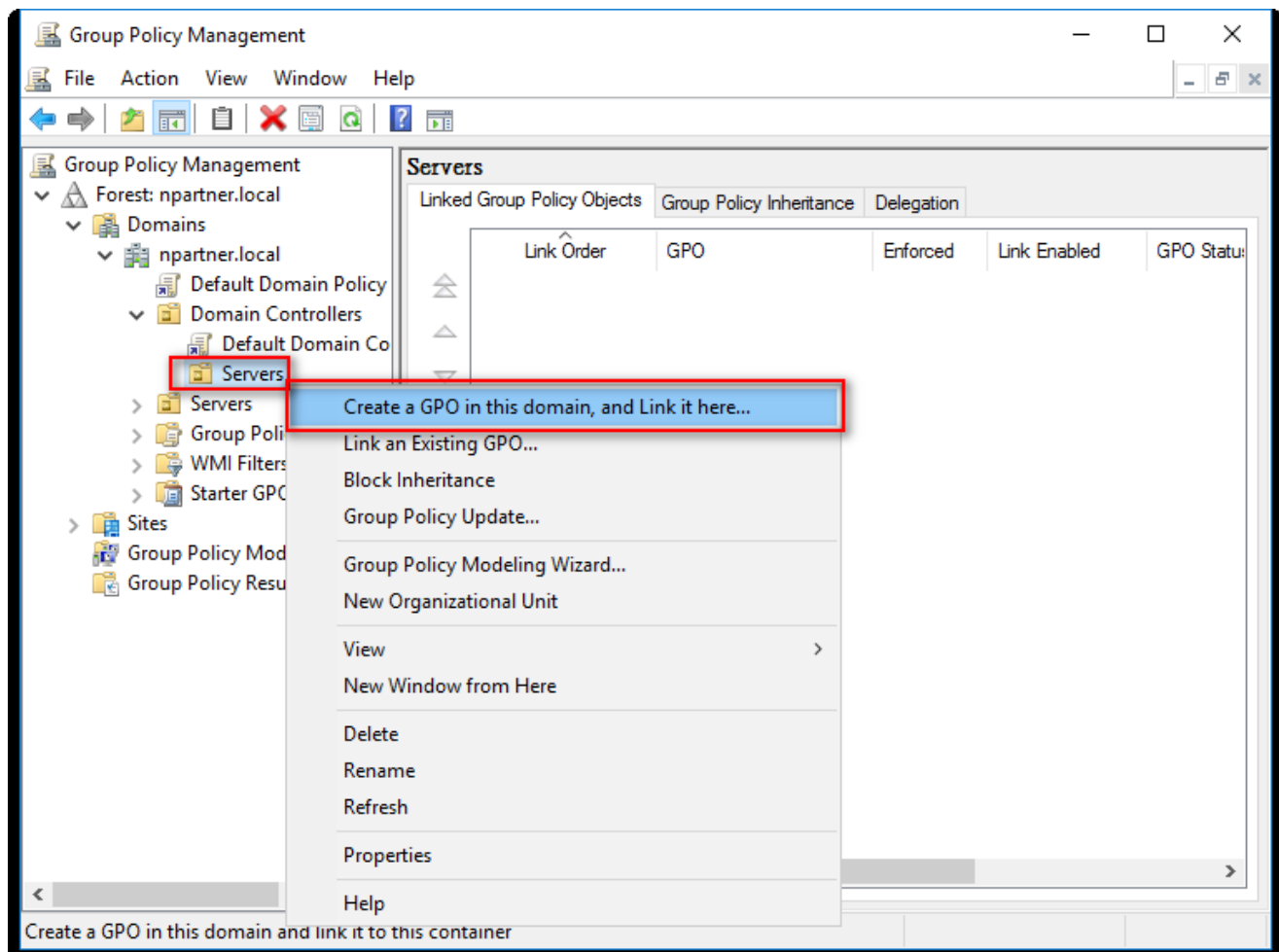


5.2 Group Policy Settings

(1) Click “Group Policy Management.”



(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”

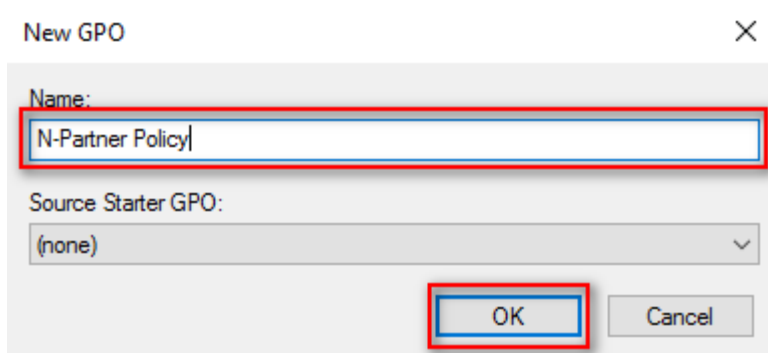


(3) Enter your Group Policy Object Name

Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the client's environment.

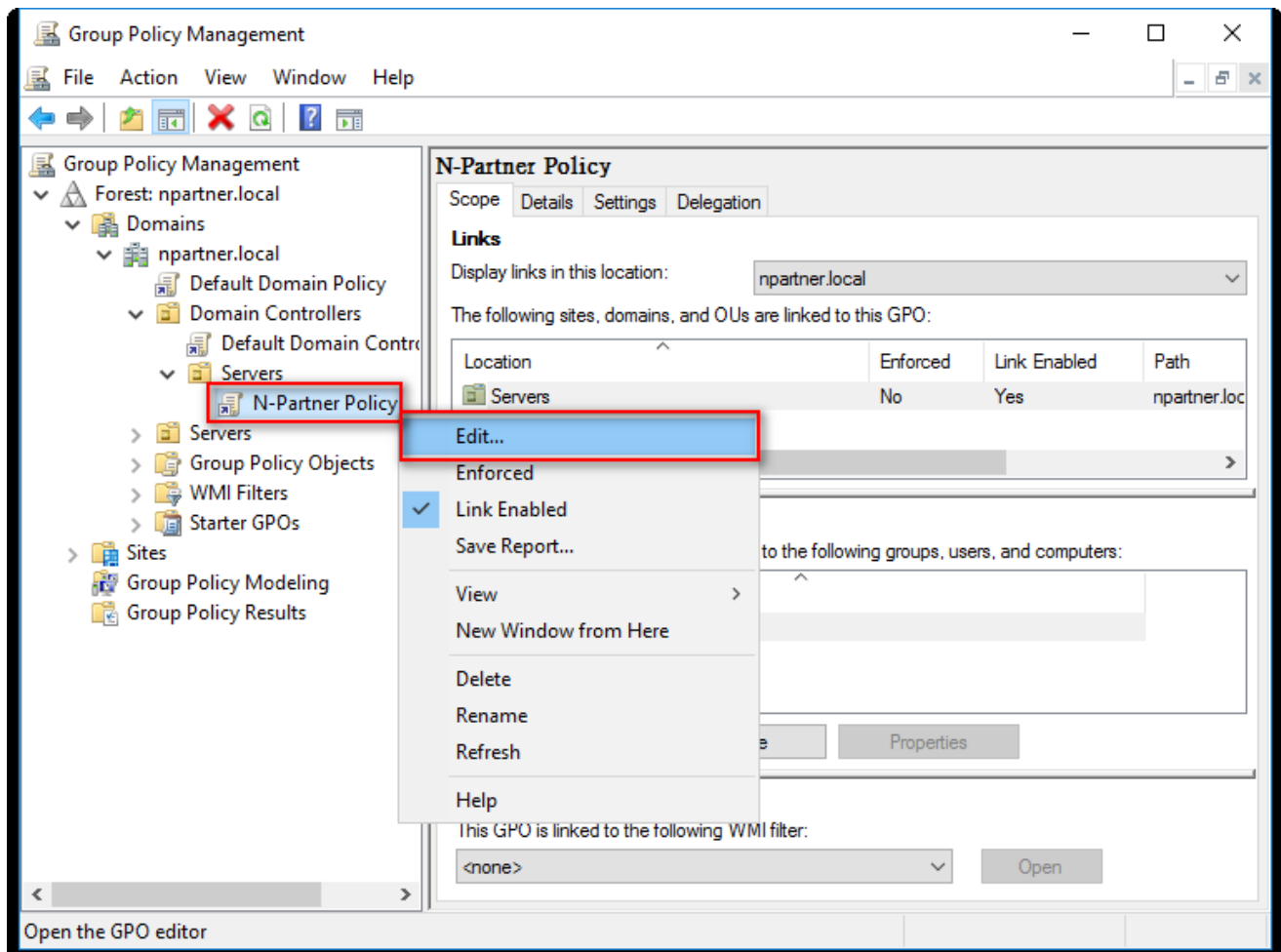
Then click “Edit.”



(4) Edit your Group Policy Object

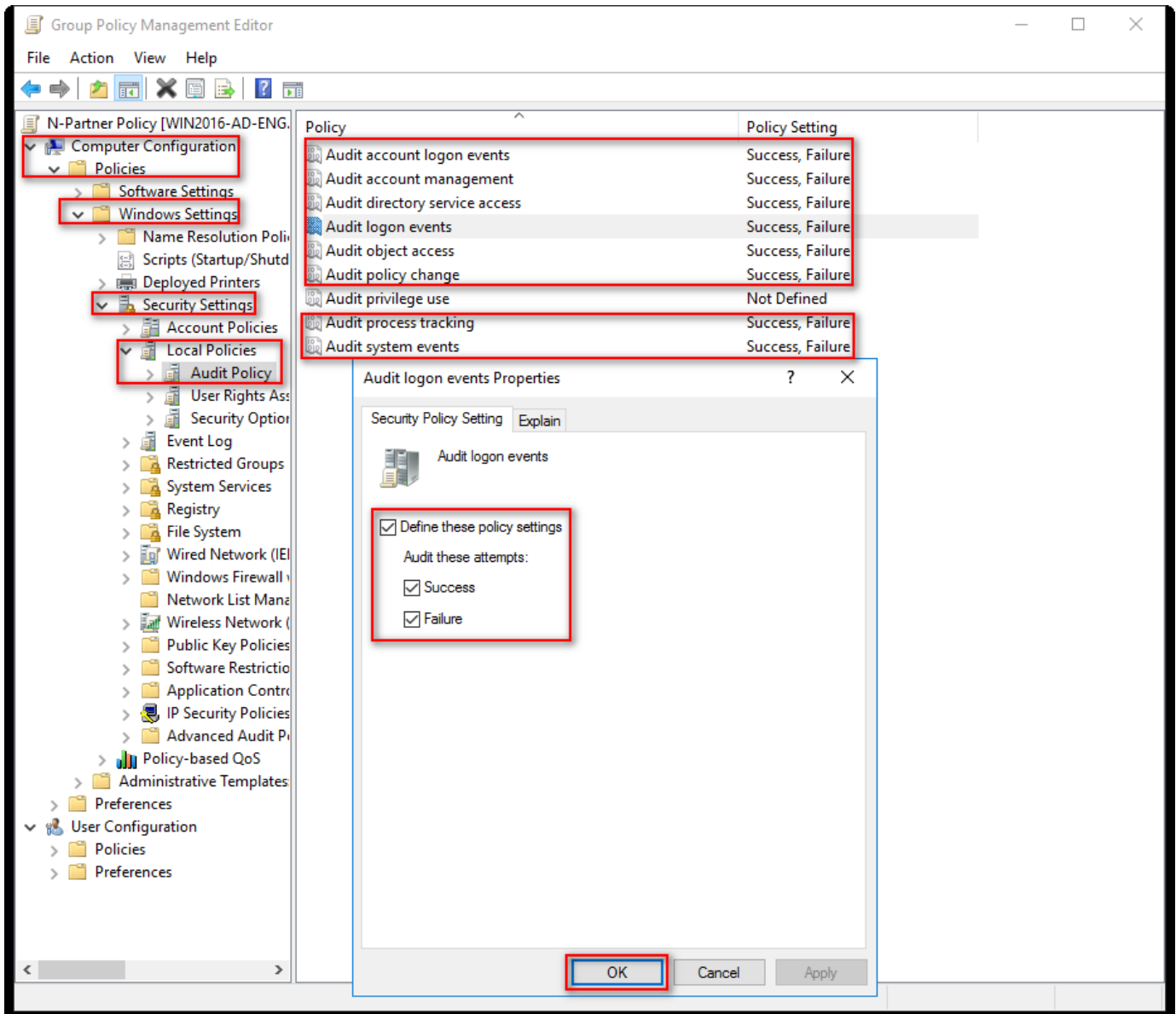
In your group policy object, (in this example, it is “N-Partner Policy”)

right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

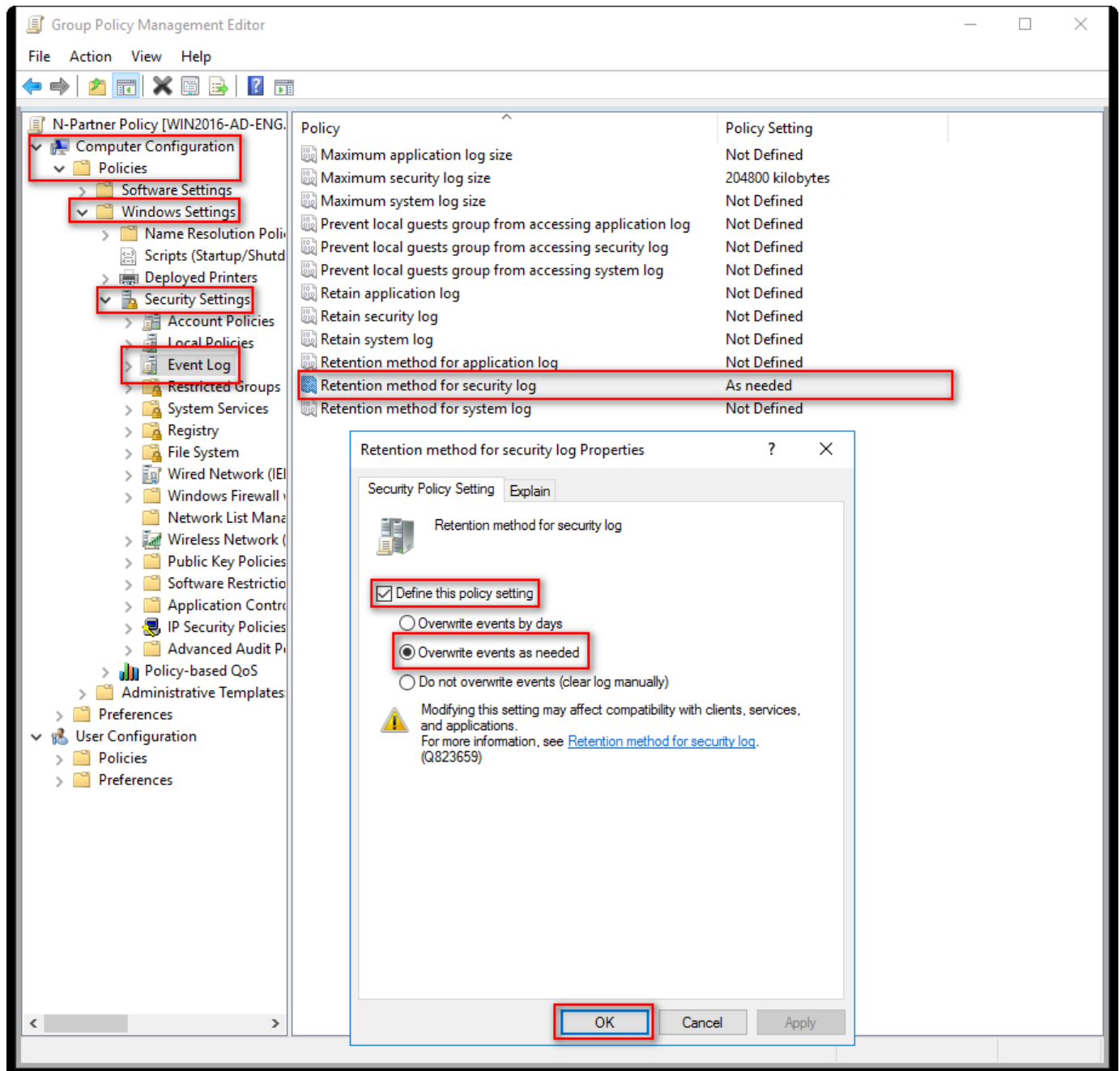
Note: Please adjust the number based on the actual environment. -> Click “OK.”

The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows a tree view where the following folders are expanded and highlighted with red boxes: Computer Configuration, Policies, Windows Settings, Security Settings, Event Log, and Settings for Event Logs. The main pane on the right lists various policies, with 'Maximum security log size' selected and highlighted in blue. Below this, a 'Maximum security log size Properties' dialog box is open. In this dialog, the 'Define this policy setting' checkbox is checked and highlighted with a red box. The value '204800 kilobytes' is entered in the text field and also highlighted with a red box. A warning message at the bottom of the dialog states: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see [Maximum security log size. \(Q823659\)](#)'. The 'OK' button at the bottom of the dialog is also highlighted with a red box.

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

(7) Event Logs: Retention Method for Security Log

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”

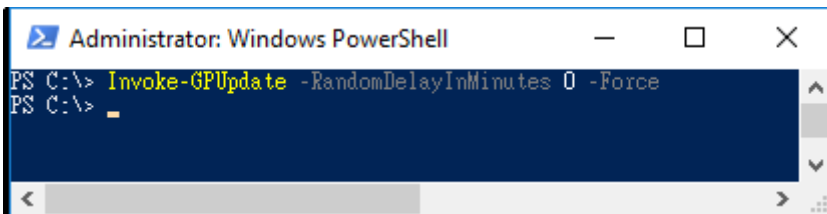


(8) Open “Windows PowerShell.”



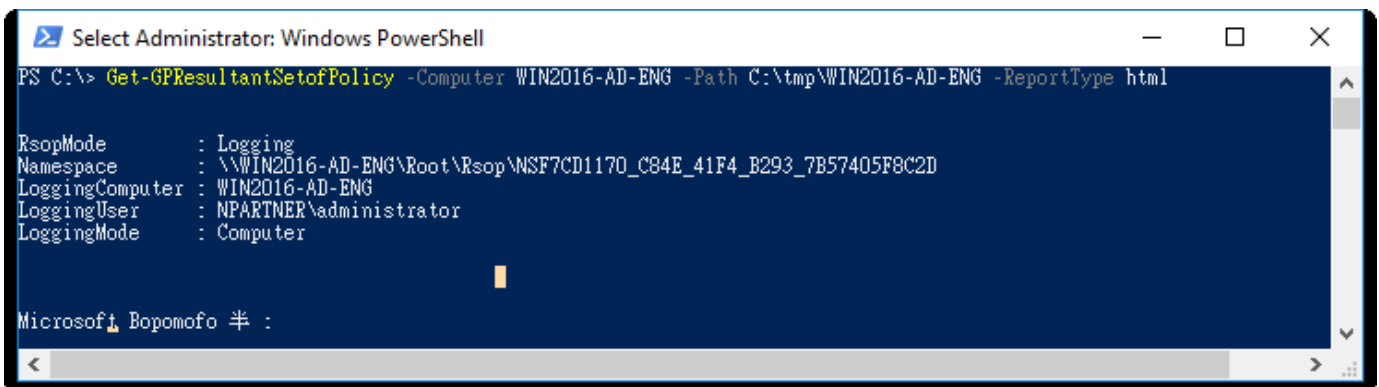
(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUUpdate -RandomDelayInMinutes 0 -Force
```



(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-AD-ENG -Path C:\tmp\WIN2016-AD-ENG.html -ReportType html
```



For the red text , please enter the Windows AD server name and the folder path/file name.

(11) Open the report and verify that the Windows AD server is applying the N-Partner Policy Group Policy.

Account Policies/Account Lockout Policy		
Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
Local Policies/Audit Policy		
Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
Local Policies/Security Options		
Network Access		
Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy
Network Security		
Policy	Setting	Winning GPO
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Event Log		
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings		
Policy	Setting	Winning GPO
Automatic certificate management	Enabled	[Default setting]
Option		Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates		Disabled
Update and manage certificates that use certificate templates from Active Directory		Disabled
Public Key Policies/Encrypting File System		
Certificates		

5.3 Add a Non-Admin Account

5.3.1 Add Users

(1) Open “Windows PowerShell.”



(2) Enter the command below to add a new account.

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the command: `New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True`. The command is executed successfully, and the prompt returns to `PS C:\>`.

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the command: `Get-ADUser npartner -Properties PasswordNeverExpires,Enabled`. The output is as follows:
`DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled : True
GivenName :
Name : npartner
ObjectClass : user
ObjectGUID : e28cc25e-7d32-412f-b97a-78b274d35900
PasswordNeverExpires : True
SamAccountName : npartner
SID : S-1-5-21-3093853764-871050084-3292464314-1105
Surname :
UserPrincipalName : npartner@npartner.local`

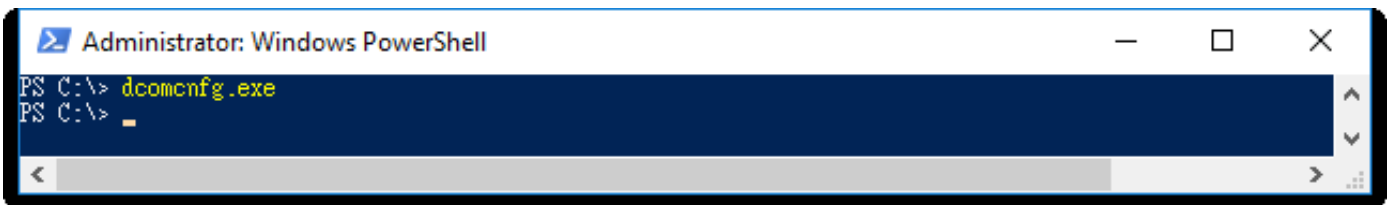
5.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”



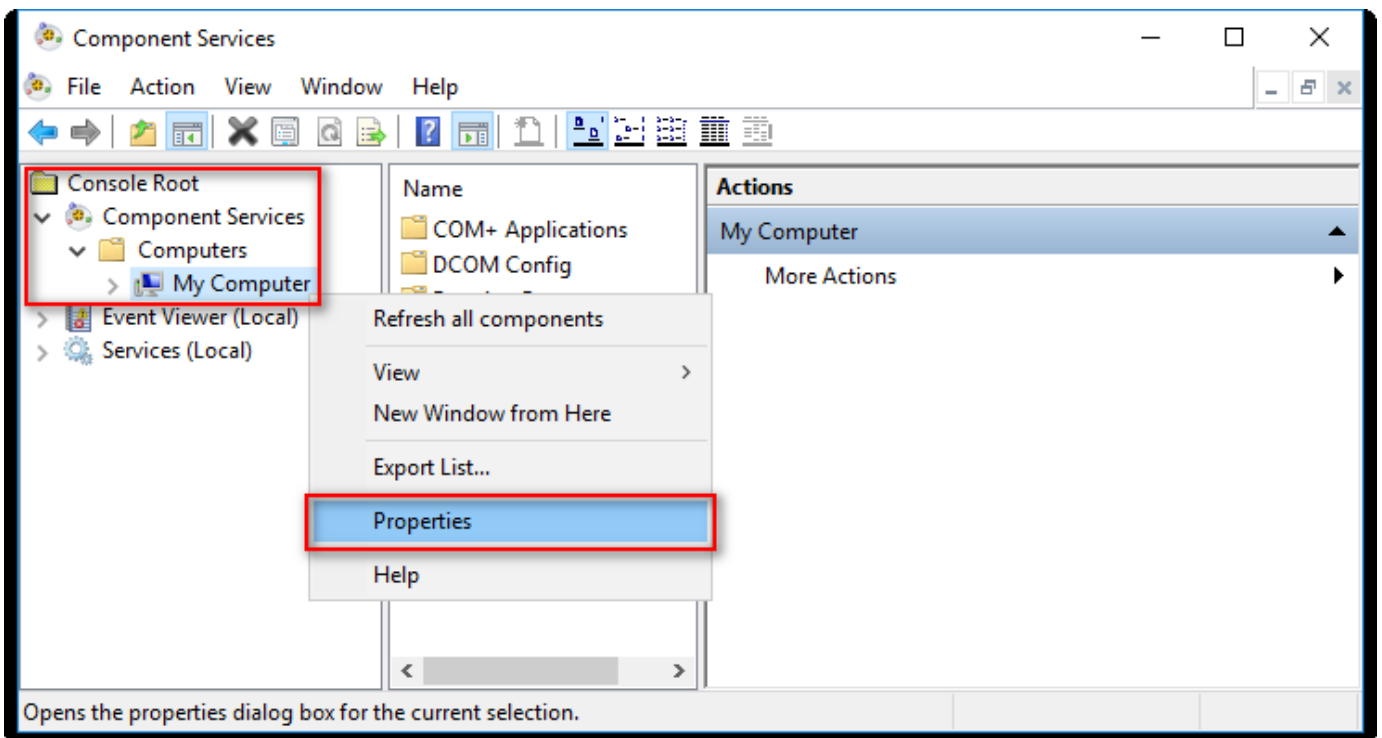
(2) Enter the command below to open component services.

```
PS C:\> dcomcnfg.exe
```



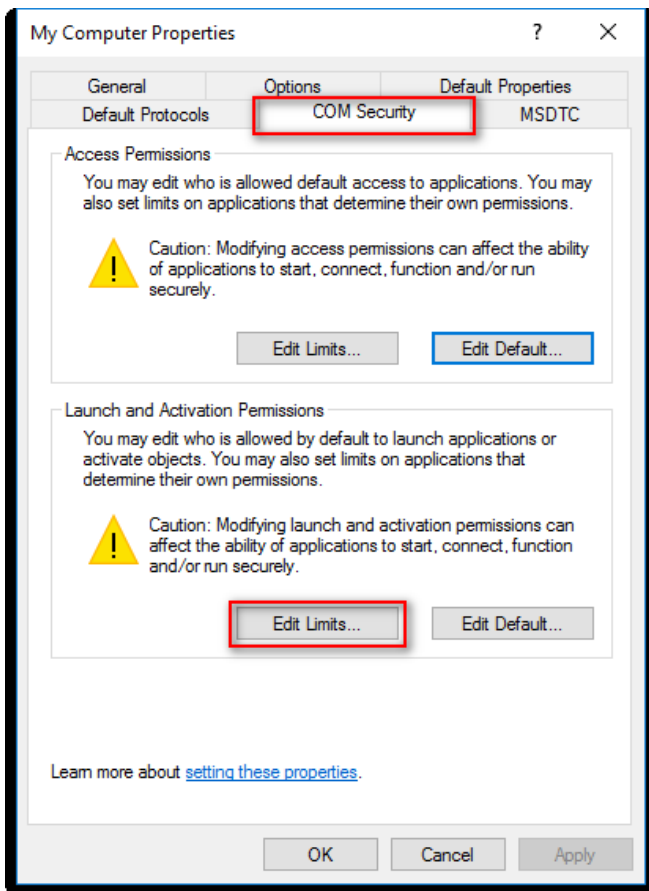
(3) Edit Computer Properties

Expand folder “Console Root” -> “Component Services” -> “Computers,” right-click on “My Computer,” and select “Properties.”



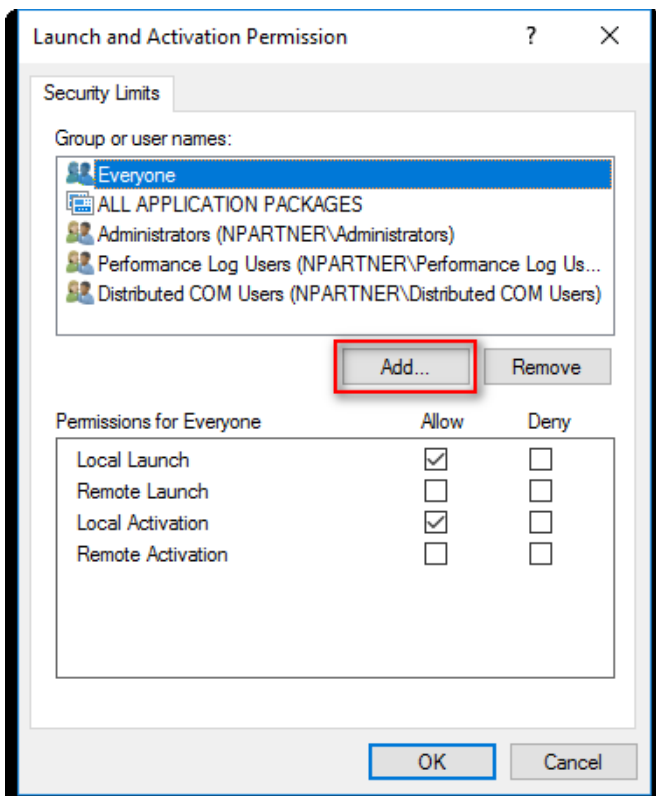
(4) Enable Permissions

Go to the “COM Security” tab, under Launch and Activation Permissions, click “Edit Limits.”



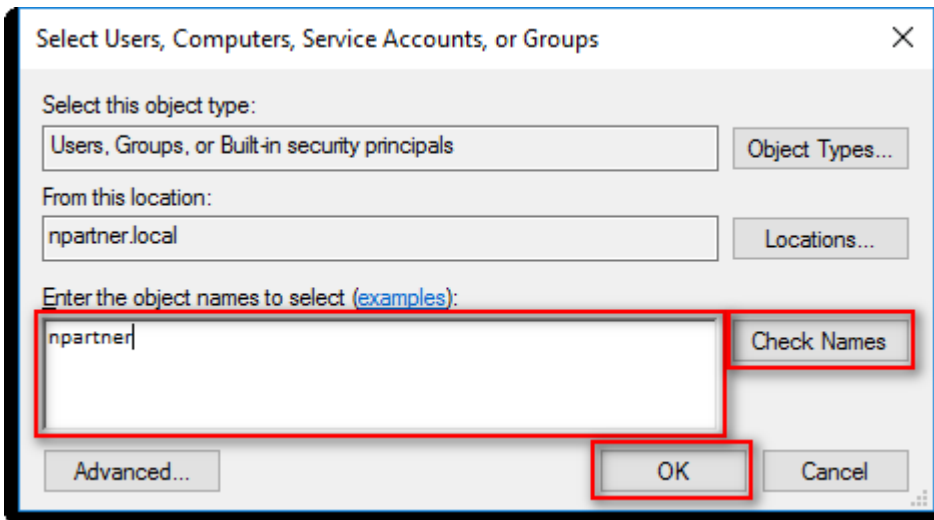
(5) Add DCOM User Permissions

Click “Add.”



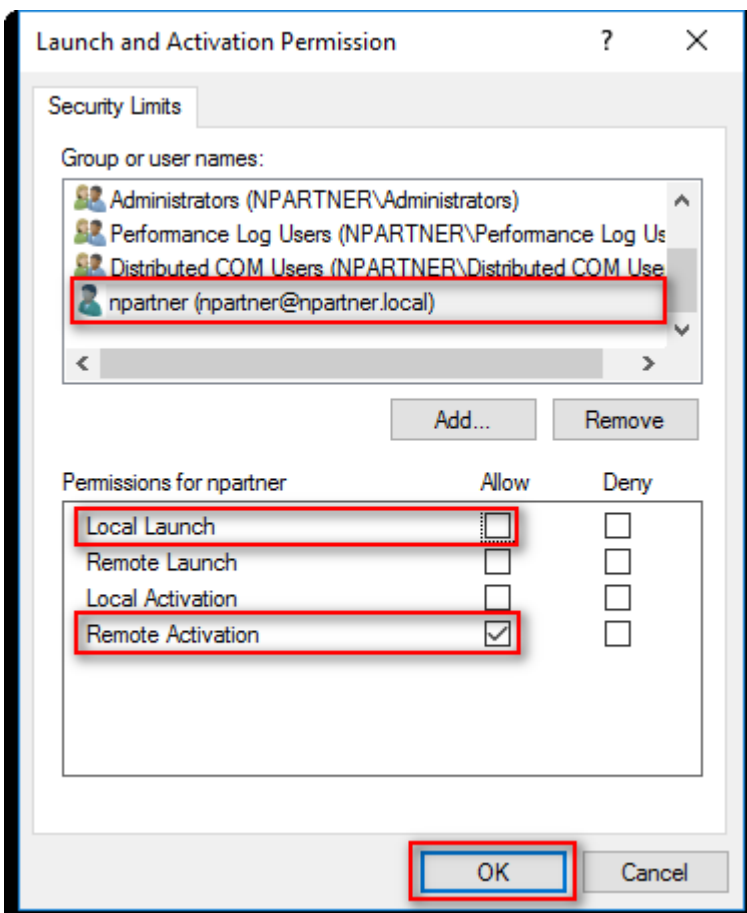
(6) Enter your Username

Input your user account: `npartner`, click “Check Names,” then click “OK.”

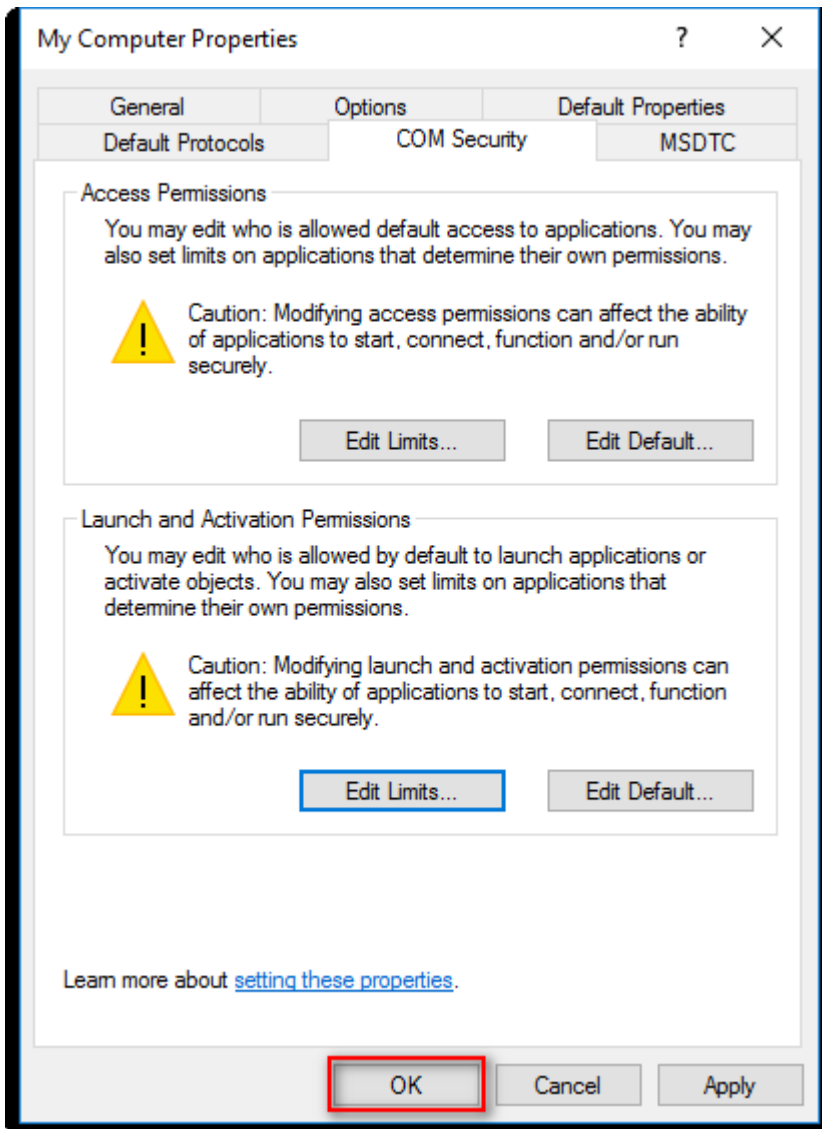


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Local Launch: Allow,” check “Remote Activation: Allow,” then click “OK.”



(8) Click "OK."



5.3.3 Configure WMI Permissions

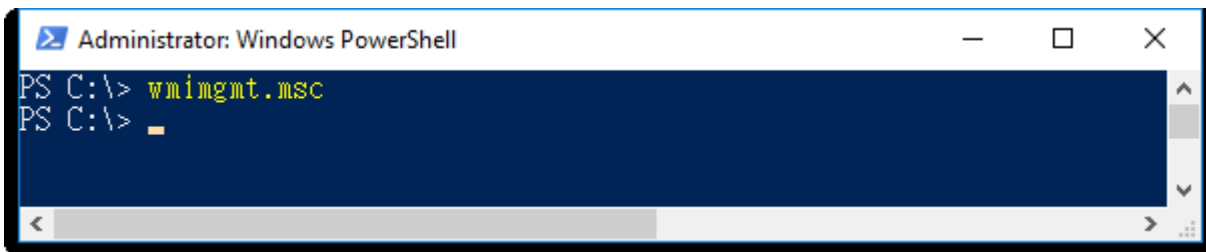
5.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”



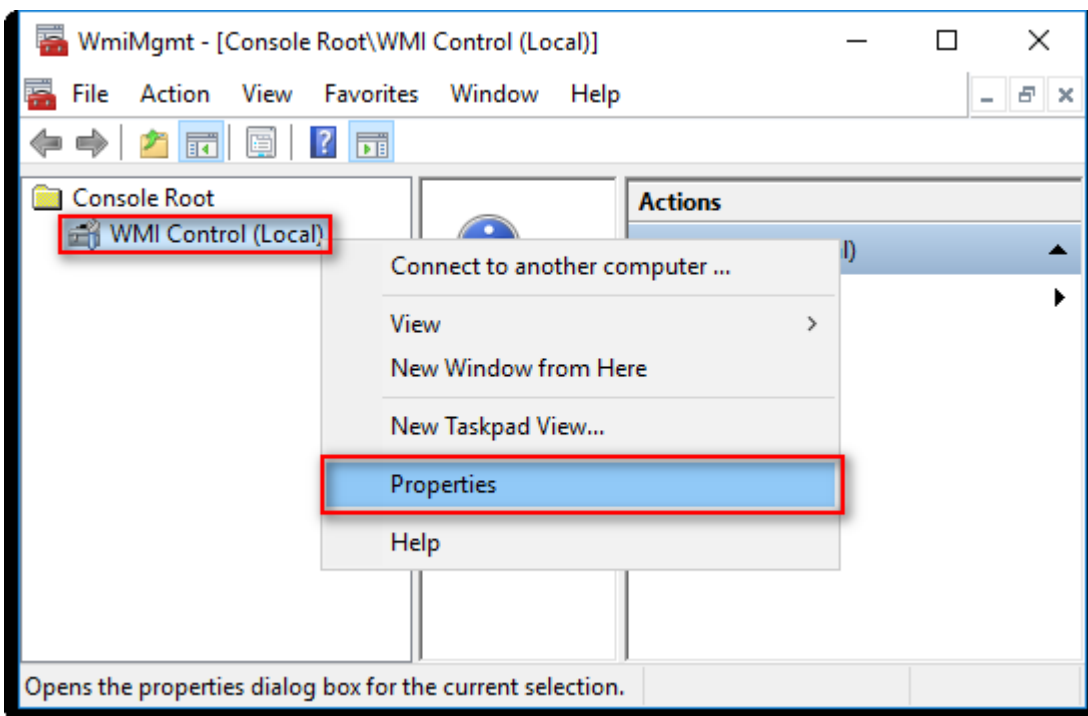
(2) Enter the command below to enable component services.

```
PS C:\> wmicmgmt.msc
```



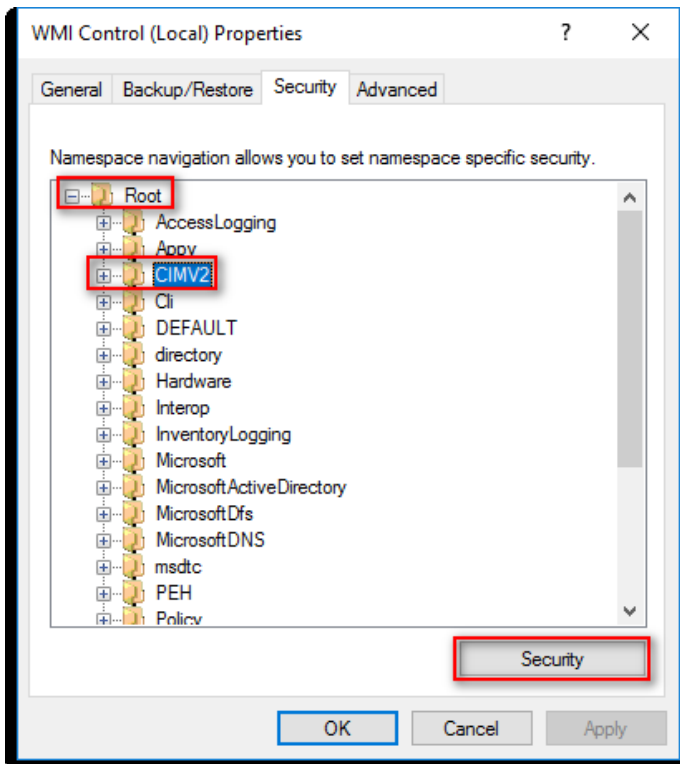
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



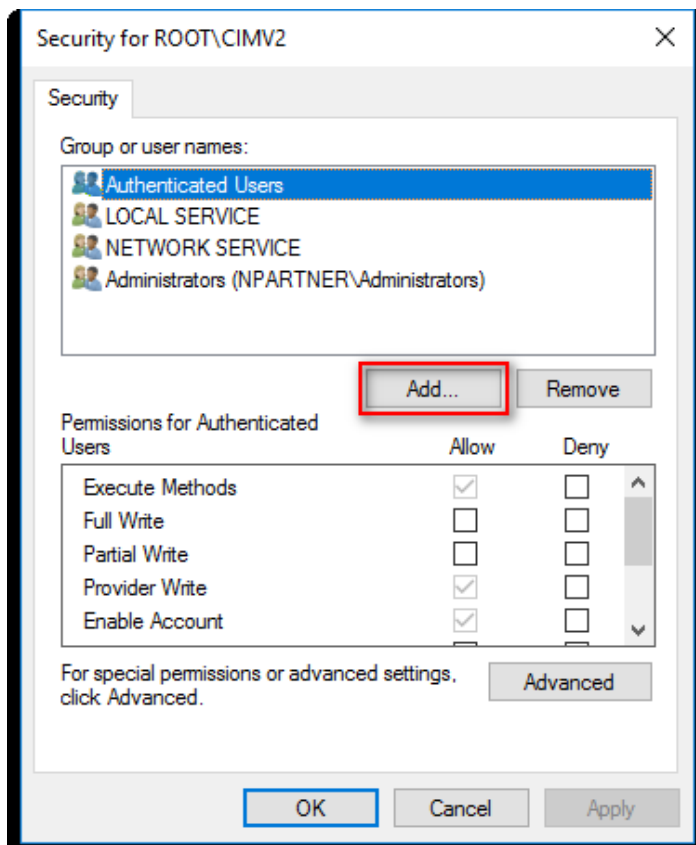
(4) Edit CIMV2 Security

On the "Security" tab, expand folder "Root" -> "CIMV2," then click "Security."



