

Partner

How to Configure Windows File Event Log

V010

2025/08/28





Copyright Declaration

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

Registered Trademark

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

Contents

Preface.....	2
References	2
1. NXLog.....	3
1.1 NXLog Installation	3
1.2 Download NXLog Configuration File	7
1.2.1 For Windows Server 2003 or earlier:	7
1.2.2 For Windows Server 2008 or later	8
1.3 NXLog Configuration	9
1.3.1 For Windows Server 2003 or earlier	9
1.3.2 For Windows Server 2008 or later	12
1.4 Starting the NXLog Service.....	14
1.4.1 For Windows Server 2003 or earlier	14
1.4.2 For Windows Server 2008 or later	17
2. Windows Server 2000	20
2.1 Domain	20
2.1.1 Organizational Unit (OU) Configuration	20
2.1.2 Group Policy Settings	23
2.2 Workgroup.....	29
2.2.1 Audit Policy Configuration	29
2.2.2 Event Log Settings	31
2.3 Folder Audit Configuration	33
3. Windows Server 2003	37
3.1 Domain	37
3.1.1 Organizational Unit (OU) Configuration	37
3.1.2 Group Policy Settings	40
3.2 Workgroup.....	46
3.2.1 Audit Policy Configuration	46
3.2.2 Event Log Settings	49
3.3 Folder Audit Configuration	51
4. Windows Server 2008	55
4.1 Domain	55
4.1.1 Organizational Unit (OU) Configuration	55
4.1.2 Group Policy Settings	58
4.2 Workgroup.....	65
4.2.1 Audit Policy Configuration	65
4.2.2 Event Log Settings	68
4.3 Folder Audit Configuration	70
5. Windows Server 2012	74
5.1 Domain	74
5.1.1 Organizational Unit (OU) Configuration	74
5.1.2 Group Policy Settings	77
5.2 Workgroup.....	84
5.2.1 Audit Policy Configuration	84
5.2.2 Event Log Settings	87
5.3 Folder Audit Configuration	89
6. Windows Server 2016	93
6.1 Domain.....	93
6.1.1 Organizational Unit (OU) Configuration	93
6.1.2 Group Policy Settings	96
6.2 Workgroup.....	103
6.2.1 Audit Policy Configuration	103
6.2.2 Event Log Settings	107
6.3 Folder Audit Configuration	109
7. Windows Server 2019	113
7.1 Domain.....	113
7.1.1 Organizational Unit (OU) Configuration	113
7.1.2 Group Policy Settings	116
7.2 Workgroup.....	123
7.2.1 Audit Policy Configuration	123
7.2.2 Event Log Settings	127
7.3 Folder Audit Configuration	129
8. Windows Server 2022	133
8.1 Domain.....	133
8.1.1 Organizational Unit (OU) Configuration	133
8.1.2 Group Policy Settings	136
8.2 Workgroup.....	143
8.2.1 Audit Policy Configuration	143
8.2.2 Event Log Settings	147
8.3 Folder Audit Configuration	149
9. N-Reporter	153
9.1 For Windows Server 2003 or earlier	154
9.2 For Windows 2008 or later	157
10. Troubleshooting	160
10.1 Invoke-GPUUpdate Error.....	160
Contact	162

Preface

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

NXLog converts Windows file 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>

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.

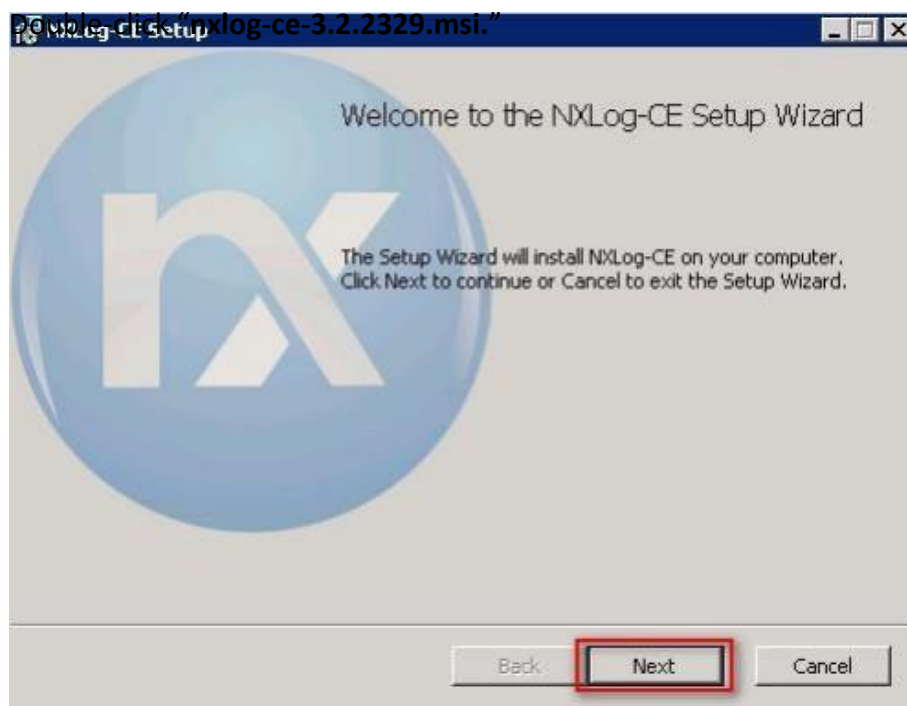
Example Here: **nxlog-ce-3.2.2329.msi**



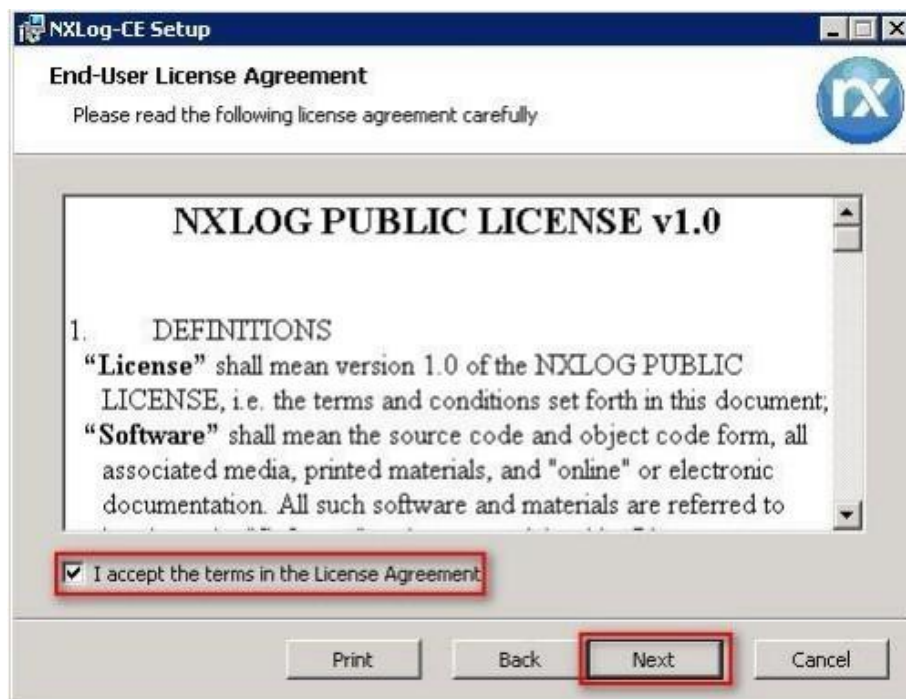
Note: If you require the **32-bit** version of NXLog, please contact our support team.

(2) Install NXLog

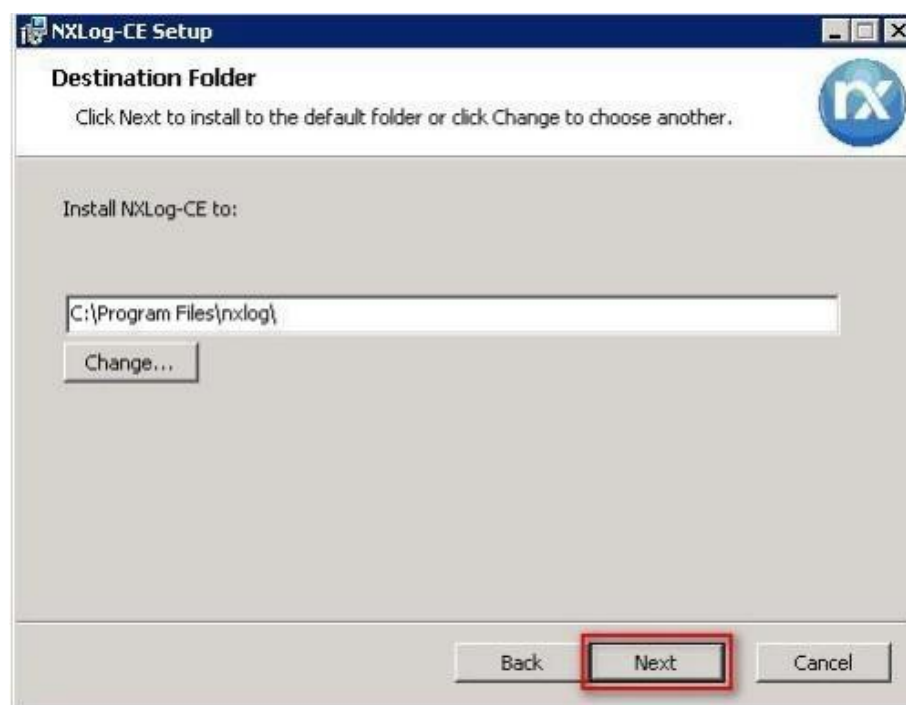
<2.1> For Windows Server **2008** or later:



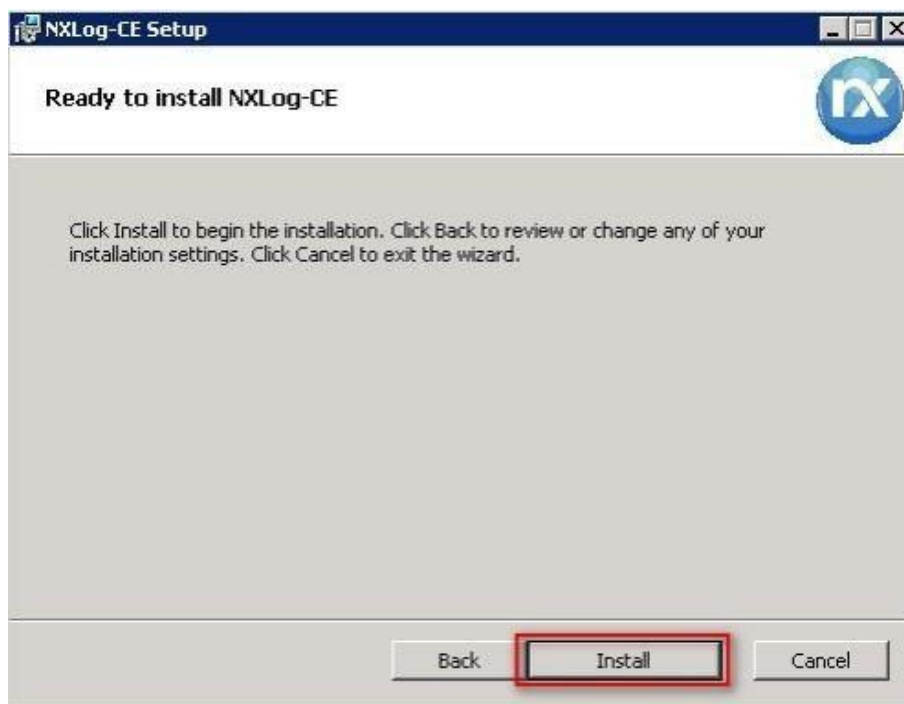
(3) Select “I accept the terms in the License Agreement,” then click “Next.”



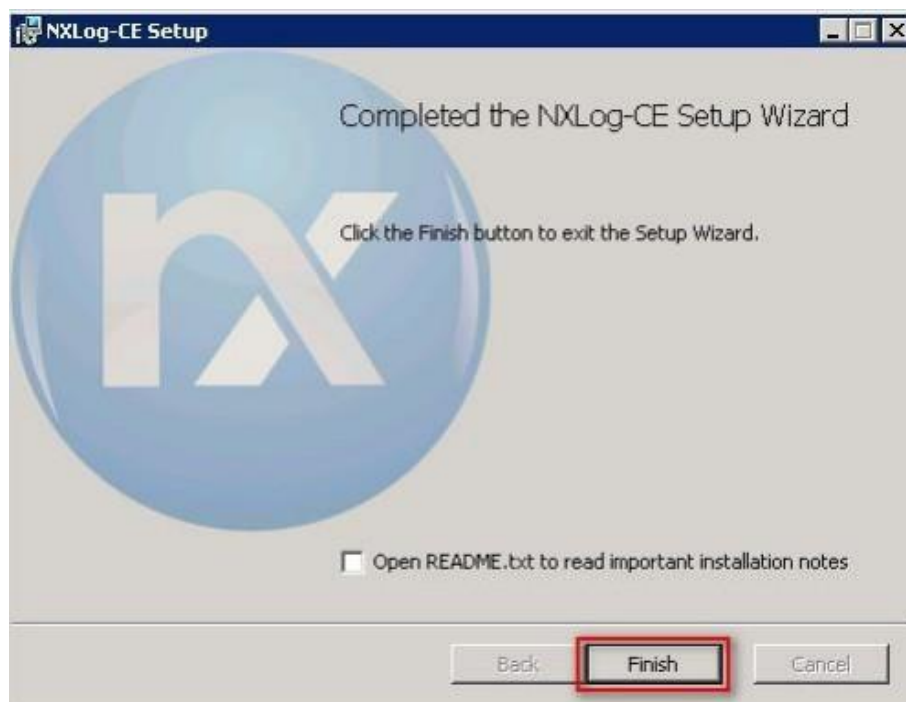
(4) Click “Next.” (The default installation path is (C:\Program Files\nxlog\)).



(5) Click "Install."

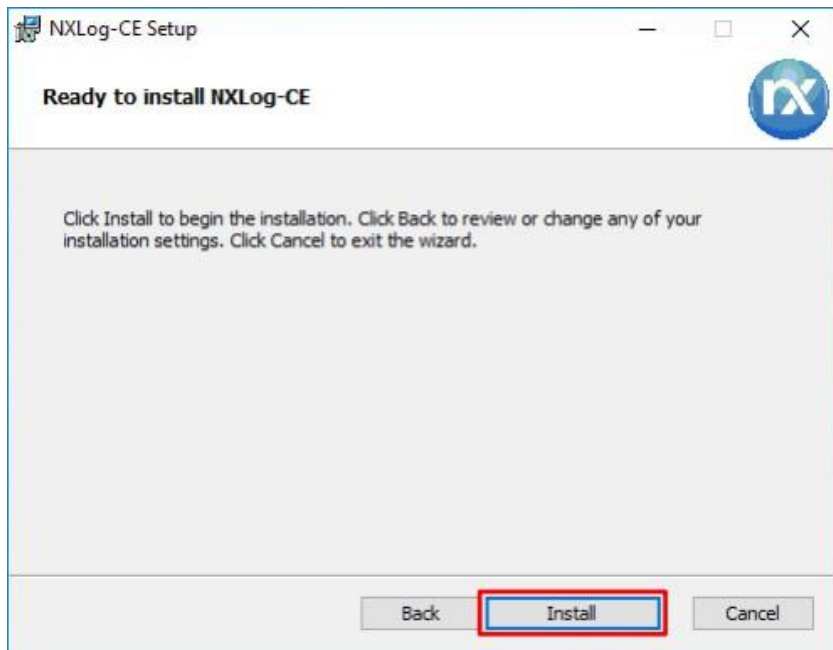


(6) Click "Finish."



<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.

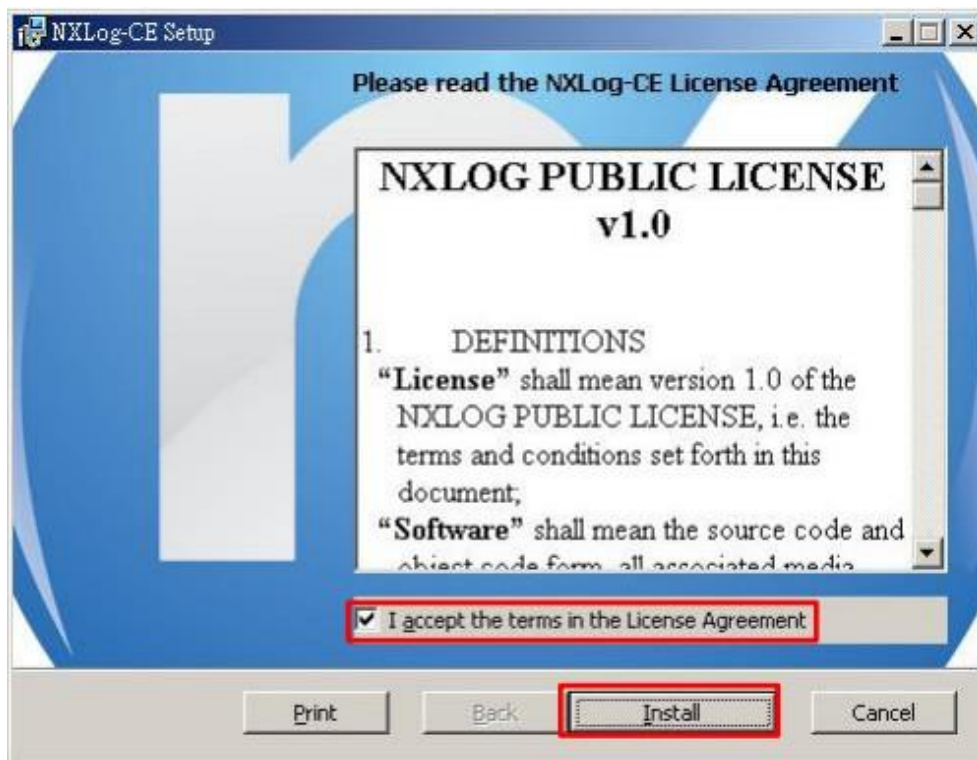


<2.3> For Windows 2000:

(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:

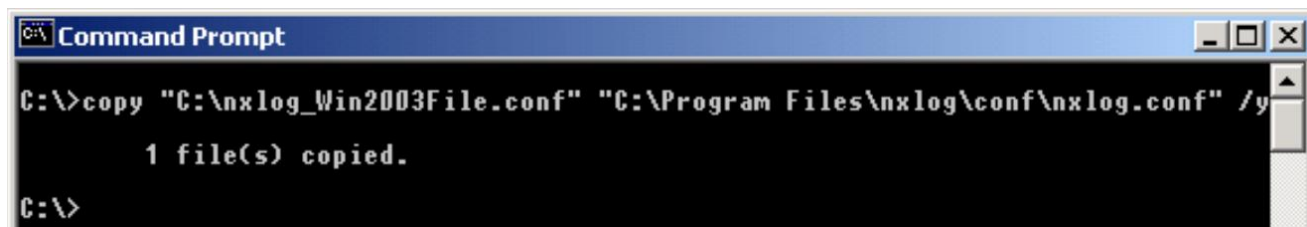
(1) Open "Command Prompt."



(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_Win2003File.conf

```
C:\> copy "C:\nxlog_Win2003File.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```



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

1.2.2 For Windows Server 2008 or later

(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_Win2008File.conf

```
PS C:\> Invoke-WebRequest -Uri 'http://www.npartner.com/download/tech/nxlog_Win2008File.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'

1.3 NXLog Configuration

1.3.1 For Windows Server 2003 or earlier

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
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>

## For windows File 2000 - 2003 Event Log use the following:
<Input in_eventlog>
  Module in_mseventlog
  ReadFromLast TRUE
  SavePos TRUE
  Exec parse_syslog_bsd(); \
    if ($EventID == 560 or $EventID == 561 or $EventID == 562 or $EventID == 563 or $EventID == 564 or $EventID == 567 or $EventID == 528 or
$EventID == 529 or $EventID == 530 or $EventID == 531 or $EventID == 532 or $EventID == 533 or $EventID == 534 or $EventID == 535 or
$EventID == 536 or $EventID == 537 or $EventID == 538 or $EventID == 539 or $EventID == 540 or $EventID == 551 or $EventID == 552 or
$EventID == 682 or $EventID == 683 or $EventID == 672 or $EventID == 673 or $EventID == 674 or $EventID == 675 or $EventID == 676 or
$EventID == 677 or $EventID == 678 or $EventID == 679 or $EventID == 680 or $EventID == 681) { $SyslogFacilityValue = 17; } \
    else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 17; } \
    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>
```

Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.

```
define NCloud 192.168.8.4

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>
```

```
## For windows File 2000 - 2003 Event Log use the following:
```

```
<Input in_eventlog>
```

```
Module im_mseventlog
```

```
ReadFromLast TRUE
```

```
SavePos TRUE
```

```
Exec parse_syslog_bsd(); \
```

```
if ($EventID == 560 or $EventID == 561 or $EventID == 562 or $EventID == 563 or $EventID == 564 or $EventID == 567  
or $EventID == 528 or $EventID == 529 or $EventID == 530 or $EventID == 531 or $EventID == 532 or $EventID == 533 or  
$EventID == 534 or $EventID == 535 or $EventID == 536 or $EventID == 537 or $EventID == 538 or $EventID == 539 or  
$EventID == 540 or $EventID == 551 or $EventID == 552 or $EventID == 682 or $EventID == 683 or $EventID == 672 or  
$EventID == 673 or $EventID == 674 or $EventID == 675 or $EventID == 676 or $EventID == 677 or $EventID == 678 or  
$EventID == 679 or $EventID == 680 or $EventID == 681) { $SyslogFacilityValue = 17; } \
```

```
else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 17; } \
```

```
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>
```

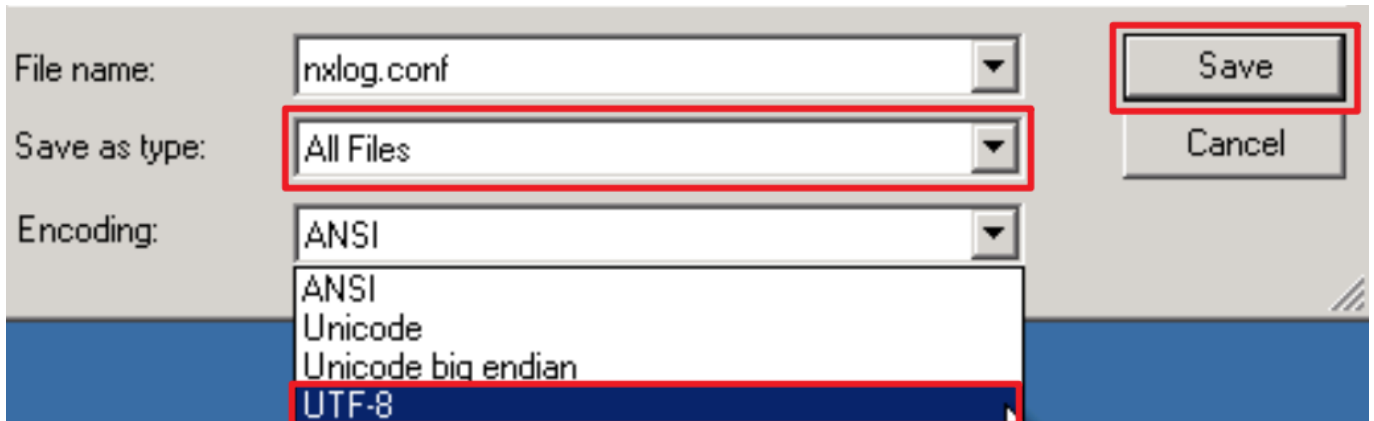

Enter the N-Reporter system IP address in the blue text section.

```
define NCloud 192.168.3.88
```

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

```
## Please set the ROOT to the folder your nxlog was installed into, otherwise it will not start.
define NCloud 192.168.8.4
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 4656, 4657, 4658, 4659, 4660, 4661, 4663, 4664, \
4665, 4666, 4667, 4668, 4670, 4671, 4688, 4690, \
4691, 4698, 4699, 4700, 4701, 4702, 5140, 5142, \
5143, 5144, 5145, 5148, 5149, 5150, 5151, 5152, \
5153, 5154, 5155, 5156, 5157, 5158, 5159, 5168, \
5888, 5889, 5890, 4768, 4769, 4770, 4771, 4772, \
4773, 4774, 4775, 4776, 4777, 4820, 4624, 4625, \
4626, 4627, 4634, 4646, 4647, 4648, 4649, 4672, \
4675, 4778, 4779, 4800, 4801, 4802, 4803, 4964, \
4976, 5378, 5632, 5633

## 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> \
    </Query> \
  </QueryList>
  Exec if ($EventID NOT IN (%SecurityEvents%)) 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>
```

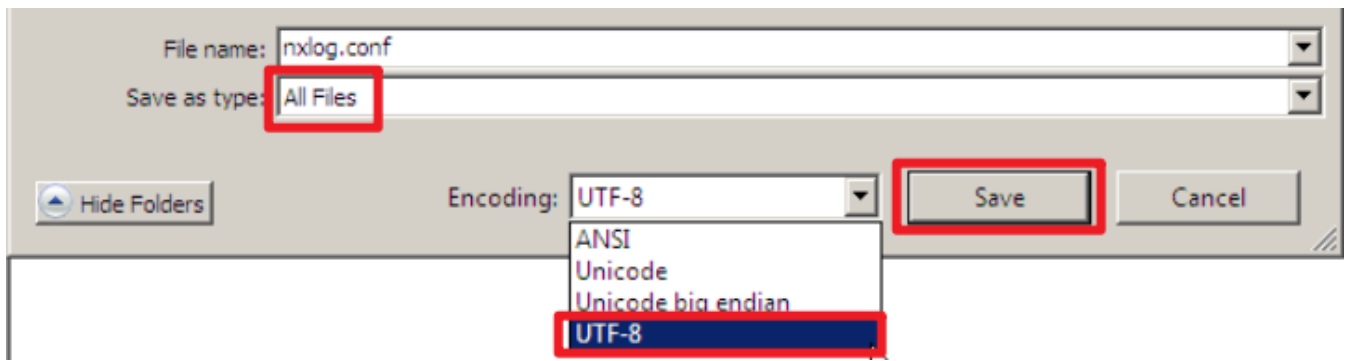
Enter the N-Reporter system IP address in the blue text section.

```
define NCloud 192.168.3.88
```

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

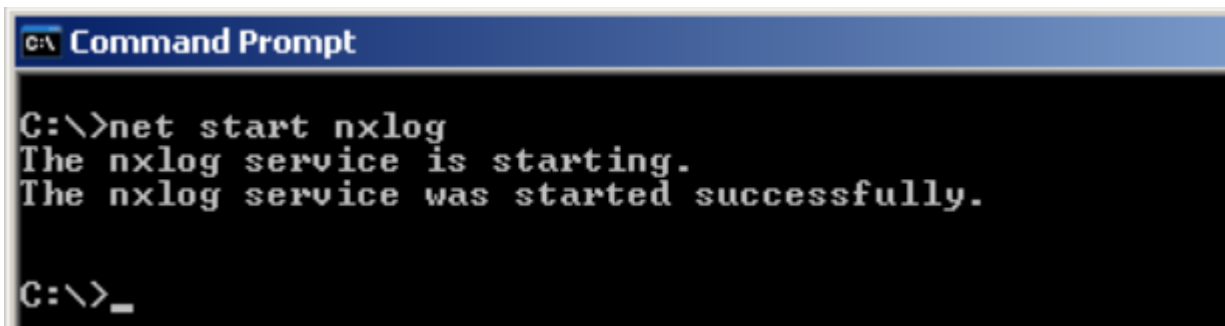
(1) Open "Command Prompt."



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

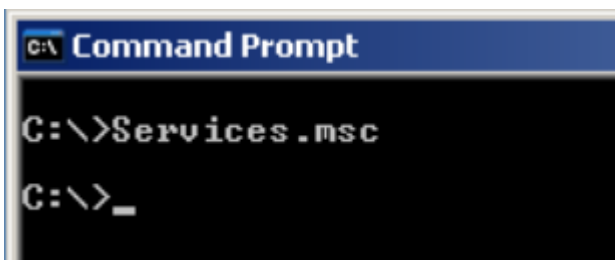
```
C:\> net start nxlog
```

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

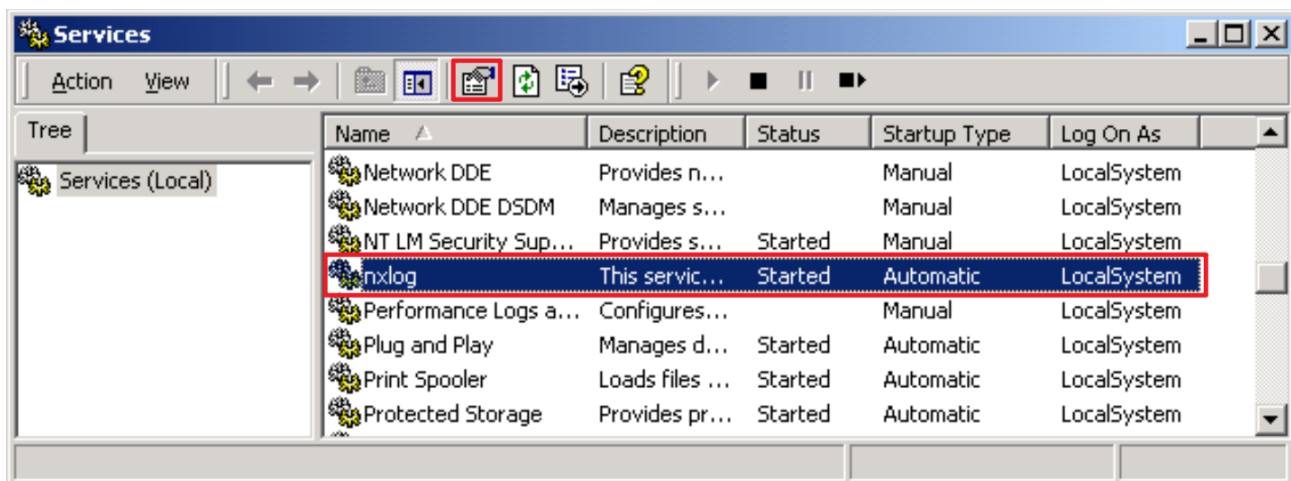
A screenshot of a Windows Command Prompt window. The title bar says "C:\ Command Prompt". The command prompt shows the command "net start nxlog" being entered, followed by the output: "The nxlog service is starting." and "The nxlog service was started successfully." The prompt is now at "C:\>_".

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

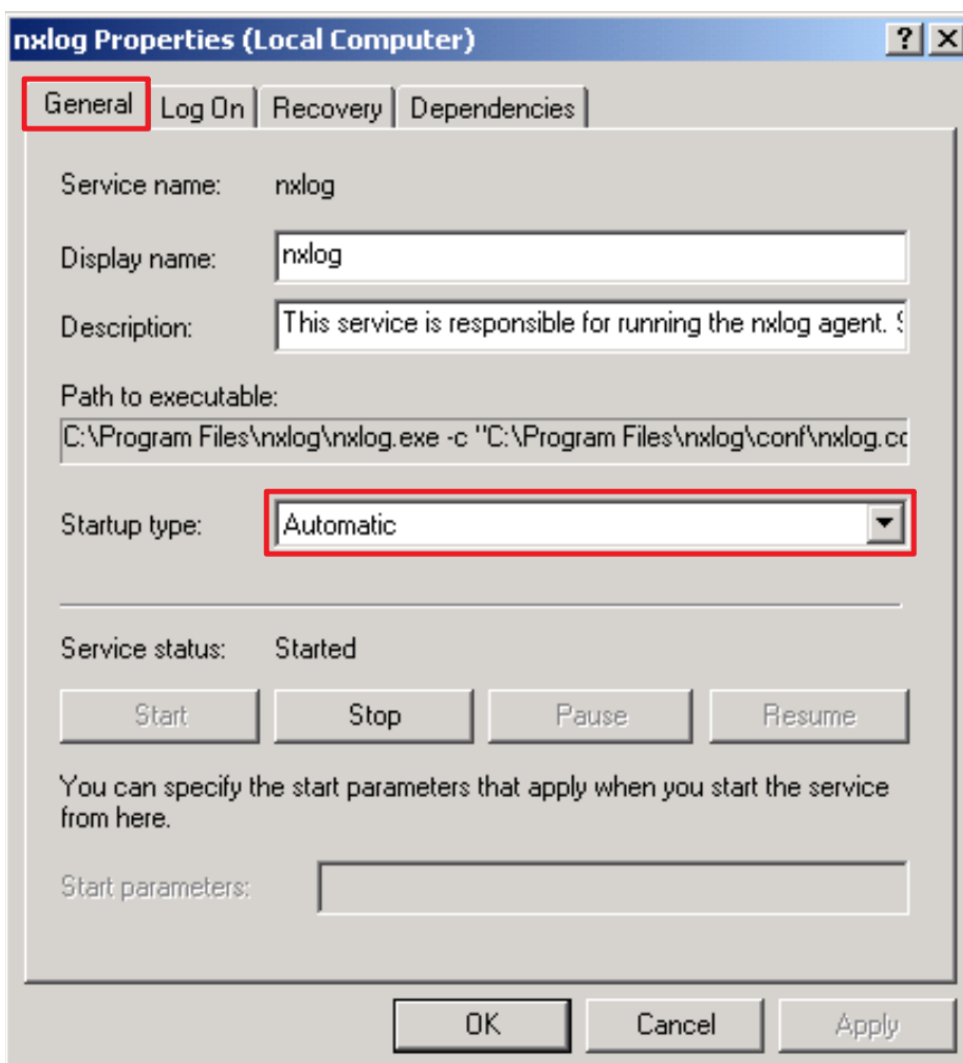
```
C:\> Services.msc
```



(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.”

The screenshot shows the 'nxlog Properties (Local Computer)' dialog box with the 'Recovery' tab selected. The 'Recovery' tab is highlighted with a red box. Below the tab, the text 'Select the computer's response if this service fails.' is displayed. Three dropdown menus are shown, each with 'Restart the Service' selected and highlighted by a red box: 'First failure:', 'Second failure:', and 'Subsequent failures:'. Below these, there are two input fields: 'Reset fail count after:' with the value '0' and 'days', and 'Restart service after:' with the value '1' and 'minutes'. A section titled 'Run file:' contains a 'File:' input field with a 'Browse...' button, a 'Command line parameters:' input field, and a checkbox labeled 'Append fail count to end of command line (/fail=%1%)'. At the bottom of the dialog, the 'OK' button is highlighted with a red box, along with 'Cancel' and 'Apply' buttons. A 'Restart Computer Options...' button is also visible.

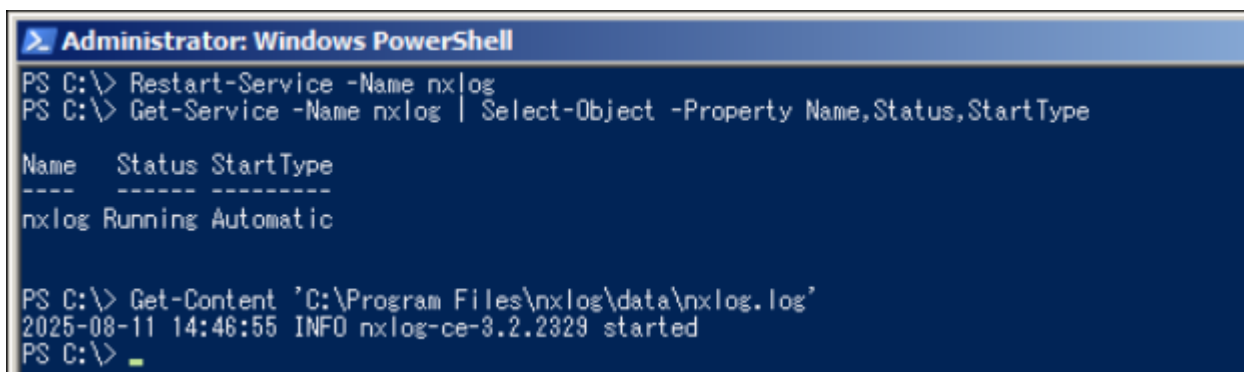
1.4.2 For Windows Server 2008 or later

(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 a Windows PowerShell console window titled "Administrator: Windows PowerShell". The console shows the following commands and output:

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

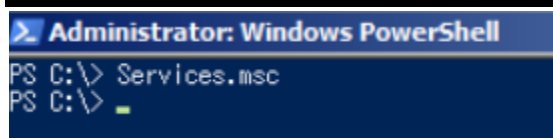
Name      Status StartType
-----
nxlog     Running Automatic


PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
2025-08-11 14:46:55 INFO nxlog-ce-3.2.2329 started
PS C:\> _
```

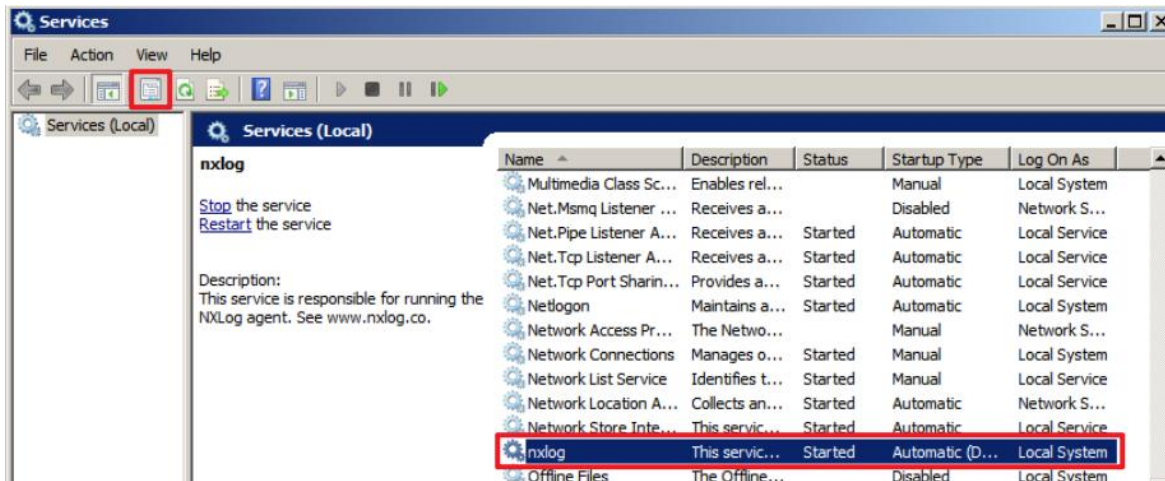
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:\Program Files(x86)\nxlog\conf\nxlog.conf'

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

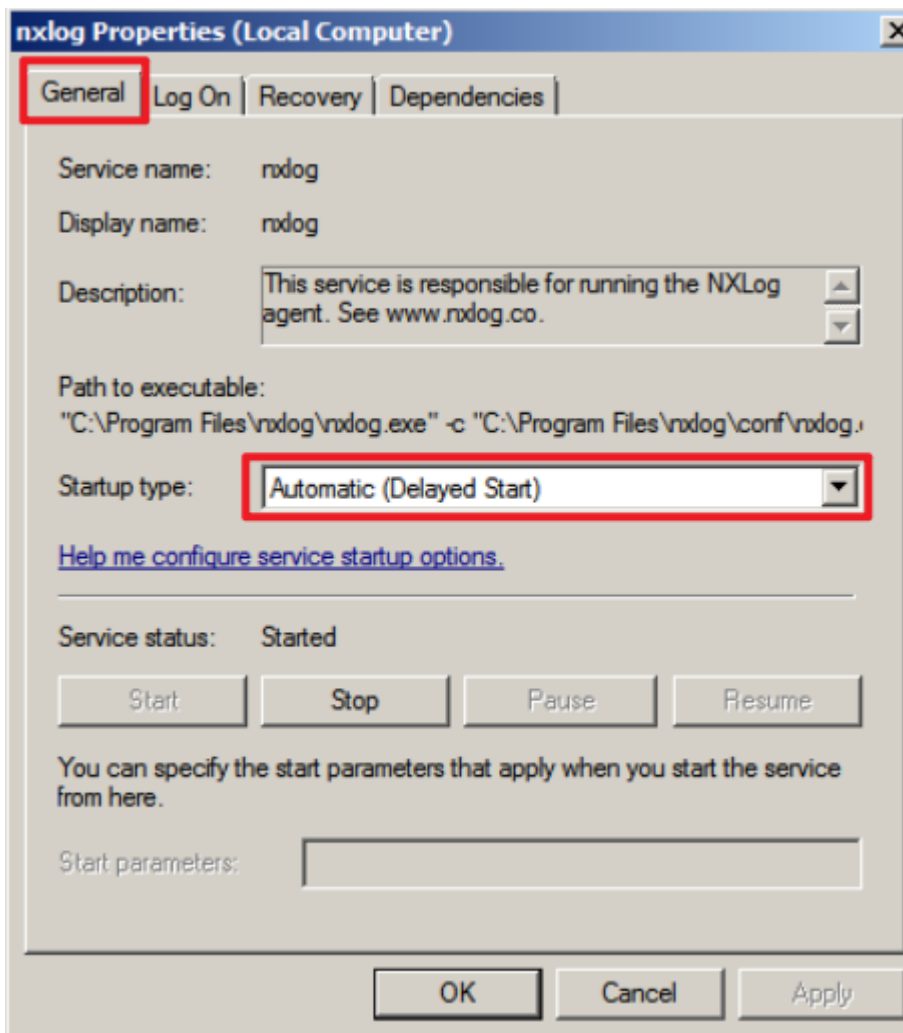
```
PS C:\> Services.msc
```



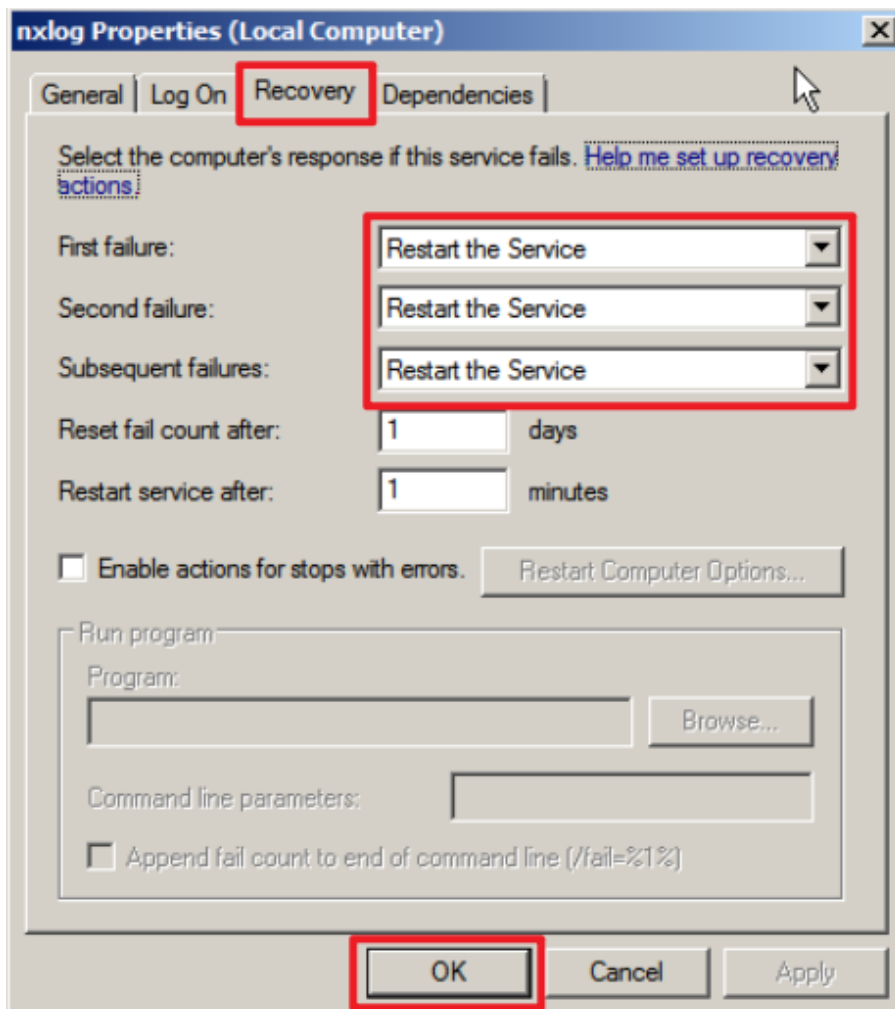
(4) Open the NXLog service properties: select “NXLog” →  Click “Properties.”



(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

2.1 Domain

Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

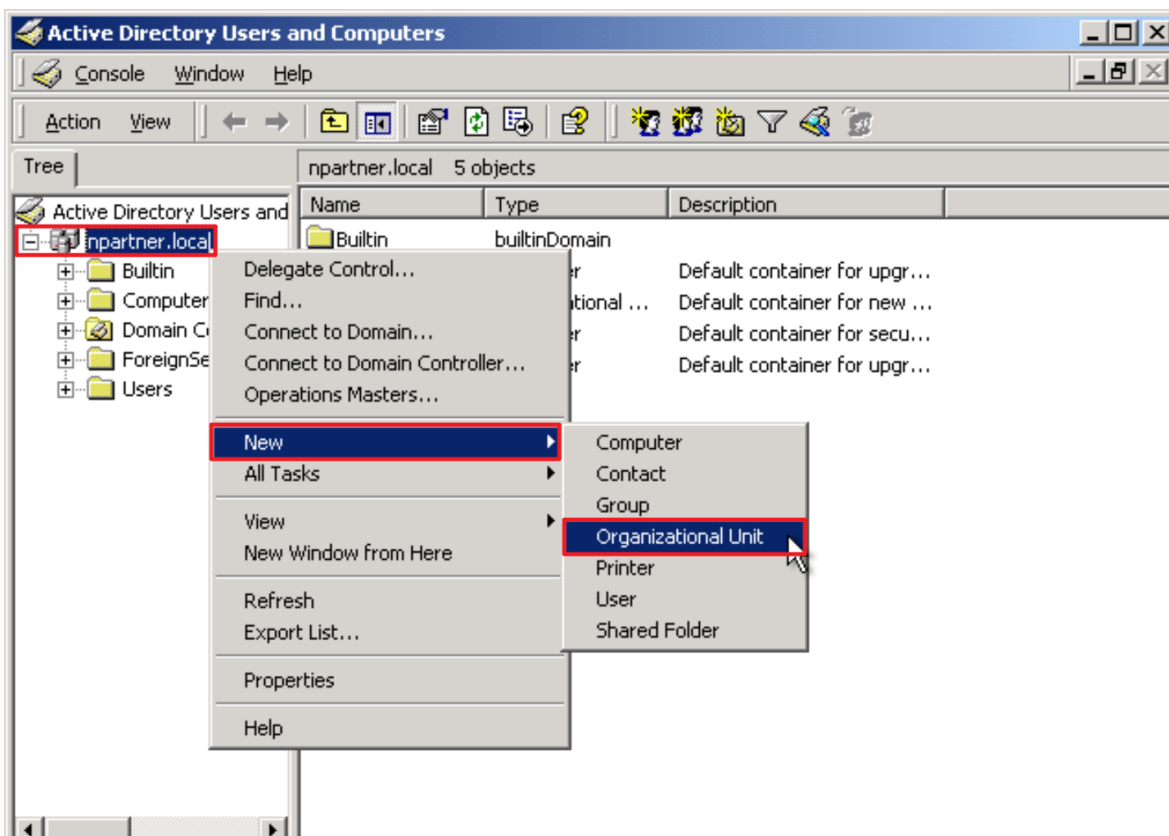
2.1.1 Organizational Unit (OU) Configuration

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



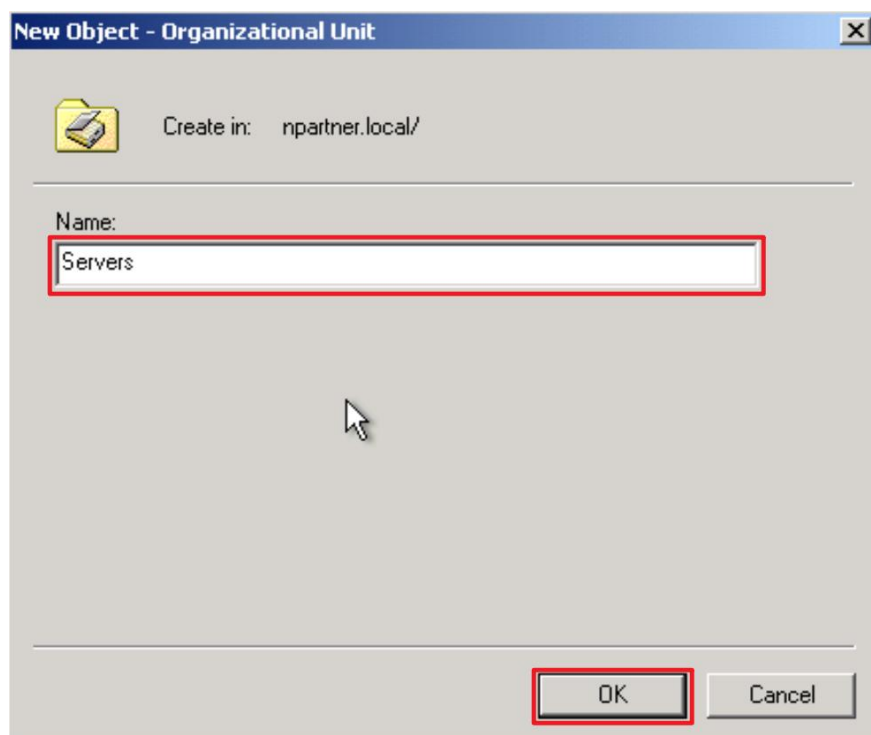
(2) Add an Organizational Unit

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



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

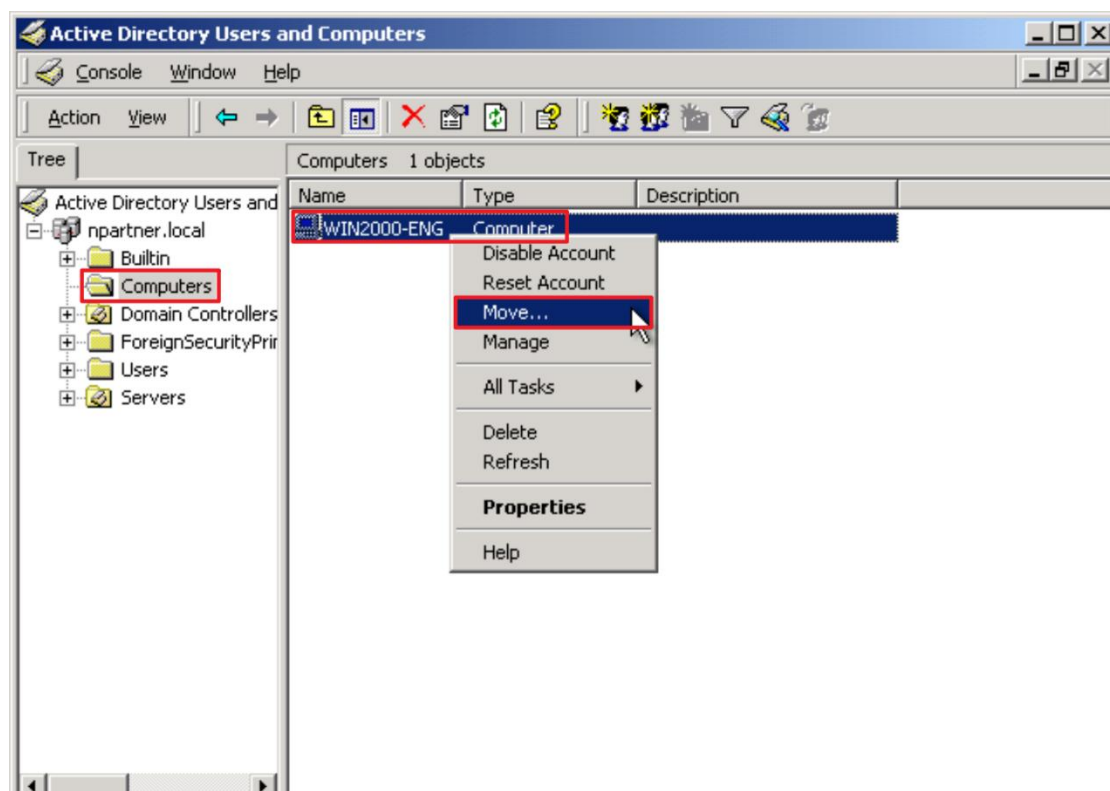
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

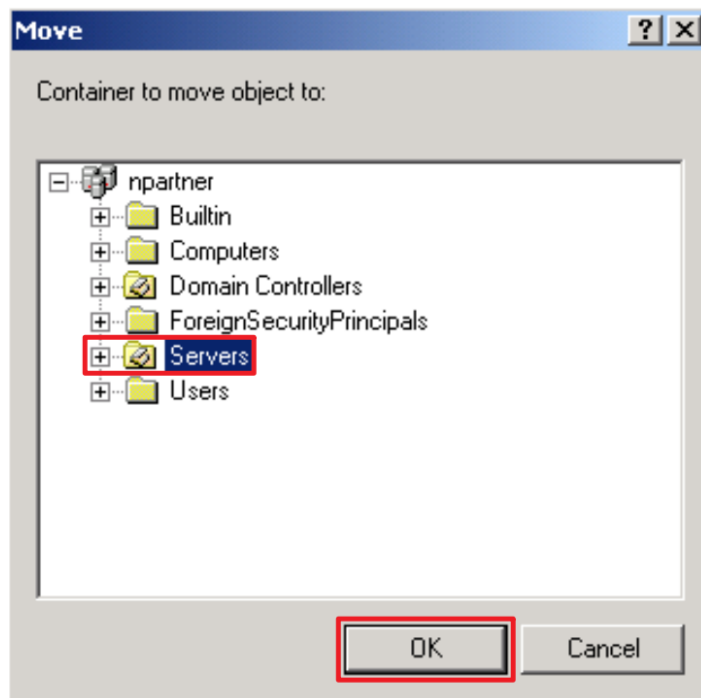
Select the “Computers” organizational unit (OU) → right-click on the “WIN2000-ENG” server.

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



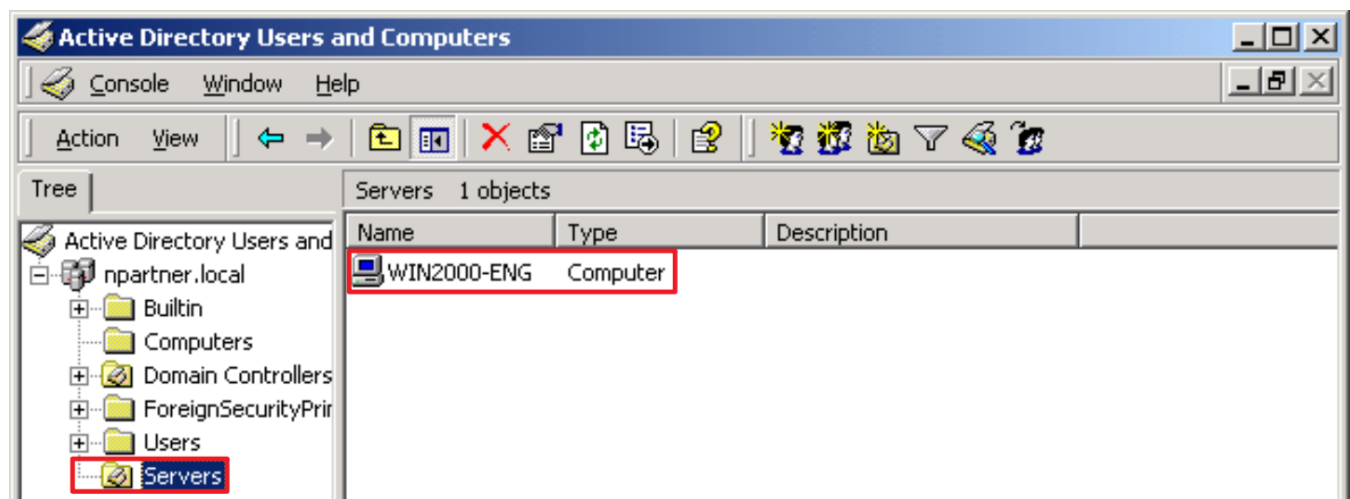
(5) Select your Organizational Unit:

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 “WIN2000-ENG” server has been moved.

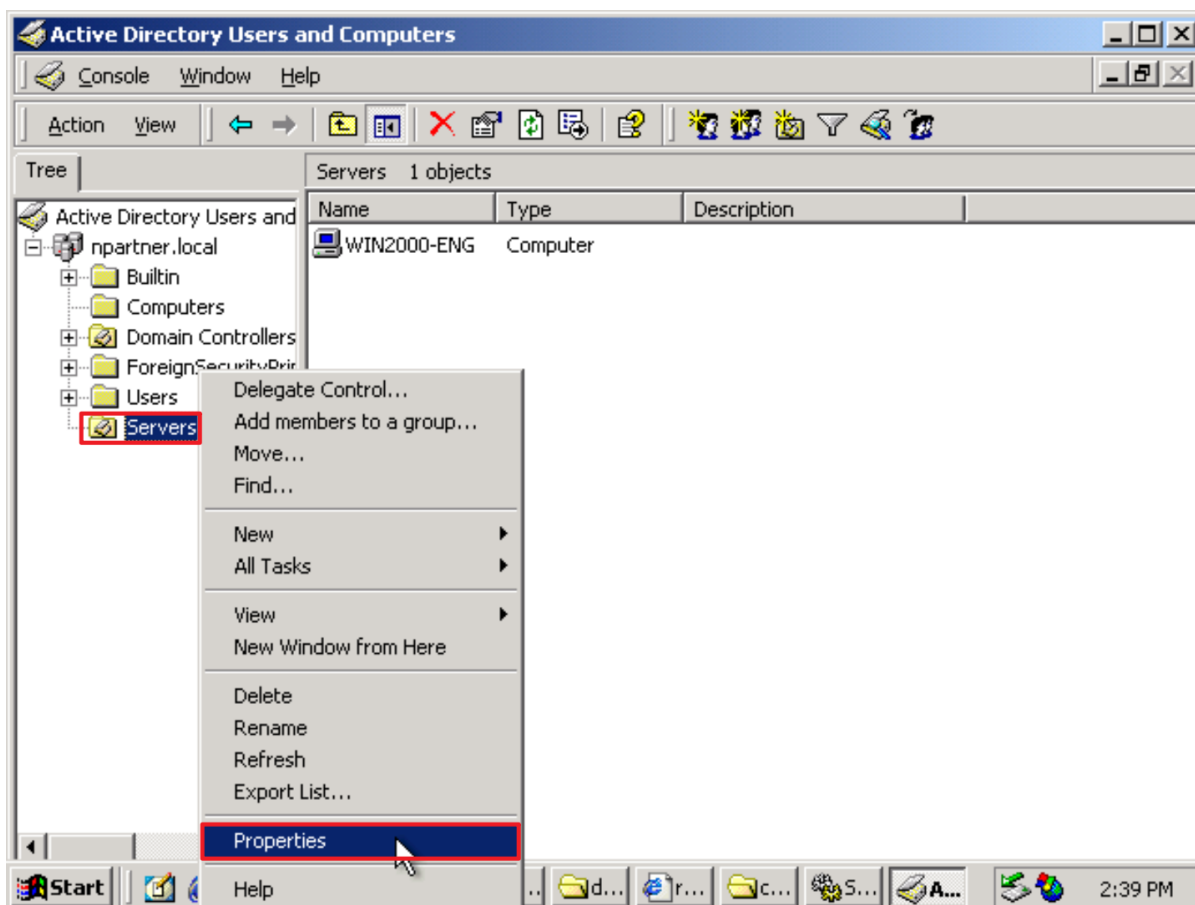


2.1.2 Group Policy Settings

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

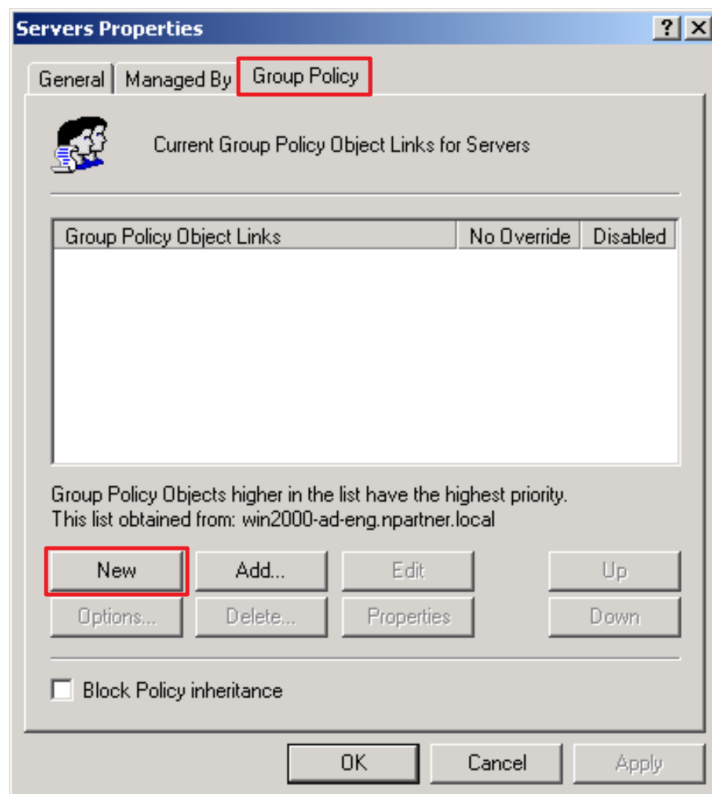


(2) In the “Servers” organizational unit (OU), right-click and select “Properties.”



