N-Partner

How to Configure Windows File Event Log

V010

2025/08/28

Copyright Declaration

Registered Trademark

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

Contents

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

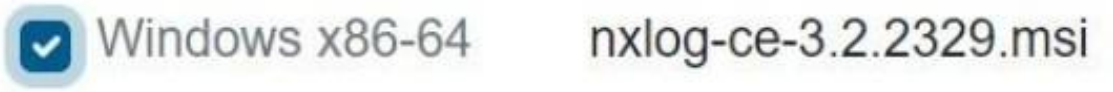
1.1 NXLog Installation

(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**

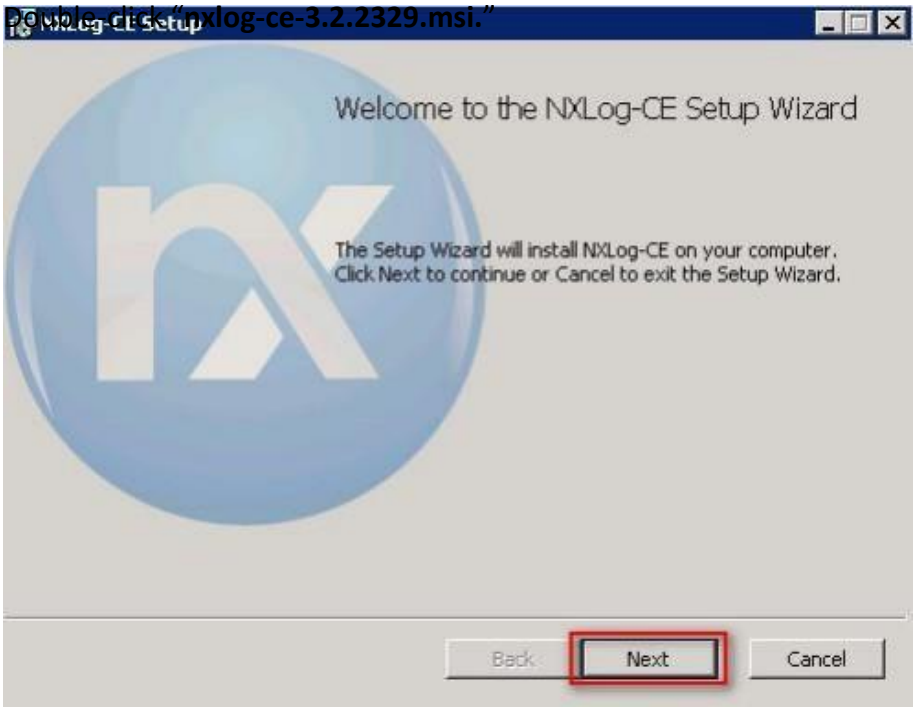


Note: If you require the 32-bit version of NXLog, please contact our support team.

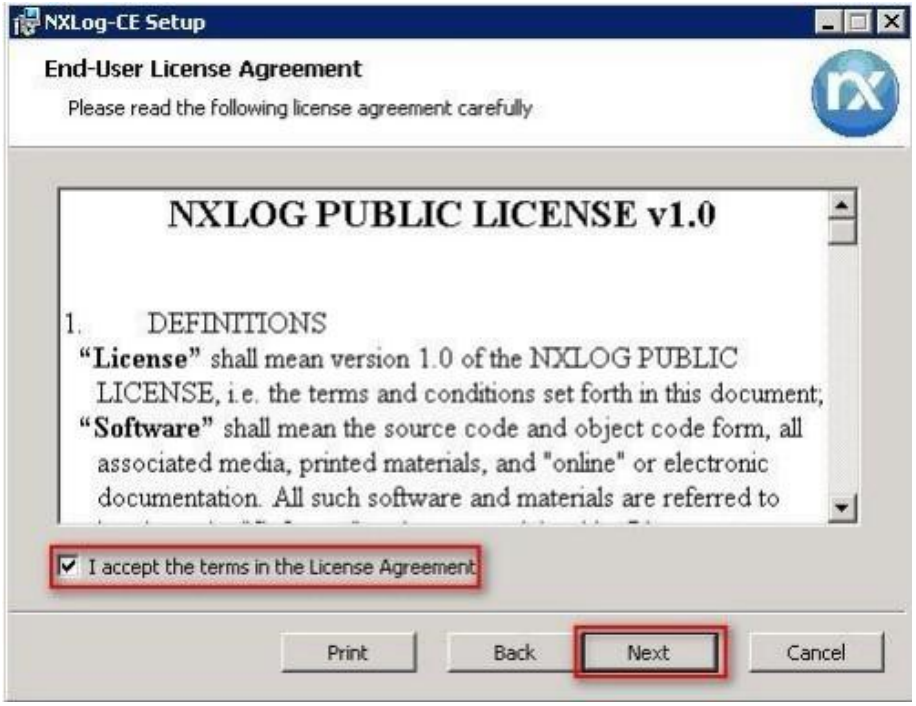
(2) Install NXLog

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

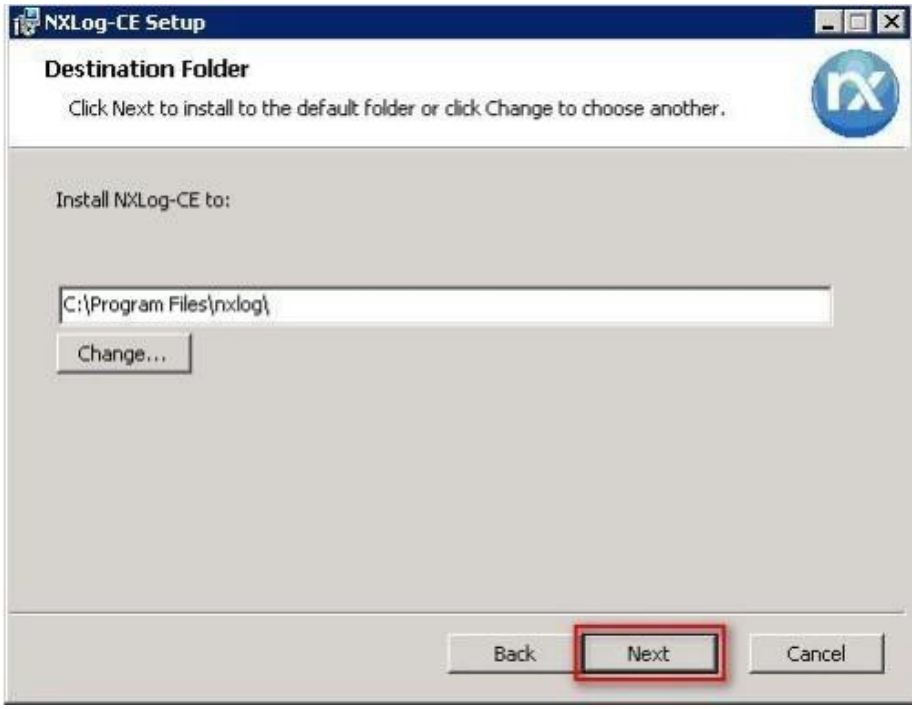
Double-click "**nxlog-ce-3.2.2329.msi.**"



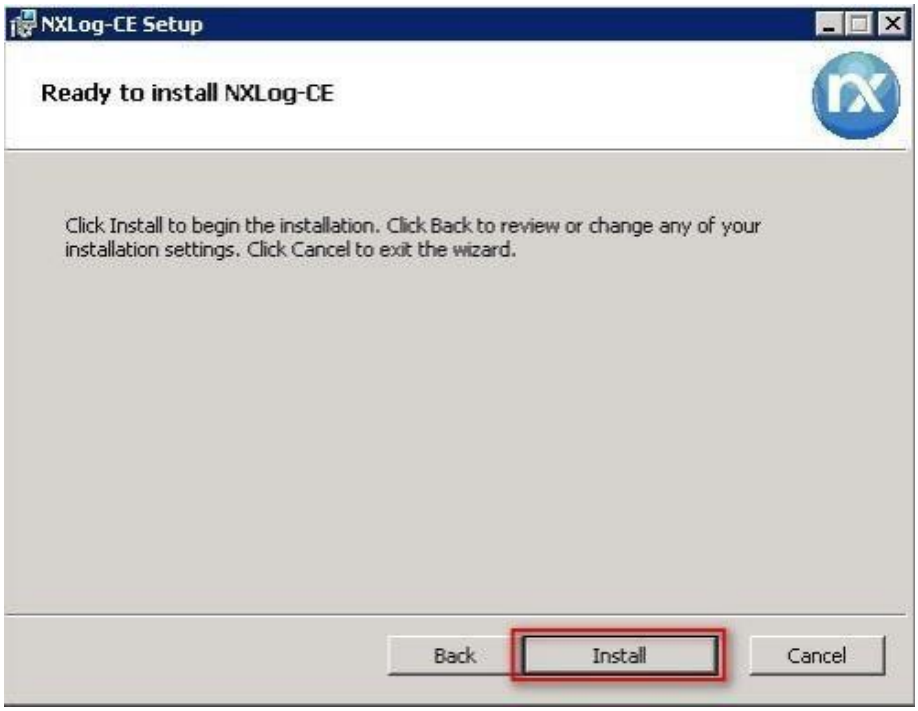
(3) Select “I accept the terms in the License Agreement,” then click “Next.”



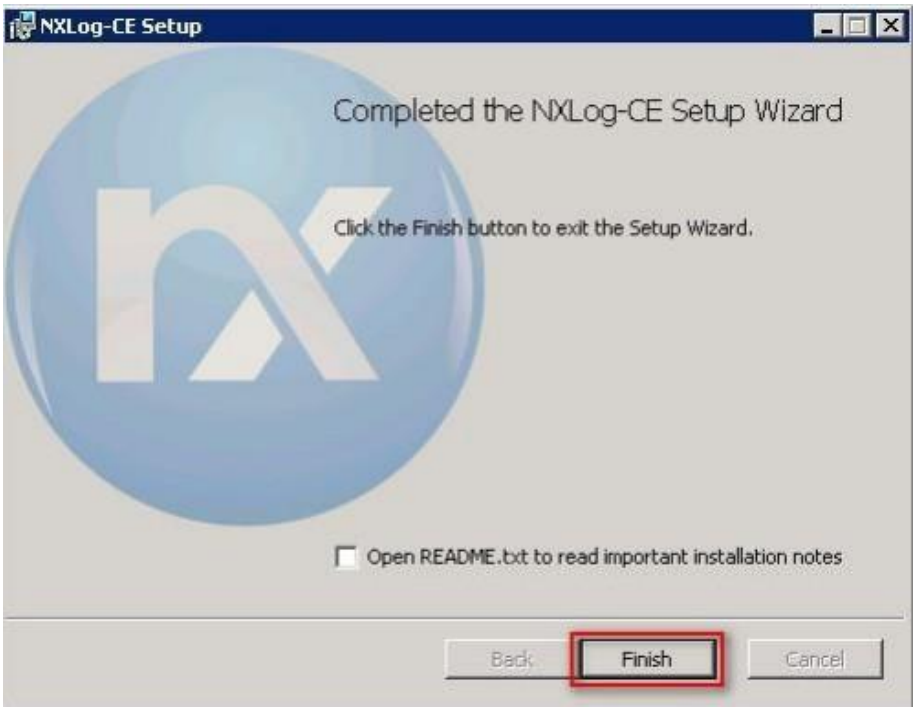
(4) Click “Next.” (The default installation path is (C:\Program Files\nxlog\).



(5) Click “Install.”

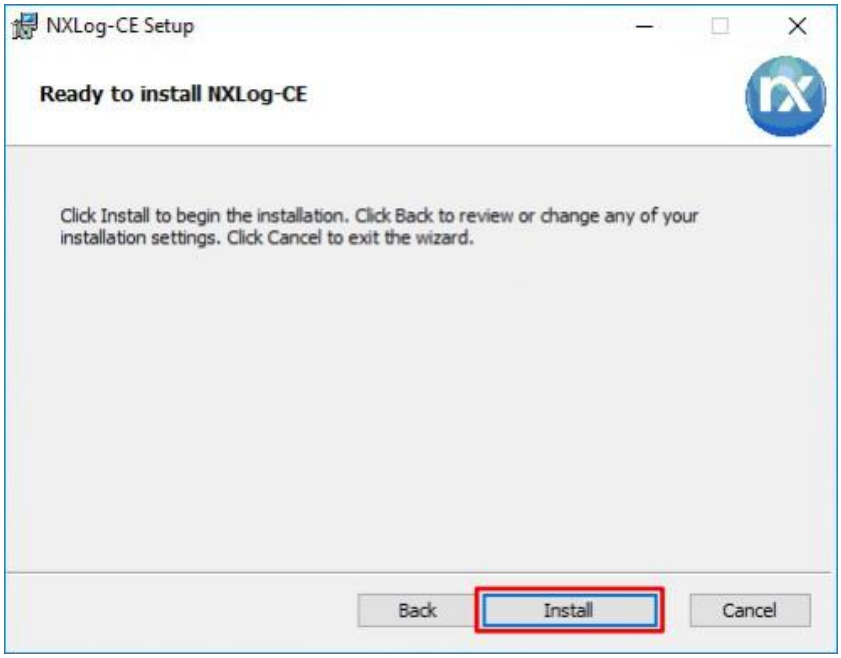


(6) Click “Finish.”



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

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

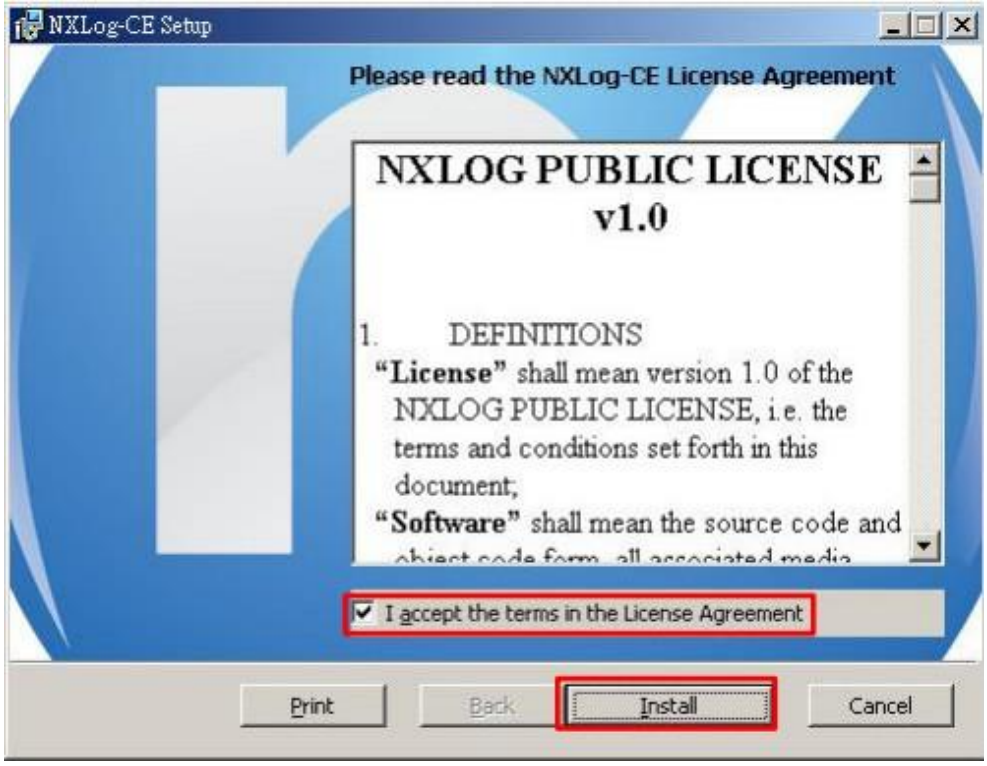


<2.3> For Windows **2000**:

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

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

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



1.2 Download NXLog Configuration File

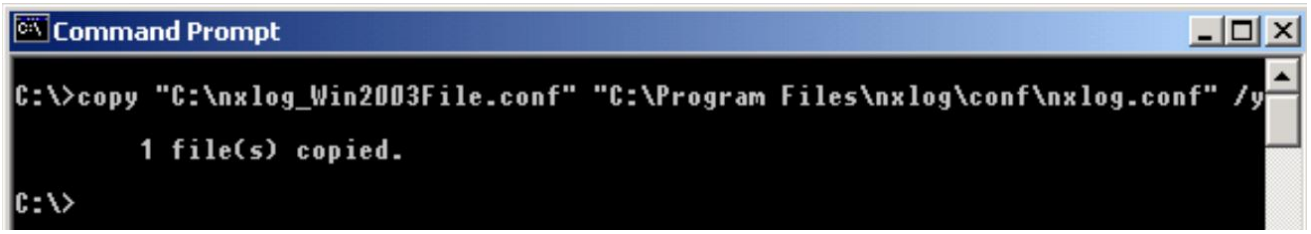
1.2.1 For Windows Server 2003 or earlier:

(1) 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       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>
```


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>
```

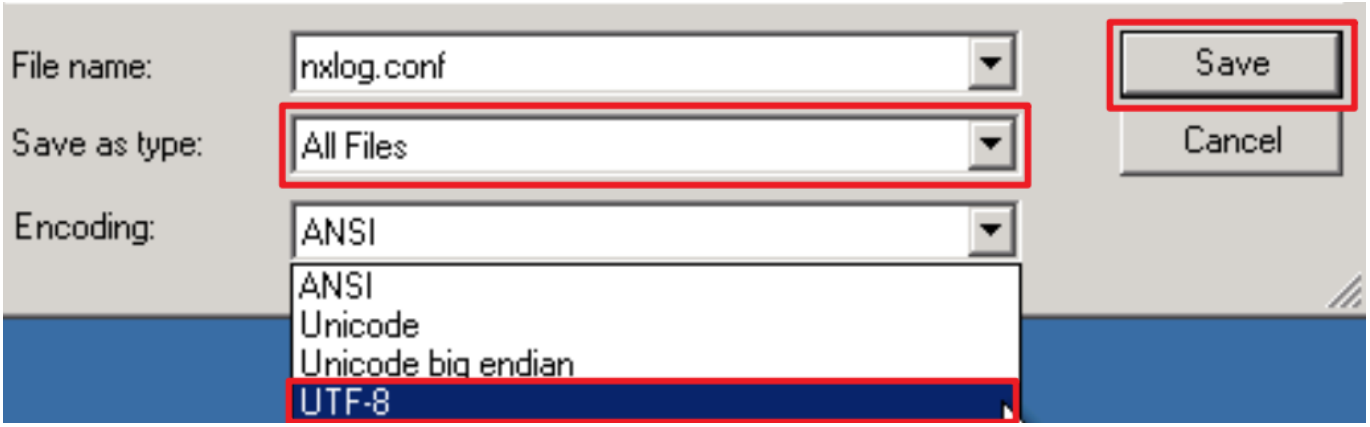
Enter the N-Reporter system IP address in the blue text section.

```
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>
```

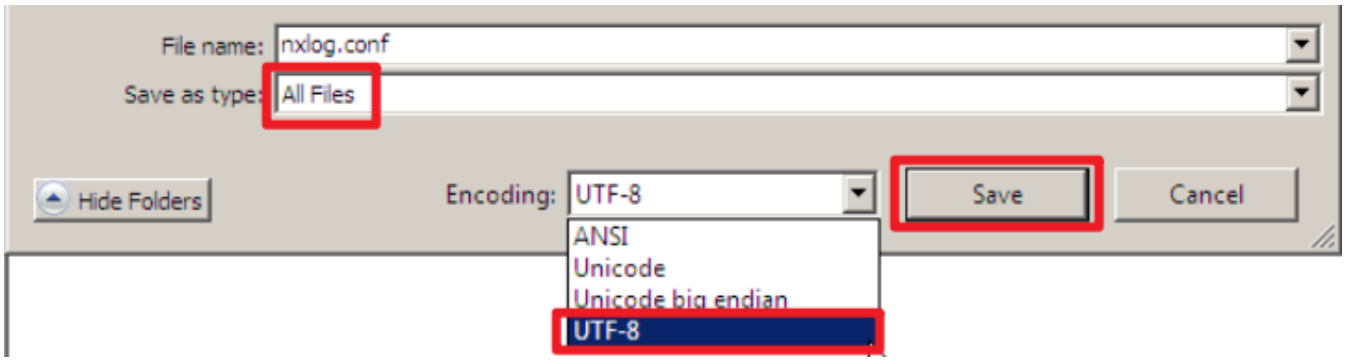
Enter the N-Reporter system IP address in the blue text section.

```
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.

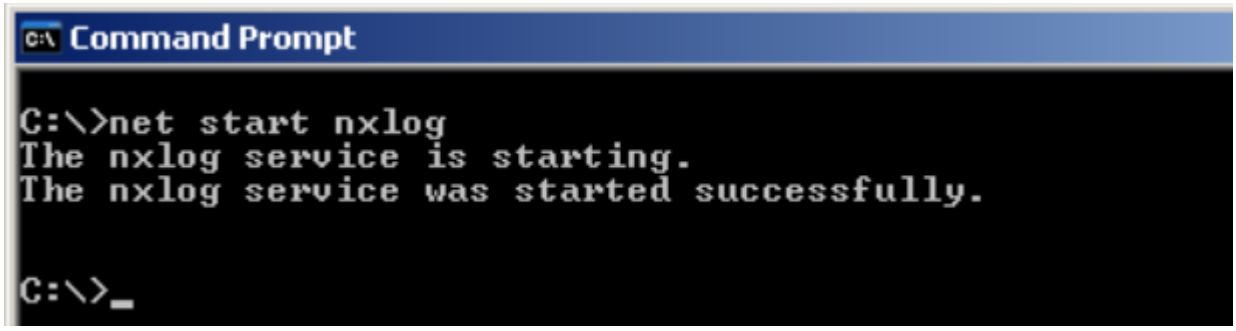
1.4 Starting the NXLog Service

1.4.1 For Windows Server 2003 or earlier

(1) Open “Command Prompt.”

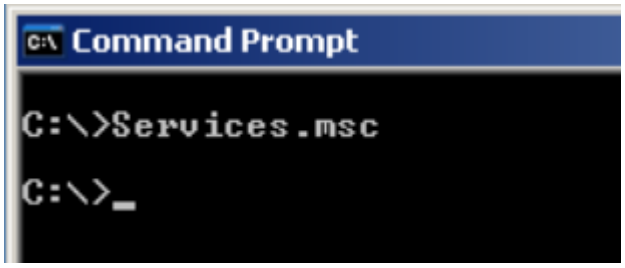
(2) Start the NXLog service and verify that there are no error messages:

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

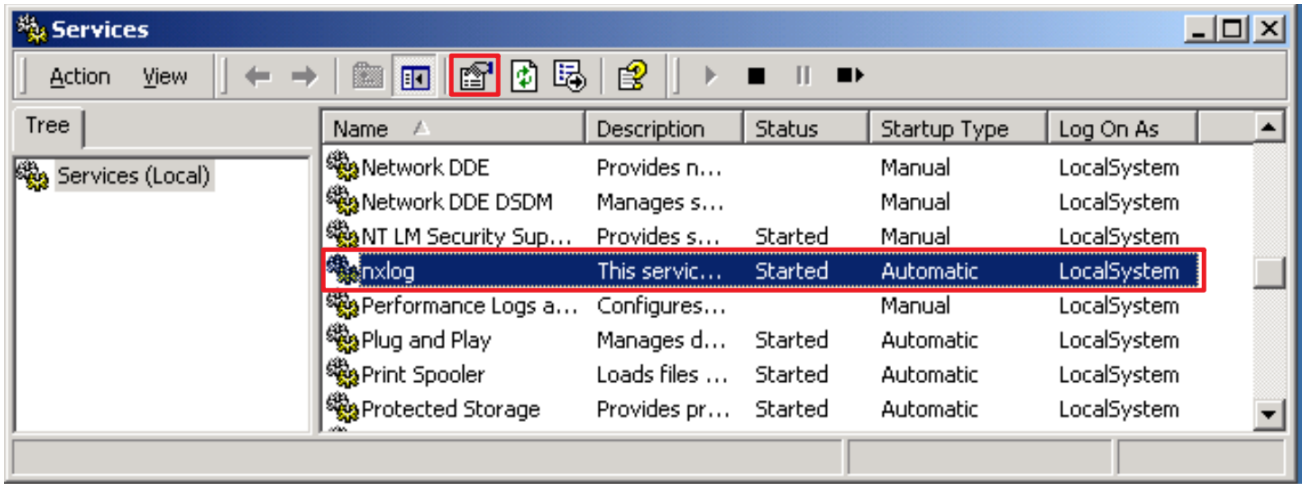


(3) Enter the command below to open the **Services** console:

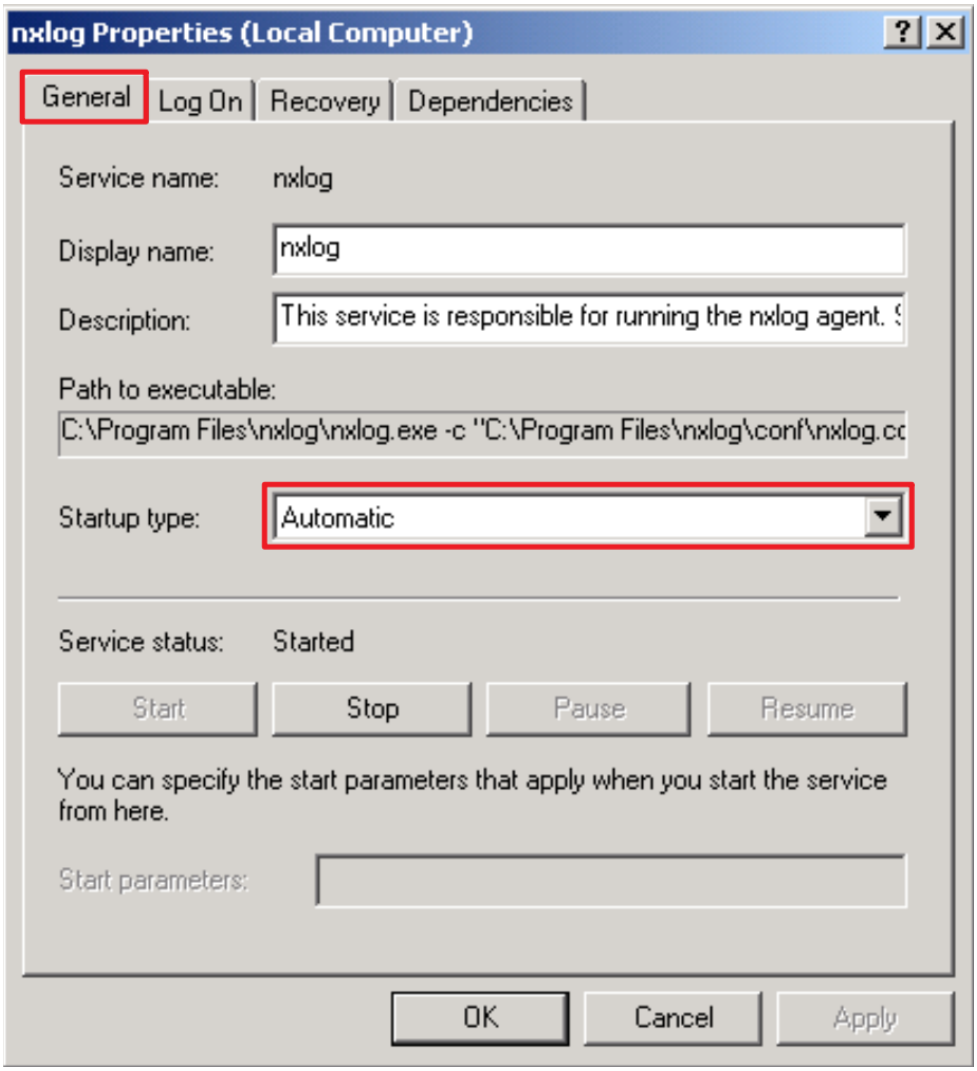
```
C:\> Services.msc
```



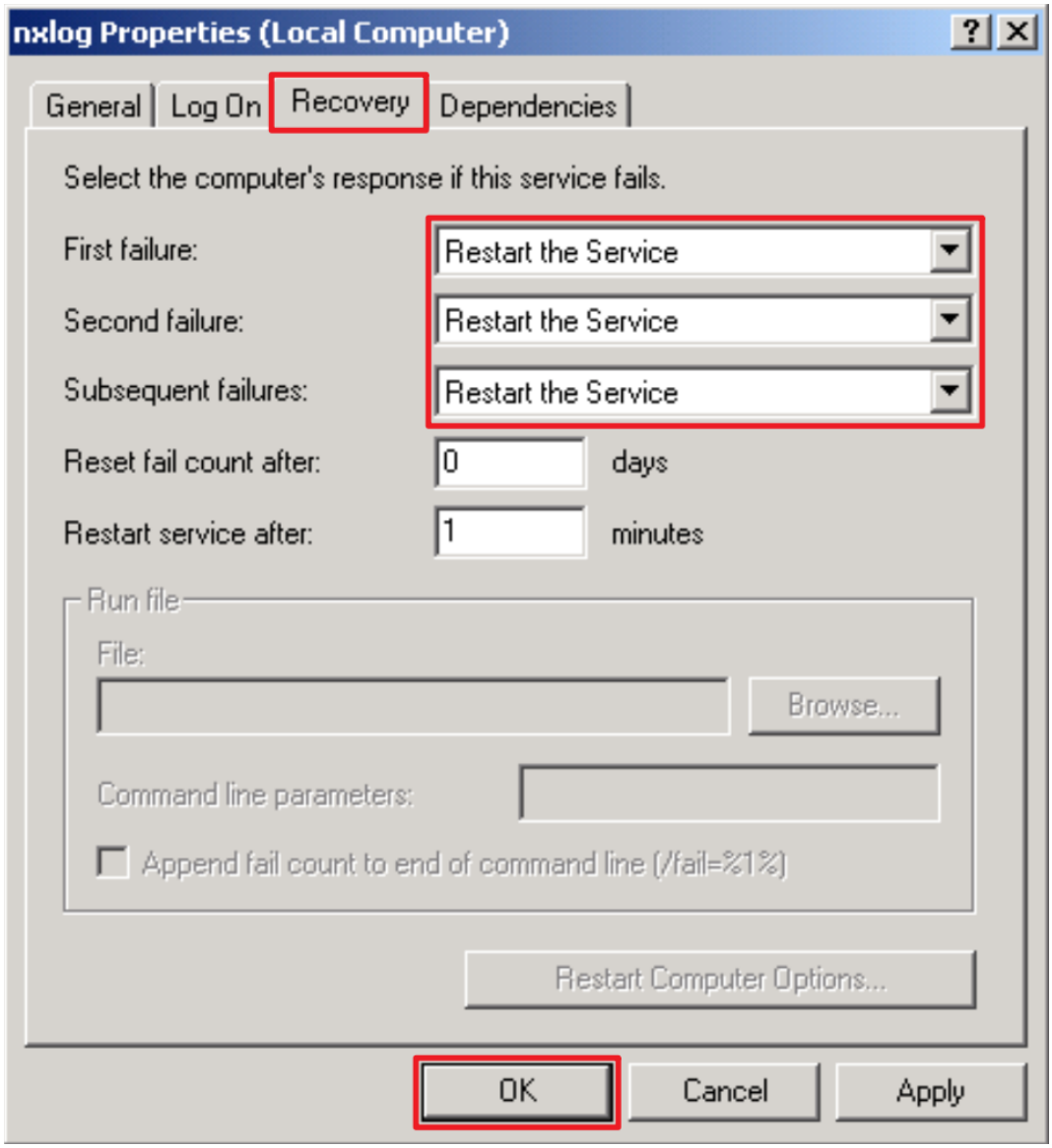
(4) Open the NXLog service properties: select “NXLog” → Click “Properties.”



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



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

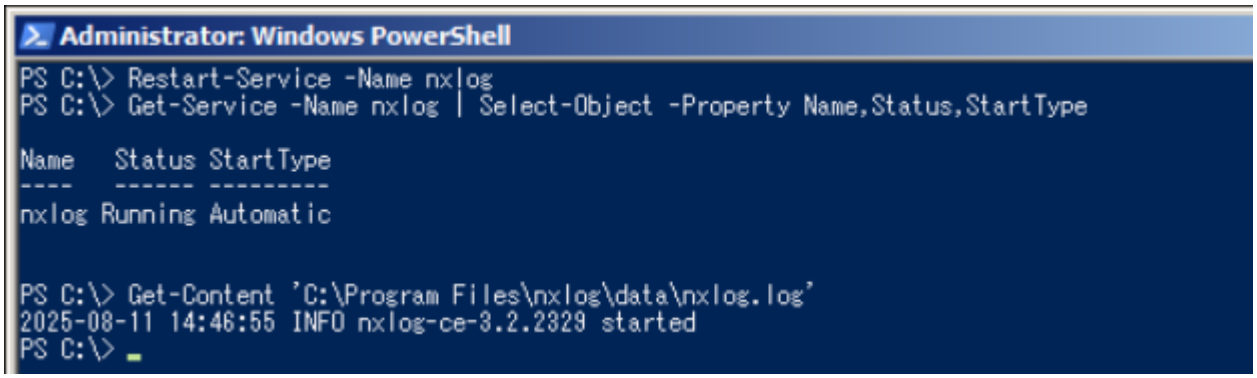


1.4.2 For Windows Server 2008 or later

(1) Open “Windows Powershell.”

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

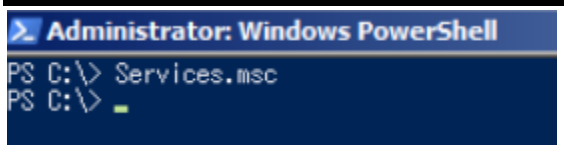
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\ Program Files\ nxlog\data\nxlog.log'
```



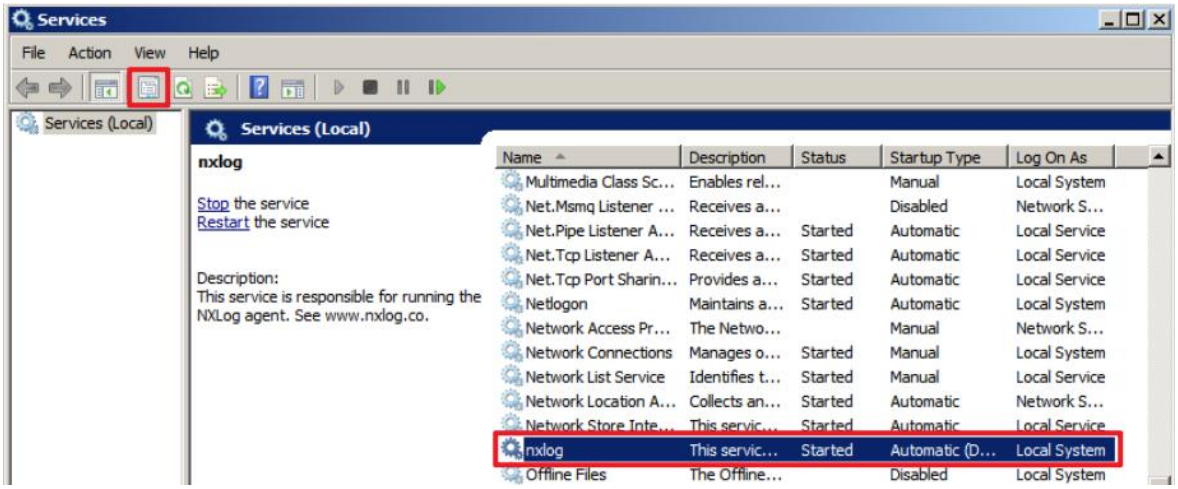
Note: This example is for a 64-bit operating system. For a 32-bit system, replace the highlighted text with: 'C:**\Program Files(x86)**\nxlog\conf\nxlog.conf'

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

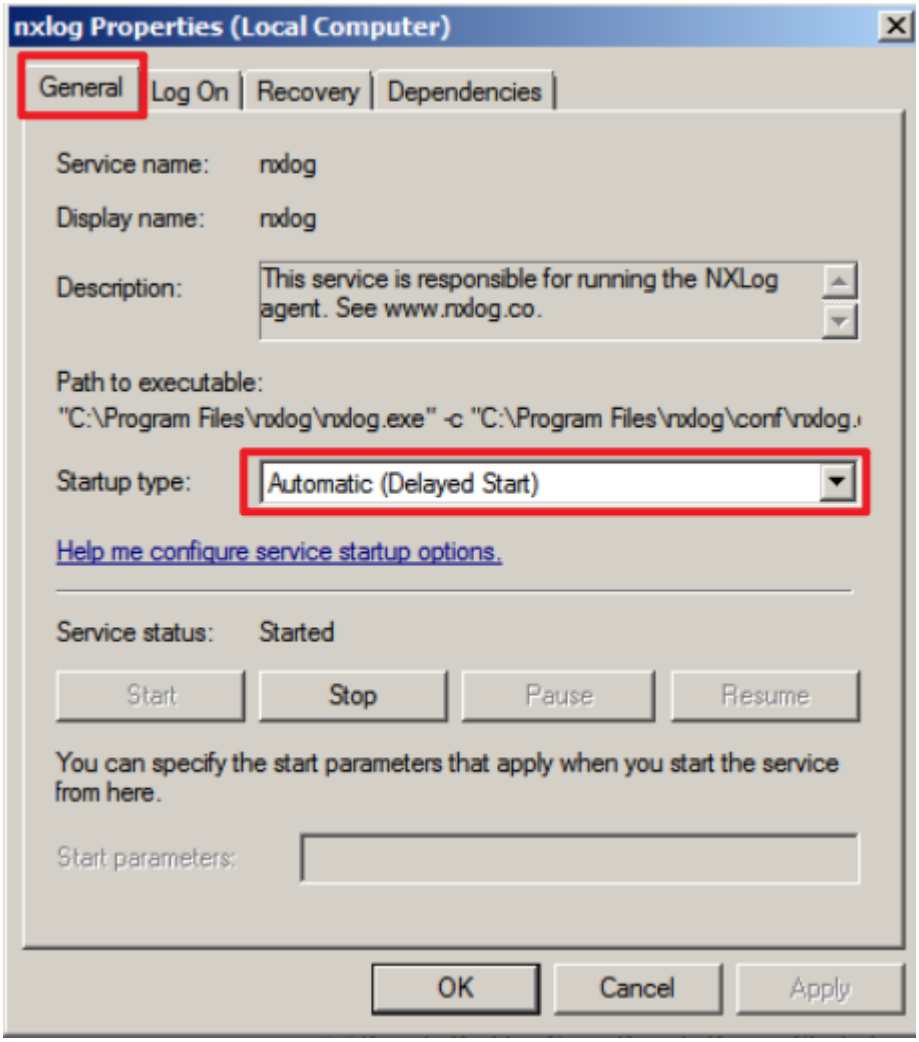
```
PS C:\> Services.msc
```



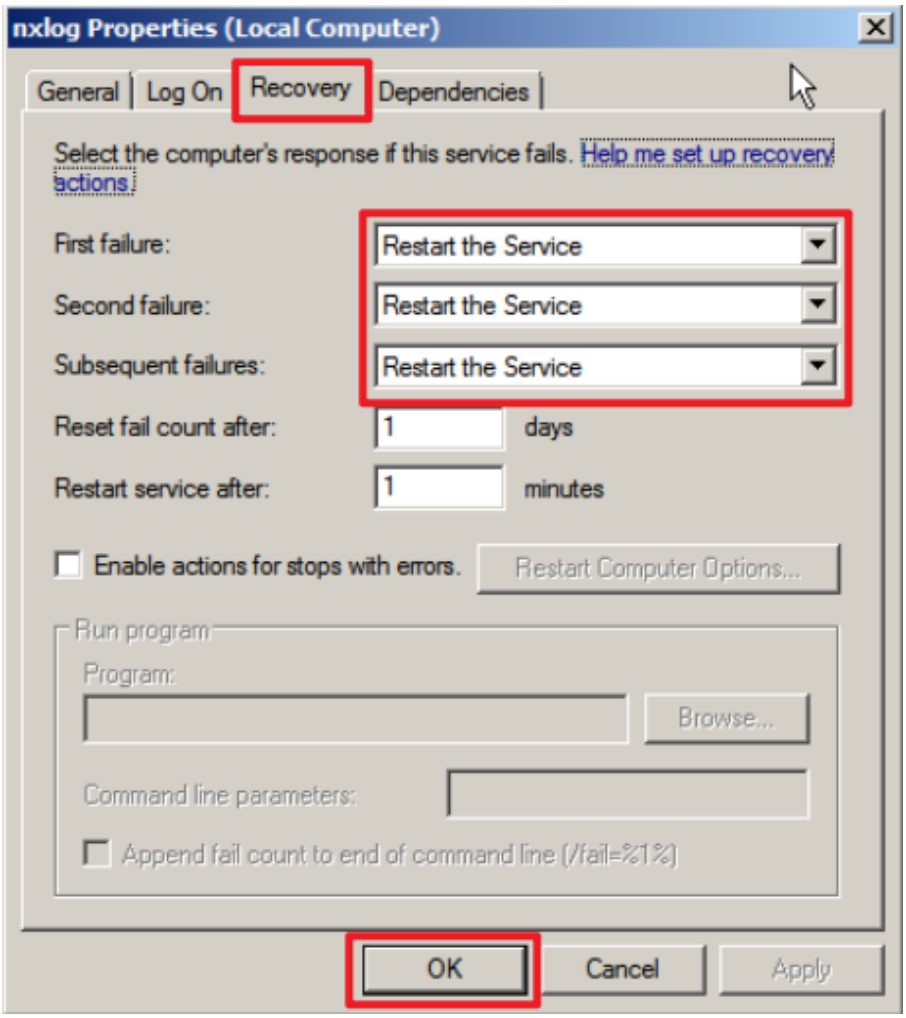
(4) Open the NXLog service properties: select “NXLog” →  Click “Properties.”



