N-Partner

WMI Syslog Management of Windows AD Server

V009

2026/03/25

Copyright Declaration

Registered Trademark

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

Contents

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

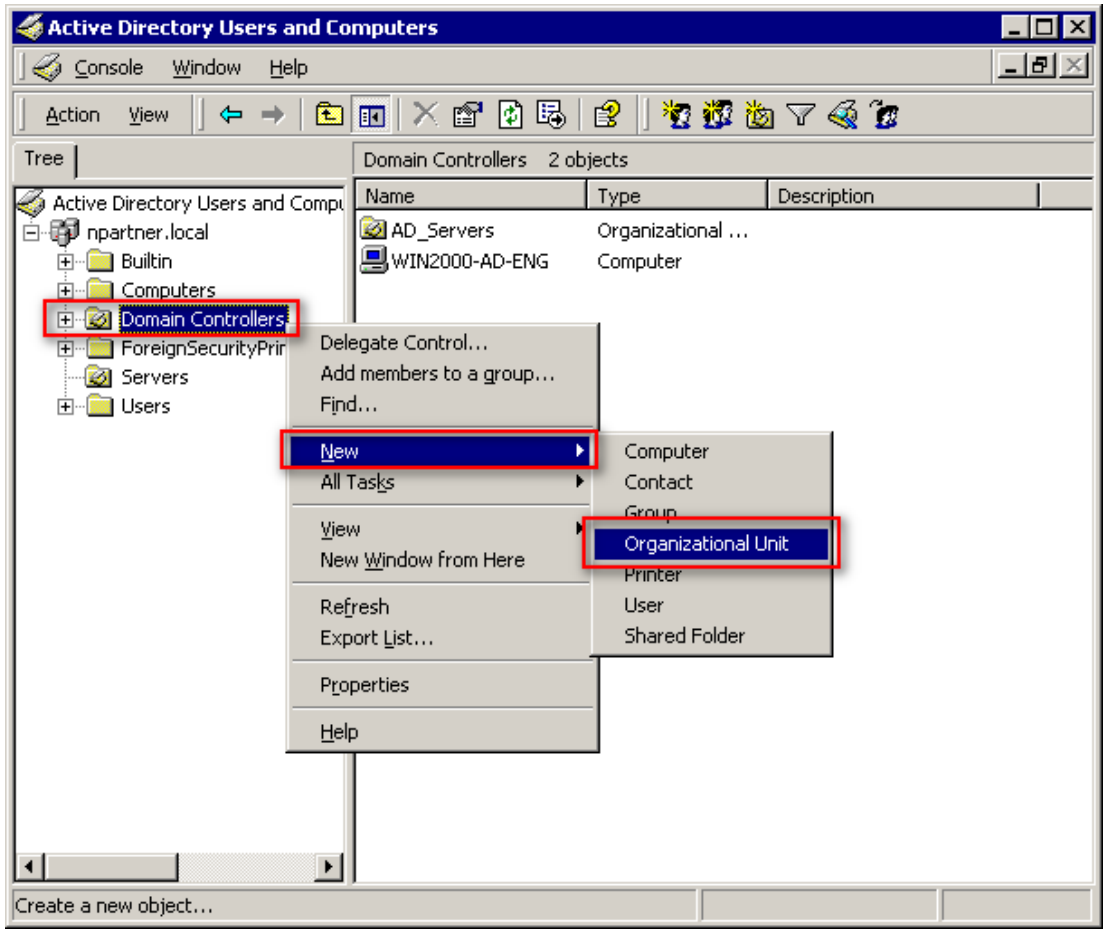
For detailed information on setting Windows audit policies, please refer to the "audit policy recommendations link" in the preface.

1.1 Organizational Unit Settings

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

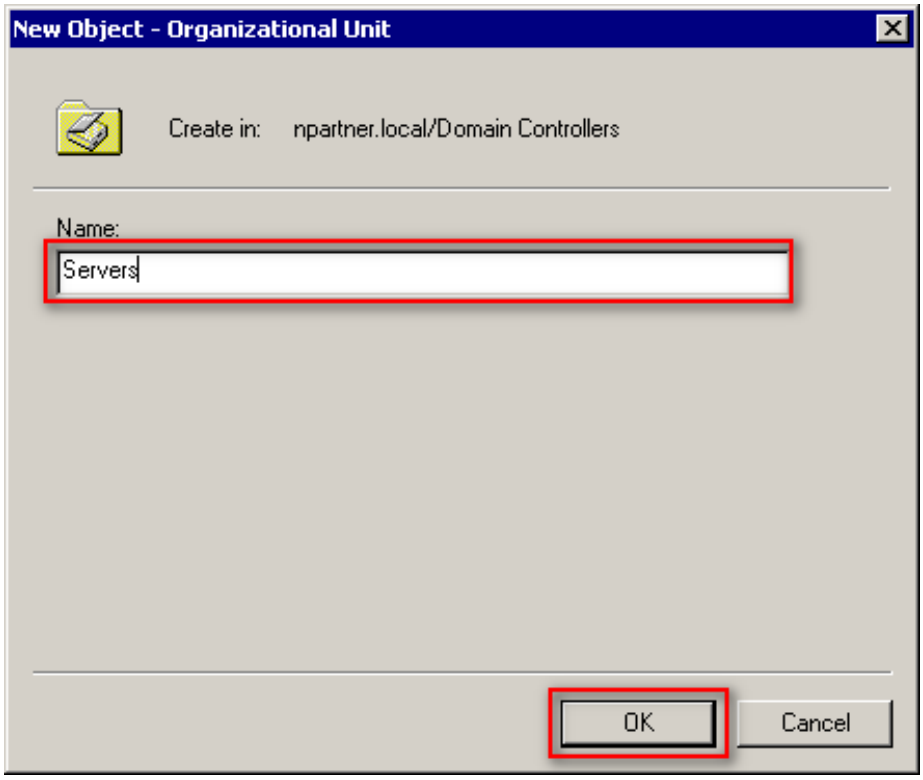
(2) Add an Organizational Unit

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



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

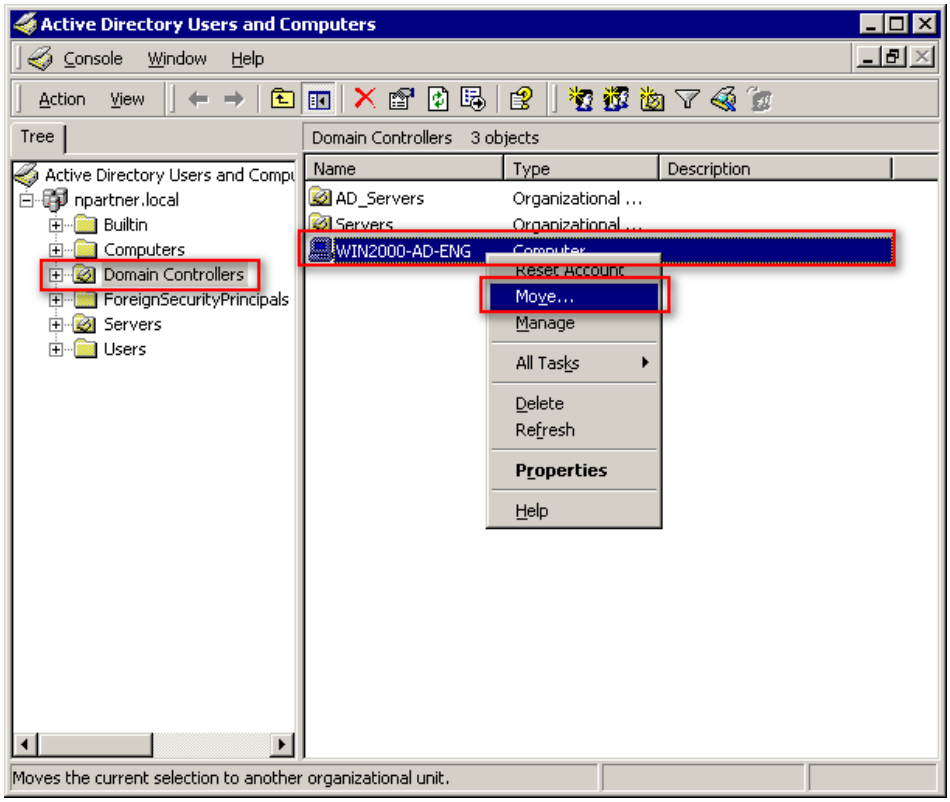
Note: Please create the organizational unit name according to the customer's environment. -> Click “OK.”



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

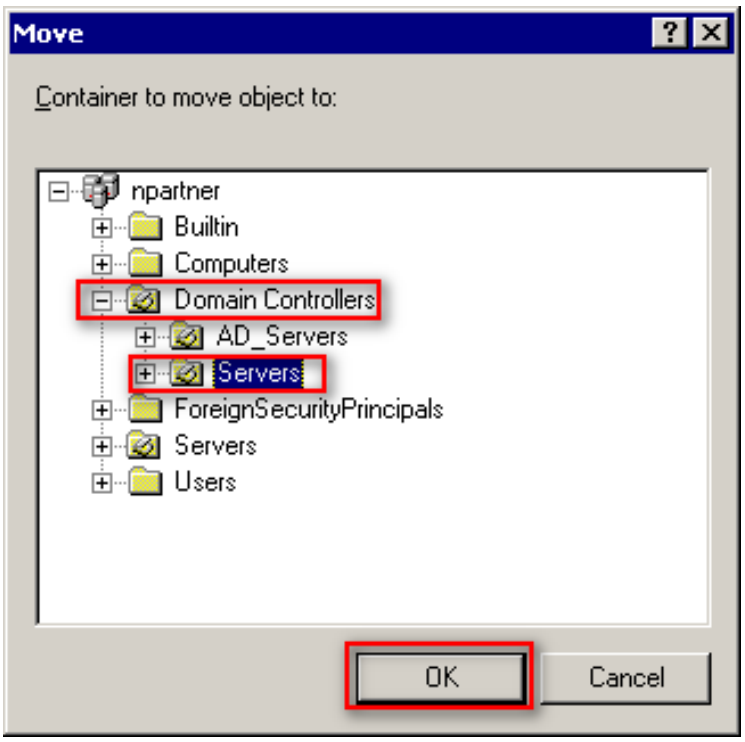
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2000-AD-ENG” server.

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



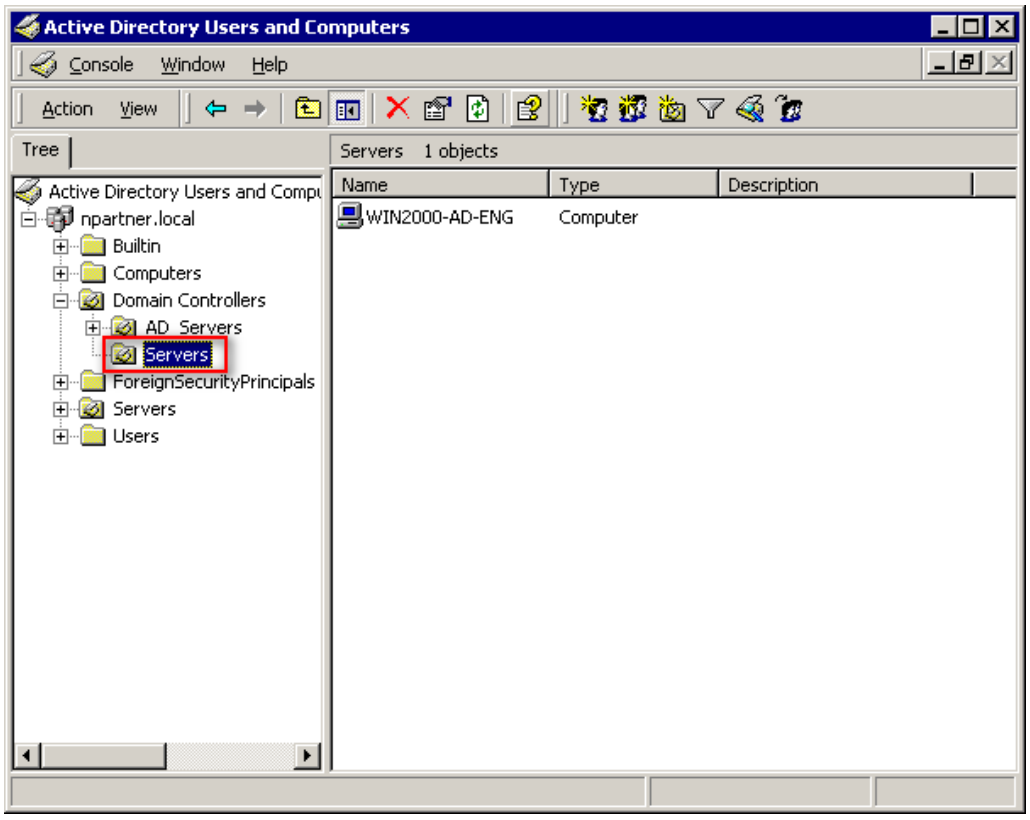
(5) Select your Organizational Unit:

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:

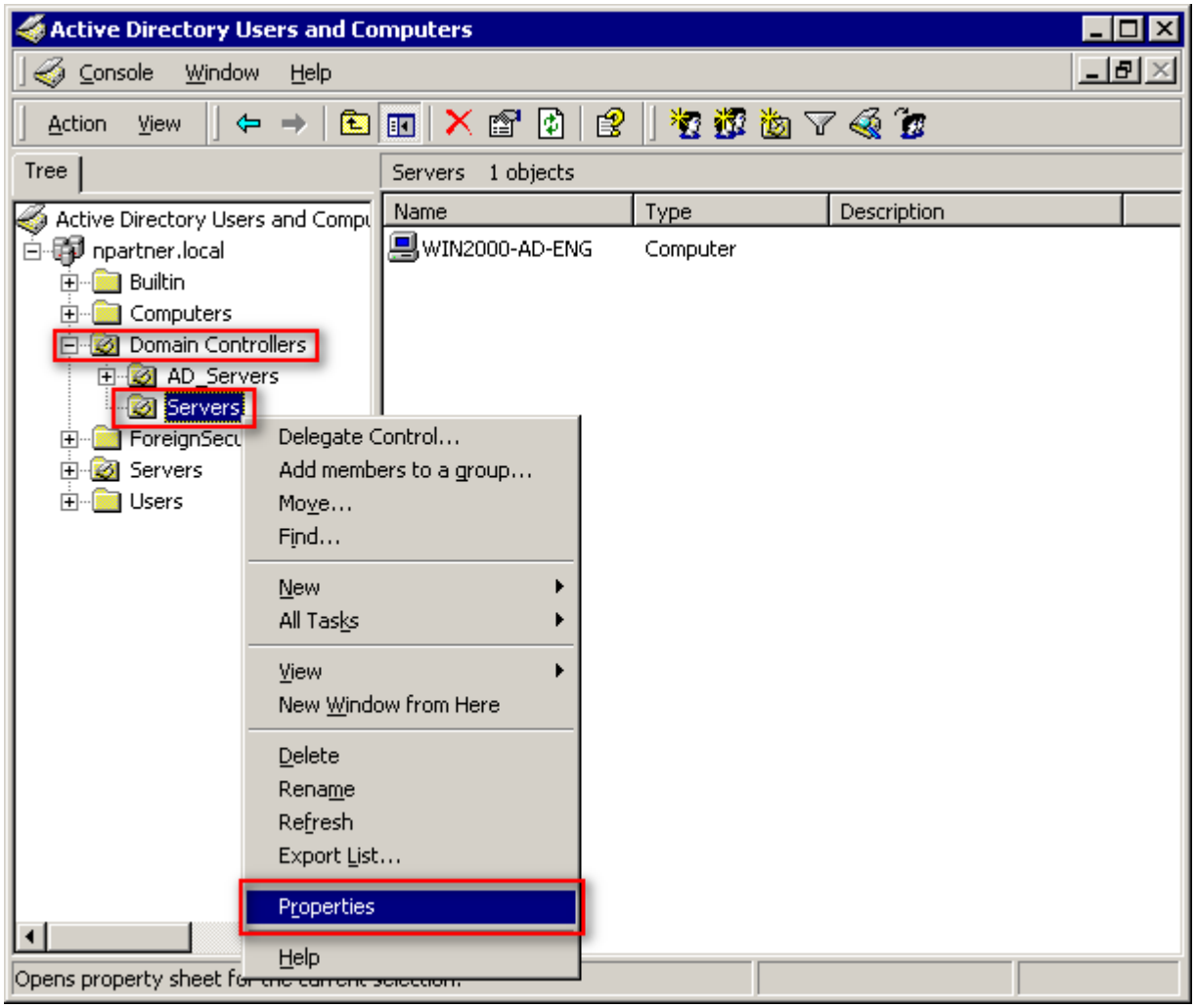
Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2000-AD-ENG” server has been moved.



1.2 Group Policy Settings

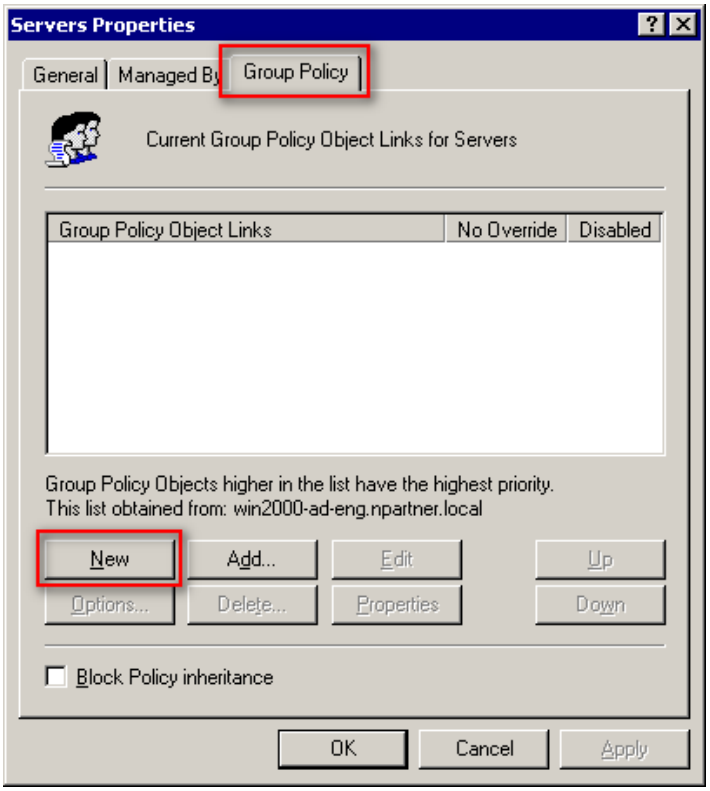
(1) Click “Active Directory Users and Computers.”

(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

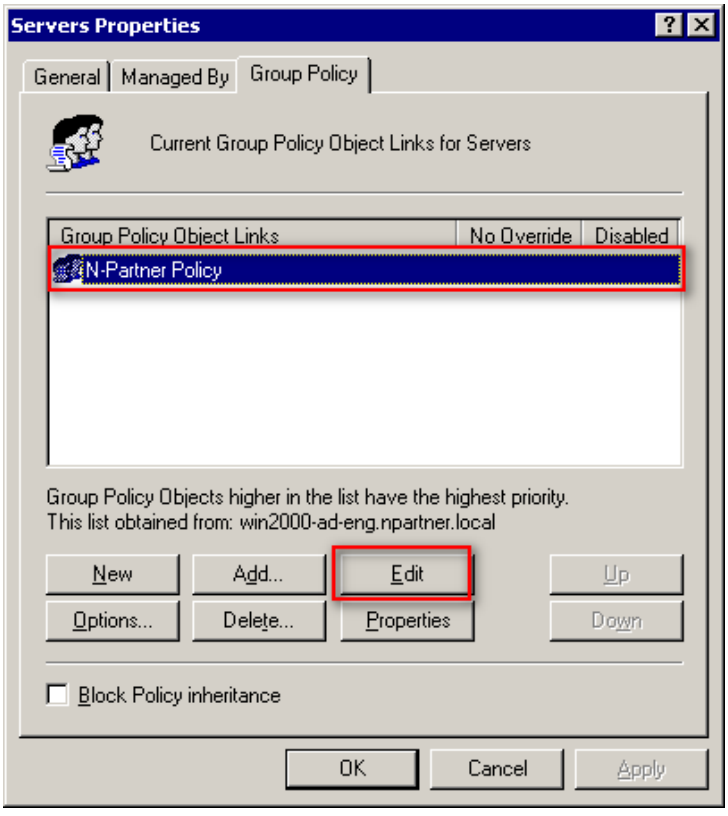
On the “Group Policy” tab, click “New.”



(4) Edit your Group Policy Object

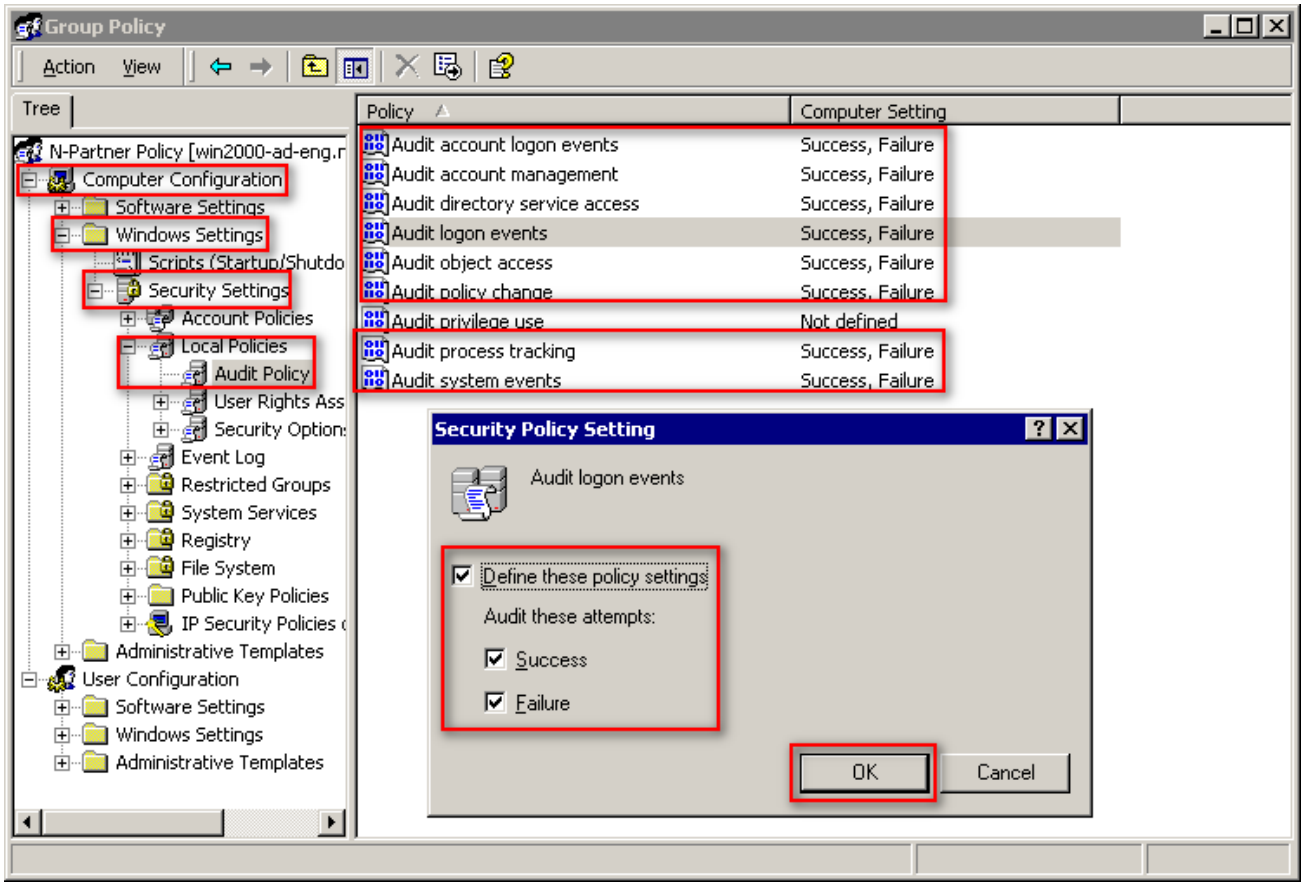
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



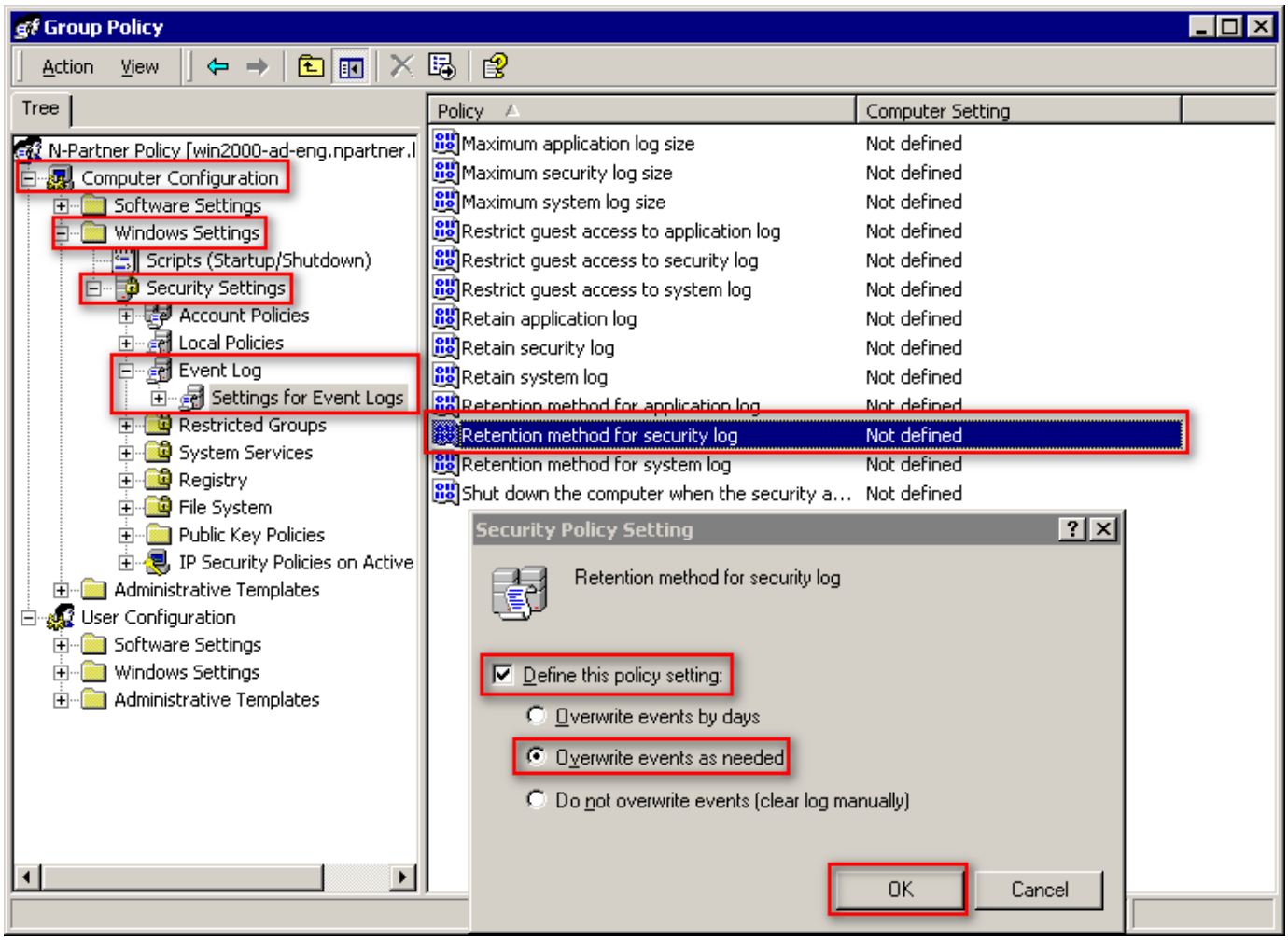
(5) Local Group Policies: Audit Policy

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

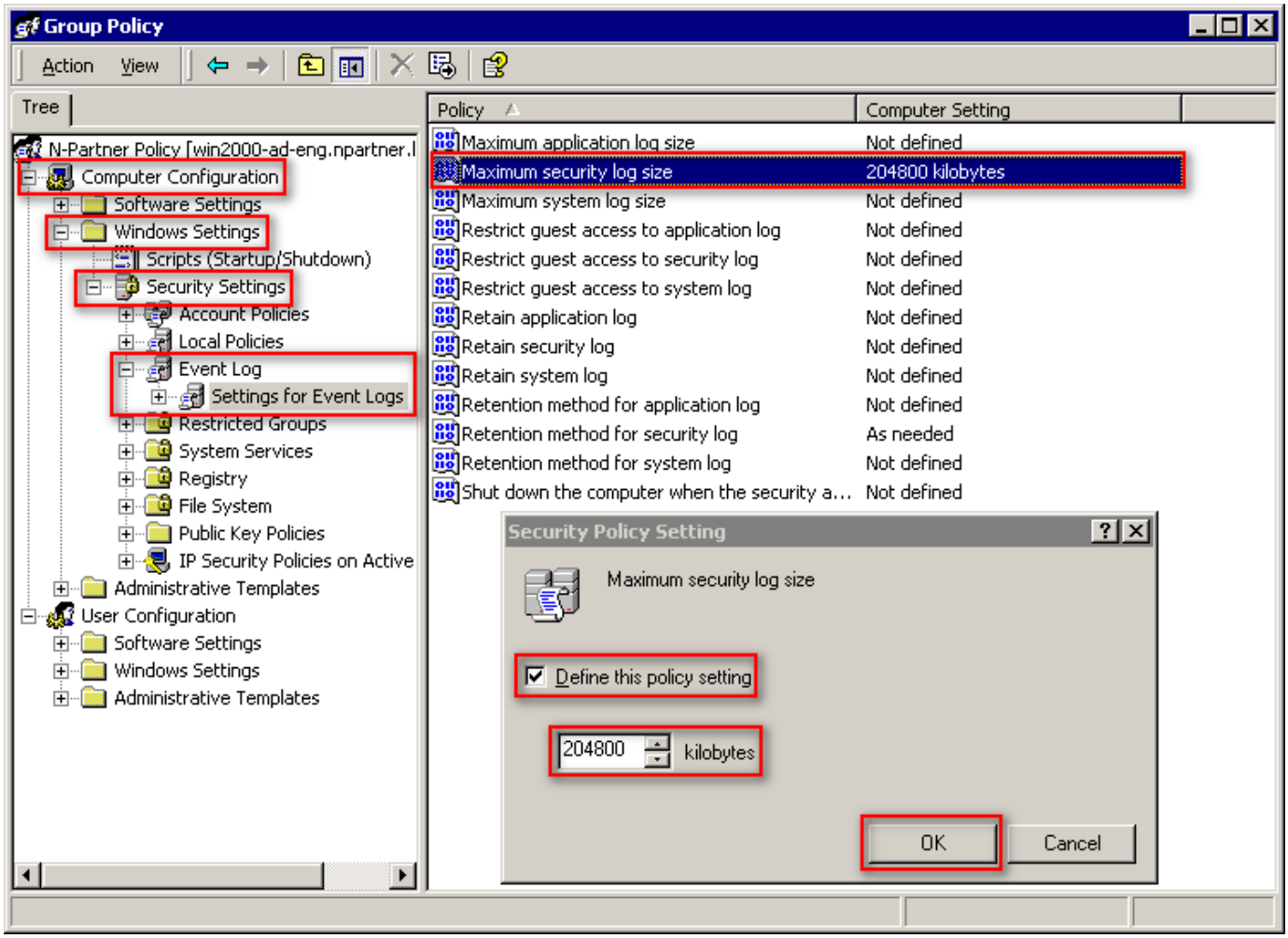
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”



(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

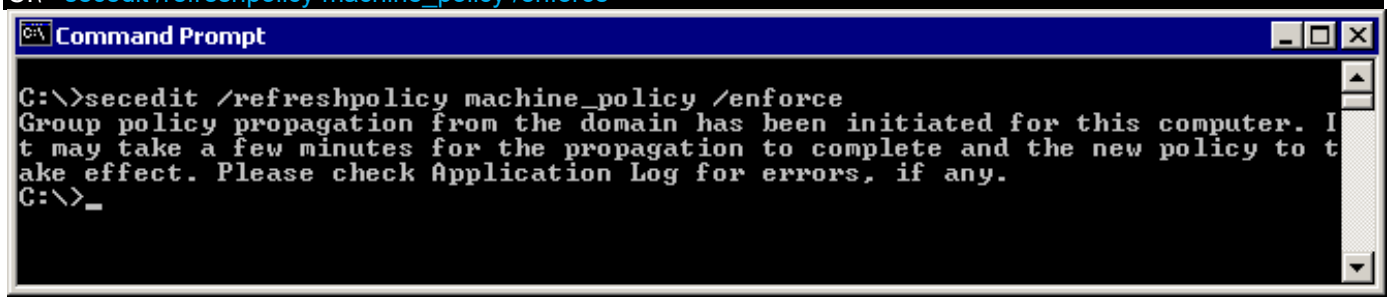
Note: Please adjust the number based on the actual environment. -> Click “OK.”



(8) Open “Command Prompt” on your Windows Server.

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

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



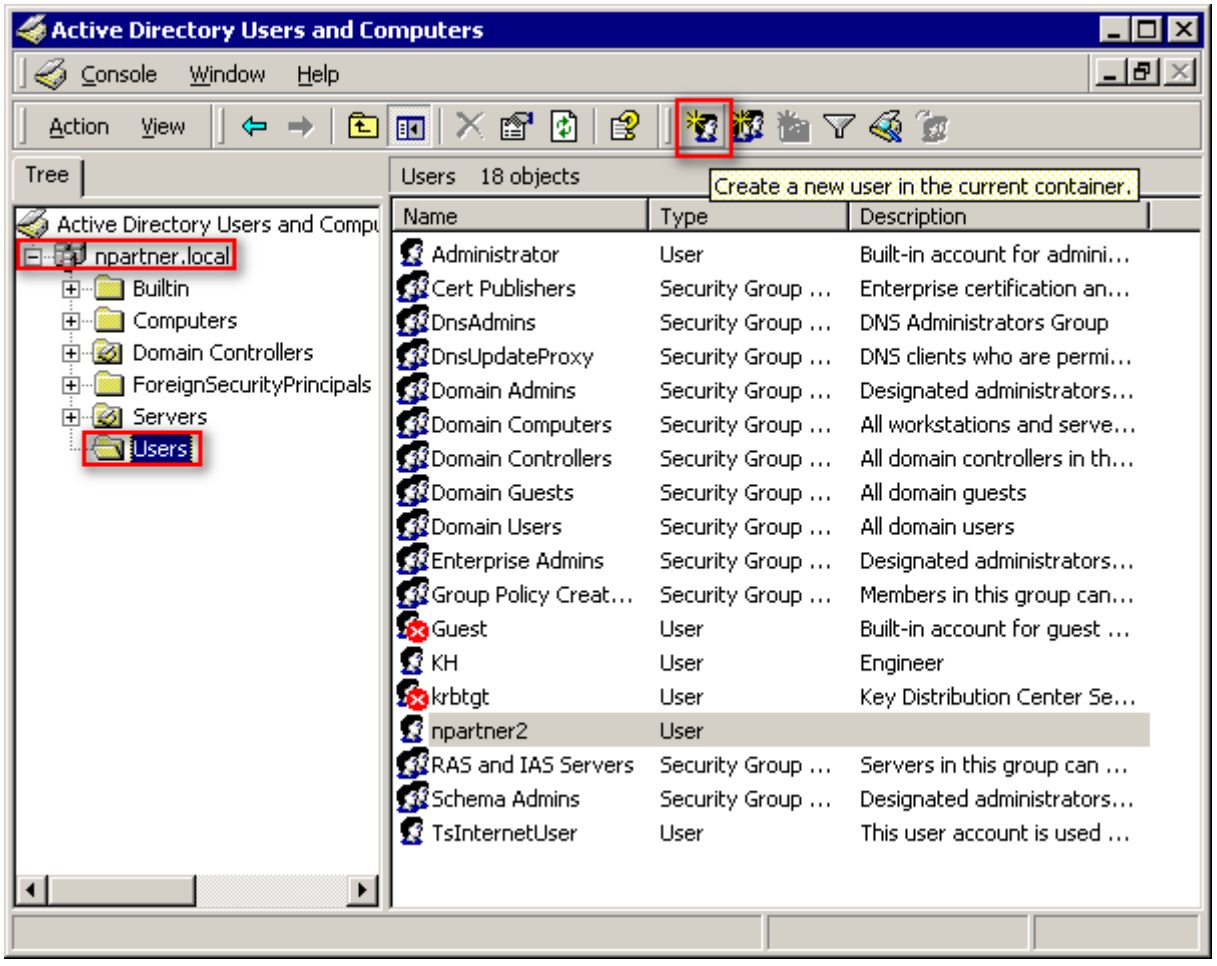
1.3 Add Non-Admin Accounts

1.3.1 Add Users

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

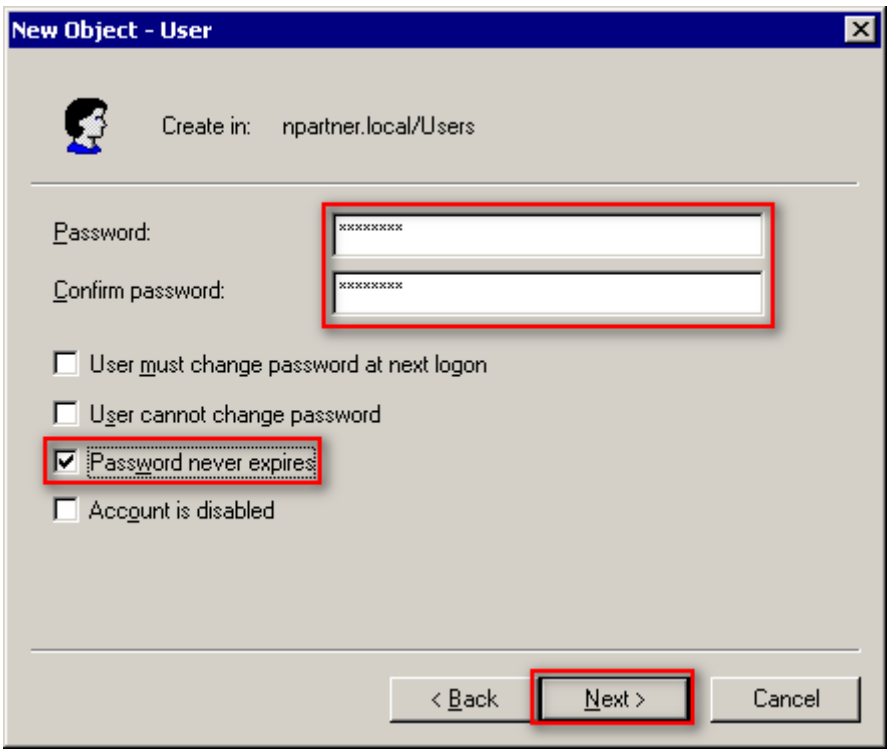
(2) In “Users” organizational unit of your domain name, click  to create a new user.

Note: Select your organizational unit according to the actual environment

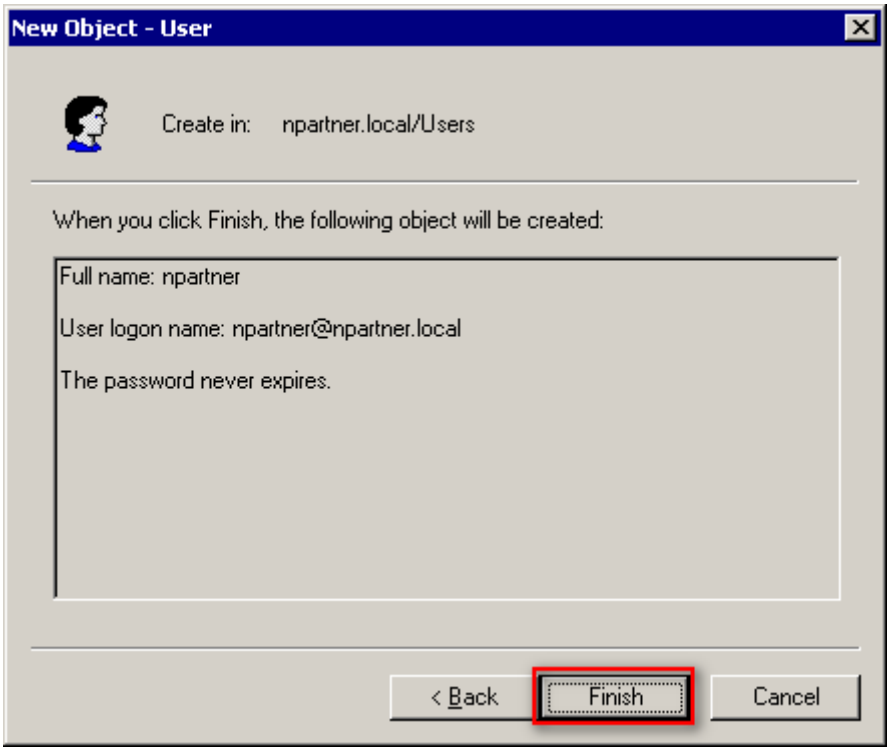


(3) Enter your full name (in this example, it is “npartner”) and user logon name (in this example, it is “npartner”), then click “Next.”

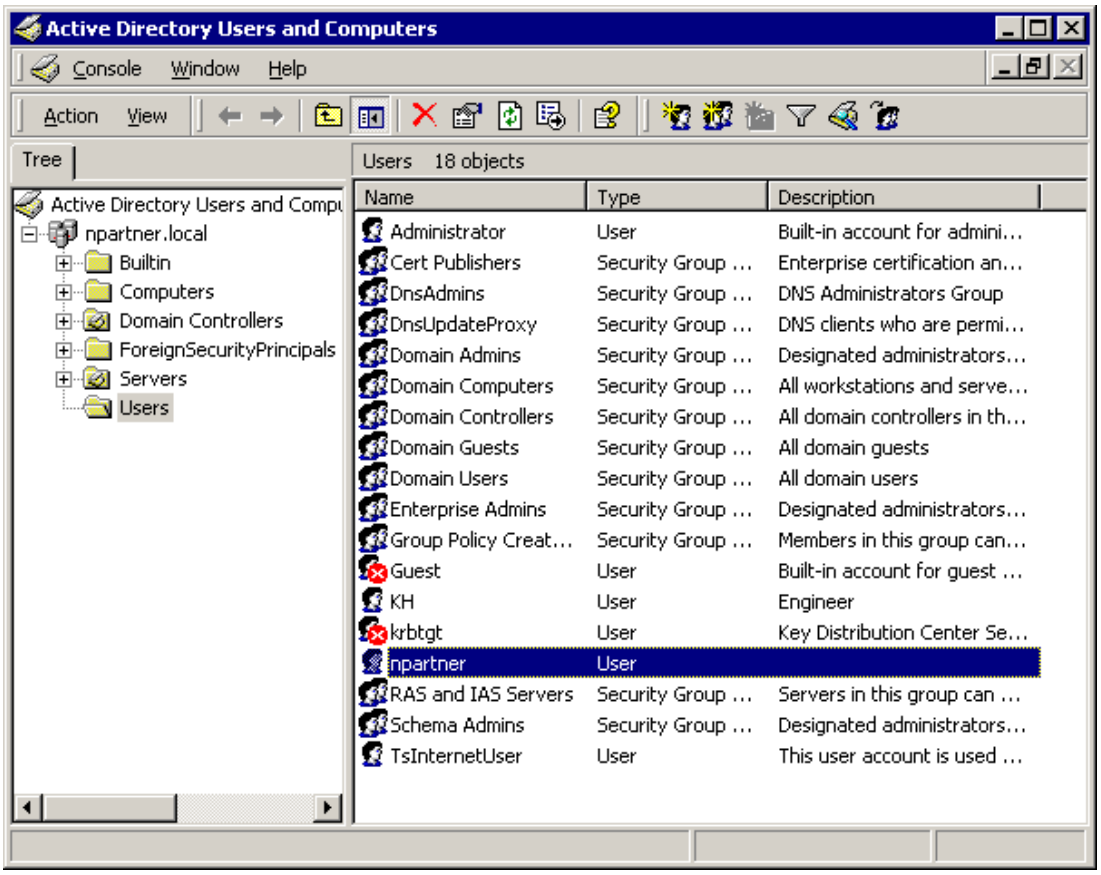
(4) Enter your password and confirm the password, check “Password never expires,” then click “Next.”



(5) Click “Finish.”



(6) Check the account status.

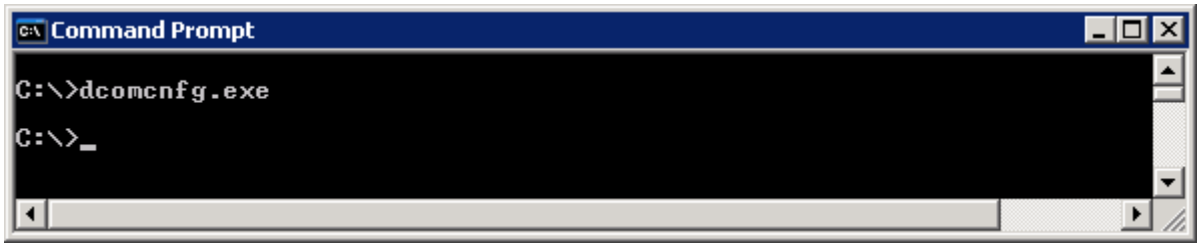


1.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”

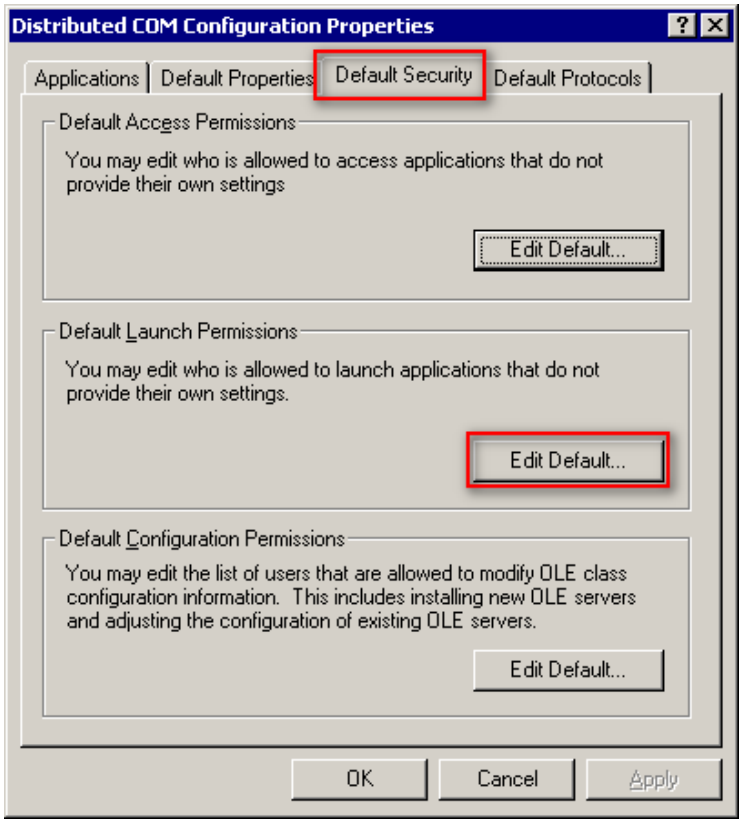
(2) Enter the command below to enable component services.

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



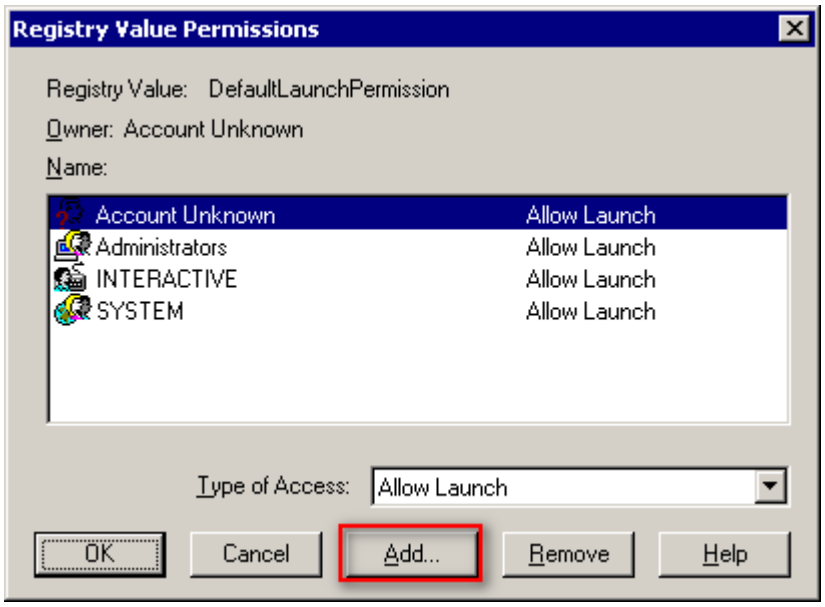
(3) Enable Default Access Permissions

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

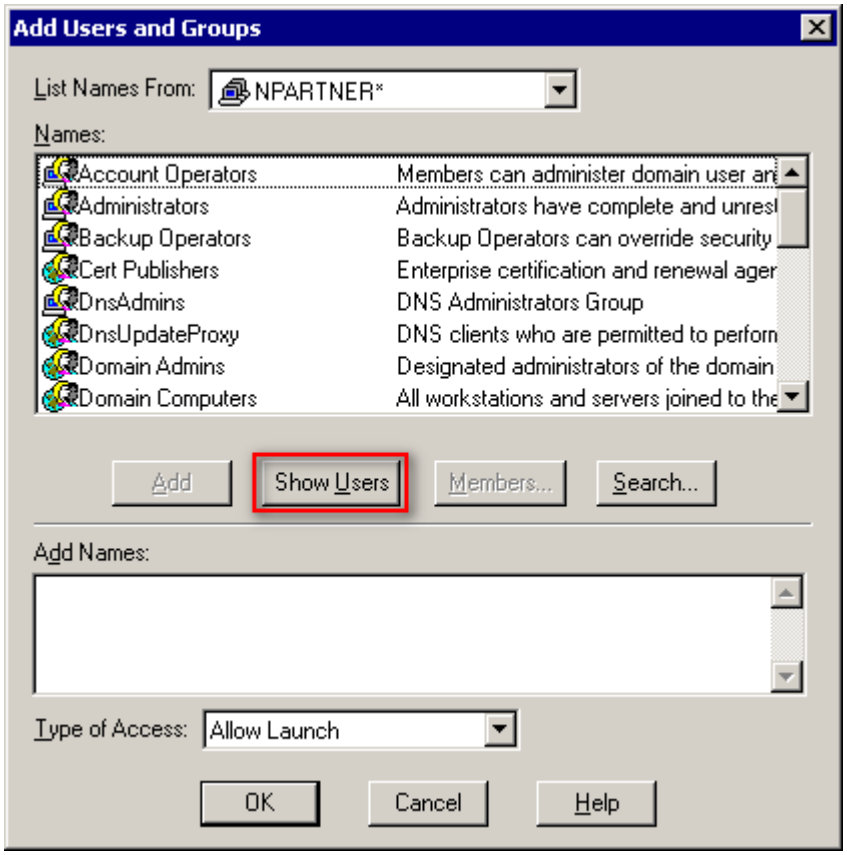


(4) Add User Permissions

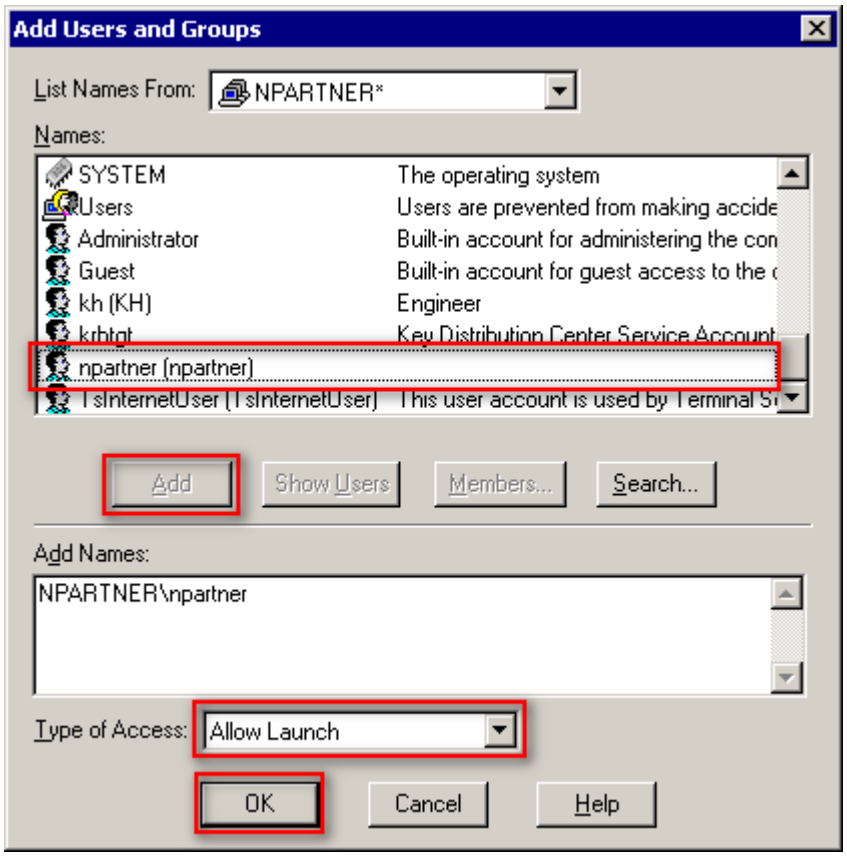
Click “Add...”.



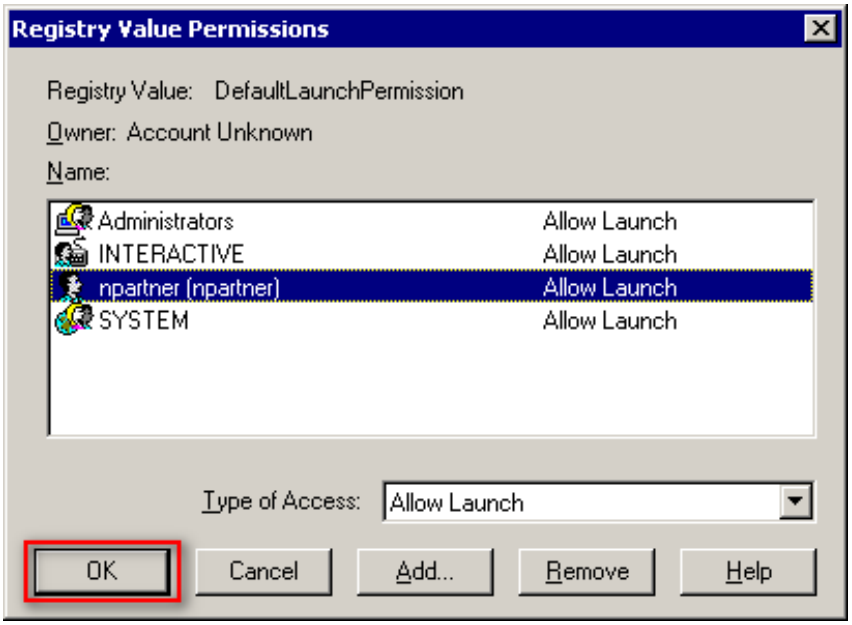
(5) Click “Show Users.”



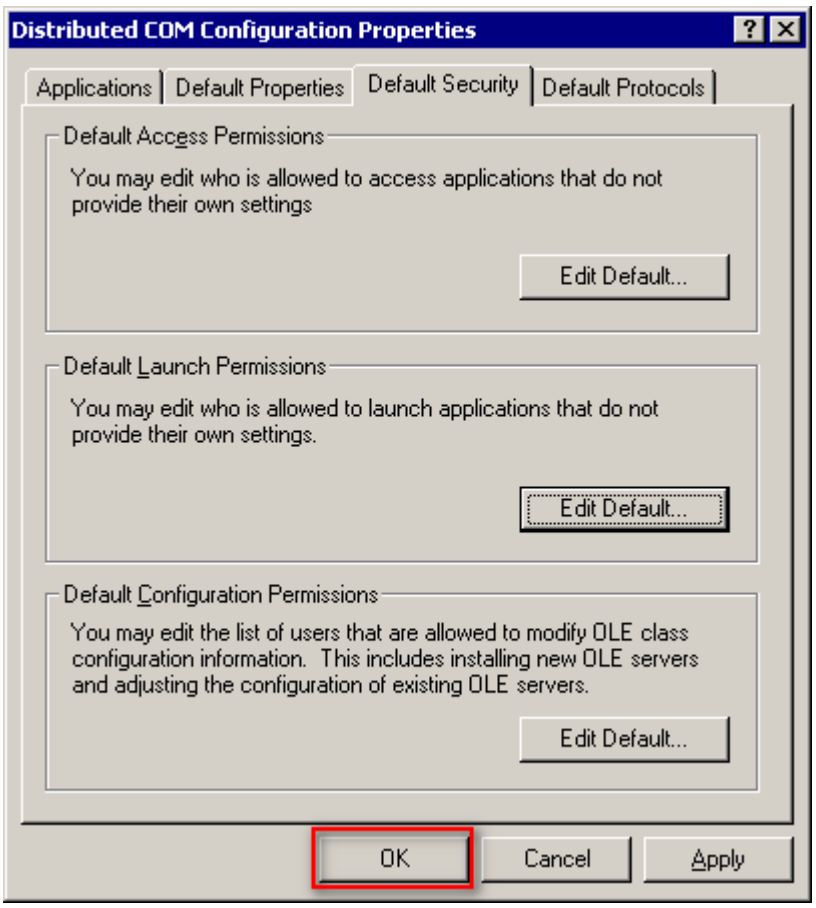
(6) Select your user account (in this example, it is “npartner”), click “Add”, set type of access to “Allow Launch,” then click “OK.”



(7) Click “OK.”



(8) Click "OK.”



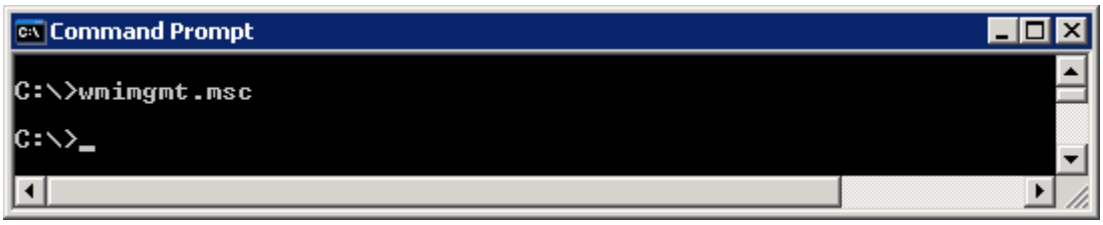
1.3.3 Configure WMI Permissions

1.3.3.1 Configure Event Log Permissions

(1) Open “Command Prompt.”

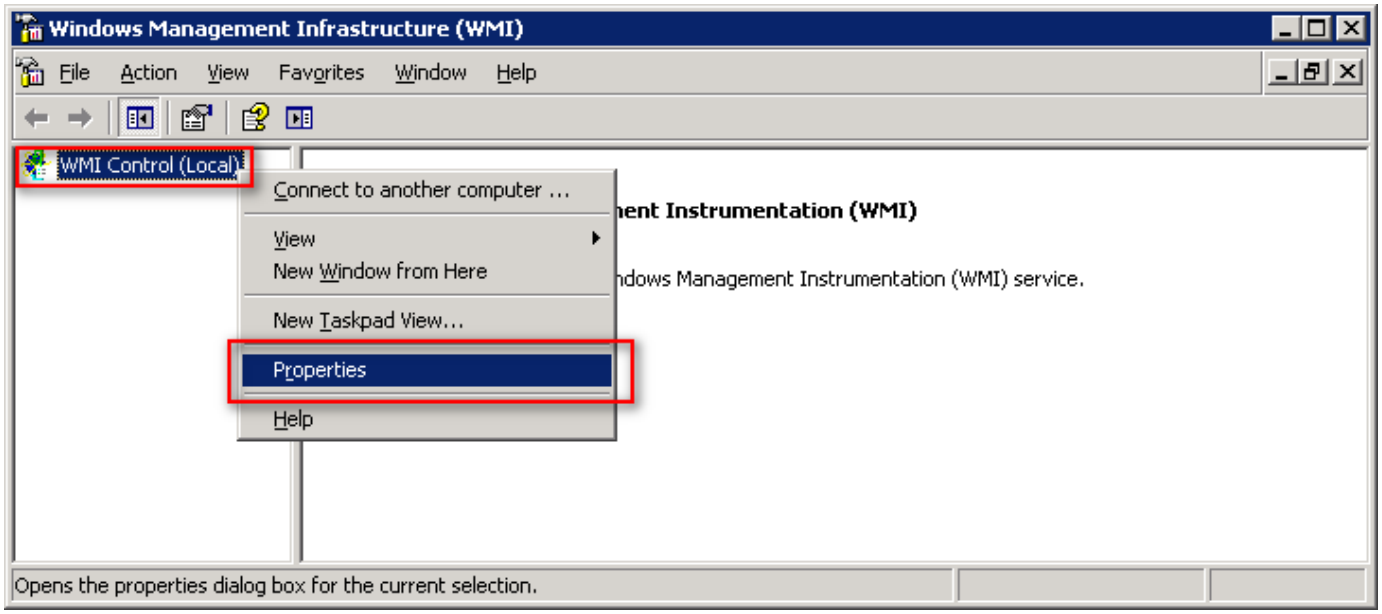
(2) Enter the command to enable WMI control service.

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



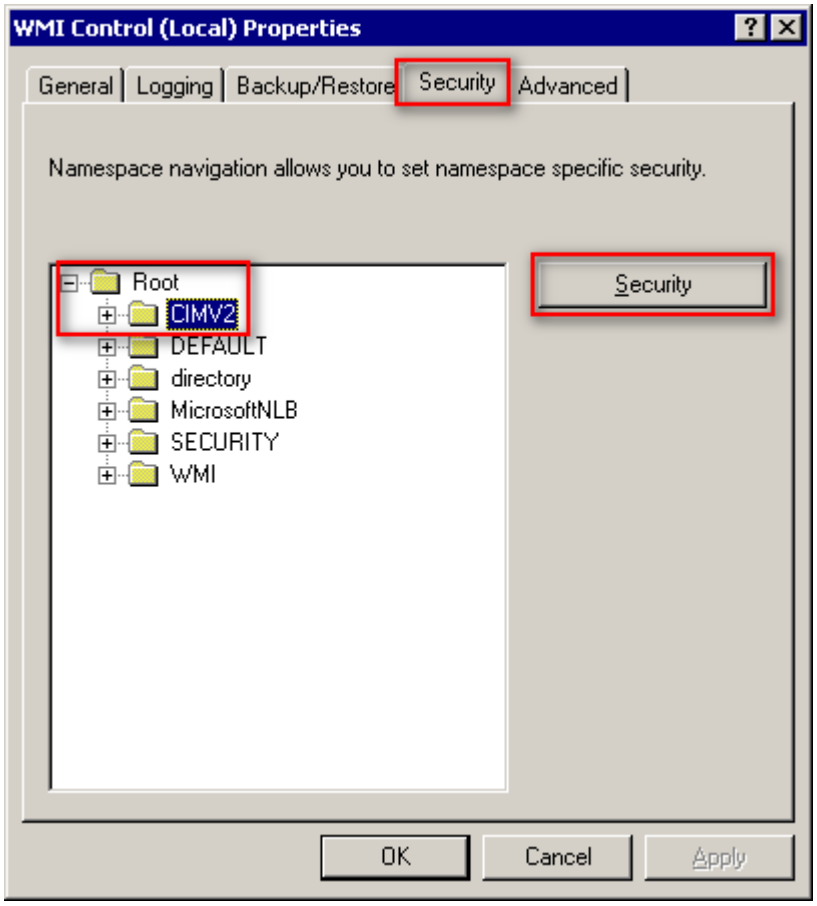
(3) Edit WMI Control

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



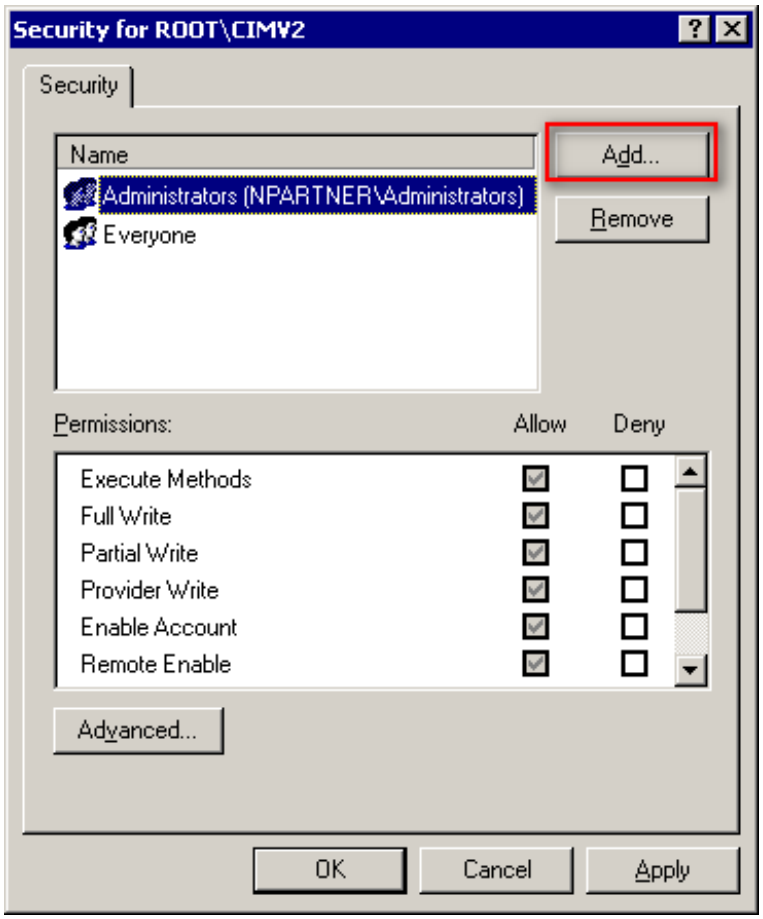
(4) Edit CIMV2 Security

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



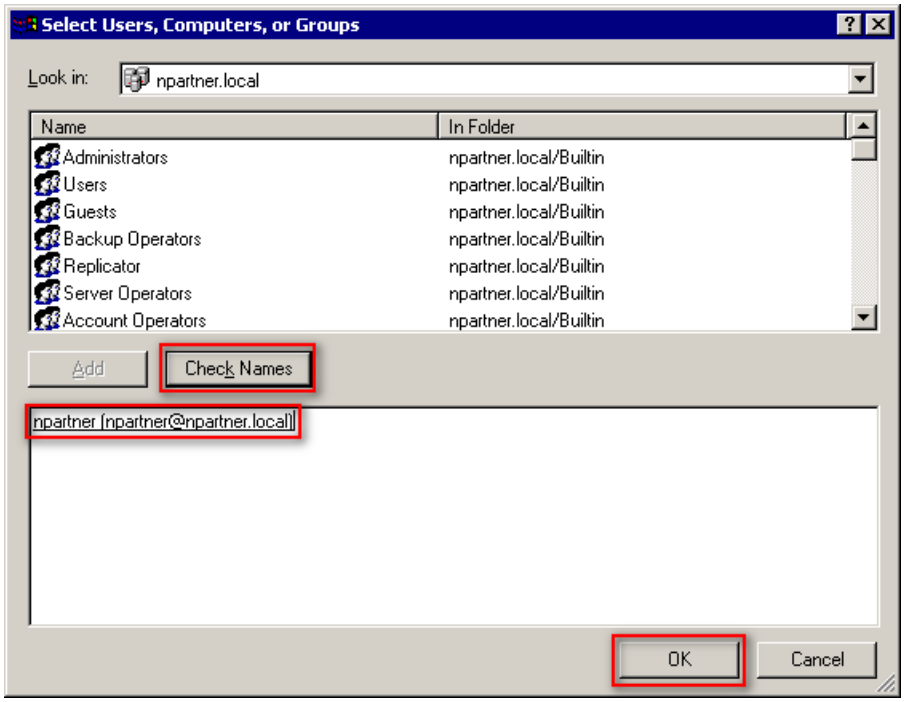
(5) Add WMI User Permissions.

Click “Add.”



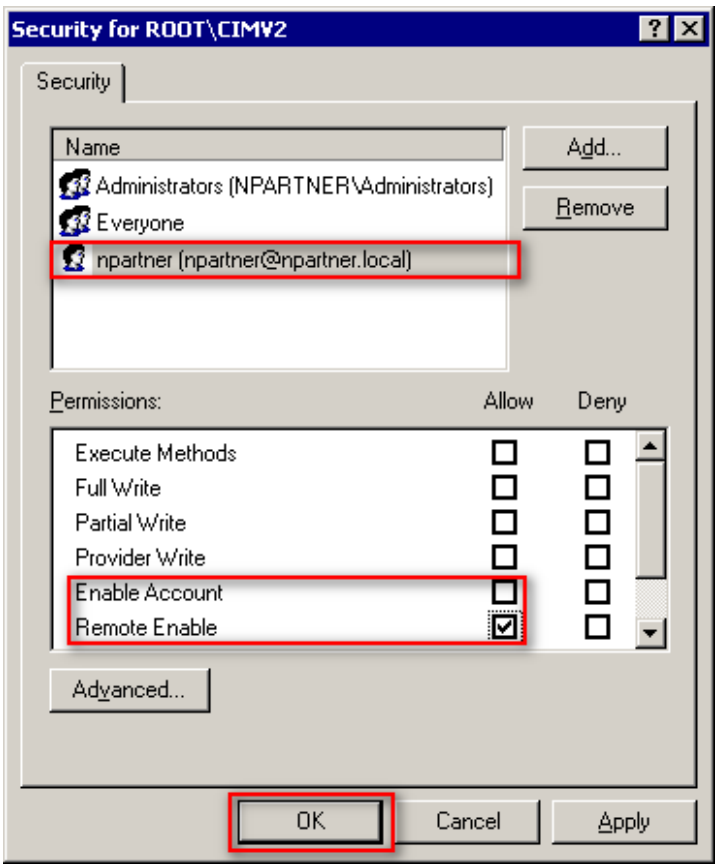
(6) Enter Your Username

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

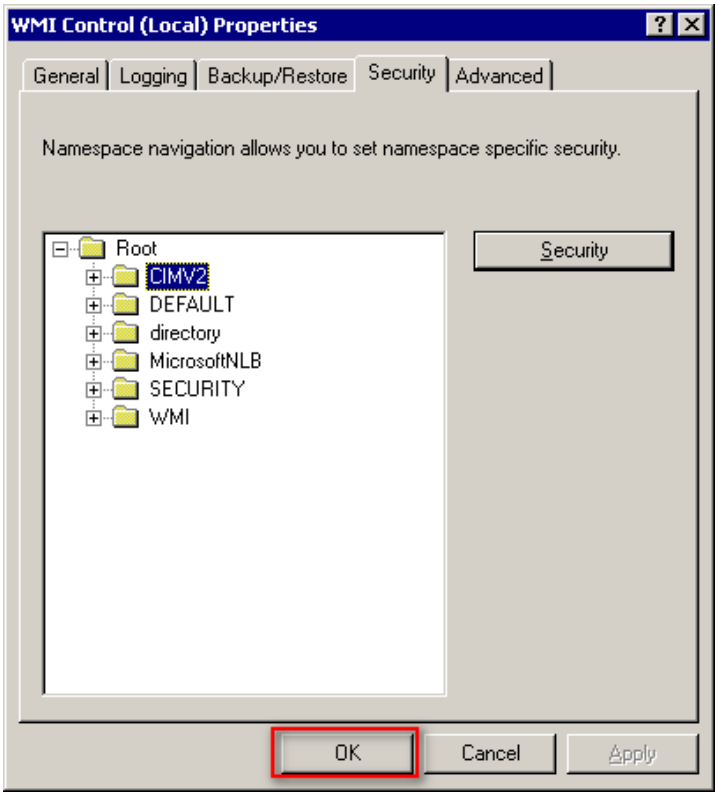


(7) Set Your User Permissions

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



(8) Click “OK.”



1.3.3.2 Configure Permissions for Reading User Data

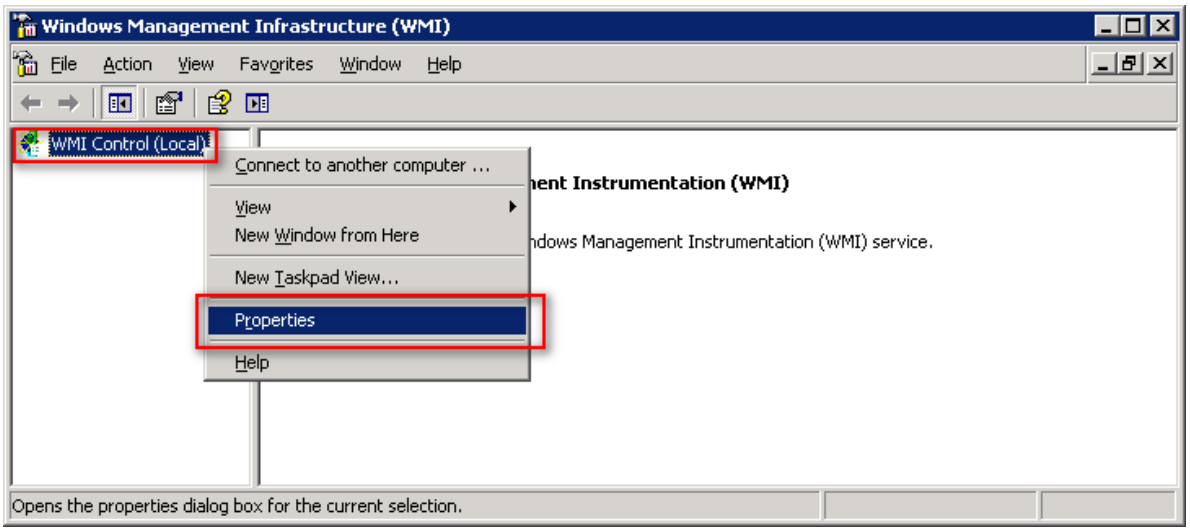
(1) Open “Command Prompt.”

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

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

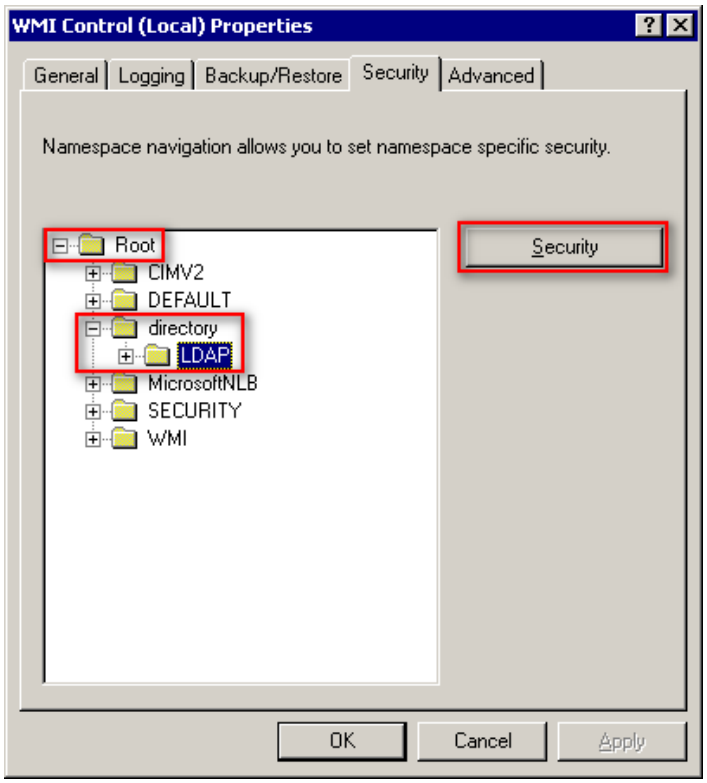
(3) Edit WMI Control

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



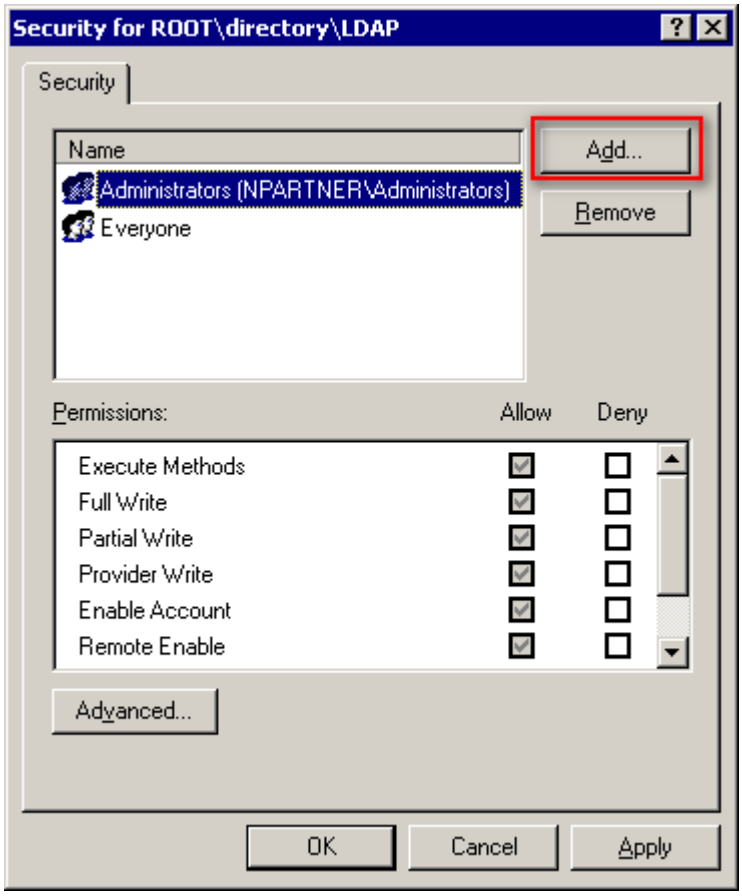
(4) Edit LDAP Security

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



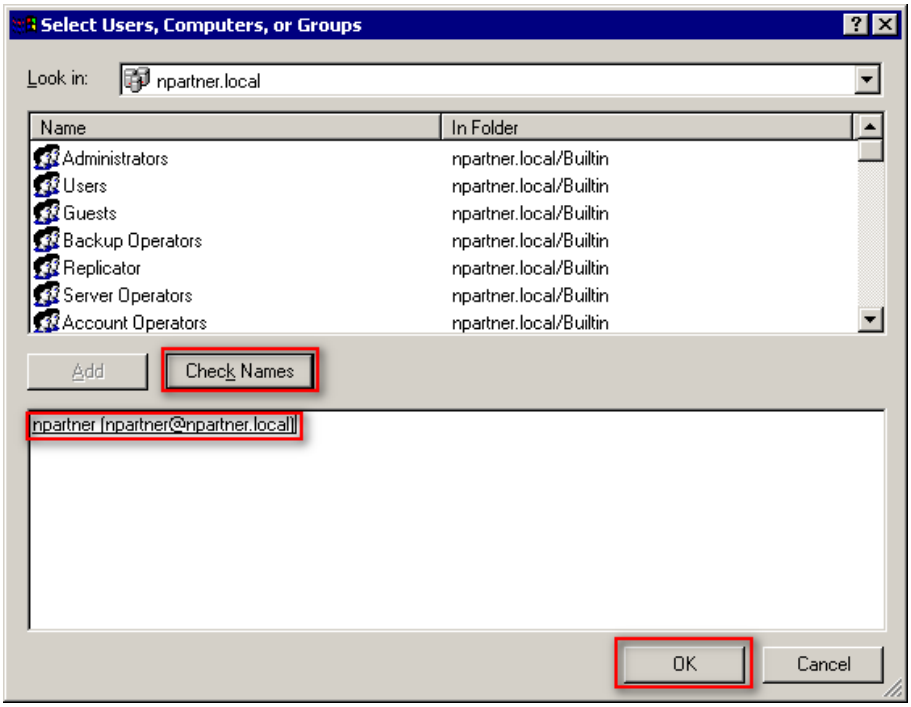
(5) Add WMI User Permissions

Click “Add.”



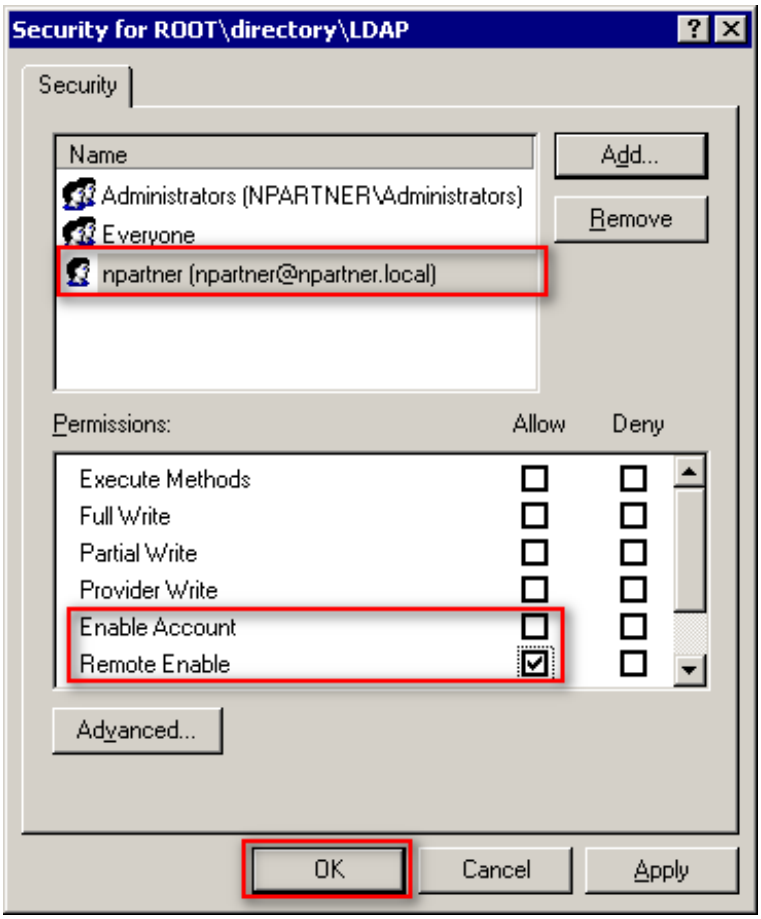
(6) Enter Your Username

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

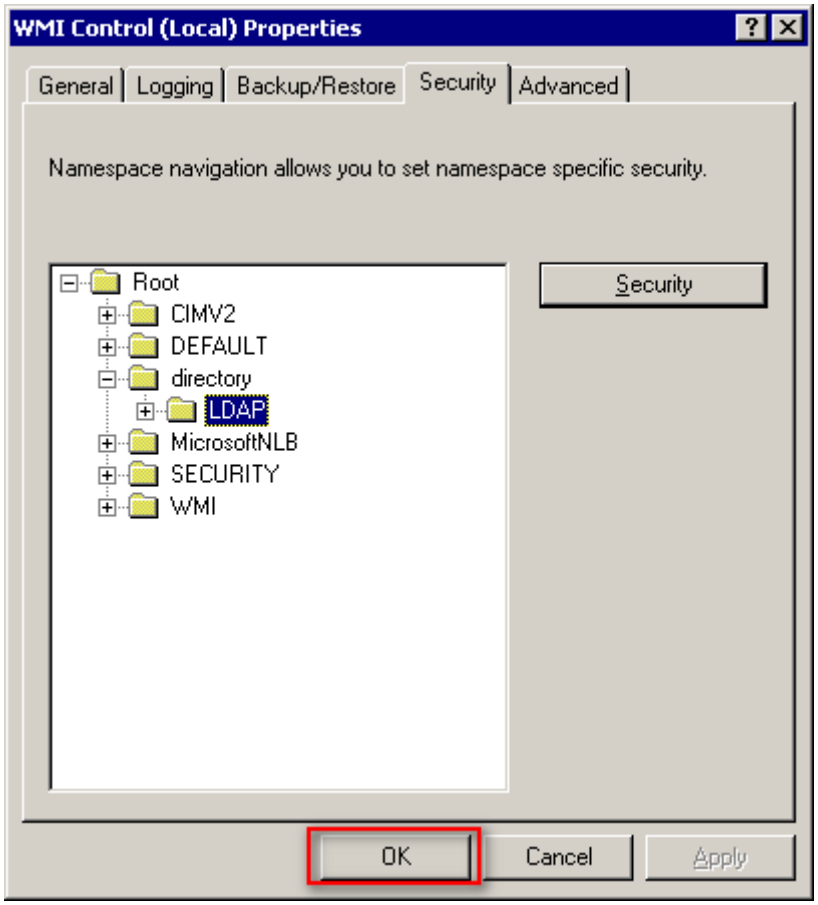


(7) Set Your User Permissions

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



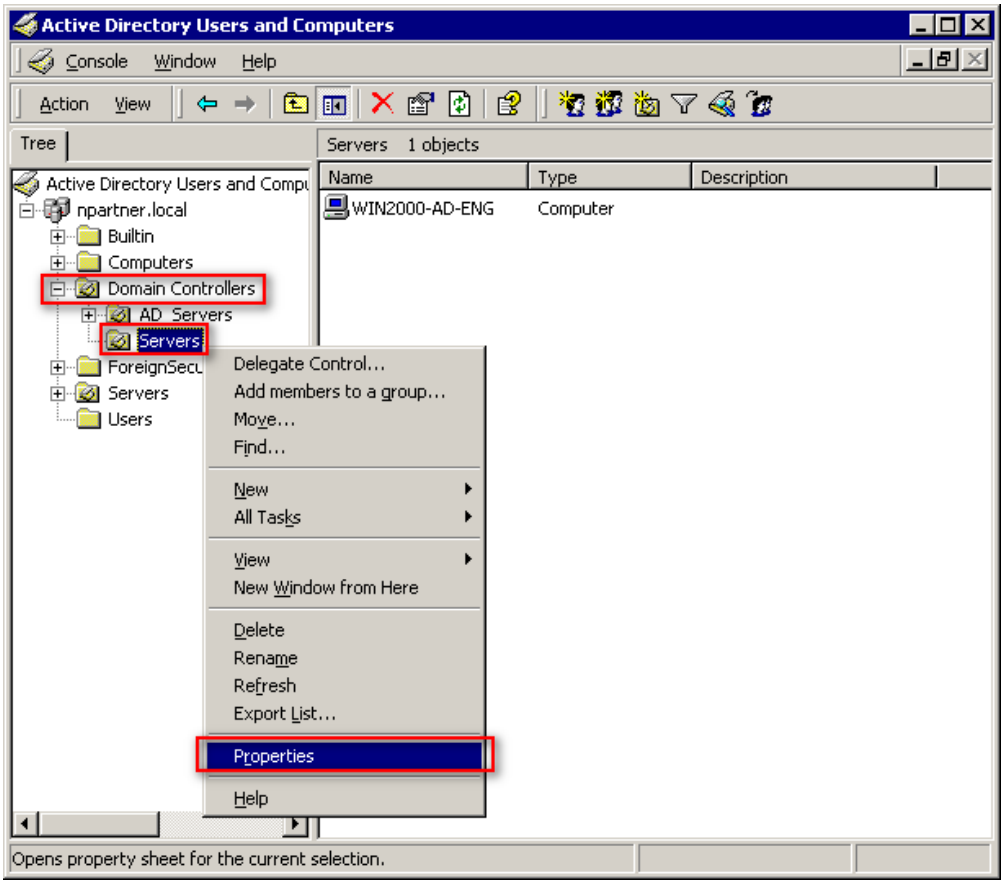
(8) Click “OK.”



1.3.4 Configure Event Log Read Permissions

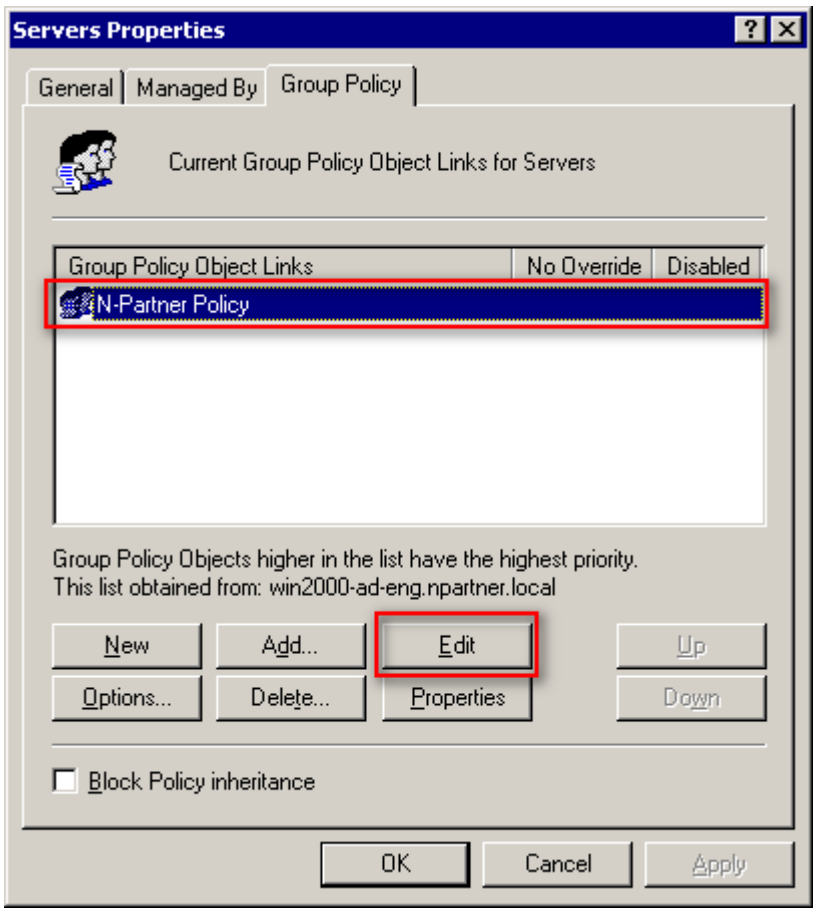
(1) Click “Active Directory Users and Computers.”

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



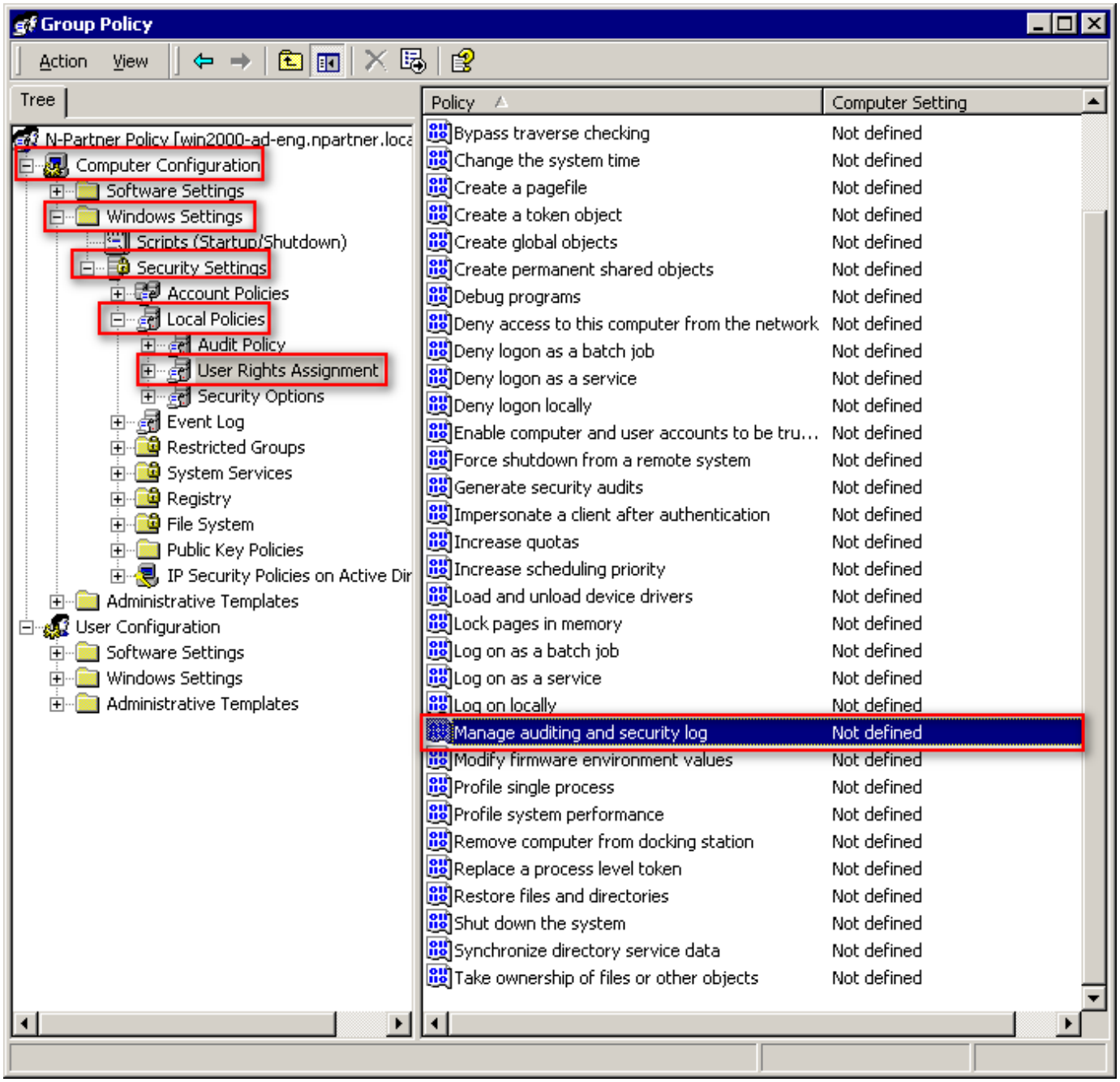
(3) Edit Group Policy Object

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.”

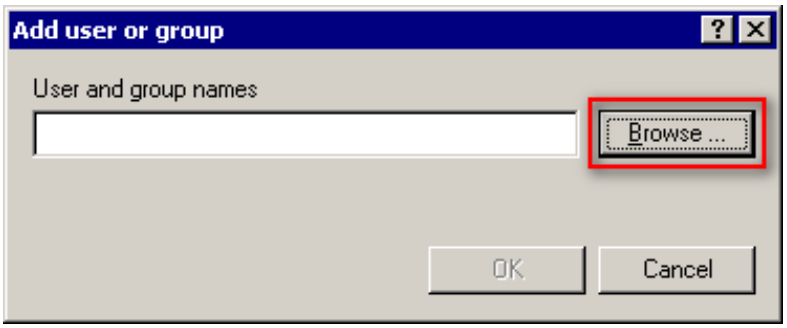


(5) Add Auditing User

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

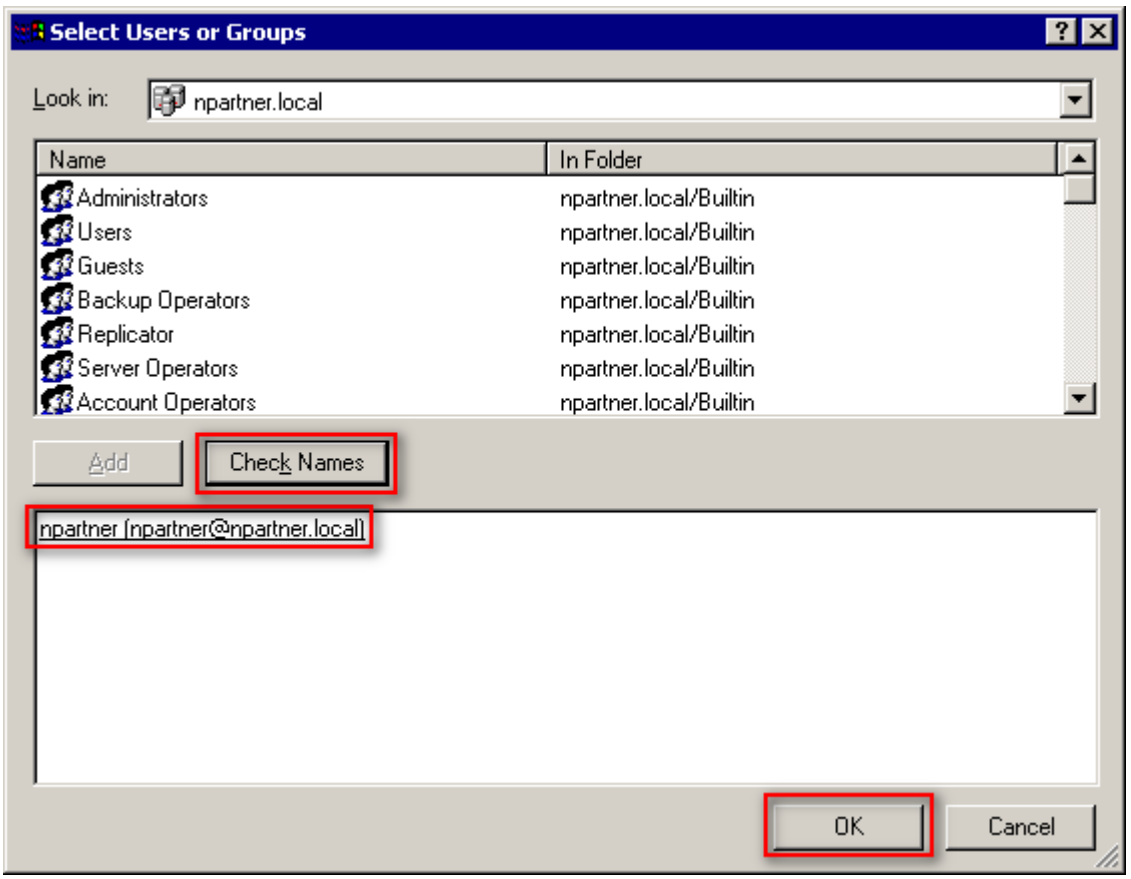
(6) Search for User

Click “Browse.”

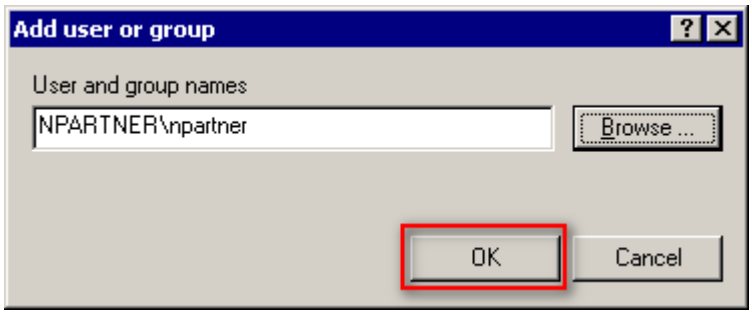


(7) Enter Your User Account

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



(8) Click “OK.”



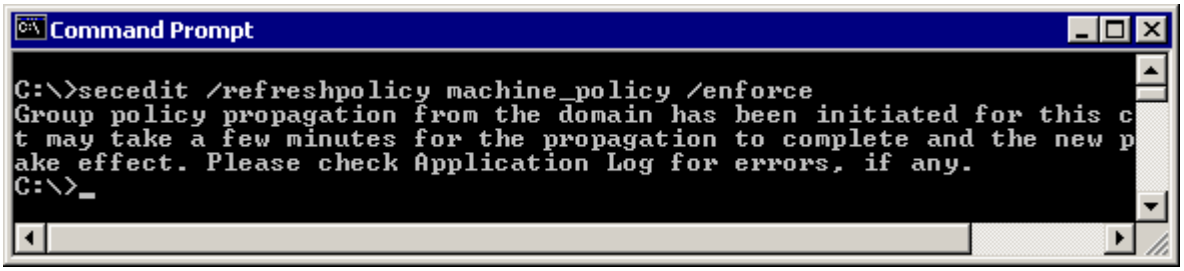
(9) Confirm Audit Log Settings

Click “OK.”

(10) Open “Command Prompt.”

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

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

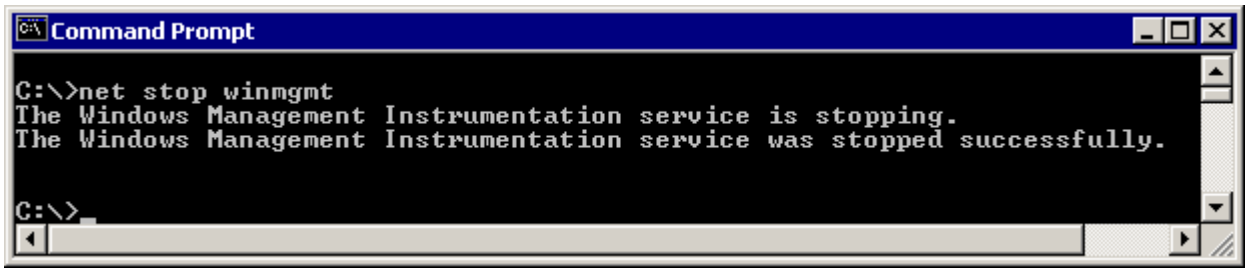


1.3.5 Restart the WMI Service

(1) Open “Command Prompt.”

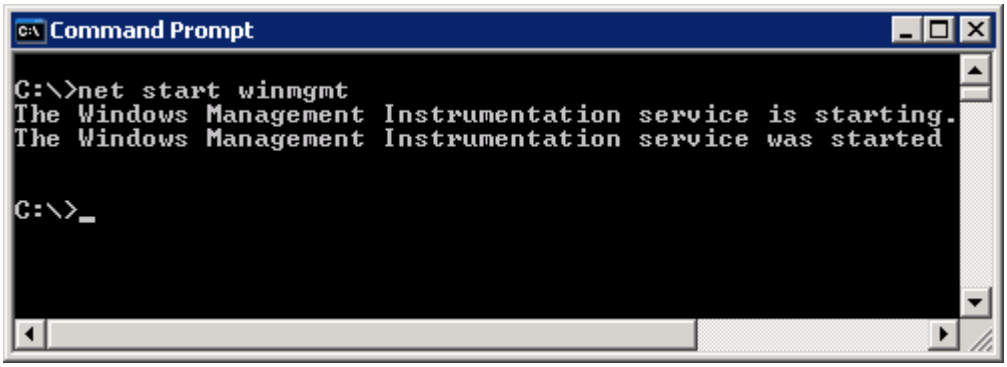
(2) Enter the command below to disable the WMI service.