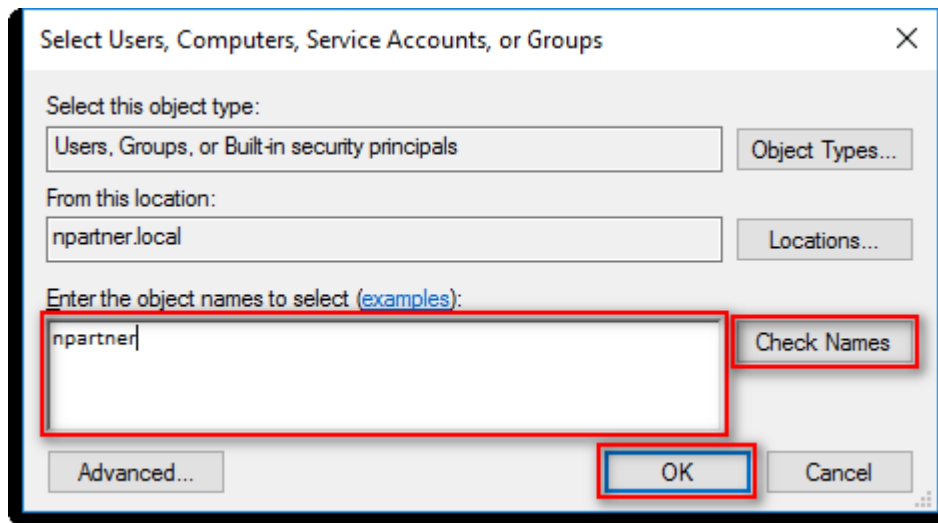
(5) Add WMI User Permissions

Click "Add."



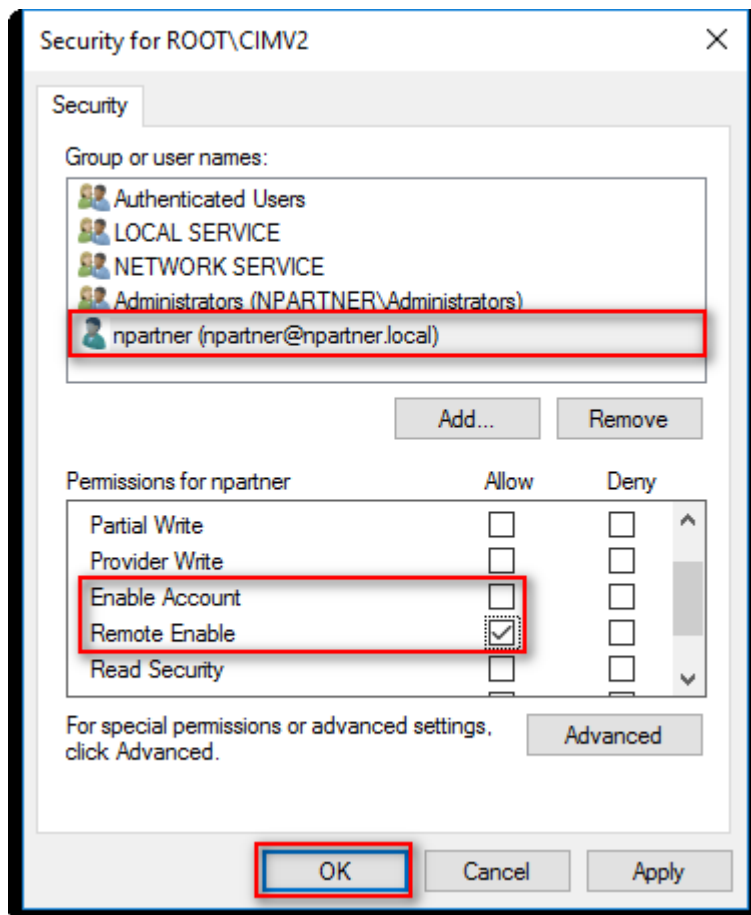
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”

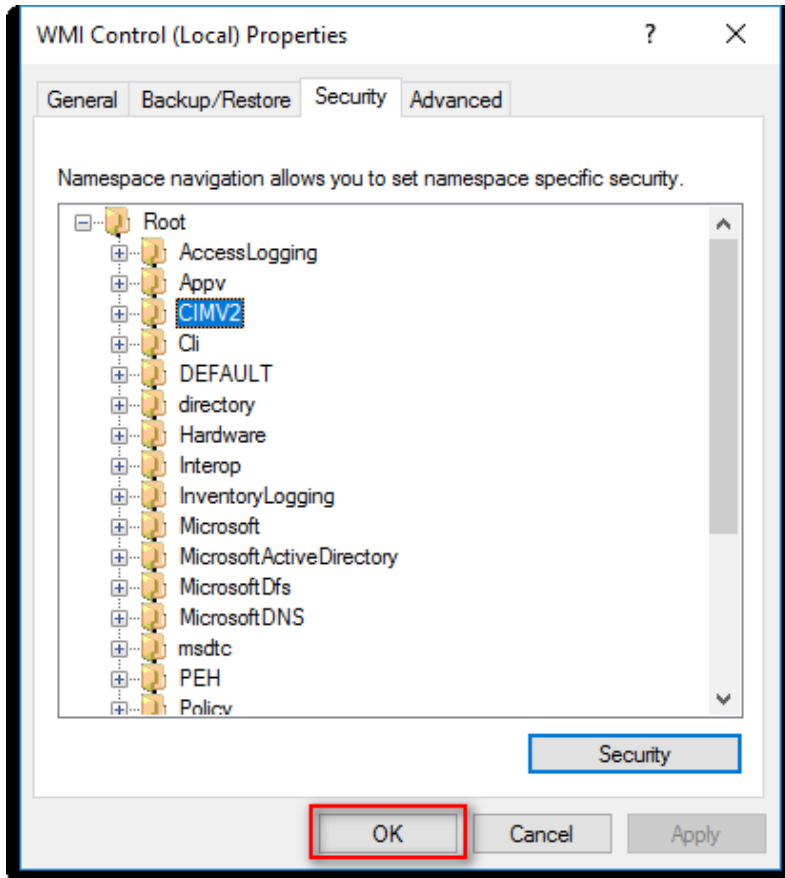


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Click "OK."



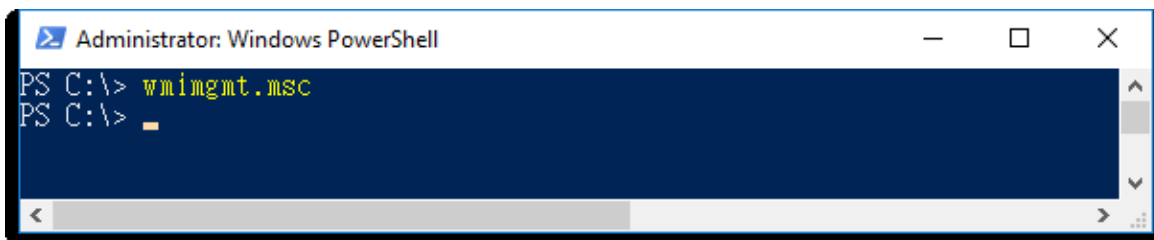
5.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”



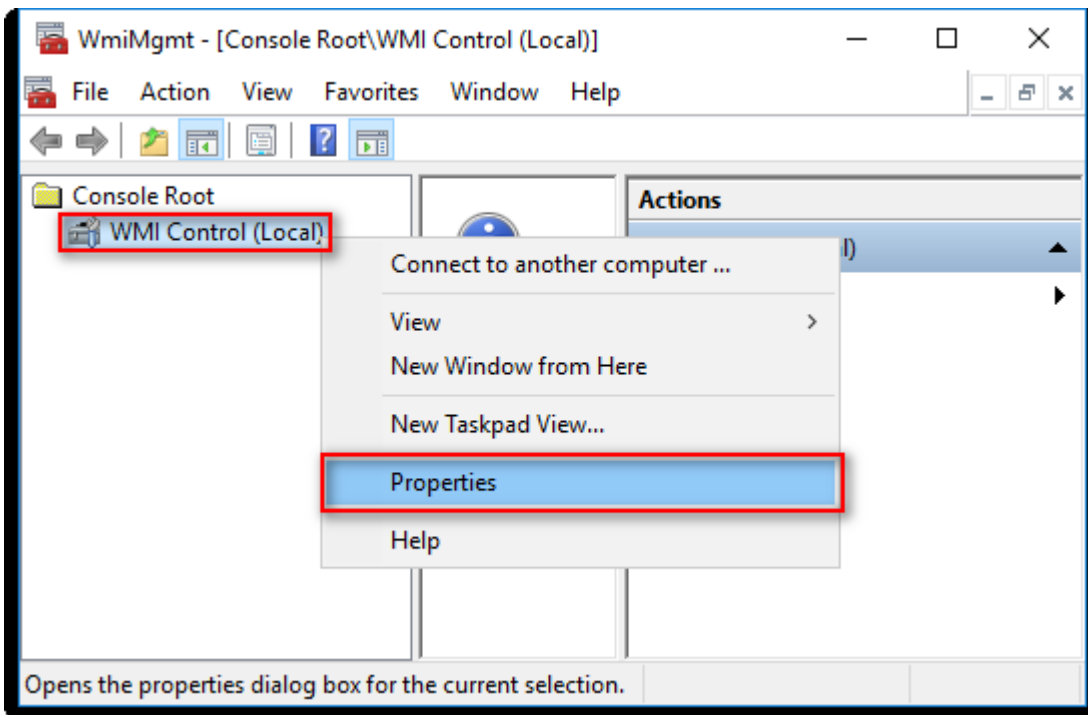
(2) Enter the command to enable component services.

```
PS C:\> wmimgmt.msc
```



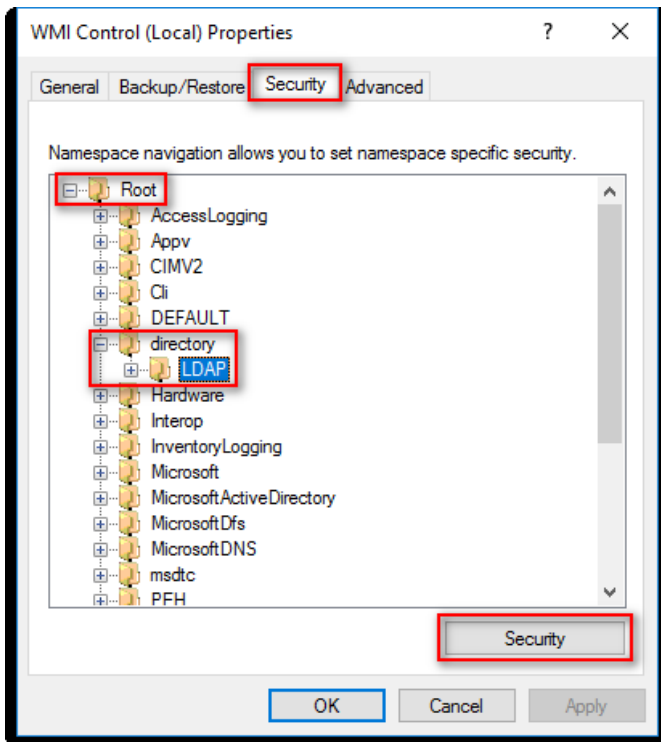
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



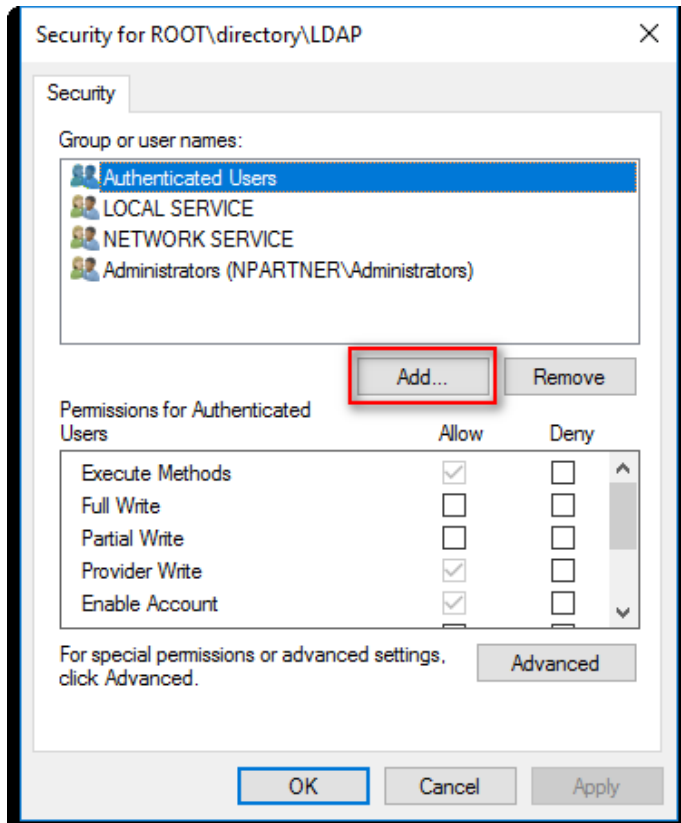
(4) Edit LDAP Security

On the "Security" tab, expand "Root"-> "directory" -> "LDAP," then click "Security."



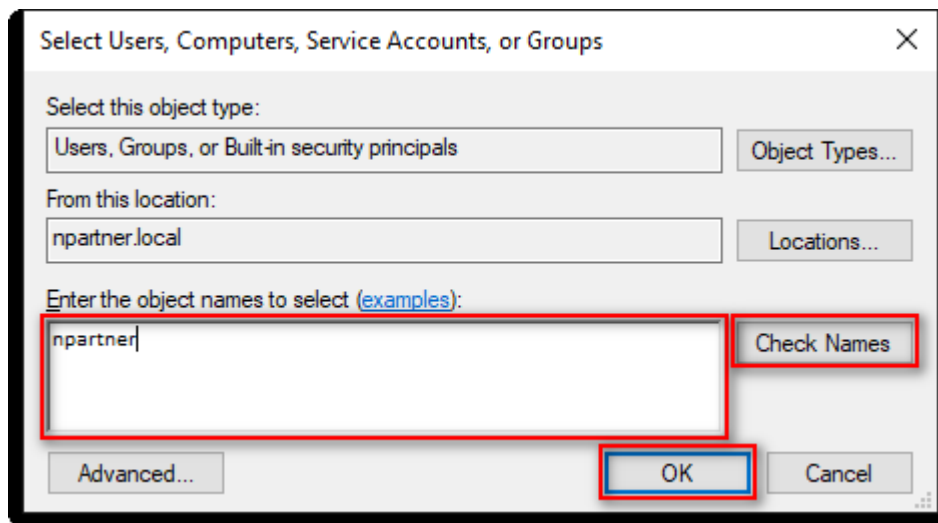
(5) Add WMI User Permissions

Click "Add."



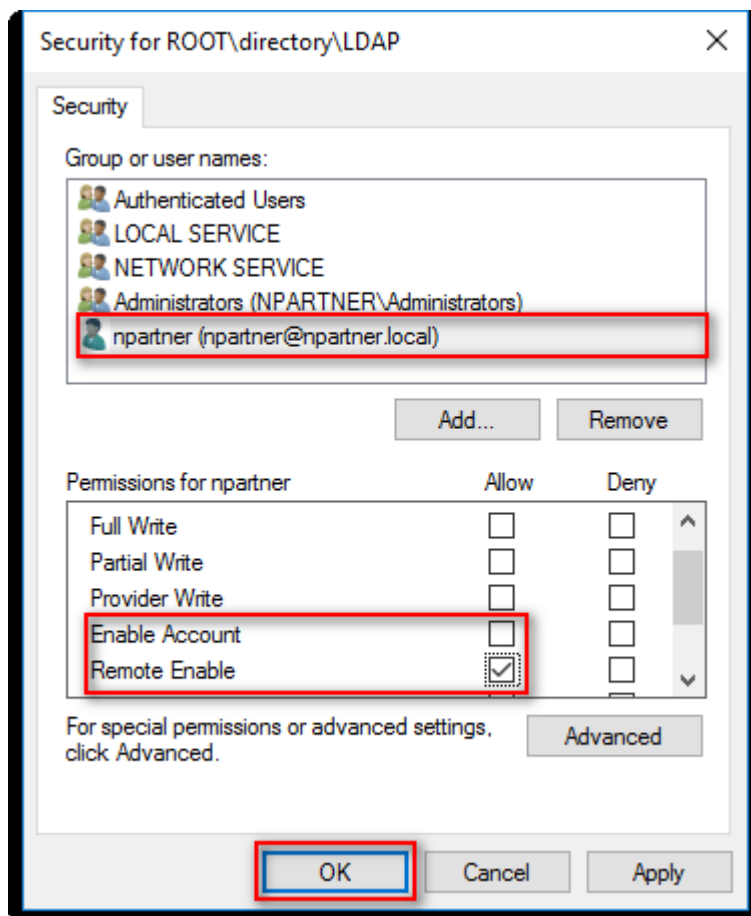
(6) Enter Your Username

Input your user account name (in this example, it is “npartner”), click “Check Names,” then click “OK.”

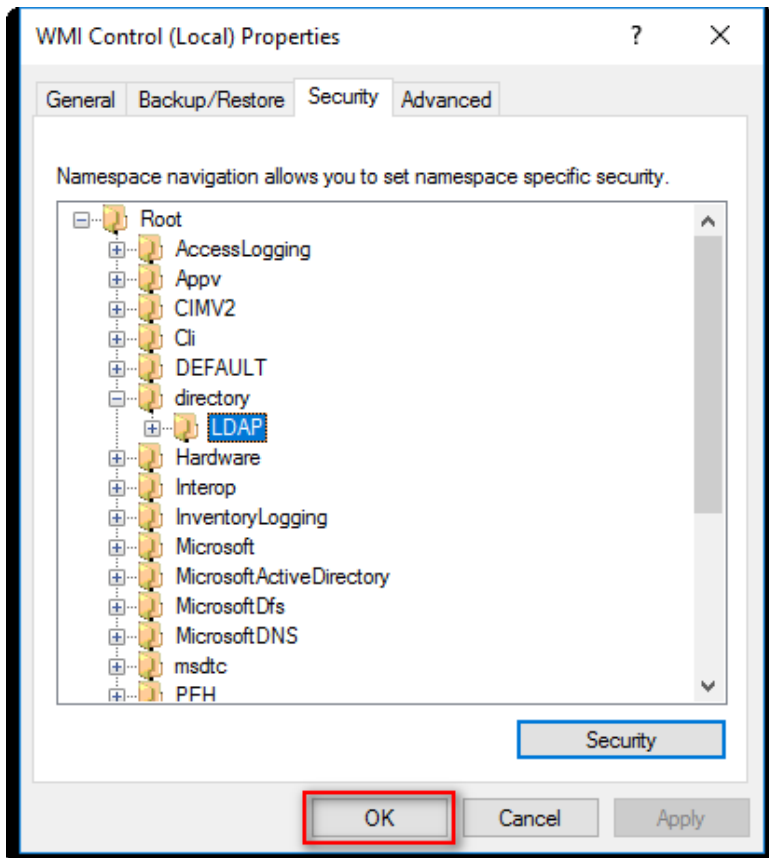


(7) Set Your User Permissions

Select your user account (in this example, it is “npartner”), uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”

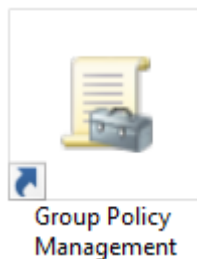


(8) Click "OK."



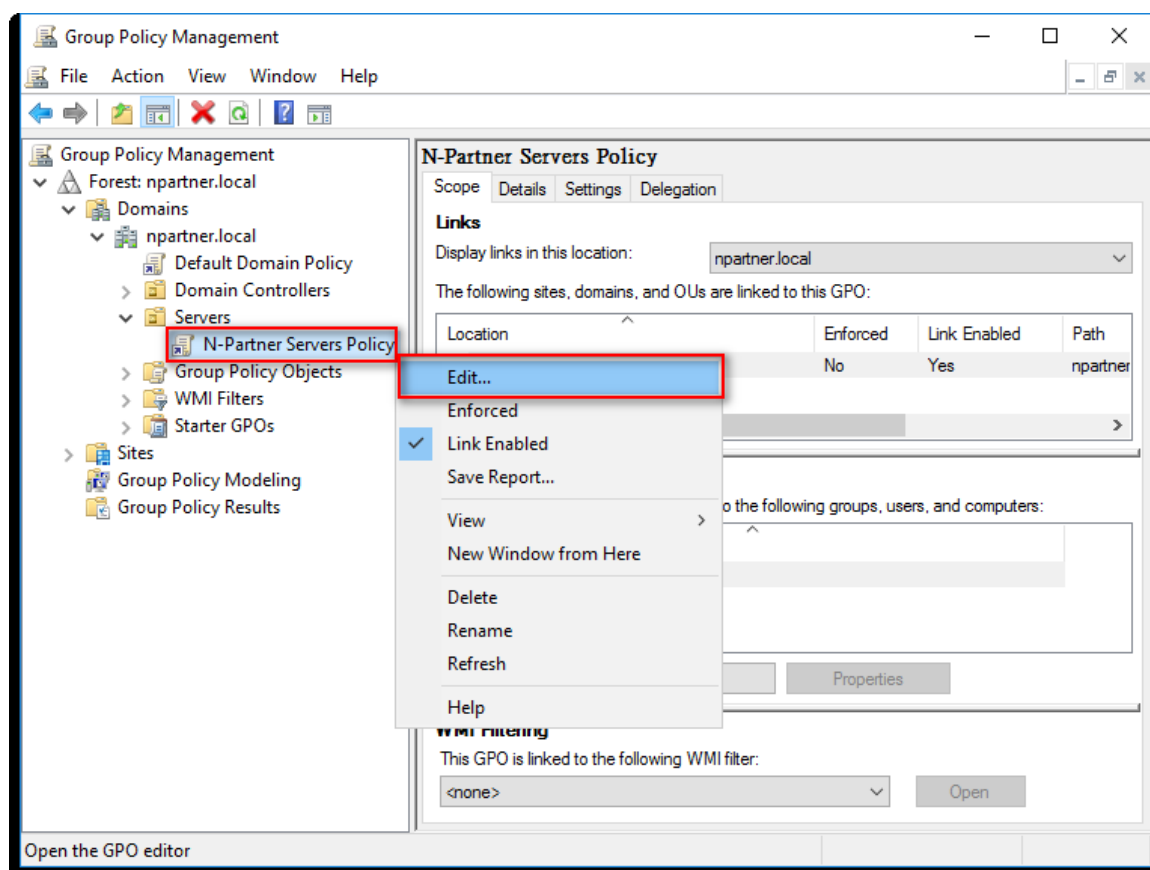
5.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object (GPO)

In the “N-Partner Policy GPO,” right-click and select “Edit.”

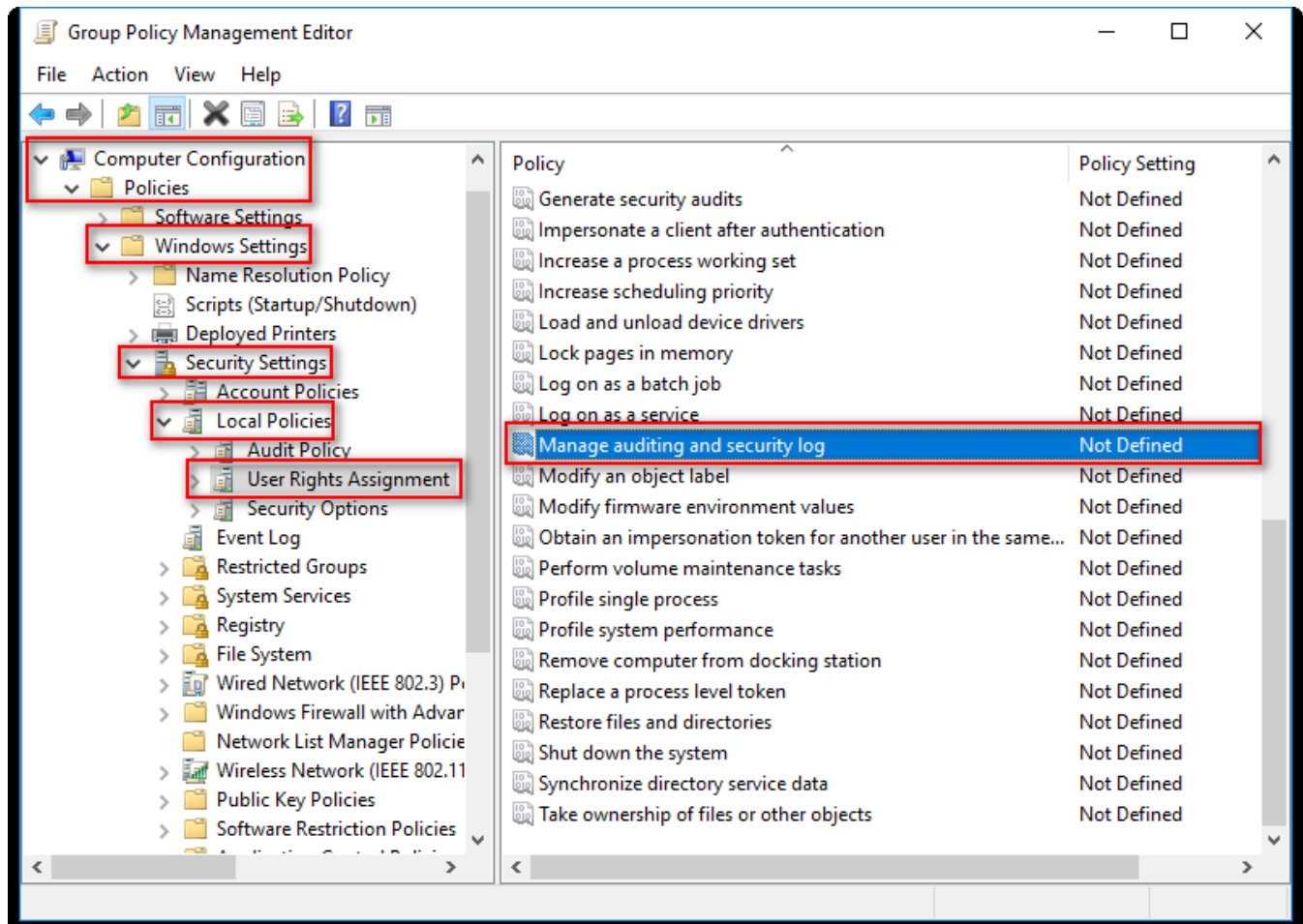


(3) Configure Log Permissions

Navigate to:

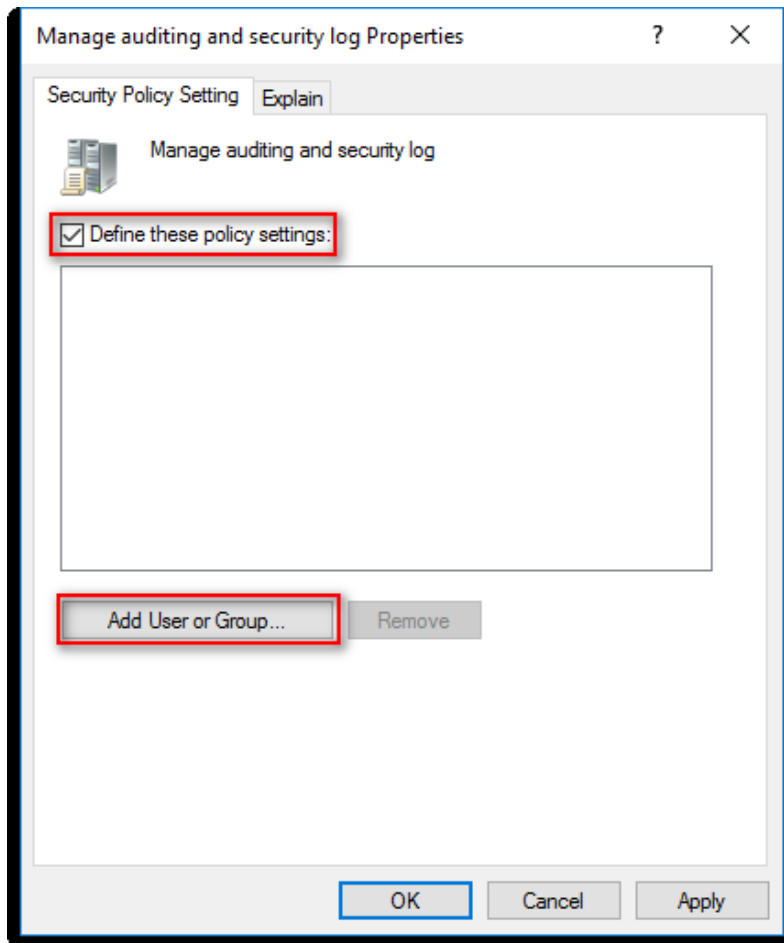
“Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

Select “Manage auditing and security log,” then click  (Properties.)



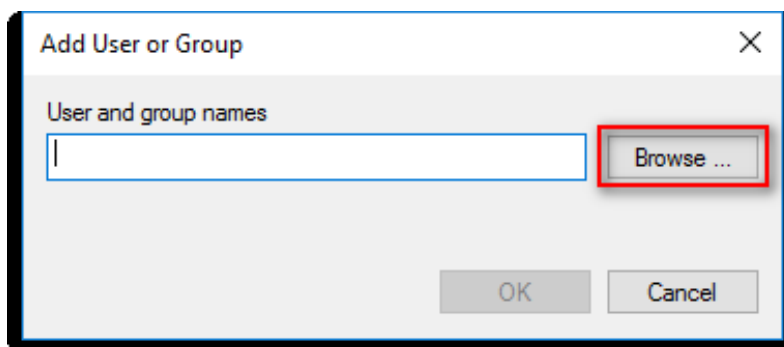
(4) Add Audit Management Users

Select “Define these policy settings,” then click “Add User or Group...”



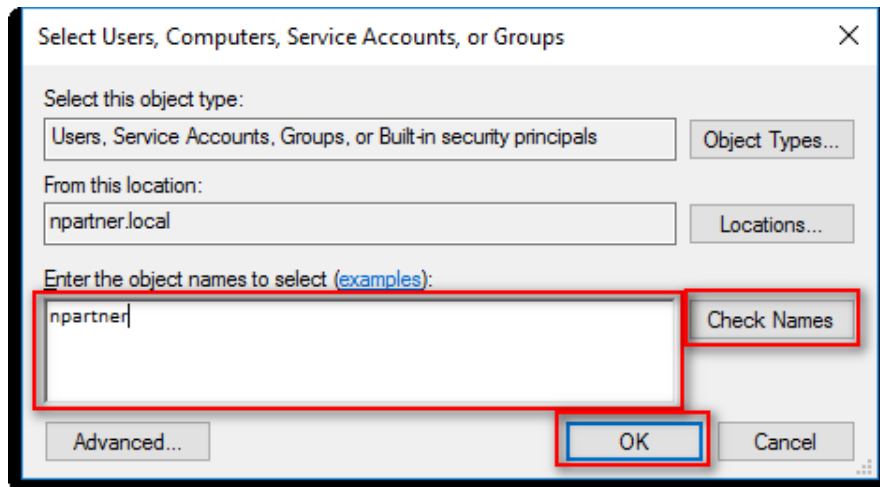
(5) Search for the User

Click “Browse.”



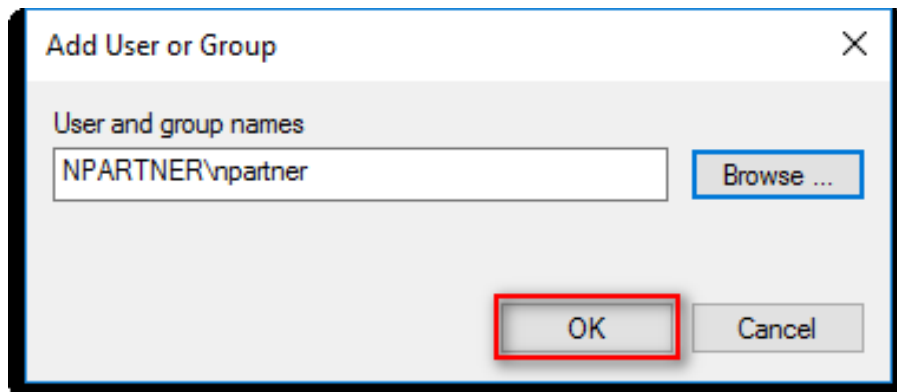
(6) Specify the User

Enter the user account (example: npartner) → click “Check Names” → click “OK.”



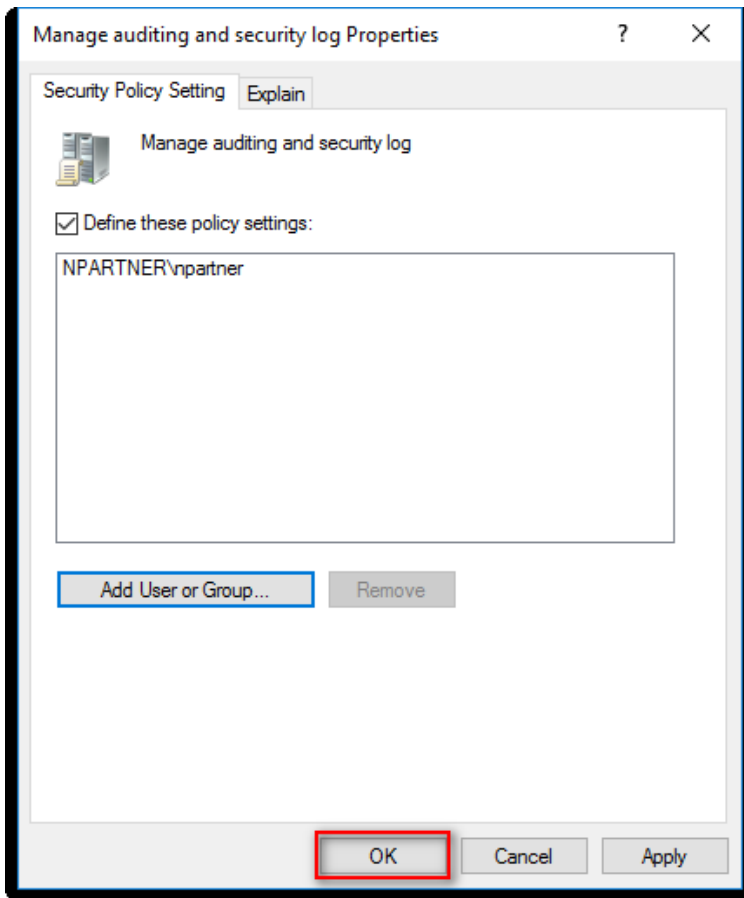
(7) Confirm the User

Click “OK.”



(8) Confirm the Logging Settings

Click "OK" to apply the configuration.

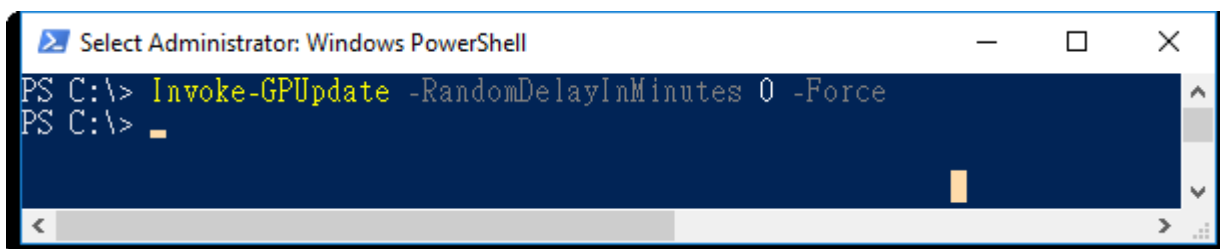


(9) Open "Windows PowerShell."



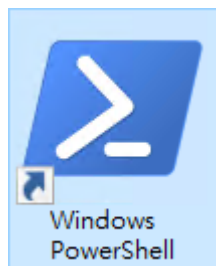
(10) Enter to update group policy:

```
PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
```



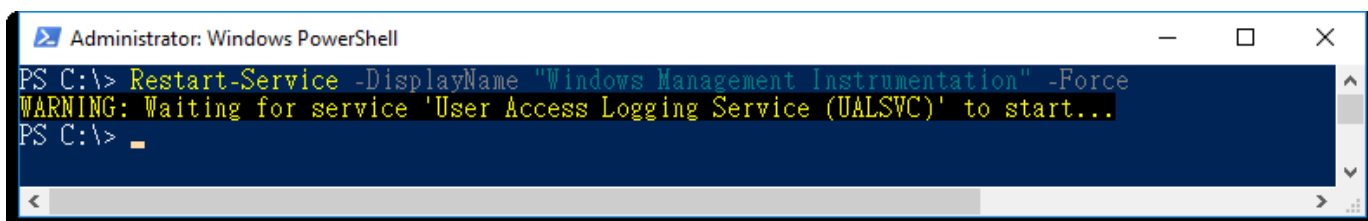
5.3.5 Restart the WMI Service

(1) Open "Windows PowerShell."



(2) Enter the command below to restart the WMI service:

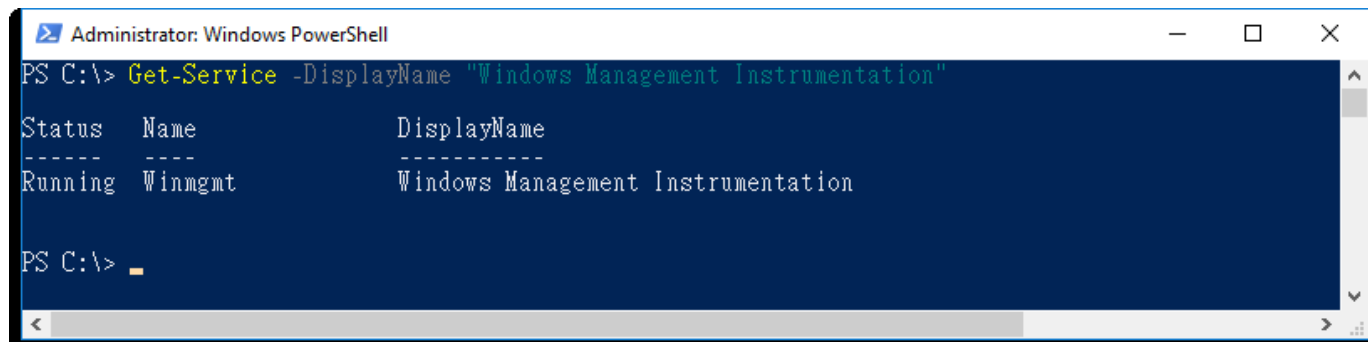
```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```

A screenshot of an Administrator Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The command entered is `Restart-Service -DisplayName "Windows Management Instrumentation" -Force`. The output shows a yellow warning message: `WARNING: Waiting for service 'User Access Logging Service (UALSVC)' to start...`. The prompt `PS C:\>` is visible at the end of the line.

```
Administrator: Windows PowerShell
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
WARNING: Waiting for service 'User Access Logging Service (UALSVC)' to start...
PS C:\>
```

(3) Enter the command below to verify the WMI service status:

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```

A screenshot of an Administrator Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The command entered is `Get-Service -DisplayName "Windows Management Instrumentation"`. The output is a table with three columns: Status, Name, and DisplayName. The status is "Running", the name is "Winmgmt", and the display name is "Windows Management Instrumentation". The prompt `PS C:\>` is visible at the end of the line.

