

Partner

How to Configure Windows AD Event Log

V019

2025/09/03



Copyright Declaration

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

Registered Trademark

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

Contents

Preface	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.

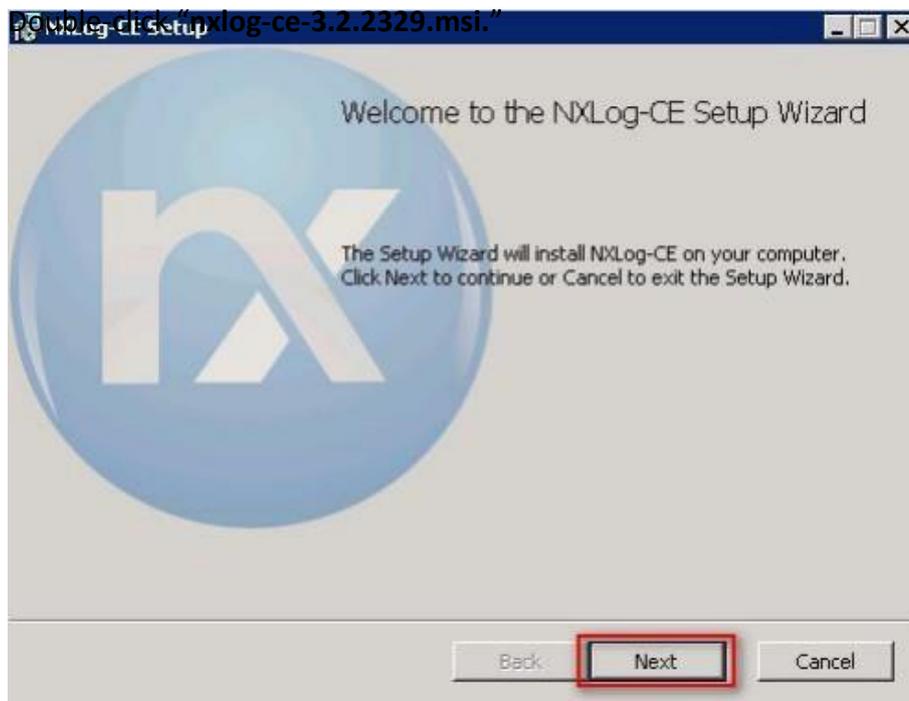
Example Here: **nxlog-ce-3.2.2329.msi**



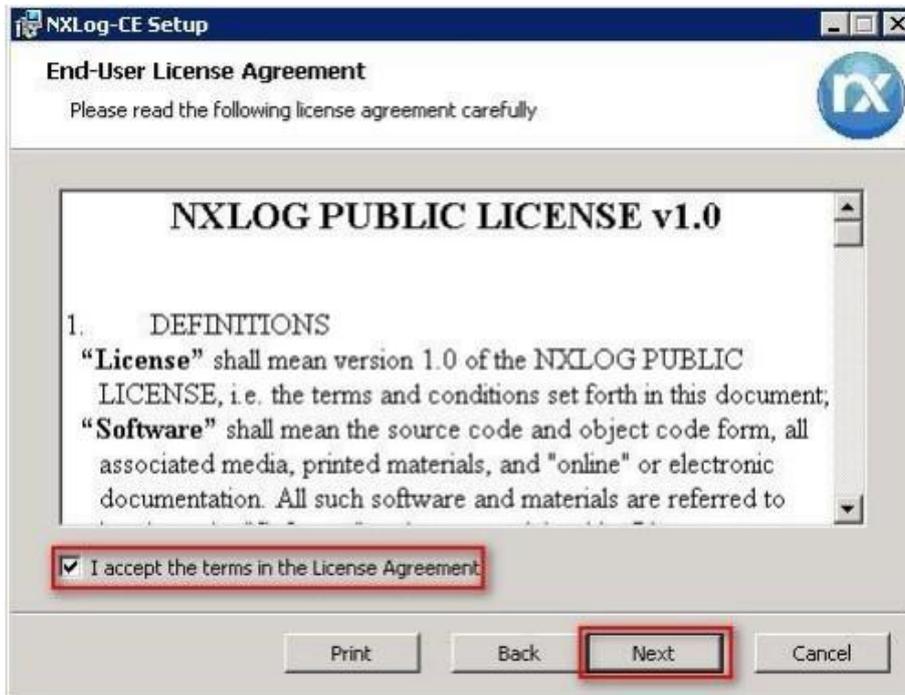
Note: If you require the **32-bit** version of NXLog, please contact our support team.

(2) Install NXLog

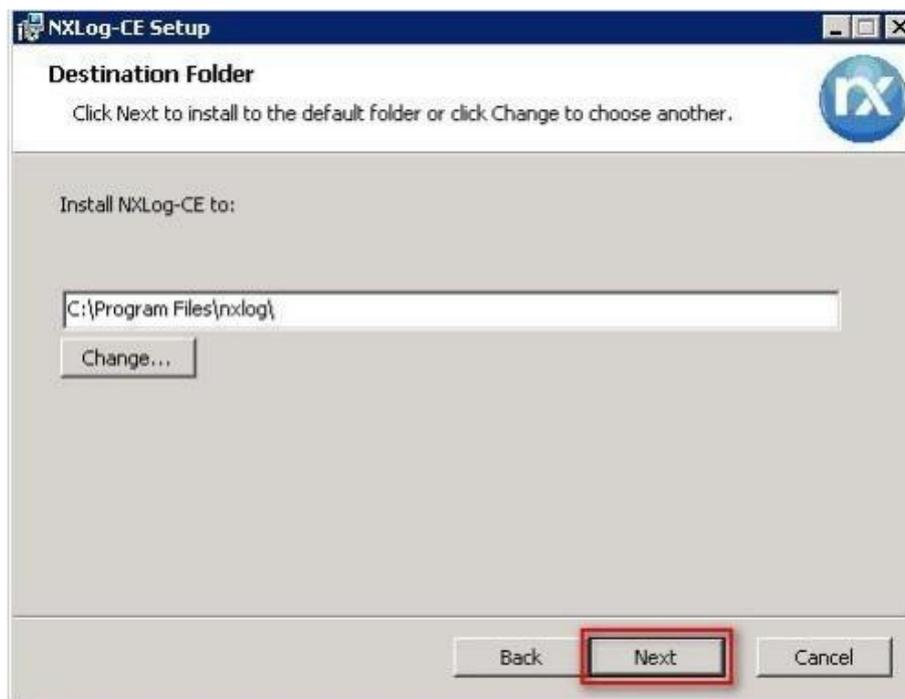
<2.1> For Windows Server **2008** or later:



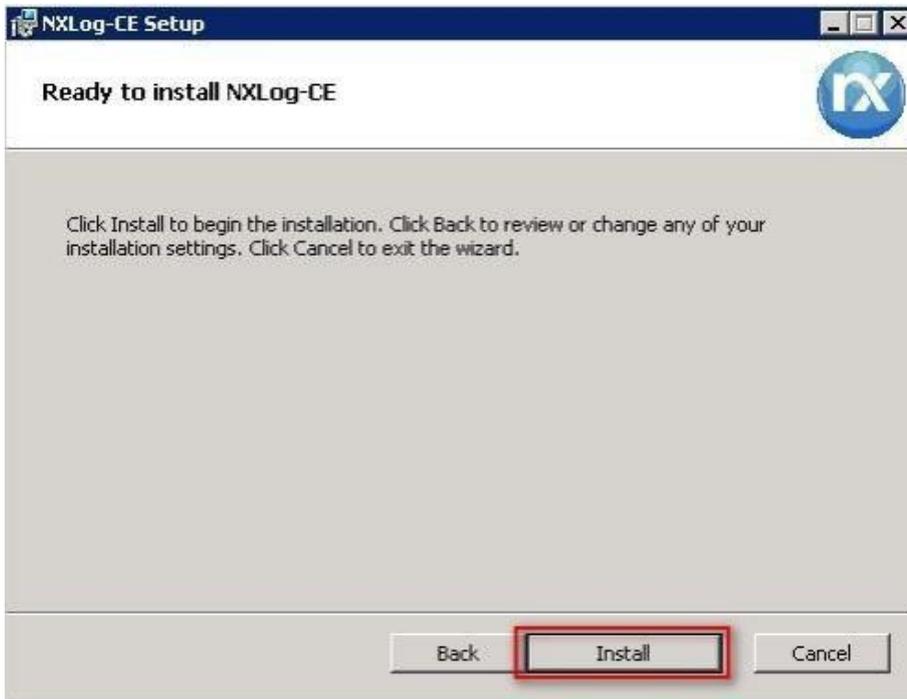
(3) Select "I accept the terms in the License Agreement," then click "Next."



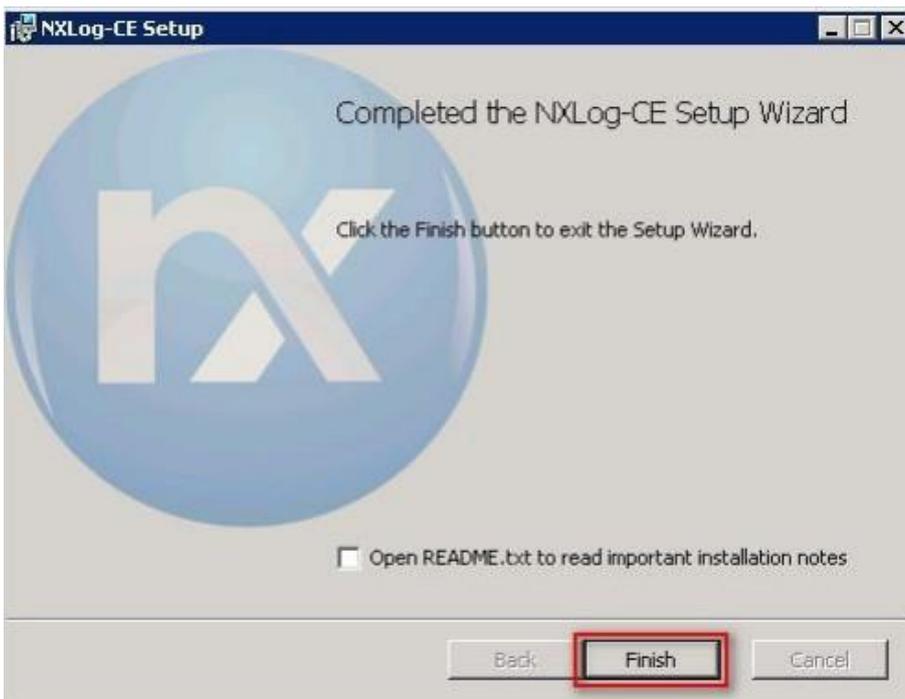
(4) Click "Next." (The default installation path is (C:\Program Files\nxlog\)).



(5) Click "Install."

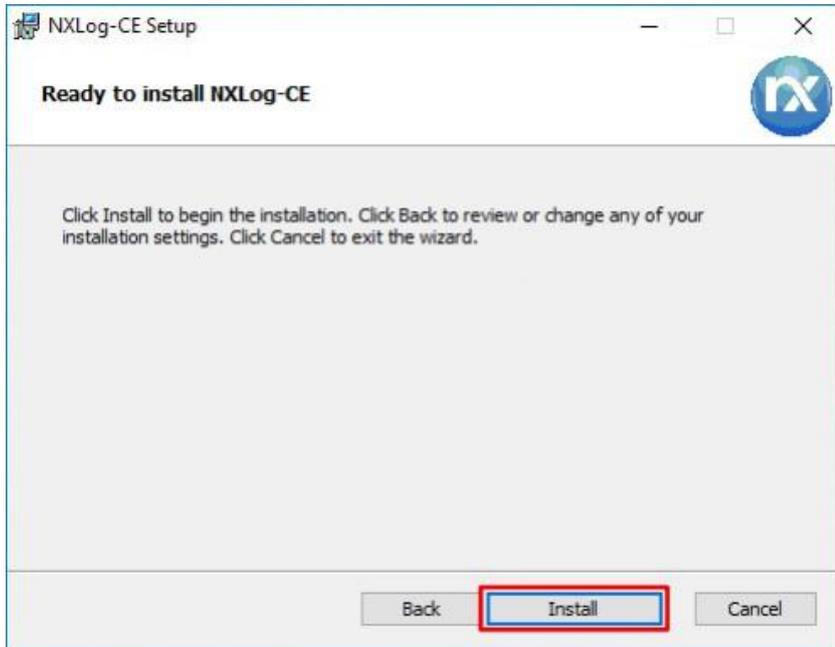


(6) Click "Finish."



<2.2> For Windows Server 2003:

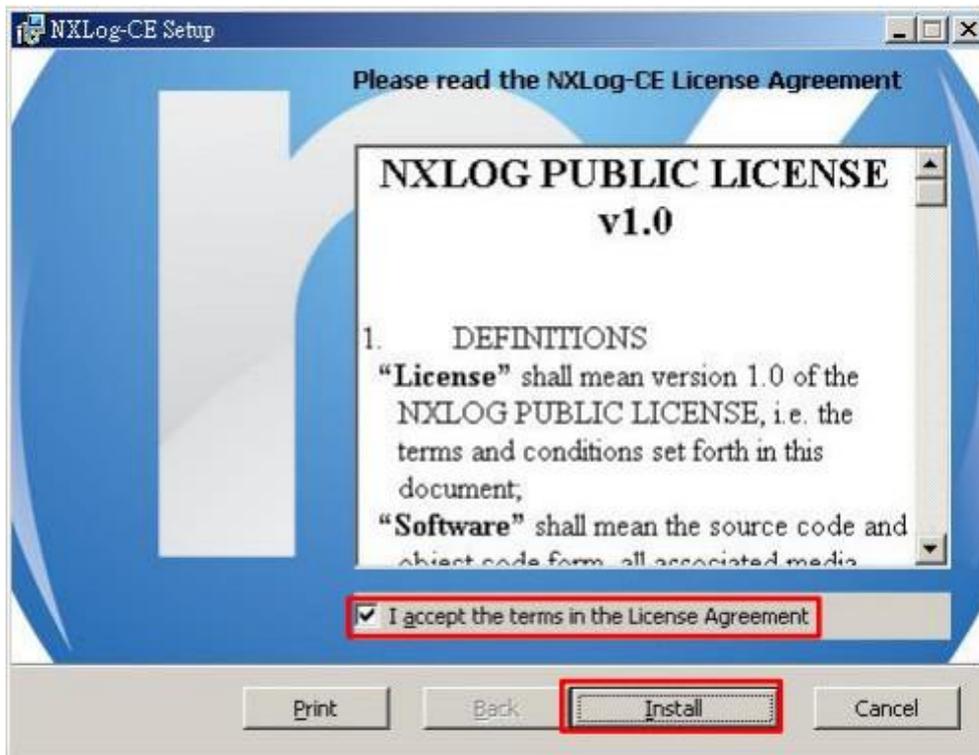
Download File: **nxlog-ce-3.2.2329.msi**. → Select “Install” and proceed until the installation completes. → Click “Finish” to exit.



<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

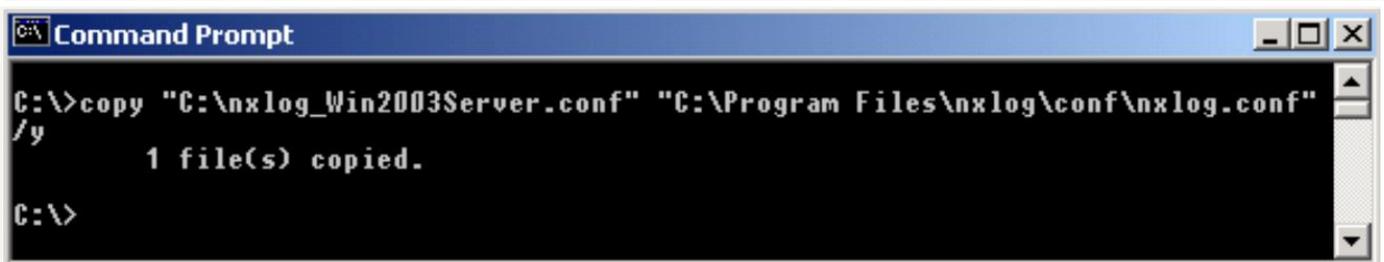
(1) Open "Command Prompt."



(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"
```



```
Command Prompt
C:\> copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf"
/y
      1 file(s) copied.
C:\>
```

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

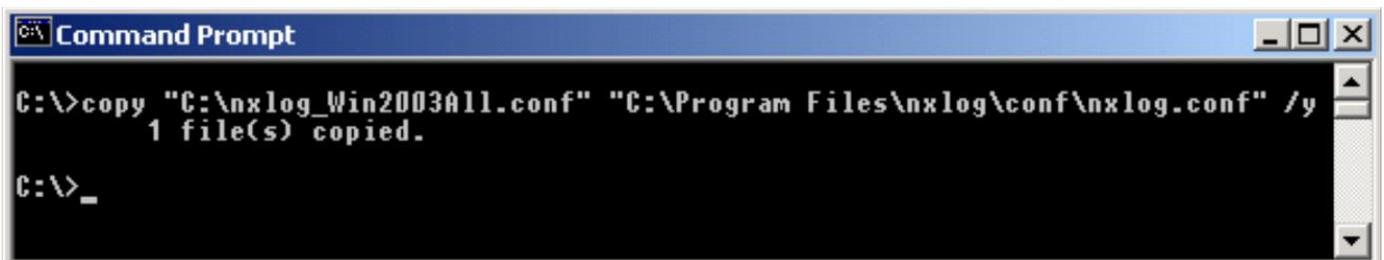
(1) Open "Command Prompt."



(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
```



```
Command Prompt
C:\>copy "C:\nxlog_Win2003All.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
        1 file(s) copied.
C:\>_
```

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

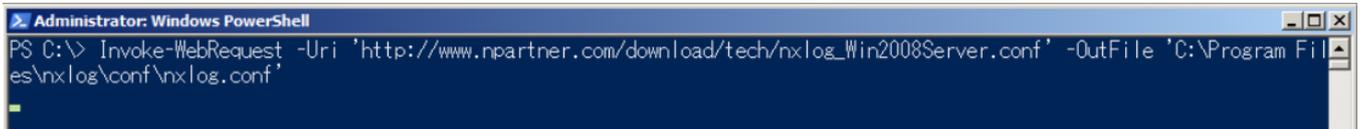
(1) Open “Command Prompt.”



(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>
```

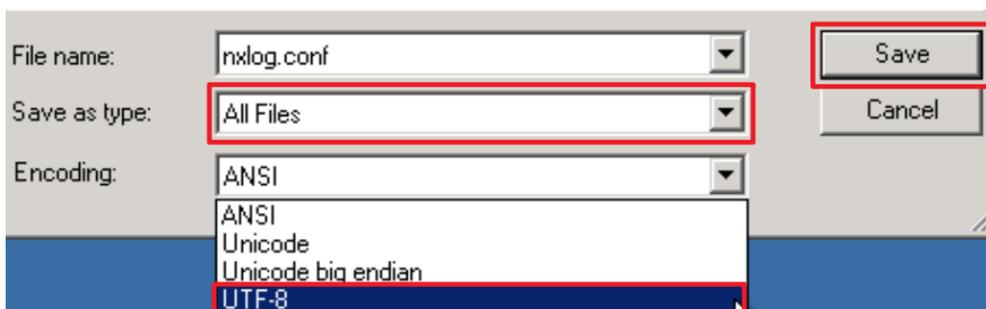
Enter the N-Cloud system IP address in the blue text section.

```
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

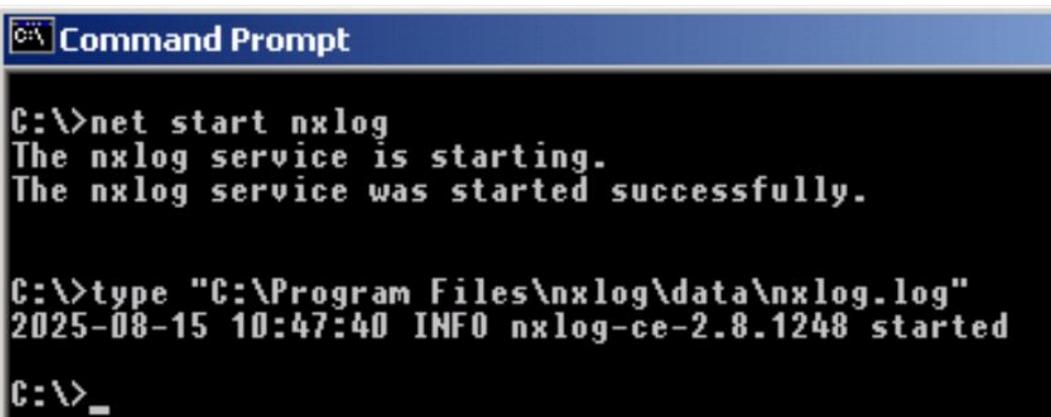
1.4.1 For Windows Server 2003 or earlier

(1) Open "Command Prompt."



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

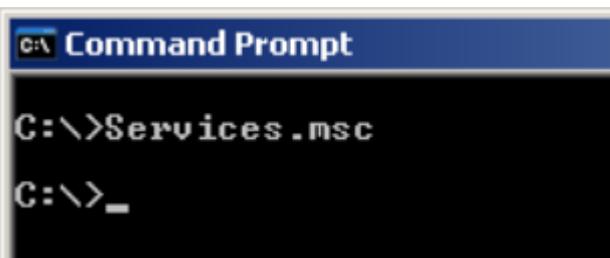
```
C:\> net start nxlog  
C:\> type "C:\Program Files\nxlog\data\nxlog.log"
```

A screenshot of a Windows Command Prompt window. The title bar reads "C:\> Command Prompt". The command prompt shows the following text:
C:\>net start nxlog
The nxlog service is starting.
The nxlog service was started successfully.

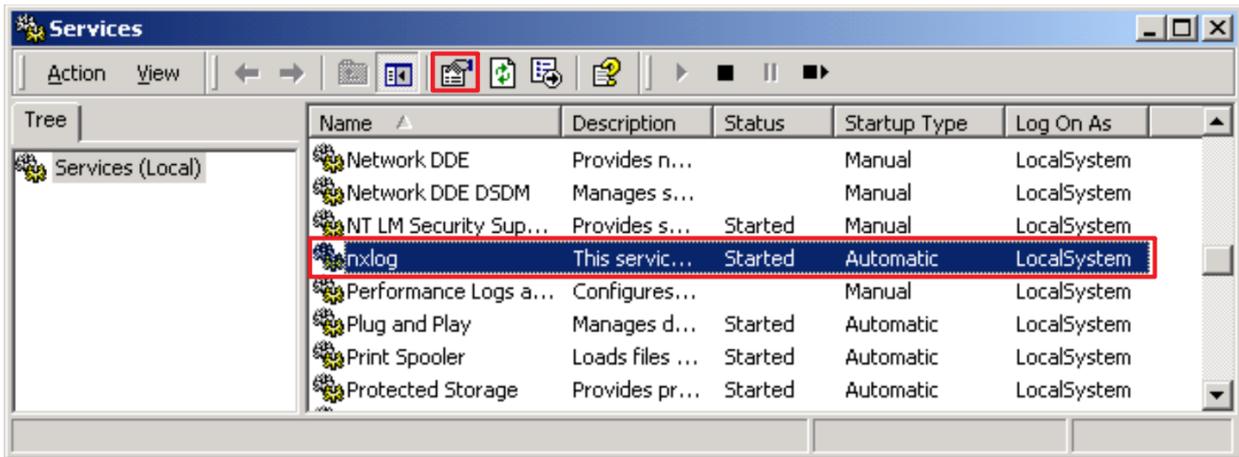
C:\>type "C:\Program Files\nxlog\data\nxlog.log"
2025-08-15 10:47:40 INFO nxlog-ce-2.8.1248 started
C:\>_

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

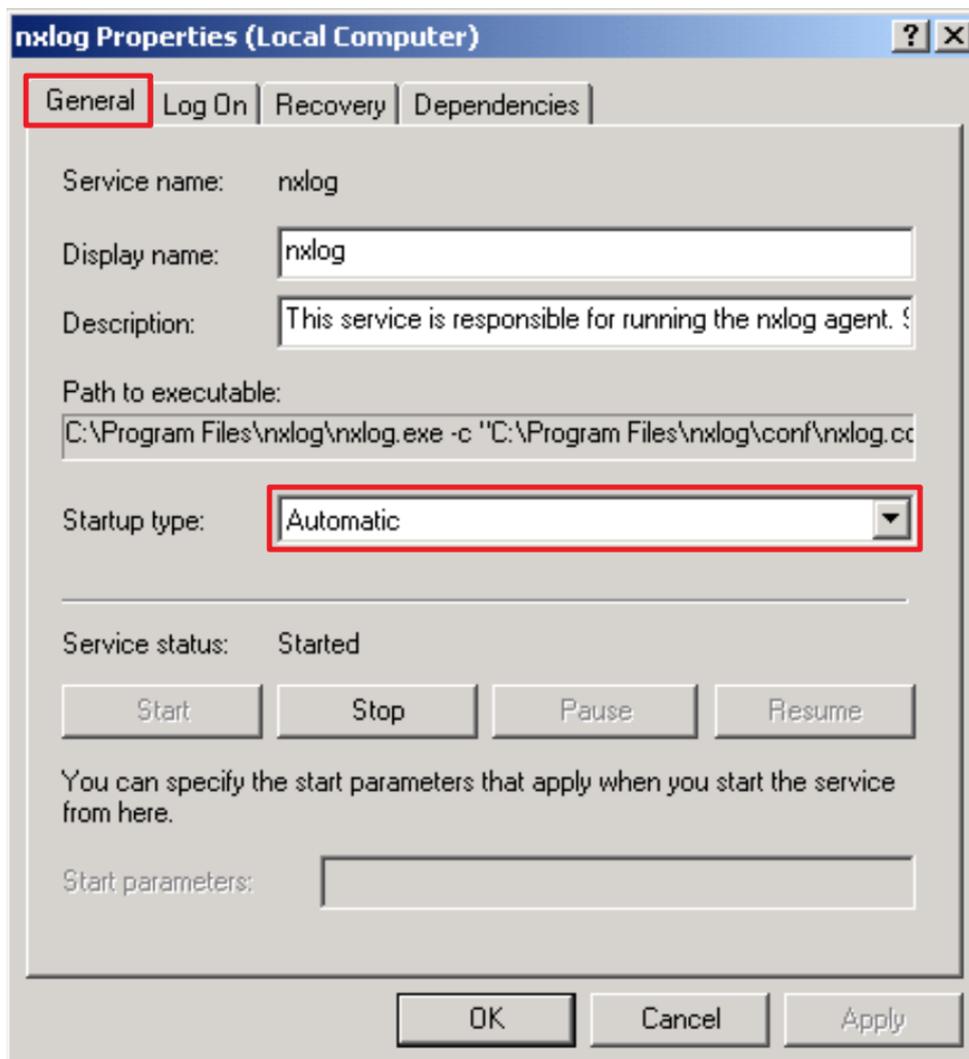
```
C:\> Services.msc
```



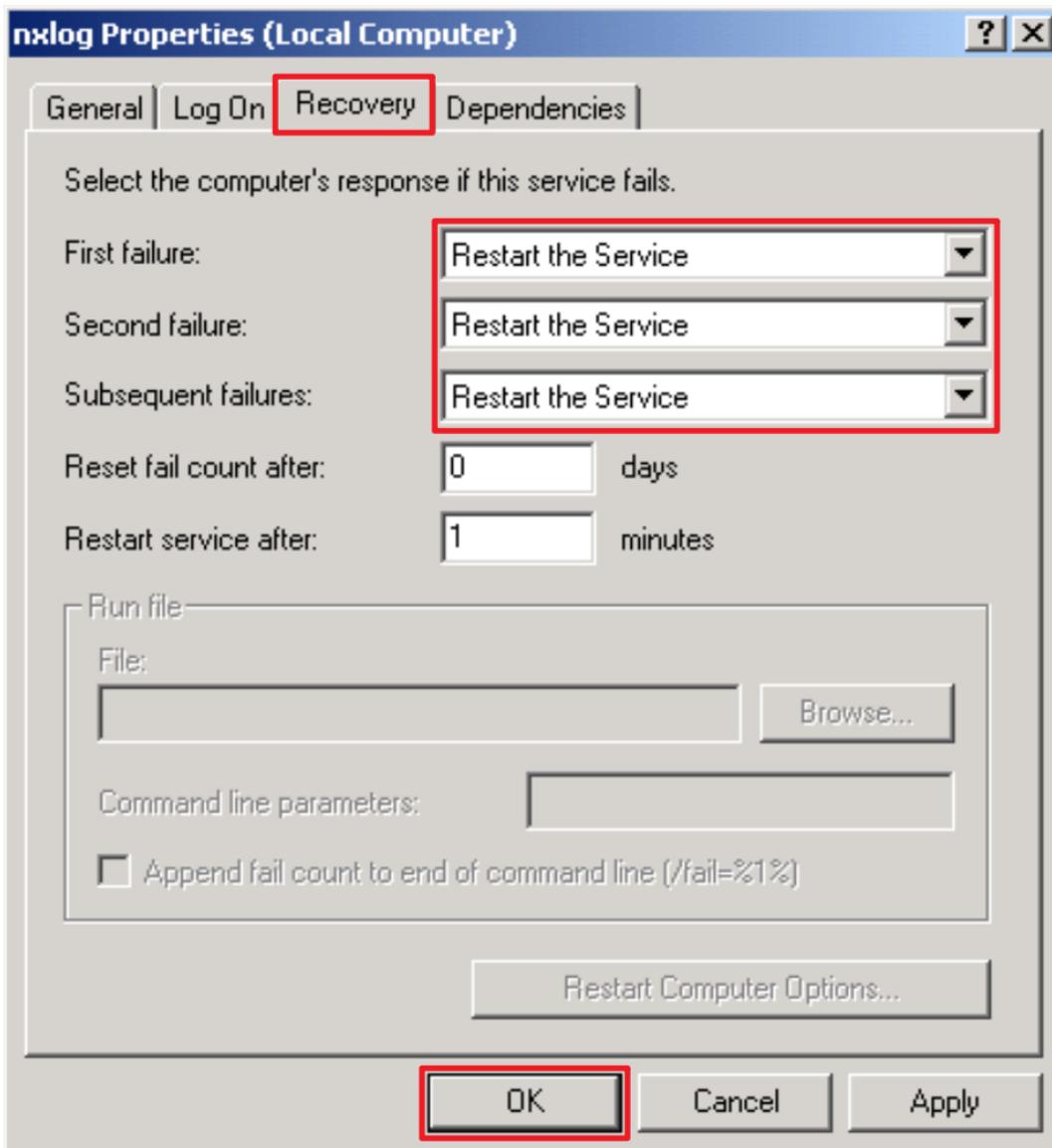
(4) Open the NXLog service properties: select “NXLog” → Click “Properties.”



(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'
```

A screenshot of an Administrator Windows PowerShell console window. The title bar reads "Administrator: Windows PowerShell". The command prompt shows the following commands and output:

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType

Name      Status StartType
-----
nxlog     Running Automatic

PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2025-08-15 11:04:35 INFO nxlog-ce-3.2.2329 started
PS C:\> _
```

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'

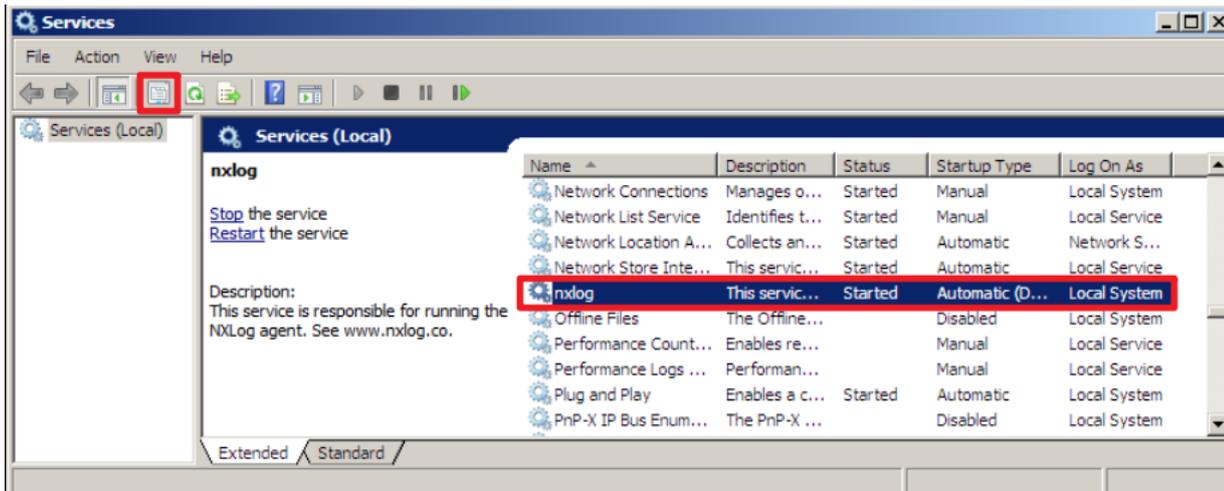
(3) Enter the command below to open the **Services** console:

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

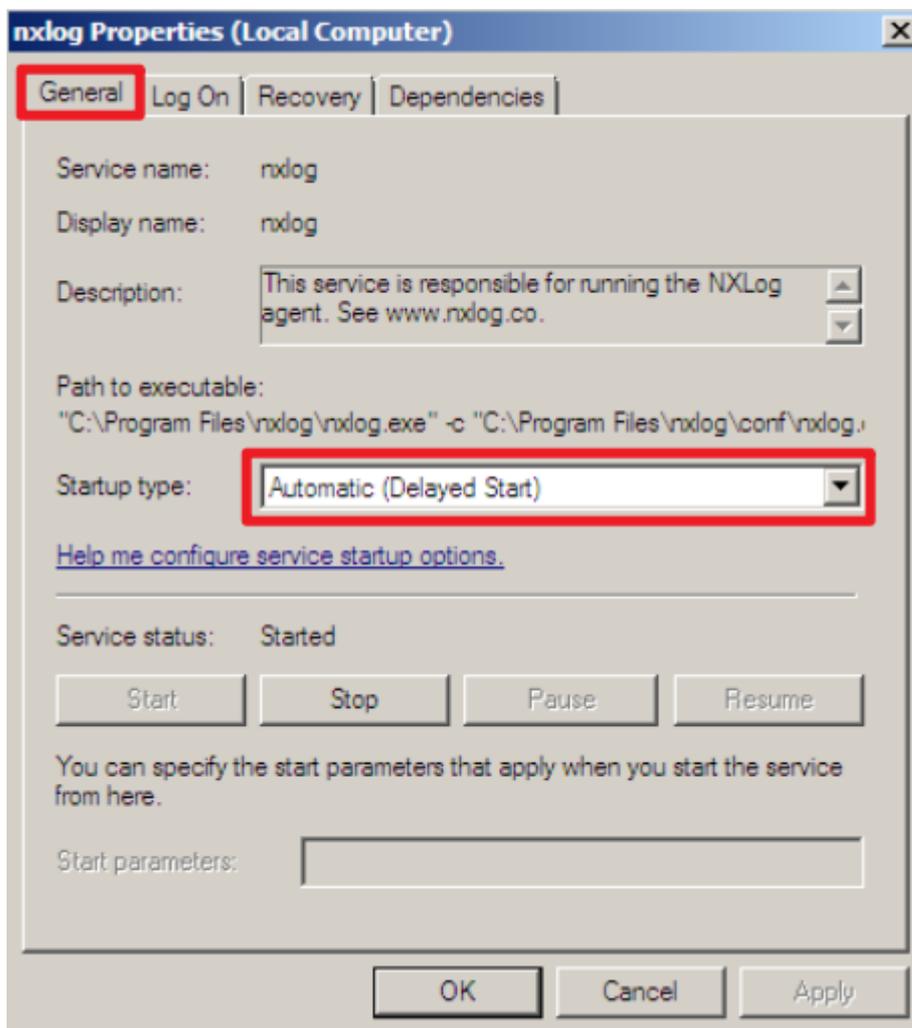
A screenshot of an Administrator Windows PowerShell console window. The title bar reads "Administrator: Windows PowerShell". The command prompt shows the following commands and output:

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

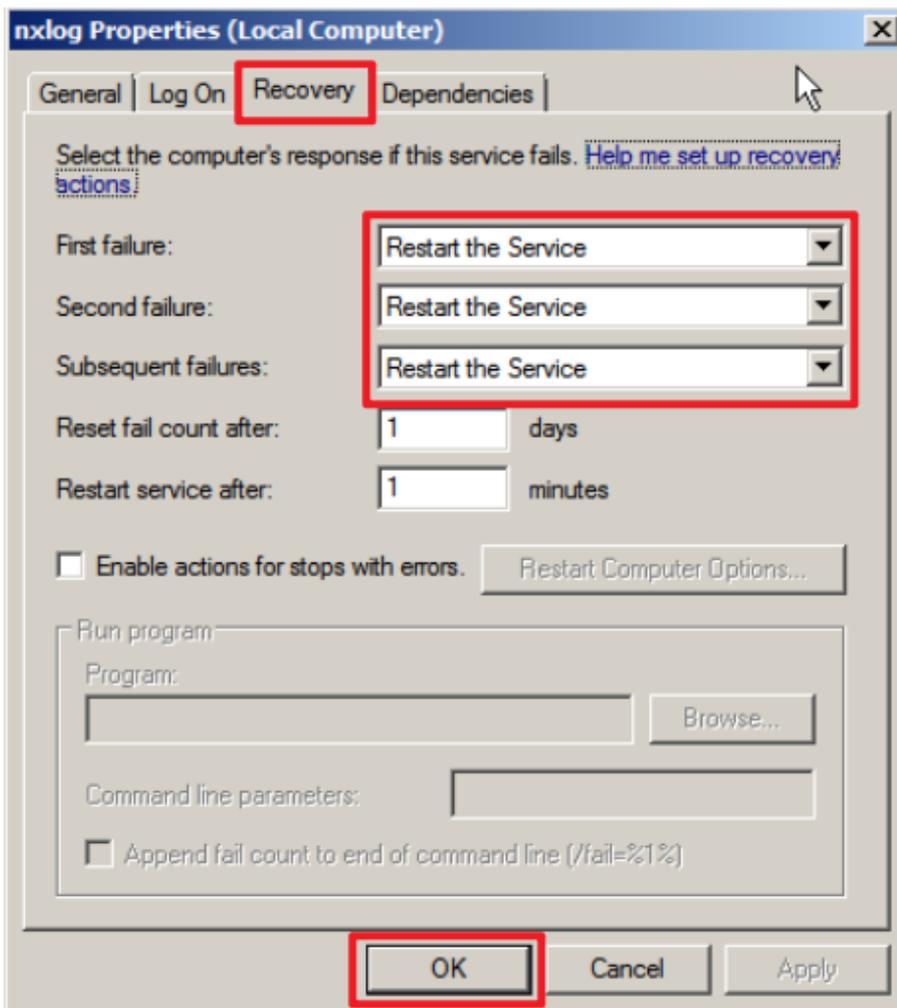
(4) Open the NXLog service properties: select "NXLog" → Click  "Properties."



(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.

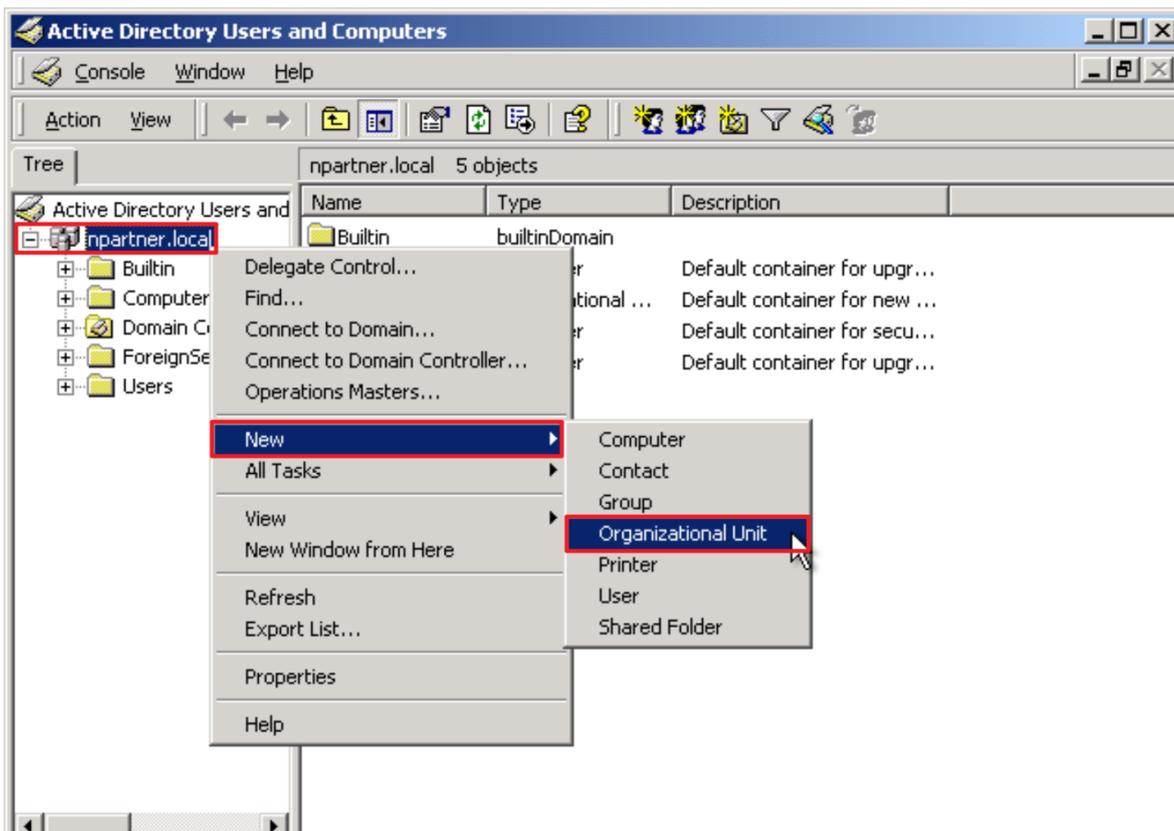
2.1 Organizational Unit (OU) Configuration

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



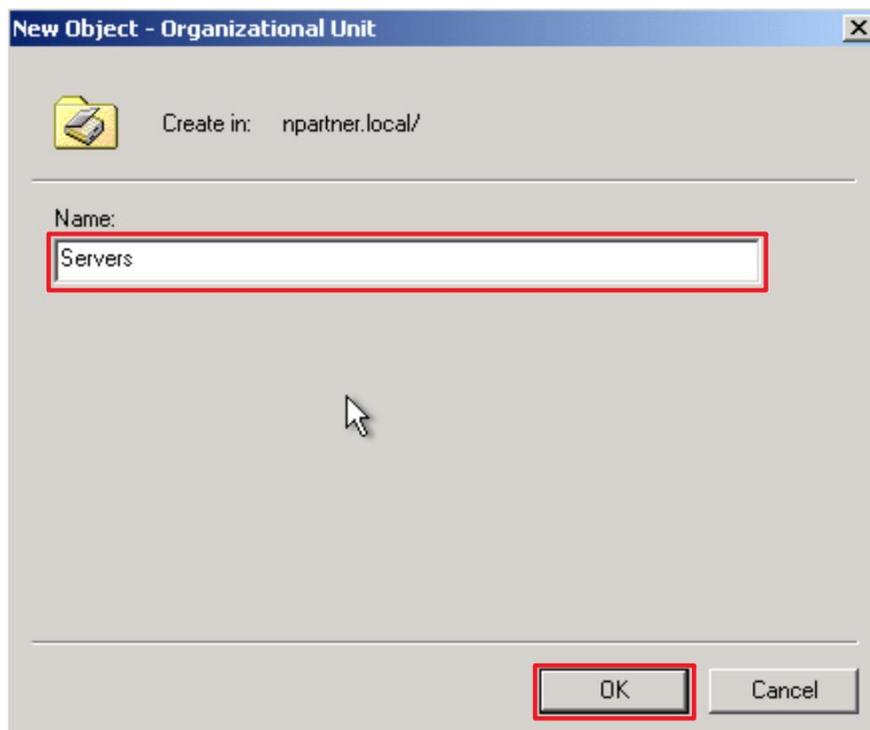
(2) Add an Organizational Unit

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



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

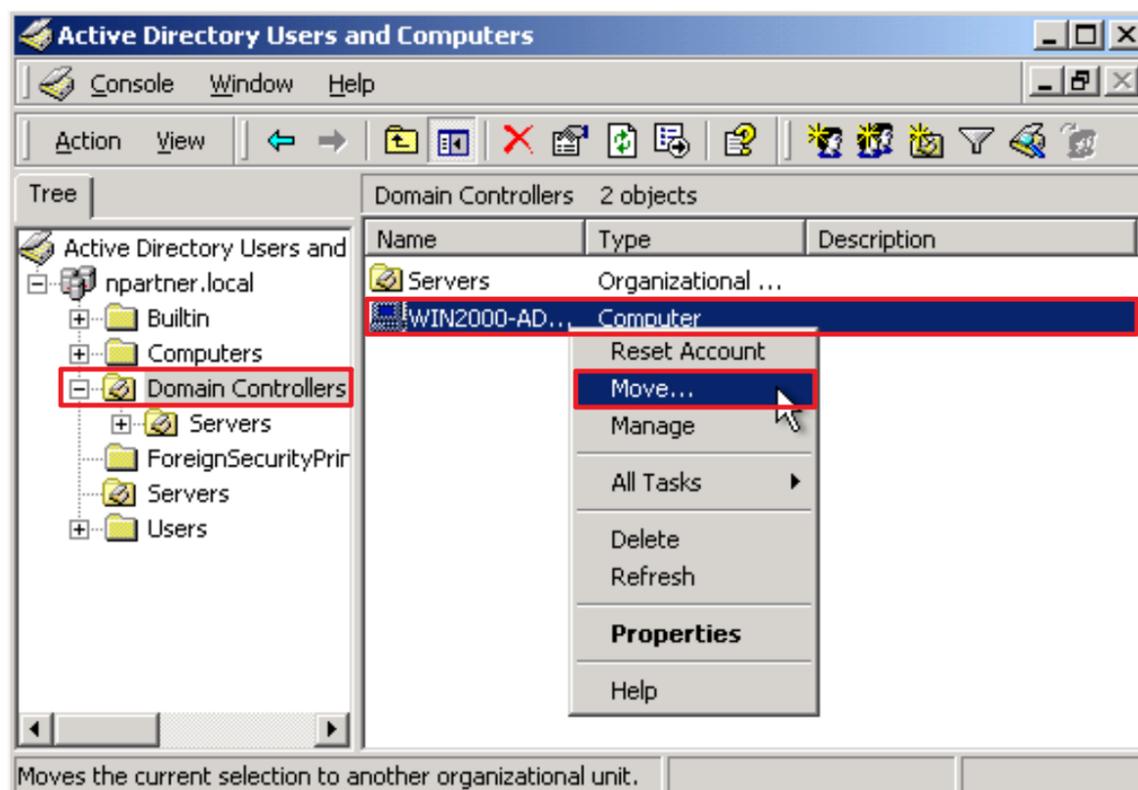
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

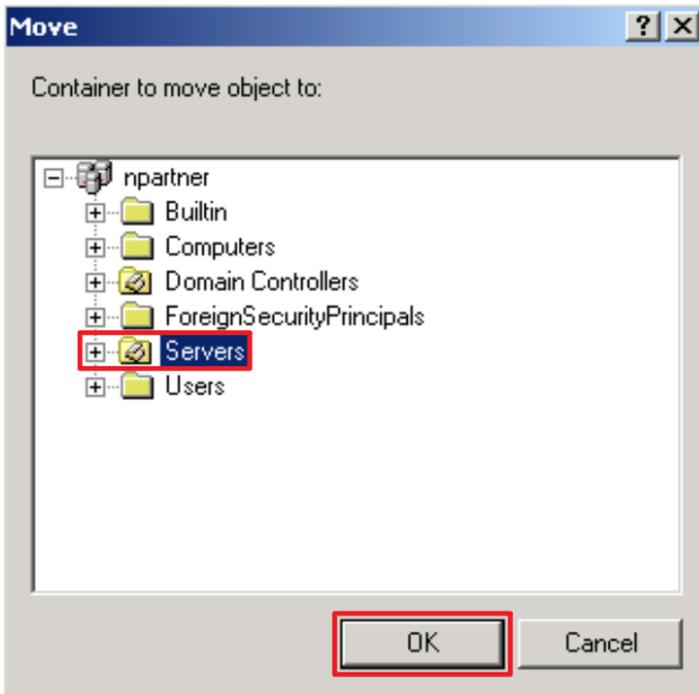
Select the “Computers” organizational unit (OU) → right-click on the “WIN2000-AD” server.

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



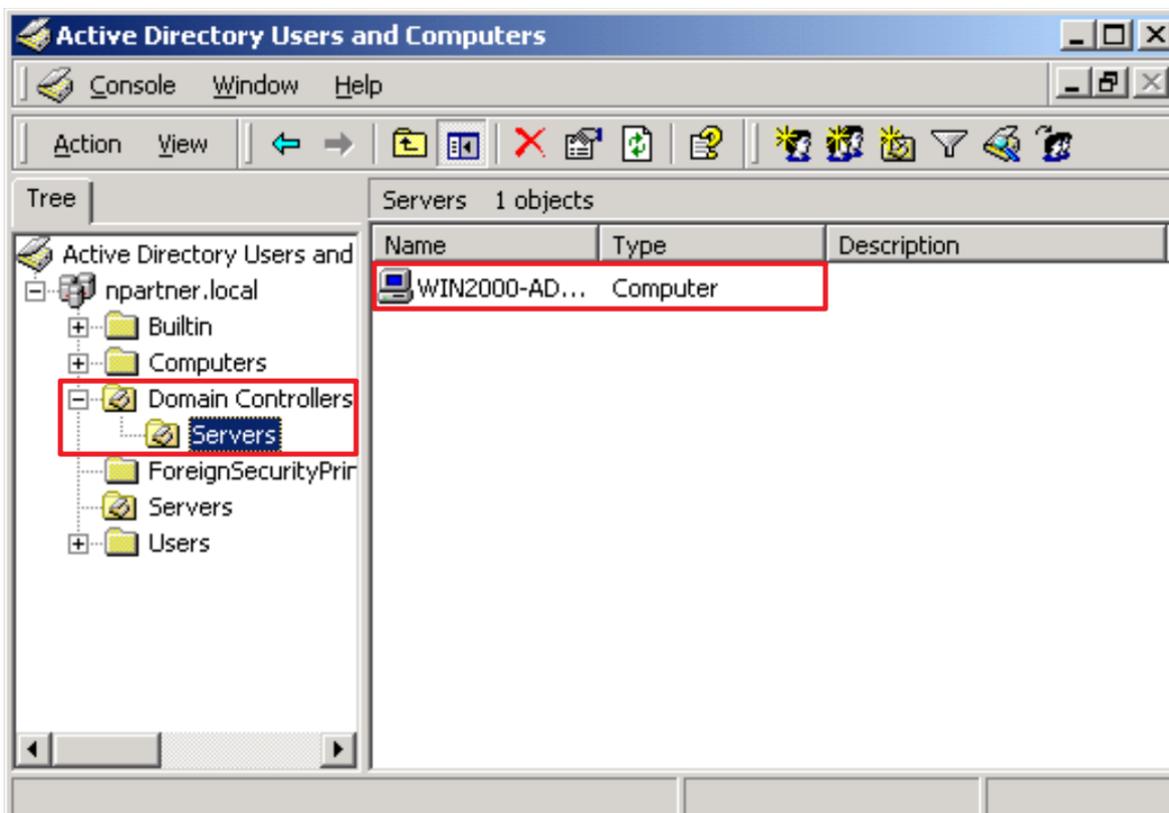
(5) Select your Organizational Unit:

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.

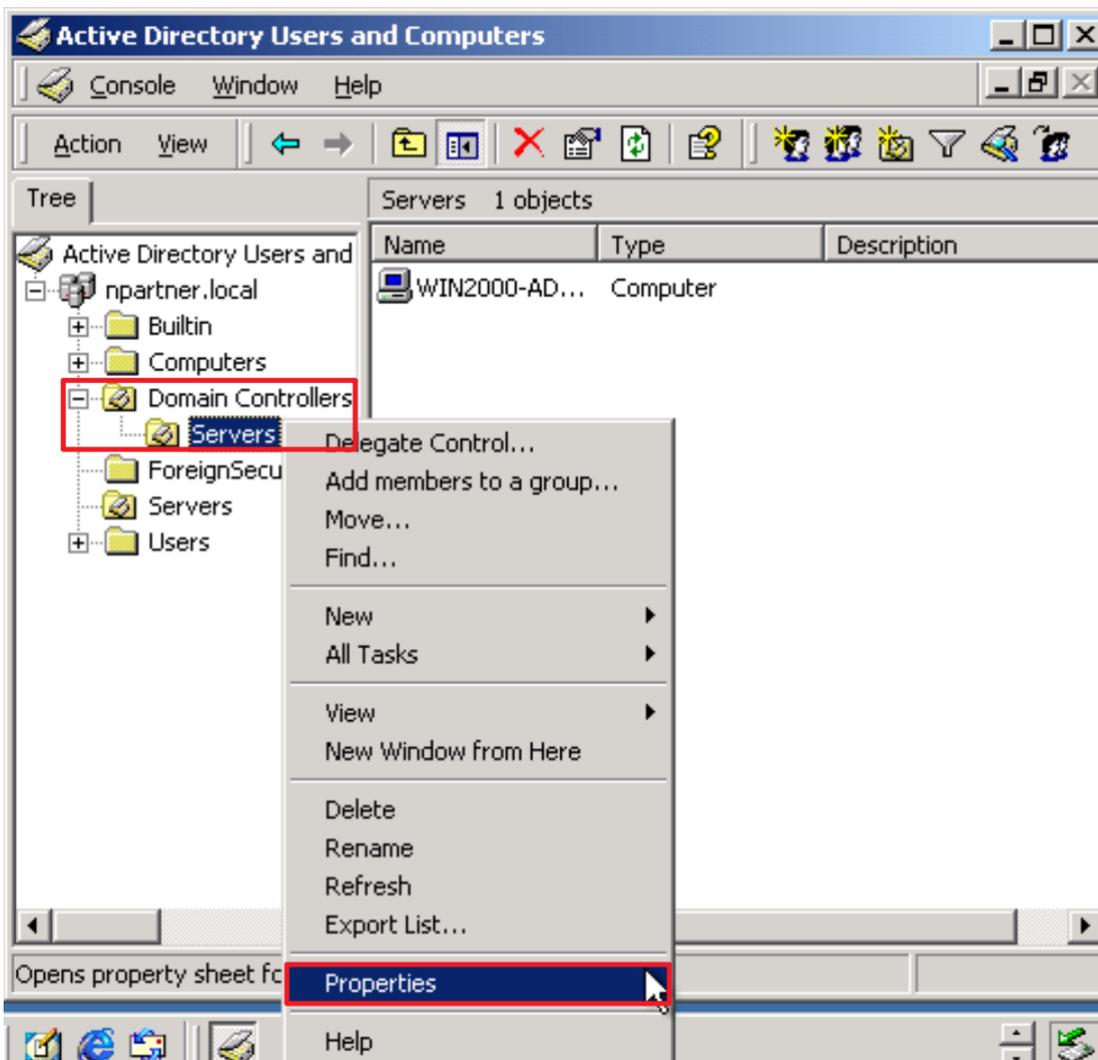


2.2 Group Policy Settings

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

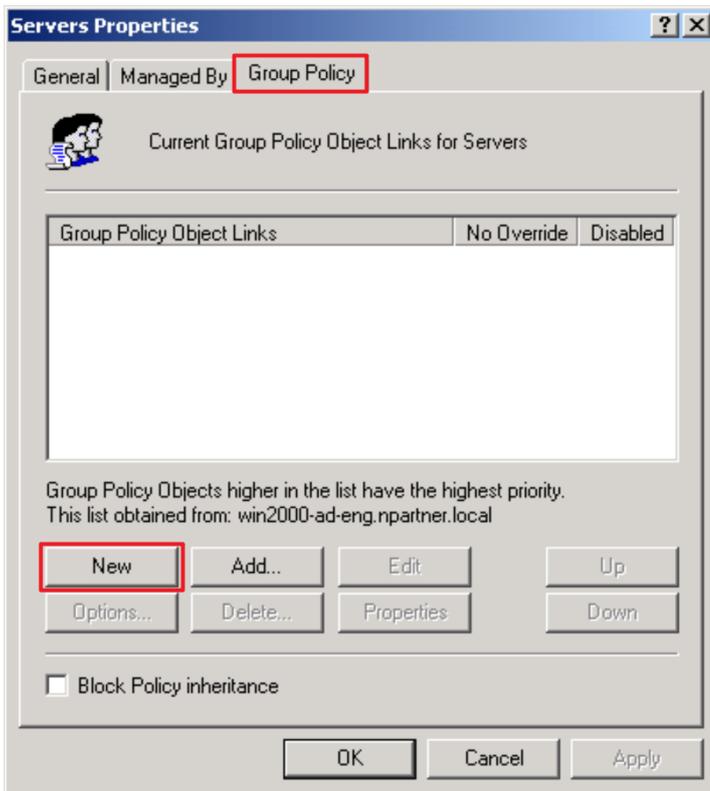


(2) In the “Servers” organizational unit (OU), right-click and select “Properties.”



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

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

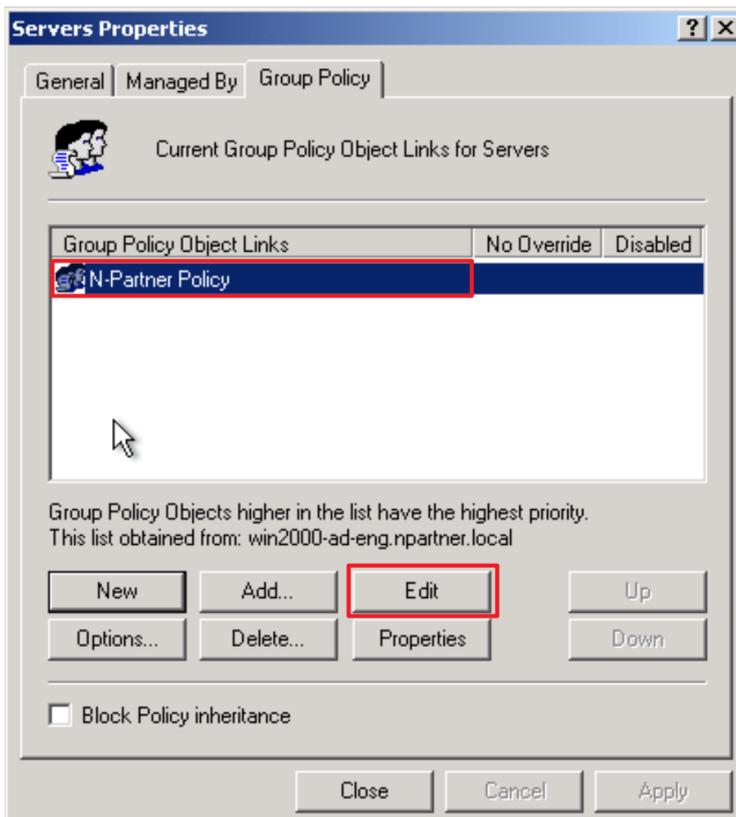


(4) Edit your Group Policy Object

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

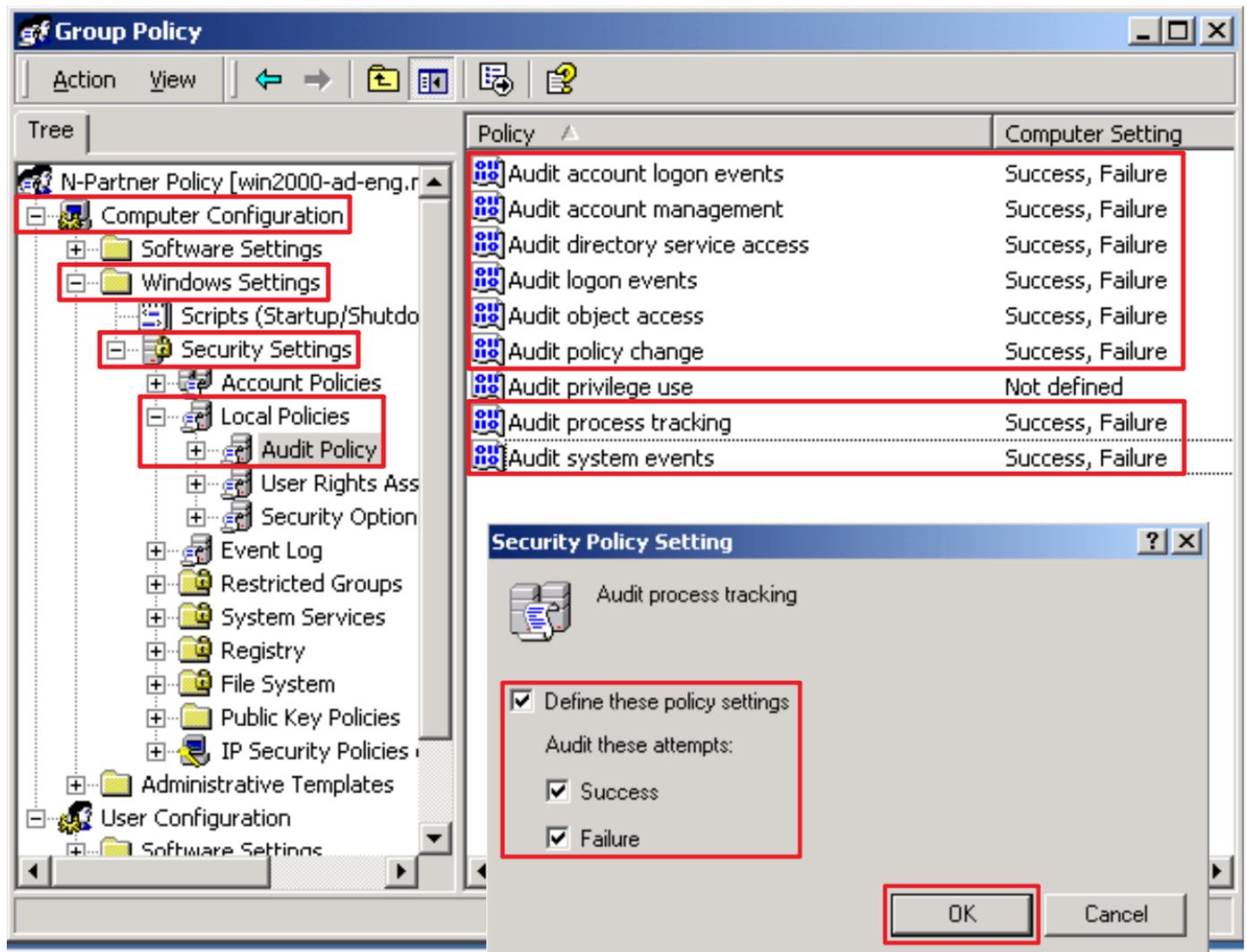
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



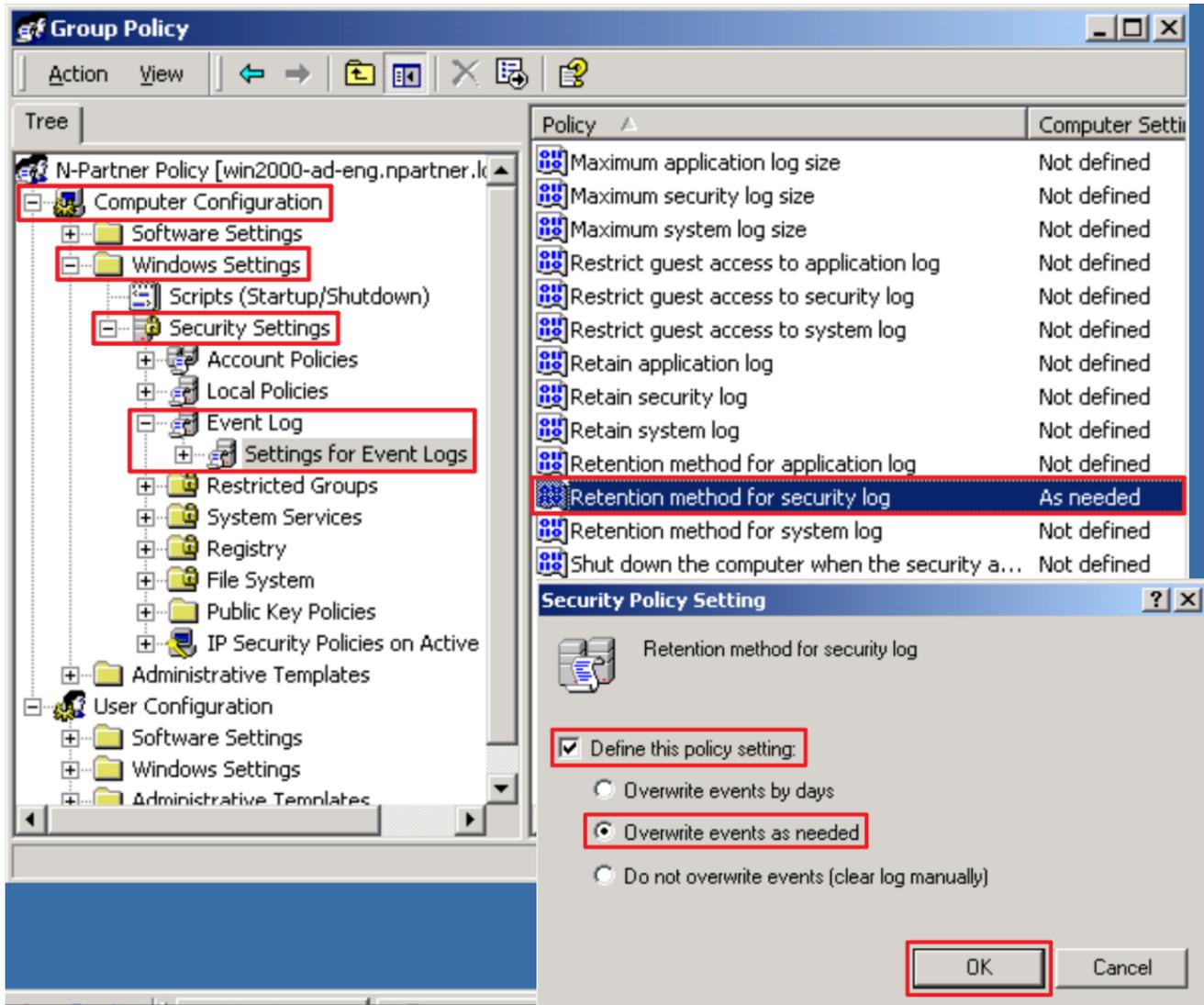
(5) Local Group Policies: Audit Policy

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

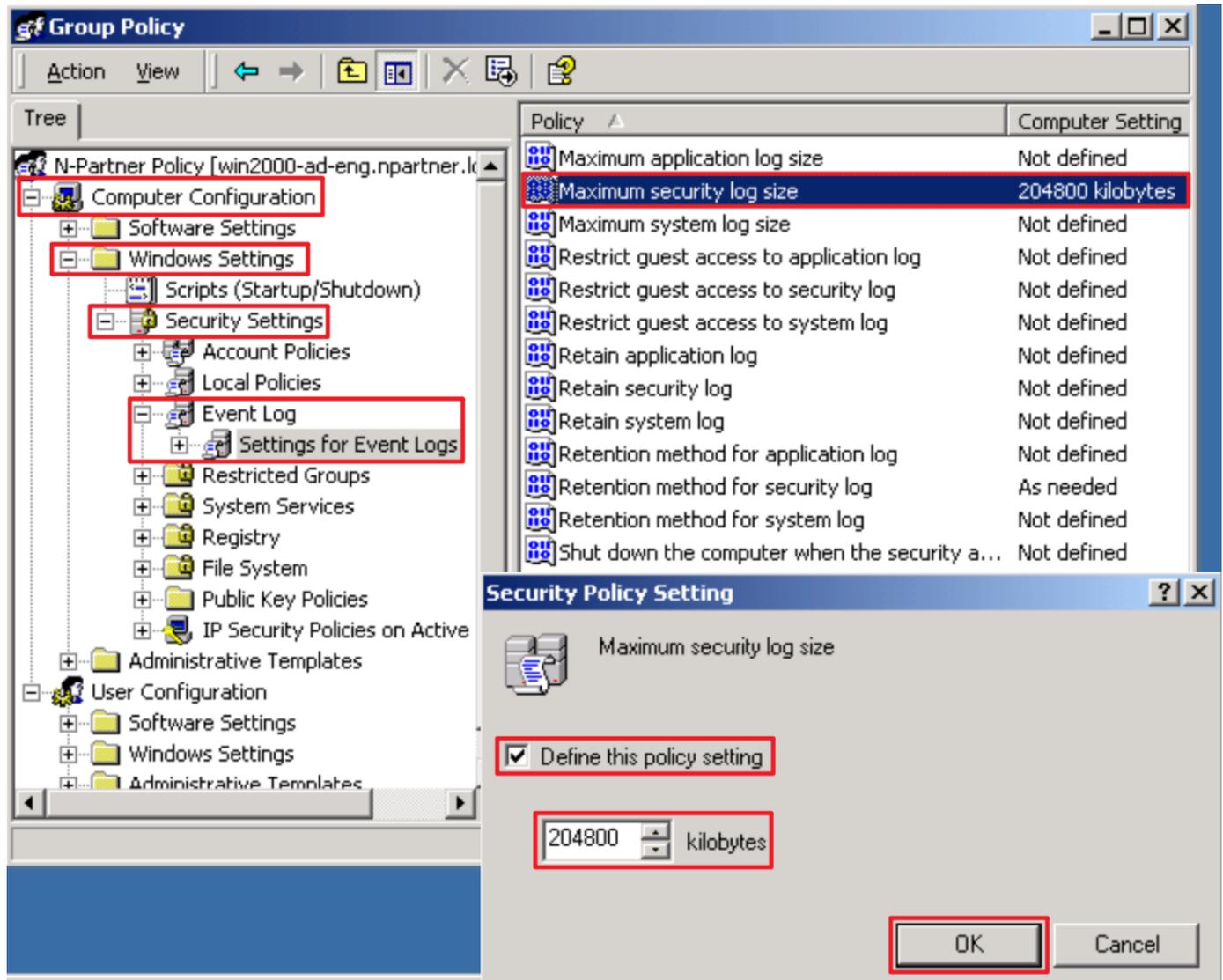
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

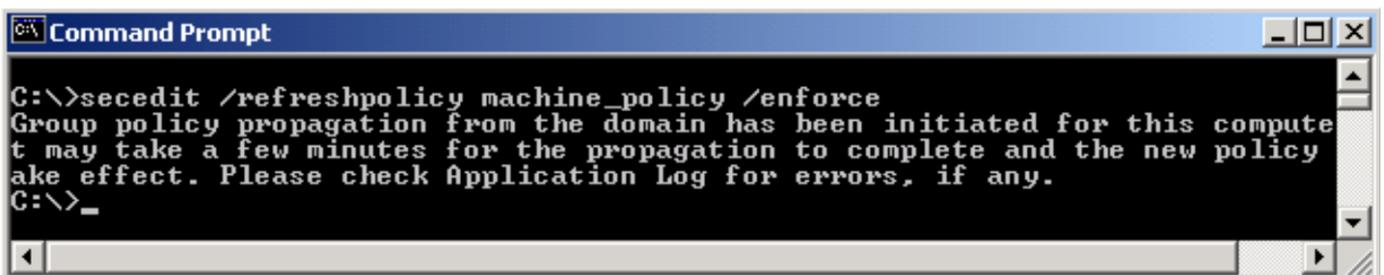


(8) On the Windows File server, open “Command Prompt.”



(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.

The screenshot shows the 'npartner Properties' dialog box with the 'General' tab selected. The 'Display name' field contains 'npartner', the 'Description' field contains 'Engineer', and the 'Office' field contains 'Taichung Office'. These three fields are enclosed in a red rectangular box. Other fields include 'First name' (npartner), 'Last name', 'Telephone number', 'E-mail', and 'Web page'. Buttons for 'Other...' are present next to the telephone and web page fields. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

The screenshot shows the 'npartner Properties' dialog box with the 'Organization' tab selected. The 'Department' field contains 'TAC' and is highlighted with a red rectangular box. Other fields include 'Title', 'Company', and 'Manager' (with a 'Name' sub-field). Buttons for 'Change...', 'View', and 'Clear' are located below the 'Manager' field. A 'Direct reports' list box is empty. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

(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.”

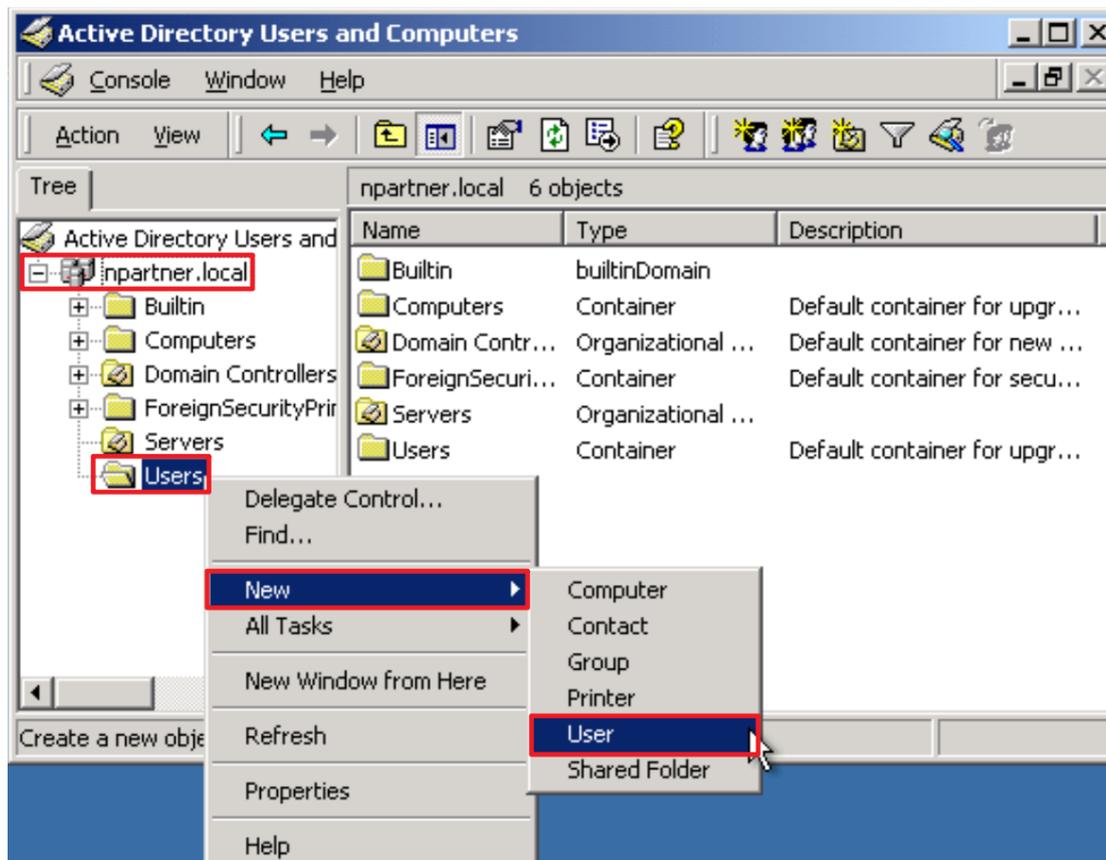


(2) Create an Account

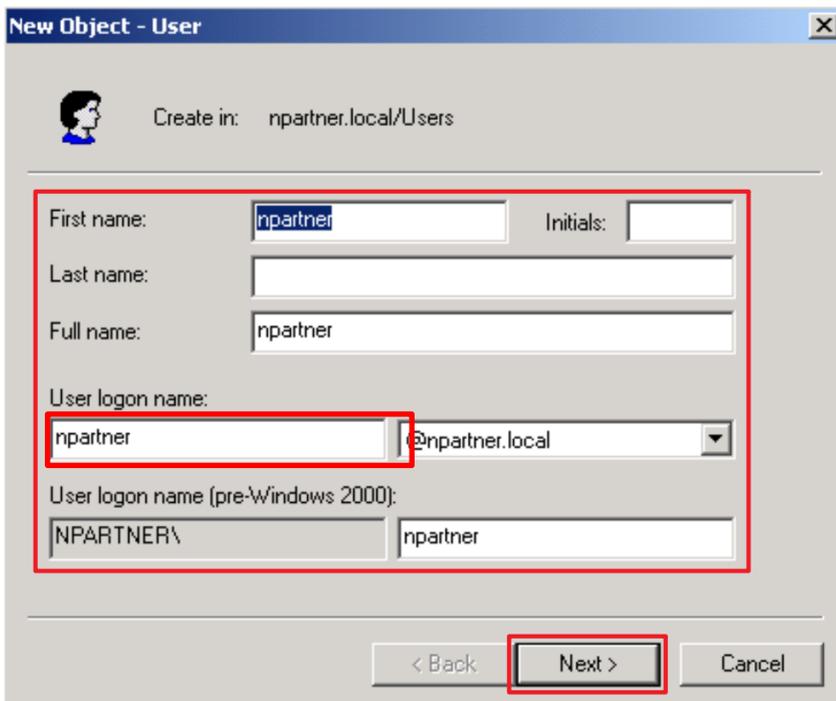
Expand “Domain Name” (the example here is [npartner.local](#)) → right-click the “Users” organizational unit

→ select “New” → select “User”

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

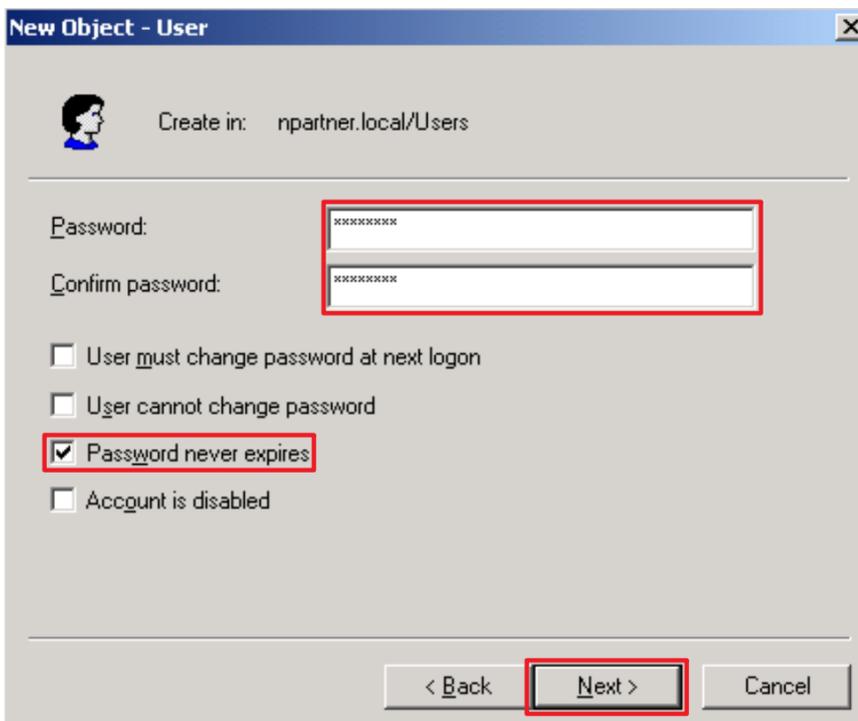


(3) Enter your **full name** (in this example, it is “npartner”) and **user logon name** (in this example, it is “npartner”), then click “Next.”



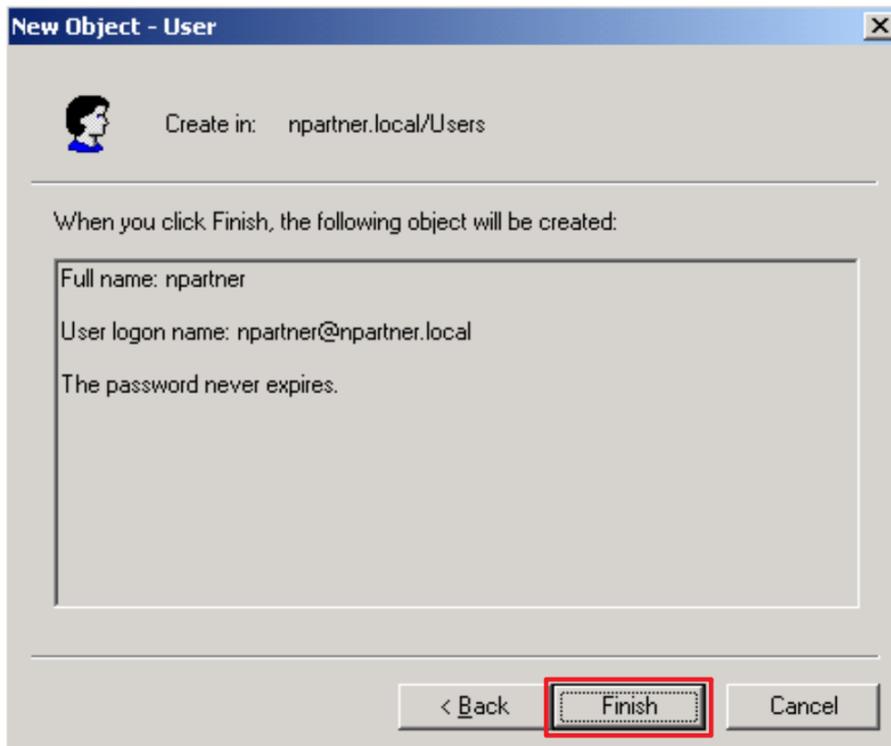
The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'npartner.local/Users'. The 'First name' field contains 'npartner', and the 'User logon name' field contains 'npartner'. The 'Next >' button is highlighted with a red box.

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



The screenshot shows the 'New Object - User' dialog box. The 'Password' and 'Confirm password' fields are filled with asterisks. The 'Password never expires' checkbox is checked. The 'Next >' button is highlighted with a red box.

(5) Click "Finish."



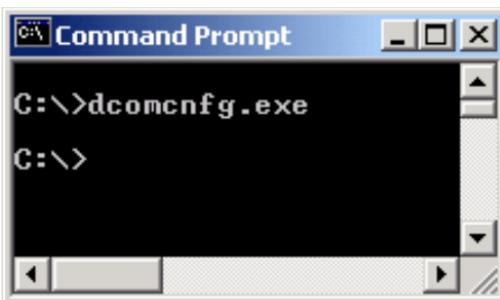
2.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”



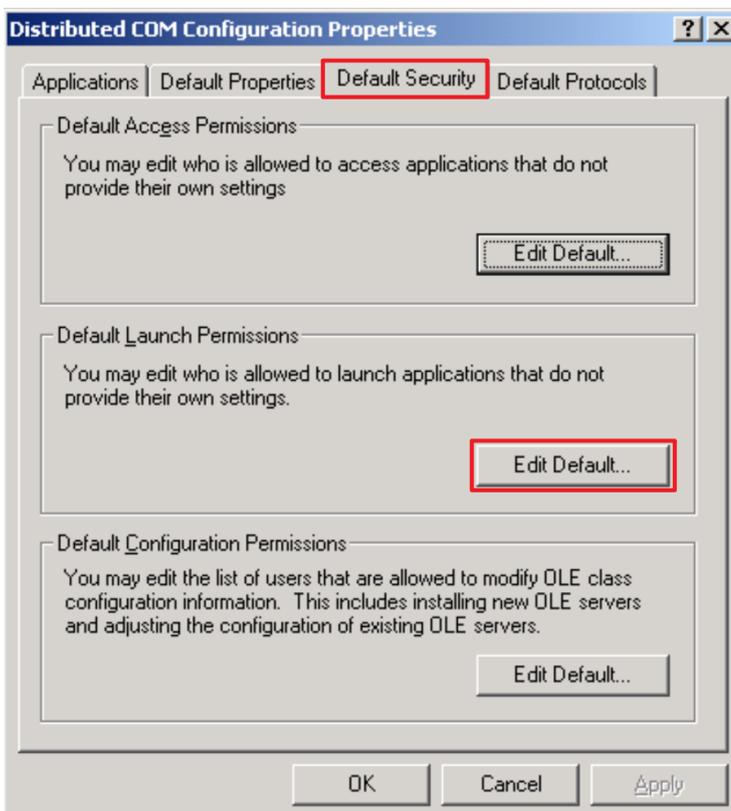
(2) Enter the command below to enable component services.

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



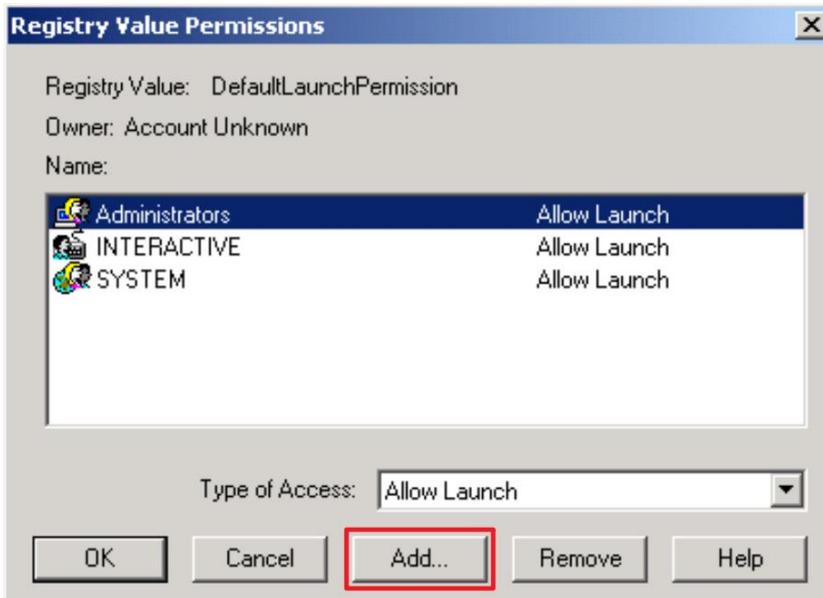
(3) Enable Default Access Permissions

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



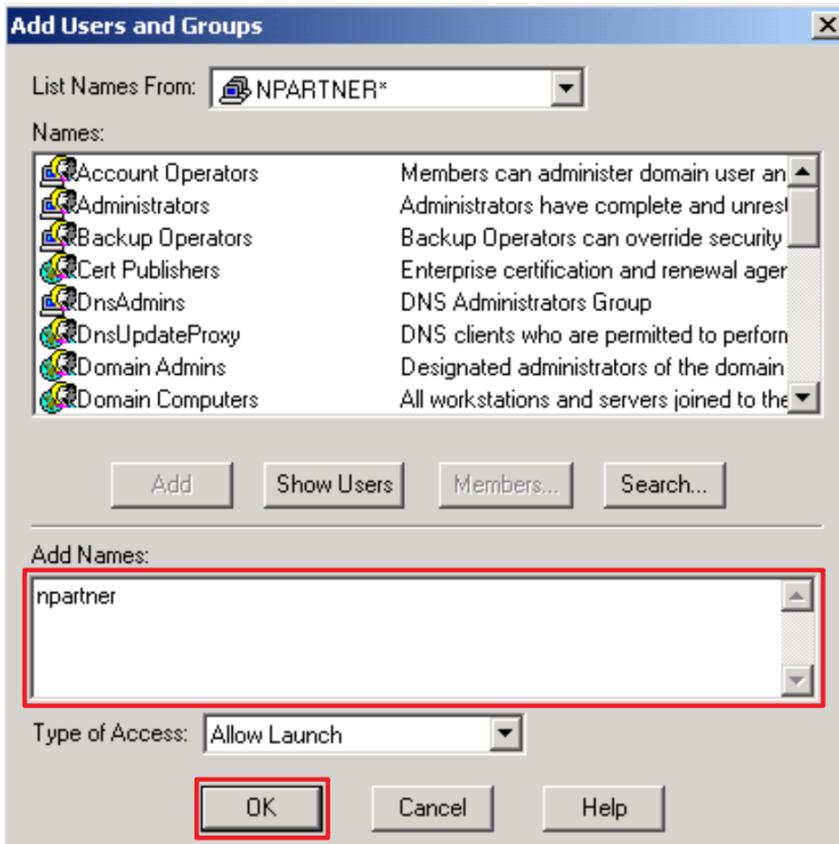
(4) Add User Permissions

Click “Add...”.

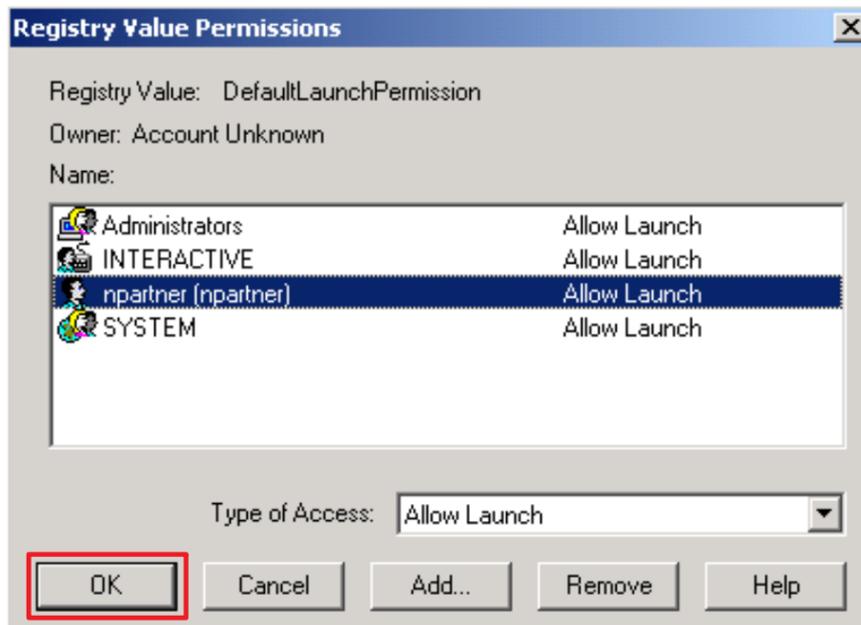


(5) Enter User

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

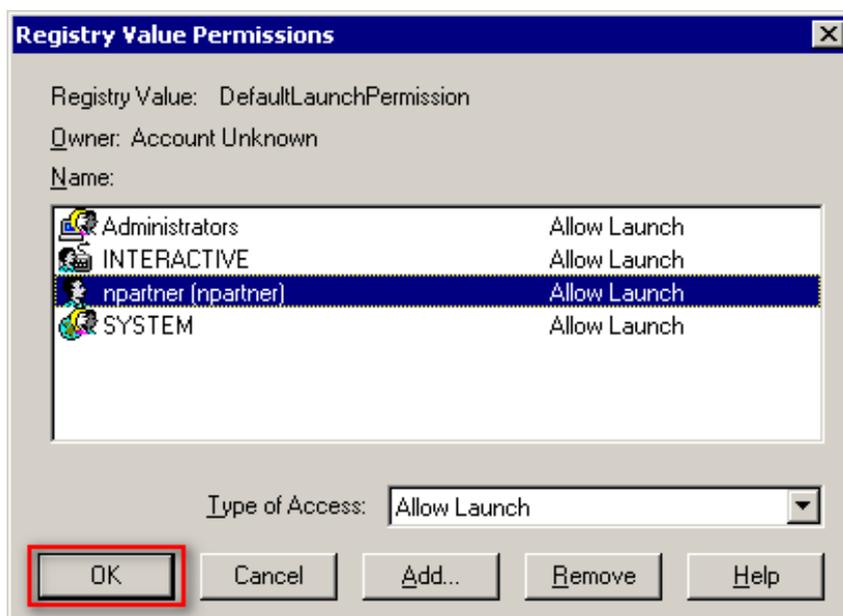


(6) Click "OK."