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



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

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



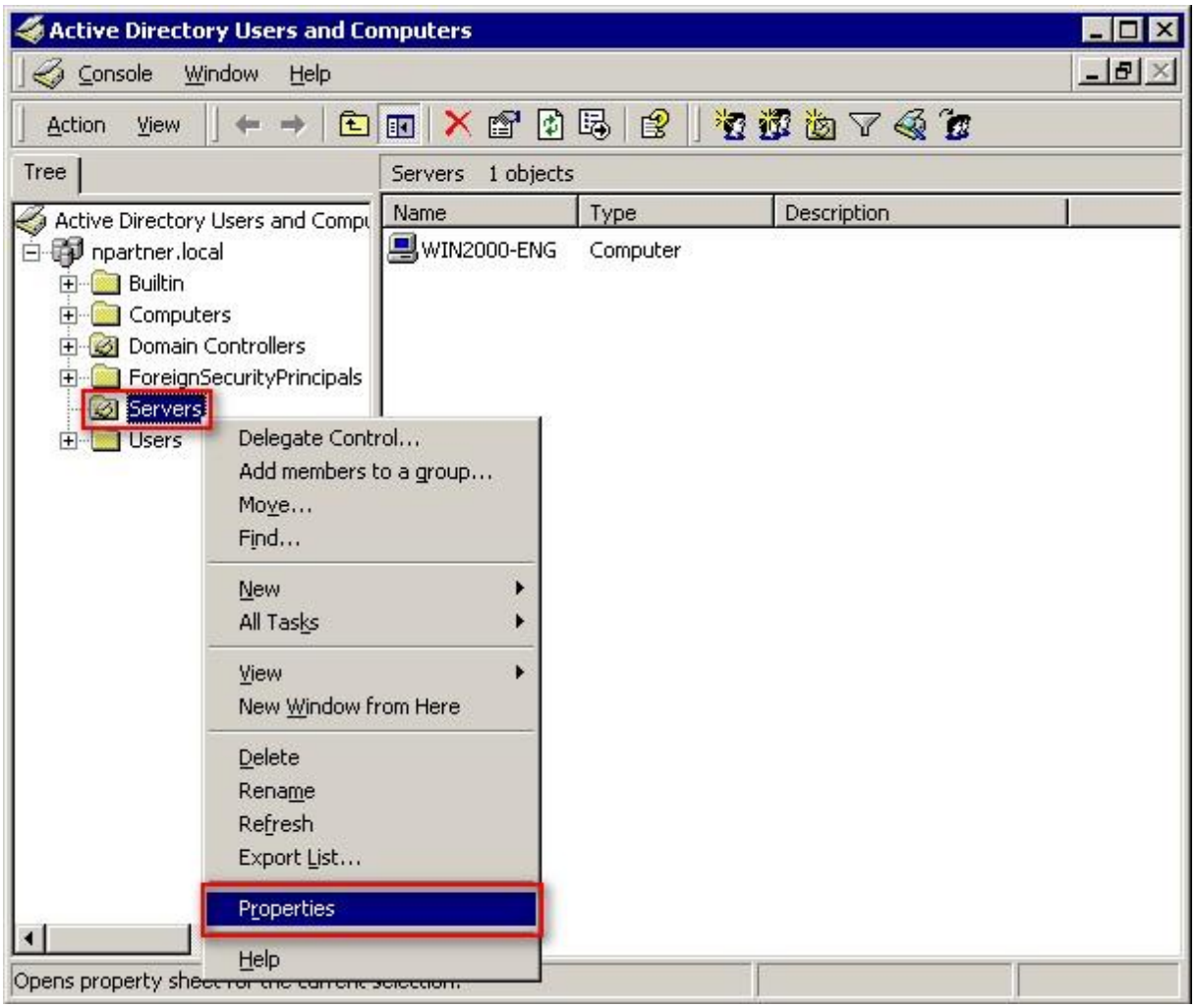
2. Windows 2003

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."

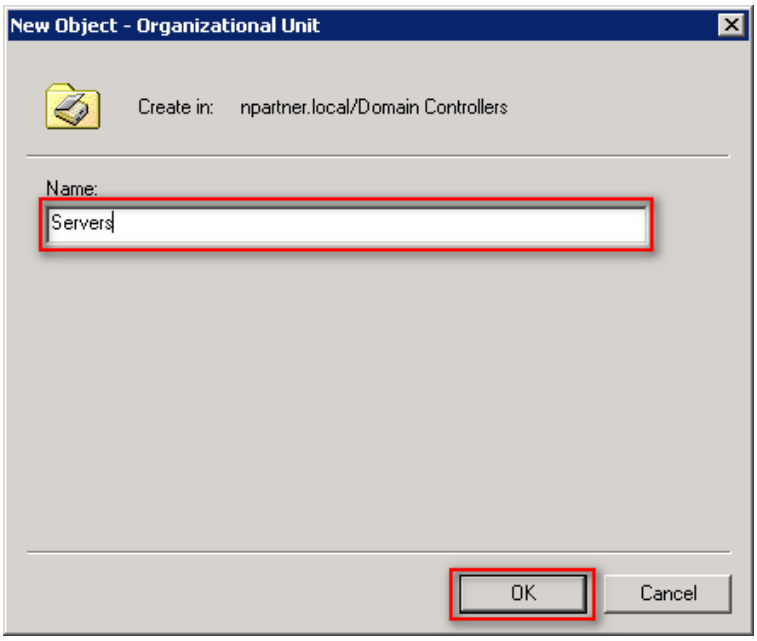
(2) Select your organizational unit (the example here is "Servers") and right-click on "Properties."



(3) Name Your Group Policy Object

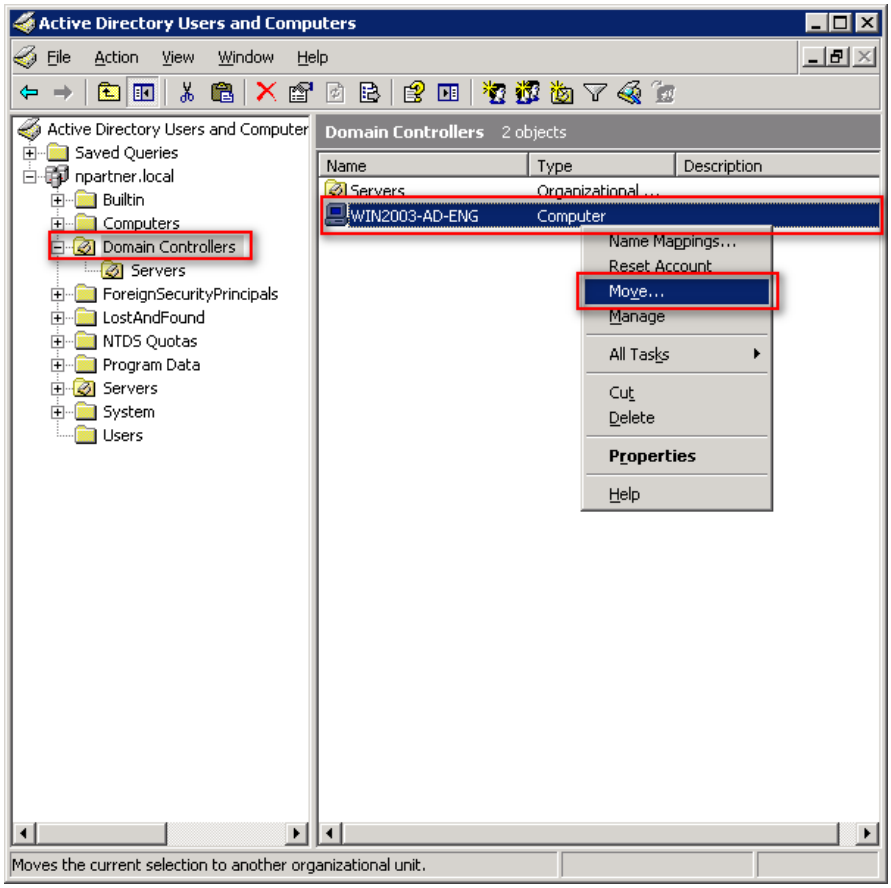
Enter your group policy object name (the example here is “N-Partner Policy”)

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



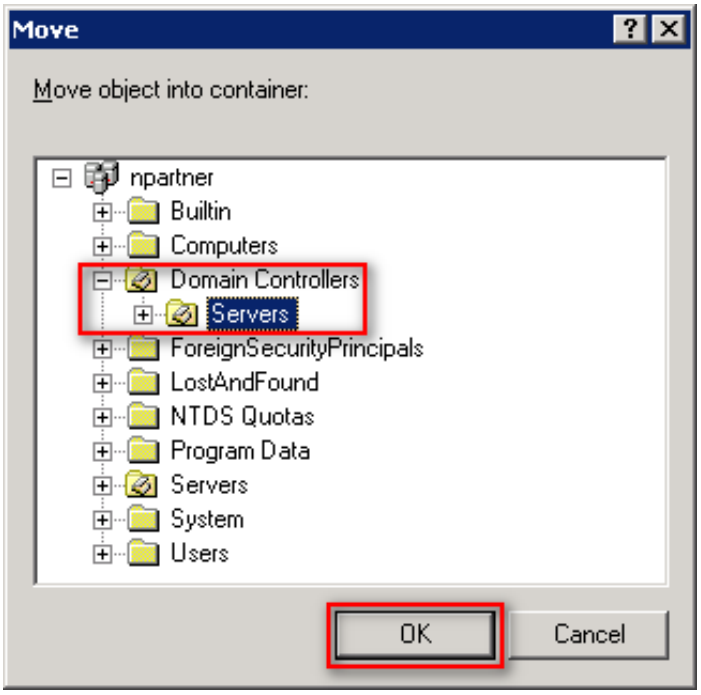
(4) Move Server to your New Organizational Unit

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.”



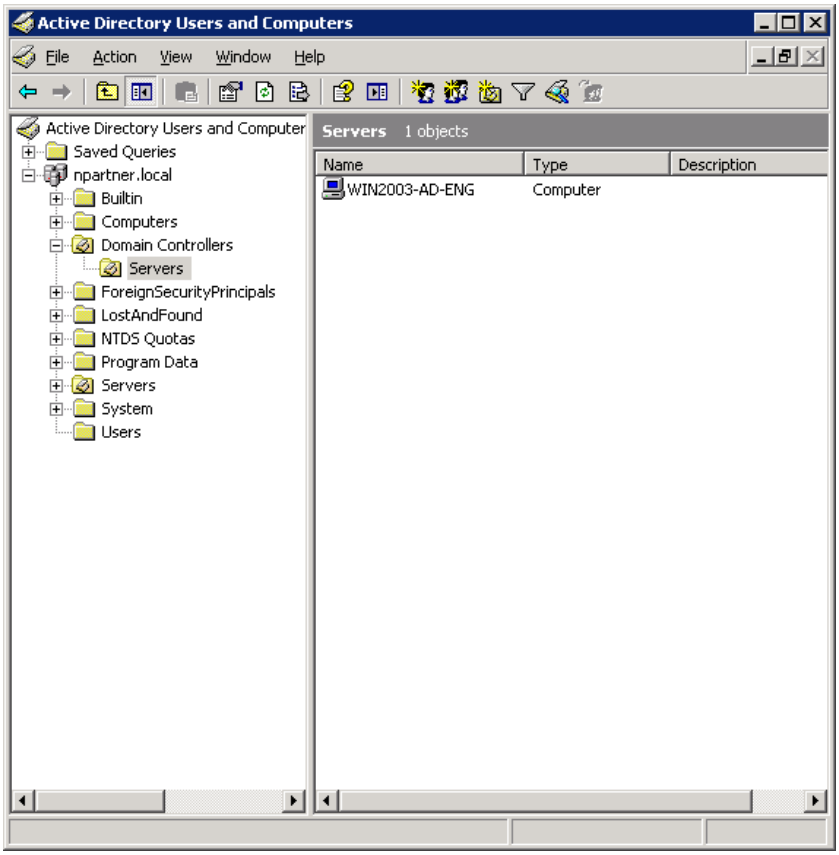
(5) Select Organizational Unit

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



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

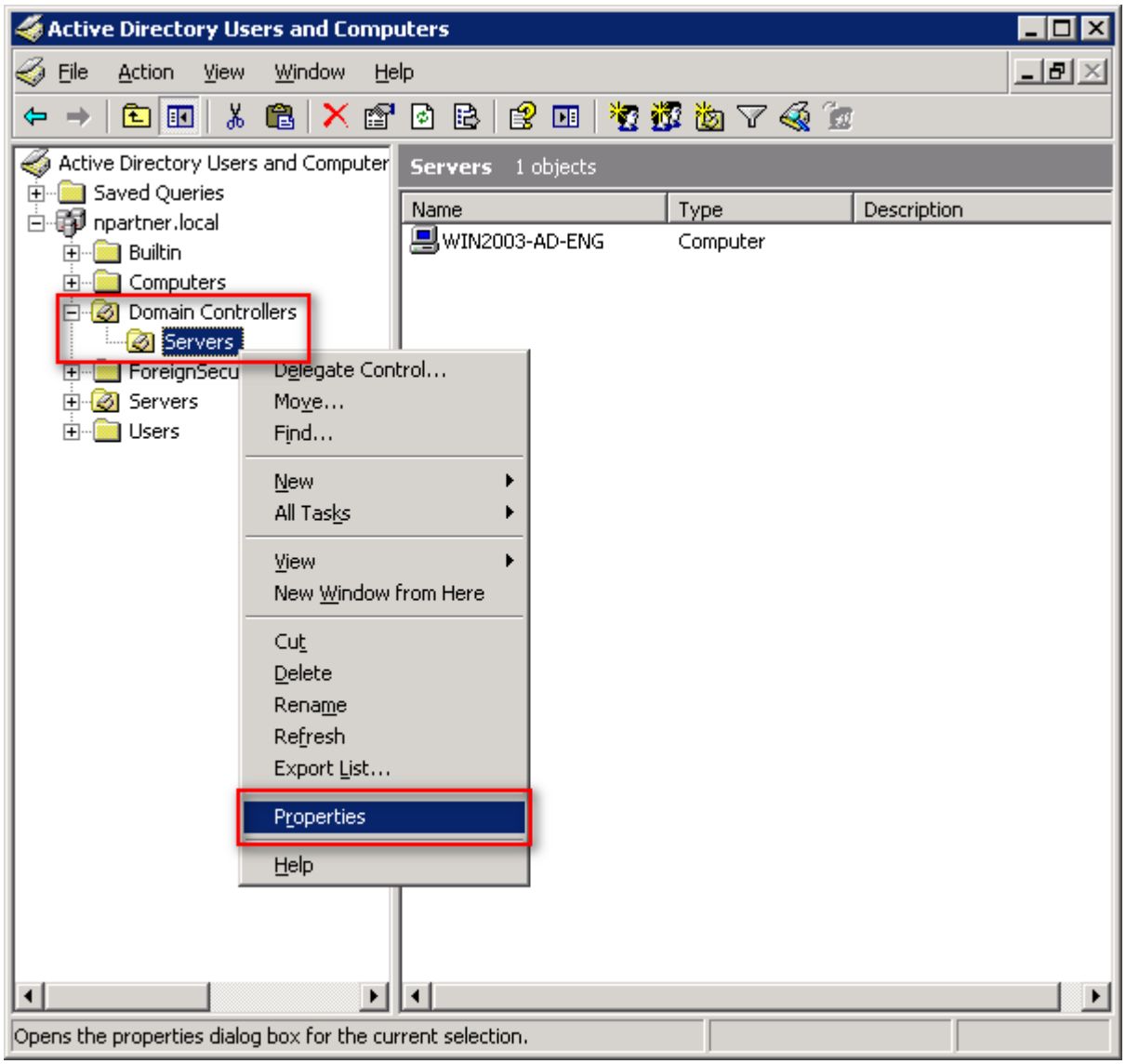
Expand the “Servers” organizational unit under “Domain Controllers” and verify that the “WIN2003-AD-ENG” server has been moved.



2.2 Group Policy Settings

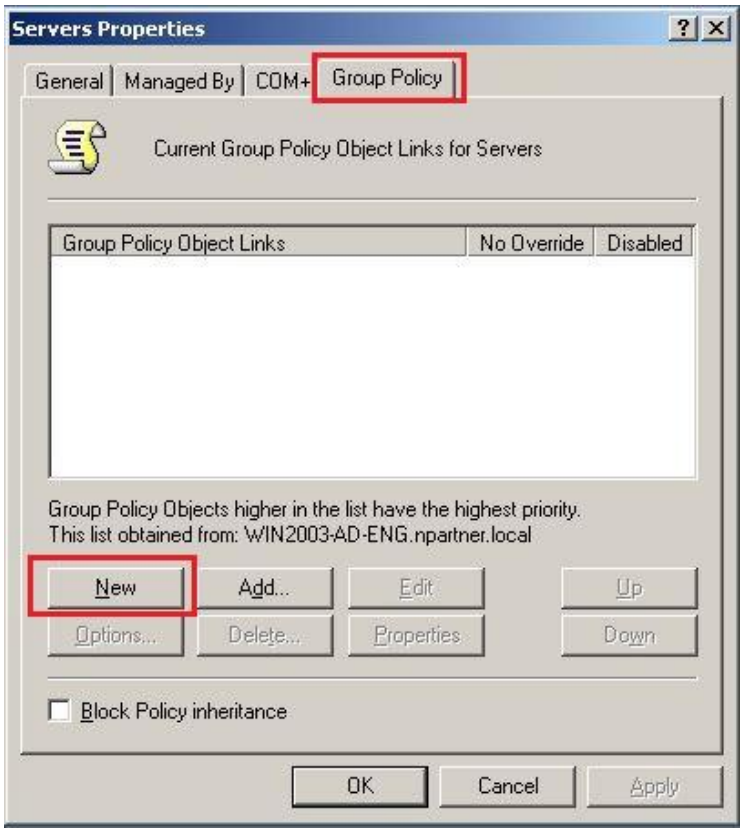
(1) Open “Active Directory Users and Computers.”

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



(3) Enter your Group Policy Object Name

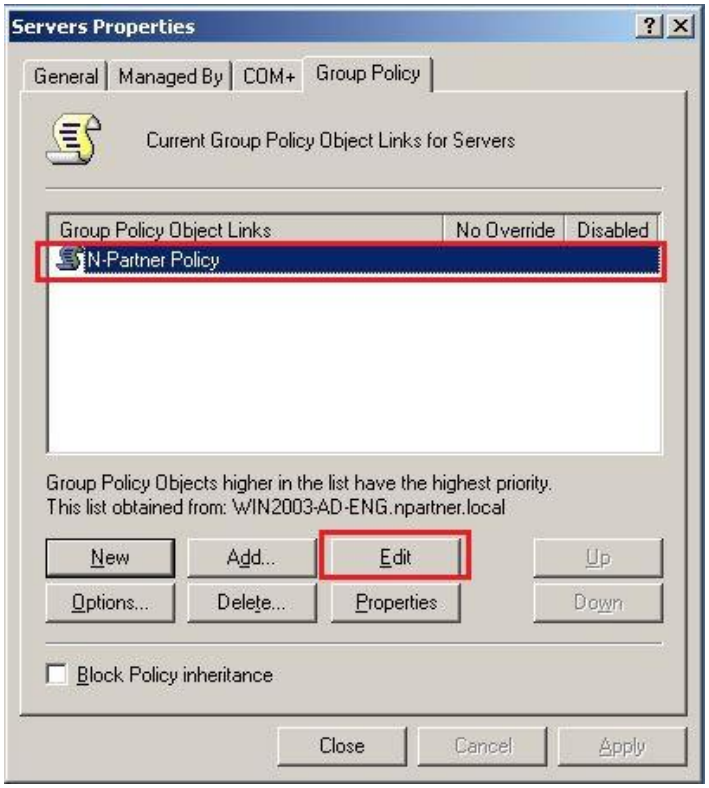
Go to the “Group Policy” tab and click “New.”



(4) Edit your Group Policy Object

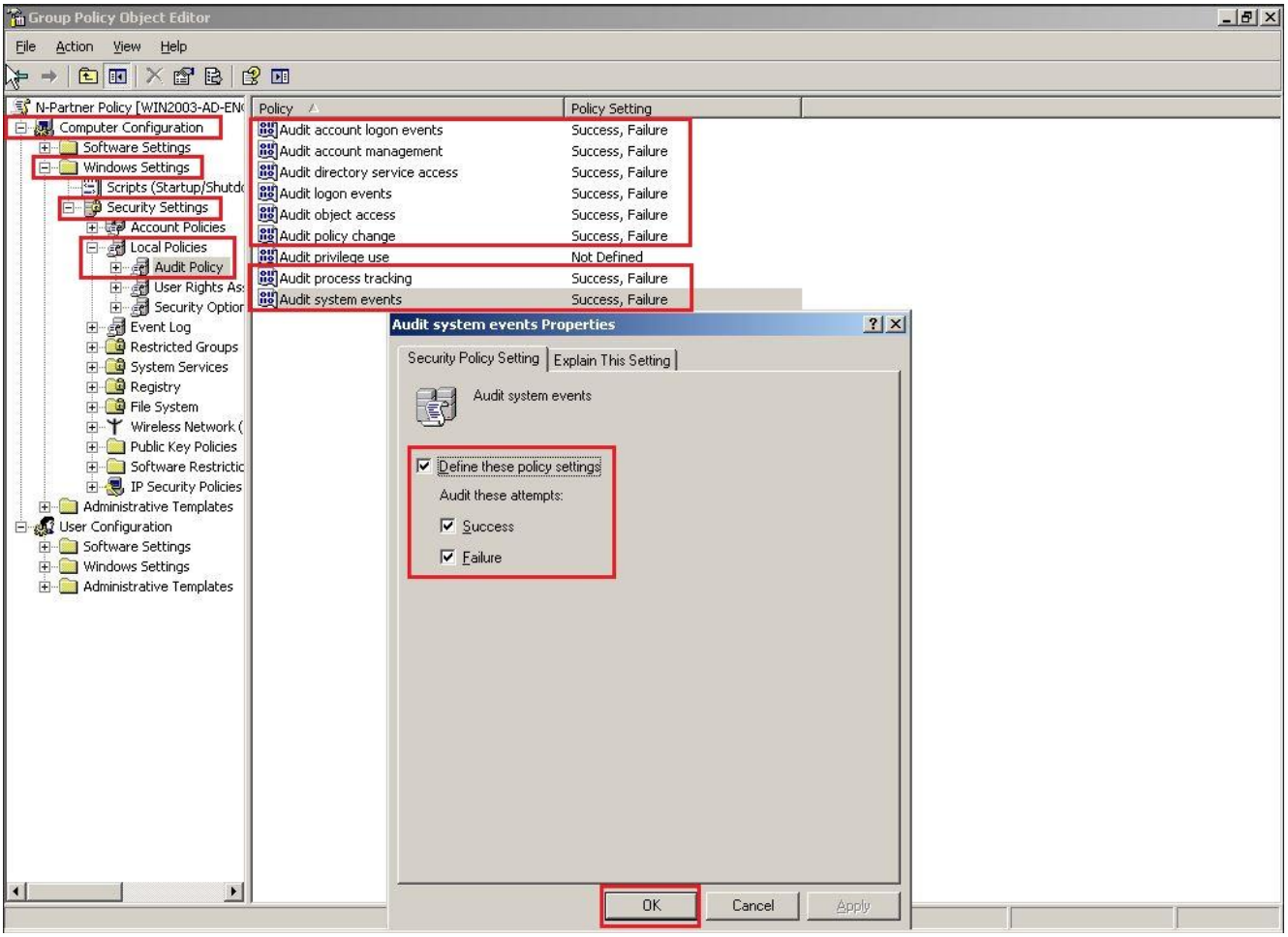
Enter the Group Policy Object name as “N-Partner Policy”

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



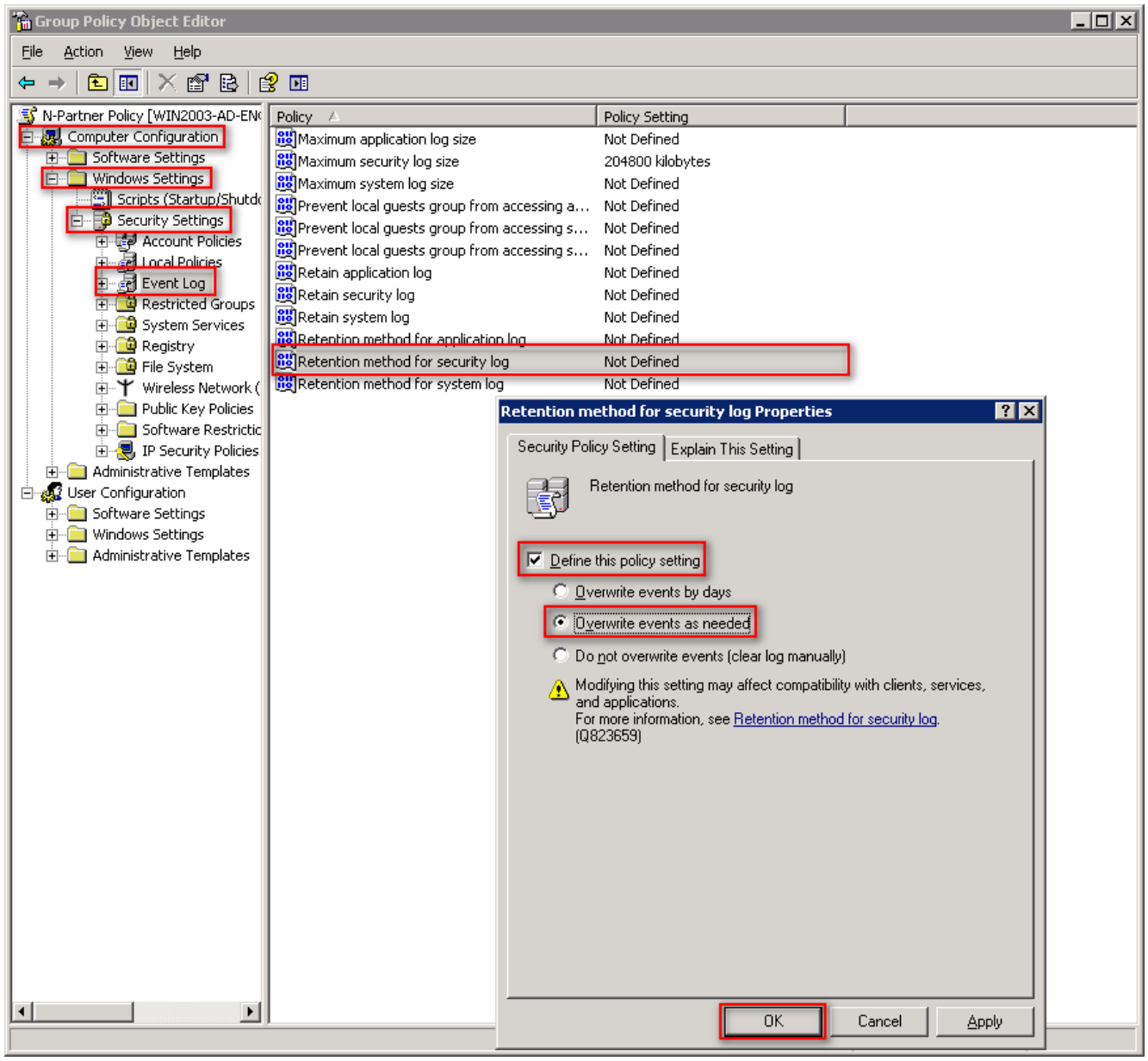
(5) Local Group Policies: Audit Policy

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

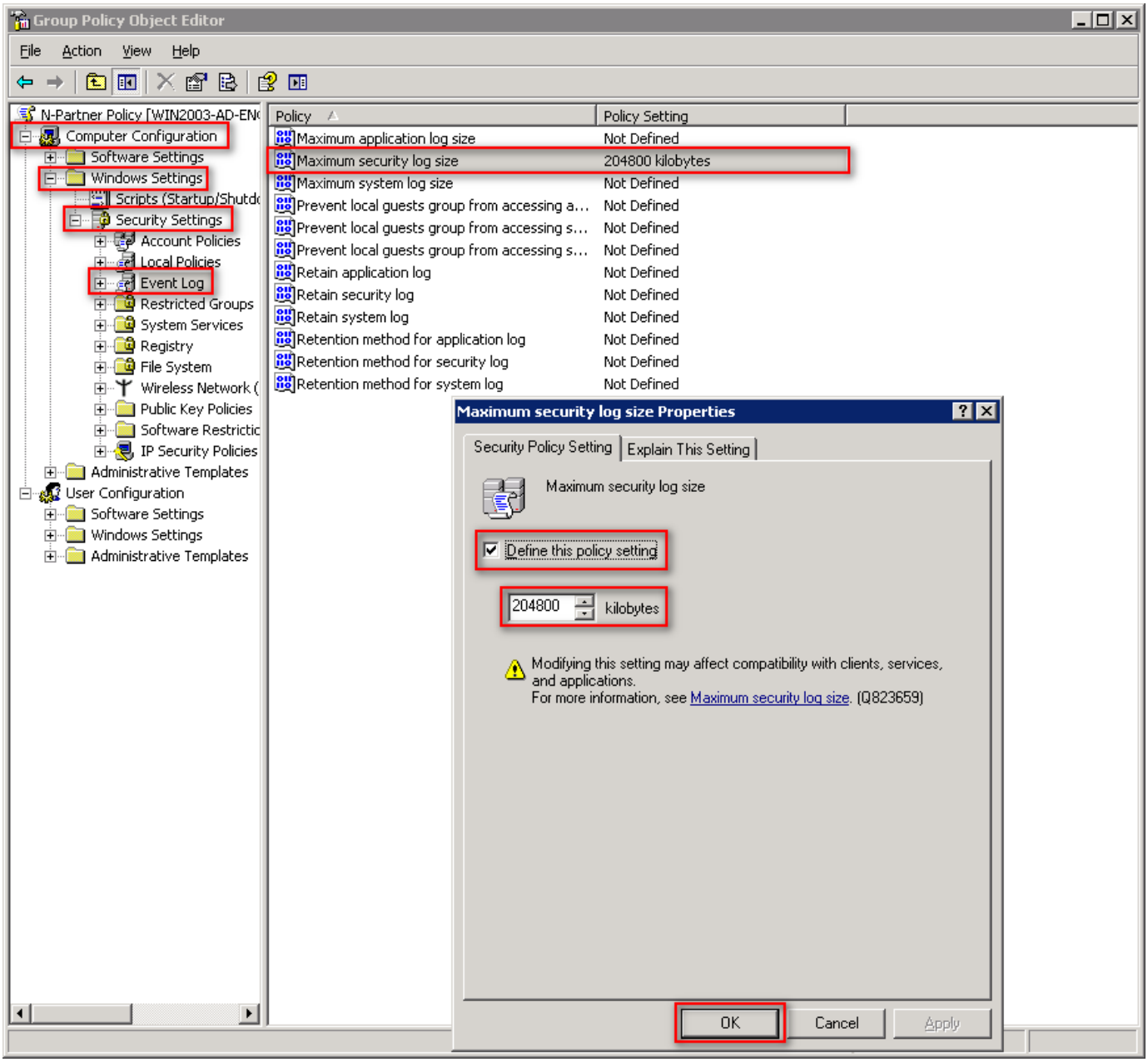
Expand “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log”, then select the “Retention Method for security method” item. Check “Define this policy setting,” select “Overwrite events as needed”, and click “OK.”



(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

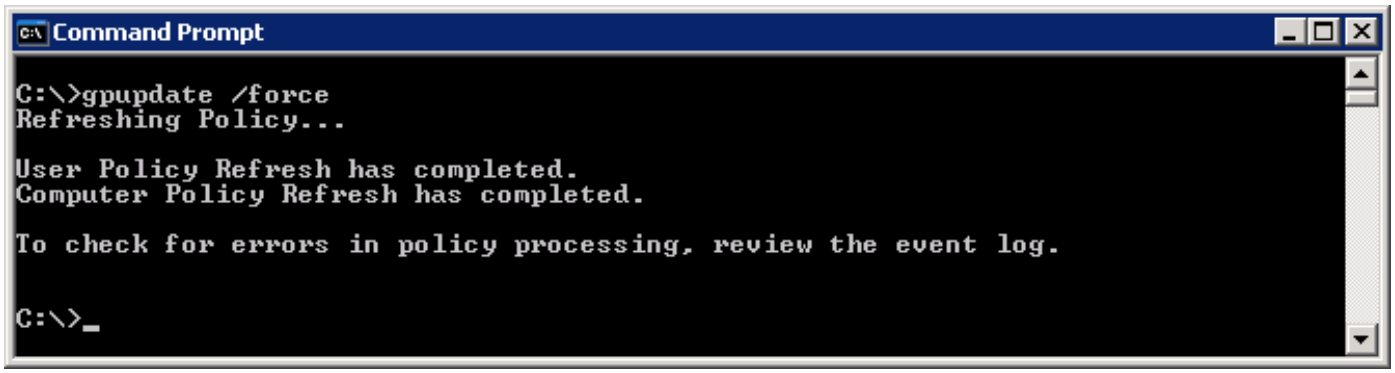
Note: Please adjust the number based on the actual environment -> Click “OK.”



(8) Open “Command Prompt” on your Windows Server.

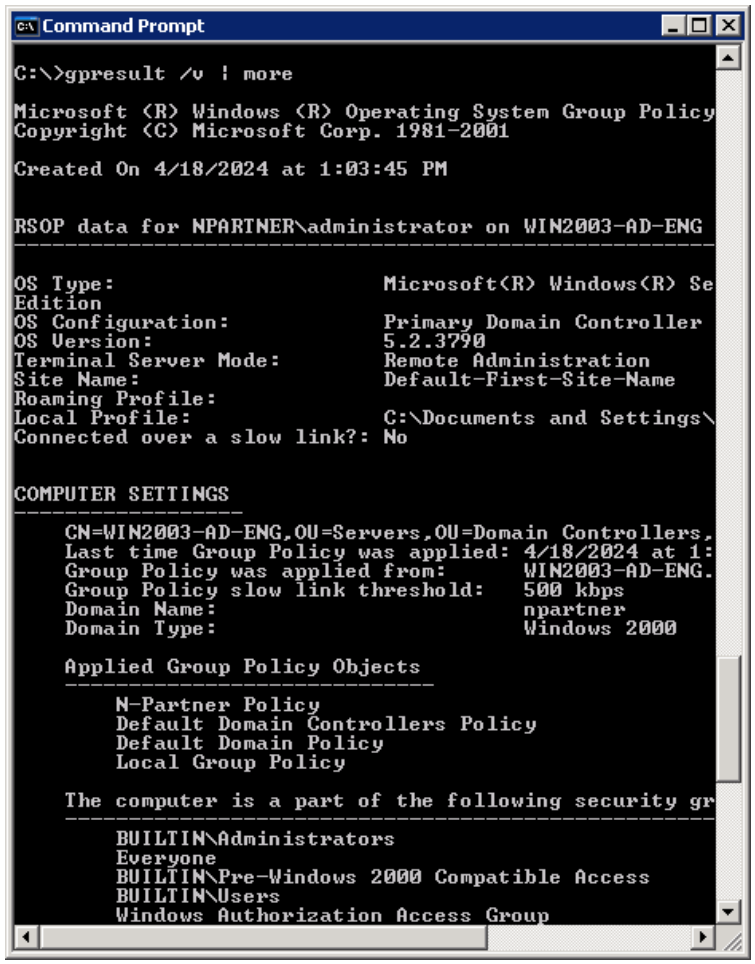
(9) Enter the command below to refresh group policy.

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



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

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



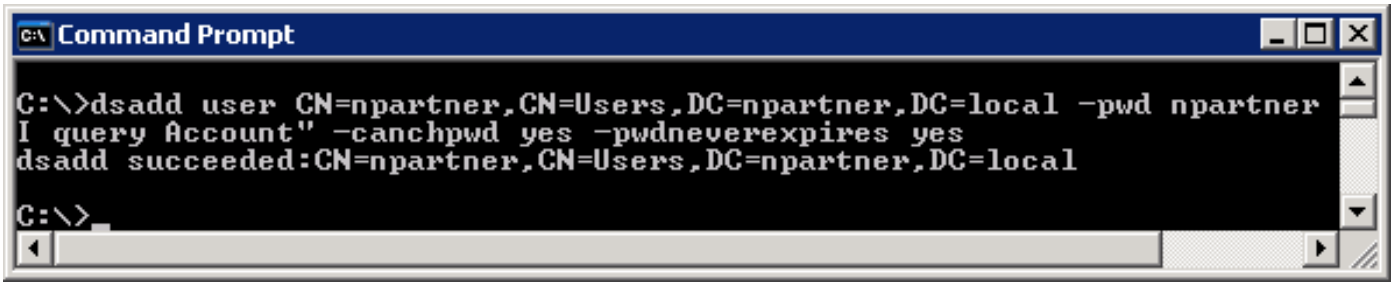
2.3 Add a Non-Admin Account

2.3.1 Add Users

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

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

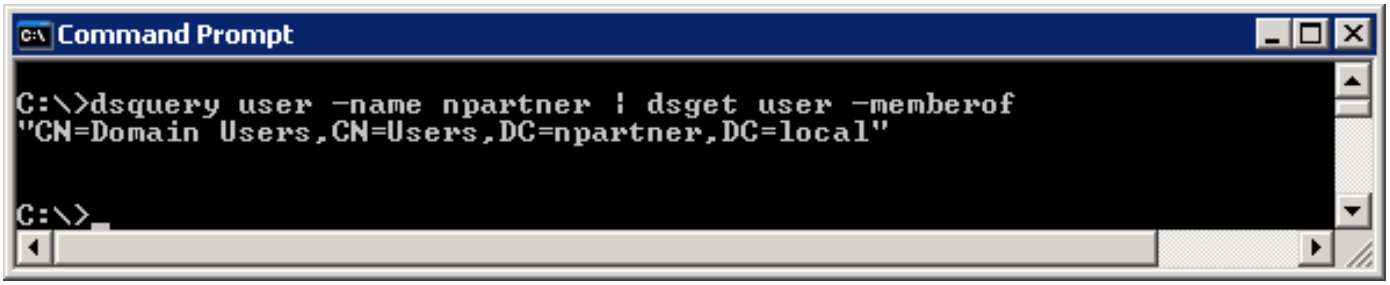
```
C:\> dsadd user CN=npartner,OU=Accounts,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
```



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

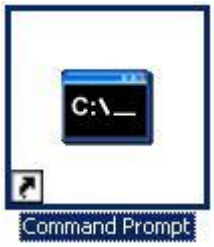
(3) Enter the command below to view the account status.

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



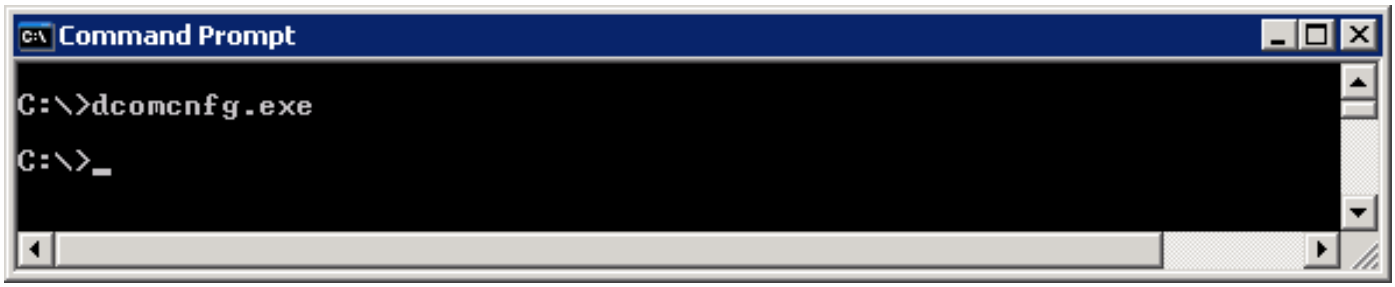
2.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”



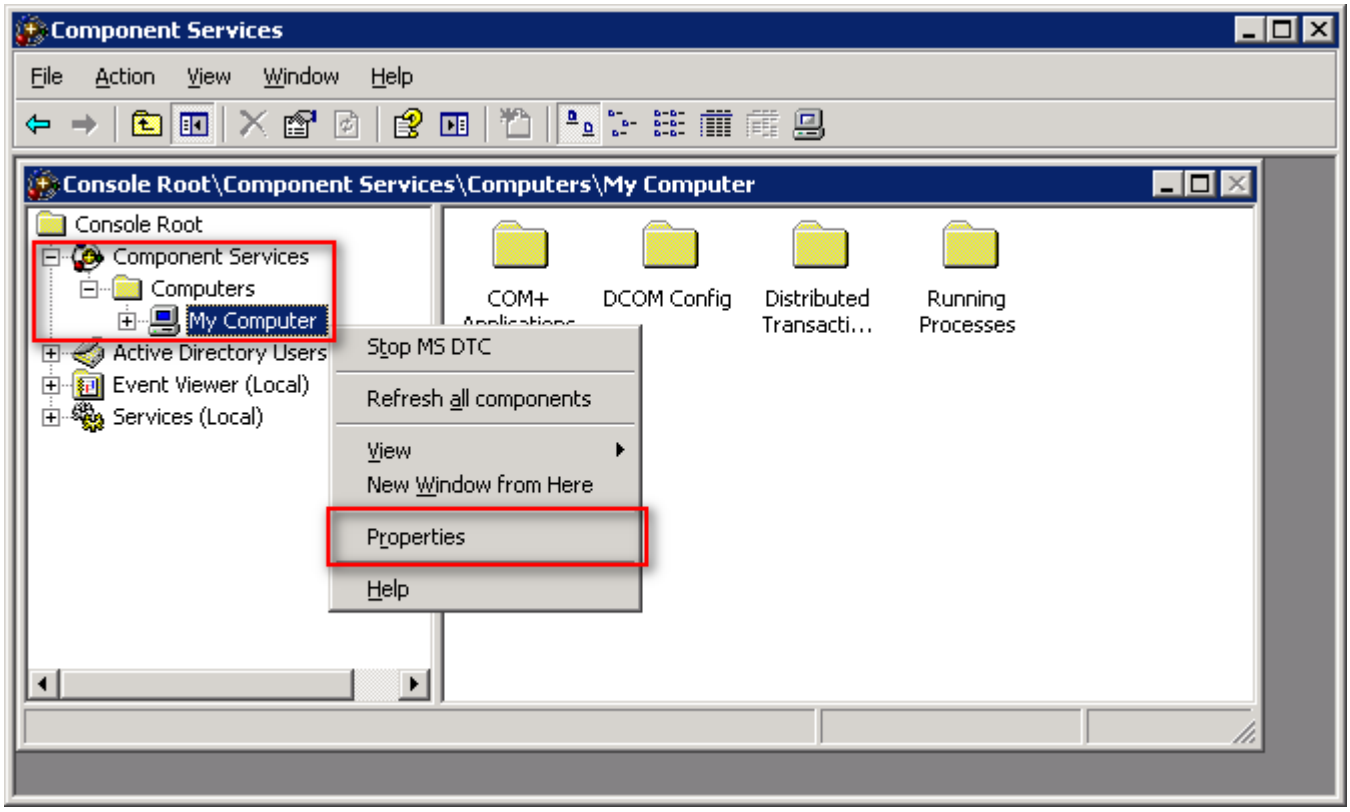
(2) Enter the command below to open component services.

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



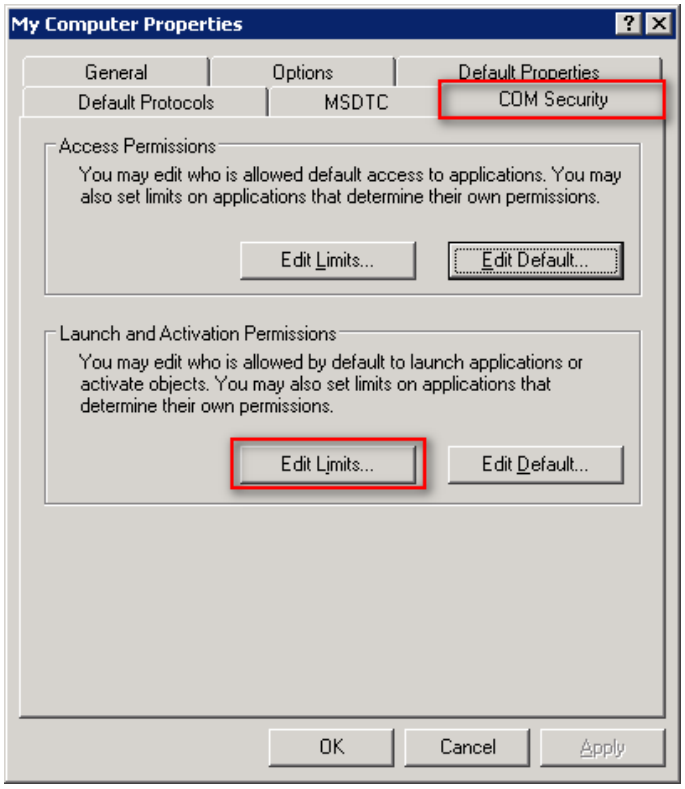
(3) Edit Computer Properties

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



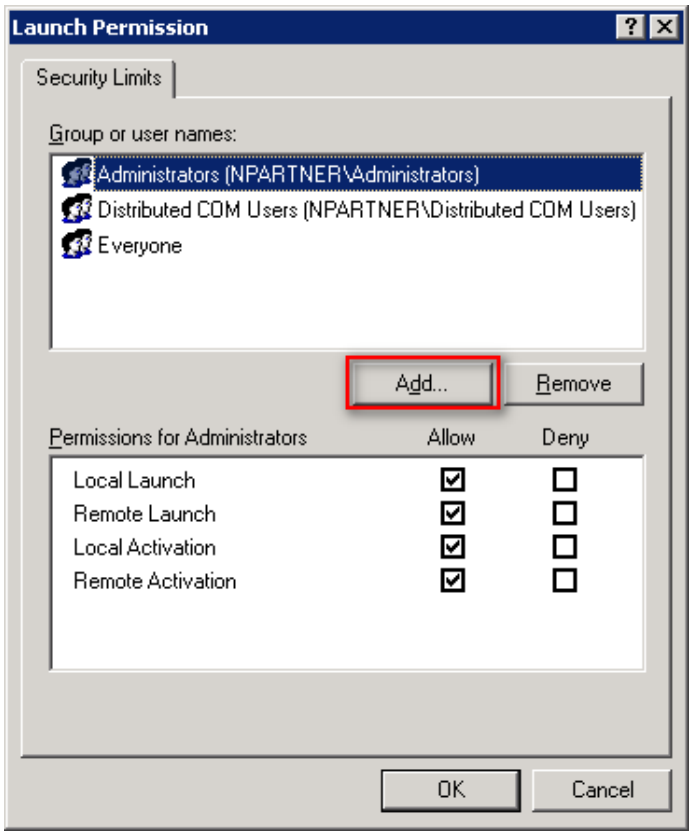
(4) Enable Permissions

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



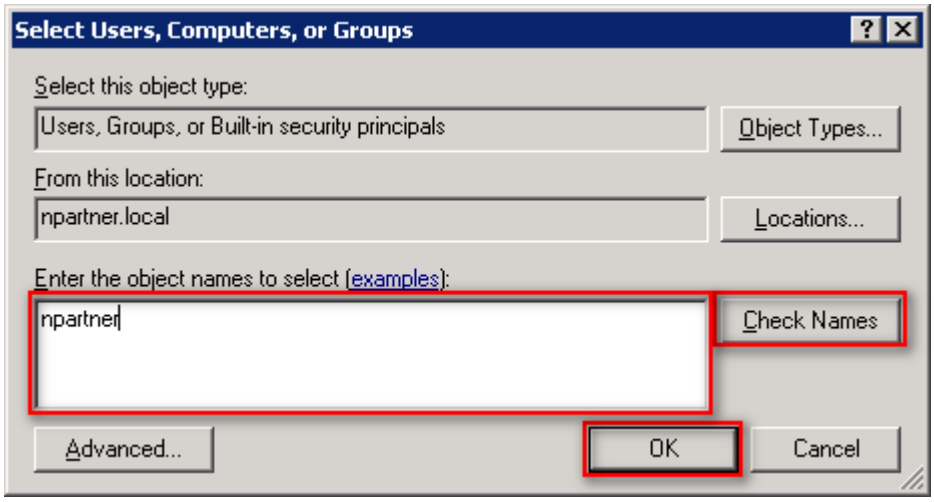
(5) Add DCOM User Permissions

Click “Add.”



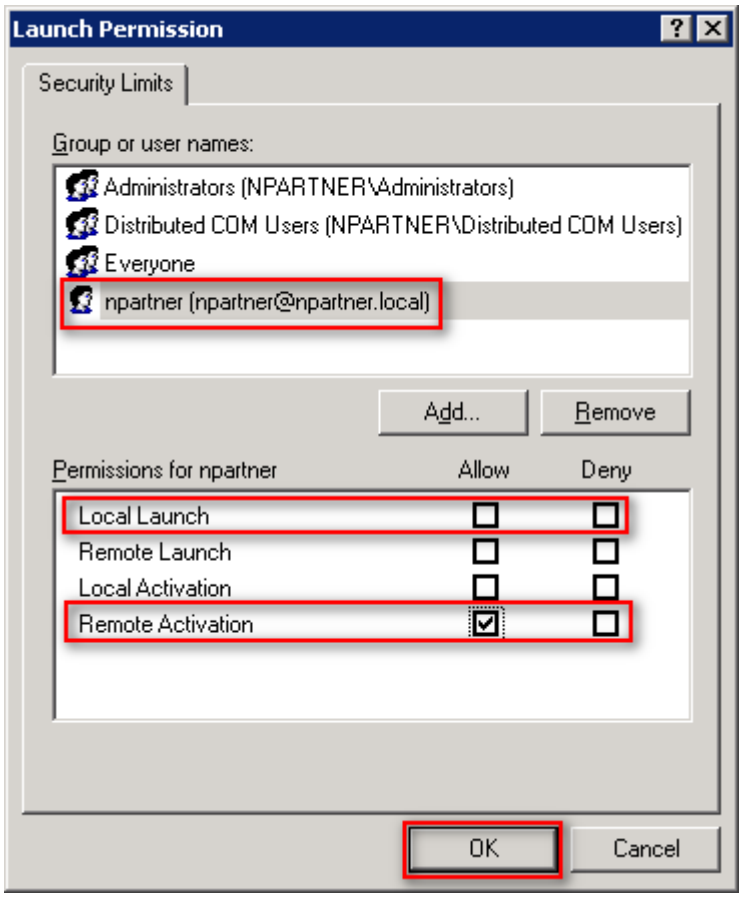
(6) Enter your Username

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

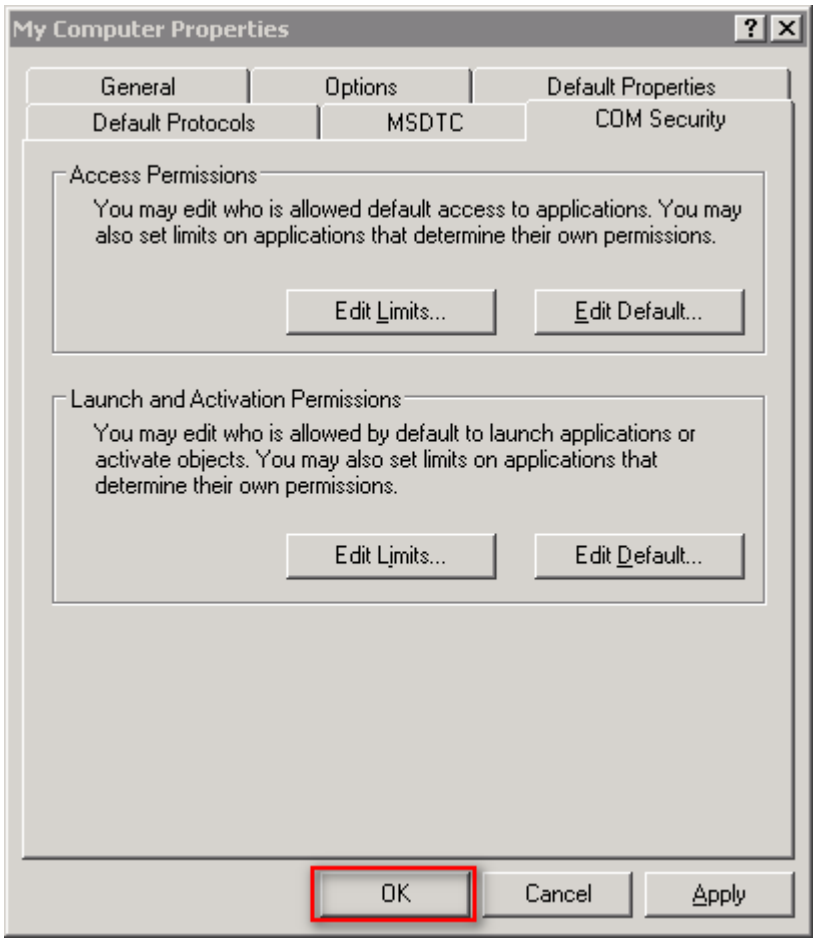


(7) Set User Permissions

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



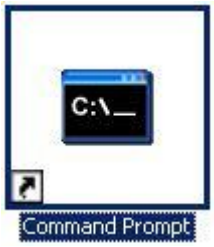
(8) Click “OK.”



2.3.3 Configure WMI Permissions

2.3.3.1 Set Event Log Permissions

(1) Open “Command Prompt.”

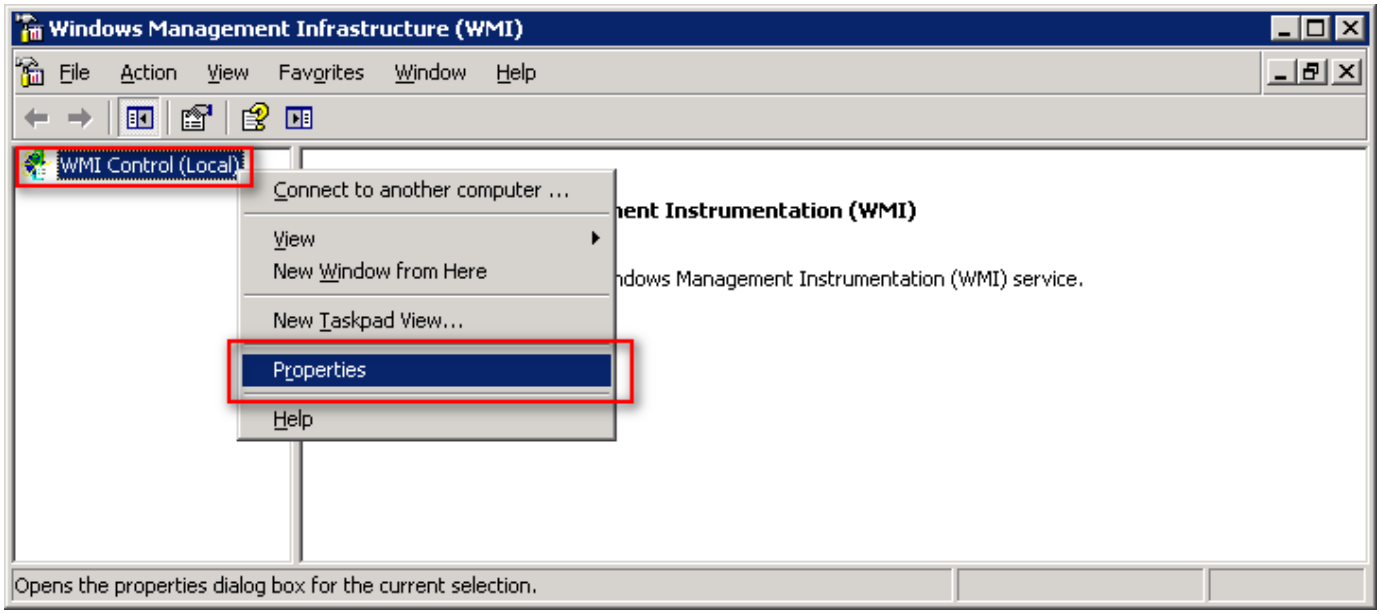


(2) Enter the command below to enable component services.

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

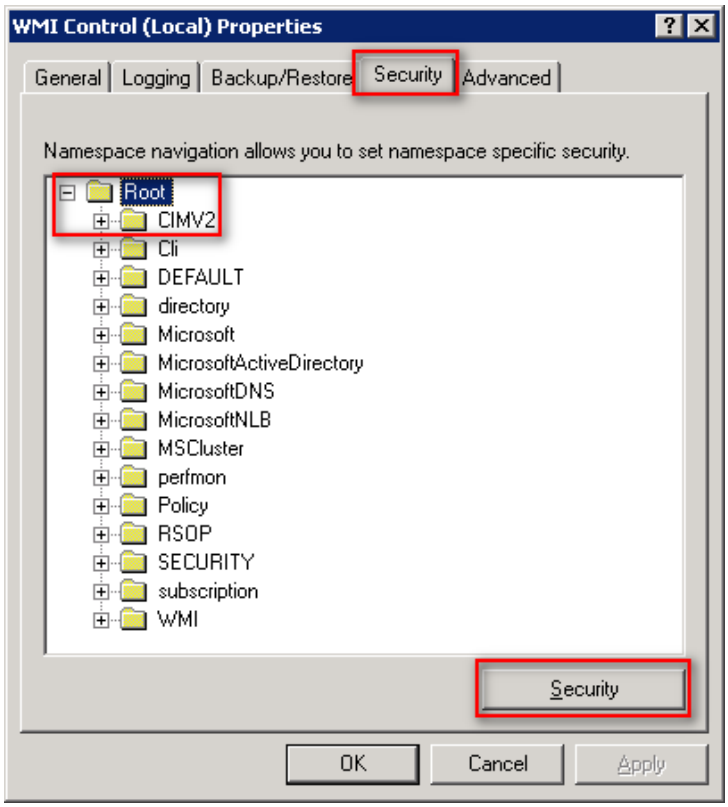
(3) Edit WMI Control

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



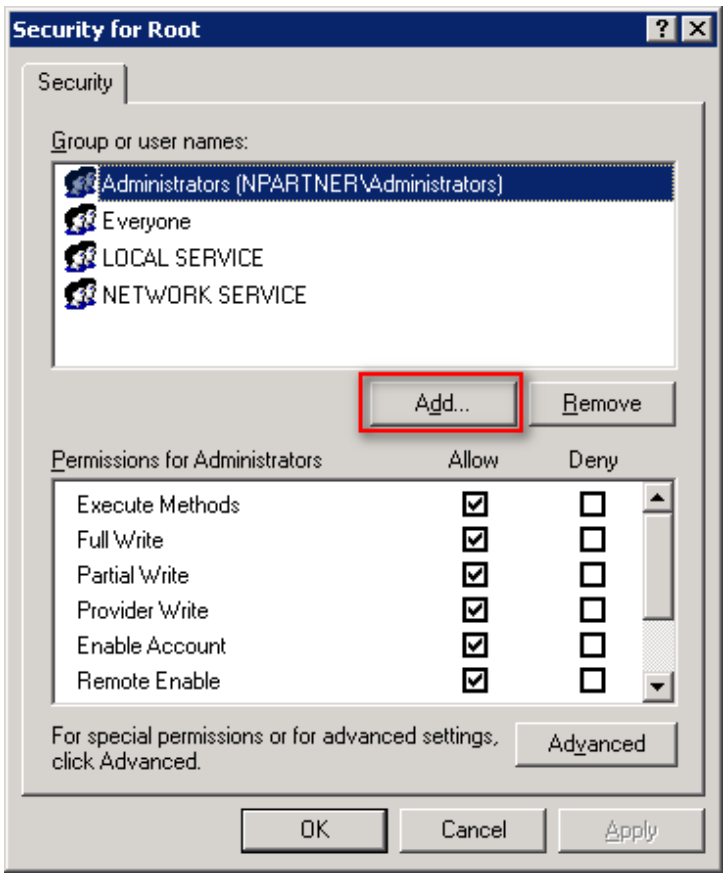
(4) Edit CIMV2 Security

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



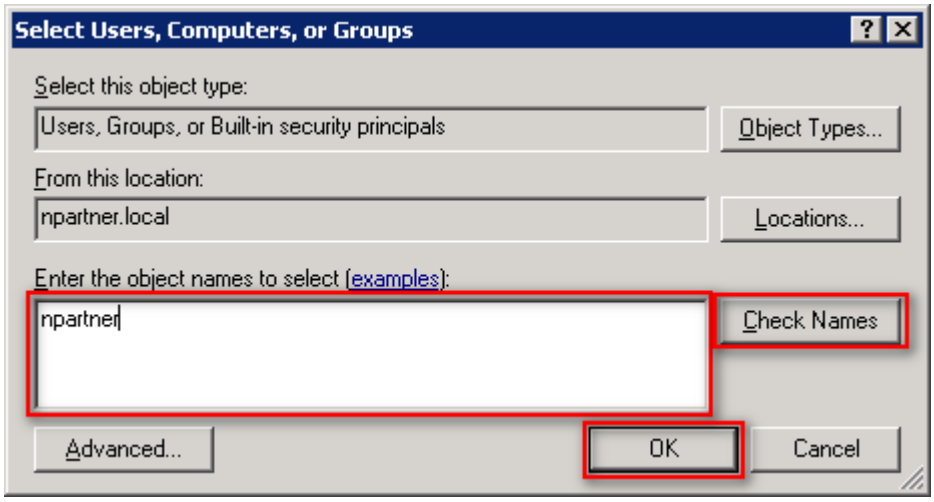
(5) Add WMI User Permissions

Click “Add.”



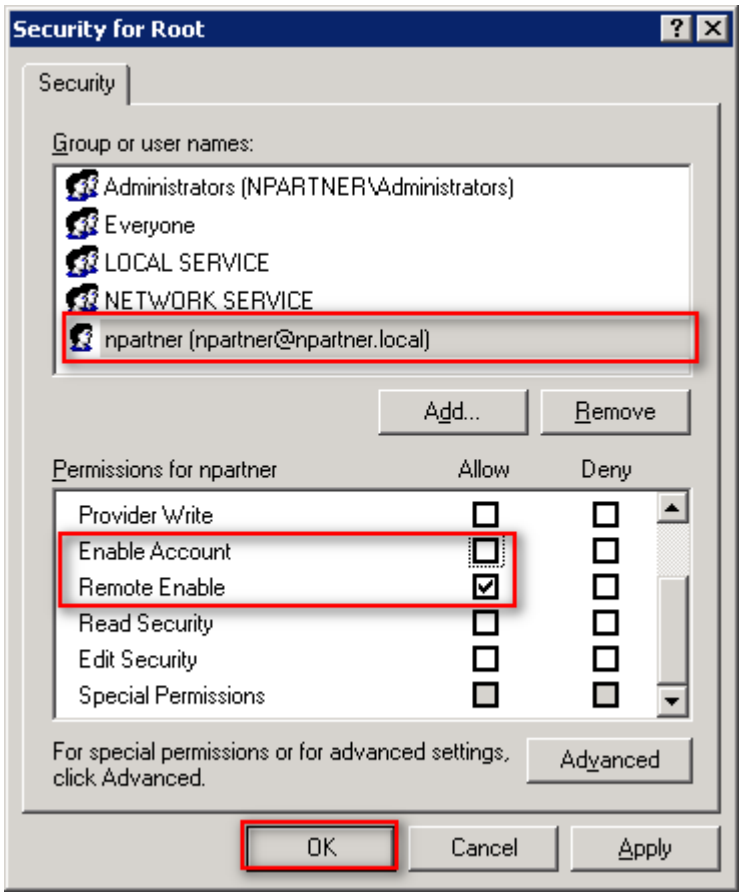
(6) Enter User

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

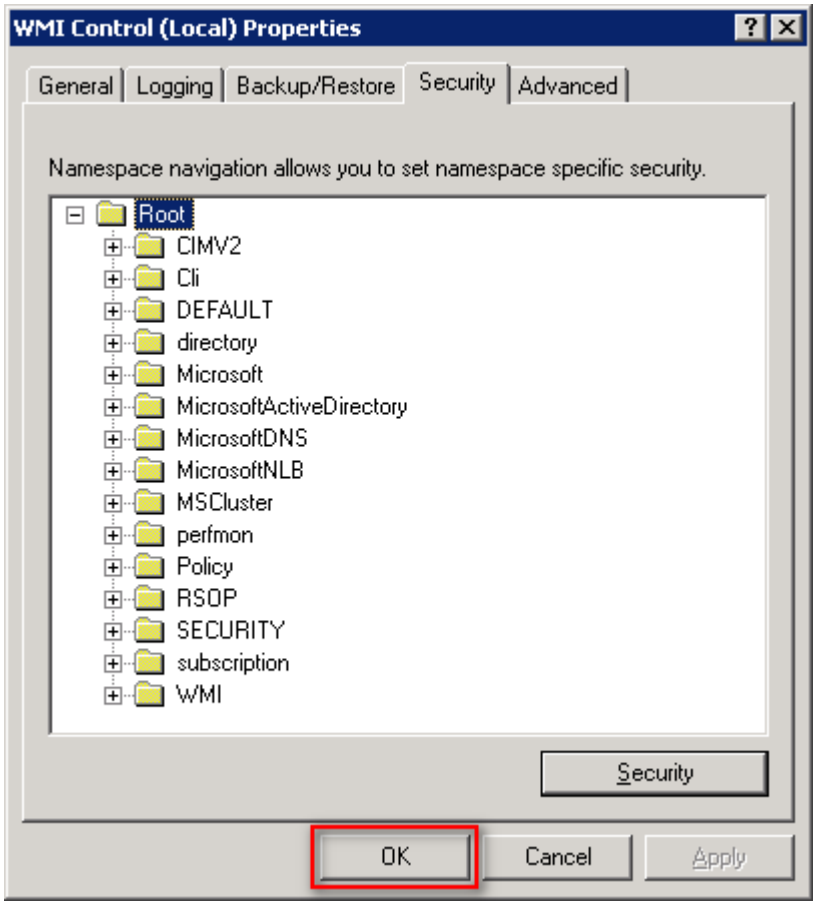


(7) Set User Permissions

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

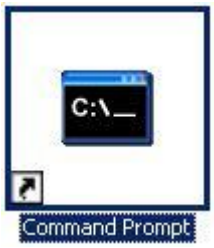


(8) Click “OK.”



2.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”

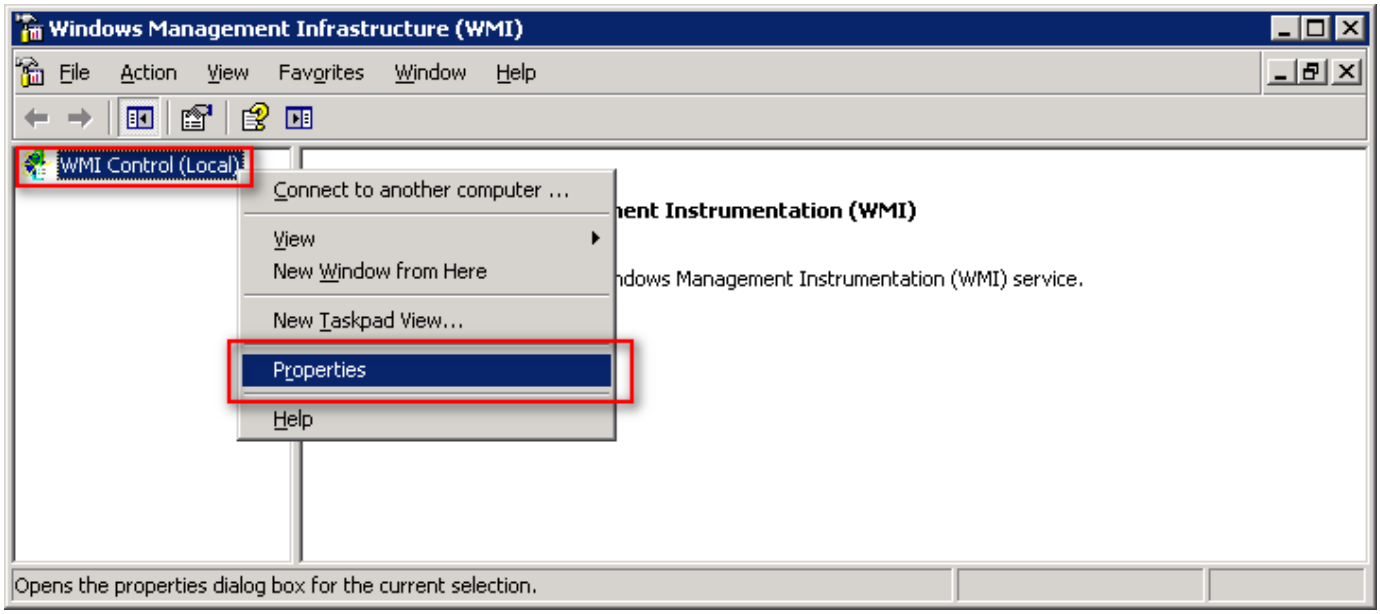


(2) Open “WMI Control.”

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

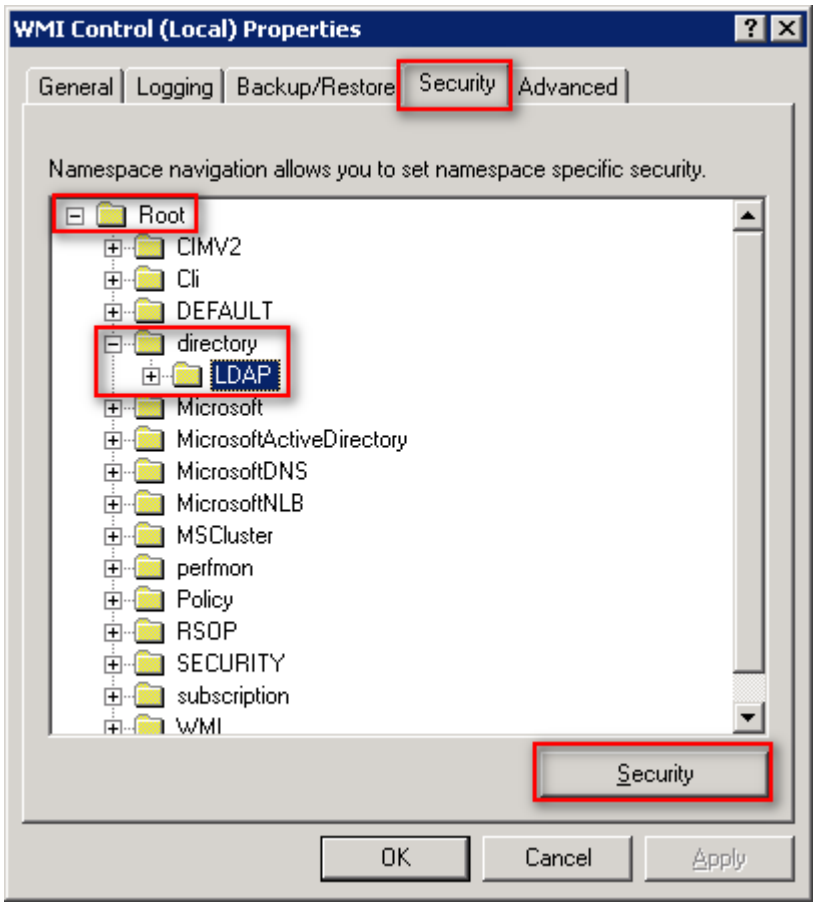
(3) Edit WMI Control

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



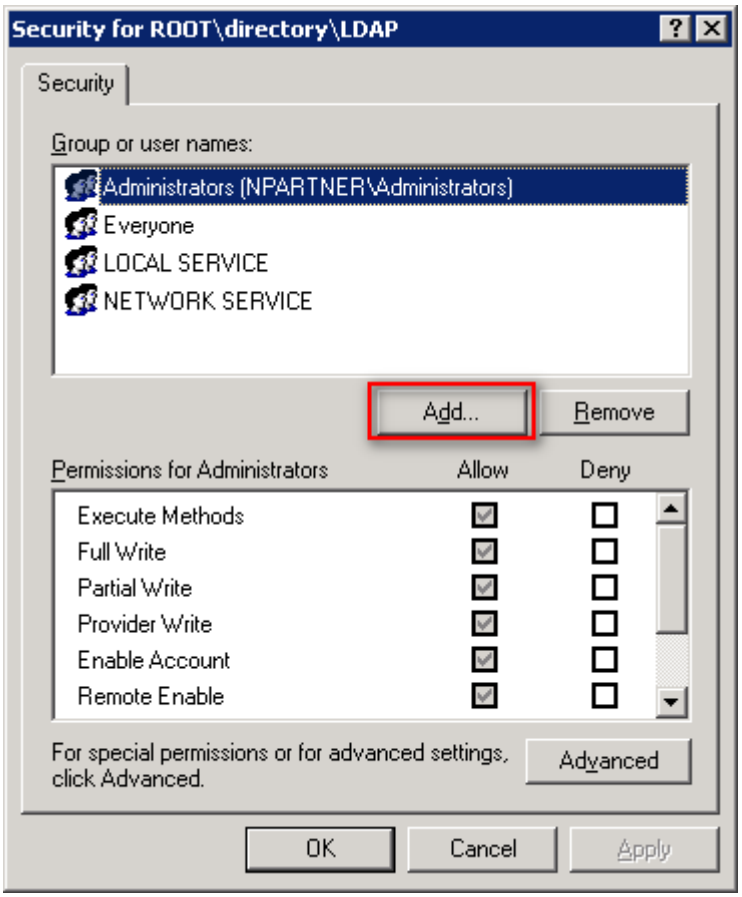
(4) Edit LDAP Security Settings

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



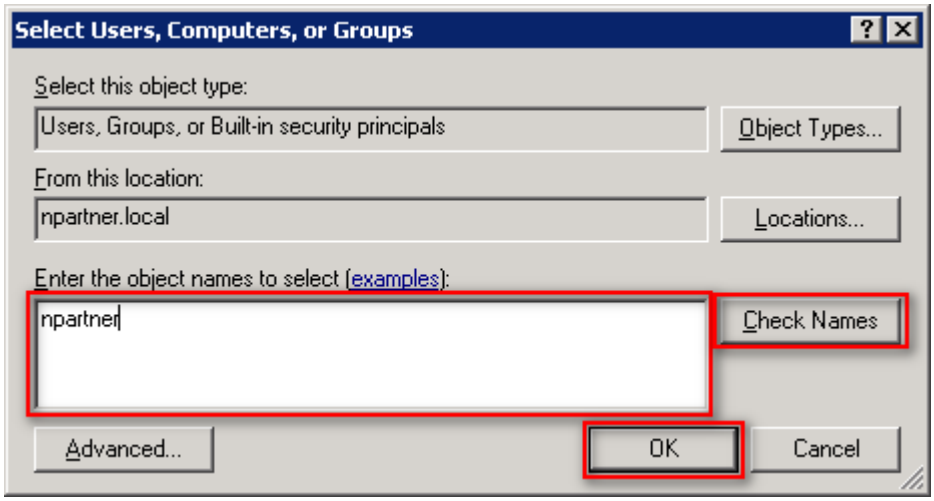
(5) Add WMI User Permissions

Click “Add.”



(6) Specify the User

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

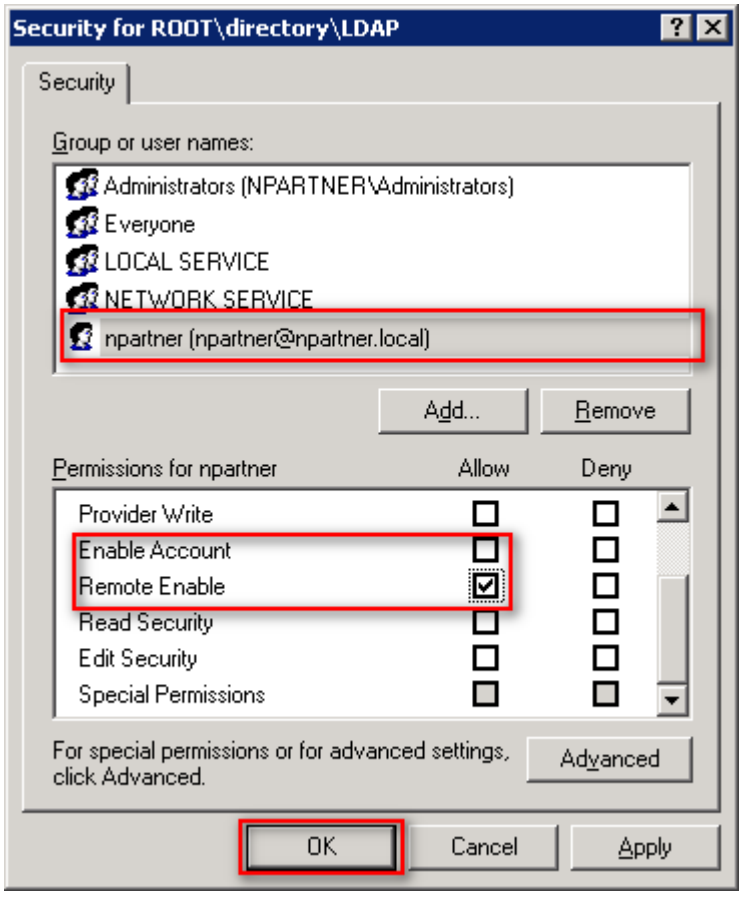


(7) Configure User Permissions

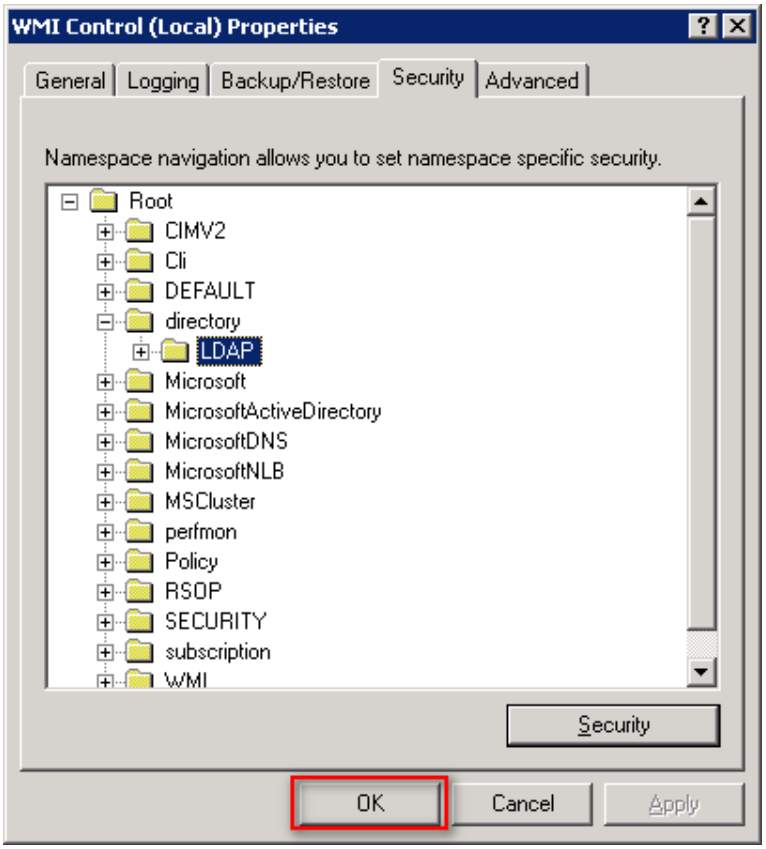
Select the user account (npartner):

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

  Click OK.



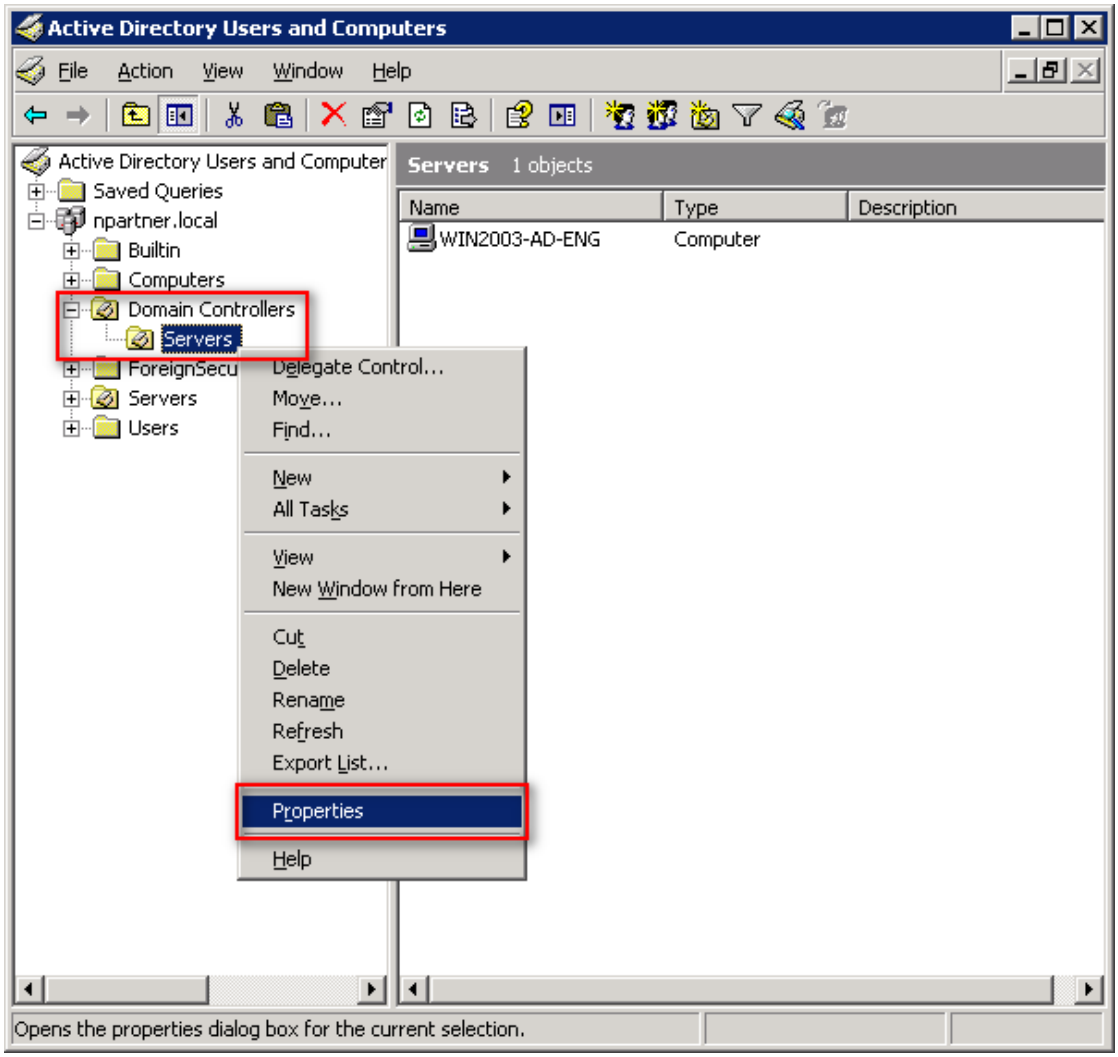
(8) Click “OK.”



2.3.4 Configure Event Log Read Permissions

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

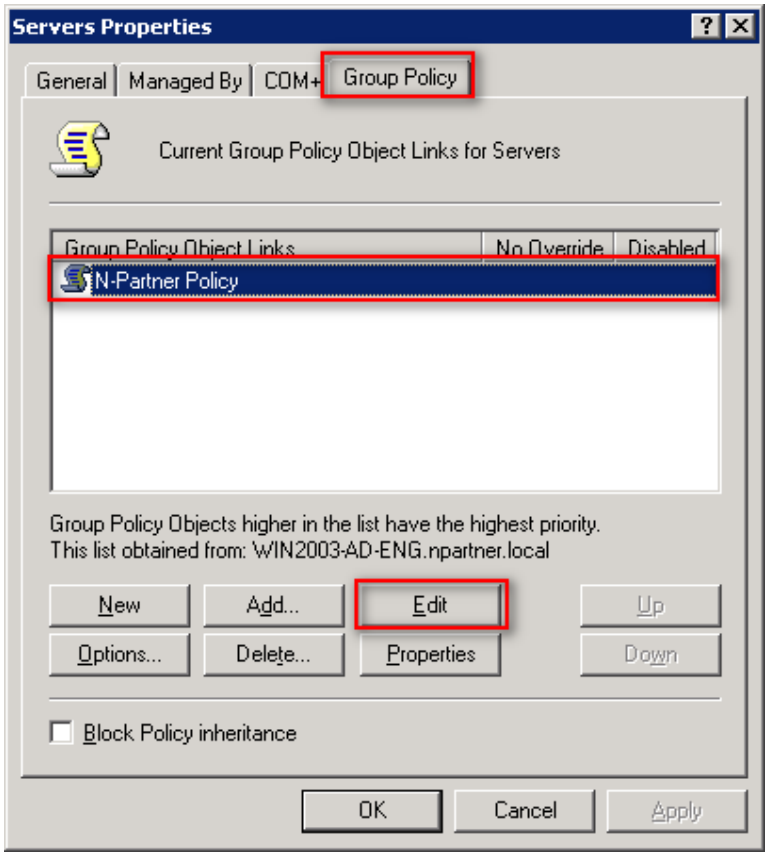
(2) Right-click the “Servers” organizational unit under Domain Controllers, then select “Properties.”



(3) Edit Your Group Policy Object

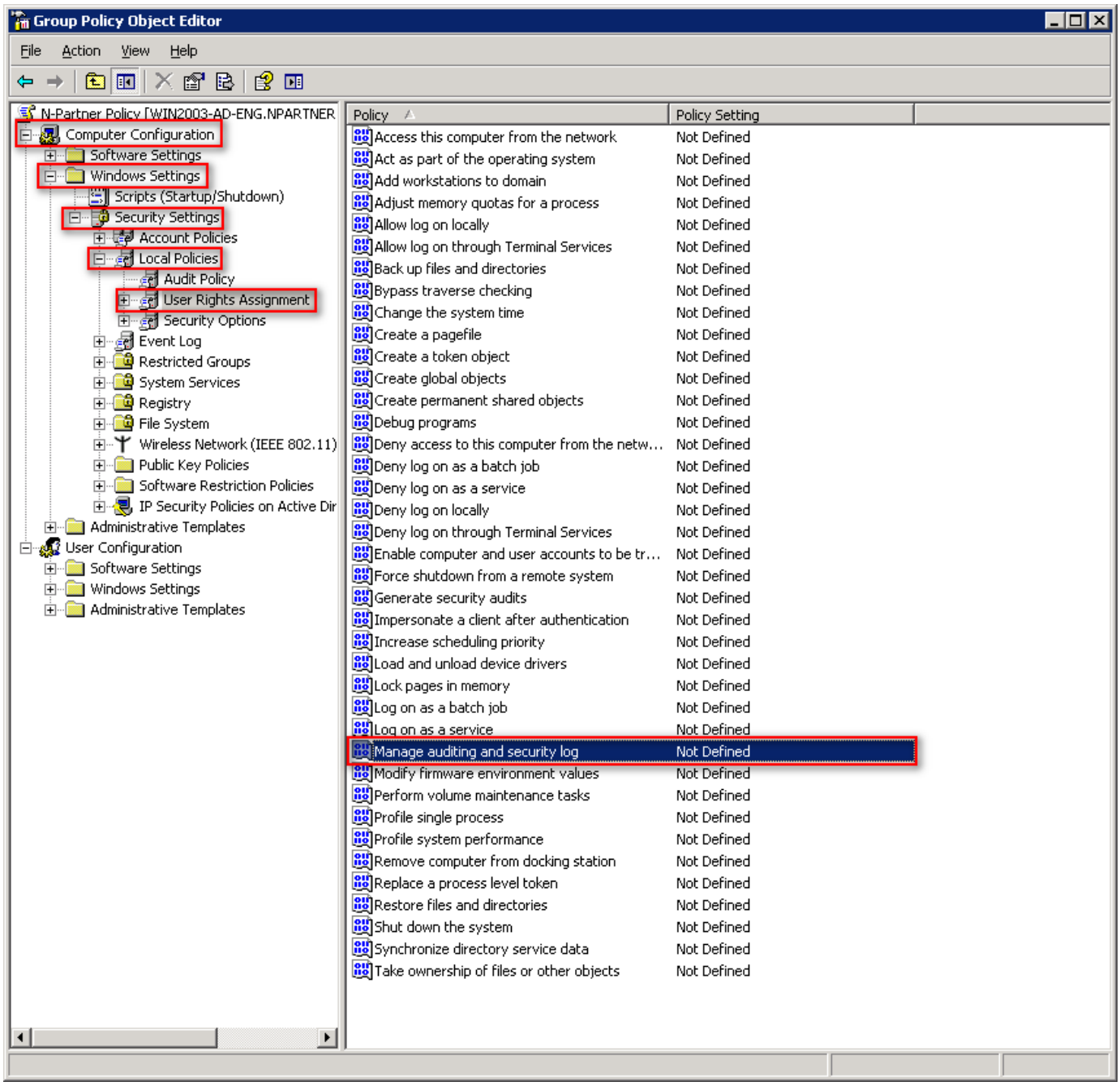
Enter your group policy object name (the example here is N-Partner Policy)

Click “Edit.”



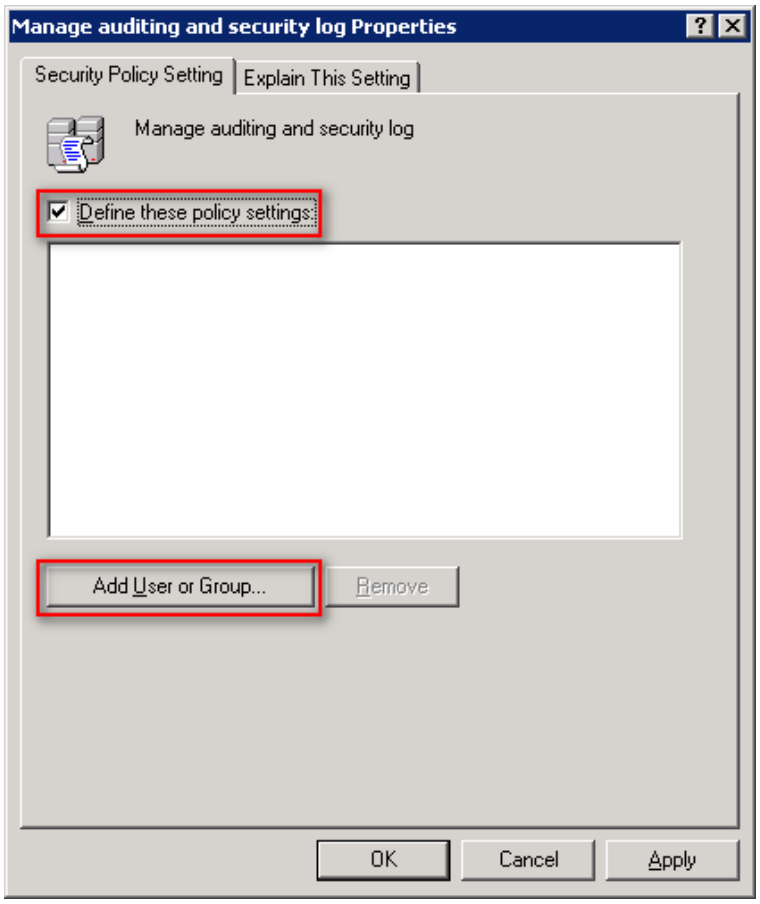
(4) Configure Logging

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



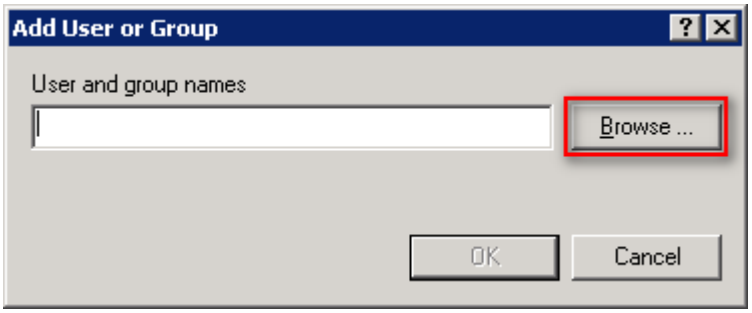
(5) Add Audit Management Users

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



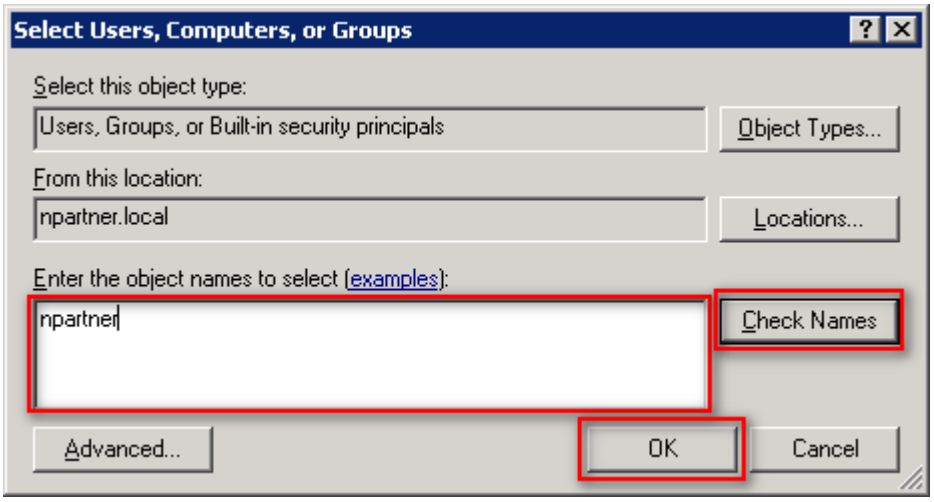
(6) Search for Users

Click “Browse.”



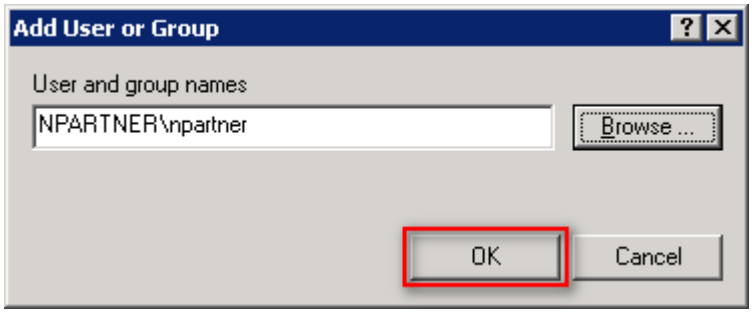
(7) Specify the User

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



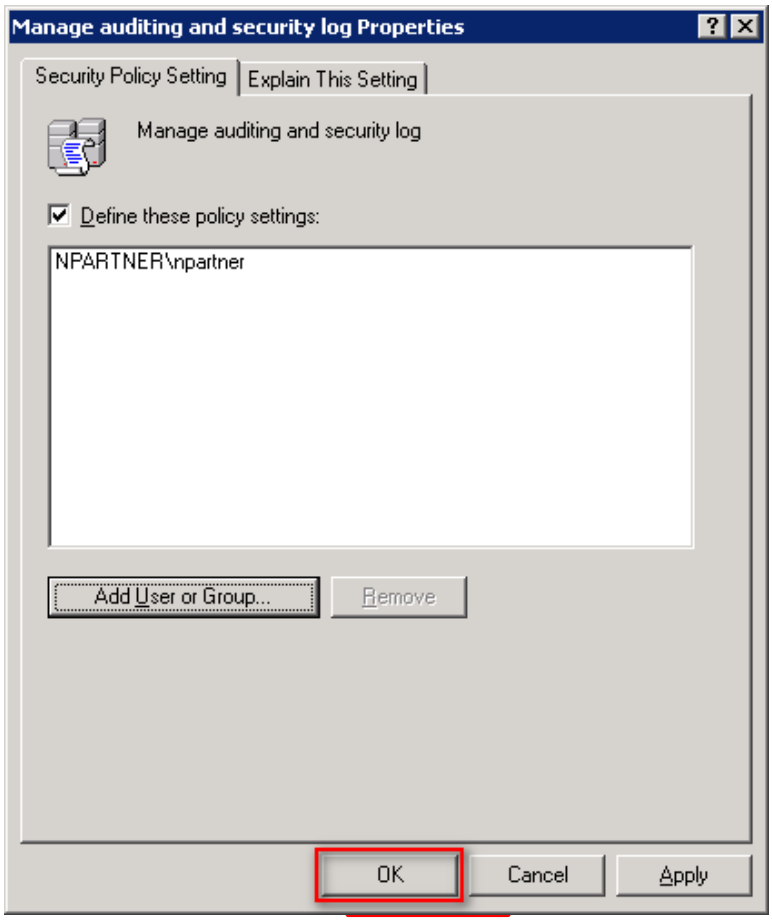
(8) Confirm the User

Click “OK.”



(9) Confirm log settings

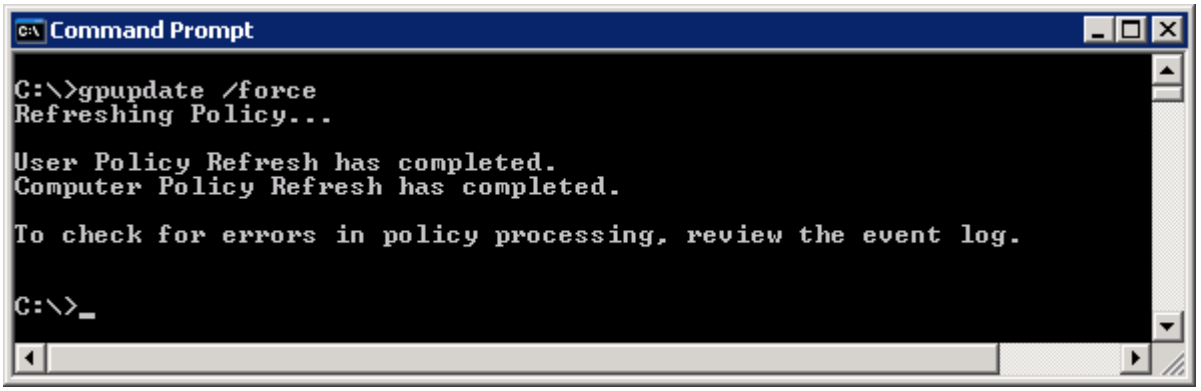
Click “OK.”



(10) Click “Command Prompt.”

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

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

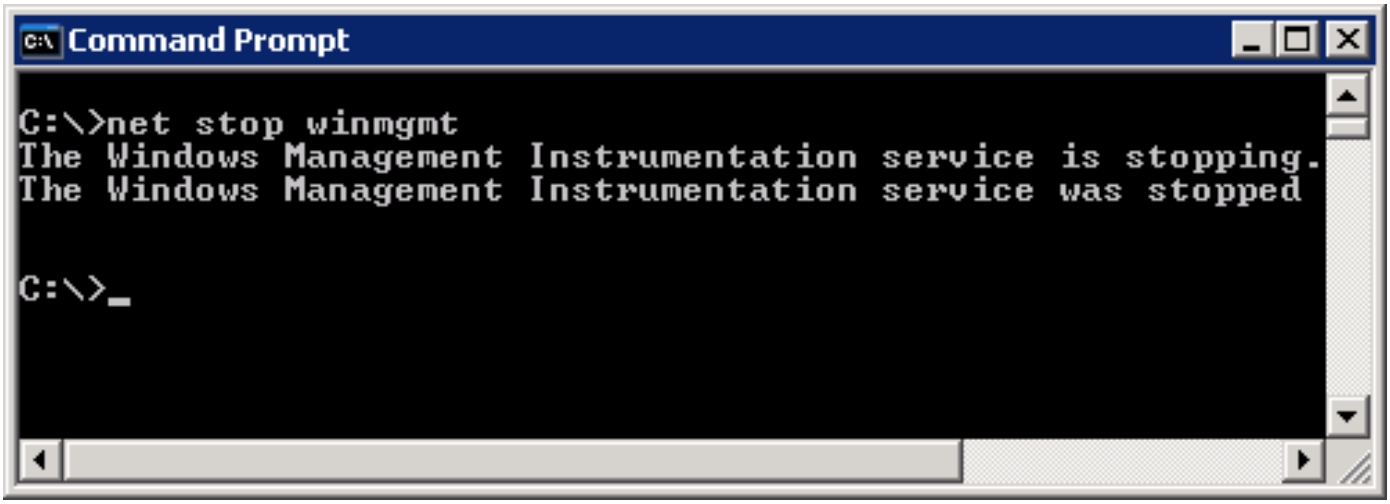


2.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”

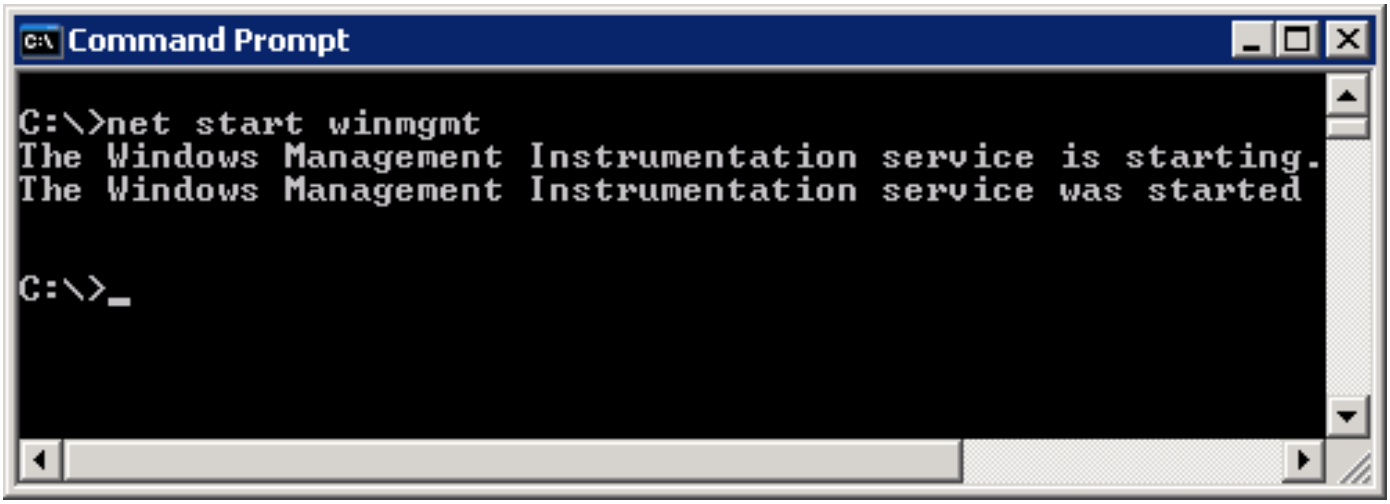
(2) Enter the command below to disable the WMI service.

