How to
Configure
Windows AD Event Log

V019

2025/09/03

Copyright Declaration

Registered Trademark

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

Contents

Preface 3
References 3
1. NXLog 4
1.1 NXLog Installation 4
1.2 Download NXLog Configuration File 8
1.2.1 For Windows Server 2003 or earlier 8
1.2.1.1 Export host audit, object access, and account management event logs 8
1.2.1.2 Export All Event Logs 9
1.2.2 For Windows Server 2008 or later 10
1.2.2.1 Export host audit, object access, and account management event logs 10
1.2.2.2 Export All Application, Security, and System Event Logs 11
1.3 NXLog Configuration 12
1.3.1 For Windows Server 2003 or earlier 12
1.3.1.1 Export host audit, object access, and account management event logs (2003Server.conf) 12
1.3.1.2 Export All Event Logs (2003All.conf) 14
1.3.2 For Windows Server 2008 or later 16
1.3.2.1 Export Host Audit, Object Access, and Account Management Event Logs (2008Server.conf) 16
1.3.2.2 Export All Application, Security, and System Event Logs (2008All.conf) 18
1.4 Starting the NXLog Service 20
1.4.1 For Windows Server 2003 or earlier 20
1.4.2 For Windows Server 2008 or later 23
2. Windows Server 2000 26
2.1 Organizational Unit (OU) Configuration 26
2.2 Group Policy Settings 29
2.3 Configure WMI 35
2.3.1 Add Non-Admin Accounts 37
2.3.2 Configure DCOM Permissions 40
2.3.3 Configure WMI Permissions 44
2.3.3.1 Configure Event Log Permissions 44
2.3.3.2 Configure Permissions for Reading User Data 48
2.3.4 Configure Event Log Read Permissions 52
2.3.5 Restart the WMI Service 58
3. Windows Server 2003 59
3.1 Organizational Unit (OU) Configuration 59
3.2 Group Policy Settings 62
3.3 Configure WMI 68
3.3.1 Add Non-Admin Accounts 70
3.3.2 Configure DCOM Permissions 71
3.3.3 Configure WMI Permissions 75
3.3.3.1 Configure Event Log Permissions 75
3.3.3.2 Configure Permissions for Reading User Data 79
3.3.4 Configure Event Log Read Permissions 83
3.3.5 Restart the WMI Service 88
3.3.6 Configure the Firewall 89
4. Windows Server 2008 91
4.1 Organizational Unit (OU) Configuration 91
4.2 Group Policy Settings 94
4.3 Configure WMI 101
4.3.1 Add Non-Admin Accounts 102
4.3.2 Configure DCOM Permissions 103
4.3.3 Configure WMI Permissions 107
4.3.3.1 Configure Event Log Permissions 107
4.3.3.2 Configure Permissions for Reading User Data 111
4.3.4 Configure Event Log Read Permissions 115
4.3.5 Restart the WMI Service 119
4.3.6 Configure the Firewall 120
5. Windows Server 2012 122
5.1 Organizational Unit (OU) Configuration 122
5.2 Group Policy Settings 125
5.3 Configure WMI 132
5.3.1 Add Non-Admin Accounts 133
5.3.2 Configure DCOM Permissions 134
5.3.3 Configure WMI Permissions 138
5.3.3.1 Configure Event Log Permissions 138
5.3.3.2 Configure Permissions for Reading User Data 142
5.3.4 Configure Event Log Read Permissions 146
5.3.5 Restart the WMI Service 150
5.3.6 Configure the Firewall 151
6. Windows Server 2016 152
6.1 Organizational Unit (OU) Configuration 152
6.2 Group Policy Settings 155
6.3 Configure WMI 162
6.3.1 Add Non-Admin Accounts 163
6.3.2 Configure DCOM Permissions 164
6.3.3 Configure WMI Permissions 168
6.3.3.1 Configure Event Log Permissions 168
6.3.3.2 Configure Permissions for Reading User Data 172
6.3.4 Configure Event Log Read Permissions 176
6.3.5 Restart the WMI Service 180
6.3.6 Configure the Firewall 181
7. Windows Server 2019 182
7.1 Organizational Unit (OU) Configuration 182

7.2 Group Policy Settings 185
7.3 Configure WMI 192
7.3.1 Add Non-Admin Accounts 193
7.3.2 Configure DCOM Permissions 194
7.3.3 Configure WMI Permissions 198
7.3.3.1 Configure Event Log Permissions 198
7.3.3.2 Configure Permissions for Reading User Data 202
7.3.4 Configure Event Log Read Permissions 206
7.3.5 Restart the WMI Service 211
7.3.6 Configure the Firewall 212
8. Windows Server 2022 213
8.1 Organizational Unit (OU) Configuration 213
8.2 Group Policy Settings 216
8.3 Configure WMI 223
8.3.1 Add Non-Admin Accounts 224
8.3.2 Configure DCOM Permissions 225
8.3.3 Configure WMI Permissions 229
8.3.3.1 Configure Event Log Permissions 229
8.3.3.2 Configure Permissions for Reading User Data 233
8.3.4 Configure Event Log Read Permissions 237
8.3.5 Restart the WMI Service 242
8.3.6 Configure the Firewall 243
9. N-Reporter 244
9.1 For Windows Server 2003 or earlier 245
9.2 For Windows 2008 or later 249
10. Troubleshooting 253
10.1 WMI Query Language Check 253
10.1.1 Query Event Logs 254
10.1.2 Query User Data 257
10.2 NXLog Installation Issues 260
Contact 261

Preface

This document describes how N-Reporter users can configure Windows AD event logging using the open-source tool NXLog.

NXLog converts Windows AD event logs into syslog format and forwards them to N-Reporter for normalization, auditing, and analysis.

This document applies to Windows Server 2000, 2003, 2008, 2012, 2016, 2019, and 2022.

References

Audit Policy Recommendations:
https://learn.microsoft.com/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Events to Monitor:
https://learn.microsoft.com/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Connect Windows Security Events:
https://docs.microsoft.com/zh-tw/azure/sentinel/connect-windows-security-events

Note: This document is provided solely as a reference for configuring log output. It is recommended that you contact the device or software vendor for assistance with the appropriate log export methods.

1. NXLog

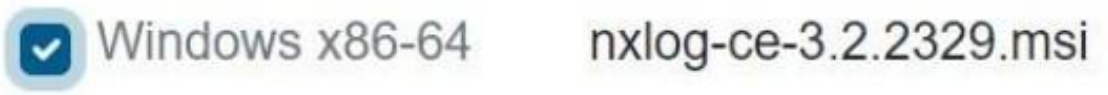
1.1 NXLog Installation

(1) Download NXLog CE (Community Edition)

Please go to: https://nxlog.co/products/nxlog-community-edition/download

Download the latest version of nxlog-ce-x.x.xxxx.msi.

Example Here: **nxlog-ce-3.2.2329.msi**

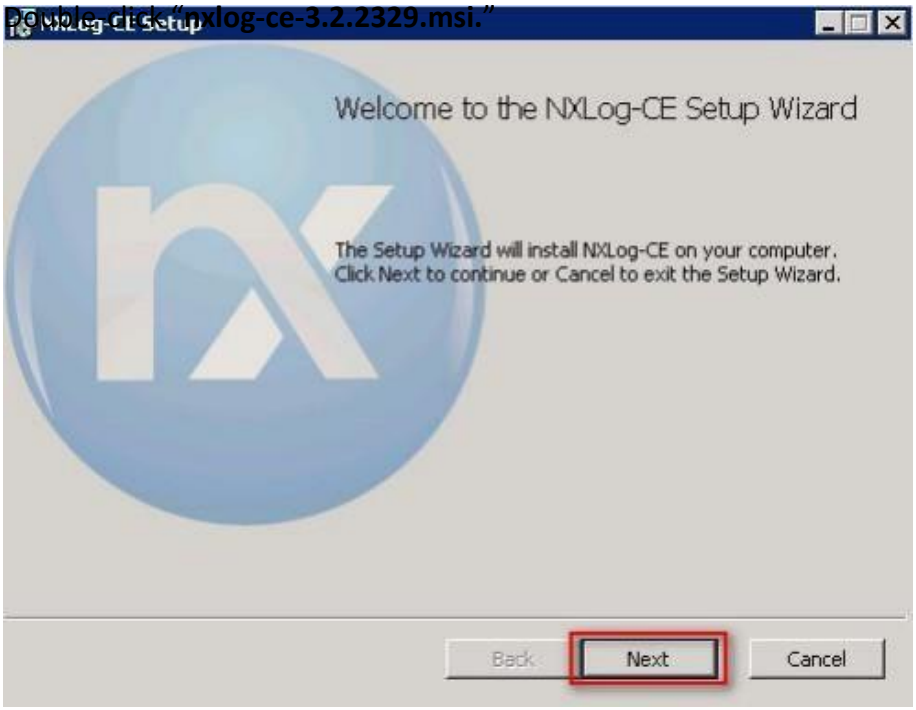


Note: If you require the 32-bit version of NXLog, please contact our support team.

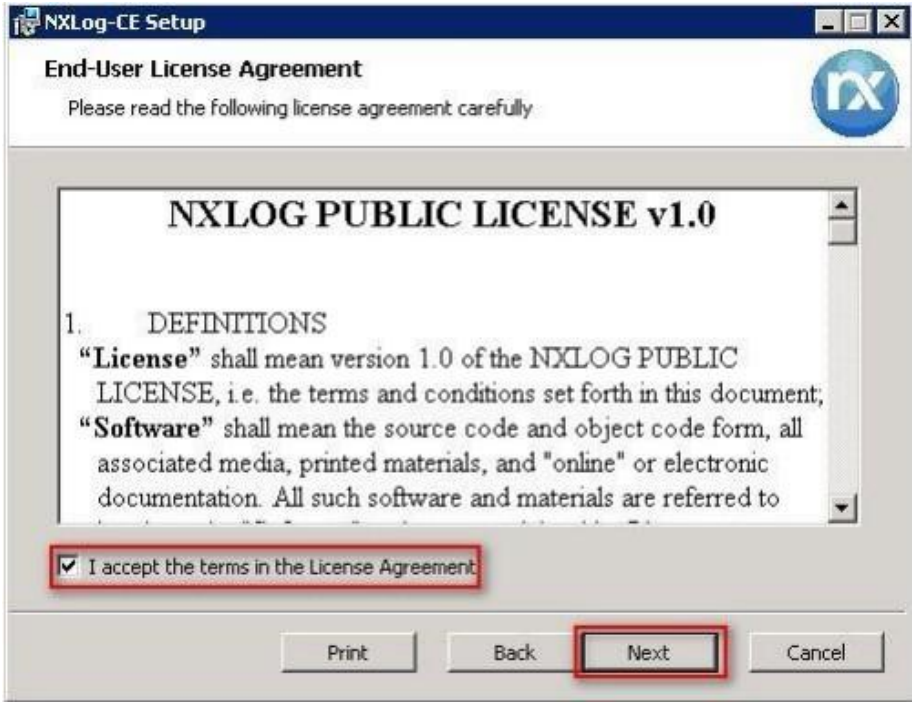
(2) Install NXLog

<2.1> For Windows Server **2008** or later:

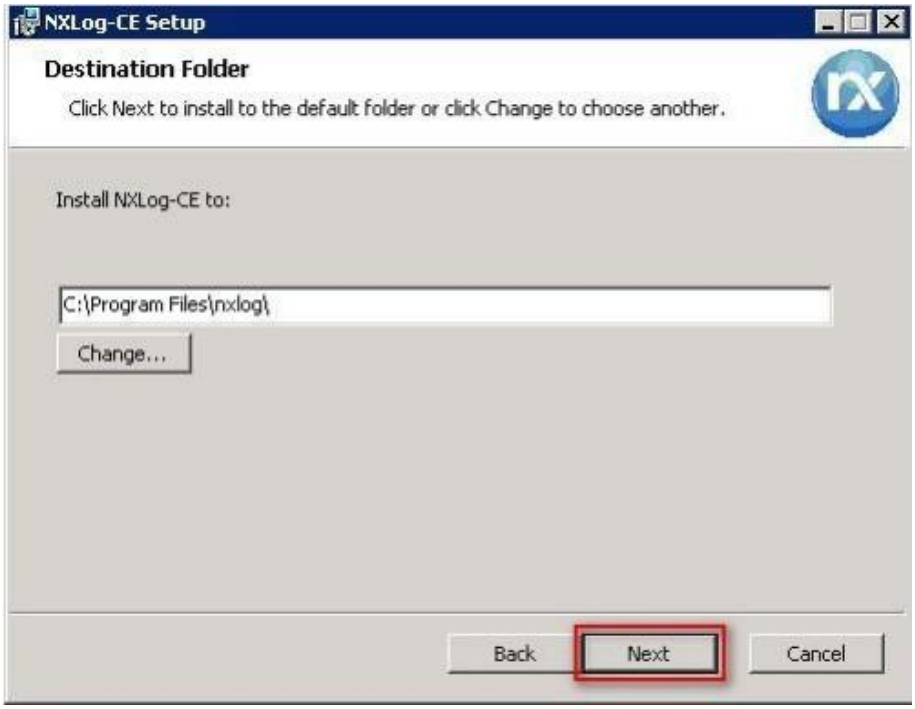
Double-click "**nxlog-ce-3.2.2329.msi.**"



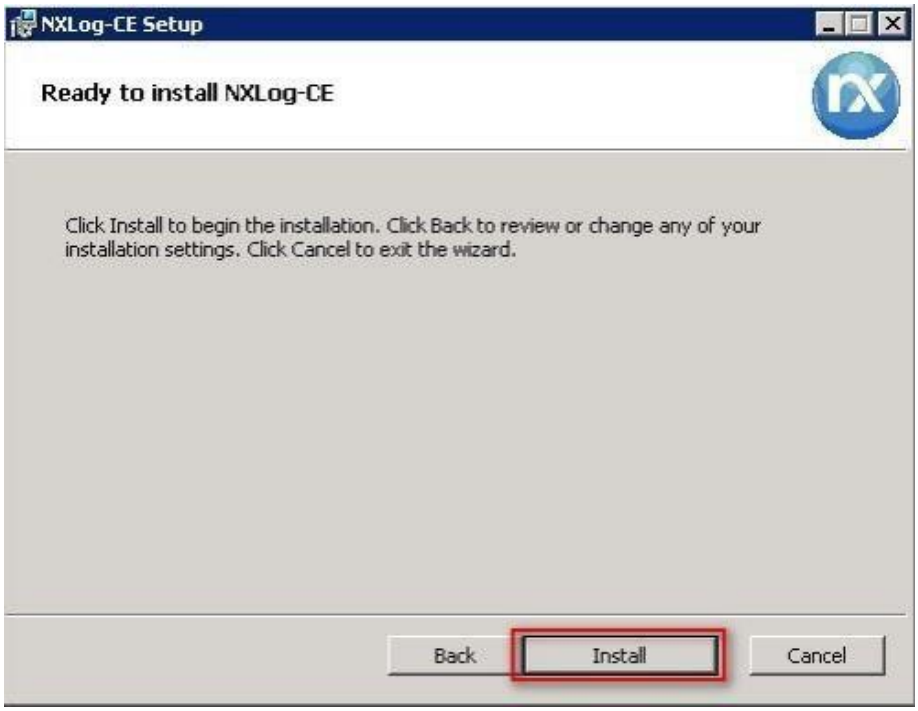
(3) Select “I accept the terms in the License Agreement,” then click “Next.”



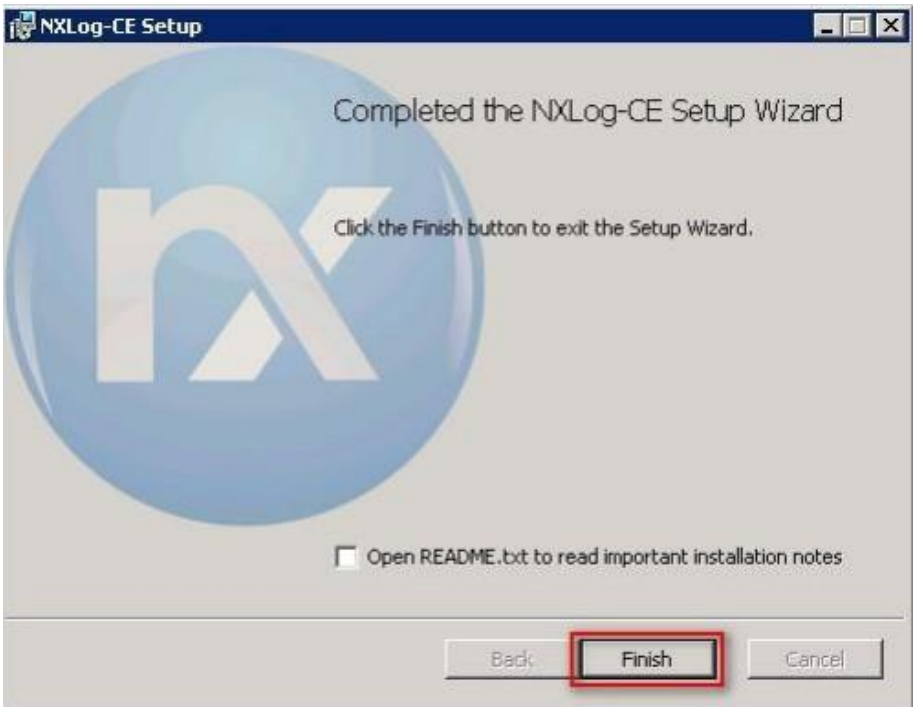
(4) Click “Next.” (The default installation path is (C:\Program Files\nxlog\).



(5) Click “Install.”

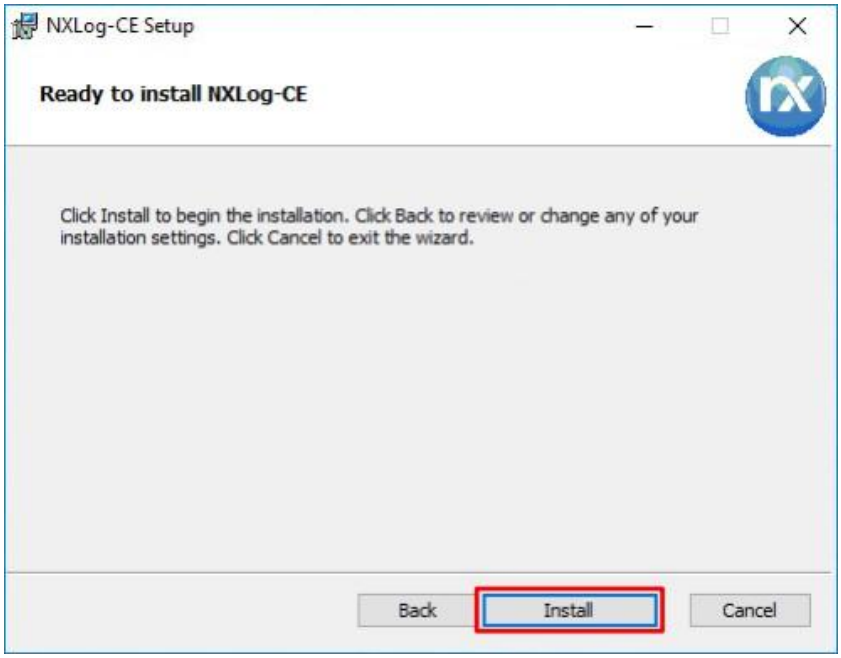


(6) Click “Finish.”



<2.2> For Windows Server **2003**:

Download File: **nxlog-ce-3.2.2329.msi.** → Select “Install” and proceed until the installation completes. → Click “Finish” to exit.

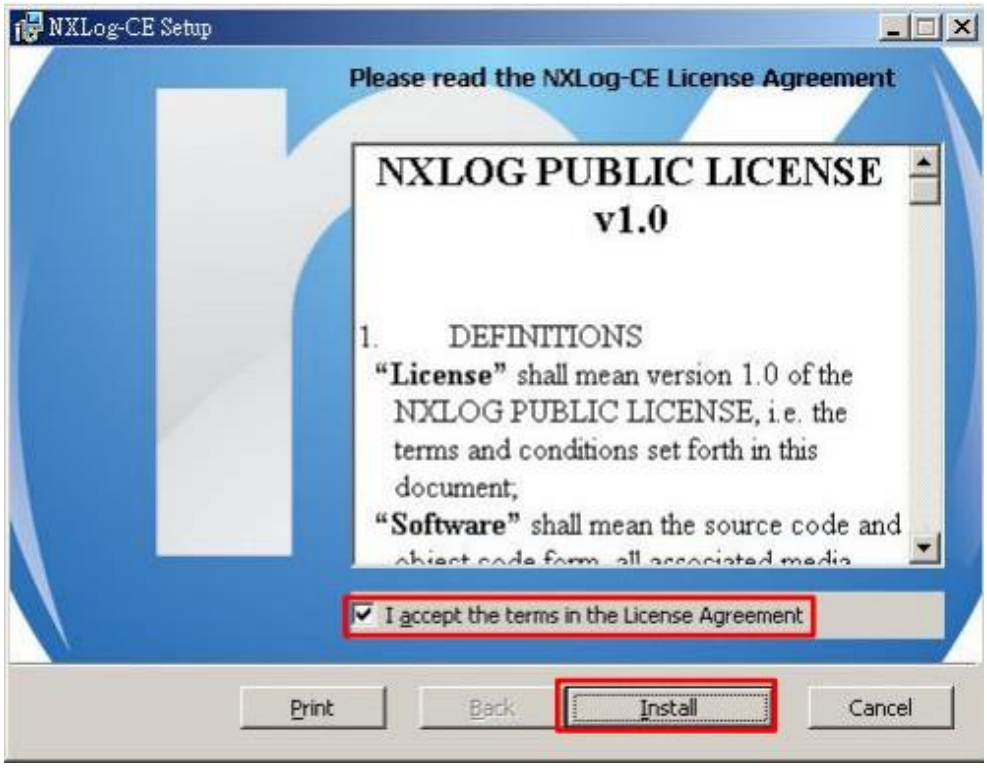


<2.3> For Windows **2000**:

(1) Navigate to the NXLog CE legacy download page: https://sourceforge.net/projects/nxlog-ce/

(2) Click “See All Activity” and download the Windows 2000–compatible version “/**nxlog-ce-2.8.1248.msi**.”

(3) Launch “**nxlog-ce-2.8.1248.msi**,” and accept the license terms, click “**Install**,” and then “**Finish**.”



1.2 Download NXLog Configuration File

1.2.1 For Windows Server 2003 or earlier

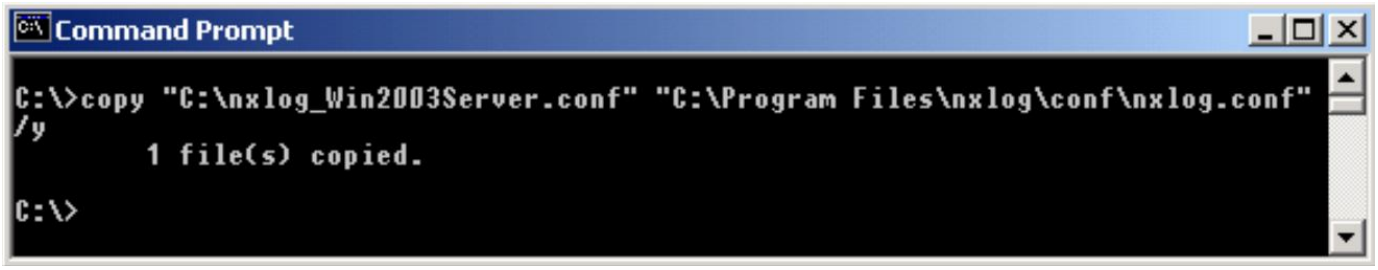
1.2.1.1 Export host audit, object access, and account management event logs

(1) Open “Command Prompt.”

(2) Download the “NXLog Windows 2003 File” and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_Win2003Server.conf

```
C:\> copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf
```



Note: The example above is for a 64-bit operating system. For a 32-bit operating system, replace the highlighted text with: 'C:**\ Program Files (x86)**\nxlog\conf\nxlog.conf'

The recommended default setting outputs only host audit, object access, and account management events, minimizing performance impact on the Windows Server host.

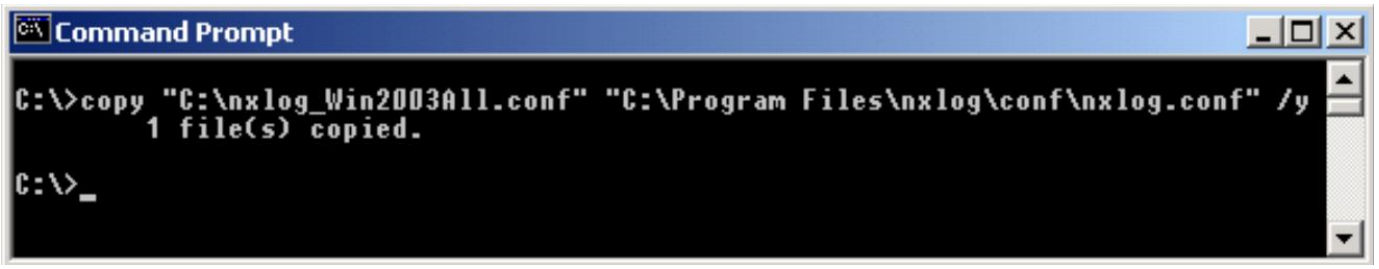
1.2.1.2 Export All Event Logs

(1) Open “Command Prompt.”

(2) Download the “NXLog Windows 2003 File” and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_Win2003All.conf

```
C:\> copy "C:\nxlog_Win2003All.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



Note: The example above is for a 64-bit operating system. For a 32-bit operating system, replace the highlighted text with: 'C:**\ Program Files (x86)**\nxlog\conf\nxlog.conf'

This configuration file exports all Windows event logs.

1.2.2 For Windows Server 2008 or later

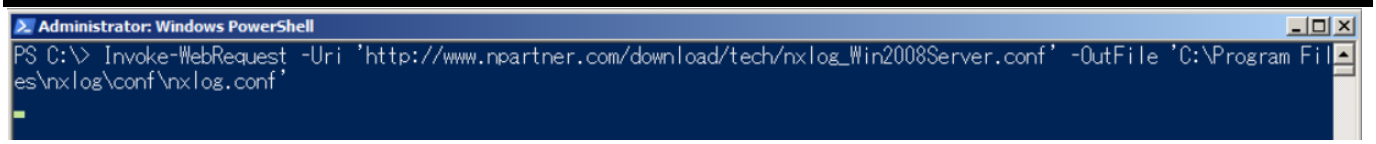
1.2.2.1 Export host audit, object access, and account management event logs

(1) Open “Windows PowerShell.”

(2) Download the “NXLog Windows 2008 File” and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_Win2008Server.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Win2008Server.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf
```



Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:**\ Program Files(x86)**\nxlog\conf\nxlog.conf'

The recommended default setting outputs only host audit, object access, and account management events, minimizing performance impact on the Windows Server host.

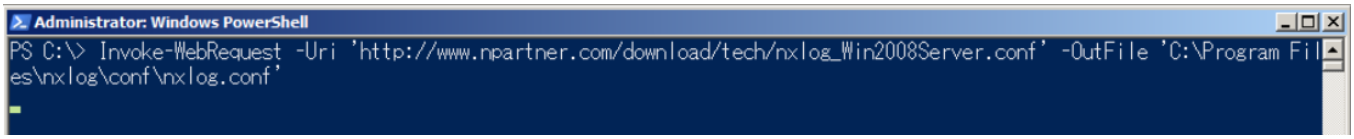
1.2.2.2 Export All Application, Security, and System Event Logs

(1) Open “Command Prompt.”

(2) Download the “NXLog Windows 2008 File” and overwrite the existing NXLog configuration file in the Windows system.

Download link: http://www.npartner.com/download/tech/nxlog_Win2008All.conf

```
C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Win2008All.conf' -OutFile 'C:\Program Files\nxlog\conf\nxlog.conf'
```



Note: The example above is for a 64-bit operating system. For a 32-bit operating system, replace the highlighted text with: 'C:**\ Program Files (x86)**\nxlog\conf\nxlog.conf'

This configuration file exports all Windows Application, Security, and System event logs.

1.3 NXLog Configuration

1.3.1 For Windows Server 2003 or earlier

1.3.1.1 Export host audit, object access, and account management event logs (2003Server.conf)

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.1.184
define ROOT        C:\Program Files\nxlog
define CERTDIR     %ROOT%\cert
define CONFDIR     %ROOT%\conf
define LOGDIR      %ROOT%\data
define LOGFILE     %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir      %ROOT%\data
Pidfile             %ROOT%\data\nxlog.pid
SpoolDir       %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
    Module       xm_syslog
</Extension>

## Windows Server 2000 - 2003 Event Log use the following:
<Input in_eventlog>
    Module                  im_mseventlog
    ReadFromLast TRUE
    SavePos                 TRUE
    Exec    parse_syslog_bsd(); \
        if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID == 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID == 628 or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635 or $EventID == 636 or $EventID
```

```
== 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 644 or $EventID == 645 or
$EventID == 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
        else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
        else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
        else\
        {\
           drop();\
        }
    </Input>

    <Output out_eventlog>
       Module    om_udp
       Host            %NCloud%
       Port             514
       Exec $Message = string($EventID) + ": " + $Message;
       Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
             else if ($EventType == 'WARNING')    { $SyslogSeverityValue = 4; } \
             else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')    { $SyslogSeverityValue = 5; }
       Exec to_syslog_bsd();
    </Output>

    <Route eventlog>
       Path       in_eventlog => out_eventlog
    </Route>
```

Enter the N-Cloud system IP address in the blue text section.

```
define NCloud 192.168.8.184
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

```
define ROOT C:\Program Files (x86)\nxlog
```

1.3.1.2 Export All Event Logs (2003All.conf)

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud          192.168.8.184
define ROOT            C:\Program Files\nxlog
define CERTDIR     %ROOT%\cert
define CONFDIR     %ROOT%\conf
define LOGDIR      %ROOT%\data
define LOGFILE     %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir      %ROOT%\data
Pidfile             %ROOT%\data\nxlog.pid
SpoolDir       %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
    Module       xm_syslog
</Extension>

## Windows Server 2000 - 2003 Event Log use the following:
<Input in_eventlog>
    Module            im_mseventlog
    ReadFromLast TRUE
    SavePos          TRUE
    Exec parse_syslog_bsd();
</Input>

<Output out_eventlog>
    Module om_udp
    Host          %NCloud%
    Port           514
    Exec $Message = string($EventID) + ": " + $Message;
    Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
            else if ($EventType == 'WARNING')    { $SyslogSeverityValue = 4; } \
```

```
        else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')    { $SyslogSeverityValue = 5; }
    Exec to_syslog_bsd();
</Output>

<Route eventlog>
    Path    in_eventlog => out_eventlog
</Route>
```

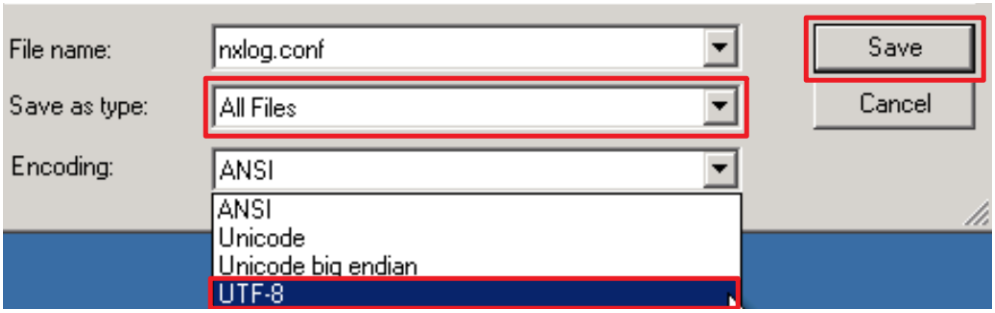
Enter the N-Cloud system IP address in the blue text section.

```
define NCloud 192.168.8.184
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

```
define ROOT C:\Program Files (x86)\nxlog
```



Note: After modifying the configuration file, save it as a new file to overwrite the original. For Save as type, select “All Files (*.*)”. For Encoding, select UTF-8 to avoid encoding errors that could prevent the service from starting.

1.3.2 For Windows Server 2008 or later

1.3.2.1 Export Host Audit, Object Access, and Account Management Event Logs (2008Server.conf)

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.3.50
define ROOT        C:\Program Files\nxlog
define CERTDIR     %ROOT%\cert
define CONFDIR     %ROOT%\conf
define LOGDIR      %ROOT%\data
define LOGFILE     %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir    %ROOT%\data
Pidfile     %ROOT%\data\nxlog.pid
SpoolDir    %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
    Module    xm_syslog
</Extension>

## define Security Events
define SecurityEvents 1100, 1102, 4768, 4769, 4771, 4616, 4657, 4624, \
4625, 4634, 4647, 4648, 5140, 5142, 5143, 5144, \
5145, 5168, 4656, 4658, 4660, 4663, 4664, 4688, \
4985, 5051, 4670, 4719, 4739, 4720, 4722, 4723, \
4724, 4725, 4726, 4738, 4740, 4767, 4727, 4728, \
4729, 4730, 4731, 4732, 4733, 4734, 4735, 4737, \
4764, 4741, 4742, 4743, 4744, 4745, 4748, 4749, \
4750, 4753, 4754, 4755, 4756, 4758, 4759, 4760, \
4763, 4778, 4783, 4800, 4801
## define Other Events
define OtherEvents 7036
```

```
## Windows Server 2008 or higher Event Log use the following:
<Input in_eventlog>
    Module          im_msvistalog
    ReadFromLast TRUE
    SavePos         TRUE
    Query           <QueryList> \
        <Query Id="0"> \
            <Select Path="Security">*</Select> \
            <Select Path="System">*</Select> \
        </Query> \
    </QueryList>
    Exec if ($EventID NOT IN (%SecurityEvents%)) and \
                ($EventID NOT IN (%OtherEvents%)) drop();
</Input>

<Output out_eventlog>
    Module om_udp
    Host     %NCloud%
    Port     514
    Exec $SyslogFacilityValue = 17;
    Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
    Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
            else if ($EventType == 'WARNING')    { $SyslogSeverityValue = 4; } \
            else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')    { $SyslogSeverityValue = 5; }
    Exec to_syslog_bsd();
</Output>

<Route eventlog>
    Path    in_eventlog => out_eventlog
</Route>
```

Enter the N-Cloud system IP address in the blue text section.

```
define NCloud 192.168.3.50
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

```
define ROOT C:\Program Files (x86)\nxlog
```

1.3.2.2 Export All Application, Security, and System Event Logs (2008All.conf)

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud      192.168.8.184
define ROOT        C:\Program Files\nxlog
define CERTDIR     %ROOT%\cert
define CONFDIR     %ROOT%\conf
define LOGDIR      %ROOT%\data
define LOGFILE     %LOGDIR%\nxlog.log
LogFile %LOGFILE%

Moduledir %ROOT%\modules
CacheDir      %ROOT%\data
Pidfile             %ROOT%\data\nxlog.pid
SpoolDir       %ROOT%\data

## Load the modules needed by the outputs
<Extension syslog>
   Module       xm_syslog
</Extension>

## Windows Server 2008 or higher Event Log use the following:
<Input in_eventlog>
   Module           im_msvistalog
   ReadFromLast TRUE
   SavePos          TRUE
   Query <QueryList>\
                <Query Id="0">\
                    <Select Path="Application">*</Select>\
                    <Select Path="Security">*</Select>\
                    <Select Path="System">*</Select>\
                </Query>\
            </QueryList>
</Input>

<Output out_eventlog>
```

```
    Module om_udp
    Host      %NCloud%
    Port      514
    Exec $SyslogFacilityValue = 17;
    Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
    Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
            else if ($EventType == 'WARNING')    { $SyslogSeverityValue = 4; } \
            else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')    { $SyslogSeverityValue = 5; }
    Exec to_syslog_bsd();
</Output>

<Route eventlog>
    Path    in_eventlog => out_eventlog
</Route>
```

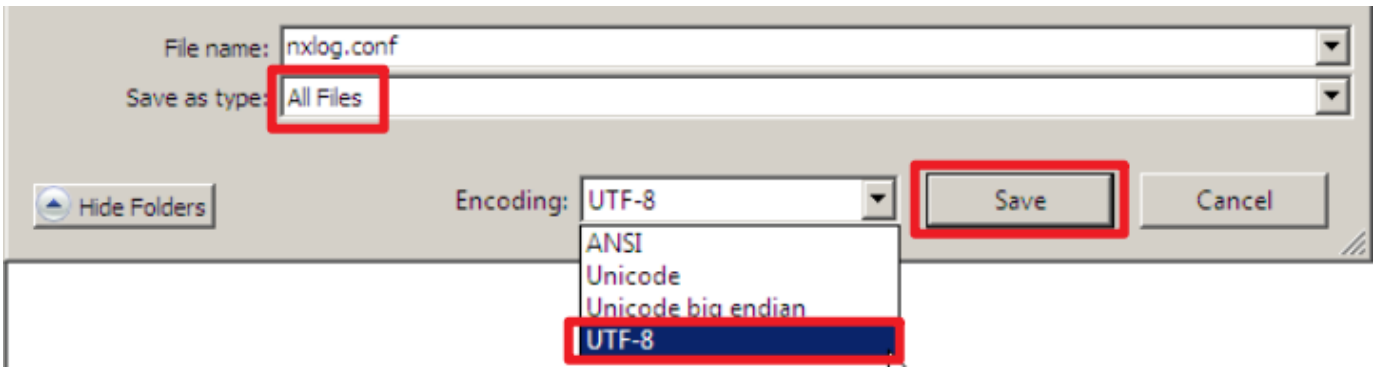
Enter the N-Cloud system IP address in the blue text section.

```
define NCloud 192.168.8.184
```

This example is based on a 64-bit operating system.

For a 32-bit operating system, use the following setting instead:

```
define ROOT C:\Program Files (x86)\nxlog
```



Note: After modifying the configuration file, save it as a new file to overwrite the original. For Save as type, select “All Files (*.*)”. For Encoding, select UTF-8 to avoid encoding errors that could prevent the service from starting.

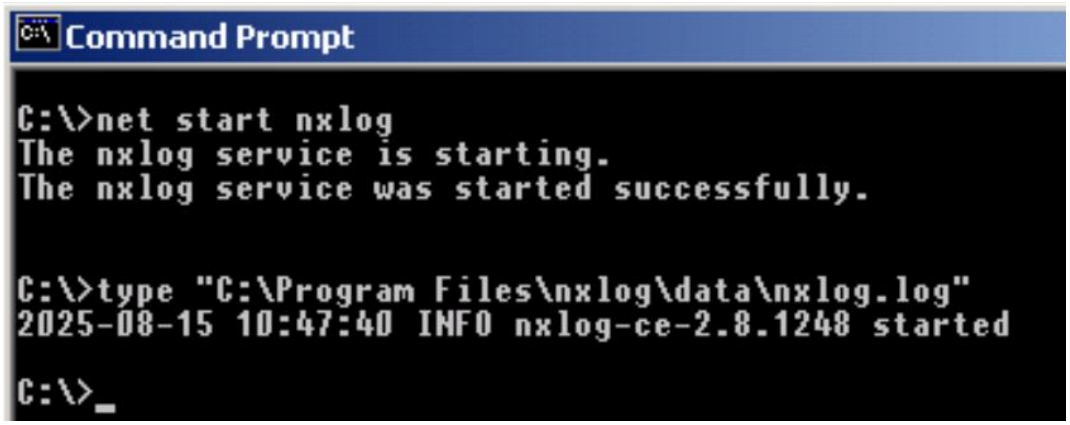
1.4 Starting the NXLog Service

1.4.1 For Windows Server 2003 or earlier

(1) Open “Command Prompt.”

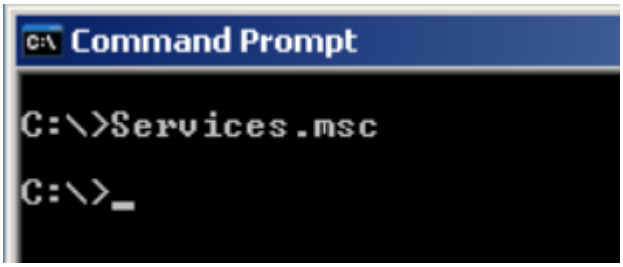
(2) Start the NXLog service and verify that there are no error messages:

```
C:\> net start nxlog
C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```

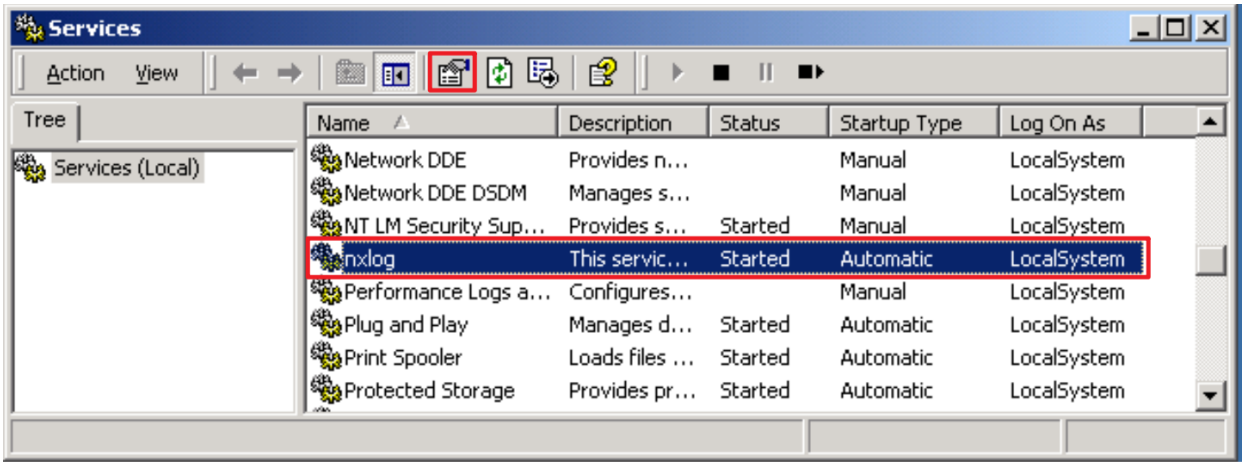


(3) Enter the command below to open the **Services** console:

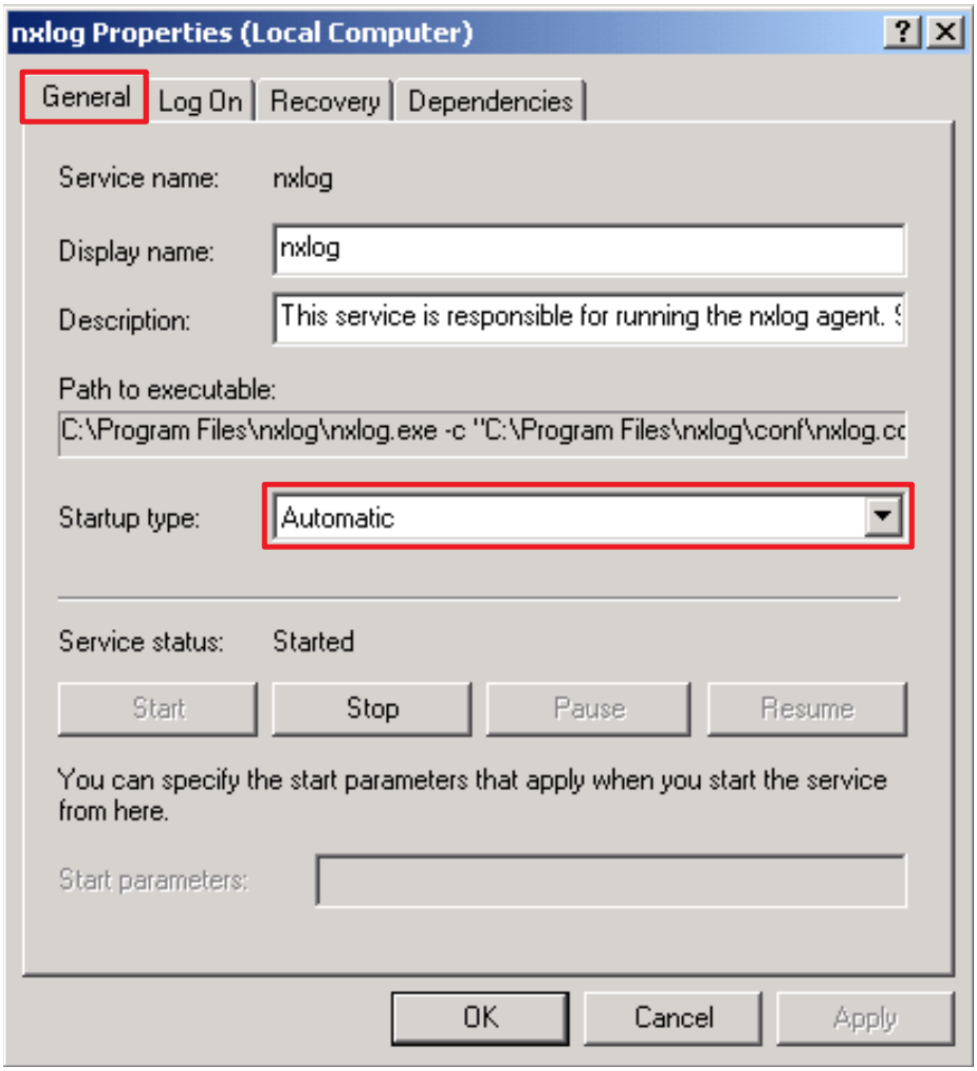
```
C:\> Services.msc
```



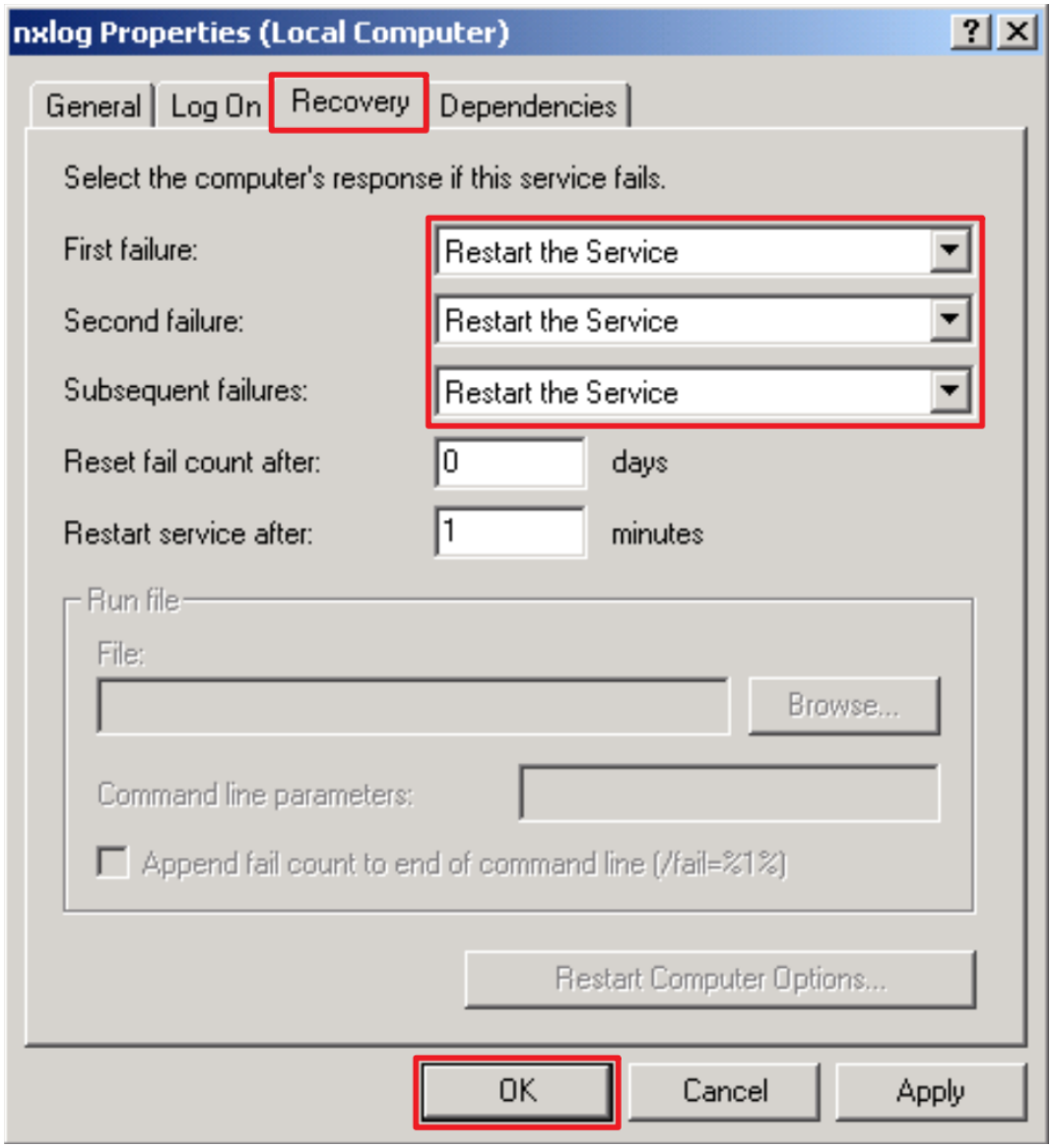
(4) Open the NXLog service properties: select “NXLog” → Click “Properties.”



(5) On the General tab, verify that Startup type is set to Automatic (Delayed Start).



(6) On the Recovery tab, verify that First failure, Second failure, and Subsequent failures are all set to "Restart the Service", then click "OK."

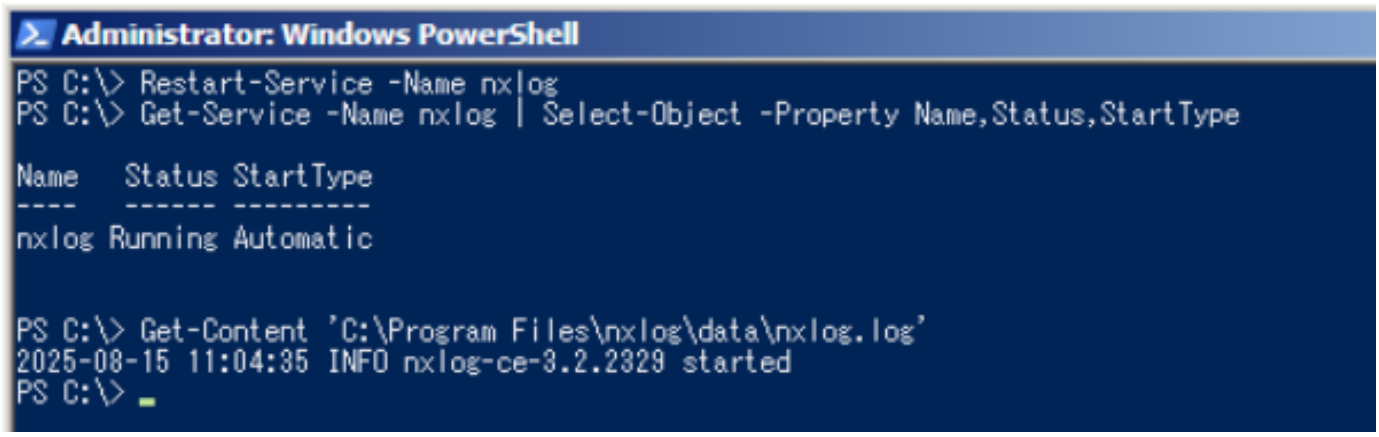


1.4.2 For Windows Server 2008 or later

(1) Open “Windows Powershell.”

(2) Restart the NXLog service, verify that it is running, and ensure there are no error messages:

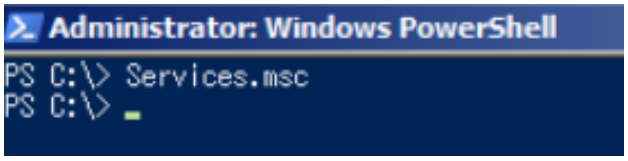
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\ Program Files\ nxlog\data\nxlog.log'
```



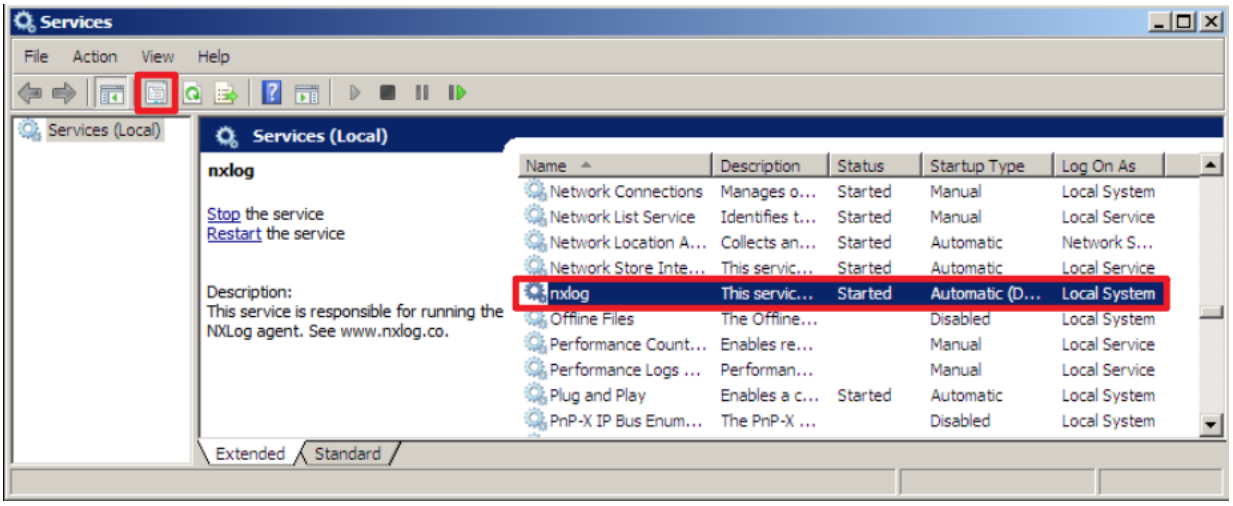
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:**\Program Files(x86)**\nxlog\conf\nxlog.conf'

(3) Enter the command below to open the **Services** console:

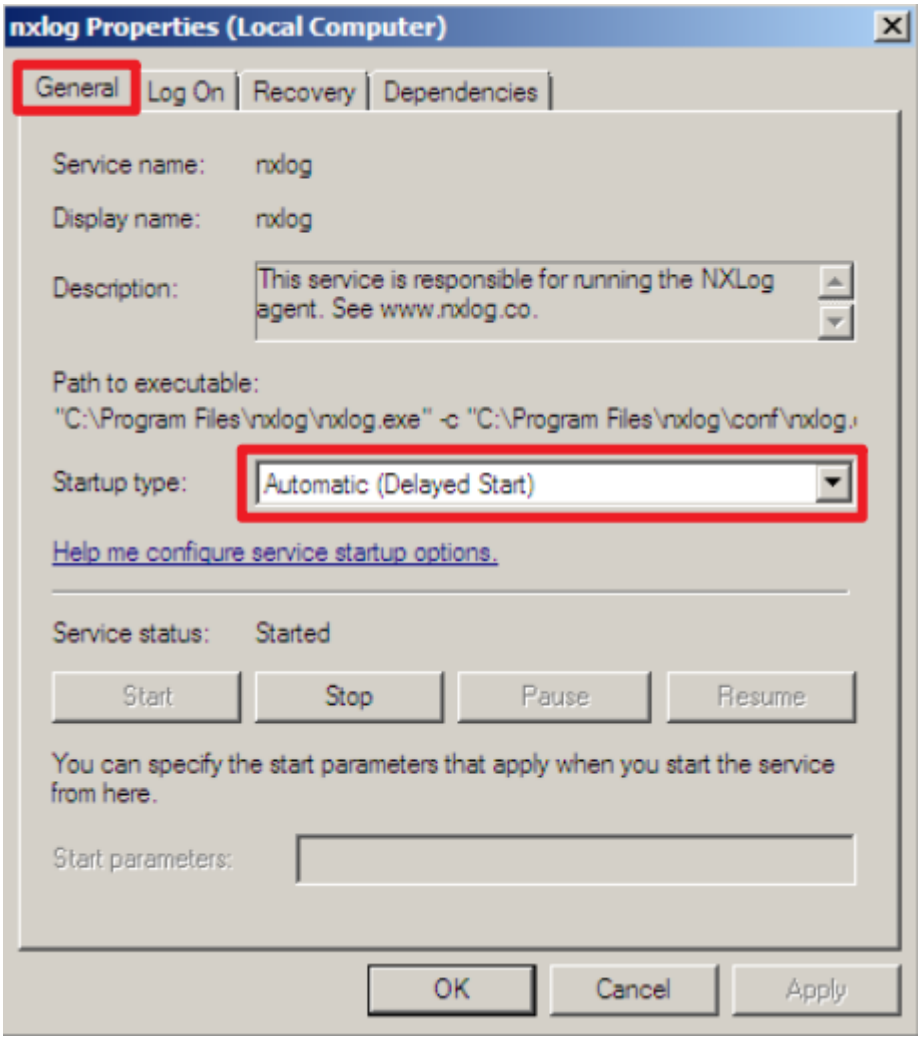
```
PS C:\> Services.msc
```



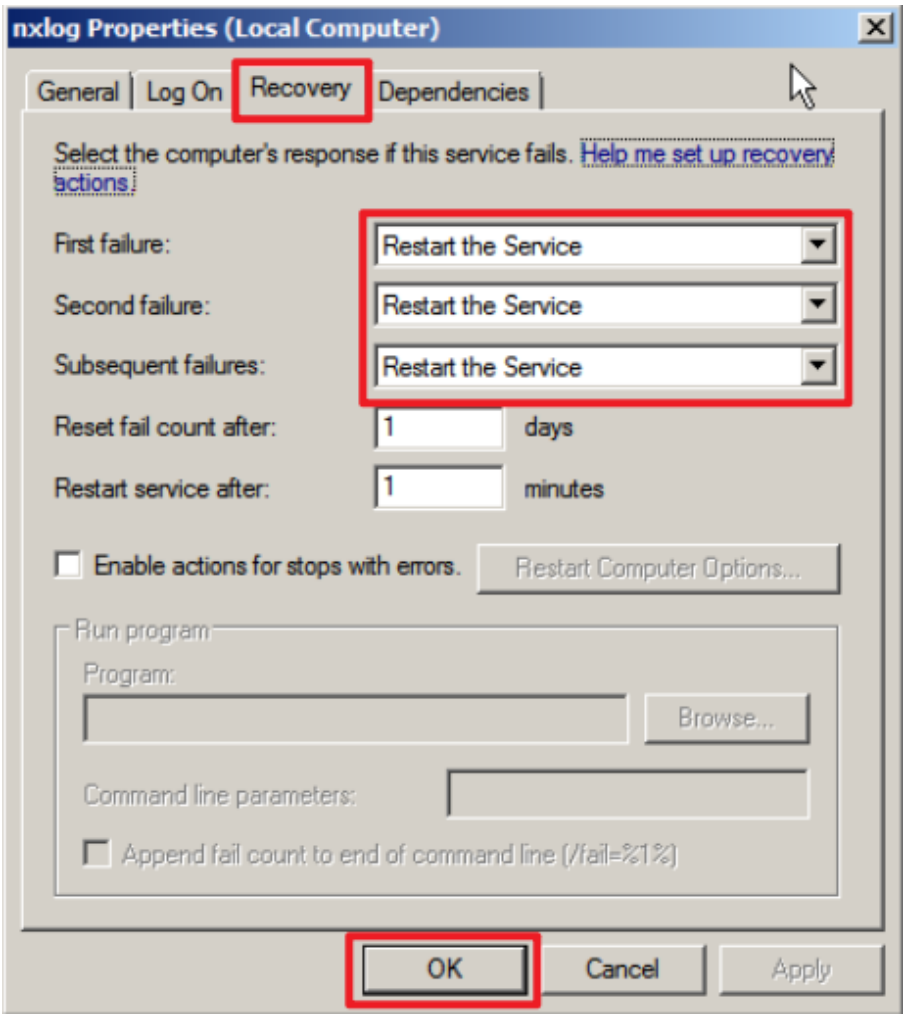
(4) Open the NXLog service properties: select “NXLog” →Click  “Properties.”



(5) On the General tab, verify that Startup type is set to Automatic (Delayed Start).



(6) On the Recovery tab, verify that First failure, Second failure, and Subsequent failures are all set to "Restart the Service", then click "OK."



2. Windows Server 2000

Windows Audit Policy Configuration:

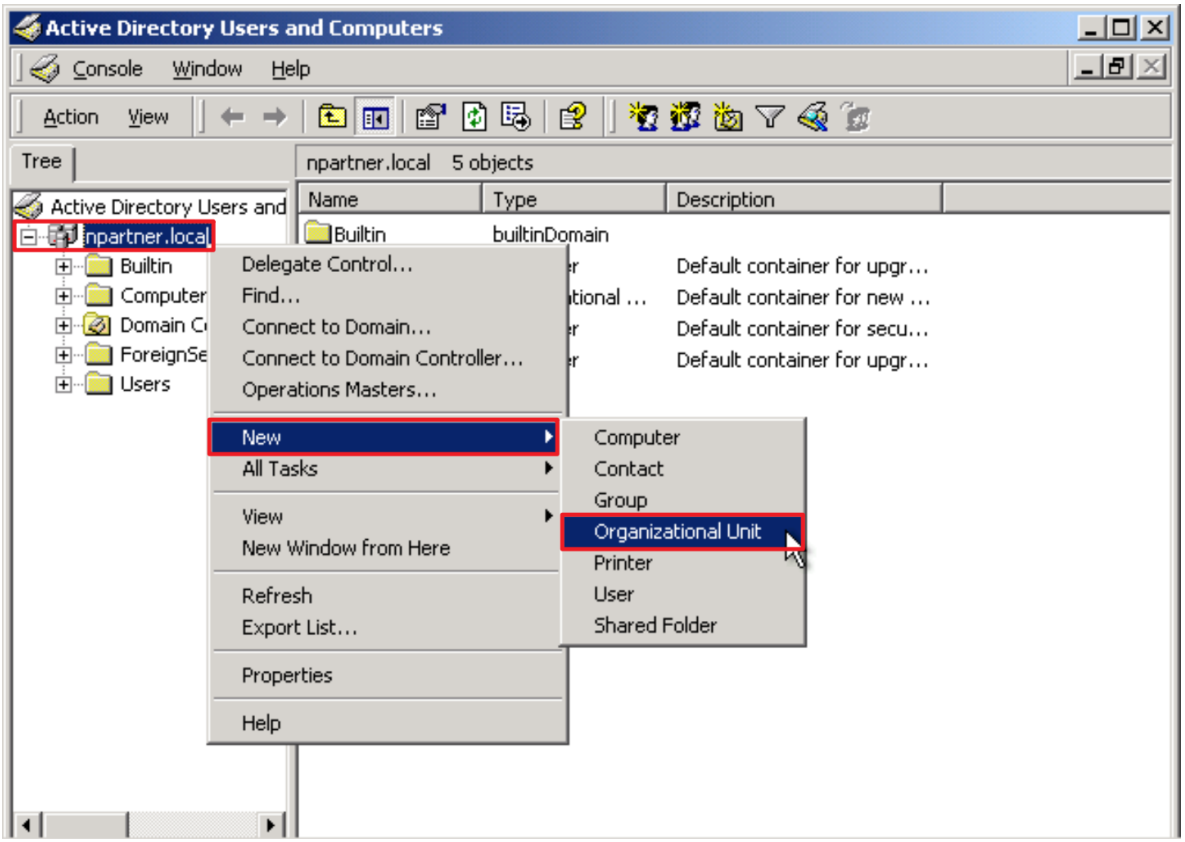
For detailed information, refer to the **Audit Policy Recommendations link** in the references.

2.1 Organizational Unit (OU) Configuration

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

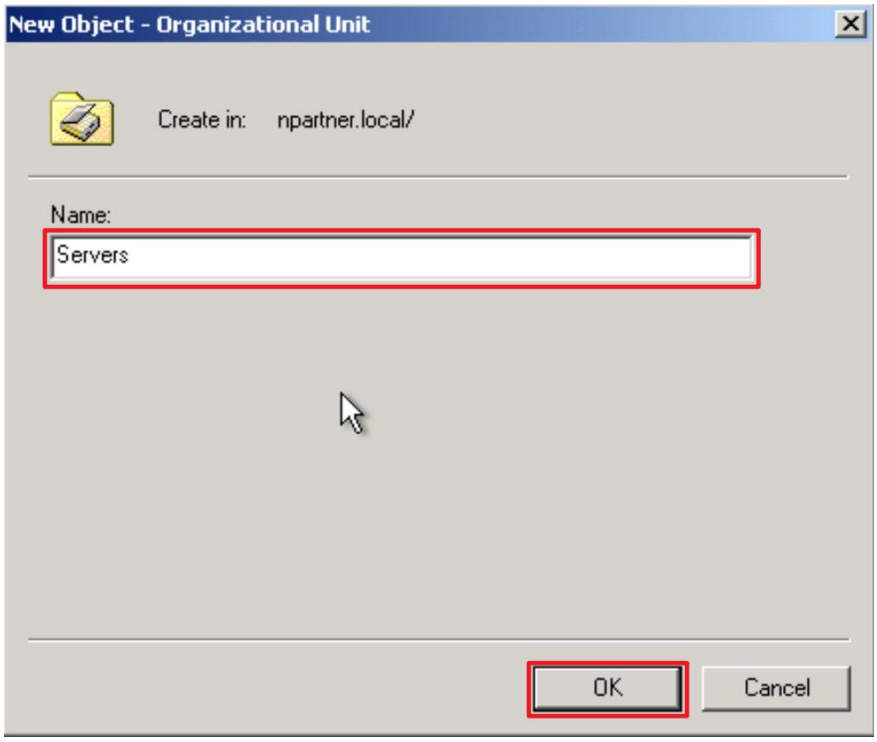
(2) Add an Organizational Unit

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



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

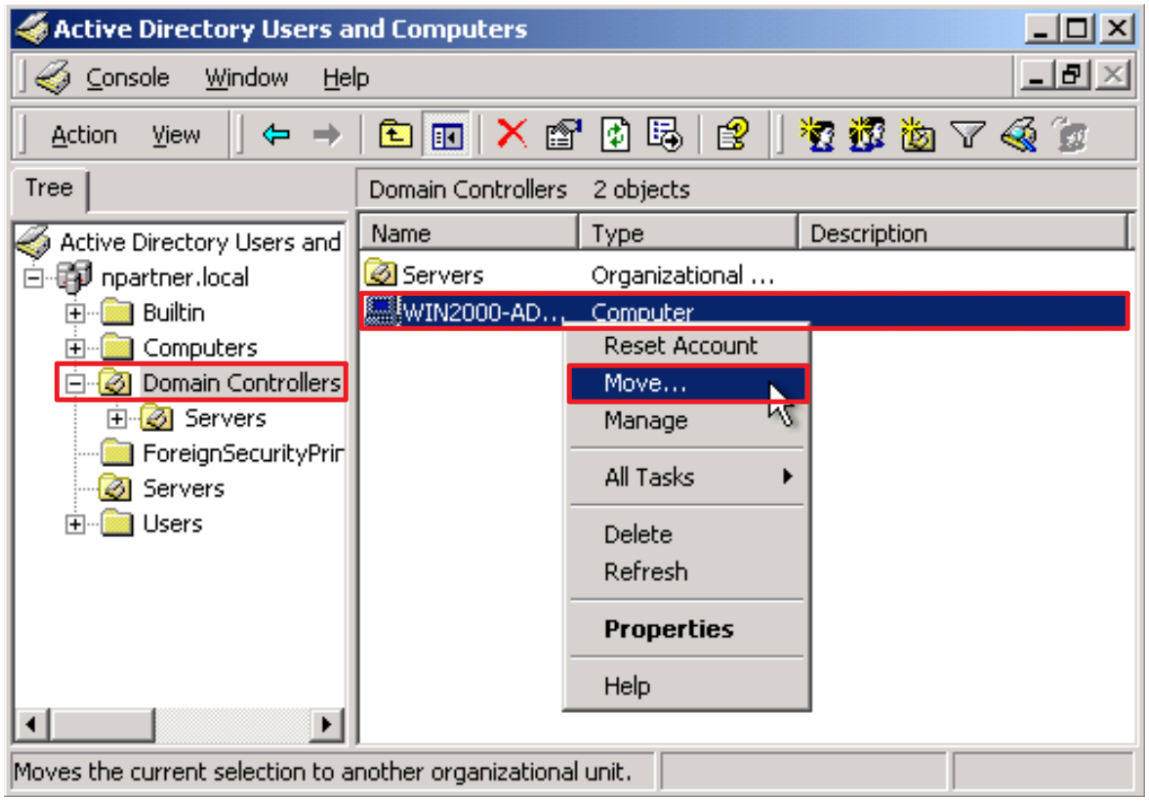
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

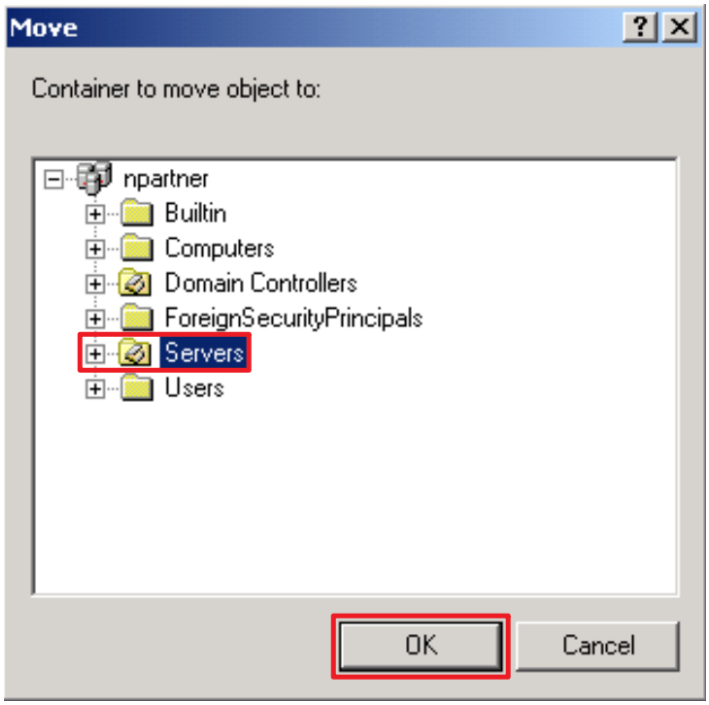
Select the “Computers” organizational unit (OU) → right-click on the “WIN2000-AD” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”



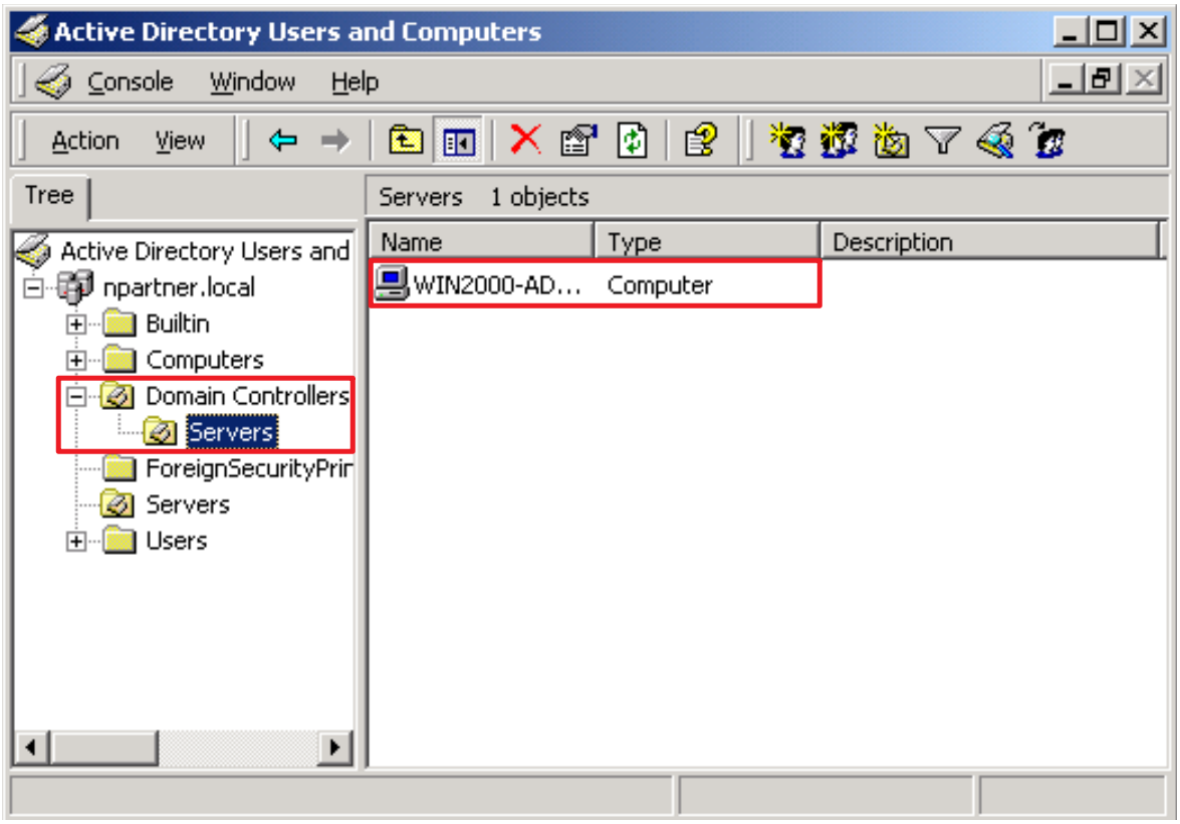
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



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

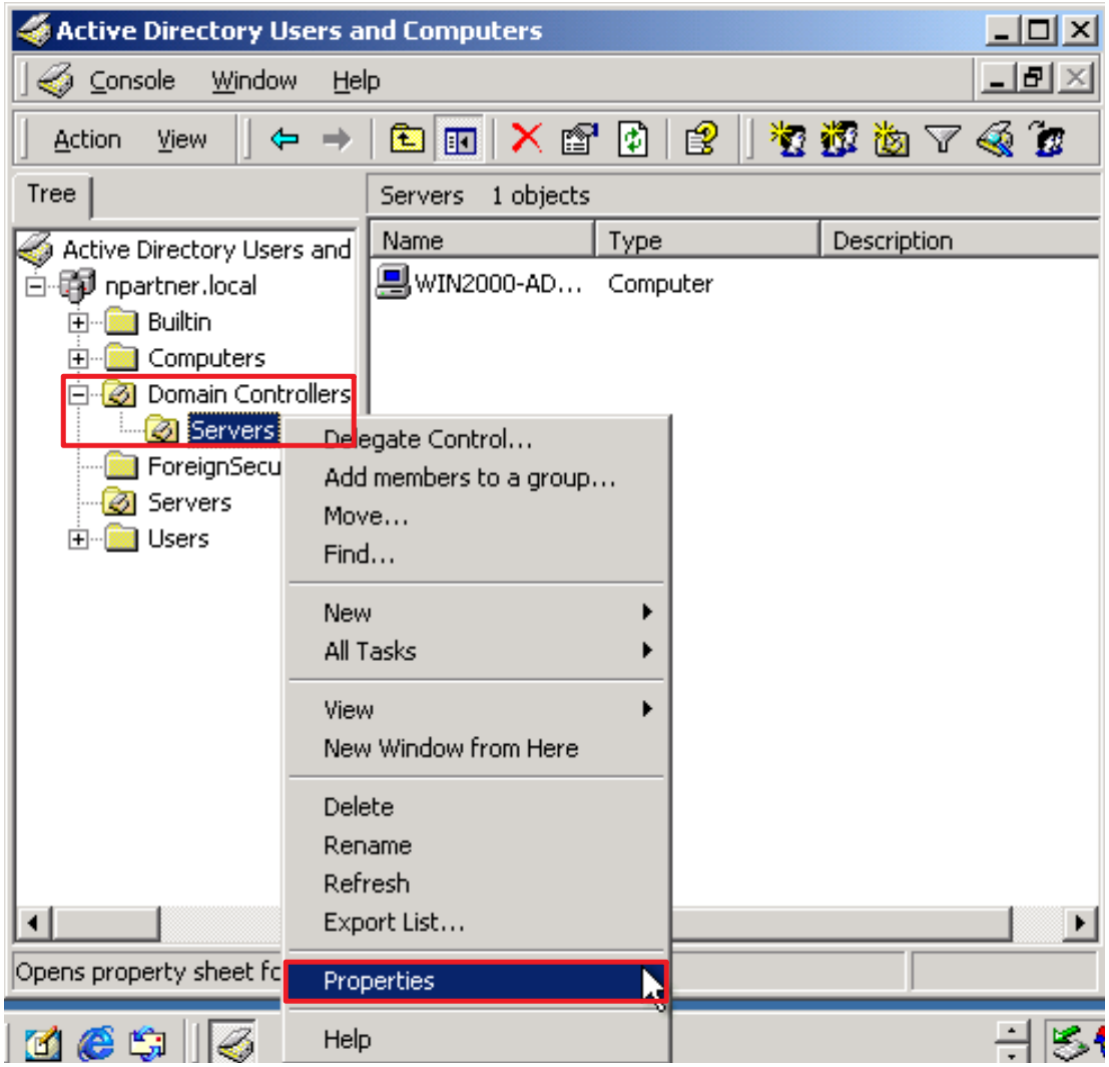
Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2000-AD” server has been moved.



2.2 Group Policy Settings

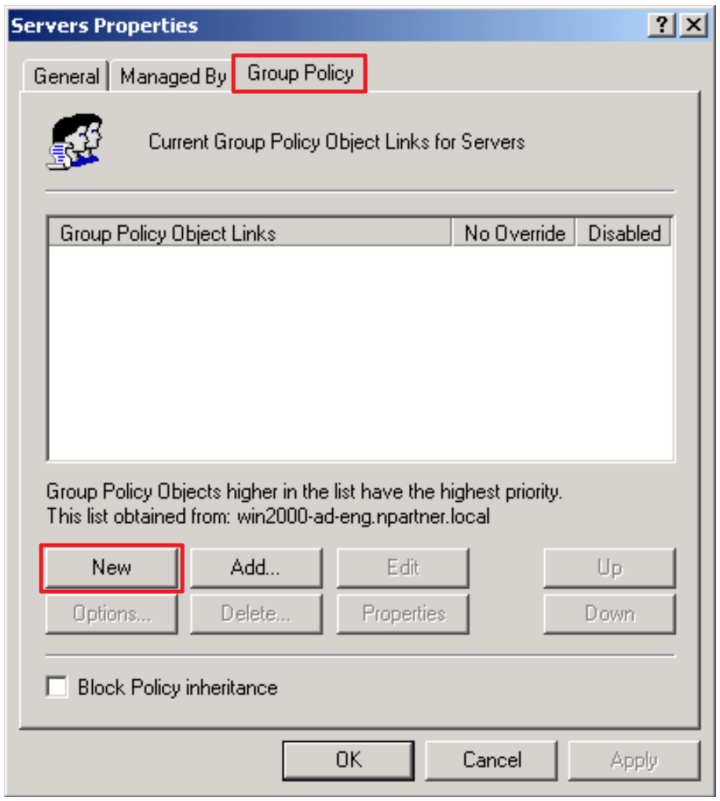
(1) Click “Active Directory Users and Computers.”

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



(3) Enter the Group Policy Object (GPO) name

On the “Group Policy” page → click “New.”

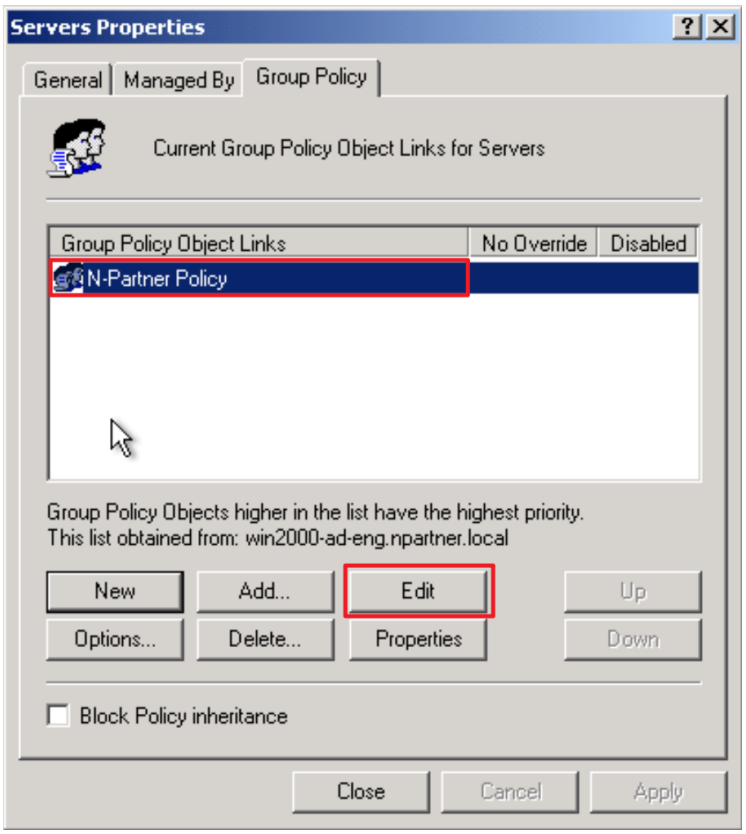


(4) Edit your Group Policy Object

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

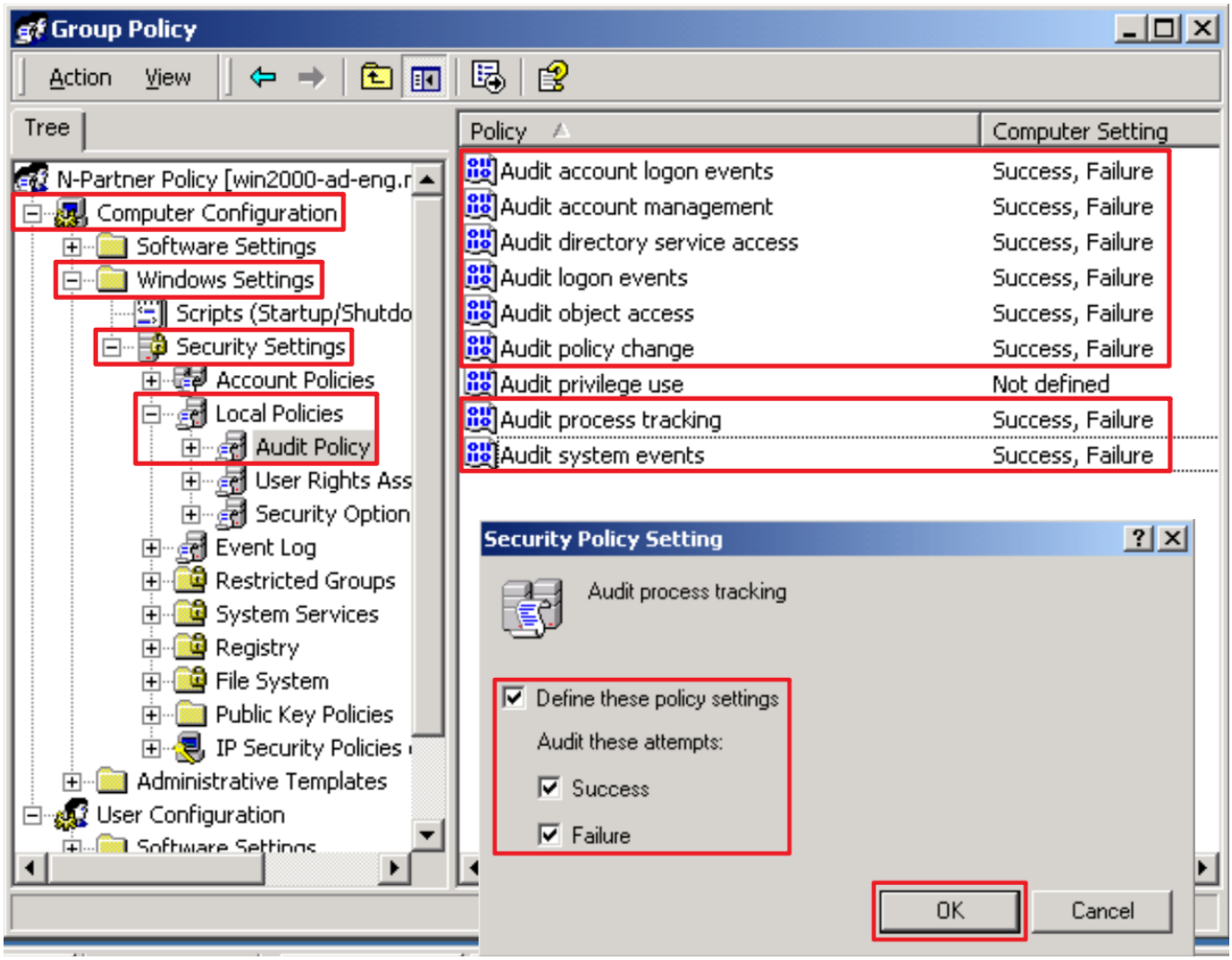
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



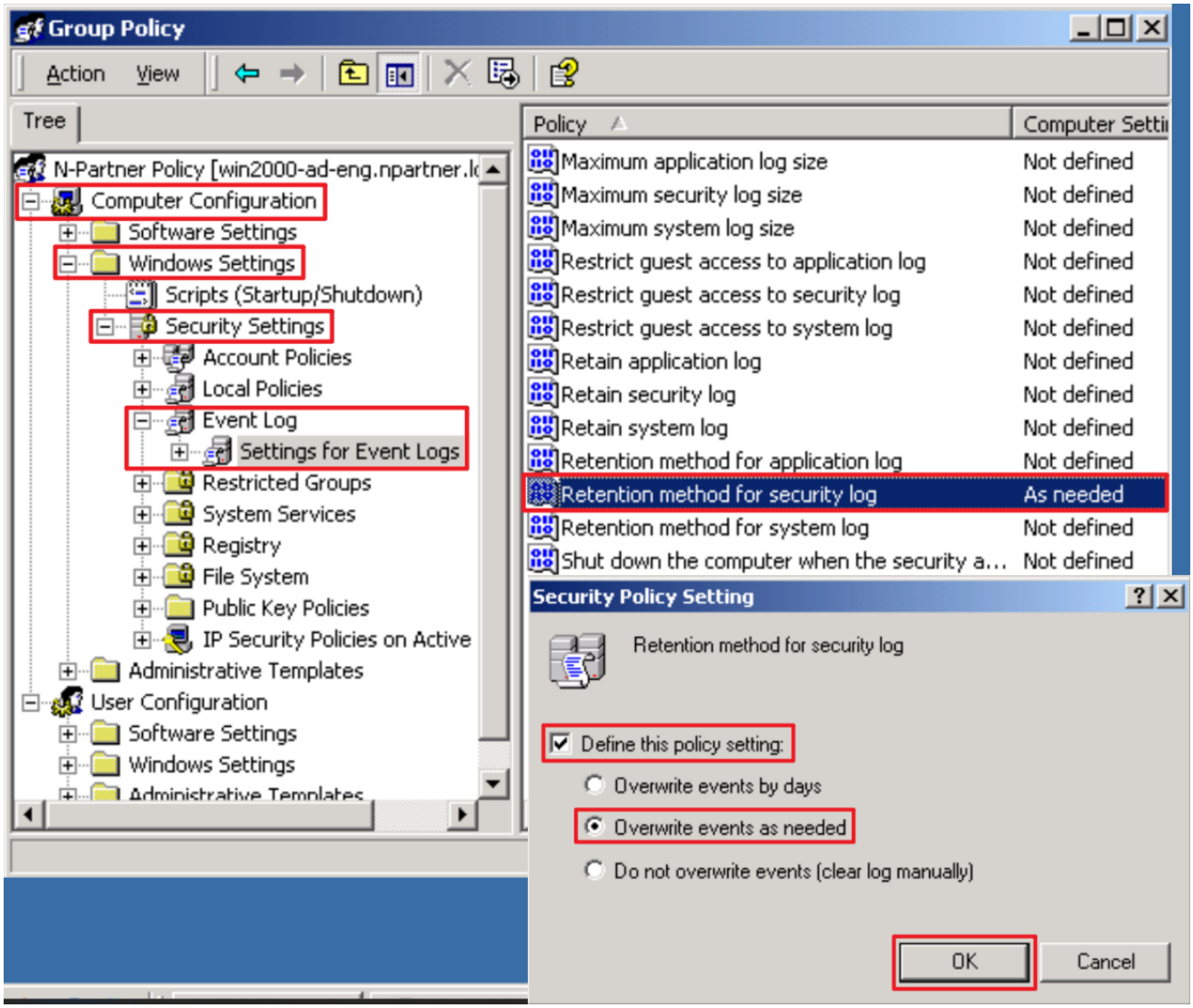
(5) Local Group Policies: Audit Policy

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” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

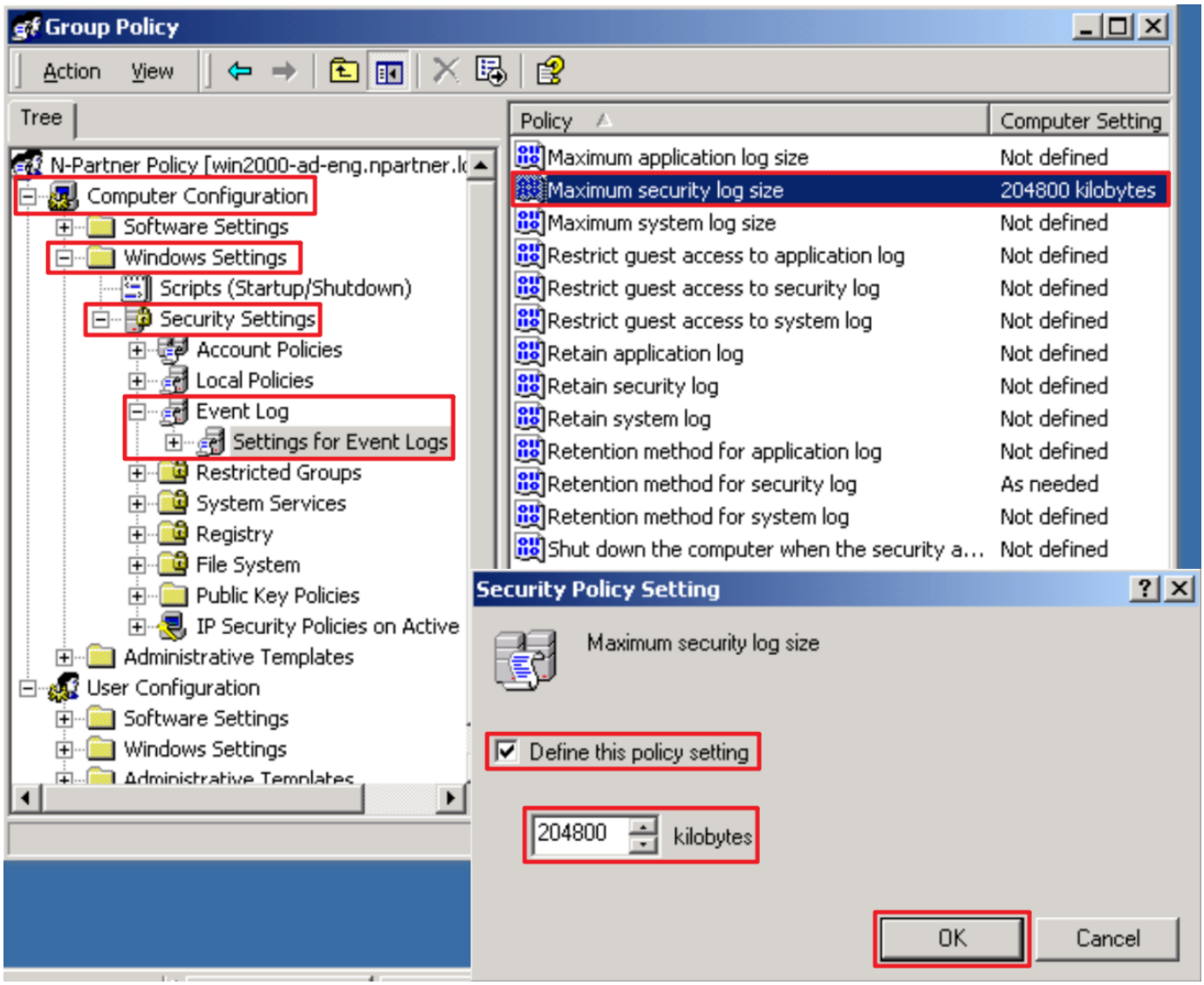
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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

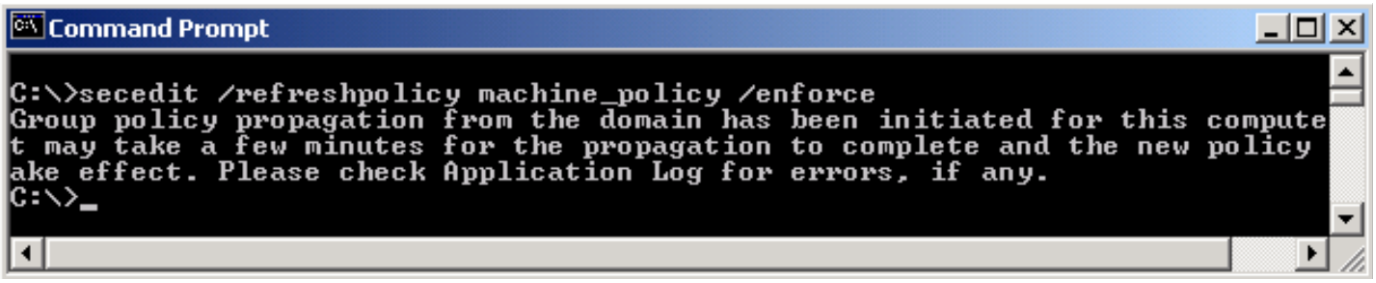
Note: Please adjust the number based on the actual environment. → click “OK.”



(8) On the Windows File server, open “Command Prompt.”

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

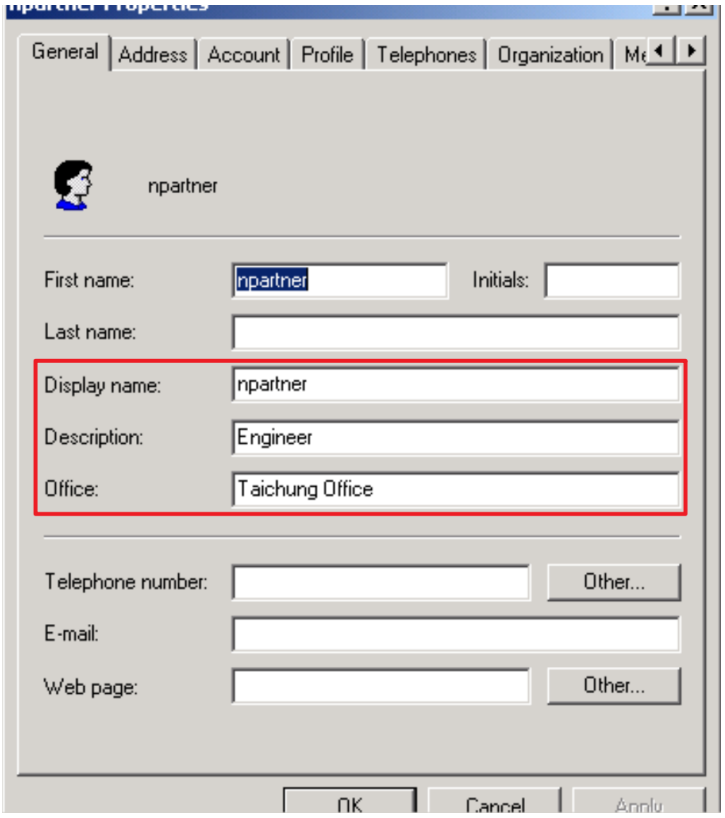
```
C:\> secedit /refreshpolicy machine_policy /enforce
```

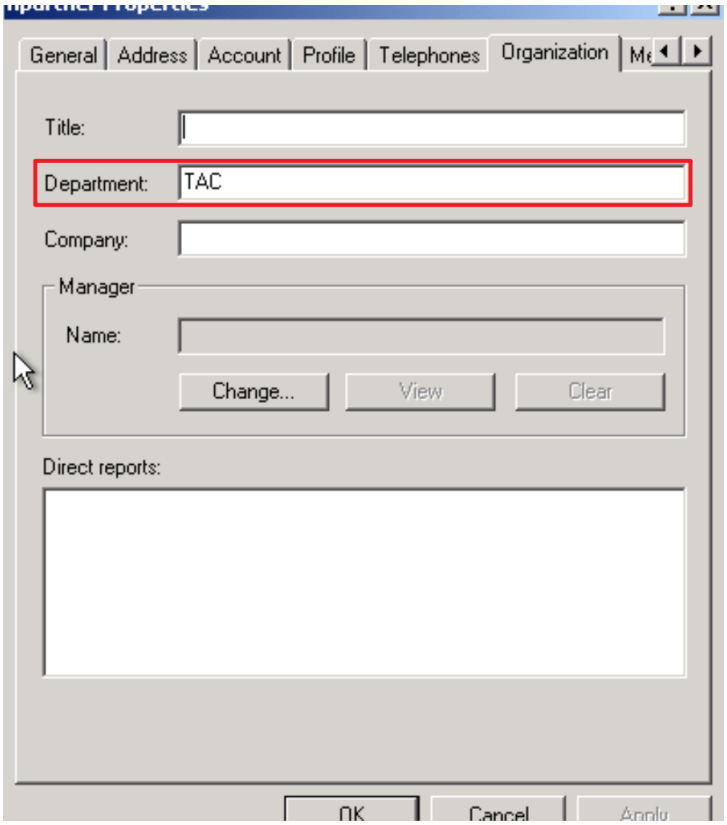


2.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Check whether N-Reporter associates Windows AD with available user data.





(2) In “Event Query,” click the information of “Username.”

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

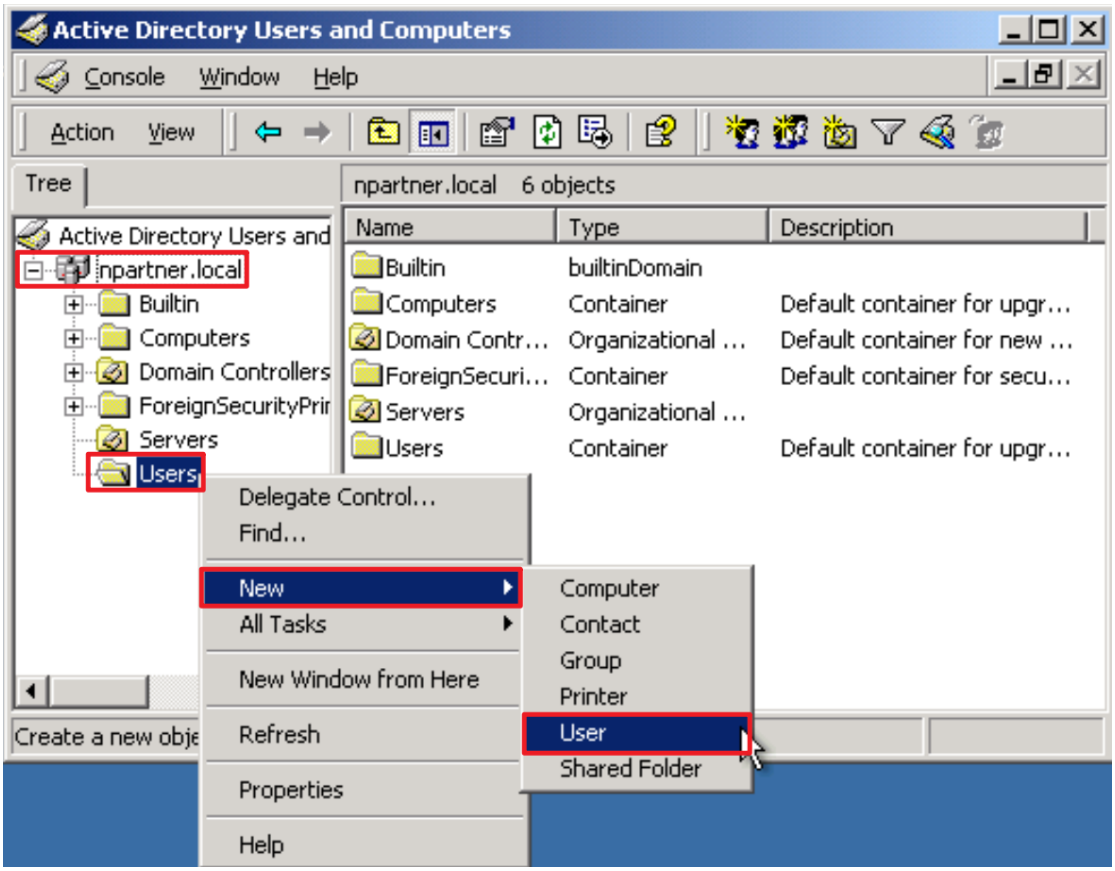
2.3.1 Add Non-Admin Accounts

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

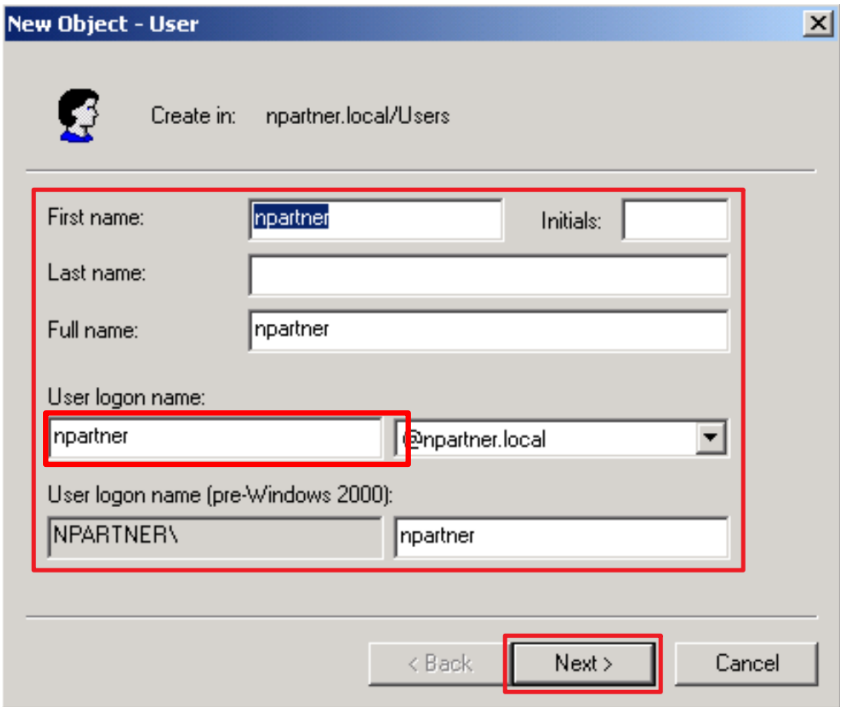
(2) Create an Account

Expand “Domain Name” (the example here is npartner.local) → right-click the “Users” organizational unit → select “New” → select “User”

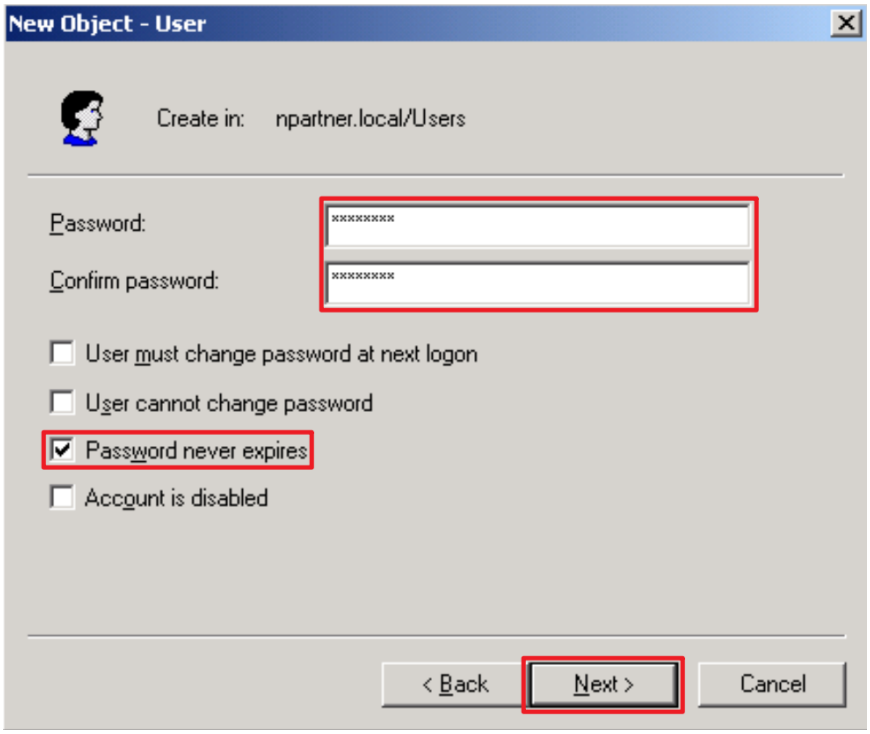
Note: Select your organizational unit according to the actual environment.



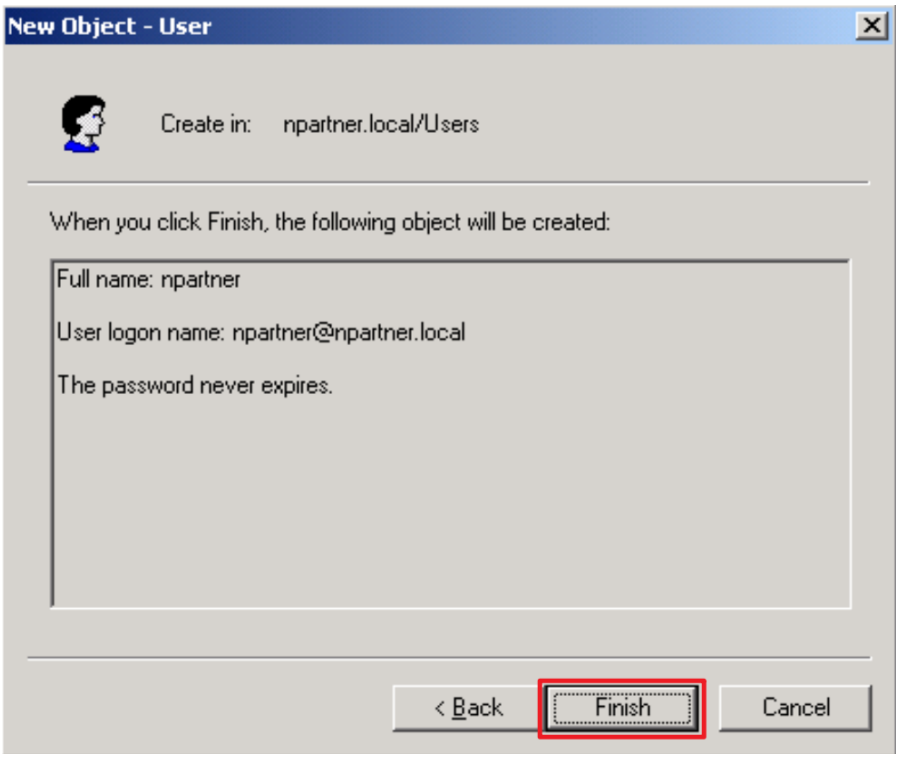
(3) Enter your full name (in this example, it is “npartner”) and user logon name (in this example, it is “npartner”), then click “Next.”



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



(5) Click “Finish.”

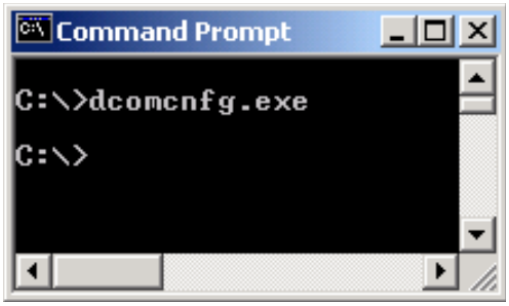


2.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”

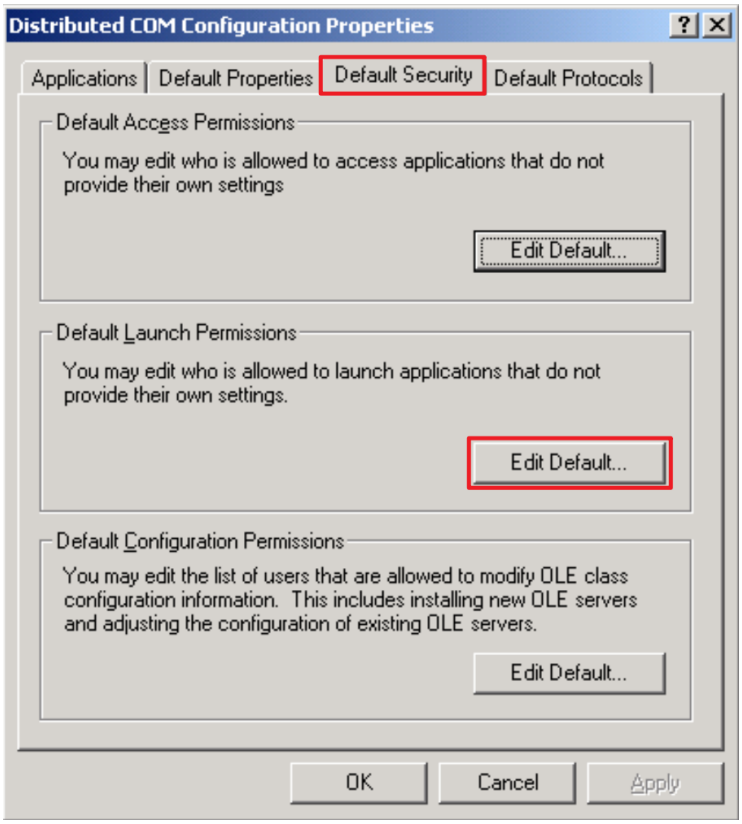
(2) Enter the command below to enable component services.

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



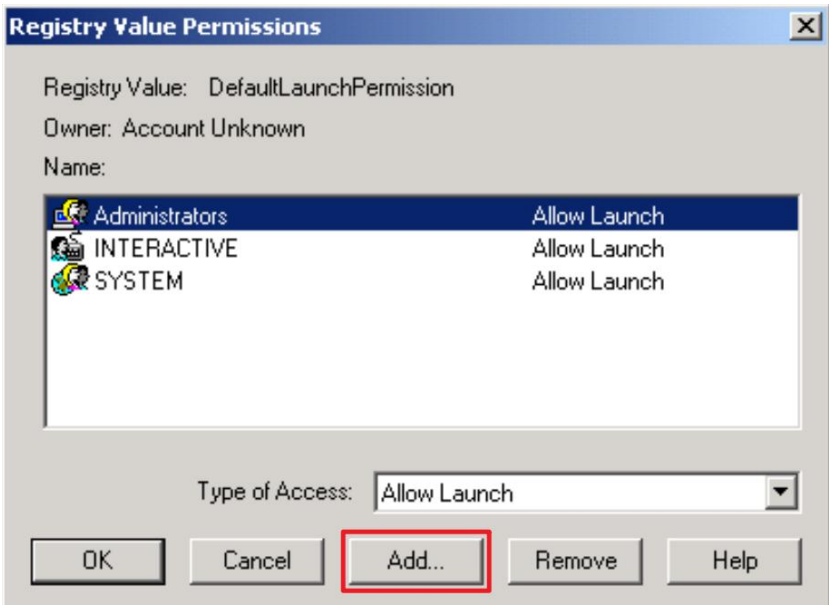
(3) Enable Default Access Permissions

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



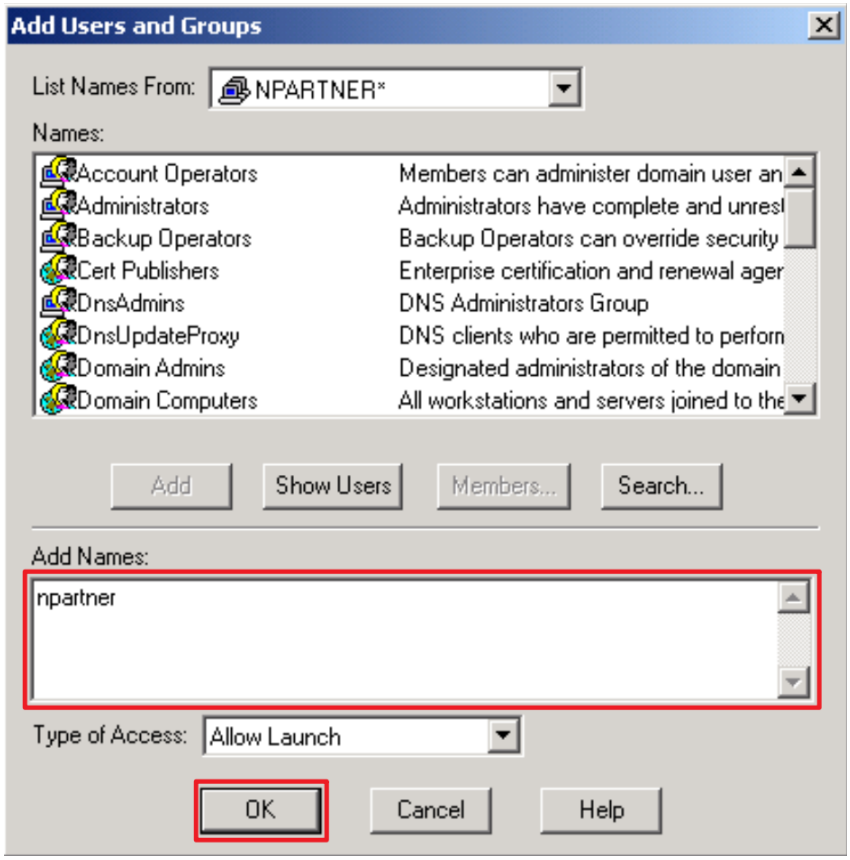
(4) Add User Permissions

Click “Add...”.

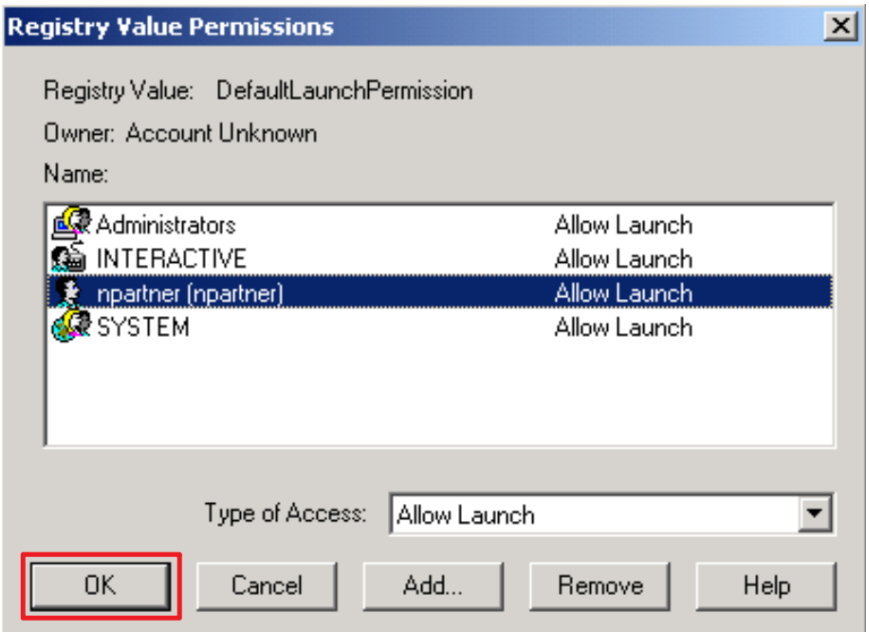


(5) Enter User

Enter the username (in this example, it is “npartner”) → click “OK.”

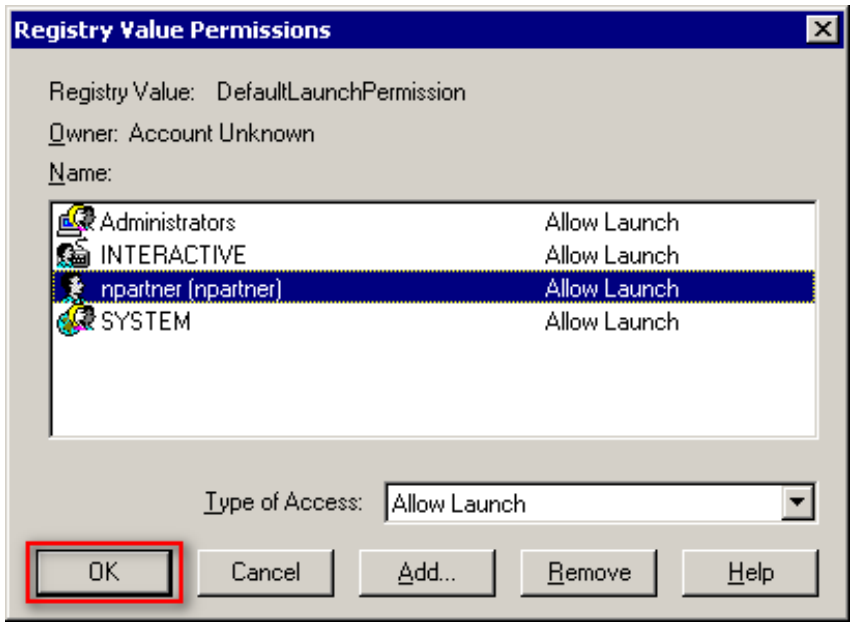


(6) Click “OK.”

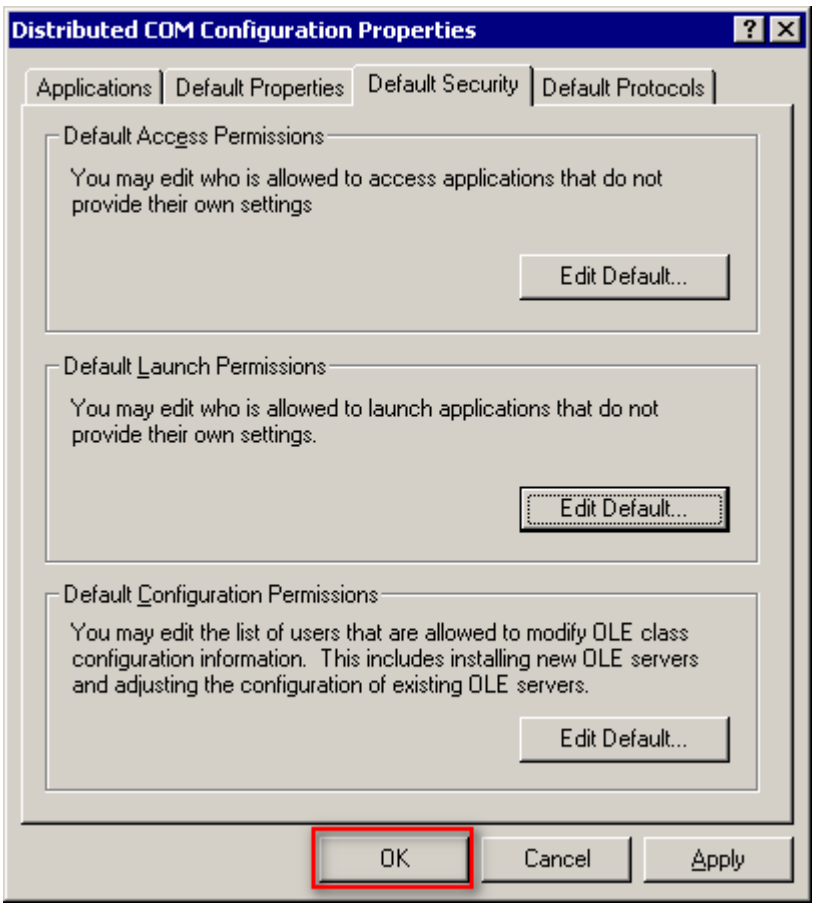


Select your user account (in this example, it is “npartner”), click “Add”, set type of access to “Allow Launch,” then click “OK.”

(7) Click “OK.”



(8) Click "OK.”



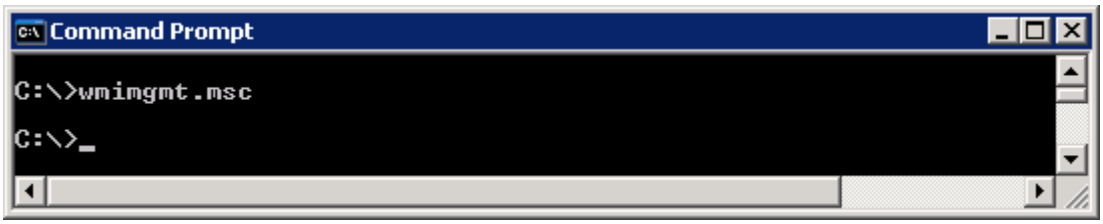
2.3.3 Configure WMI Permissions

2.3.3.1 Configure Event Log Permissions

(1) Open “Command Prompt.”

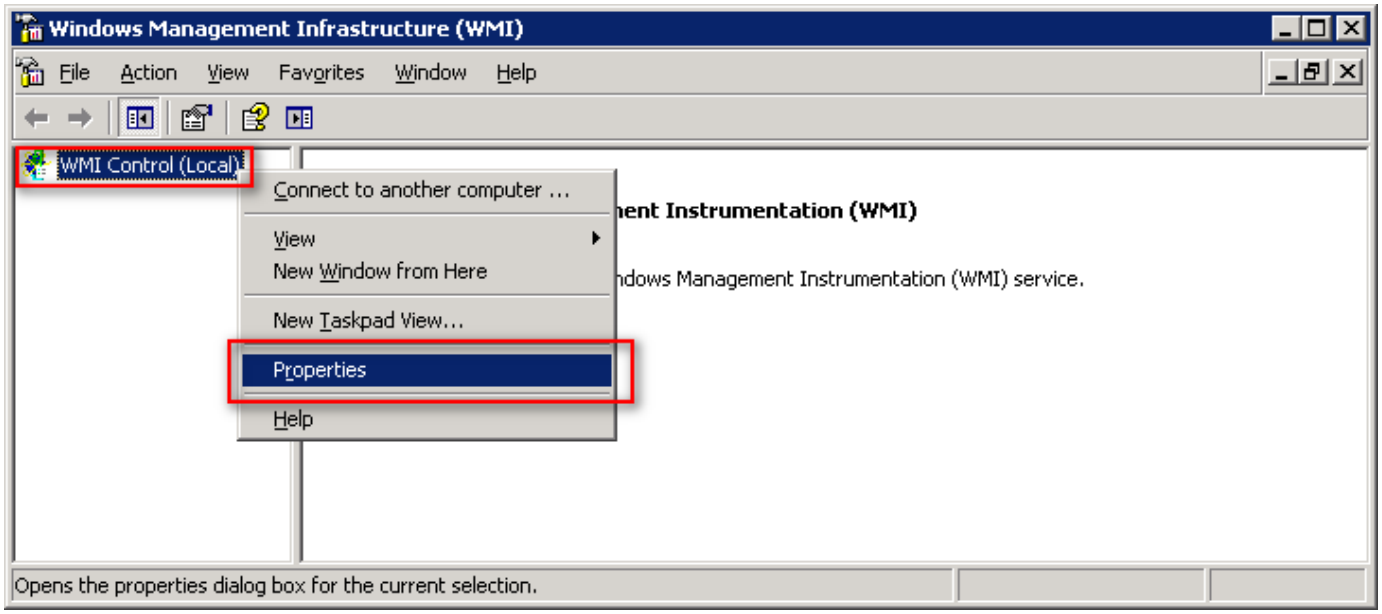
(2) Enter the command to enable WMI control service.

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



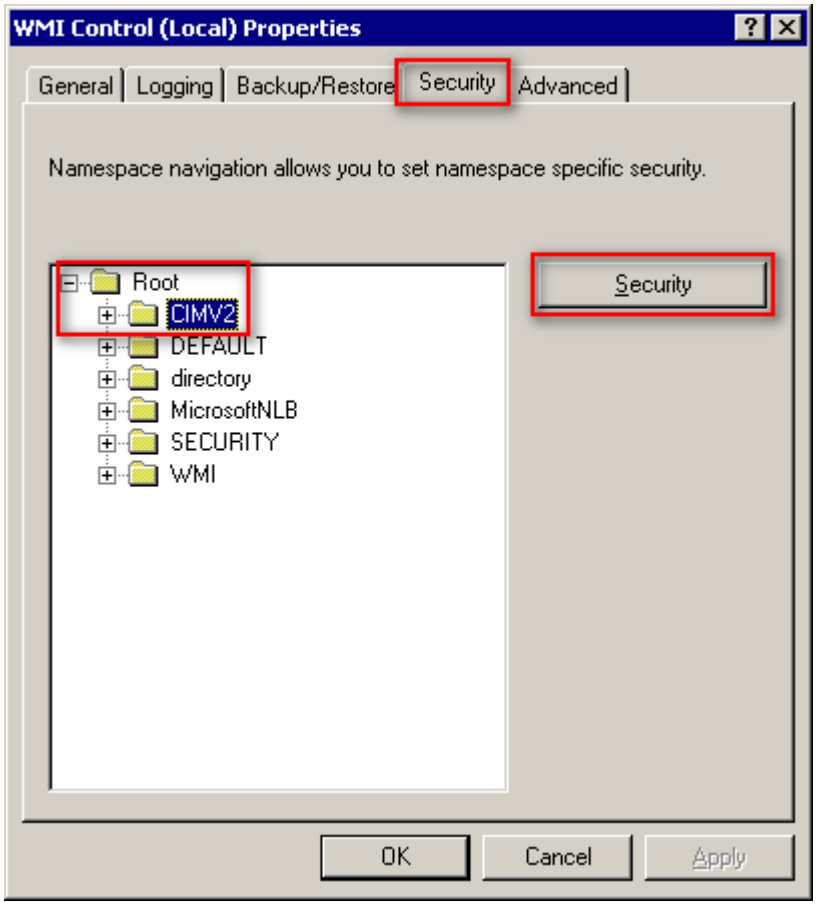
(3) Edit WMI Control

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



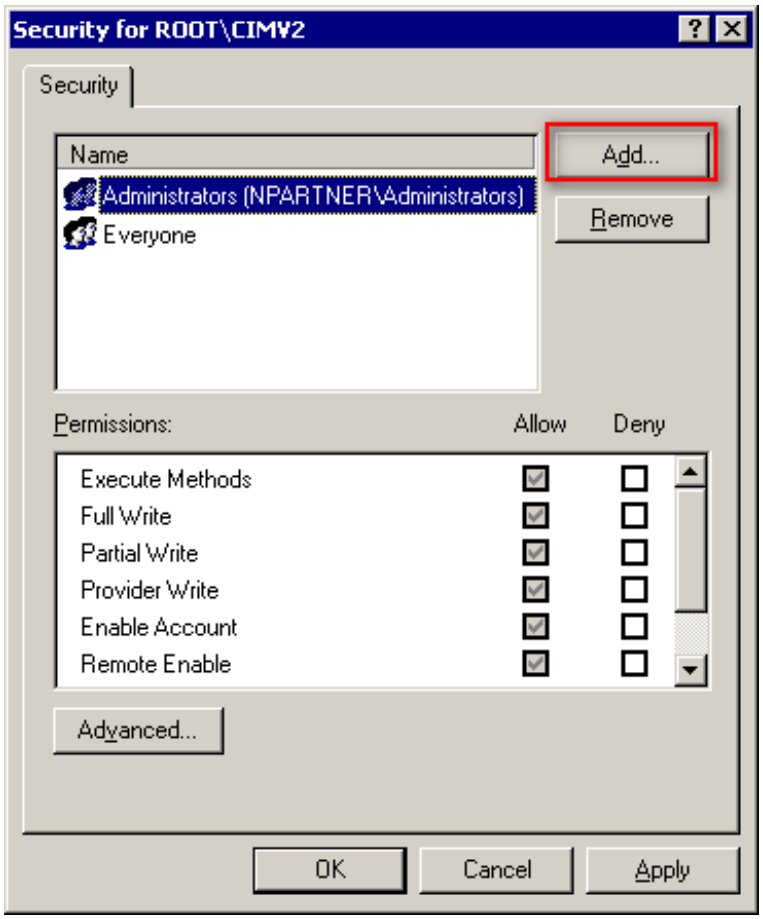
(4) Edit CIMV2 Security

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



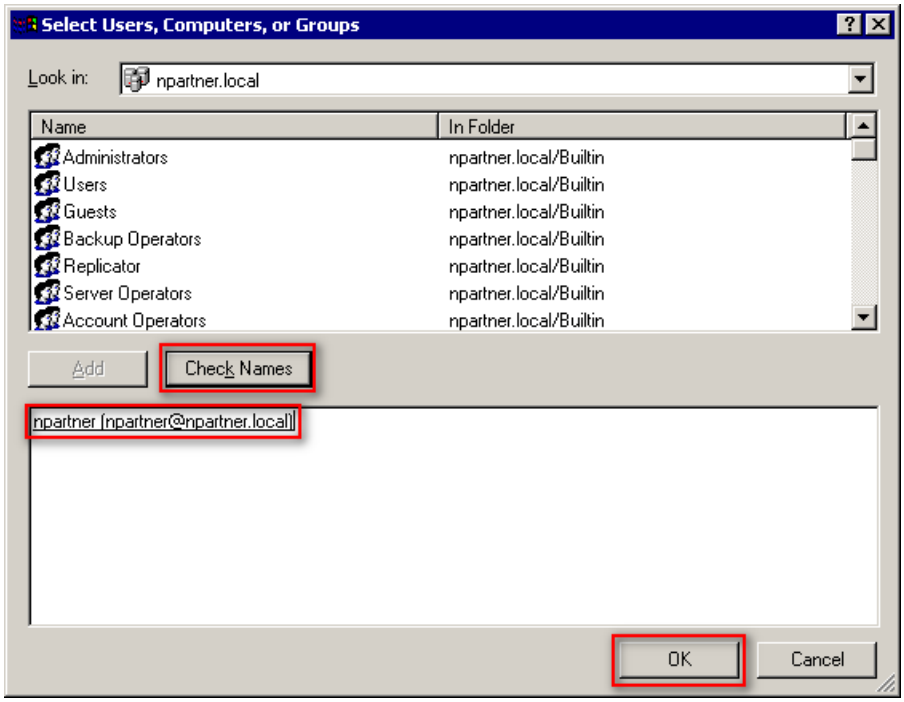
(5) Add WMI User Permissions.

Click “Add.”



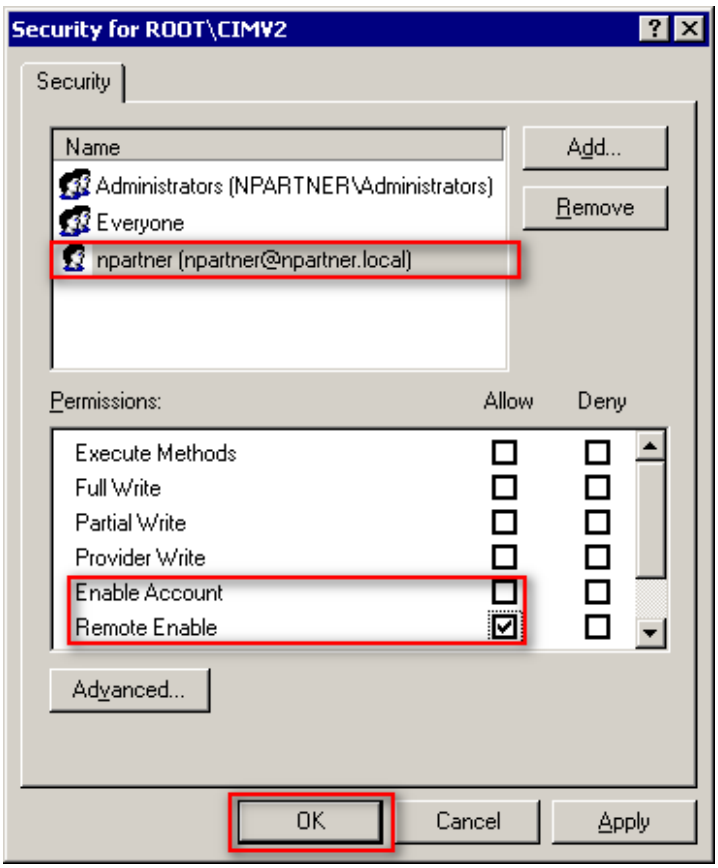
(6) Enter Your Username

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

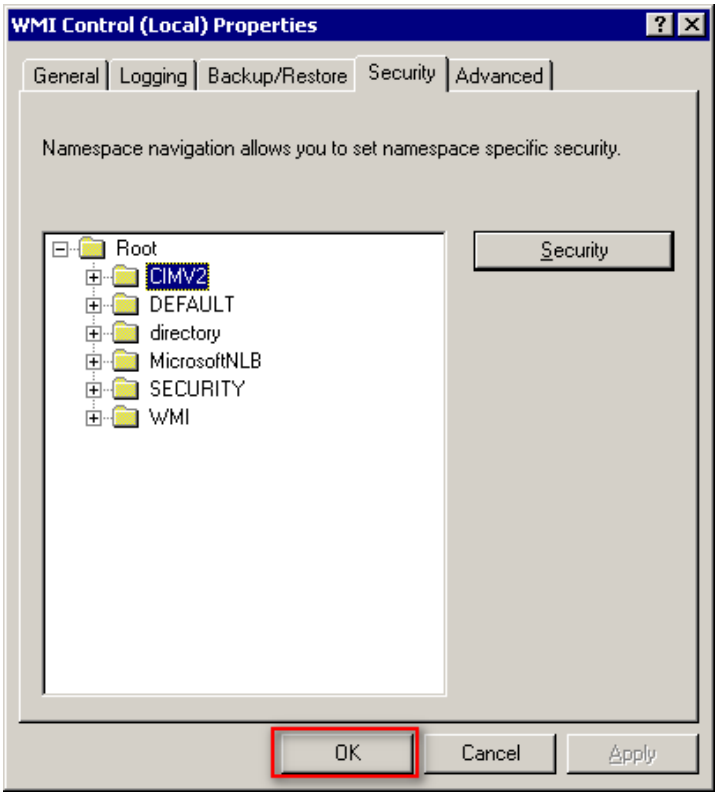


(7) Set Your User Permissions

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



(8) Click “OK.”

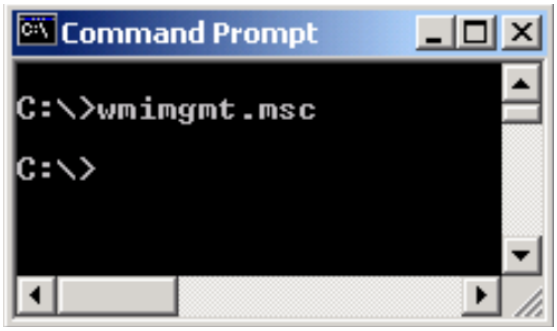


2.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”

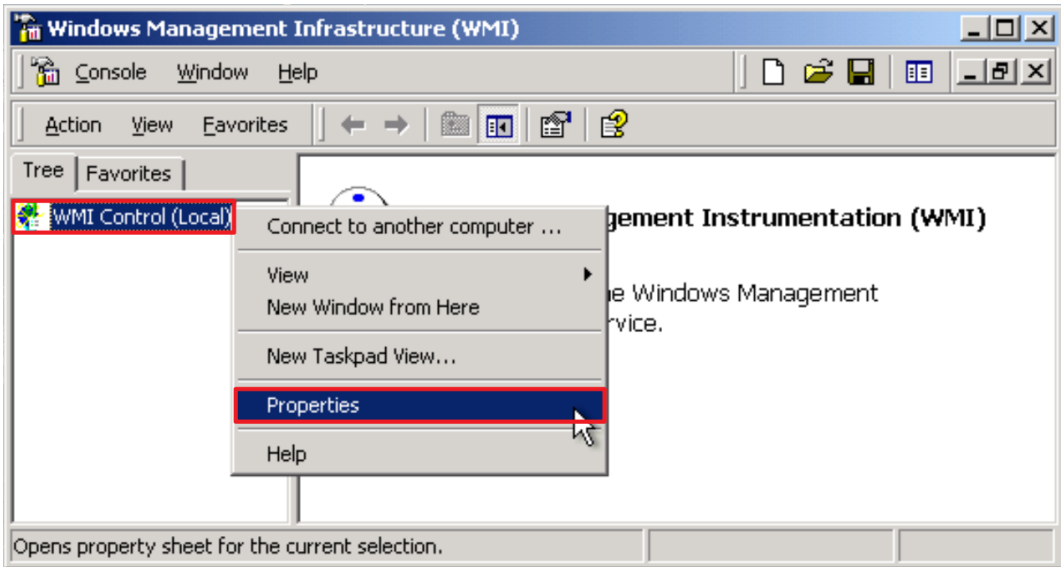
(2) Enter the command below to enable WMI Control.

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



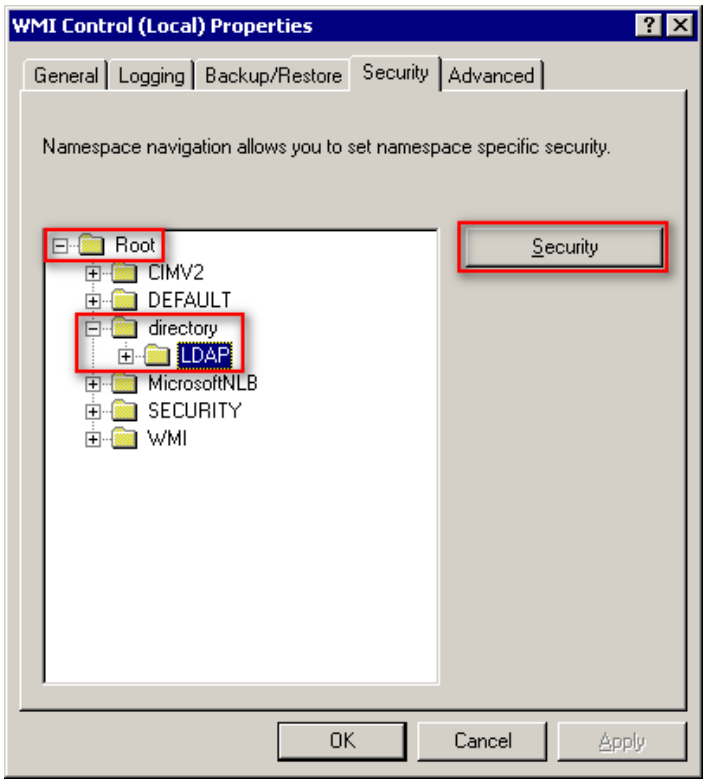
(3) Edit WMI Control

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



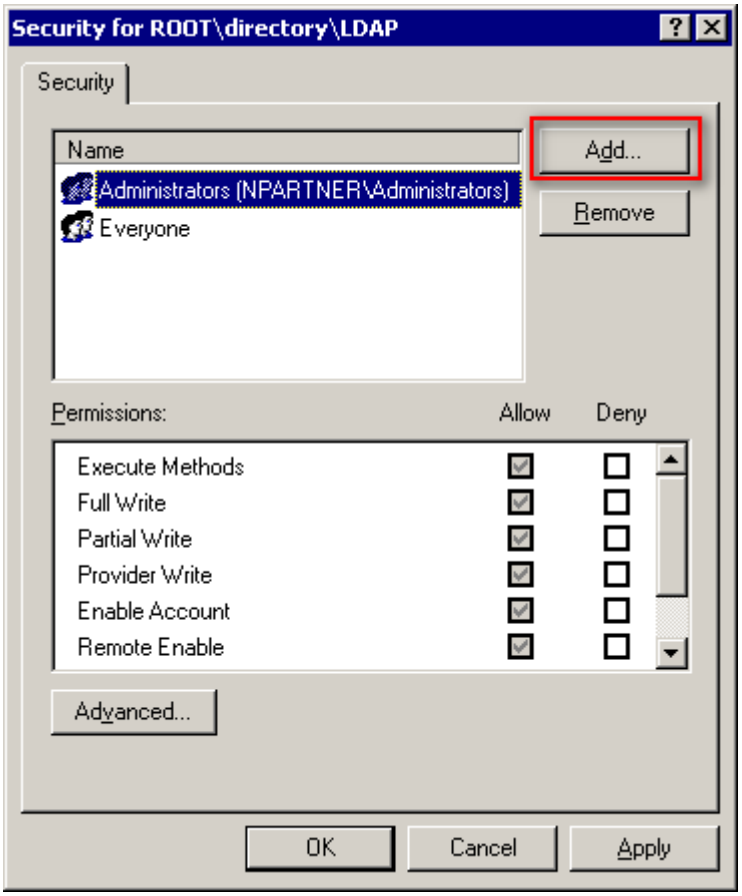
(4) Edit LDAP Security

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



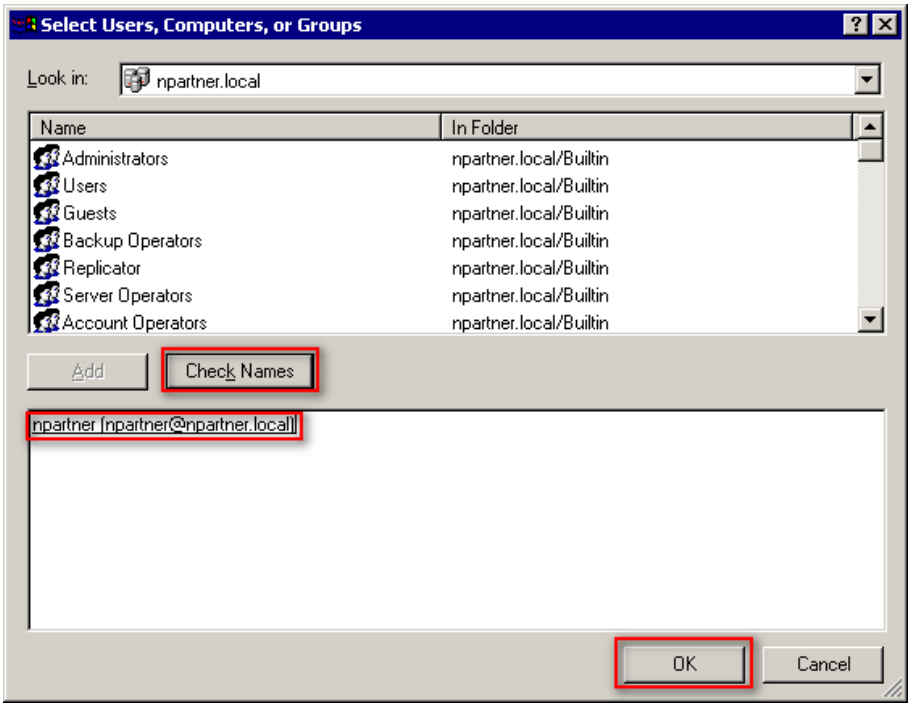
(5) Add WMI User Permissions

Click “Add.”



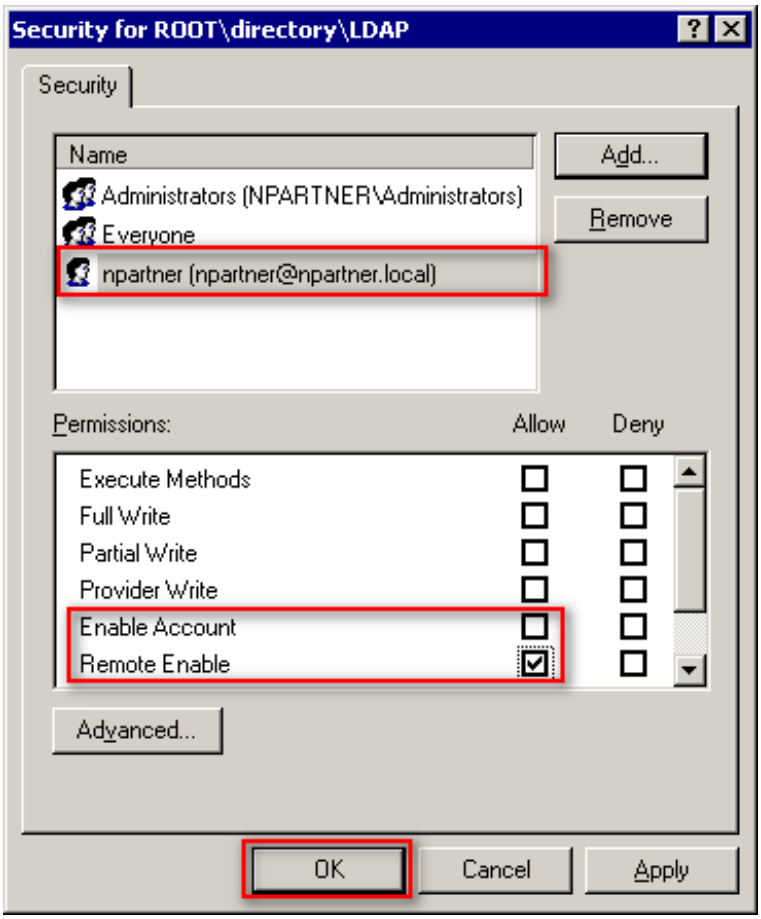
(6) Enter Your Username

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

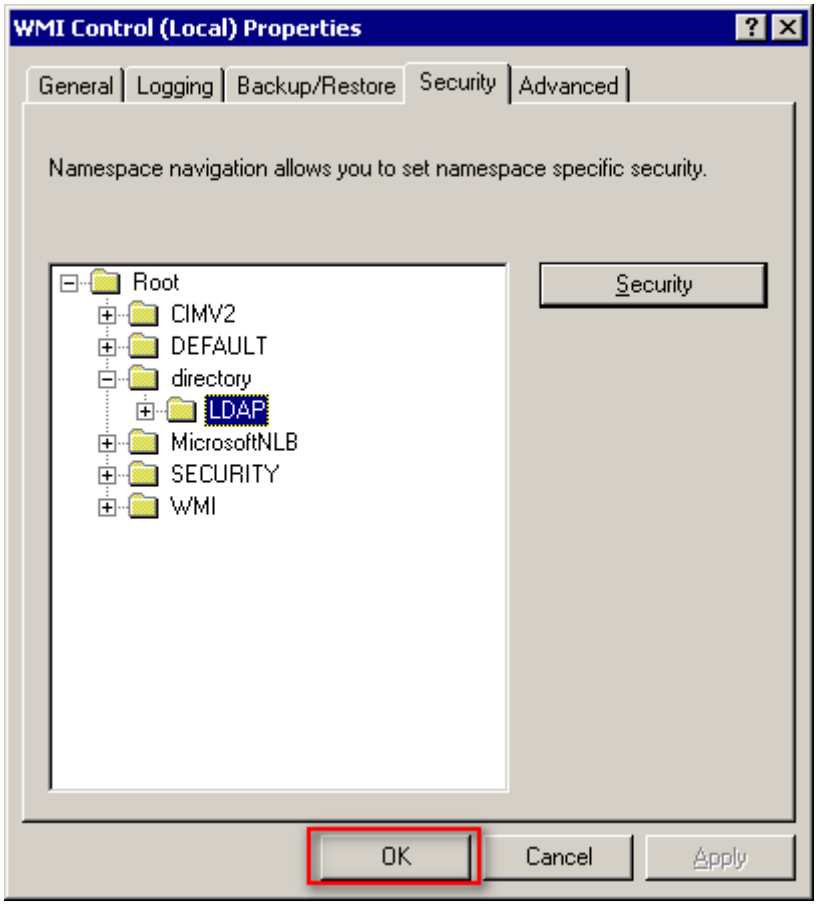


(7) Set Your User Permissions

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



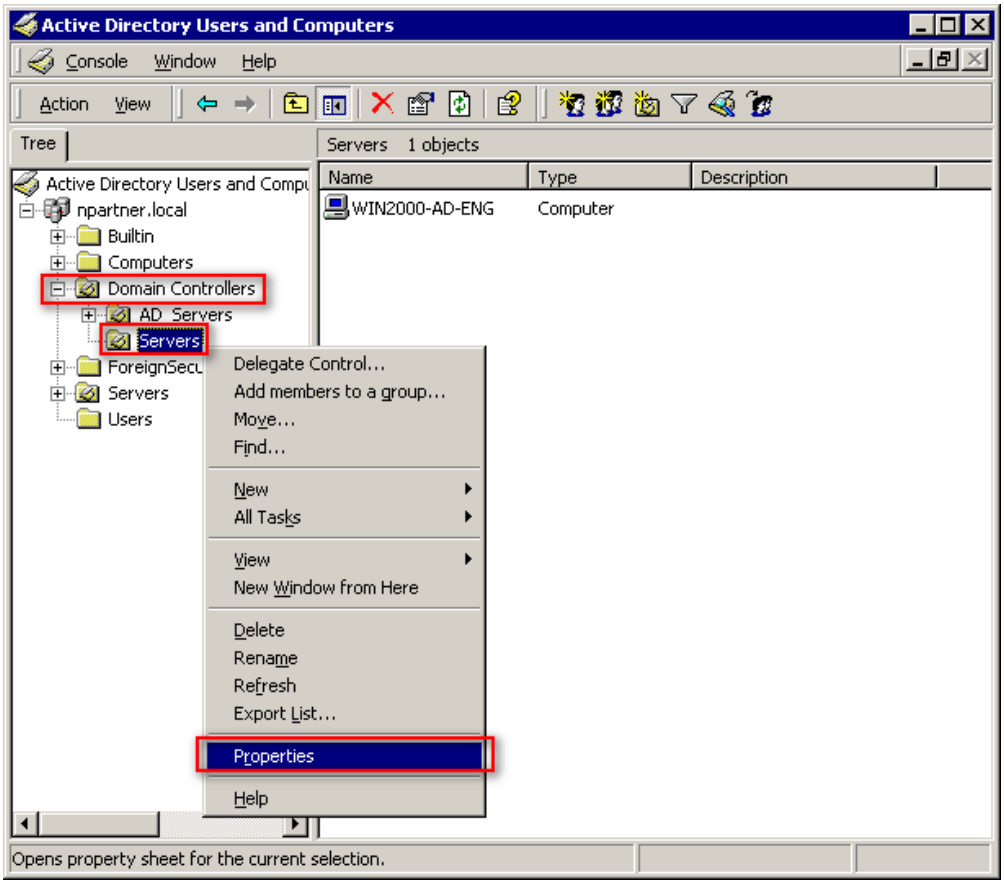
(8) Click “OK.”



2.3.4 Configure Event Log Read Permissions

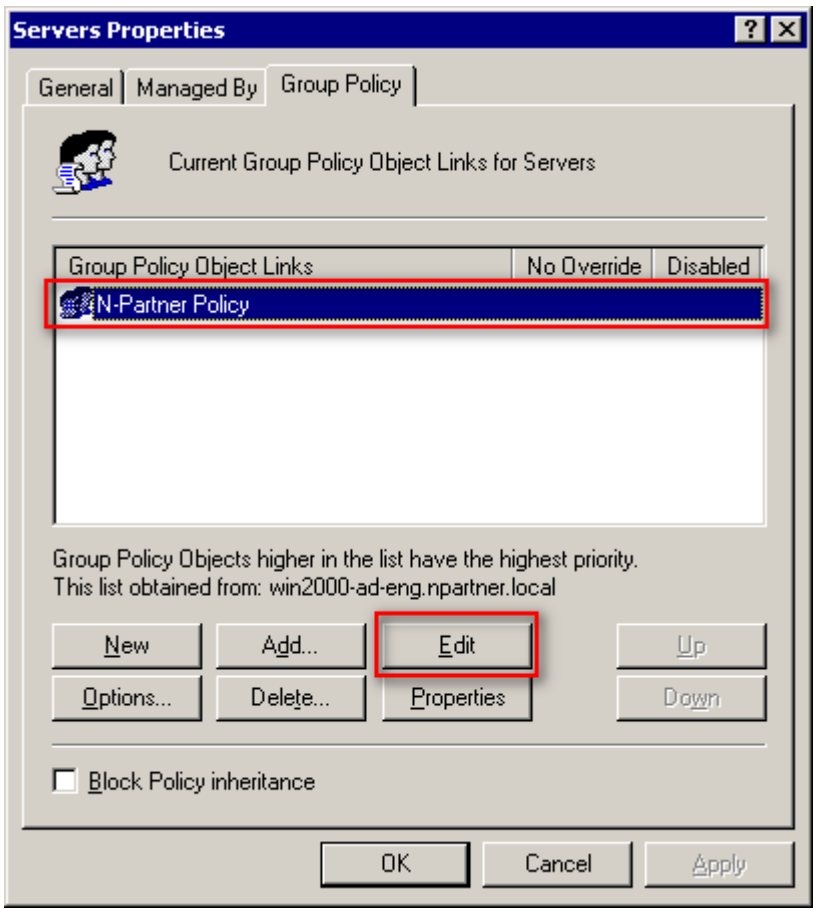
(1) Click “Active Directory Users and Computers.”

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



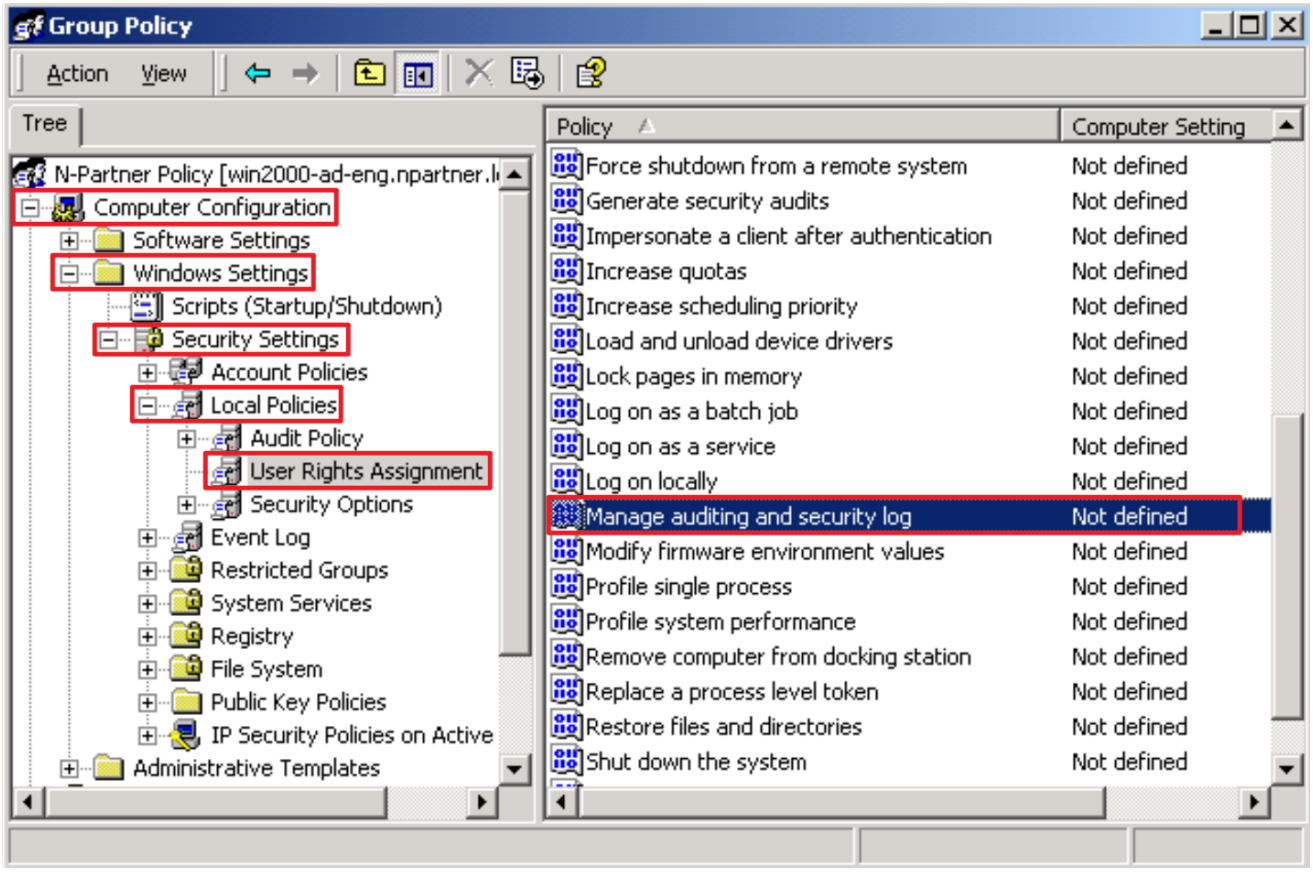
(3) Edit Group Policy Object

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.”

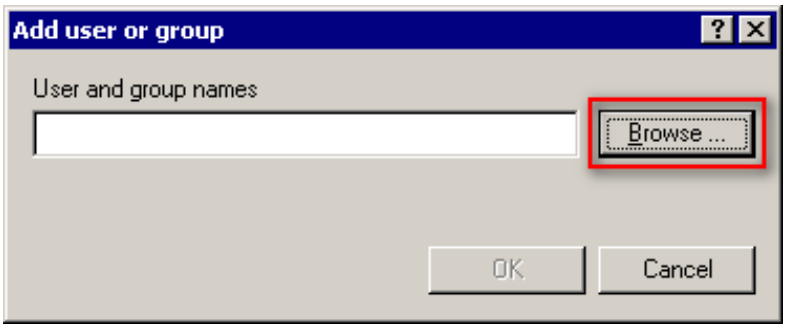


(5) Add Auditing User

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

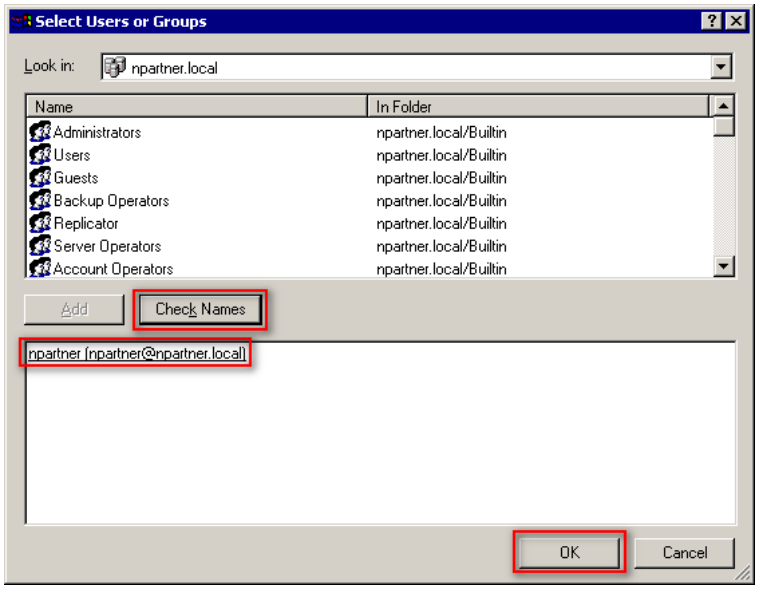
(6) Search for User

Click “Browse.”

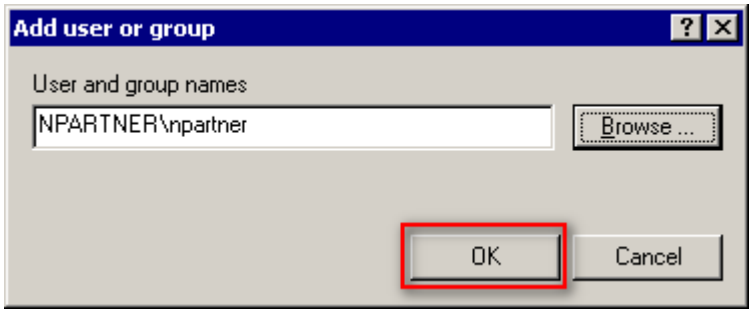


(7) Enter Your User Account

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

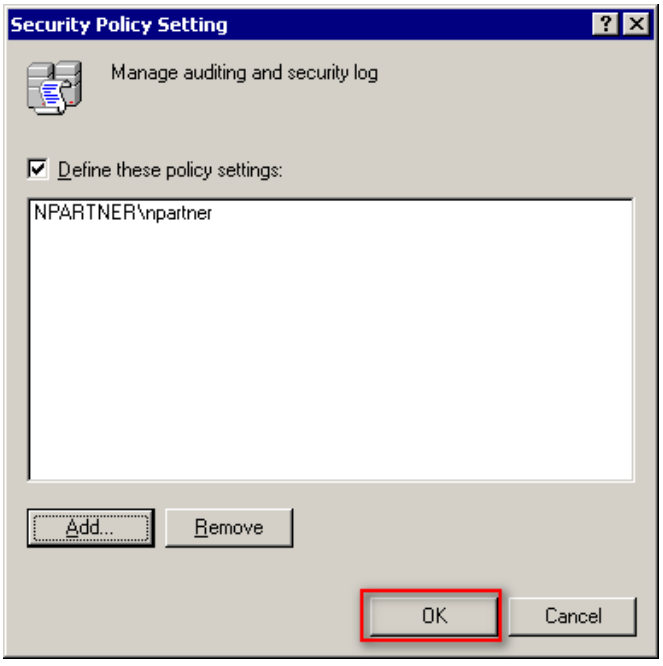


(8) Click “OK.”



(9) Confirm Audit Log Settings

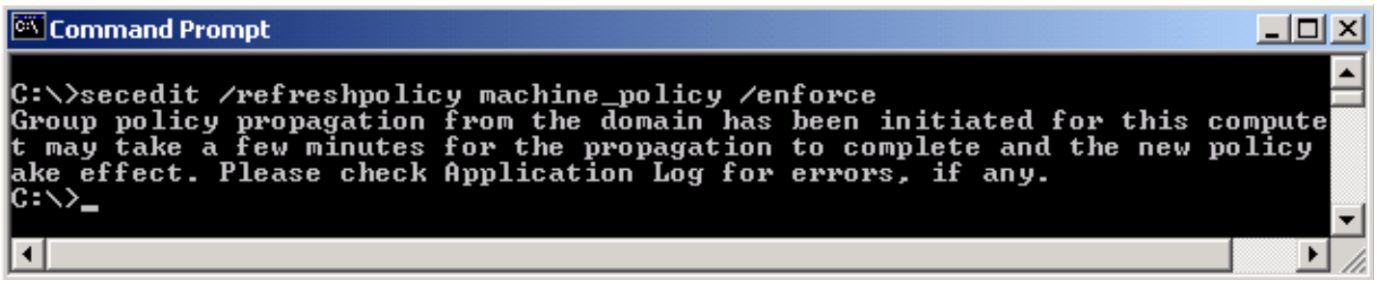
Click “OK.”



(10) Open “Command Prompt.”

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

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

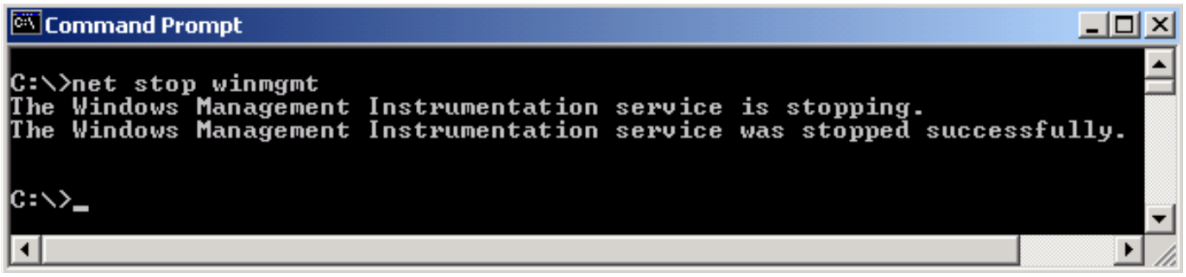


2.3.5 Restart the WMI Service

(1) Open “Command Prompt.”

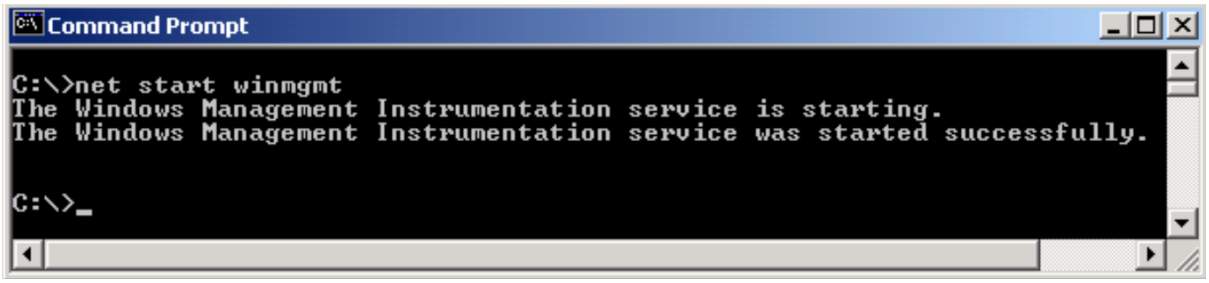
(2) Enter the command below to disable the WMI service.

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



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

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



3. Windows Server 2003

Windows Audit Policy Configuration:

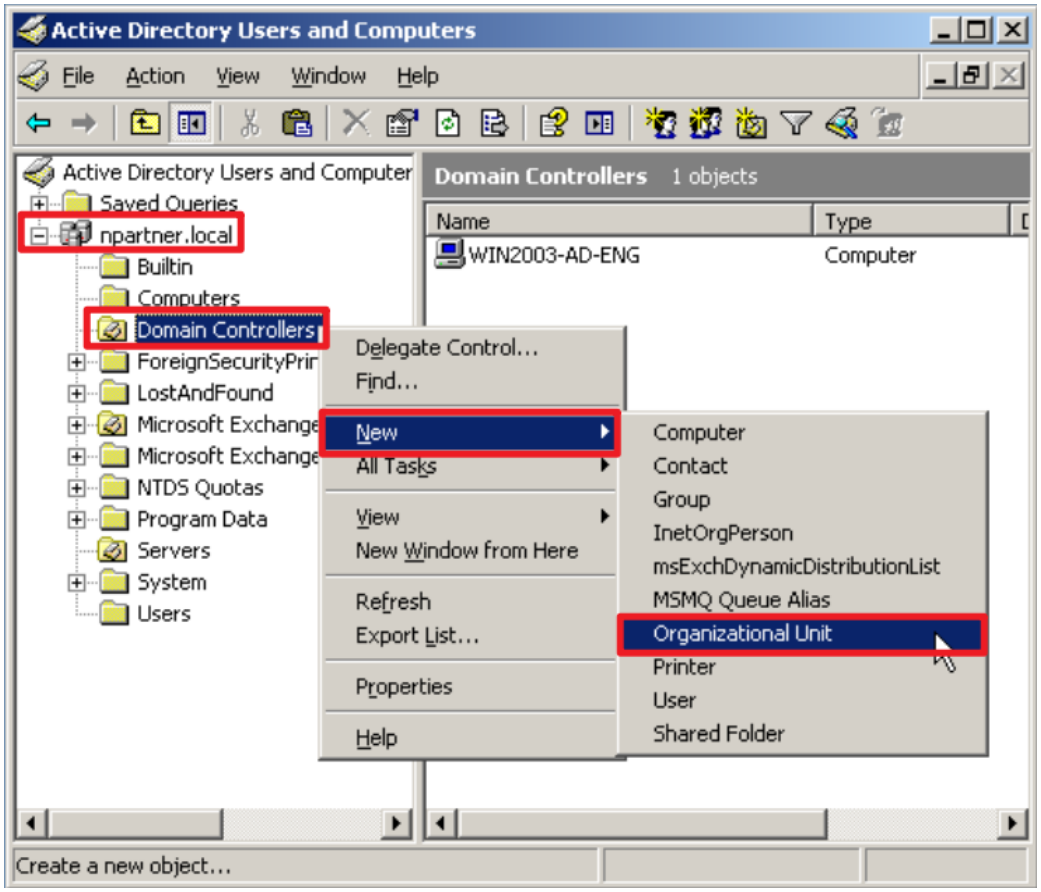
For detailed information, refer to the **Audit Policy Recommendations link** in the references.

3.1 Organizational Unit (OU) Configuration

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

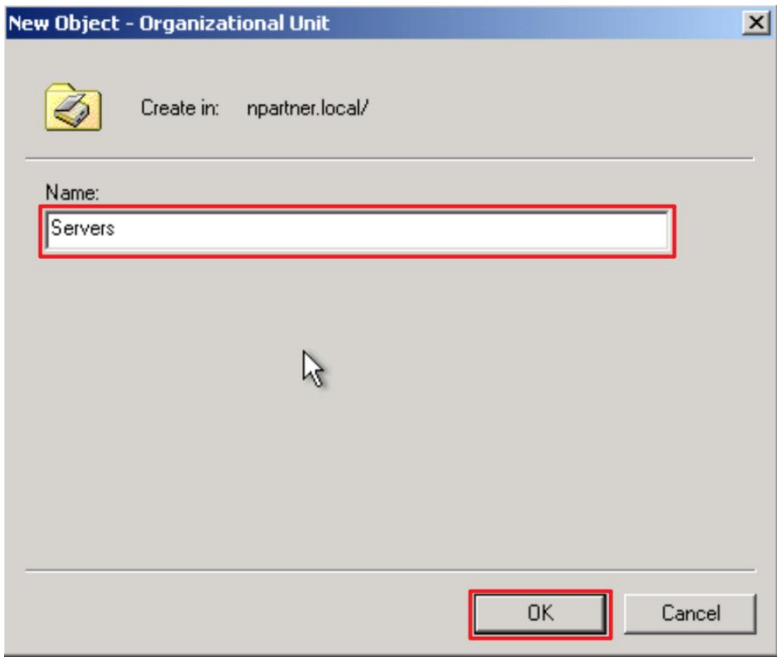
(2) Add an Organizational Unit

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



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

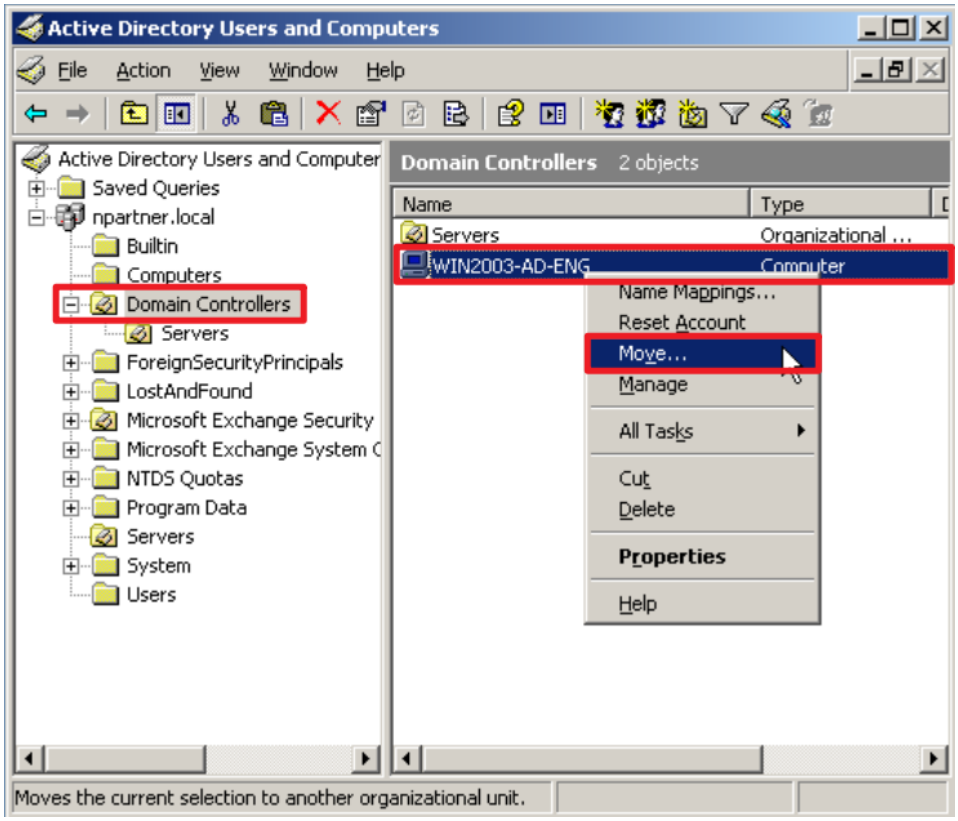
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

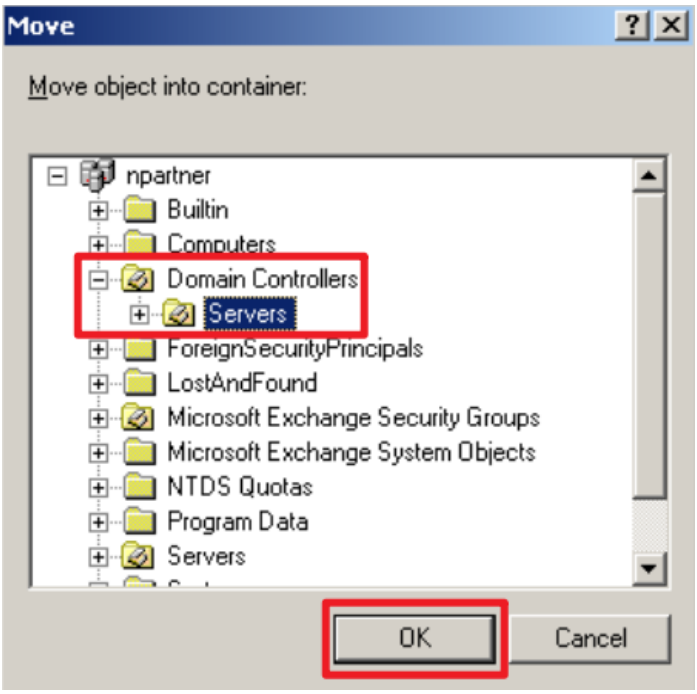
Select “Domain Controllers” → right-click on the “WIN2003-AD-ENG” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”



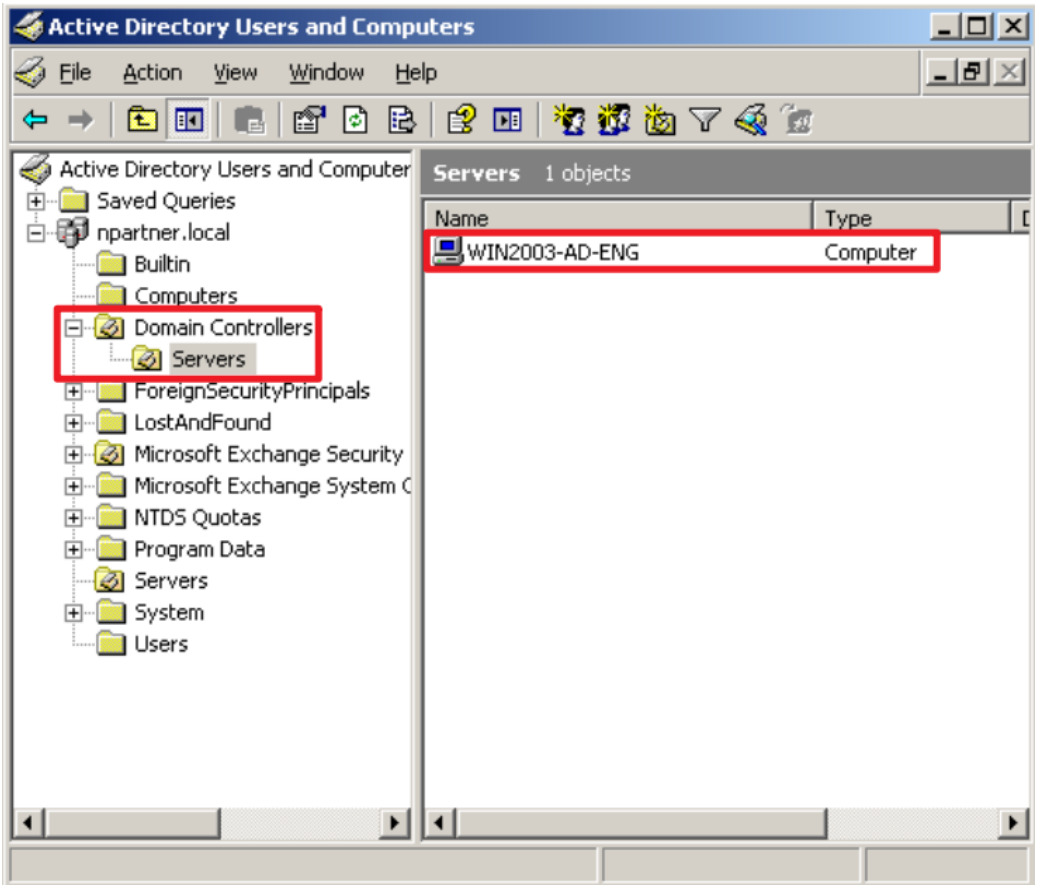
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → click “OK.”



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

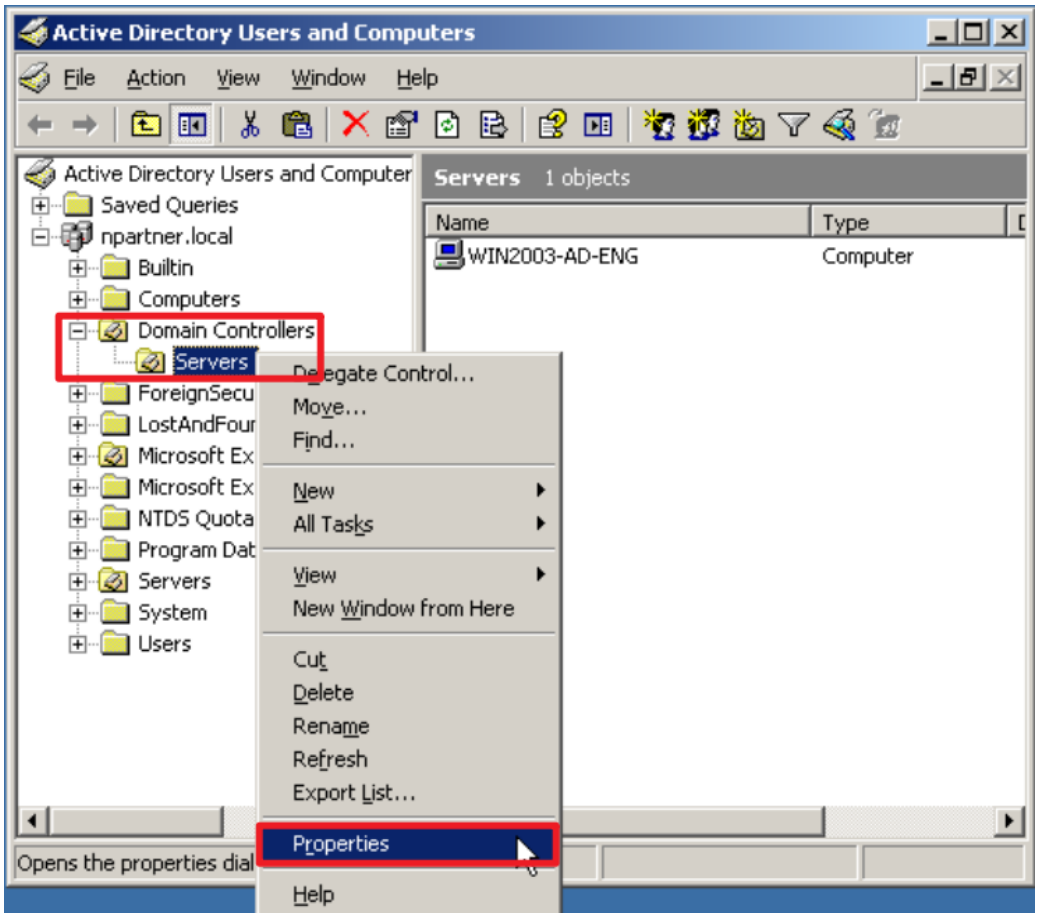
Expand “Domain Controllers” and select your OU folder (in this example, it is “Servers”) and confirm that the “WIN2003-AD-ENG” server has been moved.



3.2 Group Policy Settings

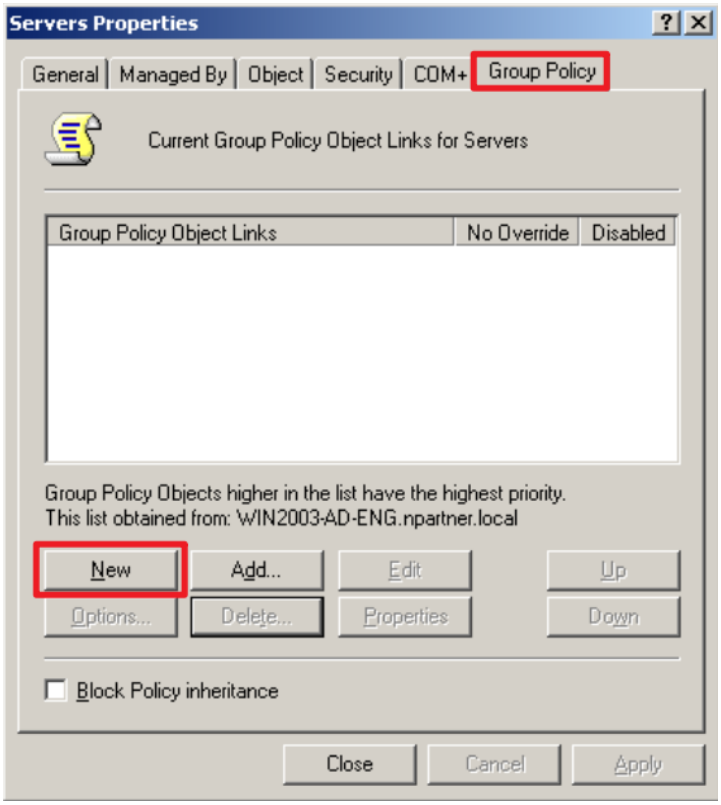
(1) Click “Active Directory Users and Computers.”

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



(3) Enter the Group Policy Object (GPO) name

On the “Group Policy” page → click “New.”

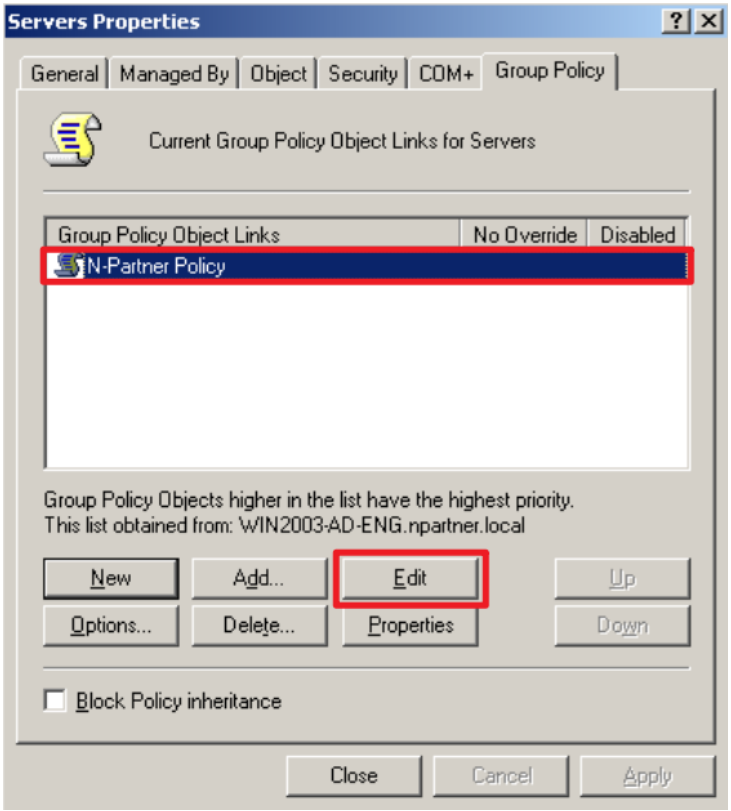


(4) Edit your Group Policy Object

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

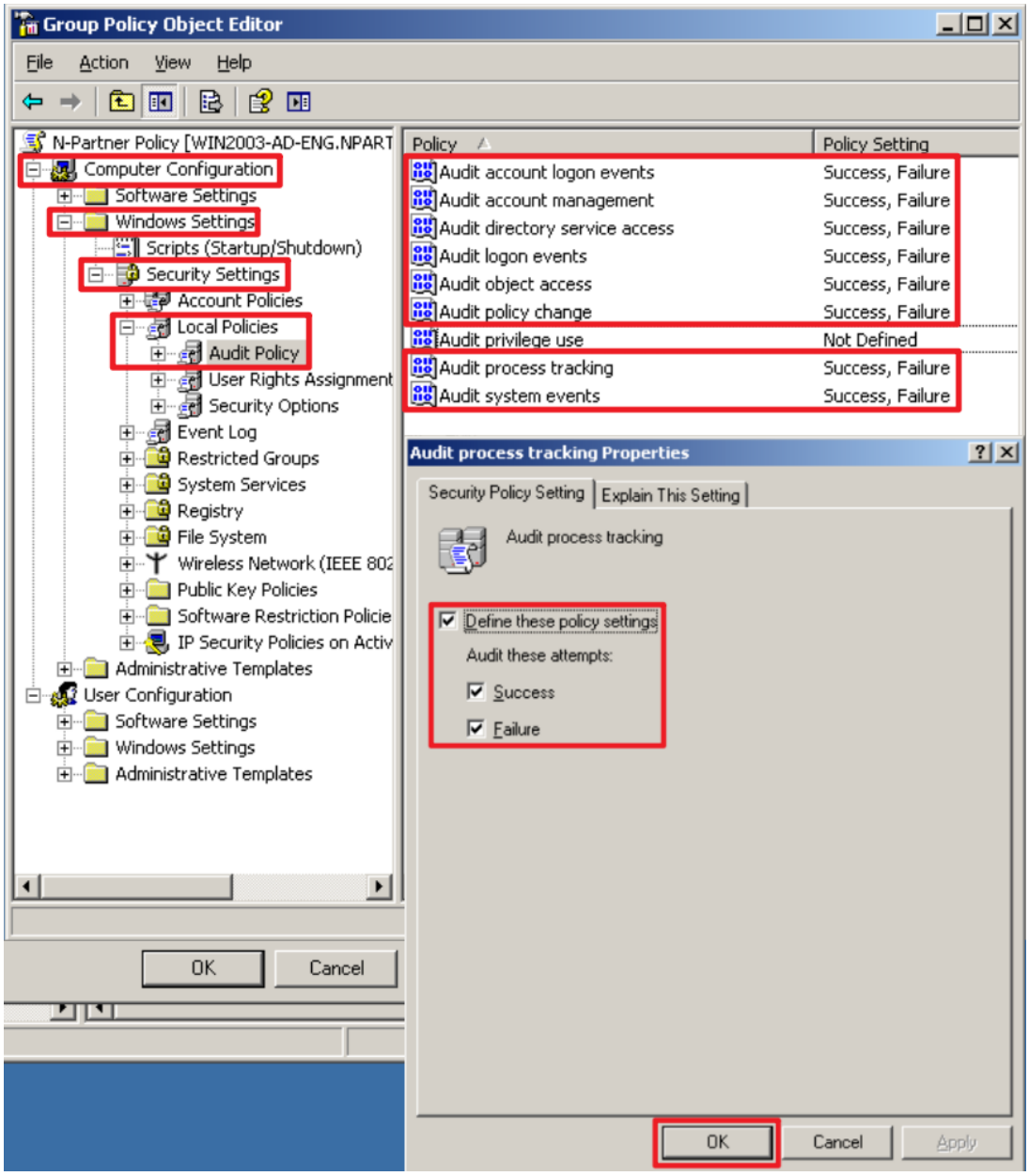
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



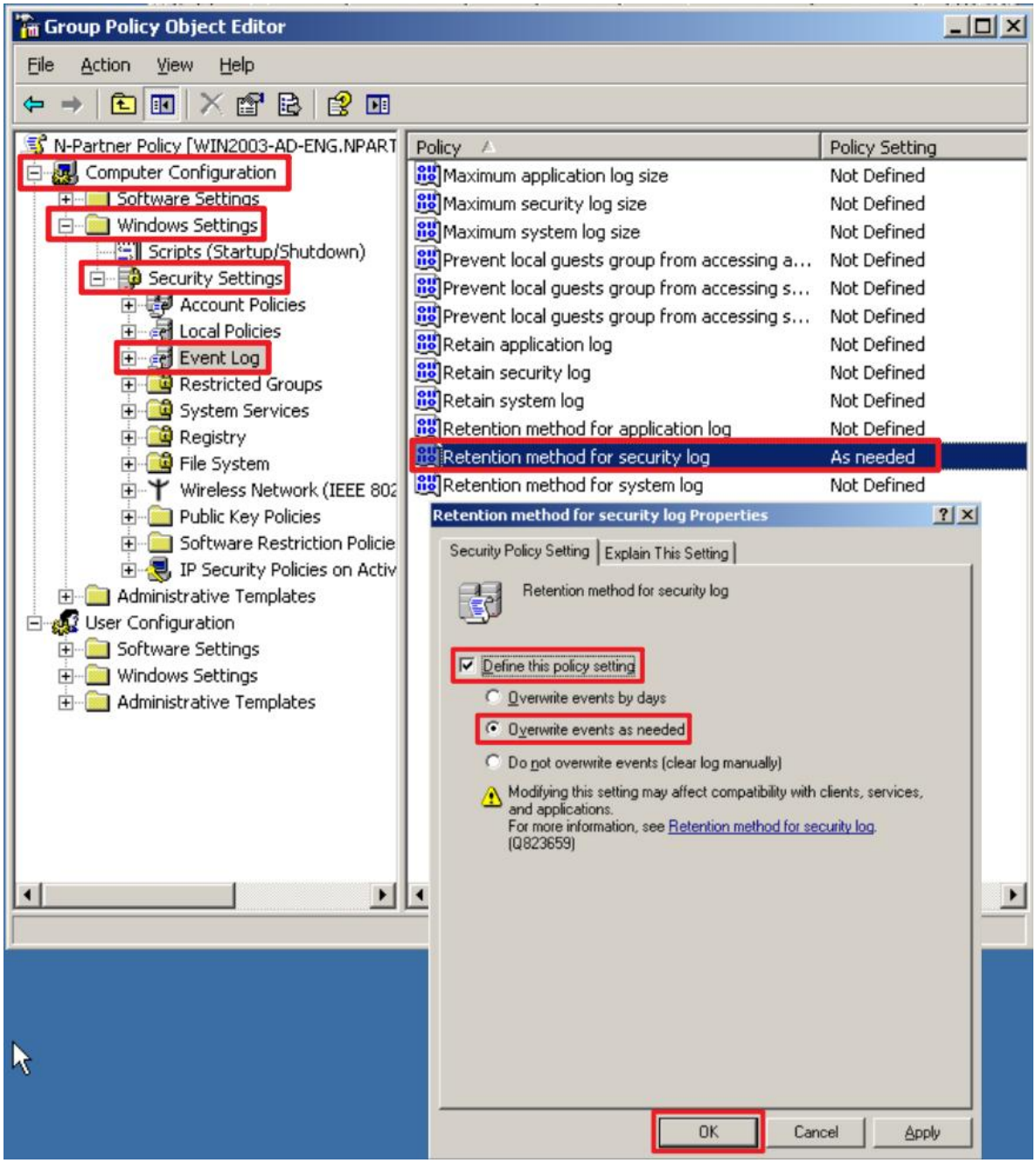
(5) Local Group Policies: Audit Policy

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” → check “Define these policy settings”: Success, Failure. → click “OK.”



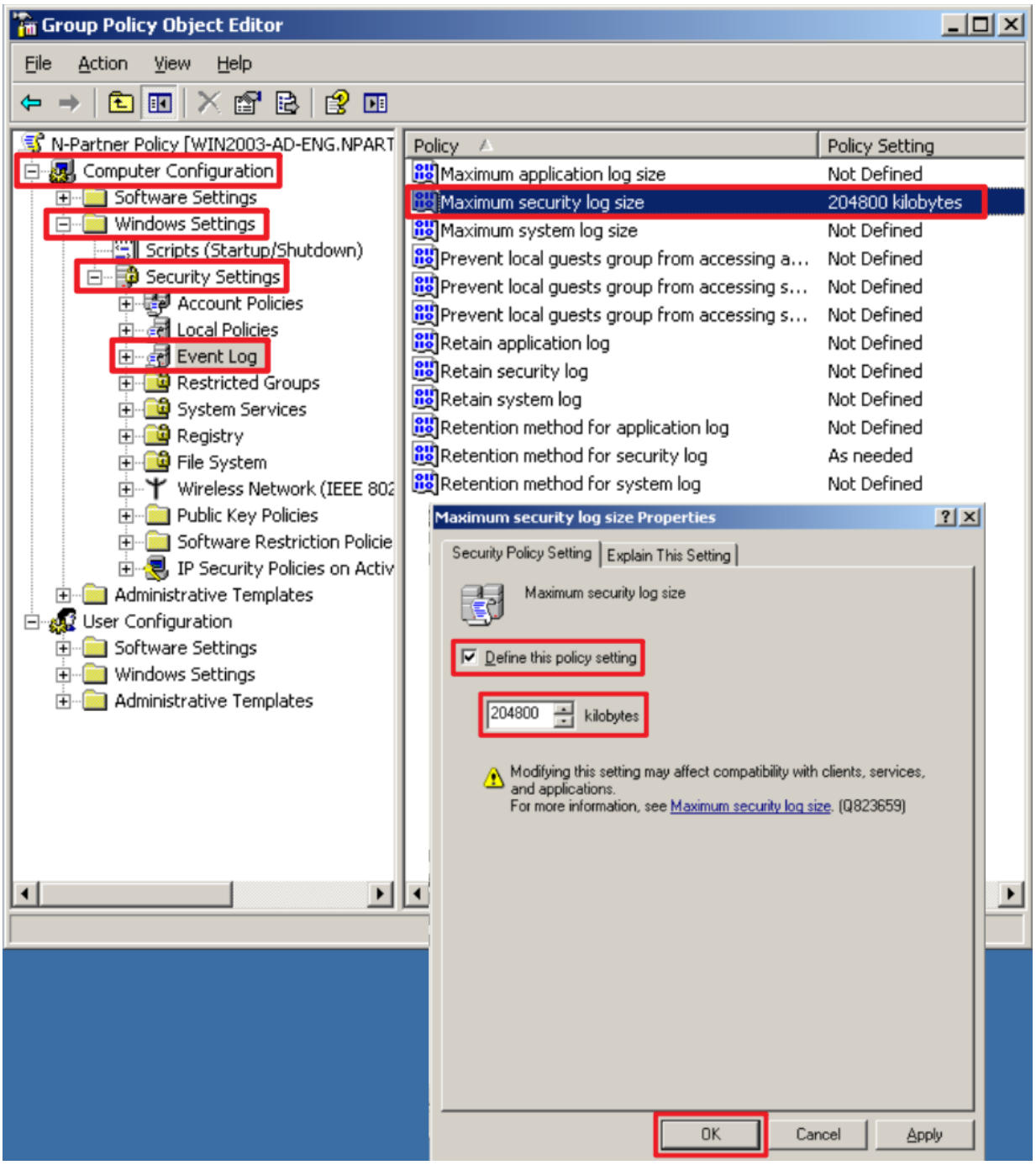
(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

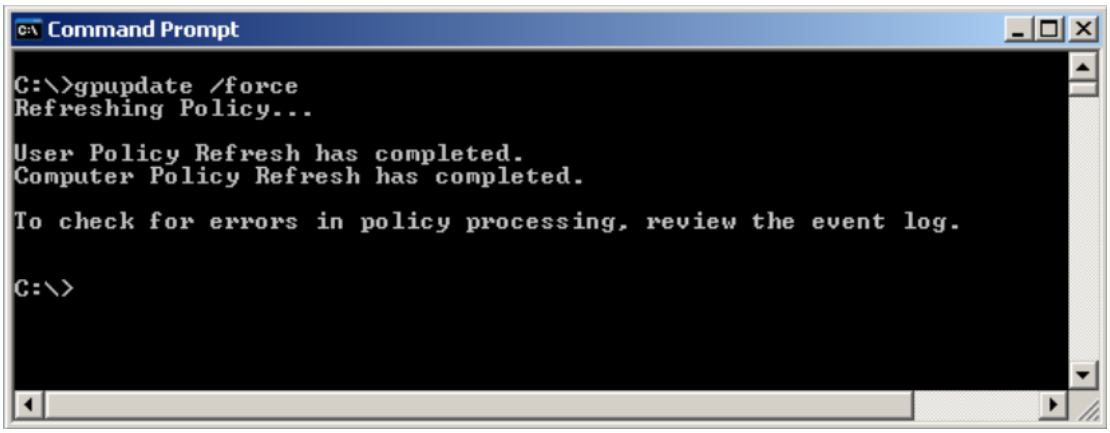
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → and click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB Note: Please adjust the number based on the actual environment. → click “OK.”



(8) On the Windows File server, open “Command Prompt.”

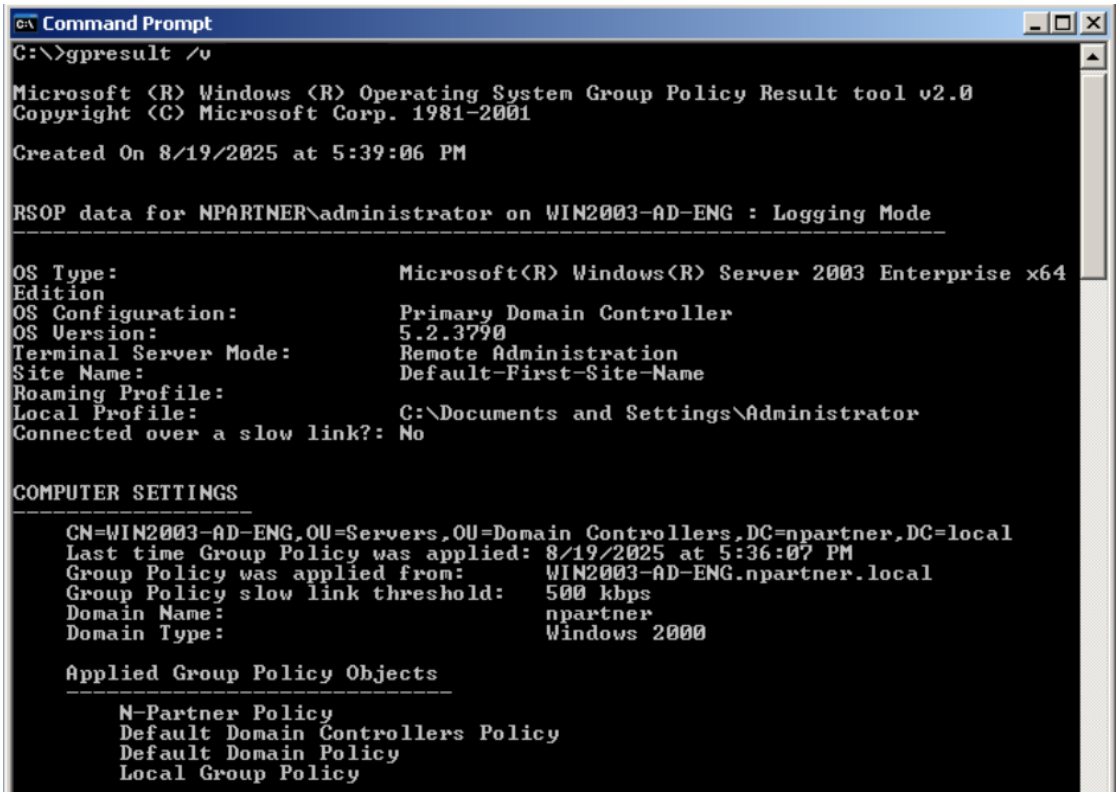
(9) Enter the command below to refresh group policy.

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



(10) Enter the command below to verify the applied group policy settings.

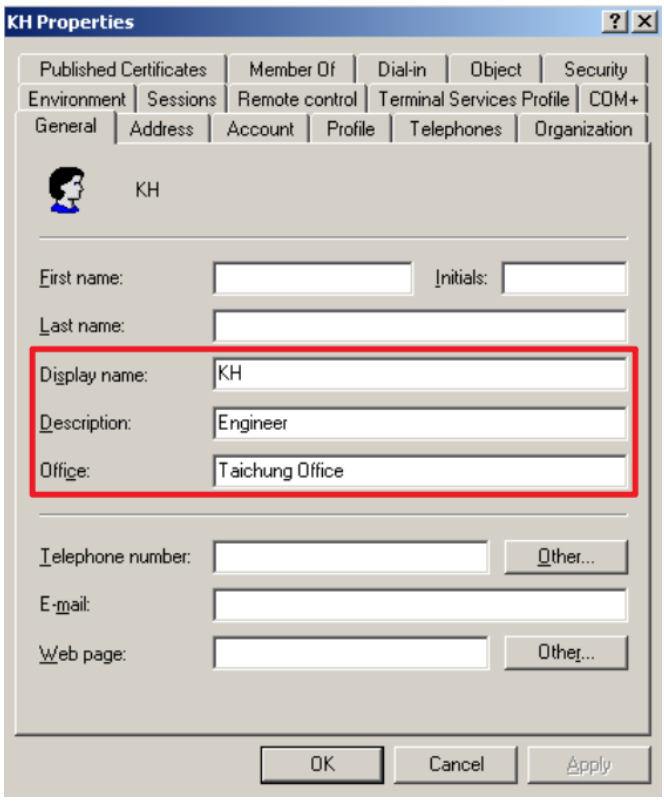
```
C:\> gpresult /v
```

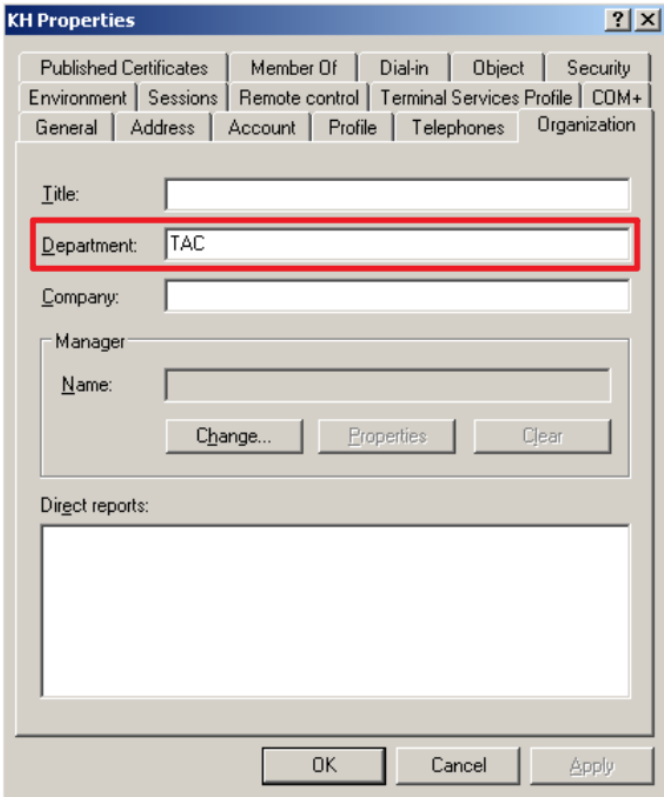


3.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Check whether N-Reporter associates Windows AD with available user data.





(2) In “Event Query,” click the information of “Username.”

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

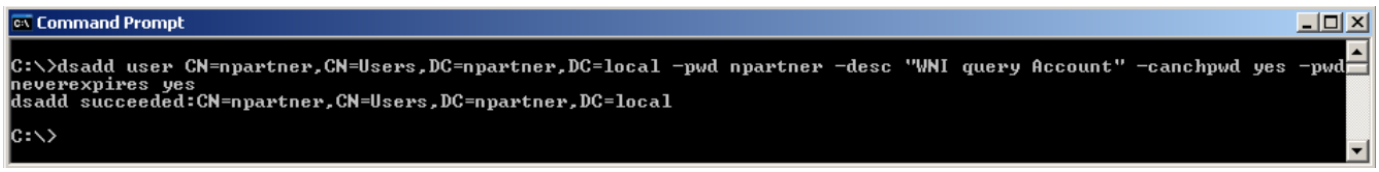
3.3.1 Add Non-Admin Accounts

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

(2) Create an Account

Enter the command below to create an account:

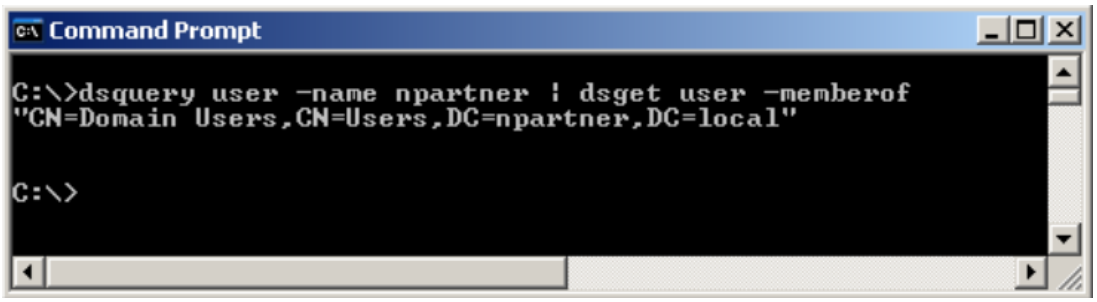
```
C:\> dsadd user CN=npartner,CN=Users,DC=npartner,DC=local -pwd npartner -desc "WMI query
Account" - canchpwd yes -pwdneverexpires yes
```



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

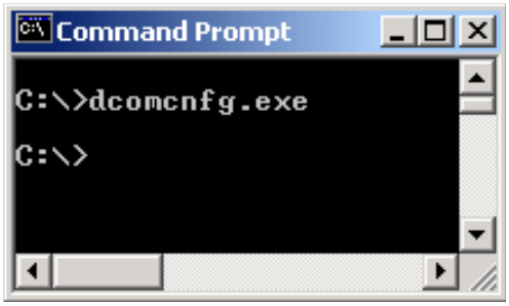


3.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”

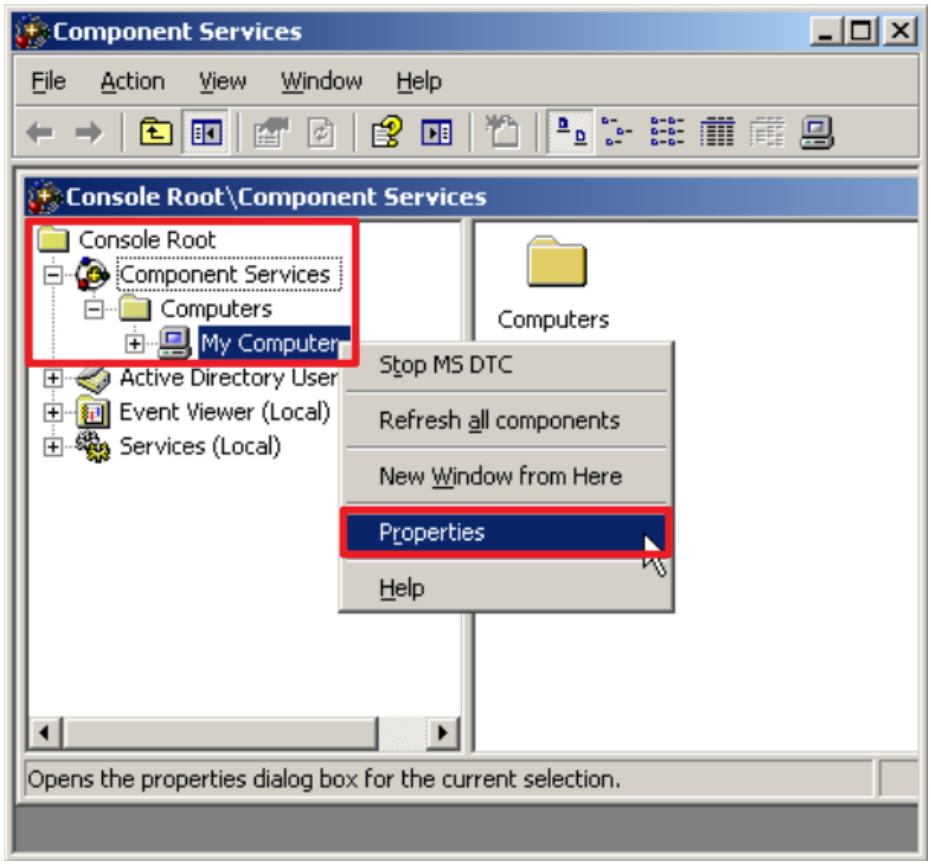
(2) Enter the command below to enable component services.

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



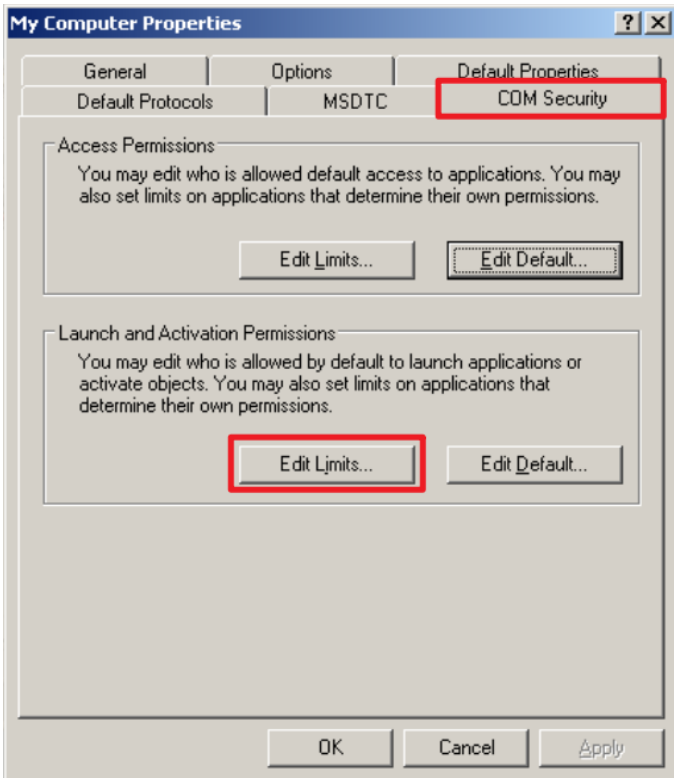
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



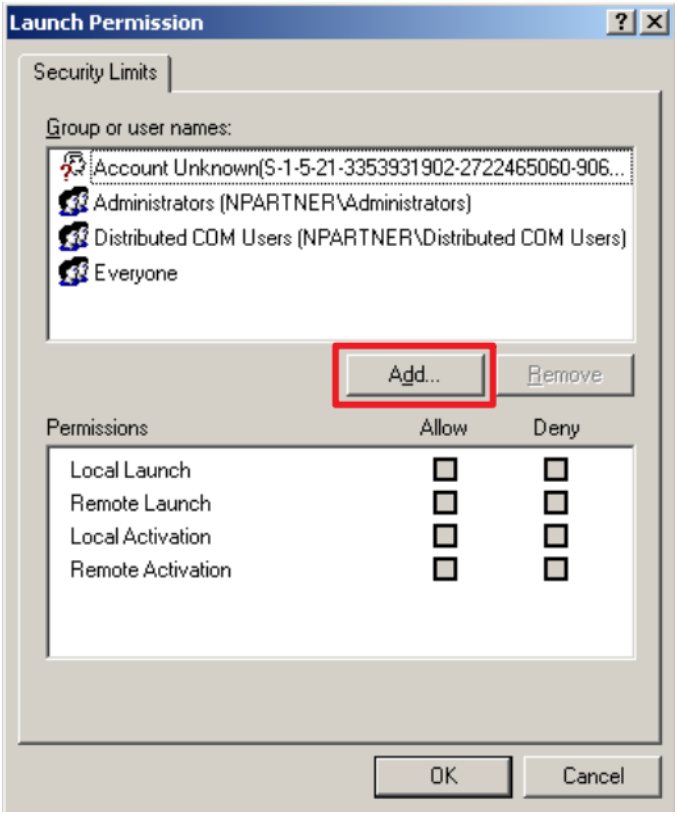
(4) Enable Permissions

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



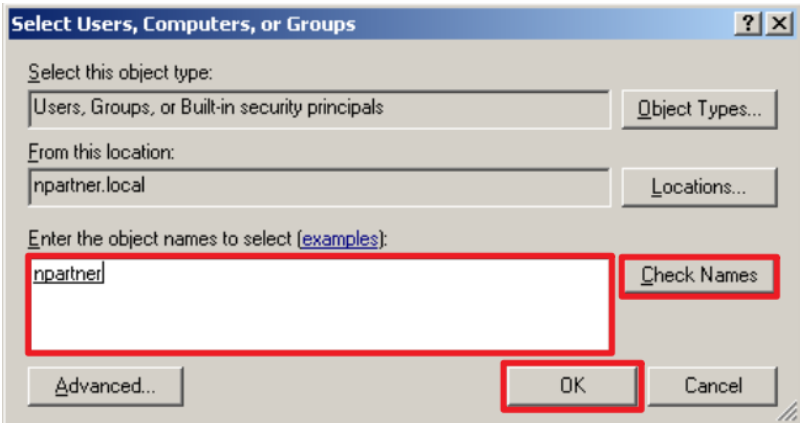
(5) Add DCOM User Permissions

Click “Add.”



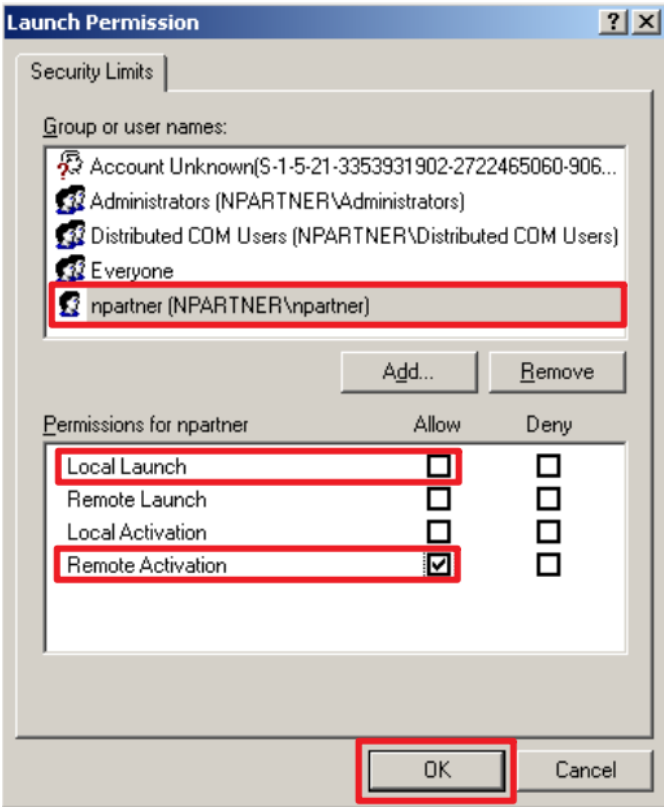
(6) Enter Your Username

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

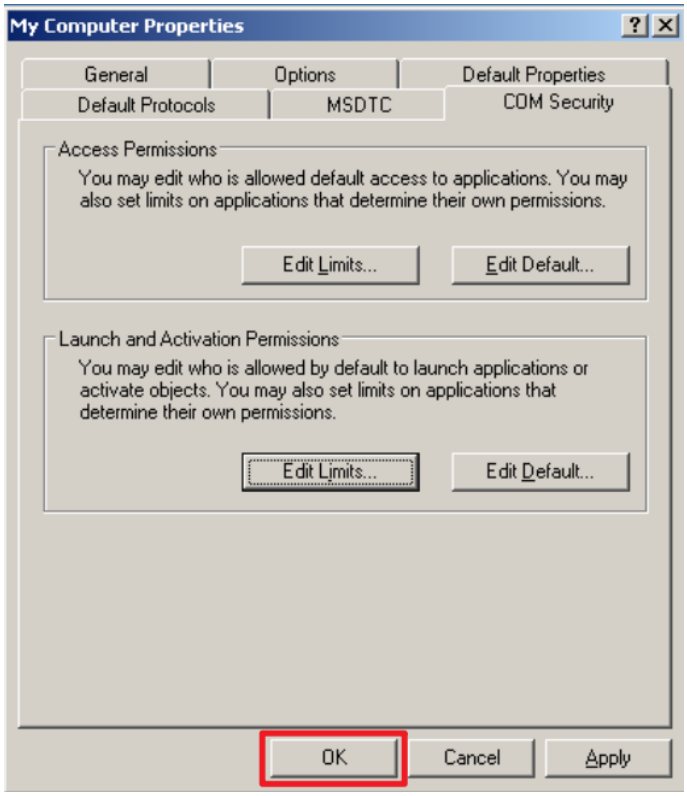


(7) Configure User Permissions

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



(8) Click "OK.”



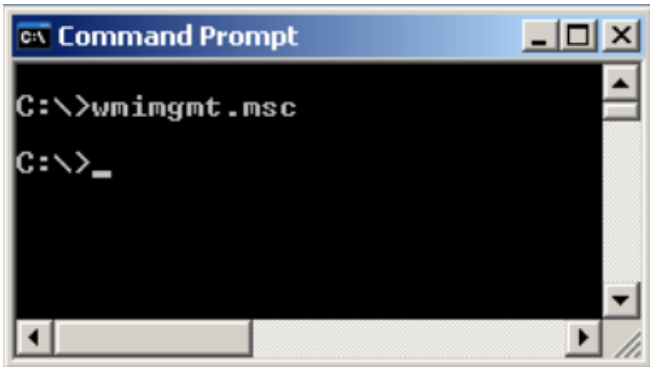
3.3.3 Configure WMI Permissions

3.3.3.1 Configure Event Log Permissions

(1) Open “Command Prompt.”

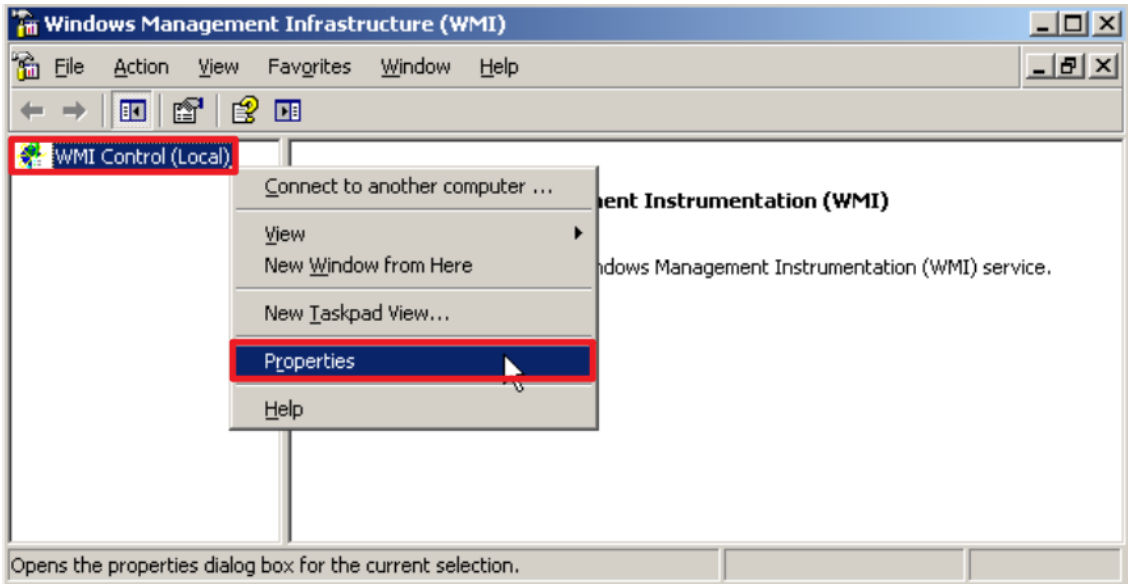
(2) Enter the command to enable WMI control service.

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



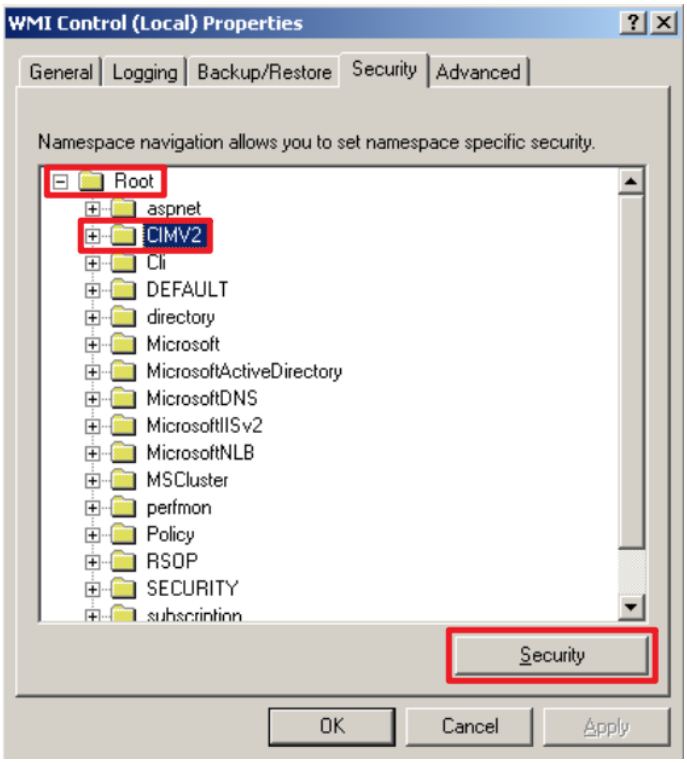
(3) Edit WMI Control

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



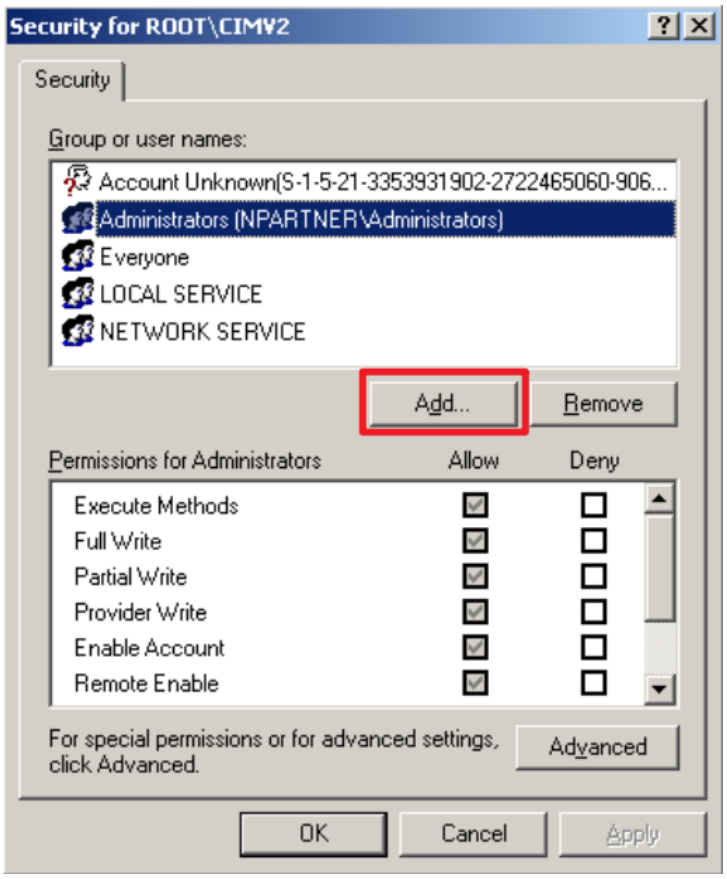
(4) Edit CIMV2 Security

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



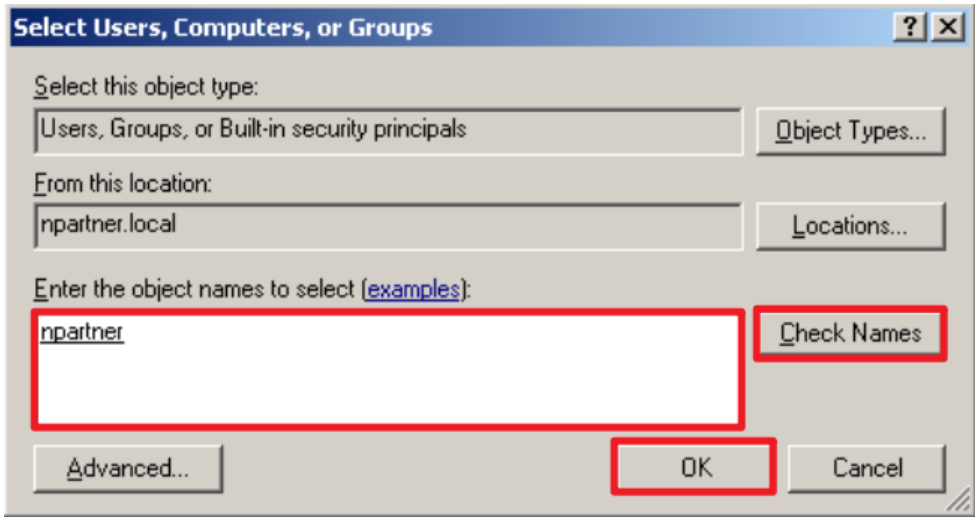
(5) Add WMI User Permissions.

Click “Add.”



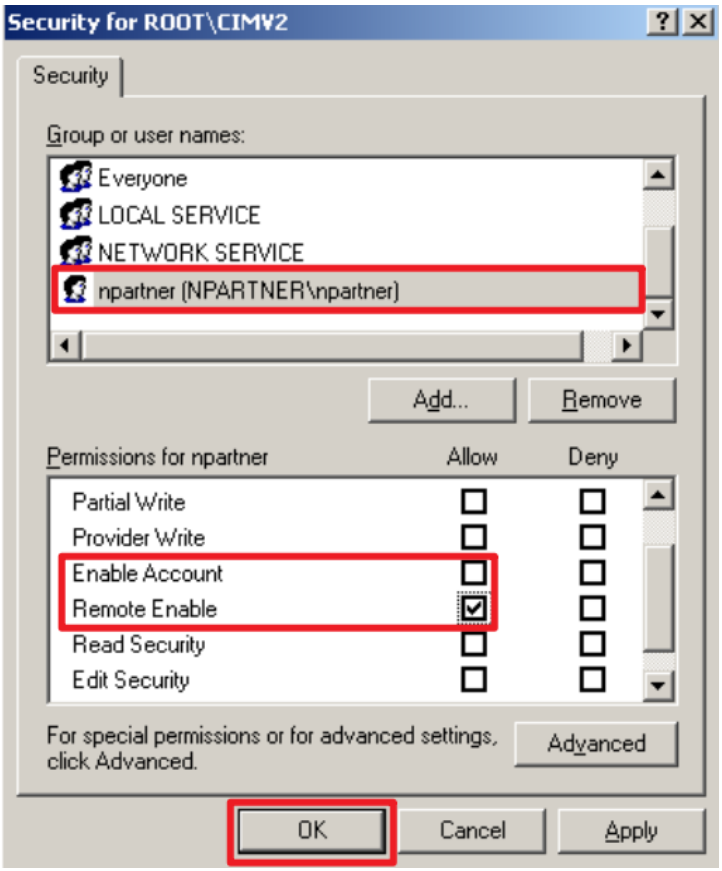
(6) Enter Your Username

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

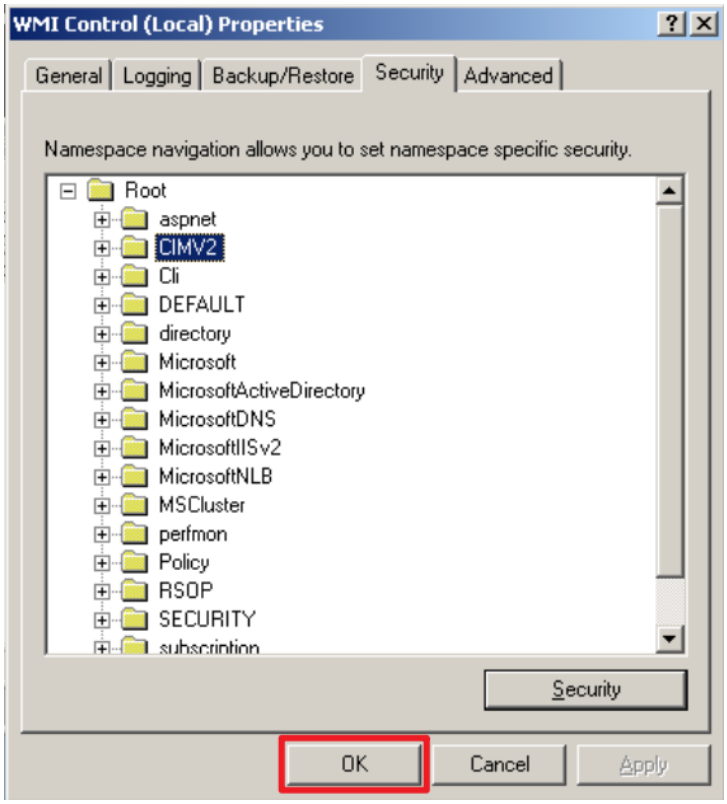


(7) Set Your User Permissions

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



(8) Click “OK.”

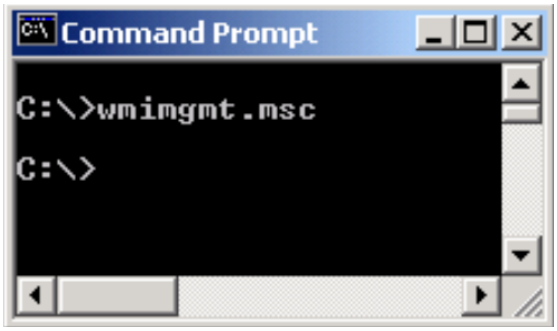


3.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”

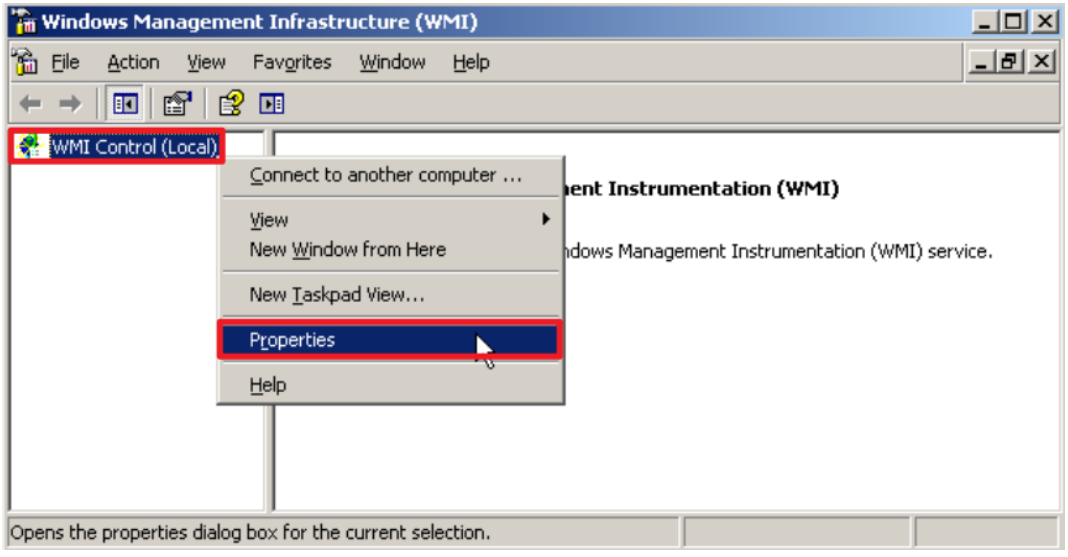
(2) Enter the command below to enable WMI Control.

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



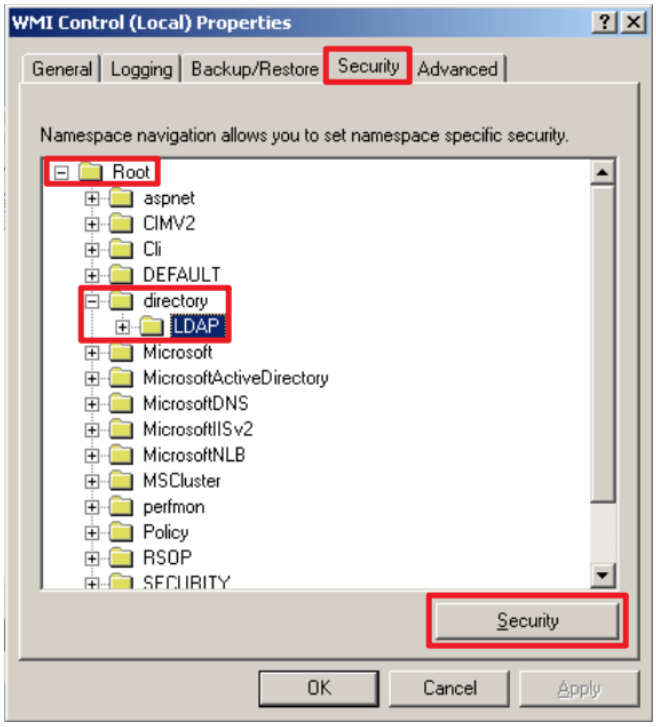
(3) Edit WMI Control

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



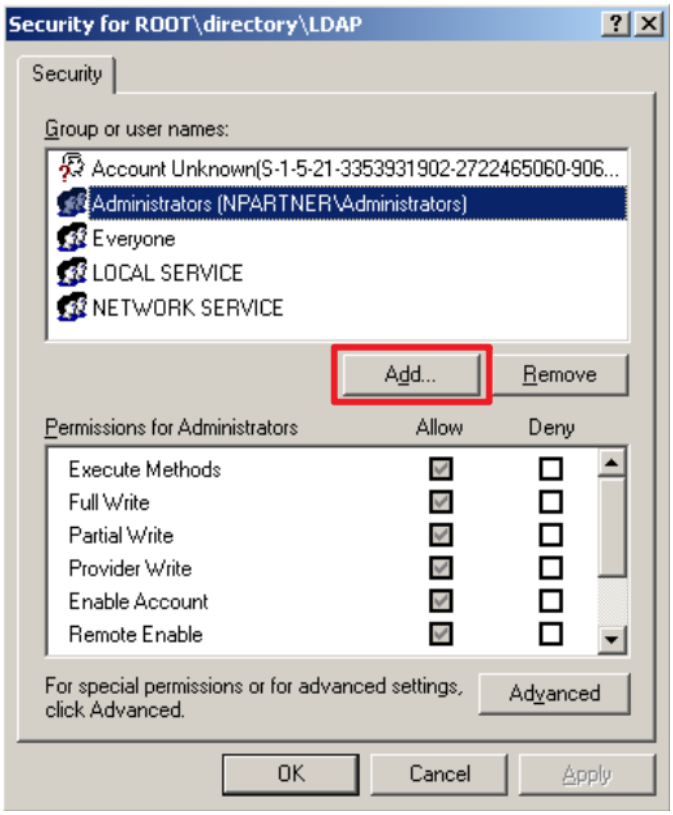
(4) Edit LDAP Security

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



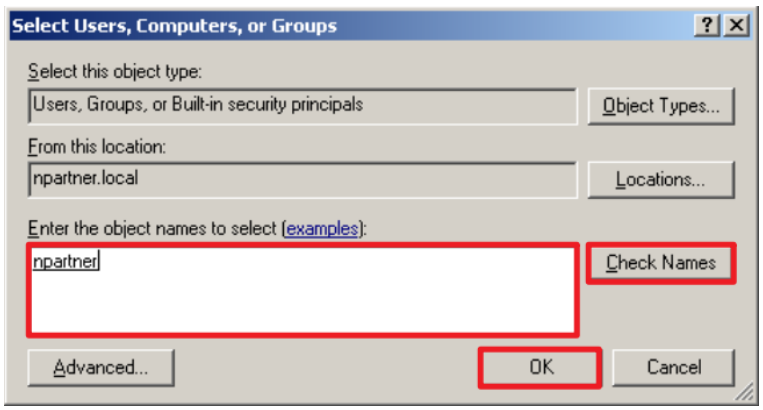
(5) Add WMI User Permissions

Click “Add.”



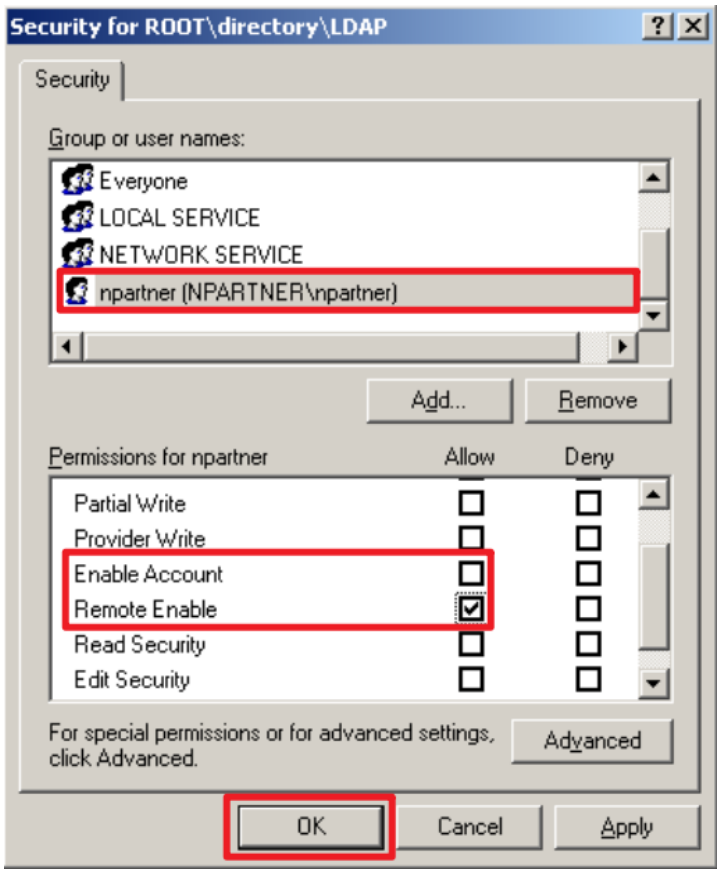
(6) Enter Your Username

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

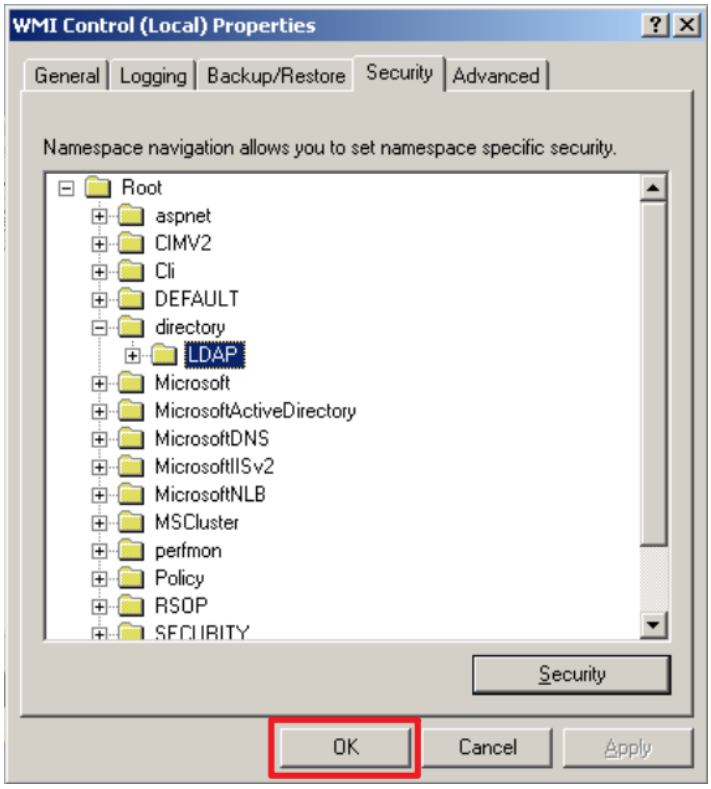


(7) Set Your User Permissions

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



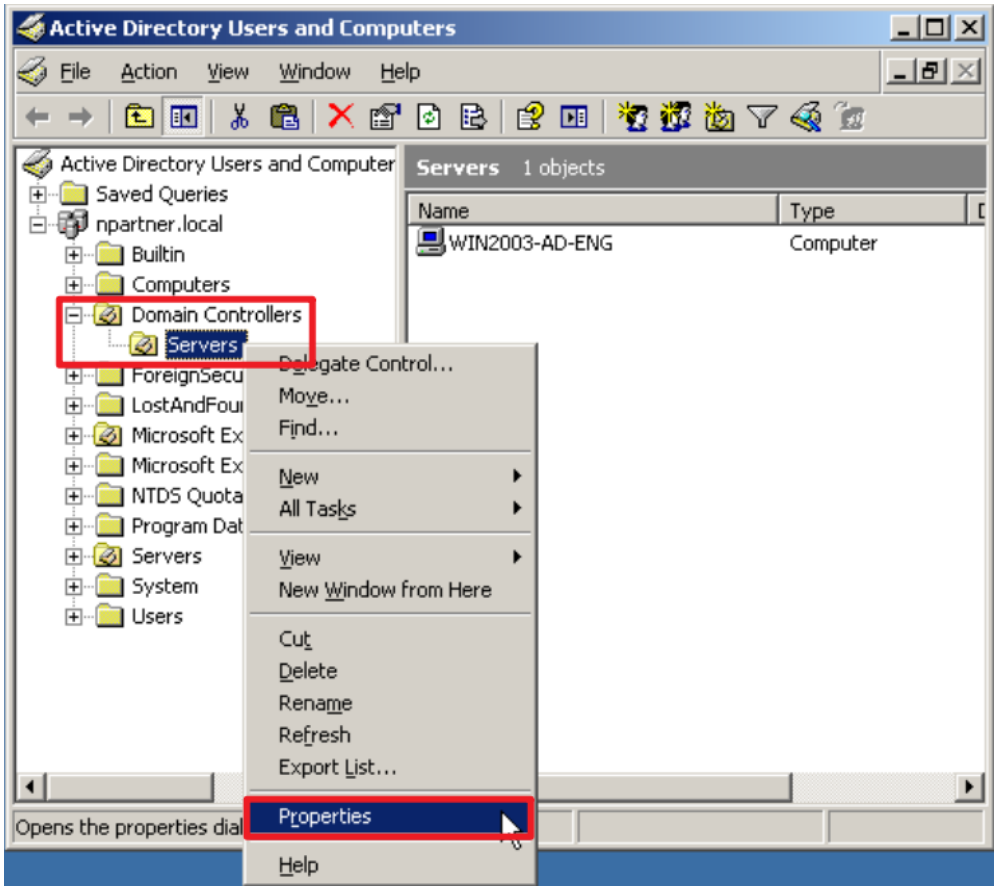
(8) Click “OK.”



3.3.4 Configure Event Log Read Permissions

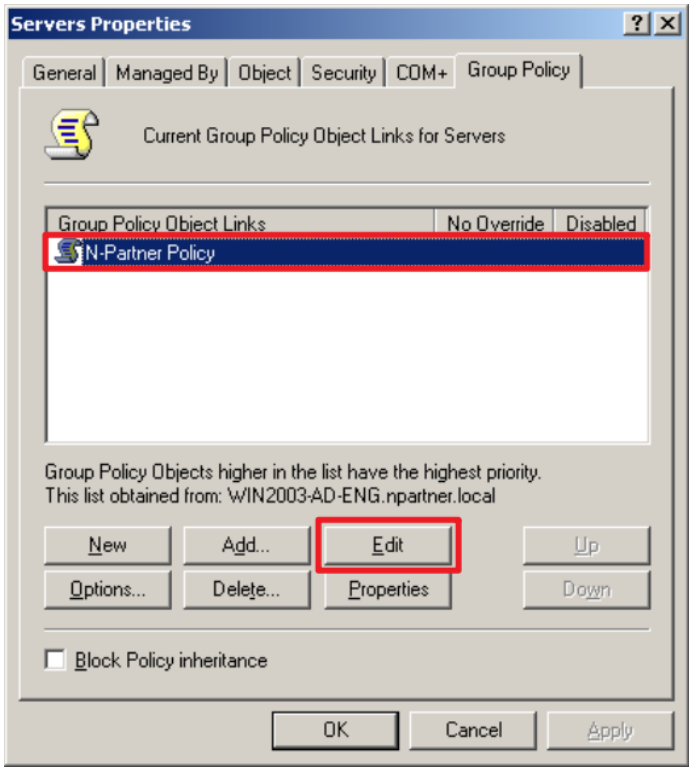
(1) Click “Active Directory Users and Computers.”

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



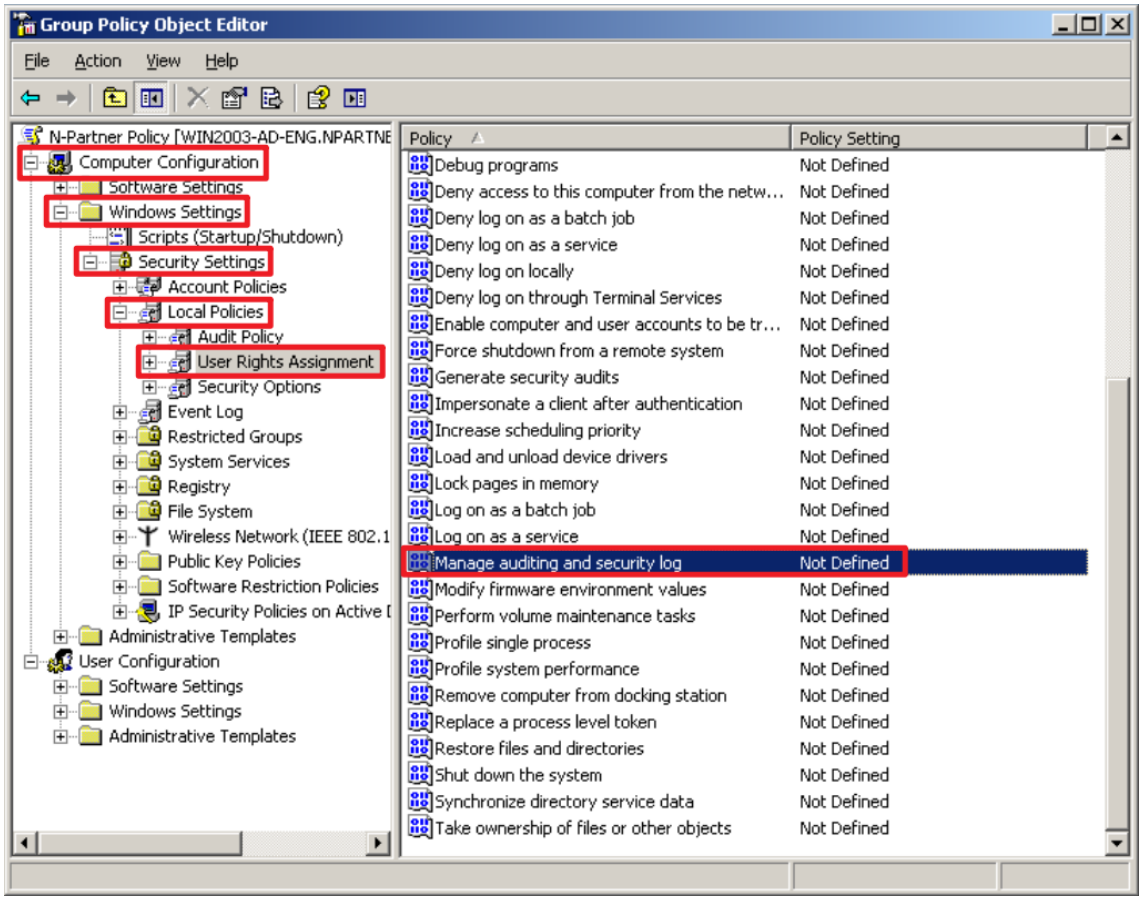
(3) Edit Group Policy Object

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



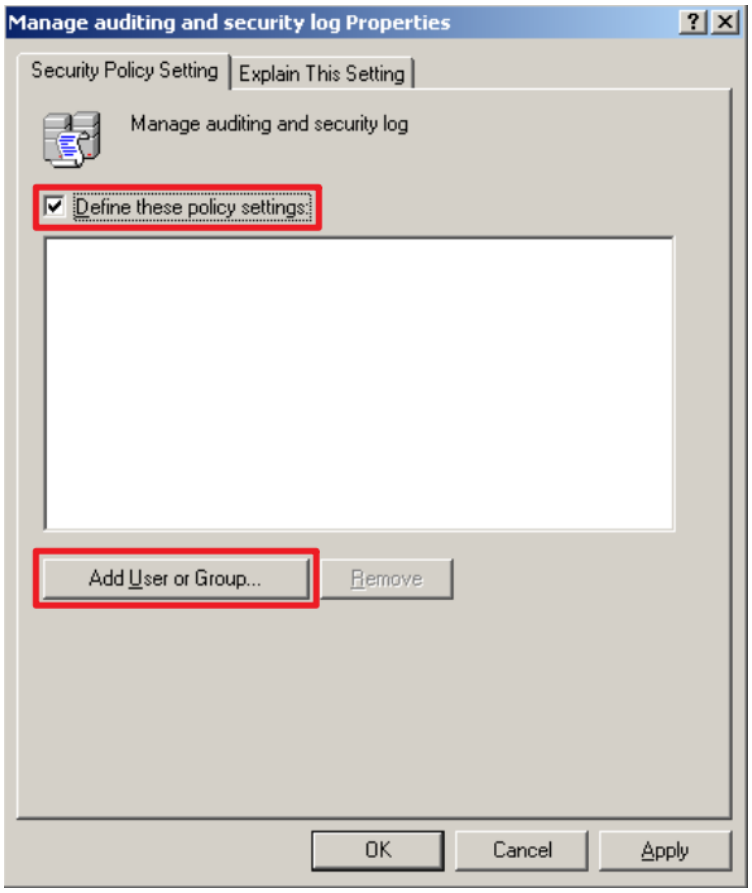
(4) Configure Audit Logs

Expand "Computer Configuration" → "Windows Settings" → "Security Settings" → "Local Policies" → "User Rights Assignment," then select "Manage Auditing and Security Log."



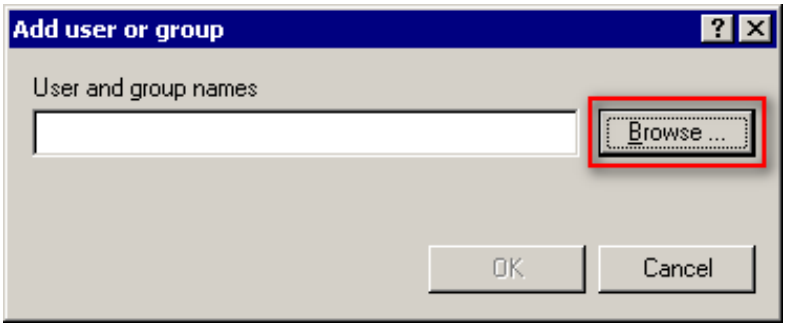
(5) Add Auditing User

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



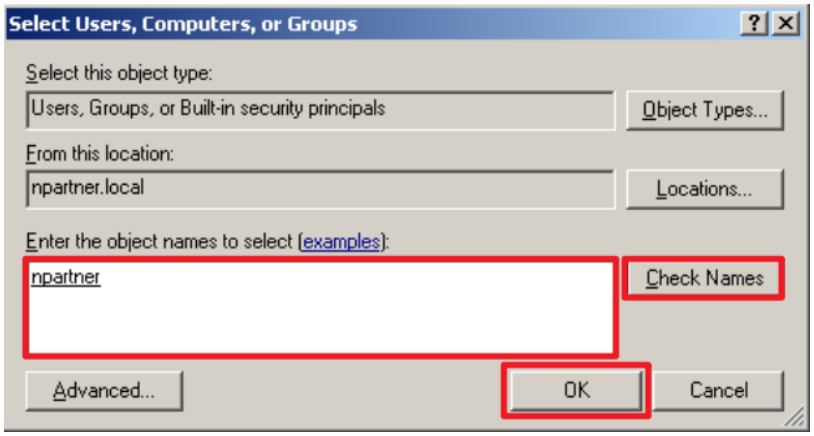
(6) Search for User

Click “Browse.”

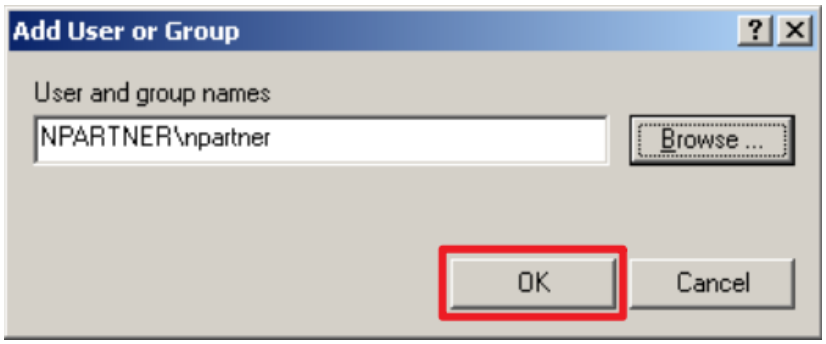


(7) Enter Your User Account

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

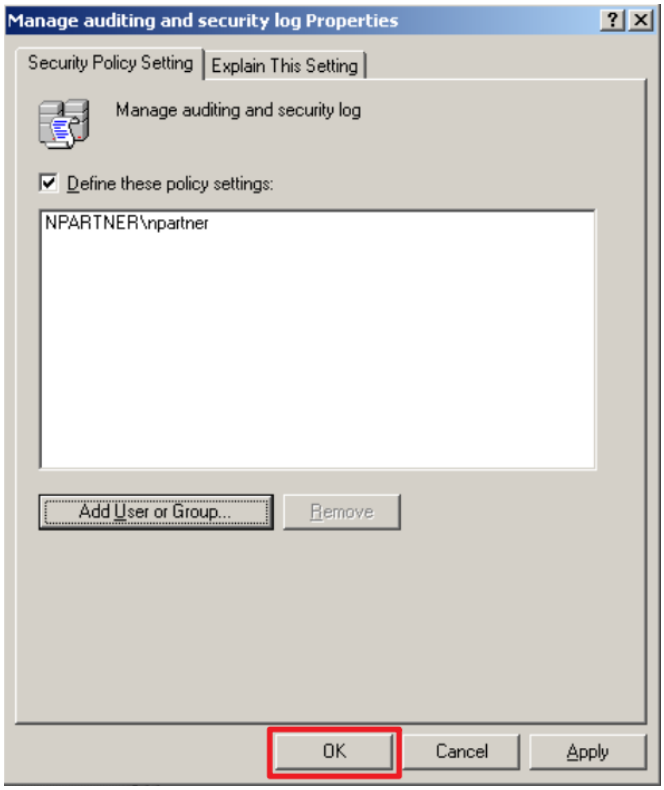


(8) Click “OK.”



(9) Confirm Audit Log Settings

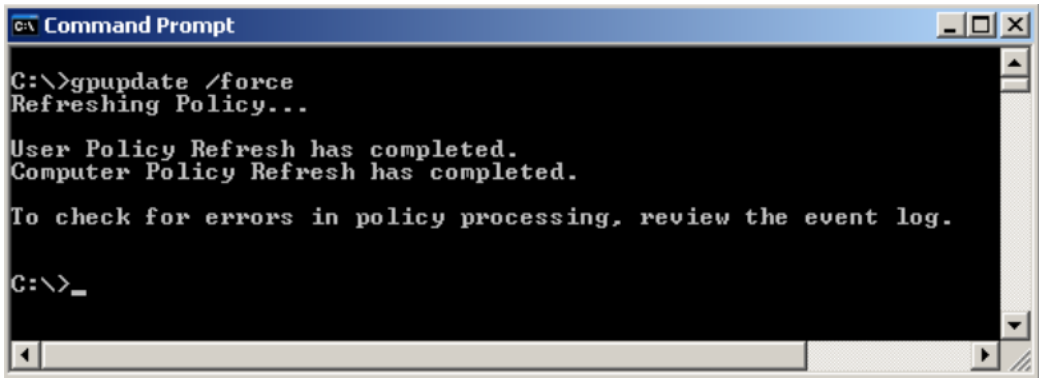
Click “OK.”



(10) Open “Command Prompt.”

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

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

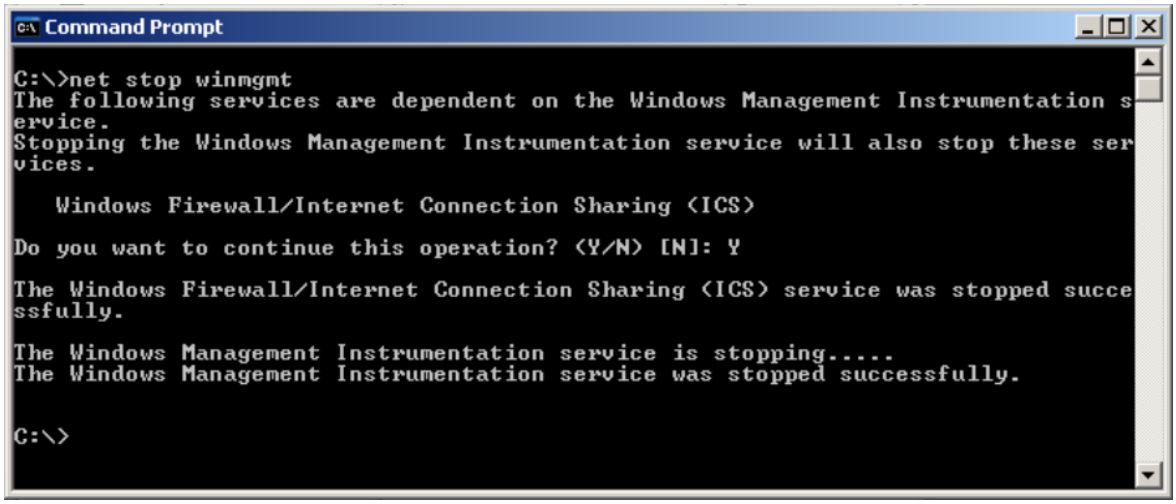


3.3.5 Restart the WMI Service

(1) Open “Command Prompt.”

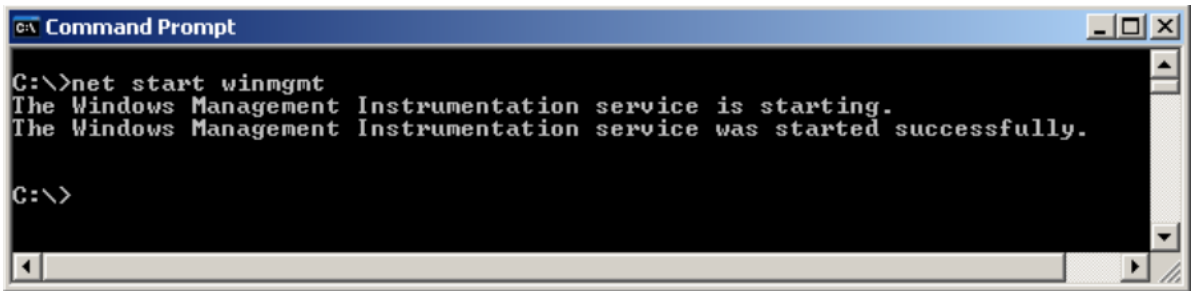
(2) Enter the command below to disable the WMI service.

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



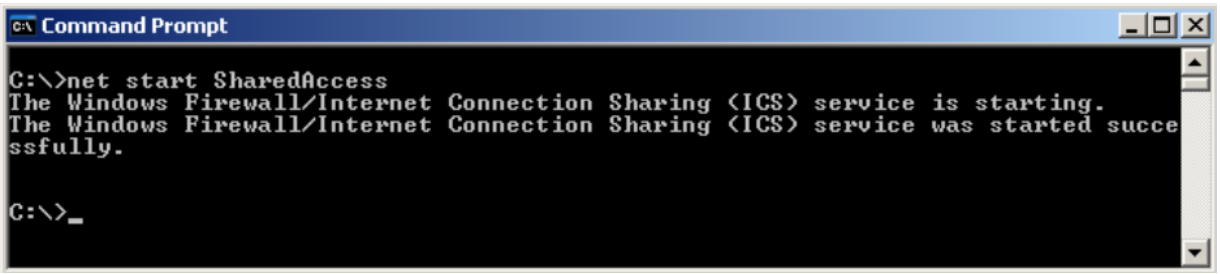
(3) Enter the command below to enable the WMI service.

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



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

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

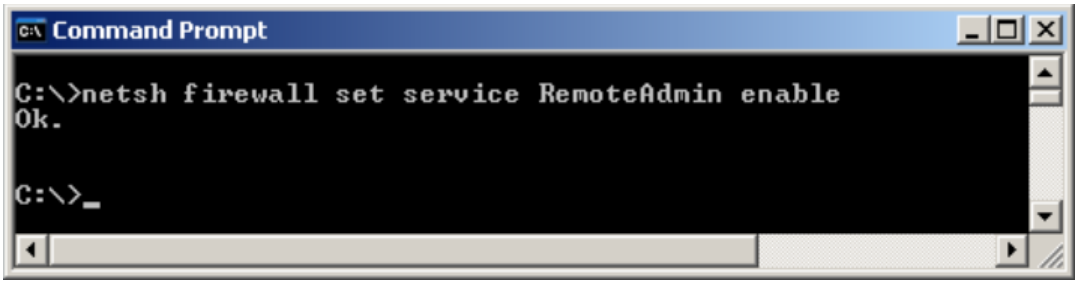


3.3.6 Configure the Firewall

(1) Open “Command Prompt.”

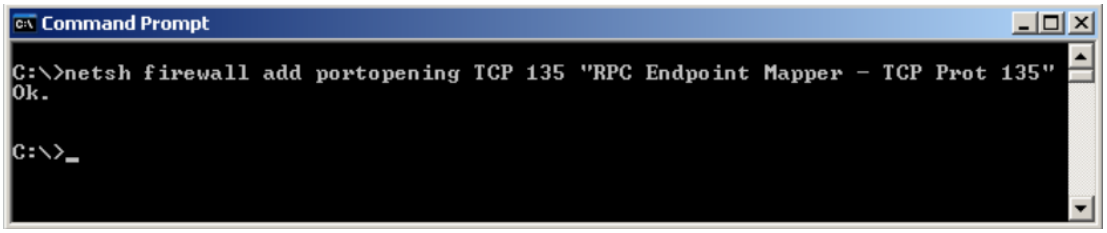
(2) Enter the command below to allow WMI through the firewall:

```
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 display the current firewall configuration:

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

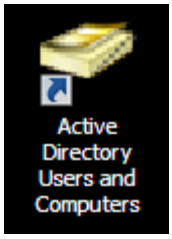
4. Windows Server 2008

Windows Audit Policy Configuration:

For detailed information, refer to the **Audit Policy Recommendations link** in the references.

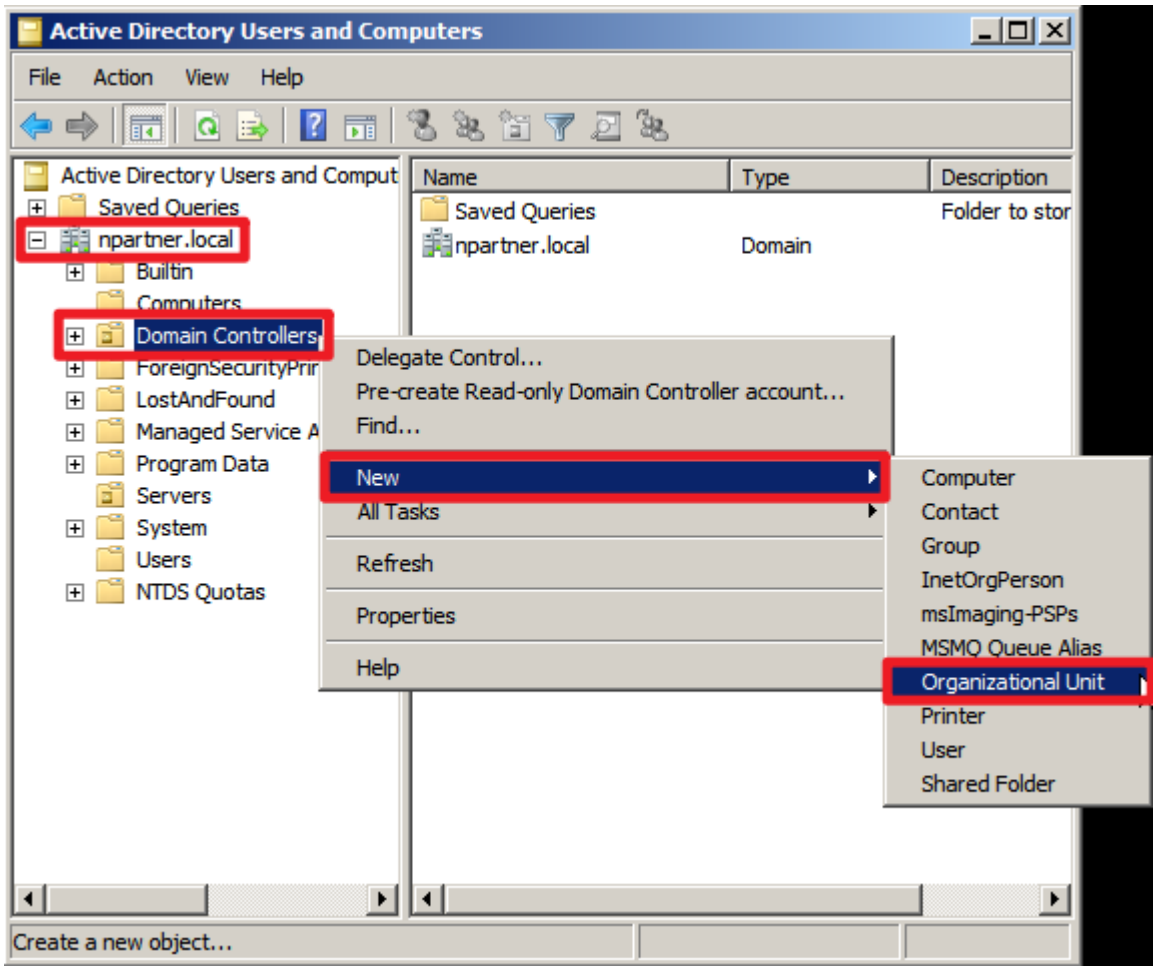
4.1 Organizational Unit (OU) Configuration

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



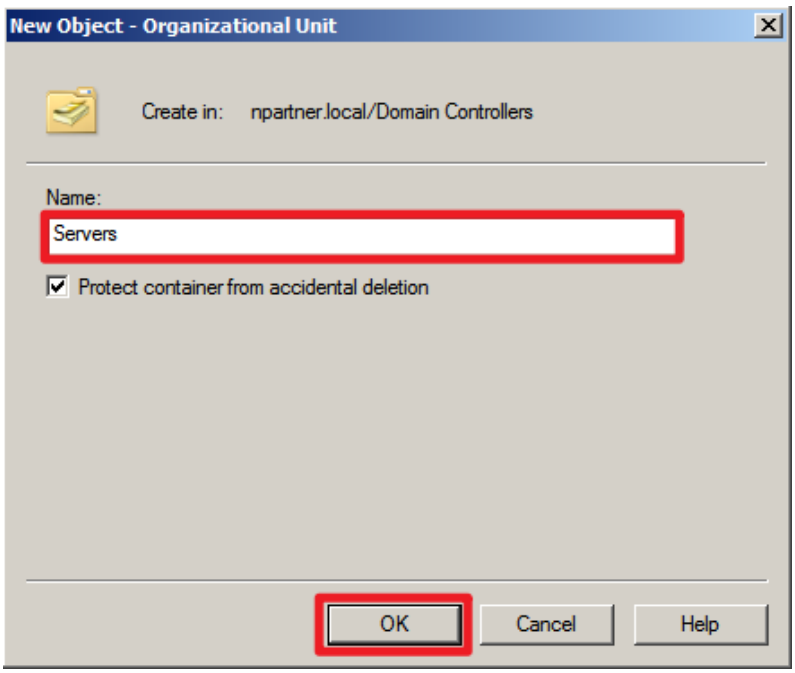
(2) Add an Organizational Unit

Right-click the “Domain Controllers” organizational unit under “Domain Name” (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



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

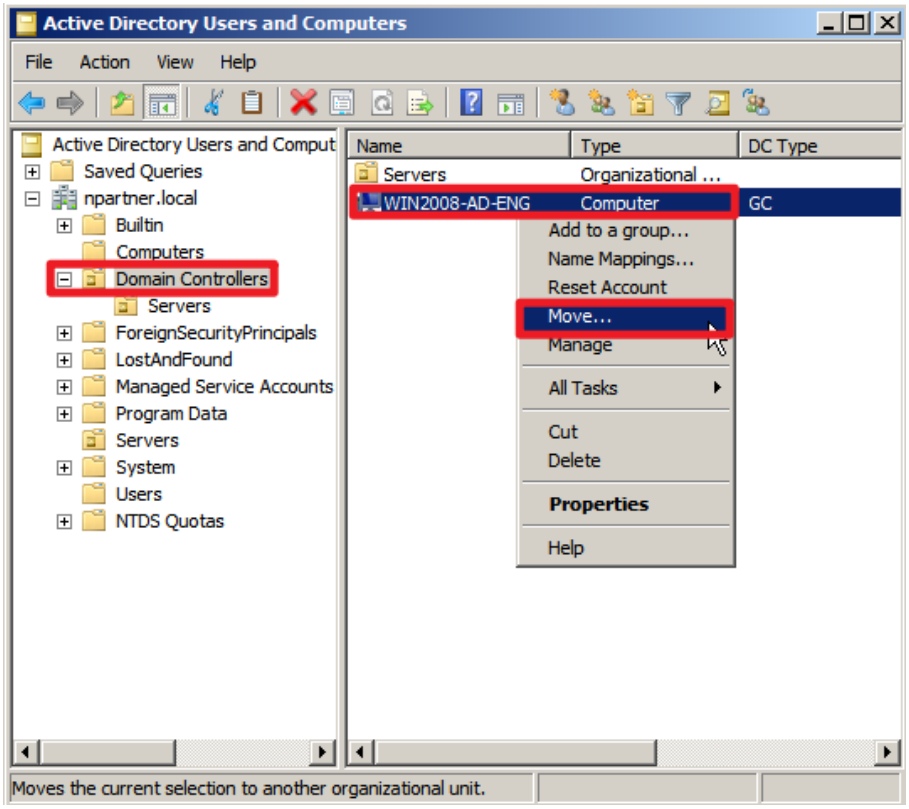
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

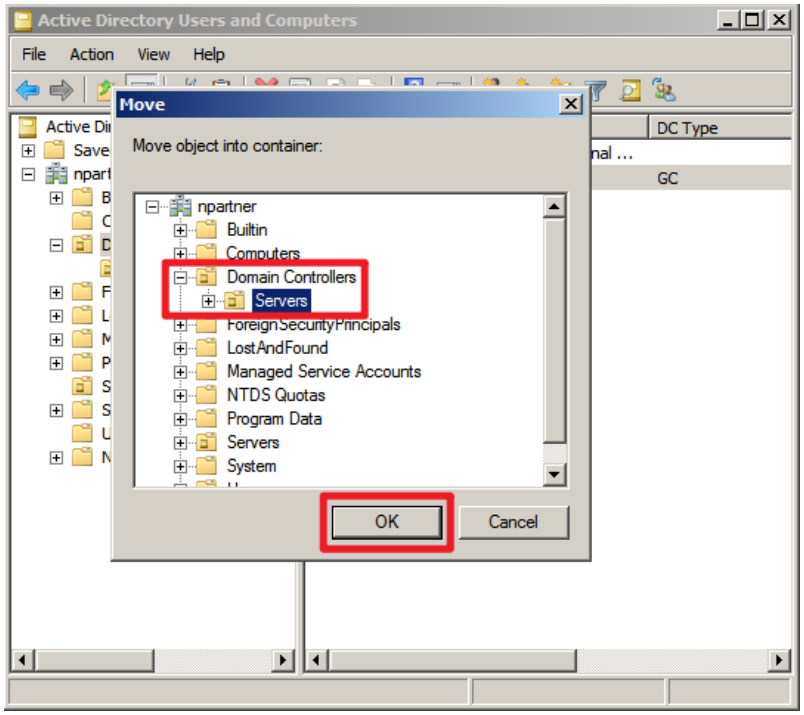
Select the “Domain Controllers” organizational unit (OU) → right-click on the “WIN2008-AD-ENG” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”



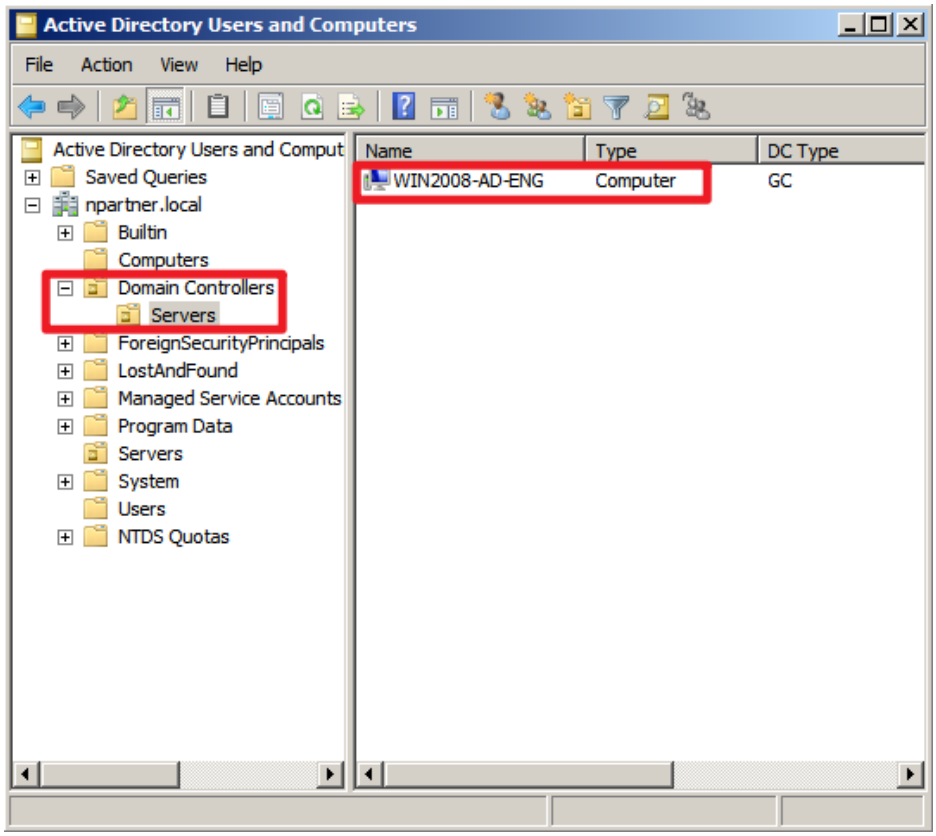
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) from the “Domain Controllers” → click “OK.”



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

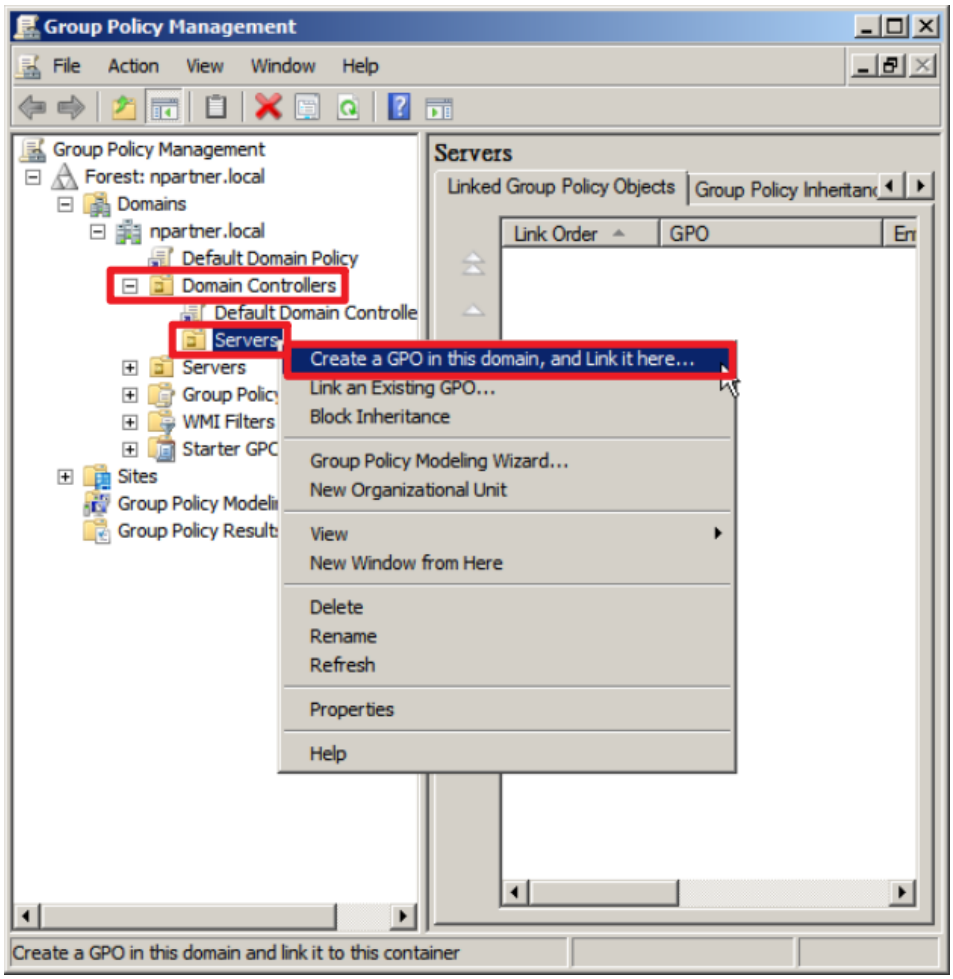
Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2008-AD-ENG” server has been moved.



4.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) Right-click the “Servers” organizational unit (OU) under “Domain Controllers” and select “Create a GPO in this domain, and Link it here…”

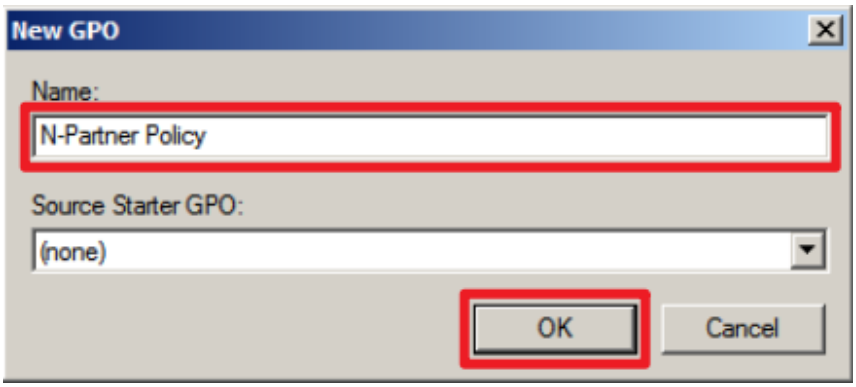


(3) Enter the Group Policy Object (GPO) name

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

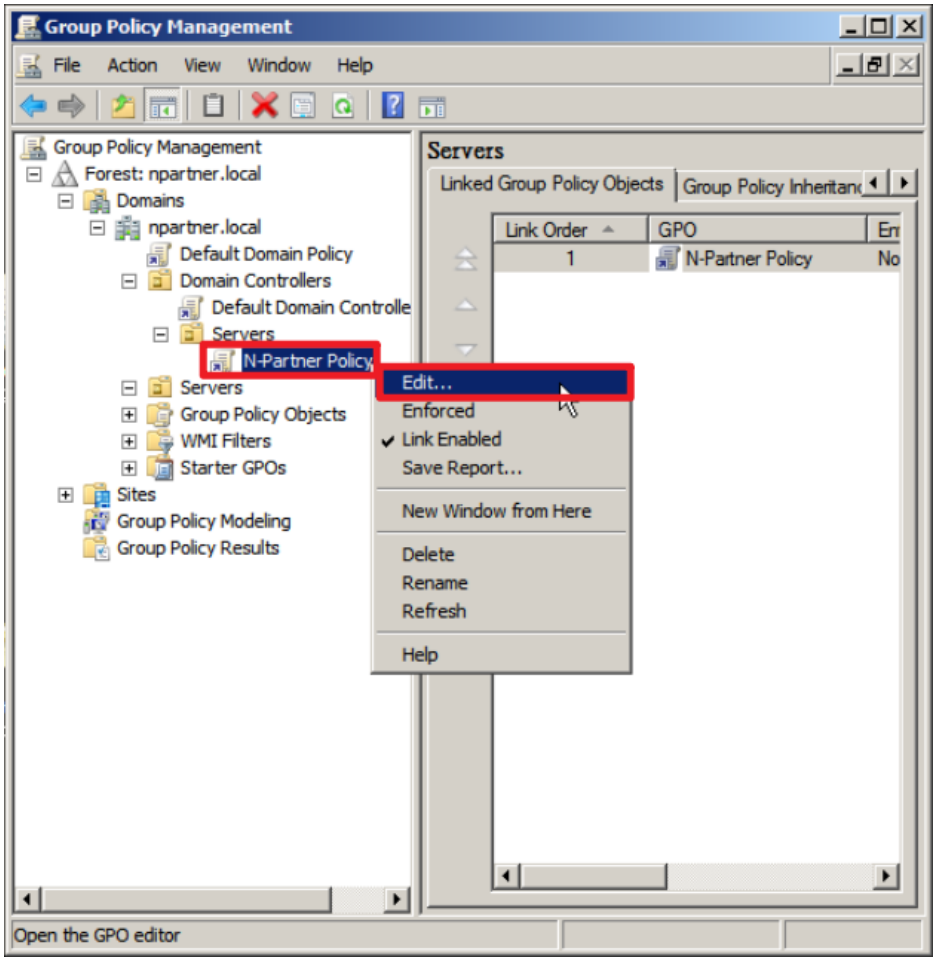
Note: Please create the GPO name according to the actual environment.

→ select “OK.”



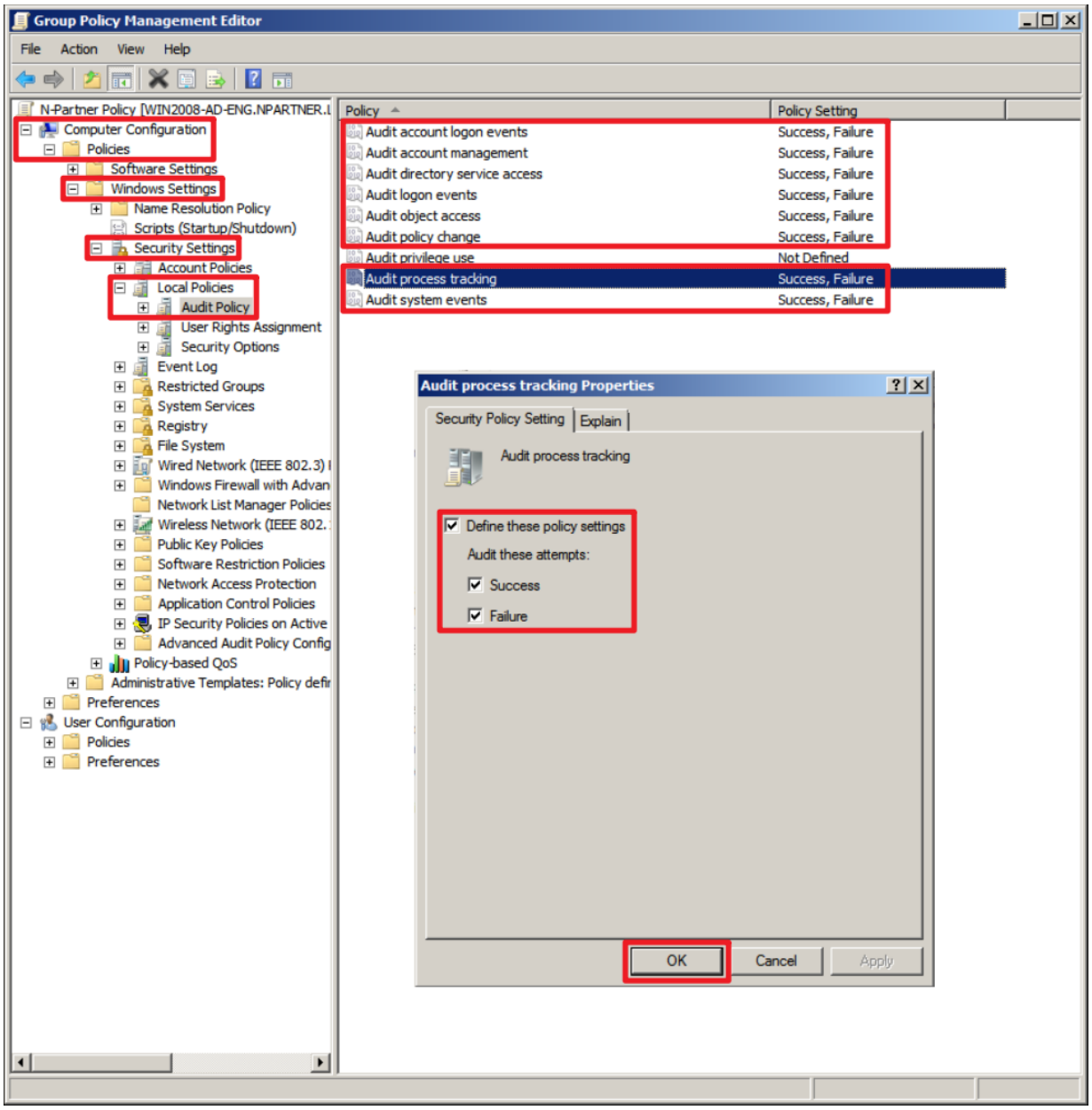
(4) Edit your Group Policy Object

Right-click the Group Policy Object (GPO) (in this example, it is “N-Partner Policy”) → select “Edit.”



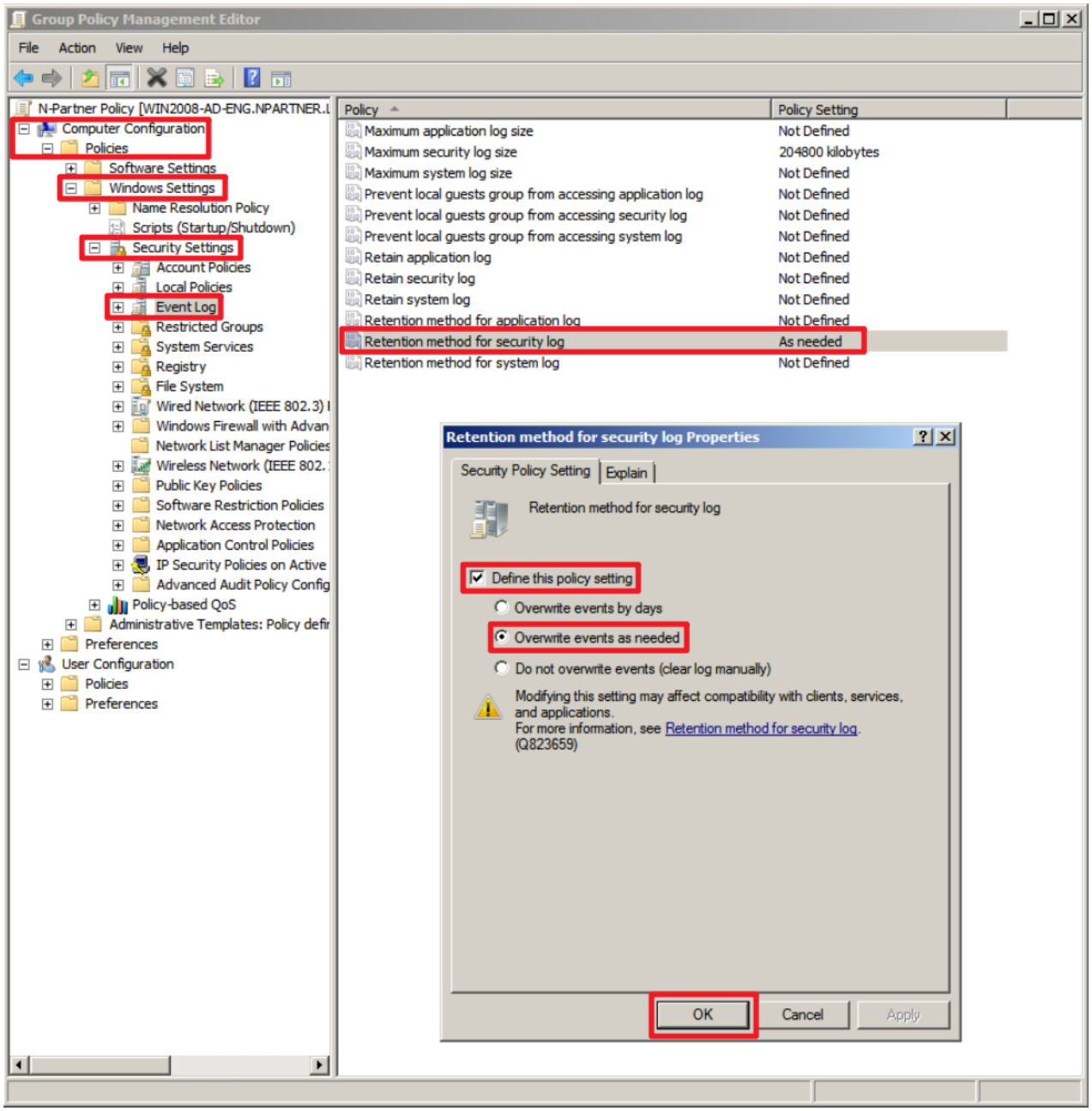
(5) Local Group Policies: Audit Policy

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” → check “Define these policy settings”: Success, Failure. → click “OK.”



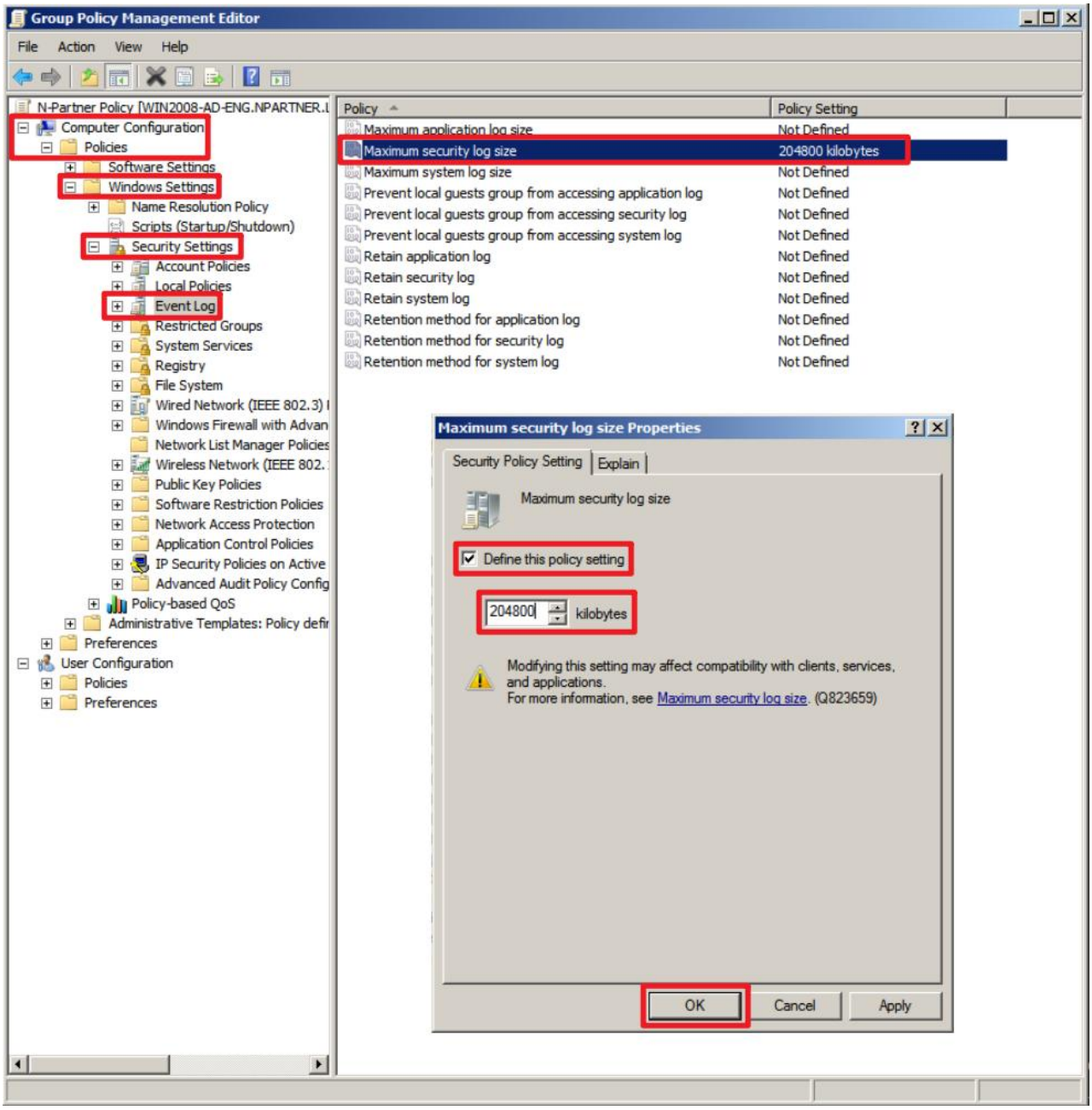
(6) Event Log: Security Log Retention Method

Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

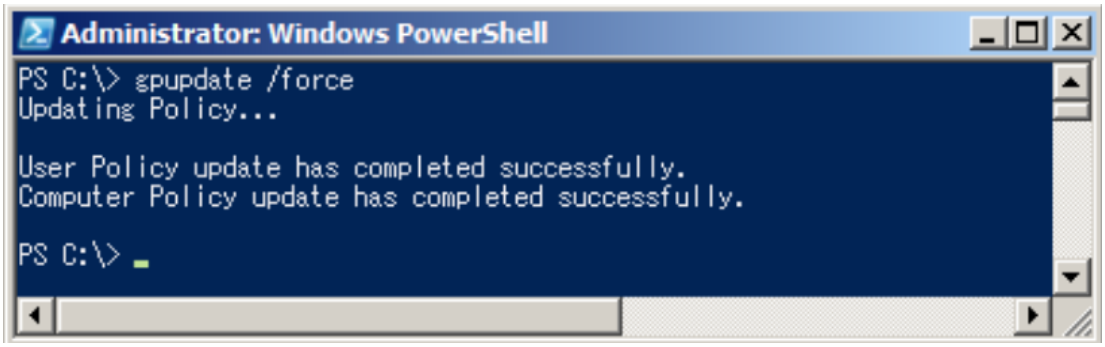
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → and click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB Note: Please adjust the number based on the actual environment. → click “OK.”



(8) On the Windows File server, open “Windows PowerShell.”

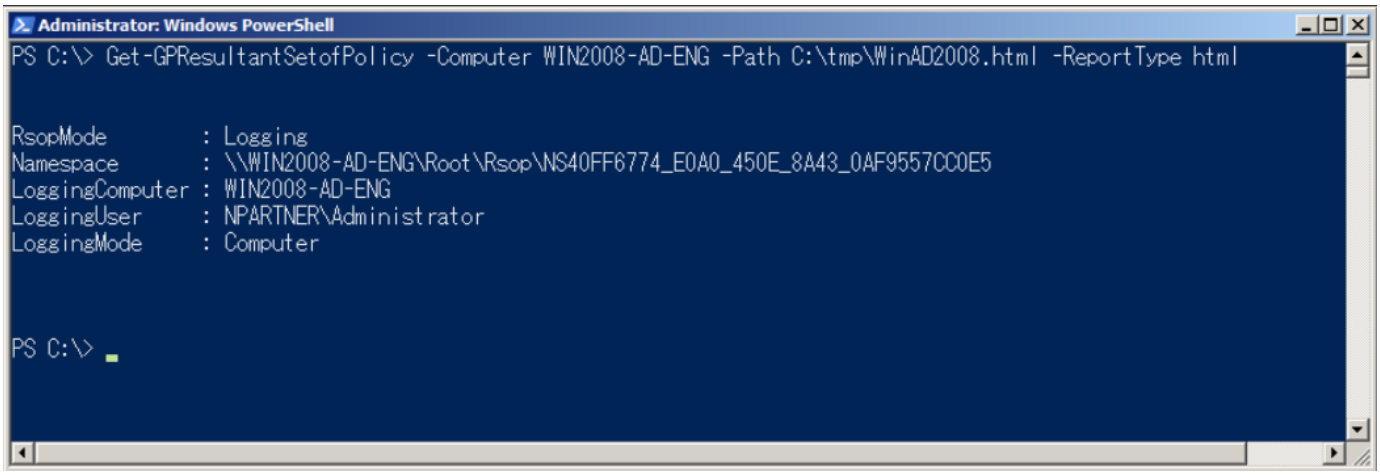
(9) Enter the command below to refresh group policy.