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



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



2. Windows Server 2000

2.1 Domain

Windows Audit Policy Configuration:

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

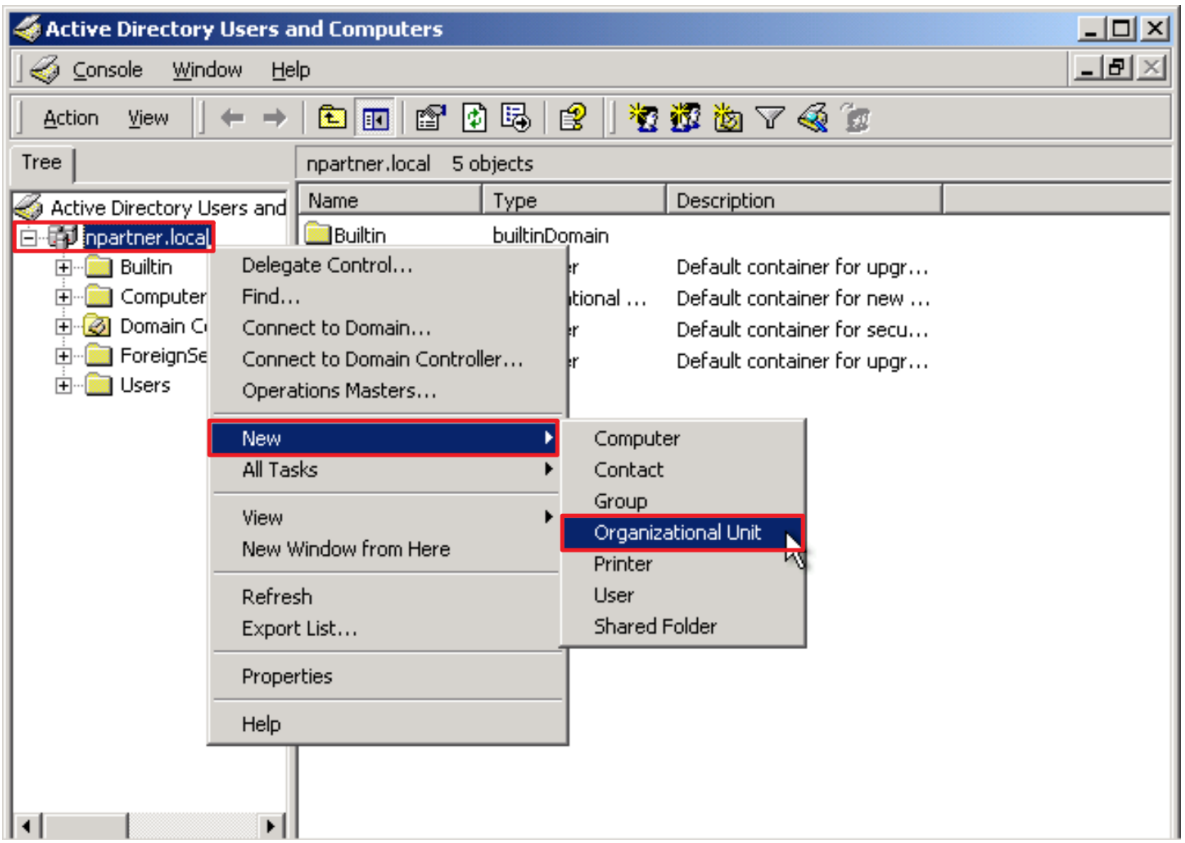
The following sections describe the configuration methods for Domain and Workgroup environments.

2.1.1 Organizational Unit (OU) Configuration

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

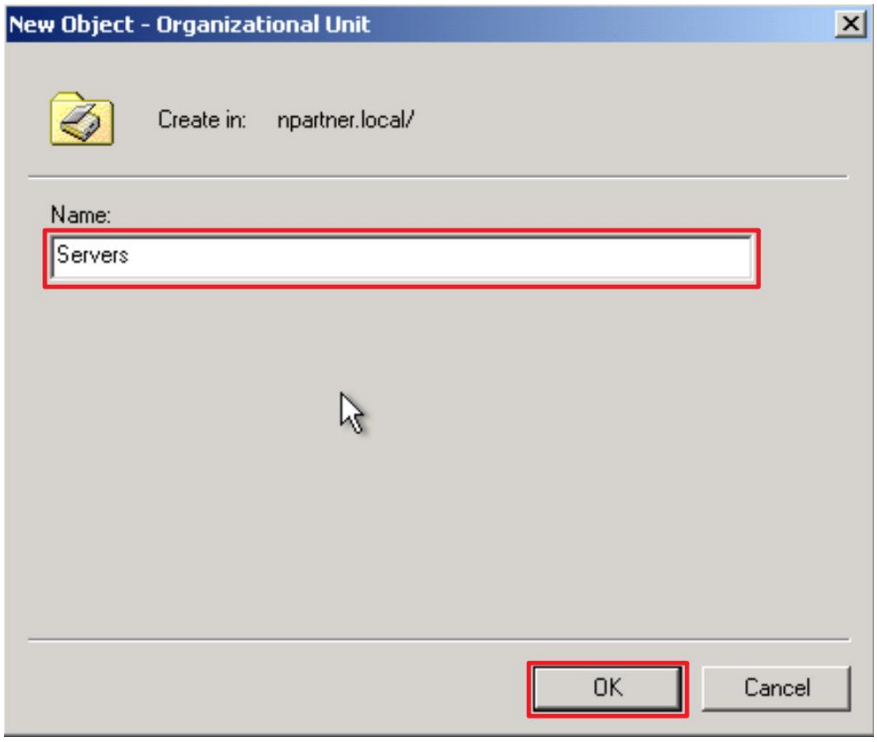
(2) Add an Organizational Unit

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



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

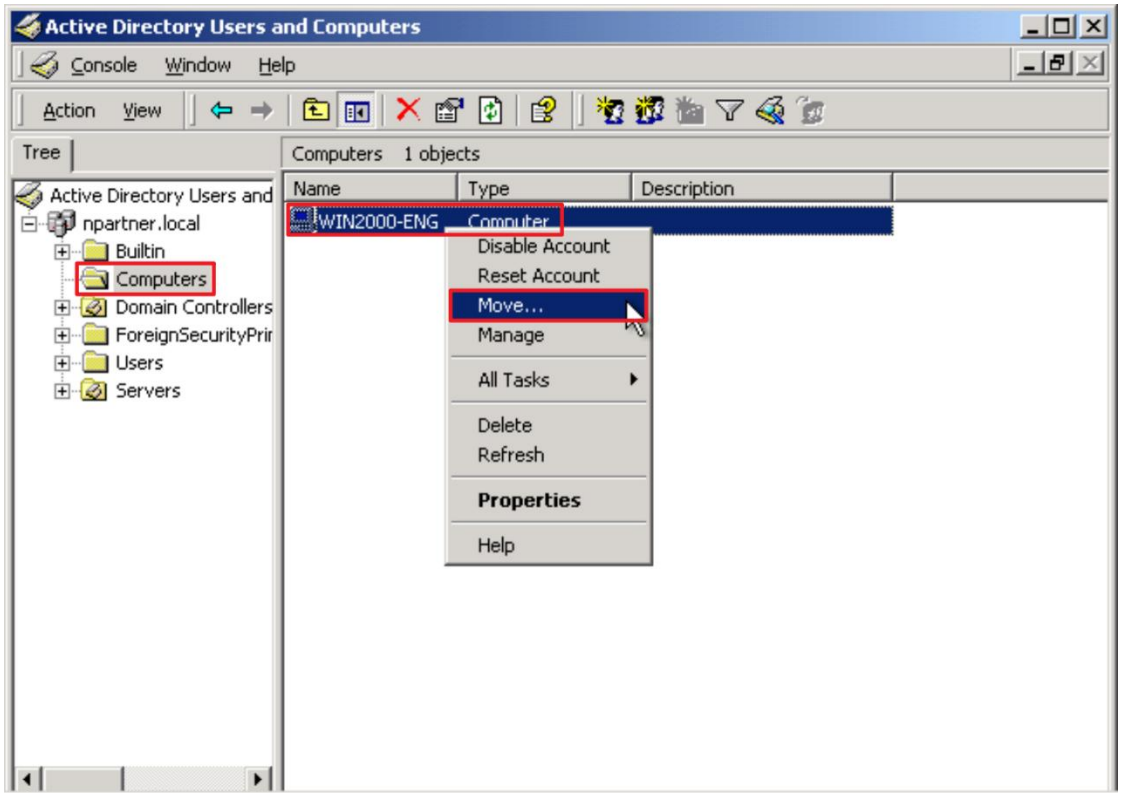
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

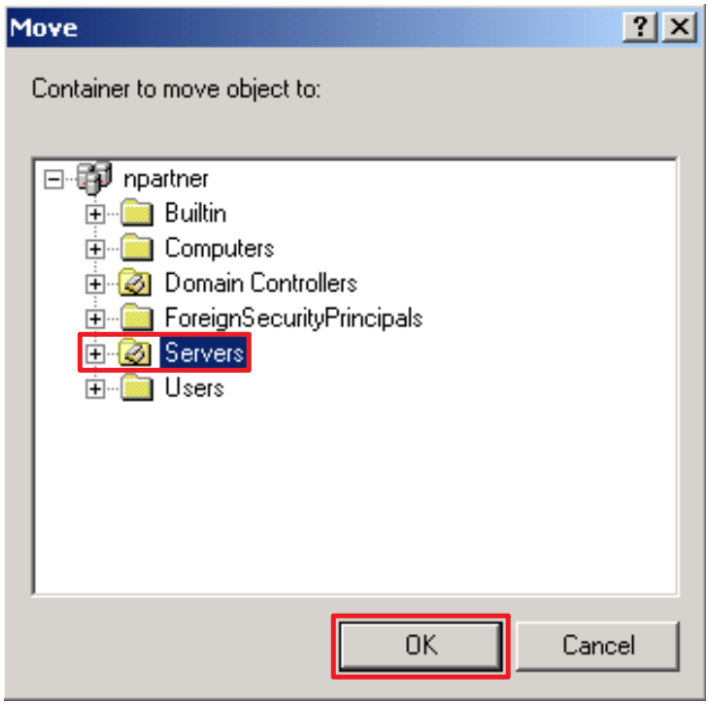
Select the “Computers” organizational unit (OU) → right-click on the “WIN2000-ENG” server.

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



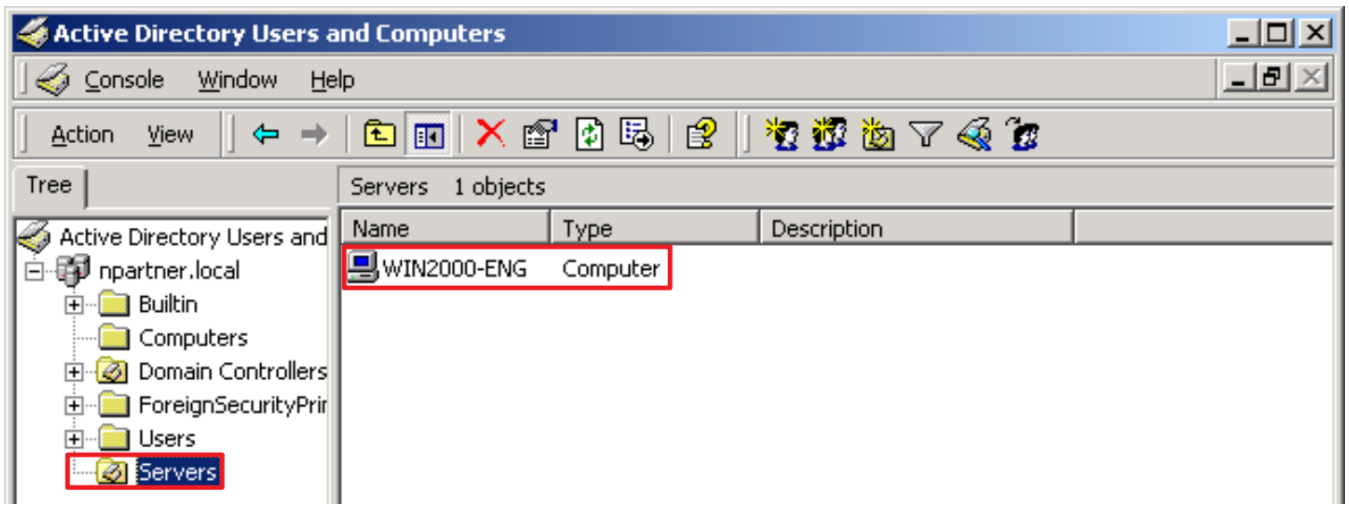
(5) Select your Organizational Unit:

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



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

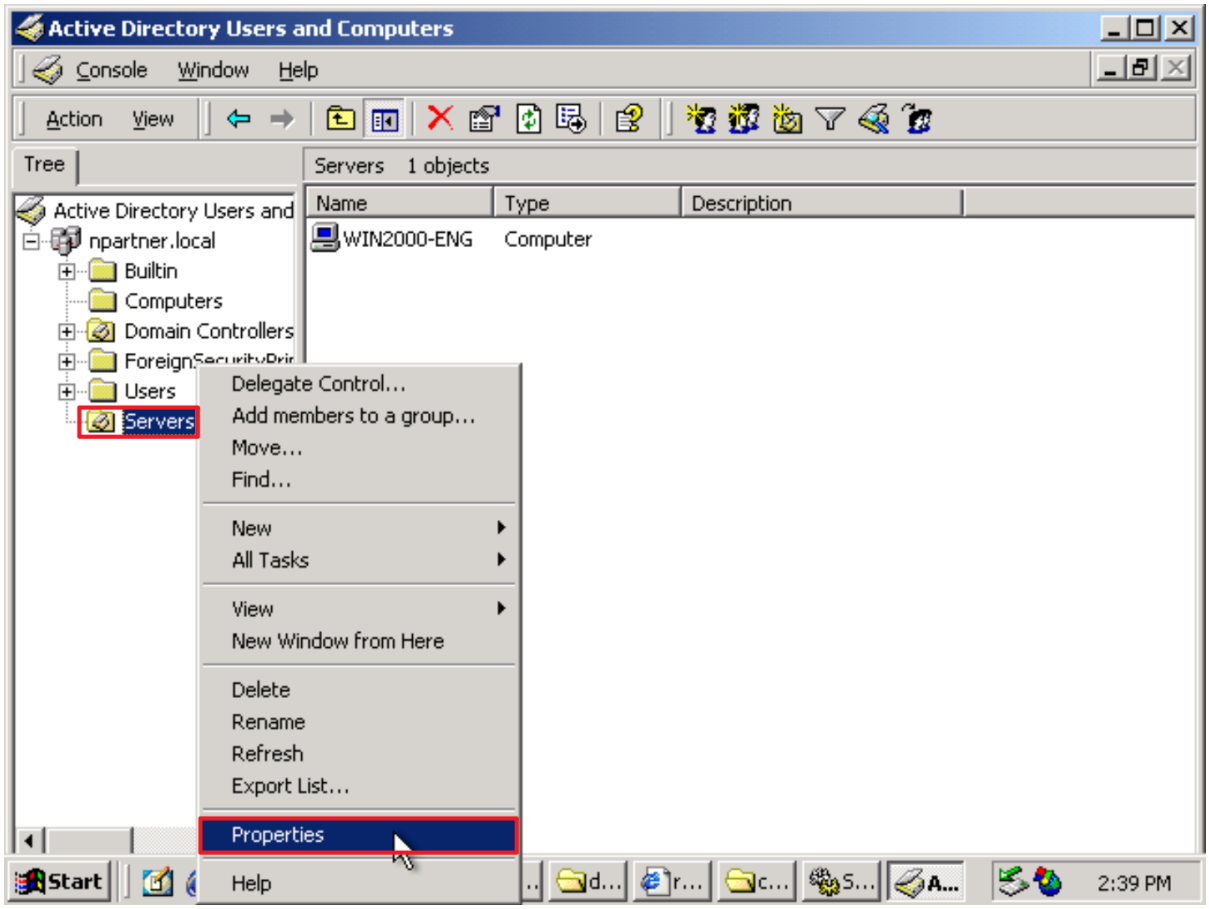
Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2000-ENG” server has been moved.



2.1.2 Group Policy Settings

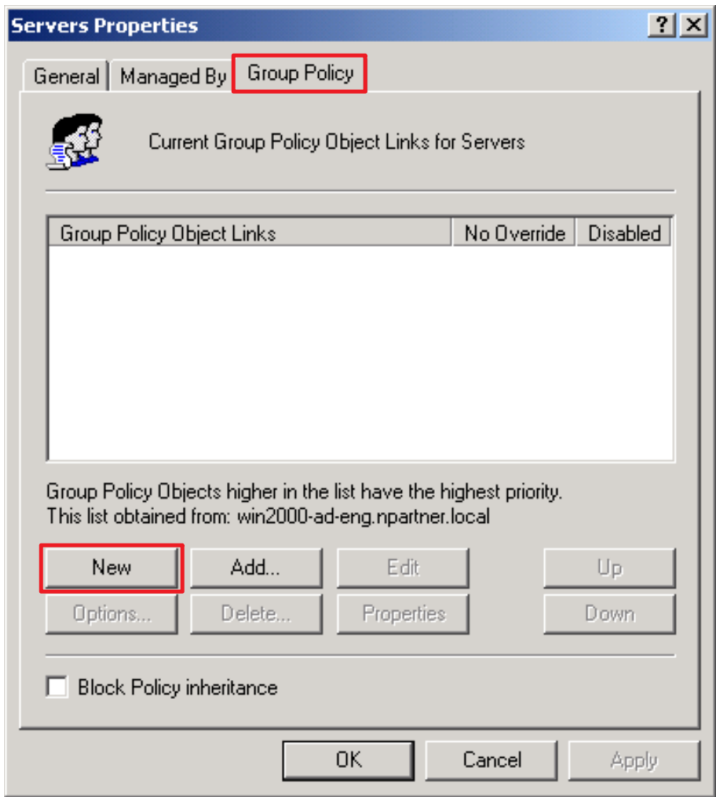
(1) Click “Active Directory Users and Computers.”

(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.”

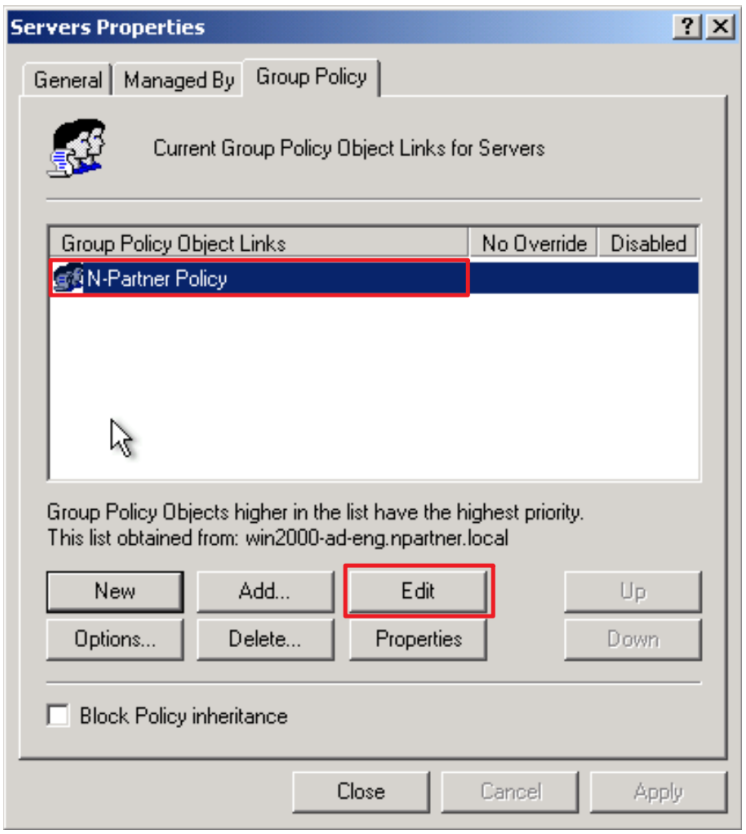


(4) Edit your Group Policy Object

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

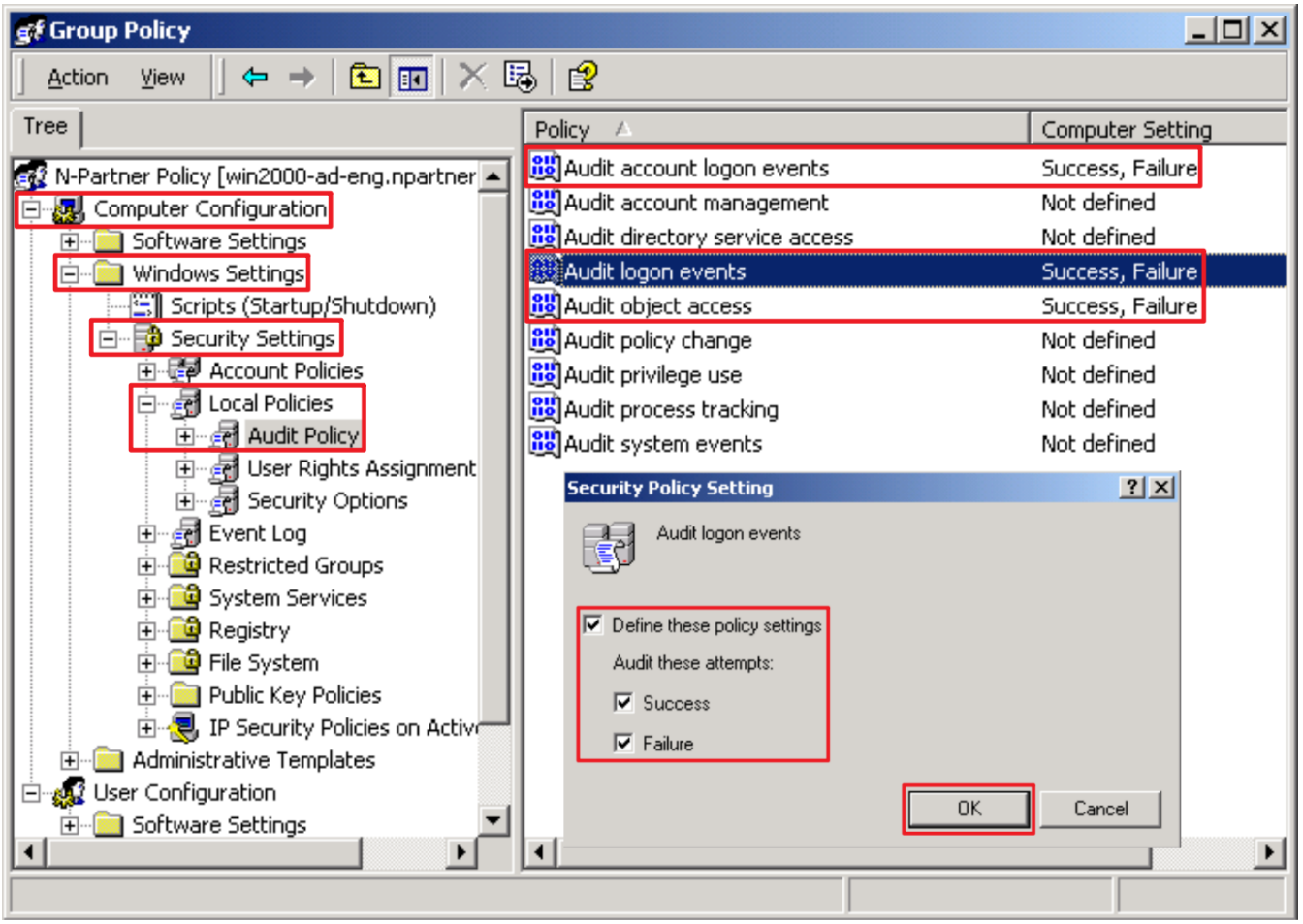
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



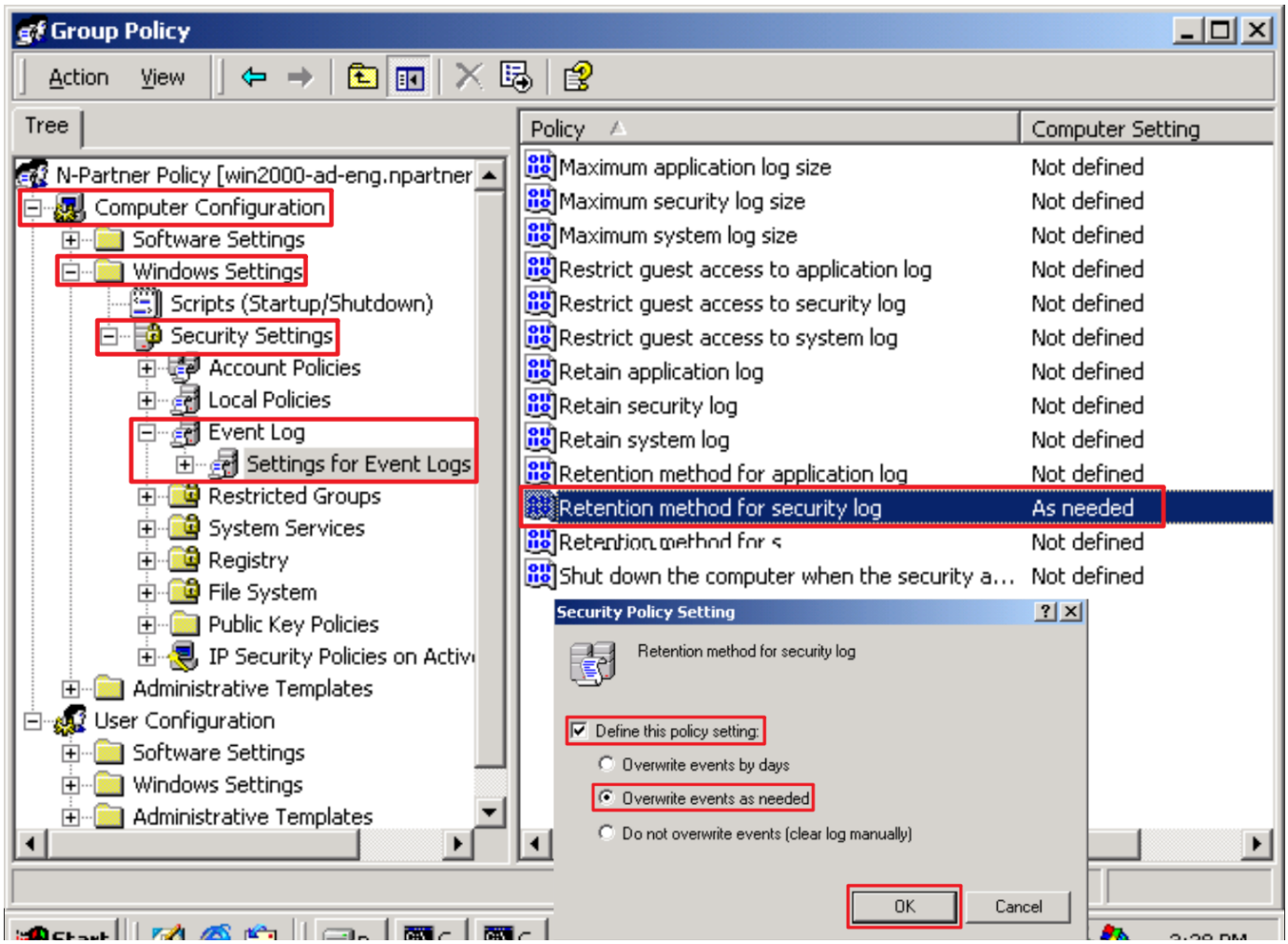
(5) Local Group Policies: Audit Policy

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

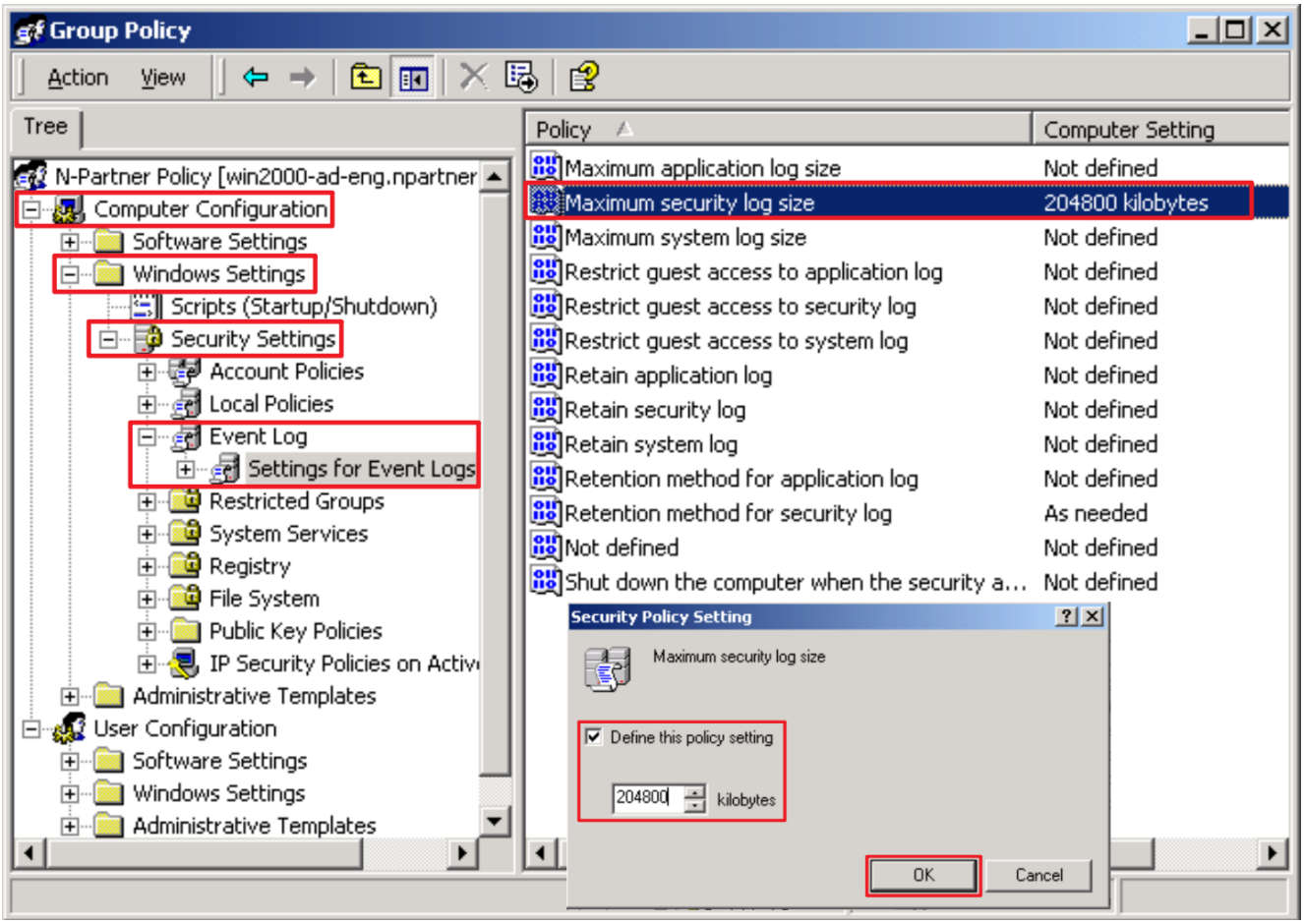
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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

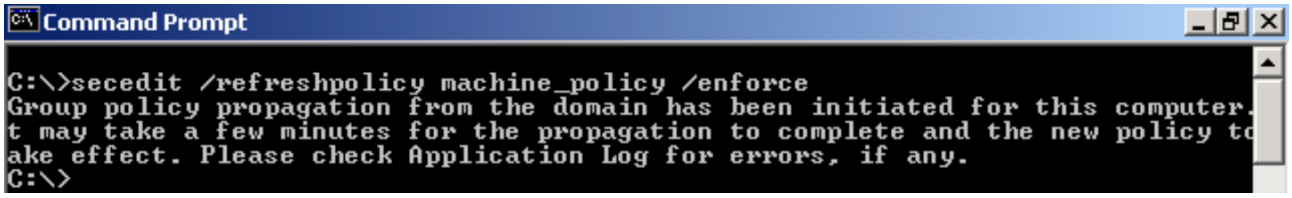
Note: Please adjust the number based on the actual environment. → click “OK.”



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

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

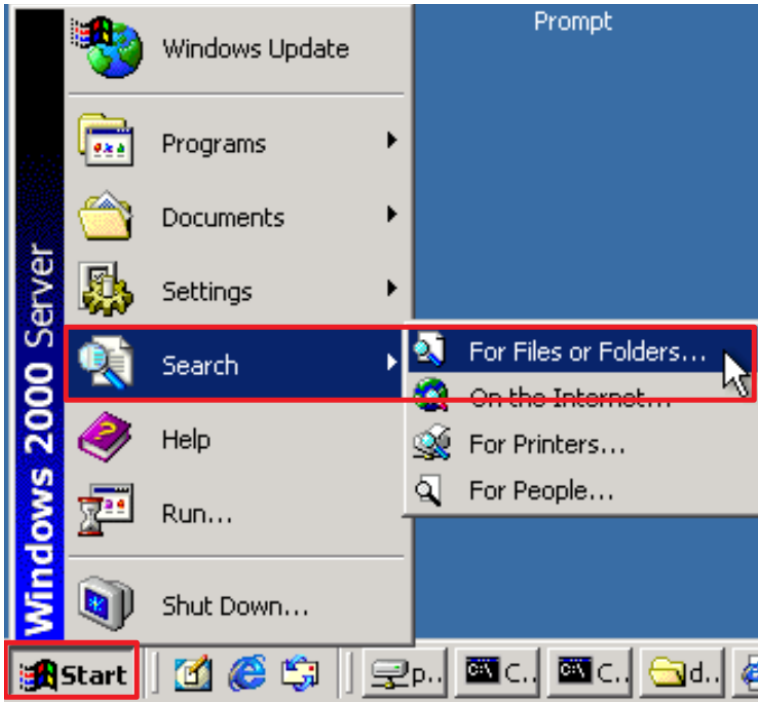
```
C:\> secedit /refreshpolicy machine_policy /enforce
```



2.2 Workgroup

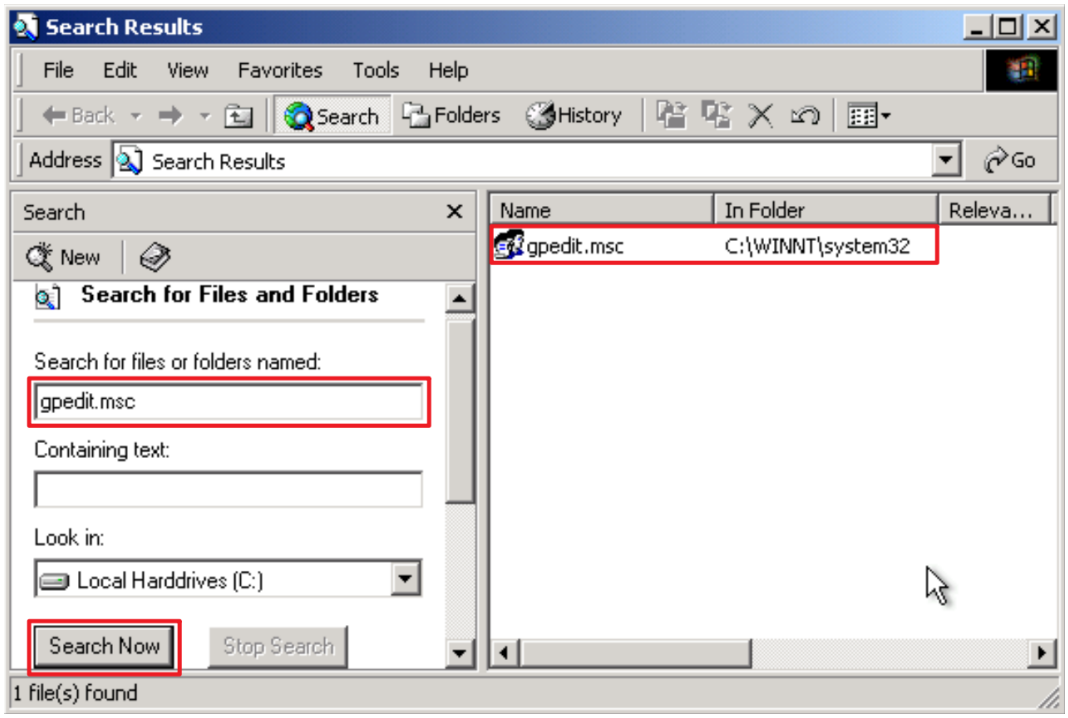
2.2.1 Audit Policy Configuration

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



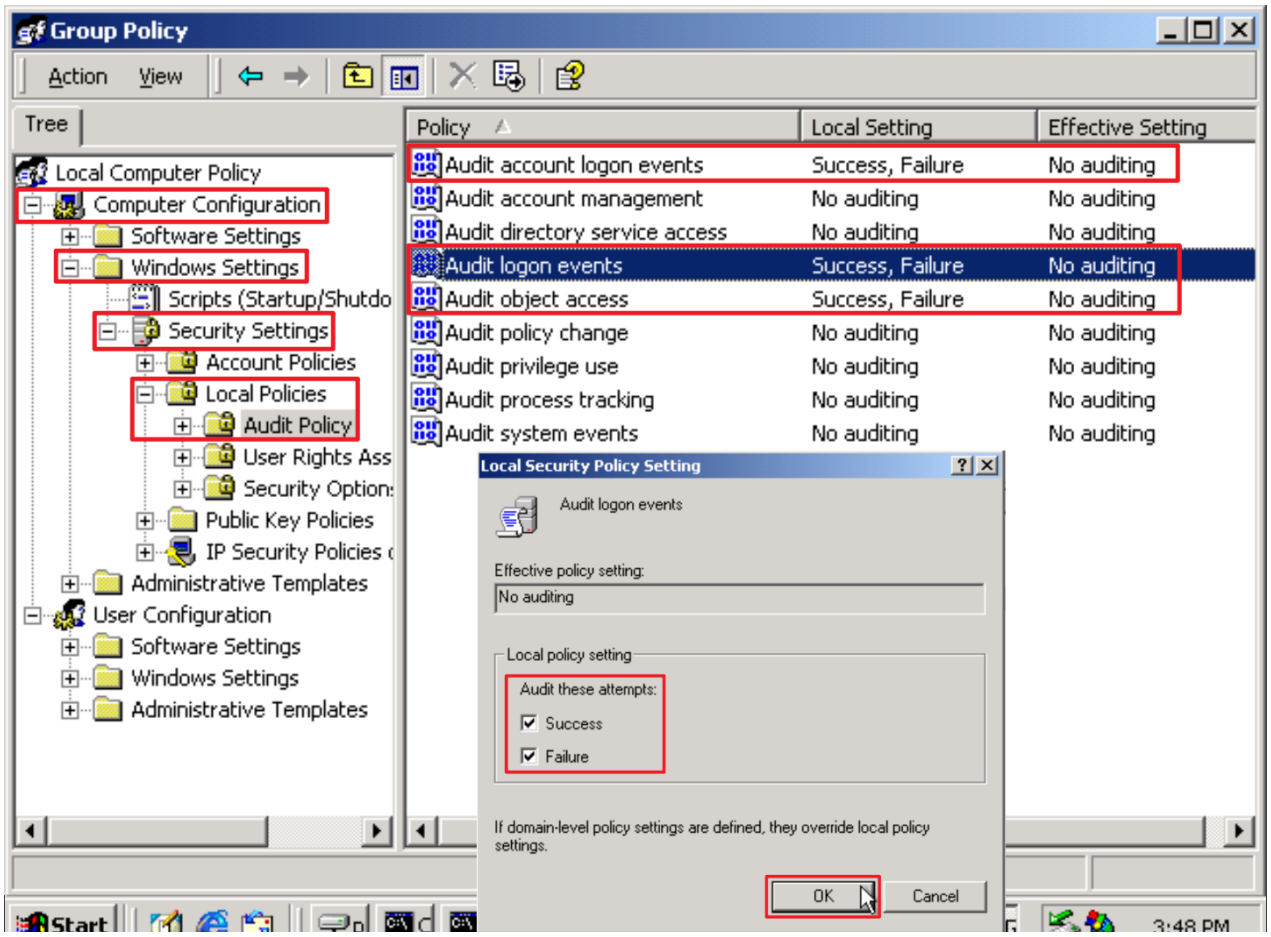
(2) Search for the Group Policy Object Editor

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



(3) Local Group Policies: Audit Policy

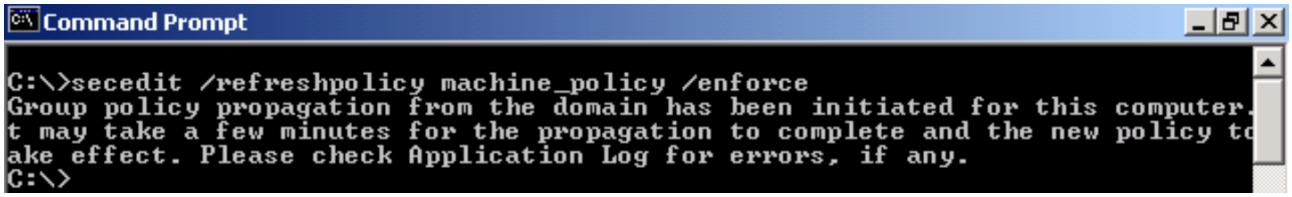
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



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

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

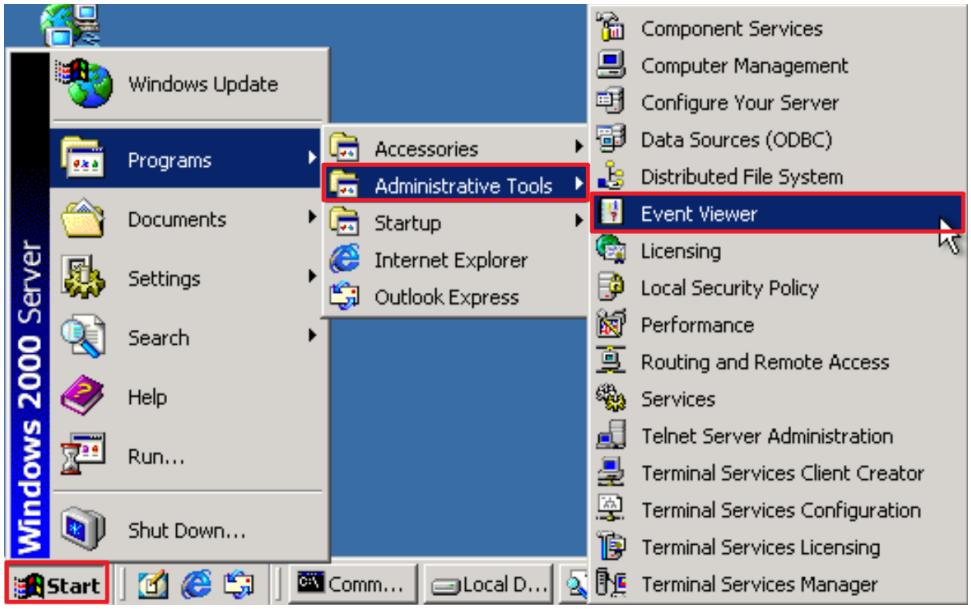
```
C:\> secedit /refreshpolicy machine_policy /enforce
```



2.2.2 Event Log Settings

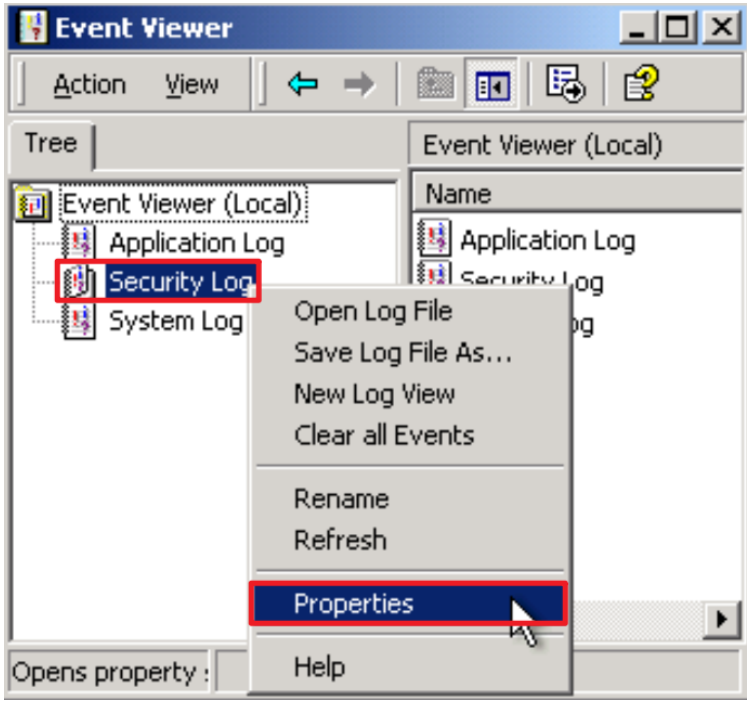
(1) Search for “Event Viewer”

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



(2) Edit Security Log

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

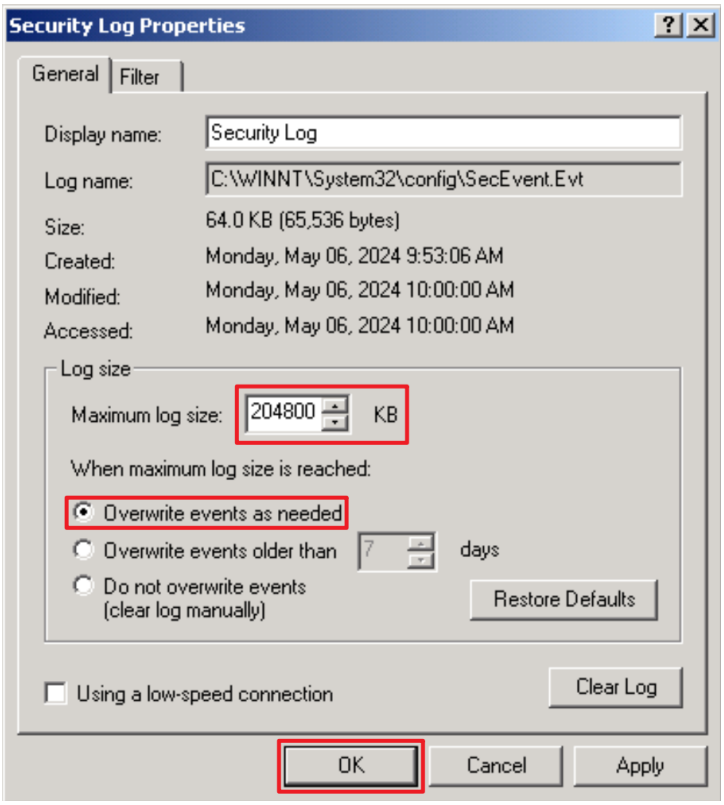


(3) Configure Security Log

Enter maximum log file size: 204800 KB

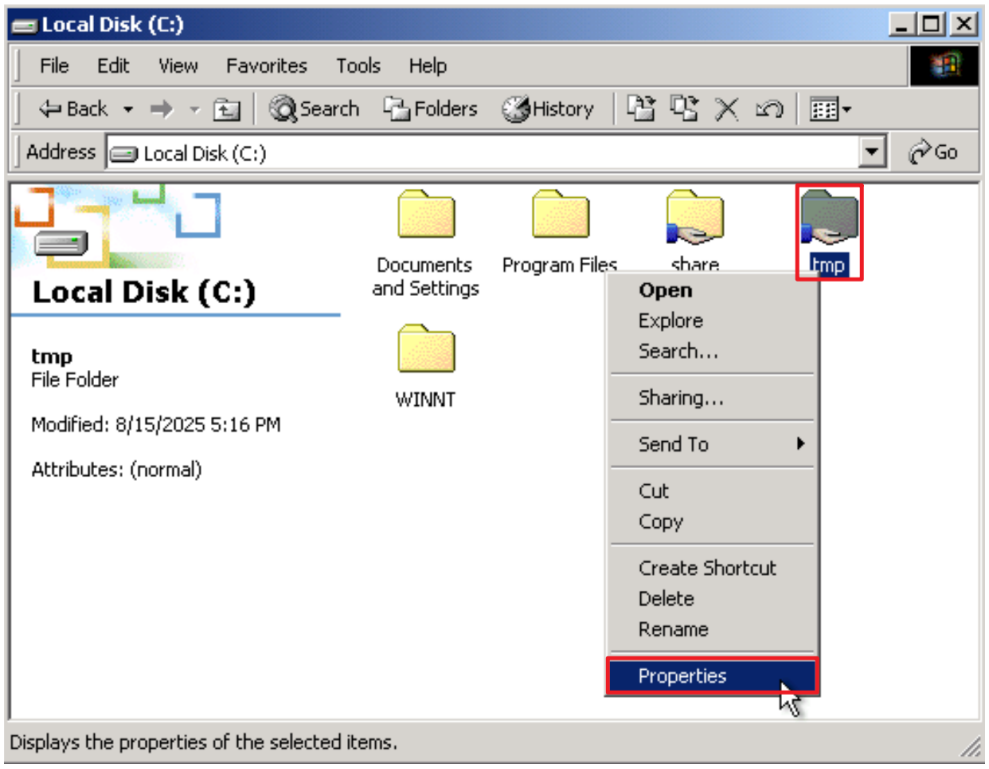
Note: Please adjust the number according to the actual environment.