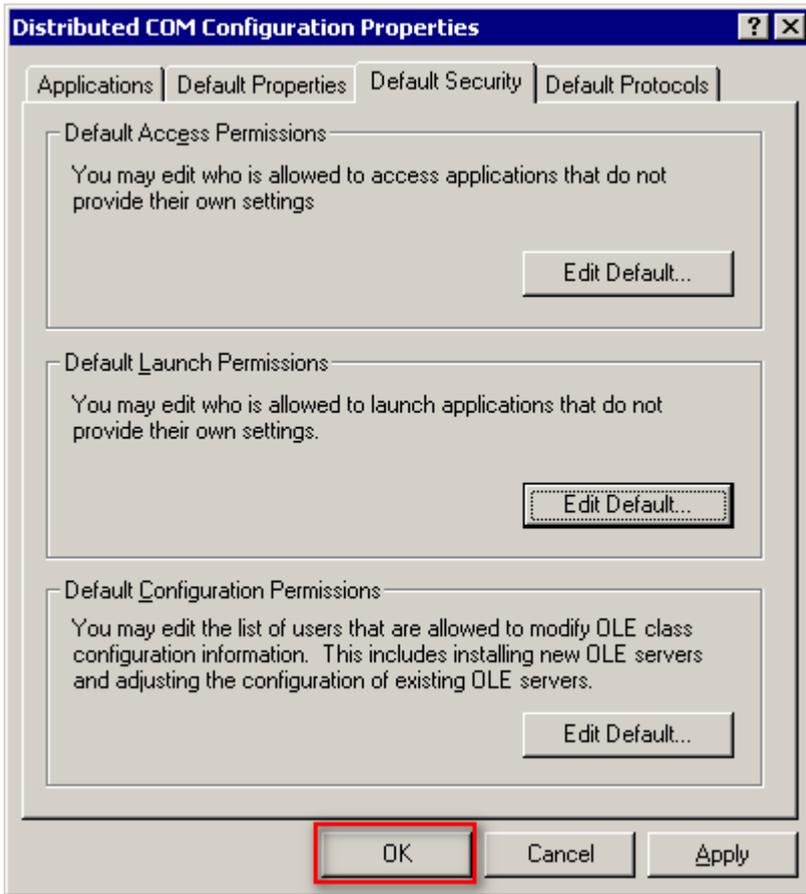


Select your user account (in this example, it is "npartner"), click "Add", set type of access to "Allow Launch," then click "OK."

(7) Click "OK."



(8) Click "OK."



2.3.3 Configure WMI Permissions

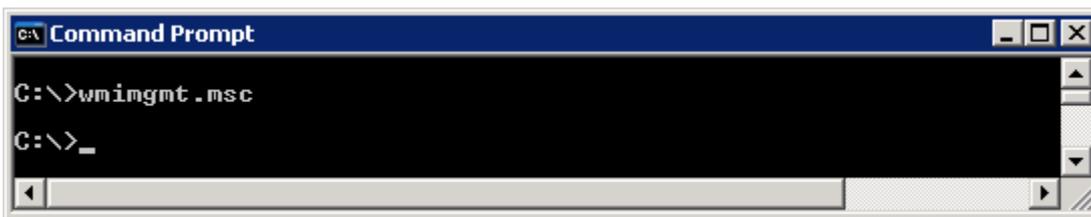
2.3.3.1 Configure Event Log Permissions

(1) Open "Command Prompt."



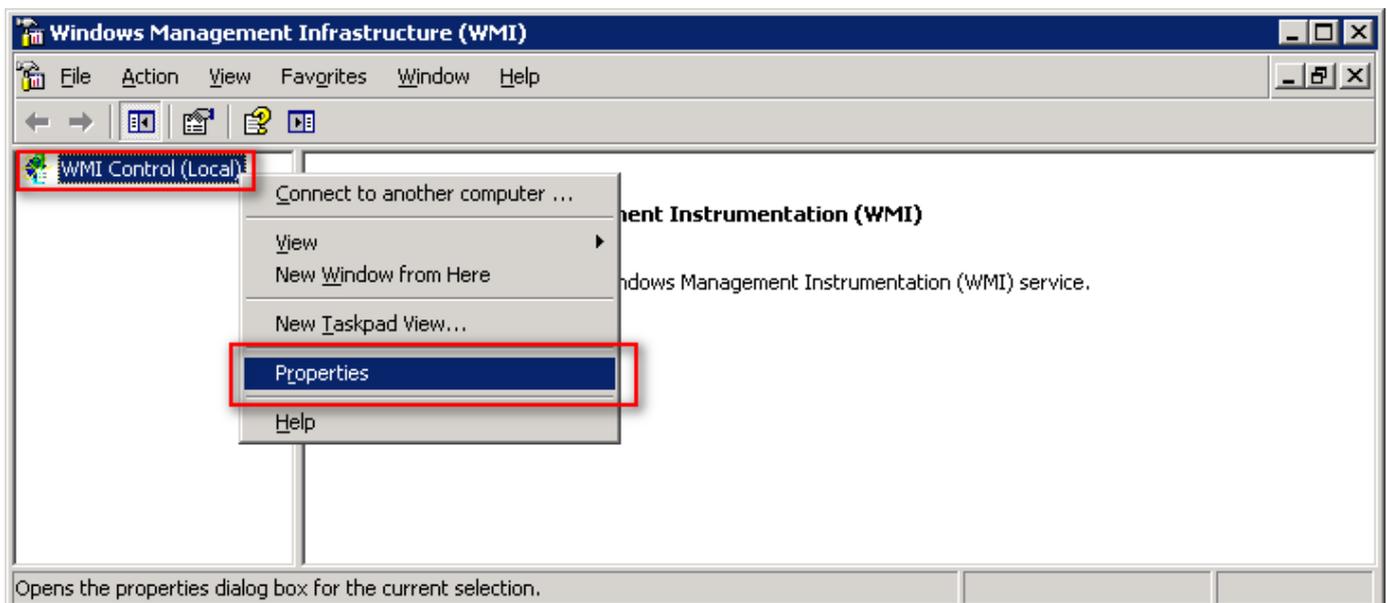
(2) Enter the command to enable WMI control service.

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



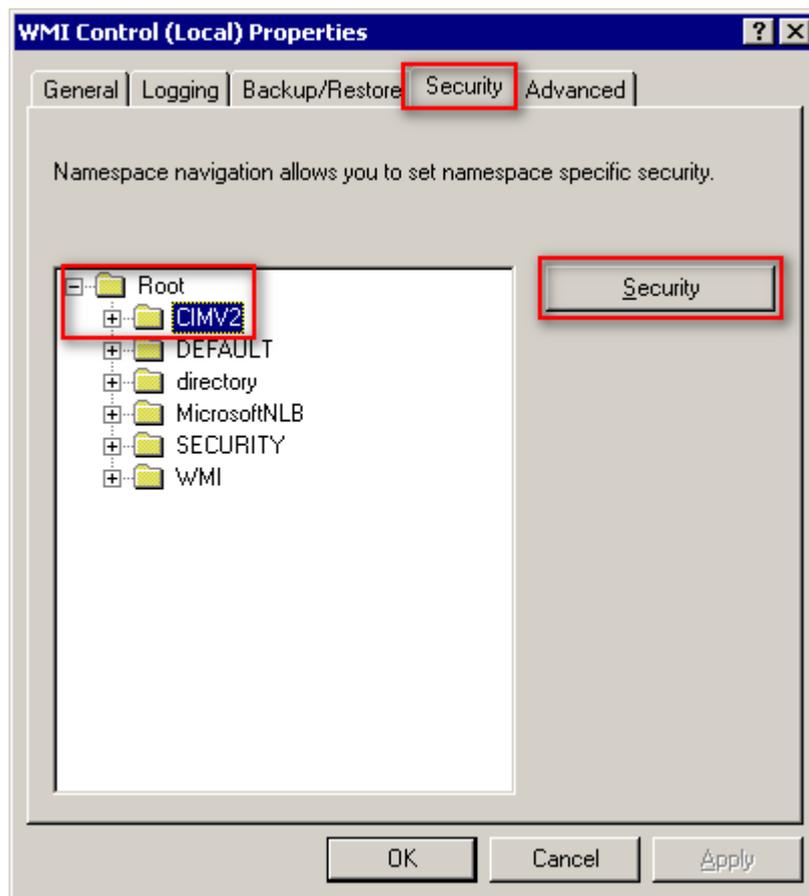
(3) Edit WMI Control

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



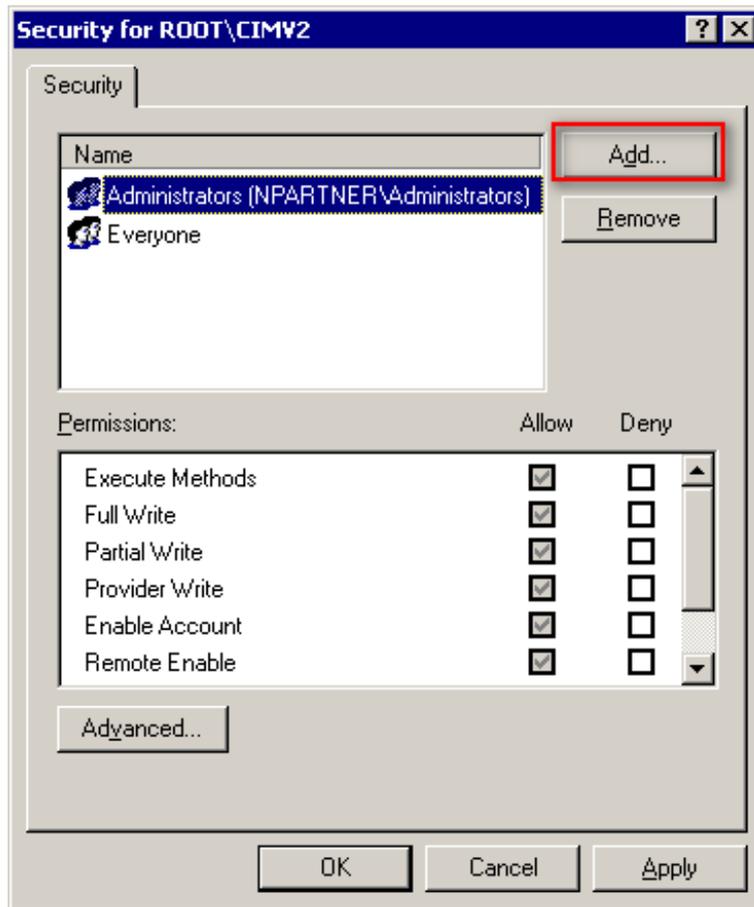
(4) Edit CIMV2 Security

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



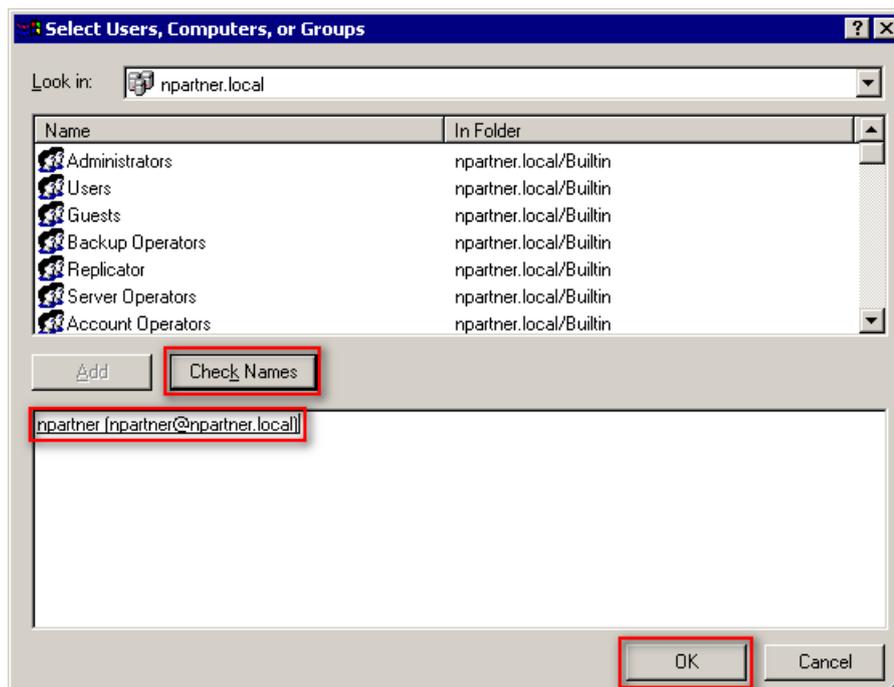
(5) Add WMI User Permissions.

Click “Add.”



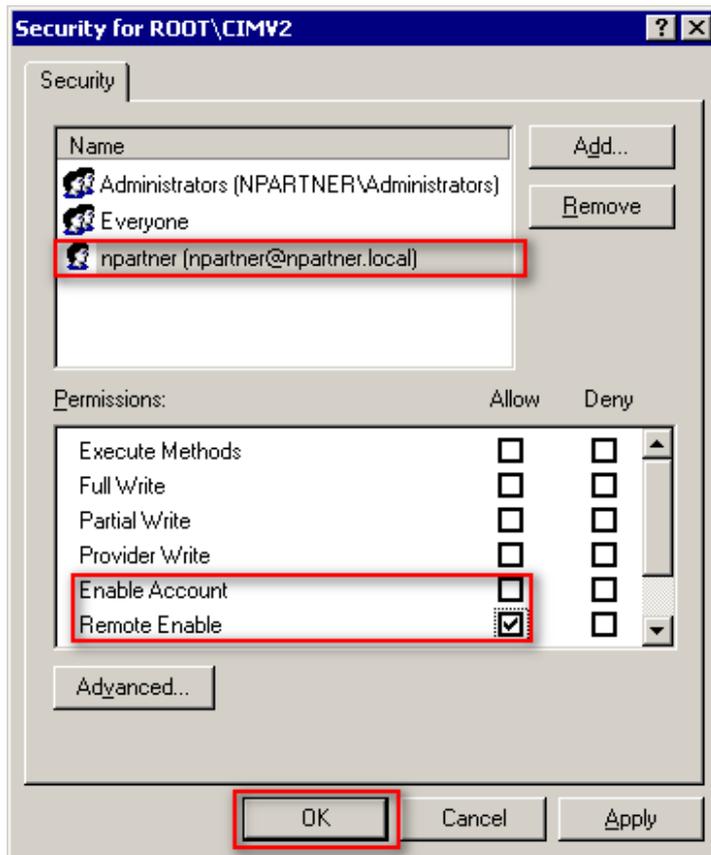
(6) Enter Your Username

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

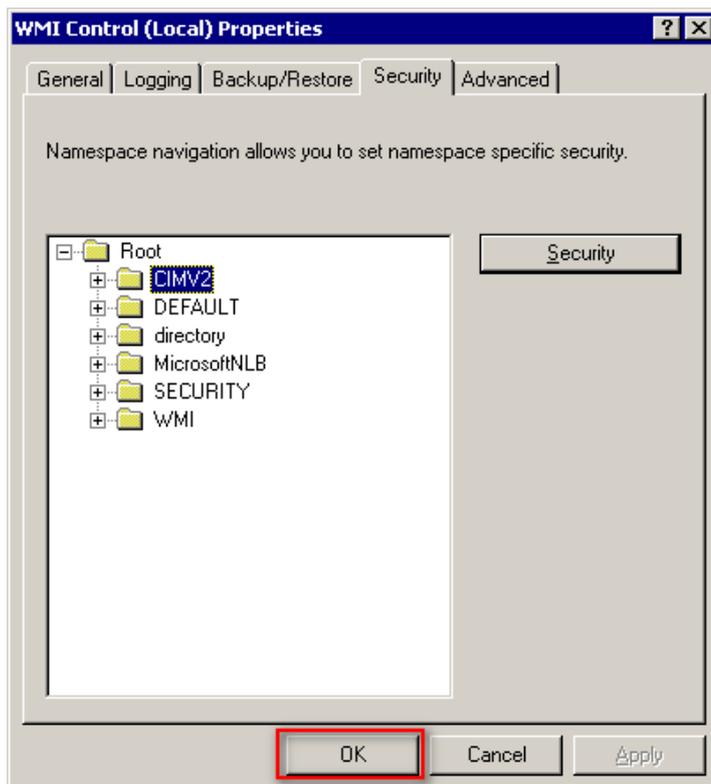


(7) Set Your User Permissions

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



(8) Click “OK.”



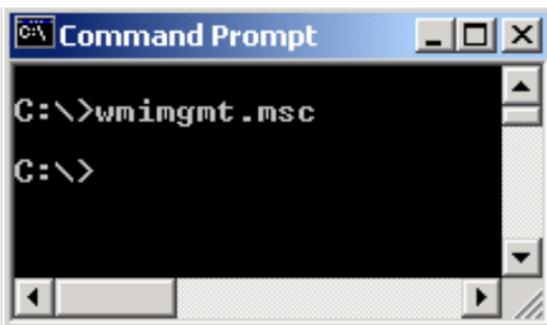
2.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”



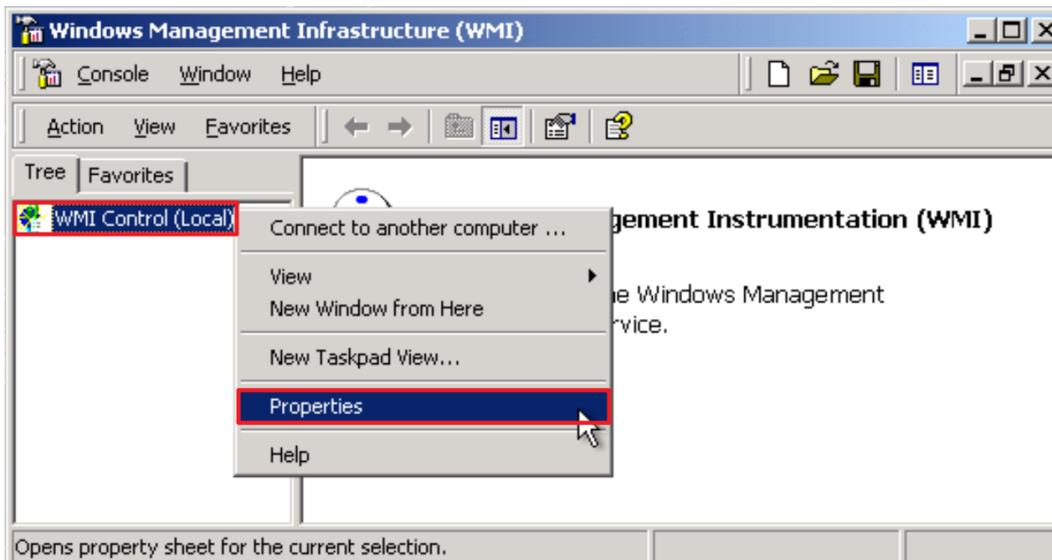
(2) Enter the command below to enable WMI Control.

```
C:\> wmicmt .msc
```



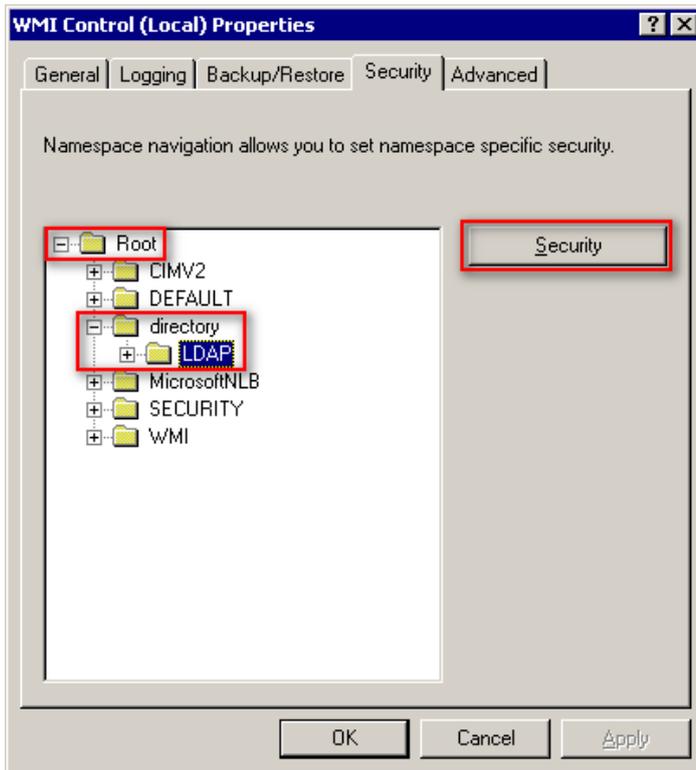
(3) Edit WMI Control

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



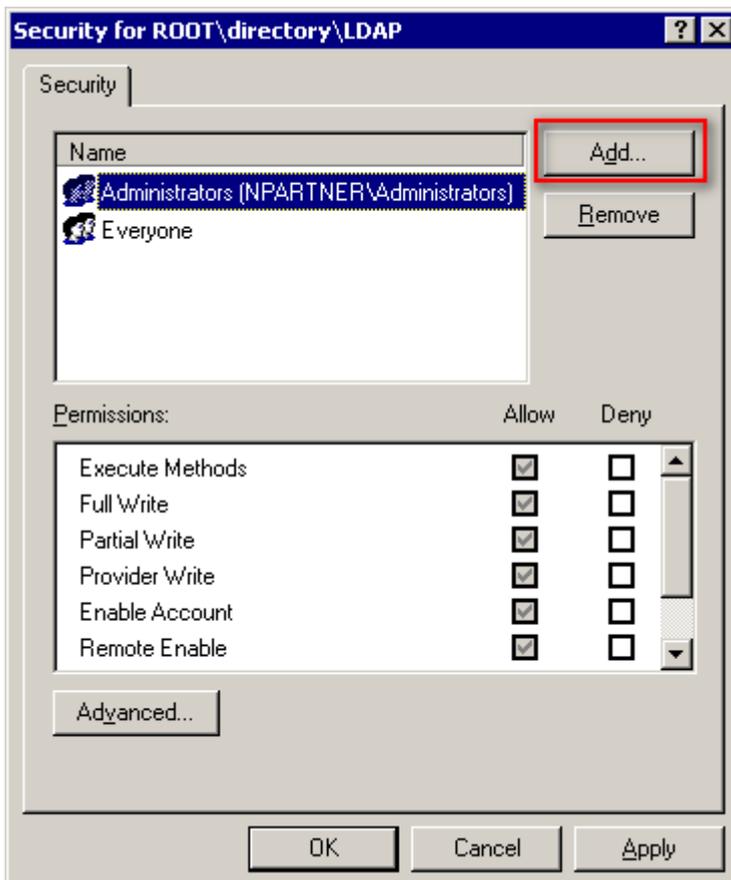
(4) Edit LDAP Security

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



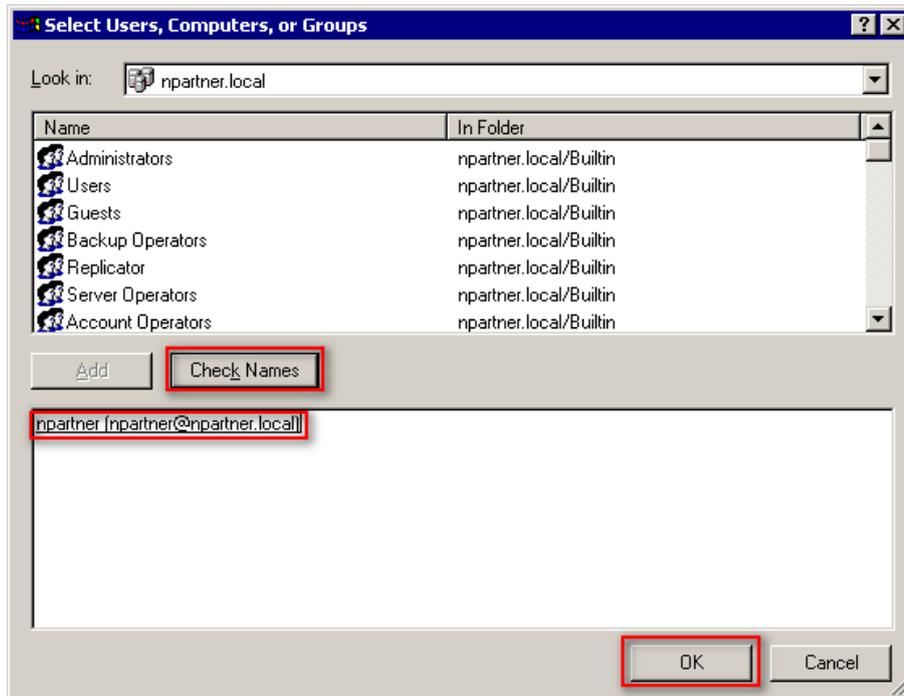
(5) Add WMI User Permissions

Click "Add."



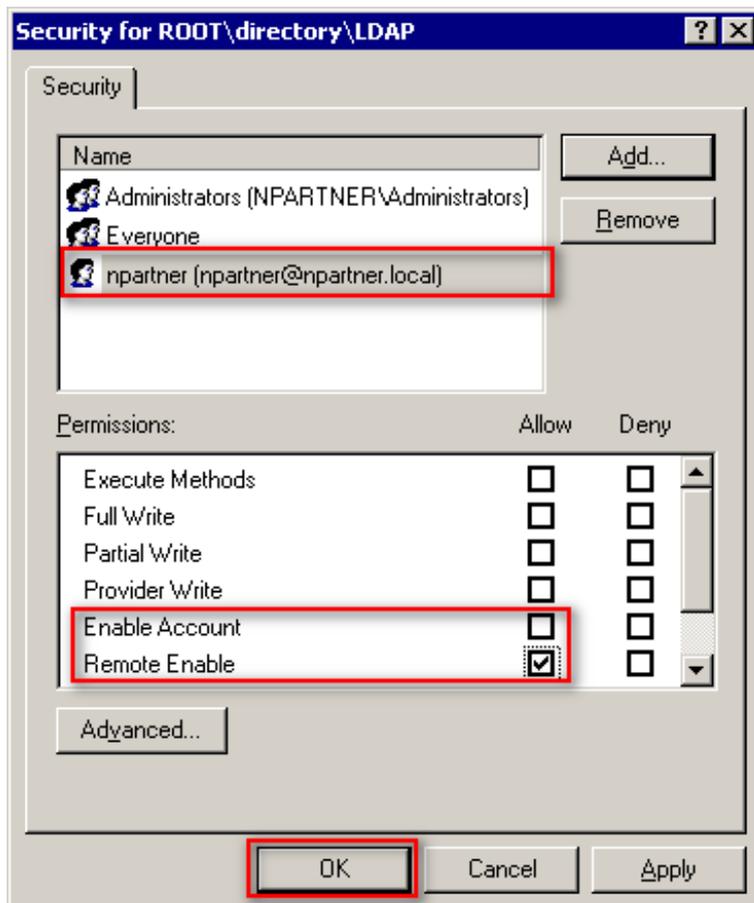
(6) Enter Your Username

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

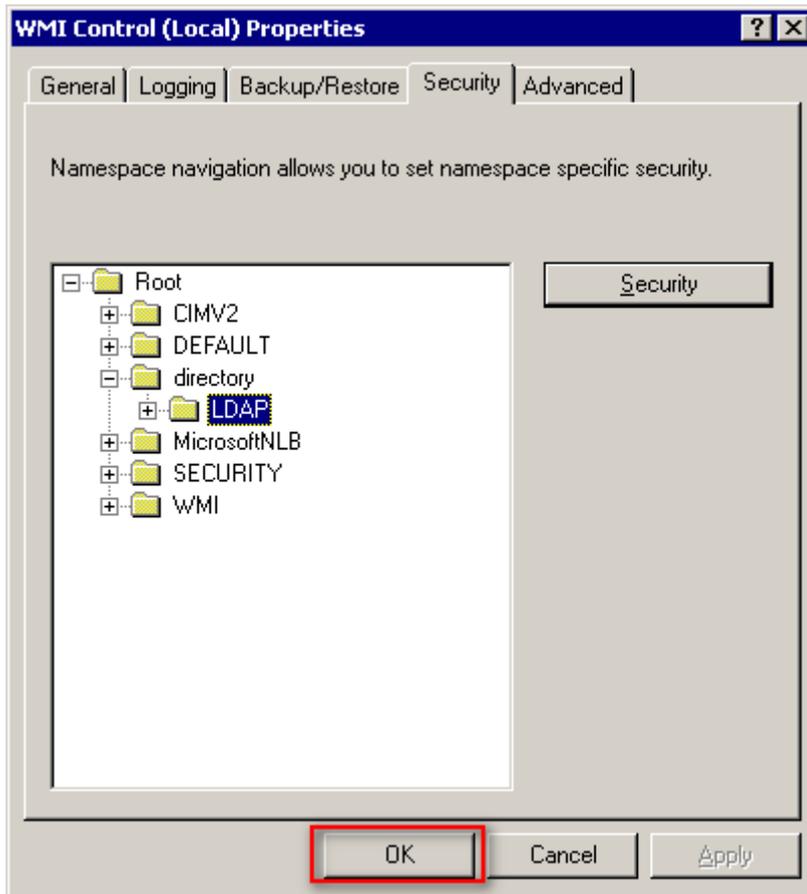


(7) Set Your User Permissions

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

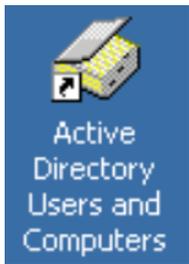


(8) Click "OK."

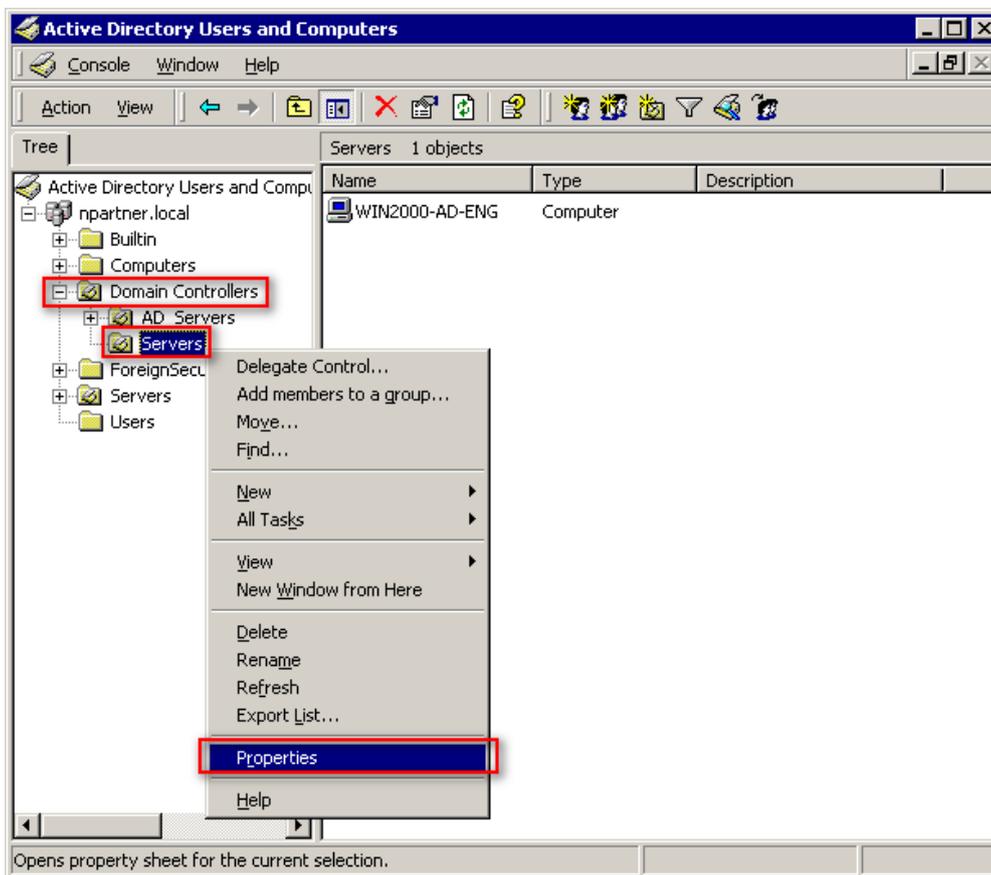


2.3.4 Configure Event Log Read Permissions

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

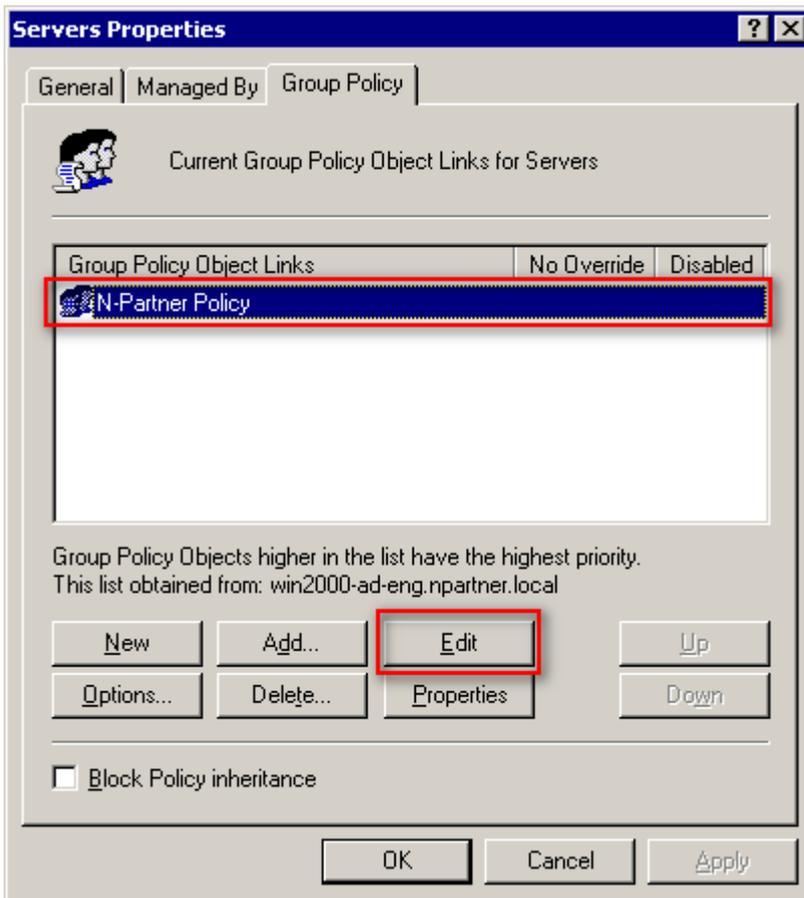


(2) Right-click the “Servers” organizational unit of “Domain Controllers,” and select “Properties.”



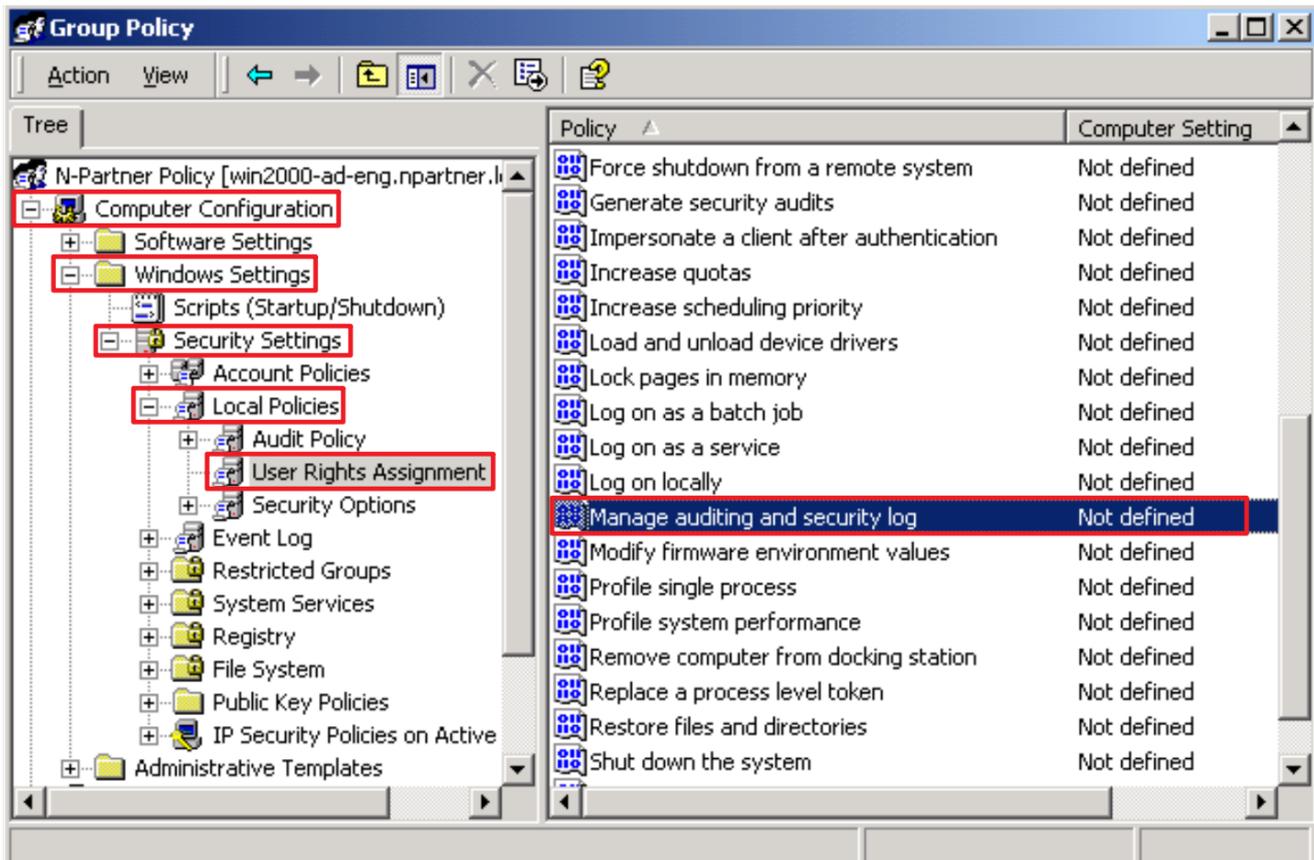
(3) Edit Group Policy Object

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.”



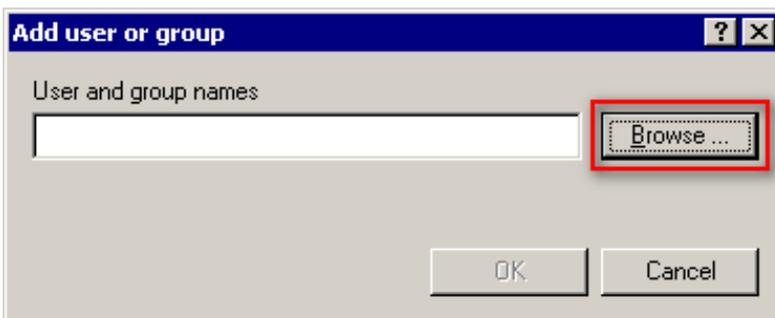
(5) Add Auditing User

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



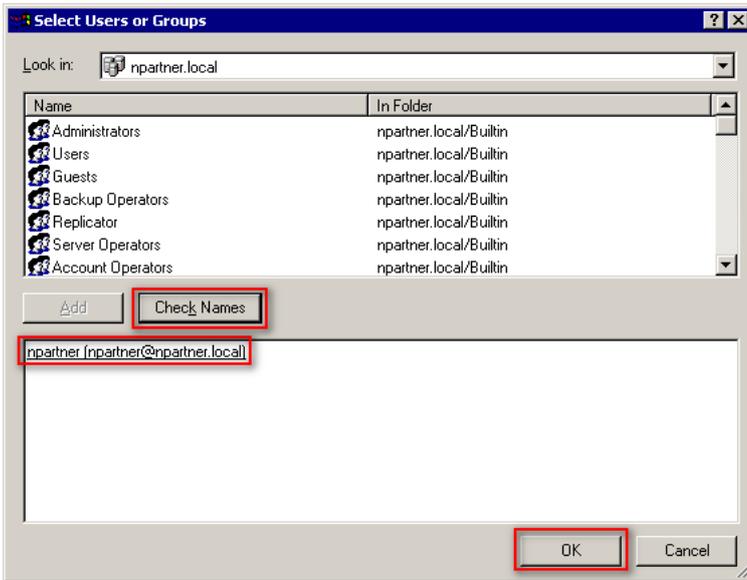
(6) Search for User

Click “Browse.”

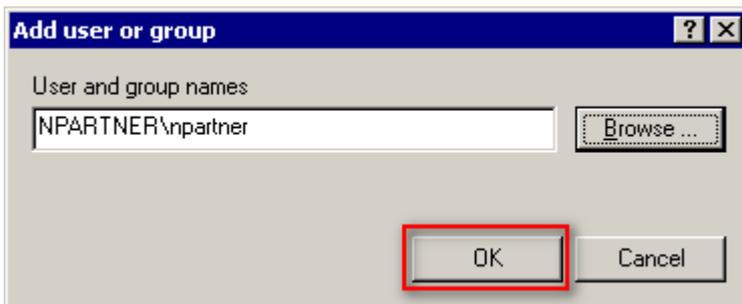


(7) Enter Your User Account

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.”

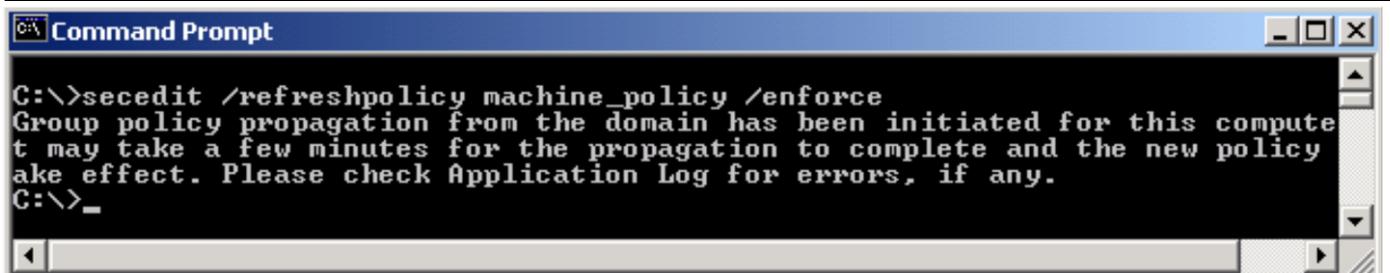


(10) Open "Command Prompt."



(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
```

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

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

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

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

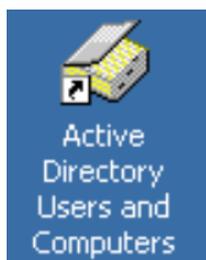
3. Windows Server 2003

Windows Audit Policy Configuration:

For detailed information, refer to the [Audit Policy Recommendations link](#) in the references.

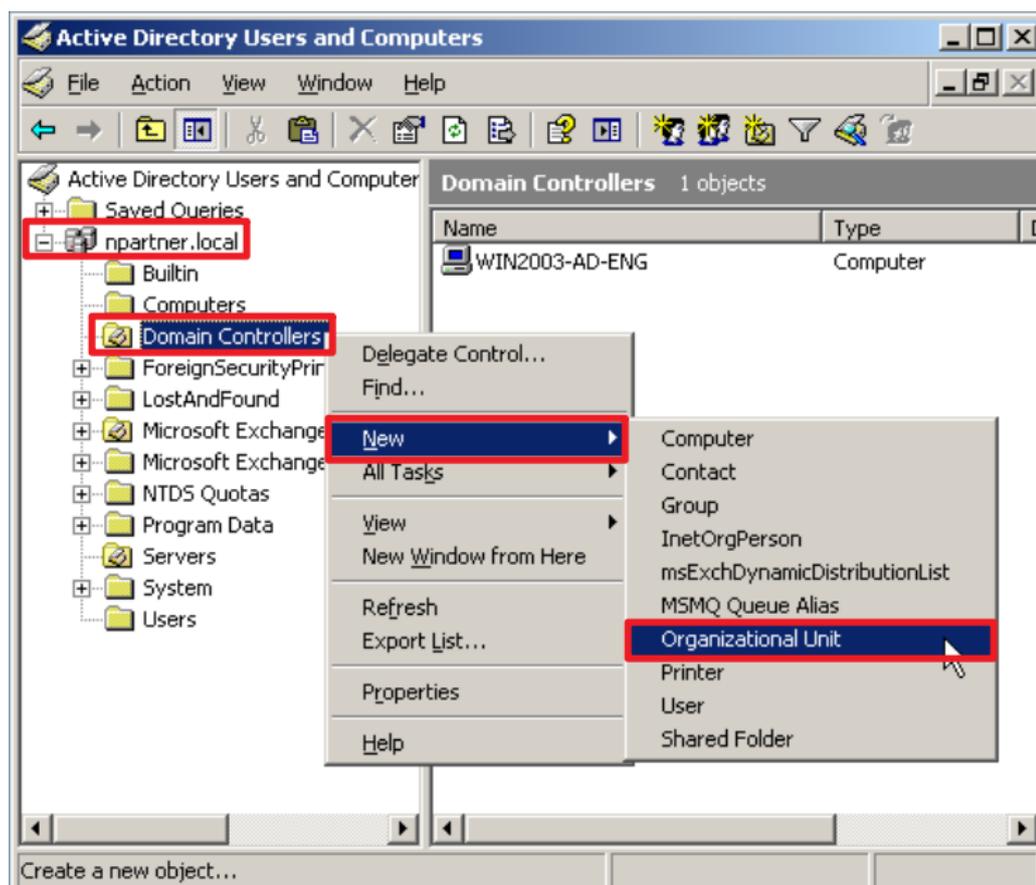
3.1 Organizational Unit (OU) Configuration

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



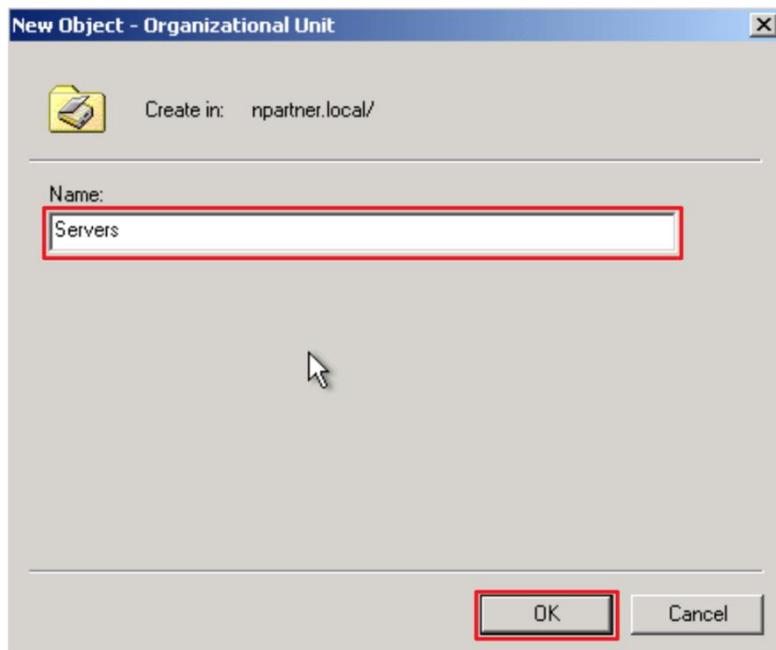
(2) Add an Organizational Unit

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



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

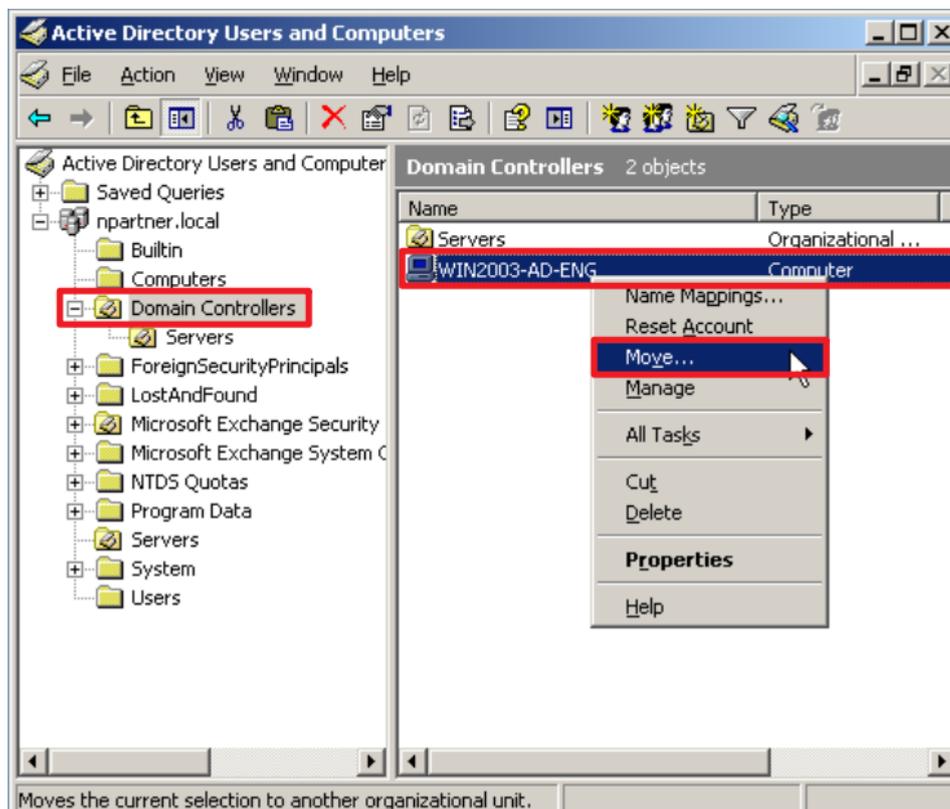
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

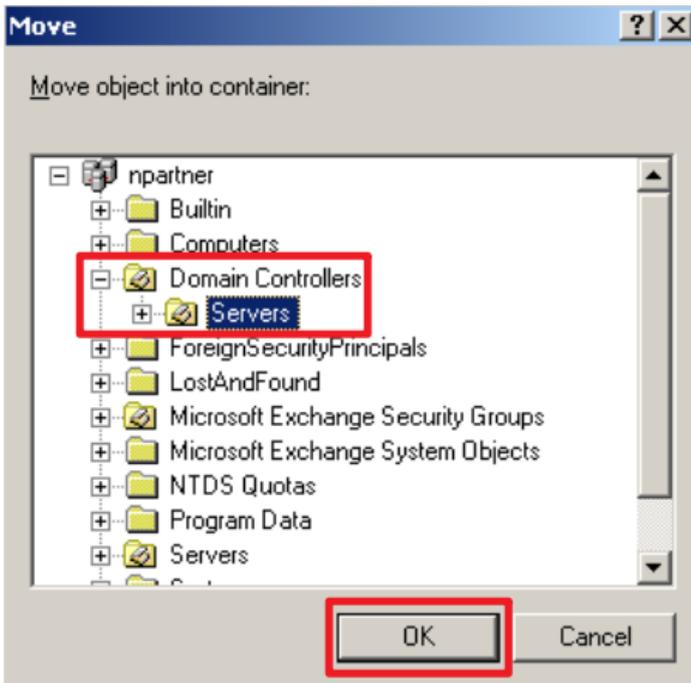
Select “Domain Controllers” → right-click on the “WIN2003-AD-ENG” server.

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



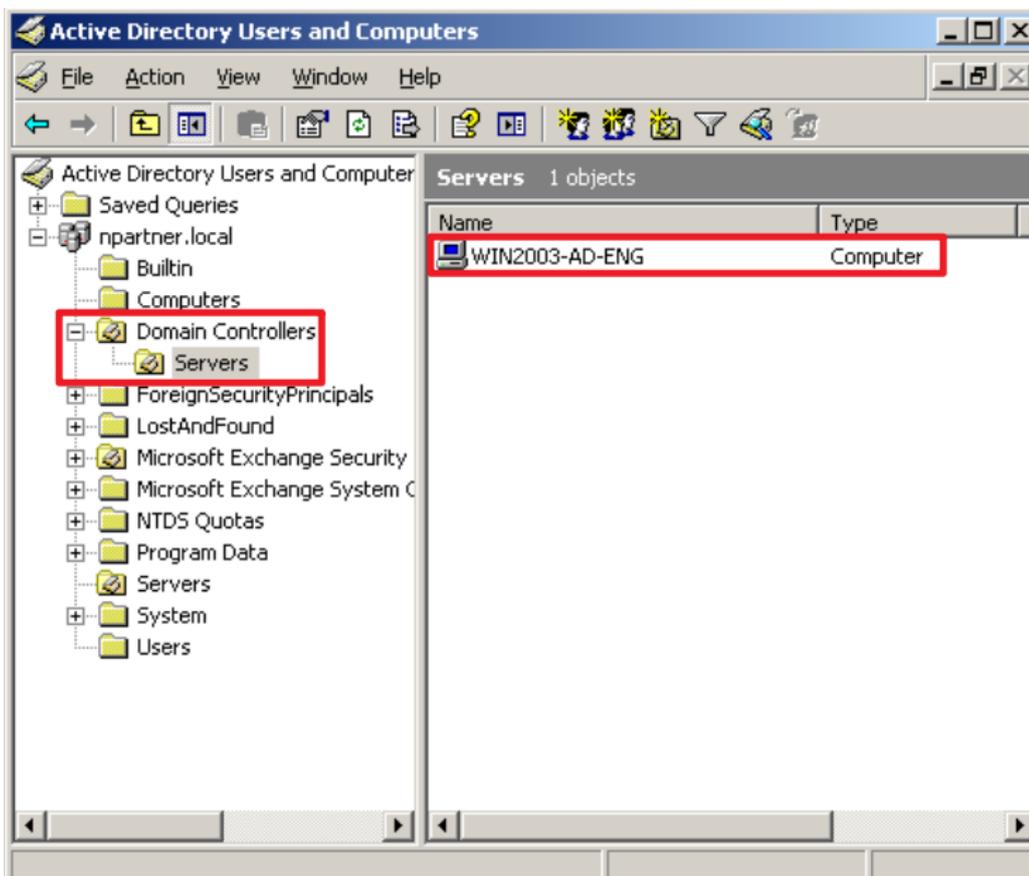
(5) Select your Organizational Unit:

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



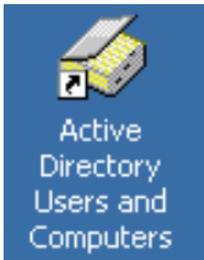
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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.

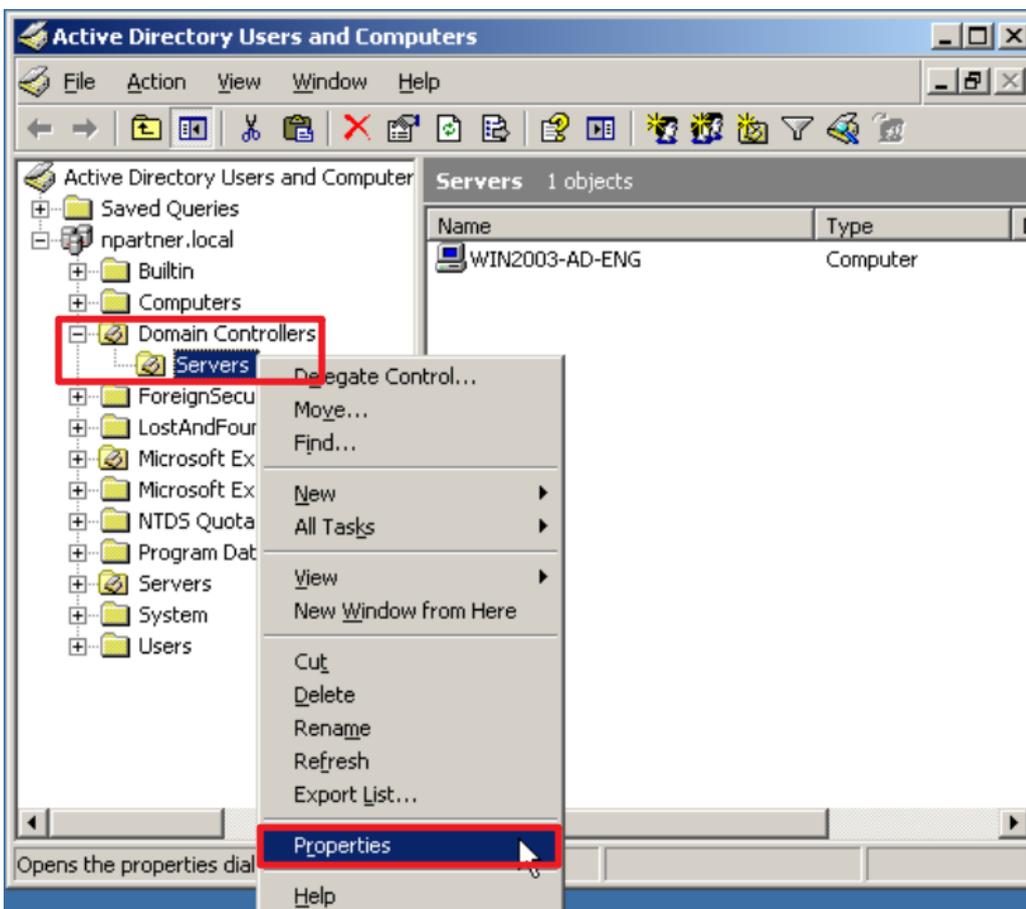


3.2 Group Policy Settings

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

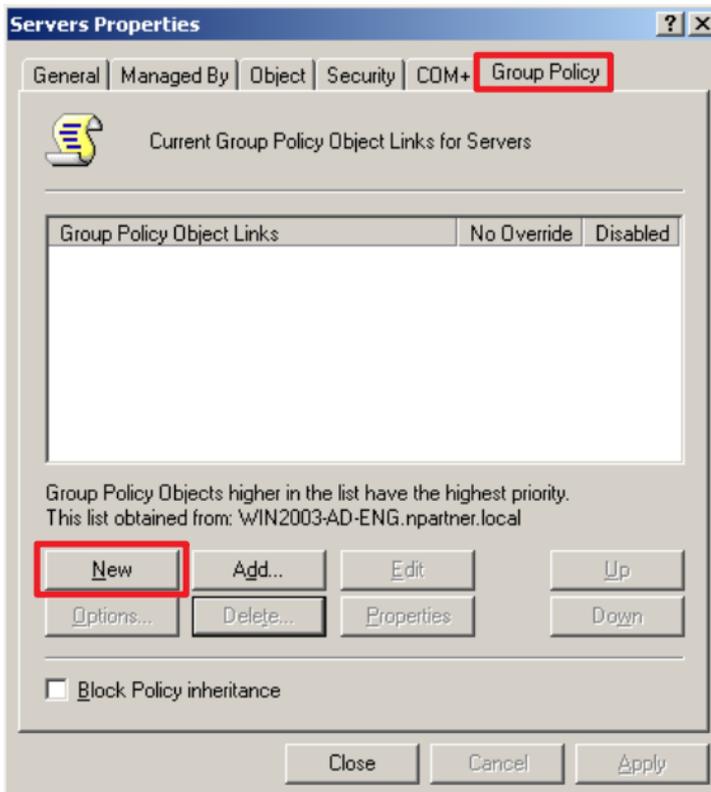


(2) In the “Servers” organizational unit (OU), right-click and select “Properties.”



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

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

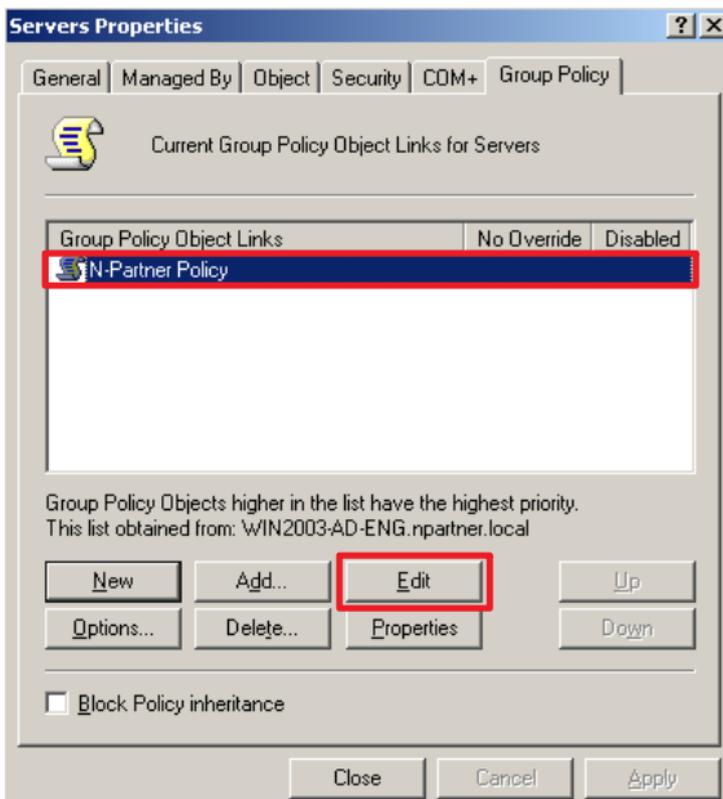


(4) Edit your Group Policy Object

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

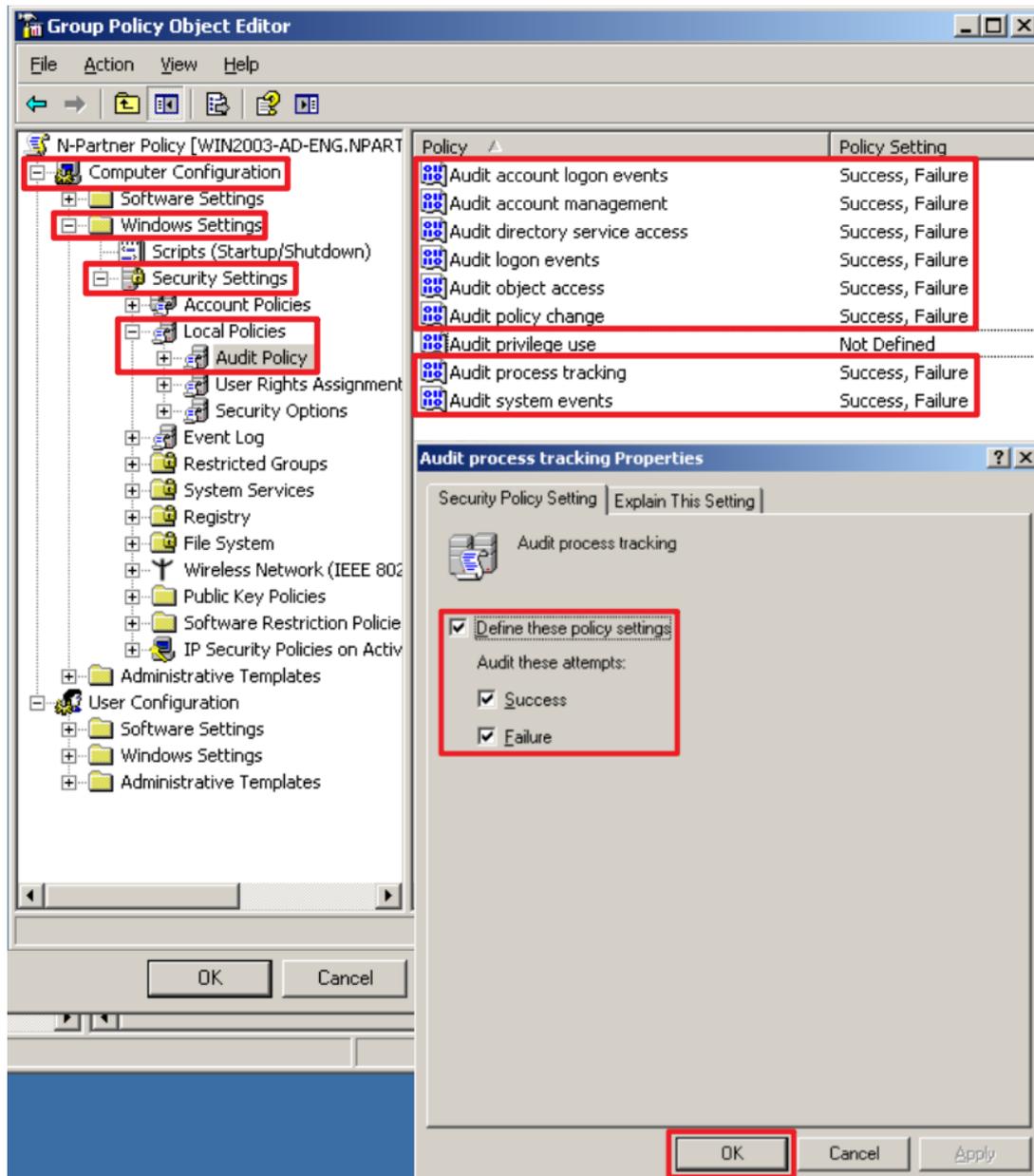
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



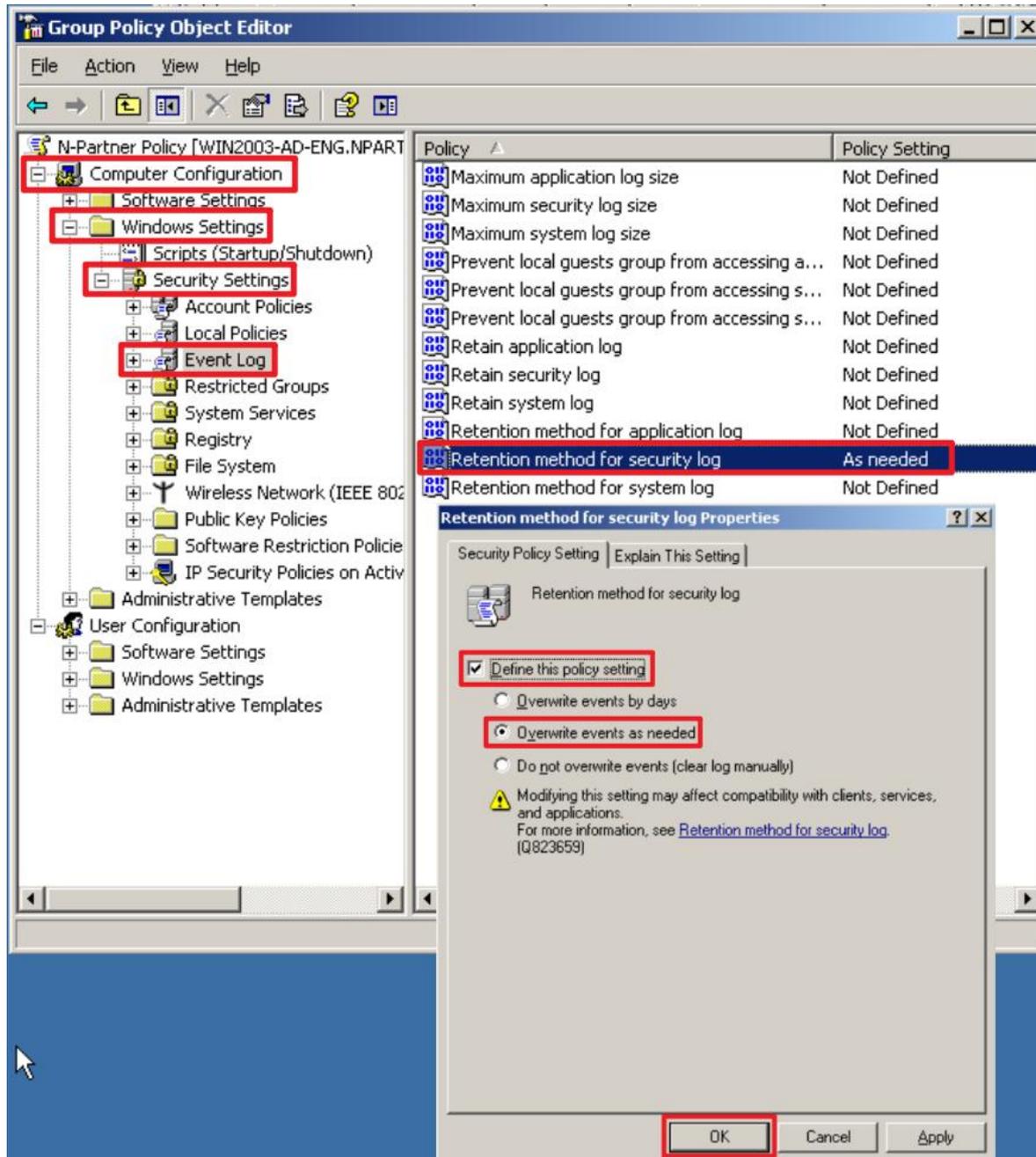
(5) Local Group Policies: Audit Policy

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

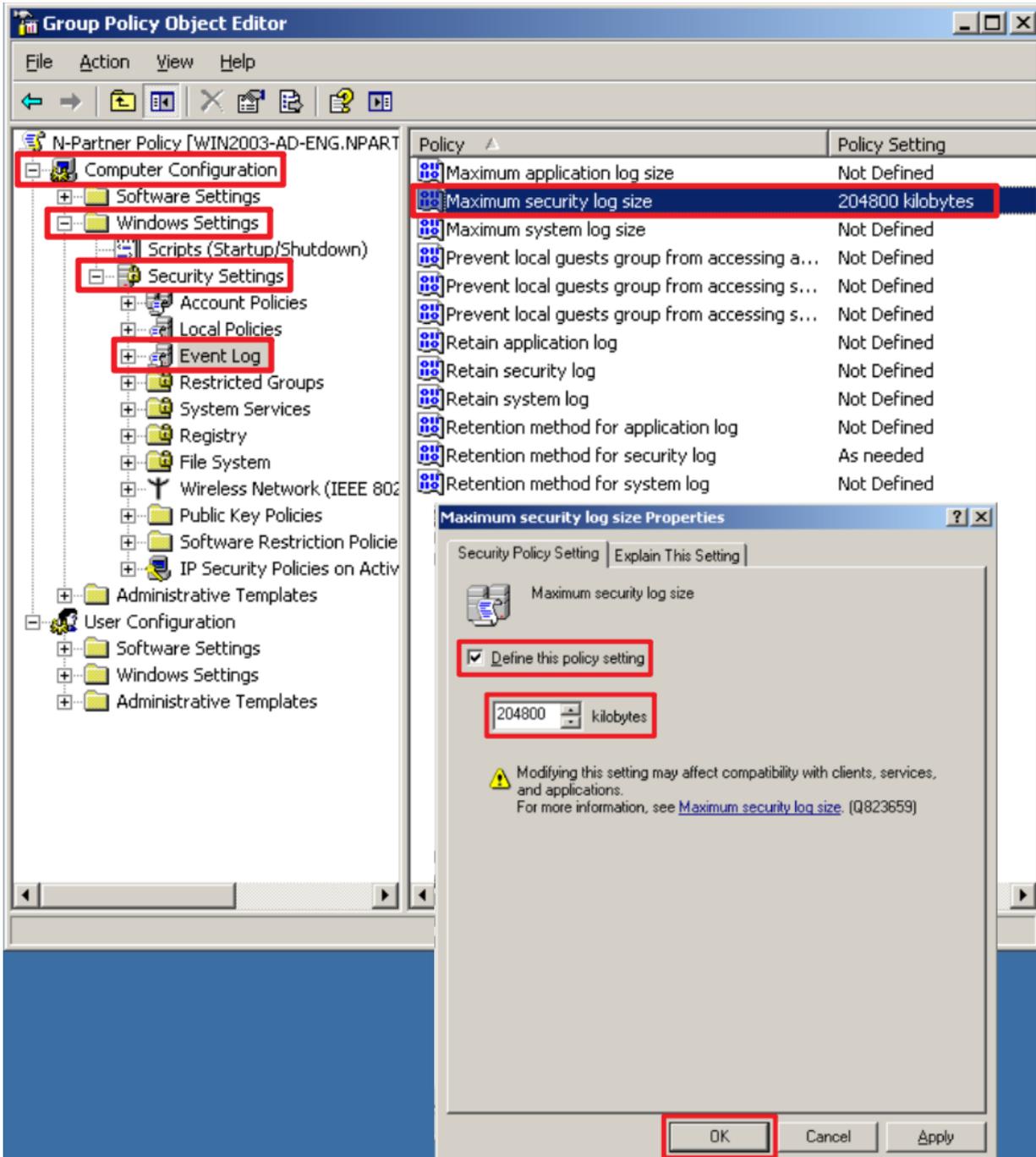
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

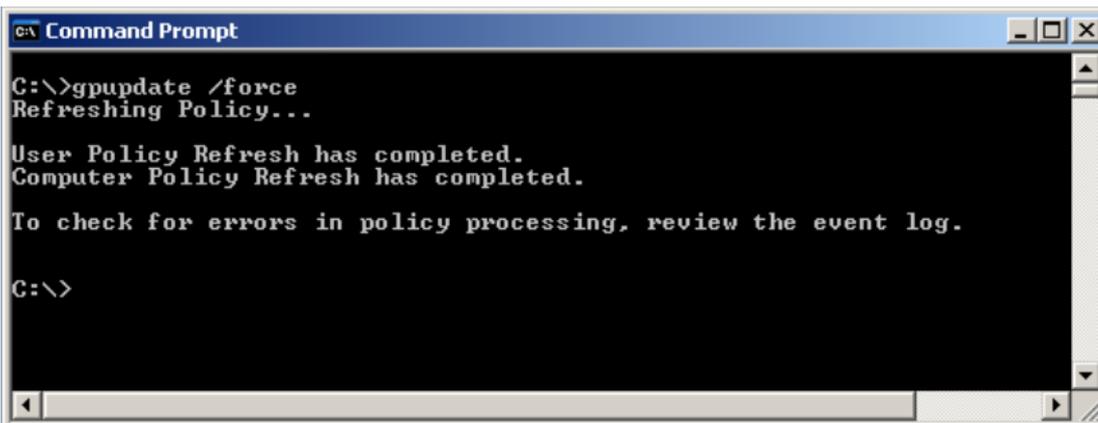


(8) On the Windows File server, open “Command Prompt.”



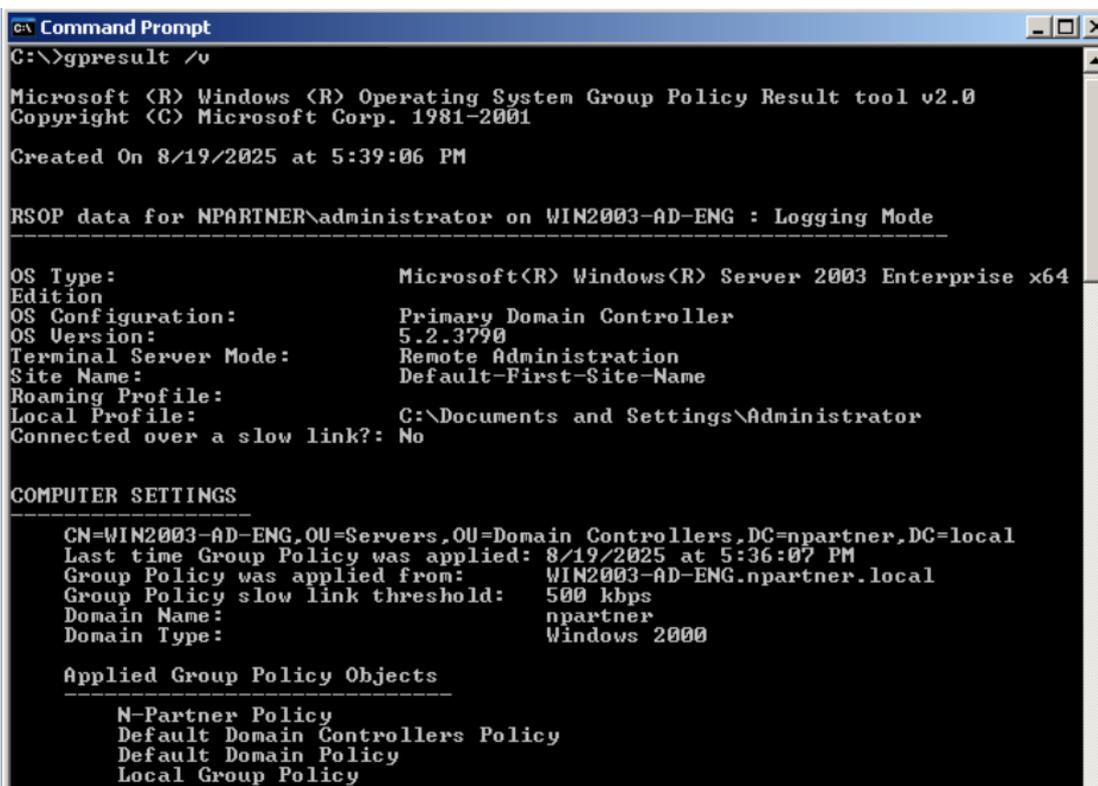
(9) Enter the command below to refresh group policy.

```
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.

The screenshot shows the 'KH Properties' dialog box with the 'General' tab selected. The 'Display name' field contains 'KH', the 'Description' field contains 'Engineer', and the 'Office' field contains 'Taichung Office'. These three fields are enclosed in a red rectangular box. Other visible fields include 'First name', 'Initials', 'Last name', 'Telephone number', 'E-mail', and 'Web page'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

The screenshot shows the 'KH Properties' dialog box with the 'Organization' tab selected. The 'Department' field contains 'TAC' and is highlighted with a red rectangular box. Other visible fields include 'Title', 'Company', and 'Manager' (with sub-fields for 'Name' and buttons for 'Change...', 'Properties', and 'Clear'). The 'Direct reports' section is empty. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

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

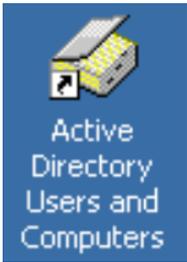
Severity	Event	Hit Count	Event Type	Src Username	Dst Username	Policy ID	Audit User	Category
● Notice	4724 An attempt was made to reset an accounts password (An attempt was made to reset an account's password) (User password changed) (npartner)	1	audit	Administrator ⓘ	npartner ⓘ	4724	Administrator	User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

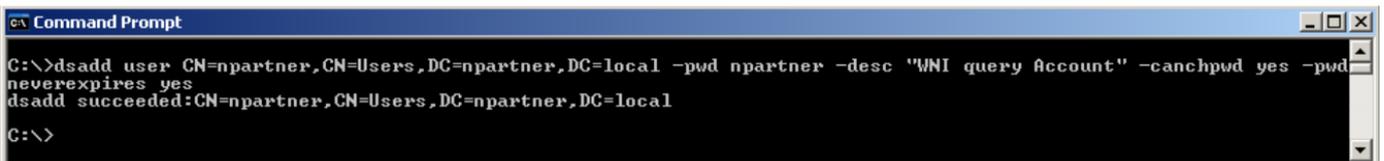
(1) Open "Active Directory Users and Computers."



(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
```

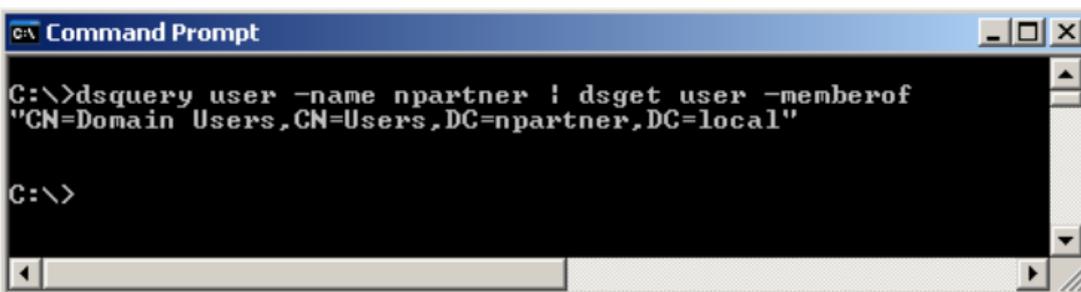


```
Command Prompt
C:\>dsadd user CN=npartner,CN=Users,DC=npartner,DC=local -pwd npartner -desc "WMI query Account" -canchpwd yes -pwdneverexpires yes
dsadd succeeded:CN=npartner,CN=Users,DC=npartner,DC=local
C:\>
```

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
```



```
Command Prompt
C:\>dsquery user -name npartner | dsget user -memberof
"CN=Domain Users,CN=Users,DC=npartner,DC=local"
C:\>
```

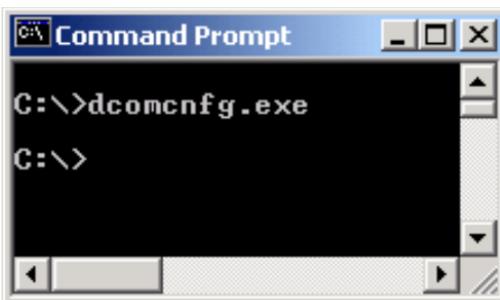
3.3.2 Configure DCOM Permissions

(1) Open “Command Prompt.”



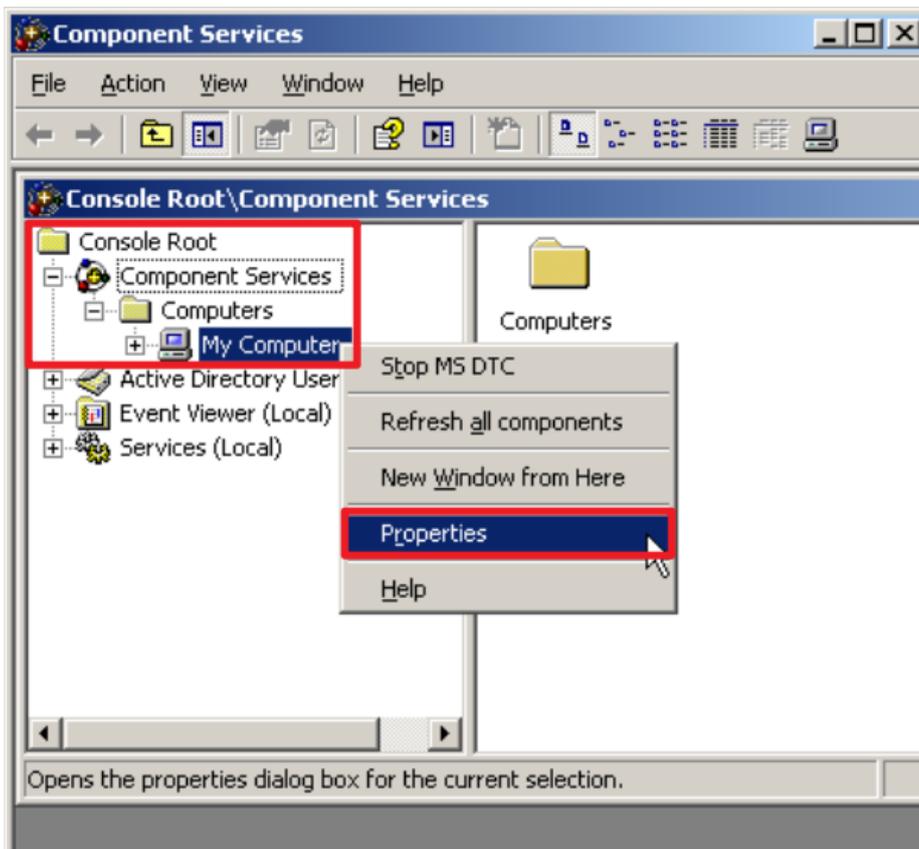
(2) Enter the command below to enable component services.

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



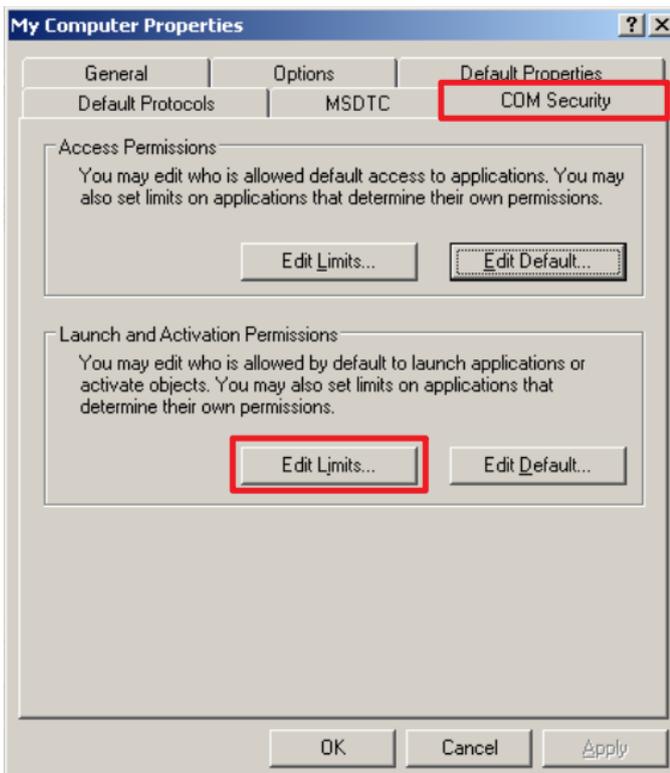
(3) Edit Computer Properties

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



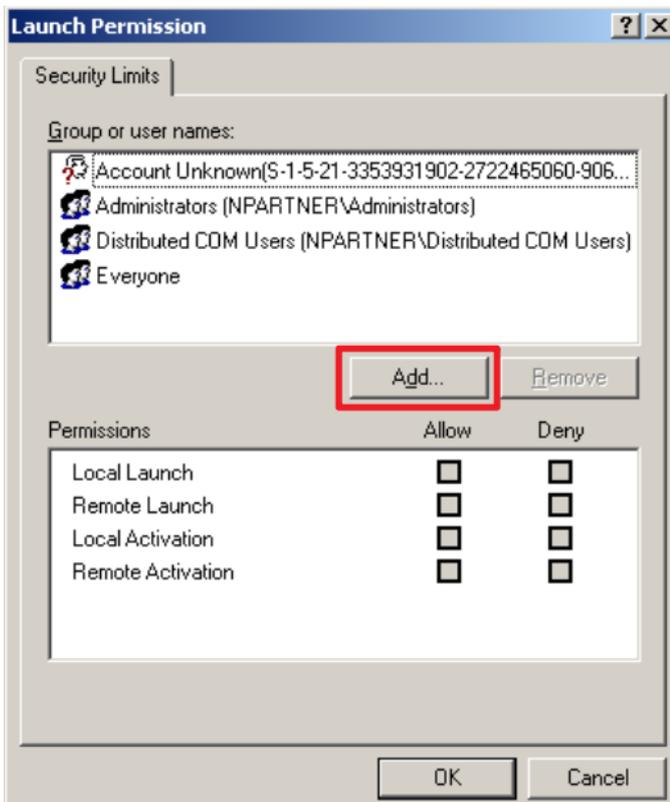
(4) Enable Permissions

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



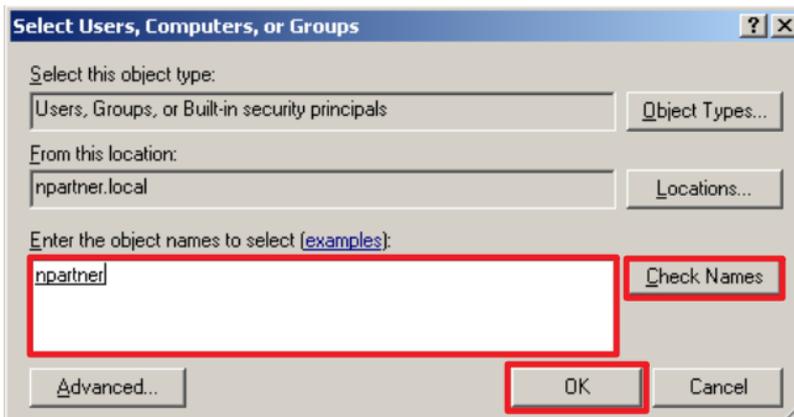
(5) Add DCOM User Permissions

Click “Add.”



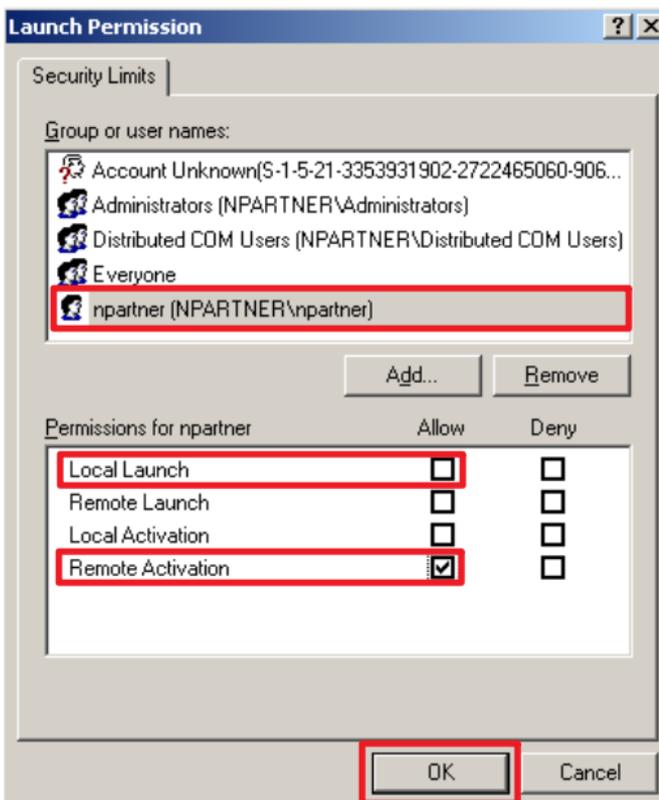
(6) Enter Your Username

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

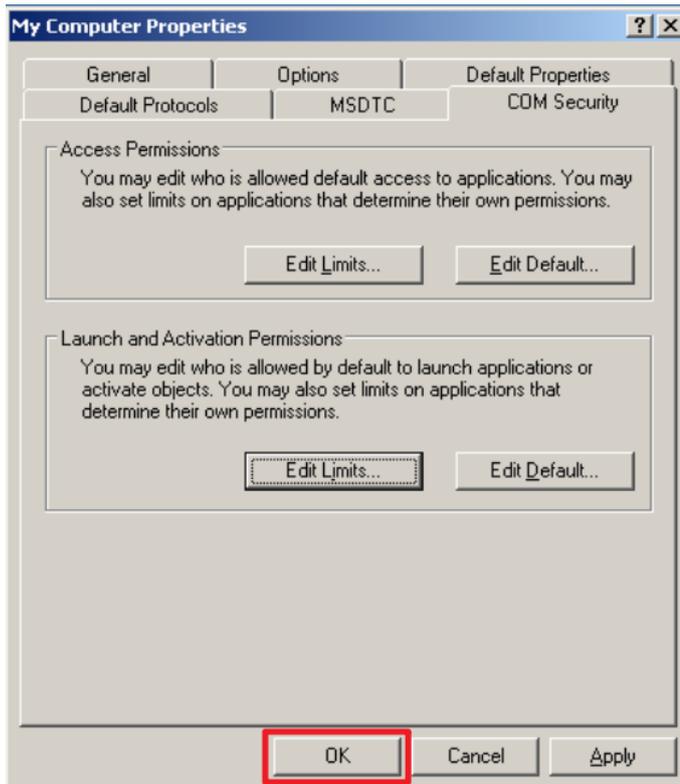


(7) Configure User Permissions

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

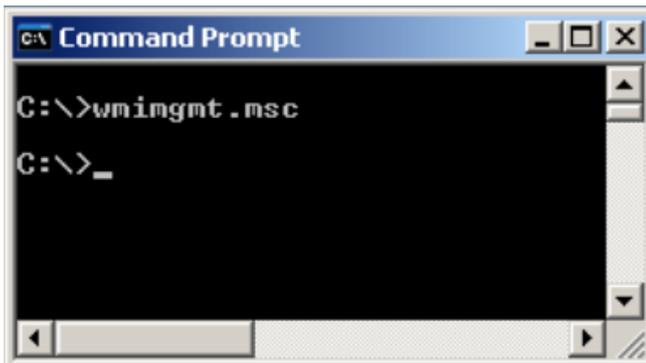
3.3.3.1 Configure Event Log Permissions

(1) Open "Command Prompt."