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

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

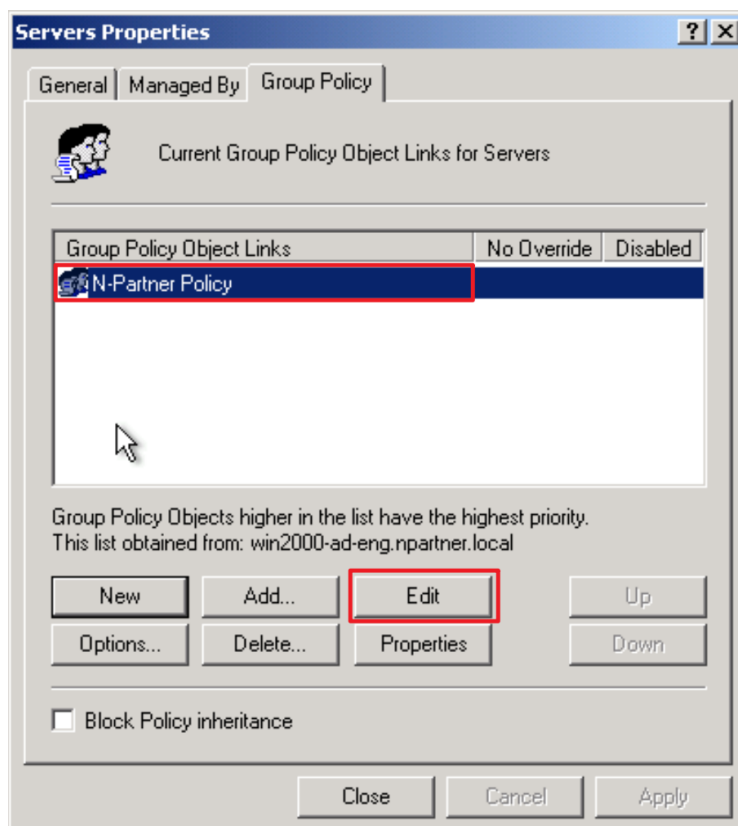


(4) Edit your Group Policy Object

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

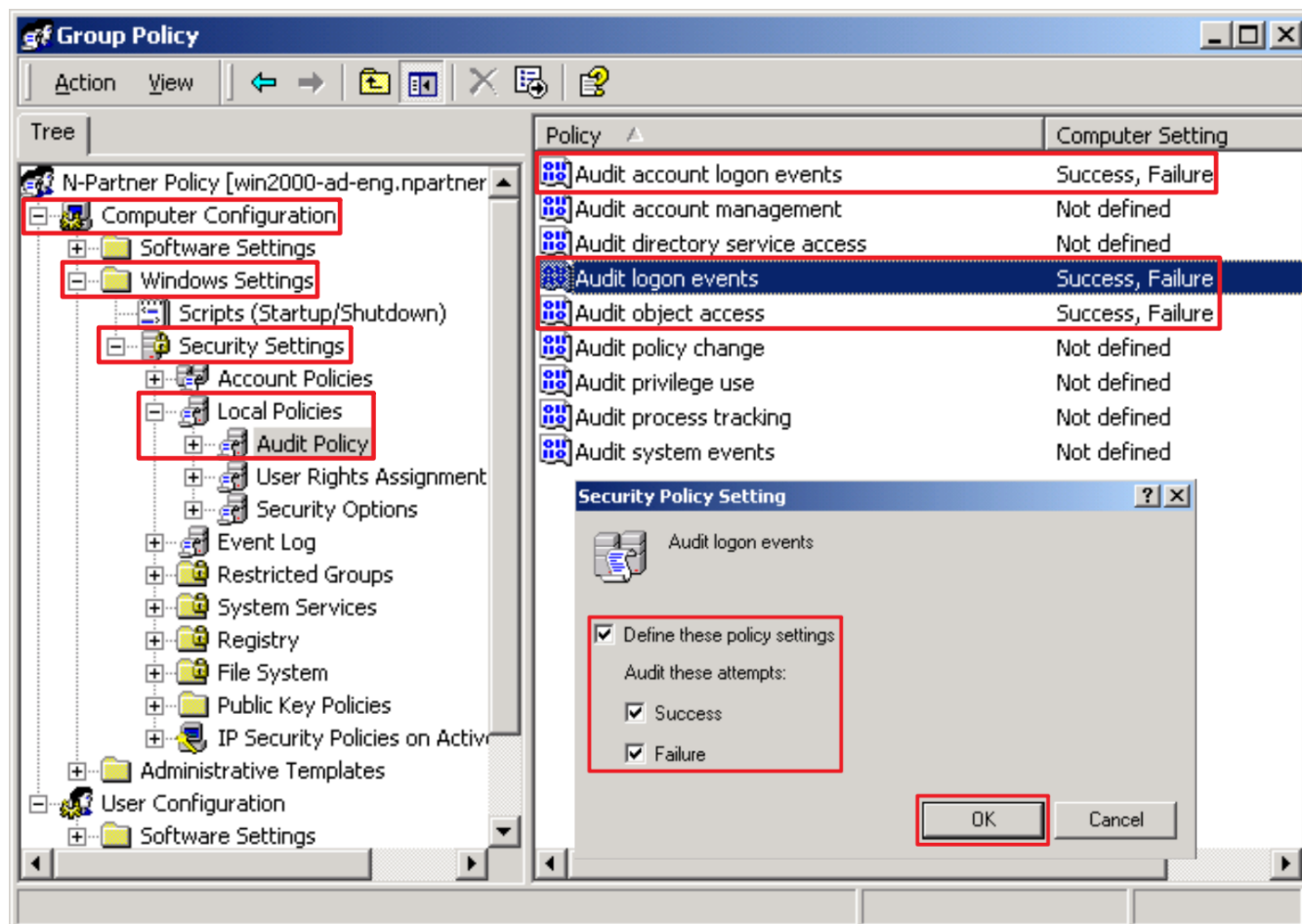
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



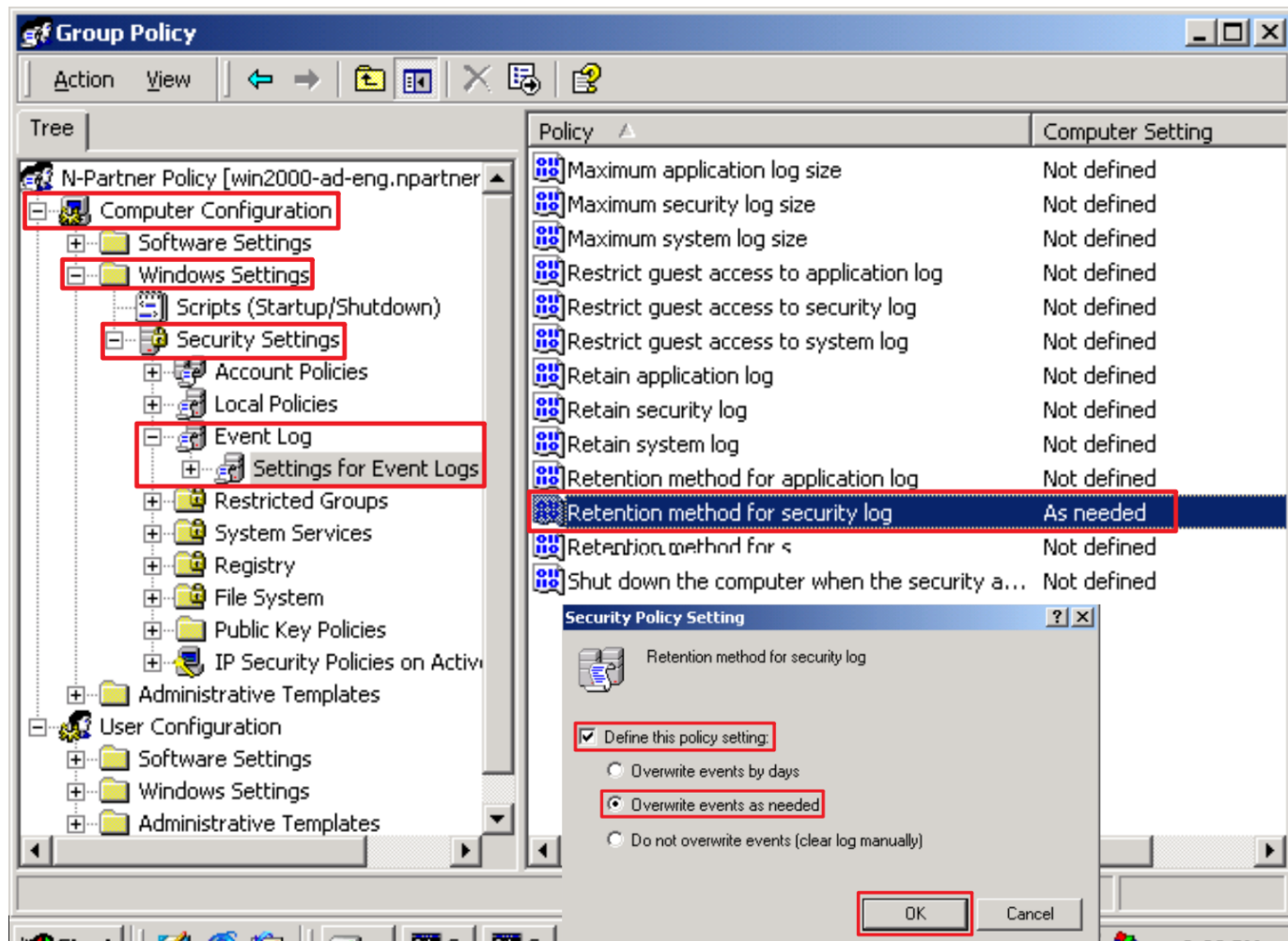
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

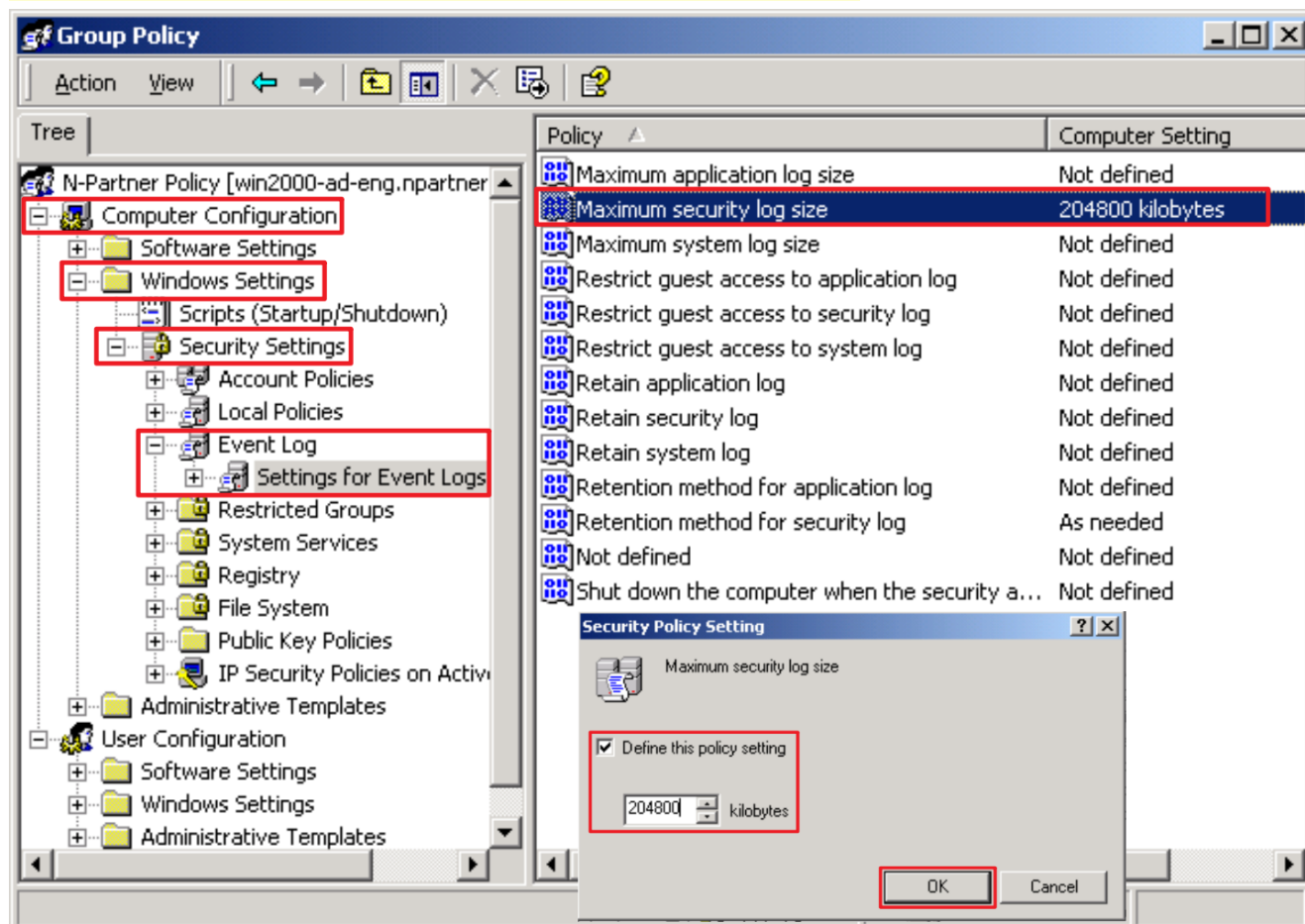
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

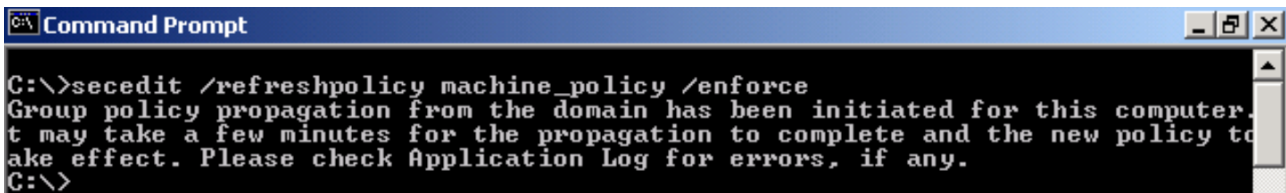


(8) On the Windows File server, open “Command Prompt.”



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

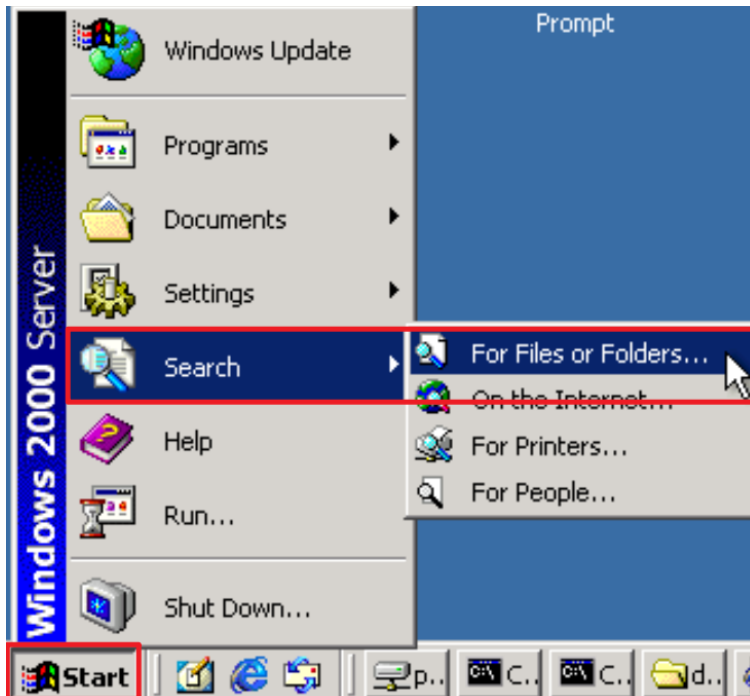
```
C:\> secedit /refreshpolicy machine_policy /enforce
```

A screenshot of a Windows Command Prompt window. The title bar is blue and says 'Command Prompt'. The window has standard Windows window controls (minimize, maximize, close) on the right. The command prompt shows the command 'C:\>secedit /refreshpolicy machine_policy /enforce' being entered. Below the command, the output is displayed: 'Group policy propagation from the domain has been initiated for this computer. It may take a few minutes for the propagation to complete and the new policy to take effect. Please check Application Log for errors, if any.' The prompt ends with 'C:\>'.

2.2 Workgroup

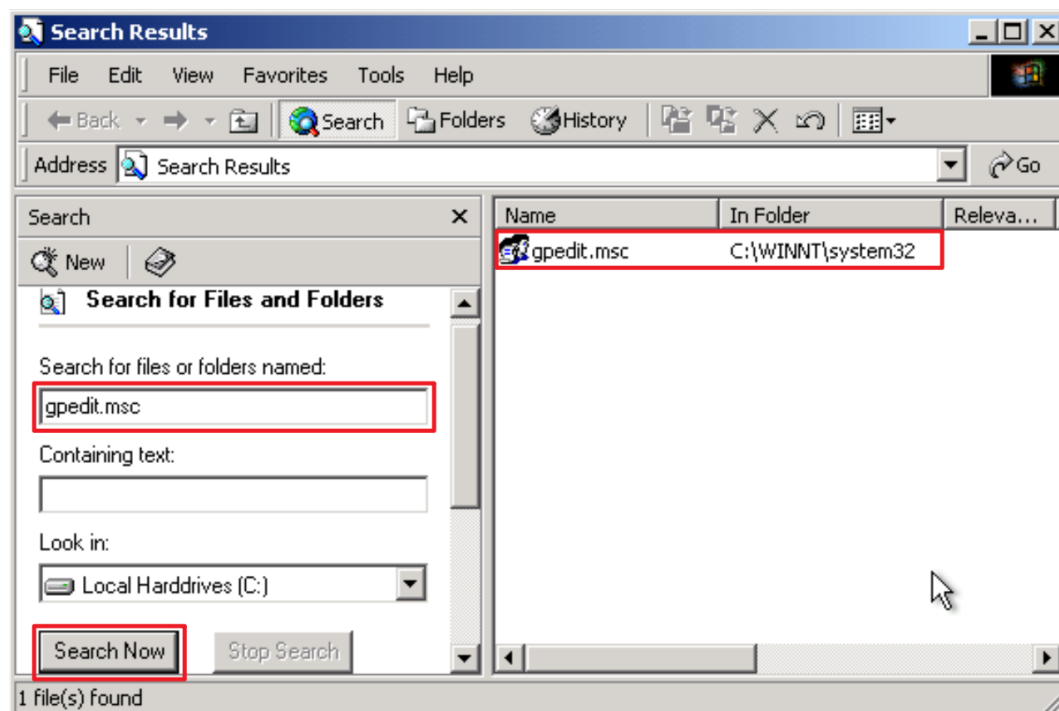
2.2.1 Audit Policy Configuration

(1) Click on “Start” → click “Search” → click on “For Files or Folders”



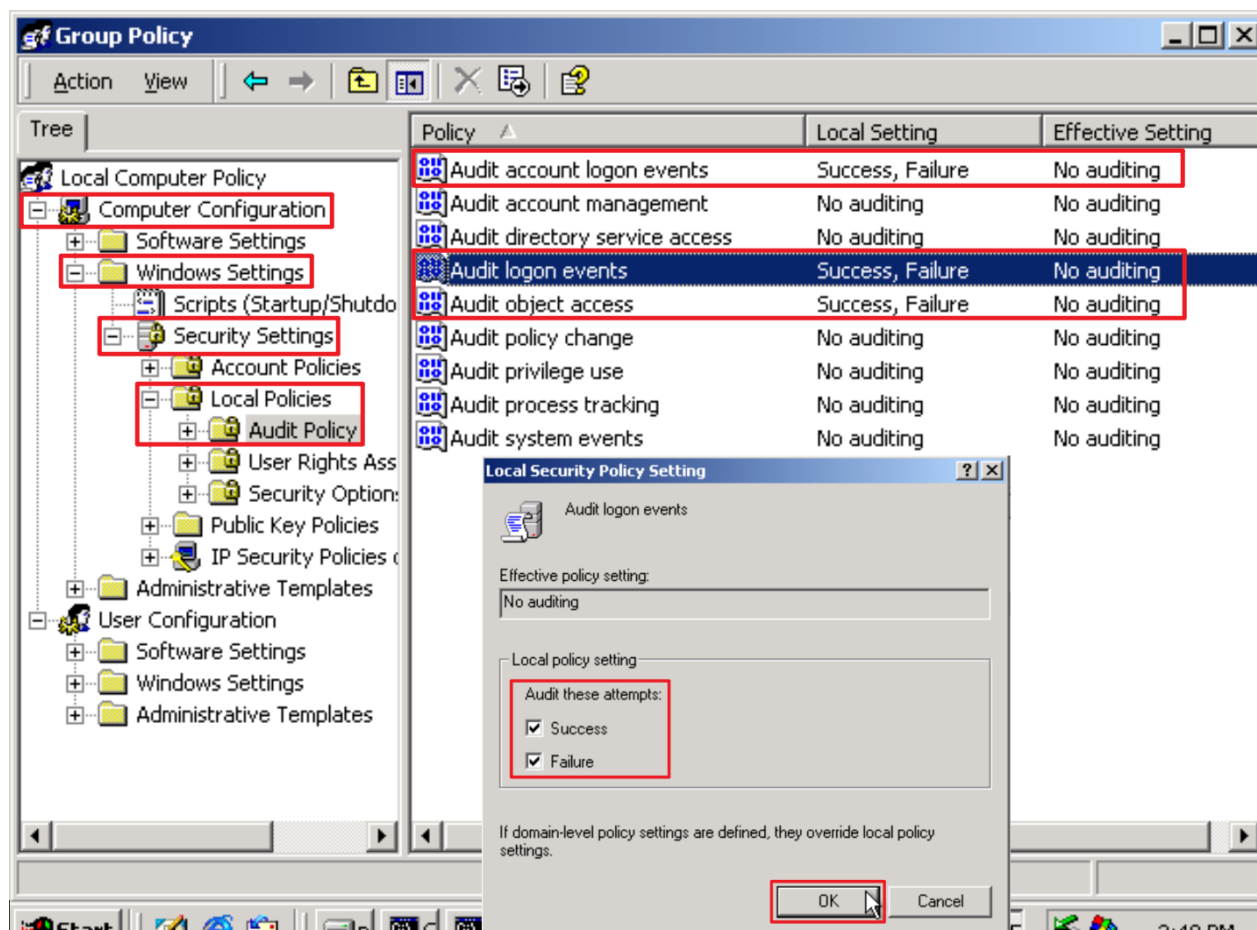
(2) Search for the Group Policy Object Editor

Type **gpedit.msc** → click “Search now” → select “gpedit.”



(3) 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 logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”

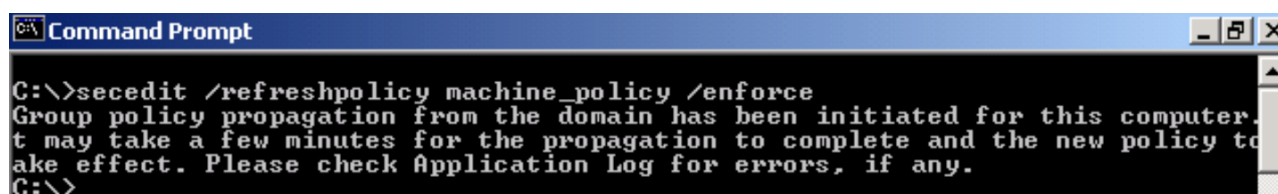


(4) On Windows File server, open “Command Prompt.”



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

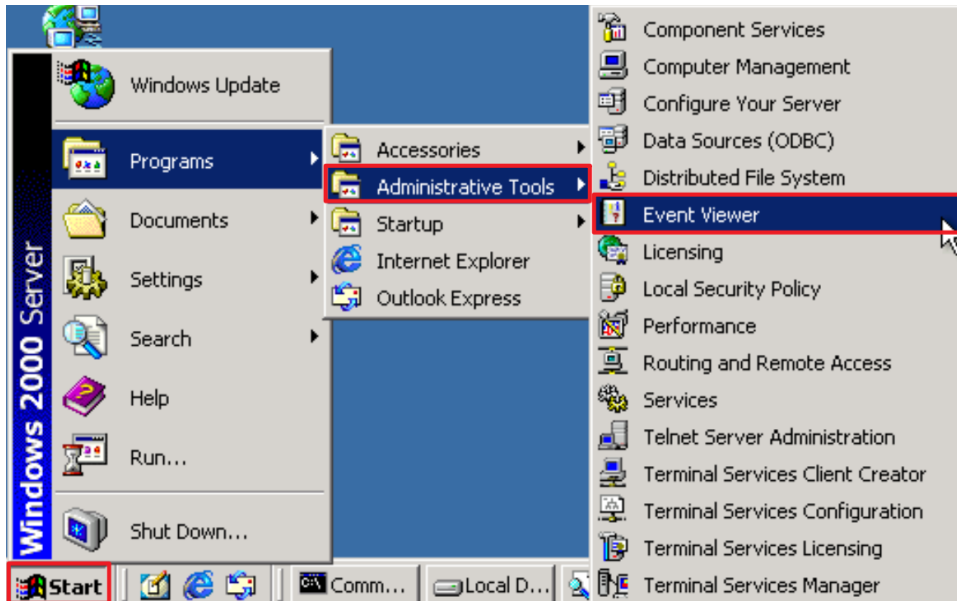
```
C:\> secedit /refreshpolicy machine_policy /enforce
```



2.2.2 Event Log Settings

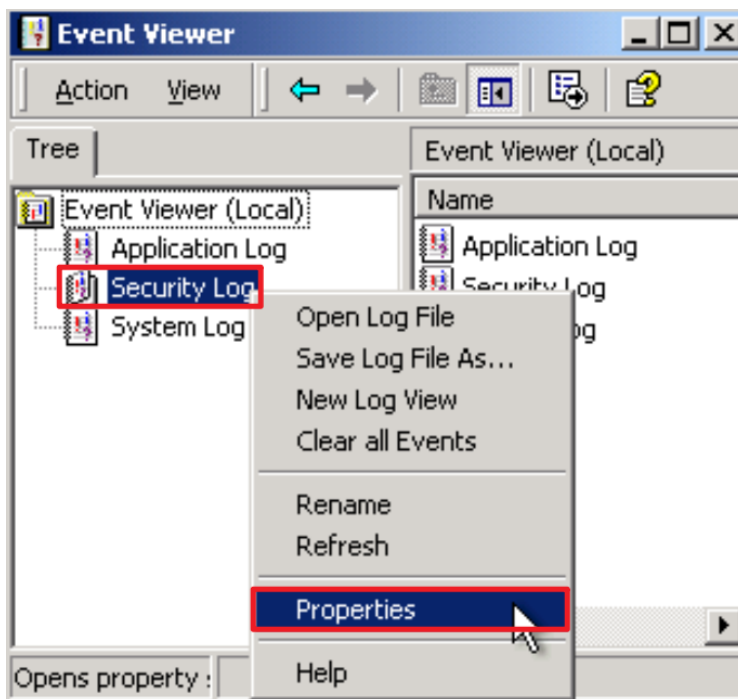
(1) Search for “Event Viewer”

Click “Start” → select “Administrative Tools” → “Event Viewer.”



(2) Edit Security Log

Right-click “Security” and select “Properties.”

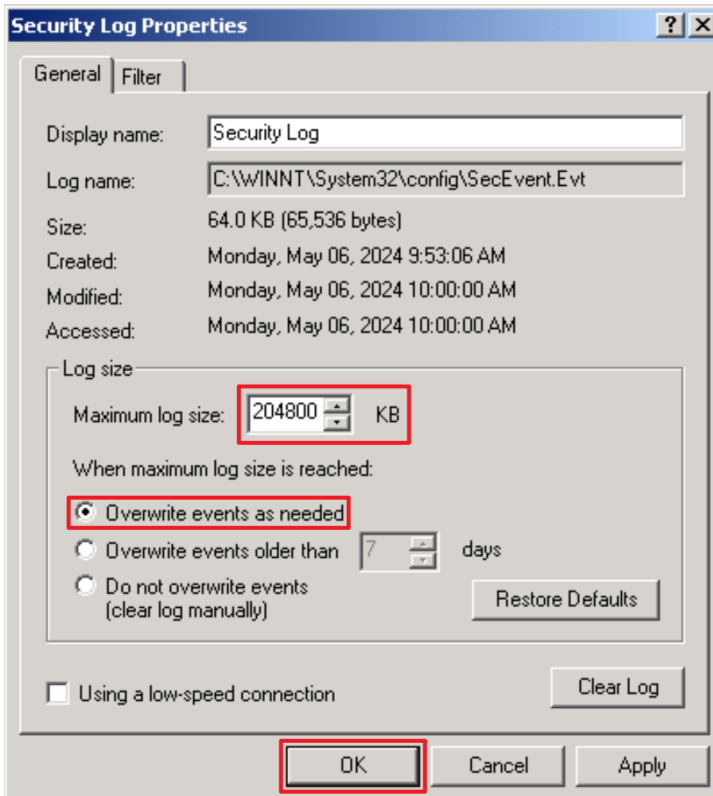


(3) Configure Security Log

Enter maximum log file size: 204800 KB

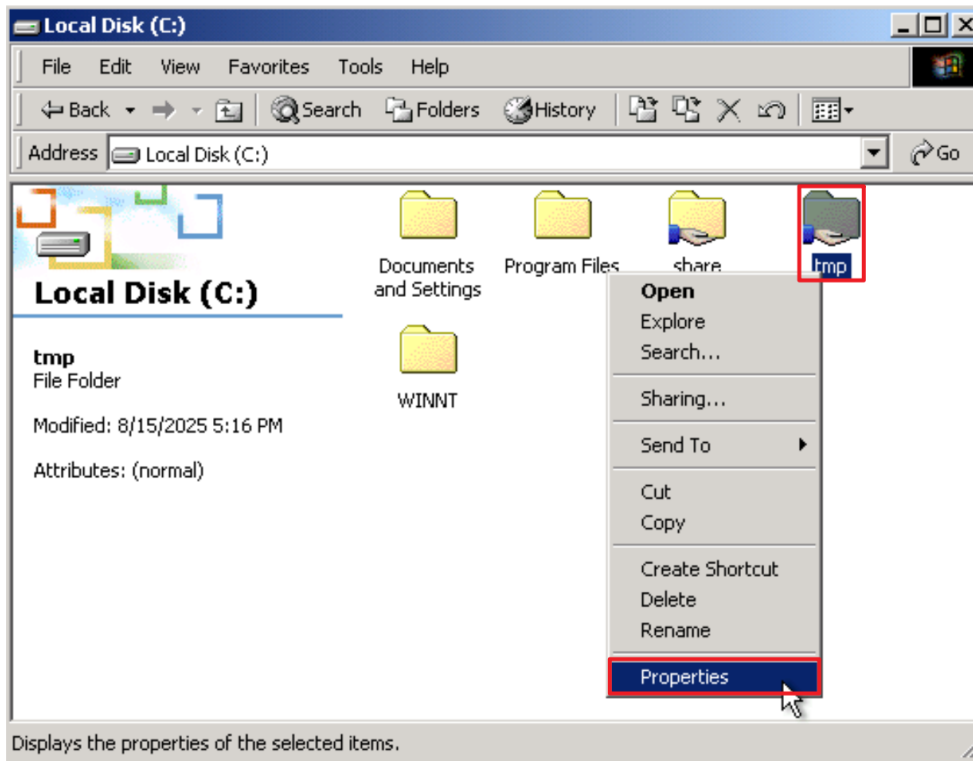
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed” → click “OK.”

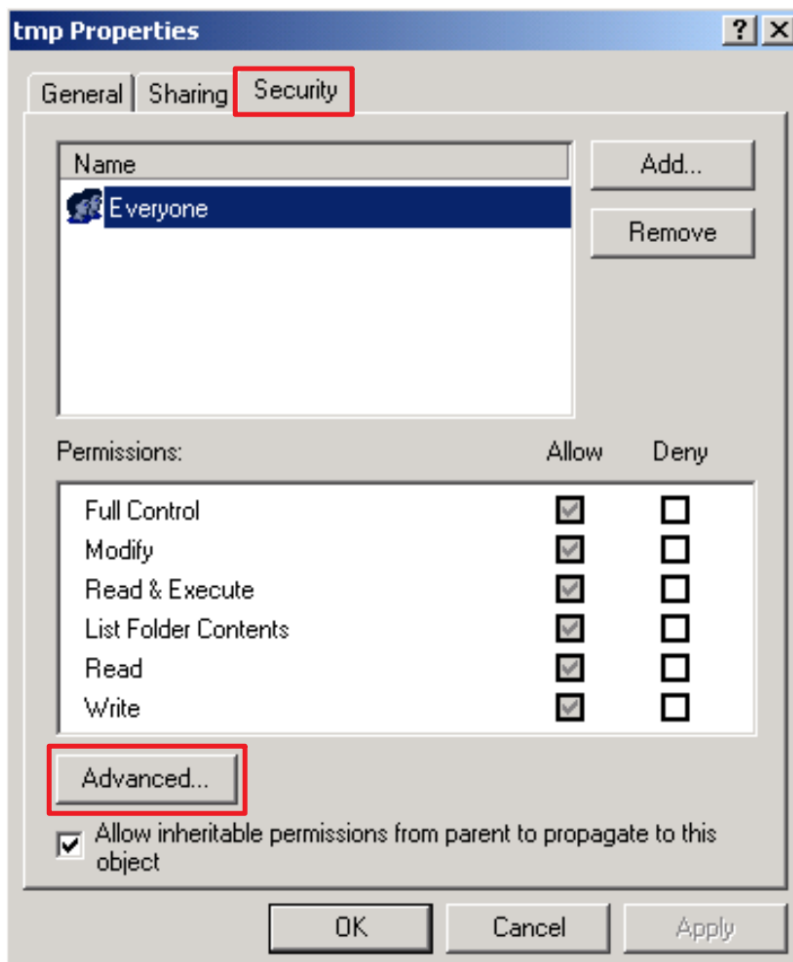


2.3 Folder Audit Configuration

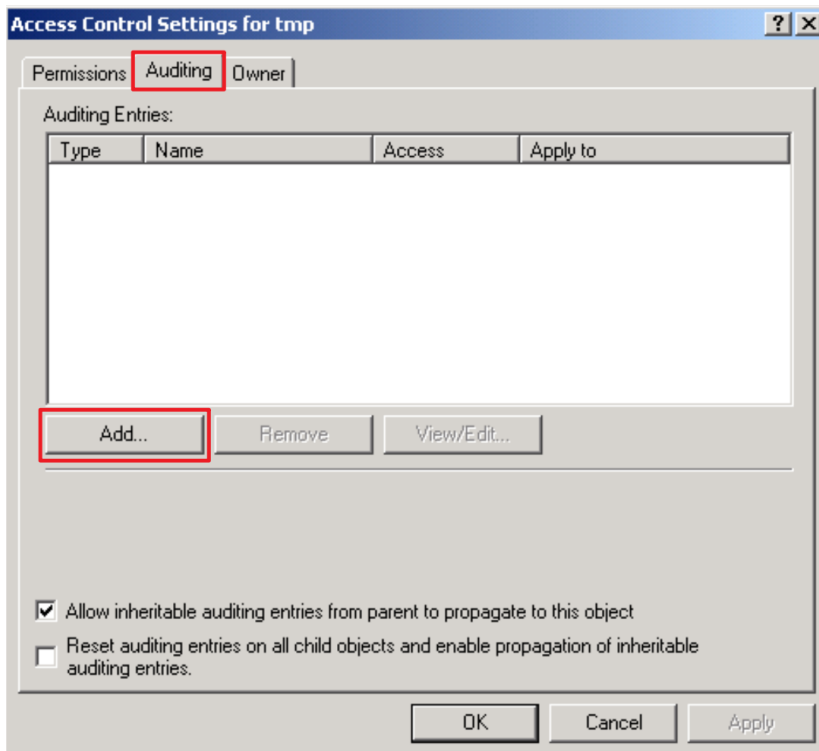
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



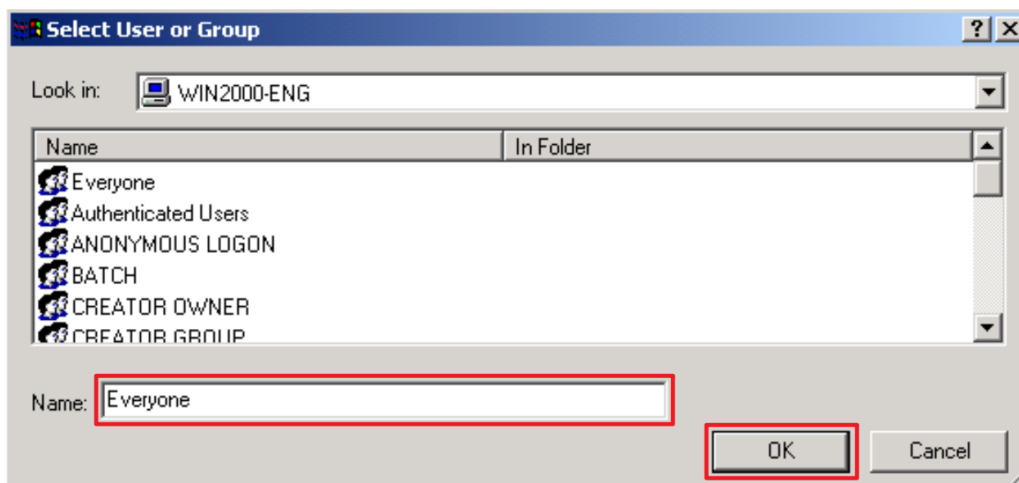
(2) Go to the “Security” tab → click “Advanced.”



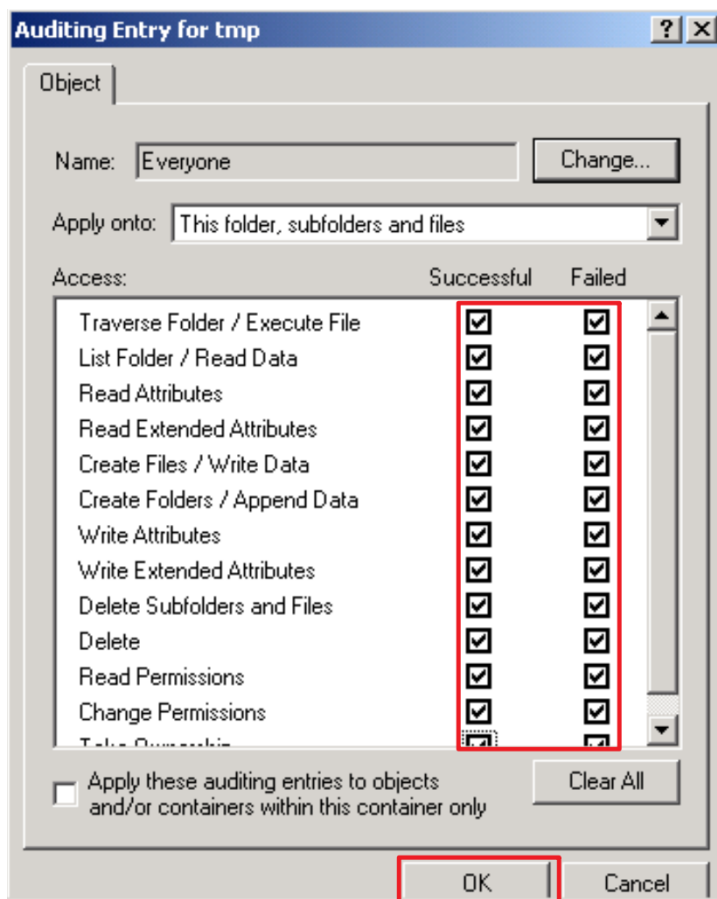
(3) Open the “Auditing” tab → click “Add.”



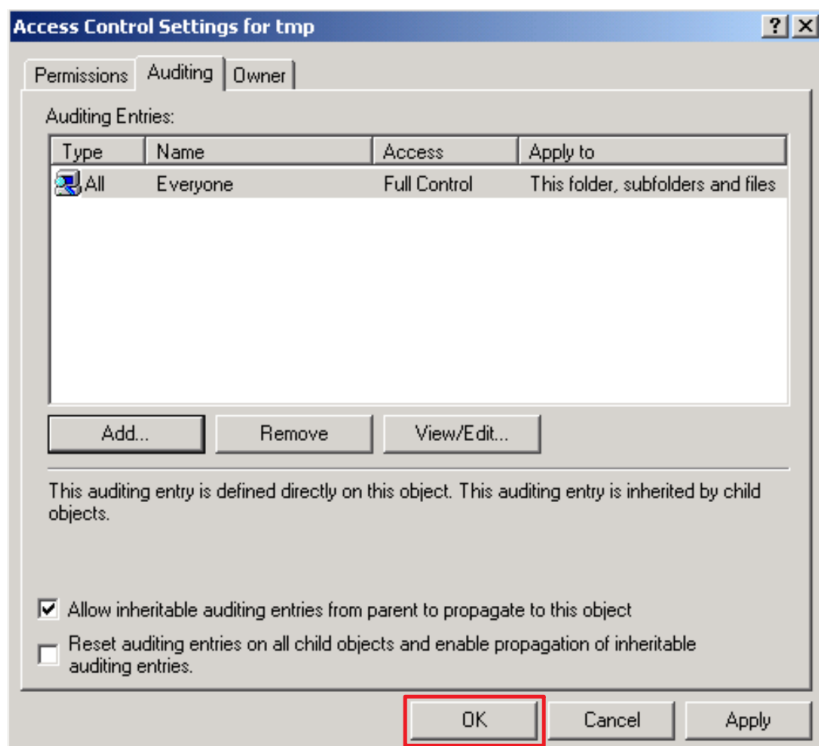
(4) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



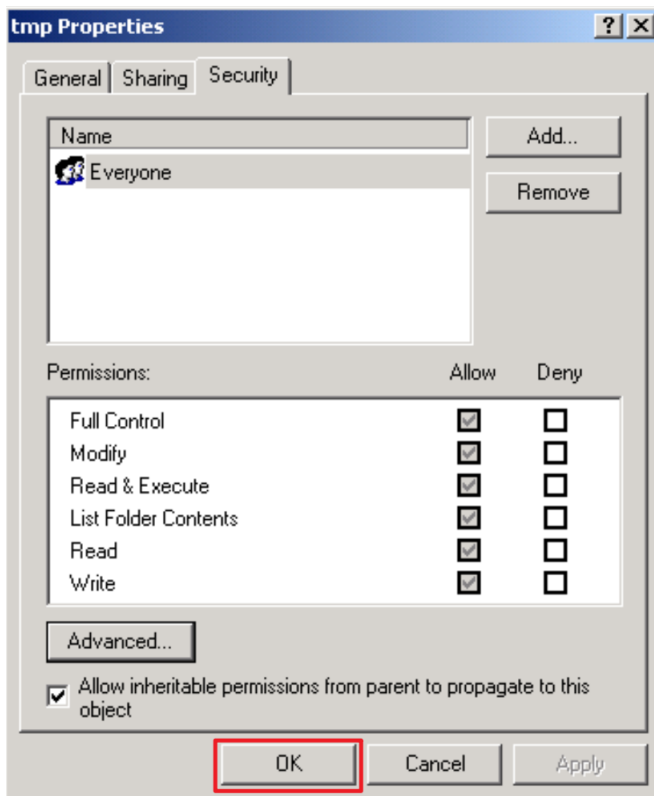
(5) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



(6) Confirm that the auditing entries shows “Everyone” → click “OK.”



(7) Click “OK” again to confirm and close.



3. Windows Server 2003

3.1 Domain

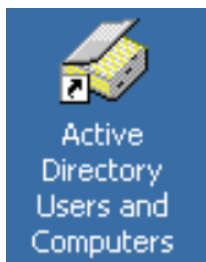
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

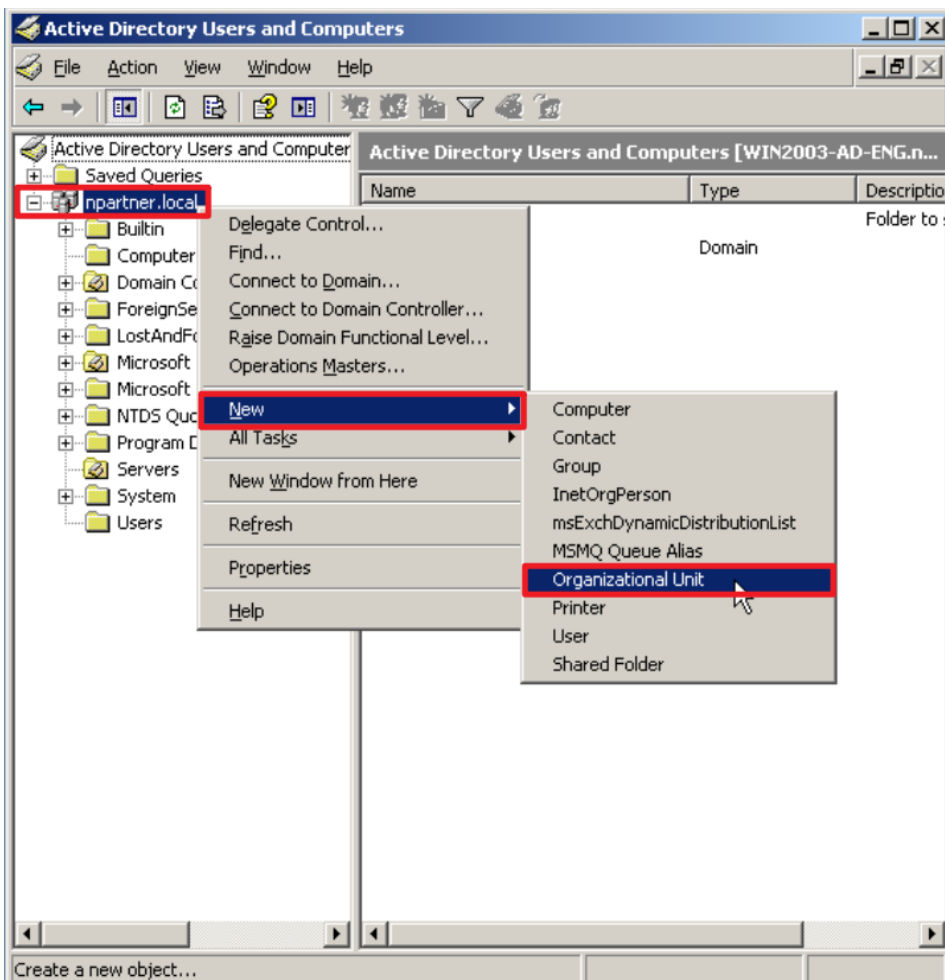
3.1.1 Organizational Unit (OU) Configuration

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



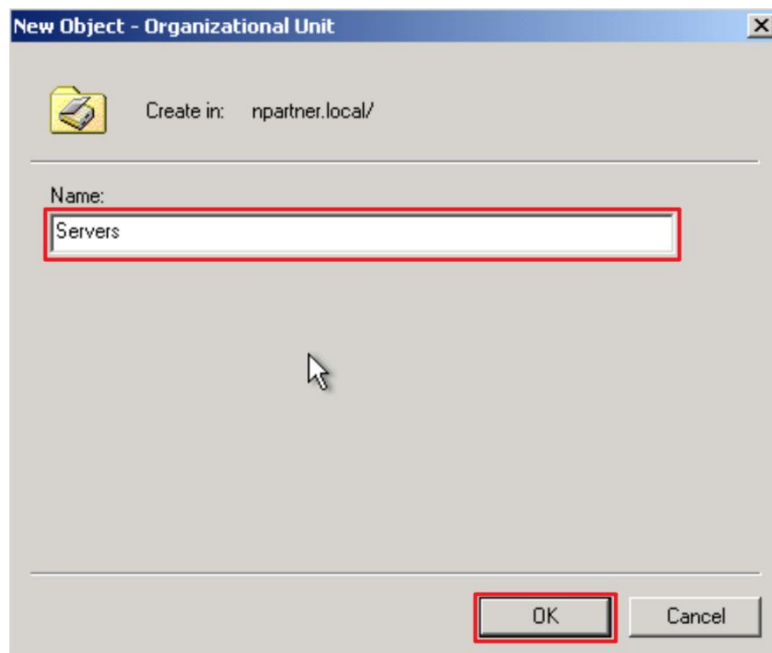
(2) Add an Organizational Unit

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



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

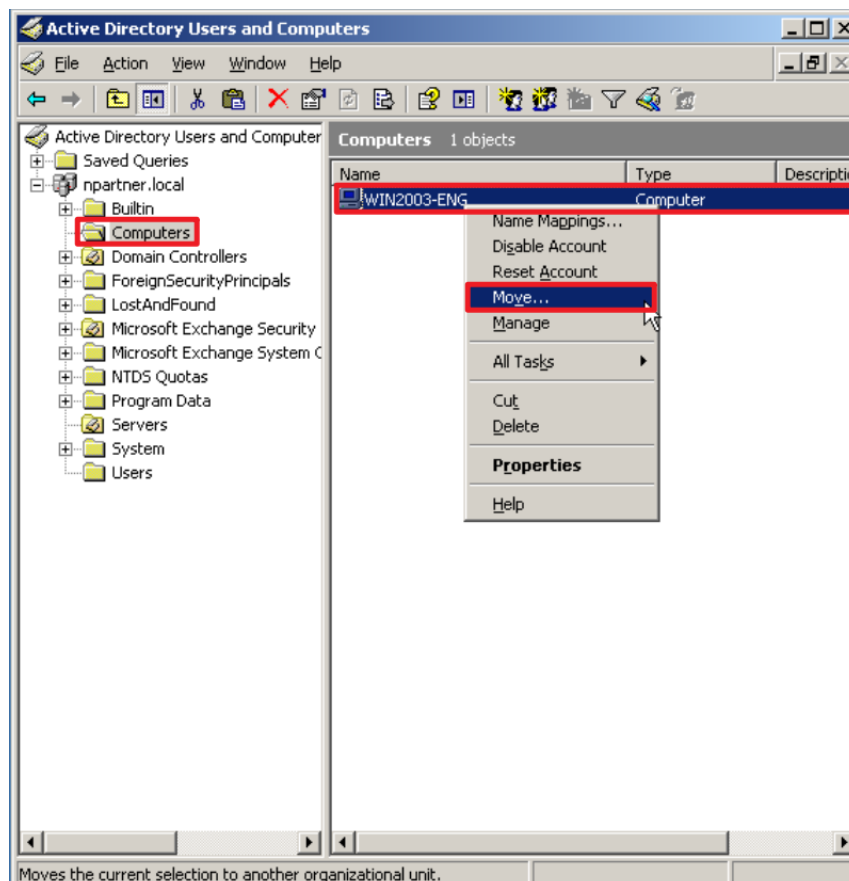
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

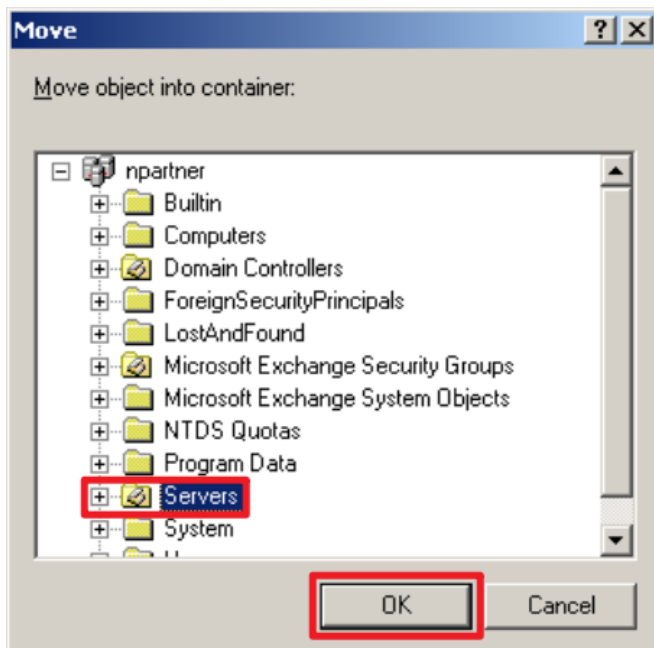
Select the “Computers” organizational unit (OU) → right-click on the “WIN2003-ENG” server.

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



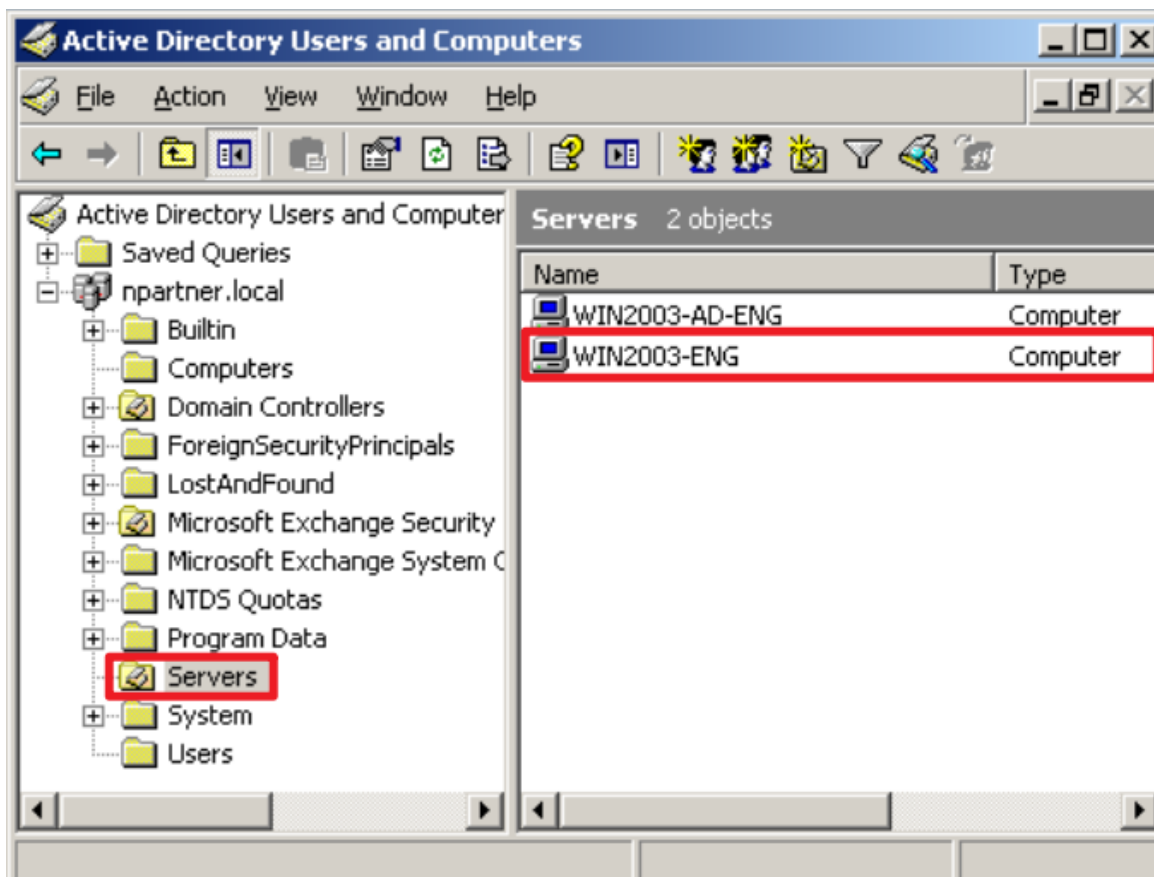
(5) Select your Organizational Unit:

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 “WIN2003-ENG” server has been moved.

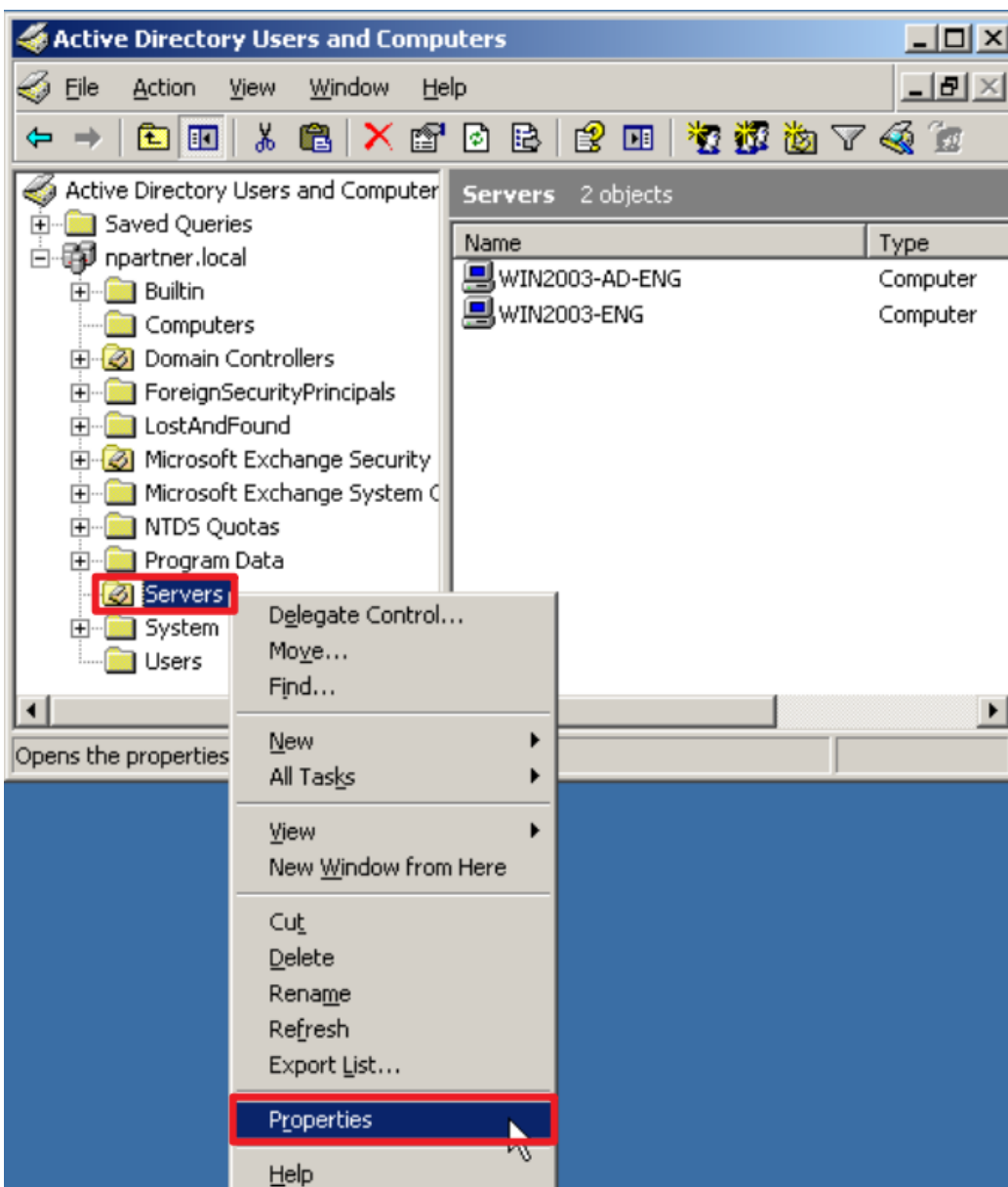


3.1.2 Group Policy Settings

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

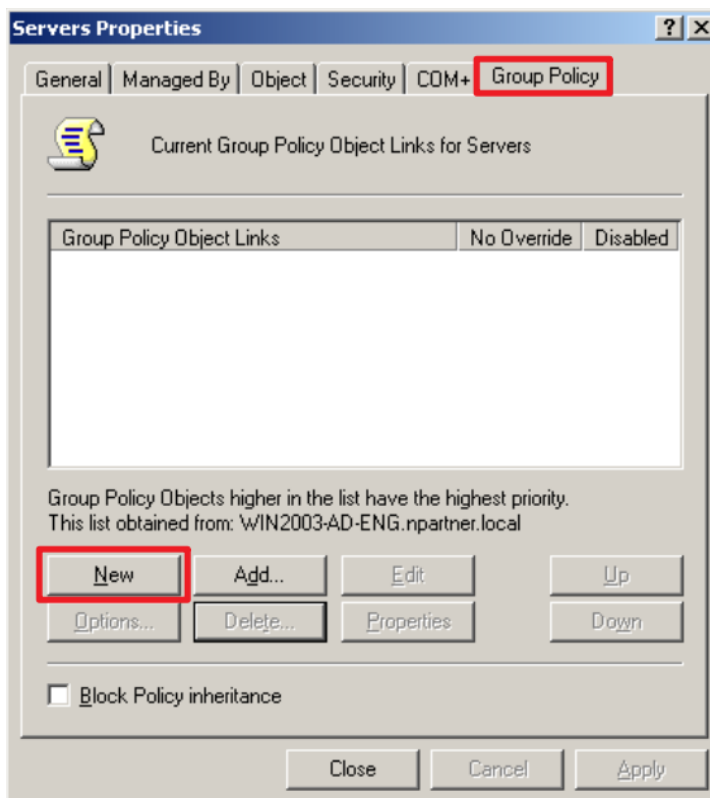


(2) In the “Servers” organizational unit (OU), right-click and select “Properties.”