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



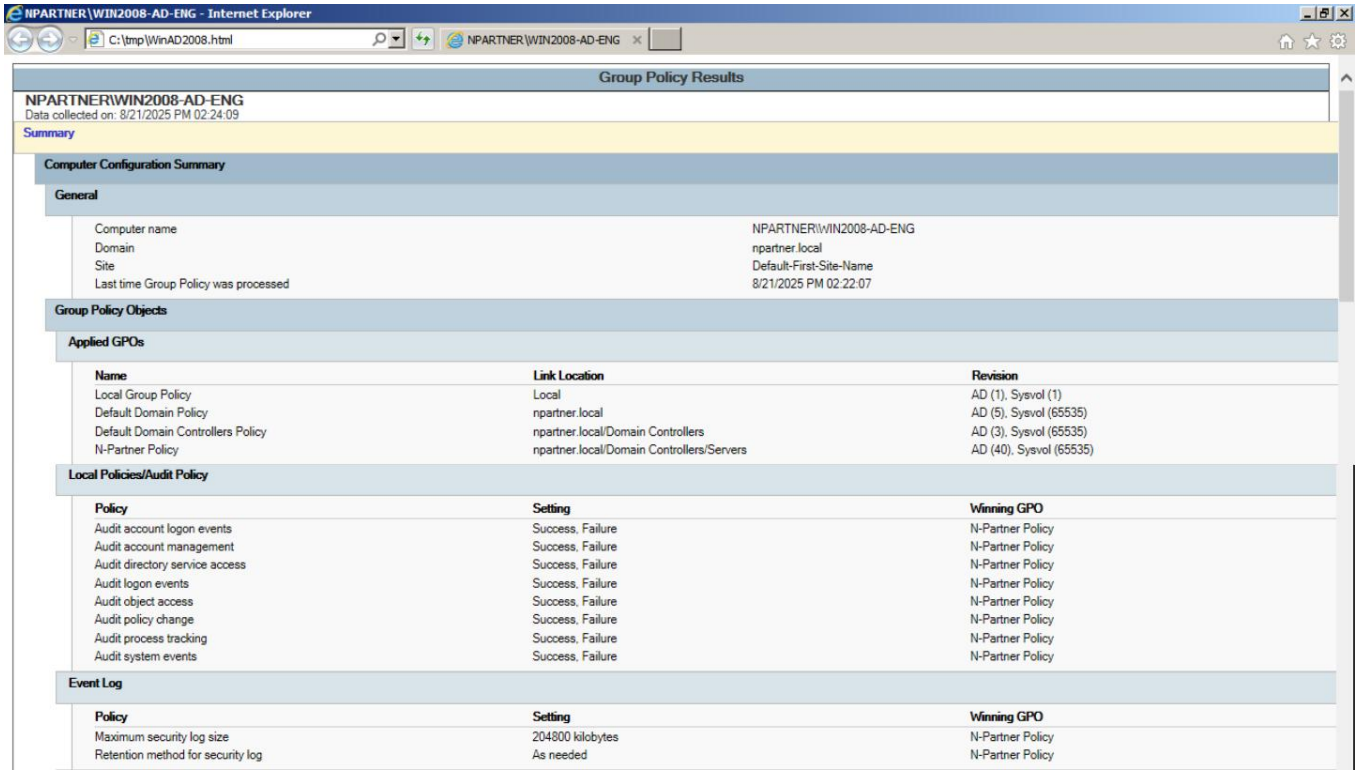
(10) On the AD domain server, open “Windows PowerShell” → enter the command below to generate the group policy report for the Windows File server.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WinAD2008 -Path C:\tmp\WinAD2008.html -ReportType html
```



Replace the text shown in red with the Windows server name and the folder path/filename.

(11) Open the report and verify that the Windows2008-AD-ENG server has applied the “N-Partner Policy” Group Policy Object (GPO).

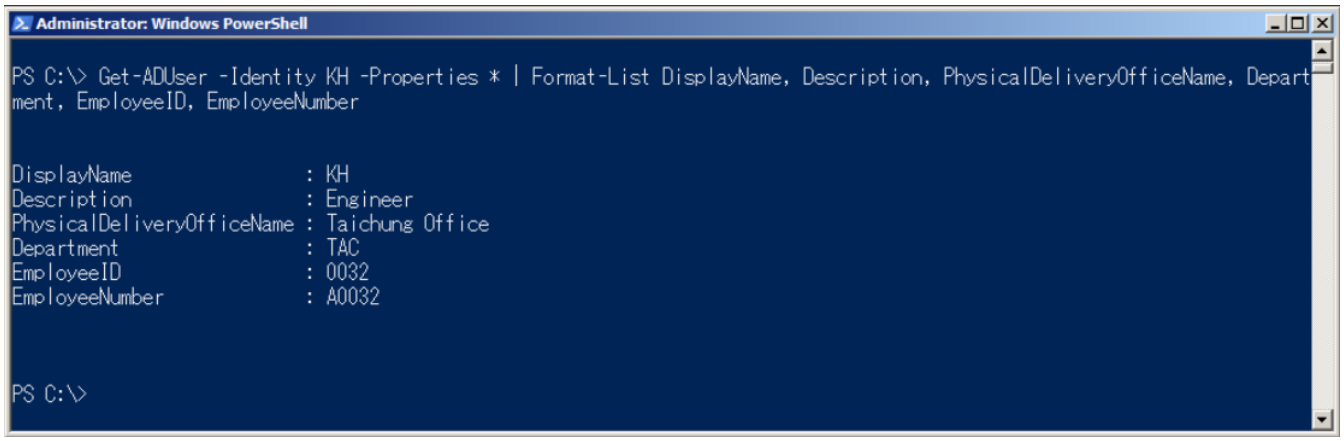


4.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Enter the command below to check whether N-Reporter associates Windows AD with available user data.

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description,
PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



Replace the red text with the username appropriate to the actual environment.

(2) In “Event Query,” click the information of “Username.”

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

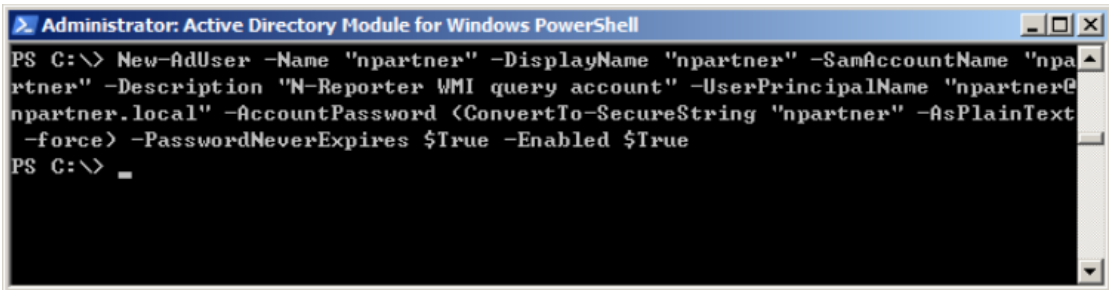
4.3.1 Add Non-Admin Accounts

(1) Open “Active Directory PowerShell Snap-In.”

(2) Create an Account

Enter the command below to create an account:

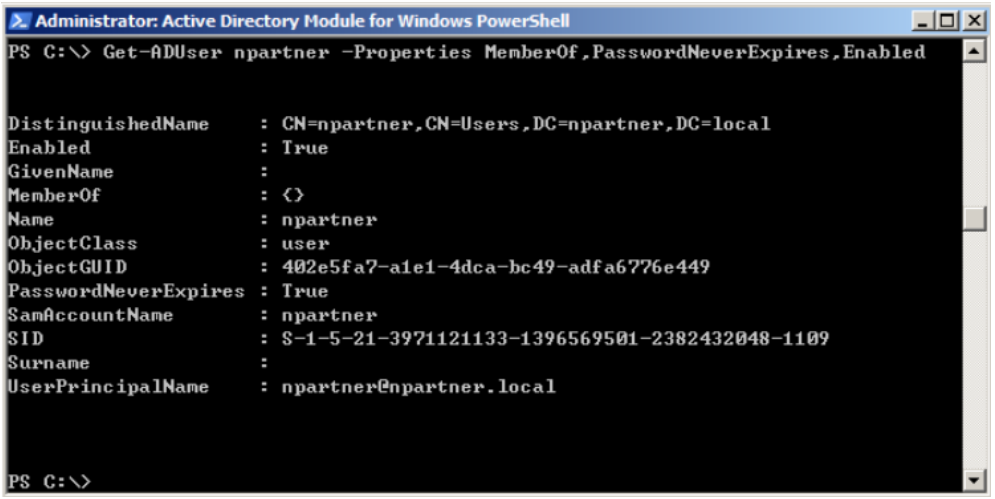
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description
"NReporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

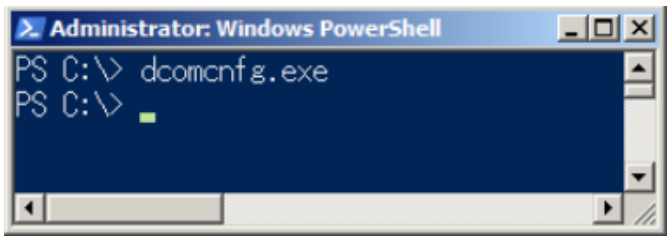


4.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”

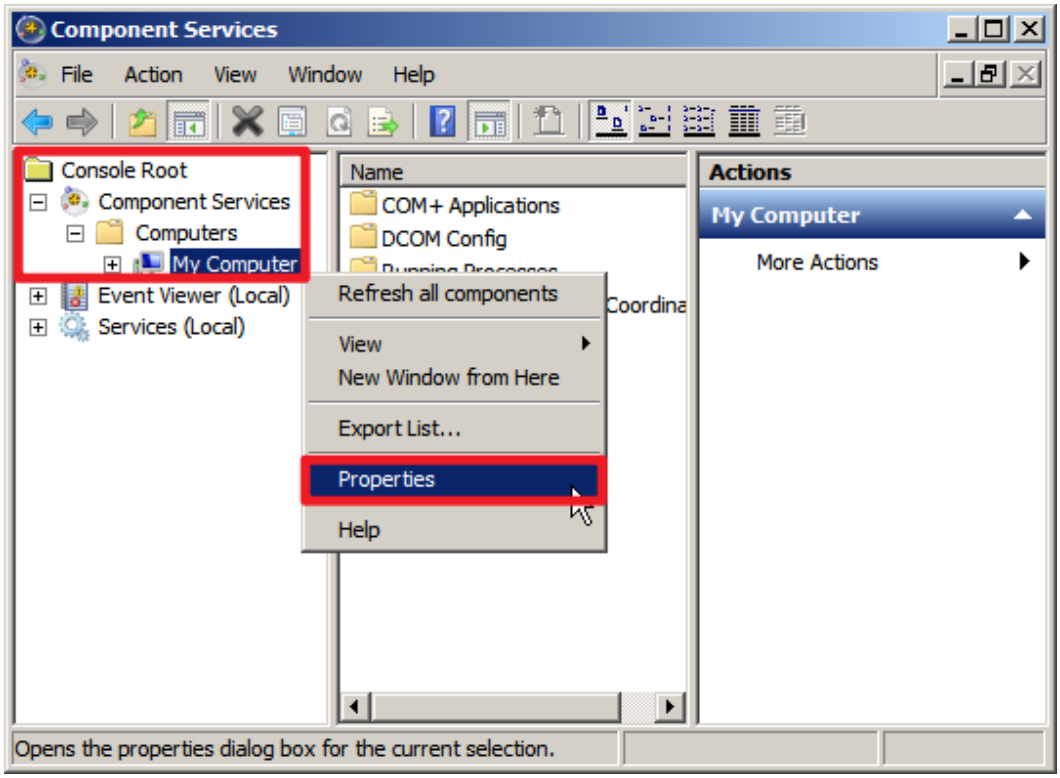
(2) Enter the command below to enable component services.

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



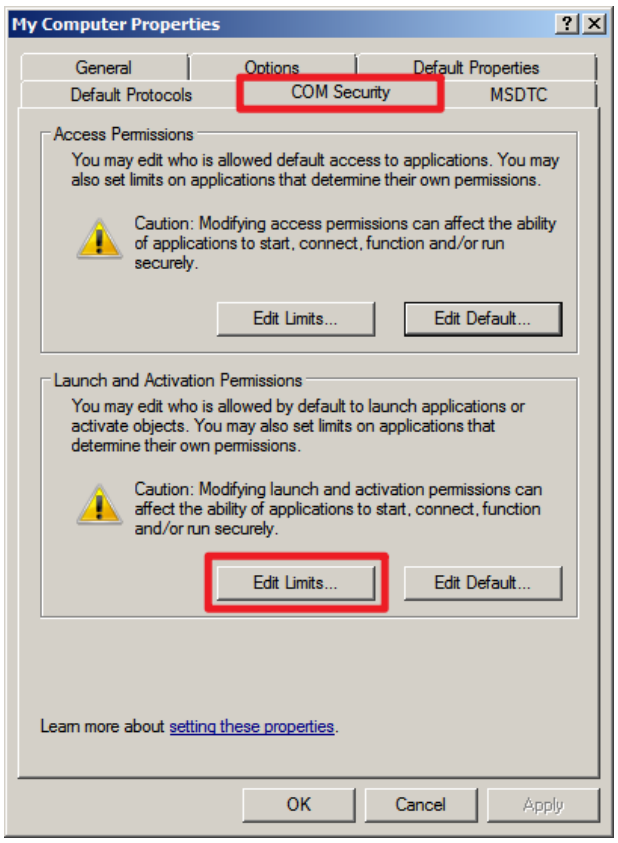
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



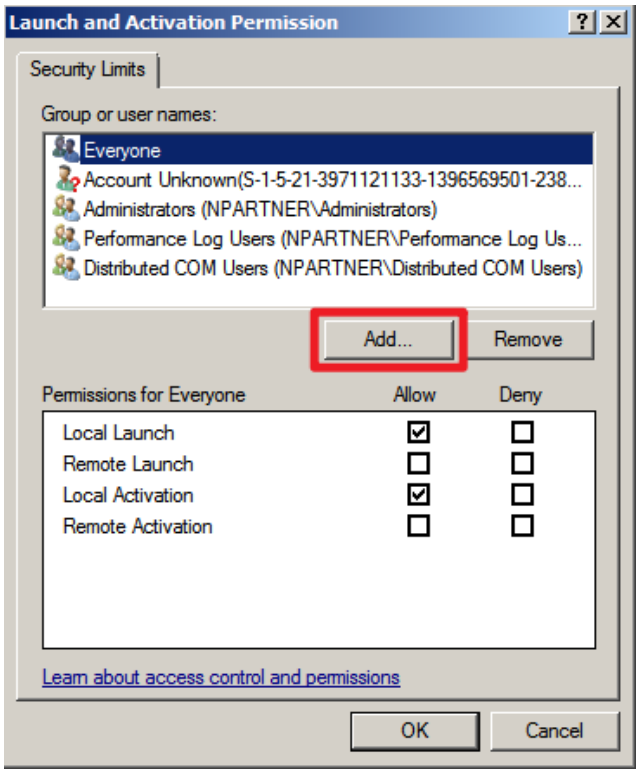
(4) Enable Permissions

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



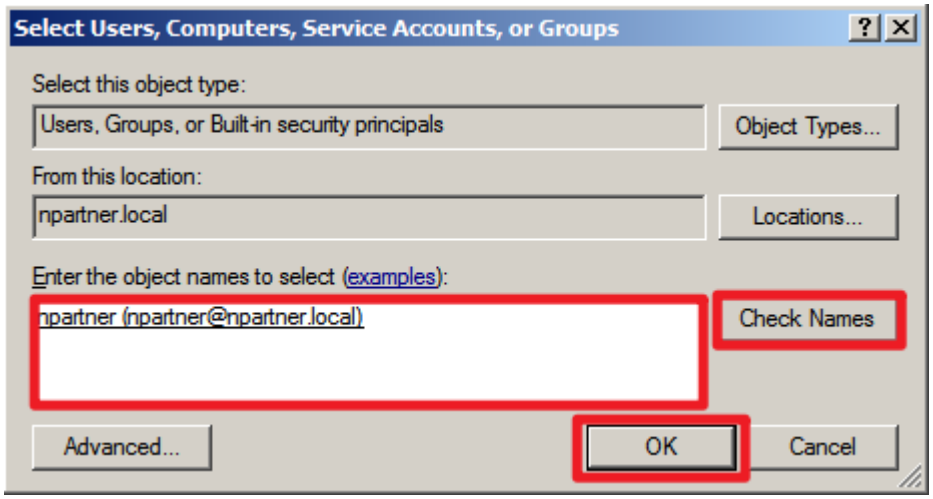
(5) Add DCOM User Permissions

Click “Add.”



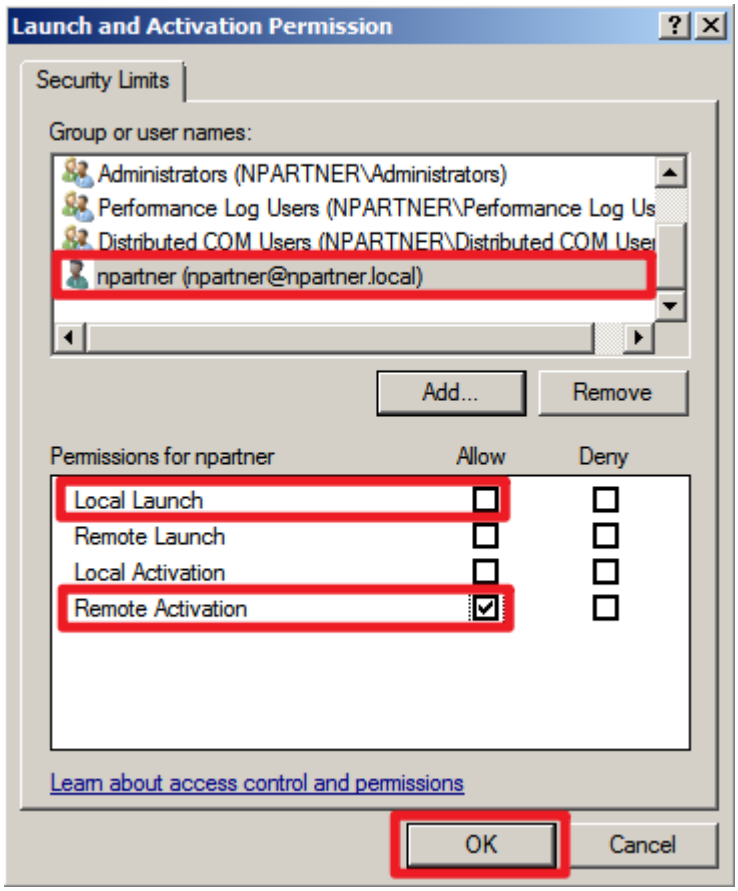
(6) Enter Your Username

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

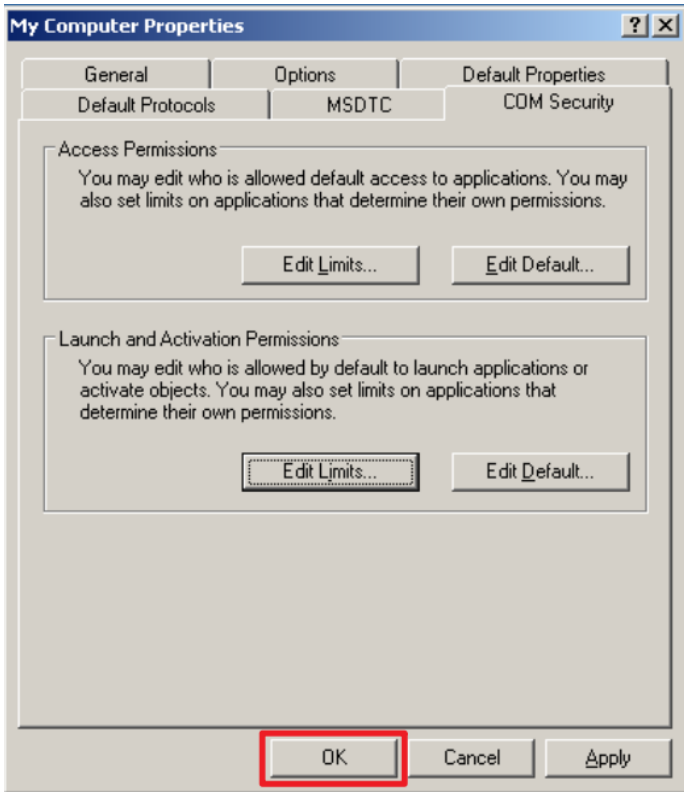


(7) Configure User Permissions

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



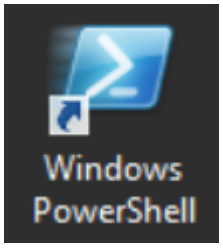
(8) Click "OK.”



4.3.3 Configure WMI Permissions

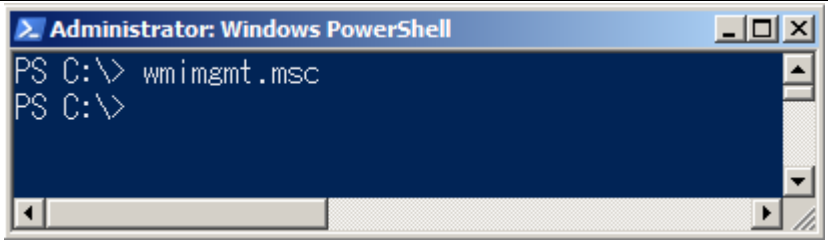
4.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



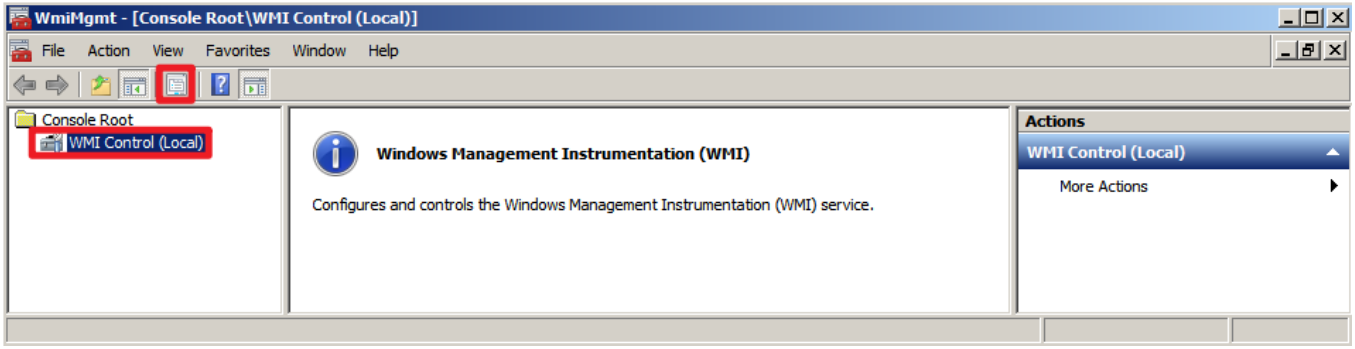
(2) Enter the command to enable WMI control service.

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



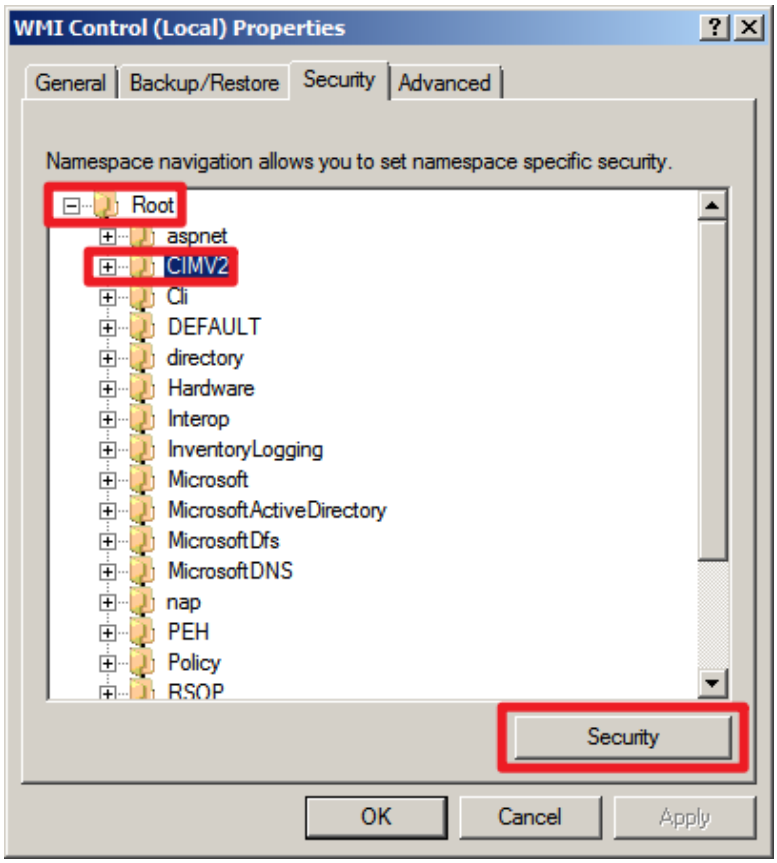
(3) Edit WMI Control

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



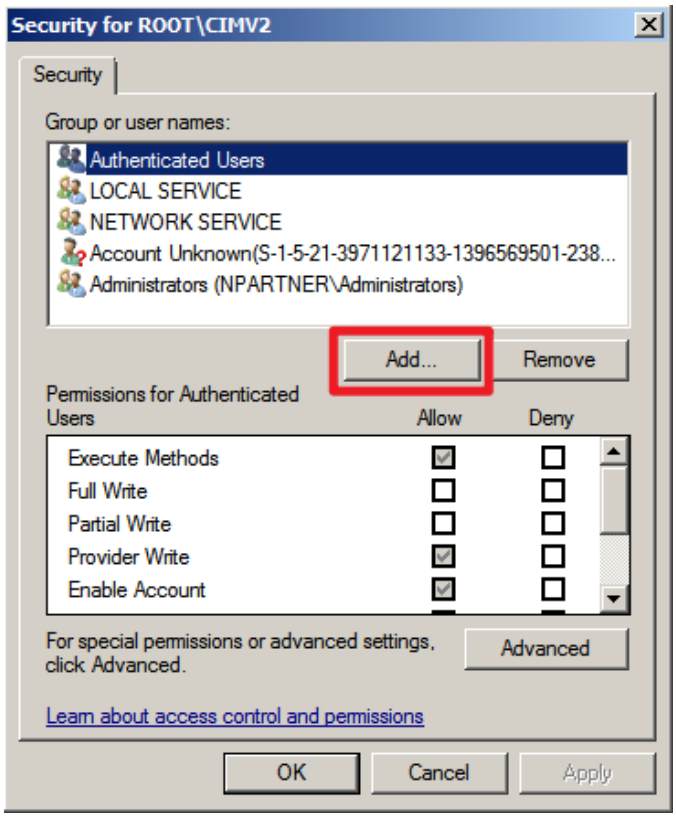
(4) Edit CIMV2 Security

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



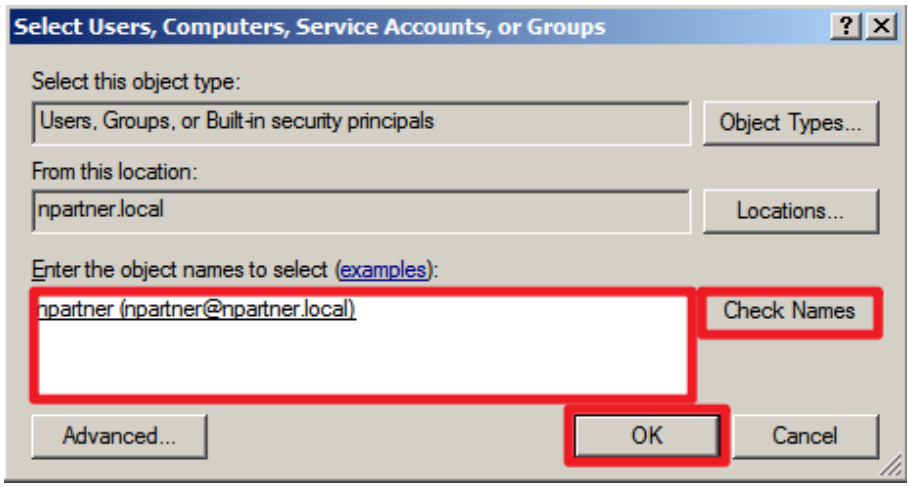
(5) Add WMI User Permissions.

Click “Add.”



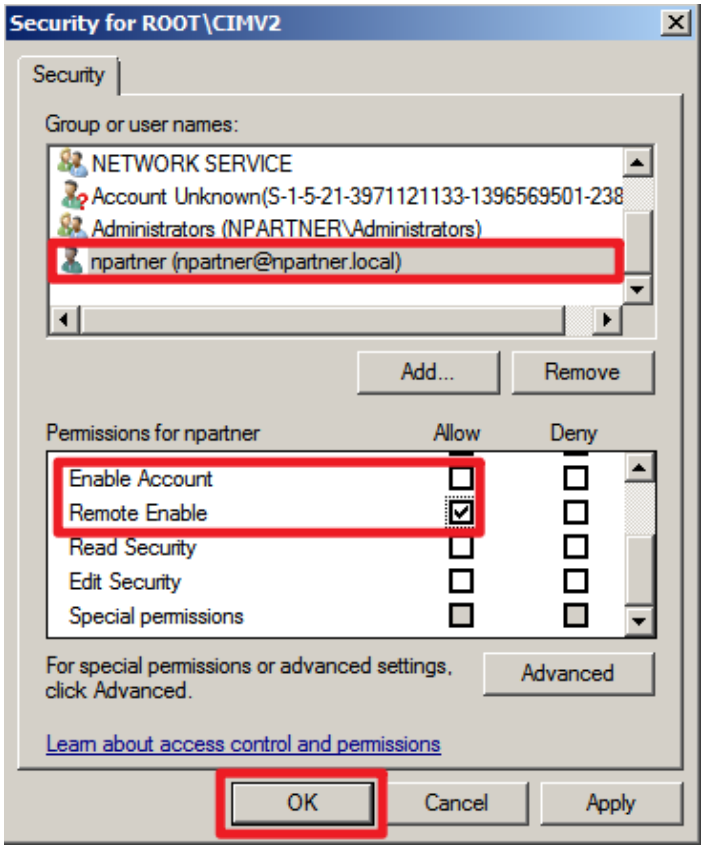
(6) Enter Your Username

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

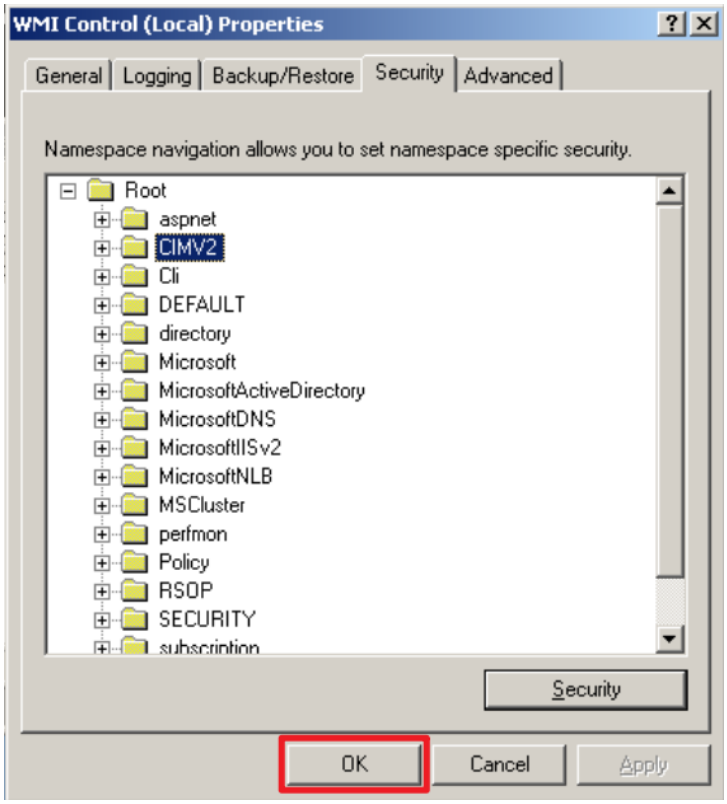


(7) Set Your User Permissions

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



(8) Click “OK.”

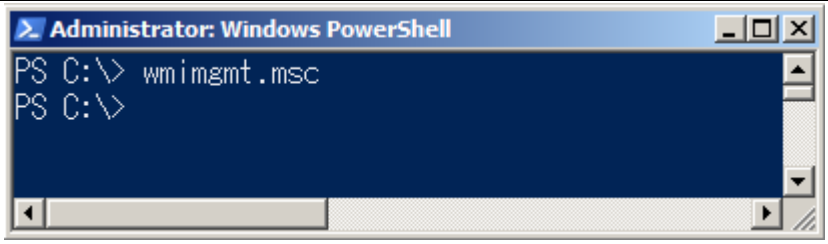


4.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”

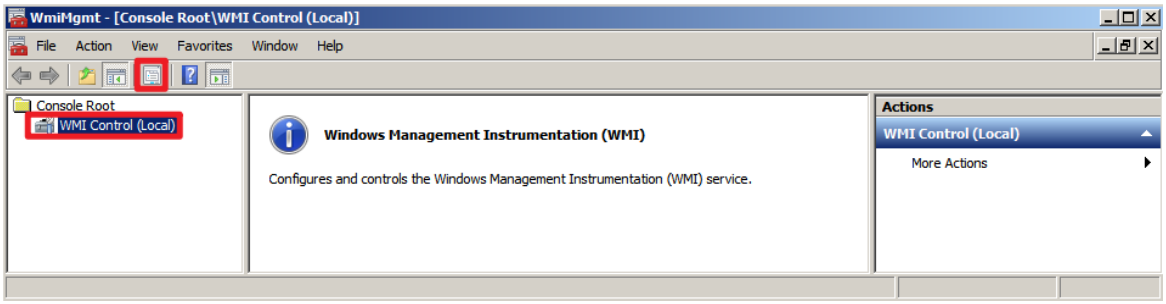
(2) Enter the command below to enable WMI Control.

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



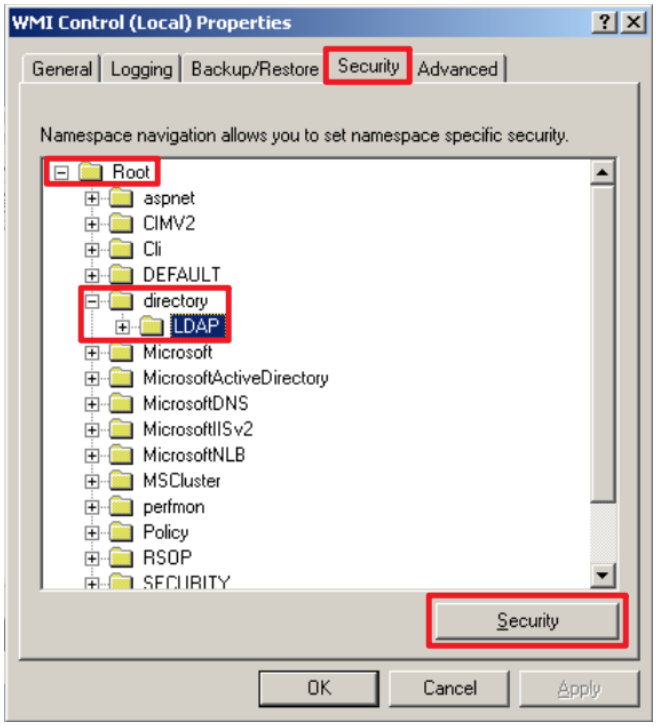
(3) Edit WMI Control

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



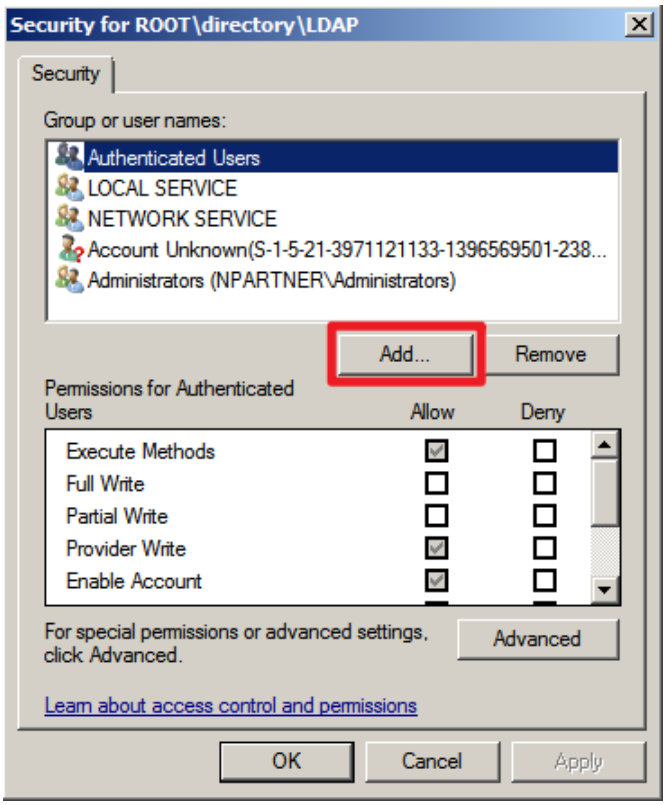
(4) Edit LDAP Security

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



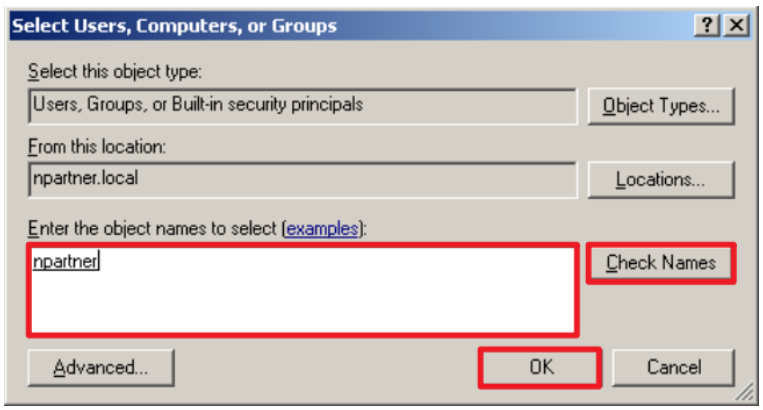
(5) Add WMI User Permissions

Click “Add.”



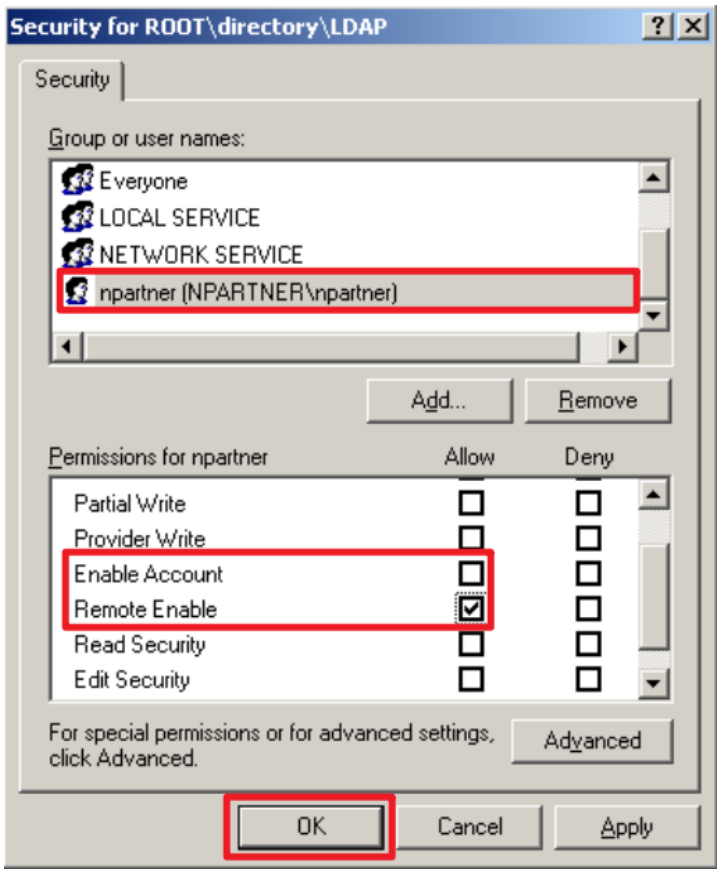
(6) Enter Your Username

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

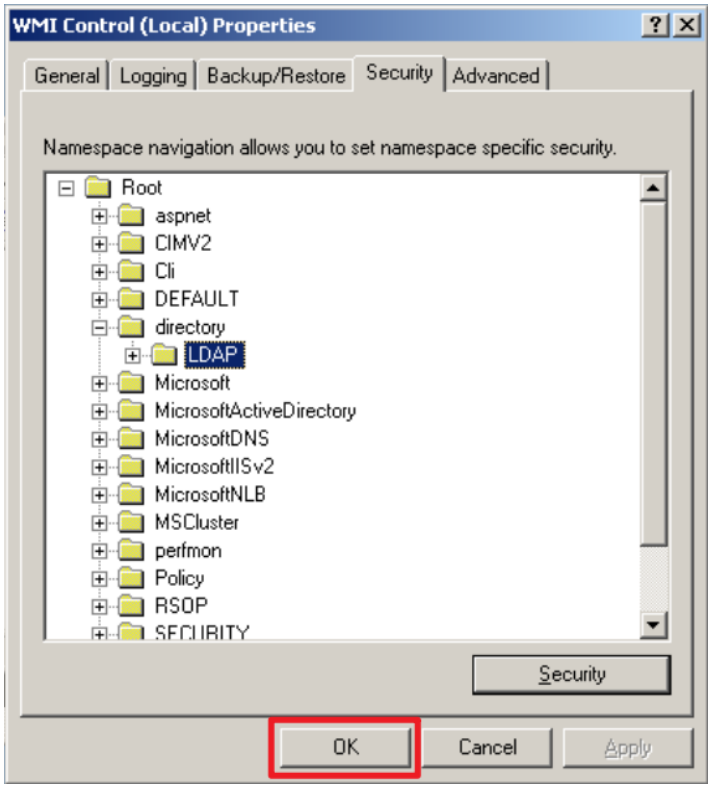


(7) Set Your User Permissions

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

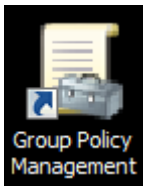


(8) Click “OK.”

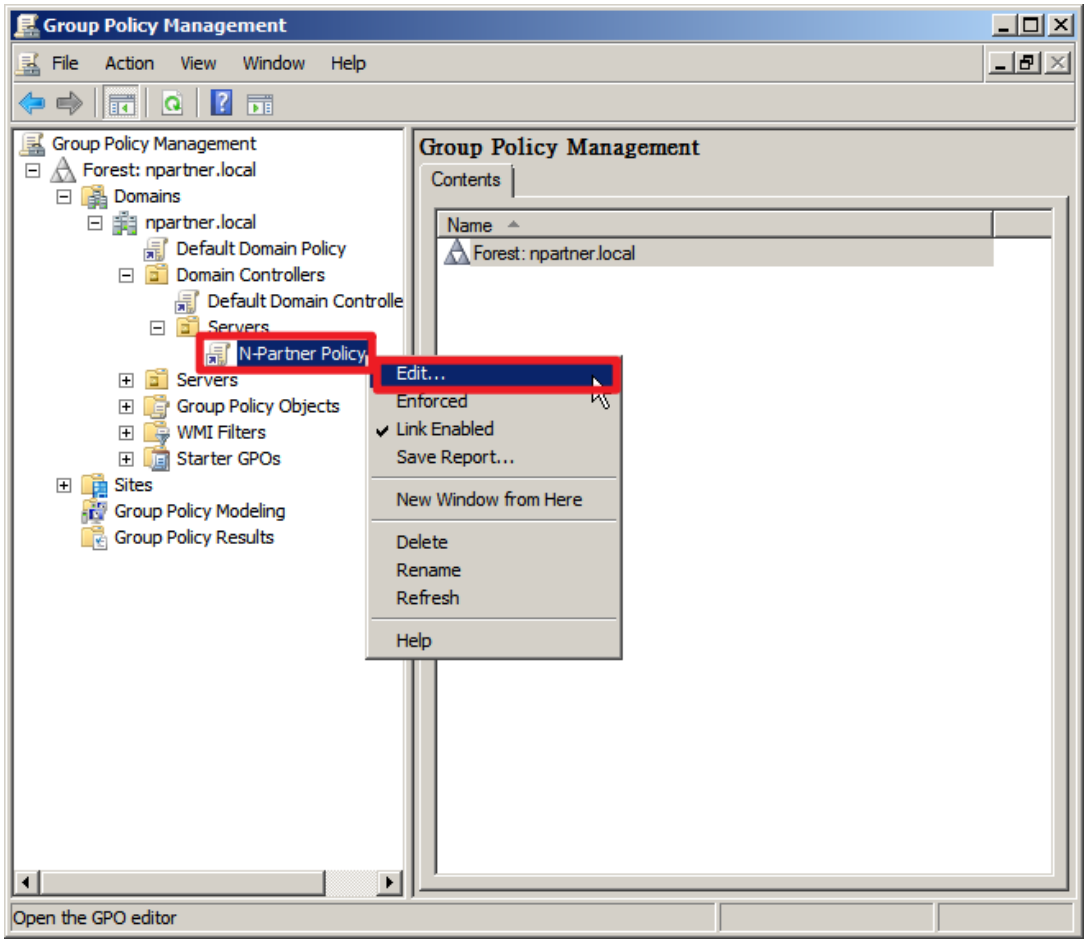


4.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

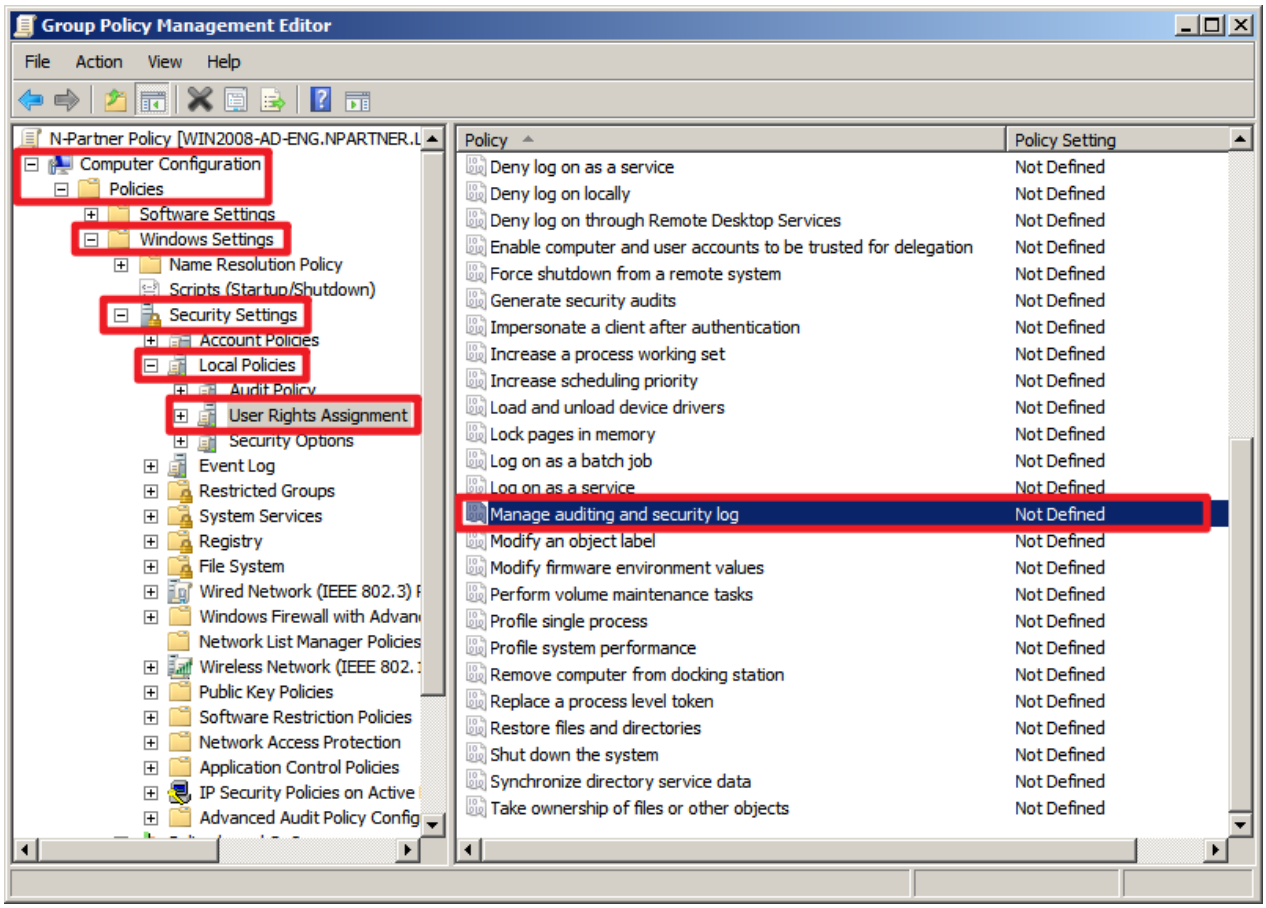


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



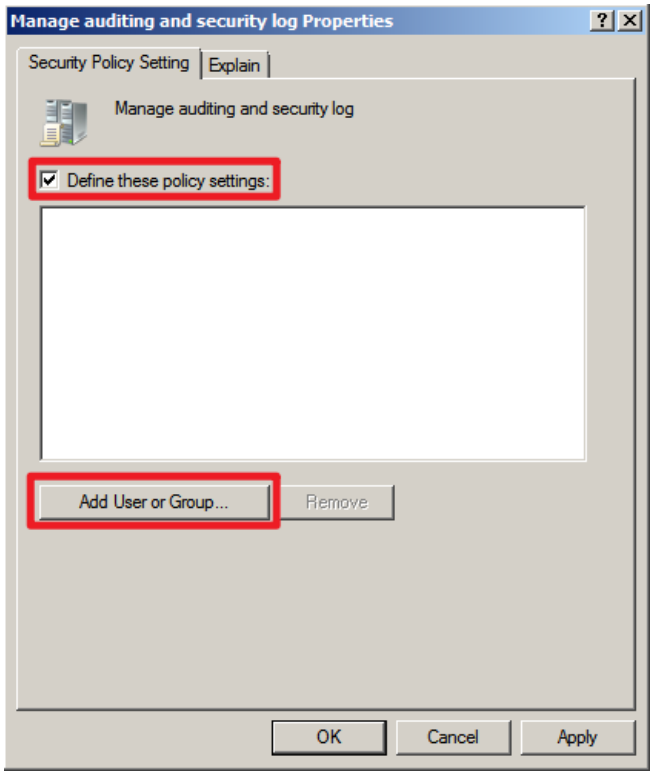
(3) Configure Auditing Log

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



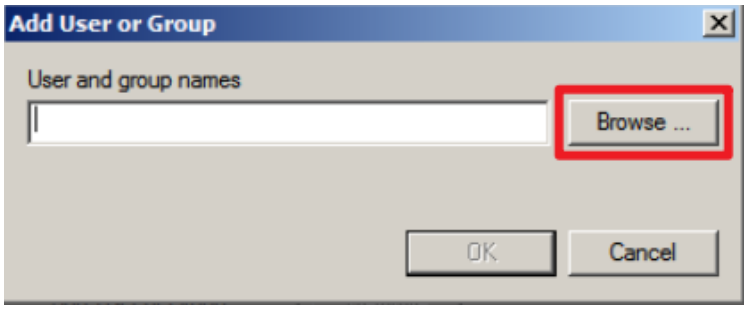
(4) Add Auditing User

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



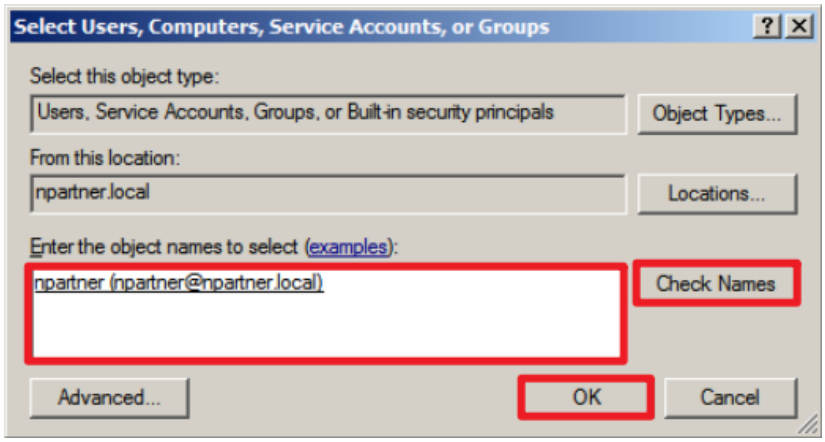
(5) Search for User

Click “Browse.”

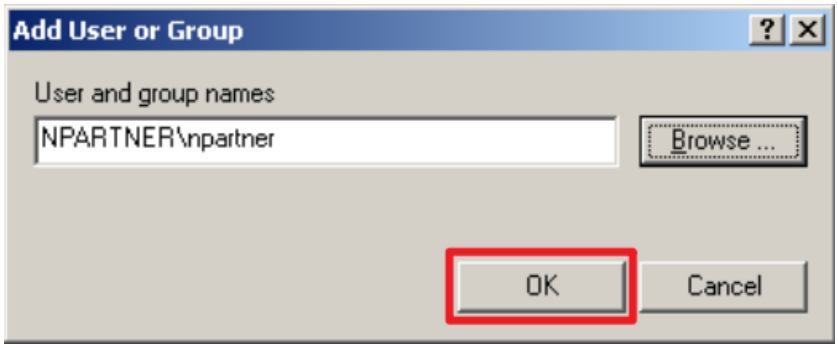


(6) Enter Your User Account

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

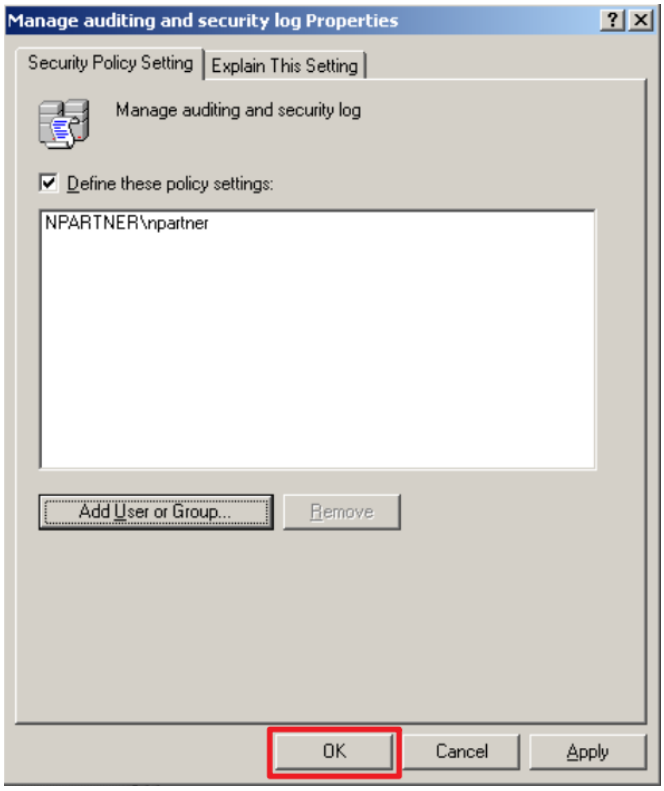


(7) Click “OK.”



(8) Confirm Audit Log Settings

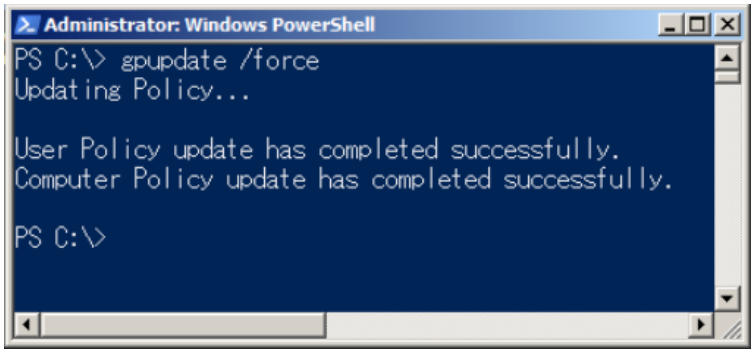
Click “OK.”



(9) Open “Windows Powershell.”

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

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

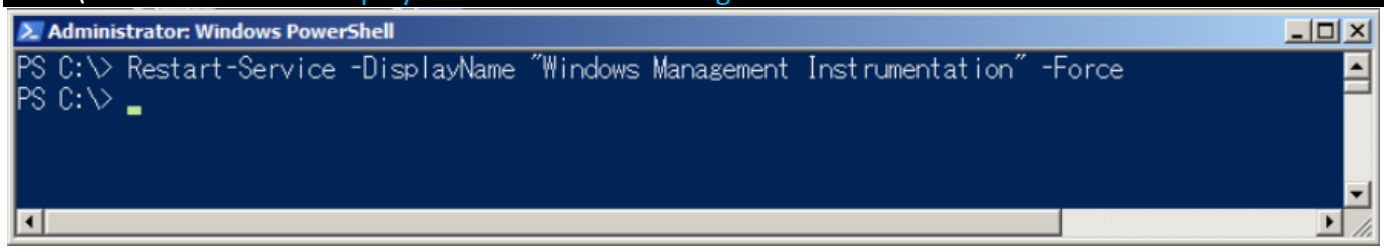


4.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”

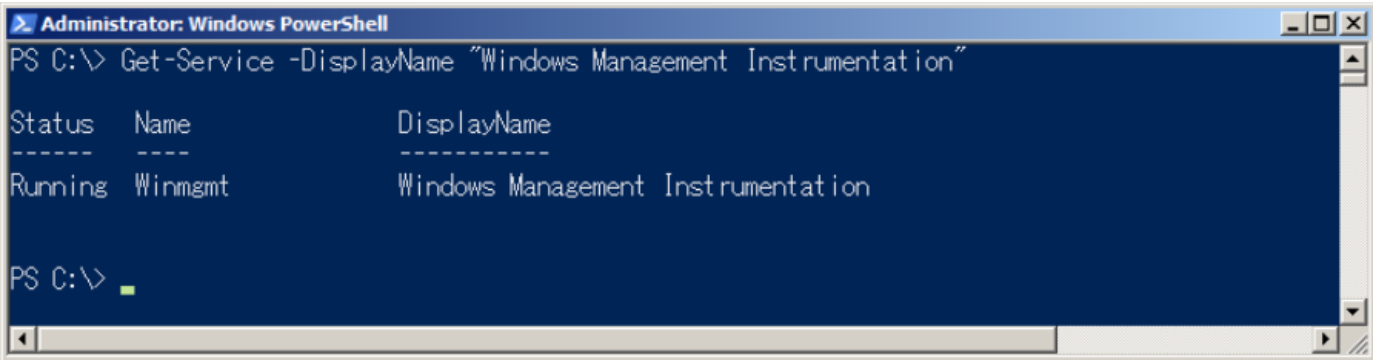
(2) Enter the command below to disable the WMI service.

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



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

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

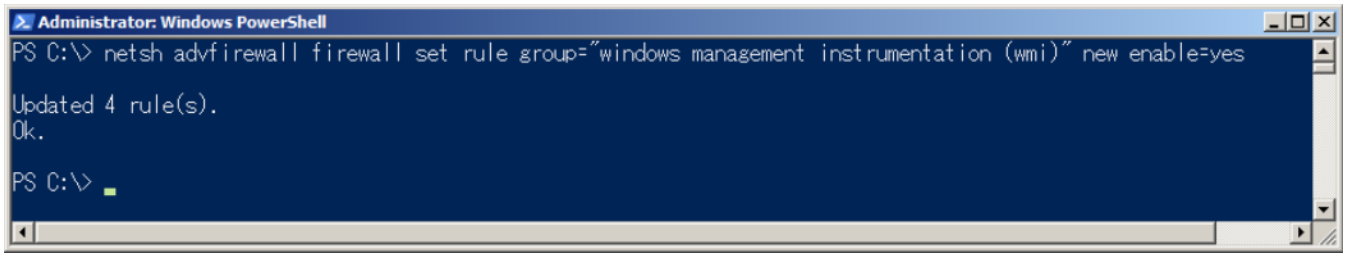


4.3.6 Configure the Firewall

(1) Open “Windows Powershell.”

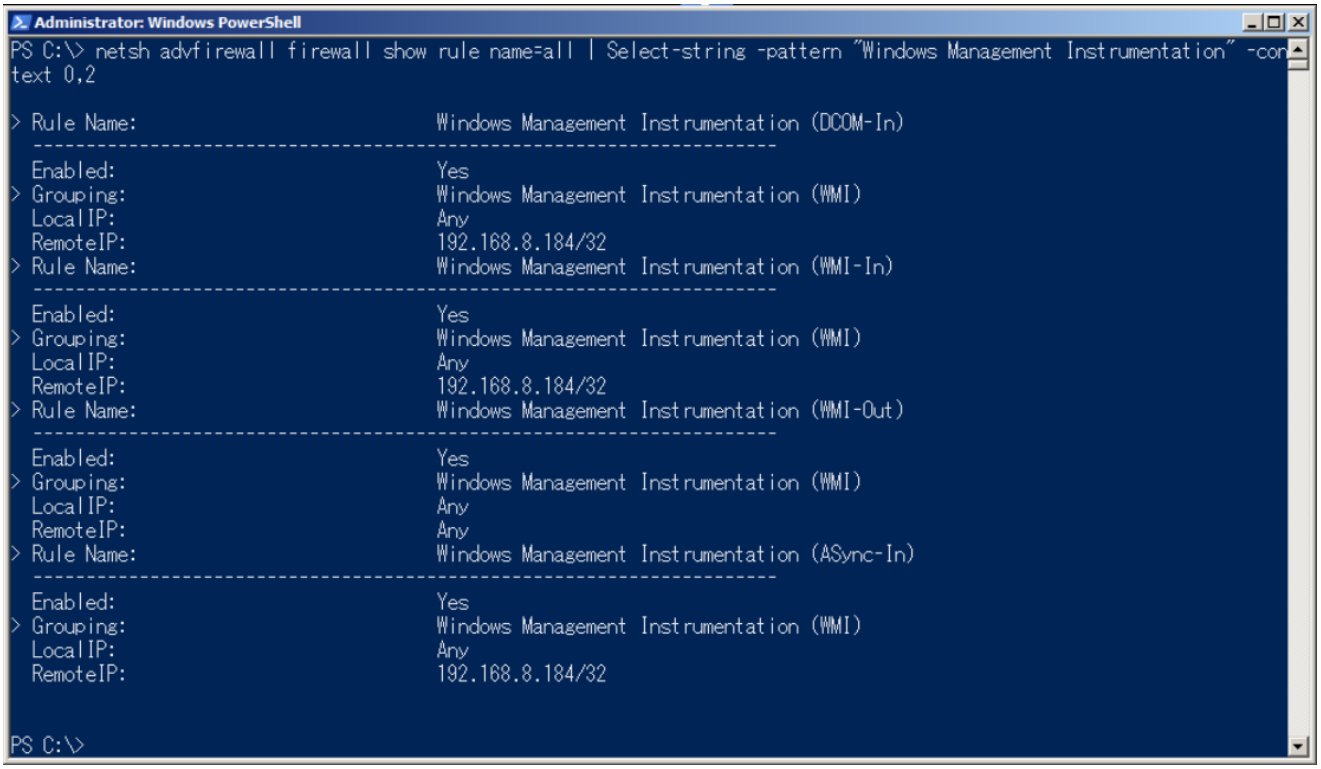
(2) Enter the command below to allow WMI through the firewall:

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



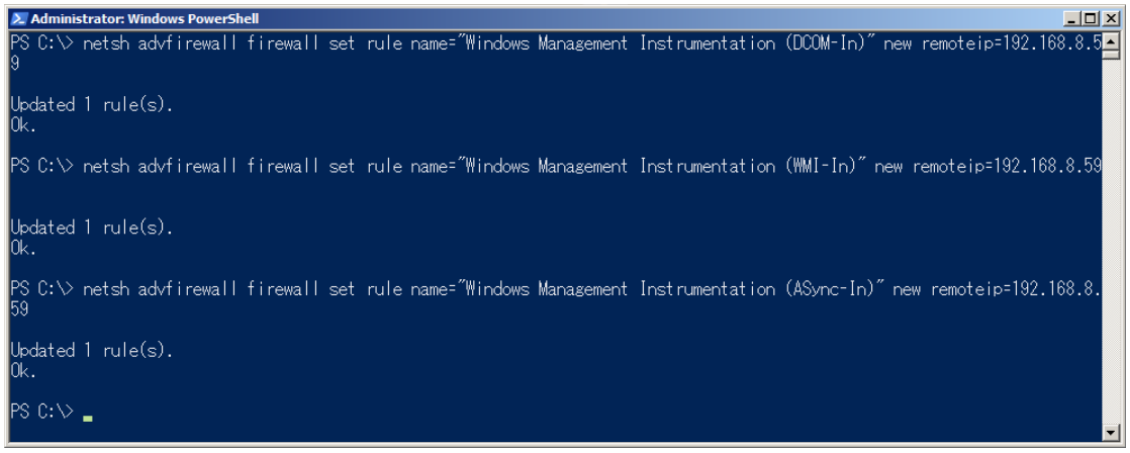
(3) Enter the command below to allow TCP port 135 through the firewall:

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



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

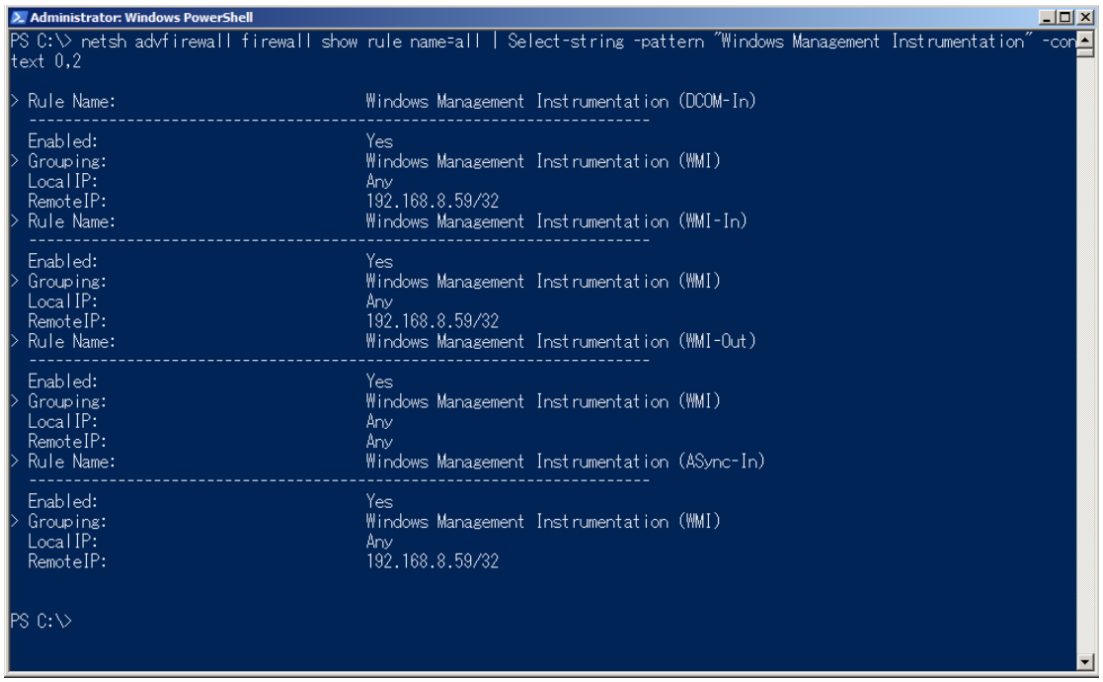
```
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.184
PS C:\> netsh advfirewall firewall set rule name="Windows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



Replace the red text with the N-Reporter IP address.

(5) Enter the command below to show the current firewall WMI configuration:

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



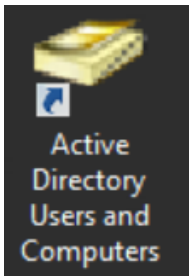
5. Windows Server 2012

Windows Audit Policy Configuration:

For detailed information, refer to the **Audit Policy Recommendations link** in the references.

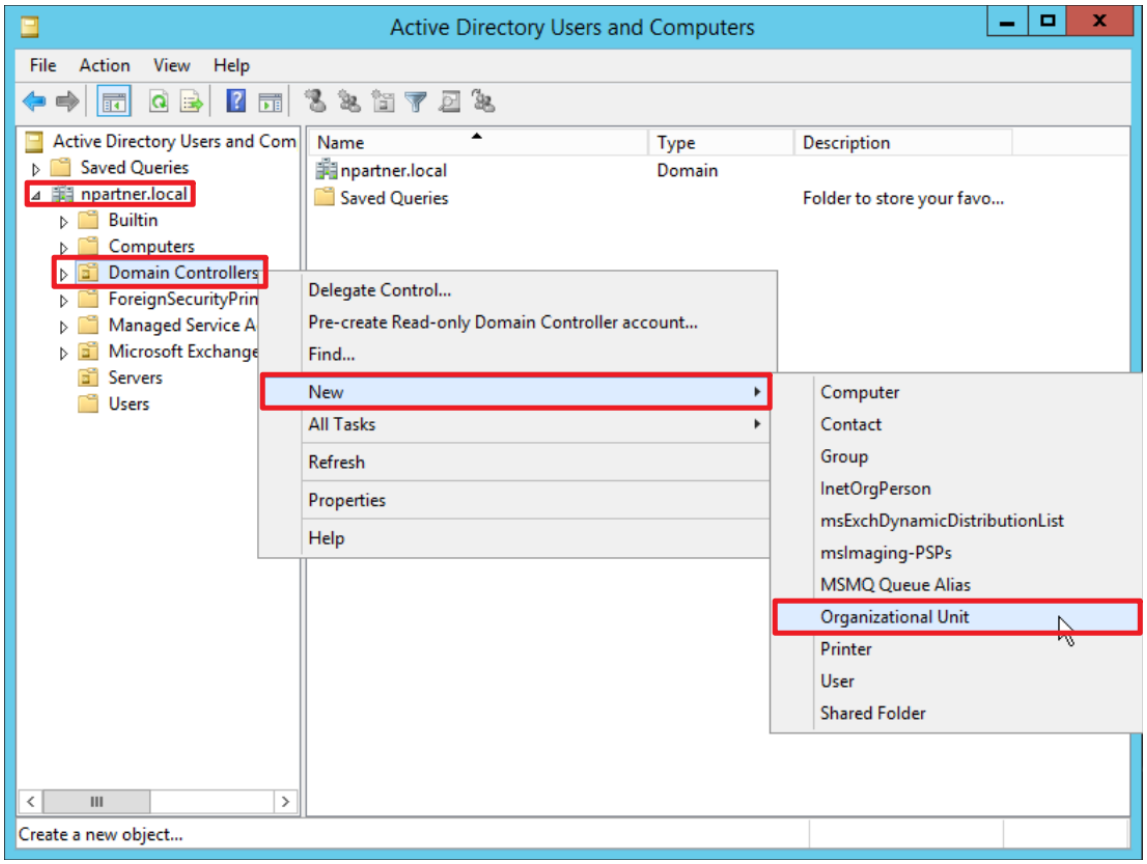
5.1 Organizational Unit (OU) Configuration

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



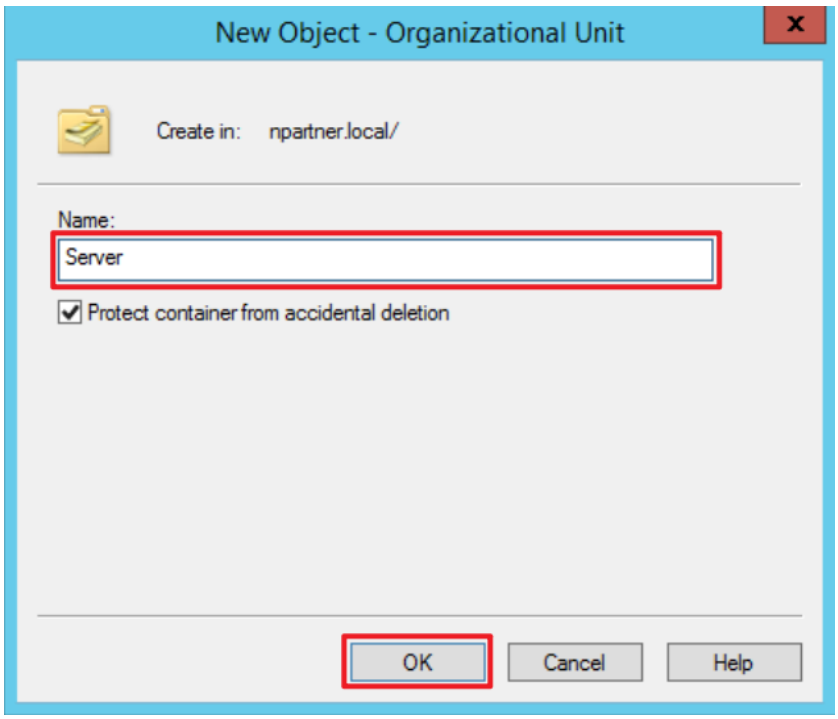
(2) Add an Organizational Unit

Right-click on the domain name (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



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

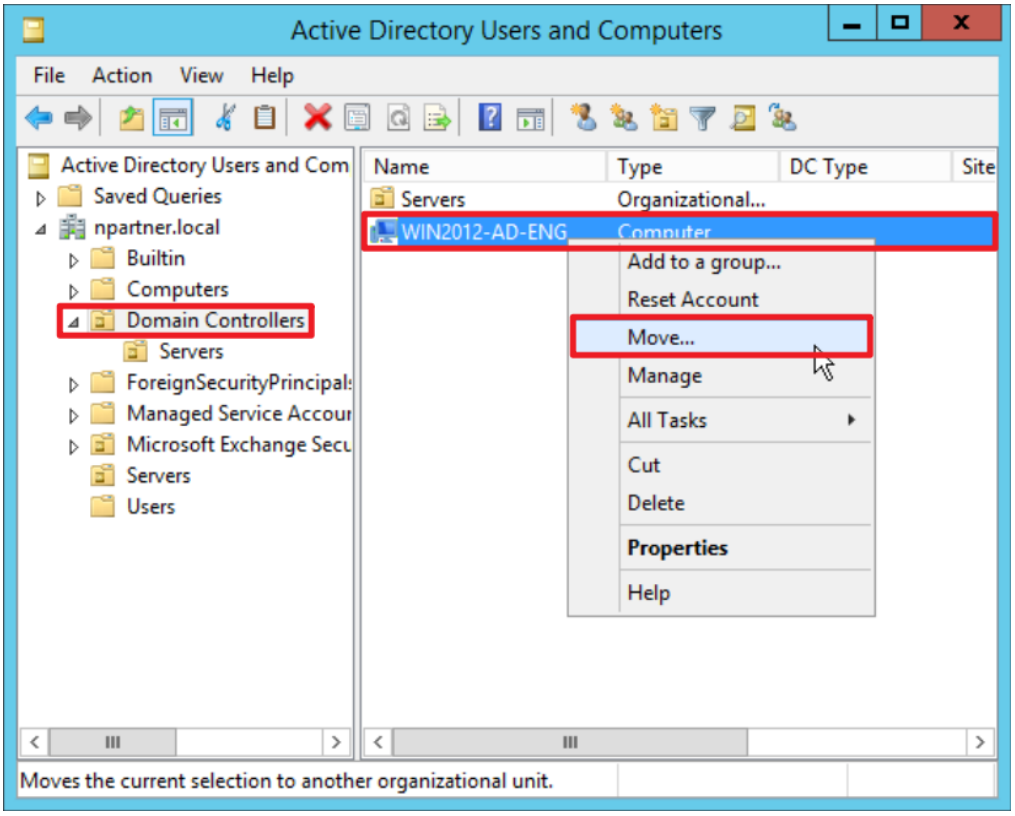
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

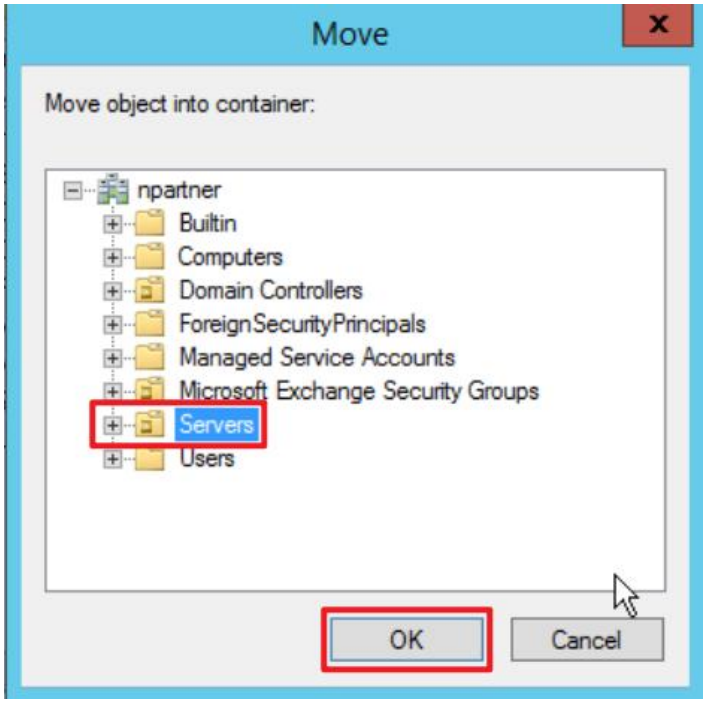
Select “Domain Controllers” → right-click on the “WIN2012-AD-ENG” server.

Note: Please select the Windows server according to the actual environment. → click “Move.”



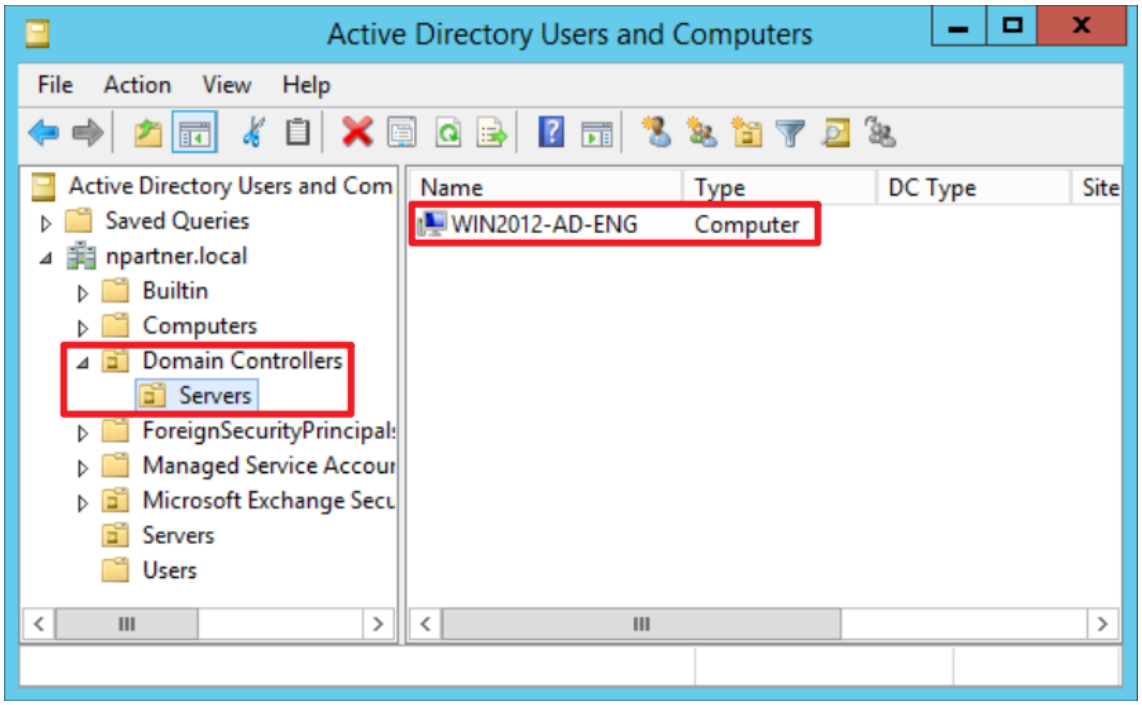
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is "Servers") → 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") and confirm that the "WIN2012-AD-ENG" server has been moved.

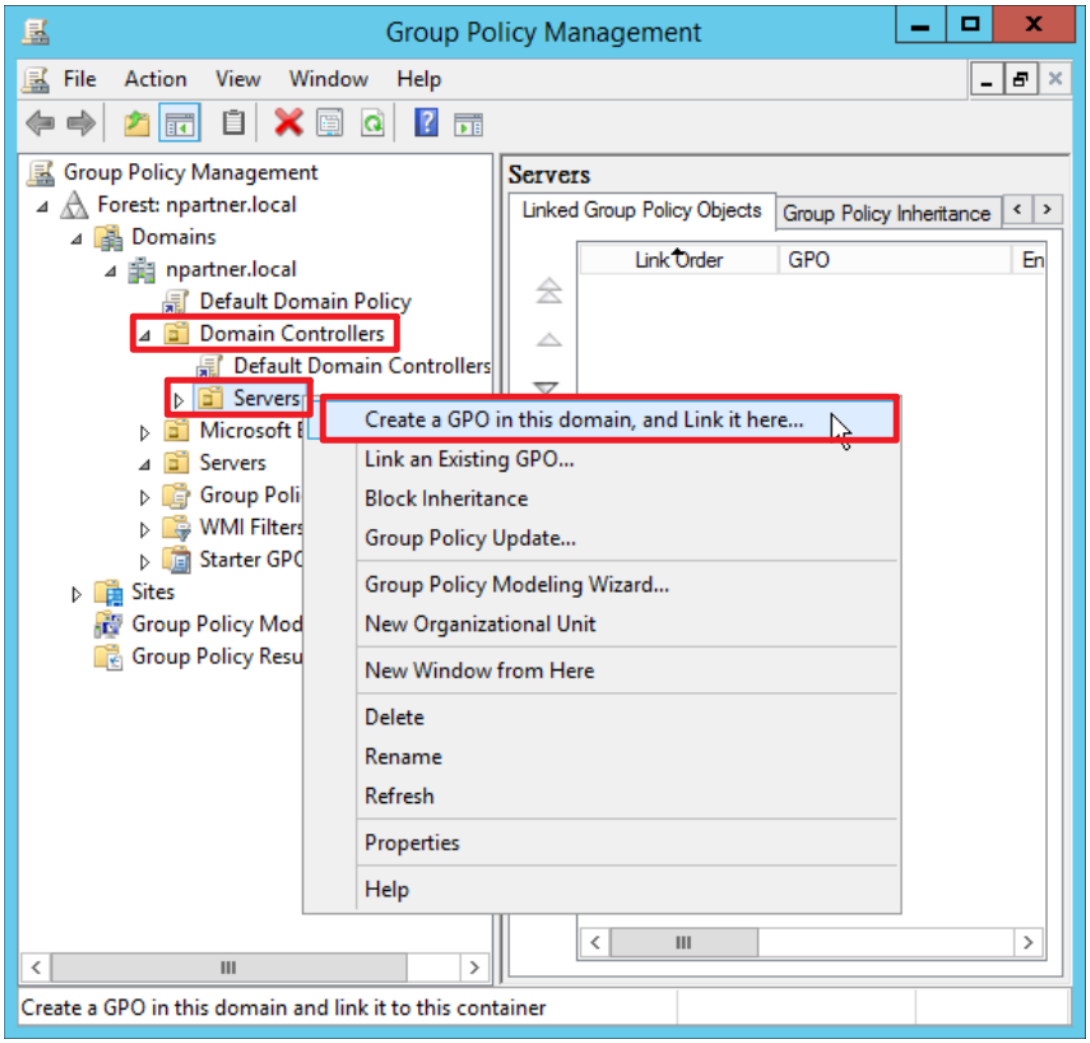


5.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

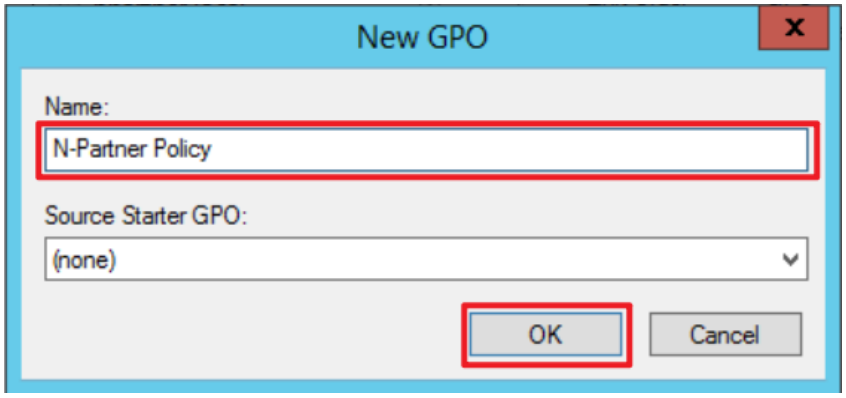
Right-click the “Servers” organizational unit under “Domain Controllers” → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

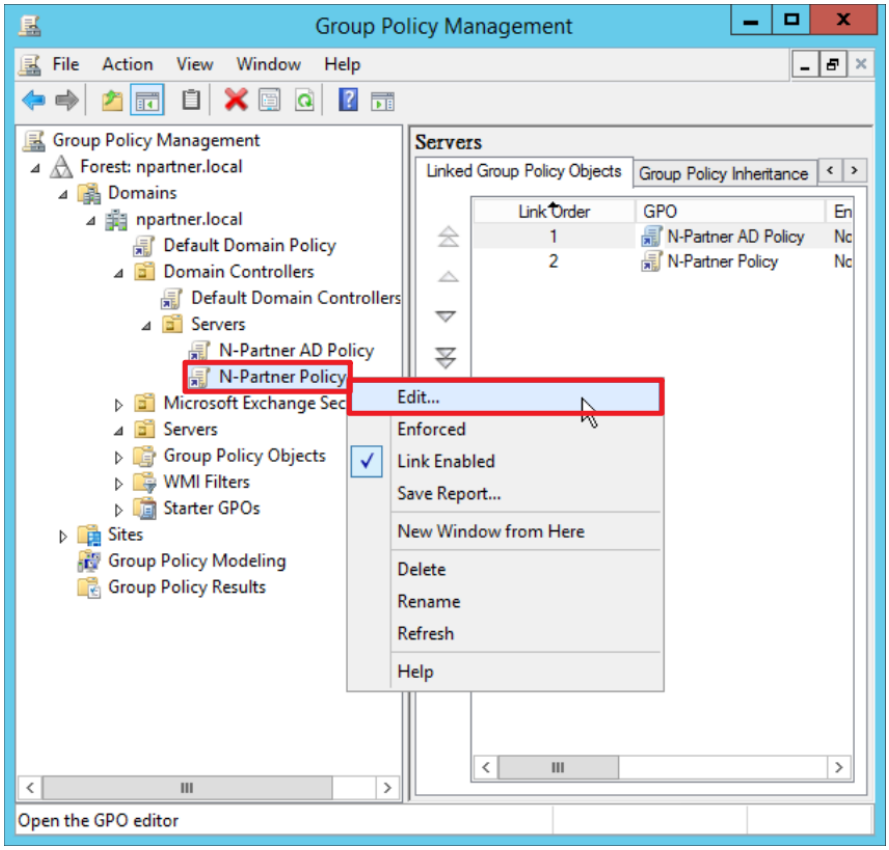
Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

Note: Create your GPO name according to the actual environment. → then click "Edit."



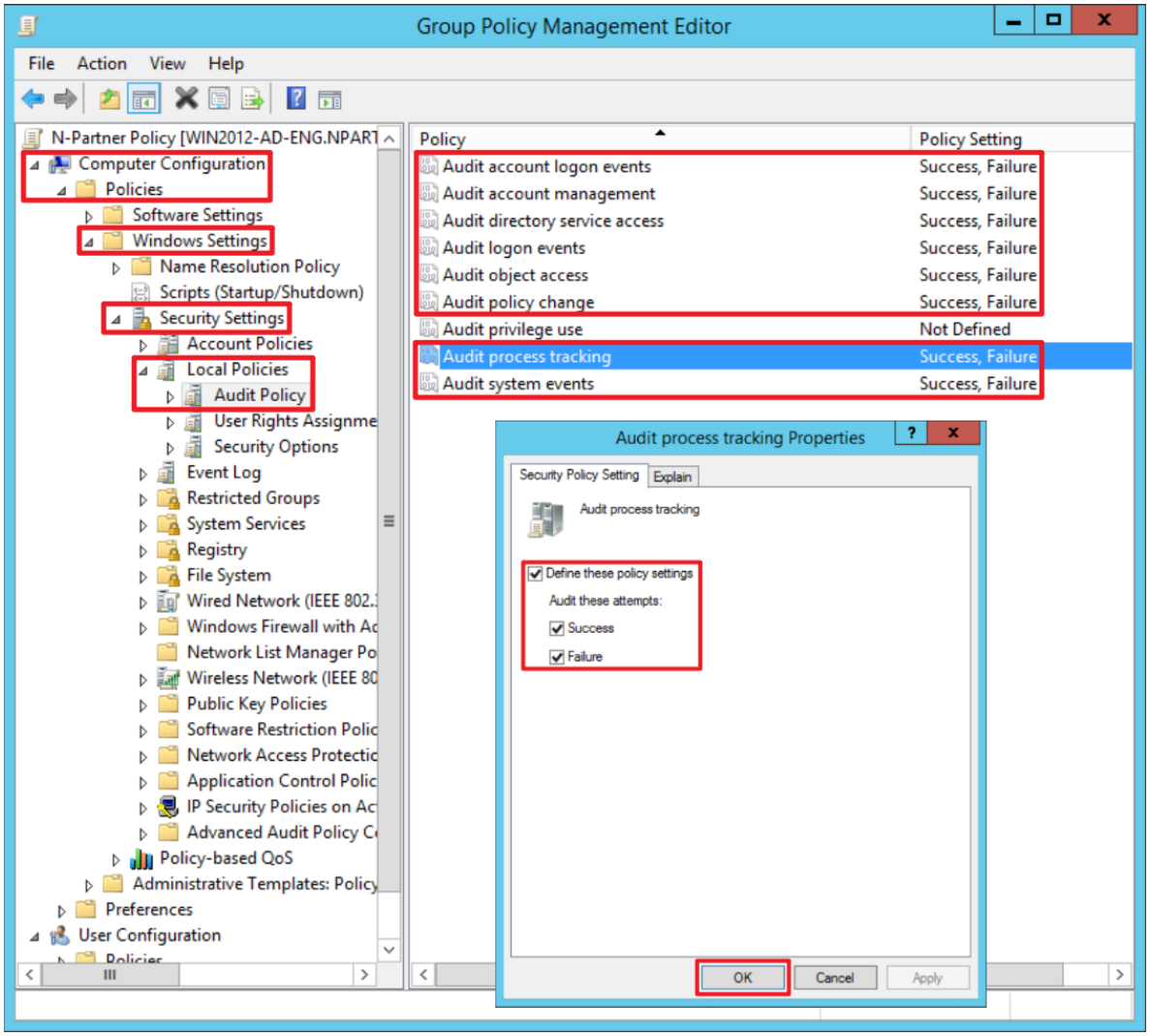
(4) Edit your Group Policy Object

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



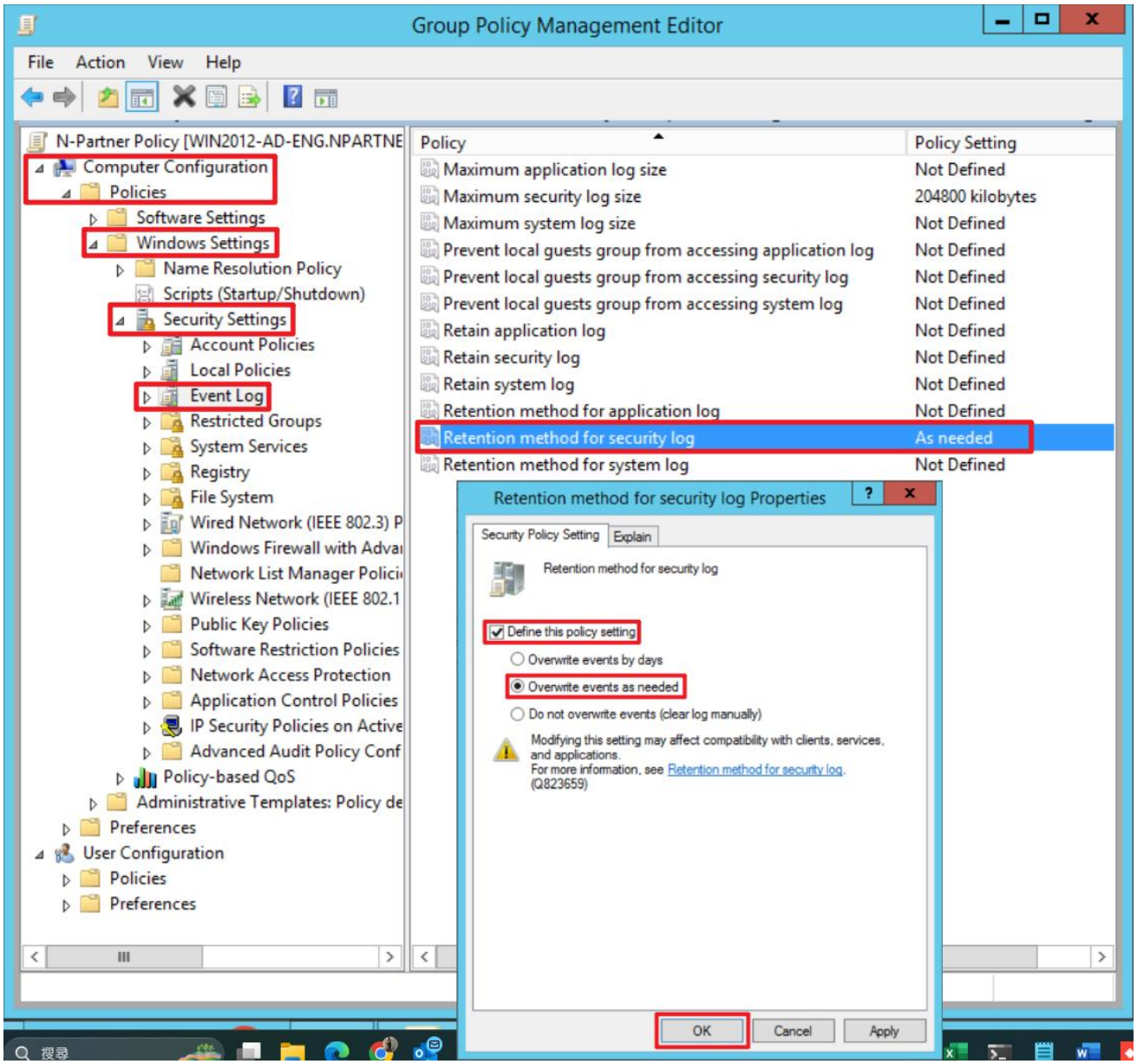
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “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” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

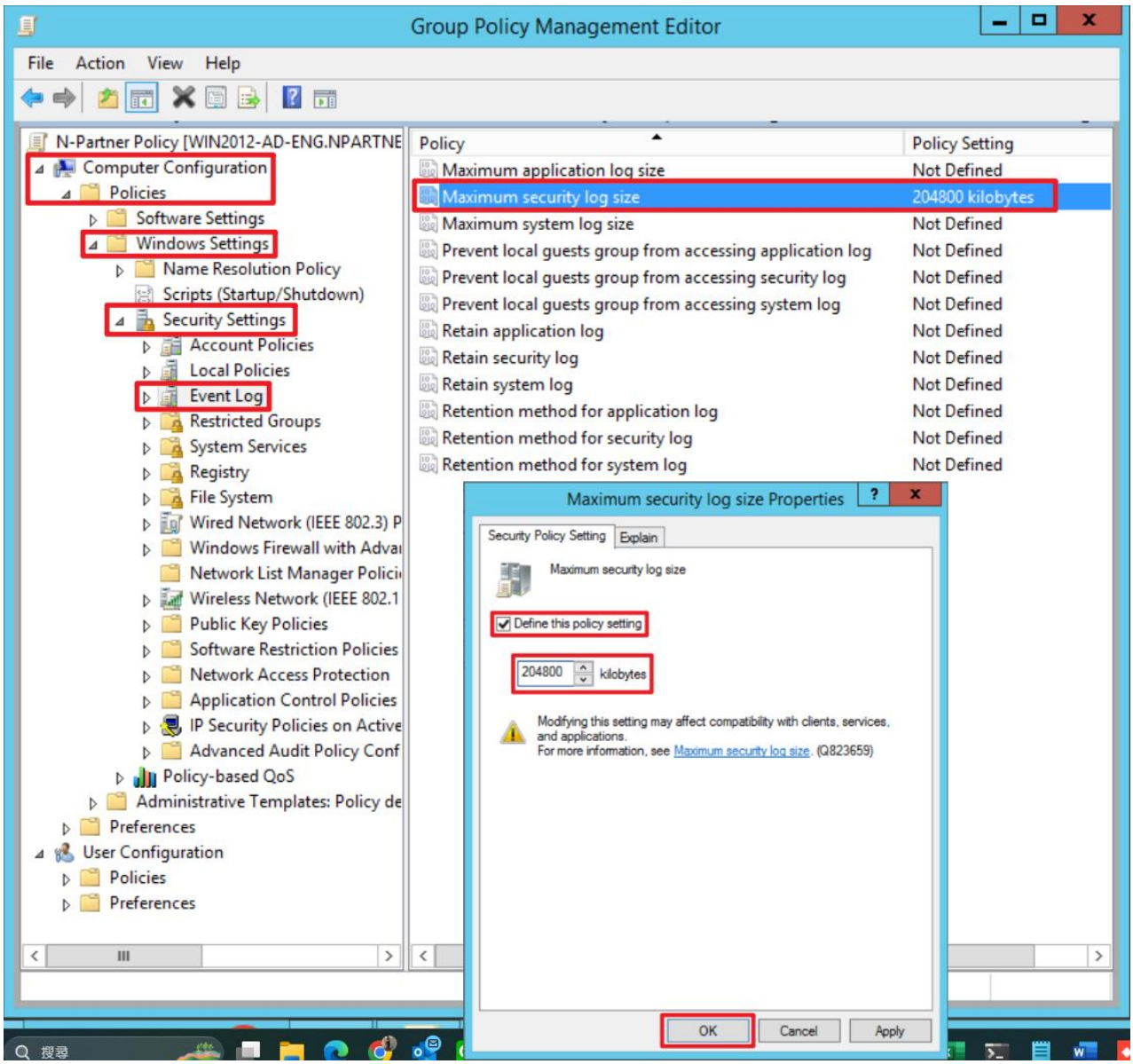
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

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

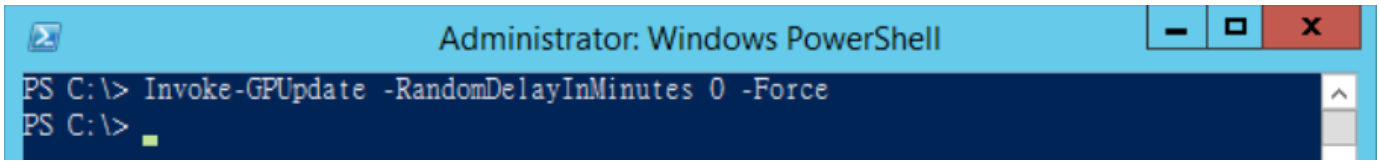
Note: Please adjust the number based on the actual environment. → click “OK.”



(8) On the AD domain server, open “Windows PowerShell.”

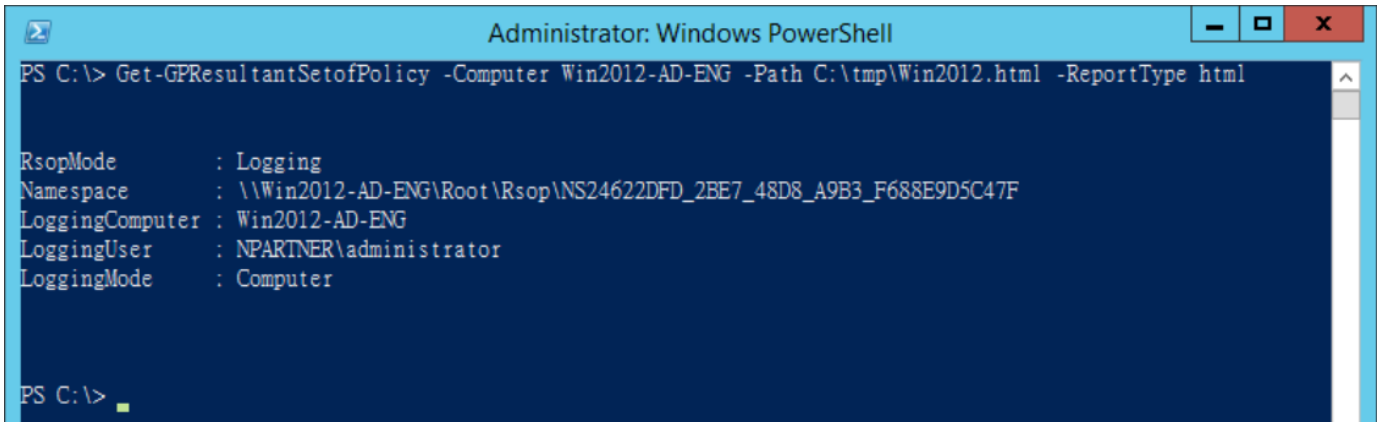
(9) Enter the command below to refresh group policy.

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



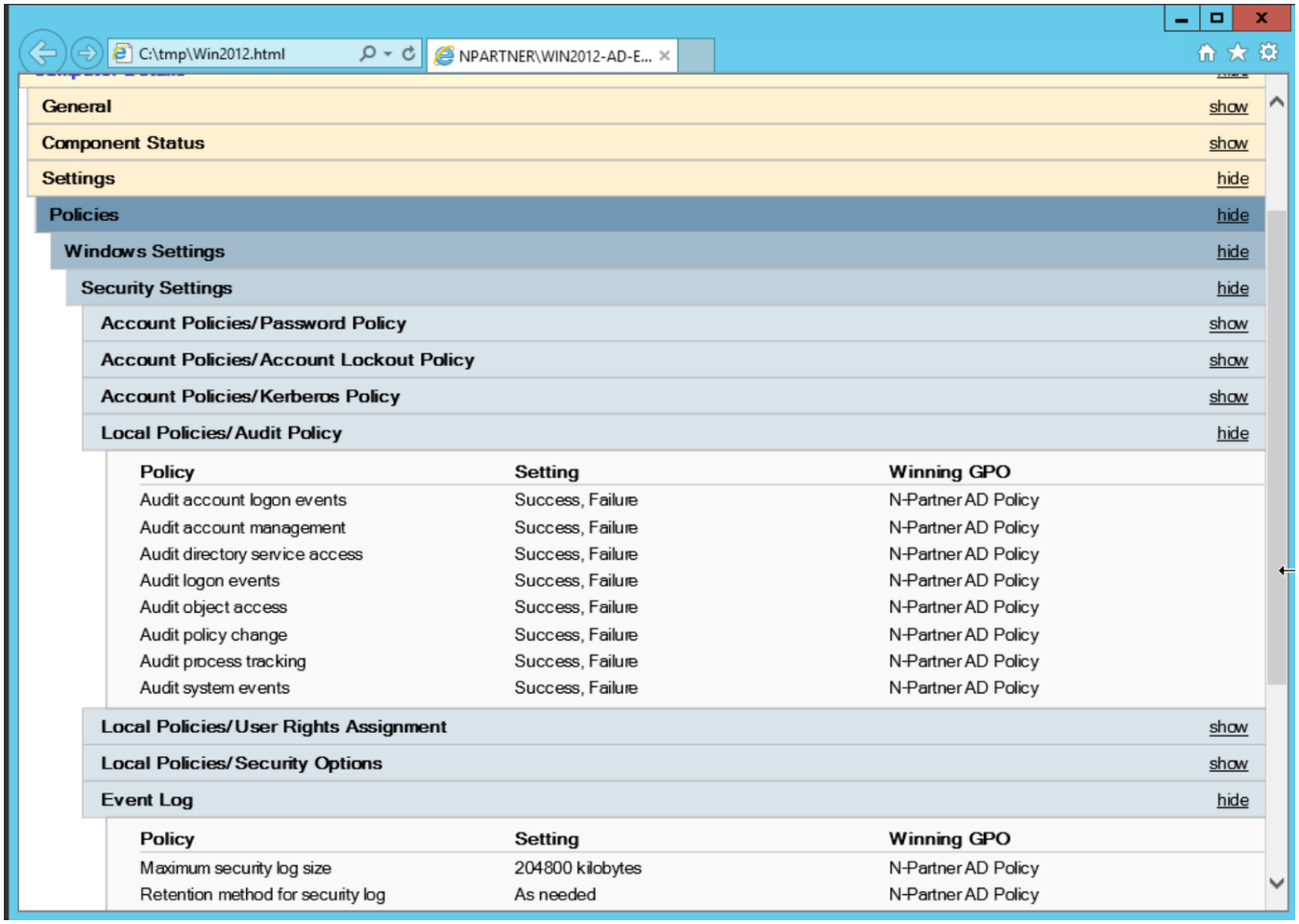
(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2012-AD-ENG -Path C:\tmp\Win2012.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.