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

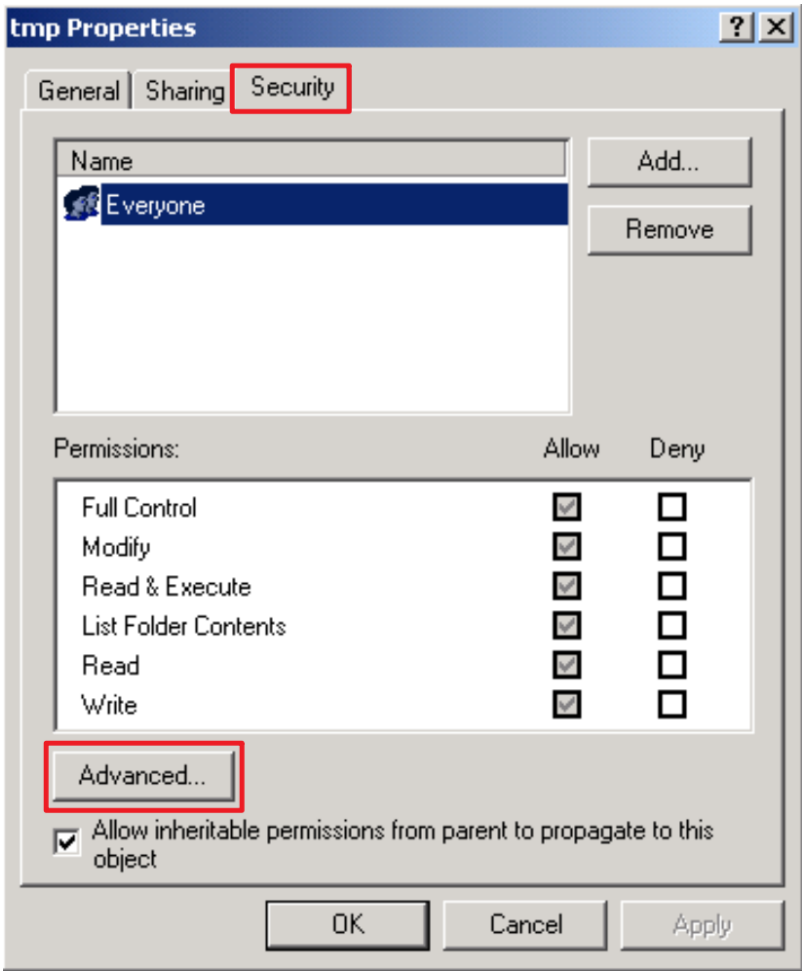


2.3 Folder Audit Configuration

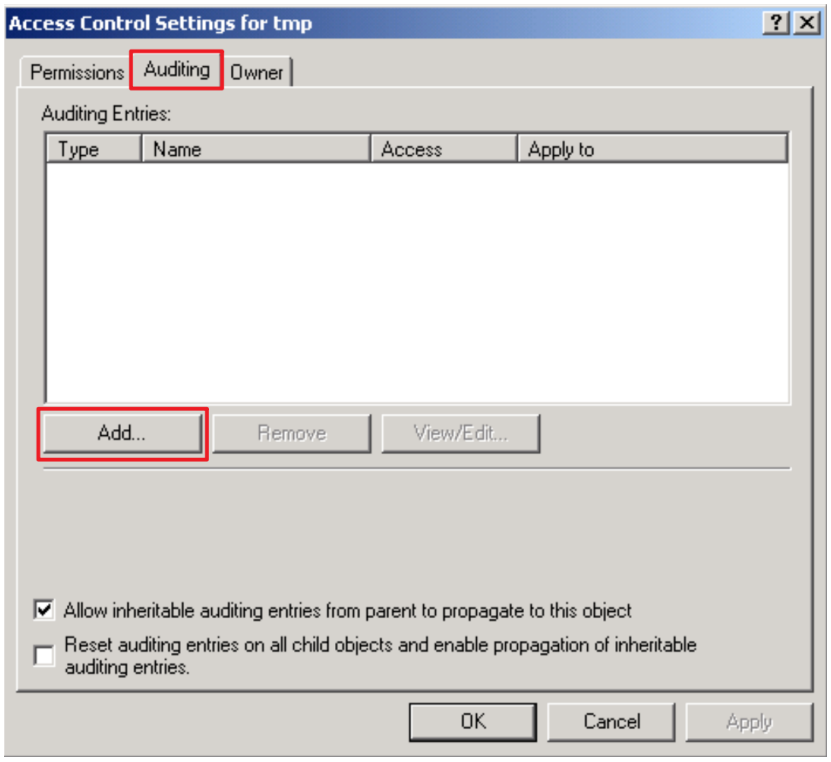
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



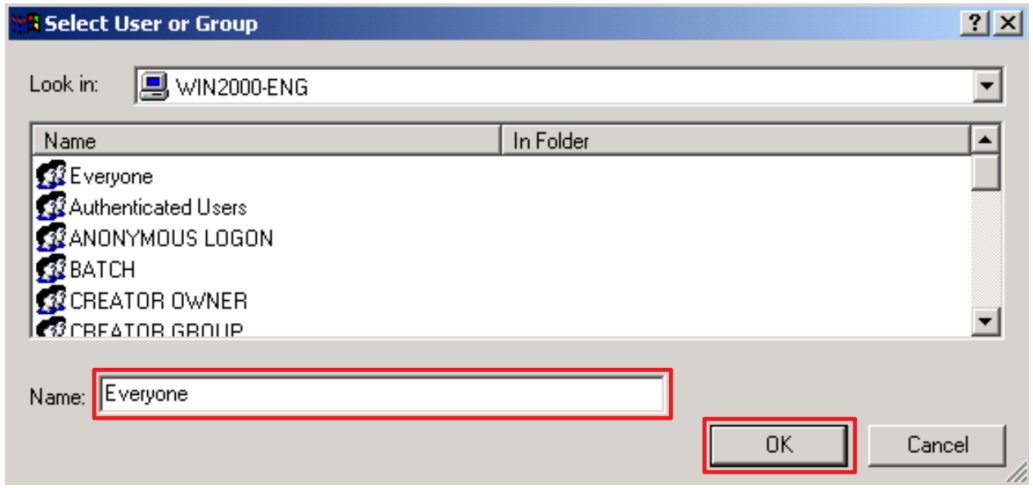
(2) Go to the “Security” tab → click “Advanced.”



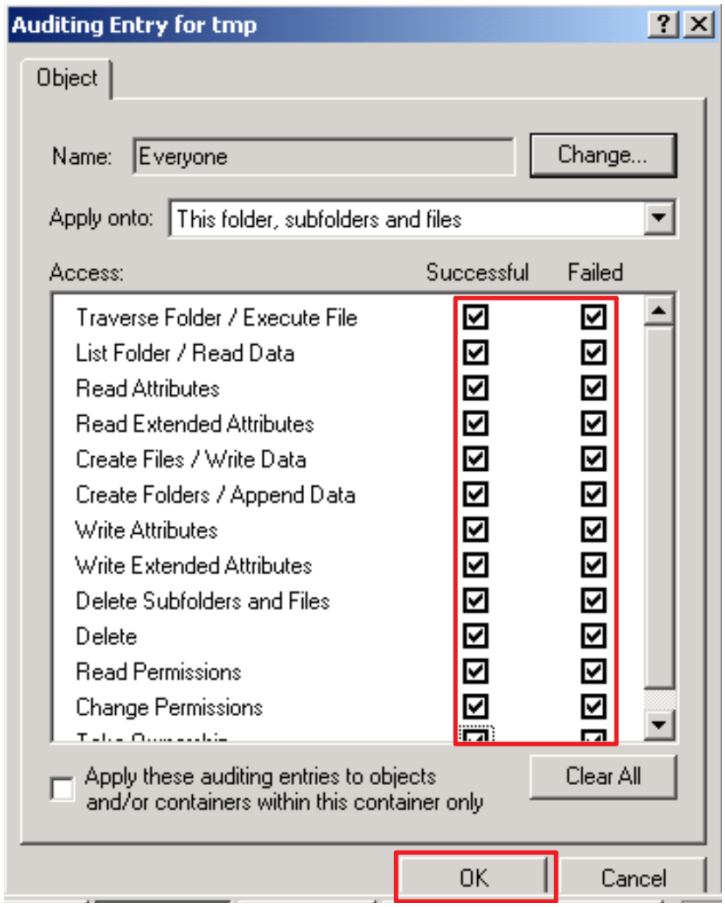
(3) Open the “Auditing” tab → click “Add.”



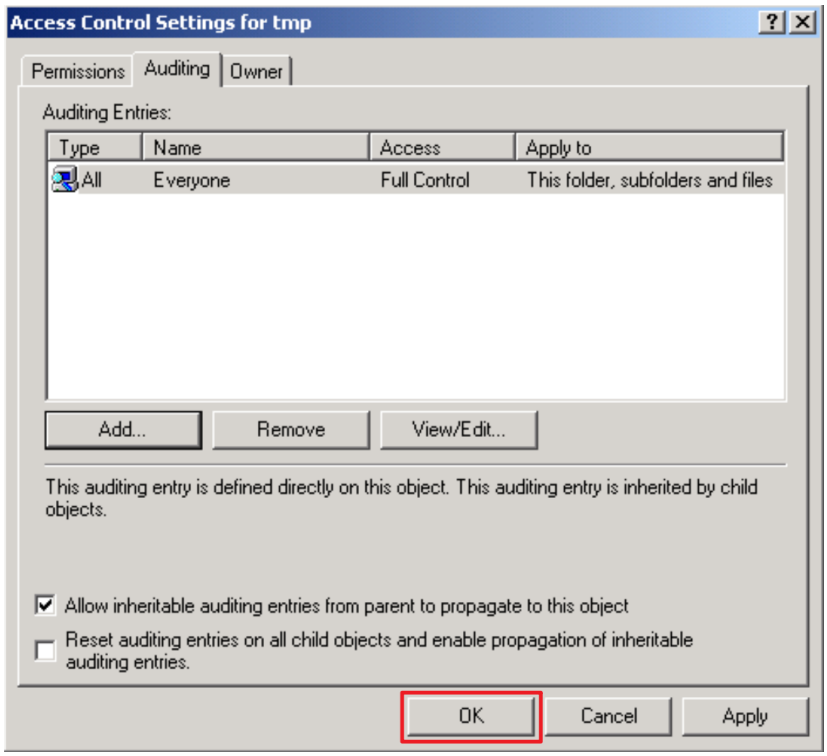
(4) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



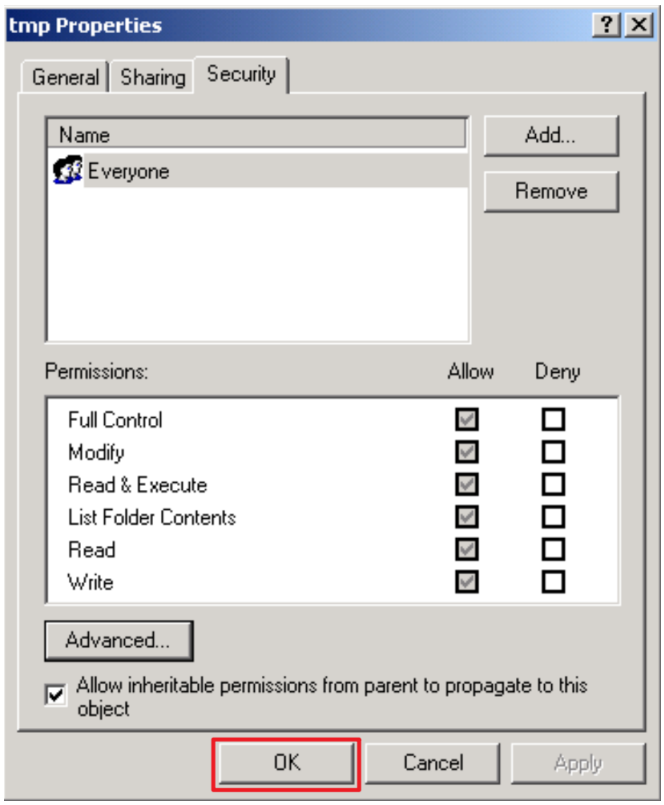
(5) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



(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.

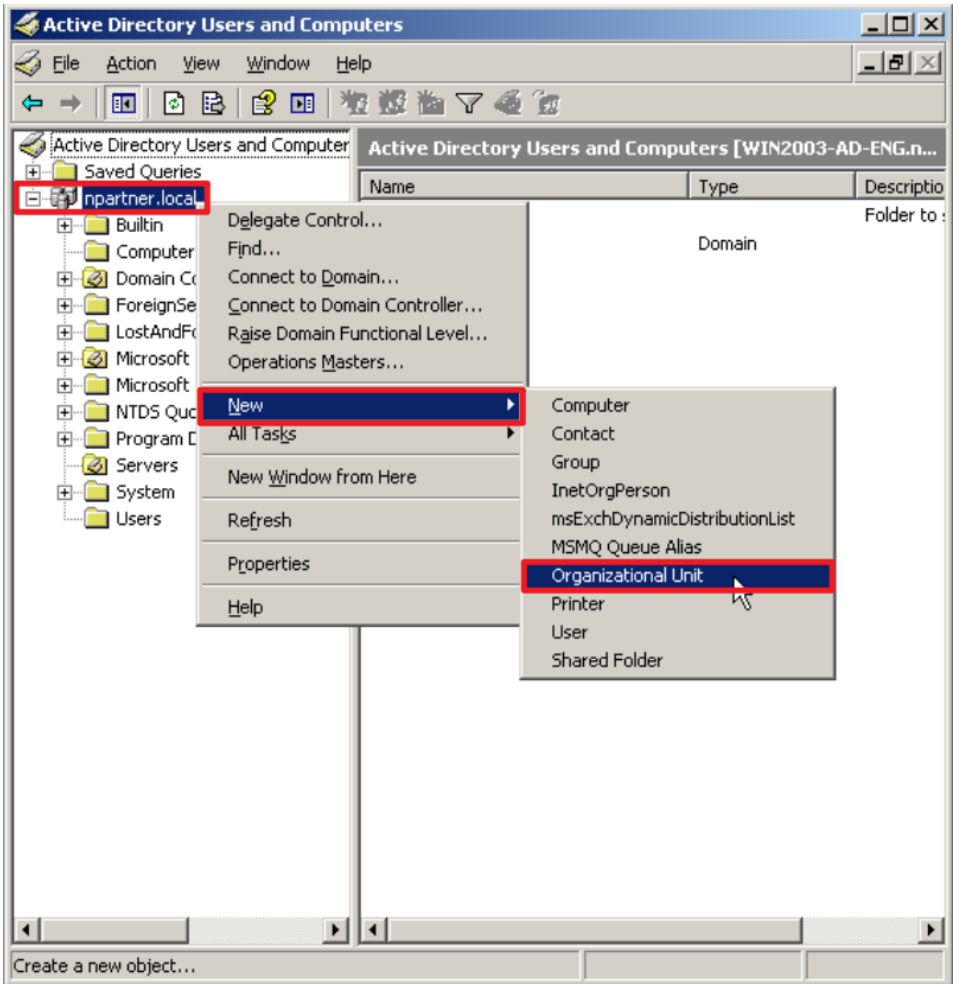
The following sections describe the configuration methods for Domain and Workgroup environments.

3.1.1 Organizational Unit (OU) Configuration

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

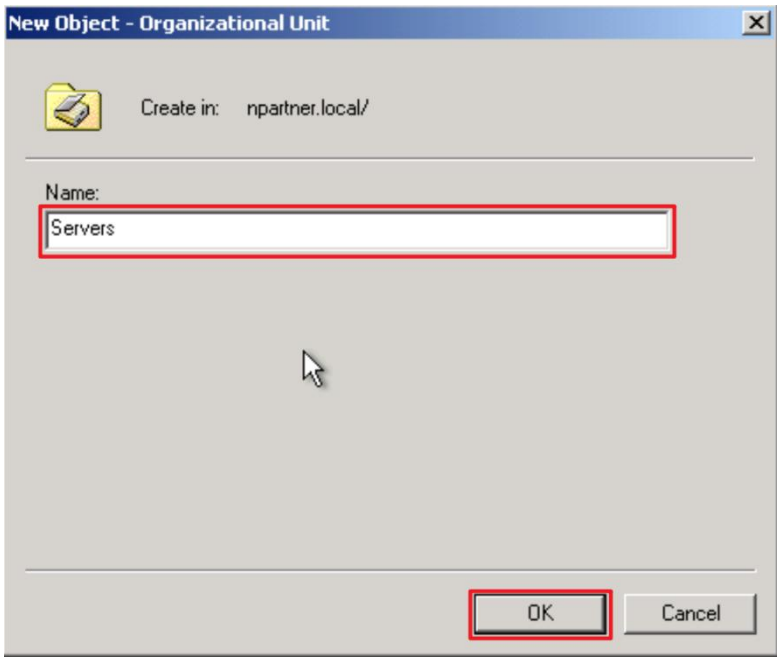
(2) Add an Organizational Unit

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



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

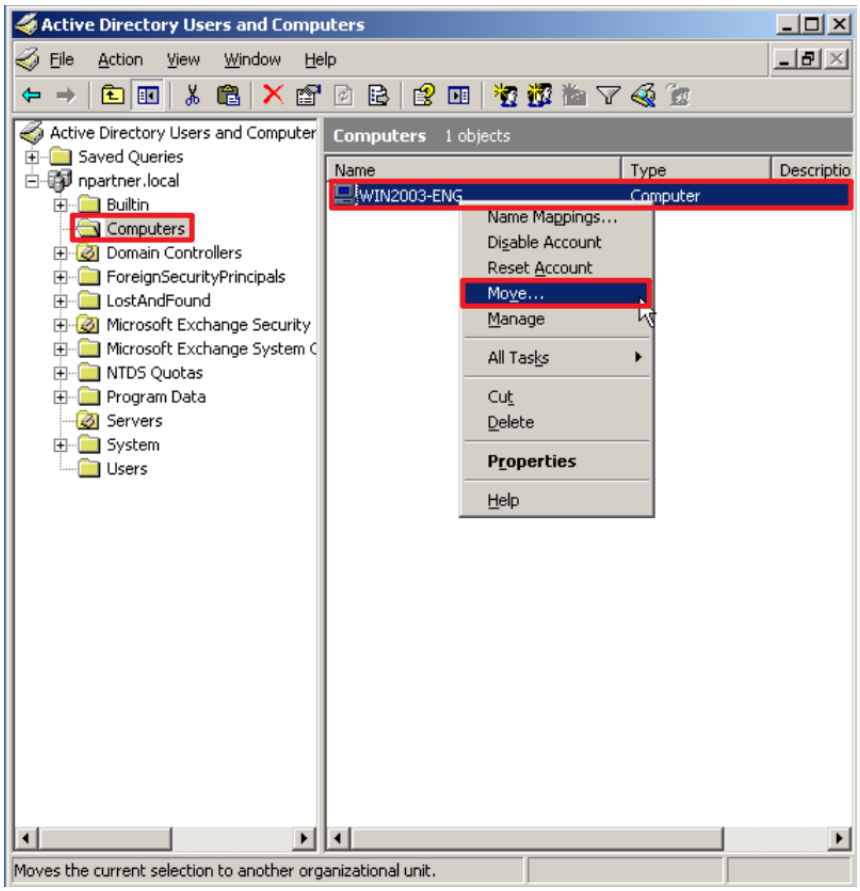
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

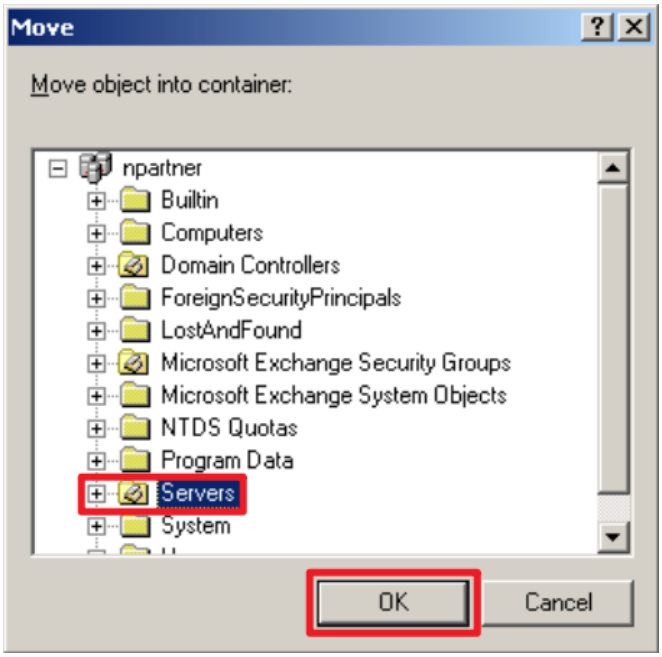
Select the “Computers” organizational unit (OU) → right-click on the “WIN2003-ENG” server.

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



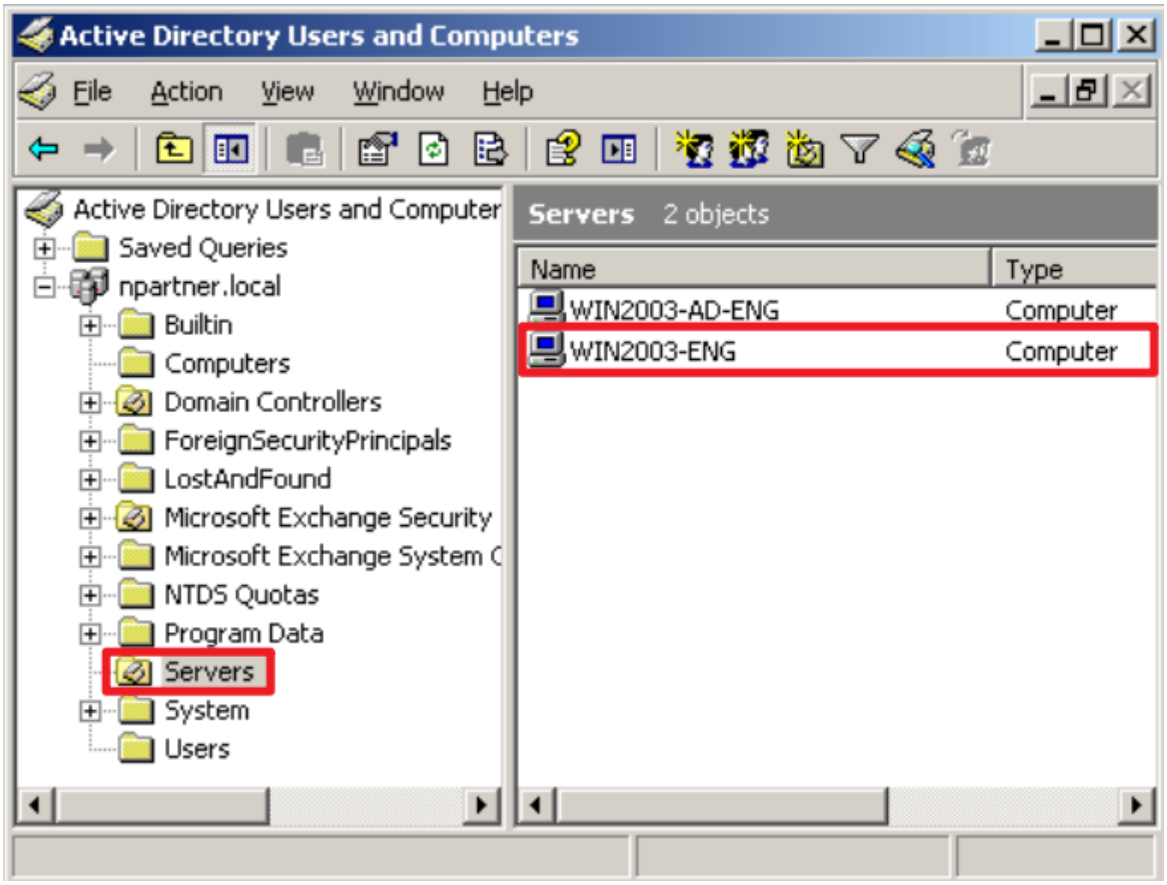
(5) Select your Organizational Unit:

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



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

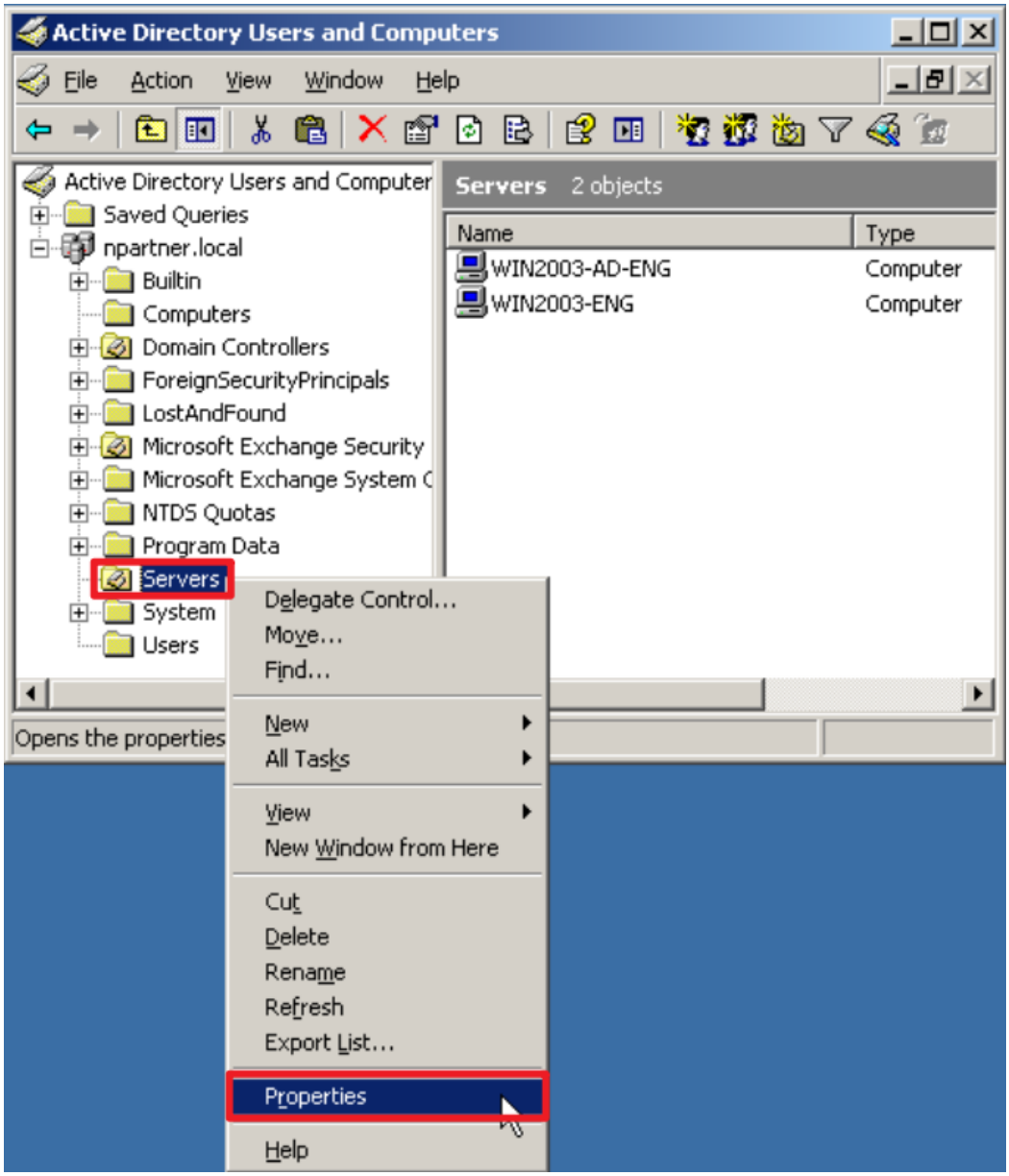
Expand your organizational unit folder (in this example, it is "Servers") and confirm that the "WIN2003-ENG" server has been moved.



3.1.2 Group Policy Settings

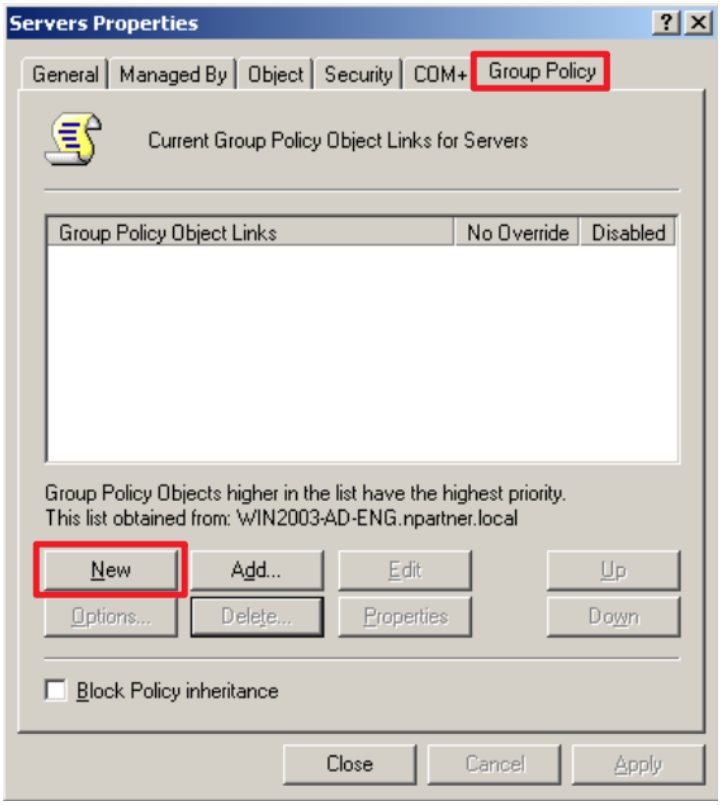
(1) Click “Active Directory Users and Computers.”

(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.”

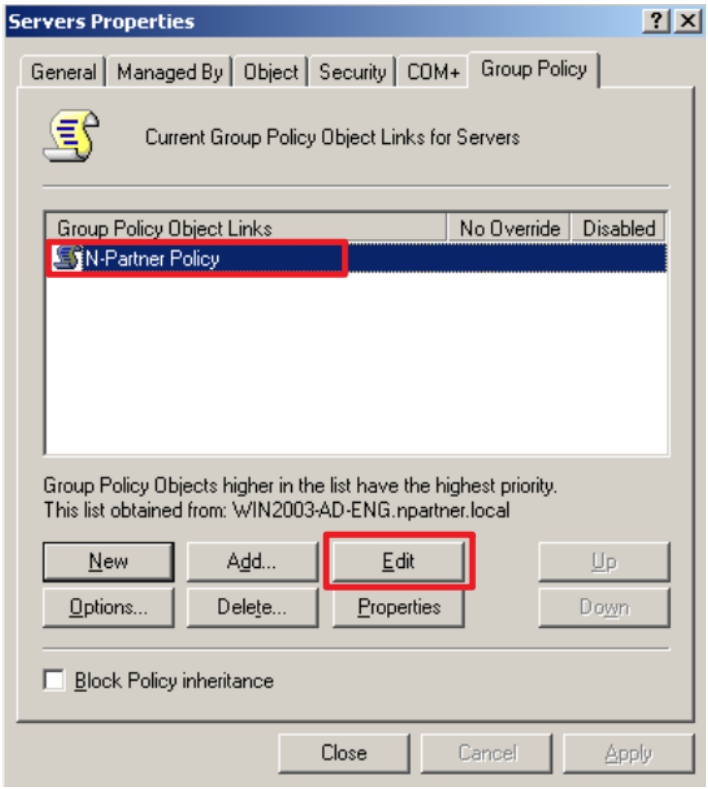


(4) Edit your Group Policy Object

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

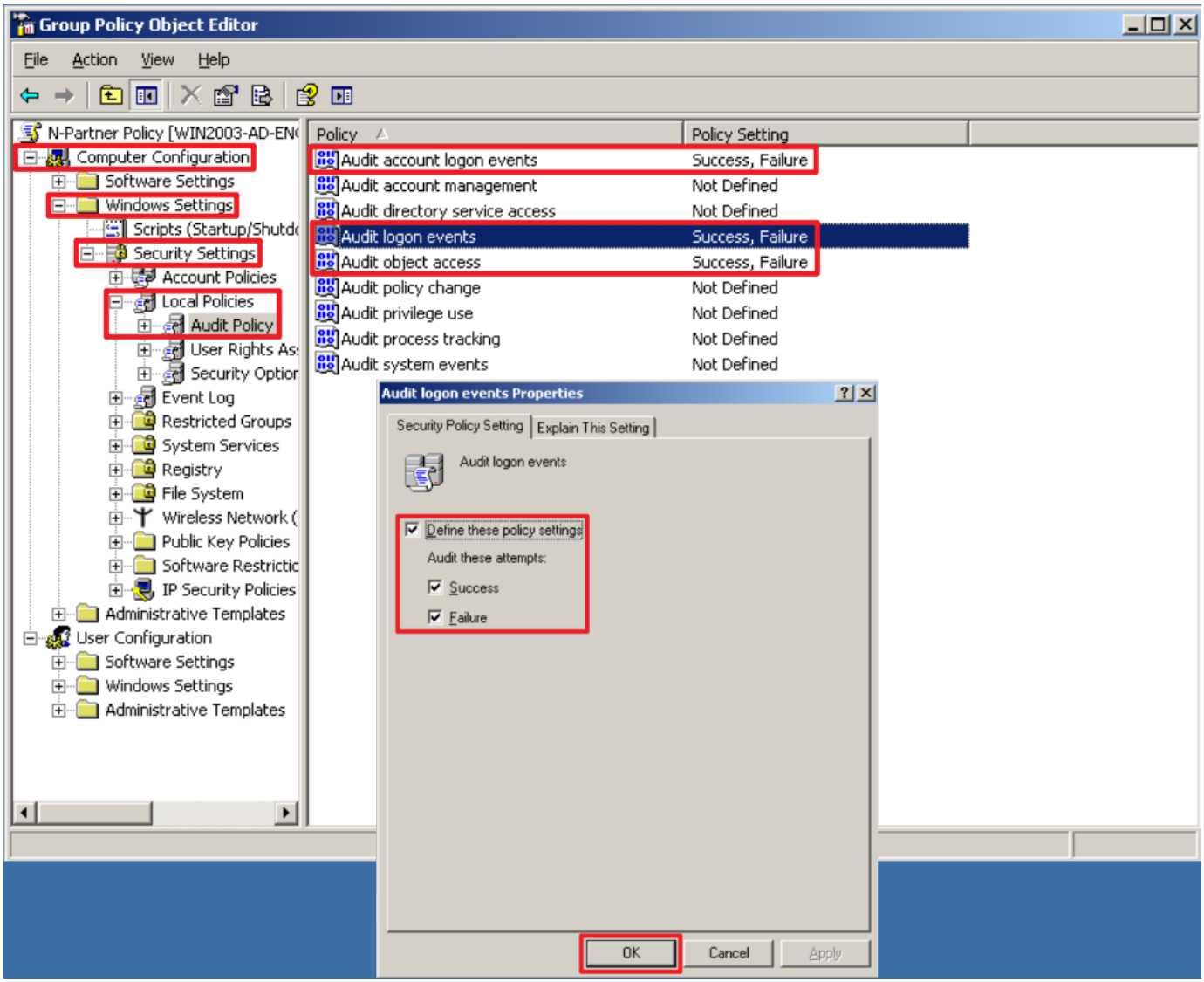
Note: Please create the GPO name according to the actual environment.

→ select “Edit.”