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

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

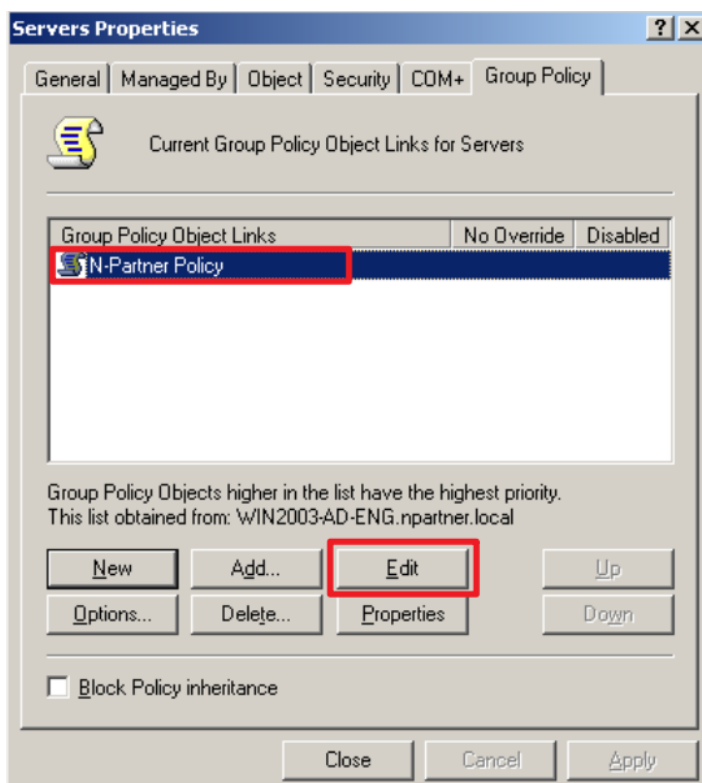


(4) Edit your Group Policy Object

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

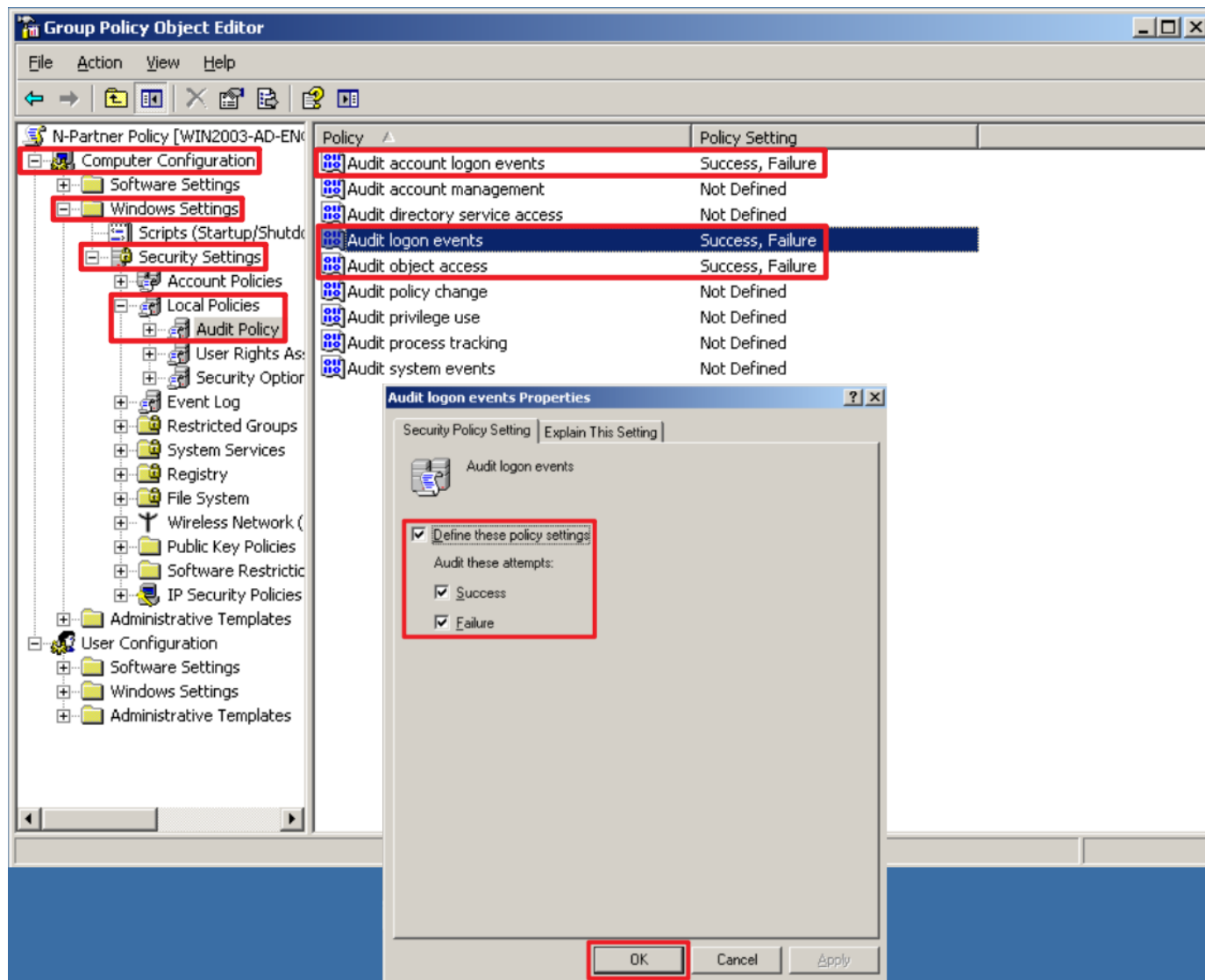
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



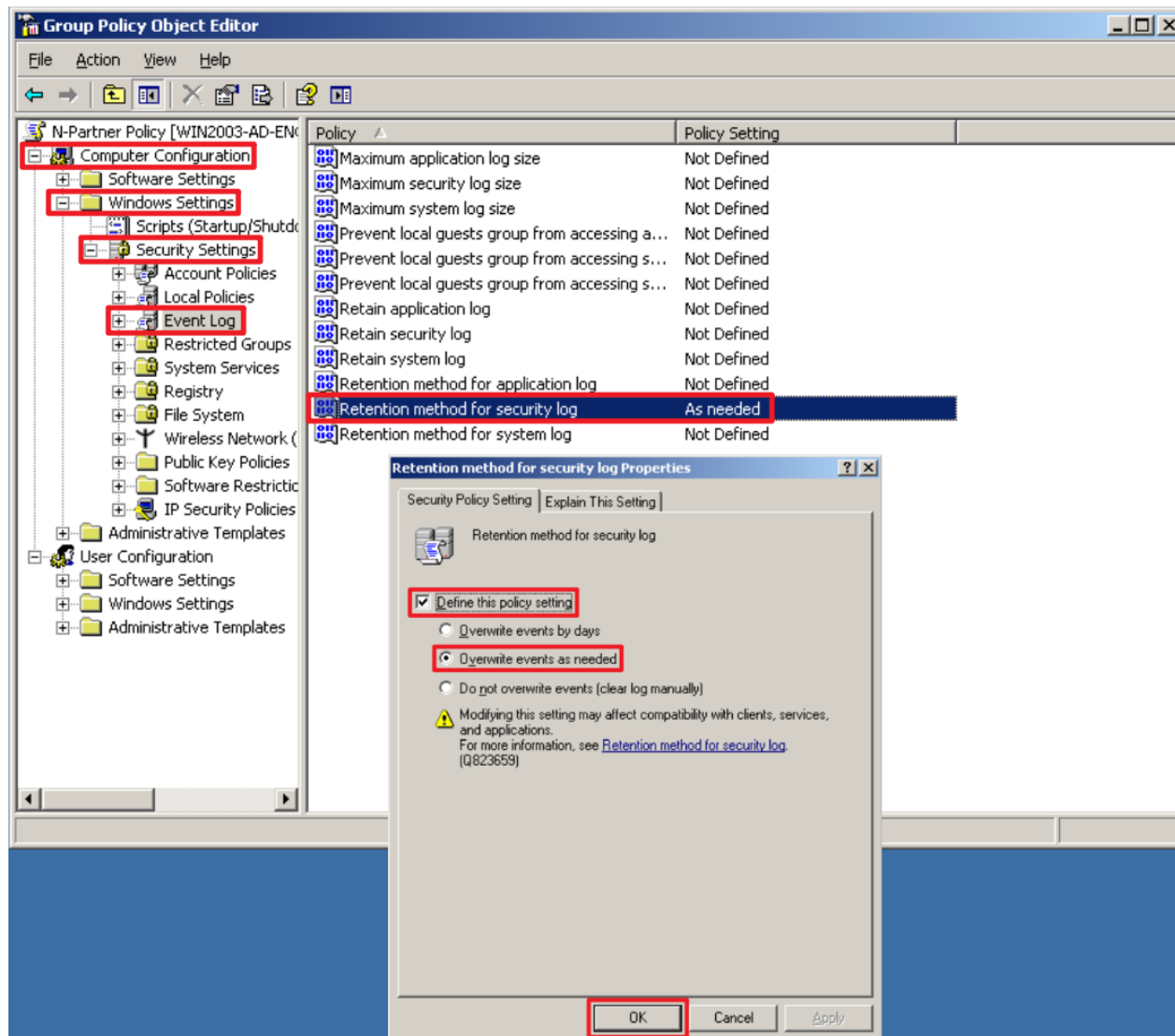
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

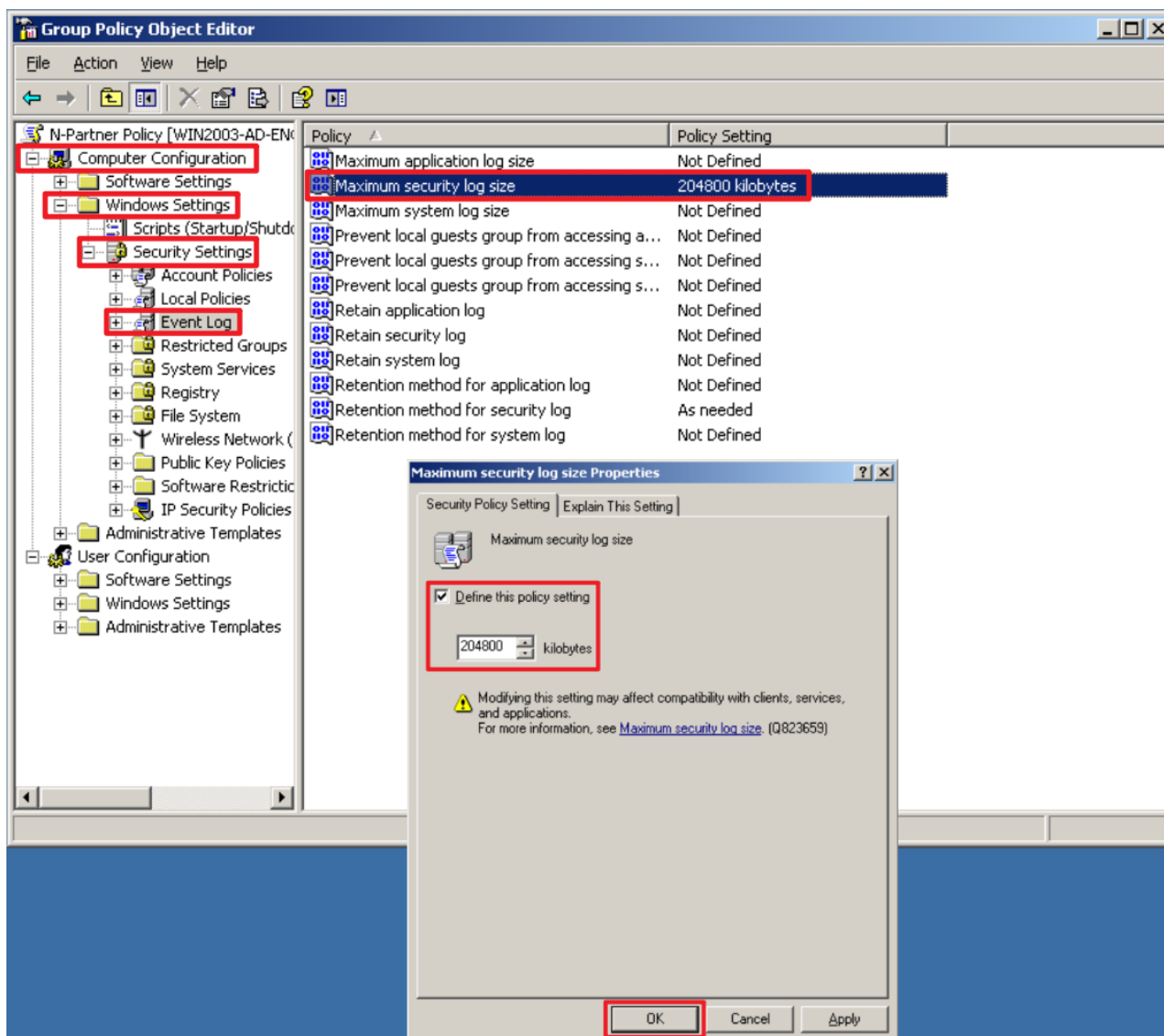
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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:\> gpupdate /force
```

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

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

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

C:\> _
```

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

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

```
C:\> gpresult /v

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Created On 8/18/2025 at 10:52:43 AM

RSOP data for WIN2003-ENG\Administrator on WIN2003-ENG : Logging Mode
-----

OS Type:                Microsoft(R) Windows(R) Server 2003 Enterprise x64
Edition
OS Configuration:      Standalone Server
OS Version:             5.2.3790
Terminal Server Mode:   Remote Administration
Site Name:              N/A
Roaming Profile:
Local Profile:          C:\Documents and Settings\Administrator
Connected over a slow link?: Yes

COMPUTER SETTINGS
-----

Last time Group Policy was applied: 8/18/2025 at 10:52:37 AM
Group Policy was applied from:    WIN2003-AD-ENG.npartner.local
Group Policy slow link threshold: 500 kbps
Domain Name:
Domain Type:              WindowsNT 4

Applied Group Policy Objects
-----
Local Group Policy

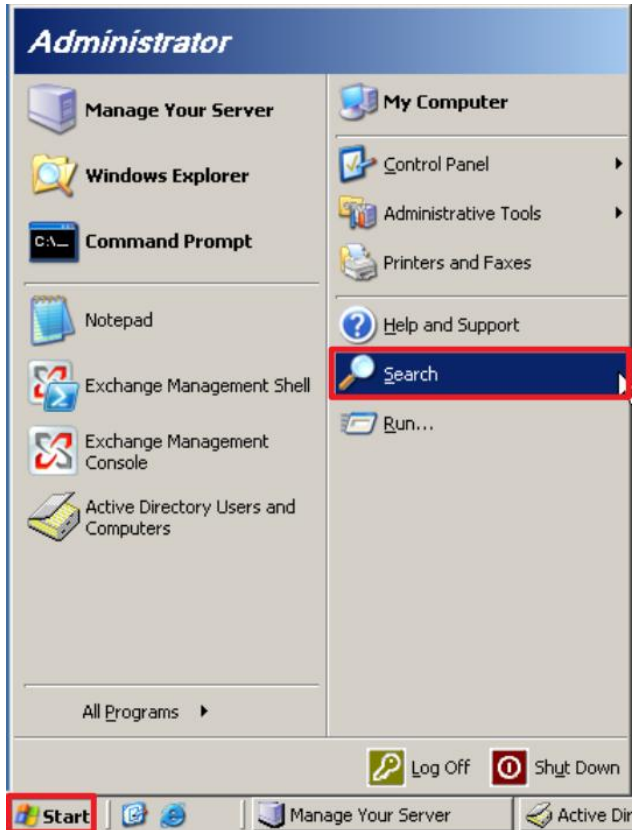
The computer is a part of the following security groups
-----
BUILTIN\Administrators
Everyone
NT AUTHORITY\Authenticated Users

Resultant Set Of Policies for Computer
```

3.2 Workgroup

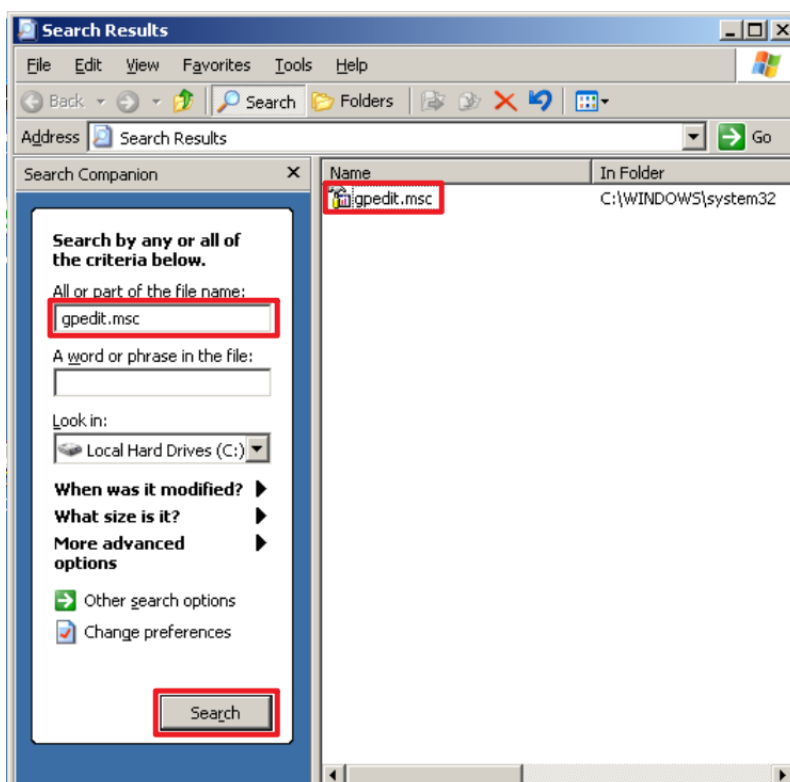
3.2.1 Audit Policy Configuration

(1) Click on “Start” → click “Search.”



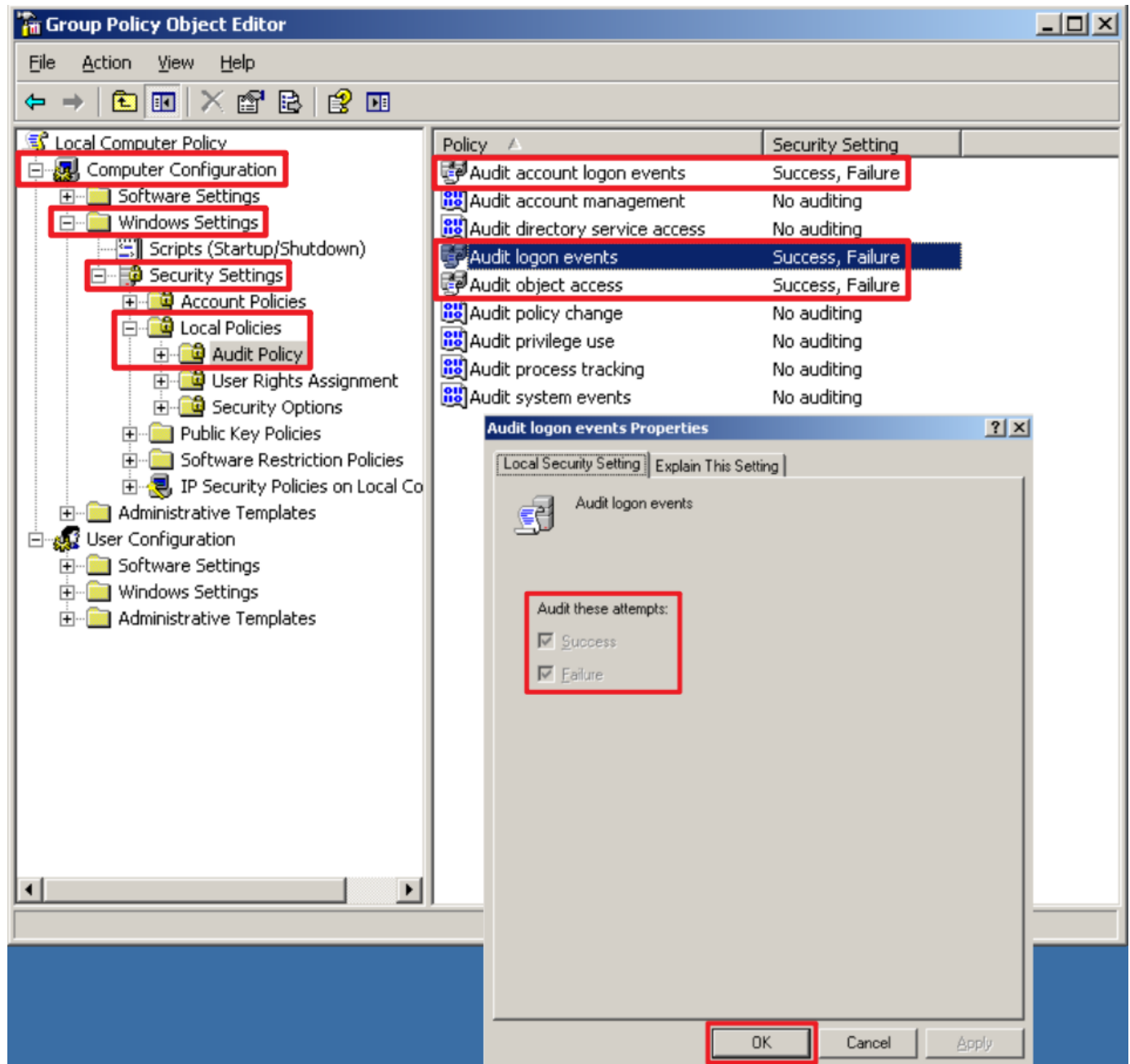
(2) Search for the Group Policy Object Editor

Type **gpedit.msc** → click “Search now” → select “gpedit.”



(3) 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 logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”

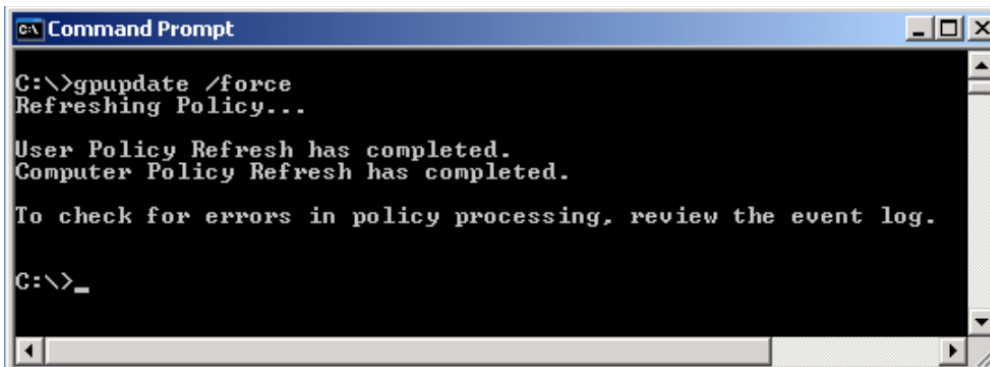


(4) On Windows File server, open “Command Prompt.”



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

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



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

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

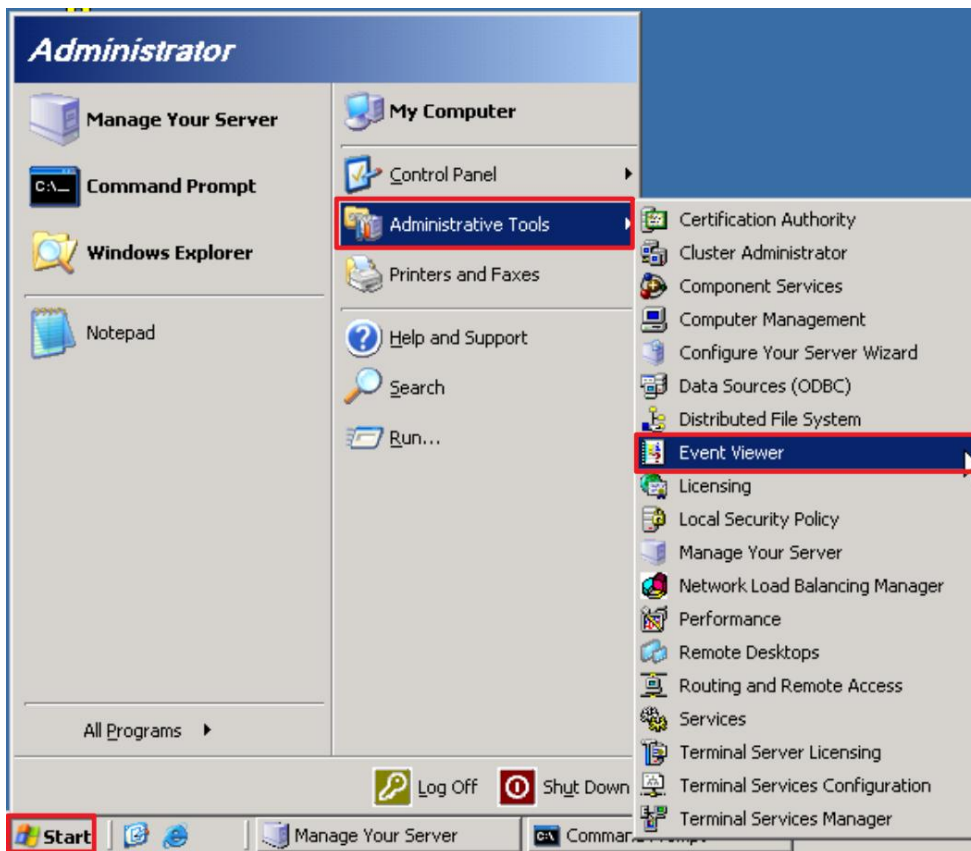
To check for errors in policy processing, review the event log.

C:\>_
```


3.2.2 Event Log Settings

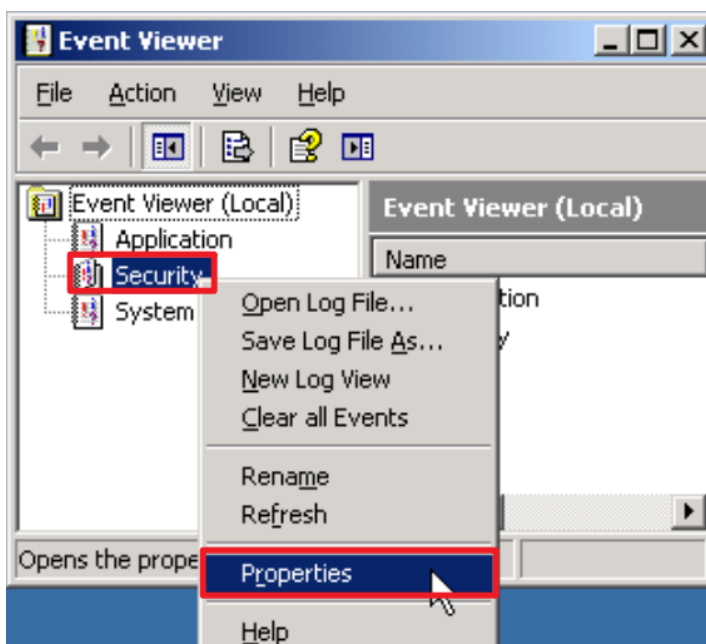
(1) Search for “Event Viewer”

Click “Start” → select “Administrative Tools” → “Event Viewer.”



(2) Edit Security Log

Right-click “Security” and select “Properties.”

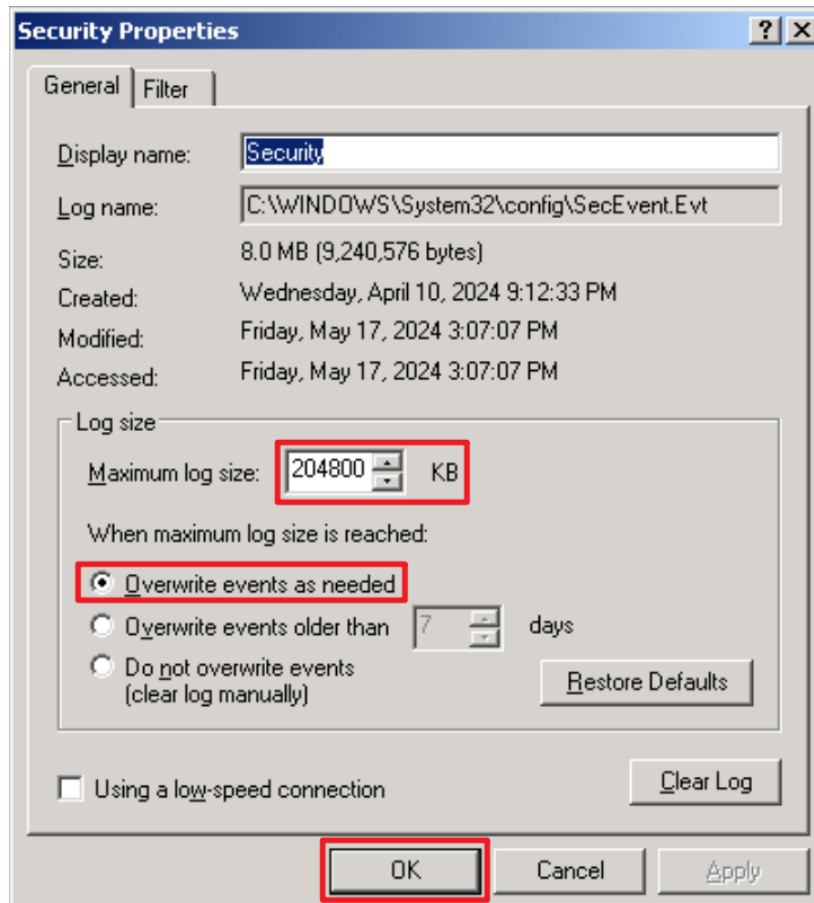


(3) Configure Security Log

Enter maximum log file size: 204800 KB

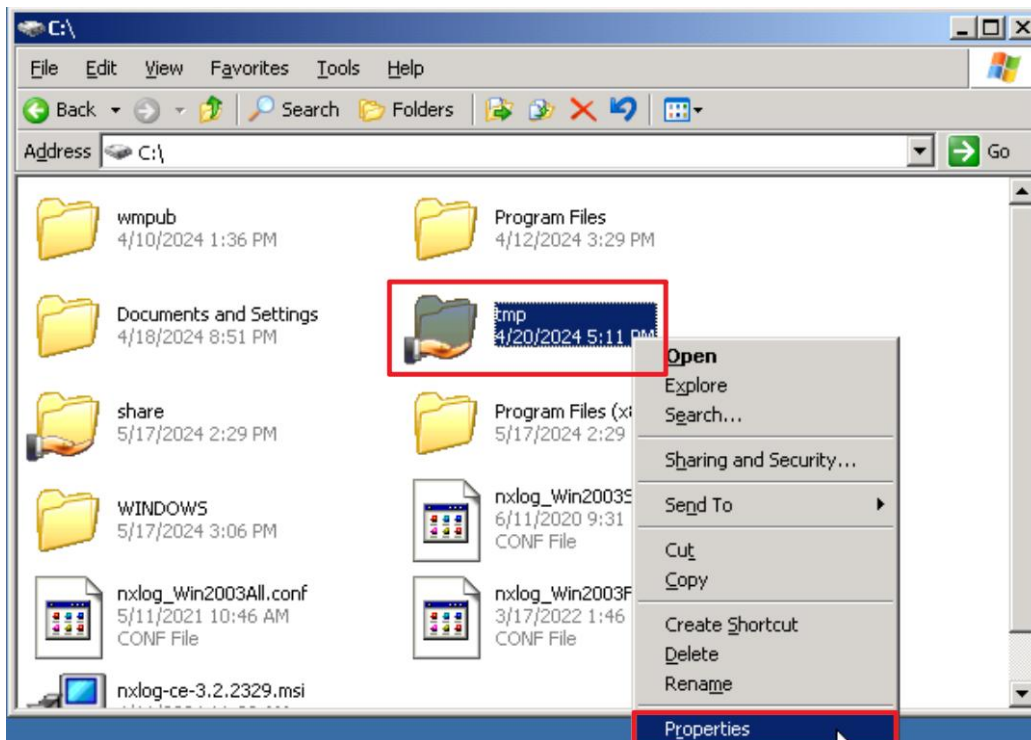
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed” → click “OK.”

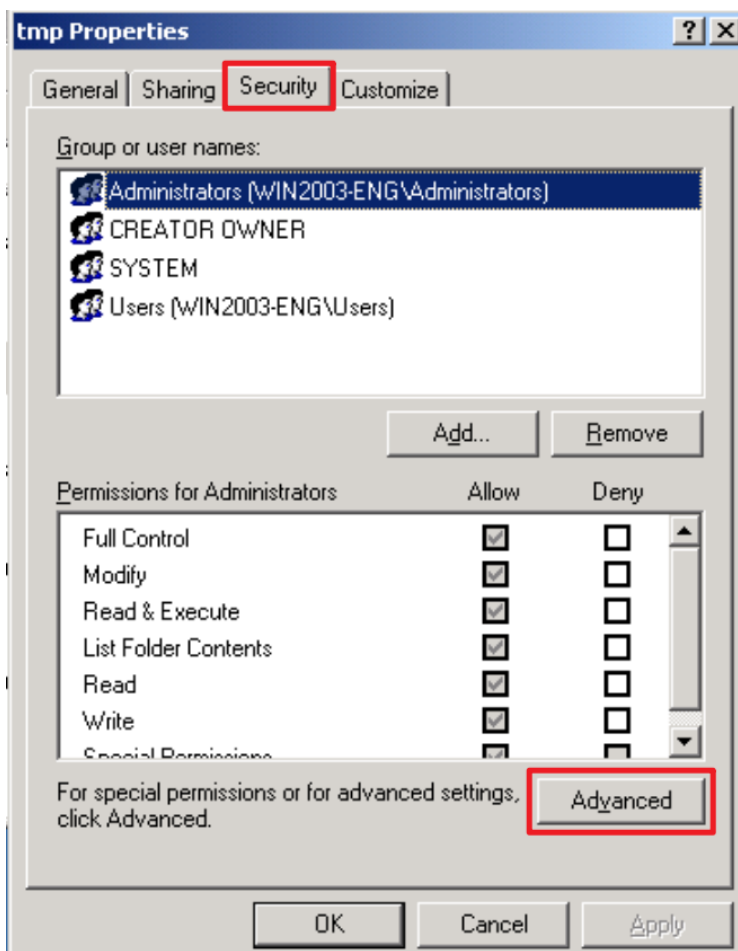


3.3 Folder Audit Configuration

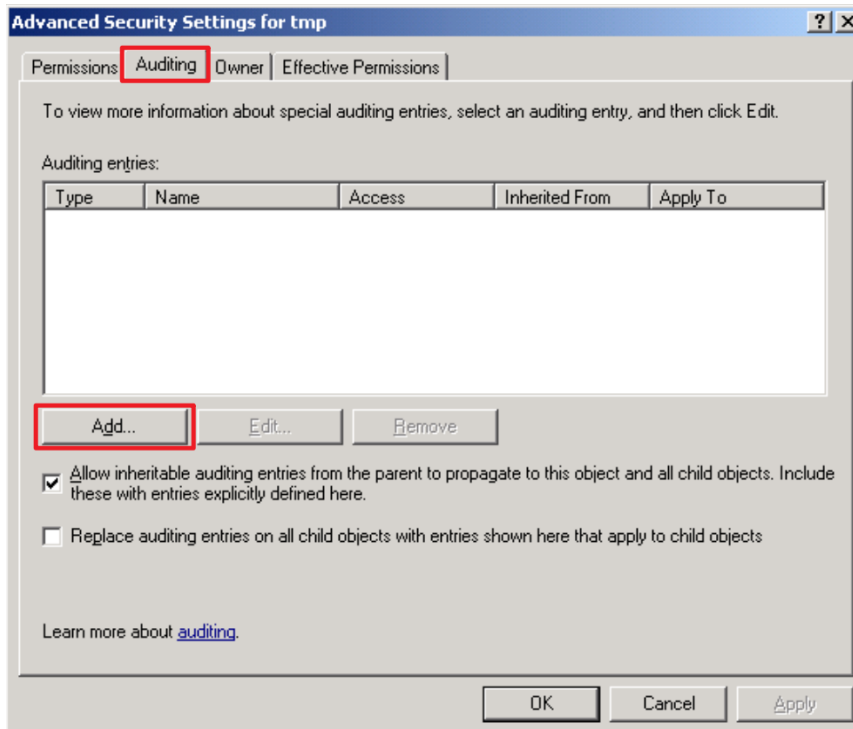
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



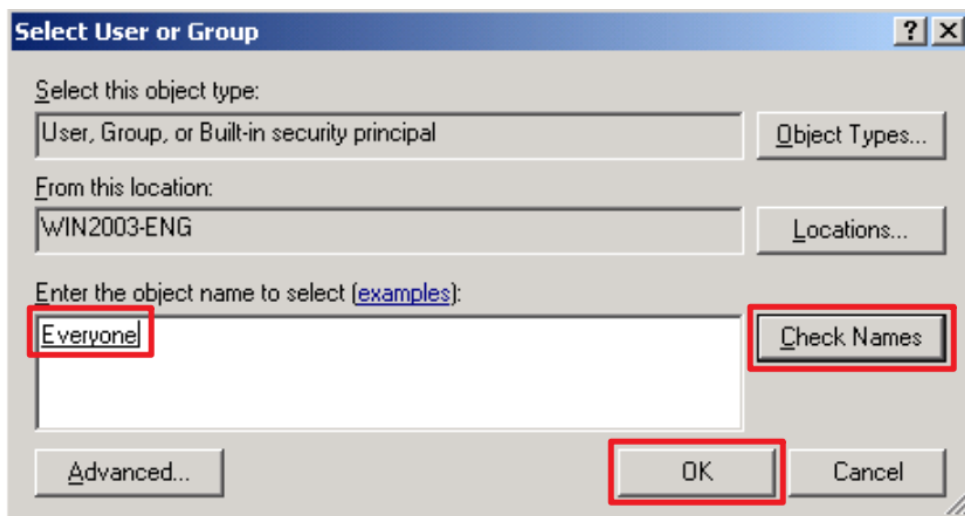
(2) Go to the “Security” tab → click “Advanced.”



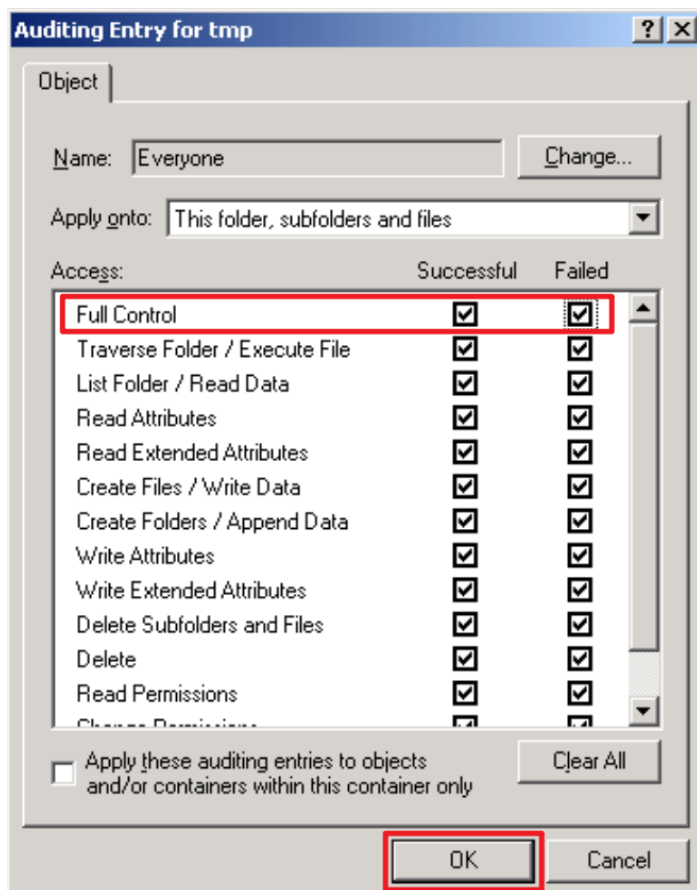
(3) Open the “Auditing” tab → click “Add.”



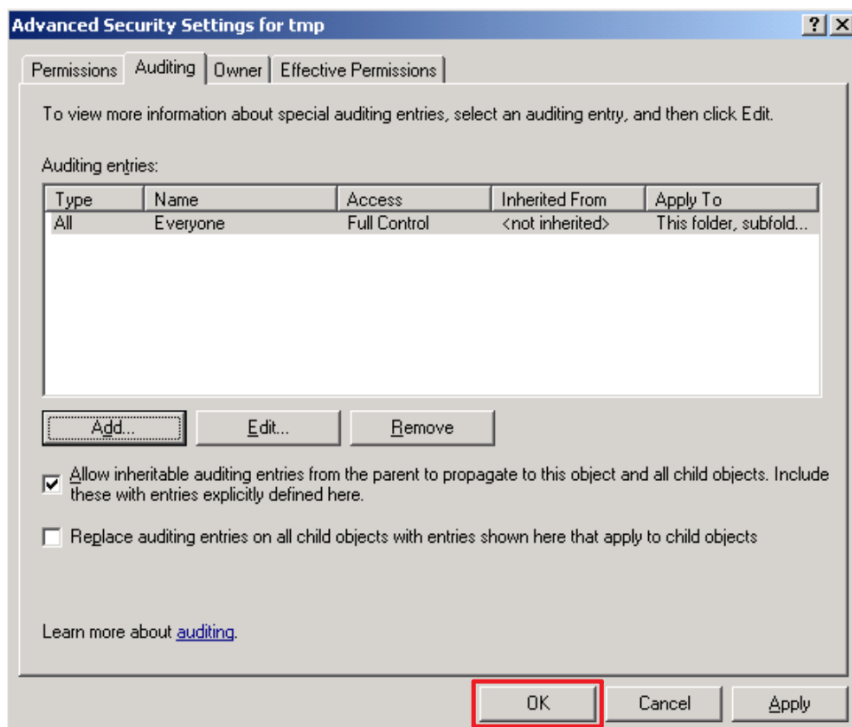
(4) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



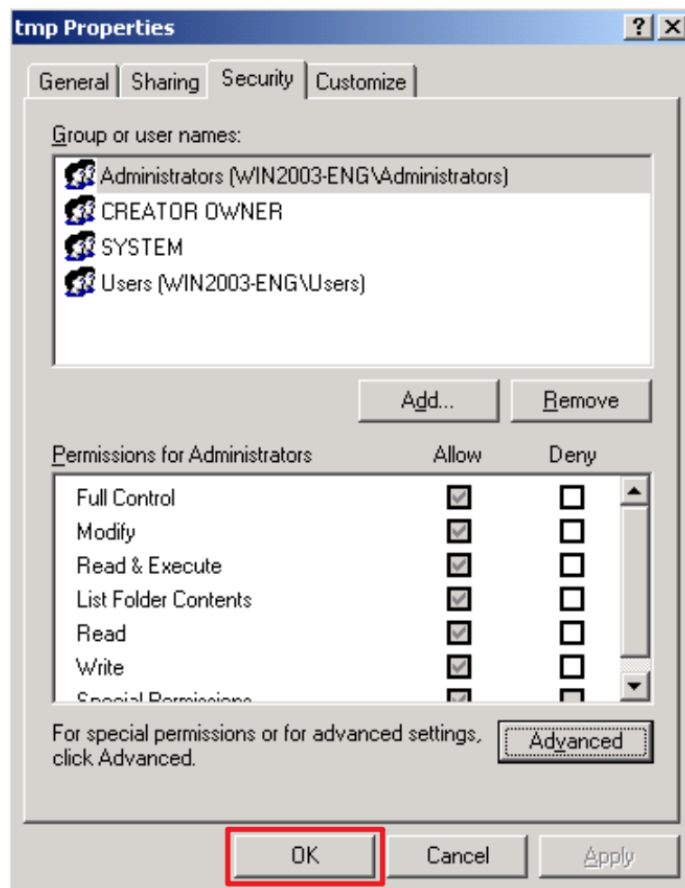
(5) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



(6) Confirm that the auditing entries shows “Everyone” → click “OK.”



(7) Click “OK” again to confirm and close.



4. Windows Server 2008

4.1 Domain

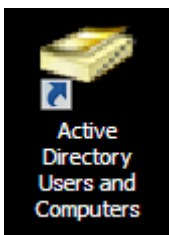
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

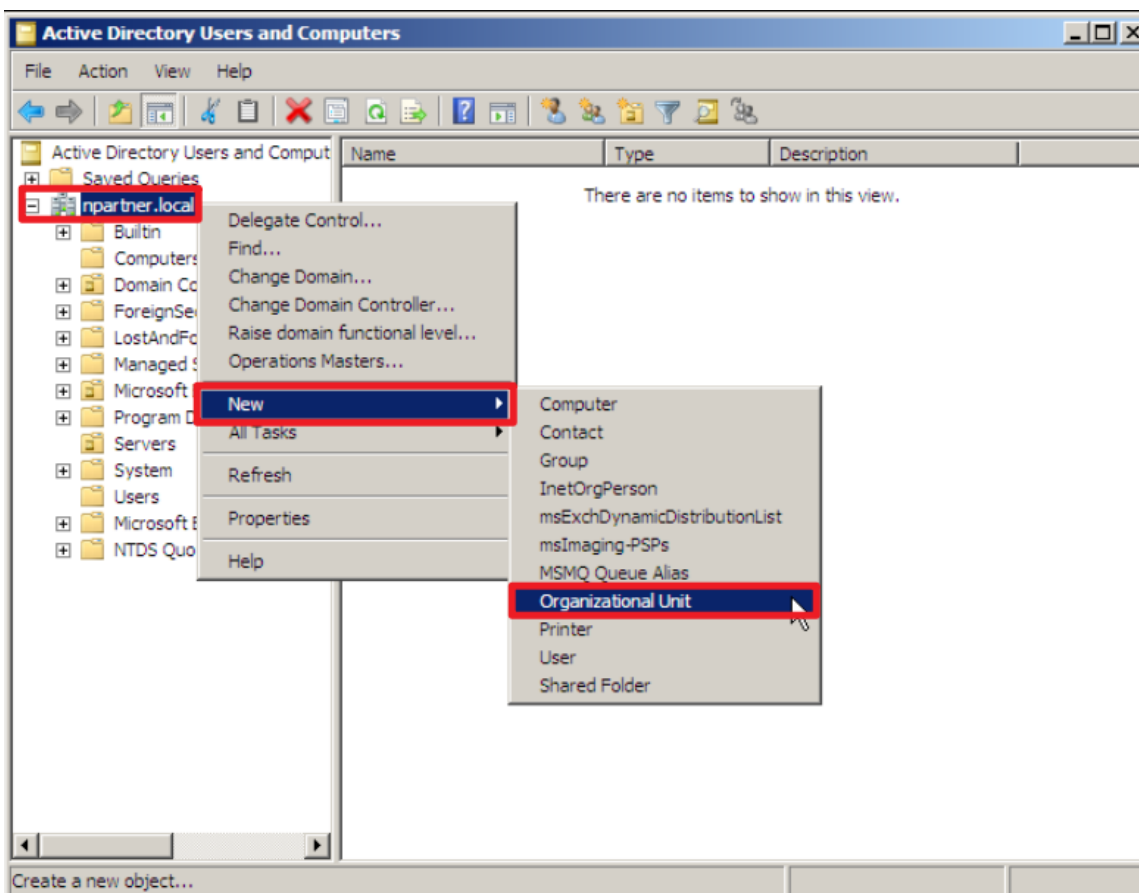
4.1.1 Organizational Unit (OU) Configuration

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



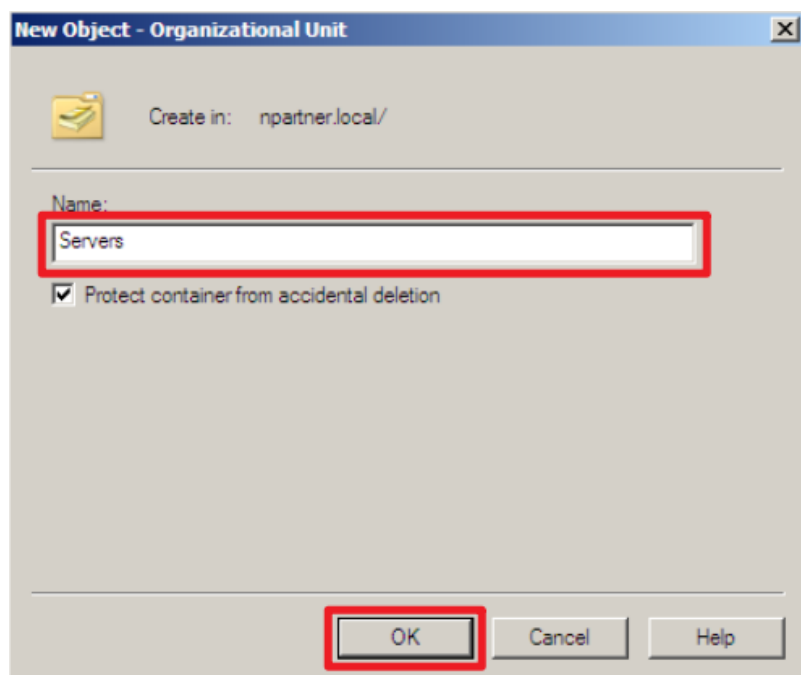
(2) Add an Organizational Unit

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”)

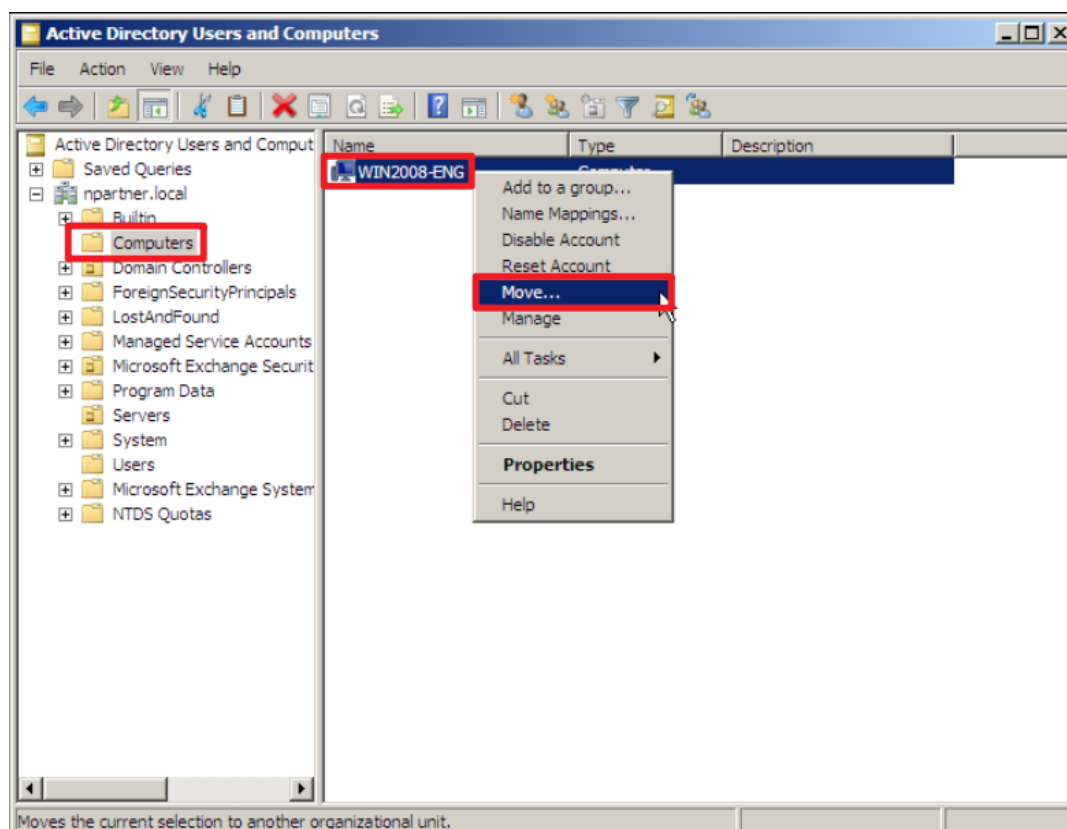
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

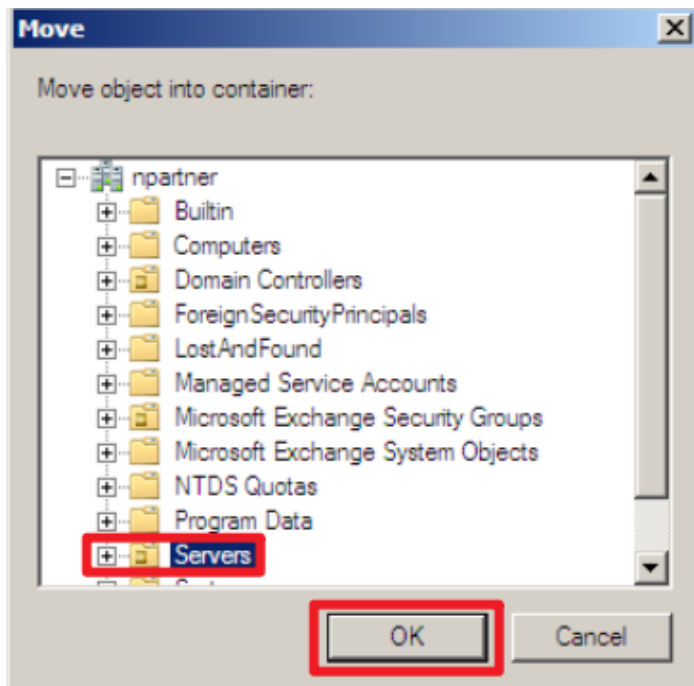
Select the “Computers” organizational unit (OU) → right-click on the “WIN2008-ENG” server.

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



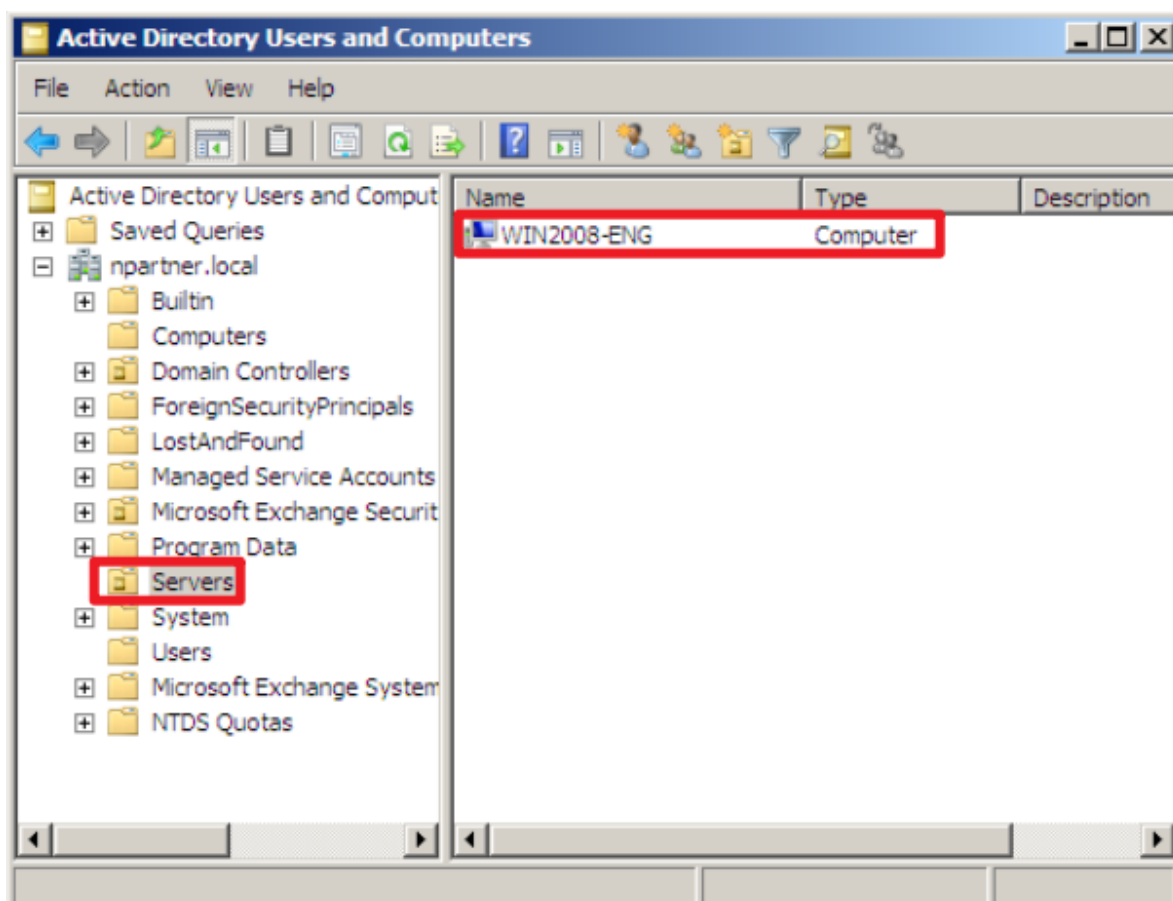
(5) Select your Organizational Unit:

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



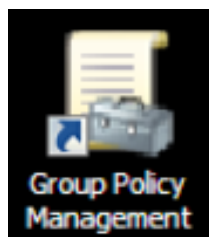
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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

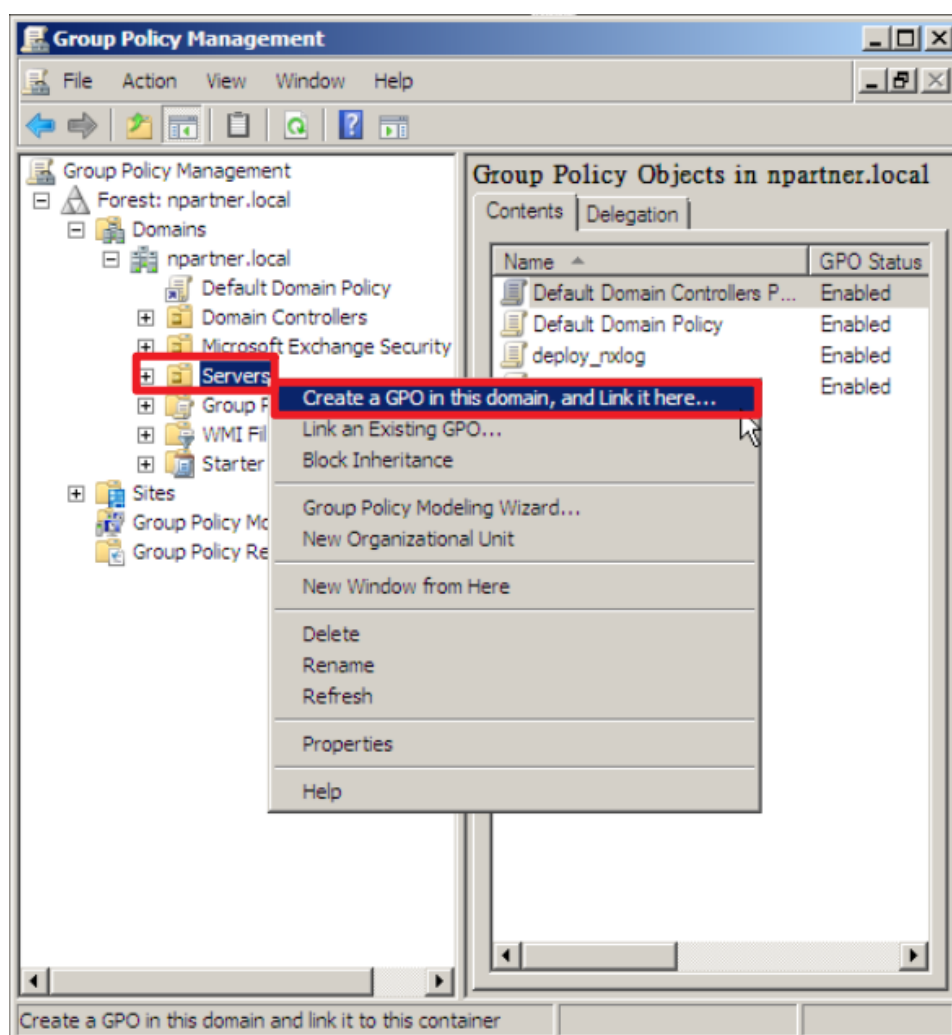


4.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



(2) In the “Servers” organizational unit (OU), right-click and select “Create a GPO in this domain, and Link it here...”

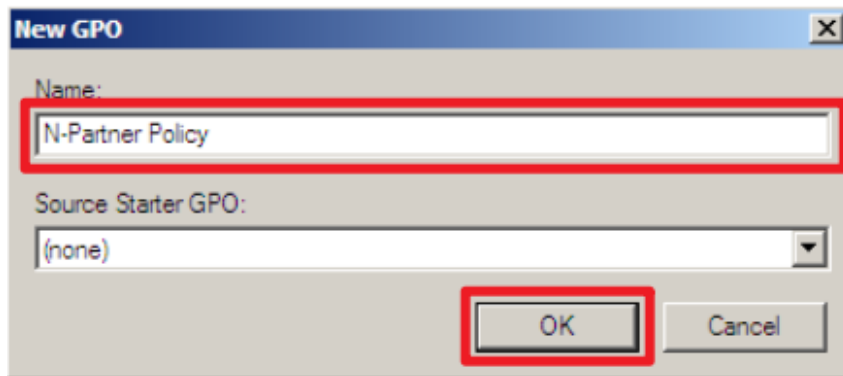


(3) Enter the Group Policy Object (GPO) name

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

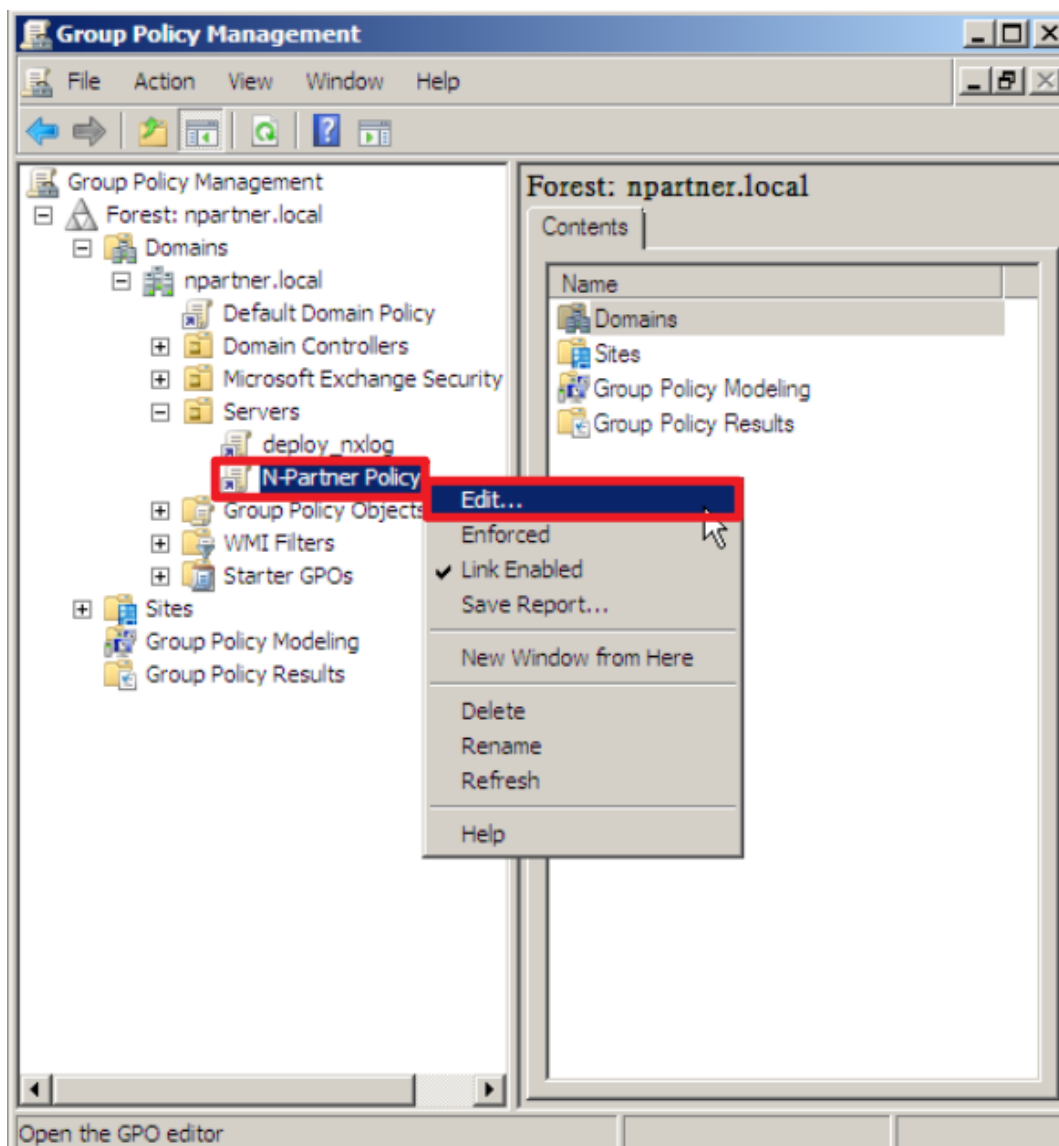
Note: Please create the GPO name according to the actual environment.

→ select “OK.”



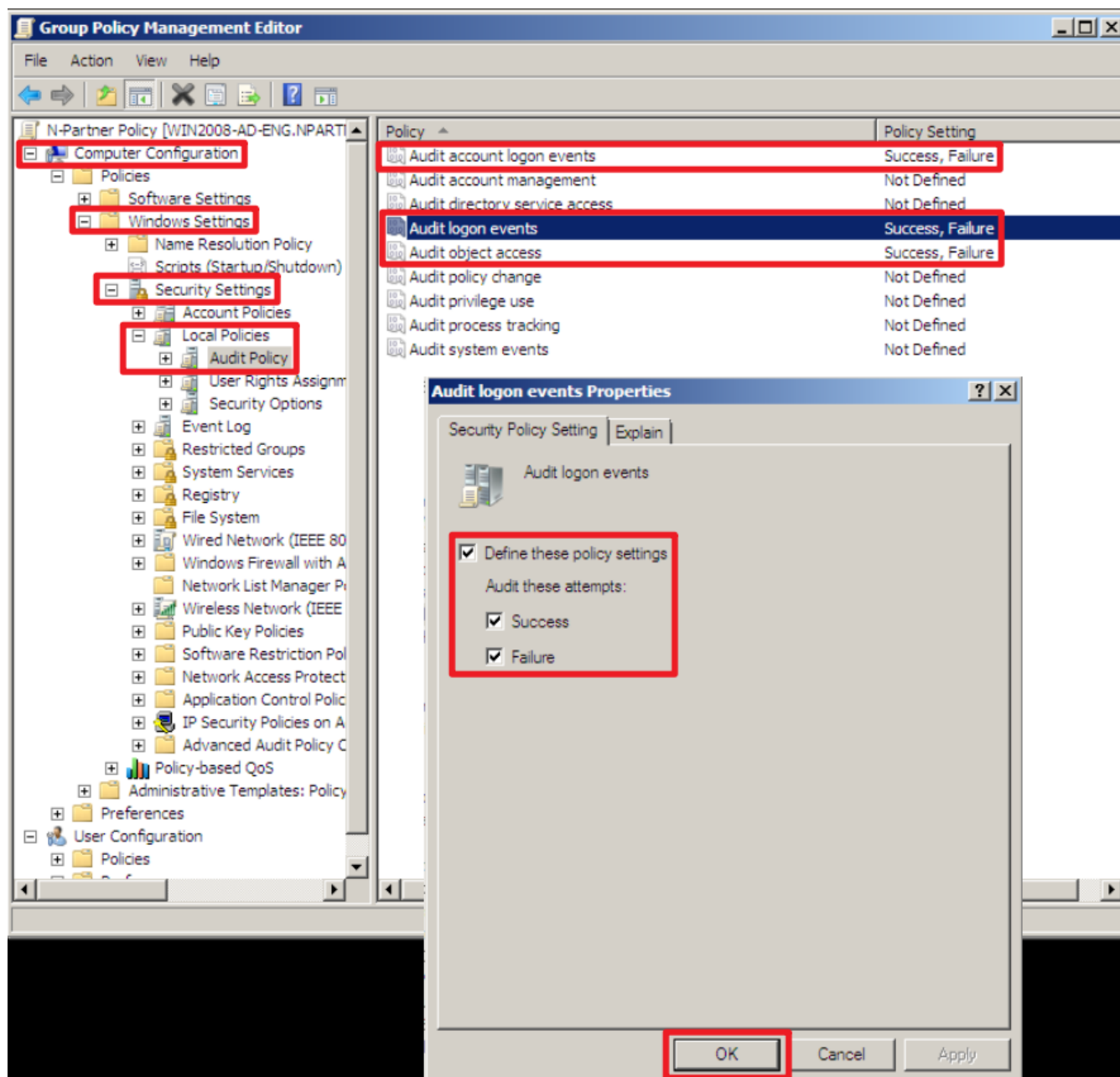
(4) Edit your Group Policy Object

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



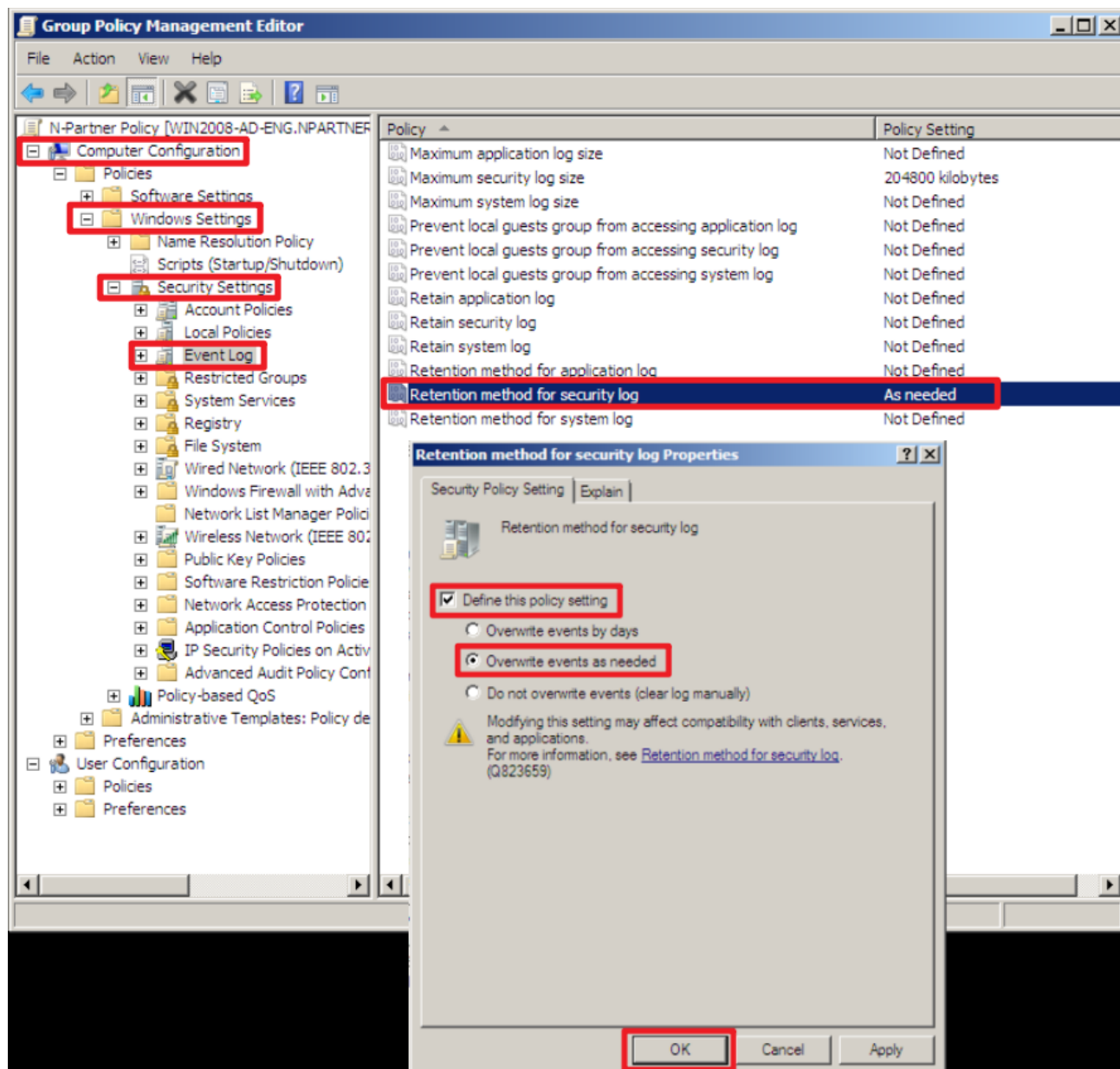
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

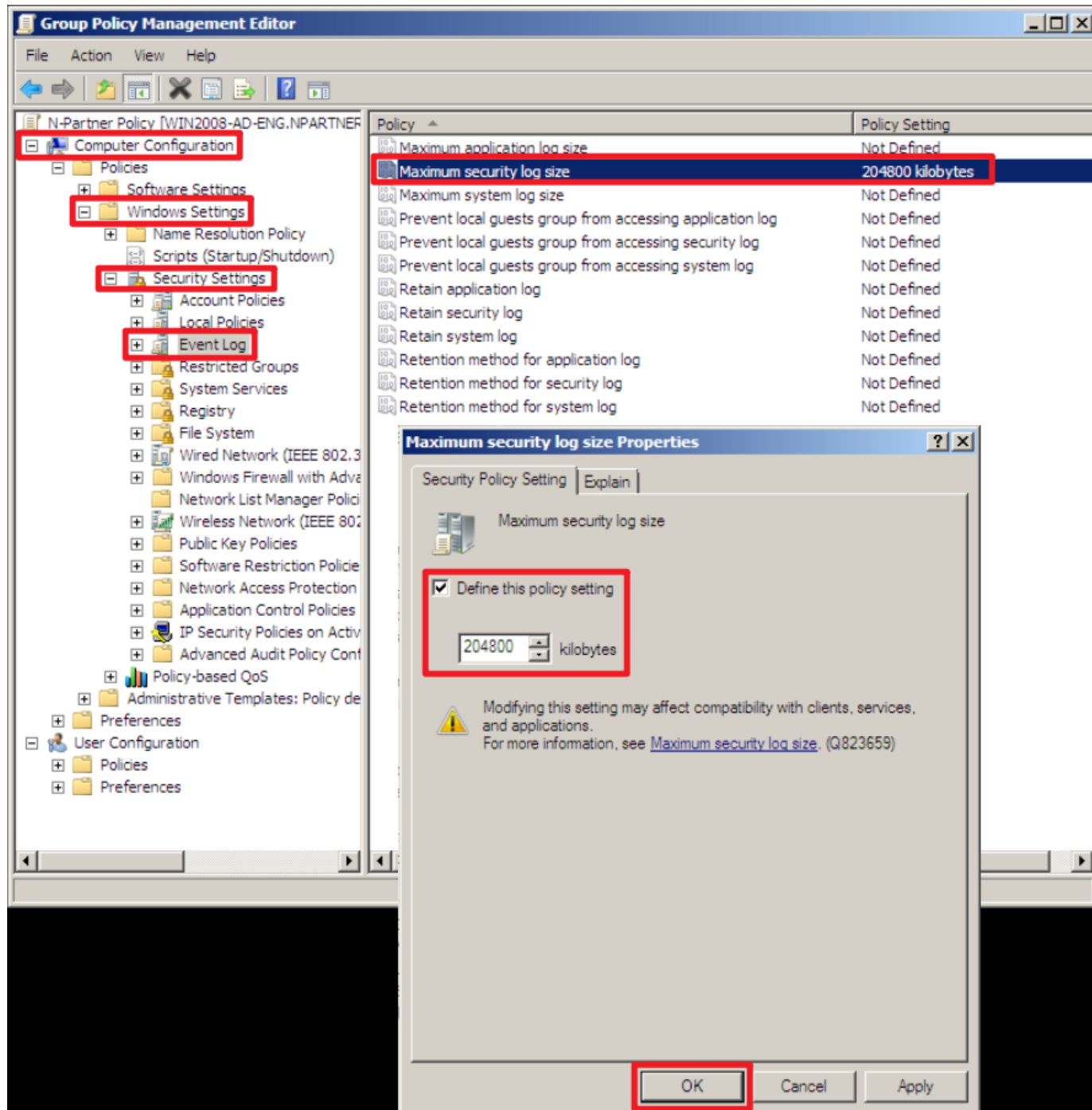
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

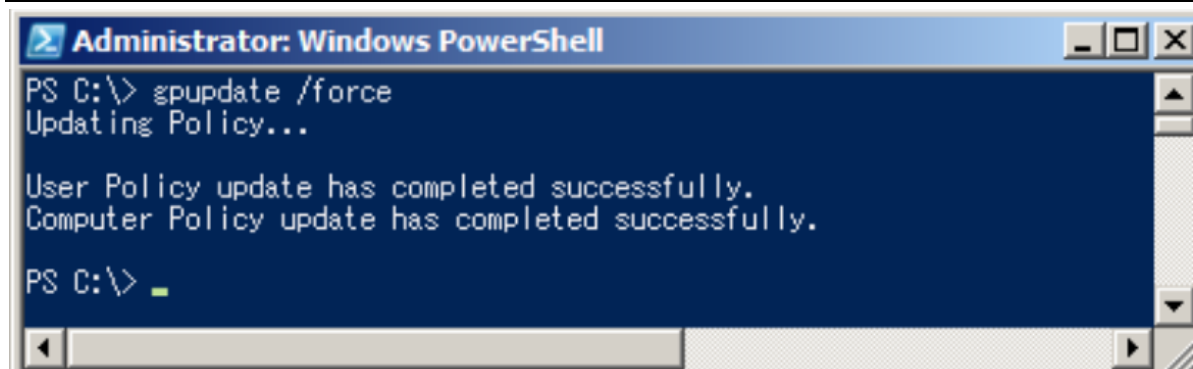


(8) On the Windows File server, open “Windows PowerShell.”



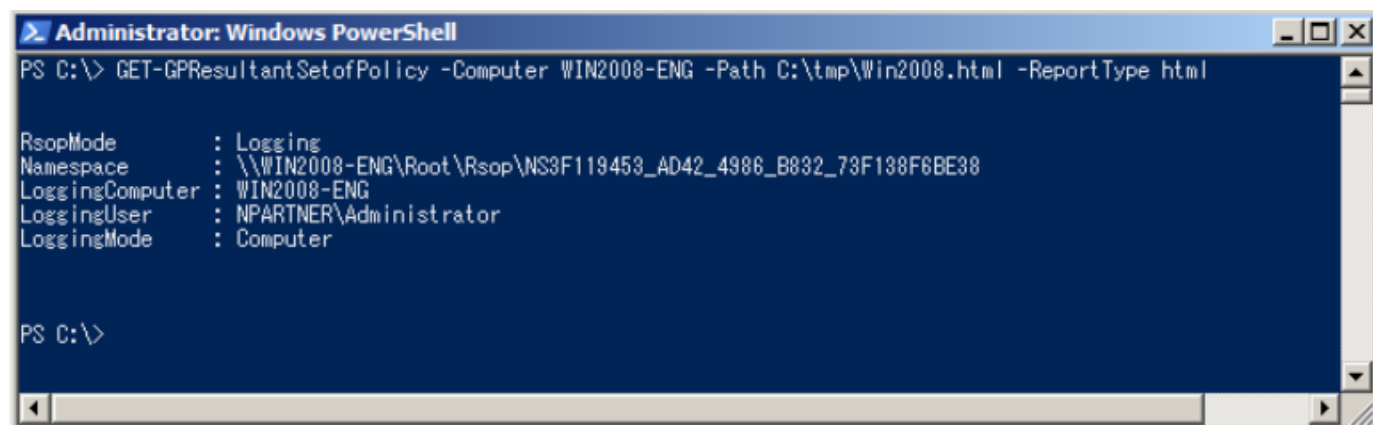
(9) Enter the command below to refresh group policy.

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



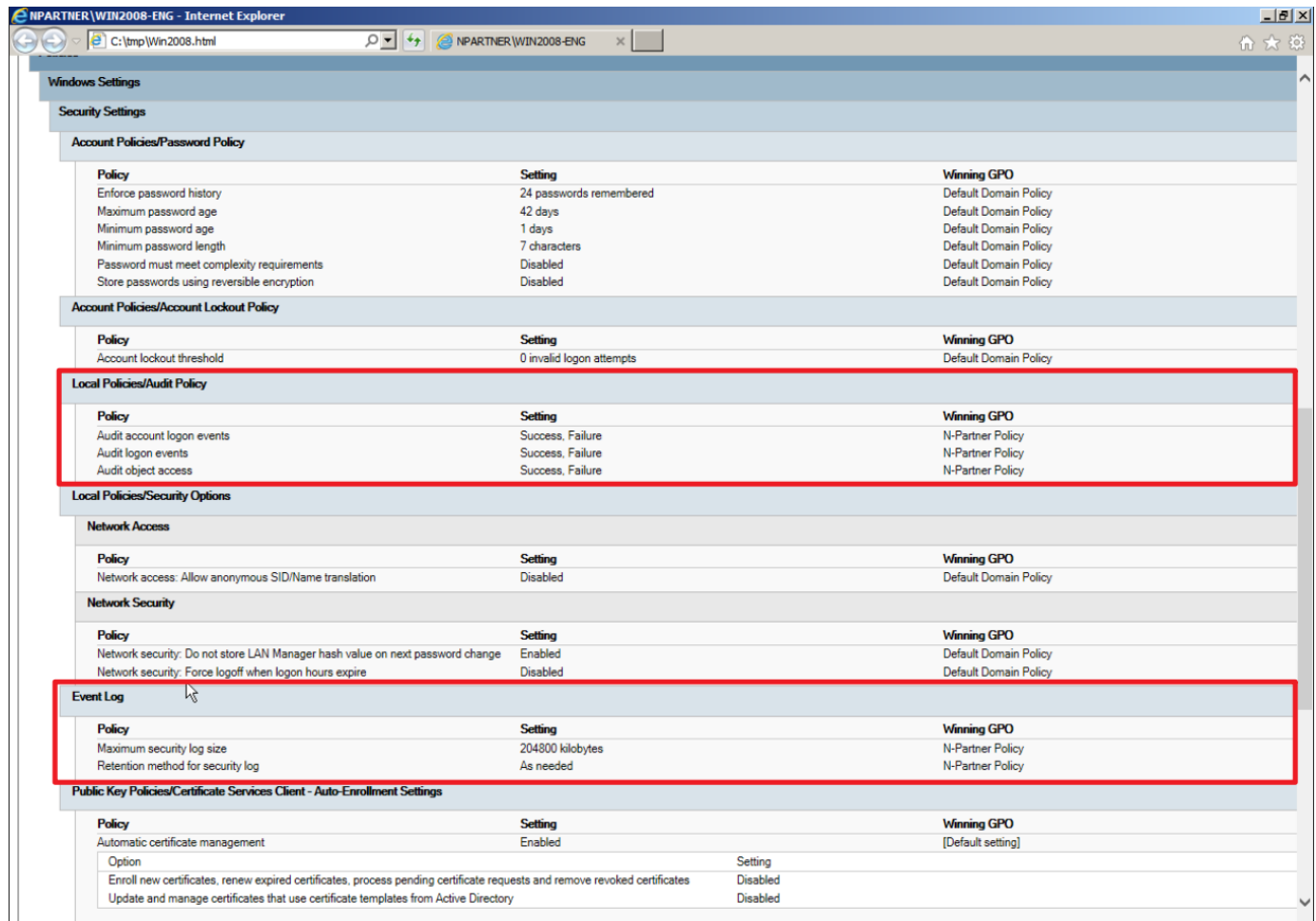
(10) On the AD domain server, open “Windows PowerShell” → enter the command below to generate the group policy report for the Windows File server.