```
Administrator: Windows PowerShell
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"

Status  Name          DisplayName
-----  -
Running Winmgmt       Windows Management Instrumentation

PS C:\>
```

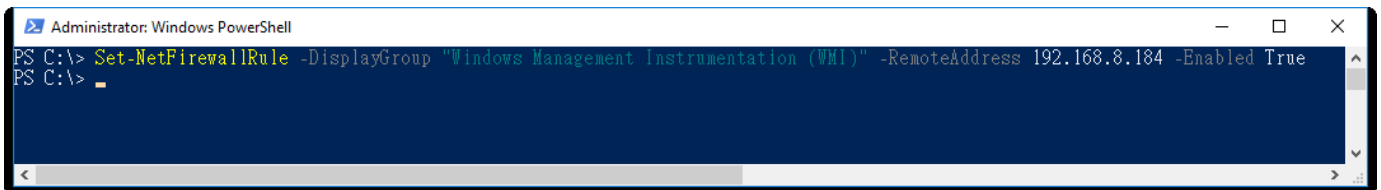
5.4 Configure the Firewall

(1) Open "Windows PowerShell."



(2) Enter the command below to configure the firewall to allow only the N-Reporter IP to query WMI:

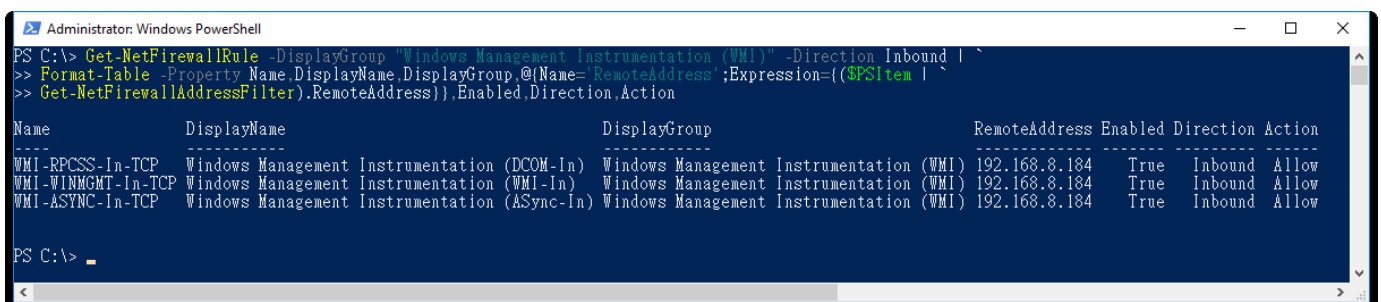
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



Enter the N-Reporter system IP address in the red text.

(3) Enter the command below to verify the WMI firewall rule status:

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={(($PSItem | Get-NetFirewallAddressFilter).RemoteAddress)},
>> Enabled,Direction,Action
```

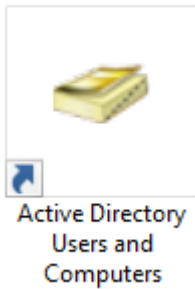


6. Windows 2019

For detailed information on setting Windows audit policies, please refer to the “audit policy recommendations link” in the preface.

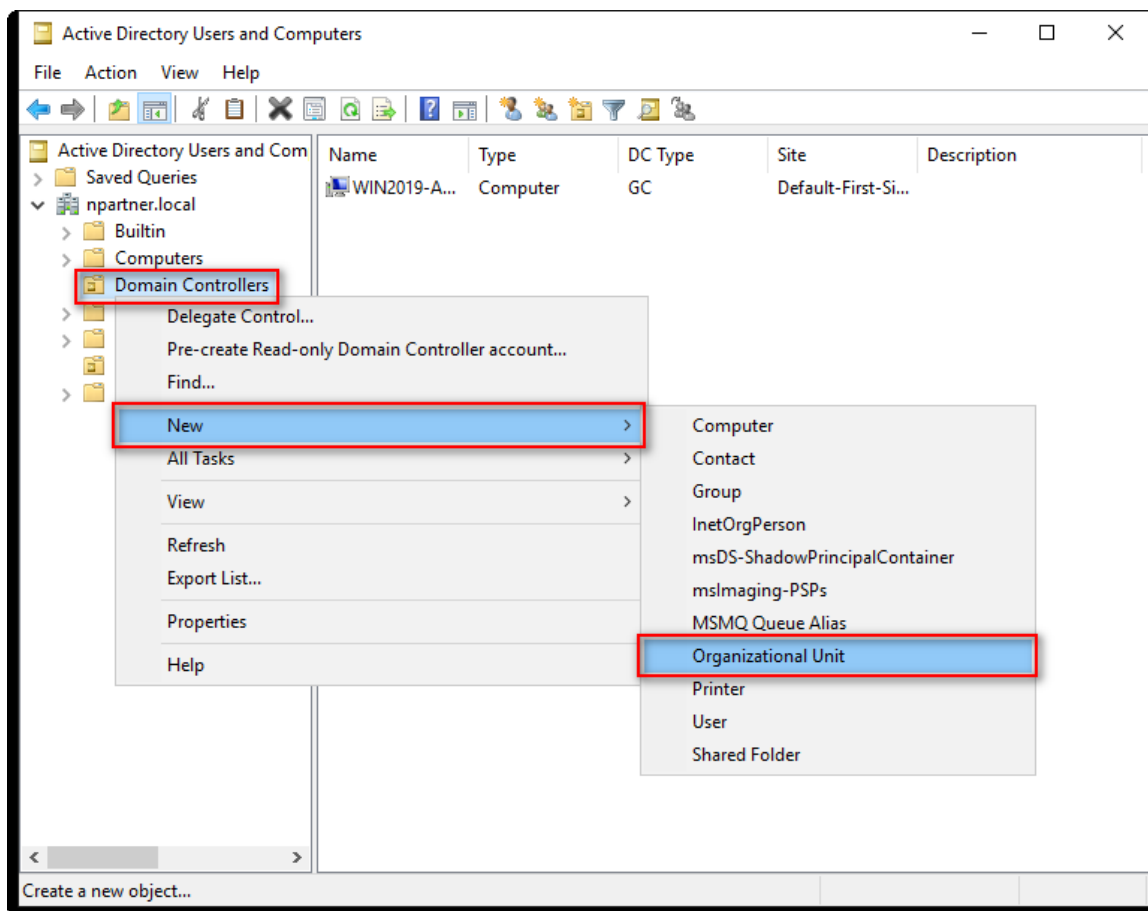
6.1 Organizational Unit Settings

(1) Open “Active Directory Users and Computers.”



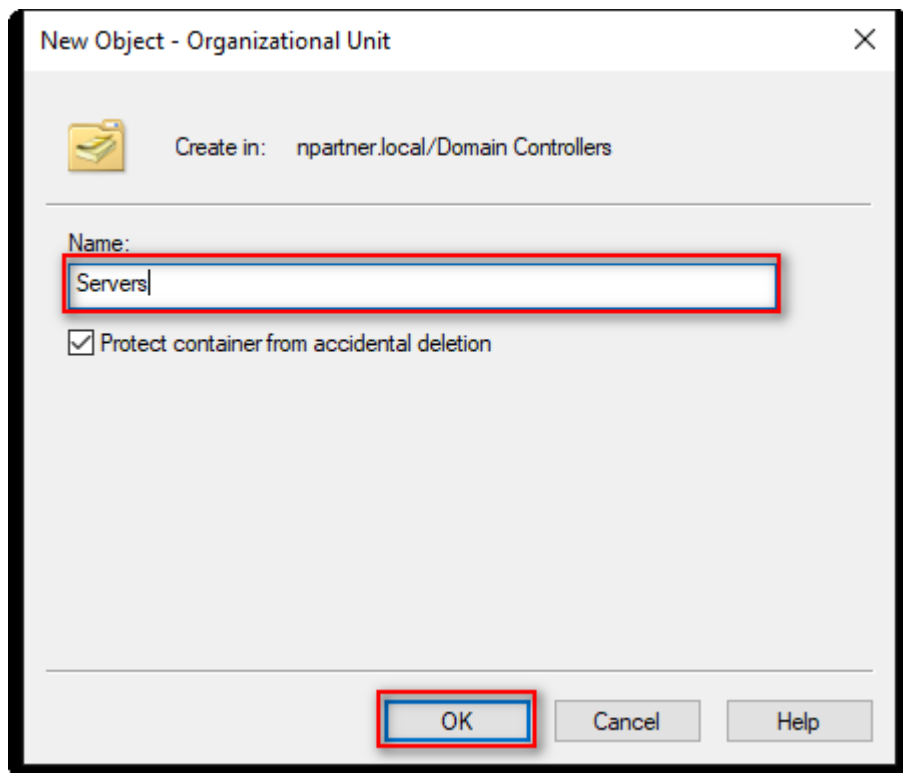
(2) Add an Organizational Unit

Right-click on “Domain Controllers,” select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

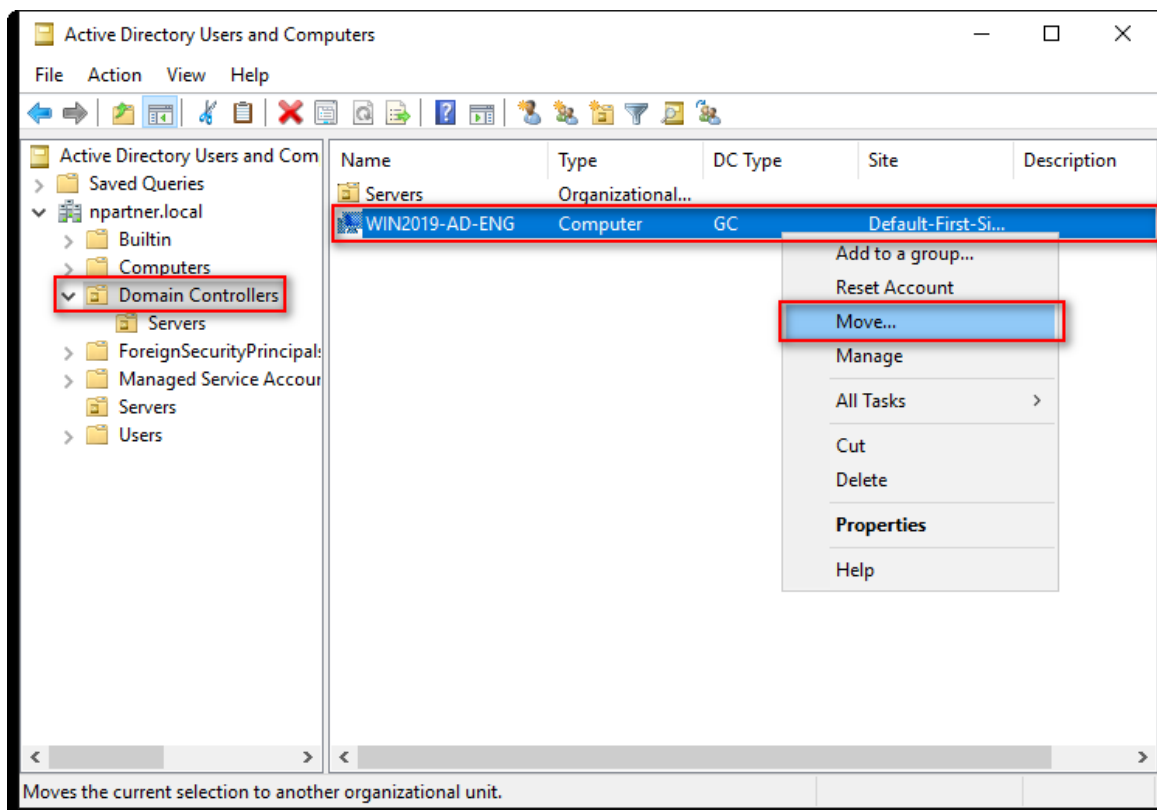
Note: Please create the organizational unit’s name according to the actual environment. -> Click “OK.”



(4) Move the Server to your New Organizational Unit:

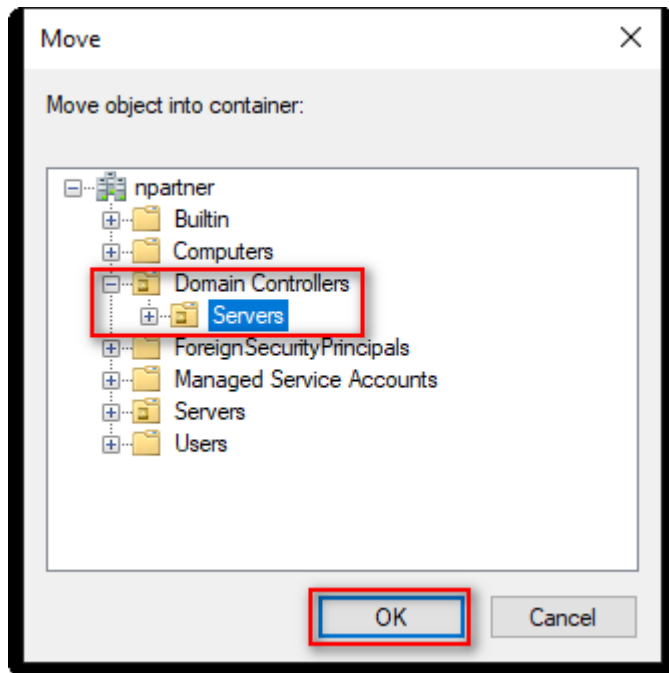
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2019-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



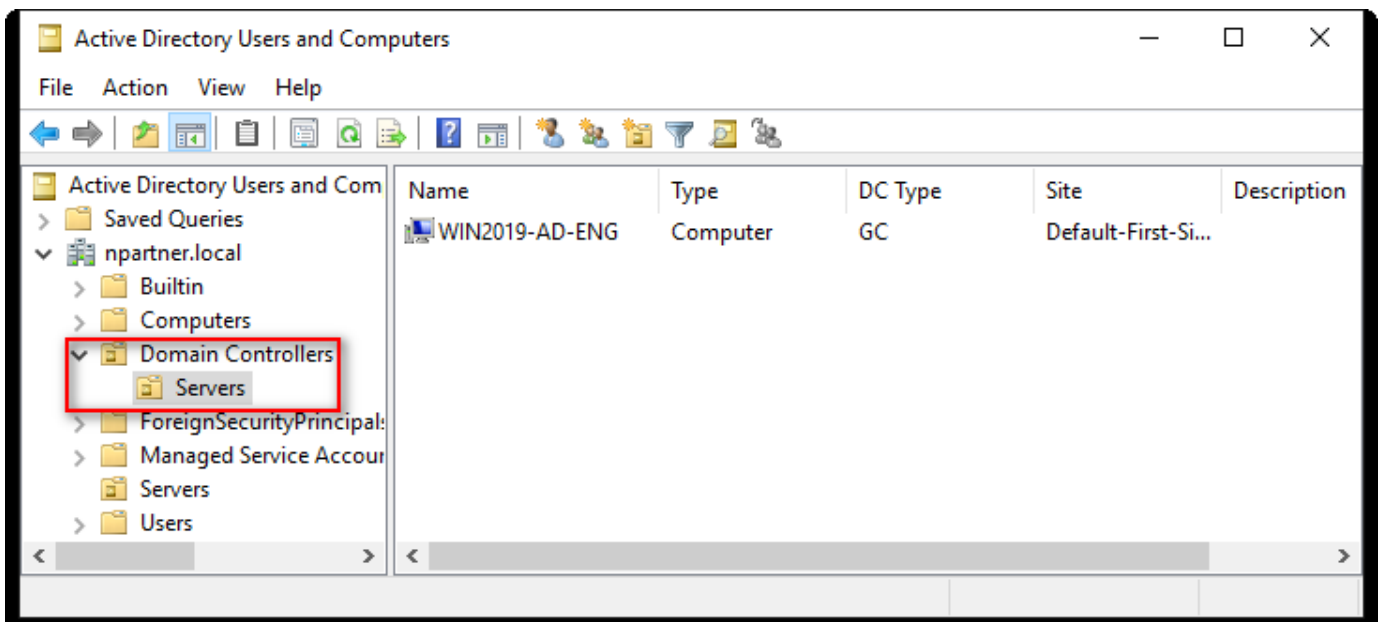
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



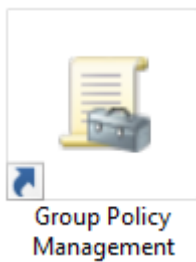
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2019-AD-ENG” server has been moved.

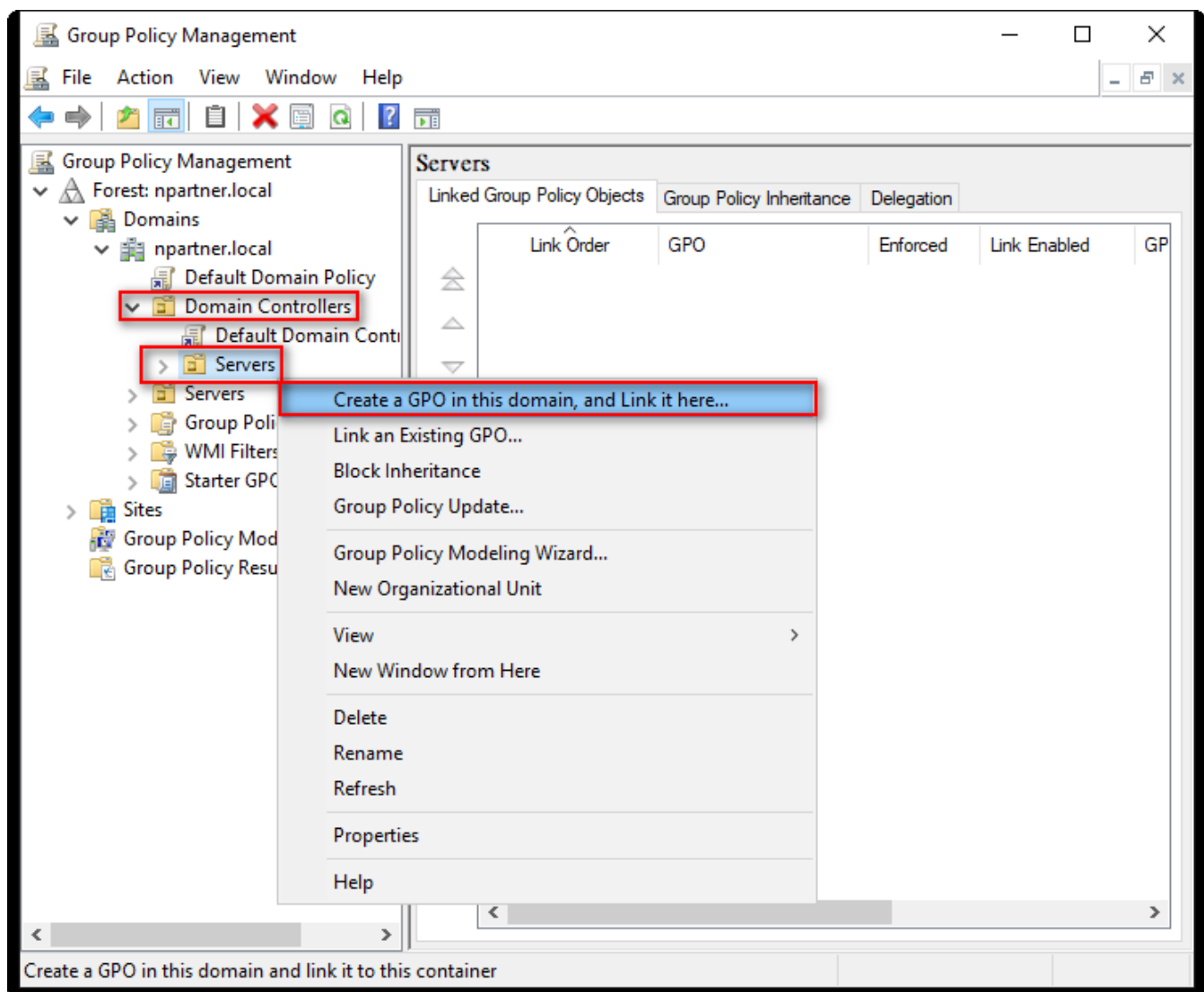


6.2 Group Policy Settings

(1) Click “Group Policy Management.”



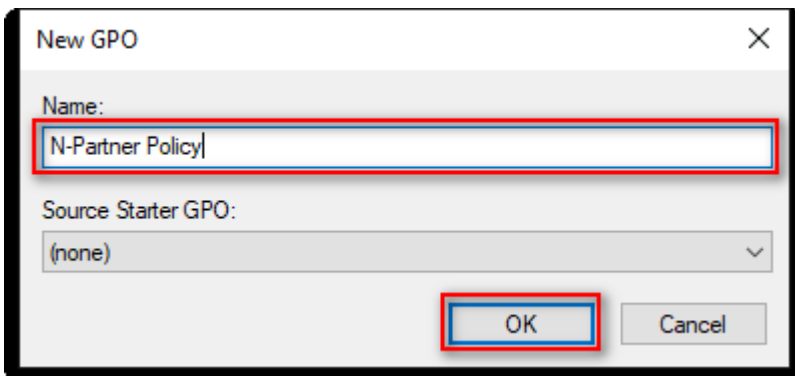
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(3) Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

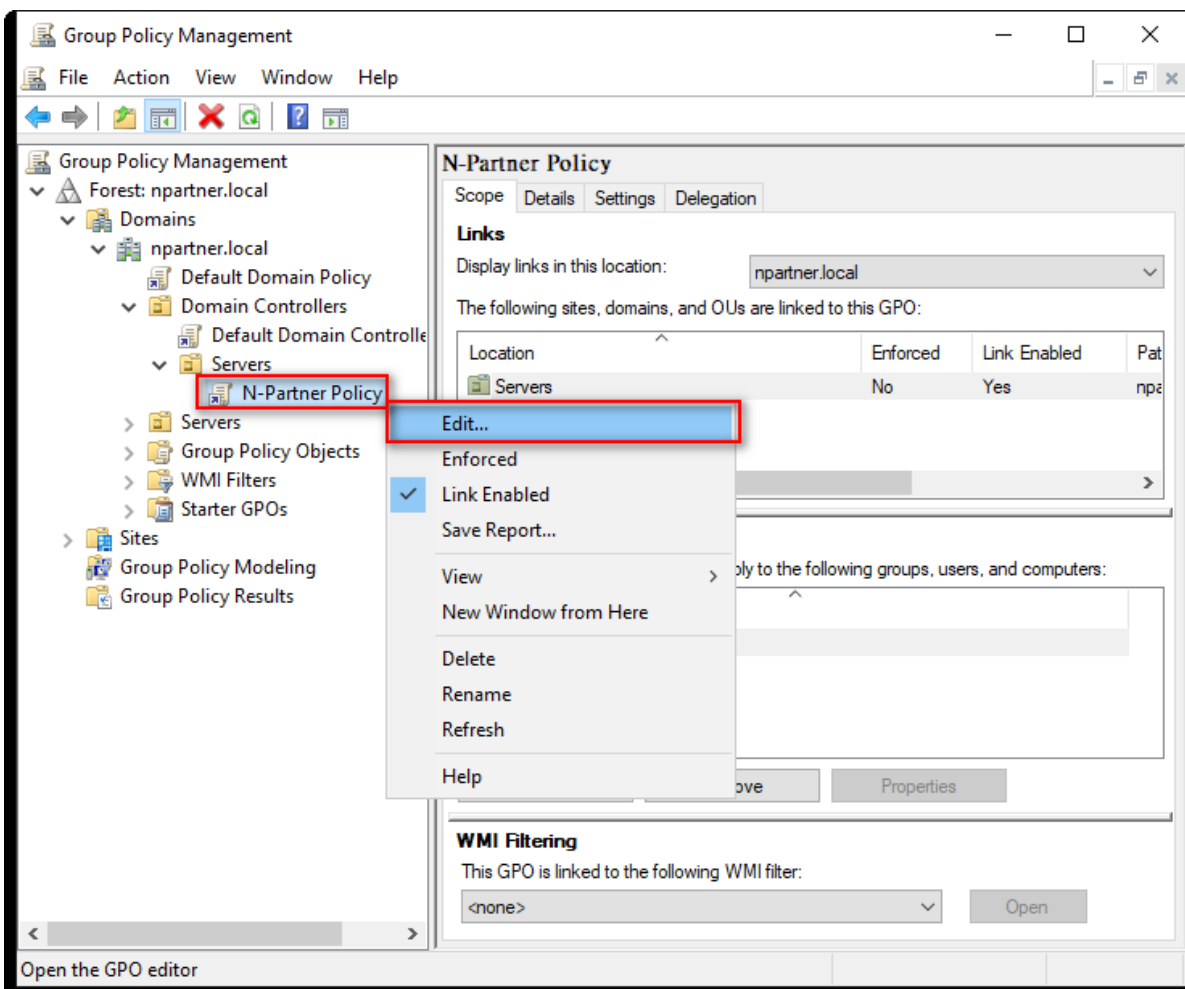
Note: Create your GPO name according to the client's environment.

Then click “OK.”



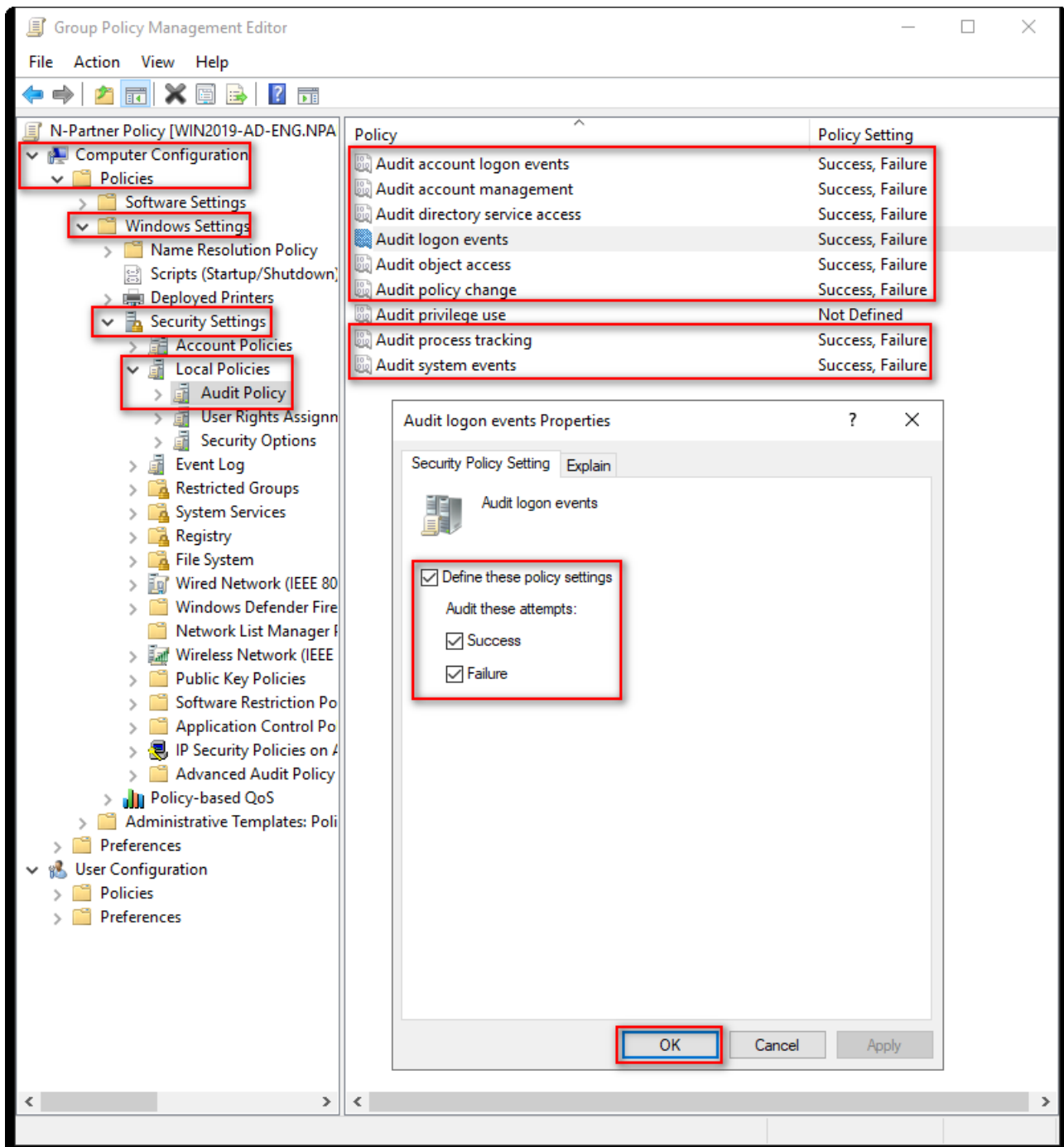
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

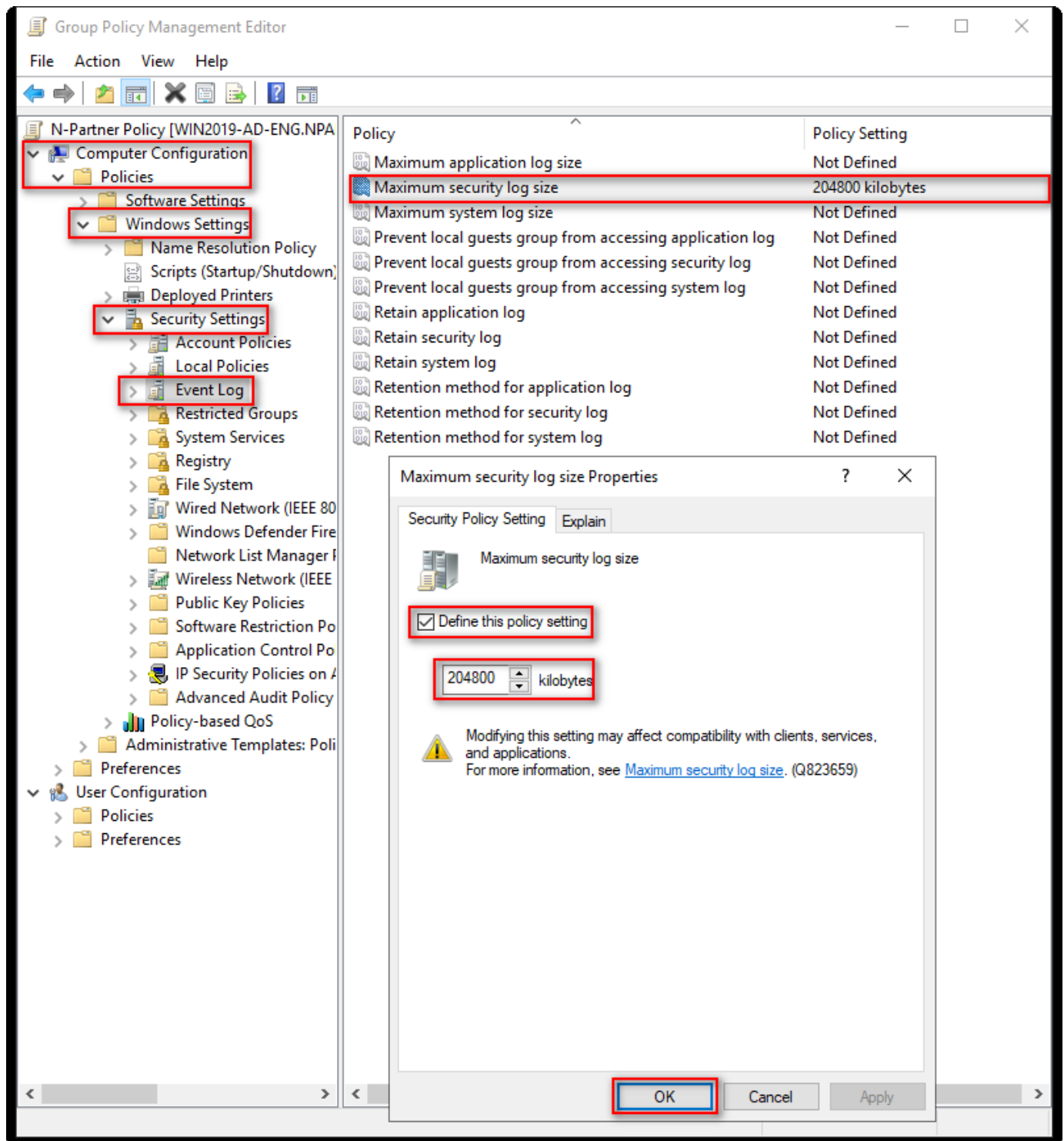
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Maximum Size of Security Log

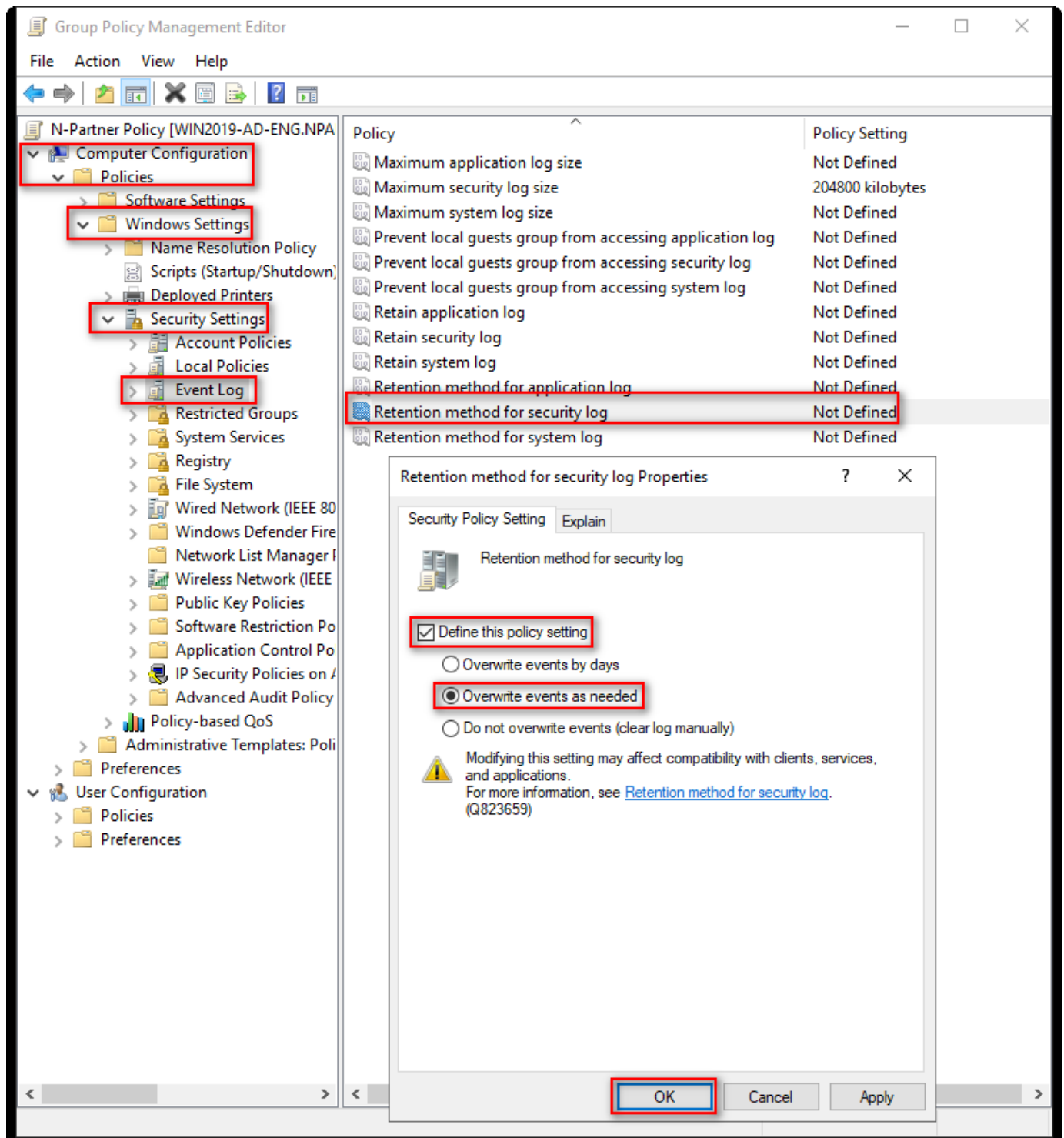
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click “OK.”



(7) Event Logs: Retention Method for Security Log

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”



(8) Open “Windows PowerShell.”



(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Invoke-GPUdate -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt `PS C:\>` is visible before and after the command. The terminal background is dark blue with white text.

(10) Enter the command to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2019-AD-ENG -Path C:\tmp\WIN2019-AD-ENG.html -ReportType html
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Get-GPResultantSetofPolicy -Computer WIN2019-AD-ENG -Path C:\tmp\WIN2019-AD-ENG.html -ReportType html` being entered and executed. The output of the command is displayed as follows:
`RsopMode : Logging`
`Namespace : \\WIN2019-AD-ENG\Root\Rsop\NS503302C9_DE9C_4C74_9A9B_9D92FD1A8182`
`LoggingComputer : WIN2019-AD-ENG`
`LoggingUser : NPARTNER\administrator`
`LoggingMode : Computer`
The terminal background is dark blue with white text.

For the red text , please enter the Windows AD server name and the folder path/file name.

(11) Open the report and verify that the Windows AD server is applying the N-Partner Policy Group Policy.

Policy	Setting	Winning GPO
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
Account Policies/Account Lockout Policy		
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
Account Policies/Kerberos Policy		
Enforce user logon restrictions	Enabled	Default Domain Policy
Maximum lifetime for service ticket	600 minutes	Default Domain Policy
Maximum lifetime for user ticket	10 hours	Default Domain Policy
Maximum lifetime for user ticket renewal	7 days	Default Domain Policy
Maximum tolerance for computer clock synchronization	5 minutes	Default Domain Policy
Local Policies/Audit Policy		
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit directory service access	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit policy change	Success, Failure	N-Partner Policy
Audit process tracking	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
Local Policies/User Rights Assignment		

6.3 Add a Non-Admin Account

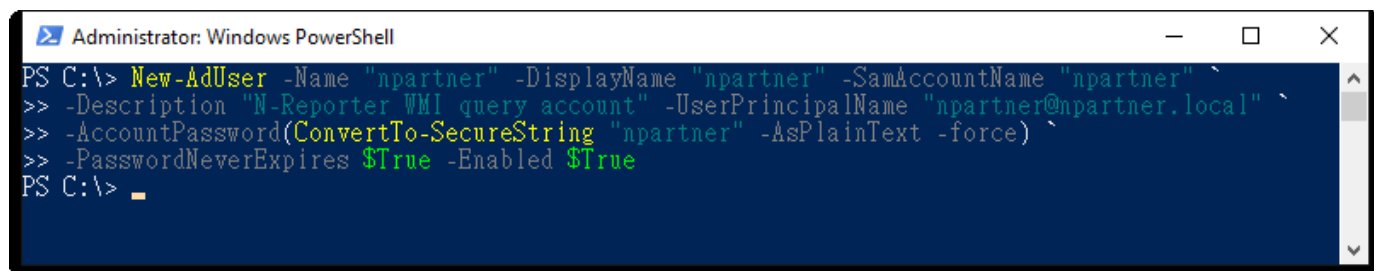
6.3.1 Add Users

(1) Open "Windows PowerShell."



(2) Enter the command below to add a new account.

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

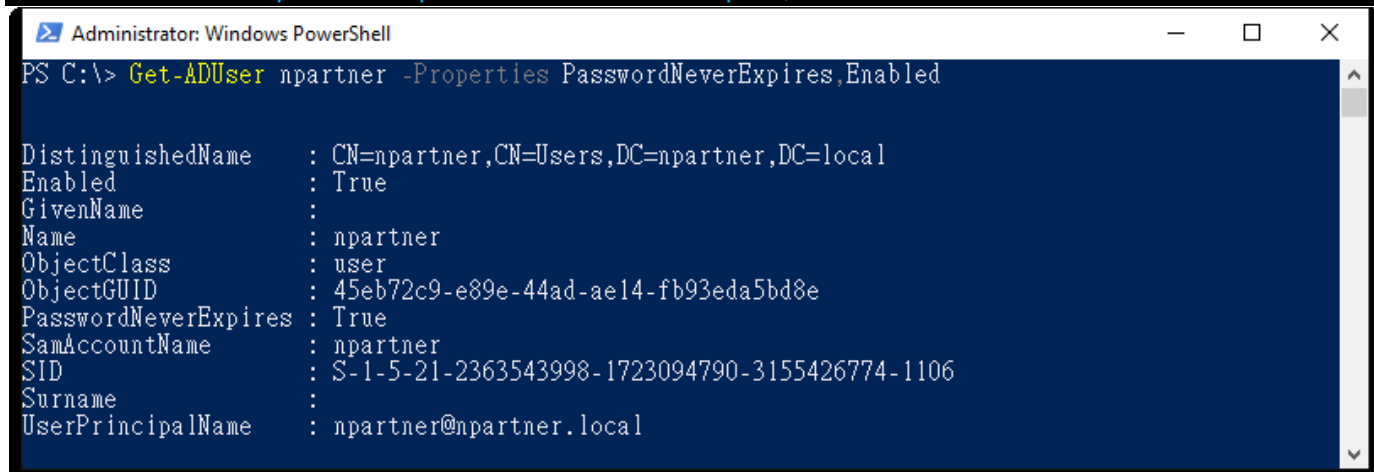
A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the New-AdUser command with the following output:

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword(ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
PS C:\> _
```

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the execution of the Get-ADUser command with the following output:

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName              :
Name                   : npartner
ObjectClass             : user
ObjectGUID              : 45eb72c9-e89e-44ad-ae14-fb93eda5bd8e
PasswordNeverExpires   : True
SamAccountName          : npartner
SID                     : S-1-5-21-2363543998-1723094790-3155426774-1106
Surname                 :
UserPrincipalName       : npartner@npartner.local
```

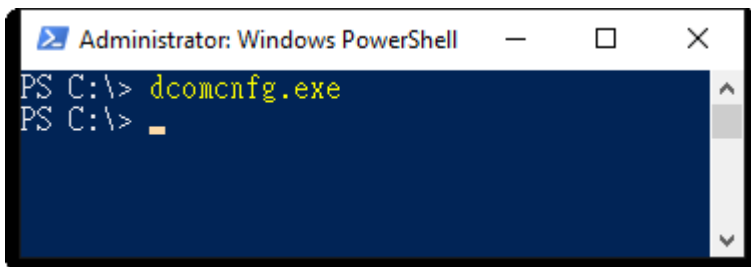
6.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”



(2) Open “Component Services.”