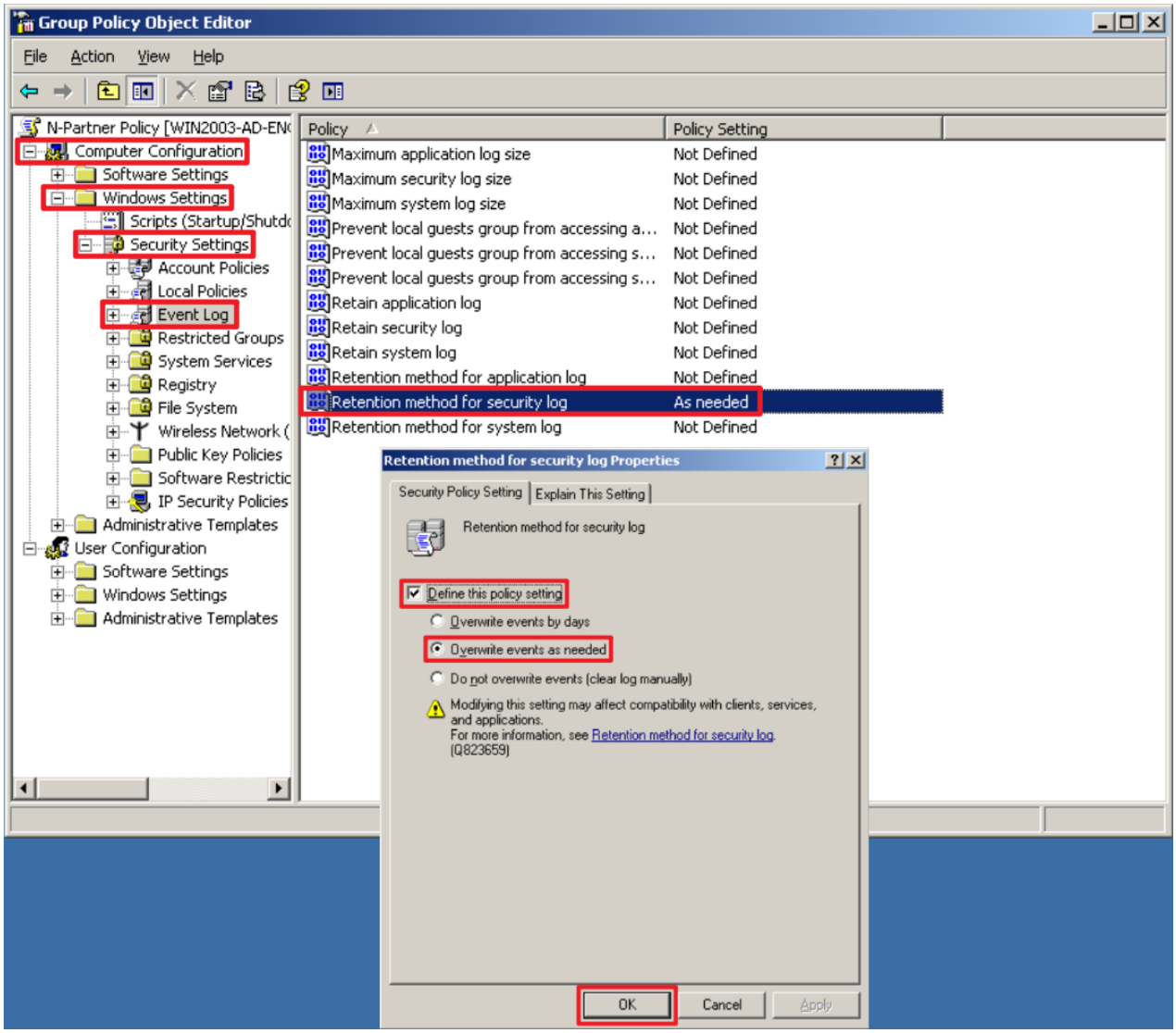
(5) Local Group Policies: Audit Policy

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

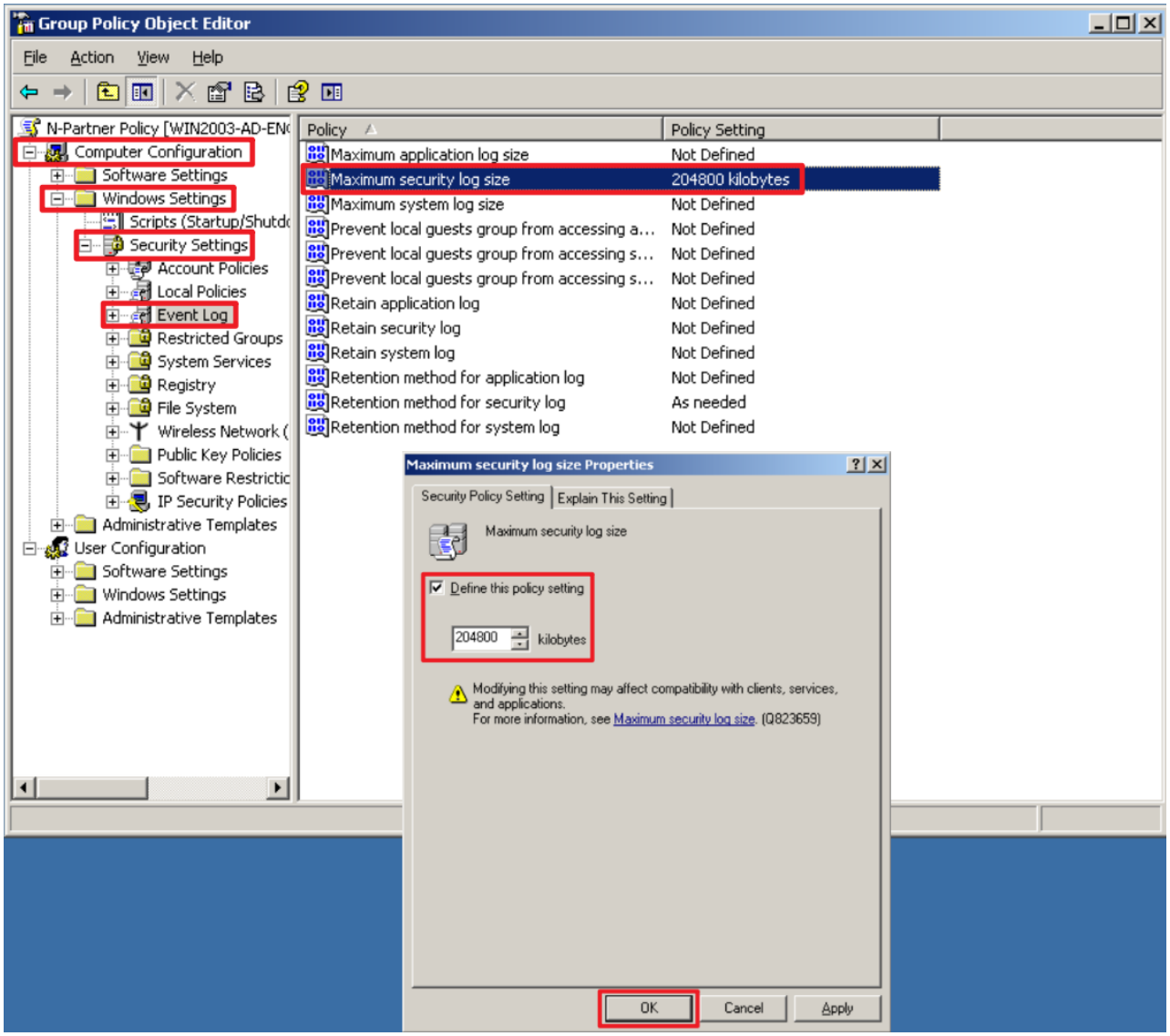
Expand “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → “Settings for Event Logs” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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

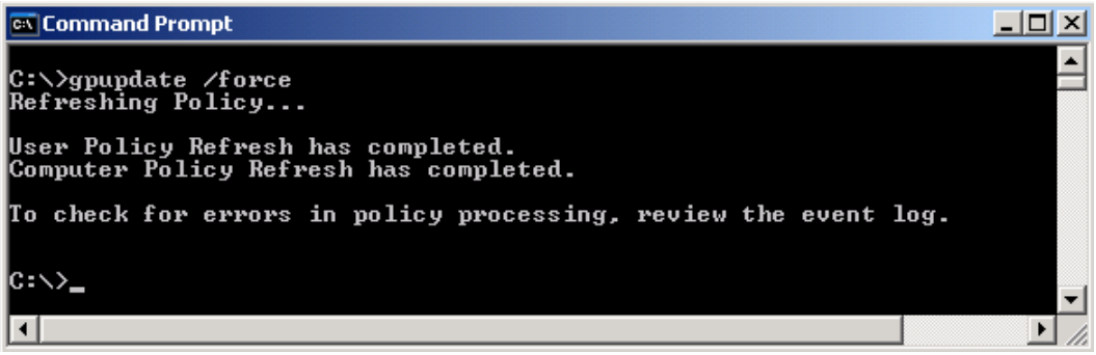
Note: Please adjust the number based on the actual environment. → click “OK.”



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

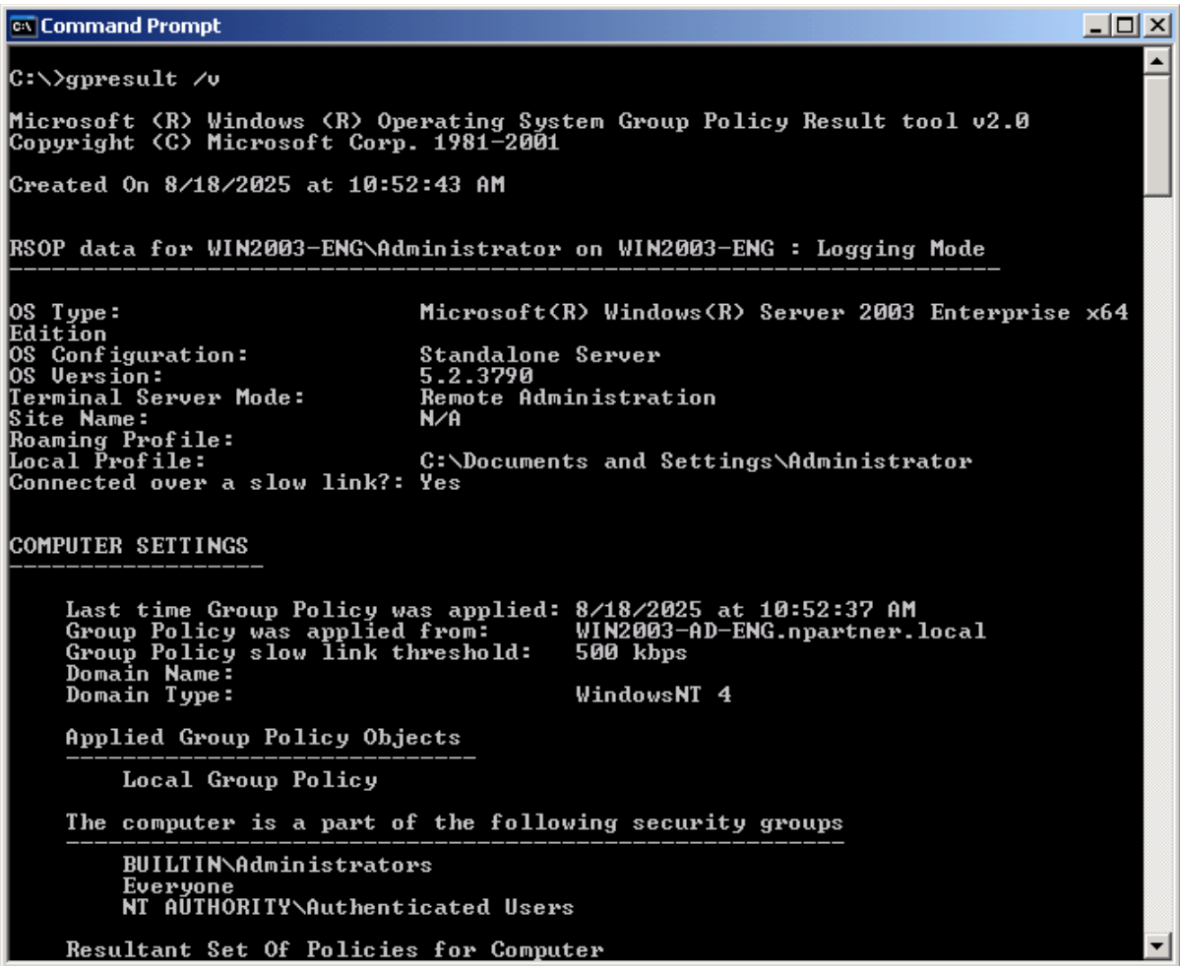
(9) Enter the command below to refresh group policy.

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



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

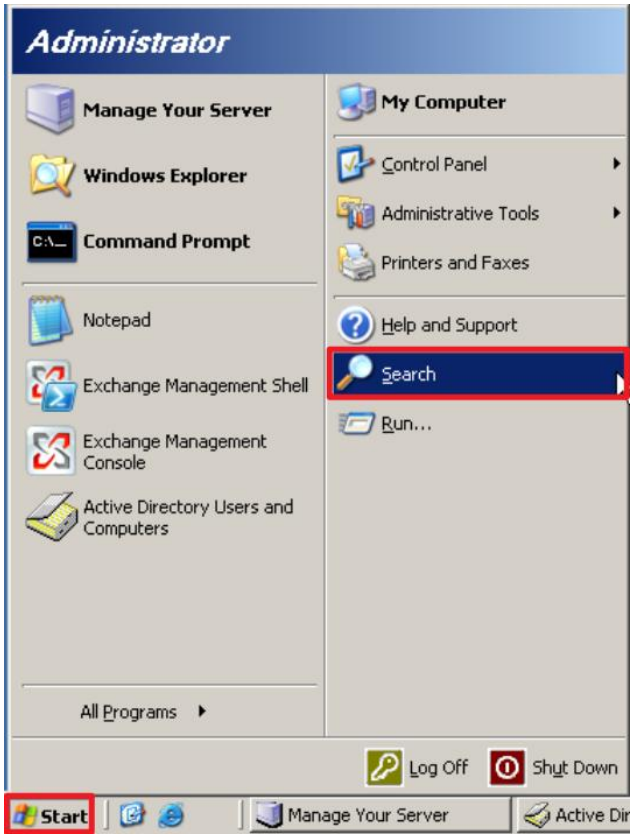
```
C:\> gpresult /v
```



3.2 Workgroup

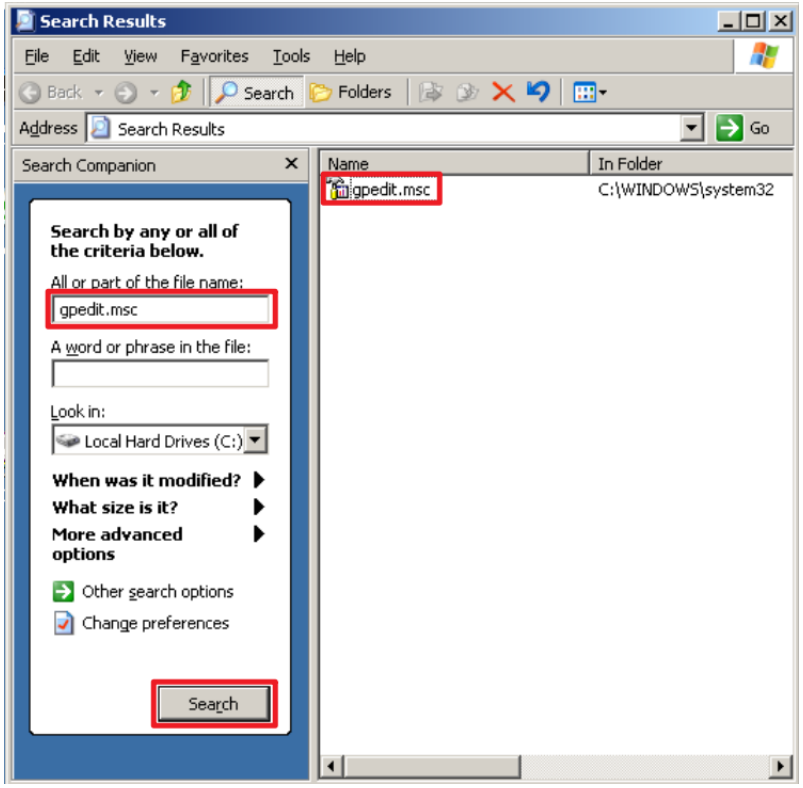
3.2.1 Audit Policy Configuration

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



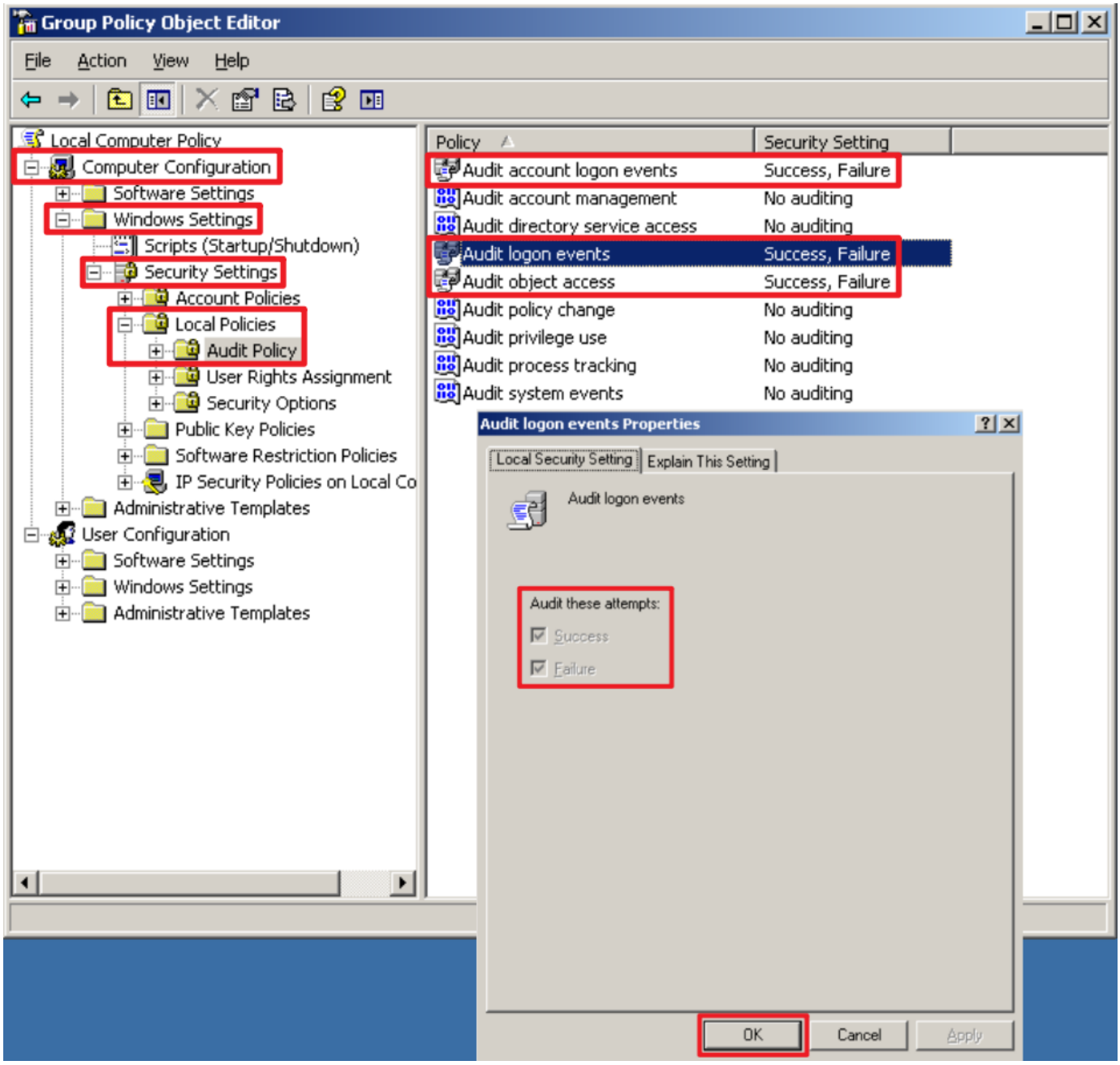
(2) Search for the Group Policy Object Editor

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



(3) Local Group Policies: Audit Policy

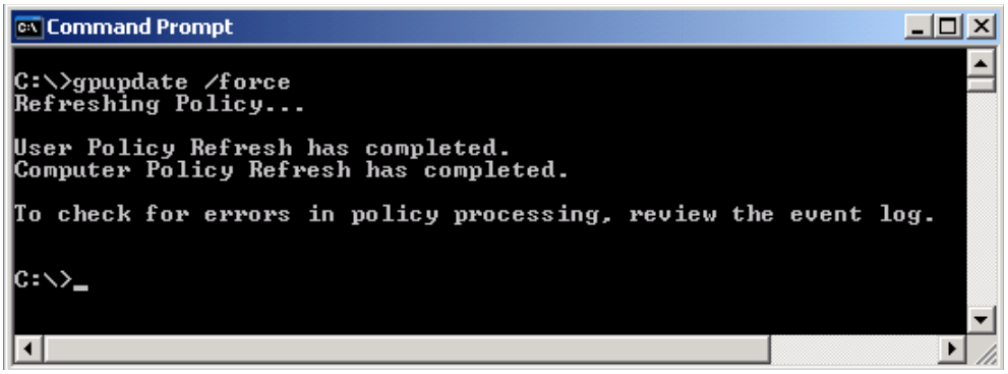
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



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

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

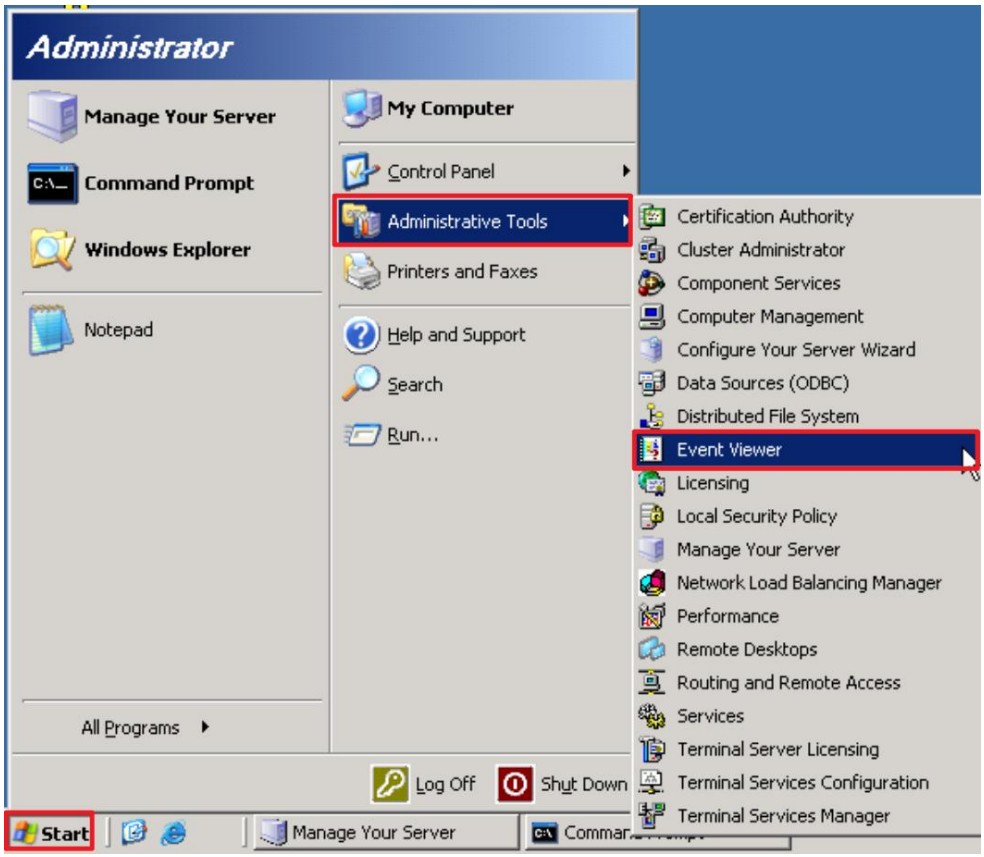
```
C:\> gpupdate /force
```



3.2.2 Event Log Settings

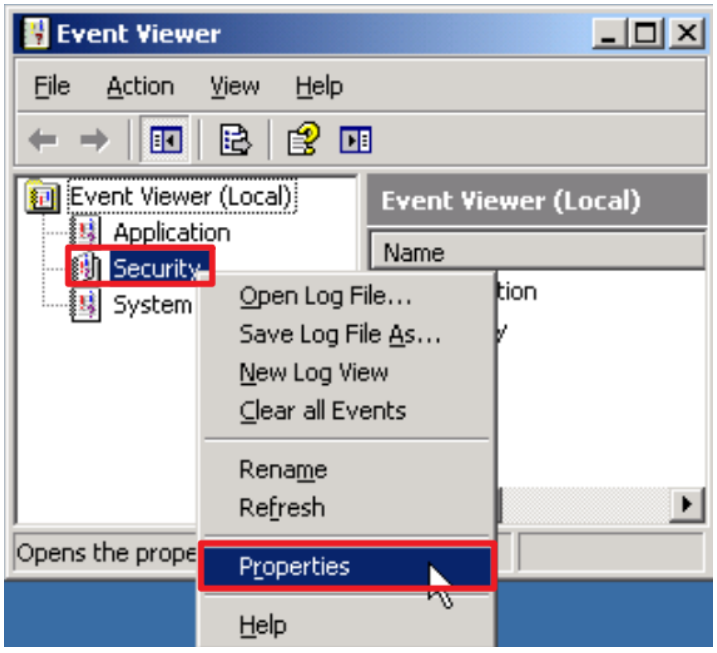
(1) Search for “Event Viewer”

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



(2) Edit Security Log

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

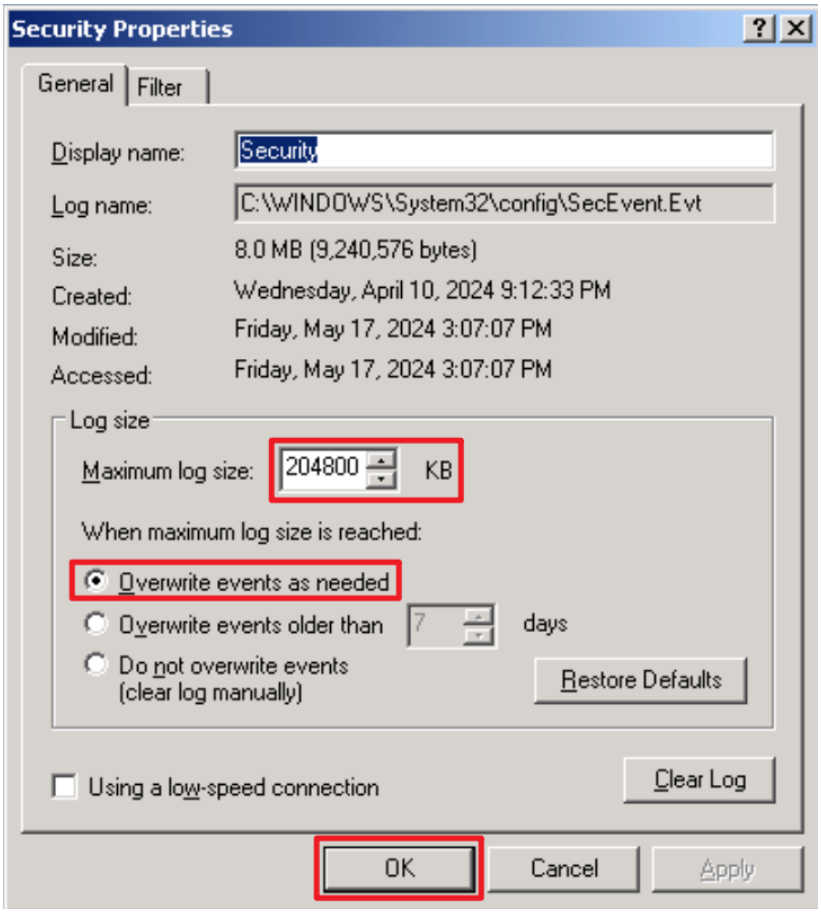


(3) Configure Security Log

Enter maximum log file size: 204800 KB

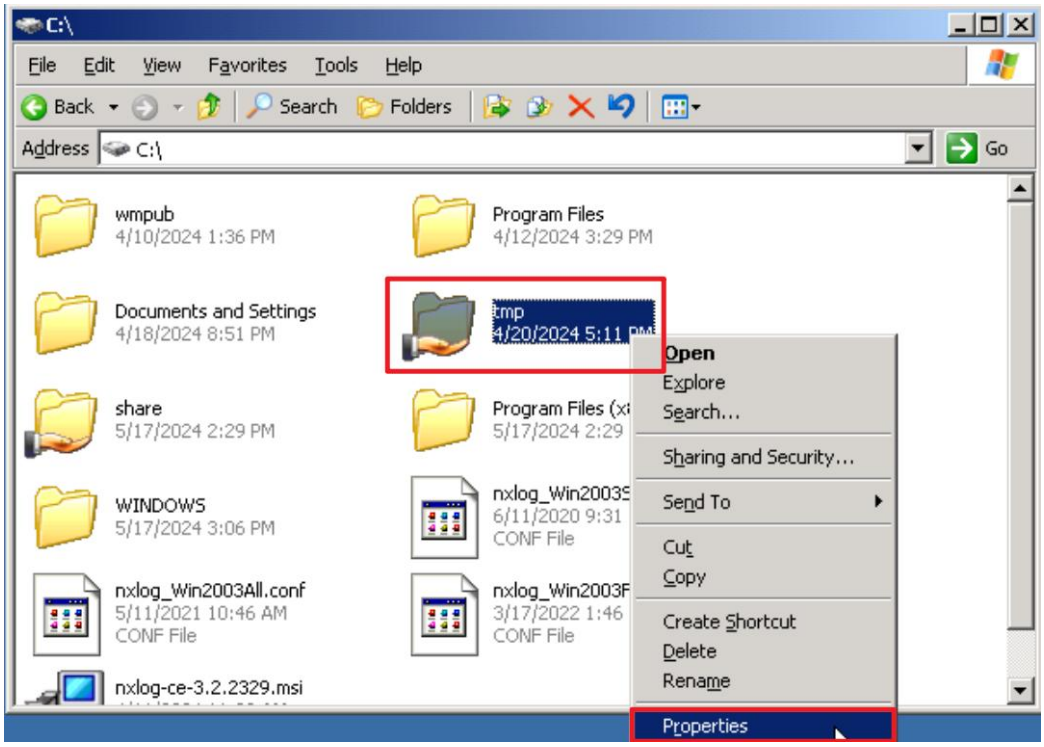
Note: Please adjust the number according to the actual environment.

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

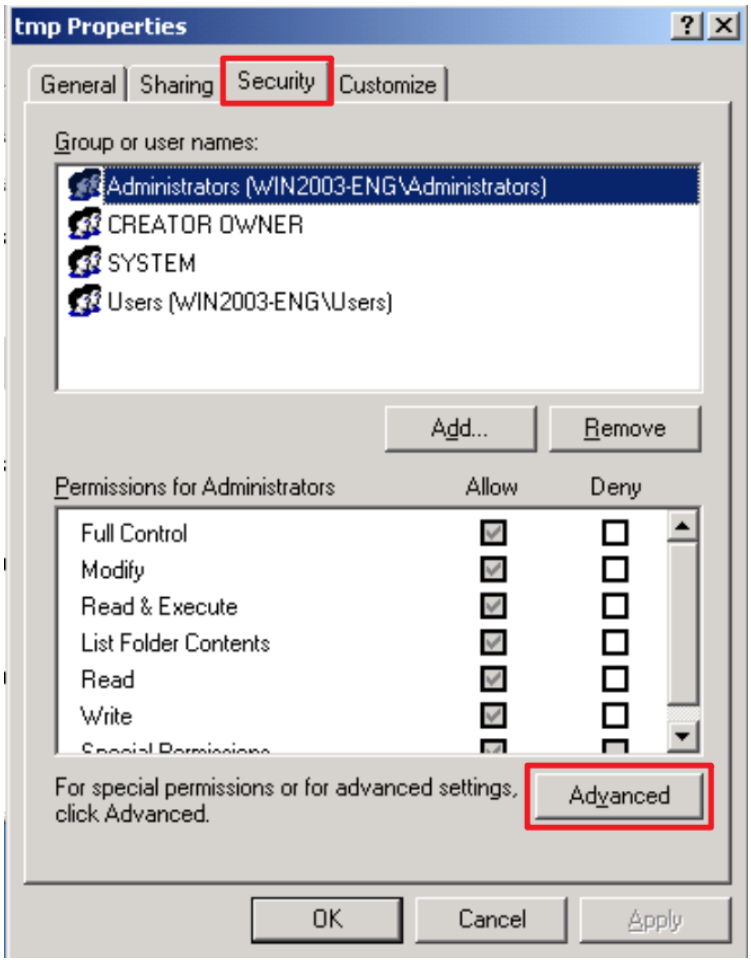


3.3 Folder Audit Configuration

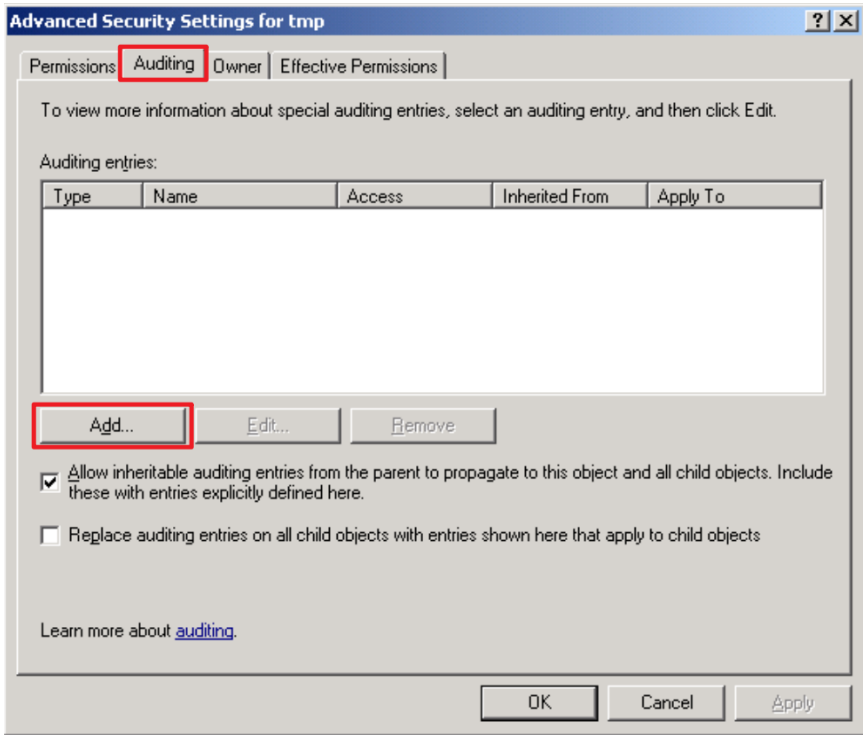
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



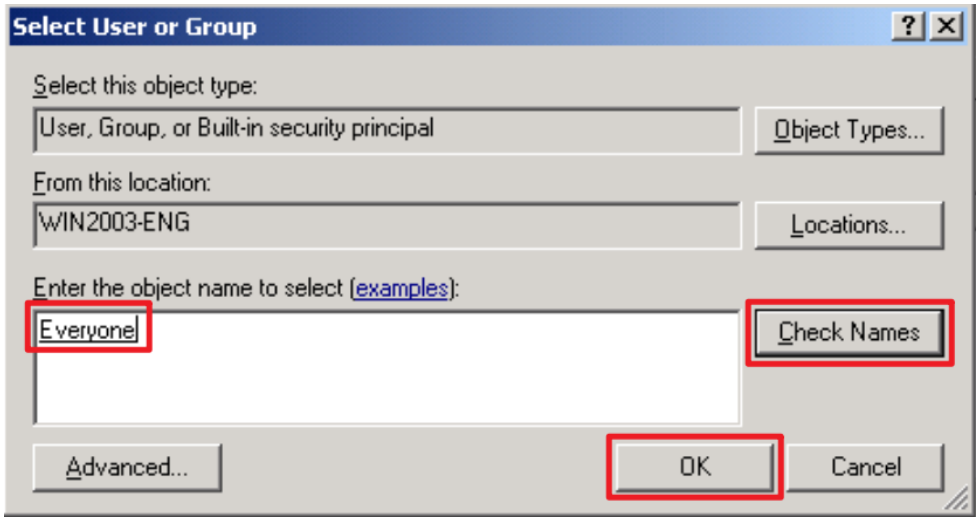
(2) Go to the “Security” tab → click “Advanced.”



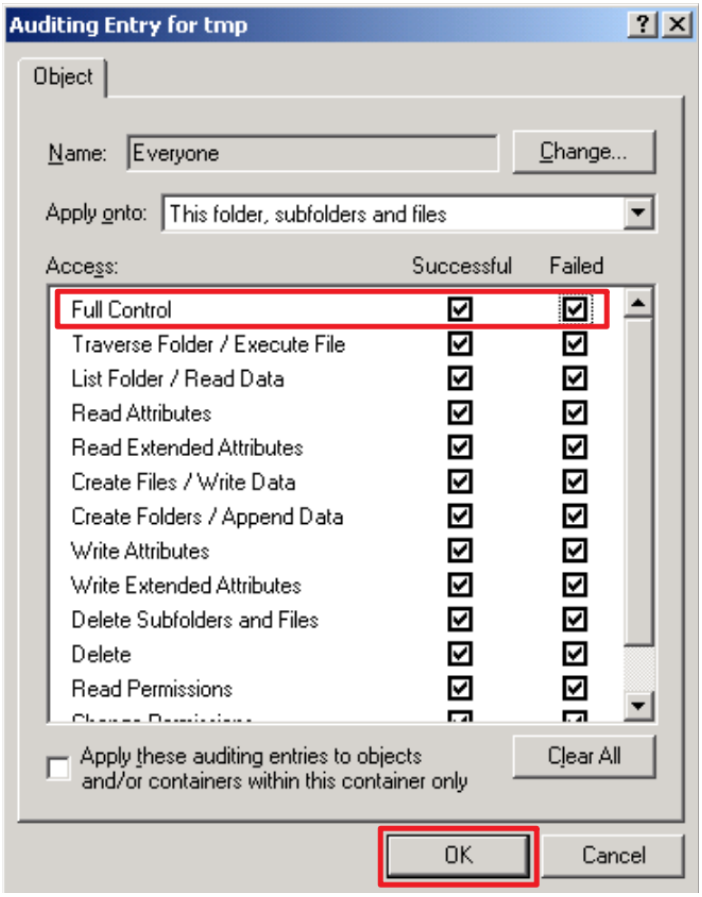
(3) Open the “Auditing” tab → click “Add.”



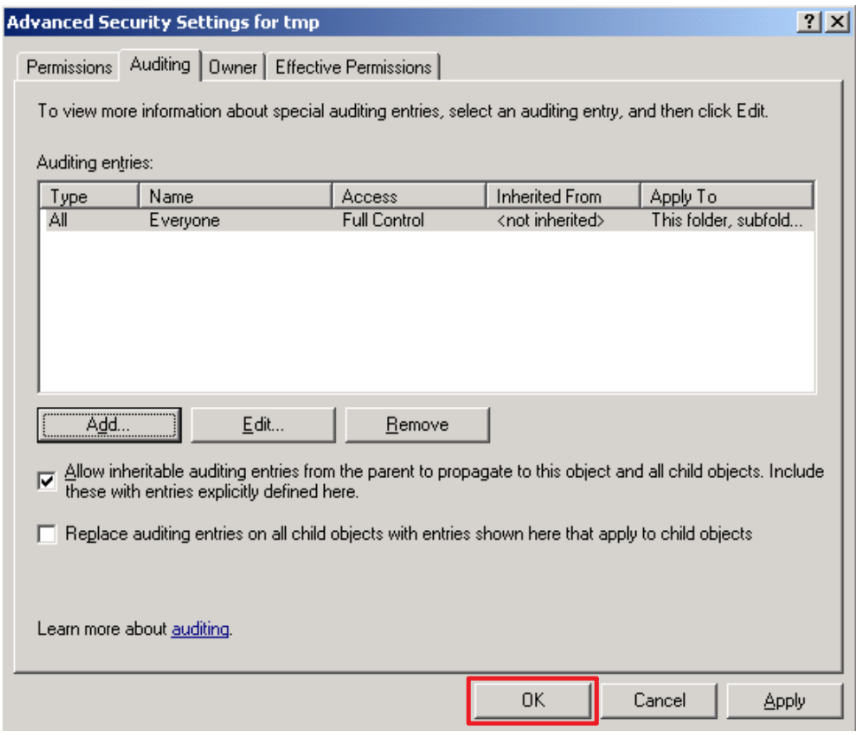
(4) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



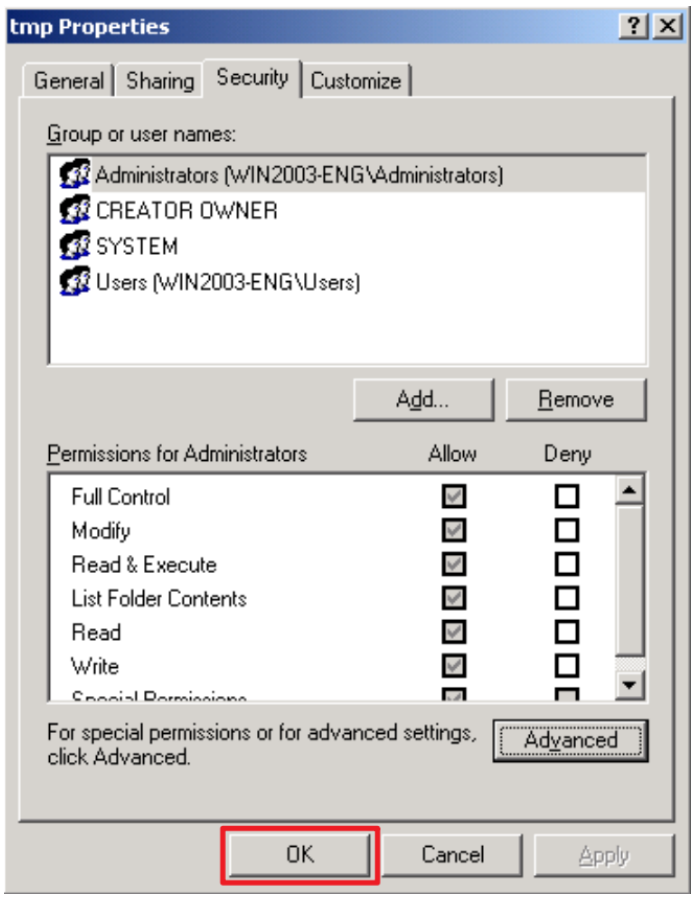
(5) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



(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

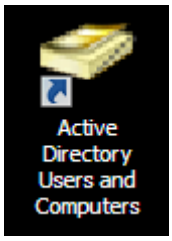
Windows Audit Policy Configuration:

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.