```
PS C:\> Get-GPResultantSetofPolicy -Computer Win2008-ENG -Path C:\tmp\Win2008.html -ReportType html
```



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

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



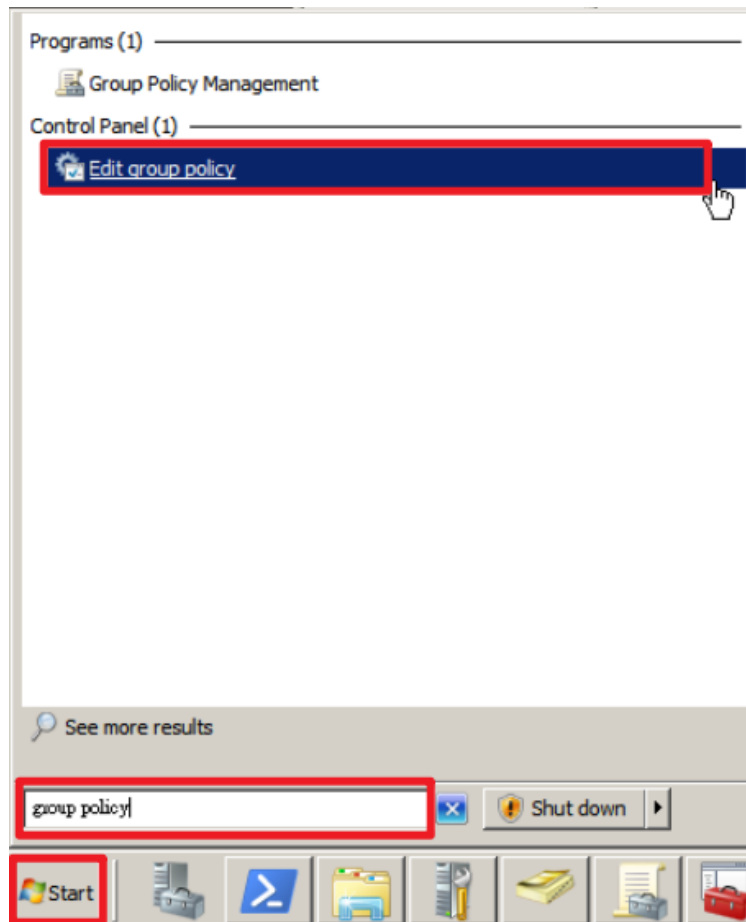
Policy	Setting	Winning GPO
Account Policies/Password Policy		
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Disabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
Account Policies/Account Lockout Policy		
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
Local Policies/Audit Policy		
Audit account logon events	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Local Policies/Security Options		
Network Access		
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy
Network Security		
Network security: Do not store LAN Manager hash value on next password change	Enabled	Default Domain Policy
Network security: Force logoff when logon hours expire	Disabled	Default Domain Policy
Event Log		
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings		
Automatic certificate management	Enabled	[Default setting]
Option	Setting	
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Disabled	
Update and manage certificates that use certificate templates from Active Directory	Disabled	

4.2 Workgroup

4.2.1 Audit Policy Configuration

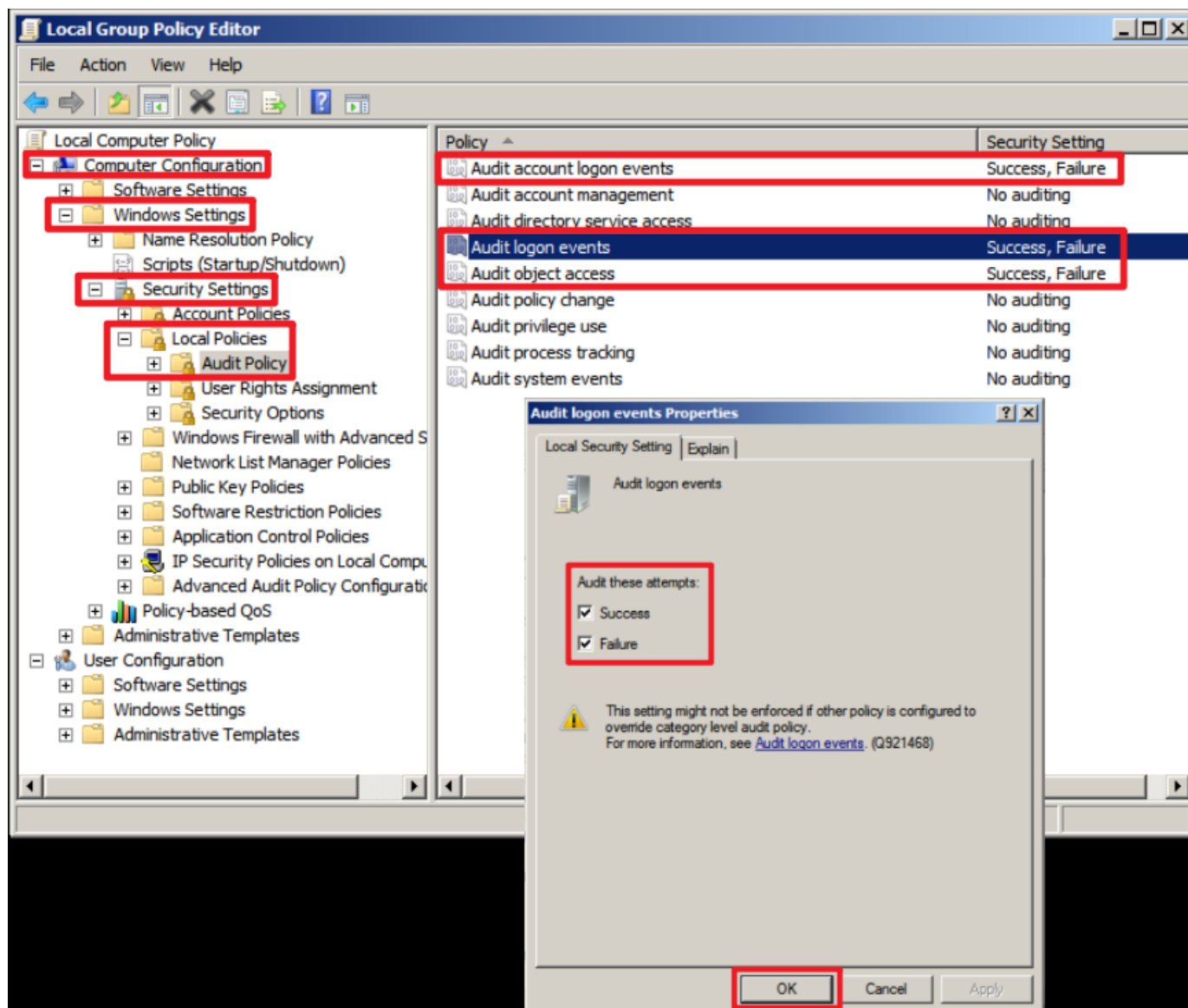
(1) Open “Local Group Policy Editor”

Click “Start” → in the “Search” field, type group policy → click “Edit group policy.”



(2) 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 logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”

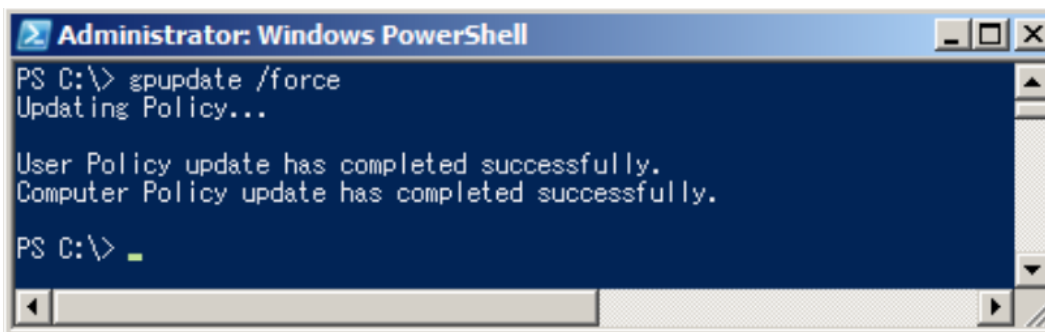


(3) Open “Windows Powershell.”



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

PS C:\> gpupdate /force



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

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

PS C:\> _
```

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

PS C:\> auditpol /get /category:*

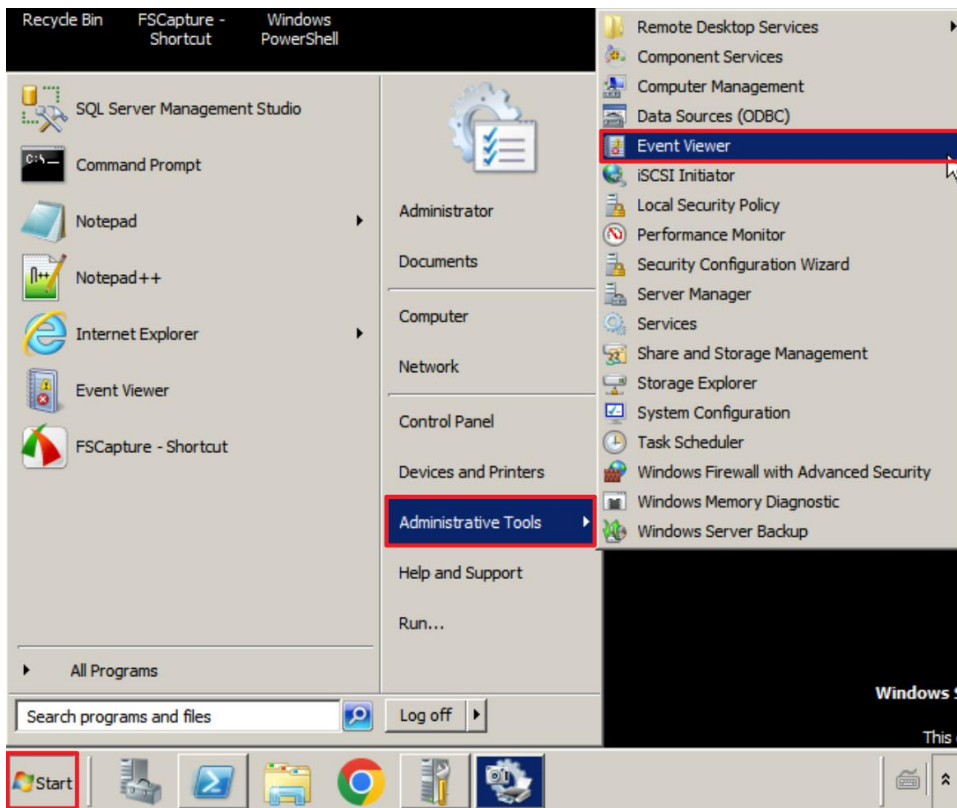


```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension No Auditing
  System Integrity         No Auditing
  IPsec Driver              No Auditing
  Other System Events       No Auditing
  Security State Change     No Auditing
Logon/Logoff
  Logon                     Success and Failure
  Logoff                    Success and Failure
  Account Lockout           Success and Failure
  IPsec Main Mode           Success and Failure
  IPsec Quick Mode          Success and Failure
  IPsec Extended Mode       Success and Failure
  Special Logon             Success and Failure
  Other Logon/Logoff Events  Success and Failure
  Network Policy Server     Success and Failure
Object Access
  File System               Success and Failure
  Registry                  Success and Failure
  Kernel Object             Success and Failure
  SAM                       Success and Failure
  Certification Services    Success and Failure
  Application Generated     Success and Failure
  Handle Manipulation        Success and Failure
  File Share                 Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events Success and Failure
  Detailed File Share       Success and Failure
Privilege Use
  Sensitive Privilege Use   No Auditing
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events No Auditing
Detailed Tracking
  Process Termination       No Auditing
  DPAPI Activity            No Auditing
  RPC Events                No Auditing
  Process Creation          No Auditing
Policy Change
  Audit Policy Change        Success
  Authentication Policy Change Success
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events No Auditing
Account Management
  User Account Management    Success and Failure
  Computer Account Management Success and Failure
  Security Group Management  Success and Failure
  Distribution Group Management Success and Failure
  Application Group Management Success and Failure
  Other Account Management Events Success and Failure
DS Access
  Directory Service Changes  No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access    Success
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events  Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation       Success and Failure
PS C:\>
```

4.2.2 Event Log Settings

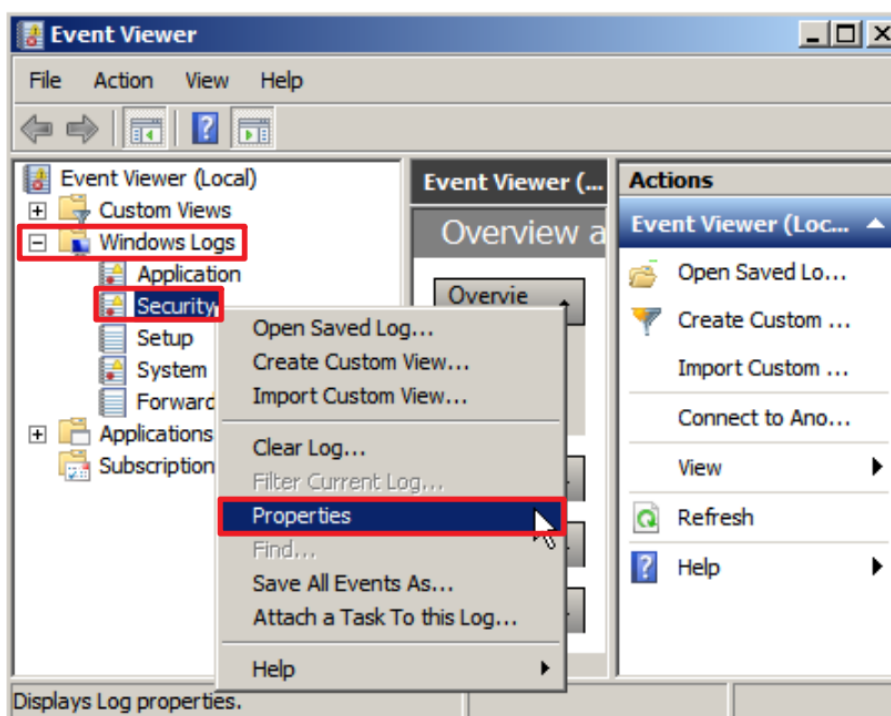
(1) Search for “Event Viewer”

Click “Start” → select “Administrative Tools” → “Event Viewer.”



(2) Edit Security Log

Expand “Windows Logs” → right-click “Security” and select “Properties.”

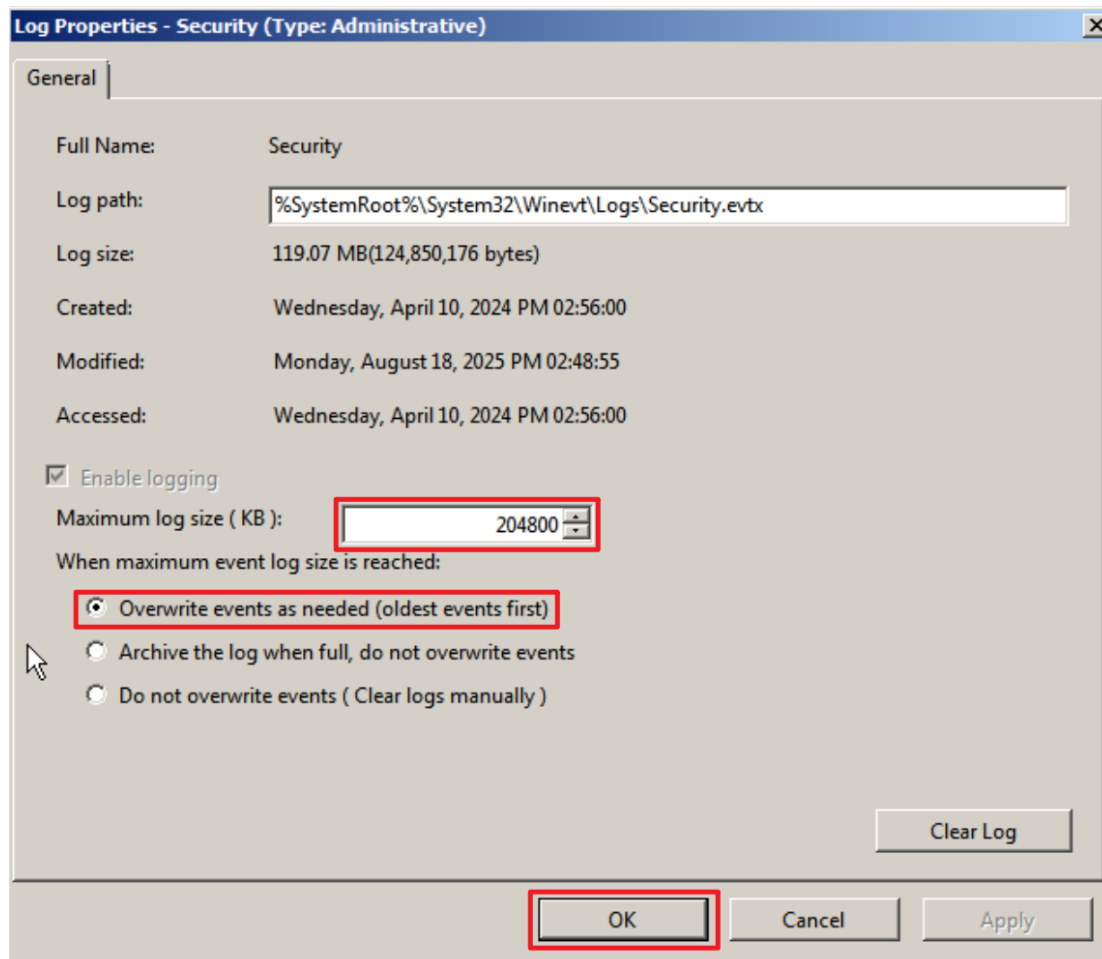


(3) Configure Security Log

Enter maximum log file size: 204800 KB

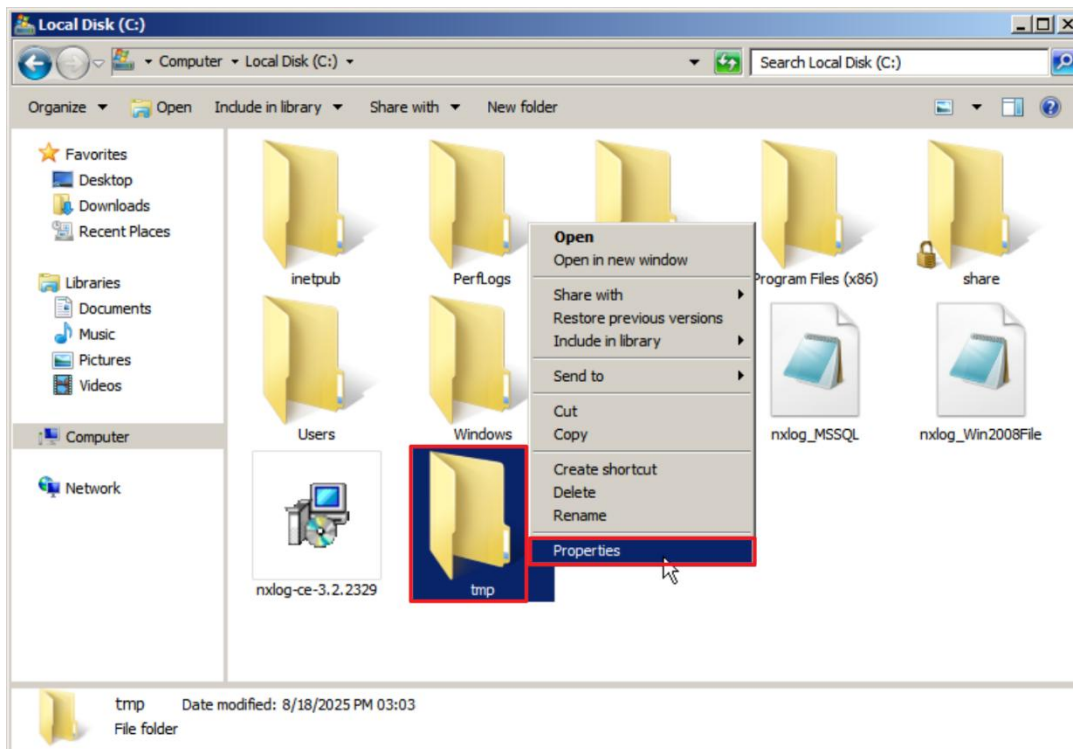
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed(oldest events first)” → click “OK.”

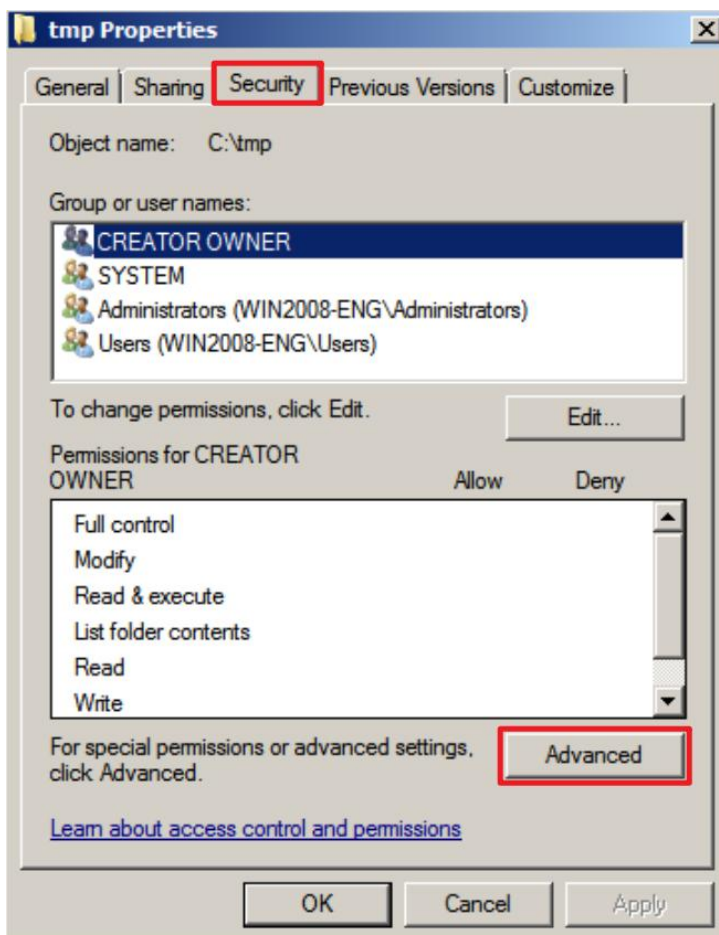


4.3 Folder Audit Configuration

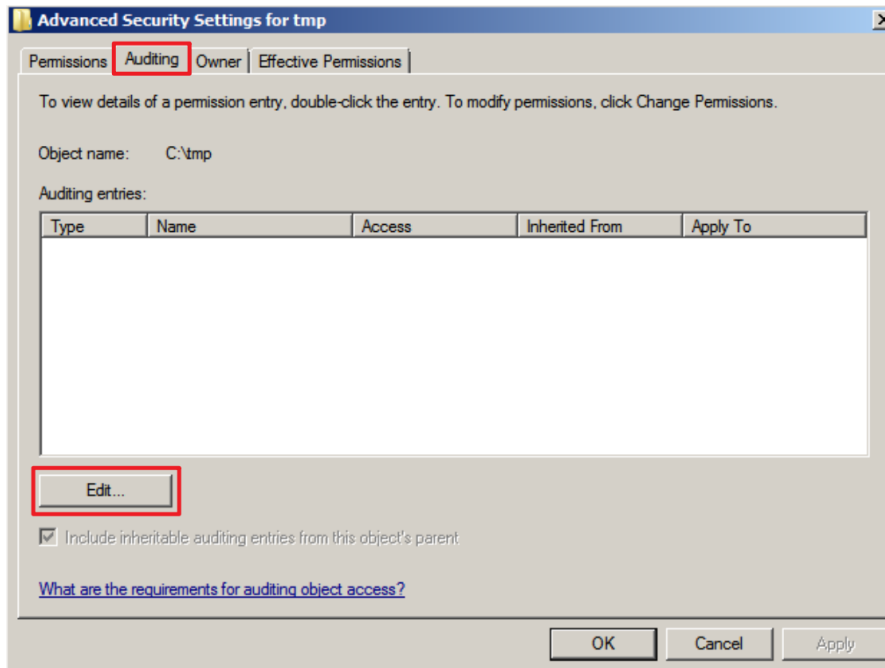
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



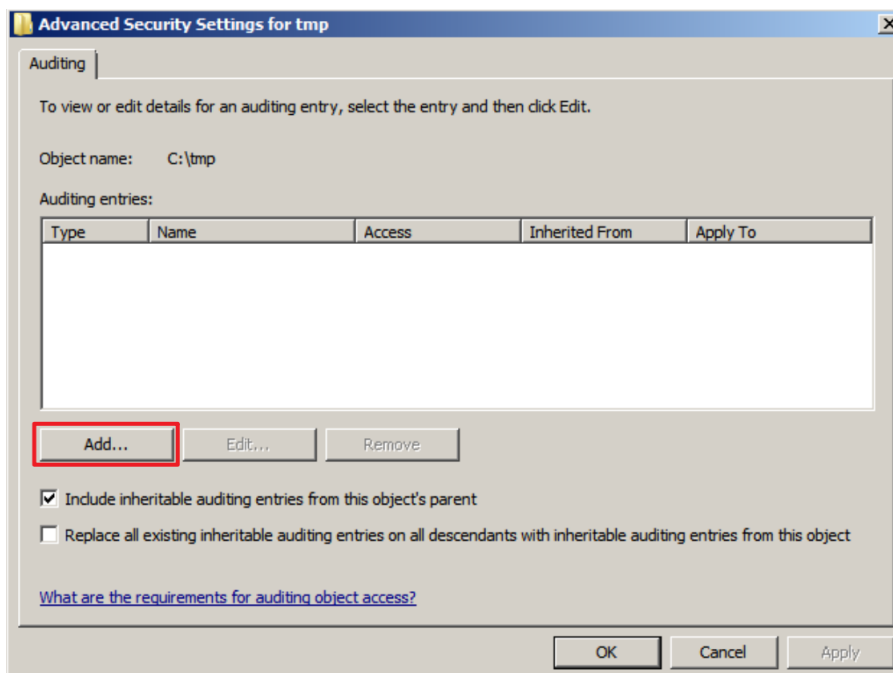
(2) Go to the “Security” tab → click “Advanced.”



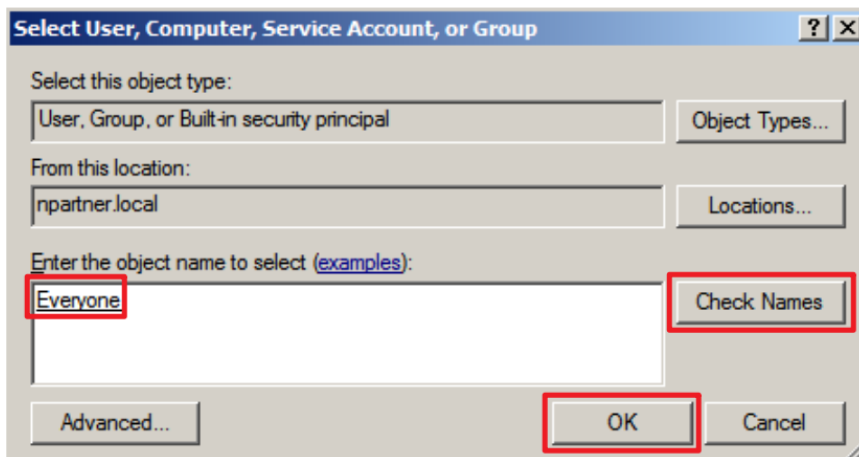
(3) Open the “Auditing” tab → click “Edit.”



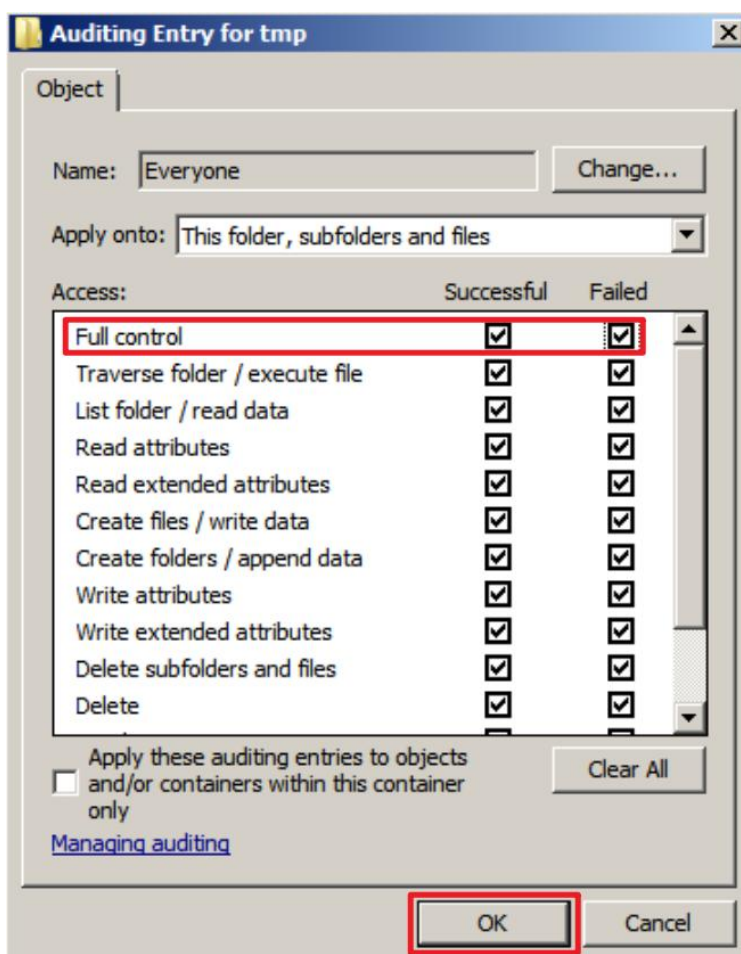
(4) Click “Add.”



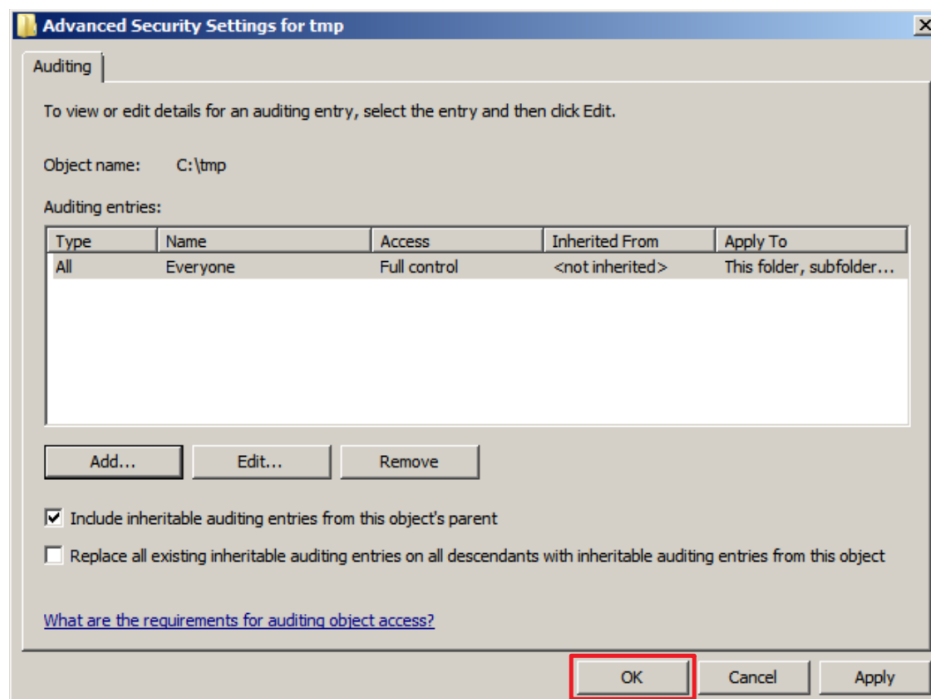
(5) In the object name field, enter Everyone to audit all users → click “Check Names” → click “OK.”



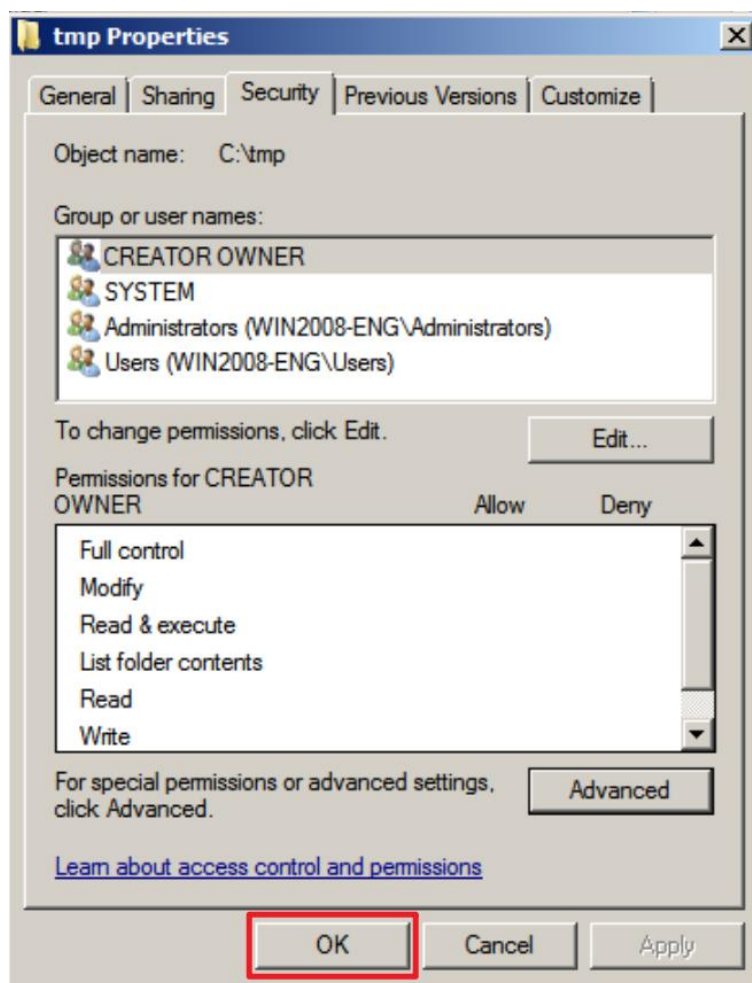
(6) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



(7) Confirm that the auditing entries shows “Everyone.”



(8) Click “OK” again to confirm and close.



5. Windows Server 2012

5.1 Domain

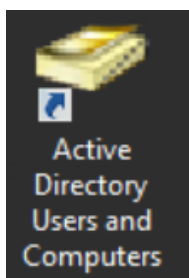
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

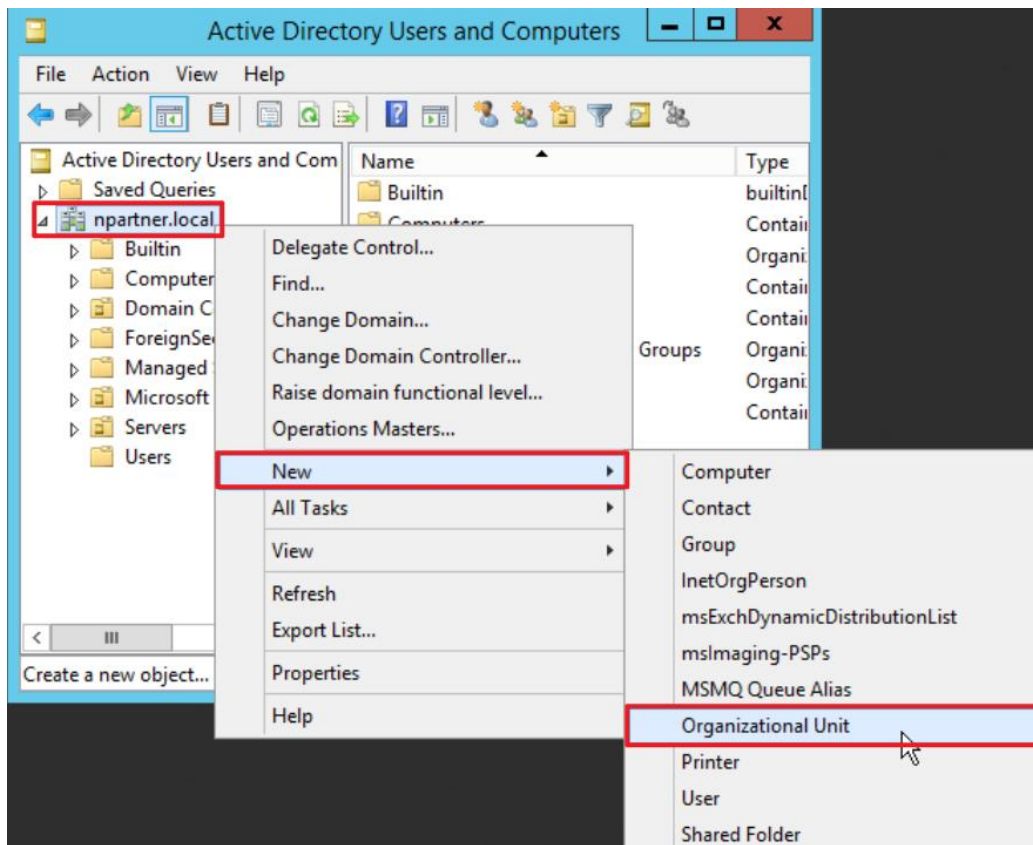
5.1.1 Organizational Unit (OU) Configuration

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



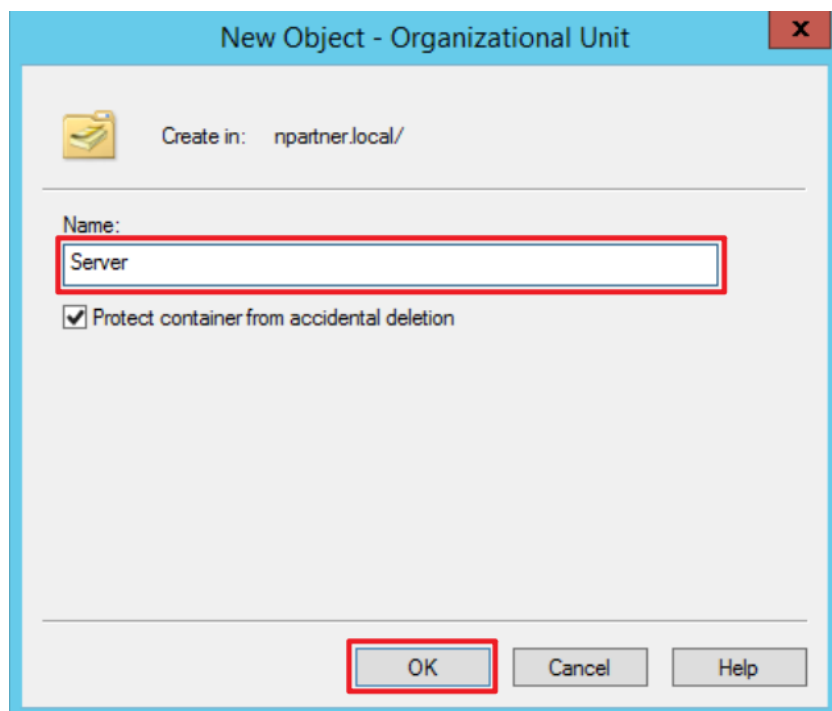
(2) Add an Organizational Unit

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”)

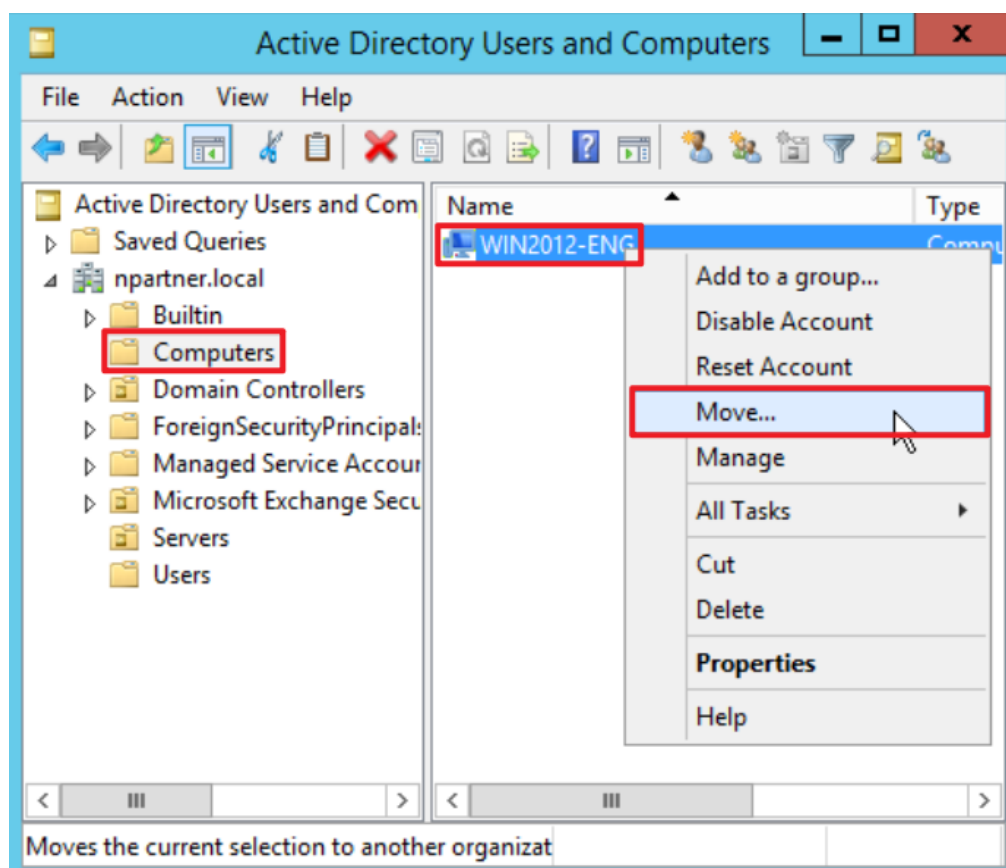
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

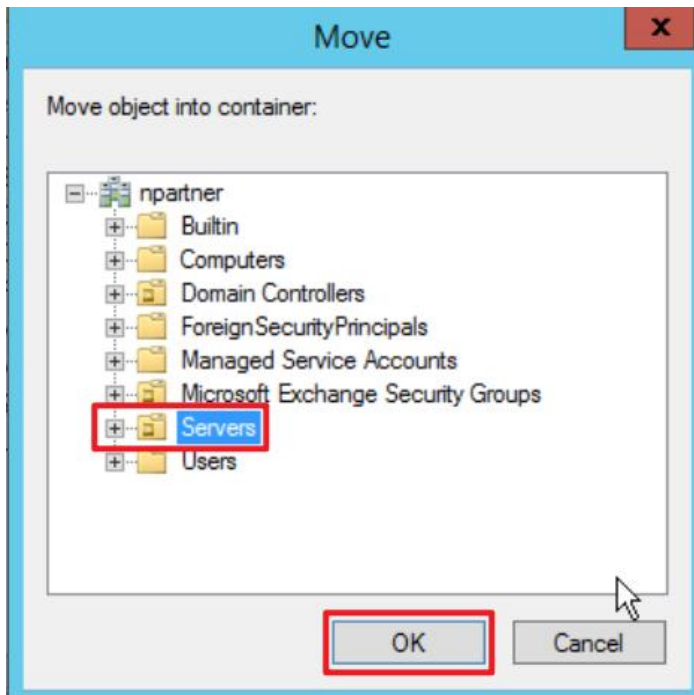
Select the “Computers” organizational unit (OU) → right-click on the “WIN2012” server.