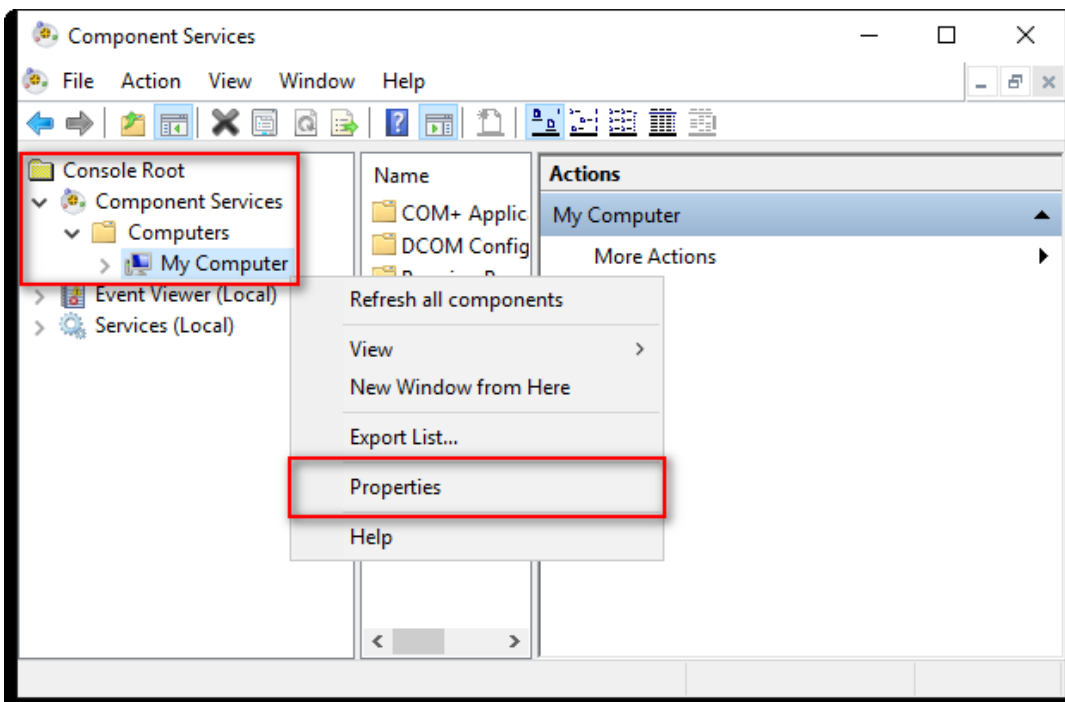
```
PS C:\> dcomcnfg.exe
```



(3) Edit Computer Properties

Expand “Console Root → Component Services → Computers.”

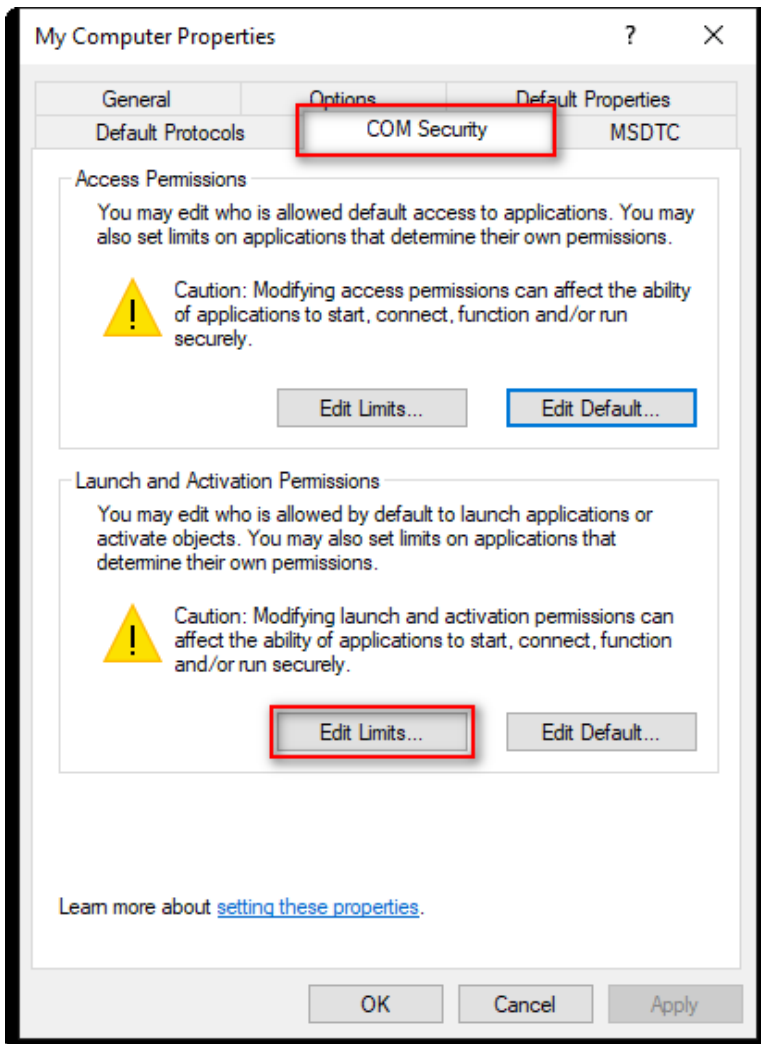
Right-click “My Computer” → select “Properties.”



(4) Enable Permissions

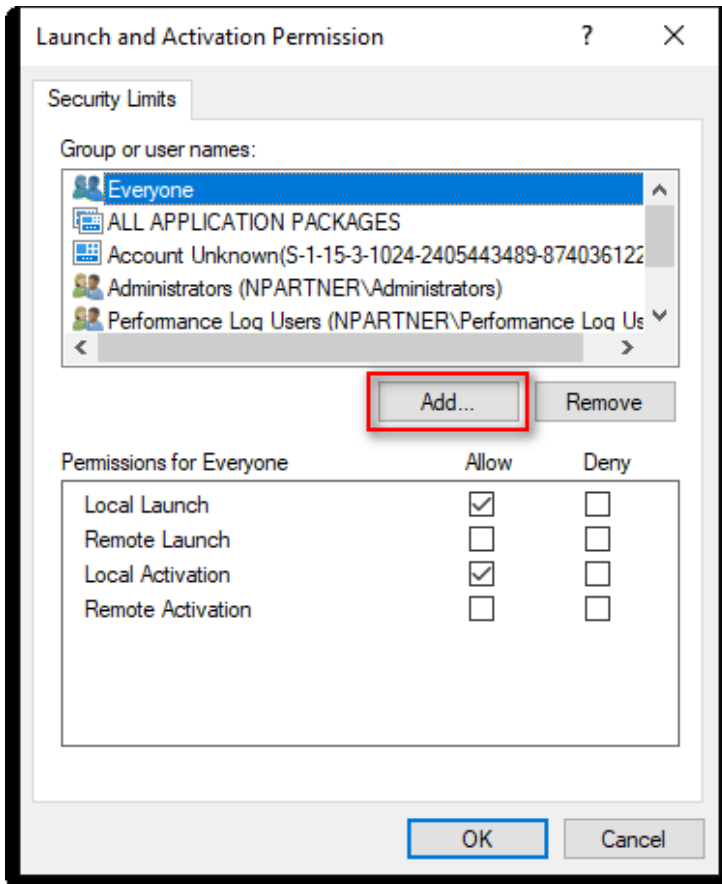
Go to the COM Security tab.

Under Launch and Activation Permissions, click Edit Limits.



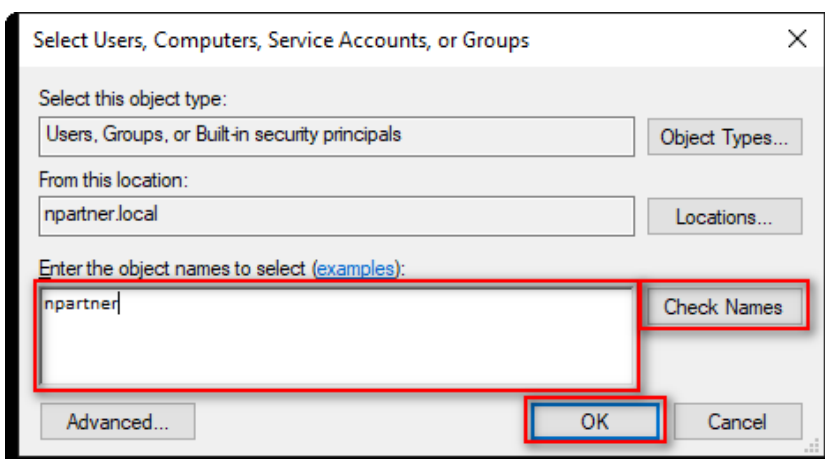
(5) Add DCOM User Permissions

Click "Add."



(6) Specify the User

Enter the user account (example: npartner) → click "Check Names" → click "OK."

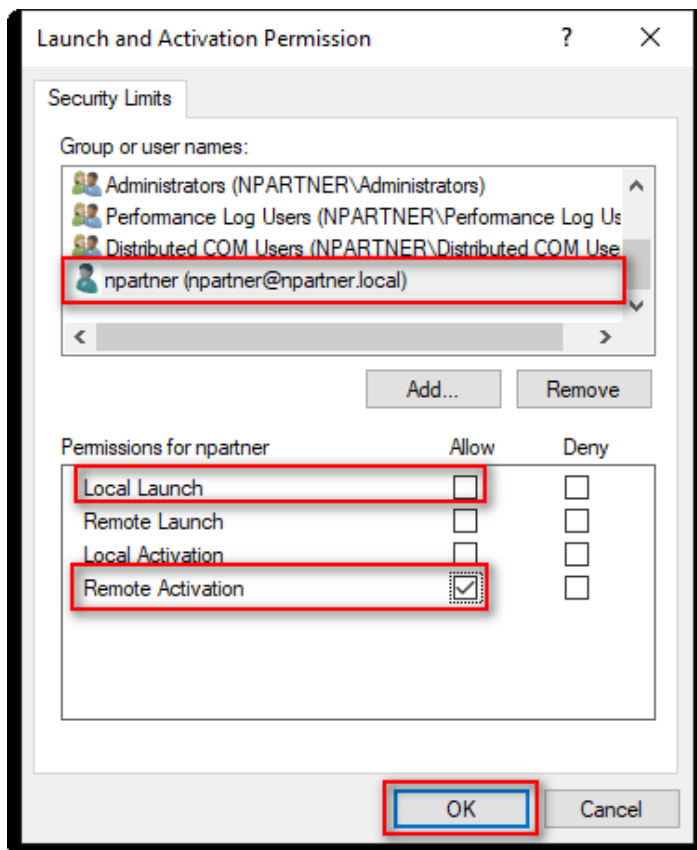


(7) Configure User Permissions

Select the user account (**npartner**):

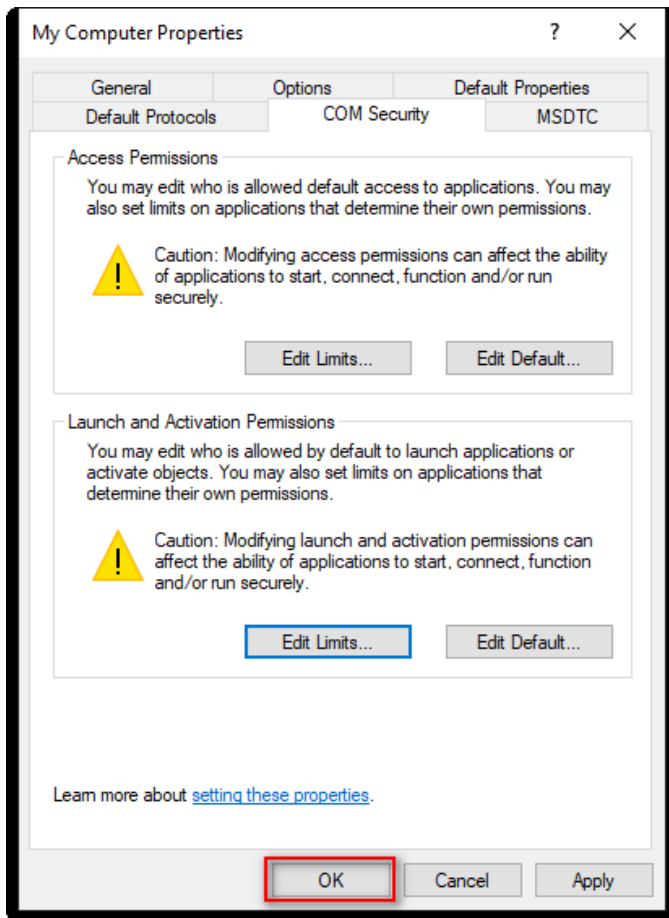
- Clear **Local Launch: Allow**
- Select **Remote Activation: Allow**

Click **OK**.



(8) Confirm User Permissions

Click "OK" to apply the settings.



6.3.3 Configure WMI Permissions

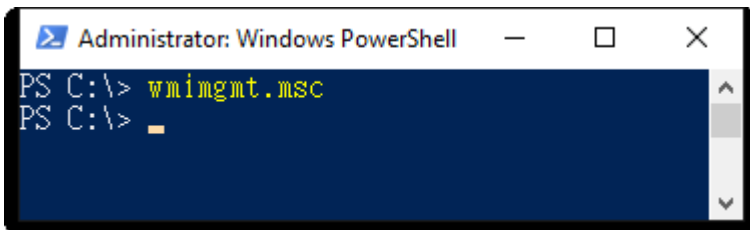
6.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”



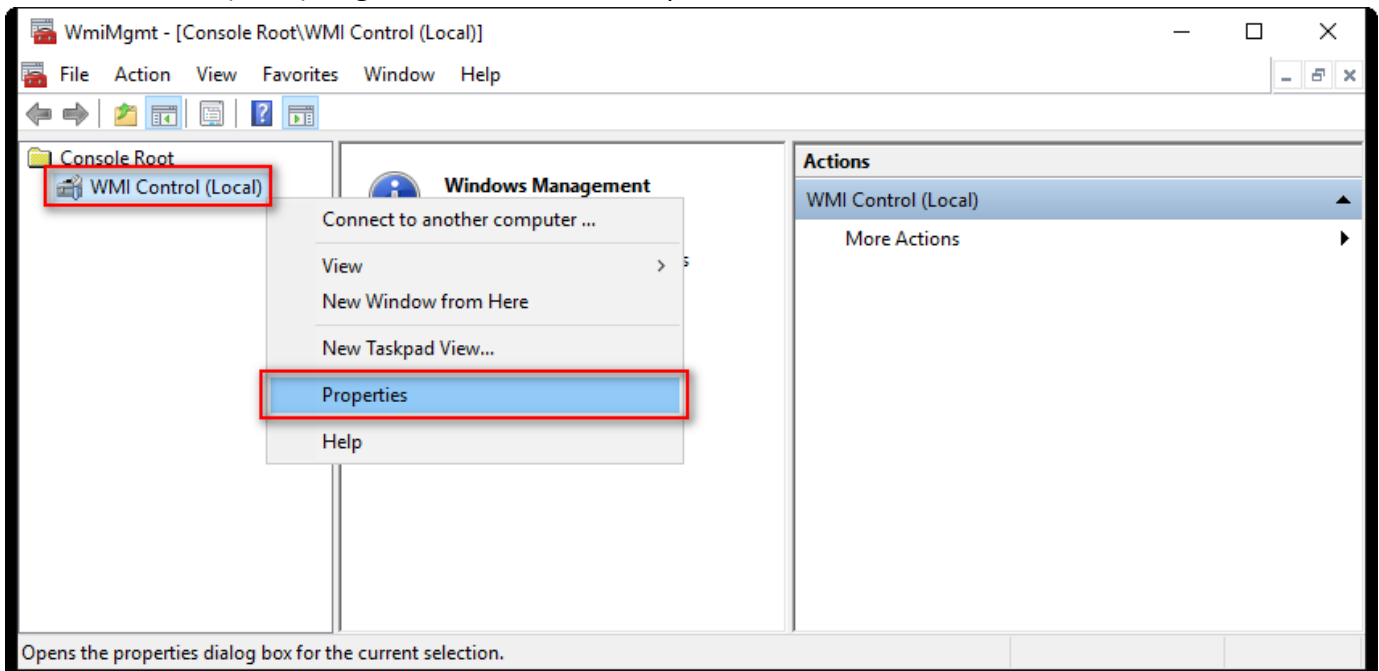
(2) Enter the command below to enable component services.

```
PS C:\> wmicmgmt.msc
```



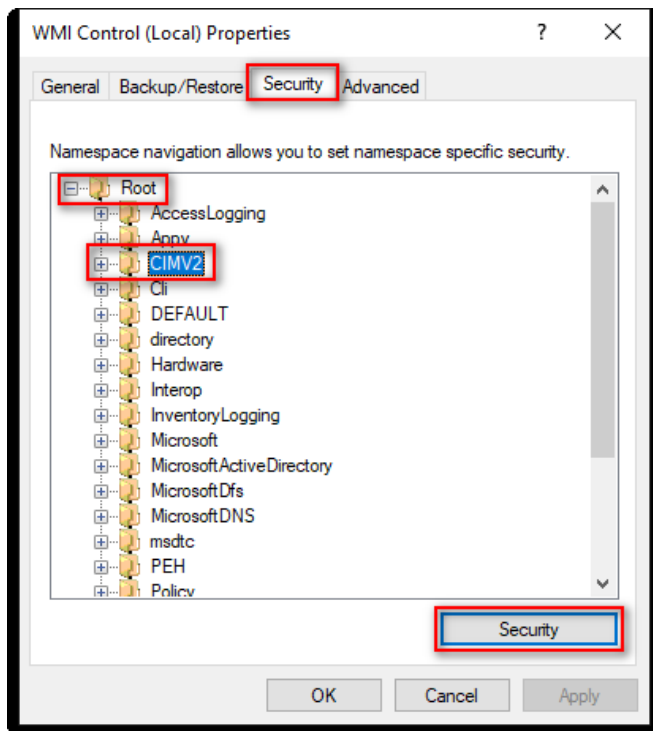
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



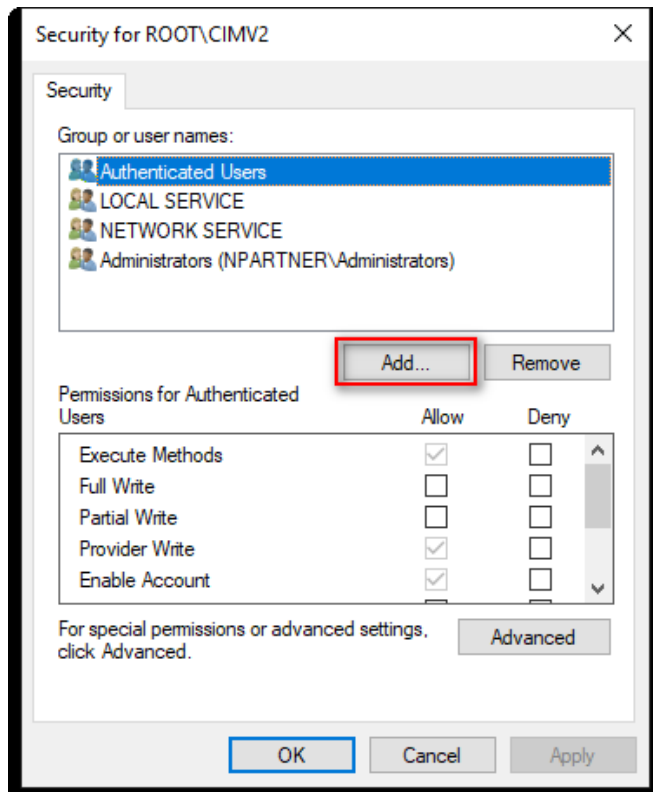
(4) Edit CIMV2 Security

On the "Security" tab, expand folder "Root" -> "CIMV2," then click "Security."



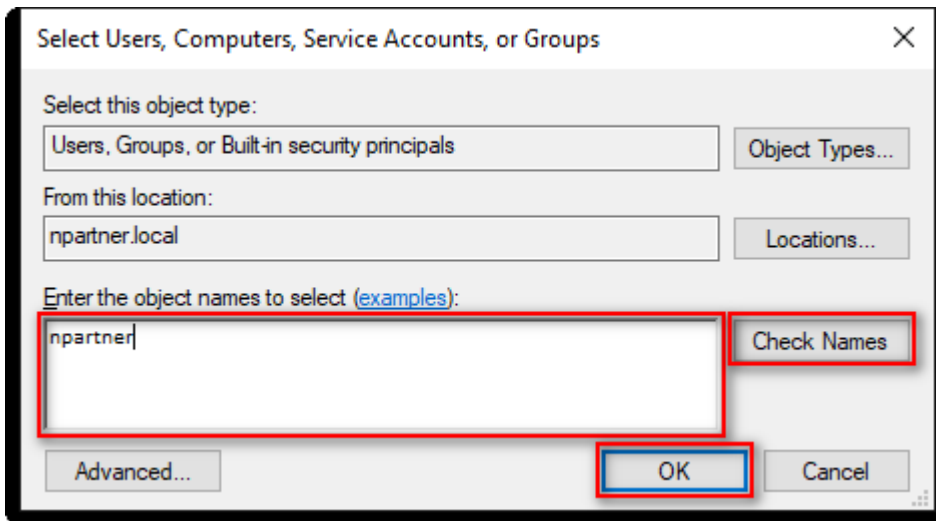
(5) Add WMI User Permissions

Click "Add."



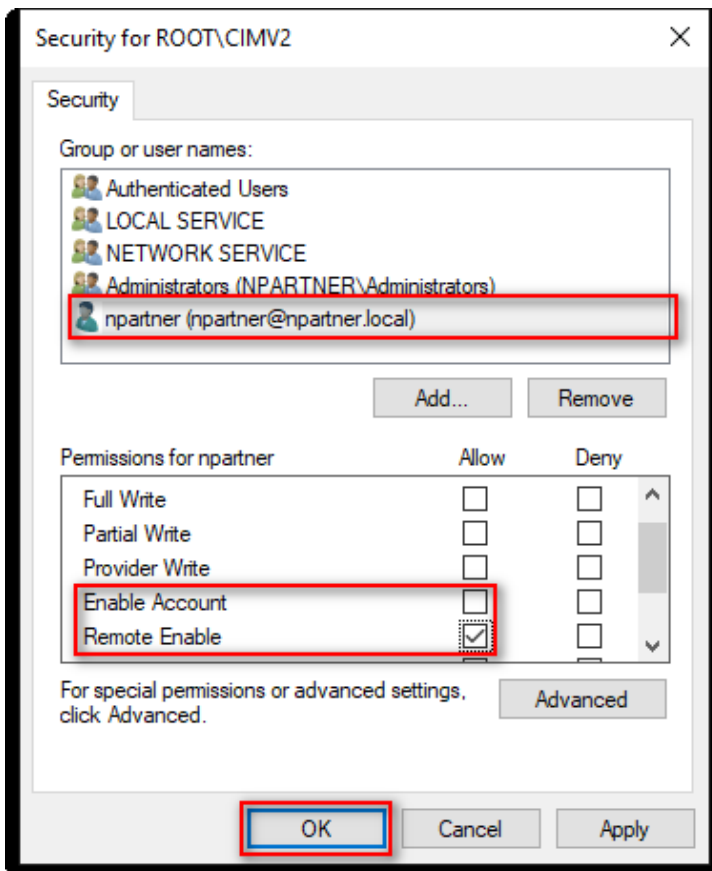
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”



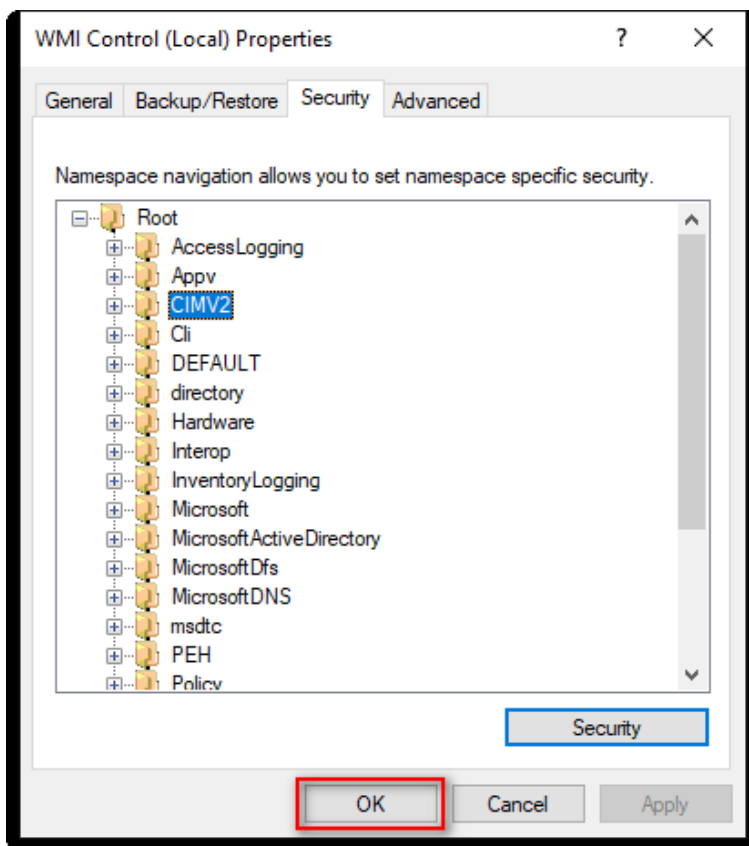
(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Confirm User Permissions

Click "OK."



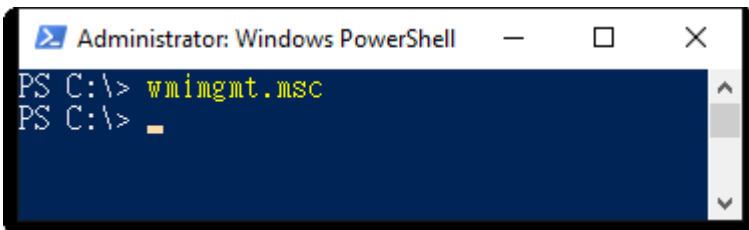
6.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”



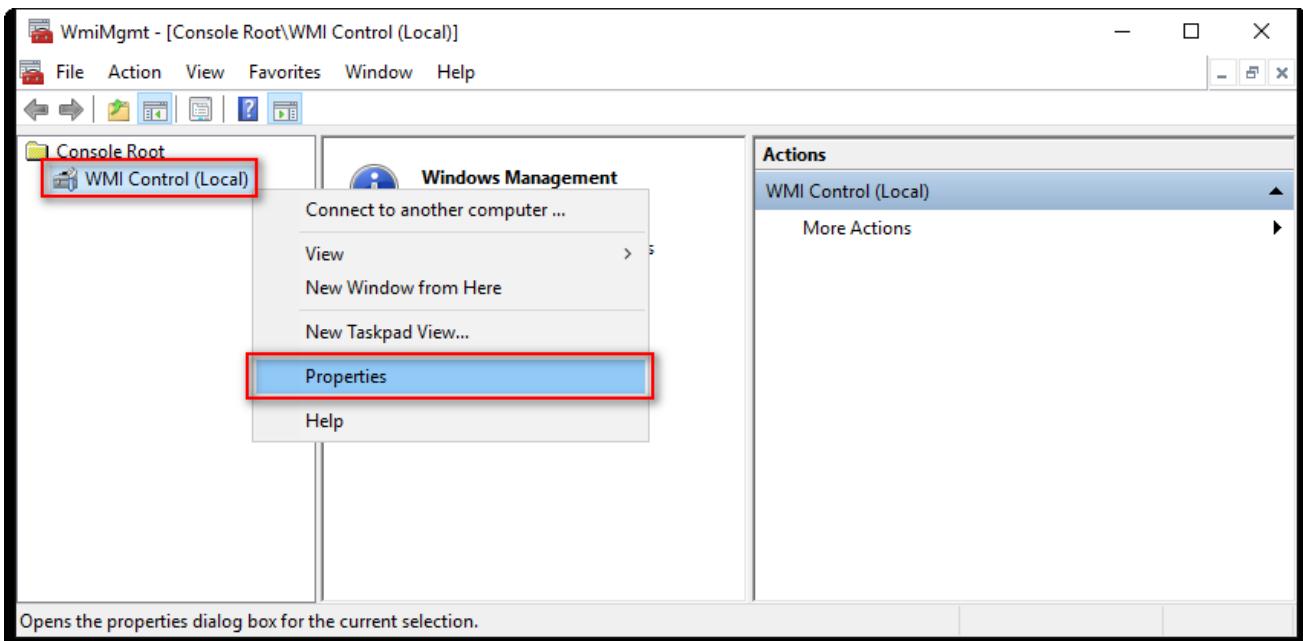
(2) Open “WMI Control.”

```
PS C:\> wmicmgmt.msc
```



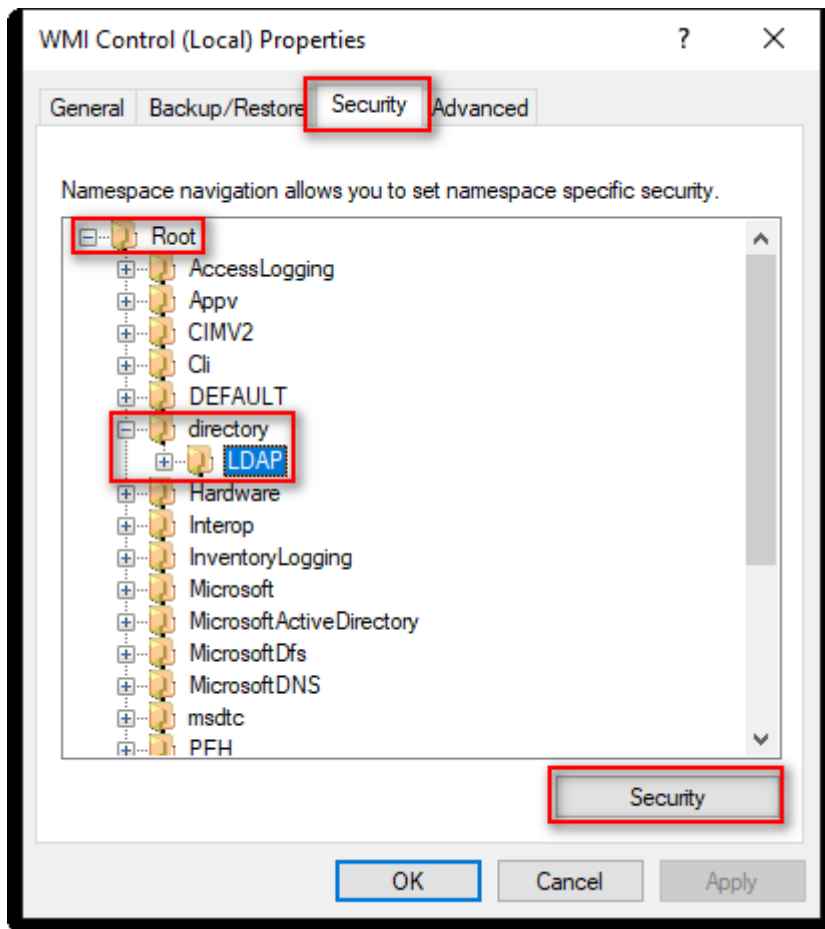
(3) Edit WMI Control

Right-click WMI Control (Local) → select “Properties.”



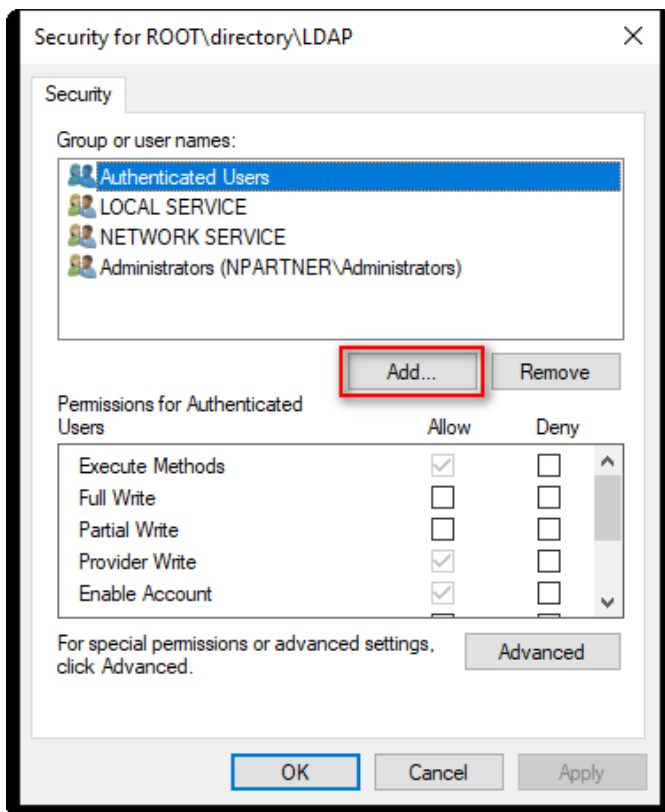
(4) Edit LDAP Security

Go to the “Security tab → expand Root → directory → LDAP” → click “Security.”



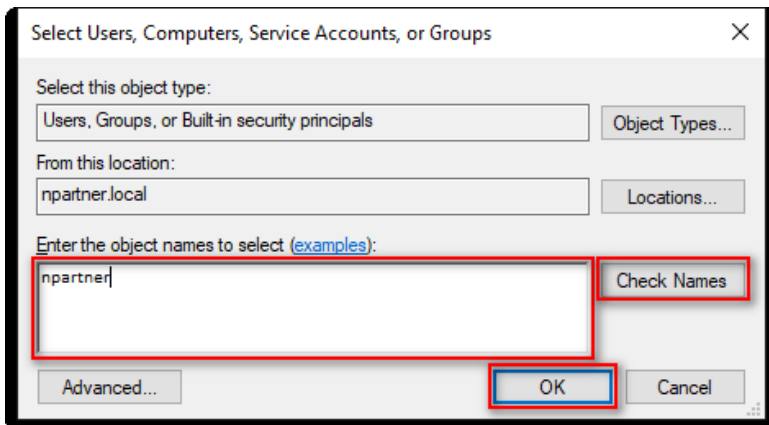
(5) Add WMI User Permissions

Click "Add."



(6) Specify the User

Enter the user account (example: npartner) → click “Check Names” → click “OK.”

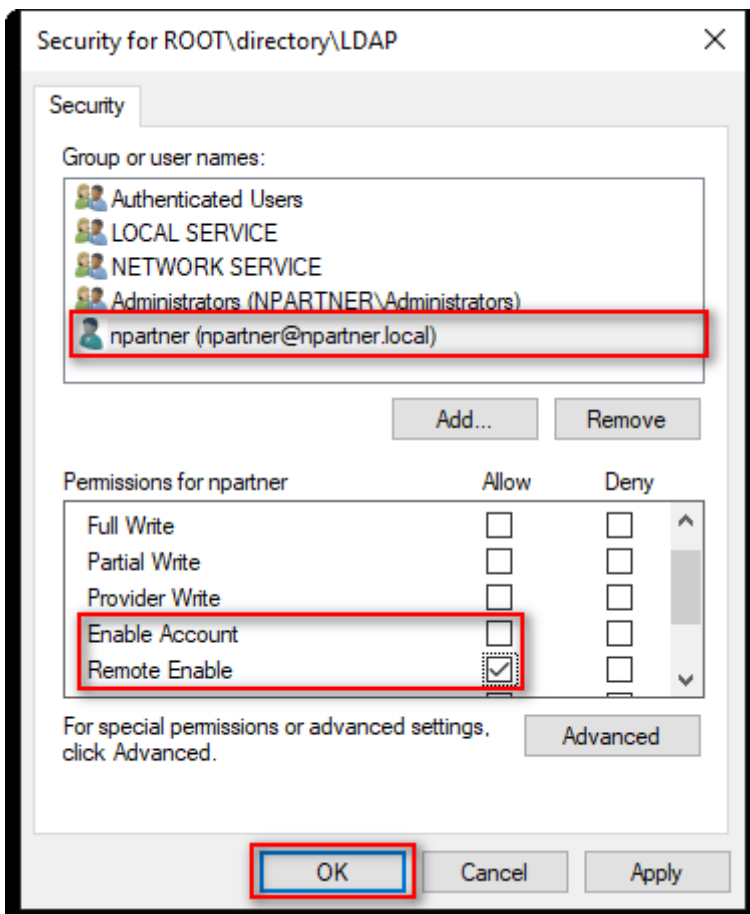


(7) Configure User Permissions

Select the user account (**npartner**):

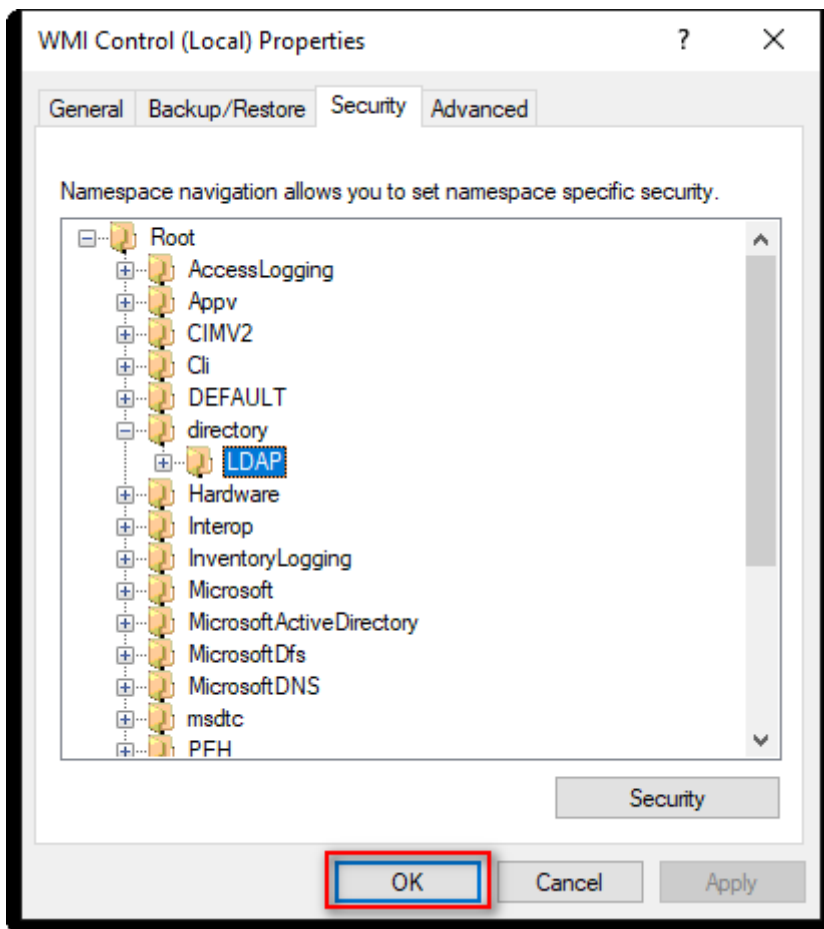
- Clear **Enable Account: Allow**
- Select **Remote Enable: Allow**

Click **OK**.



(8) Confirm User Permissions

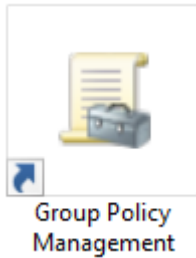
Click "OK" to apply the settings.