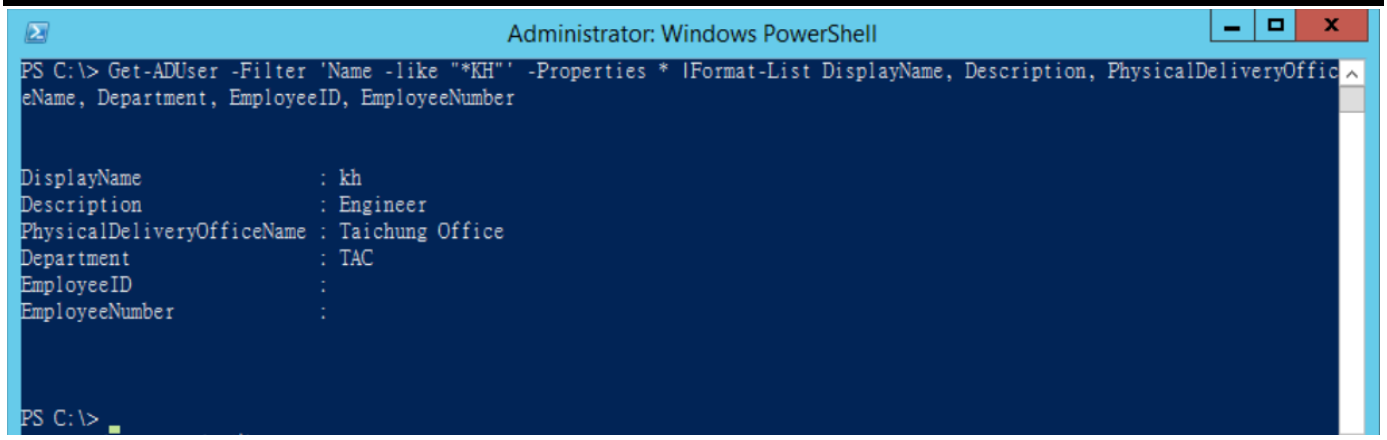


5.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Enter the command below to check whether N-Reporter associates Windows AD with available user data.

```
PS C:\> Get-ADUser -Filter 'Name -like "*KH"' -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



Replace the red text with the username according to the actual environment.

(2) In “Event Query,” click the information of “Username.”

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartne	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

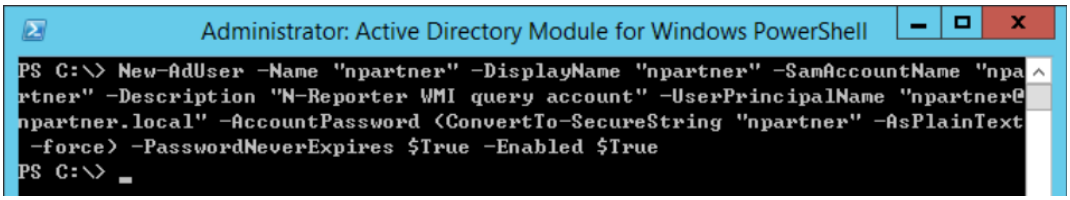
5.3.1 Add Non-Admin Accounts

(1) Open “Active Directory Module for Windows PowerShell.”

(2) Create an Account

Enter the command below to create an account:

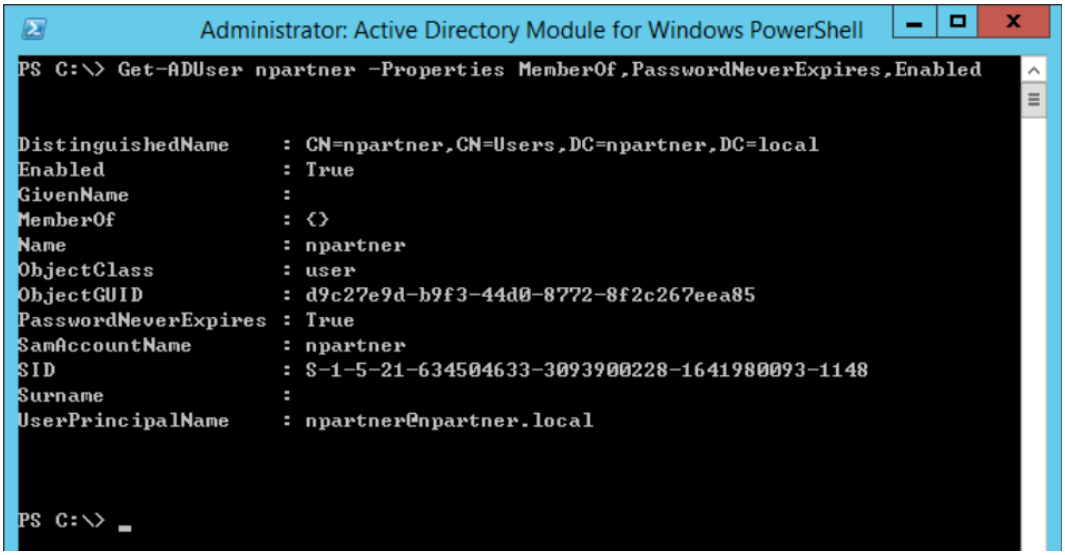
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description
"NReporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

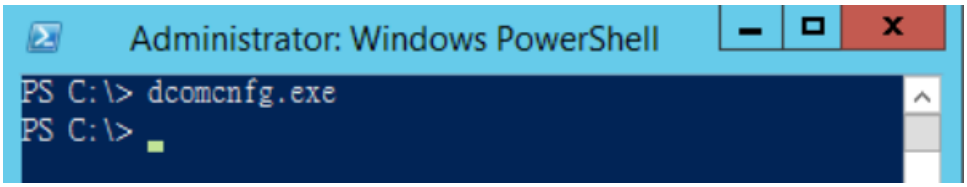


5.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”

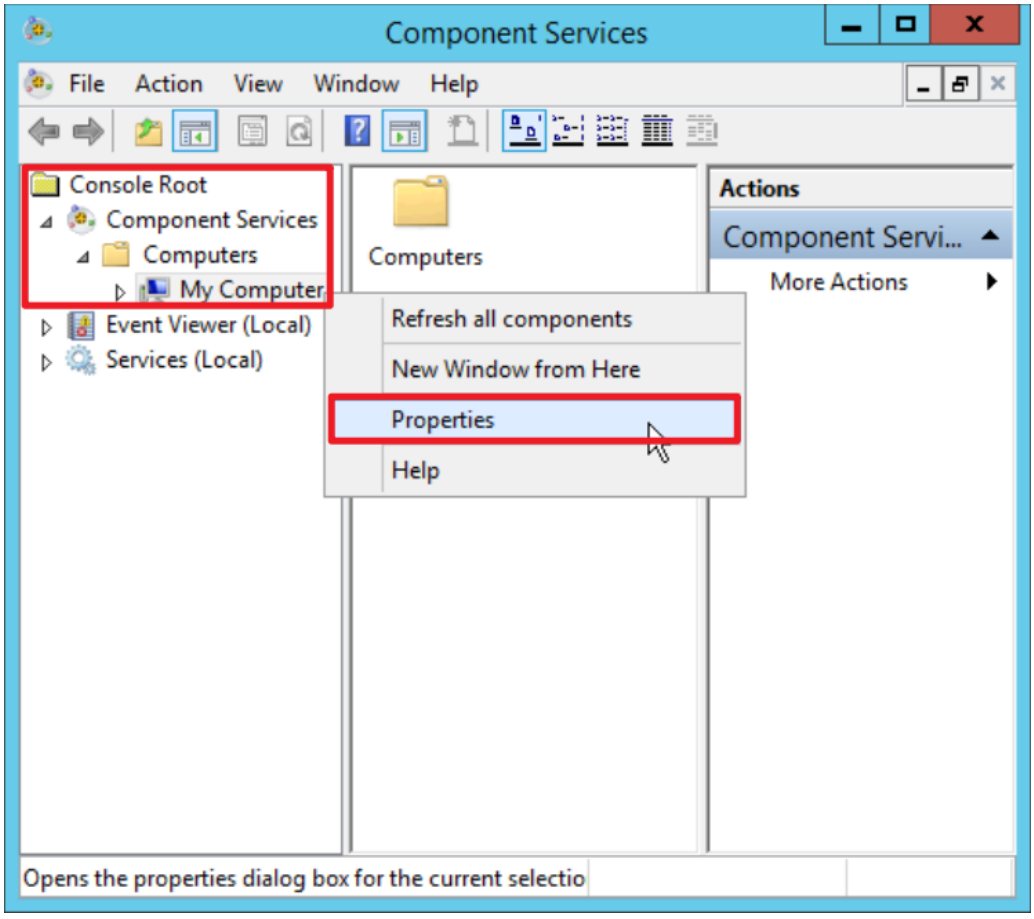
(2) Enter the command below to enable component services.

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



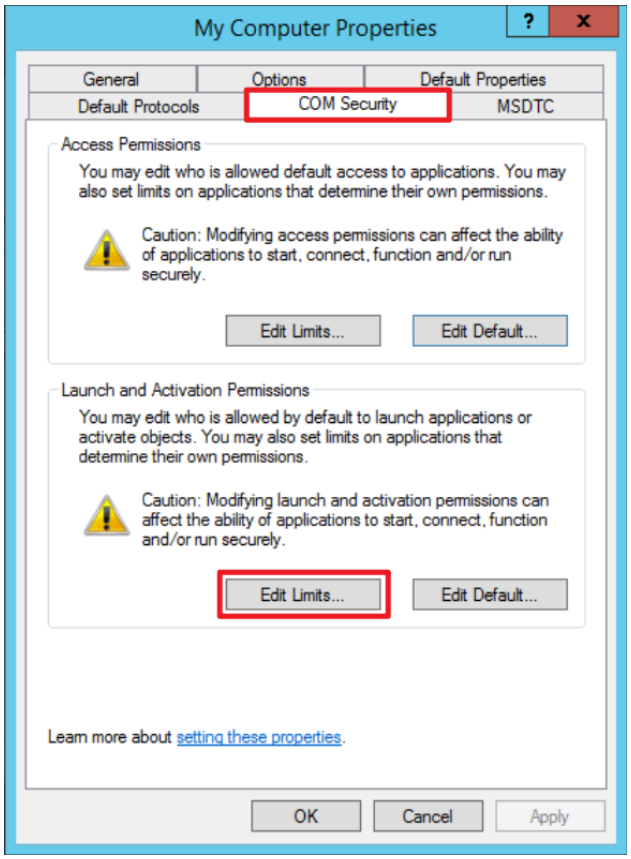
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



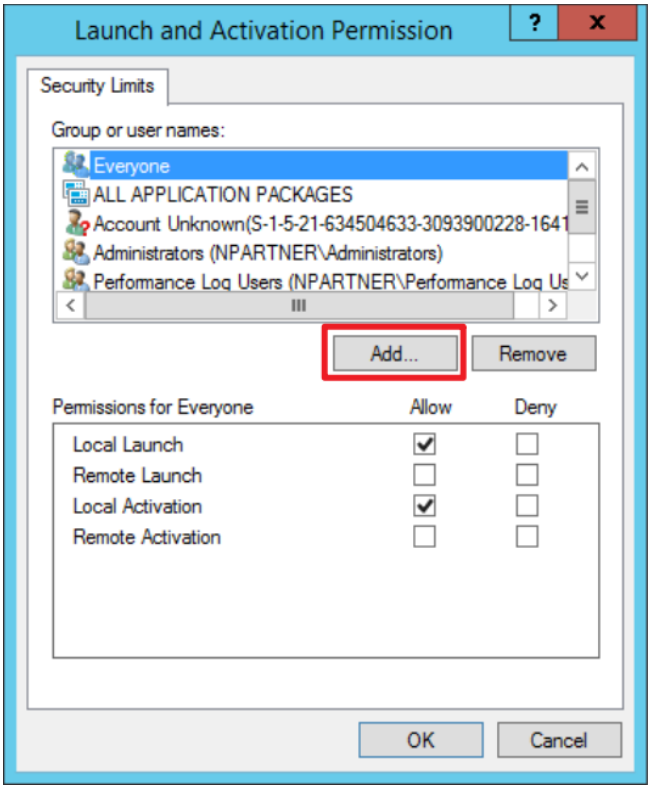
(4) Enable Permissions

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



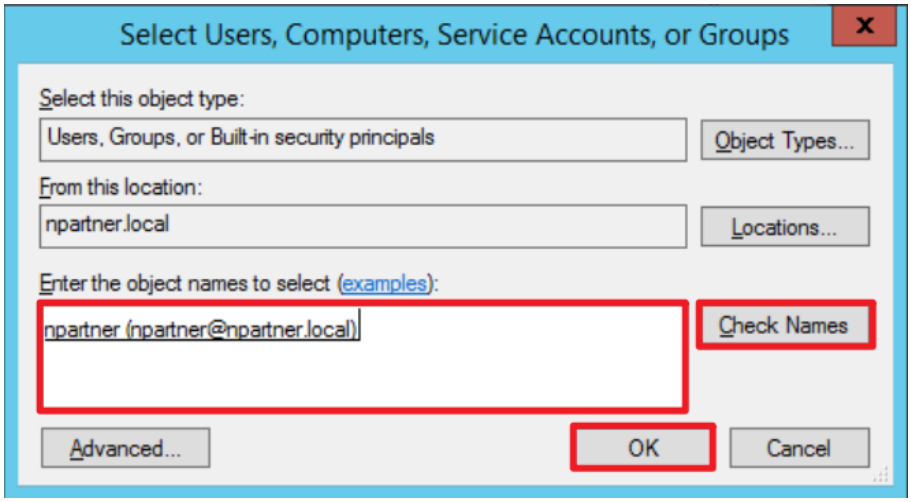
(5) Add DCOM User Permissions

Click “Add.”



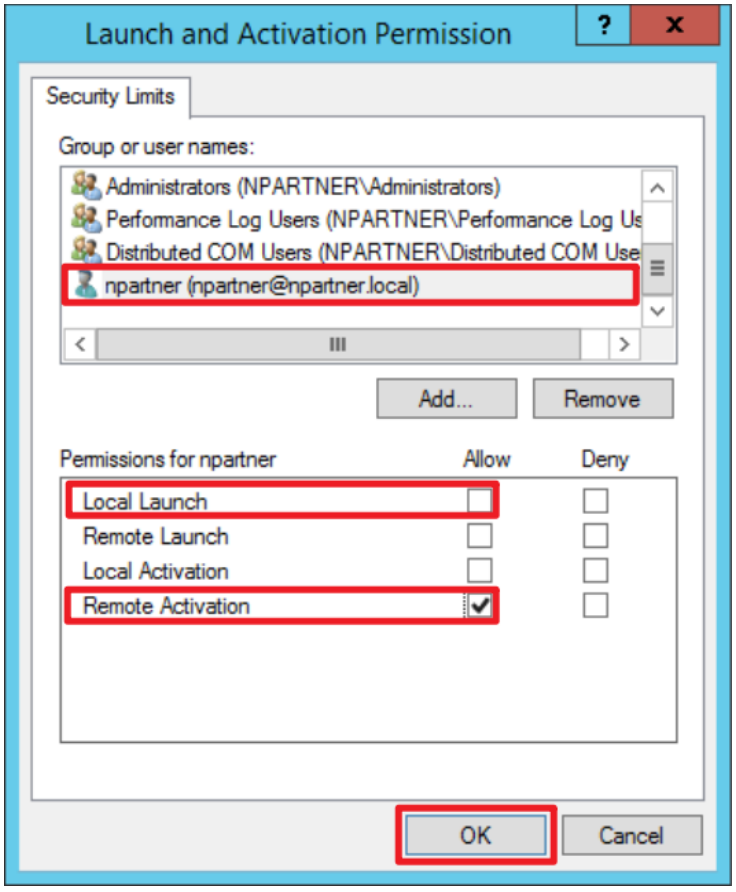
(6) Enter Your Username

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

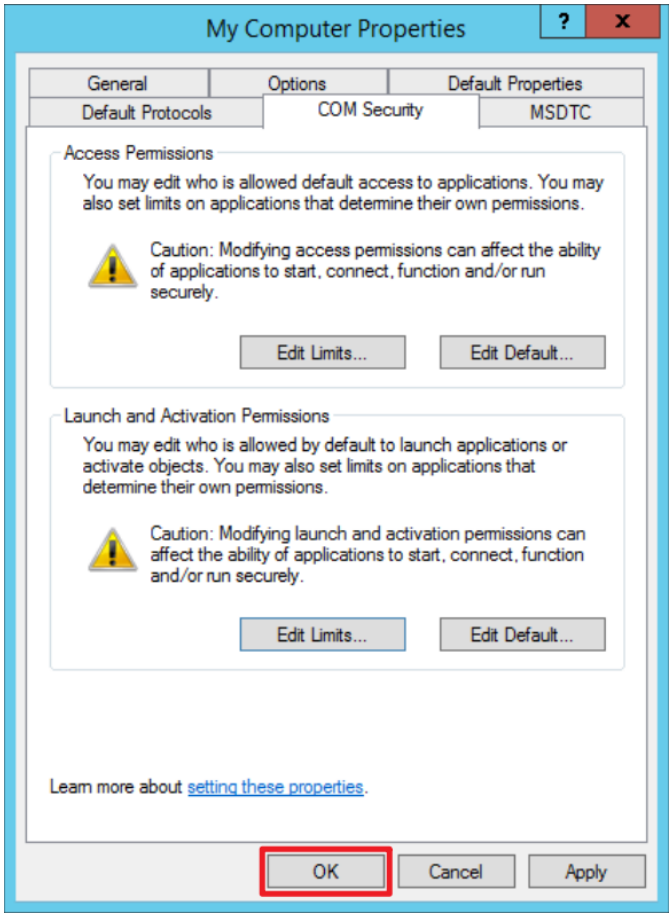


(7) Configure your User Permission

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



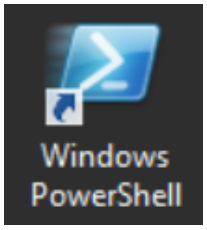
(8) Click "OK."



5.3.3 Configure WMI Permissions

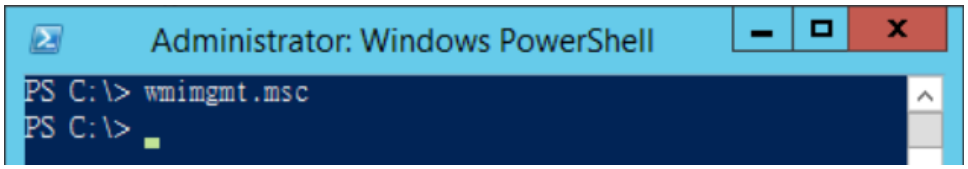
5.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



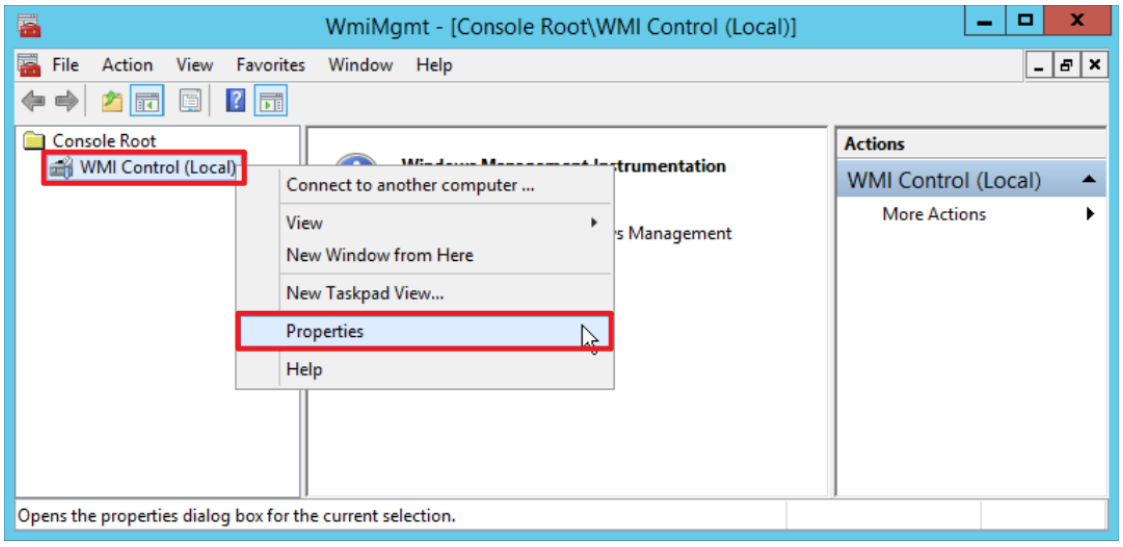
(2) Enter the command to enable WMI control service.

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



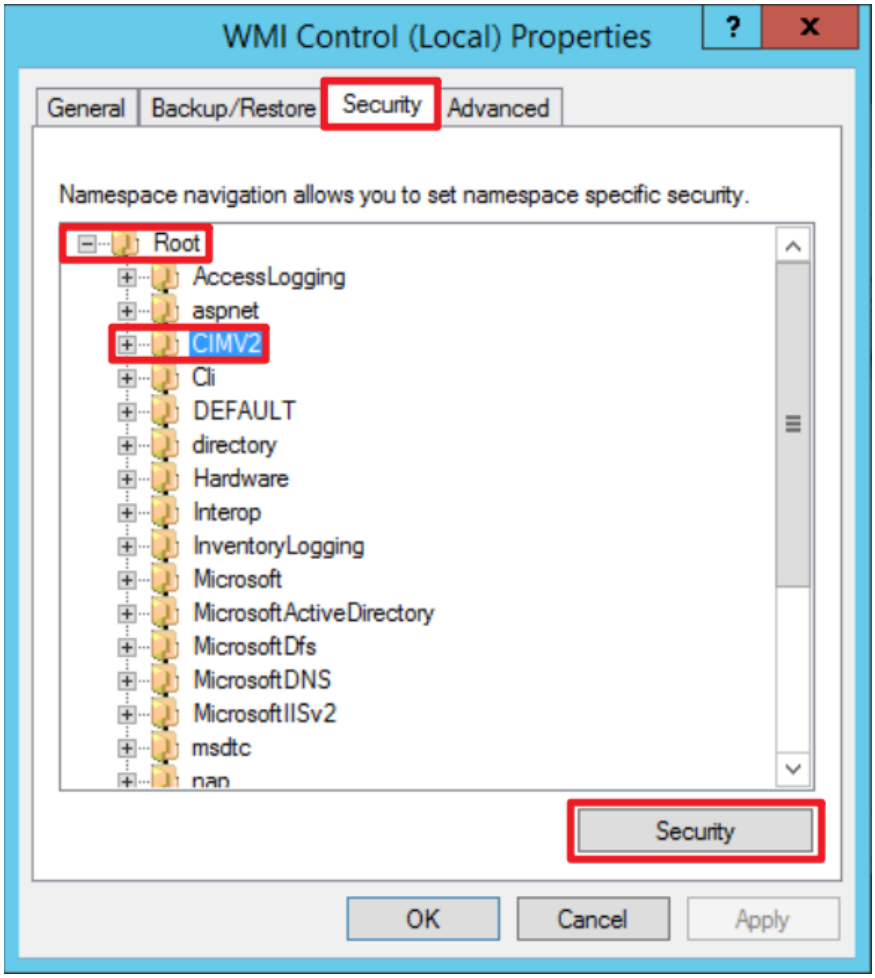
(3) Edit WMI Control

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



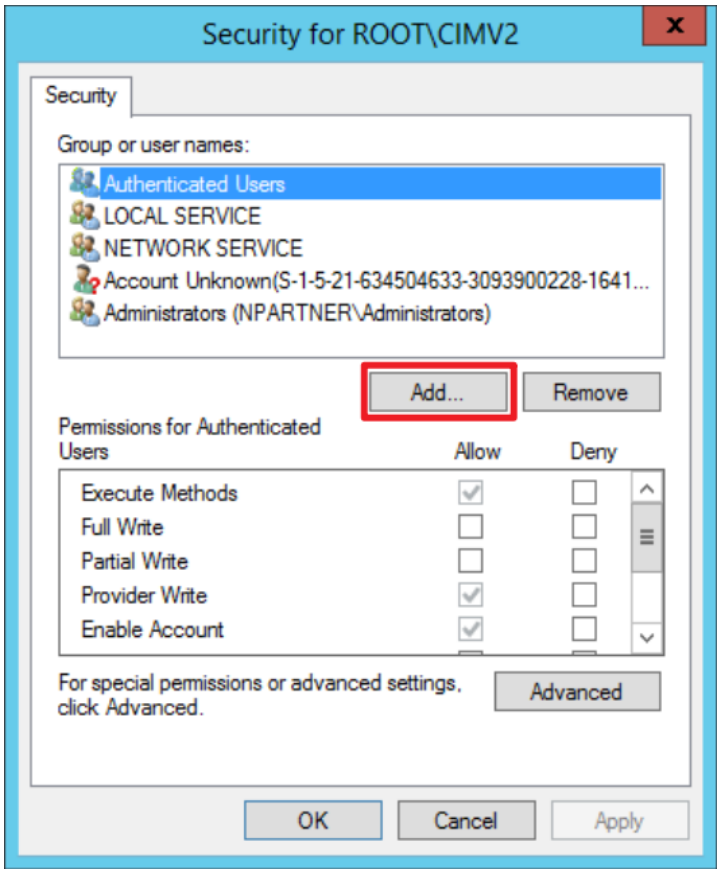
(4) Edit CIMV2 Security

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



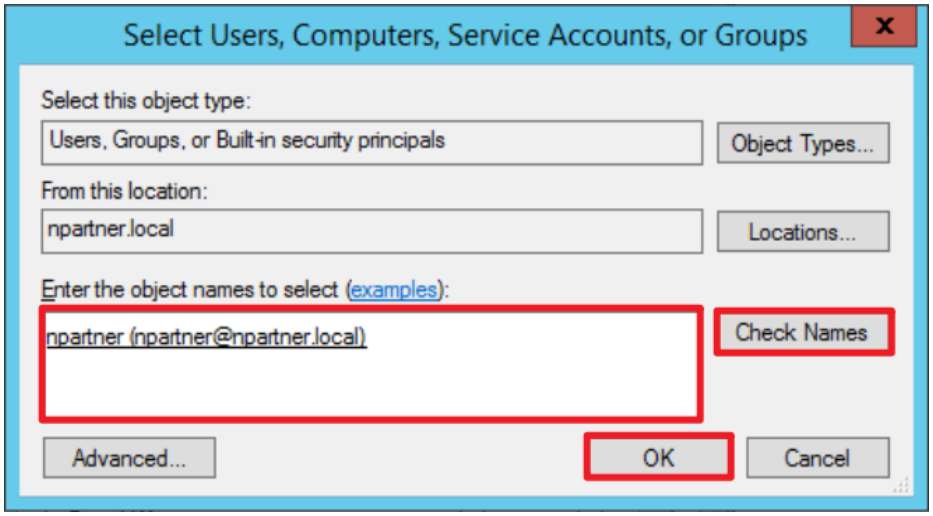
(5) Add WMI User Permissions.

Click “Add.”



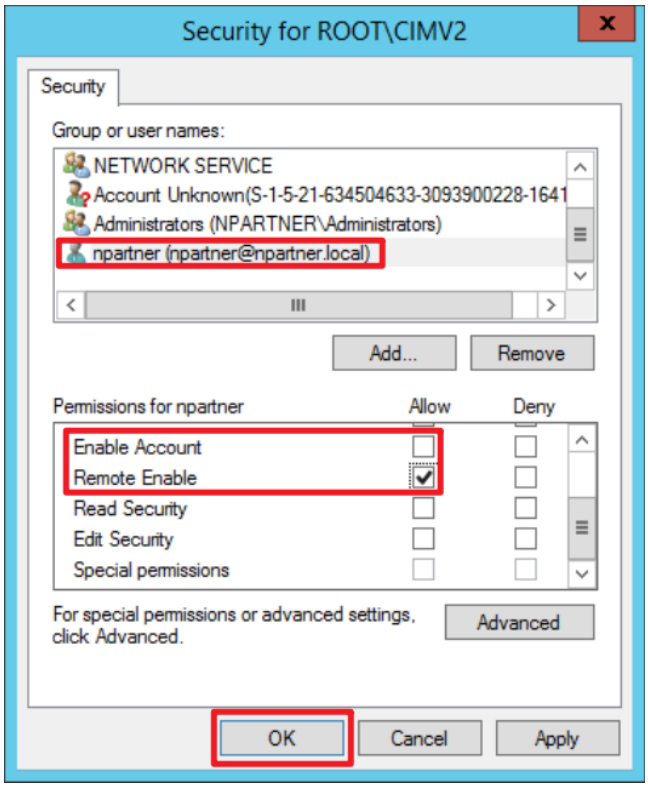
(6) Enter Your Username

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

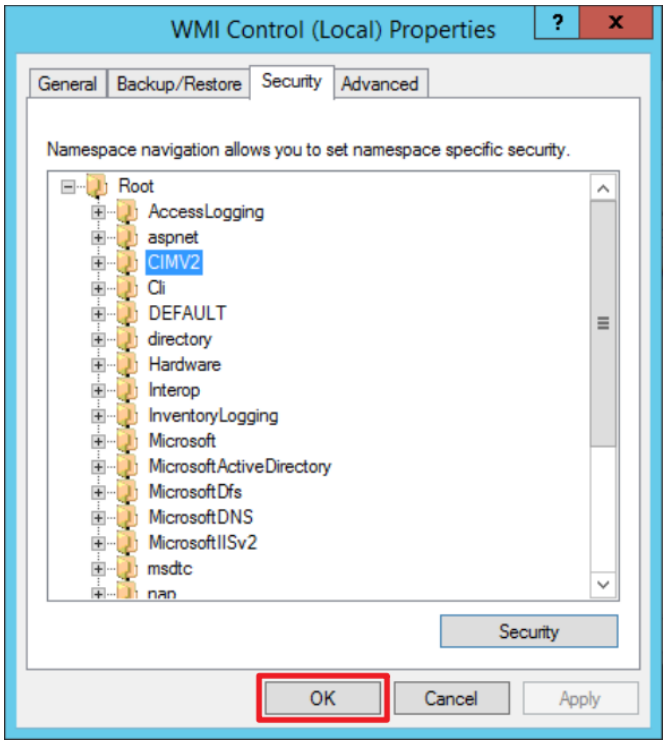


(7) Set Your User Permissions

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

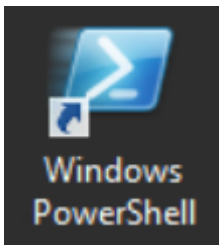


(8) Click “OK.”



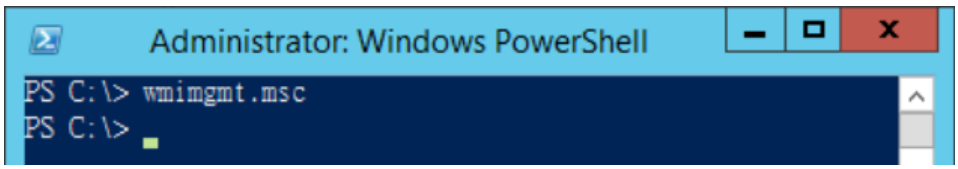
5.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



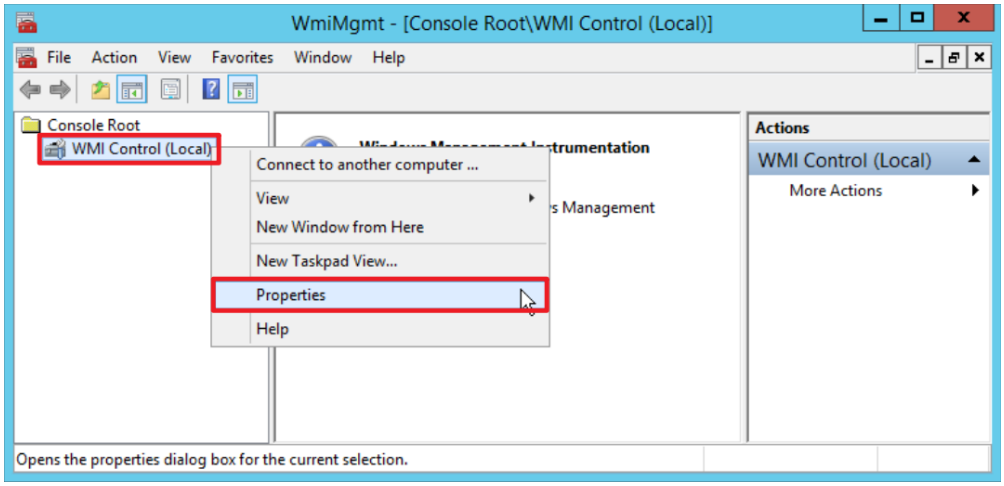
(2) Enter the command below to enable WMI Control.

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



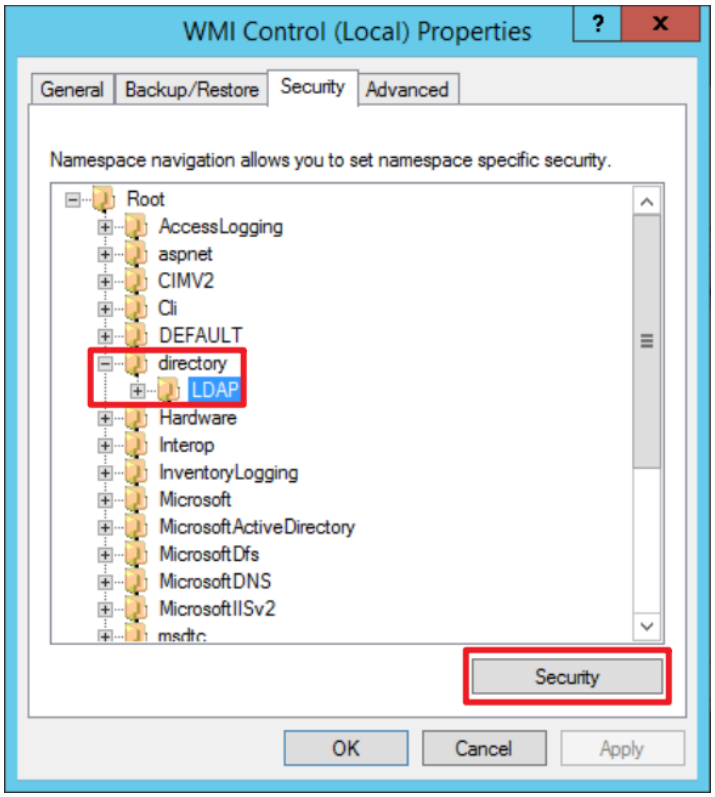
(3) Edit WMI Control

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



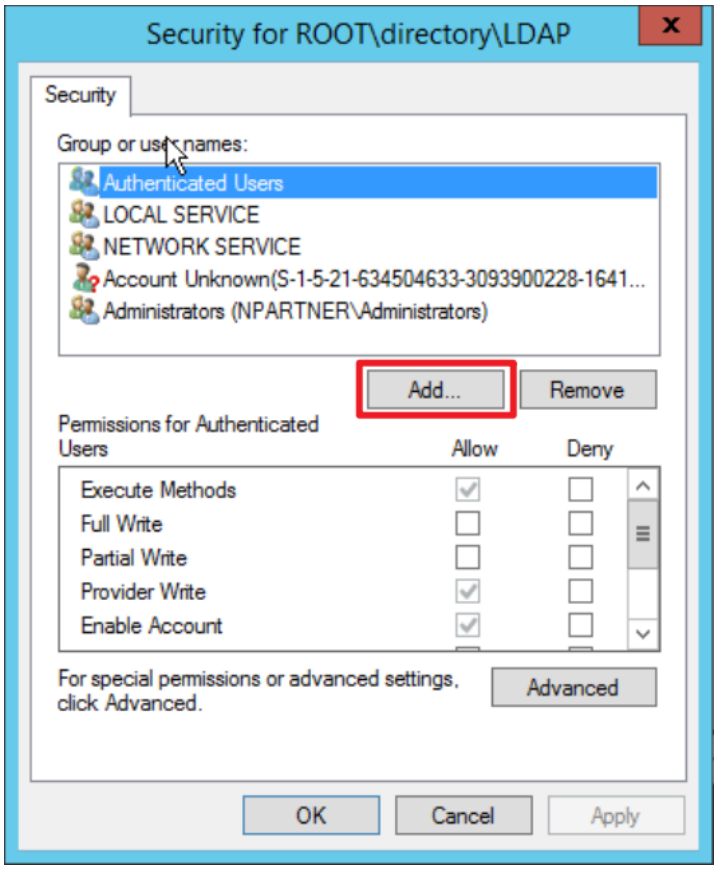
(4) Edit LDAP Security

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



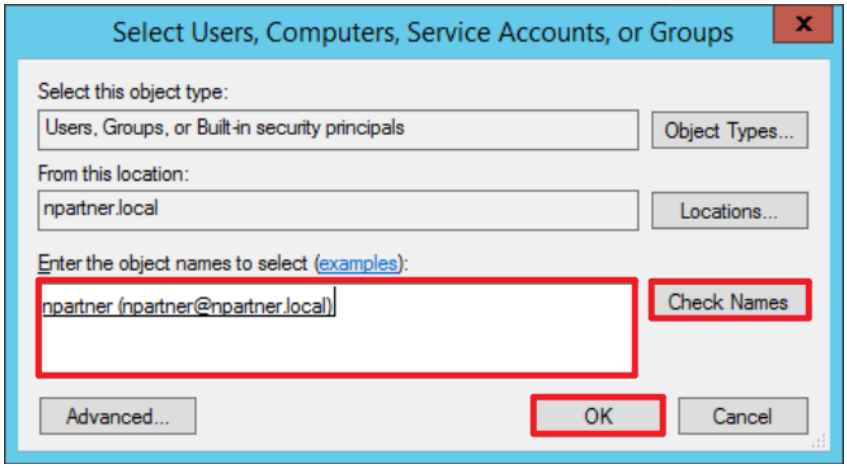
(5) Add WMI User Permissions

Click “Add.”



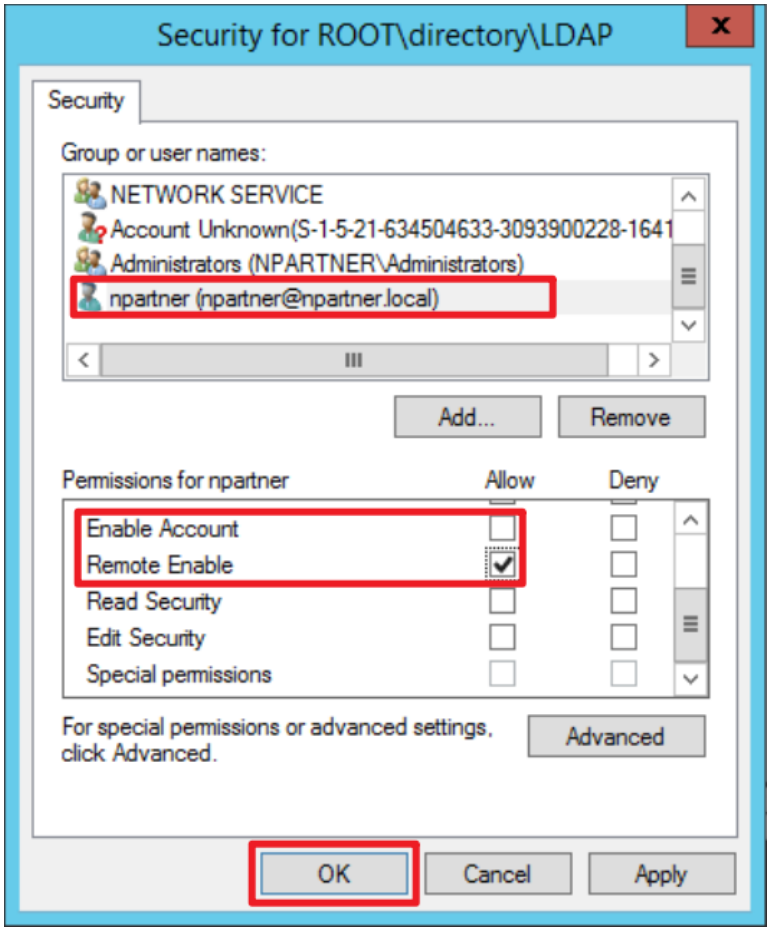
(6) Enter Your Username

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

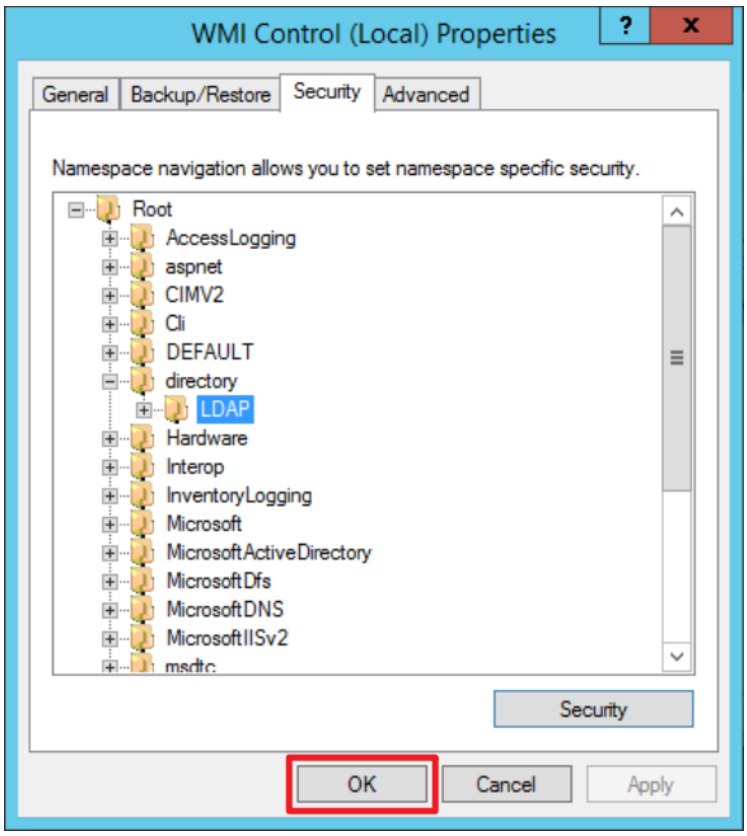


(7) Set Your User Permissions

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

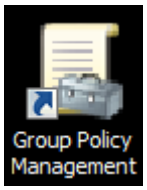


(8) Click “OK.”

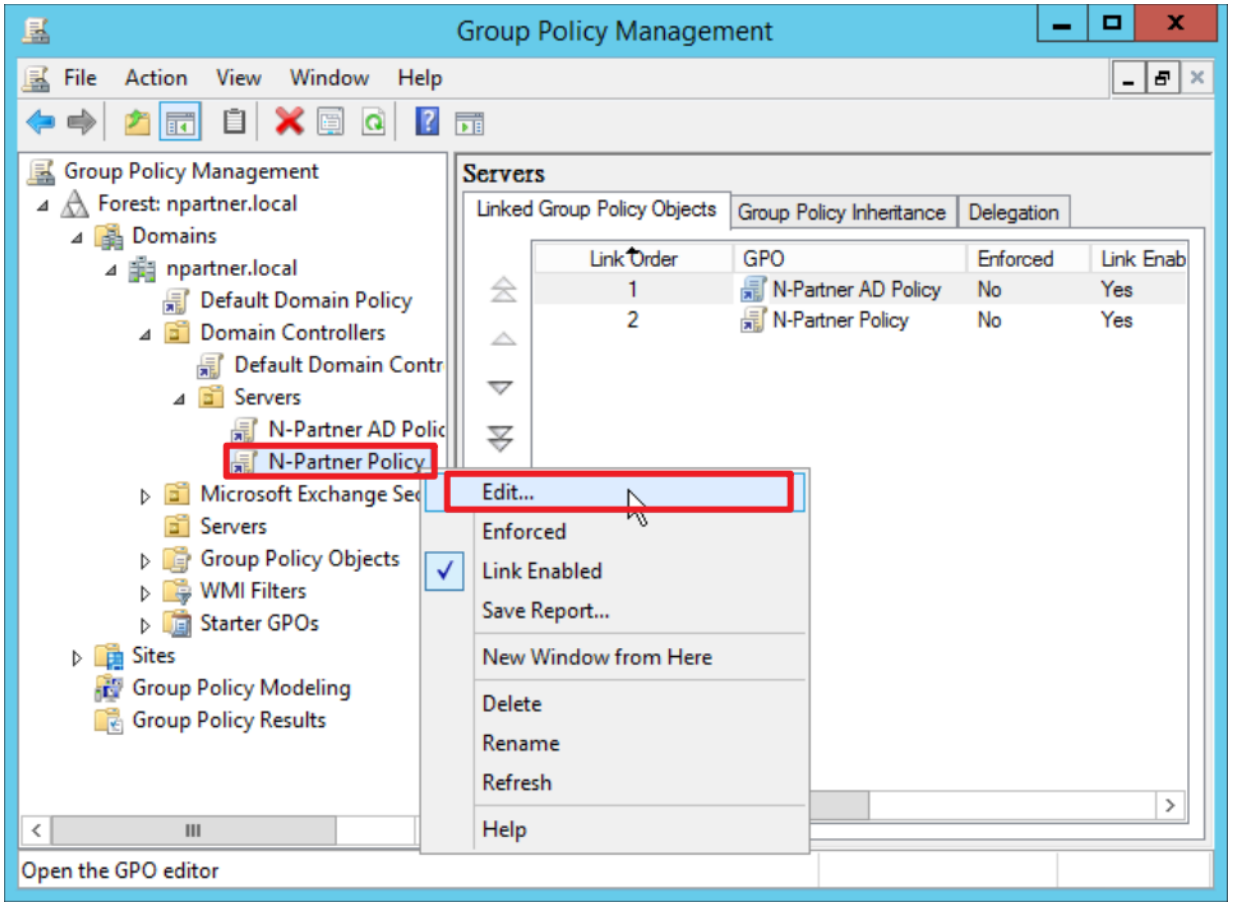


5.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

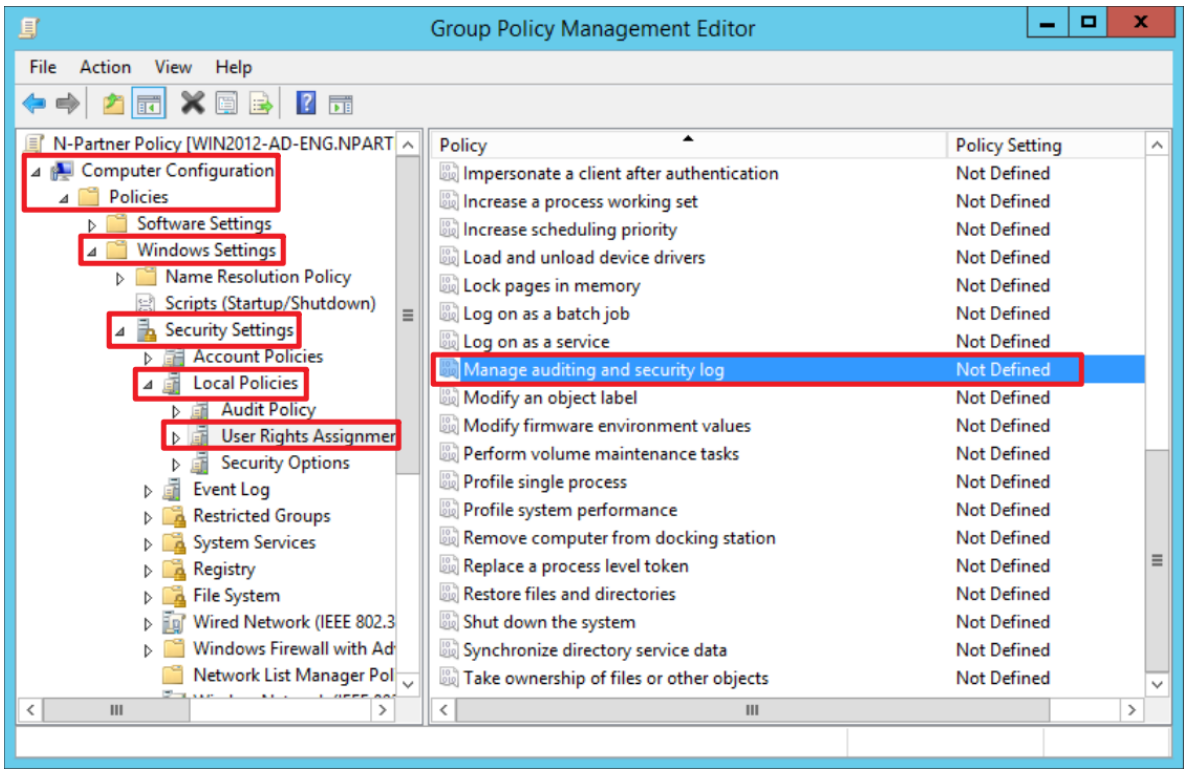


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



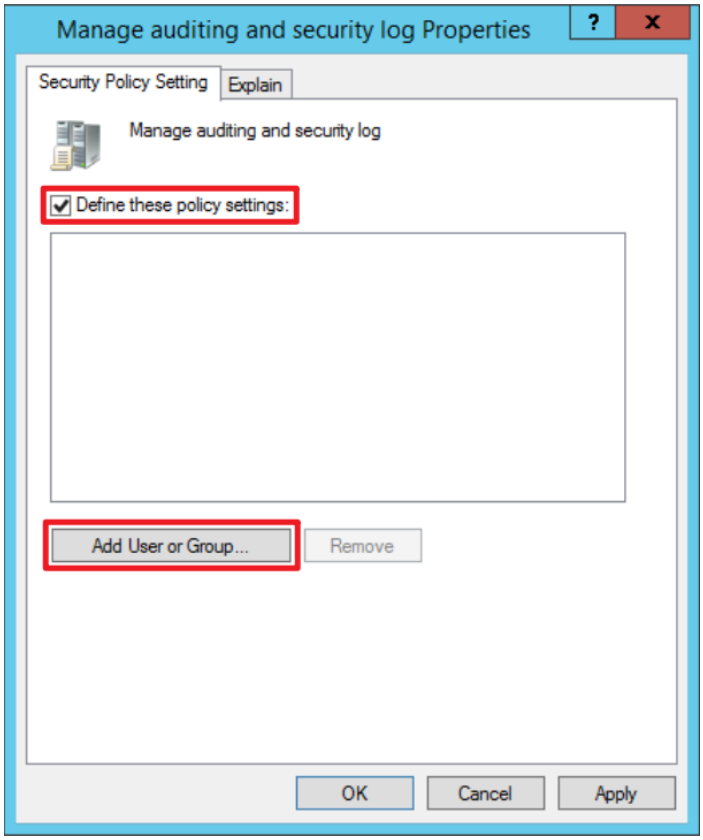
(3) Configure Auditing Log

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



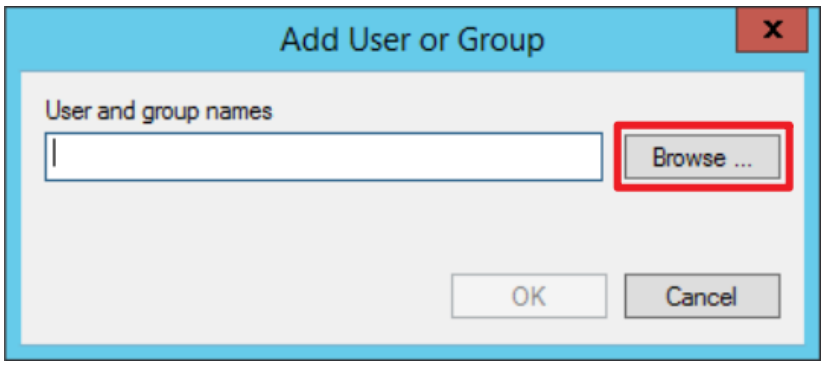
(4) Add Auditing User

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



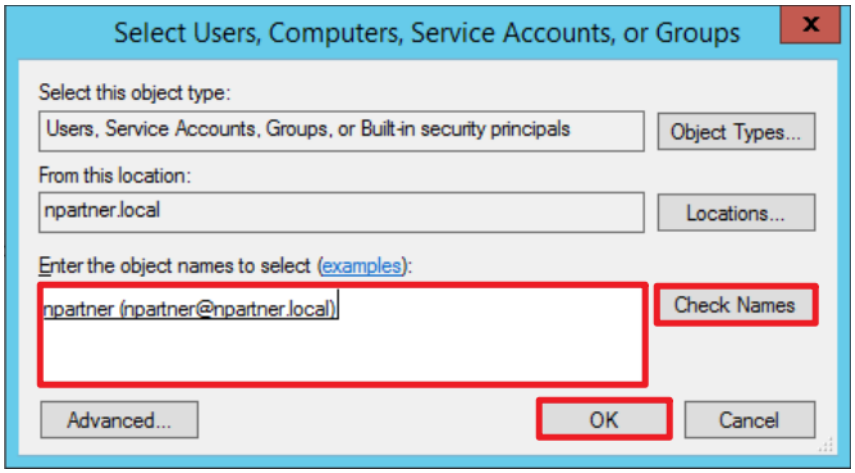
(5) Search for User

Click “Browse.”

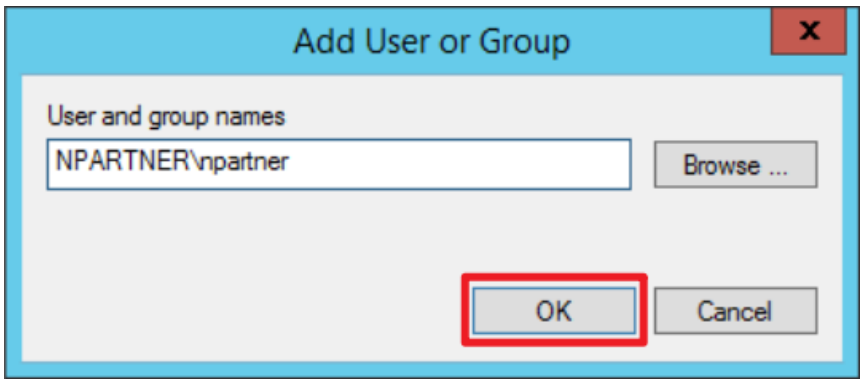


(6) Enter Your User Account

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

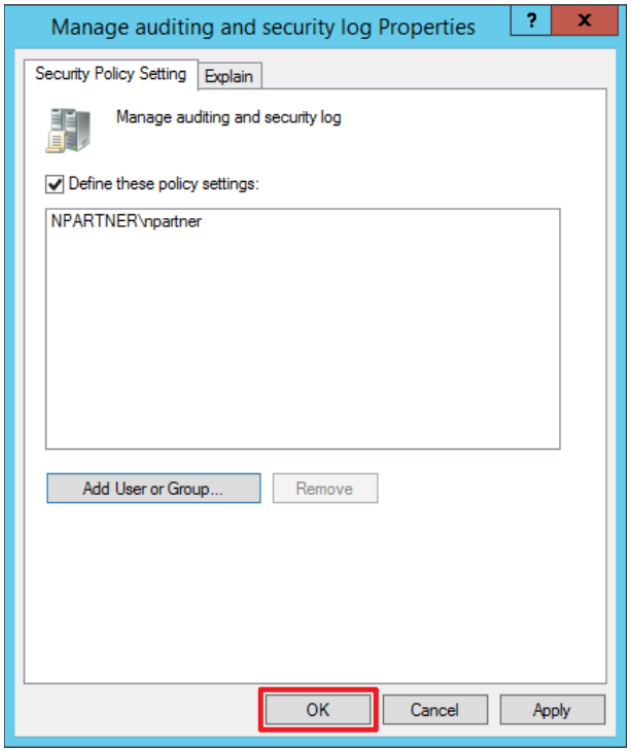


(7) Click “OK.”

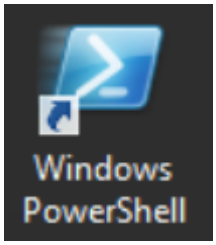


(8) Confirm Audit Log Settings

Click “OK.”

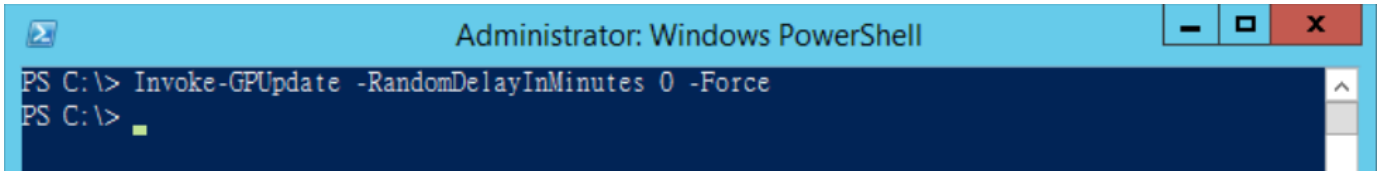


(9) Open “Windows Powershell.”



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

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

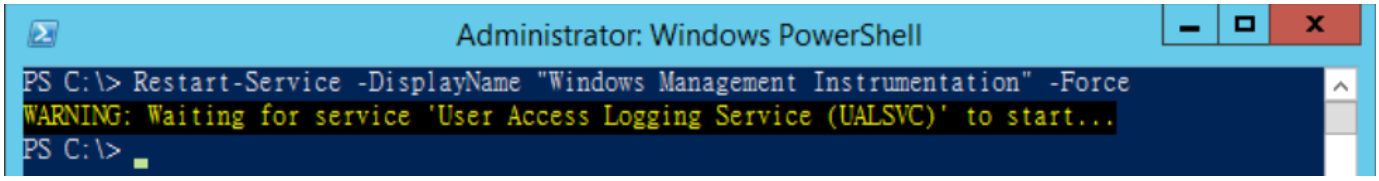


5.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”

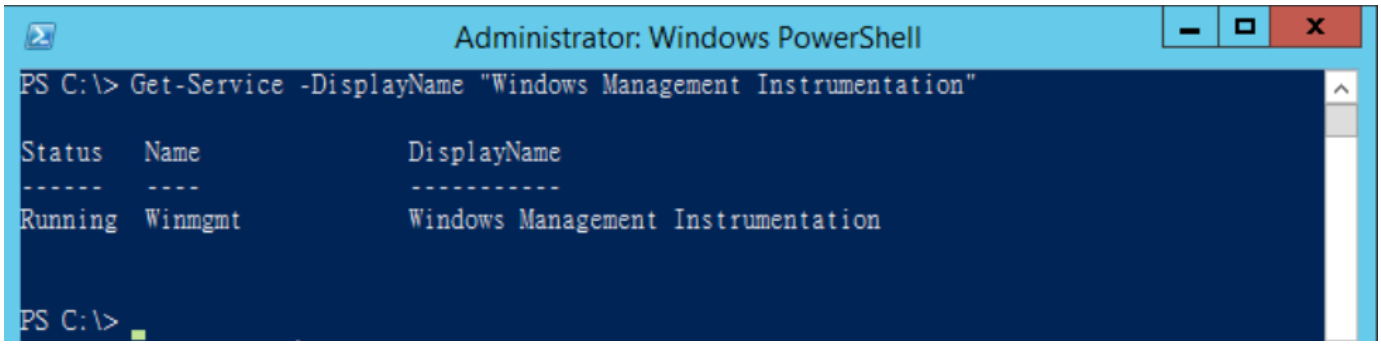
(2) Enter the command below to disable the WMI service.

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



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

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

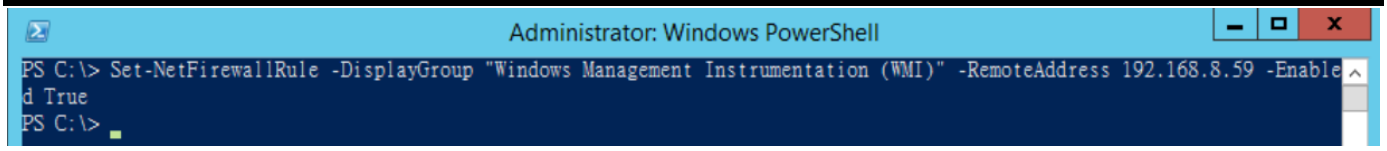


5.3.6 Configure the Firewall

(1) Open “Windows Powershell.”

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

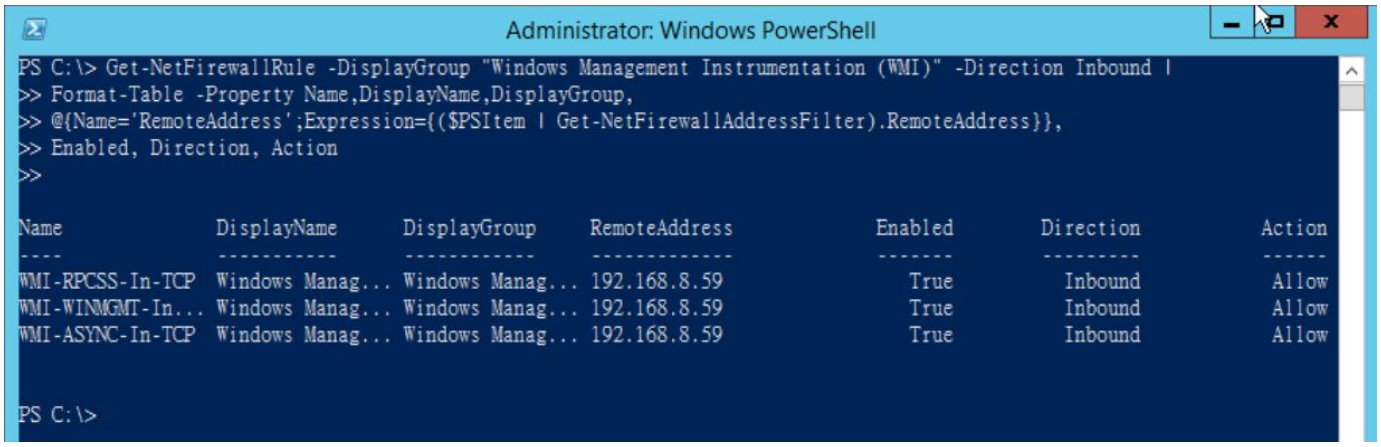
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.59 -Enabled True
```



Replace the red text with the N-Reporter IP address.

(3) Enter the command below to show the current firewall WMI configuration:

```
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
```



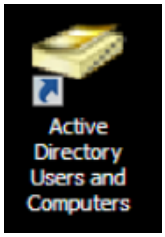
6. Windows Server 2016

Windows Audit Policy Configuration:

For detailed information, refer to the **Audit Policy Recommendations link** in the references.

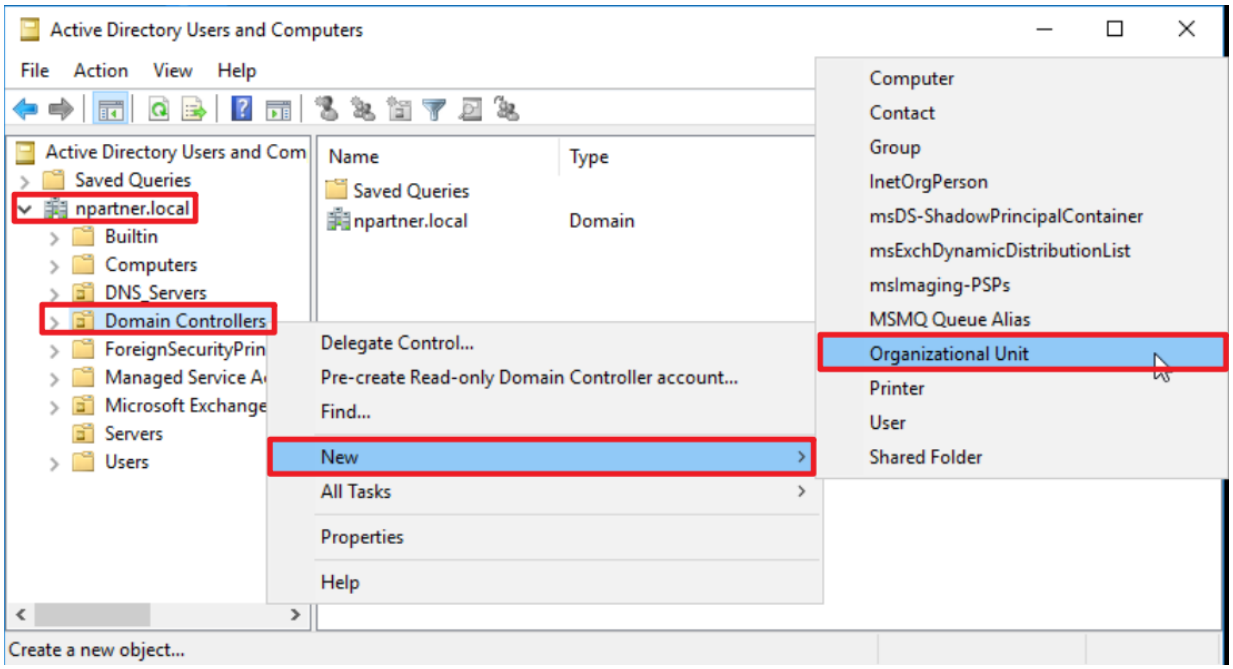
6.1 Organizational Unit (OU) Configuration

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



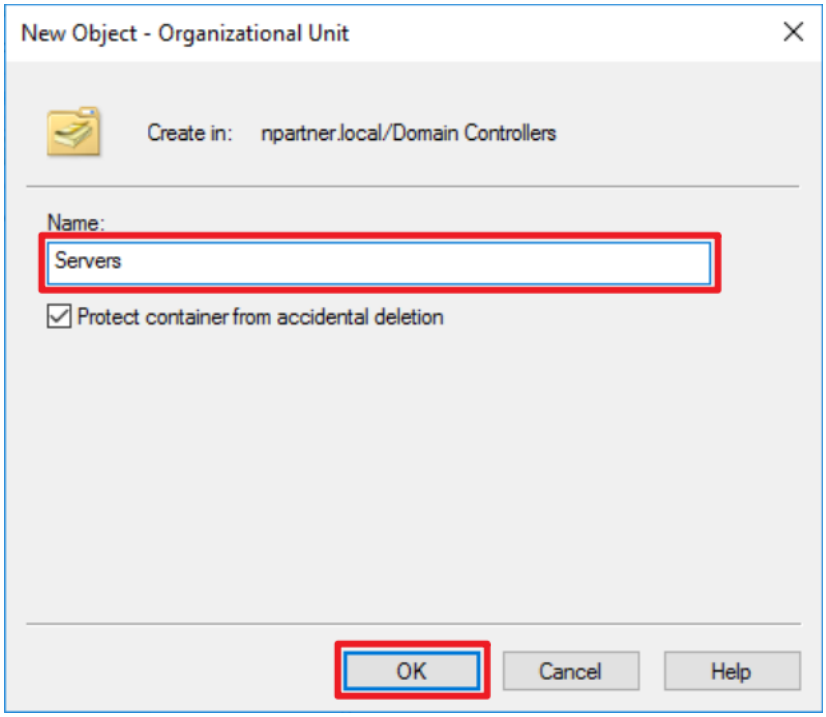
(2) Add an Organizational Unit

Right-click on the domain name (the example here is npartner.local) → select “New,” and click “Organizational Unit.”



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

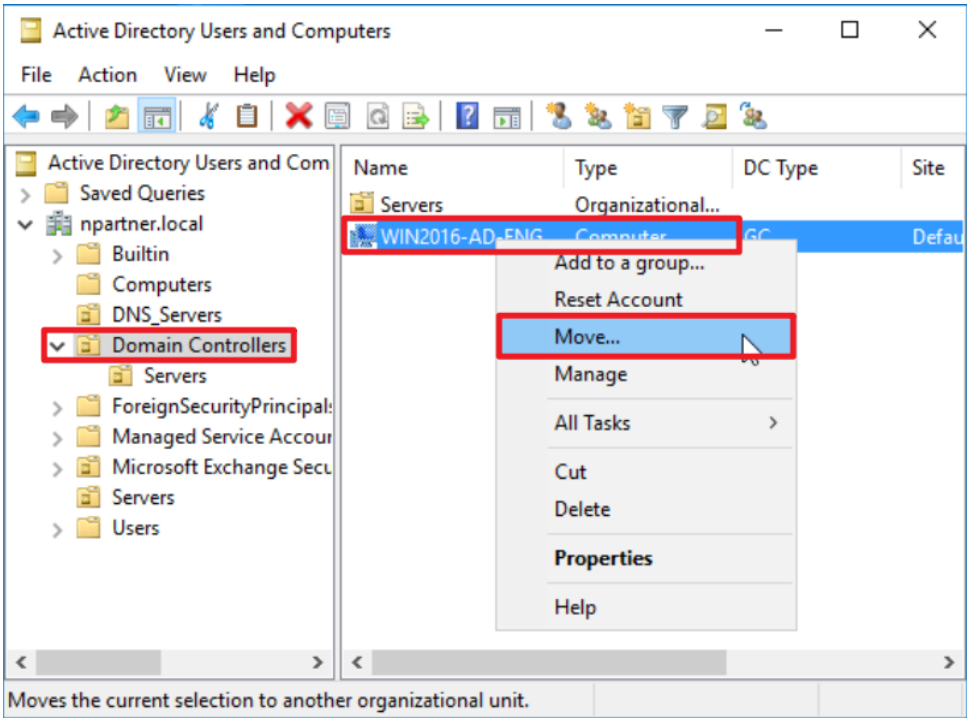
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

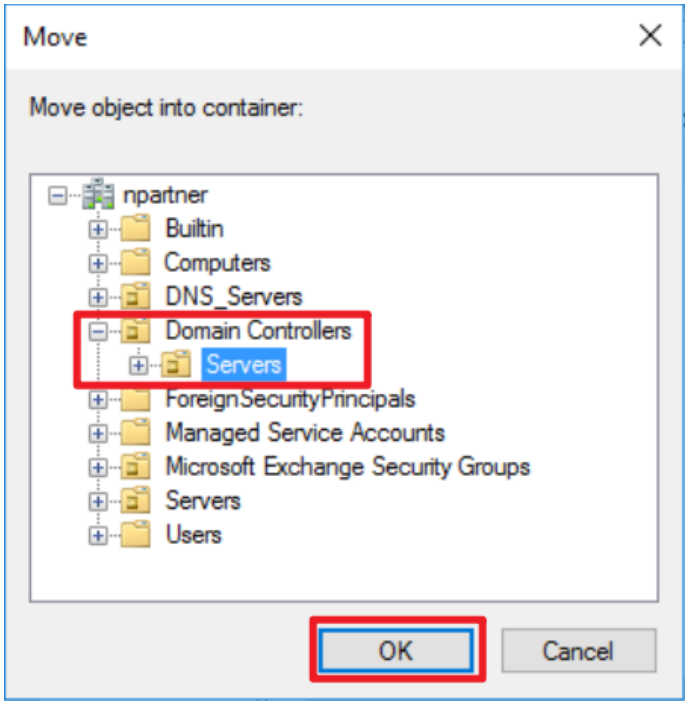
Select “Domain Controllers” → right-click on the “WIN2016-AD-ENG” server.

Note: Please select the Windows file server according to the actual environment. → click “Move.”



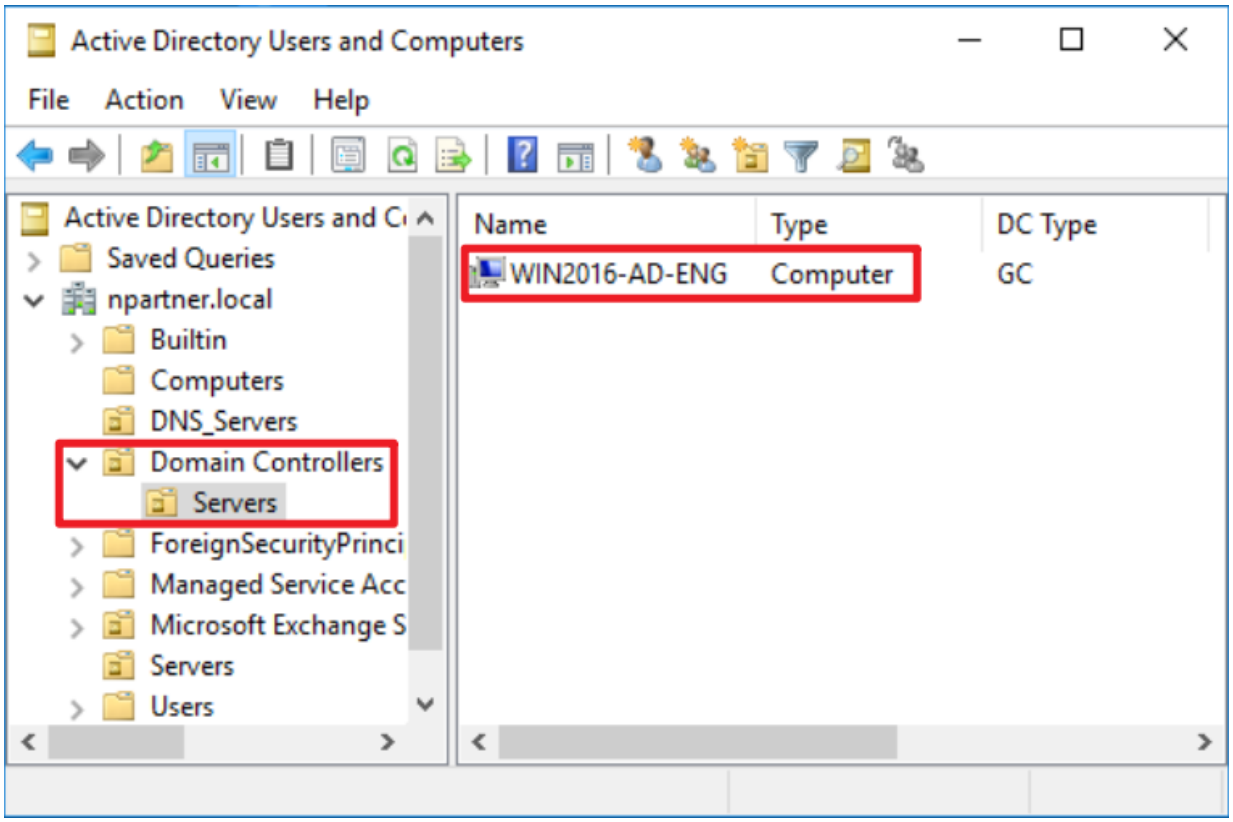
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → 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”) and confirm that the “WIN2016-AD-ENG” server has been moved.

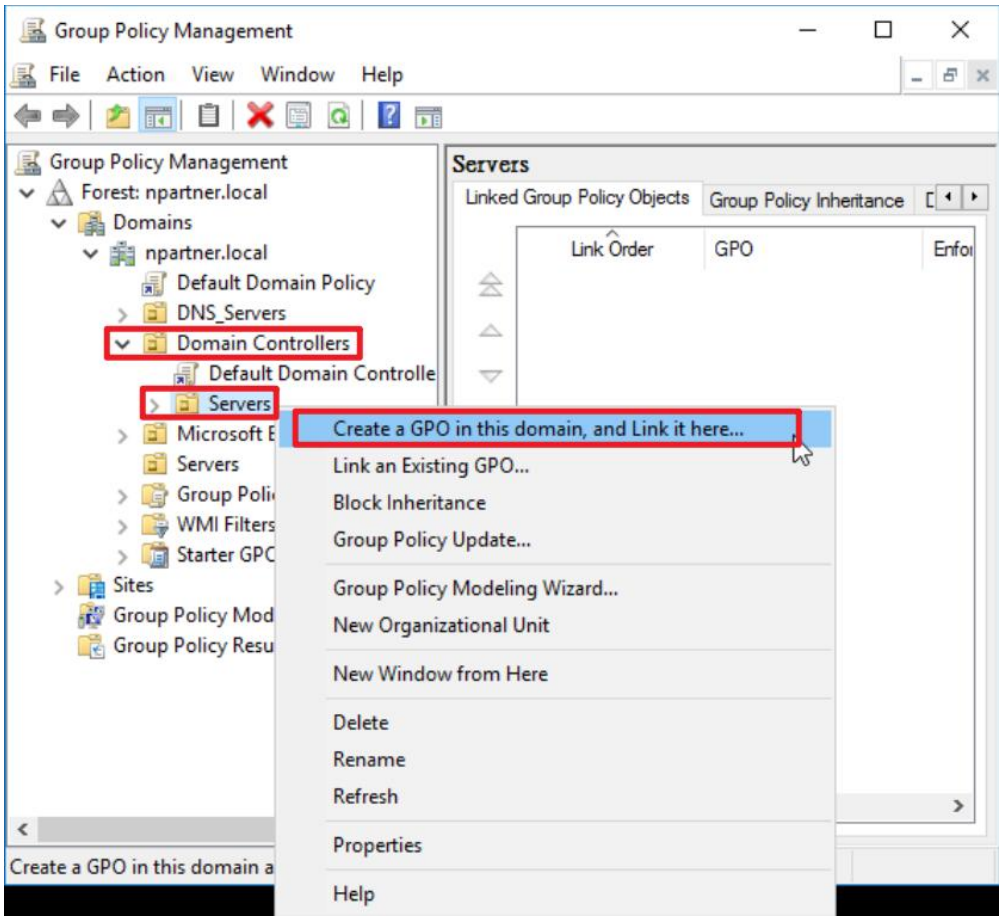


6.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

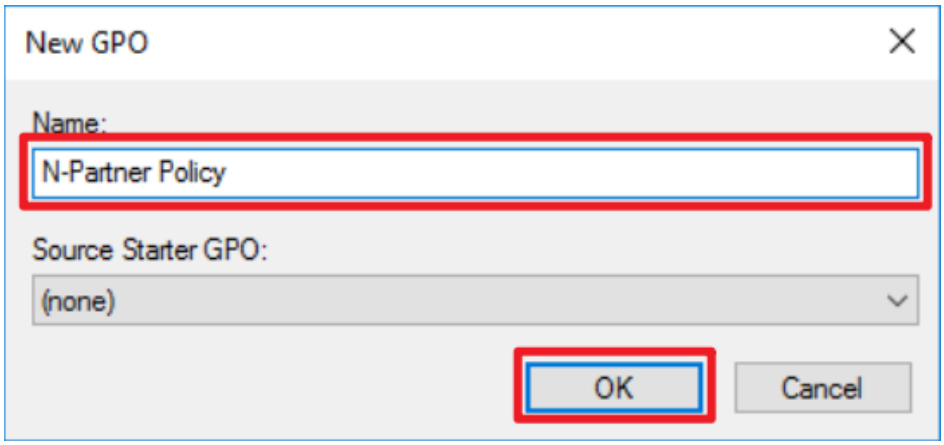
Right-click the “Servers” organizational unit under “Domain Controllers”→ select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

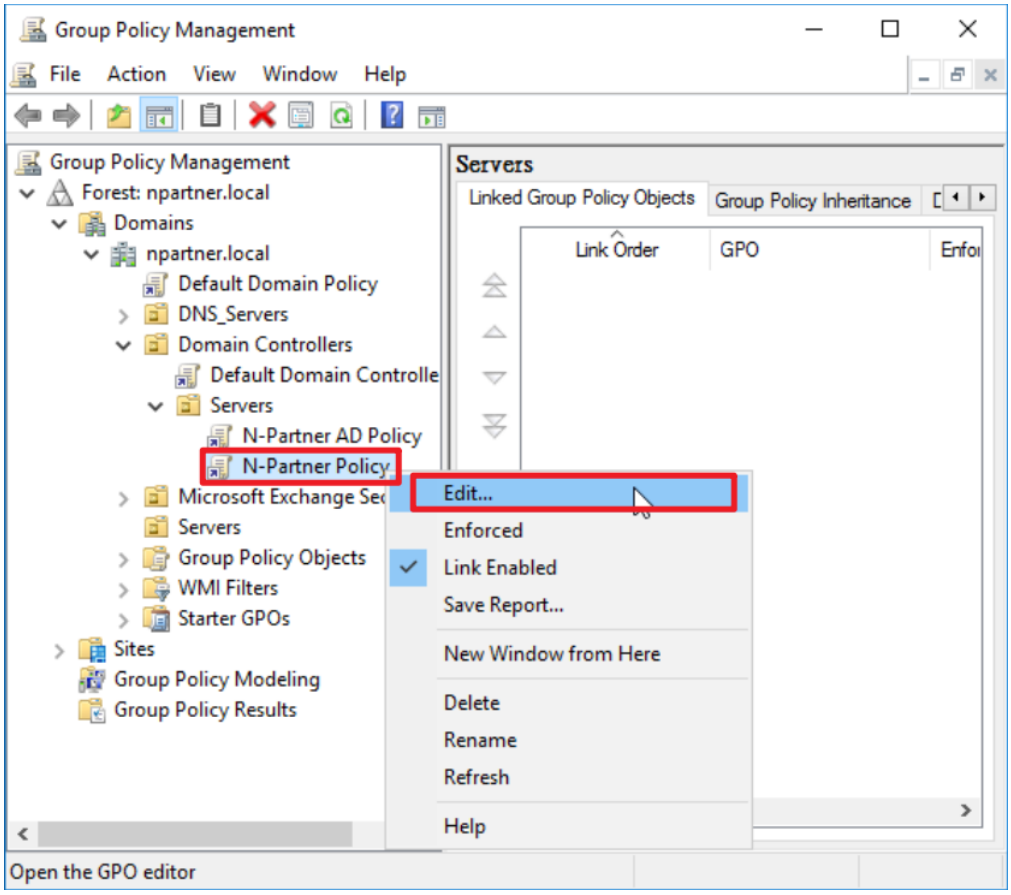
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



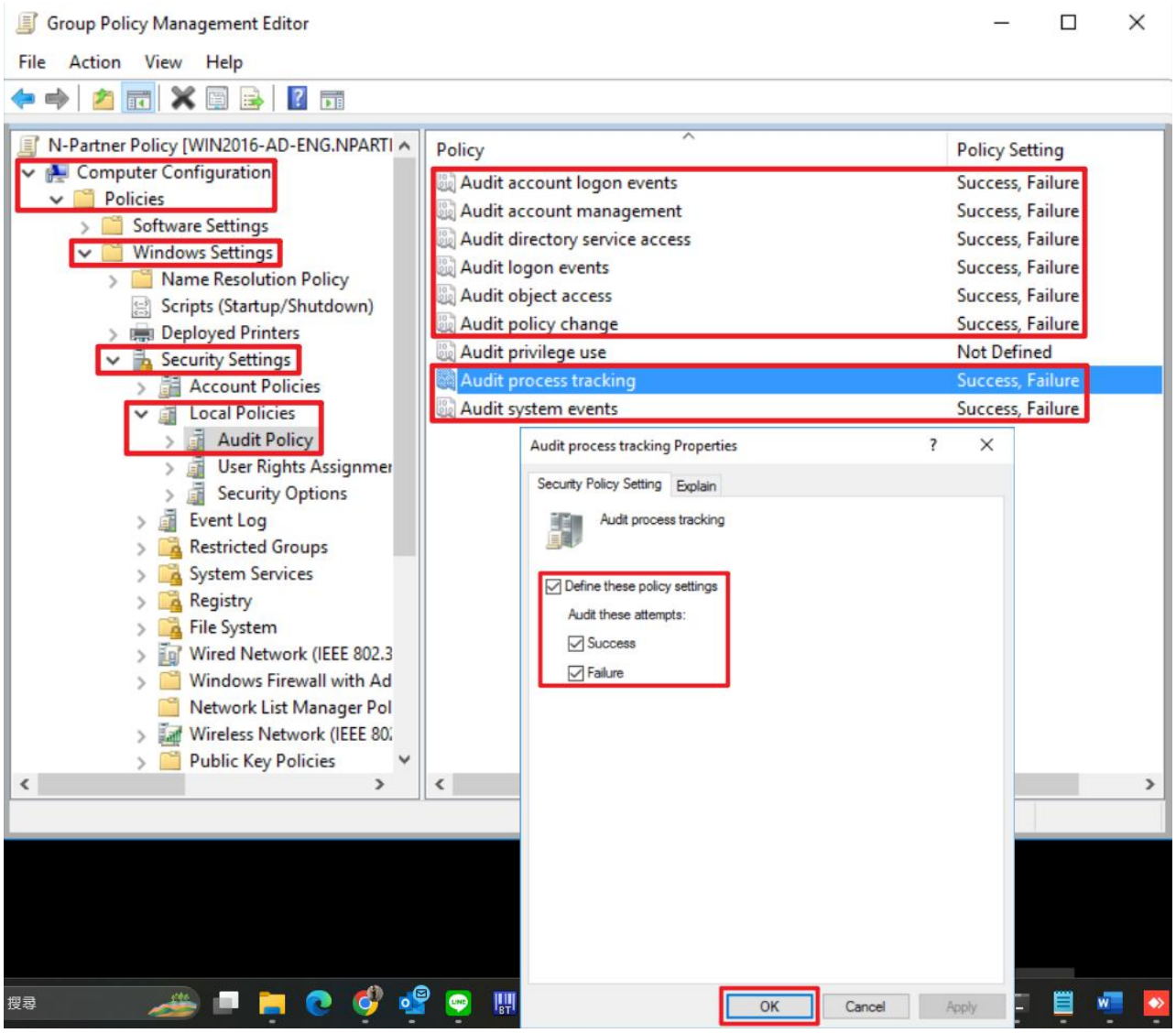
(4) Edit your Group Policy Object

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



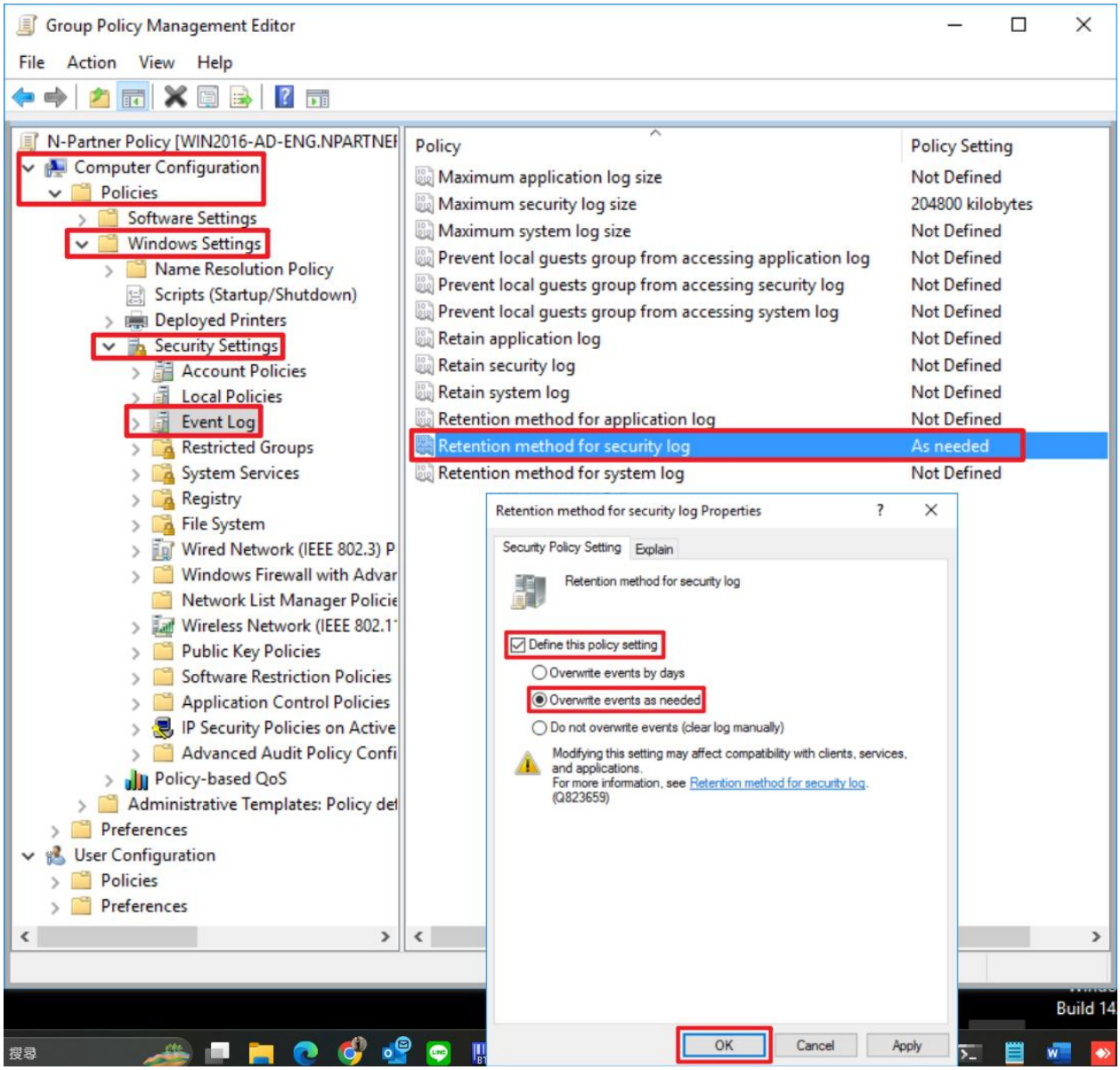
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “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” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

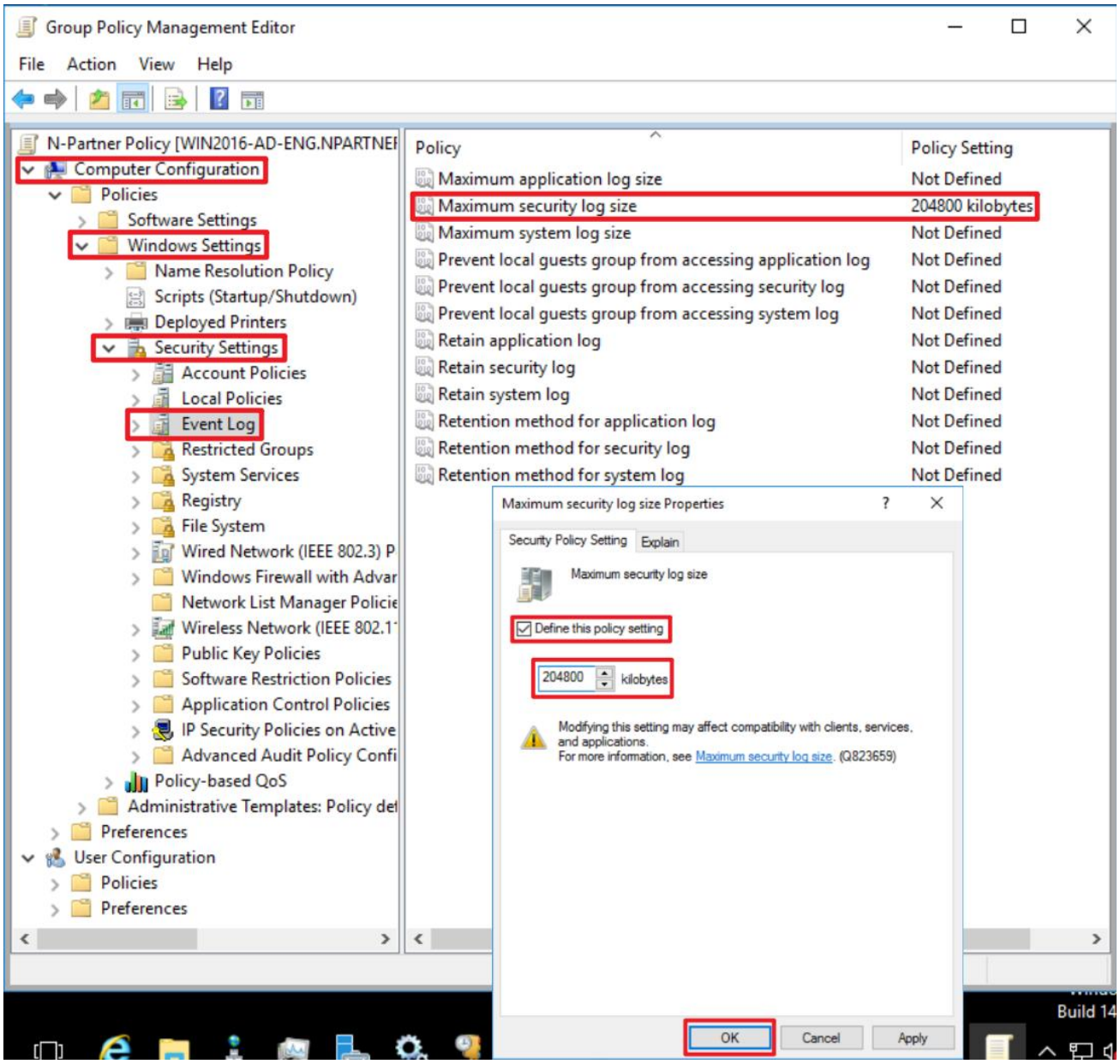
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “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.”



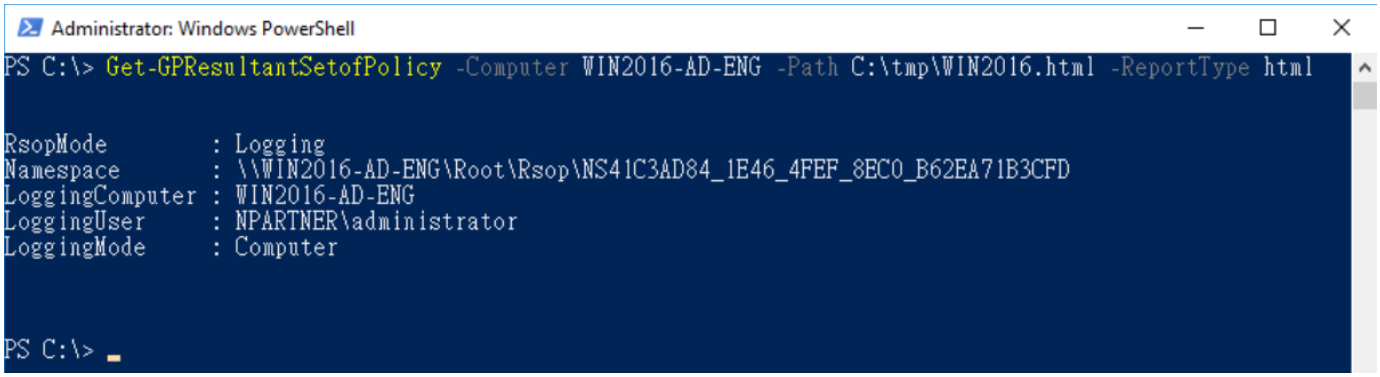
(8) Open “Windows PowerShell.”