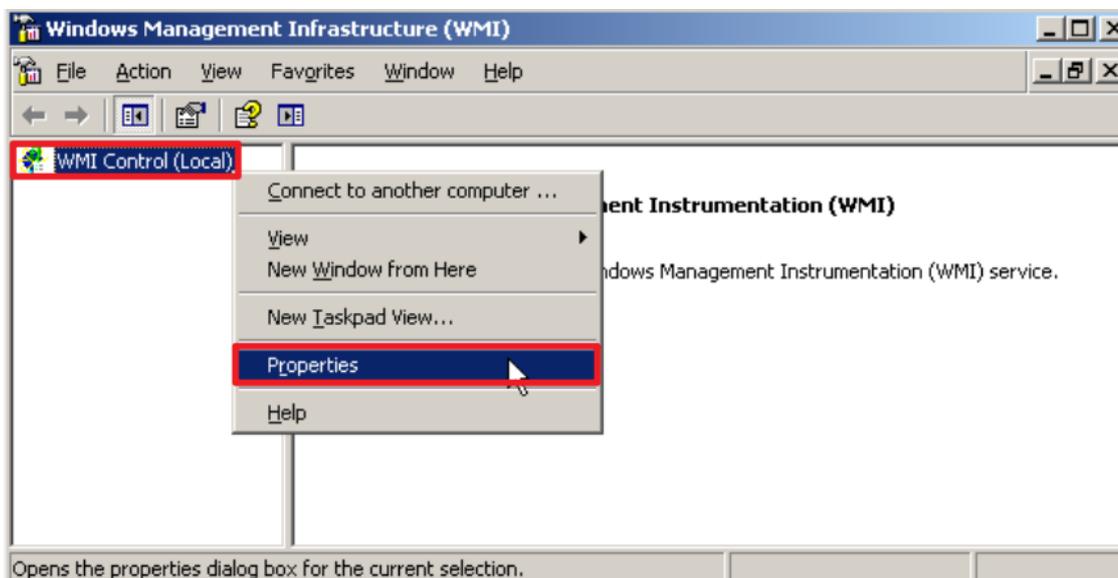
(2) Enter the command to enable WMI control service.

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



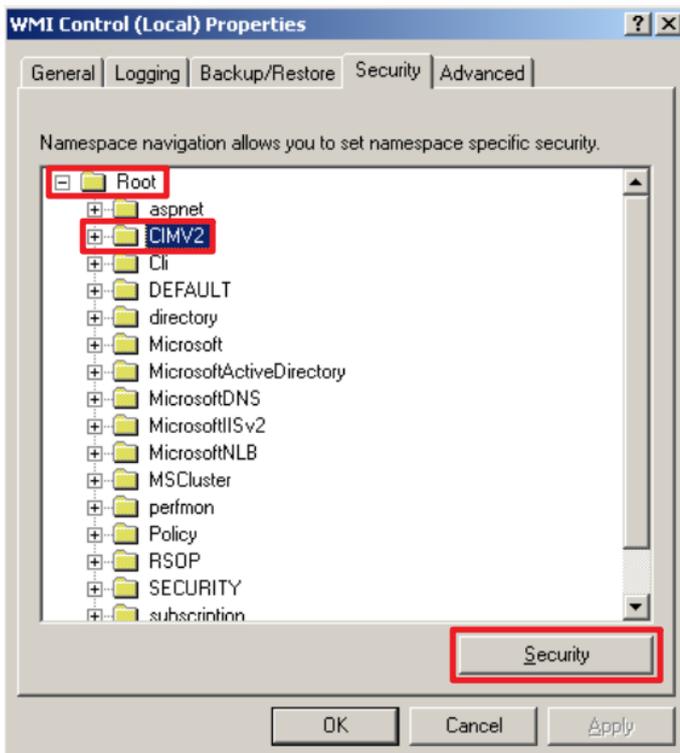
(3) Edit WMI Control

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



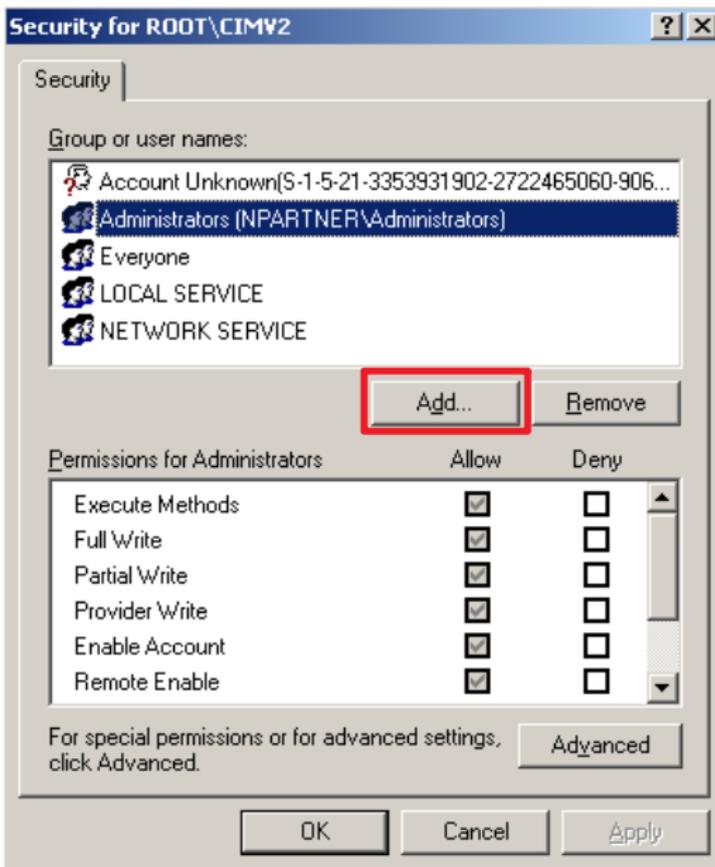
(4) Edit CIMV2 Security

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



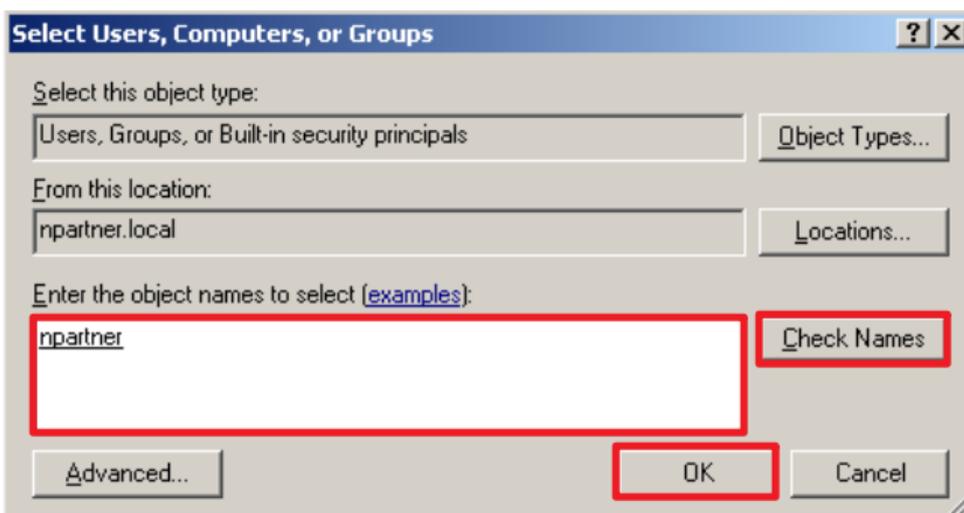
(5) Add WMI User Permissions.

Click “Add.”



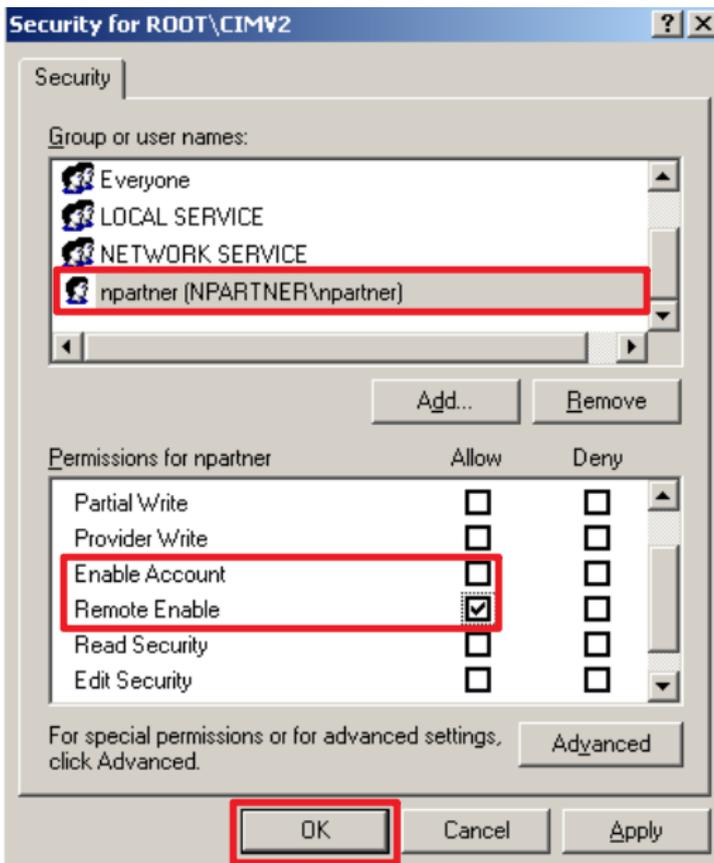
(6) Enter Your Username

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

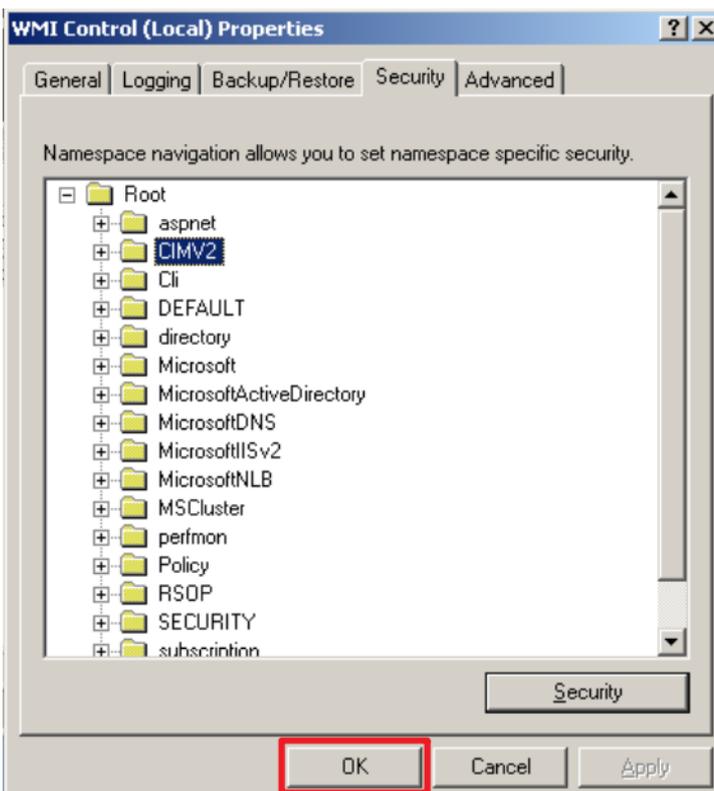


(7) Set Your User Permissions

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



(8) Click “OK.”



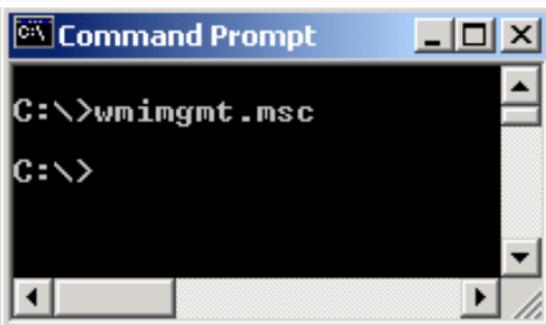
3.3.3.2 Configure Permissions for Reading User Data

(1) Open “Command Prompt.”



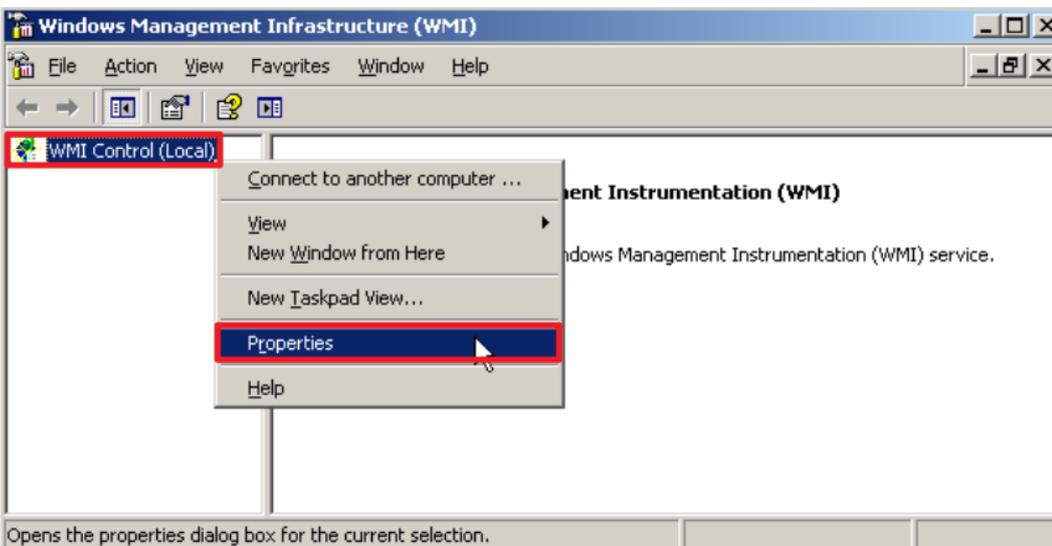
(2) Enter the command below to enable WMI Control.

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



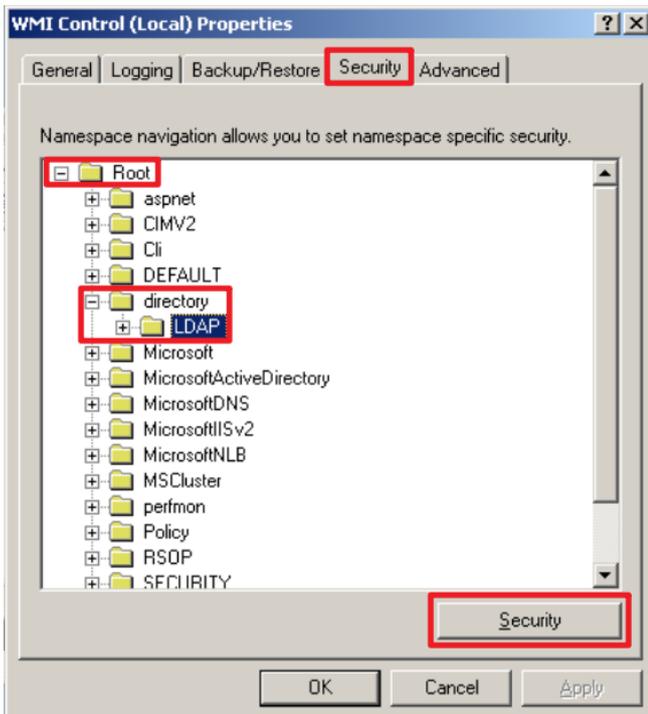
(3) Edit WMI Control

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



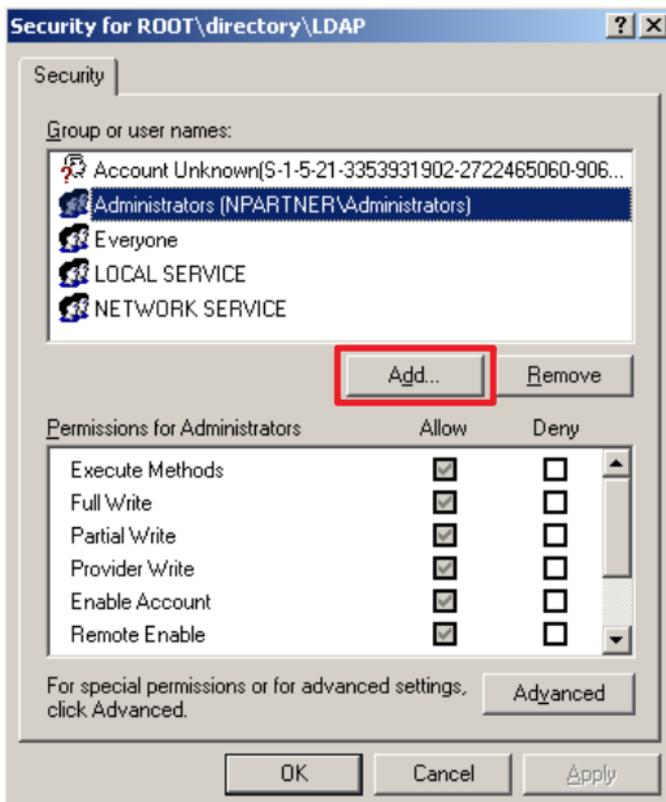
(4) Edit LDAP Security

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



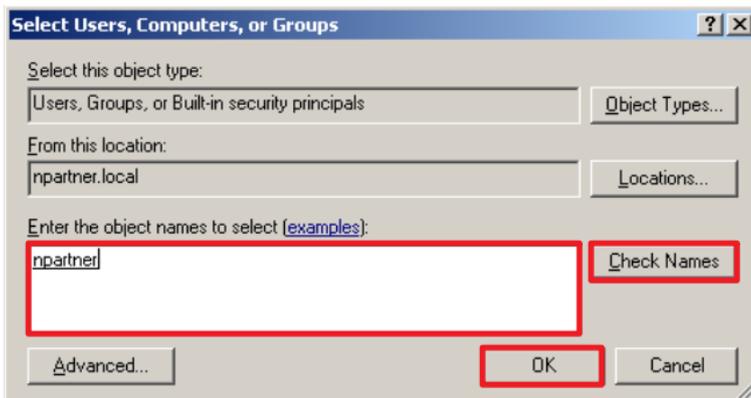
(5) Add WMI User Permissions

Click "Add."



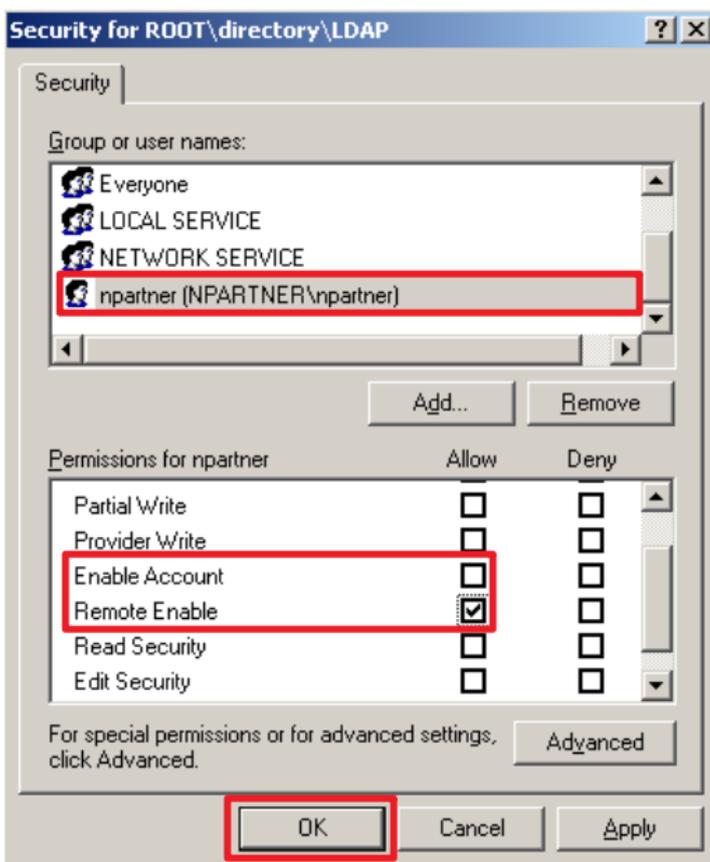
(6) Enter Your Username

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

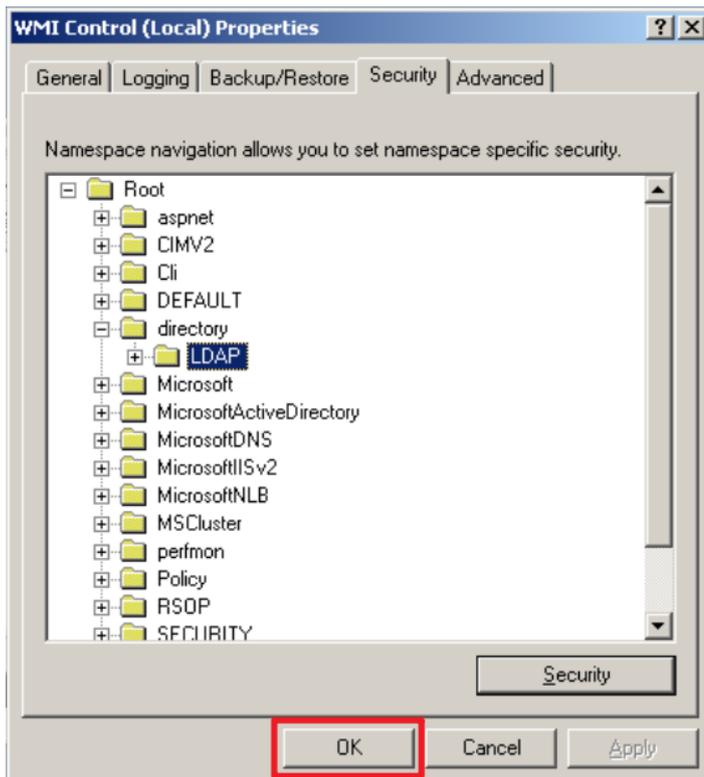


(7) Set Your User Permissions

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



(8) Click "OK."

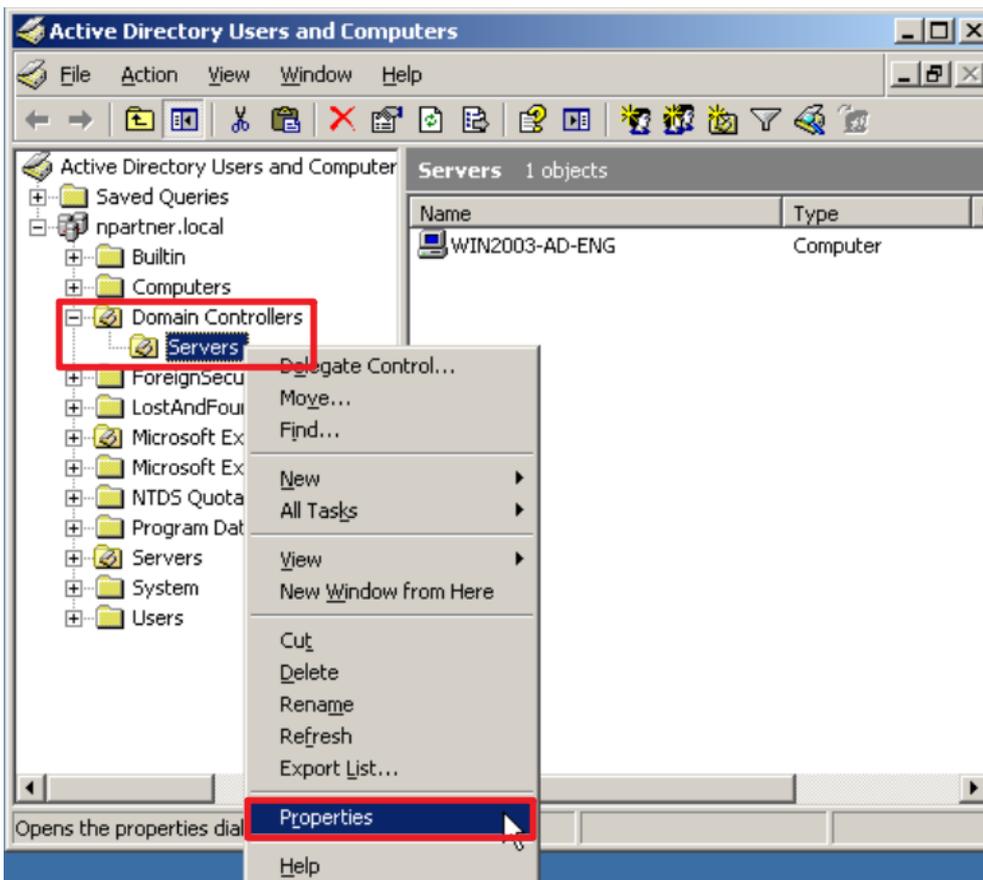


3.3.4 Configure Event Log Read Permissions

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

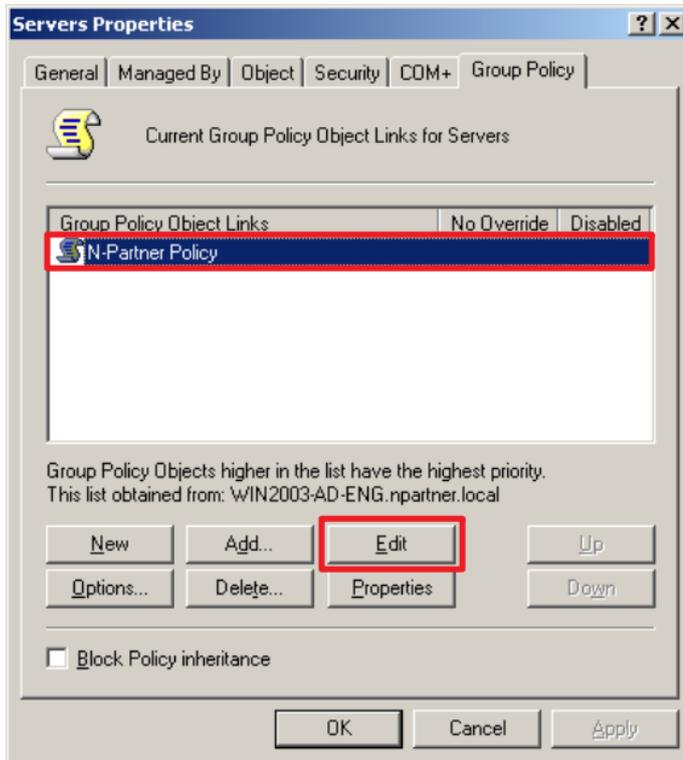


(2) Right-click the “Servers” organizational unit of “Domain Controllers,” and select “Properties.”



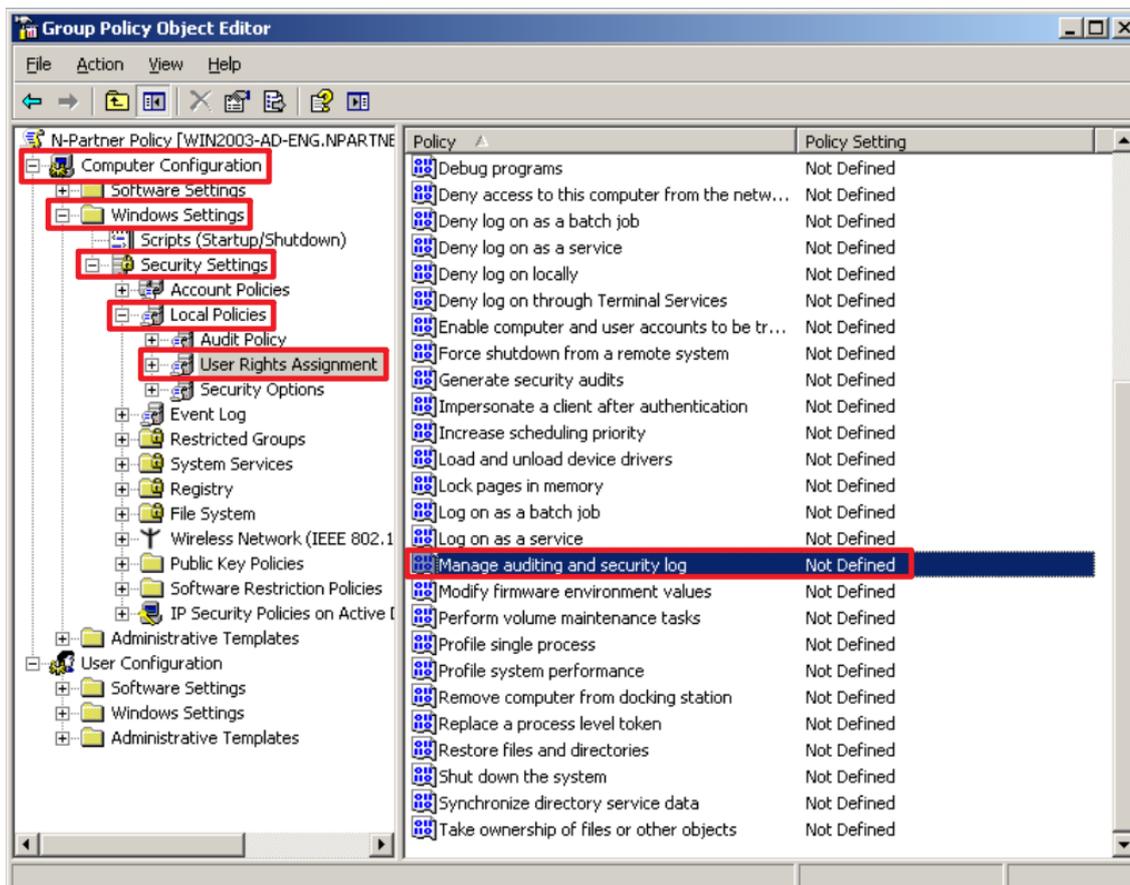
(3) Edit Group Policy Object

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



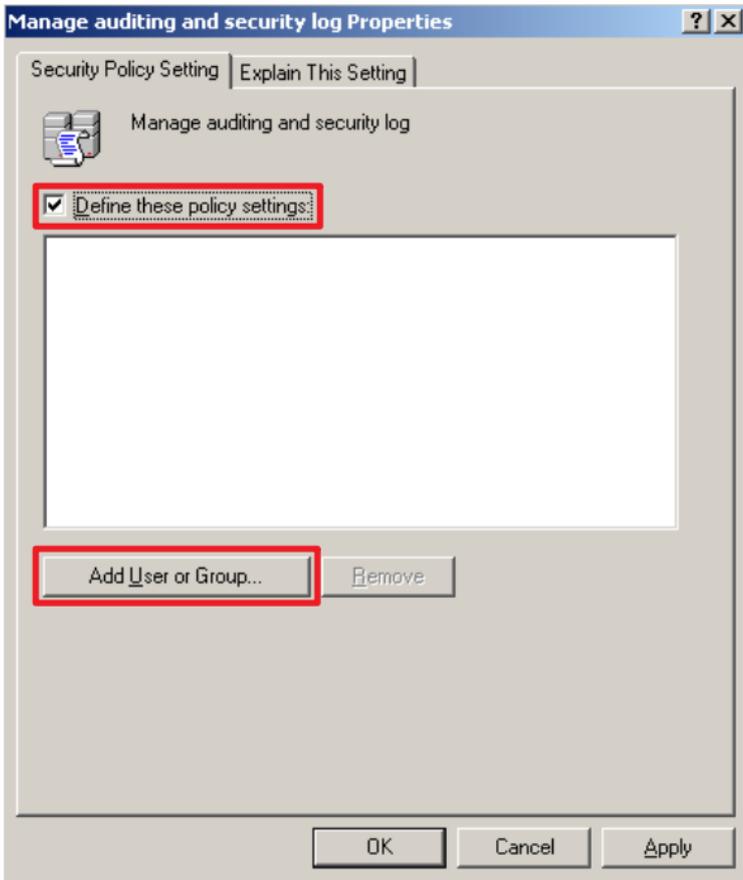
(4) Configure Audit Logs

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



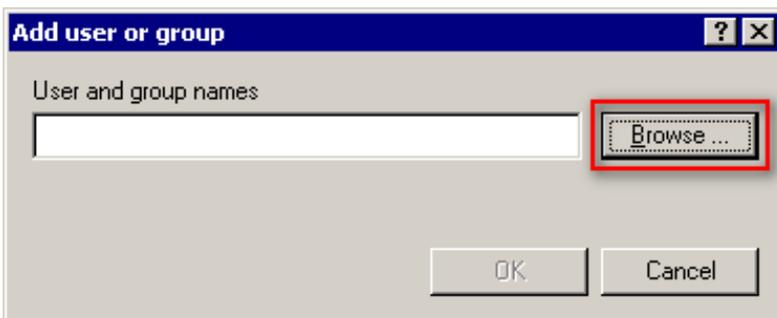
(5) Add Auditing User

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



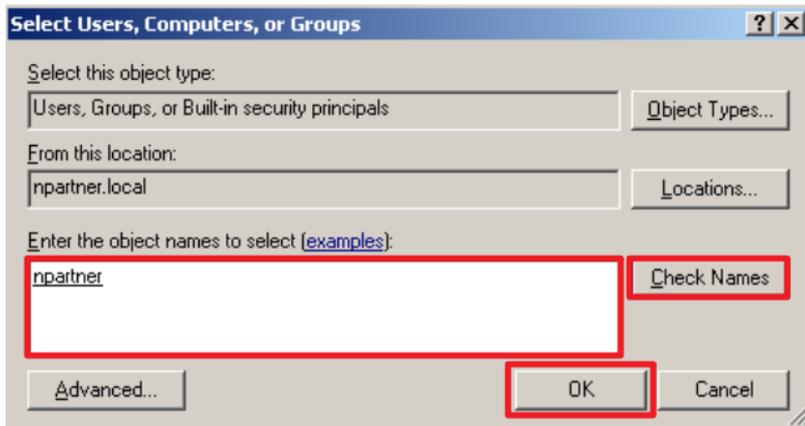
(6) Search for User

Click “Browse.”

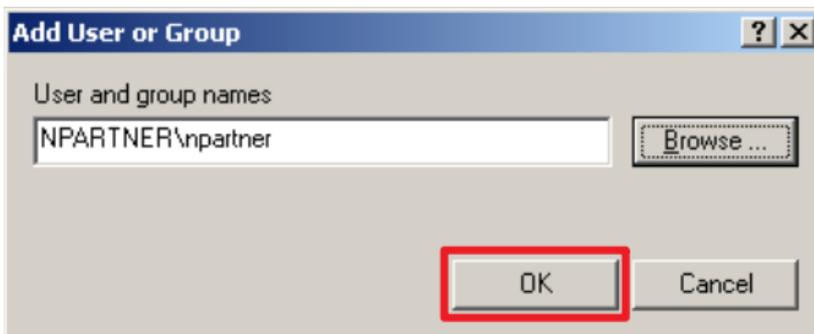


(7) Enter Your User Account

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

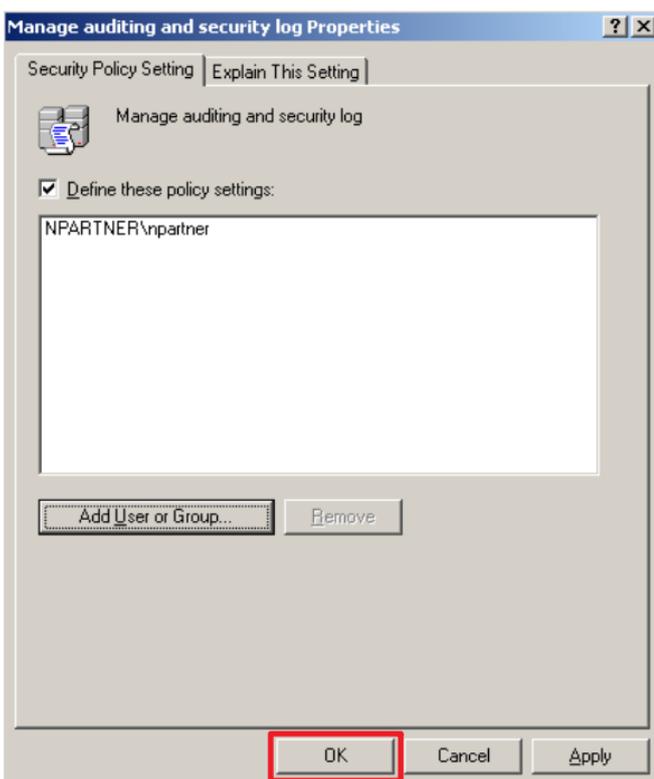


(8) Click “OK.”



(9) Confirm Audit Log Settings

Click “OK.”



(10) Open "Command Prompt."



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

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

A screenshot of the Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command prompt shows the command 'C:\>gpupdate /force' being entered. The output is: 'Refreshing Policy...', 'User Policy Refresh has completed.', 'Computer Policy Refresh has completed.', and 'To check for errors in policy processing, review the event log.' The prompt ends with 'C:\>_'.

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

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

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

C:\>_
```

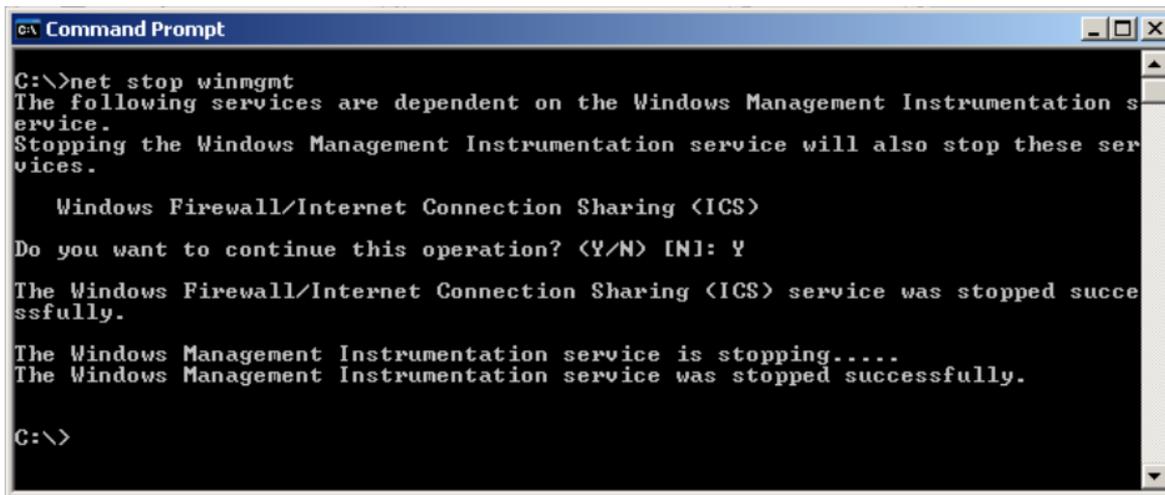
3.3.5 Restart the WMI Service

(1) Open "Command Prompt."



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

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



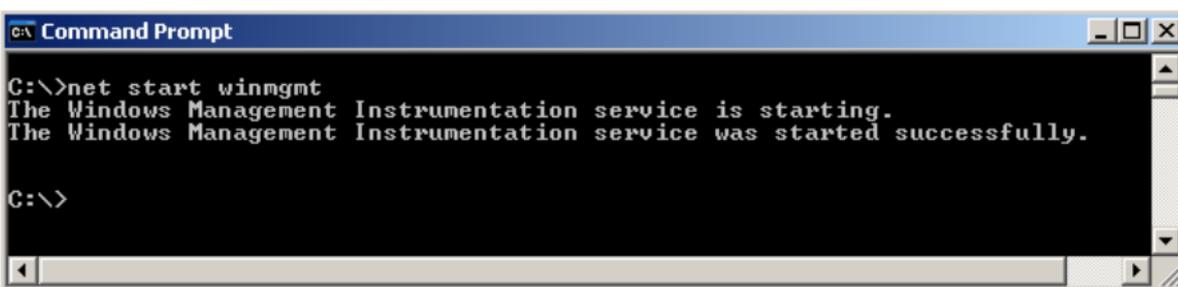
```
C:\> net stop winmgmt
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.

    Windows Firewall/Internet Connection Sharing (ICS)
Do you want to continue this operation? (Y/N) [N]: Y
The Windows Firewall/Internet Connection Sharing (ICS) service was stopped successfully.
The Windows Management Instrumentation service is stopping....
The Windows Management Instrumentation service was stopped successfully.

C:\>
```

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

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

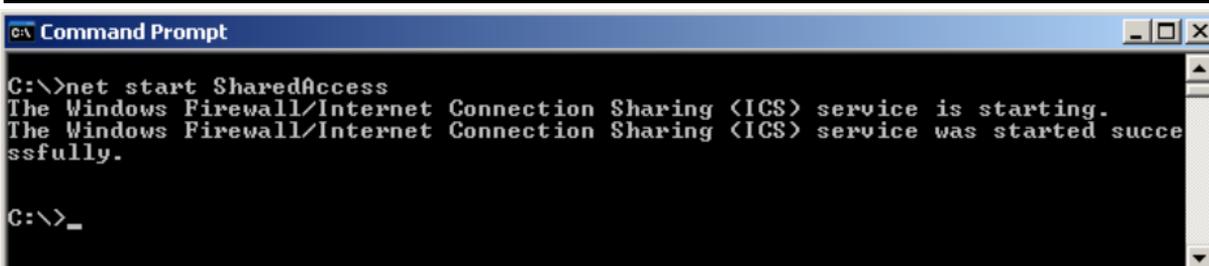


```
C:\> net start winmgmt
The Windows Management Instrumentation service is starting.
The Windows Management Instrumentation service was started successfully.

C:\>
```

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

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



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

C:\> _
```

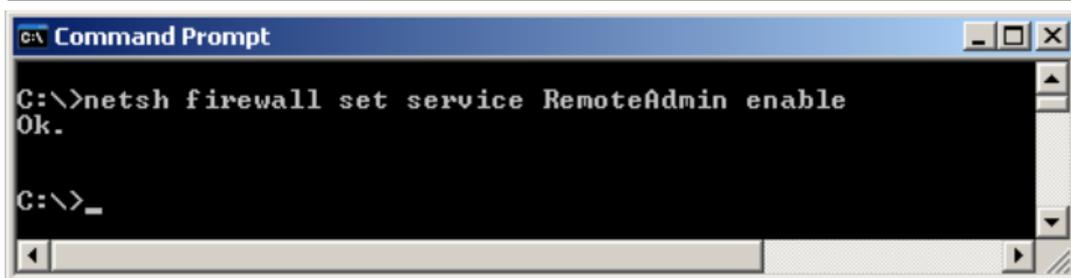
3.3.6 Configure the Firewall

(1) Open "Command Prompt."



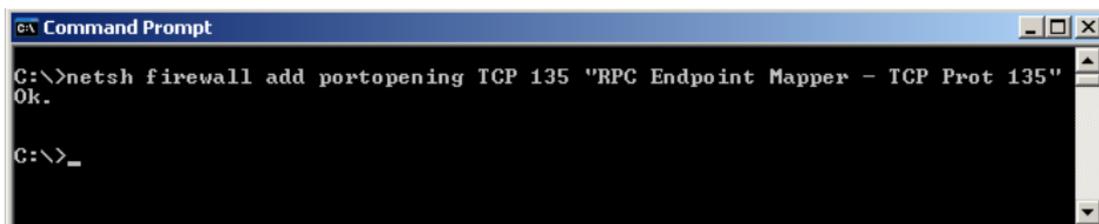
(2) Enter the command below to allow WMI through the firewall:

```
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
```

```
C:\> netsh firewall show config
Domain profile configuration:
-----
Operational mode           = Disable
Exception mode             = Enable
Multicast/broadcast response mode = Enable
Notification mode         = Enable

Service configuration for Domain profile:
Mode      Customized  Name
-----
Enable    No          File and Printer Sharing

Port configuration for Domain profile:
Port      Protocol  Mode      Name
-----
139       TCP       Enable    NetBIOS Session Service
445       TCP       Enable    SMB over TCP
137       UDP       Enable    NetBIOS Name Service
138       UDP       Enable    NetBIOS Datagram Service

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

Service configuration for Standard profile:
Mode      Customized  Name
-----
Enable    No          File and Printer Sharing
Enable    No          Remote Desktop
Enable    No          Remote Administration

Port configuration for Standard profile:
Port      Protocol  Mode      Name
-----
135       TCP       Enable    RPC Endpoint Mapper - TCP Prot 135
161       UDP       Enable    SNMP
139       TCP       Enable    NetBIOS Session Service
445       TCP       Enable    SMB over TCP
137       UDP       Enable    NetBIOS Name Service
138       UDP       Enable    NetBIOS Datagram Service
3389      TCP       Enable    Remote Desktop

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

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

4. Windows Server 2008

Windows Audit Policy Configuration:

For detailed information, refer to the [Audit Policy Recommendations link](#) in the references.

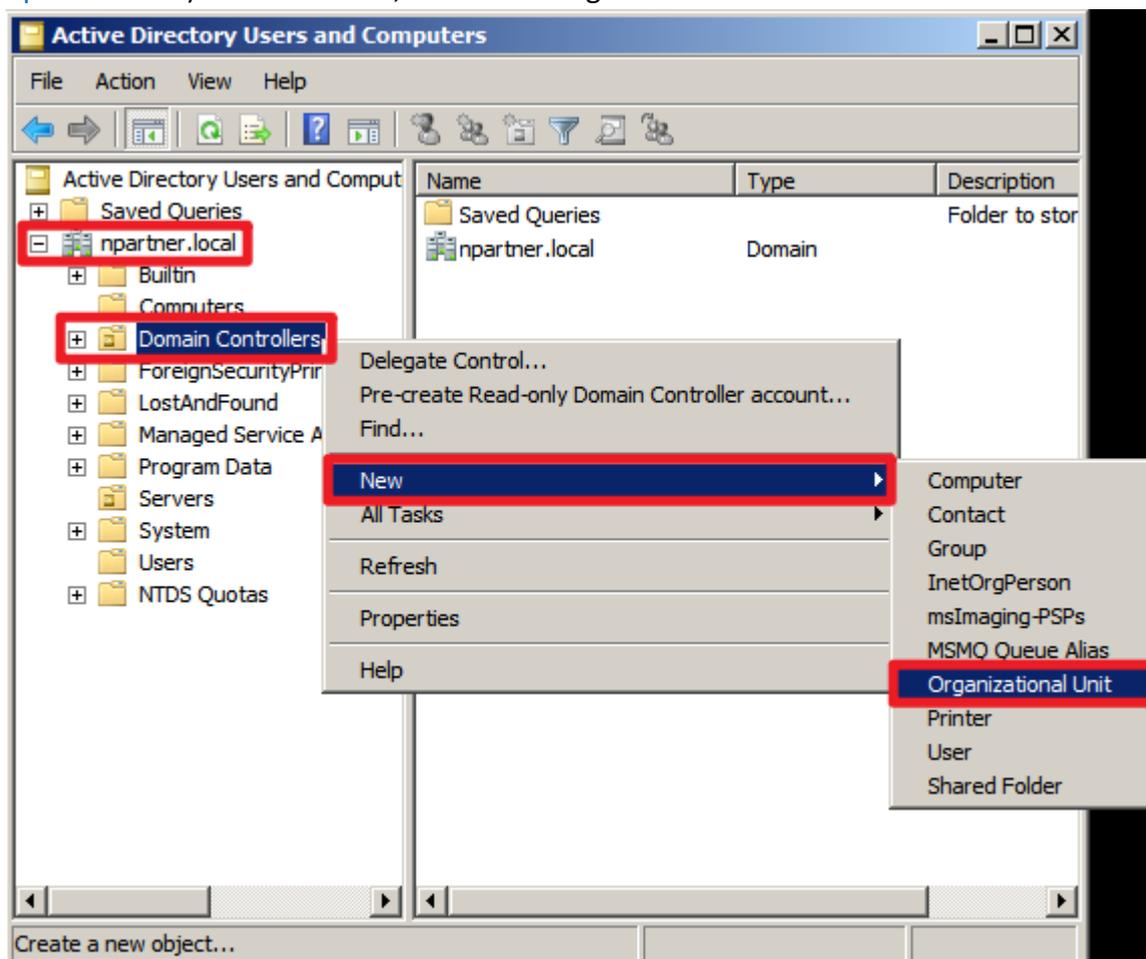
4.1 Organizational Unit (OU) Configuration

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



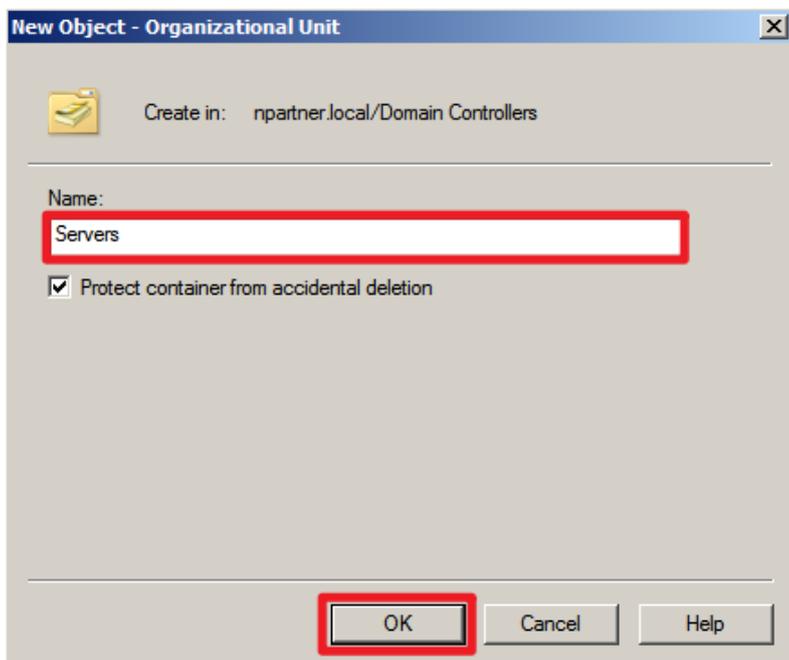
(2) Add an Organizational Unit

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”)

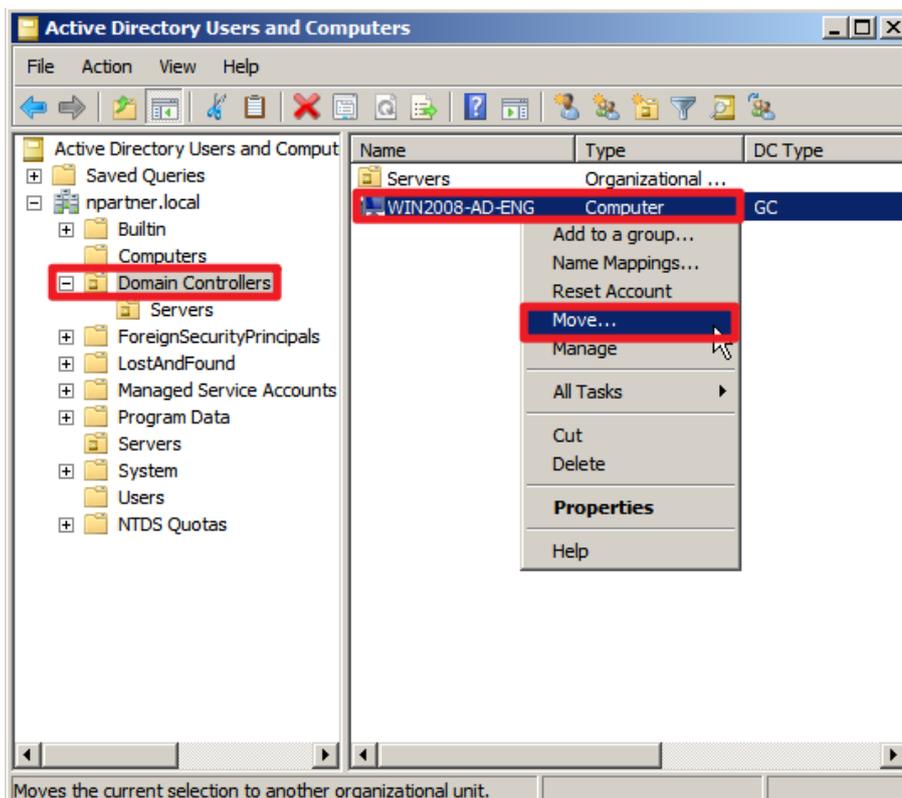
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

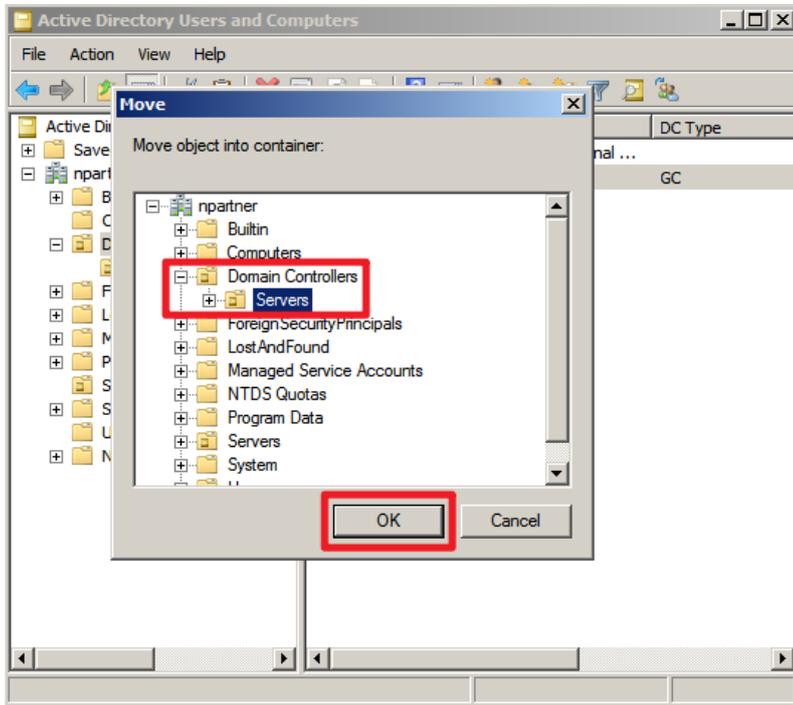
Select the “Domain Controllers” organizational unit (OU) → right-click on the “WIN2008-AD-ENG” server.

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



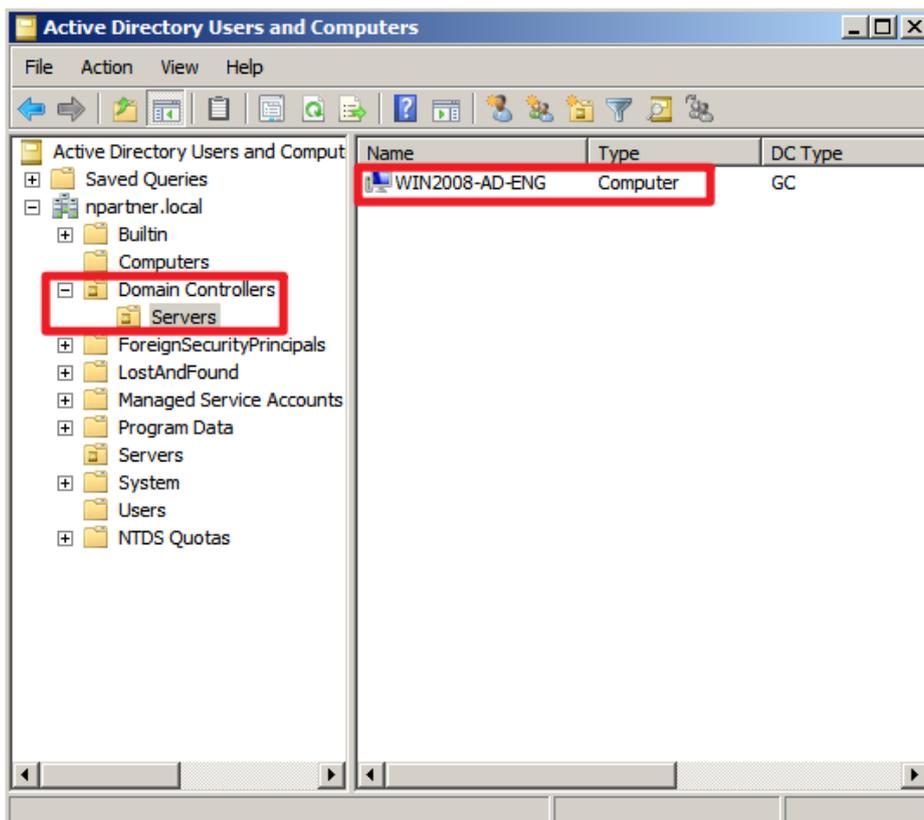
(5) Select your Organizational Unit:

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.

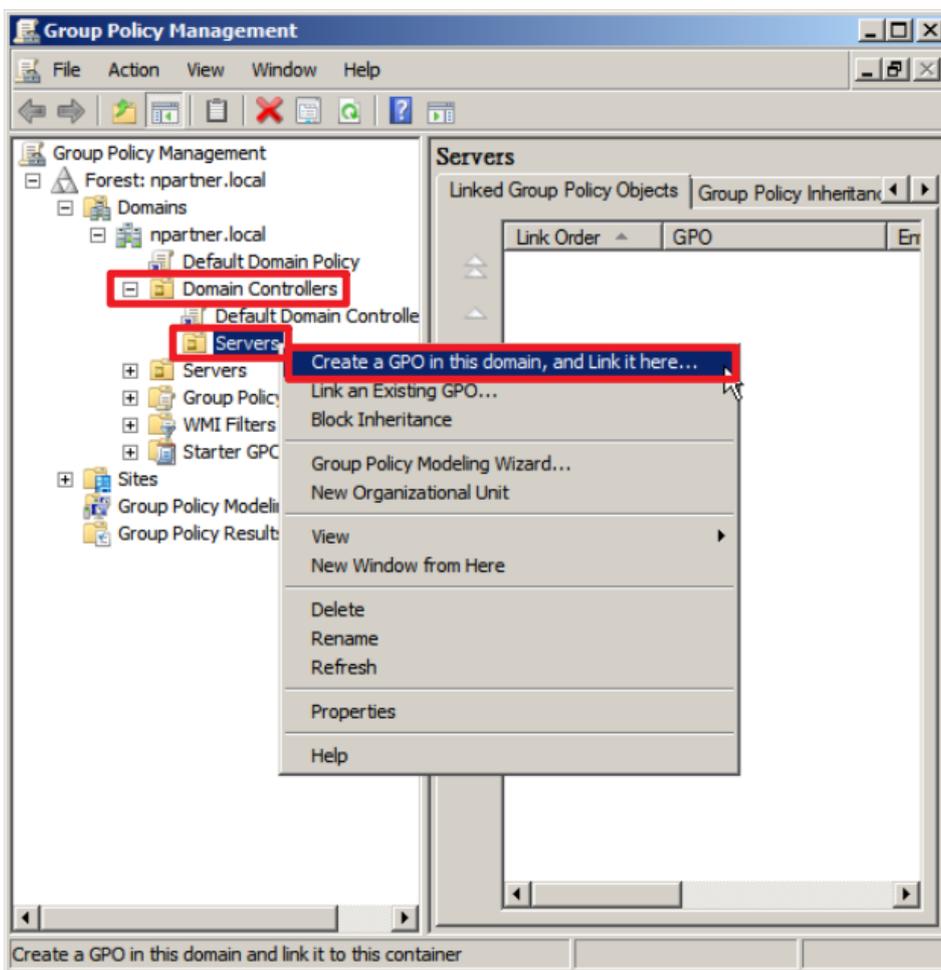


4.2 Group Policy Settings

(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”)

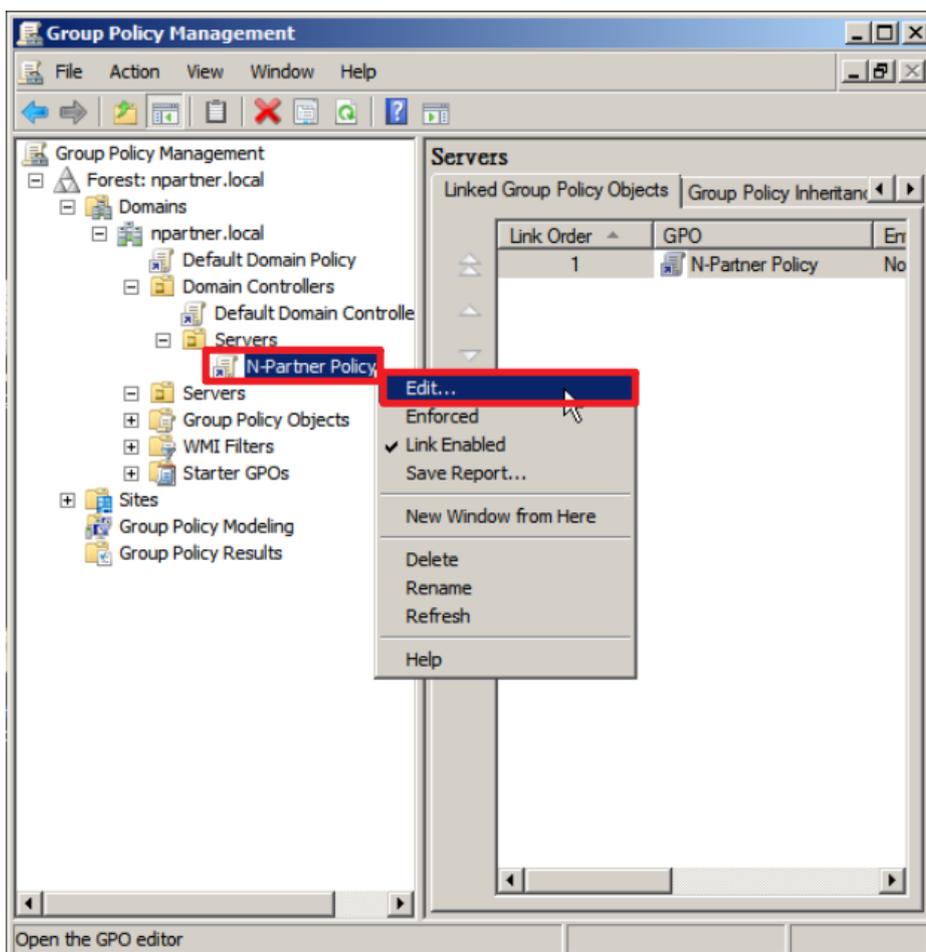
Note: Please create the GPO name according to the actual environment.

→ select “OK.”



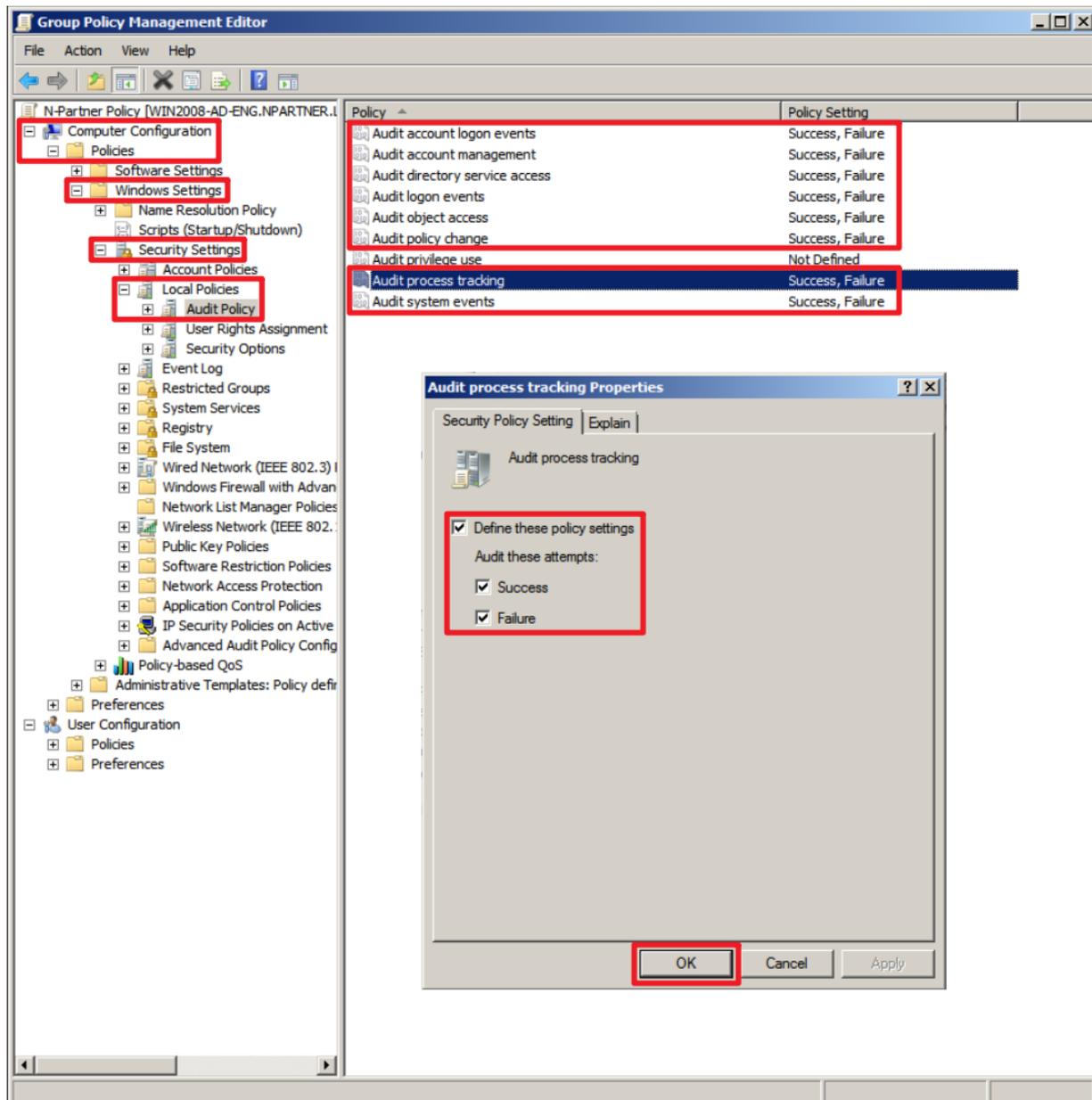
(4) Edit your Group Policy Object

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



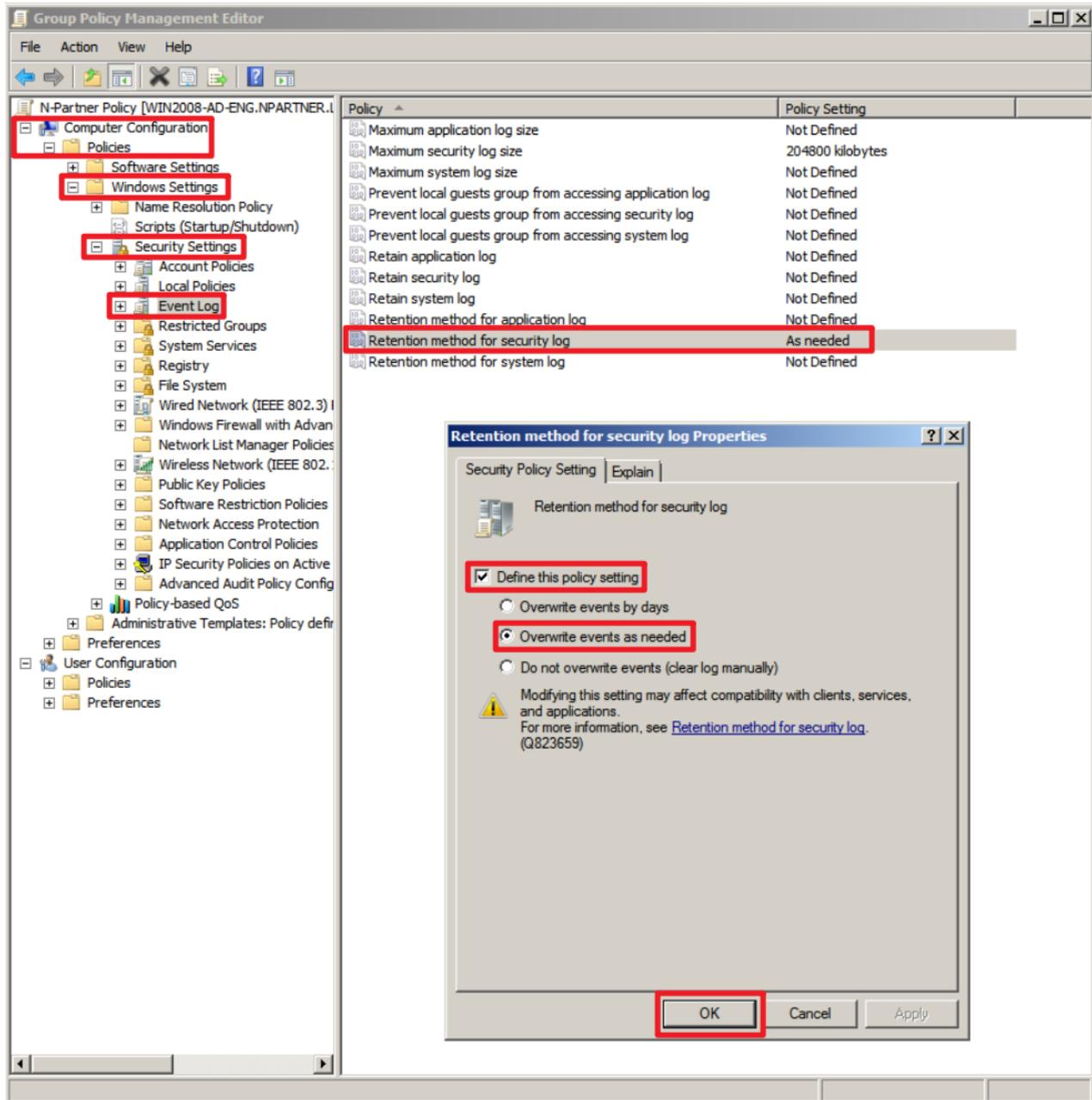
(5) Local Group Policies: Audit Policy

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

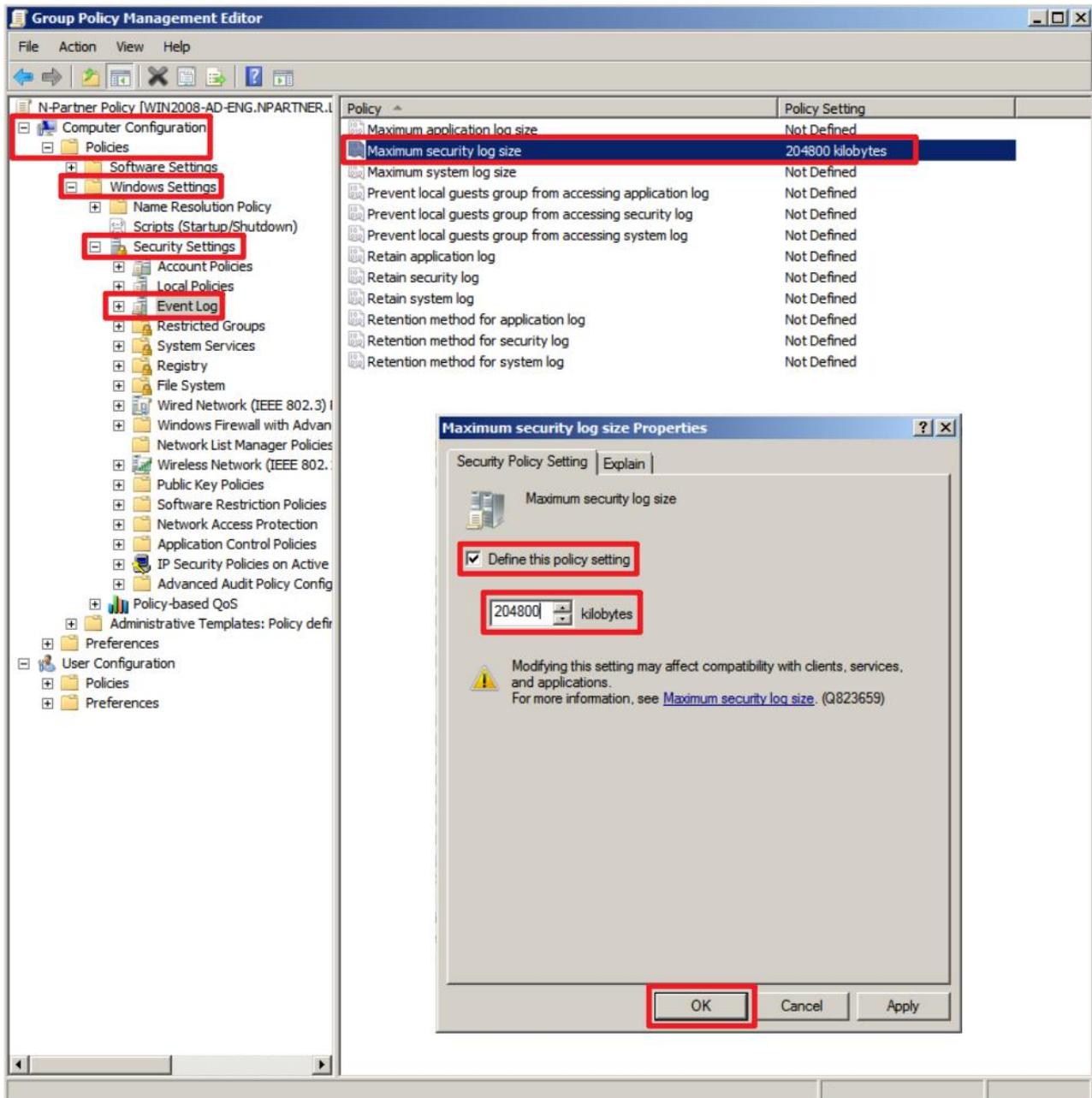
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

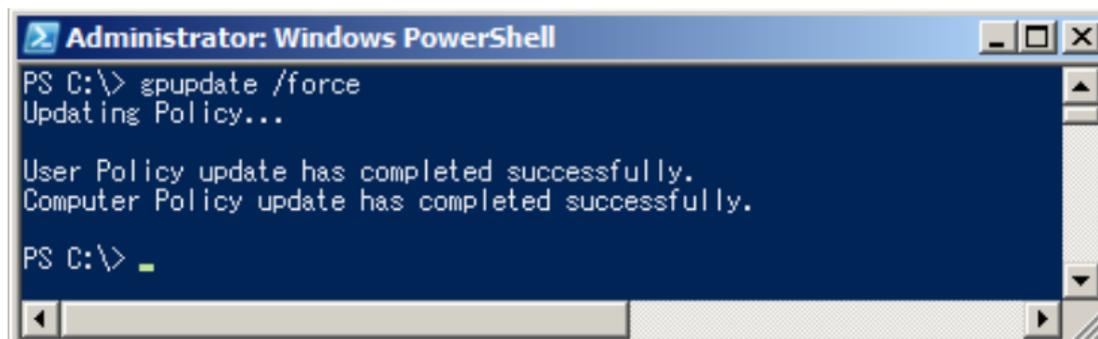


(8) On the Windows File server, open “Windows PowerShell.”



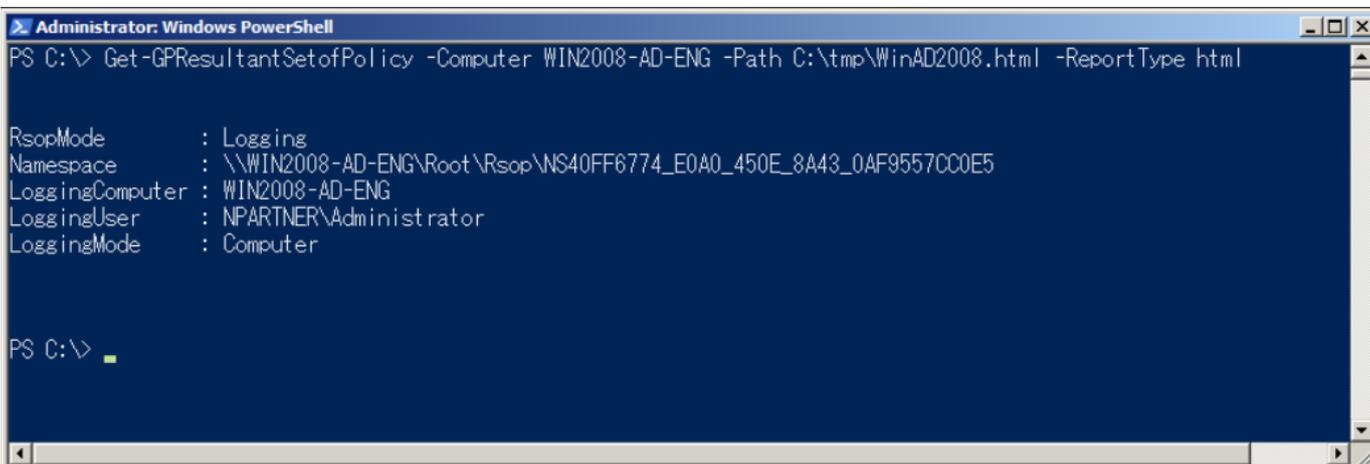
(9) Enter the command below to refresh group policy.

```
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).

Group Policy Results
 NPARTNER\WIN2008-AD-ENG
 Data collected on: 8/21/2025 PM 02:24:09

Summary

Computer Configuration Summary

General

Computer name	NPARTNER\WIN2008-AD-ENG
Domain	npartner.local
Site	Default-First-Site-Name
Last time Group Policy was processed	8/21/2025 PM 02:22:07

Group Policy Objects

Applied GPOs

Name	Link Location	Revision
Local Group Policy	Local	AD (1), Sysvol (1)
Default Domain Policy	npartner.local	AD (5), Sysvol (65535)
Default Domain Controllers Policy	npartner.local/Domain Controllers	AD (3), Sysvol (65535)
N-Partner Policy	npartner.local/Domain Controllers/Servers	AD (40), Sysvol (65535)

Local Policies/Audit Policy

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

Event Log

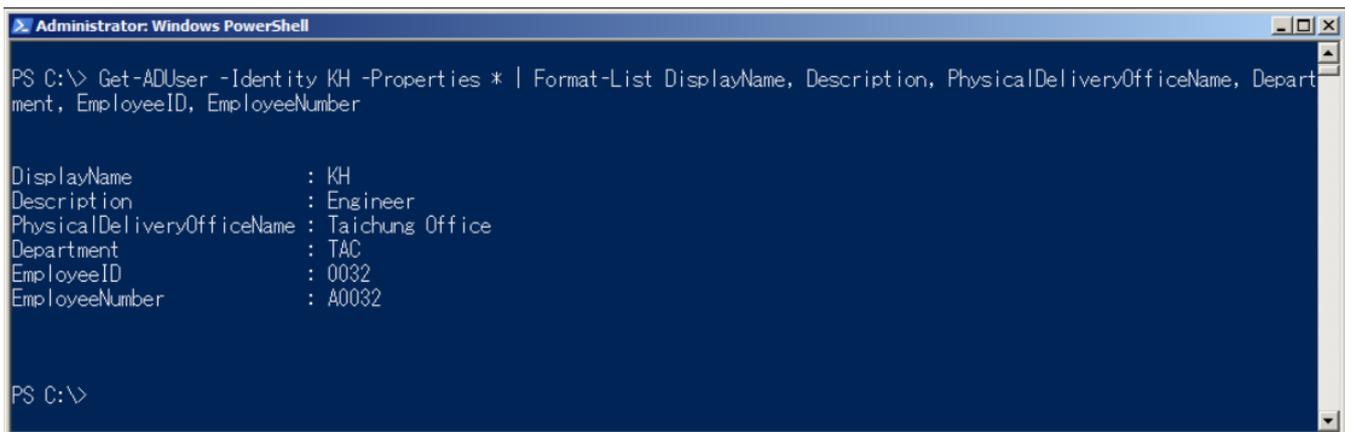
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

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

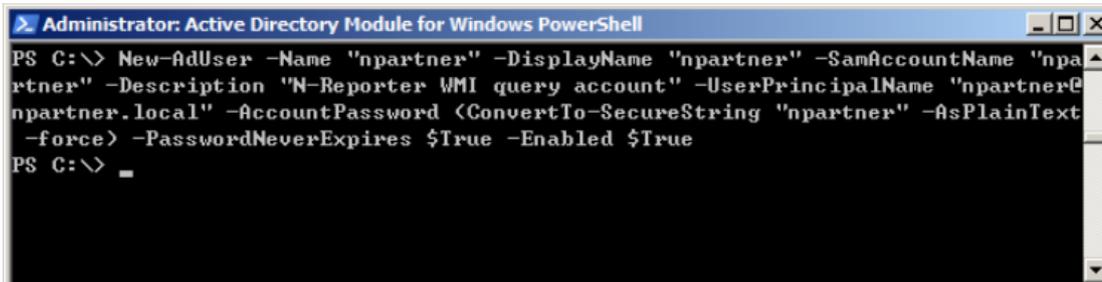
(1) Open "Active Directory PowerShell Snap-In."