6.3.4 Configure Event Log Read Permissions

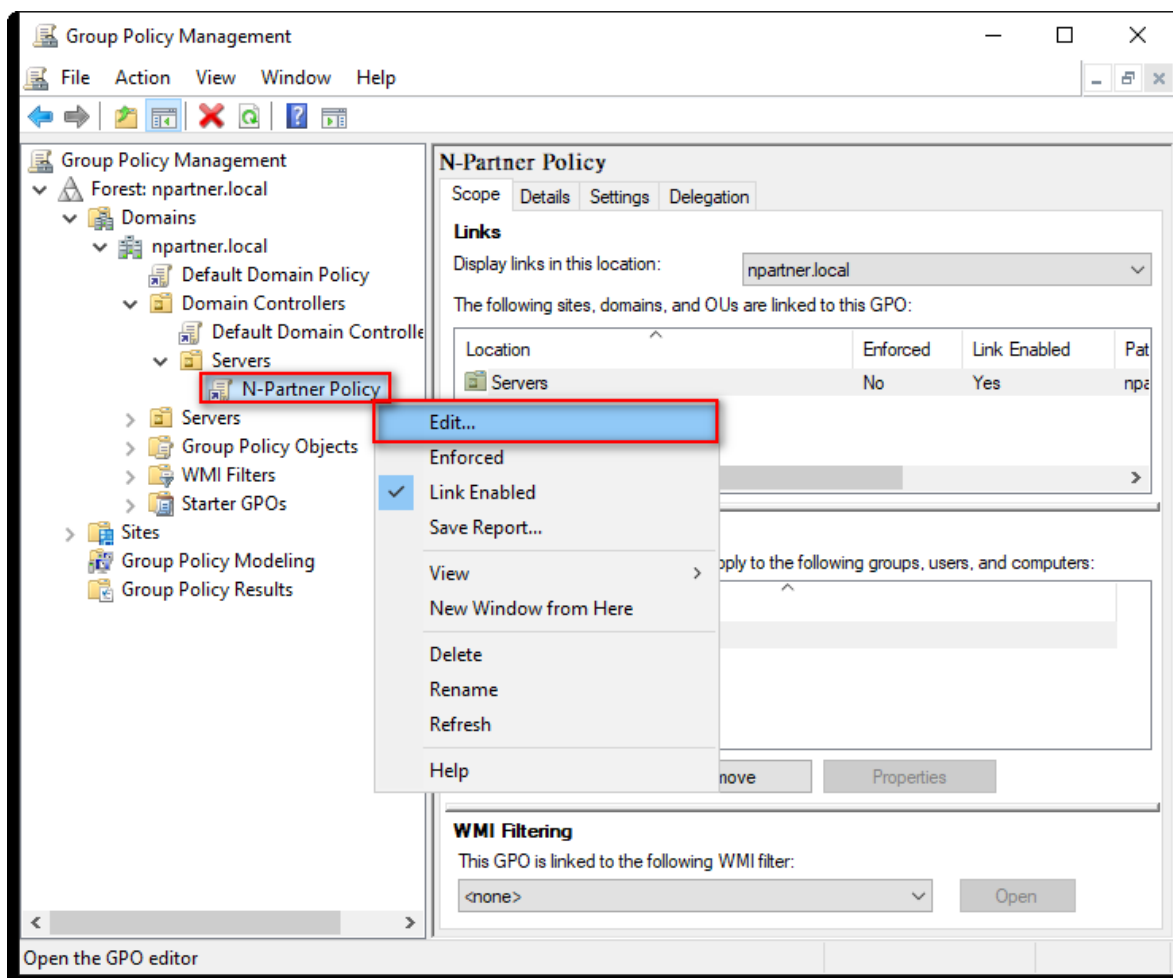
(1) Open Group Policy Management

Open “Group Policy Management.”



(2) Edit the Group Policy Object

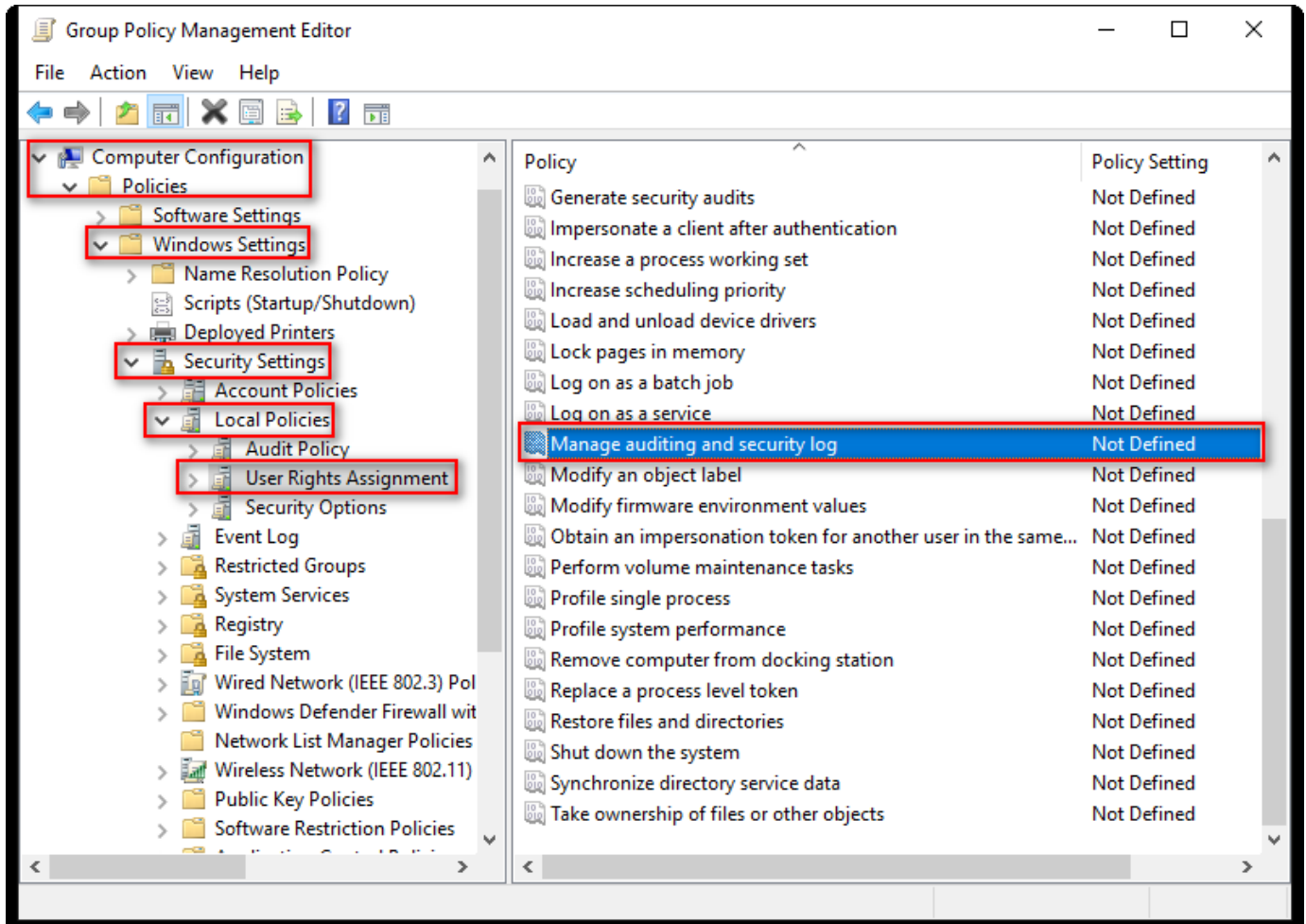
Right-click the “N-Partner Policy” Group Policy Object and select “Edit.”



(3) Configure Log Permissions

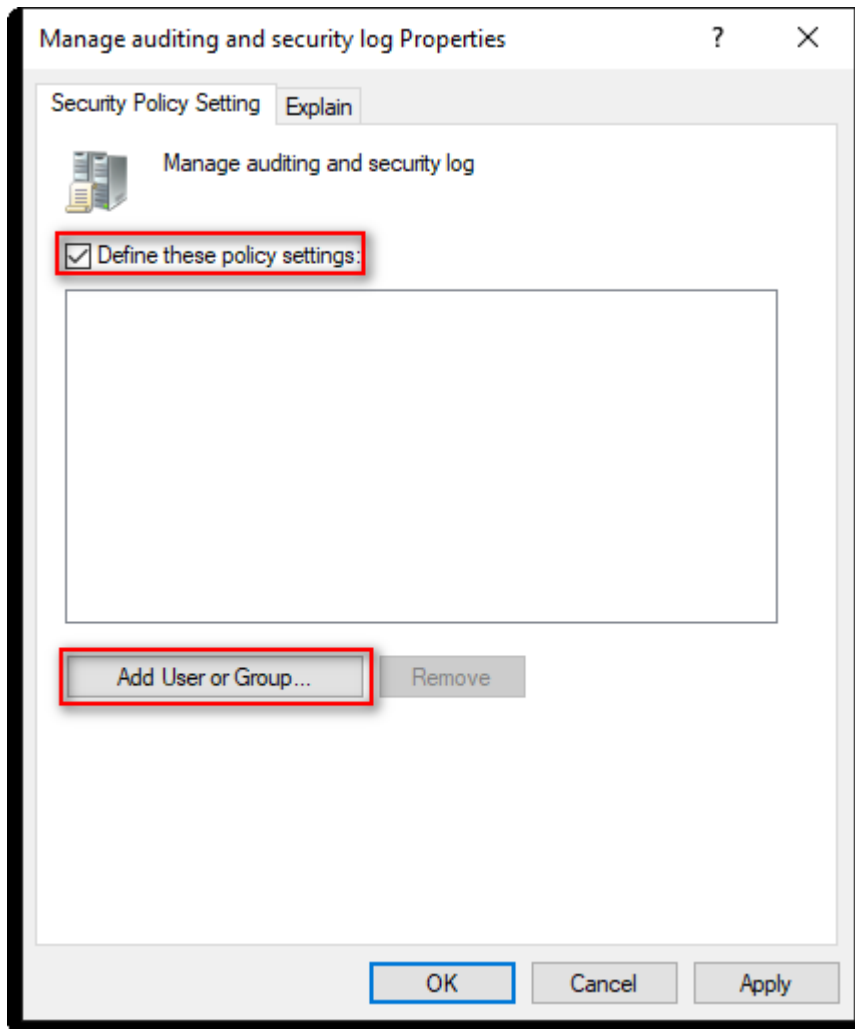
Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

Select “Manage auditing and security log,” then click “Properties.”



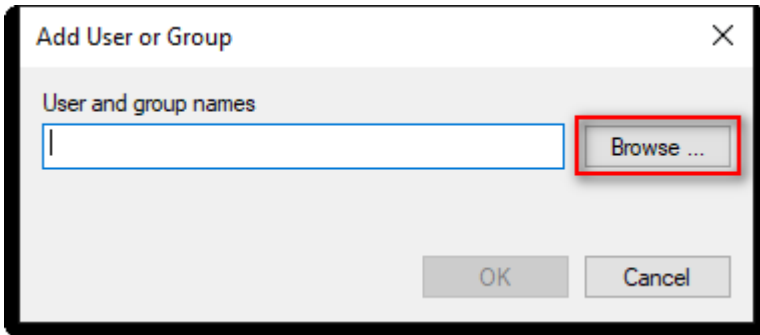
(4) Add User for Audit Log Management

Check “Define these policy settings,” then click “Add User or Group...”



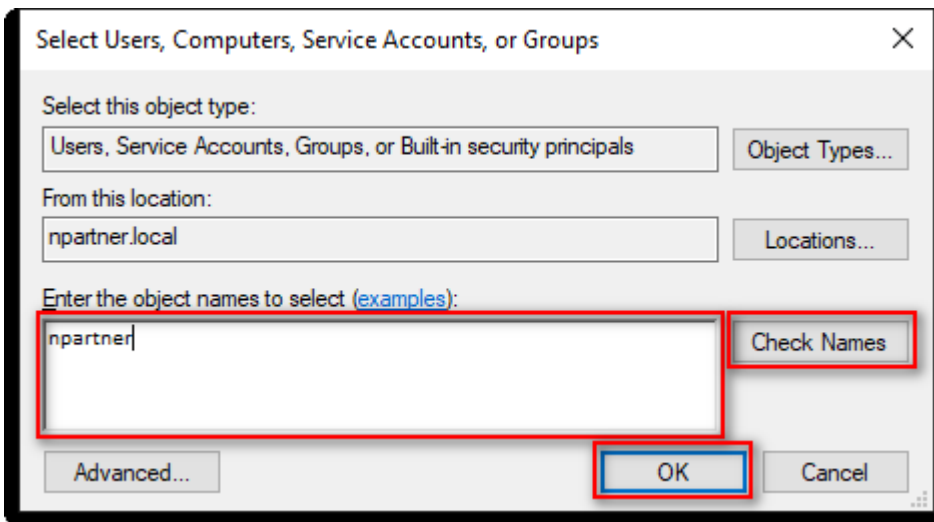
(5) Search for User

Click "Browse."



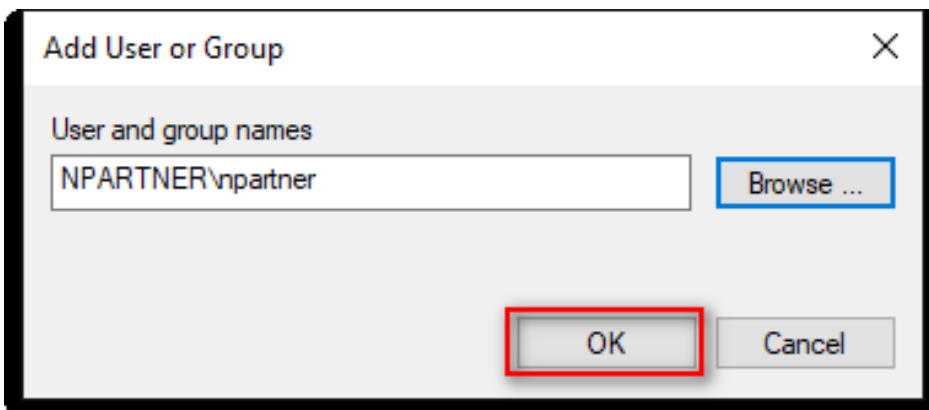
(6) Enter User Account

Enter the user account "npartner," click "Check Names," then click "OK."



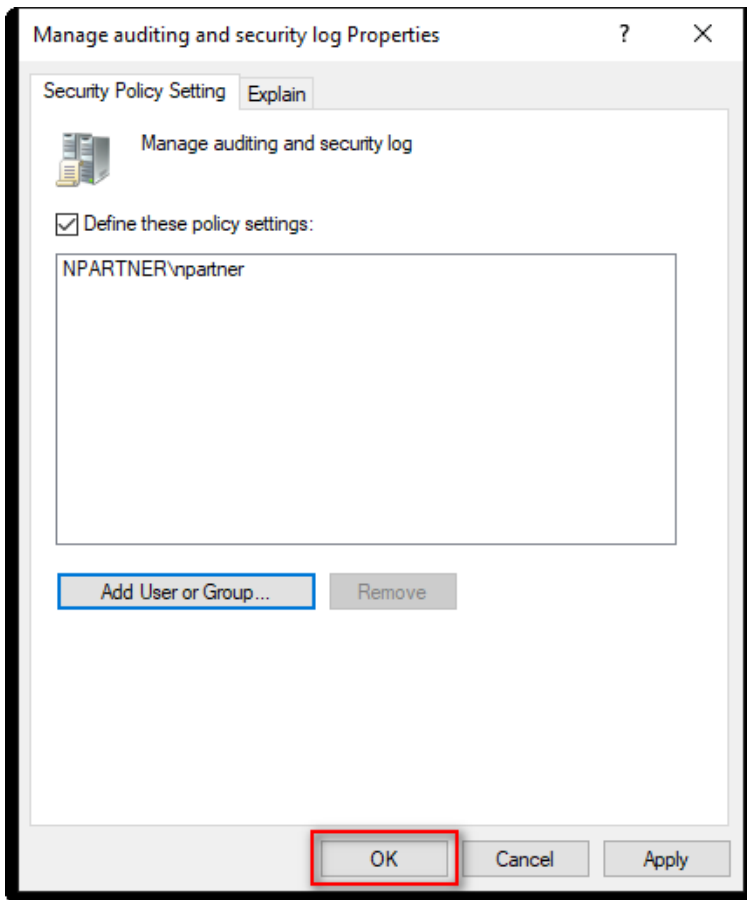
(7) Confirm User

Click "OK."



(8) Confirm Log Settings

Click "OK" to save the settings.

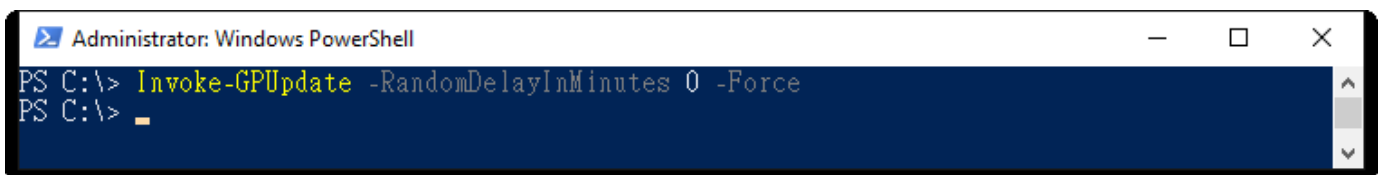


(9) Open "Windows PowerShell."



(10) Run the following command to update the policy:

```
PS C:\> Invoke-GPUupdate -RandomDelayInMinutes 0 -Force
```



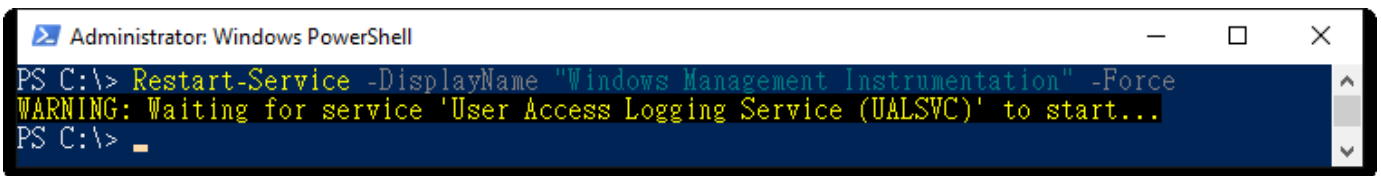
6.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”



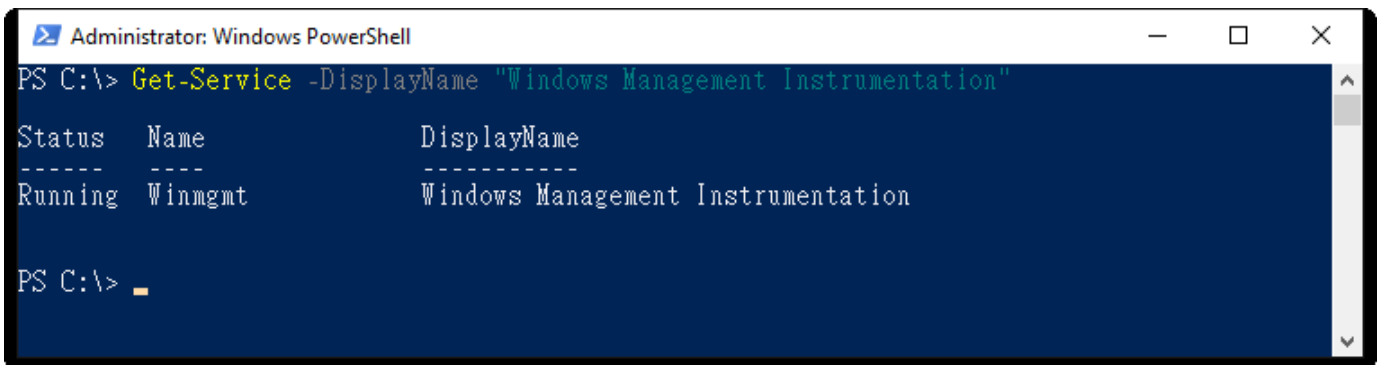
(2) Run the following command to restart the WMI service:

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) Run the following command to verify the WMI service status:

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



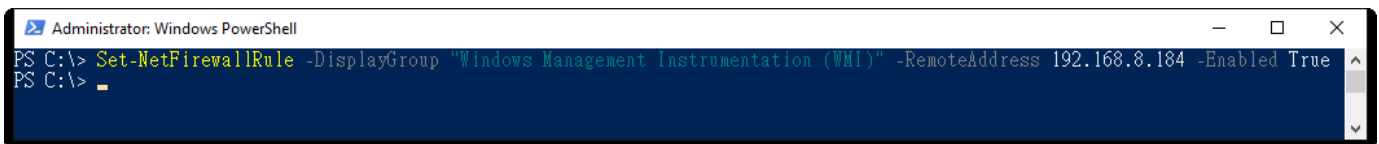
6.4 Configure Firewall

(1) Open “Windows PowerShell.”



(2) Configure the Firewall (Allow Only the N-Reporter IP to Query WMI):

```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```

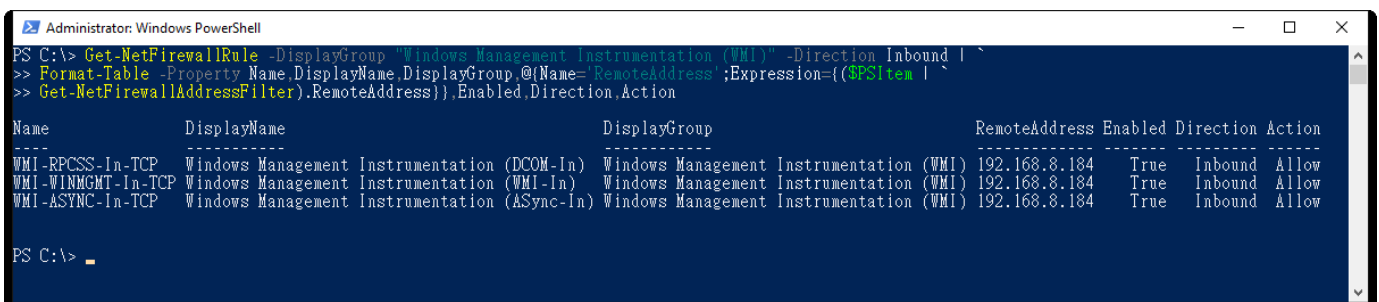


Replace the IP address with the **N-Reporter system IP address**.

(3) Check the WMI Firewall Status

Run the following command to verify the firewall rule:

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={{($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```

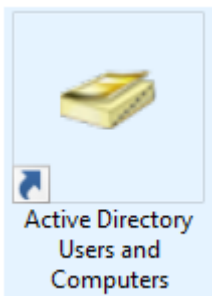


7. Windows 2022

For detailed information on setting Windows audit policies, please refer to the “audit policy recommendations link” in the preface.

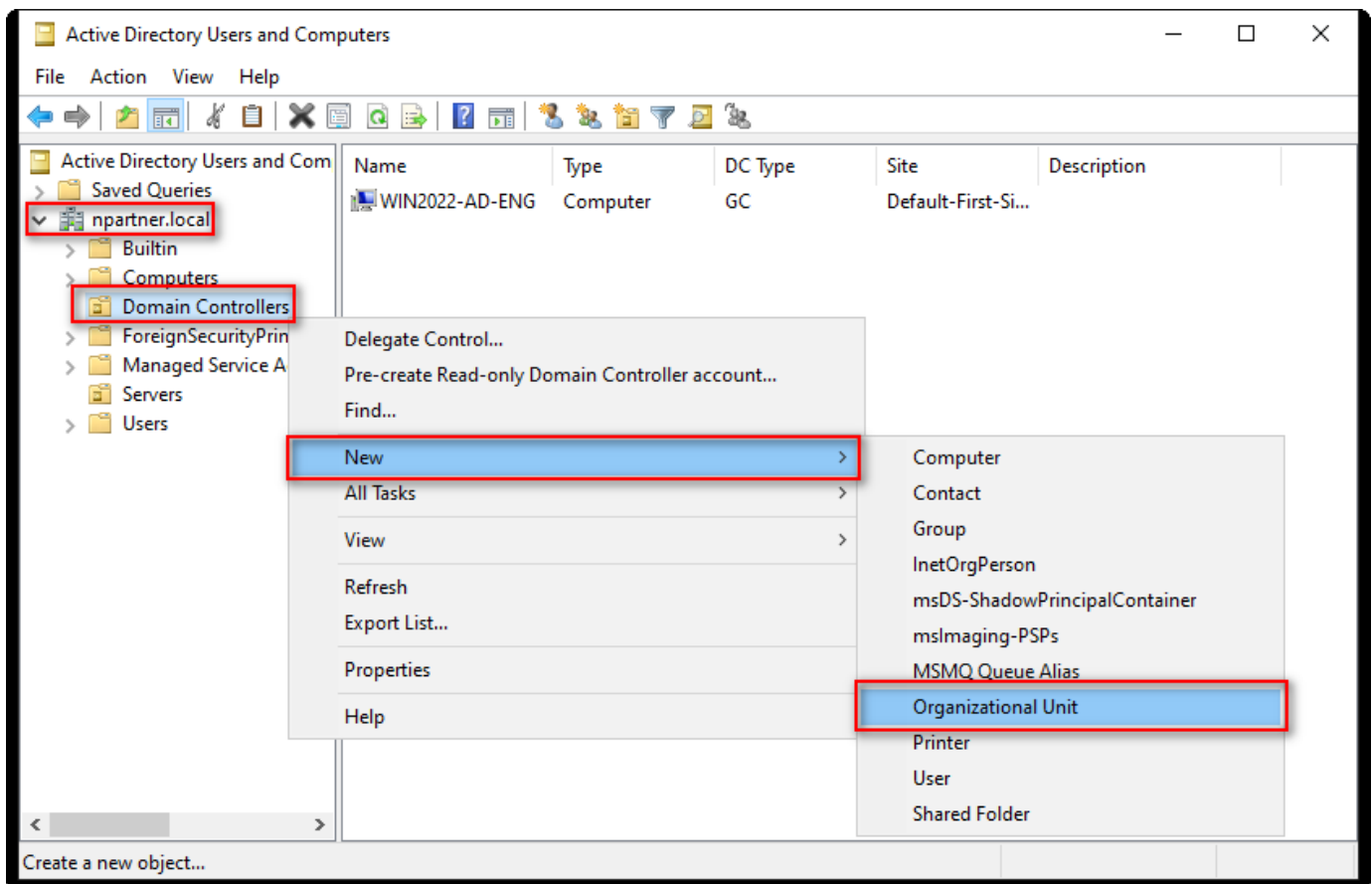
7.1 Organizational Unit Settings

(1) Open “Active Directory Users and Computers.”



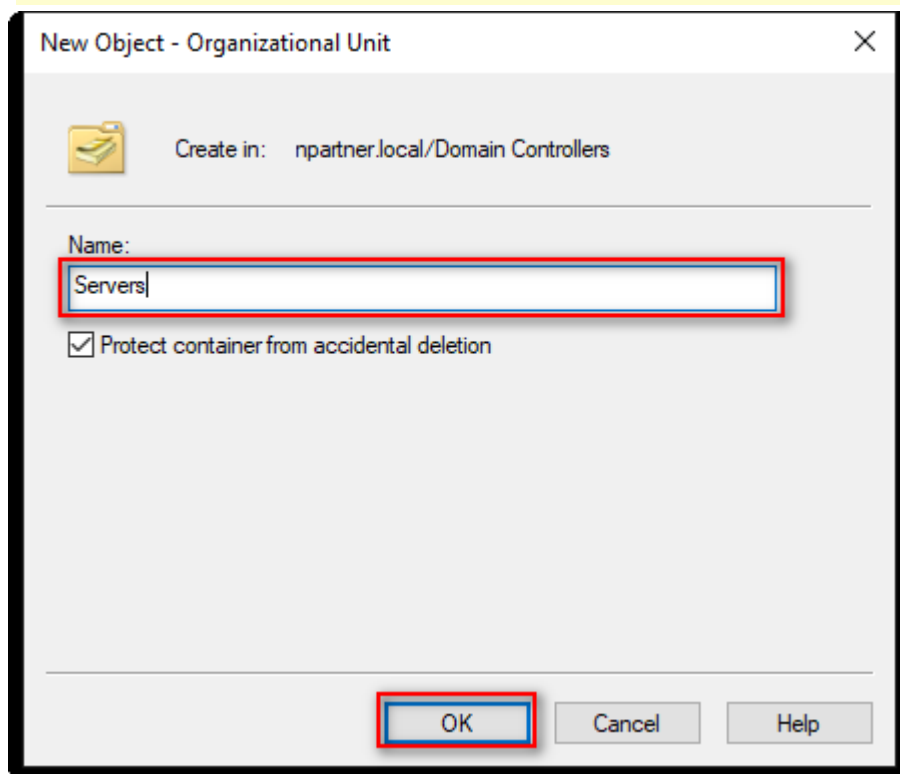
(2) Add an Organizational Unit

Right-click on “Domain Controllers,” select “New,” and click “Organizational Unit.”



(3) Enter your Organizational Unit name: (in this example, it is “Servers”)

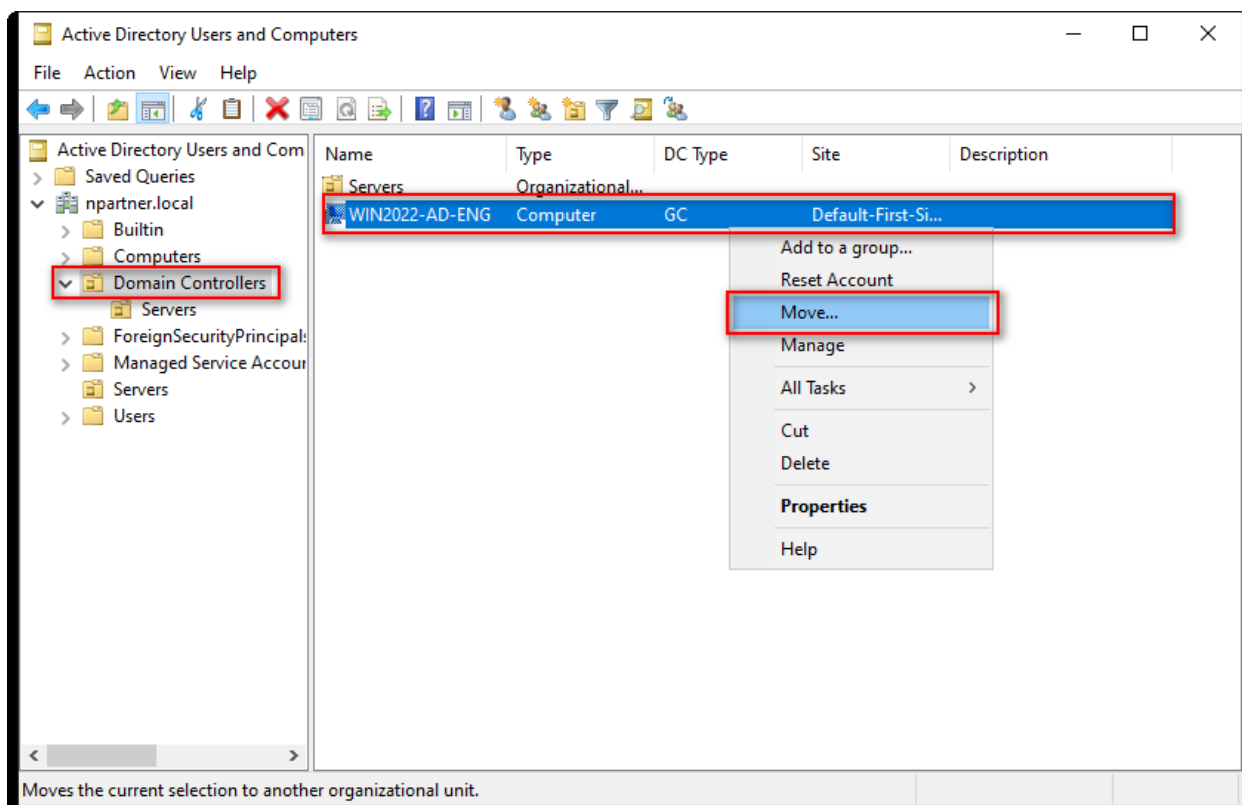
Note: Please create the organizational unit name according to the actual environment. -> Click “OK.”



(4) Move the Server to your New Organizational Unit:

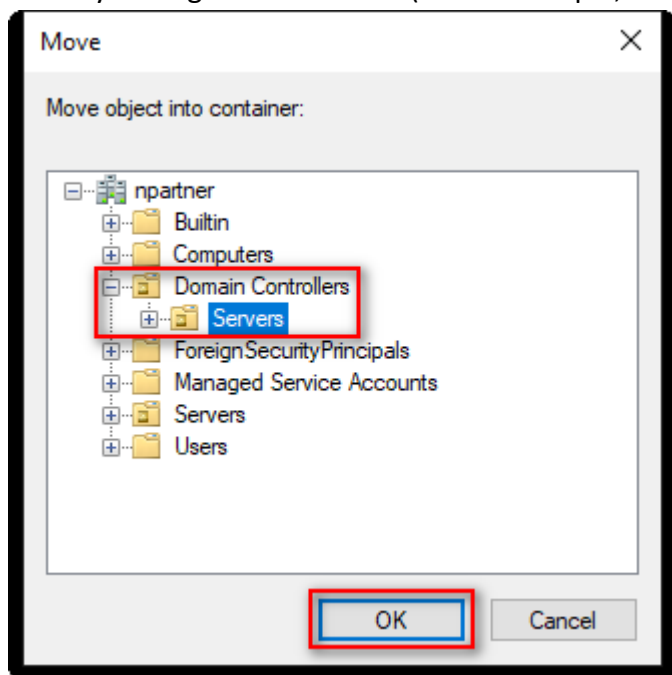
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2022-AD-ENG” server.

Note: Please select the Windows AD host according to the actual environment. -> Click “Move.”



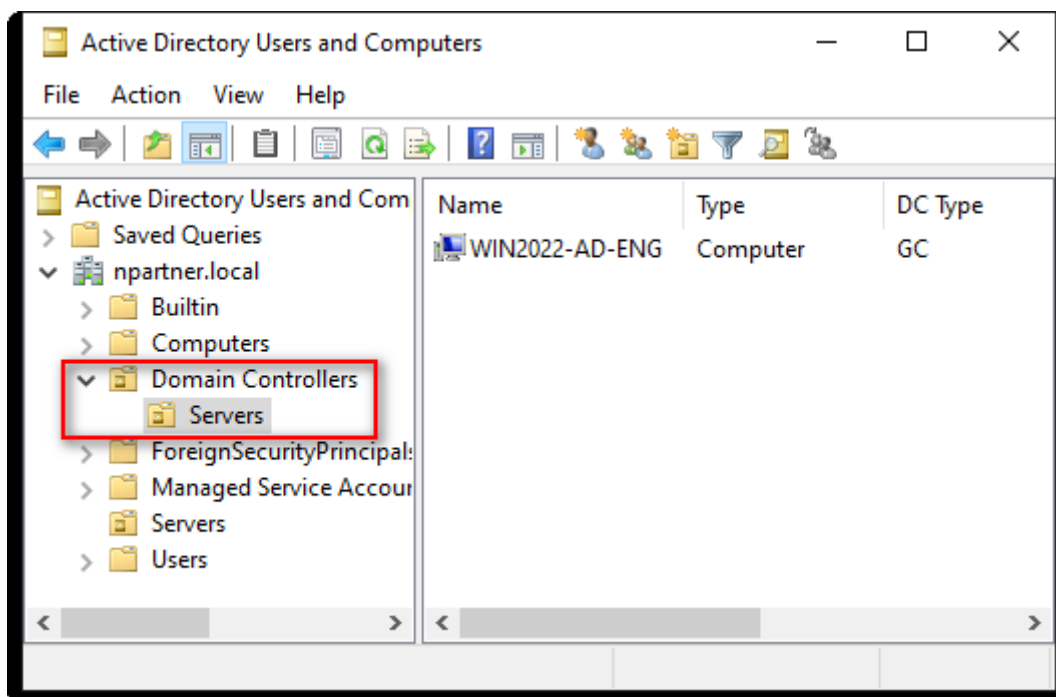
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) under “Domain Controllers” -> Click “OK.”



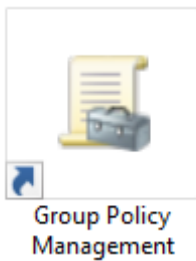
(6) Verify the Server Has Been Moved to your New Organizational Unit:

Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2022-AD-ENG” server has been moved.

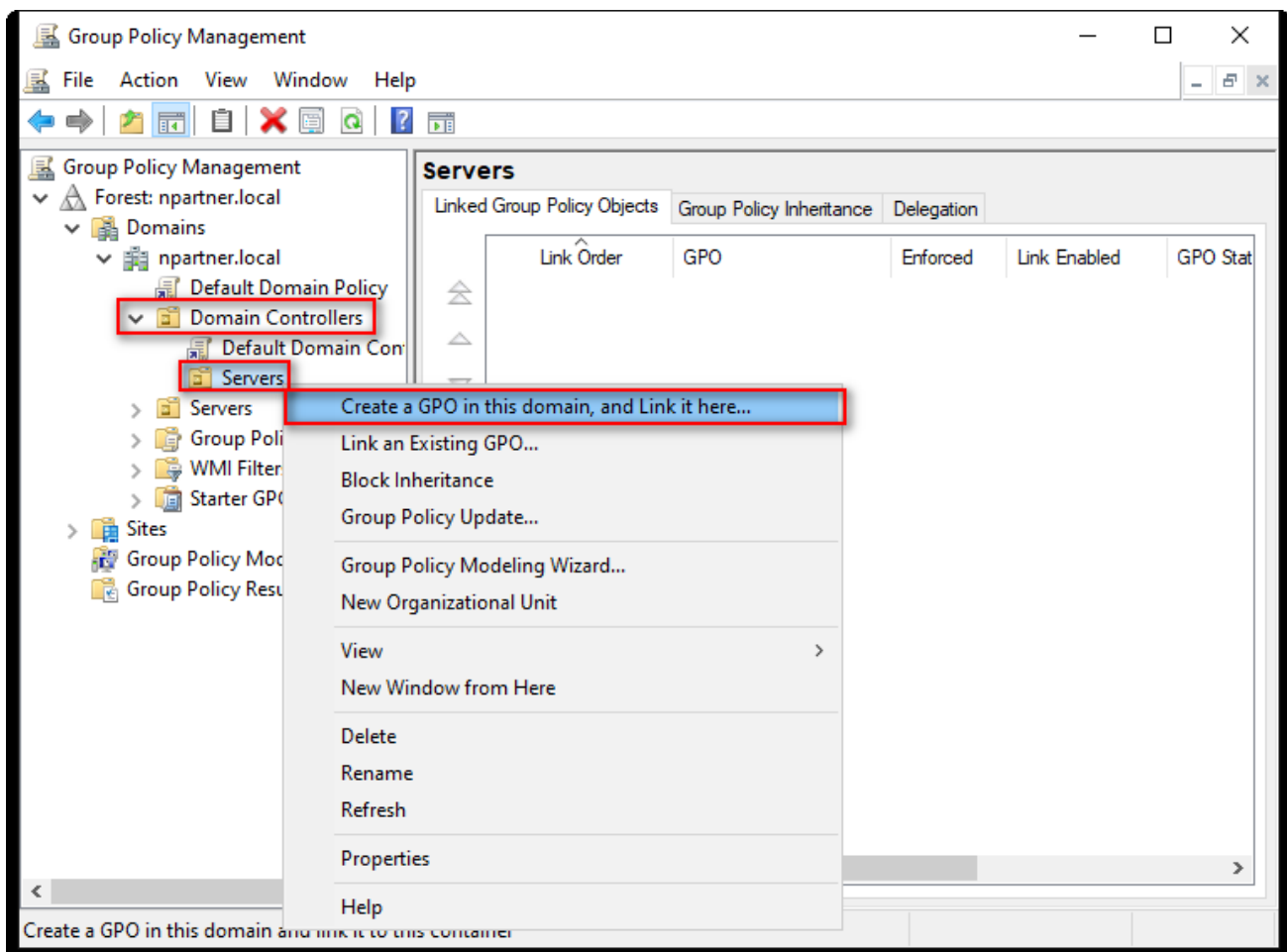


7.2 Group Policy Settings

(1) Click “Group Policy Management.”

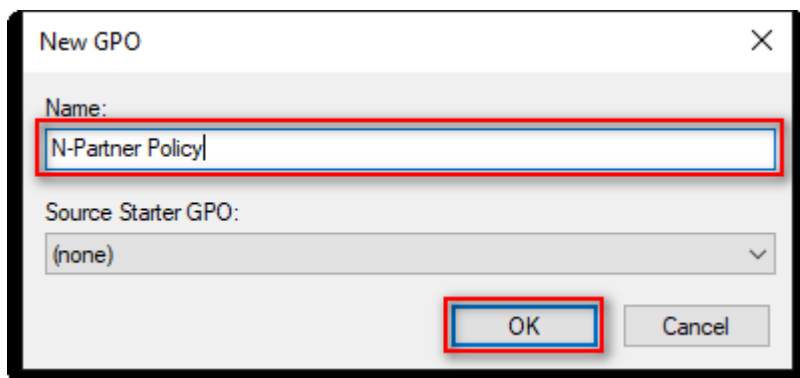


(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



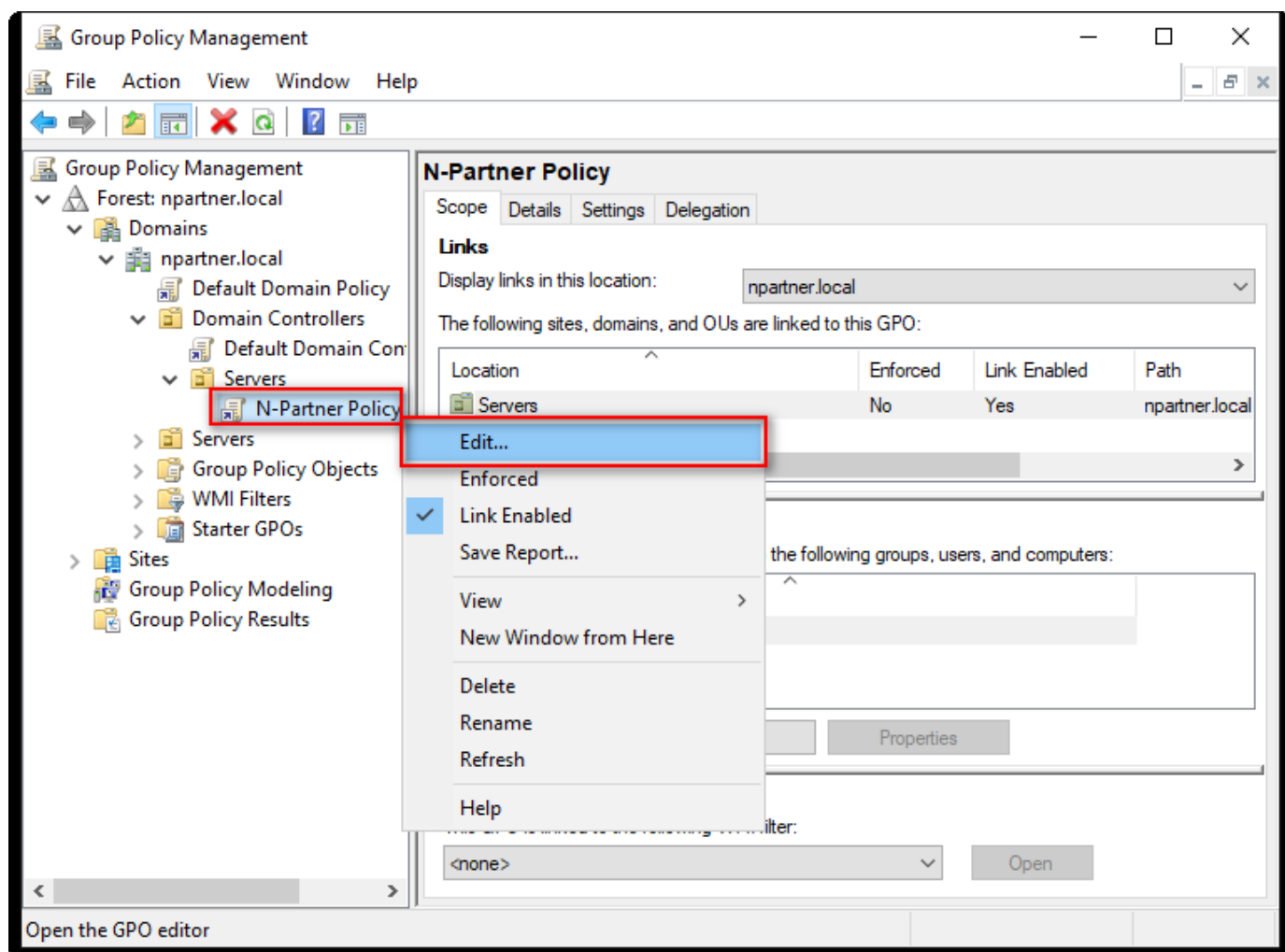
(3) Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the client's environment. Then click “Edit.”



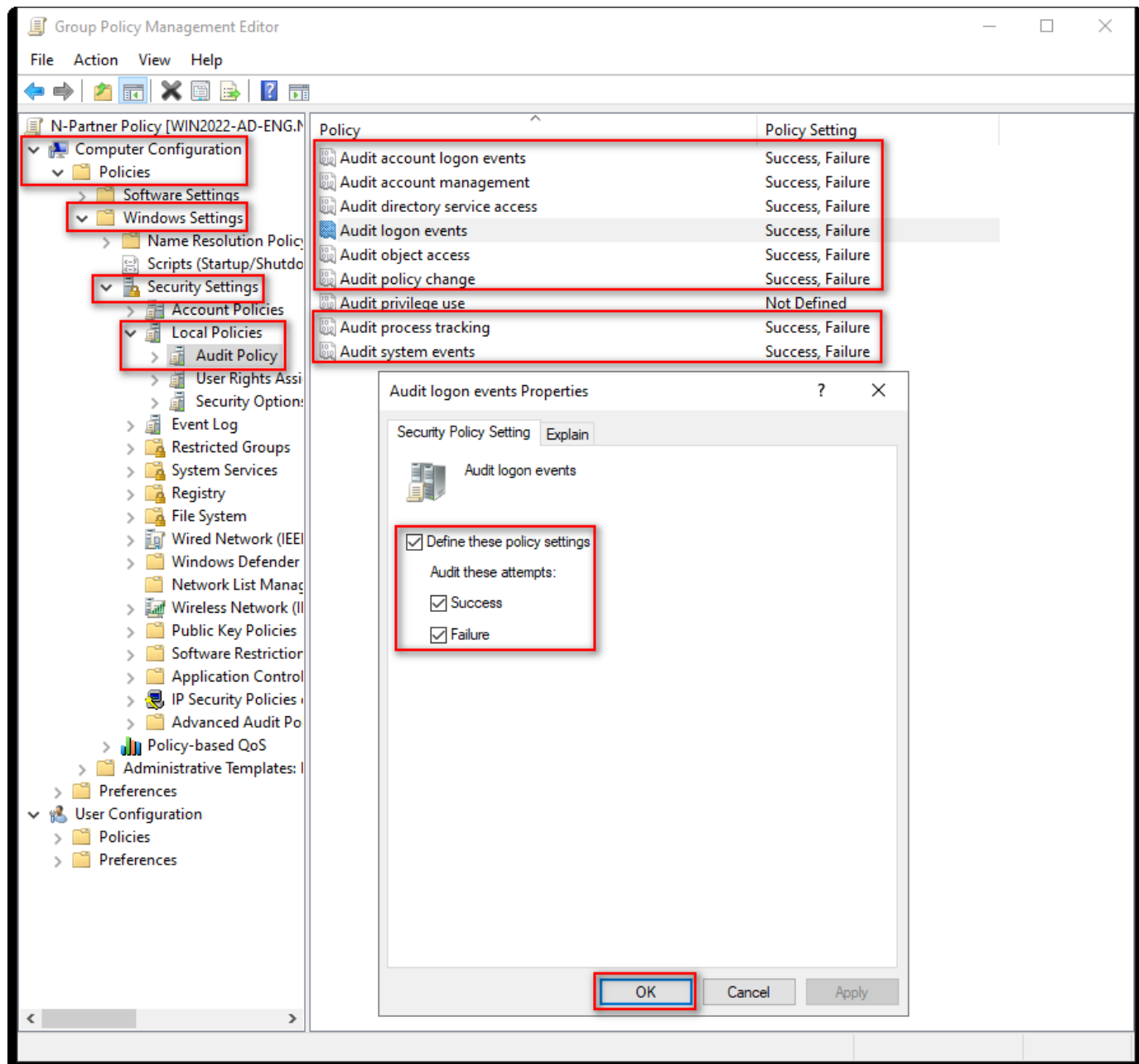
(4) Edit your Group Policy Object

In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(6) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment.

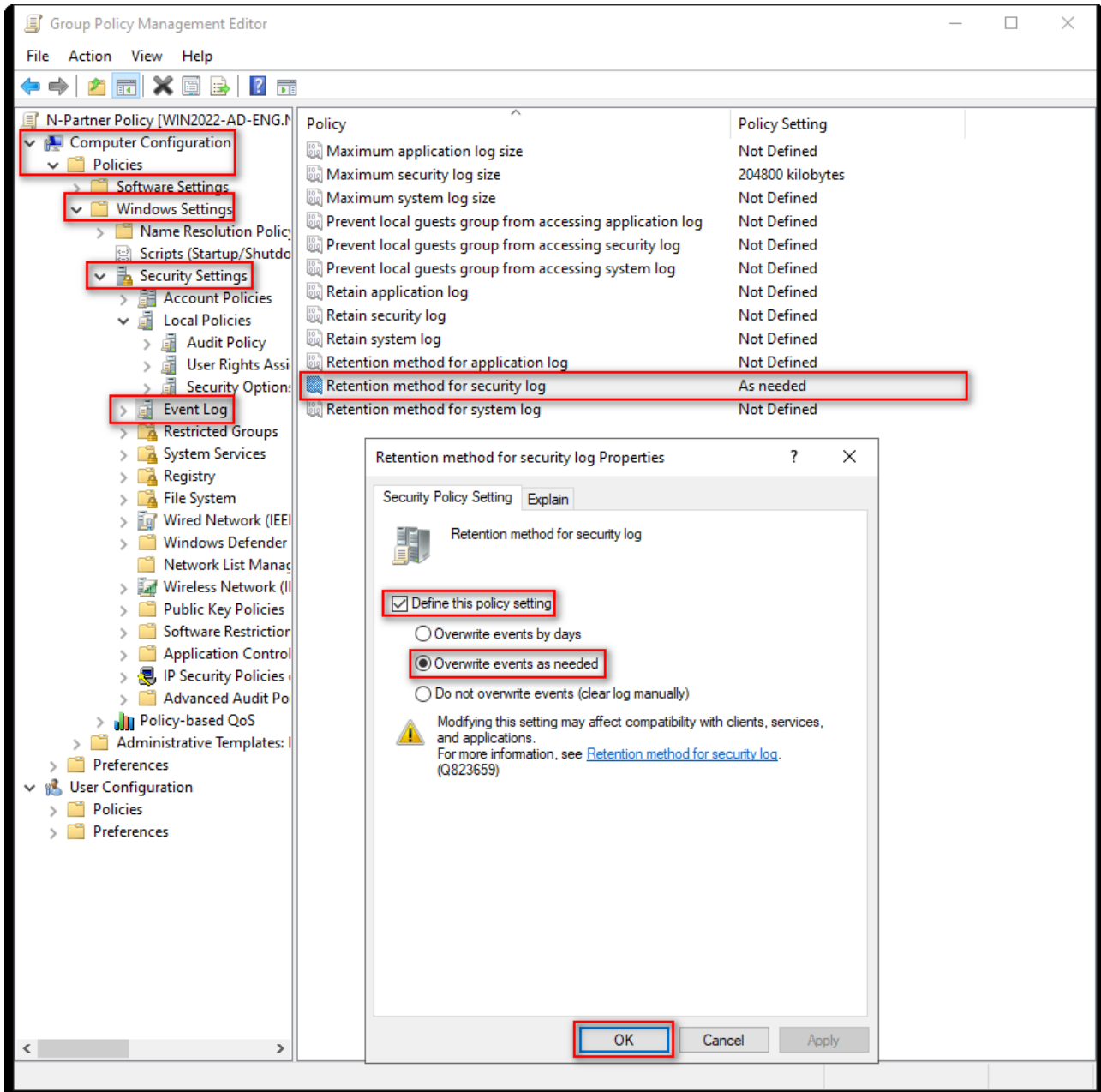
-> Click “OK.”

The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Event Log. The right-hand pane shows a list of policies, with 'Maximum security log size' selected and highlighted. A 'Maximum security log size Properties' dialog box is open, showing the 'Define this policy setting' checkbox checked and the value '204800 kilobytes' entered in the spin box. The 'OK' button is highlighted.

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	Not Defined
Retention method for system log	Not Defined

(7) Event Log: Maximum Size of Security Log

Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Event Log.”
Select “Retention method for Security log,” check “Define this policy setting,” choose “Overwrite events as needed,” and click “OK.”

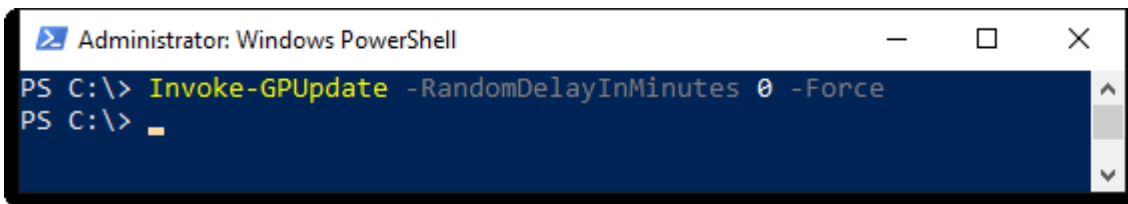


(8) Open “Windows PowerShell.”



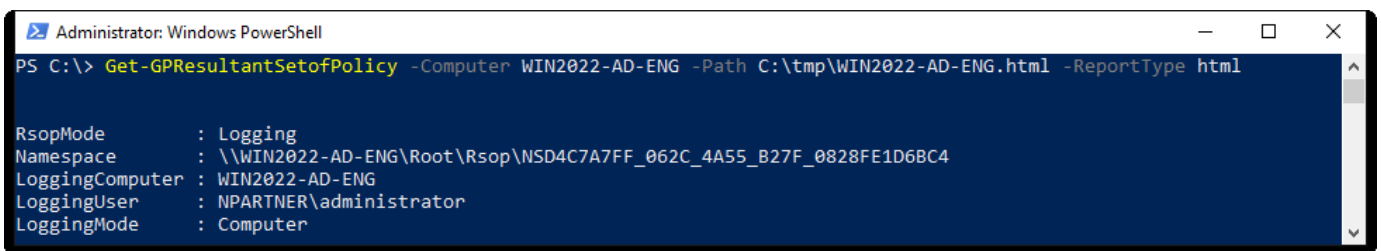
(9) Run the following command to update group policy:

```
PS C:\> Invoke-GPUdate -RandomDelayInMinutes 0 -Force
```



(10) Run the following command to generate the Server Group Policy Report:

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-AD-ENG -Path C:\tmp\WIN2022-AD-ENG.html -ReportType html
```



Replace the highlighted text with the Windows AD server name and the file path for the report.

(11) Open the report and verify that the **WIN2022-AD-ENG** server has the N-Partner Policy Group Policy applied.

The screenshot displays a web browser window with the following content:

Computer Information:

- Computer name: NPARTNER\WIN2022-AD-ENG
- Domain: npartner.local
- Site: Default-First-Site-Name
- Organizational Unit: npartner.local/Domain Controllers/Servers
- Security Group Membership: [show](#)

Component Status:

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	448 Millisecond(s)	4/22/2024 PM 04:05:45	View Log
Registry	Success	110 Millisecond(s)	4/22/2024 PM 04:05:44	View Log
Security	Success	938 Millisecond(s)	4/22/2024 PM 04:05:45	View Log

Settings:

- Policies:** [hide](#)
- Windows Settings:** [hide](#)
- Security Settings:** [hide](#)
- Account Policies/Password Policy:** [show](#)
- Account Policies/Account Lockout Policy:** [show](#)
- Account Policies/Kerberos Policy:** [show](#)
- Local Policies/Audit Policy:** [hide](#)

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit directory service access	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit policy change	Success, Failure	N-Partner Policy
Audit process tracking	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy

Local Policies/User Rights Assignment: [show](#)

Local Policies/Security Options: [show](#)

7.3 Add a Non-Admin Account

7.3.1 Add Users

(1) Open “Windows PowerShell.”



(2) Enter the command below to add a new account.

```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the same command sequence as in the previous block, with the output of the command execution. The command is: `New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) -PasswordNeverExpires $True -Enabled $True`. The terminal shows the command being entered and executed, with the prompt returning to `PS C:\>`.

For the red text, please enter the account password and domain information.

(3) Enter the command below to view the account status.

```
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires,Enabled
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Get-ADUser npartner -Properties PasswordNeverExpires,Enabled` being executed. The output is as follows:
`DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local`
`Enabled : True`
`GivenName :`
`Name : npartner`
`ObjectClass : user`
`ObjectGUID : 68cecf78-33cd-4fa8-a4f5-bc01843b0fdf`
`PasswordNeverExpires : True`
`SamAccountName : npartner`
`SID : S-1-5-21-475969428-1156914179-1979101651-1105`
`Surname :`
`UserPrincipalName : npartner@npartner.local`

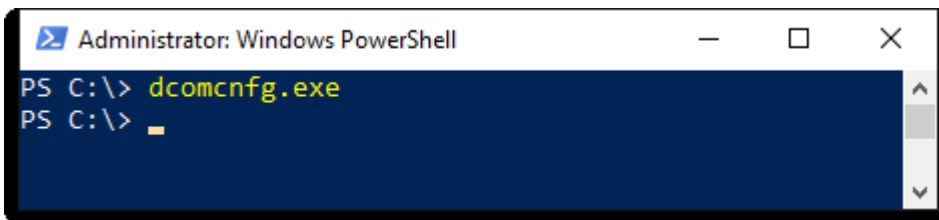
7.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”



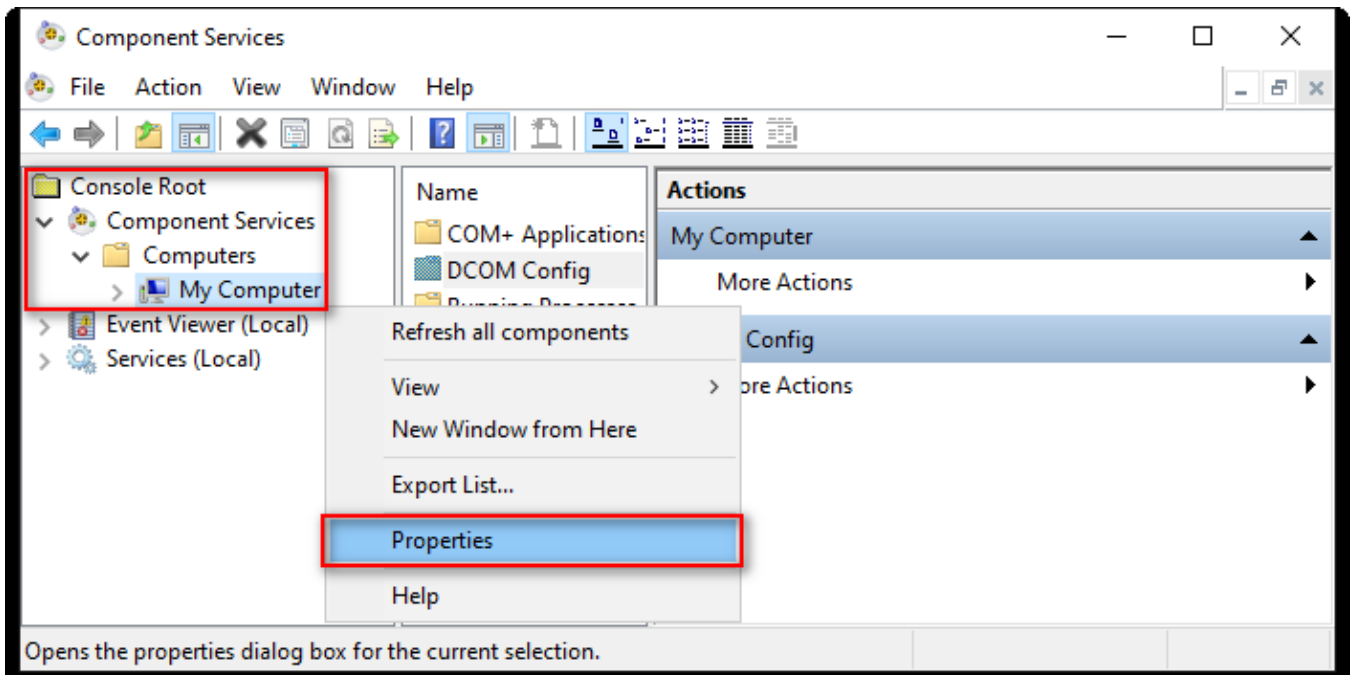
(2) Enter the command below to open component services.

```
PS C:\> dcomcnfg.exe
```



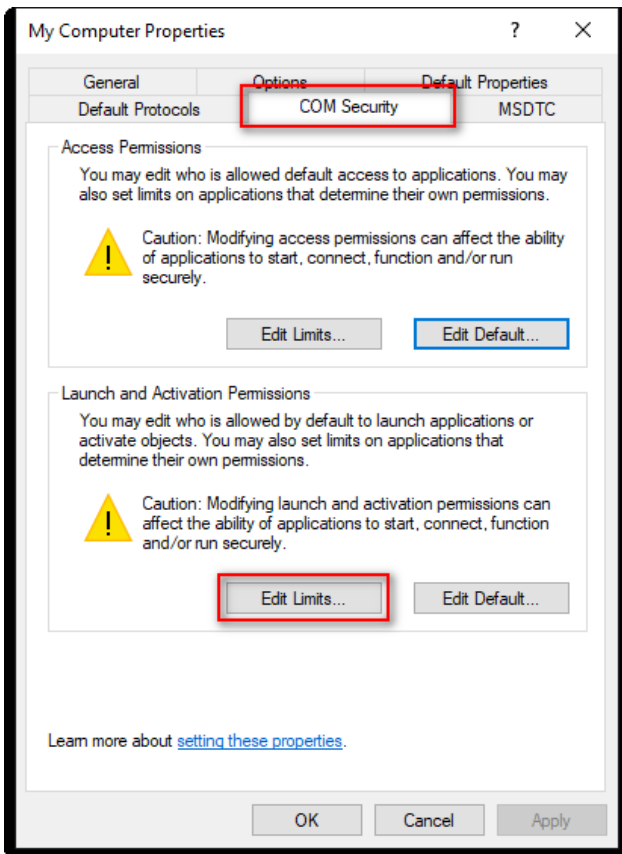
(3) Edit Computer Properties

Expand folder “Console Root” -> “Component Services” -> “Computers,” right-click on “My Computer,” and select “Properties.”



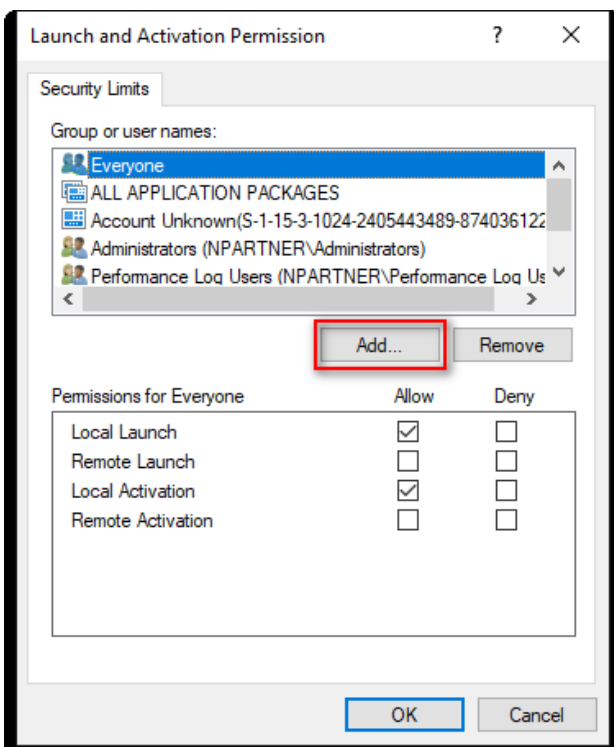
(4) Enable Permissions

Go to the “COM Security” tab, under Launch and Activation Permissions, click “Edit Limits.”



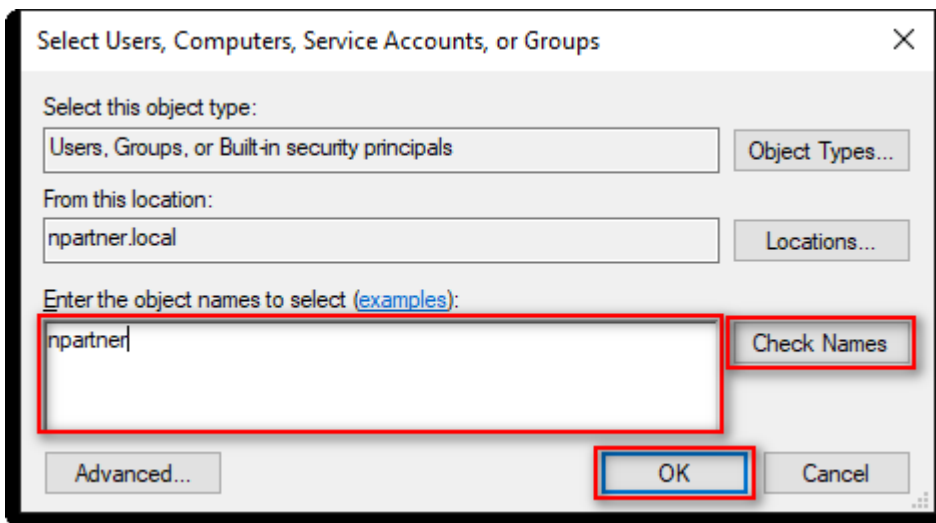
(5) Add DCOM User Permissions

Click “Add.”



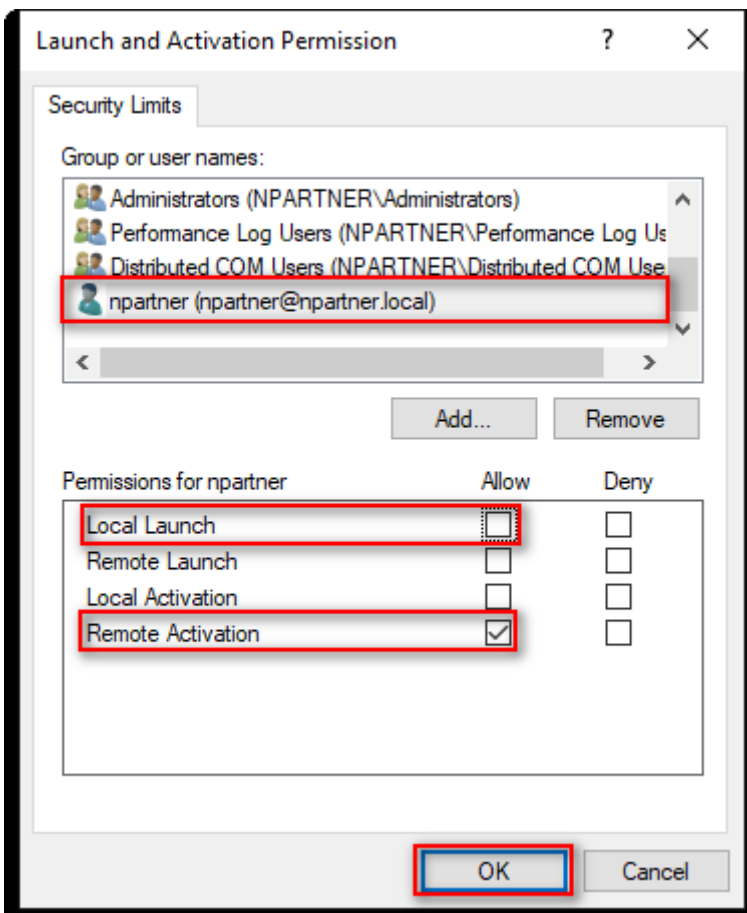
(6) Enter your Username

Input your user account: `npartner`, click “Check Names,” then click “OK.”

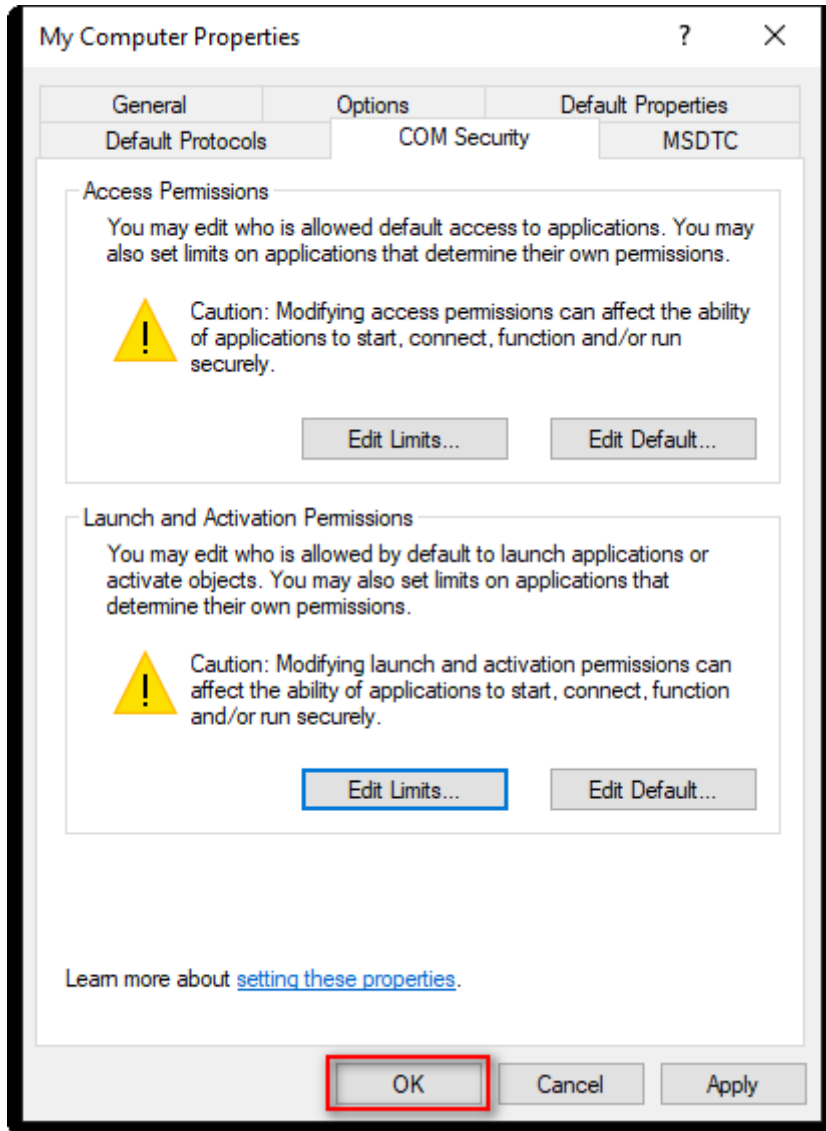


(7) Set User Permissions

Select the user account: `npartner`, uncheck “Local Launch: Allow,” check “Remote Activation: Allow,” then click “OK.”



(8) Click "OK."



7.3.3 Configure WMI Permissions

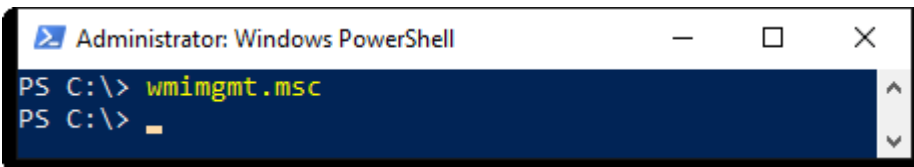
7.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”



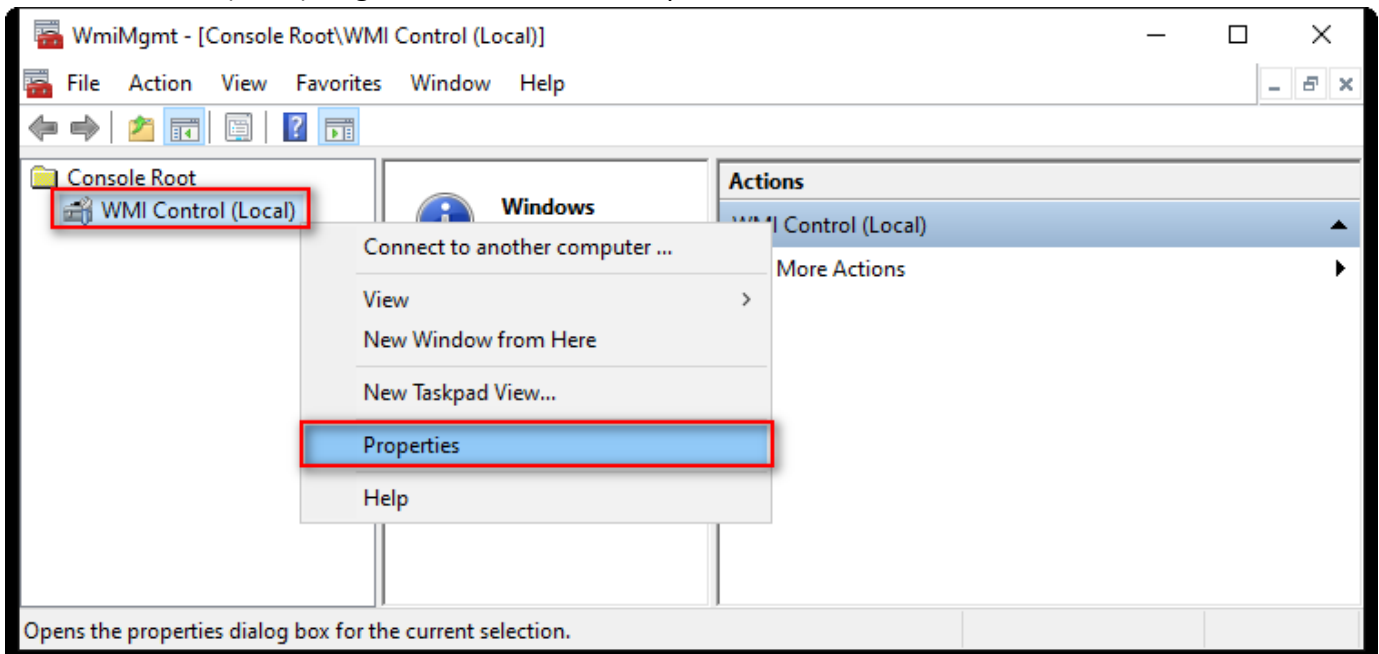
(2) Enter the command below to enable component services.

```
PS C:\> wmicmgmt.msc
```



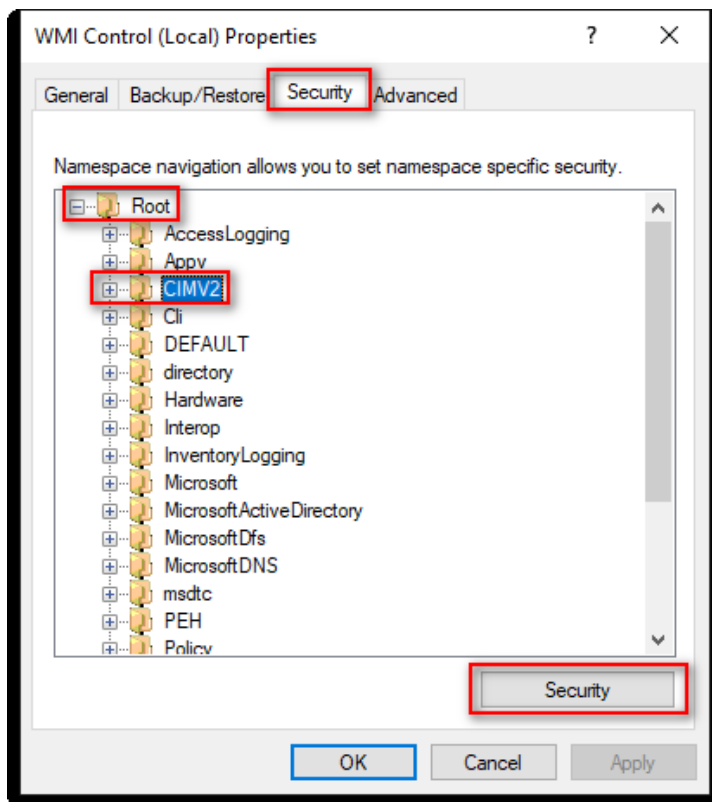
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



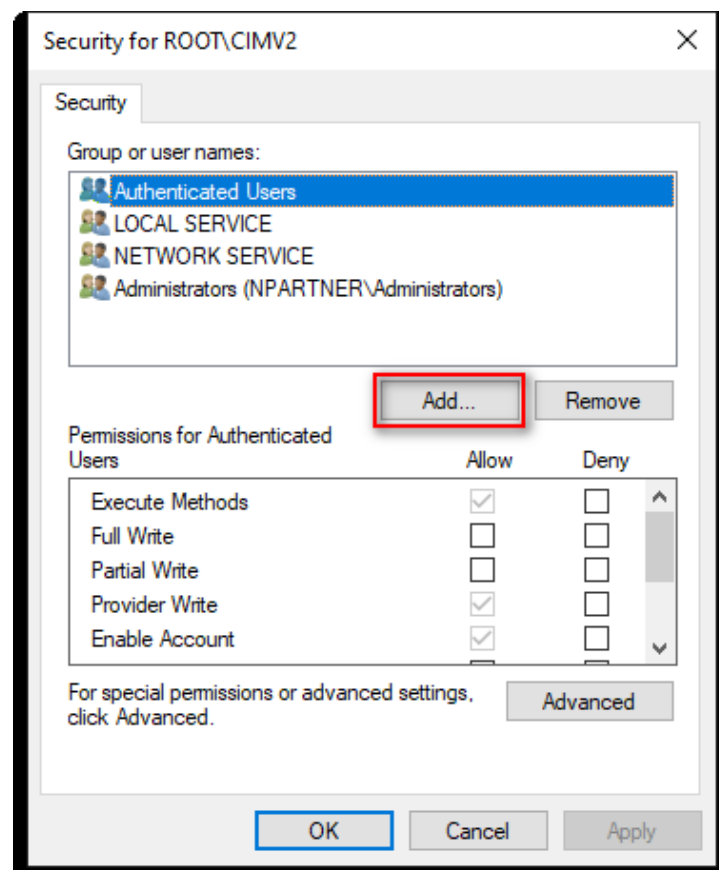
(4) Edit CIMV2 Security

On the "Security" tab, expand folder "Root" -> "CIMV2," then click "Security."



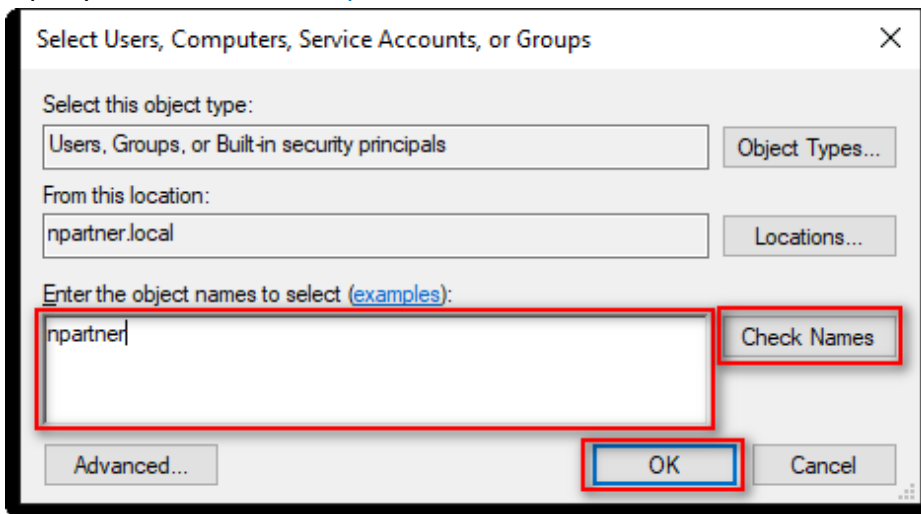
(5) Add WMI User Permissions

Click "Add."



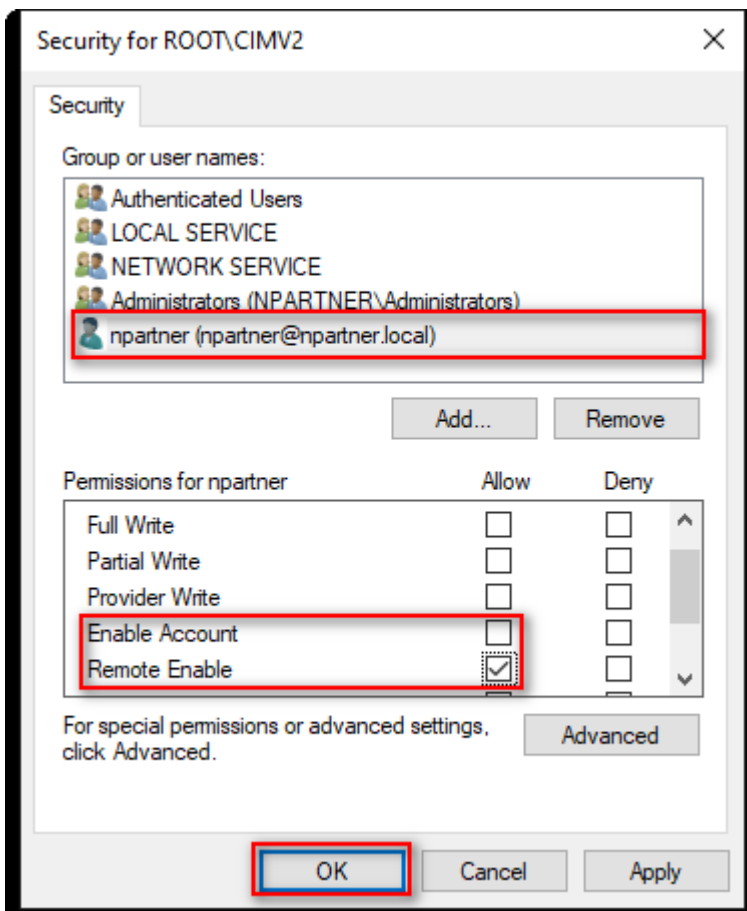
(6) Enter User

Input your user account: `npartner`, click “Check Names,” then click “OK.”