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

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

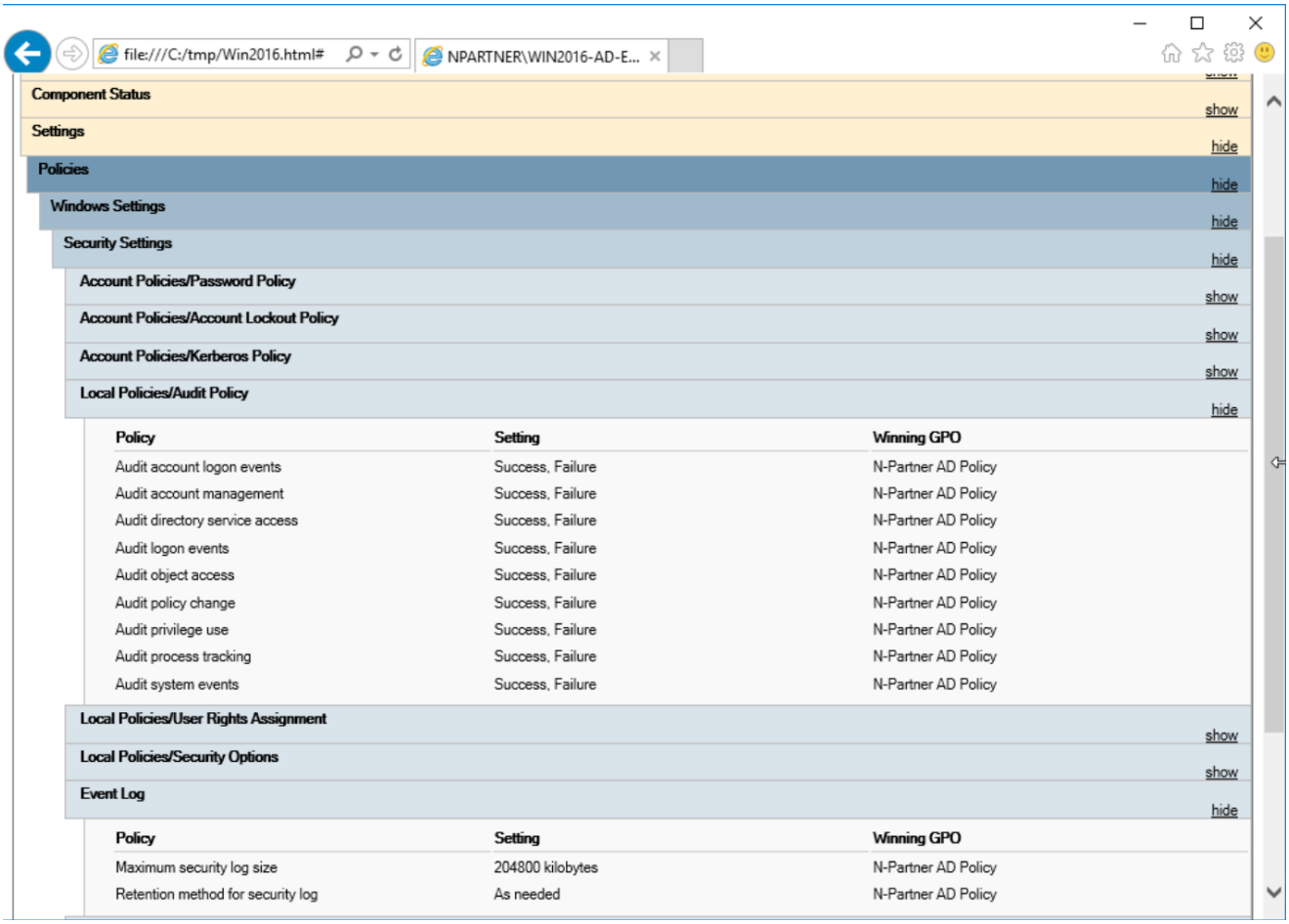
(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2016-AD-ENG -Path C:\tmp\Win2016.html -ReportType html
```



For the red text , please enter the Windows file 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.

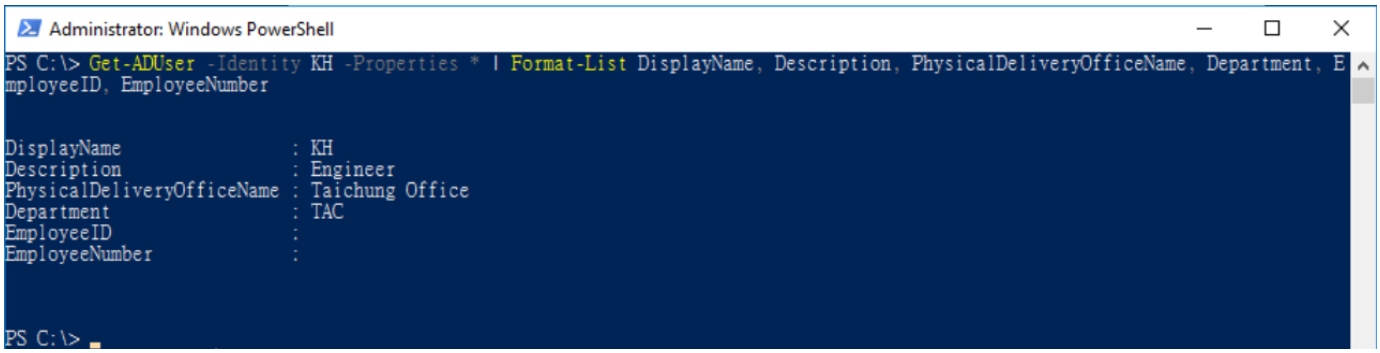


6.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Enter the command below to check whether N-Reporter associates Windows AD with available user data.

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description,
PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



Replace the red text with the username according to the actual environment.

(2) In “Event Query,” click the information of “Username.”

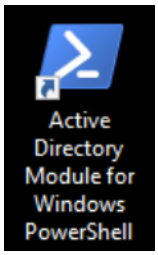
Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

6.3.1 Add Non-Admin Accounts

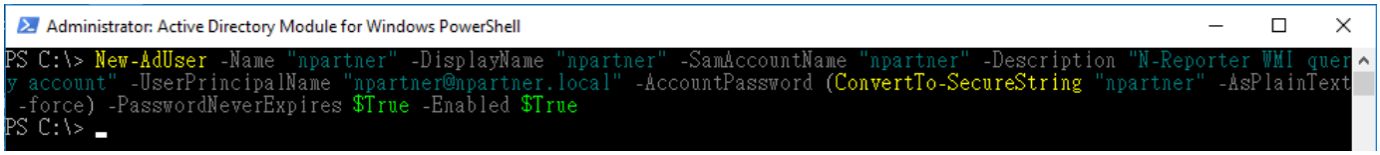
(1) Open “Active Directory Module for Windows PowerShell.”



(2) Create an Account

Enter the command below to create an account:

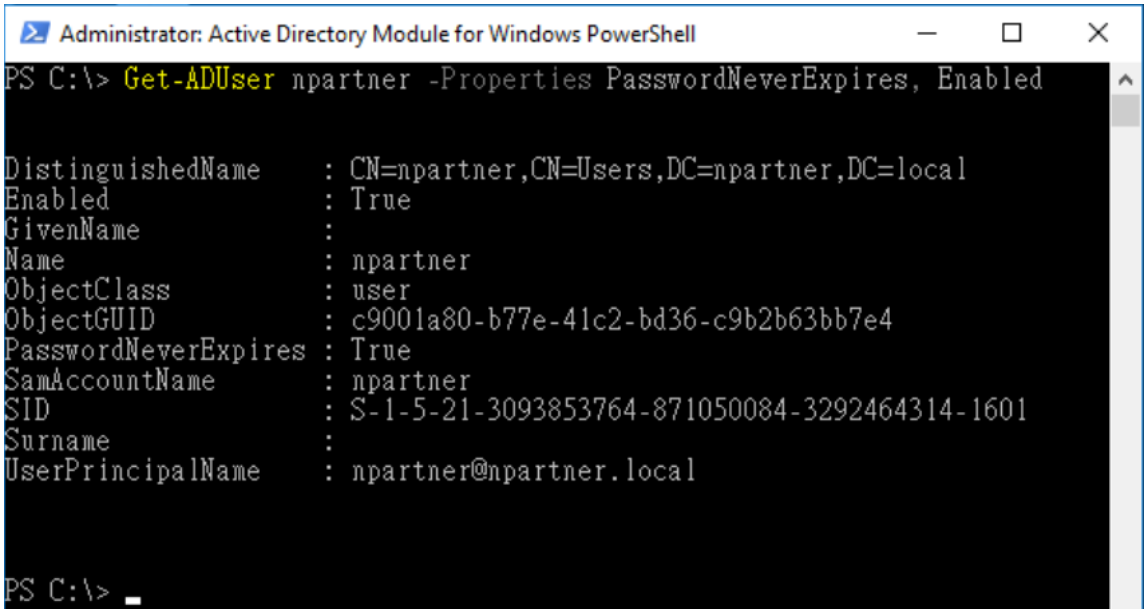
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

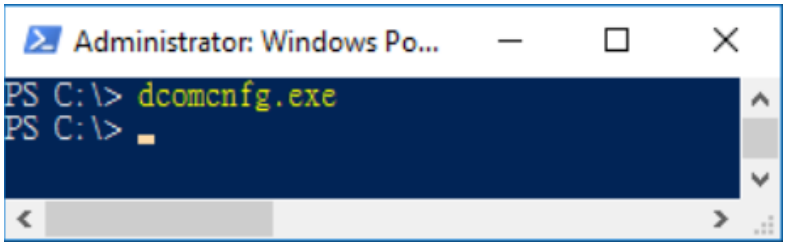


6.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”

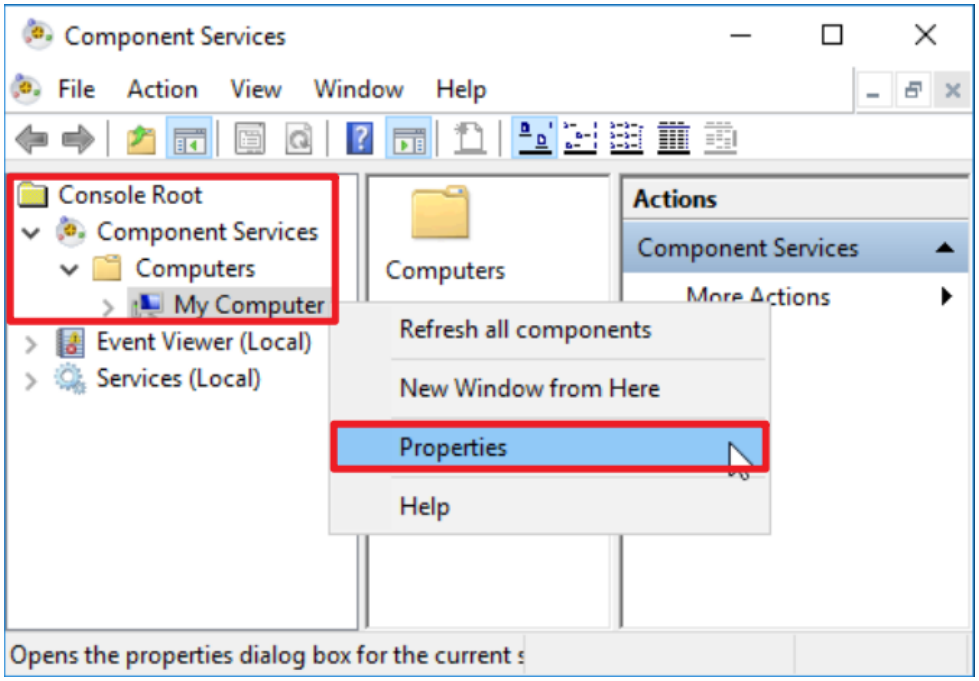
(2) Enter the command below to enable component services.

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



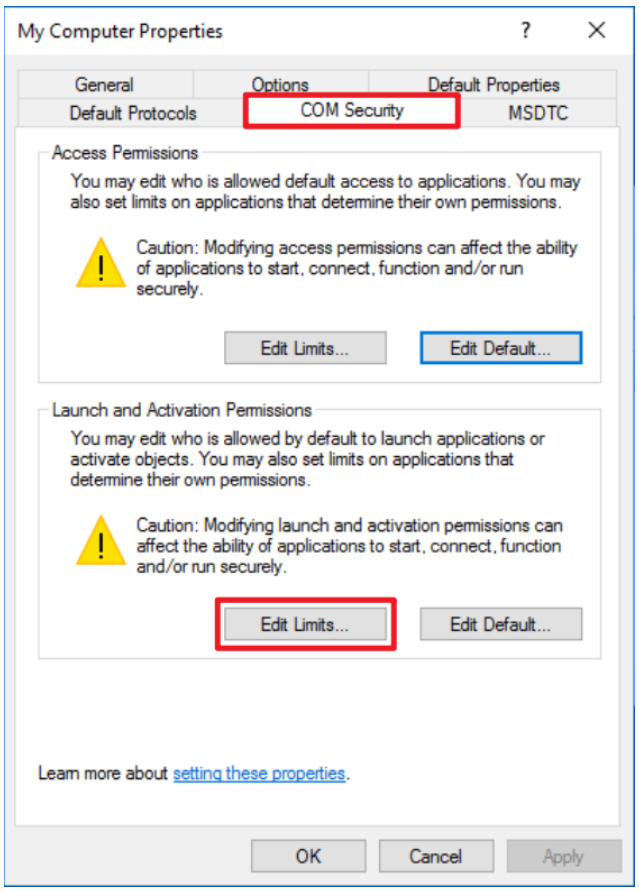
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



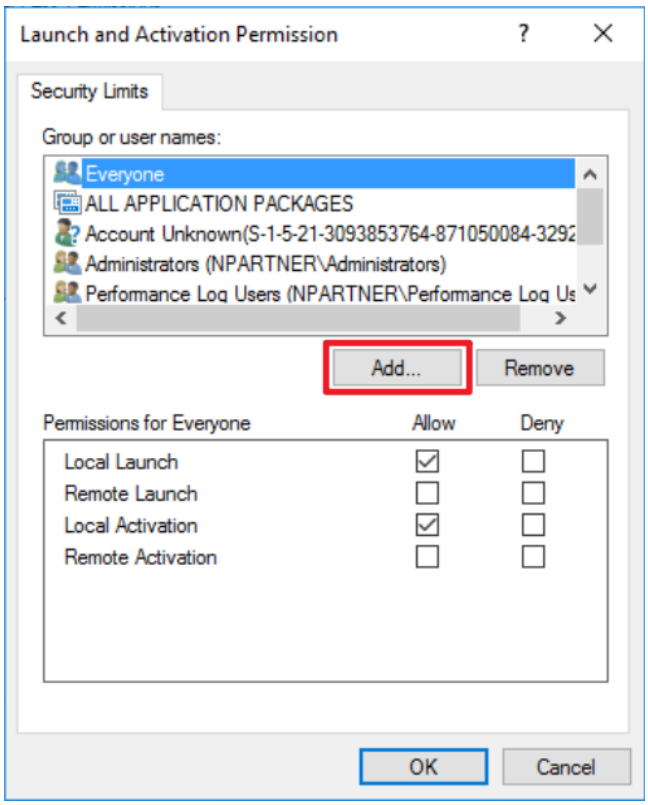
(4) Enable Permissions

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



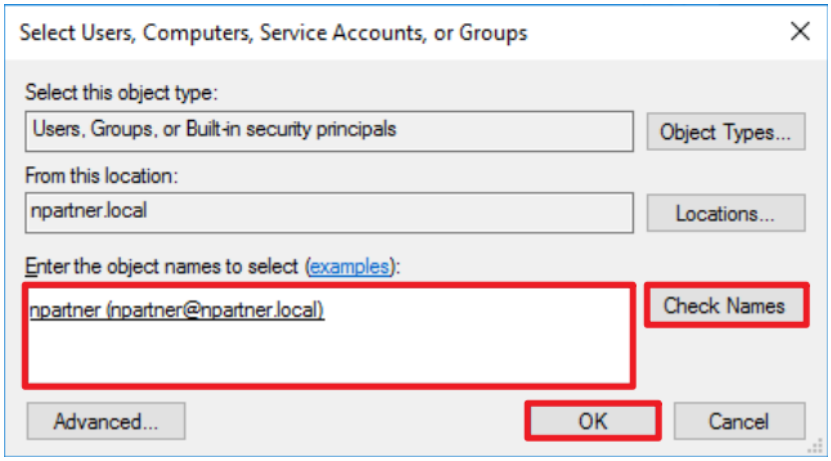
(5) Add DCOM User Permissions

Click “Add.”



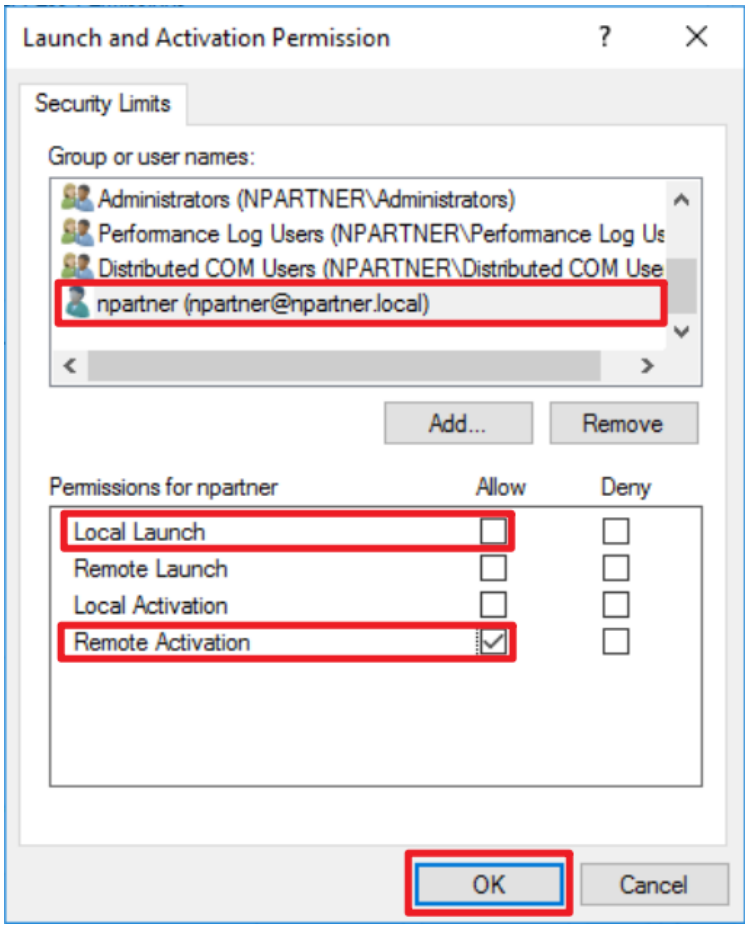
(6) Enter Your Username

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

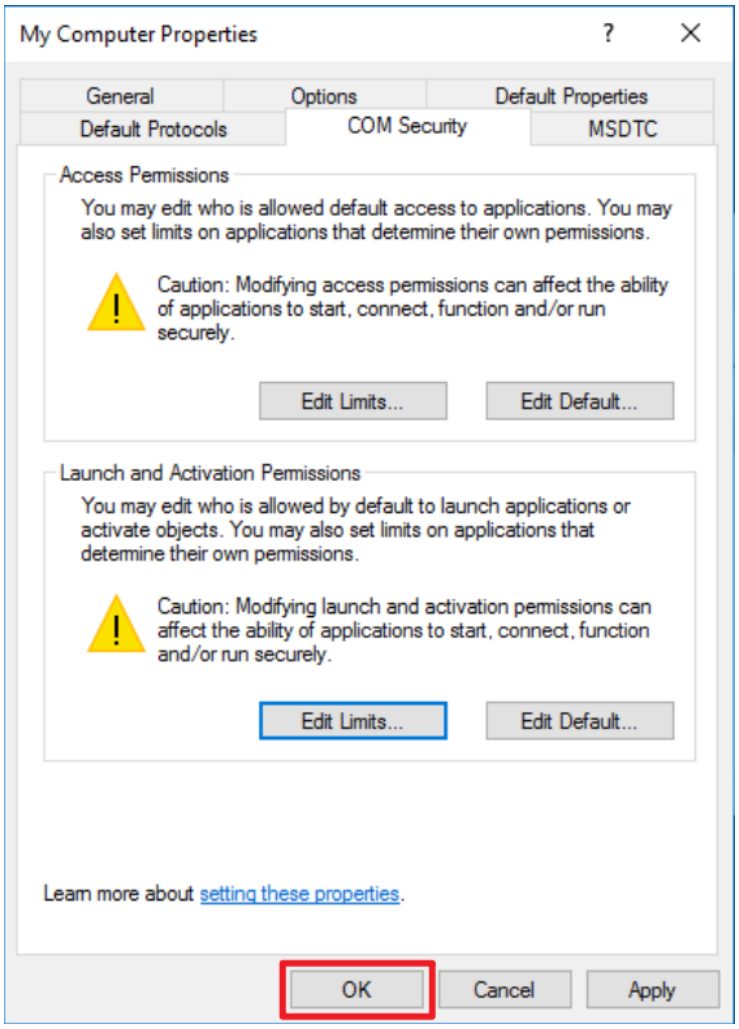


(7) Configure your User Permission

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



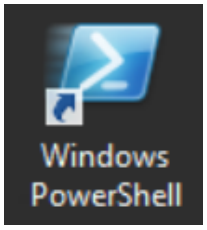
(8) Click "OK.”



6.3.3 Configure WMI Permissions

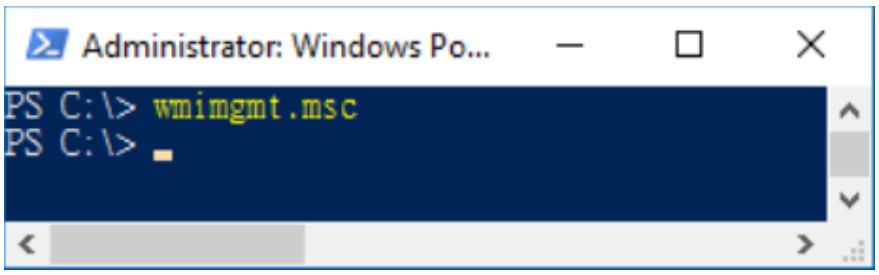
6.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



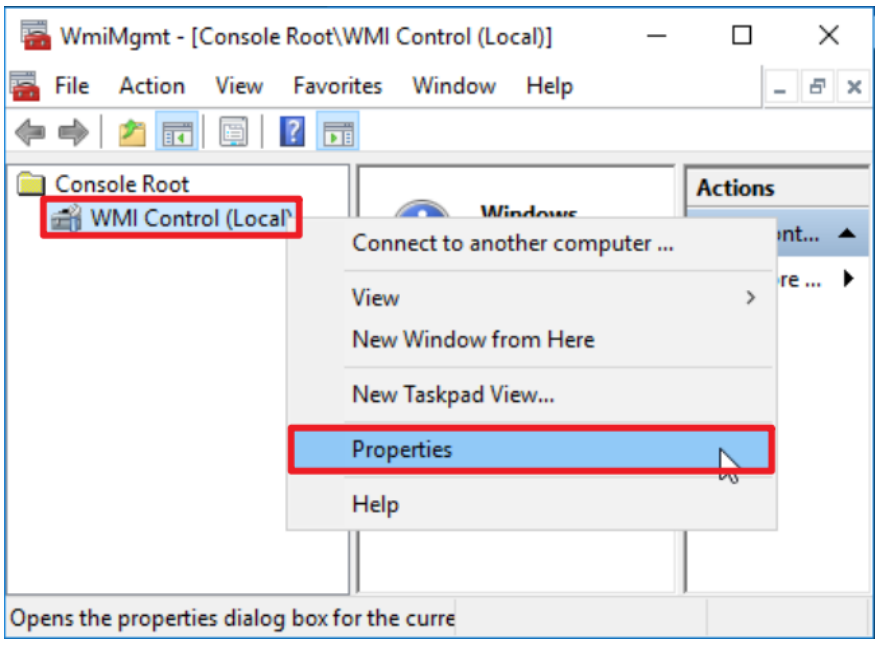
(2) Enter the command to enable WMI control service.

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



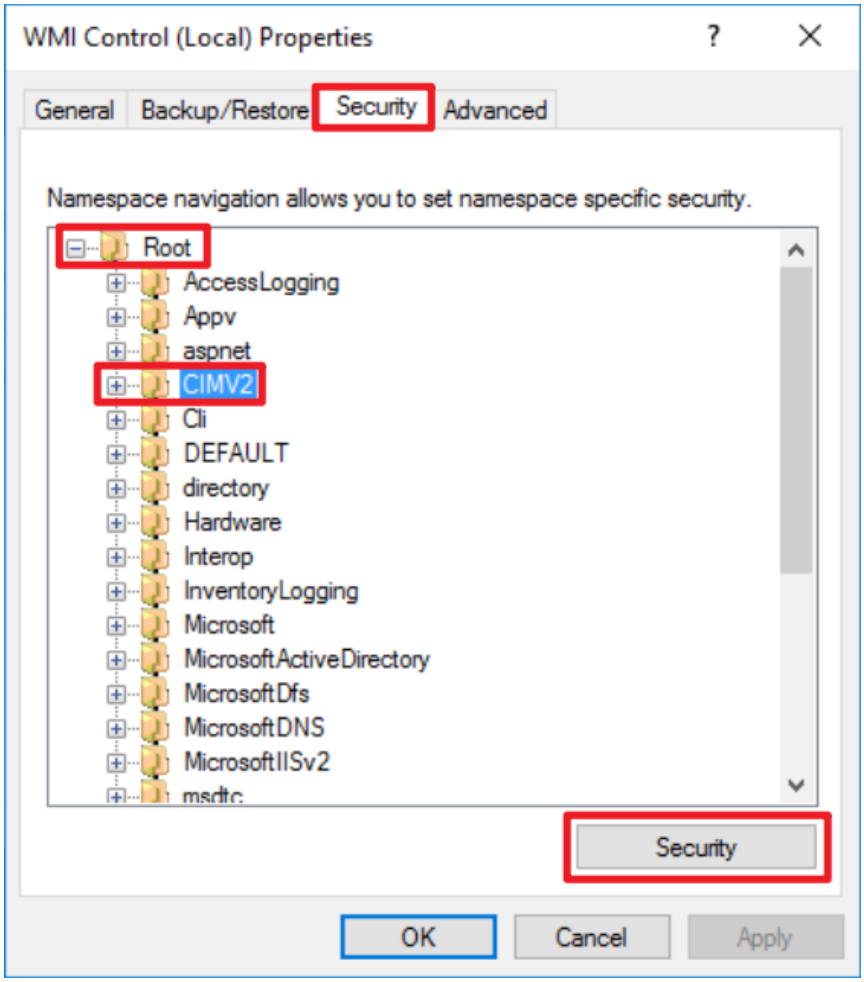
(3) Edit WMI Control

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



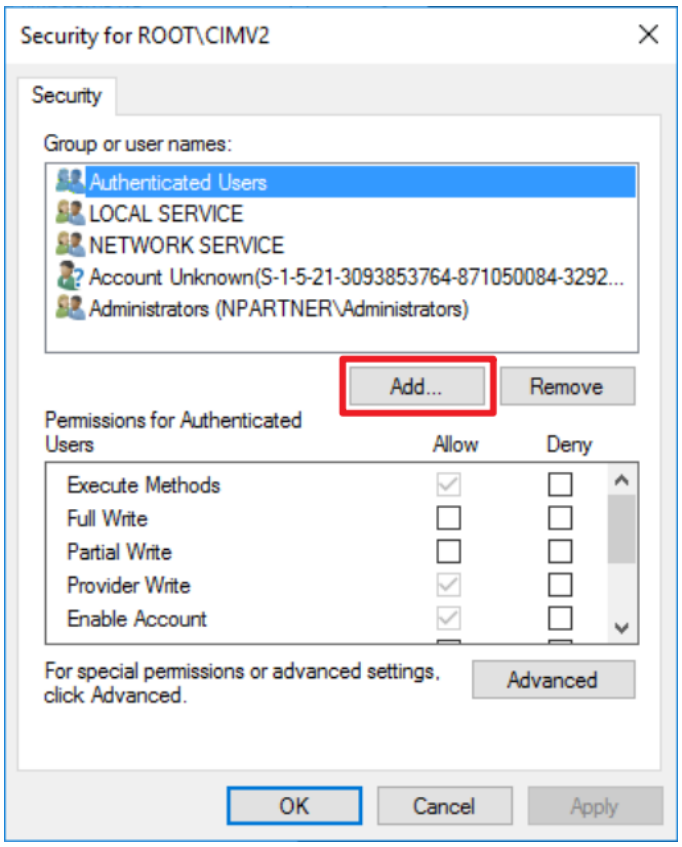
(4) Edit CIMV2 Security

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



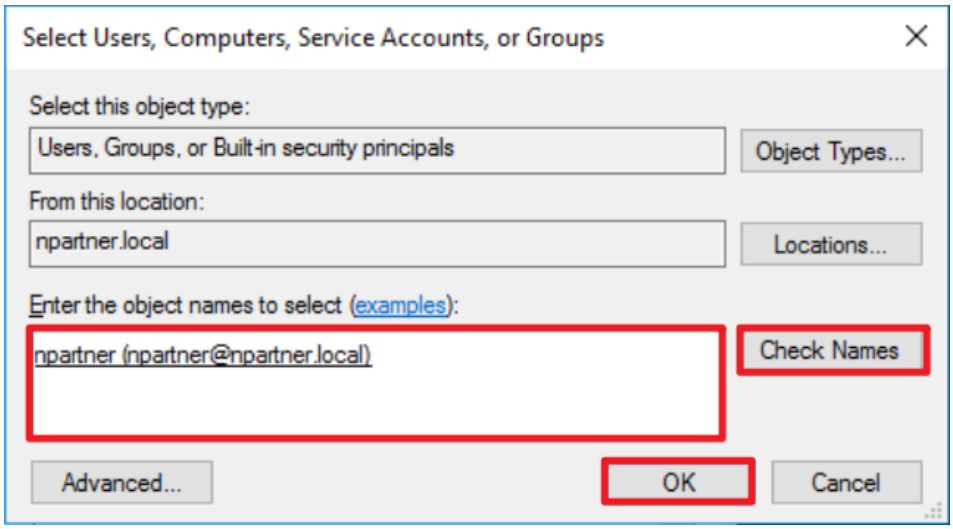
(5) Add WMI User Permissions.

Click “Add.”



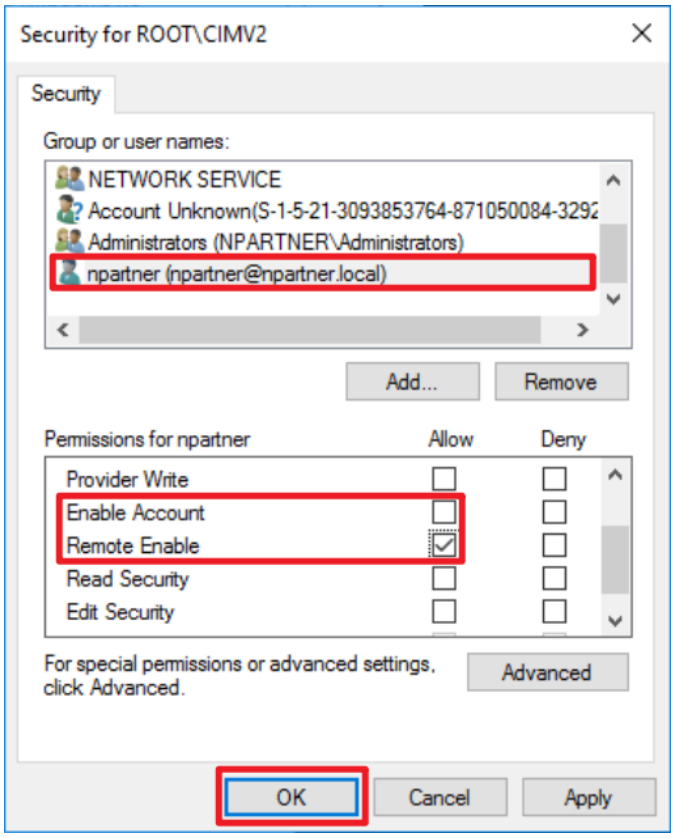
(6) Enter Your Username

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

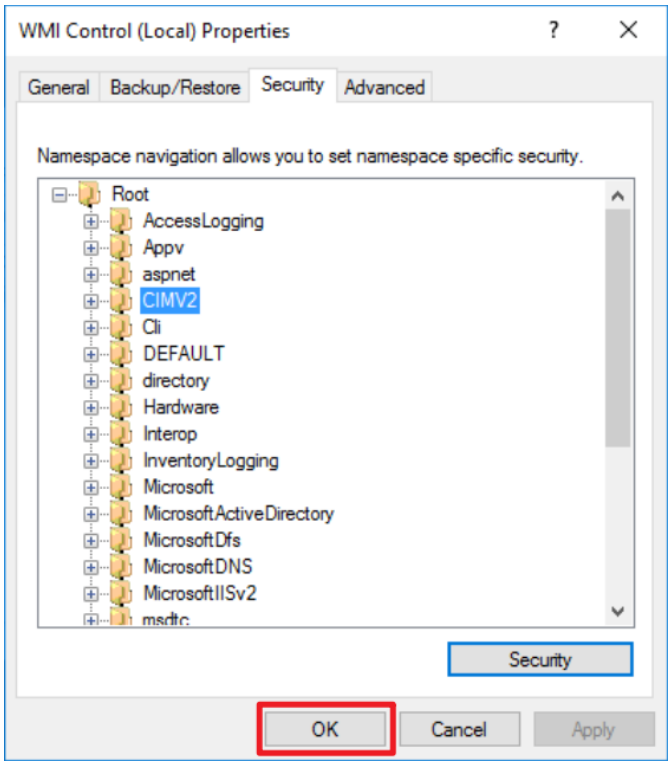


(7) Set Your User Permissions

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

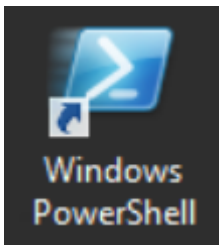


(8) Click “OK.”



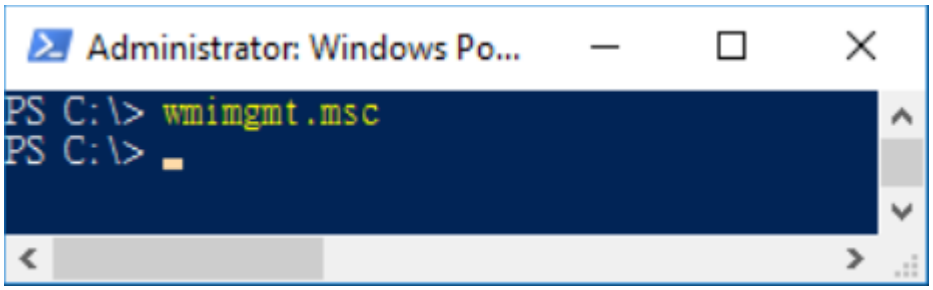
6.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



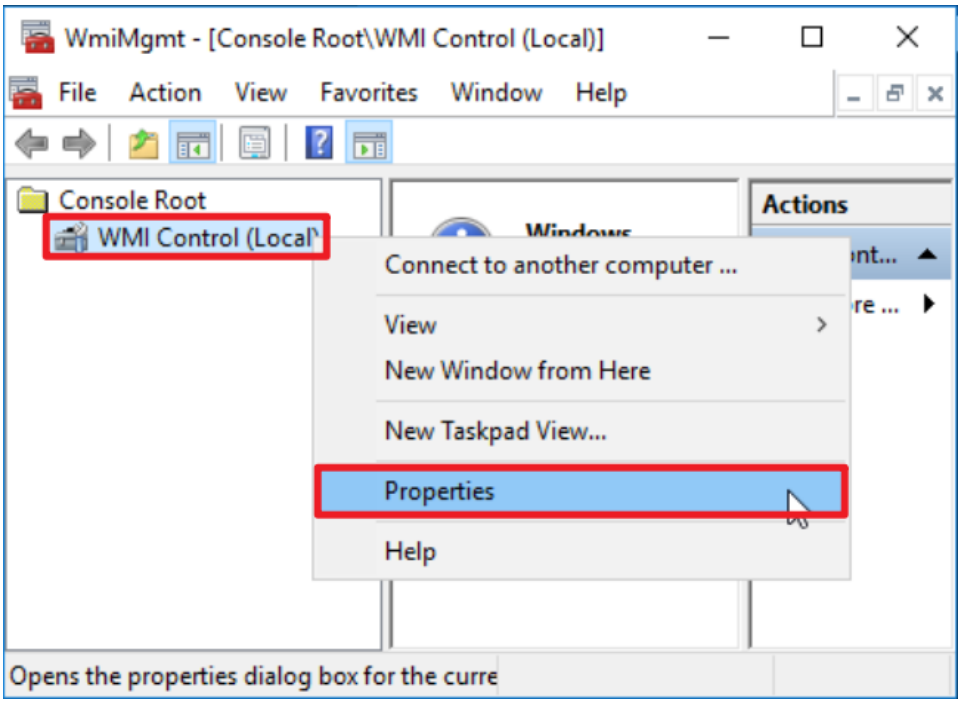
(2) Enter the command below to enable WMI Control.

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



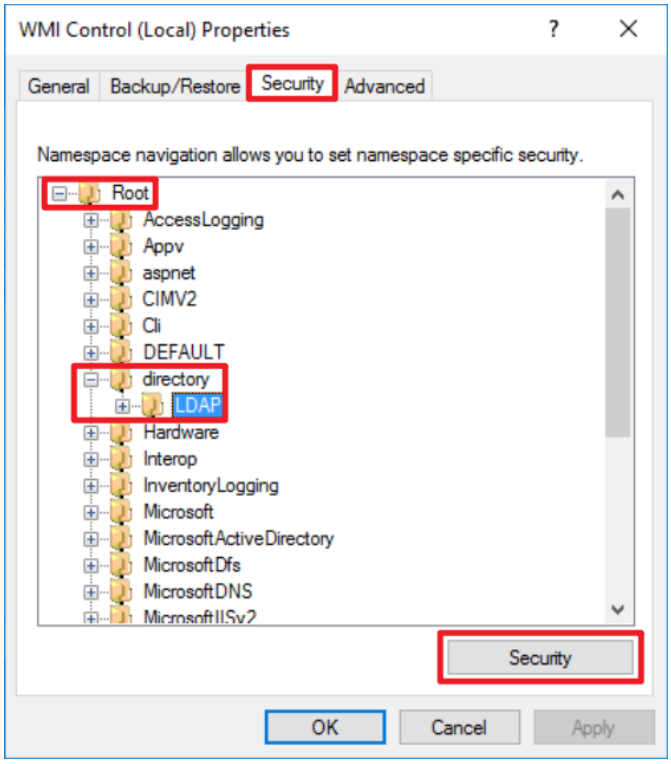
(3) Edit WMI Control

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



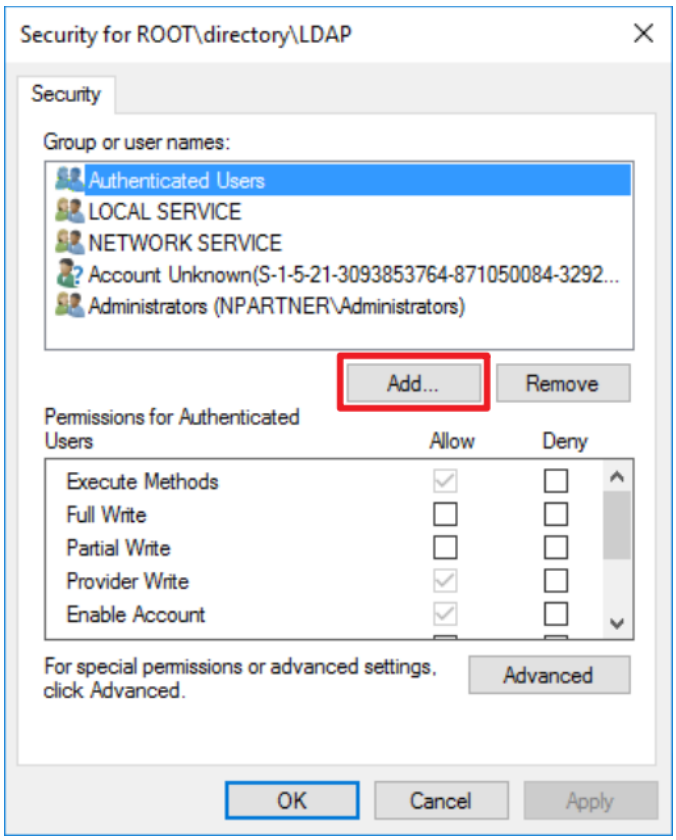
(4) Edit LDAP Security

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



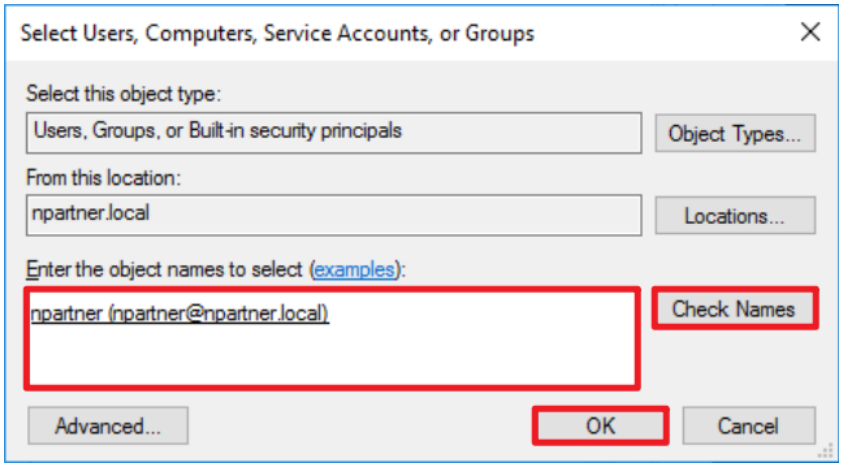
(5) Add WMI User Permissions

Click “Add.”



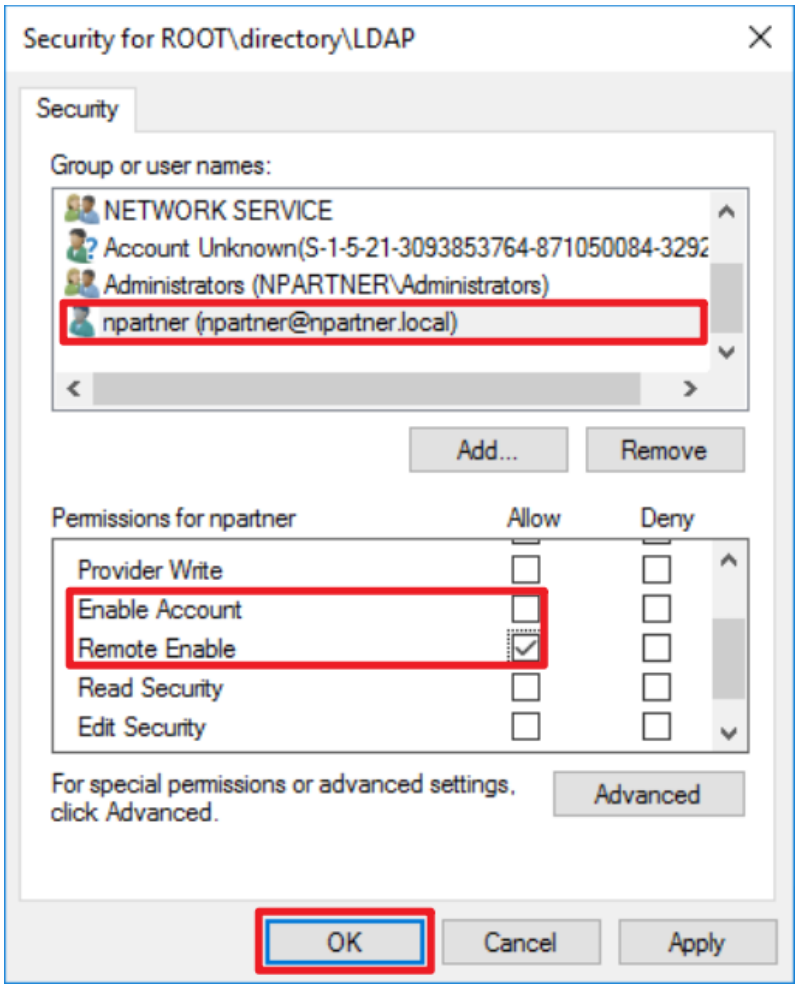
(6) Enter Your Username

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

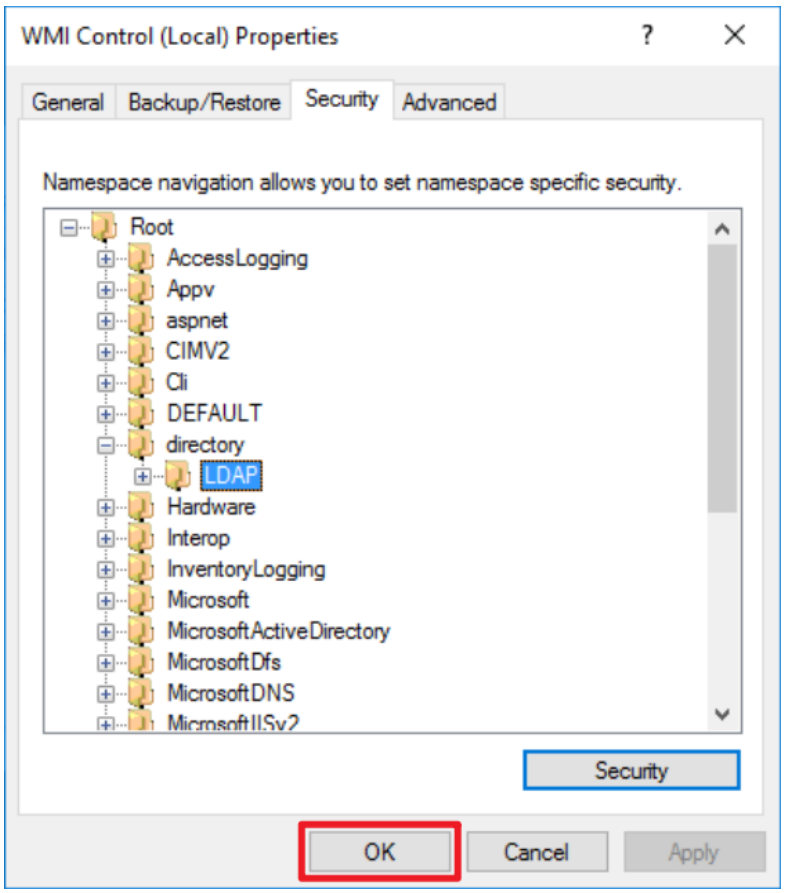


(7) Set Your User Permissions

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

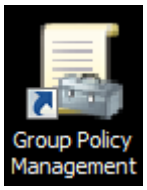


(8) Click “OK.”

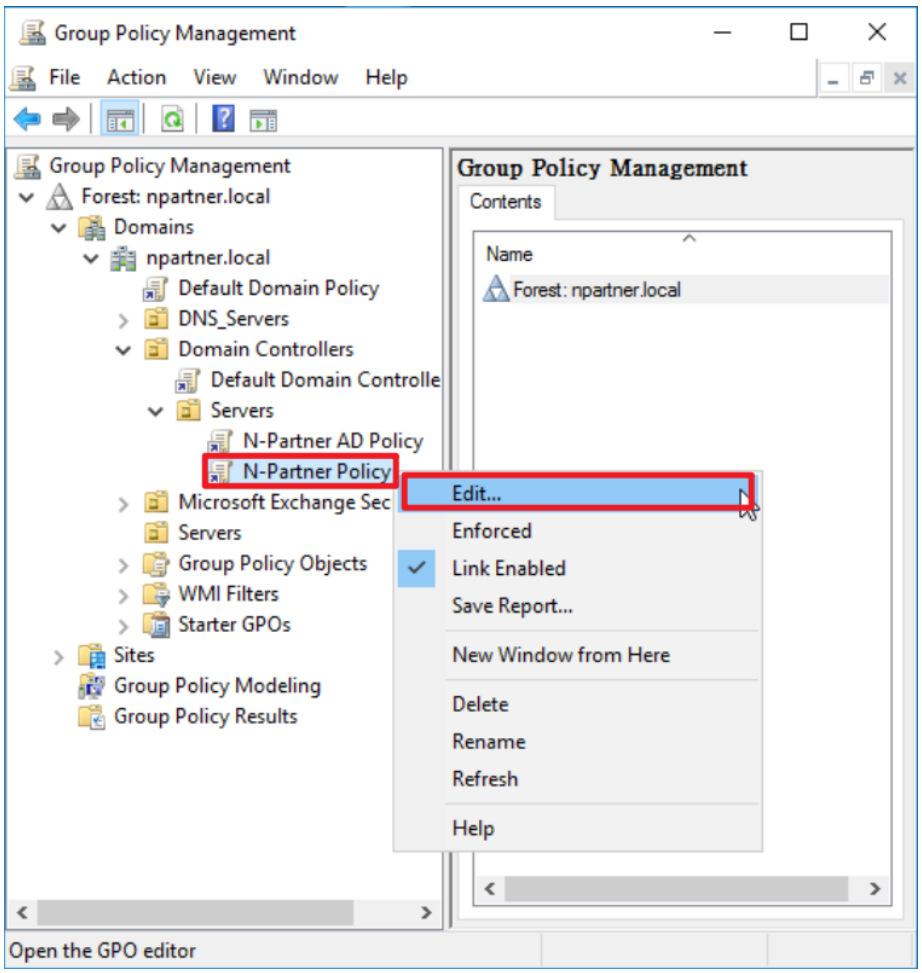


6.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

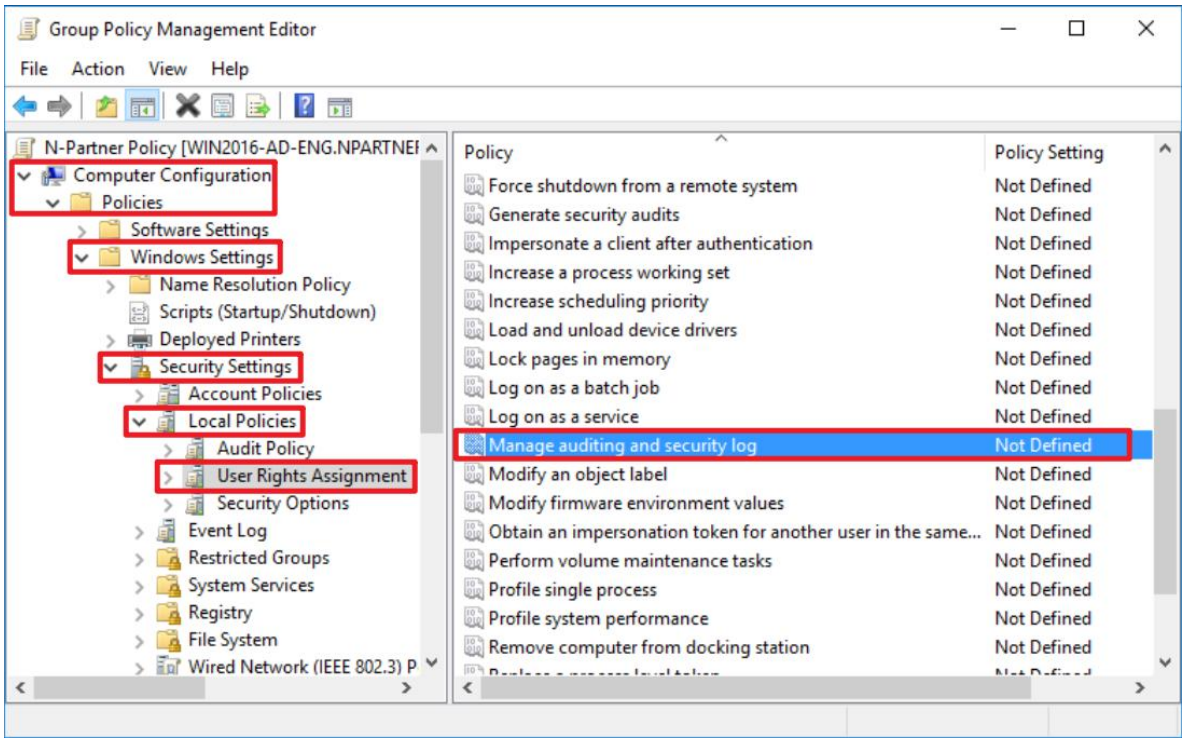


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



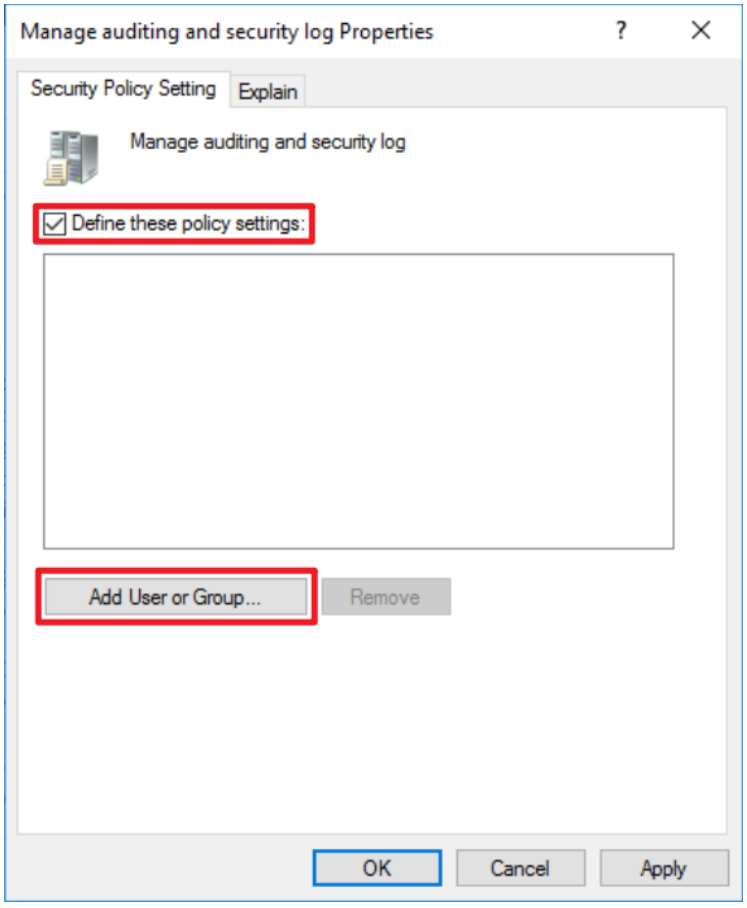
(3) Configure Auditing Log

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



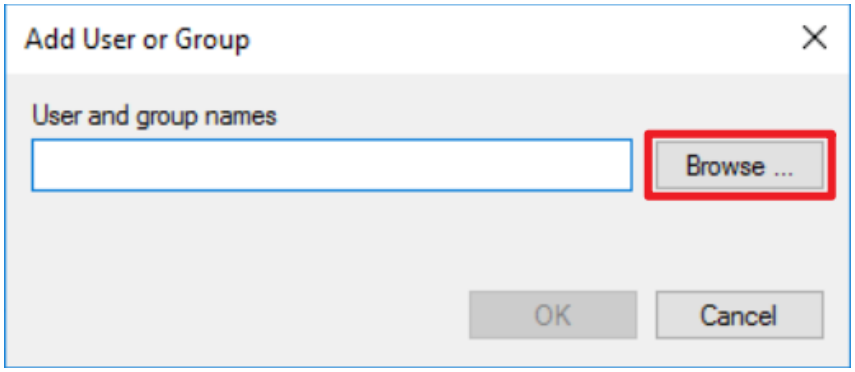
(4) Add Auditing User

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



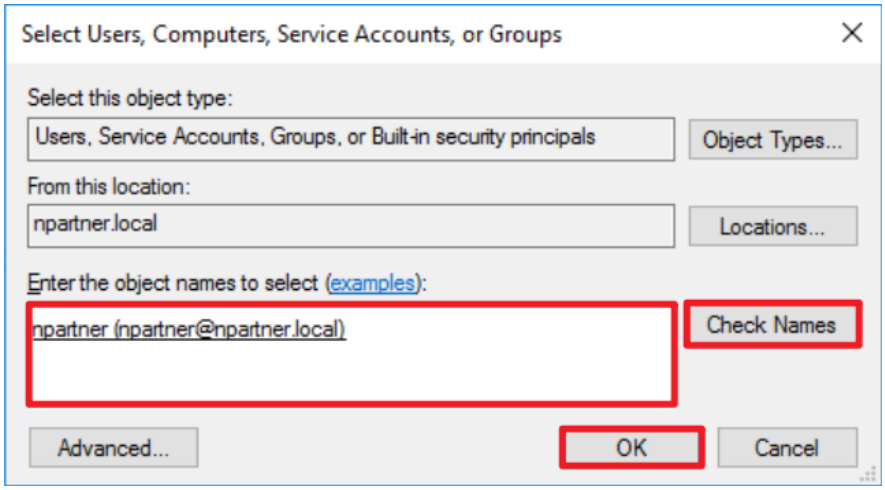
(5) Search for User

Click “Browse.”

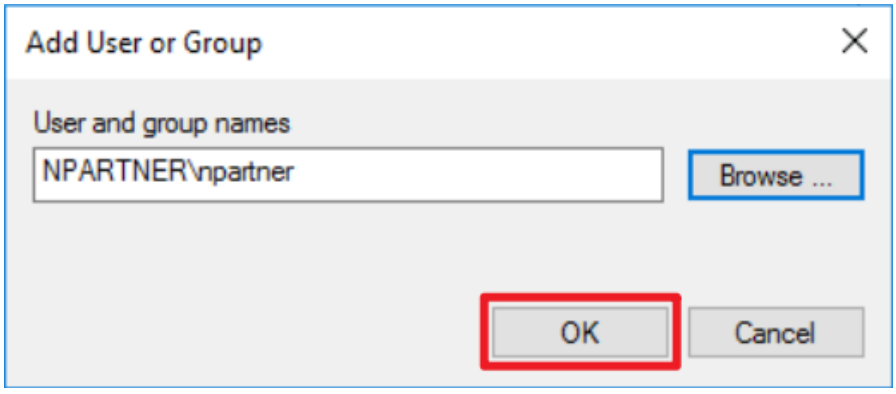


(6) Enter Your User Account

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

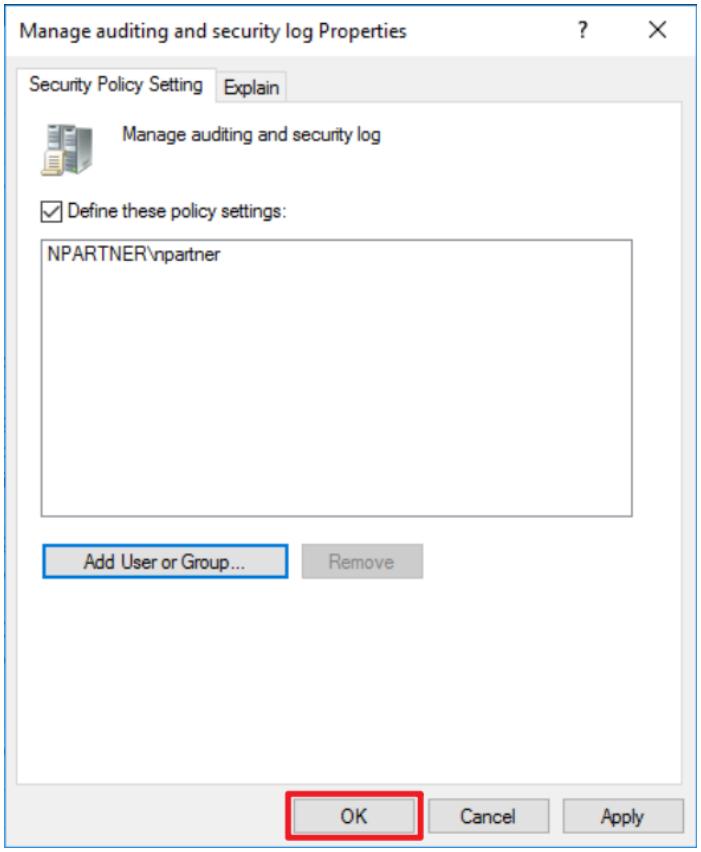


(7) Click “OK.”



(8) Confirm Audit Log Settings

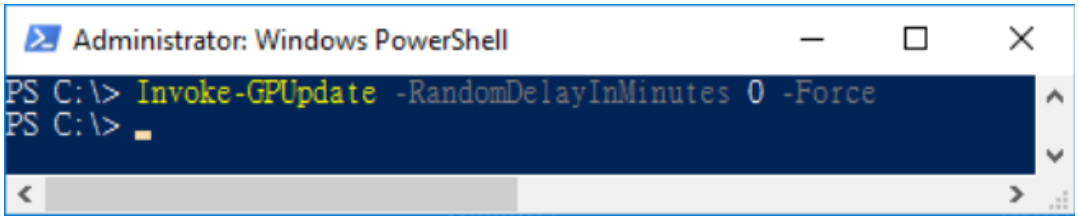
Click “OK.”



(9) Open “Windows Powershell.”

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

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

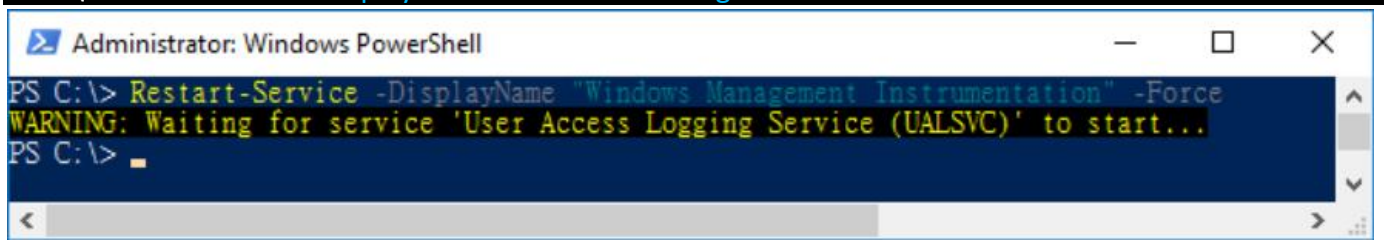


6.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”

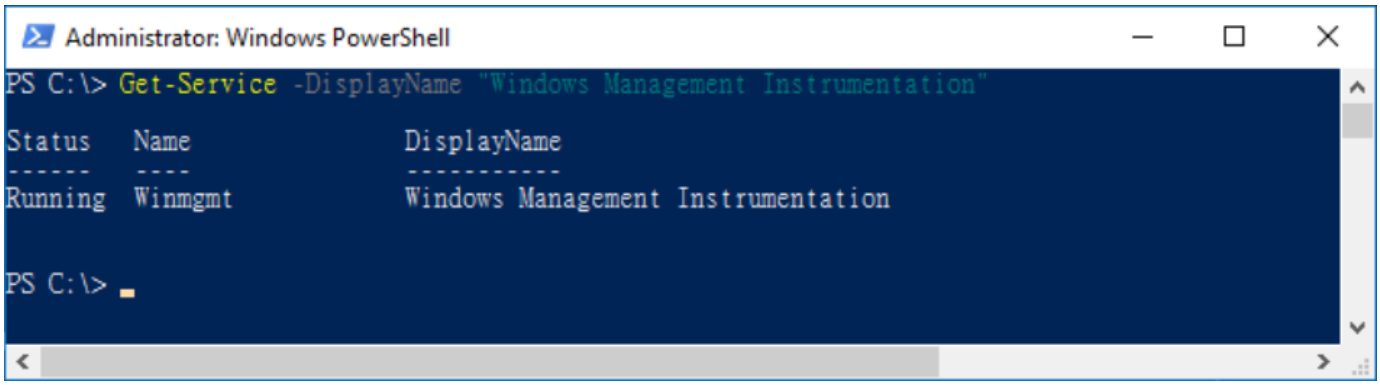
(2) Enter the command below to disable the WMI service.

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



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

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

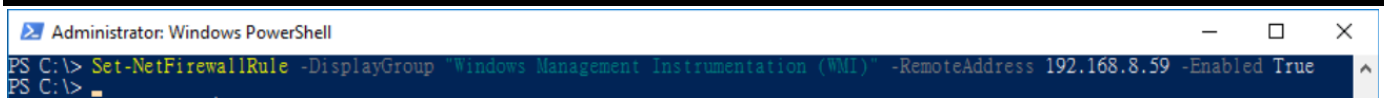


6.3.6 Configure the Firewall

(1) Open “Windows Powershell.”

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

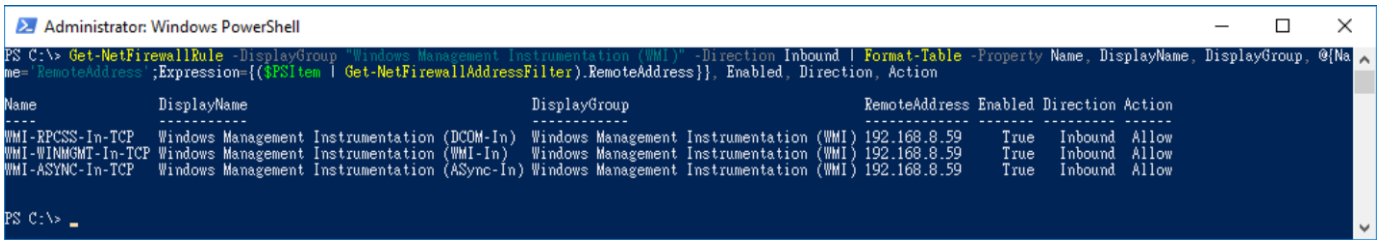
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress
192.168.8.59 -Enabled True
```



Replace the red text with the N-Reporter IP address.

(3) Enter the command below to show the current firewall WMI configuration:

```
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
```



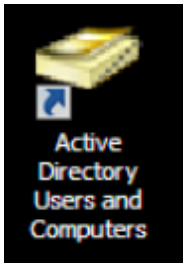
7. Windows Server 2019

Windows Audit Policy Configuration:

For detailed information, refer to the **Audit Policy Recommendations link** in the references.

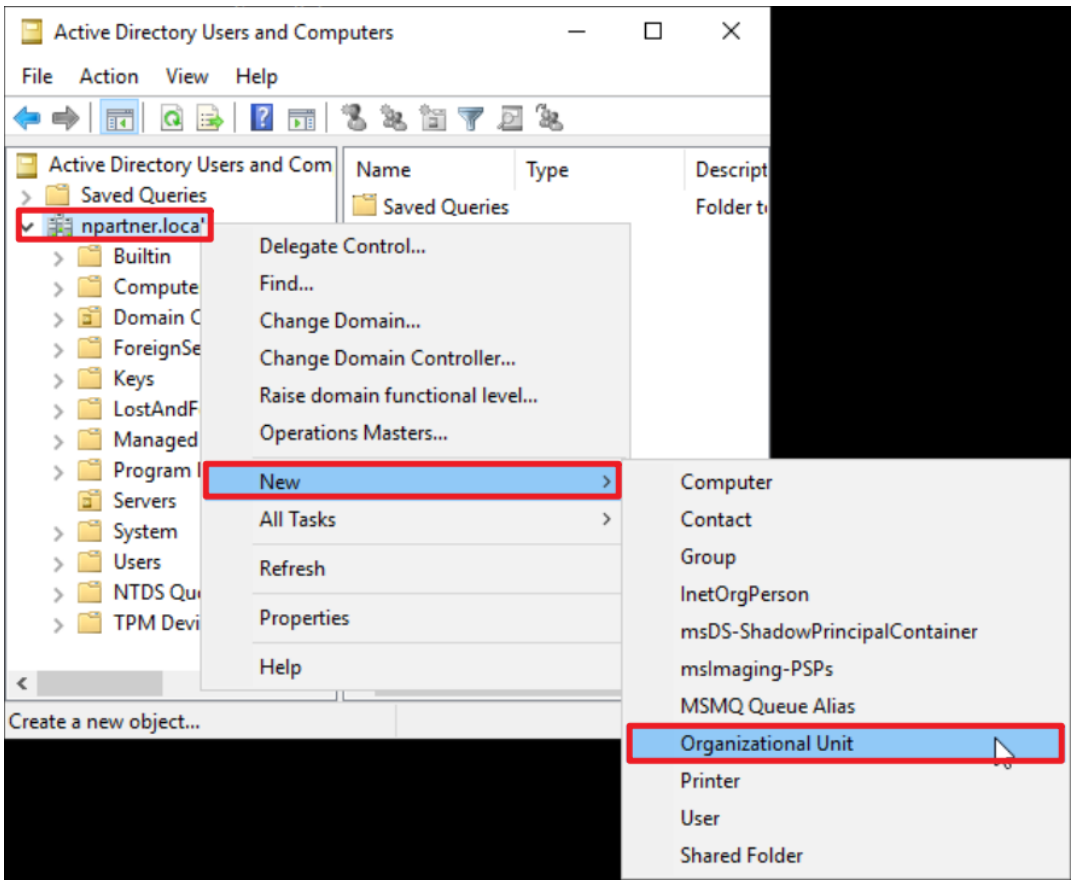
7.1 Organizational Unit (OU) Configuration

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



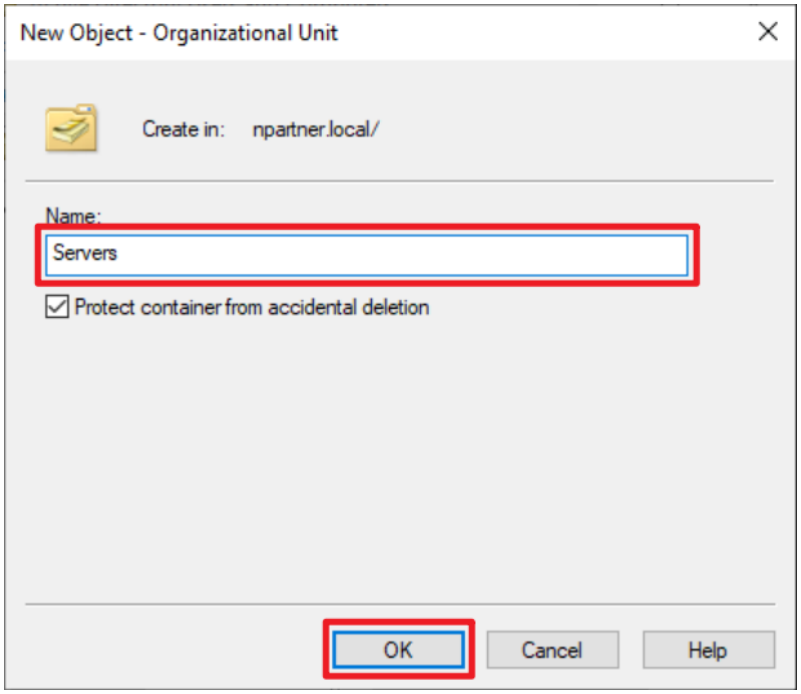
(2) Add an Organizational Unit

Right-click on the domain name (the example here is nparnter.local) → select “New,” and click “Organizational Unit.”



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

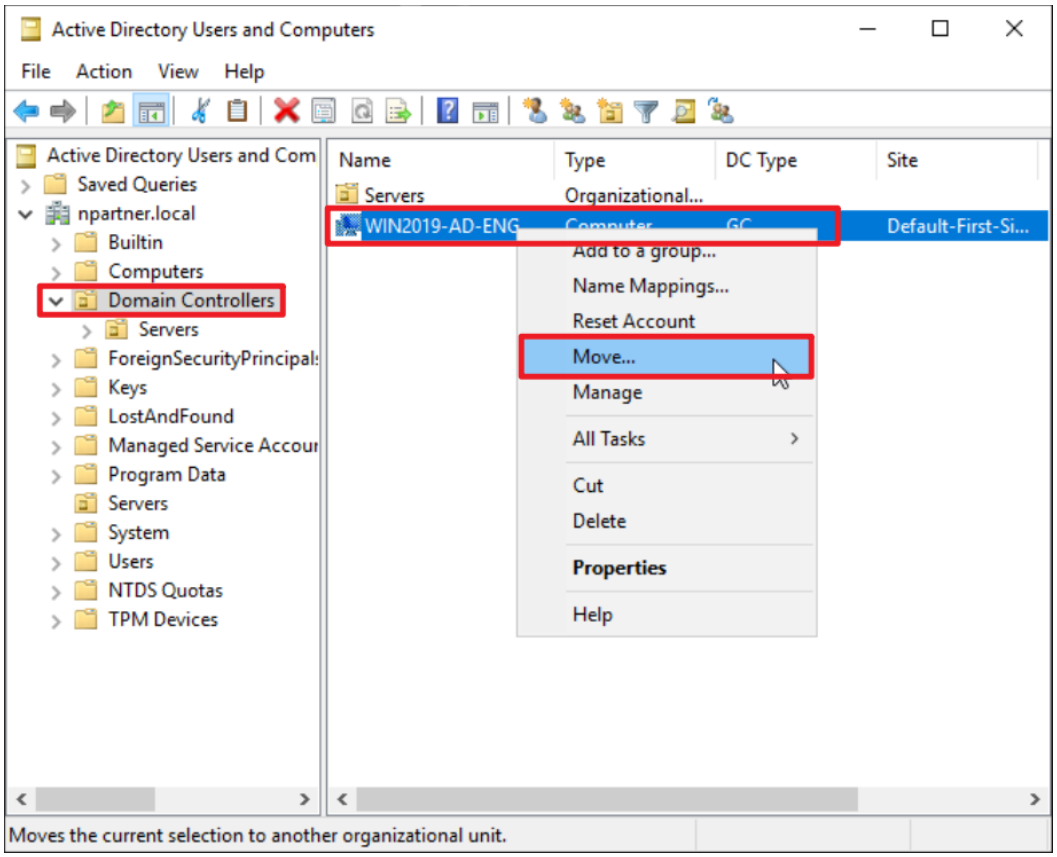
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

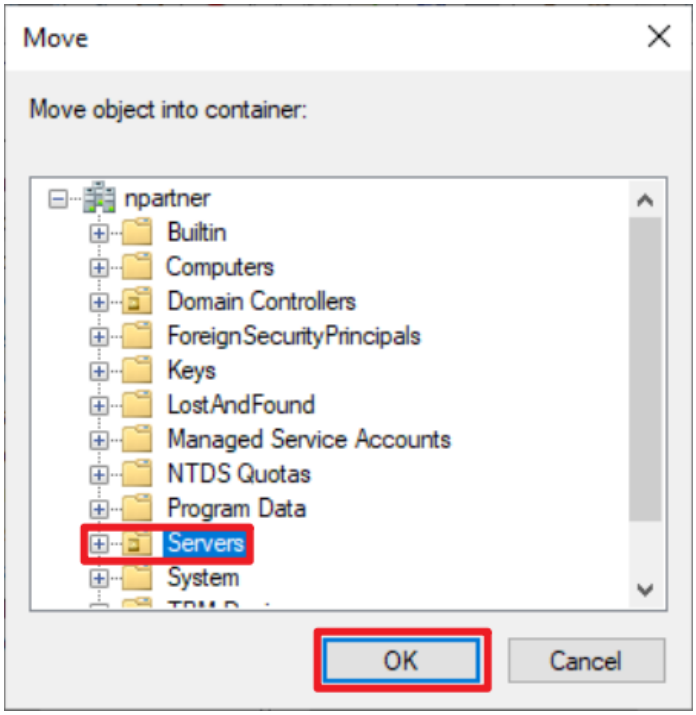
Select “Domain Controllers” → right-click on the “WIN2019-AD-ENG” server.

Note: Please select the Windows file server according to the actual environment. → click “Move.”



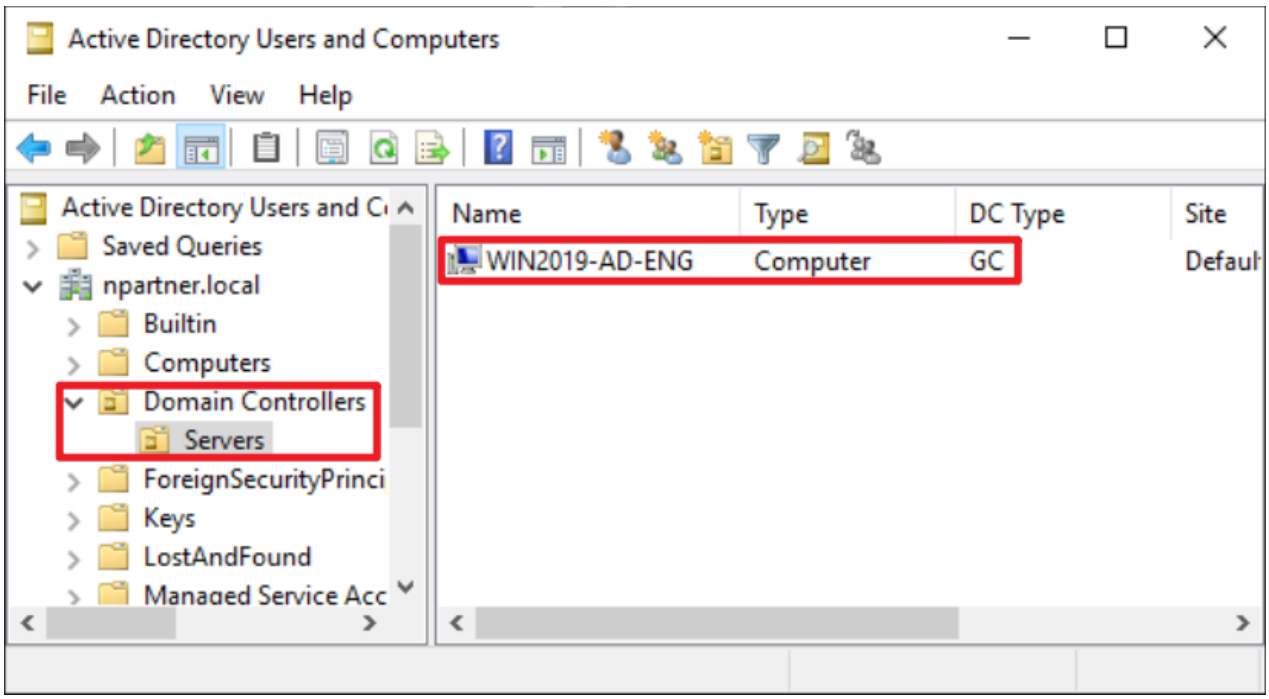
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → 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”) and confirm that the “WIN2019-AD-ENG” server has been moved.

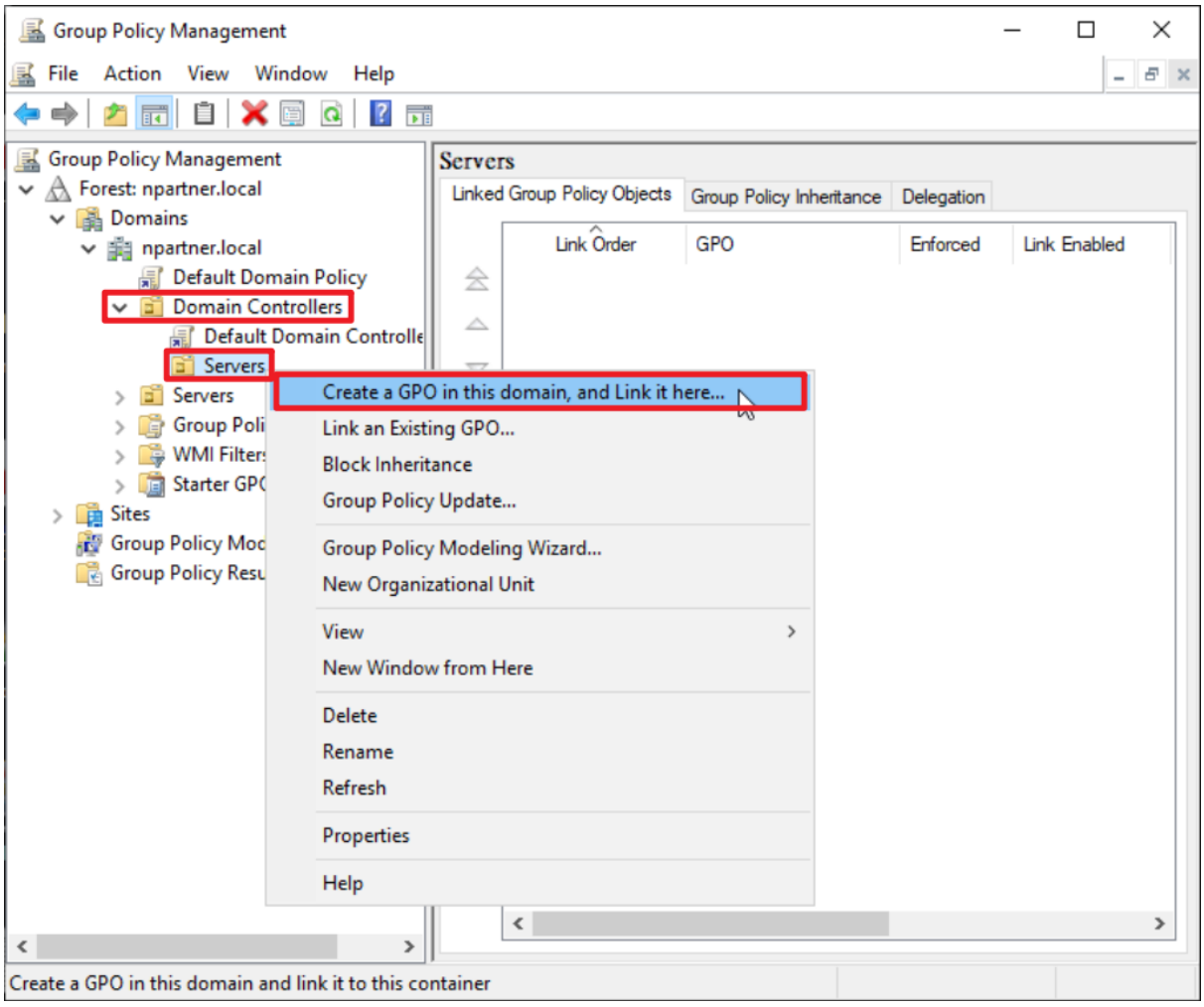


7.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

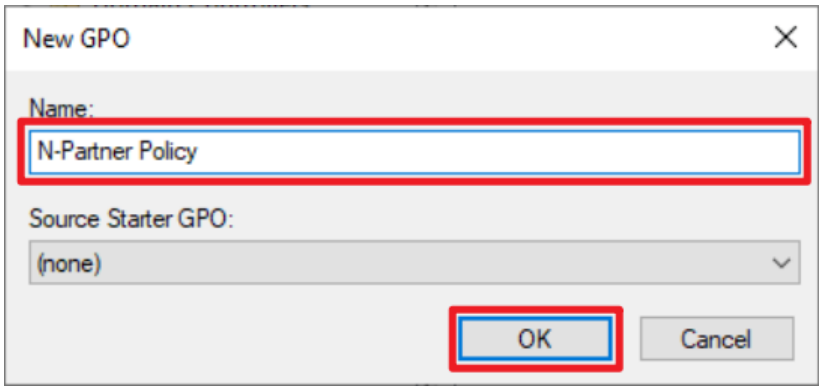
Right-click the “Servers” organizational unit under “Domain Controllers” → select “Create a GPO in this domain, and Link it here...”



(3) Enter your Group Policy Object

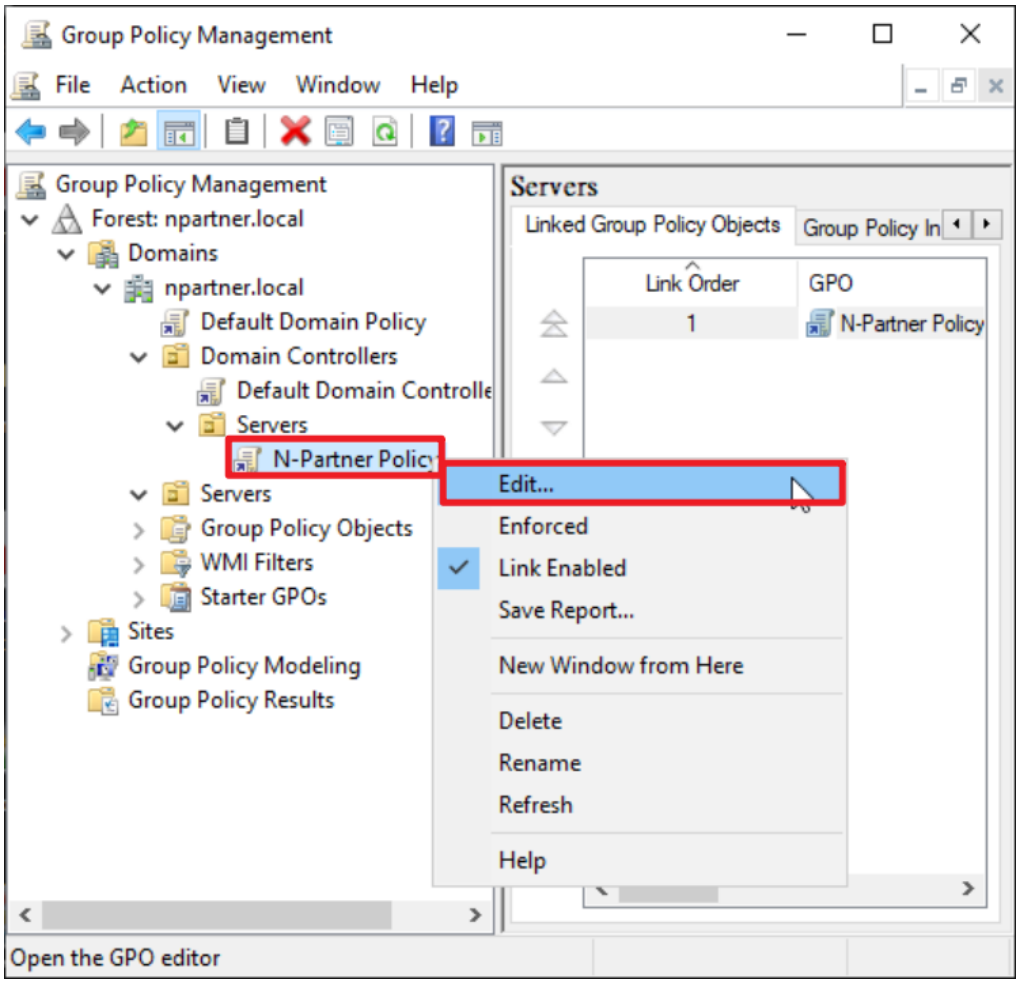
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

Note: Create your GPO name according to the actual environment. → then click “OK.”



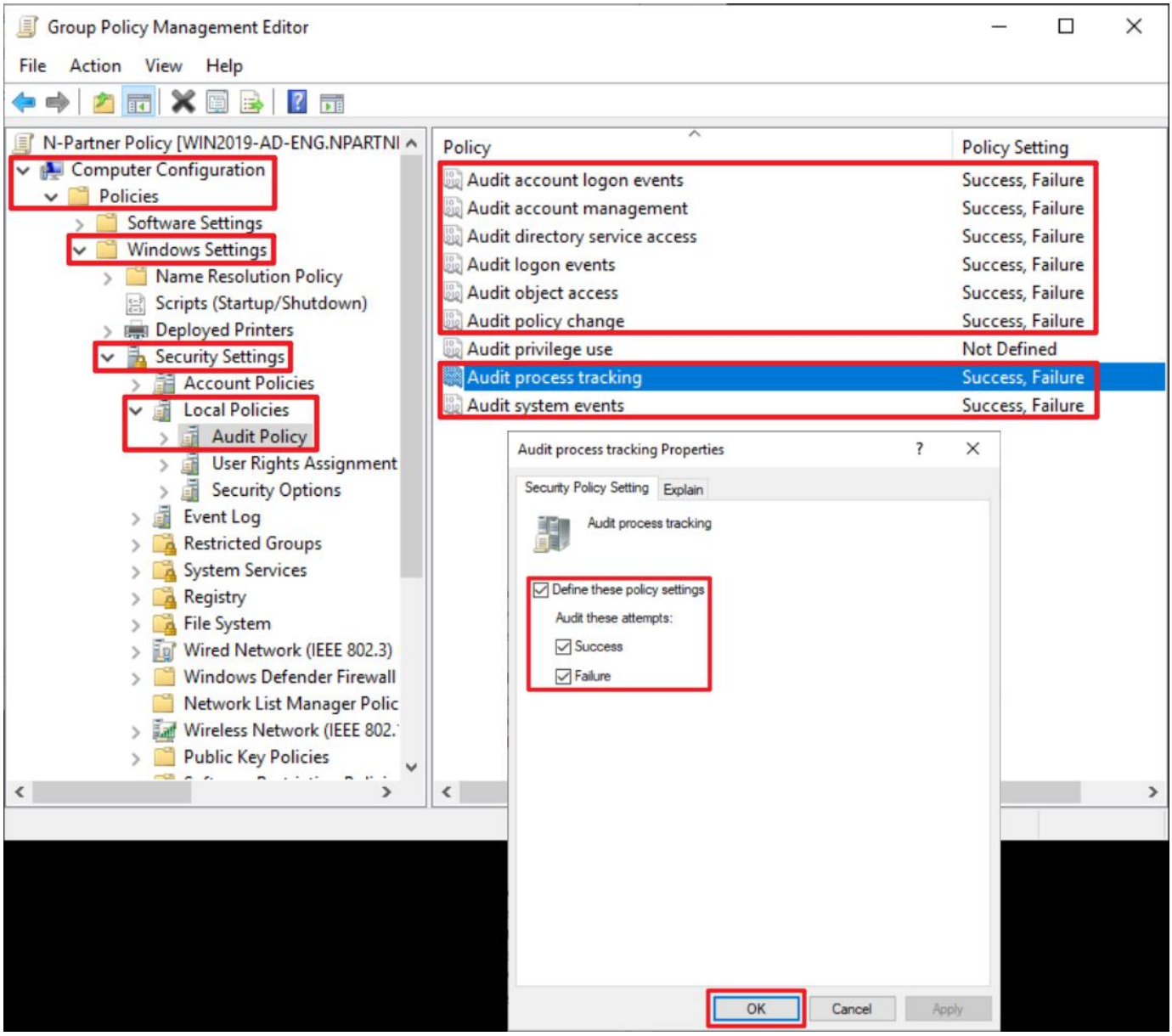
(4) Edit your Group Policy Object

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



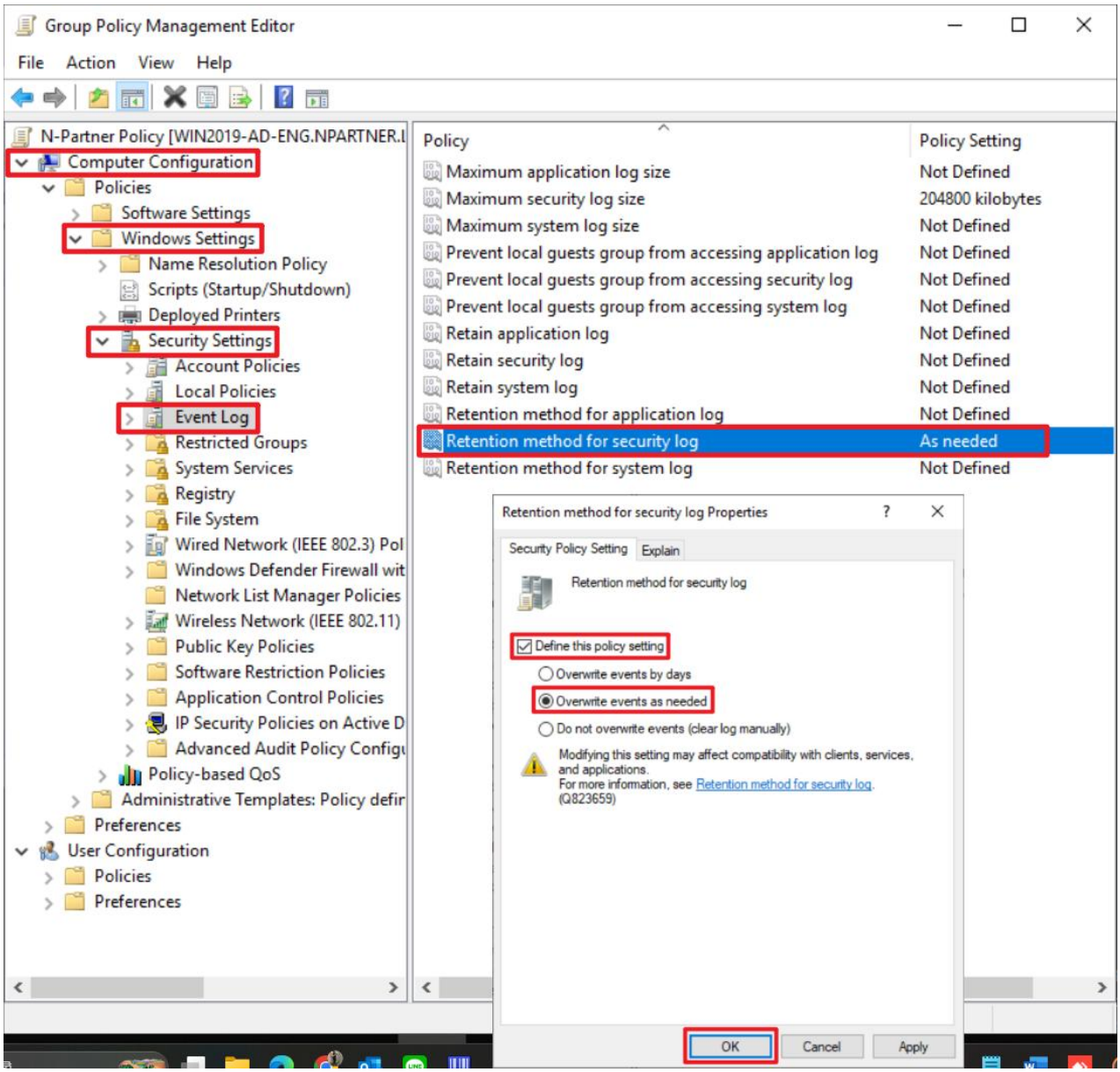
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “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” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

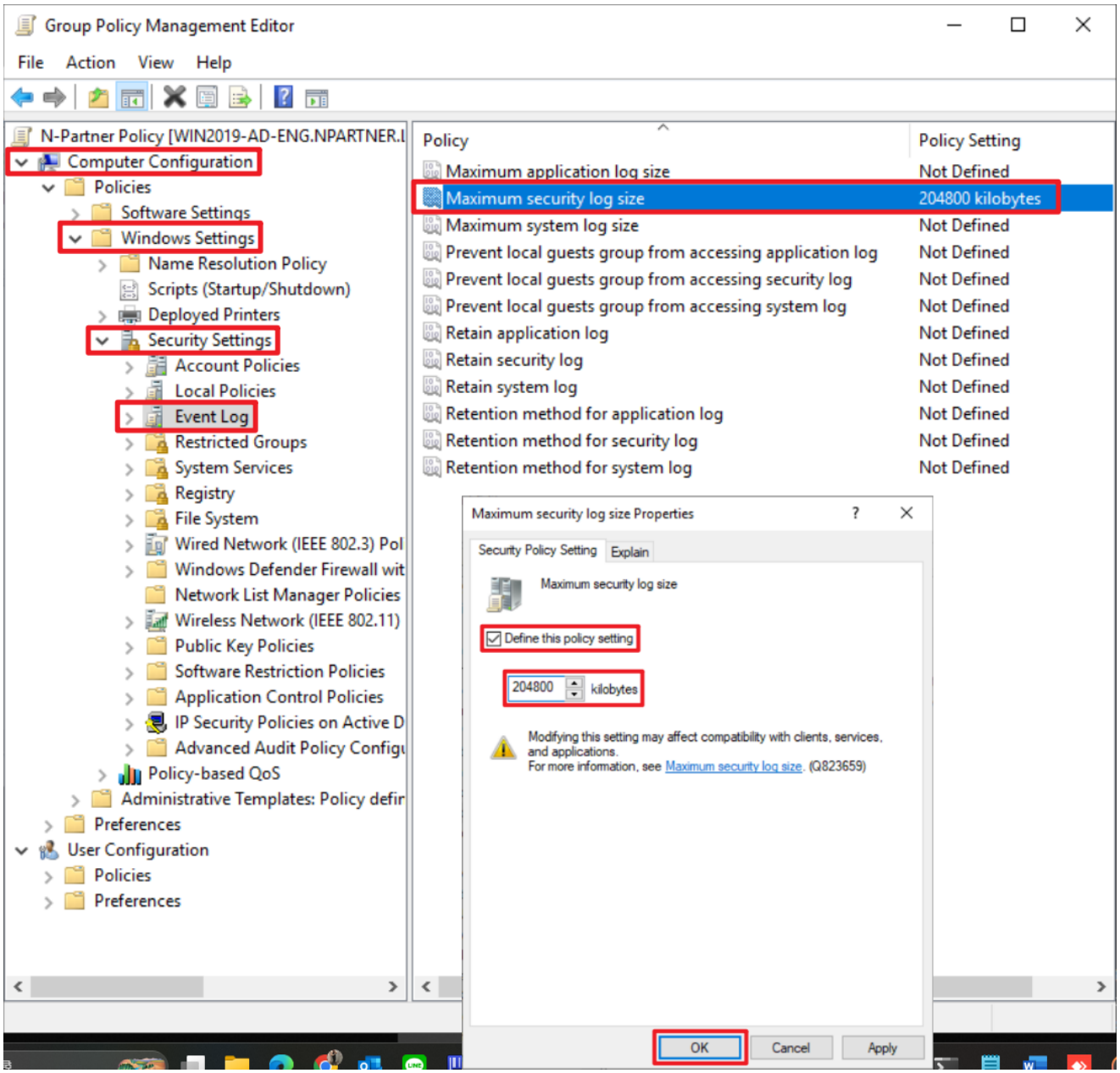
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

Expand folder “Computer Configuration” → “Policies” → “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.”



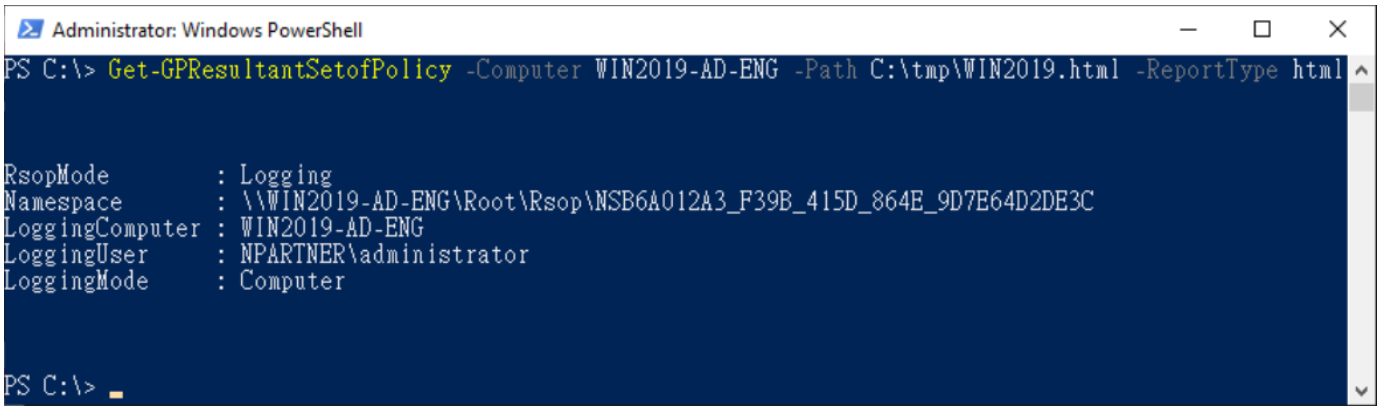
(8) On the AD domain server, open “Windows PowerShell.”