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



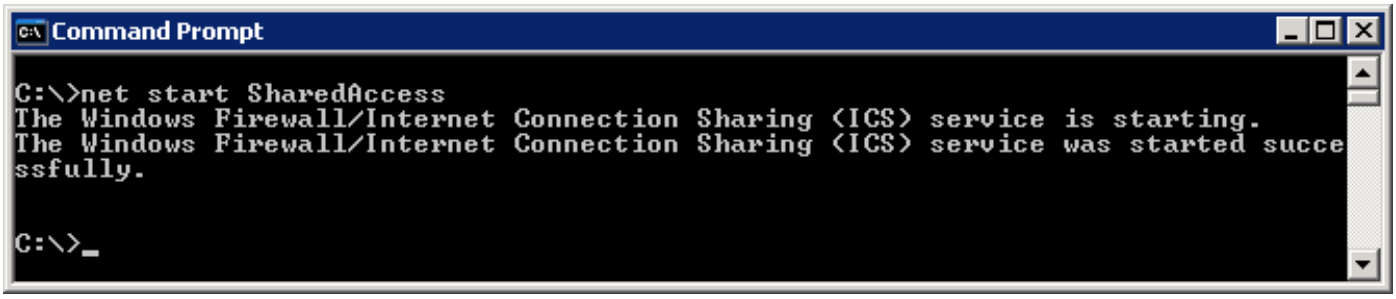
(3) Enter the command below to enable WMI service.

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



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

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

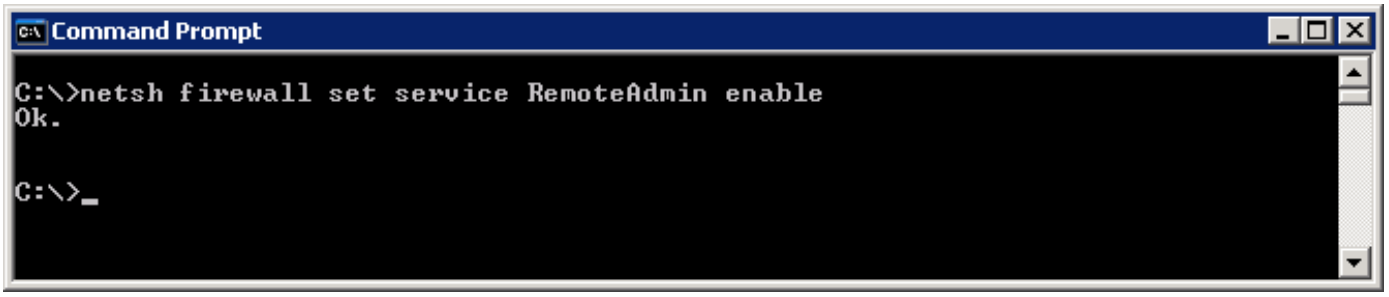


2.4 Firewall Configuration

(1) Open “Command Prompt.”

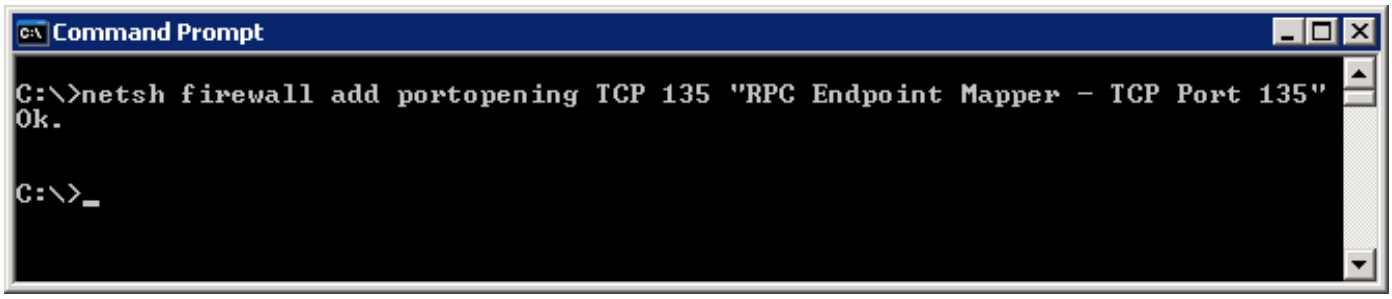
(2) Enter the command below to allow WMI traffic through the firewall.

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



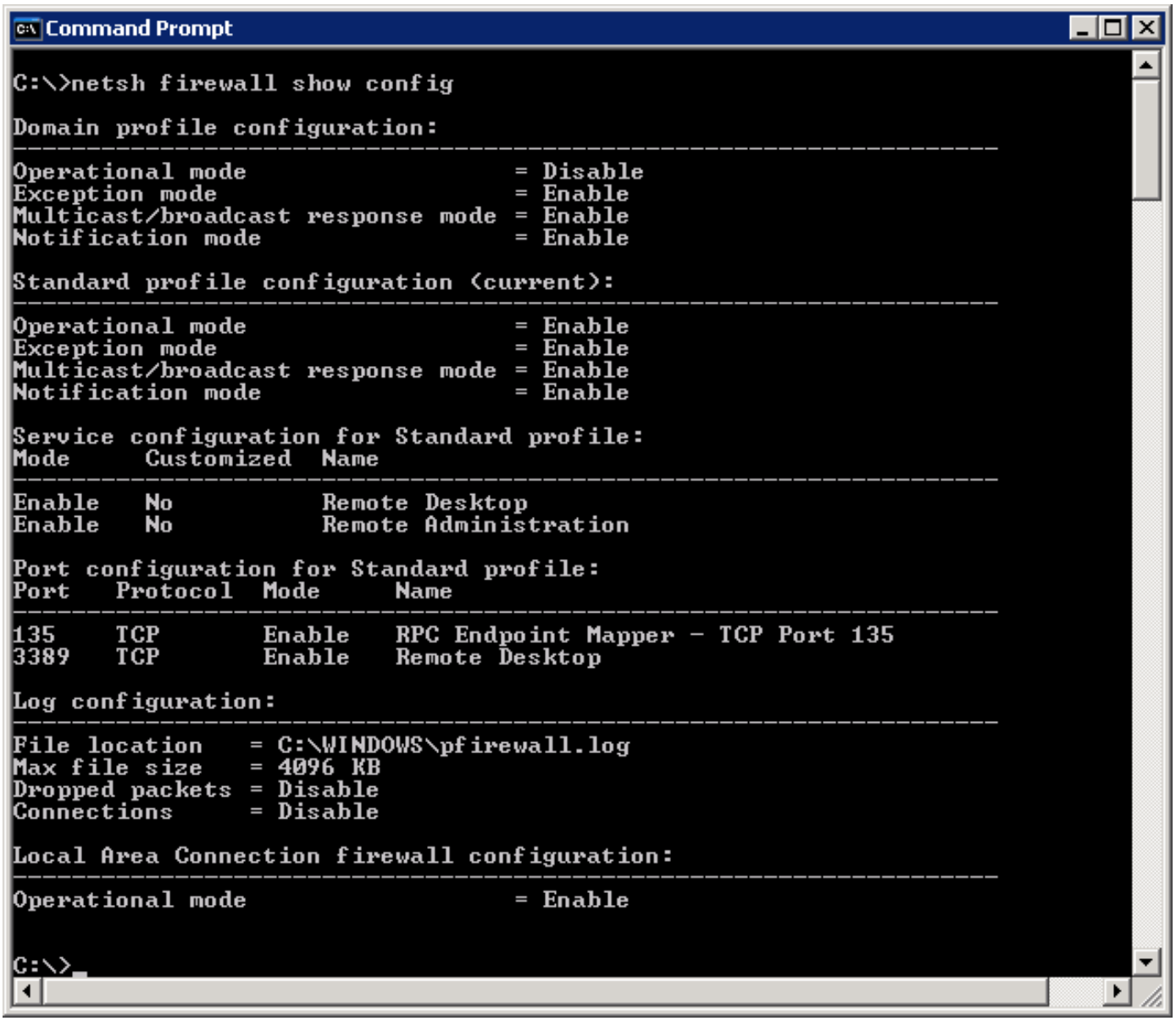
(3) Enter the command below to allow TCP Port 135 through the firewall.

```
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
```

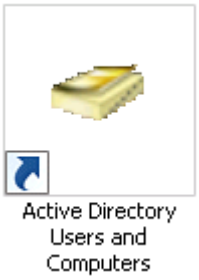


3. Windows 2008

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

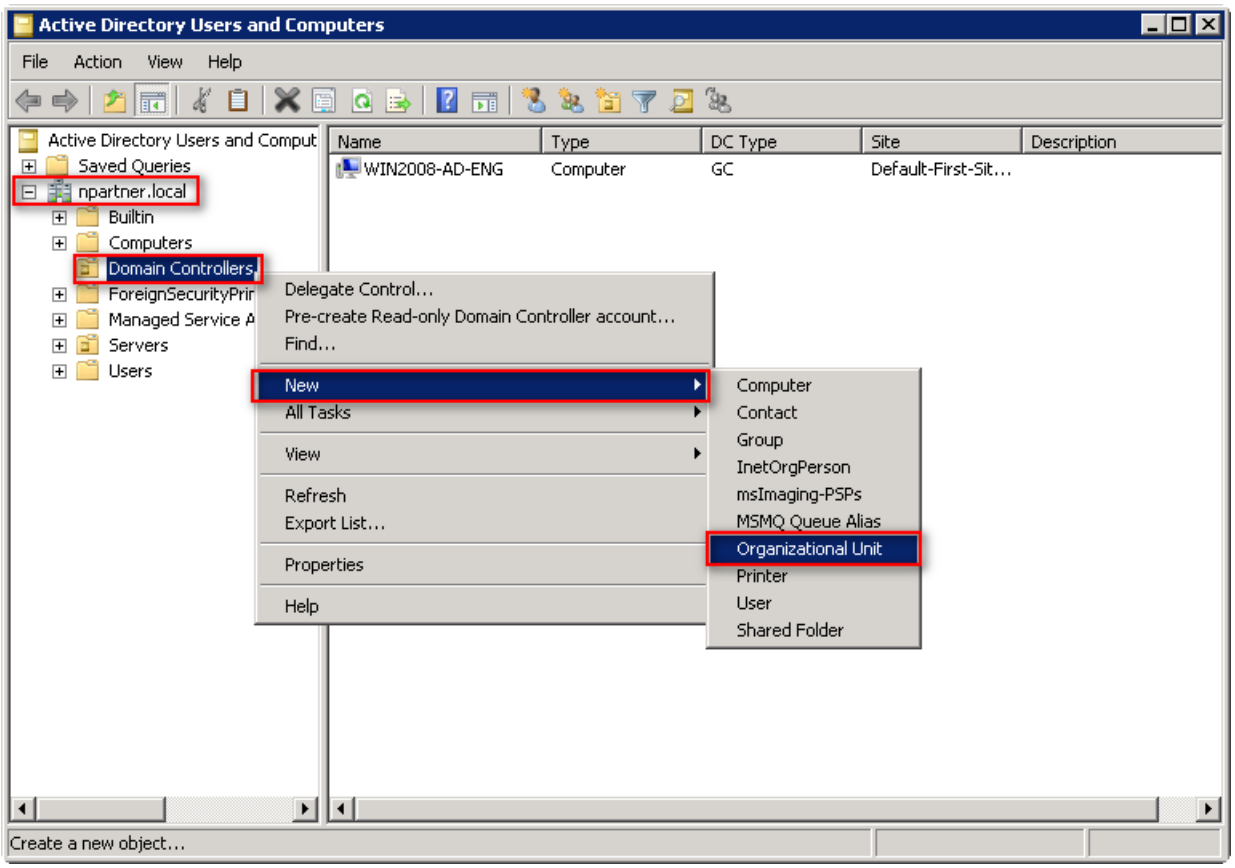
3.1 Organizational Unit Settings

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



(2) Add an Organizational Unit

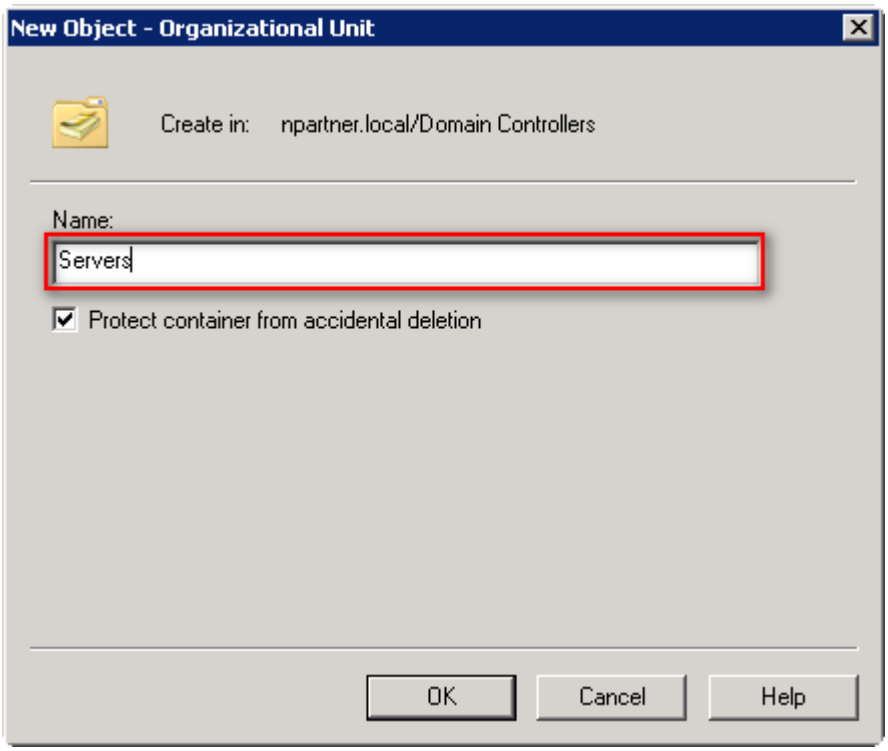
Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(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.

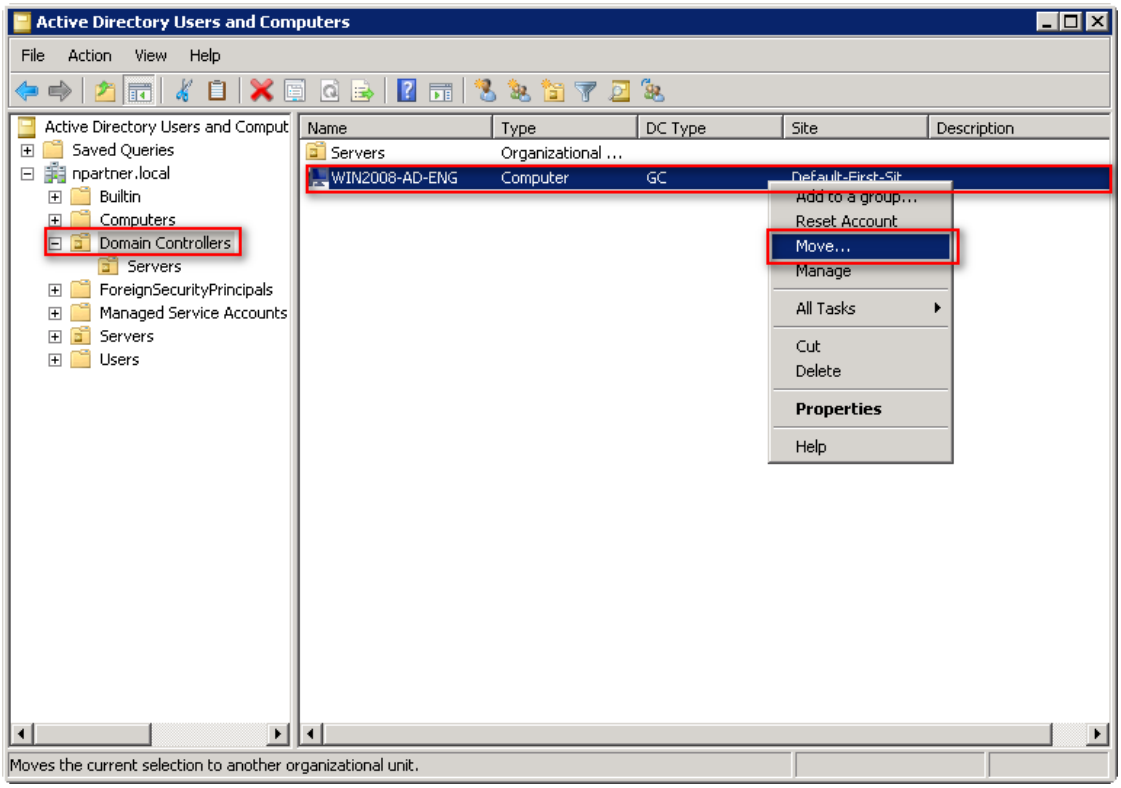
-> Click “OK.”



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

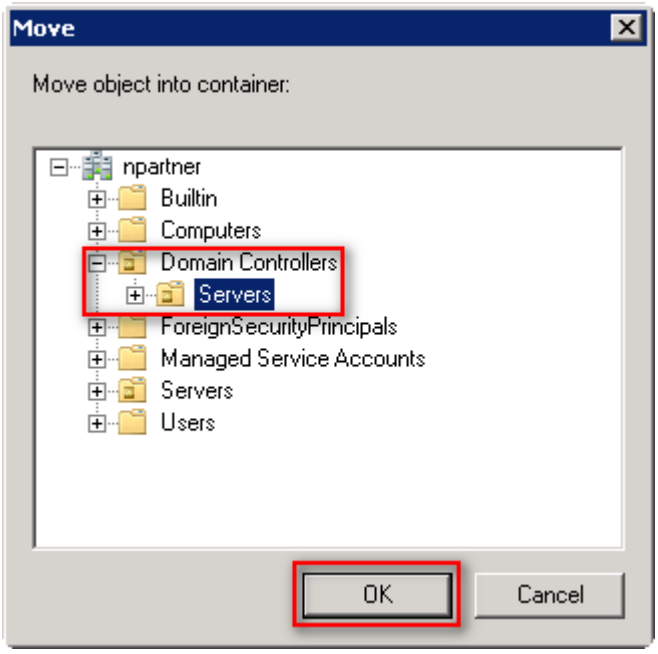
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2008-AD-ENG” server.

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



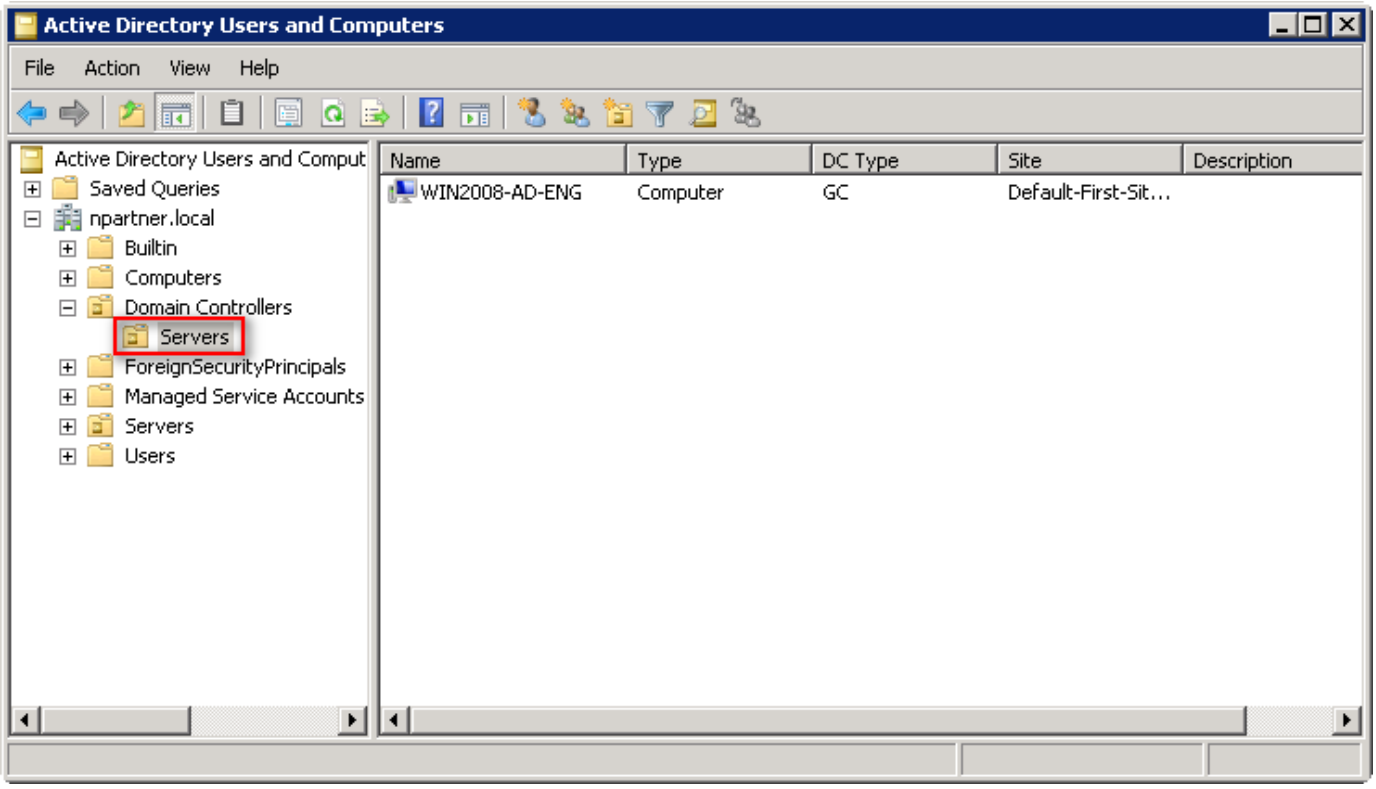
(5) Select your Organizational Unit:

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:

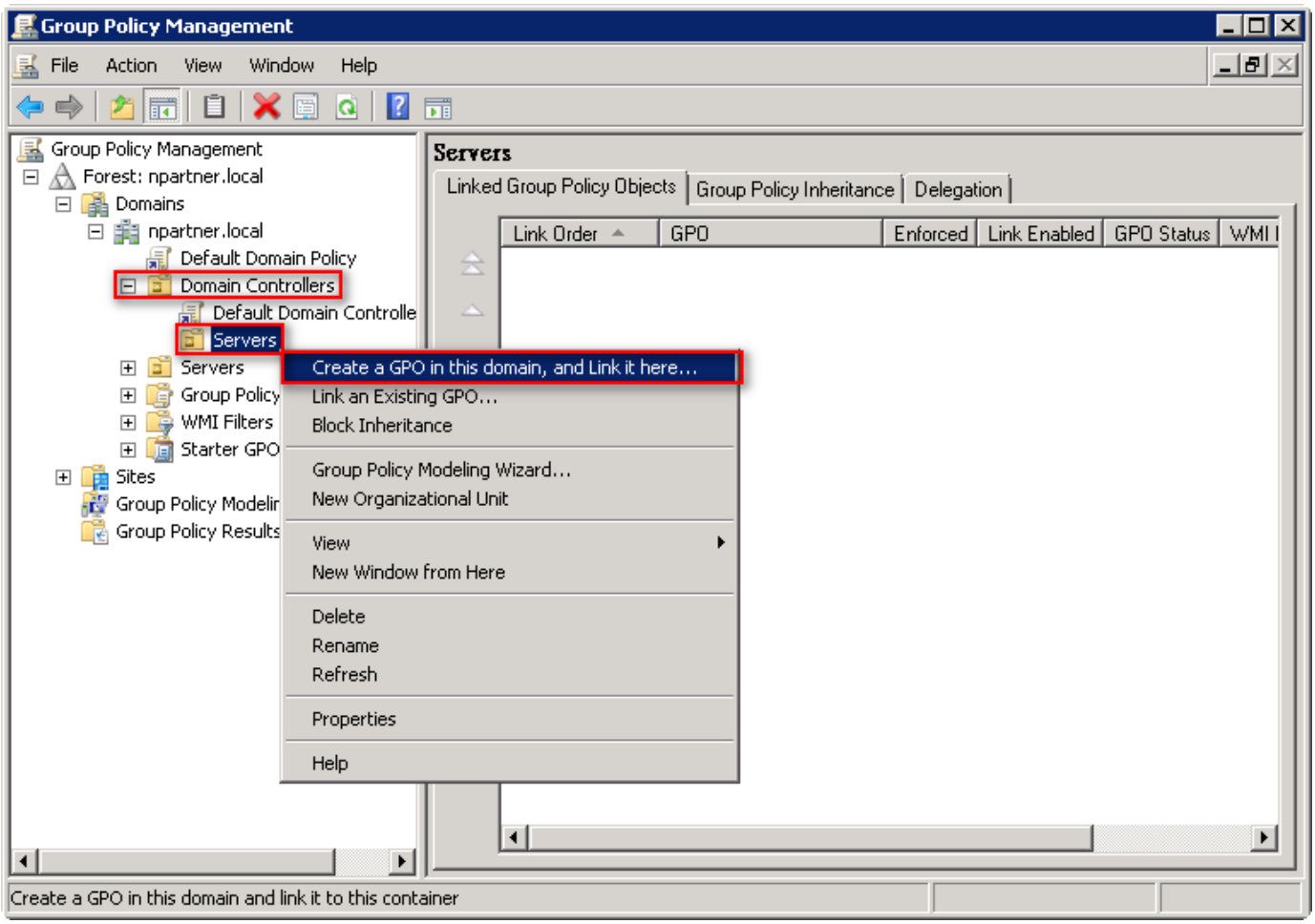
Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2008-AD-ENG” server has been moved.



3.2 Group Policy Settings

(1) Open “Group Policy Management.”

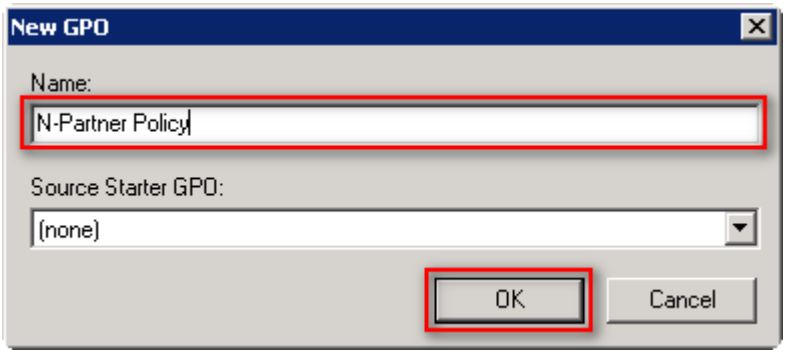
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(3) Edit your Group Policy Object

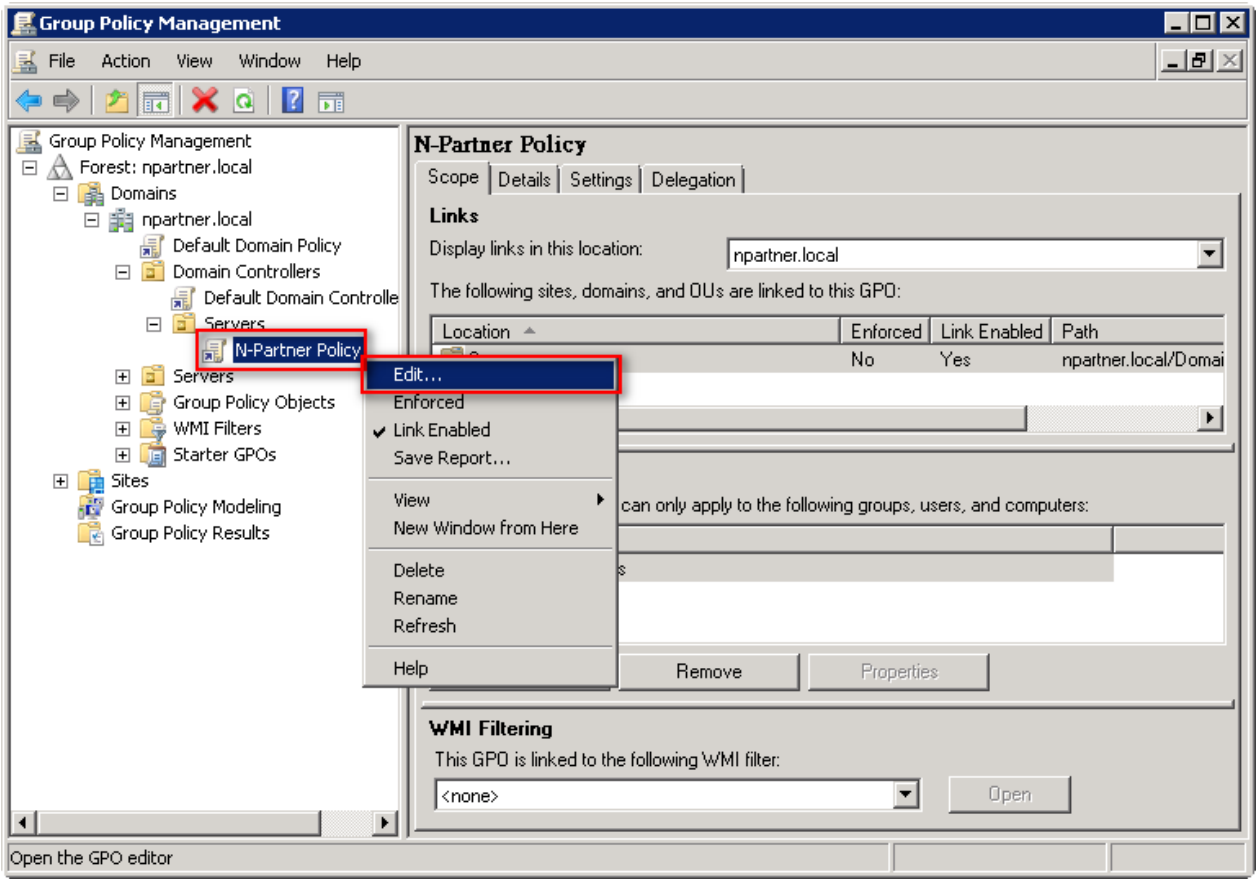
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



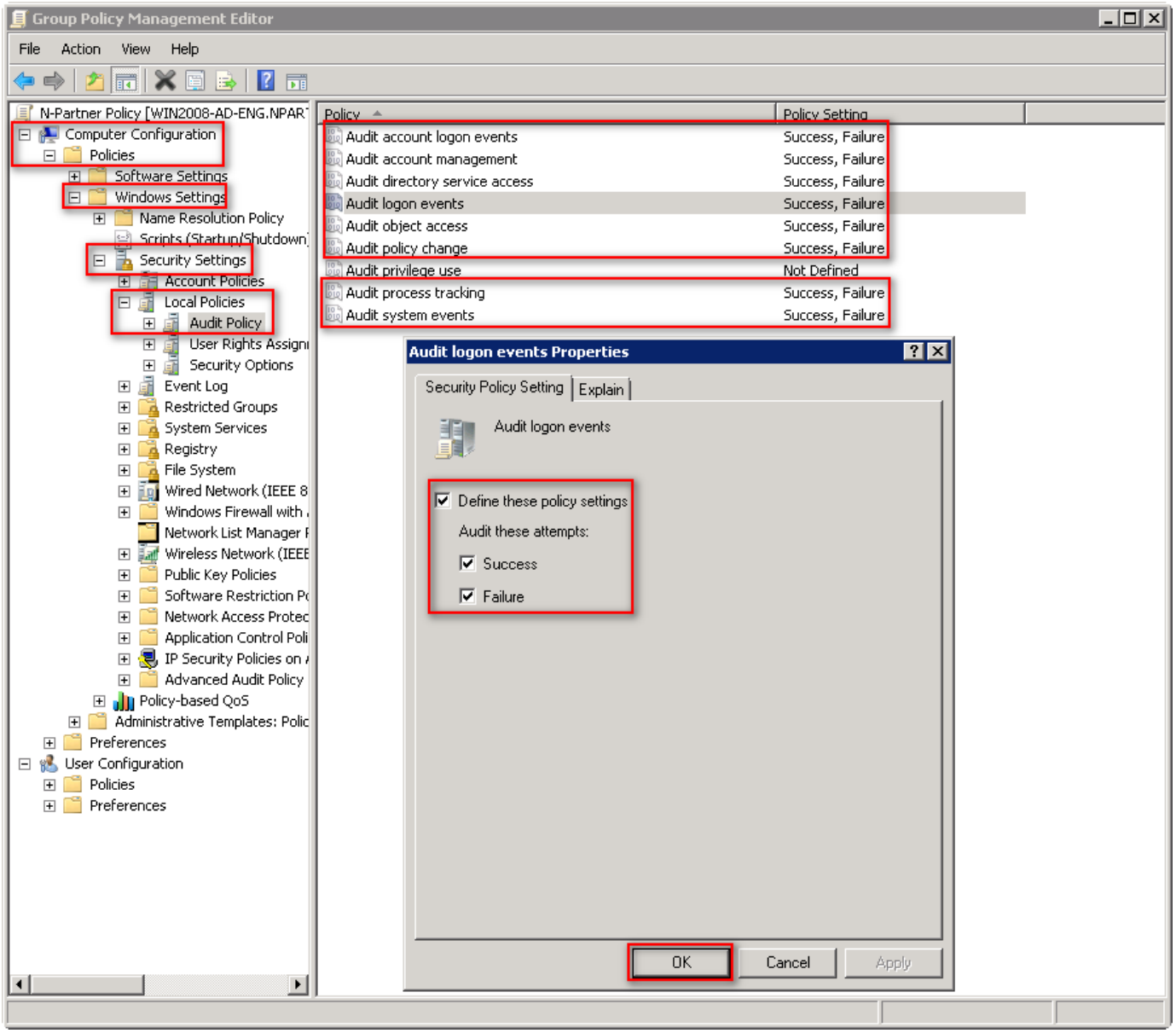
(4) Edit your Group Policy Object

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



(5) Local Group Policies: Audit Policy

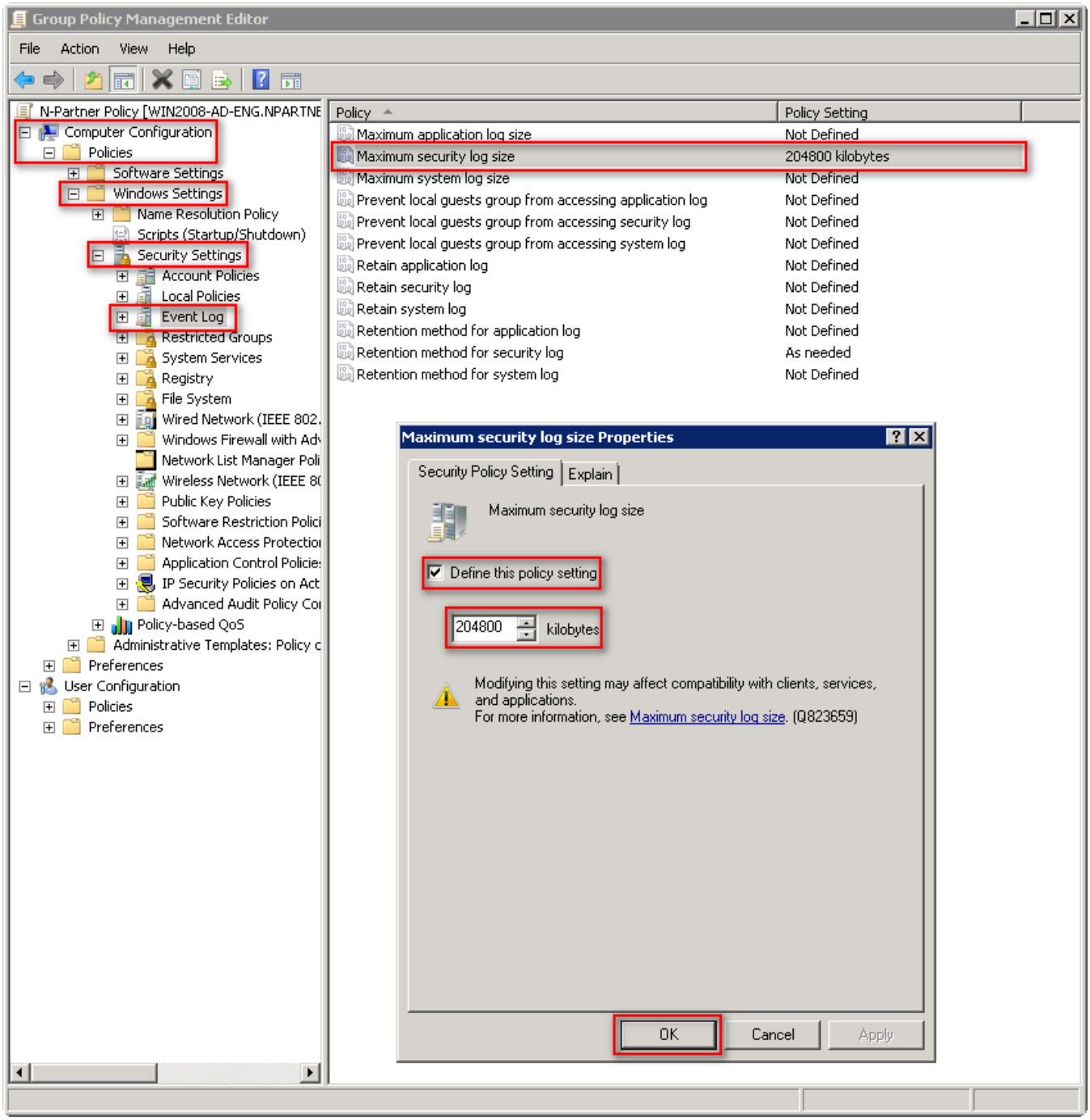
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit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



(6) Event Logs: Maximum Size of Security Log

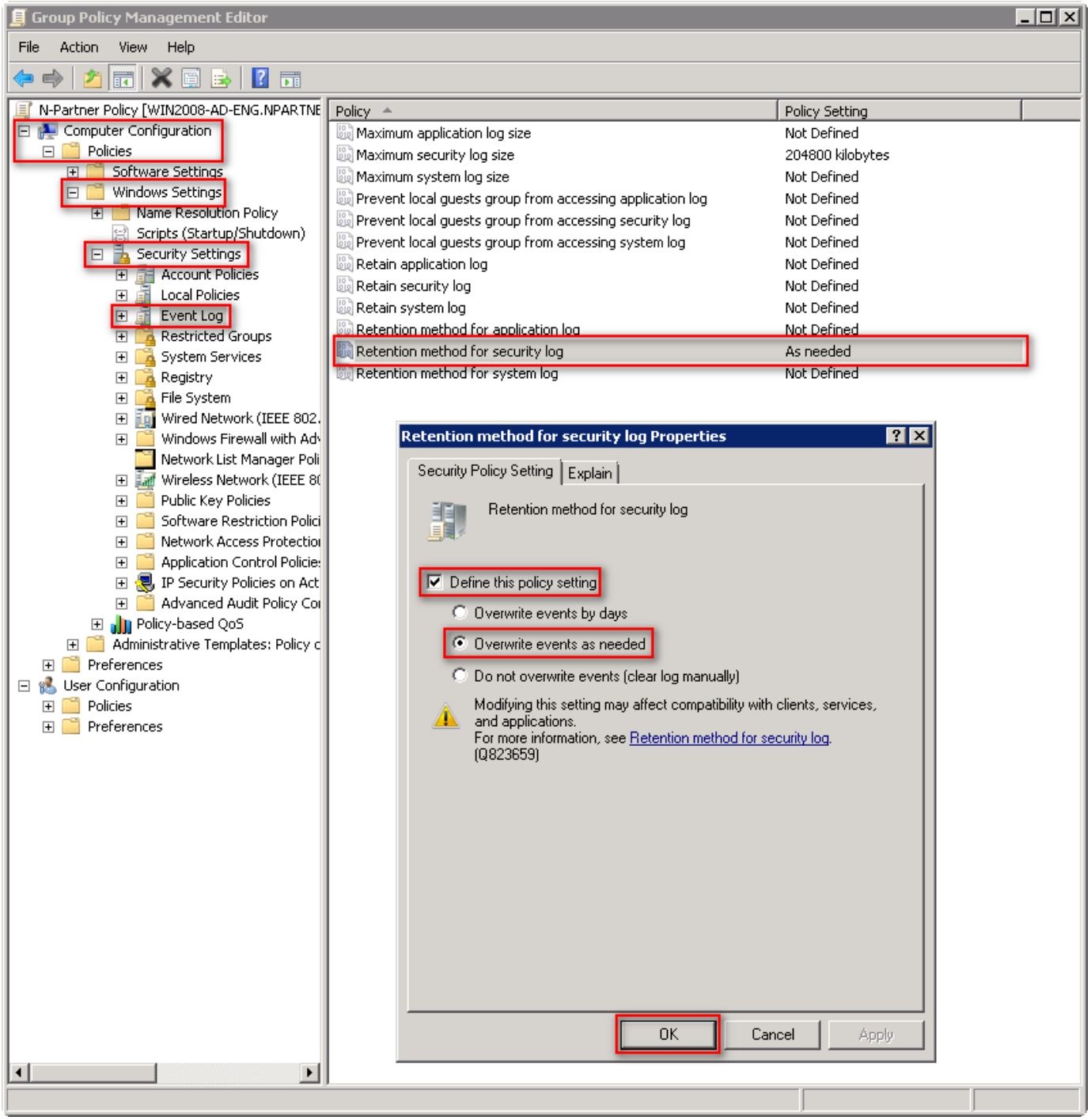
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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



(7) Event Logs: Retention Method for Security Log

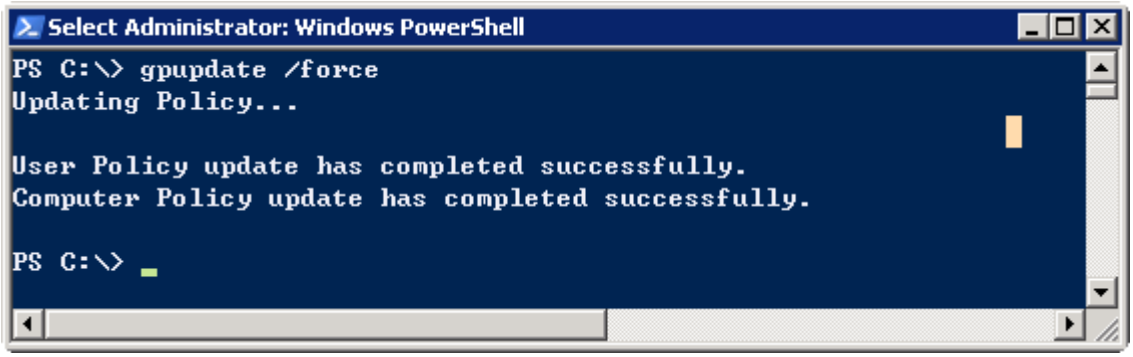
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”



(8) Open “Windows PowerShell.”

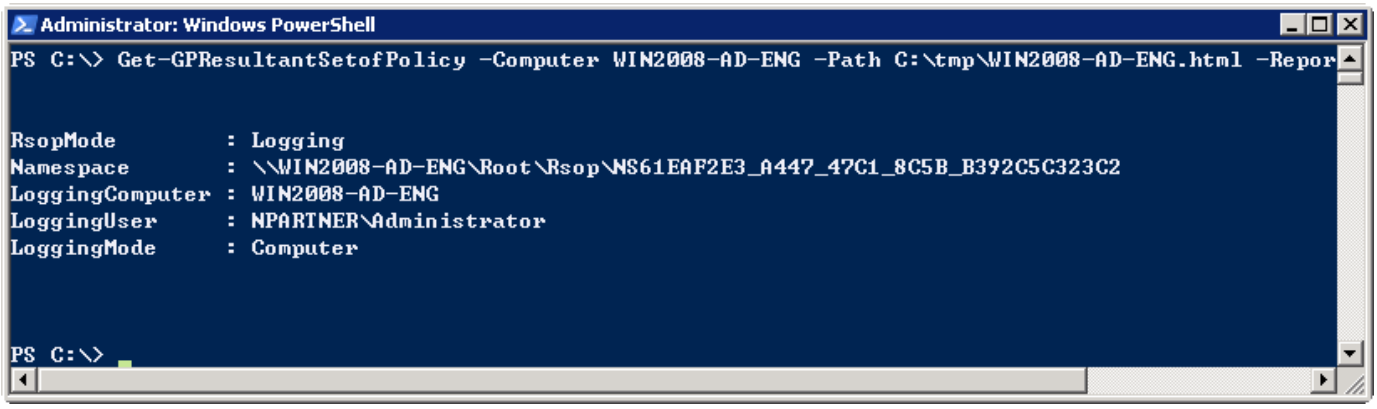
(9) Enter the command below to refresh group policy.

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



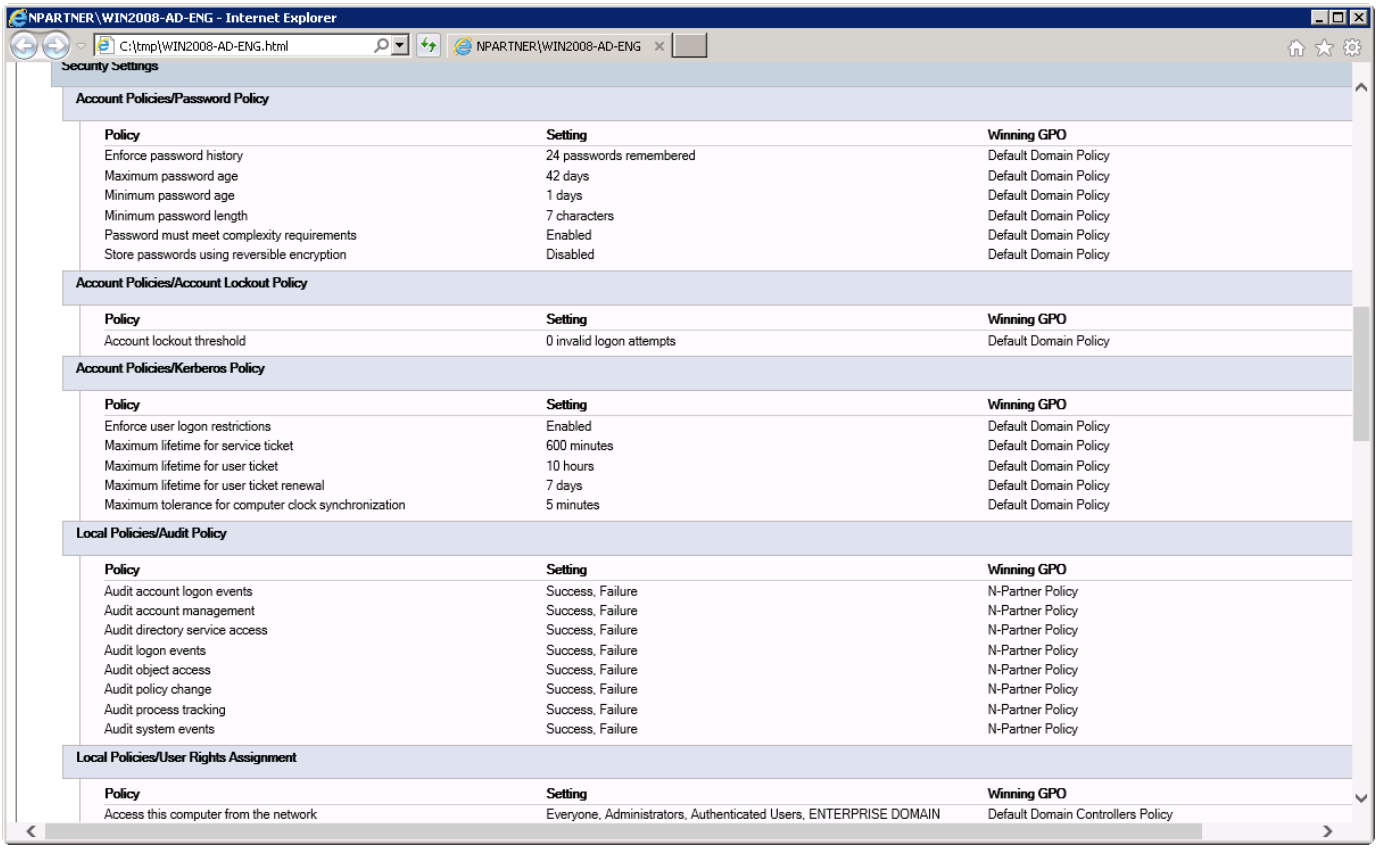
(10) Enter the command below to generate server group policy report.

```
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.



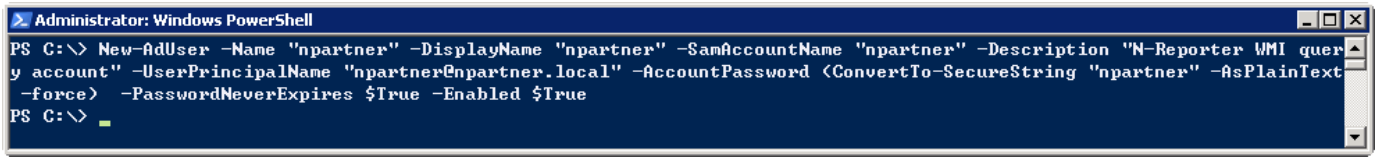
3.3 Add a Non-Admin Account

3.3.1 Add Users

(1) Open “Windows PowerShell.”

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

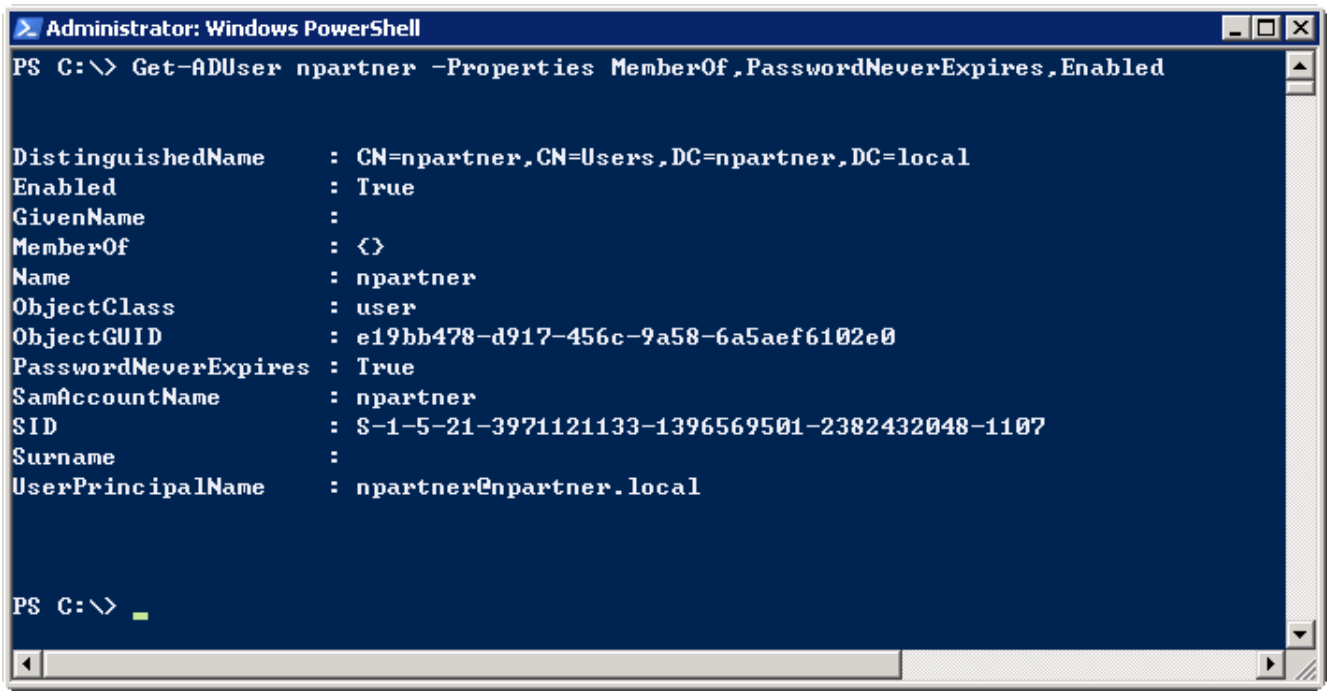
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

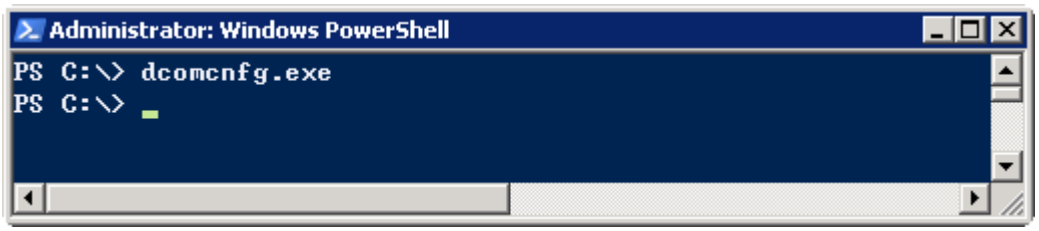


3.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”

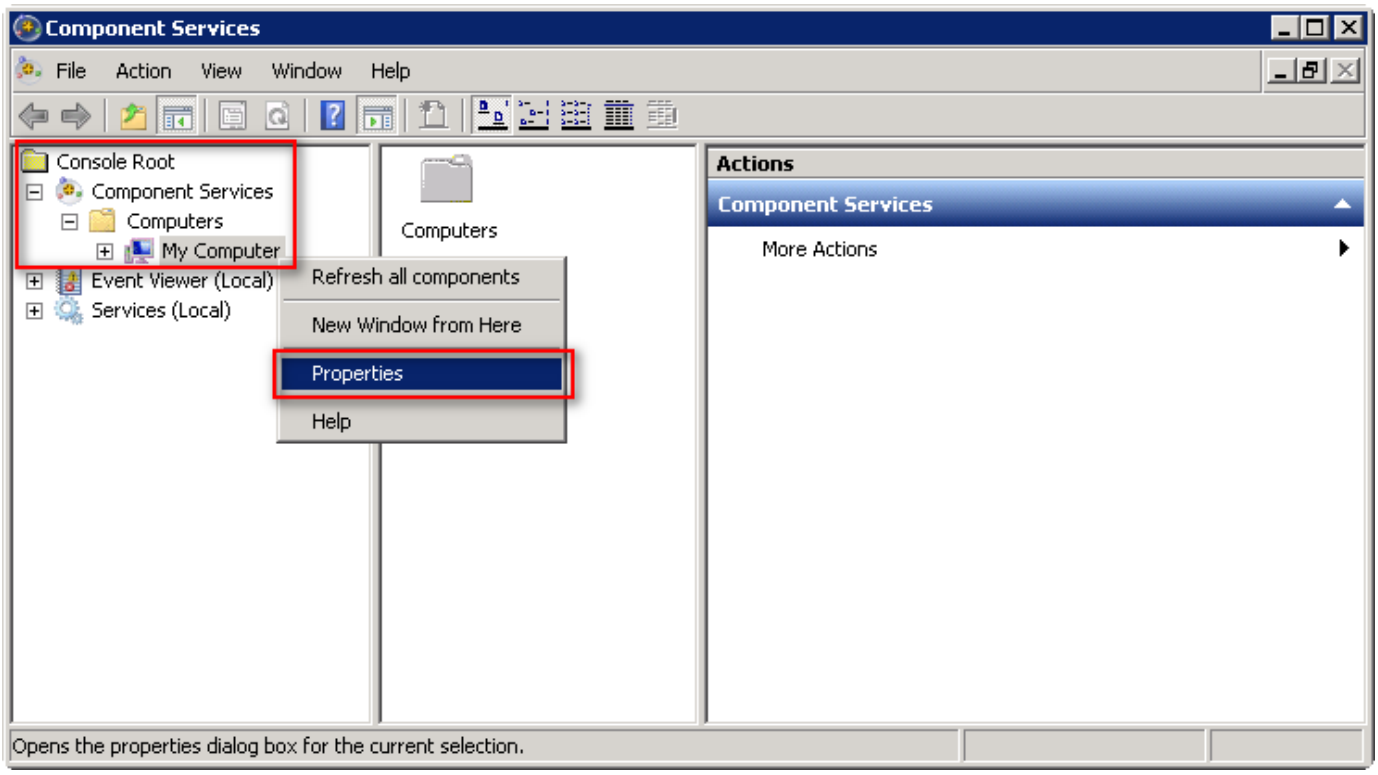
(2) Enter the command below to open component services.

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



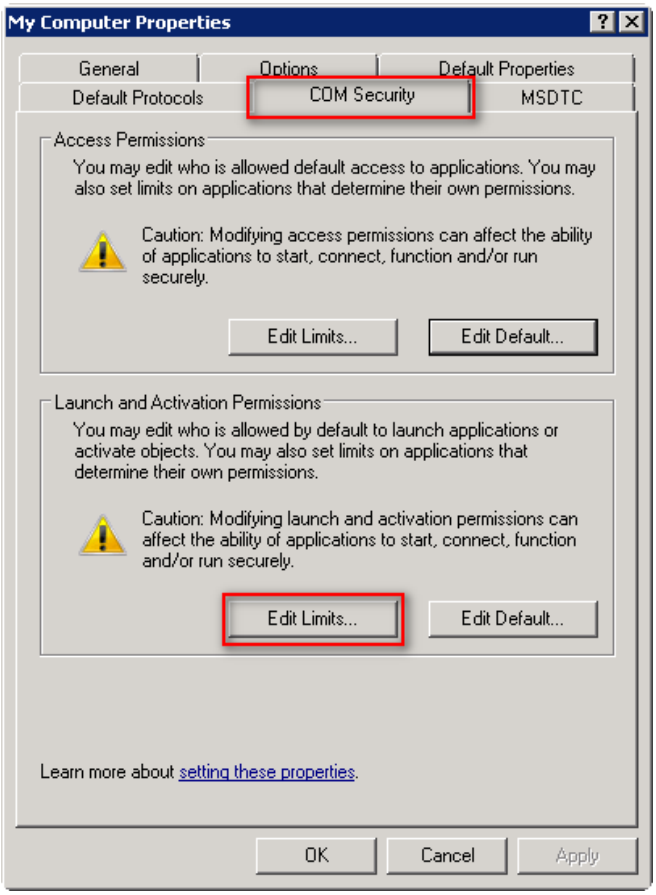
(3) Edit Computer Properties

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



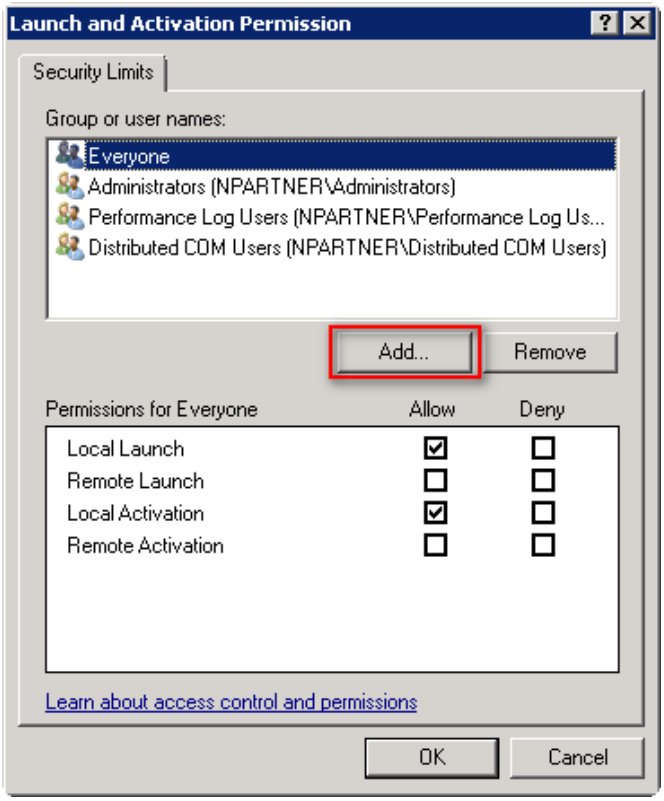
(4) Enable Permissions

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



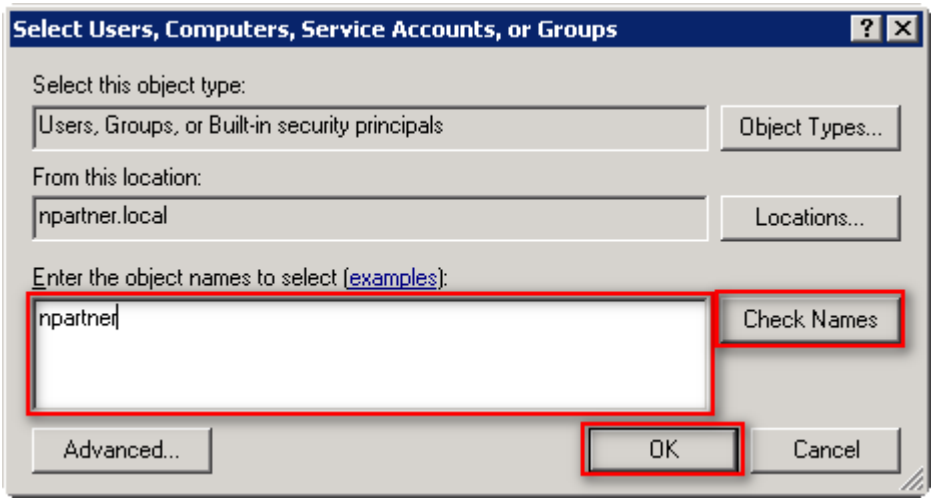
(5) Add DCOM User Permissions

Click “Add.”



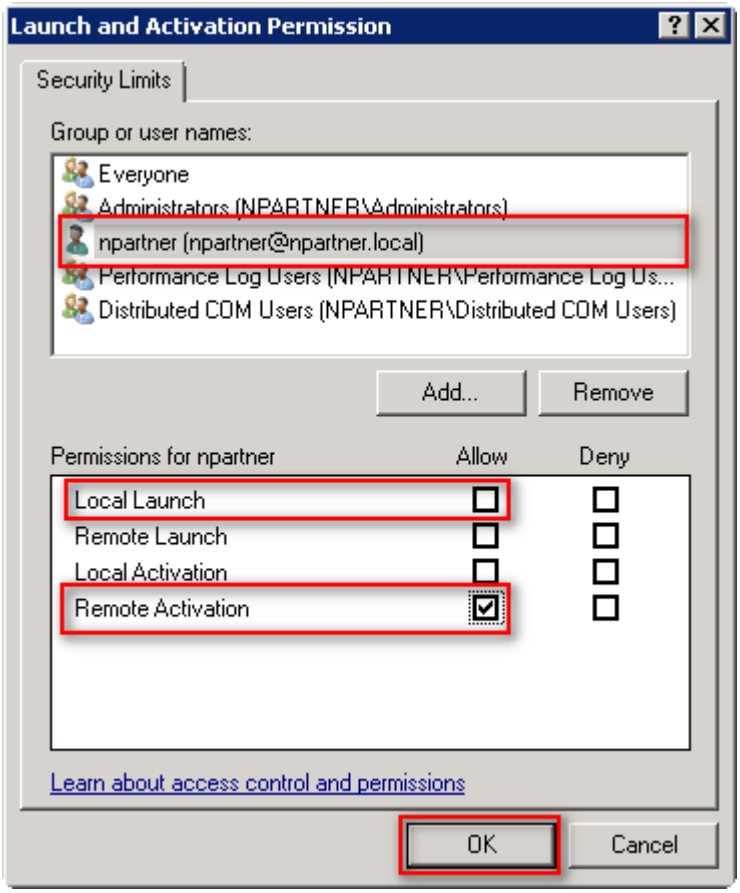
(6) Enter your Username

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

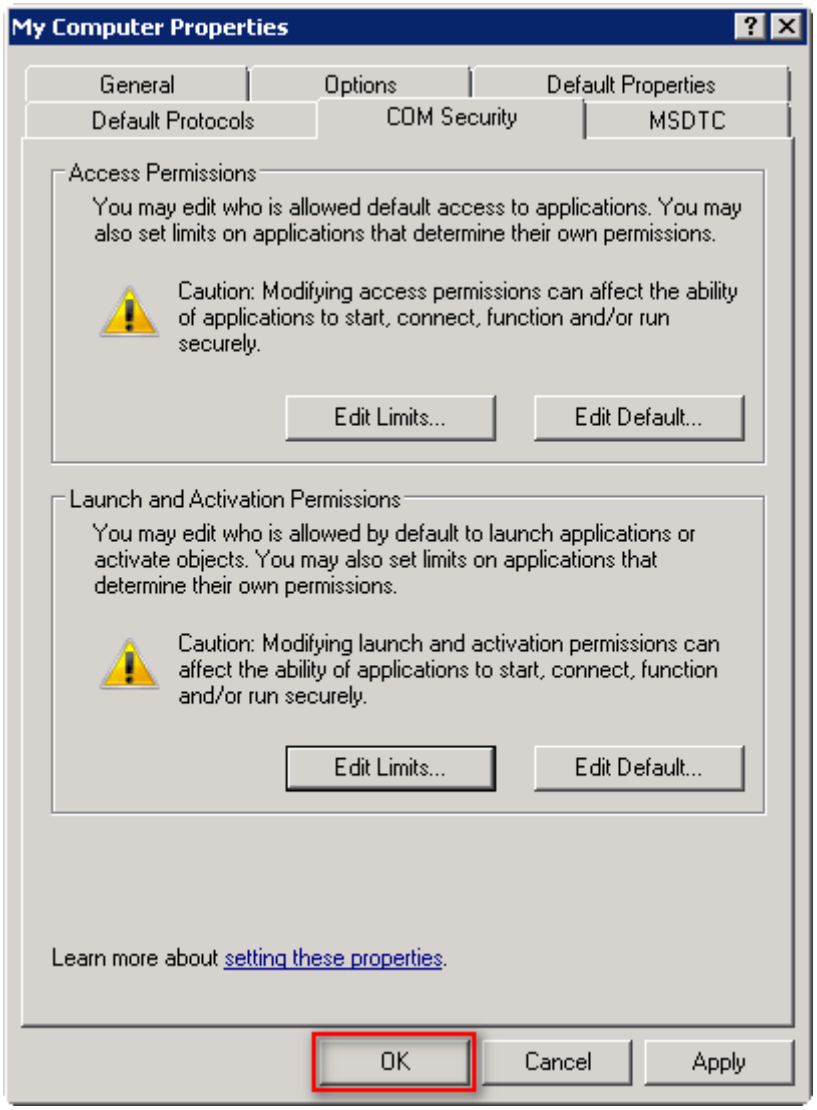


(7) Set User Permissions

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



(8) Click “OK.”



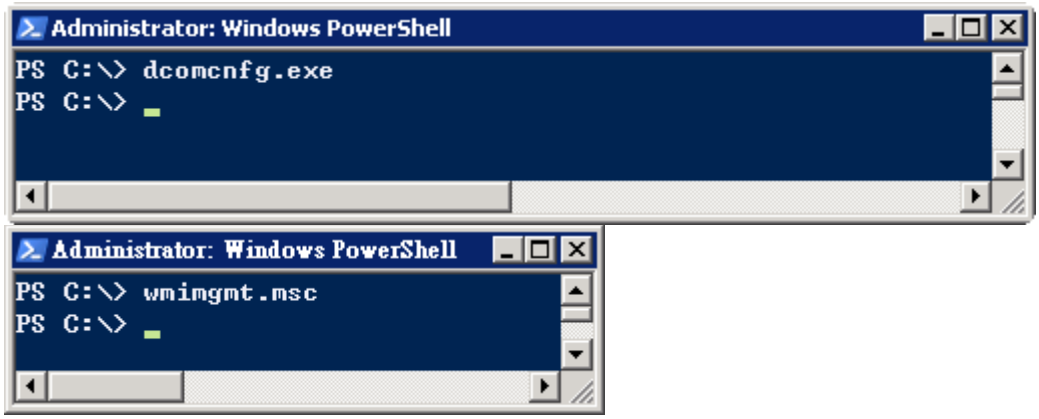
3.3.3 Configure WMI Permissions

3.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”

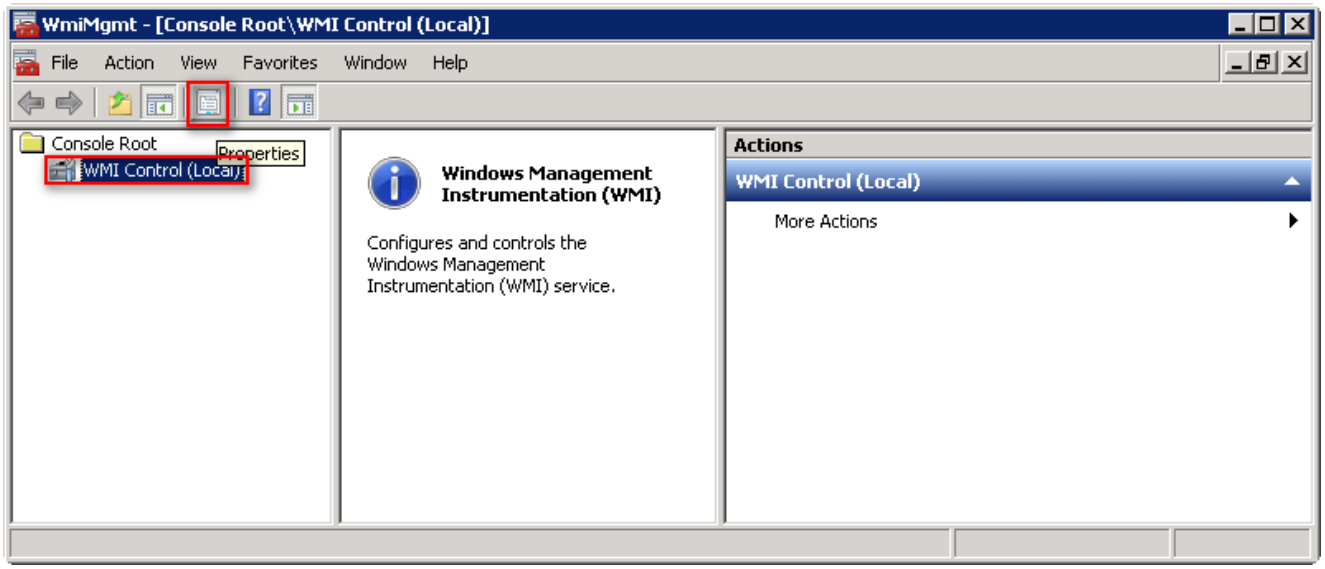
(2) Enter the command below to enable WMI control.

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



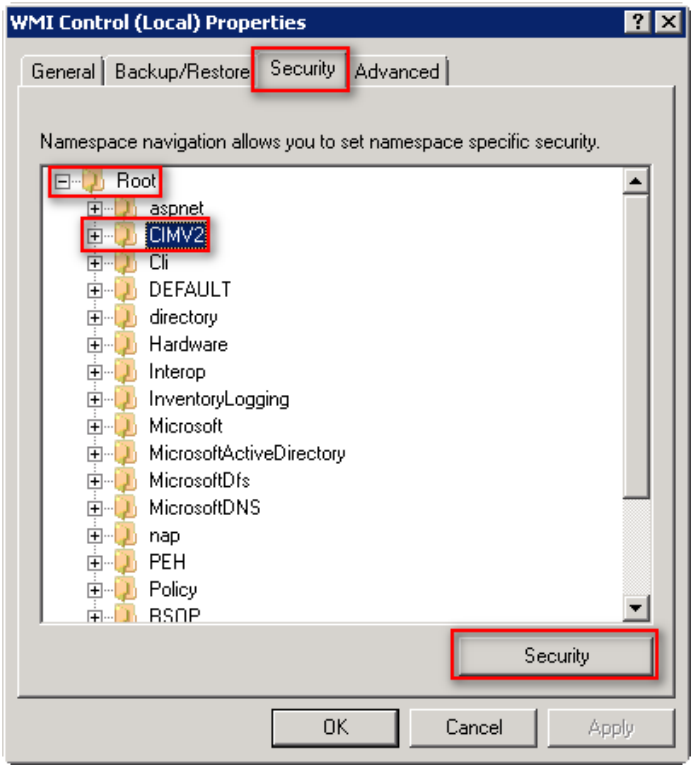
(3) Edit WMI Control

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



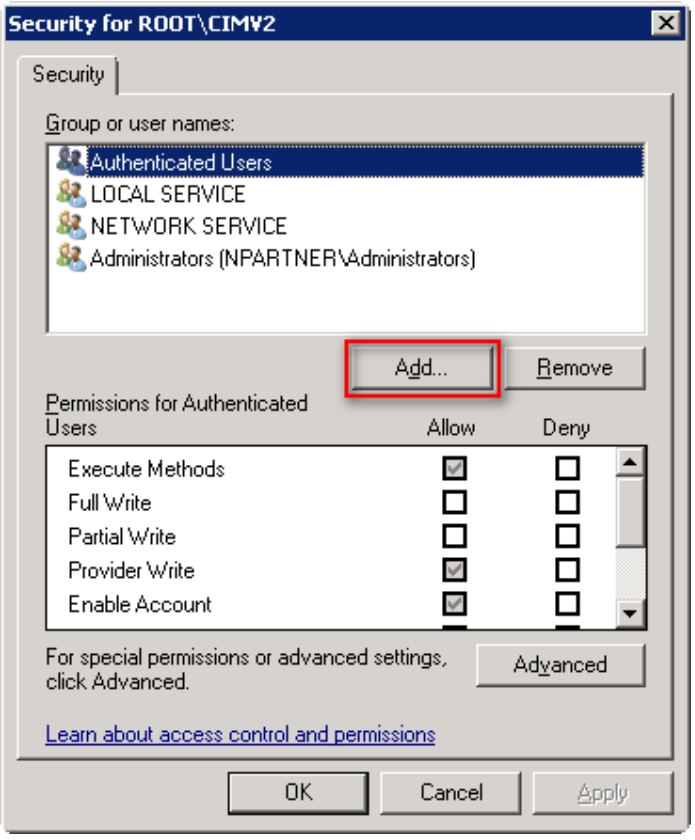
(4) Edit CIMV2 Security

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



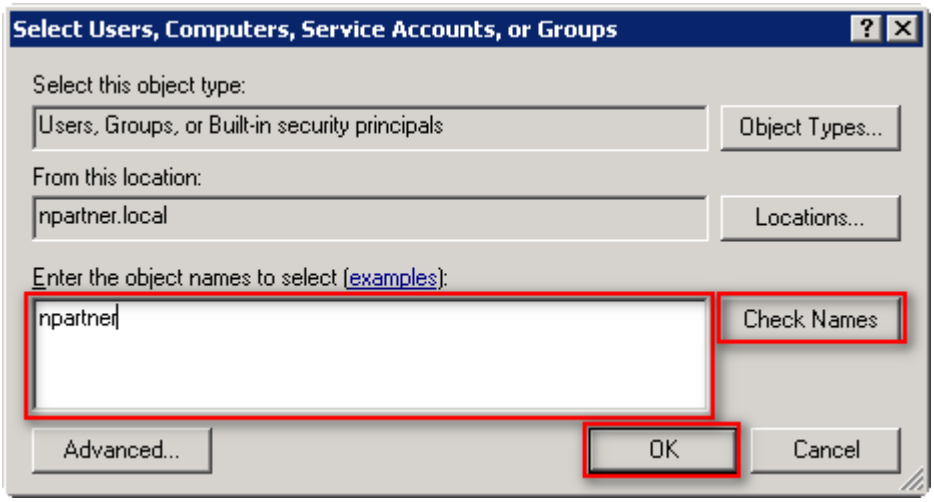
(5) Add WMI User Permissions

Click “Add.”



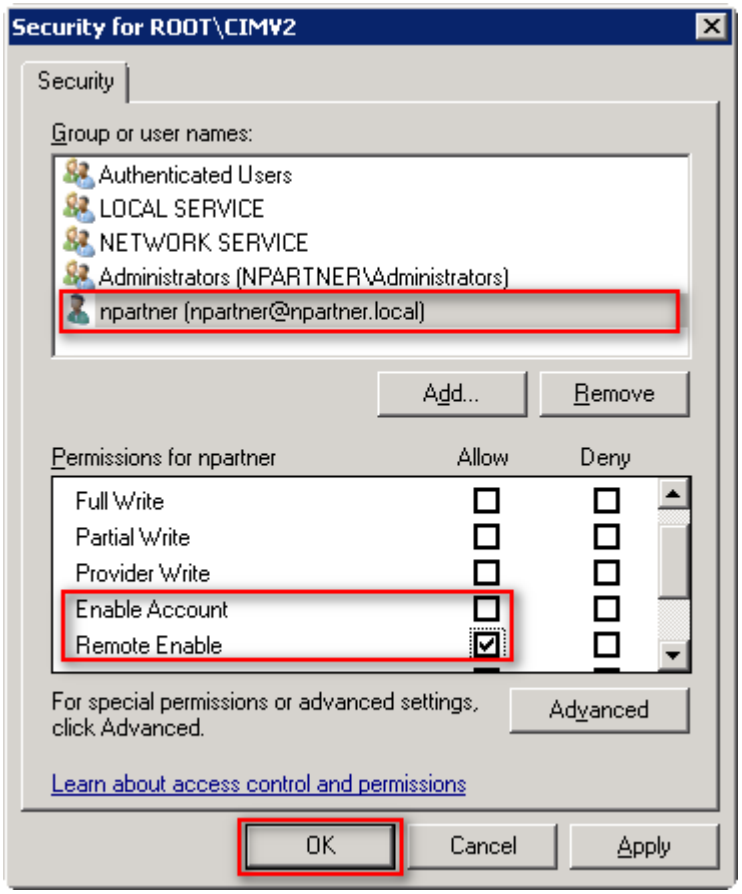
(6) Enter User

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

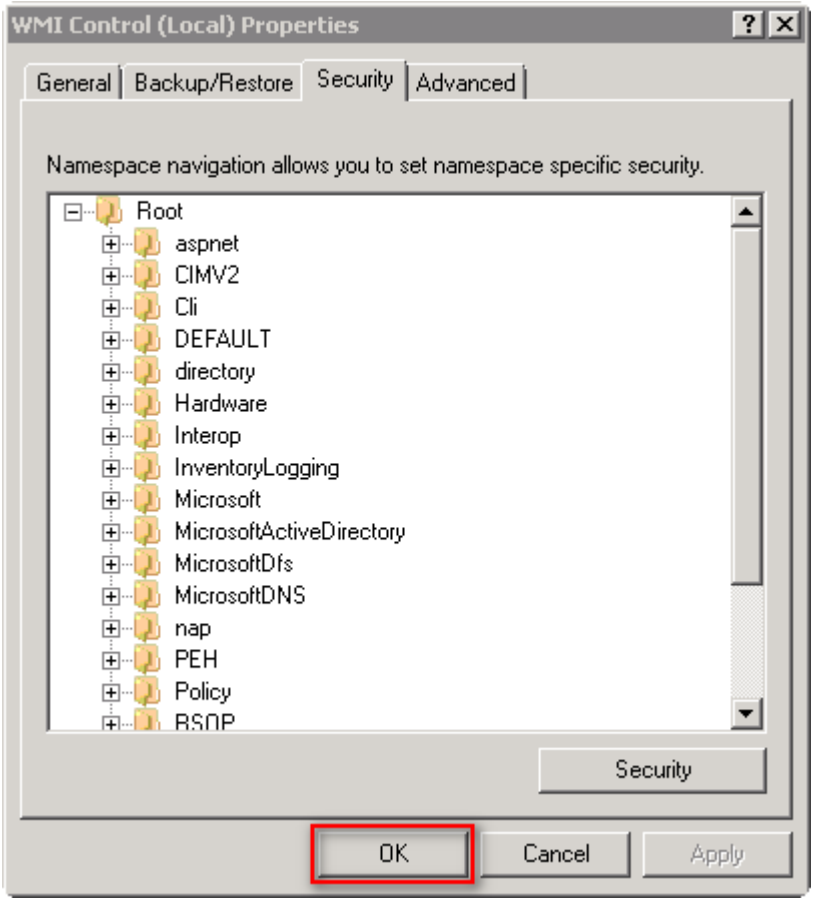


(7) Set User Permissions

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



(8) Click “OK.”

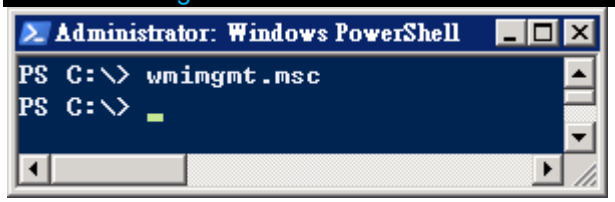


3.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”

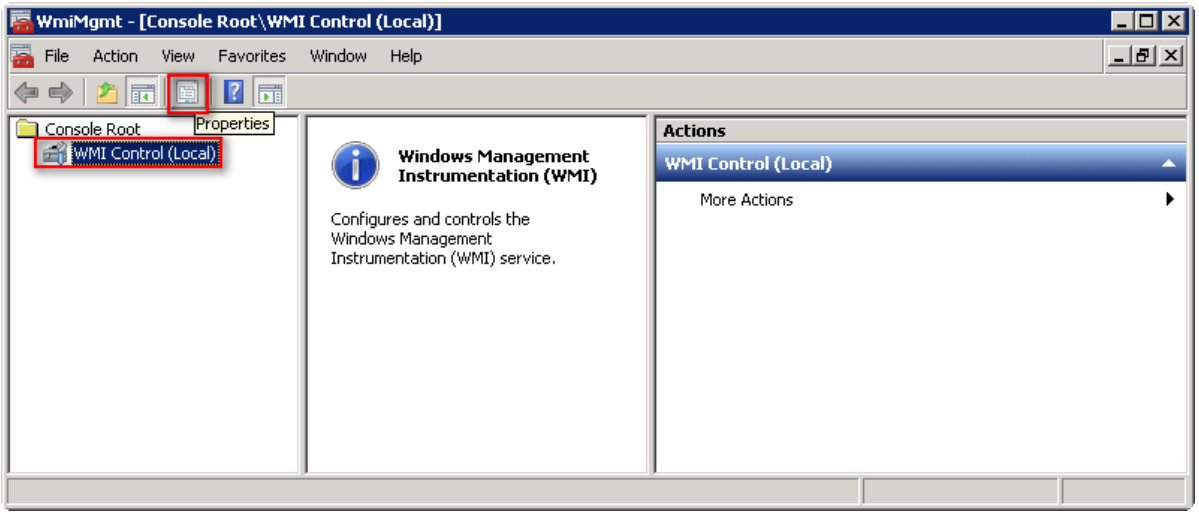
(2) Enter the command below to open component services.

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



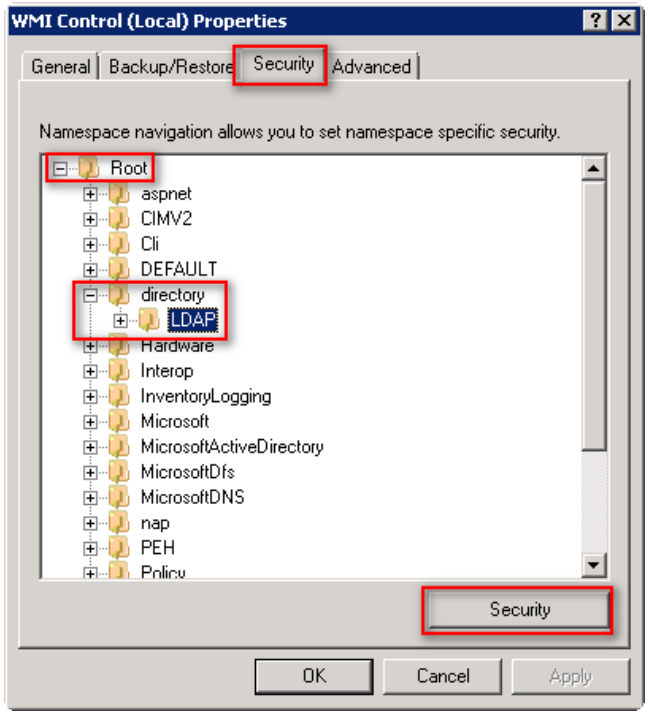
(3) Edit WMI Control

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



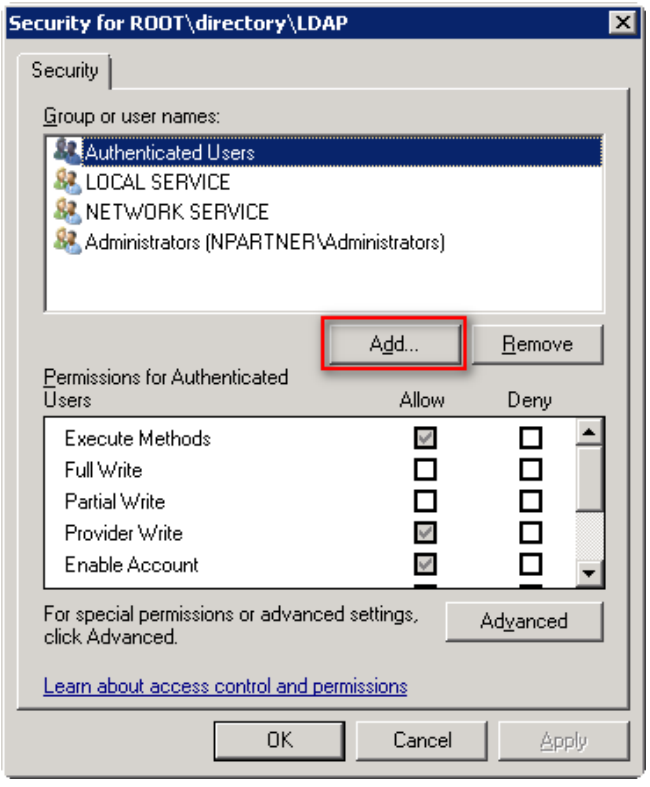
(4) Edit LDAP Security

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



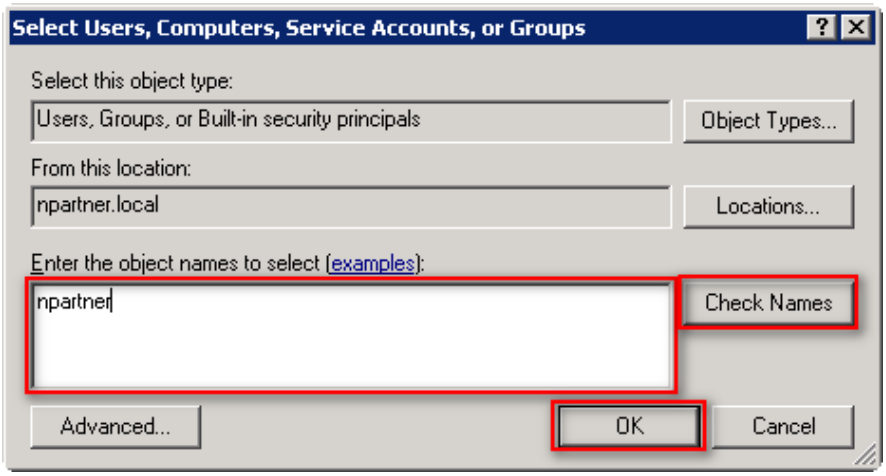
(5) Add WMI User Permissions

Click “Add.”



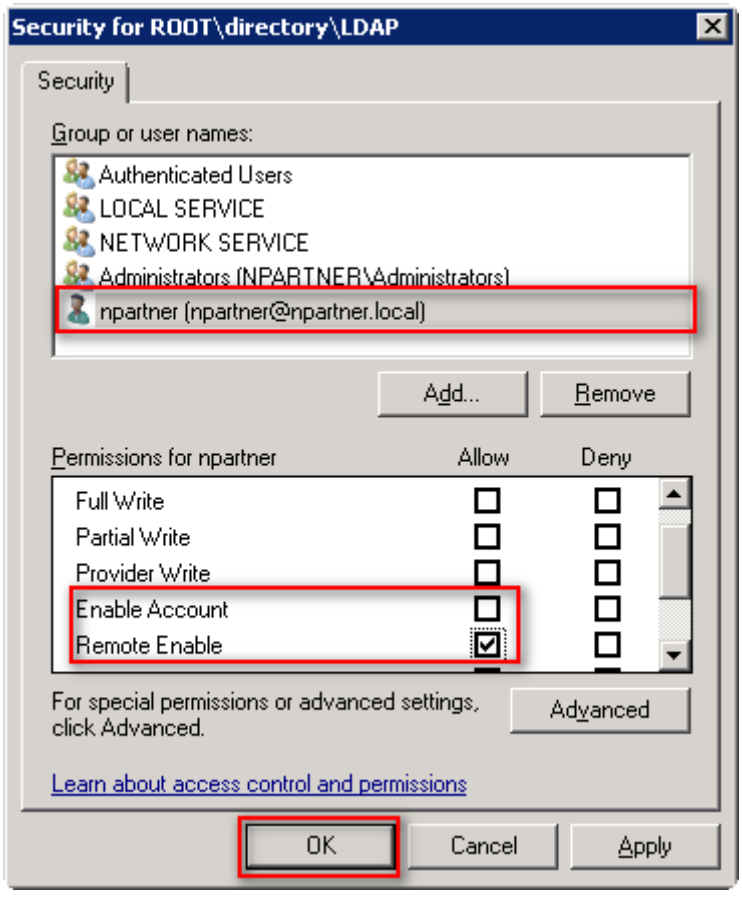
(6) Enter Your Username

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

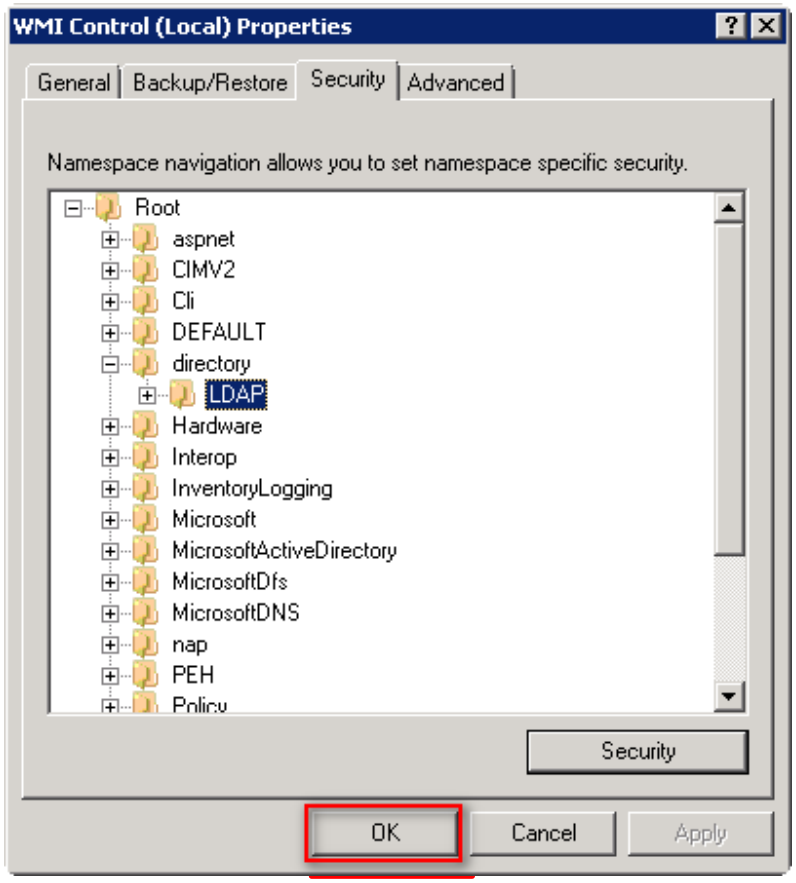


(7) Set Your User Permissions

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



(8) Click “OK.”

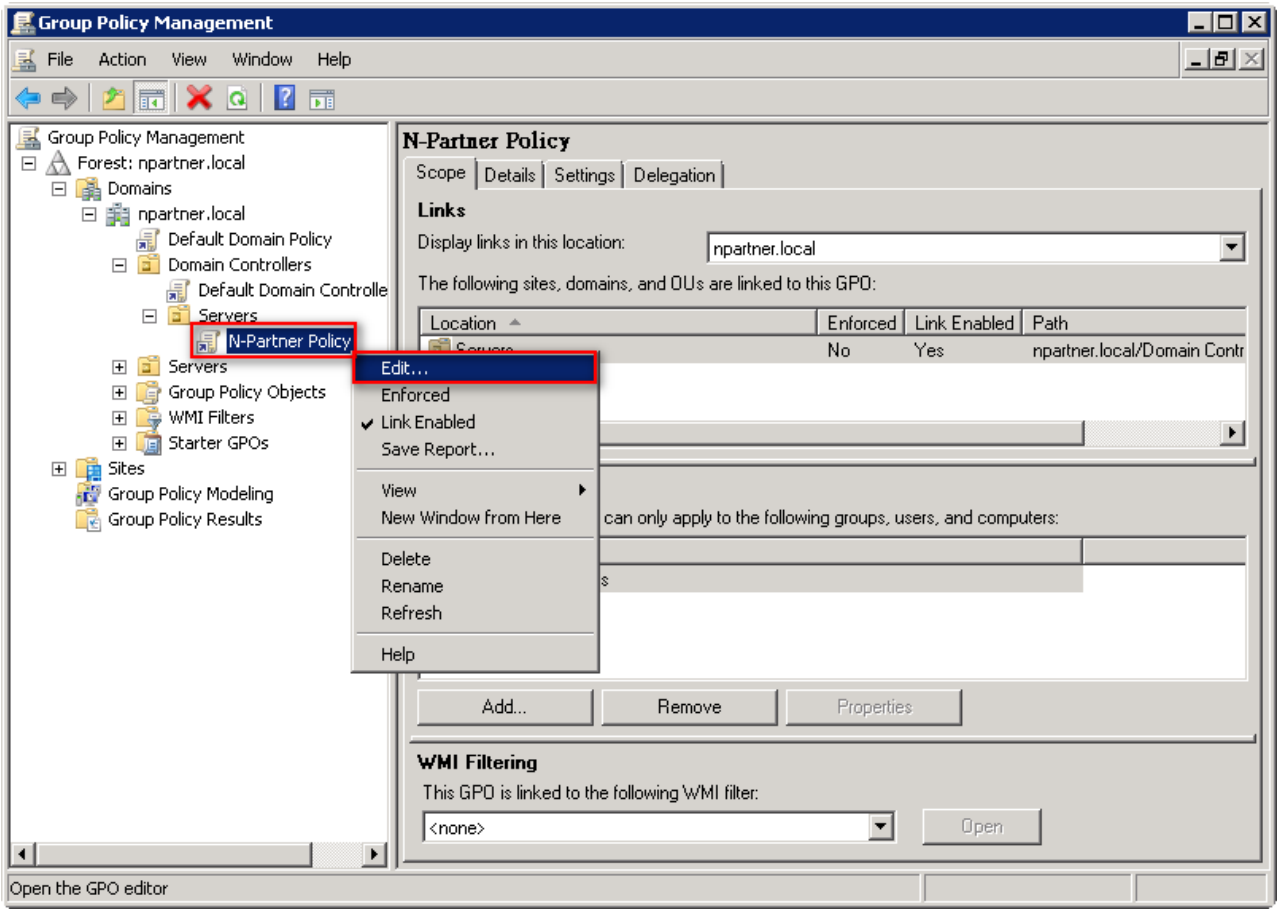


3.3.4 Configure Event Log read permissions

(1) Open Group Policy Management

(2) Edit the Group Policy Object

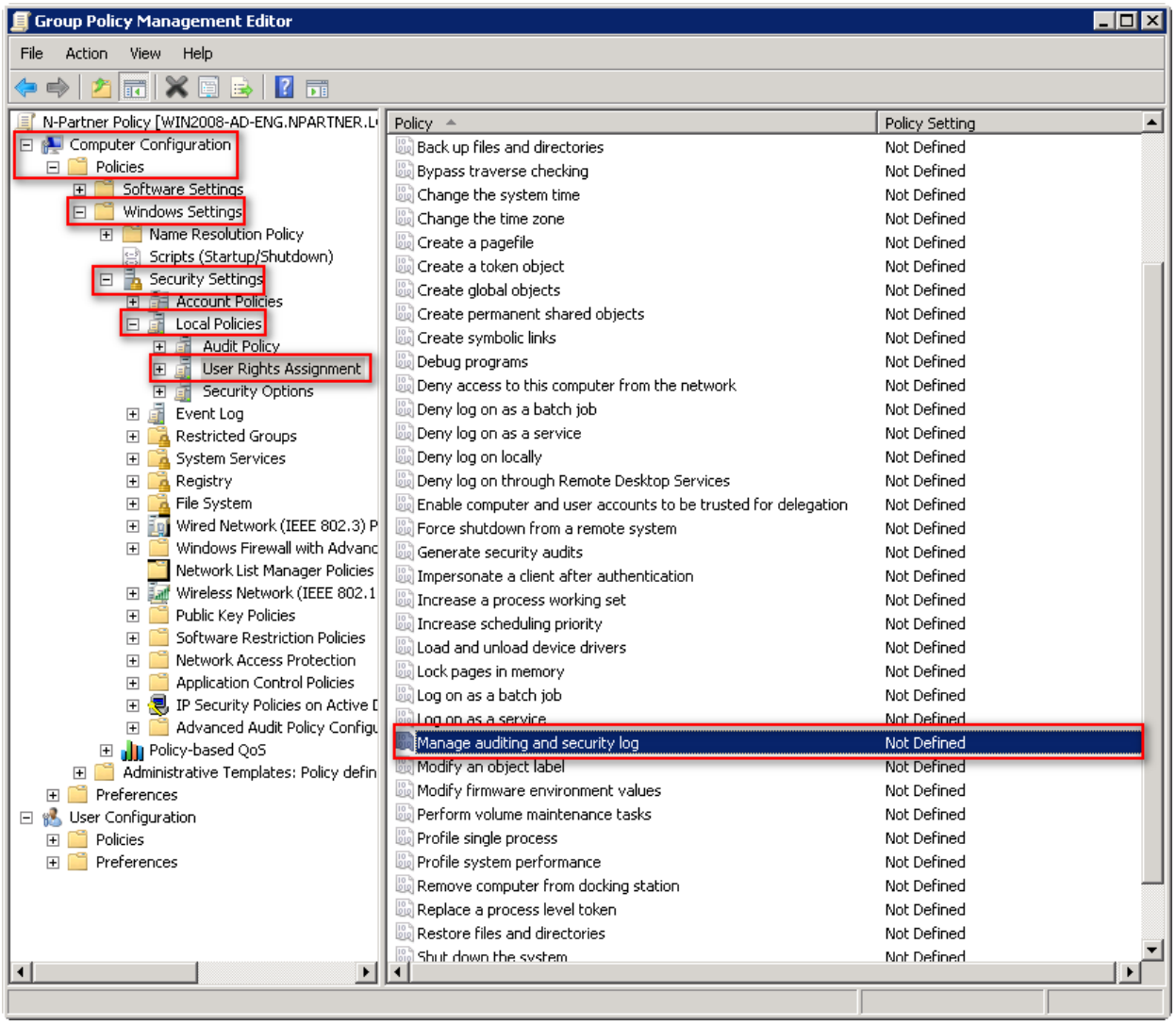
In the “N-Partner Policy” Group Policy Object, right-click and select “Edit.”



(3) Configure Log Settings

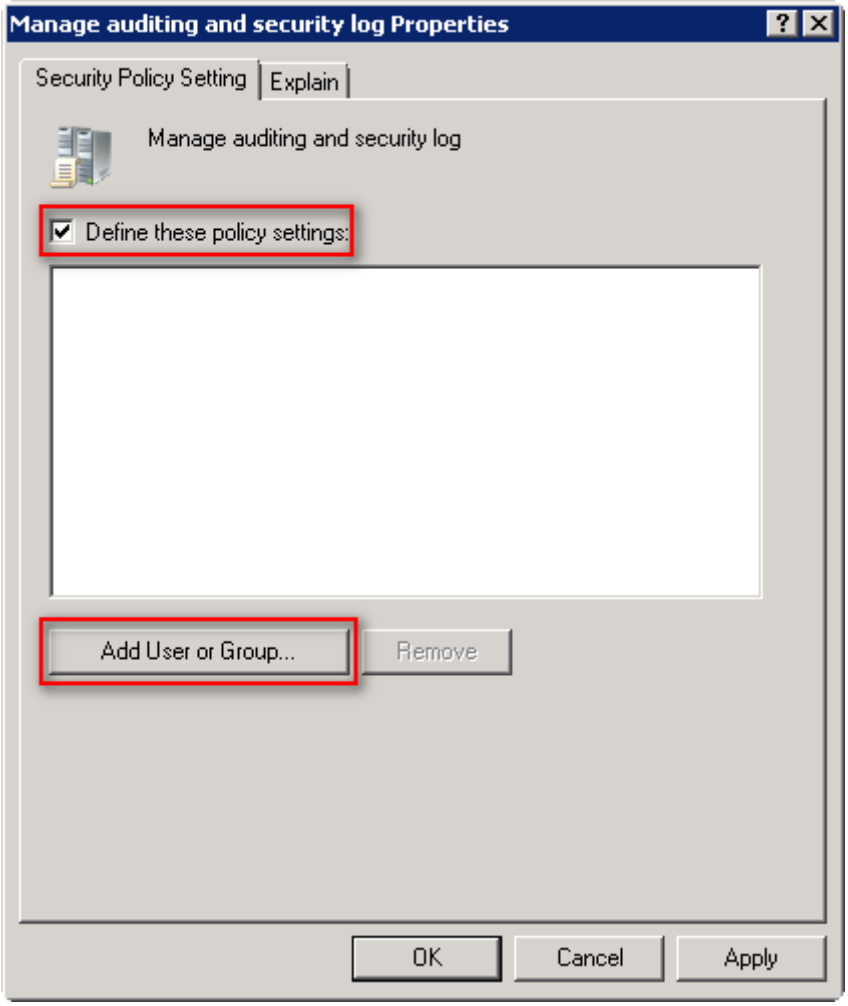
Click “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

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



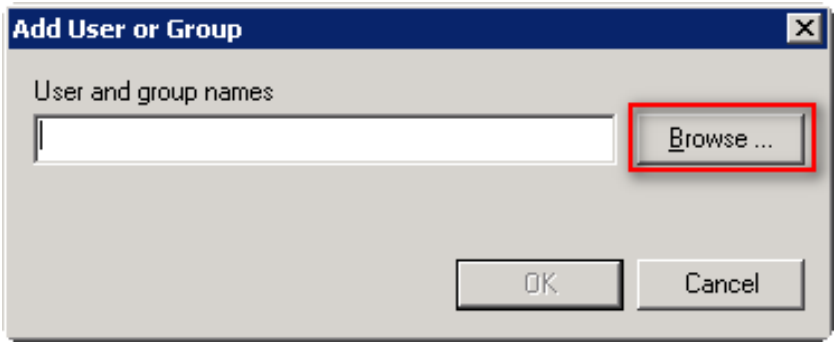
(4) Add Audit Management User

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



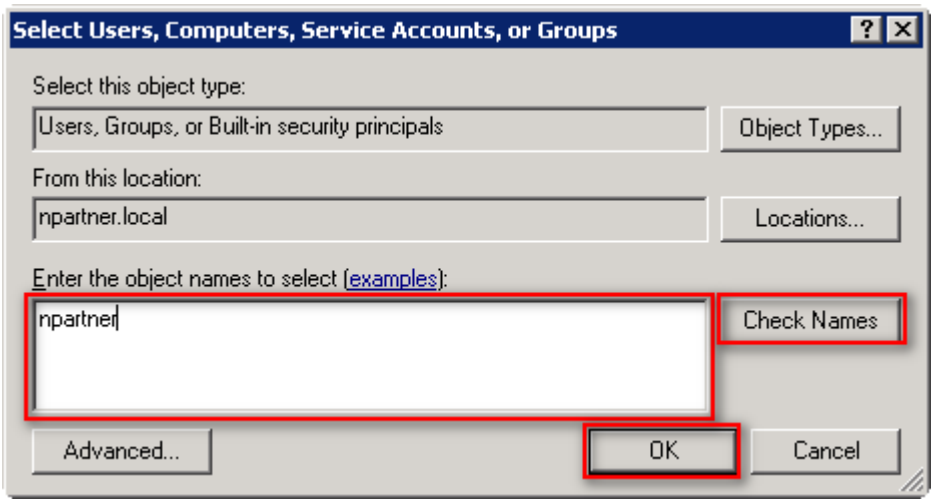
(5) Search for User

Click “Browse.”



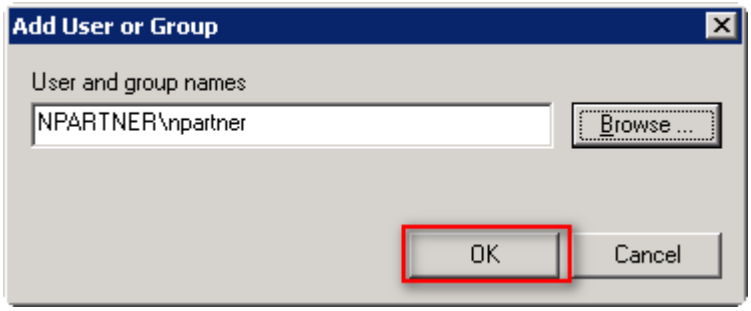
(6) Enter User

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



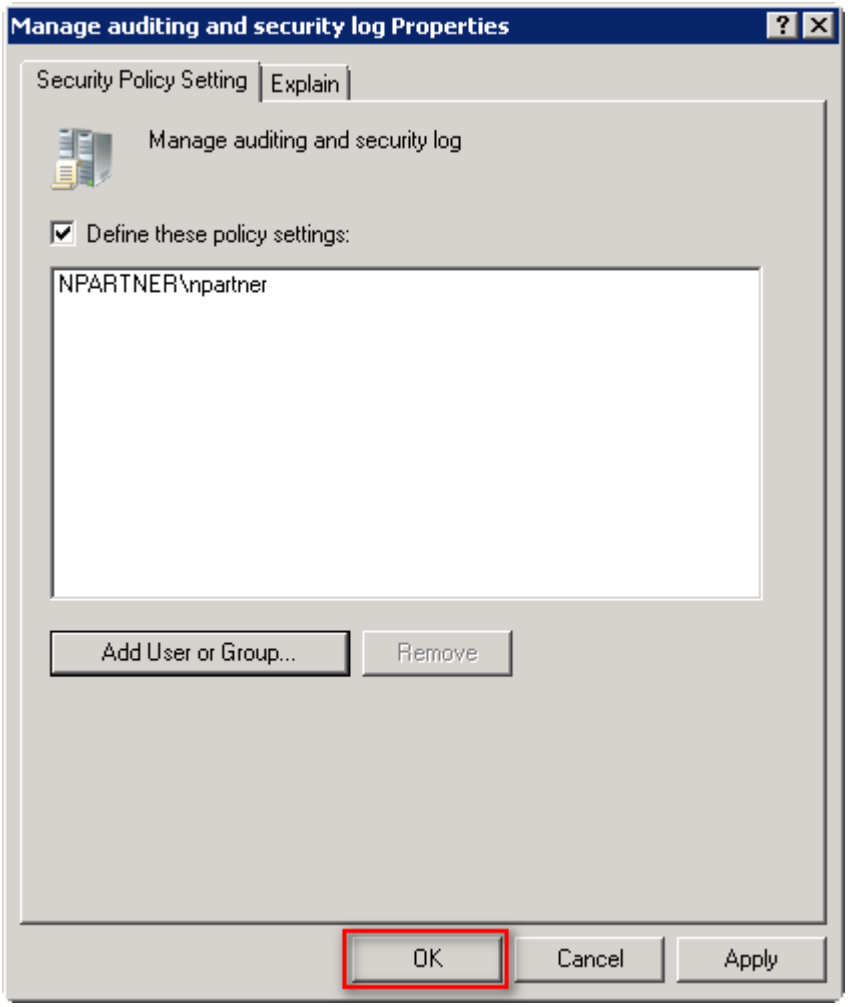
(7) Confirm User

Click “OK.”



(8) Confirm Log Settings

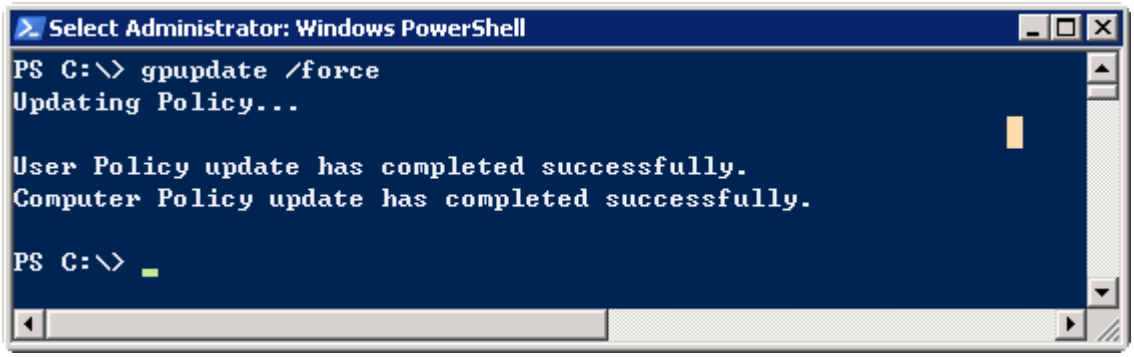
Click “OK.”



(9) Open “Windows PowerShell.”

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

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



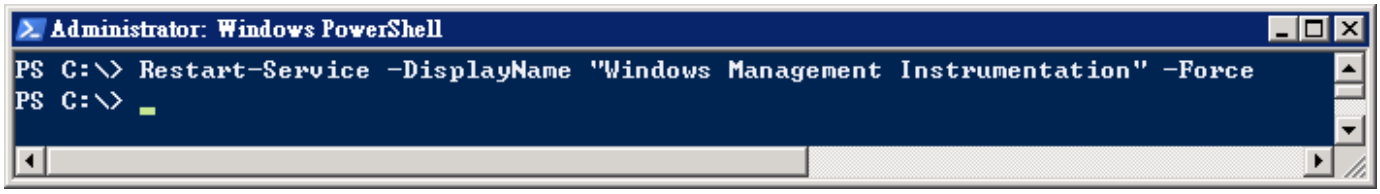
3.3.5 Restart WMI Service

(1) Click “Windows PowerShell.”

(2) Restart WMI Service

Run the following command to restart the WMI service:

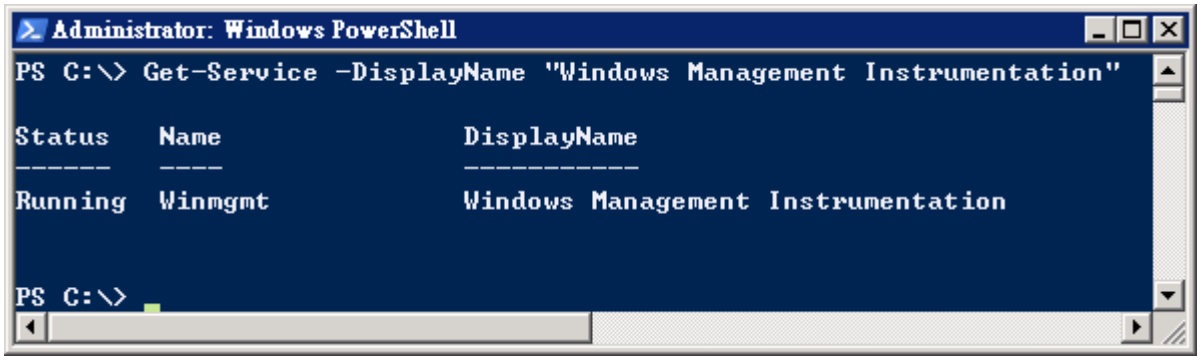
```
PS C:\> Restart-Service -DisplayName "Windows Management Instrumentation" -Force
```



(3) Check WMI Service Status

Verify the status of the WMI service:

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



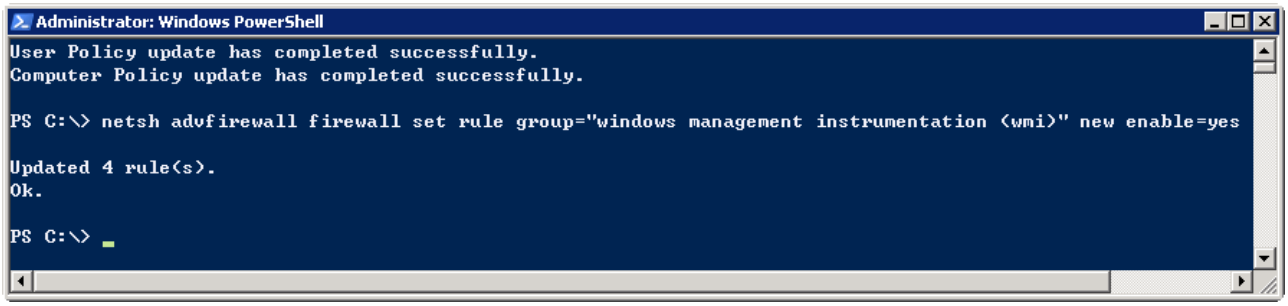
3.4 Configure Firewall

(1) Open “Windows PowerShell.”

(2) Allow WMI Through the Firewall

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

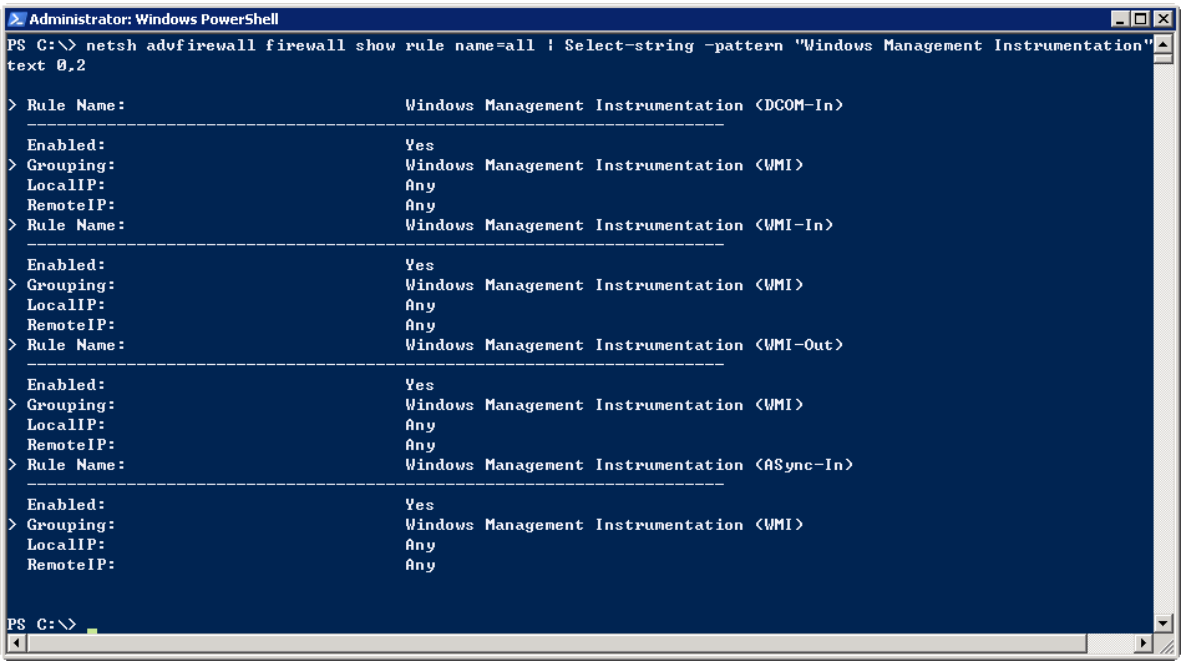
```
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```