(2) Create an Account

Enter the command below to create an account:

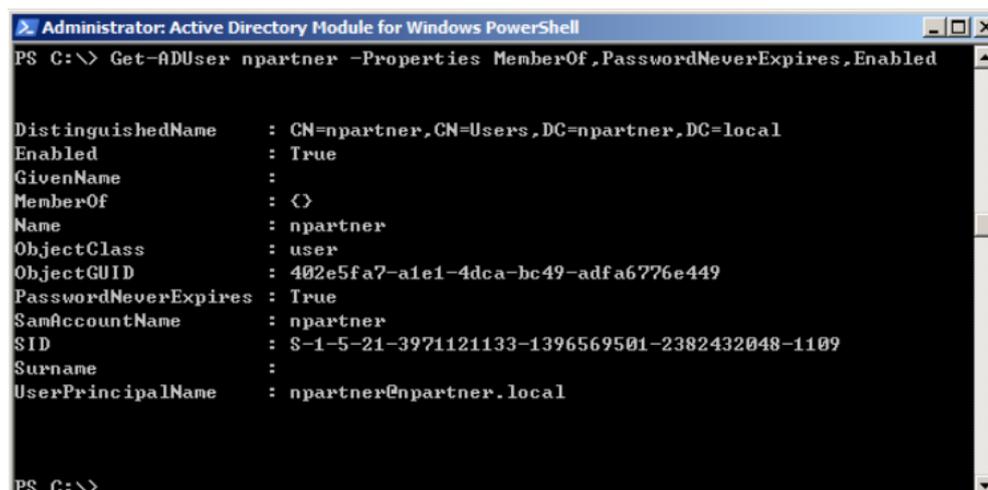
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description
"NReporter WMI query account" `
>> -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -
AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled $True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



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
```



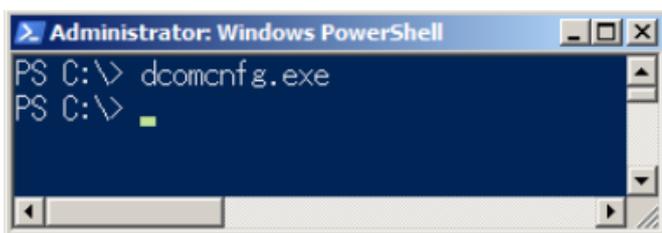
4.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”



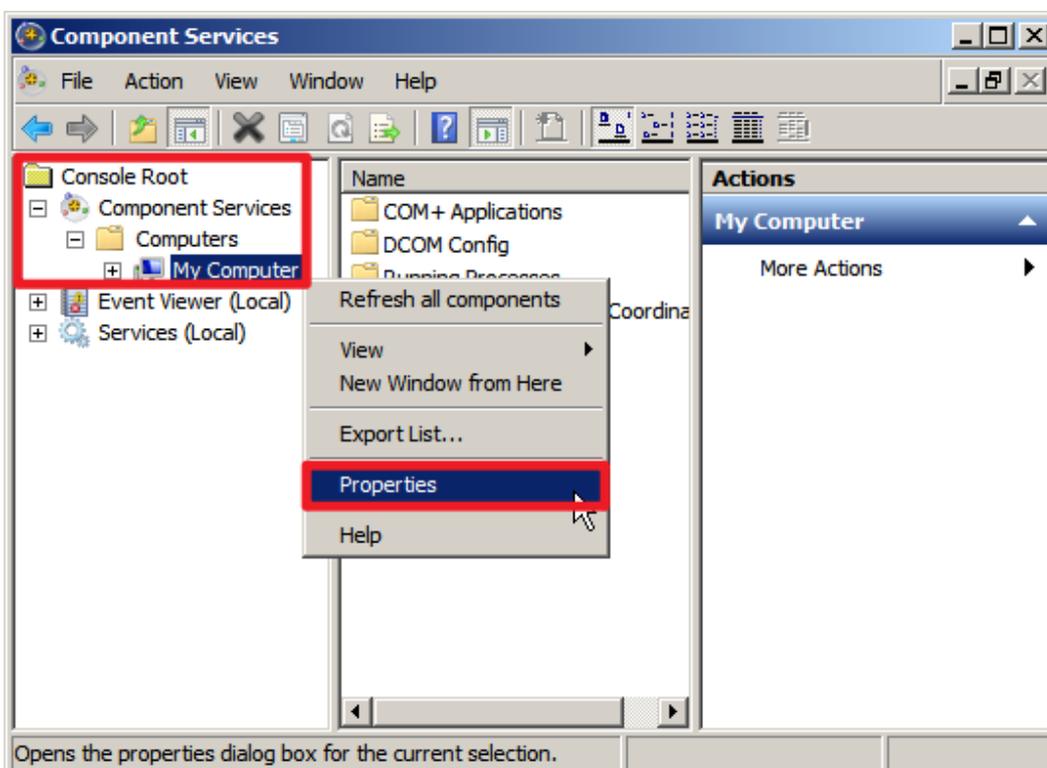
(2) Enter the command below to enable component services.

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



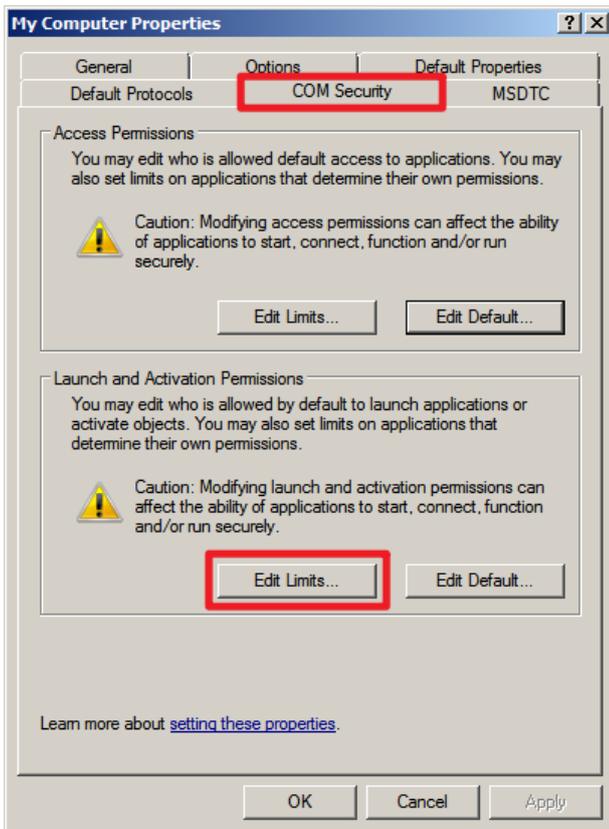
(3) Edit Computer Properties

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



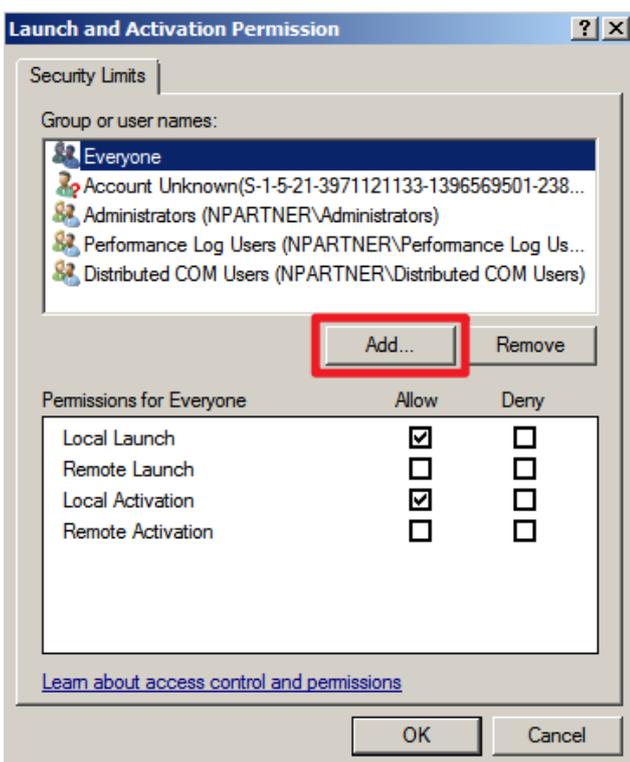
(4) Enable Permissions

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



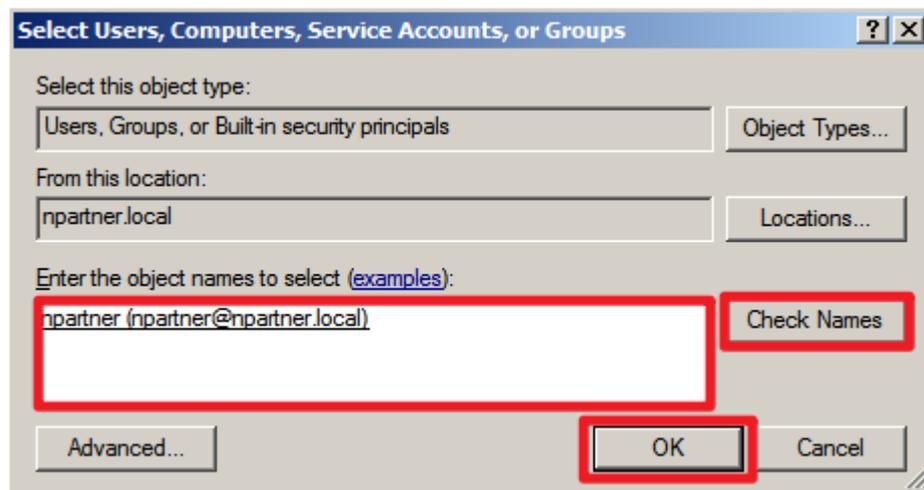
(5) Add DCOM User Permissions

Click “Add.”



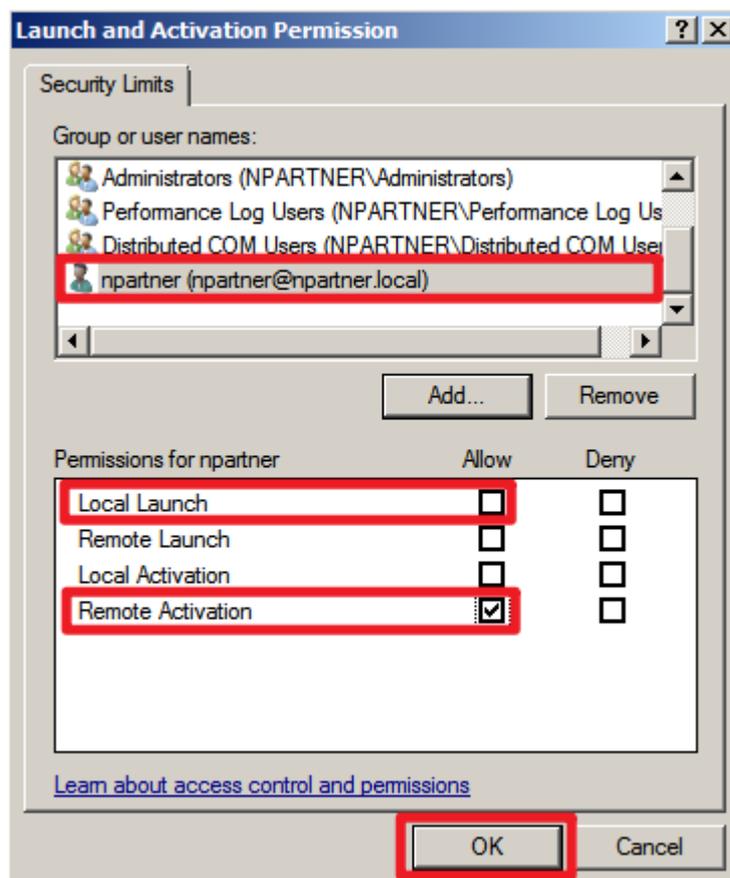
(6) Enter Your Username

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

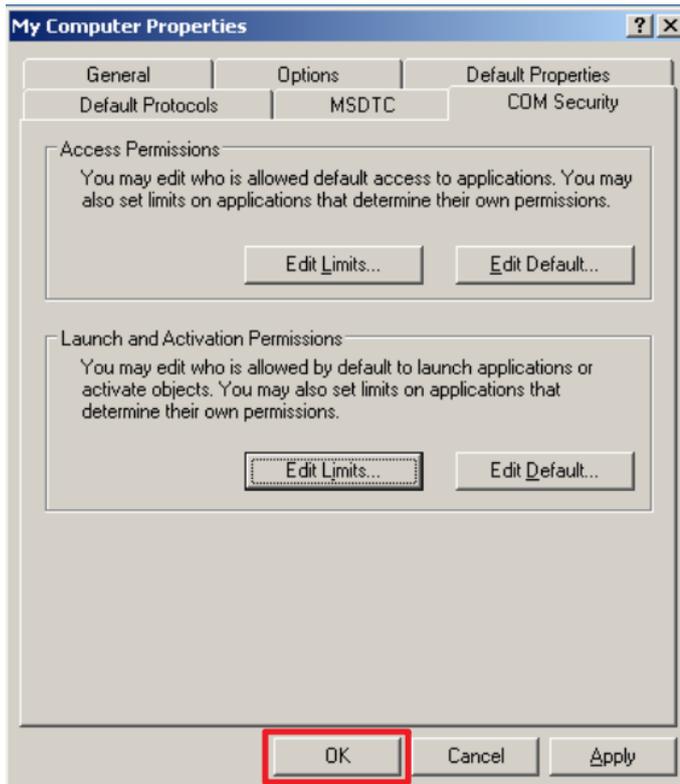


(7) Configure User Permissions

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

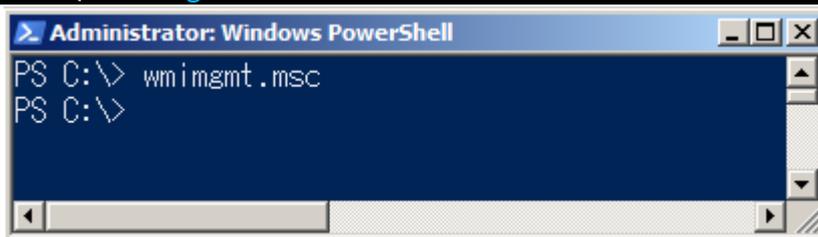
4.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



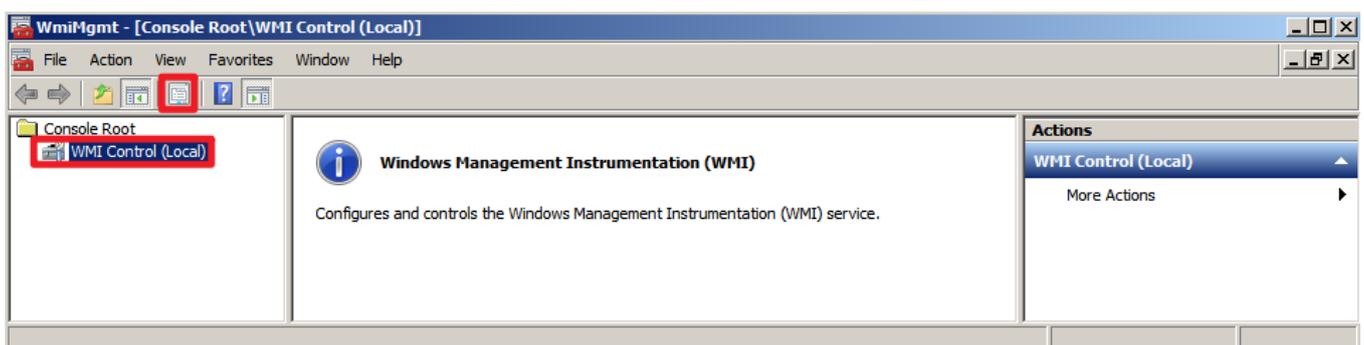
(2) Enter the command to enable WMI control service.

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



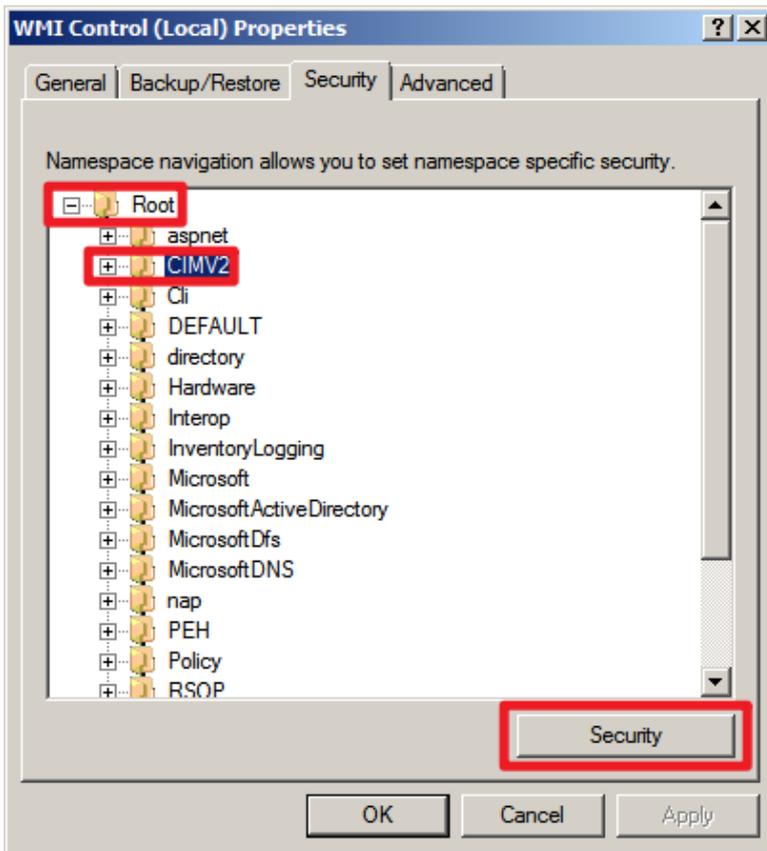
(3) Edit WMI Control

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



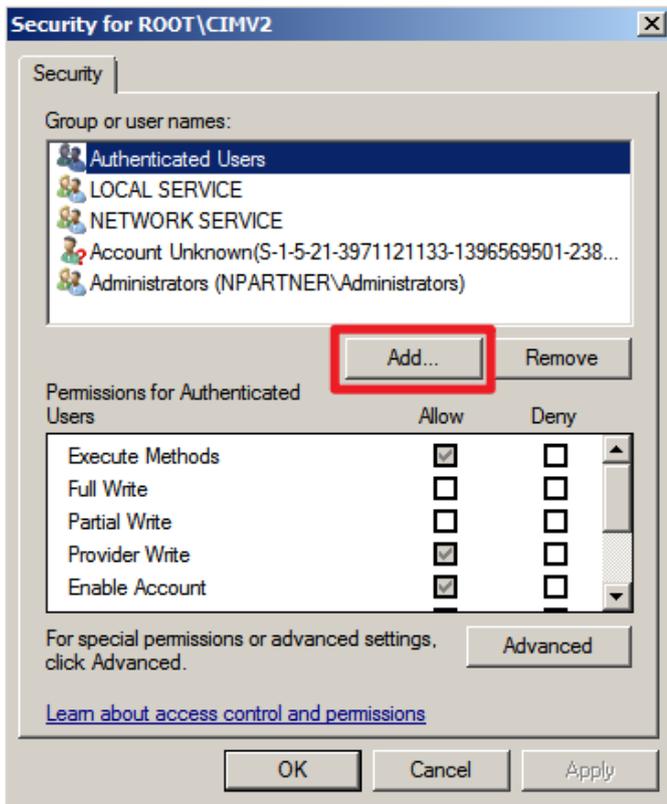
(4) Edit CIMV2 Security

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



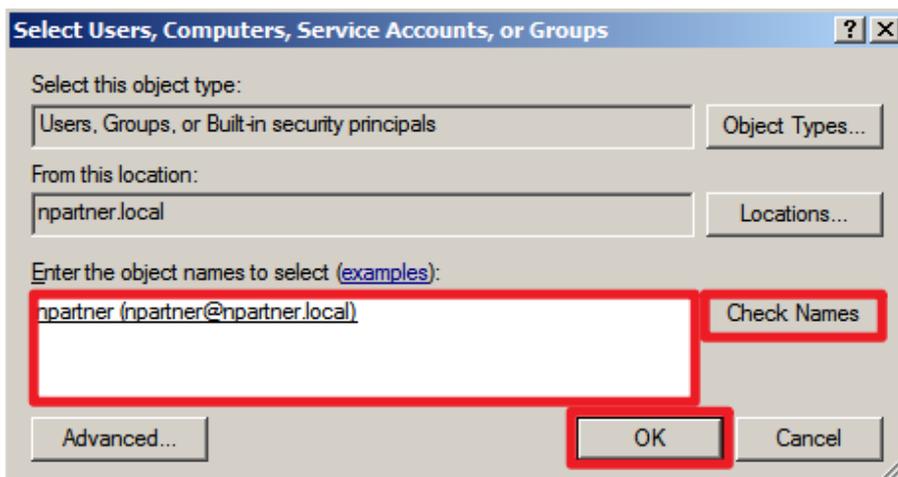
(5) Add WMI User Permissions.

Click “Add.”



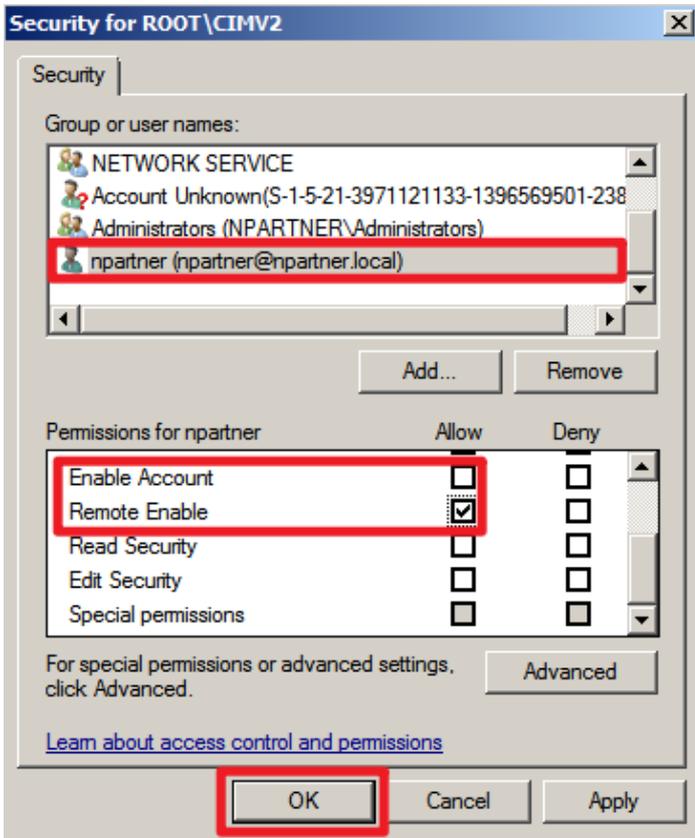
(6) Enter Your Username

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

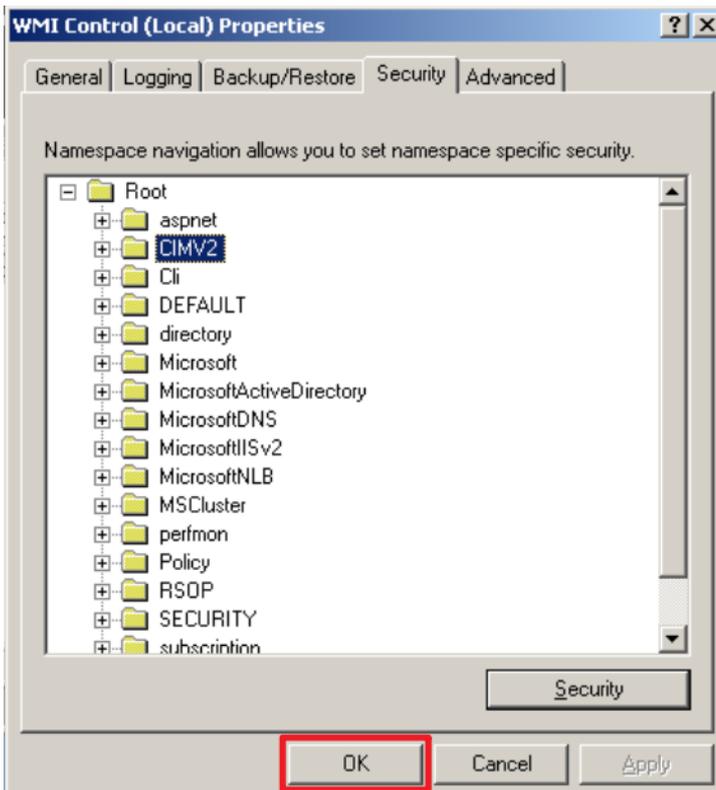


(7) Set Your User Permissions

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



(8) Click “OK.”



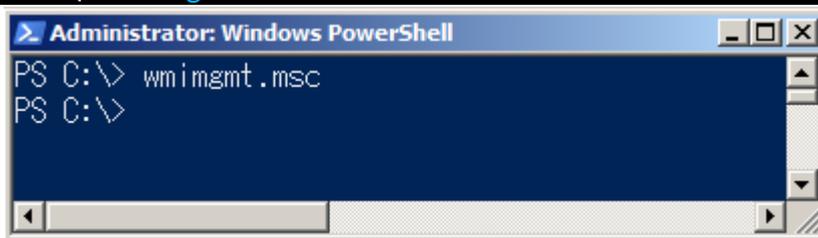
4.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



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

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



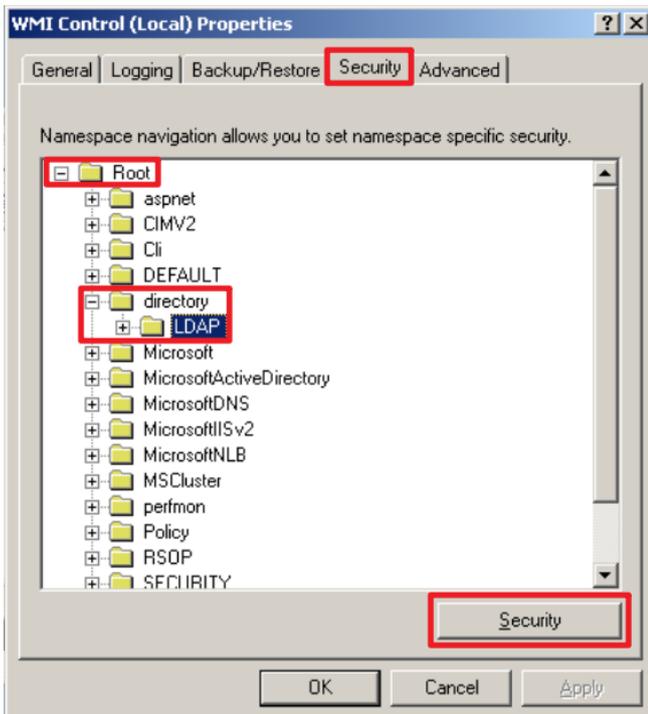
(3) Edit WMI Control

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



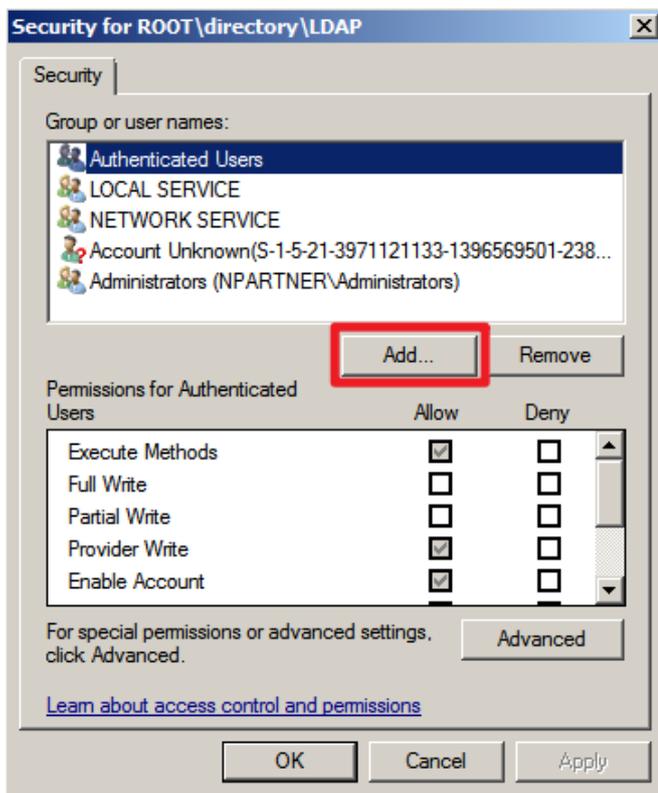
(4) Edit LDAP Security

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



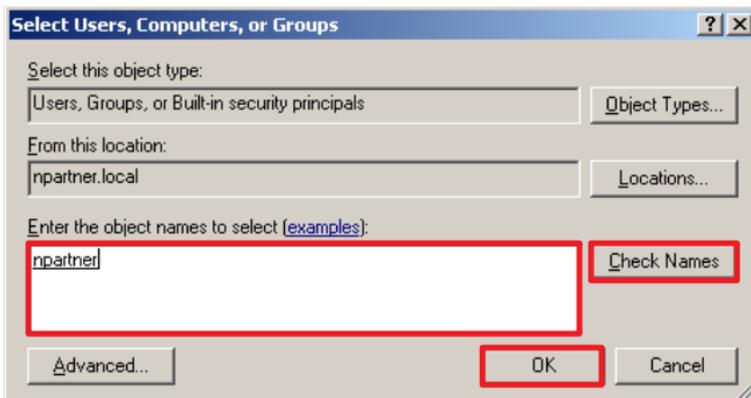
(5) Add WMI User Permissions

Click “Add.”



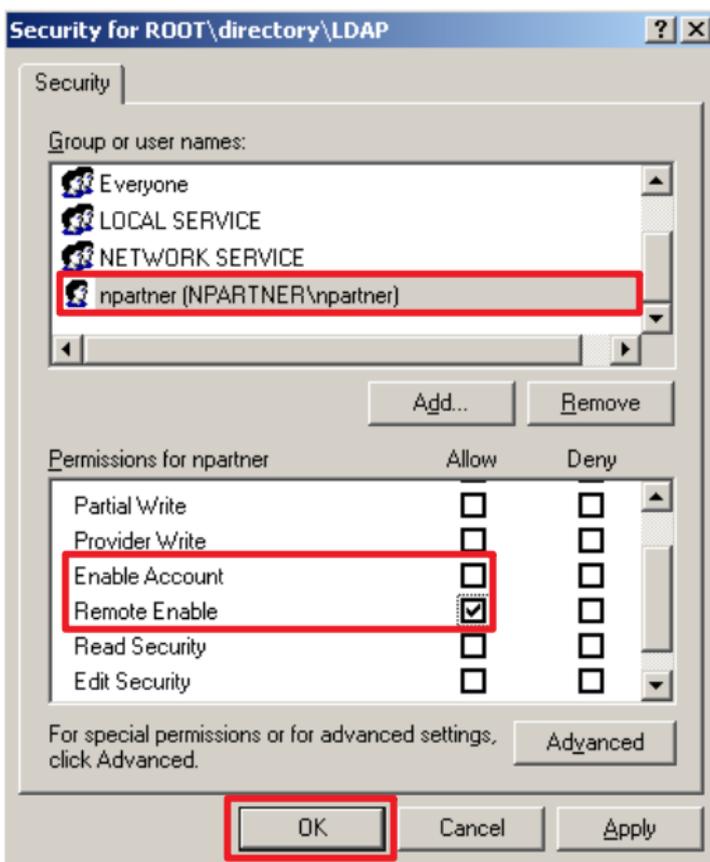
(6) Enter Your Username

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

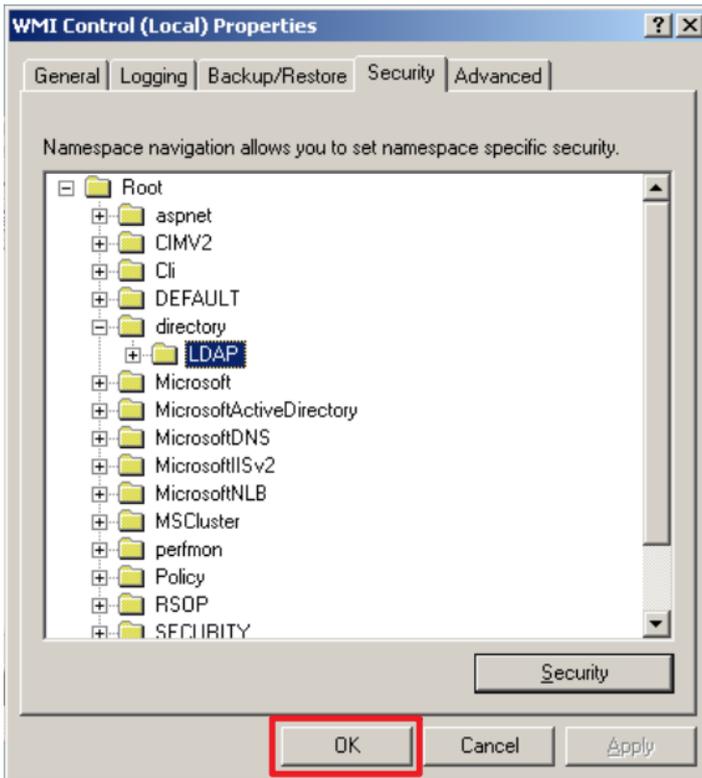


(7) Set Your User Permissions

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



(8) Click "OK."

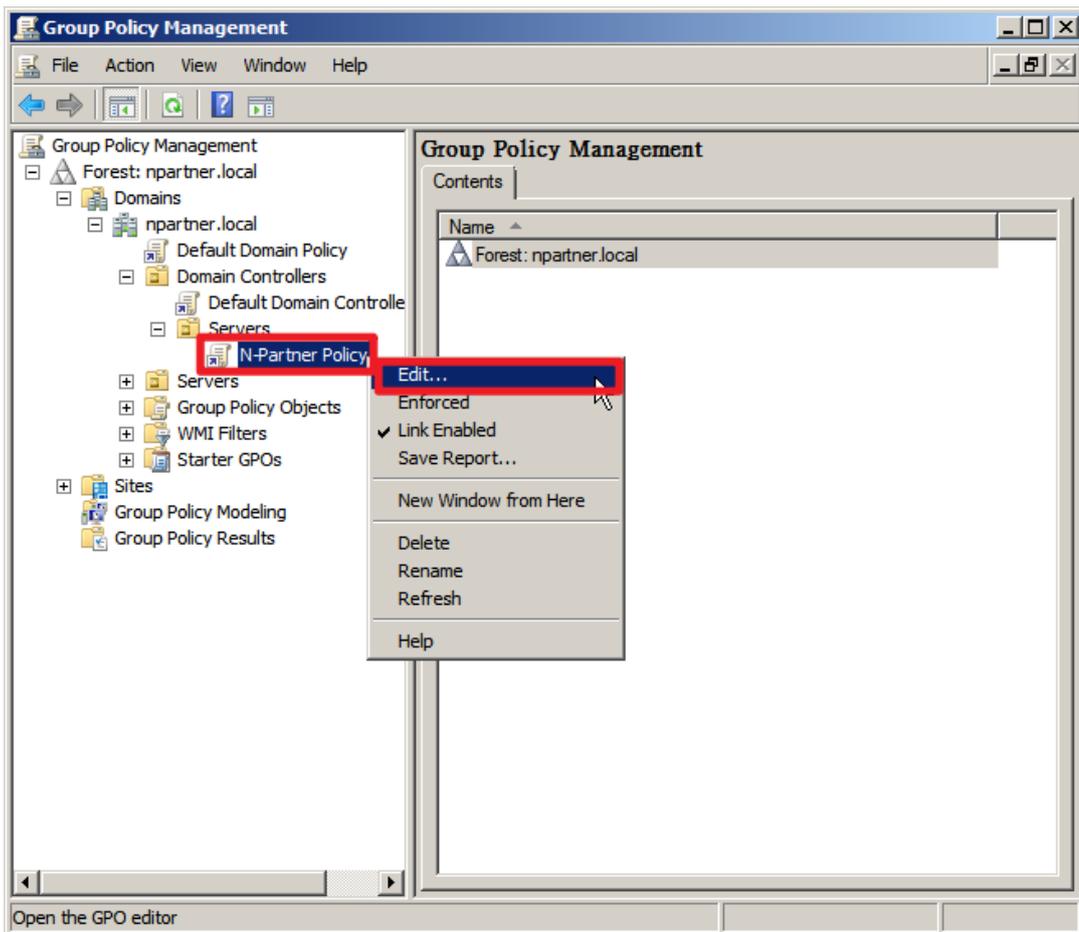


4.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

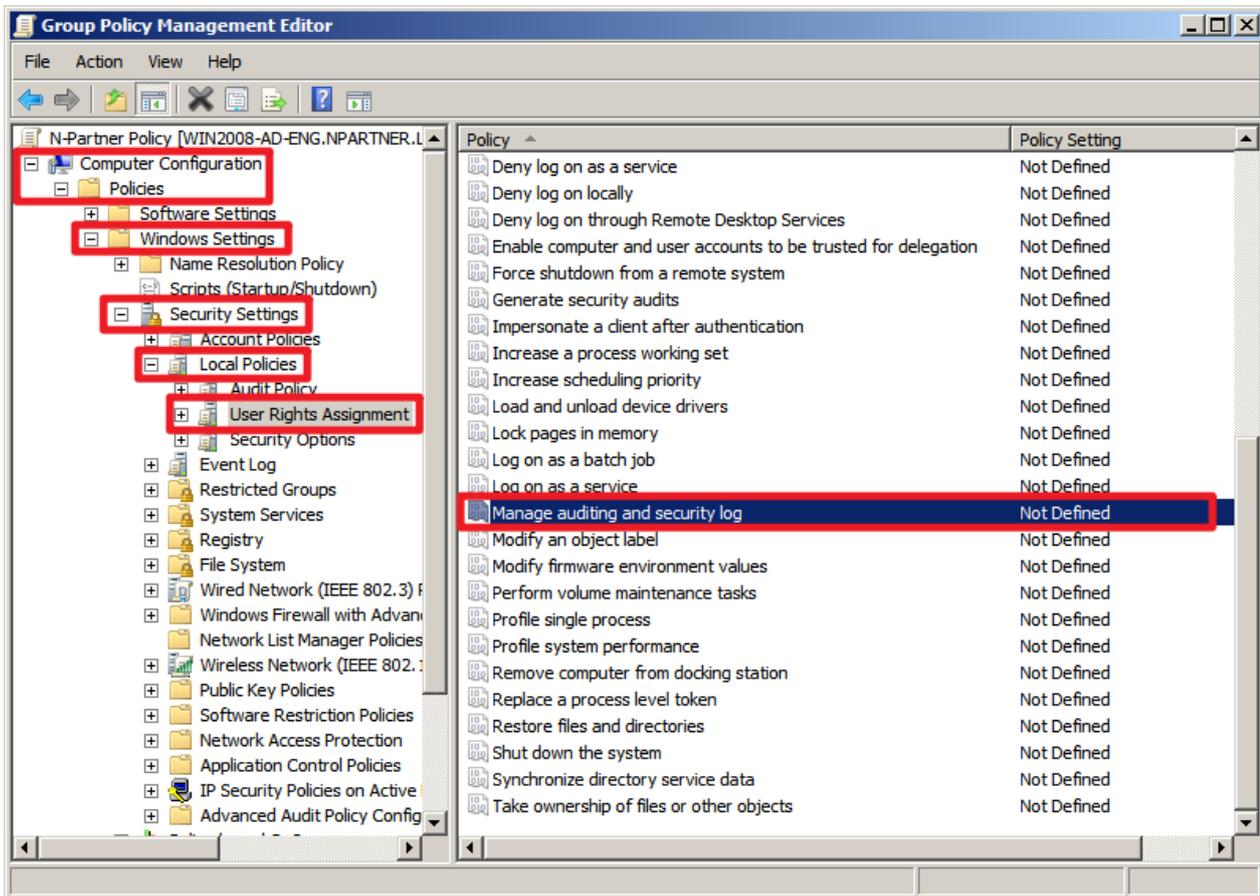


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



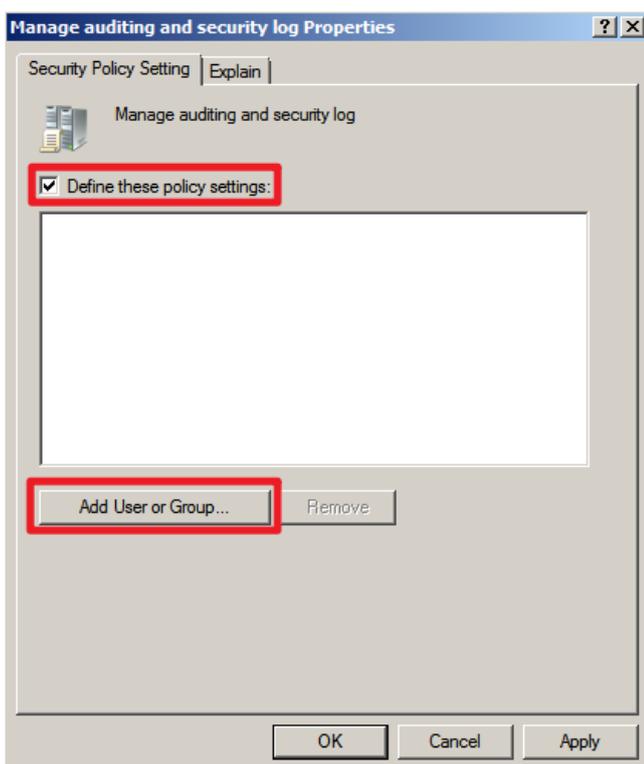
(3) Configure Auditing Log

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



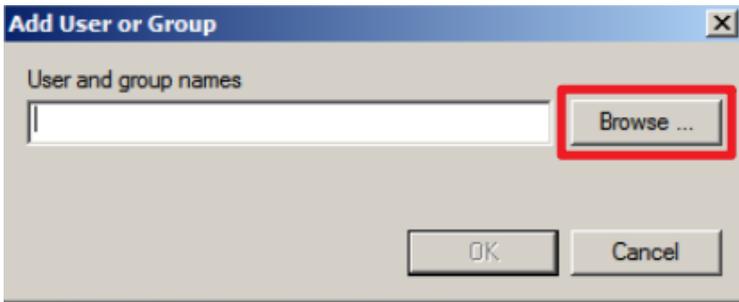
(4) Add Auditing User

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



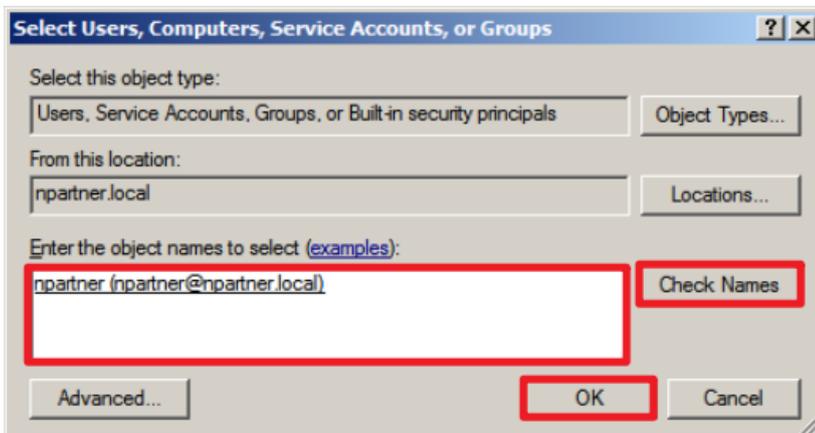
(5) Search for User

Click "Browse."

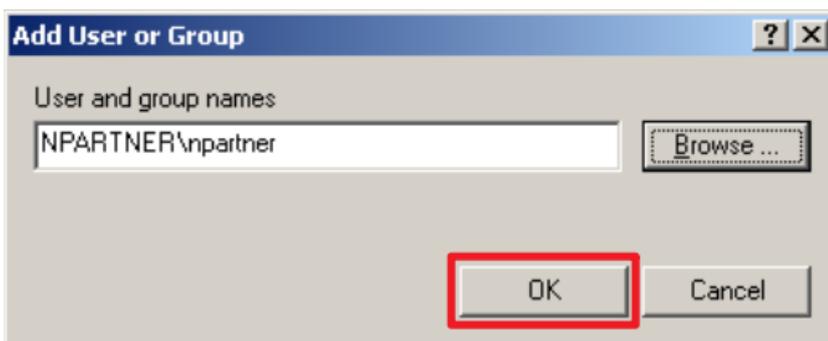


(6) Enter Your User Account

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

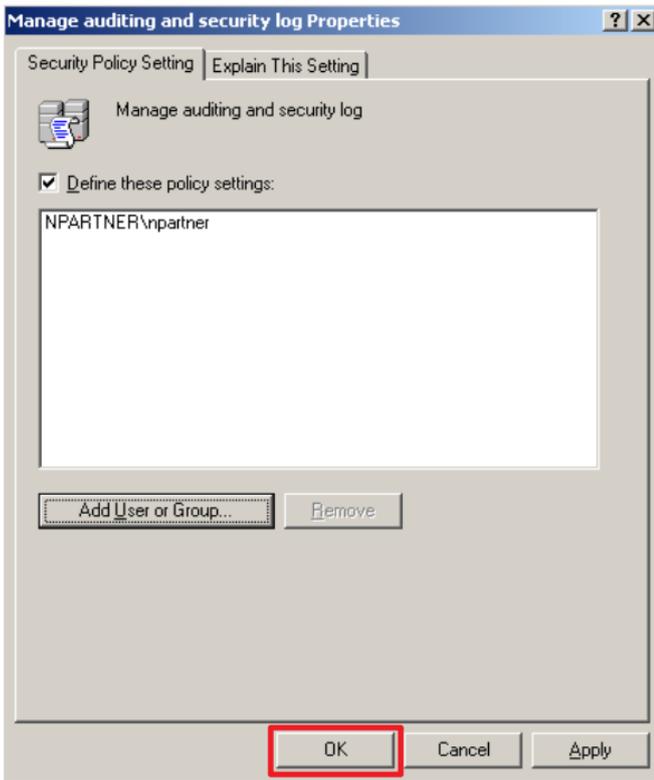


(7) Click "OK."



(8) Confirm Audit Log Settings

Click "OK."

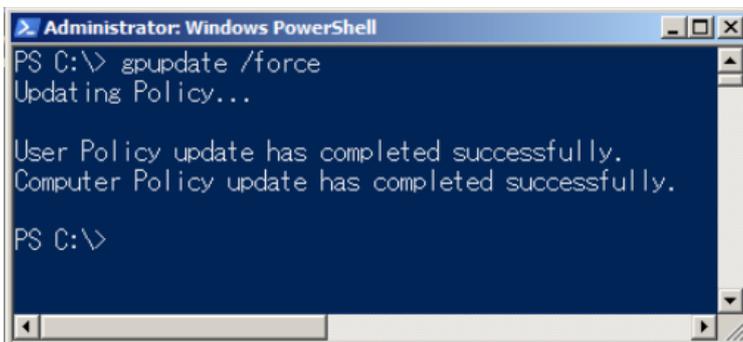


(9) Open "Windows Powershell."



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

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



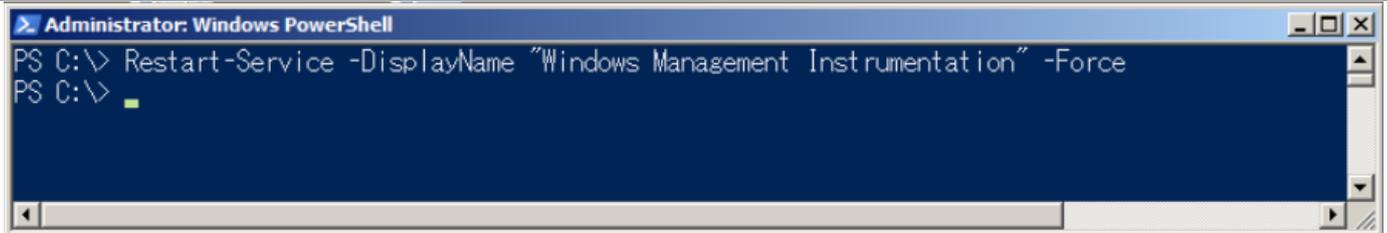
4.3.5 Restart the WMI Service

(1) Open "Windows Powershell."



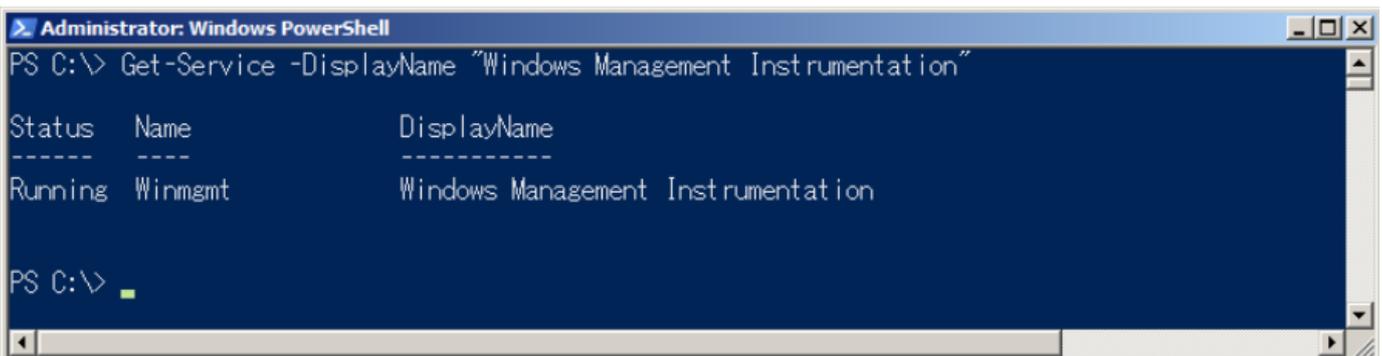
(2) Enter the command below to disable the WMI service.

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



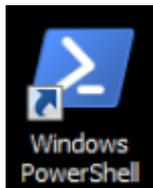
(3) Enter the command below to enable the WMI service.

```
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
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered is "netsh advfirewall firewall set rule group='windows management instrumentation (wmi)' new enable=yes". The output shows "Updated 4 rule(s). Ok." followed by a new prompt "PS C:\>".

```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
Updated 4 rule(s).
Ok.
PS C:\>
```

(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
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered is "netsh advfirewall firewall show rule name=all | Select-string -pattern 'Windows Management Instrumentation' -context 0,2". The output lists four firewall rules related to Windows Management Instrumentation (WMI) with their status and configuration details.

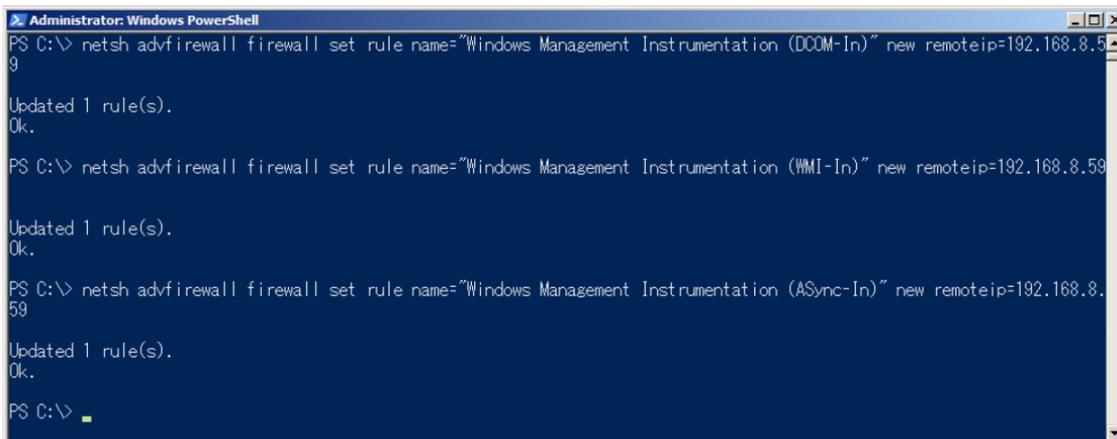
```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
> Rule Name: Windows Management Instrumentation (DCOM-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
Local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

(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
```

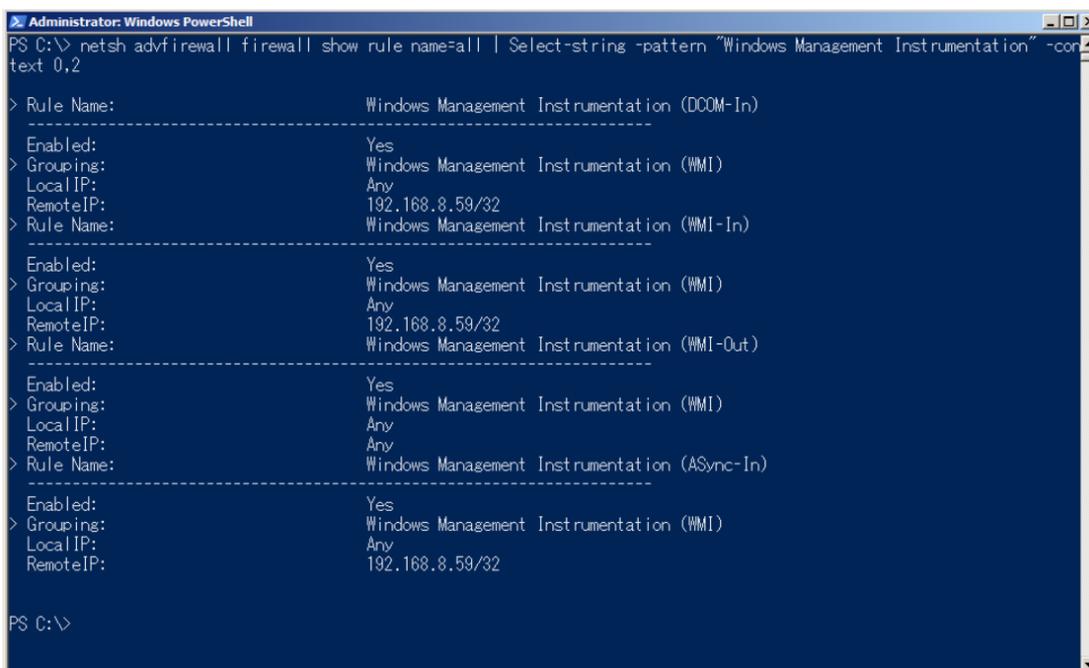


```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (DCOM-In)" new remoteip=192.168.8.59
Updated 1 rule(s).
Ok.
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (WMI-In)" new remoteip=192.168.8.59
Updated 1 rule(s).
Ok.
PS C:\> netsh advfirewall firewall set rule name="Windows Management Instrumentation (ASync-In)" new remoteip=192.168.8.59
Updated 1 rule(s).
Ok.
PS C:\>
```

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
```



```
Administrator: Windows PowerShell
PS C:\> netsh advfirewall firewall show rule name=all | Select-string -pattern "Windows Management Instrumentation" -context 0,2
> Rule Name: Windows Management Instrumentation (DCOM-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
Local IP: Any
Remote IP: 192.168.8.59/32
> Rule Name: Windows Management Instrumentation (WMI-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
Local IP: Any
Remote IP: 192.168.8.59/32
> Rule Name: Windows Management Instrumentation (WMI-Out)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
Local IP: Any
Remote IP: Any
> Rule Name: Windows Management Instrumentation (ASync-In)
-----
Enabled: Yes
> Grouping: Windows Management Instrumentation (WMI)
Local IP: Any
Remote IP: 192.168.8.59/32
PS C:\>
```

5. Windows Server 2012

Windows Audit Policy Configuration:

For detailed information, refer to the [Audit Policy Recommendations link](#) in the references.

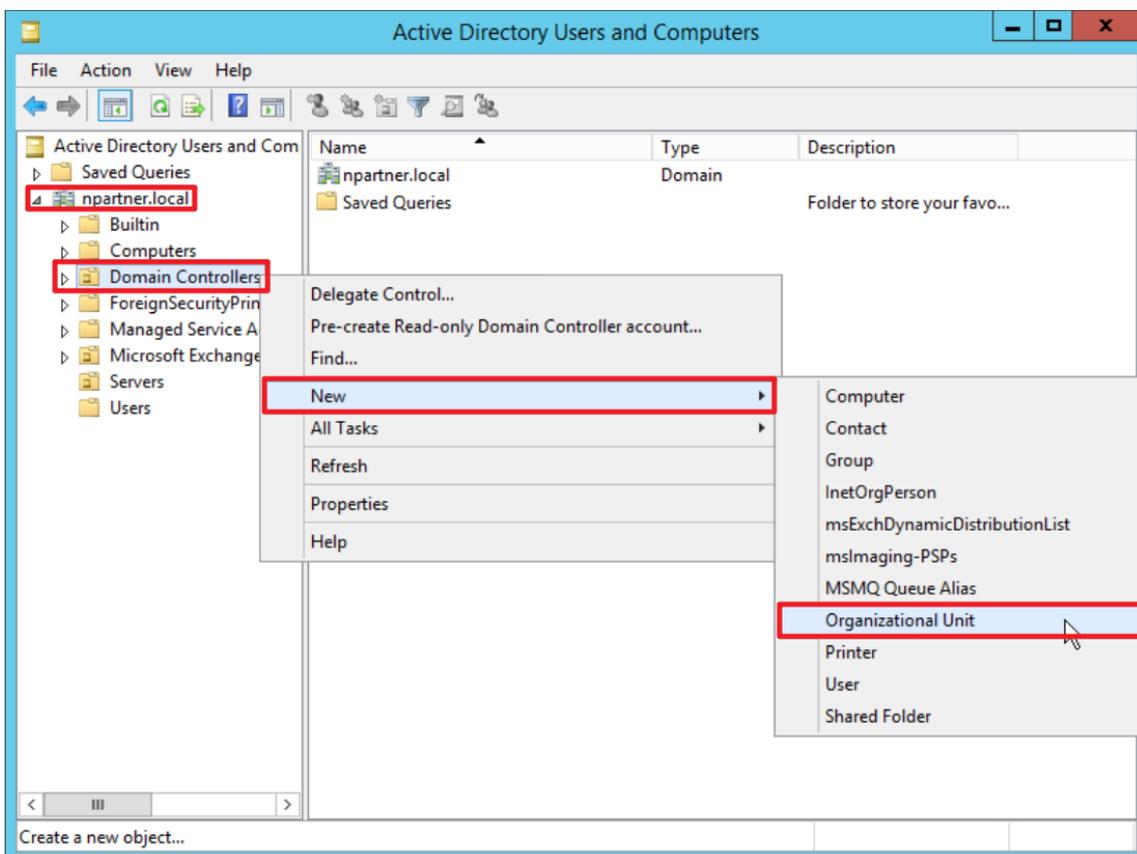
5.1 Organizational Unit (OU) Configuration

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



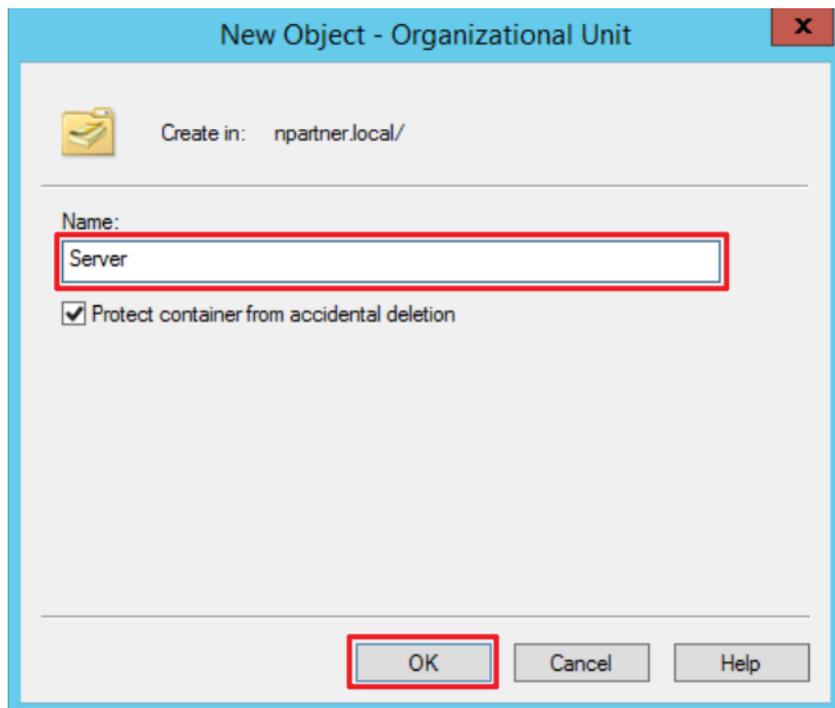
(2) Add an Organizational Unit

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”)

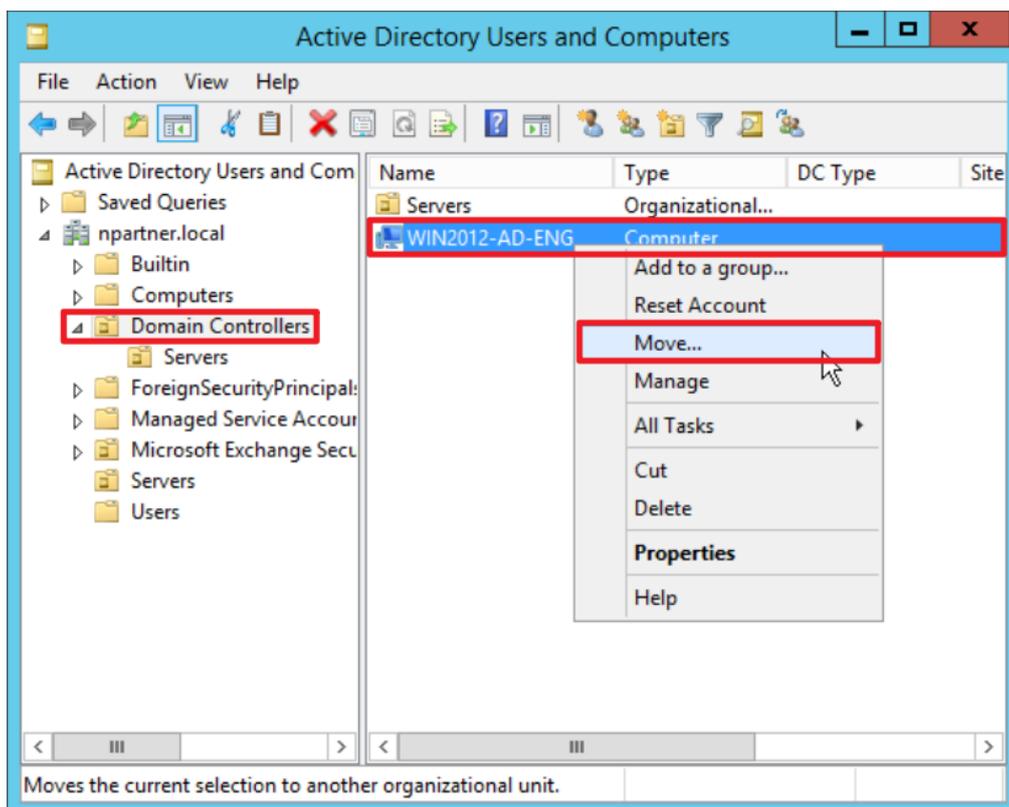
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

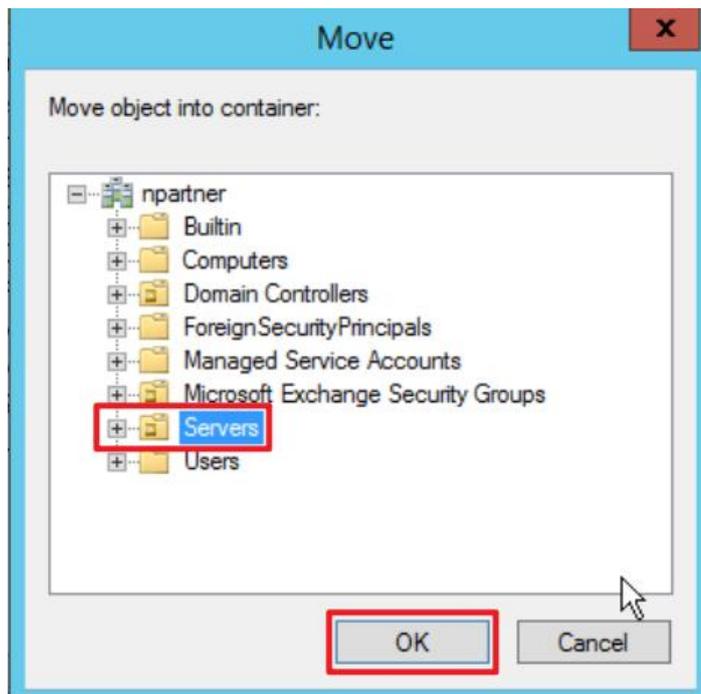
Select “Domain Controllers” → right-click on the “WIN2012-AD-ENG” server.

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



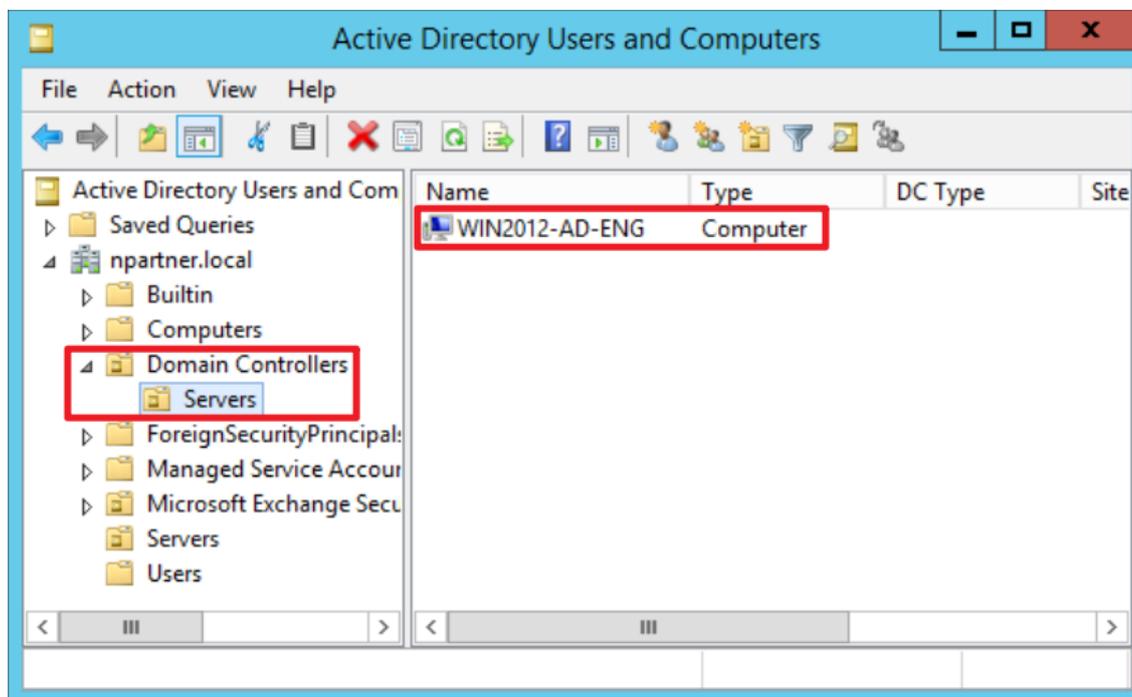
(5) Select your Organizational Unit:

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



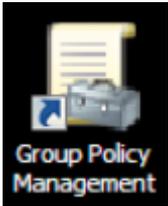
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



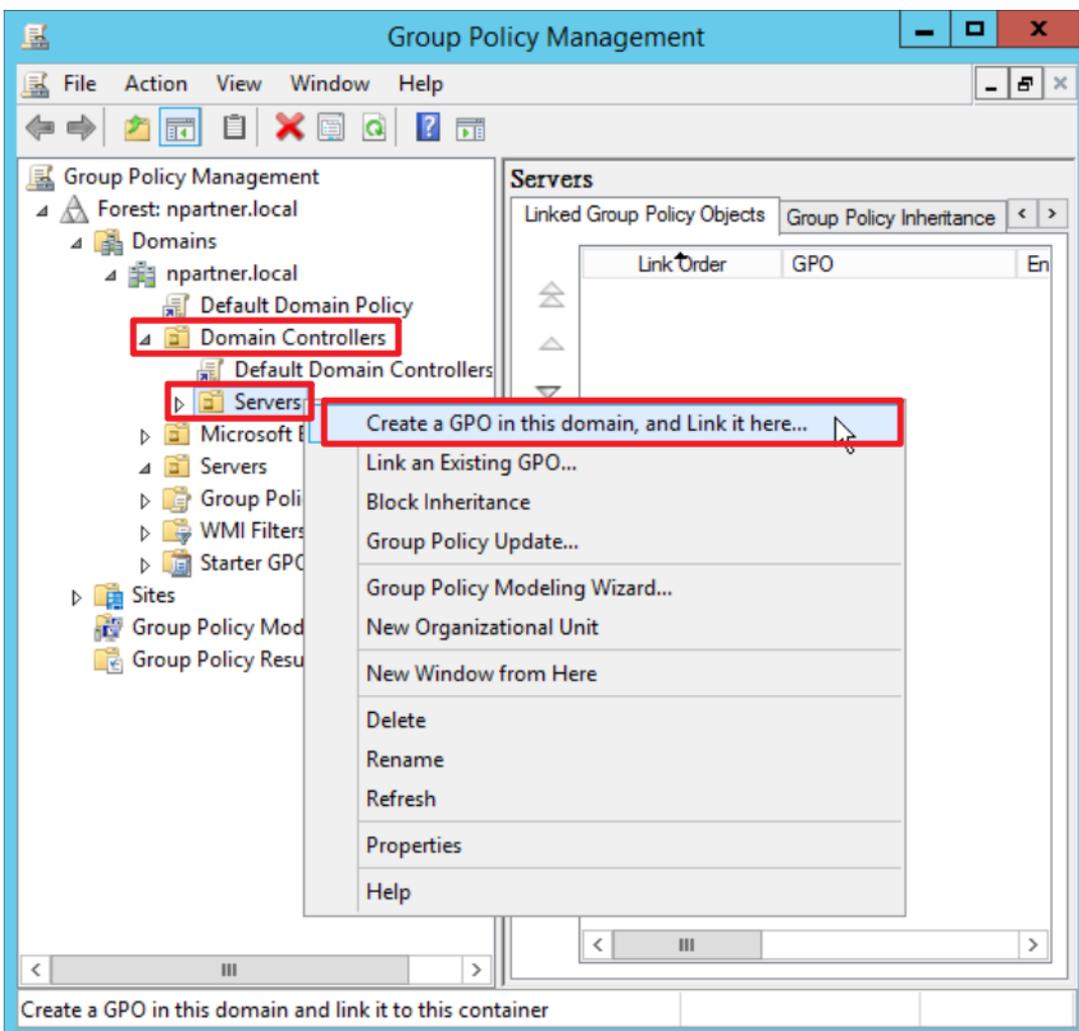
5.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

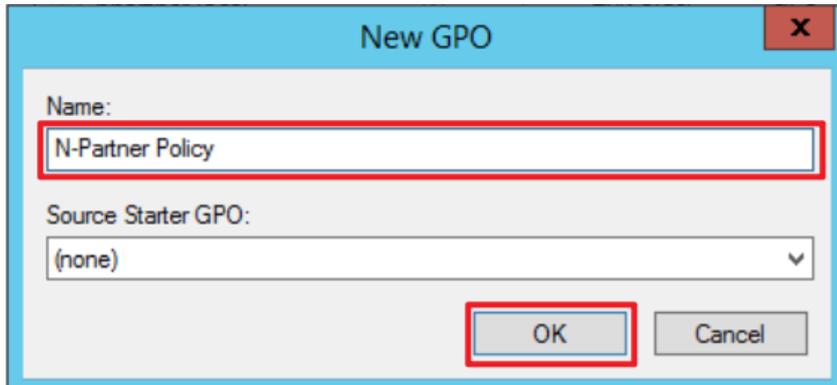
Right-click the “Servers” organizational unit under “Domain Controllers” → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

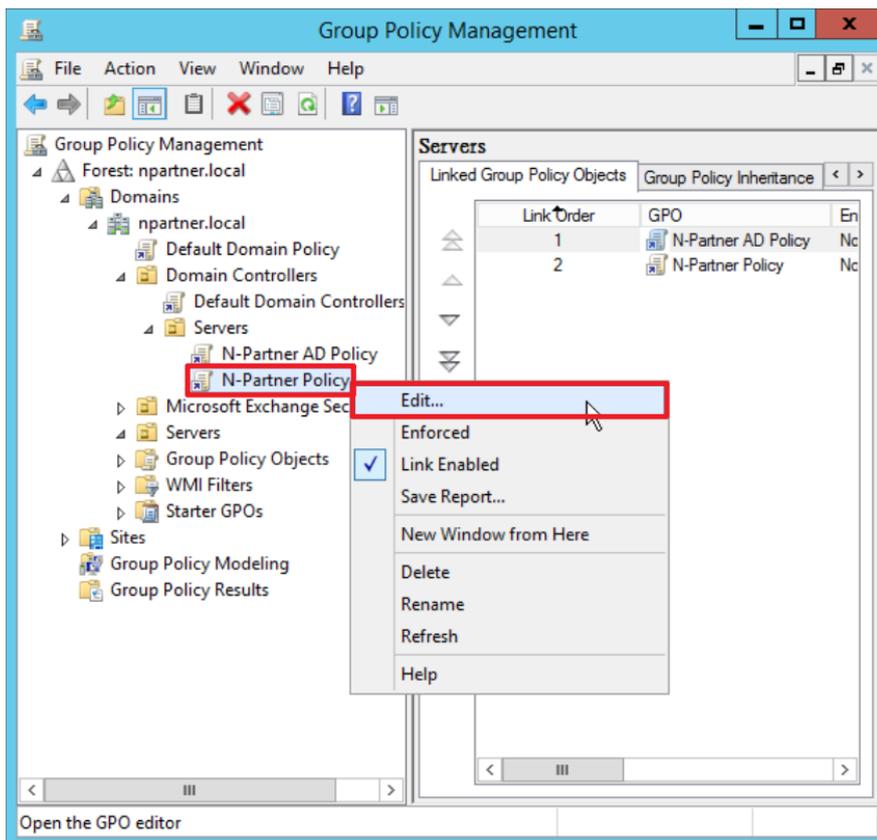
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



(4) Edit your Group Policy Object

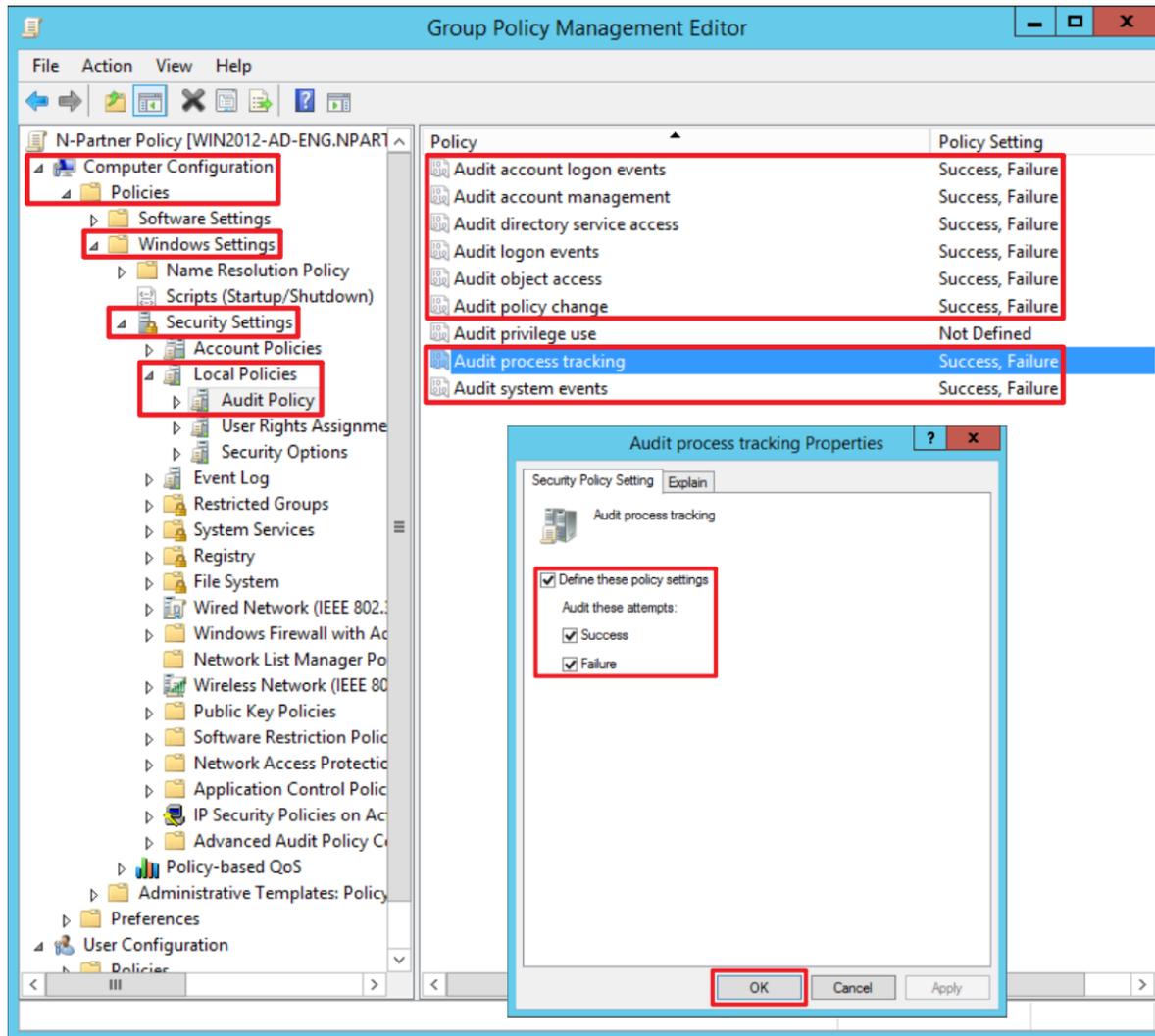
In your group policy object, (in this example, it is “N-Partner Policy”) right-click and select “Edit.”



(5) Local Group Policies: Audit Policy

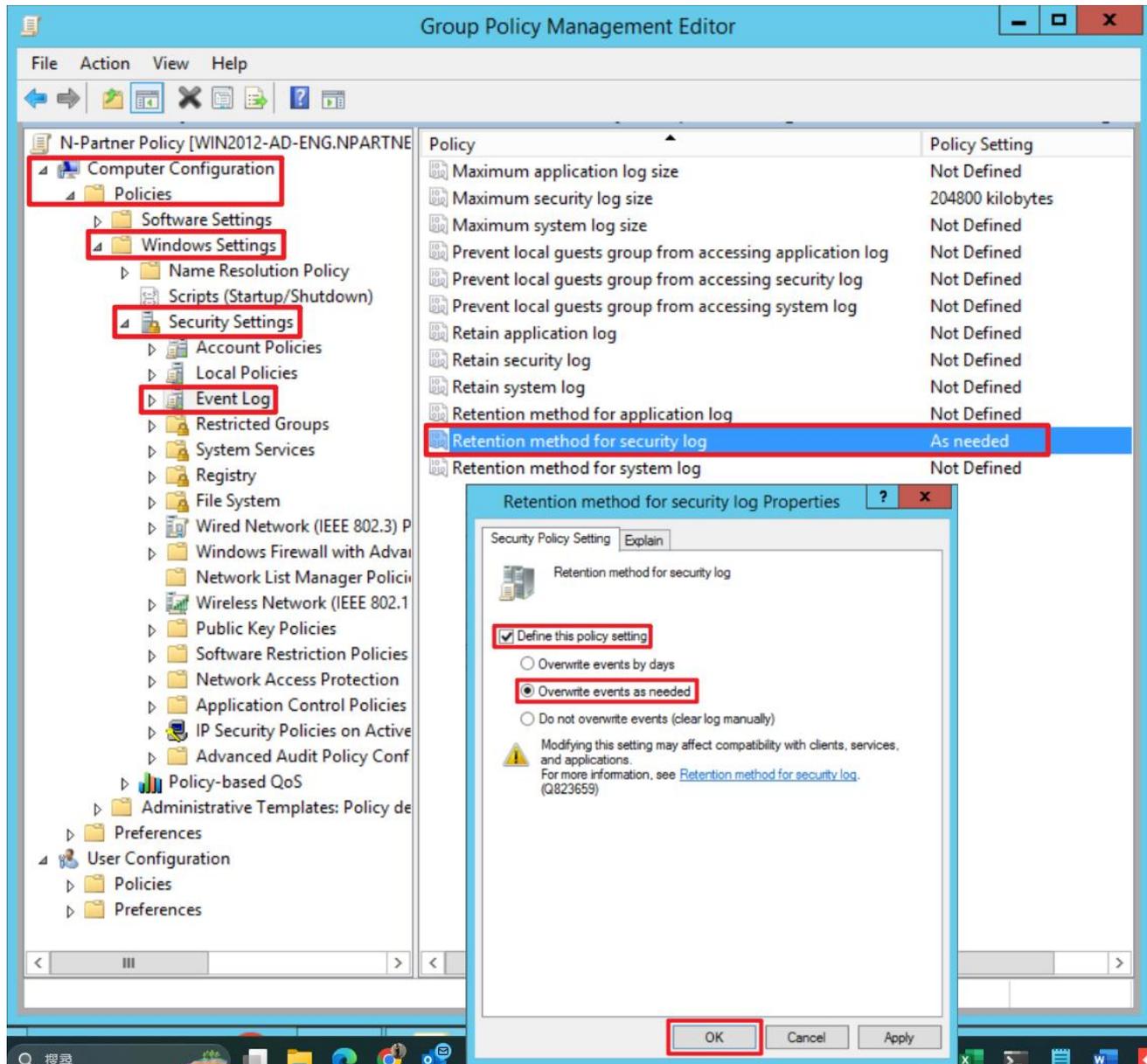
Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit directory service access,” “Audit logon events,” “Audit object access,” “Audit policy change,” “Audit process tracking” and “Audit system events” → check “Define these policy settings”:

Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

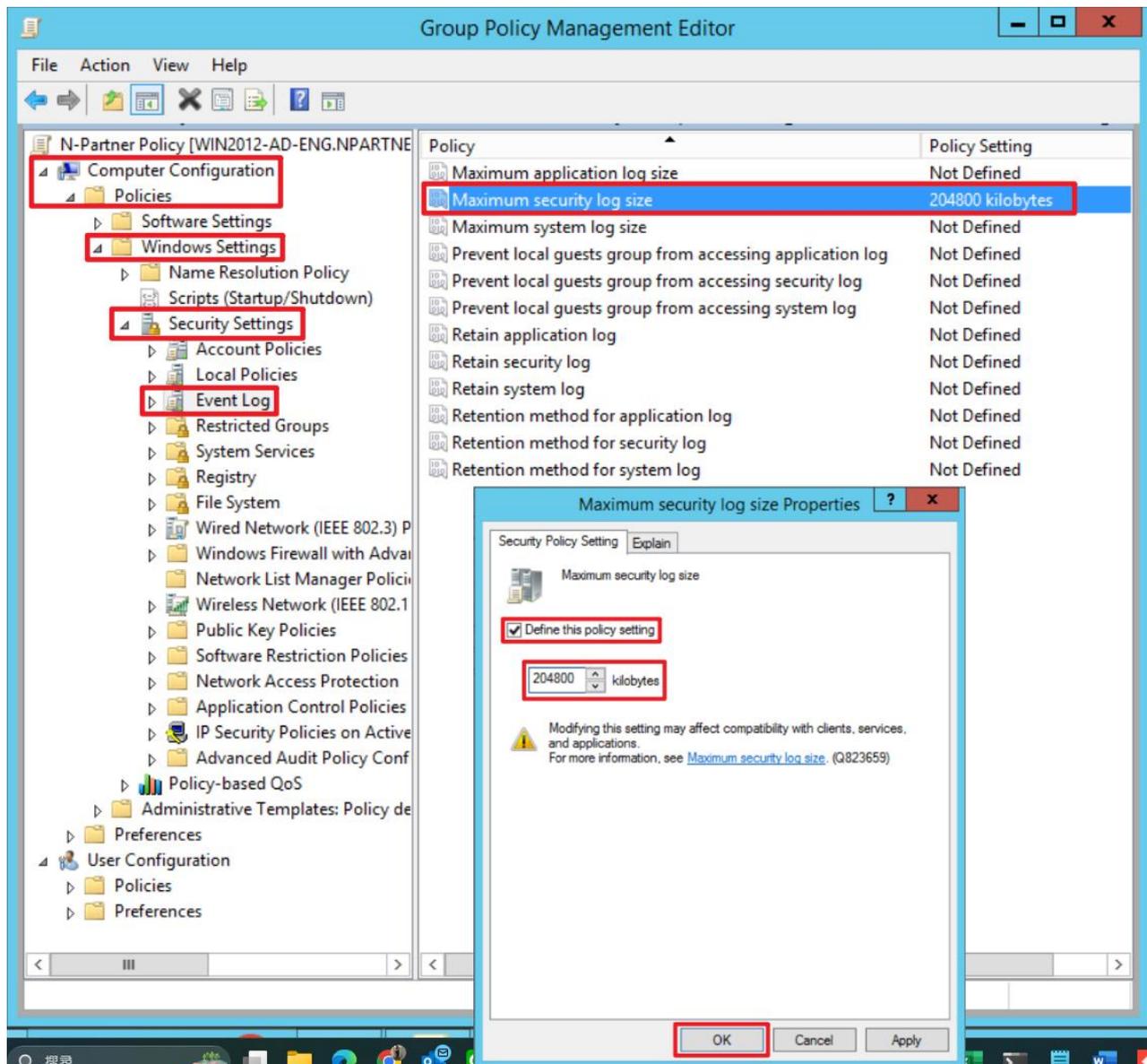
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

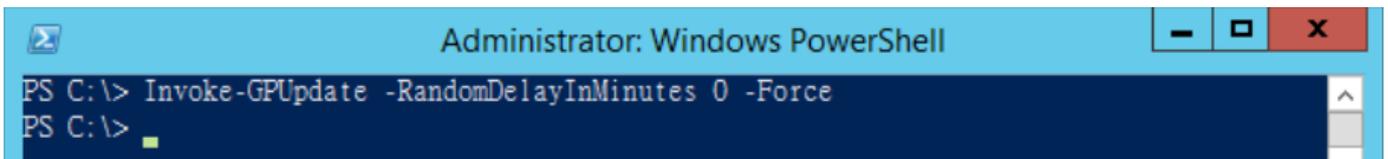


(8) On the AD domain server, open “Windows PowerShell.”



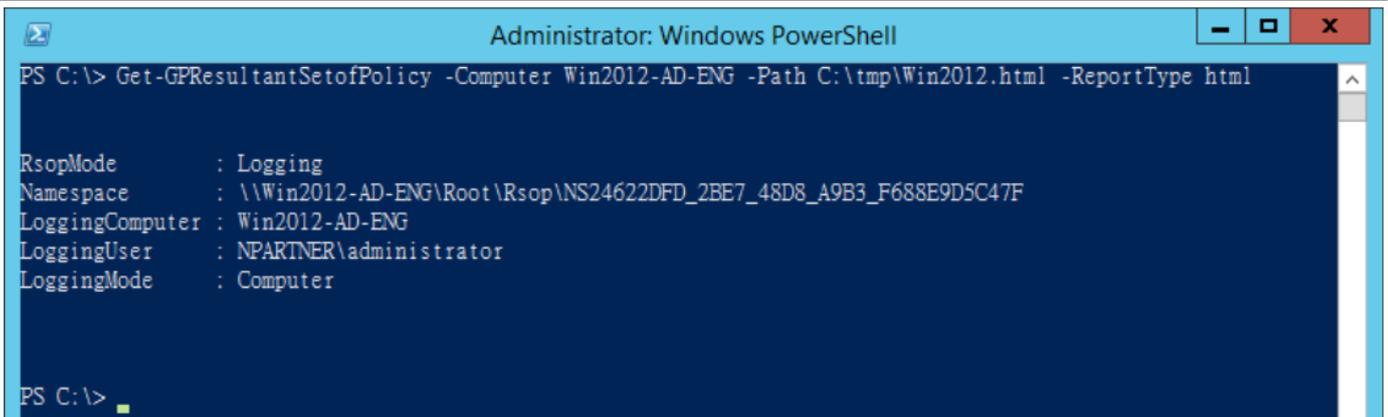
(9) Enter the command below to refresh group policy.

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



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

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



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

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

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

- Address bar: C:\tmp\Win2012.html
- Page title: NPARTNER\WIN2012-AD-E...
- Navigation tabs: General (show), Component Status (show), Settings (hide), Policies (hide), Windows Settings (hide), Security Settings (hide), Account Policies/Password Policy (show), Account Policies/Account Lockout Policy (show), Account Policies/Kerberos Policy (show), Local Policies/Audit Policy (hide), Local Policies/User Rights Assignment (show), Local Policies/Security Options (show), Event Log (hide).
- Local Policies/Audit Policy Table:**

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner AD Policy
Audit account management	Success, Failure	N-Partner AD Policy
Audit directory service access	Success, Failure	N-Partner AD Policy
Audit logon events	Success, Failure	N-Partner AD Policy
Audit object access	Success, Failure	N-Partner AD Policy
Audit policy change	Success, Failure	N-Partner AD Policy
Audit process tracking	Success, Failure	N-Partner AD Policy
Audit system events	Success, Failure	N-Partner AD Policy
- Local Policies/Security Options Table:**

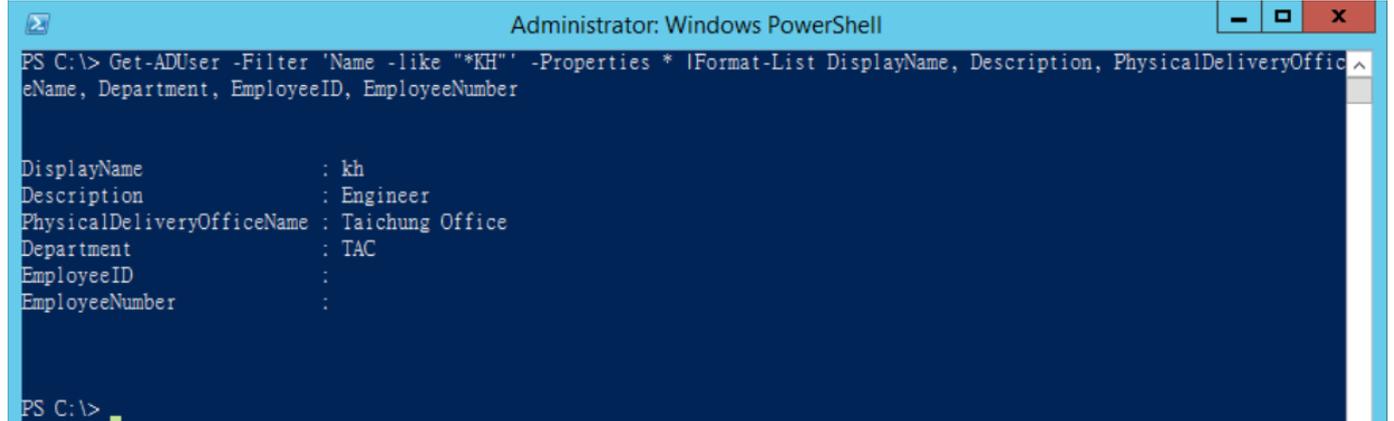
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner AD Policy
Retention method for security log	As needed	N-Partner AD Policy

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	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

5.3.1 Add Non-Admin Accounts

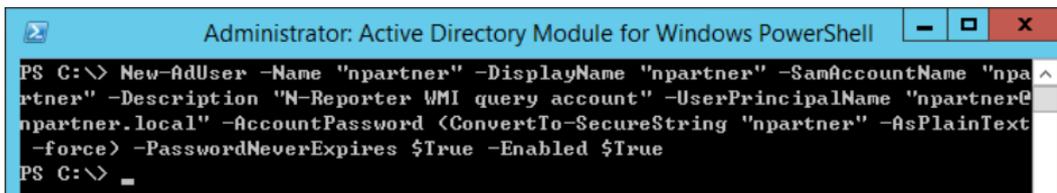
(1) Open “Active Directory Module for Windows PowerShell.”



(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
```

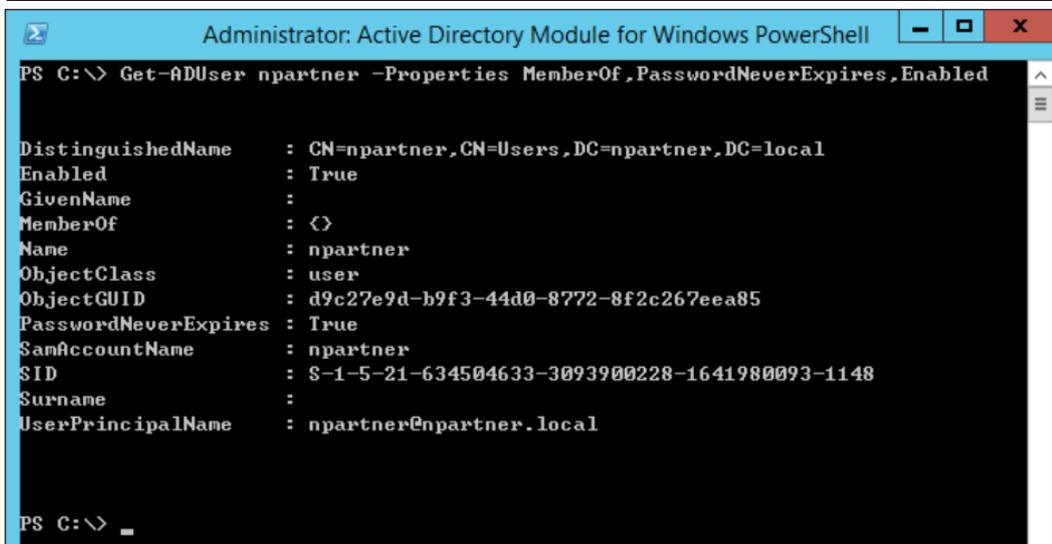


```
Administrator: Active Directory Module for Windows PowerShell
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText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

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
```



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\> Get-ADUser npartner -Properties MemberOf,PasswordNeverExpires,Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
MemberOf                : {}
Name                   : npartner
ObjectClass             : user
ObjectGUID              : d9c27e9d-b9f3-44d0-8772-8f2c267eea85
PasswordNeverExpires   : True
SamAccountName         : npartner
SID                    : S-1-5-21-634504633-3093900228-1641980093-1148
Surname                 :
UserPrincipalName      : npartner@npartner.local