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

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

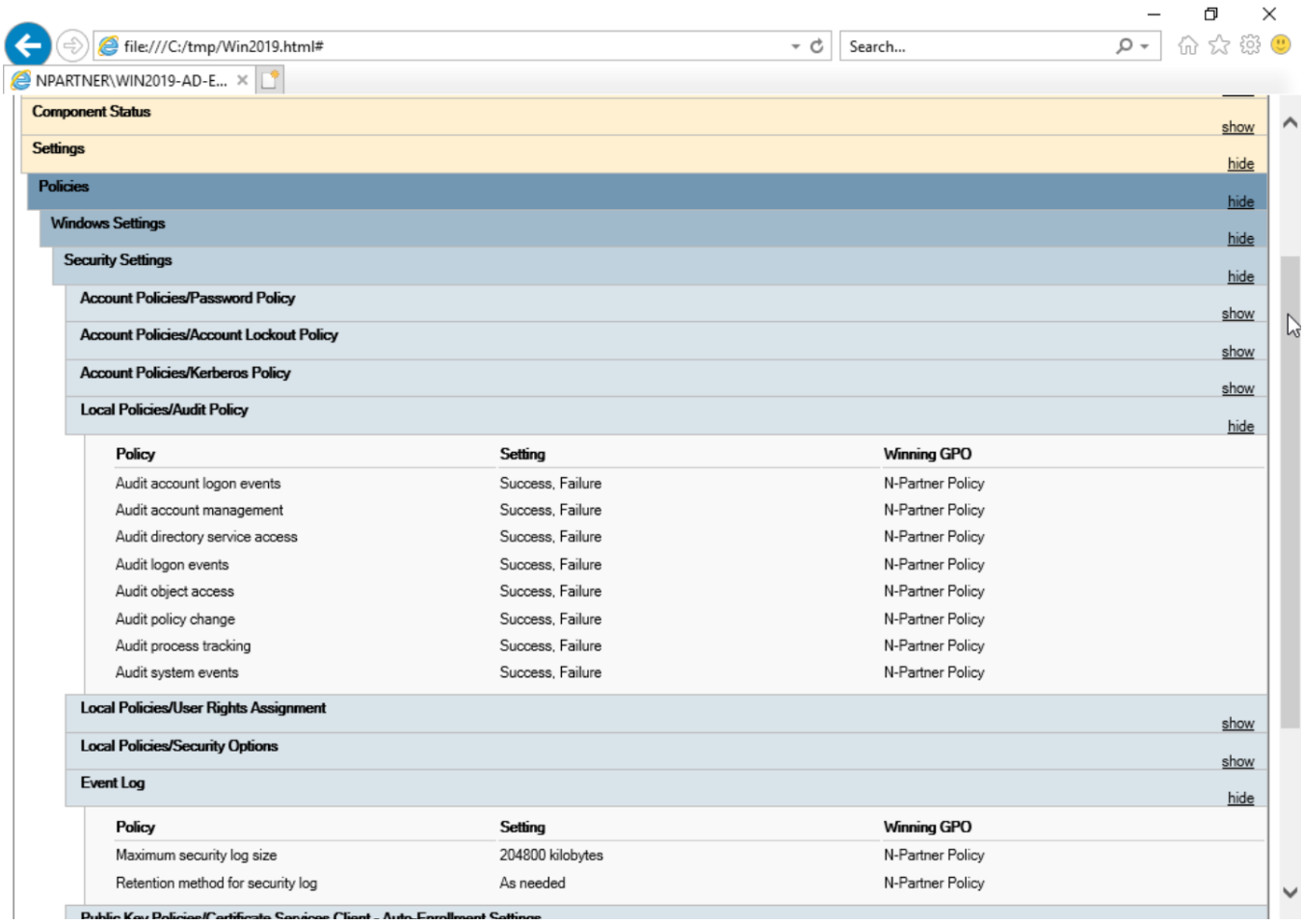
(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2019-AD-ENG -Path C:\tmp\Win2019.html -ReportType html
```



For the red text , please enter the Windows File 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.

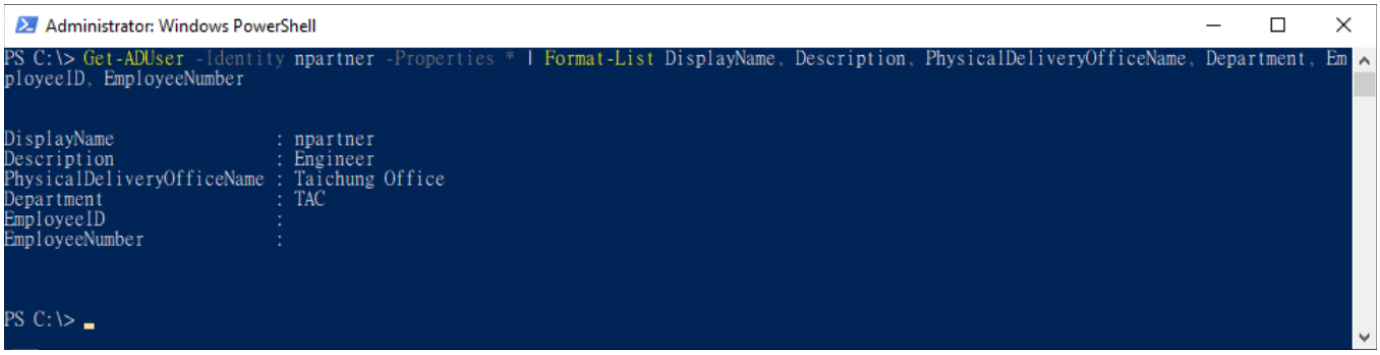


7.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Enter the command below to check whether N-Reporter associates Windows AD with available user data.

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description,
PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



Replace the red text with the username according to the actual environment.

(2) In “Event Query,” click the information of “Username.”

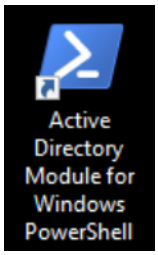
Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

7.3.1 Add Non-Admin Accounts

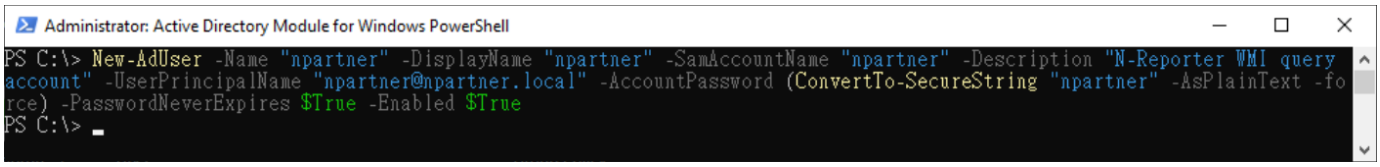
(1) Open “Active Directory Module for Windows PowerShell.”



(2) Create an Account

Enter the command below to create an account:

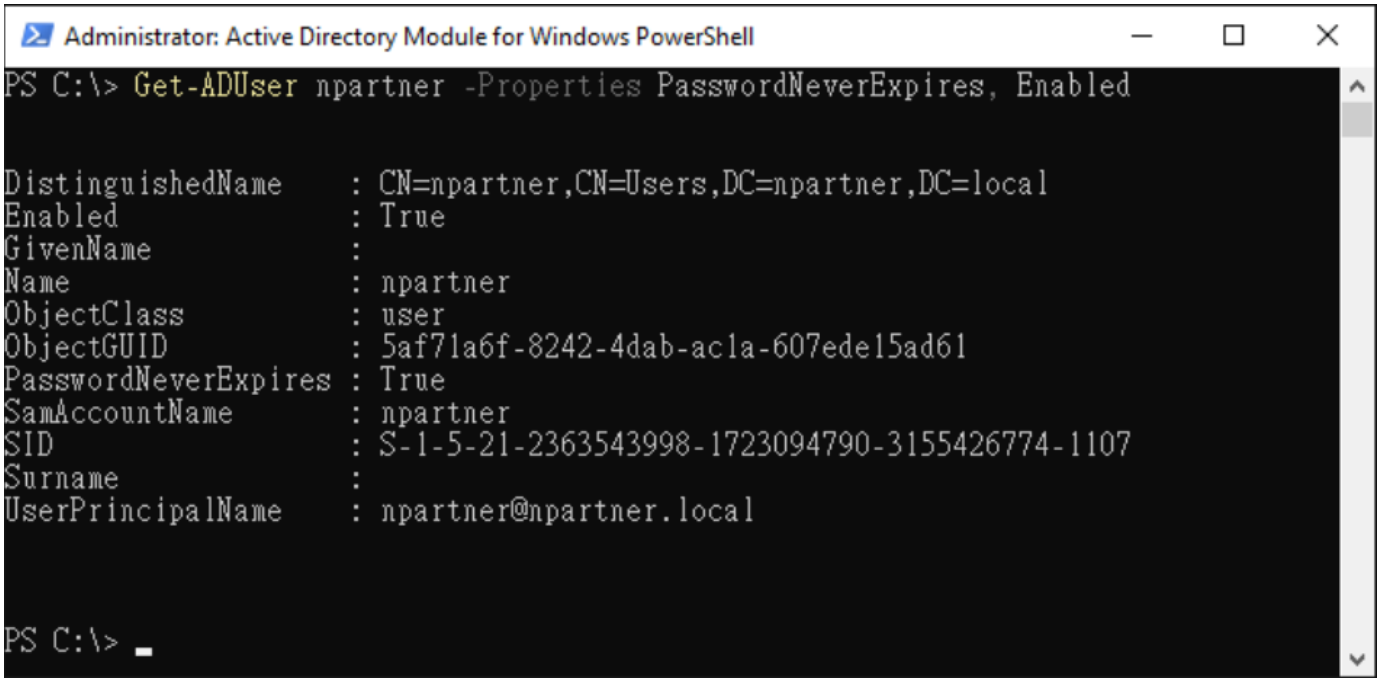
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

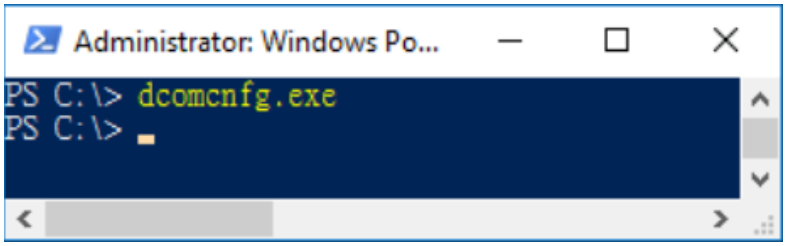


7.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”

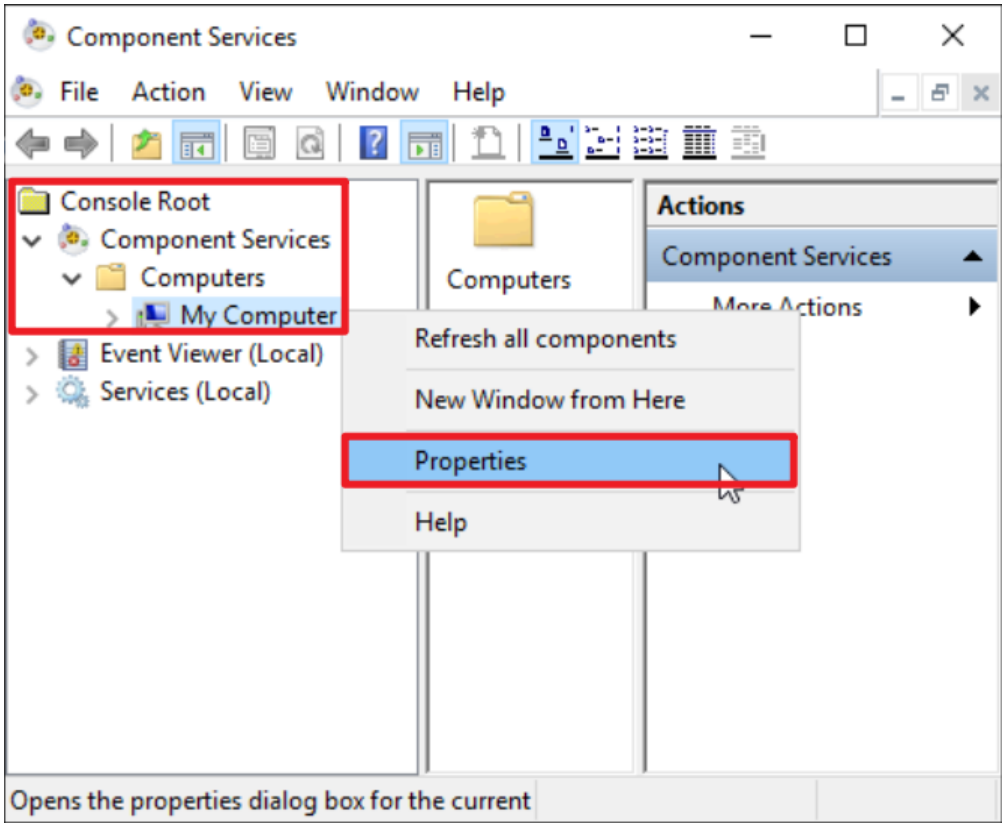
(2) Enter the command below to enable component services.

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



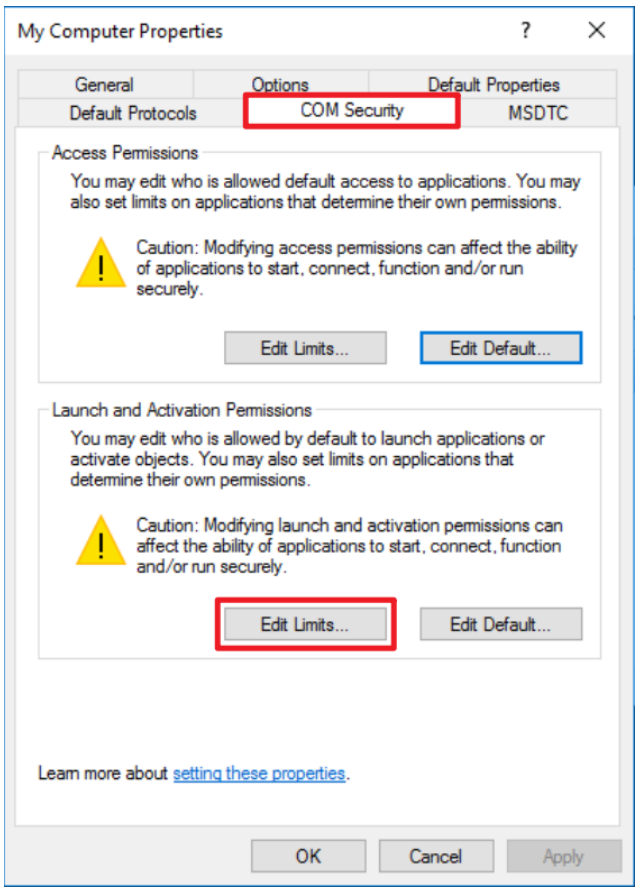
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



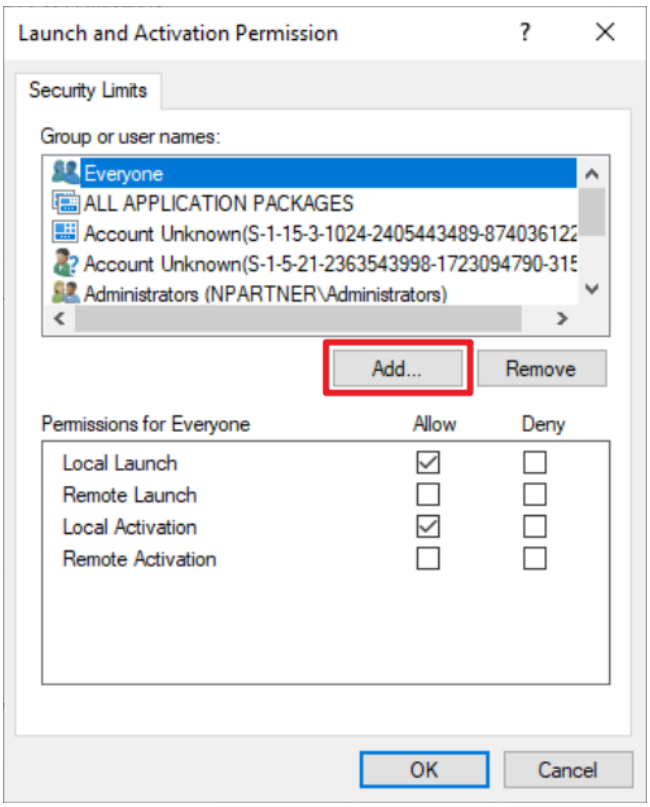
(4) Enable Permissions

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



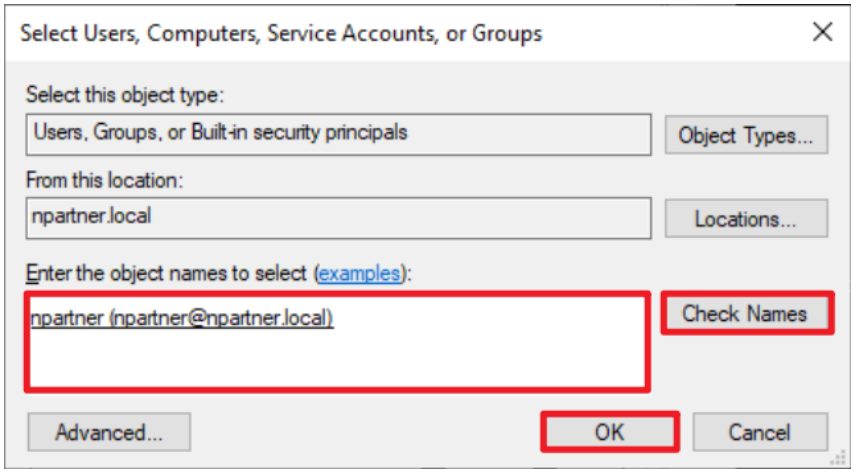
(5) Add DCOM User Permissions

Click “Add.”



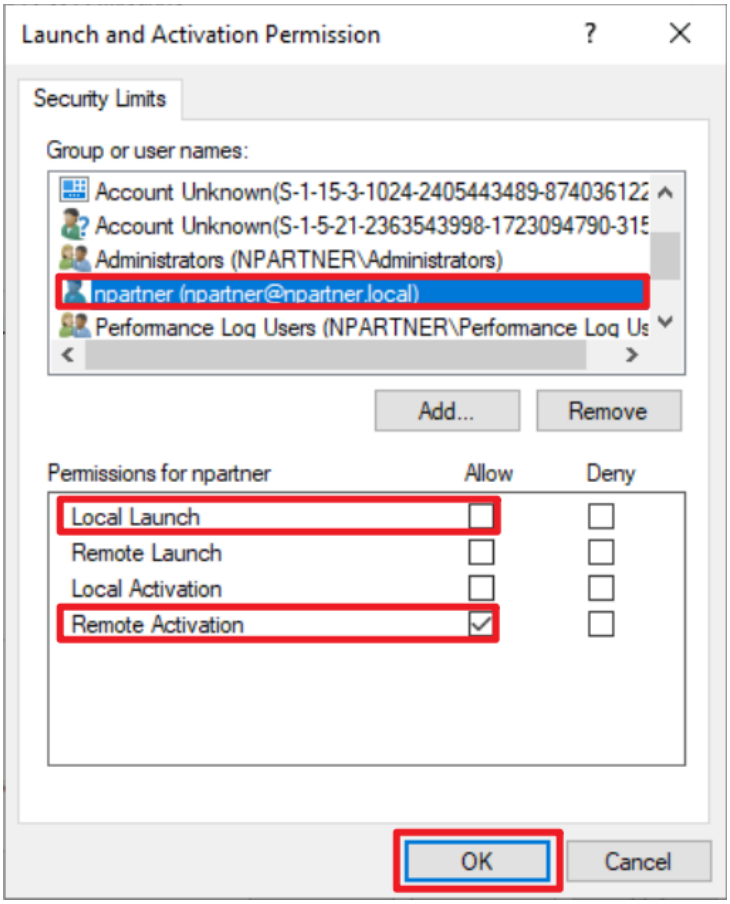
(6) Enter Your Username

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

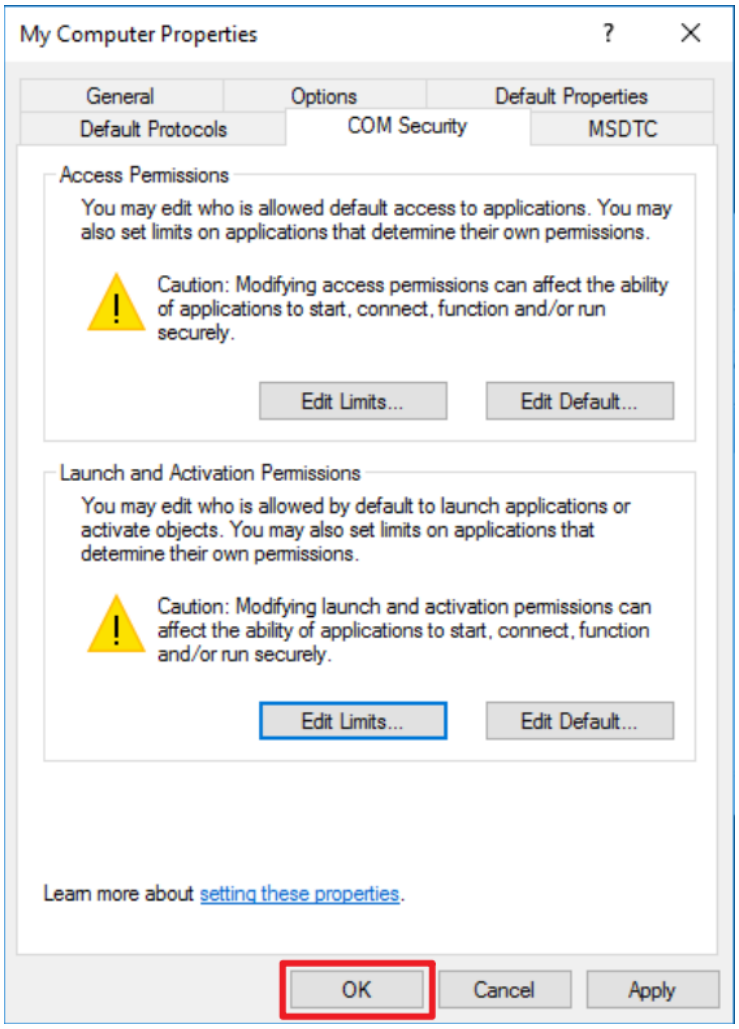


(7) Configure your User Permission

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



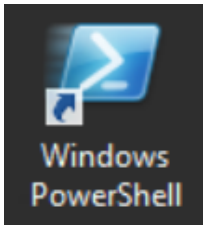
(8) Click "OK.”



7.3.3 Configure WMI Permissions

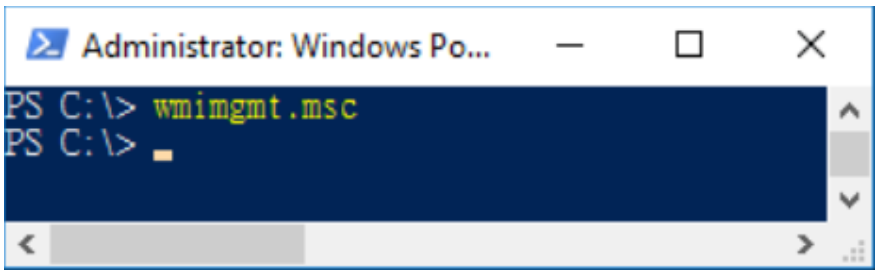
7.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



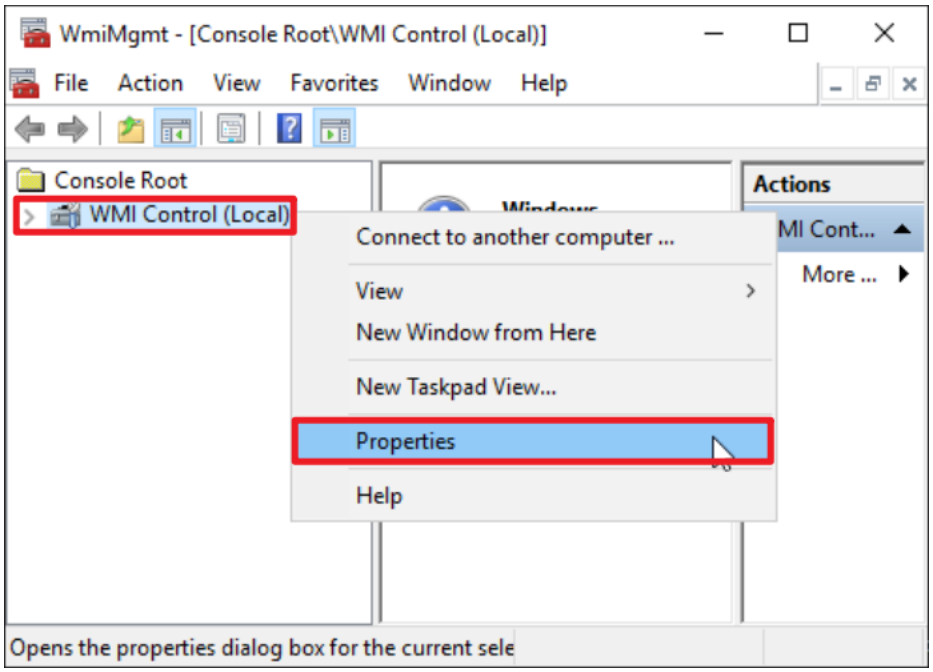
(2) Enter the command to enable WMI control service.

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



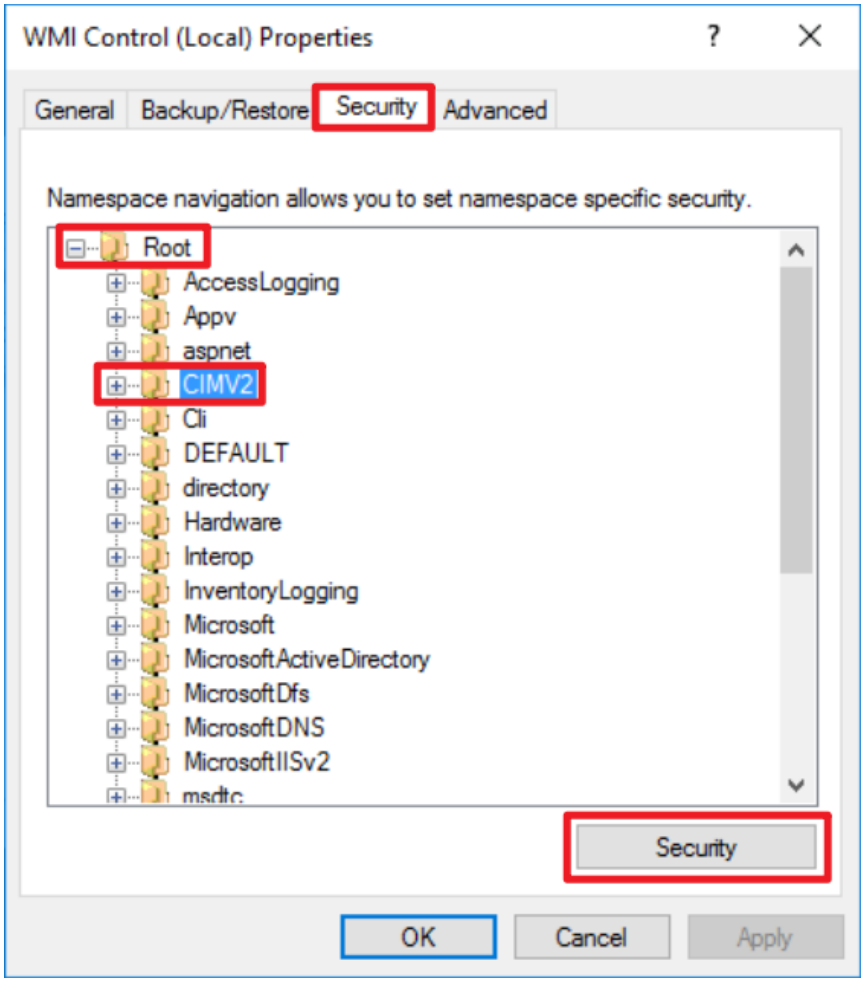
(3) Edit WMI Control

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



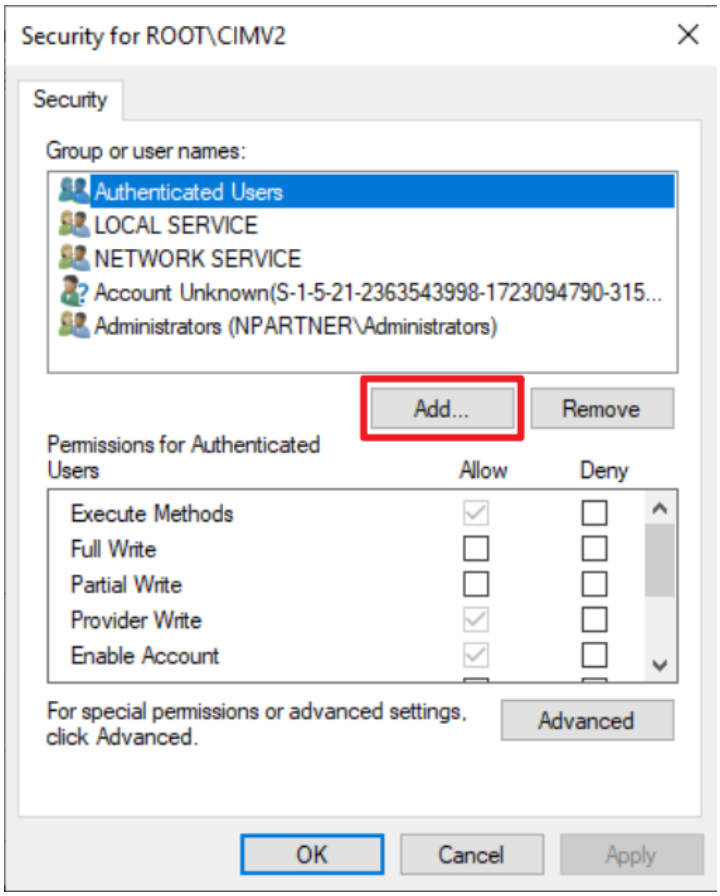
(4) Edit CIMV2 Security

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



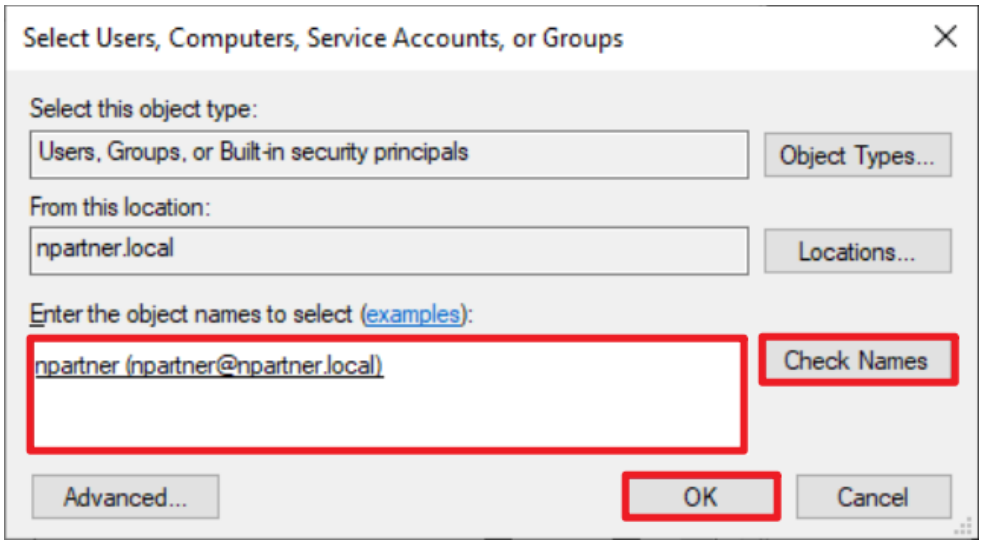
(5) Add WMI User Permissions.

Click “Add.”



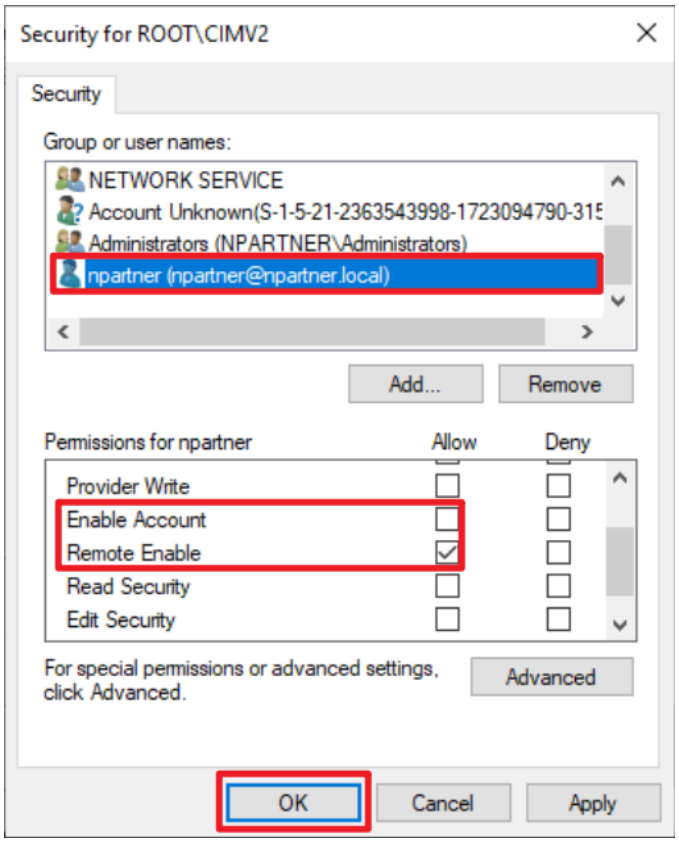
(6) Enter Your Username

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

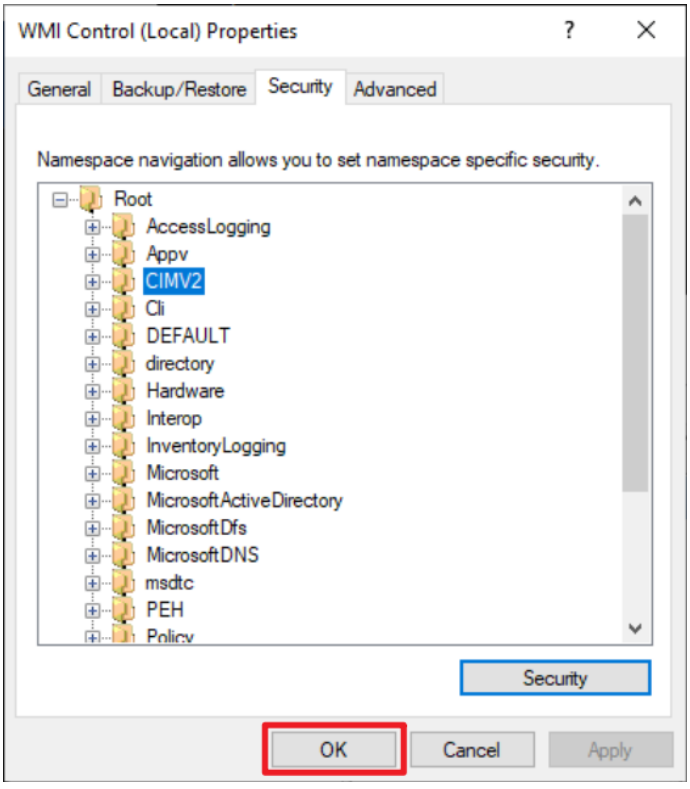


(7) Set Your User Permissions

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

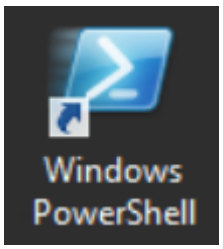


(8) Click “OK.”



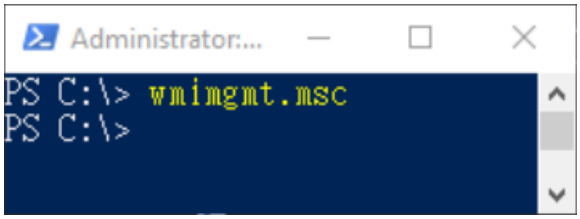
7.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



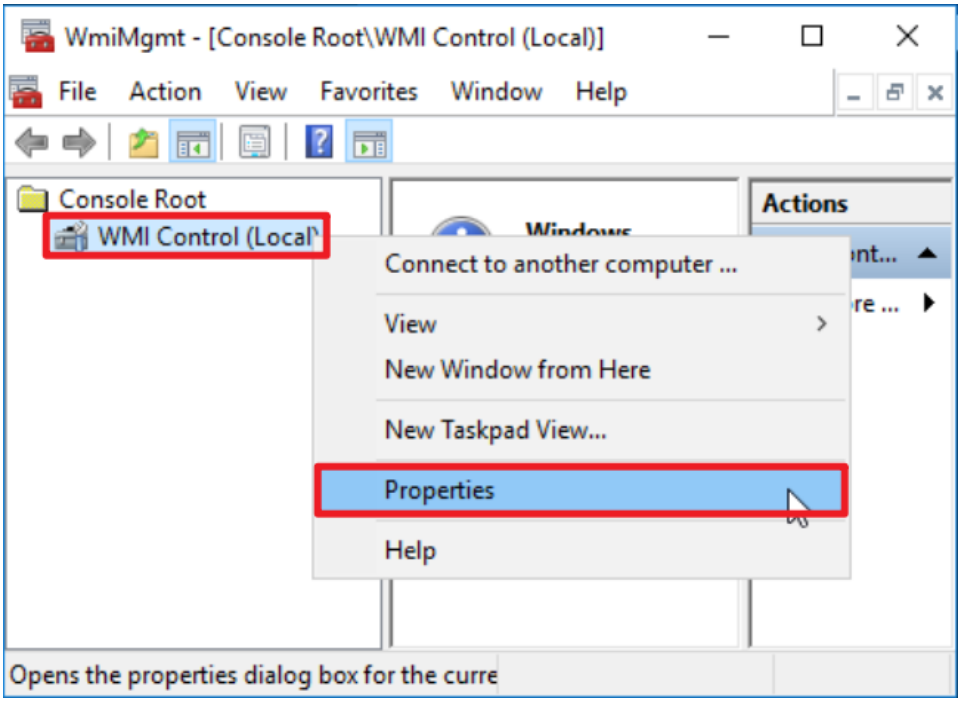
(2) Enter the command below to enable WMI Control.

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



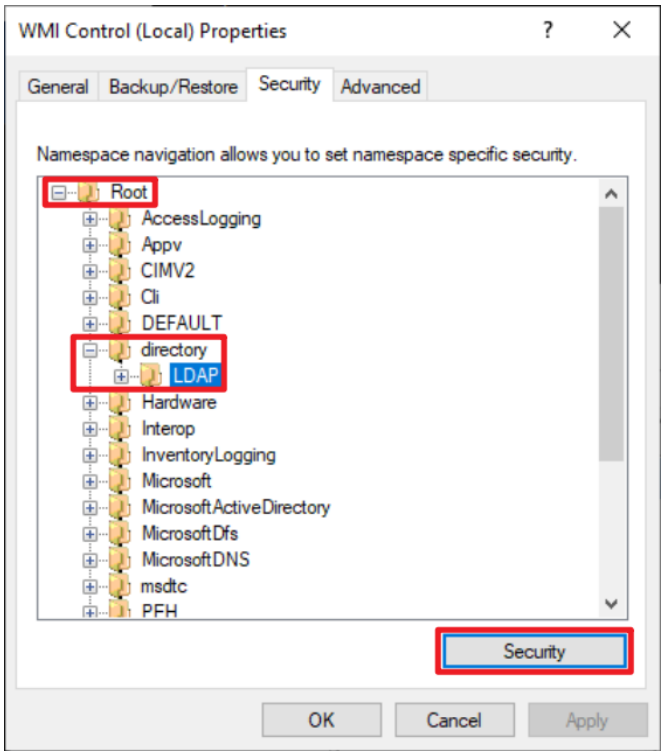
(3) Edit WMI Control

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



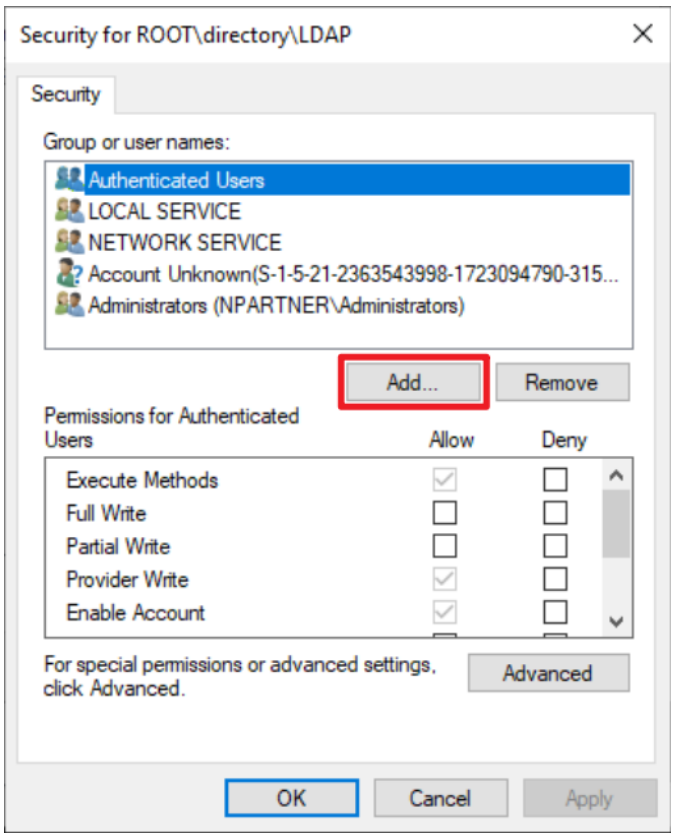
(4) Edit LDAP Security

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



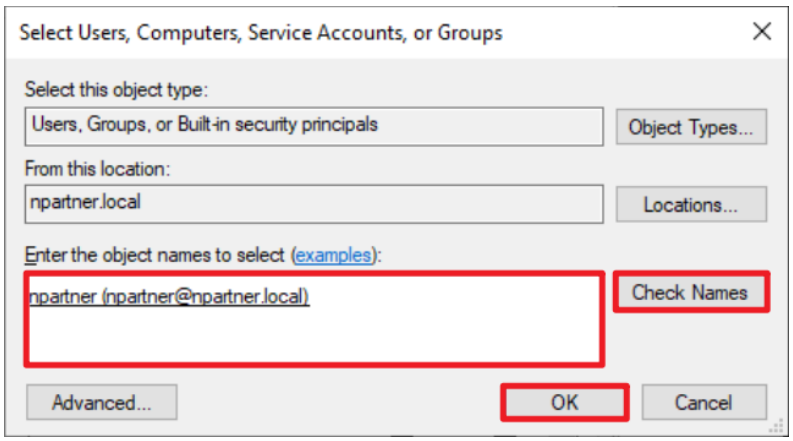
(5) Add WMI User Permissions

Click “Add.”



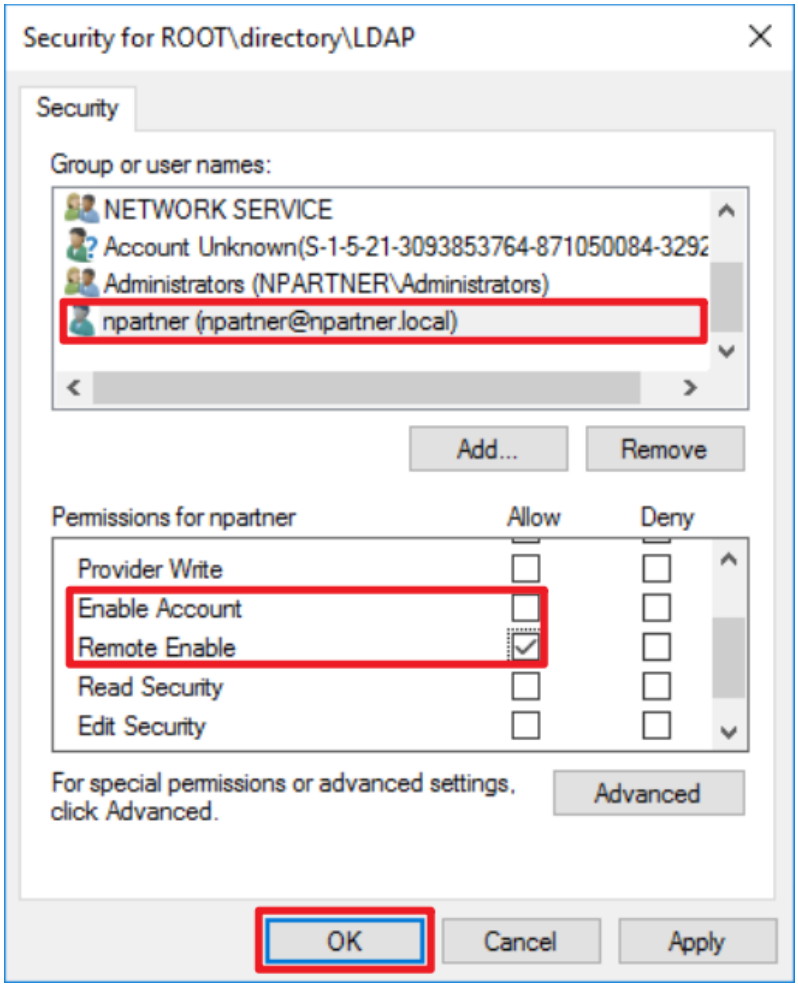
(6) Enter Your Username

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

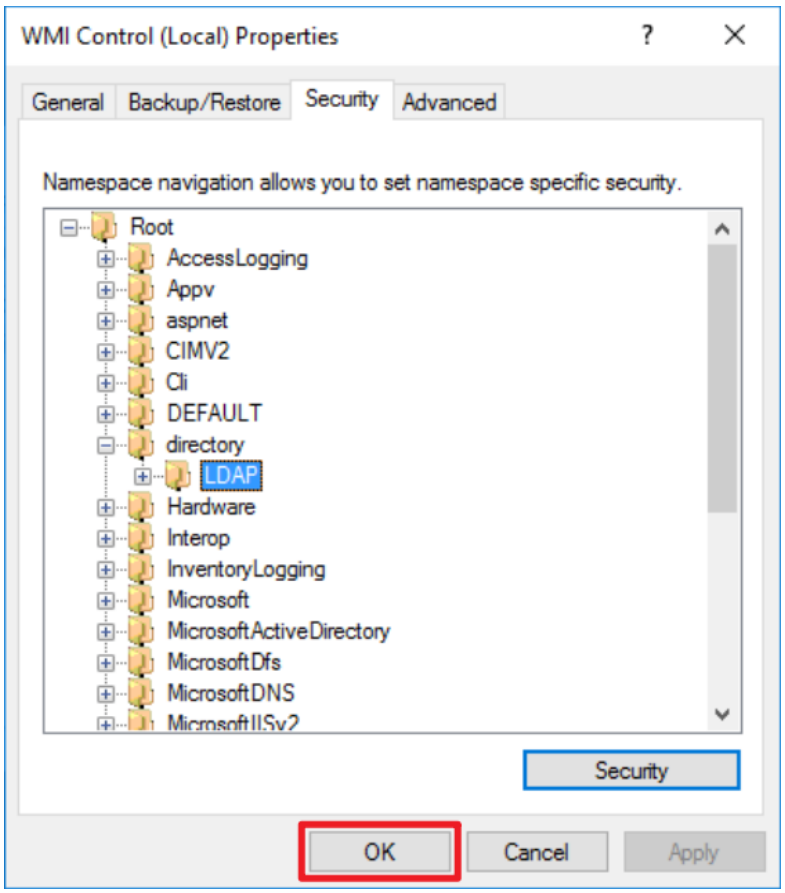


(7) Set Your User Permissions

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

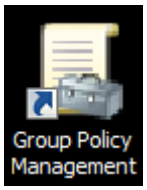


(8) Click “OK.”

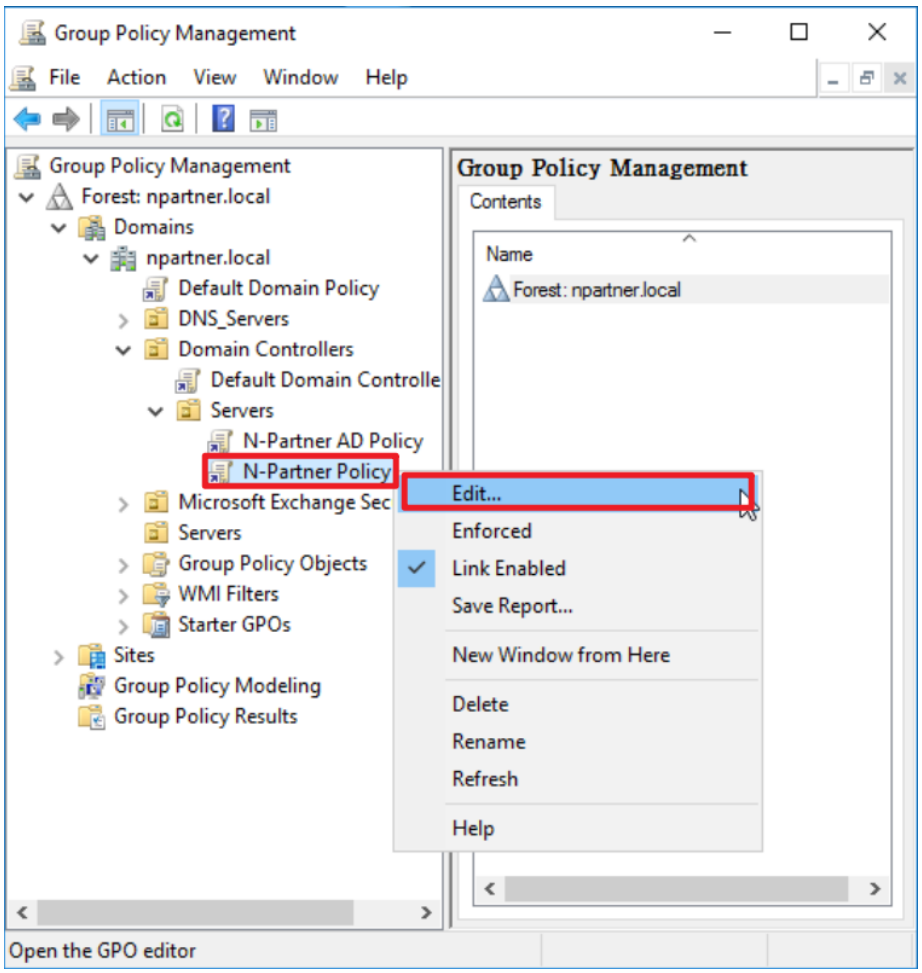


7.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

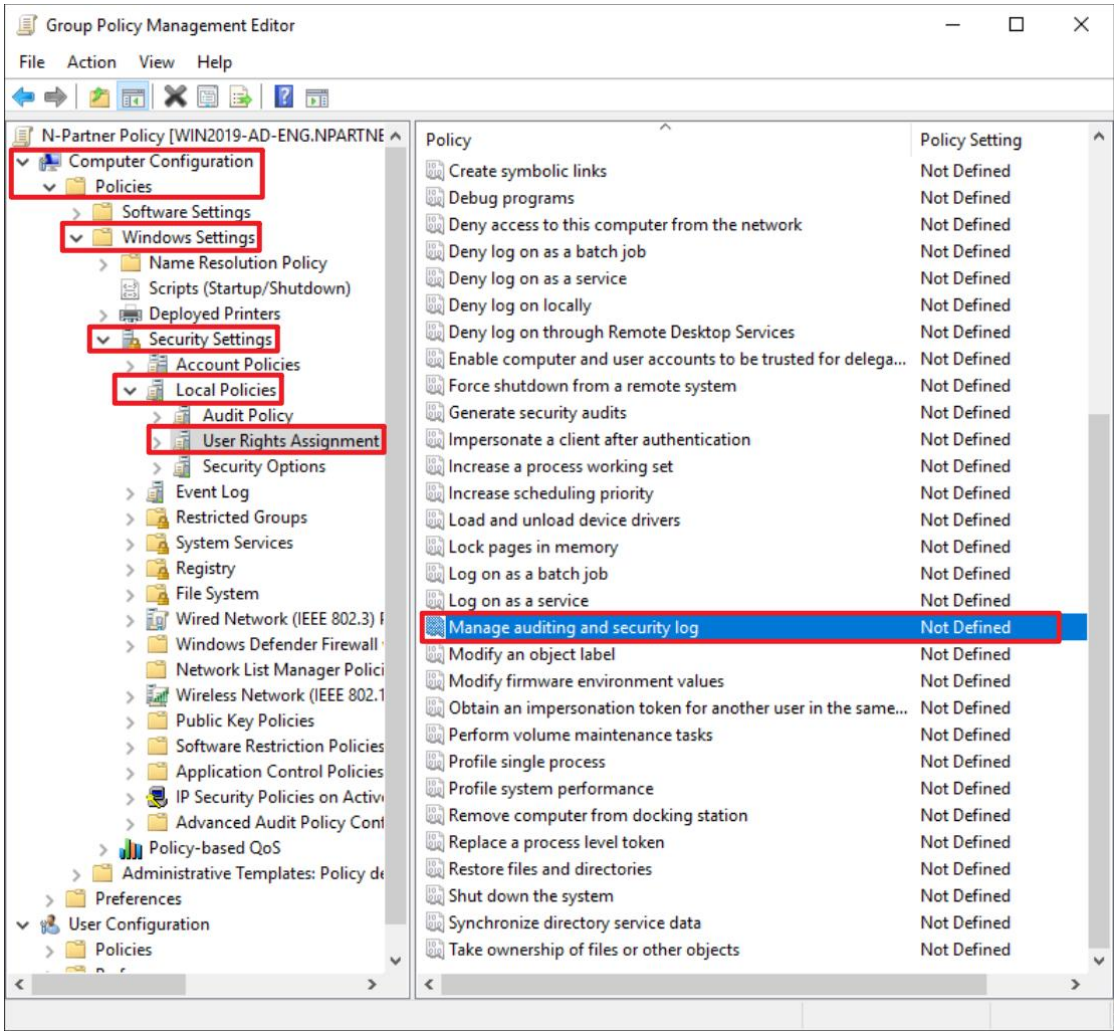


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



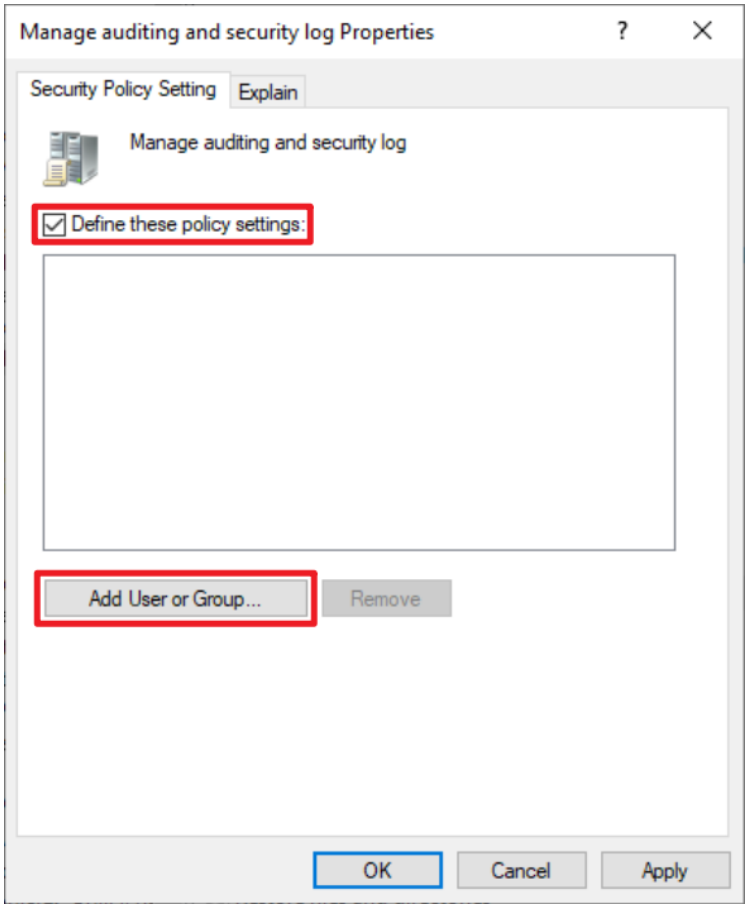
(3) Configure Auditing Log

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



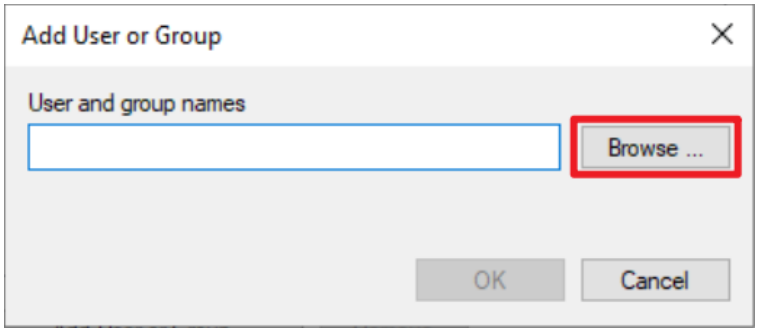
(4) Add Auditing User

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



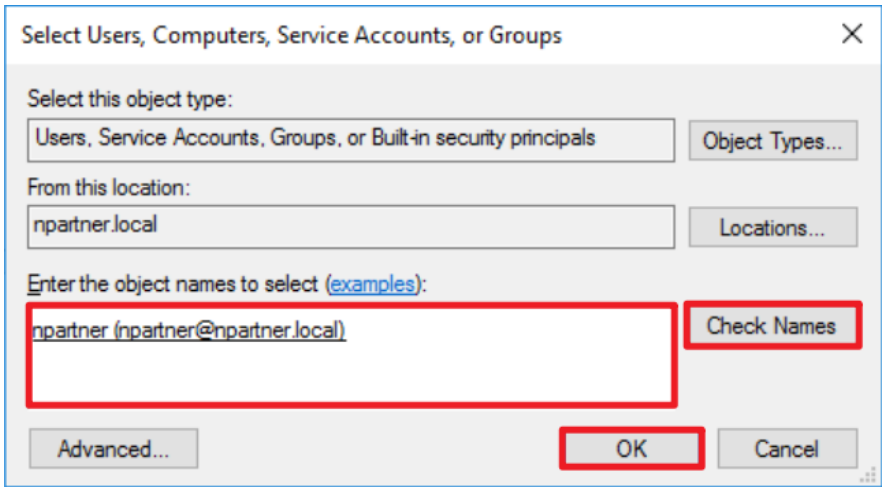
(5) Search for User

Click “Browse.”

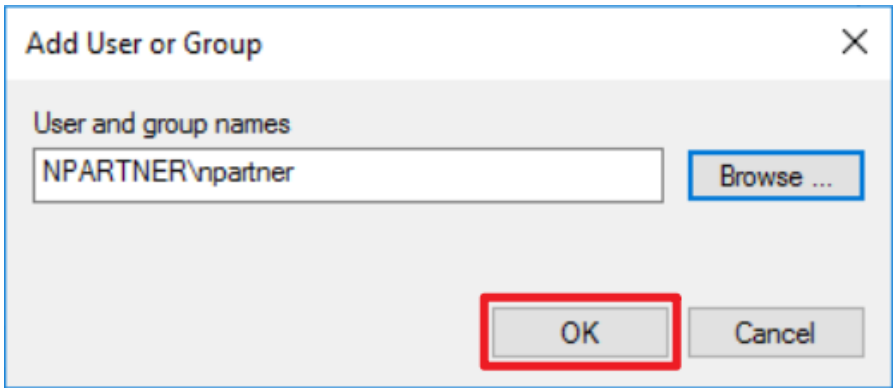


(6) Enter Your User Account

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

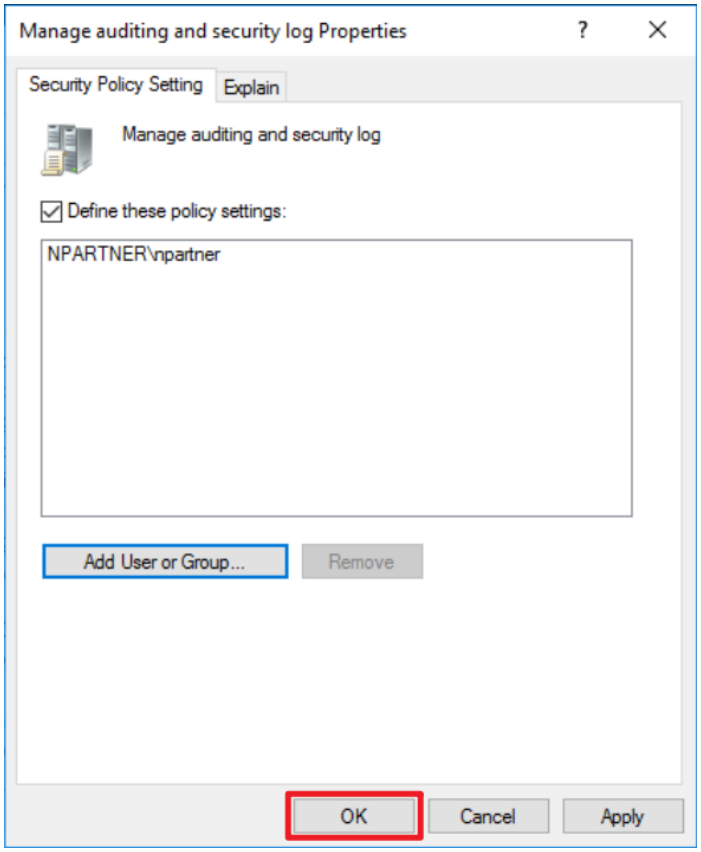


(7) Click “OK.”



(8) Confirm Audit Log Settings

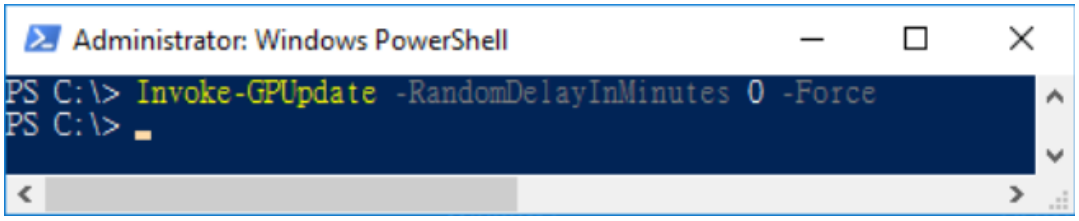
Click “OK.”



(9) Open “Windows Powershell.”

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

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

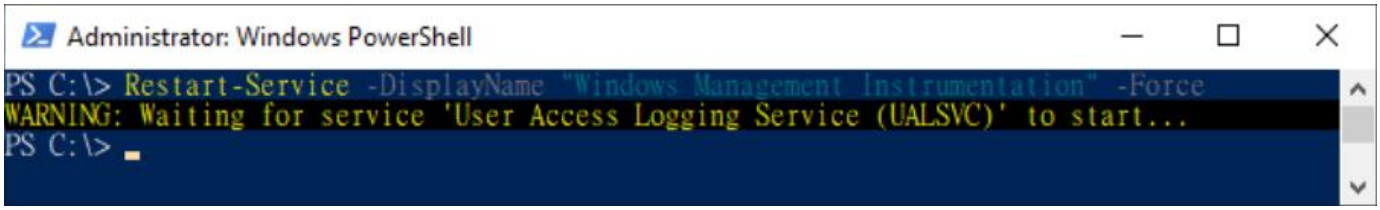


7.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”

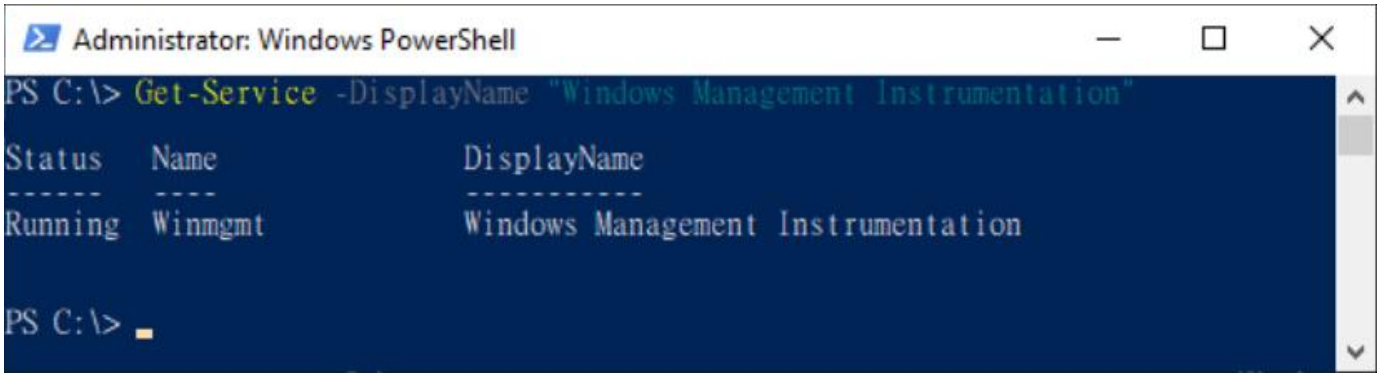
(2) Enter the command below to disable the WMI service.

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



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

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

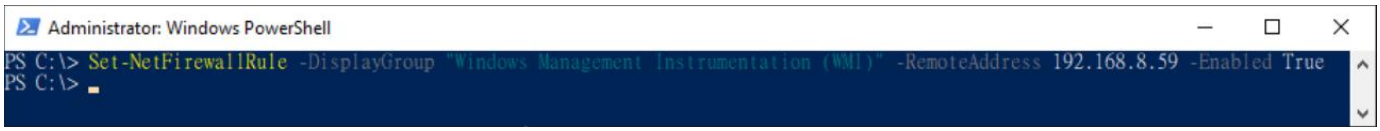


7.3.6 Configure the Firewall

(1) Open “Windows Powershell.”

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

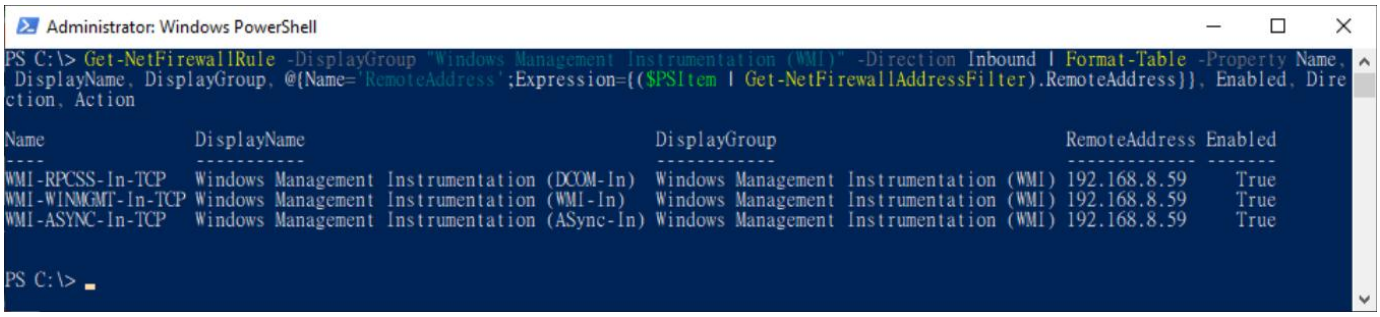
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True
```



Replace the red text with the N-Reporter IP address.

(3) Enter the command below to show the current firewall WMI configuration:

```
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
```



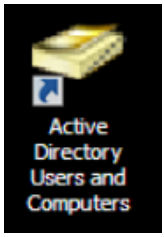
8. Windows Server 2022

Windows Audit Policy Configuration:

For detailed information, refer to the **Audit Policy Recommendations link** in the references.

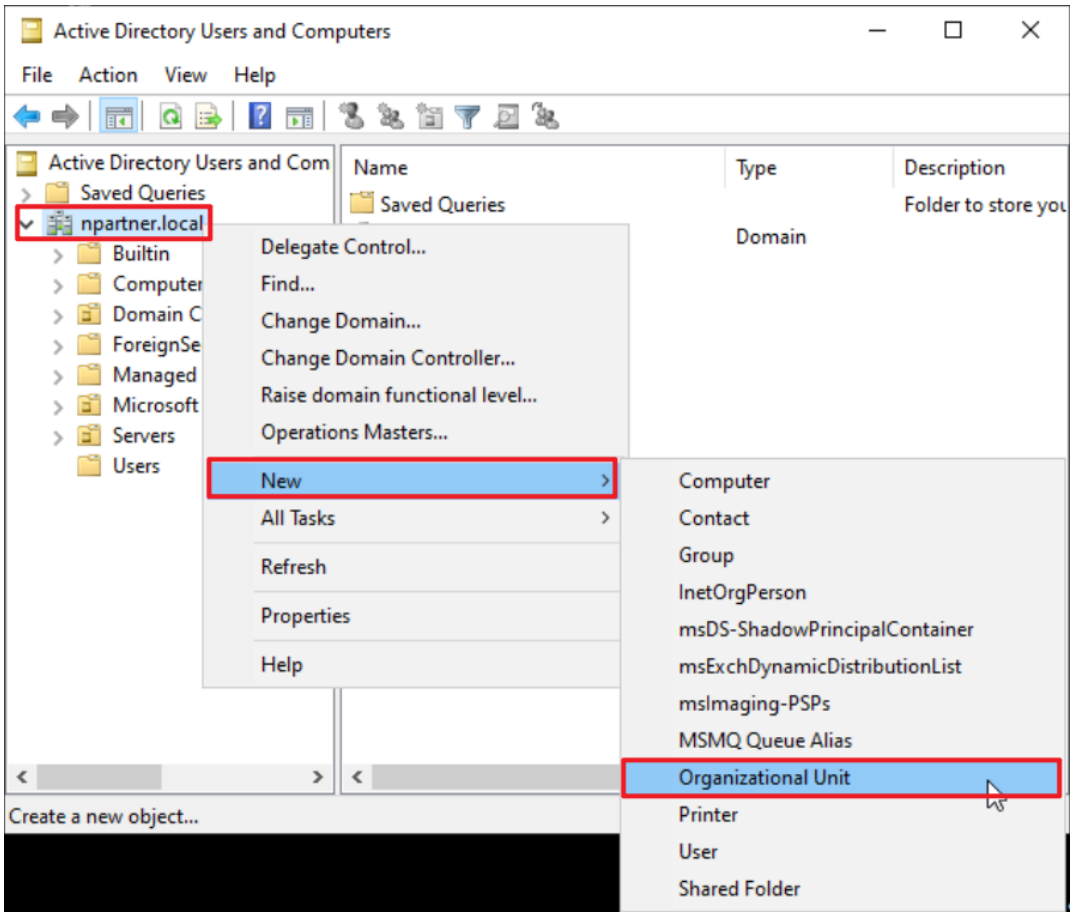
8.1 Organizational Unit (OU) Configuration

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



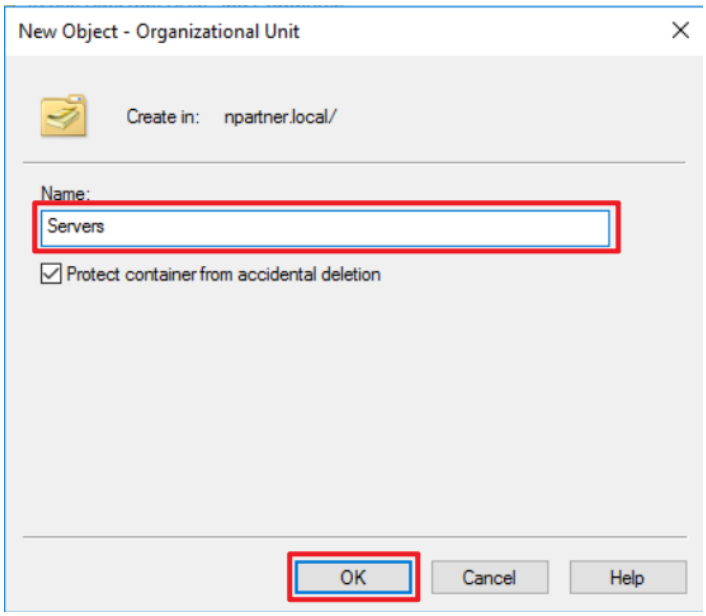
(2) Add an Organizational Unit

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



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

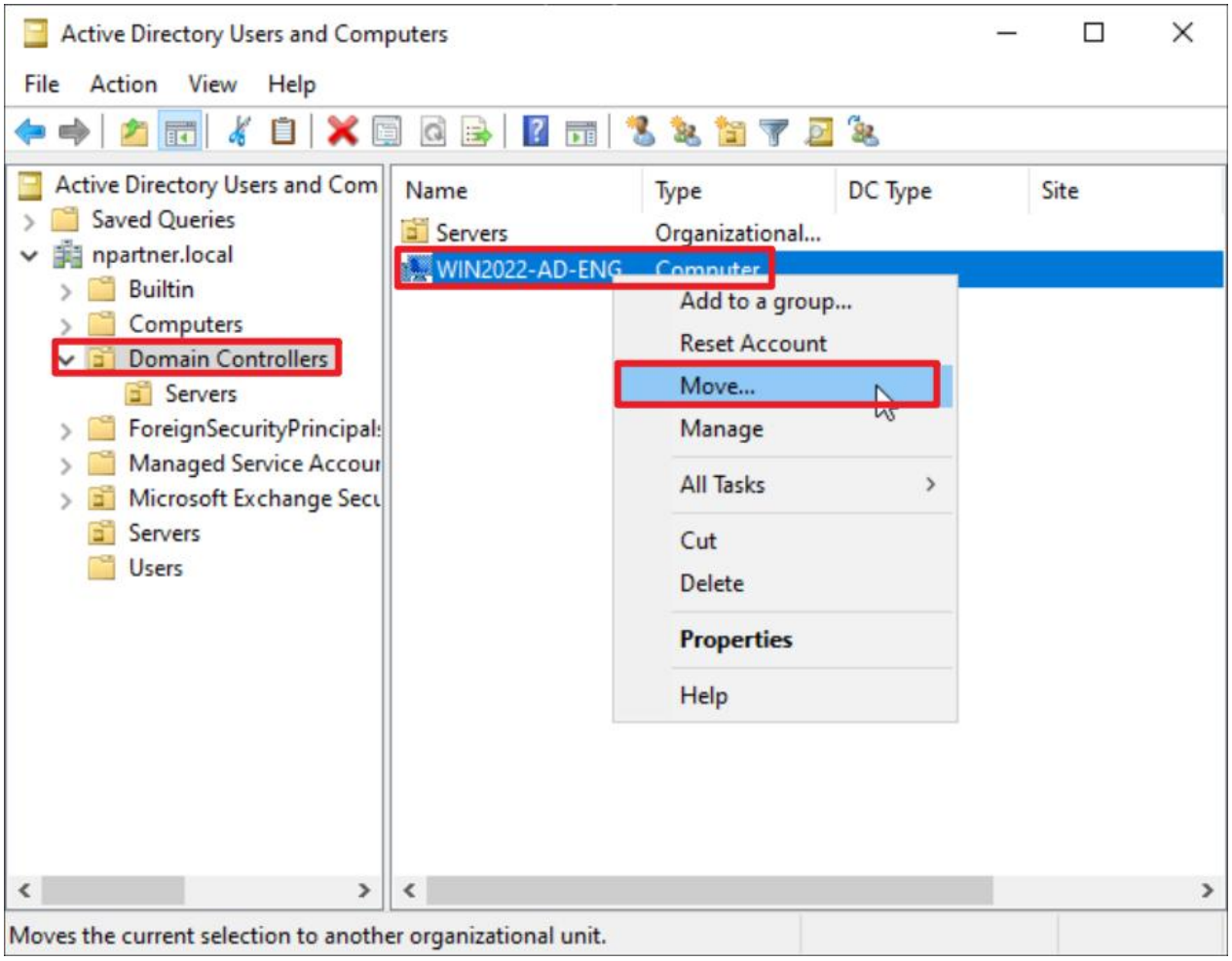
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

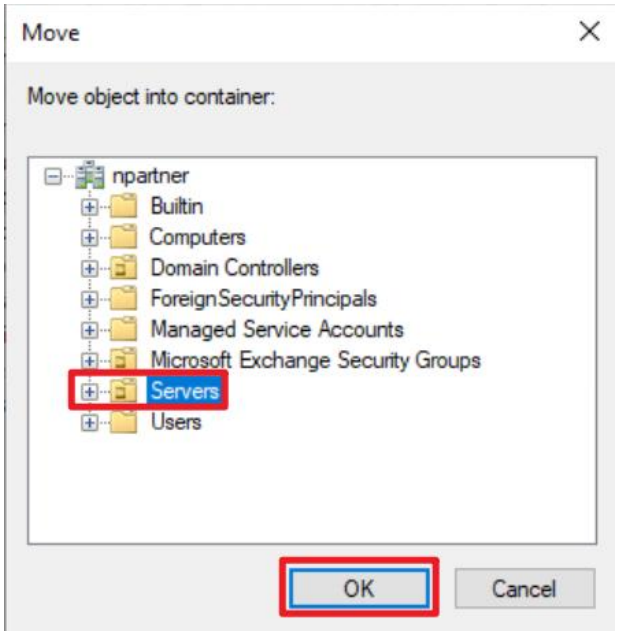
Select your organizational unit in “Domain Controllers” → right-click on the “WIN2022-AD-ENG” server.

Note: Please select the Windows AD server according to the actual environment. → click “Move.”



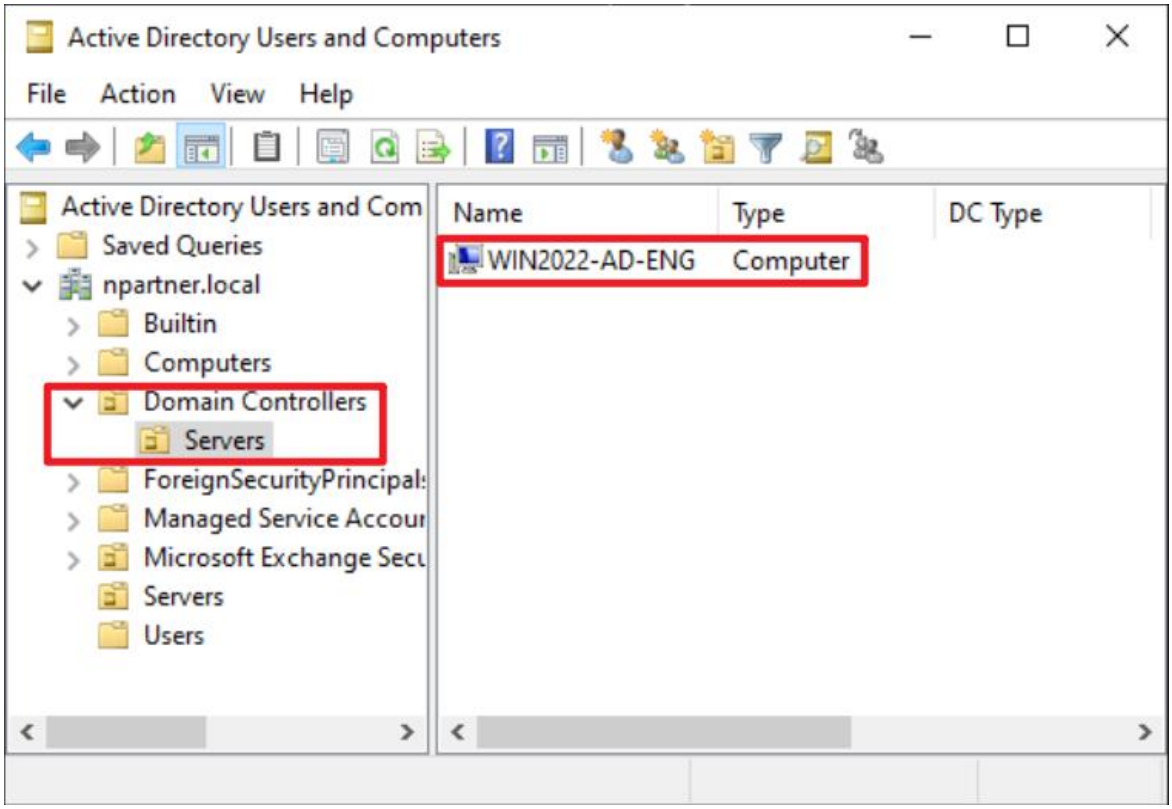
(5) Select your Organizational Unit:

Select your organizational unit (in this example, it is “Servers”) → 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”) and confirm that the “WIN2022-AD-ENG” server has been moved.

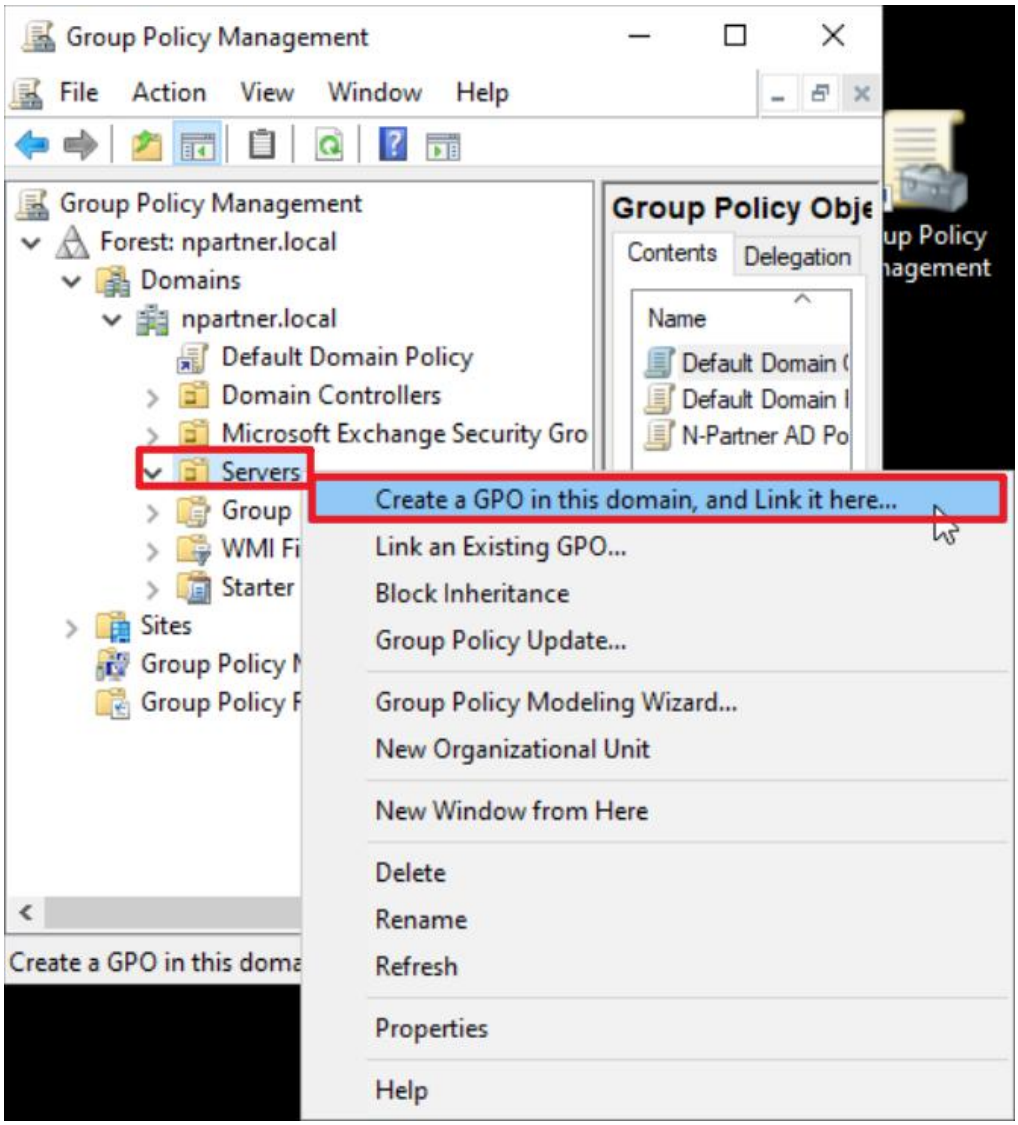


8.2 Group Policy Settings

(1) Click “Group Policy Management.”

(2) In the Servers organizational unit (OU), create a new Group Policy Object (GPO):

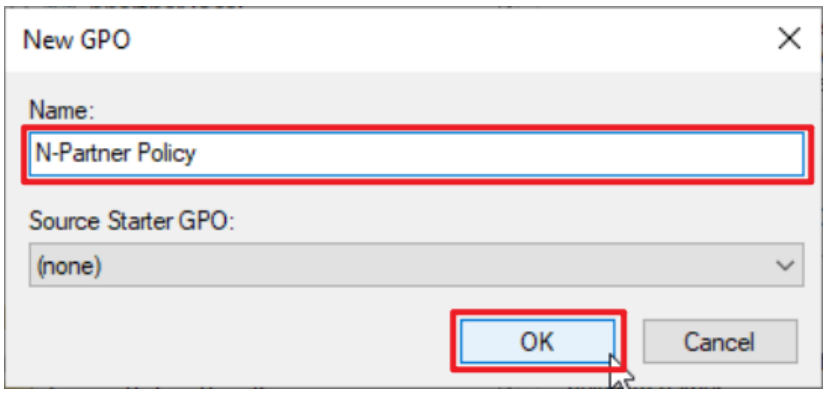
Right-click the “Servers” organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

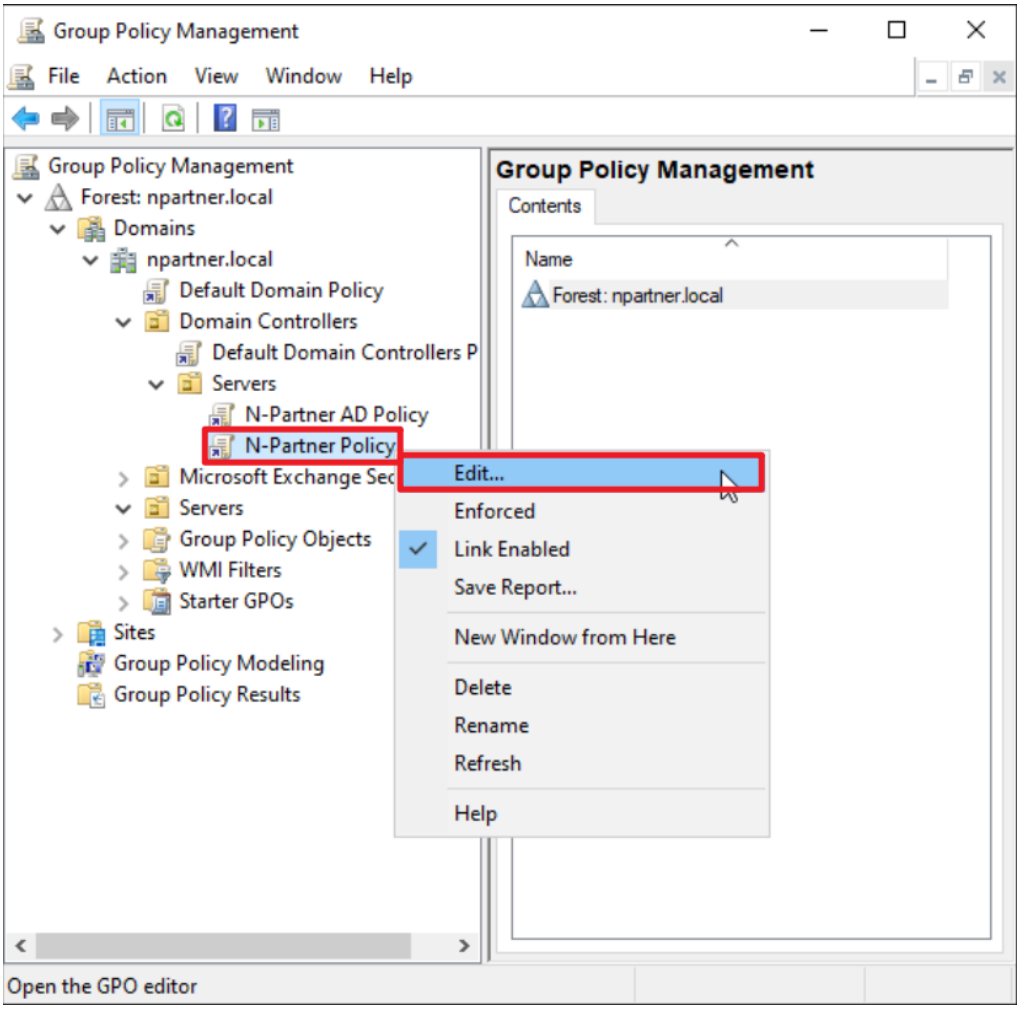
Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

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



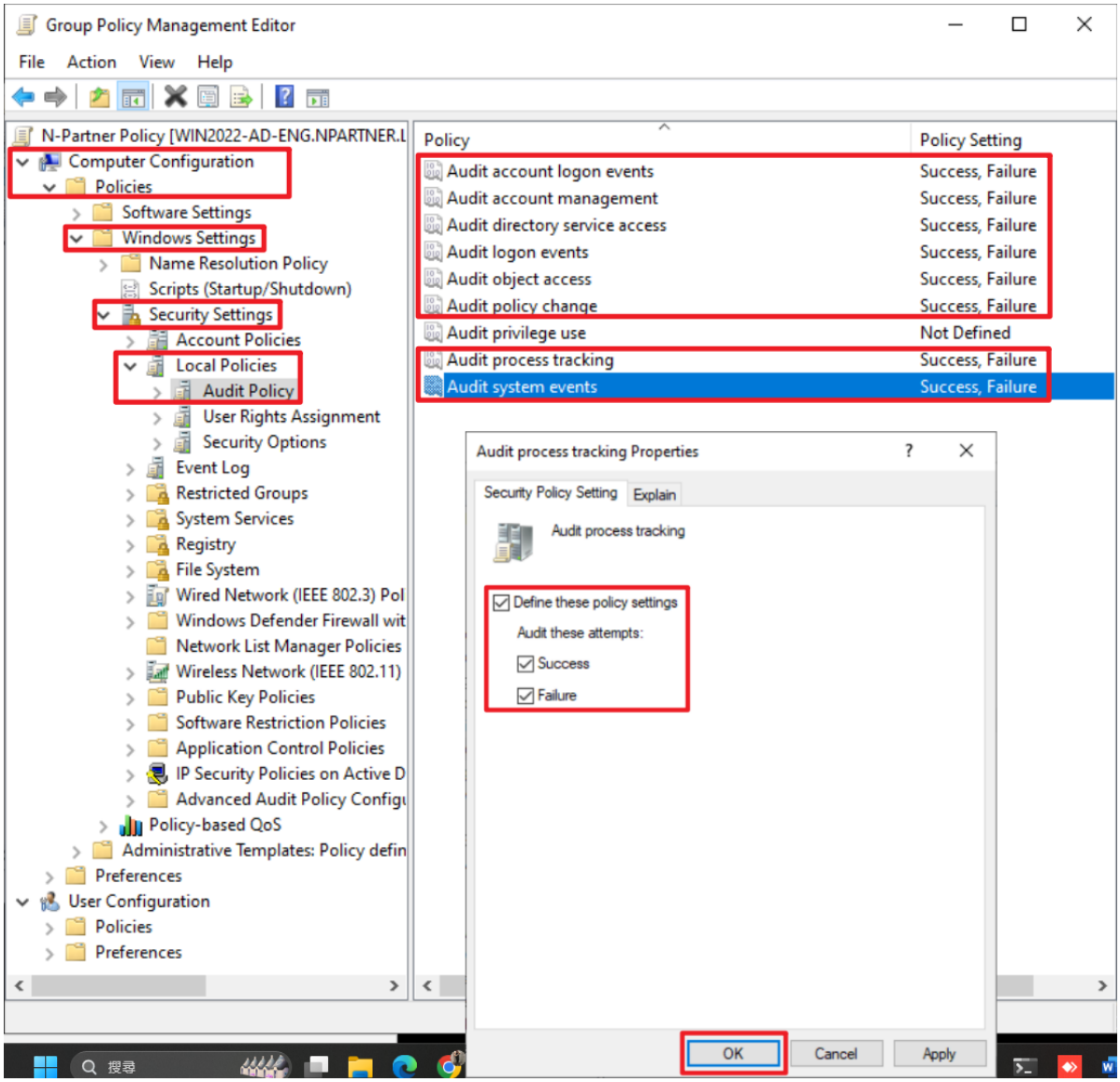
(4) Edit your Group Policy Object

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



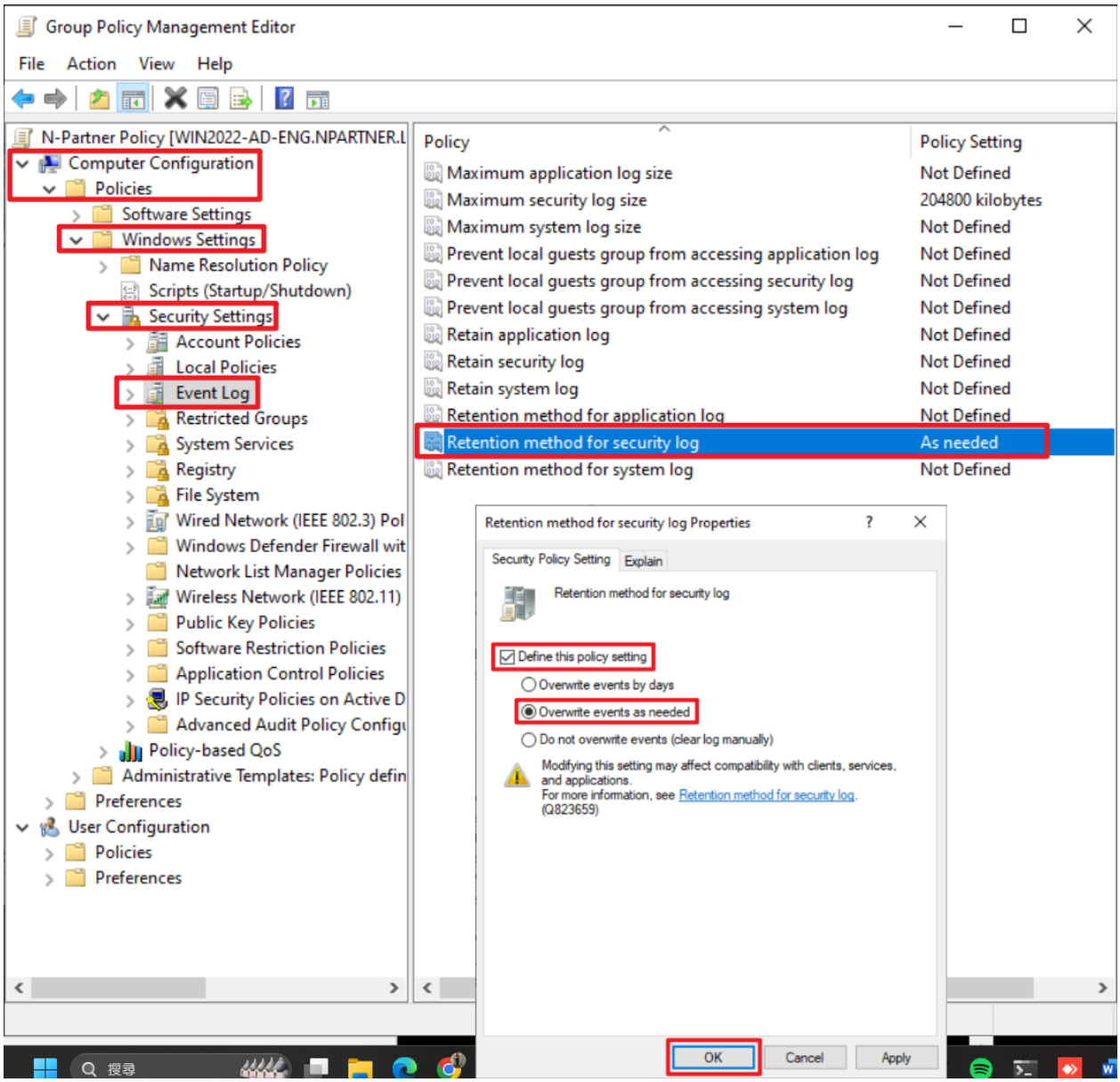
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “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” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

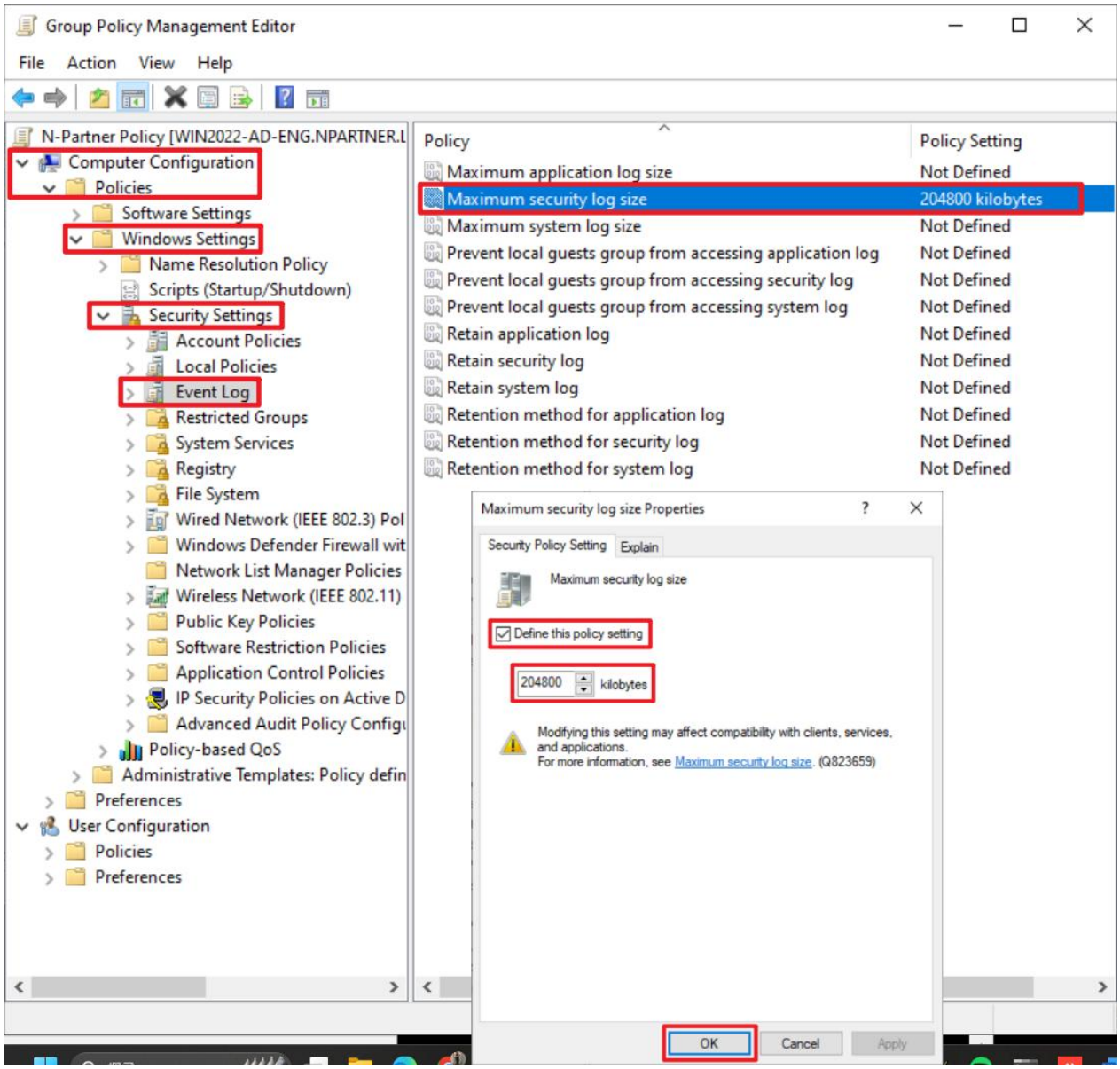
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(7) Event Logs: Maximum Size of Security Log

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

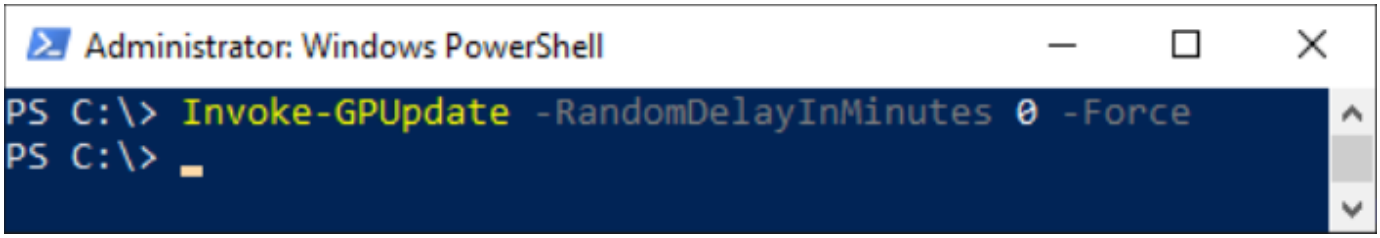
Note: Please adjust the number based on the actual environment. → click “OK.”



(8) Open “Windows PowerShell.”

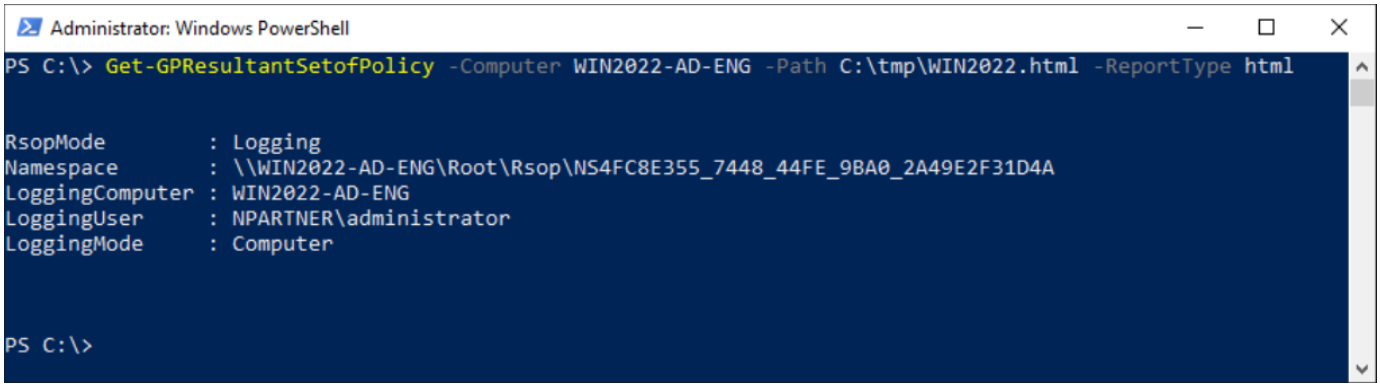
(9) Enter the command below to refresh group policy.

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



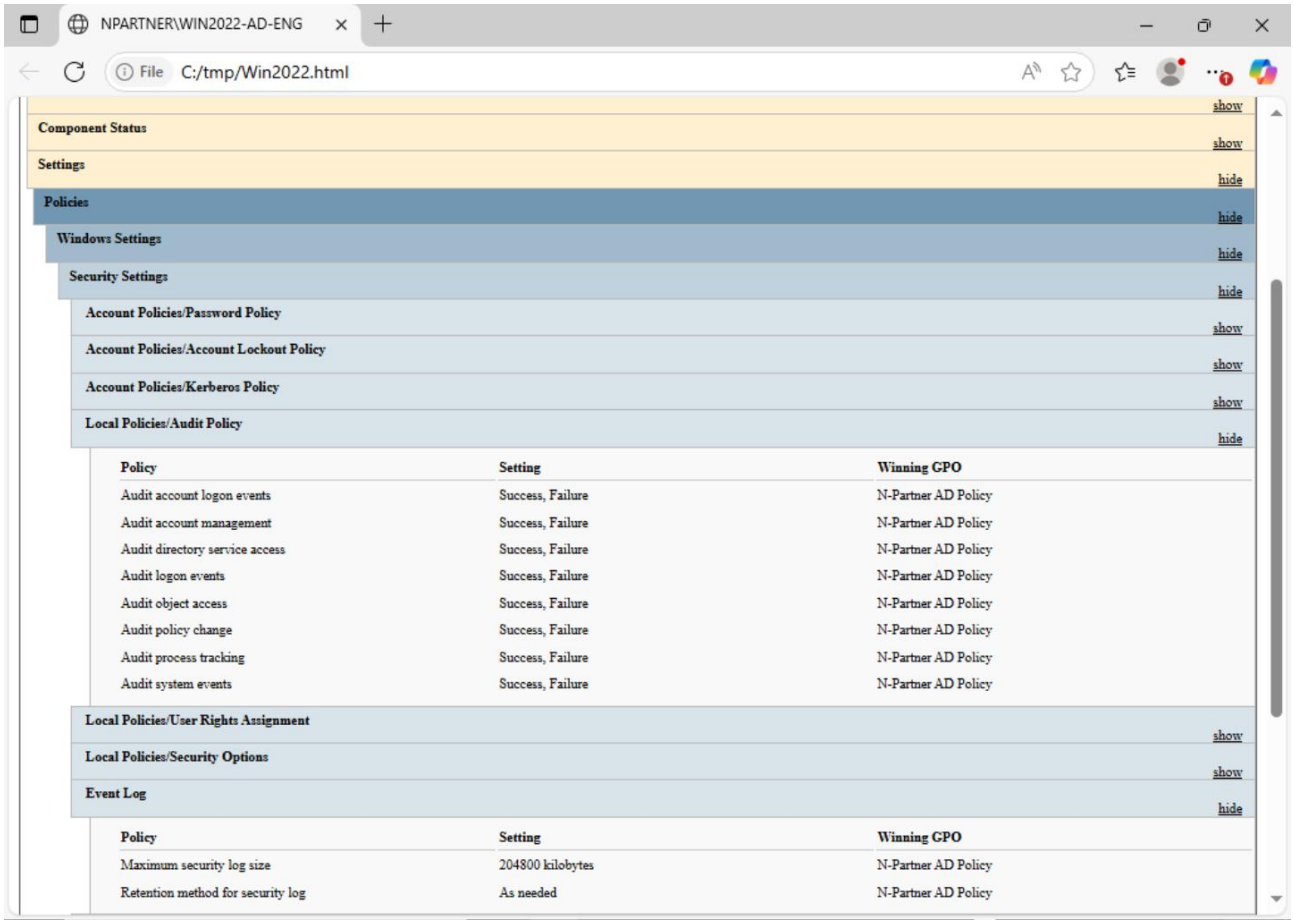
(10) Enter the command below to generate server group policy report.

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

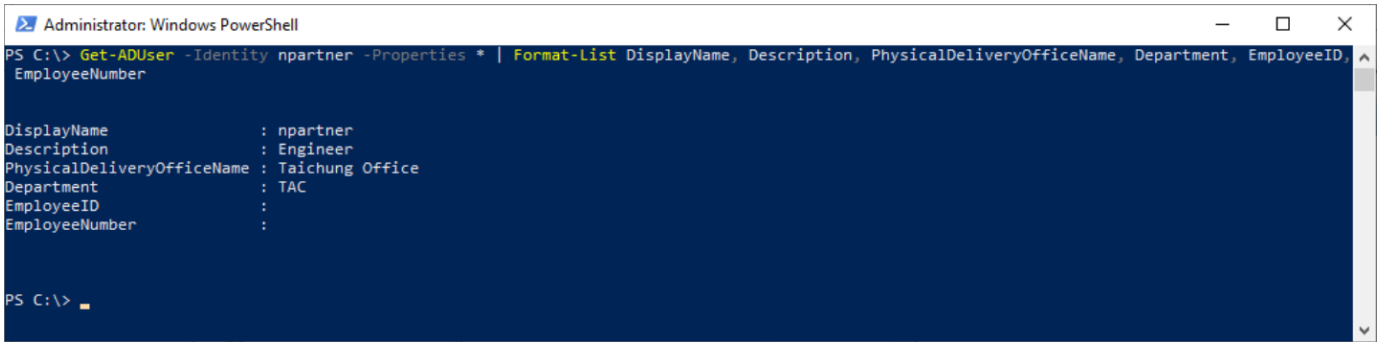


8.3 Configure WMI

Configuring WMI associates Windows account information with the “Username” field in “Event Query” of N-Reporter.

(1) Enter the command below to check whether N-Reporter associates Windows AD with available user data.

```
PS C:\> Get-ADUser -Identity KH -Properties * | Format-List DisplayName, Description,
PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
```



Replace the red text with the username according to the actual environment.

(2) In “Event Query,” click the information of “Username.”

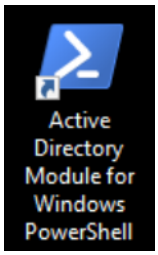
Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner	4724	Administrator	User Managem

(3) The system will show the full information of username.

Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator	npartner (npartner, TAC, npartner, [32])	4724	Administrator	User Managem

8.3.1 Add Non-Admin Accounts

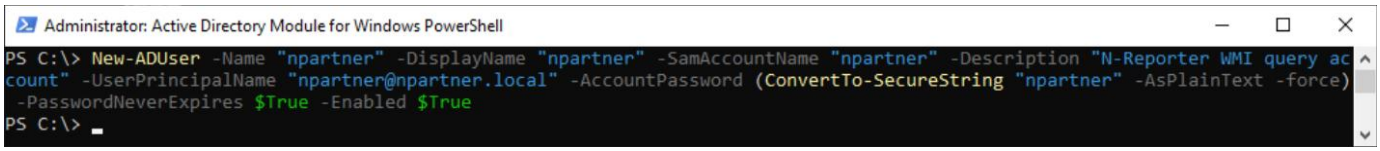
(1) Open “Active Directory Module for Windows PowerShell.”



(2) Create an Account

Enter the command below to create an account:

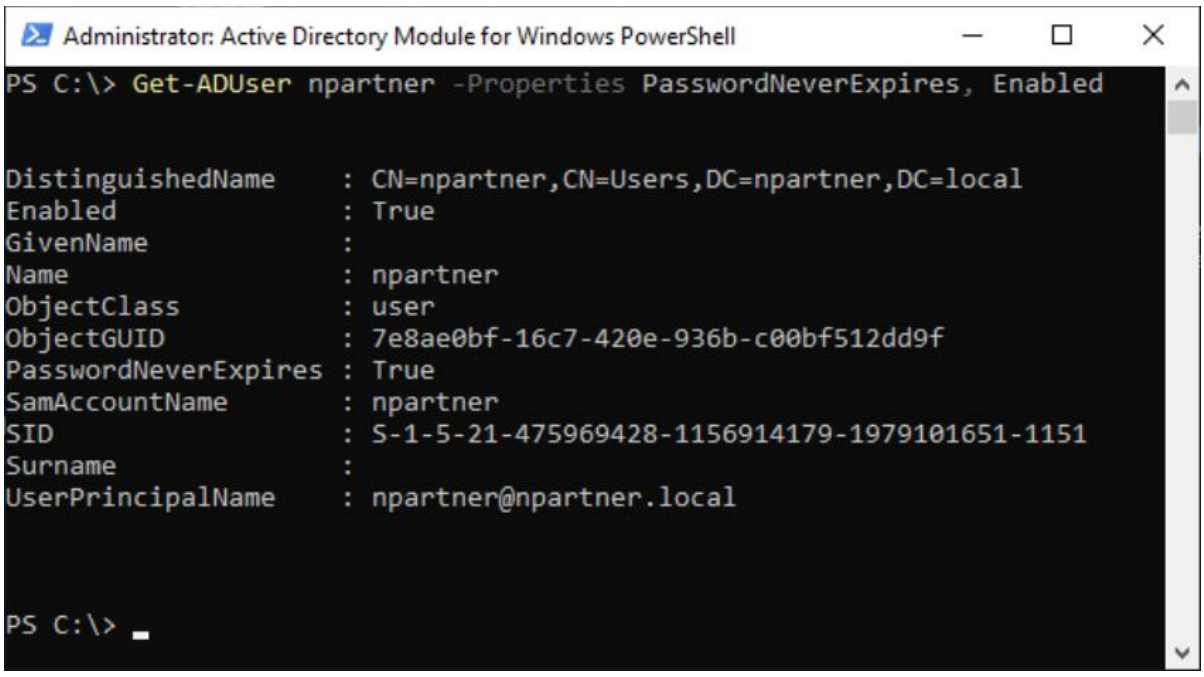
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



Note: Replace the red text with the appropriate account, password, and domain information.

(3) Enter the command below to check account status:

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

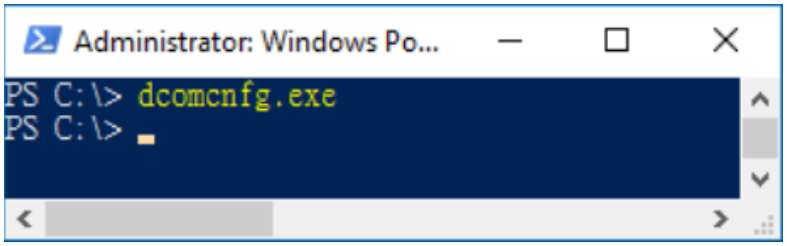


8.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”

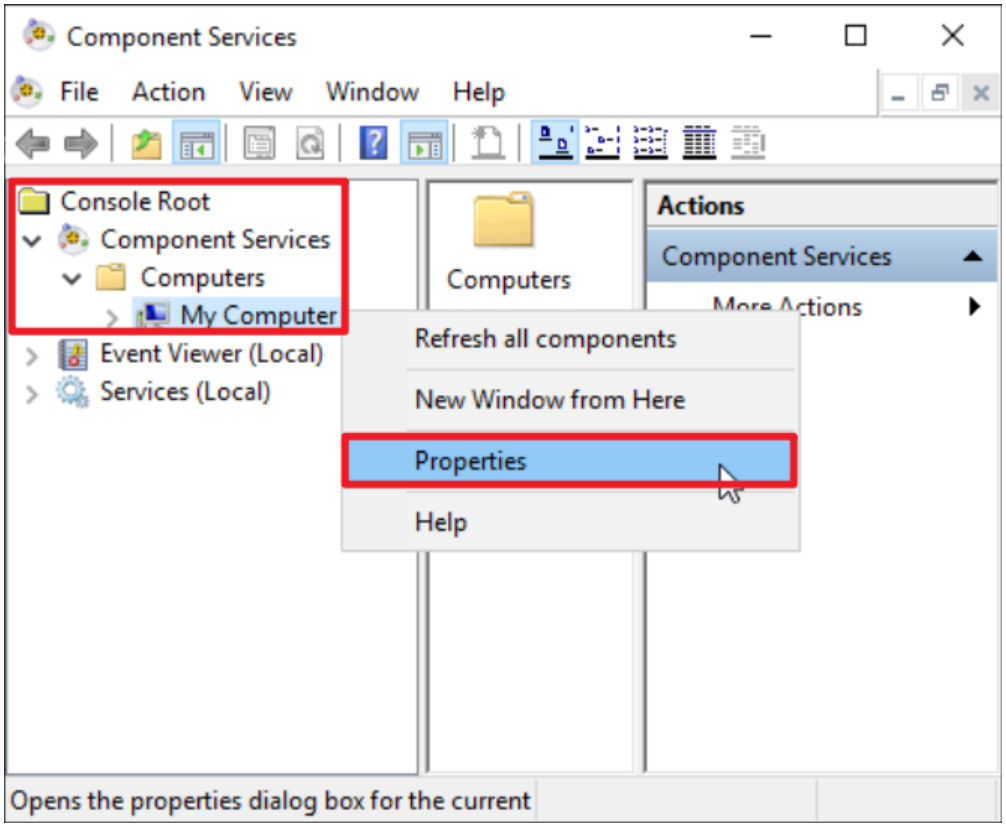
(2) Enter the command below to enable component services.

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



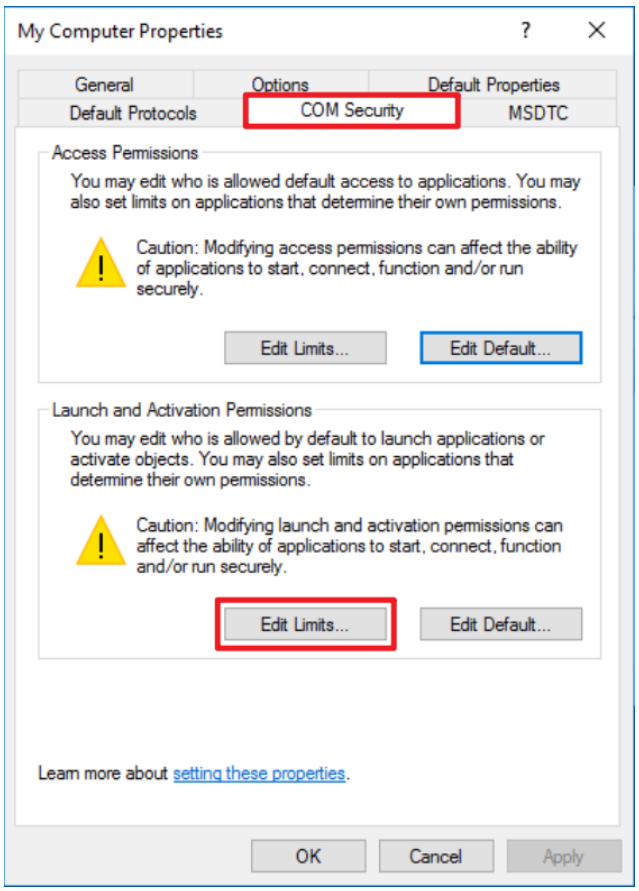
(3) Edit Computer Properties

Expand “Console Root” → “Component Services” → “Computers” → right-click “My Computer” → select “Properties.”



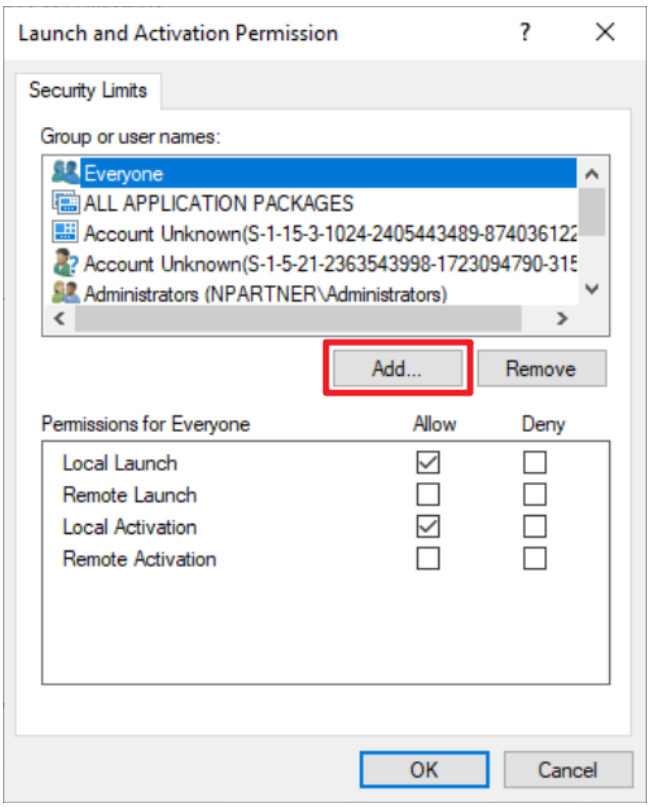
(4) Enable Permissions

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



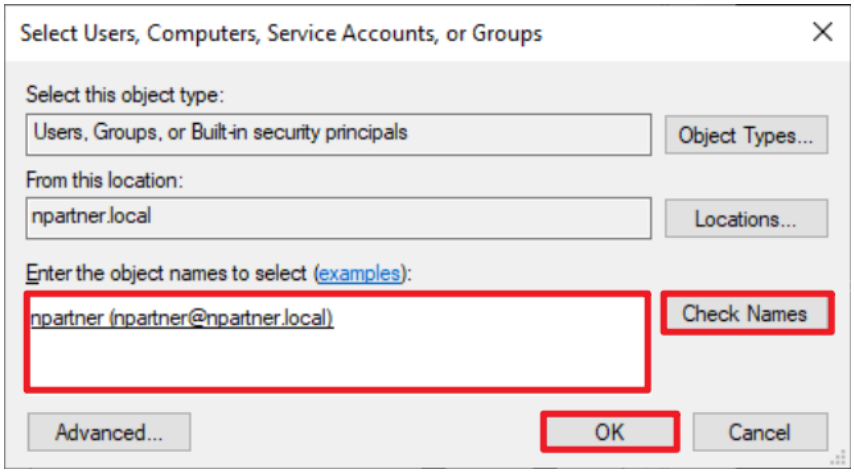
(5) Add DCOM User Permissions

Click “Add.”



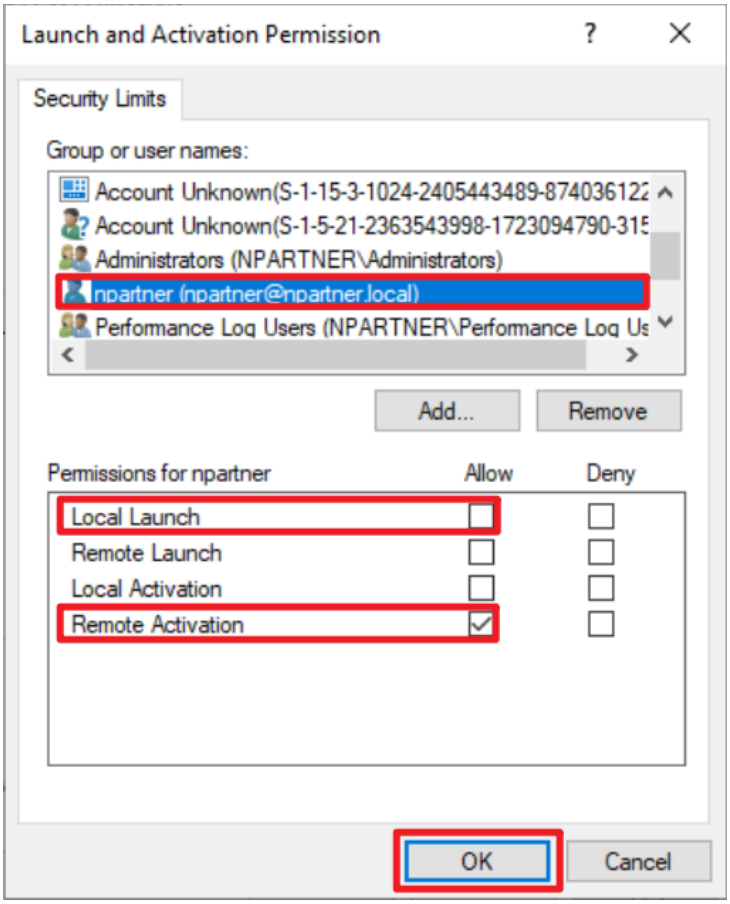
(6) Enter Your Username

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

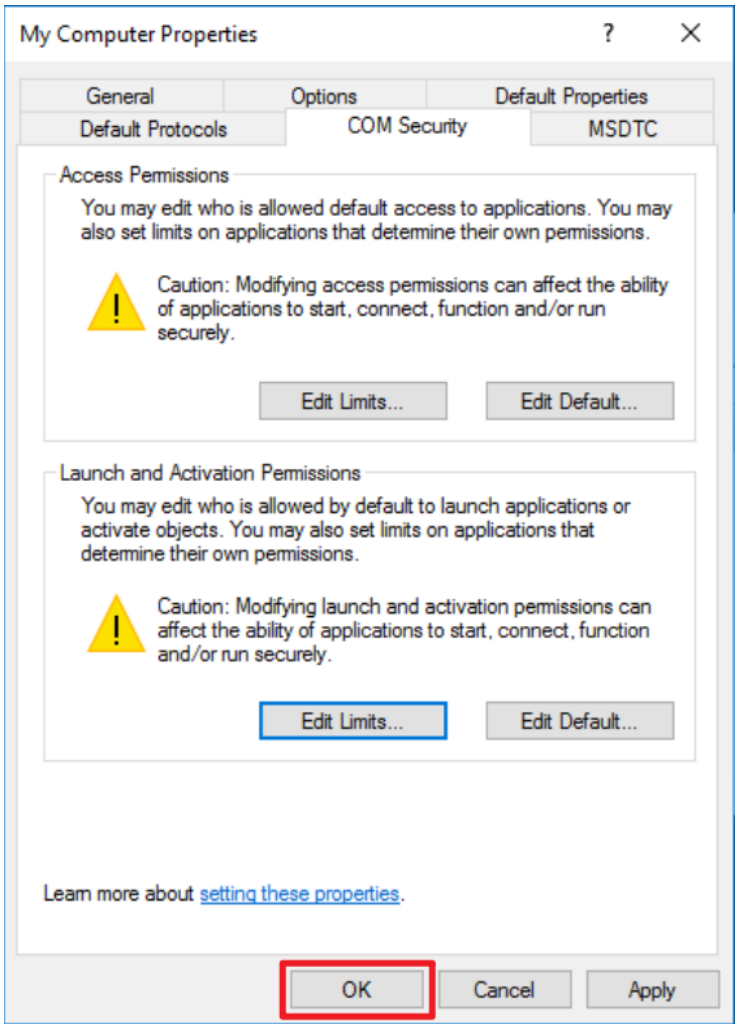


(7) Configure your User Permission

Click your user account (in this example, it is “npartner”) → uncheck “Local Launch: Allow” → check “Remote Activation: Allow” → click “OK.”



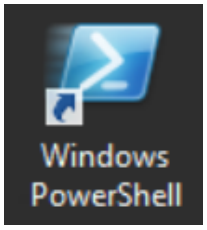
(8) Click "OK."



8.3.3 Configure WMI Permissions

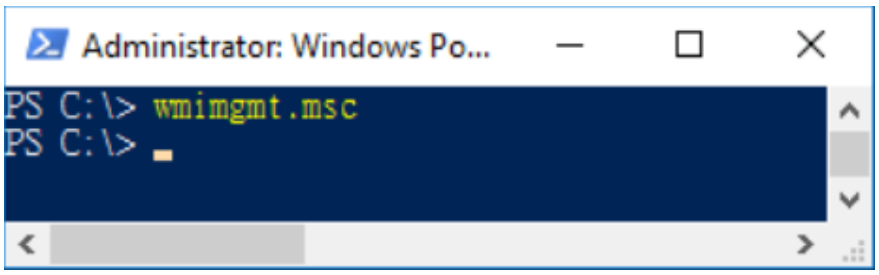
8.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



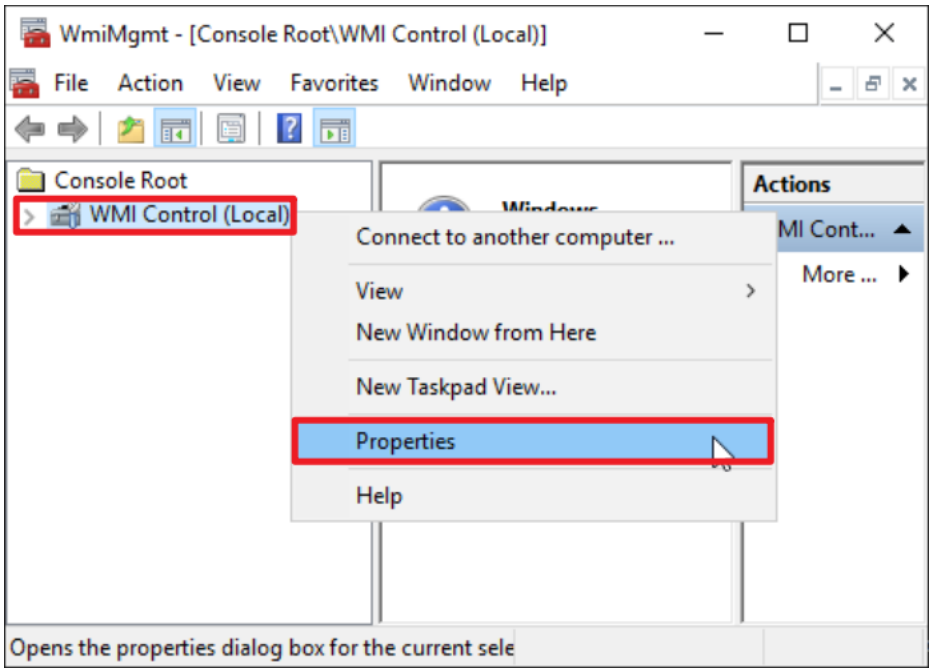
(2) Enter the command to enable WMI control service.

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



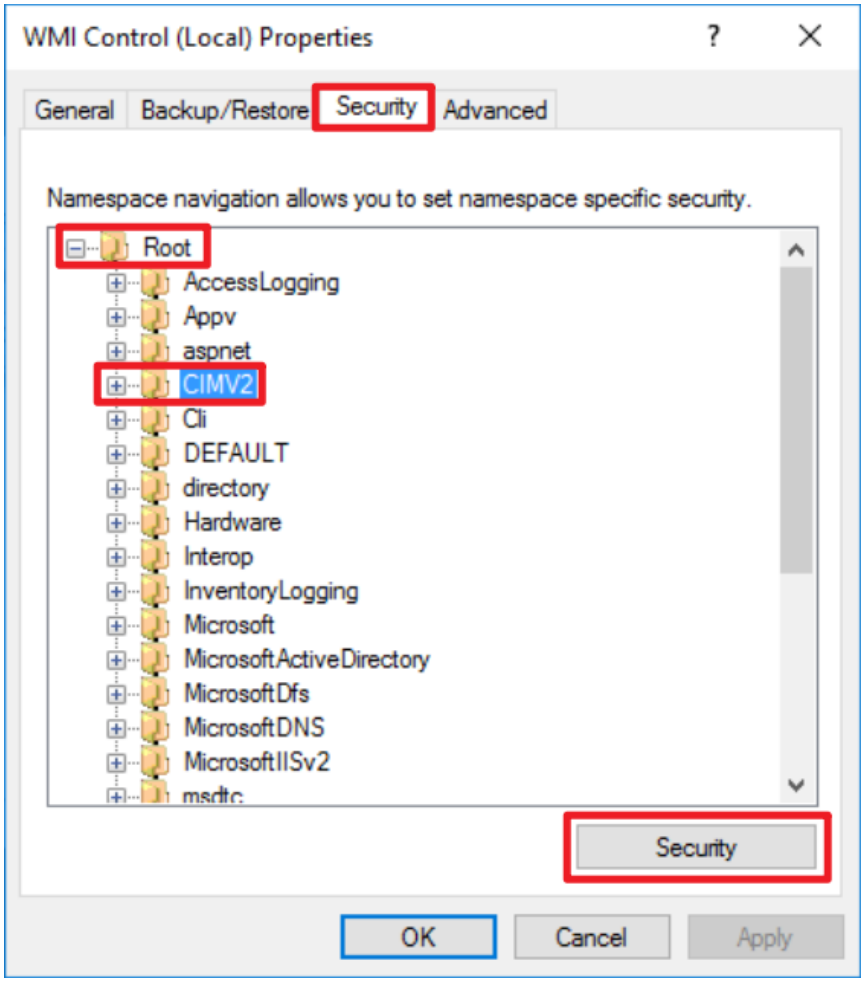
(3) Edit WMI Control

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



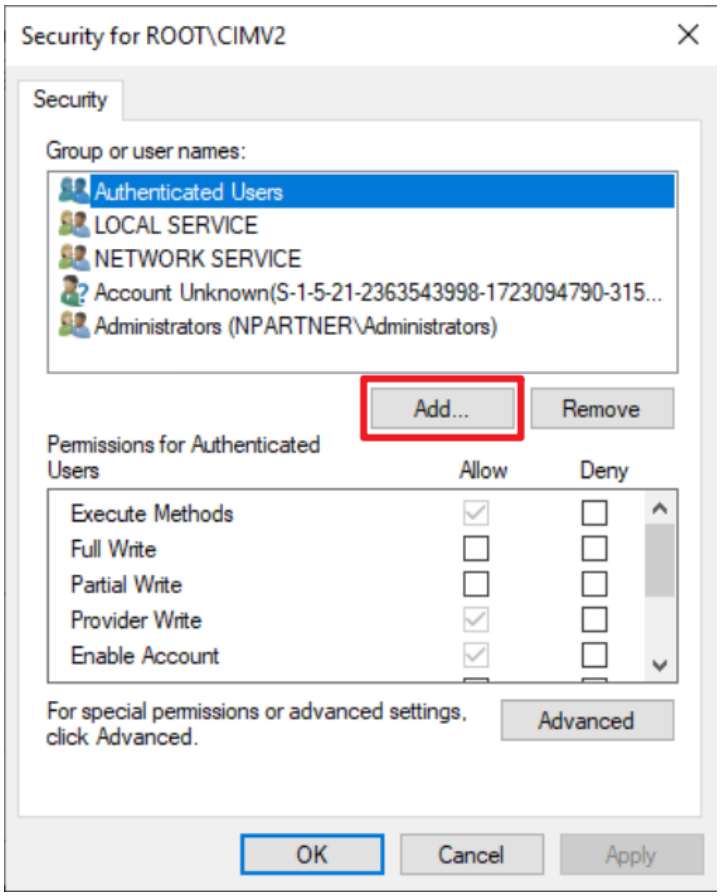
(4) Edit CIMV2 Security

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



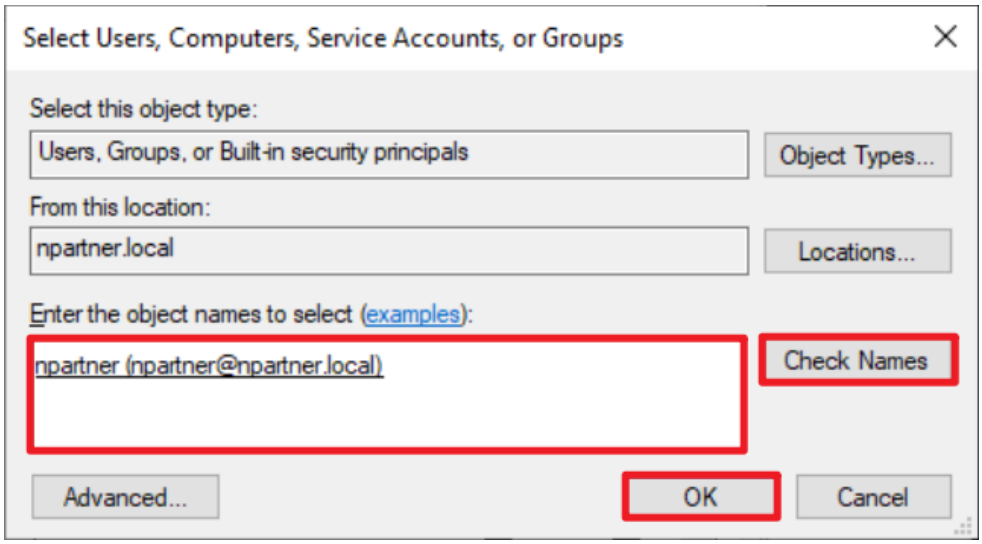
(5) Add WMI User Permissions.