(3) Check WMI Firewall Rule Status

View the current WMI firewall rule status:

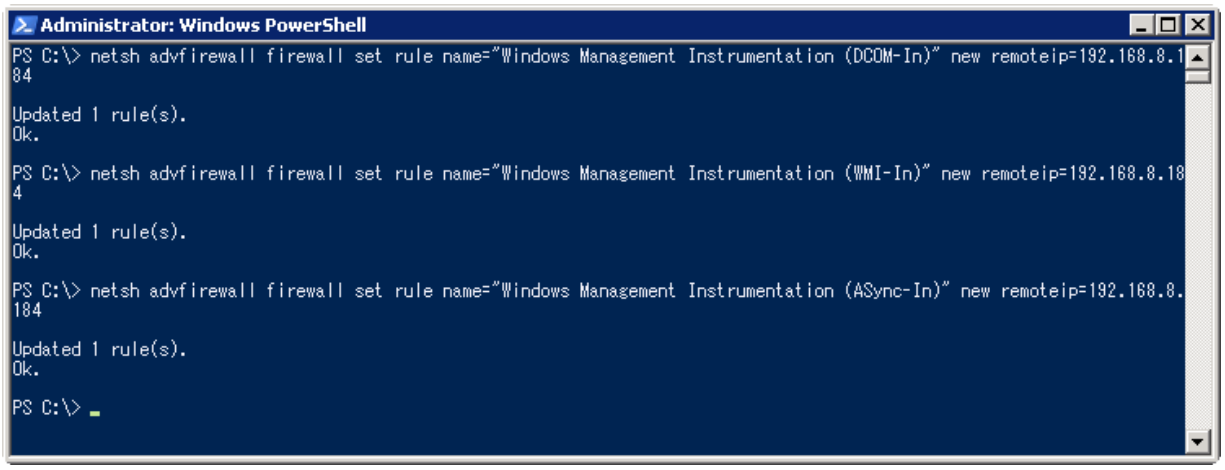
```
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
```



(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
```

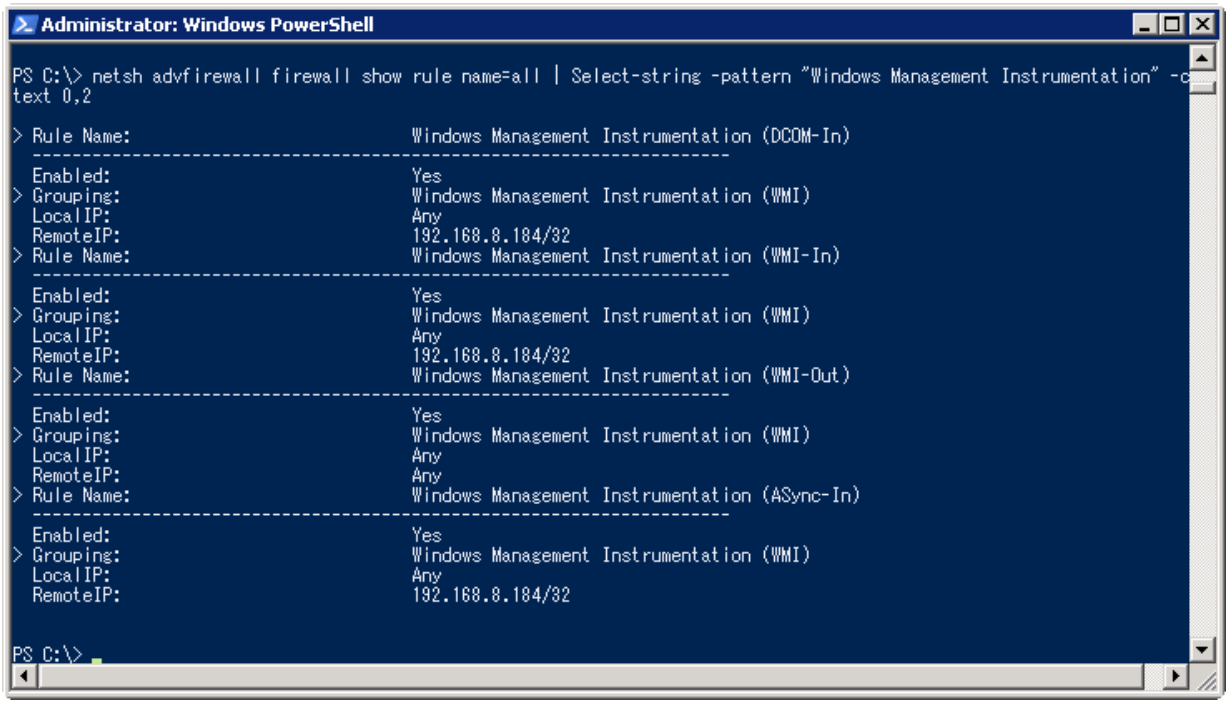


Note: Replace the IP address in red text with the N-Reporter IP address.

(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
```

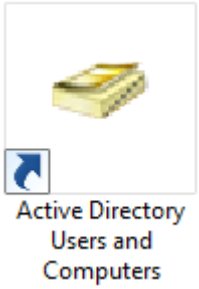


4. Windows 2012

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

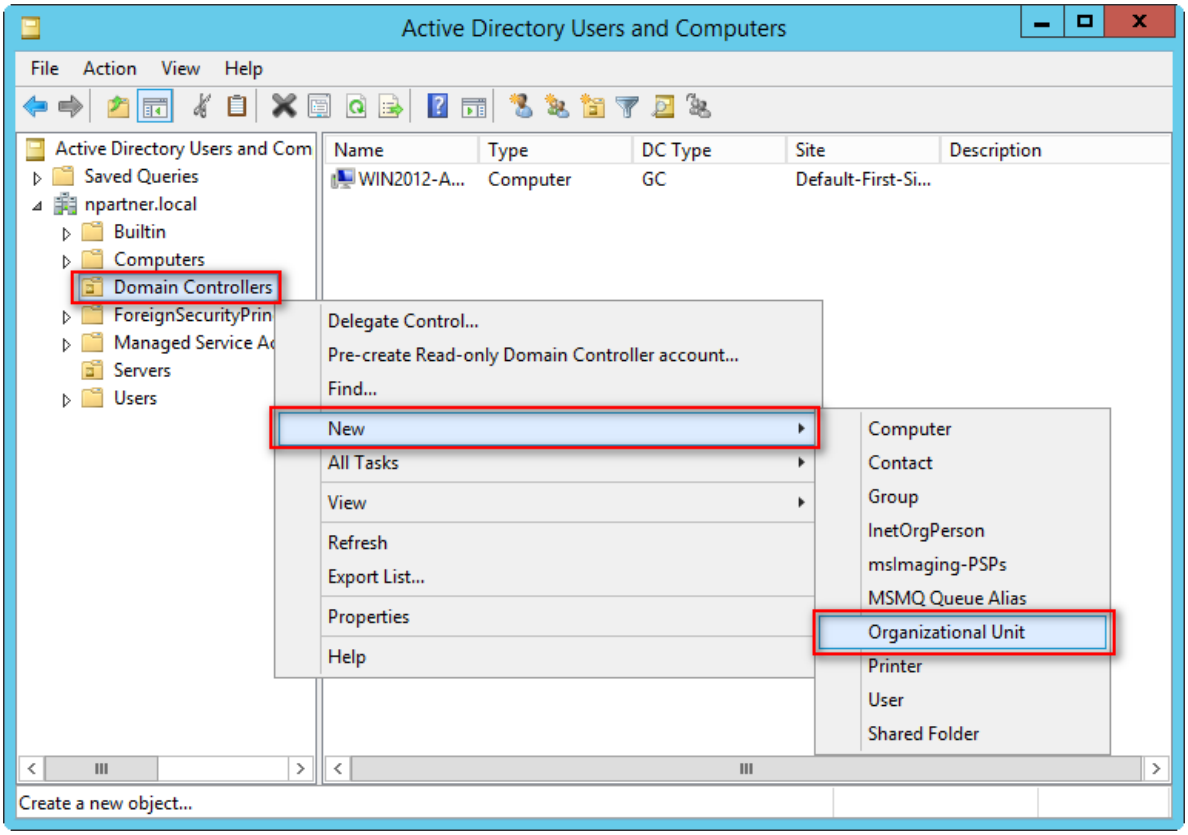
4.1 Organizational Unit Settings

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



(2) Add an Organizational Unit

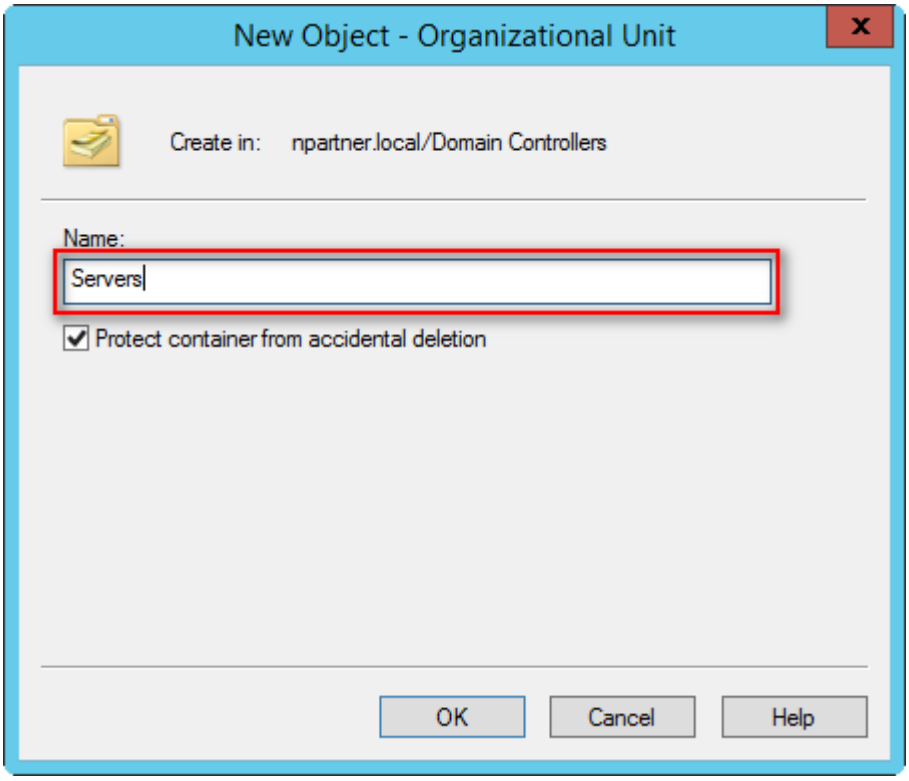
Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



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

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

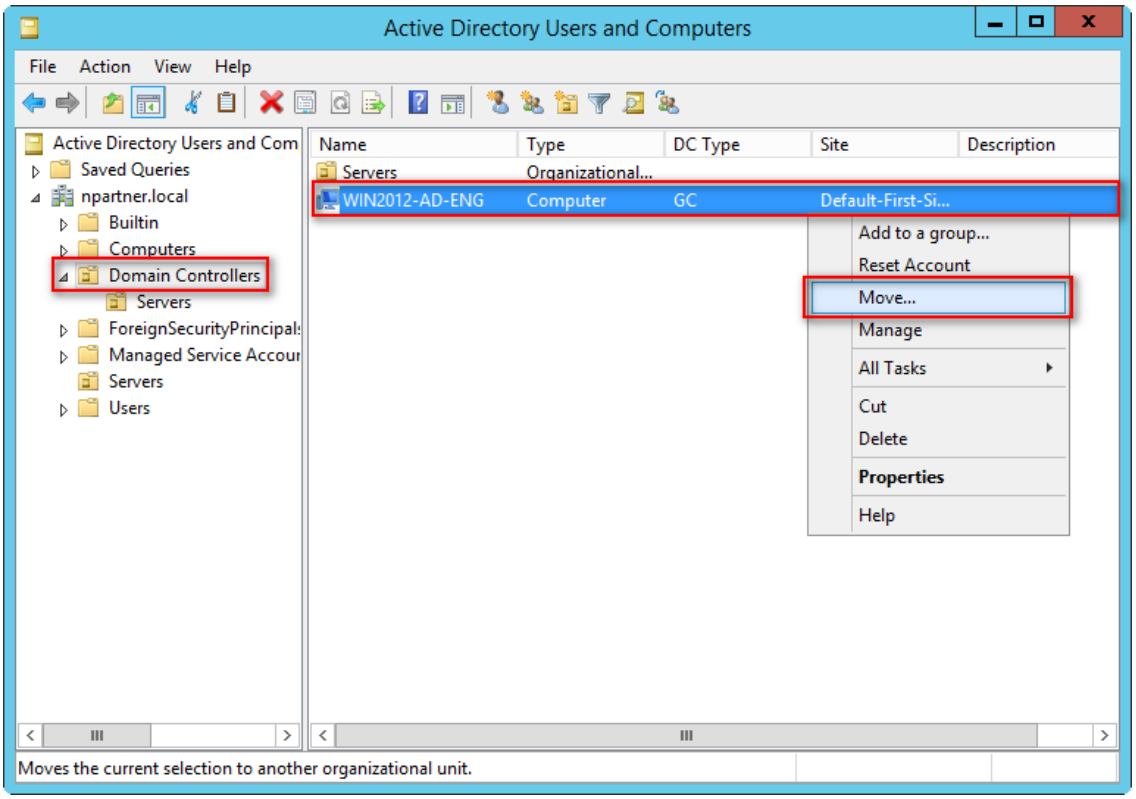
-> Click “OK.”



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

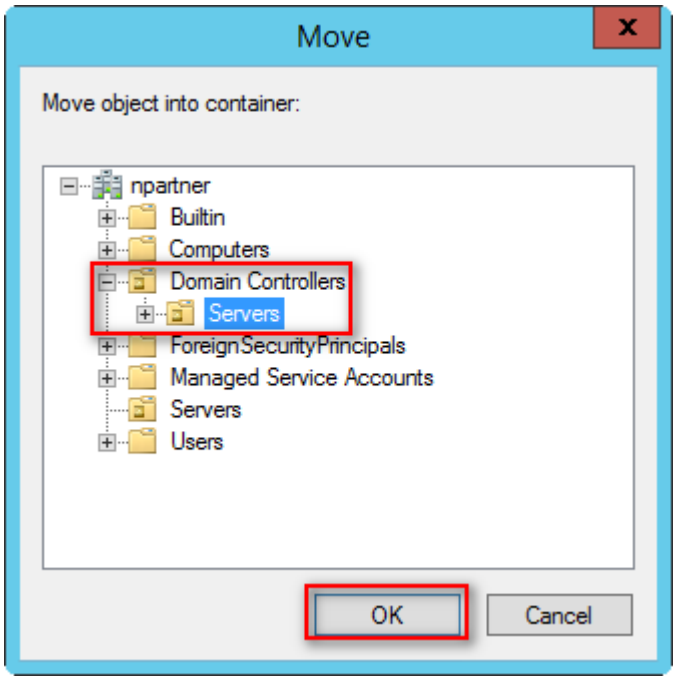
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2012-AD-ENG” server.

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



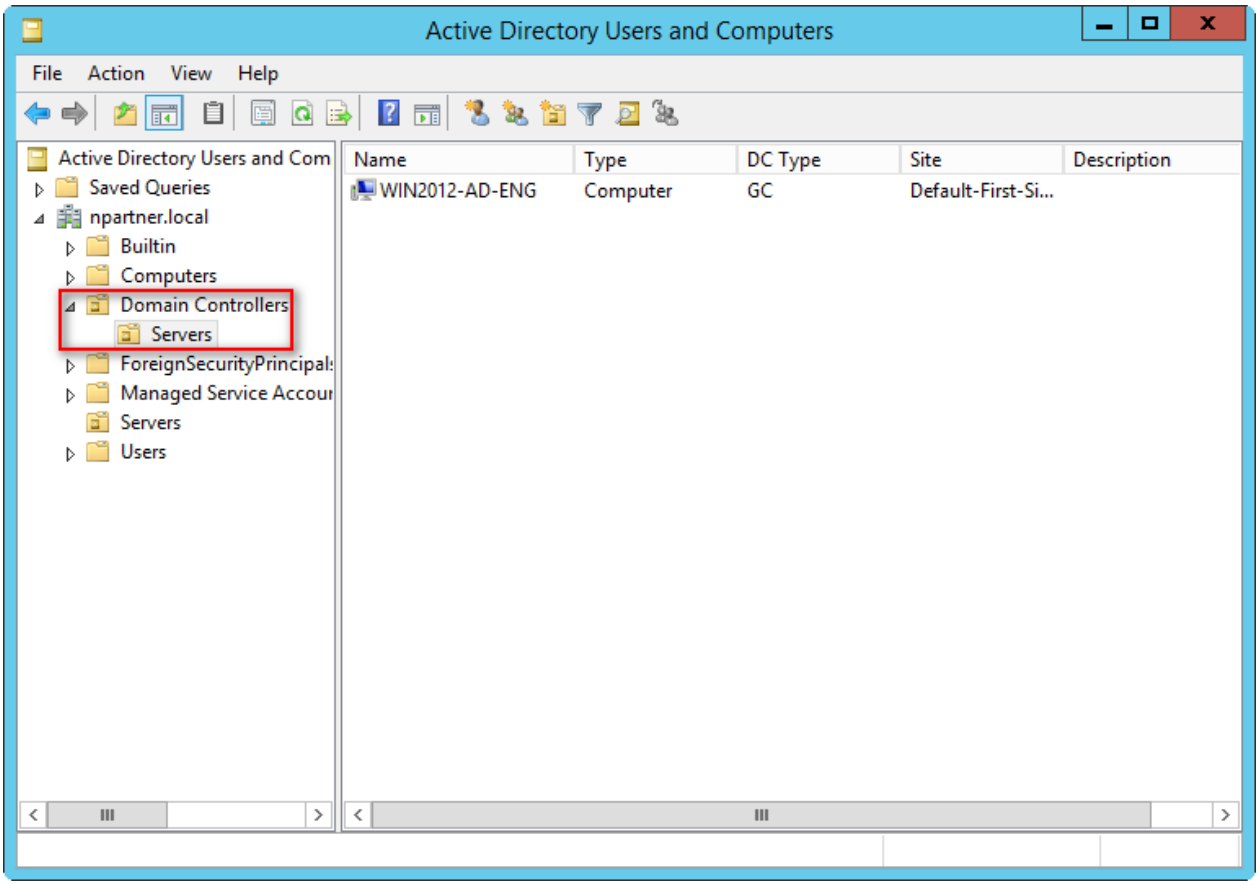
(5) Select your Organizational Unit:

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:

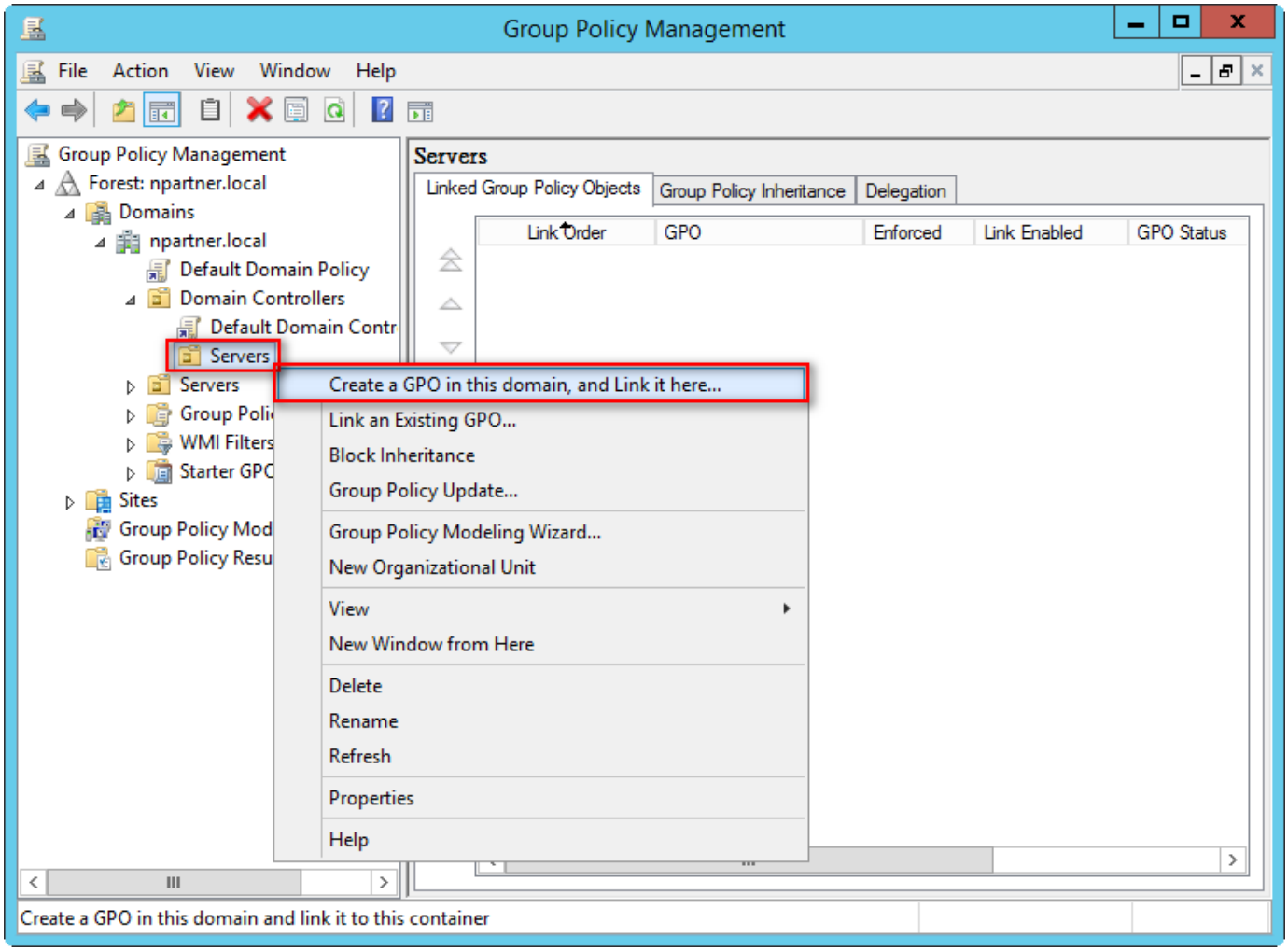
Expand your organizational unit folder (in this example, it is “Servers”) under “Domain Controllers” and confirm that the “WIN2012-AD-ENG” server has been moved.



4.2 Group Policy Settings

(1) Click “Group Policy Management.”

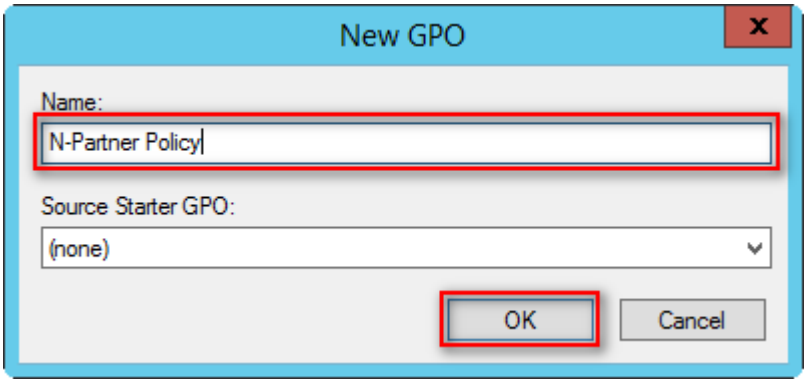
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(3) Enter your Group Policy Object Name

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

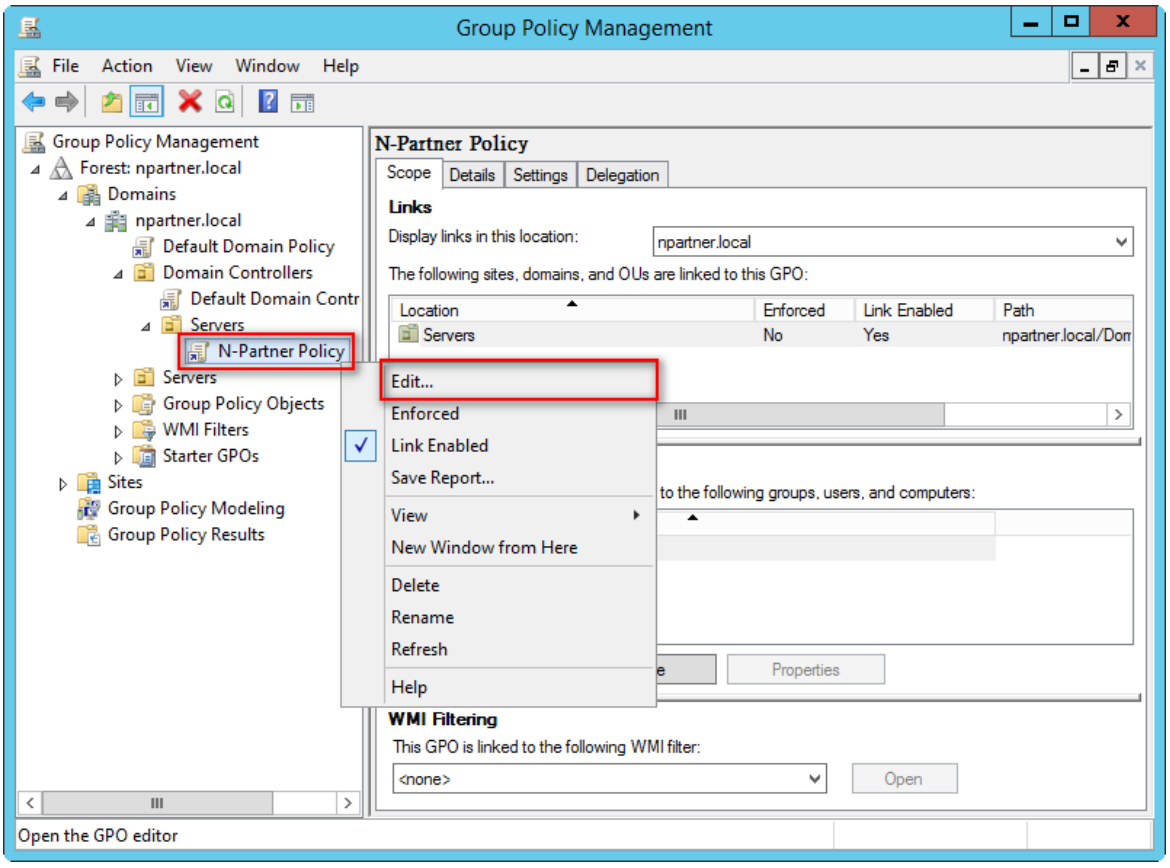
Note: Create your GPO name according to the client's environment. Then click “OK.”



(4) Edit your Group Policy Object

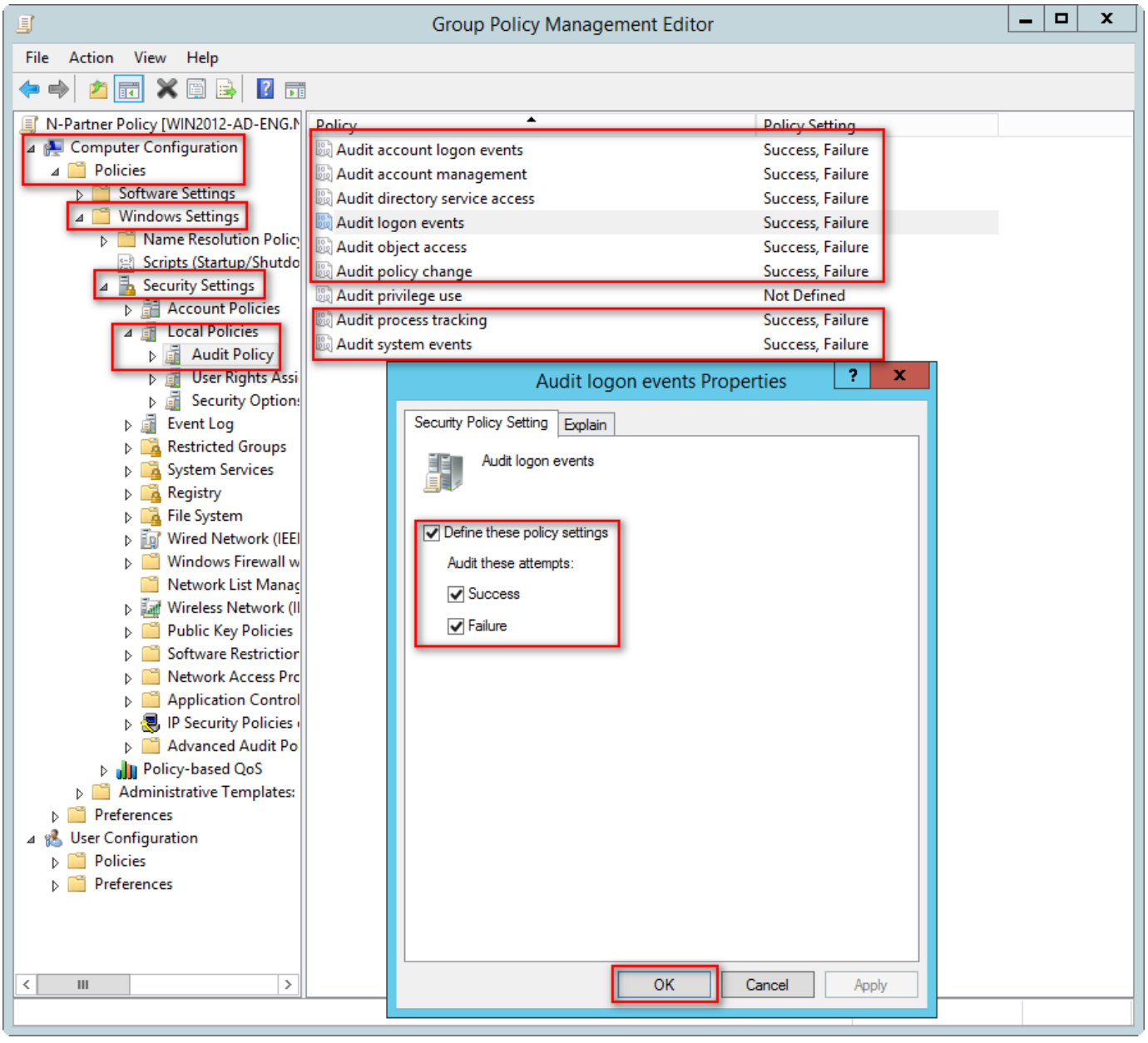
In your group policy object, (in this example, it is “N-Partner Policy”)

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.”

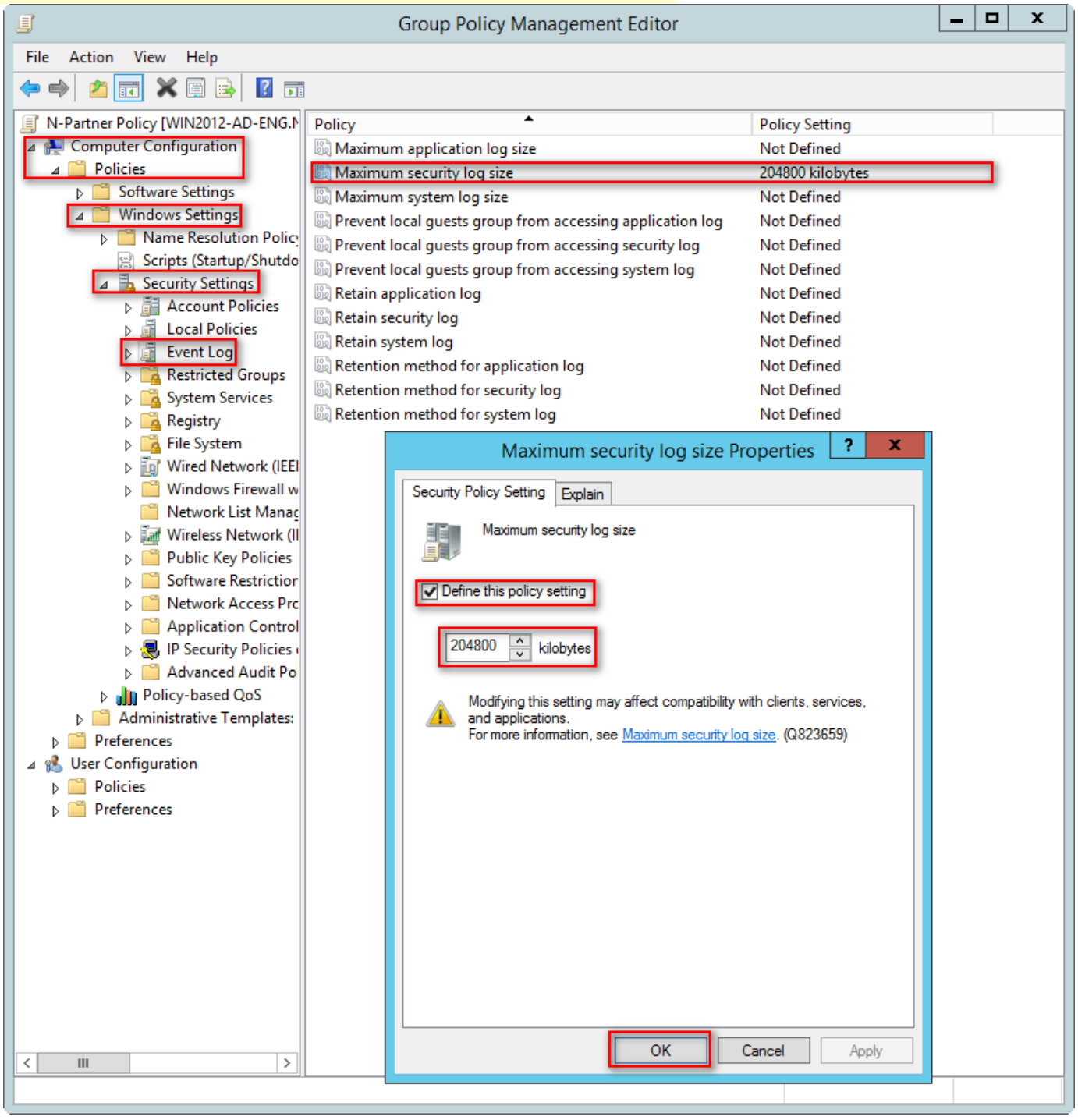


(6) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” ->

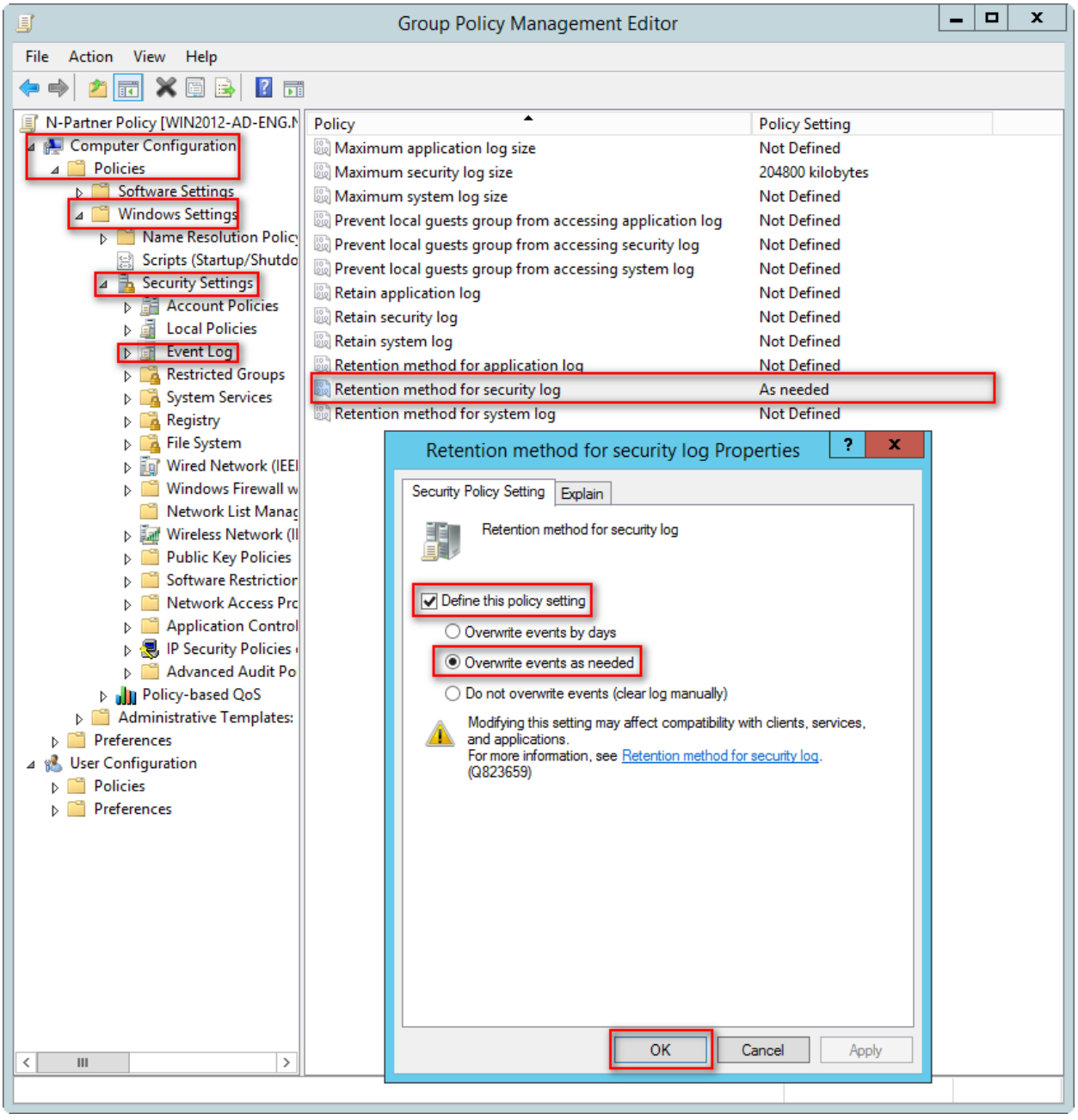
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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



(7) Event Logs: Retention Method for Security Log

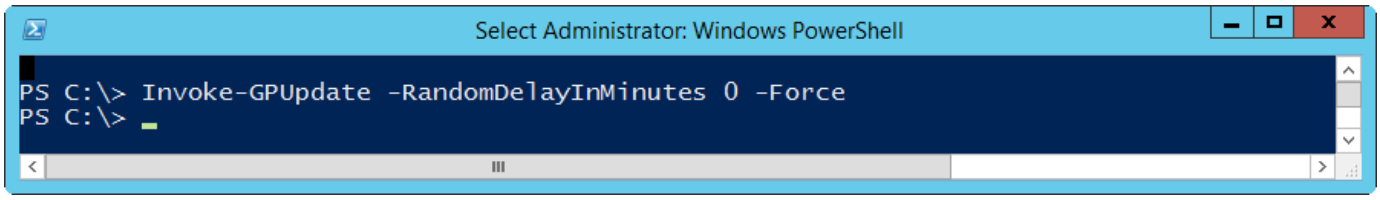
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”



(8) Open “Windows PowerShell.”

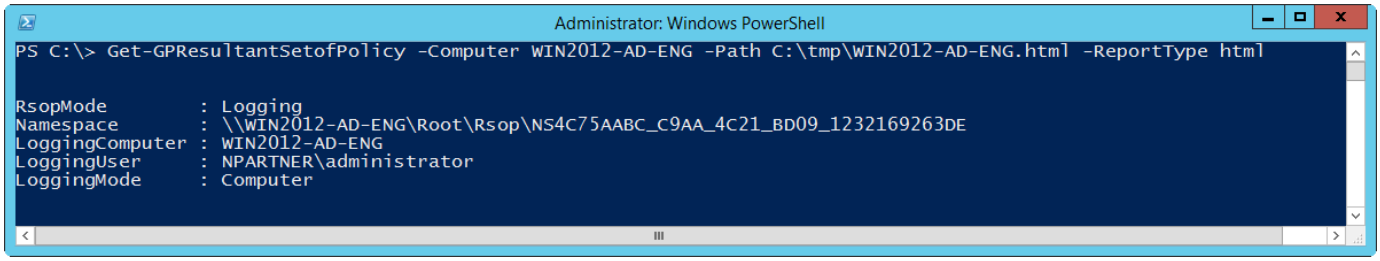
(9) Enter the command below to refresh group policy.

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



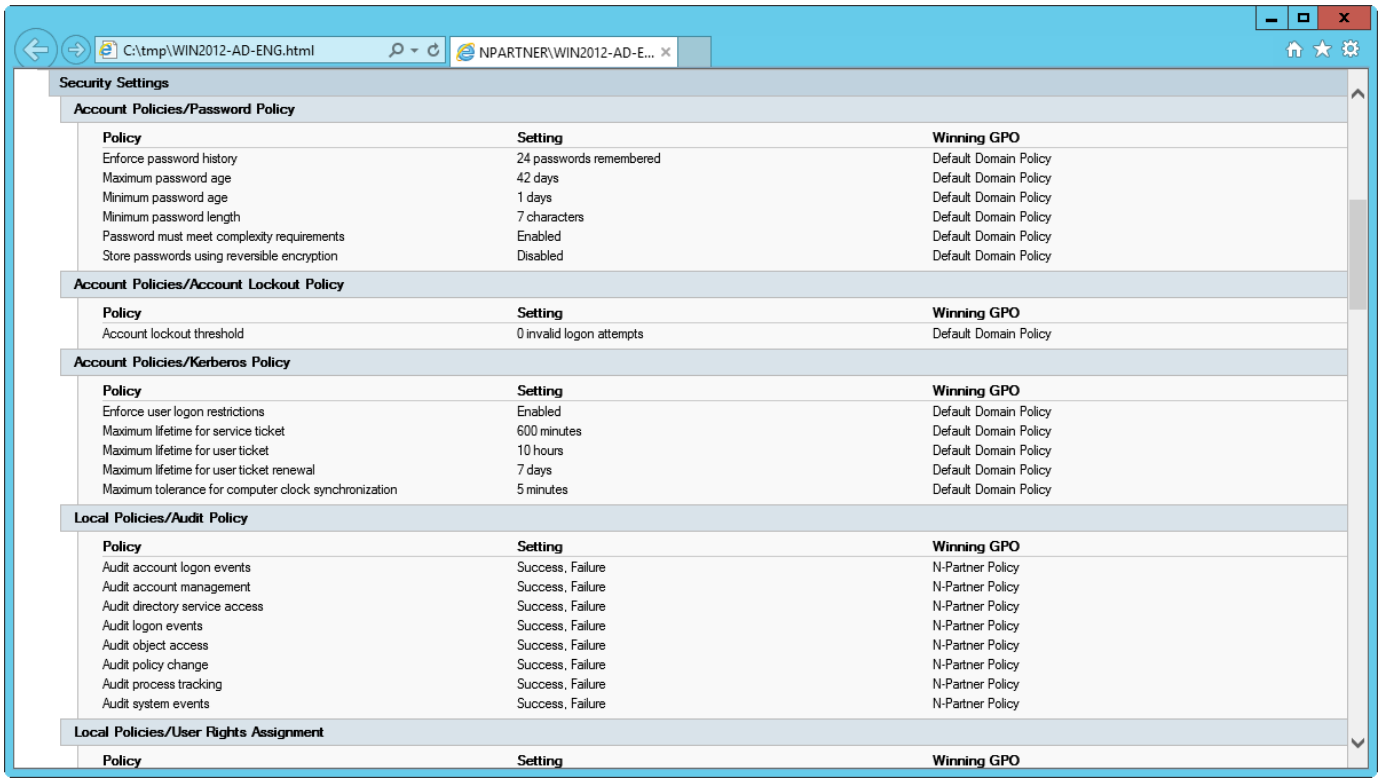
(10) Enter the command below to generate server group policy report.

```
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.



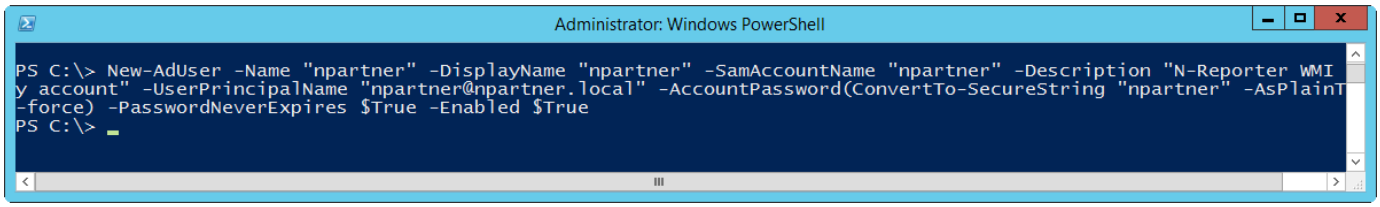
4.3 Add a Non-Admin Account

4.3.1 Add Users

(1) Open “Windows PowerShell.”

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

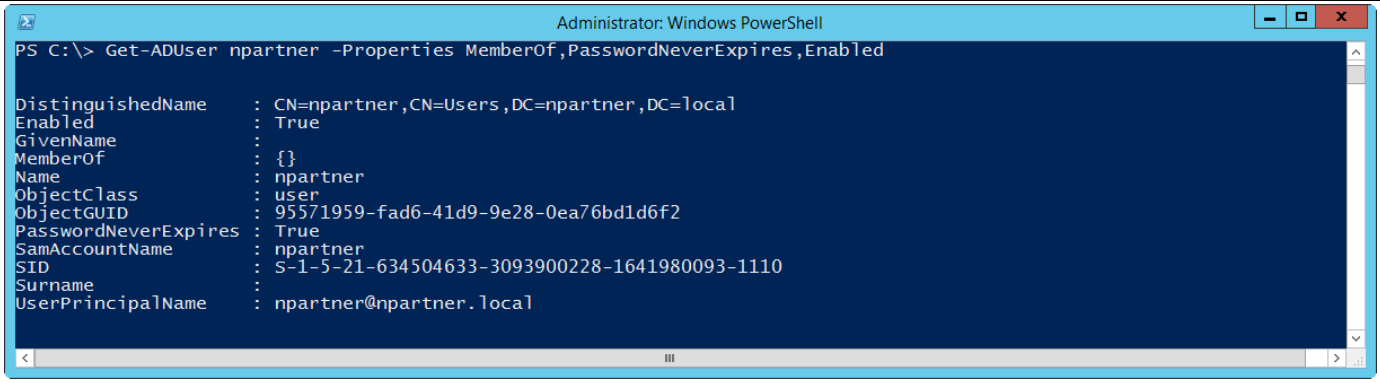
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```

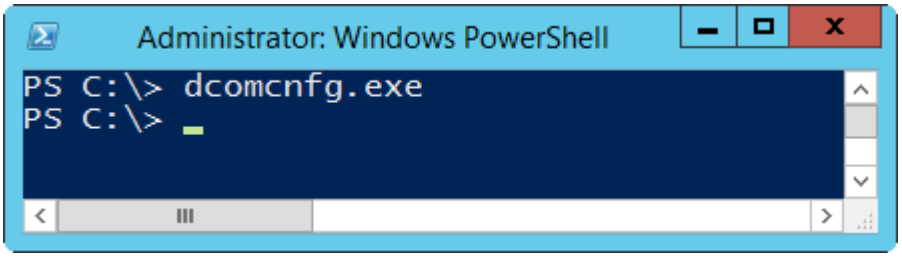


4.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”

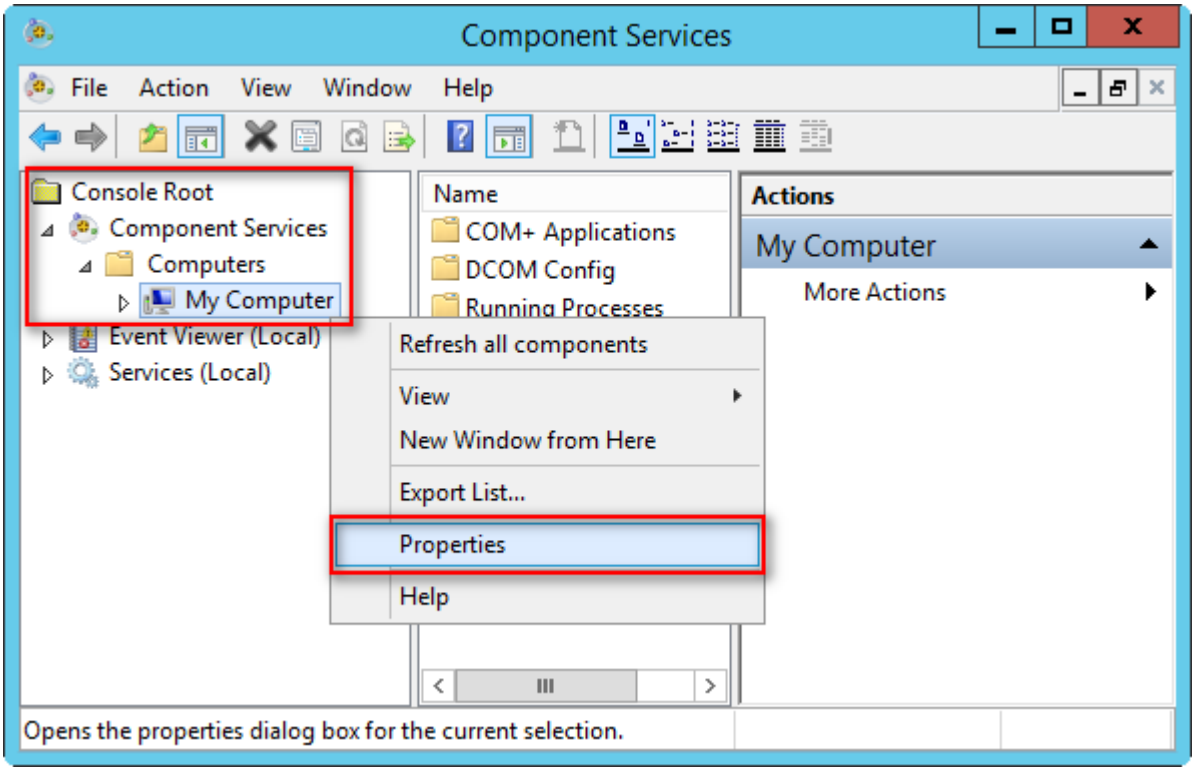
(2) Enter the command below to open component services.

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



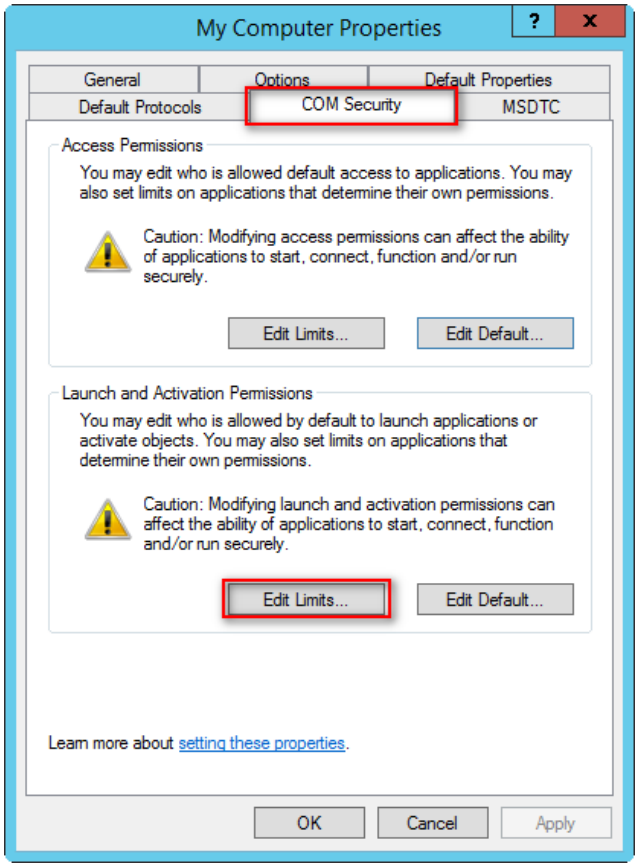
(3) Edit Computer Properties

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



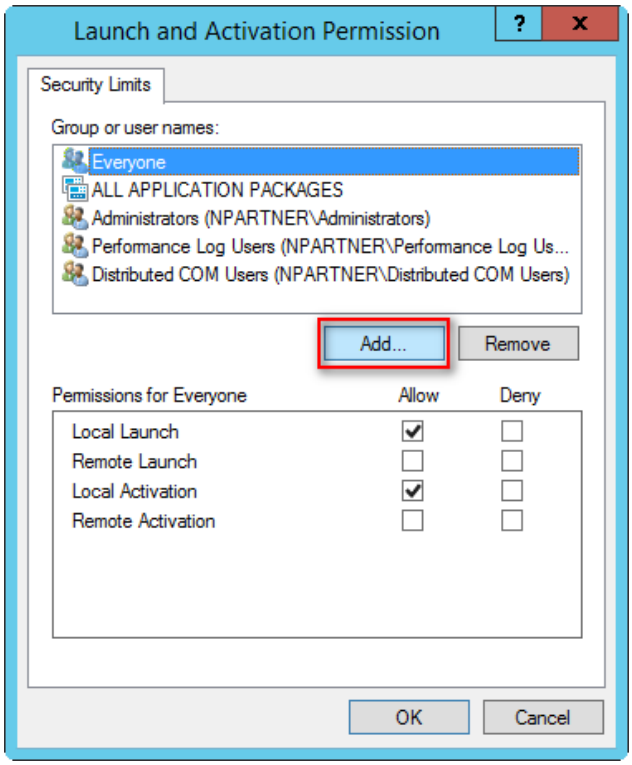
(4) Enable Permissions

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



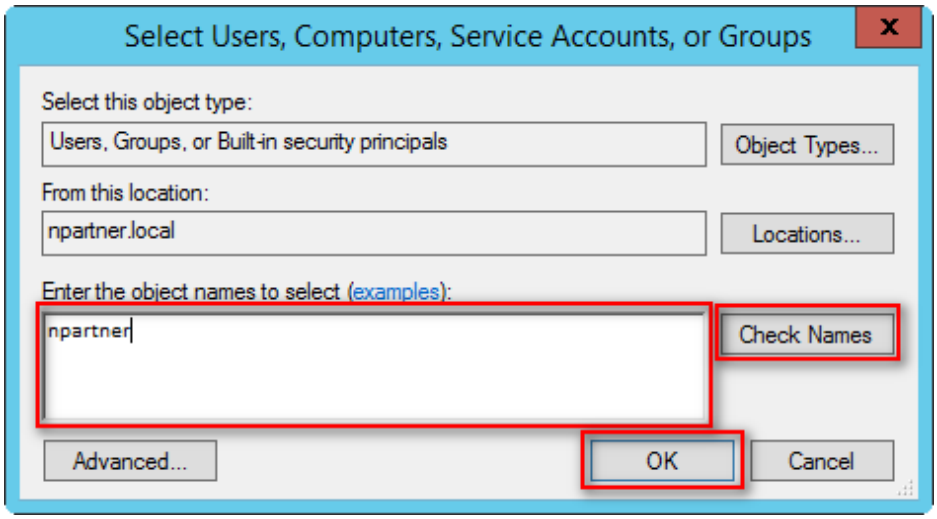
(5) Add DCOM User Permissions

Click “Add.”



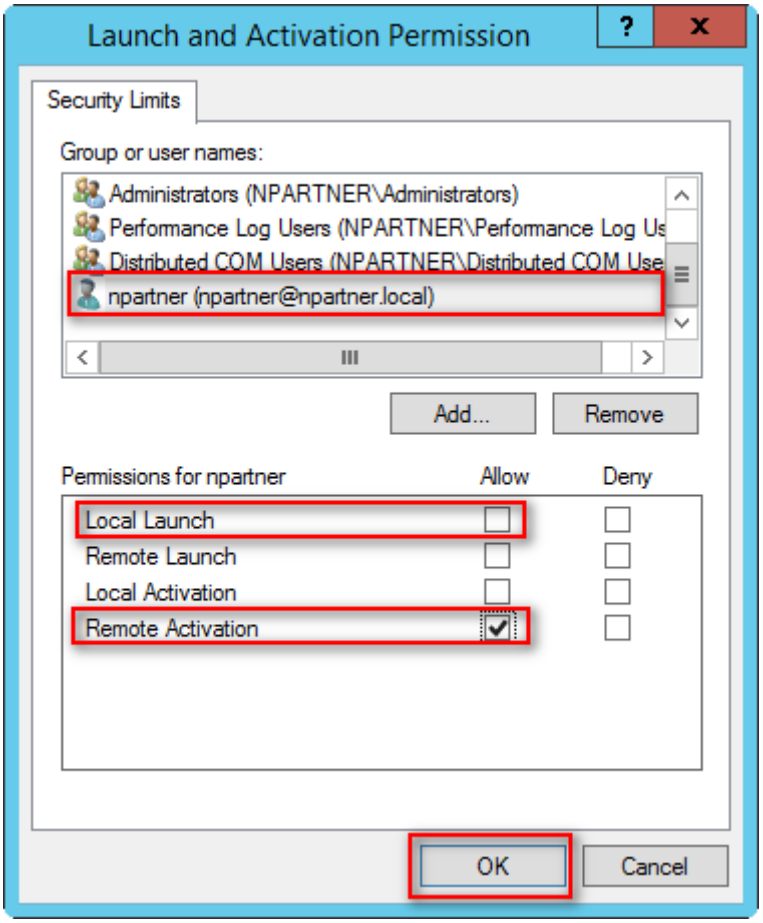
(6) Enter your Username

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

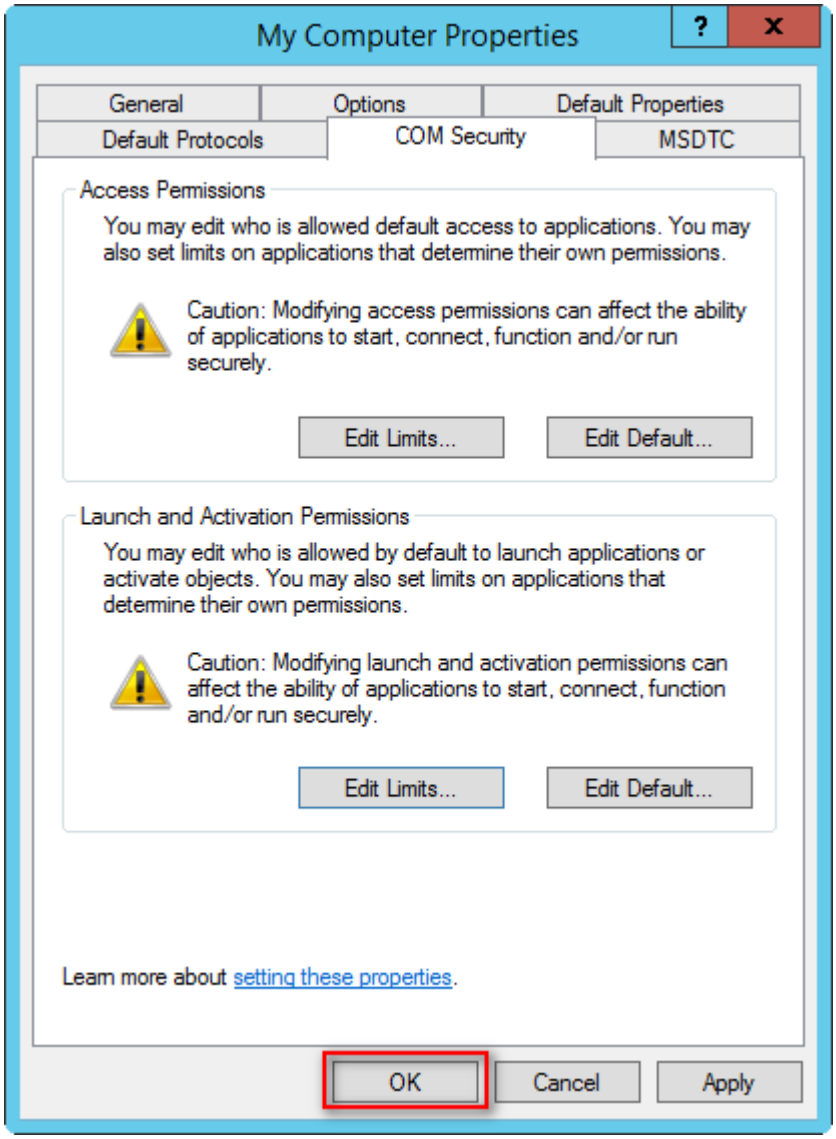


(7) Set User Permissions

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



(8) Click “OK.”



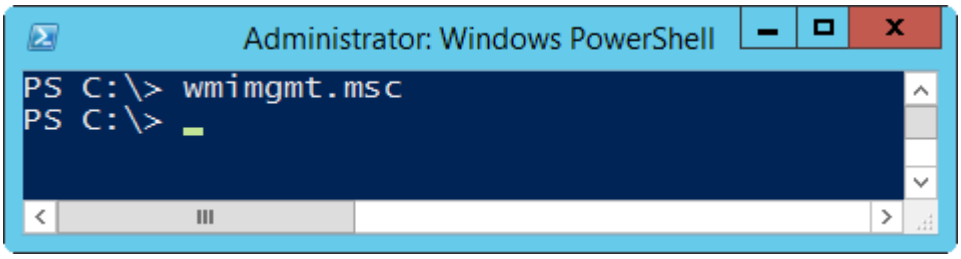
4.3.3 Configure WMI Permissions

4.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”

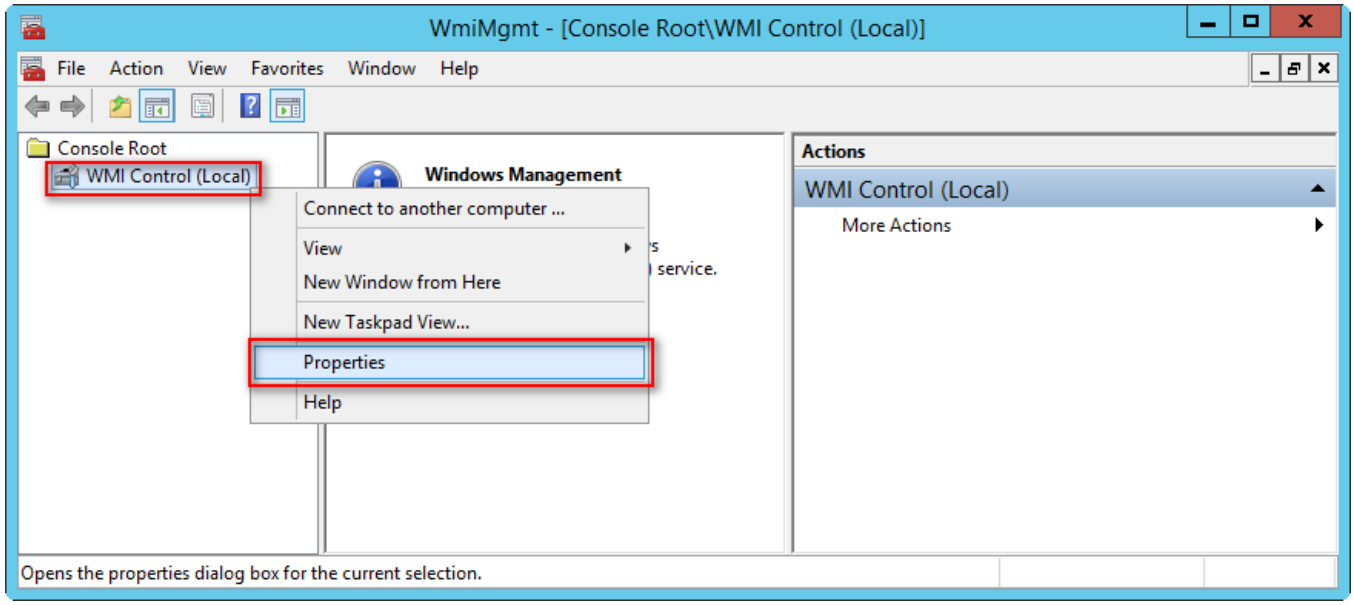
(2) Enter the command below to enable component services.

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



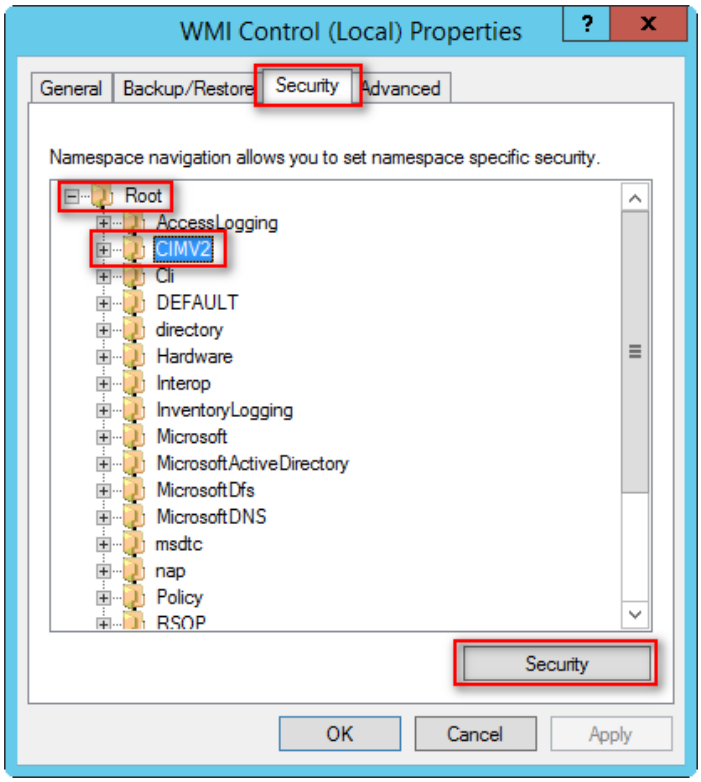
(3) Edit WMI Control

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



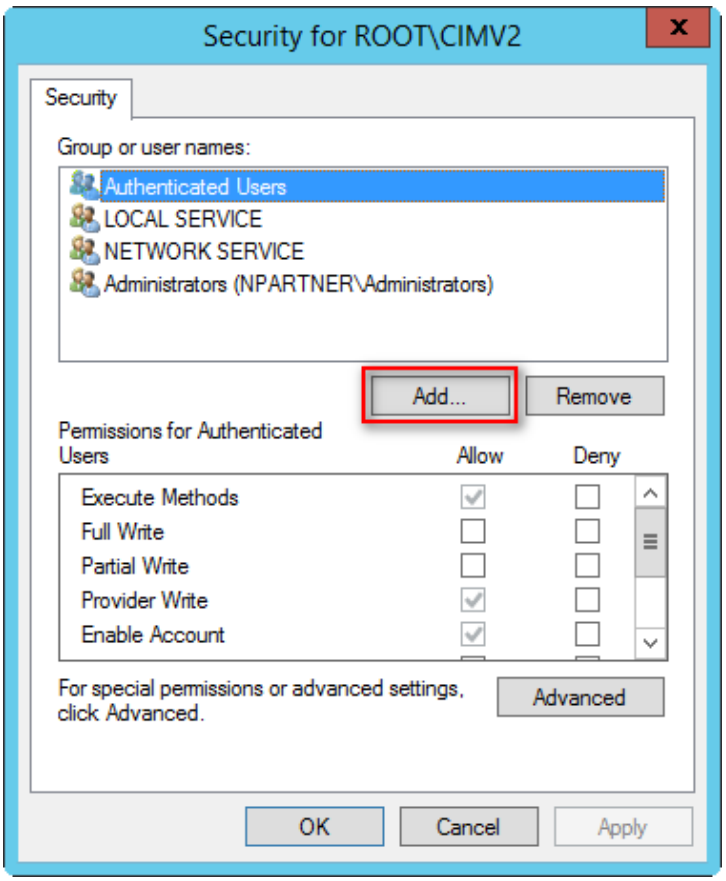
(4) Edit CIMV2 Security

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



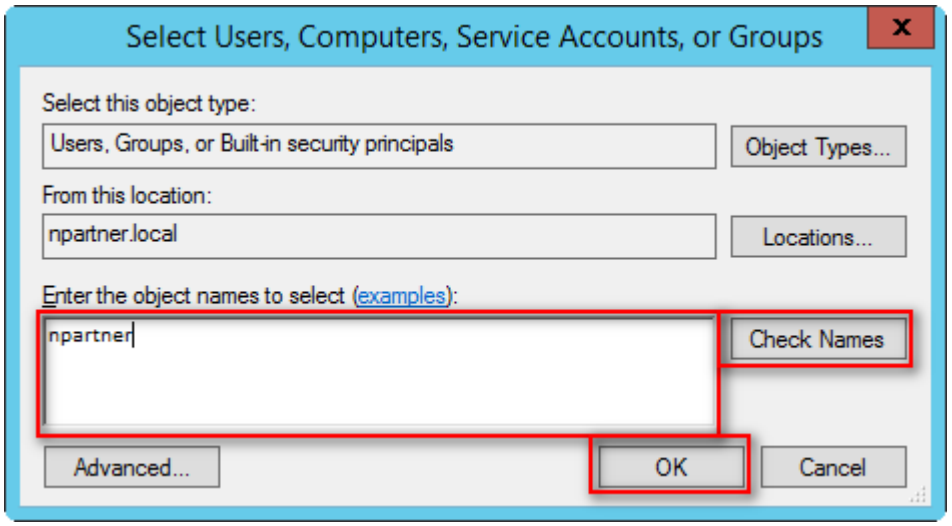
(5) Add WMI User Permissions

Click “Add.”



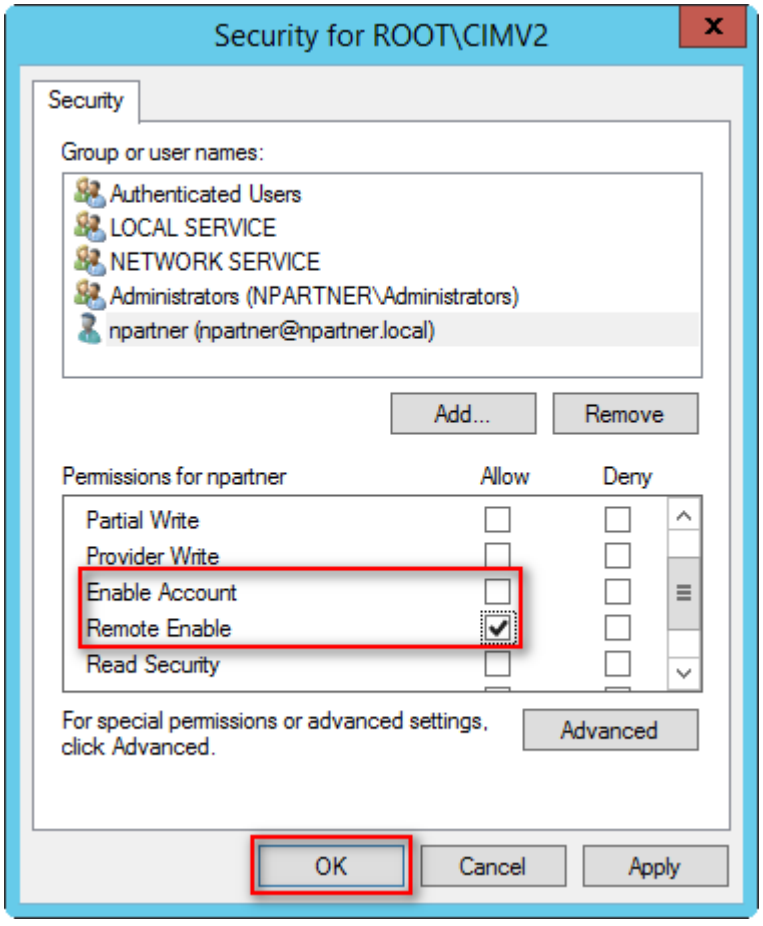
(6) Enter User

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

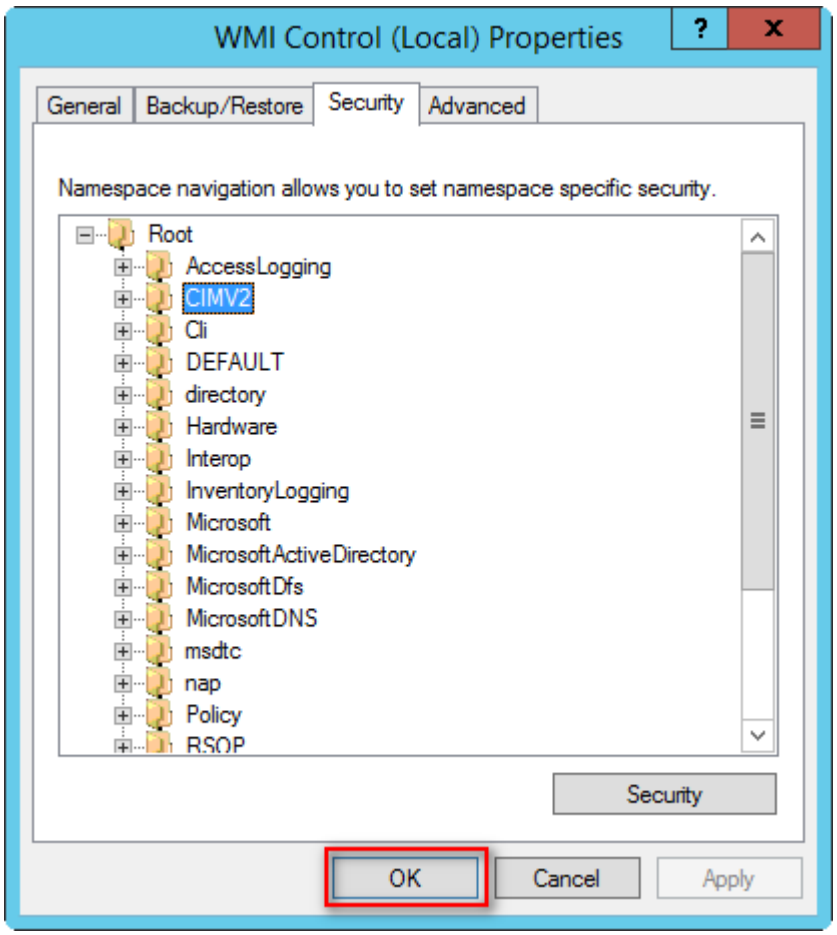


(7) Set User Permissions

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



(8) Click “OK.”

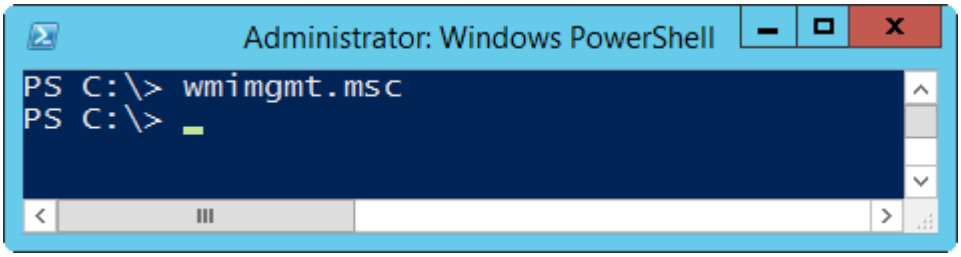


4.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”

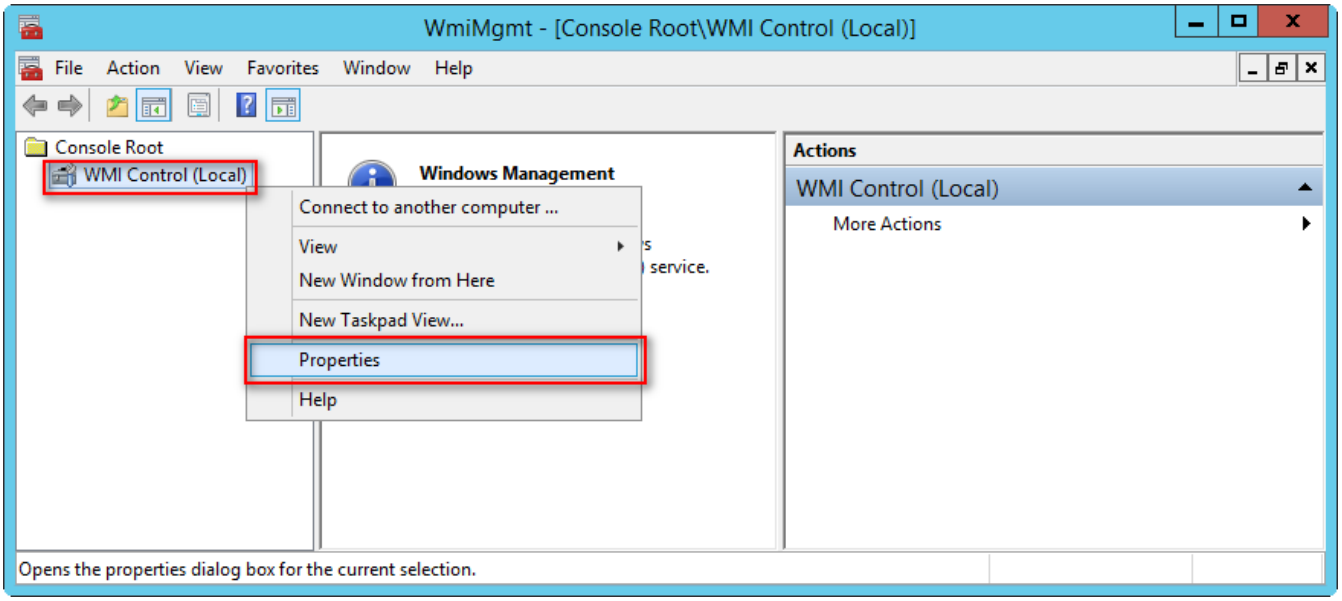
(2) Enter the command below to enable WMI Control.

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



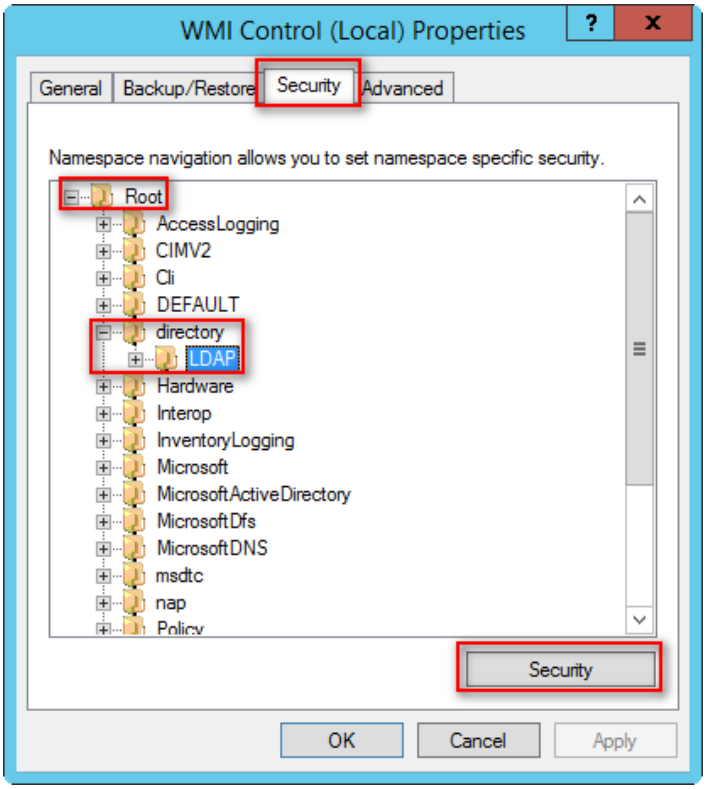
(3) Edit WMI Control

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



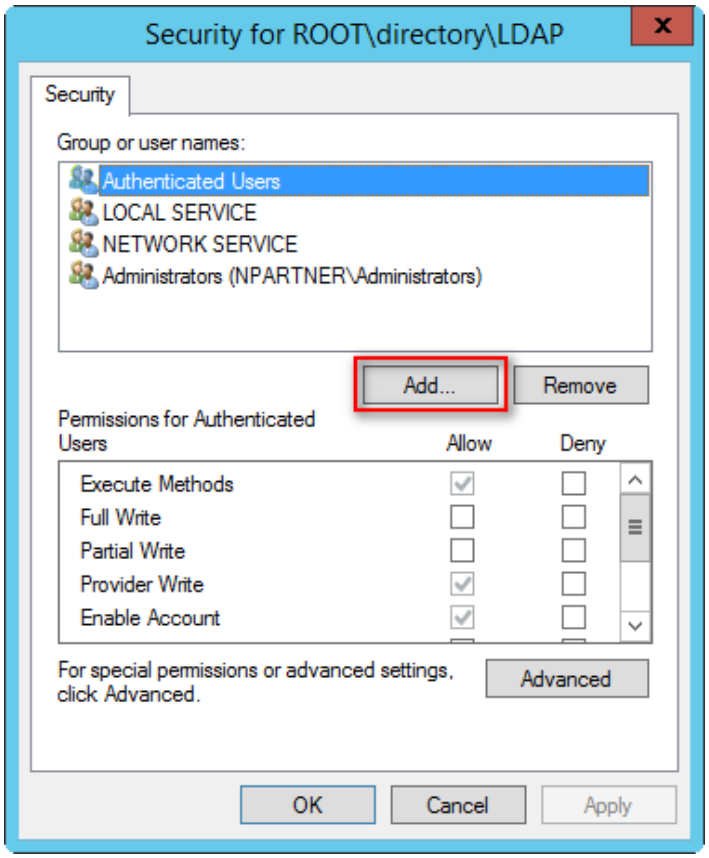
(4) Edit LDAP Security

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



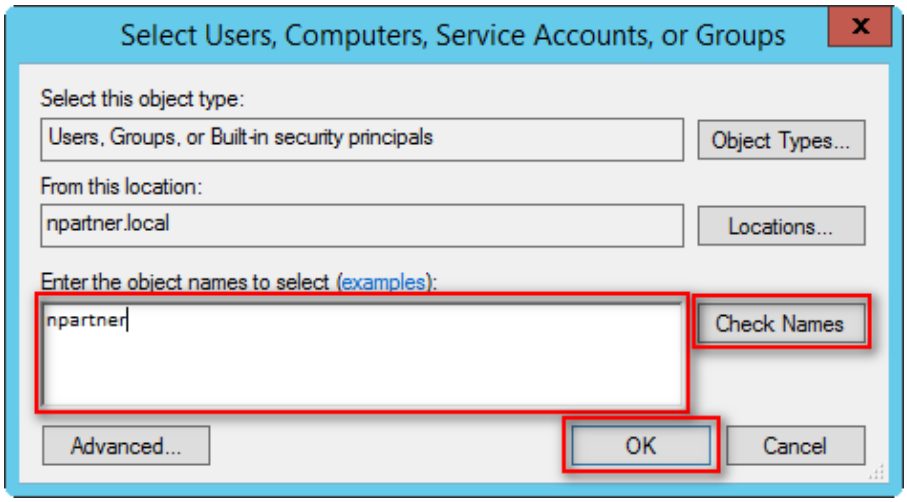
(5) Add WMI User Permissions

Click “Add.”



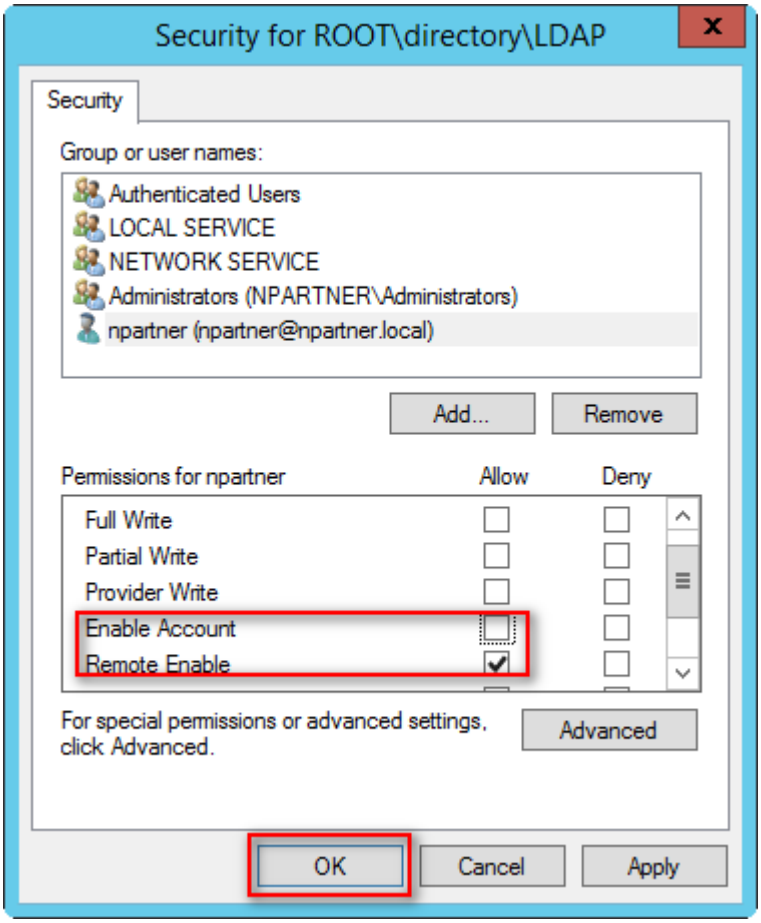
(6) Enter Your Username

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

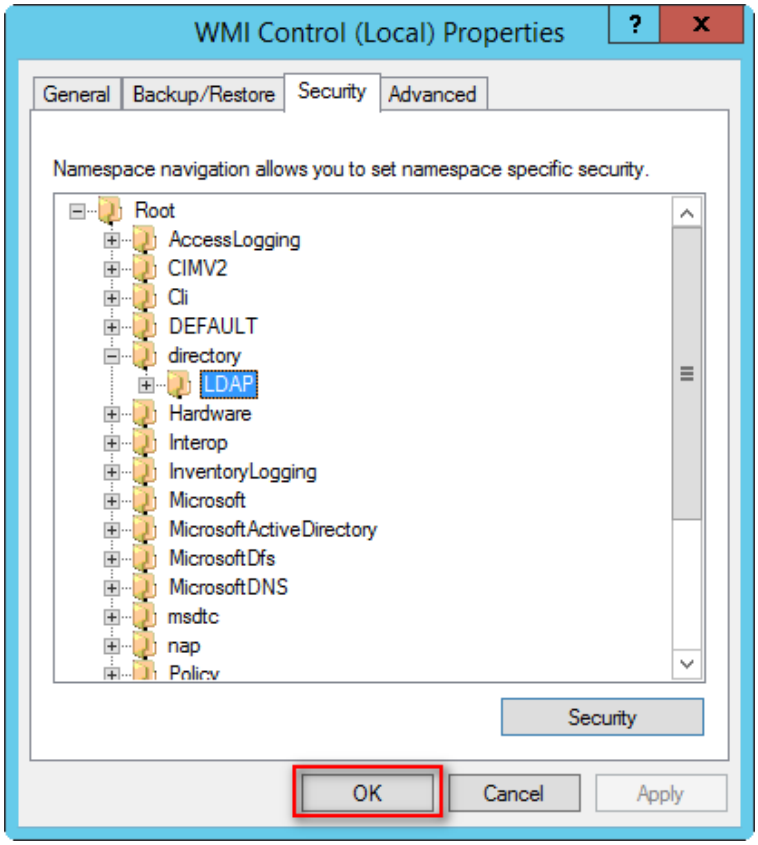


(7) Set Your User Permissions

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

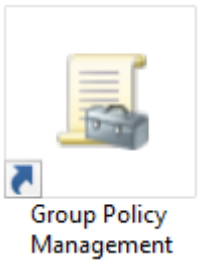


(8) Click “OK.”



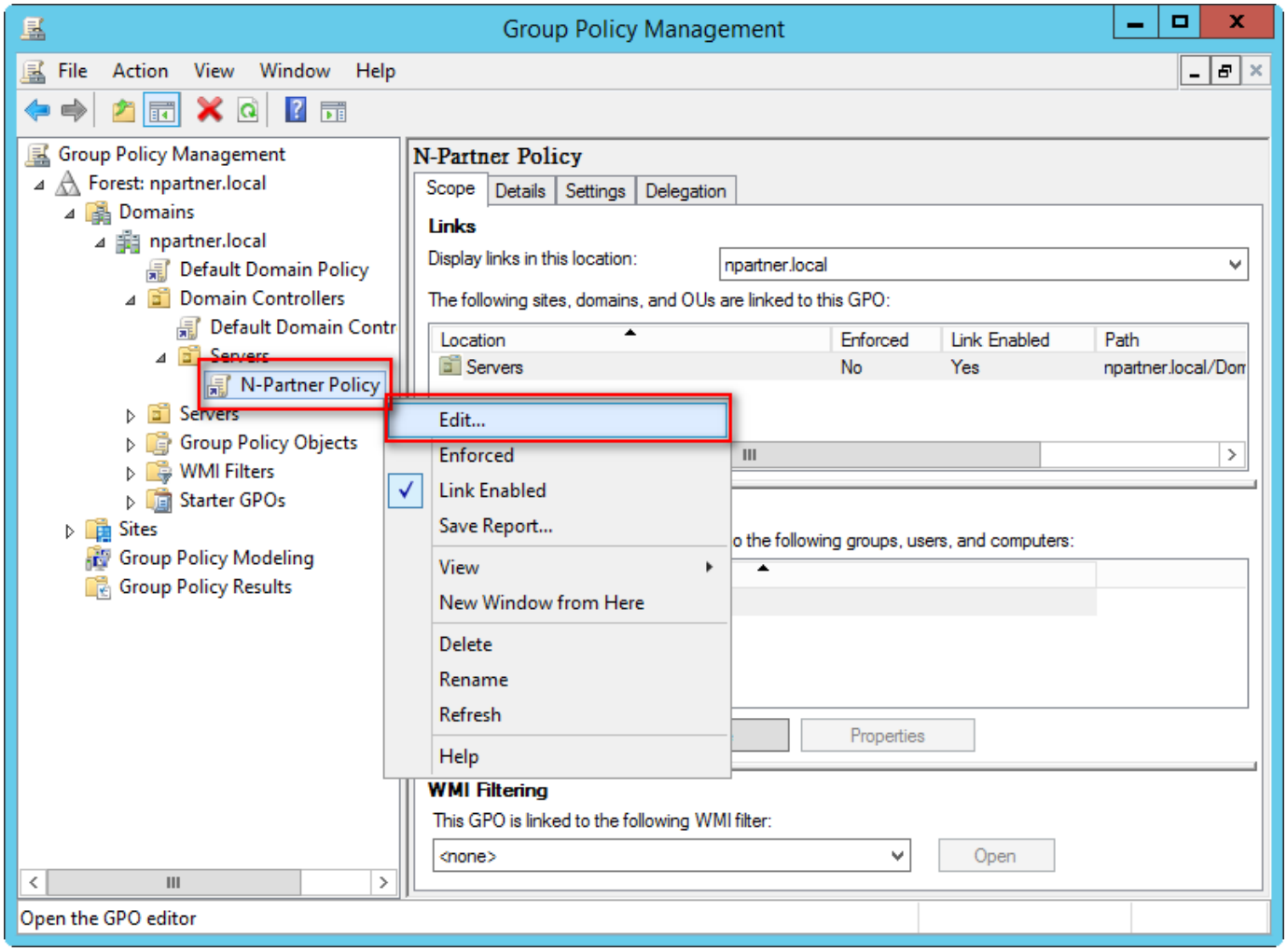
4.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object

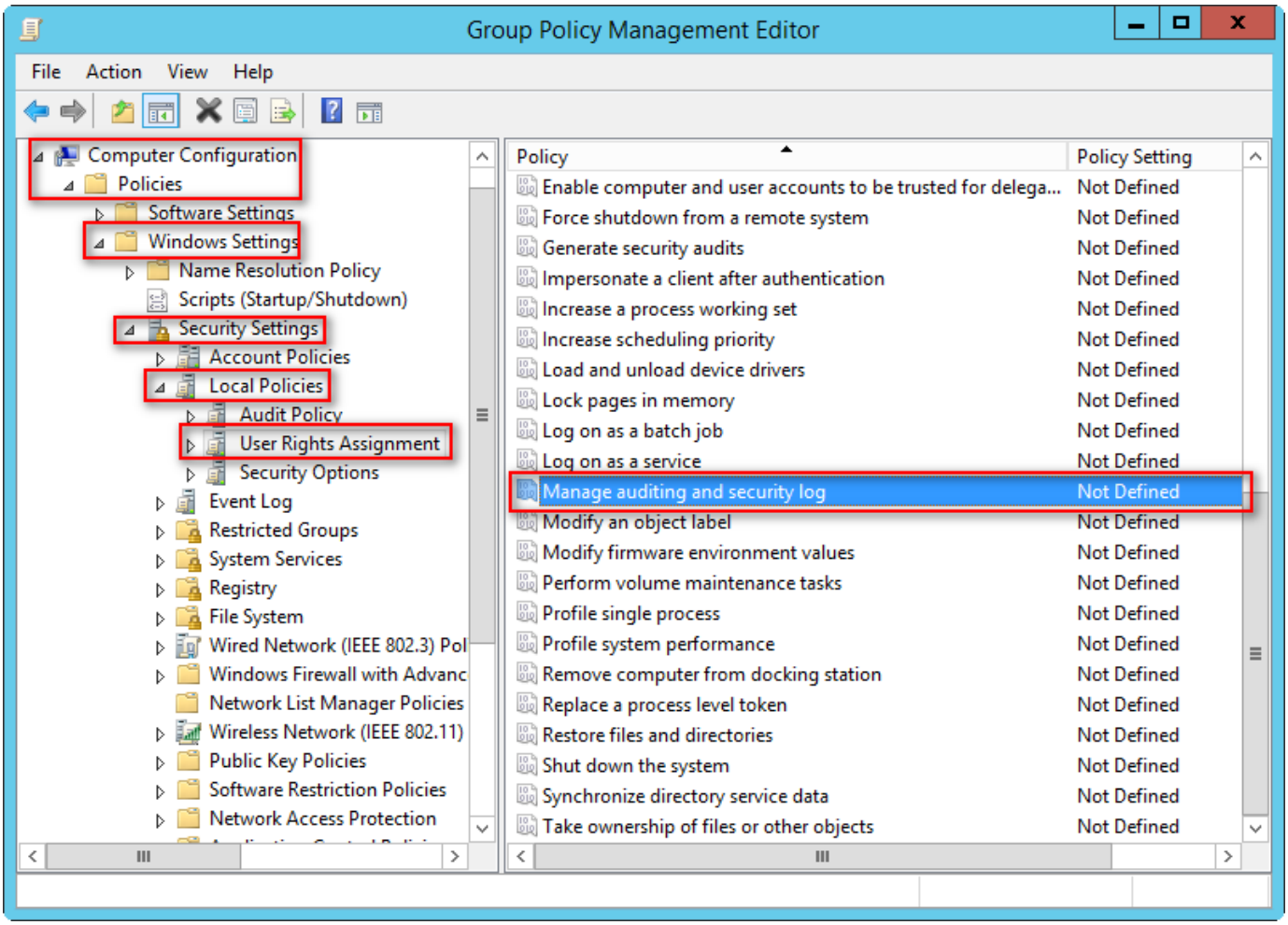
In the “N-Partner Policy” Group Policy Object, right-click and select “Edit.”



(3) Configure Log Settings

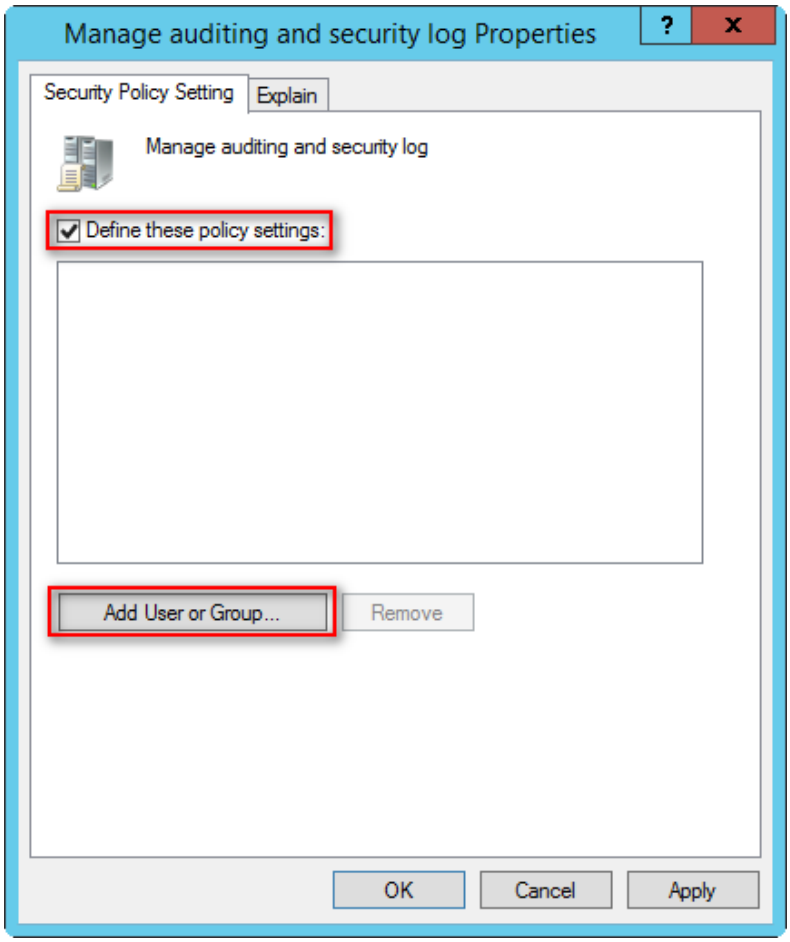
“Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “User Rights Assignment”

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



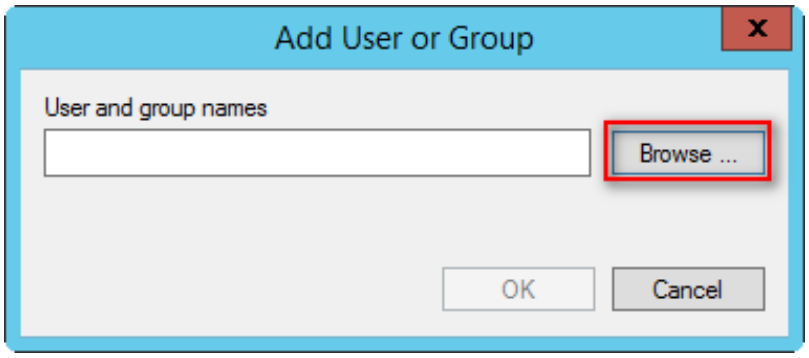
(4) Add Audit Management Users

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



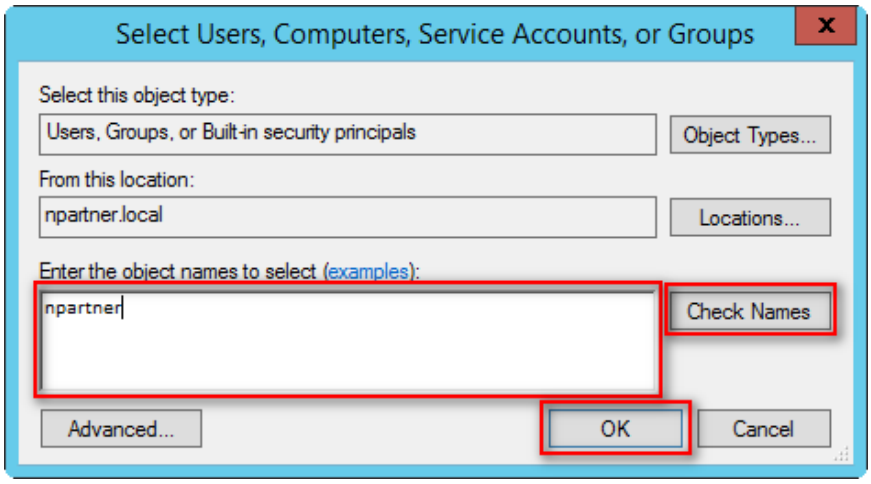
(5) Search for Users

Click “Browse.”



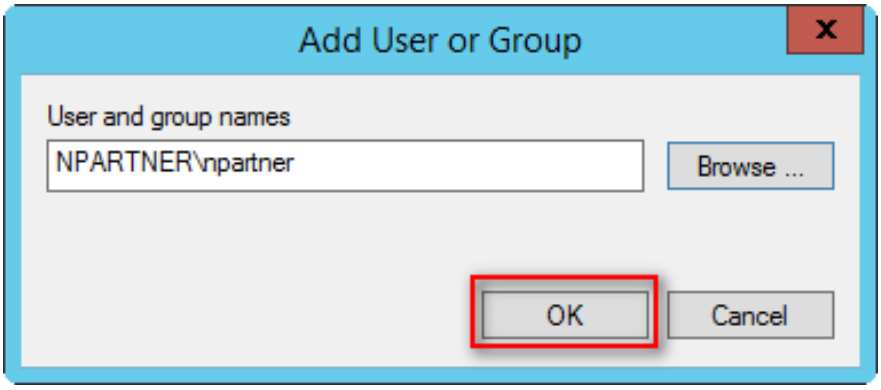
(6) Enter the User

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



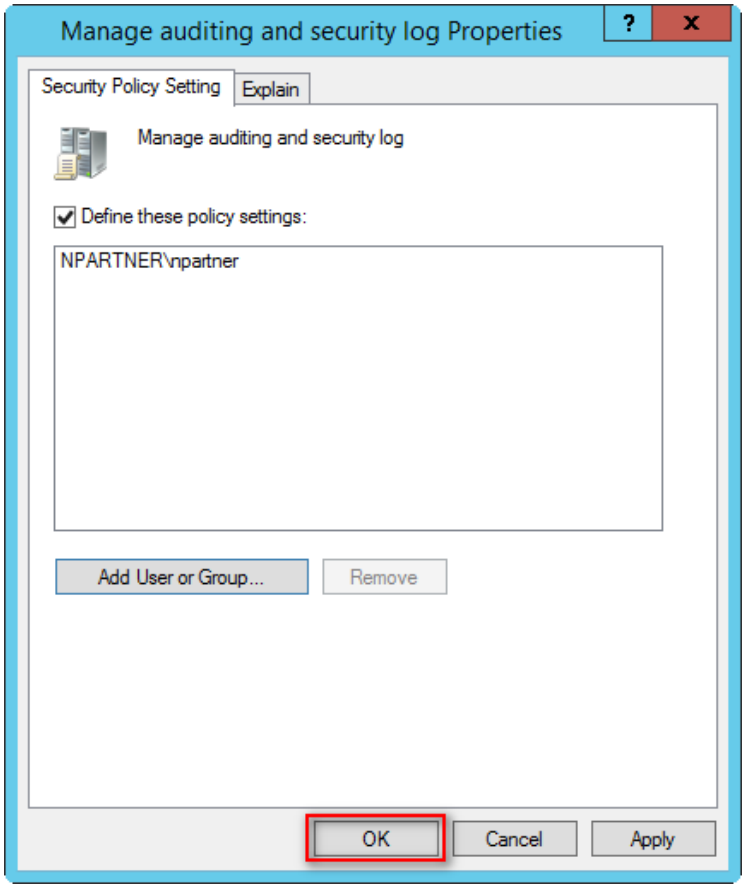
(7) Confirm the User

Click “OK.”



(8) Confirm Logging Settings

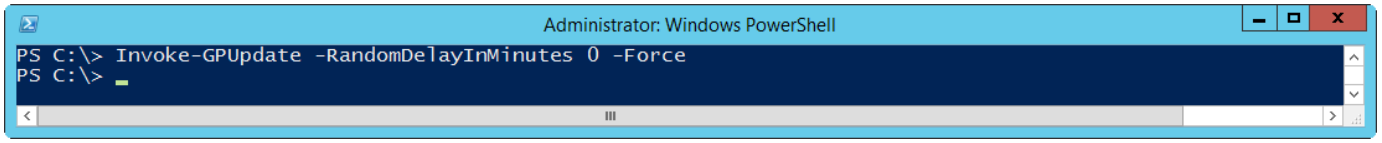
Click “OK” to apply the configuration.



(9) Click “Windows PowerShell.”

(10) Enter the command to update group policy:

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

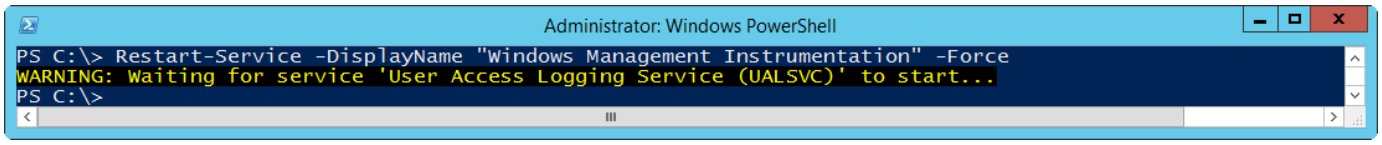


4.3.5 Restart the WMI Service

(1) Click “Windows PowerShell.”

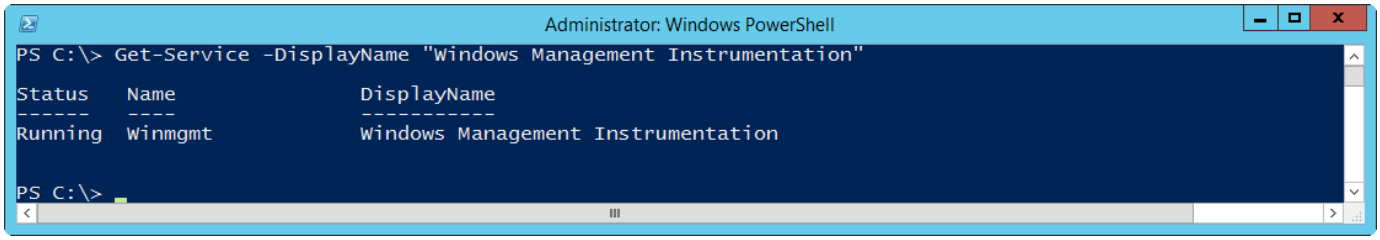
(2) Enter the command below to restart the WMI service:

```
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"
```

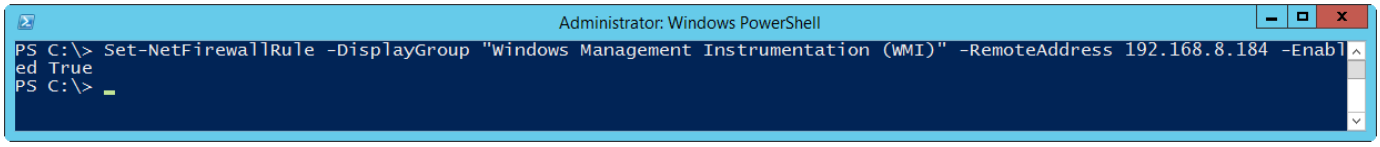


4.4 Configure the Firewall

(1) Open “Windows PowerShell.”

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

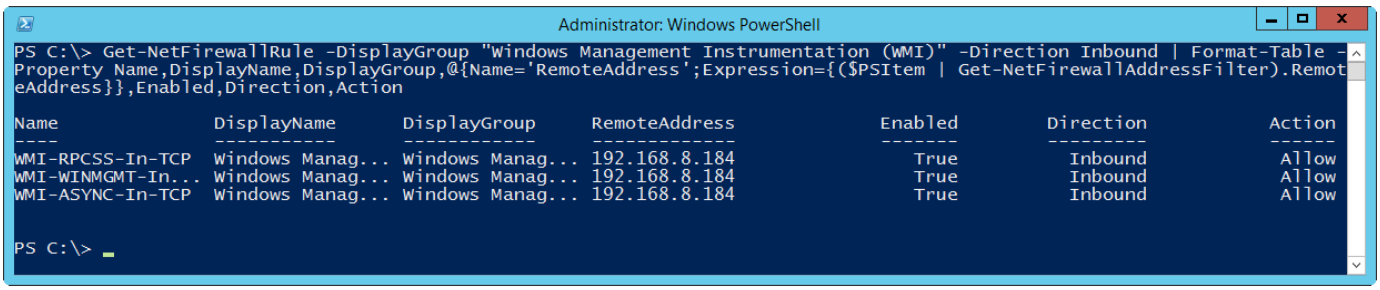
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -
RemoteAddress 192.168.8.184 -Enabled True
```



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
```

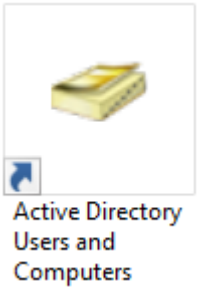


5. Windows 2016

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

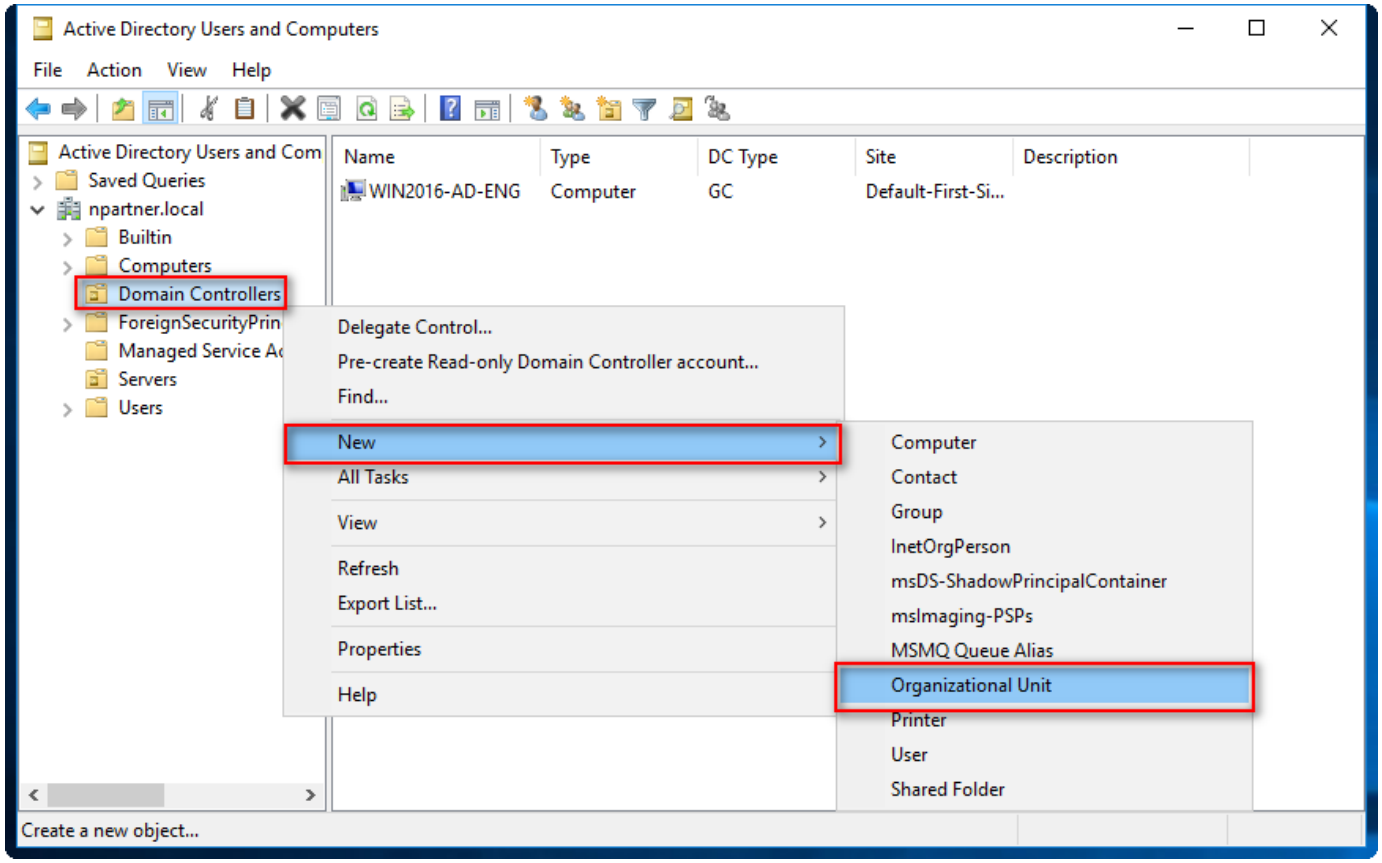
5.1 Organizational Unit Settings

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



(2) Add an Organizational Unit

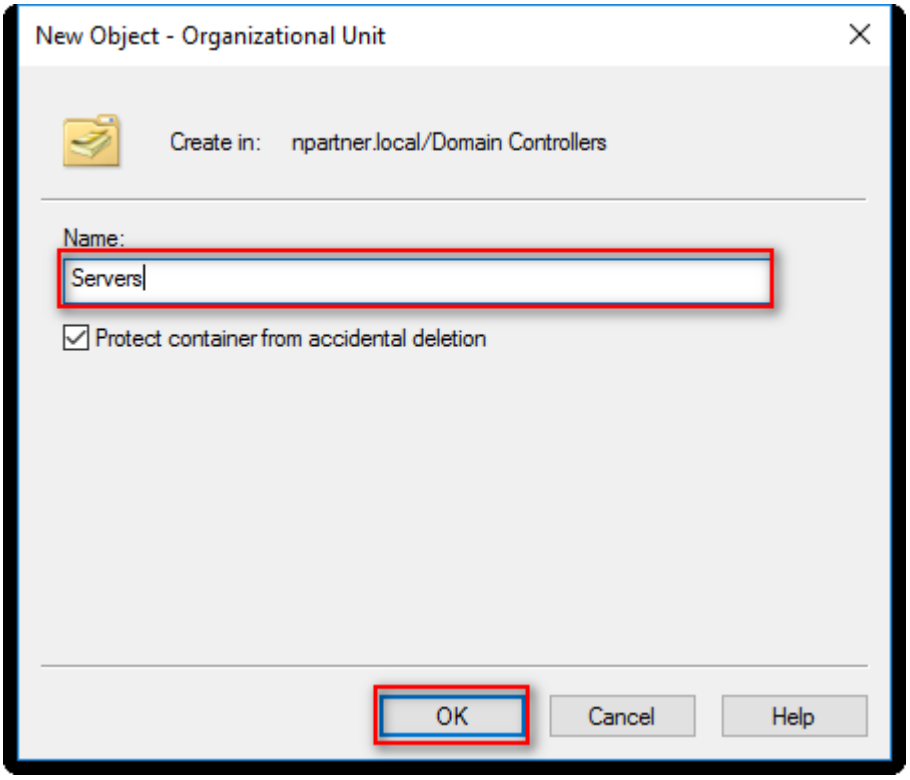
Right-click on “Domain Controllers, select “New,” and click “Organizational Unit.”



(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.

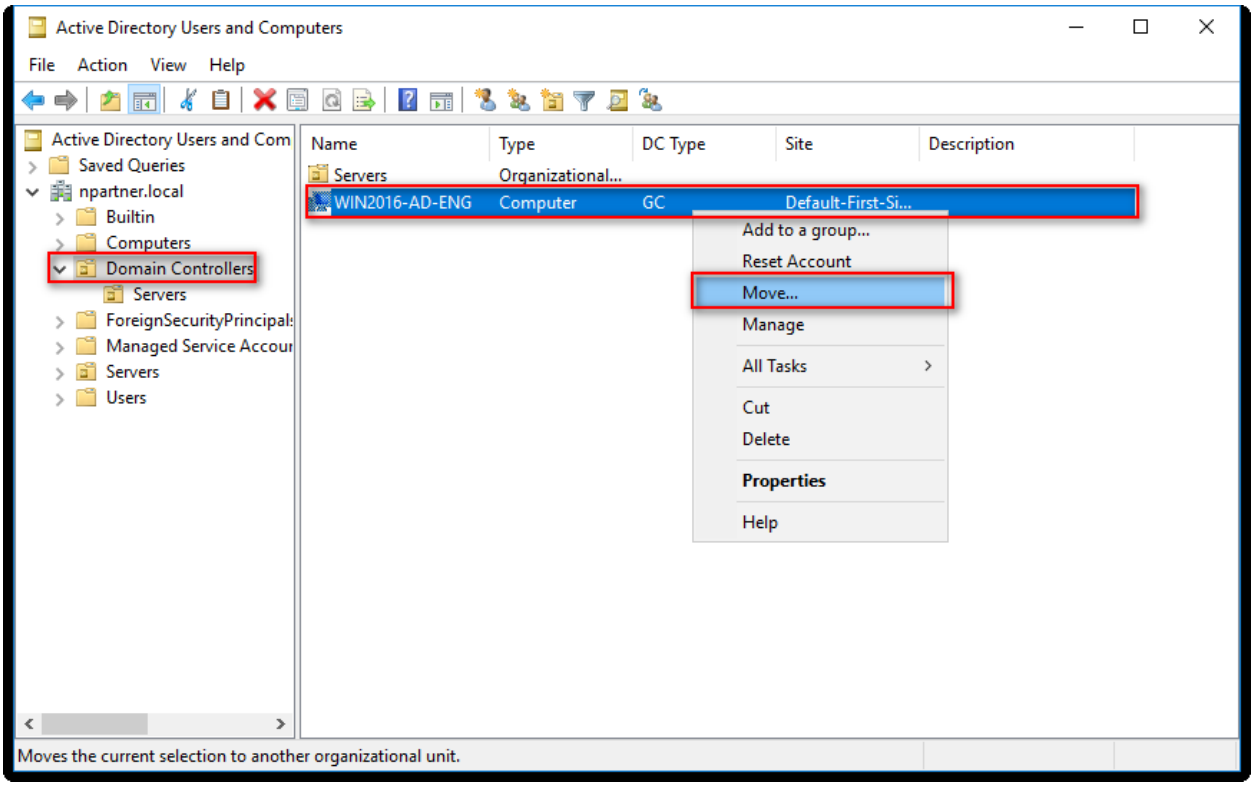
-> Click “OK.”



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

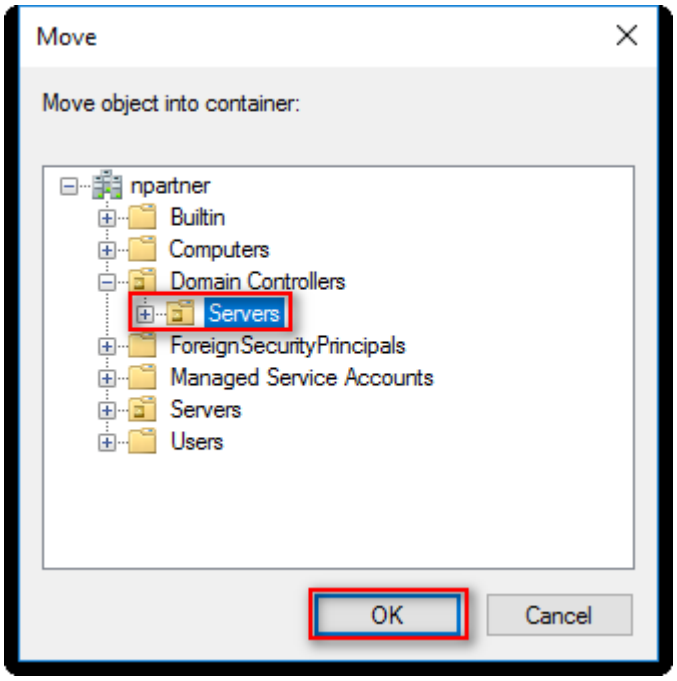
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2016-AD-ENG” server.

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



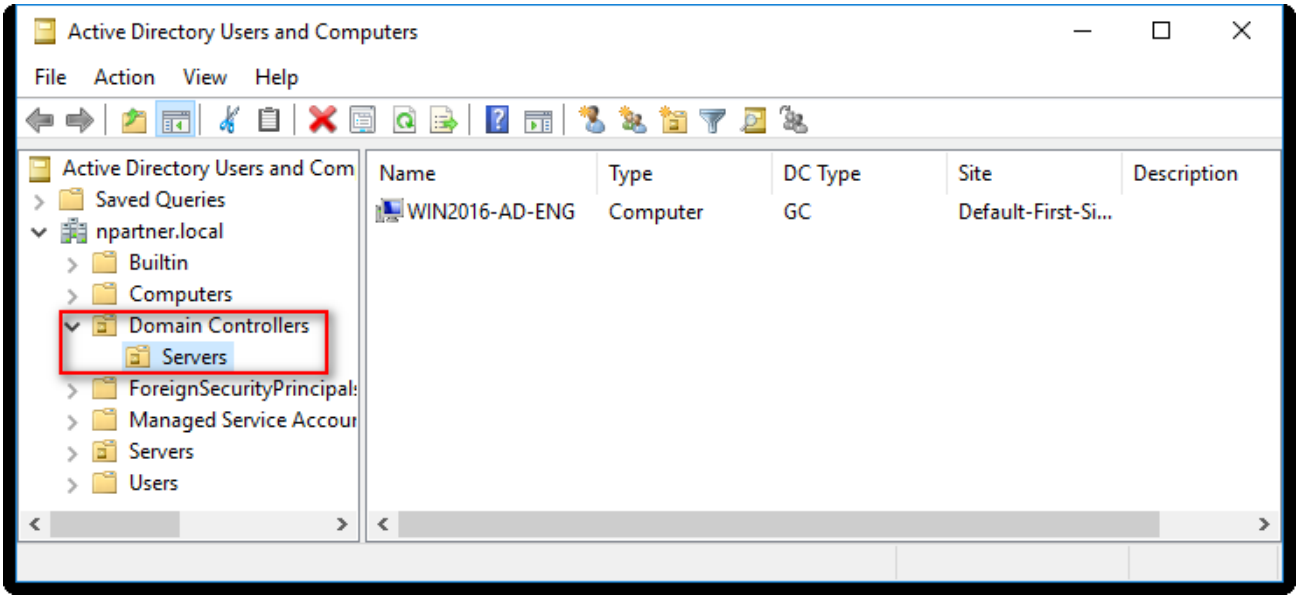
(5) Select your Organizational Unit:

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



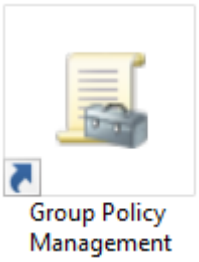
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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.

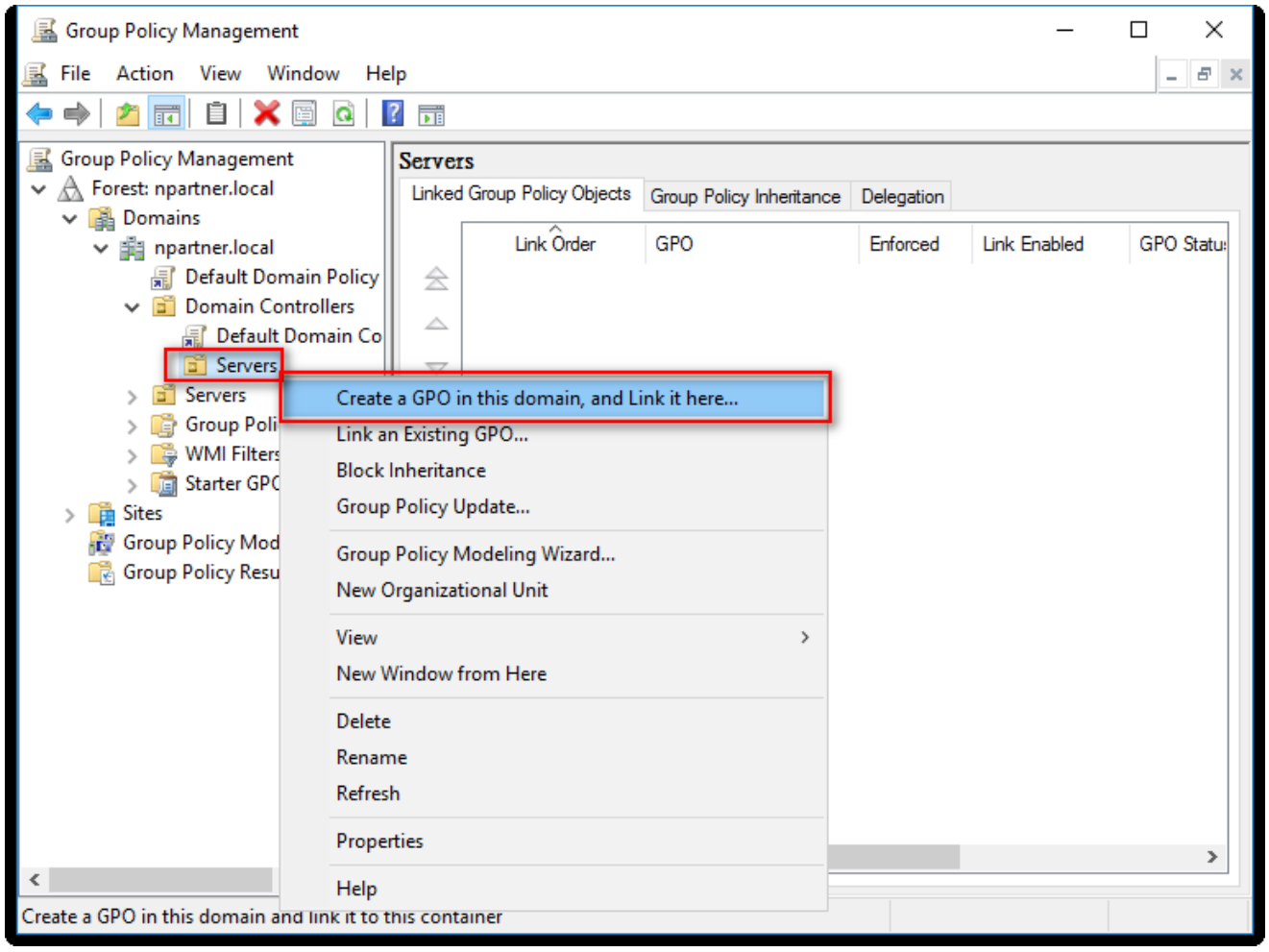


5.2 Group Policy Settings

(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.”

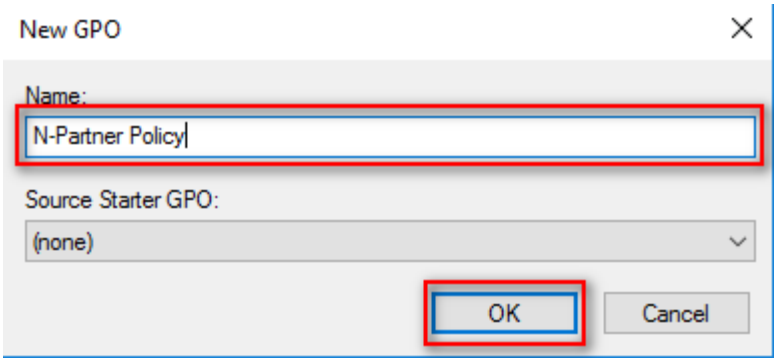


(3) Enter your Group Policy Object Name

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.

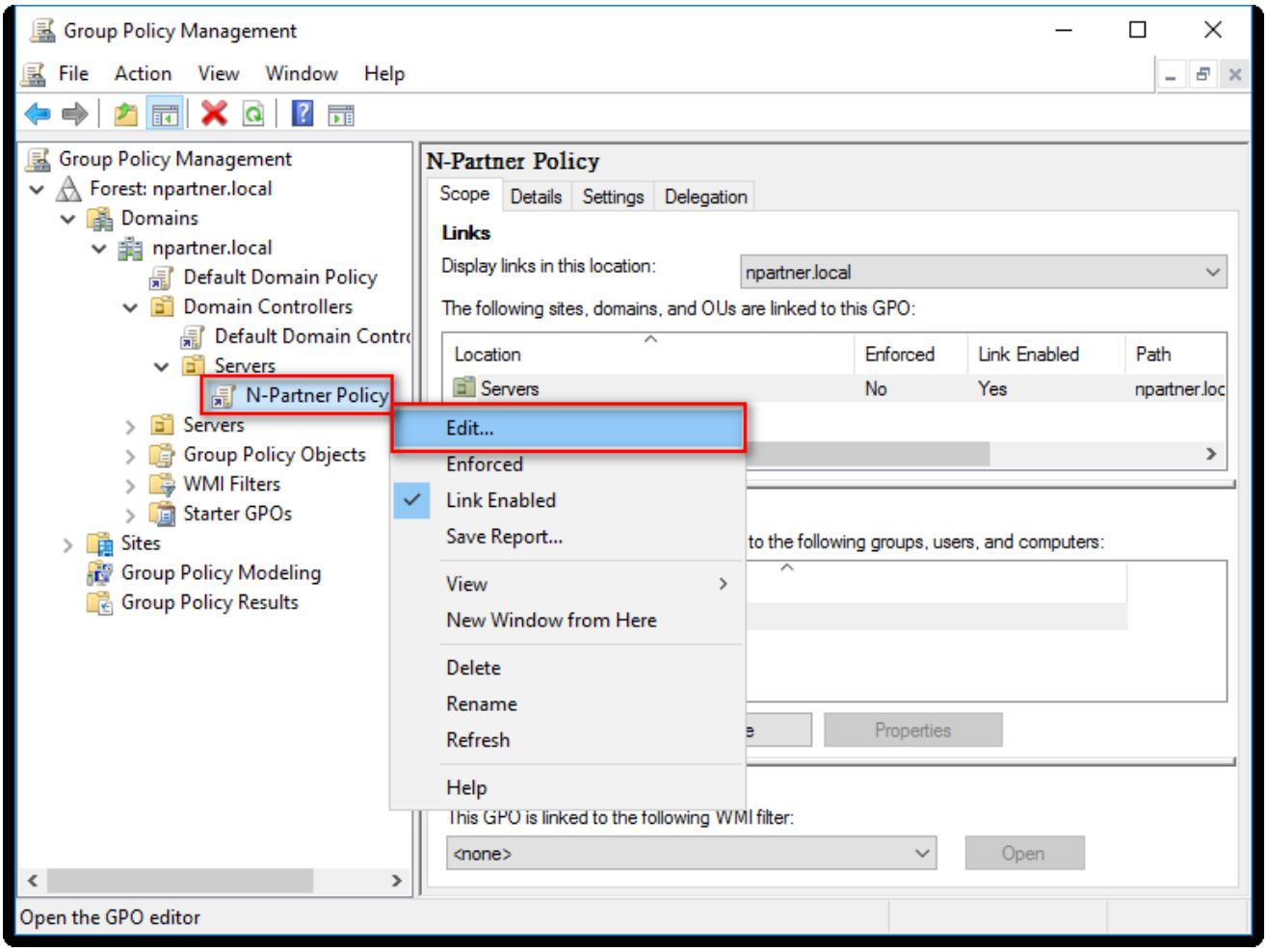
Then click “Edit.”



(4) Edit your Group Policy Object

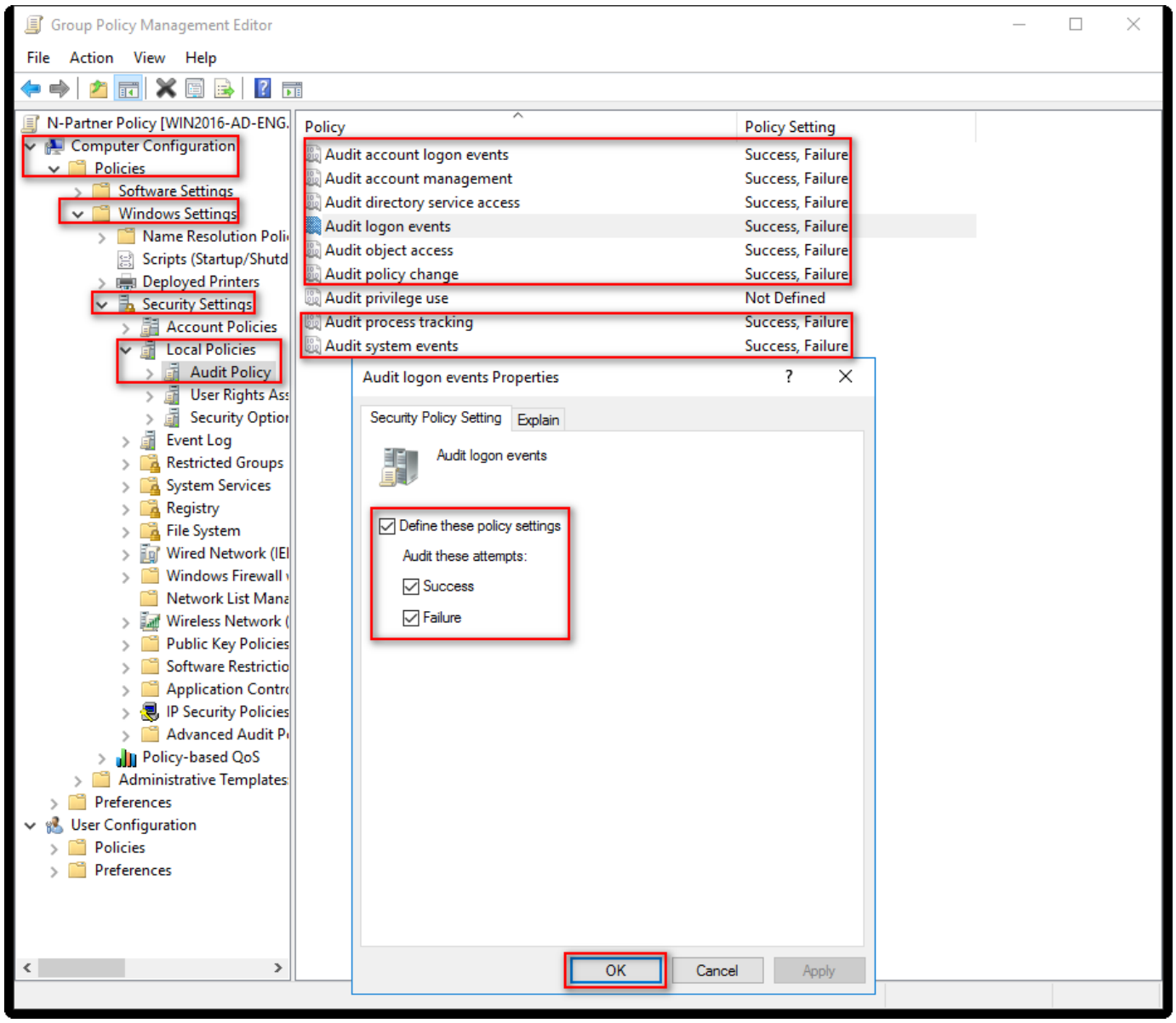
In your group policy object, (in this example, it is “N-Partner Policy”)

right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

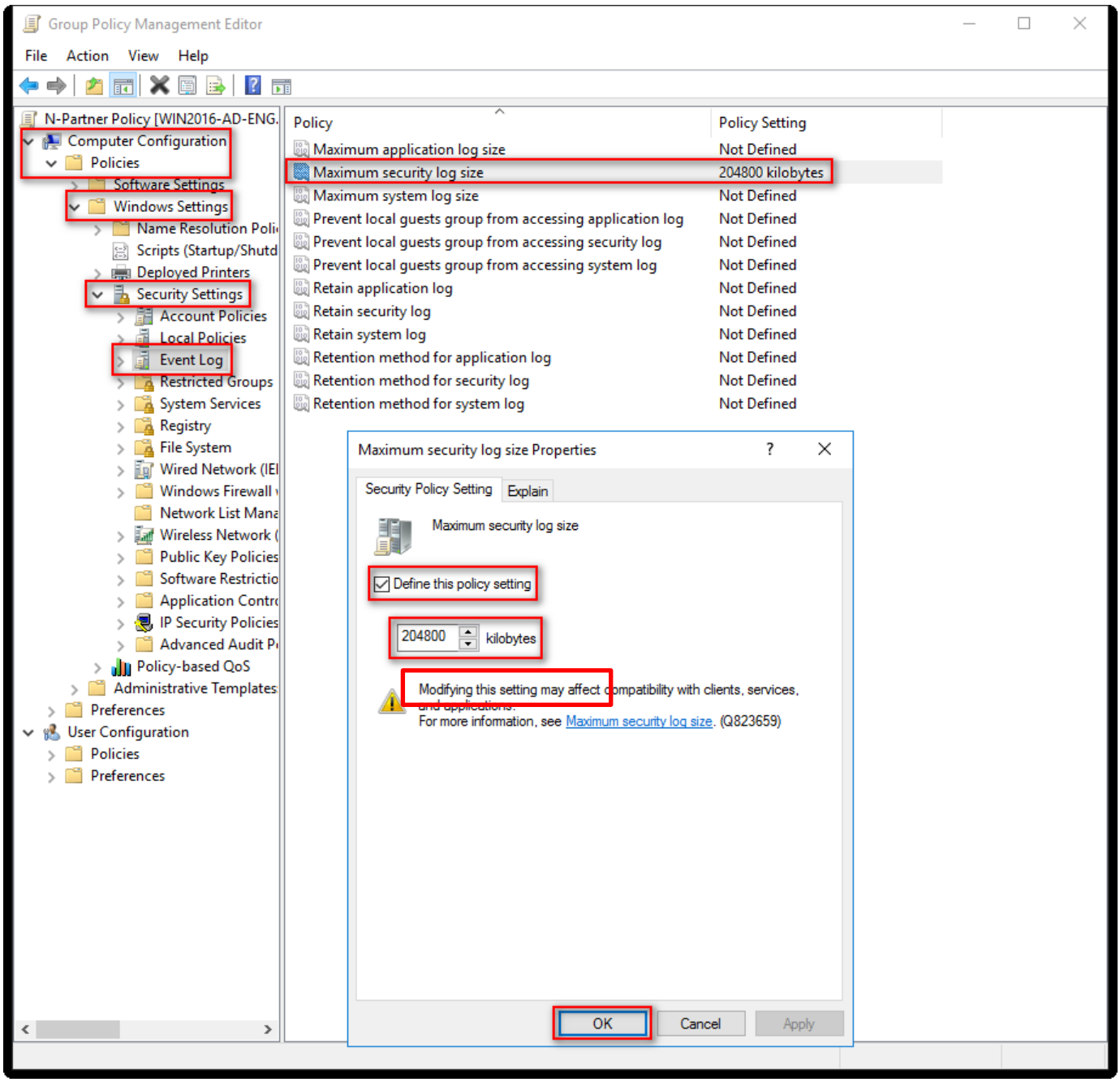
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “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

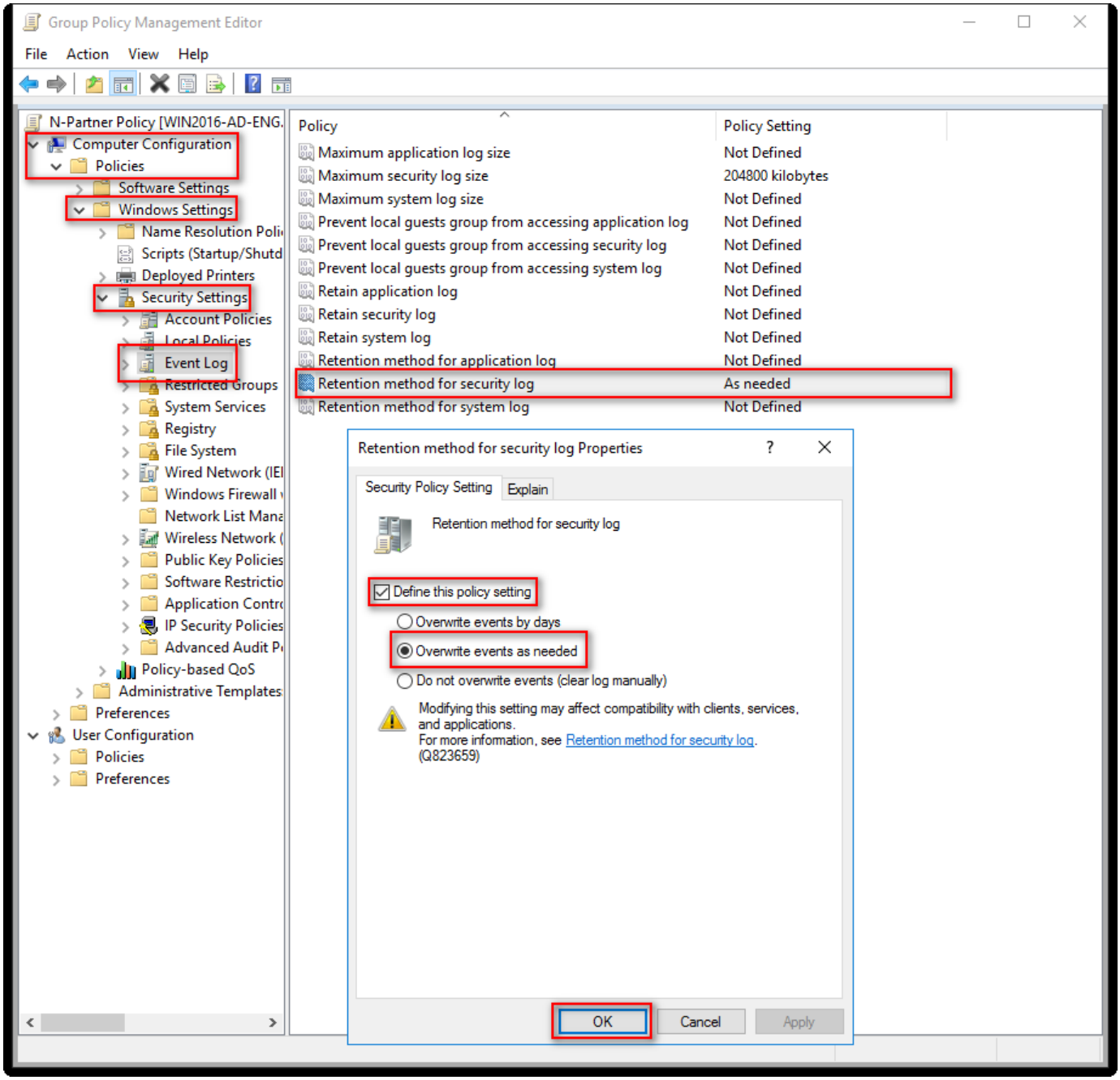
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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

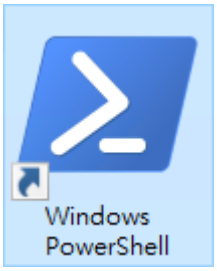


(7) Event Logs: Retention Method for Security Log

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.”

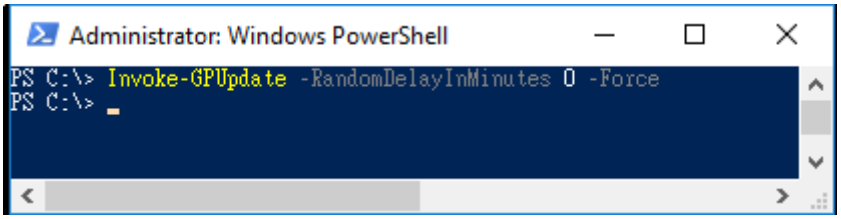


(8) Open “Windows PowerShell.”



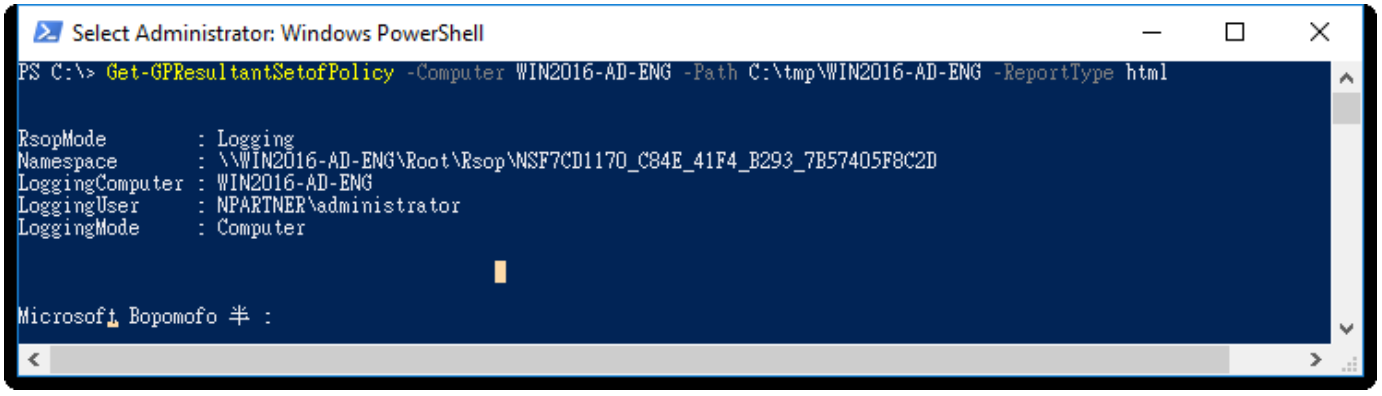
(9) Enter the command below to refresh group policy.

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



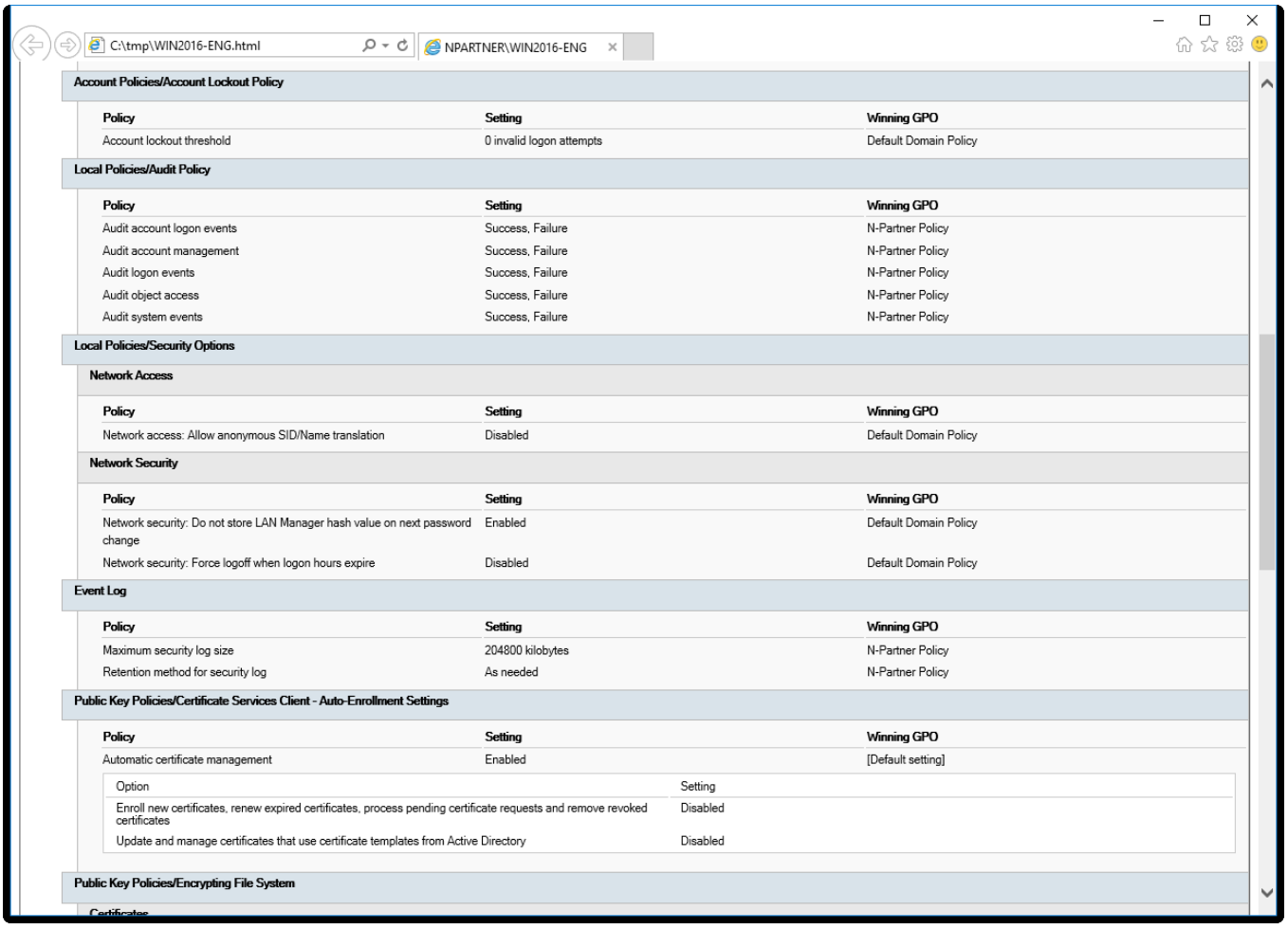
(10) Enter the command below to generate server group policy report.

```
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.



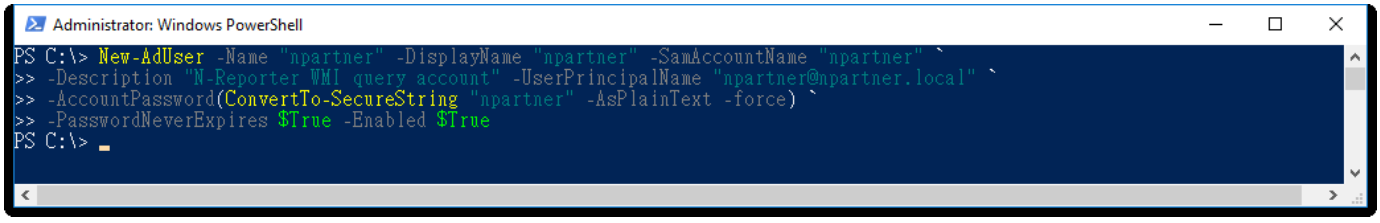
5.3 Add a Non-Admin Account

5.3.1 Add Users

(1) Open “Windows PowerShell.”

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

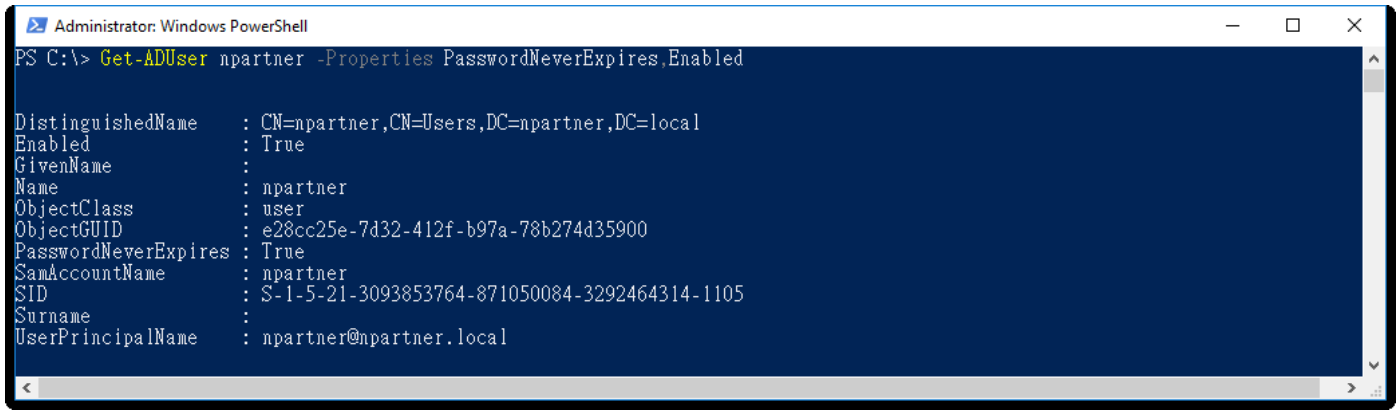
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



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
```



5.3.2 Configure DCOM Permissions

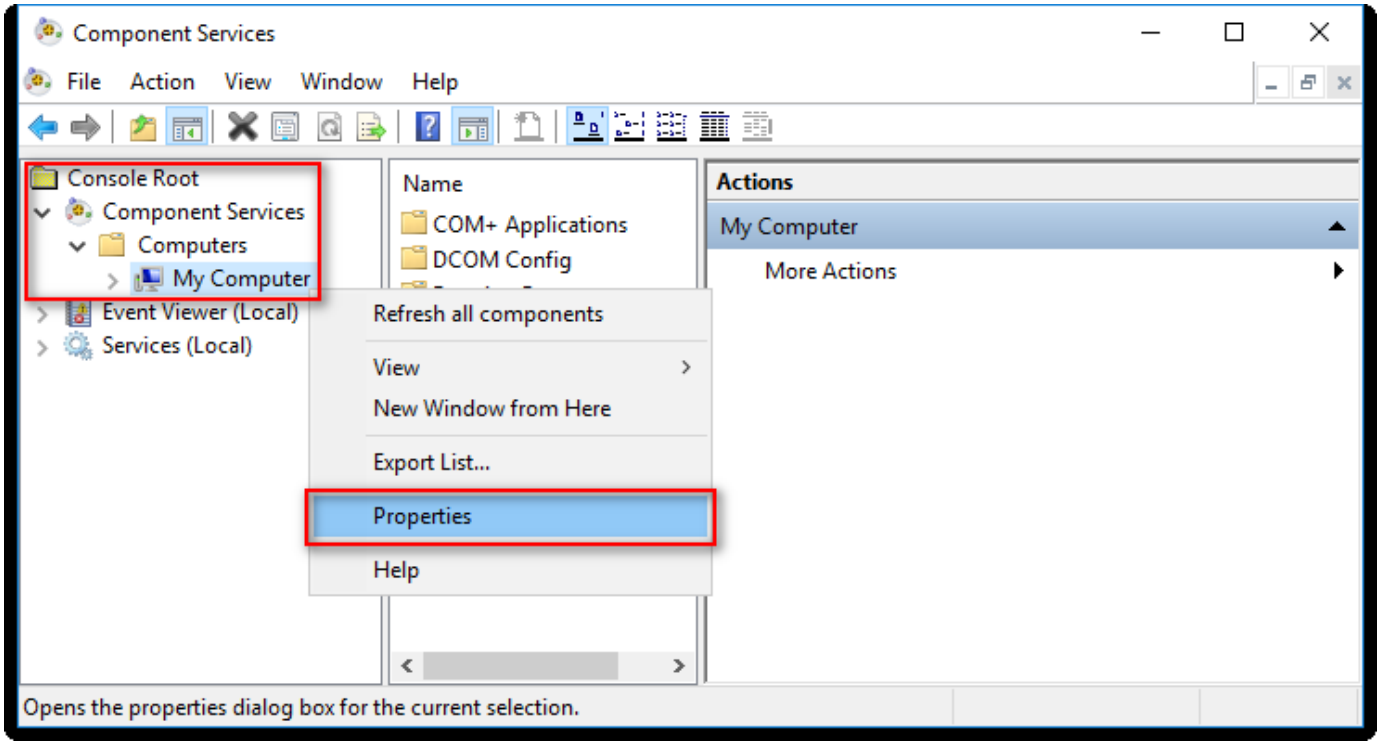
(1) Open “Windows PowerShell.”

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

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

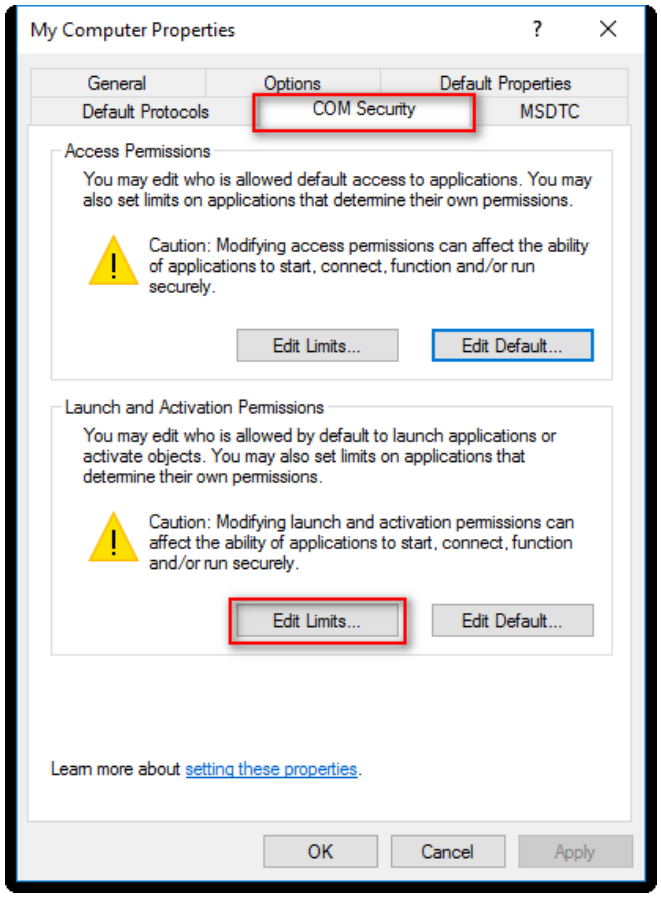
(3) Edit Computer Properties

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



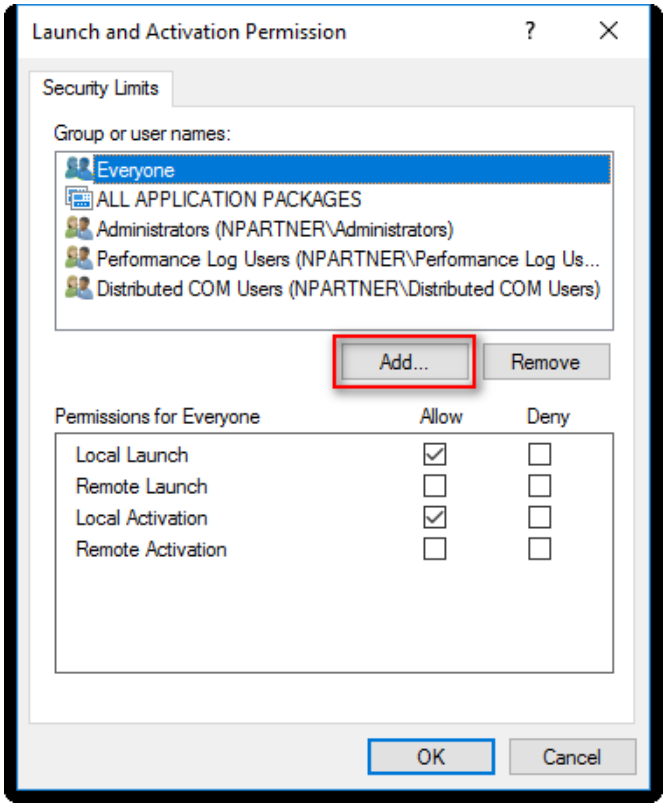
(4) Enable Permissions

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



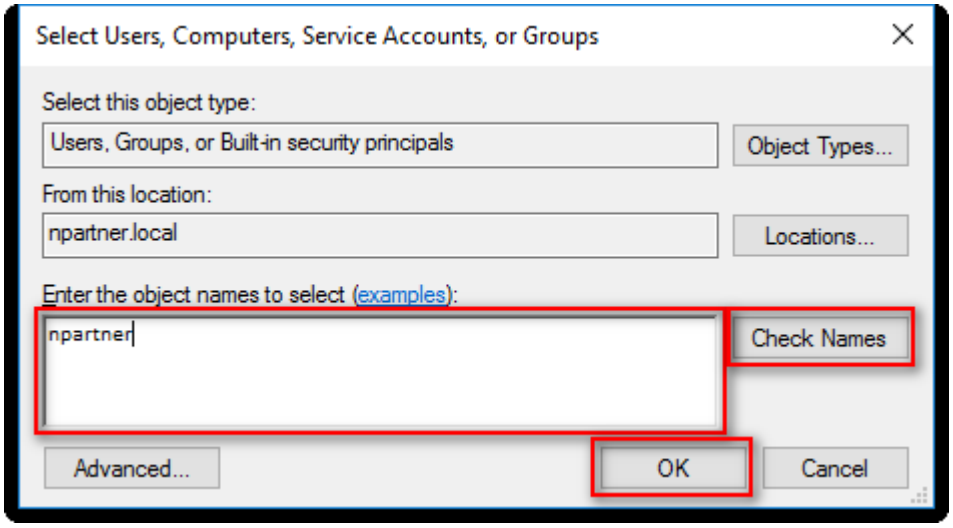
(5) Add DCOM User Permissions

Click “Add.”



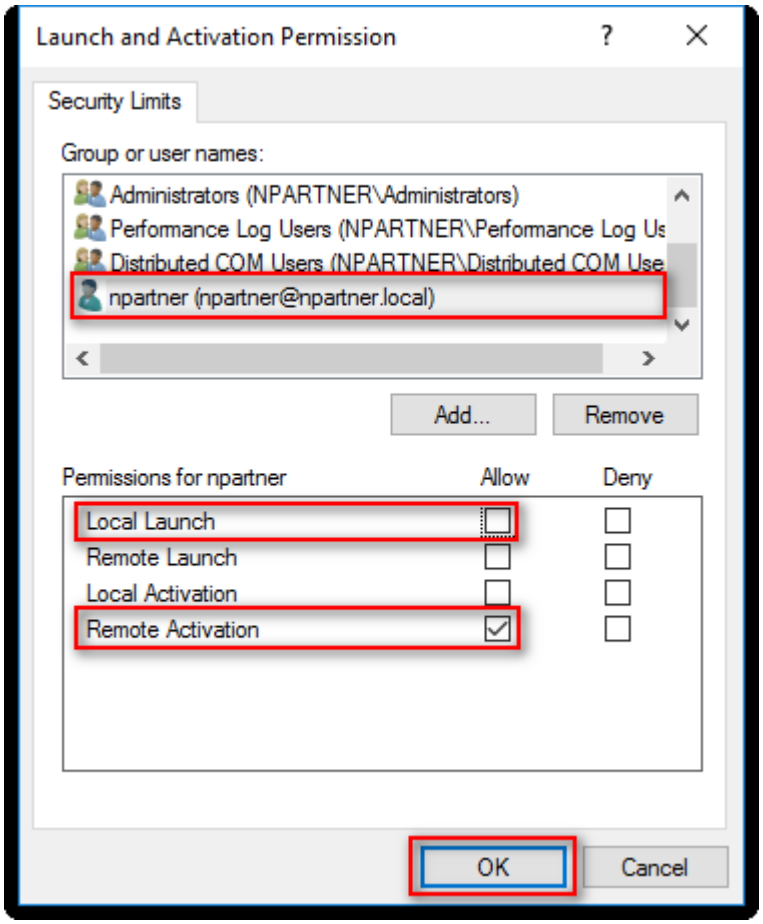
(6) Enter your Username

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

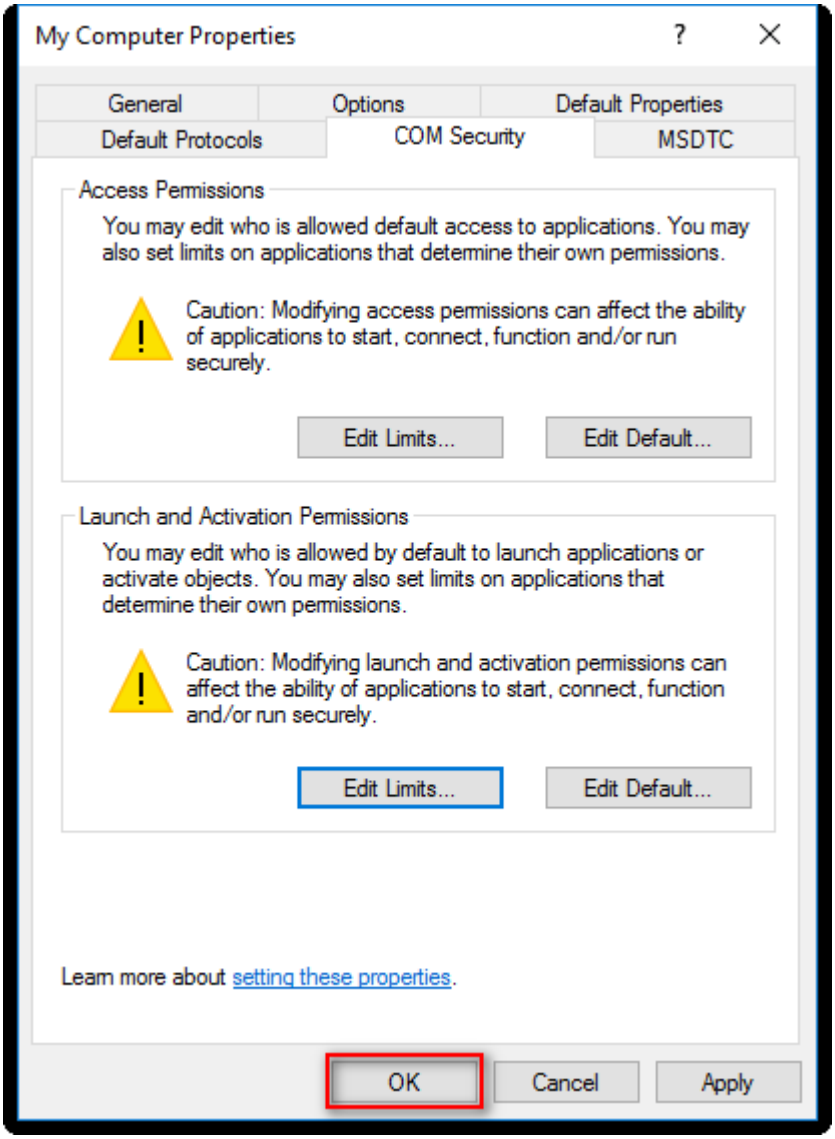


(7) Set User Permissions

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



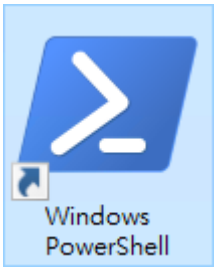
(8) Click “OK.”



5.3.3 Configure WMI Permissions

5.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”

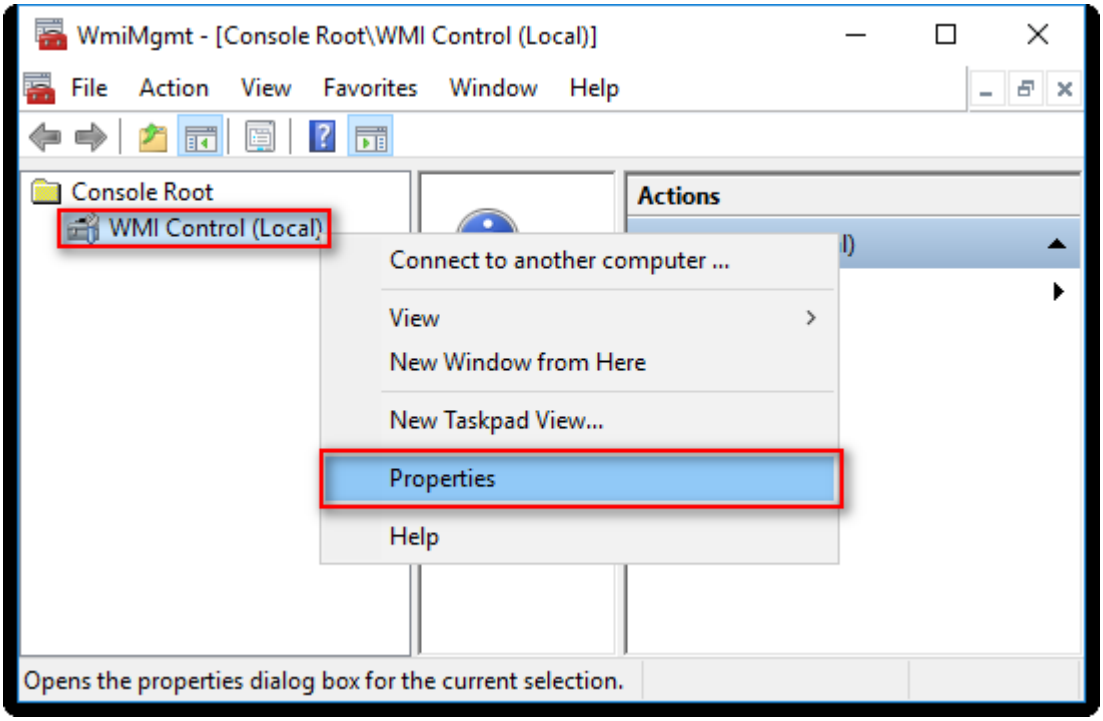


(2) Enter the command below to enable component services.

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

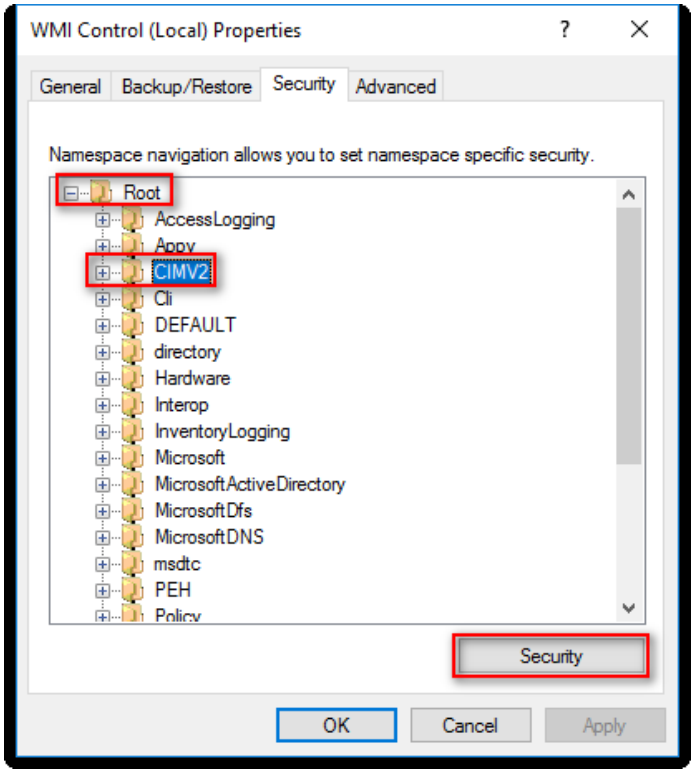
(3) Edit WMI Control

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



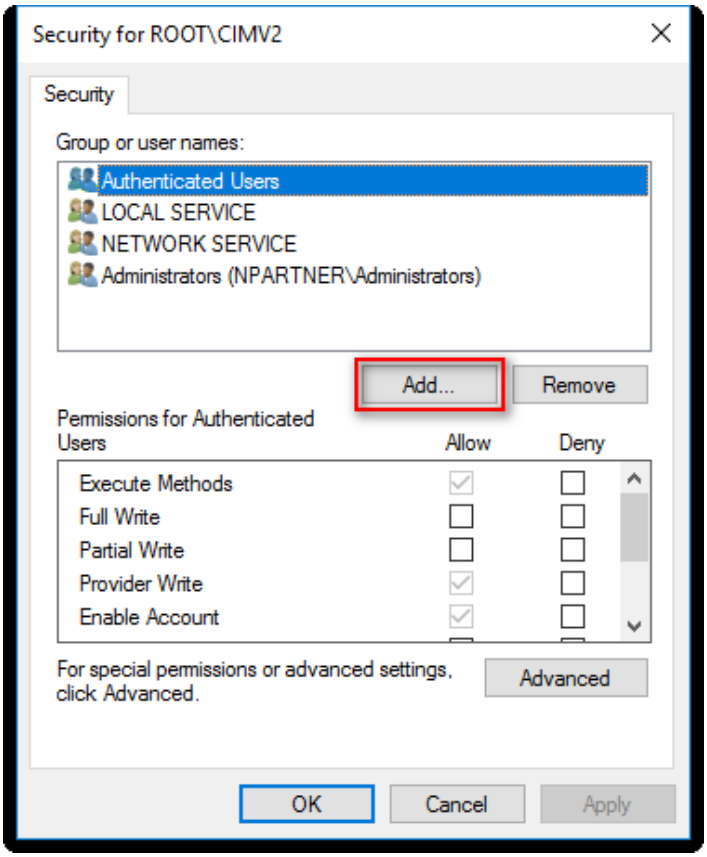
(4) Edit CIMV2 Security

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



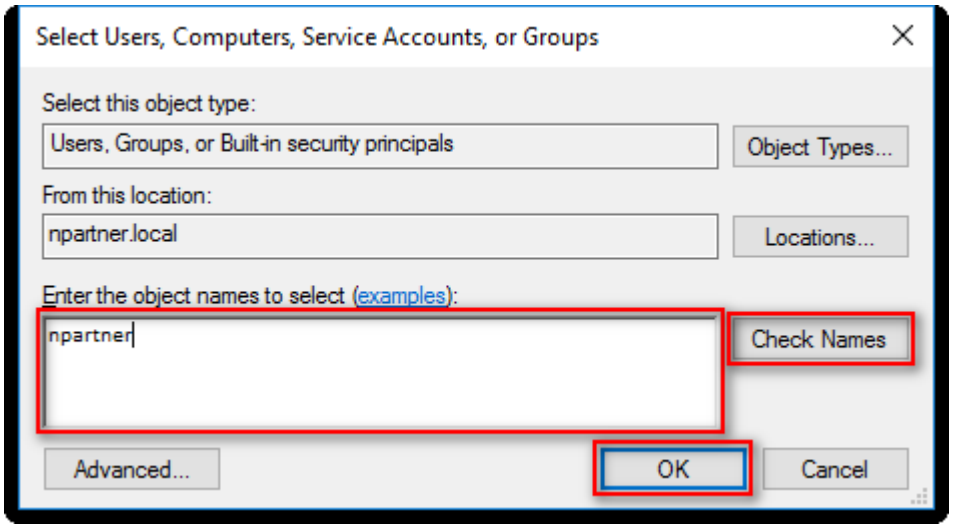
(5) Add WMI User Permissions

Click “Add.”



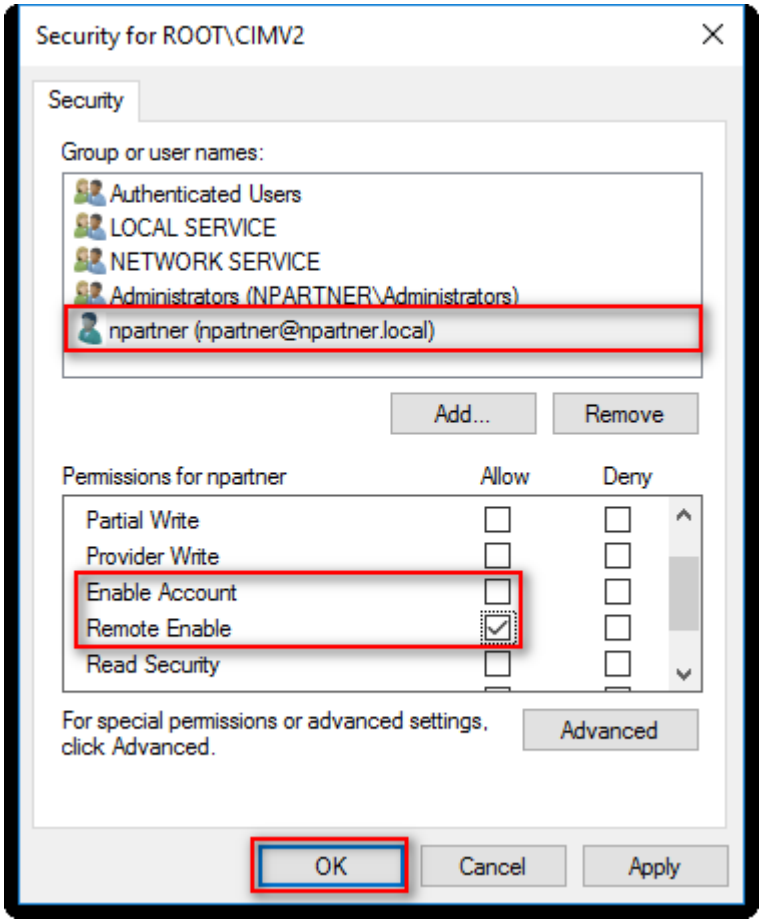
(6) Enter User

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

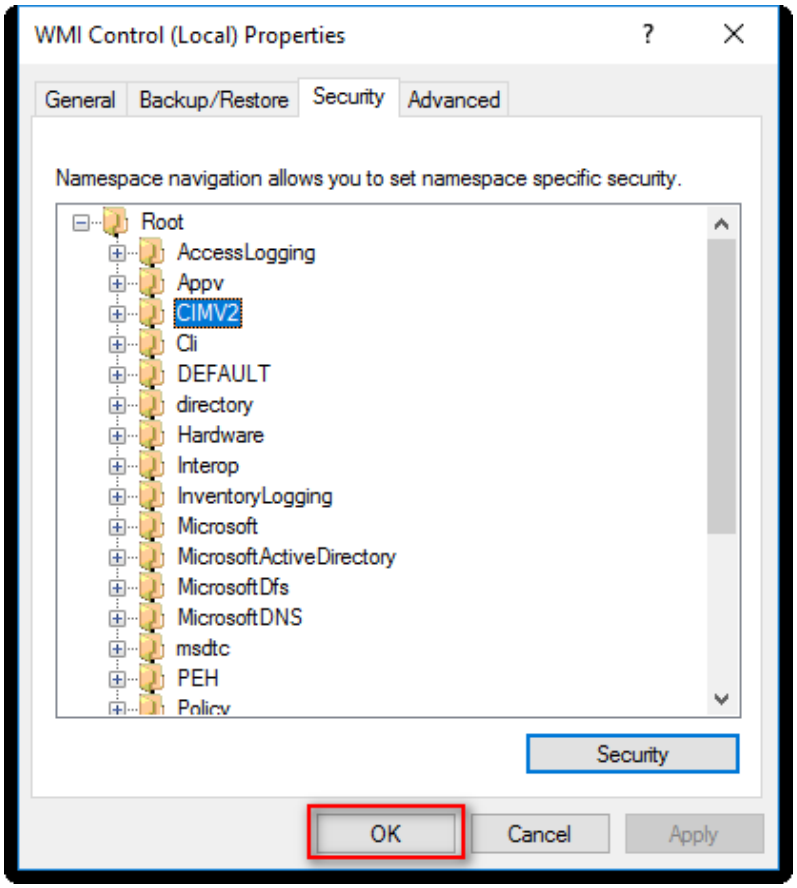


(7) Set User Permissions

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

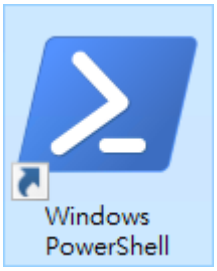


(8) Click “OK.”



5.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”

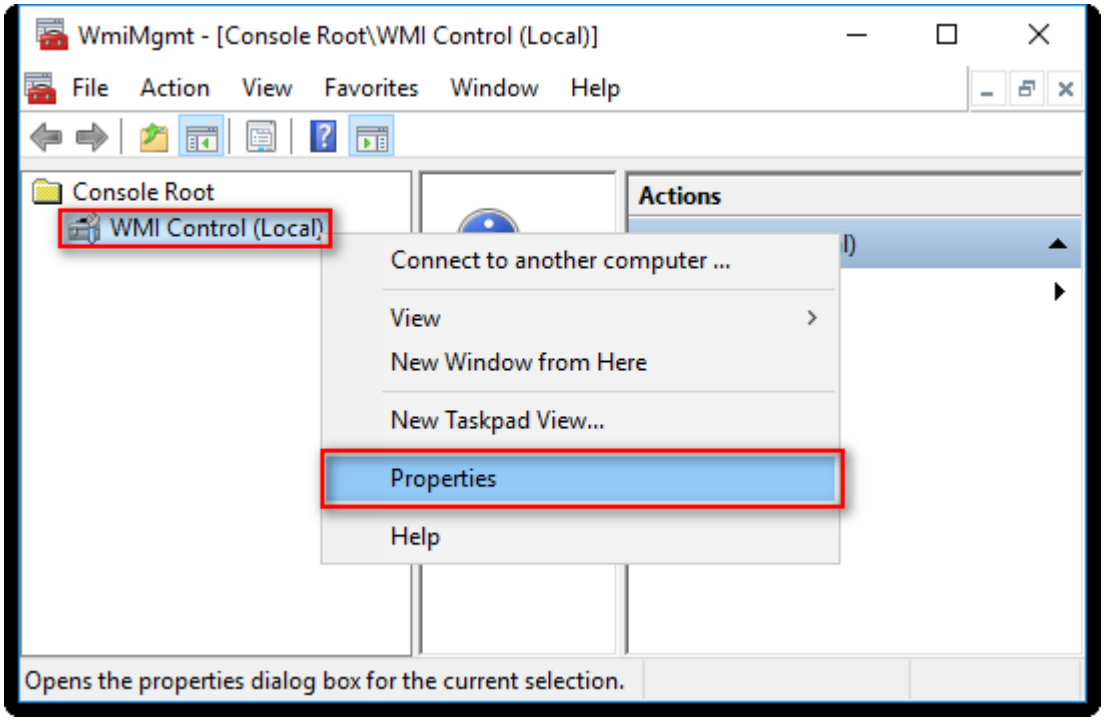


(2) Enter the command to enable component services.

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

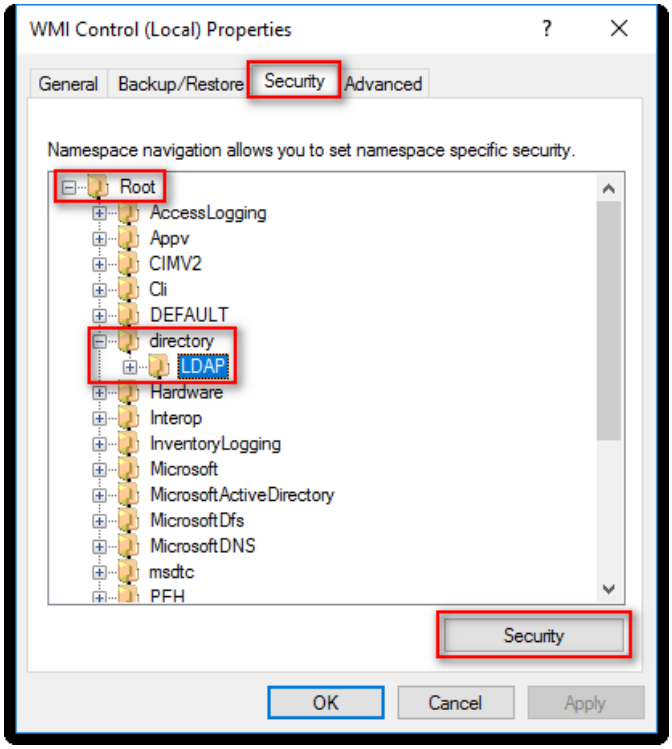
(3) Edit WMI Control

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



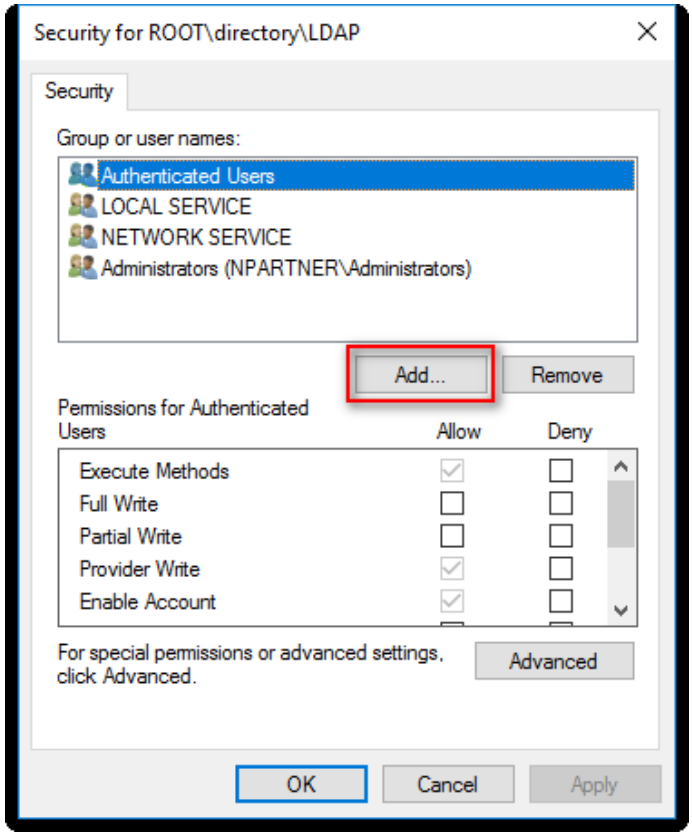
(4) Edit LDAP Security

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



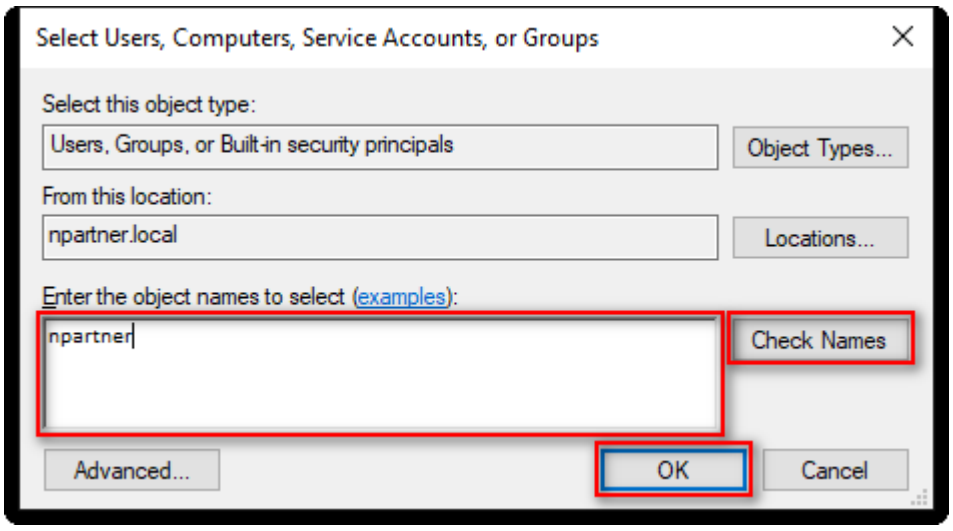
(5) Add WMI User Permissions

Click “Add.”



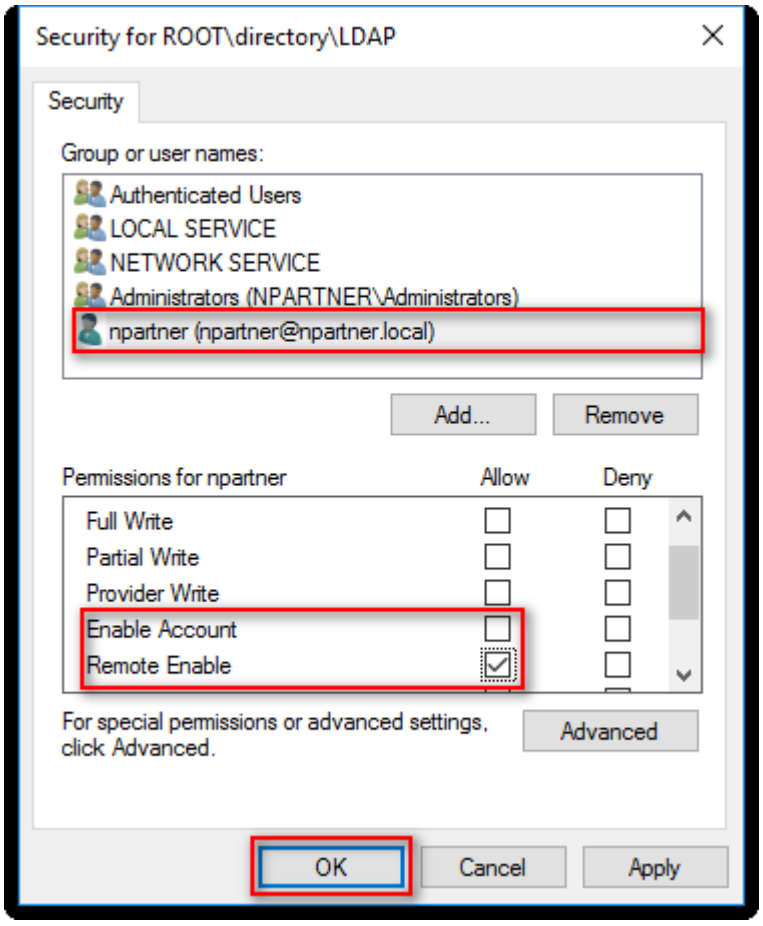
(6) Enter Your Username

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

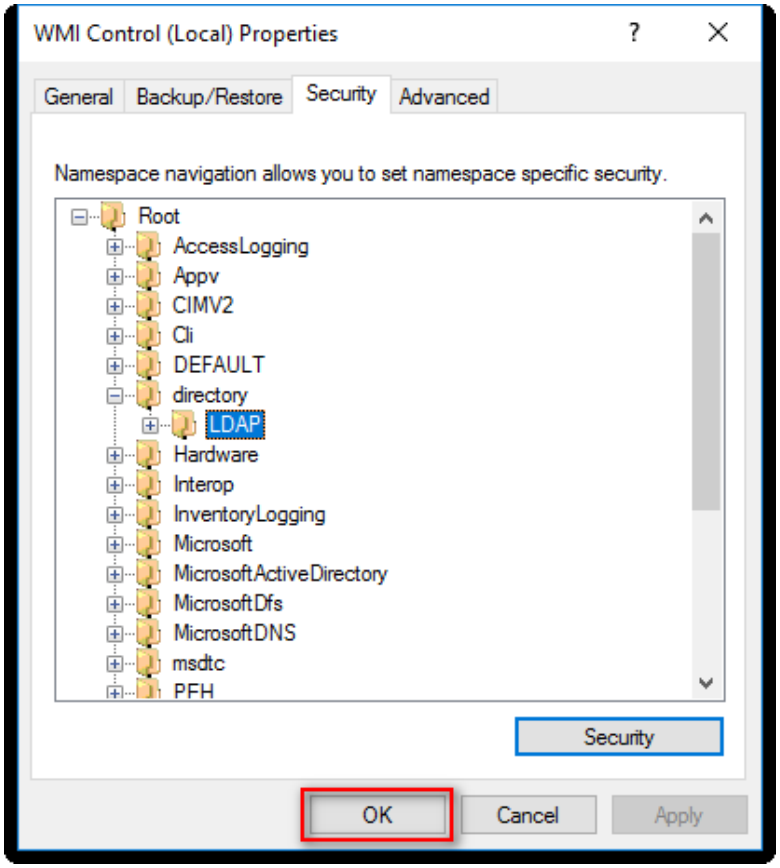


(7) Set Your User Permissions

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

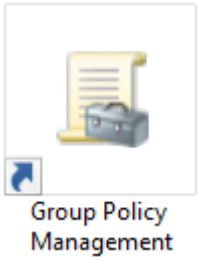


(8) Click “OK.”



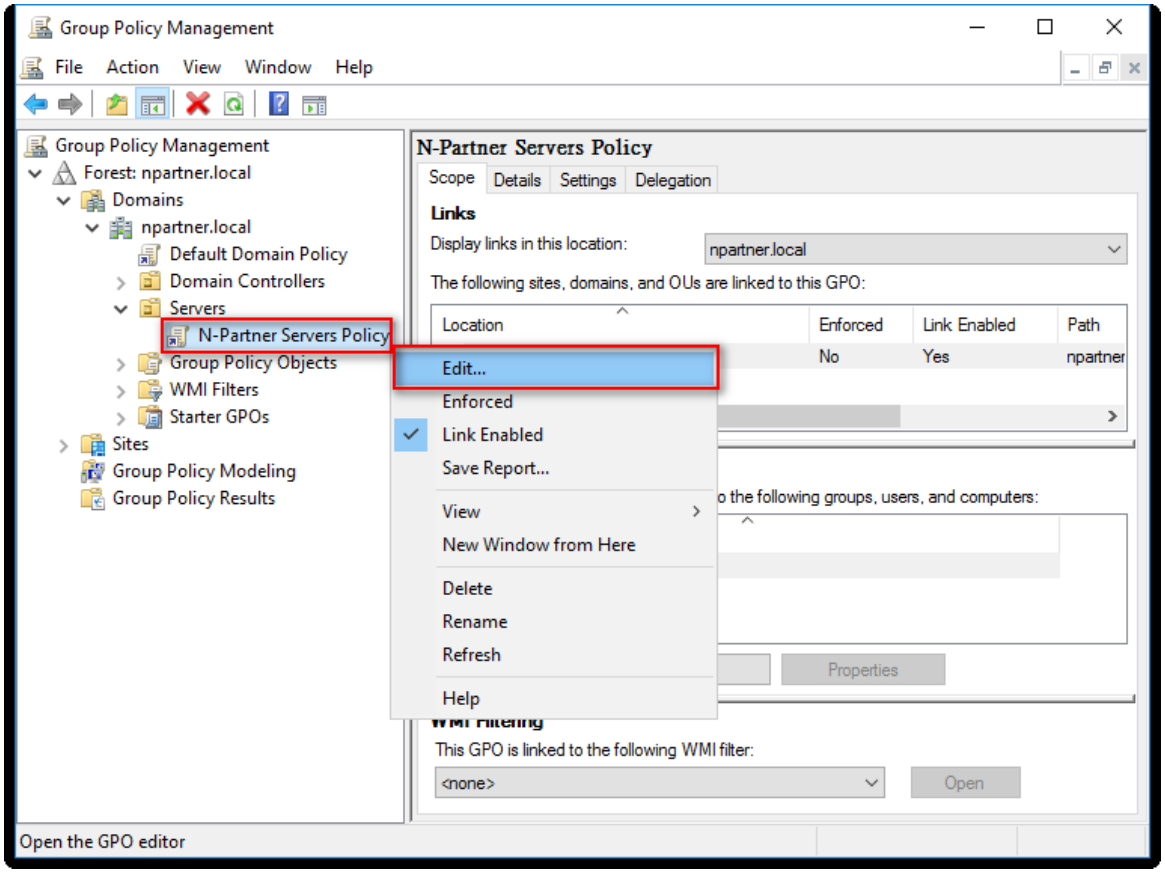
5.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object (GPO)

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

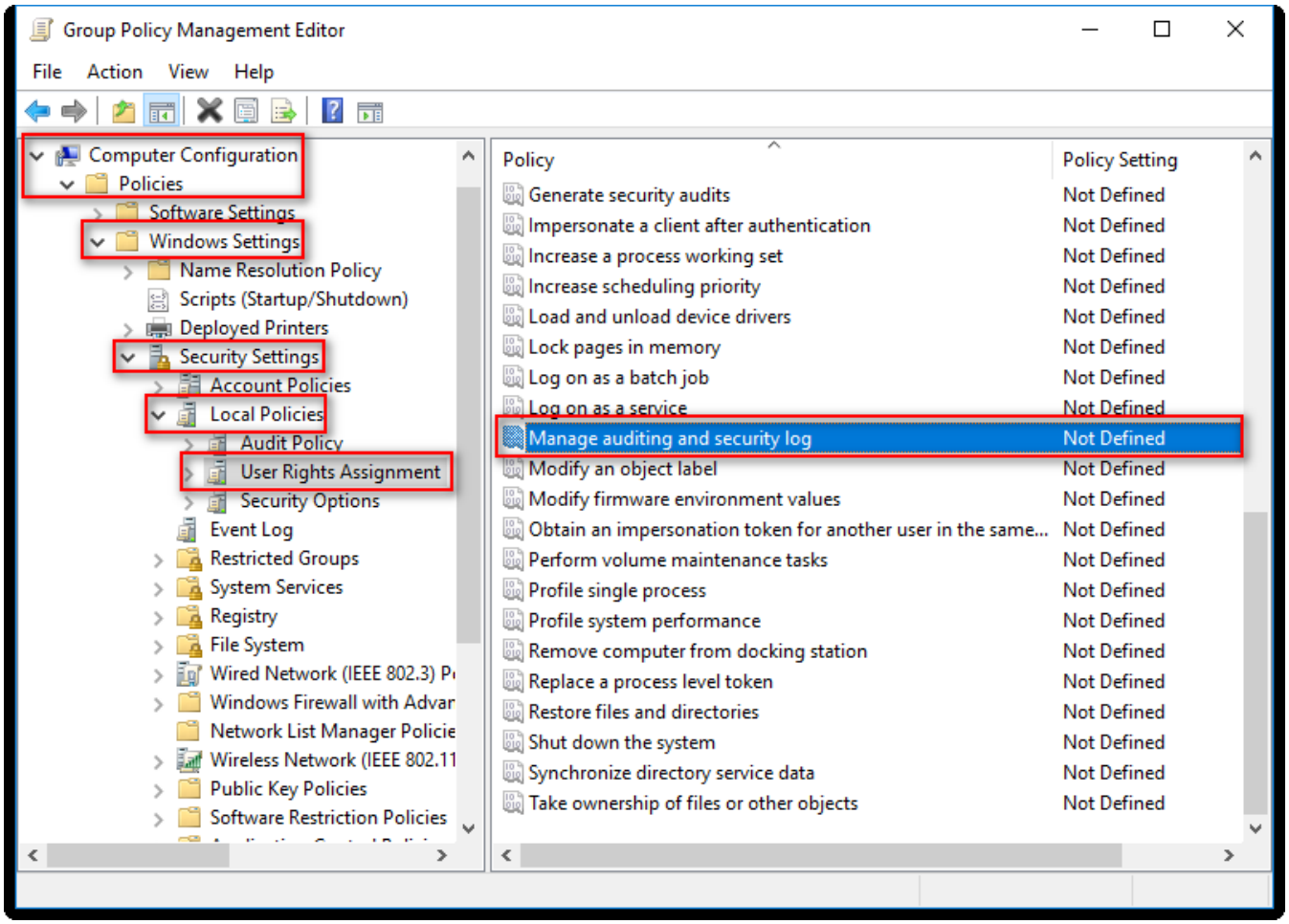


(3) Configure Log Permissions

Navigate to:

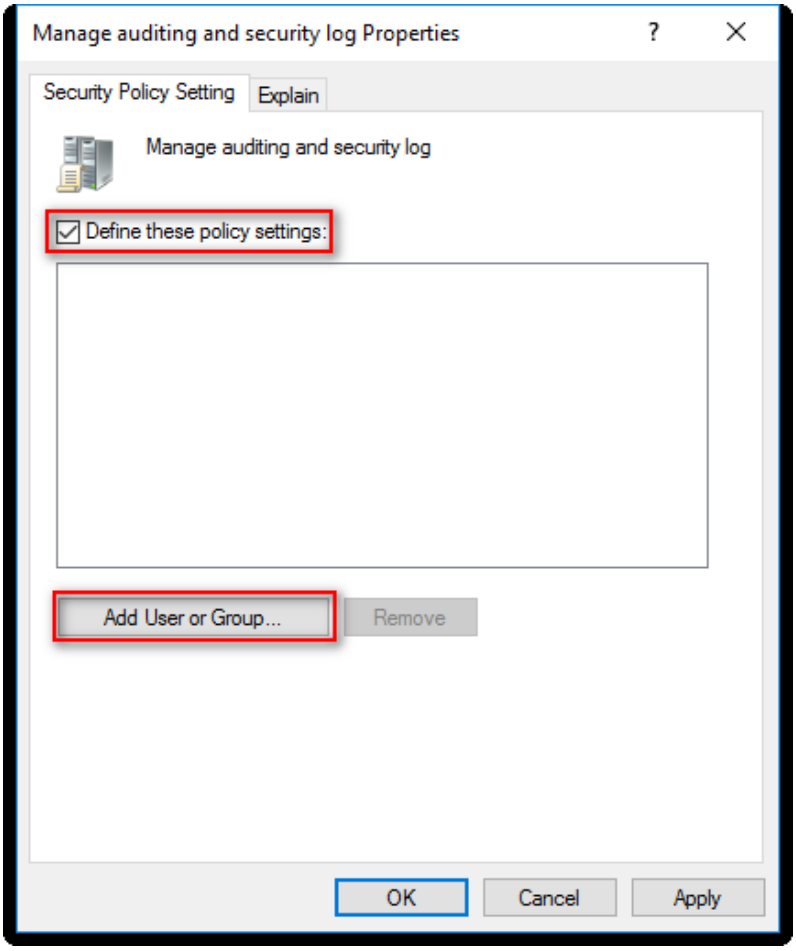
“Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

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



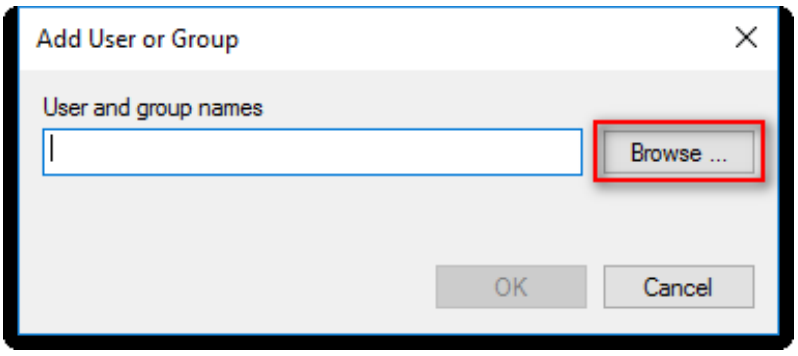
(4) Add Audit Management Users

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



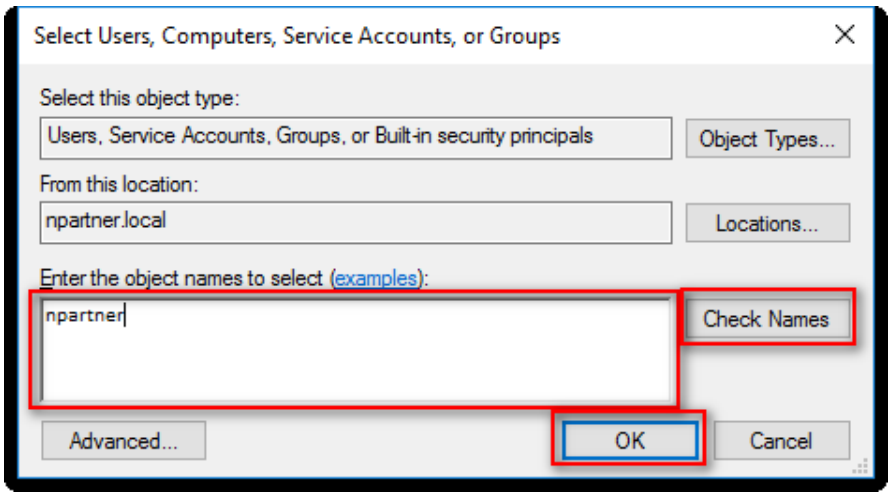
(5) Search for the User

Click “Browse.”



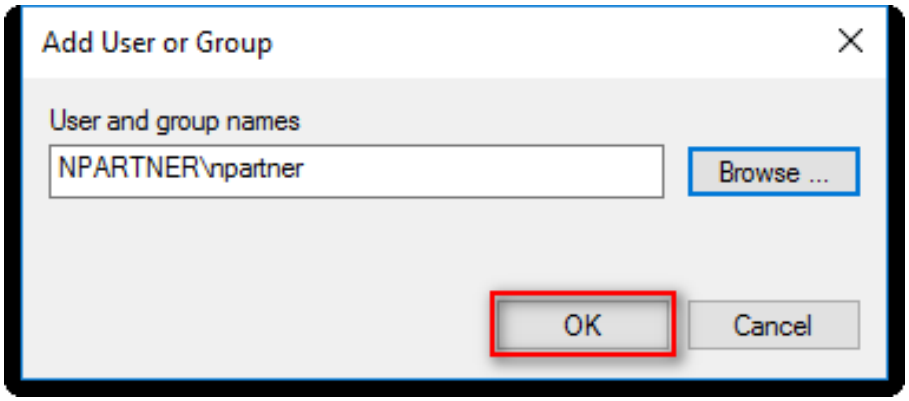
(6) Specify the User

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



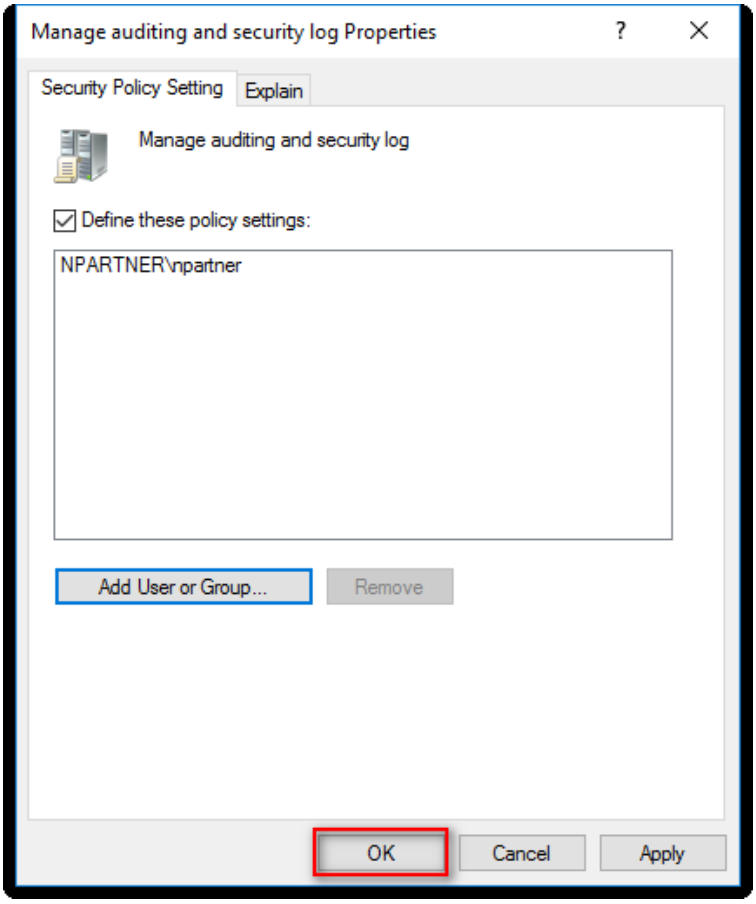
(7) Confirm the User

Click “OK.”



(8) Confirm the Logging Settings

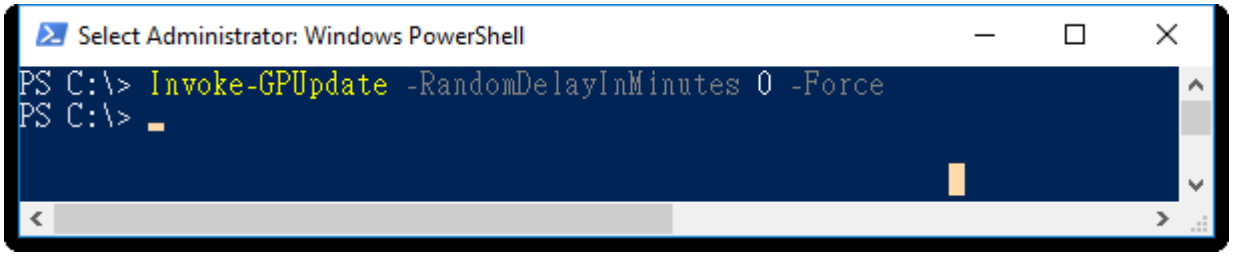
Click “OK” to apply the configuration.



(9) Open “Windows PowerShell.”

(10) Enter to update group policy:

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

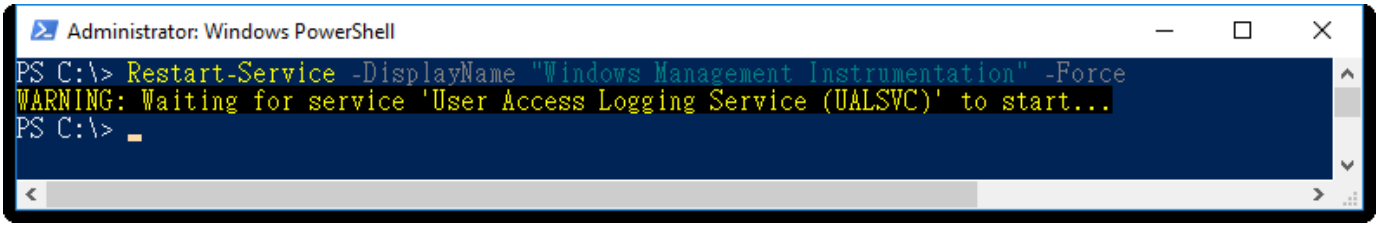


5.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”

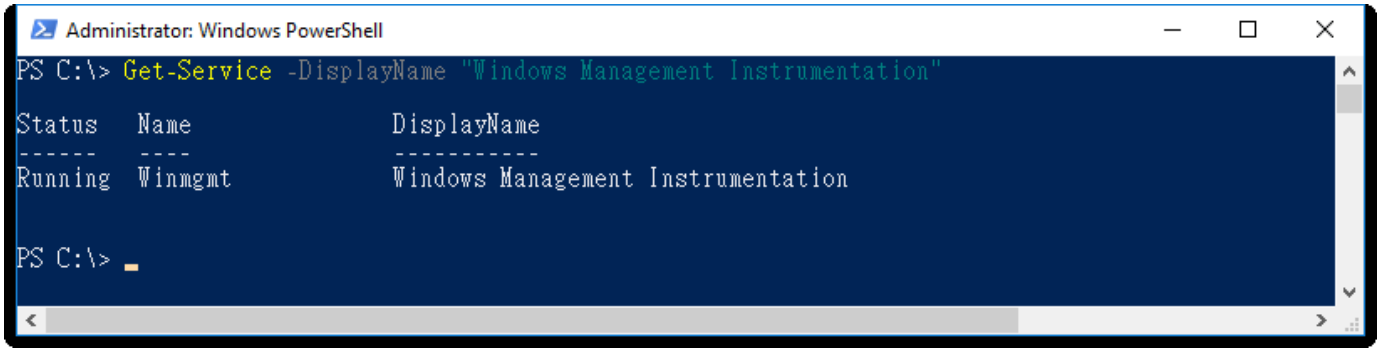
(2) Enter the command below to restart the WMI service:

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



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

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

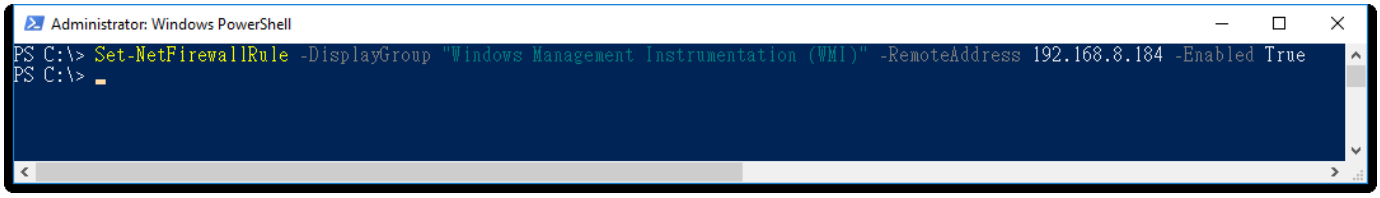


5.4 Configure the Firewall

(1) Open “Windows PowerShell.”

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

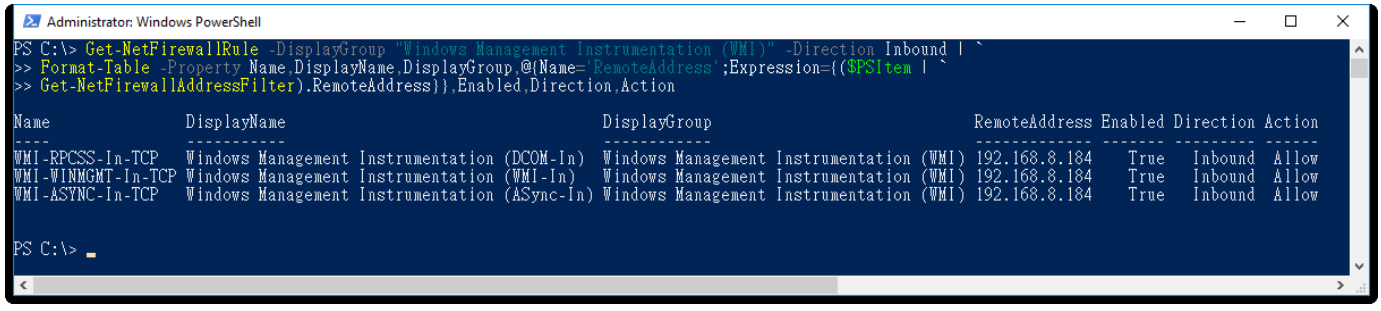
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -
RemoteAddress 192.168.8.184 -Enabled True
```