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



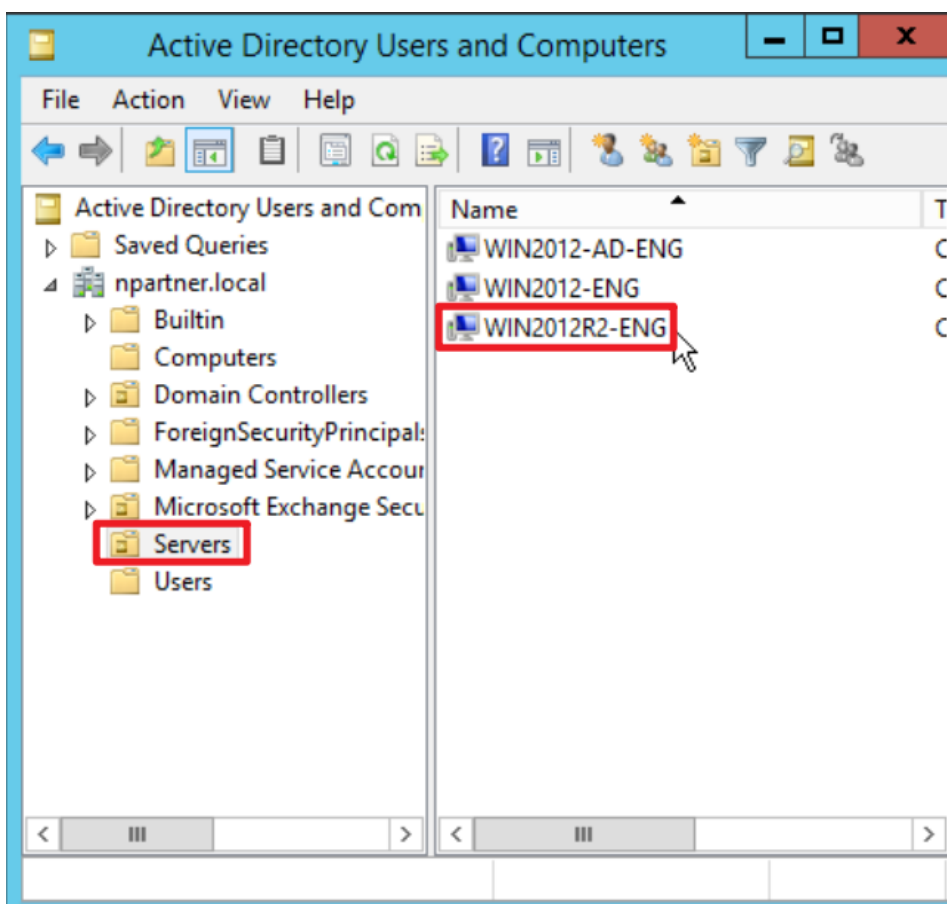
(5) Select your Organizational Unit:

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



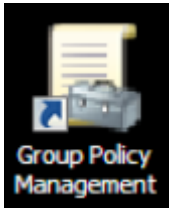
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



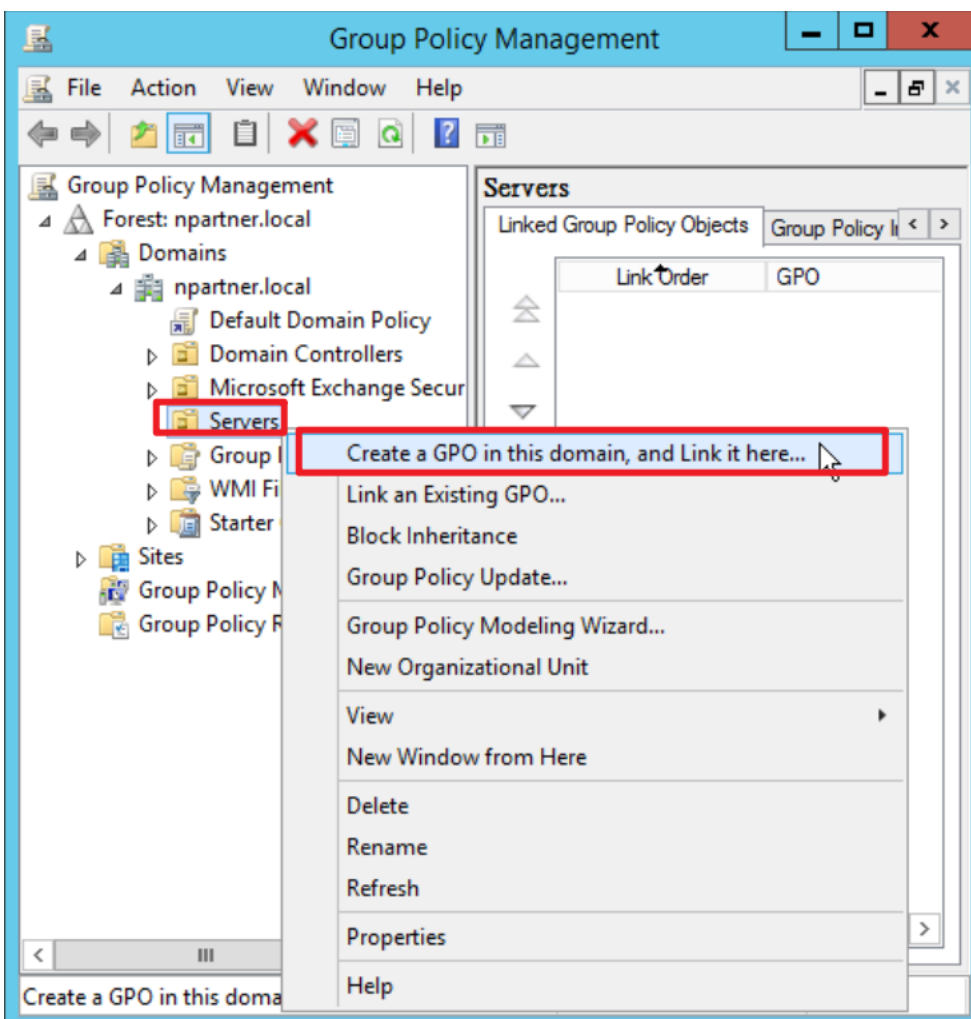
5.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

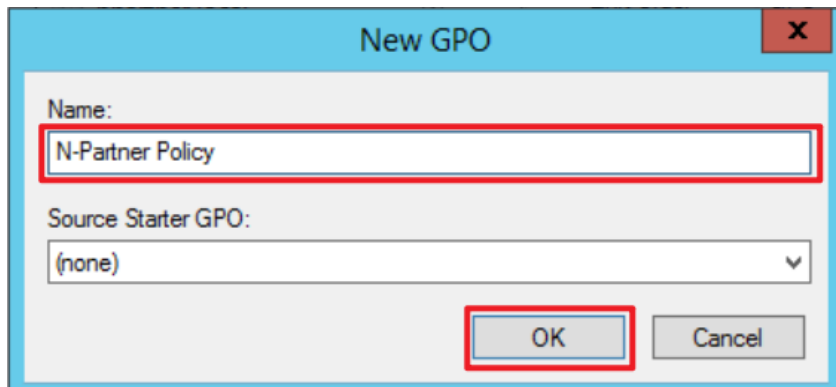
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

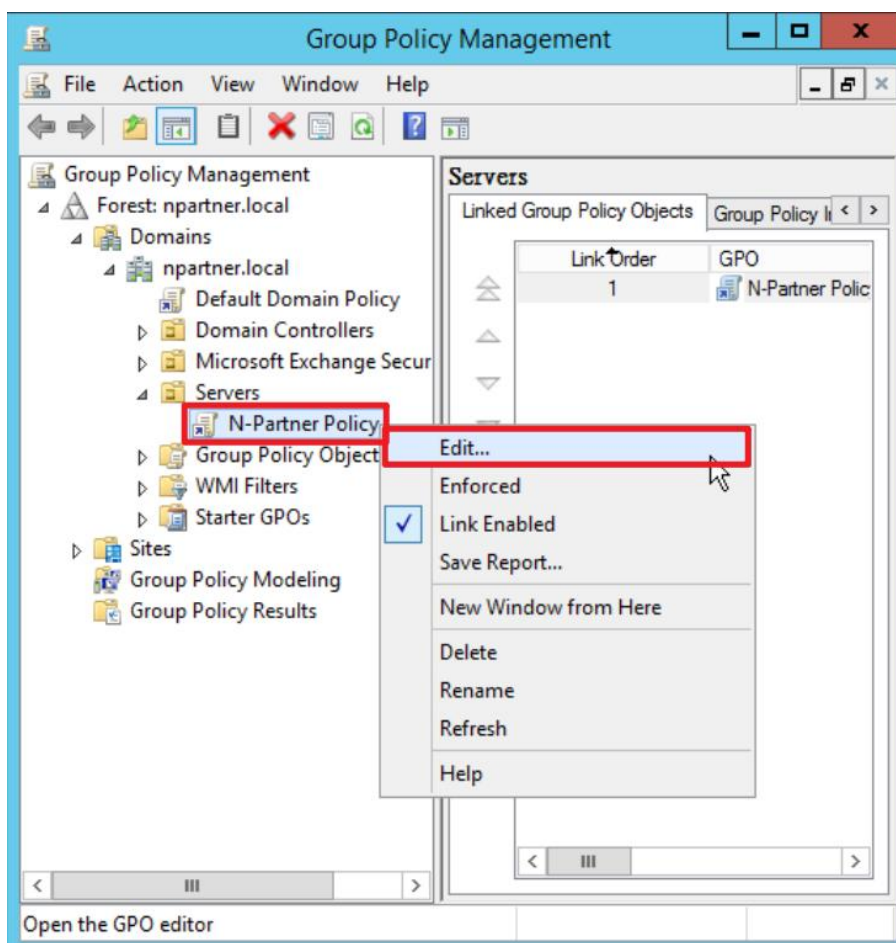
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



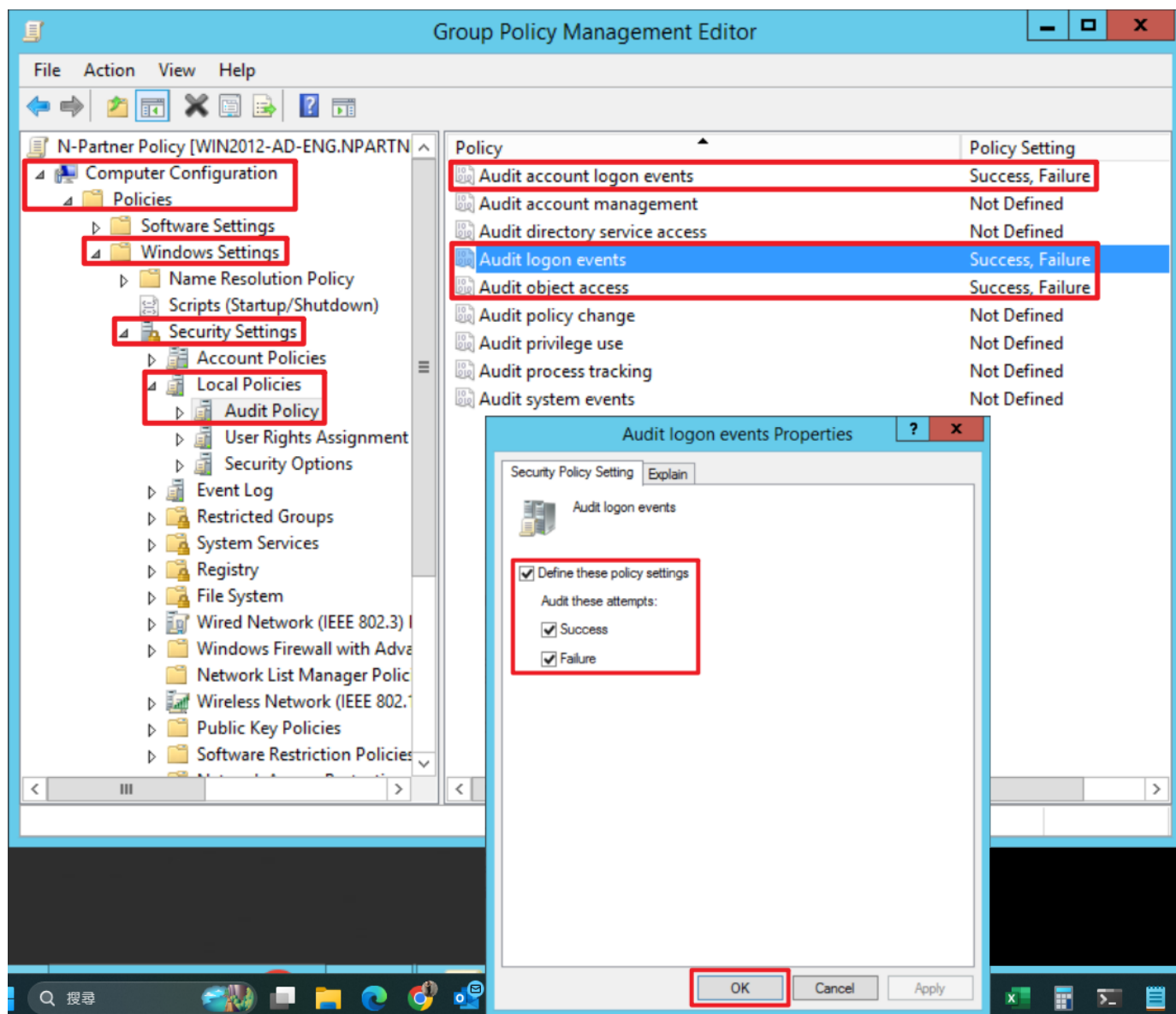
(4) Edit your Group Policy Object

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



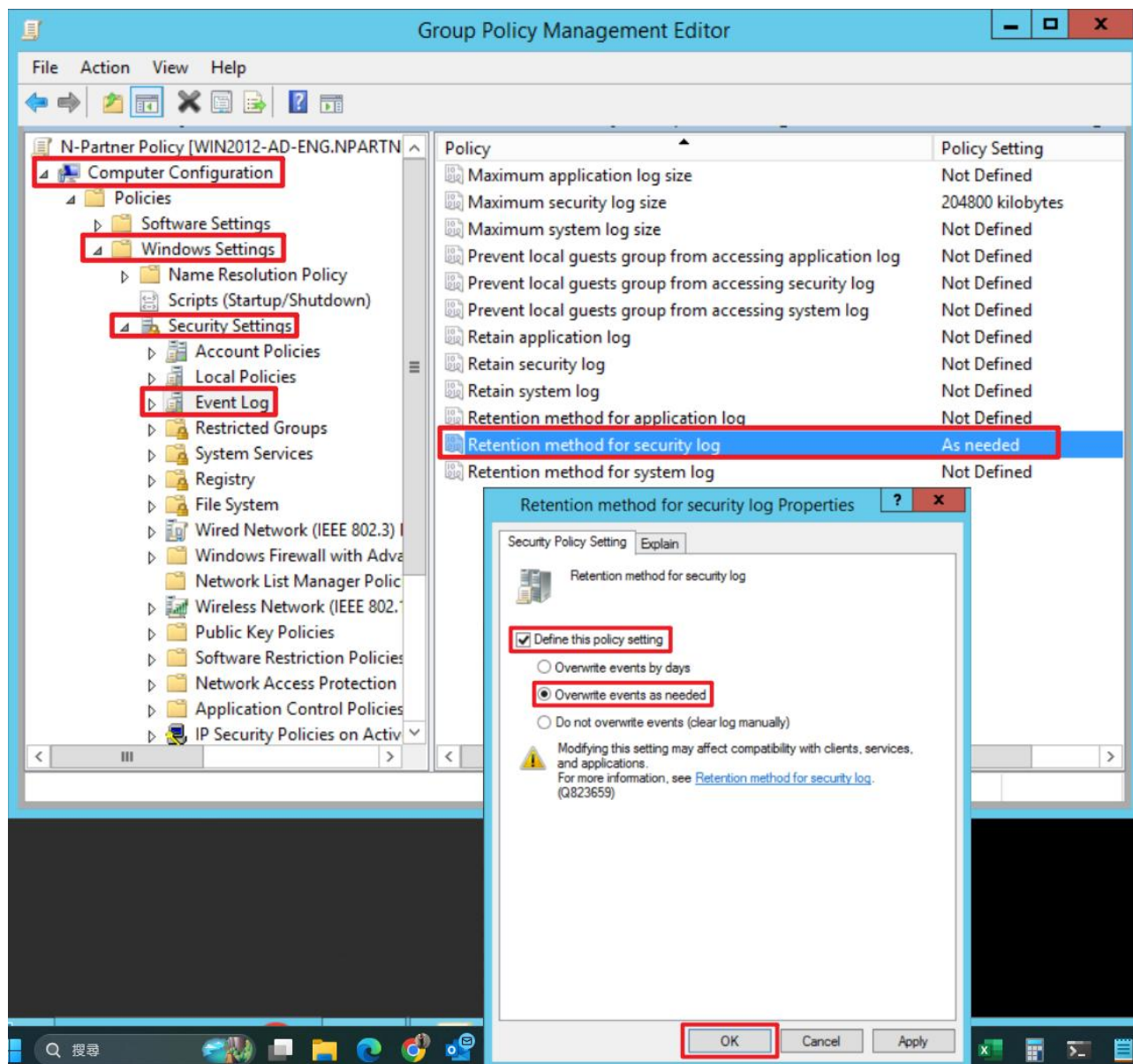
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

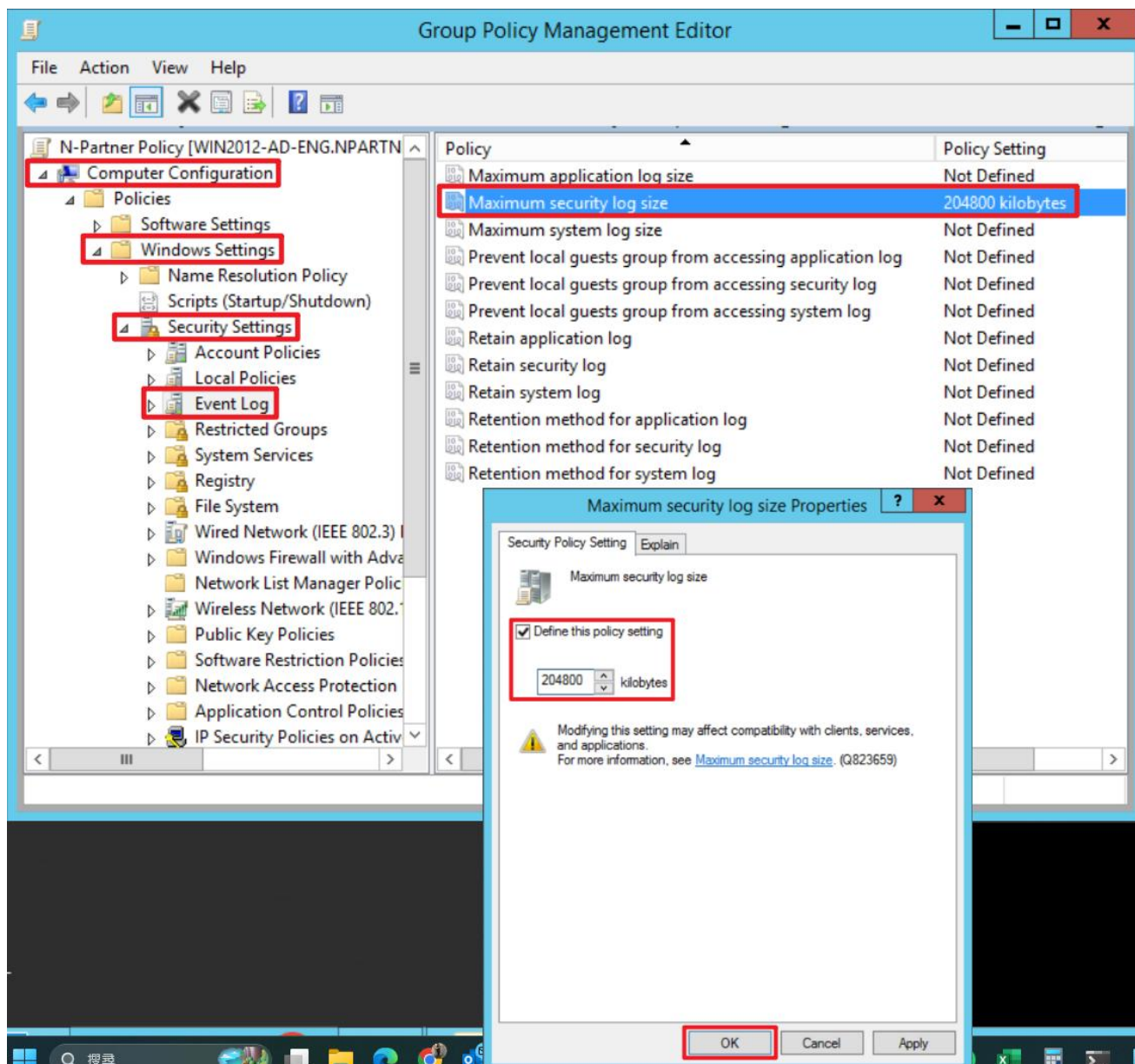
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

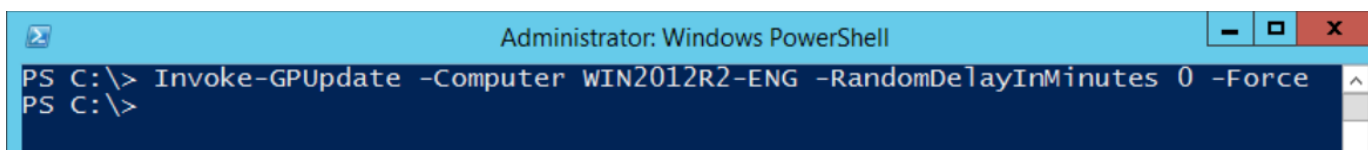


(8) On the AD domain server, open “Windows PowerShell.”



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

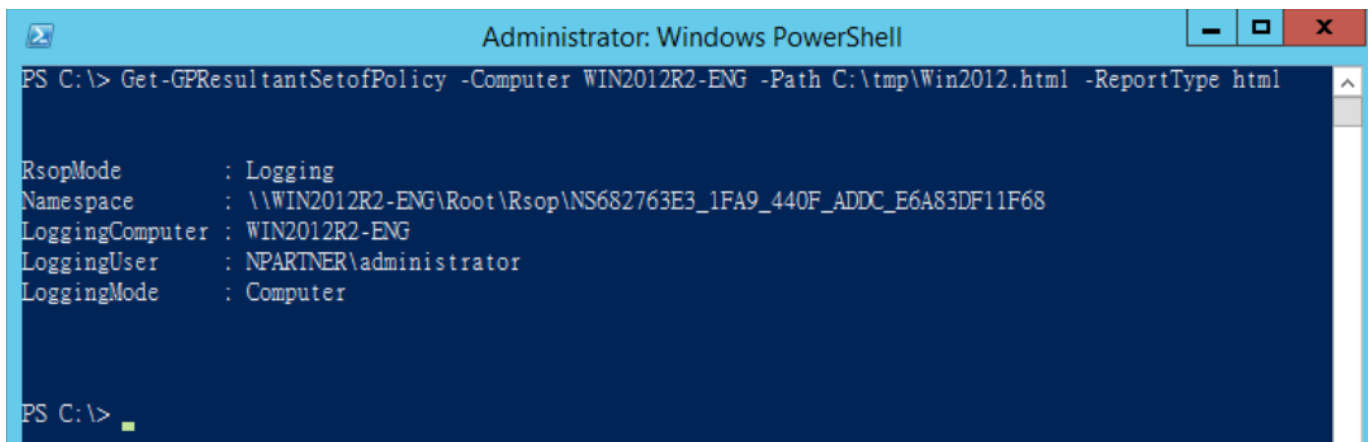
```
PS C:\> Invoke-GPUdate -Computer WIN2012-ENG -RandomDelayInMinutes 0 -Force
```



Replace the text shown in red with the **Windows File server** name.

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

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-ENG -Path C:\tmp\WIN2012.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 File server is applying the N-Partner Policy Group Policy.

Group Policy Results

NPARTNER\WIN2012R2-ENG
Data collected on: 8/18/2025 PM 03:43:20

Summary [show all](#) [show](#)

Computer Details [hide](#)

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](#)

Local Policies/Audit Policy [hide](#)

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy

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

Local Policies/Security Options [show](#)

Event Log [hide](#)

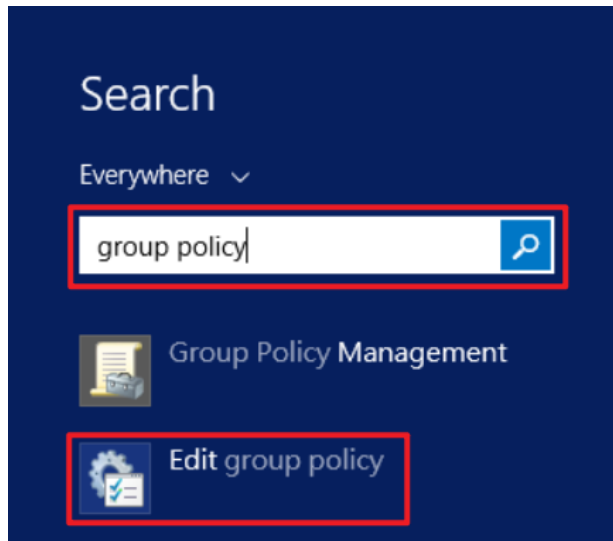
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy

5.2 Workgroup

5.2.1 Audit Policy Configuration

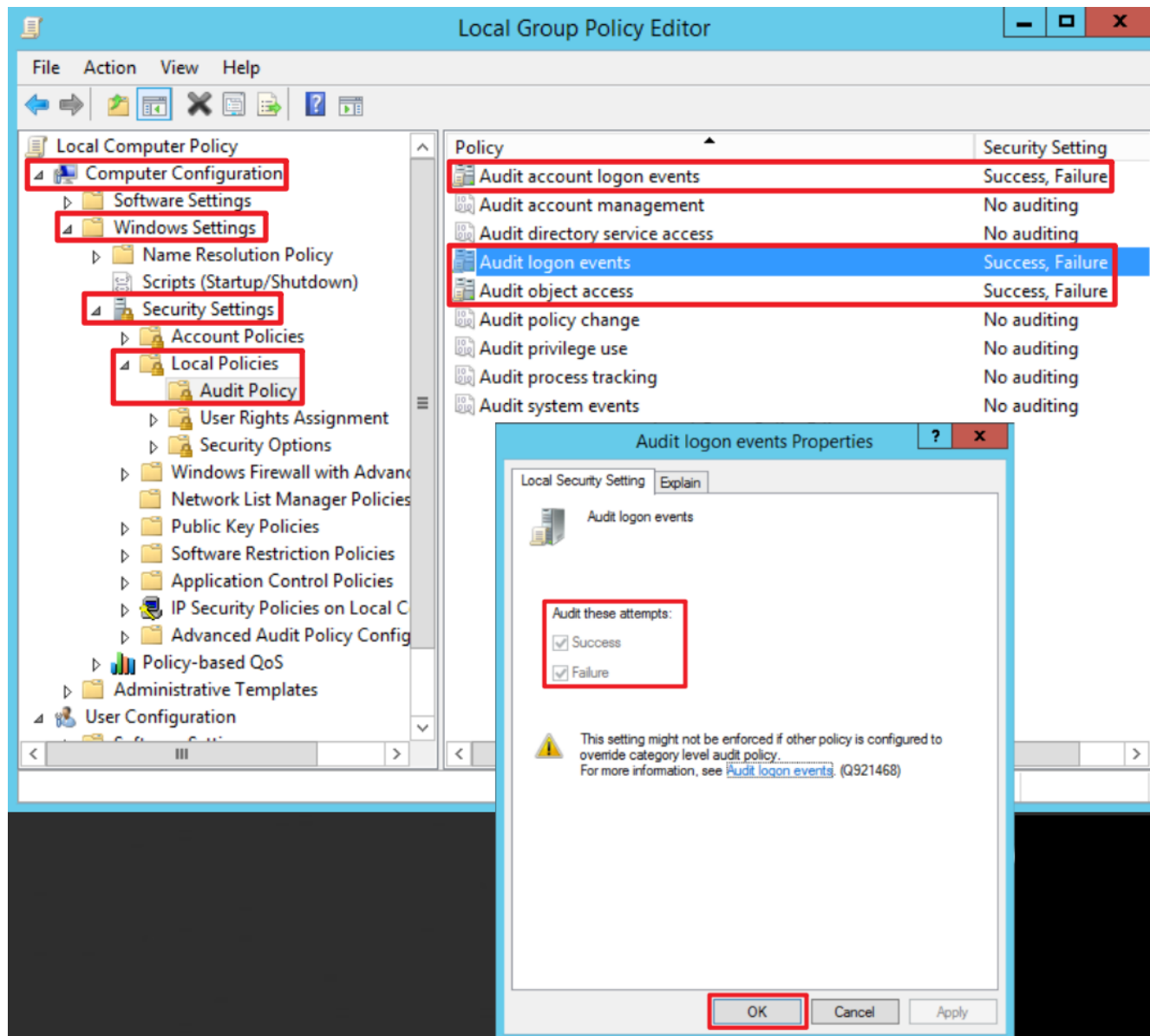
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) 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 logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”



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

PS C:\> gpupdate /force

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

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

PS C:\> █
```

(5) Enter the command below to view group policy applied status.

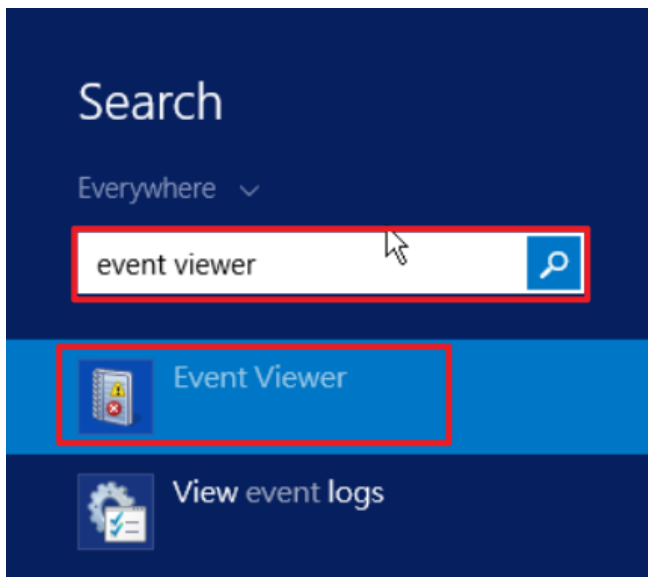
PS C:\> auditpol /get /category:*

```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
  Security System Extension No Auditing
  System Integrity         No Auditing
  IPsec Driver              No Auditing
  Other System Events      No Auditing
  Security State Change     No Auditing
Logon/Logoff
  Logon                    Success and Failure
  Logoff                   Success and Failure
  Account Lockout          Success and Failure
  IPsec Main Mode           Success and Failure
  IPsec Quick Mode          Success and Failure
  IPsec Extended Mode       Success and Failure
  Special Logon             Success and Failure
  Other Logon/Logoff Events Success and Failure
  Network Policy Server     Success and Failure
  User / Device Claims      Success and Failure
Object Access
  File System              Success and Failure
  Registry                 Success and Failure
  Kernel Object            Success and Failure
  SAM                      Success and Failure
  Certification Services   Success and Failure
  Application Generated     Success and Failure
  Handle Manipulation       Success and Failure
  File Share                Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events Success and Failure
  Detailed File Share       Success and Failure
  Removable Storage         Success and Failure
  Central Policy Staging    Success and Failure
Privilege Use
  Non Sensitive Privilege Use No Auditing
  Other Privilege Use Events  No Auditing
  Sensitive Privilege Use     No Auditing
Detailed Tracking
  Process Creation          No Auditing
  Process Termination       No Auditing
  DPAPI Activity            No Auditing
  RPC Events                No Auditing
  Plug and Play Events      No Auditing
Policy Change
  Authentication Policy Change No Auditing
  Authorization Policy Change No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events  No Auditing
  Audit Policy Change        No Auditing
Account Management
  User Account Management    No Auditing
  Computer Account Management No Auditing
  Security Group Management   No Auditing
  Distribution Group Management No Auditing
  Application Group Management No Auditing
  Other Account Management Events No Auditing
DS Access
  Directory Service Changes  No Auditing
  Directory Service Replication No Auditing
  Detailed Directory Service Replication No Auditing
  Directory Service Access    No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events  Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation       Success and Failure
PS C:\>
```

5.2.2 Event Log Settings

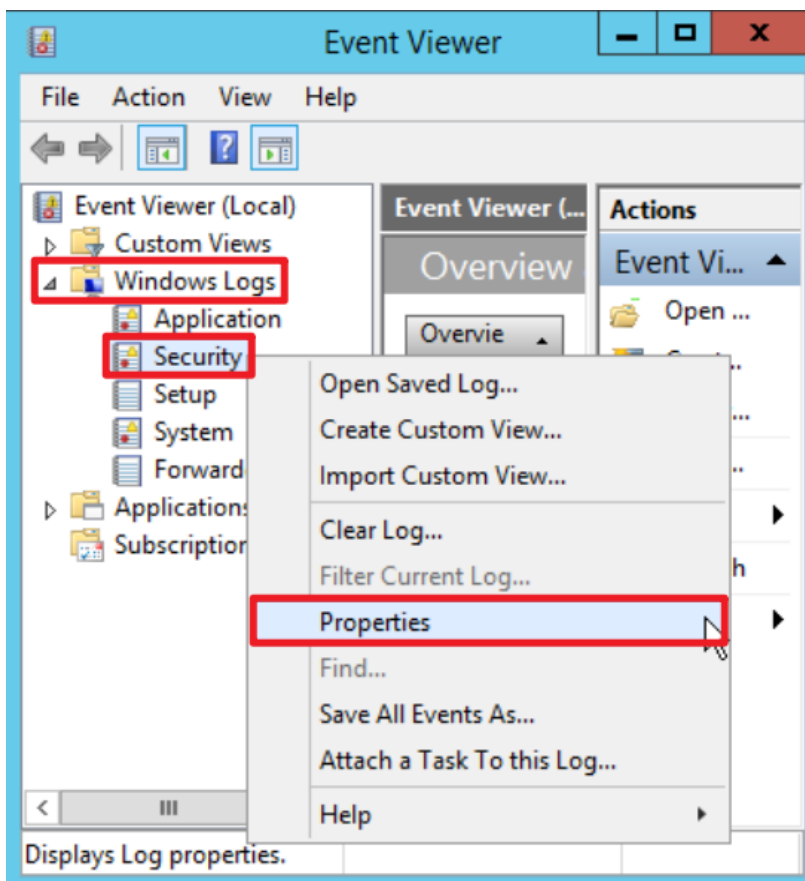
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “[Event Viewer](#)” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Application” → And click on “Properties.”



(3) Configure Security Log

Enter maximum log file size: 204800 KB

Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”

Log Properties - Security (Type: Administrative)

General

Full Name: Security

Log path: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Log size: 200.00 MB(209,719,296 bytes)

Created: Wednesday, April 10, 2024 PM 03:30:07

Modified: Monday, August 18, 2025 PM 03:11:26

Accessed: Wednesday, April 10, 2024 PM 03:30:07

☒ Enable logging

Maximum log size (KB): 204800

When maximum event log size is reached:

☒ Overwrite events as needed (oldest events first)

☐ Archive the log when full, do not overwrite events

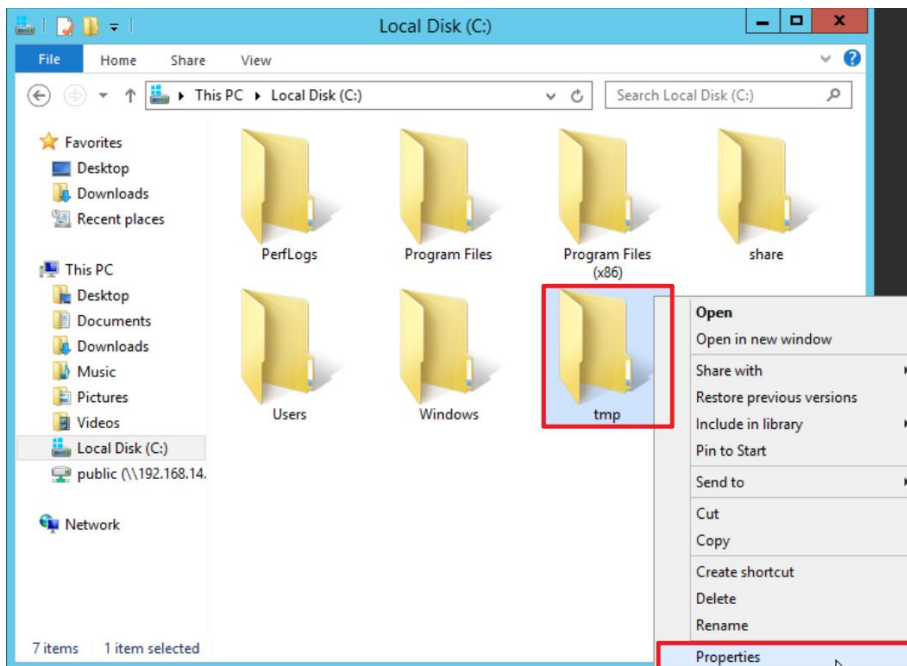
☐ Do not overwrite events (Clear logs manually)

Clear Log

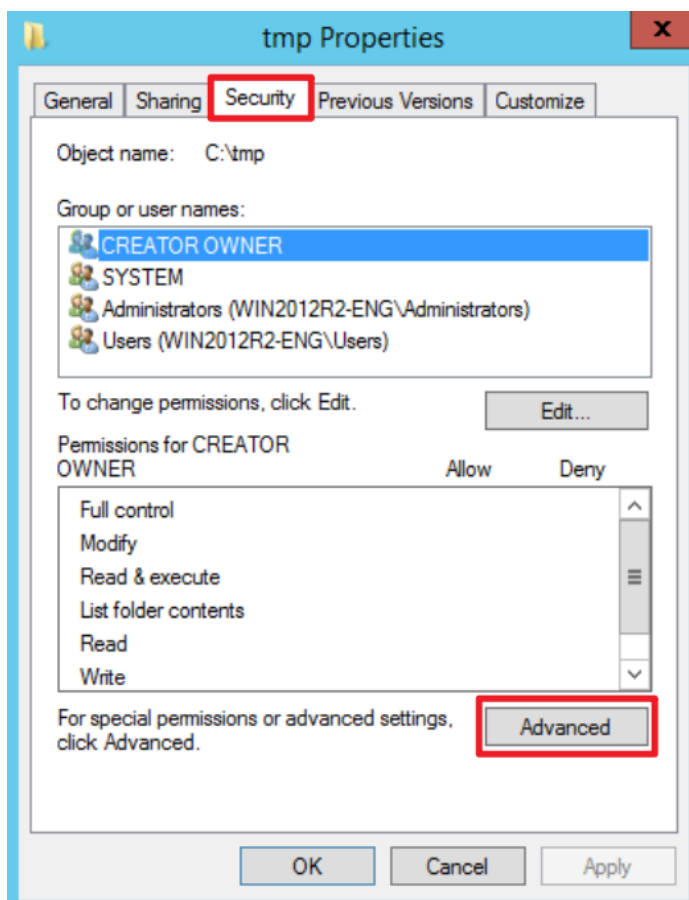
OK Cancel Apply

5.3 Folder Audit Configuration

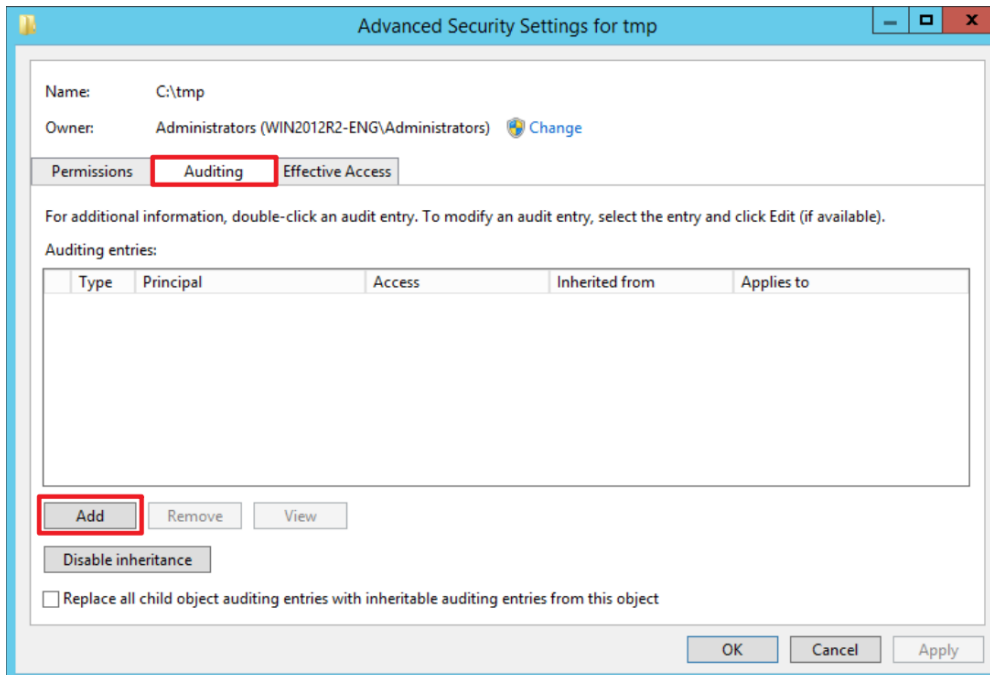
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



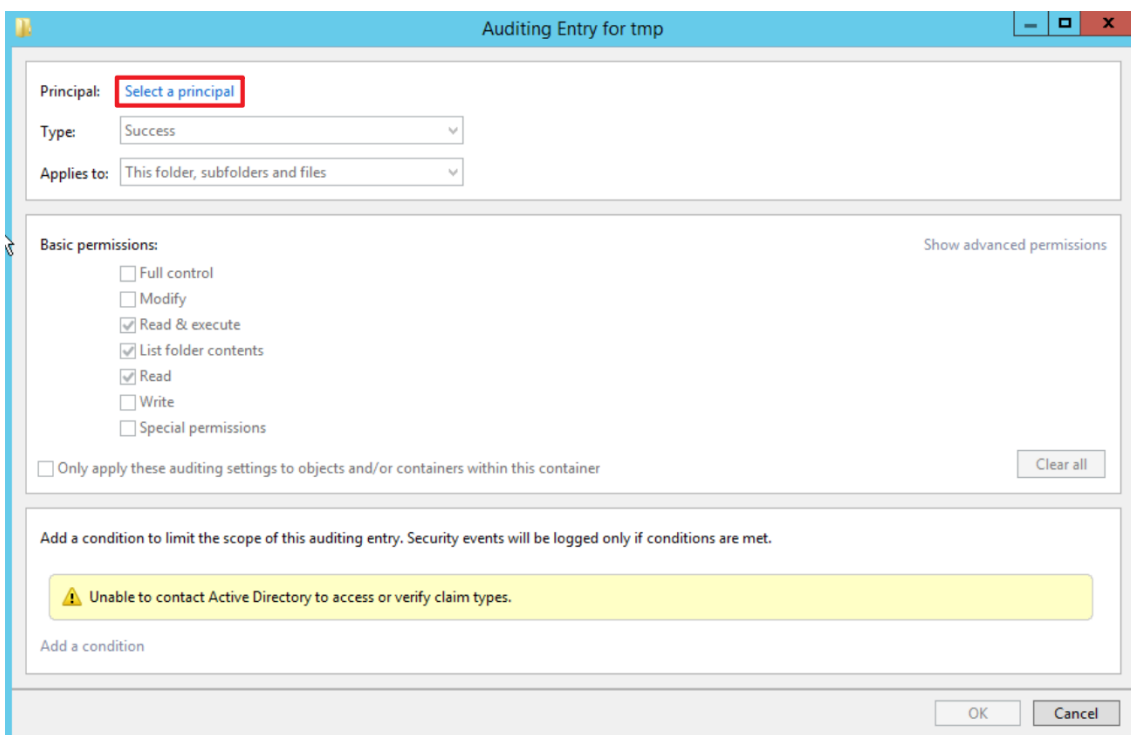
(2) Go to the “Security” tab → click “Advanced.”



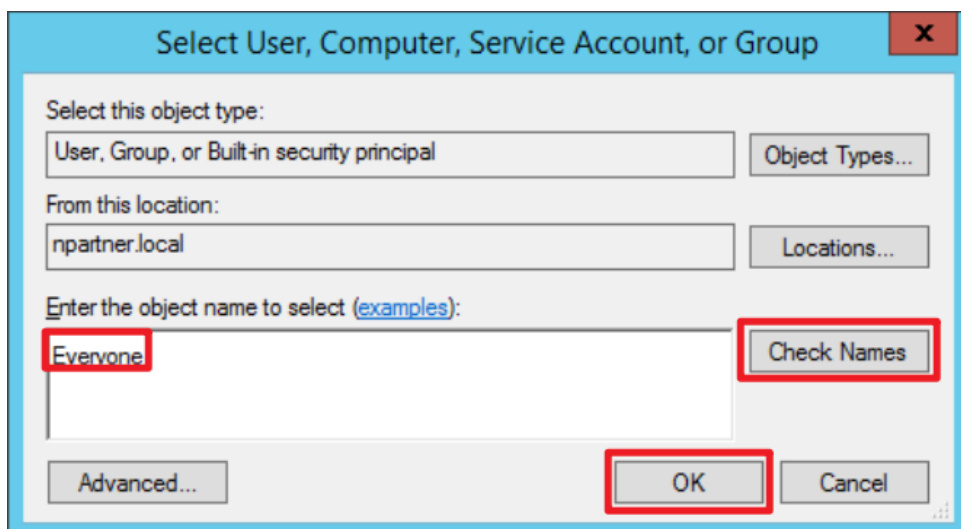
(3) Open the “Auditing” tab → click “Add.”



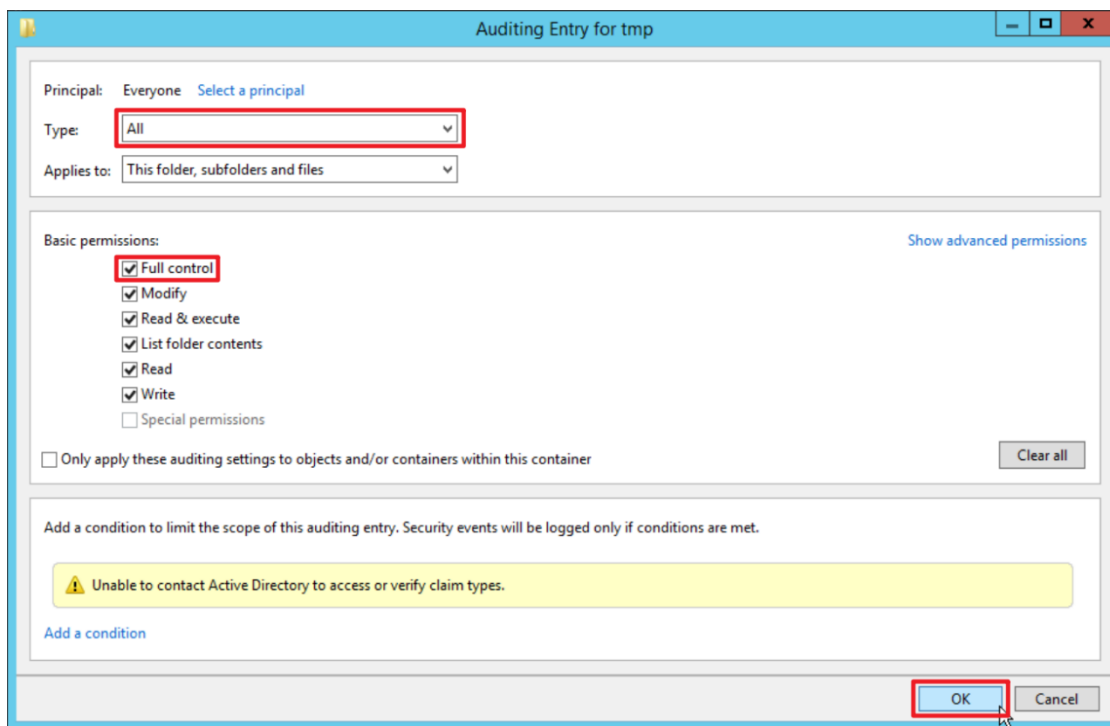
(4) Click “Select a principal.”



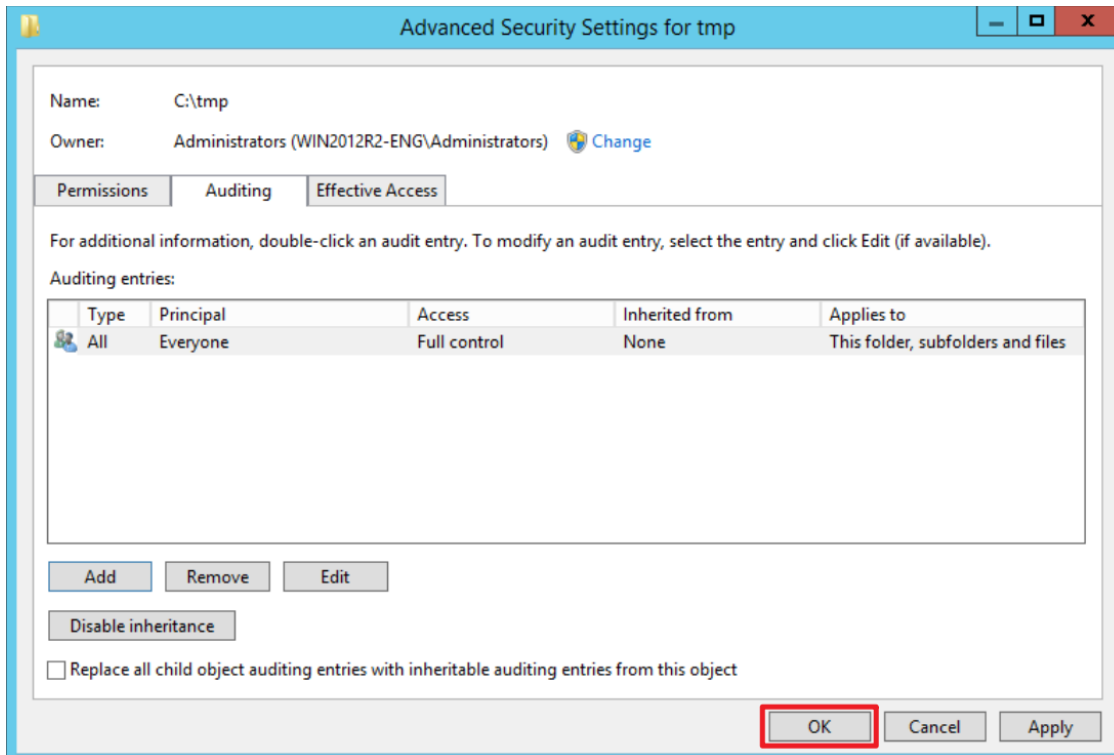
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



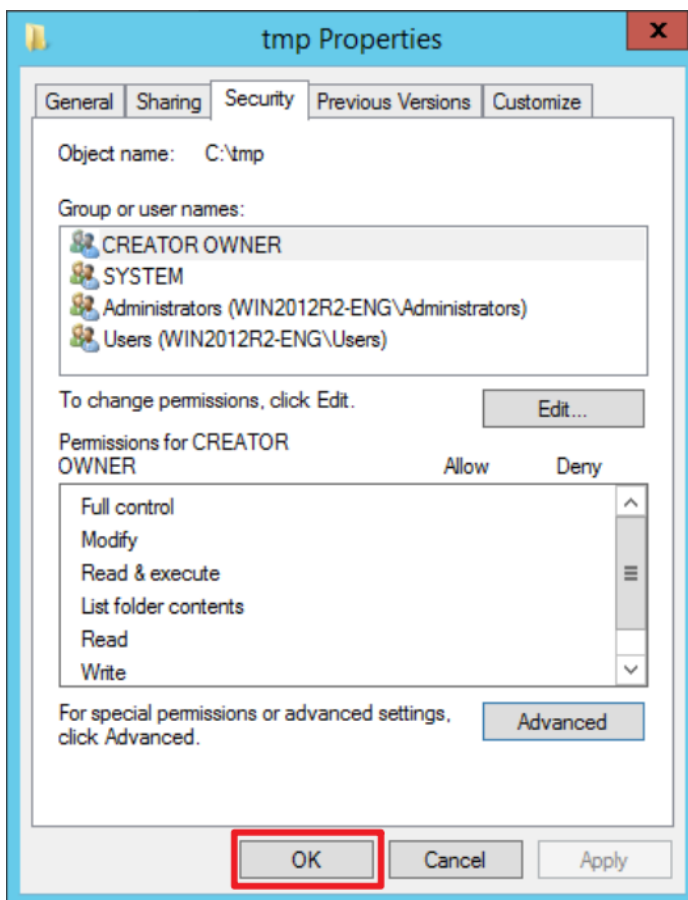
(6) Select “All” in type → enable “Full Control” → click “OK.”



(7) Confirm that the auditing entries shows “Everyone” → click “OK.”



(8) Click “OK” again to confirm and close.



6. Windows Server 2016

6.1 Domain

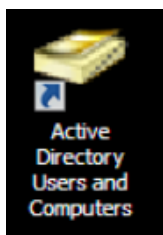
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

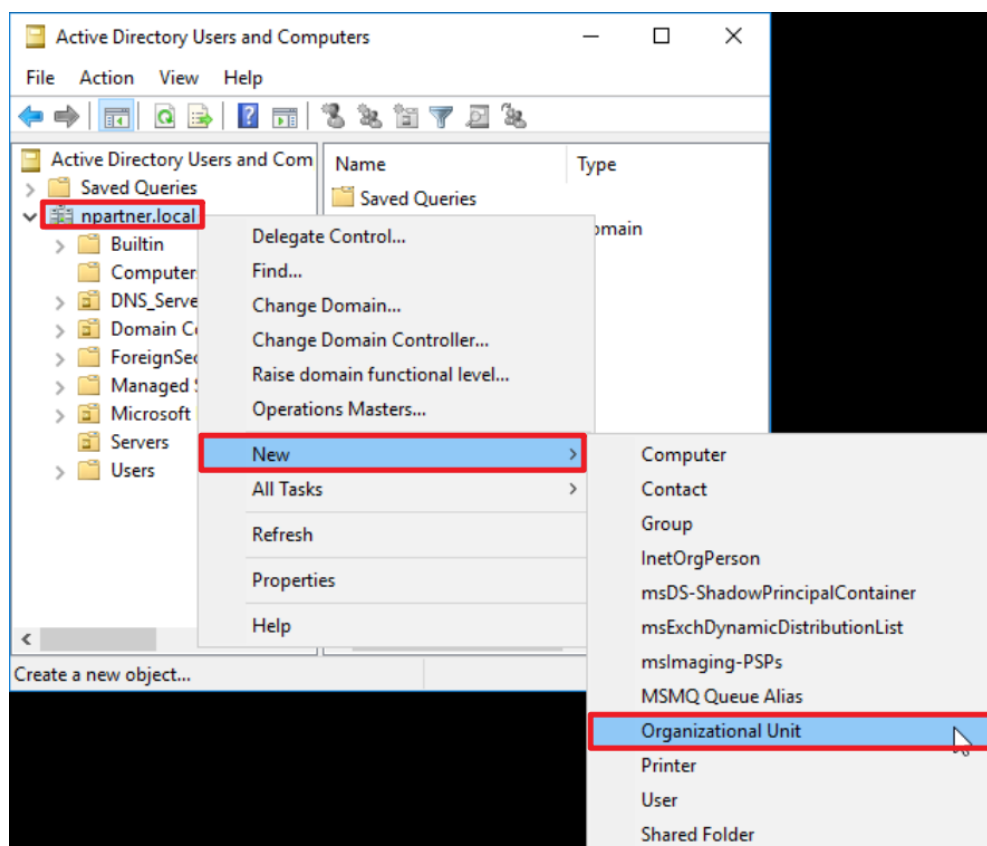
6.1.1 Organizational Unit (OU) Configuration

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



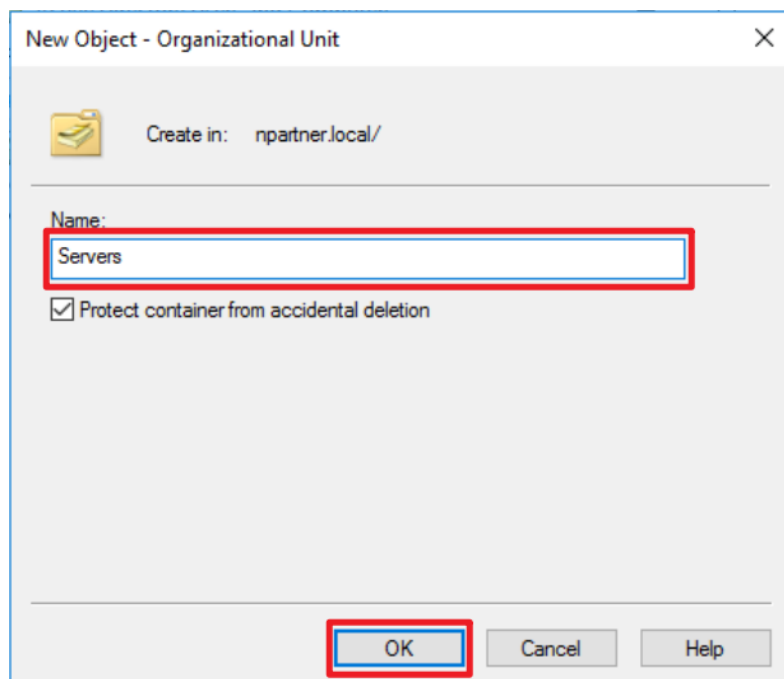
(2) Add an Organizational Unit

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”)

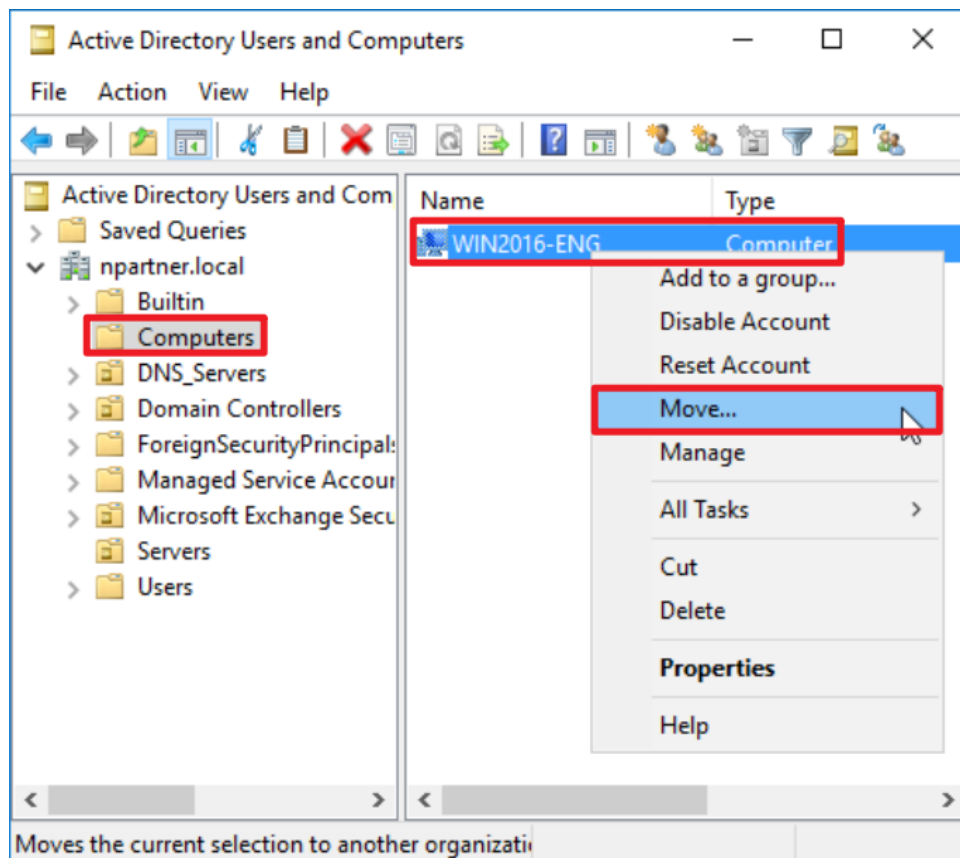
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

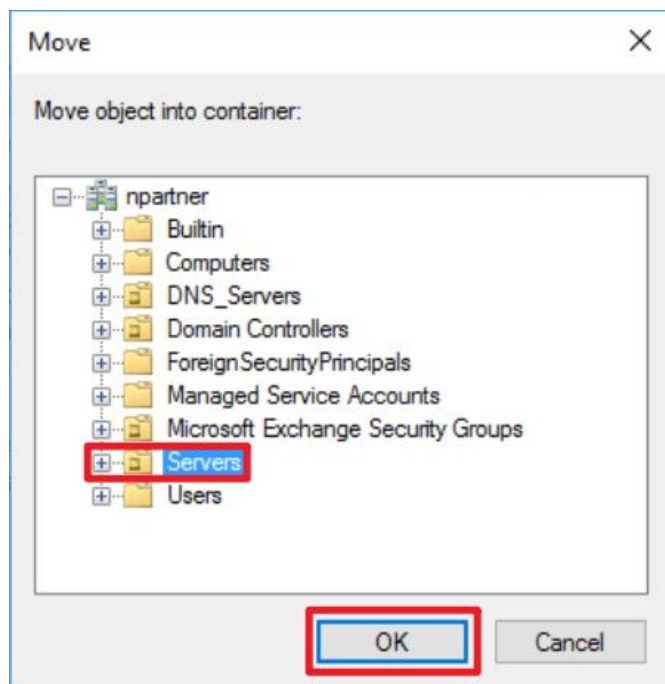
Select “Computers” organizational unit (OU) → right-click on the “WIN2016” server.

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



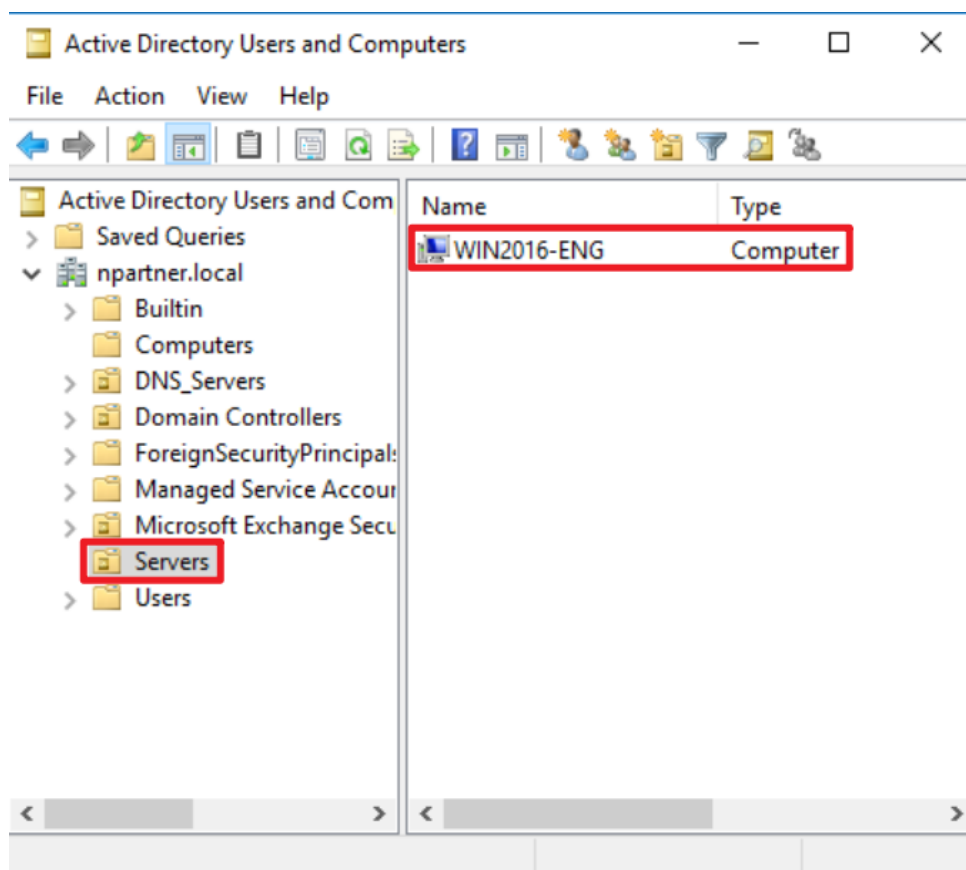
(5) Select your Organizational Unit:

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



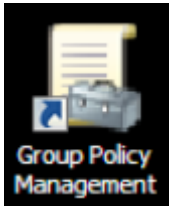
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



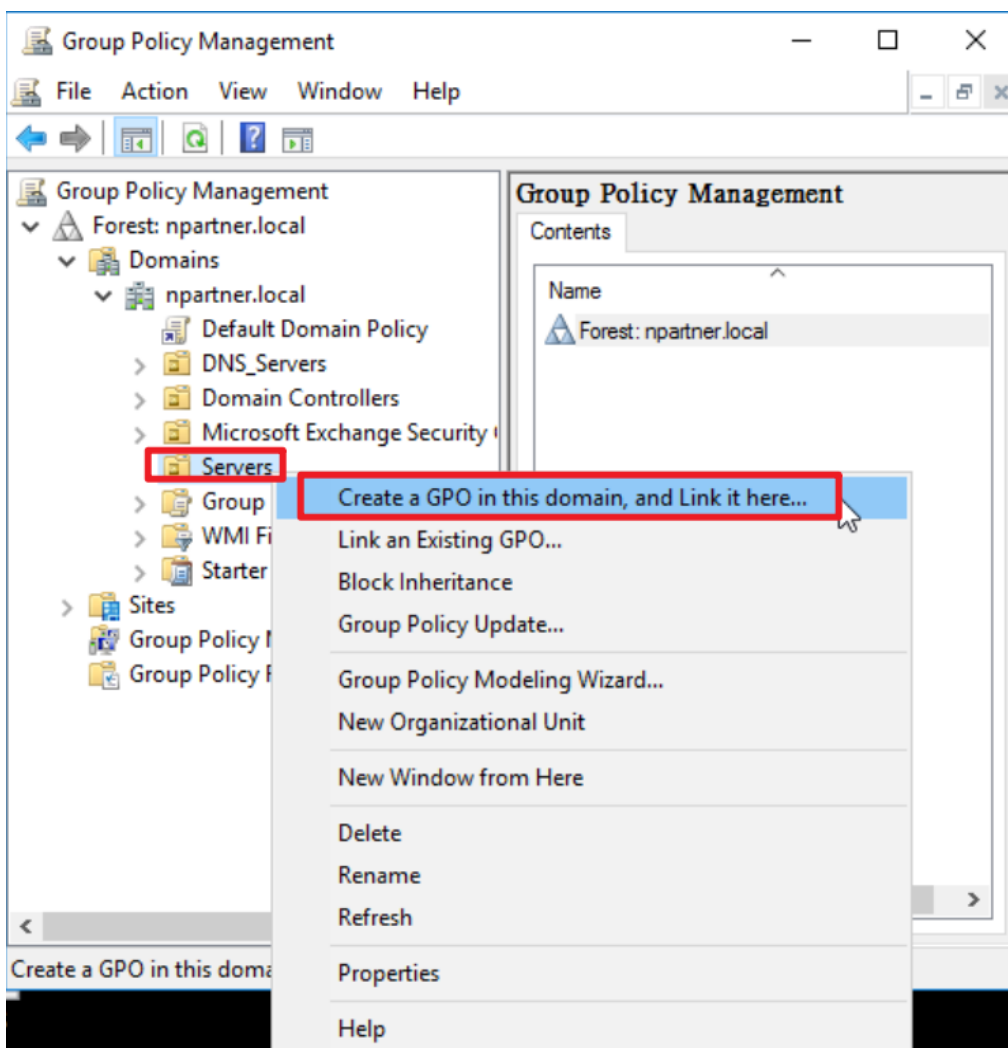
6.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

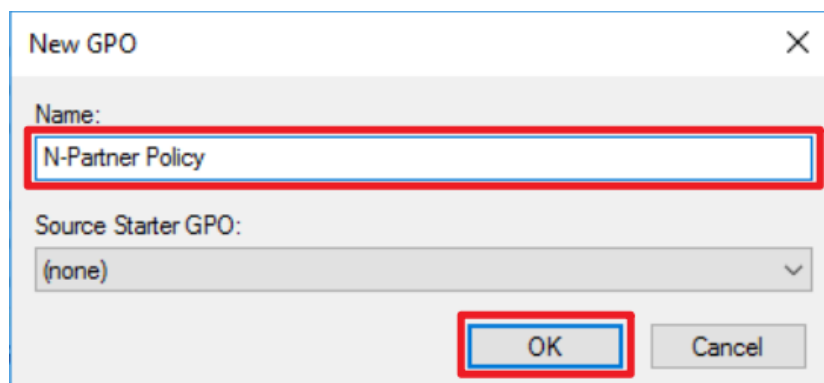
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

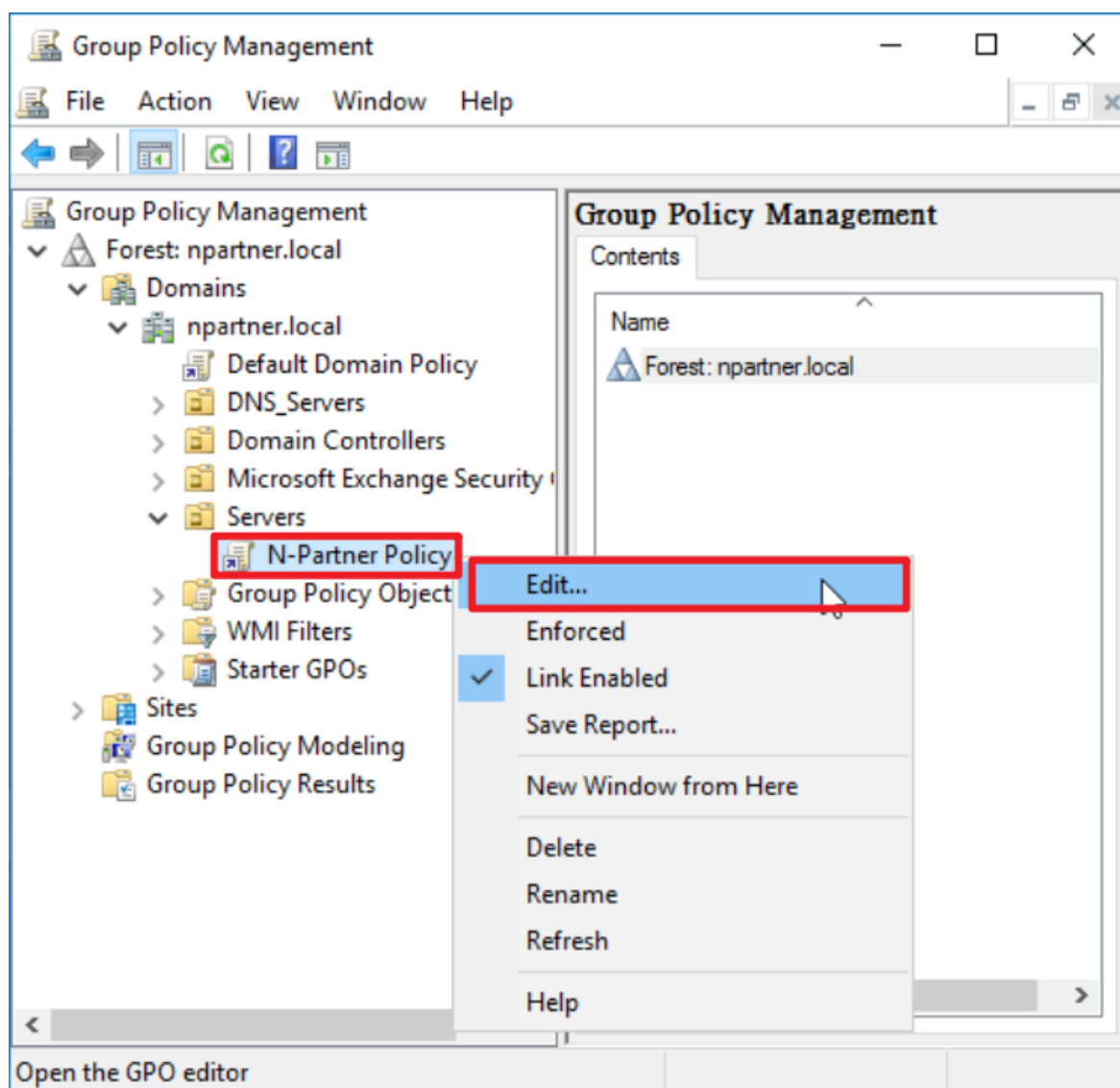
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



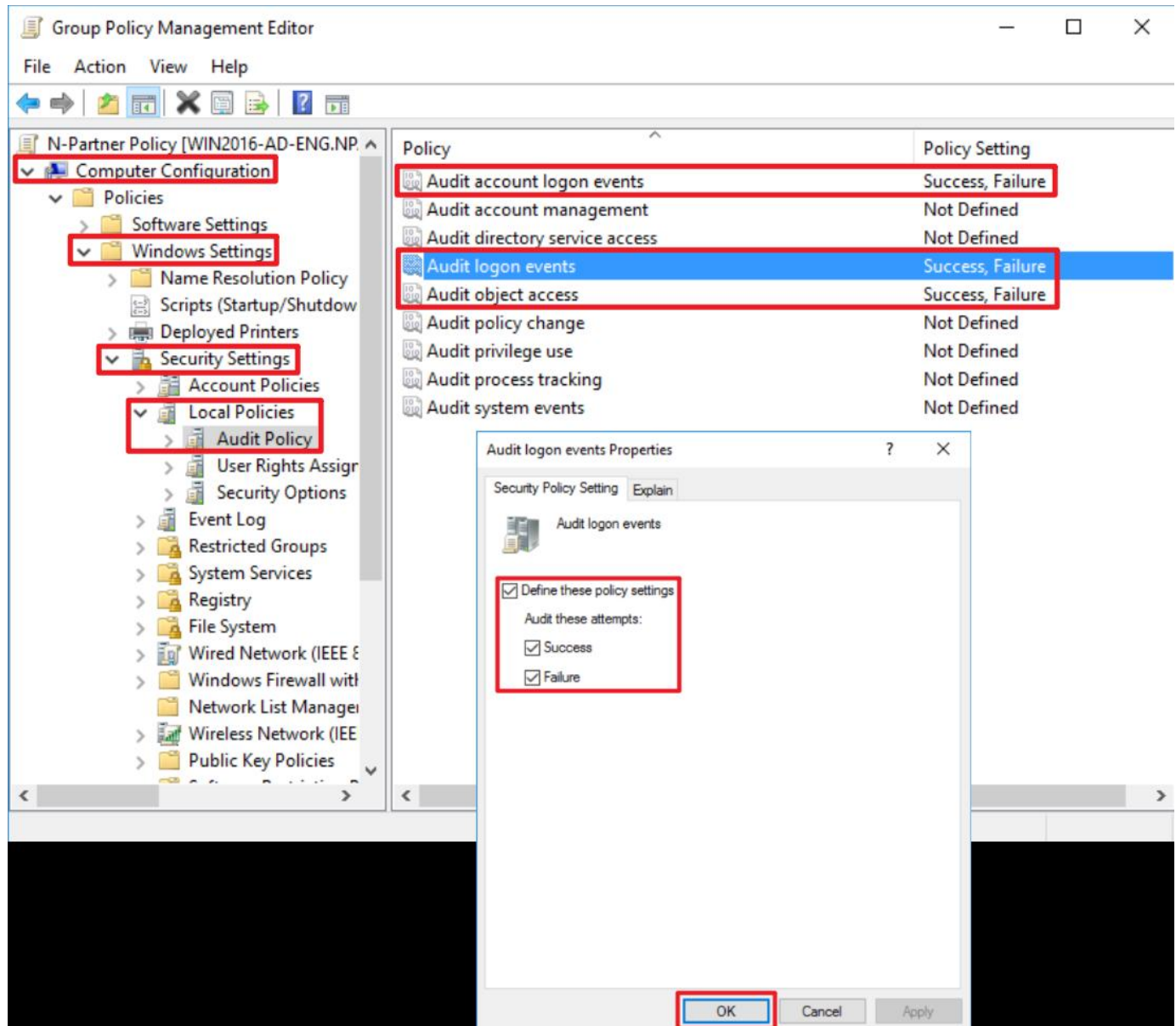
(4) Edit your Group Policy Object

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



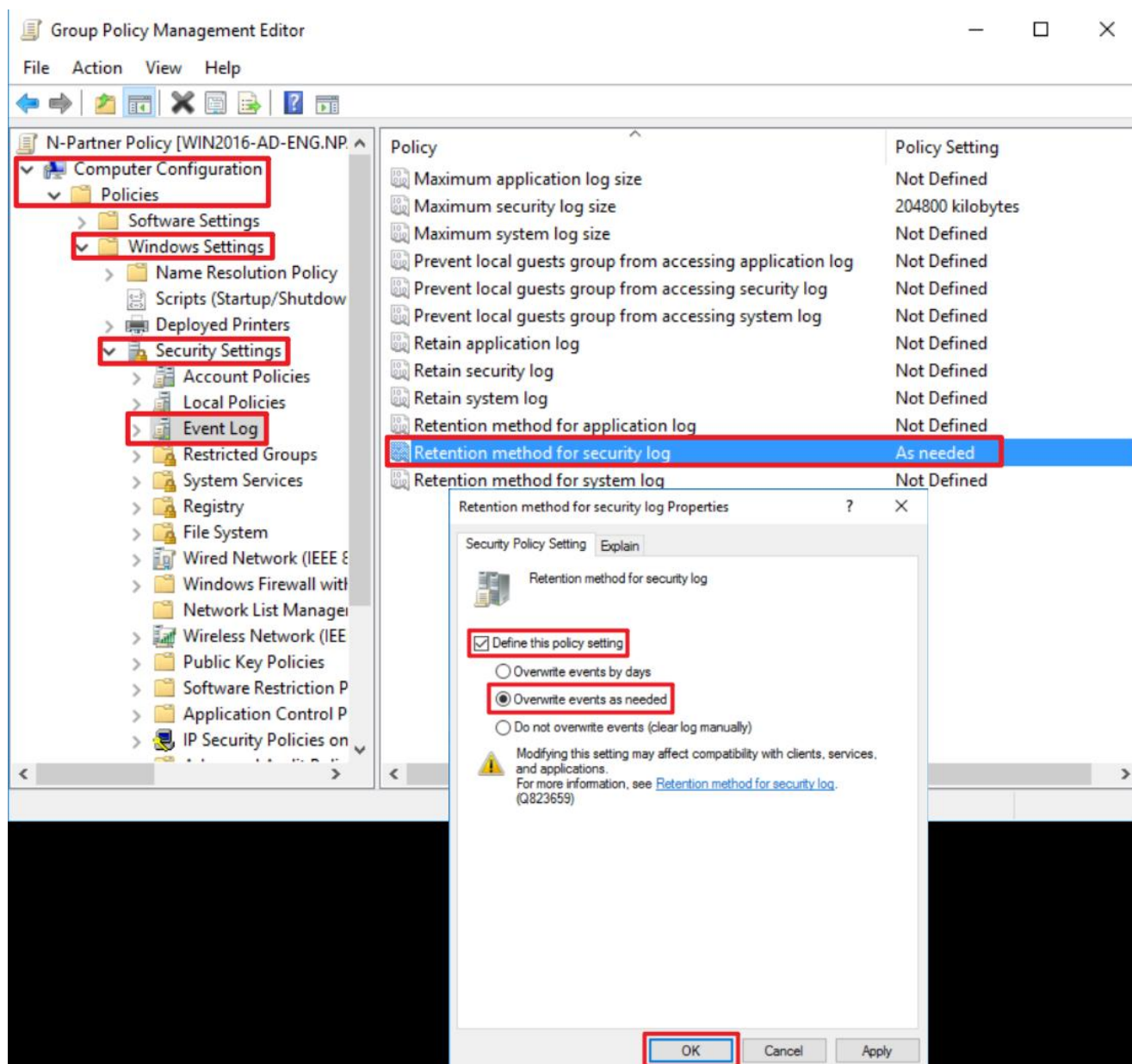
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

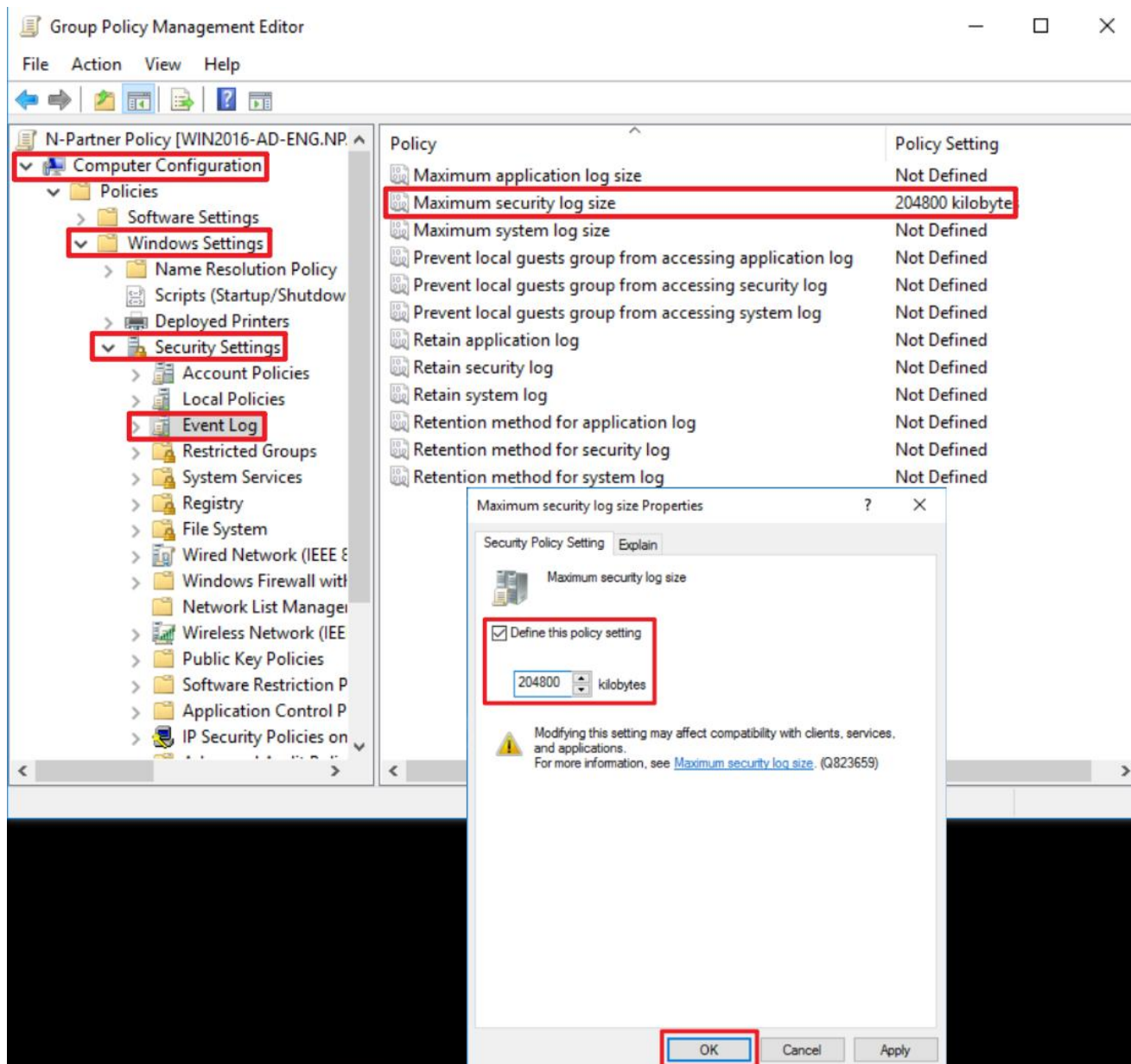
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

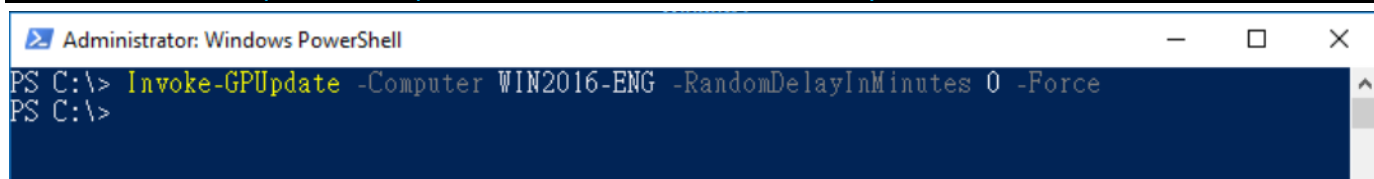


(8) On the AD domain server, open “Windows PowerShell.”



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

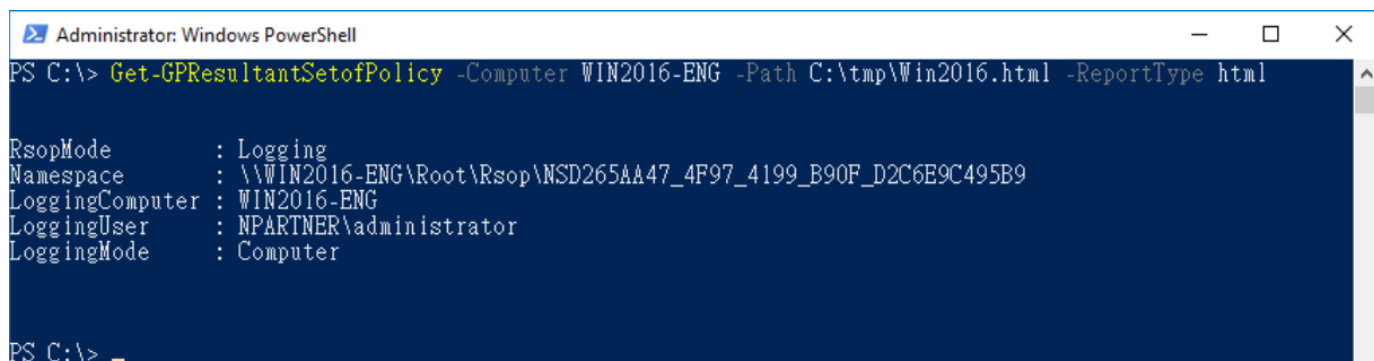
```
PS C:\> Invoke-GPUUpdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
```



Replace the text shown in red with the **Windows file server** name.

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

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-ENG -Path C:\tmp\SQL2016.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 File server is applying the N-Partner Policy Group Policy.

Group Policy Results

NPARTNER\WIN2016-ENG
Data collected on: 8/18/2025 PM 04:24:14 [show all](#)

Summary [show](#)

Computer Details [hide](#)

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](#)

Local Policies/Audit Policy [hide](#)

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy

Local Policies/Security Options [show](#)

Event Log [hide](#)

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

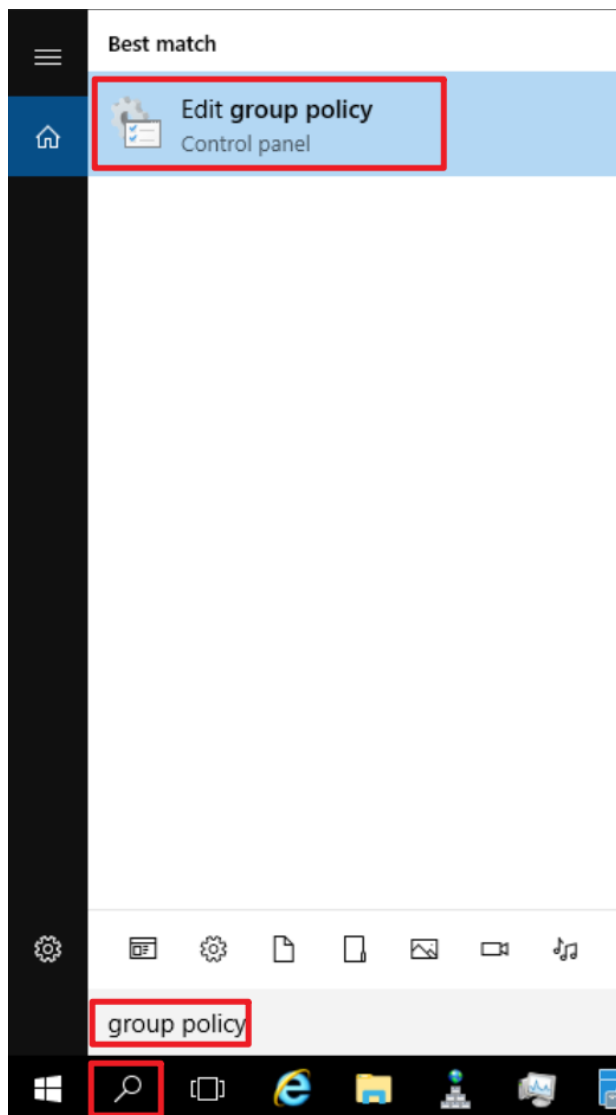
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings [show](#)

6.2 Workgroup

6.2.1 Audit Policy Configuration

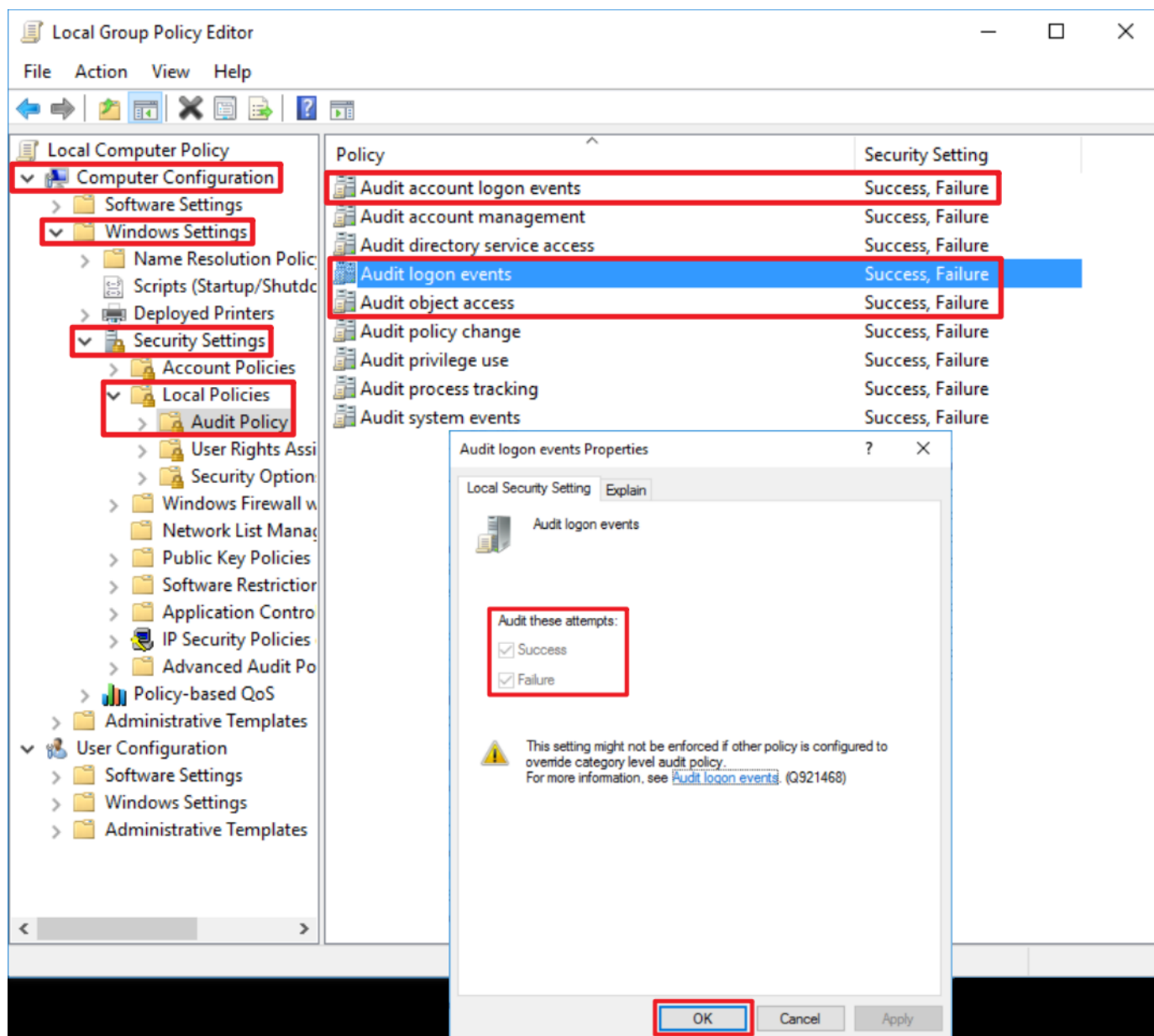
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) 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 logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”

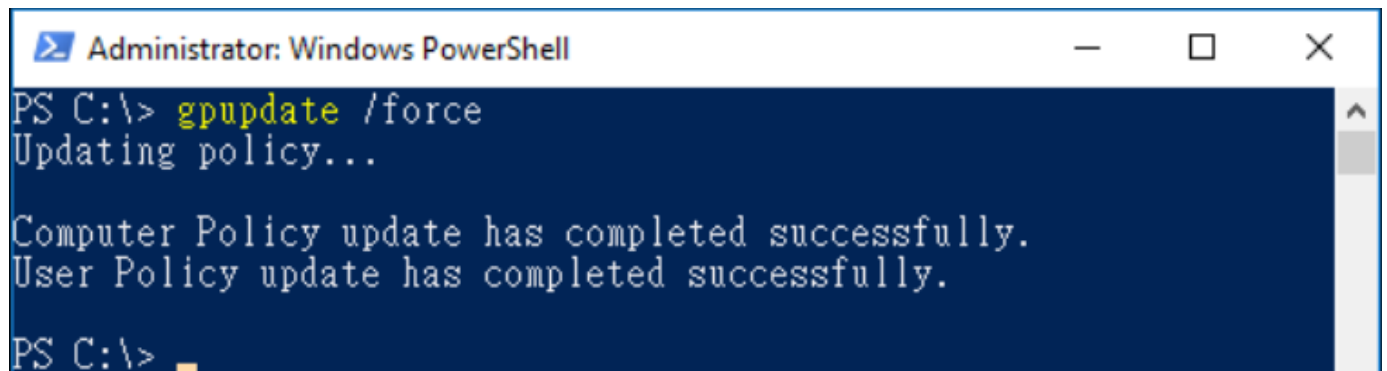


(3) Open “Windows PowerShell.”



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

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

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background and a white border. The command prompt shows the command "gpupdate /force" being entered. The output of the command is displayed in white text: "Updating policy...", "Computer Policy update has completed successfully.", and "User Policy update has completed successfully." The prompt "PS C:\>" is visible at the bottom of the window.

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

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

PS C:\>
```