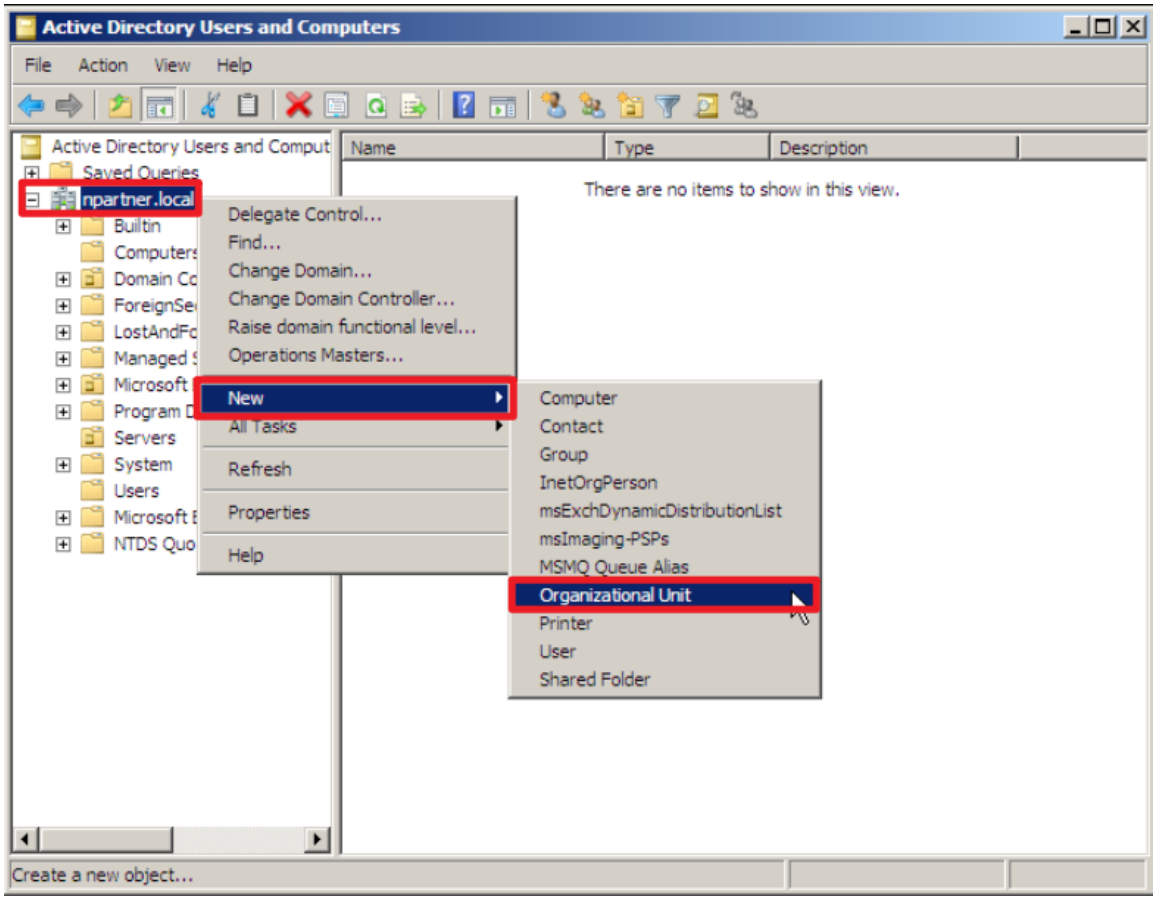
4.1.1 Organizational Unit (OU) Configuration

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



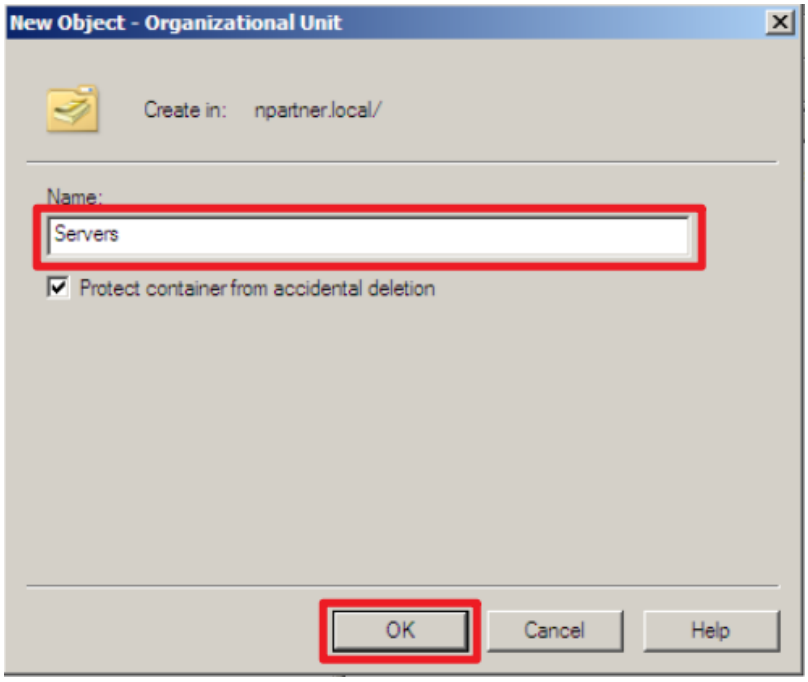
(2) Add an Organizational Unit

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”)

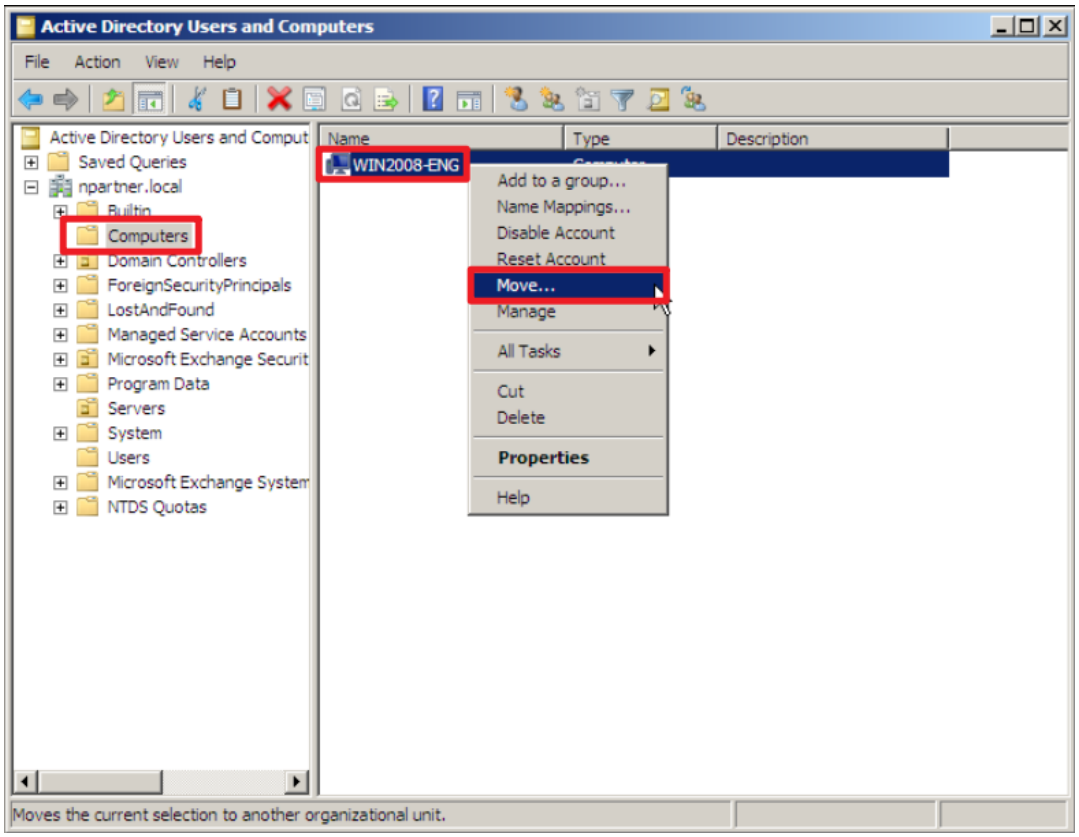
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

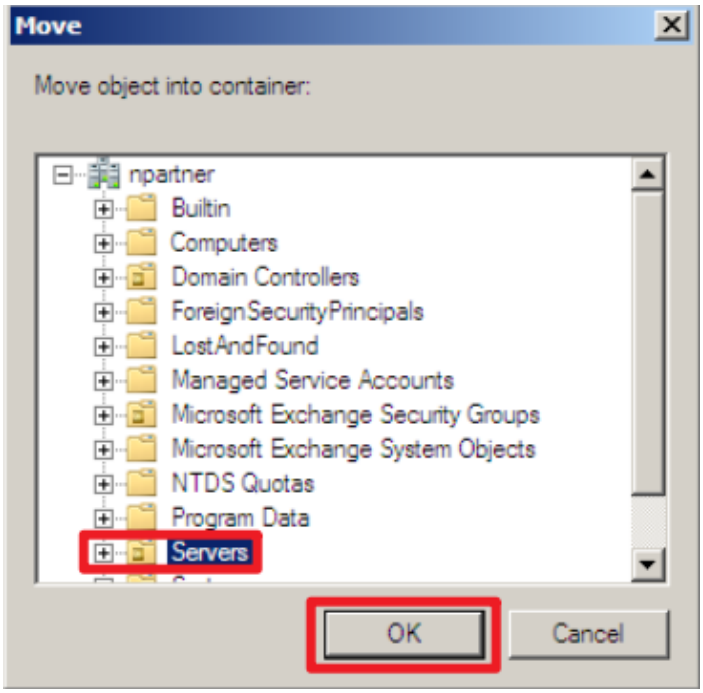
Select the “Computers” organizational unit (OU) → right-click on the “WIN2008-ENG” server.

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



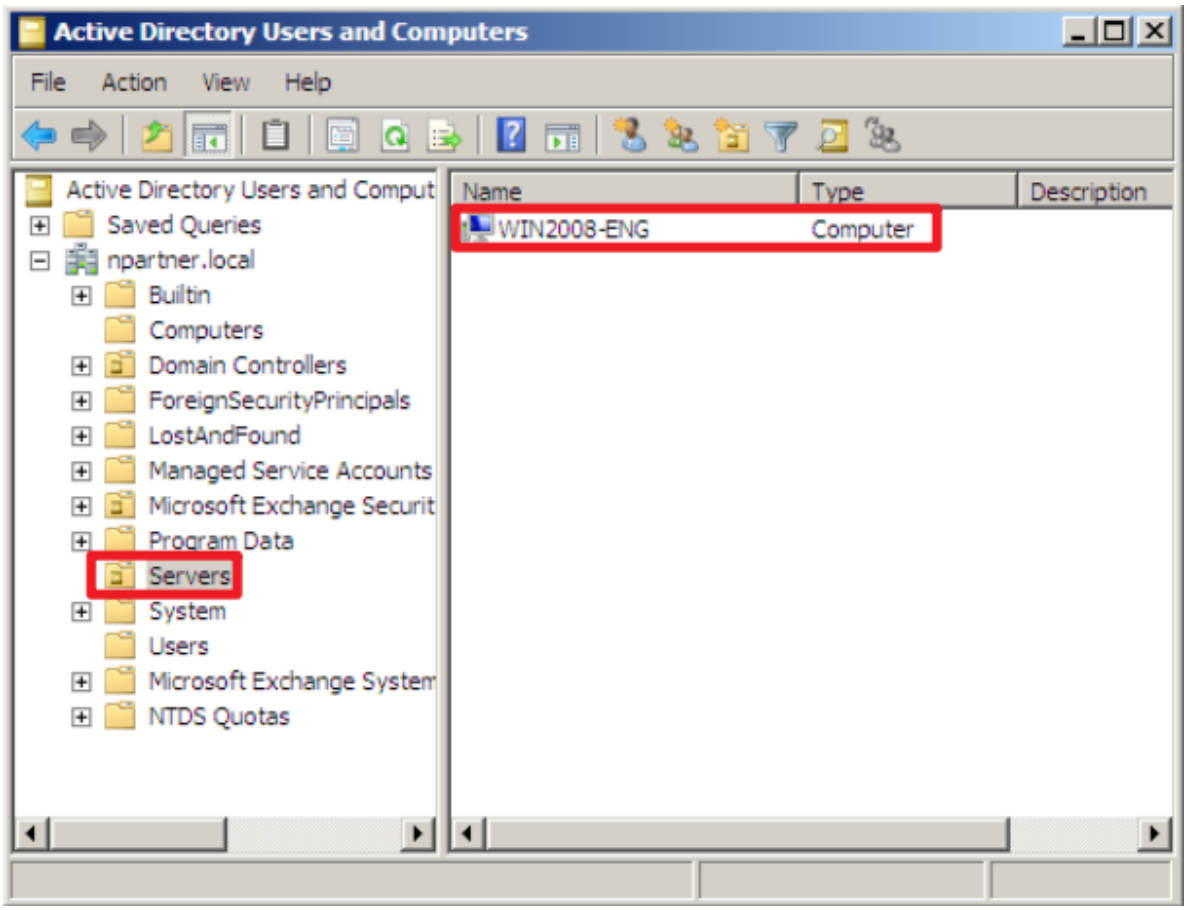
(5) Select your Organizational Unit:

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



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

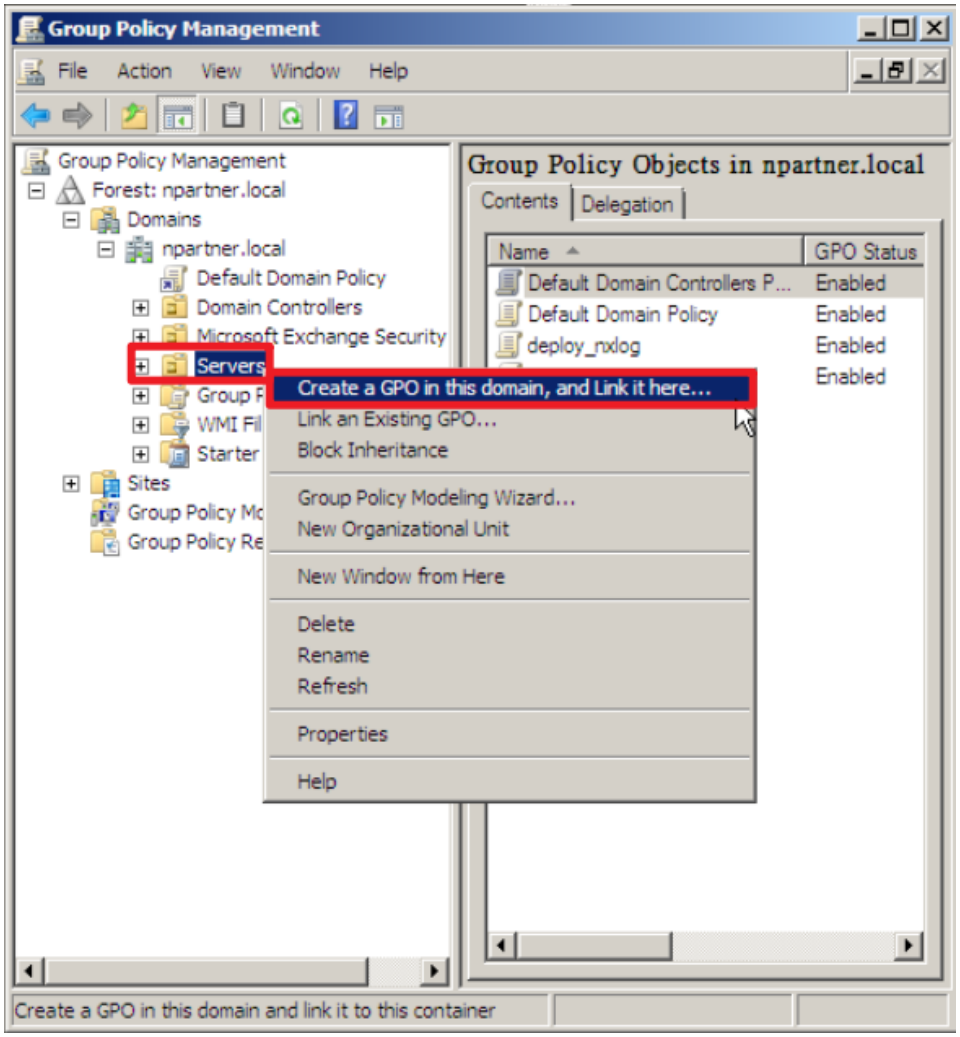
Expand your organizational unit folder (in this example, it is “Servers”) and confirm that the “WIN2008-ENG” server has been moved.



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…”

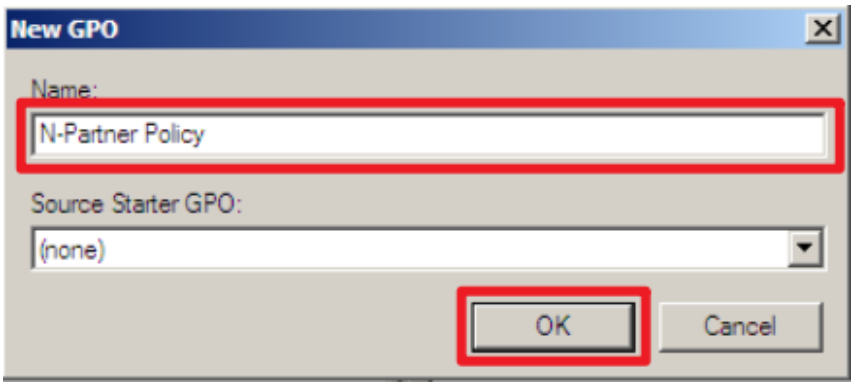


(3) Enter the Group Policy Object (GPO) name

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

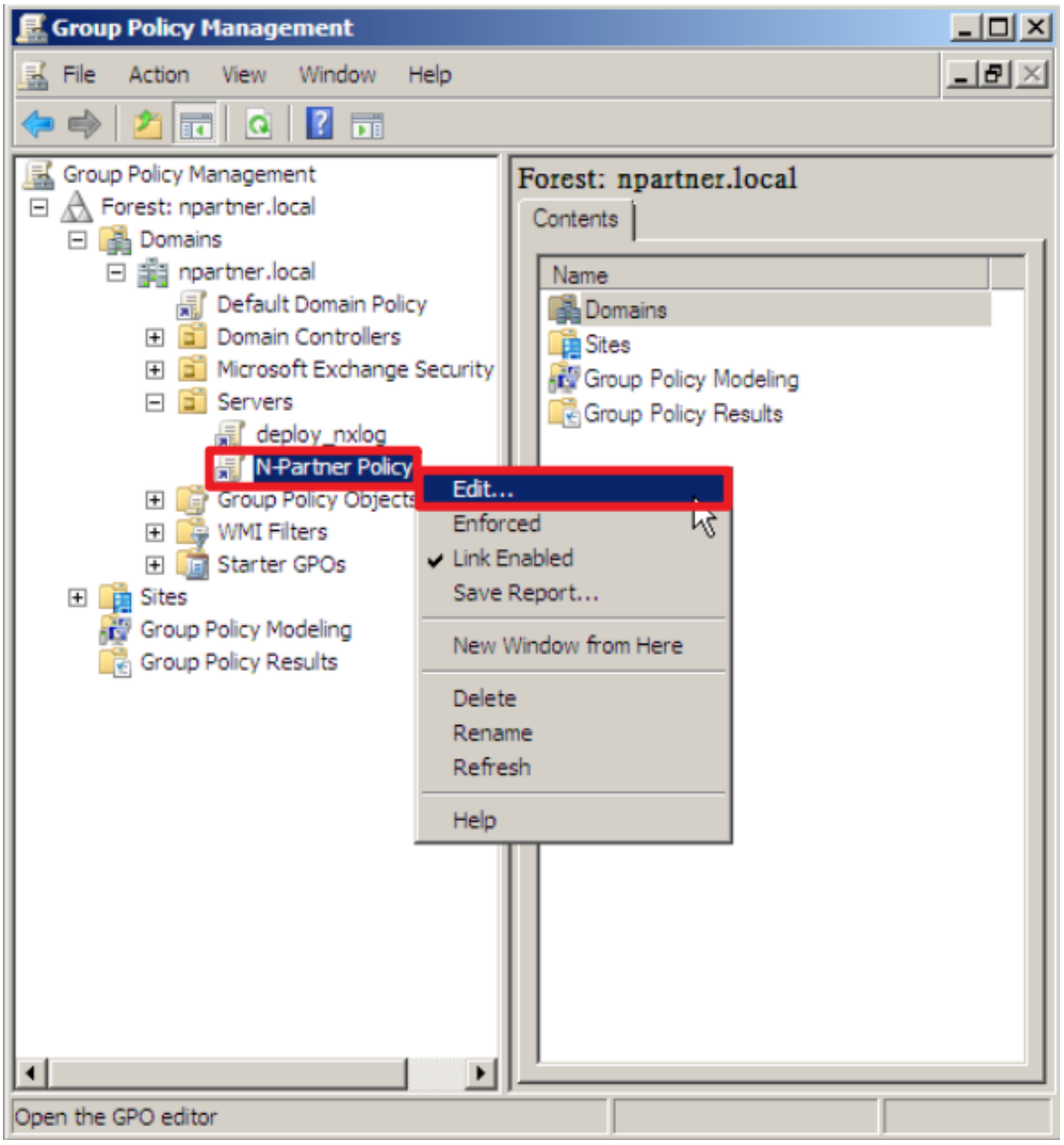
Note: Please create the GPO name according to the actual environment.

→ select “OK.”



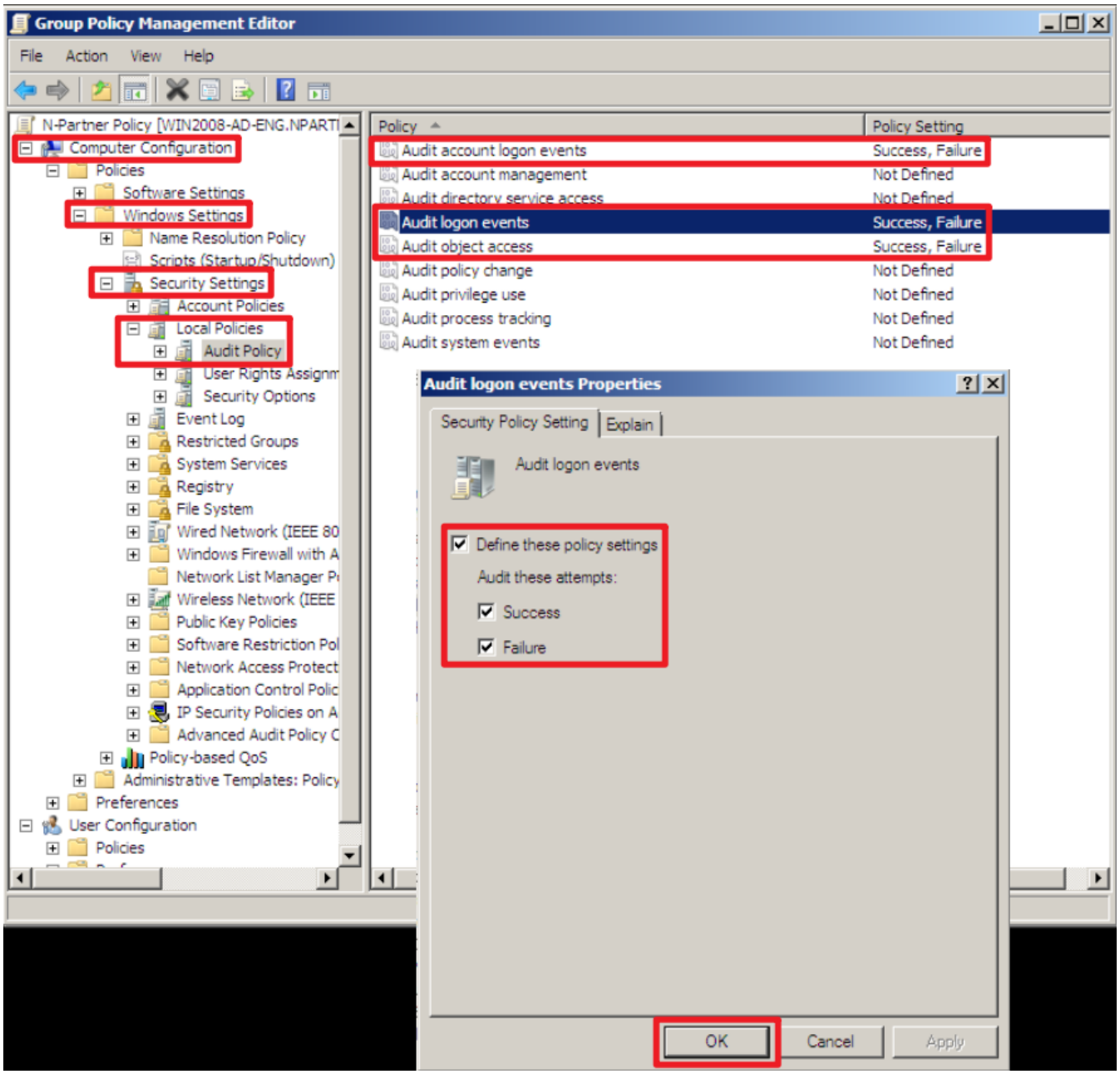
(4) Edit your Group Policy Object

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



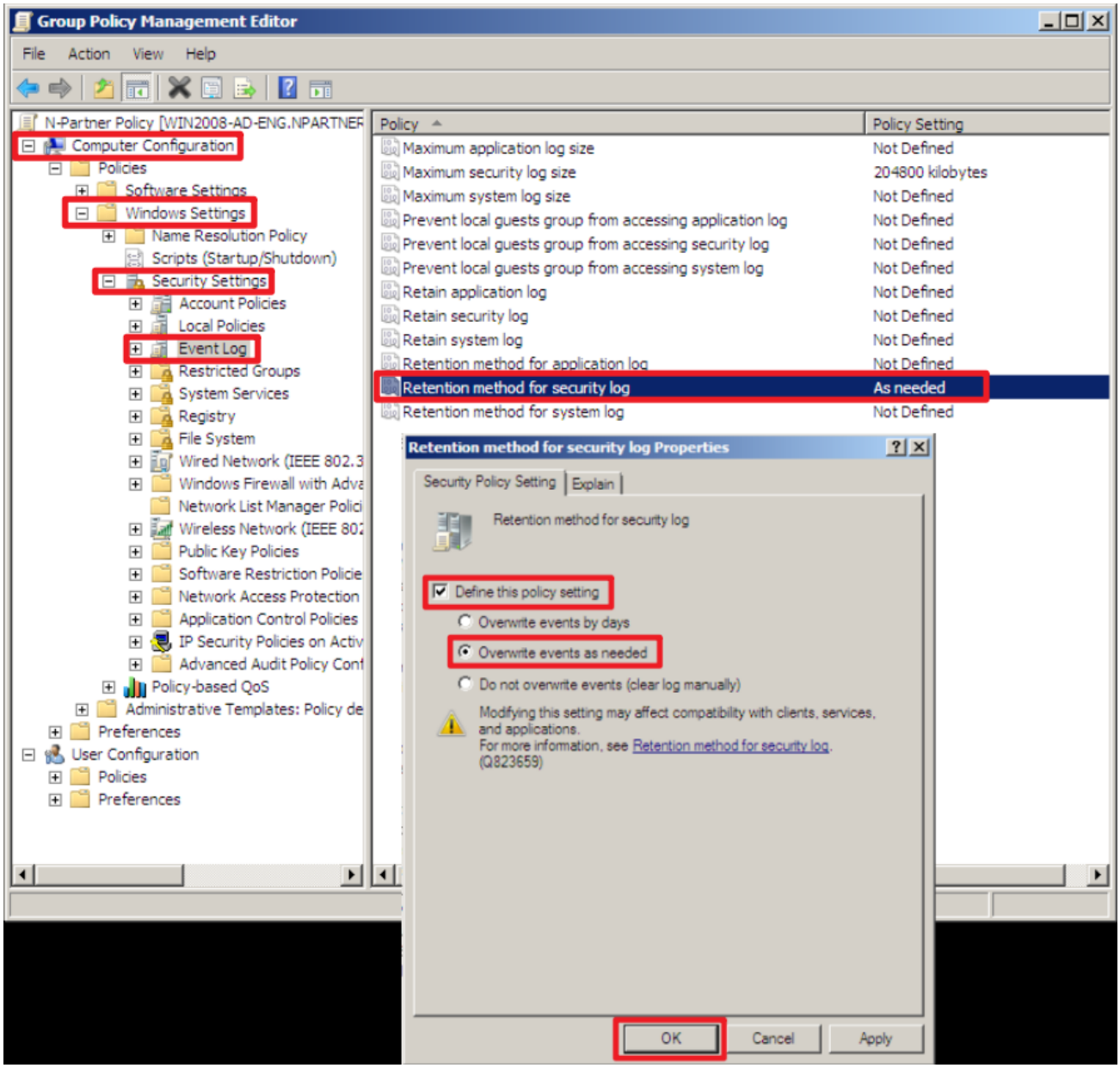
(5) Local Group Policies: Audit Policy

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.”



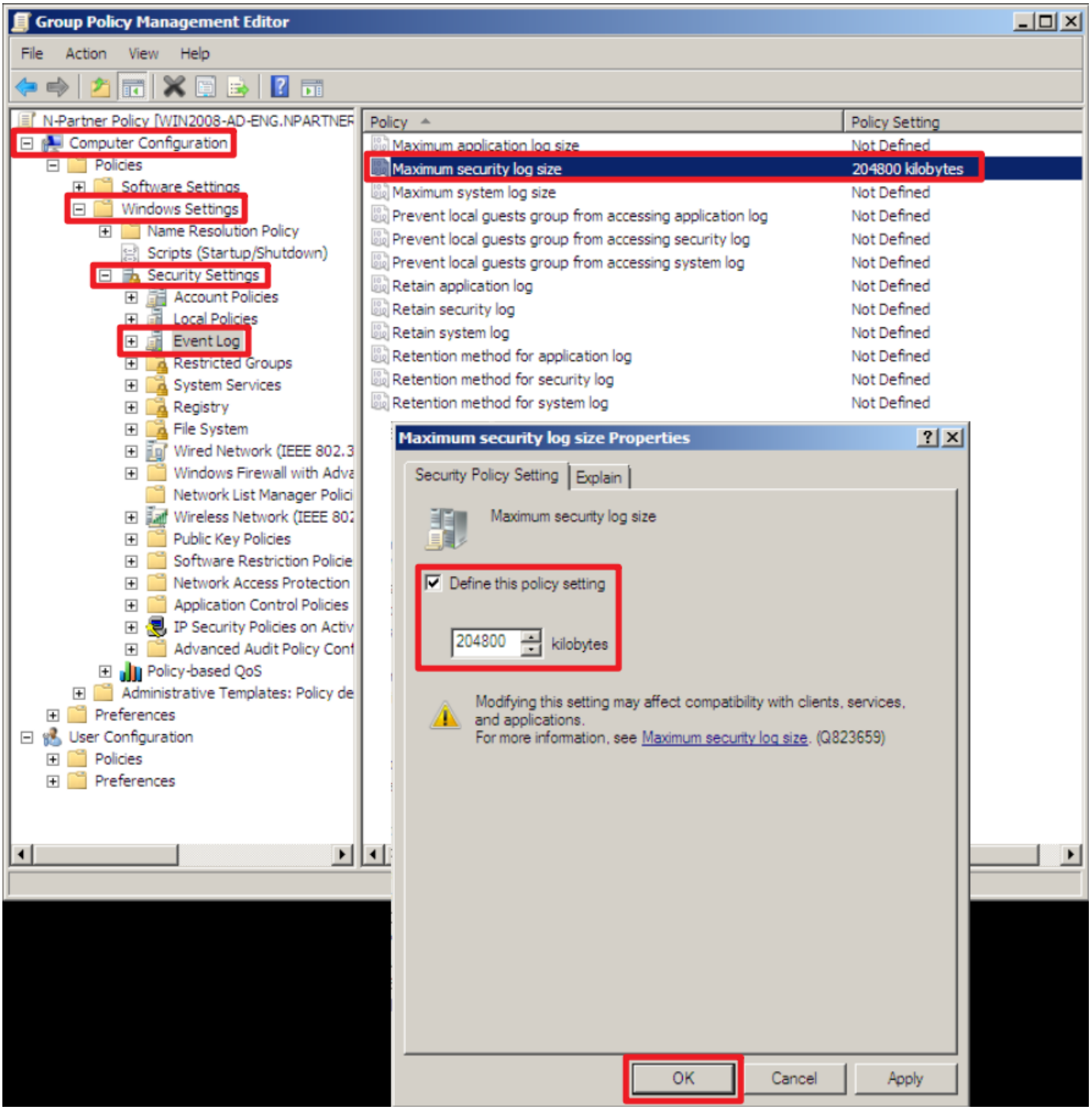
(6) Event Log: Security Log Retention Method

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

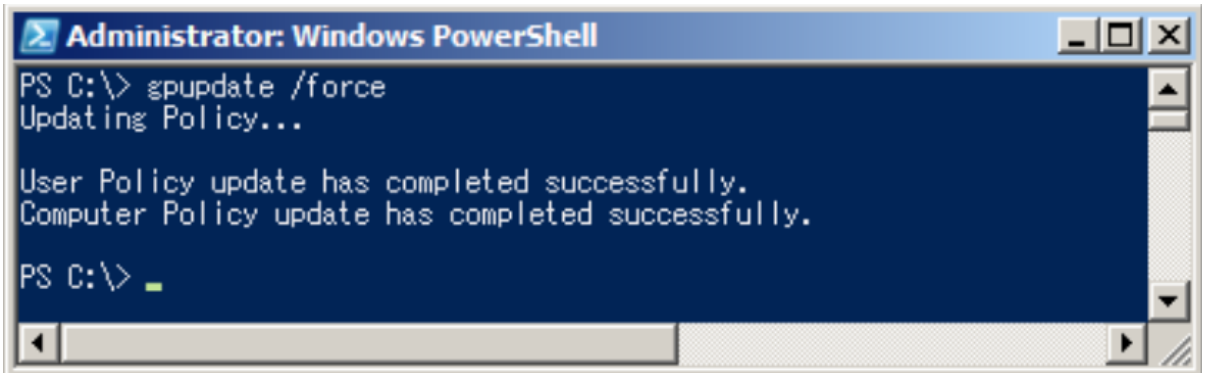
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Event Log” → and click on “Maximum security log size” → Check “Define this policy setting” → enter 204800 KB Note: Please adjust the number based on the actual environment. → click “OK.”



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

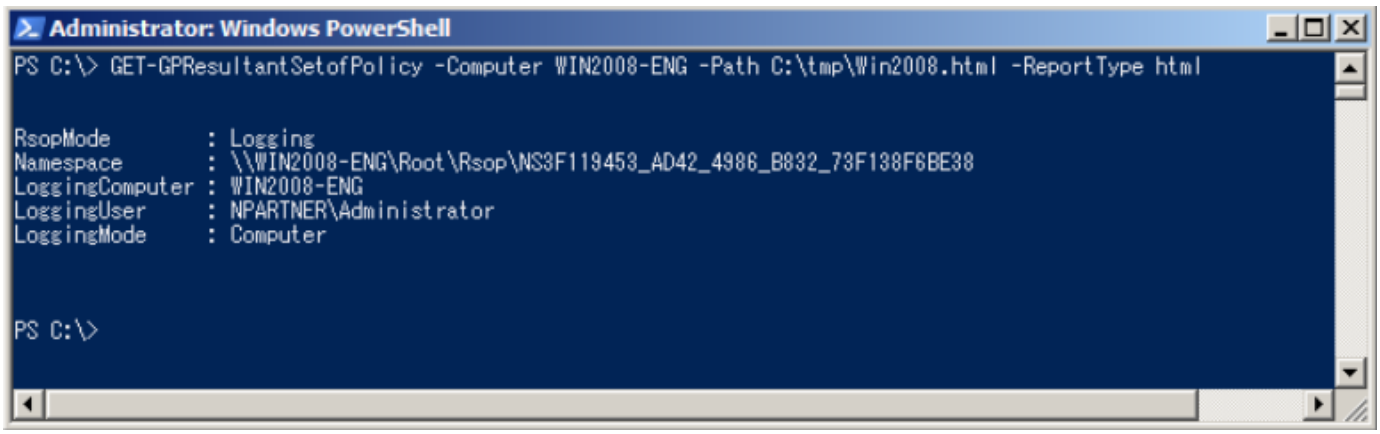
(9) Enter the command below to refresh group policy.