PS C:\> _
```

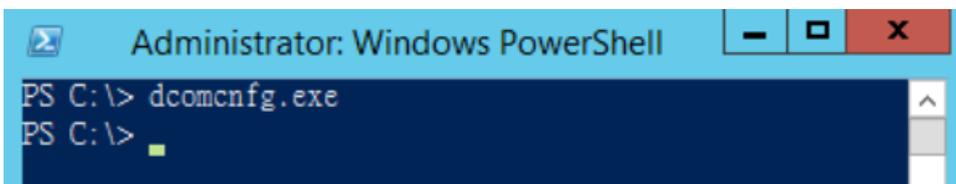
5.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”



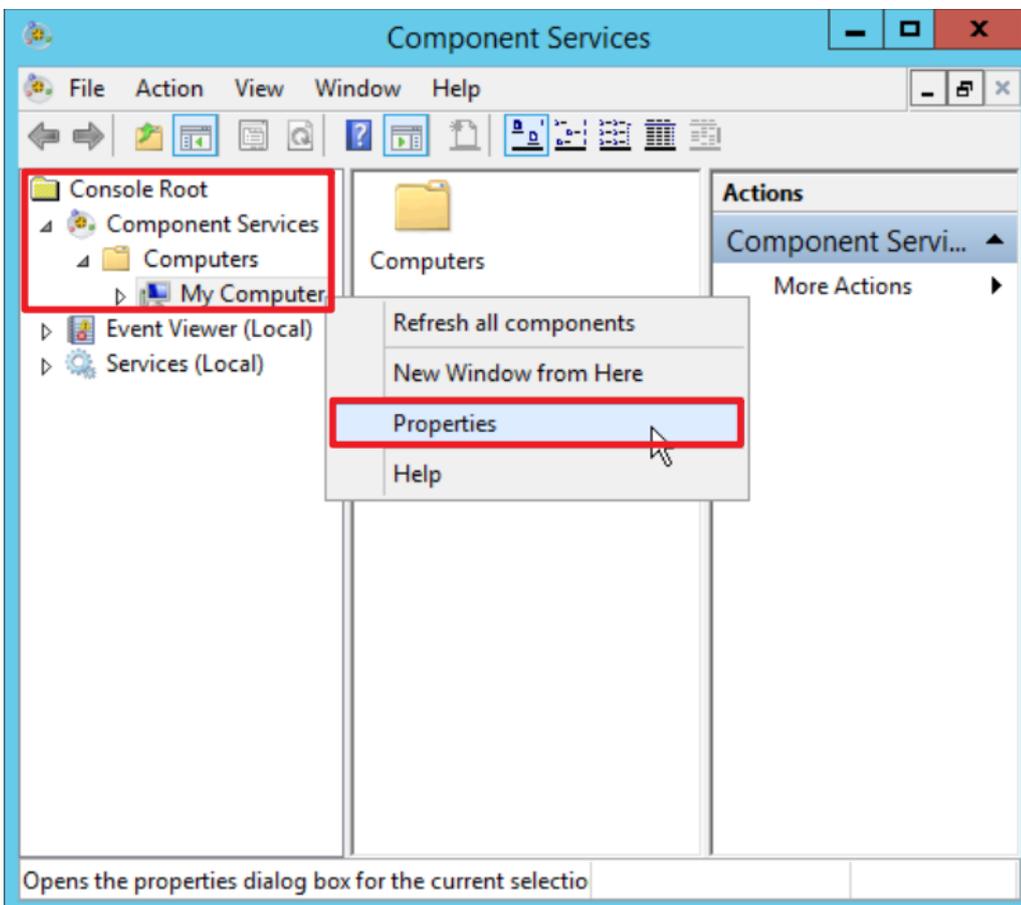
(2) Enter the command below to enable component services.

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



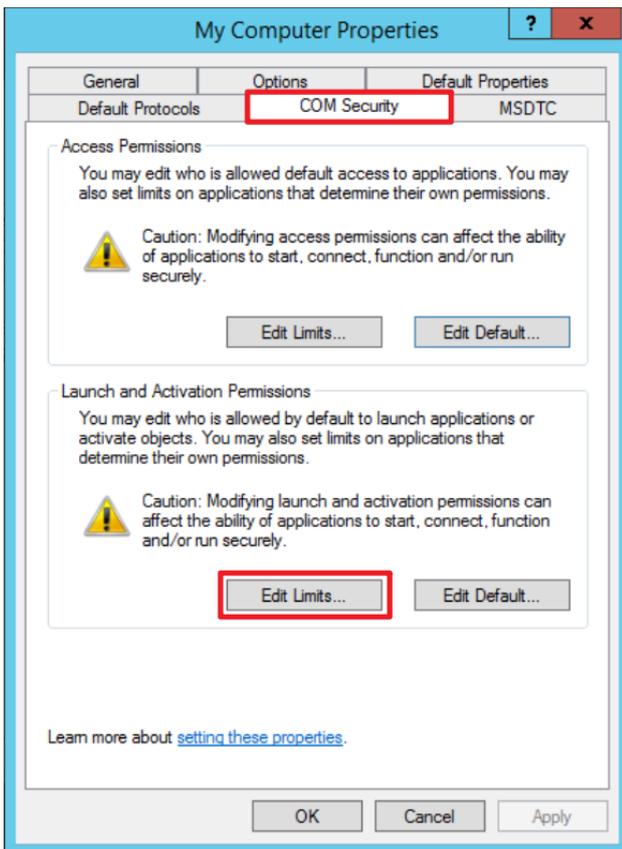
(3) Edit Computer Properties

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



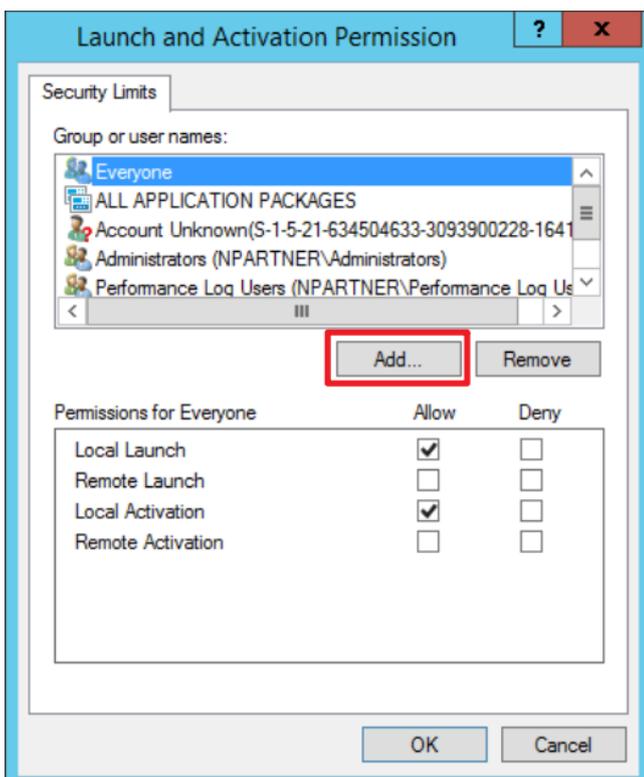
(4) Enable Permissions

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



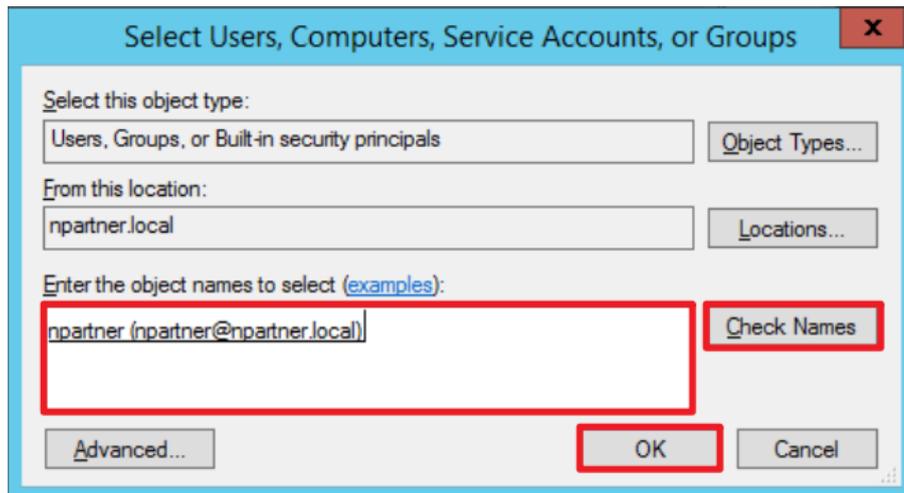
(5) Add DCOM User Permissions

Click "Add."



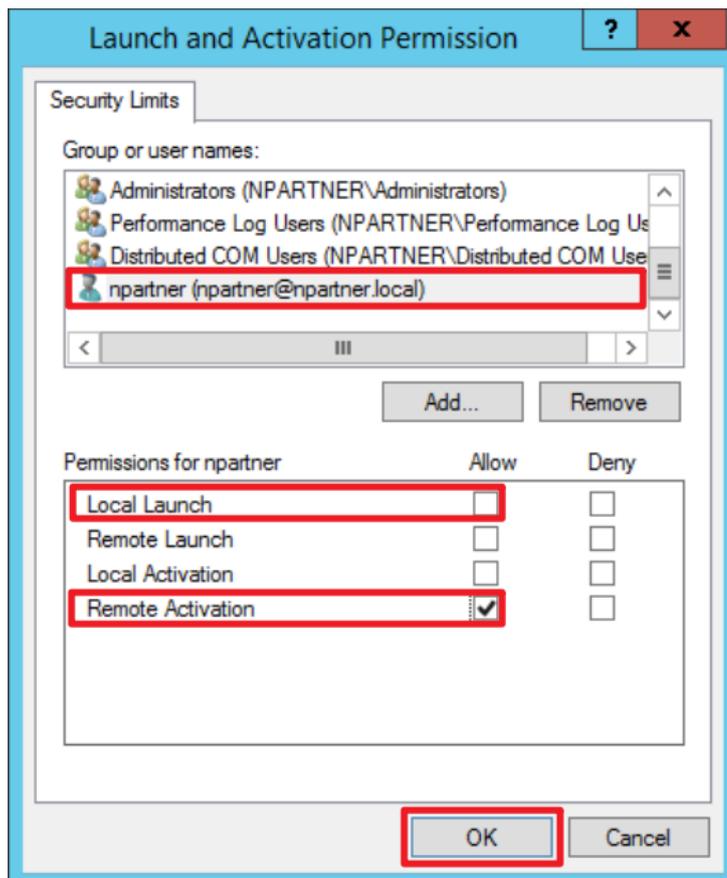
(6) Enter Your Username

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

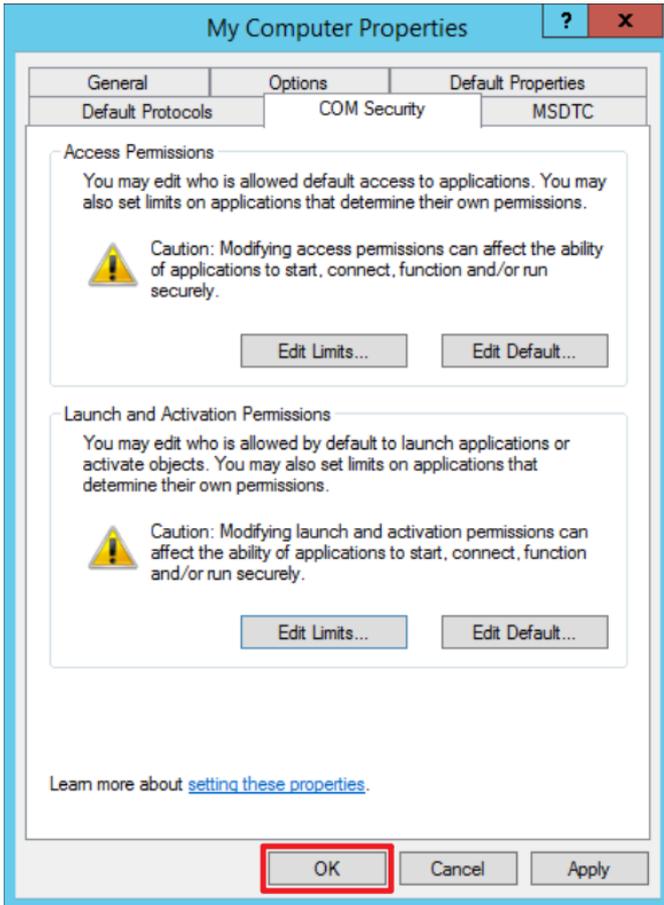


(7) Configure your User Permission

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

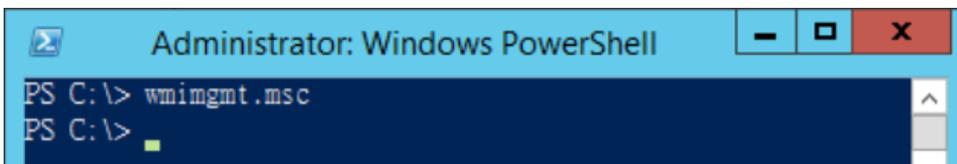
5.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



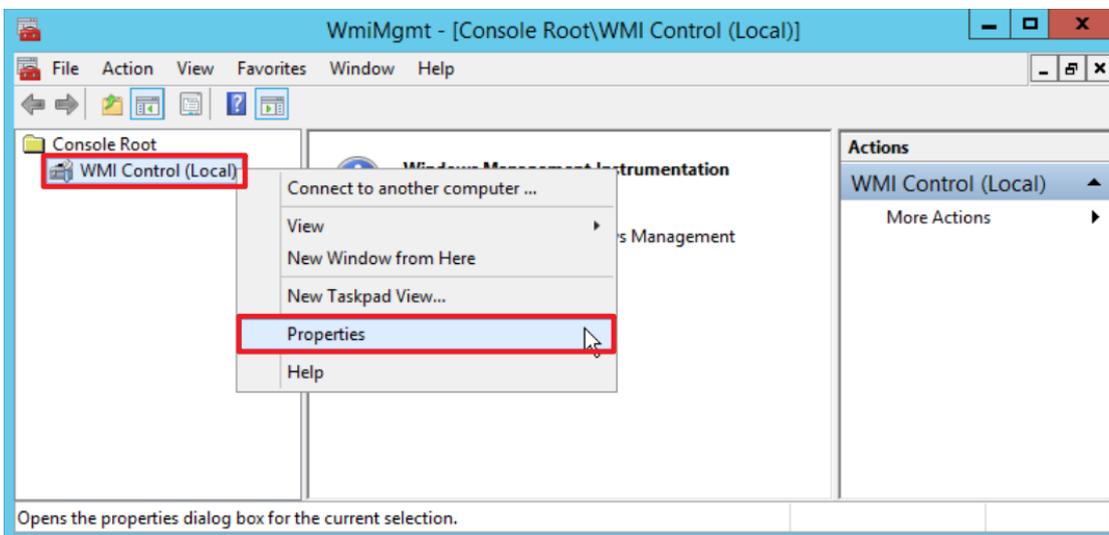
(2) Enter the command to enable WMI control service.

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



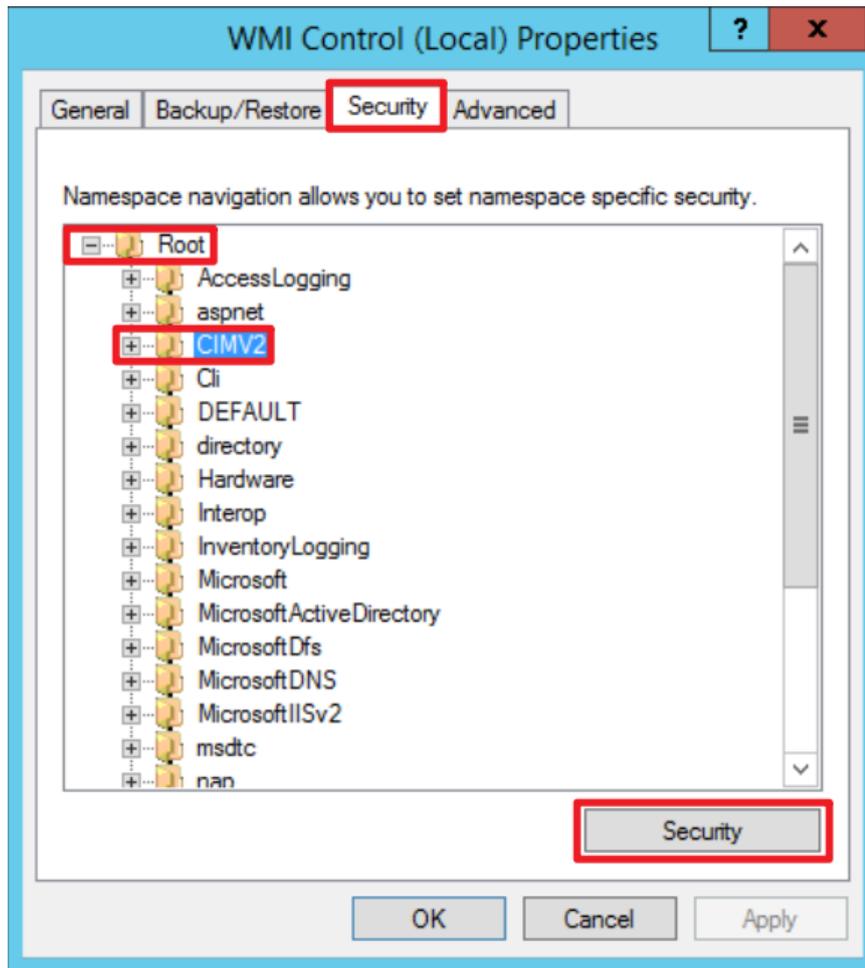
(3) Edit WMI Control

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



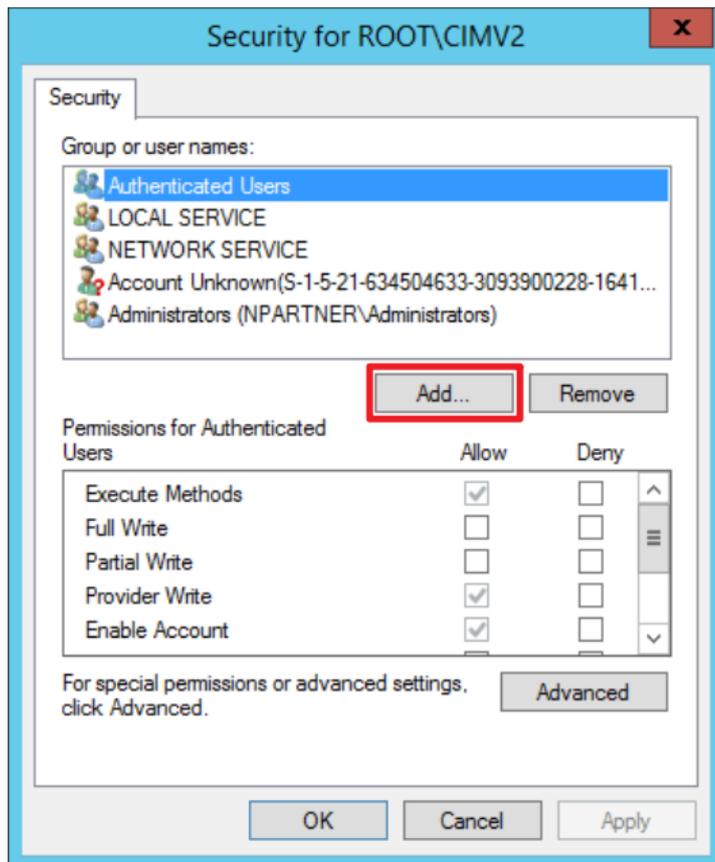
(4) Edit CIMV2 Security

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



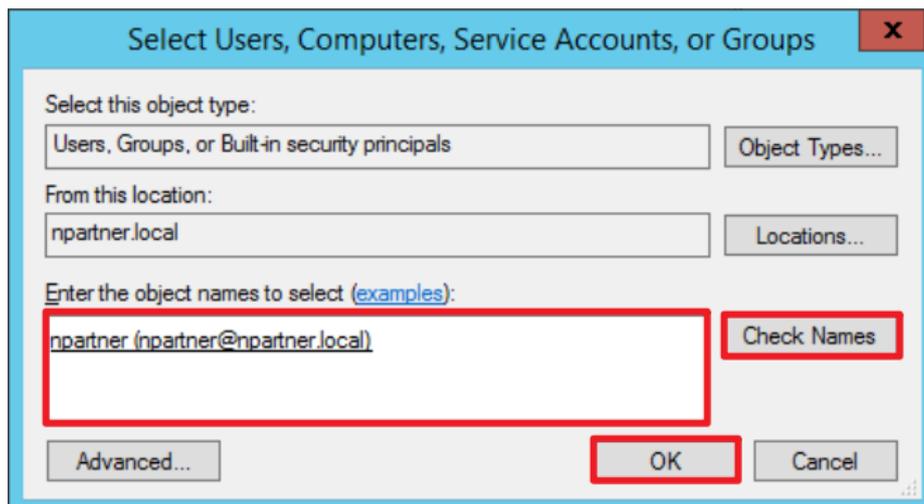
(5) Add WMI User Permissions.

Click "Add."



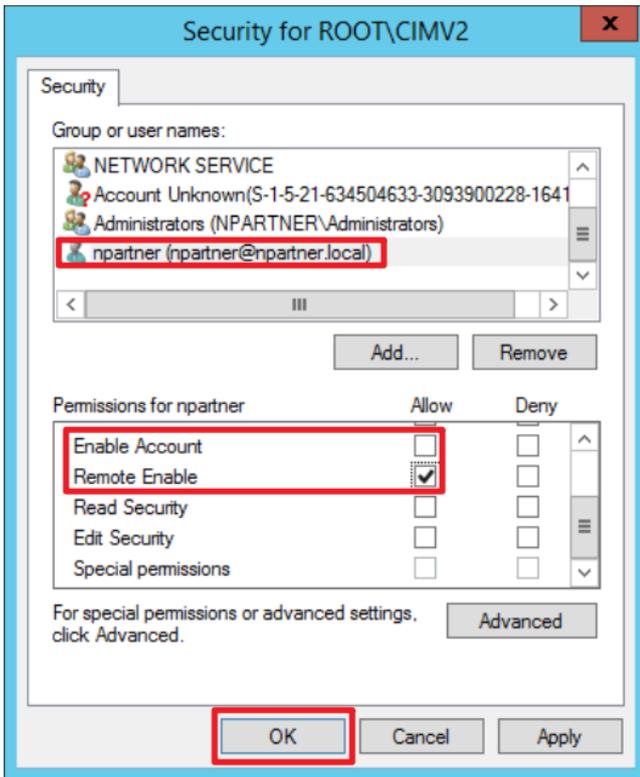
(6) Enter Your Username

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

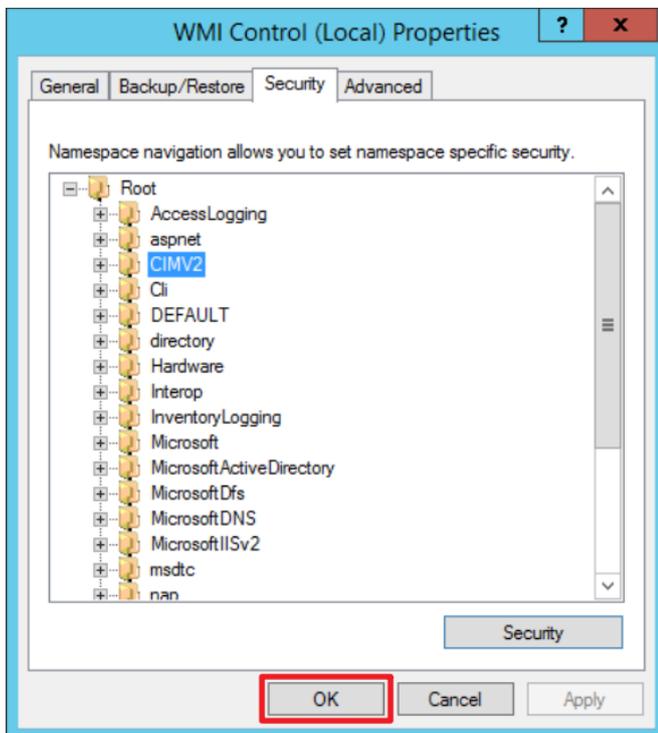


(7) Set Your User Permissions

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



(8) Click “OK.”



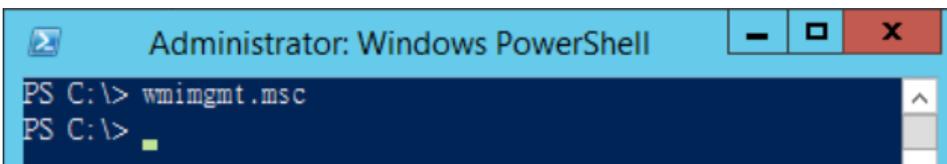
5.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



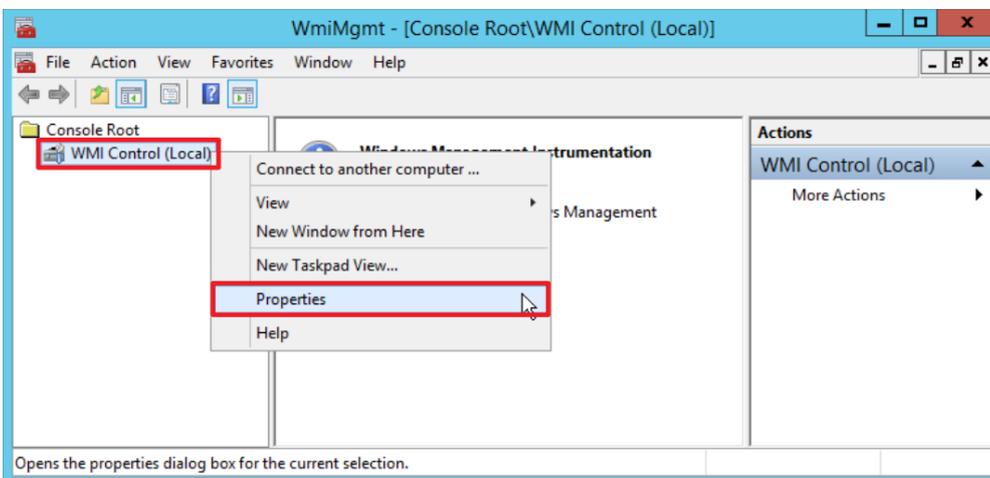
(2) Enter the command below to enable WMI Control.

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



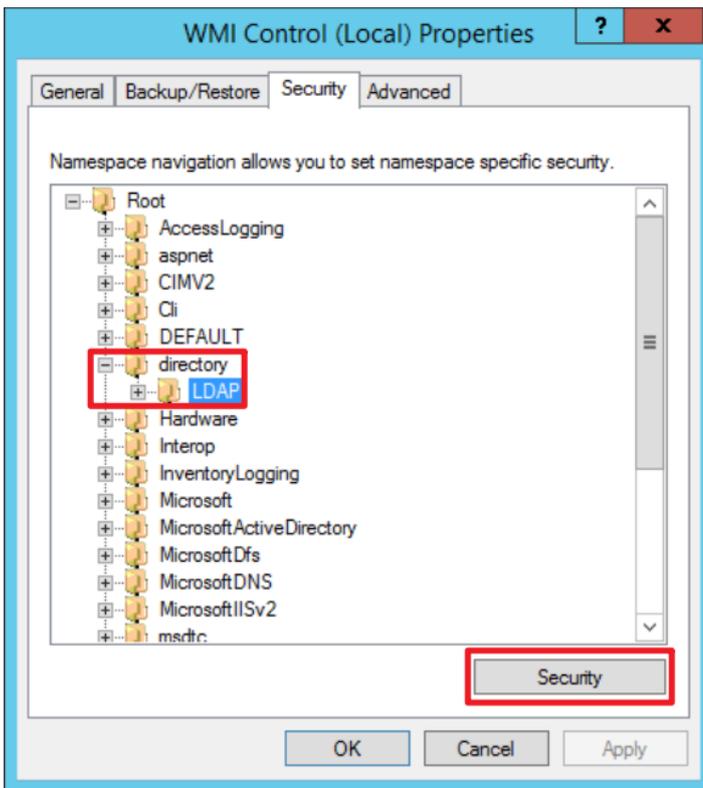
(3) Edit WMI Control

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



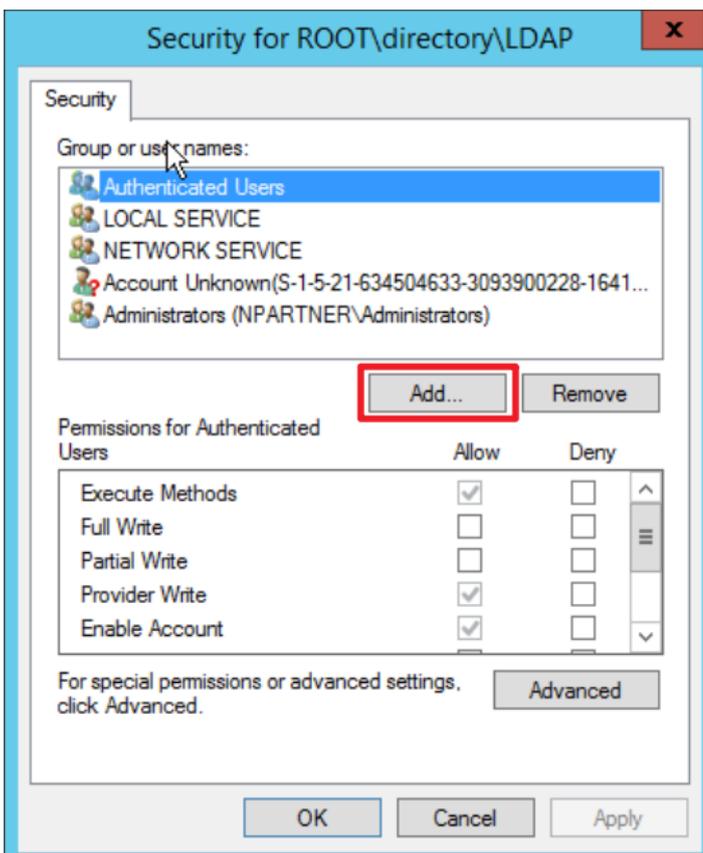
(4) Edit LDAP Security

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



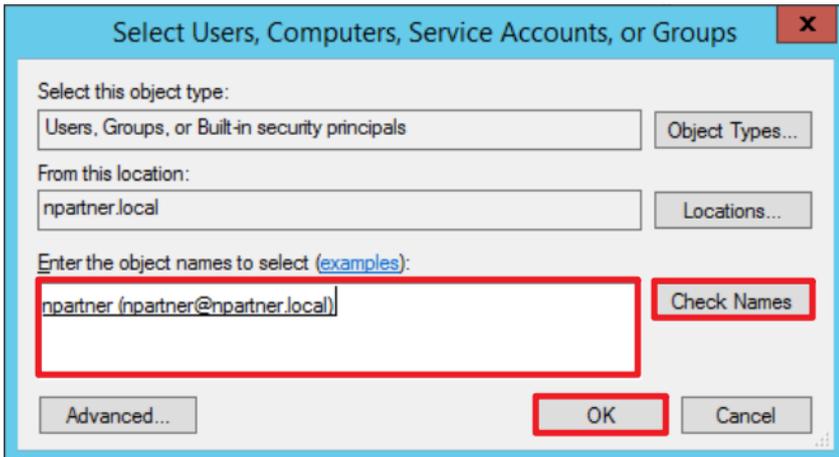
(5) Add WMI User Permissions

Click "Add."



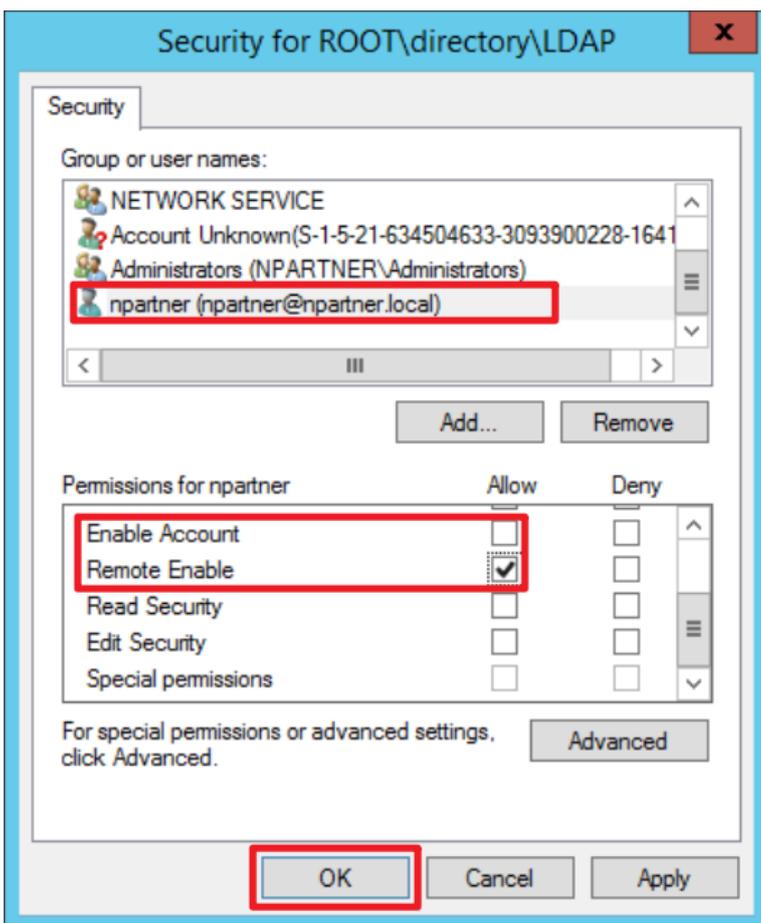
(6) Enter Your Username

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

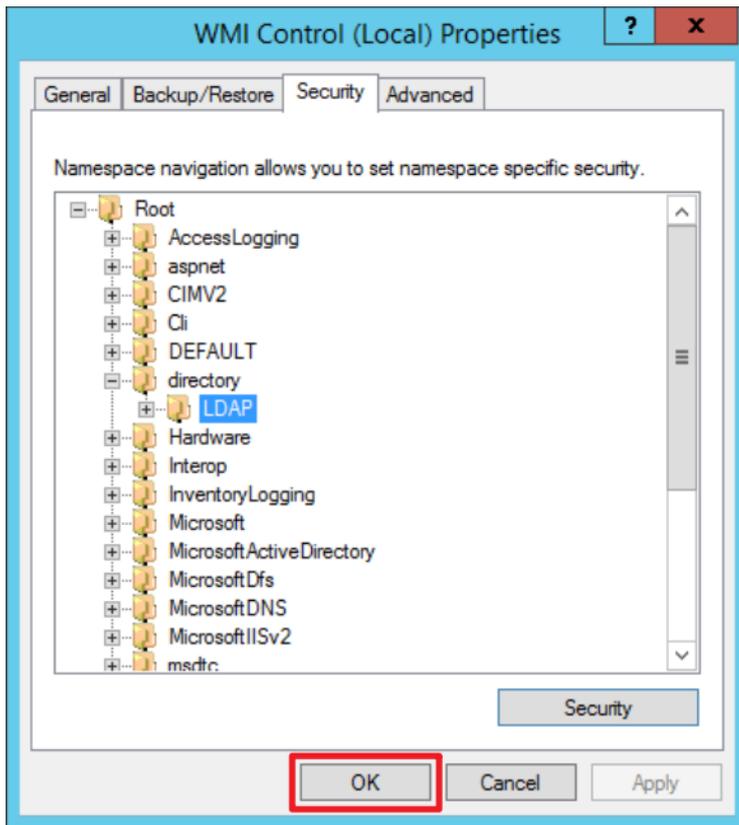


(7) Set Your User Permissions

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

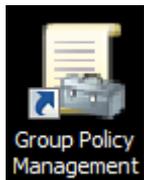


(8) Click "OK."

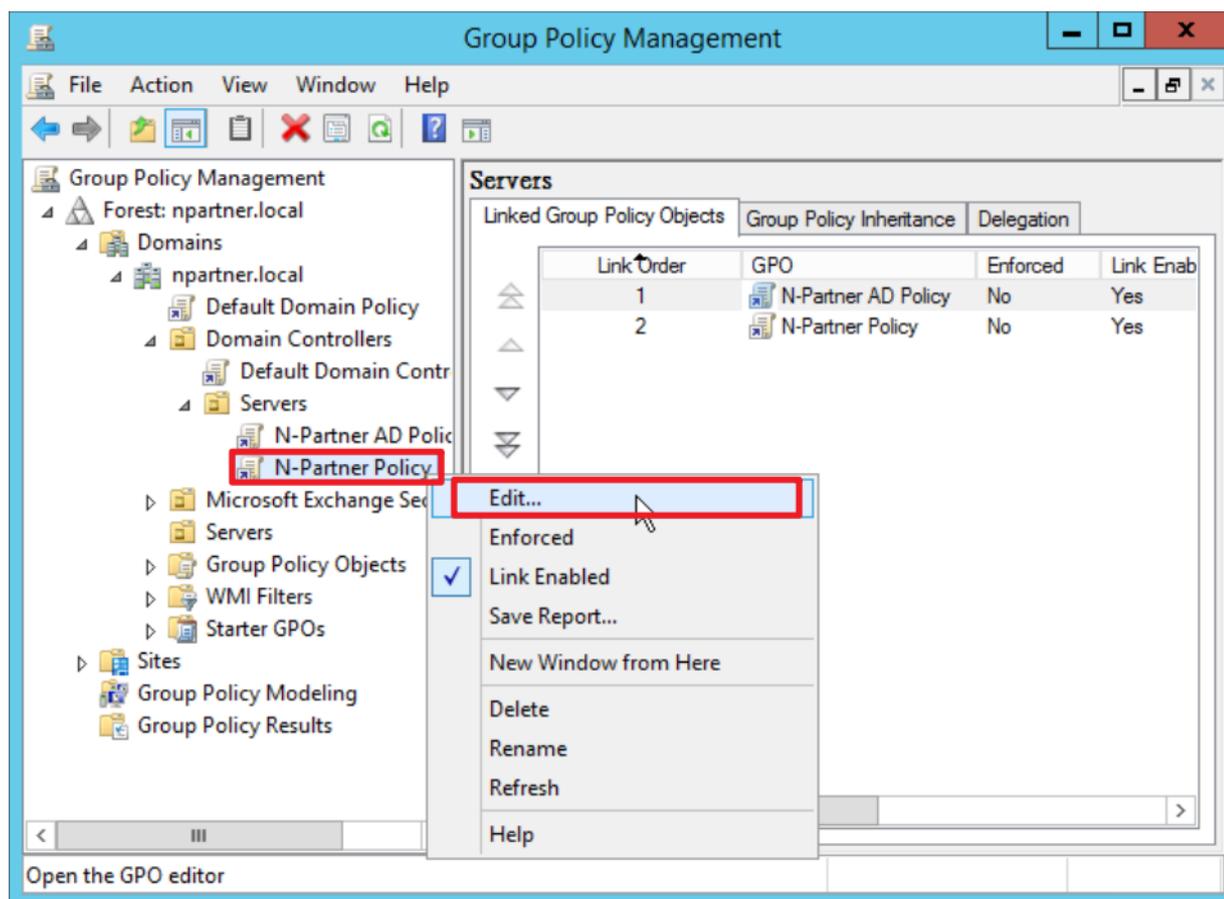


5.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

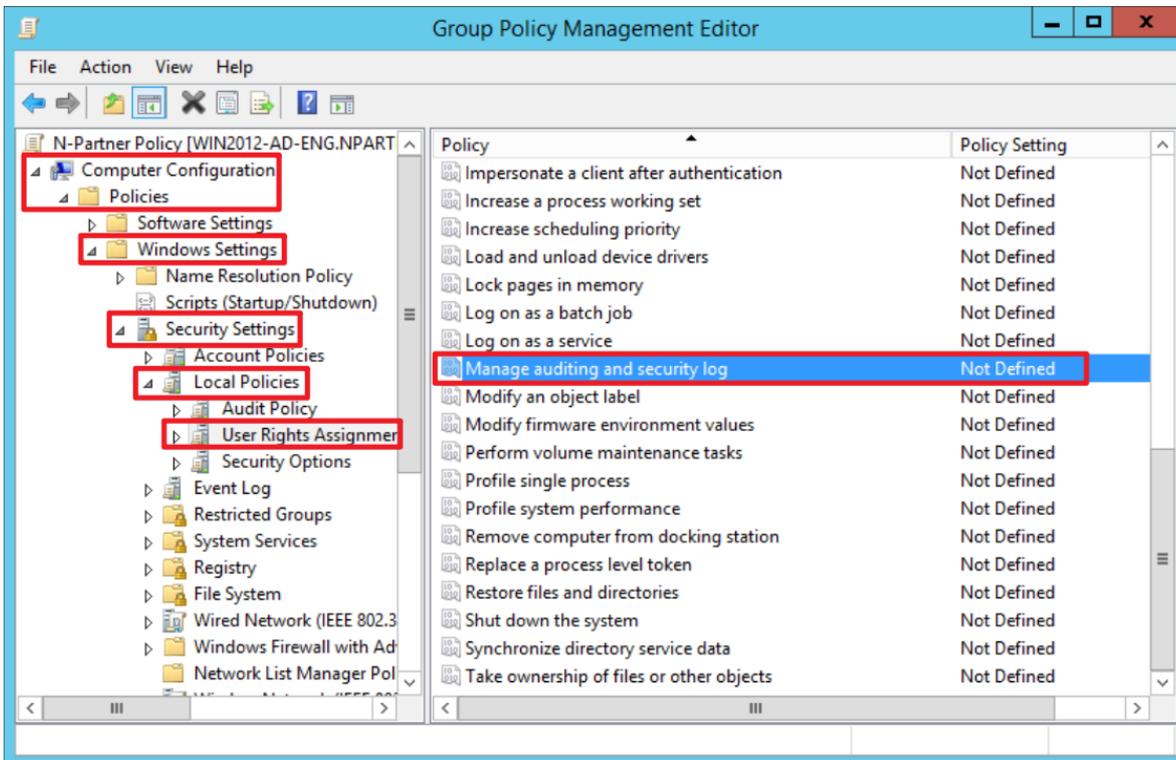


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



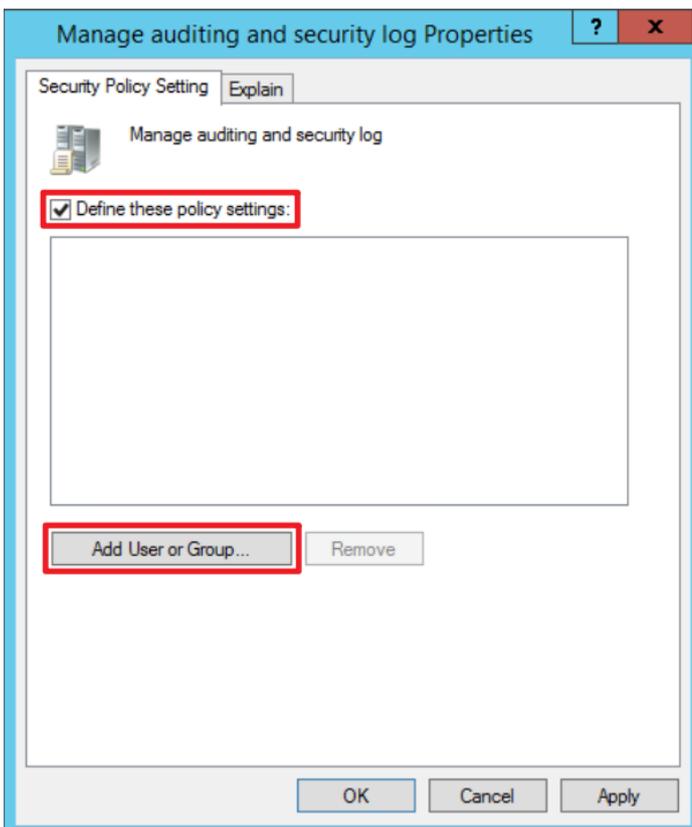
(3) Configure Auditing Log

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



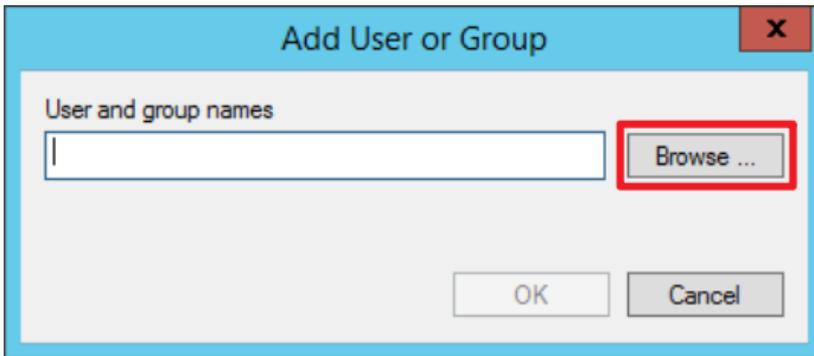
(4) Add Auditing User

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



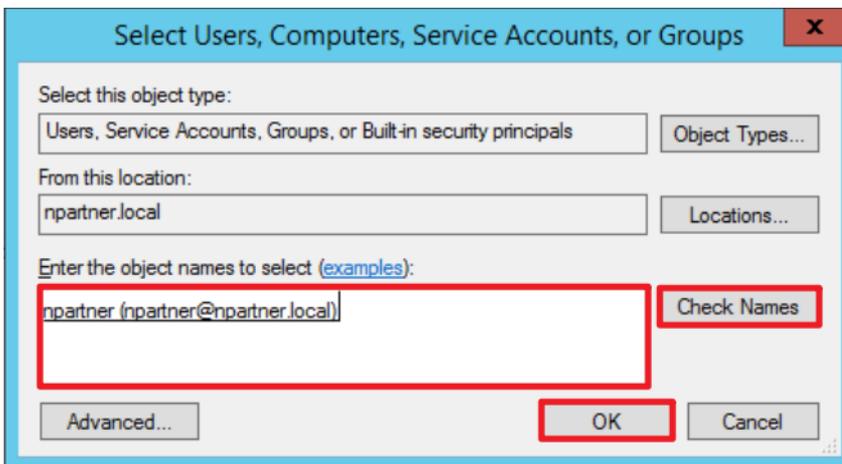
(5) Search for User

Click "Browse."



(6) Enter Your User Account

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

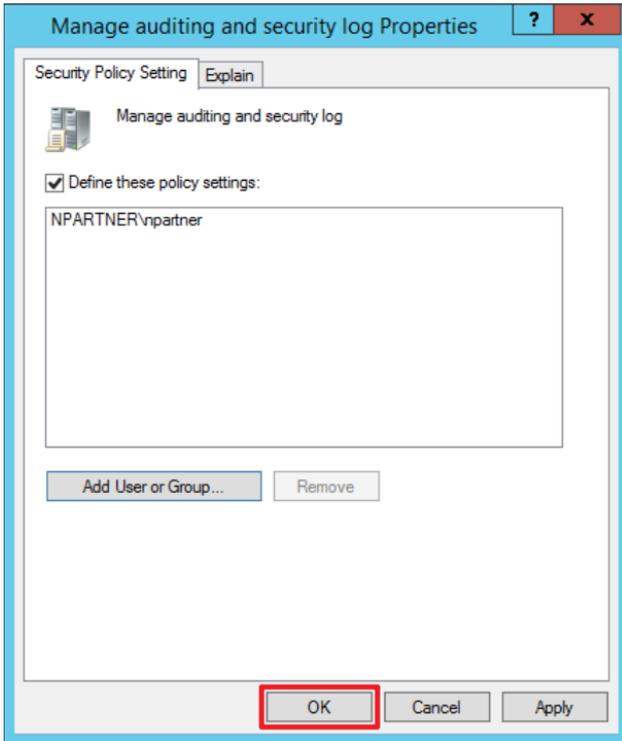


(7) Click "OK."



(8) Confirm Audit Log Settings

Click "OK."

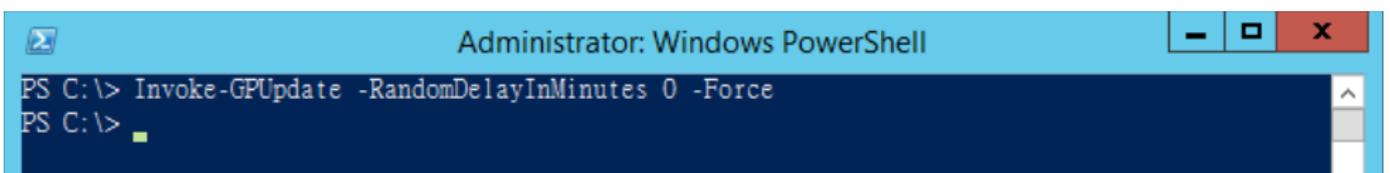


(9) Open "Windows Powershell."



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

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



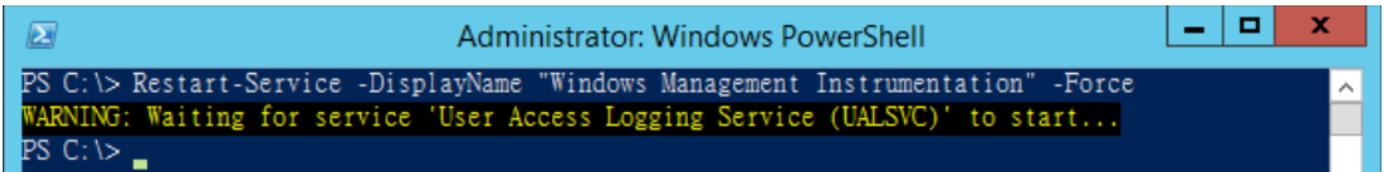
5.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”



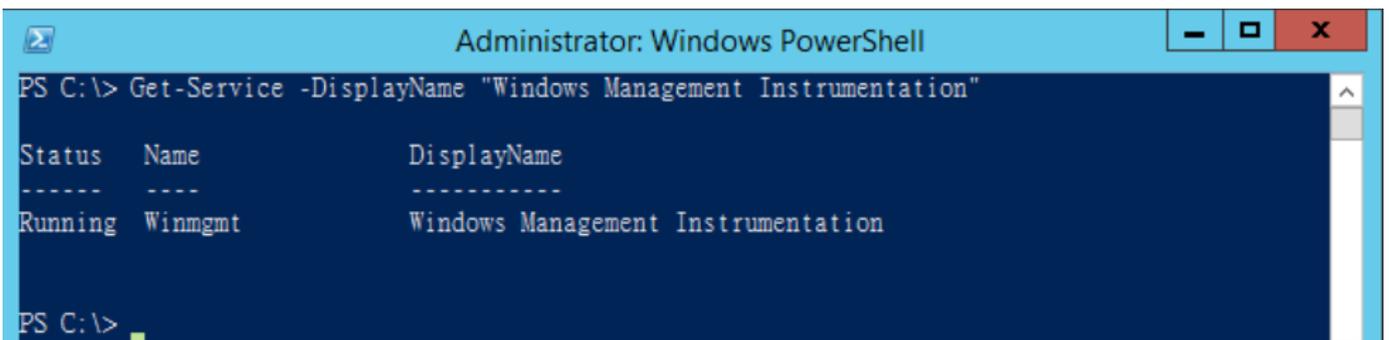
(2) Enter the command below to disable the WMI service.

```
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"
```



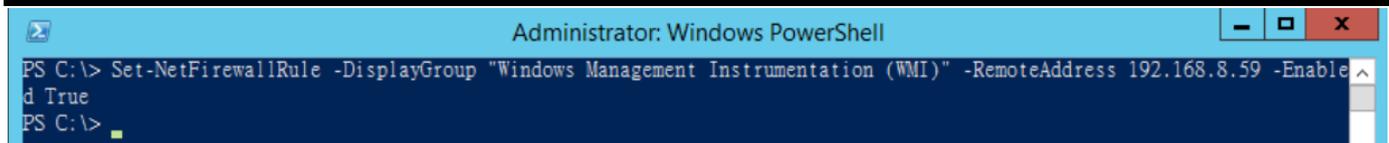
5.3.6 Configure the Firewall

(1) Open "Windows Powershell."



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

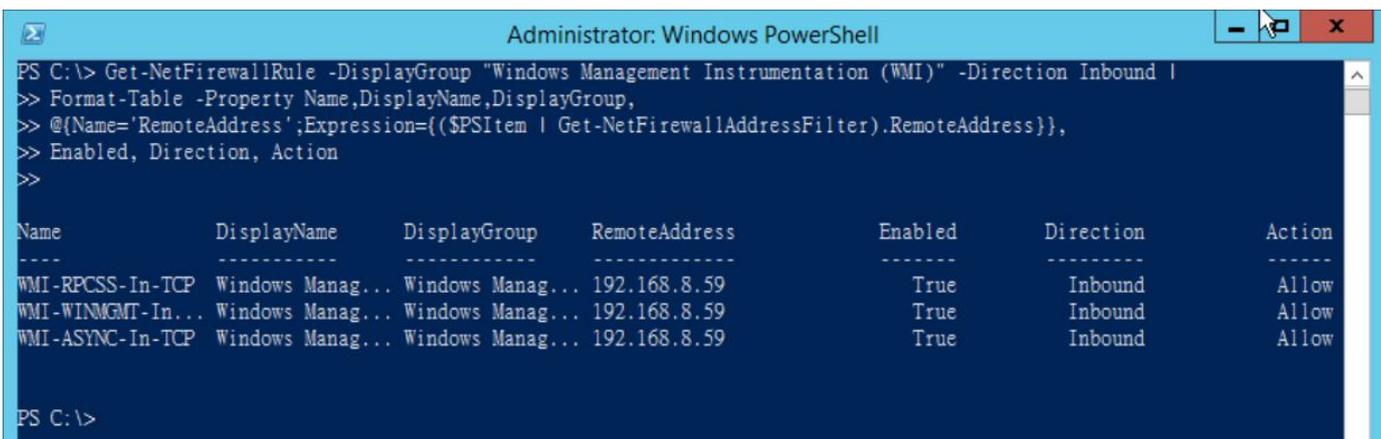
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True
```



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.

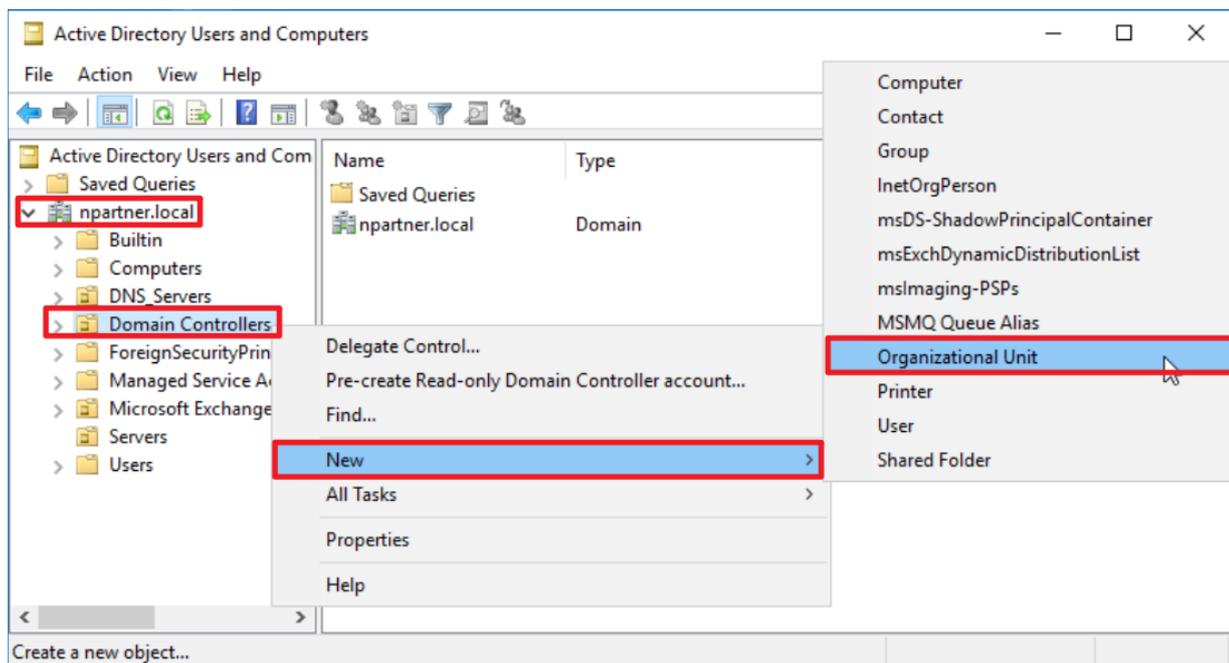
6.1 Organizational Unit (OU) Configuration

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



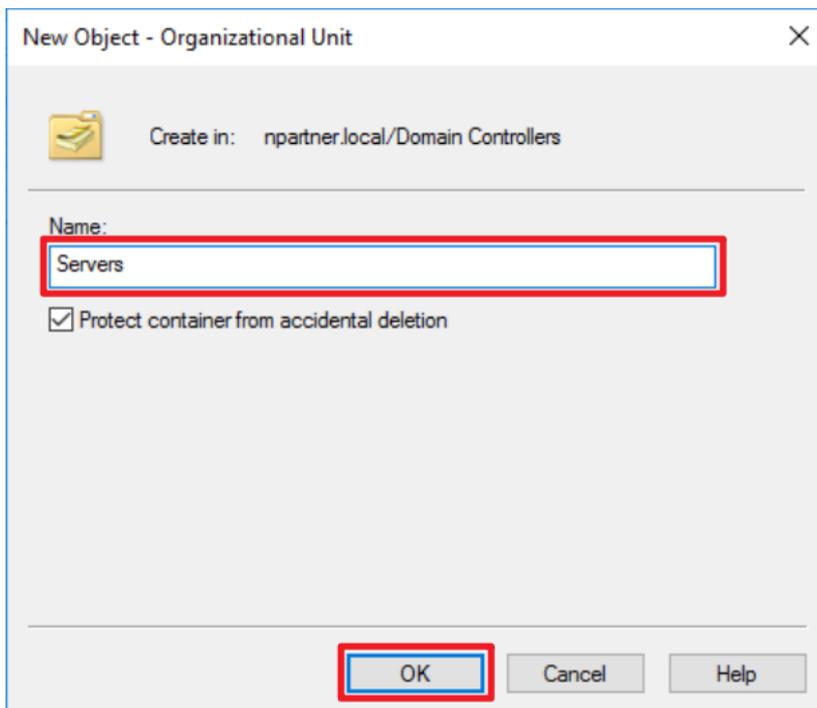
(2) Add an Organizational Unit

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”)

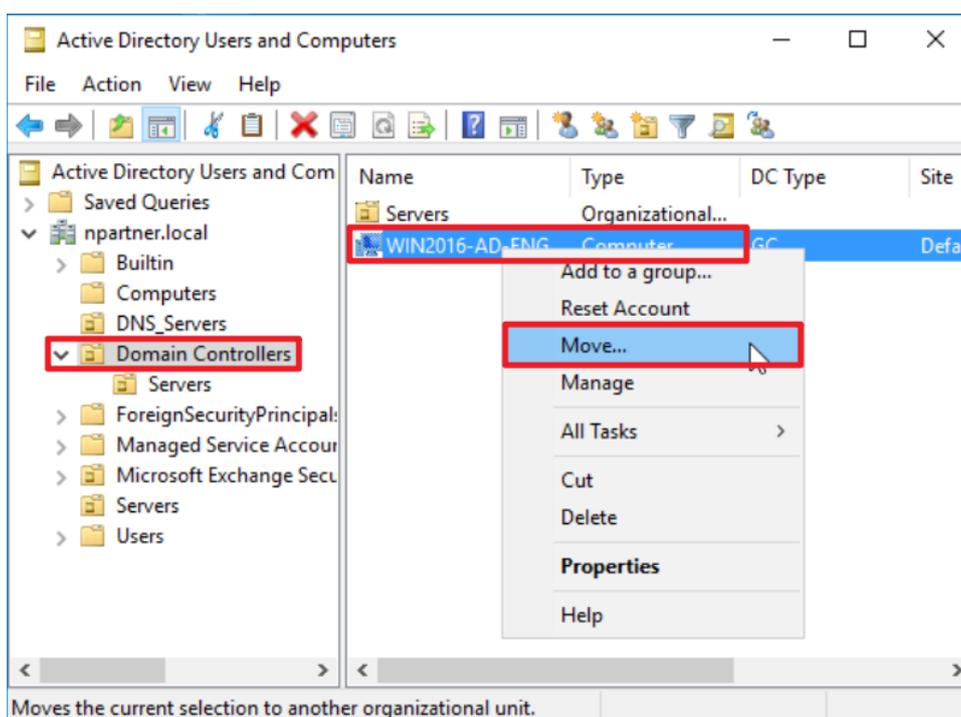
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

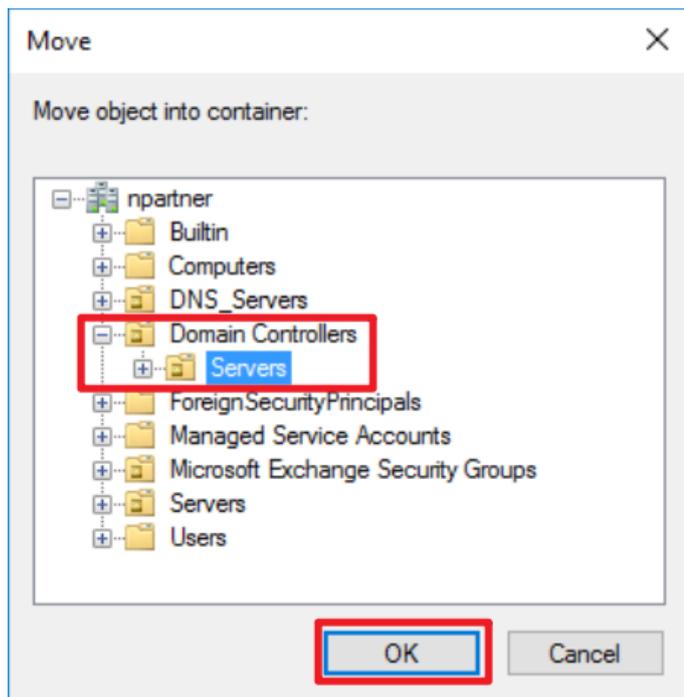
Select “Domain Controllers” → right-click on the “WIN2016-AD-ENG” server.

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



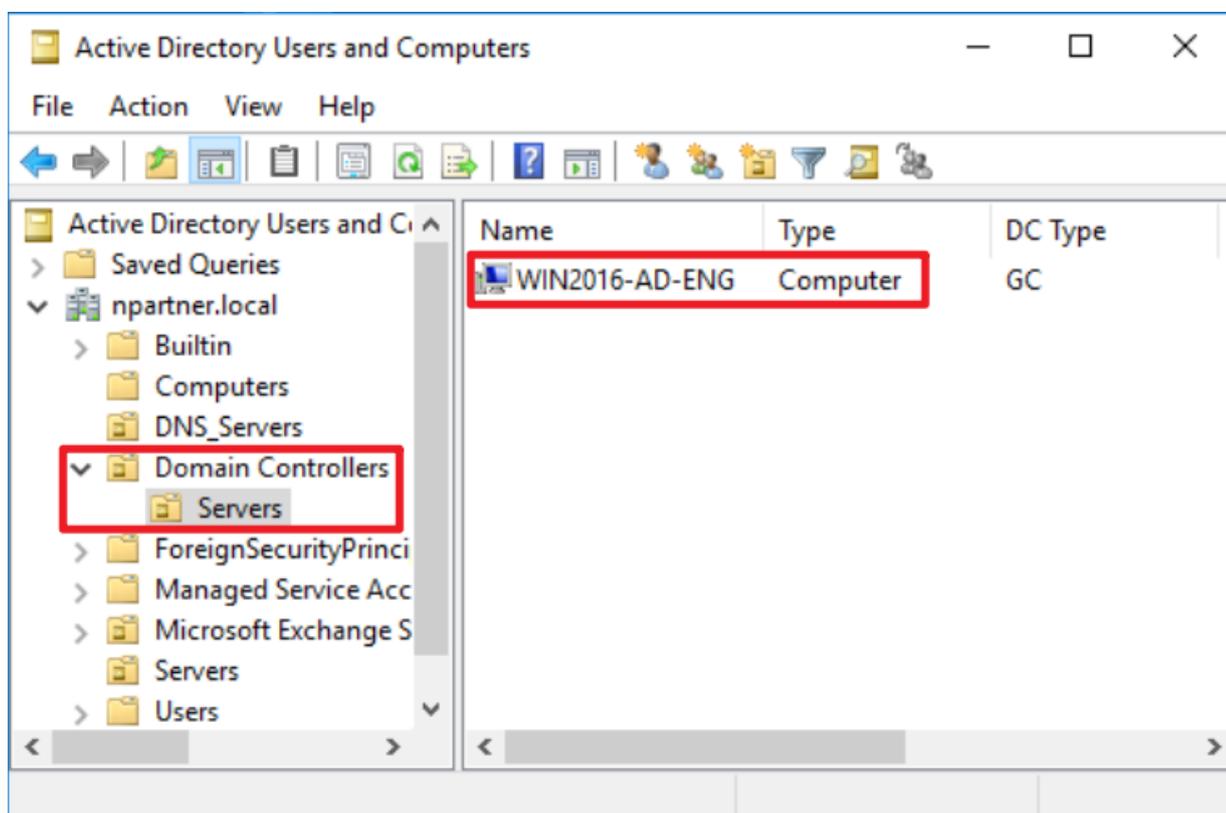
(5) Select your Organizational Unit:

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.



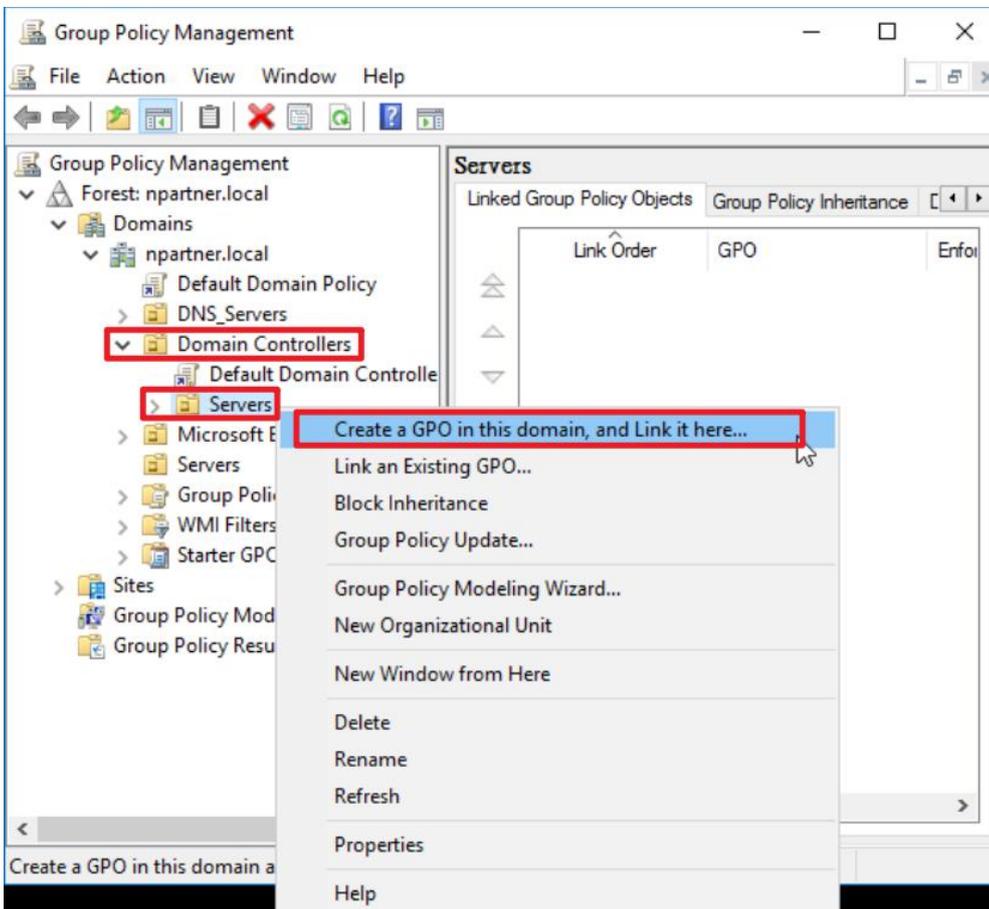
6.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

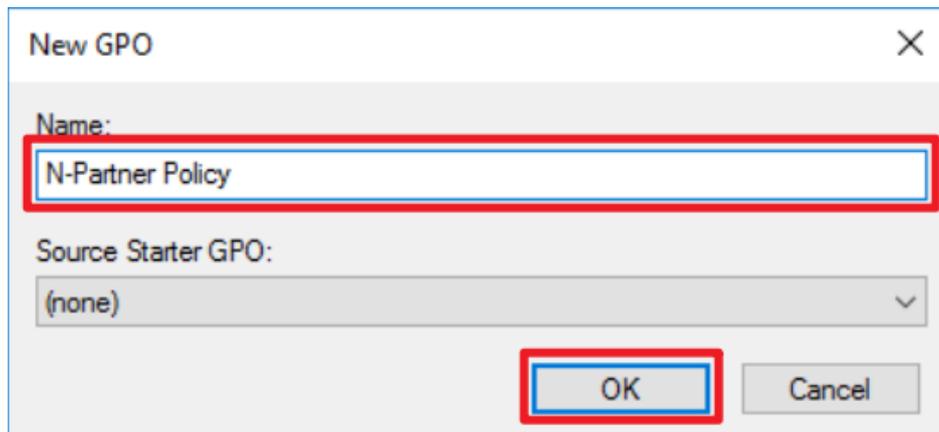
Right-click the “Servers” organizational unit under “Domain Controllers” → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

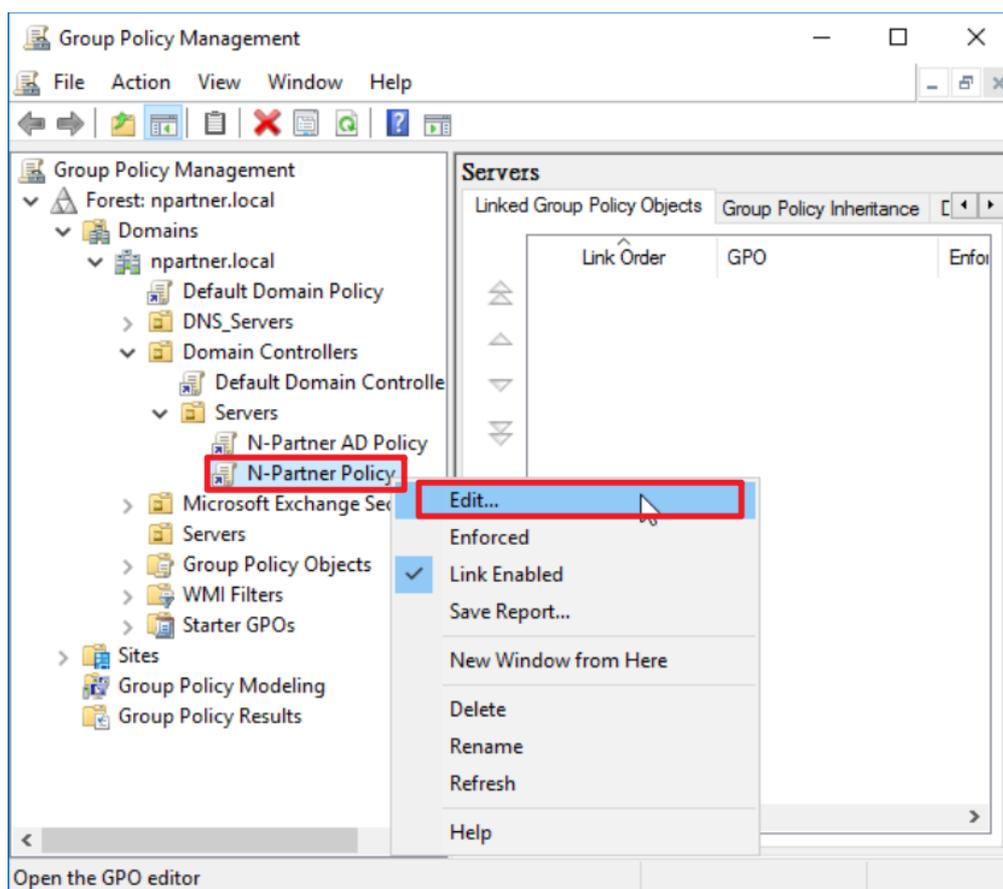
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



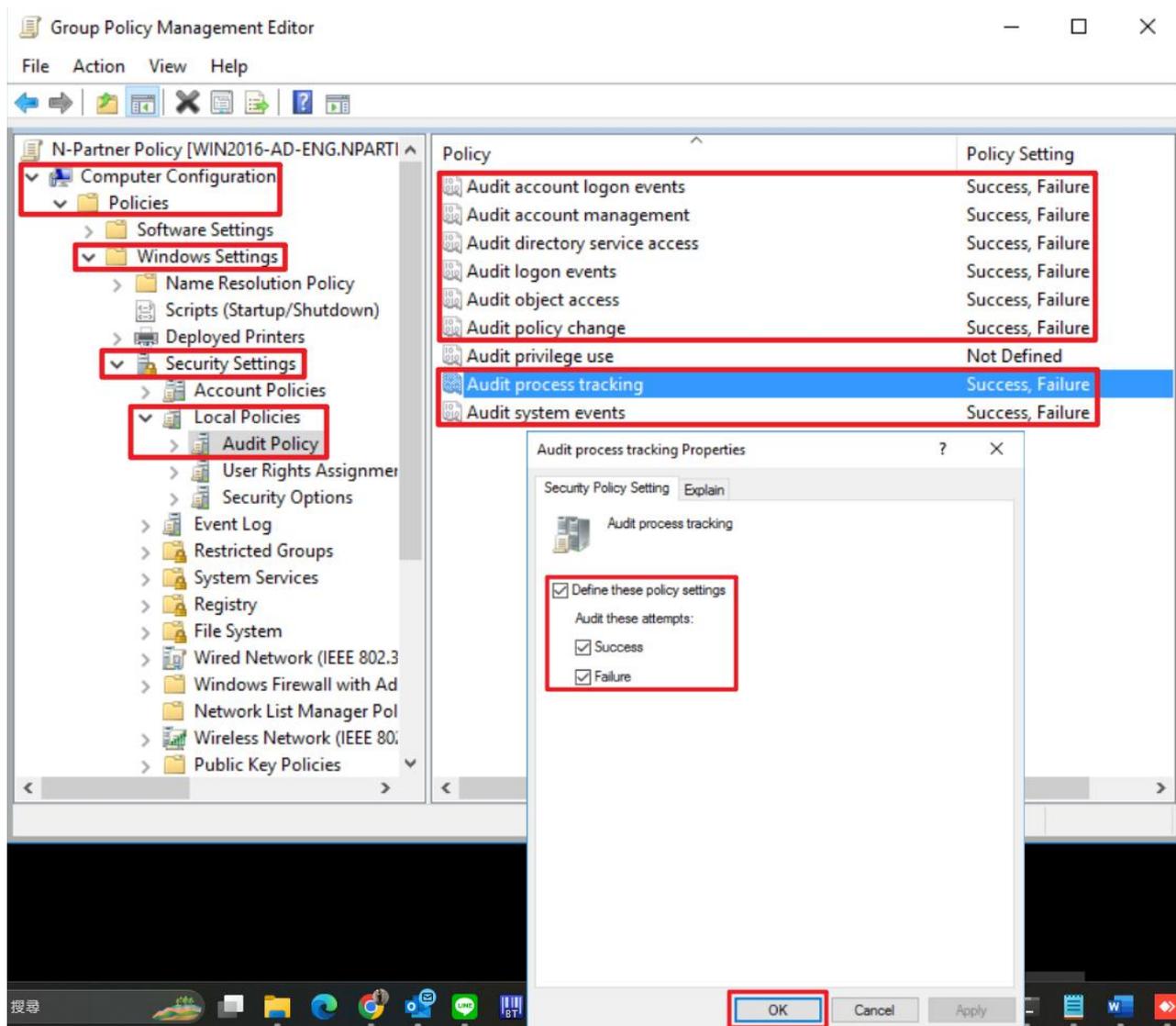
(4) Edit your Group Policy Object

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



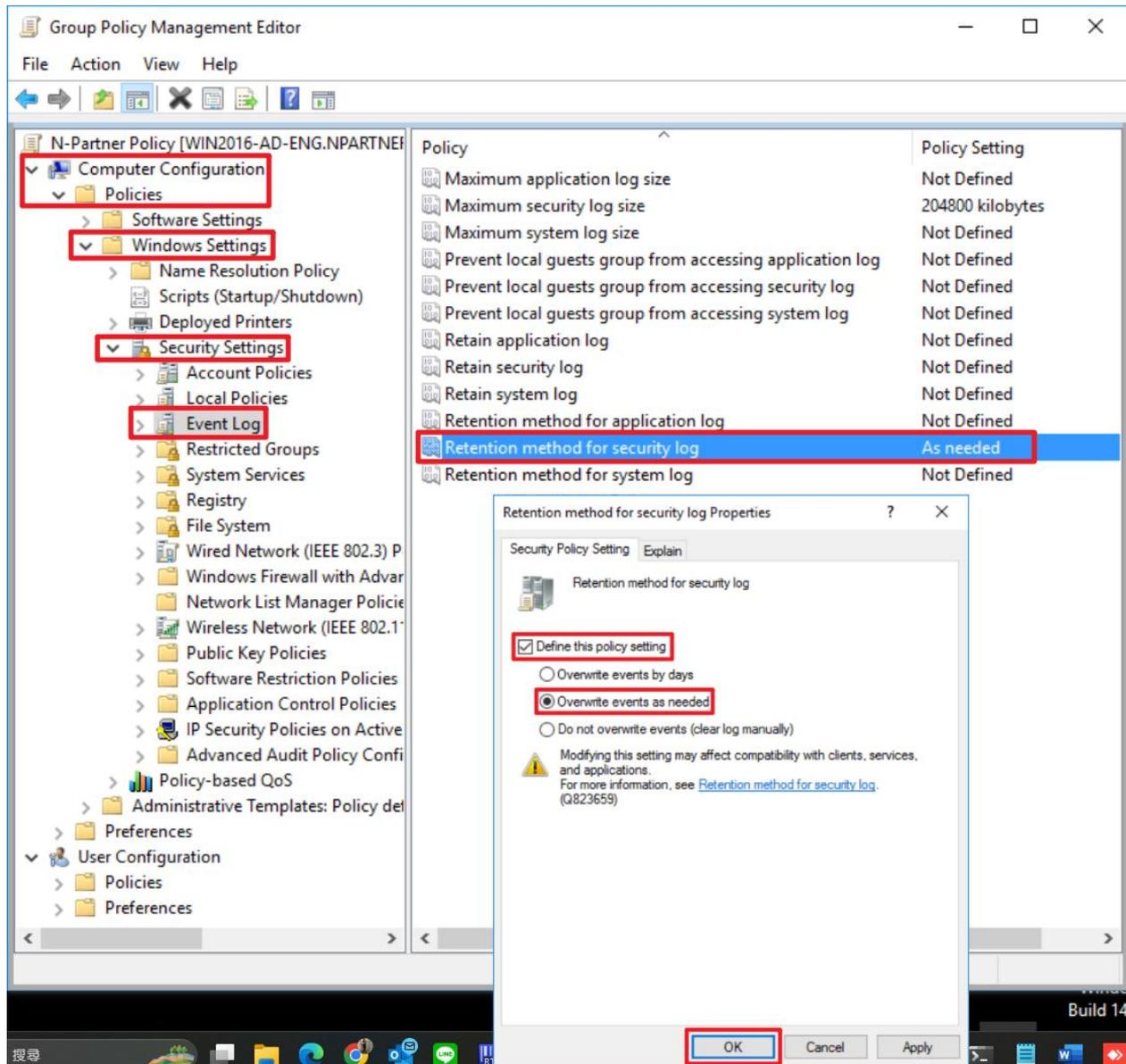
(5) Local Group Policies: Audit Policy

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

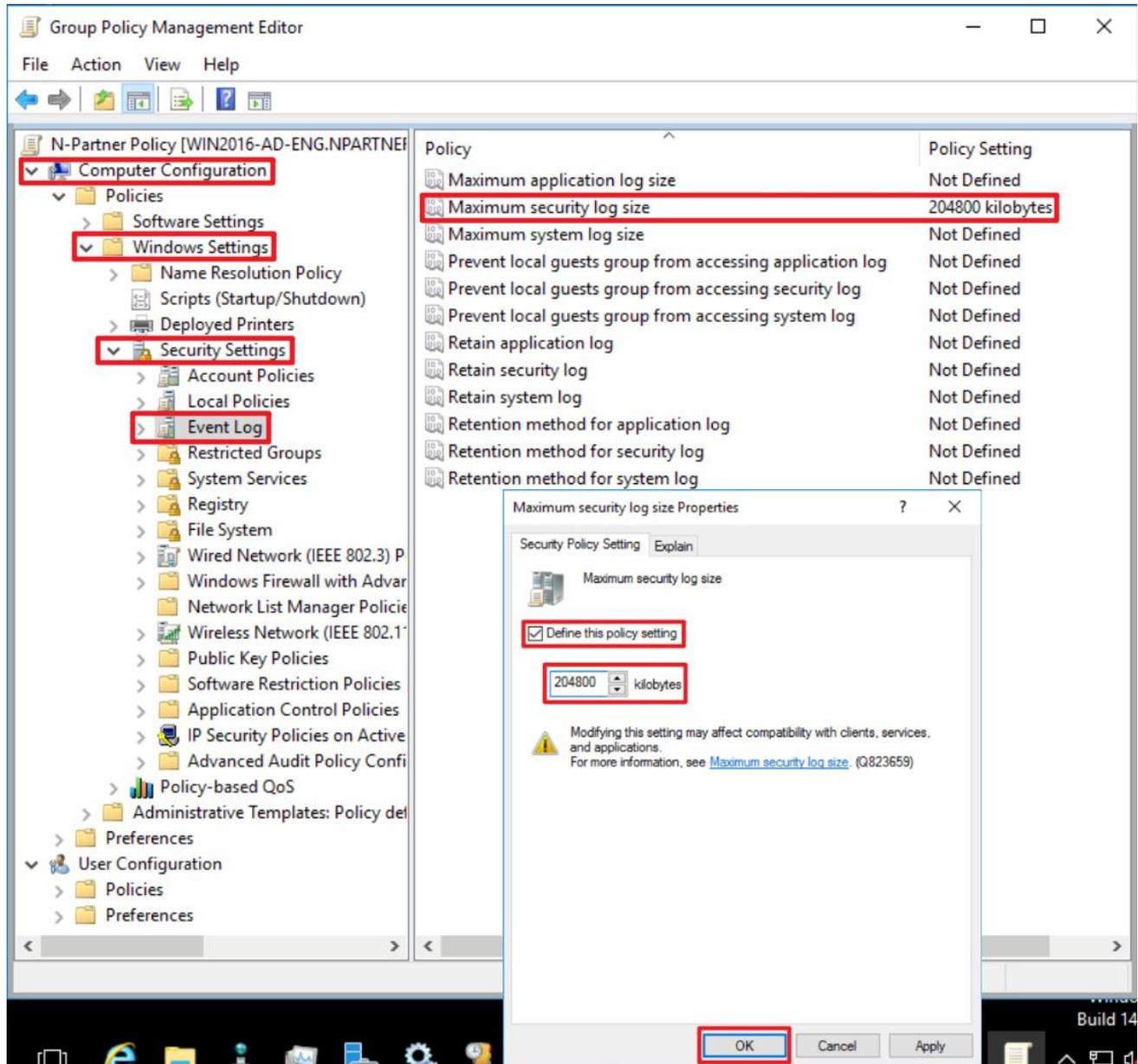
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

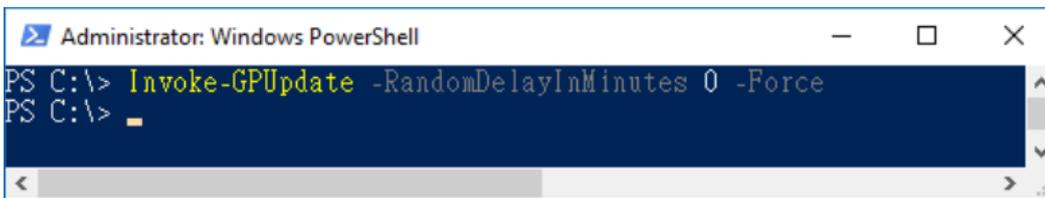


(8) Open “Windows PowerShell.”



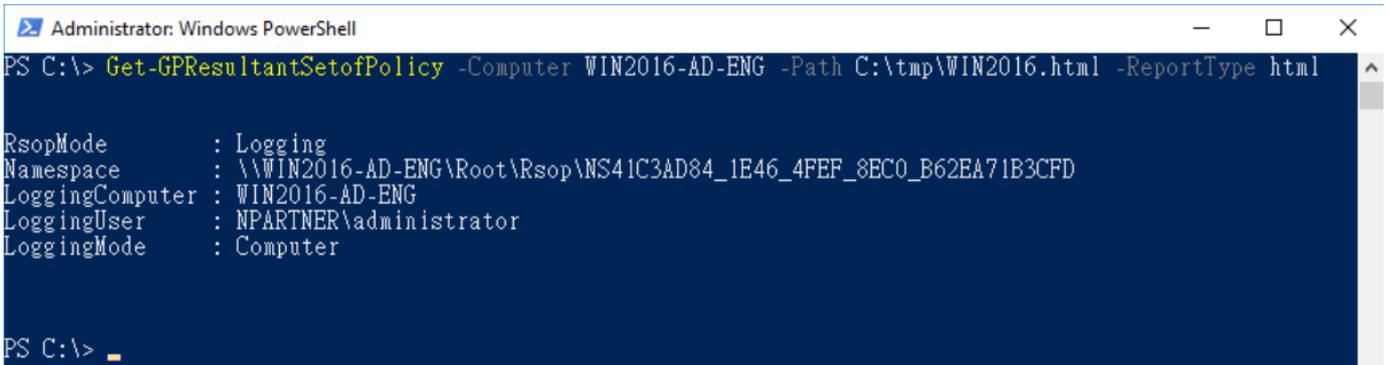
(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUdate -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.

The screenshot shows a web browser window with the address bar displaying 'file:///C:/tmp/Win2016.html#' and a tab for 'NPARTNER\WIN2016-AD-E...'. The main content area displays a report with a tree view on the left and a table of data on the right.

Component Status [show](#)

Settings [hide](#)

Policies [hide](#)

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

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

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

Local Policies/Security Options [show](#)

Event Log [hide](#)

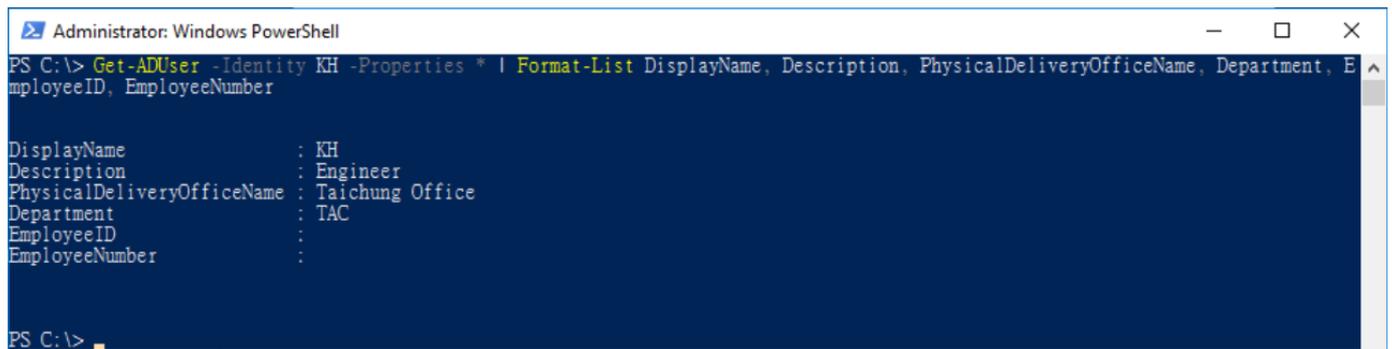
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner AD Policy
Retention method for security log	As needed	N-Partner AD Policy

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

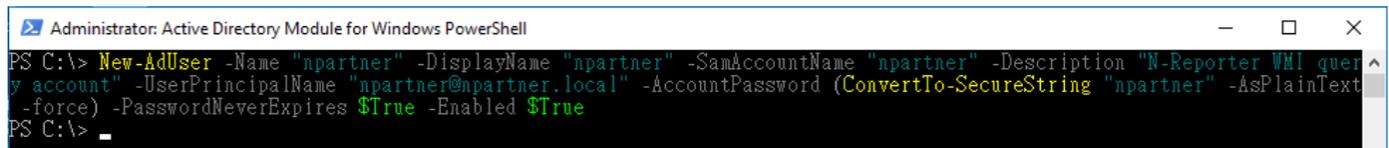
(1) Open “Active Directory Module for Windows PowerShell.”



(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
```

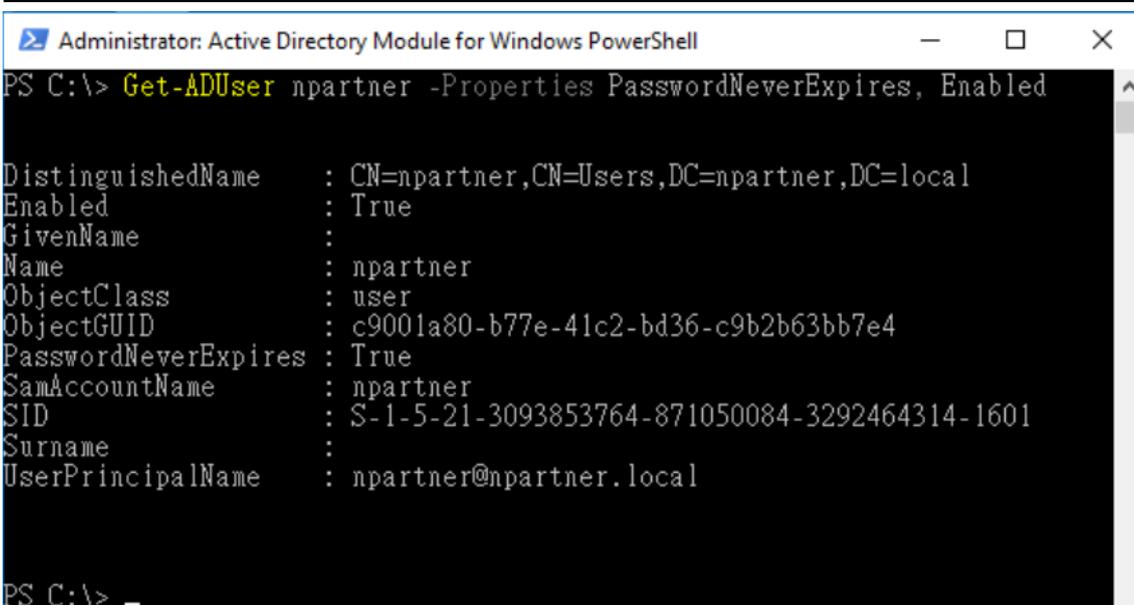


```
Administrator: Active Directory Module for Windows PowerShell
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText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

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
```



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires, Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                 : True
GivenName               :
Name                   : npartner
ObjectClass             : user
ObjectGUID              : c9001a80-b77e-41c2-bd36-c9b2b63bb7e4
PasswordNeverExpires   : True
SamAccountName          : npartner
SID                     : S-1-5-21-3093853764-871050084-3292464314-1601
Surname                 :
UserPrincipalName       : npartner@npartner.local

PS C:\> _
```

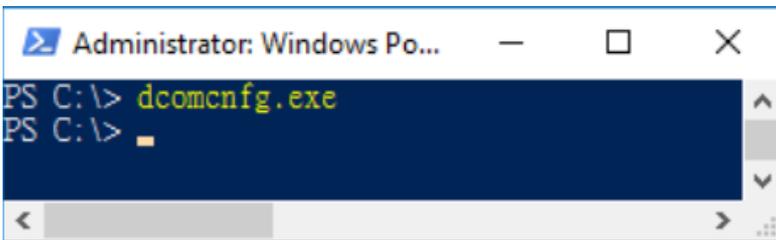
6.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”



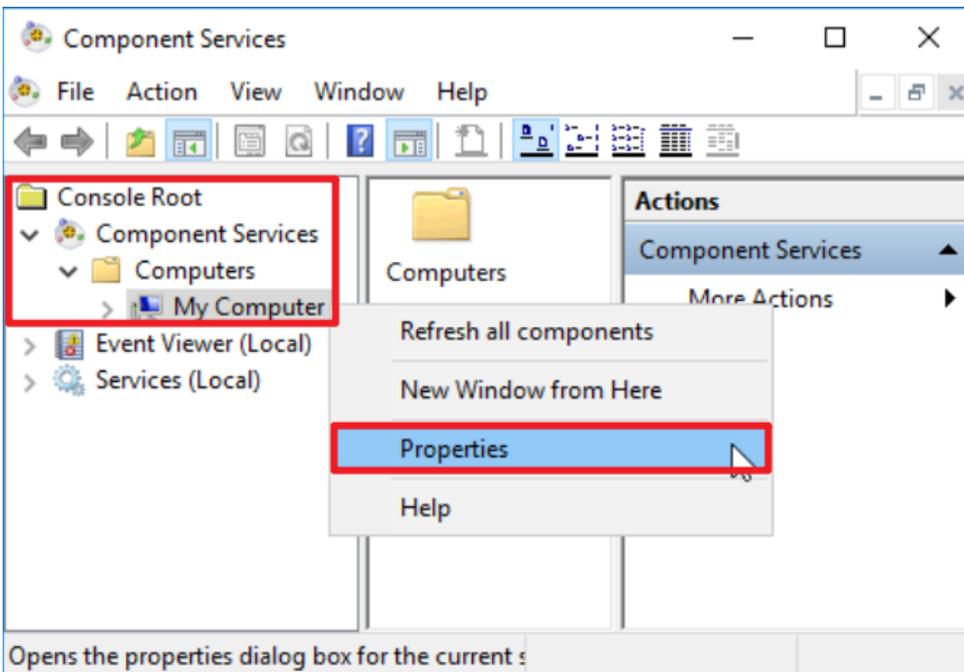
(2) Enter the command below to enable component services.

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



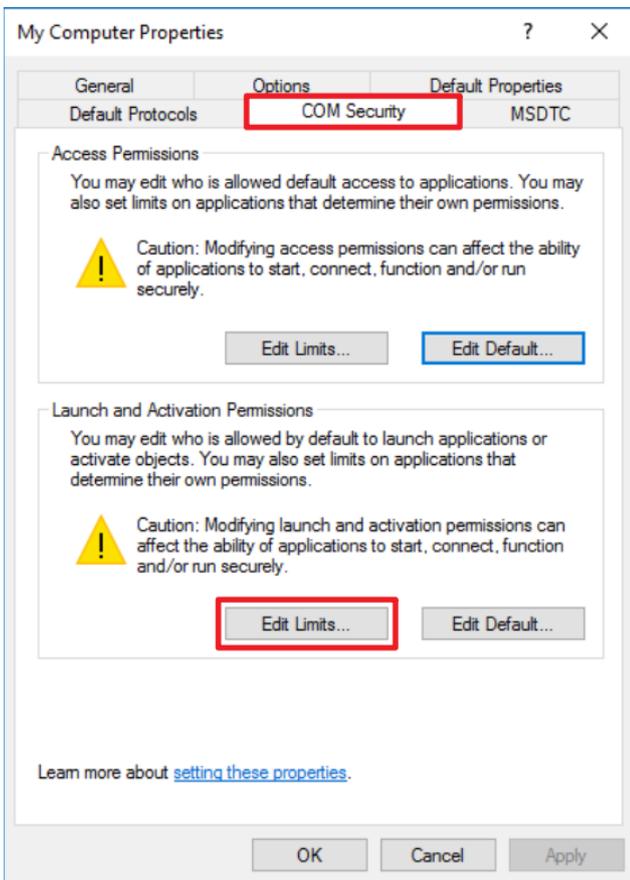
(3) Edit Computer Properties

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



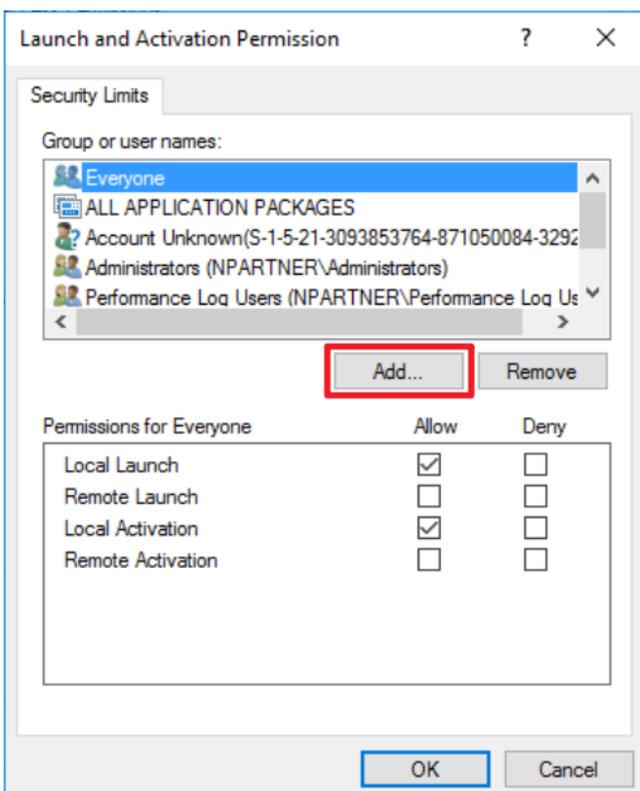
(4) Enable Permissions

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



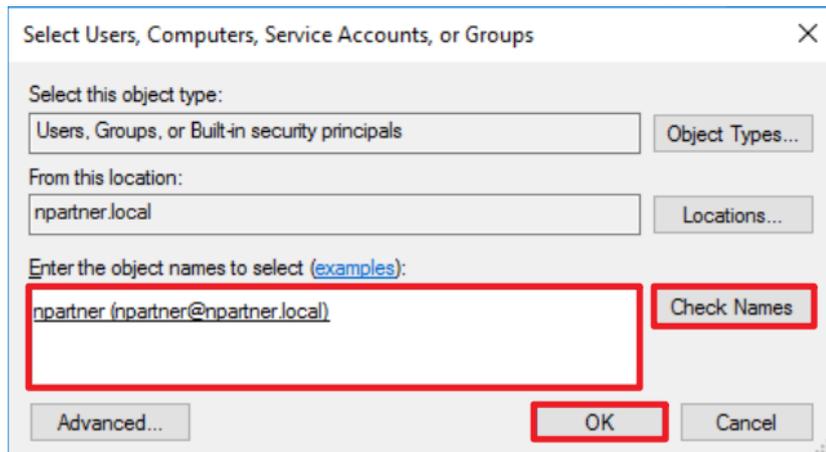
(5) Add DCOM User Permissions

Click “Add.”