Click “Add.”



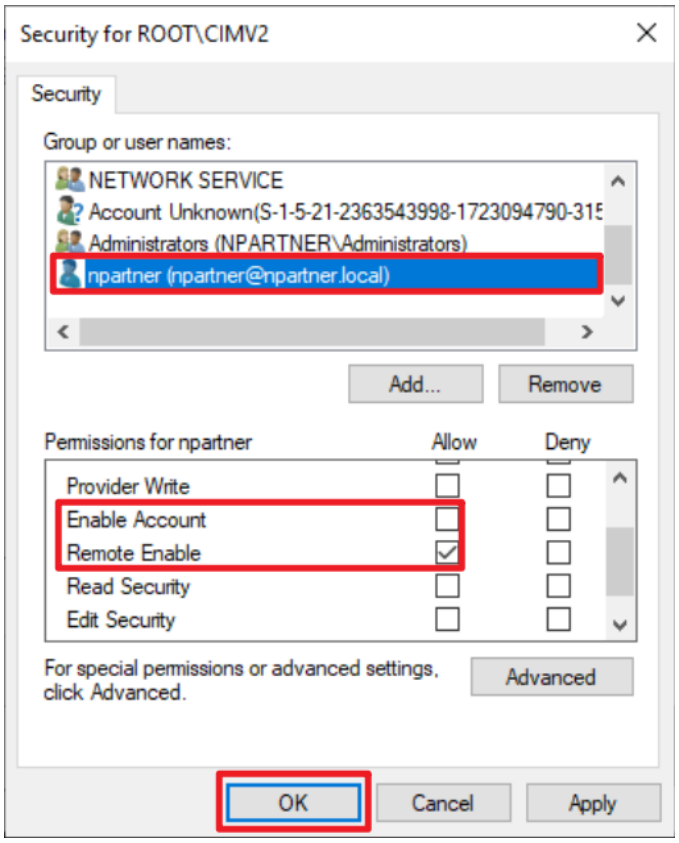
(6) Enter Your Username

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

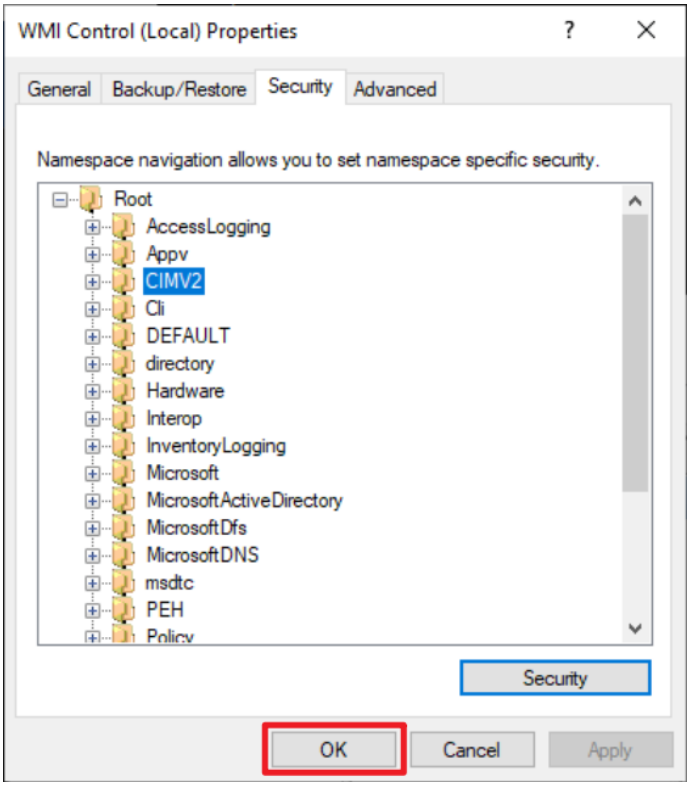


(7) Set Your User Permissions

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

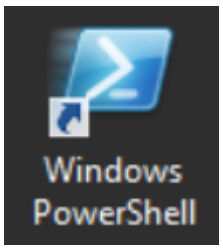


(8) Click “OK.”



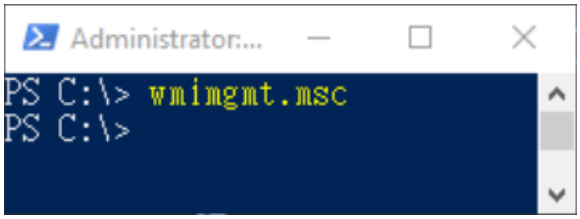
8.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



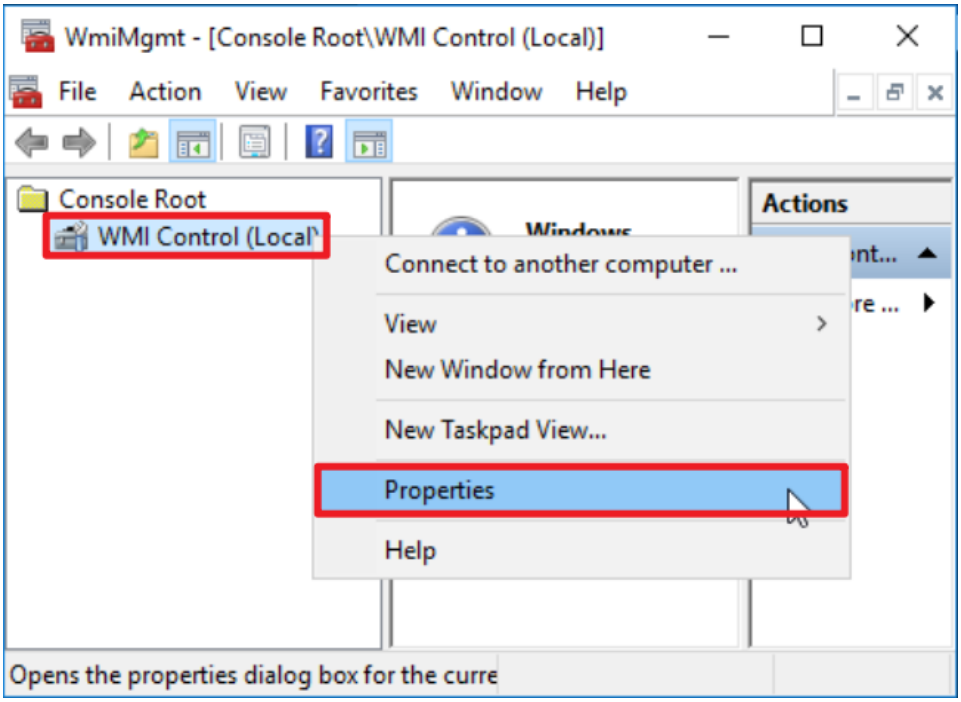
(2) Enter the command below to enable WMI Control.

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



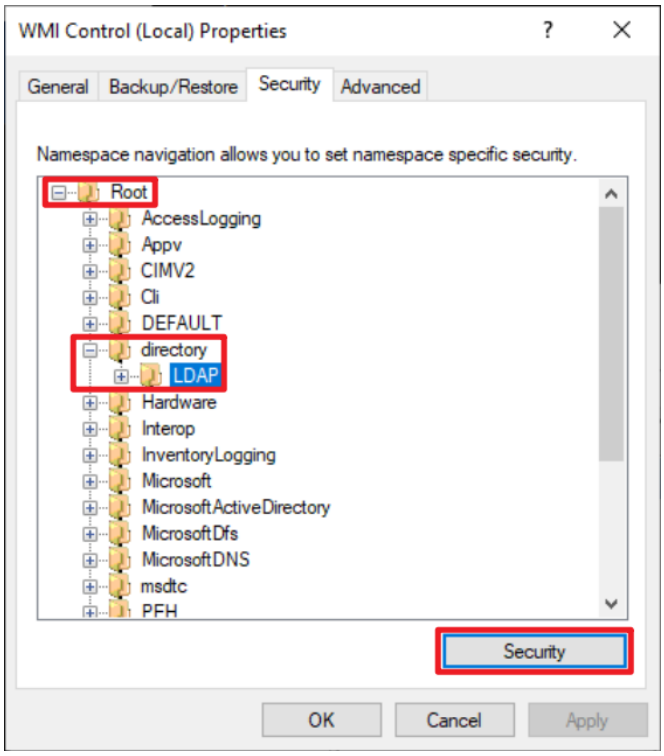
(3) Edit WMI Control

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



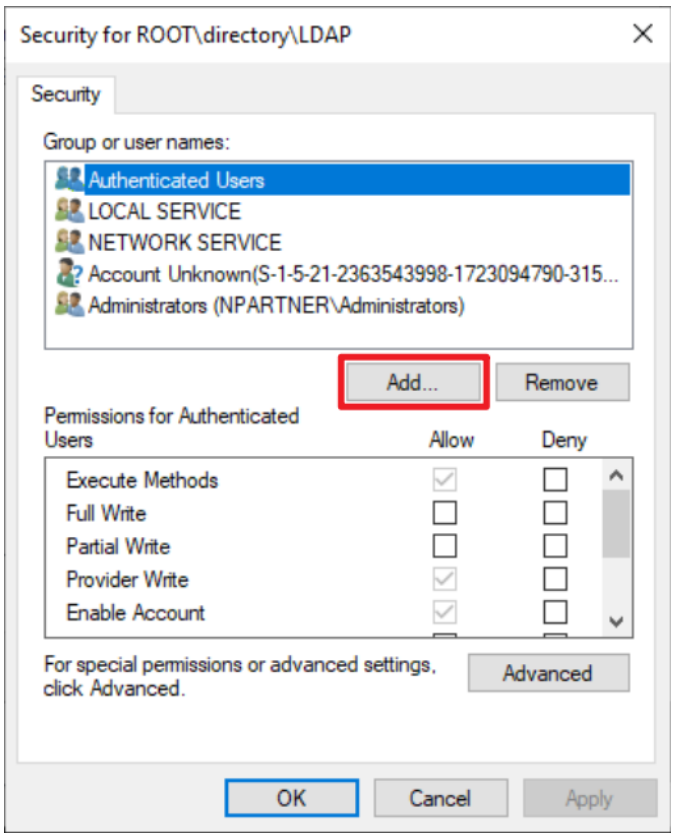
(4) Edit LDAP Security

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



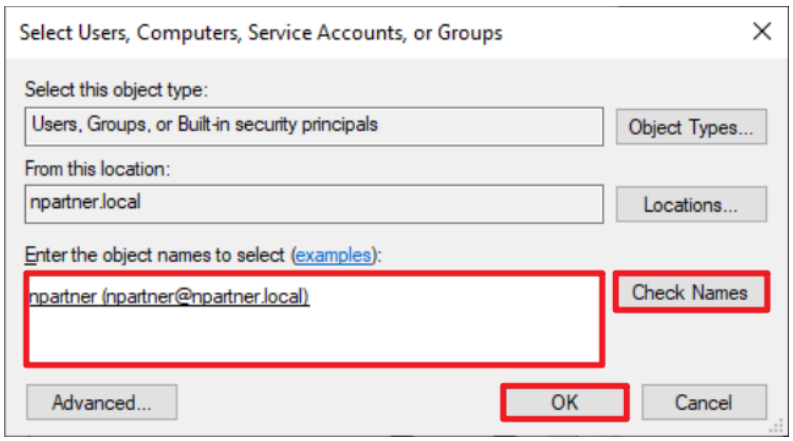
(5) Add WMI User Permissions

Click “Add.”



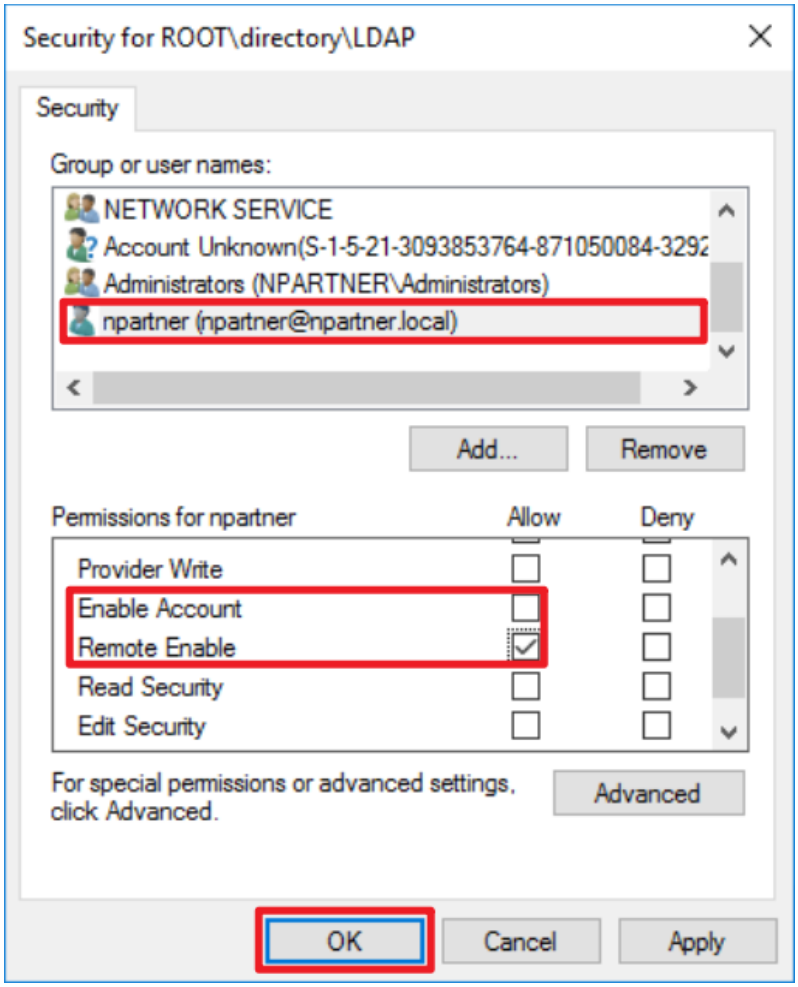
(6) Enter Your Username

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

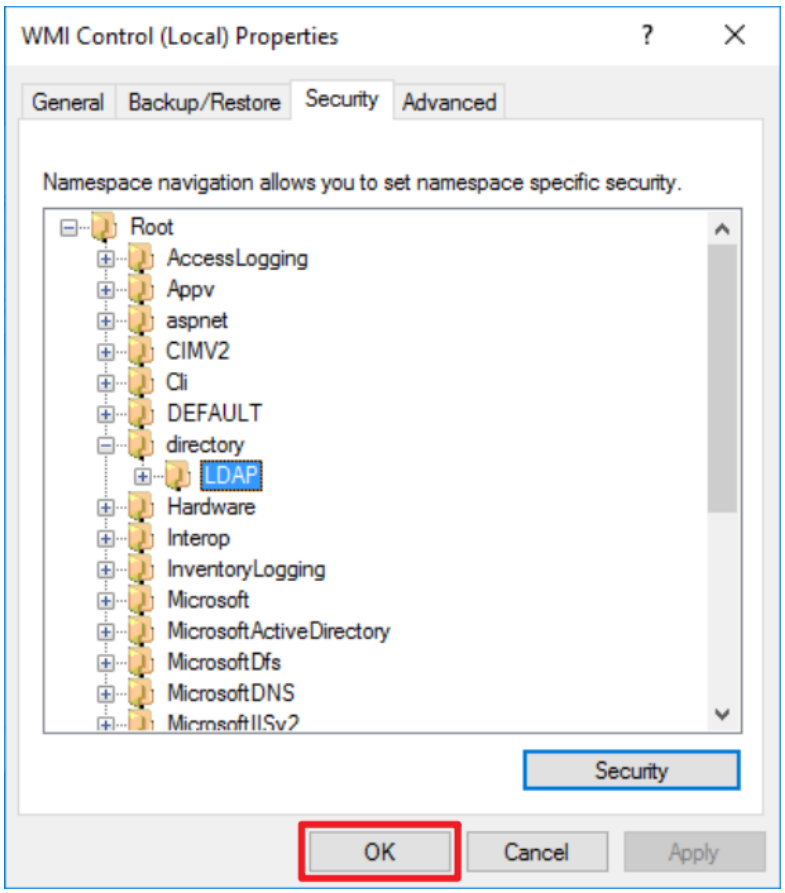


(7) Set Your User Permissions

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

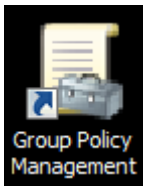


(8) Click “OK.”

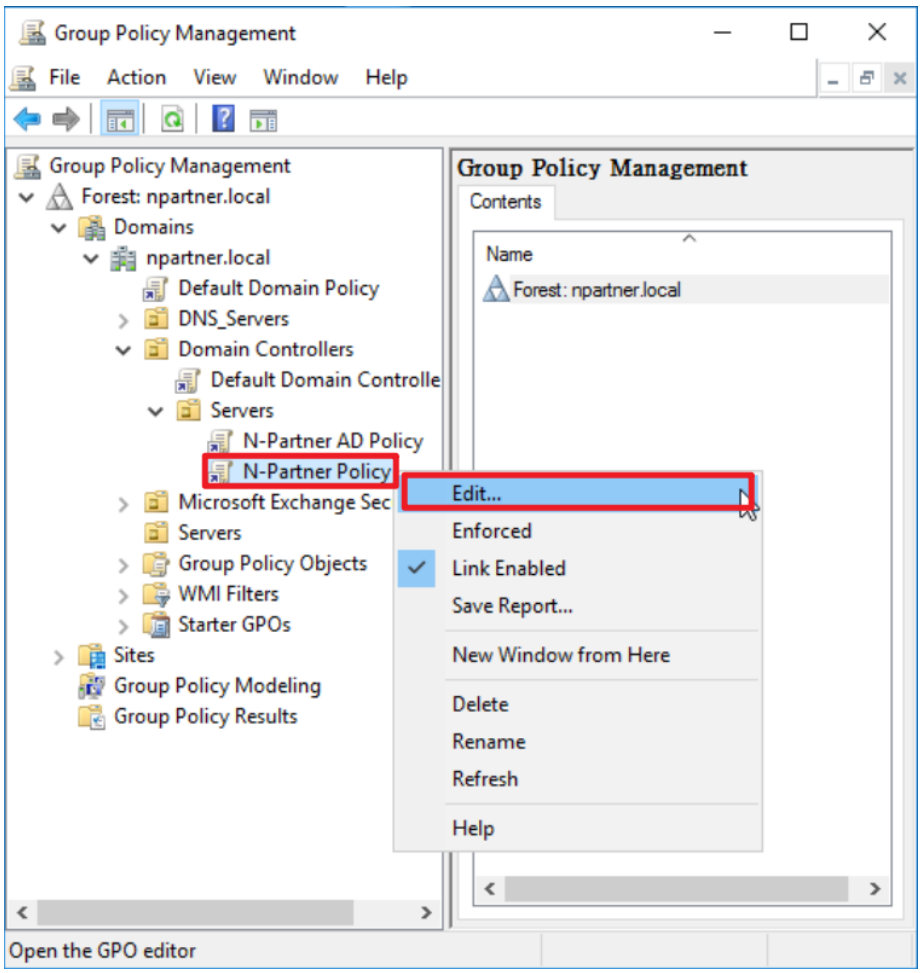


8.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

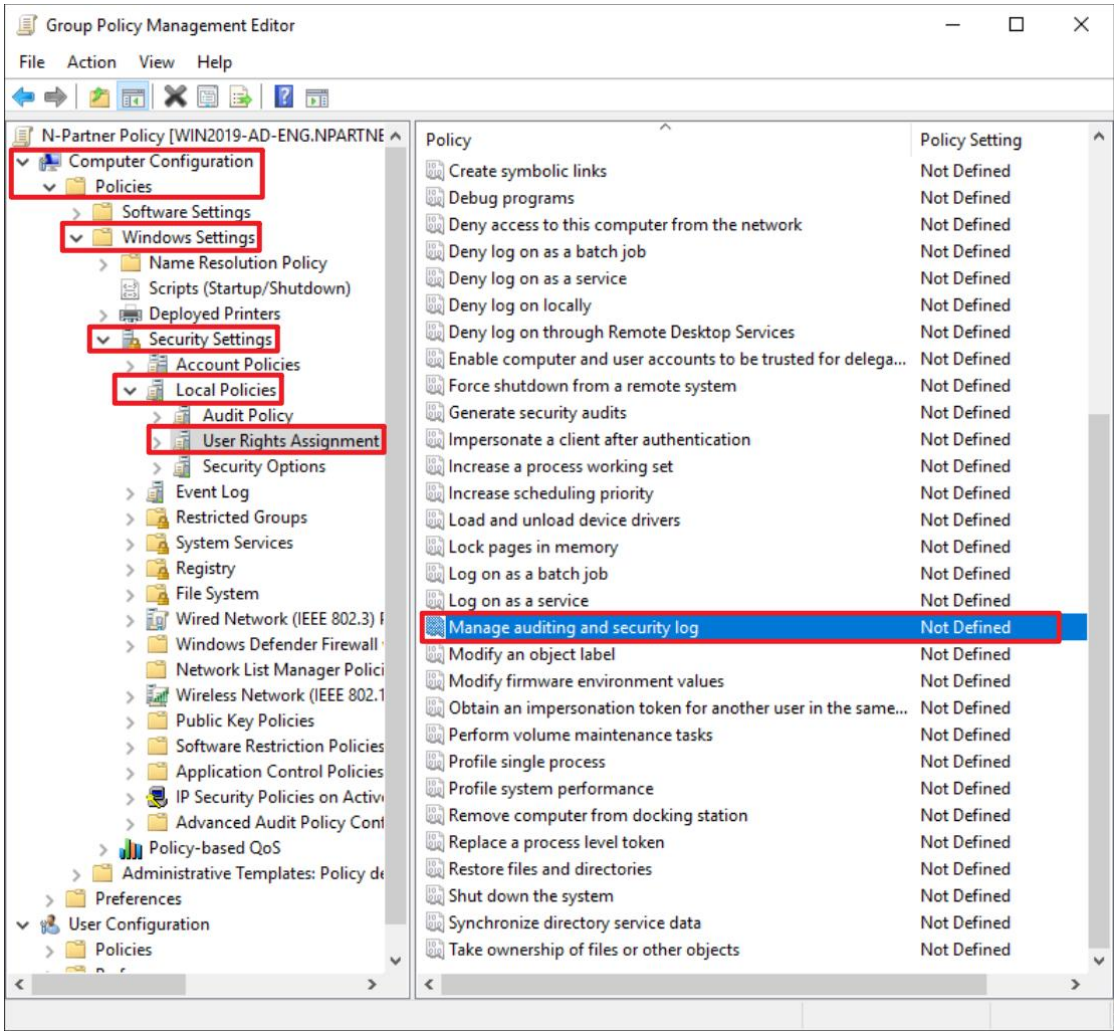


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



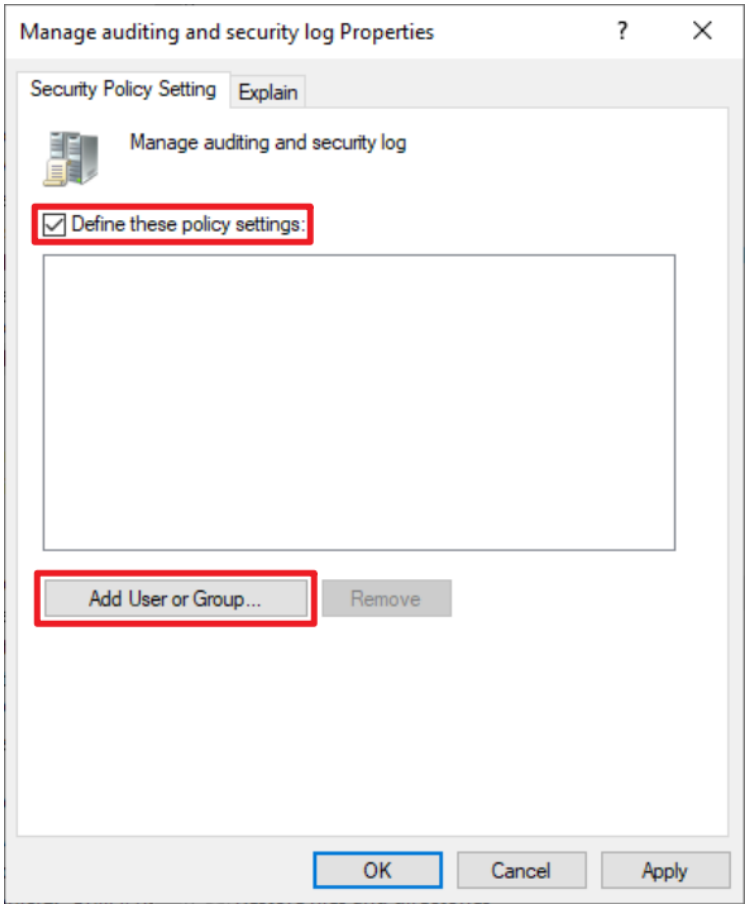
(3) Configure Auditing Log

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



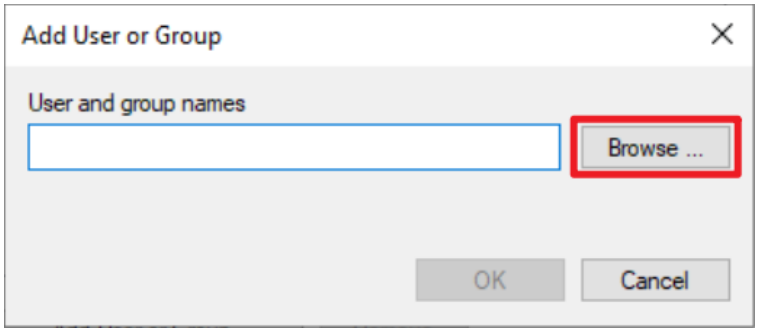
(4) Add Auditing User

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



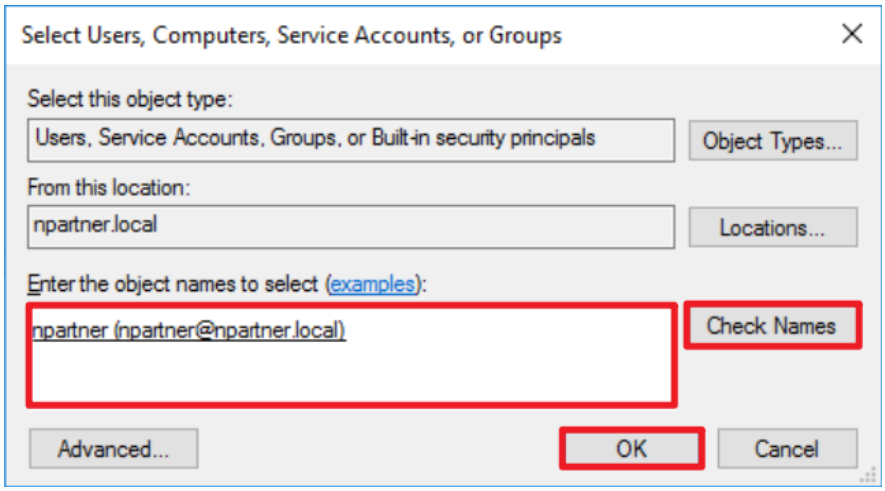
(5) Search for User

Click “Browse.”

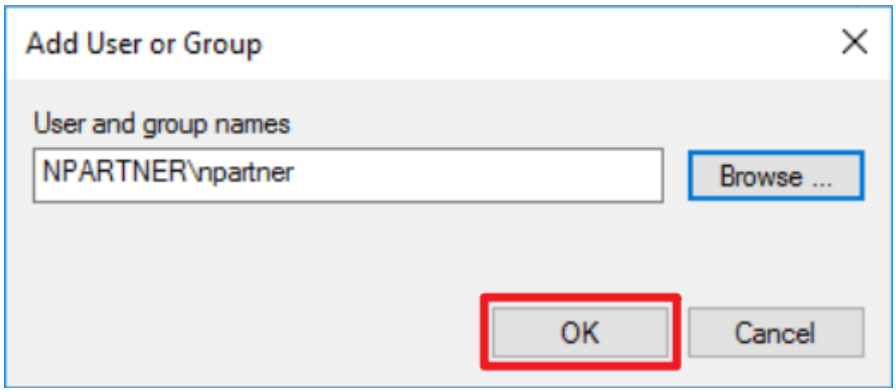


(6) Enter Your User Account

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

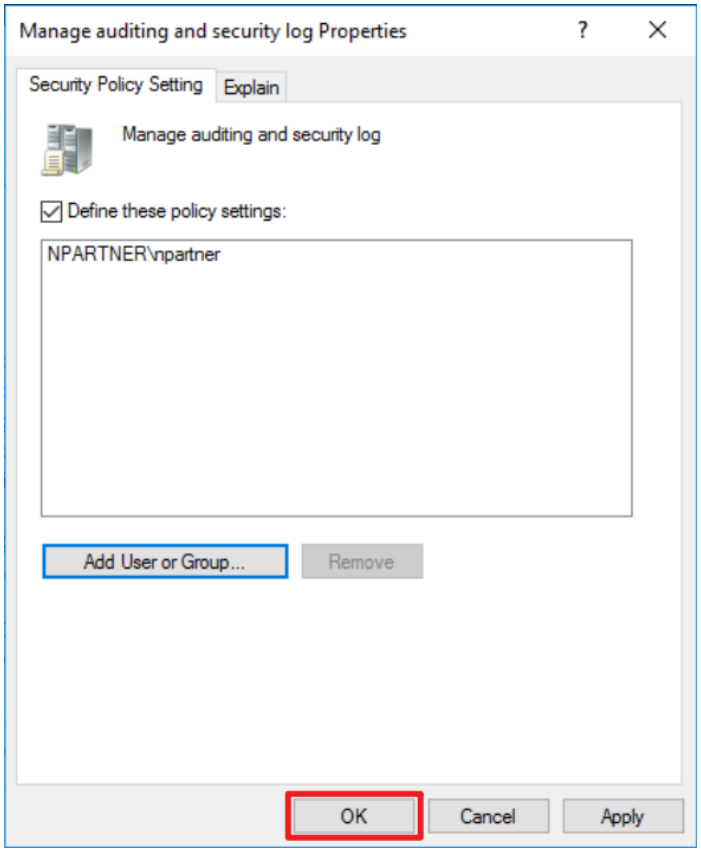


(7) Click “OK.”



(8) Confirm Audit Log Settings

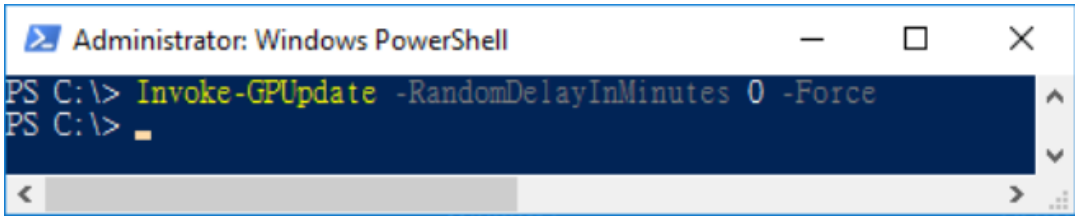
Click “OK.”



(9) Open “Windows Powershell.”

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

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

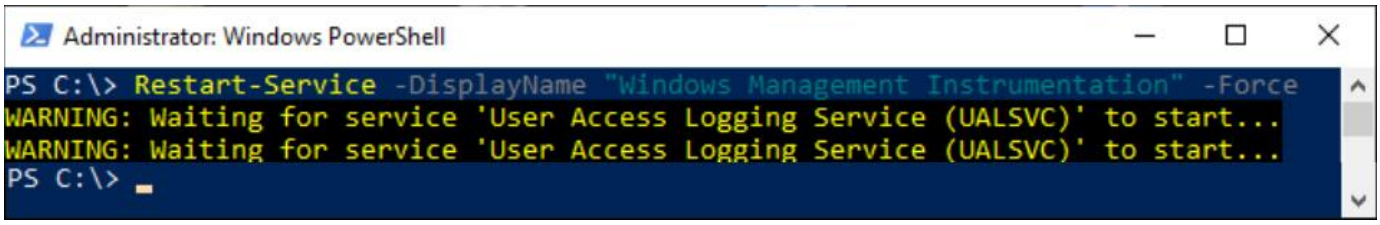


8.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”

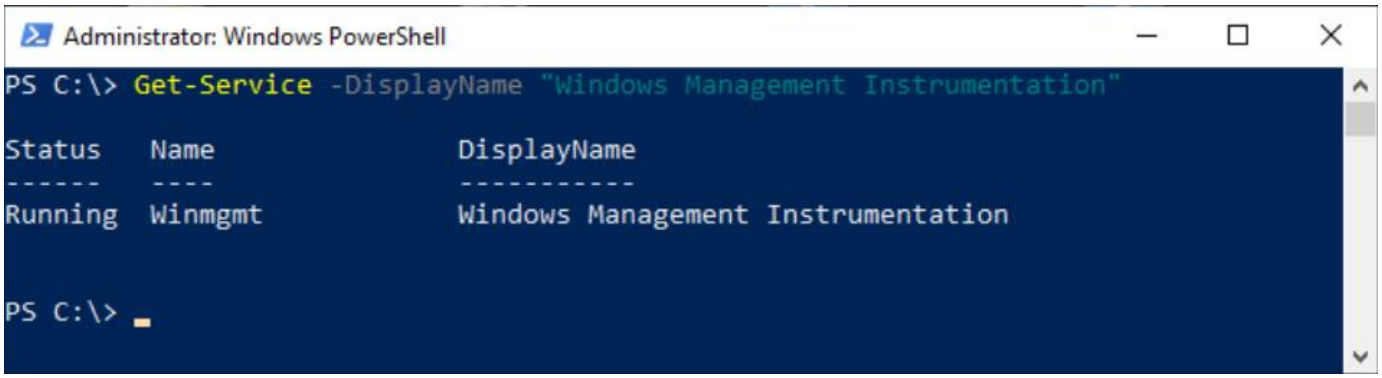
(2) Enter the command below to disable the WMI service.

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



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

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

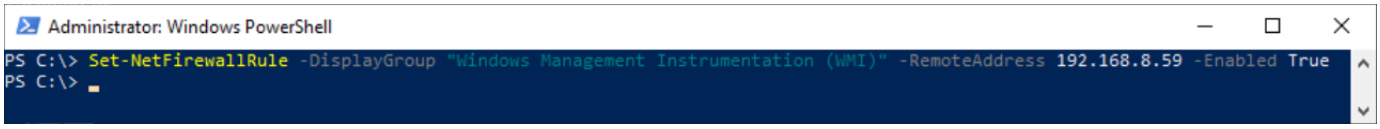


8.3.6 Configure the Firewall

(1) Open “Windows Powershell.”

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

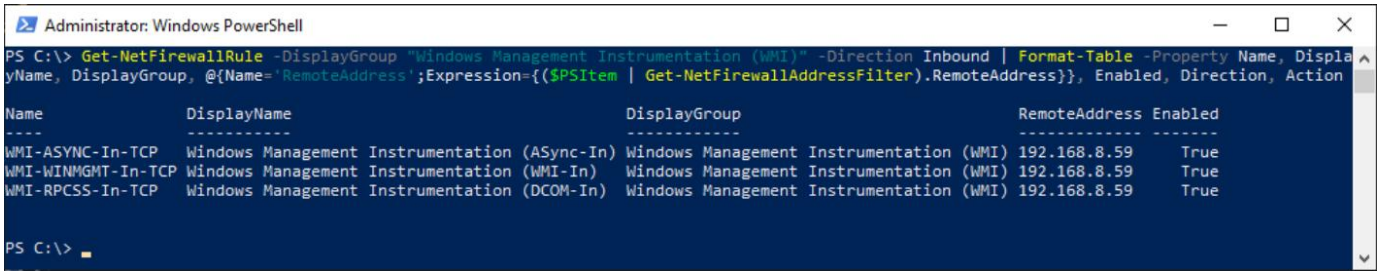
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True
```



Replace the red text with the N-Reporter IP address.

(3) Enter the command below to show the current firewall WMI configuration:

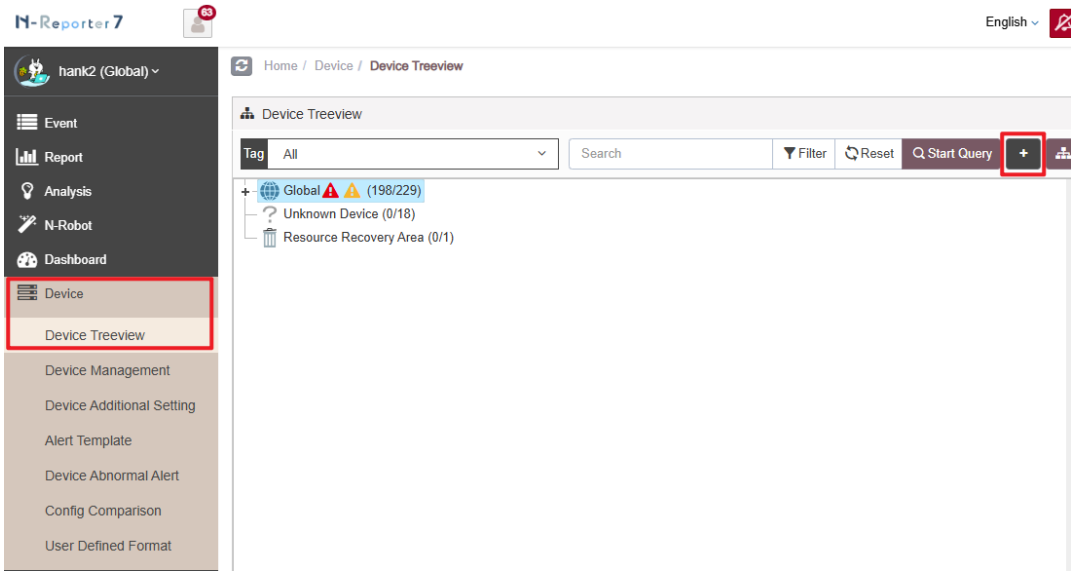
```
PS C:\> Get-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -Direction Inbound | >> Format-Table -Property Name,DisplayName,DisplayGroup, >> @{Name='RemoteAddress';Expression={($PSItem | Get-NetFirewallAddressFilter).RemoteAddress}}, >> Enabled,Direction,Action
```



9. N-Reporter

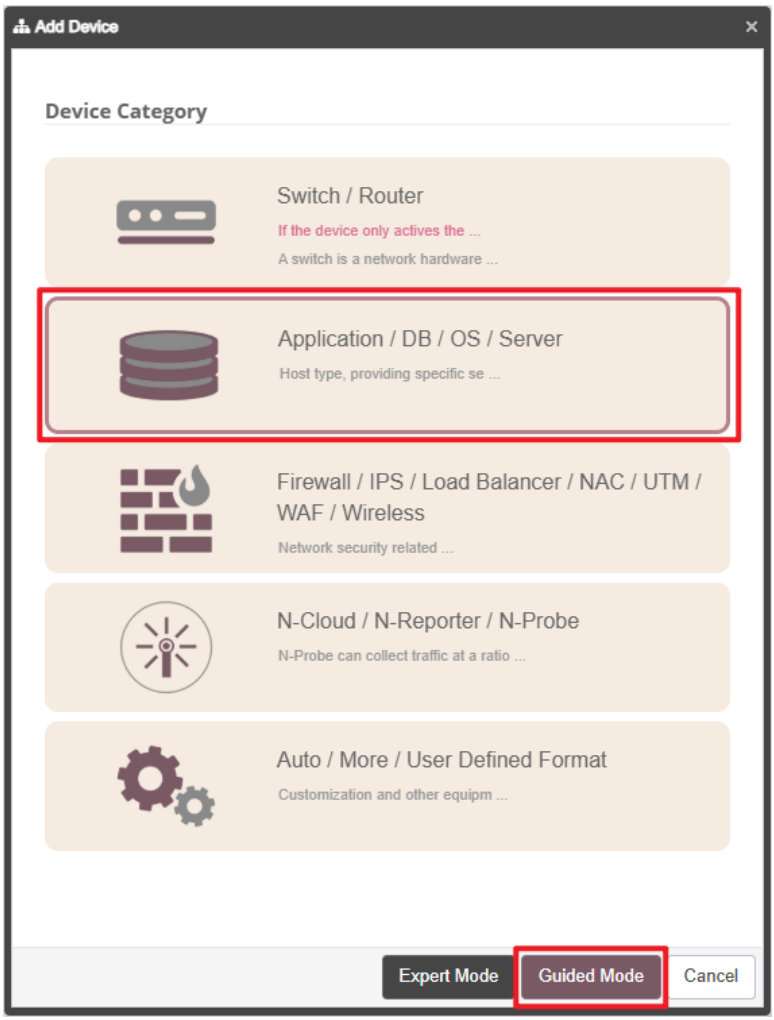
(1) Add a Windows AD device:

Go to “Device Management” → “Device Treeview” → click “Add.”



(2) Select the device type:

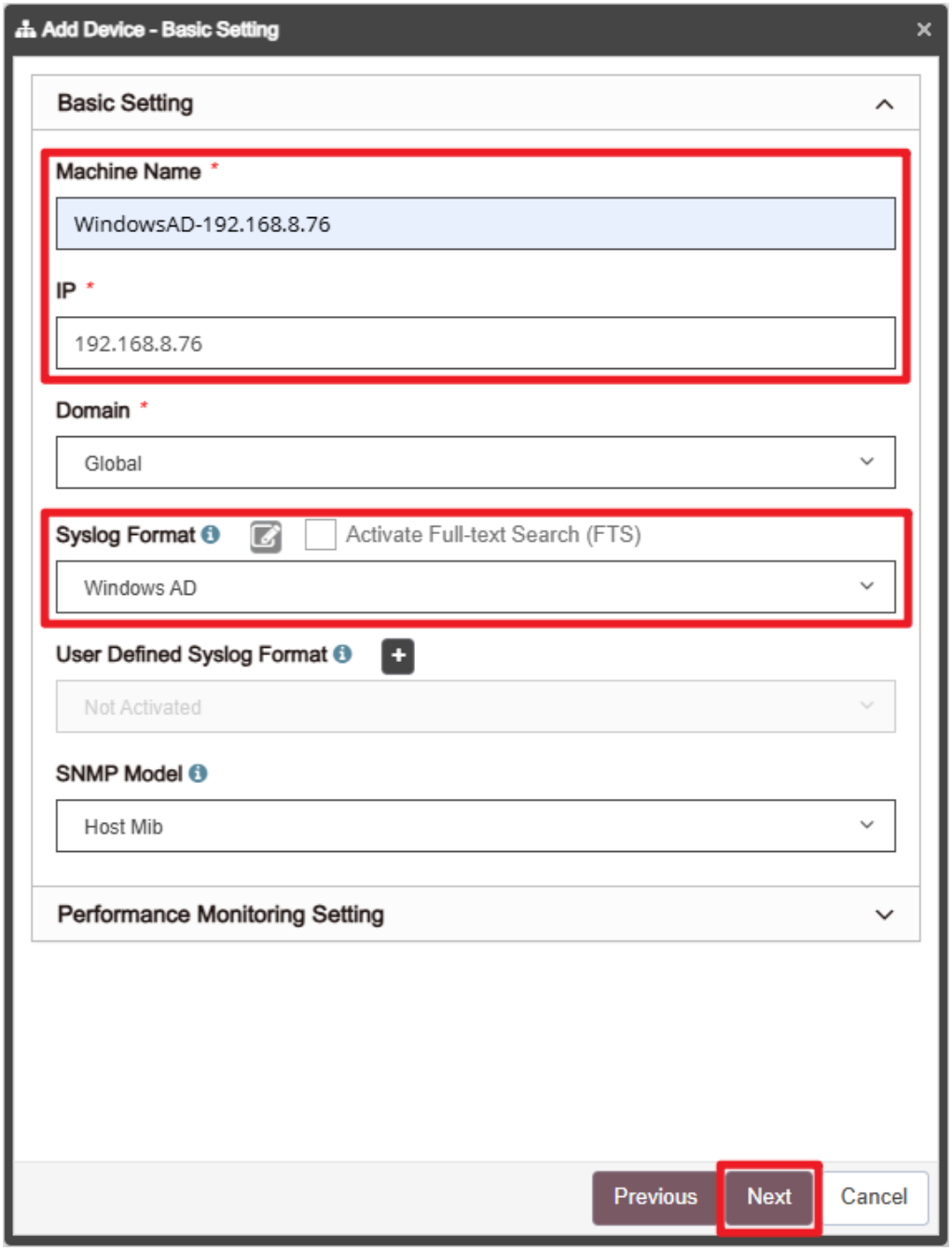
Choose “Application/DB/OS/Server” → click “Guided Mode.”



9.1 For Windows Server 2003 or earlier

(1) Basic Device Settings:

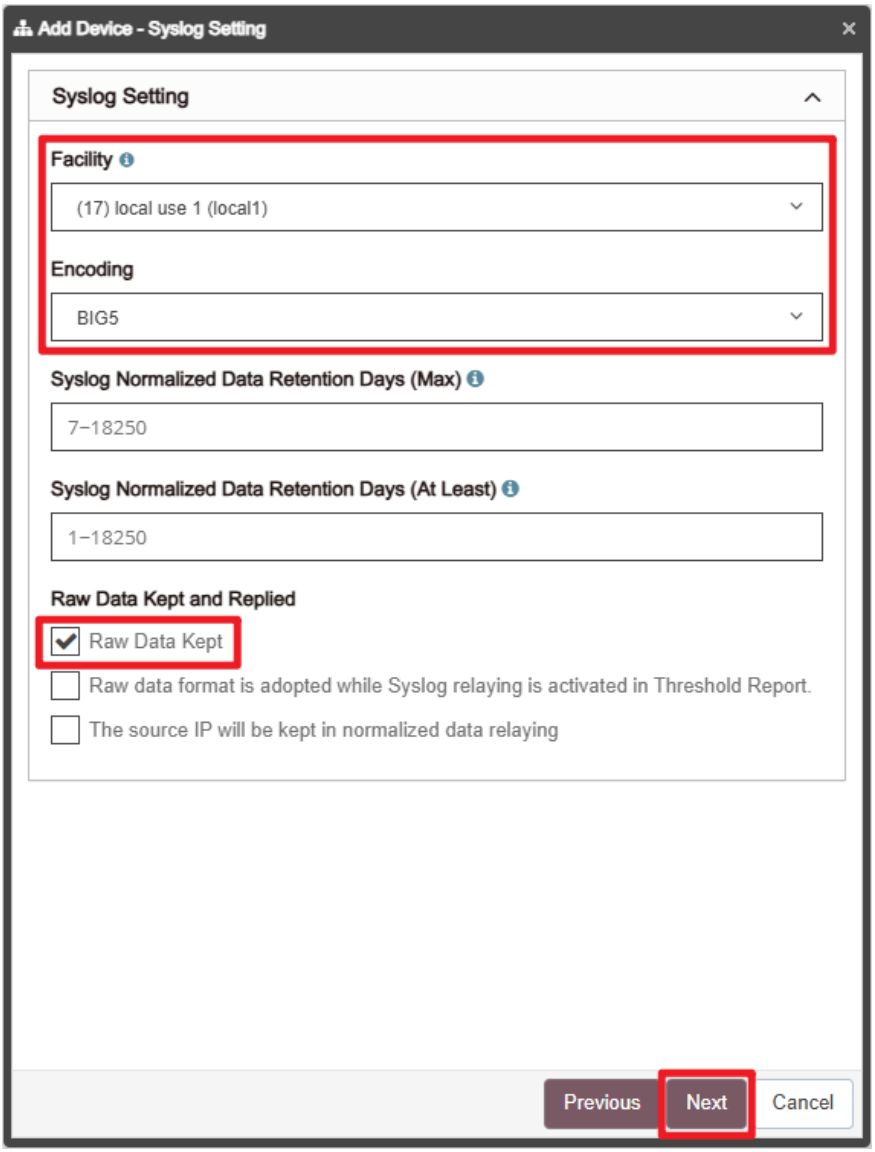
Enter the device name and IP address → For Syslog Data Format, select “Windows AD” → click “Next.”



(2) Syslog Settings

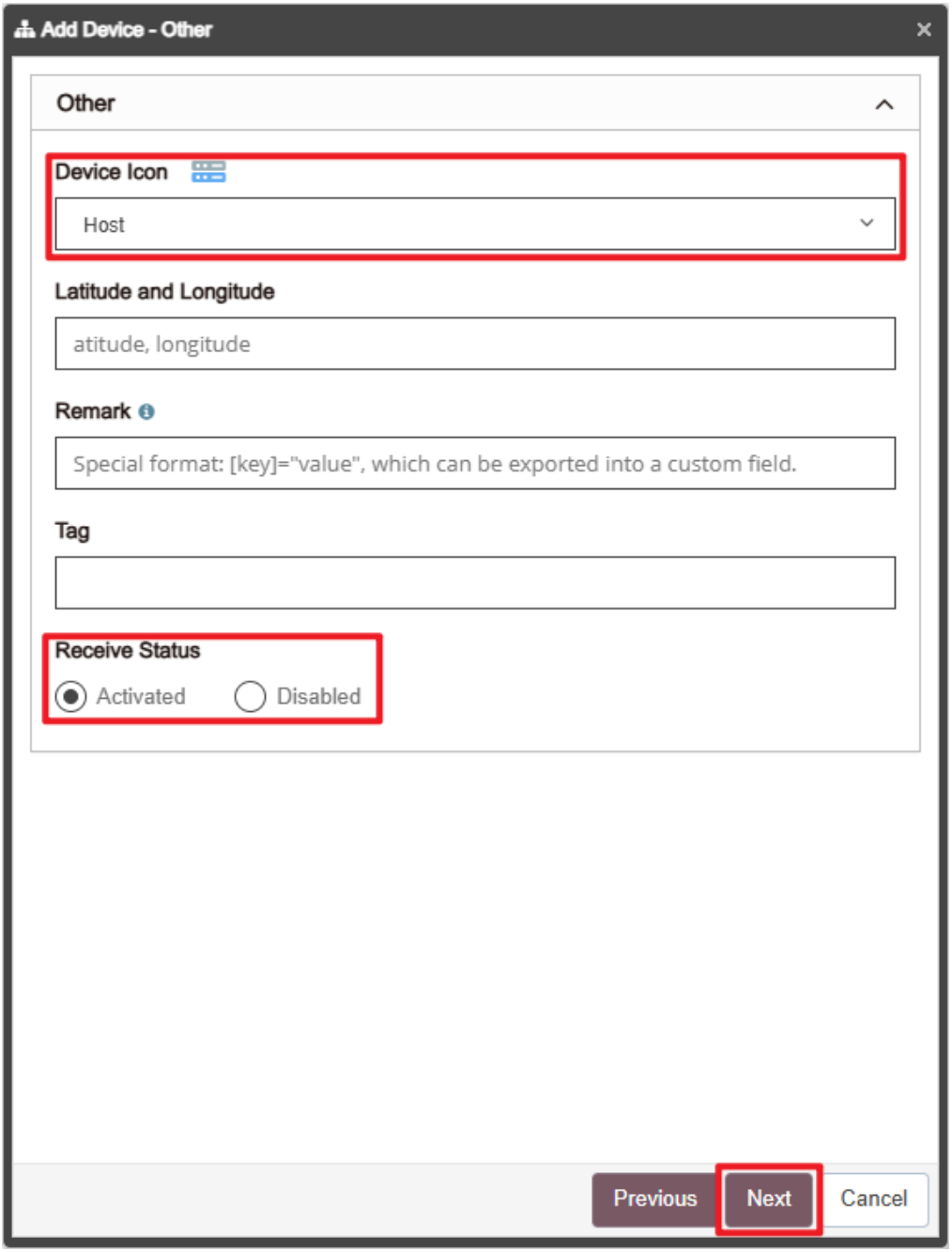
Set “Facility” to “(18) local use 2 (local2)” and “Encoding” to “BIG5” → click “Next.”

If “Raw Data Kept” function is enabled, the “Event Query” page will display raw data information.



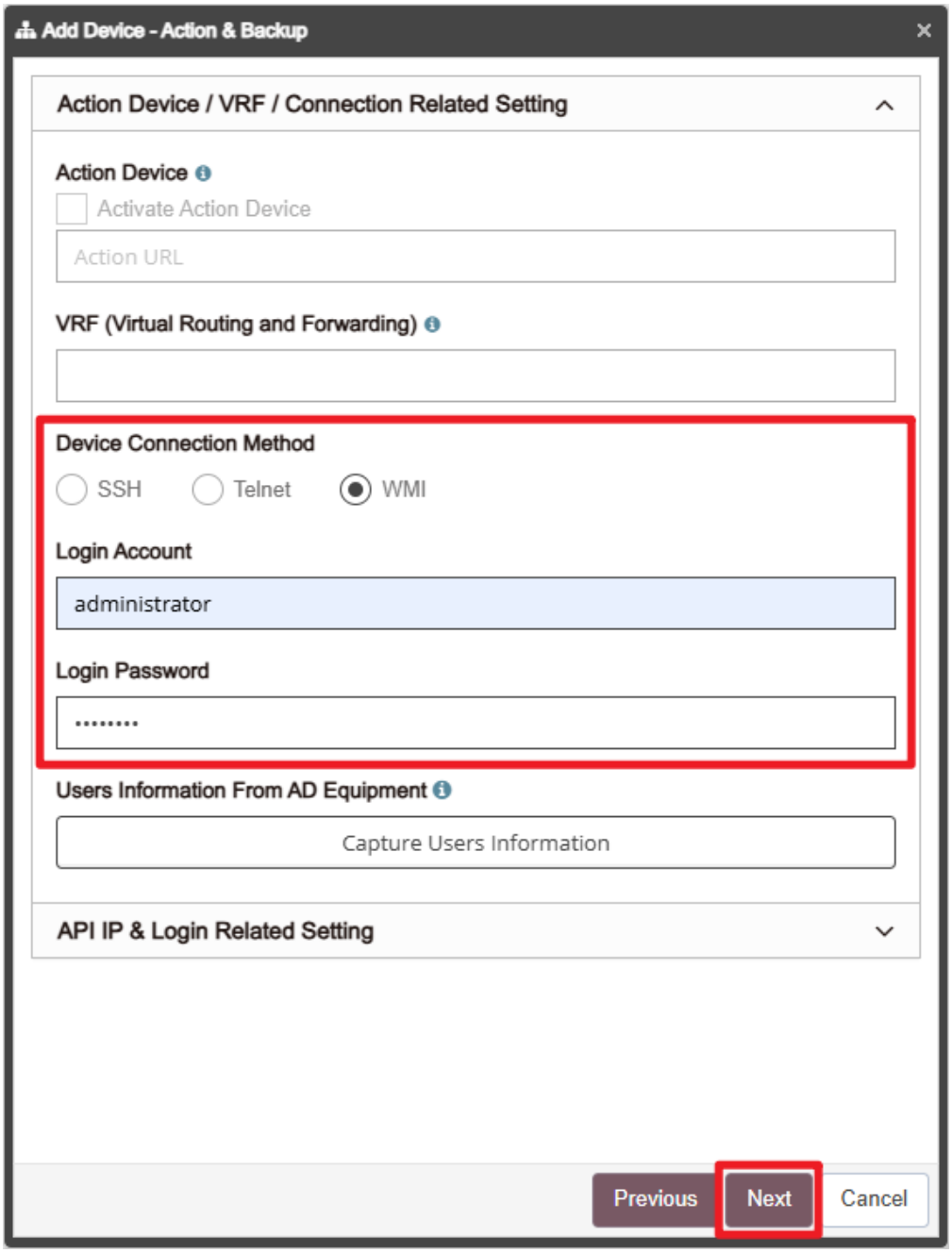
(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next” → Confirm.



(4) WMI Configuration

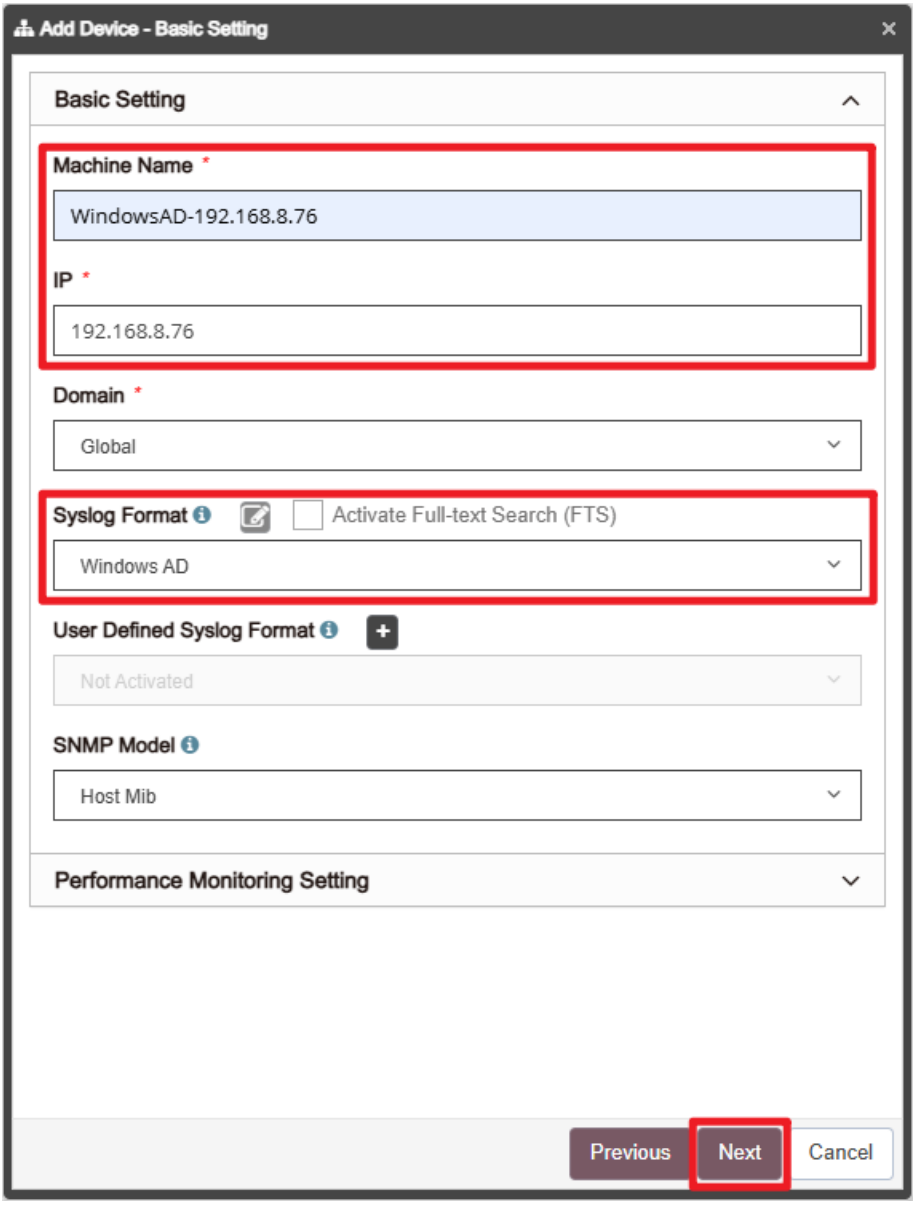
Enter the Windows AD WMI login account and password. If WMI is not configured, leave these fields blank.



9.2 For Windows 2008 or later

(1) Device Basic Settings

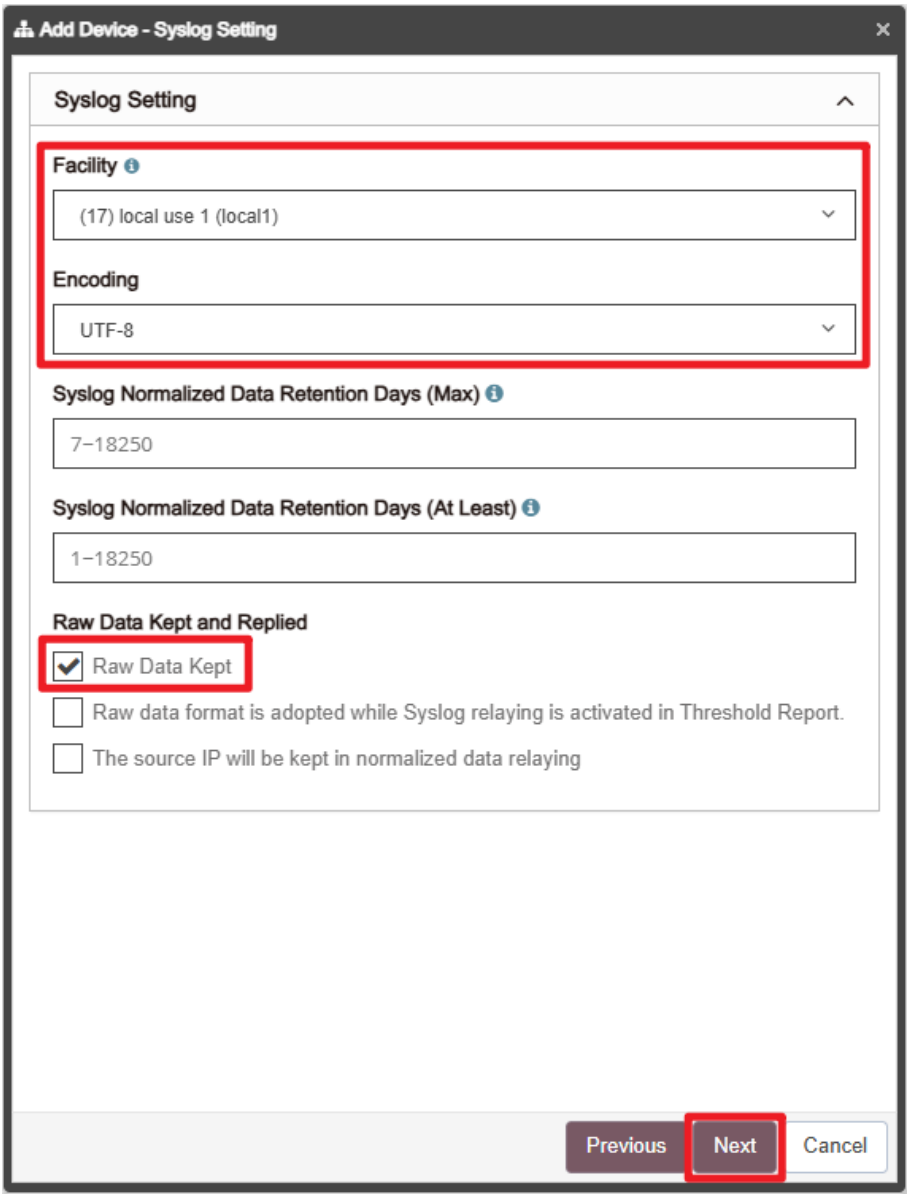
Enter the device name and IP → Select “Windows AD” for the Syslog data format → click “Next.”



(2) Syslog Settings

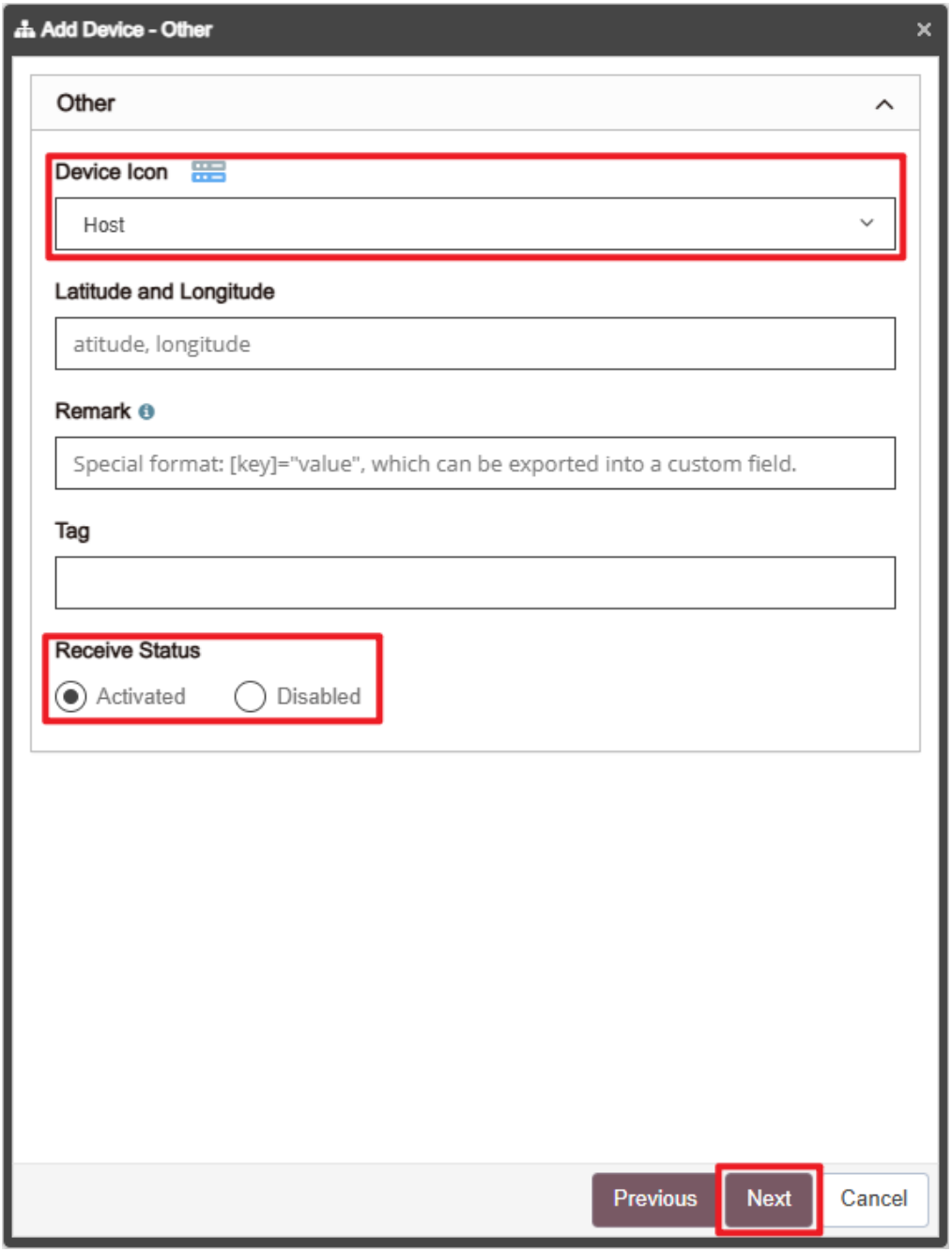
Set “Facility” to “(17) local use 1 (local1)” and “Encoding” to “UTF-8” → click “Next.”

If “Raw Data Kept” is checked, the “Event Query” page will display raw data information.



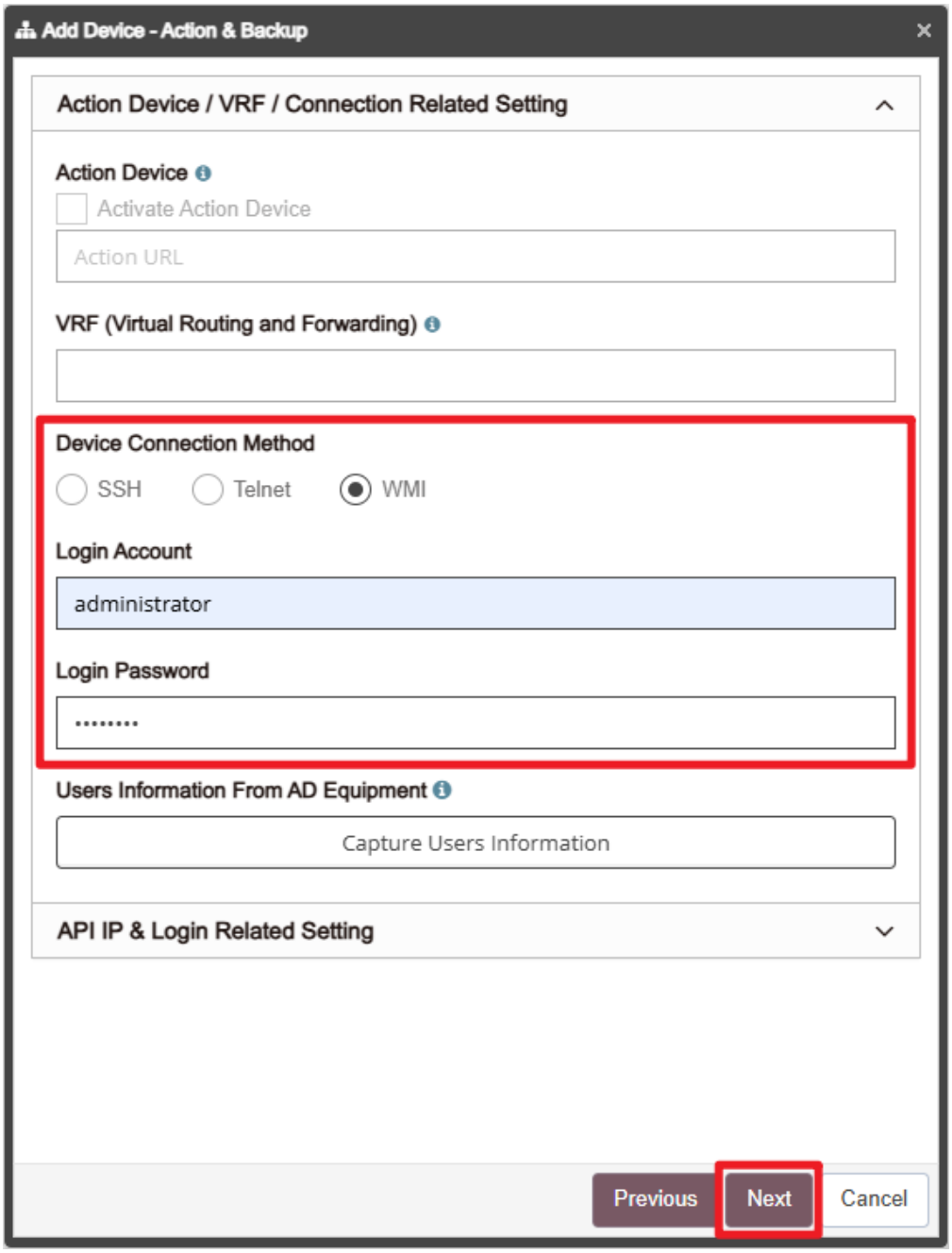
(3) Others

Set “Device Icon” to “Host” → Set “Receiving Status” to “Activated” → click “Next” → Confirm.



(4) WMI Configuration

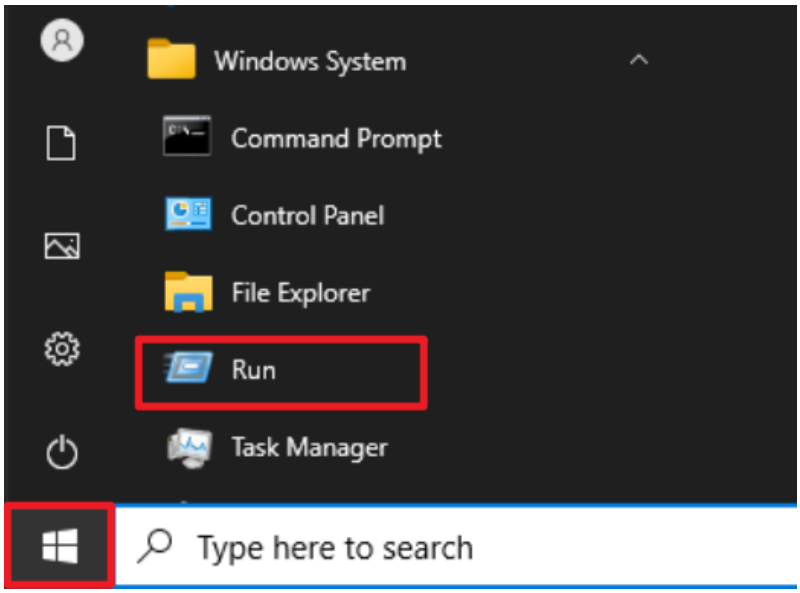
Enter the Windows AD WMI login account and password. If WMI is not configured, leave these fields blank.



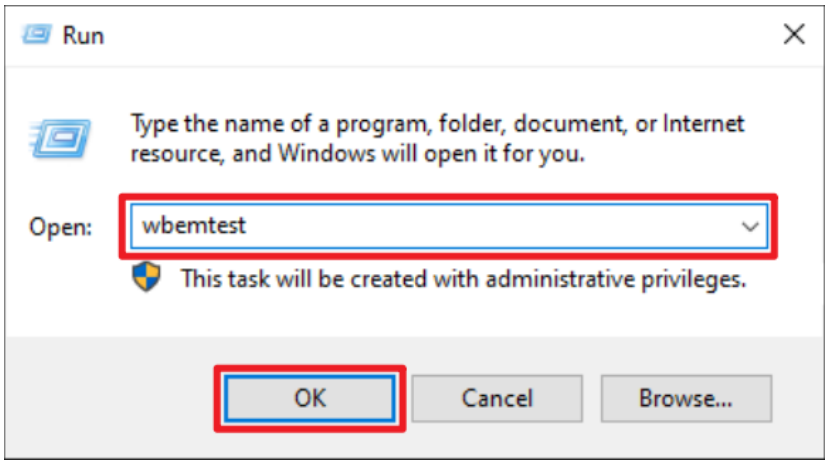
10. Troubleshooting

10.1 WMI Query Language Check

(1) Click “Start” → select “Run.”

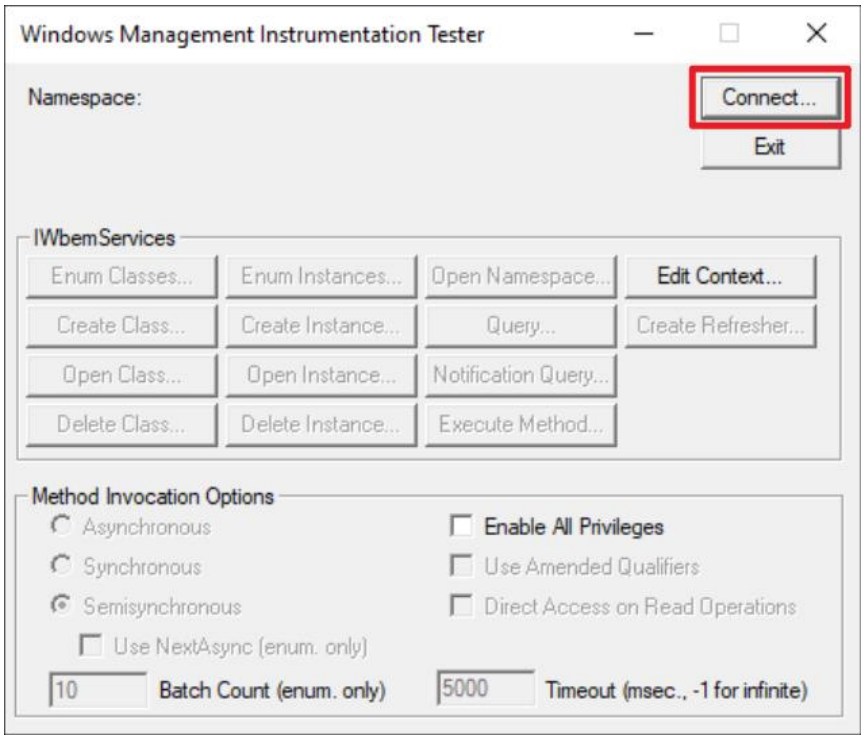


(2) Enter “wbemtest” → click “OK”

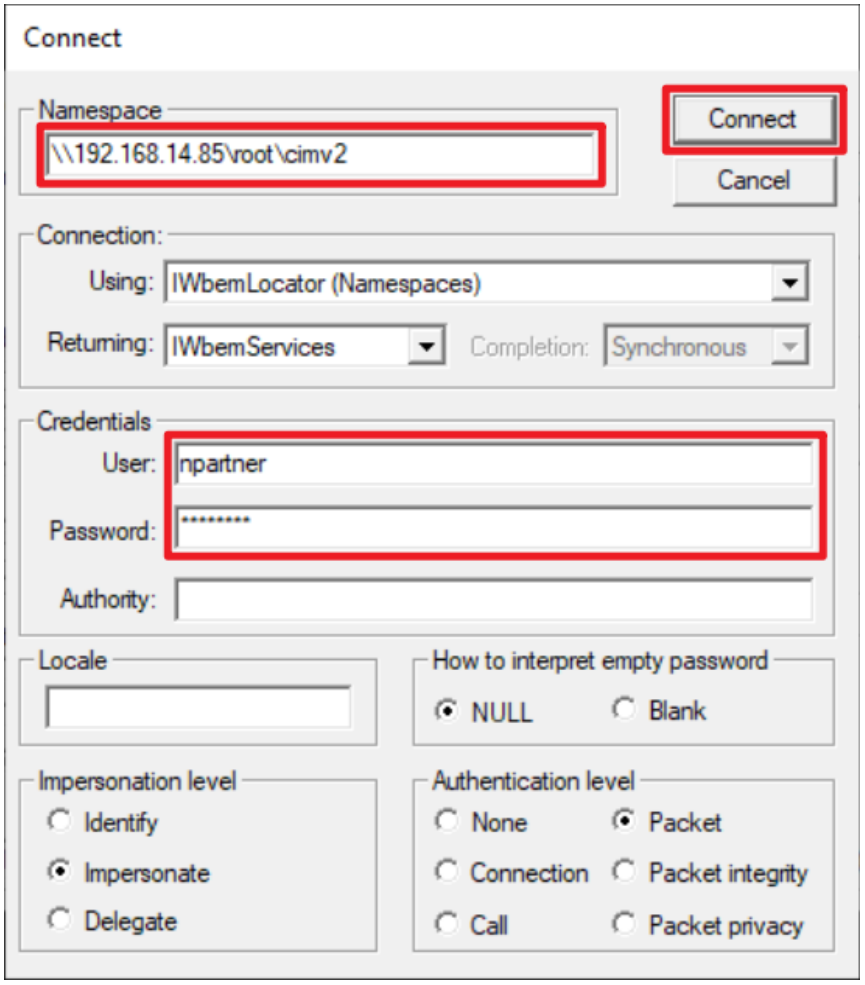


10.1.1 Query Event Logs

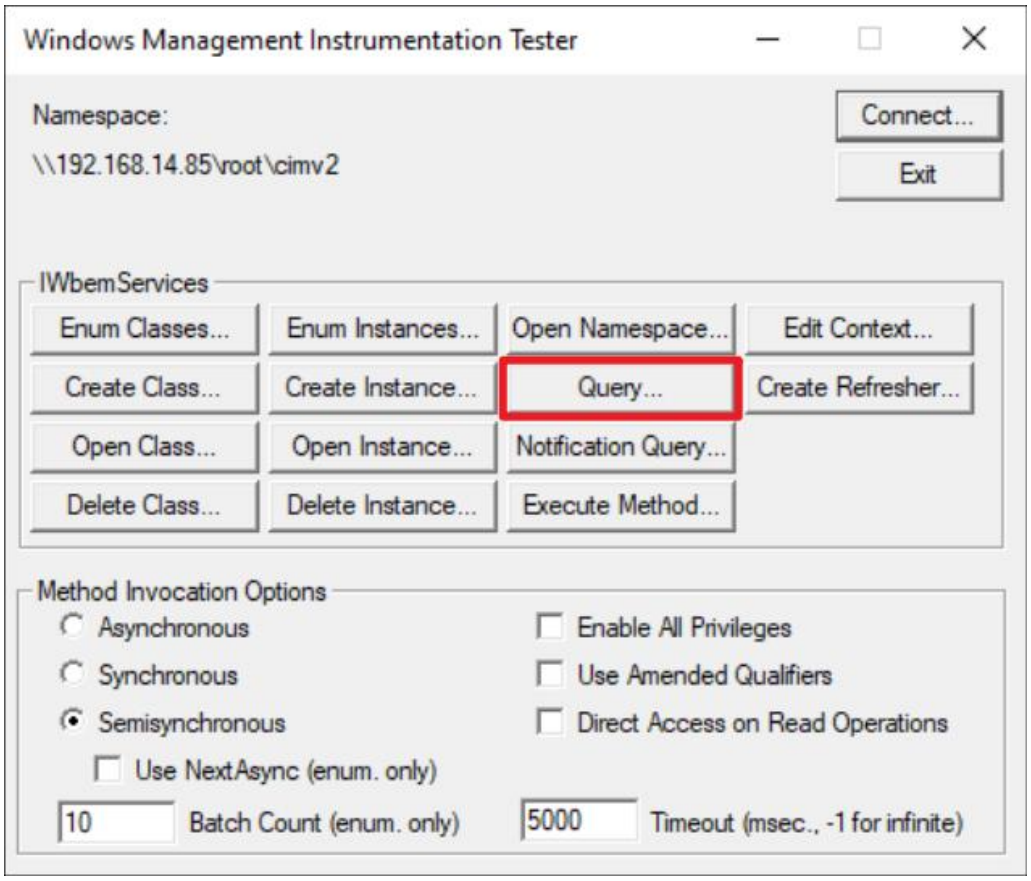
(1) Click “Connect.”



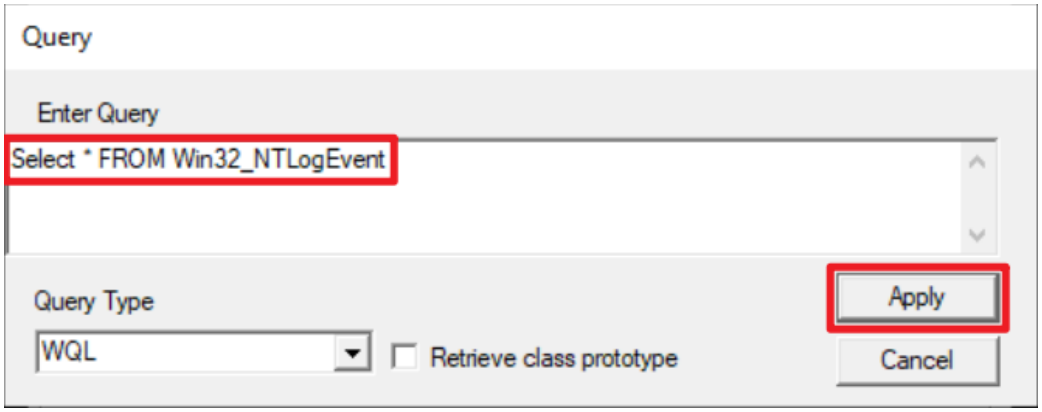
(2) Enter the namespace: (the example here is \\192.168.14.85\root\cimv2) → provide the username and password → click “Connect.”



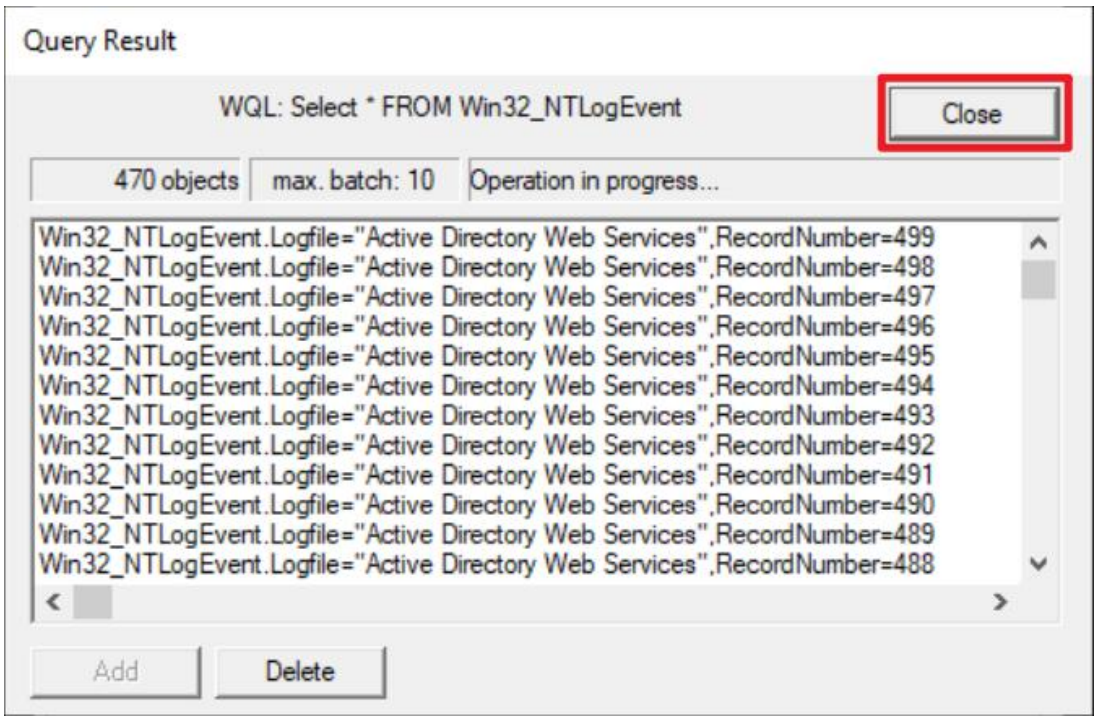
(3) Click “Query.”



(4) Enter the query: Select * FROM Win32_NTLogEvent → click “Apply.”

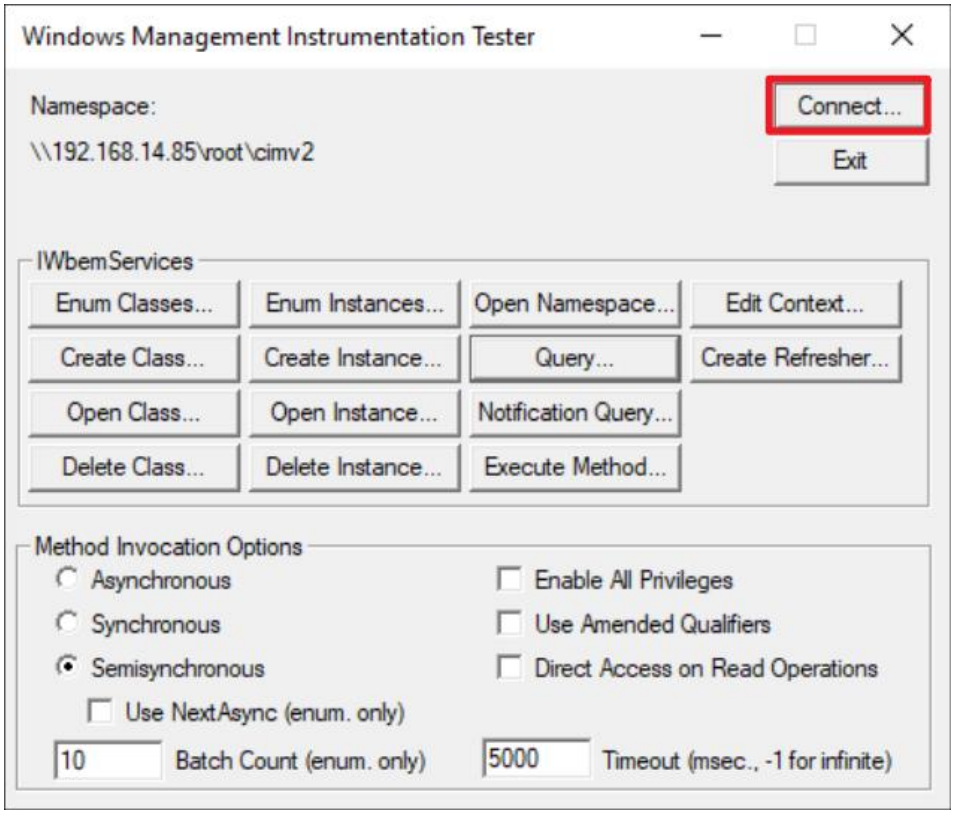


(5) The query results are displayed → click “Close.”

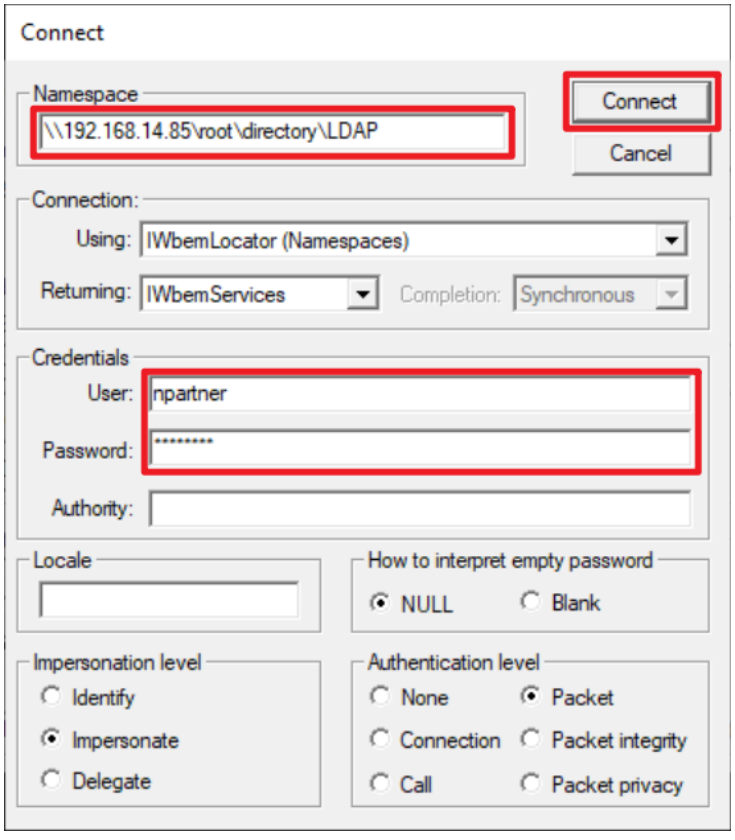


10.1.2 Query User Data

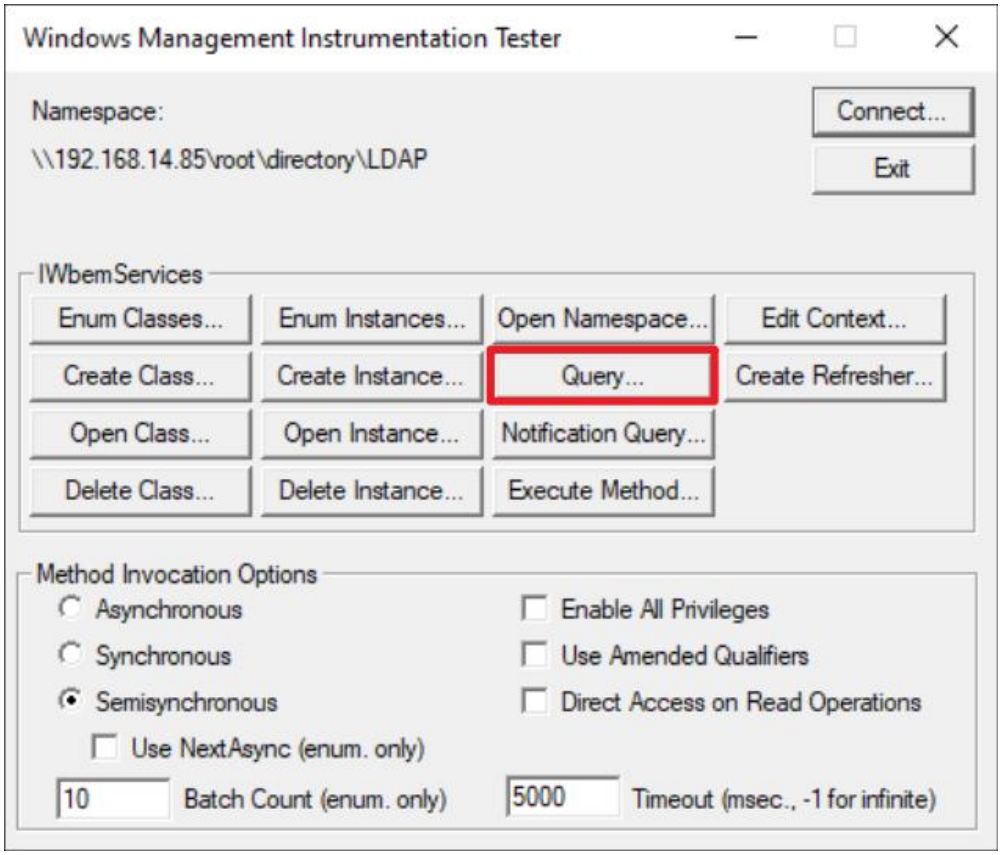
(1) Click “Connect.”



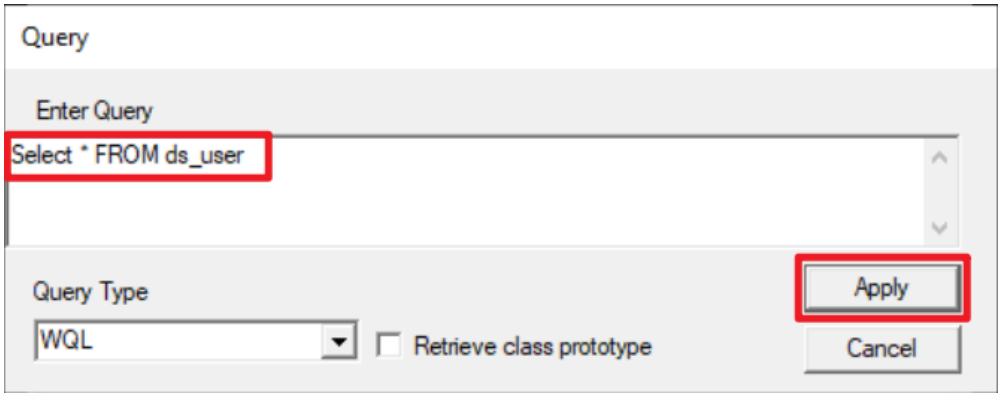
(2) Verify user data; enter the namespace: (the example here is \\192.168.14.85\root\cimv2) → provide the username and password → click “Connect.”



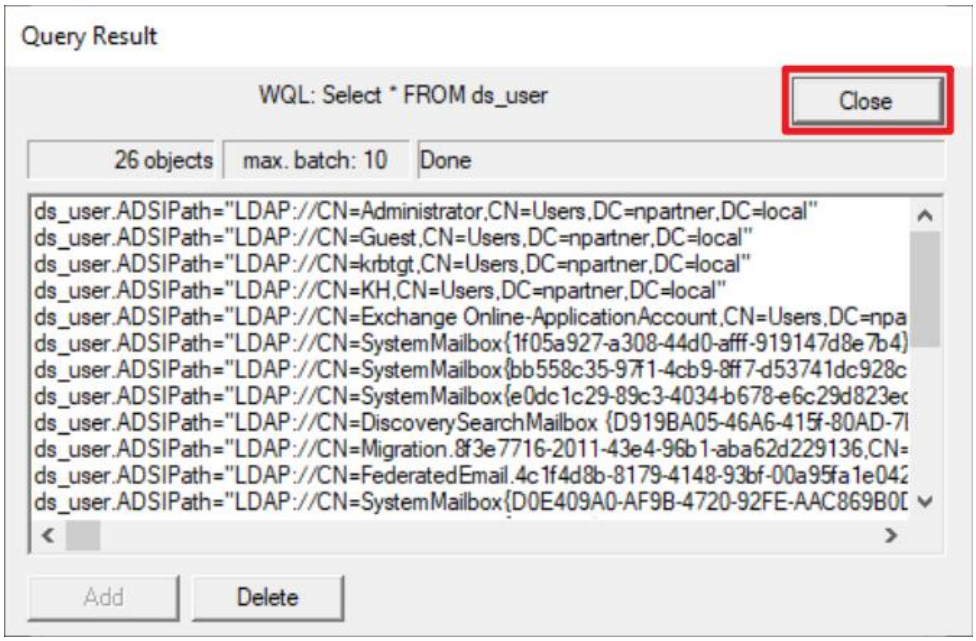
(3) Click “Query.”



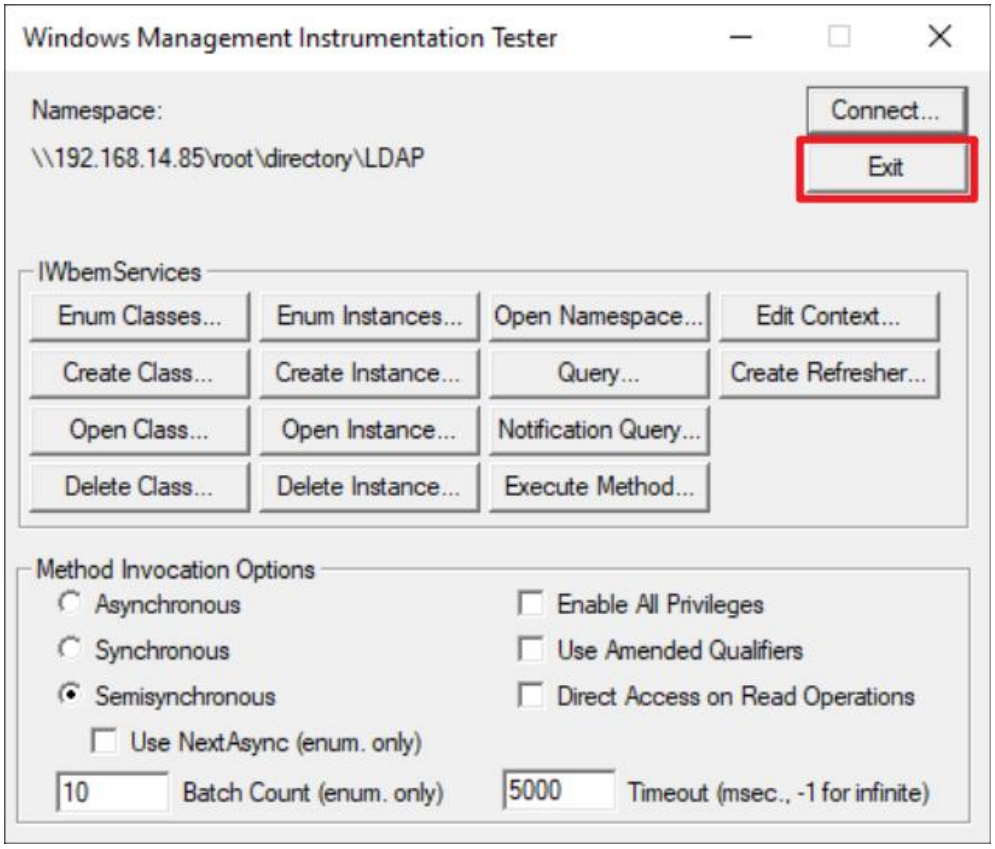
(4) Enter the query: Select * FROM ds_user → click “Apply.”



(5) The query results are displayed → click “Close.”

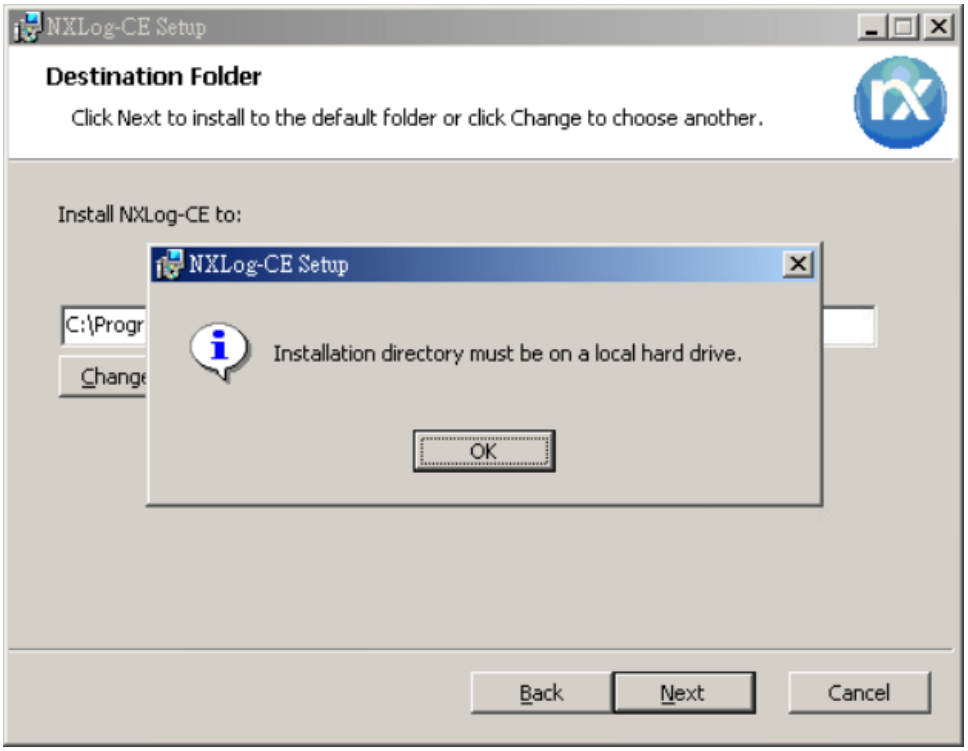


(6) If the user account and password can successfully query data, click “Exit” to close the WMI Tester.



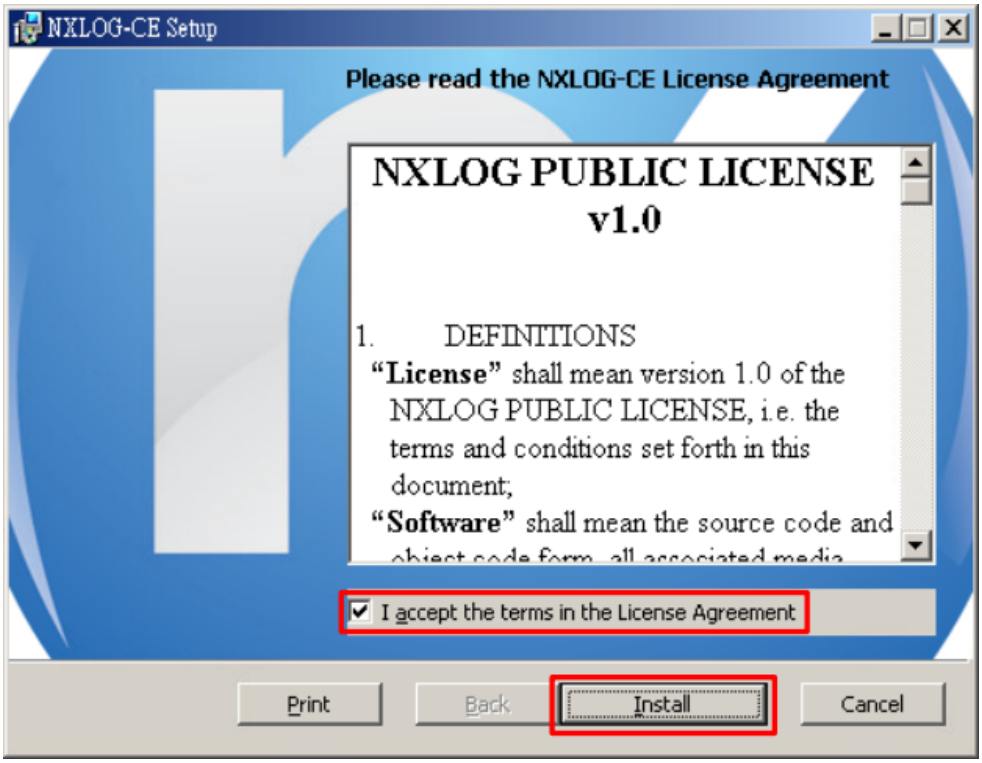
10.2 NXLog Installation Issues

(1) If Installing NXLog (2.10.2150) displays the message: Installation directory must be on a local hard drive.



(2) Install an earlier version of NXLog:

Click “nxlog-ce-2.9.1716.msi” → check “I accept the terms in the License Agreement.” → click “Install” until “Finish.”



Tel：+886-4-23752865　Fax：+886-4-23757458
Sales Information：sales@npartner.com
Technical Support：support@npartner.com