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



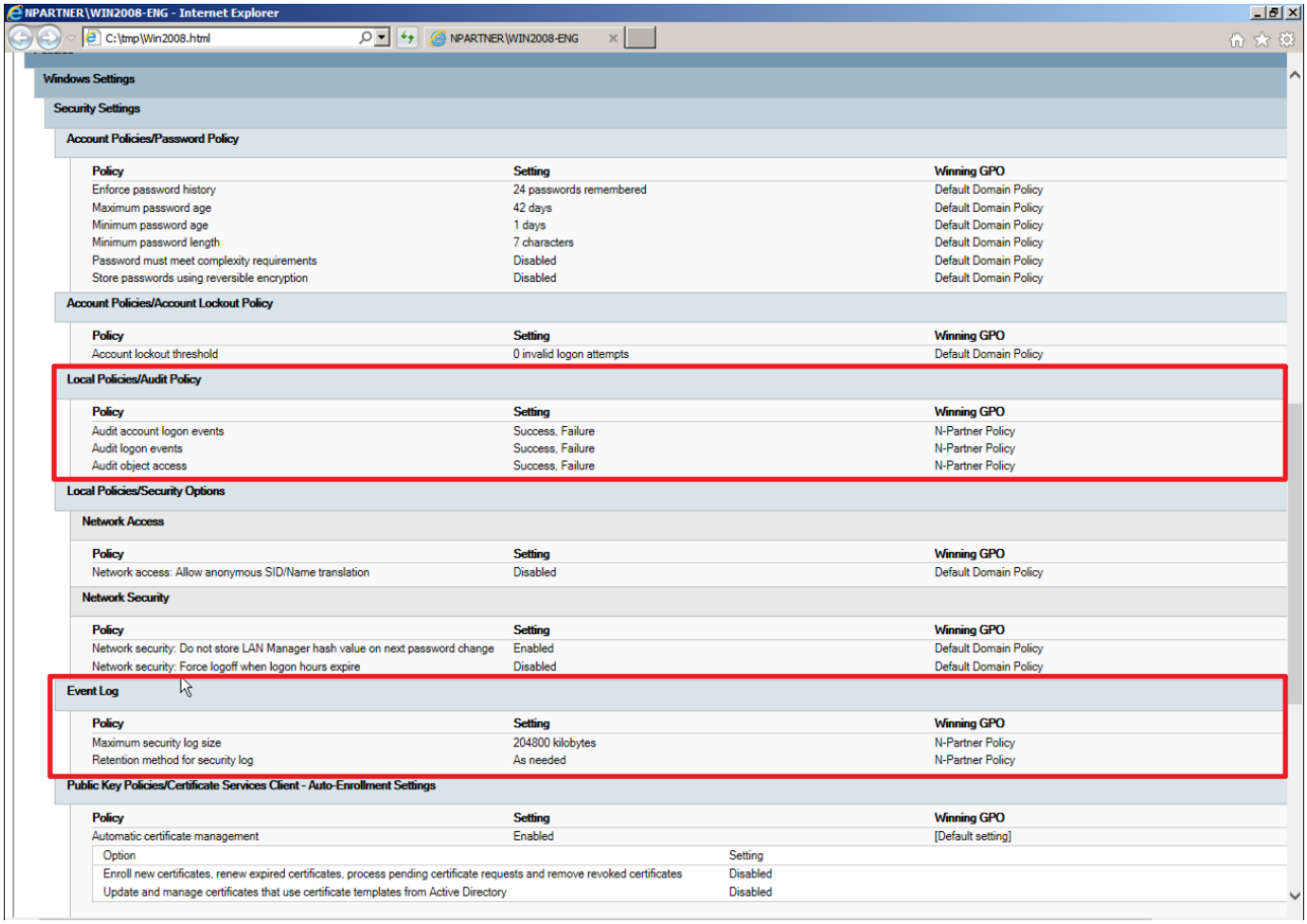
(10) On the AD domain server, open “Windows PowerShell” → enter the command below to generate the group policy report for the Windows File server.

```
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).

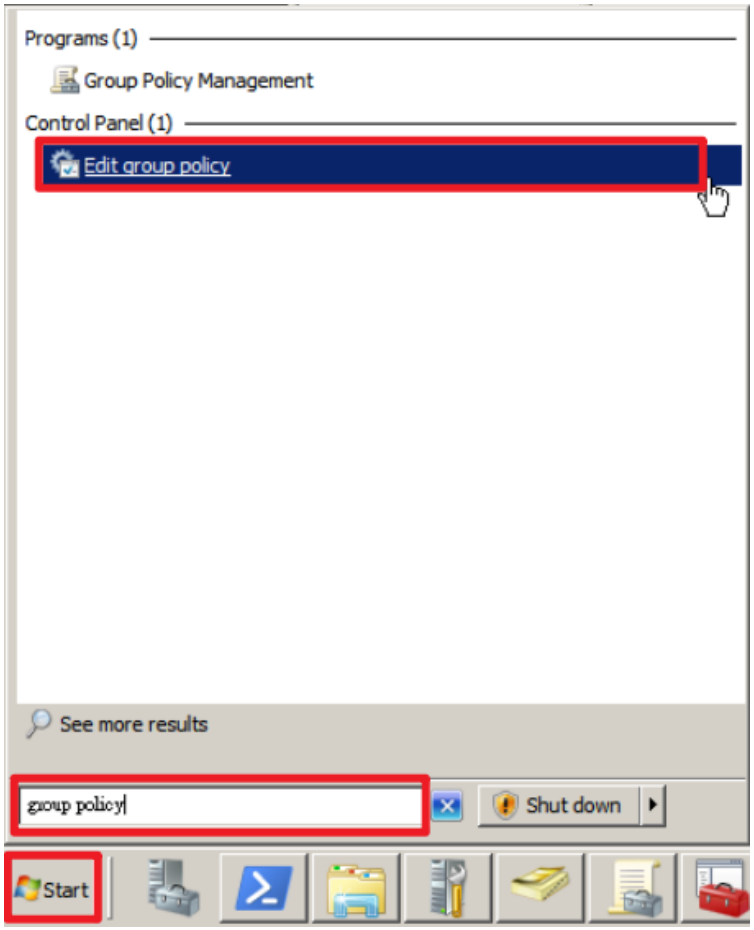


4.2 Workgroup

4.2.1 Audit Policy Configuration

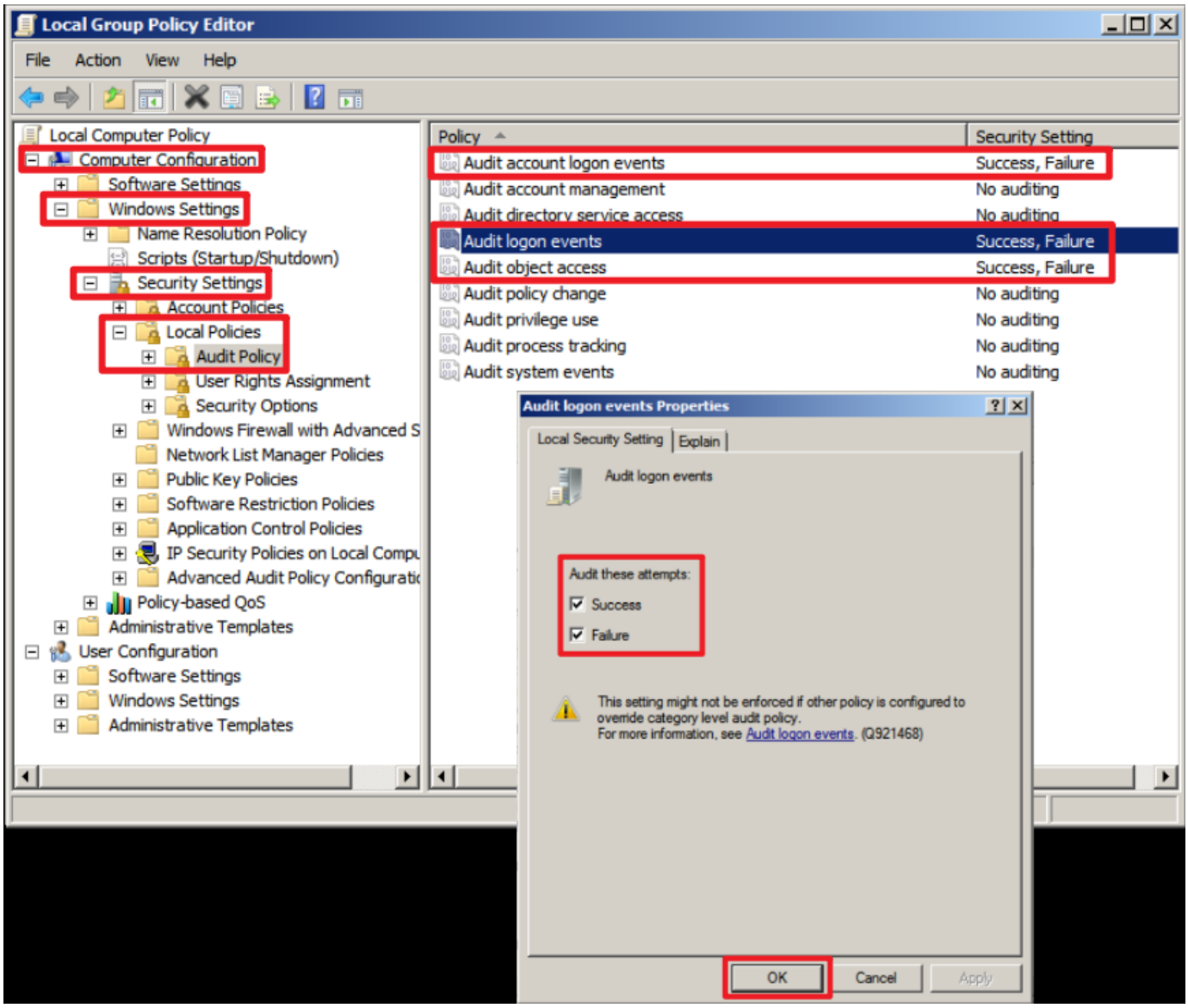
(1) Open “Local Group Policy Editor”

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



(2) Local Group Policies: Audit Policy

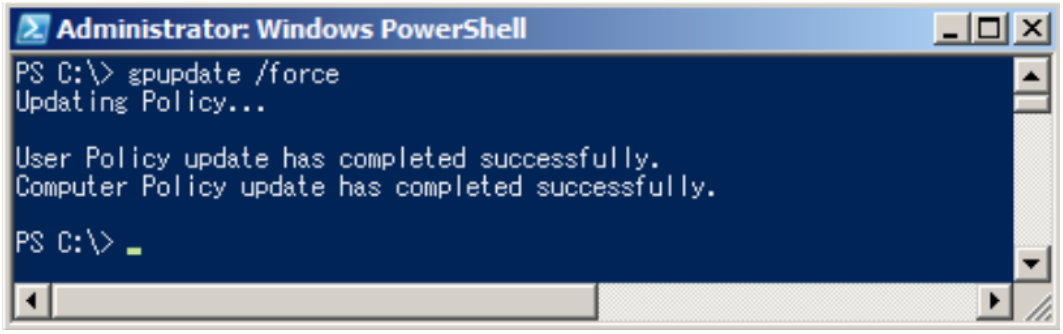
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” → “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events,” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows Powershell.”

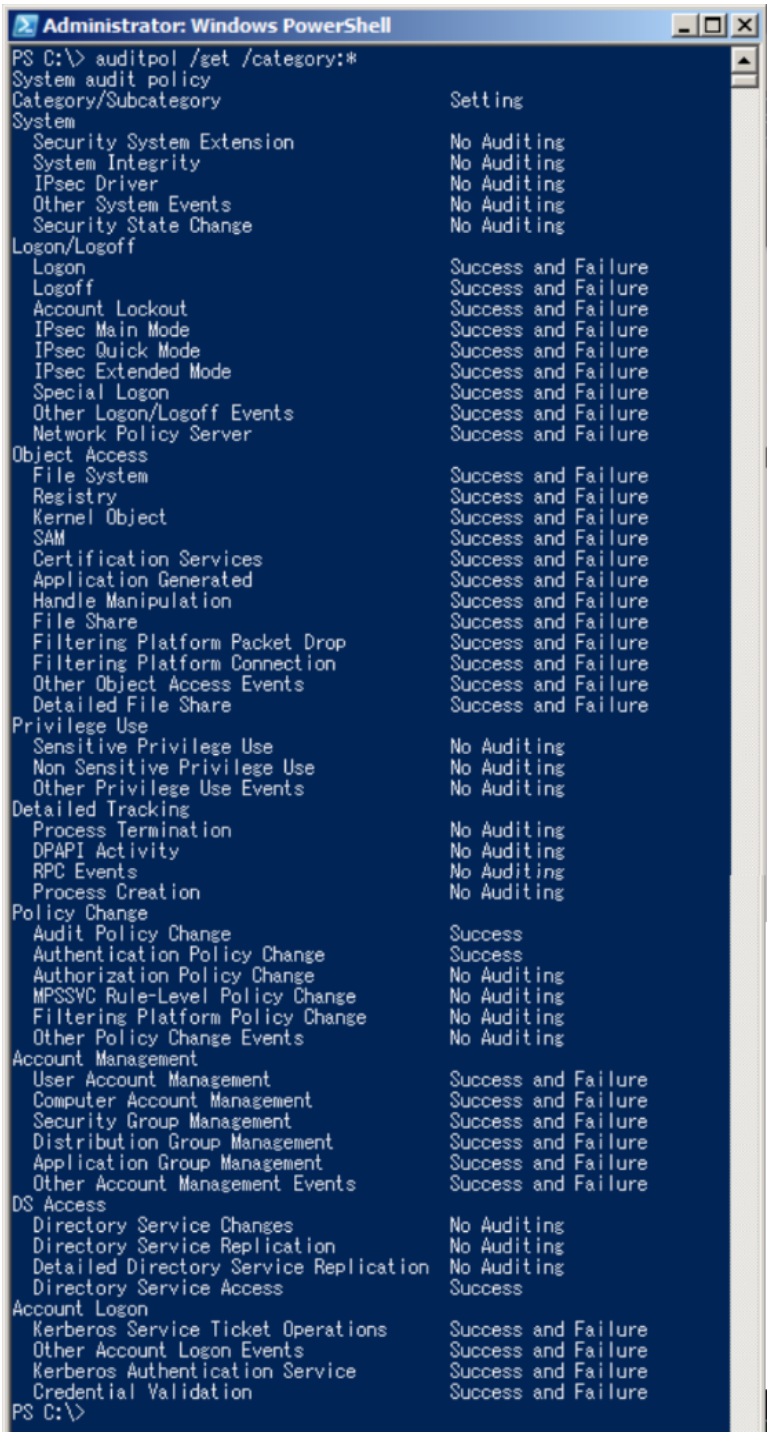
(4) Enter the command below to refresh group policy.

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



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

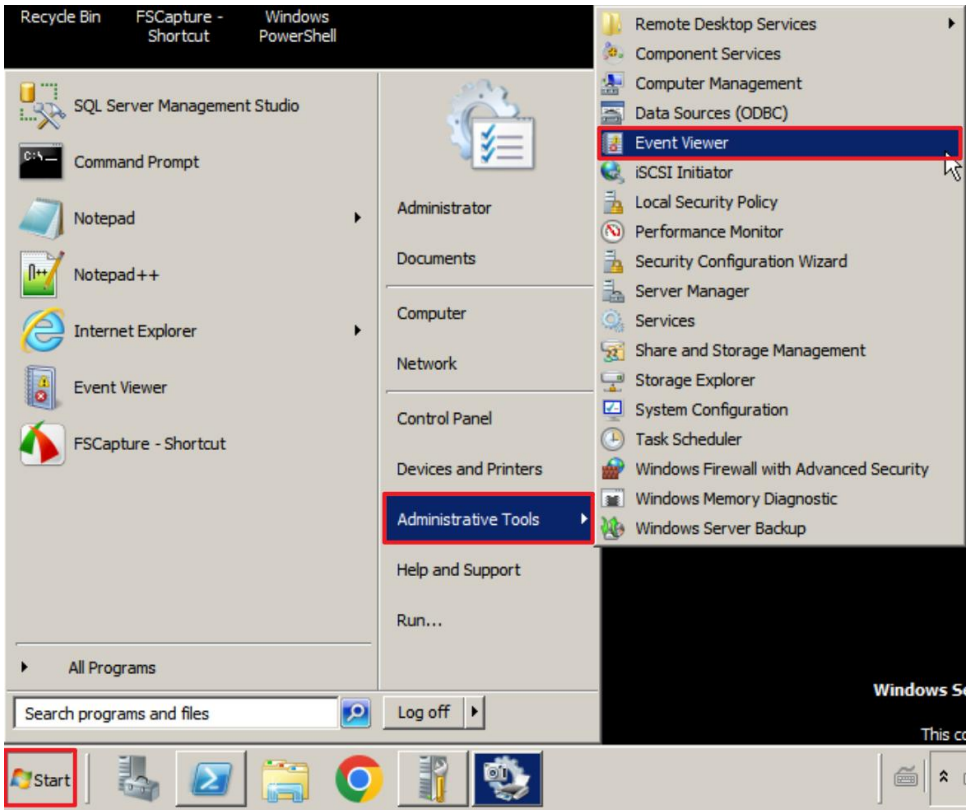
```
PS C:\> auditpol /get /category:*
```



4.2.2 Event Log Settings

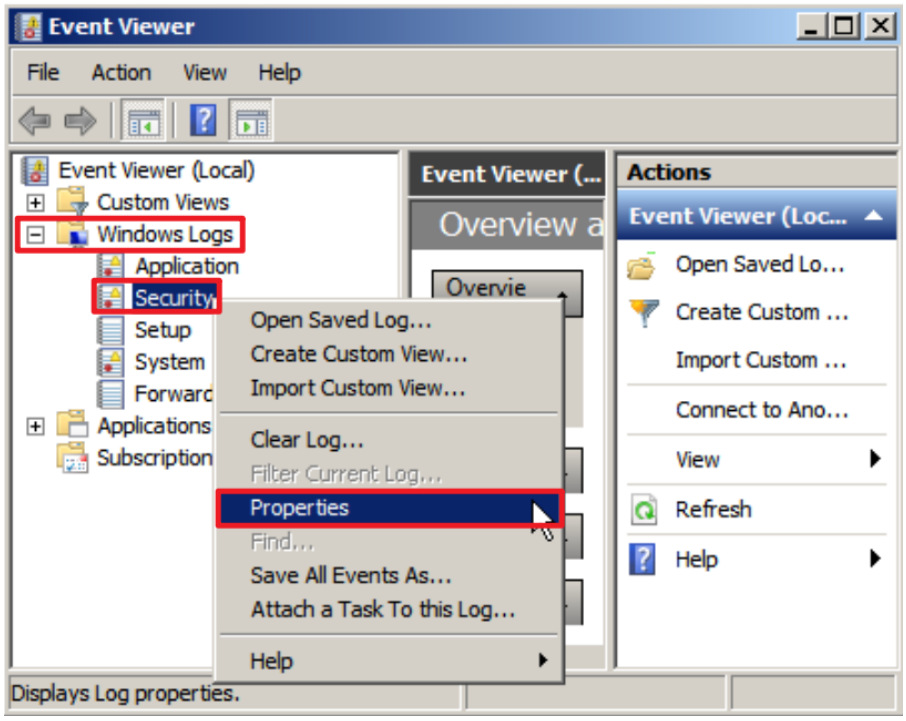
(1) Search for “Event Viewer”

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



(2) Edit Security Log

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

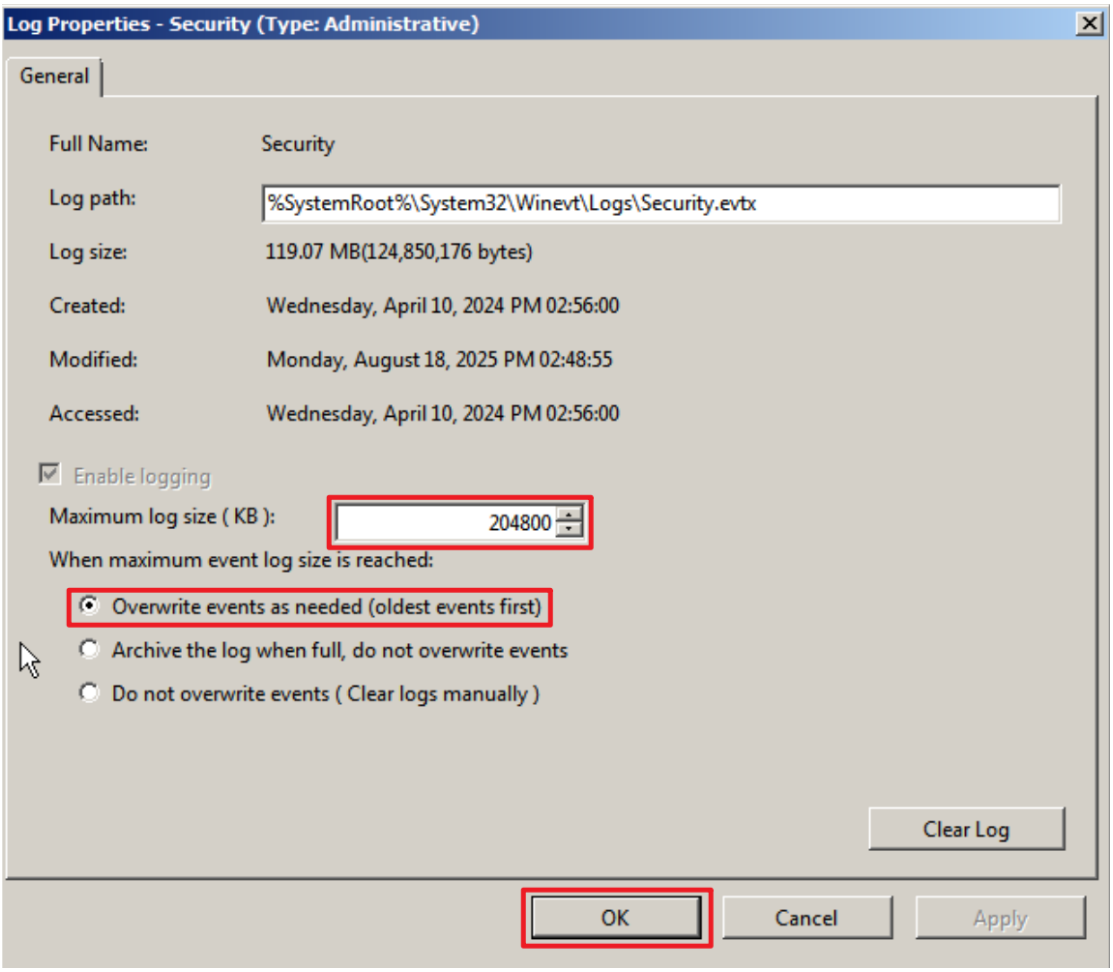


(3) Configure Security Log

Enter maximum log file size: 204800 KB

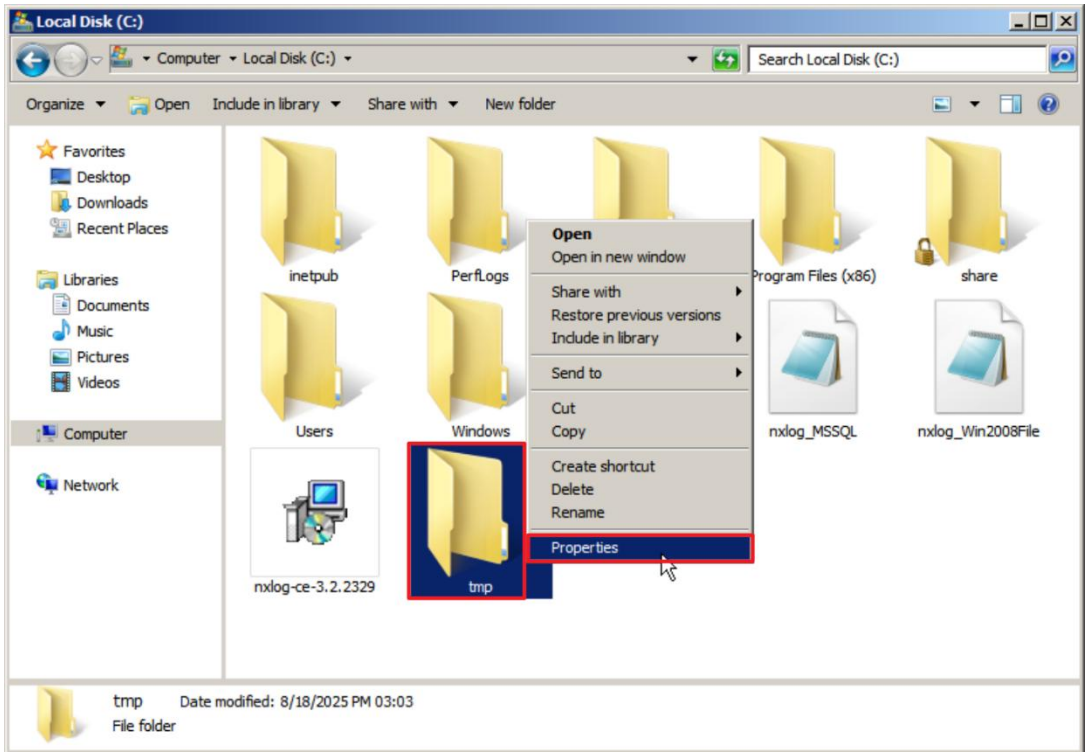
Note: Please adjust the number according to the actual environment.

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

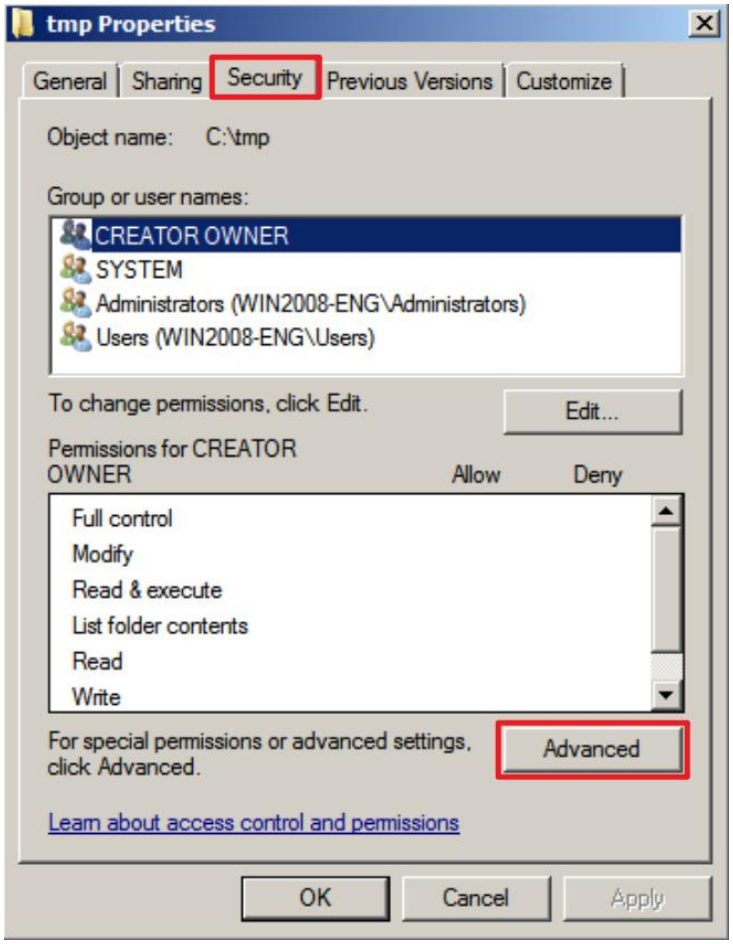


4.3 Folder Audit Configuration

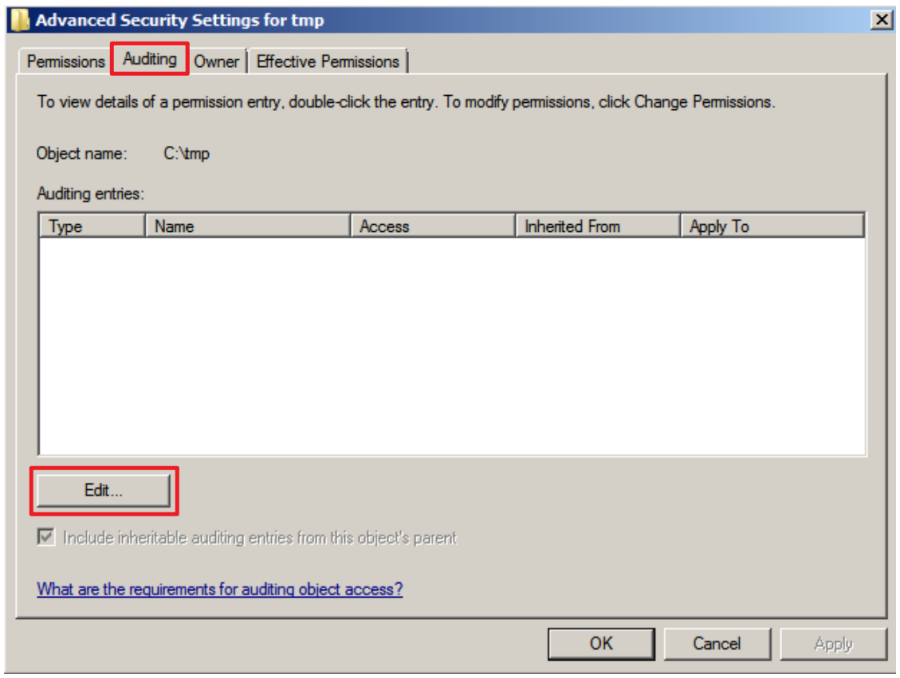
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



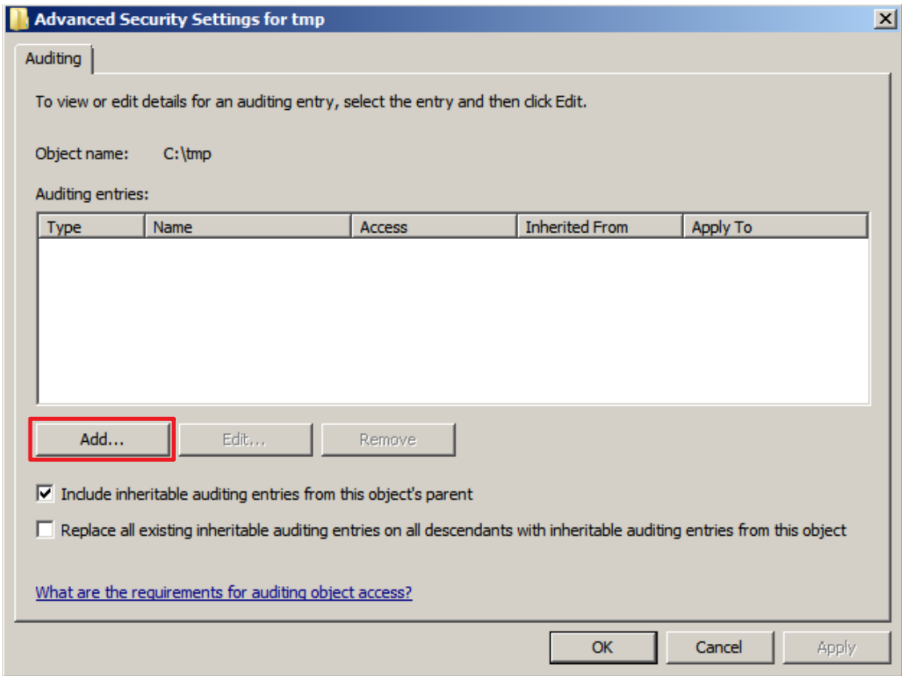
(2) Go to the “Security” tab → click “Advanced.”



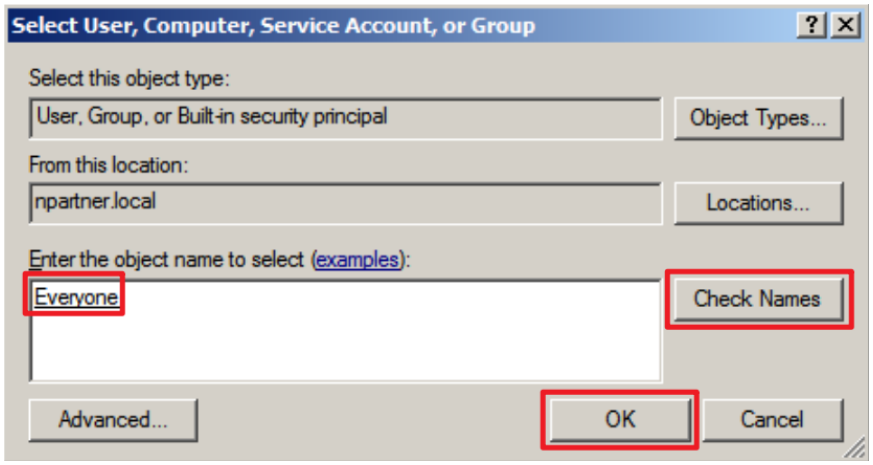
(3) Open the “Auditing” tab → click “Edit.”



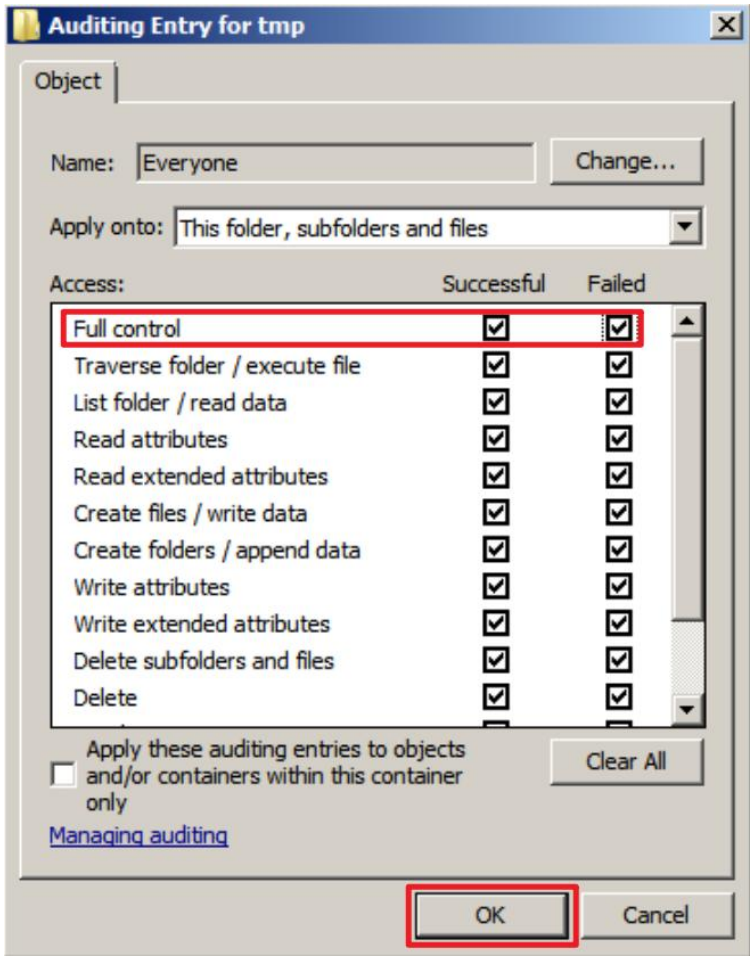
(4) Click “Add.”



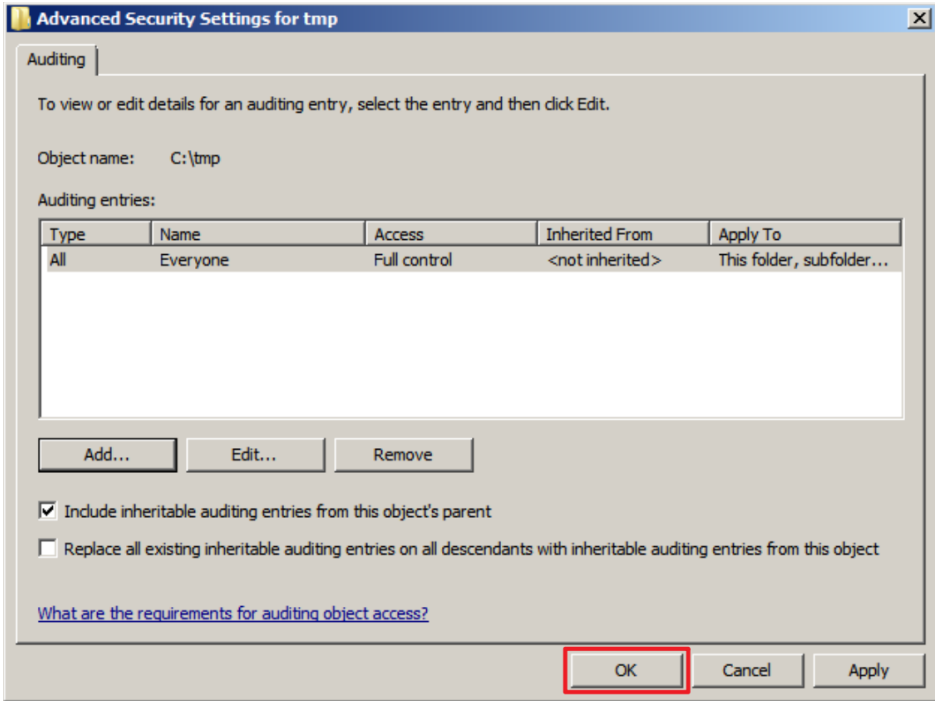
(5) In the object name field, enter Everyone to audit all users → click “Check Names” → click “OK.”



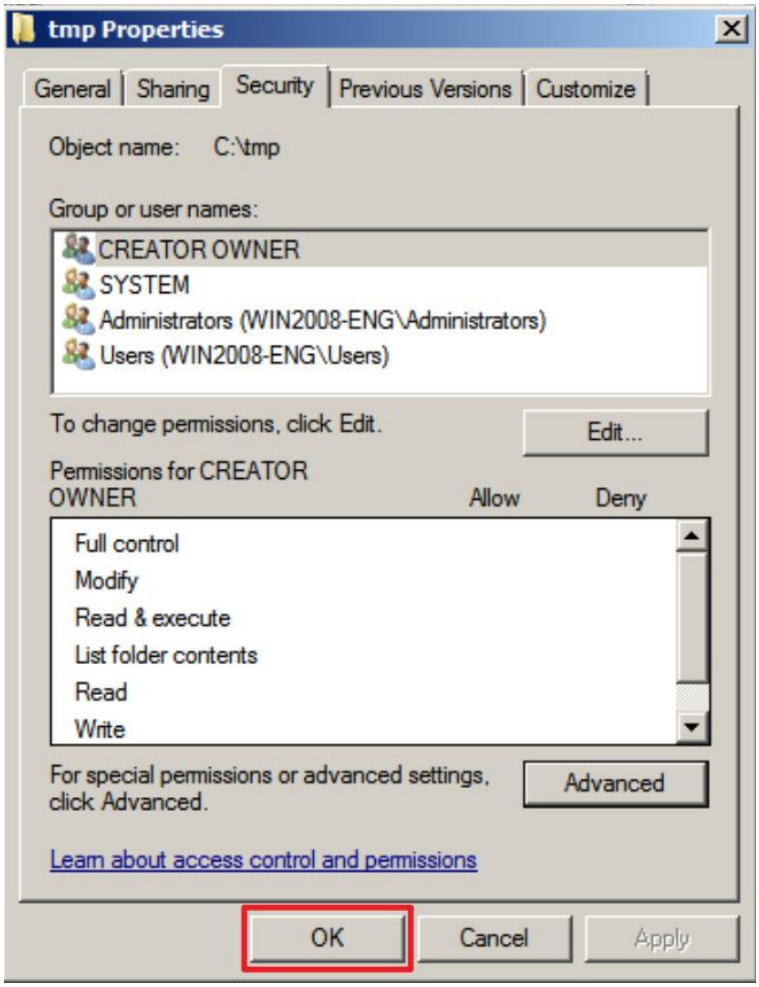
(6) For access types, select “Full Control” for both “Success” and “Failure,” and then click “OK.”



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



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



5. Windows Server 2012

5.1 Domain

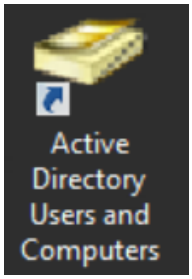
Windows Audit Policy Configuration:

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.

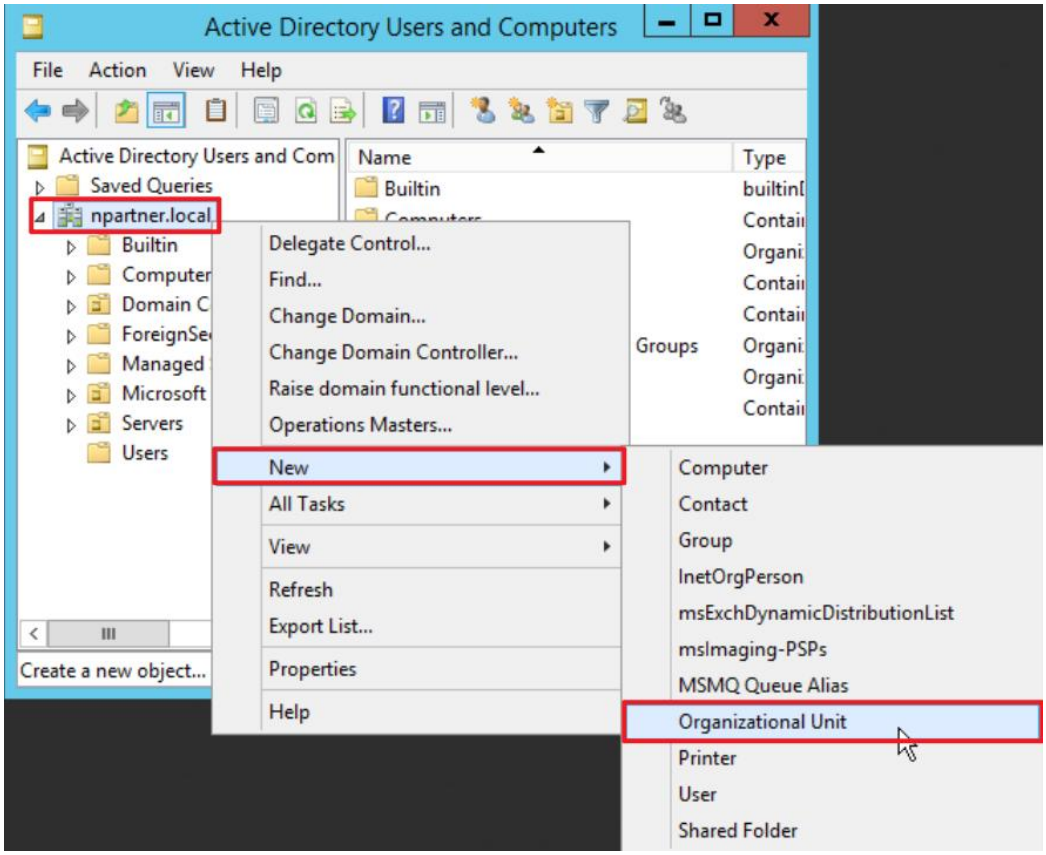
5.1.1 Organizational Unit (OU) Configuration