(5) Enter the command below to view group policy applied status.

PS C:\> **auditpol /get /category:***

```

Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
  User / Device Claims         Success and Failure
  Group Membership             Success and Failure
Object Access
  File System                  Success and Failure
  Registry                    Success and Failure
  Kernel Object                Success and Failure
  SAM                         Success and Failure
  Certification Services       Success and Failure
  Application Generated         Success and Failure
  Handle Manipulation           Success and Failure
  File Share                    Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events    Success and Failure
  Detailed File Share           Success and Failure
  Removable Storage             Success and Failure
  Central Policy Staging        Success and Failure
Privilege Use
  Non Sensitive Privilege Use   Success and Failure
  Other Privilege Use Events     Success and Failure
  Sensitive Privilege Use       Success and Failure
Detailed Tracking
  Process Creation              Success and Failure
  Process Termination           Success and Failure
  DPAPI Activity                Success and Failure
  RPC Events                    Success and Failure
  Plug and Play Events          Success and Failure
  Token Right Adjusted Events   Success and Failure
Policy Change
  Audit Policy Change           Success and Failure
  Authentication Policy Change  Success and Failure
  Authorization Policy Change   Success and Failure
  MPSSVC Rule-Level Policy Change Success and Failure
  Filtering Platform Policy Change Success and Failure
  Other Policy Change Events     Success and Failure
Account Management
  Computer Account Management    Success and Failure
  Security Group Management      Success and Failure
  Distribution Group Management  Success and Failure
  Application Group Management   Success and Failure
  Other Account Management Events Success and Failure
  User Account Management        Success and Failure
DS Access
  Directory Service Access       Success and Failure
  Directory Service Changes      Success and Failure
  Directory Service Replication  Success and Failure
  Detailed Directory Service Replication Success and Failure
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events     Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation           Success and Failure
PS C:\>

```

6.2.2 Event Log Settings

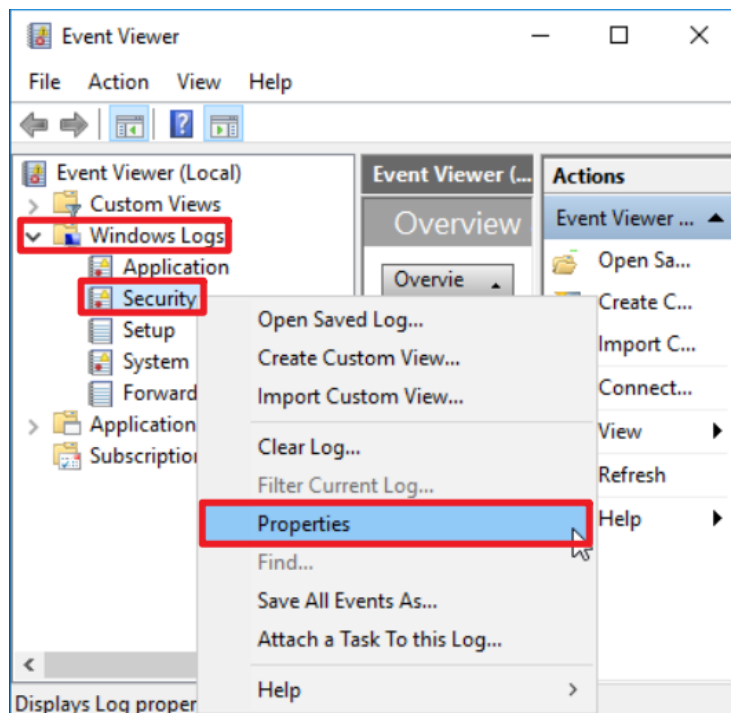
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “[Event Viewer](#)” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Security” → And click on “Properties.”

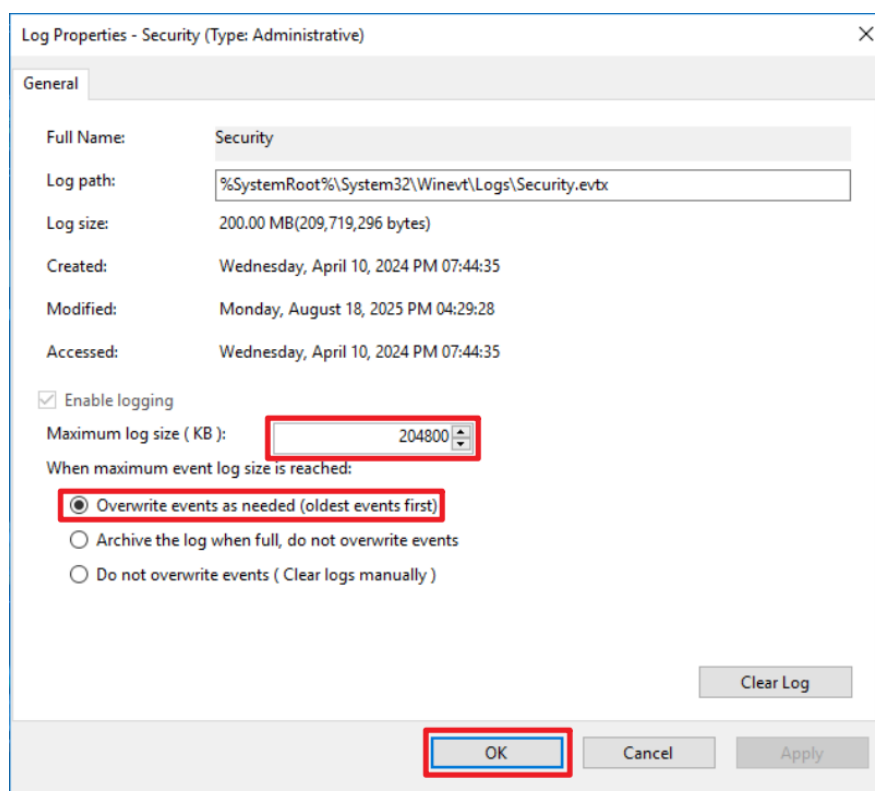


(3) Configure Security Log

Enter maximum log file size: 204800 KB

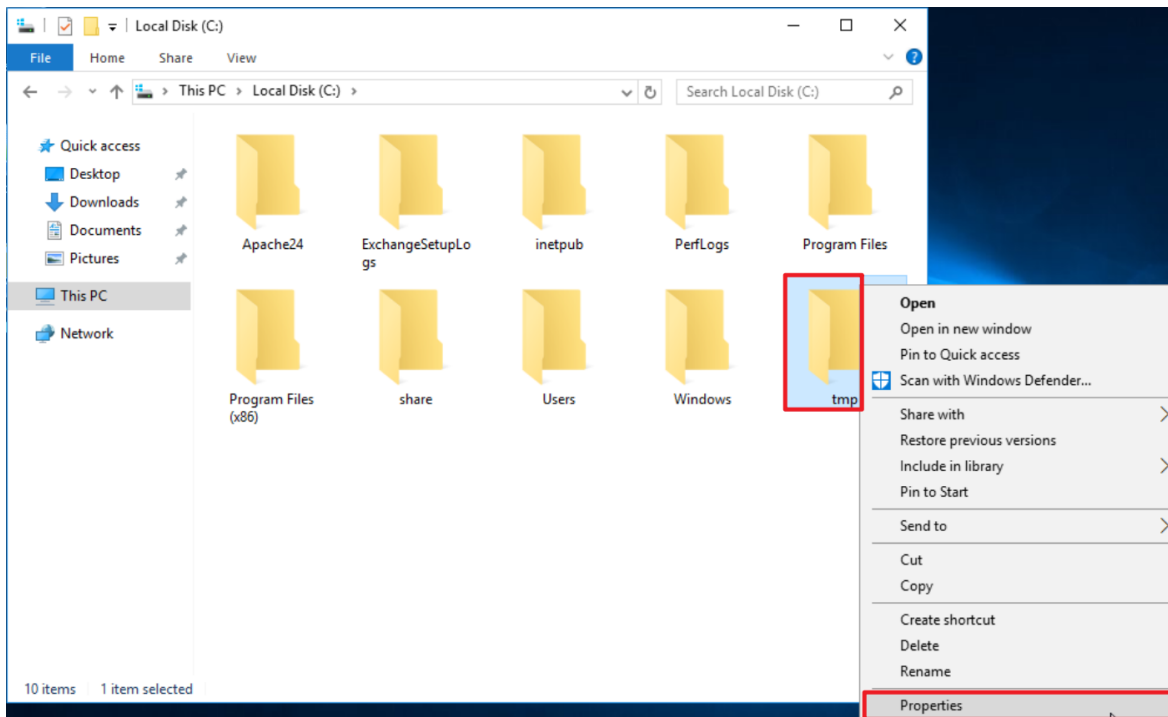
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”

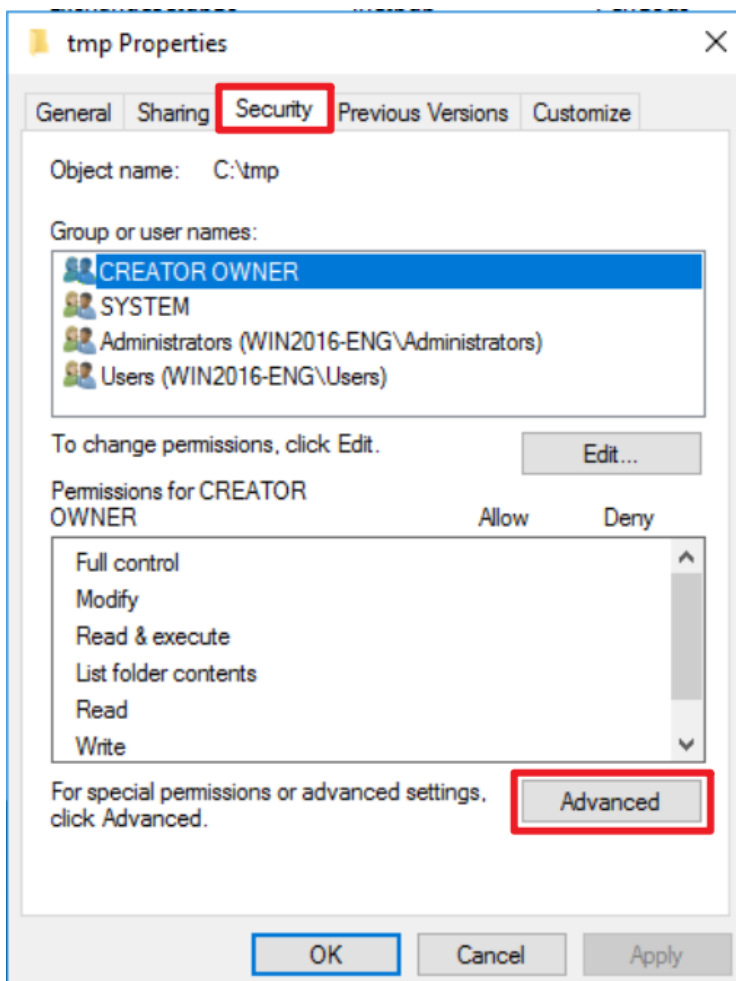


6.3 Folder Audit Configuration

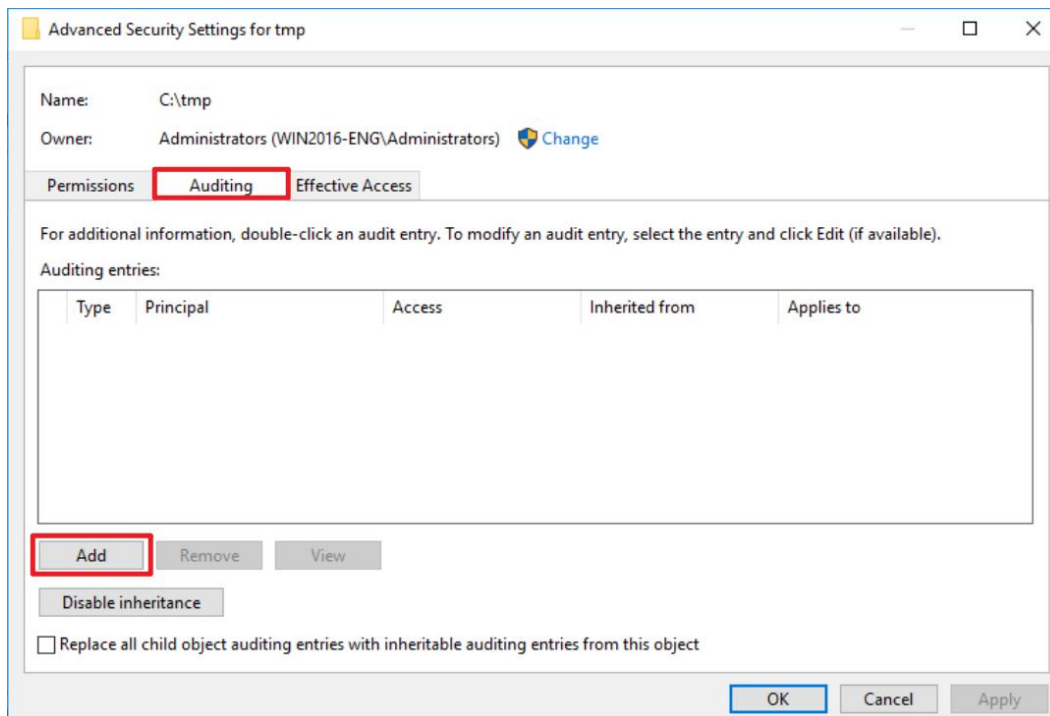
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



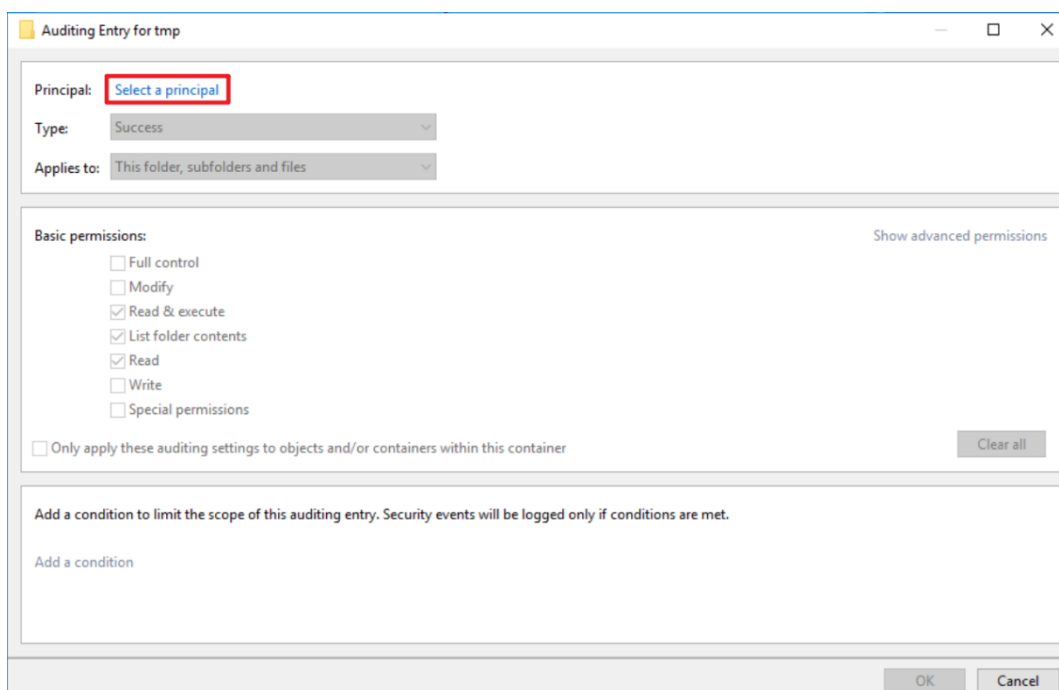
(2) Go to the “Security” tab → click “Advanced.”



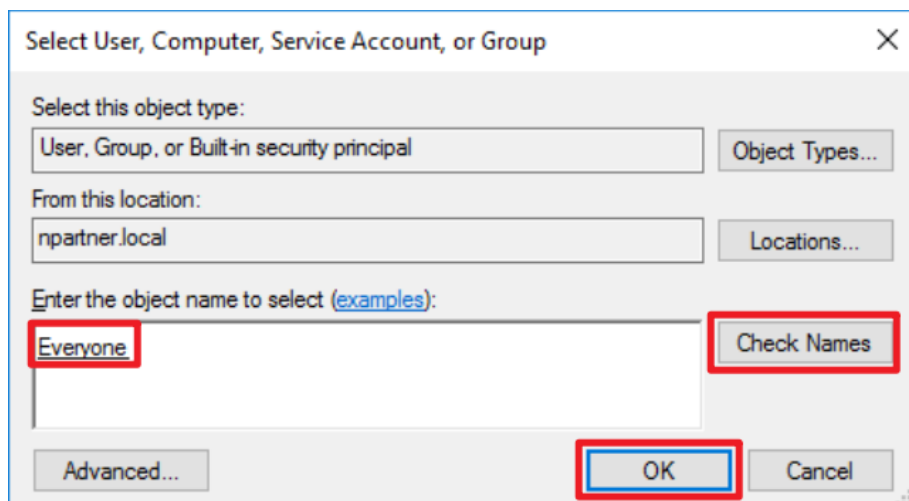
(3) Open the “Auditing” tab → click “Add.”



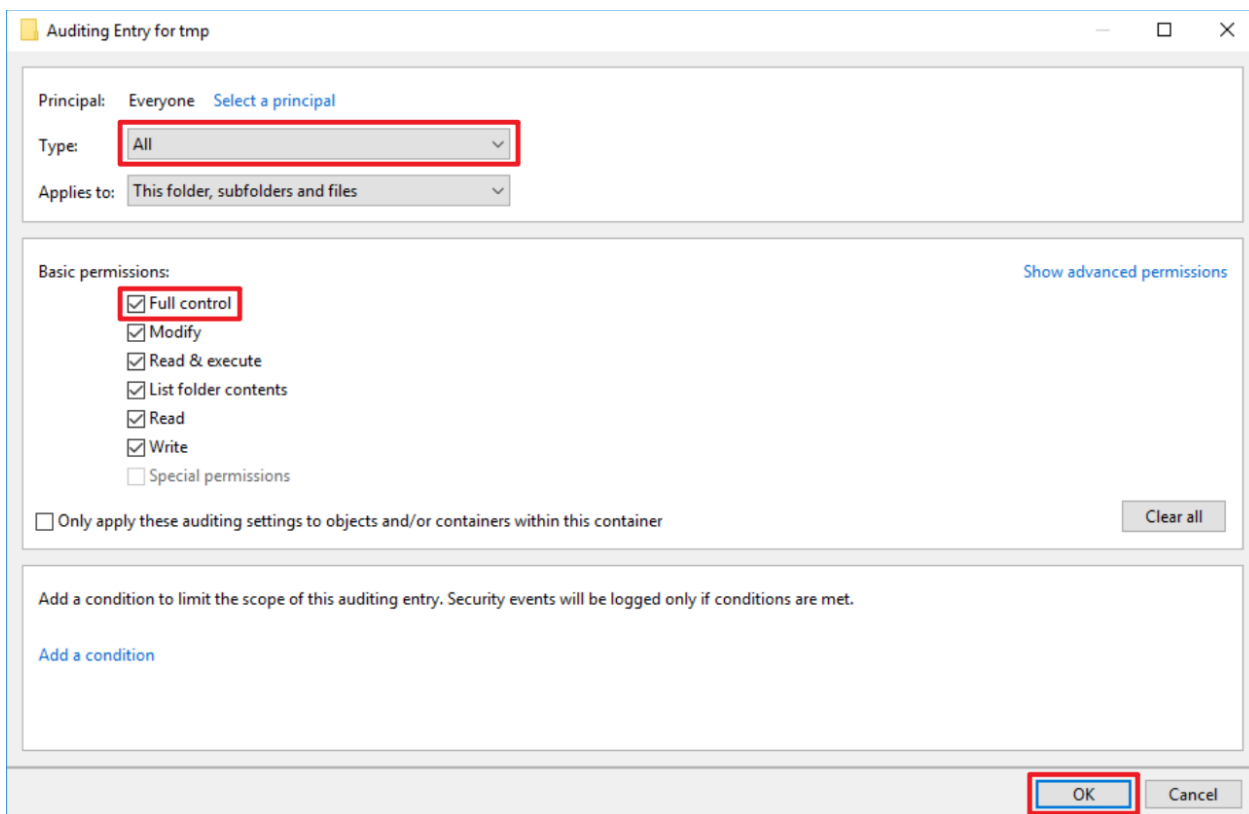
(4) Click “Select a principal.”



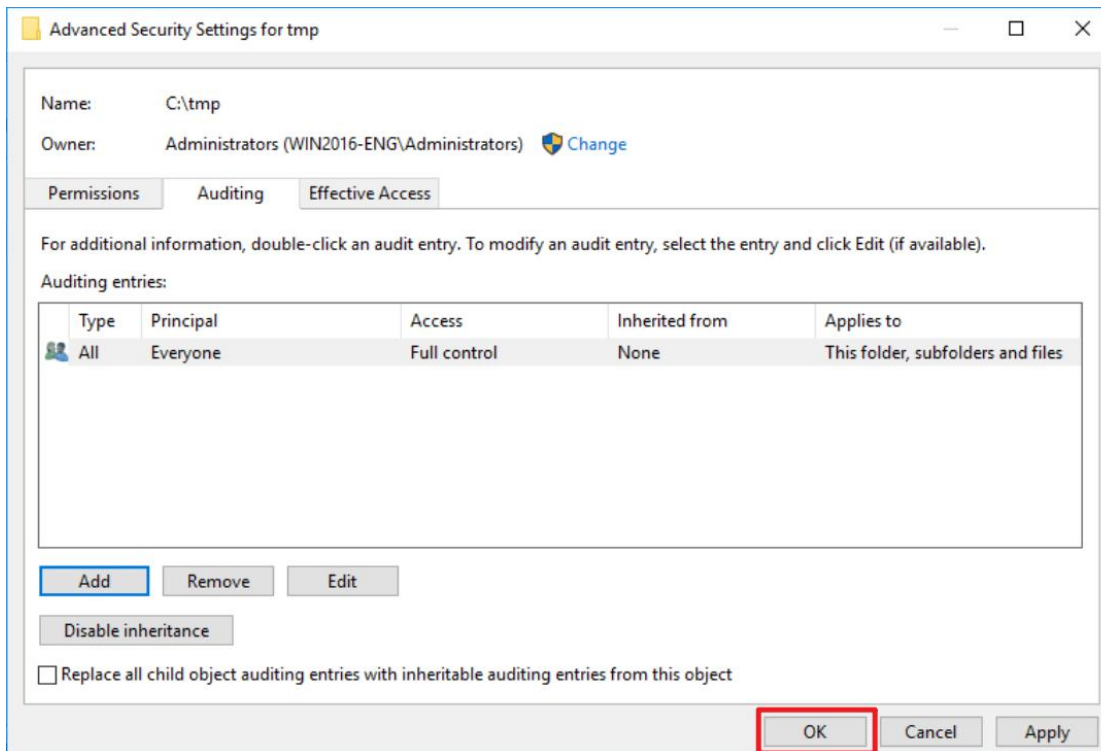
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



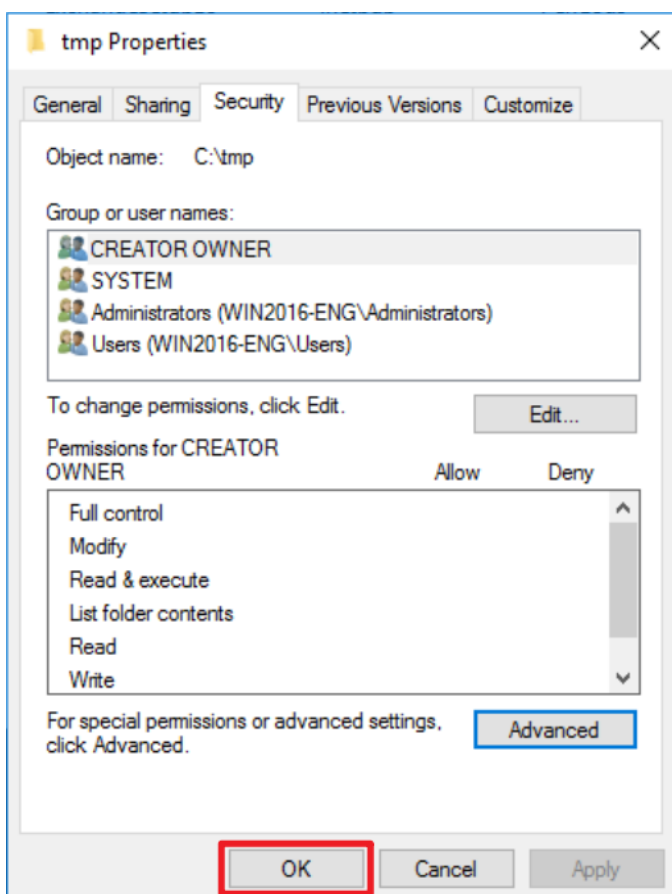
(6) Select “All” in type → enable “Full Control” → click “OK.”



(7) Confirm that the auditing entries shows “Everyone” → click “OK.”



(8) Click “OK” again to confirm and close.



7. Windows Server 2019

7.1 Domain

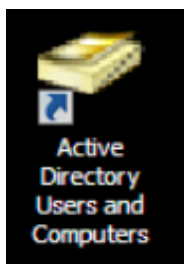
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

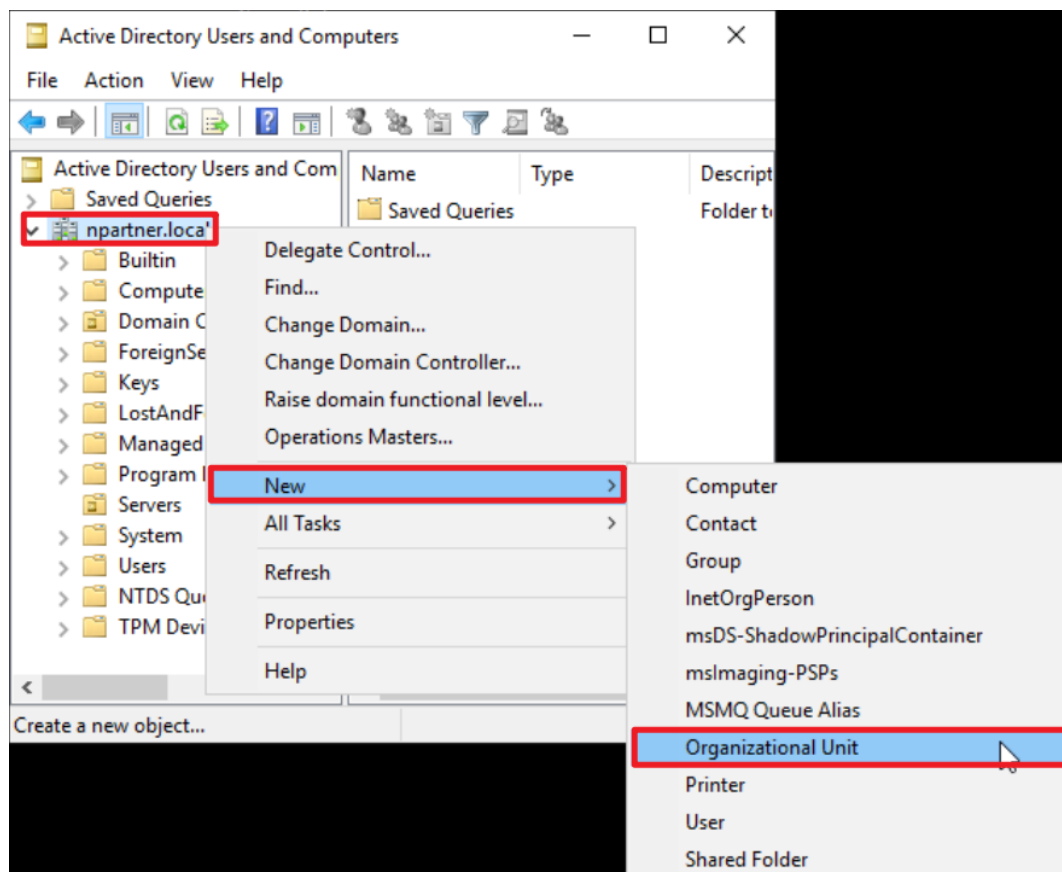
7.1.1 Organizational Unit (OU) Configuration

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



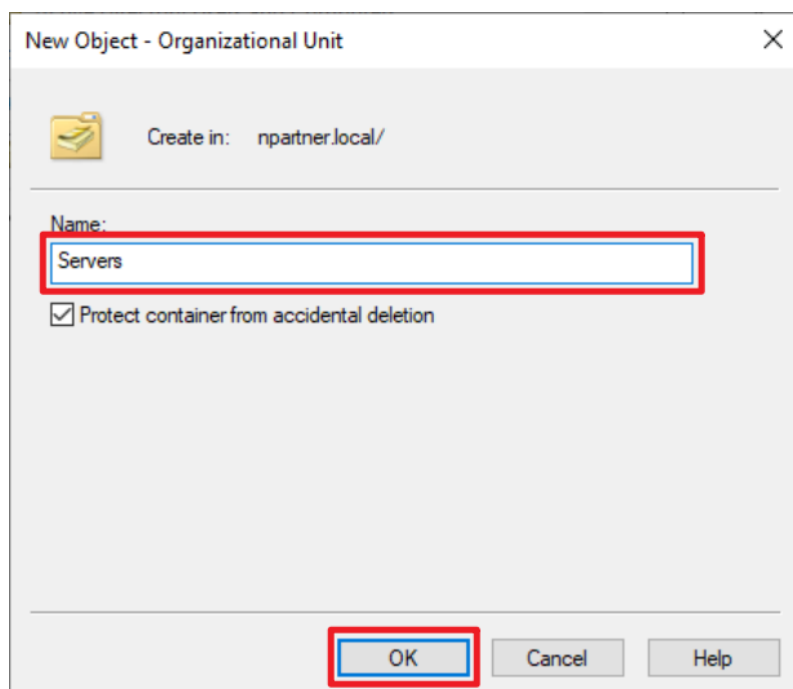
(2) Add an Organizational Unit

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”)

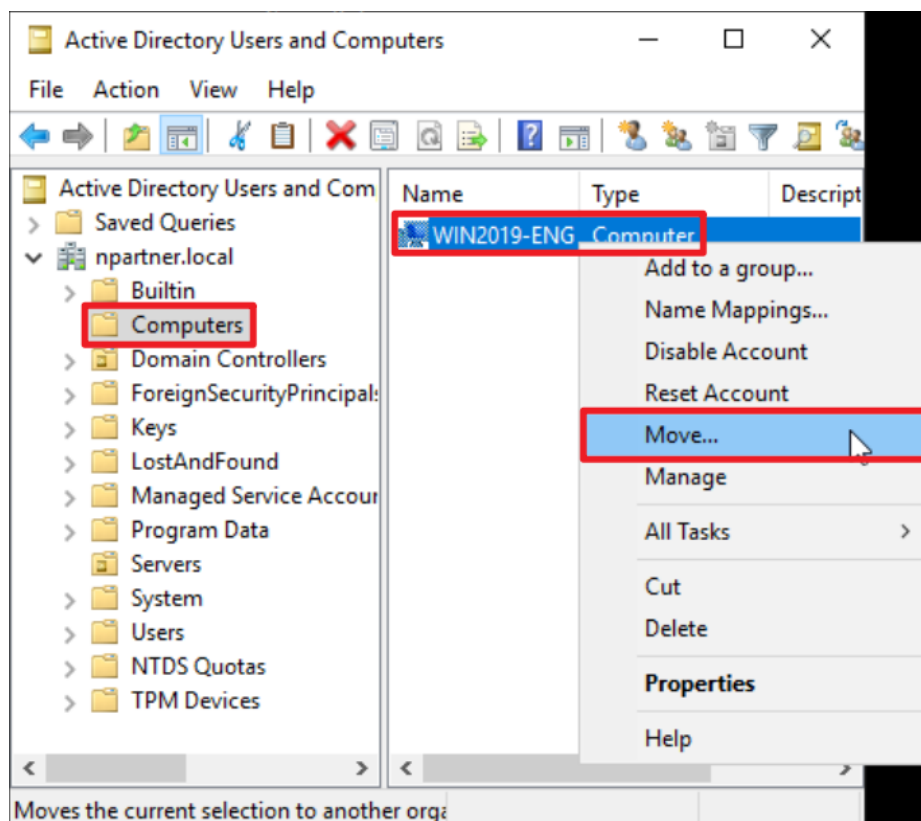
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

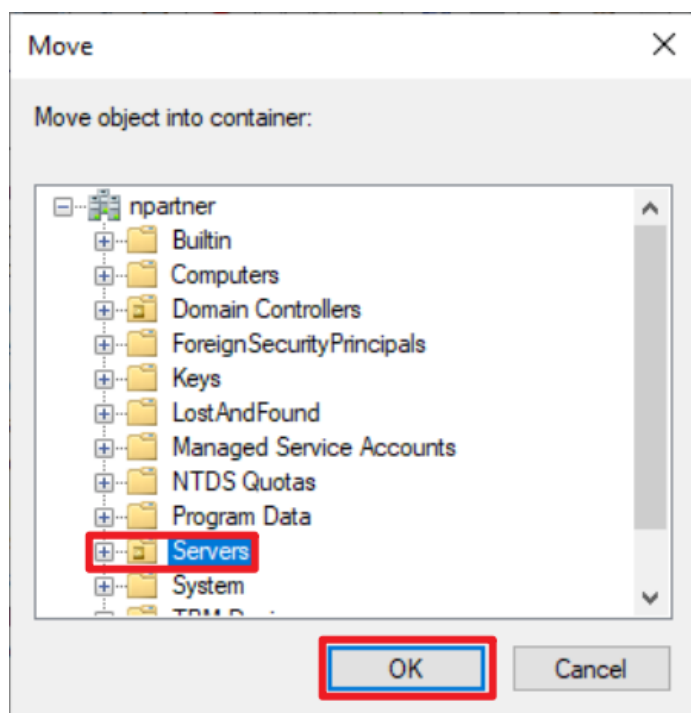
Select the “Computers” organizational unit (OU) → right-click on the “WIN2019-ENG” server.