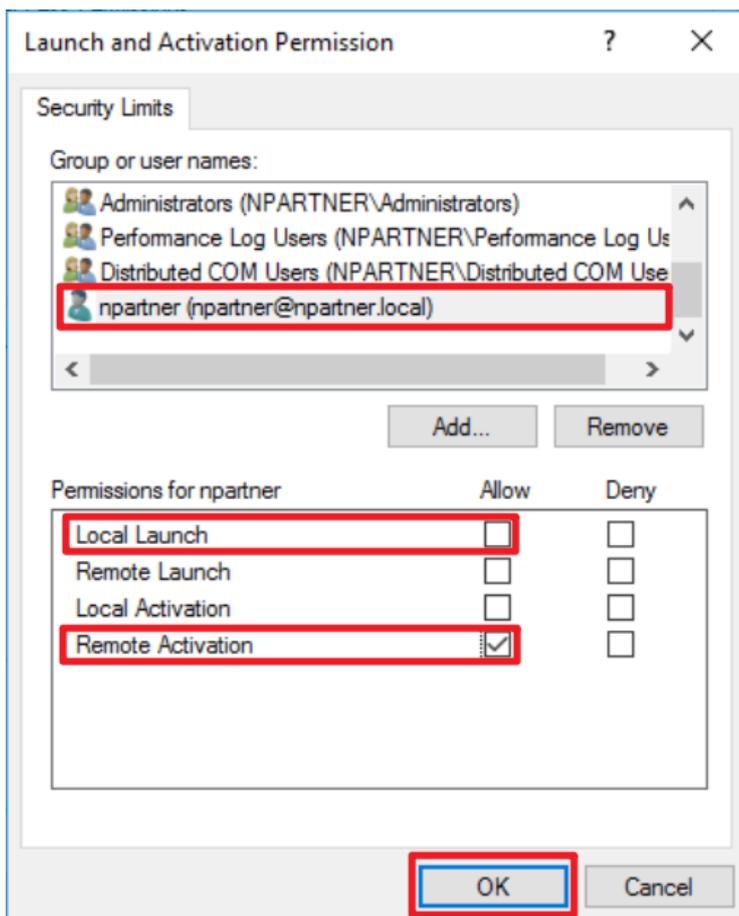
(6) Enter Your Username

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

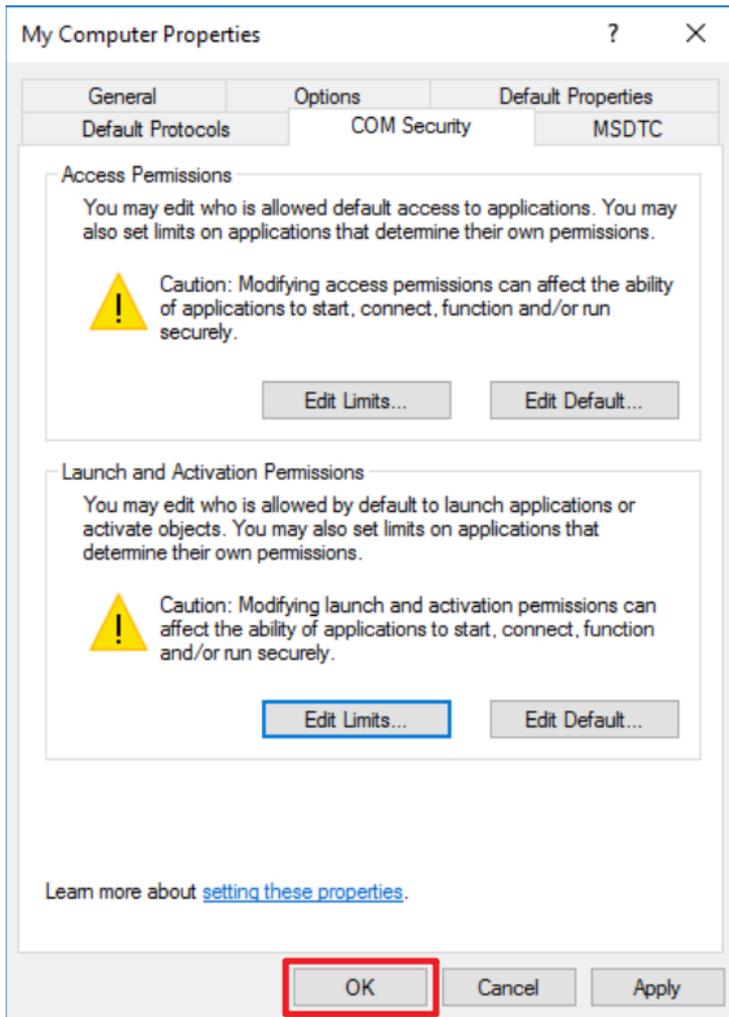


(7) Configure your User Permission

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

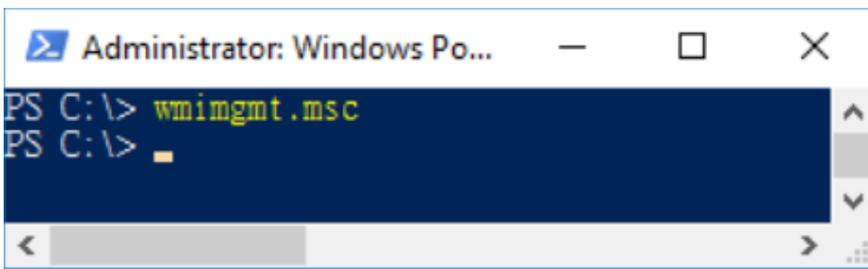
6.3.3.1 Configure Event Log Permissions

(1) Open "Windows Powershell."



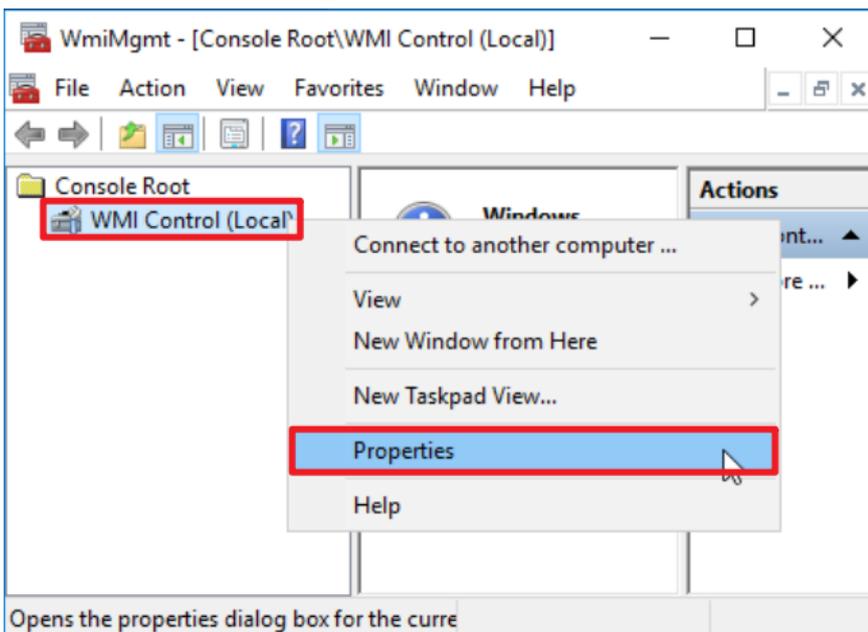
(2) Enter the command to enable WMI control service.

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



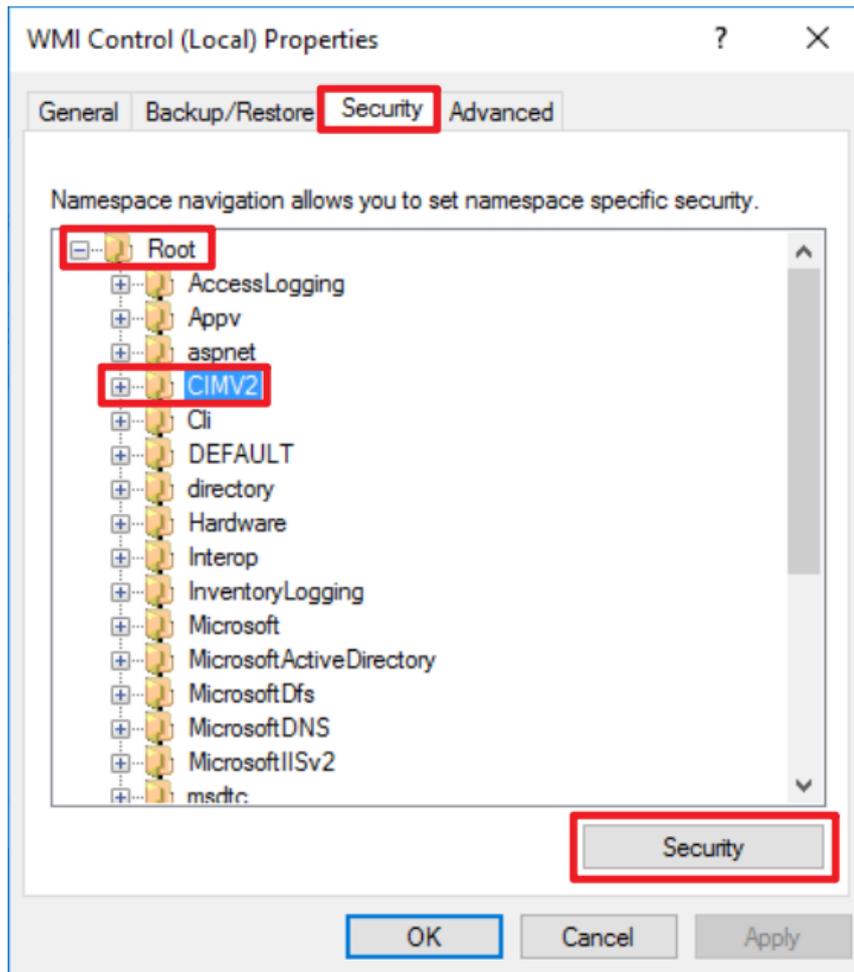
(3) Edit WMI Control

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



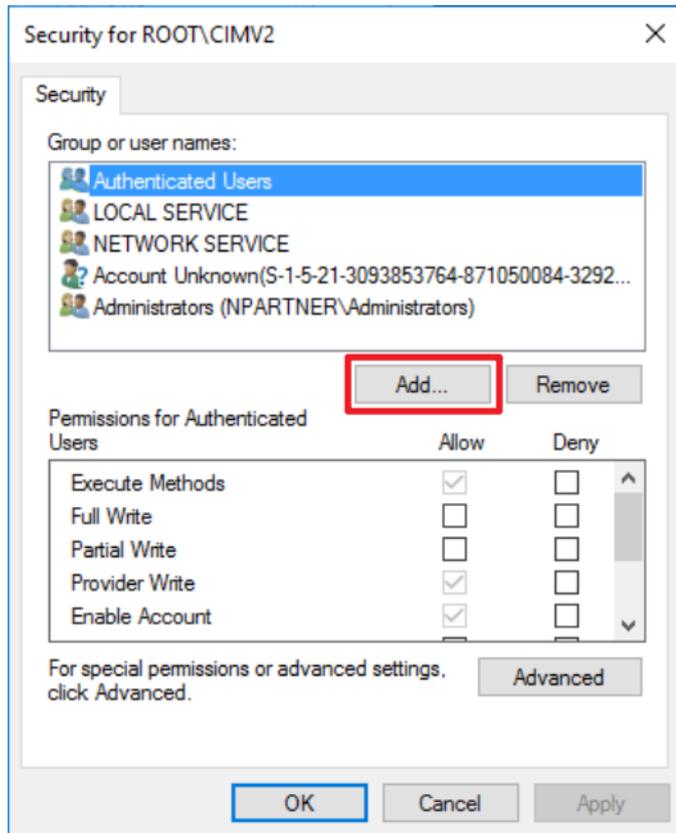
(4) Edit CIMV2 Security

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



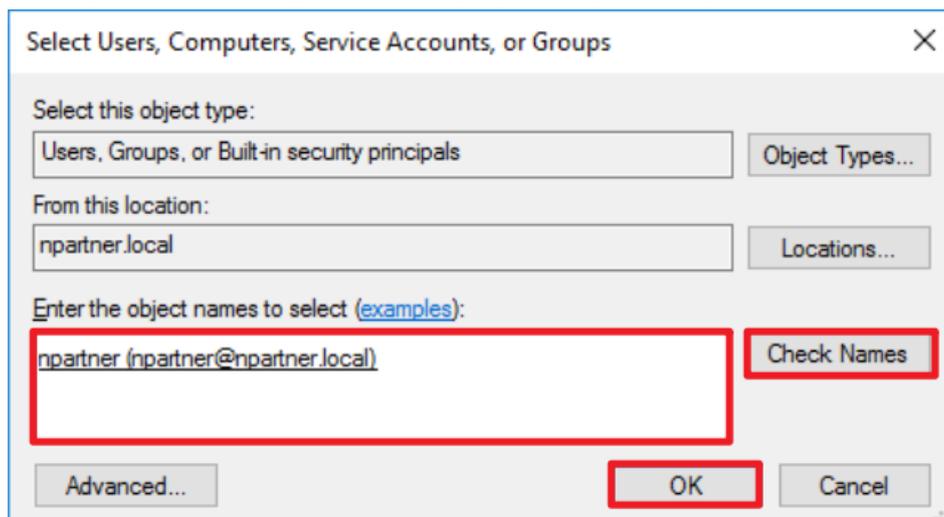
(5) Add WMI User Permissions.

Click "Add."



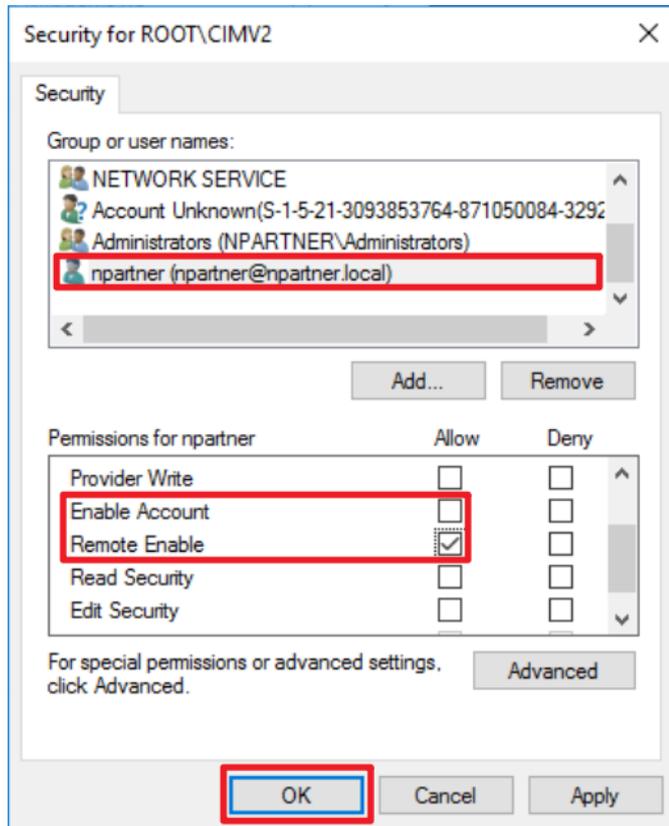
(6) Enter Your Username

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

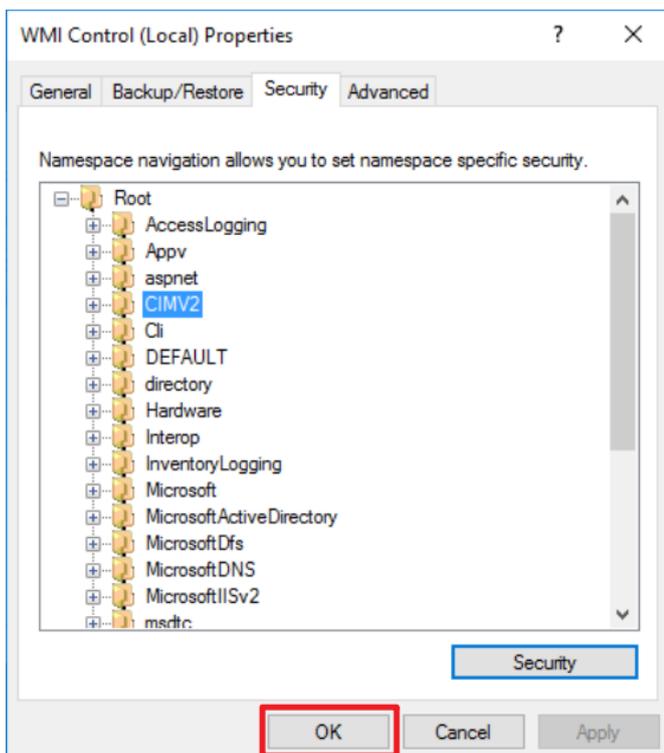


(7) Set Your User Permissions

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



(8) Click “OK.”



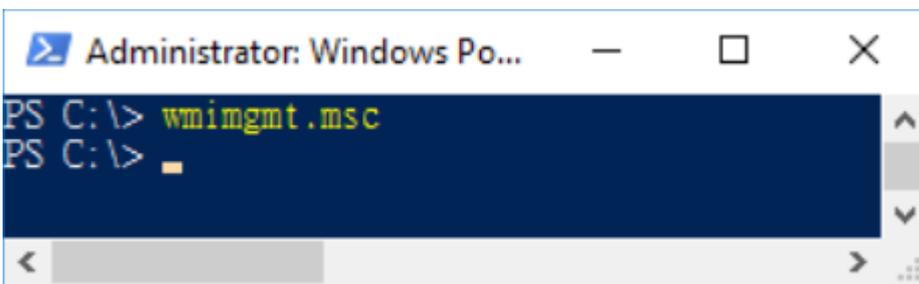
6.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



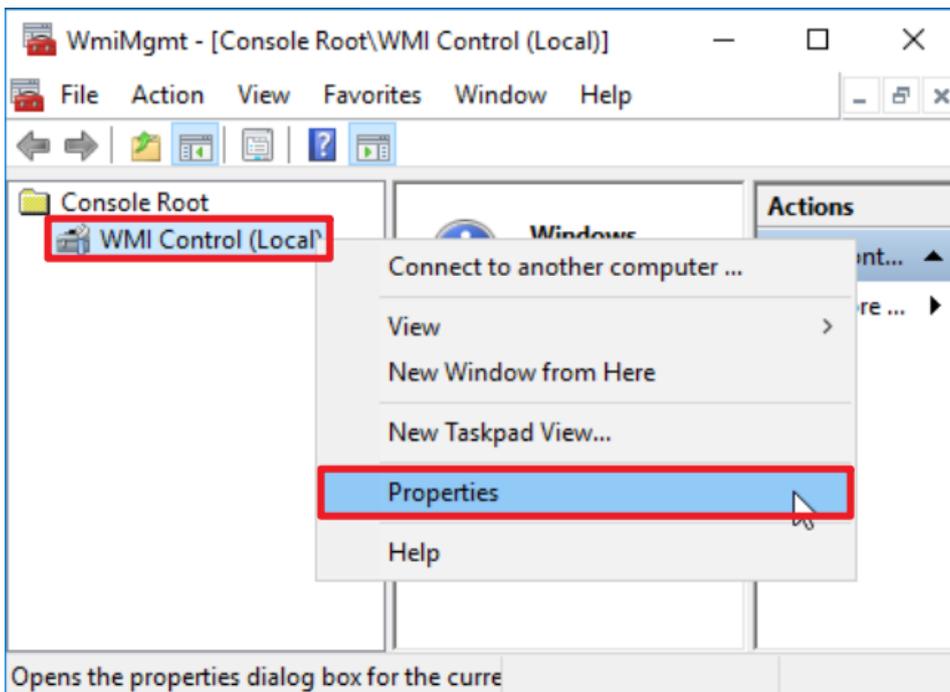
(2) Enter the command below to enable WMI Control.

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



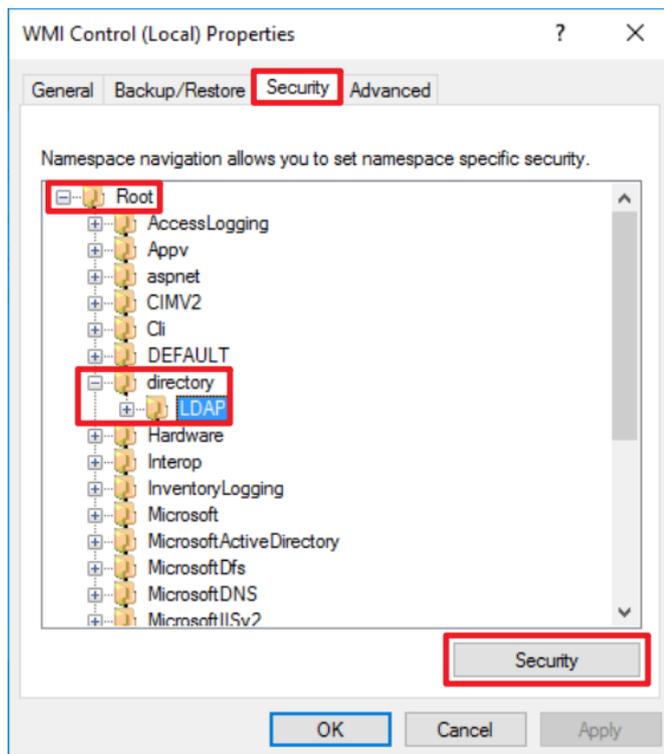
(3) Edit WMI Control

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



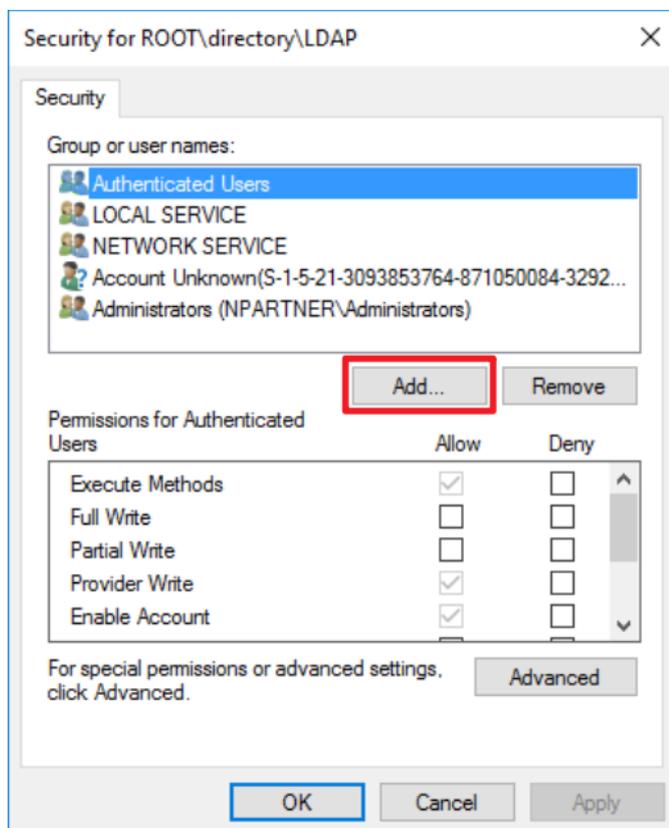
(4) Edit LDAP Security

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



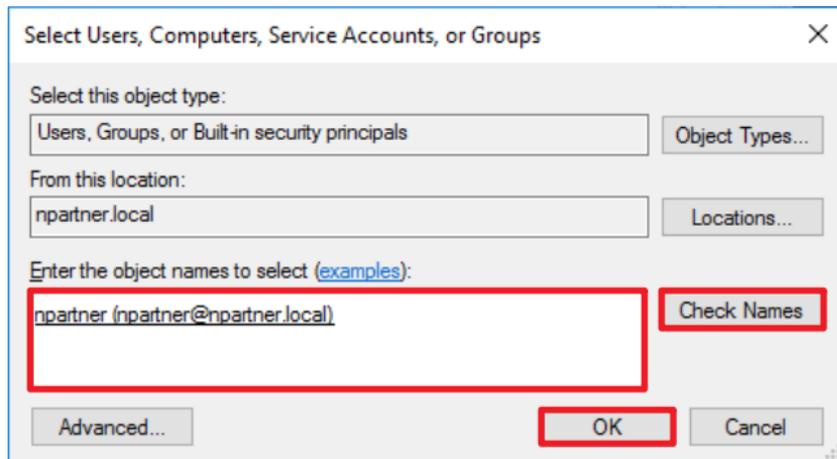
(5) Add WMI User Permissions

Click "Add."



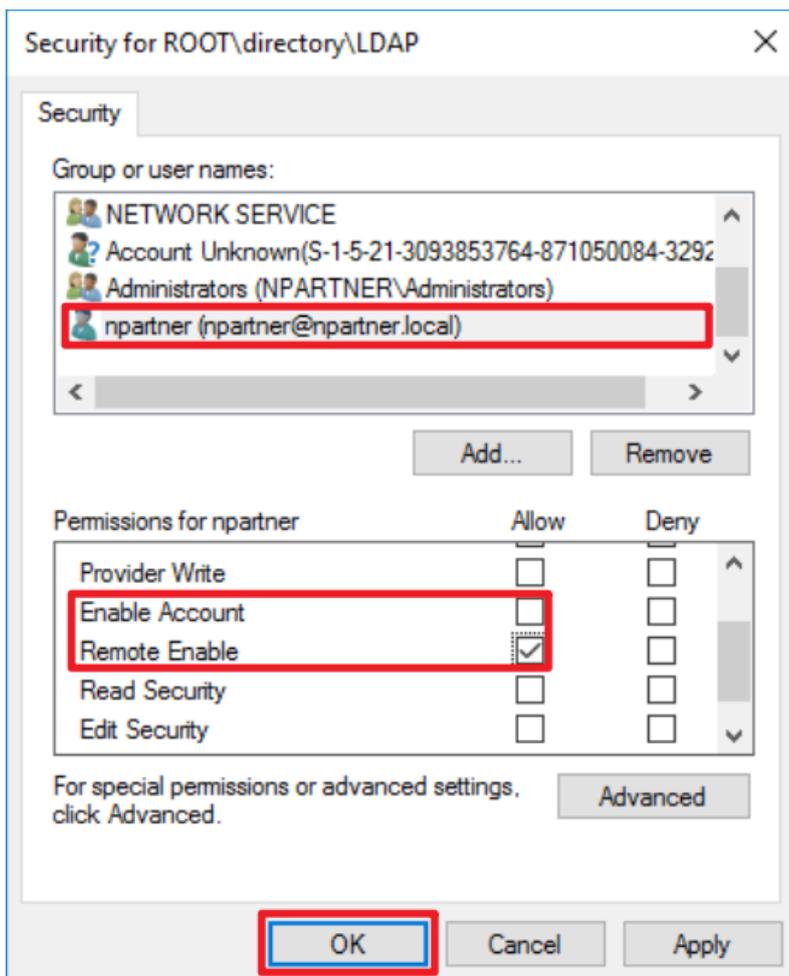
(6) Enter Your Username

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

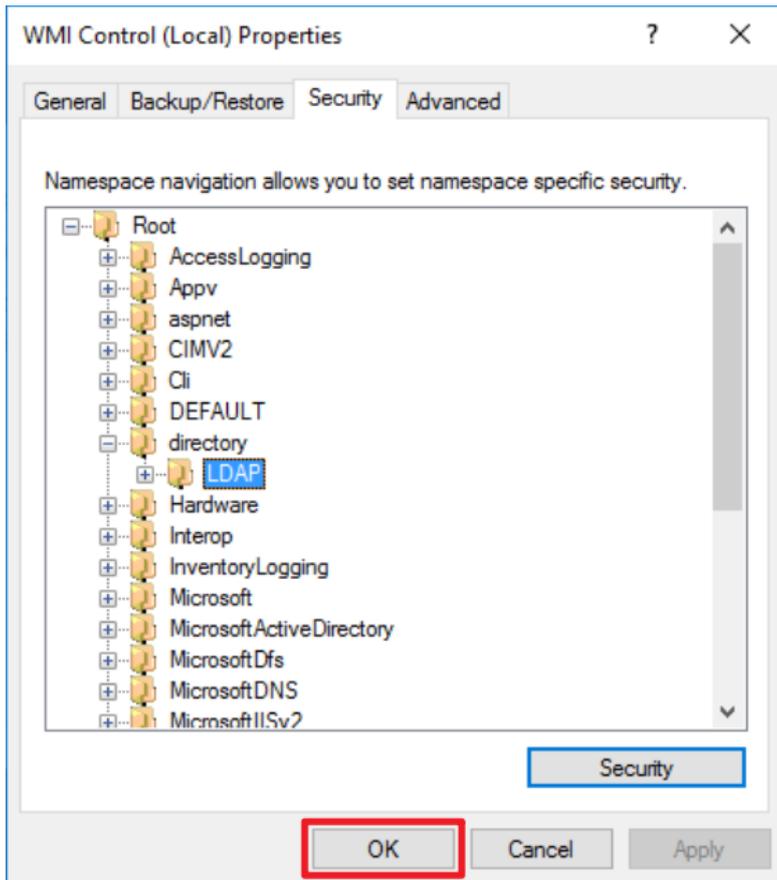


(7) Set Your User Permissions

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

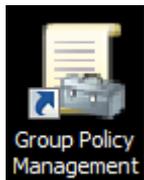


(8) Click "OK."

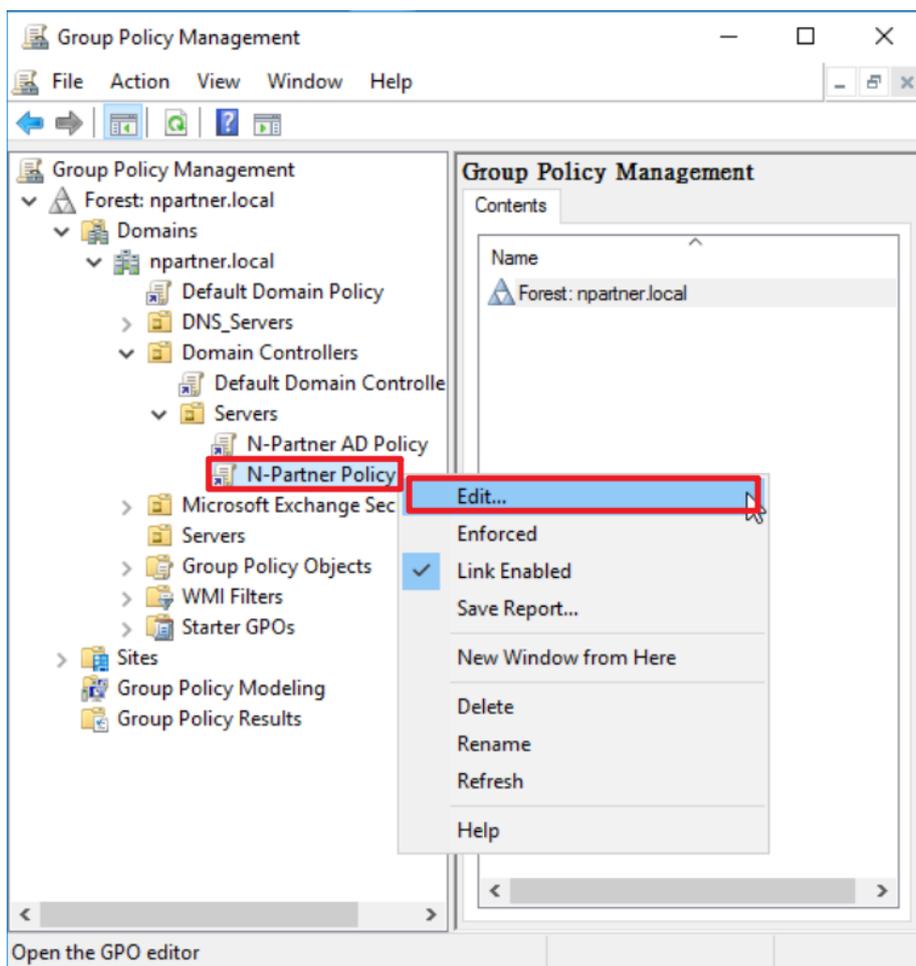


6.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

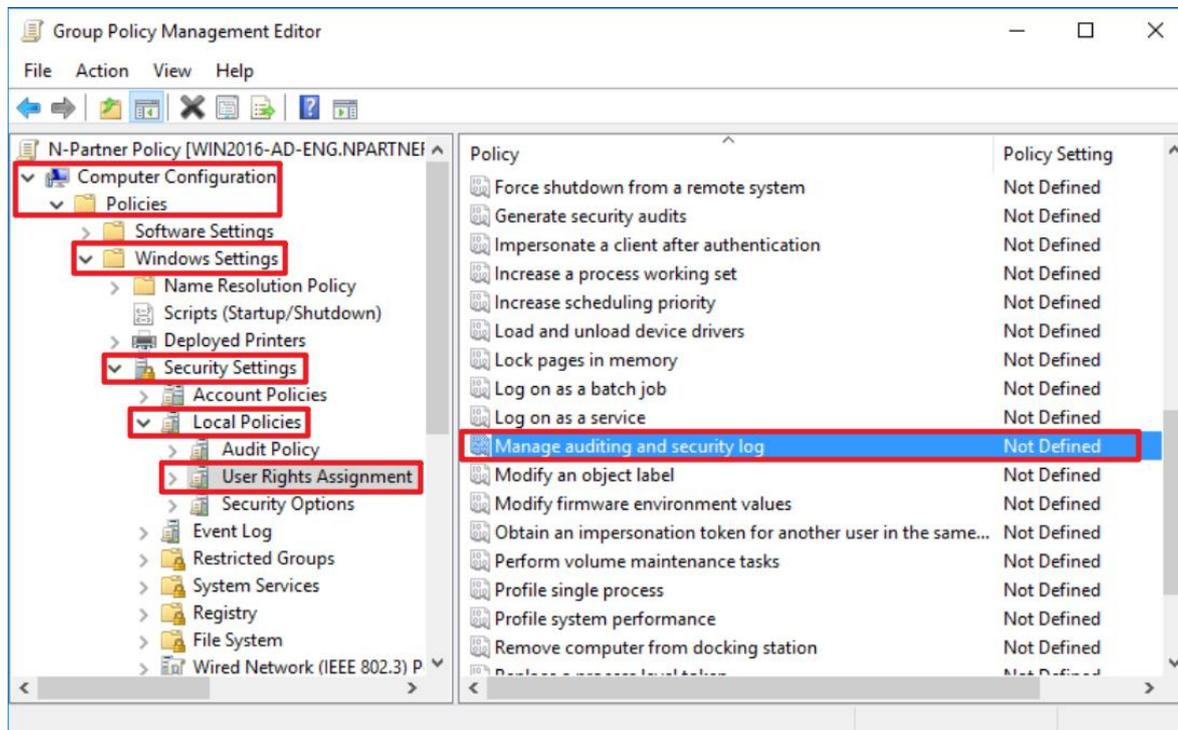


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



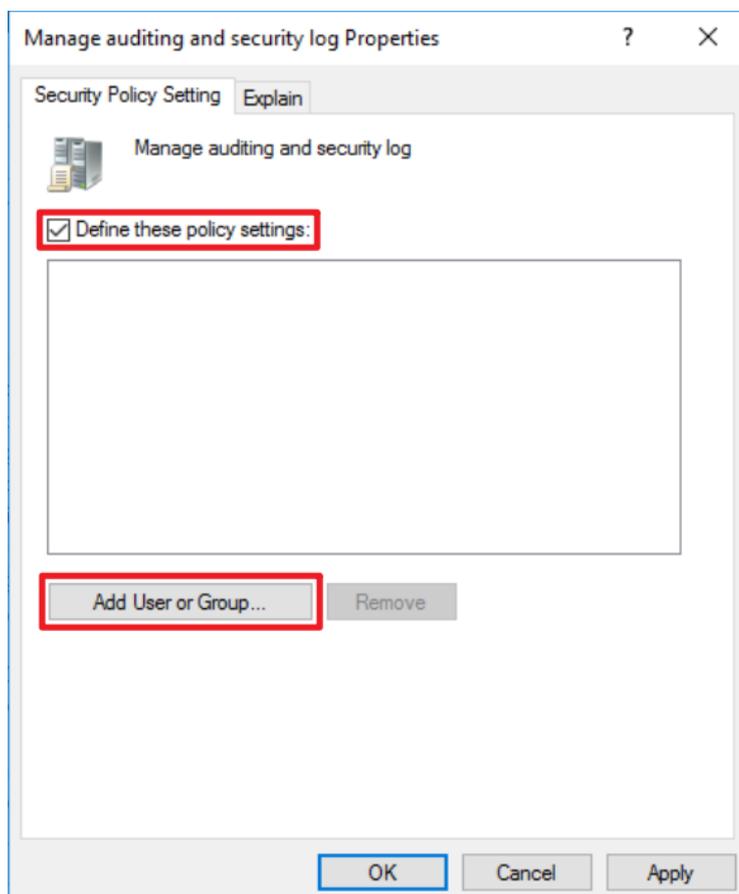
(3) Configure Auditing Log

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



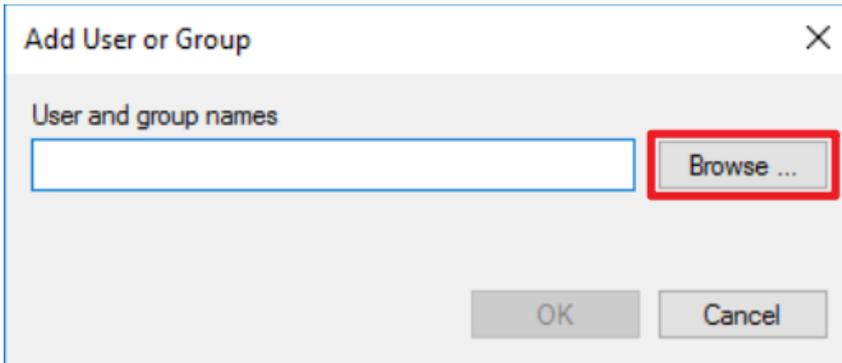
(4) Add Auditing User

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



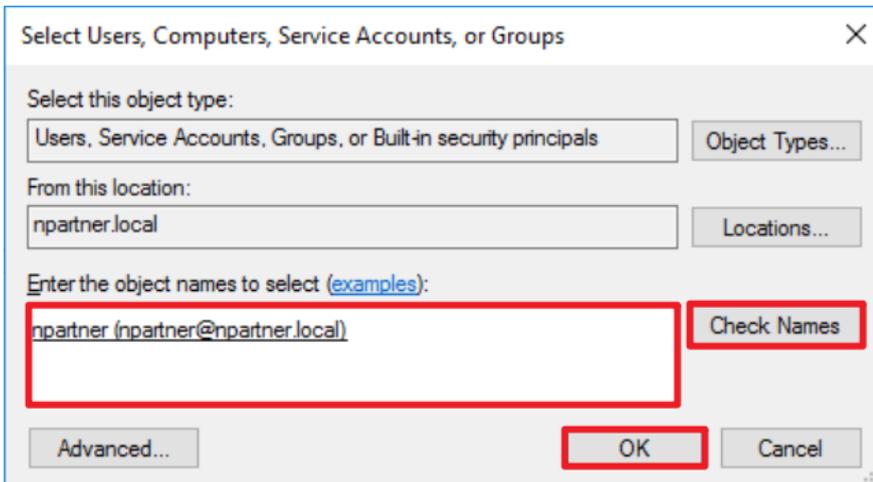
(5) Search for User

Click "Browse."

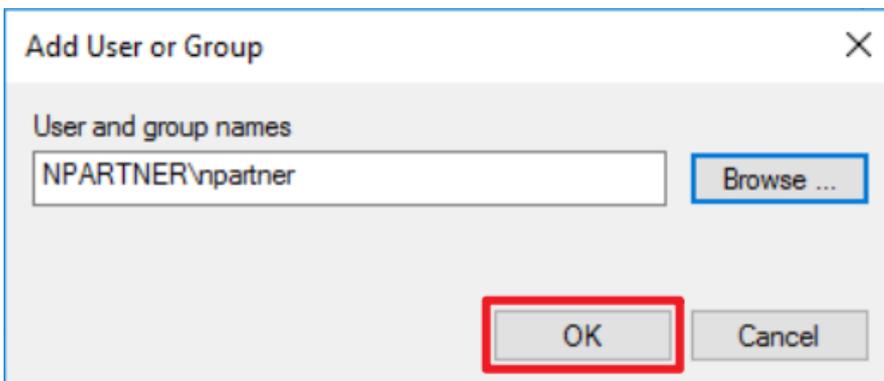


(6) Enter Your User Account

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

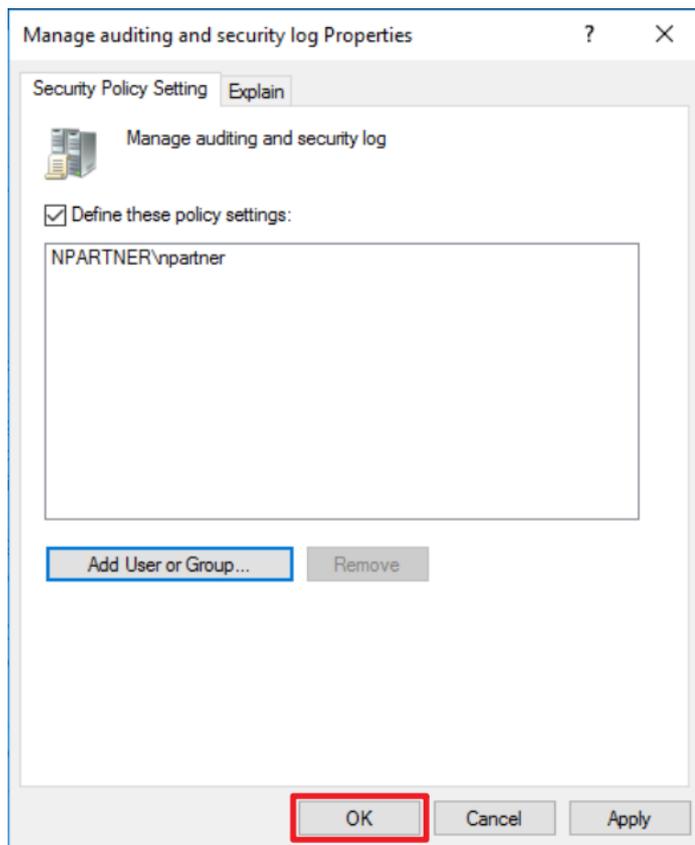


(7) Click "OK."



(8) Confirm Audit Log Settings

Click "OK."

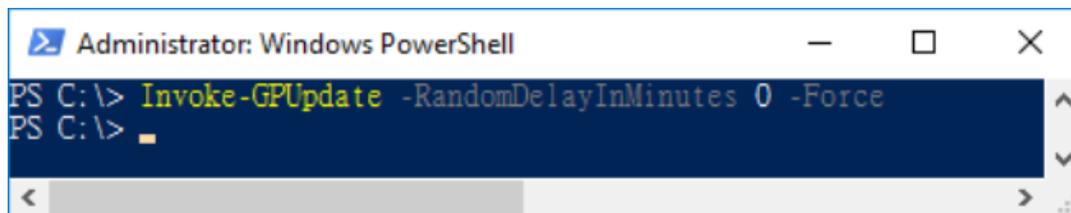


(9) Open "Windows Powershell."



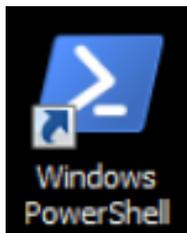
(10) Enter the command below to update group policy.

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



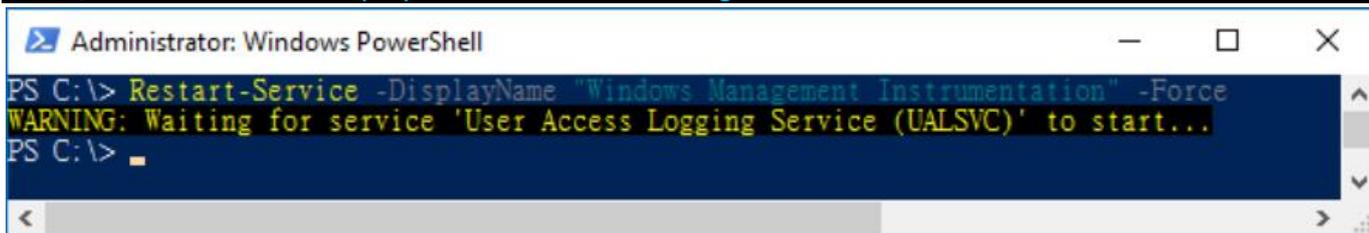
6.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”



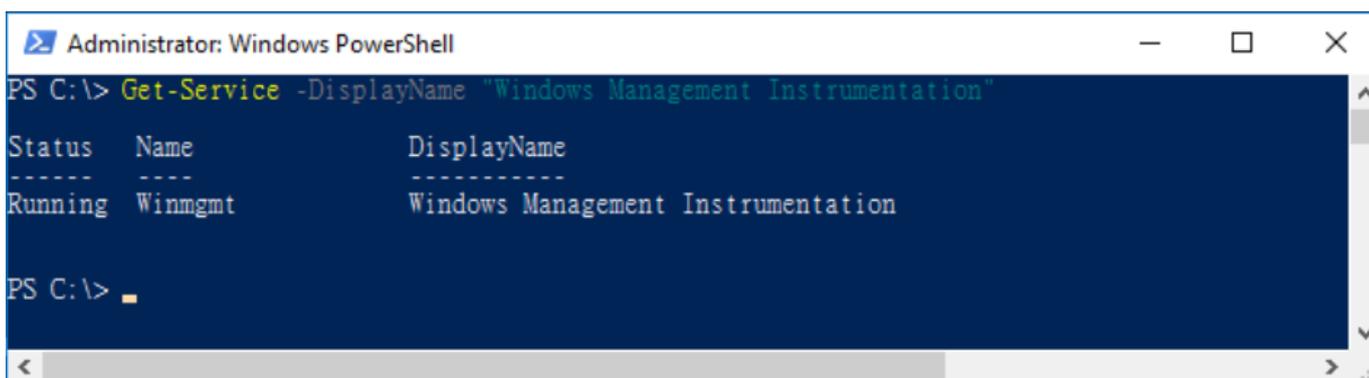
(2) Enter the command below to disable the WMI service.

```
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:

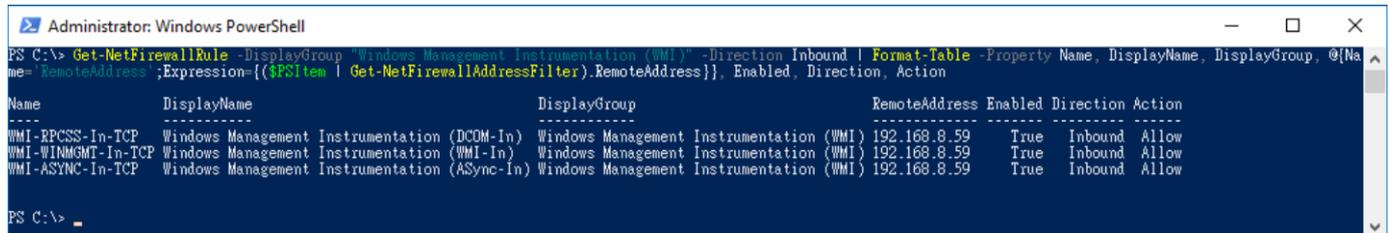
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True
```



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.

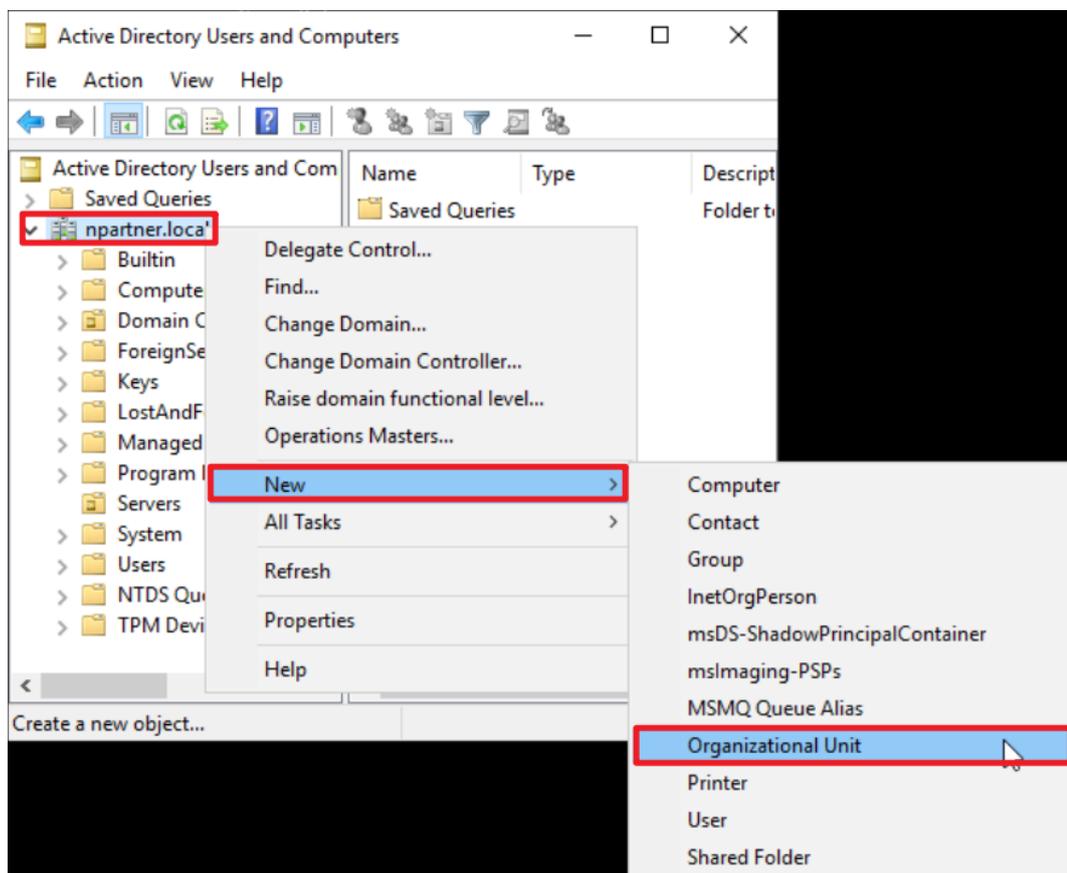
7.1 Organizational Unit (OU) Configuration

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



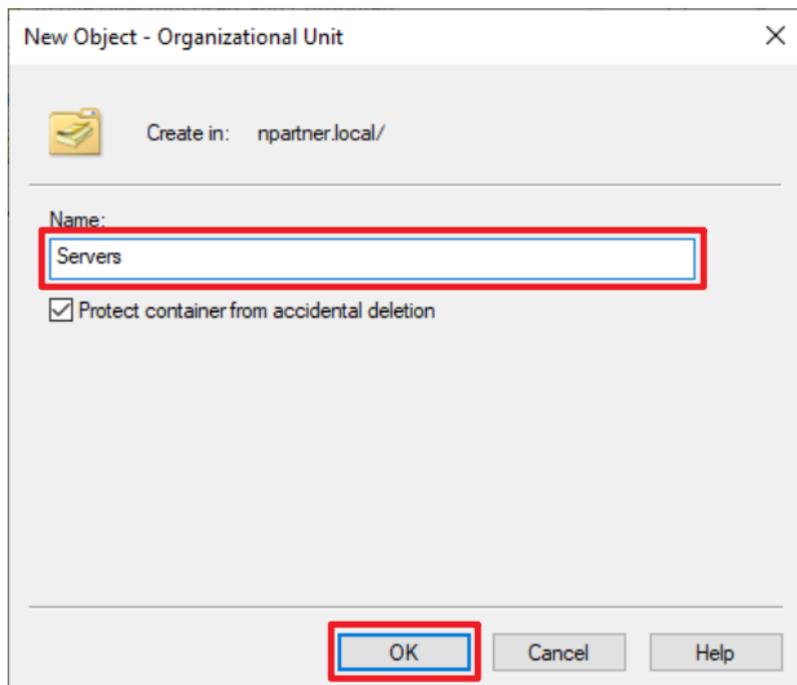
(2) Add an Organizational Unit

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



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

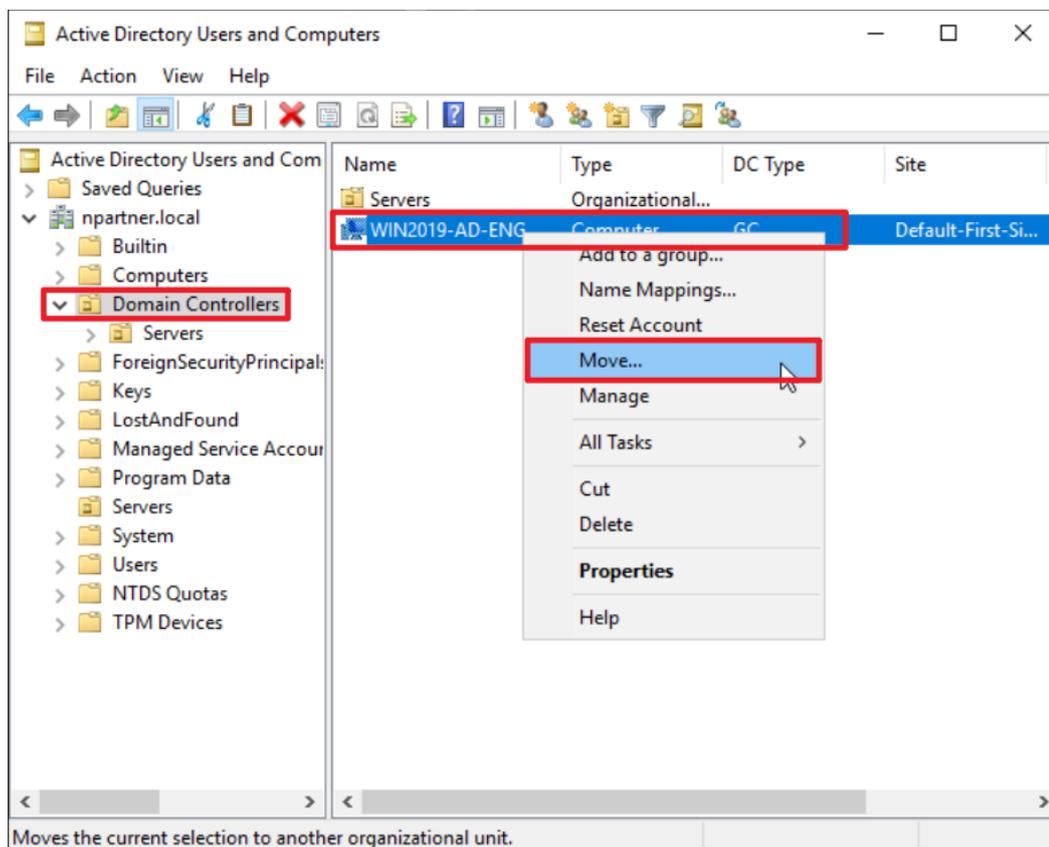
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

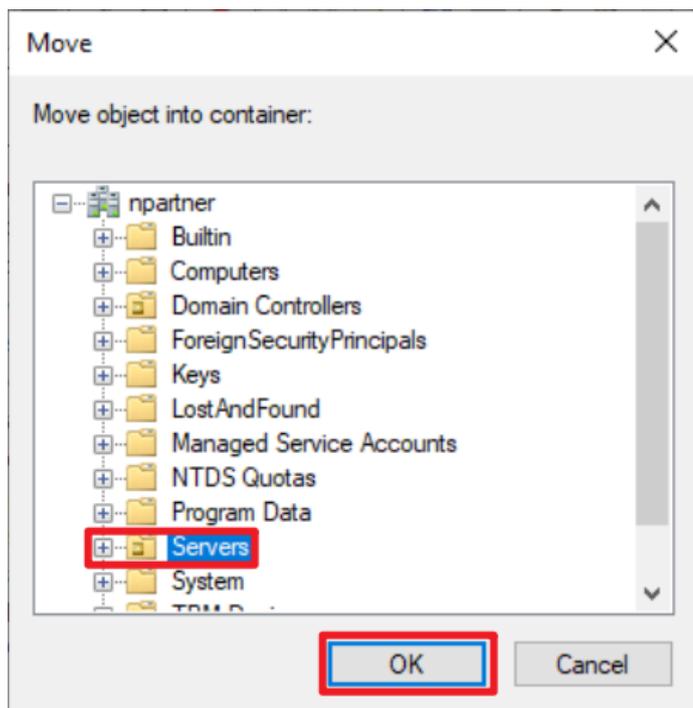
Select “Domain Controllers” → right-click on the “WIN2019-AD-ENG” server.

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



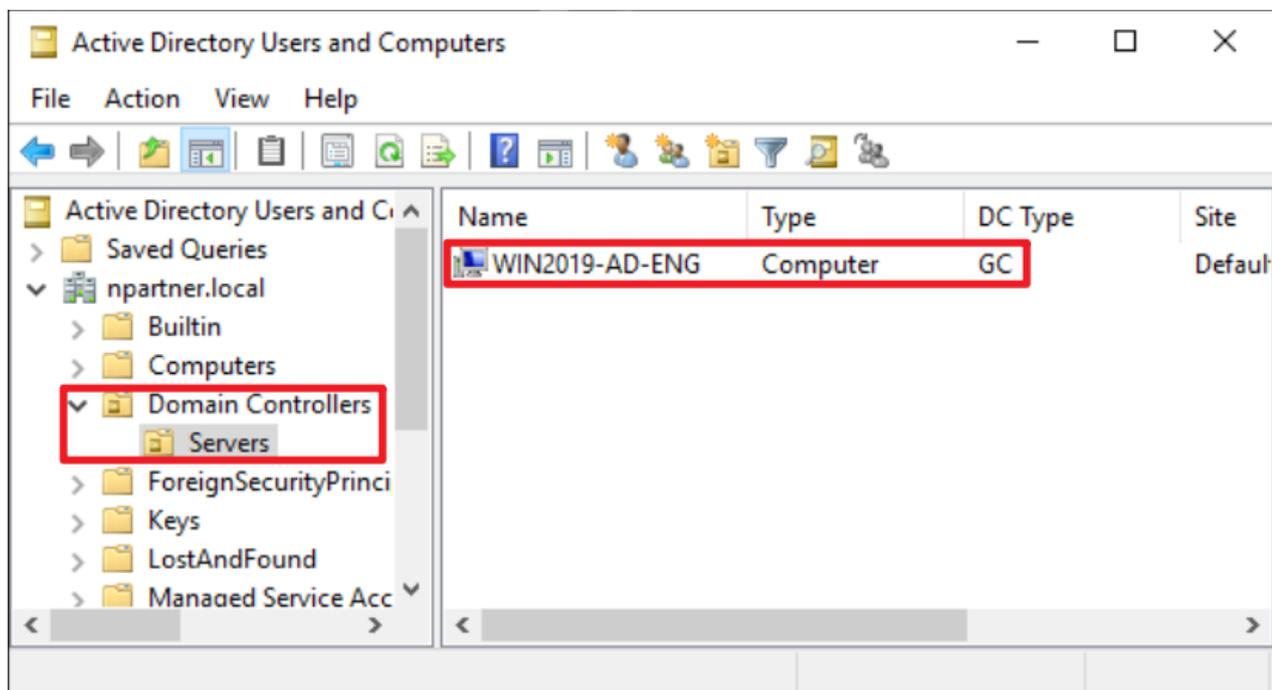
(5) Select your Organizational Unit:

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



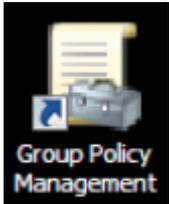
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



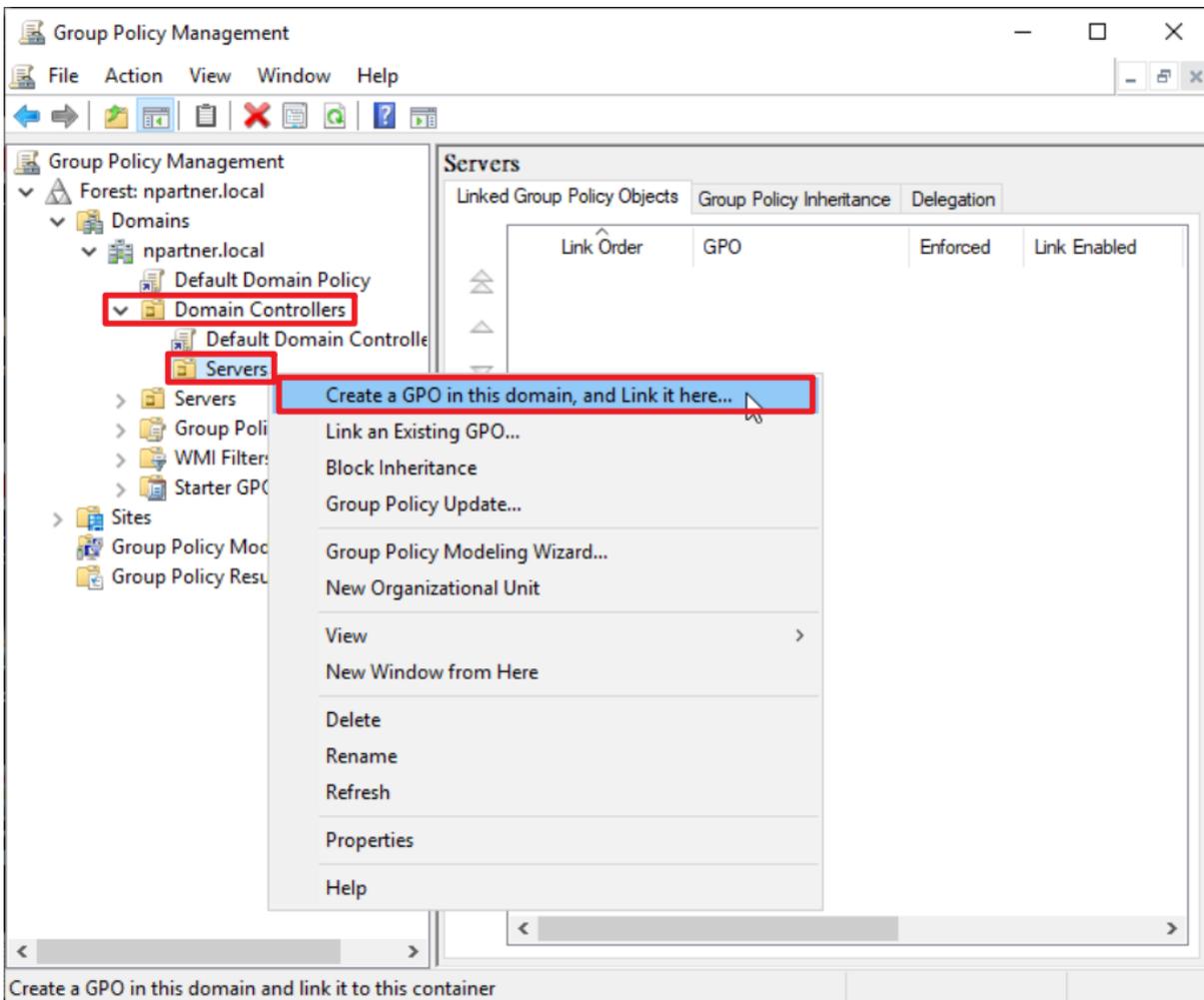
7.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

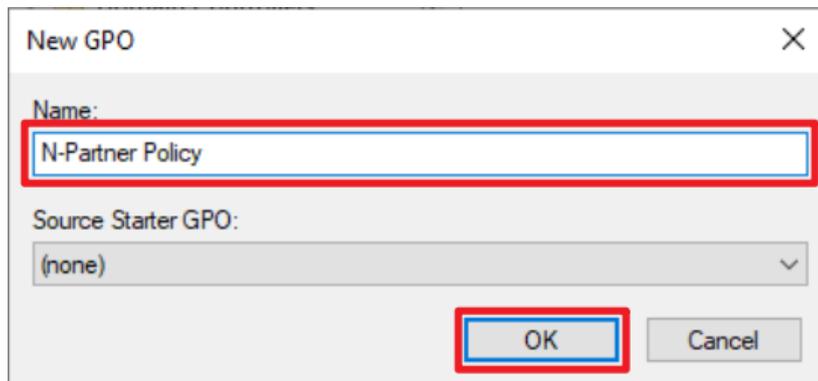
Right-click the “Servers” organizational unit under “Domain Controllers” → select “Create a GPO in this domain, and Link it here...”



(3) Enter your Group Policy Object

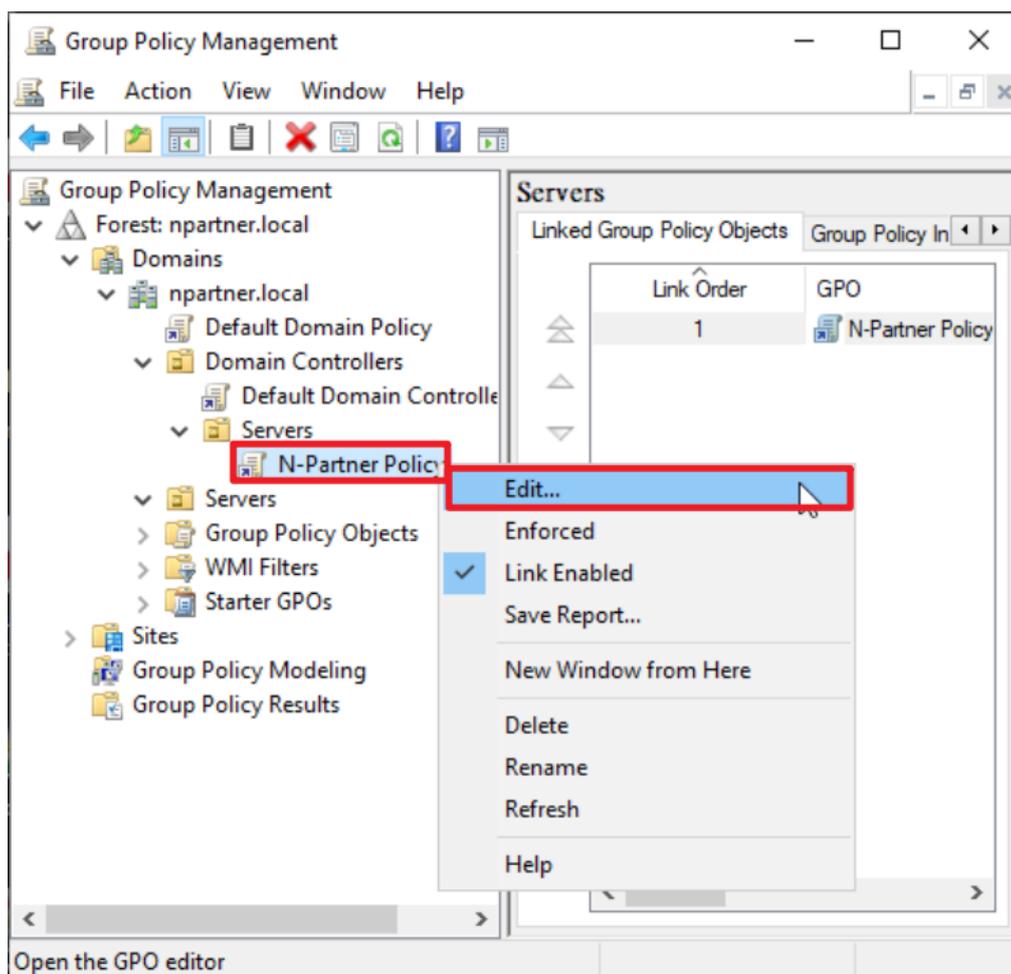
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



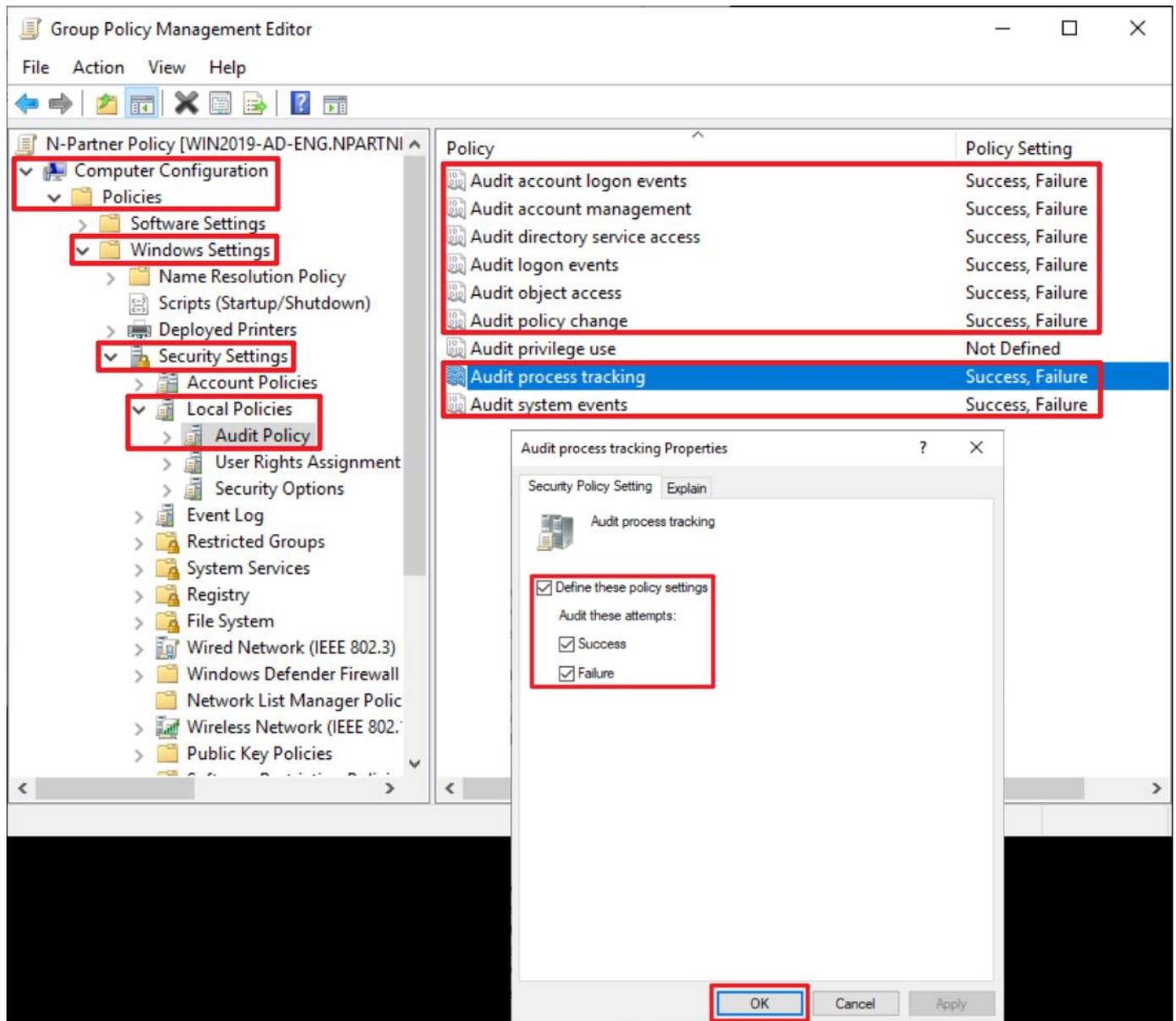
(4) Edit your Group Policy Object

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



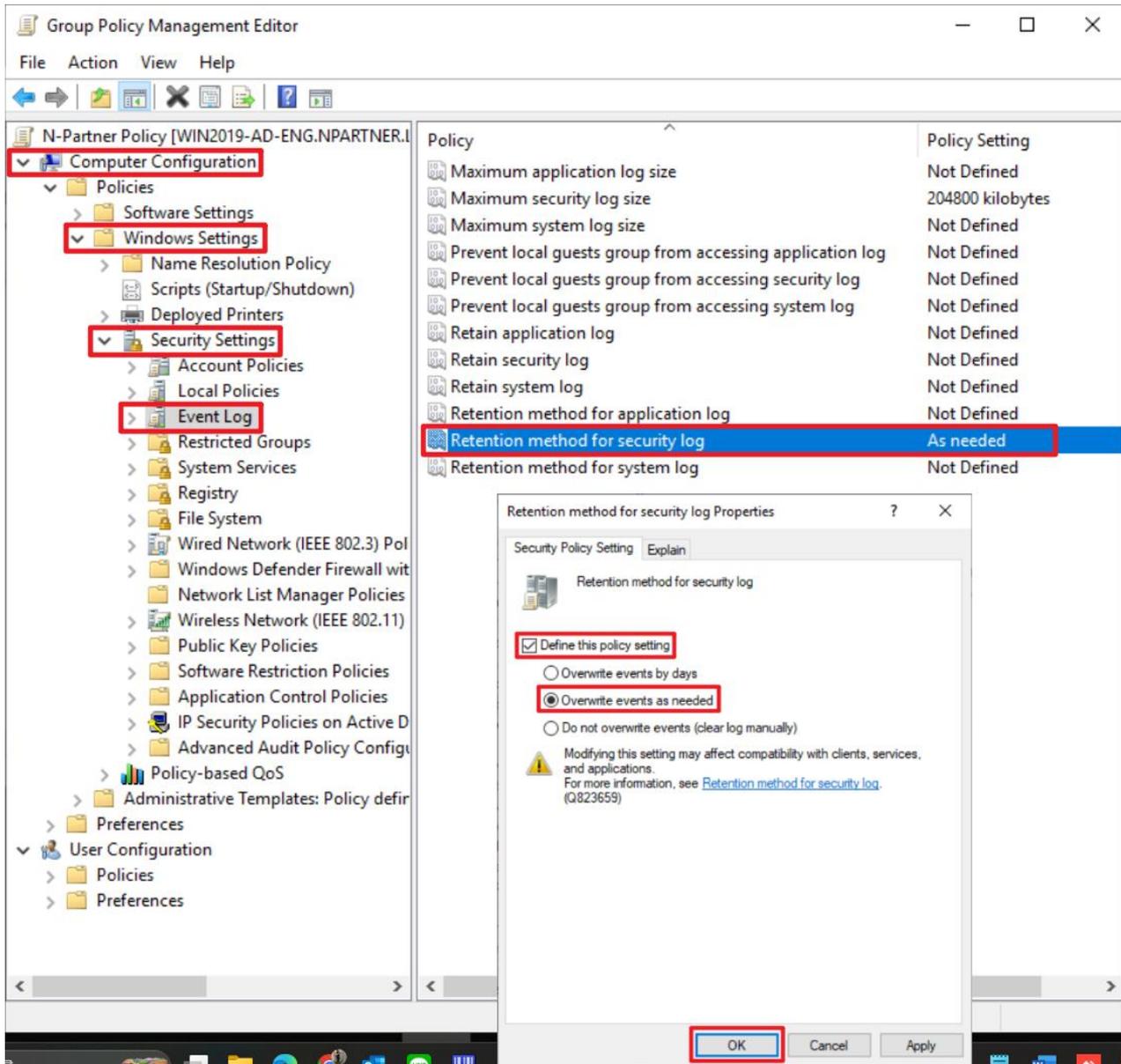
(5) Local Group Policies: Audit Policy

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.”

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

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

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



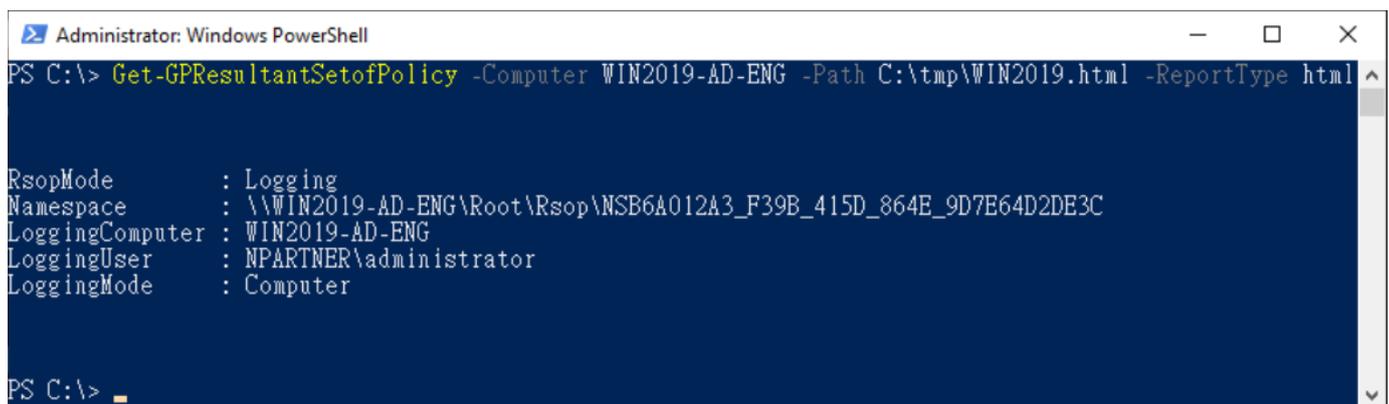
(9) Enter the command below to refresh group policy.