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



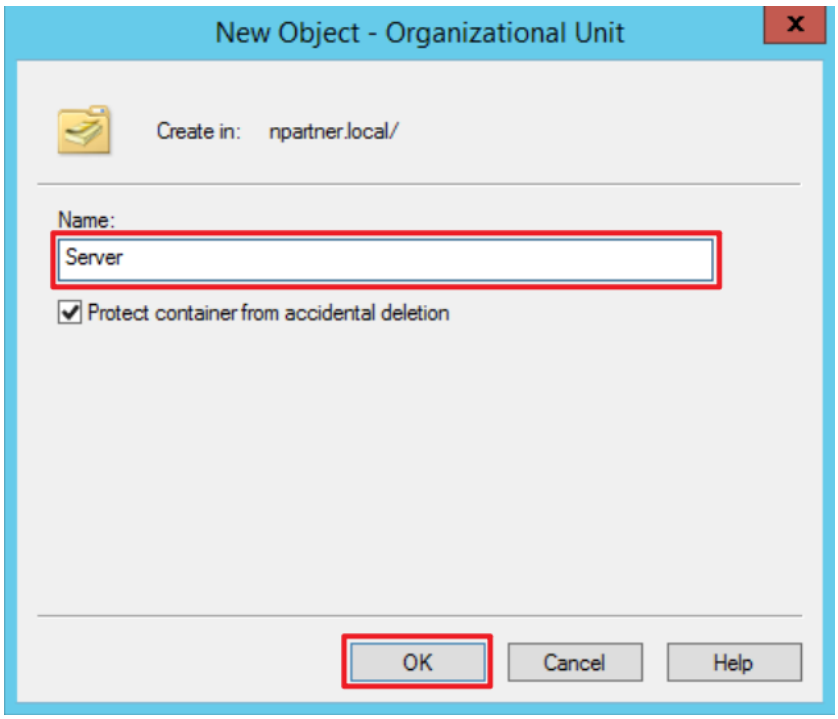
(2) Add an Organizational Unit

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”)

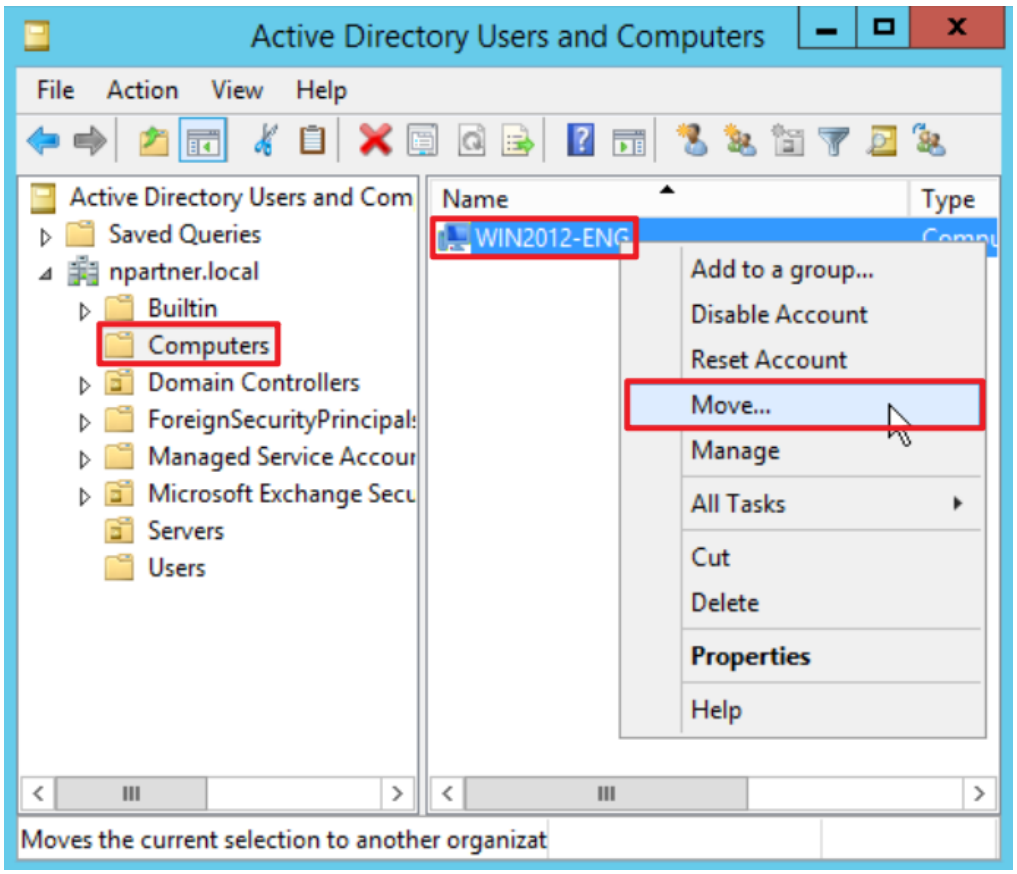
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

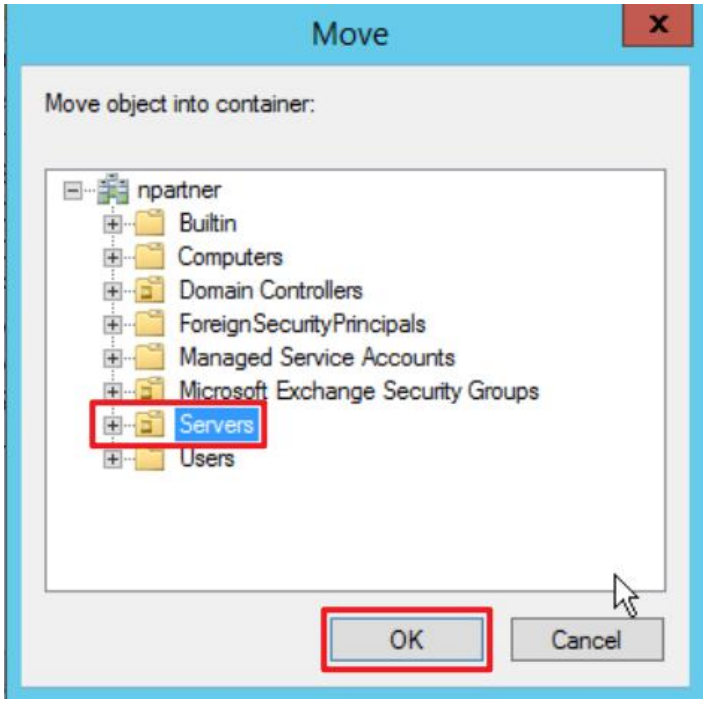
Select the “Computers” organizational unit (OU) → right-click on the “WIN2012” server.

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



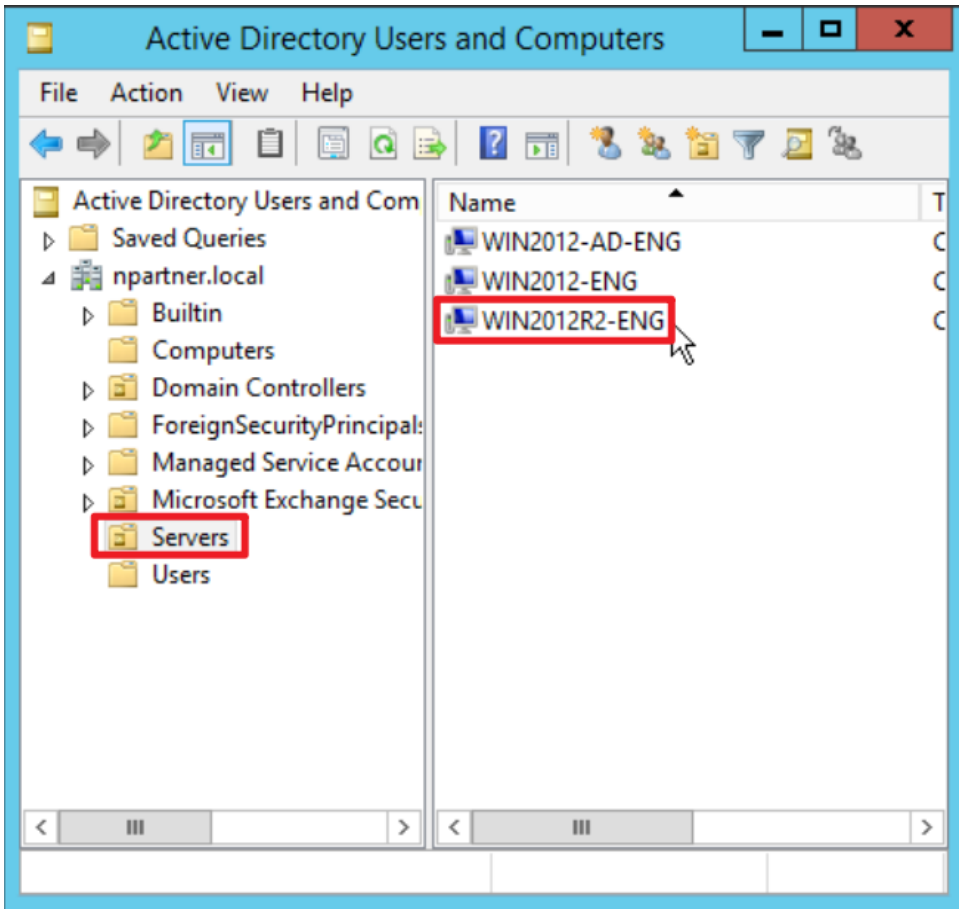
(5) Select your Organizational Unit:

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.

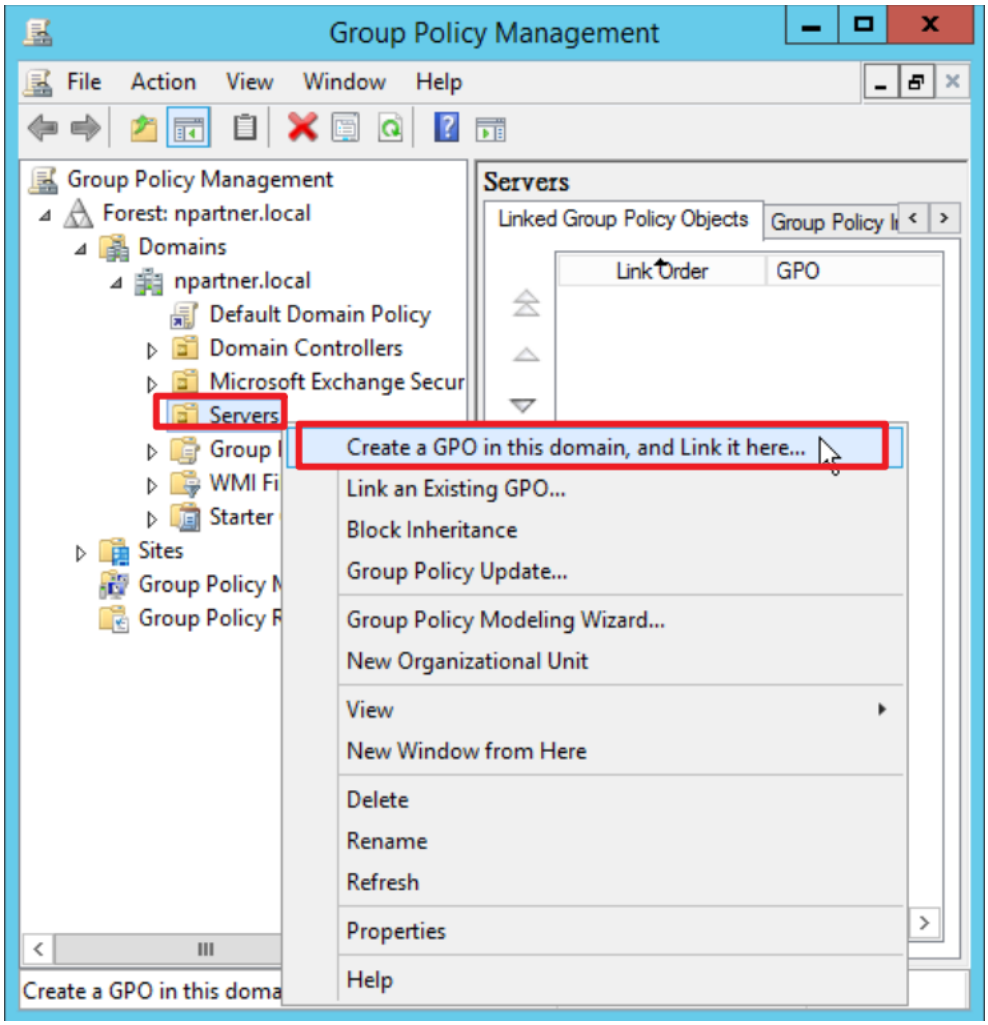


5.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

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

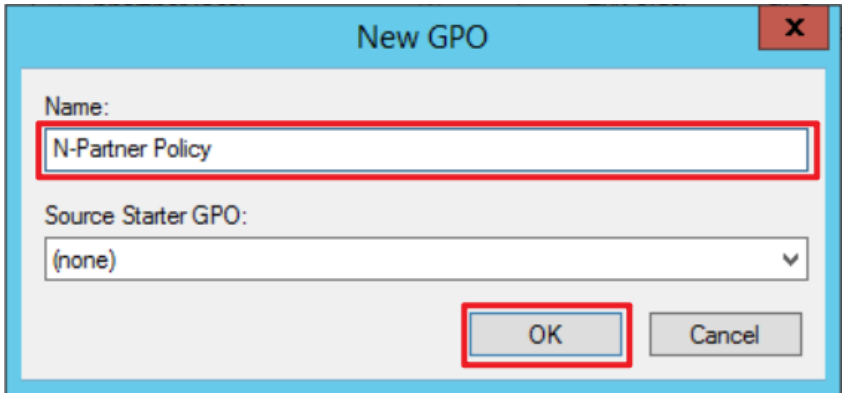
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

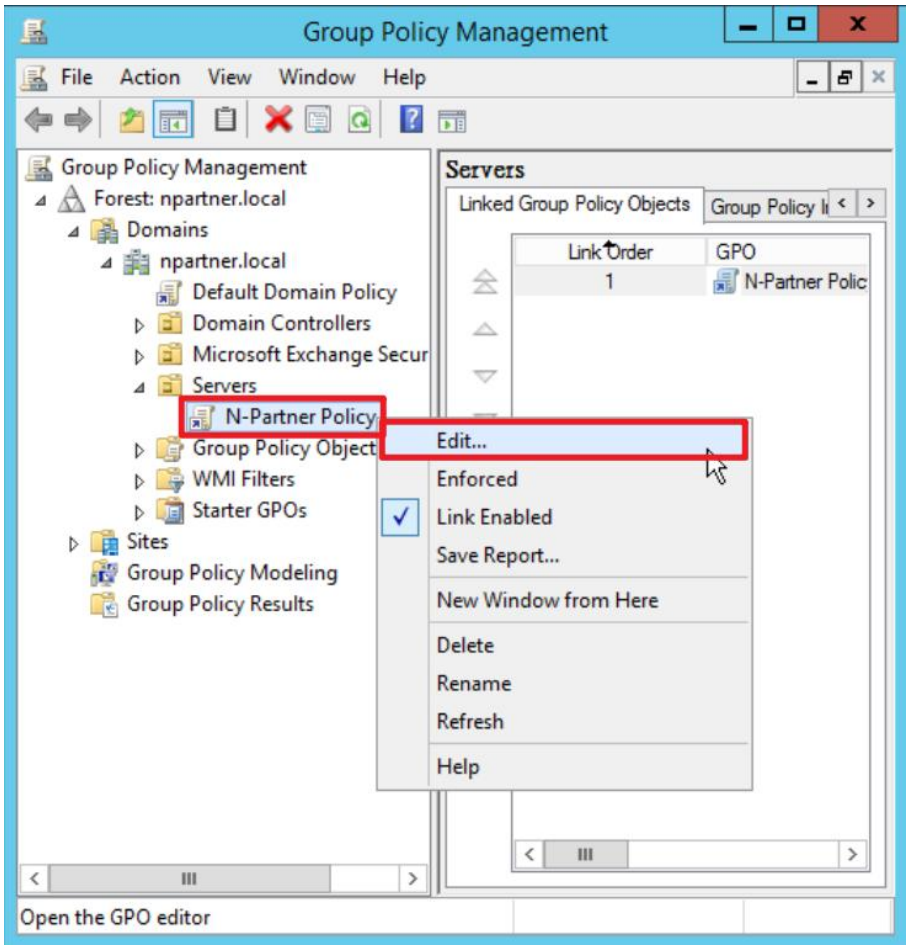
Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

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



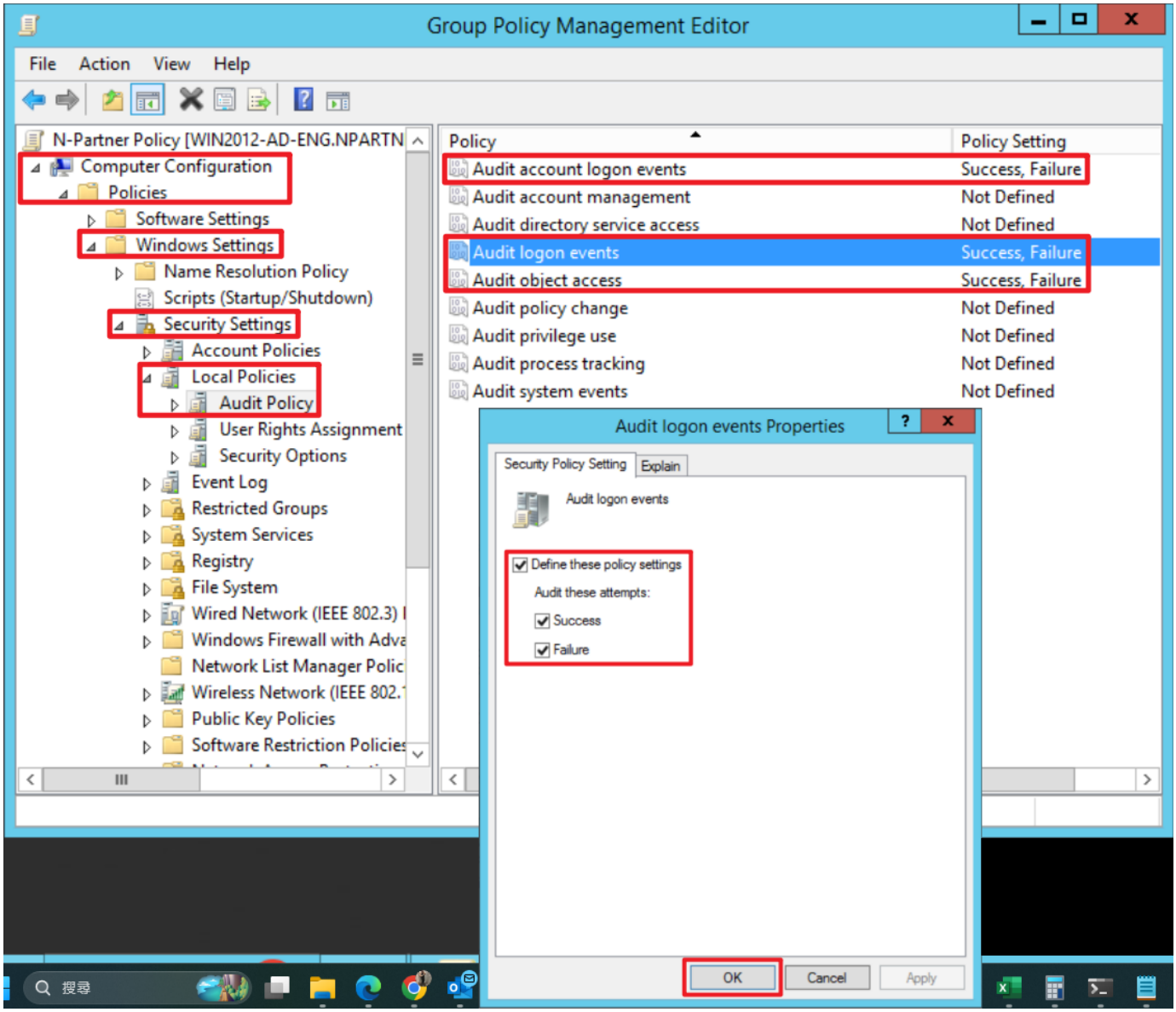
(4) Edit your Group Policy Object

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



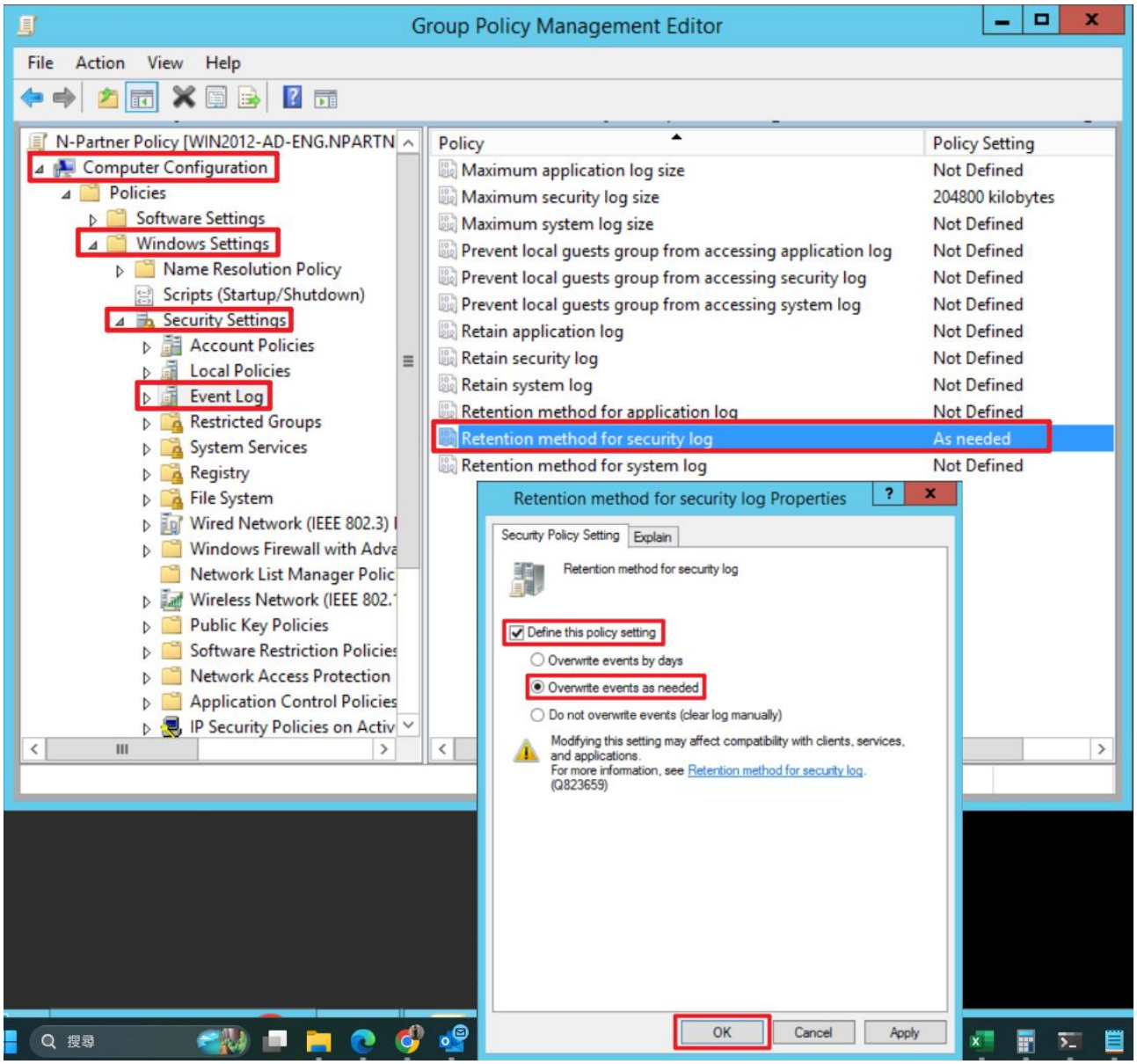
(5) Local Group Policies: Audit Policy

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

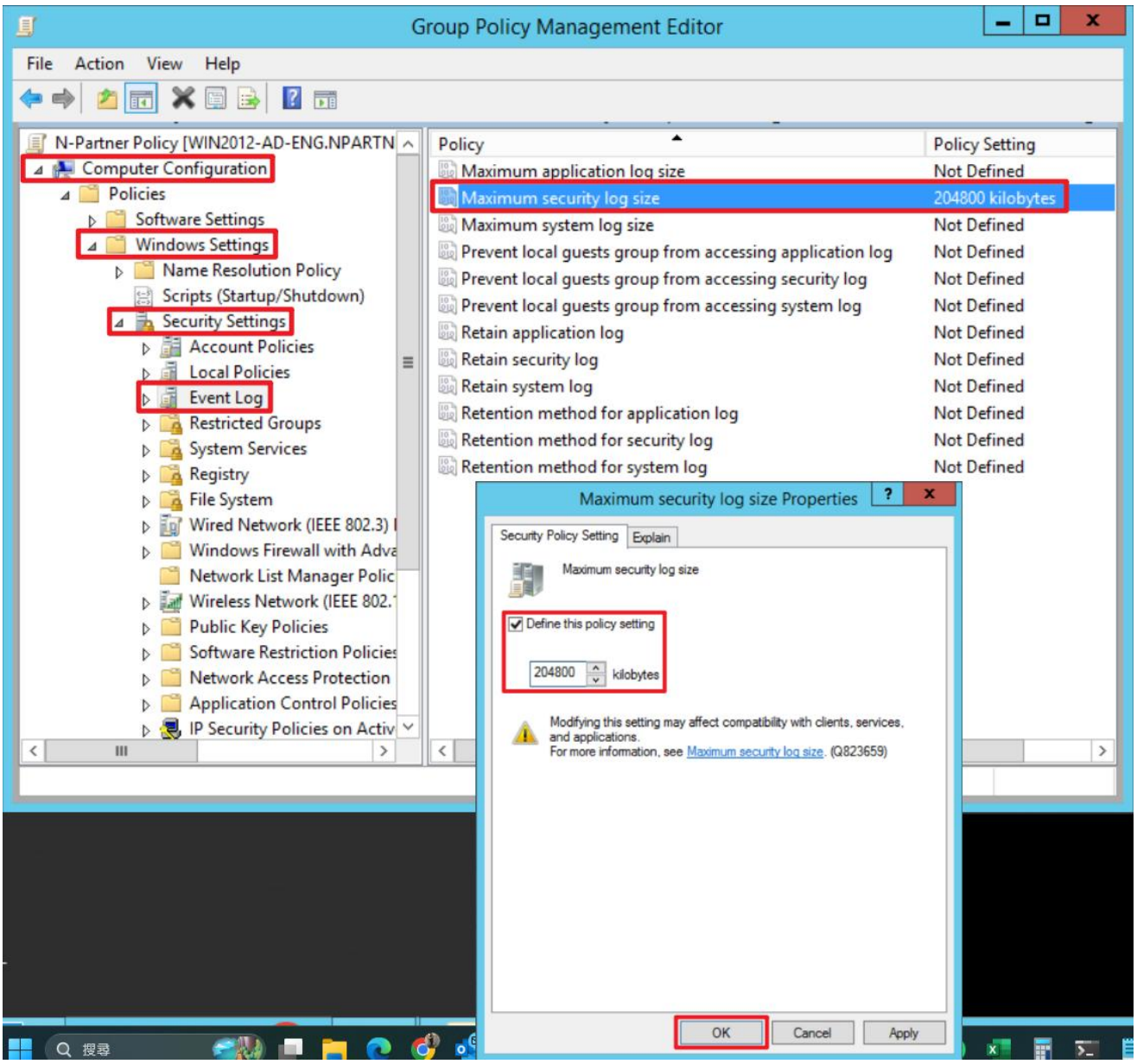
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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

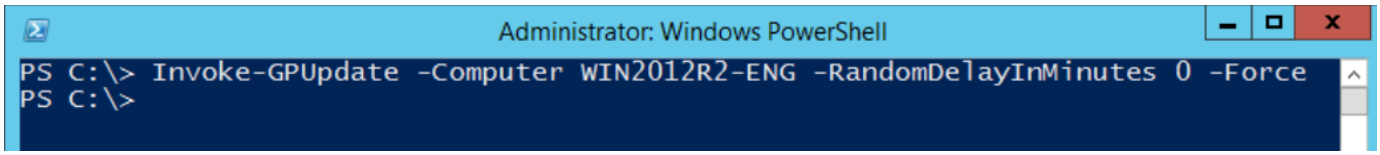
Note: Please adjust the number based on the actual environment. → click “OK.”



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

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

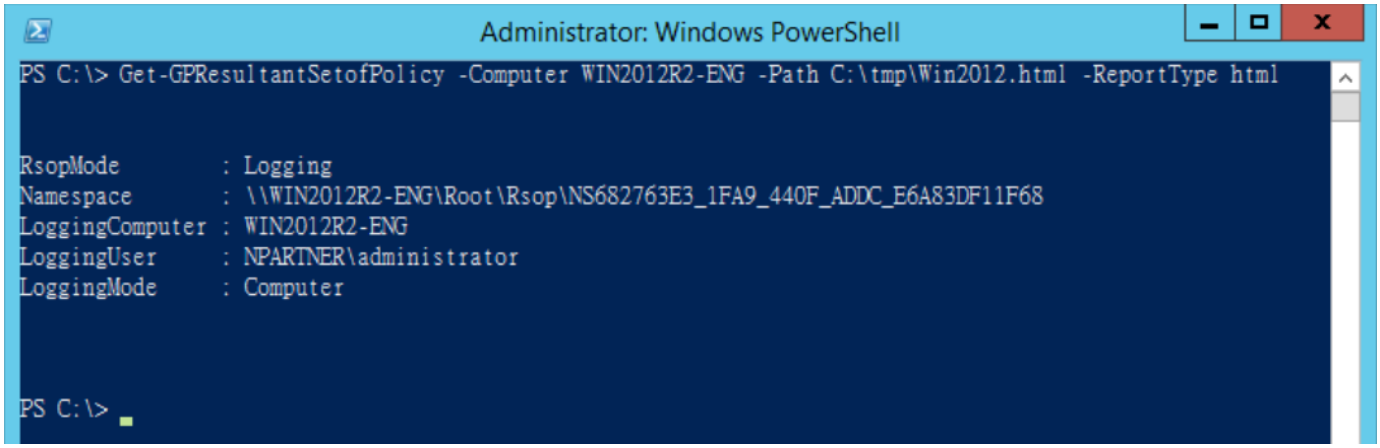
```
PS C:\> Invoke-GPUpdate -Computer WIN2012-ENG -RandomDelayInMinutes 0 -Force
```



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

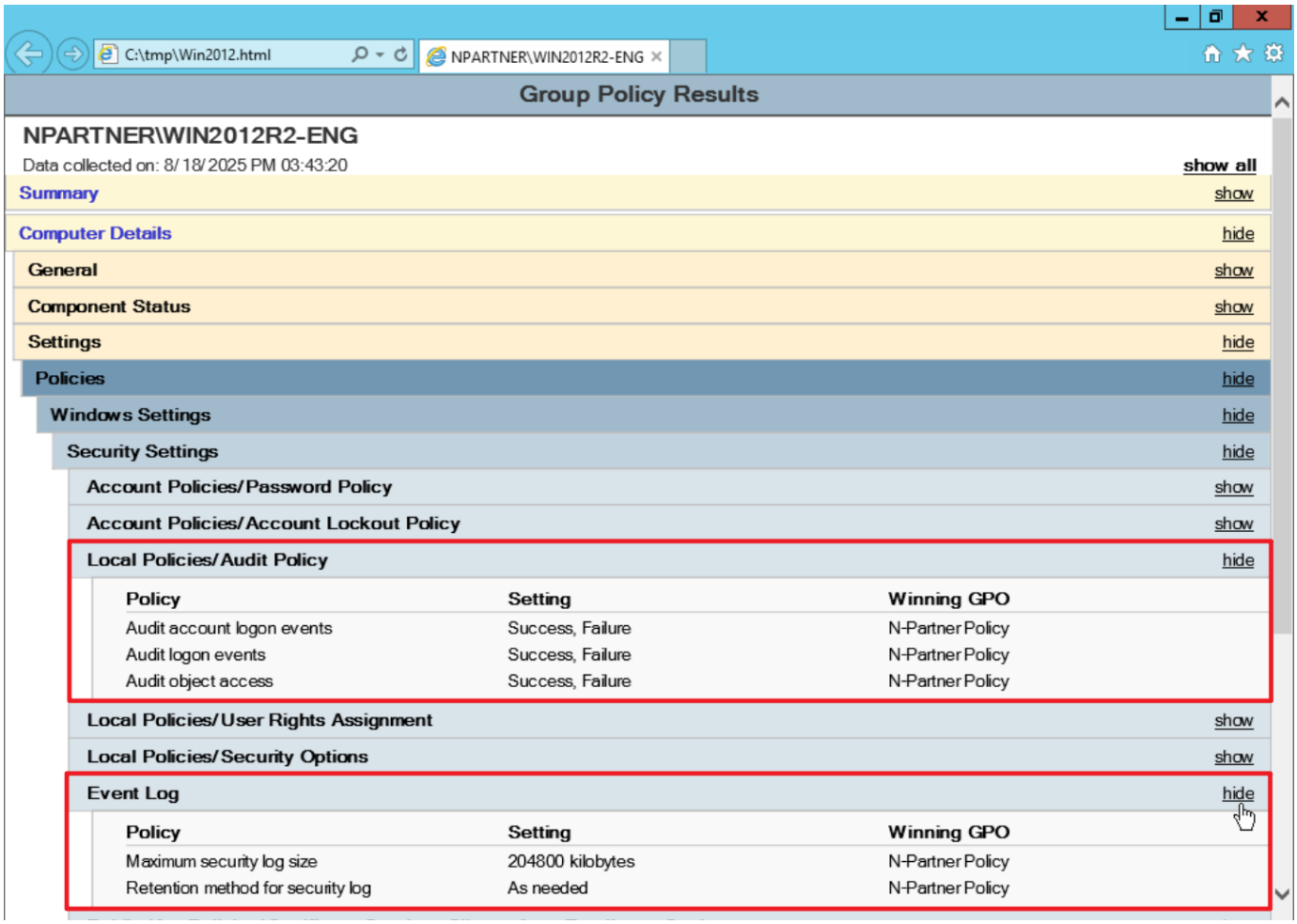
(10) Enter the command below to generate server group policy report.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2012-ENG -Path C:\tmp\WIN2012.htnl -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.

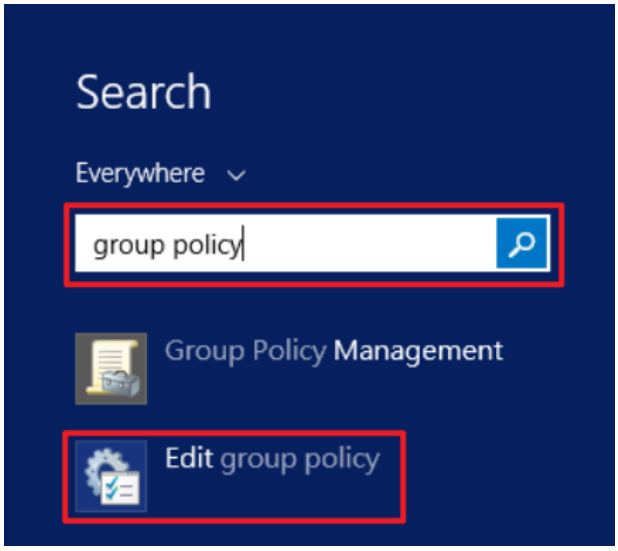


5.2 Workgroup

5.2.1 Audit Policy Configuration

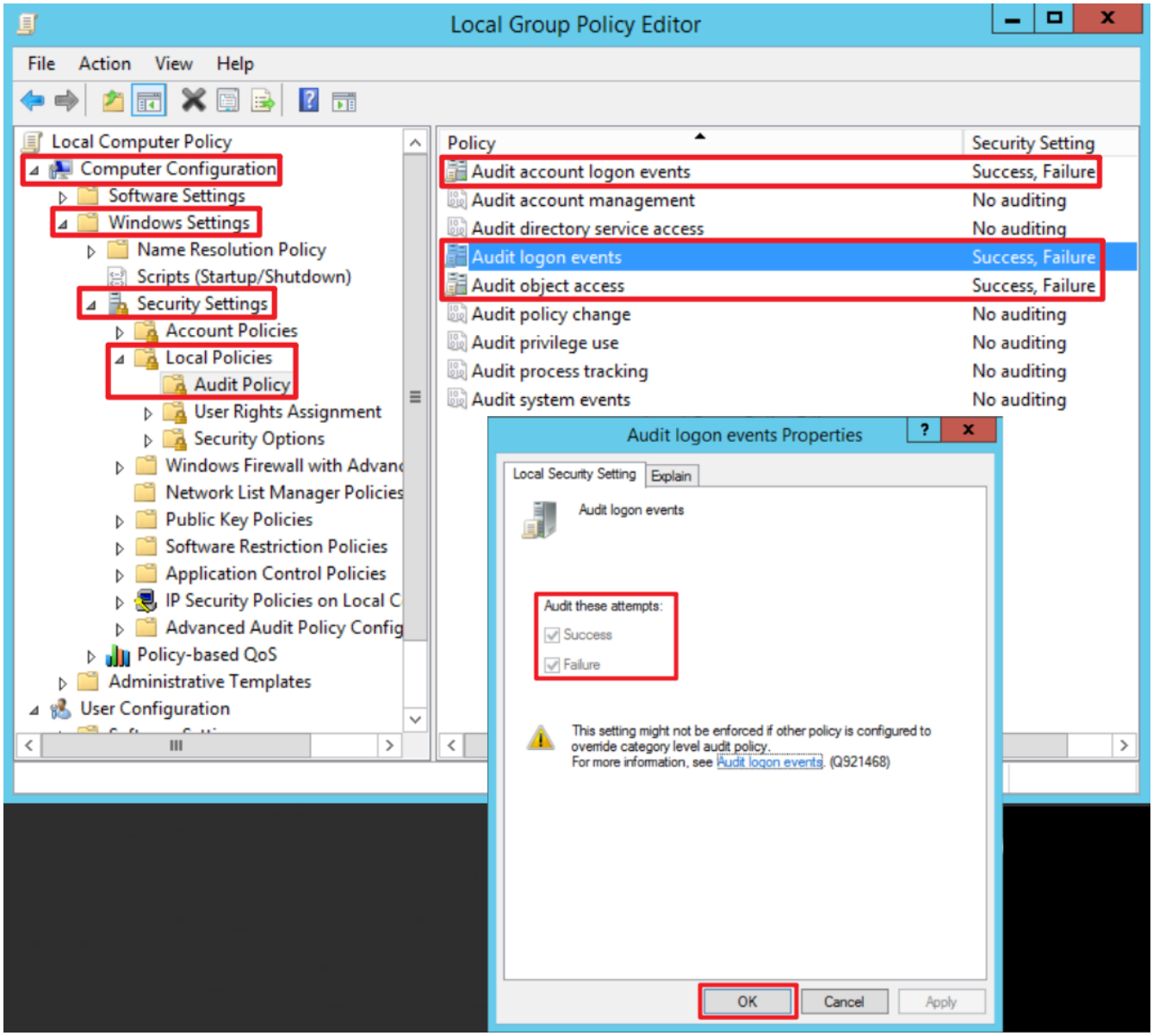
(1) Open Local Group Policy Editor

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



(2) Local Group Policies: Audit Policy

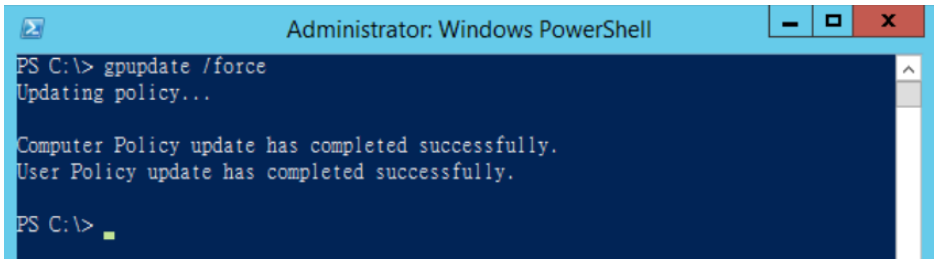
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”

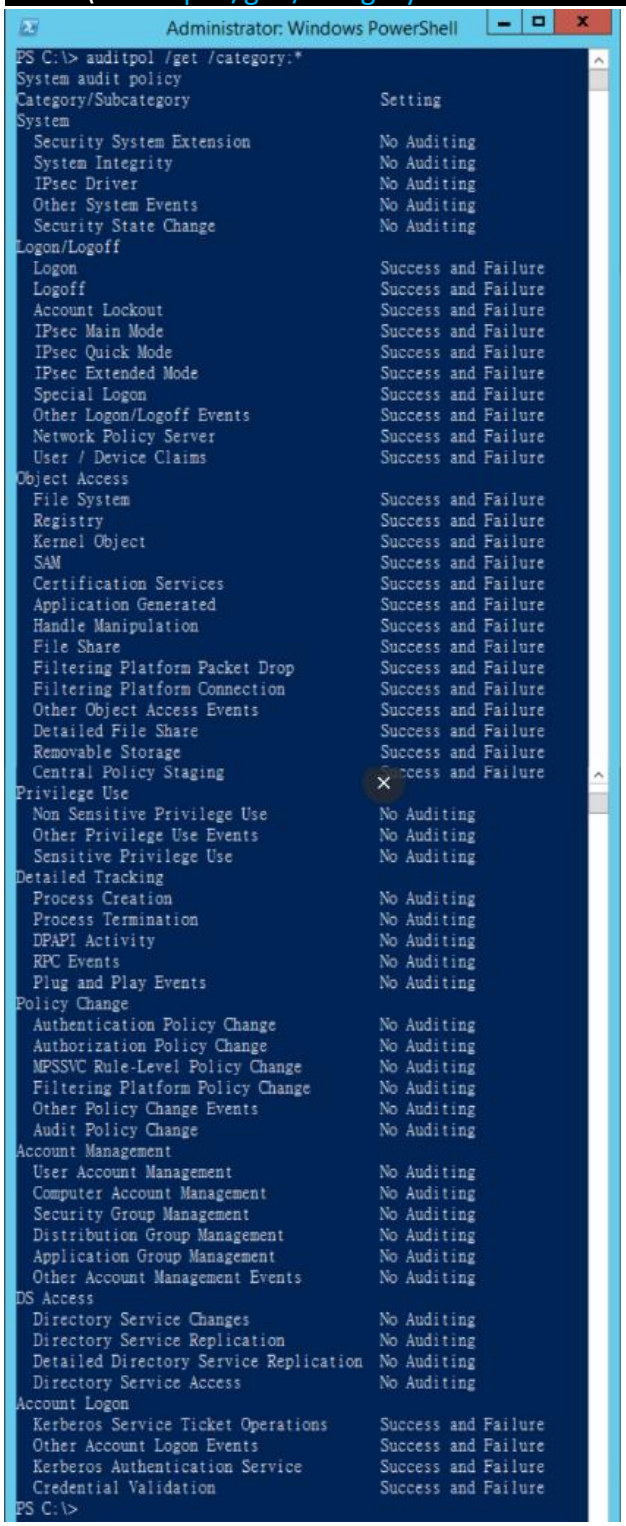
(4) Enter the command below to refresh group policy.

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



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