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



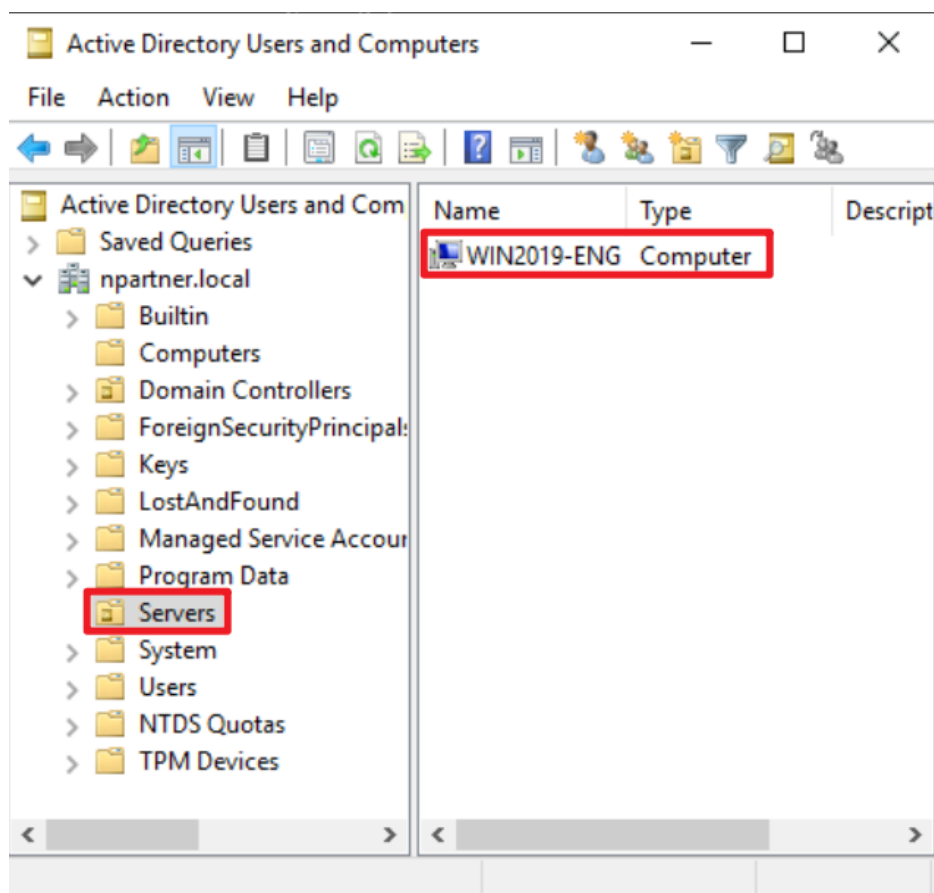
(5) Select your Organizational Unit:

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



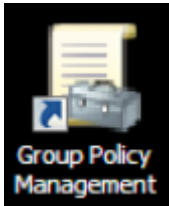
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



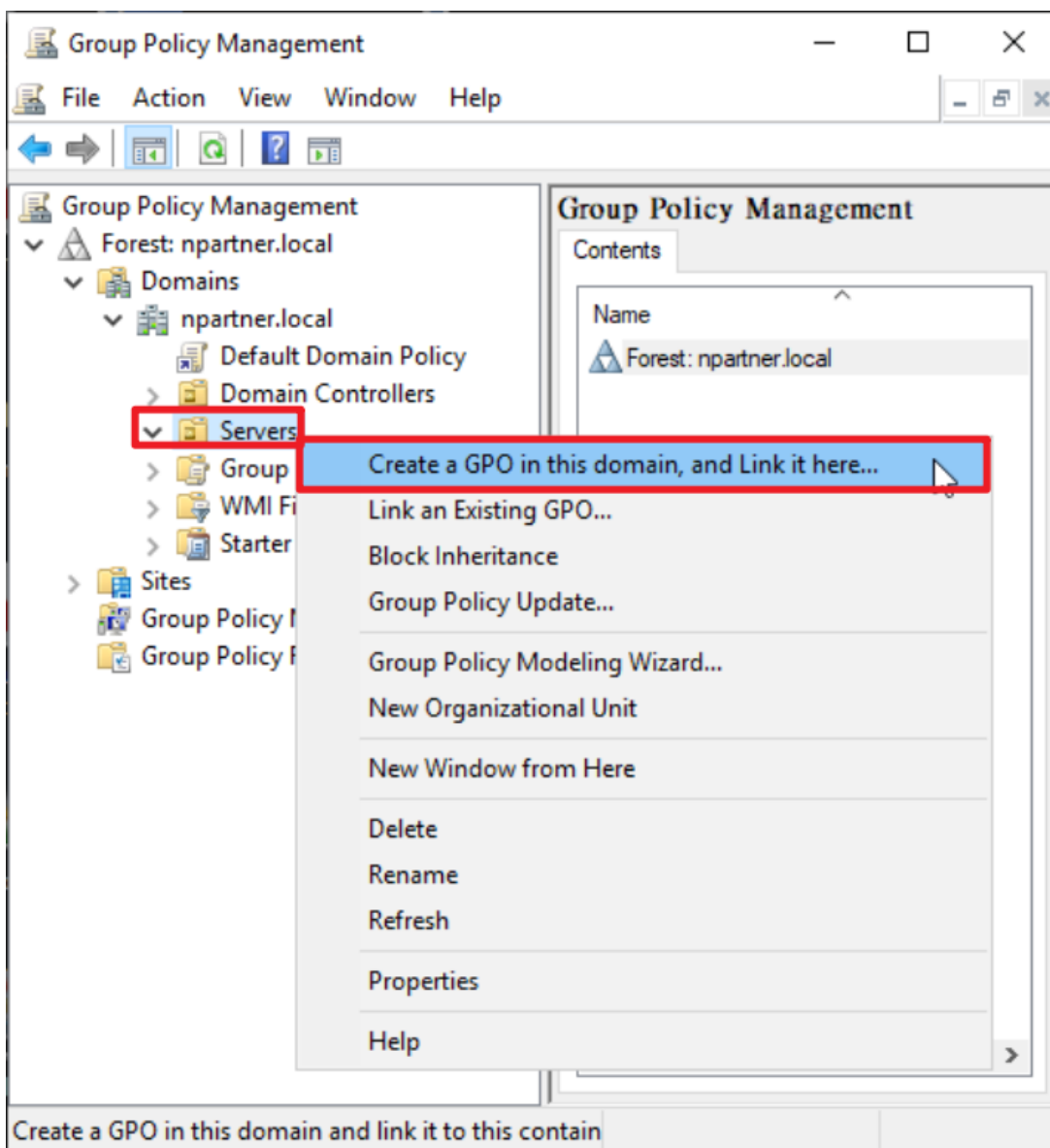
7.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

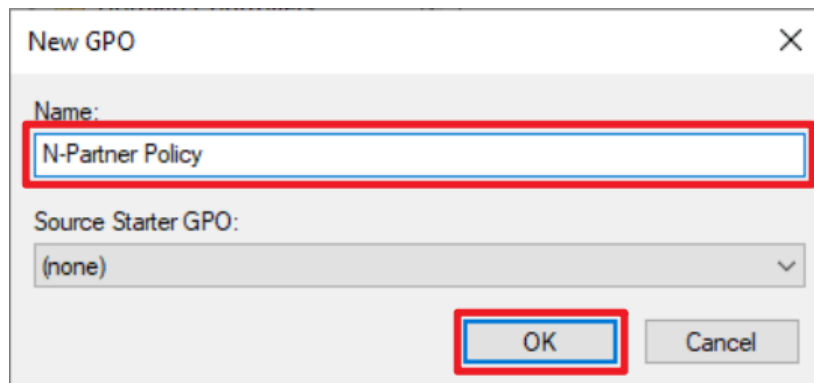
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Enter your Group Policy Object

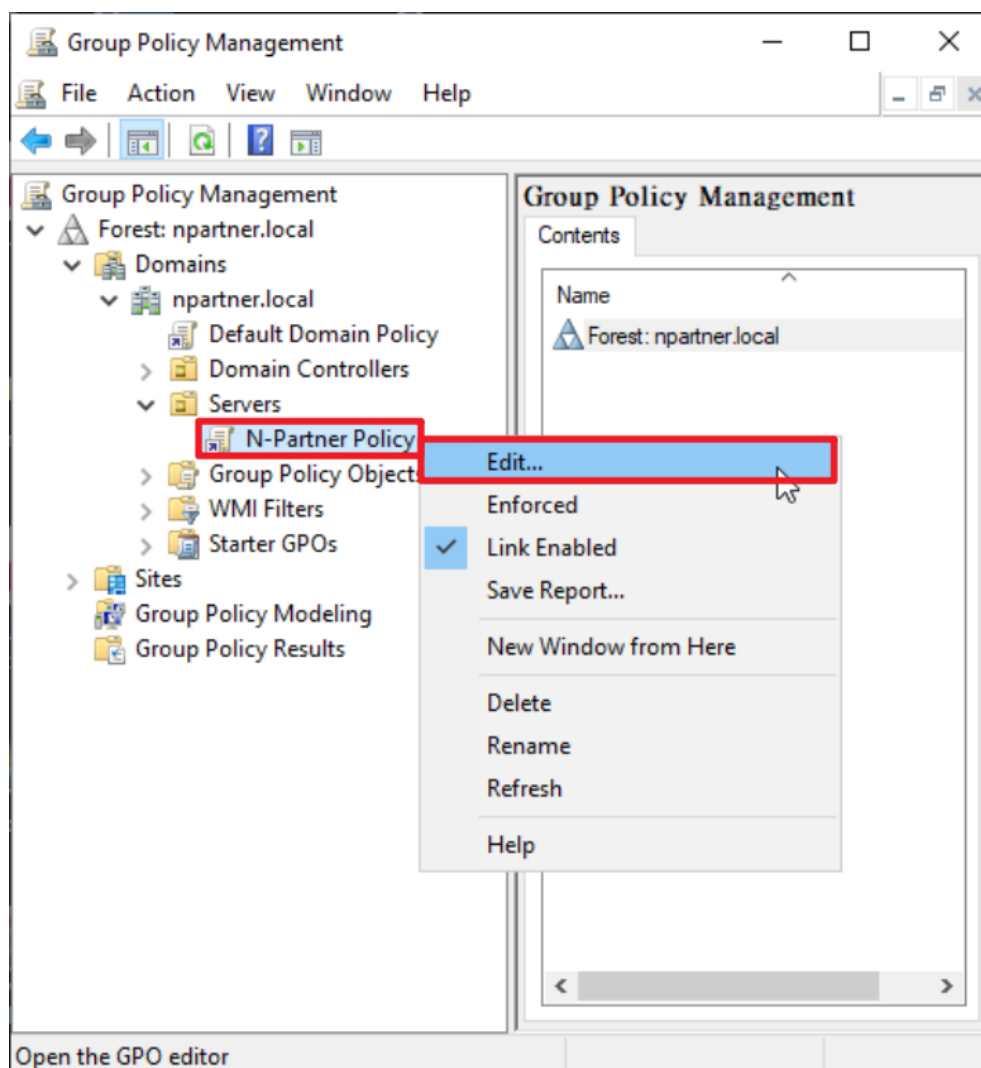
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



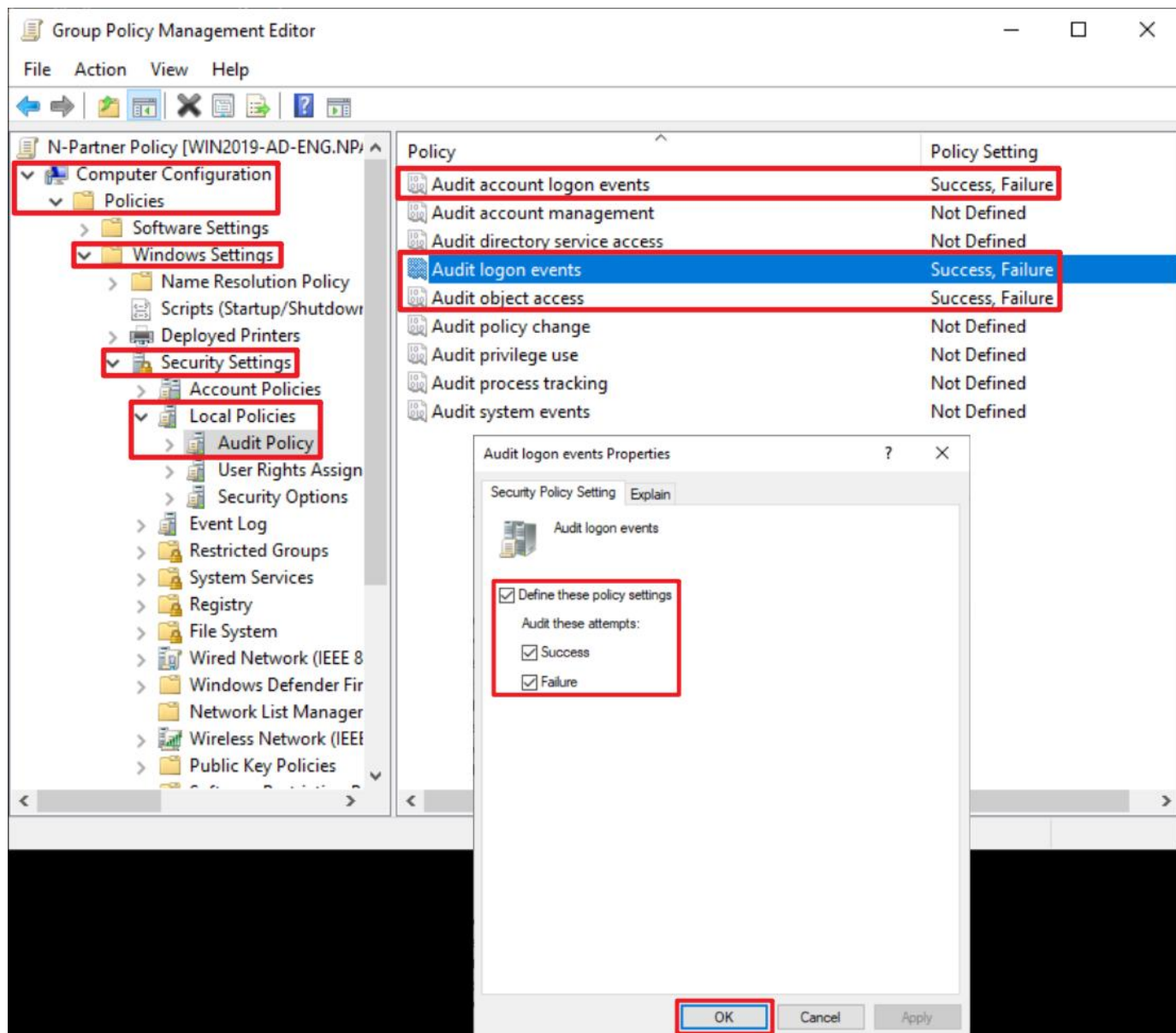
(4) Edit your Group Policy Object

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



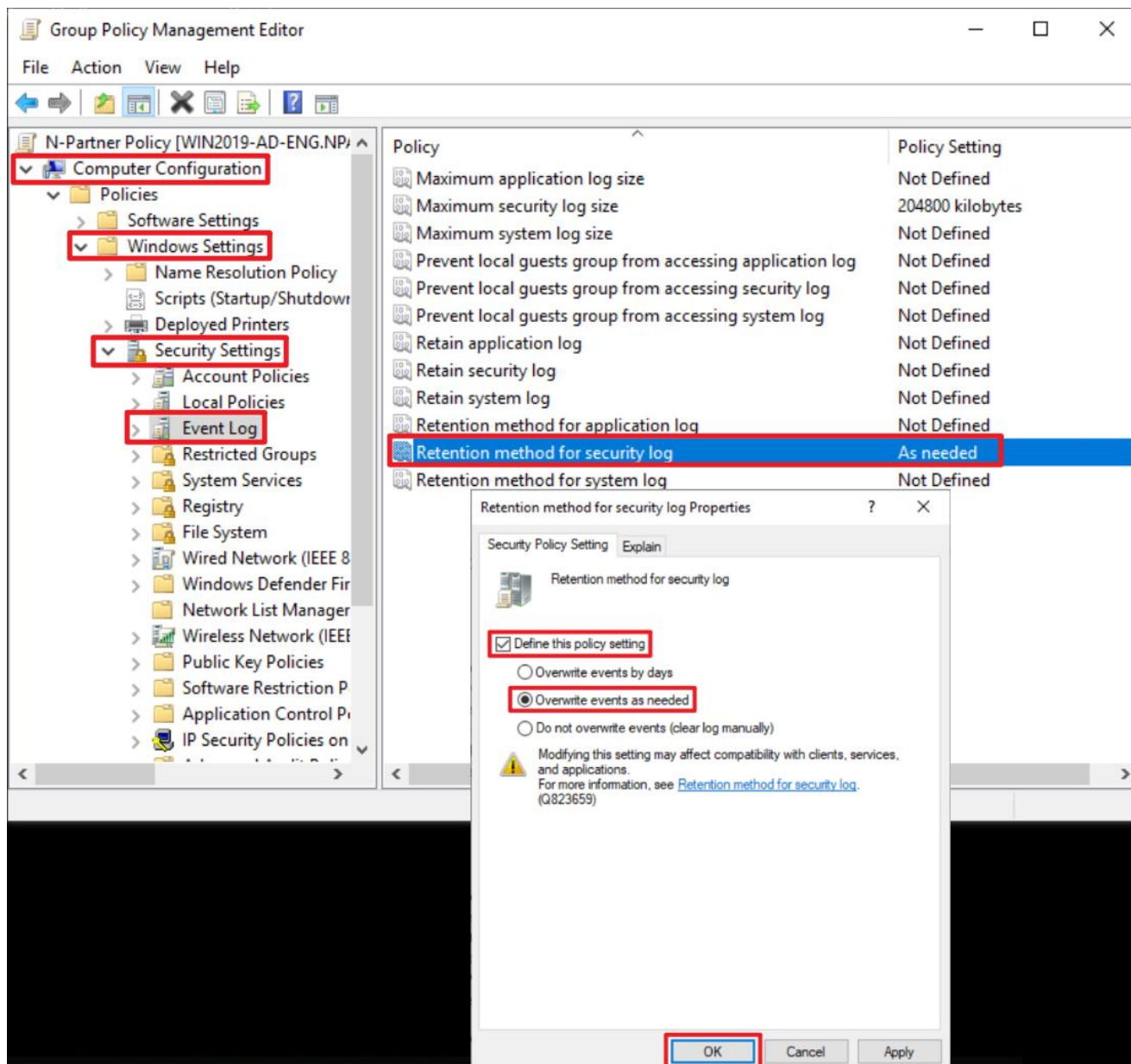
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

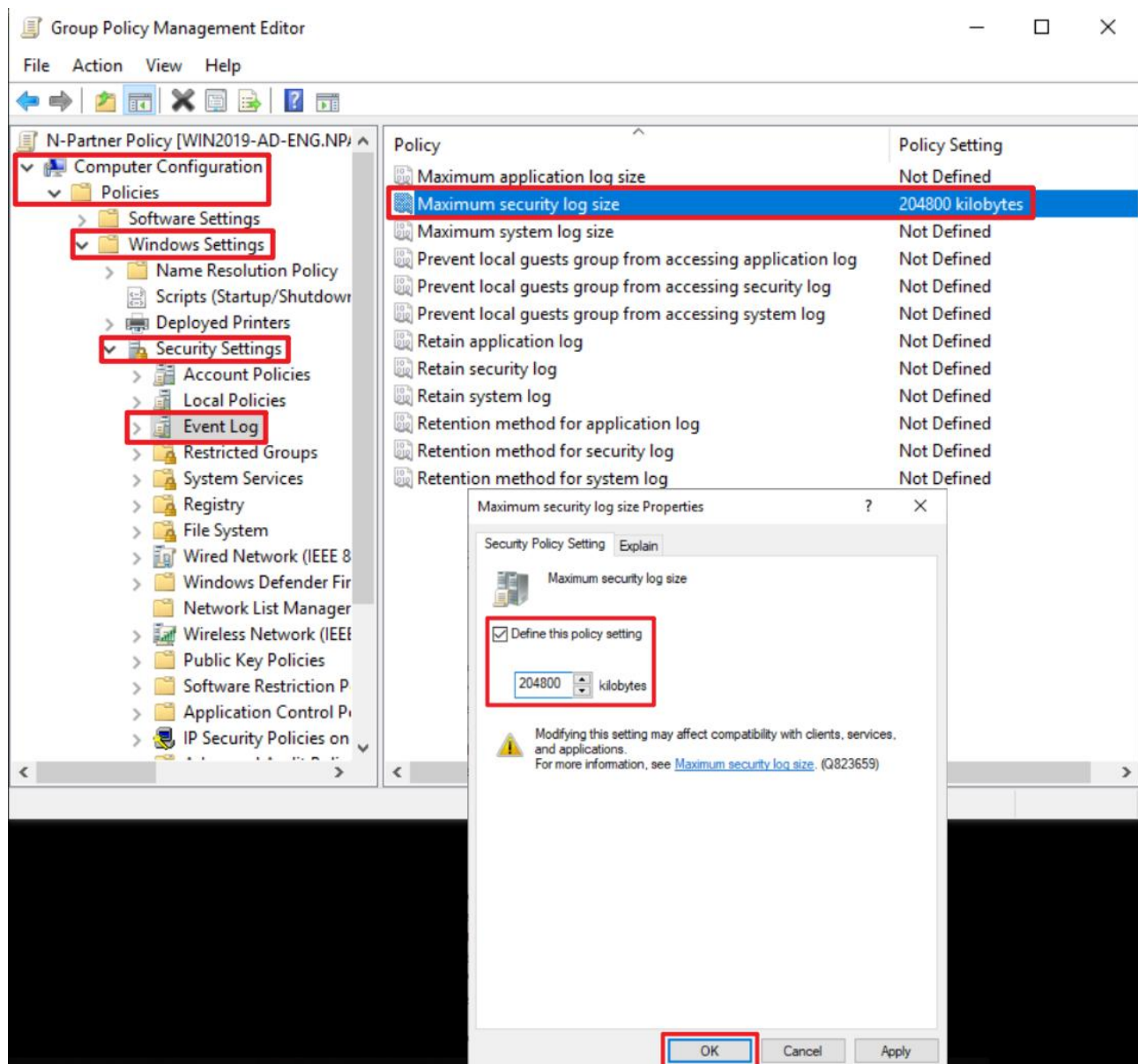
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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-GPUUpdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `Invoke-GPUUpdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt returns to `PS C:\>`.

Replace the text shown in red with the Windows File server name.

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

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\SQL2019.html -ReportType.html
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `Get-GPResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\Win2019.html -ReportType html` being entered and executed. The output displays the following information:
RsopMode : Logging
Namespace : \\WIN2019-ENG\Root\Rsop\NS05A8F953_3BD1_457A_A211_6C03568D96B7
LoggingComputer : WIN2019-ENG
LoggingUser : NPARTNER\administrator
LoggingMode : Computer
The prompt then returns to `PS C:\>`.

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 file server is applying the N-Partner Policy Group Policy.

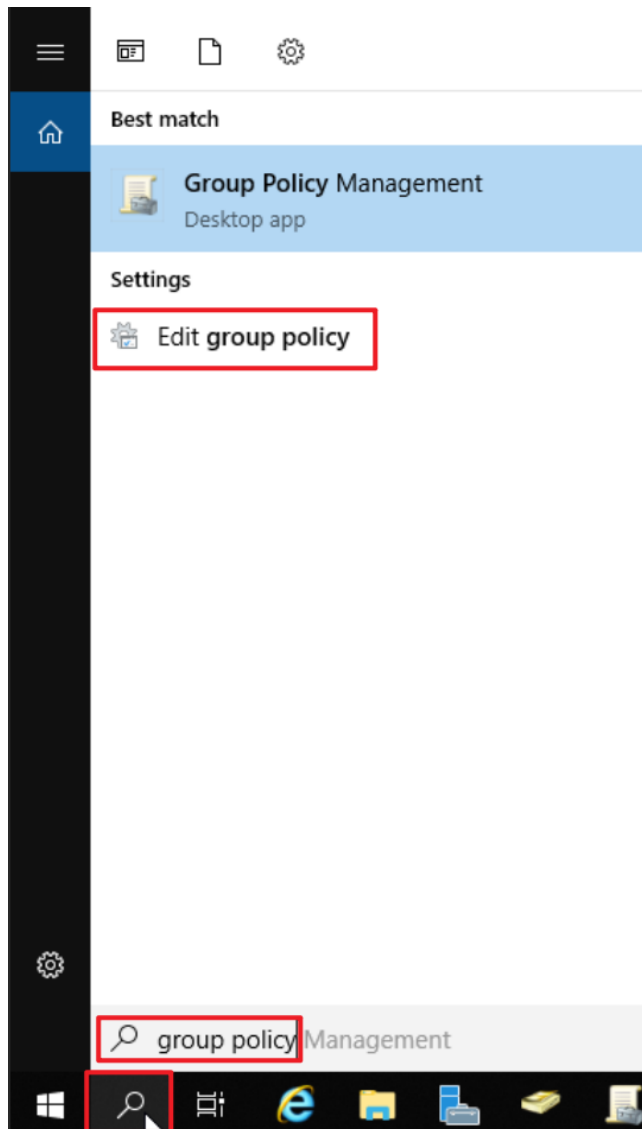
Group Policy Results		
NPARTNER\WIN2016-ENG		
Data collected on: 8/13/2025 PM 02:27:06		
show all		
Summary		
show		
Computer Details		
hide		
General		
show		
Component Status		
show		
Settings		
hide		
Policies		
hide		
Windows Settings		
hide		
Security Settings		
hide		
Account Policies/Password Policy		
show		
Account Policies/Account Lockout Policy		
show		
Local Policies/Audit Policy		
hide		
Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Local Policies/User Rights Assignment		
show		
Local Policies/Security Options		
show		
Event Log		
hide		
Policy	Setting	Winning GPO
Maximum application log size	204800 kilobytes	N-Partner Policy
Retention method for application log	As needed	N-Partner Policy

7.2 Workgroup

7.2.1 Audit Policy Configuration

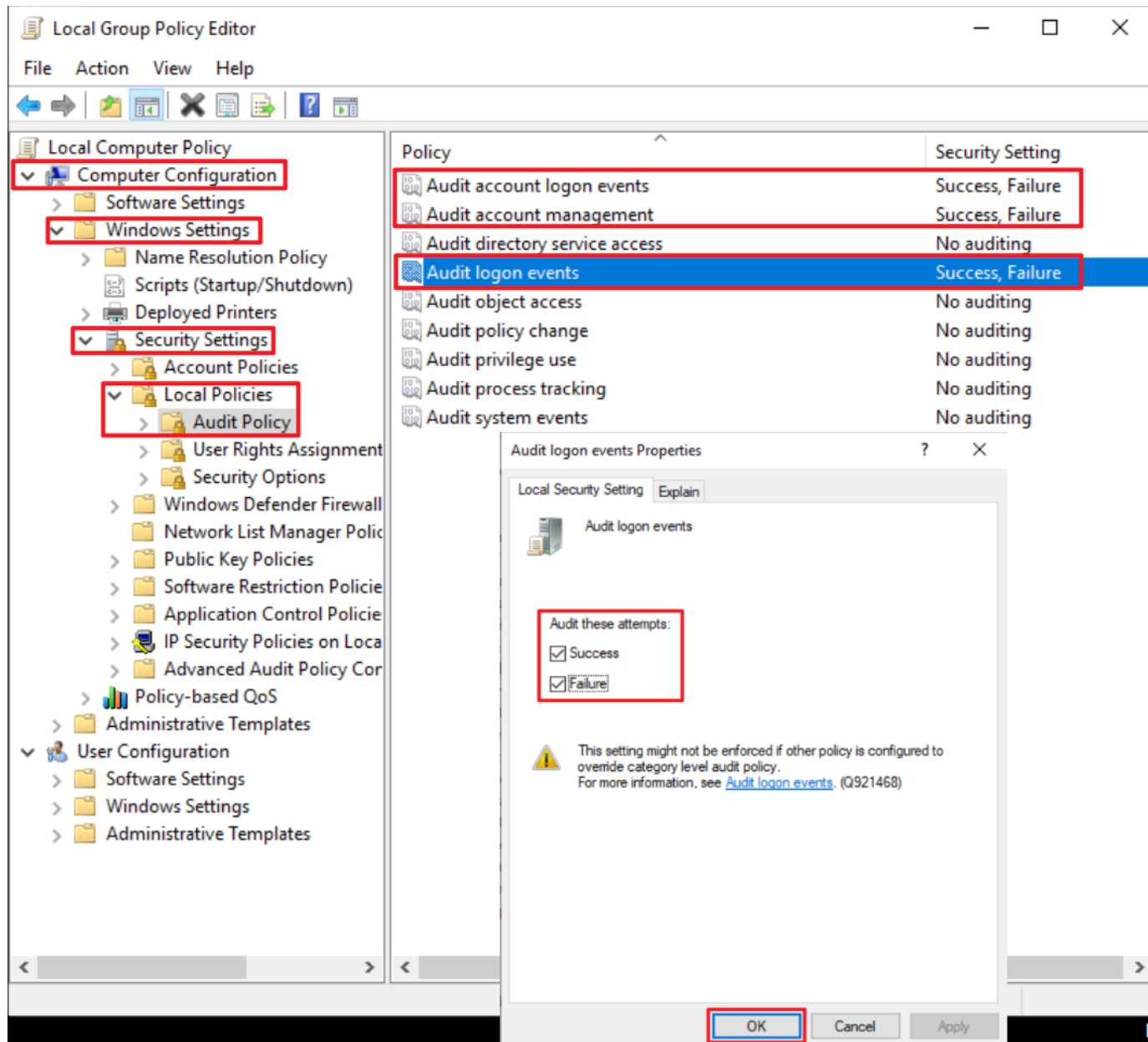
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) 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 logon events” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”



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

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

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The window has a dark blue background and a white border. The command prompt shows the command `PS C:\> gpupdate /force` being entered. The output of the command is displayed in white text: `Updating policy...`, `Computer Policy update has completed successfully.`, and `User Policy update has completed successfully.`. The prompt `PS C:\>` is shown again at the bottom. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.

(5) Enter the command below to view group policy applied status.

PS C:\> **auditpol /get /category:***

```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    No Auditing
  System Integrity             No Auditing
  IPsec Driver                 No Auditing
  Other System Events          No Auditing
  Security State Change        No Auditing
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
  User / Device Claims          Success and Failure
  Group Membership             Success and Failure
Object Access
  File System                  Success and Failure
  Registry                    Success and Failure
  Kernel Object                Success and Failure
  SAM                          Success and Failure
  Certification Services       Success and Failure
  Application Generated        Success and Failure
  Handle Manipulation           Success and Failure
  File Share                   Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events    Success and Failure
  Detailed File Share           Success and Failure
  Removable Storage            Success and Failure
  Central Policy Staging        Success and Failure
Privilege Use
  Non Sensitive Privilege Use   No Auditing
  Other Privilege Use Events     No Auditing
  Sensitive Privilege Use       No Auditing
Detailed Tracking
  Process Creation              No Auditing
  Process Termination           No Auditing
  DPAPI Activity                No Auditing
  RPC Events                    No Auditing
  Plug and Play Events          No Auditing
  Token Right Adjusted Events    No Auditing
Policy Change
  Audit Policy Change           No Auditing
  Authentication Policy Change  No Auditing
  Authorization Policy Change   No Auditing
  MPSSVC Rule-Level Policy Change No Auditing
  Filtering Platform Policy Change No Auditing
  Other Policy Change Events     No Auditing
Account Management
  Computer Account Management    No Auditing
  Security Group Management      No Auditing
  Distribution Group Management No Auditing
  Application Group Management   No Auditing
  Other Account Management Events No Auditing
  User Account Management        No Auditing
DS Access
  Directory Service Access       No Auditing
  Directory Service Changes      No Auditing
  Directory Service Replication  No Auditing
  Detailed Directory Service Replication No Auditing
Account Logon
  Kerberos Service Ticket Operations Success and Failure
  Other Account Logon Events     Success and Failure
  Kerberos Authentication Service Success and Failure
  Credential Validation           Success and Failure
PS C:\>
```

7.2.2 Event Log Settings

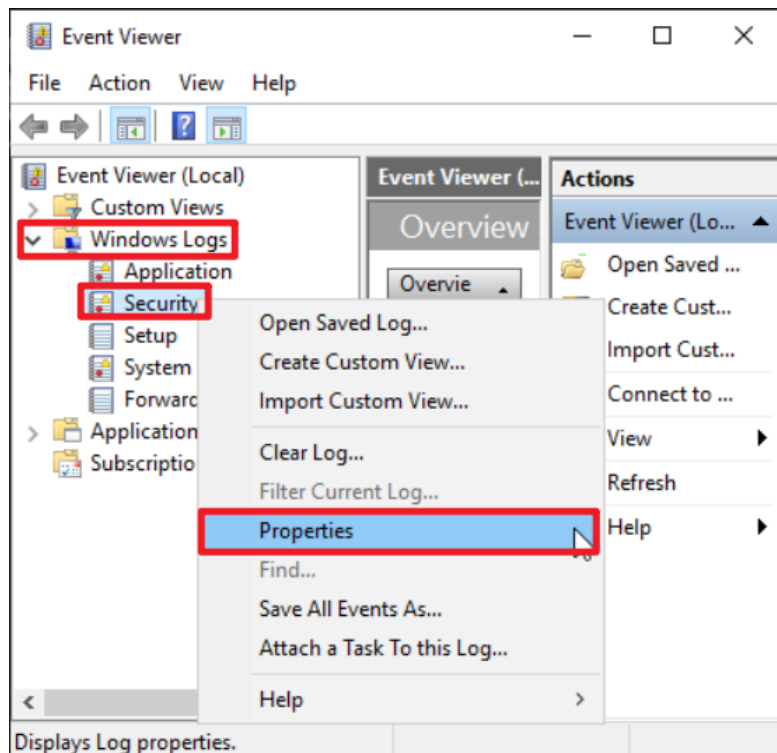
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “[Event Viewer](#)” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Security” → And click on “Properties.”

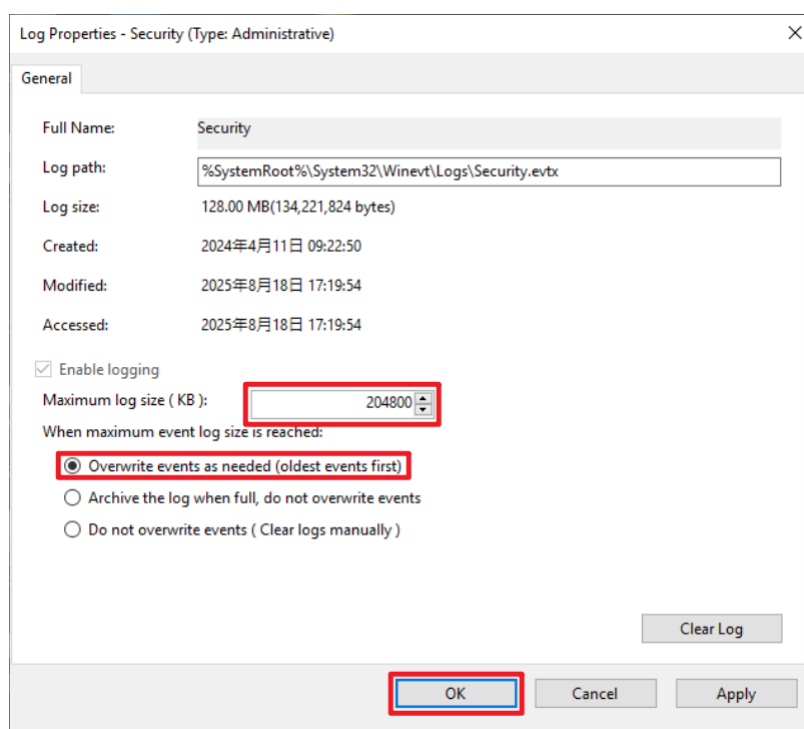


(3) Configure Security Log

Enter maximum log file size: 204800 KB

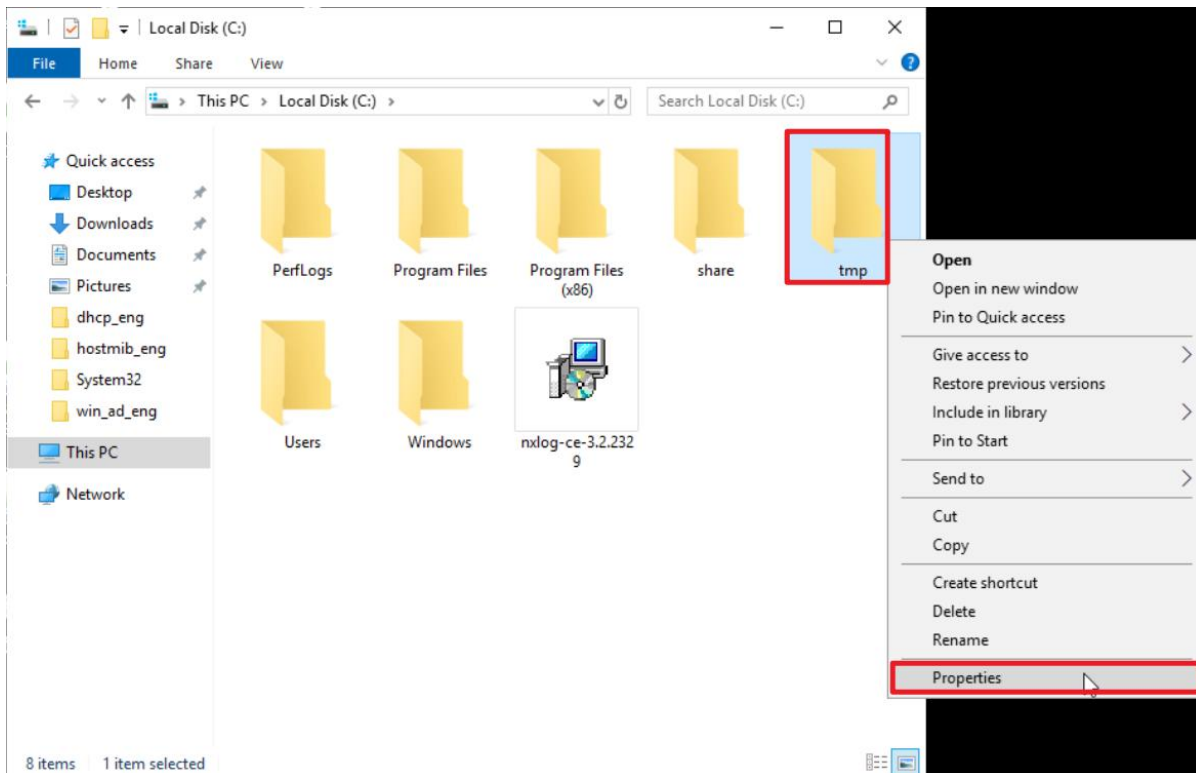
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”

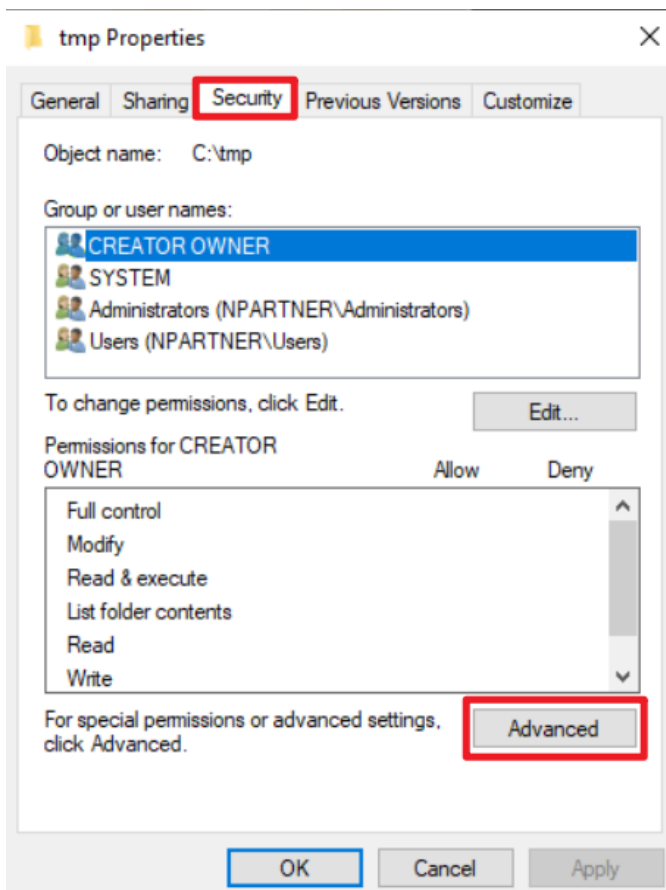


7.3 Folder Audit Configuration

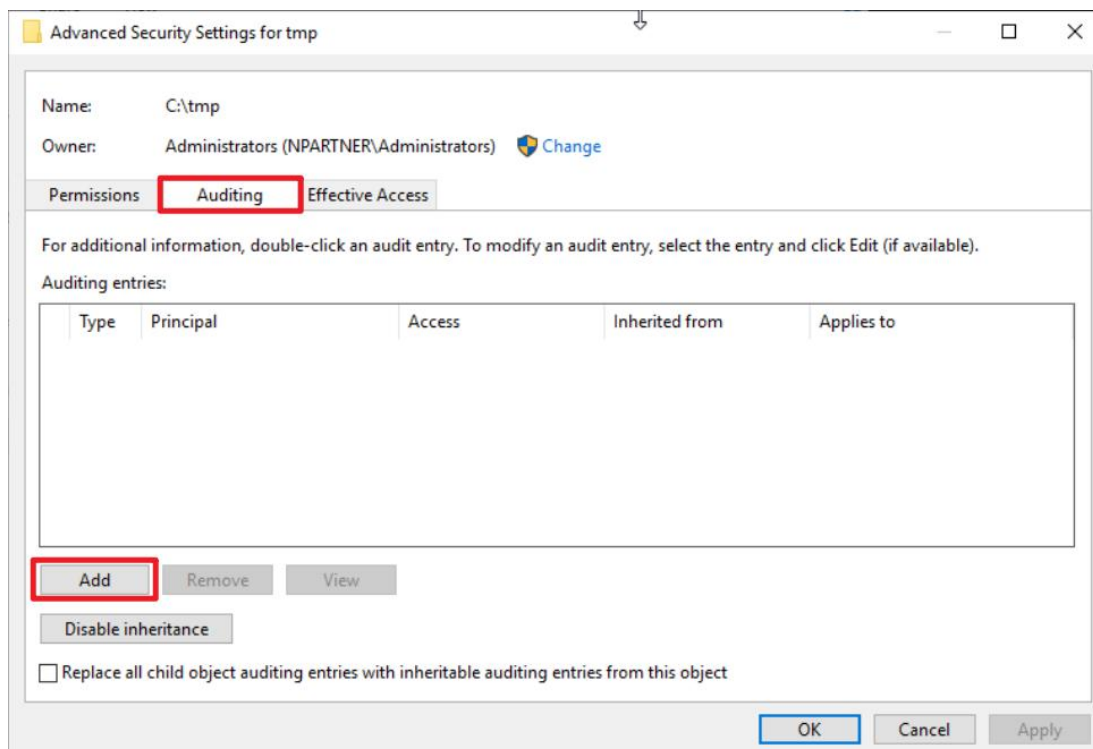
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



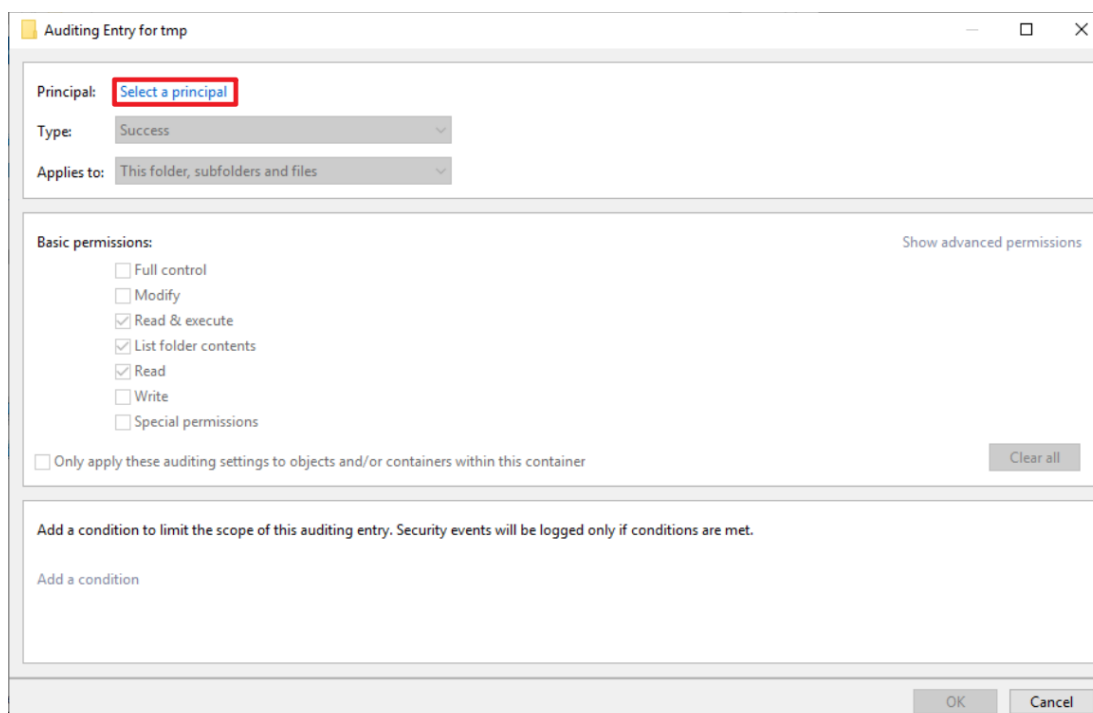
(2) Go to the “Security” tab → click “Advanced.”



(3) Open the “Auditing” tab → click “Add.”



(4) Click “Select a principal.”



(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”

Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
npartner.local

Enter the object name to select (examples):
Everyone

Check Names

Advanced... OK Cancel

(6) Select “All” in type → enable “Full Control” → click “OK.”

Auditing Entry for tmp

Principal: Everyone Select a principal

Type: All

Applies to: This folder, subfolders and files

Basic permissions:
☒ Full control
☒ Modify
☒ Read & execute
☒ List folder contents
☒ Read
☒ Write
☐ Special permissions

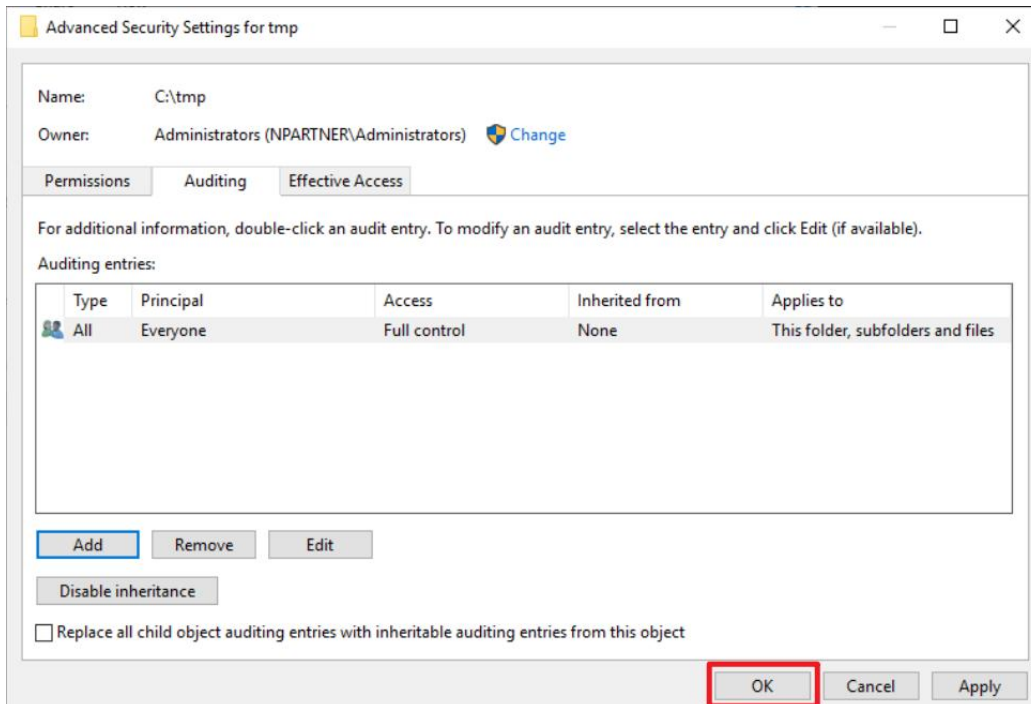
Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

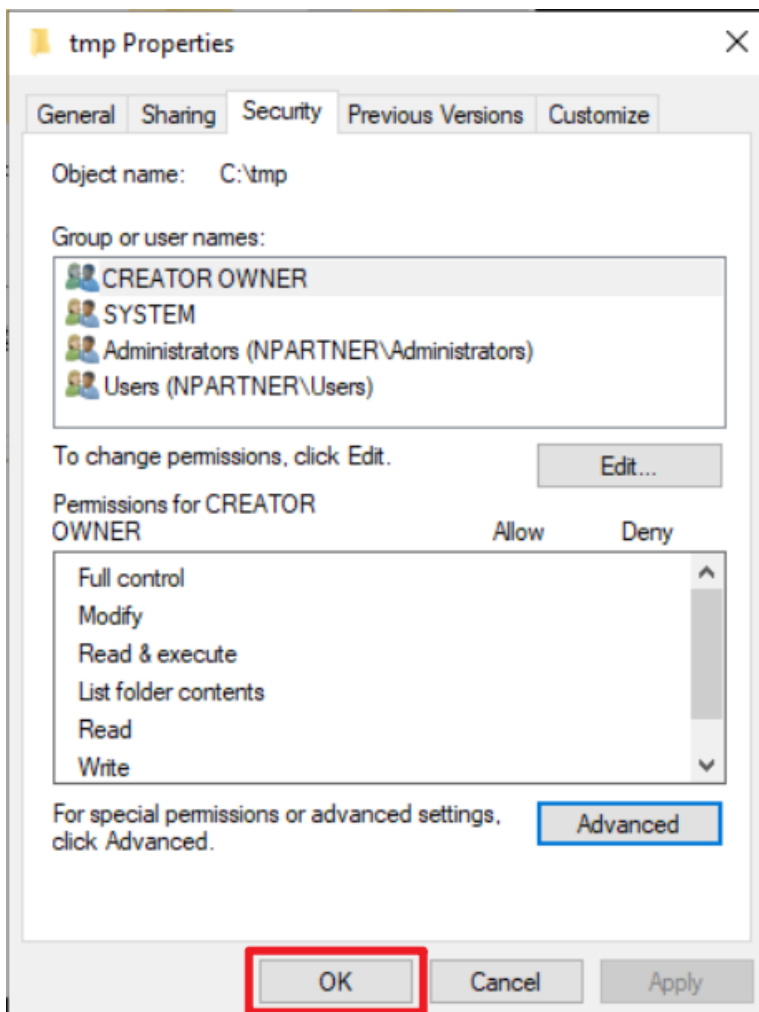
Add a condition

OK Cancel

(7) Confirm that the auditing entries shows “Everyone” → click “OK.”



(8) Click “OK” again to confirm and close.



8. Windows Server 2022

8.1 Domain

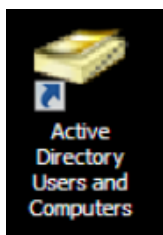
Windows Audit Policy Configuration:

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

The following sections describe the configuration methods for Domain and Workgroup environments.

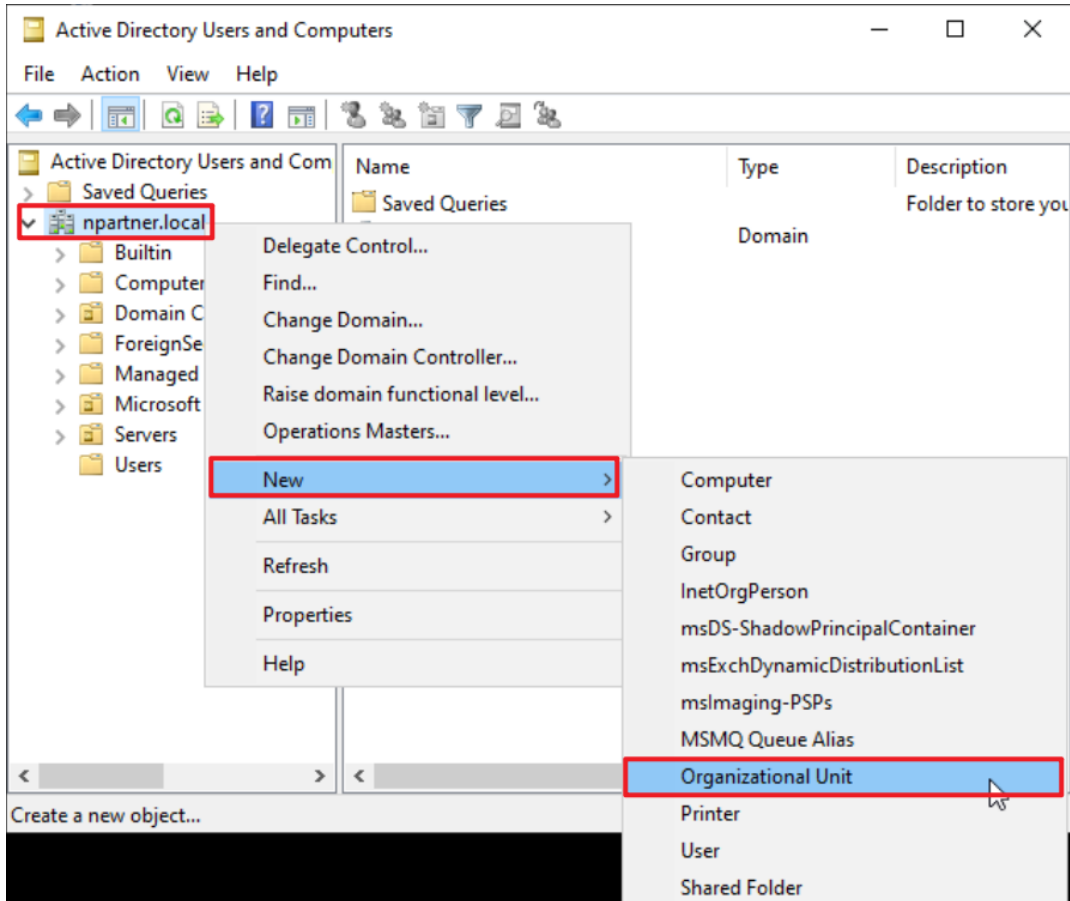
8.1.1 Organizational Unit (OU) Configuration

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



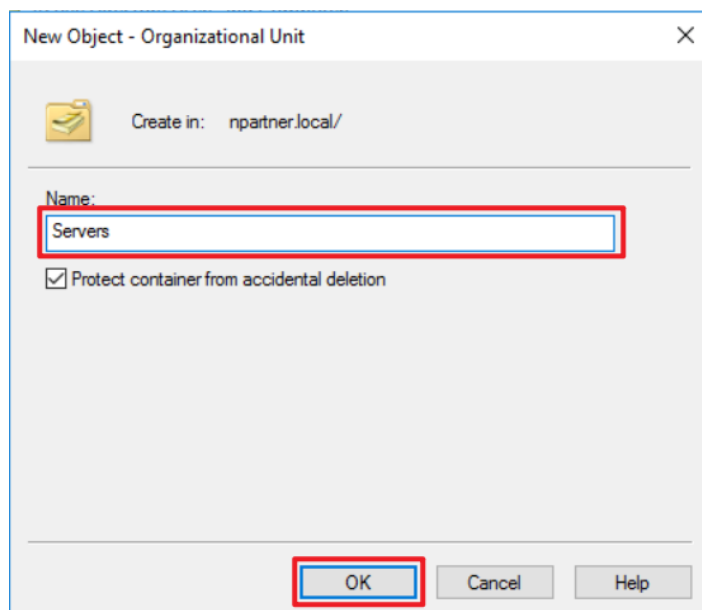
(2) Add an Organizational Unit

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



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

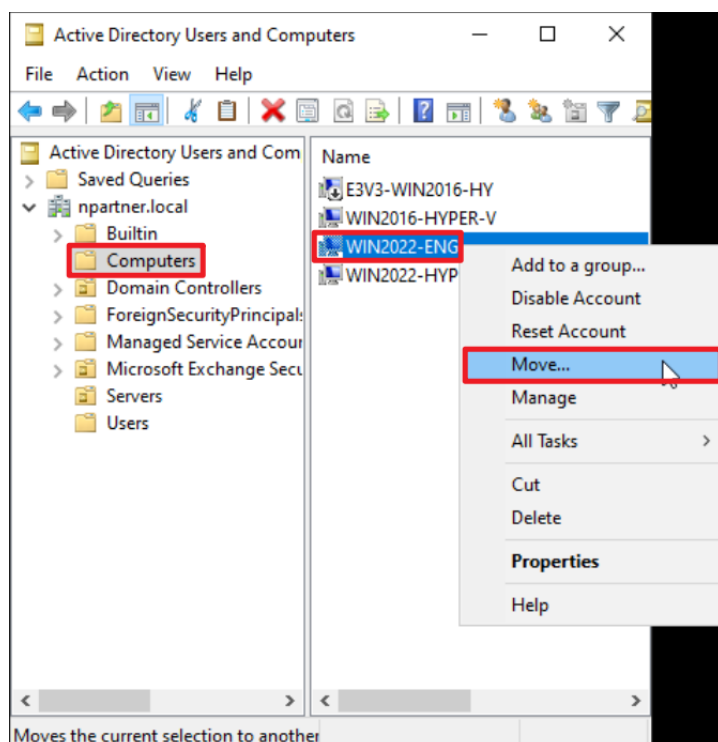
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

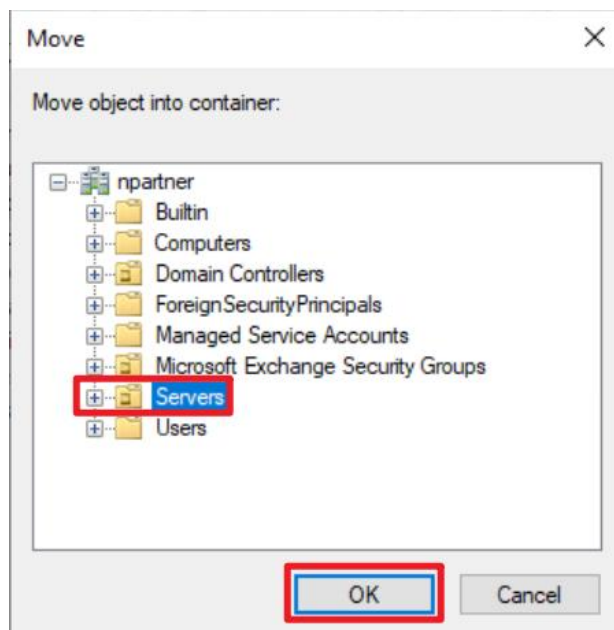
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2022-ENG” server.

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



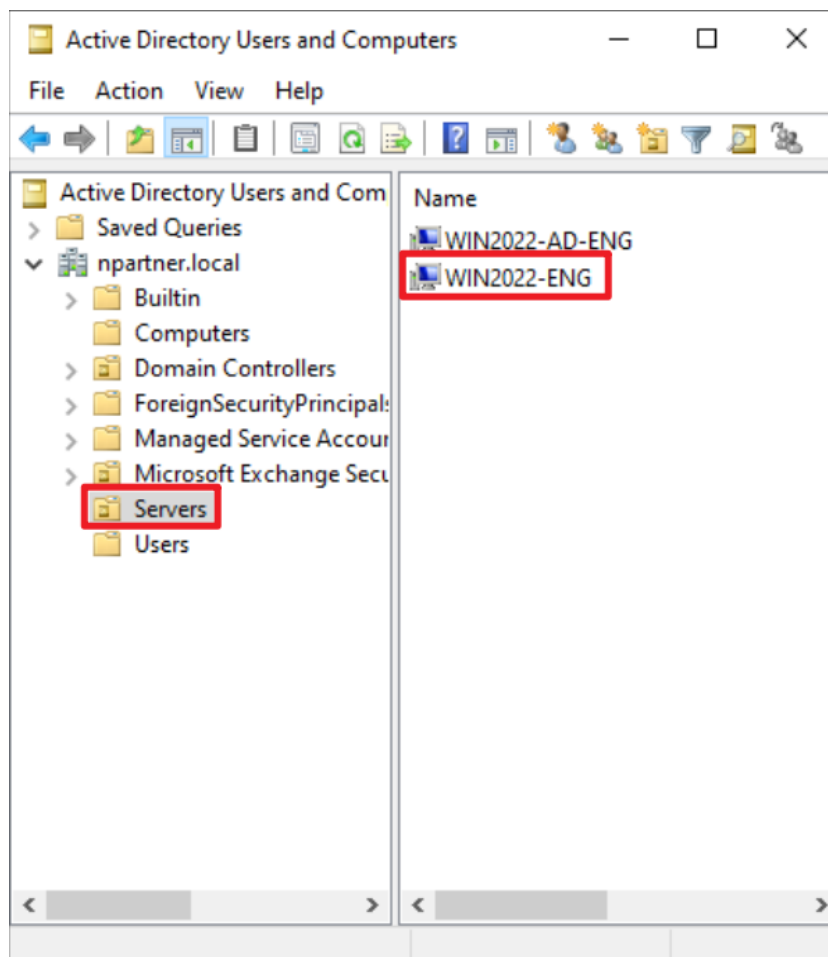
(5) Select your Organizational Unit:

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



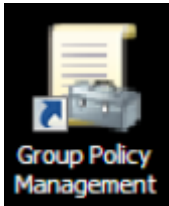
(6) Verify the Server Has Been Moved to your New Organizational Unit:

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



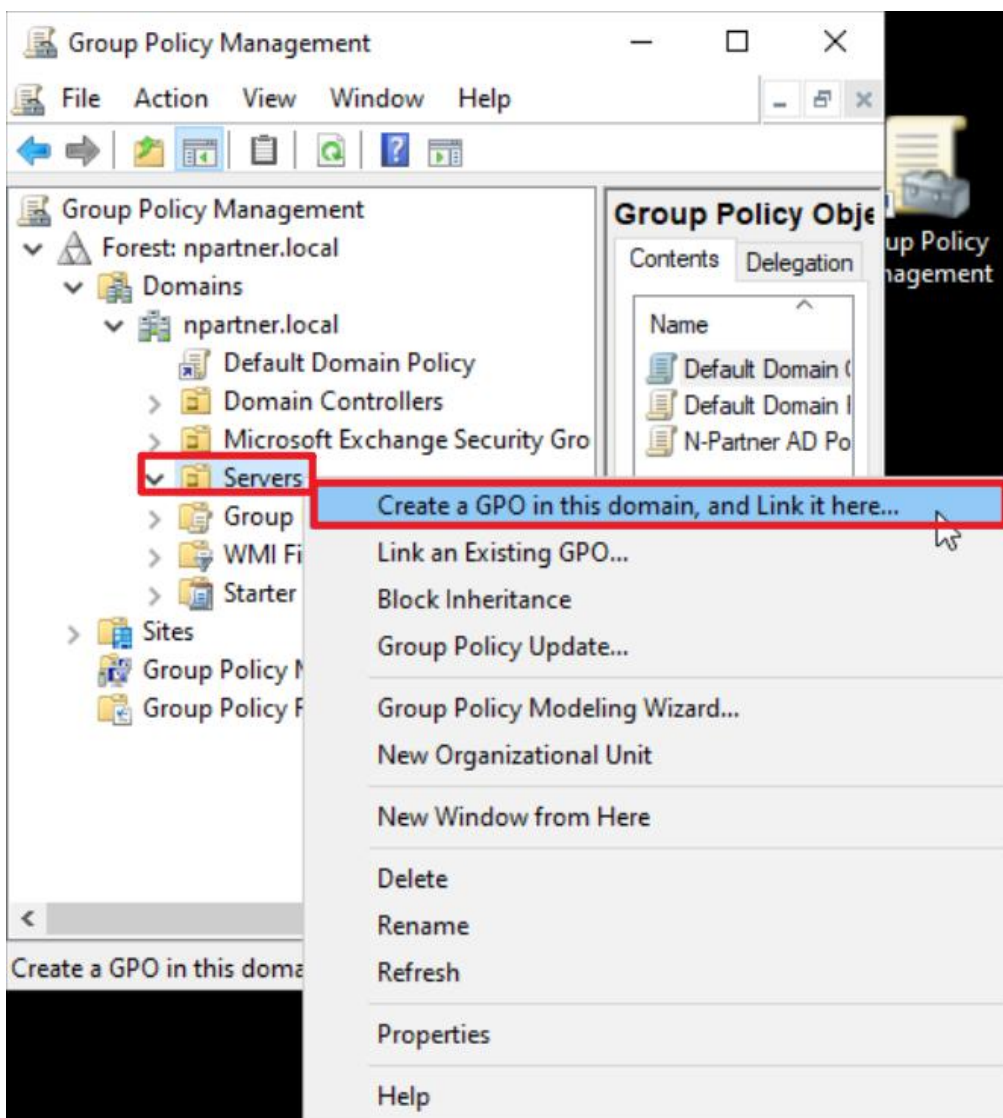
8.1.2 Group Policy Settings

(1) Click “Group Policy Management.”