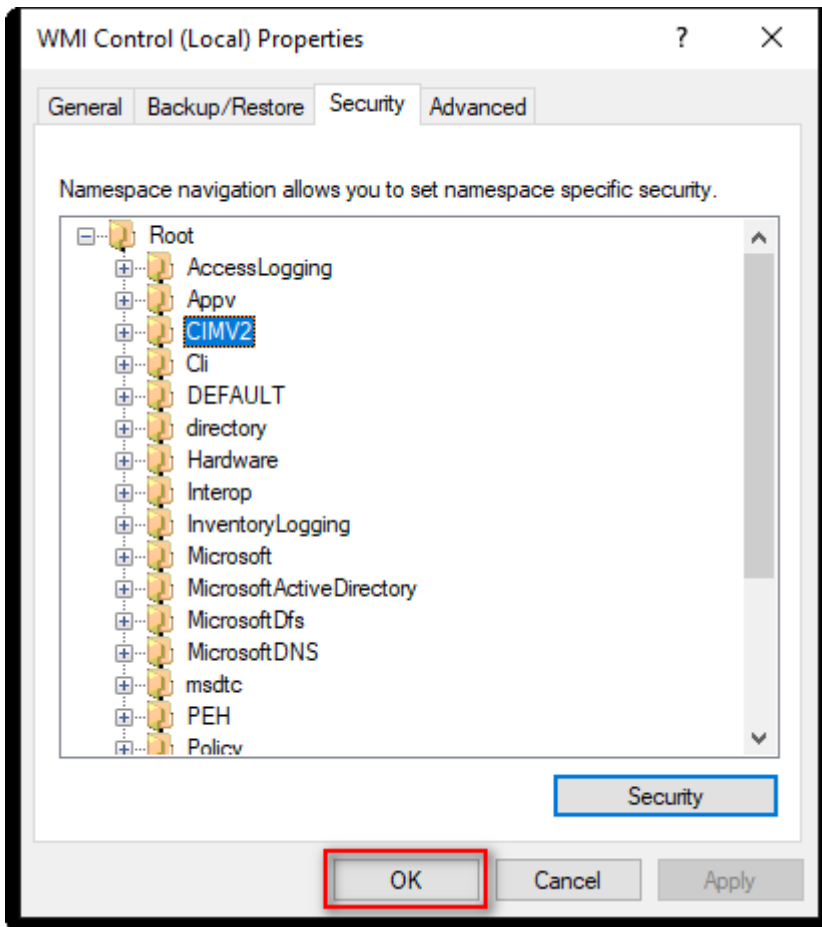
(7) Set User Permissions

Select the user account: `npartner`, uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



(8) Confirm User Permissions

Click "OK."



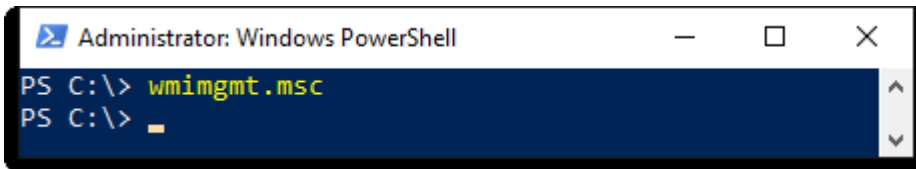
7.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”



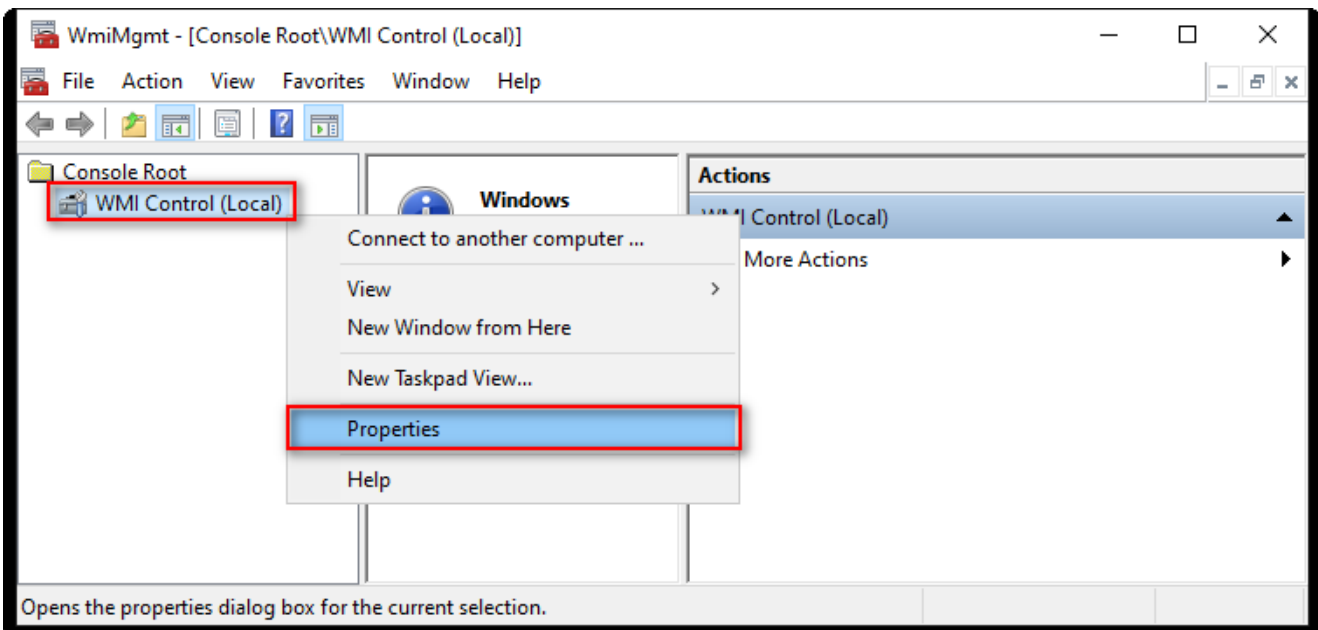
(2) Enter the command below to enable component services.

```
PS C:\> wmicmgmt.msc
```



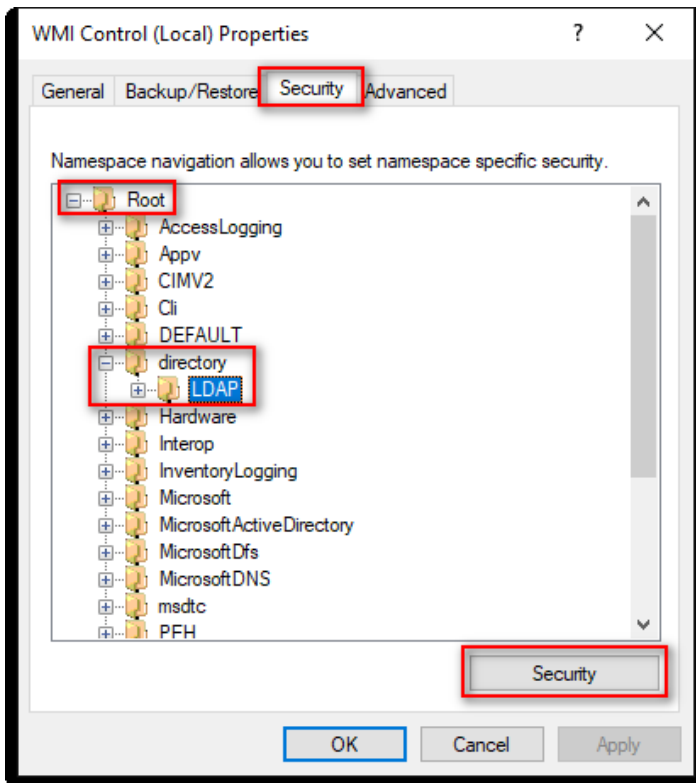
(3) Edit WMI Control

In “WMI Control (Local),” right-click and select “Properties.”



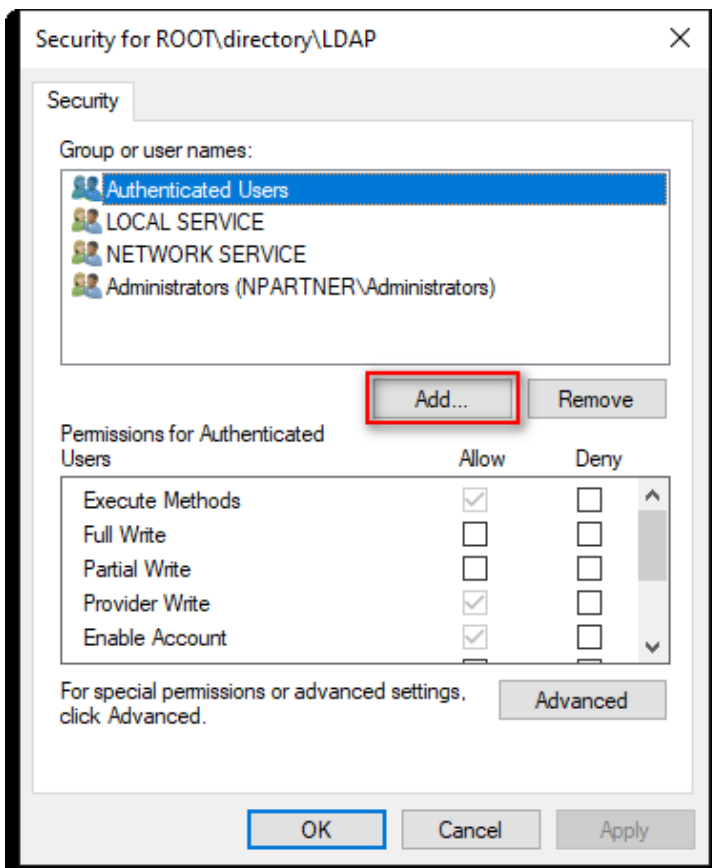
(4) Edit LDAP Security

On the “Security” tab, expand “Root”-> “directory” -> “LDAP,” then click “Security.”



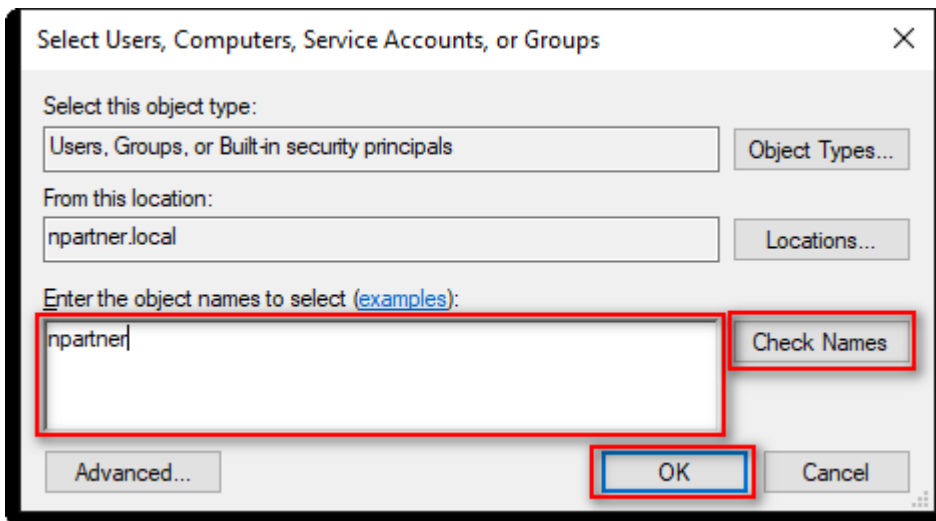
(5) Add WMI User Permissions

Click “Add.”



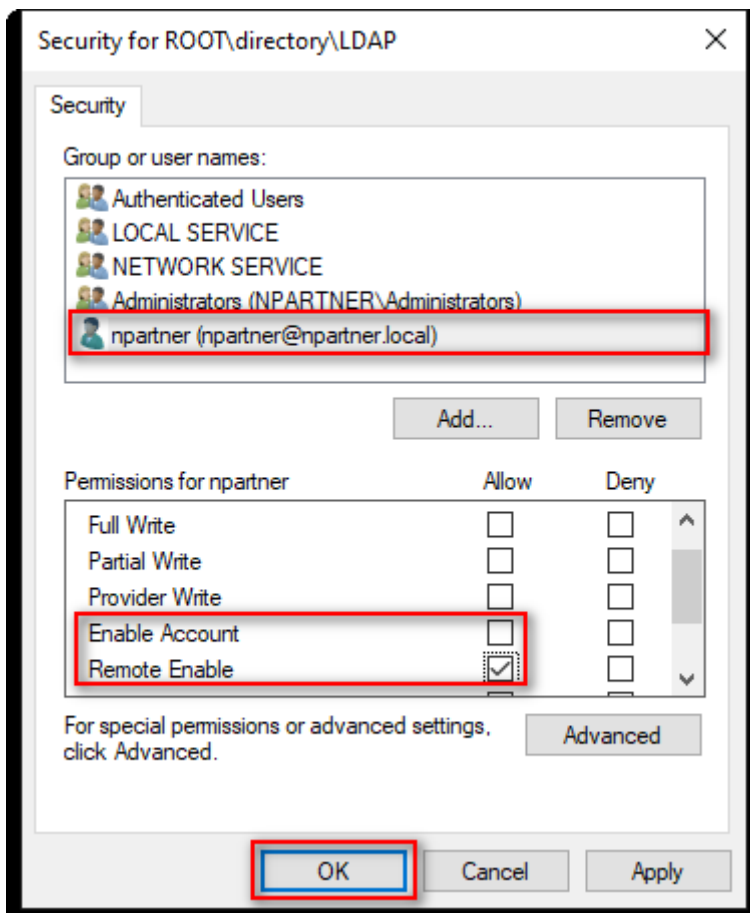
(6) Enter Your Username

Input your user account name (in this example, it is “npartner”), click “Check Names,” then click “OK.”



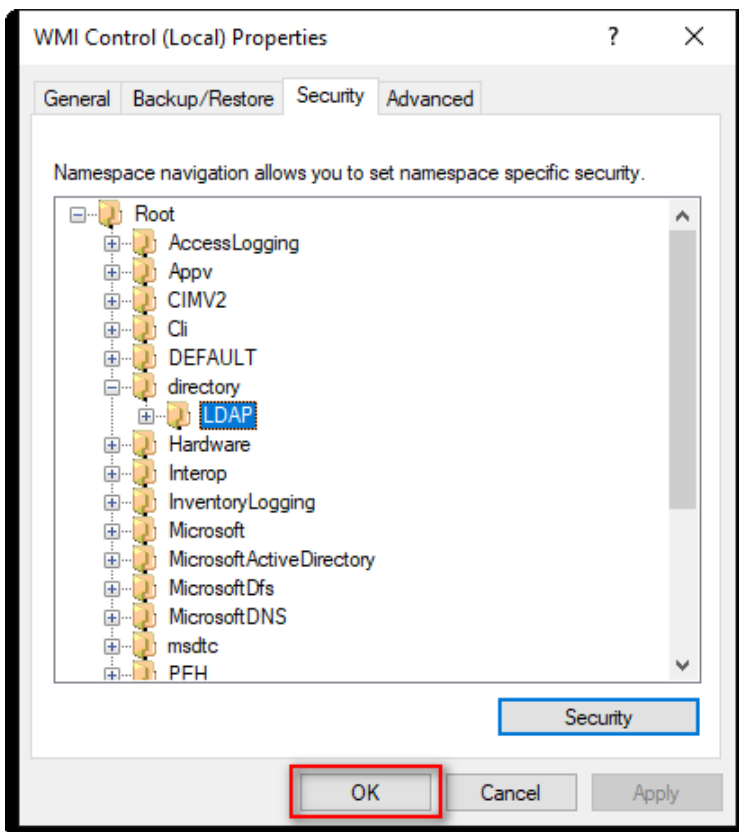
(7) Set Your User Permissions

Select your user account (in this example, it is “npartner”), uncheck “Enable Account: Allow,” check “Remote Enable: Allow,” then click “OK.”



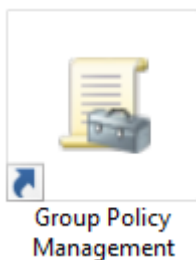
(8) Confirm User Permissions

Click "OK."



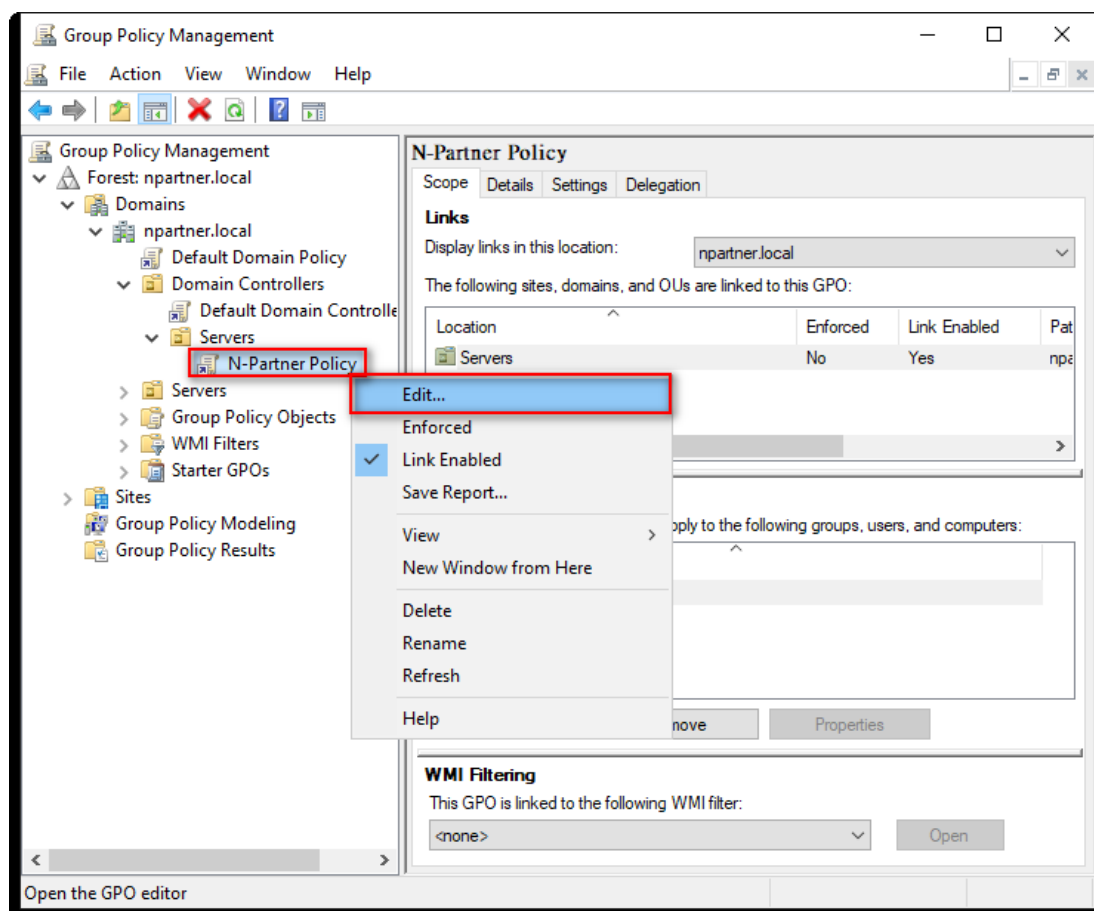
7.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object

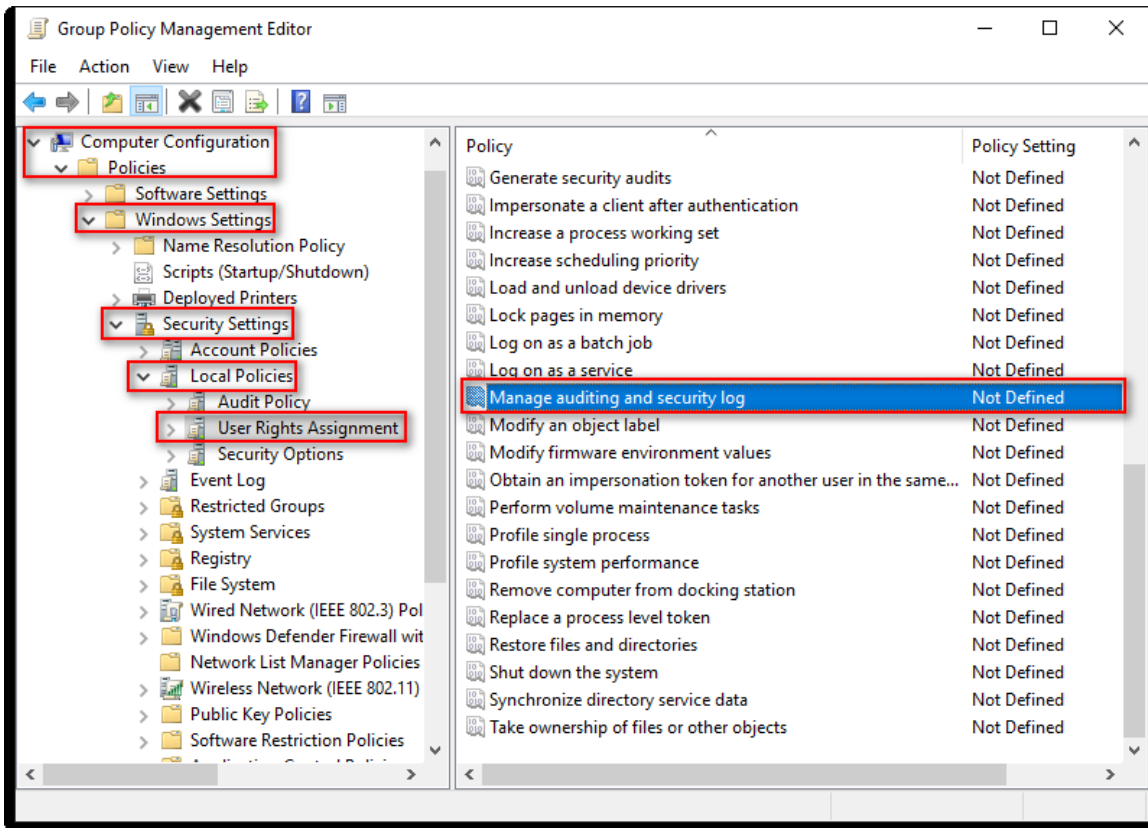
Right-click the “N-Partner Policy” Group Policy Object and select “Edit.”



(3) Configure Log Permissions

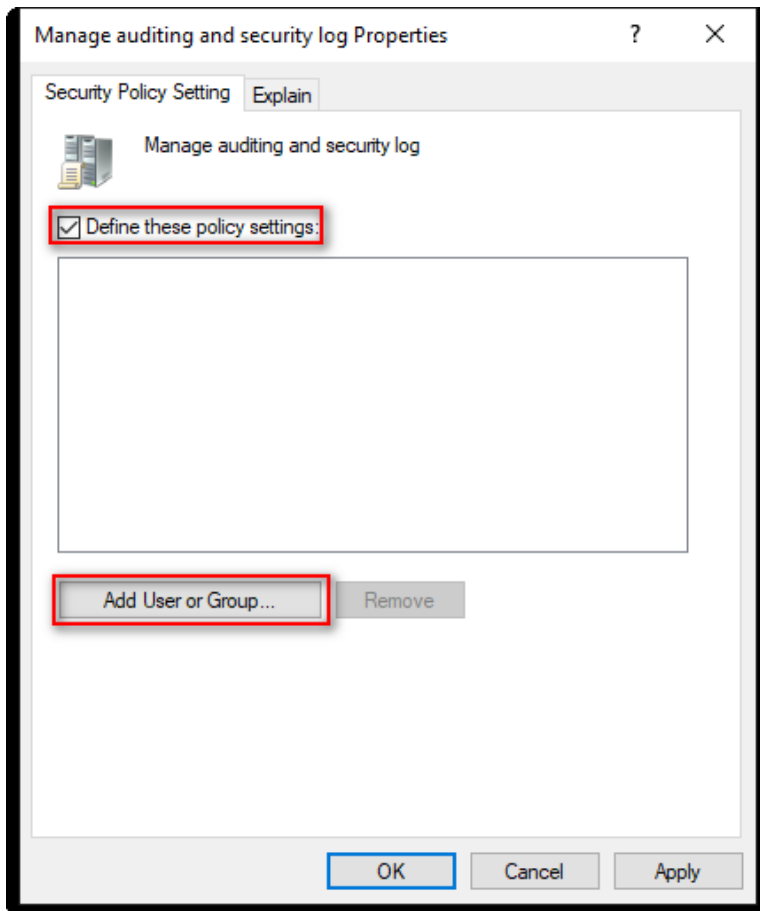
Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

Select “Manage auditing and security log,” then click  “Properties.”



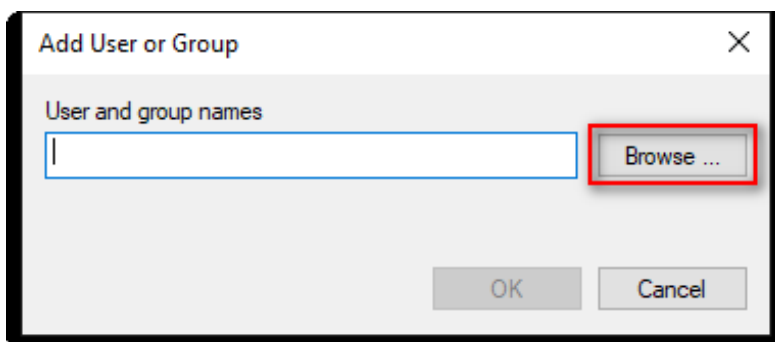
(4) Add Audit Log Management User

Check “Define these policy settings, then click Add Users or Groups...”



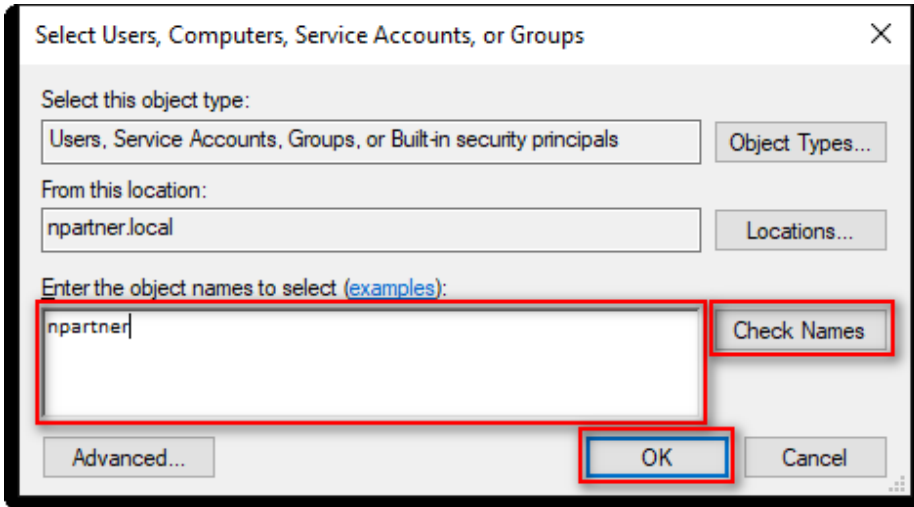
(5) Search for User

Click “Browse.”



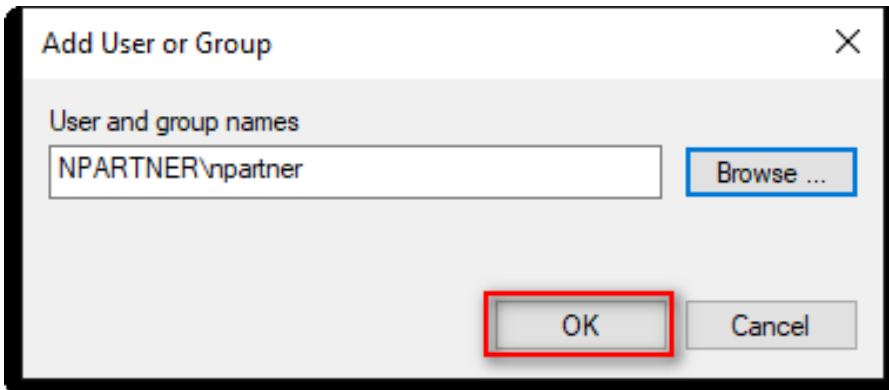
(6) Enter User Account

Enter the user account "npartner," click "Check Names," then click "OK."



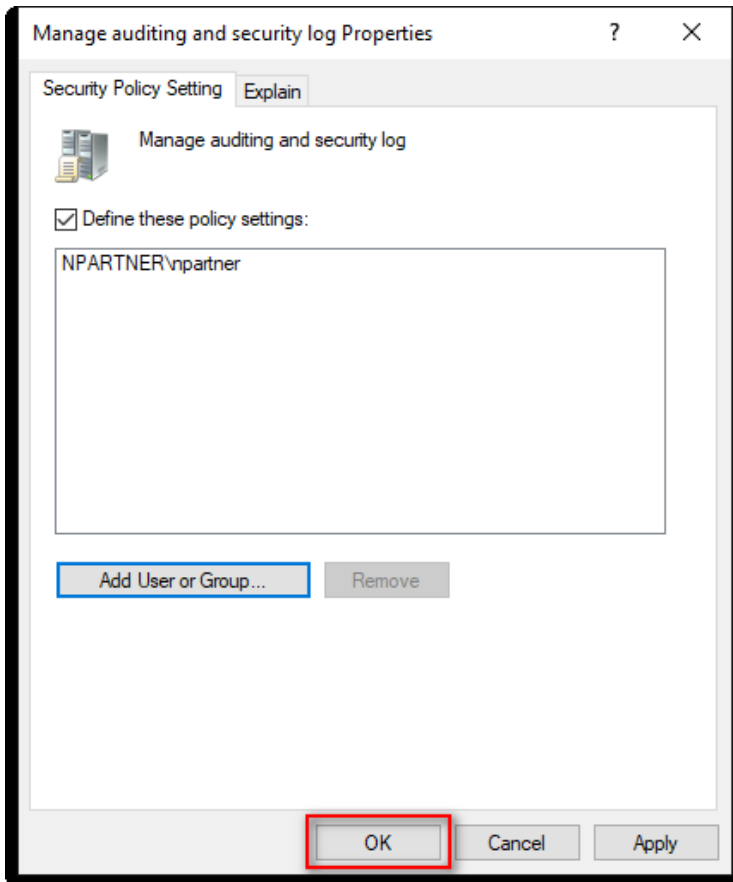
(7) Confirm User

Click "OK."



(8) Confirm Log Settings

Click "OK" to save the configuration.

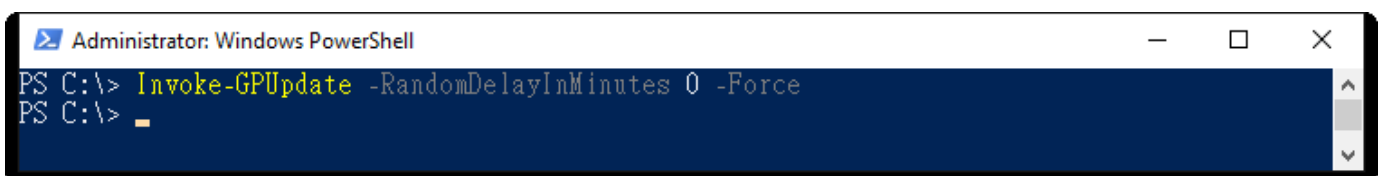


(9) Open "Windows PowerShell."



(10) Run the following command to update group policy:

```
PS C:\> Invoke-GPUUpdate -RandomDelayInMinutes 0 -Force
```



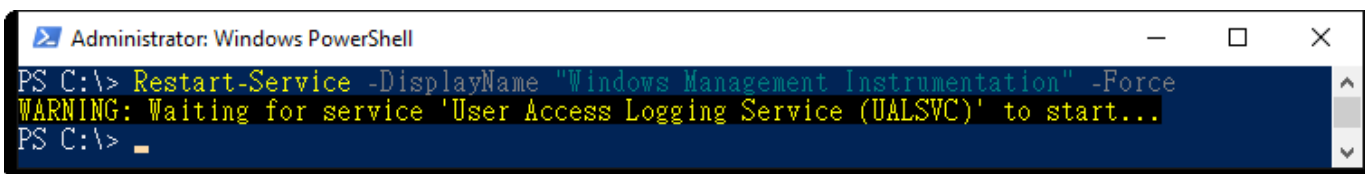
7.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”



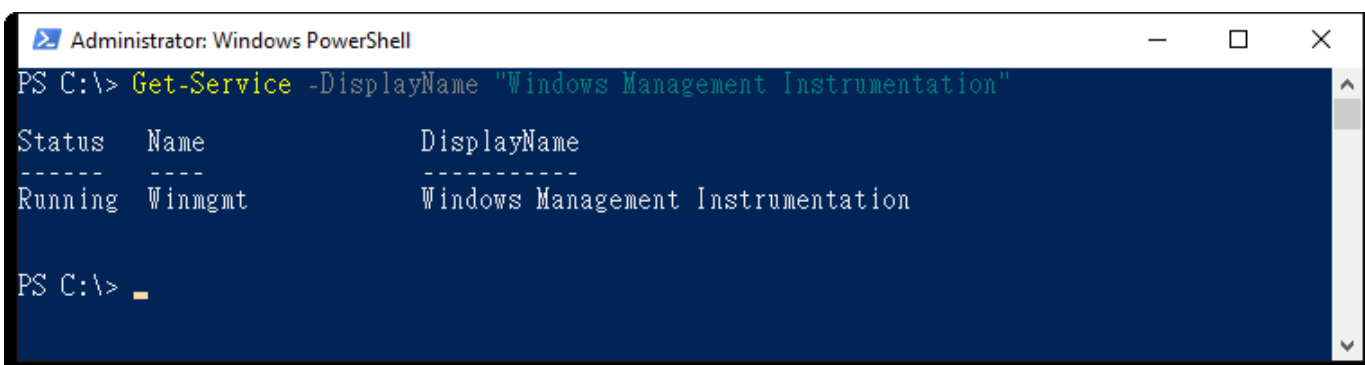
(2) Run the following command to restart the WMI Service:

```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) Run the following command to check the WMI Service Status:

```
PS C:\> Get-Service -DisplayName "Windows Management Instrumentation"
```



7.4 Configure Firewall

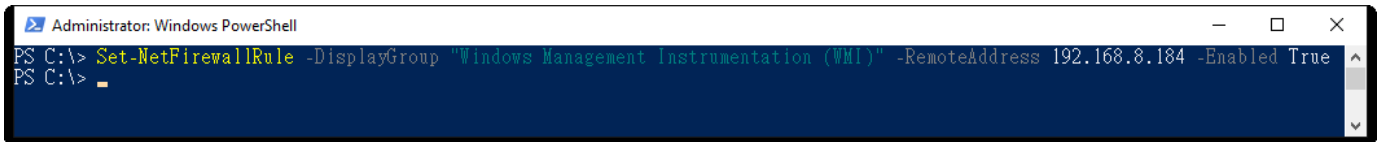
(1) Open "Windows PowerShell."



(2) Configure the Firewall (Allow Only the N-Reporter IP to Query WMI)

Run the following command:

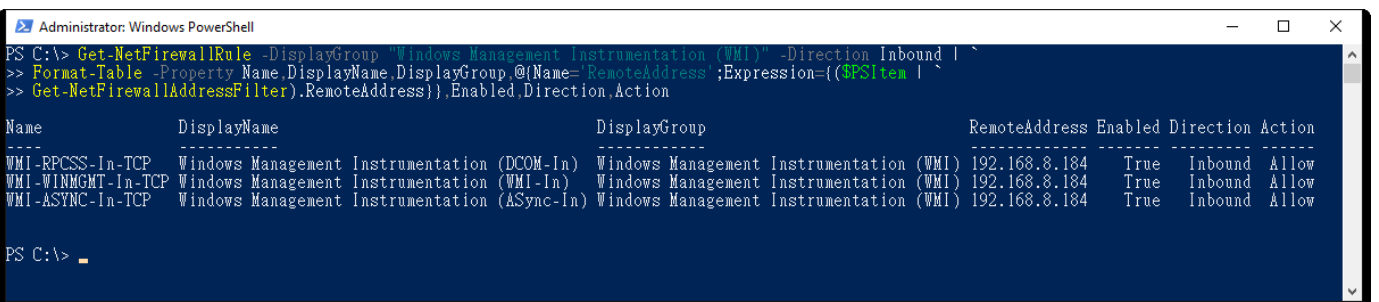
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.184 -Enabled True
```



Replace the highlighted IP address with the N-Reporter system IP address.