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



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

```
PS C:\> Get-GPResultantSetofPolicy -Computer 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.

The screenshot shows a web browser window with the address bar displaying 'file:///C:/tmp/Win2019.html#'. The browser tab is labeled 'NPARTNER\WIN2019-AD-E...'. The main content area displays a report titled 'Component Status' with a 'show' link. Below this are sections for 'Settings' (hide), 'Policies' (hide), 'Windows Settings' (hide), and 'Security Settings' (hide). Under 'Security Settings', there are sub-sections for 'Account Policies/Password Policy' (show), 'Account Policies/Account Lockout Policy' (show), 'Account Policies/Kerberos Policy' (show), and 'Local Policies/Audit Policy' (hide). The 'Local Policies/Audit Policy' section contains a table with the following data:

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

Below the table are sections for 'Local Policies/User Rights Assignment' (show), 'Local Policies/Security Options' (show), and 'Event Log' (hide). The 'Event Log' section contains a table with the following data:

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

At the bottom of the report, there is a partially visible section for 'Public Key Policies/Certificate Services Client - Auto Enrollment Settings'.

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
```

```
Administrator: Windows PowerShell
PS C:\> Get-ADUser -Identity npartner -Properties * | Format-List DisplayName, Description, PhysicalDeliveryOfficeName, Department, EmployeeID, EmployeeNumber
DisplayName           : npartner
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department           : TAC
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
```

```
Administrator: Active Directory Module for Windows PowerShell
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 -fo
rce) -PasswordNeverExpires $True -Enabled $True
PS C:\> _
```

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
```

```
Administrator: Active Directory Module for Windows PowerShell
PS C:\> Get-ADUser npartner -Properties PasswordNeverExpires, Enabled

DistinguishedName      : CN=npartner,CN=Users,DC=npartner,DC=local
Enabled                : True
GivenName              :
Name                   : npartner
ObjectClass            : user
ObjectGUID             : 5af71a6f-8242-4dab-ac1a-607ede15ad61
PasswordNeverExpires  : True
SamAccountName         : npartner
SID                    : S-1-5-21-2363543998-1723094790-3155426774-1107
Surname                :
UserPrincipalName      : npartner@npartner.local

PS C:\> _
```

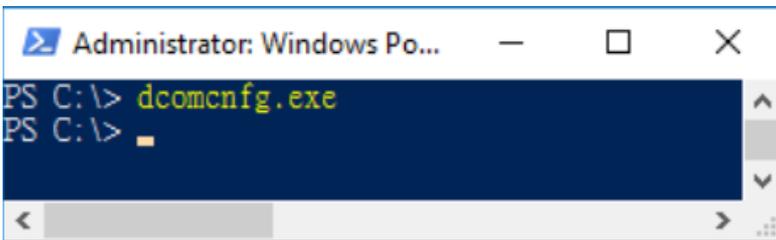
7.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”



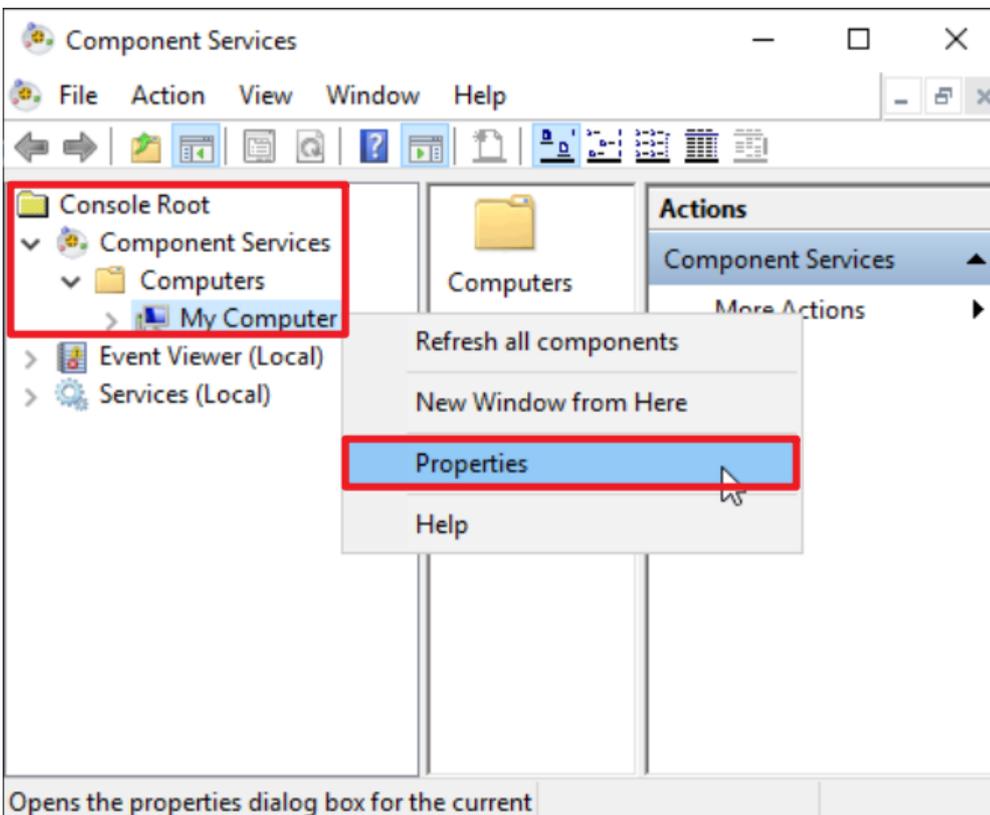
(2) Enter the command below to enable component services.

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



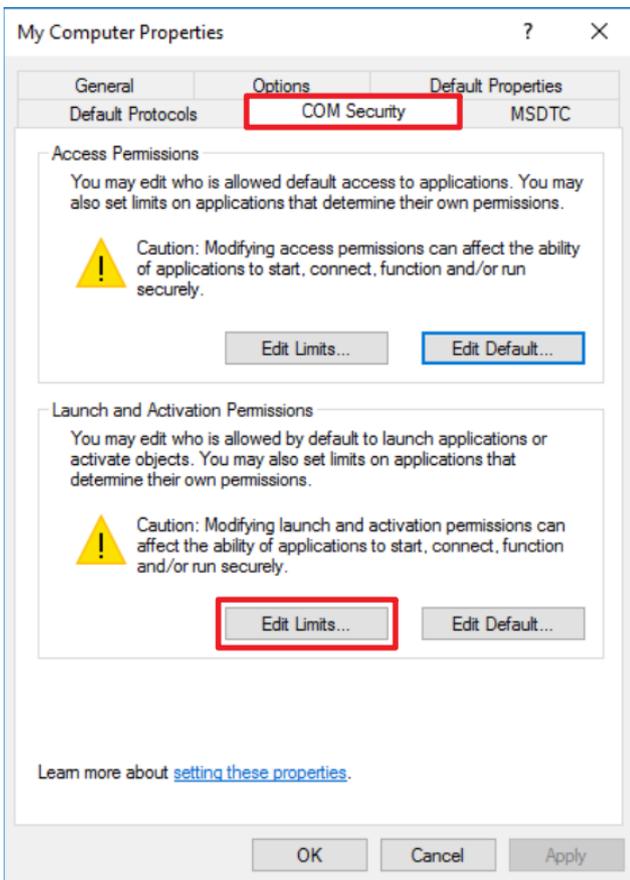
(3) Edit Computer Properties

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



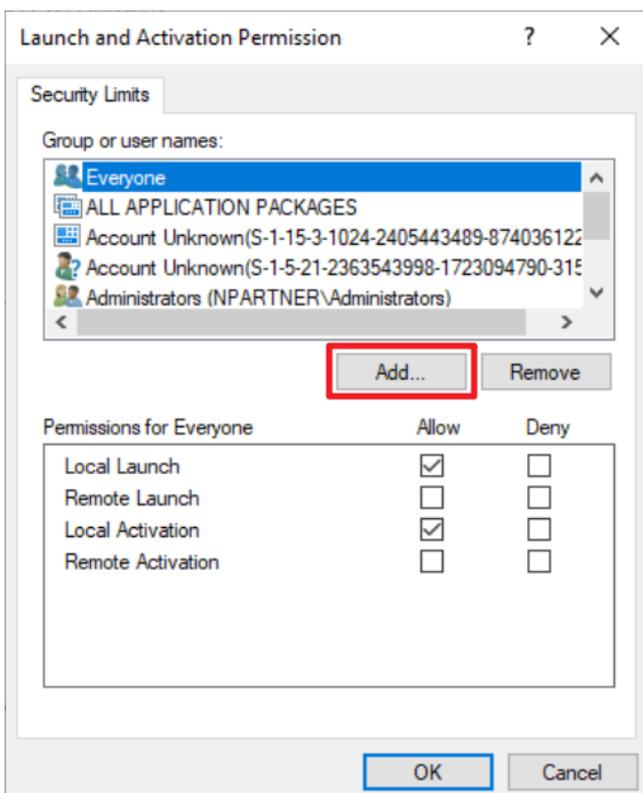
(4) Enable Permissions

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



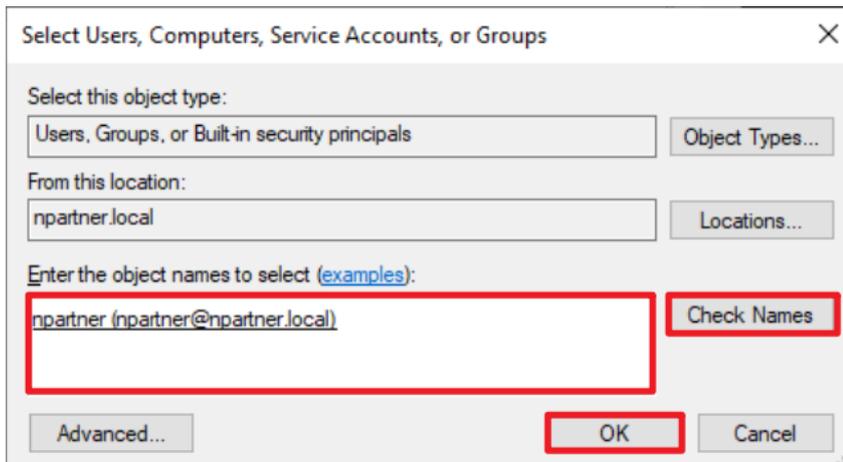
(5) Add DCOM User Permissions

Click “Add.”



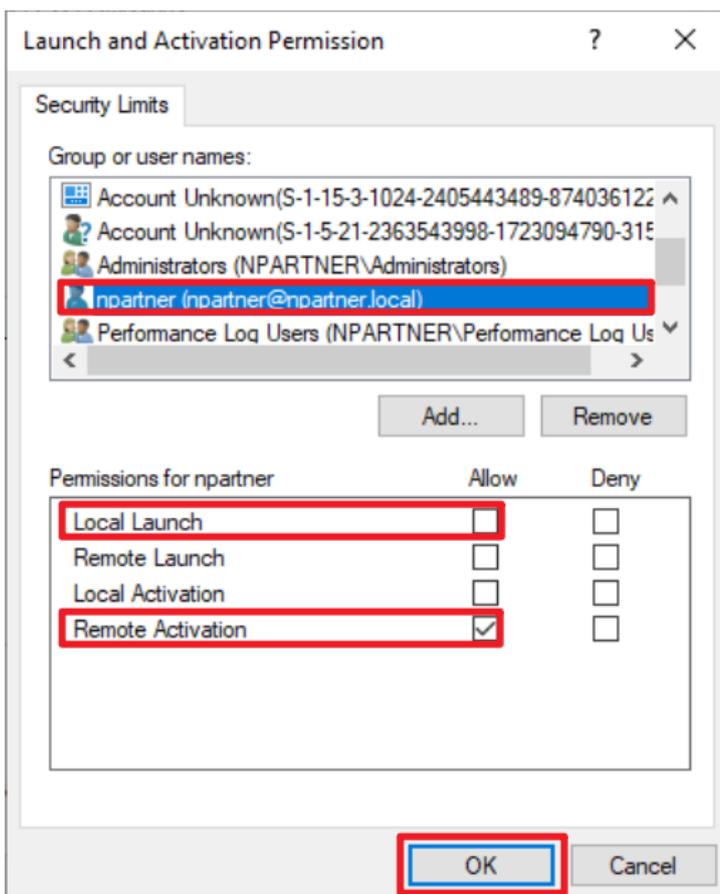
(6) Enter Your Username

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

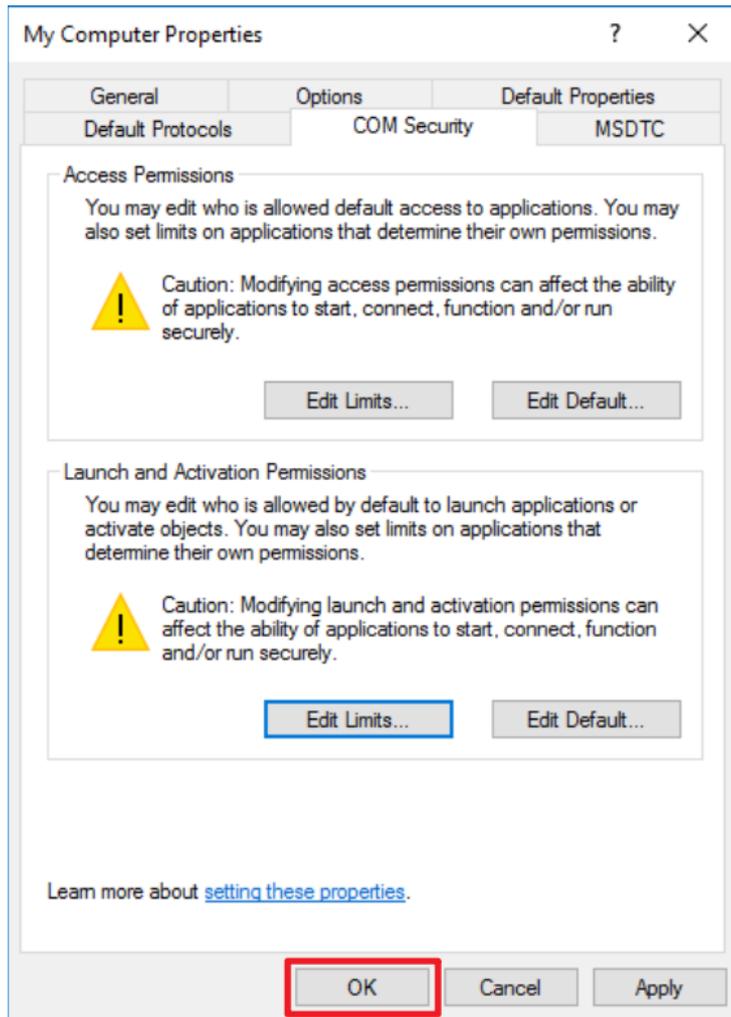


(7) Configure your User Permission

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

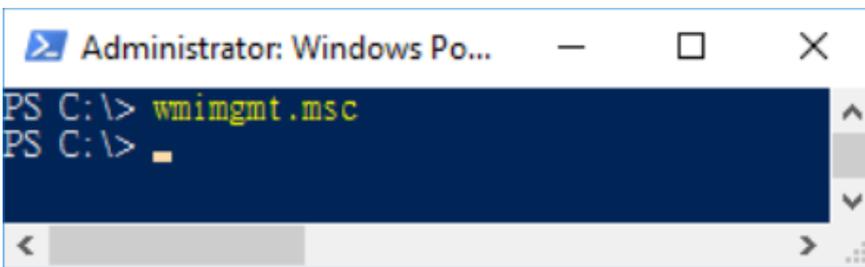
7.3.3.1 Configure Event Log Permissions

(1) Open “Windows Powershell.”



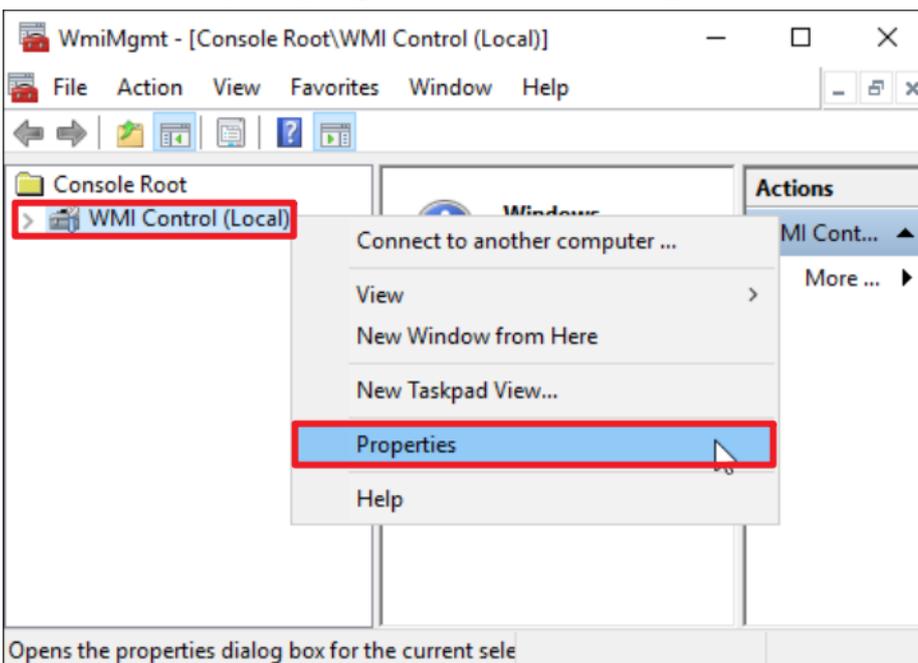
(2) Enter the command to enable WMI control service.

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



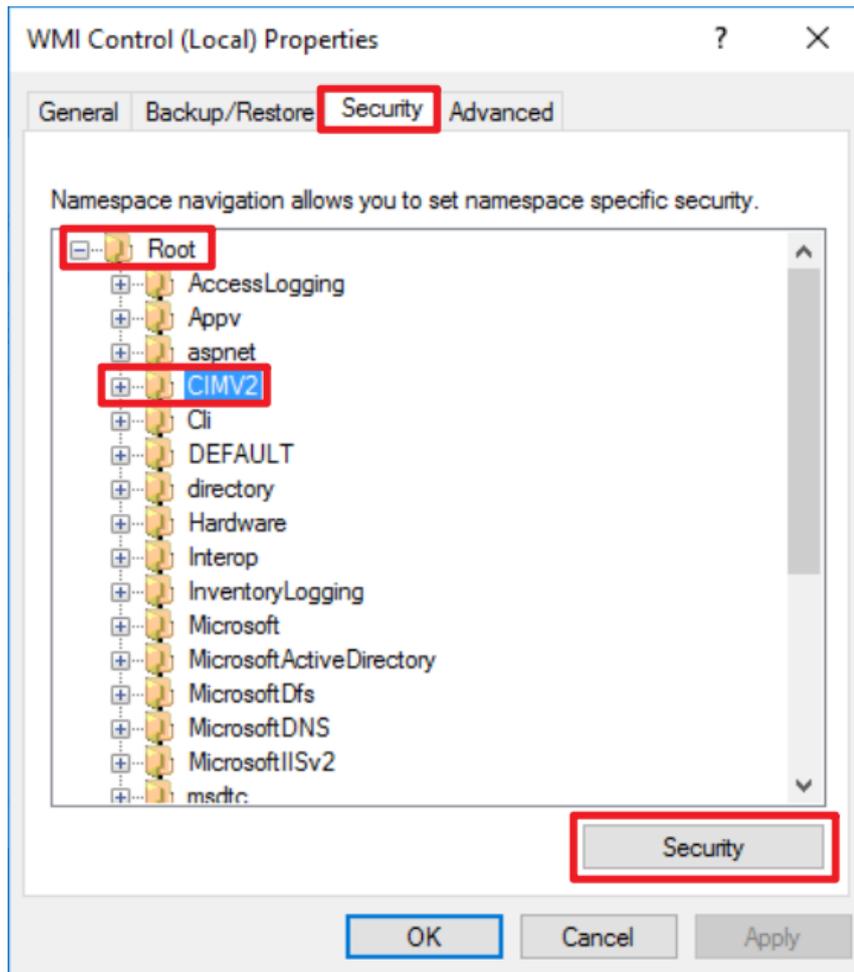
(3) Edit WMI Control

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



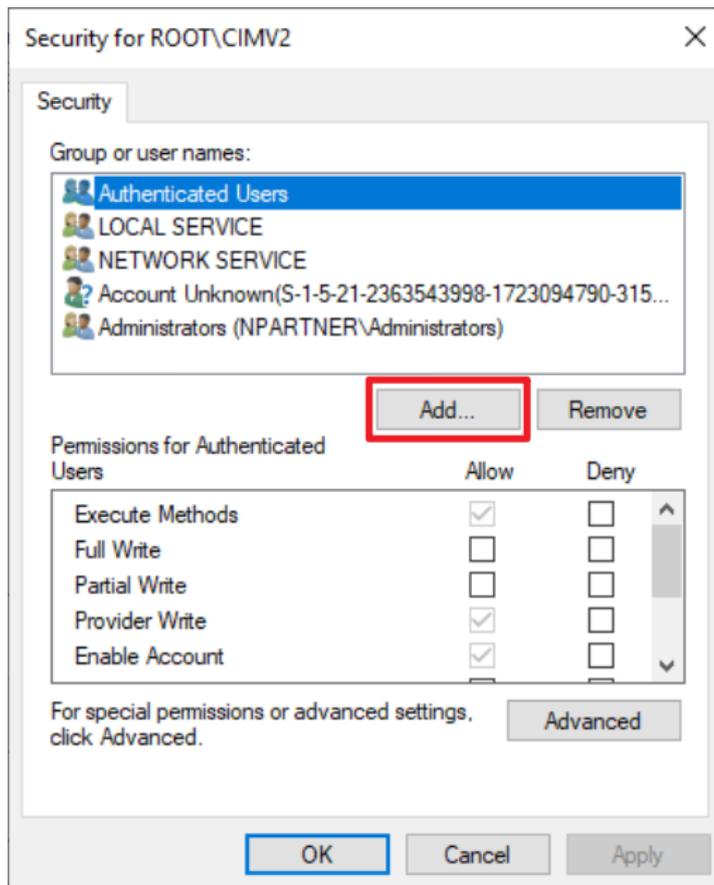
(4) Edit CIMV2 Security

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



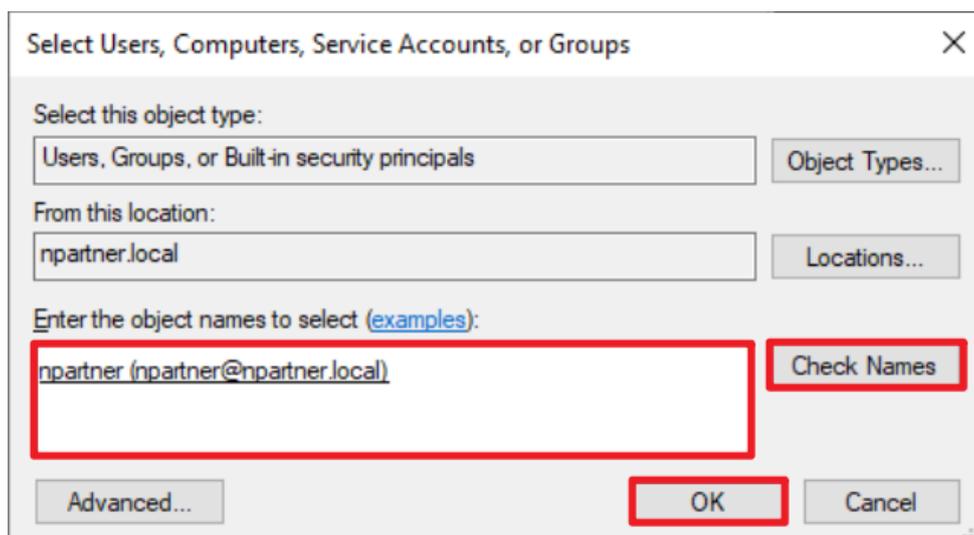
(5) Add WMI User Permissions.

Click “Add.”



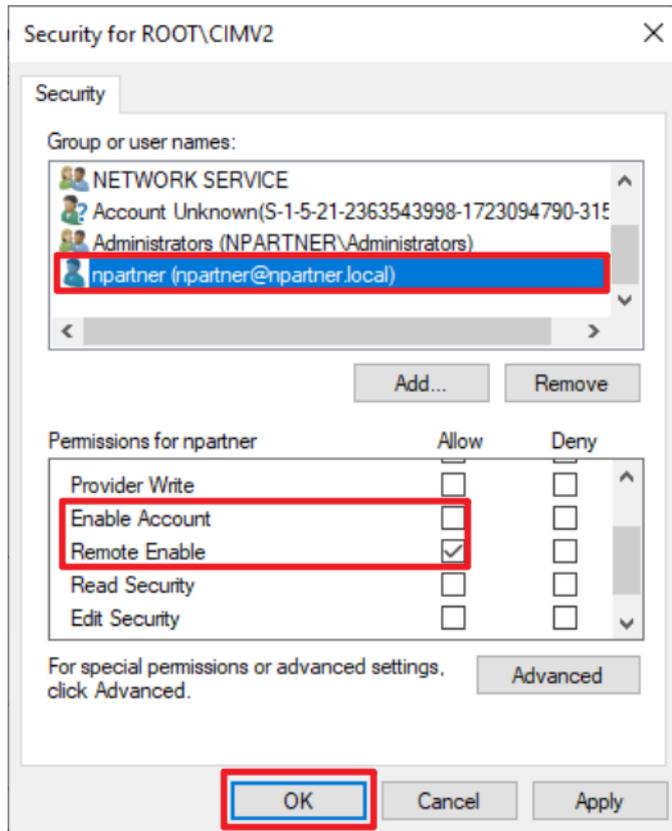
(6) Enter Your Username

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

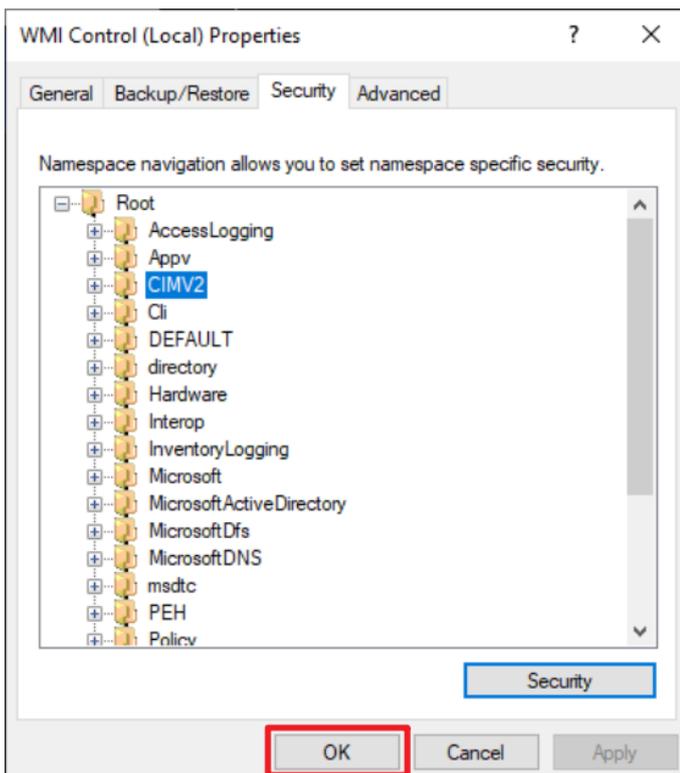


(7) Set Your User Permissions

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



(8) Click “OK.”



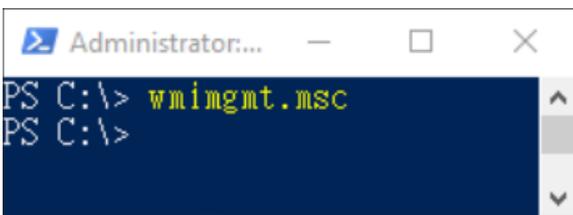
7.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



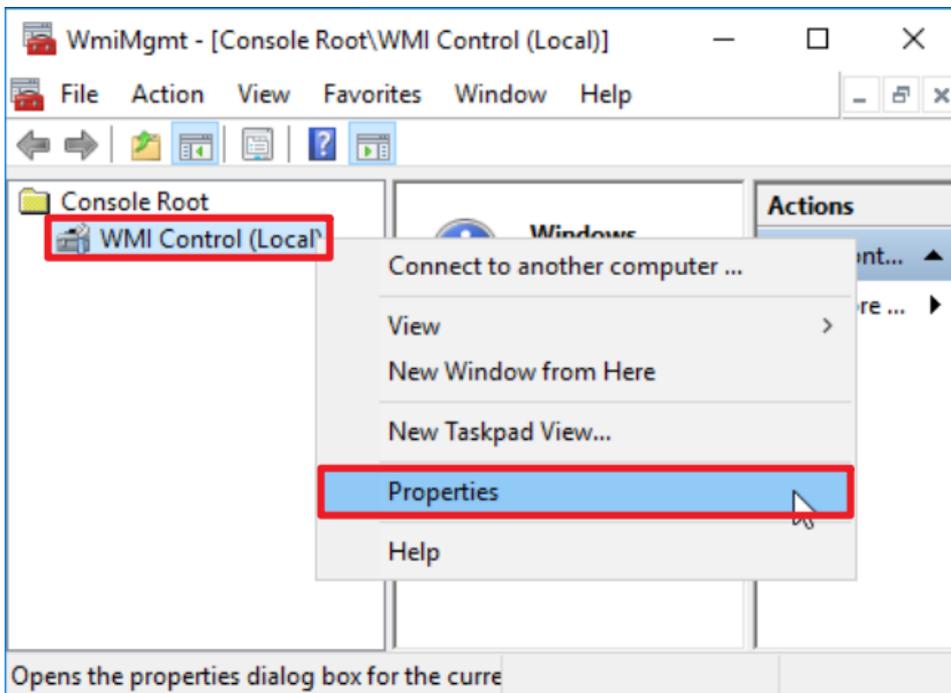
(2) Enter the command below to enable WMI Control.

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



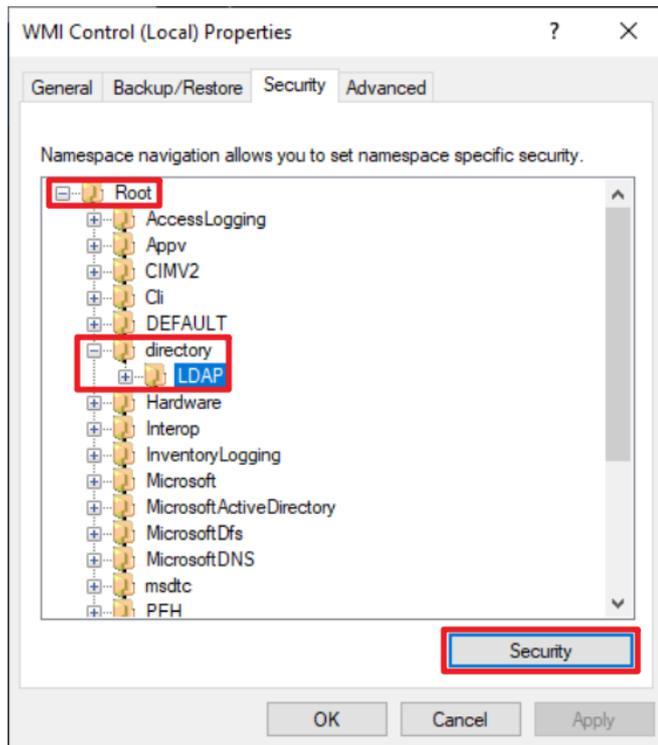
(3) Edit WMI Control

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



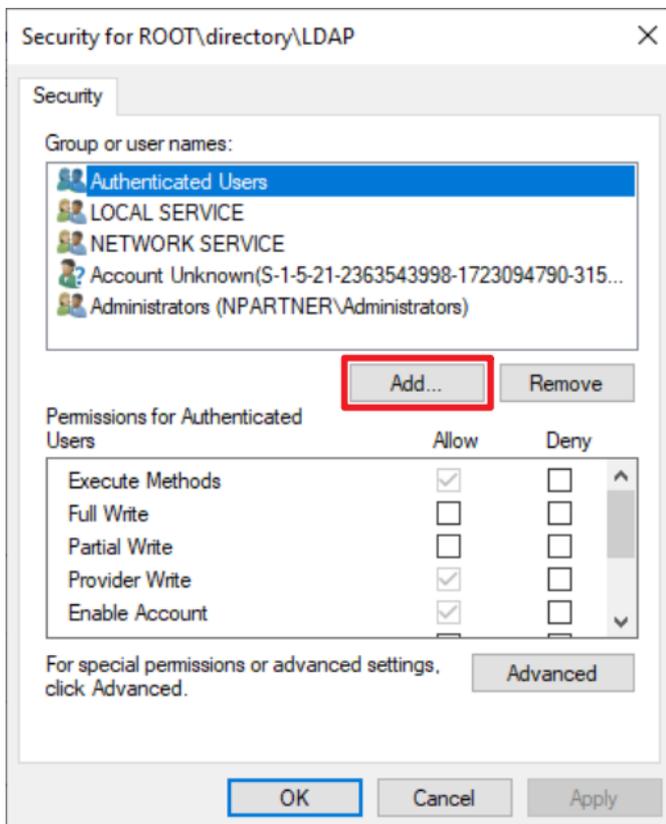
(4) Edit LDAP Security

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



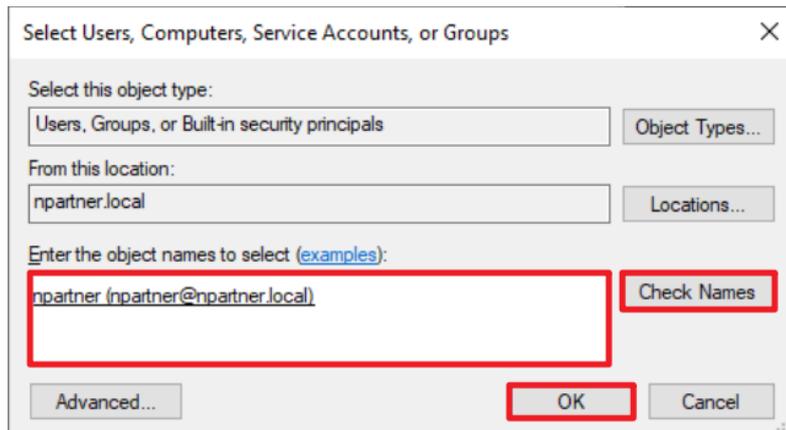
(5) Add WMI User Permissions

Click "Add."



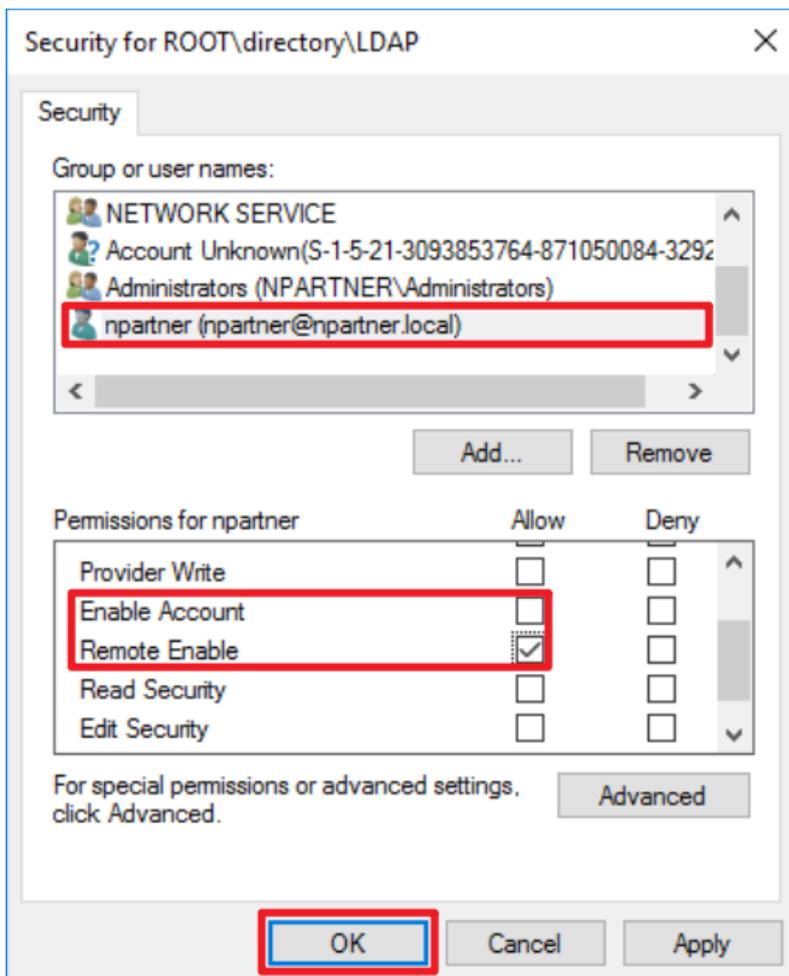
(6) Enter Your Username

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

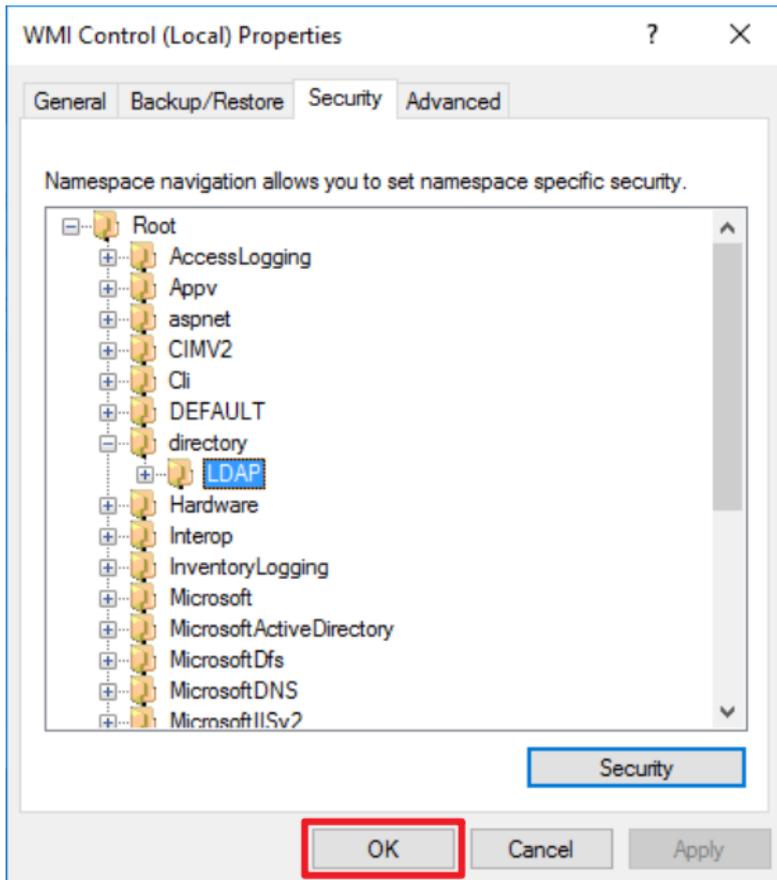


(7) Set Your User Permissions

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

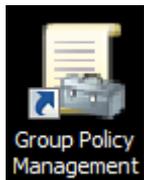


(8) Click "OK."

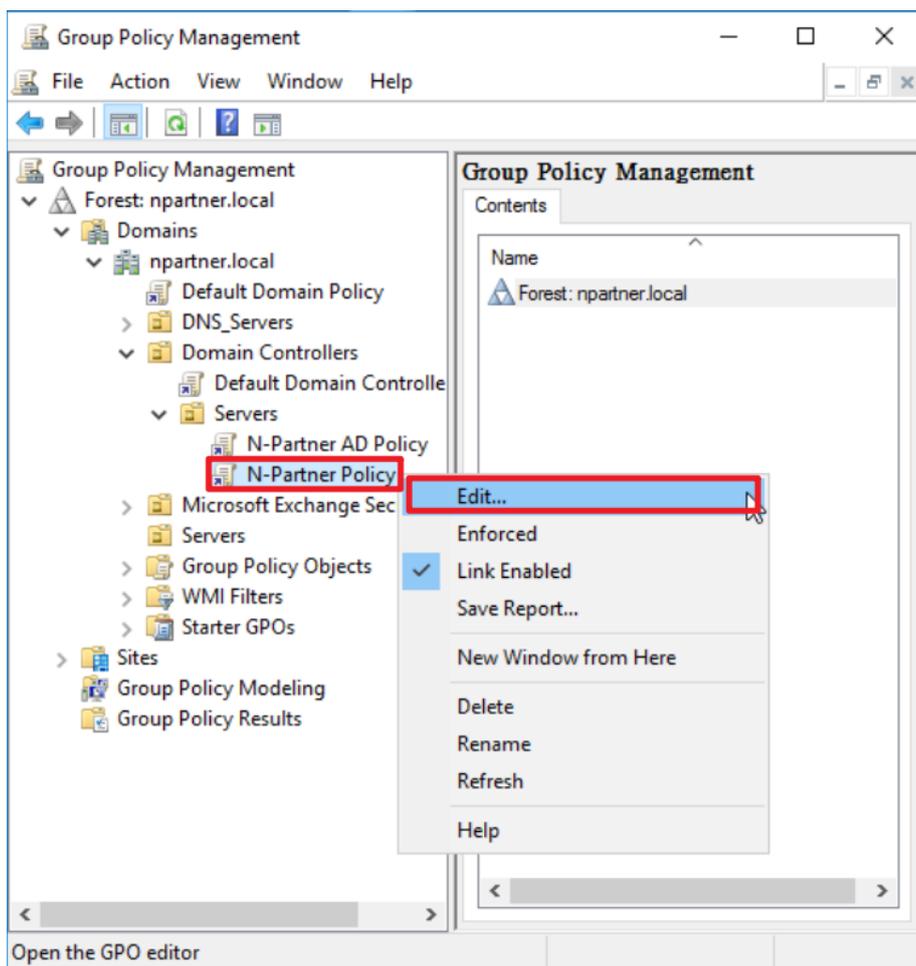


7.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

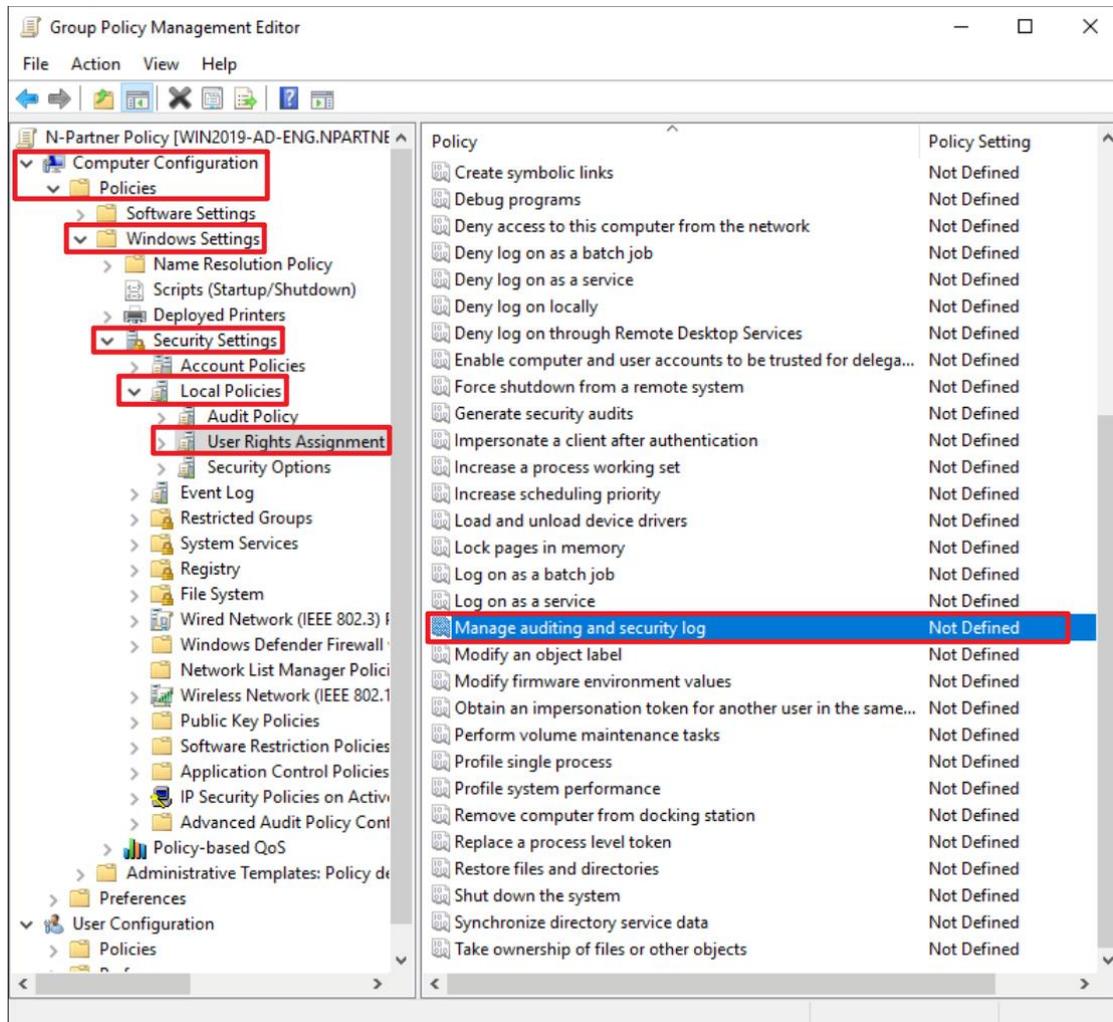


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



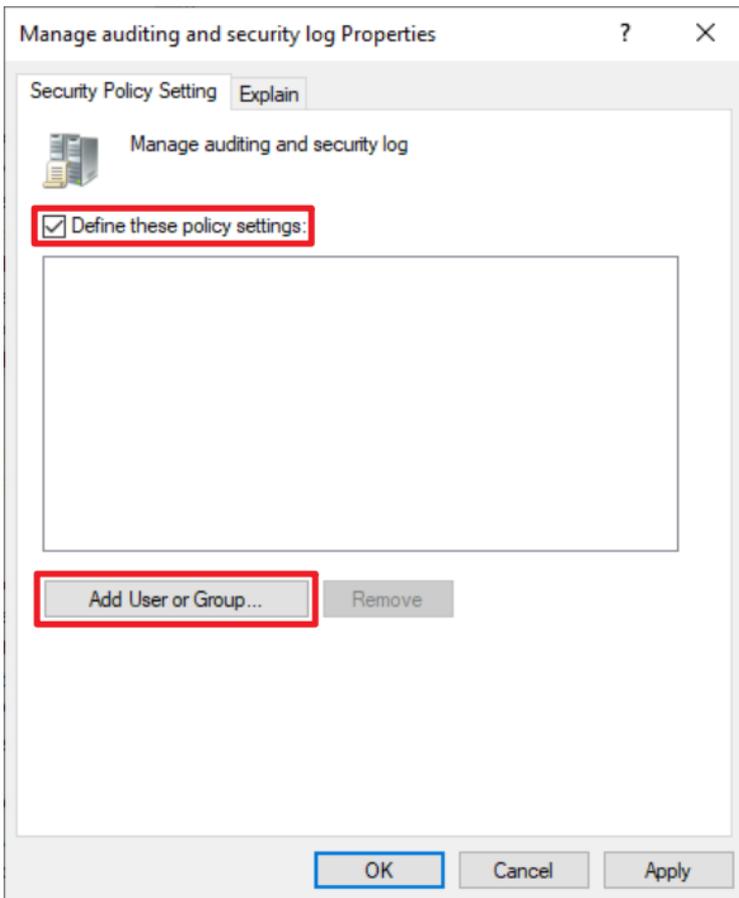
(3) Configure Auditing Log

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



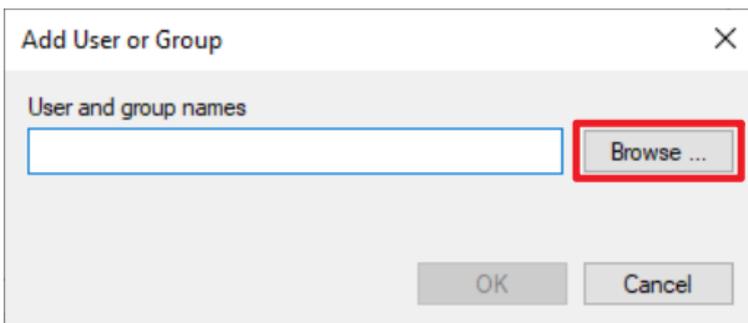
(4) Add Auditing User

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



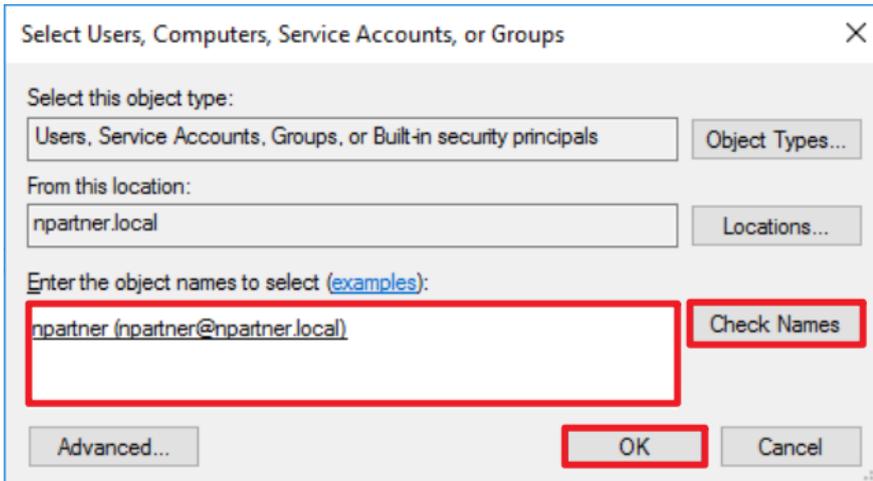
(5) Search for User

Click “Browse.”

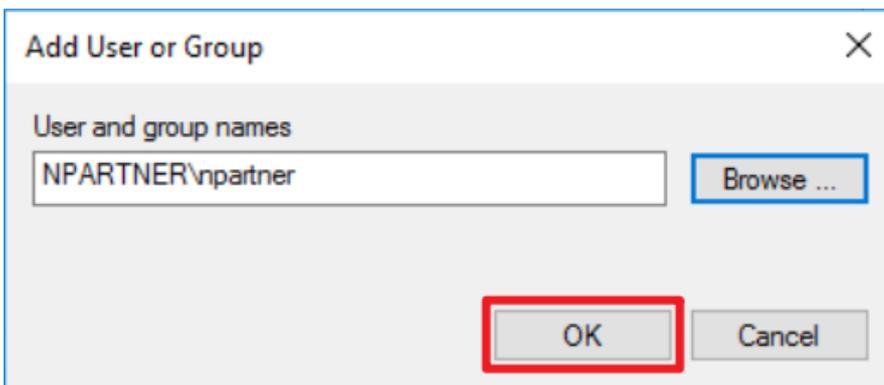


(6) Enter Your User Account

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

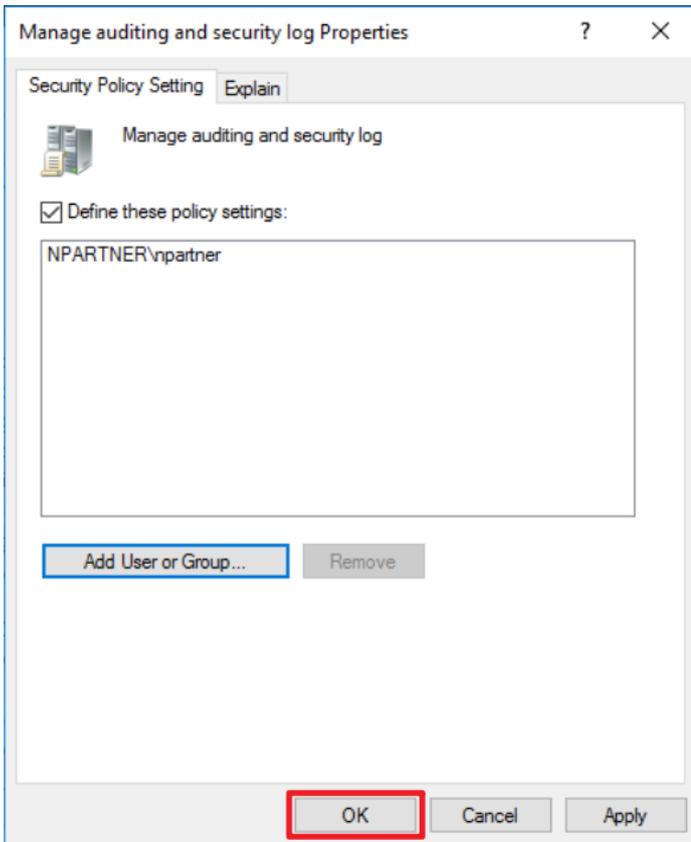


(7) Click “OK.”



(8) Confirm Audit Log Settings

Click "OK."

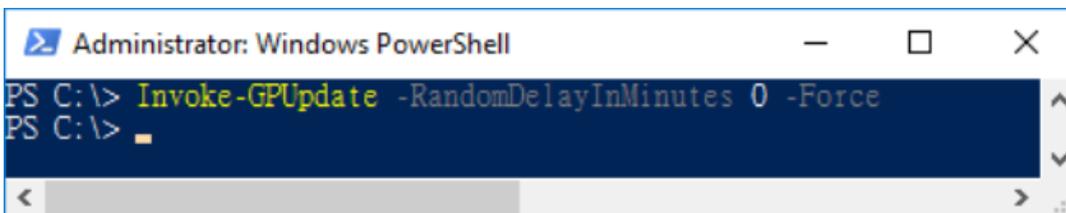


(9) Open "Windows Powershell."



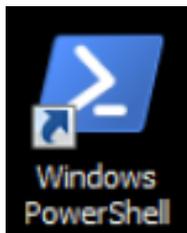
(10) Enter the command below to update group policy.

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



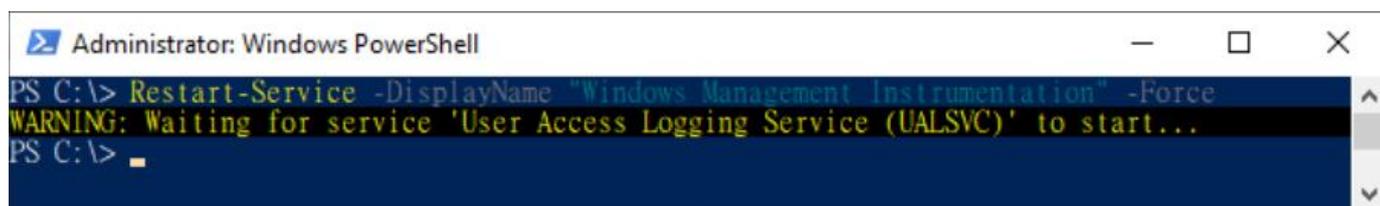
7.3.5 Restart the WMI Service

(1) Open “Windows Powershell.”



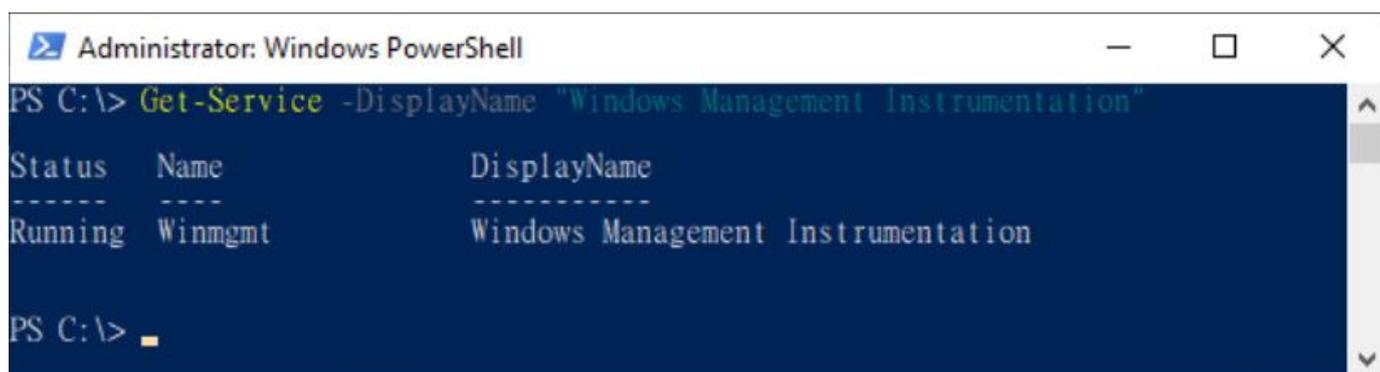
(2) Enter the command below to disable the WMI service.

```
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:

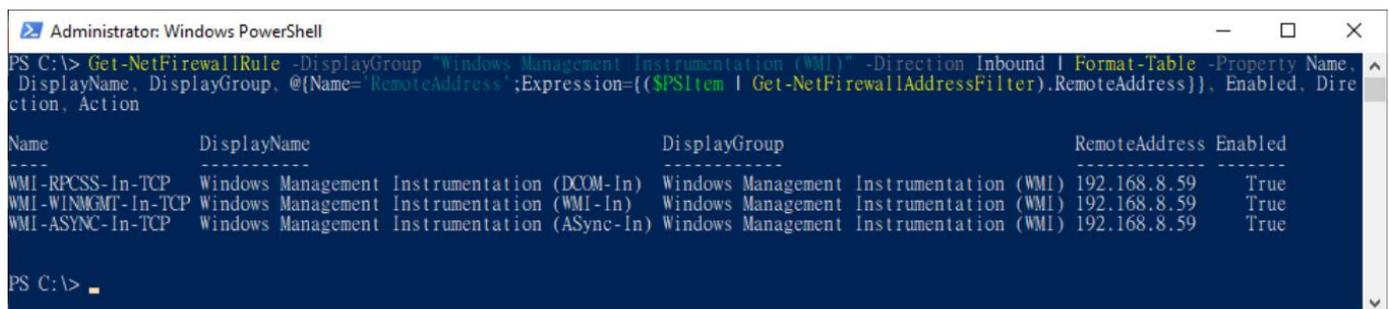
```
PS C:\> Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True
```



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.

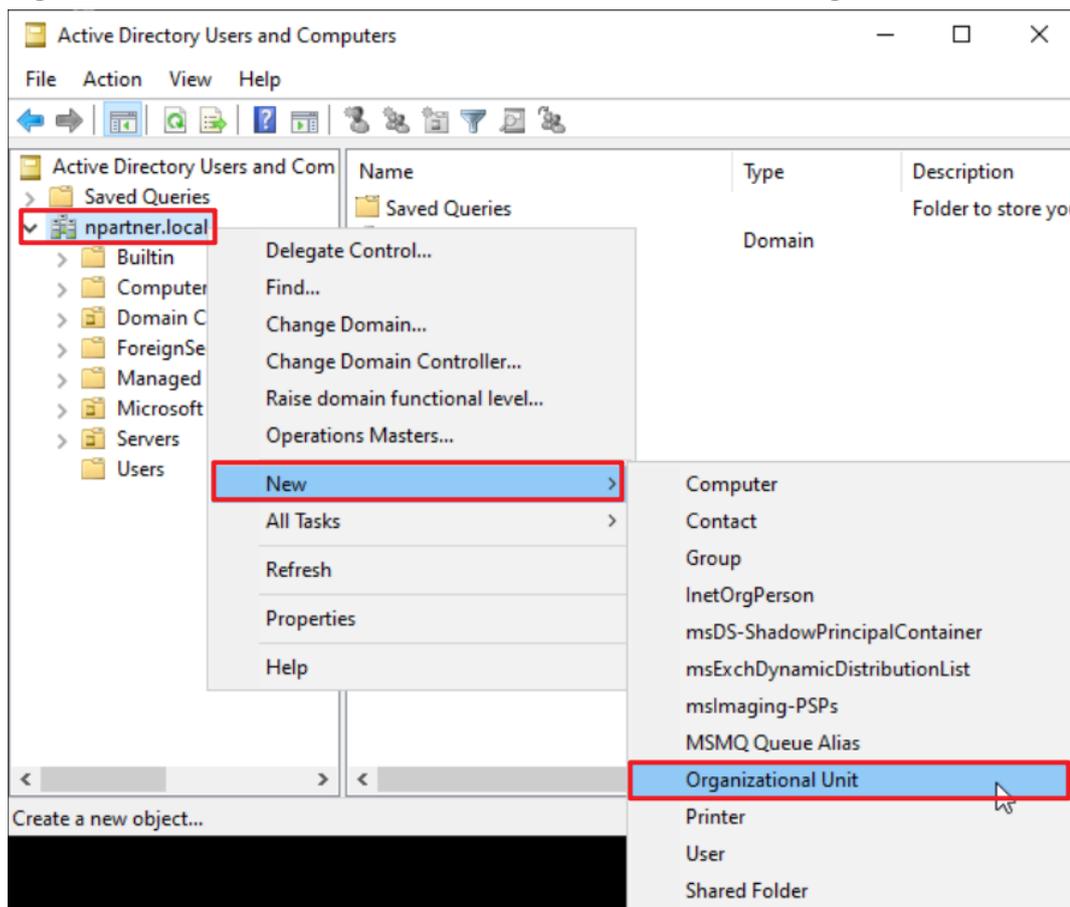
8.1 Organizational Unit (OU) Configuration

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



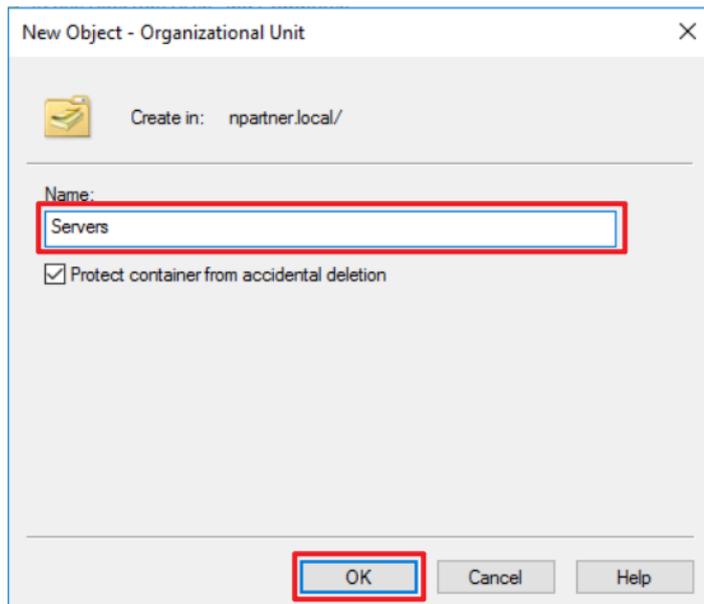
(2) Add an Organizational Unit

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



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

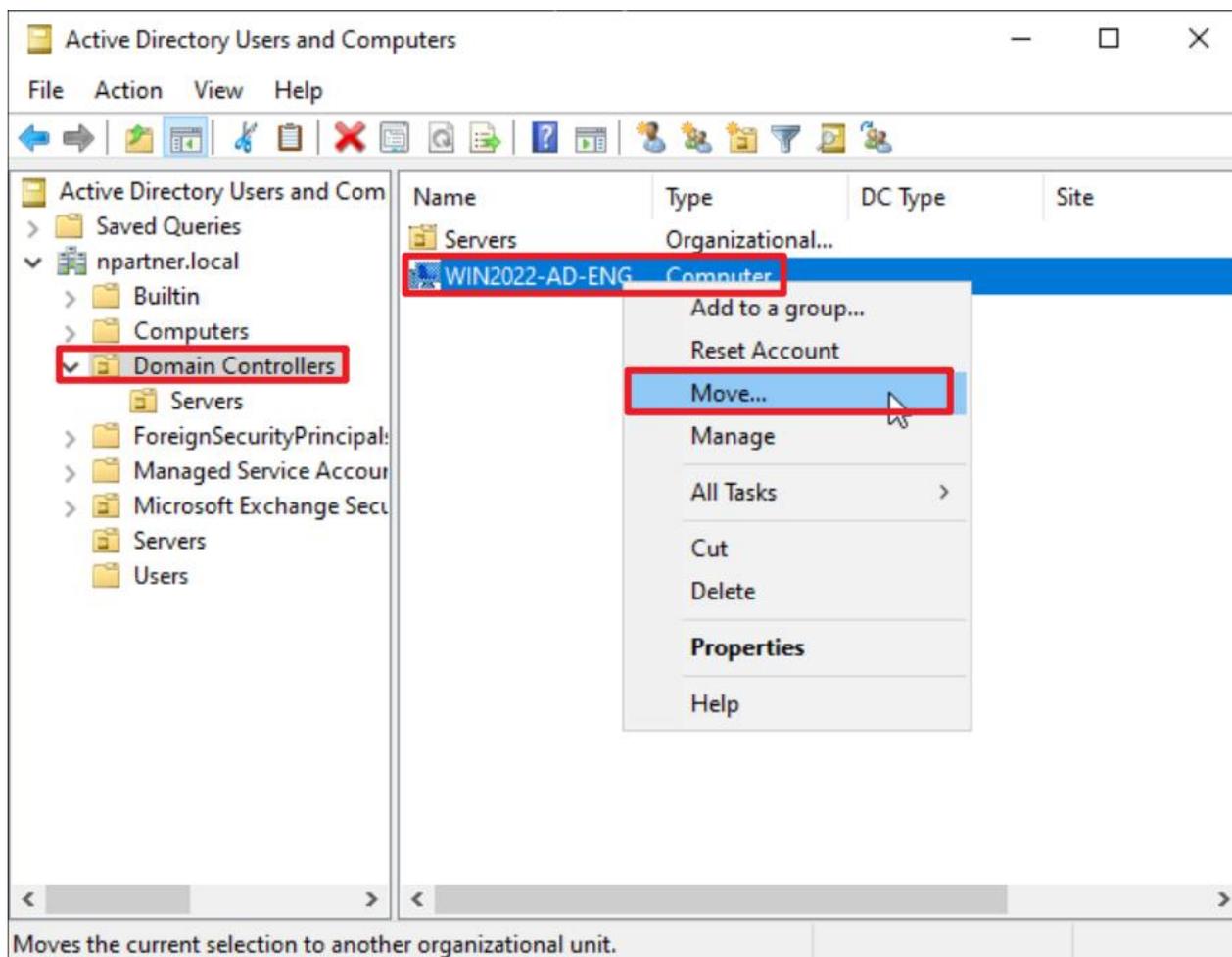
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

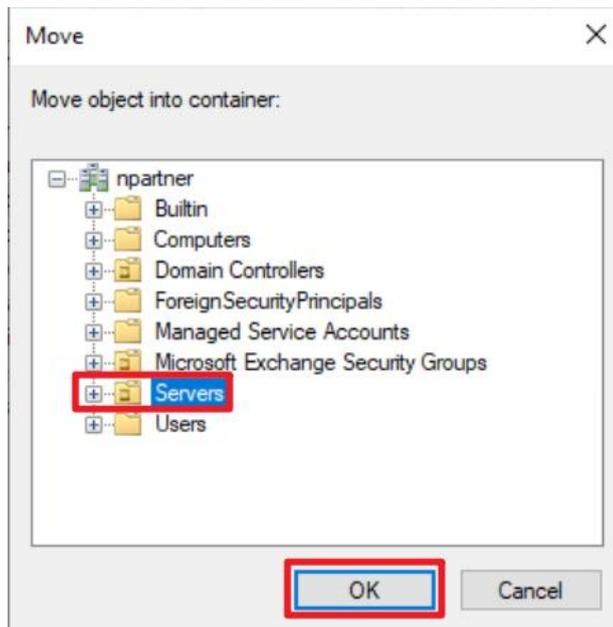
Select your organizational unit in “Domain Controllers” → right-click on the “WIN2022-AD-ENG” server.

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



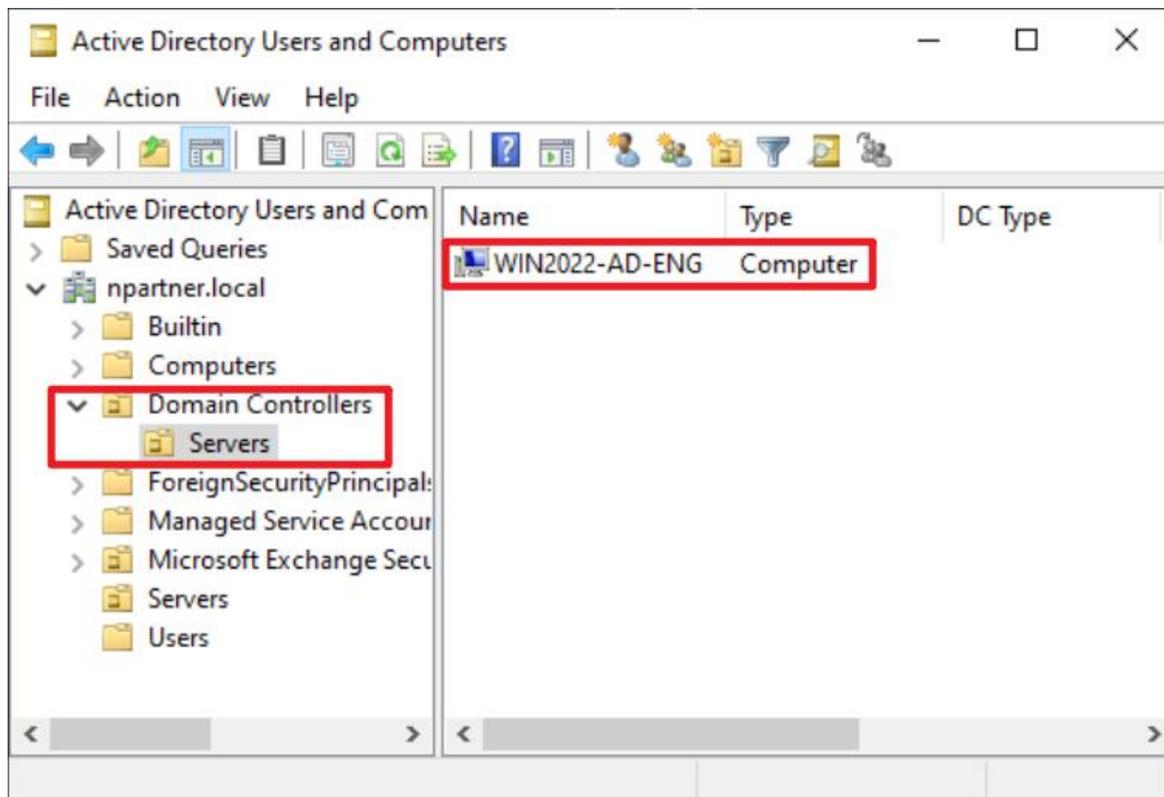
(5) Select your Organizational Unit:

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.



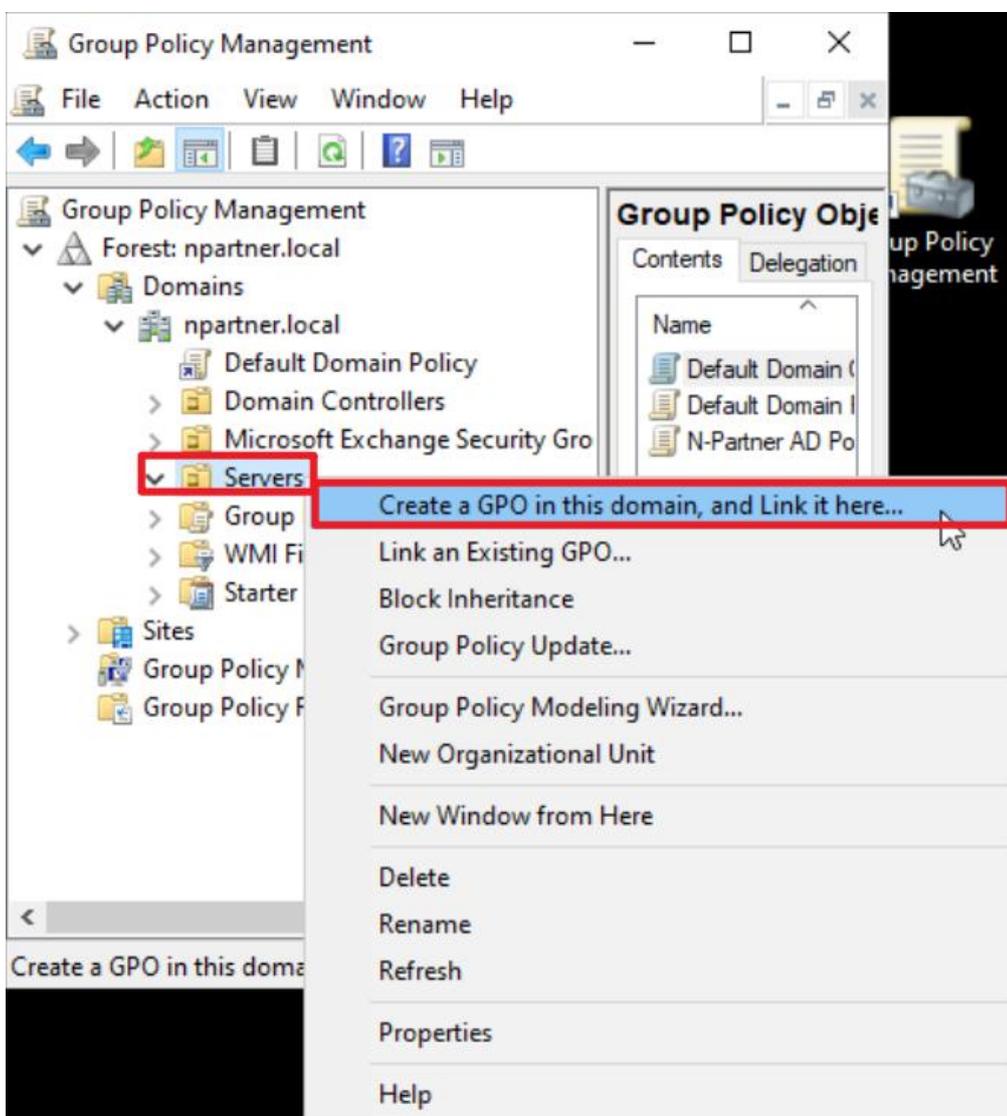
8.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

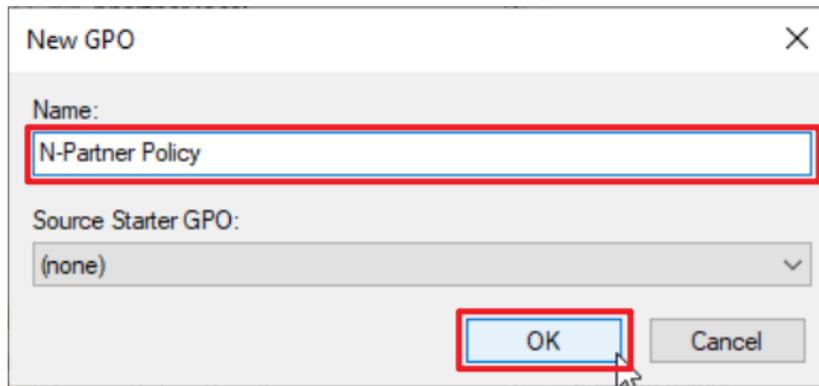
Right-click the “Servers” organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

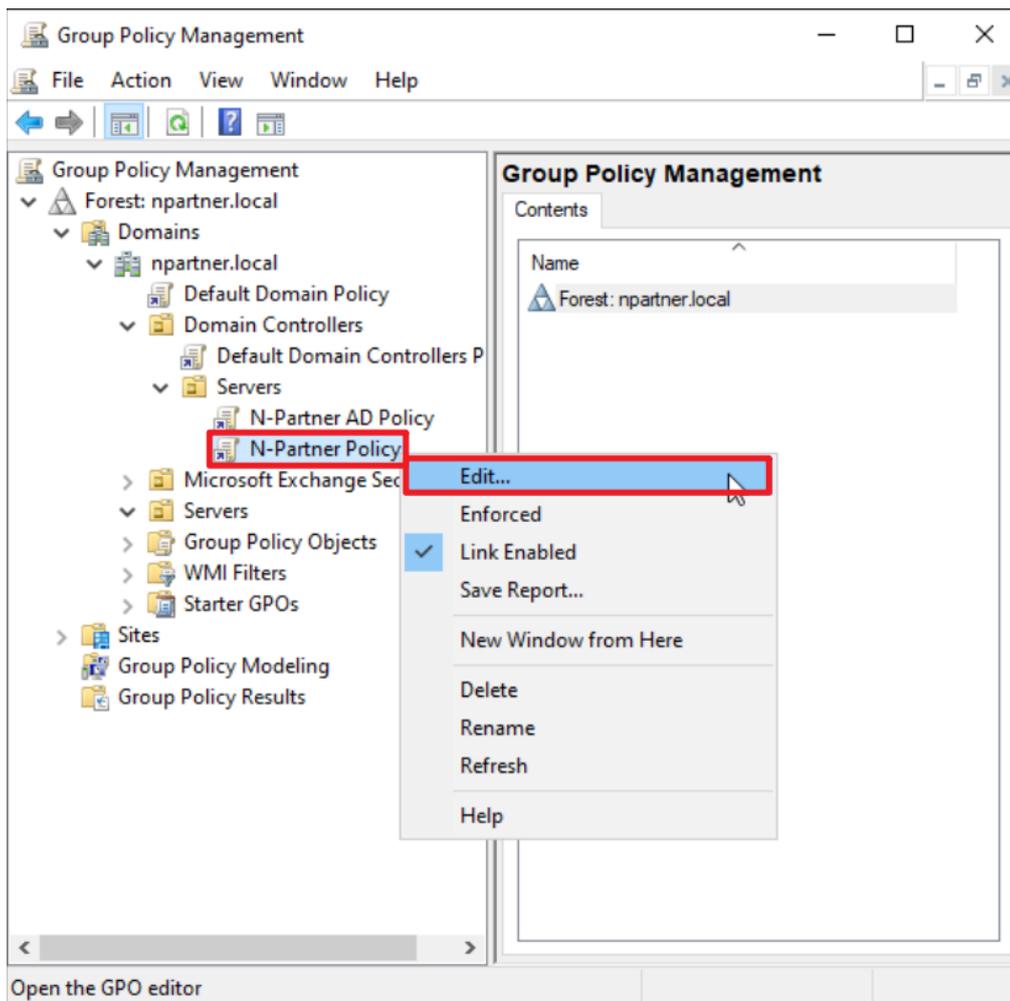
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



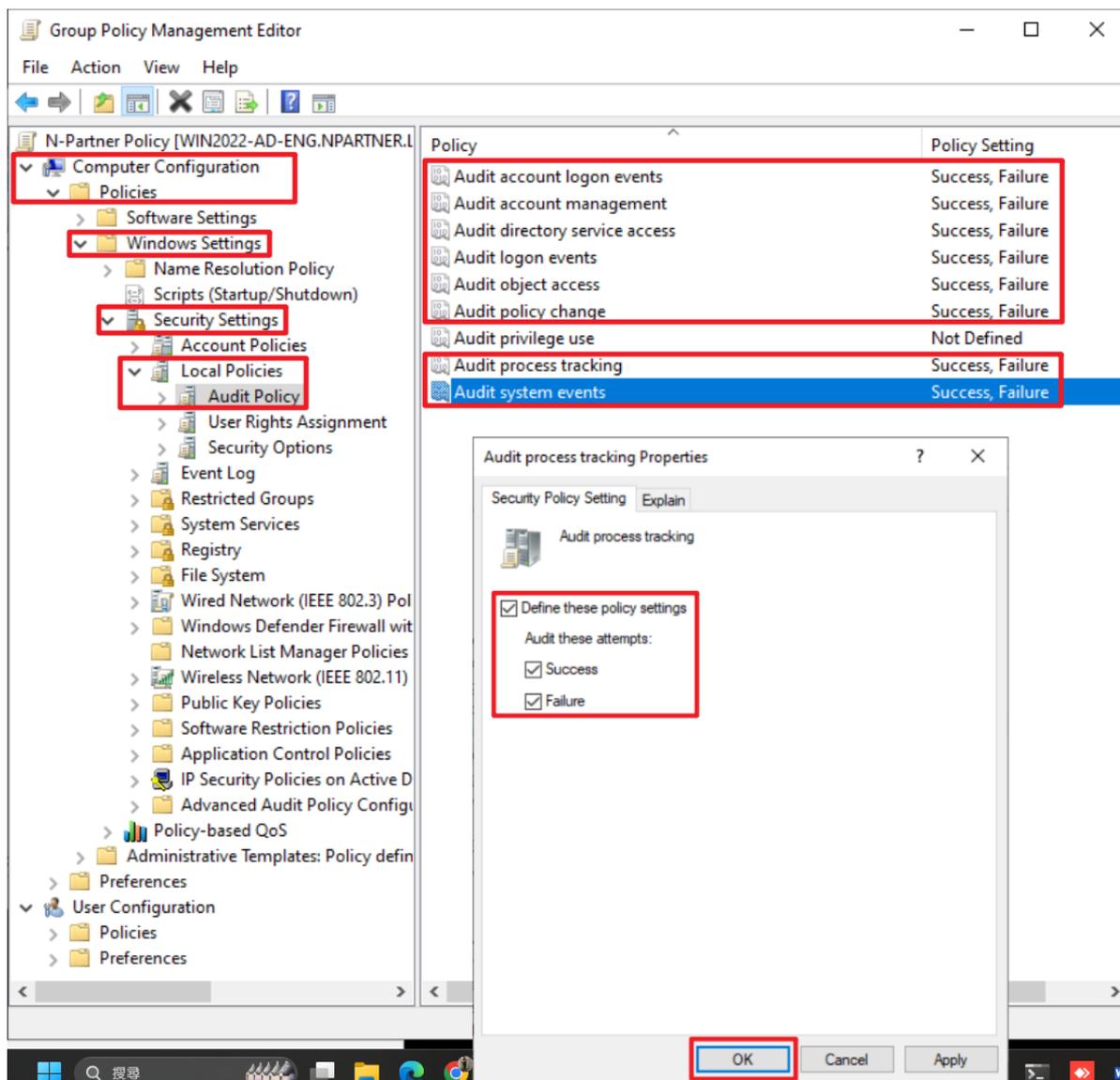
(4) Edit your Group Policy Object

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



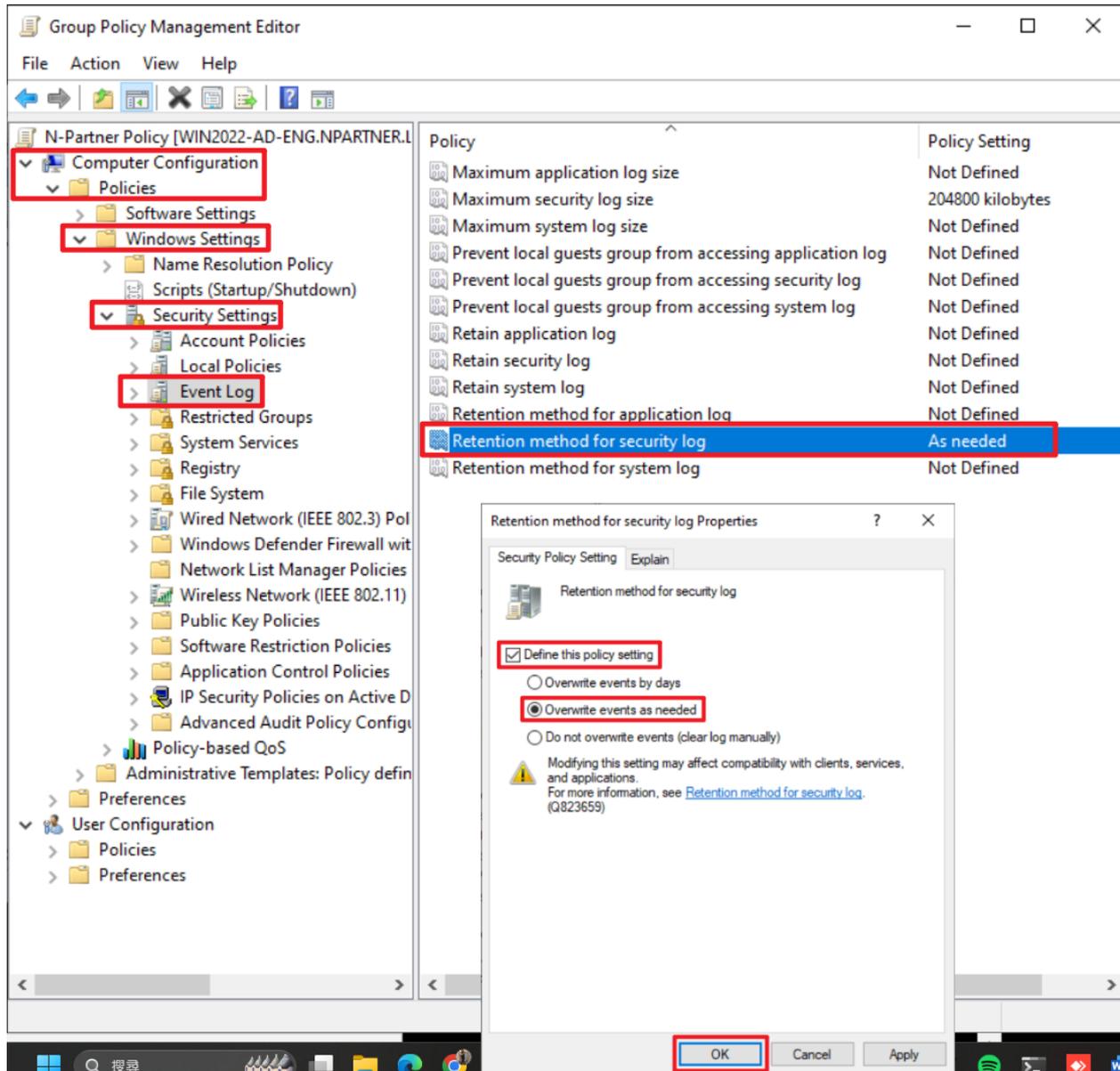
(5) Local Group Policies: Audit Policy

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

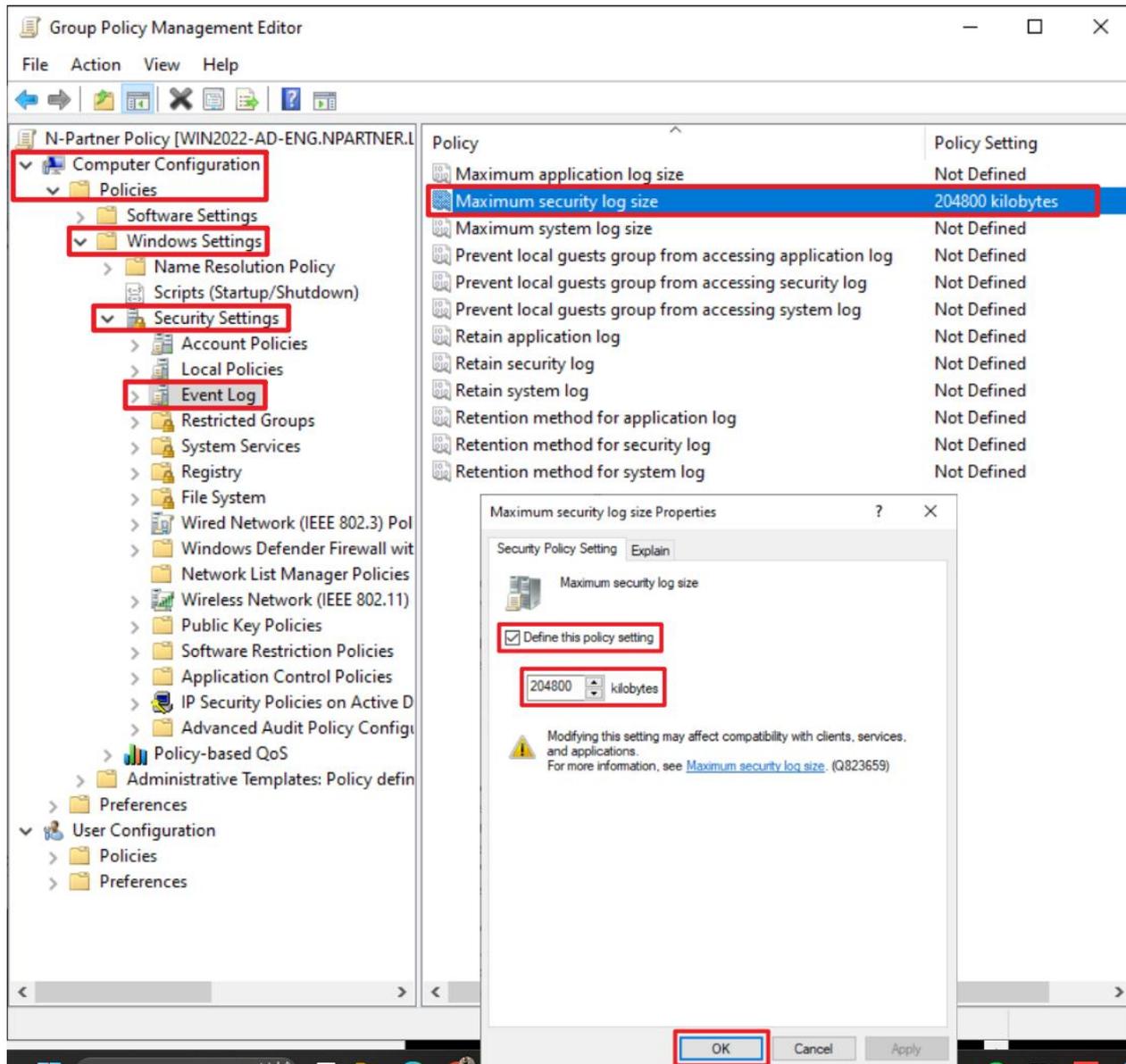
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

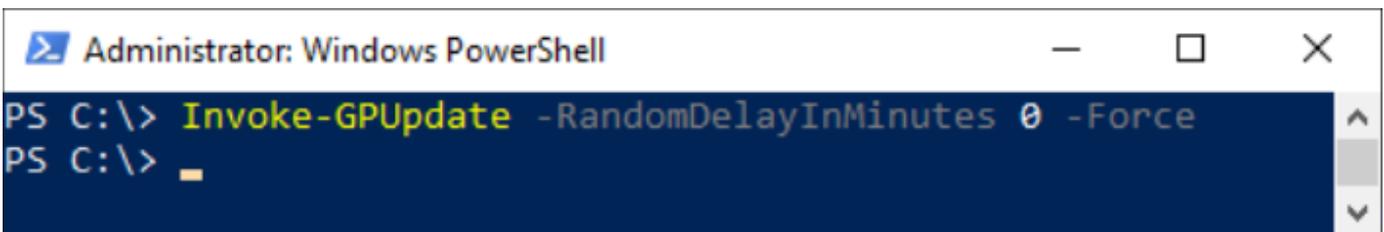


(8) Open “Windows PowerShell.”



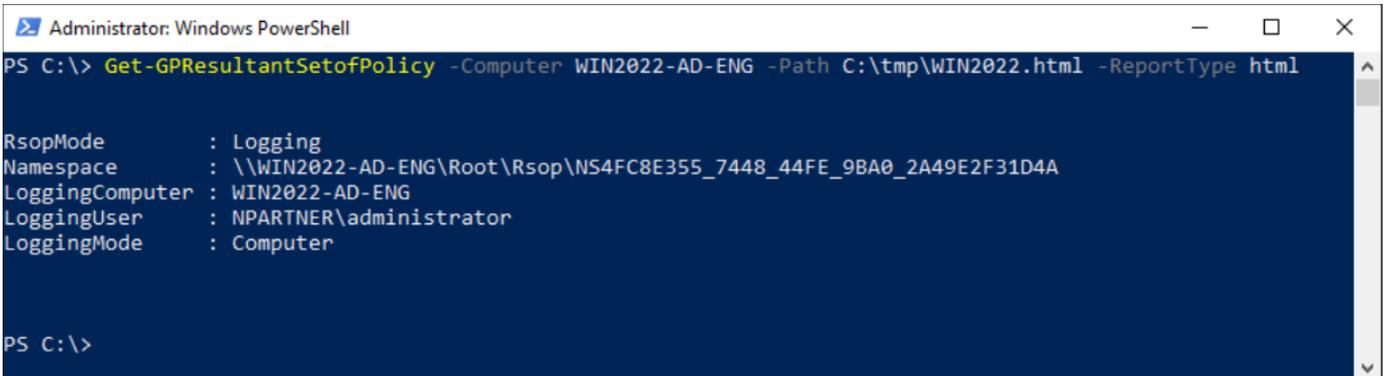
(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUUpdate -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.

The screenshot shows a web browser window with the address bar displaying "NPARTNER\WIN2022-AD-ENG" and the file path "C:/tmp/Win2022.html". The main content area displays a Group Policy report with the following sections:

- Component Status** (show)
- Settings** (hide)
- Policies** (hide)
 - Windows Settings** (hide)
 - Security Settings** (hide)
 - Account Policies/Password Policy** (show)
 - Account Policies/Account Lockout Policy** (show)
 - Account Policies/Kerberos Policy** (show)
 - Local Policies/Audit Policy** (hide)

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner AD Policy
Audit account management	Success, Failure	N-Partner AD Policy
Audit directory service access	Success, Failure	N-Partner AD Policy
Audit logon events	Success, Failure	N-Partner AD Policy
Audit object access	Success, Failure	N-Partner AD Policy
Audit policy change	Success, Failure	N-Partner AD Policy
Audit process tracking	Success, Failure	N-Partner AD Policy
Audit system events	Success, Failure	N-Partner AD Policy
 - Local Policies/User Rights Assignment** (show)
 - Local Policies/Security Options** (show)
 - Event Log** (hide)

Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner AD Policy
Retention method for security log	As needed	N-Partner AD 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
```

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

DisplayName           : npartner
Description           : Engineer
PhysicalDeliveryOfficeName : Taichung Office
Department           : TAC
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

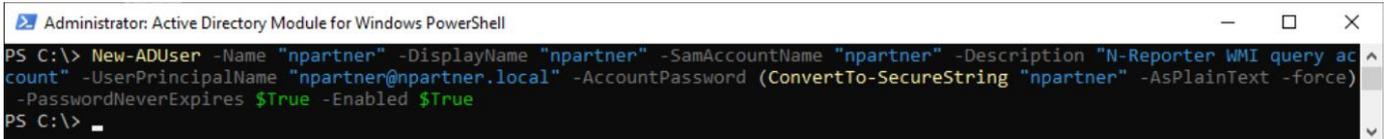
(1) Open "Active Directory Module for Windows PowerShell."



(2) Create an Account

Enter the command below to create an account:

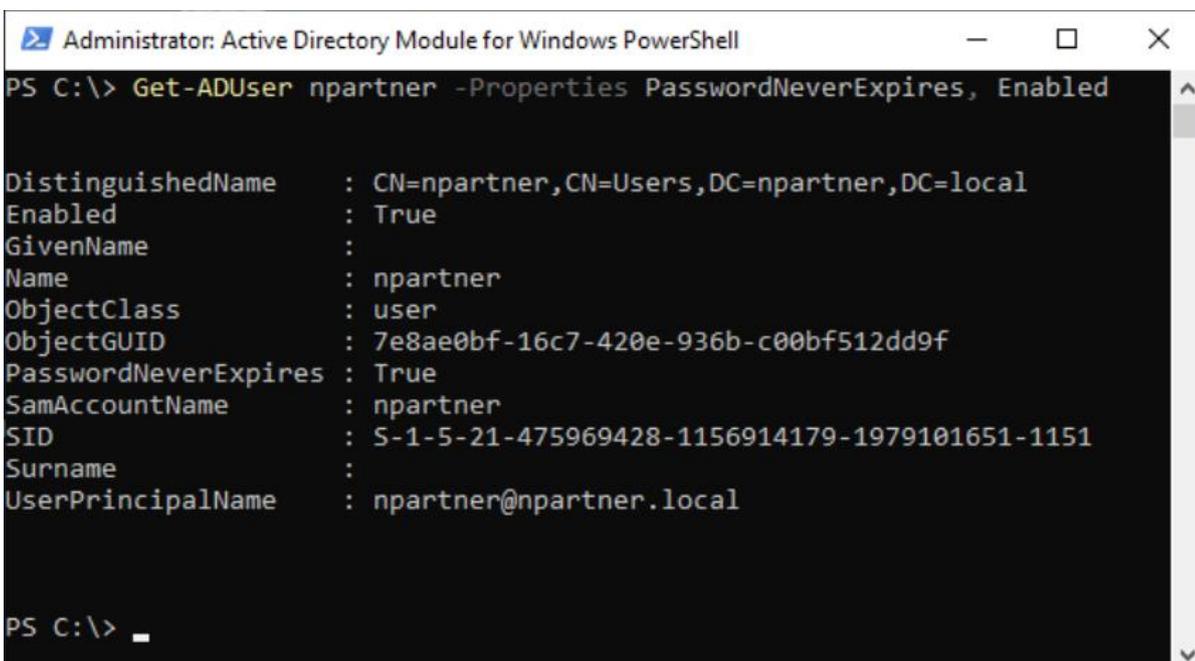
```
PS C:\> New-AdUser -Name "npartner" -DisplayName "npartner" -SamAccountName "npartner" `
>> -Description "N-Reporter WMI query account" -UserPrincipalName "npartner@npartner.local" `
>> -AccountPassword (ConvertTo-SecureString "npartner" -AsPlainText -force) `
>> -PasswordNeverExpires $True -Enabled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



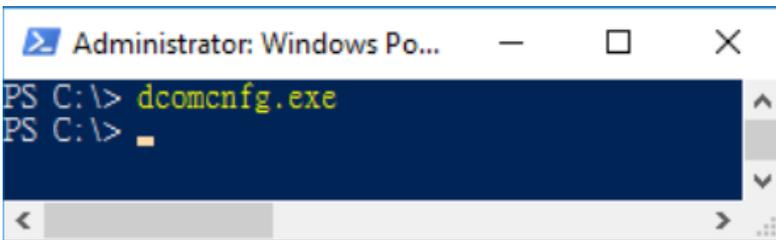
8.3.2 Configure DCOM Permissions

(1) Open “Windows Powershell.”



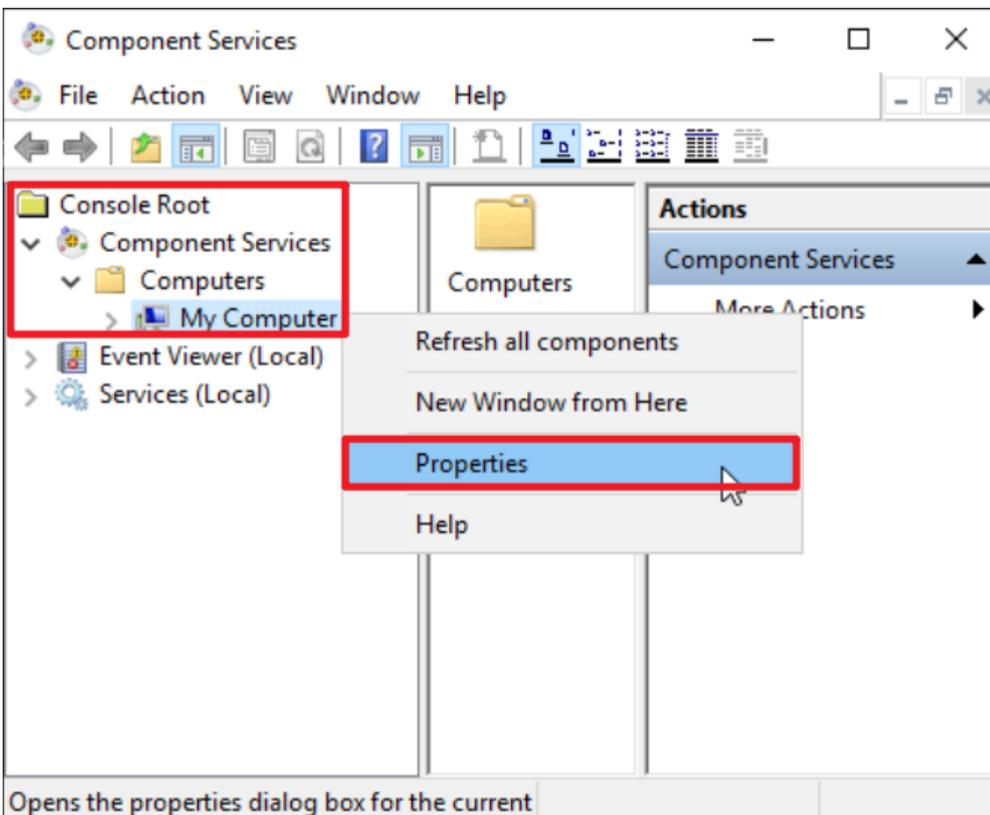
(2) Enter the command below to enable component services.

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



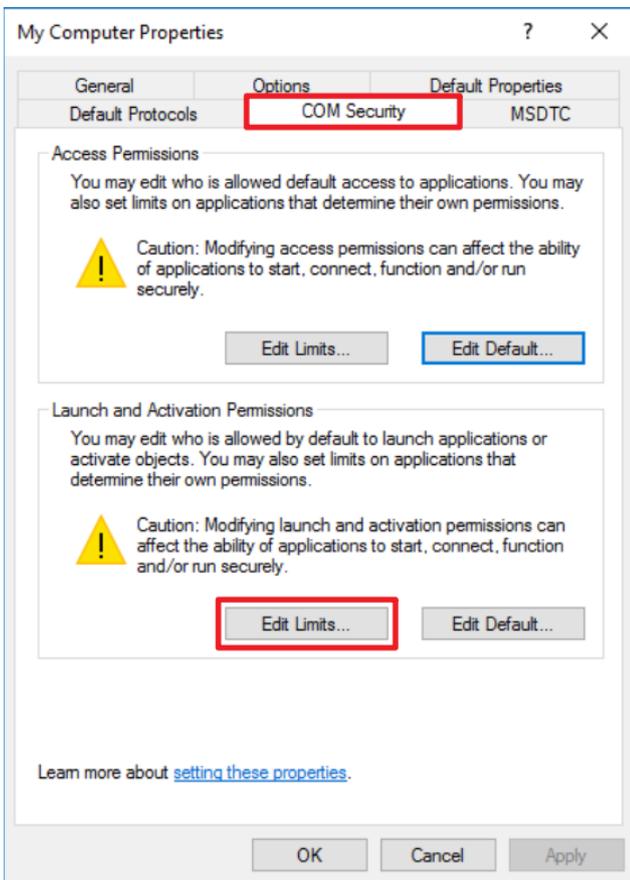
(3) Edit Computer Properties

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



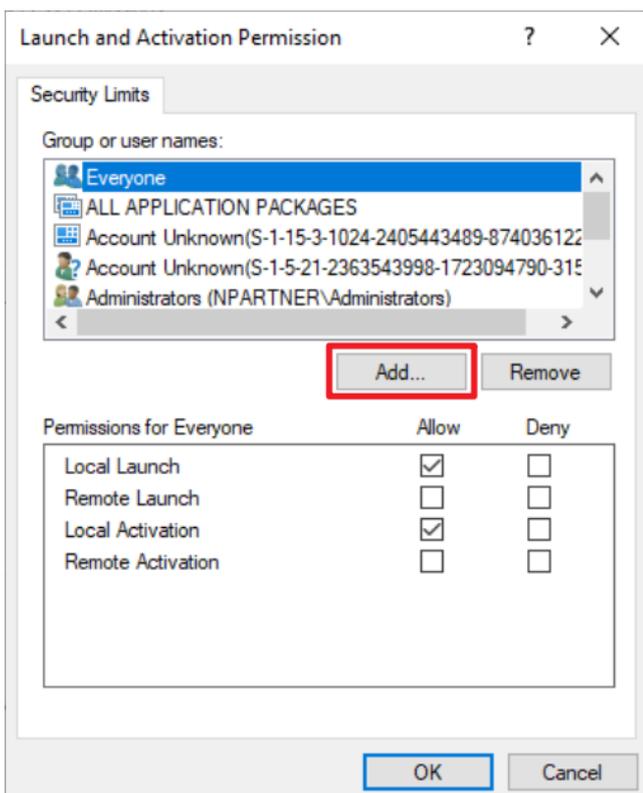
(4) Enable Permissions

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



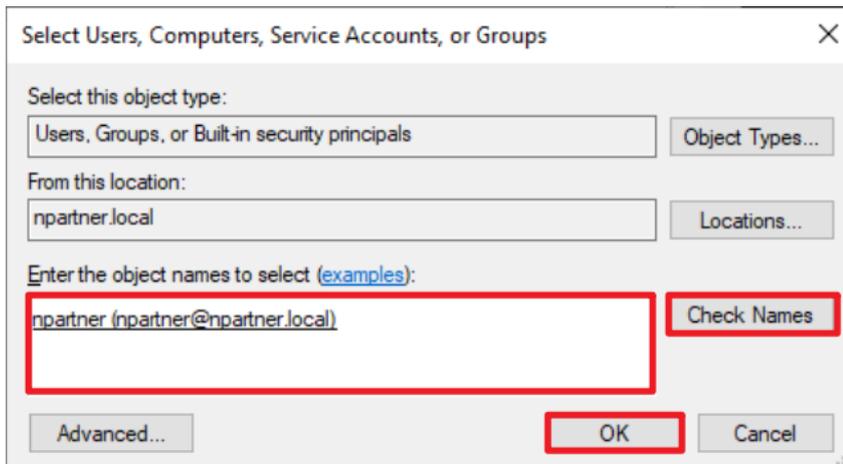
(5) Add DCOM User Permissions

Click “Add.”