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
```

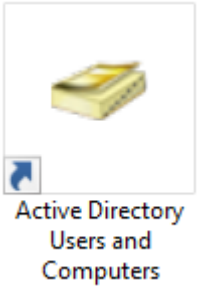


6. Windows 2019

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

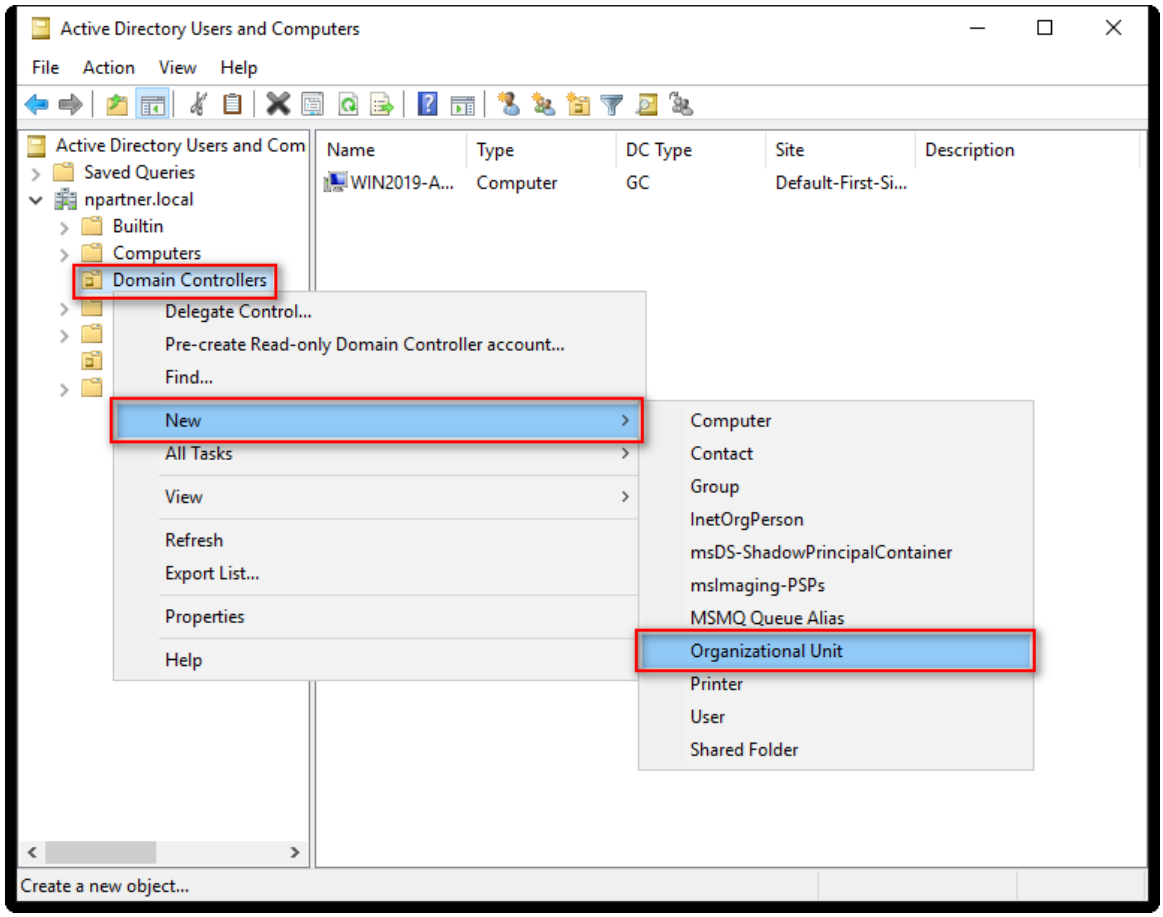
6.1 Organizational Unit Settings

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



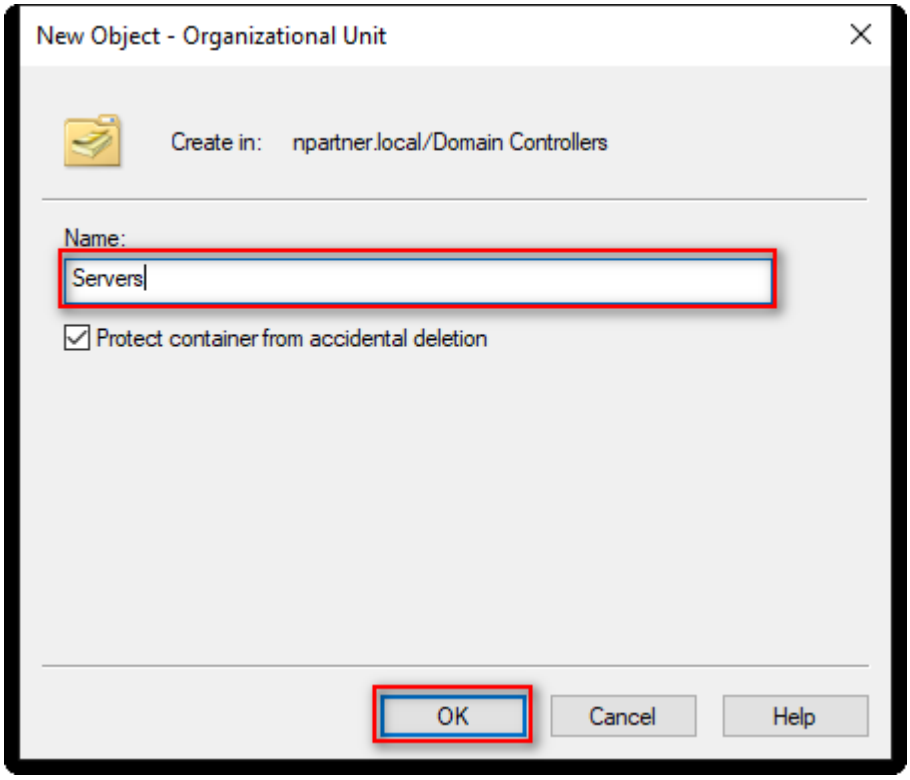
(2) Add an Organizational Unit

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



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

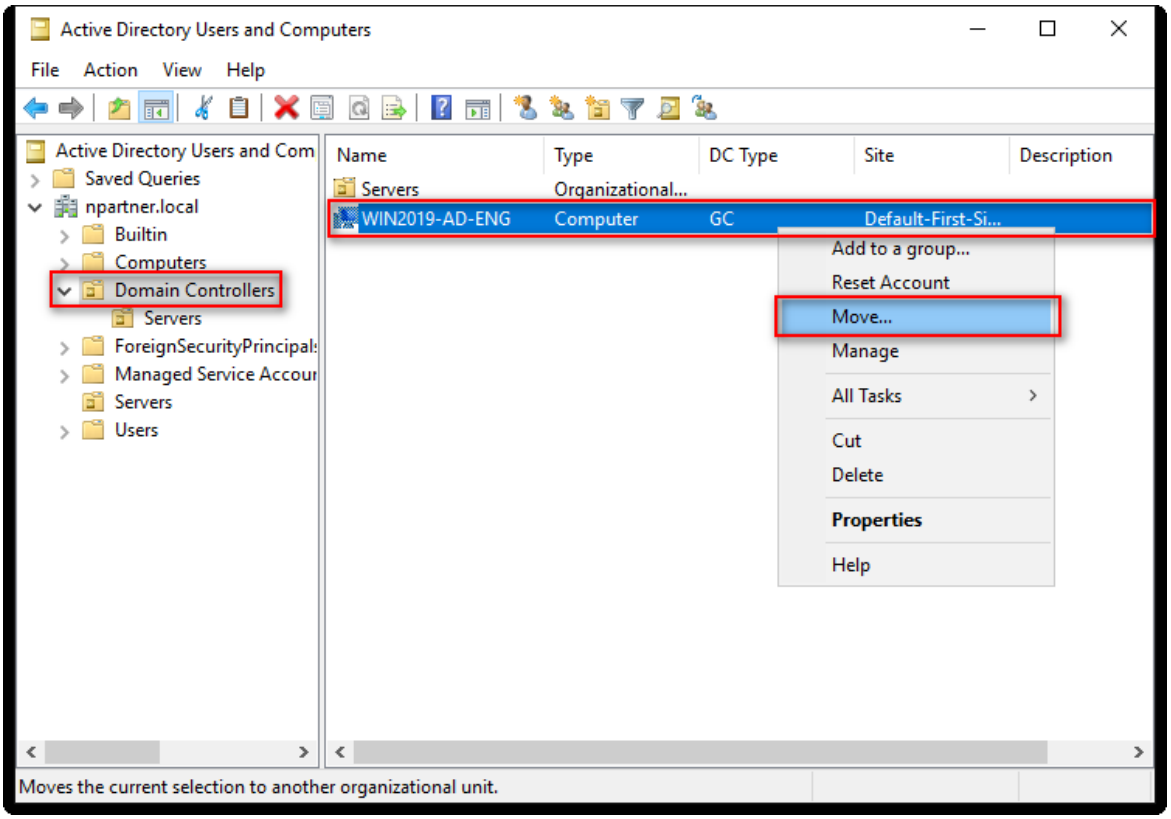
Note: Please create the organizational unit’s name according to the actual environment. -> Click “OK.”



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

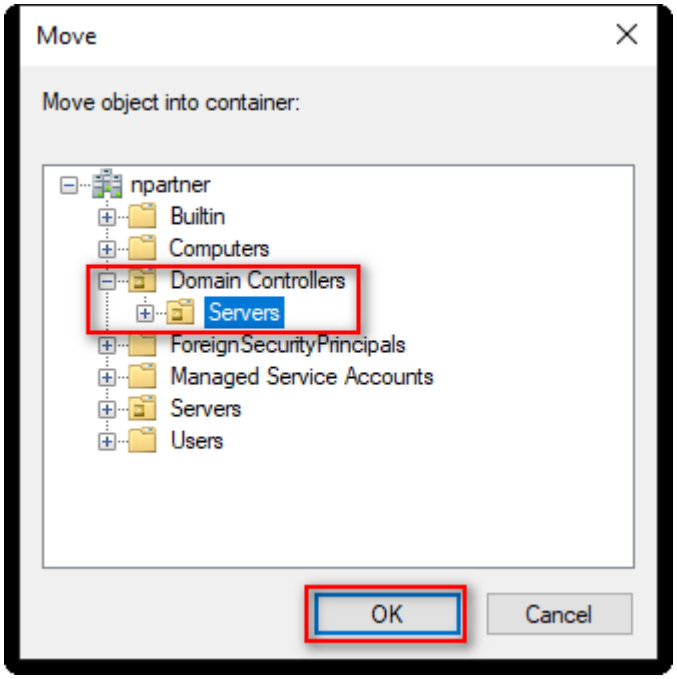
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2019-AD-ENG” server.

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



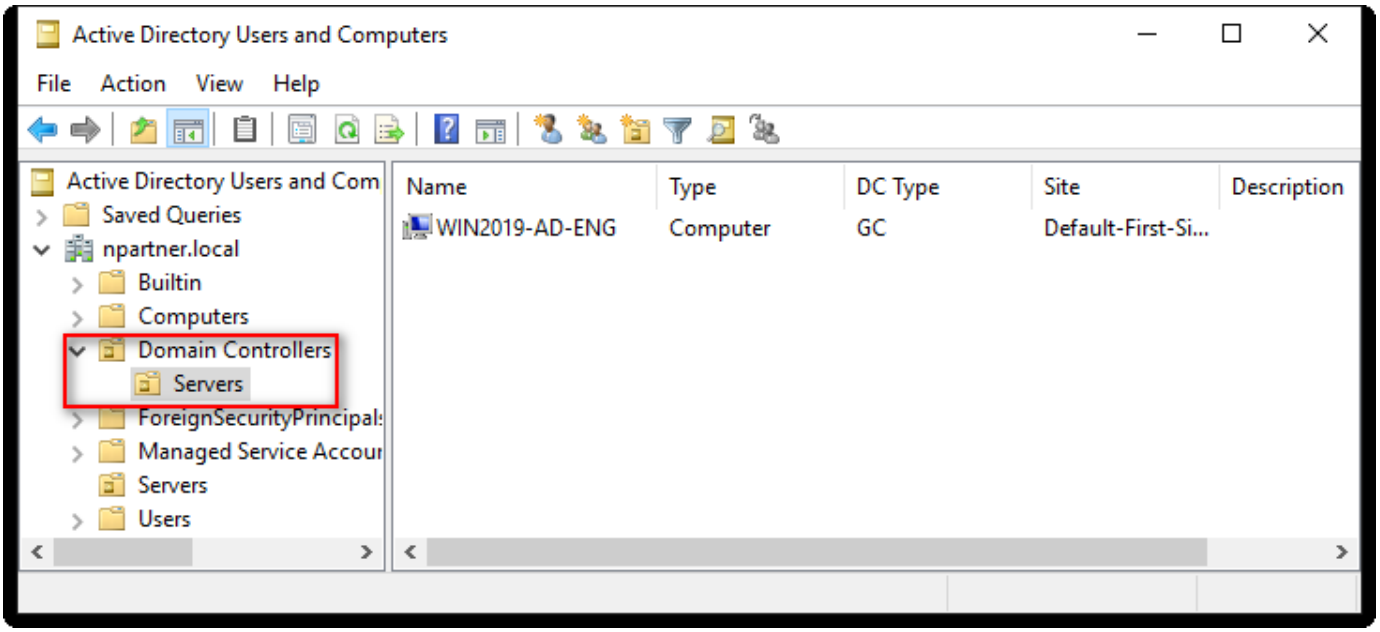
(5) Select your Organizational Unit:

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



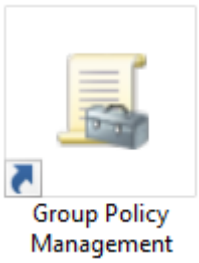
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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.

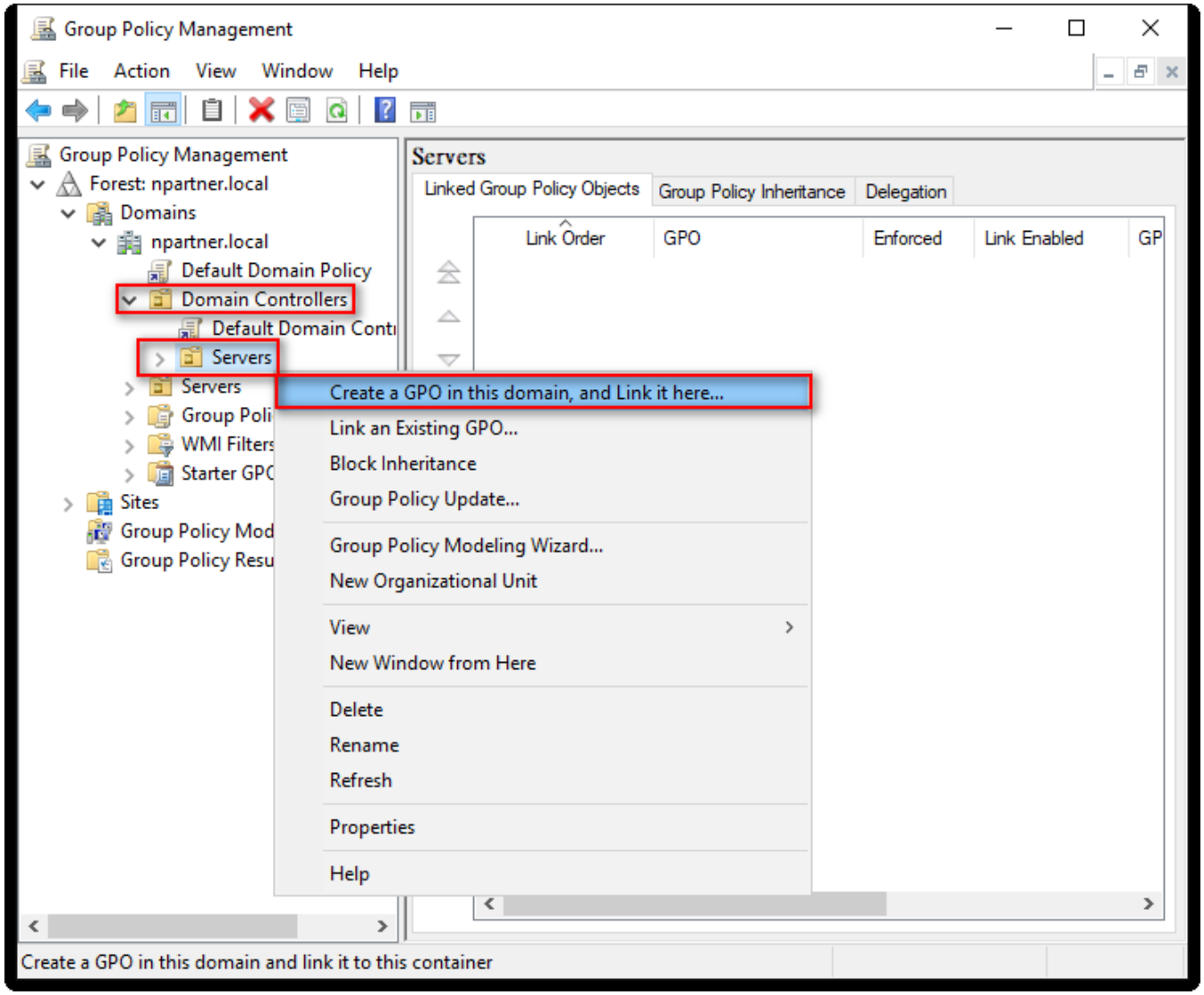


6.2 Group Policy Settings

(1) Click “Group Policy Management.”



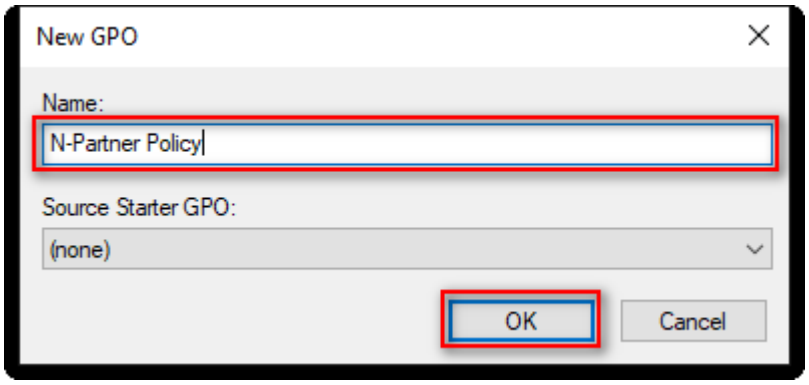
(2) In “Domain Controllers,” right-click on your organizational unit (in this example, it is “Servers”) and select “Create a GPO in this domain and Link it here.”



(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.

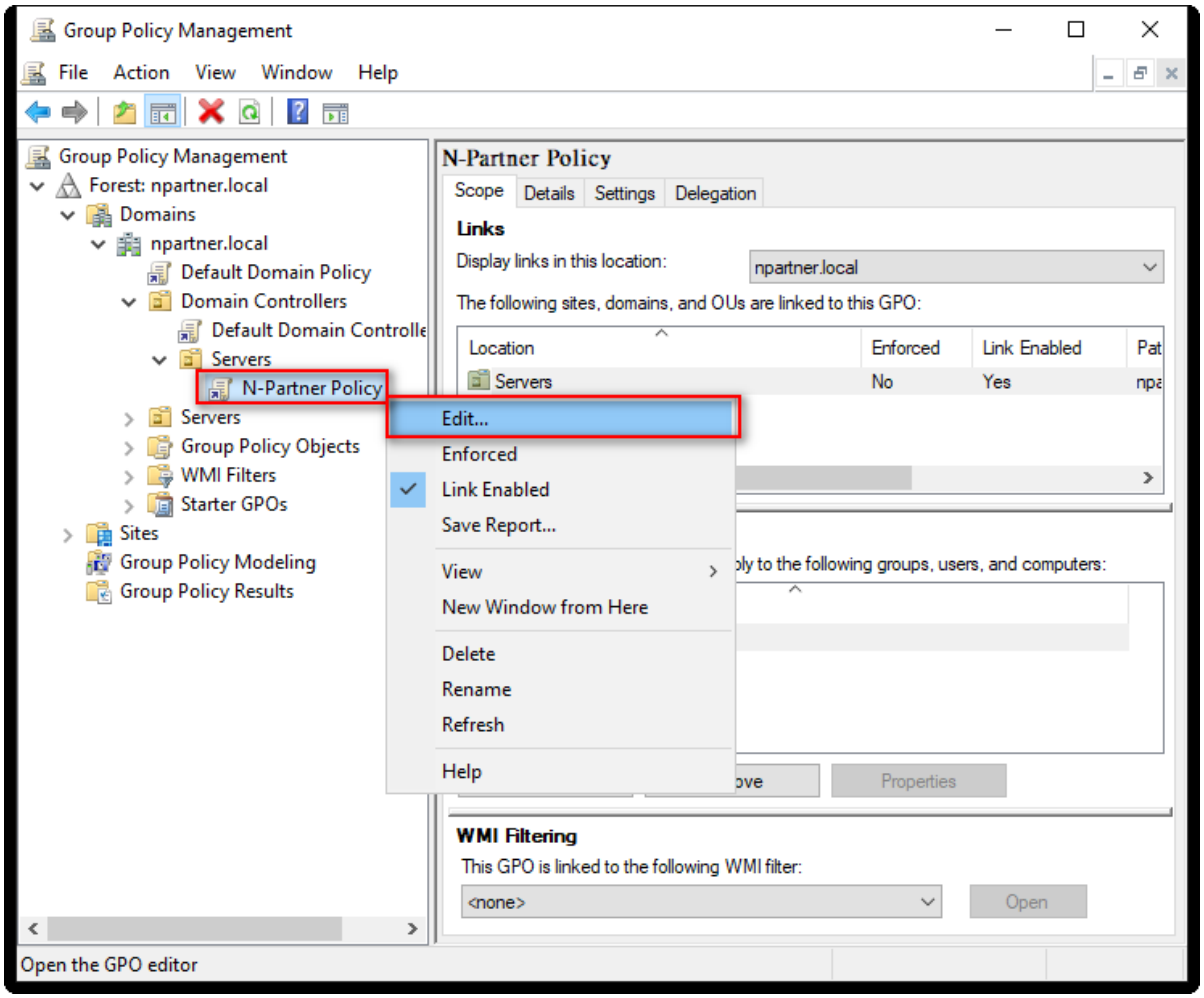
Then click “OK.”



(4) Edit your Group Policy Object

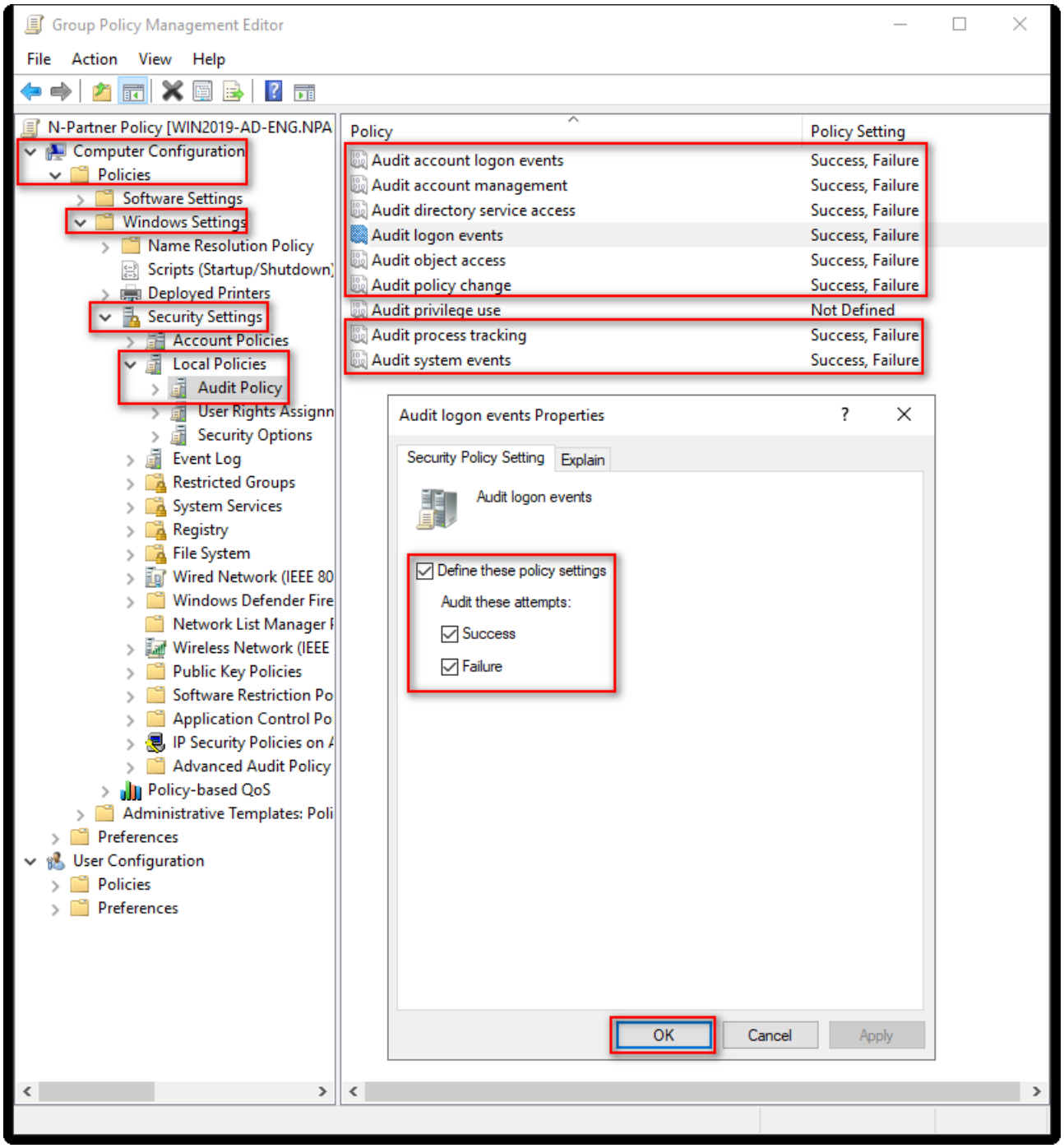
In your group policy object, (in this example, it is “N-Partner Policy”)

right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

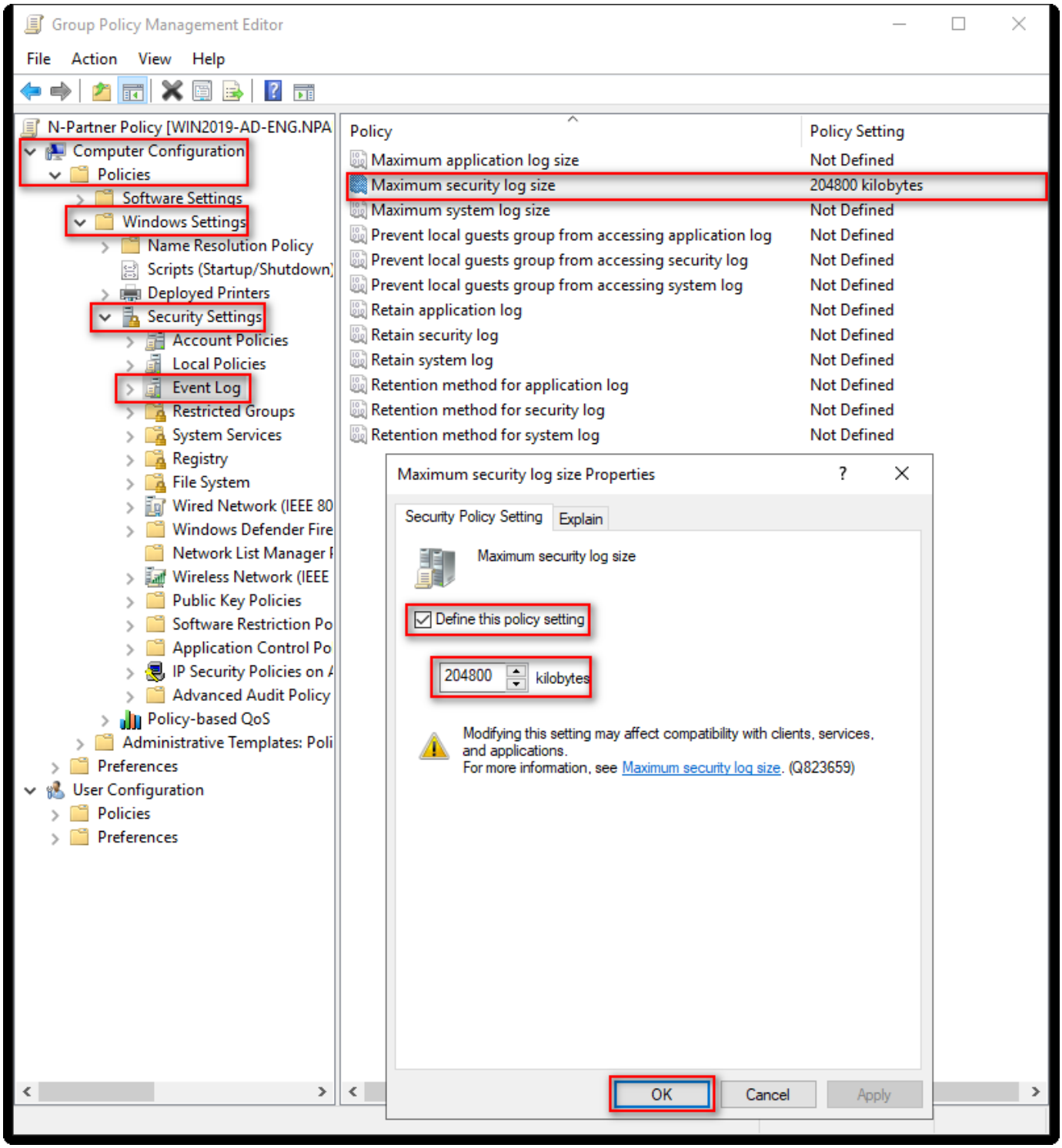
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit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



(6) Event Logs: Maximum Size of Security Log

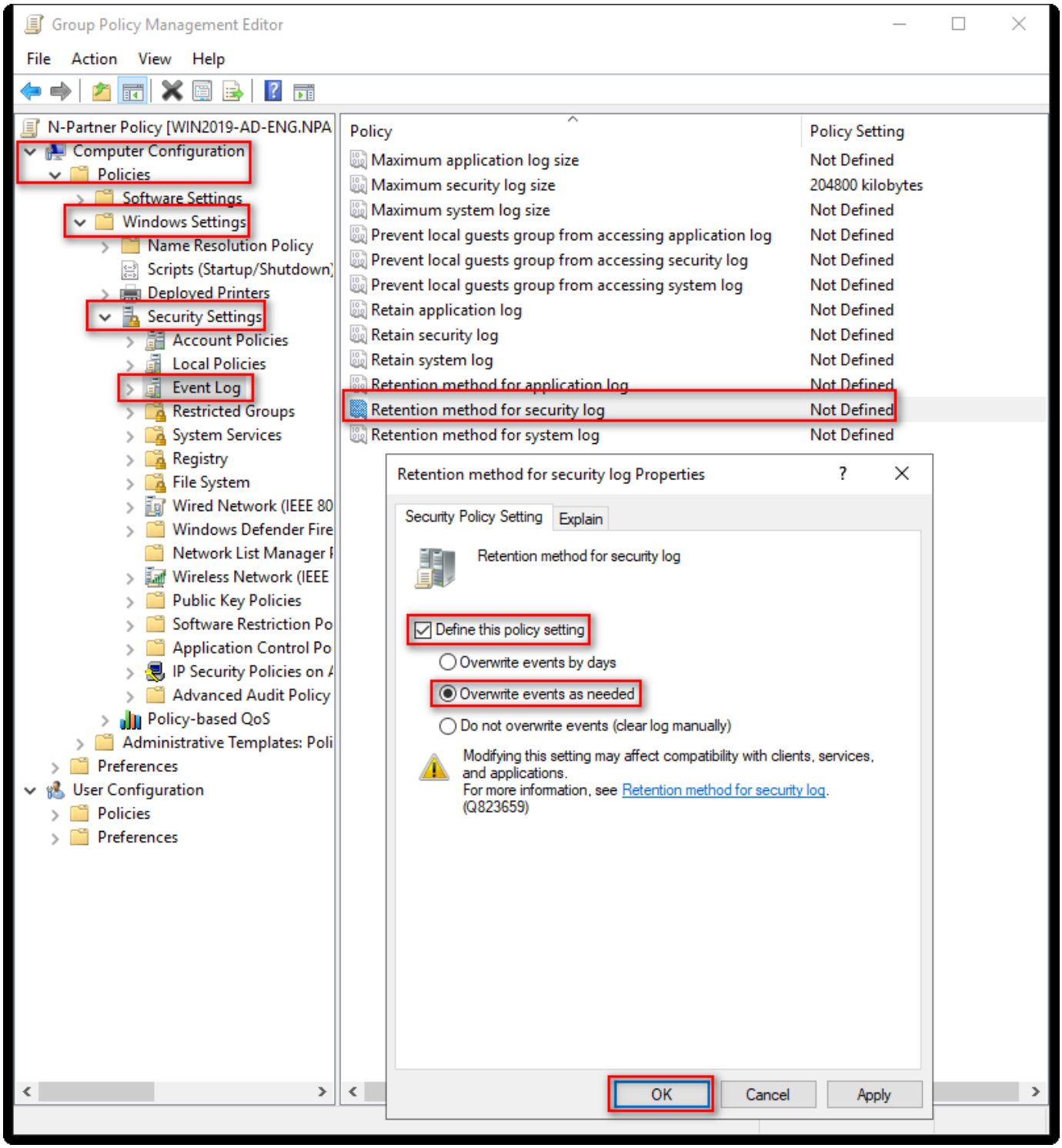
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Logs”-> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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



(7) Event Logs: Retention Method for Security Log

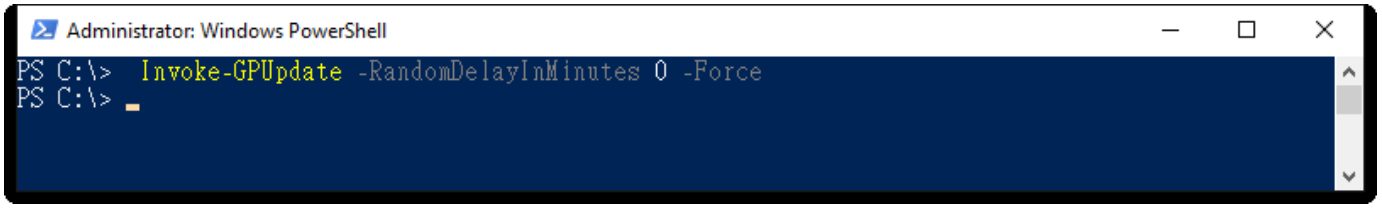
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> And check “Define this policy setting”-> Select “Overwrite events as needed” -> Then click “OK.”



(8) Open “Windows PowerShell.”

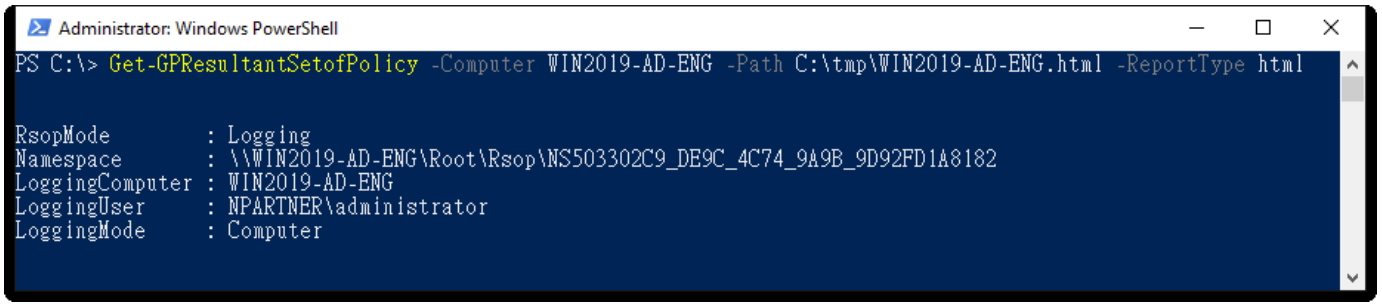
(9) Enter the command below to refresh group policy.

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



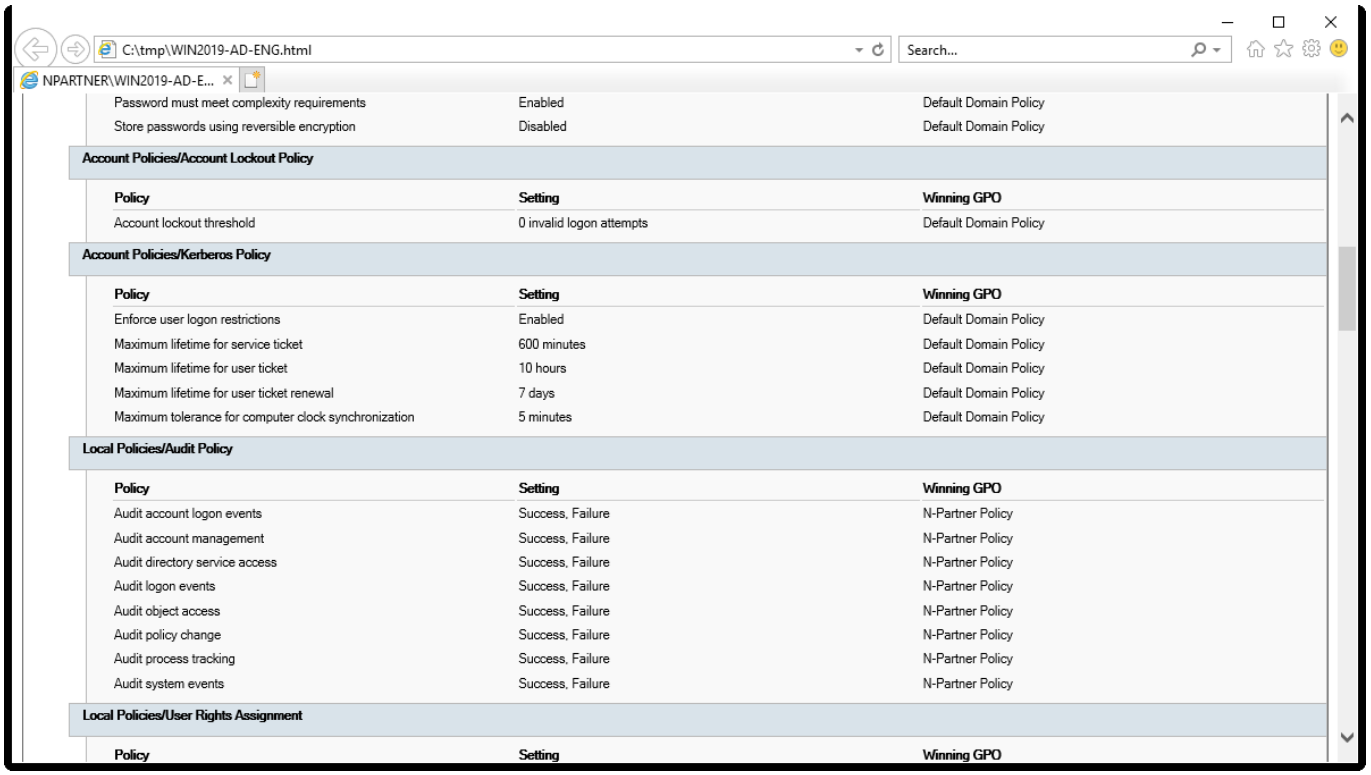
(10) Enter the command to generate server group policy report.

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



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.



6.3 Add a Non-Admin Account

6.3.1 Add Users

(1) Open “Windows PowerShell.”

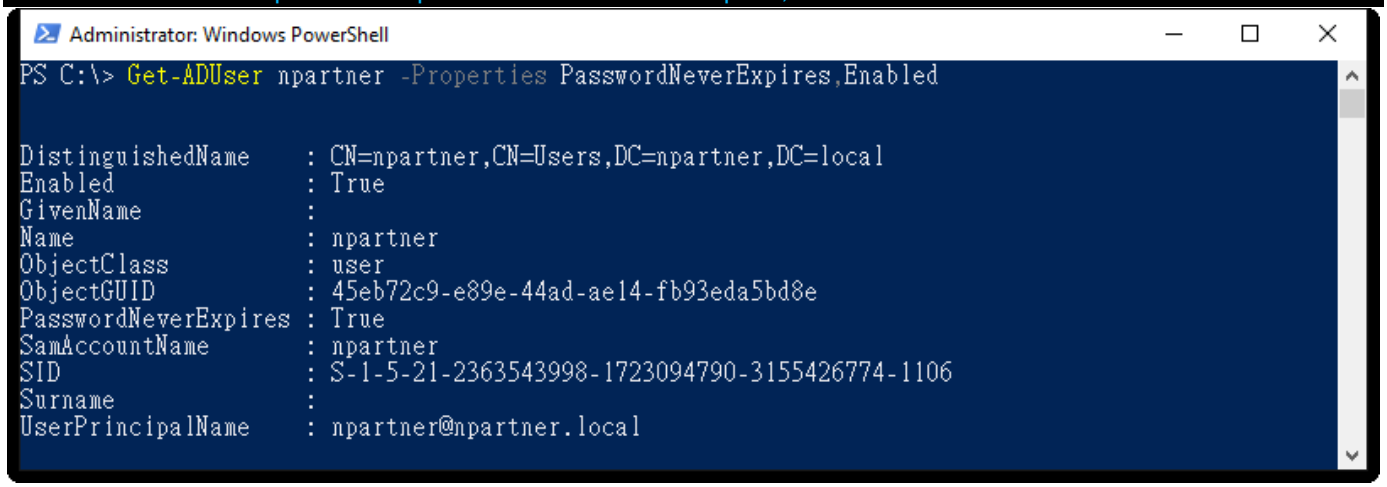
(2) Enter the command below to add a new account.

```
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
```

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
```

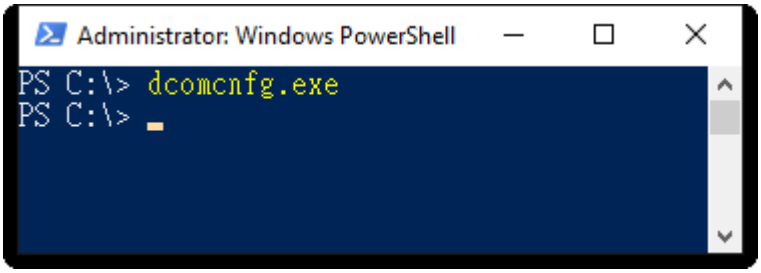


6.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”

(2) Open “Component Services.”

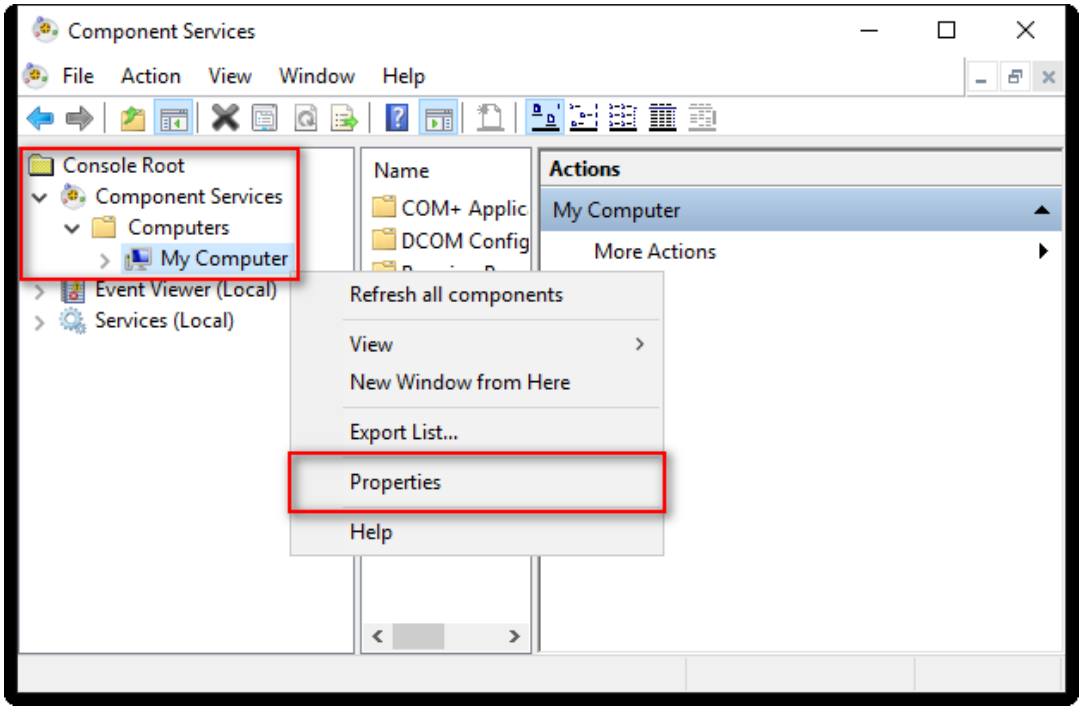
```
PS C:\> dcomcnfg.exe
```



(3) Edit Computer Properties

Expand “Console Root → Component Services → Computers.”

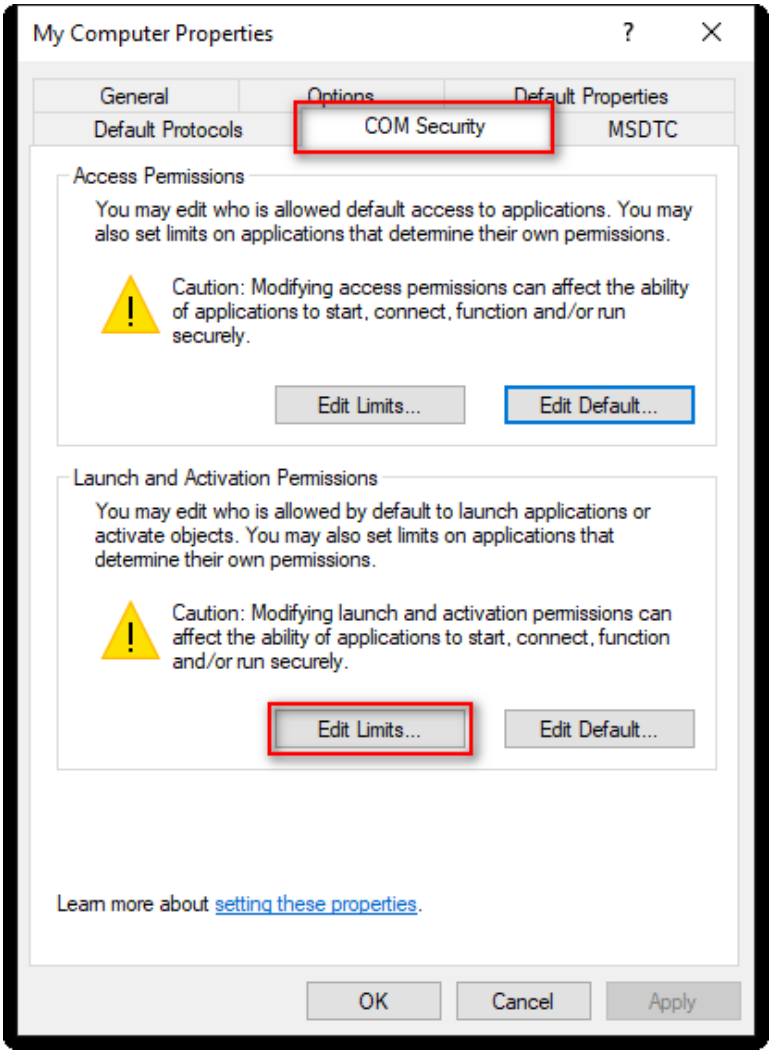
Right-click “My Computer” → select “Properties.”



(4) Enable Permissions

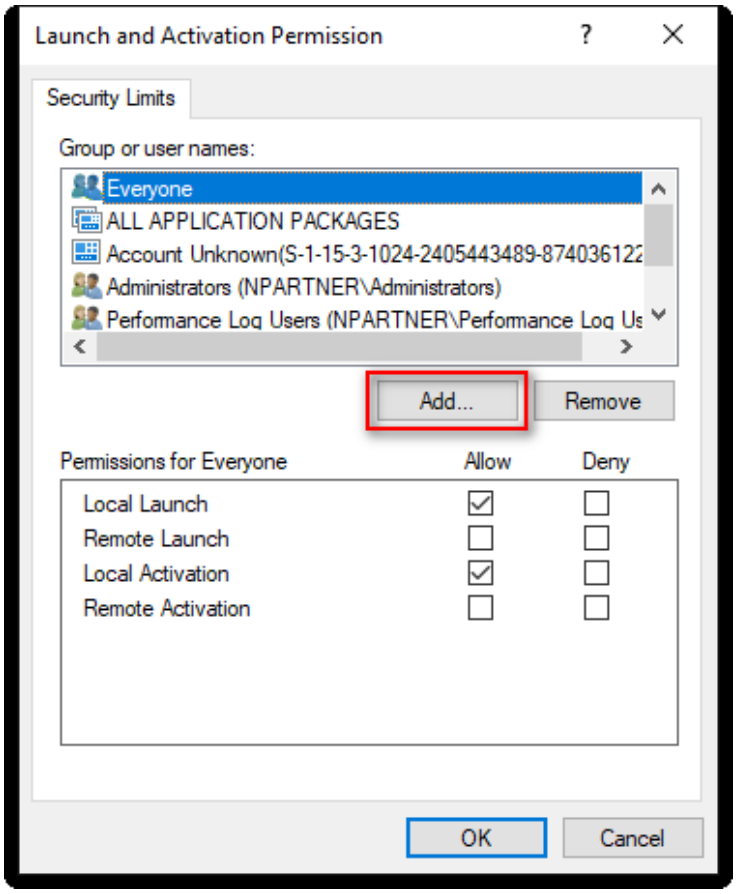
Go to the COM Security tab.

Under Launch and Activation Permissions, click Edit Limits.



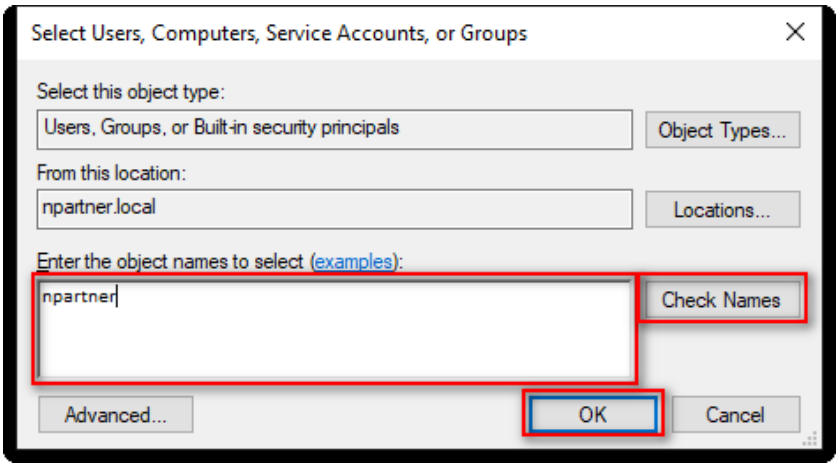
(5) Add DCOM User Permissions

Click “Add.”



(6) Specify the User

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

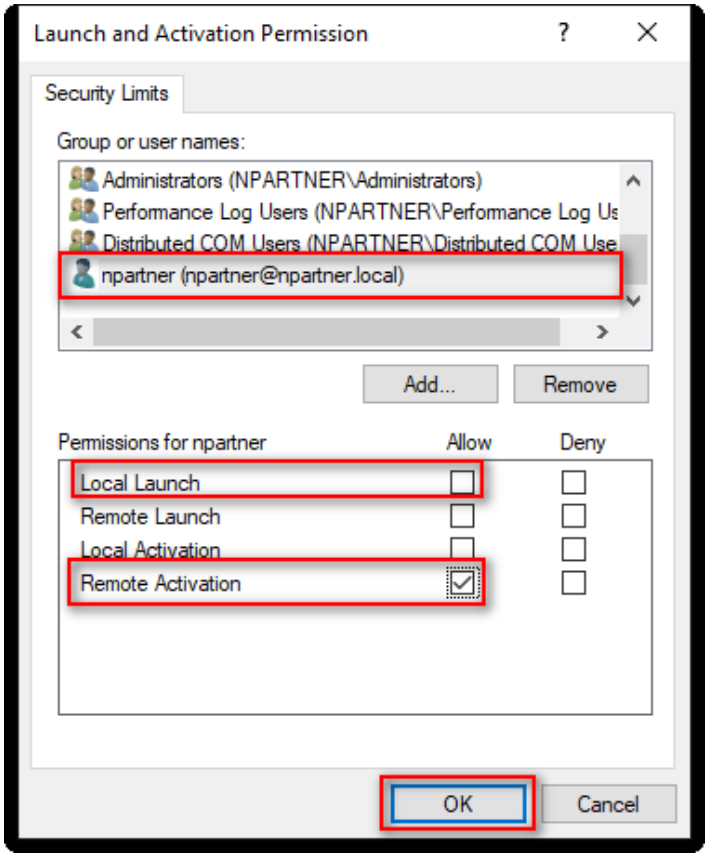


(7) Configure User Permissions

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

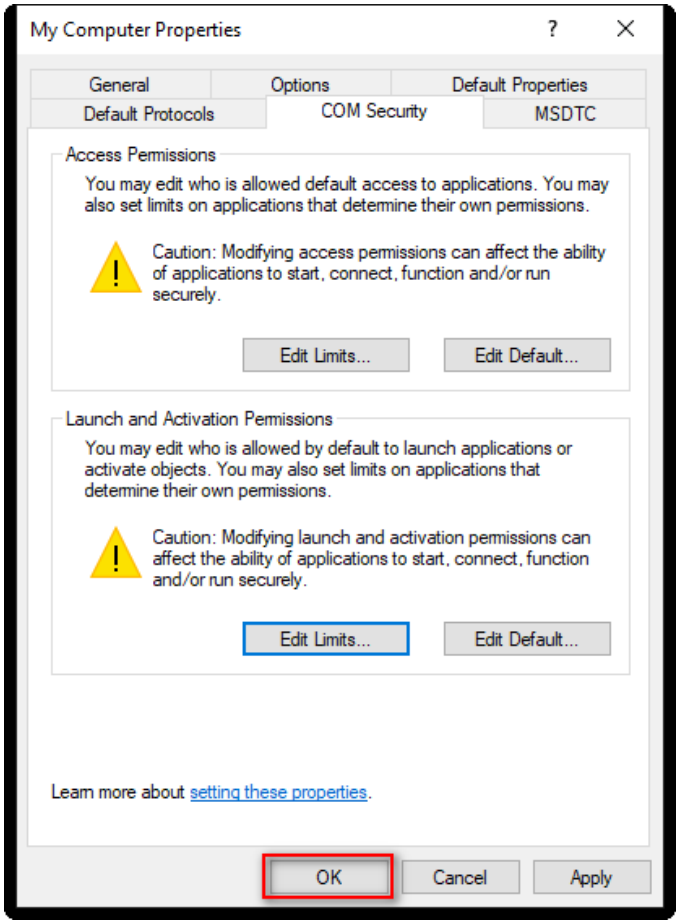
- Clear **Local Launch: Allow**
- Select **Remote Activation: Allow**

  Click **OK**.



(8) Confirm User Permissions

Click “OK” to apply the settings.



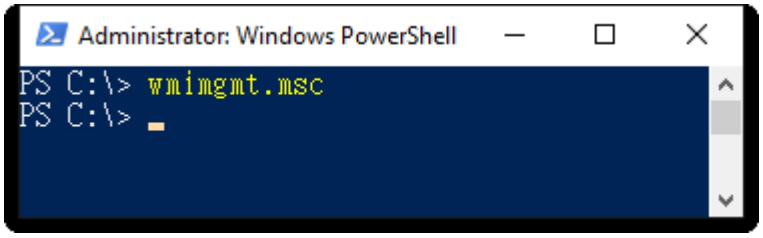
6.3.3 Configure WMI Permissions

6.3.3.1 Set Event Log Permissions

(1) Open “Windows PowerShell.”

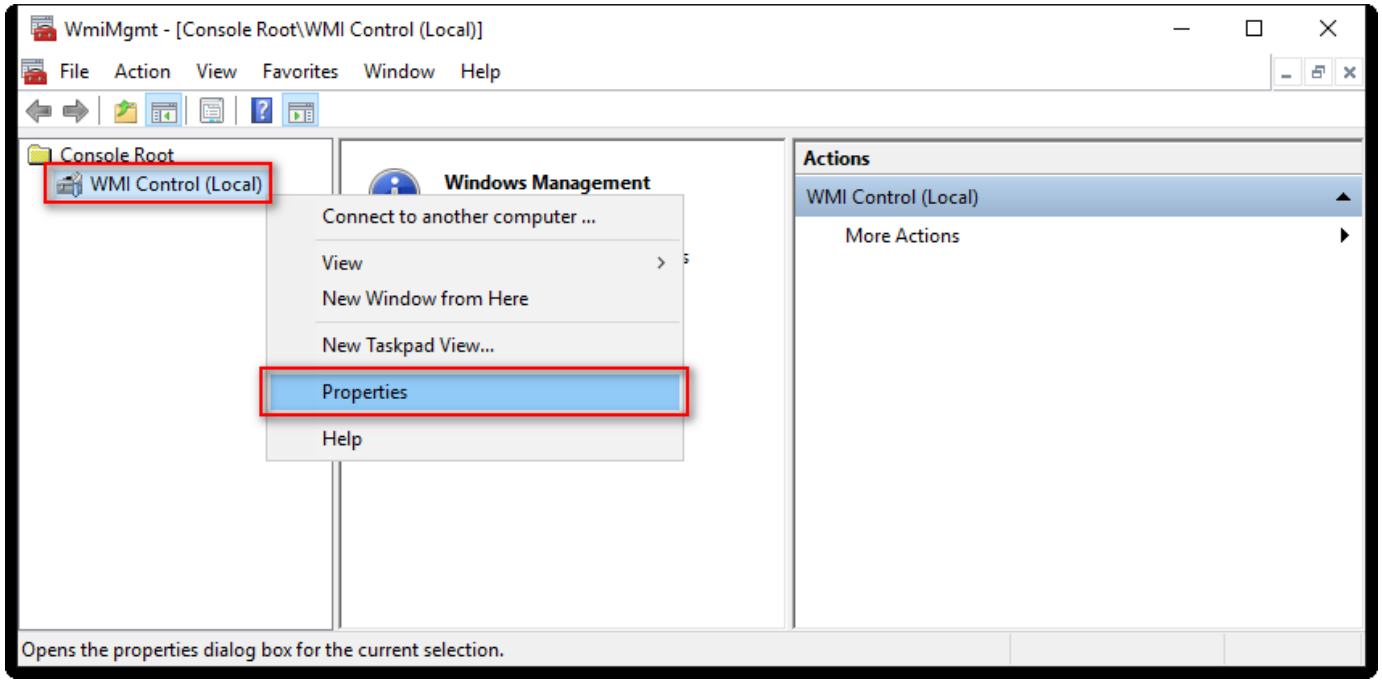
(2) Enter the command below to enable component services.

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



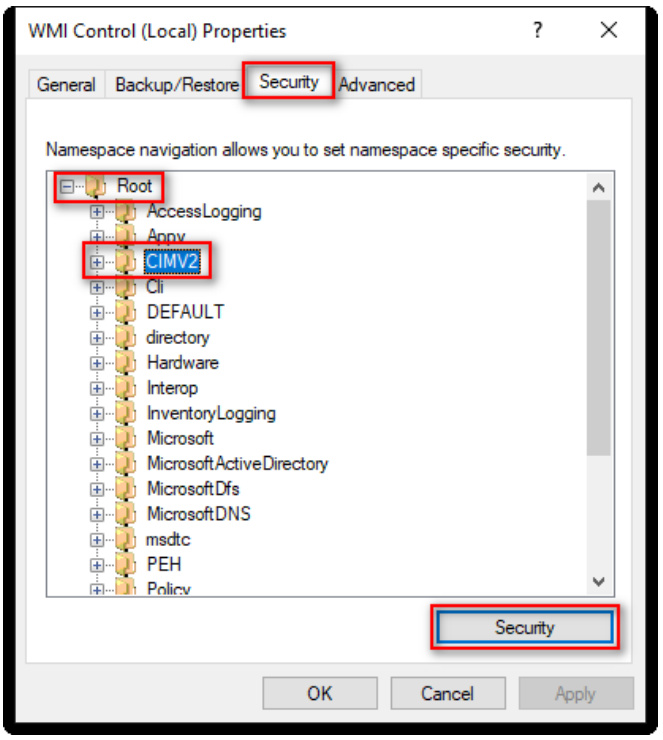
(3) Edit WMI Control

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



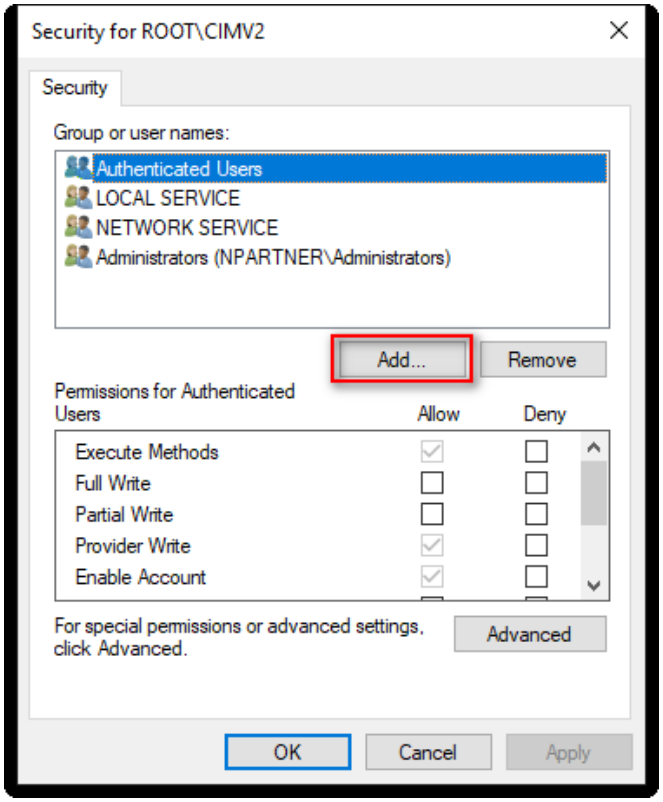
(4) Edit CIMV2 Security

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



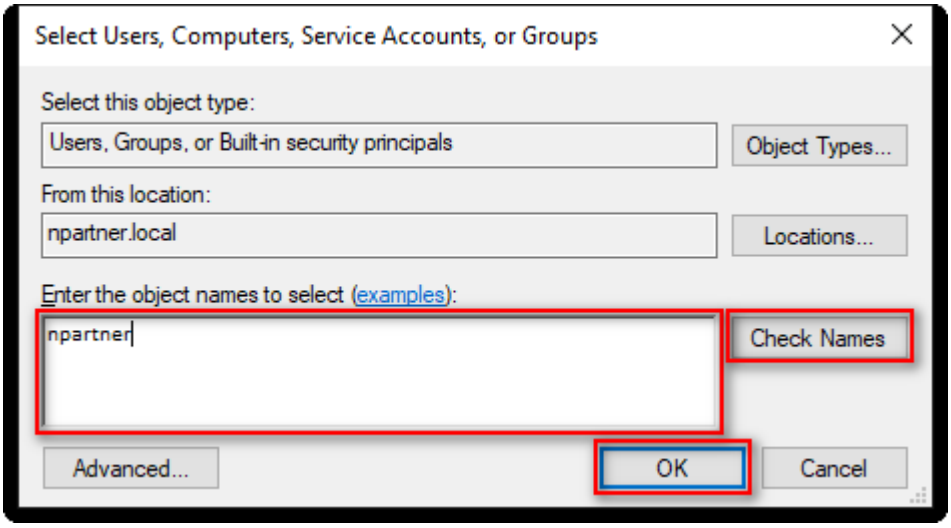
(5) Add WMI User Permissions

Click “Add.”



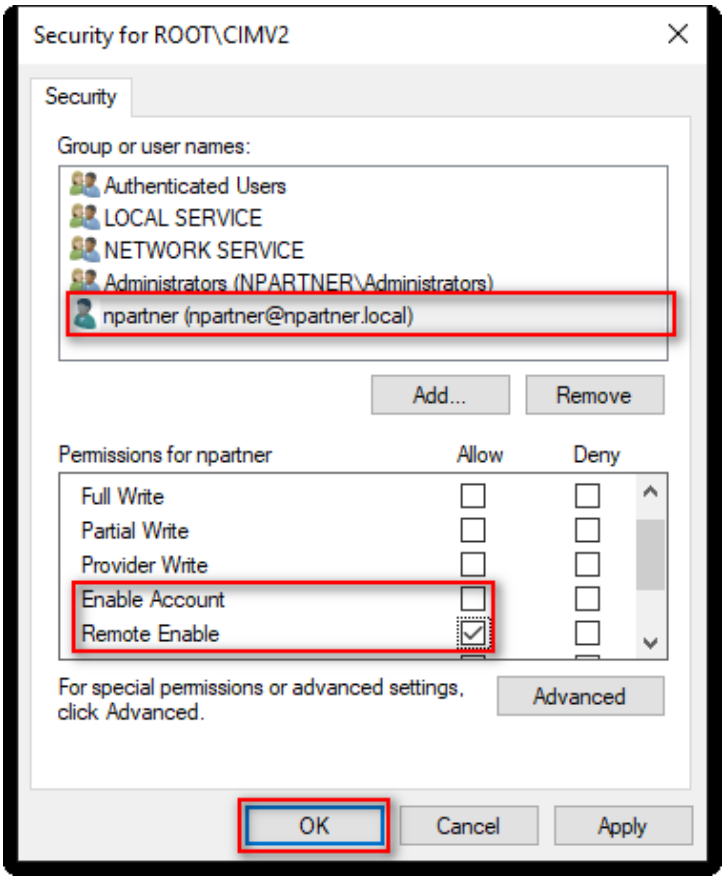
(6) Enter User

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



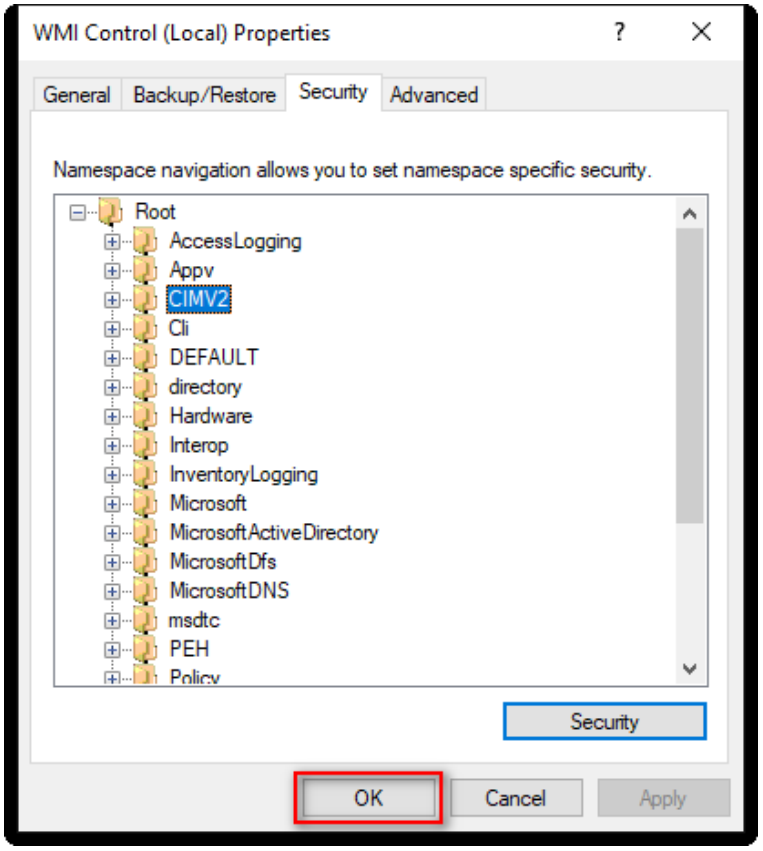
(7) Set User Permissions

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



(8) Confirm User Permissions

Click “OK.”

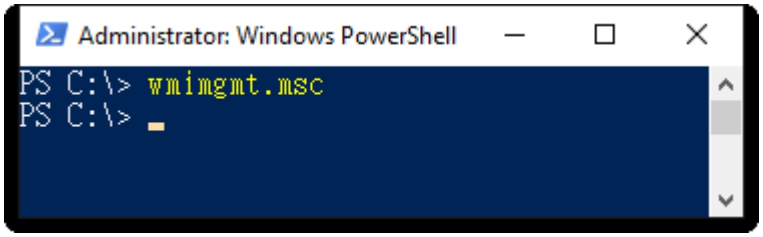


6.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”

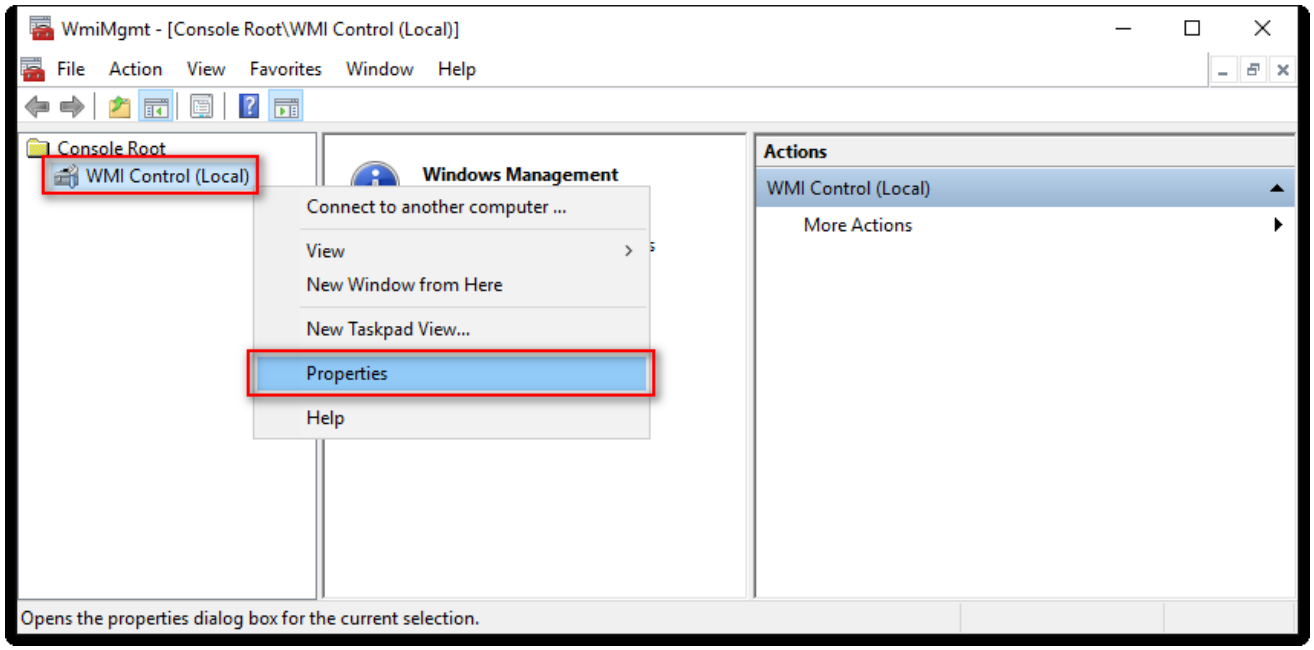
(2) Open “WMI Control.”

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



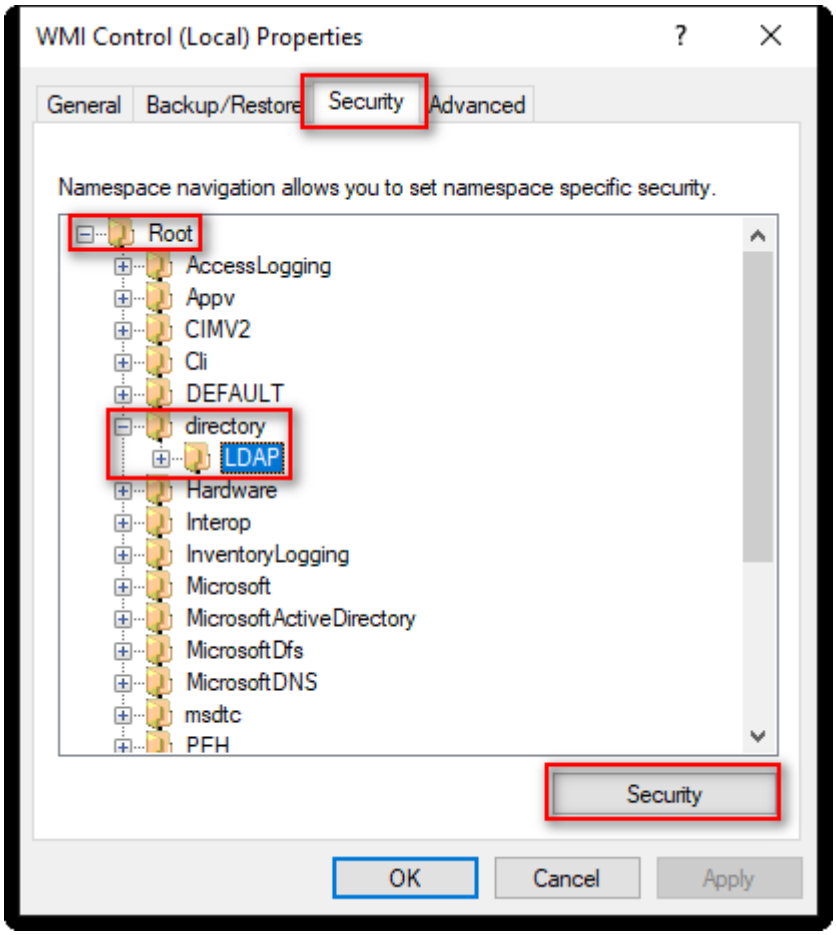
(3) Edit WMI Control

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



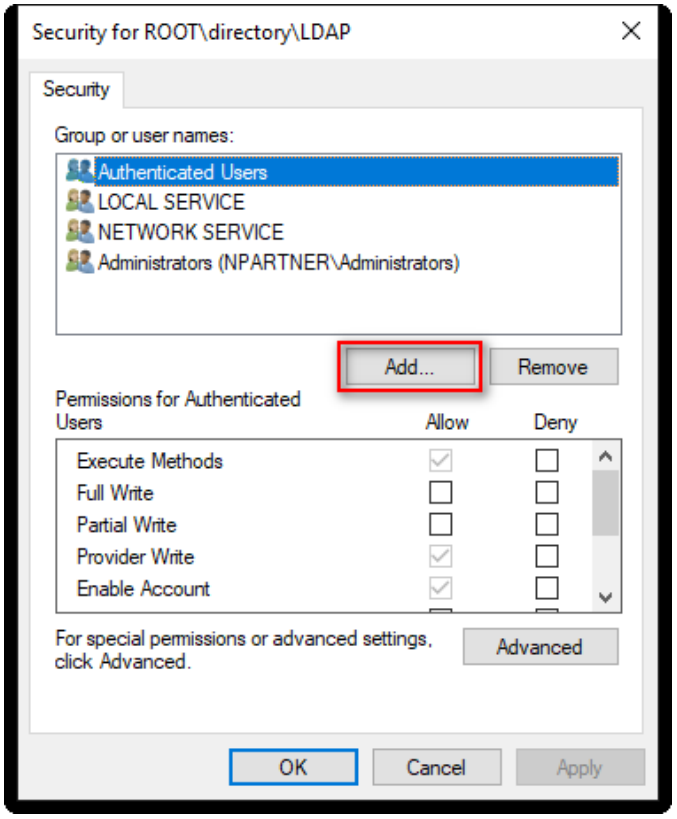
(4) Edit LDAP Security

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



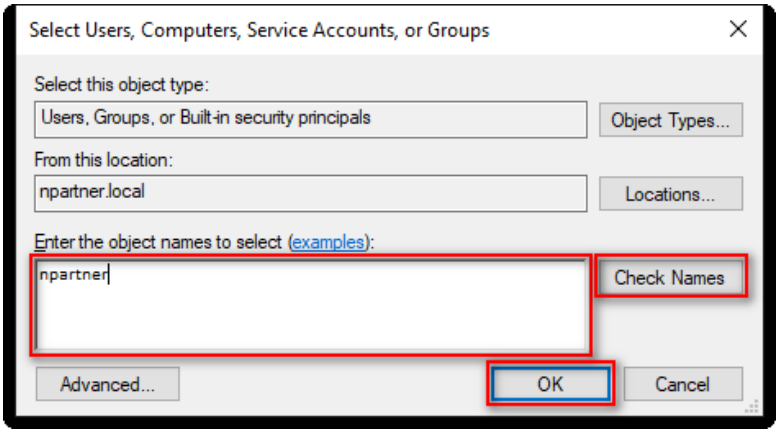
(5) Add WMI User Permissions

Click “Add.”



(6) Specify the User

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

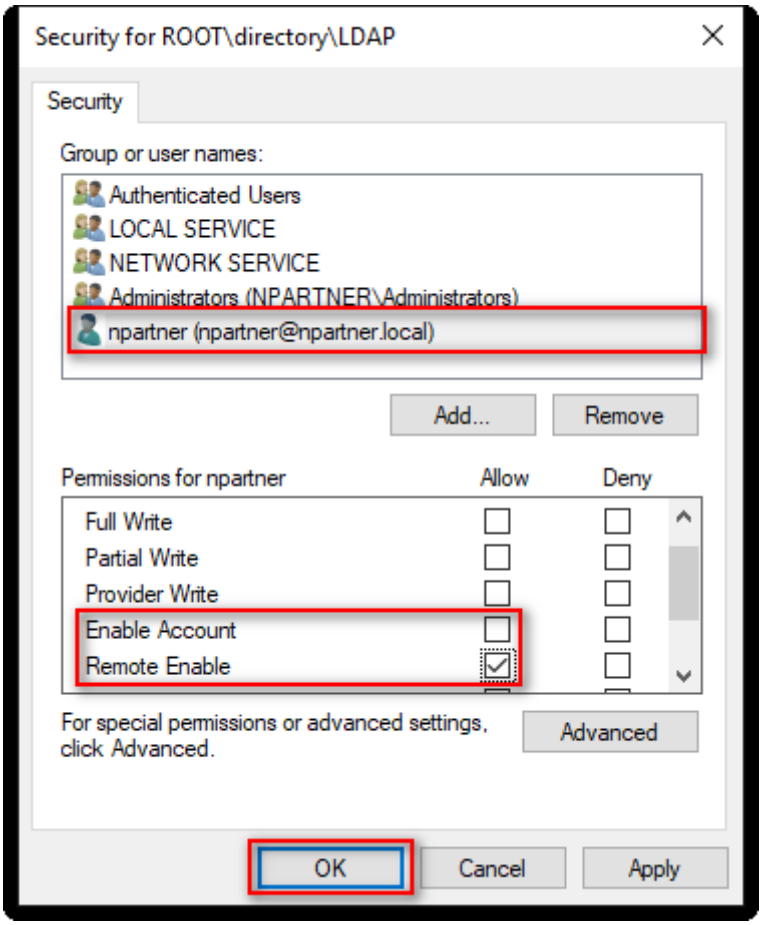


(7) Configure User Permissions

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

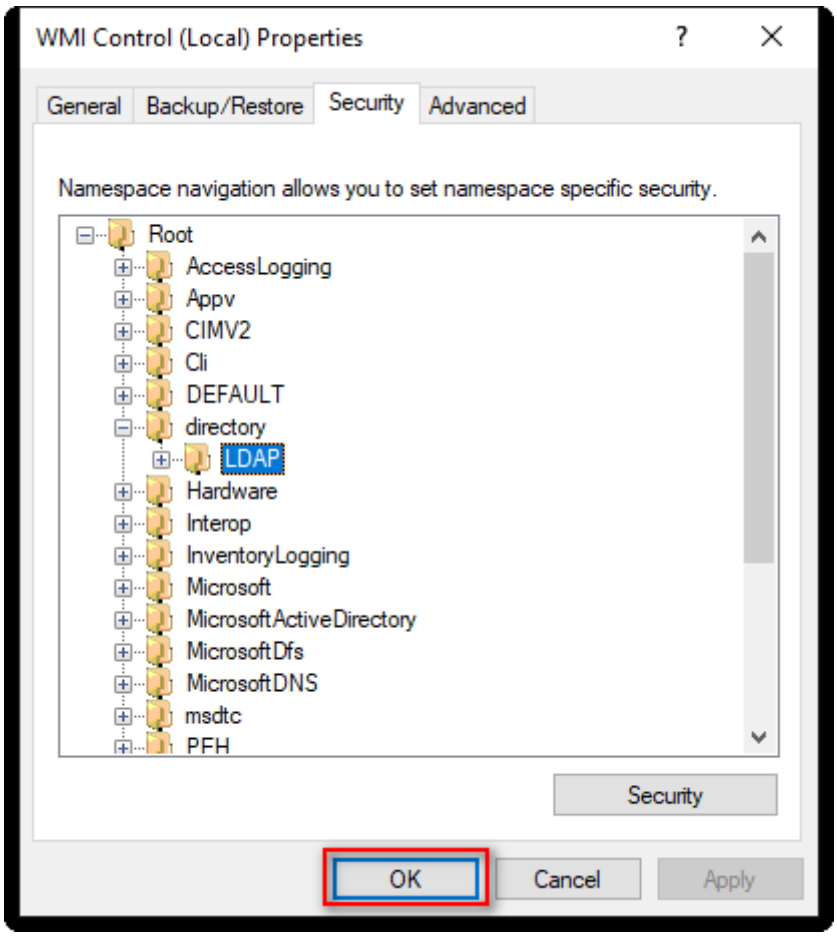
- Clear **Enable Account: Allow**
- Select **Remote Enable: Allow**

  Click **OK**.



(8) Confirm User Permissions

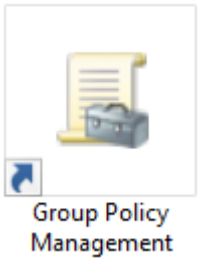
Click “OK” to apply the settings.