(3) Run the following command to check the WMI Firewall Status:

```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={(Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



8. N-Reporter

(1) Add a Windows AD WMI Device

Go to "Device → Device Treeview," then click "Add."

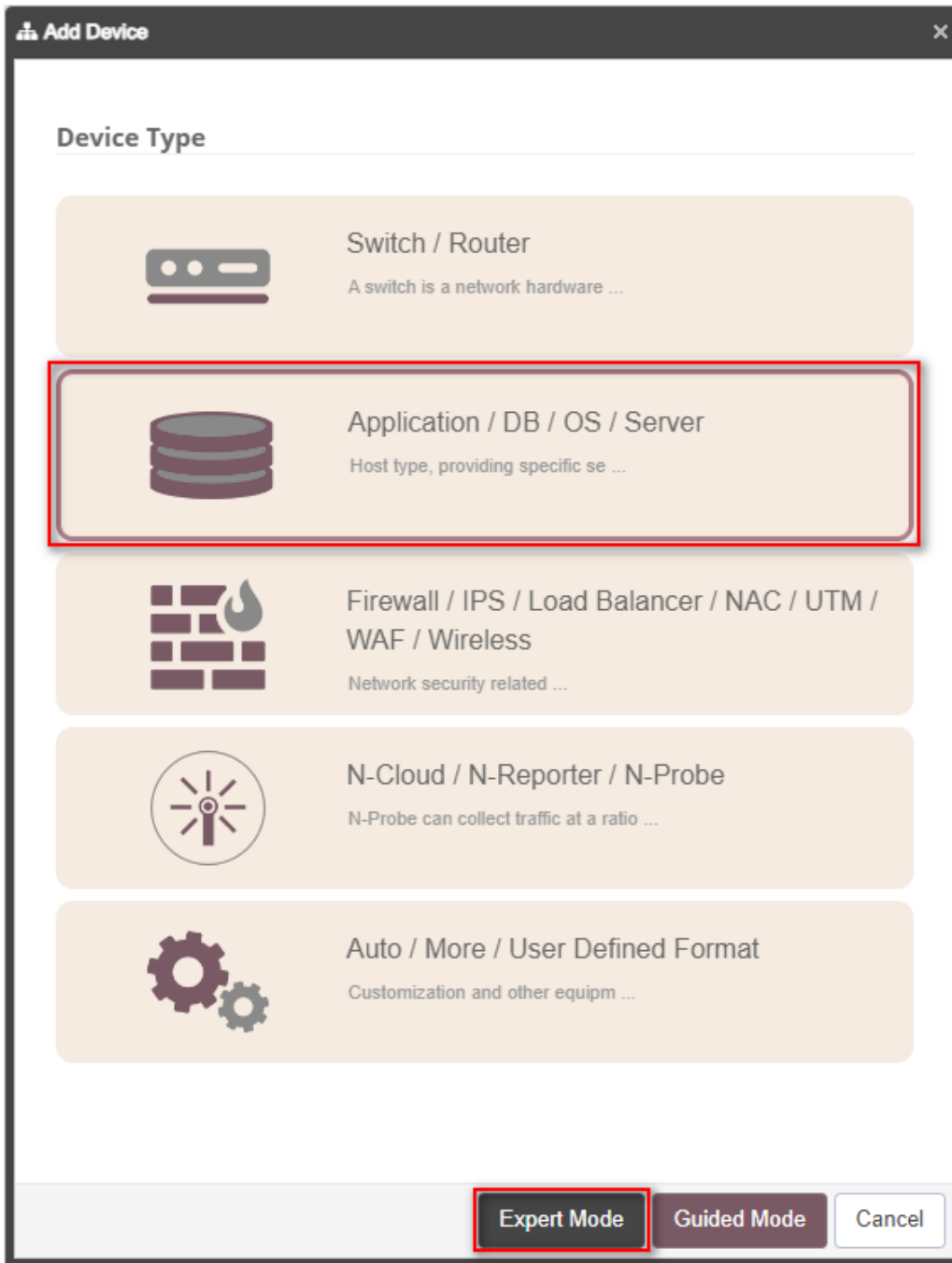
The screenshot shows the N-Reporter web interface. The left sidebar menu has 'Device' selected, with 'Device Treeview' highlighted. The main content area is titled 'Device Treeview' and contains a search bar, a 'Reset' button, a 'Start Query' button, and an 'Add' button (highlighted with a red box). Below the search bar, there is a tree view showing 'Global (479/495)' and 'Unknown Device (0/39)'. The right panel displays details for a device named 'Win2003 AD Eng WMI 192.168.14.74'. The details include IP, Device Type, Data Type, Device Description, Device Alert Template, and ICMP Alert Template. Below the details, there are tabs for 'Interface' and 'Partition', and a table for 'Interface Monitoring Status'. The table is currently empty, showing 'No data!'. The footer contains copyright information and the last account activity timestamp.

Operation	Interface Name	Inte	IfSpec	IfType	Interface Des	IfAlias	Mon	Oper	View
No data!									

8.1 For Windows 2003 or Earlier

(1) Configure a Windows AD WMI Device

Click “Application / DB / OS / Server,” then select “Expert Mode.”



(2) Enter the “device name” and “IP address.” For Syslog Data Type, select “Windows 2003 AD Server (WMI).”

The screenshot shows the 'Edit Device Setting' window with the following configuration details:

- Machine Name ***: Win2003 AD WMI 192.168.14.75
- IP ***: 192.168.14.75
- Domain ***: Global
- Syslog Data Type ⓘ**: Windows 2003 AD Server (WMI)
- User Defined Syslog Format ⓘ +**: Please select ...
- SNMP Model ⓘ**: Please select ...
- Web Monitor ⓘ**: Activate Page Monitoring

Buttons at the bottom: Previous, Submit, Cancel

(3) Click “Syslog” tab and set “Encoding” to “UTF-8.”

The screenshot shows the 'Edit Device Setting' window with the 'Syslog' tab selected. The 'Syslog Setting' section is expanded. The 'Encoding' dropdown menu is highlighted with a red box and set to 'UTF-8'. Below it, the 'Syslog Normalized Data Retention Days (Max)' field is empty. The 'Raw Data Kept and Replied' section contains three unchecked checkboxes: 'Raw Data Kept', 'Raw data format is adopted while Syslog relaying is activated in Threshold Report.', and 'The source IP will be kept in normalized data relaying'. At the bottom, there are 'Previous', 'Submit', and 'Cancel' buttons.

(4) Click “Action & Backup,” tab then enter the WMI Login Account and Password.

The screenshot shows the 'Edit Device Setting' window with the following elements:

- Navigation tabs: Essentials, SNMP, Syslog, Flow, **Action & Backup** (highlighted), Monitor & Alert, Other.
- Section: Action Device / VRF / SSH Related Setting
- Section: Action Device
 - Activate Action Device
 - Action URL
- Section: VRF (Virtual Routing and Forwarding)
- Section: Device Connection Method
 - SSH
 - Telnet
- Section: Login Account
 - Login Account: npartner
 - Login Password: *****
- Section: Enable Password
- Section: API IP & Login Related Setting
- Buttons: Previous, Submit, Cancel

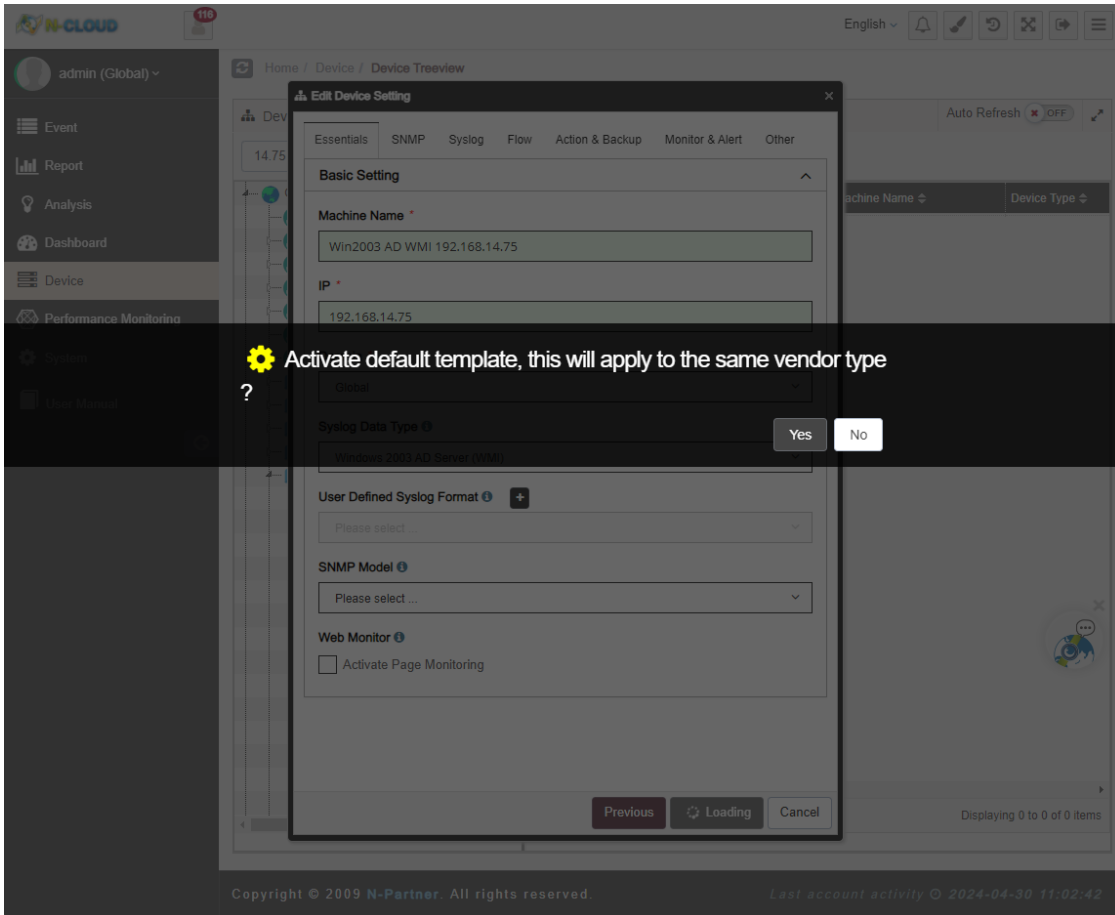
(5) Click “Monitor & Alert” tab. For Testing Device, select the N-Cloud device. Click “Device Connection Test.” If the Test Result shows “Connection Test Succeeded”, the WMI login test is successful. Then click “Submit.”

Note: If the Windows WMI device is managed by an N-Probe device, select N-Probe as the Testing Device. The N-Probe will perform the WMI login test to the Windows device.

The screenshot shows the 'Edit Device Setting' window with the 'Monitor & Alert' tab selected. The 'Testing Device' dropdown menu is set to 'N-Cloud 14.1'. Below this, there is a 'Start Test' button. A table lists various test items, with 'Device Connection Test' selected and showing a 'Connection Test Succeeded' result. At the bottom, the 'Submit' button is highlighted.

Function Item	Test Result
Ping Test	
SNMP Test	
IP/MAC SNMP Test	
IP/MAC Connection Test	
Device Connection Test	Connection Test Succeeded
API Connection Test	

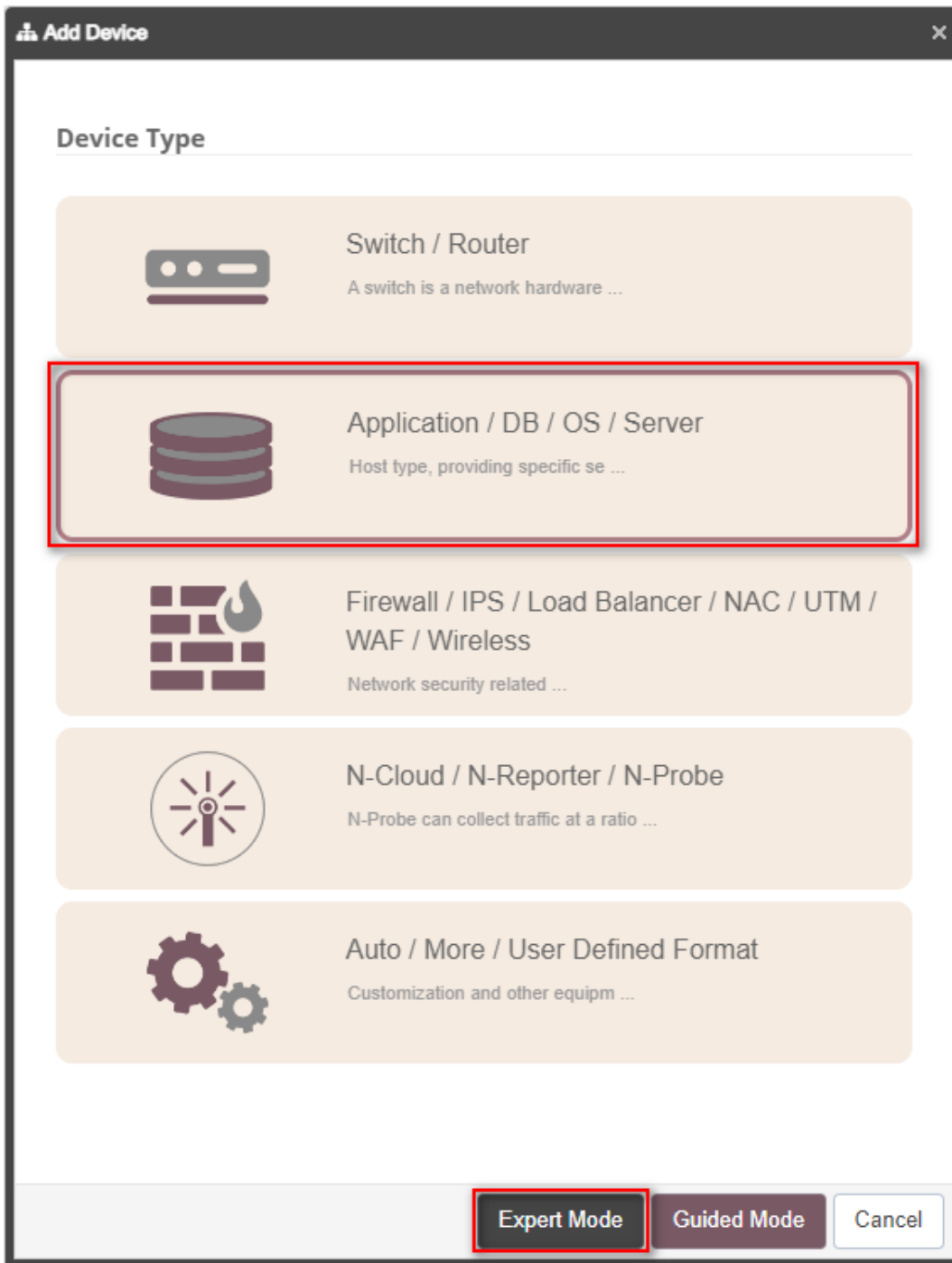
(6) To enable the default reports for the Windows WMI device, click “Yes.” To disable them, click “No.”



8.2 For Windows 2008 or Later

(1) Configure a Windows AD WMI Device

Click “Application / DB / OS / Server,” then select “Expert Mode.”



(2) Enter the device name and IP address. For “Syslog Data Type,” select “Windows 2003 AD Server (WMI).”

The screenshot shows the 'Edit Device Setting' window with the 'Syslog' tab selected. The 'Basic Setting' section is expanded, showing the following fields:

- Machine Name ***: Win2008 AD WMI 192.168.14.77
- IP ***: 192.168.14.77
- Domain ***: Global
- Syslog Data Type ⓘ**: Windows 2008/2012 AD Server (WMI)
- User Defined Syslog Format ⓘ +**: Please select ...
- SNMP Model ⓘ**: Please select ...
- Web Monitor ⓘ**: Activate Page Monitoring

At the bottom of the window, there are three buttons: 'Previous', 'Submit', and 'Cancel'.

(3) Click “Syslog” tab and set Encoding to “UTF-8.”

The screenshot shows a web interface titled "Edit Device Setting" with a close button (X) in the top right corner. Below the title bar are several tabs: "Essentials", "SNMP", "Syslog", "Flow", "Action & Backup", "Monitor & Alert", and "Other". The "Syslog" tab is highlighted with a red box. Below the tabs is a section titled "Syslog Setting" with an expand/collapse arrow. Under this section, there are three main areas: 1. "Facility" with a dropdown menu showing a dashed line. 2. "Encoding" with a dropdown menu showing "UTF-8", which is highlighted with a red box. 3. "Syslog Normalized Data Retention Days (Max)" with an empty text input field. Below these is a section titled "Raw Data Kept and Replied" containing three checkboxes: "Raw Data Kept", "Raw data format is adopted while Syslog relaying is activated in Threshold Report.", and "The source IP will be kept in normalized data relaying". At the bottom of the window are three buttons: "Previous", "Submit", and "Cancel".

(4) Left click “Action & Backup,” then enter the WMI login account and password.

The screenshot shows the 'Edit Device Setting' window with the following configuration:

- Tab: **Action & Backup** (highlighted with a red box)
- Section: **Action Device / VRF / SSH Related Setting**
- Action Device**
 - Activate Action Device
 - Action URL: [Empty]
- VRF (Virtual Routing and Forwarding)**
 - [Empty]
- Device Connection Method**
 - SSH
 - Telnet
- Login Account**
 - Field: npartner
- Login Password**
 - Field: [Masked]
- Enable Password**
 - Field: [Empty]
- Section: **API IP & Login Related Setting**

Buttons at the bottom: Previous, Submit, Cancel

(5) Left-click “Monitor & Alert” and select the N-Cloud device for Testing Device. Click [Device Connection Test]. If the Test Result shows “Connection Test Succeeded,” the WMI login is successful. Then click [Submit].

Note: If the Windows WMI device is managed by an N-Probe, select N-Probe as the Testing Device. The WMI login will be tested via the N-Probe.

The screenshot shows the 'Edit Device Setting' window with the 'Monitor & Alert' tab selected. The 'Testing Device' dropdown menu is set to 'N-Cloud 14.1'. Below this, there is a 'Start Test' button. A table displays the results of various tests:

Function Item	Test Result
Ping Test	
SNMP Test	
IP/MAC SNMP Test	
IP/MAC Connection Test	
Device Connection Test	Connection Test Succeeded
API Connection Test	

At the bottom of the window, there are three buttons: 'Previous', 'Submit', and 'Cancel'. The 'Submit' button is highlighted.

(6) To enable the default reports for Windows WMI devices, click “Yes.” To disable, click “No.”

The screenshot shows the N-Cloud management interface. A modal window titled "Edit Device Setting" is open, showing configuration for a device. The "Essentials" tab is active, displaying fields for "Machine Name" (Win2003 AD WMI 192.168.14.75) and "IP" (192.168.14.75). Below these, the "Syslog Data Type ID" is set to "Windows 2003 AD Server (WMI)". There are also fields for "User Defined Syslog Format" and "SNMP Model", both currently showing "Please select...". A "Web Monitor" section includes a checkbox for "Activate Page Monitoring". A black overlay with a gear icon and the text "Activate default template, this will apply to the same vendor type" is positioned over the dialog, with a "Yes" button highlighted. The background interface shows a sidebar with navigation options like "Event", "Report", "Analysis", "Dashboard", "Device", "Performance Monitoring", "System", and "User Manual". The footer contains copyright information: "Copyright © 2009 N-Partner. All rights reserved." and "Last account activity © 2024-04-30 11:02:42".

9. Troubleshooting

9.1 Invoke-GPUUpdate Error

(1) On the AD domain server, an error message appears when running **Invoke-GPUUpdate** to update the Windows Server Group Policy.

```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
Invoke-GPUUpdate : Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled
Tasks Management Firewall rules are disabled.
Parameter name: computer
At line:1 char:1
+ Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
+ ~~~~~
+ CategoryInfo          : OperationTimeout: (:) [Invoke-GPUUpdate], ArgumentException
+ FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUUpdateCommand
PS C:\>
```

(2) Open “Windows PowerShell” on the Windows Server.



(3) Check the Windows Firewall rules for **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**.

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```

```
Administrator: Windows PowerShell
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
Name                DisplayName                Enabled Direction Action
-----
WMI-WINMGMT-In-TCP  Windows Management Instrumentation (WMI-In)    True   Inbound Allow
vm-monitoring-rpc   Virtual Machine Monitoring (RPC)                False  Inbound Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP) False  Inbound Allow
PS C:\>
```

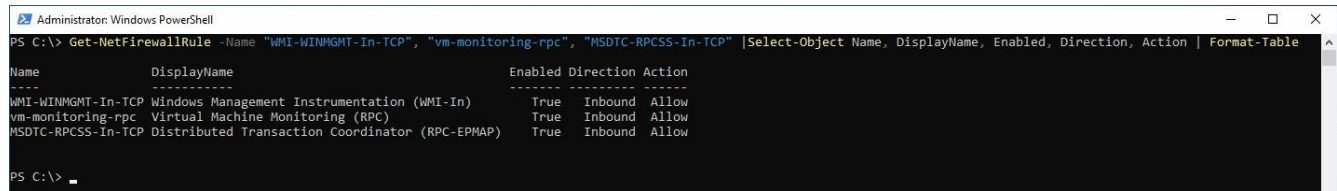
(4) Enable the Windows Firewall rules: **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**.

```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
```

```
Administrator: Windows PowerShell
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
PS C:\>
```

(5) Check the Windows Firewall rules for WMI-WINMGMT-In-TCP, vm-monitoring-rpc, and MSDTC-RPCSS-In-TCP.

```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



```
Administrator: Windows PowerShell
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
Name                DisplayName                Enabled Direction Action
-----
WMI-WINMGMT-In-TCP  Windows Management Instrumentation (WMI-In)      True    Inbound Allow
vm-monitoring-rpc   Virtual Machine Monitoring (RPC)                  True    Inbound Allow
MSDTC-RPCSS-In-TCP Distributed Transaction Coordinator (RPC-EPMAP)    True    Inbound Allow
PS C:\>
```

(6) On the AD domain server, update the Windows Server Group Policy.

```
PS C:\> Invoke-GPUdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
```

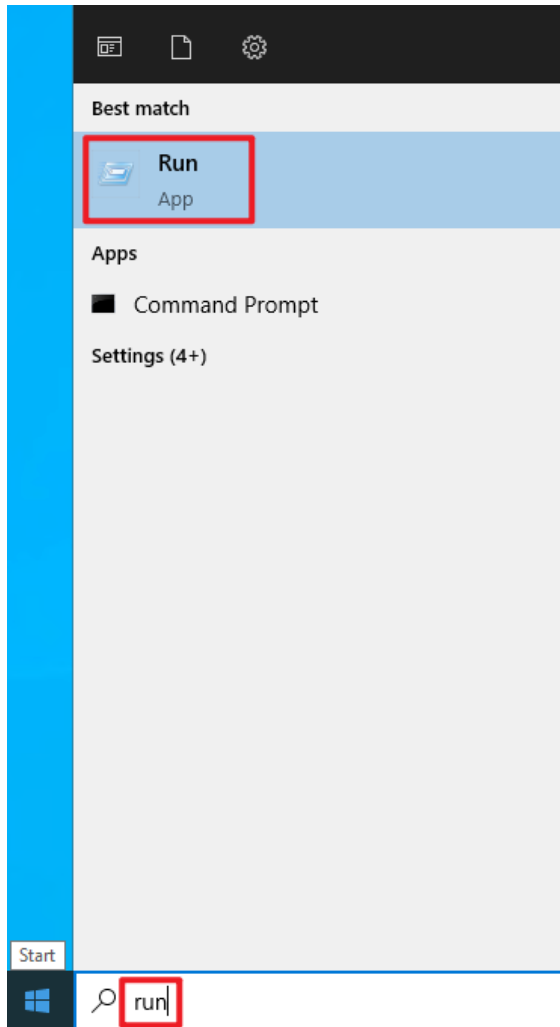


```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUdate -Computer $_.name -RandomDelayInMinutes 0 -Force
PS C:\>
```

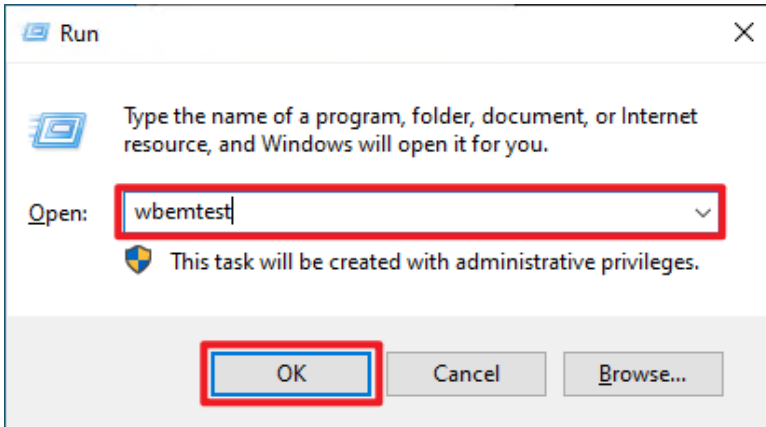
Enter the Windows Server name in the red-highlighted field.

9.2 WMI Query Language Verification

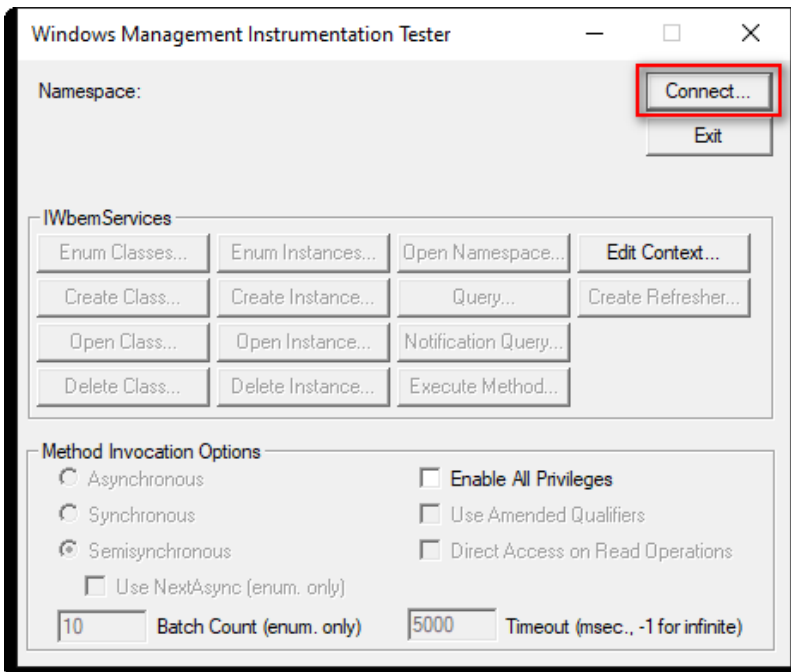
(1) Click "Start" → type "Run" → select "Run."



(2) Enter “wbemtest” → Click “OK.”



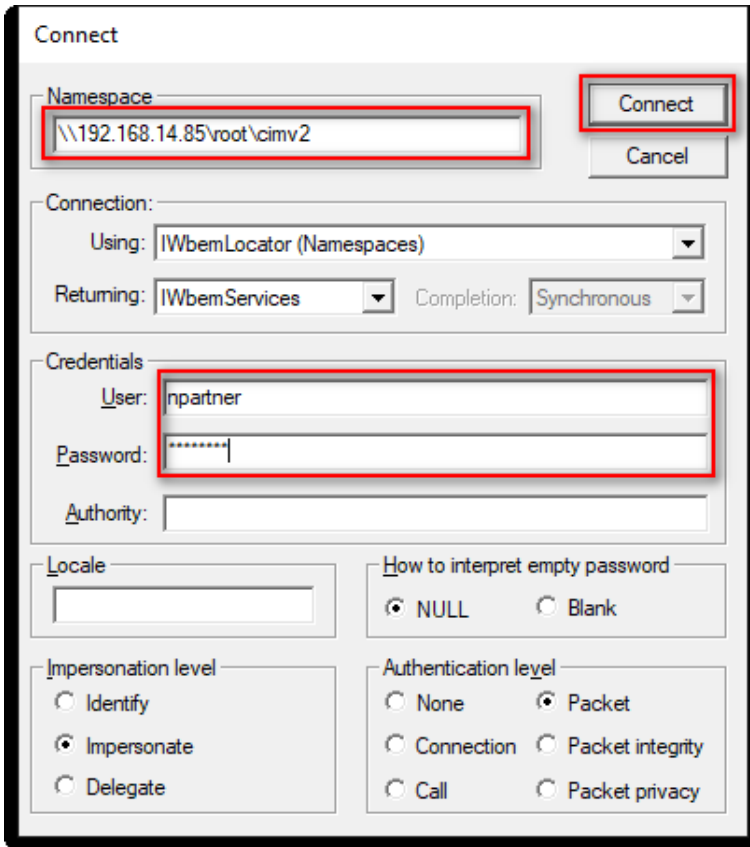
(3) Click “Connect.”



(4) Enter the namespace:

\\<Windows AD IP>\root\cimv2

Enter the username and password → Click “Connect.”



Connect

Namespace: \\192.168.14.85\root\cimv2

Connect

Cancel

Connection:

Using: IWbemLocator (Namespaces)

Returning: IWbemServices Completion: Synchronous

Credentials

User: npartner

Password: *****

Authority:

Locale:

How to interpret empty password

NULL Blank

Impersonation level

Identify

Impersonate

Delegate

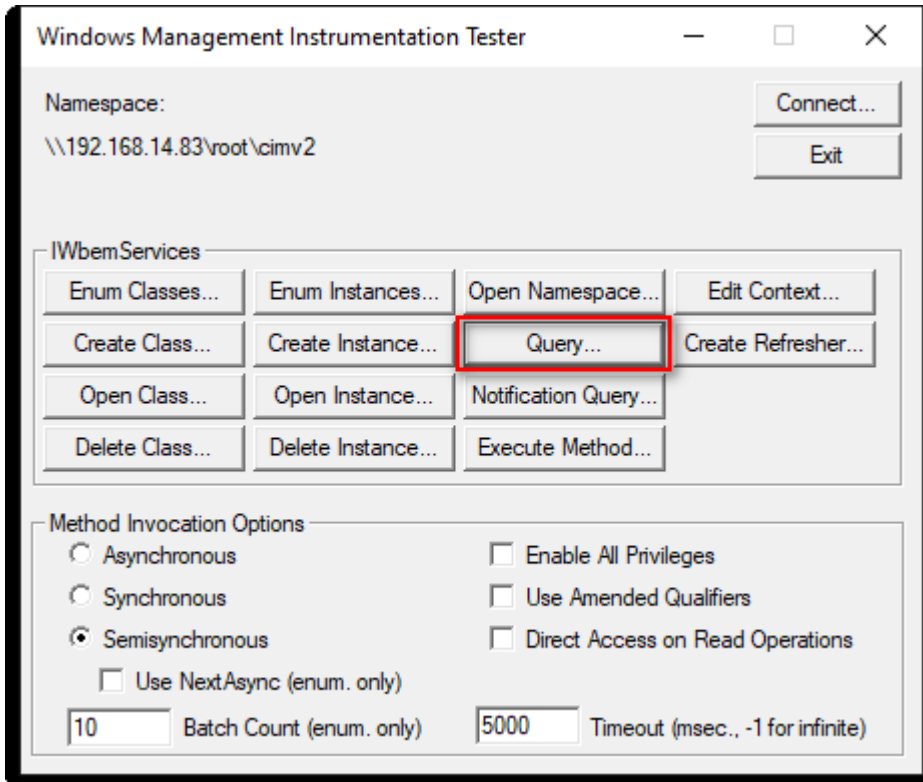
Authentication level

None Packet

Connection Packet integrity

Call Packet privacy

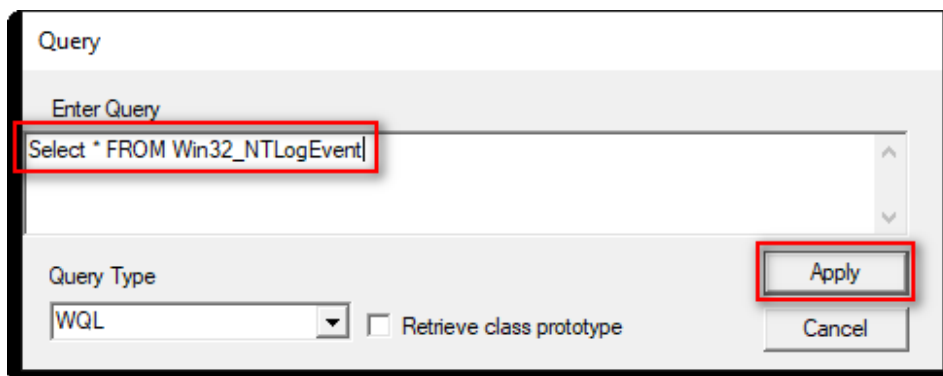
(5) Click “Query.”



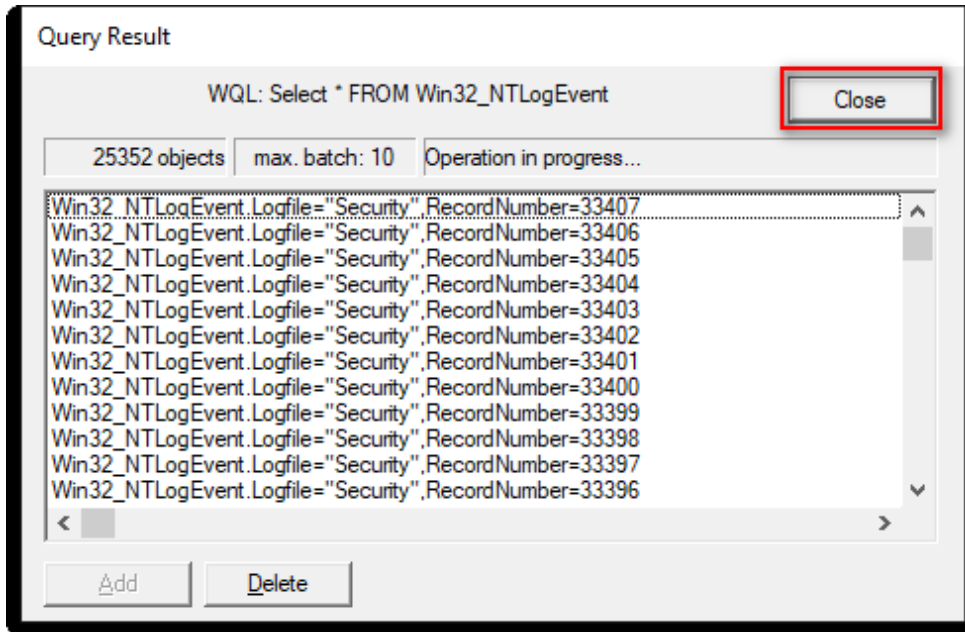
(6) Enter the query:

```
SELECT * FROM Win32_NTLogEvent
```

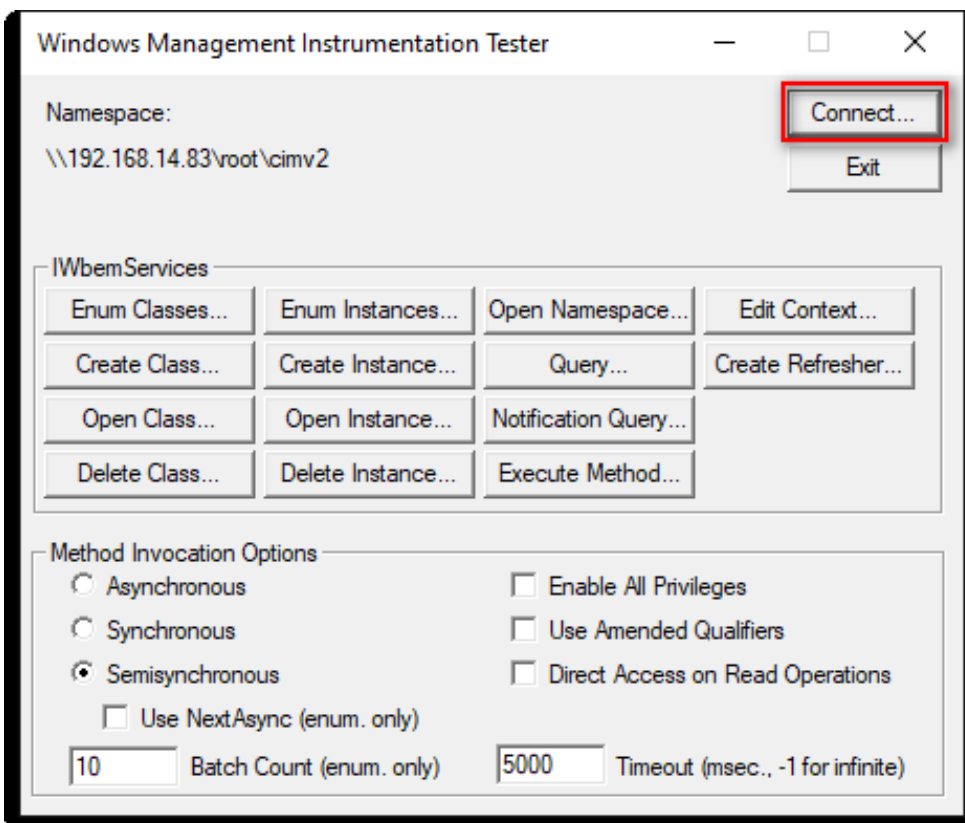
→ Click “Apply.”



(7) If data is returned, click "Close."



(8) Click "Connect."



(9) Enter the namespace:

\\<Windows AD IP>\root\directory\LDAP

Enter the username and password → Click “Connect.”

The screenshot shows the 'Connect' dialog box with the following fields and options:

- Namespace:** \\192.168.14.83\root\directory\LDAP
- Connection:** Using: IWbemLocator (Namespaces); Returning: IWbemServices; Completion: Synchronous
- Credentials:** User: inpartner; Password: *****
- Locale:** (empty)
- How to interpret empty password:** NULL, Blank
- Impersonation level:** Identify, Impersonate, Delegate
- Authentication level:** None, Packet, Connection, Packet integrity, Call, Packet privacy

(10) Click “Query.”

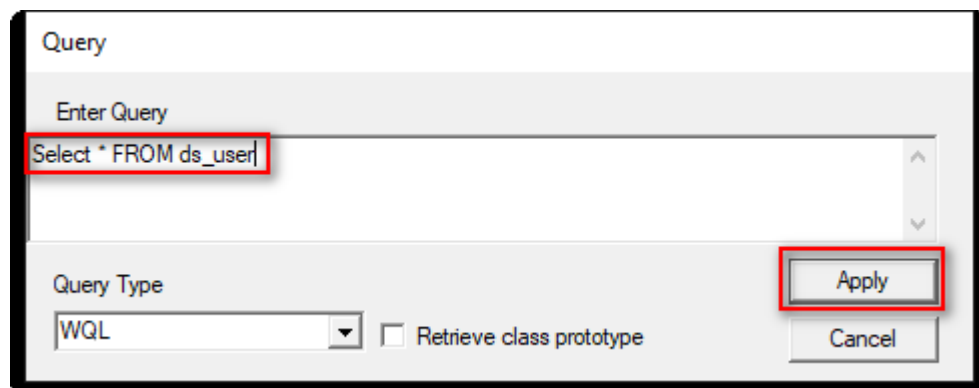
The screenshot shows the 'Windows Management Instrumentation Tester' application with the following fields and options:

- Namespace:** \\192.168.14.83\root\directory\LDAP
- IWbemServices:** Enum Classes..., Enum Instances..., Open Namespace..., Edit Context..., Create Class..., Create Instance..., Query..., Create Refresher..., Open Class..., Open Instance..., Notification Query..., Delete Class..., Delete Instance..., Execute Method...
- Method Invocation Options:** Asynchronous, Synchronous, Semisynchronous, Use NextAsync (enum. only), Enable All Privileges, Use Amended Qualifiers, Direct Access on Read Operations
- Batch Count (enum. only):** 10
- Timeout (msec., -1 for infinite):** 5000

(11) Enter the query:

```
SELECT * FROM ds_user
```

→ Click “Apply.”



Query

Enter Query

Select * FROM ds_user

Query Type

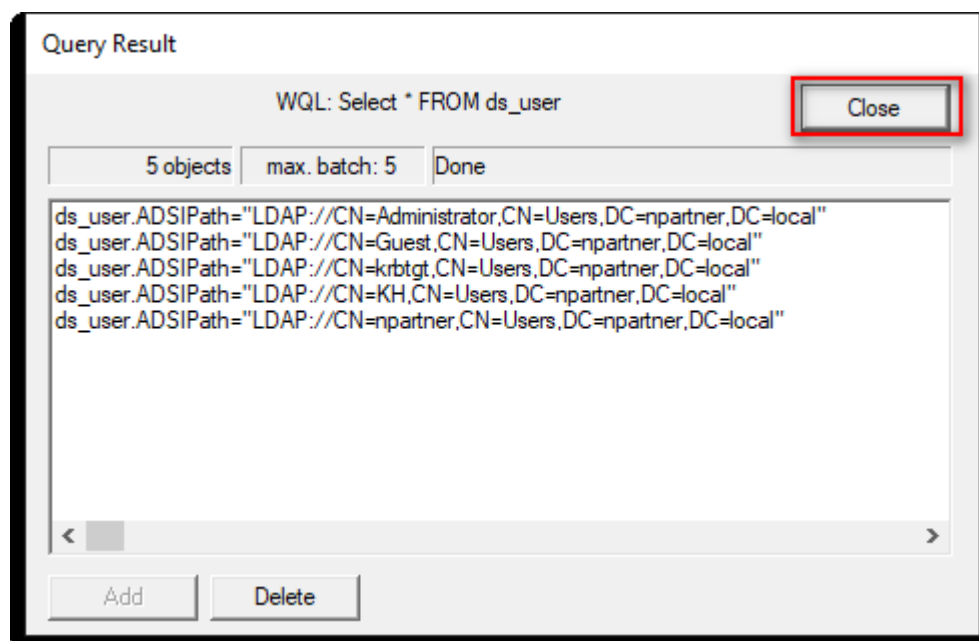
WQL

Retrieve class prototype

Apply

Cancel

(12) If data is returned, click “Close.”



Query Result

WQL: Select * FROM ds_user

Close

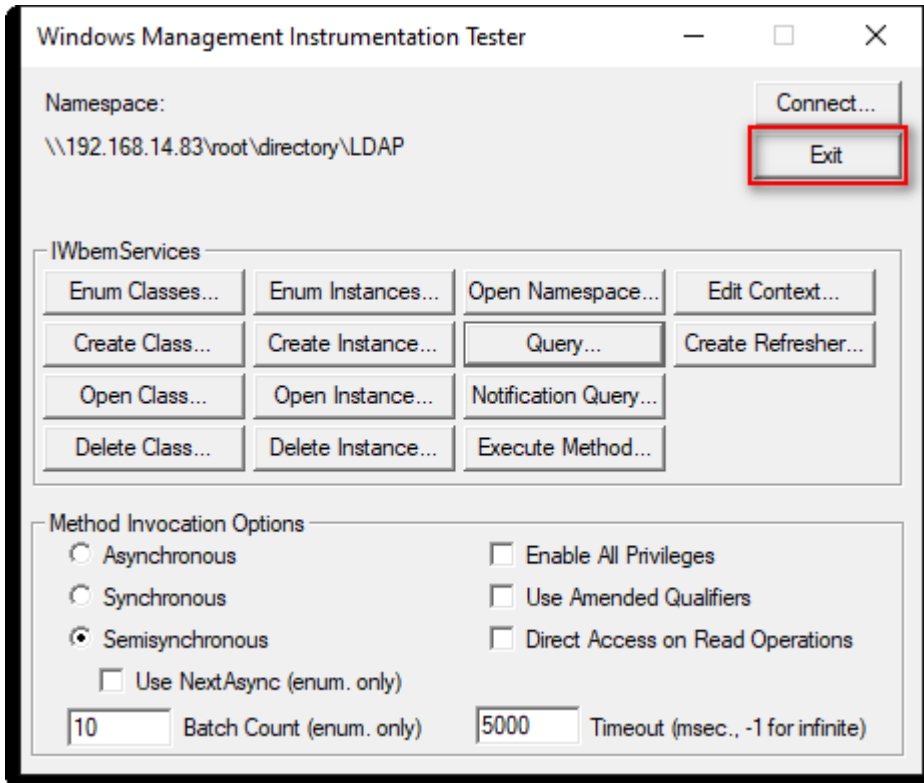
5 objects | max. batch: 5 | Done

ds_user.ADSIPath="LDAP://CN=Administrator,CN=Users,DC=npartner,DC=local"
ds_user.ADSIPath="LDAP://CN=Guest,CN=Users,DC=npartner,DC=local"
ds_user.ADSIPath="LDAP://CN=krbtgt,CN=Users,DC=npartner,DC=local"
ds_user.ADSIPath="LDAP://CN=KH,CN=Users,DC=npartner,DC=local"
ds_user.ADSIPath="LDAP://CN=npartner,CN=Users,DC=npartner,DC=local"

Add | Delete

(13) If both event logs and user data can be queried successfully, the configuration is correct.

Click "Exit" to close the WMI Tester.





Tel : +886-4-23752865 Fax : +886-4-23757458

Sales Information : sales@npartner.com

Technical Support : support@npartner.com