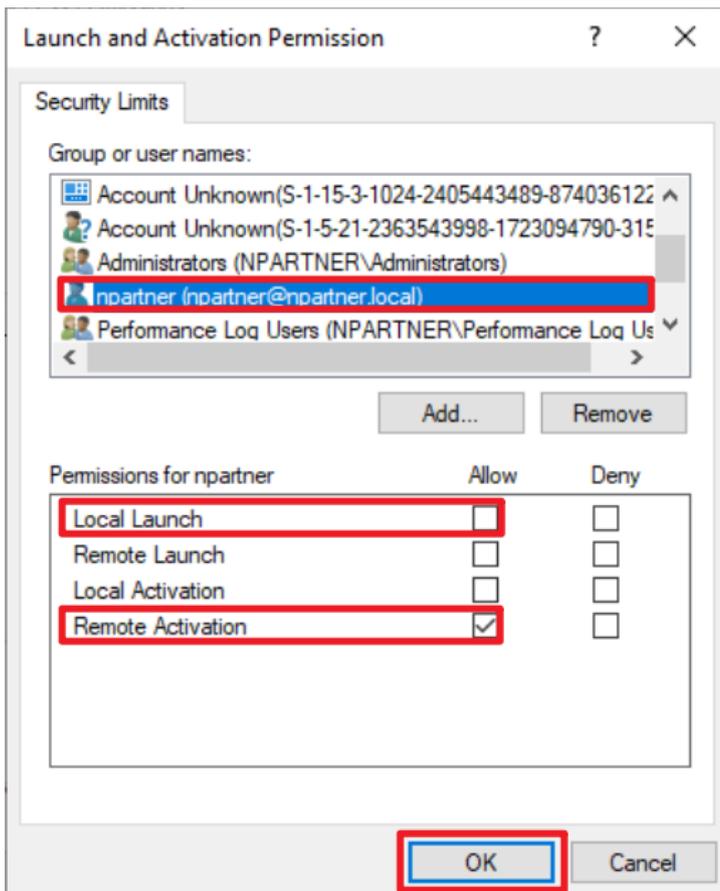
(6) Enter Your Username

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

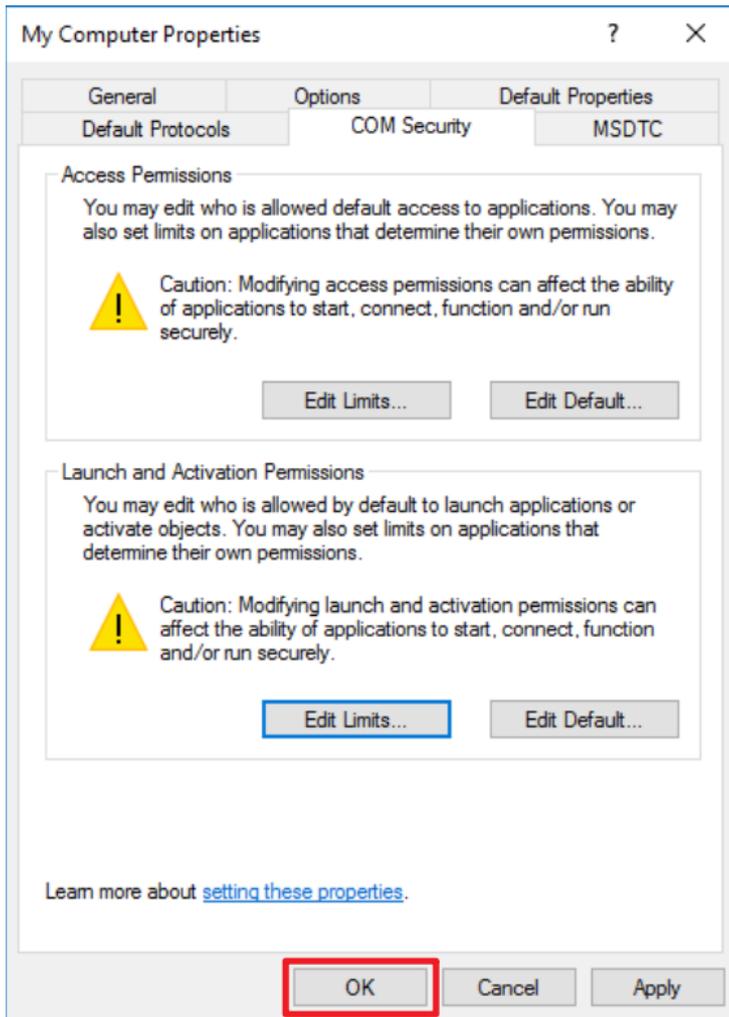


(7) Configure your User Permission

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

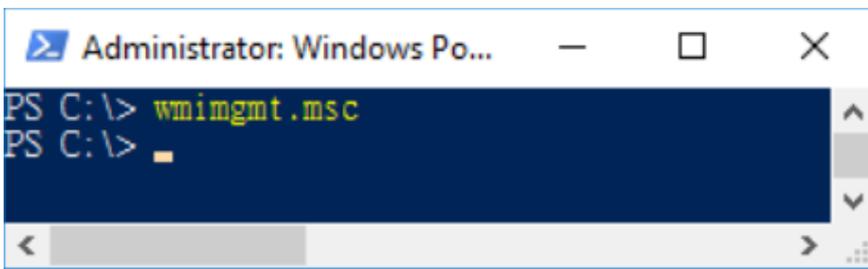
8.3.3.1 Configure Event Log Permissions

(1) Open "Windows Powershell."



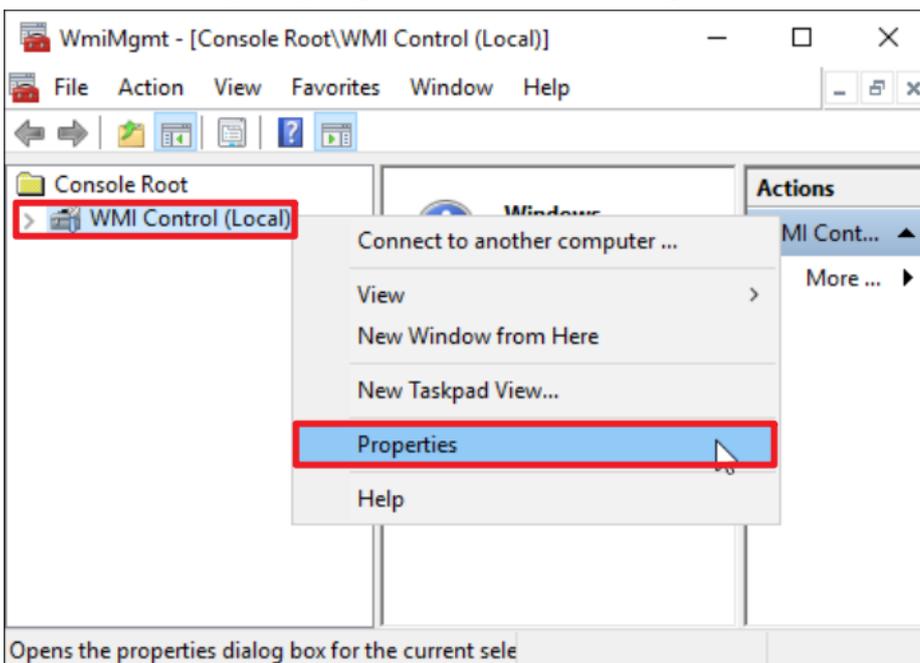
(2) Enter the command to enable WMI control service.

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



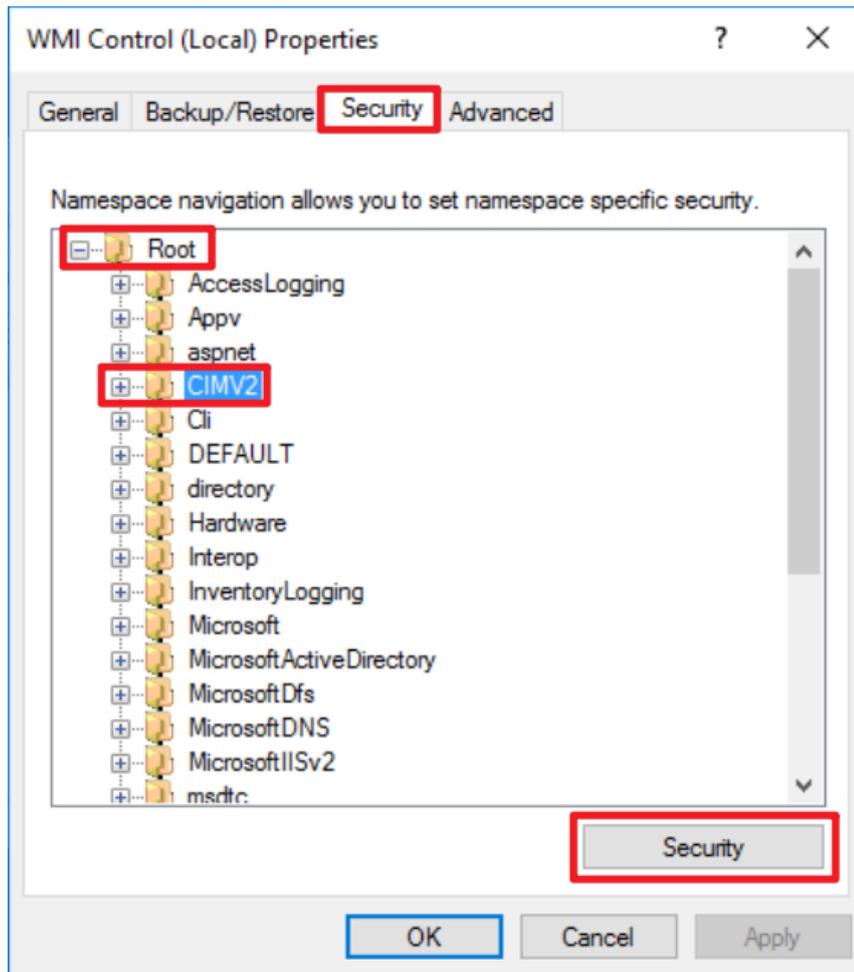
(3) Edit WMI Control

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



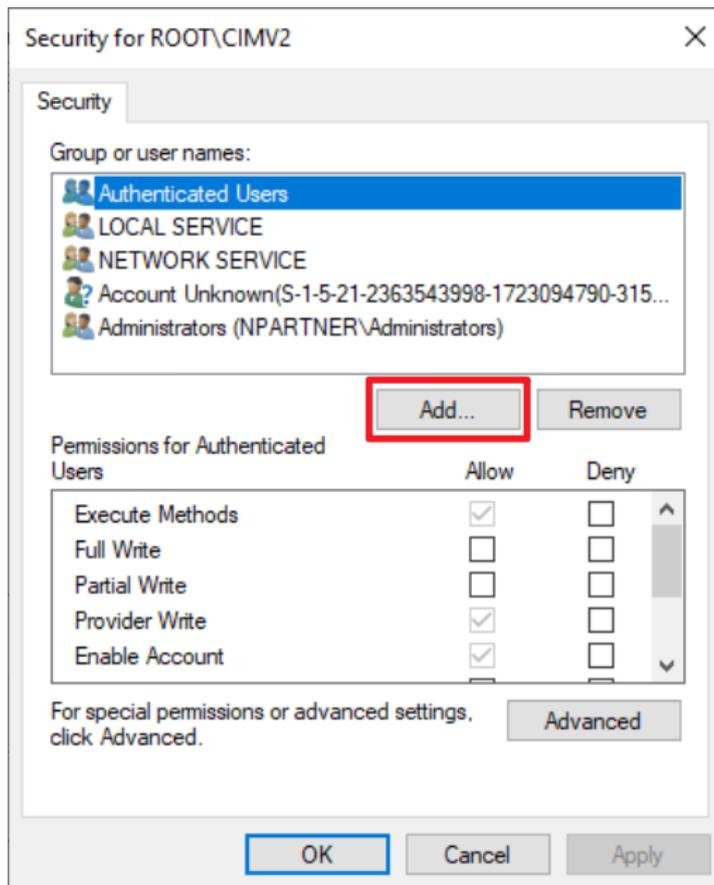
(4) Edit CIMV2 Security

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



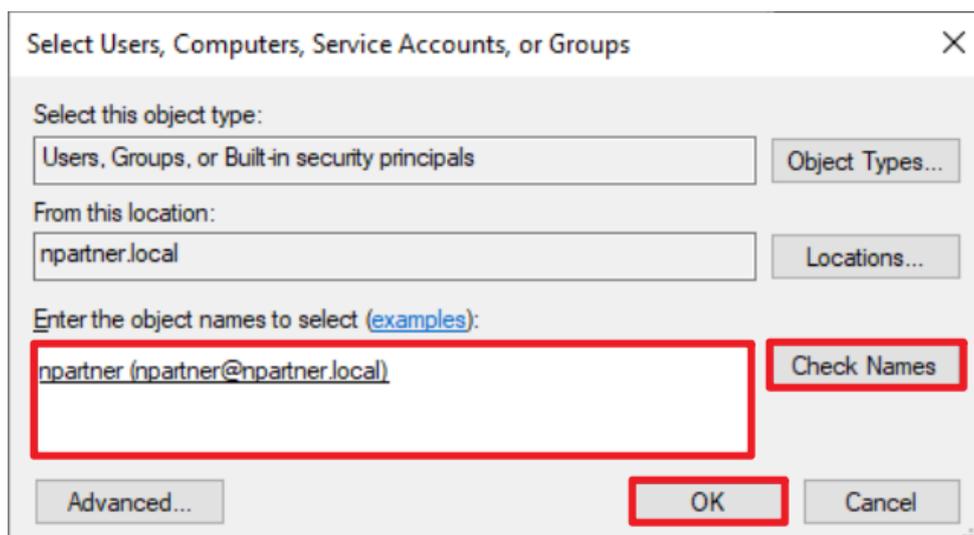
(5) Add WMI User Permissions.

Click “Add.”



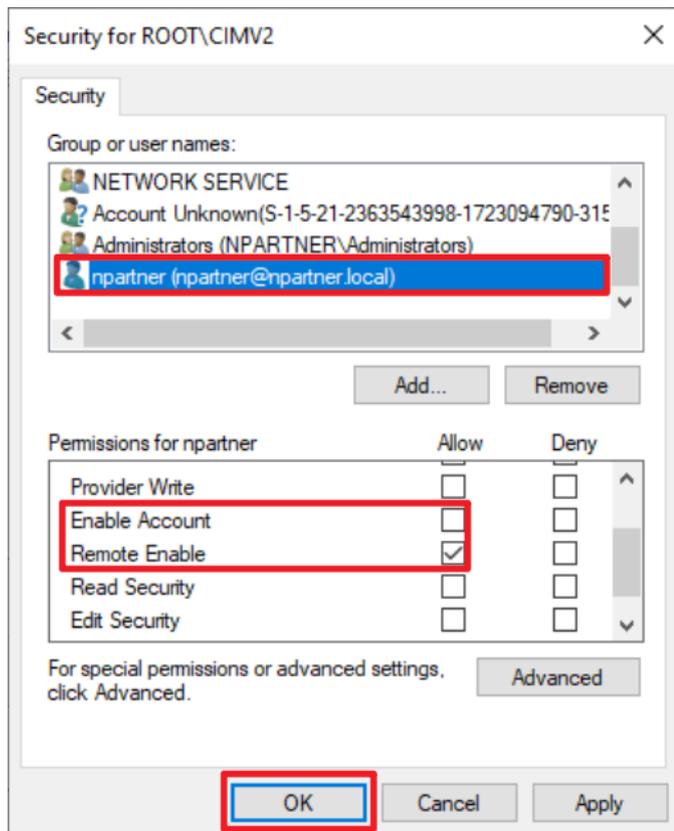
(6) Enter Your Username

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

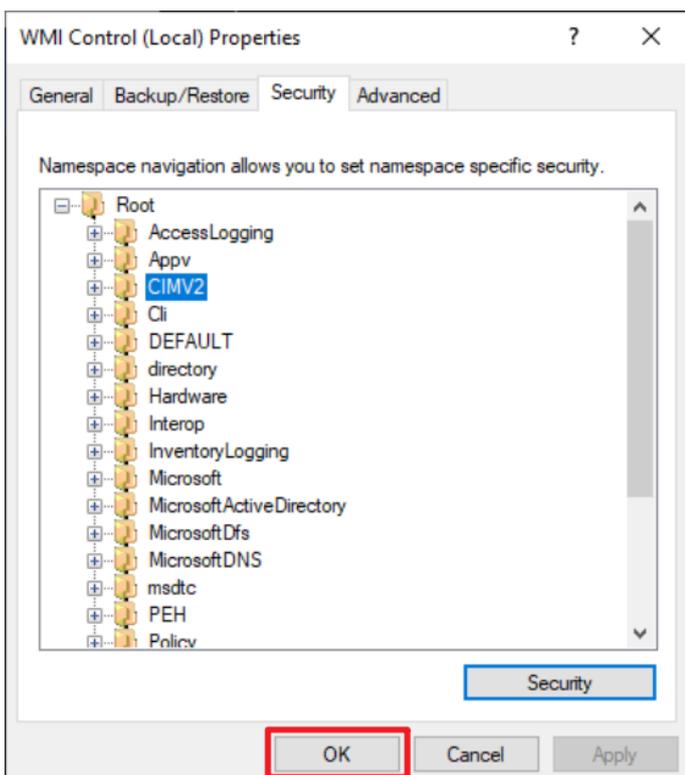


(7) Set Your User Permissions

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



(8) Click “OK.”



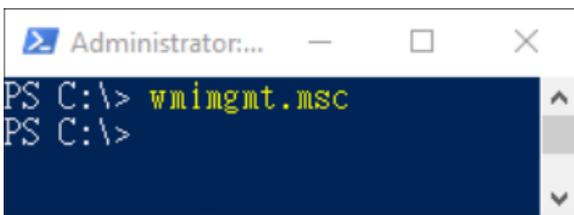
8.3.3.2 Configure Permissions for Reading User Data

(1) Open “Windows Powershell.”



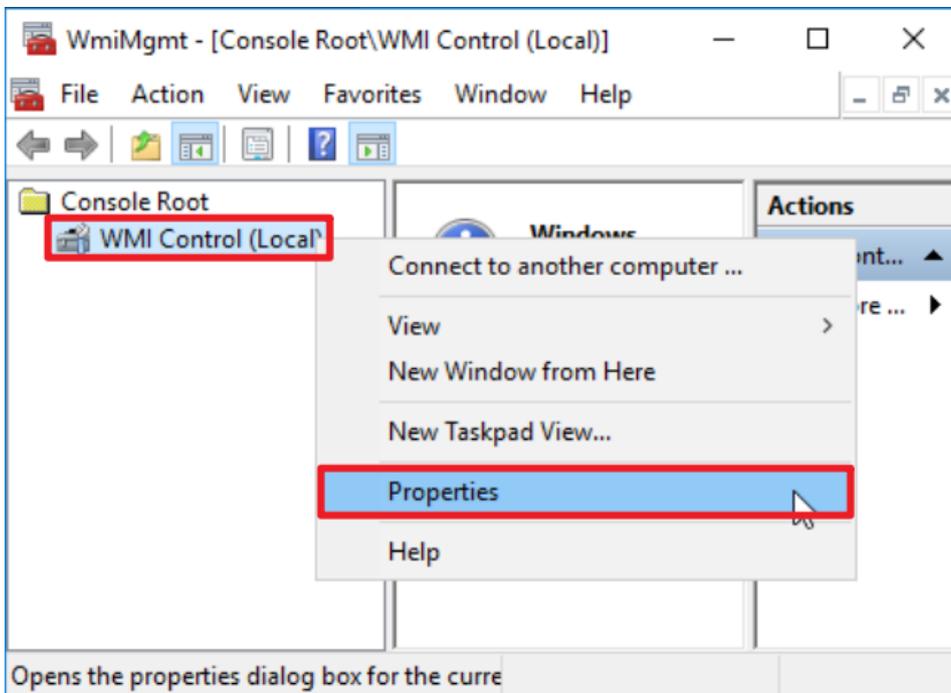
(2) Enter the command below to enable WMI Control.

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



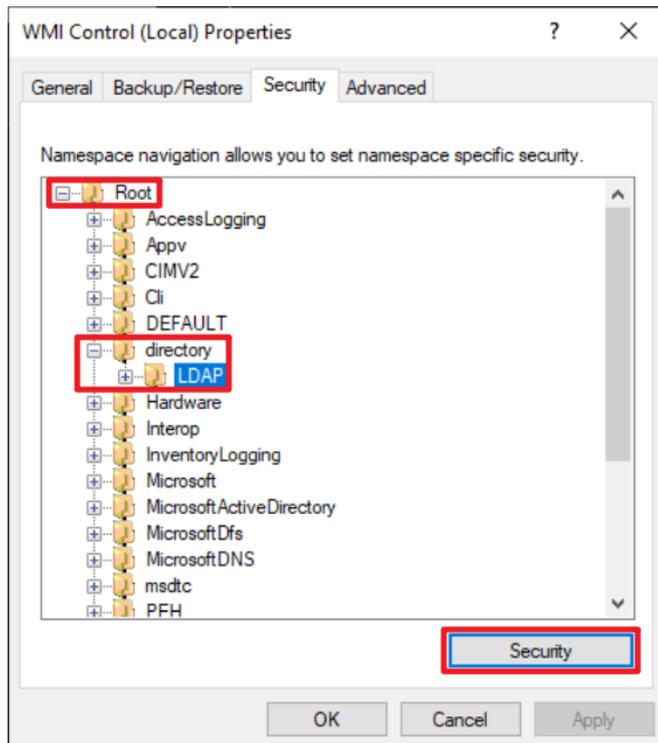
(3) Edit WMI Control

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



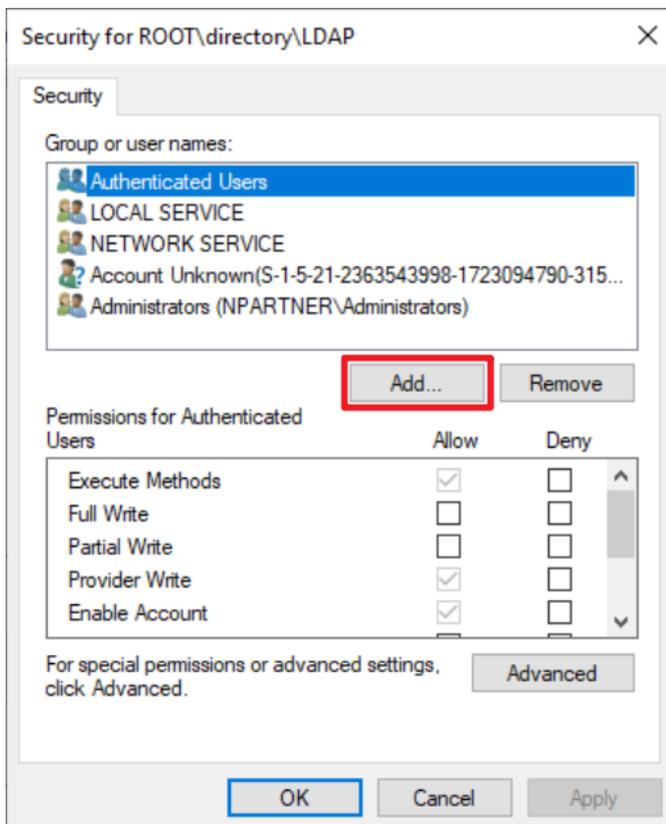
(4) Edit LDAP Security

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



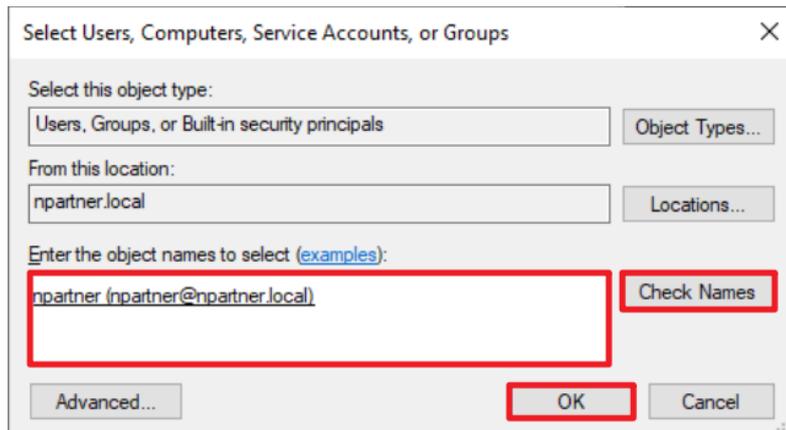
(5) Add WMI User Permissions

Click "Add."



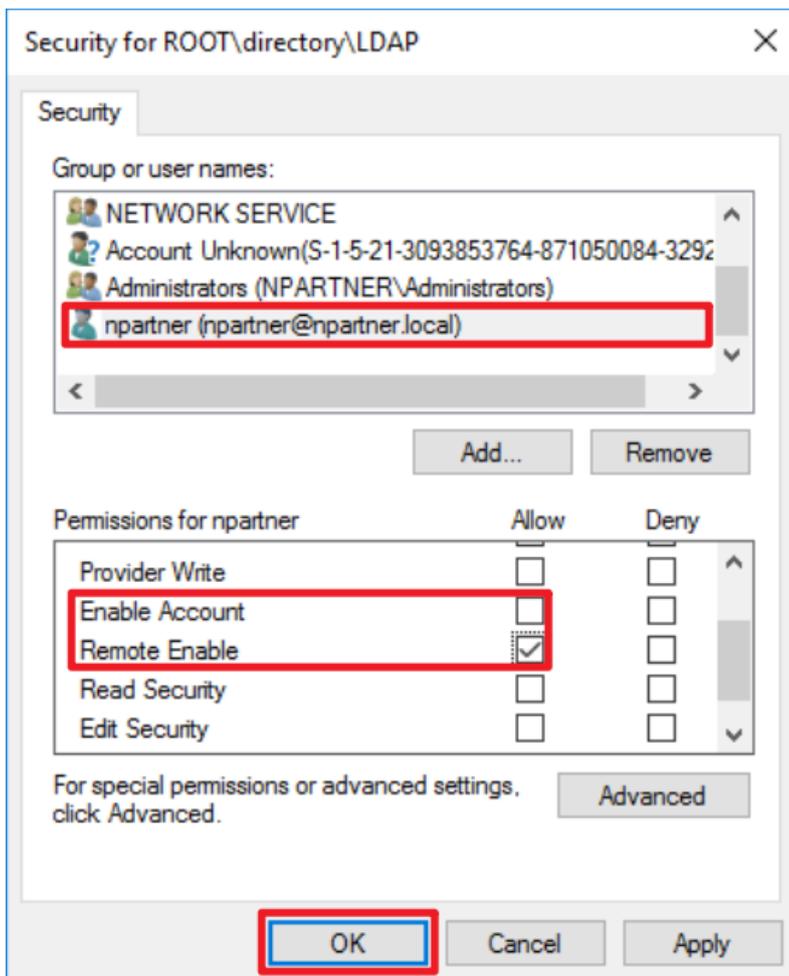
(6) Enter Your Username

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

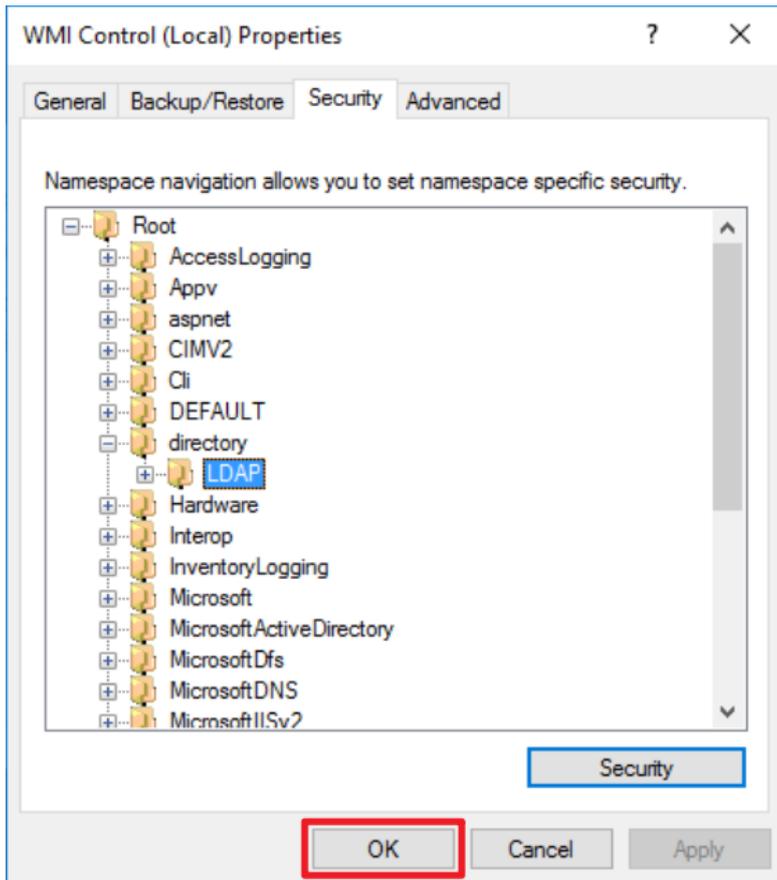


(7) Set Your User Permissions

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

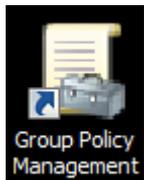


(8) Click "OK."

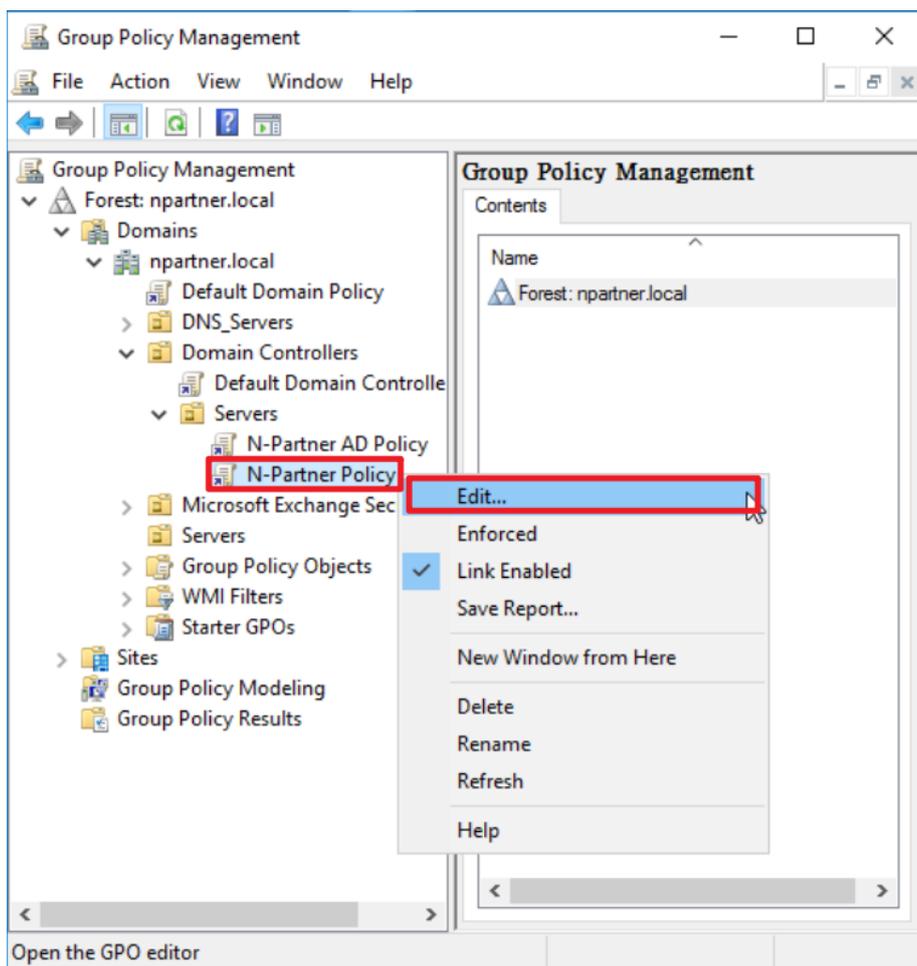


8.3.4 Configure Event Log Read Permissions

(1) Click “Group Policy Management.”

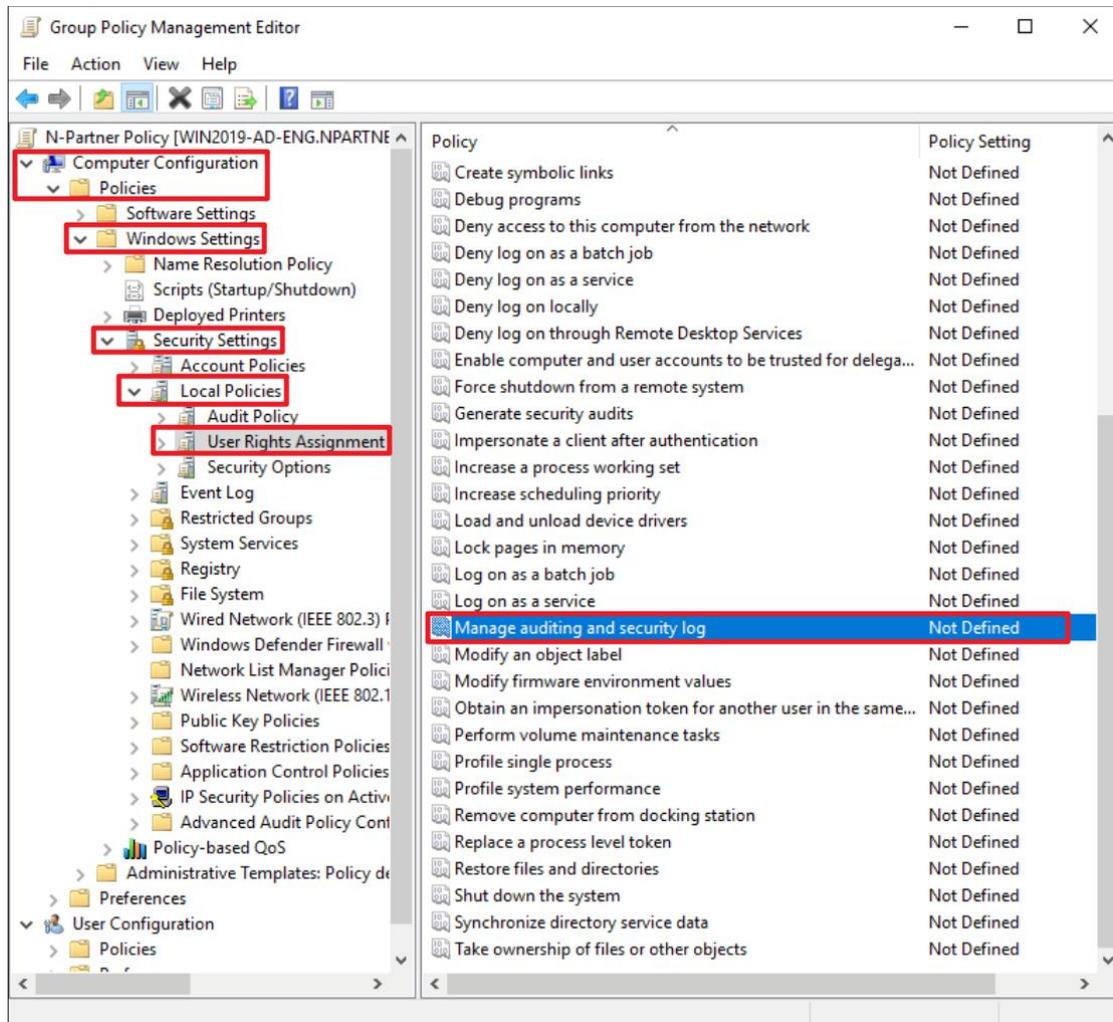


(2) Expand “Domain Controllers” → “Servers” → right-click “N-Partner Policy” and select “Edit.”



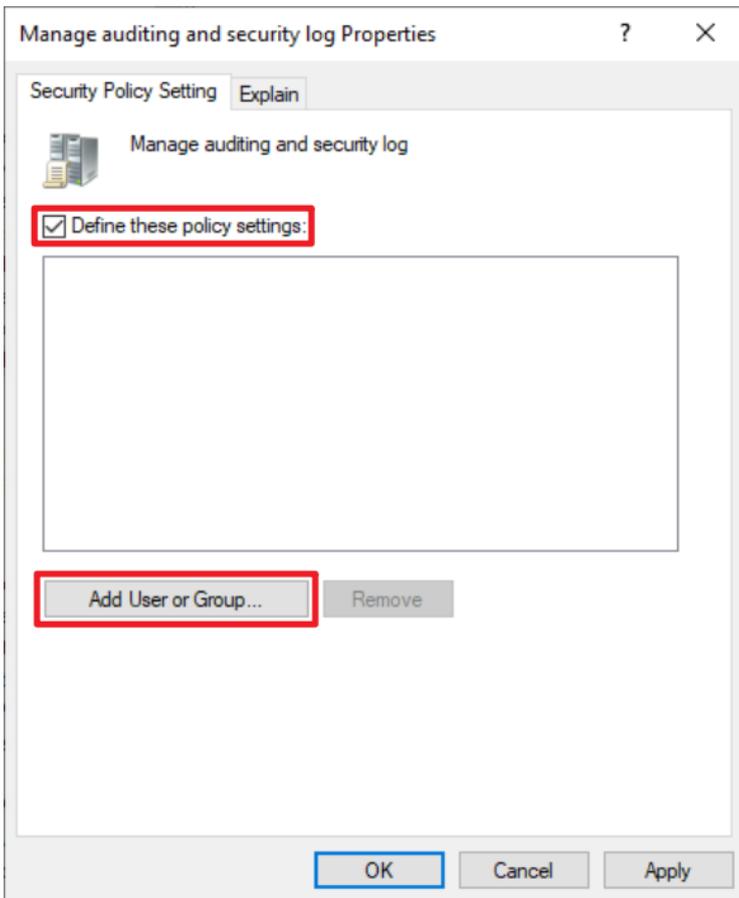
(3) Configure Auditing Log

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



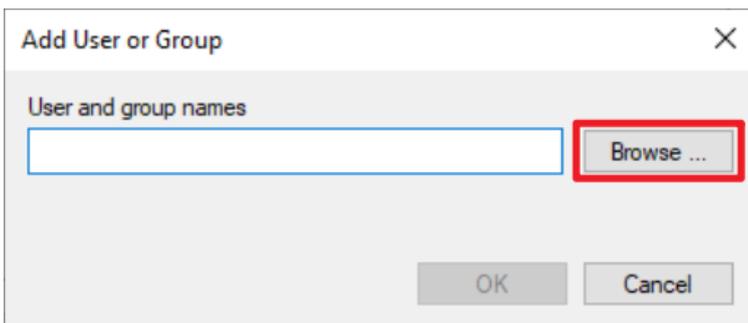
(4) Add Auditing User

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



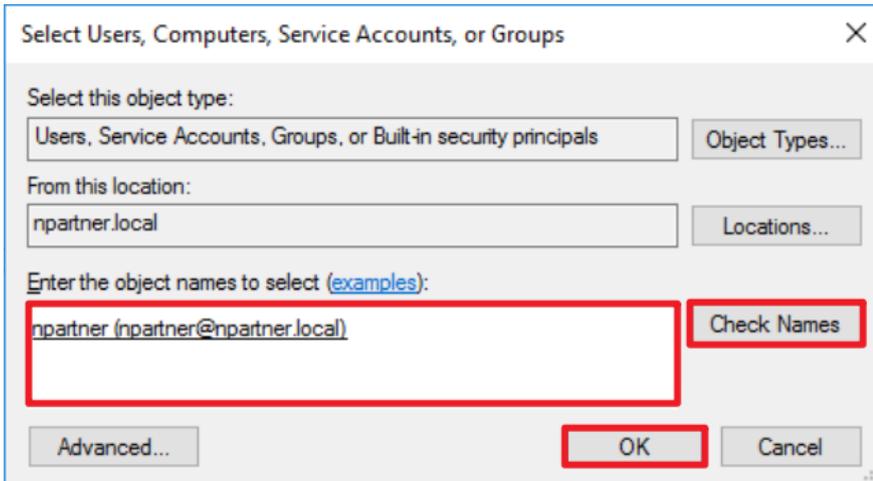
(5) Search for User

Click “Browse.”

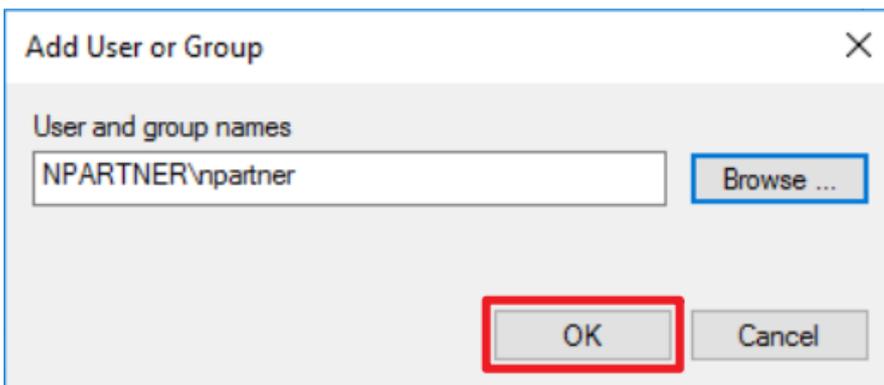


(6) Enter Your User Account

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

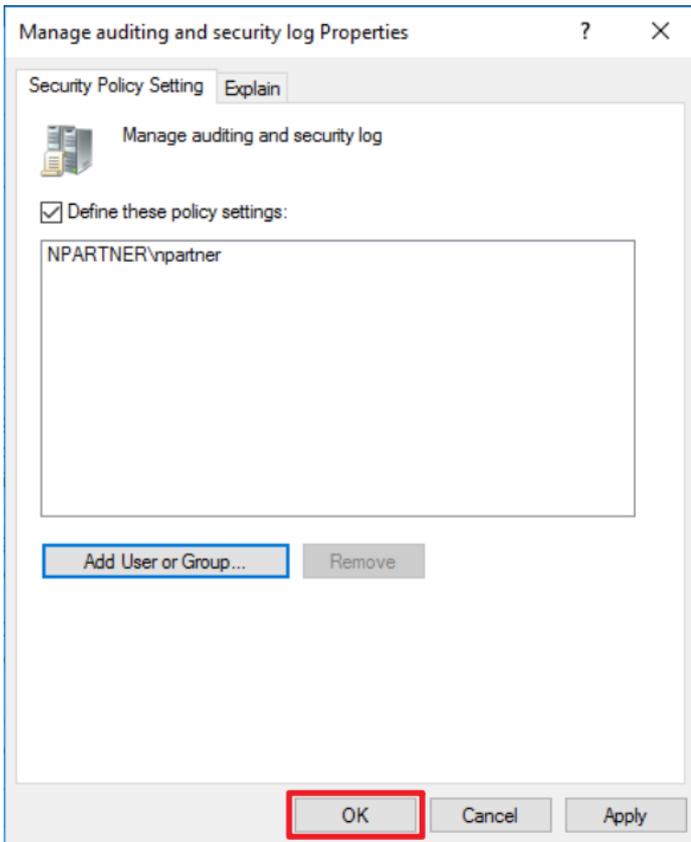


(7) Click “OK.”



(8) Confirm Audit Log Settings

Click "OK."

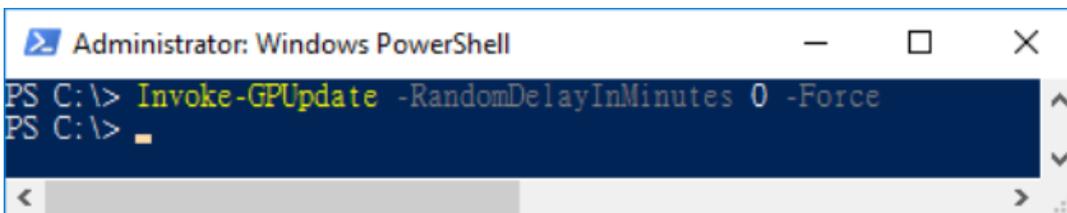


(9) Open "Windows Powershell."



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

```
PS C:\> Invoke-GPUdate -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
```

A screenshot of an Administrator Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The command entered is `Restart-Service -DisplayName "Windows Management Instrumentation" -Force`. The output shows two yellow warning messages: "WARNING: Waiting for service 'User Access Logging Service (UALSVC)' to start..." followed by a cursor on the next line.

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

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

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

A screenshot of an Administrator Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The command entered is `Get-Service -DisplayName "Windows Management Instrumentation"`. The output is a table showing the service status.

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

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

PS C:\> _
```

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
```

A screenshot of an Administrator Windows PowerShell window. The command entered is `Set-NetFirewallRule -DisplayGroup "Windows Management Instrumentation (WMI)" -RemoteAddress 192.168.8.59 -Enabled True`. The prompt is `PS C:\>`.

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
```

A screenshot of an Administrator Windows PowerShell window showing the output of the `Get-NetFirewallRule` command. The output is a table with columns: Name, DisplayName, DisplayGroup, RemoteAddress, and Enabled.

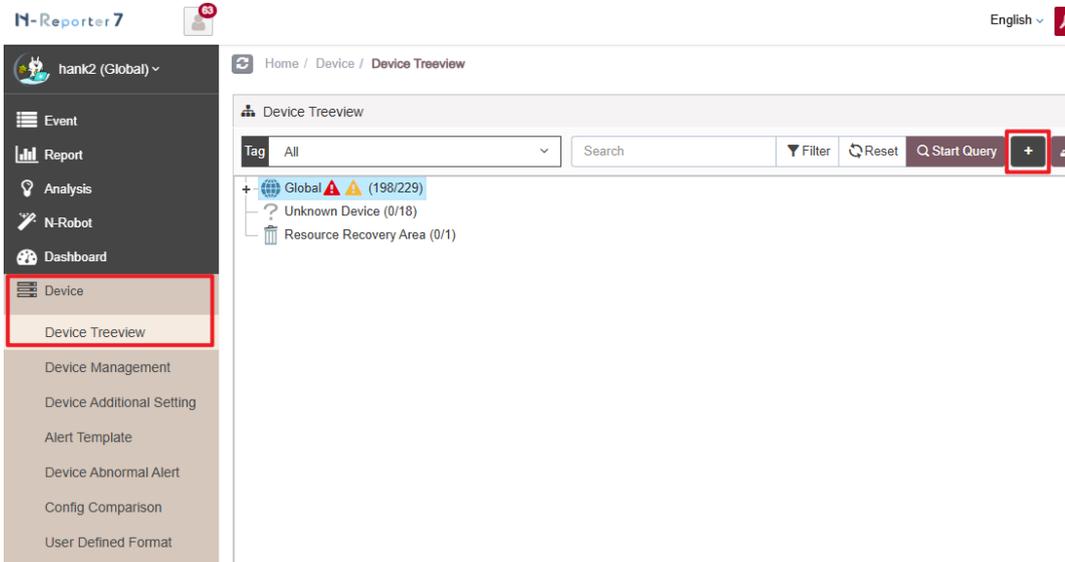
Name	DisplayName	DisplayGroup	RemoteAddress	Enabled
WMI-ASYNC-In-TCP	Windows Management Instrumentation (ASync-In)	Windows Management Instrumentation (WMI)	192.168.8.59	True
WMI-WINMGMT-In-TCP	Windows Management Instrumentation (WMI-In)	Windows Management Instrumentation (WMI)	192.168.8.59	True
WMI-RPCSS-In-TCP	Windows Management Instrumentation (DCOM-In)	Windows Management Instrumentation (WMI)	192.168.8.59	True

The prompt is `PS C:\>`.

9. N-Reporter

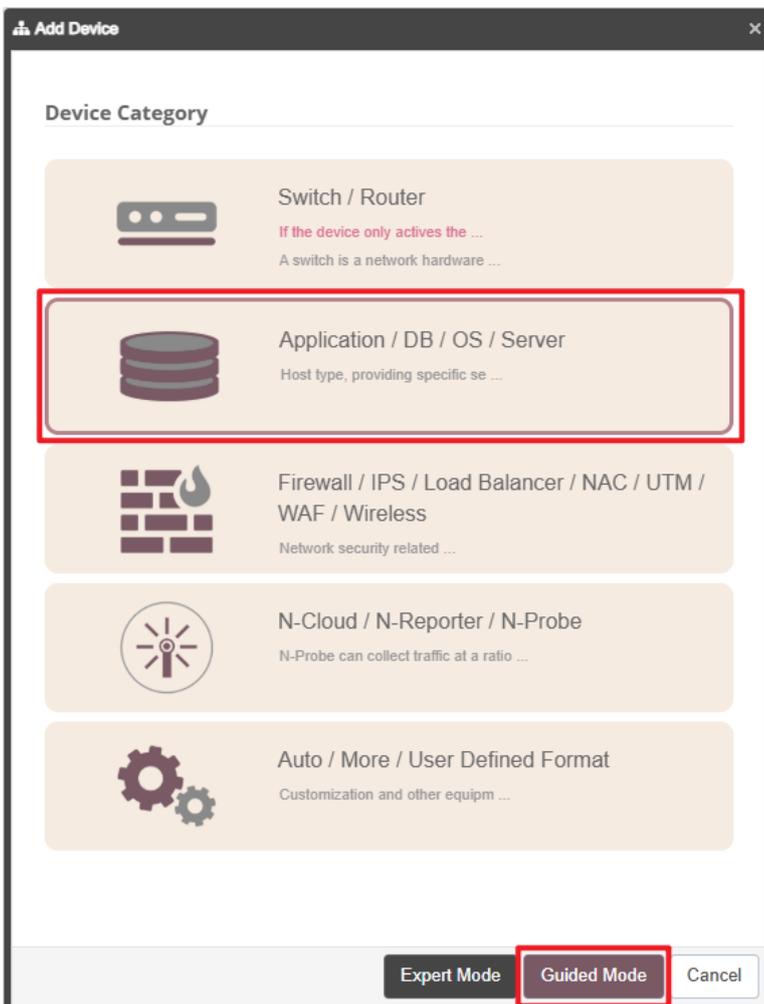
(1) Add a Windows AD device:

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



(2) Select the device type:

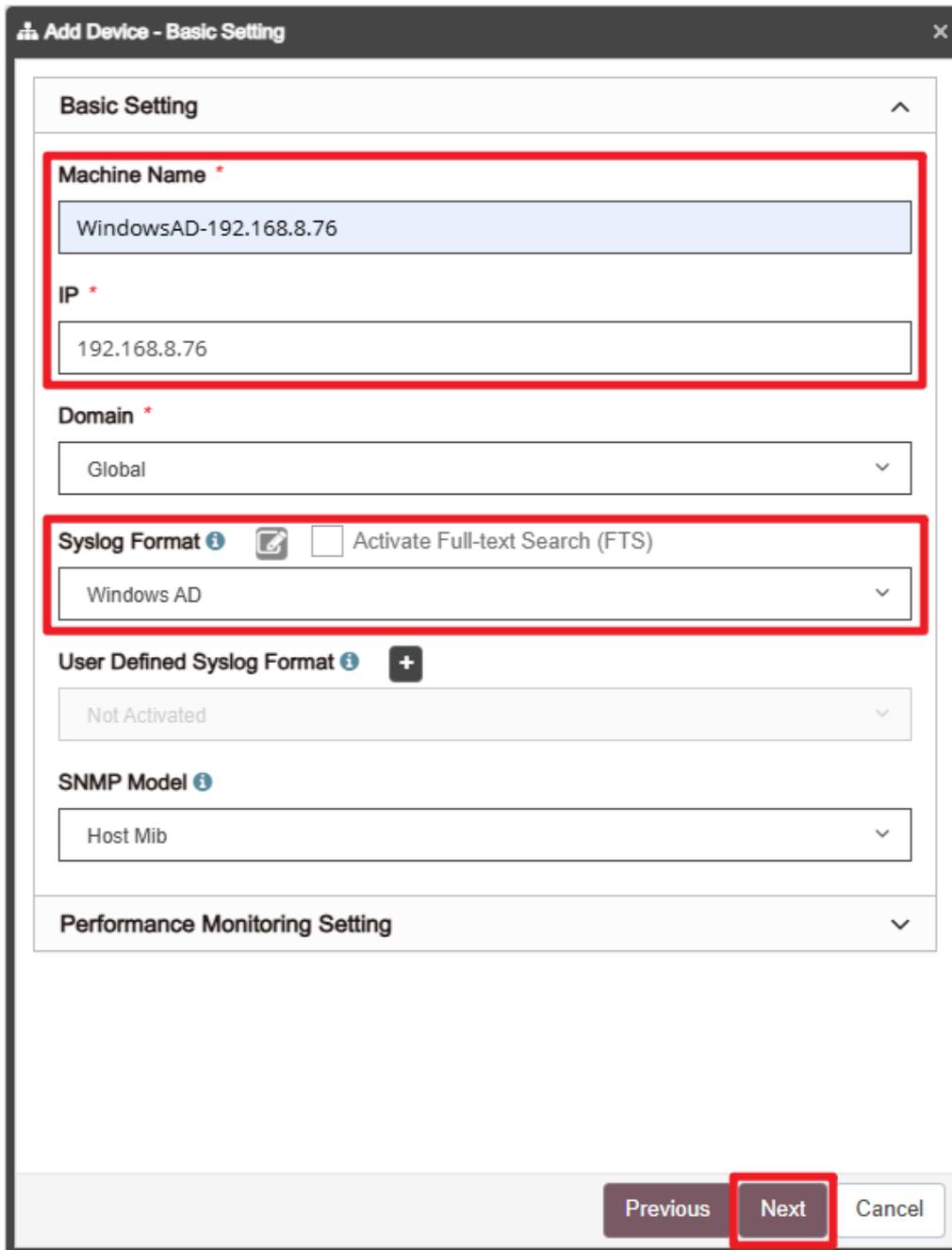
Choose “Application/DB/OS/Server” → click “Guided Mode.”



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.”



Add Device - Basic Setting

Basic Setting

Machine Name *
WindowsAD-192.168.8.76

IP *
192.168.8.76

Domain *
Global

Syslog Format ⓘ Activate Full-text Search (FTS)
Windows AD

User Defined Syslog Format ⓘ +
Not Activated

SNMP Model ⓘ
Host Mib

Performance Monitoring Setting

Previous **Next** Cancel

(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.

The screenshot shows the 'Add Device - Syslog Setting' dialog box. The 'Syslog Setting' section is expanded. The 'Facility' dropdown menu is set to '(17) local use 1 (local1)'. The 'Encoding' dropdown menu is set to 'BIG5'. Below these, there are two text input fields for 'Syslog Normalized Data Retention Days (Max)' and 'Syslog Normalized Data Retention Days (At Least)', both containing the value '7-18250'. Under the 'Raw Data Kept and Replied' section, the 'Raw Data Kept' checkbox is checked. Below it are two unchecked checkboxes: 'Raw data format is adopted while Syslog relaying is activated in Threshold Report.' and 'The source IP will be kept in normalized data relaying'. At the bottom of the dialog, there are three buttons: 'Previous', 'Next', and 'Cancel'. The 'Next' button is highlighted with a red box.

(3) Others

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

The screenshot shows a web form titled "Add Device - Other". The form contains several input fields and a status selection section. The "Device Icon" dropdown menu is set to "Host" and is highlighted with a red box. Below it is a "Latitude and Longitude" text field containing "atitude, longitude". The "Remark" field contains the text "Special format: [key]="value", which can be exported into a custom field.". The "Tag" field is empty. The "Receive Status" section has two radio buttons: "Activated" (which is selected) and "Disabled". This section is also highlighted with a red box. At the bottom of the form, there are three buttons: "Previous", "Next" (highlighted with a red box), and "Cancel".

(4) WMI Configuration

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

Add Device - Action & Backup

Action Device / VRF / Connection Related Setting

Action Device

Activate Action Device

Action URL

VRF (Virtual Routing and Forwarding)

Device Connection Method

SSH Telnet WMI

Login Account

administrator

Login Password

.....

Users Information From AD Equipment

Capture Users Information

API IP & Login Related Setting

Previous **Next** Cancel

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.”

The screenshot shows a dialog box titled "Add Device - Basic Setting". It contains several input fields and a dropdown menu. The "Machine Name" field is highlighted with a red box and contains the text "WindowsAD-192.168.8.76". The "IP" field is also highlighted with a red box and contains "192.168.8.76". The "Syslog Format" dropdown menu is highlighted with a red box and is set to "Windows AD". There is a checkbox for "Activate Full-text Search (FTS)" which is unchecked. Below the Syslog Format field is a section for "User Defined Syslog Format" which is currently set to "Not Activated". There is also a section for "SNMP Model" set to "Host Mib". At the bottom of the dialog, there are three buttons: "Previous", "Next", and "Cancel". The "Next" button is highlighted with a red box.

(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.

The screenshot shows a dialog box titled "Add Device - Syslog Setting". It contains several configuration fields:

- Syslog Setting** (header)
- Facility**: A dropdown menu with the selected value "(17) local use 1 (local1)".
- Encoding**: A dropdown menu with the selected value "UTF-8".
- Syslog Normalized Data Retention Days (Max)**: A text input field containing "7-18250".
- Syslog Normalized Data Retention Days (At Least)**: A text input field containing "1-18250".
- Raw Data Kept and Replied**: A section with three checkboxes:
 - Raw Data Kept
 - Raw data format is adopted while Syslog relaying is activated in Threshold Report.
 - The source IP will be kept in normalized data relaying

At the bottom of the dialog, there are three buttons: "Previous", "Next", and "Cancel". The "Next" button is highlighted with a red box.

(3) Others

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

The screenshot shows a web form titled "Add Device - Other". The form contains several fields: "Device Icon" (a dropdown menu with "Host" selected), "Latitude and Longitude" (a text input field with "atitude, longitude" entered), "Remark" (a text input field with "Special format: [key]='value', which can be exported into a custom field." entered), and "Tag" (an empty text input field). Below these fields is the "Receive Status" section, which has two radio buttons: "Activated" (which is selected) and "Disabled". At the bottom of the form, there are three buttons: "Previous", "Next", and "Cancel". The "Next" button is highlighted with a red box, as is the "Device Icon" dropdown and the "Receive Status" section.

(4) WMI Configuration

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

Add Device - Action & Backup

Action Device / VRF / Connection Related Setting

Action Device

Activate Action Device

Action URL

VRF (Virtual Routing and Forwarding)

Device Connection Method

SSH Telnet WMI

Login Account

administrator

Login Password

.....

Users Information From AD Equipment

Capture Users Information

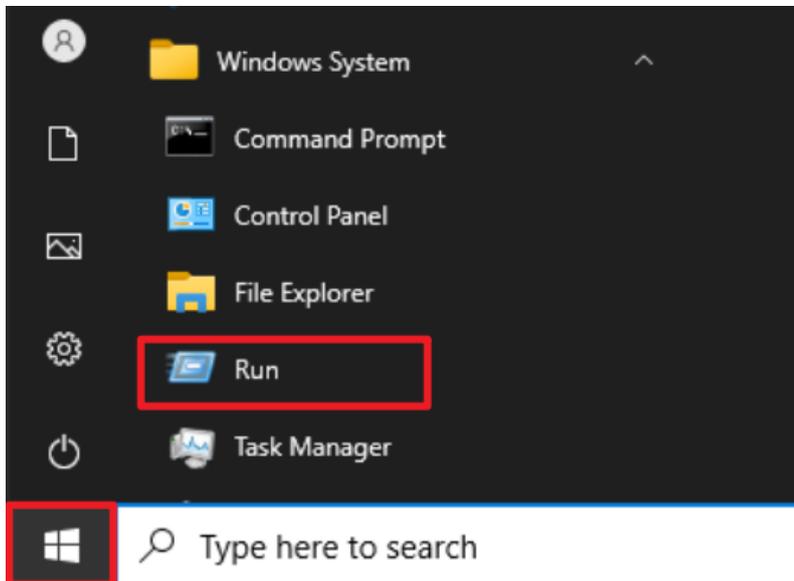
API IP & Login Related Setting

Previous **Next** Cancel

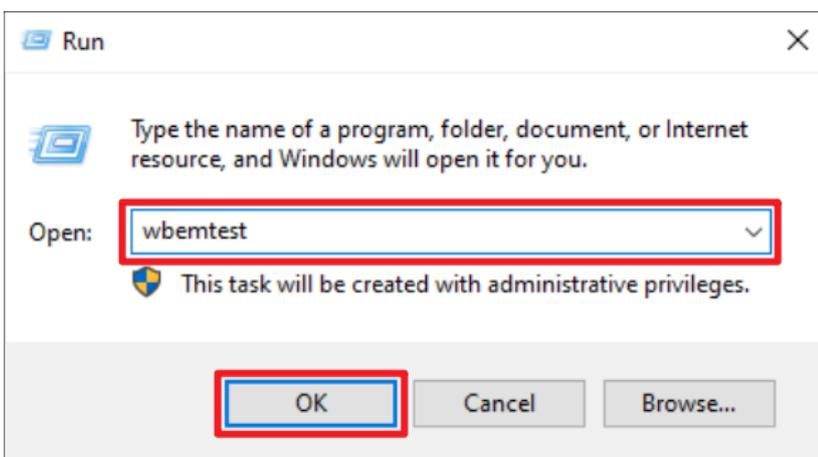
10. Troubleshooting

10.1 WMI Query Language Check

(1) Click “Start” → select “Run.”

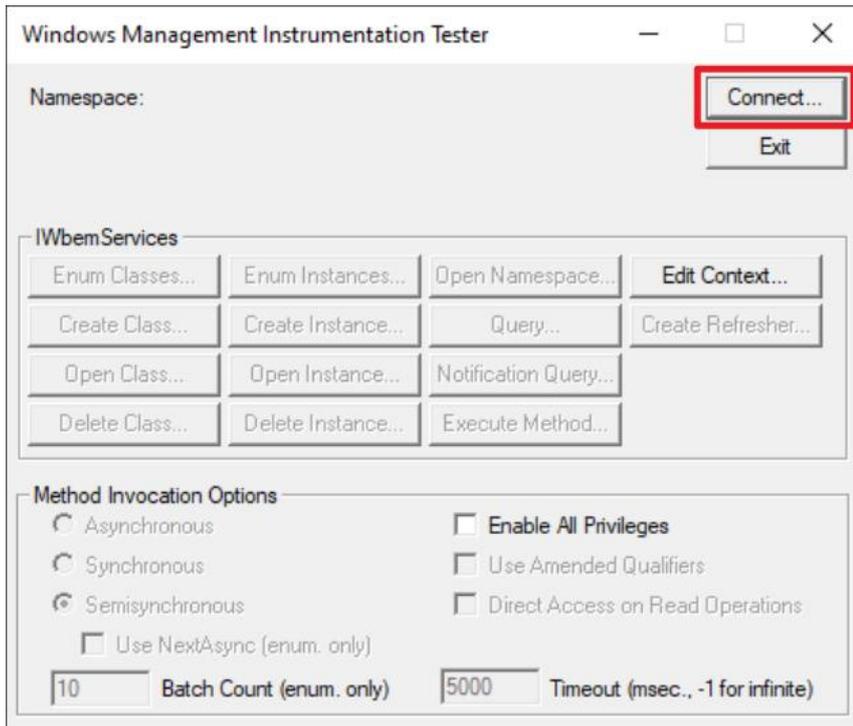


(2) Enter “wbemtest” → click “OK”

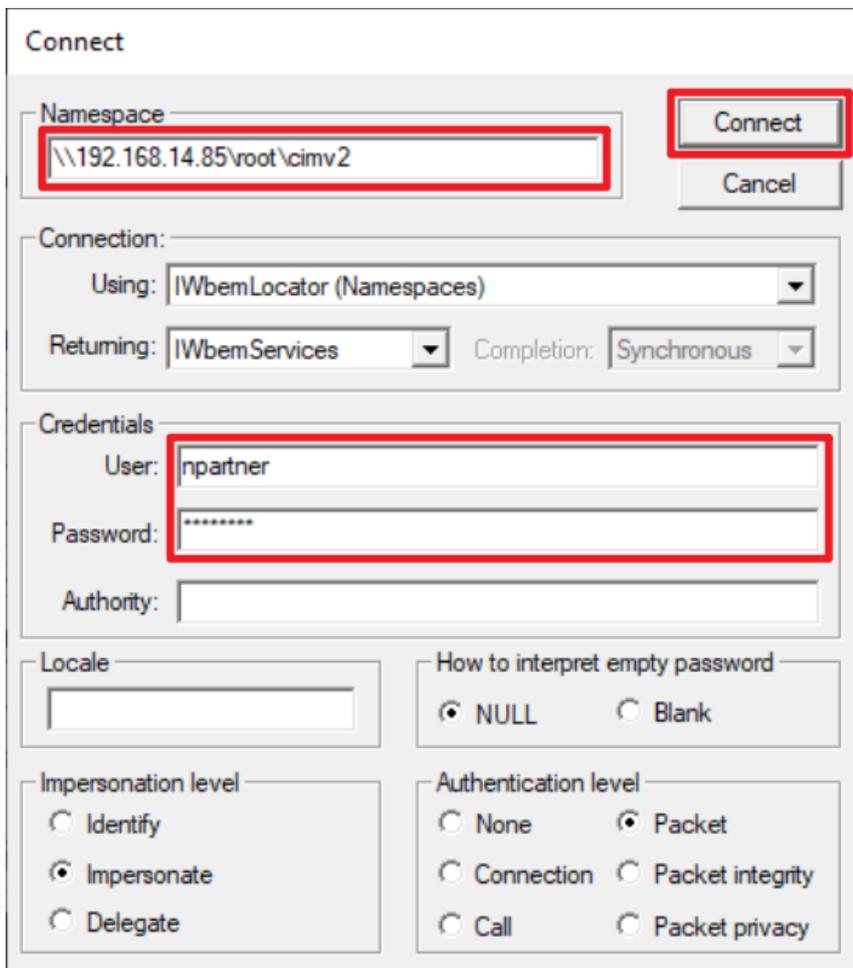


10.1.1 Query Event Logs

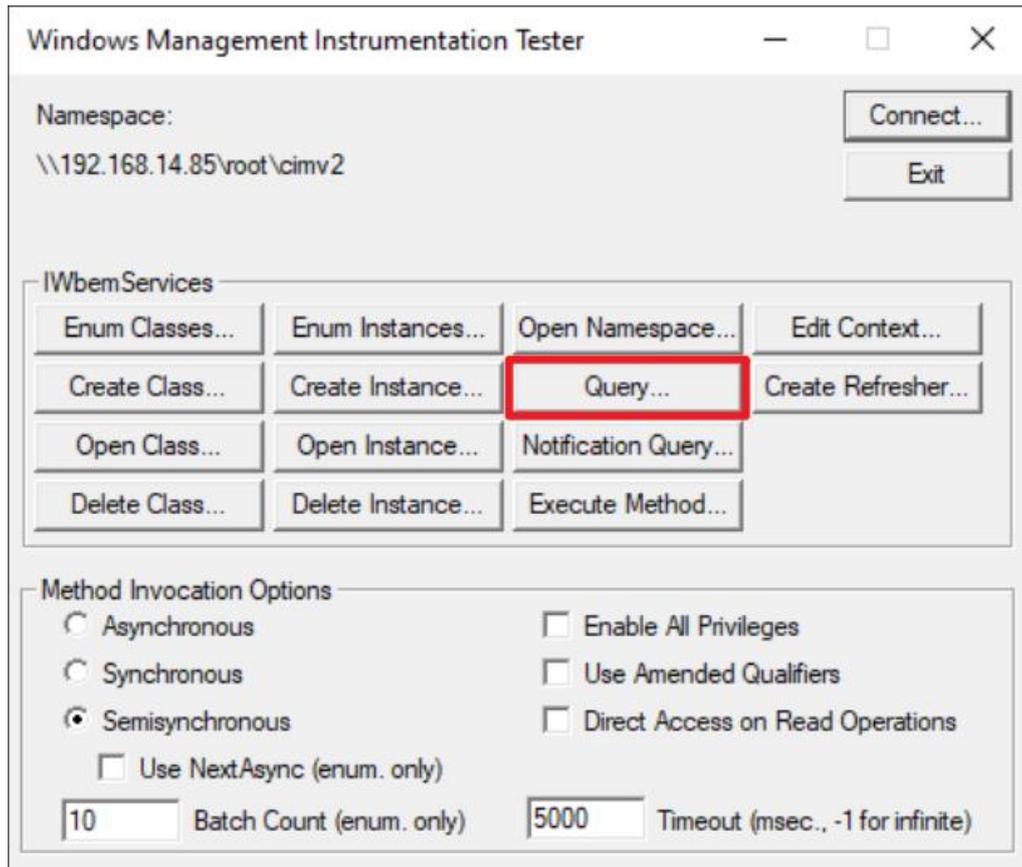
(1) Click "Connect."



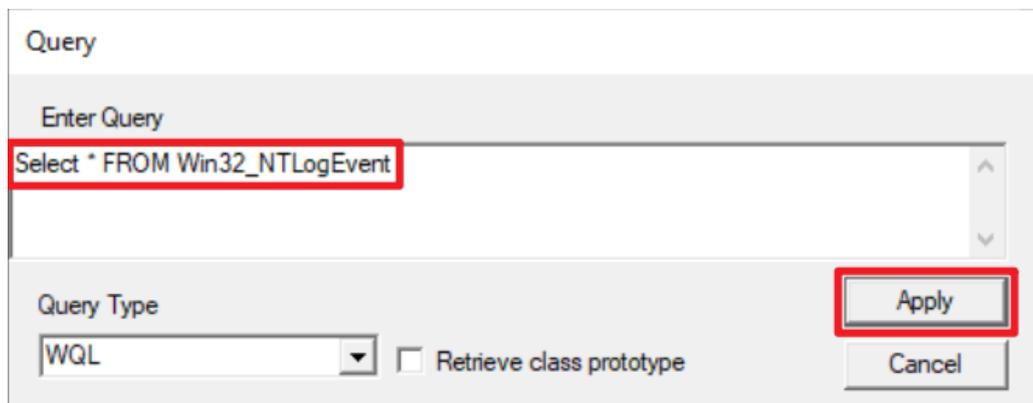
(2) Enter the namespace: (the example here is `\\192.168.14.85\root\cimv2`) → provide the username and password → click "Connect."



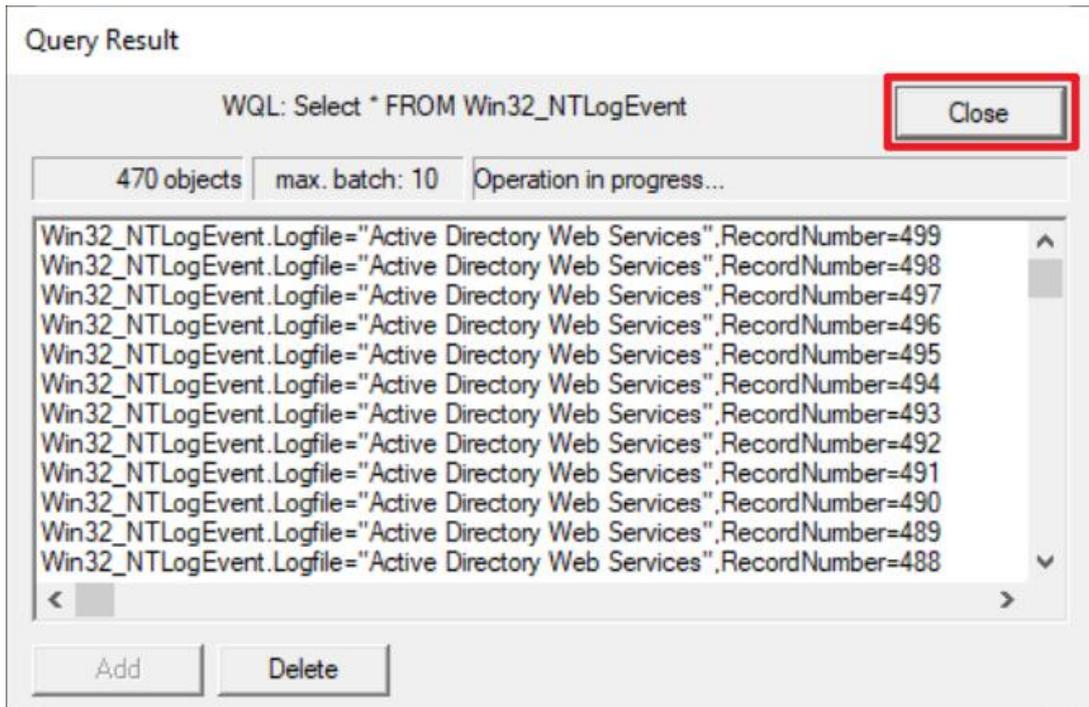
(3) Click “Query.”



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

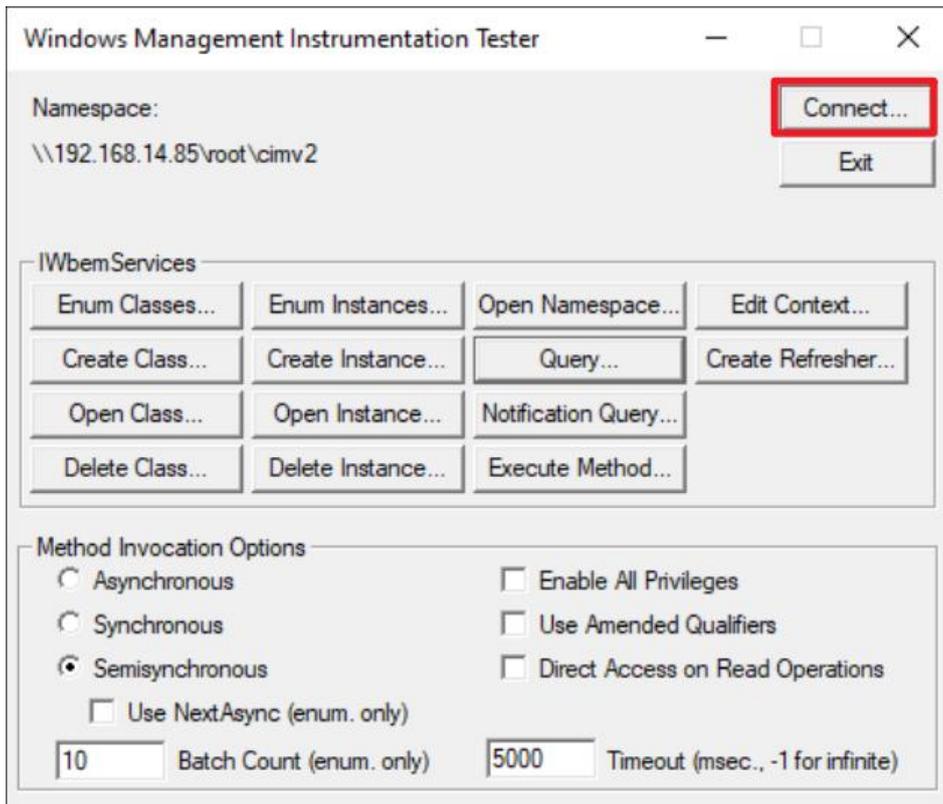


(5) The query results are displayed → click “Close.”

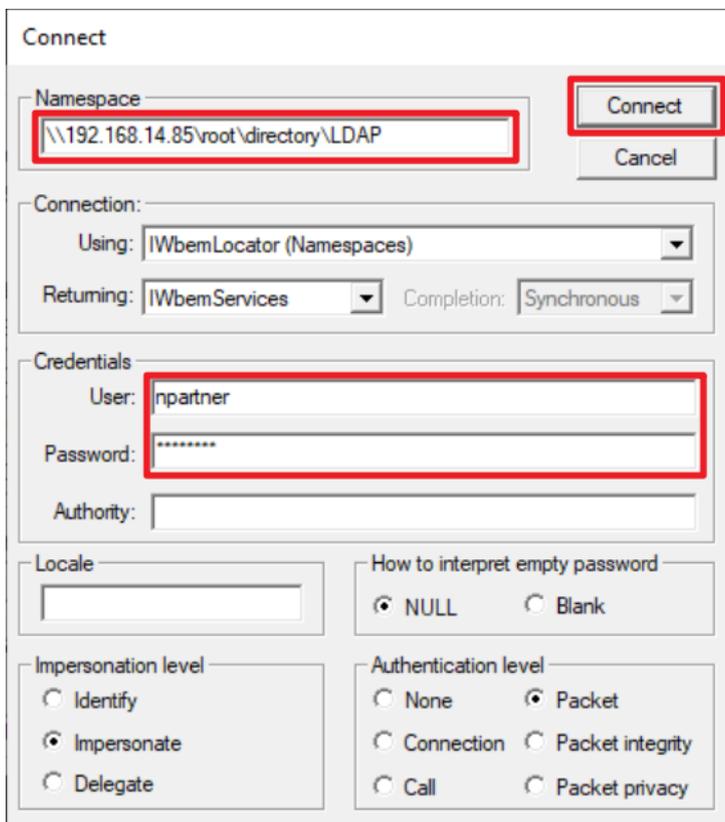


10.1.2 Query User Data

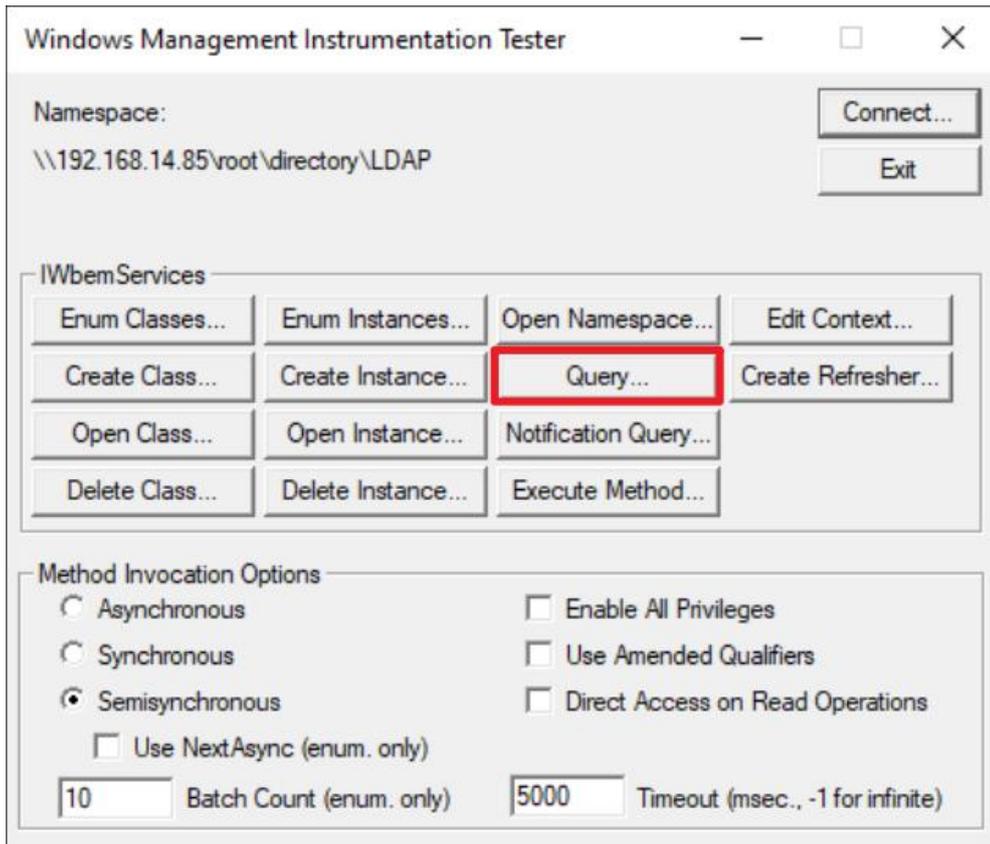
(1) Click “Connect.”



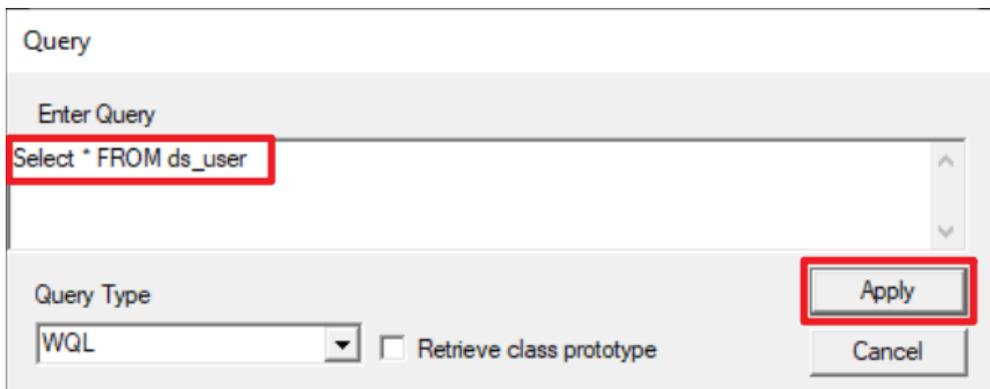
(2) Verify user data; enter the namespace: (the example here is \\192.168.14.85\root\cimv2) → provide the username and password → click “Connect.”



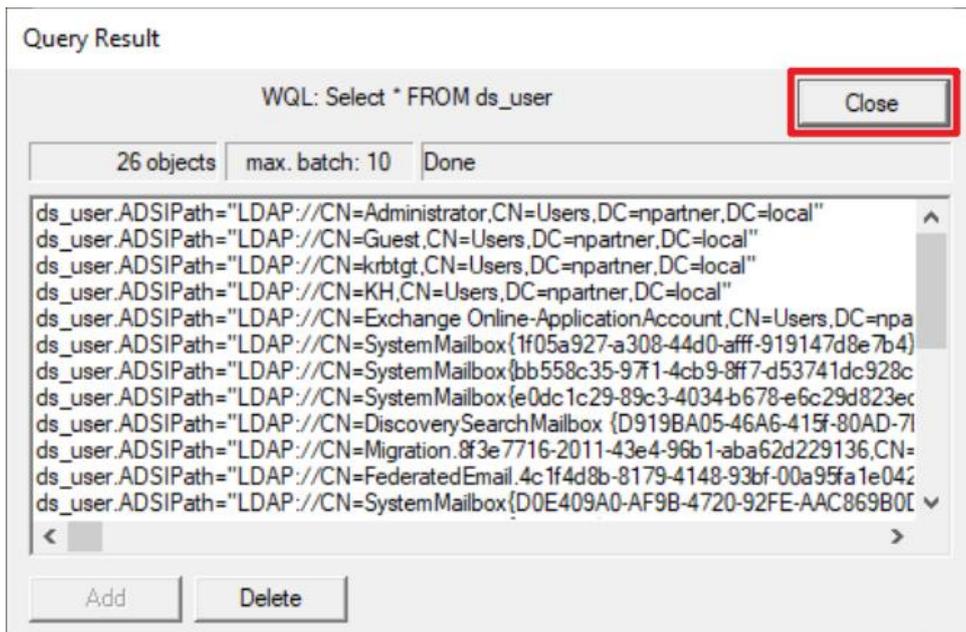
(3) Click “Query.”



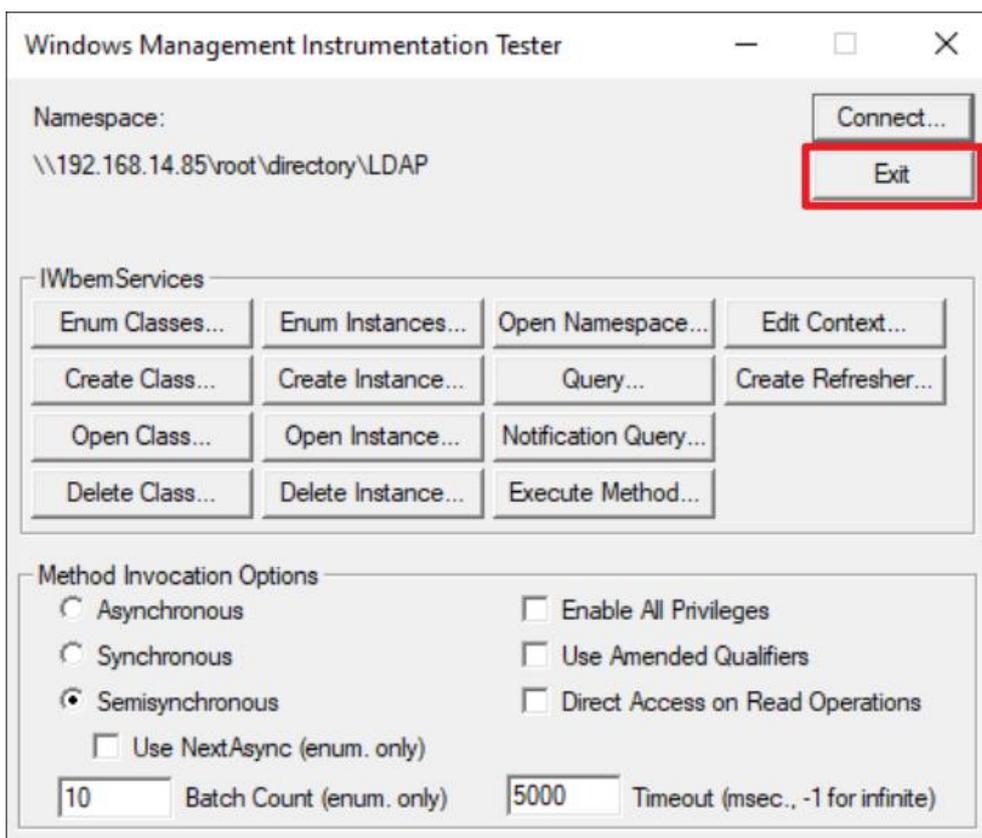
(4) Enter the query: `Select * FROM ds_user` → click “Apply.”



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

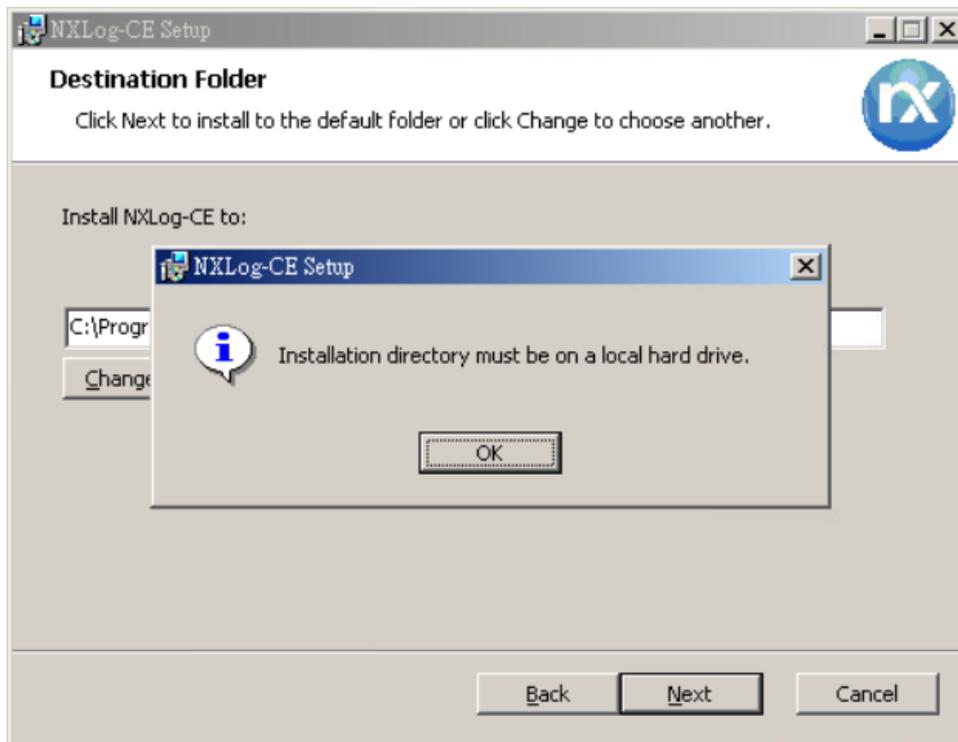


(6) If the user account and password can successfully query data, click “Exit” to close the WMI Tester.



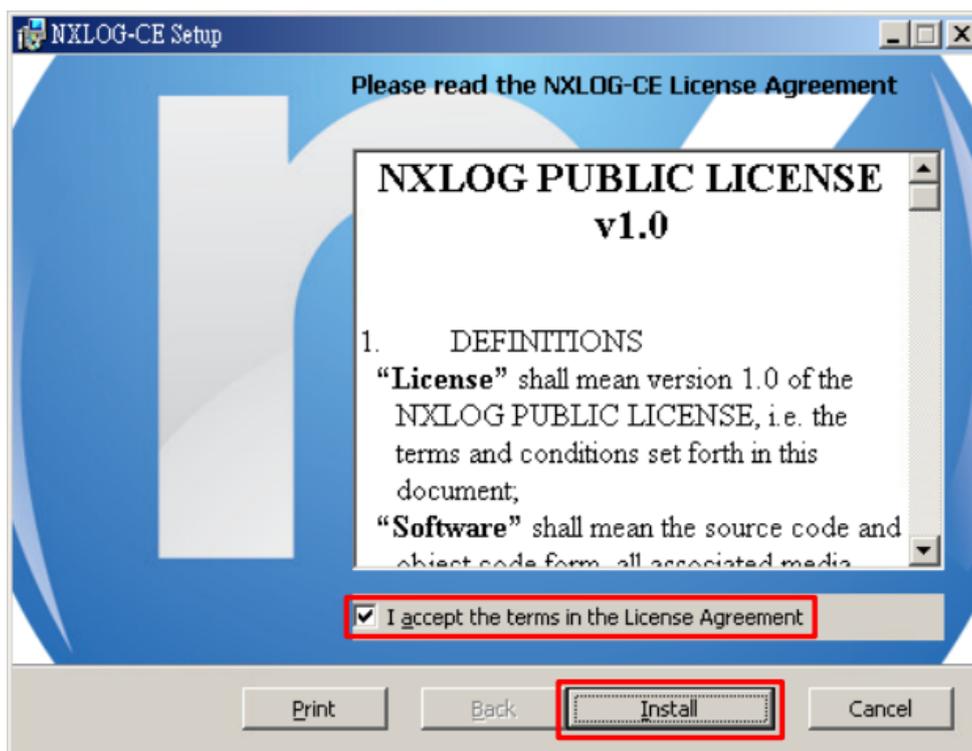
10.2 NXLog Installation Issues

(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