6.3.4 Configure Event Log Read Permissions

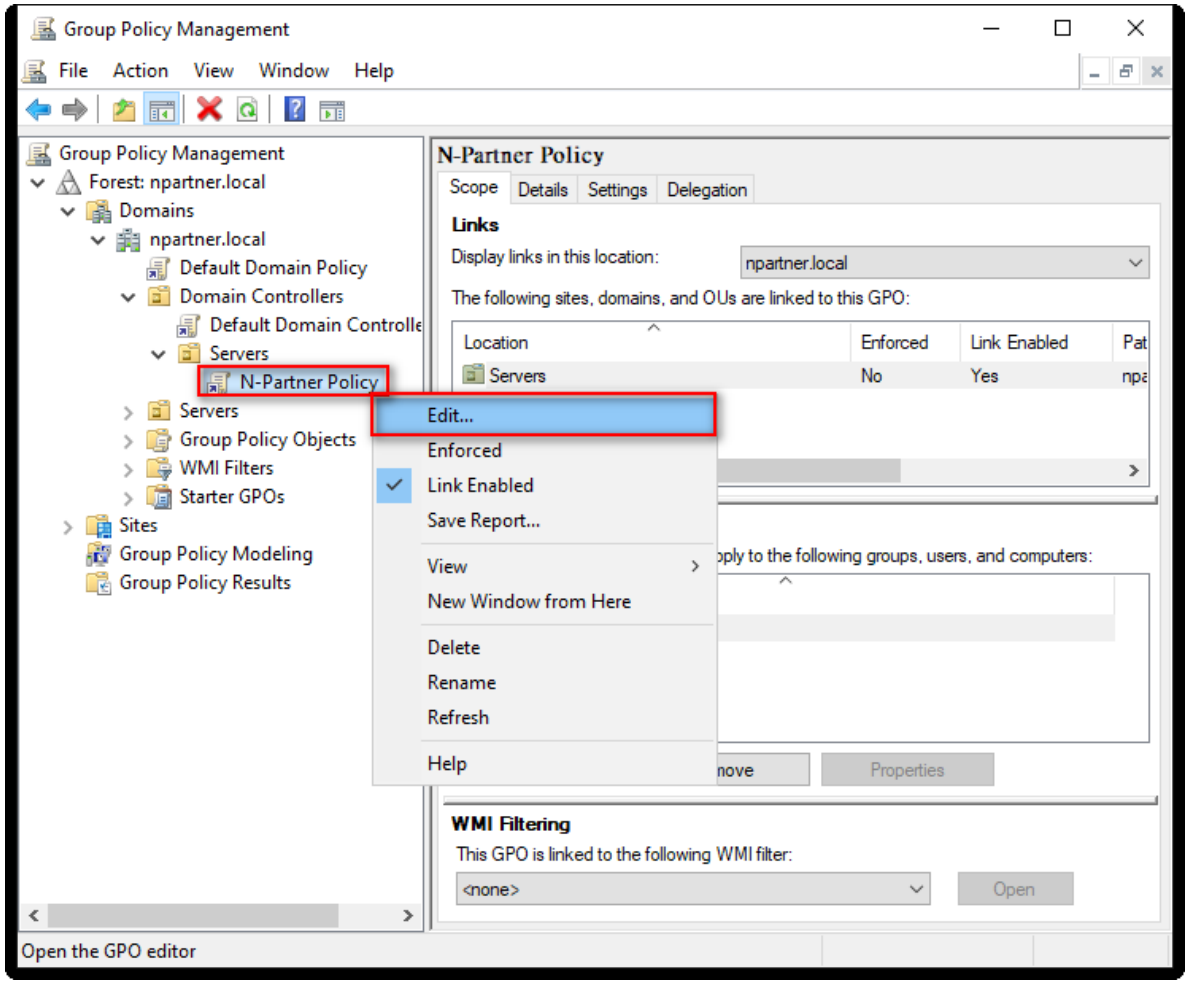
(1) Open Group Policy Management

Open “Group Policy Management.”



(2) Edit the Group Policy Object

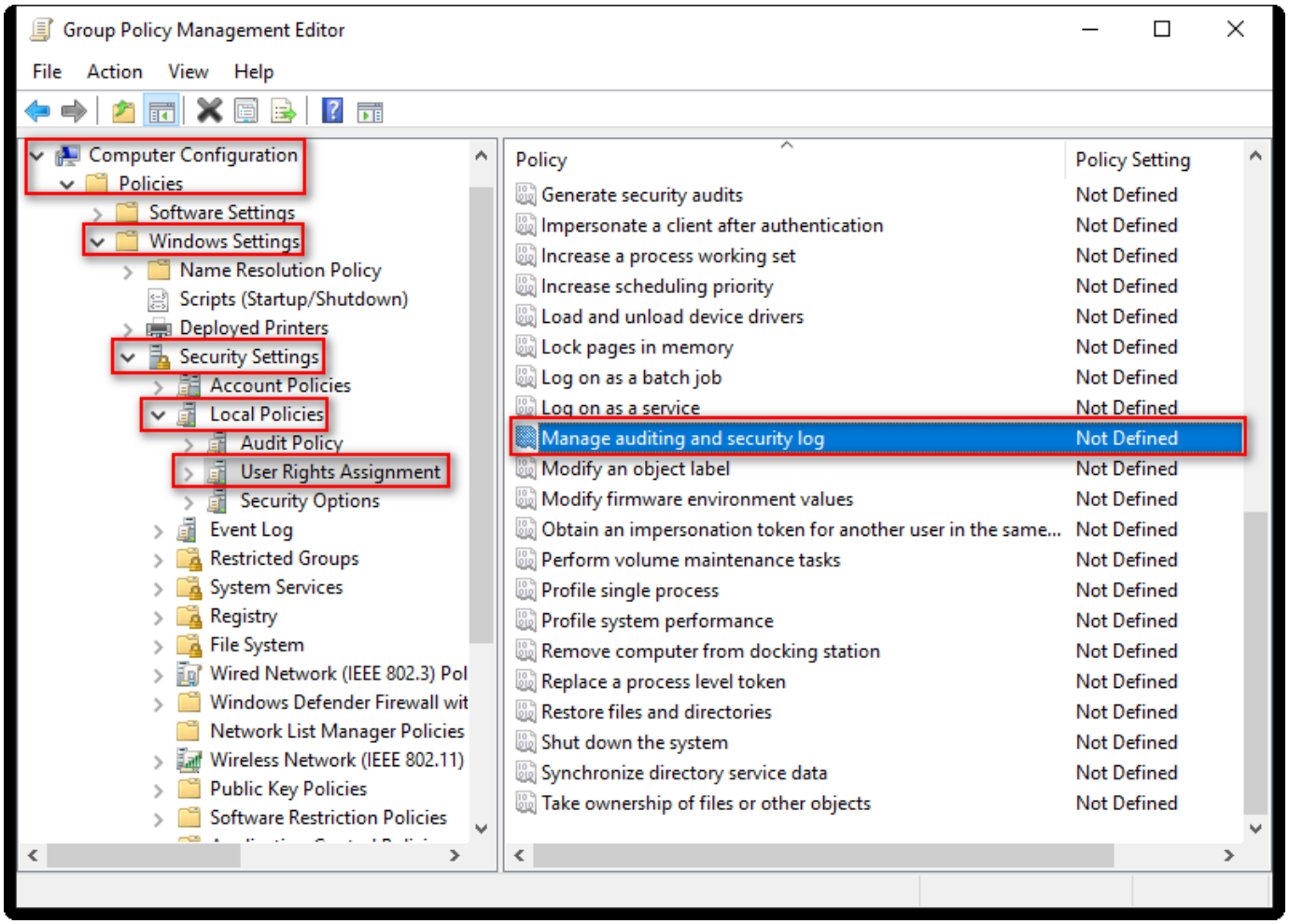
Right-click the “N-Partner Policy” Group Policy Object and select “Edit.”



(3) Configure Log Permissions

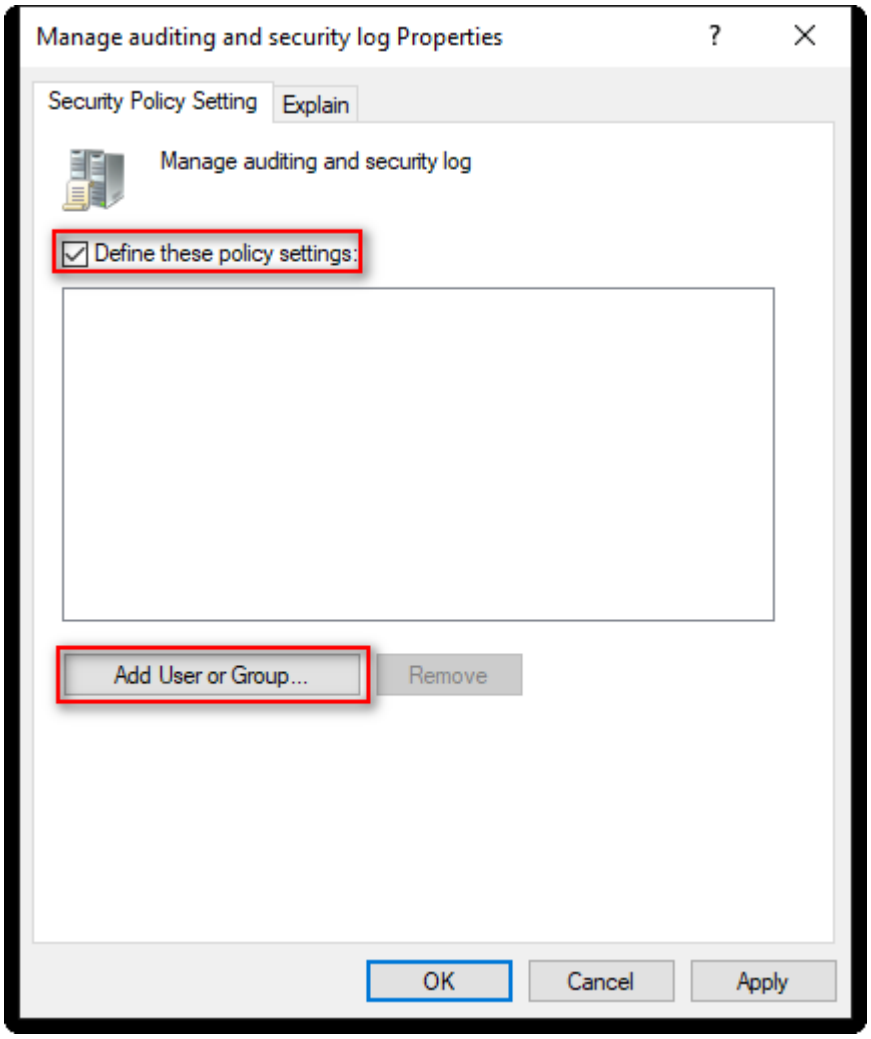
Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

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



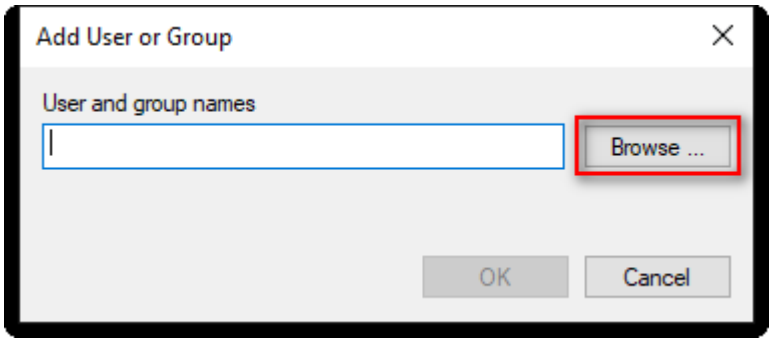
(4) Add User for Audit Log Management

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



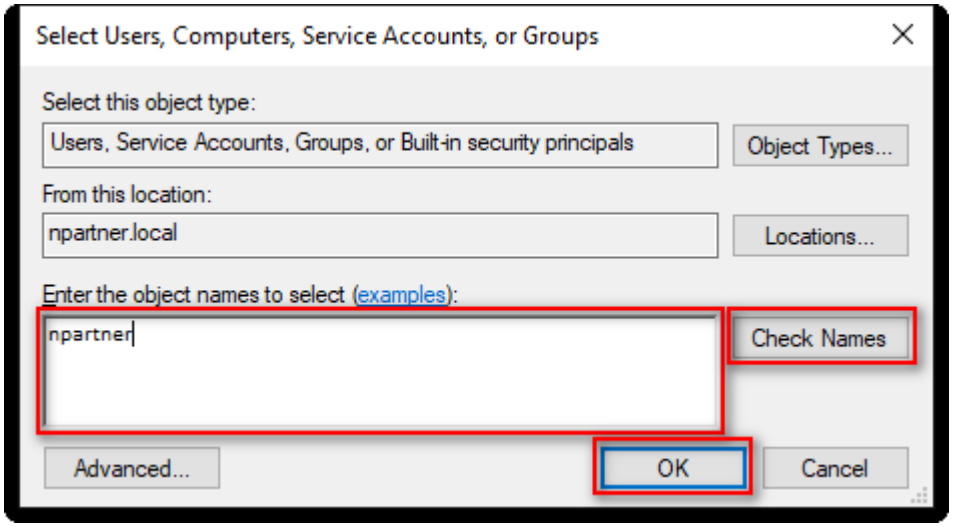
(5) Search for User

Click “Browse.”



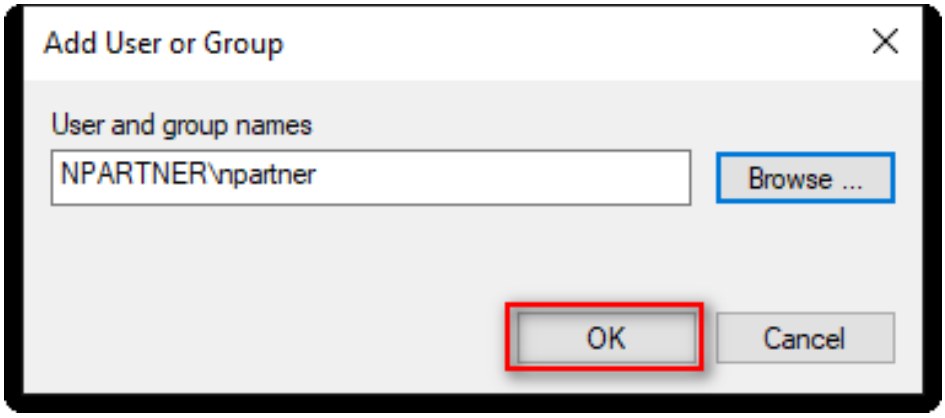
(6) Enter User Account

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



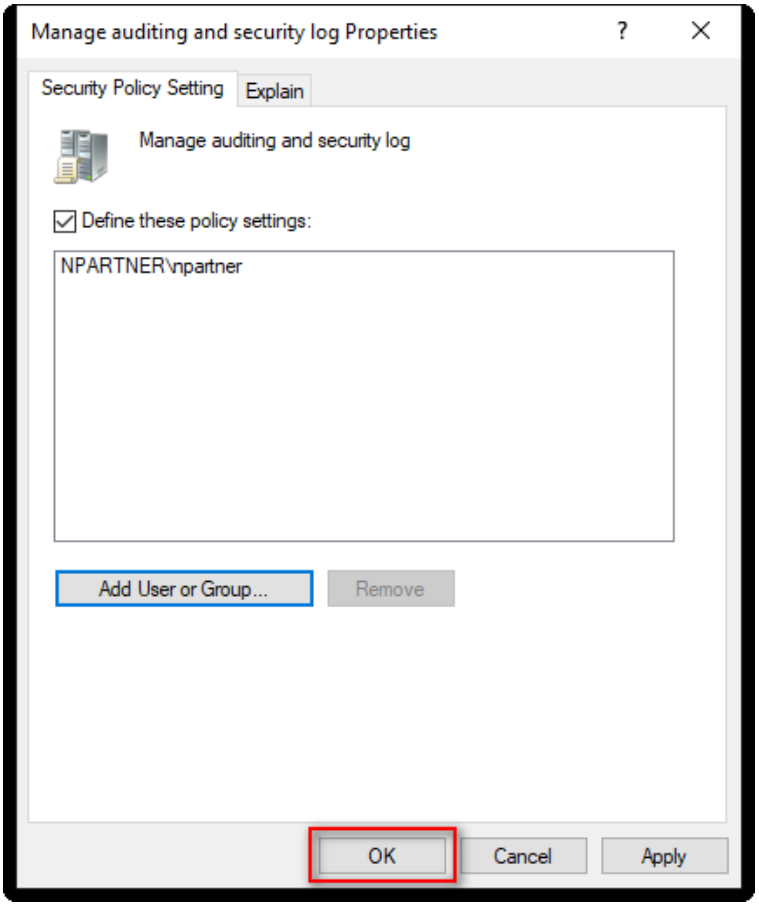
(7) Confirm User

Click “OK.”



(8) Confirm Log Settings

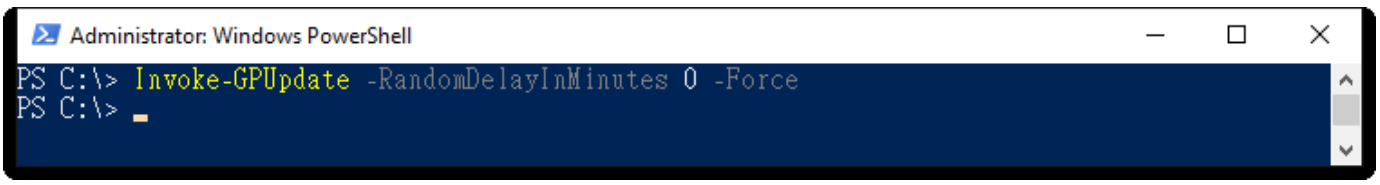
Click “OK” to save the settings.



(9) Open “Windows PowerShell.”

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

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

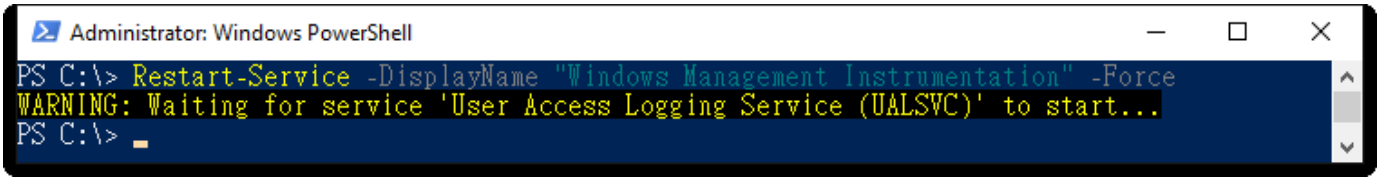


6.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”

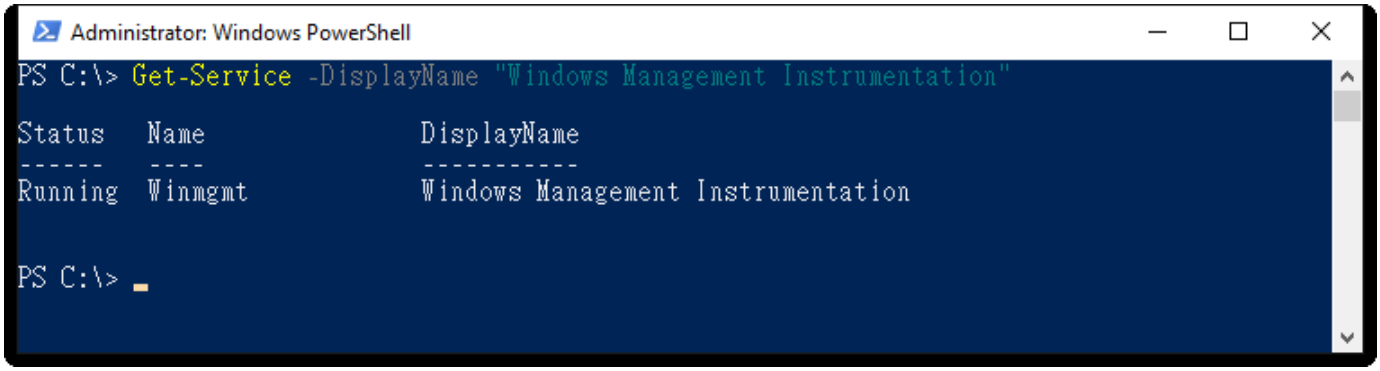
(2) Run the following command to restart the WMI service:

```
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"
```

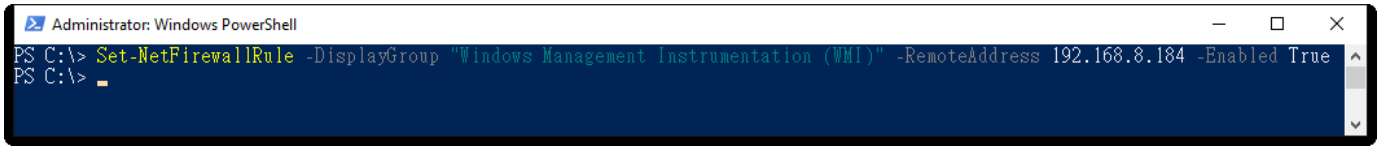


6.4 Configure Firewall

(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
```

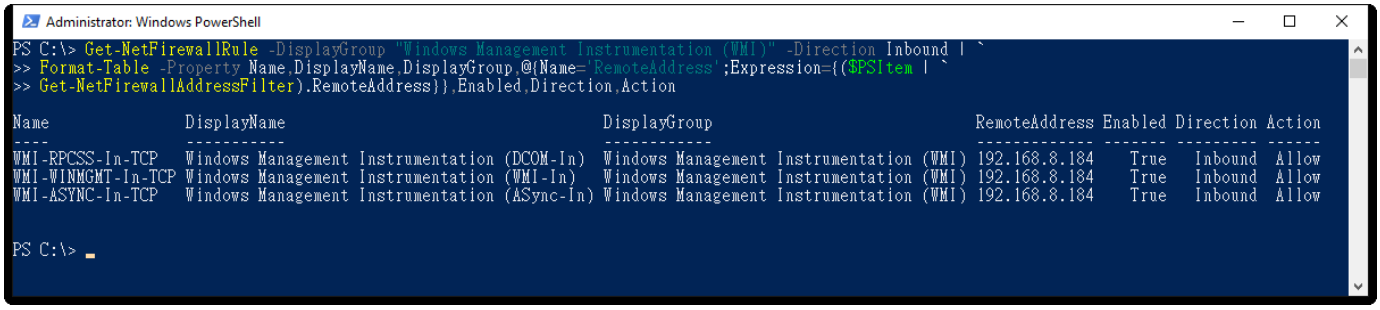


Replace the IP address with the N-Reporter system IP address.

(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
```

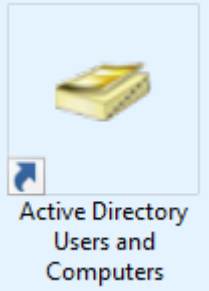


7. Windows 2022

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

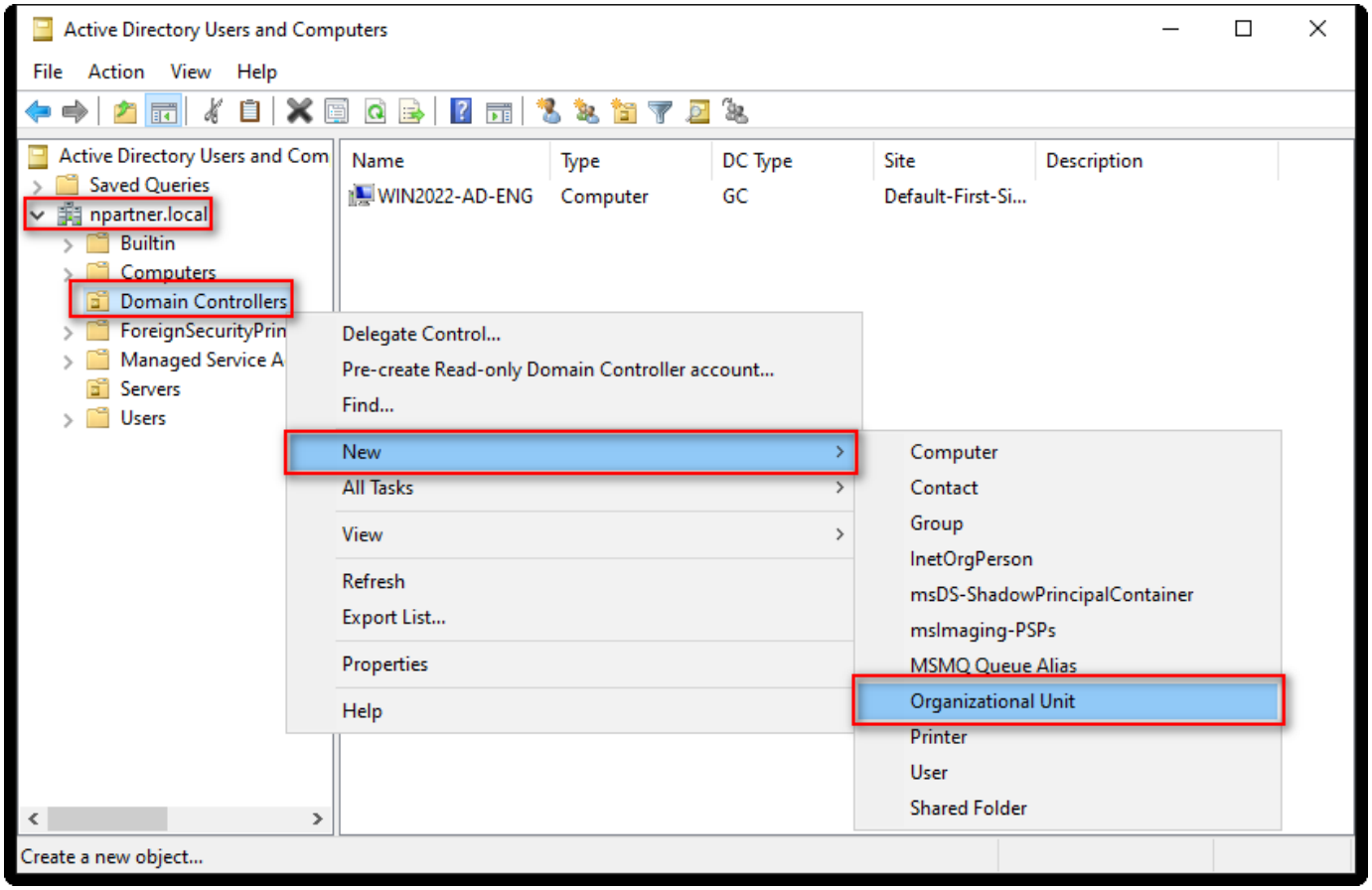
7.1 Organizational Unit Settings

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



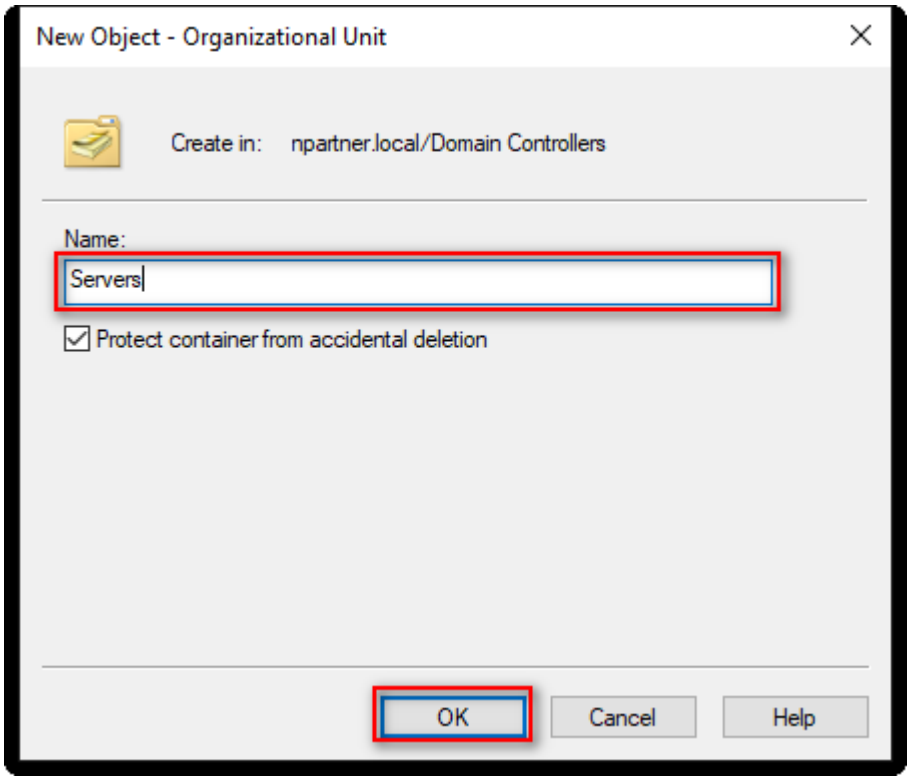
(2) Add an Organizational Unit

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



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

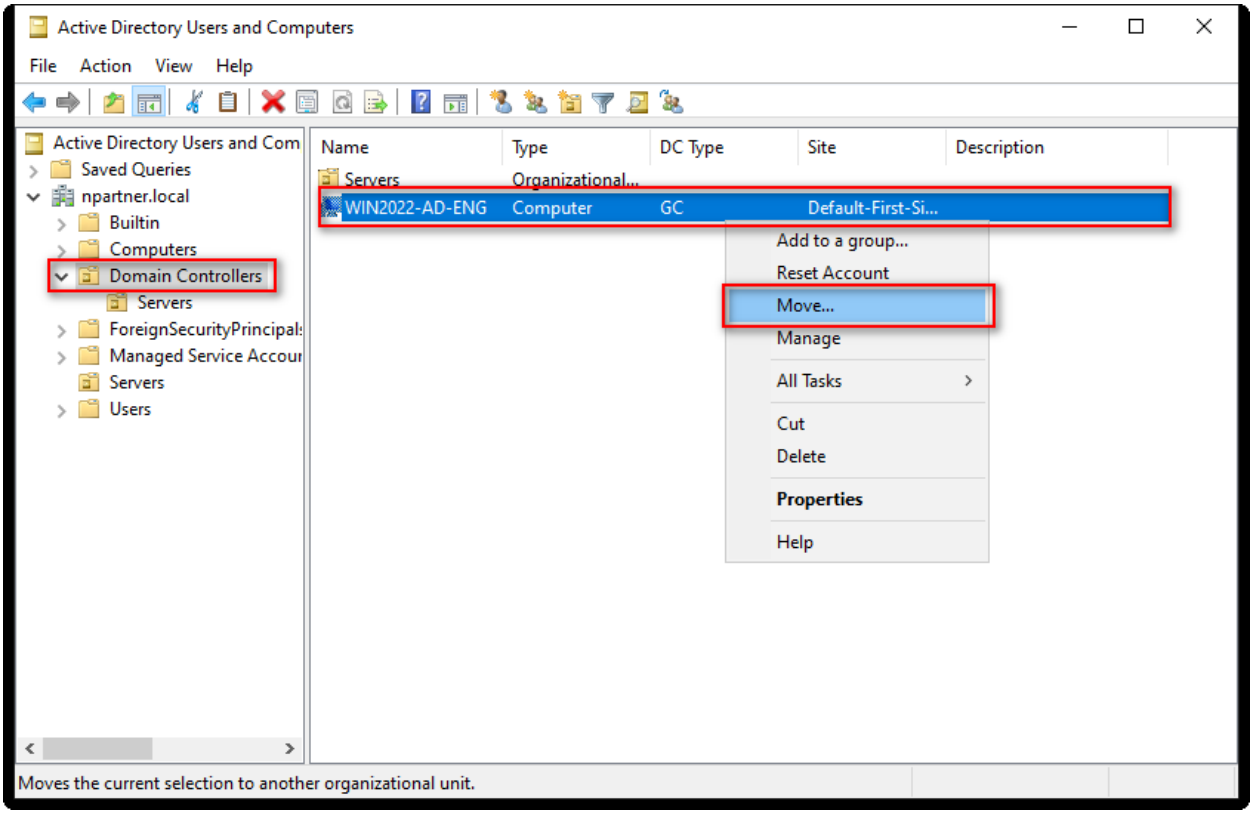
Note: Please create the organizational unit name according to the actual environment. -> Click “OK.”



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

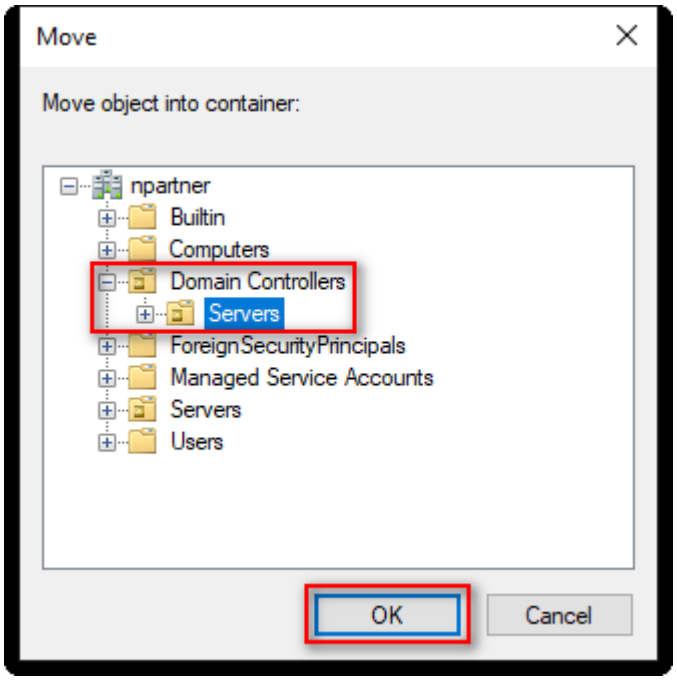
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2022-AD-ENG” server.

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



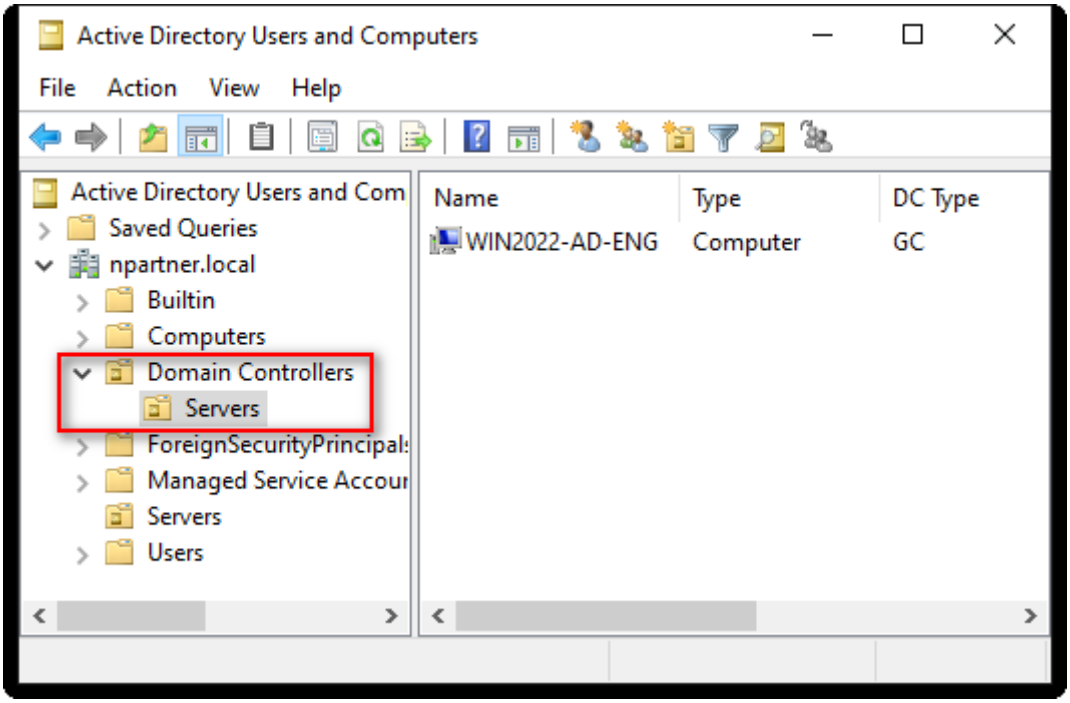
(5) Select your Organizational Unit:

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



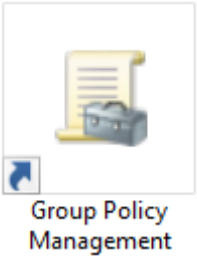
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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.

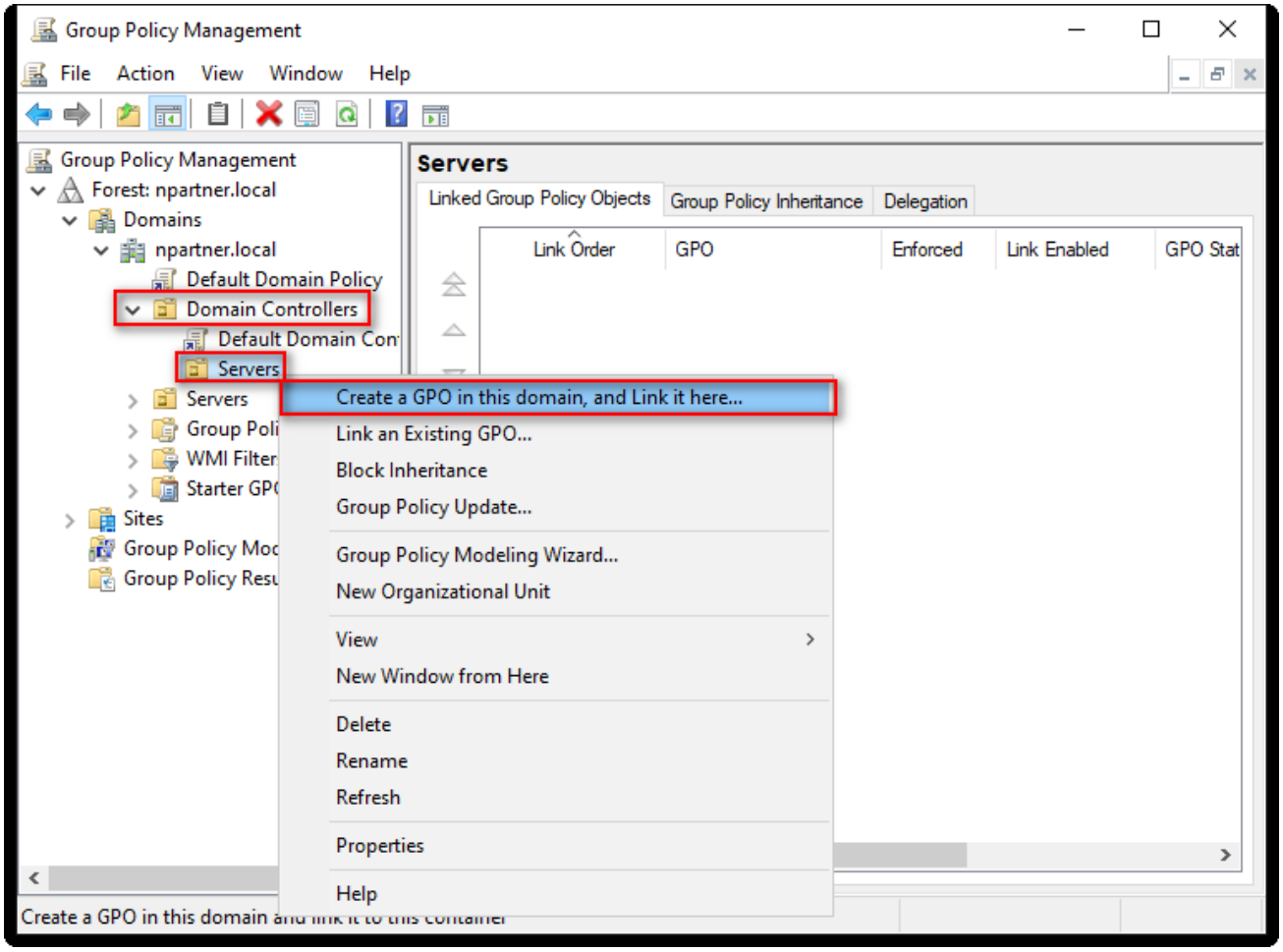


7.2 Group Policy Settings

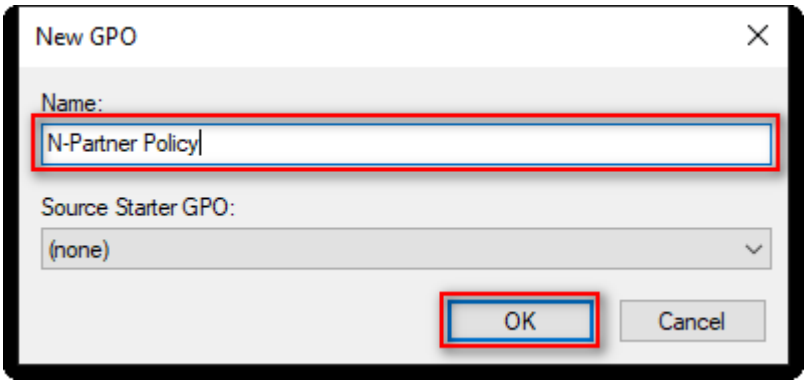
(1) Click “Group Policy Management.”



(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.”

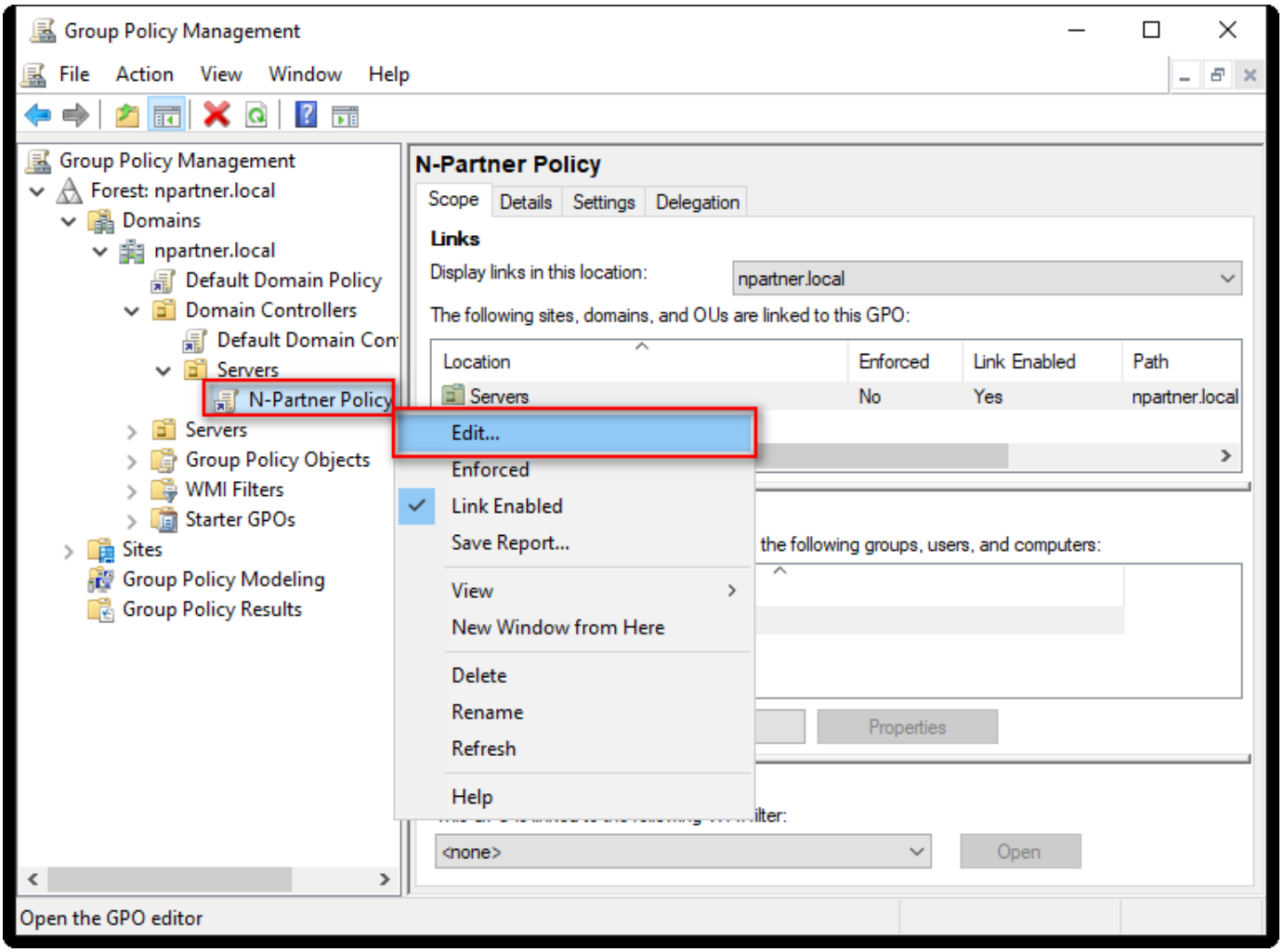


(3) Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)
Note: Create your GPO name according to the client's environment. Then click “Edit.”



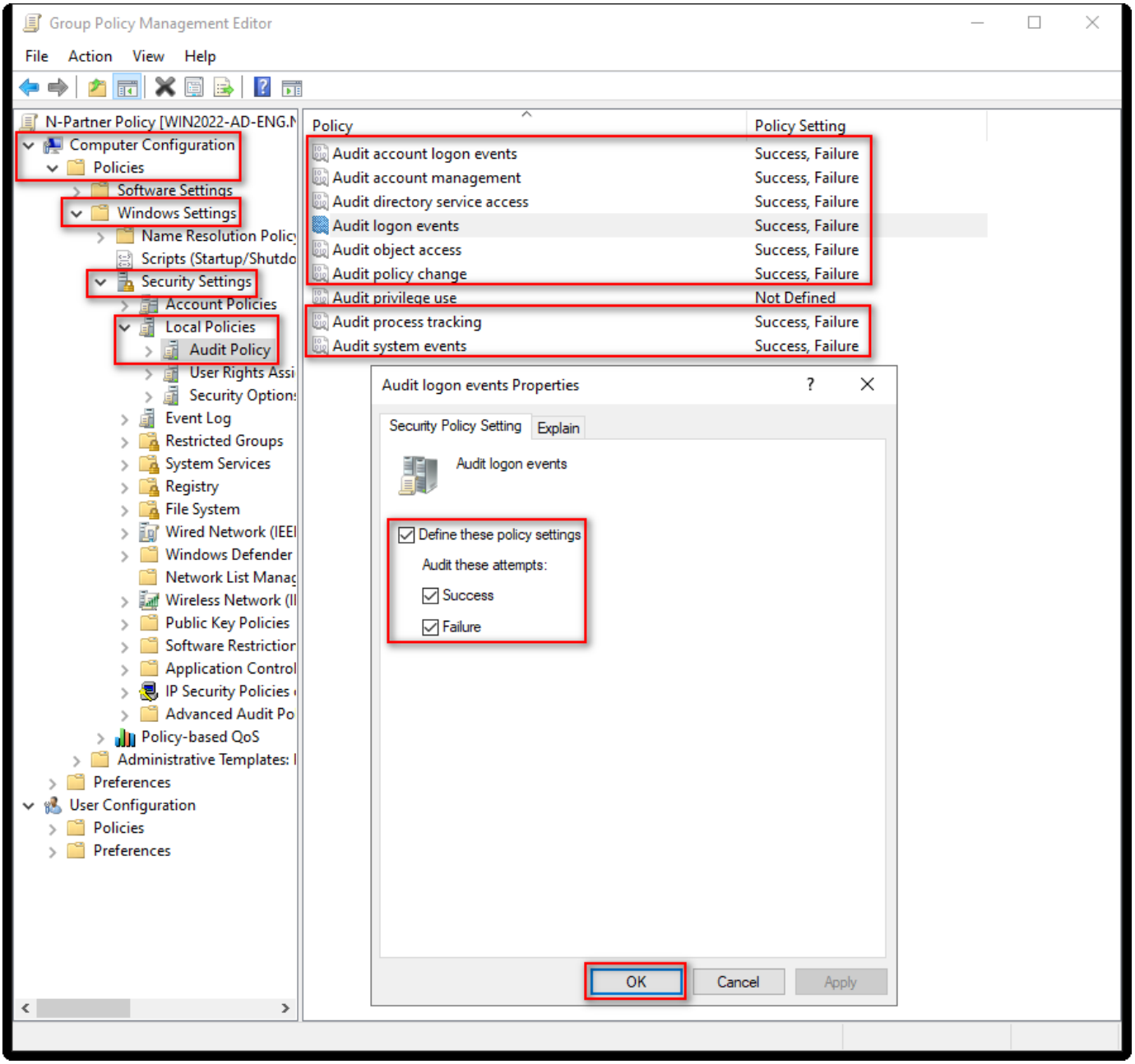
(4) Edit your Group Policy Object

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.”

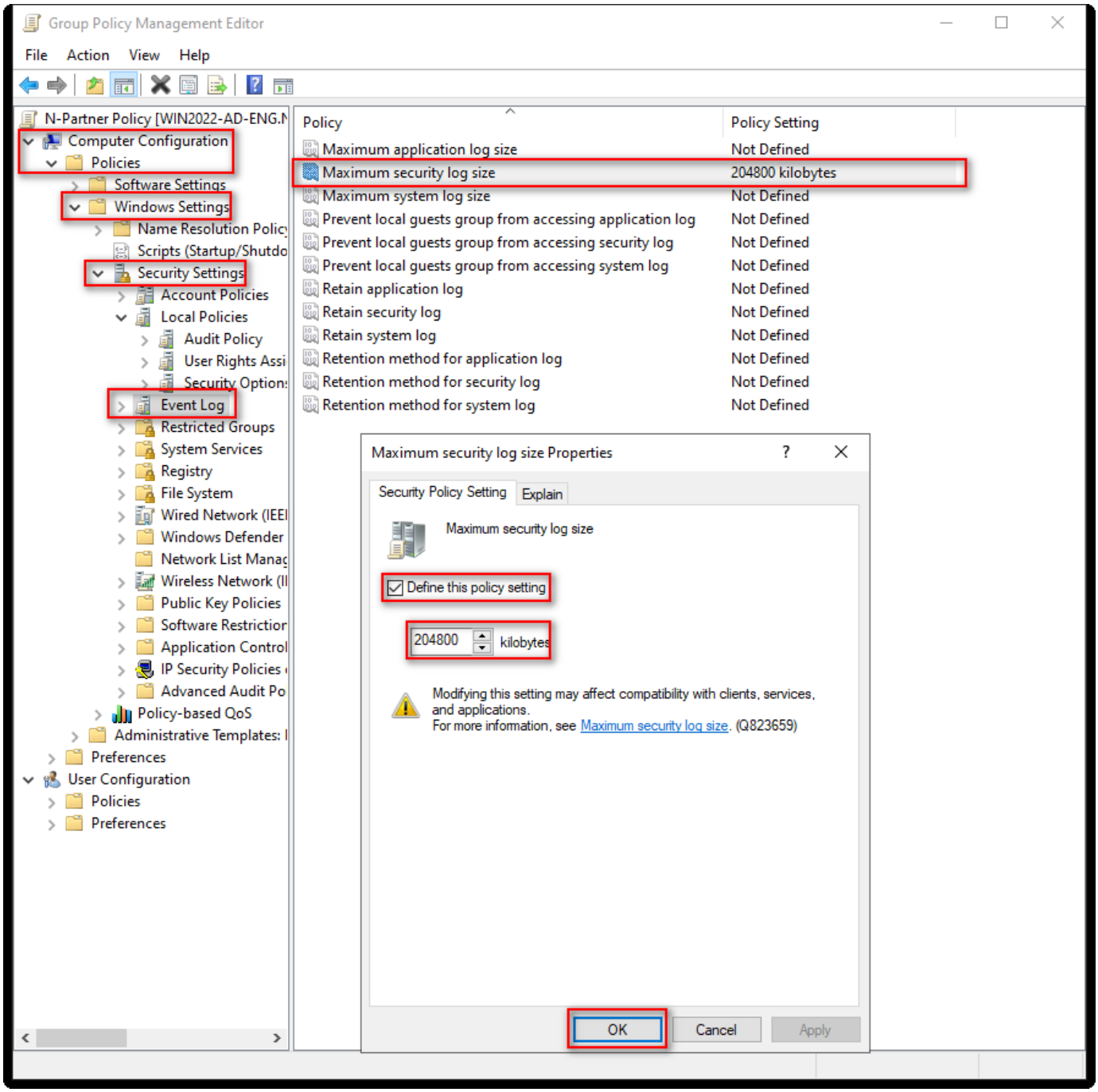


(6) Event Logs: Maximum Size of Security Log

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

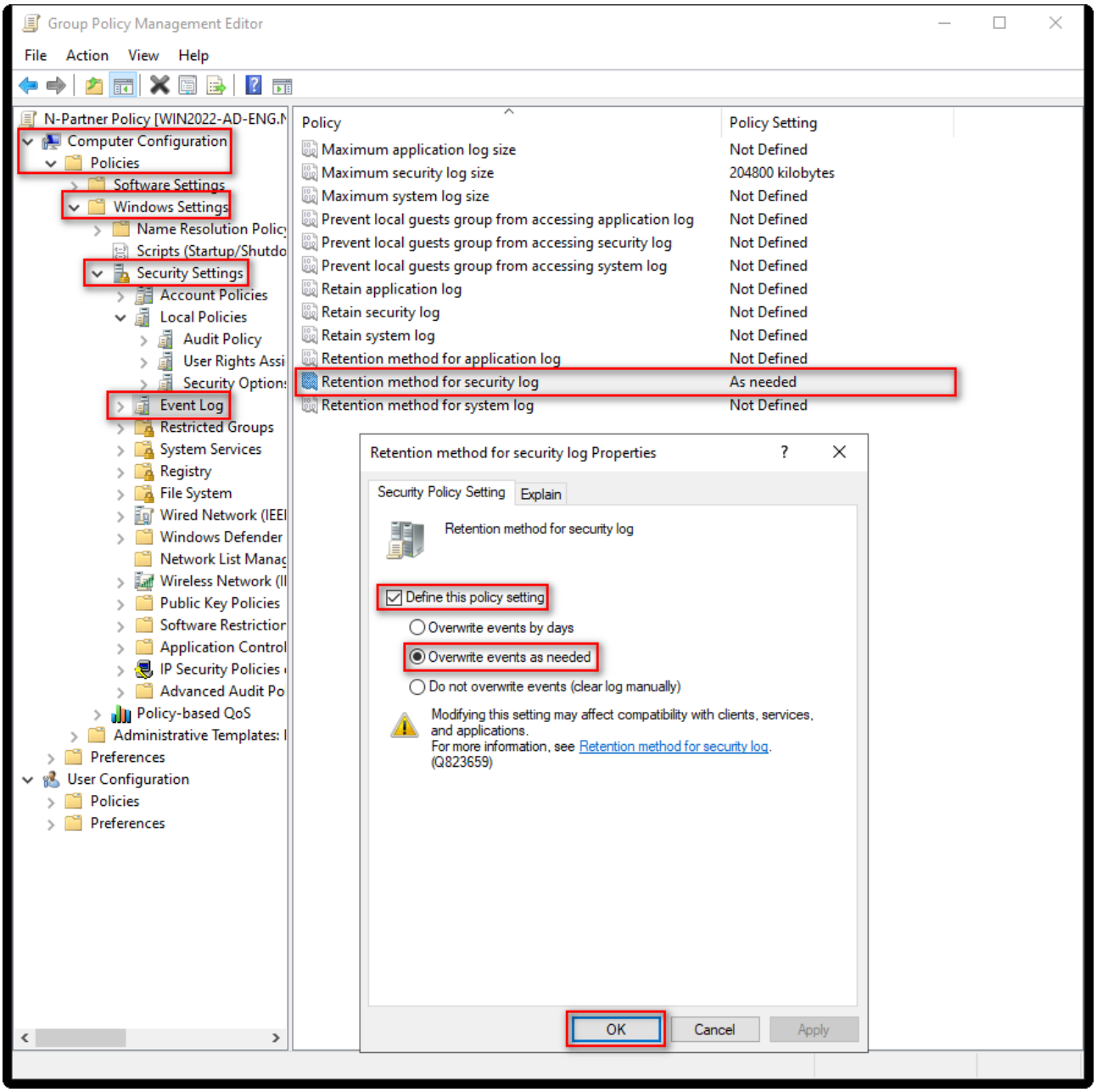
Note: Please adjust the number based on the actual environment.

-> Click “OK.”



(7) Event Log: Maximum Size of Security Log

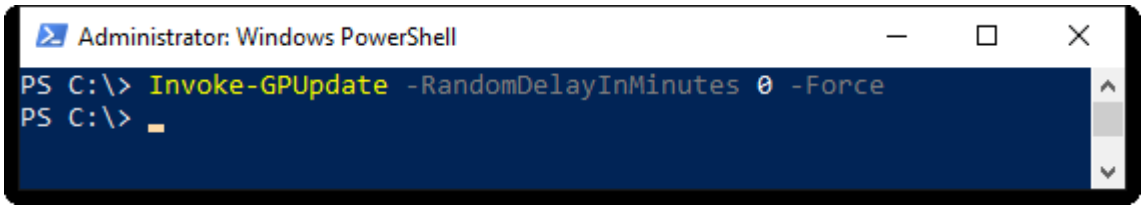
Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Event Log.” Select “Retention method for Security log,” check “Define this policy setting,” choose “Overwrite events as needed,” and click “OK.”



(8) Open “Windows PowerShell.”

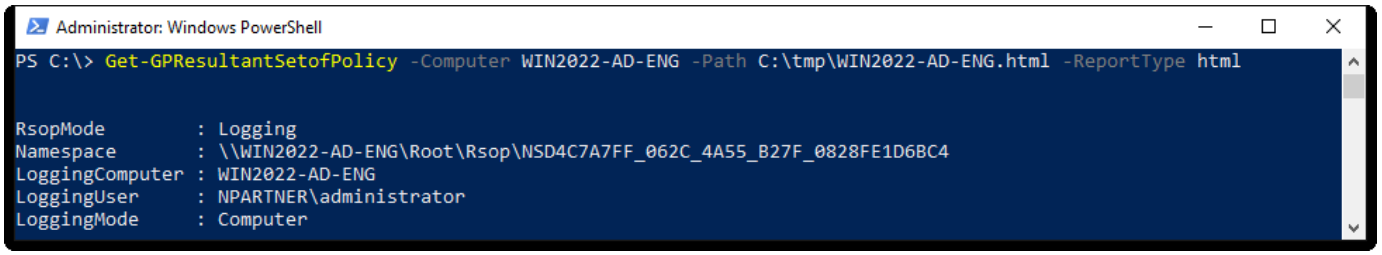
(9) Run the following command to update group policy:

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



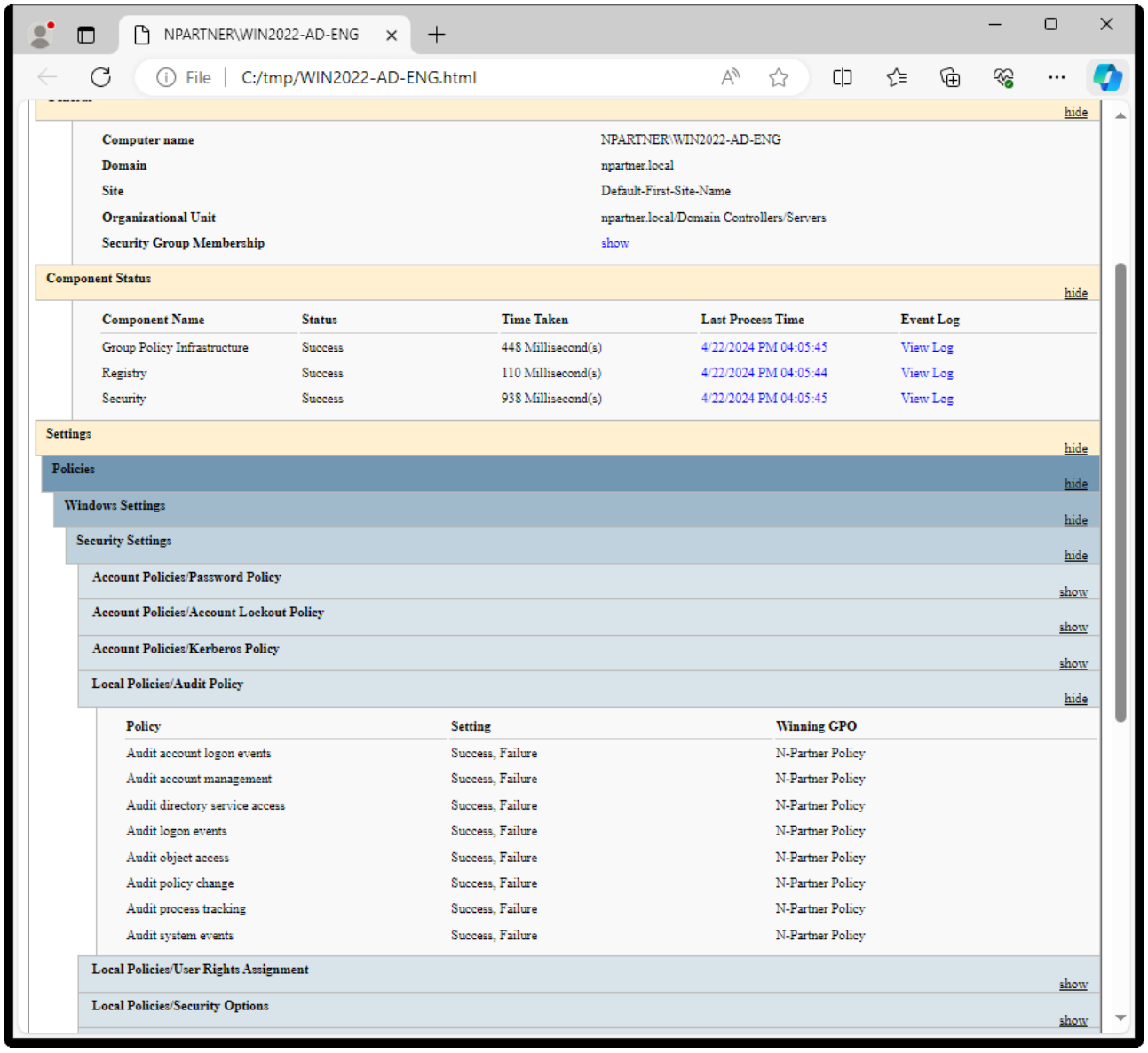
(10) Run the following command to generate the Server Group Policy Report:

```
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.



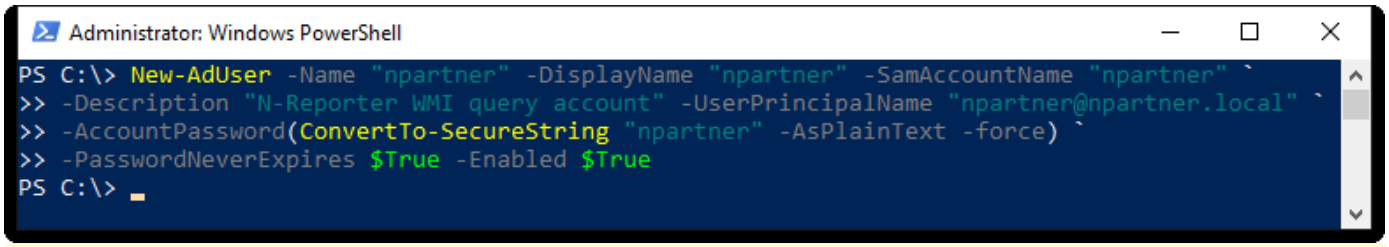
7.3 Add a Non-Admin Account

7.3.1 Add Users

(1) Open “Windows PowerShell.”

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

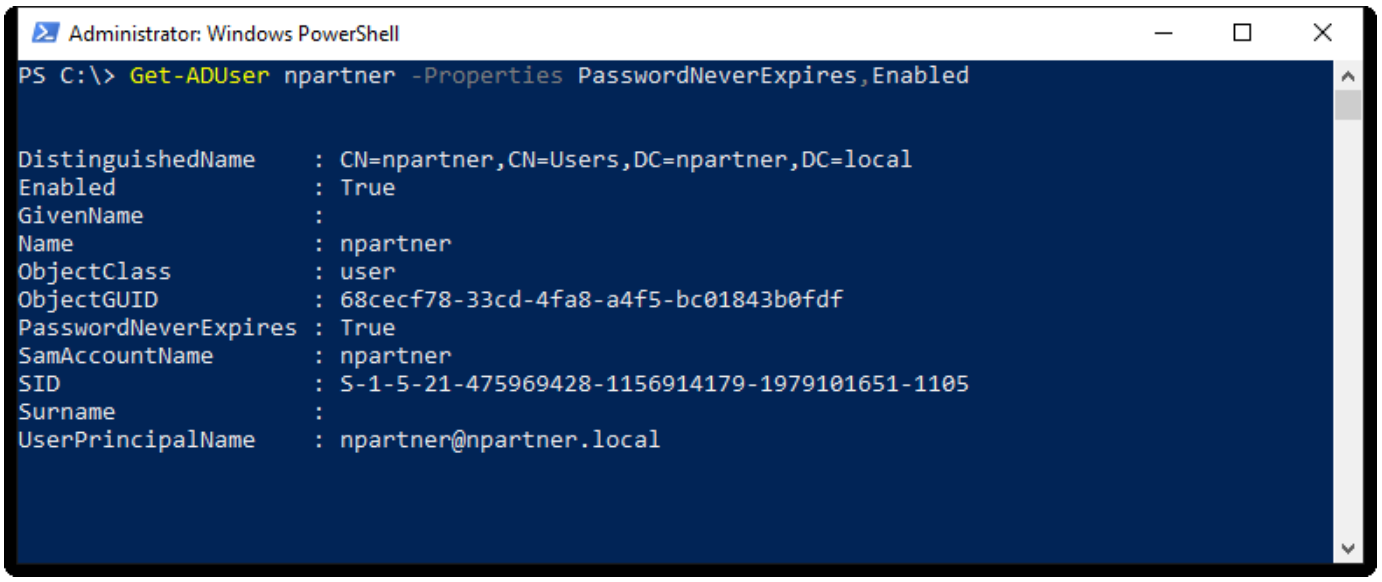
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



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
```

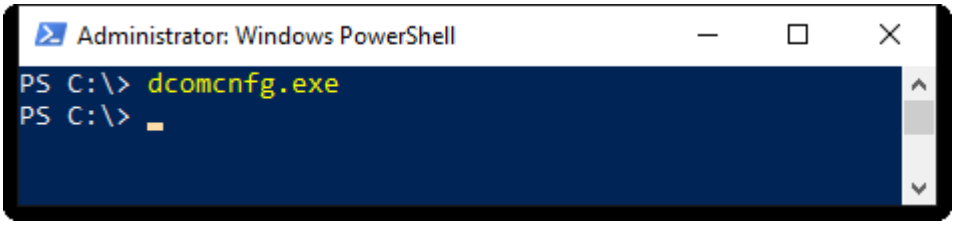


7.3.2 Configure DCOM Permissions

(1) Open “Windows PowerShell.”

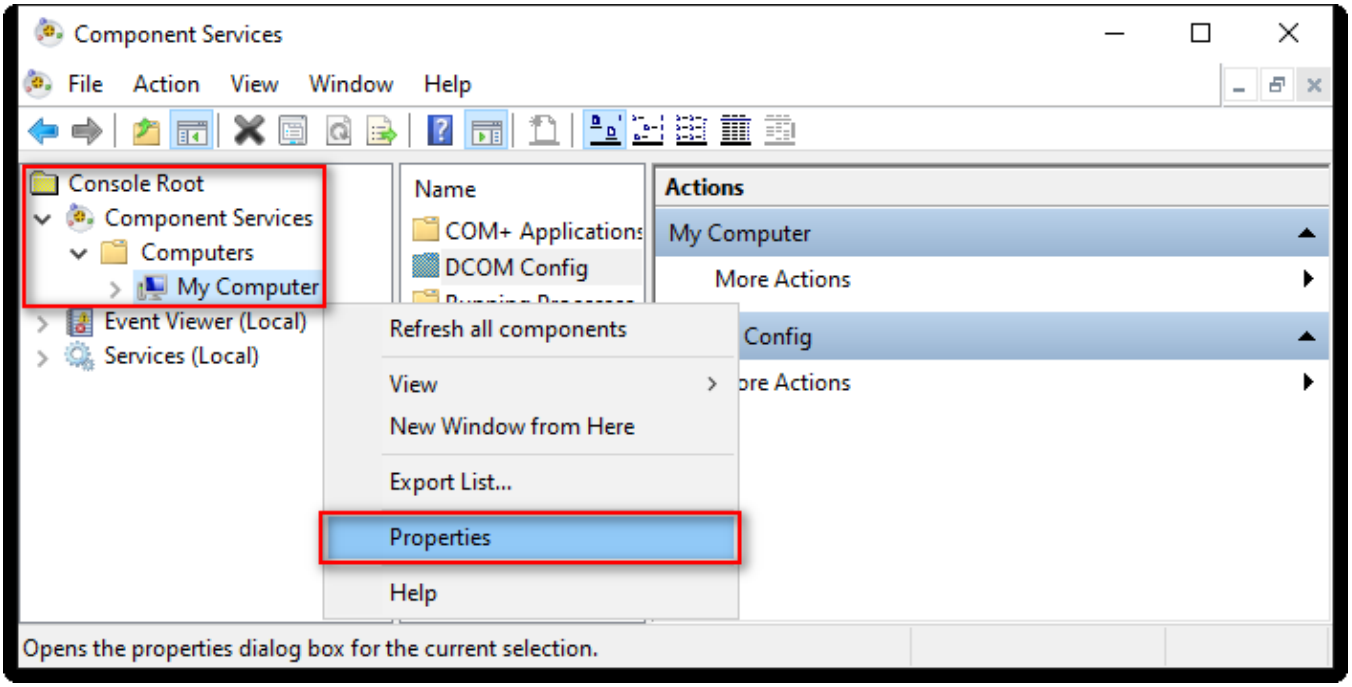
(2) Enter the command below to open component services.

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



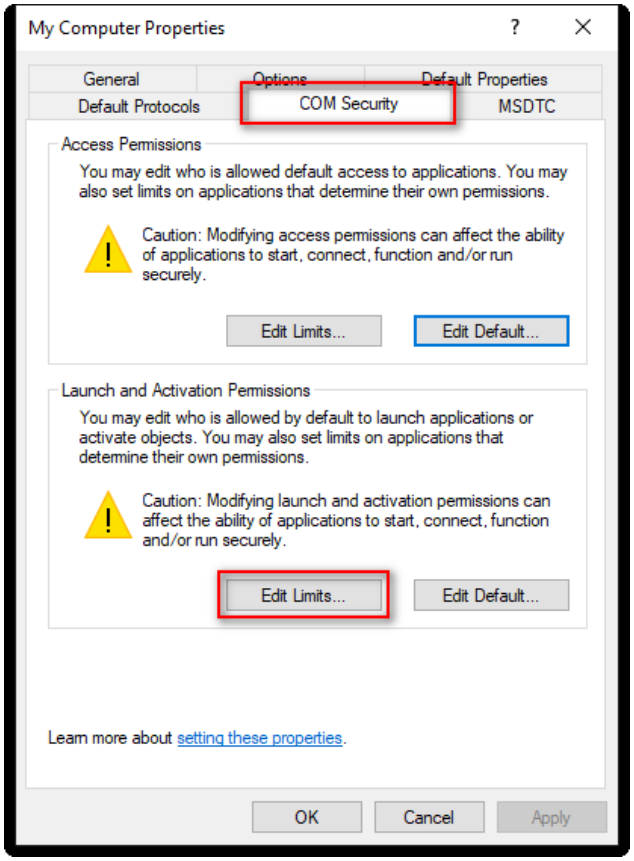
(3) Edit Computer Properties

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



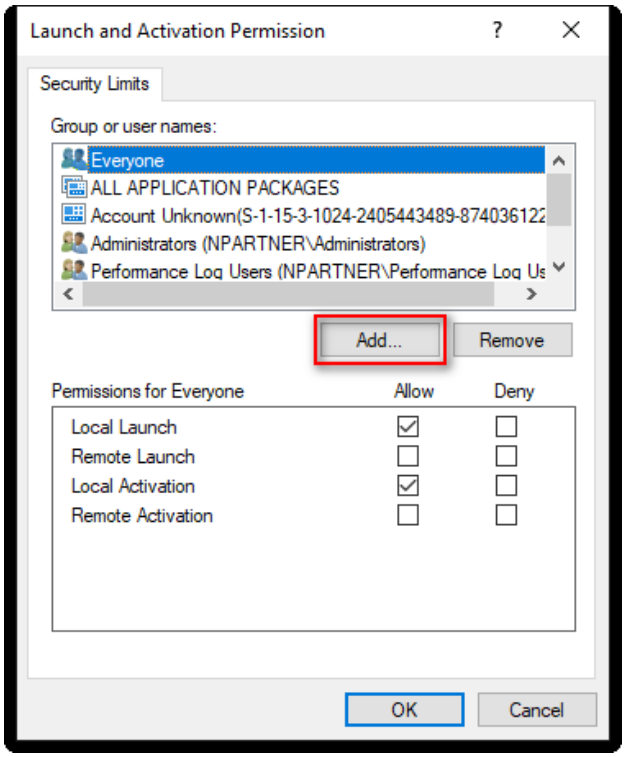
(4) Enable Permissions

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



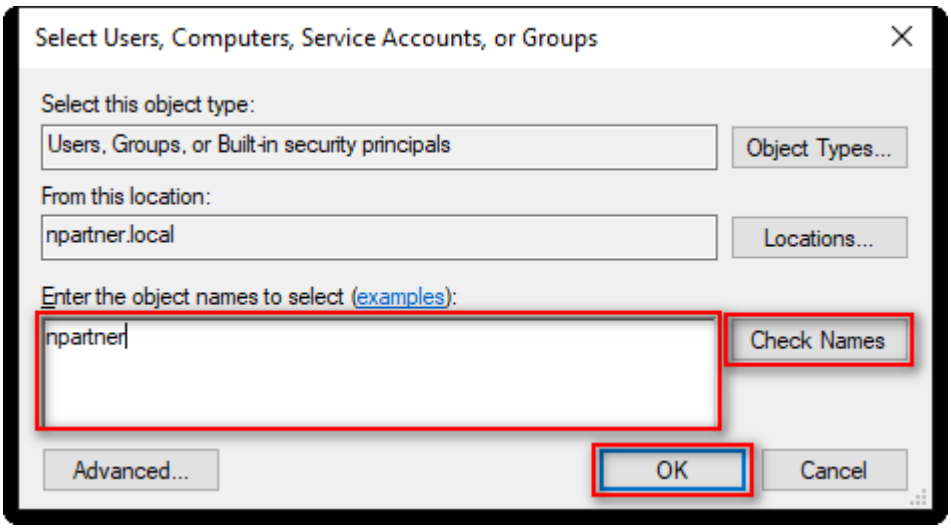
(5) Add DCOM User Permissions

Click “Add.”



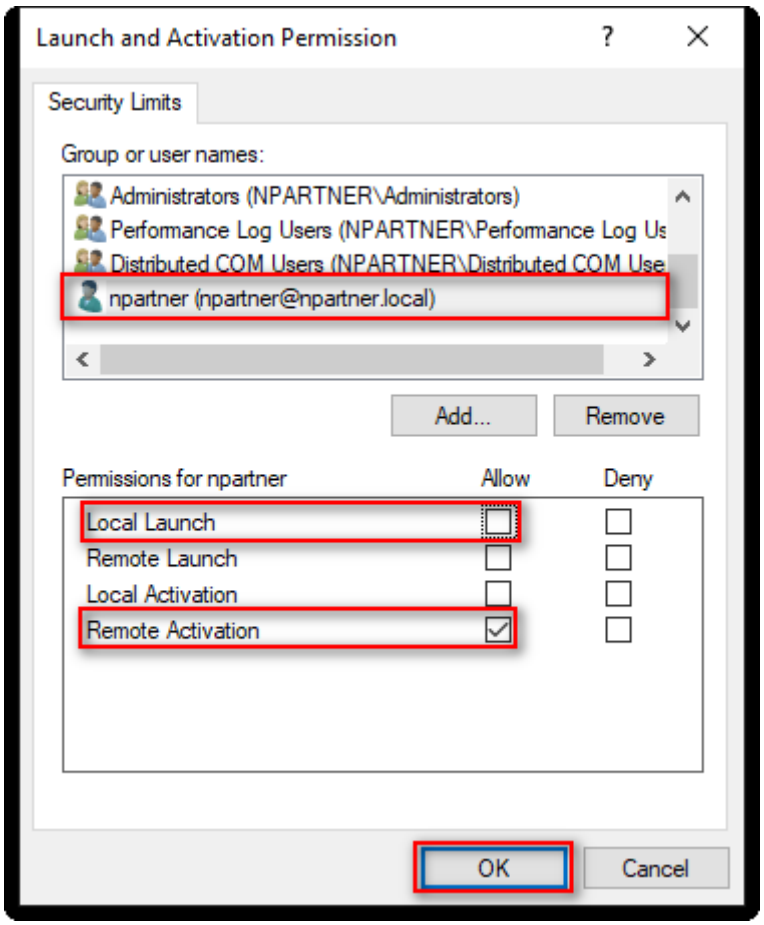
(6) Enter your Username

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

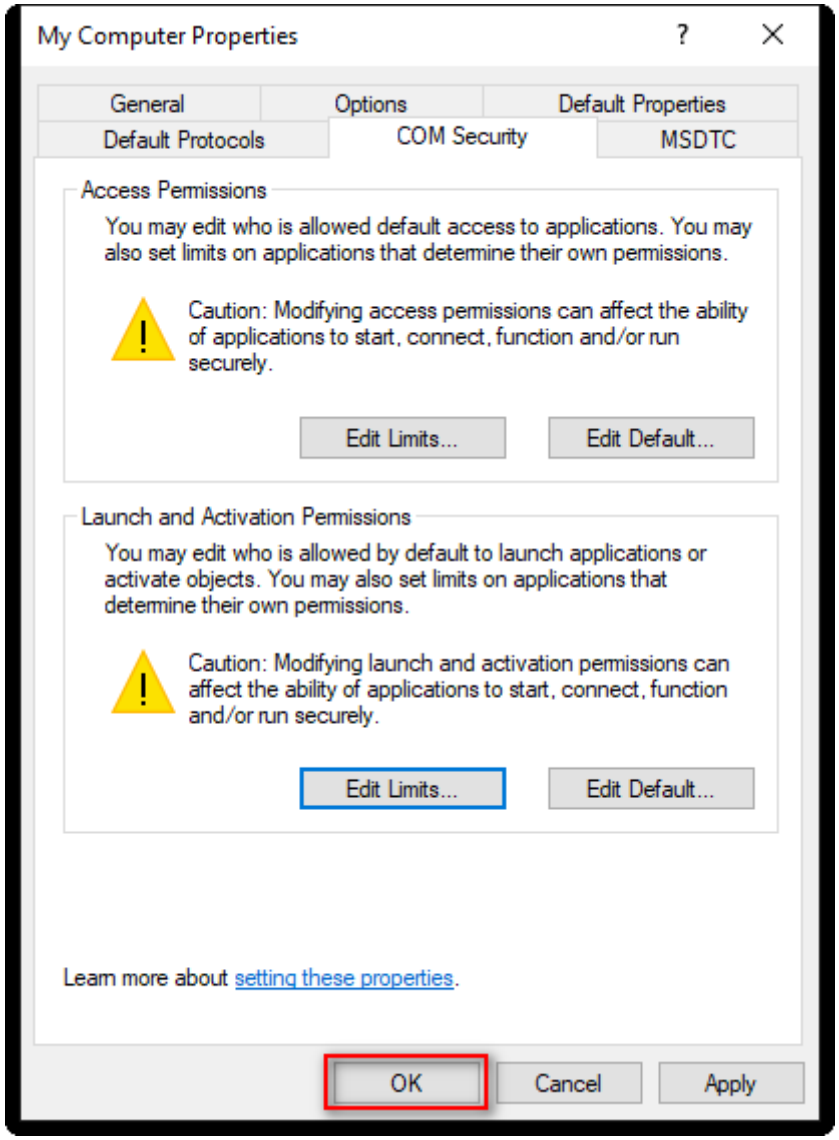


(7) Set User Permissions

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

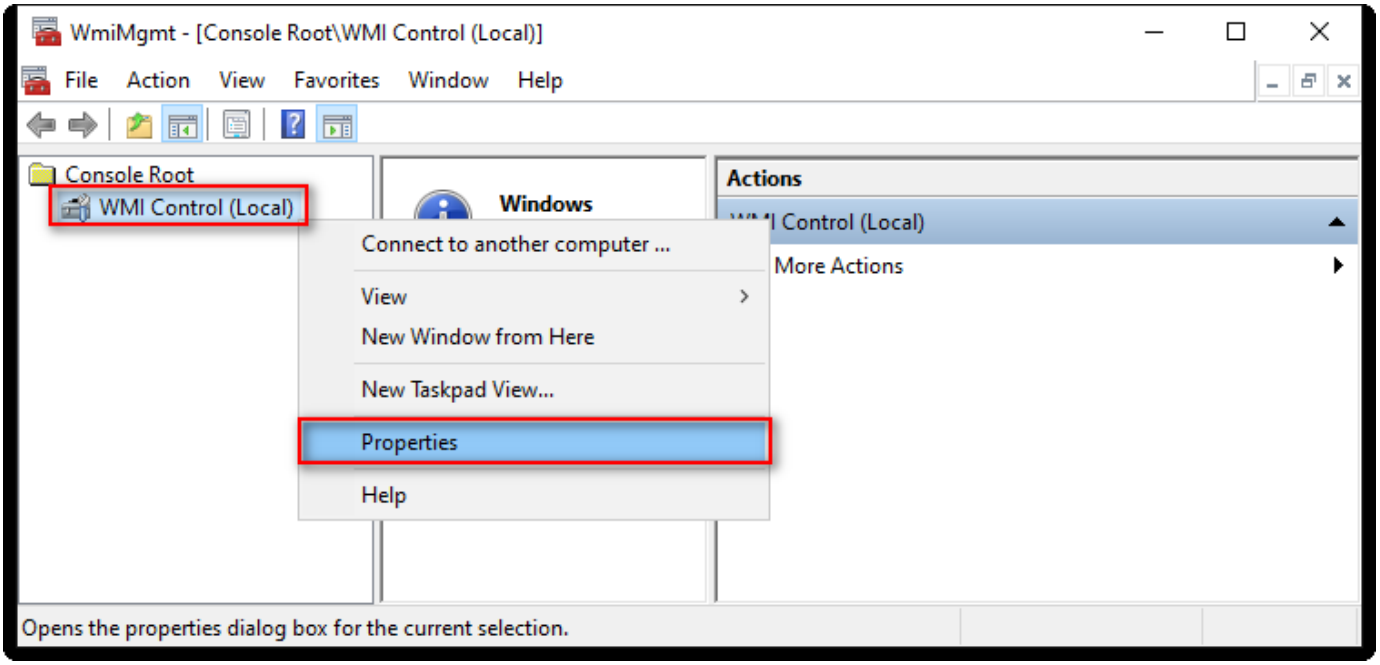
(1) Open “Windows PowerShell.”

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

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

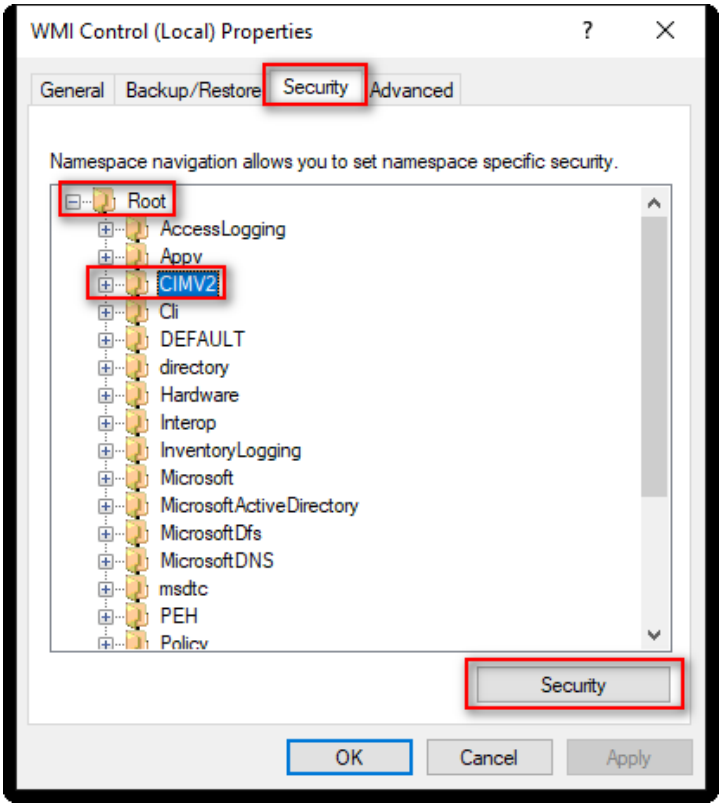
(3) Edit WMI Control

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



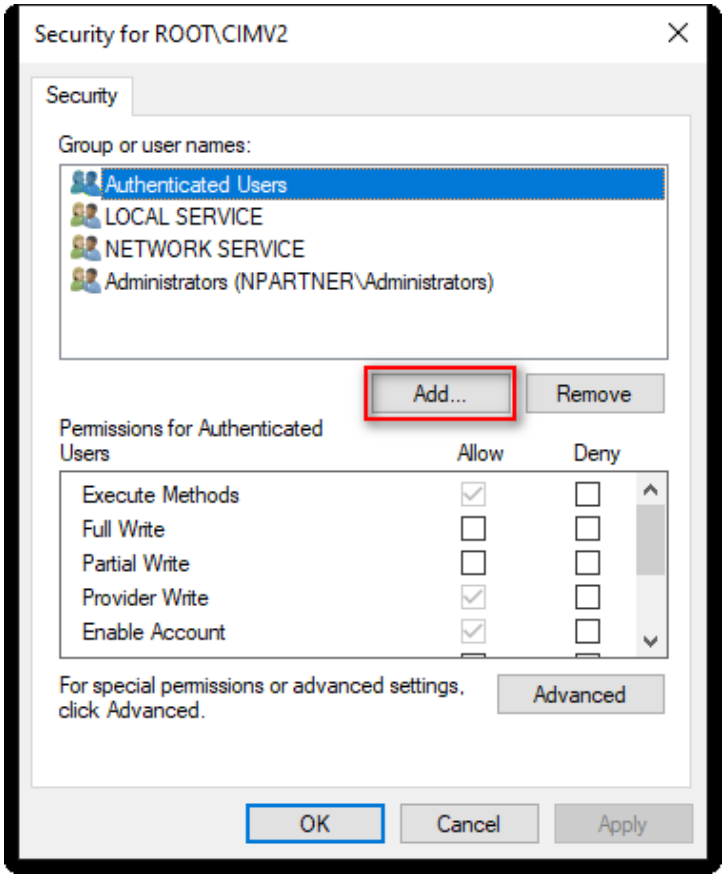
(4) Edit CIMV2 Security

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



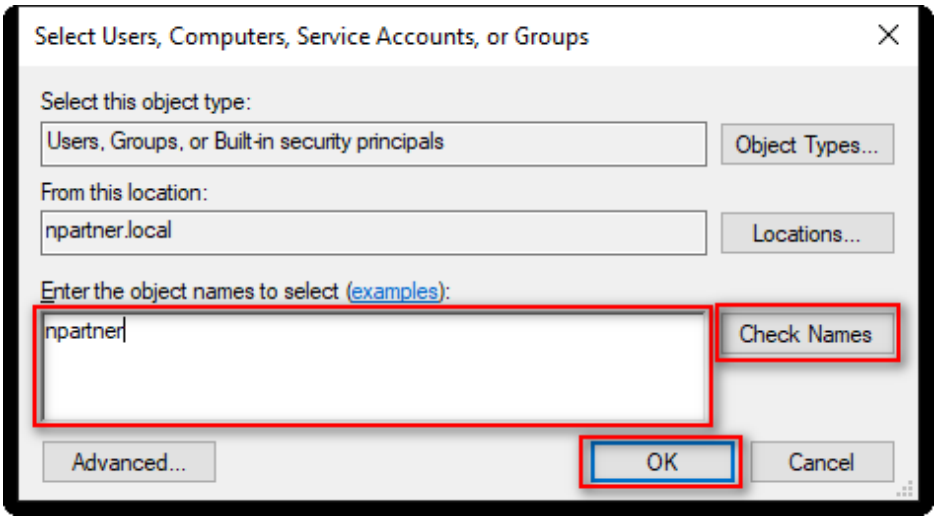
(5) Add WMI User Permissions

Click “Add.”



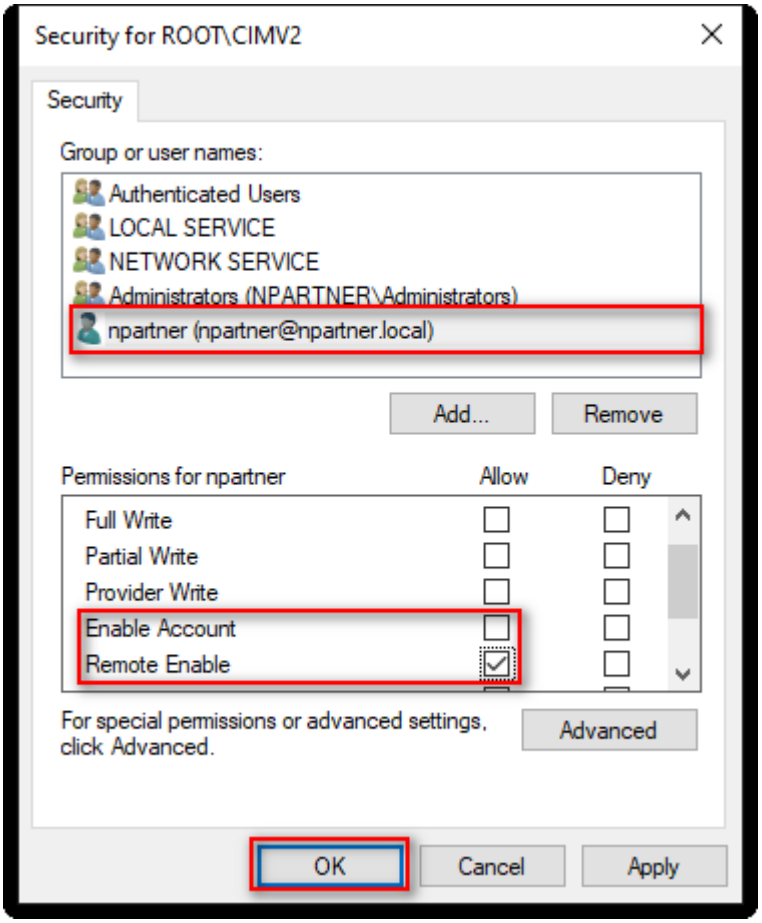
(6) Enter User

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



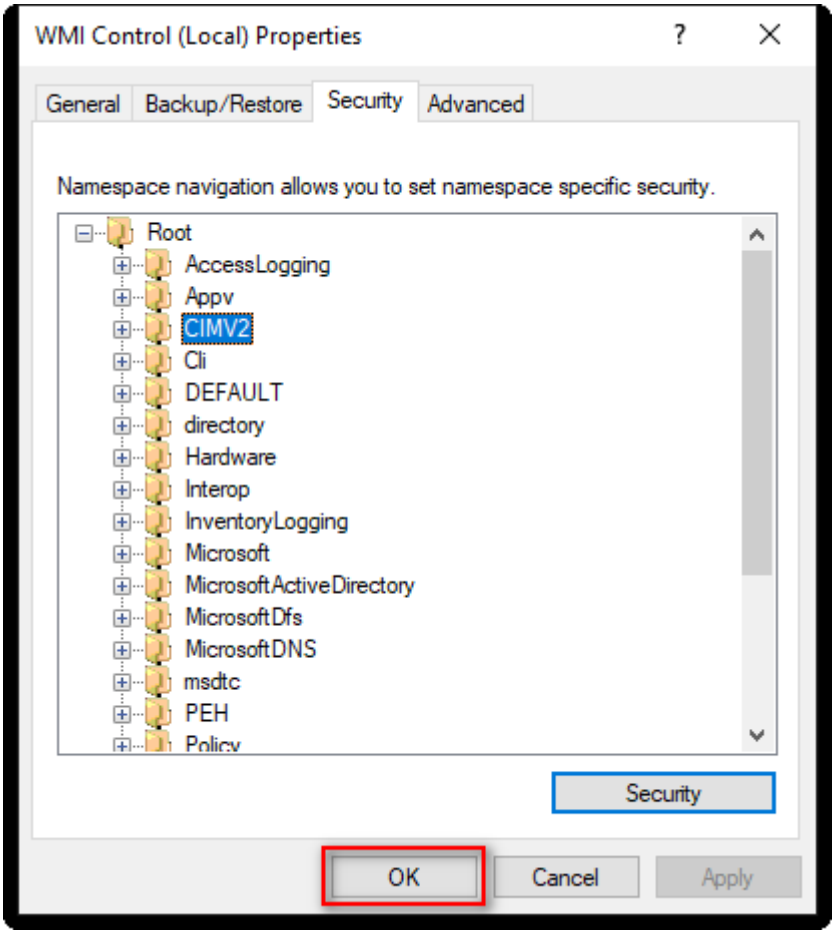
(7) Set User Permissions

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



(8) Confirm User Permissions

Click “OK.”

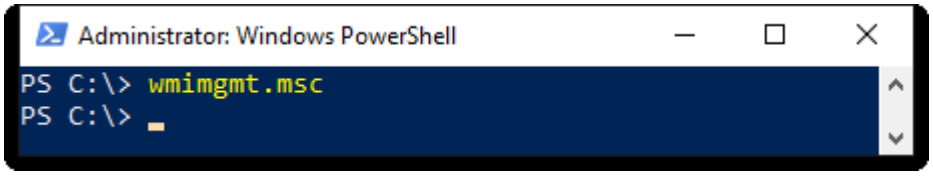


7.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows PowerShell.”

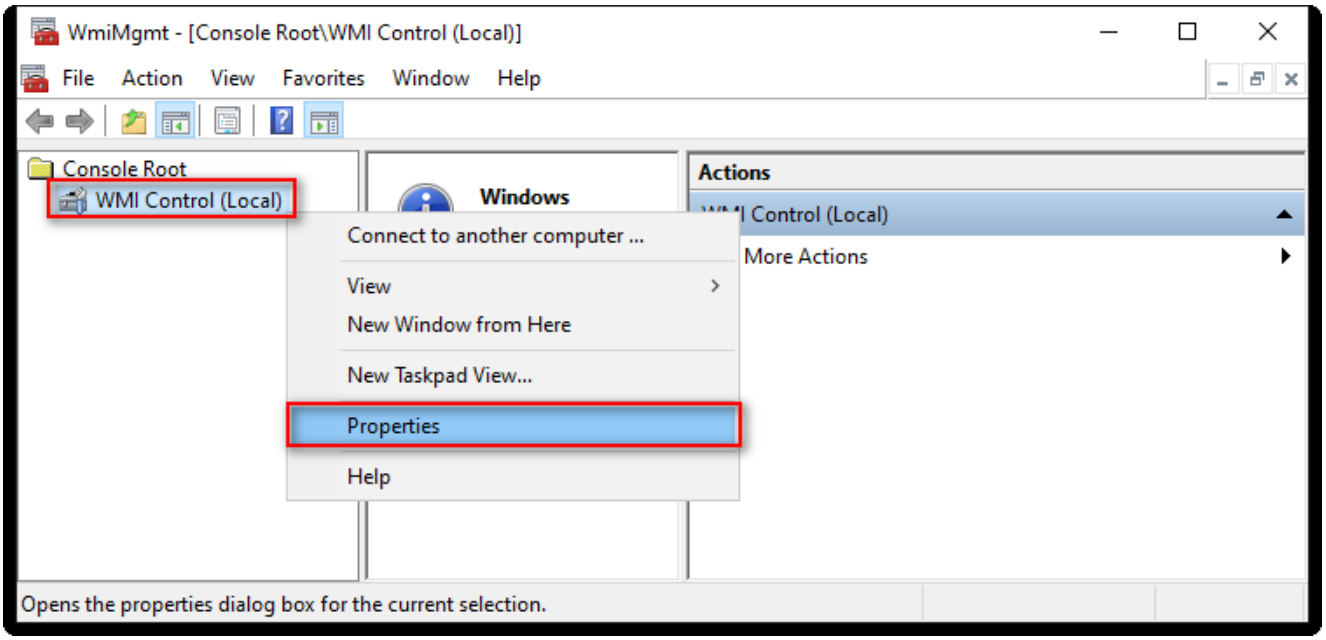
(2) Enter the command below to enable component services.

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



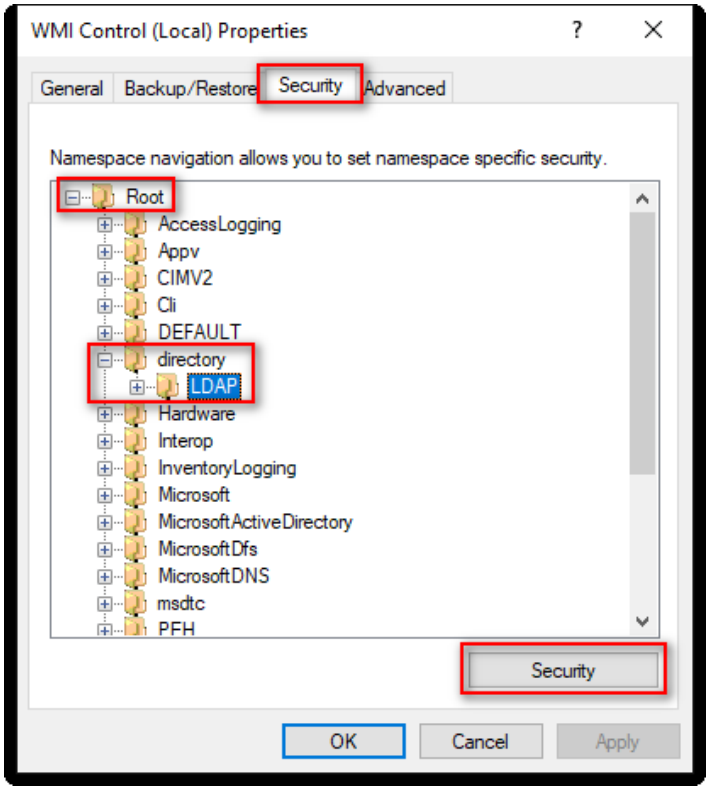
(3) Edit WMI Control

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



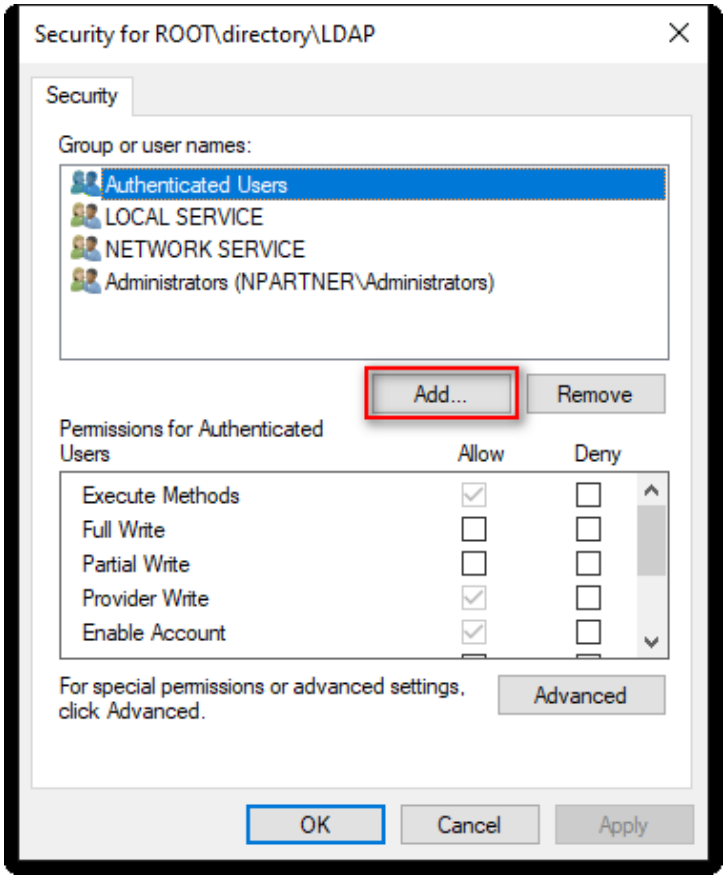
(4) Edit LDAP Security

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



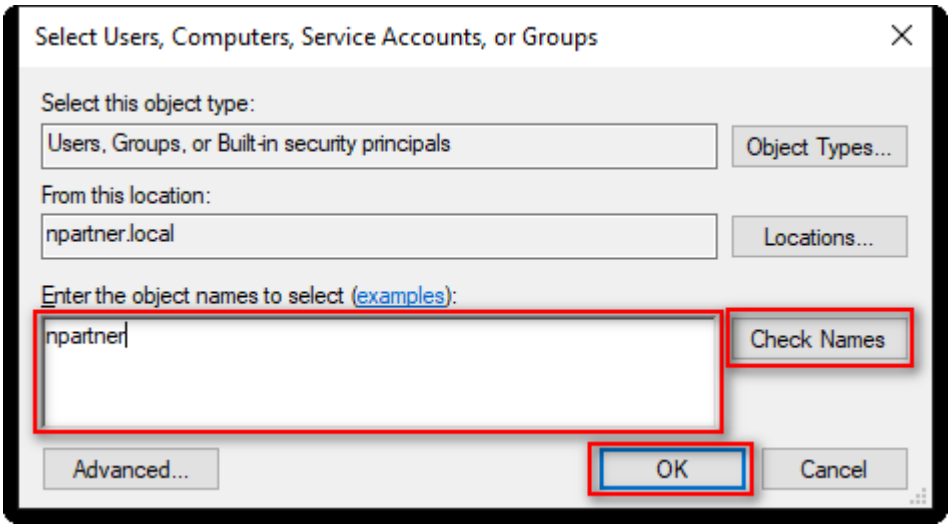
(5) Add WMI User Permissions

Click “Add.”