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

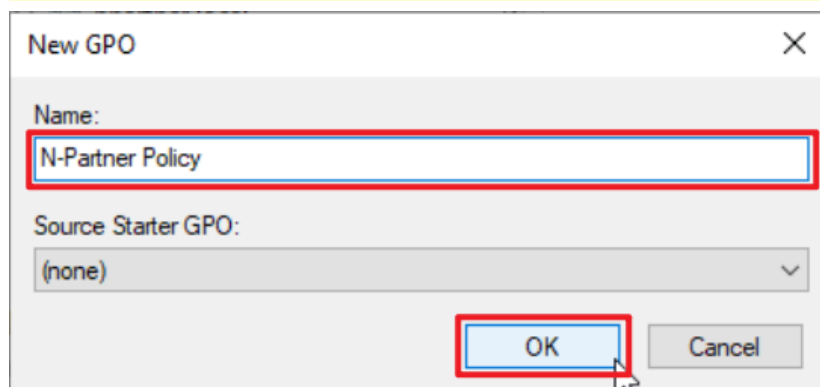
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

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

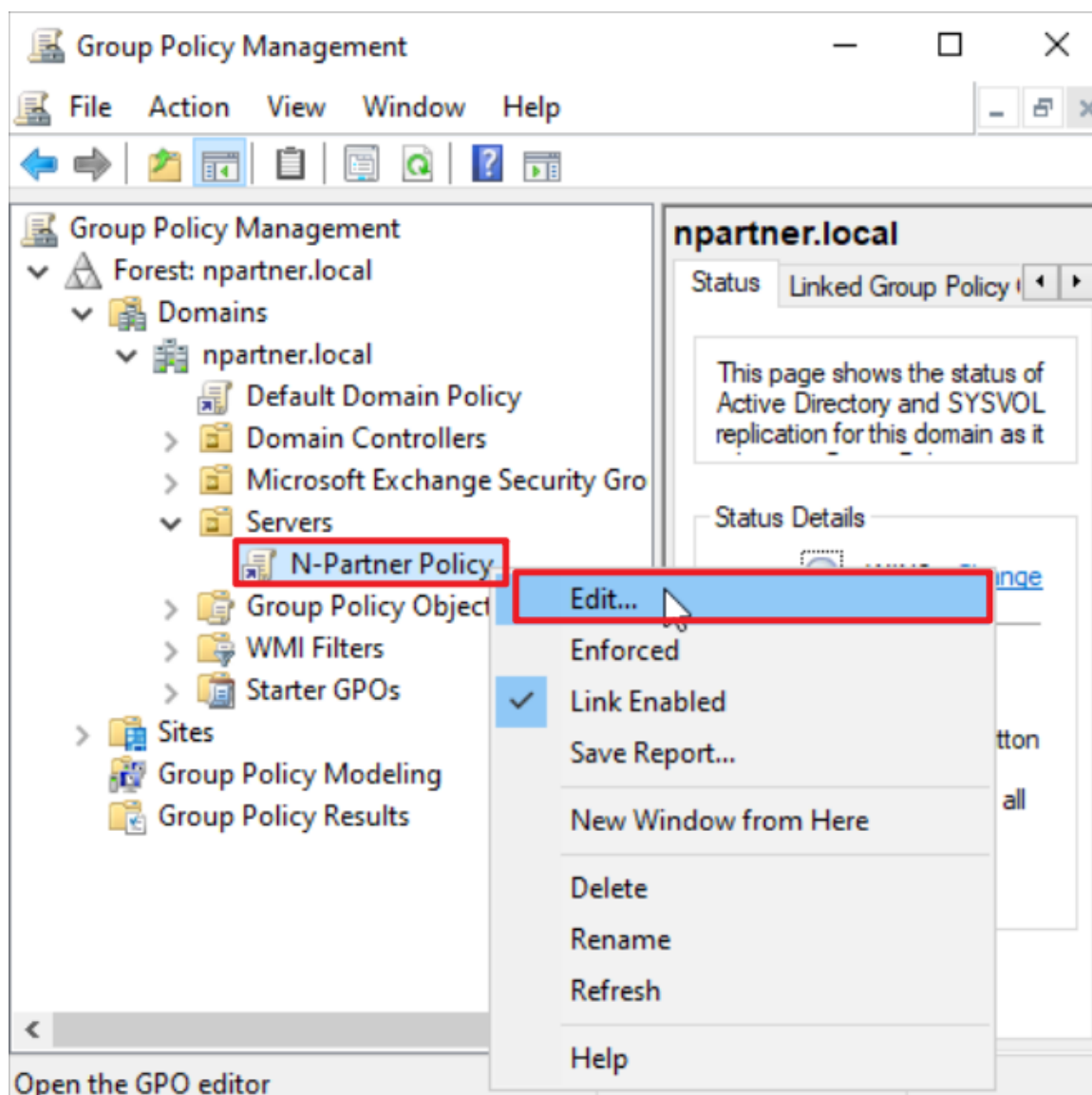
Note: Create your GPO name according to the actual environment. Then click “Edit.”



(4) Edit your Group Policy Object

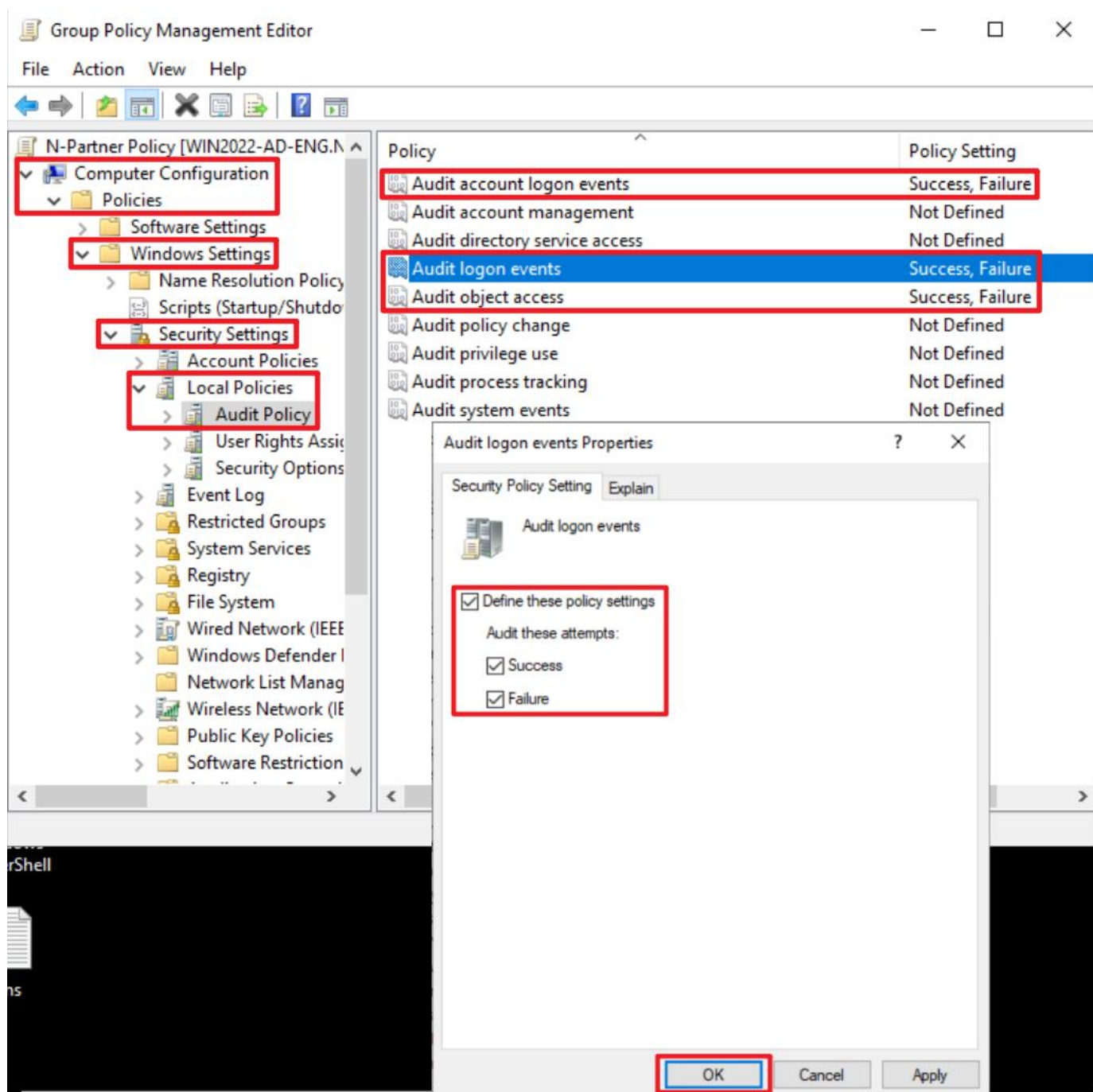
In your group policy object, (in this example, it is “N-Partner Policy”)

right-click and select “Edit.”



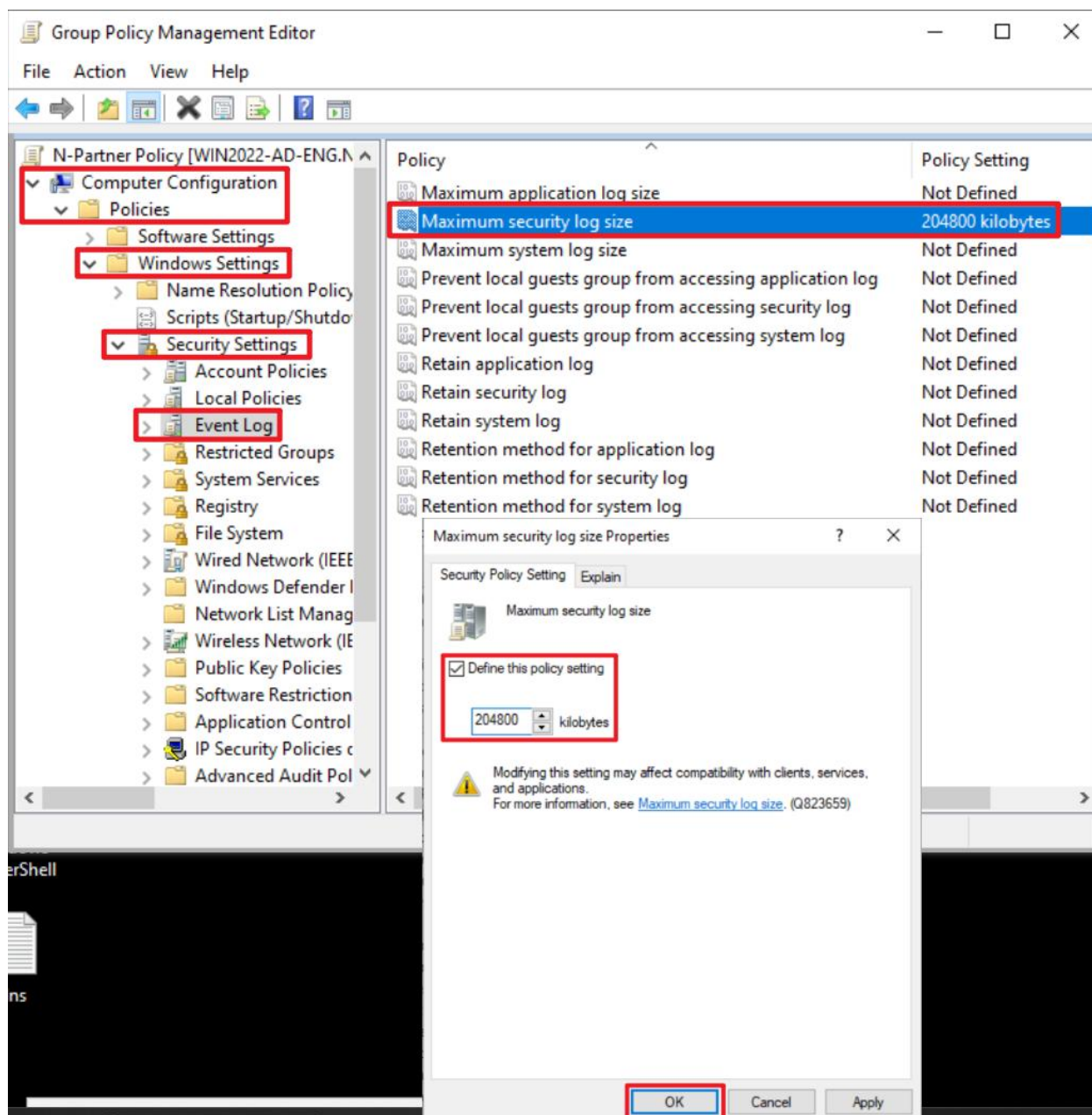
(5) Local Group Policies: Audit Policy

Expand folder “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” → check “Define these policy settings”: Success, Failure. → click “OK.”



(6) Event Log: Security Log Retention Method

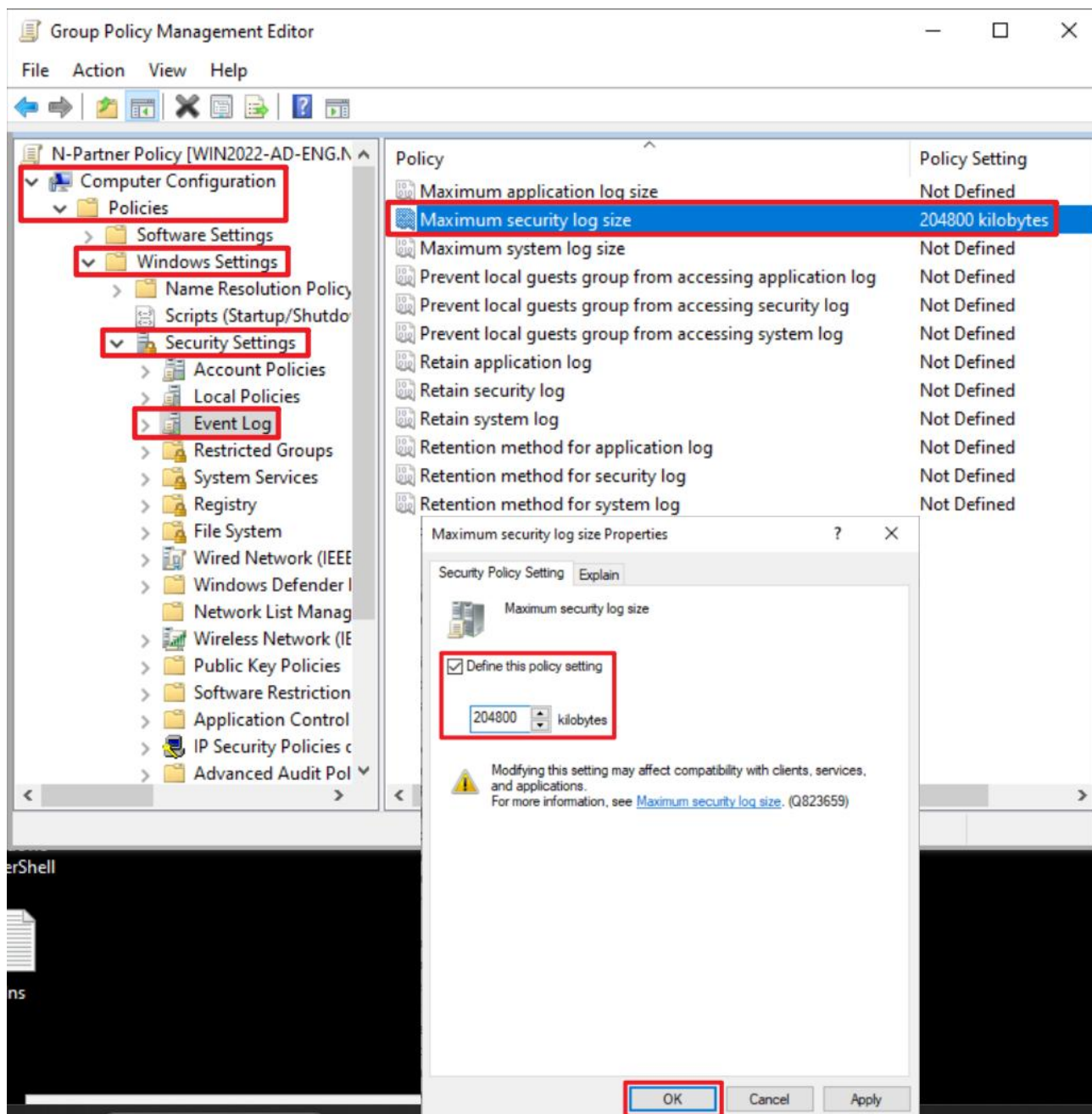
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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 Windows File server, open “Windows PowerShell.”



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

```
PS C:\> Invoke-GPUUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `Invoke-GPUUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt returns to `PS C:\>`.

```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
PS C:\>
```

Replace the text shown in red with the Windows File server name.

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

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\SQL2022.html -ReportType html
```

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the command `Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\Win2022.html -ReportType html` being entered and executed. The output shows the logging mode, namespace, logging computer, logging user, and logging mode.

```
Administrator: Windows PowerShell
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\Win2022.html -ReportType html

RsopMode       : Logging
Namespace      : \\WIN2022-ENG\Root\Rsop\NS1D95751A_30CE_4E92_B7D7_1740B22E0DE1
LoggingComputer : WIN2022-ENG
LoggingUser    : NPARTNER\administrator
LoggingMode    : Computer

PS C:\>
```

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 FILE server is applying the N-Partner Policy Group Policy.

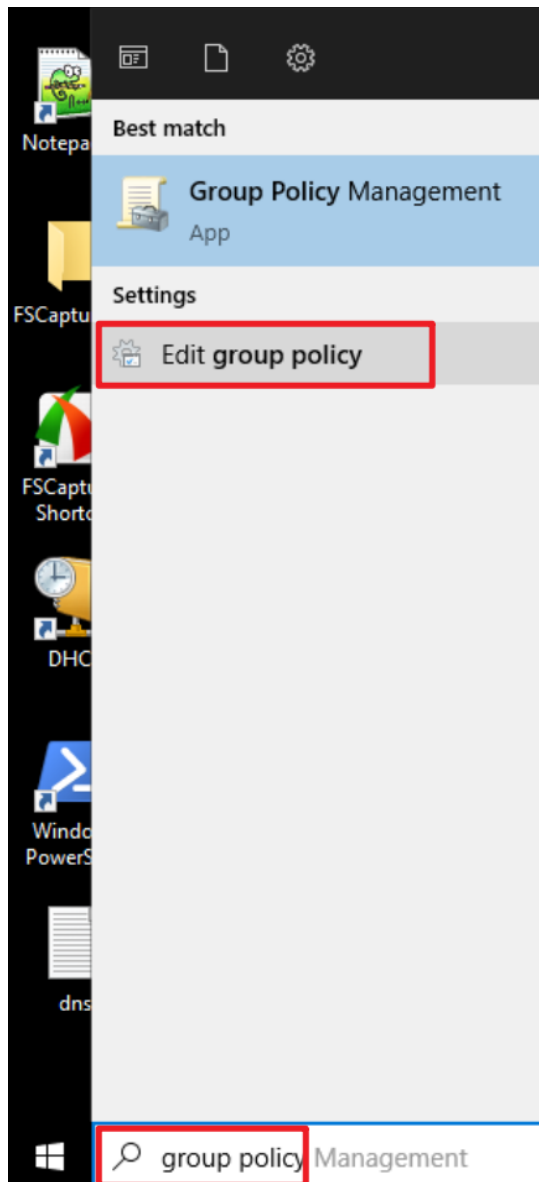
Group Policy Results		
NPARTNER\WIN2022-ENG		
Data collected on: 8/14/2025 PM 03:35:27		show all
Computer Details		hide
General		show
Component Status		show
Settings		hide
Policies		hide
Windows Settings		hide
Security Settings		hide
Account Policies/Password Policy		show
Account Policies/Account Lockout Policy		show
Local Policies/Audit Policy		hide
Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
Local Policies/Security Options		show
Event Log		hide
Policy	Setting	Winning GPO
Maximum security log size	204800 kilobytes	N-Partner Policy
Retention method for security log	As needed	N-Partner Policy
Public Key Policies/Certificate Services Client - Auto-Enrollment Settings		show

8.2 Workgroup

8.2.1 Audit Policy Configuration

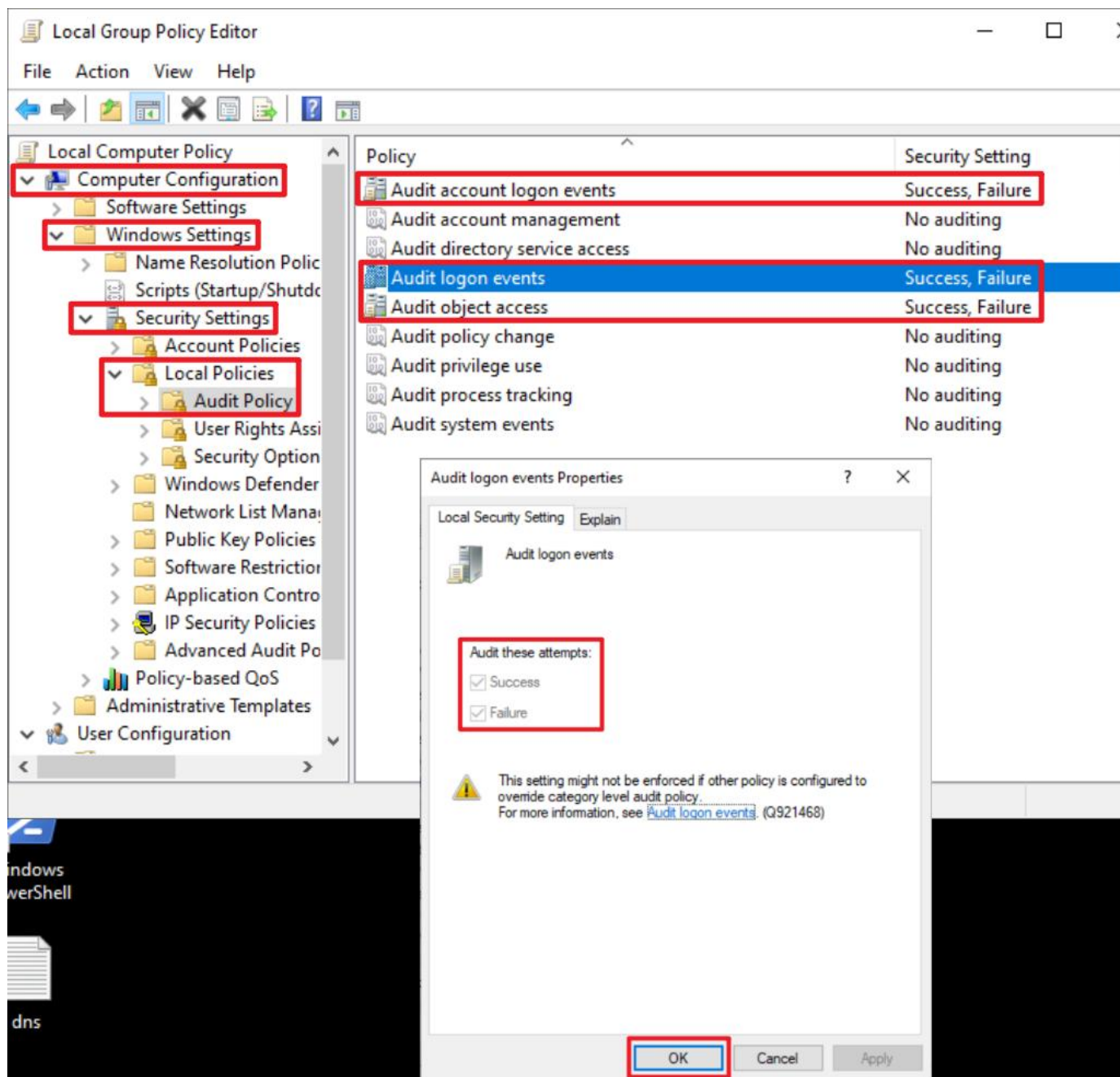
(1) Open Local Group Policy Editor

Click on “Start” → enter “group policy” to search → click on “Edit Group Policy.”



(2) 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 logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”

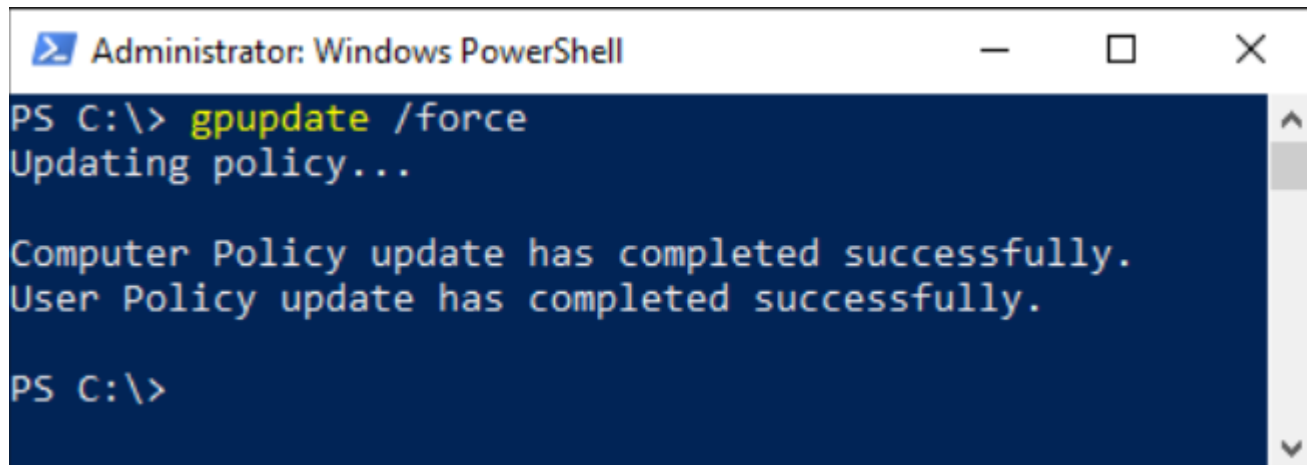


(3) Open "Windows PowerShell."



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

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

The image shows a screenshot of an "Administrator: Windows PowerShell" window. The window has a title bar with the text "Administrator: Windows PowerShell" and standard window controls (minimize, maximize, close). The background is dark blue. The text in the window is as follows:
PS C:\> gpupdate /force
Updating policy...

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

PS C:\>

(5) Enter the command below to view group policy applied status.

PS C:\> **auditpol /get /category:***

```

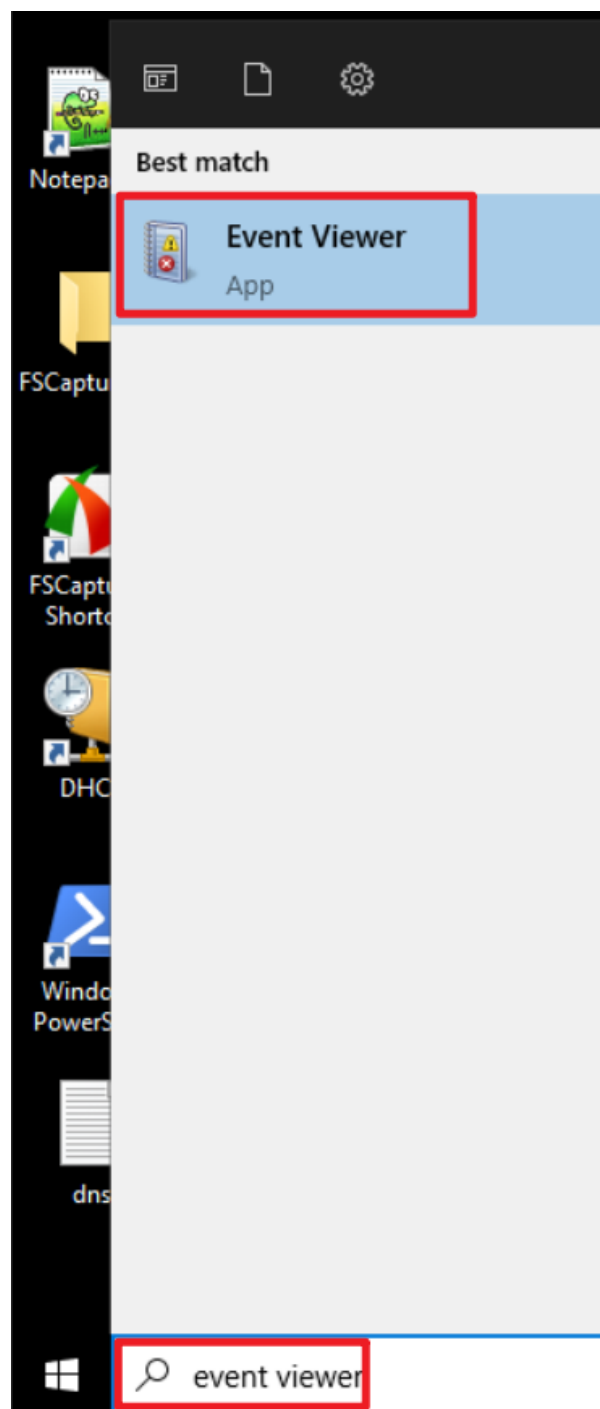
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory                                Setting
System
  Security System Extension                          No Auditing
  System Integrity                                  No Auditing
  IPsec Driver                                       No Auditing
  Other System Events                               No Auditing
  Security State Change                             No Auditing
Logon/Logoff
  Logon                                              Success and Failure
  Logoff                                             Success and Failure
  Account Lockout                                   Success and Failure
  IPsec Main Mode                                   Success and Failure
  IPsec Quick Mode                                 Success and Failure
  IPsec Extended Mode                              Success and Failure
  Special Logon                                     Success and Failure
  Other Logon/Logoff Events                         Success and Failure
  Network Policy Server                            Success and Failure
  User / Device Claims                             Success and Failure
  Group Membership                                  Success and Failure
Object Access
  File System                                       Success and Failure
  Registry                                          Success and Failure
  Kernel Object                                    Success and Failure
  SAM                                               Success and Failure
  Certification Services                           Success and Failure
  Application Generated                            Success and Failure
  Handle Manipulation                              Success and Failure
  File Share                                        Success and Failure
  Filtering Platform Packet Drop                    Success and Failure
  Filtering Platform Connection                     Success and Failure
  Other Object Access Events                       Success and Failure
  Detailed File Share                              Success and Failure
  Removable Storage                                Success and Failure
  Central Policy Staging                           Success and Failure
Privilege Use
  Non Sensitive Privilege Use                       No Auditing
  Other Privilege Use Events                        No Auditing
  Sensitive Privilege Use                           No Auditing
Detailed Tracking
  Process Creation                                 No Auditing
  Process Termination                             No Auditing
  DPAPI Activity                                   No Auditing
  RPC Events                                       No Auditing
  Plug and Play Events                             No Auditing
  Token Right Adjusted Events                      No Auditing
Policy Change
  Audit Policy Change                              No Auditing
  Authentication Policy Change                     No Auditing
  Authorization Policy Change                      No Auditing
  MPSSVC Rule-Level Policy Change                  No Auditing
  Filtering Platform Policy Change                  No Auditing
  Other Policy Change Events                       No Auditing
Account Management
  Computer Account Management                      No Auditing
  Security Group Management                        No Auditing
  Distribution Group Management                    No Auditing
  Application Group Management                     No Auditing
  Other Account Management Events                  No Auditing
  User Account Management                          No Auditing
DS Access
  Directory Service Access                         No Auditing
  Directory Service Changes                        No Auditing
  Directory Service Replication                    No Auditing
  Detailed Directory Service Replication            No Auditing
Account Logon
  Kerberos Service Ticket Operations               Success and Failure
  Other Account Logon Events                       Success and Failure
  Kerberos Authentication Service                  Success and Failure
  Credential Validation                             Success and Failure
PS C:\>

```

8.2.2 Event Log Settings

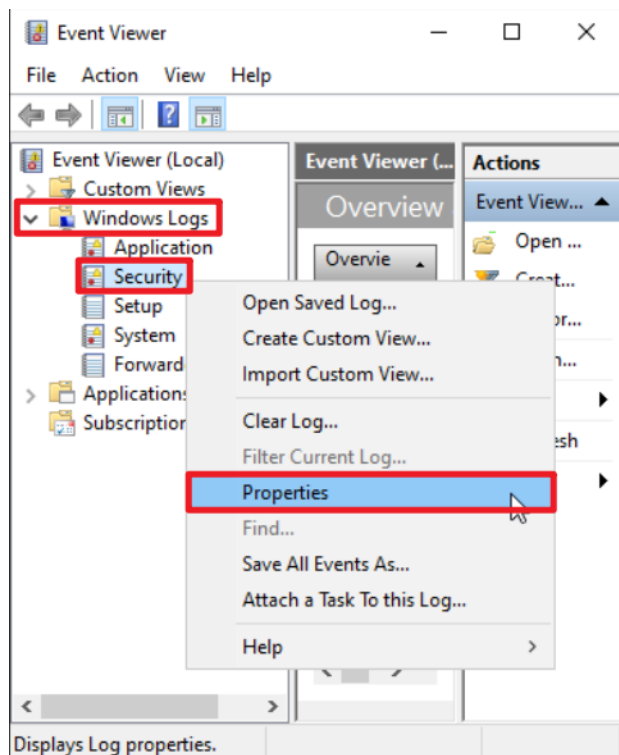
(1) Search for “Event Viewer”

Enter “Event Viewer” to search → click on “[Event Viewer](#)” in the search results.



(2) Edit Security Log

Expand folder “Windows Logs” → right-click on “Security” → And click on “Properties.”

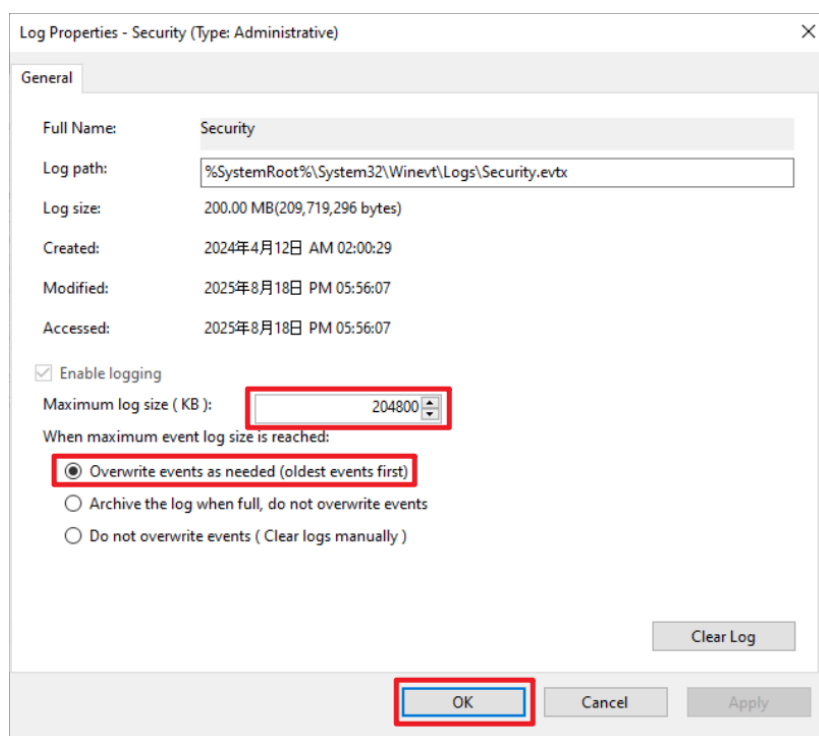


(3) Configure Security Log

Enter maximum log file size: 204800 KB

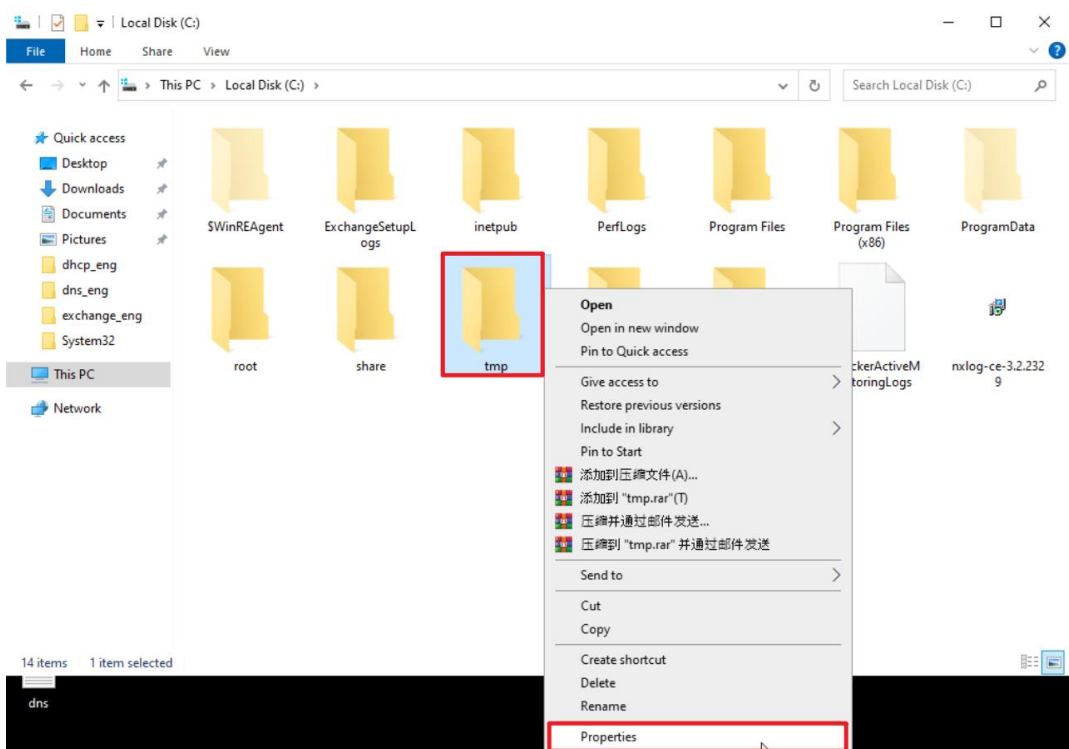
Note: Please adjust the number according to the actual environment.

→ click on “Overwrite events as needed (oldest events first)” → click “OK.”

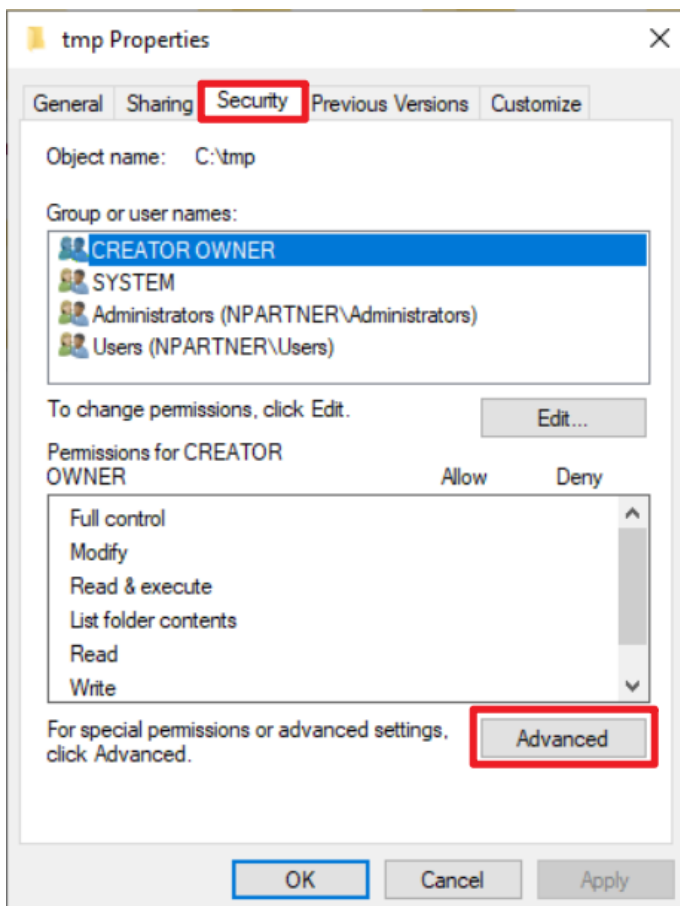


8.3 Folder Audit Configuration

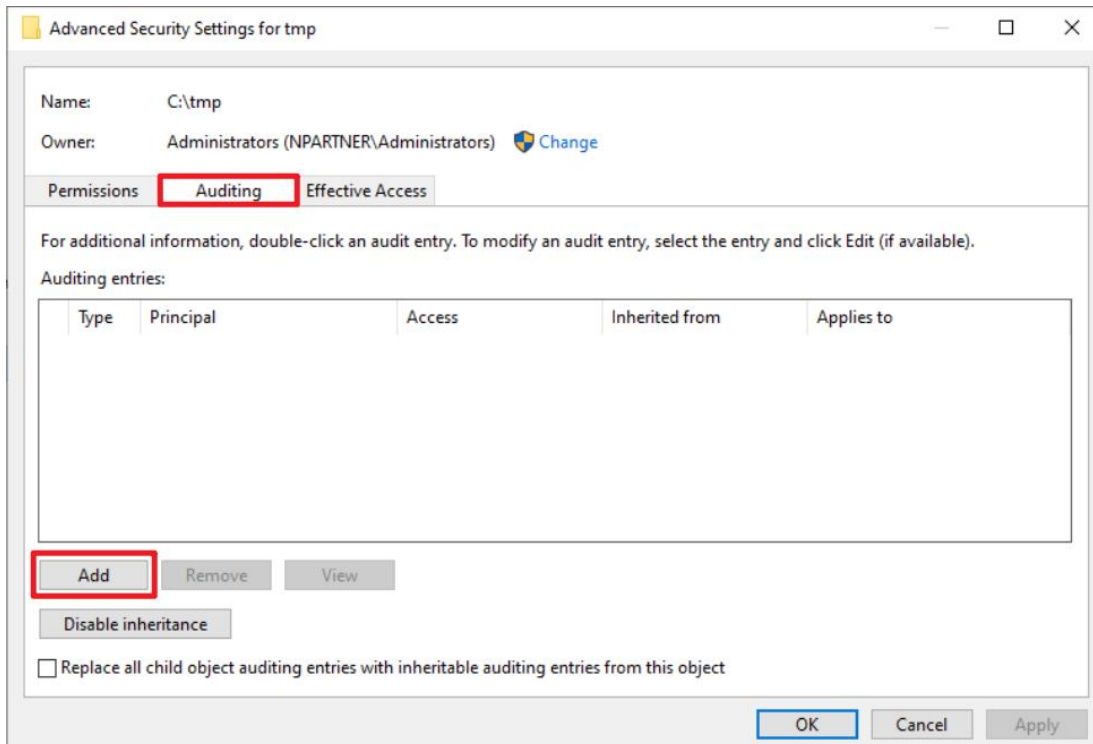
(1) Right-click the target folder to be audited (the example here is `tmp`) → select “Properties.”



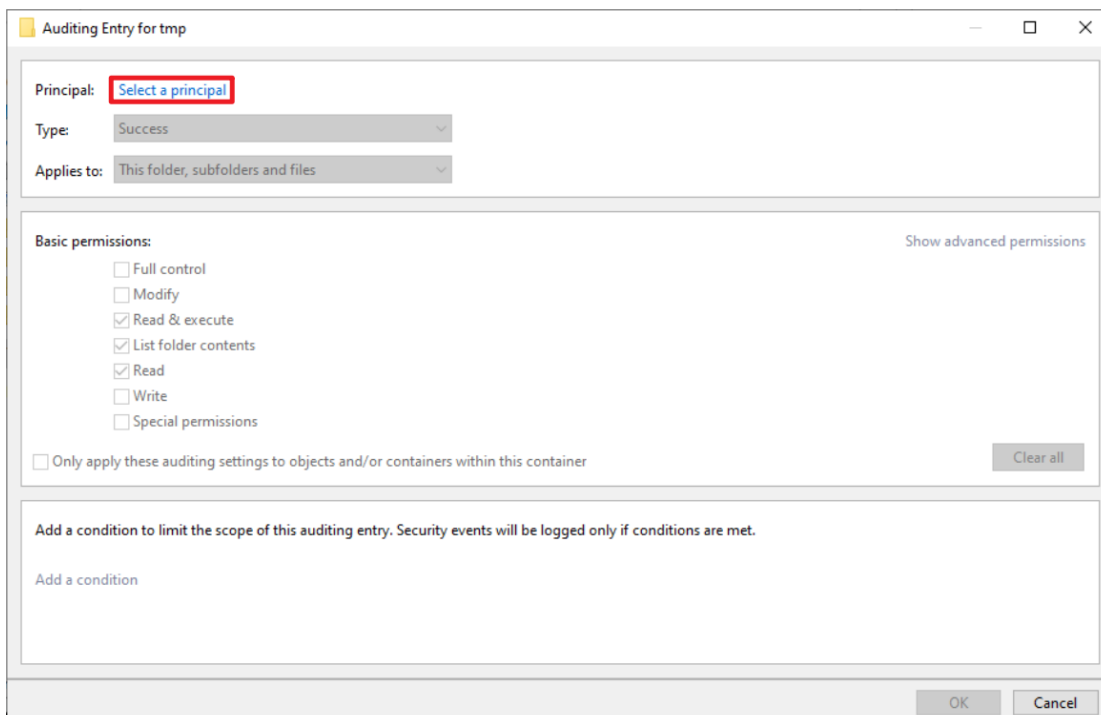
(2) Go to the “Security” tab → click “Advanced.”



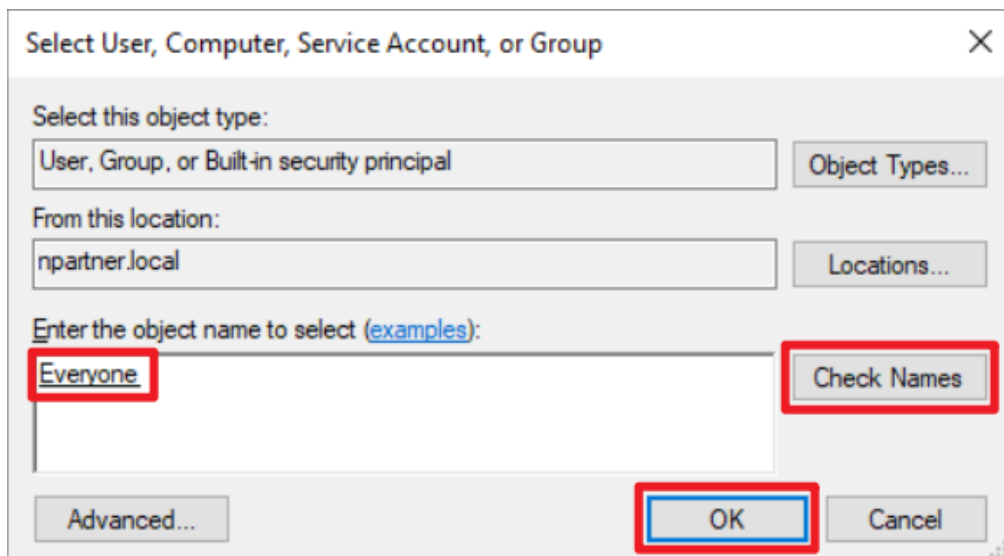
(3) Open the “Auditing” tab → click “Add.”



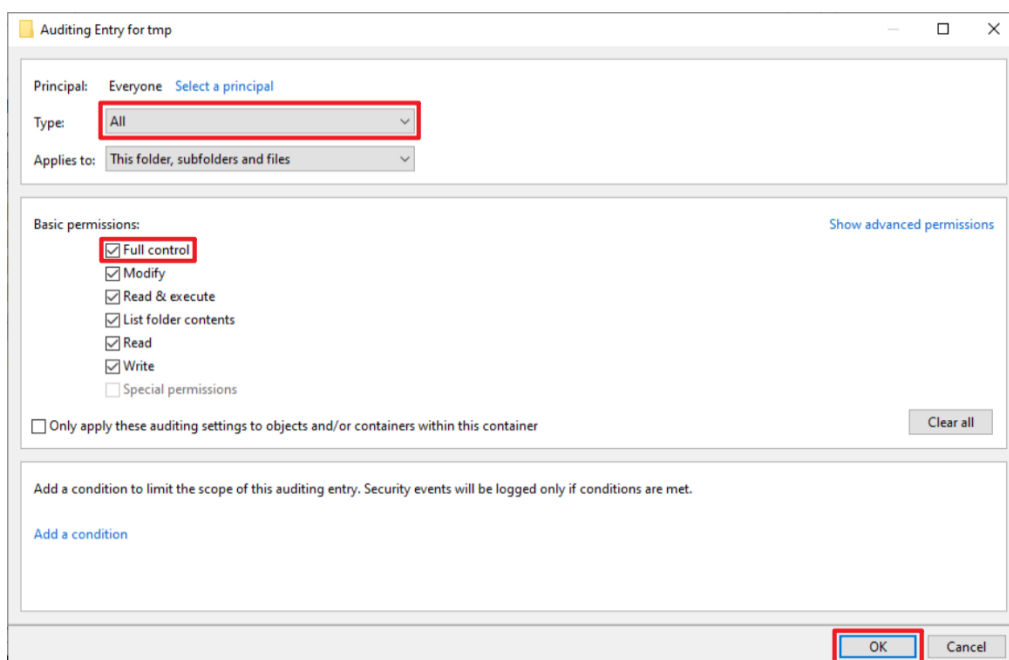
(4) Click “Select a principal.”



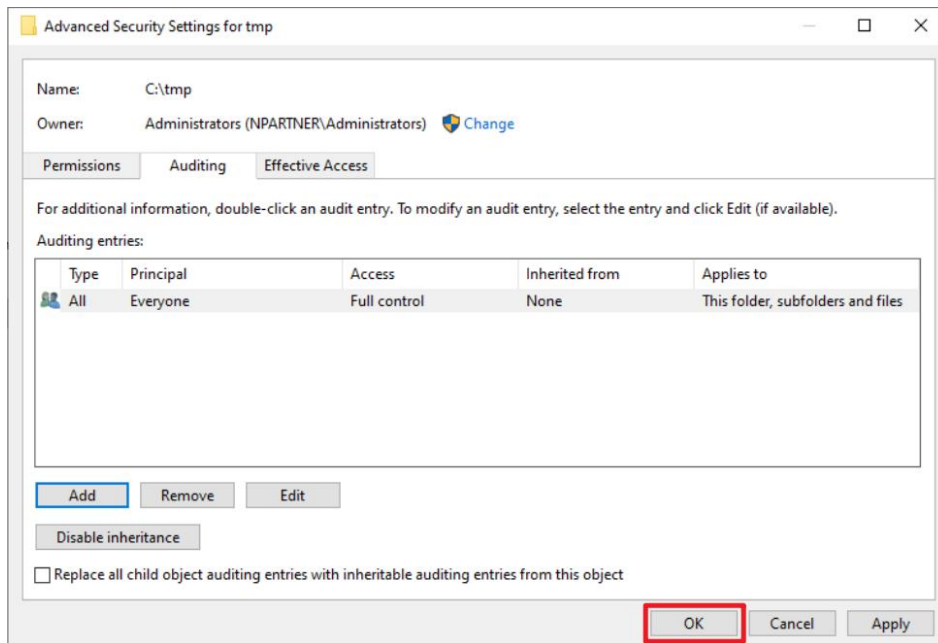
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



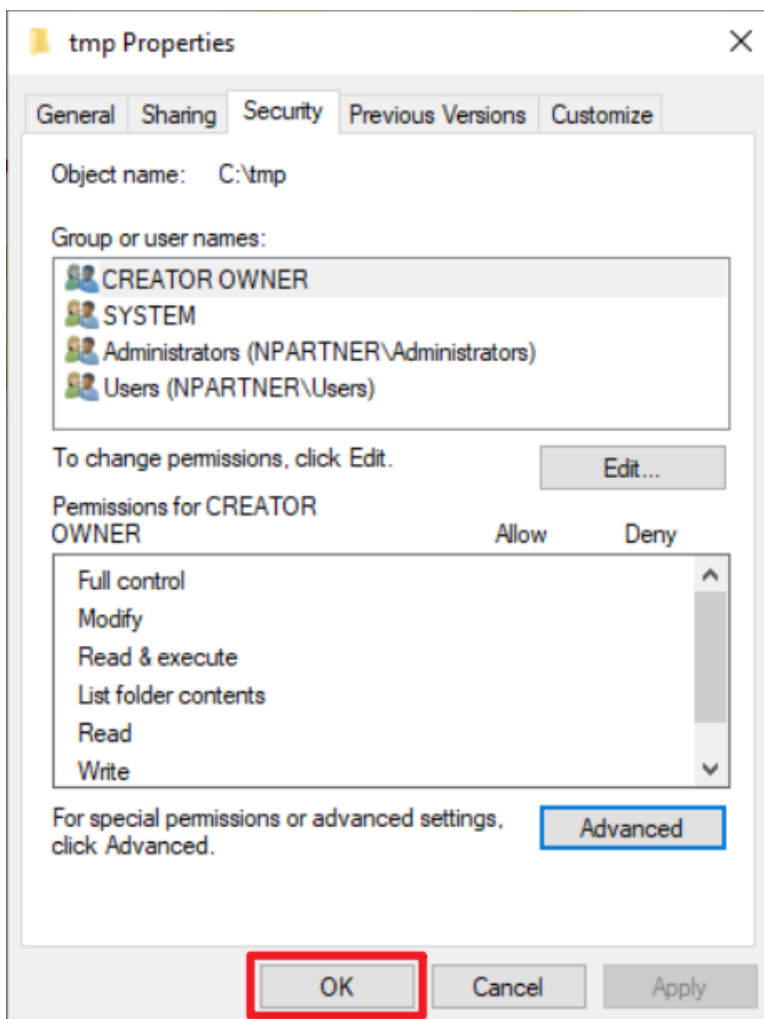
(6) Select “All” in type → enable “Full Control” → click “OK.”



(7) Confirm that the auditing entries shows “Everyone” → click “OK.”



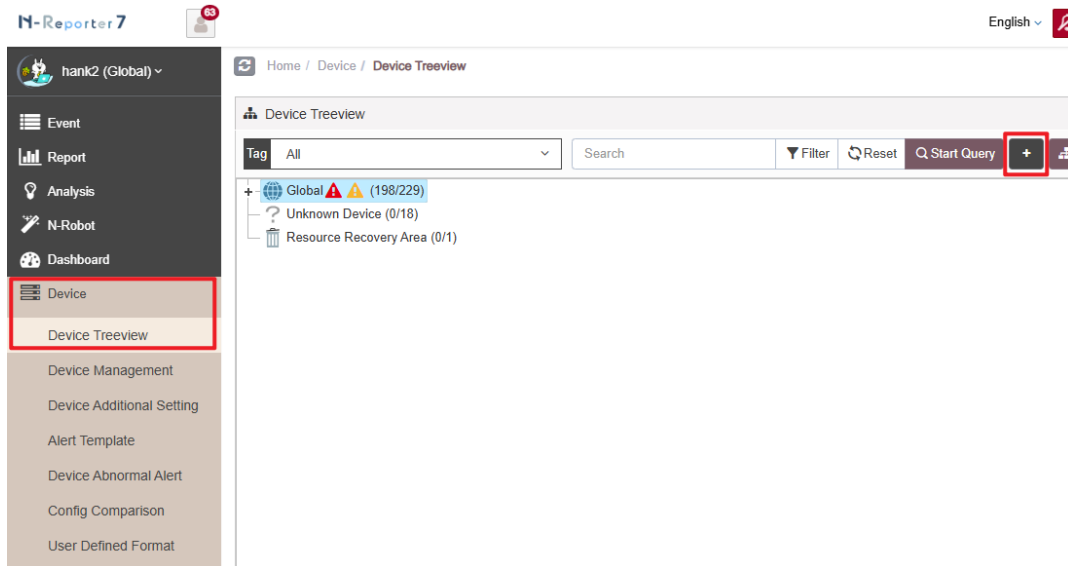
(8) Click “OK” again to confirm and close.



9. N-Reporter

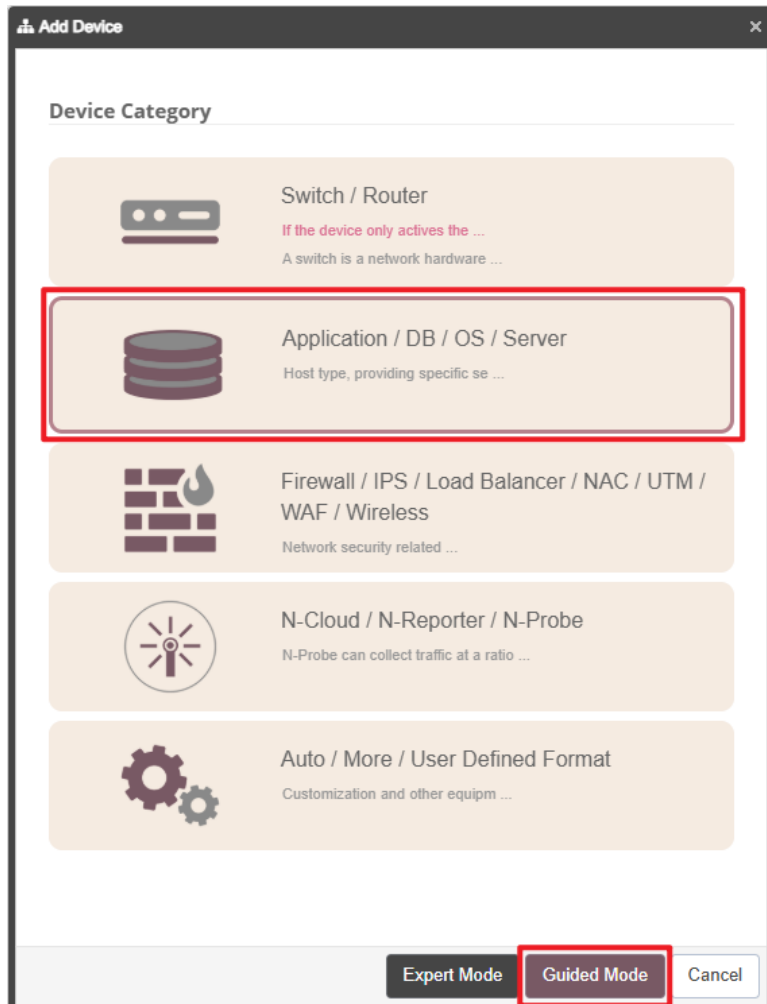
(1) Add a Windows WINDOWS FILE device:

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” → click “Next.”

Add Device - Basic Setting

Basic Setting

Machine Name *
WinFiles-192.168.8.76

IP *
192.168.8.76

Domain *
Global

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

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.

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ
(17) local use 1 (local1) ▼

Encoding
BIG5 ▼

Syslog Normalized Data Retention Days (Max) ⓘ
7-18250

Syslog Normalized Data Retention Days (At Least) ⓘ
1-18250

Raw Data Kept and Replied

☒ 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

Previous **Next** Cancel

(3) Others

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

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

Activate default templates for devices of the same vendor type, click "No."

The screenshot shows a confirmation dialog box with a gear icon and the text "Activate default template, this will apply to the same vendor type ?". At the bottom right, there are two buttons: "Yes" and "No" (highlighted with a red box).

9.2 For Windows 2008 or later

(1) Device Basic Settings

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

Add Device - Basic Setting

Basic Setting

Machine Name *
WinFiles-192.168.8.76

IP *
192.168.8.76

Domain *
Global

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

User Defined Syslog Format ⓘ
Not Activated

SNMP Model ⓘ
Host Mib

Performance Monitoring Setting ▾

Previous **Next** Cancel

(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.

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ

(17) local use 1 (local1) ▼

Encoding

UTF-8 ▼

Syslog Normalized Data Retention Days (Max) ⓘ

7-18250

Syslog Normalized Data Retention Days (At Least) ⓘ

1-18250

Raw Data Kept and Replied

☒ 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

Previous **Next** Cancel

(3) Others

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

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

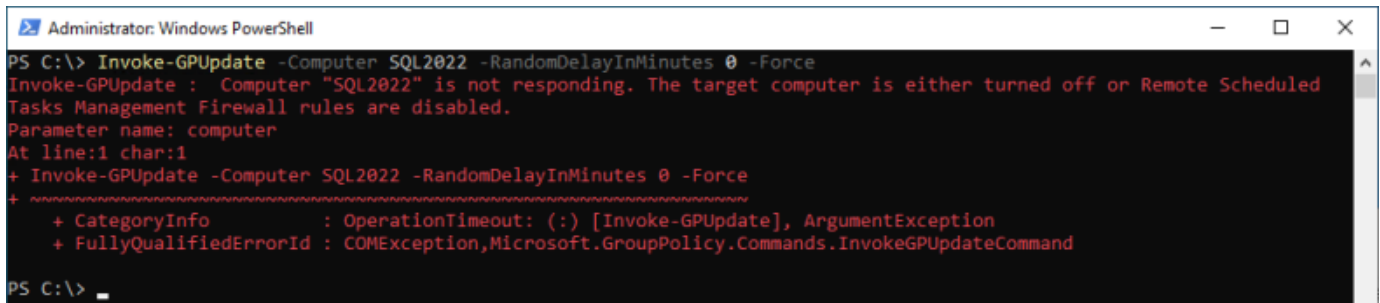
Activate default templates for devices of the same vendor type, click "No."

The screenshot shows a confirmation dialog box with a gear icon and the text "Activate default template, this will apply to the same vendor type ?". At the bottom right, there are two buttons: "Yes" and "No" (highlighted with a red box).

10. Troubleshooting

10.1 Invoke-GPUUpdate Error

(1) On the server, run Invoke-GPUUpdate to update the Windows Server Group Policy. An error message may appear.

A screenshot of an Administrator: Windows PowerShell window. The command 'Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force' has been executed. The output shows an error: 'Invoke-GPUUpdate : Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled Tasks Management Firewall rules are disabled. Parameter name: computer. At line:1 char:1'. Below this, a detailed error message is shown: '+ CategoryInfo : OperationTimeout: (:) [Invoke-GPUUpdate], ArgumentException' and '+ FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUUpdateCommand'.

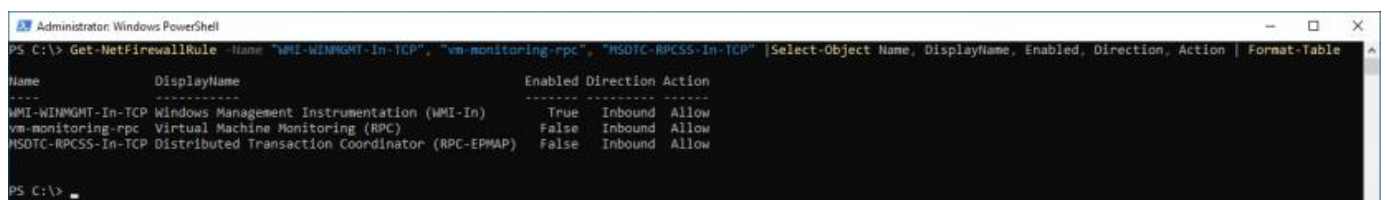
```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUUpdate -Computer SQL2022 -RandomDelayInMinutes 0 -Force
Invoke-GPUUpdate : Computer "SQL2022" is not responding. The target computer is either turned off or Remote Scheduled
Tasks Management Firewall rules are disabled.
Parameter name: computer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

(2) On the Windows Server, open "Windows PowerShell."



(3) Enter the following command to check the Windows Firewall rules for **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, **MSDTC-RPCSS-In-TCP**:

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

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, Enabled, Direction, and Action. The rows are: WMI-WINMGMT-In-TCP (Windows Management Instrumentation (WMI-In), True, Inbound, Allow), vm-monitoring-rpc (Virtual Machine Monitoring (RPC), False, Inbound, Allow), and MSDTC-RPCSS-In-TCP (Distributed Transaction Coordinator (RPC-EPMAP), False, Inbound, Allow).

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

(4) Enter the following command to enable the Windows Firewall rules **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**:

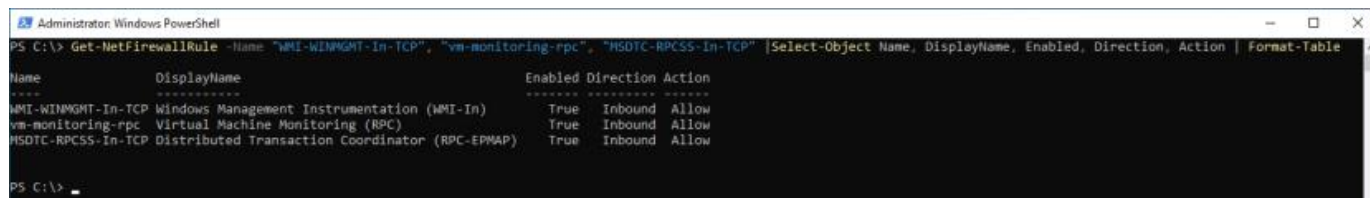
```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -
Enabled True
```

A screenshot of an Administrator: Windows PowerShell window showing the execution of the 'Set-NetFirewallRule' command. The command is: 'Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True'.

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

(5) Enter the following command to verify the Windows Firewall rules **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, **MSDTC-RPCSS-In-TCP** again:

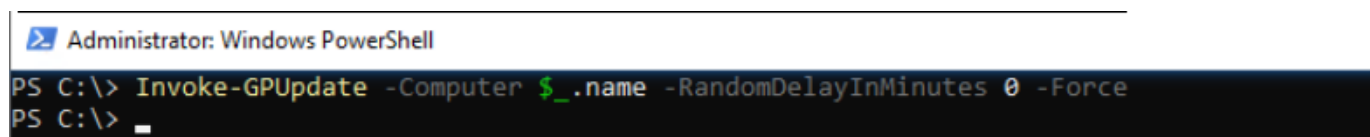
```
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" |  
Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
```



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

(6) On the server, enter the following command to update the Windows Server Group Policy:

```
PS C:\> Invoke-GPUUpdate -Computer Win2019 -RandomDelayInMinutes 0 -Force
```



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

Note: Replace the text shown in **red** with the Windows Server name.



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

Sales Information : sales@npartner.com

Technical Support : support@npartner.com