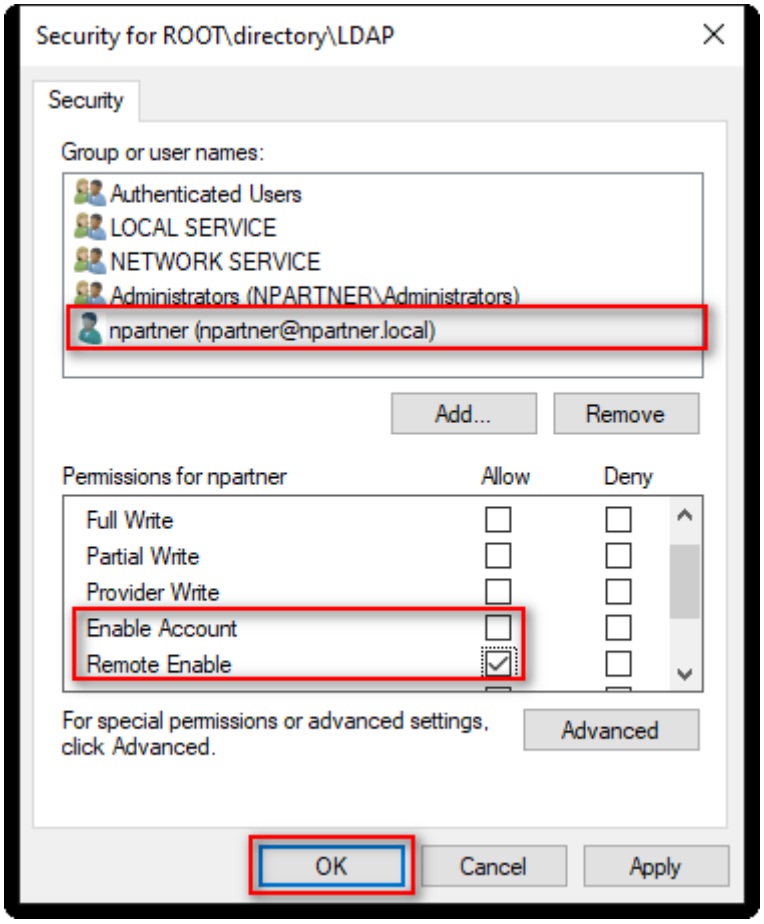
(6) Enter Your Username

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



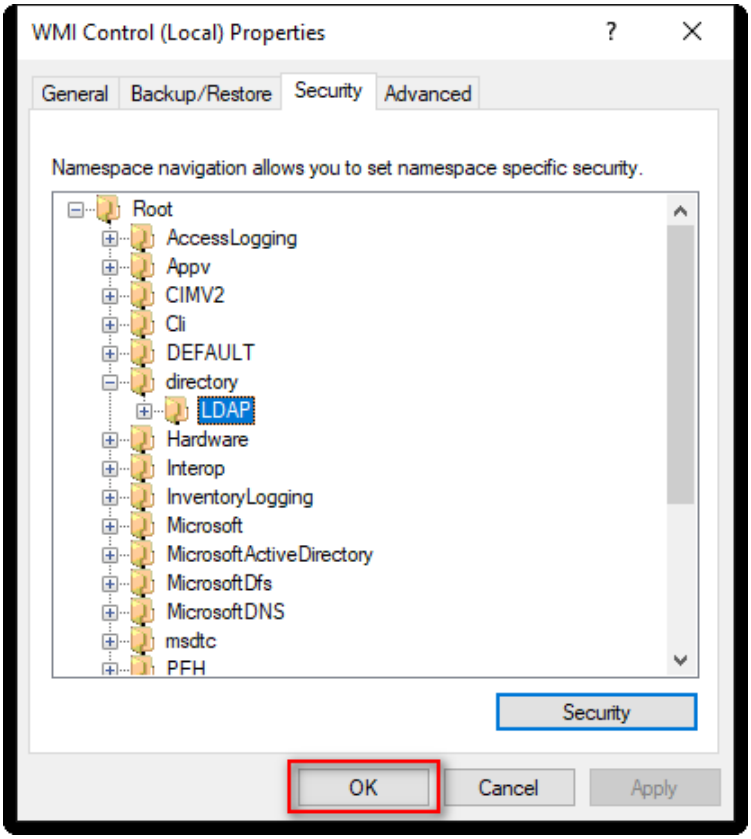
(7) Set Your User Permissions

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



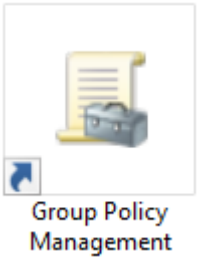
(8) Confirm User Permissions

Click "OK."



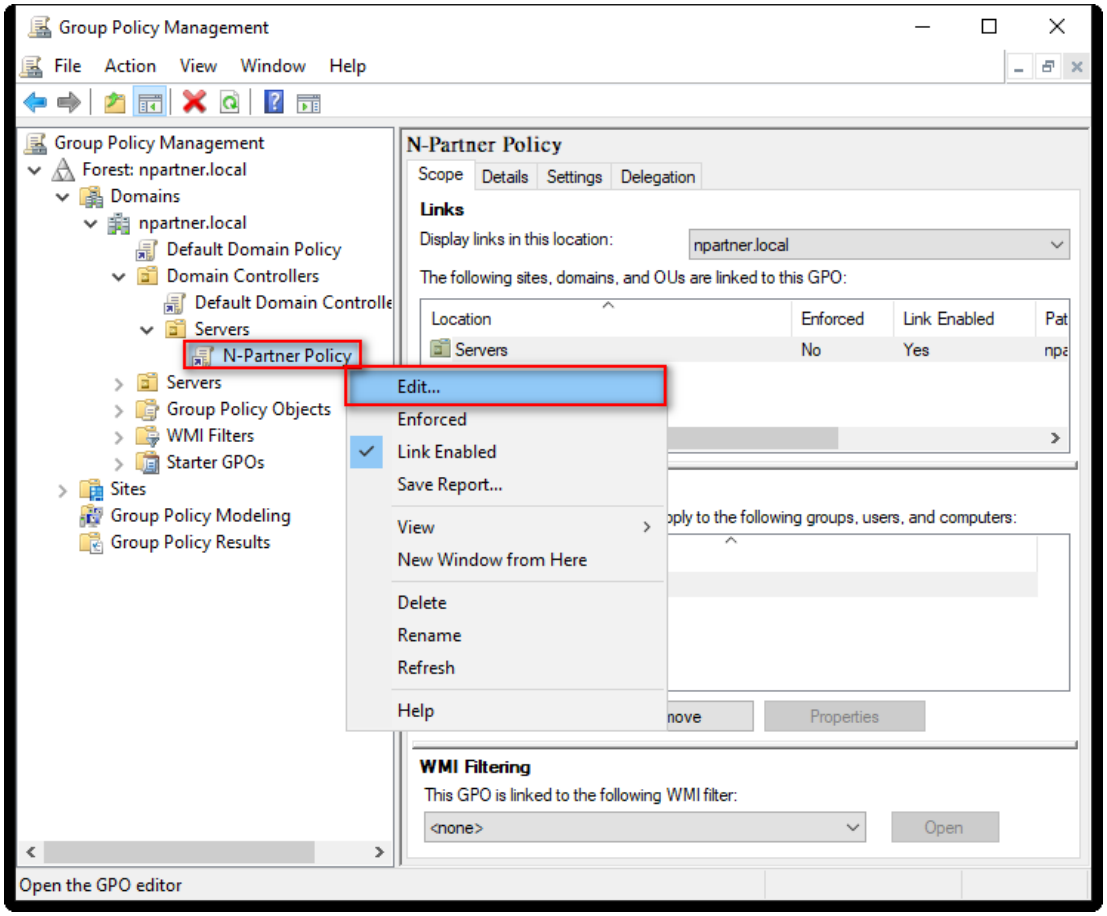
7.3.4 Configure Event Log Read Permissions

(1) Open “Group Policy Management.”



(2) Edit the Group Policy Object

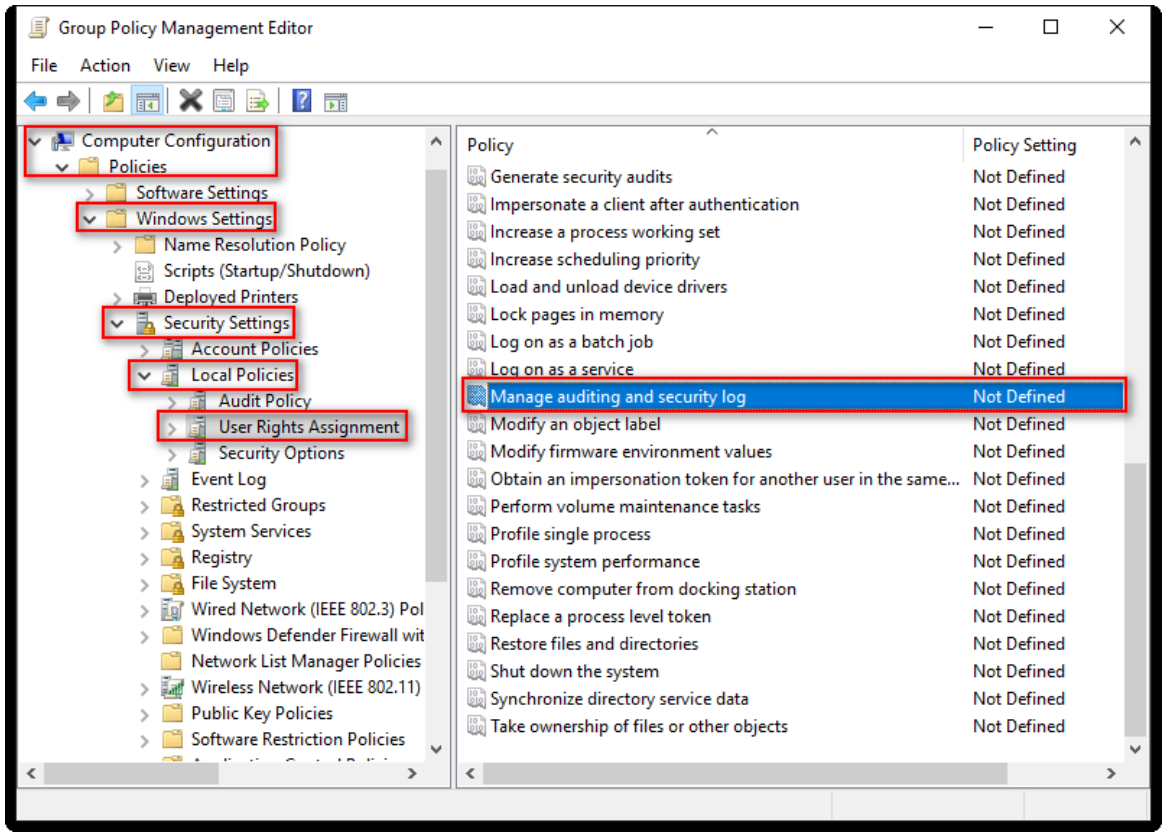
Right-click the “N-Partner Policy” Group Policy Object and select “Edit.”



(3) Configure Log Permissions

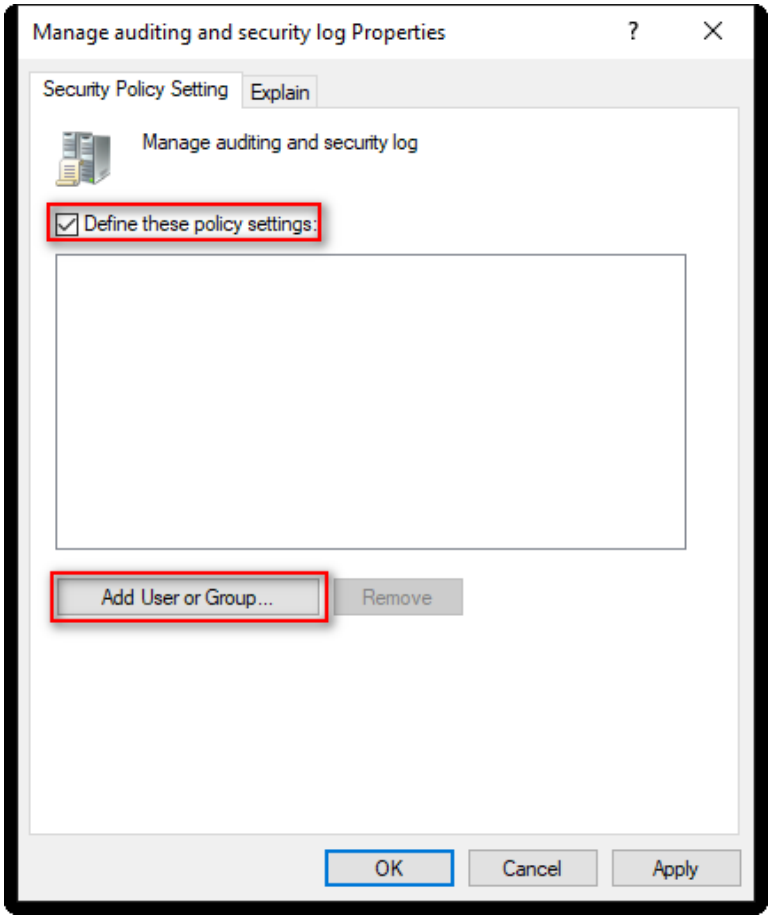
Navigate to “Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → User Rights Assignment.”

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



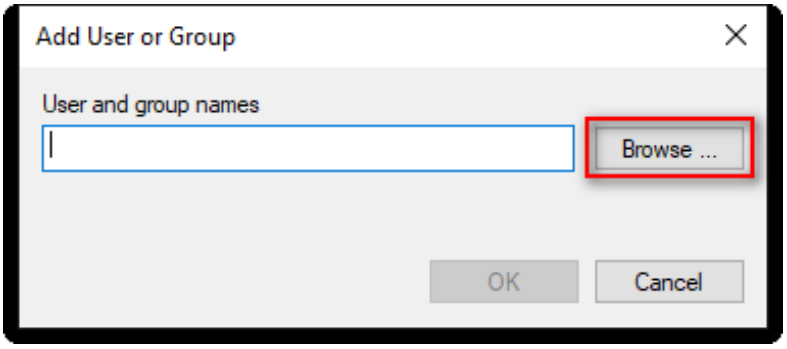
(4) Add Audit Log Management User

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



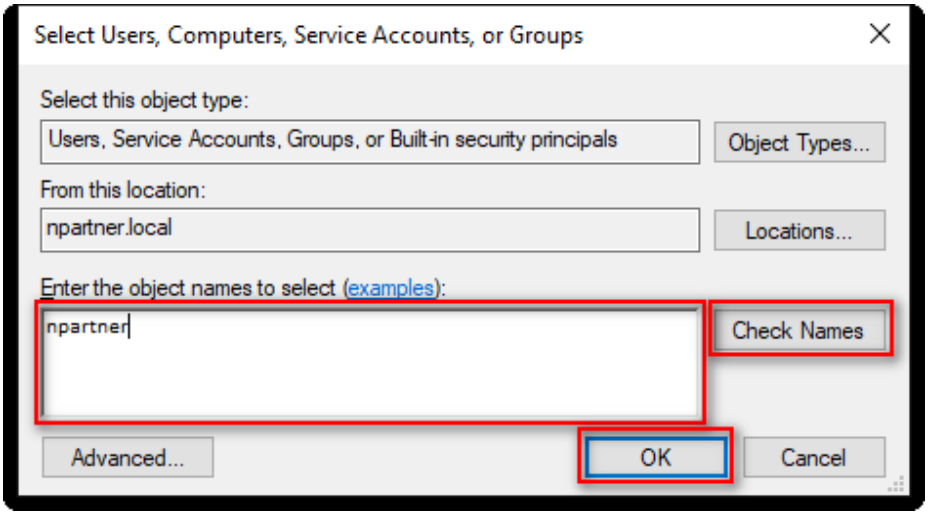
(5) Search for User

Click “Browse.”



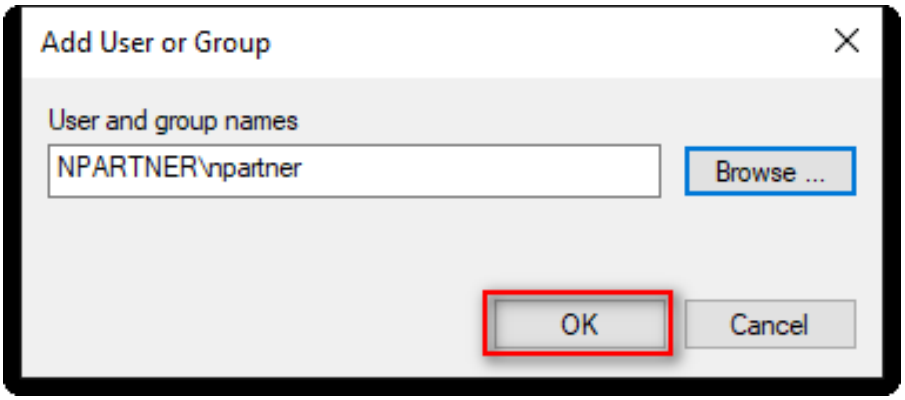
(6) Enter User Account

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



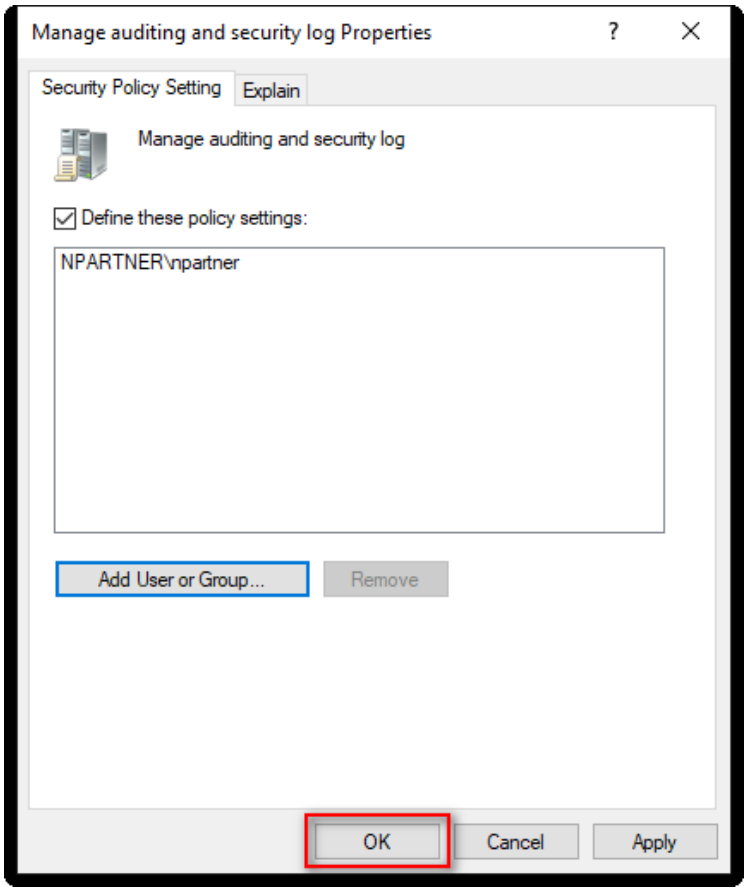
(7) Confirm User

Click “OK.”



(8) Confirm Log Settings

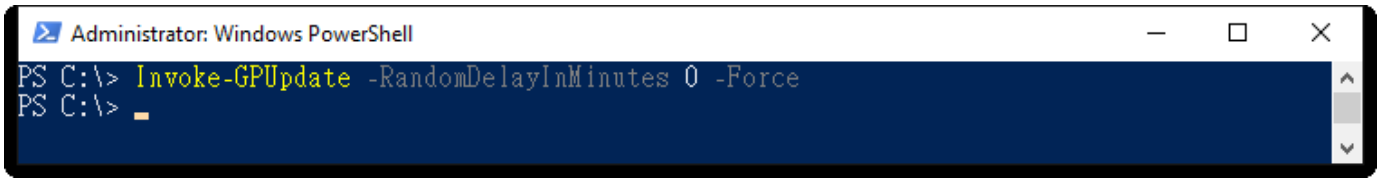
Click “OK” to save the configuration.



(9) Open “Windows PowerShell.”

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

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

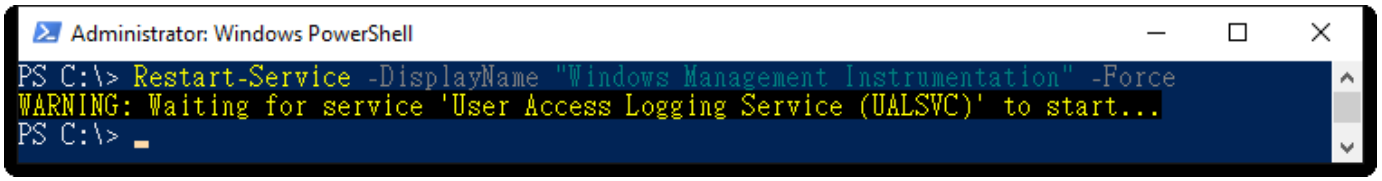


7.3.5 Restart the WMI Service

(1) Open “Windows PowerShell.”

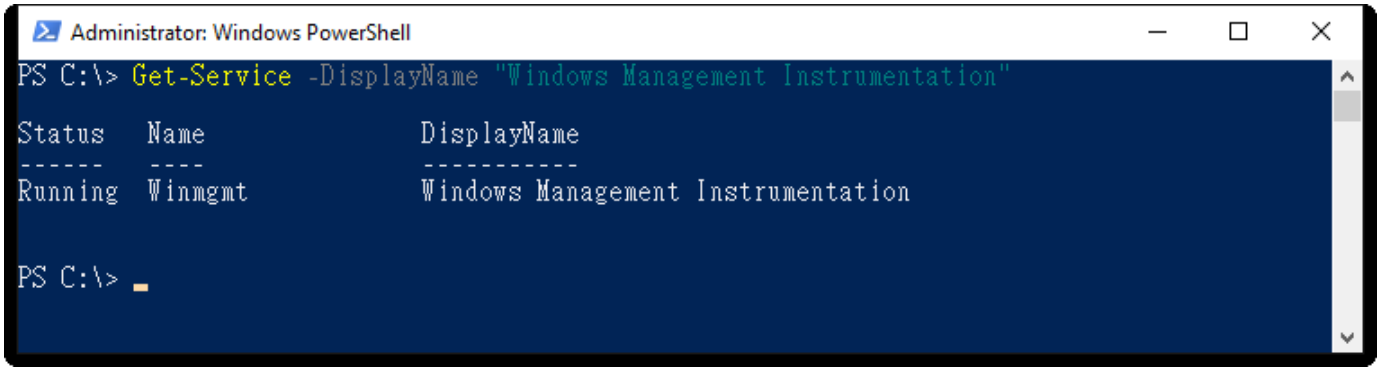
(2) Run the following command to restart the WMI Service:

```
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"
```



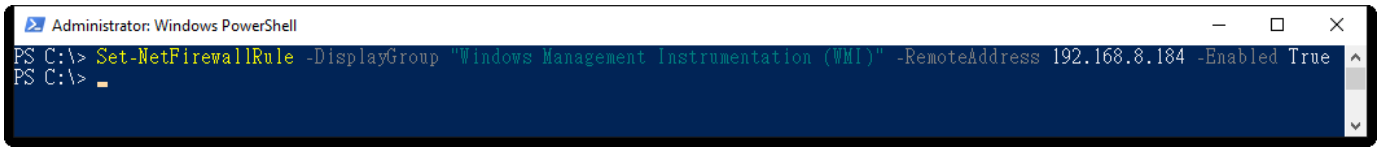
7.4 Configure Firewall

(1) Open “Windows PowerShell.”

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

Run the following command:

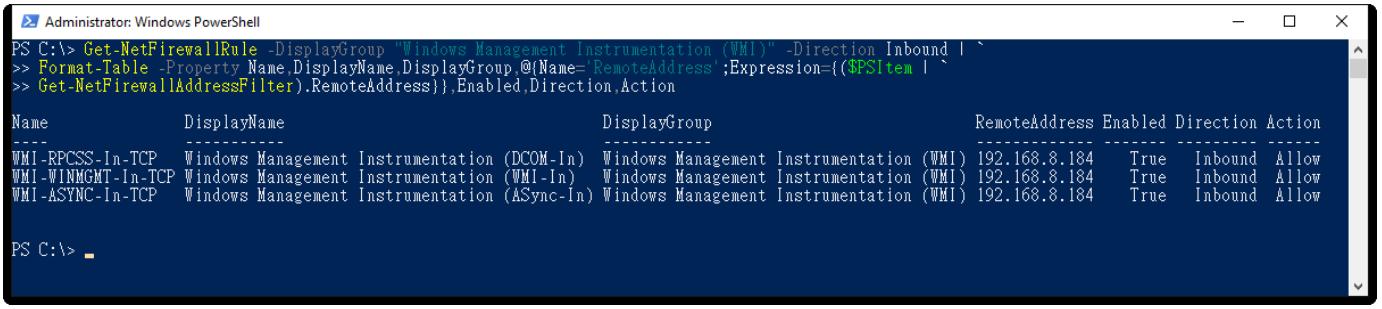
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -
RemoteAddress 192.168.8.184 -Enabled True
```



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

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

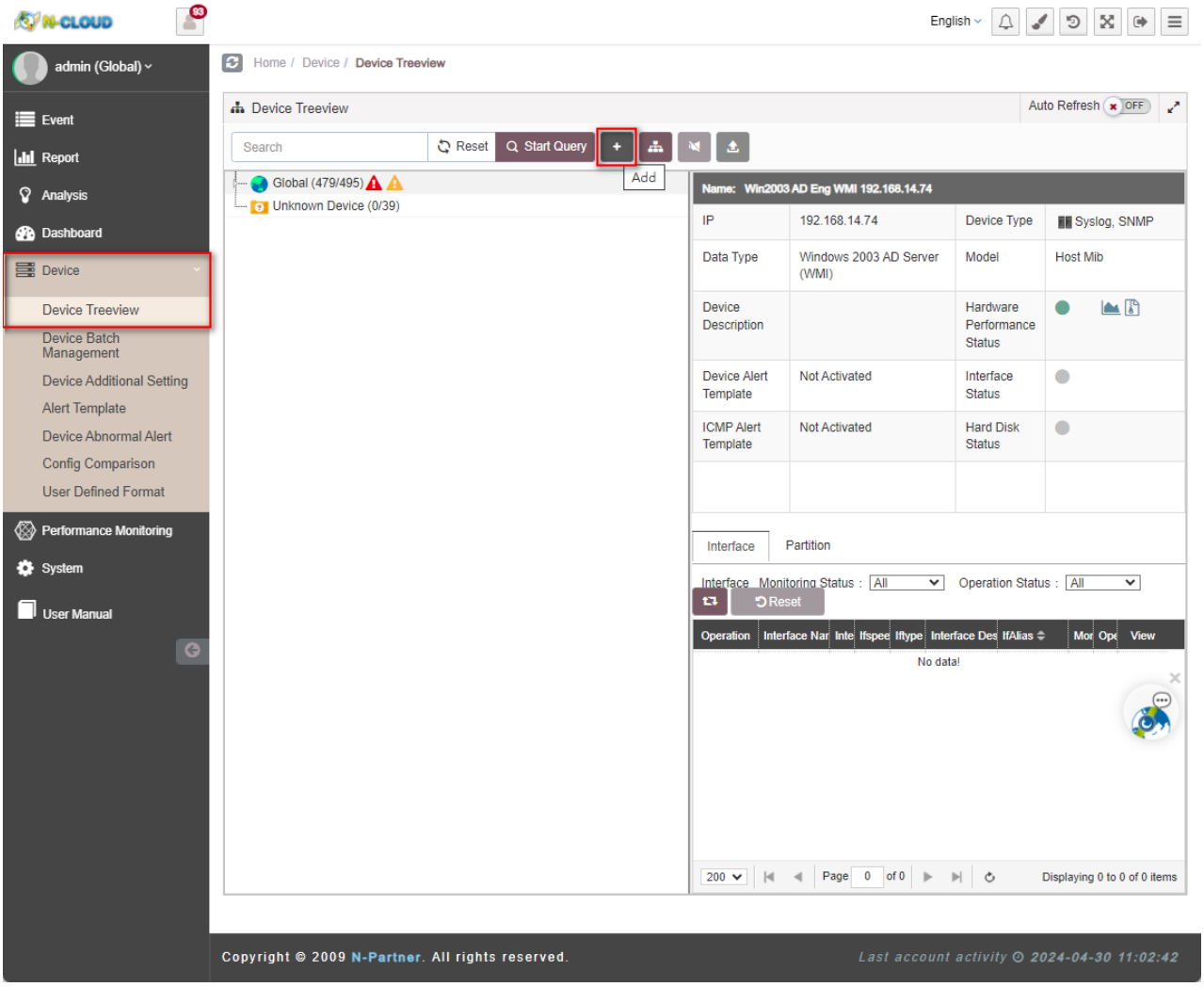
```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction
Inbound |
>> Format-Table -Property Name,DisplayName,DisplayGroup,
>> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}},
>> Enabled,Direction,Action
```



8. N-Reporter

(1) Add a Windows AD WMI Device

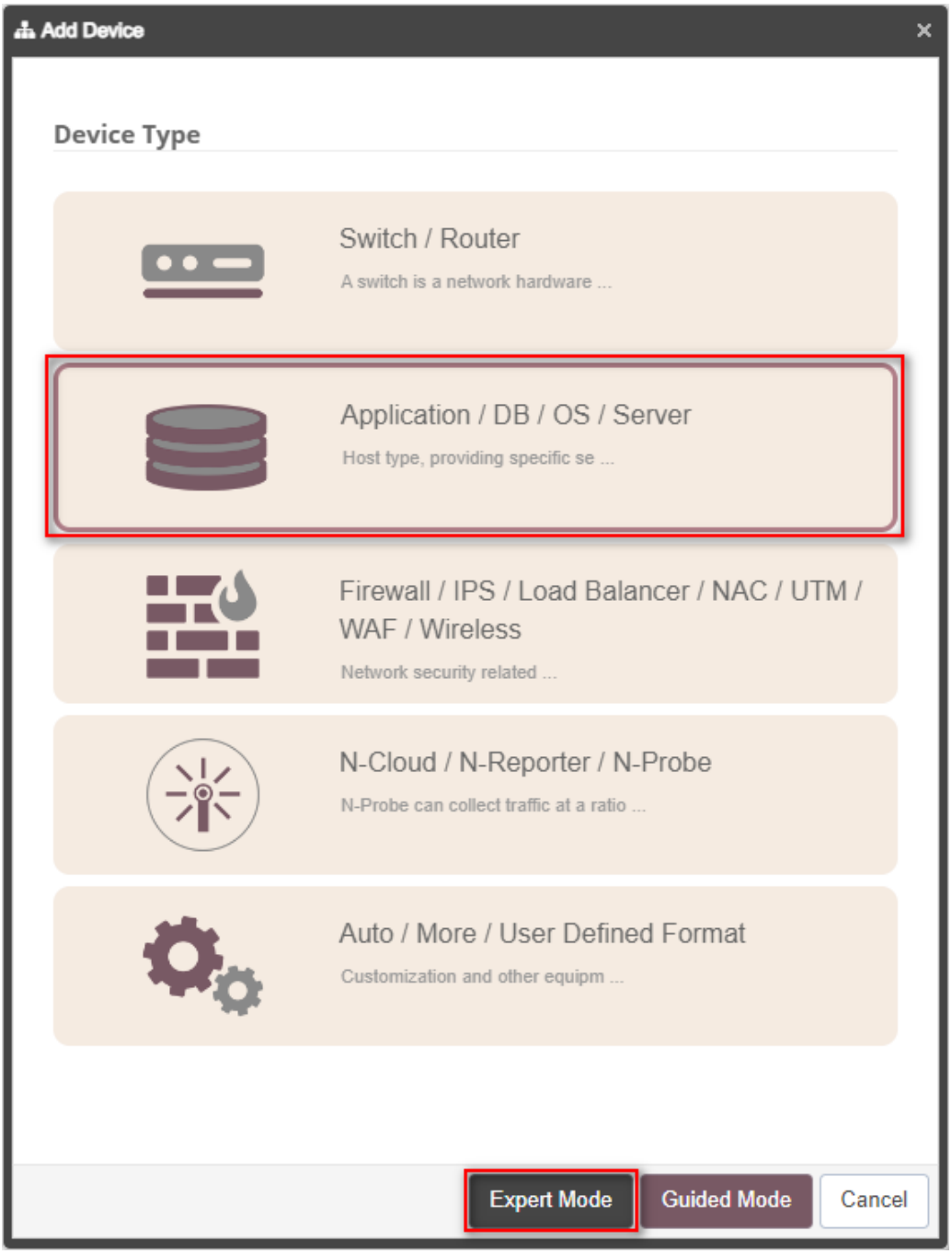
Go to “Device → Device Treeview,” then click “Add.”



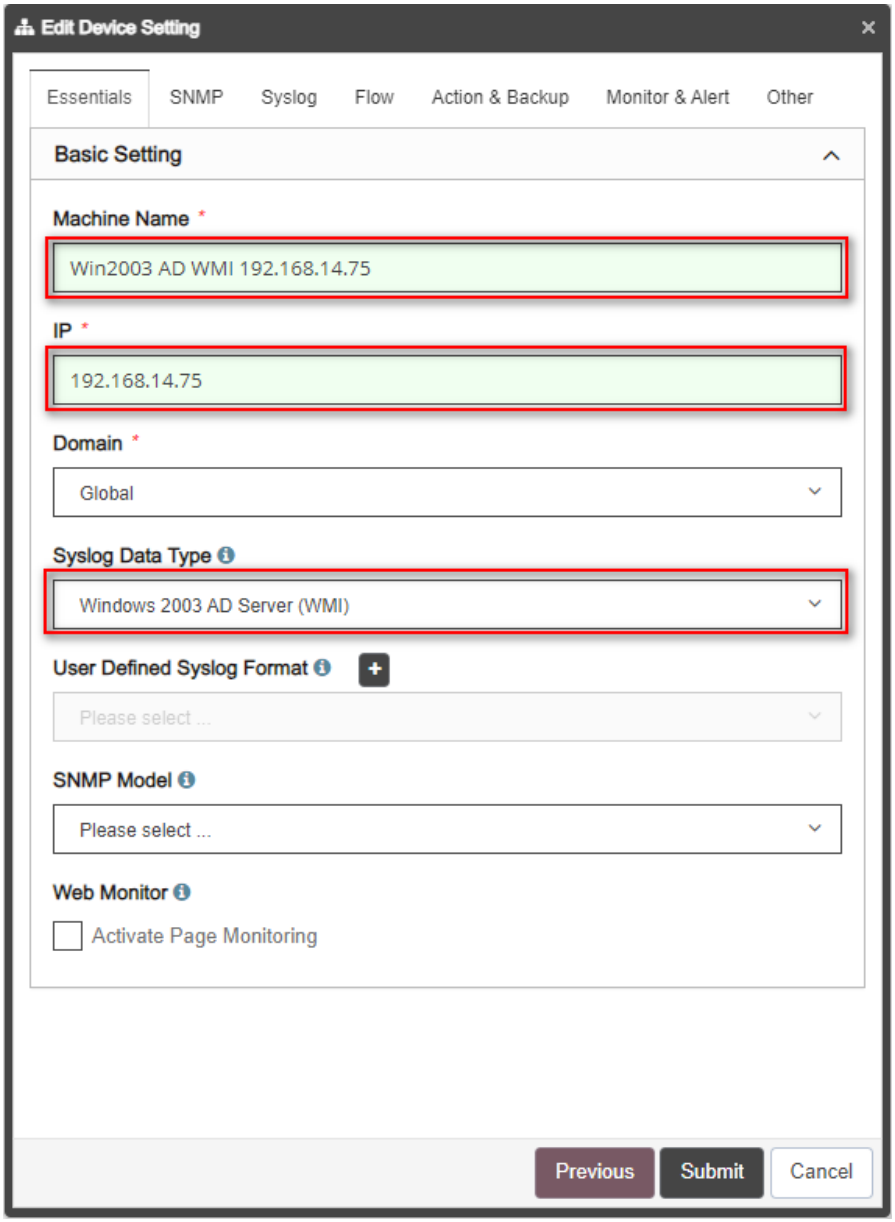
8.1 For Windows 2003 or Earlier

(1) Configure a Windows AD WMI Device

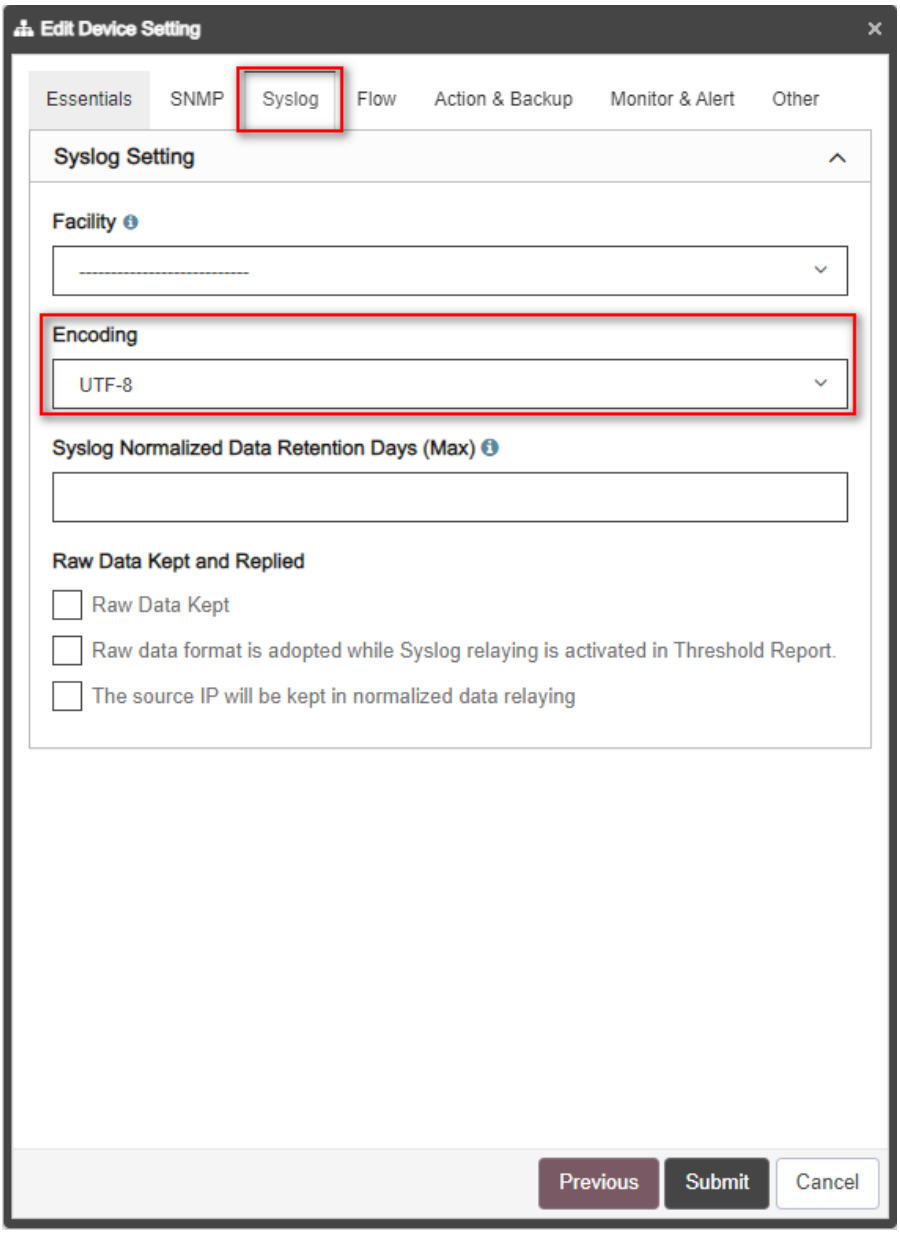
Click “Application / DB / OS / Server,” then select “Expert Mode.”



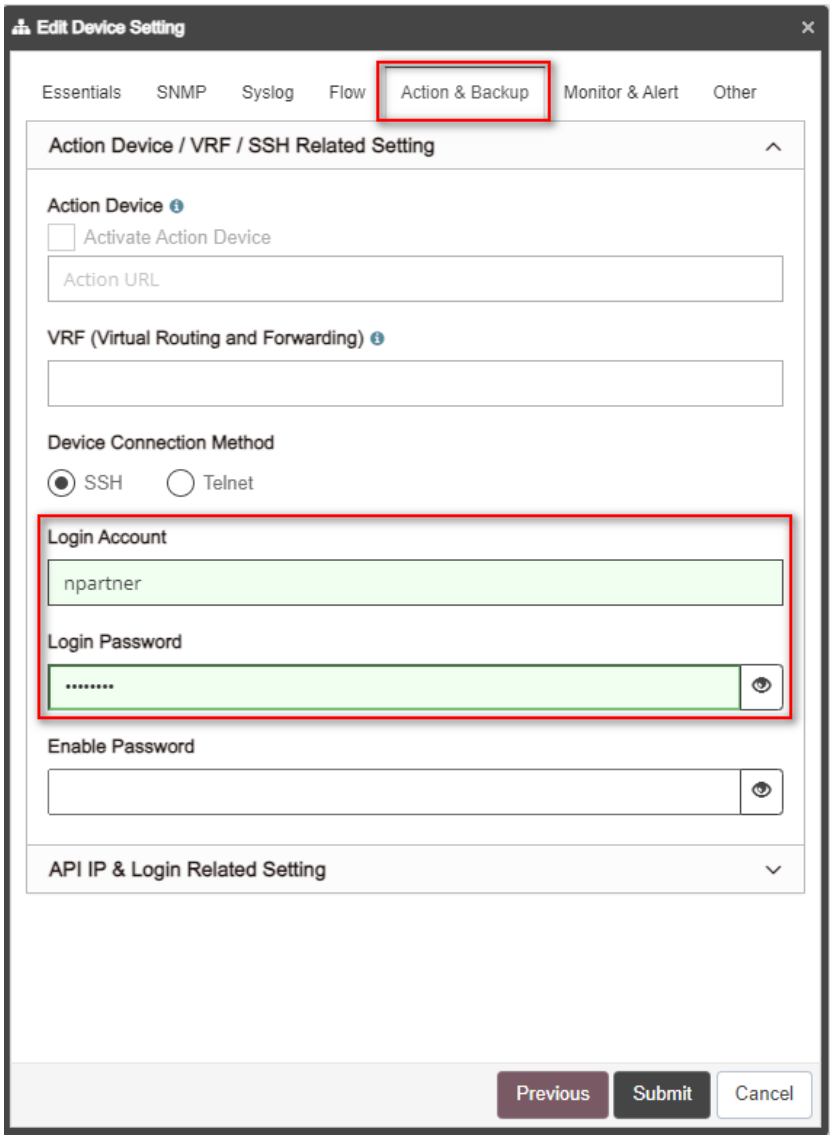
(2) Enter the “device name” and “IP address.” For Syslog Data Type, select “Windows 2003 AD Server (WMI).”



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

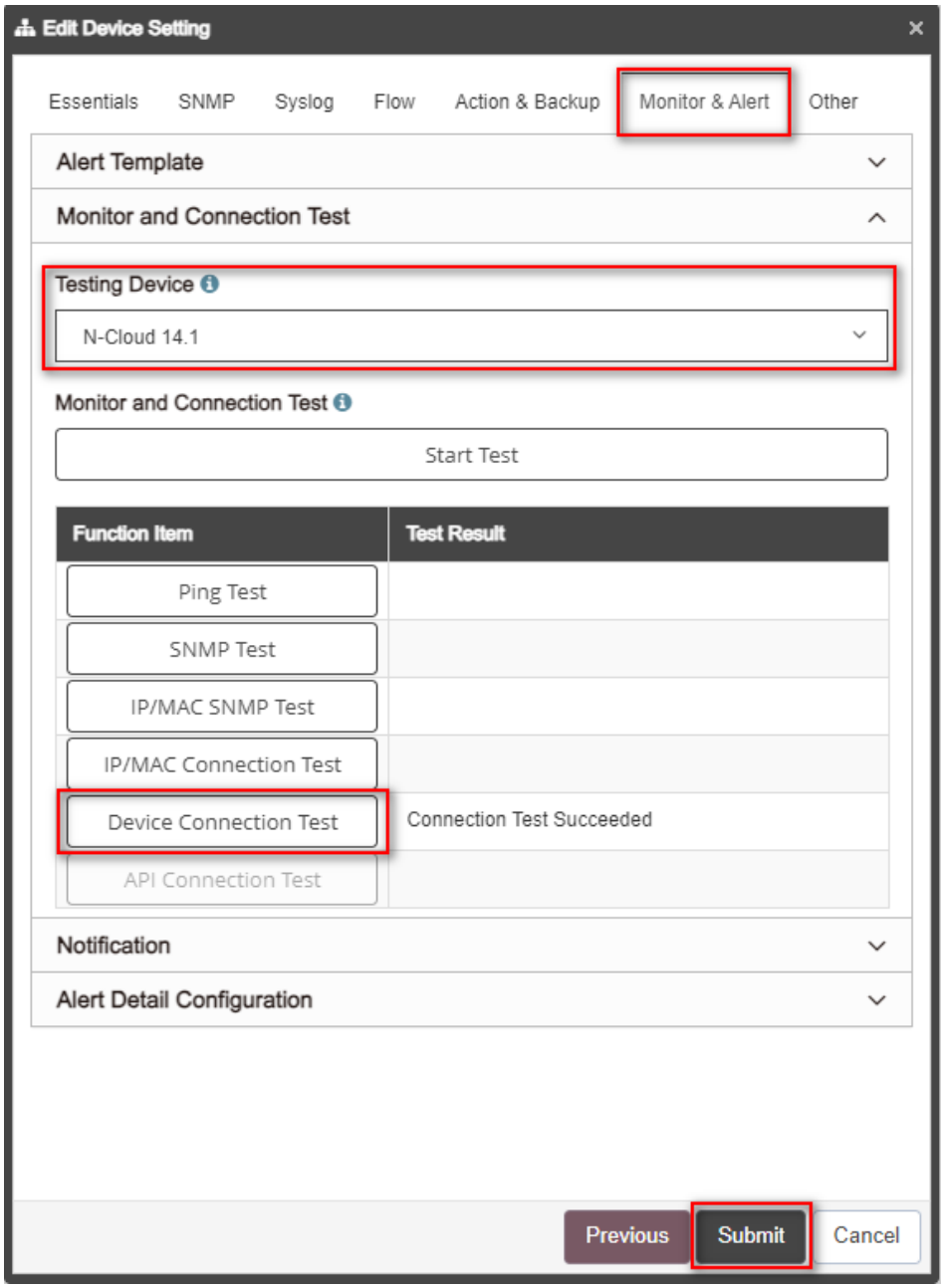


(4) Click “Action & Backup,” tab then enter the WMI Login Account and Password.

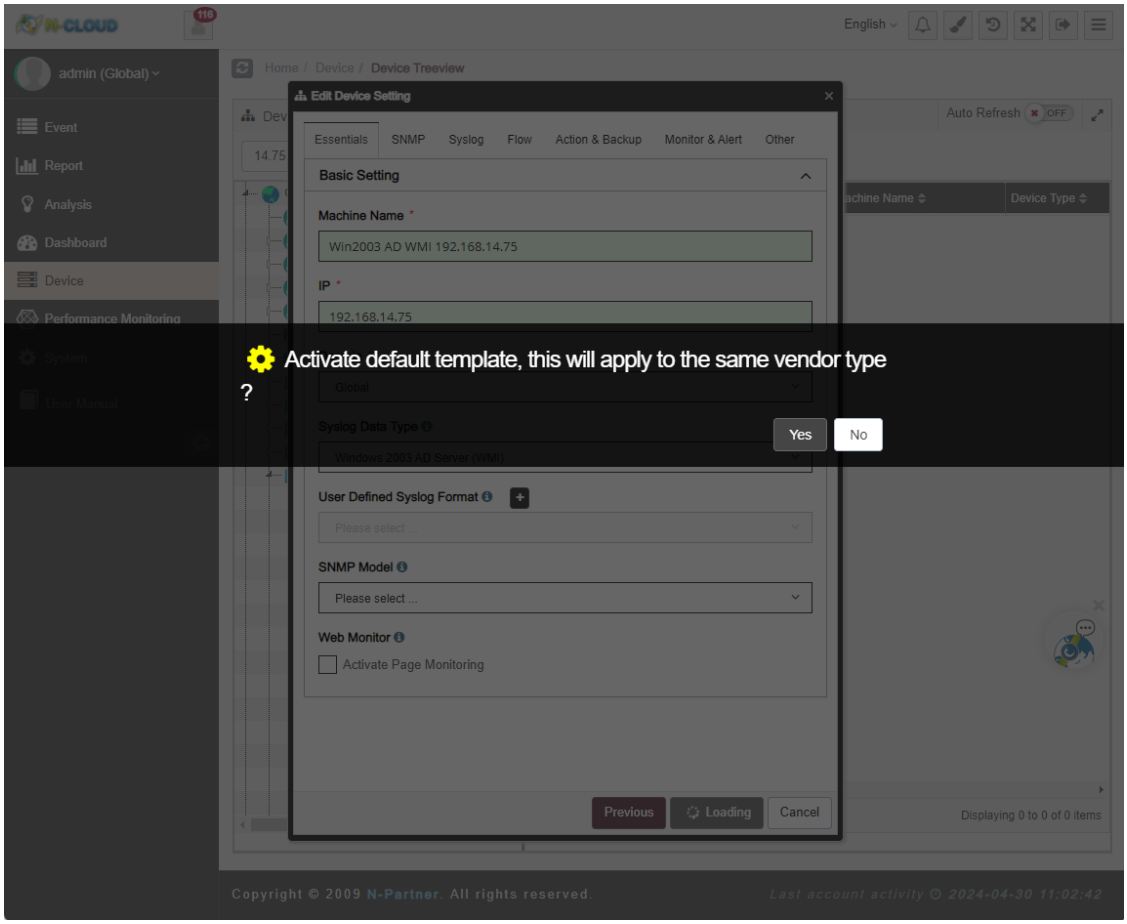


(5) Click “Monitor & Alert” tab. For Testing Device, select the N-Cloud device. Click “Device Connection Test.” If the Test Result shows “Connection Test Succeeded”, the WMI login test is successful. Then click “Submit.”

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.



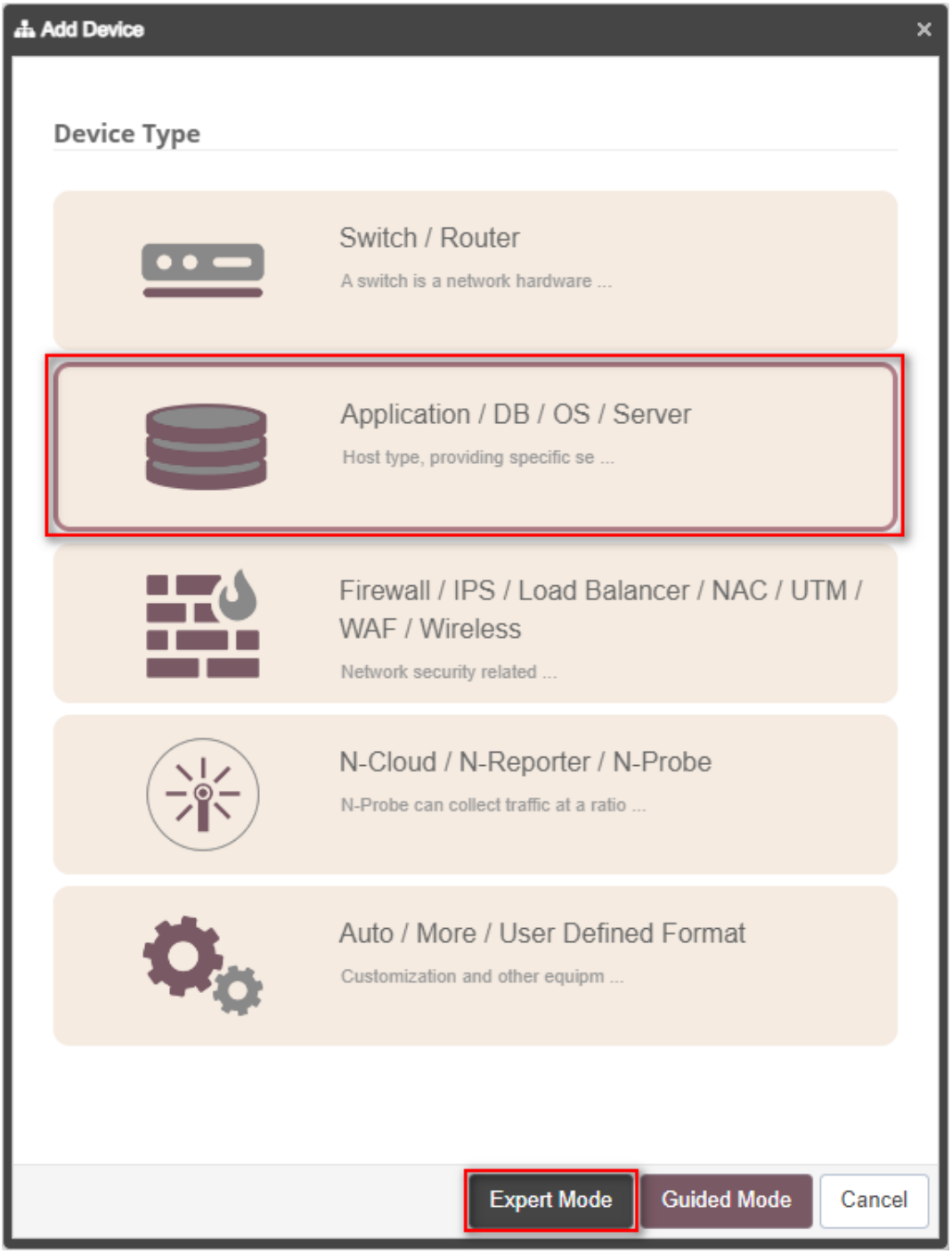
(6) To enable the default reports for the Windows WMI device, click “Yes.” To disable them, click “No.”



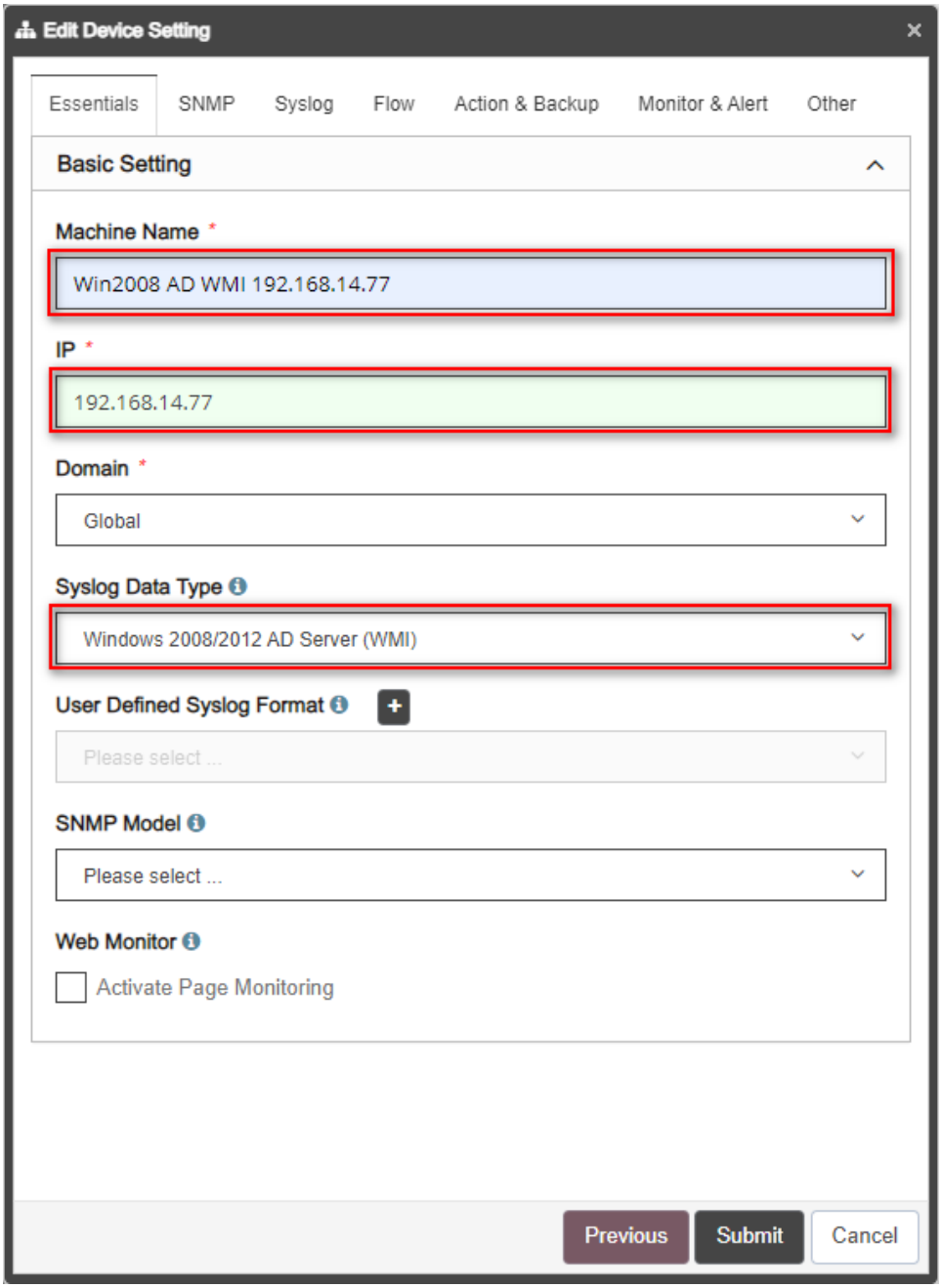
8.2 For Windows 2008 or Later

(1) Configure a Windows AD WMI Device

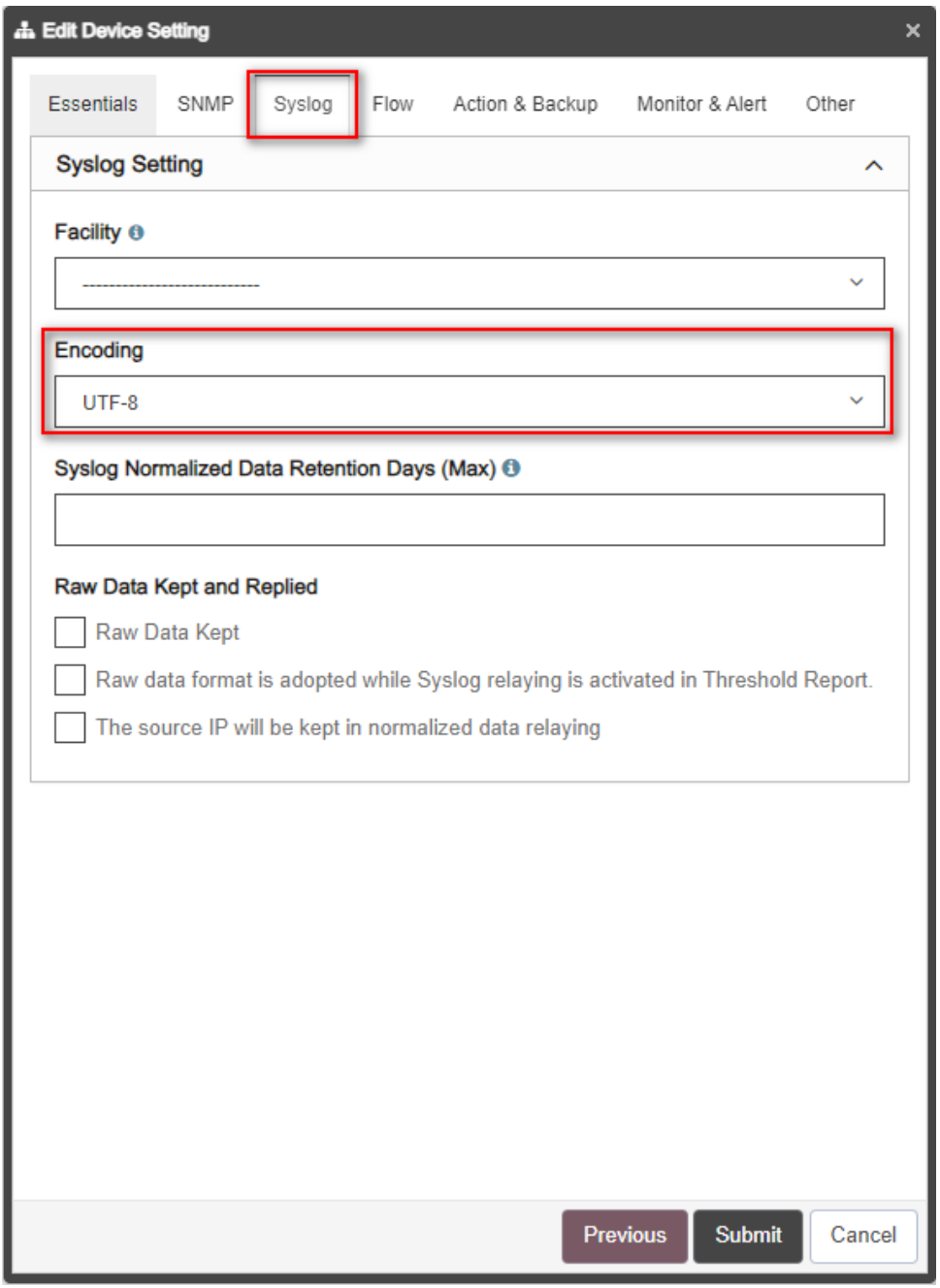
Click “Application / DB / OS / Server,” then select “Expert Mode.”



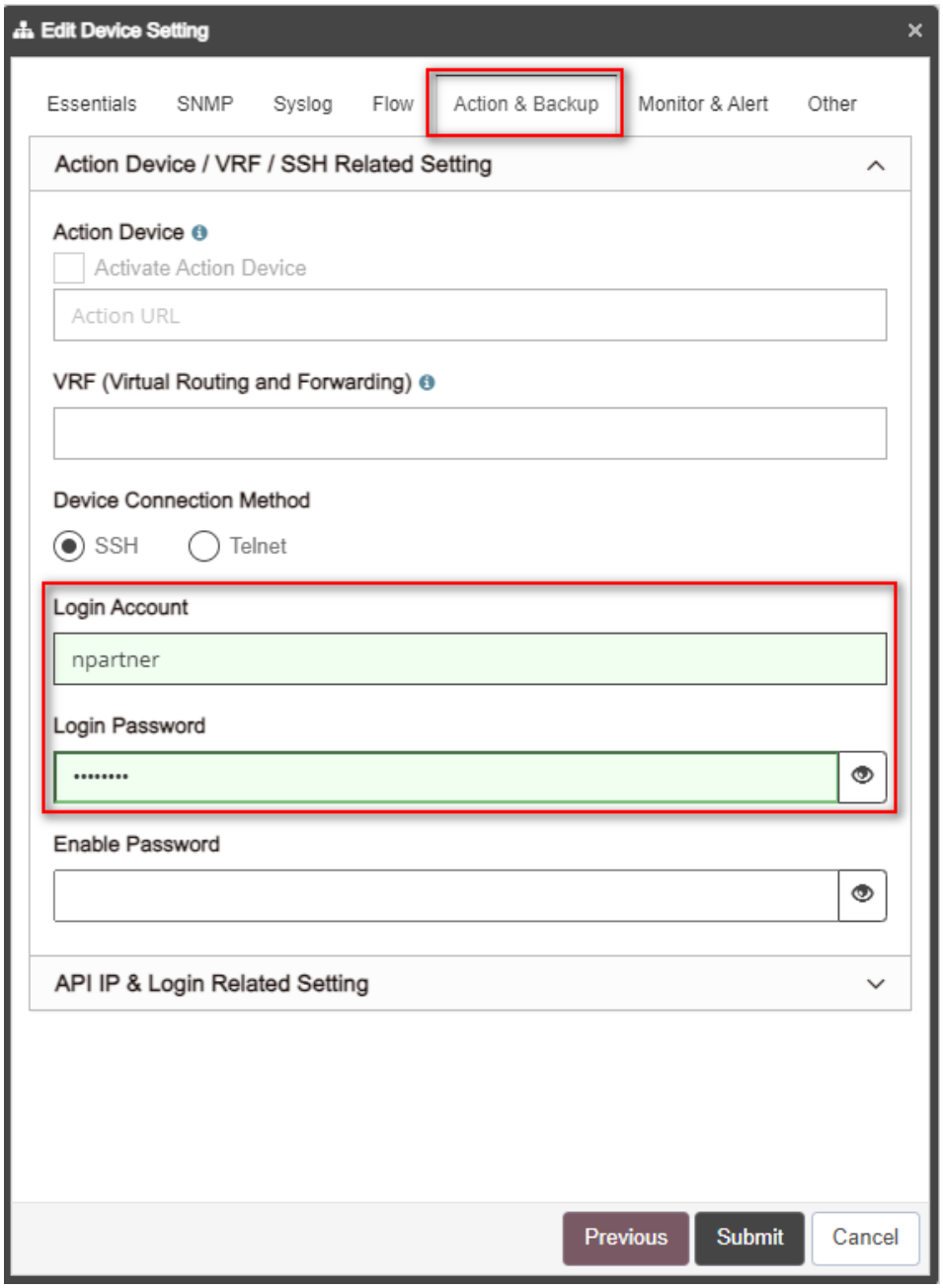
(2) Enter the device name and IP address. For “Syslog Data Type,” select “Windows 2003 AD Server (WMI).”



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

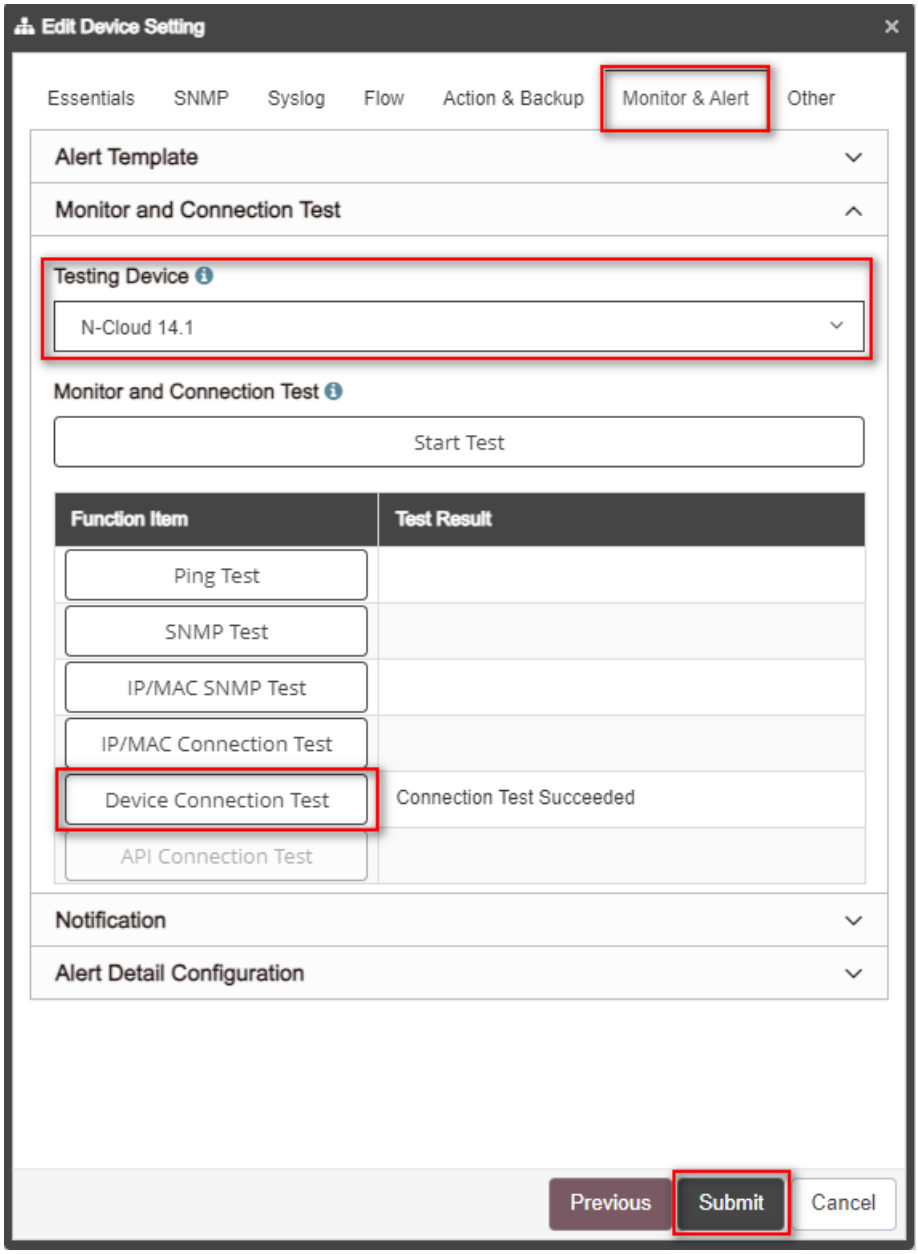


(4) Left click “Action & Backup,” then enter the WMI login account and password.

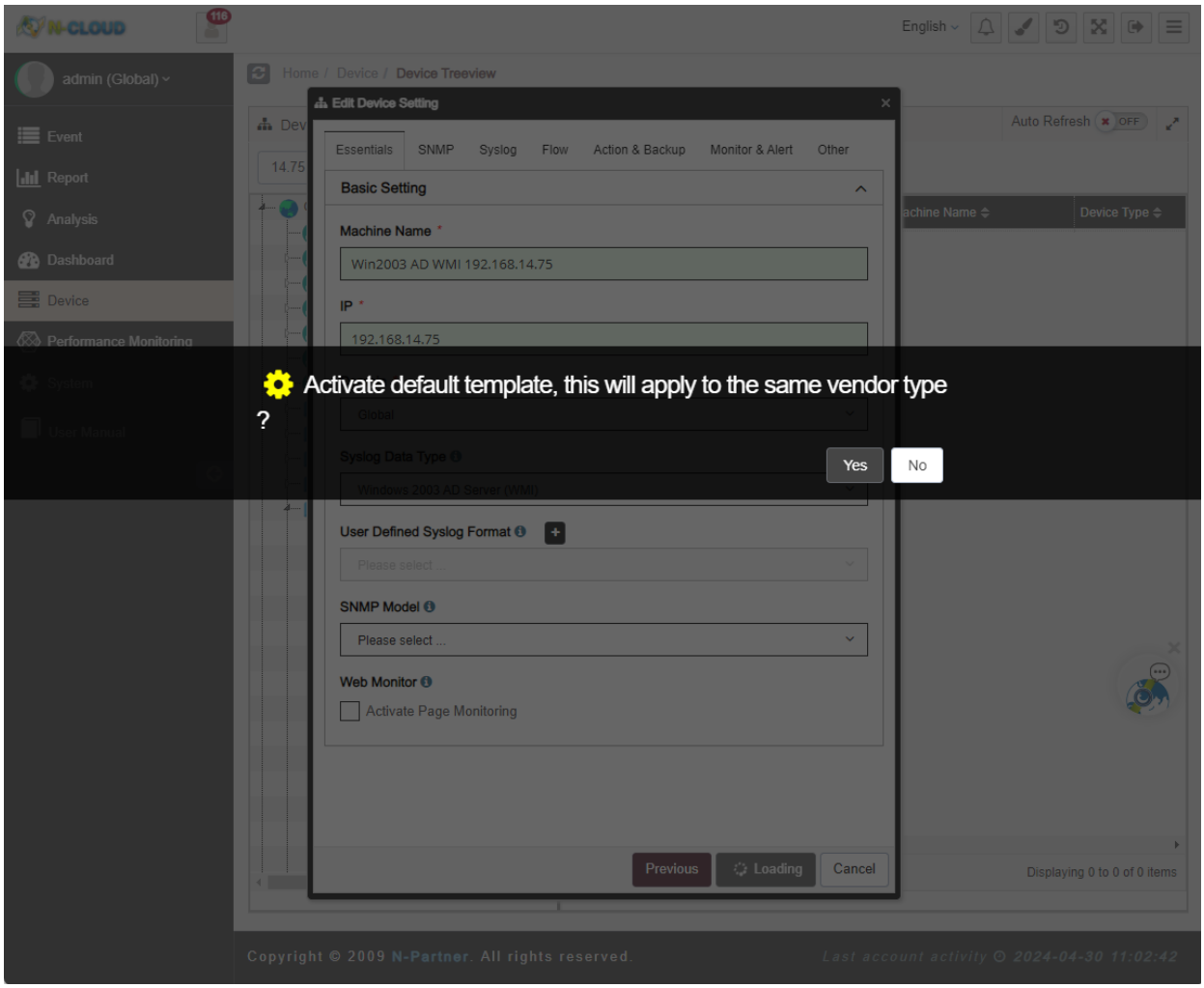


(5) Left-click “Monitor & Alert” and select the N-Cloud device for Testing Device.
Click [Device Connection Test]. If the Test Result shows “Connection Test Succeeded,” the WMI login is successful. Then click [Submit].

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.



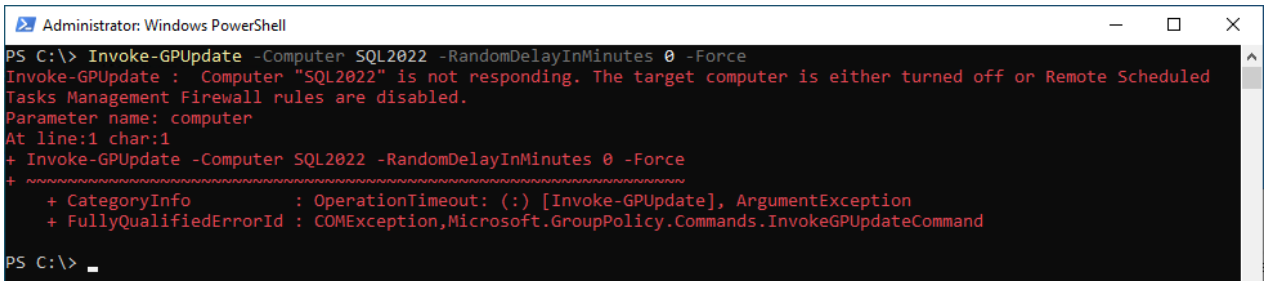
(6) To enable the default reports for Windows WMI devices, click “Yes.” To disable, click “No.”



9. Troubleshooting

9.1 Invoke-GPUpdate Error

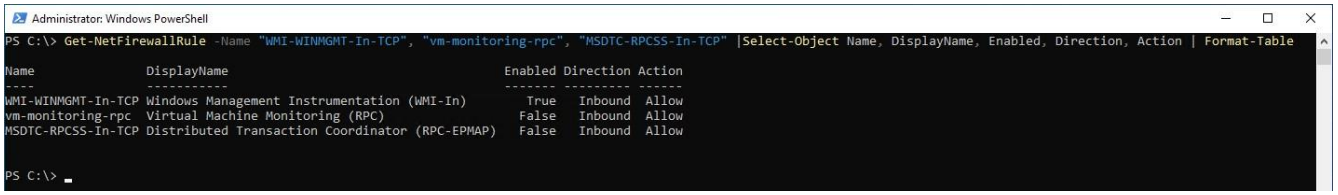
(1) On the AD domain server, an error message appears when running **Invoke-GPUpdate** to update the Windows Server Group Policy.



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

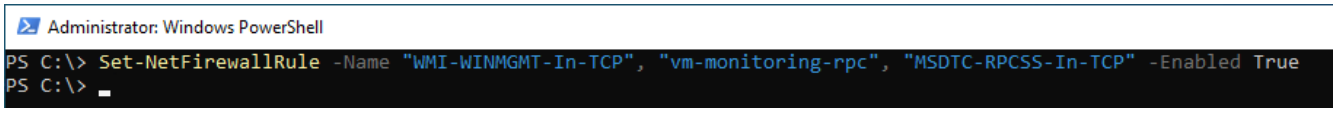
(3) Check the Windows Firewall rules for **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**.

```
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
```



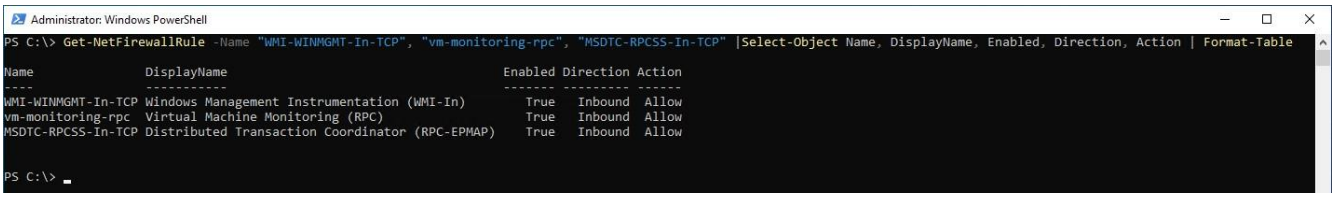
(4) Enable the Windows Firewall rules: WMI-WINMGMT-In-TCP, vm-monitoring-rpc, and MSDTC-RPCSS-In-TCP.

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



(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
```



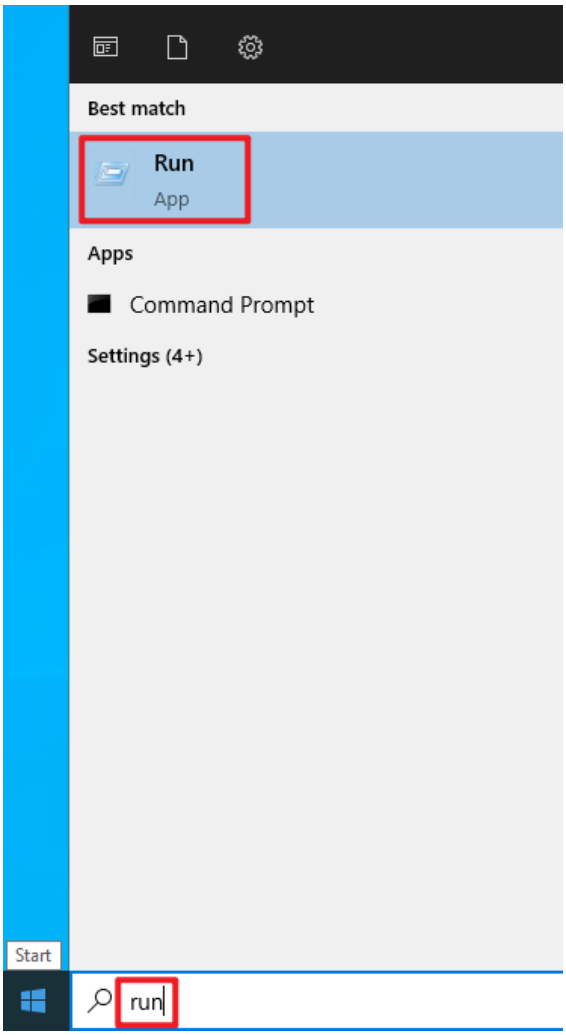
(6) On the AD domain server, update the Windows Server Group Policy.

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

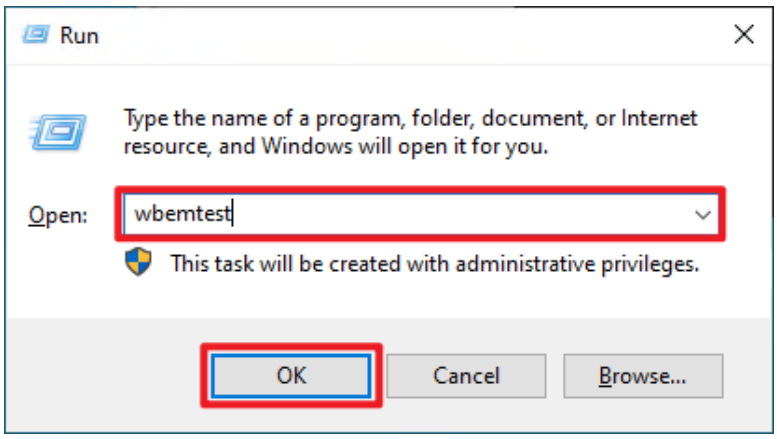
Enter the Windows Server name in the red-highlighted field.

9.2 WMI Query Language Verification

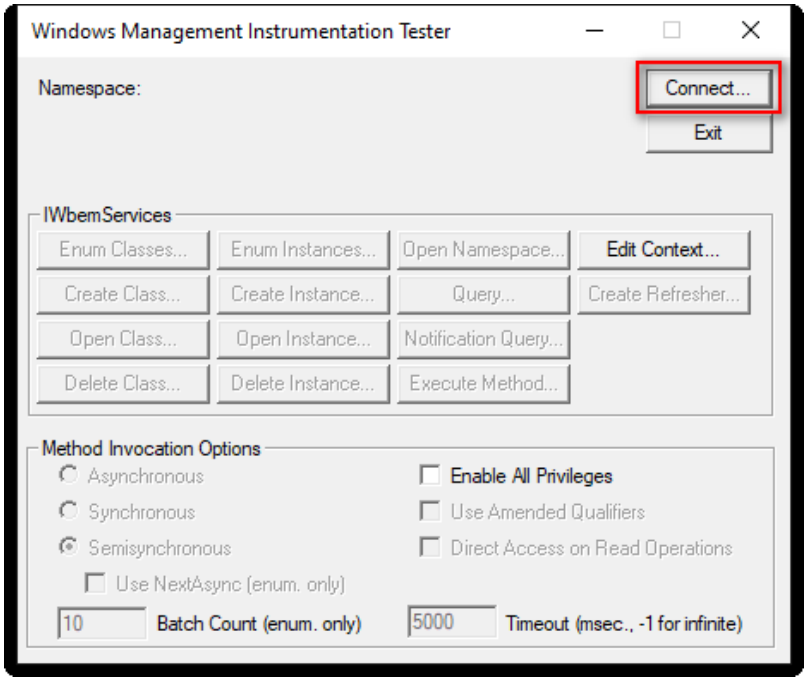
(1) Click “Start” → type “Run” → select “Run.”



(2) Enter “wbemtest” → Click “OK.”



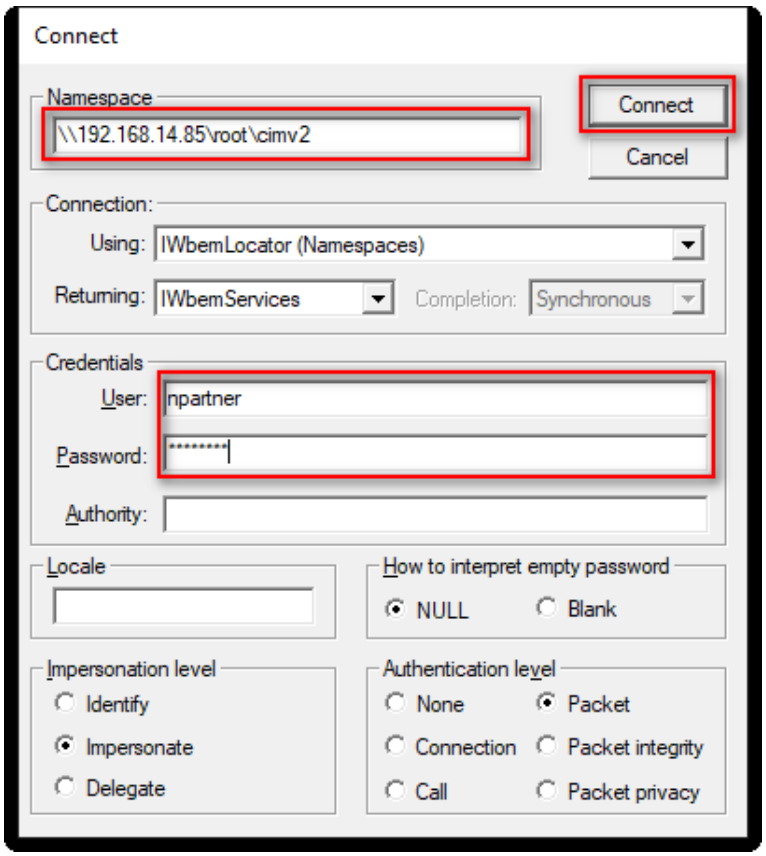
(3) Click “Connect.”



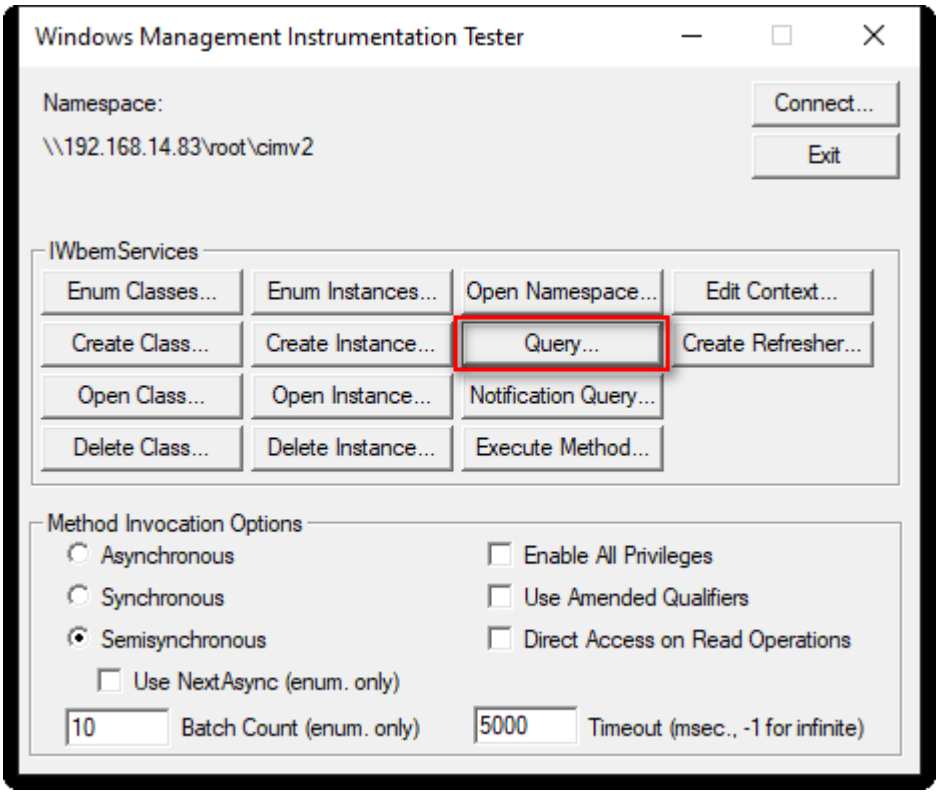
(4) Enter the namespace:

\\<Windows AD IP>\root\cimv2

Enter the username and password → Click “Connect.”



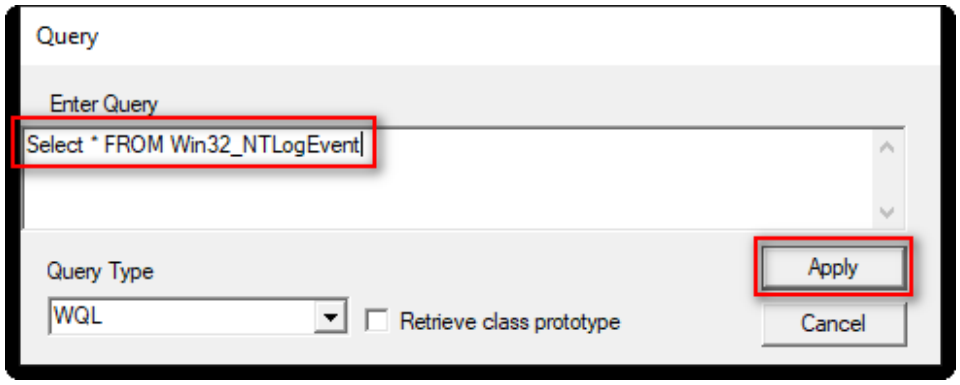
(5) Click “Query.”



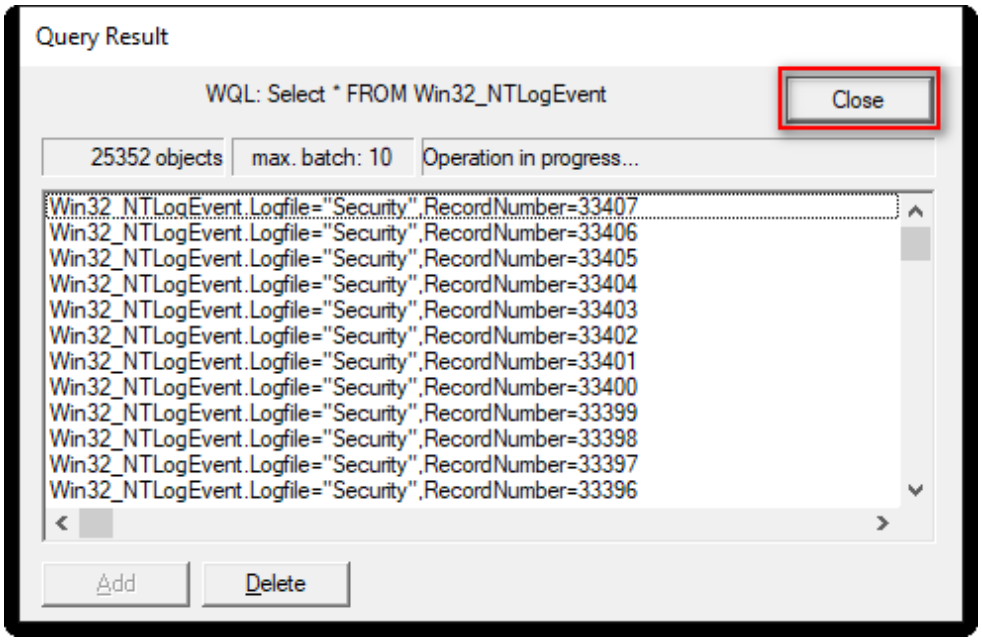
(6) Enter the query:

SELECT * FROM Win32_NTLogEvent

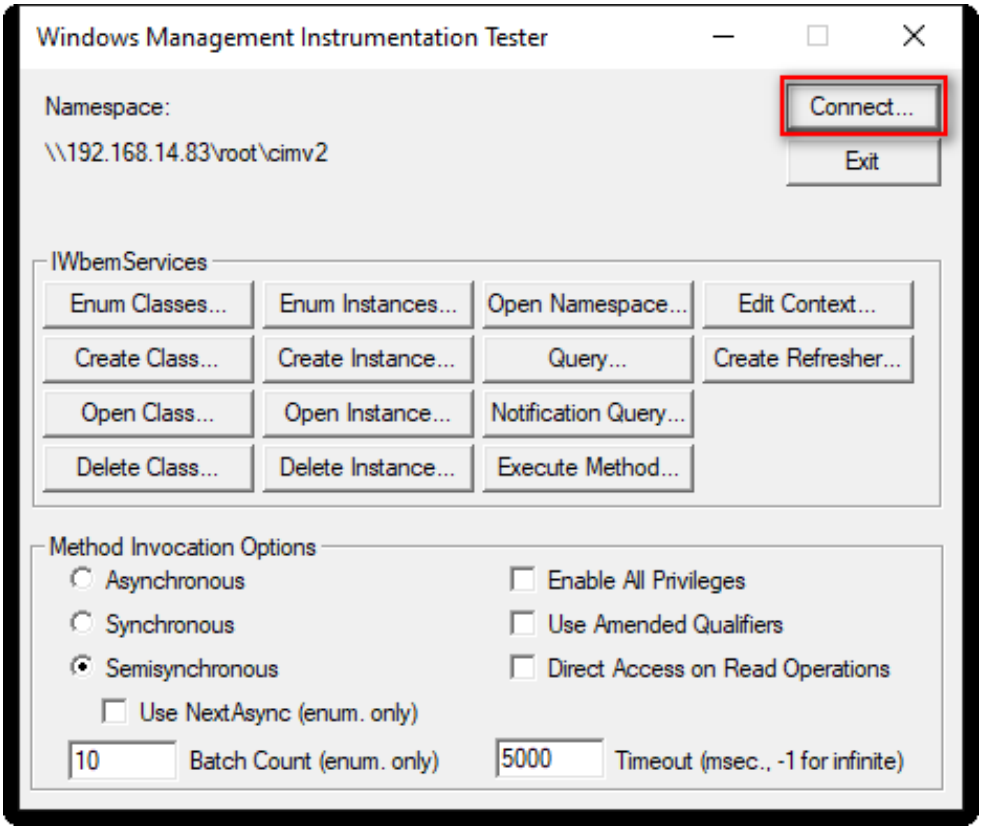
→ Click “Apply.”



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



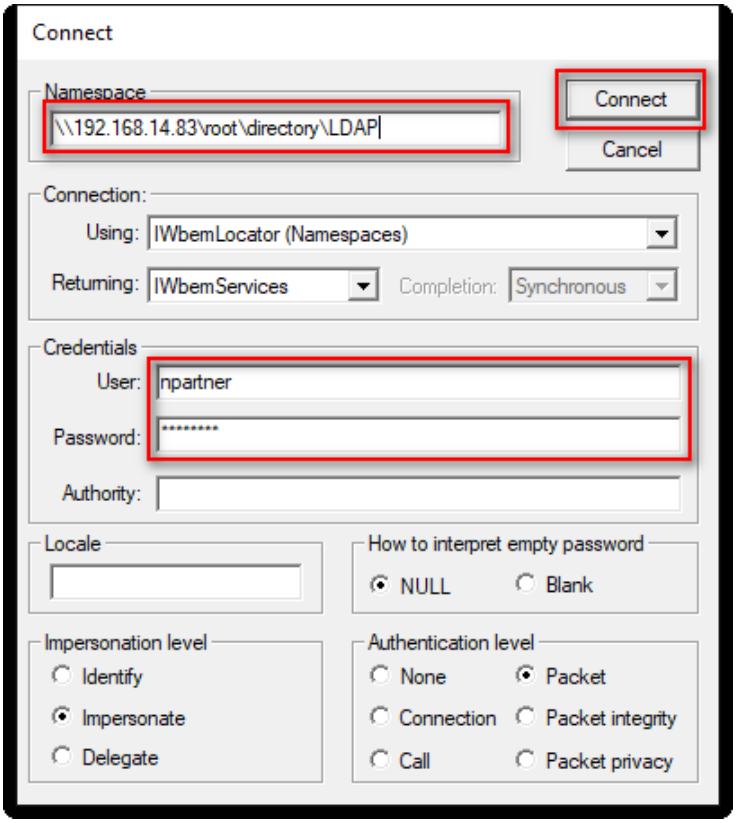
(8) Click “Connect.”



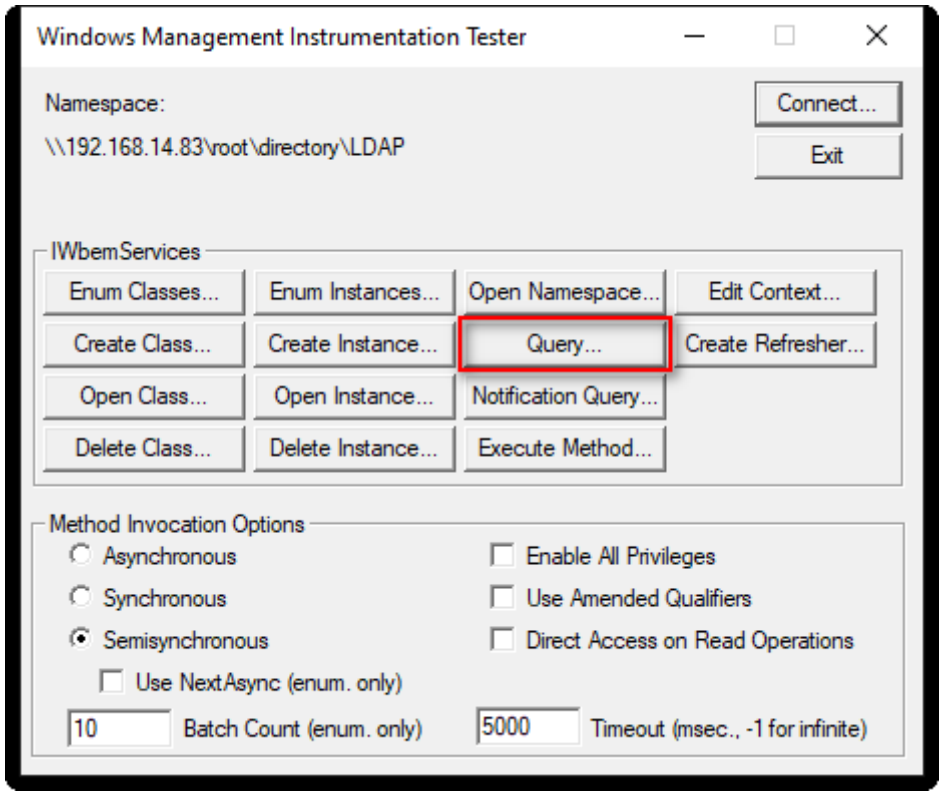
(9) Enter the namespace:

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

Enter the username and password → Click “Connect.”



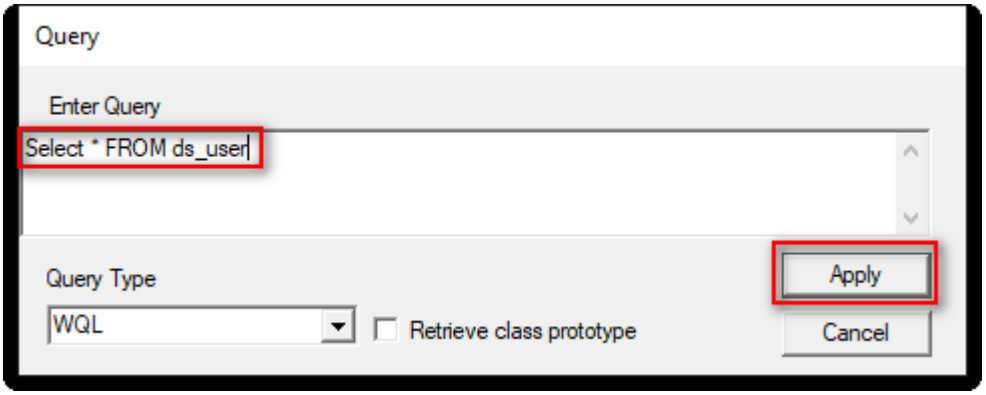
(10) Click “Query.”



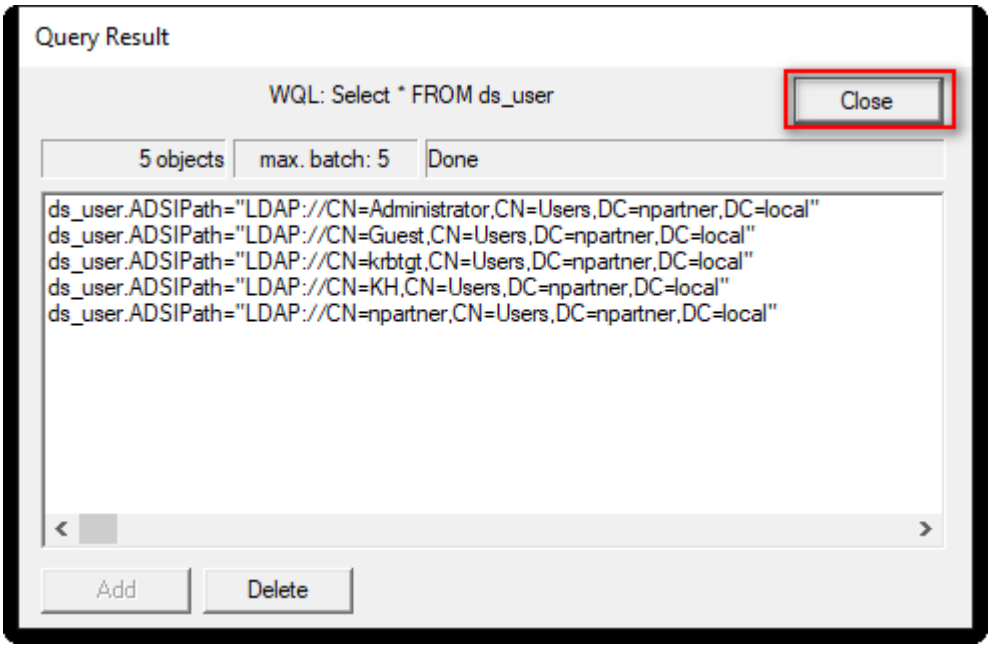
(11) Enter the query:

SELECT * FROM ds_user

→ Click “Apply.”

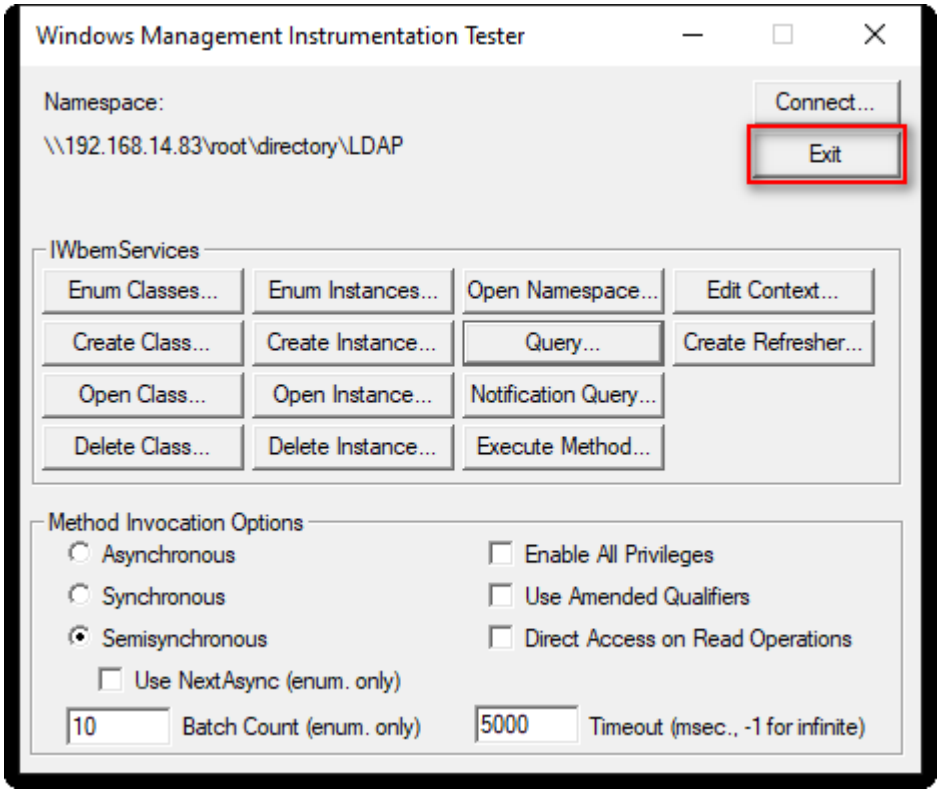


(12) If data is returned, click “Close.”



(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