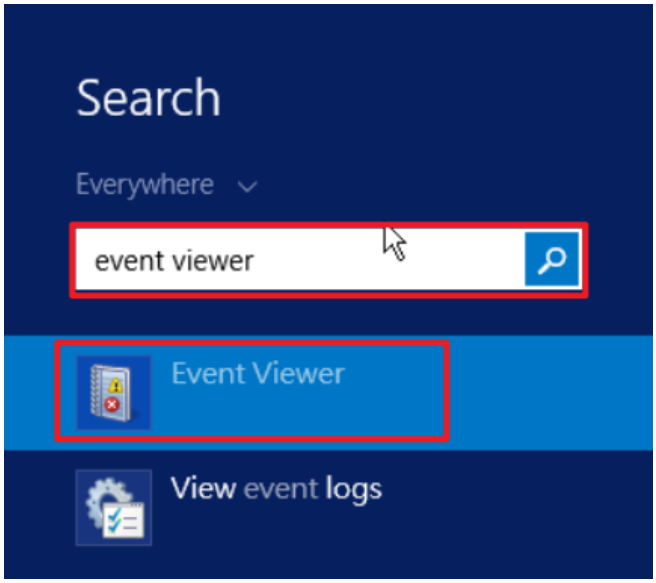
```
PS C: \> auditpol /get /category:*
```



5.2.2 Event Log Settings

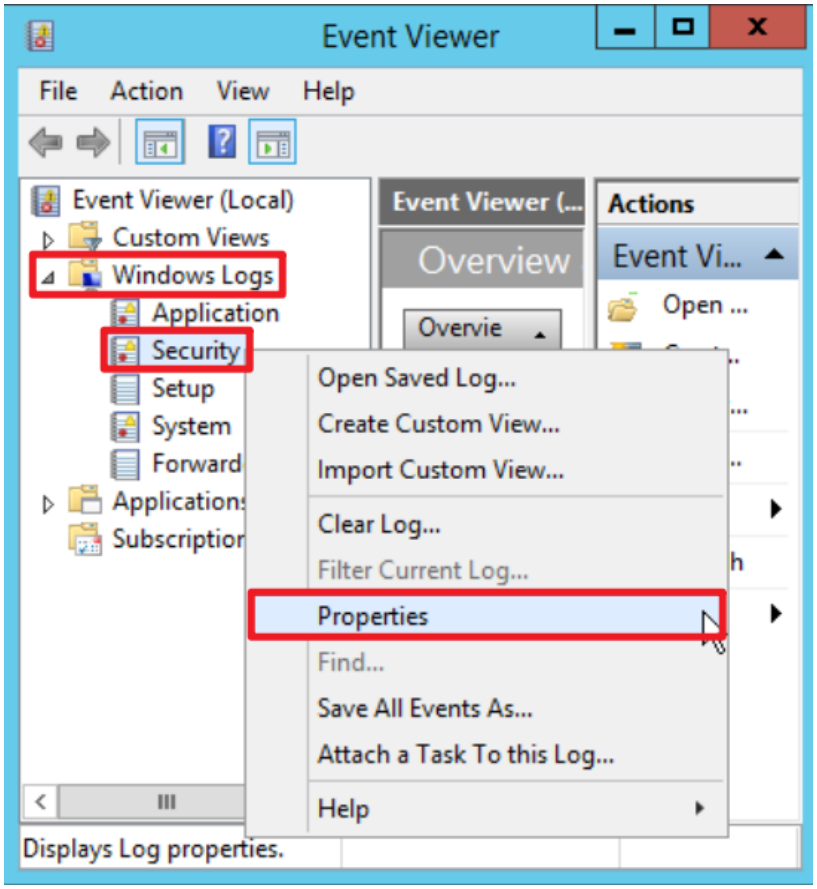
(1) Search for “Event Viewer”

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.”

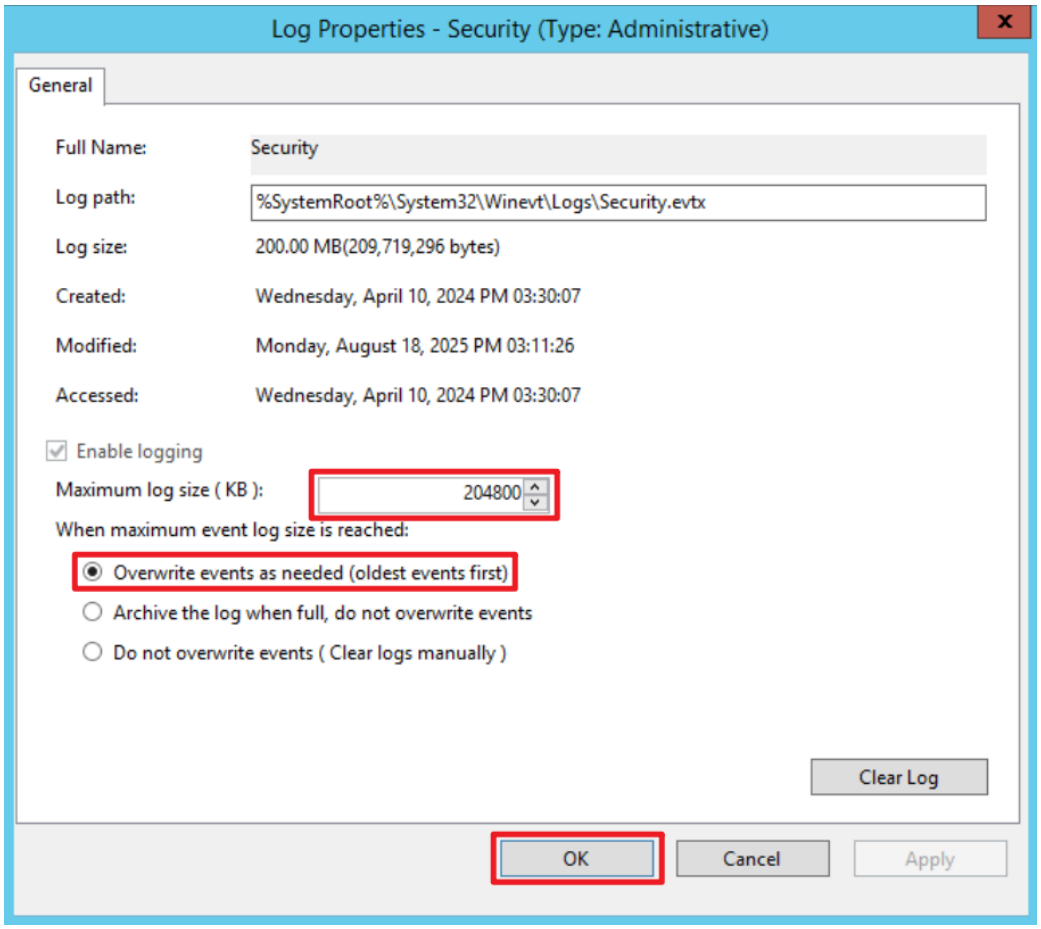


(3) Configure Security Log

Enter maximum log file size: 204800 KB

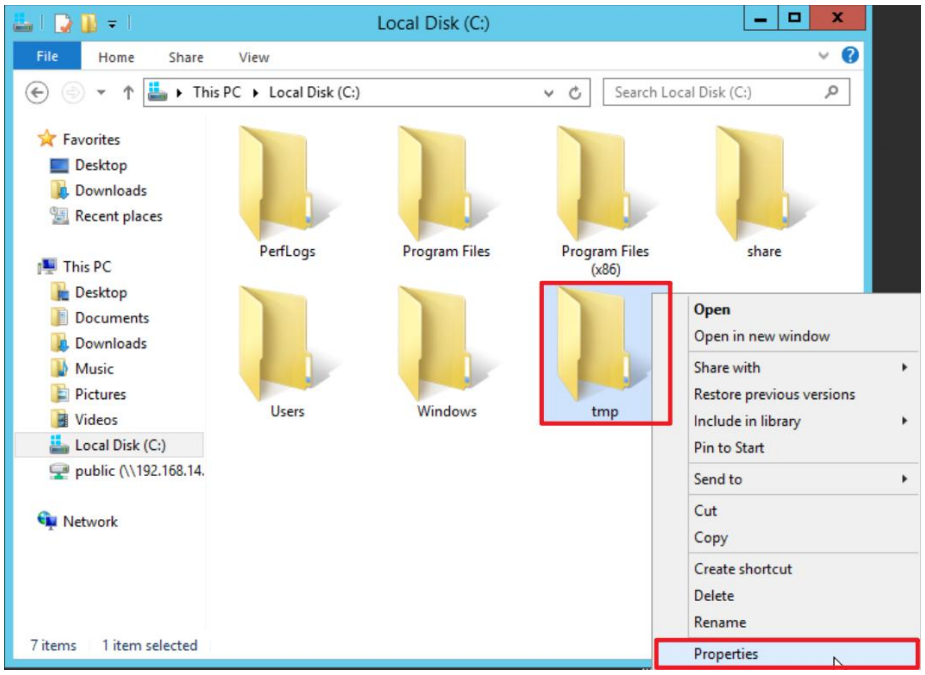
Note: Please adjust the number according to the actual environment.

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

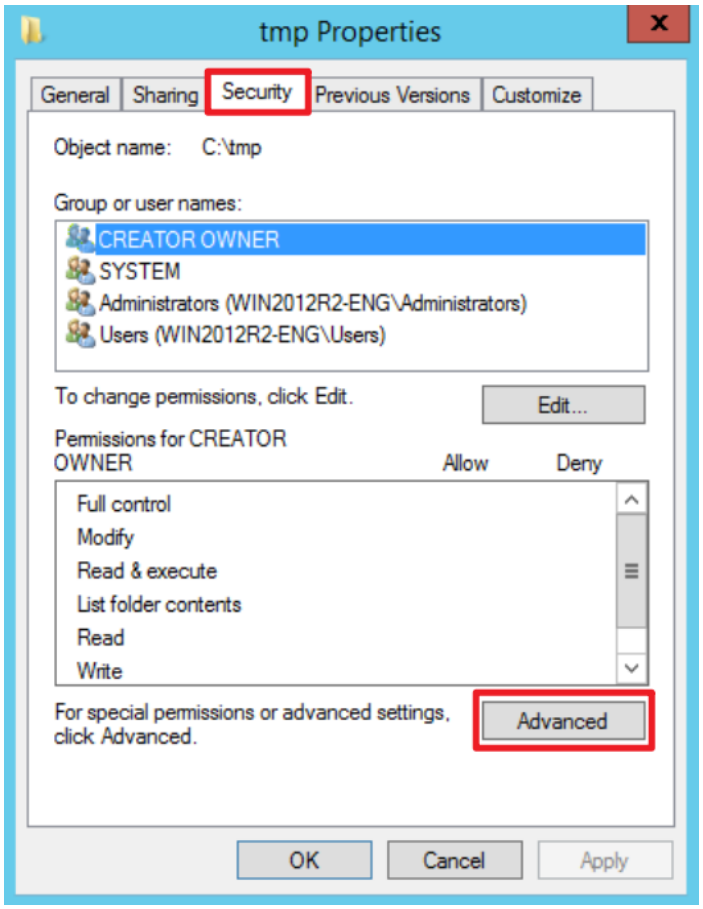


5.3 Folder Audit Configuration

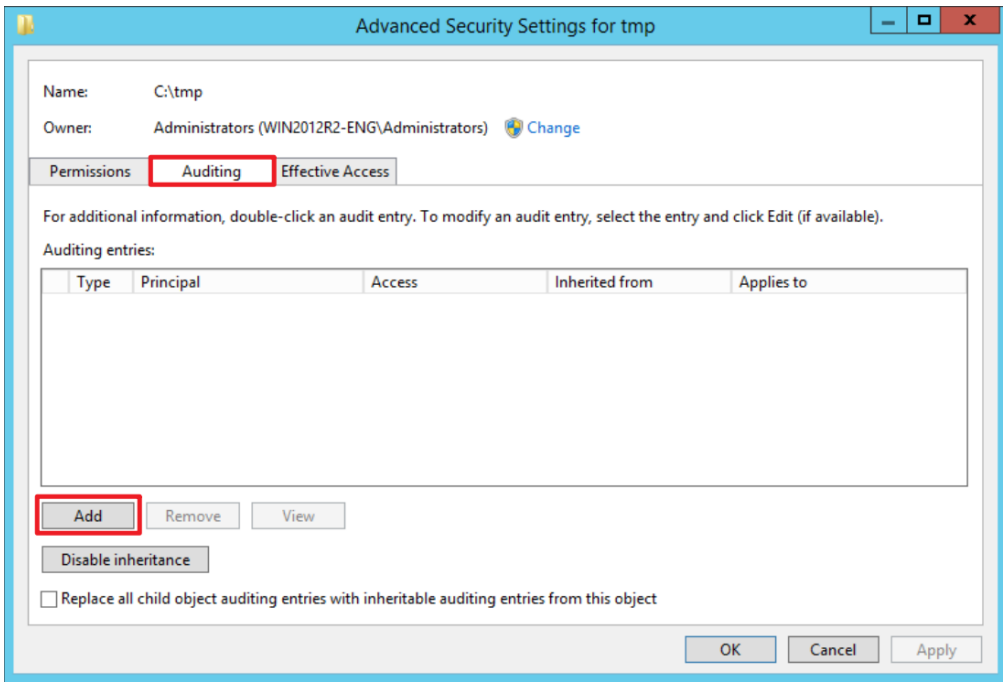
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



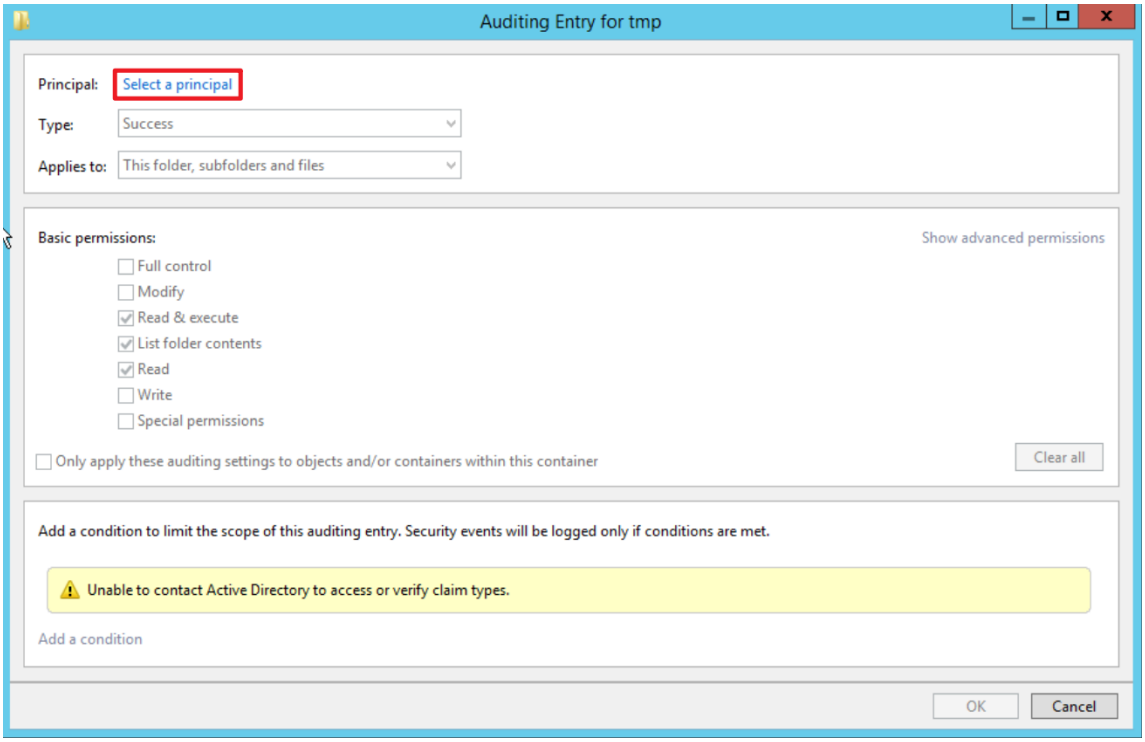
(2) Go to the “Security” tab → click “Advanced.”



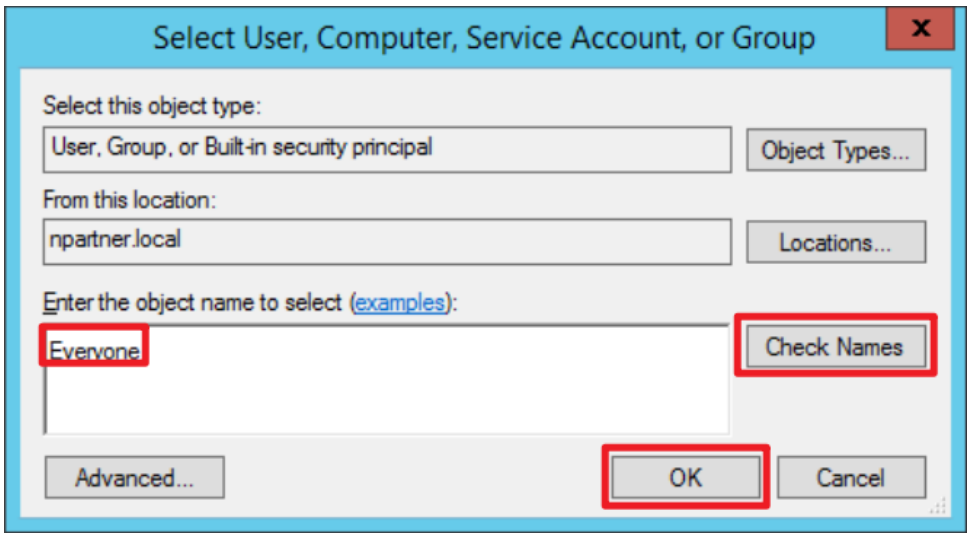
(3) Open the “Auditing” tab → click “Add.”



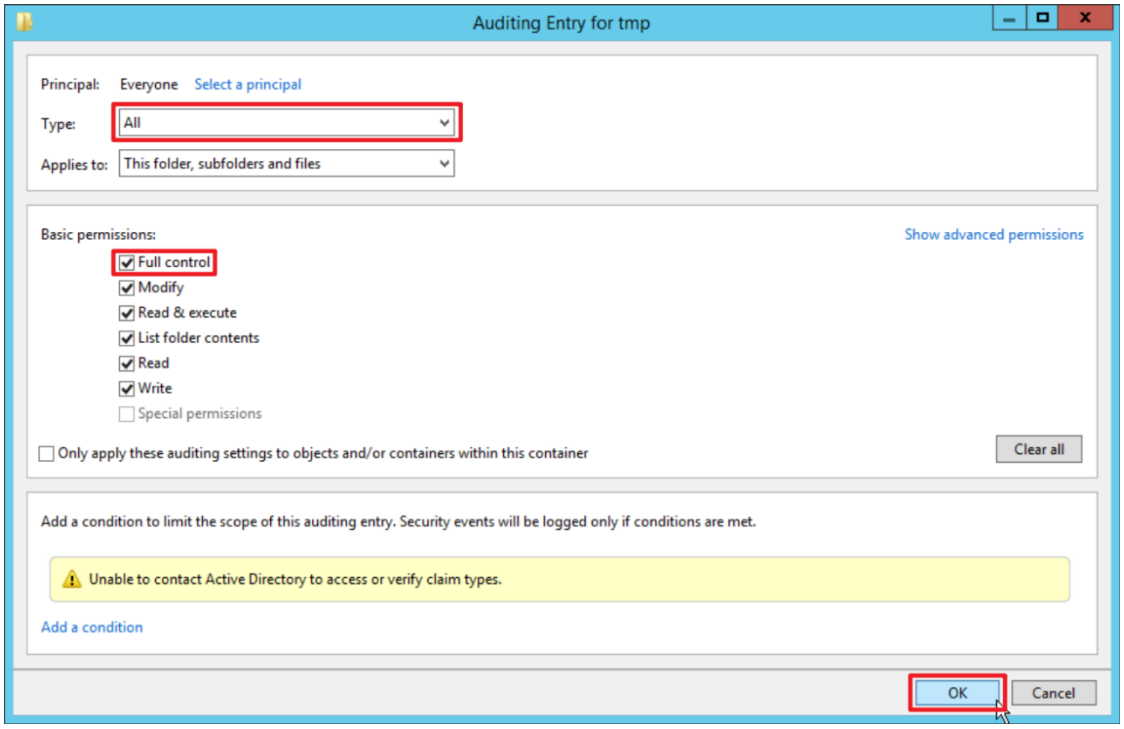
(4) Click “Select a principal.”



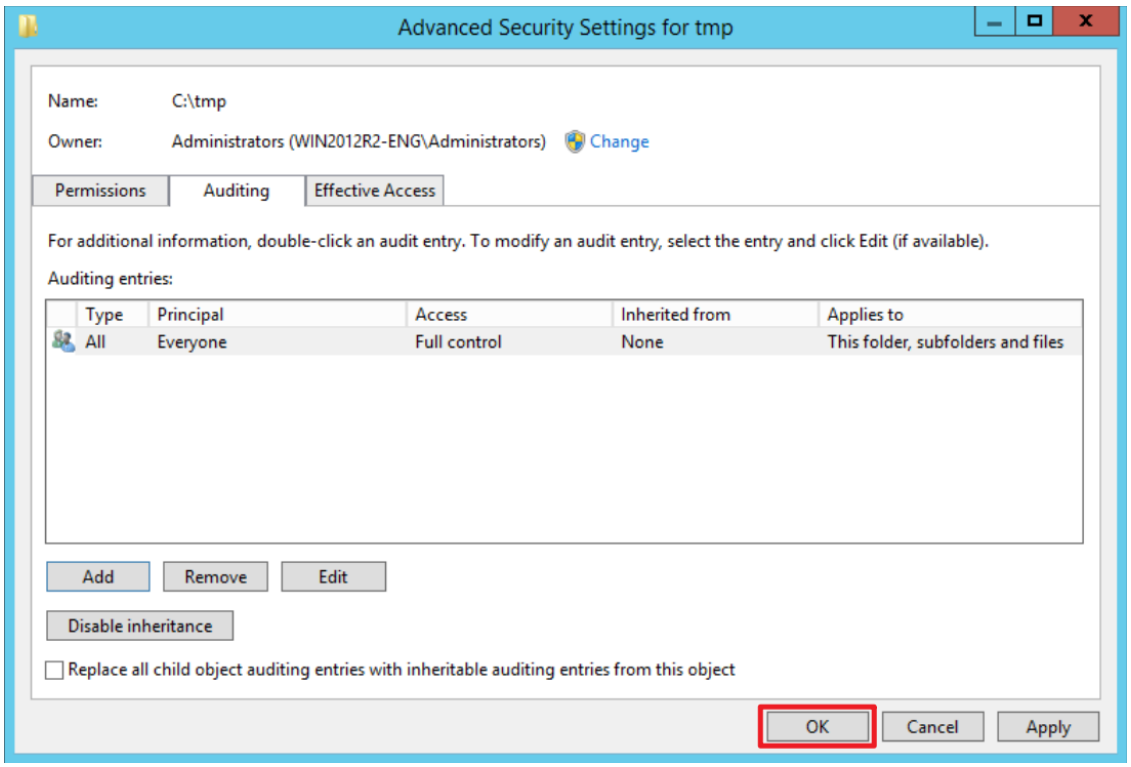
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



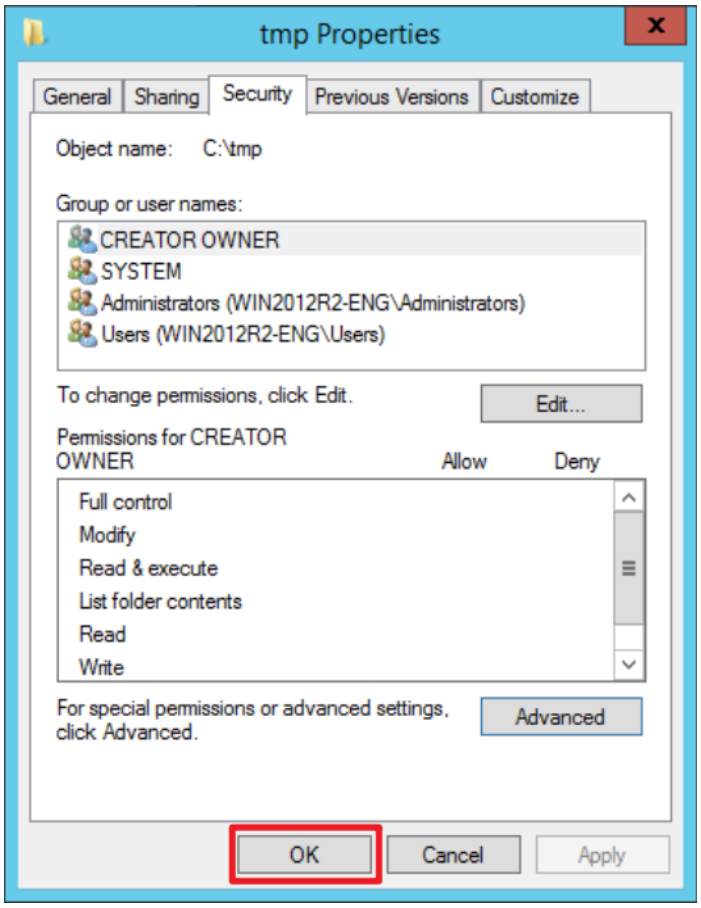
(6) Select “All” in type → enable “Full Control” → click “OK.”



(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

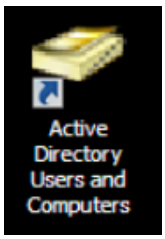
Windows Audit Policy Configuration:

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.

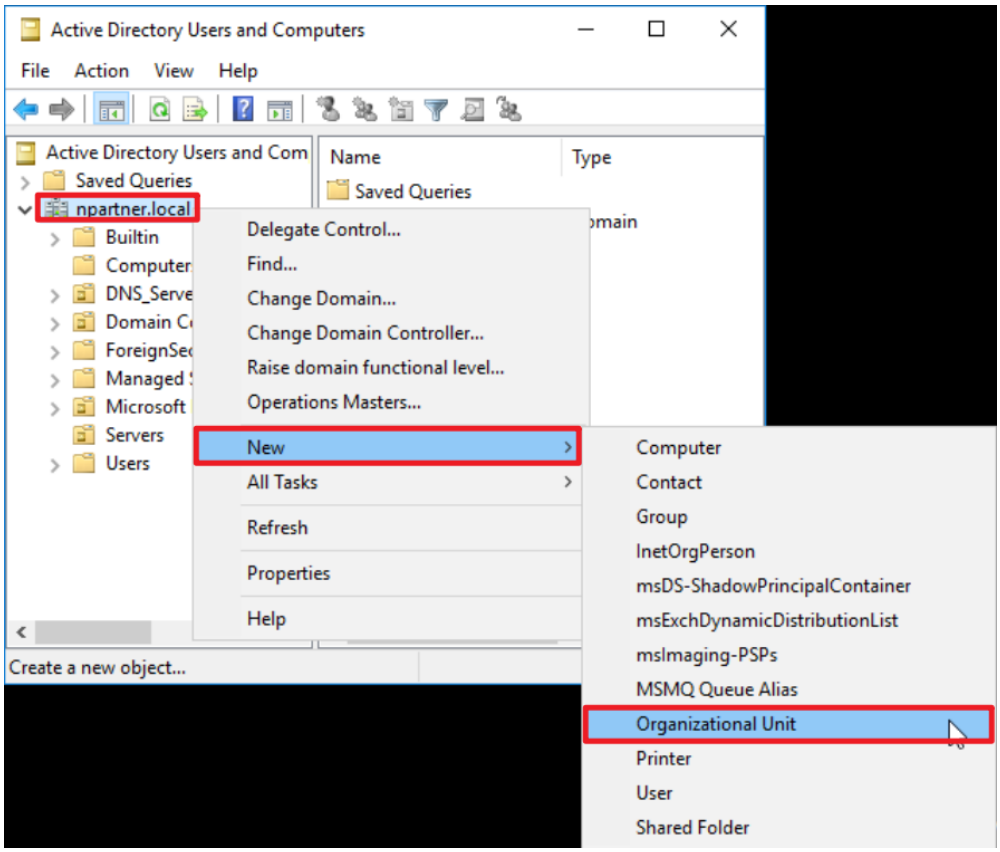
6.1.1 Organizational Unit (OU) Configuration

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



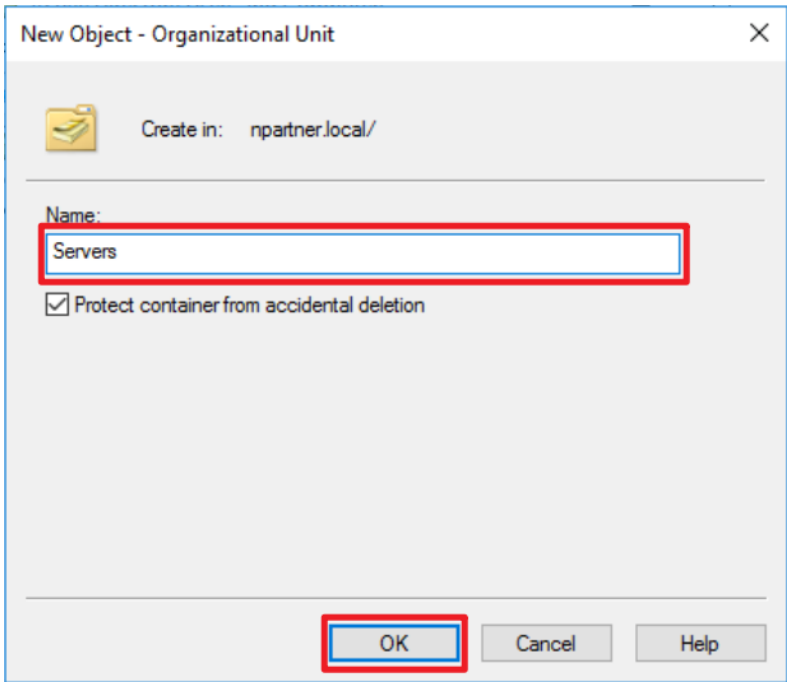
(2) Add an Organizational Unit

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”)

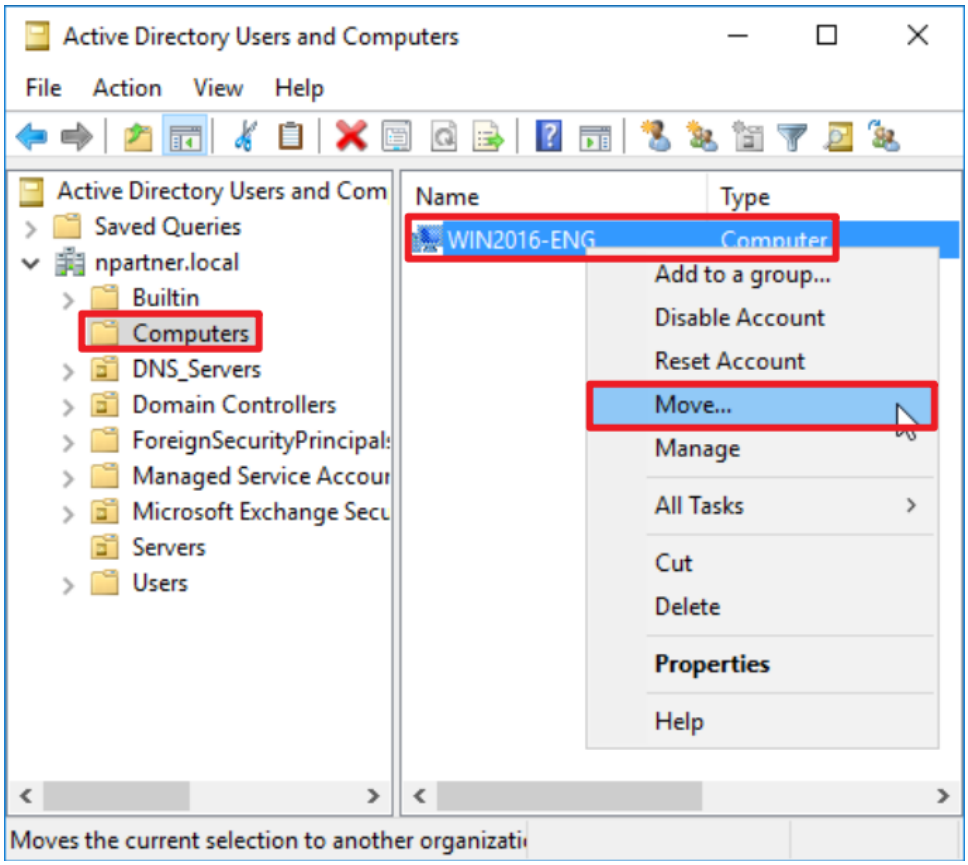
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

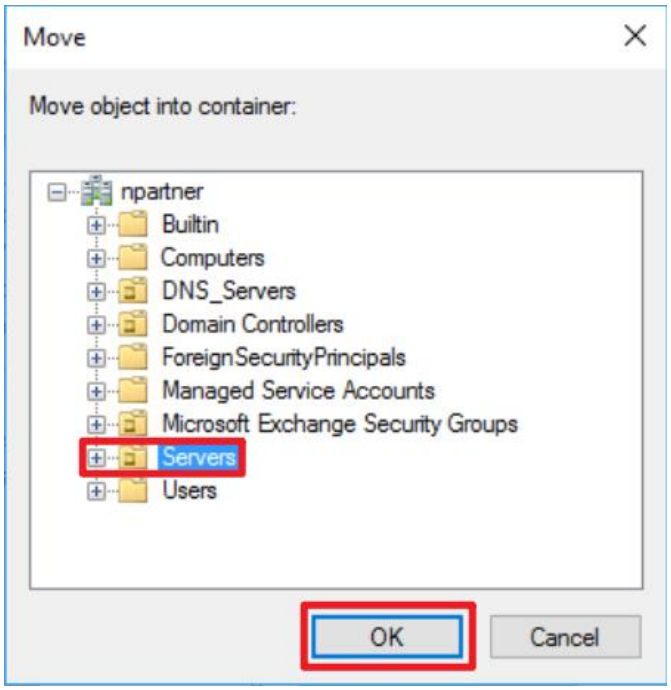
Select “Computers” organizational unit (OU) → right-click on the “WIN2016” server.

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



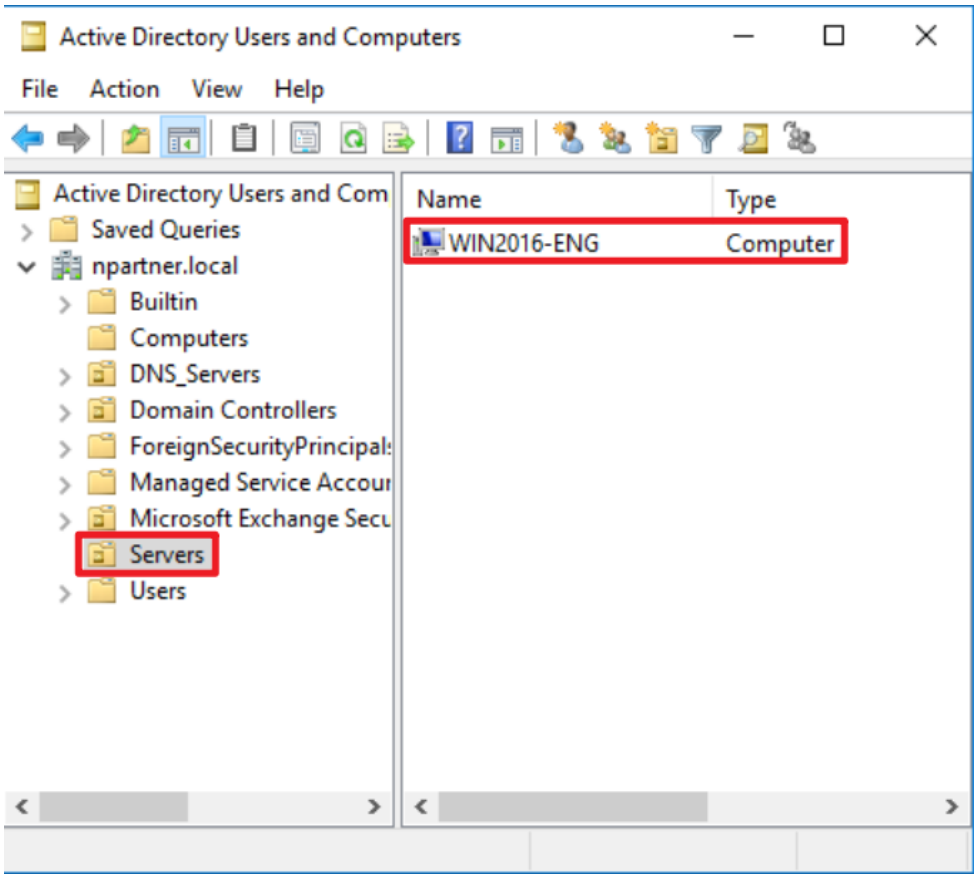
(5) Select your Organizational Unit:

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.

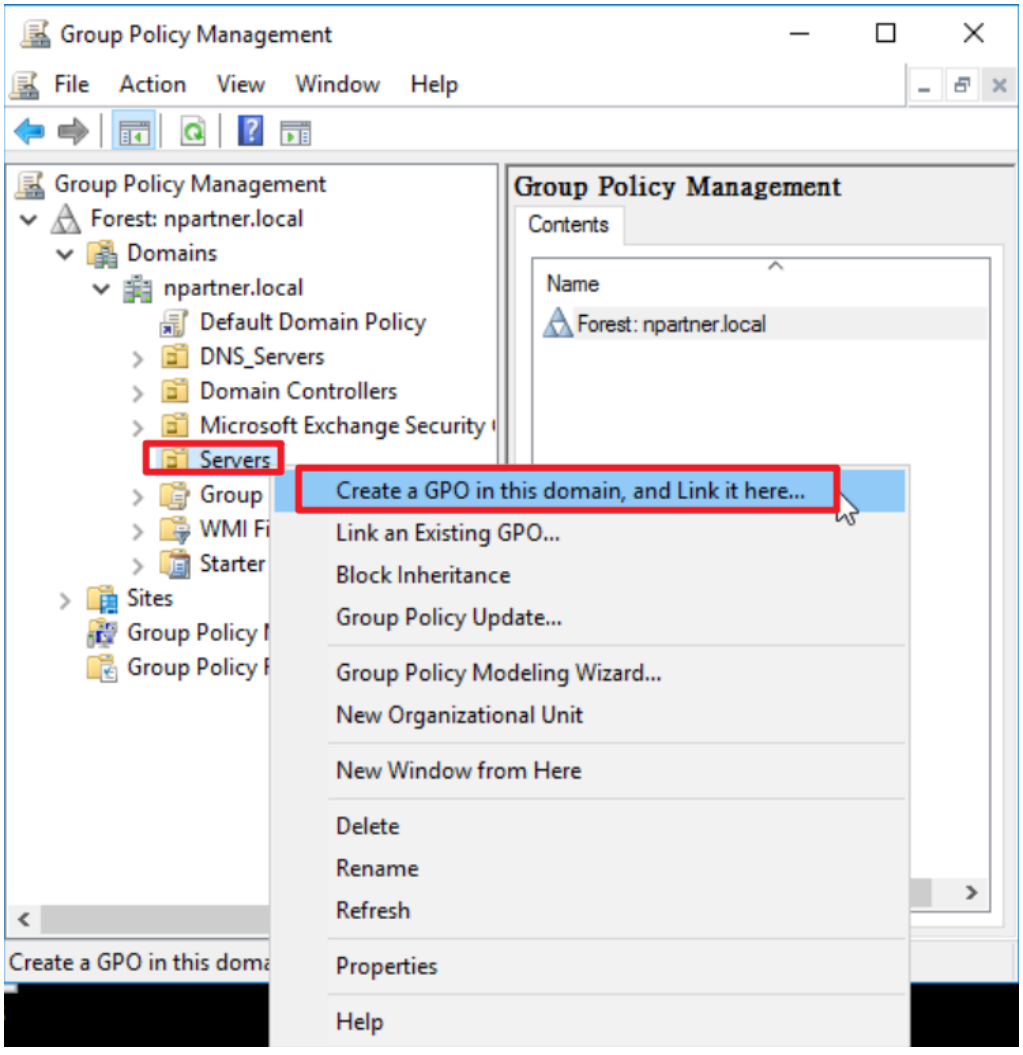


6.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

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

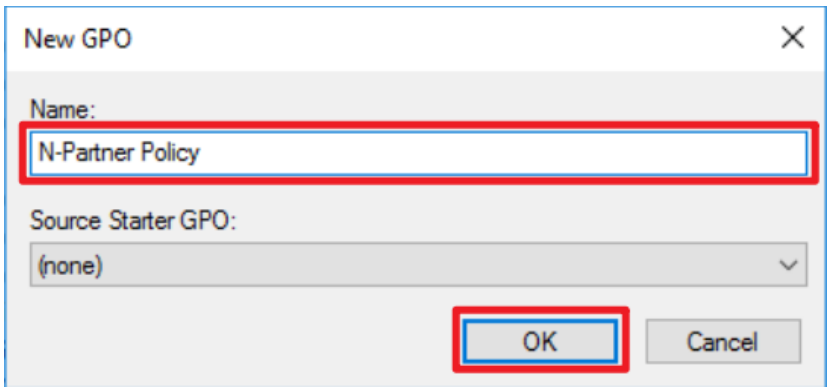
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

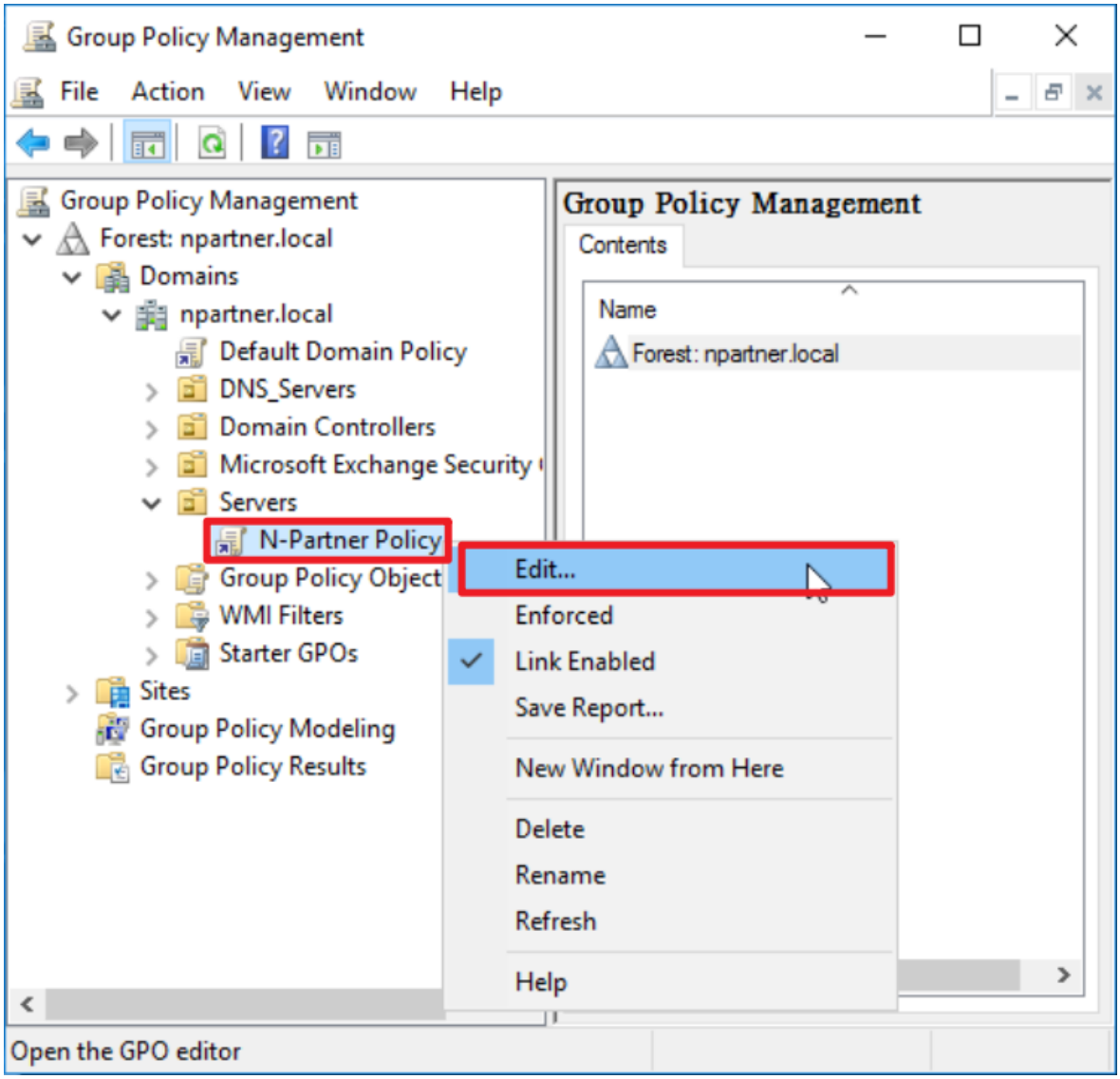
Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

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



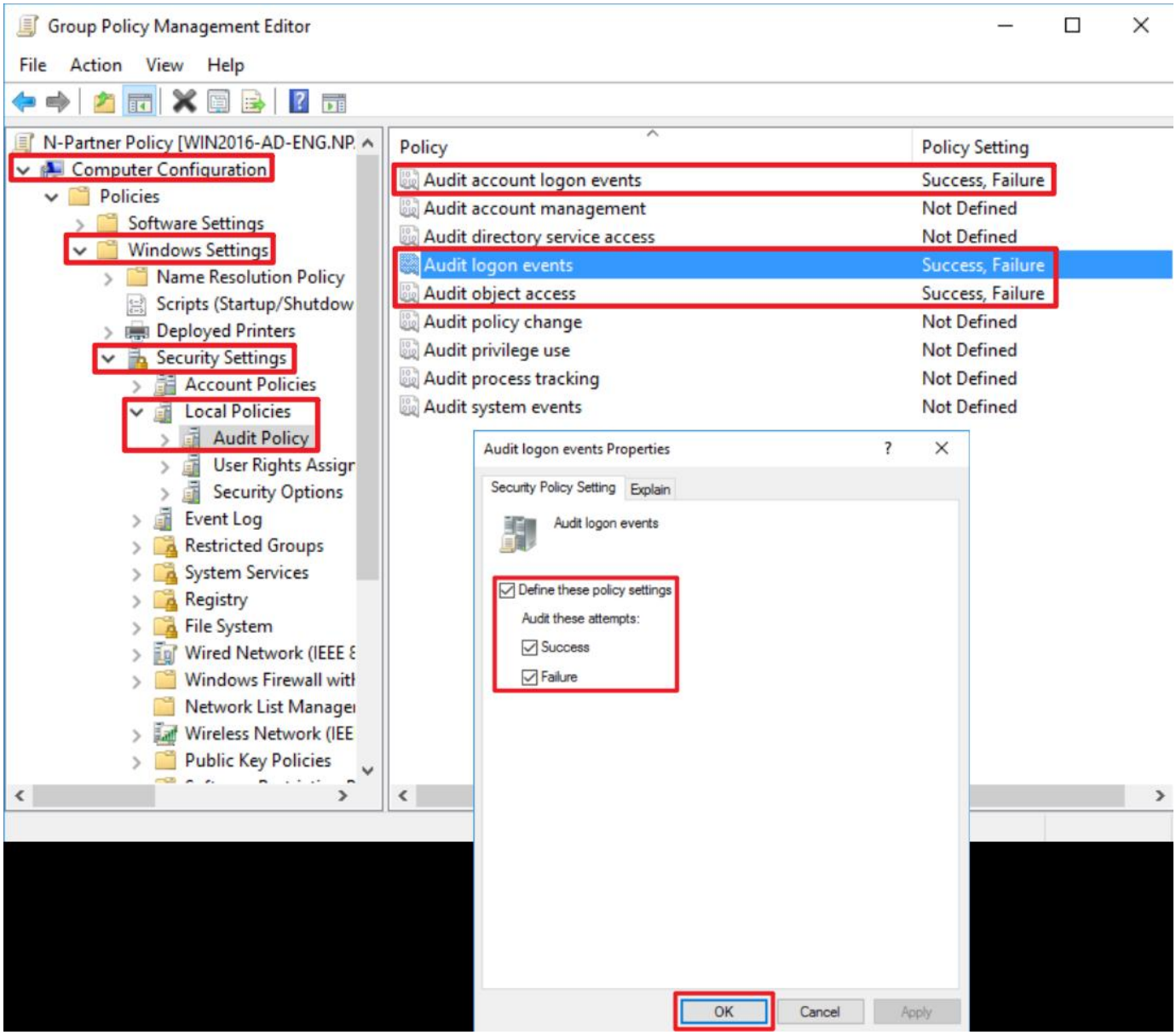
(4) Edit your Group Policy Object

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



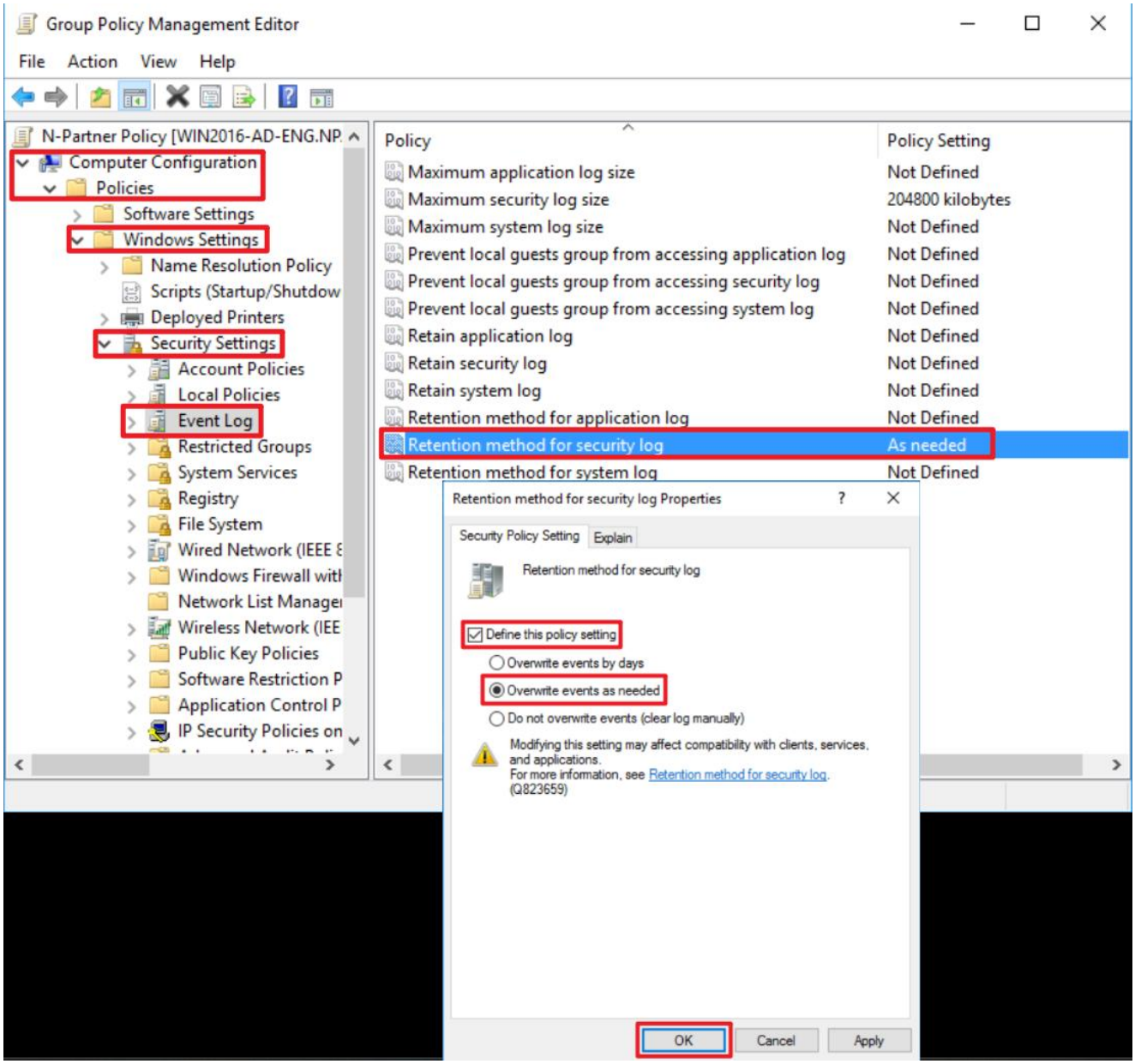
(5) Local Group Policies: Audit Policy

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

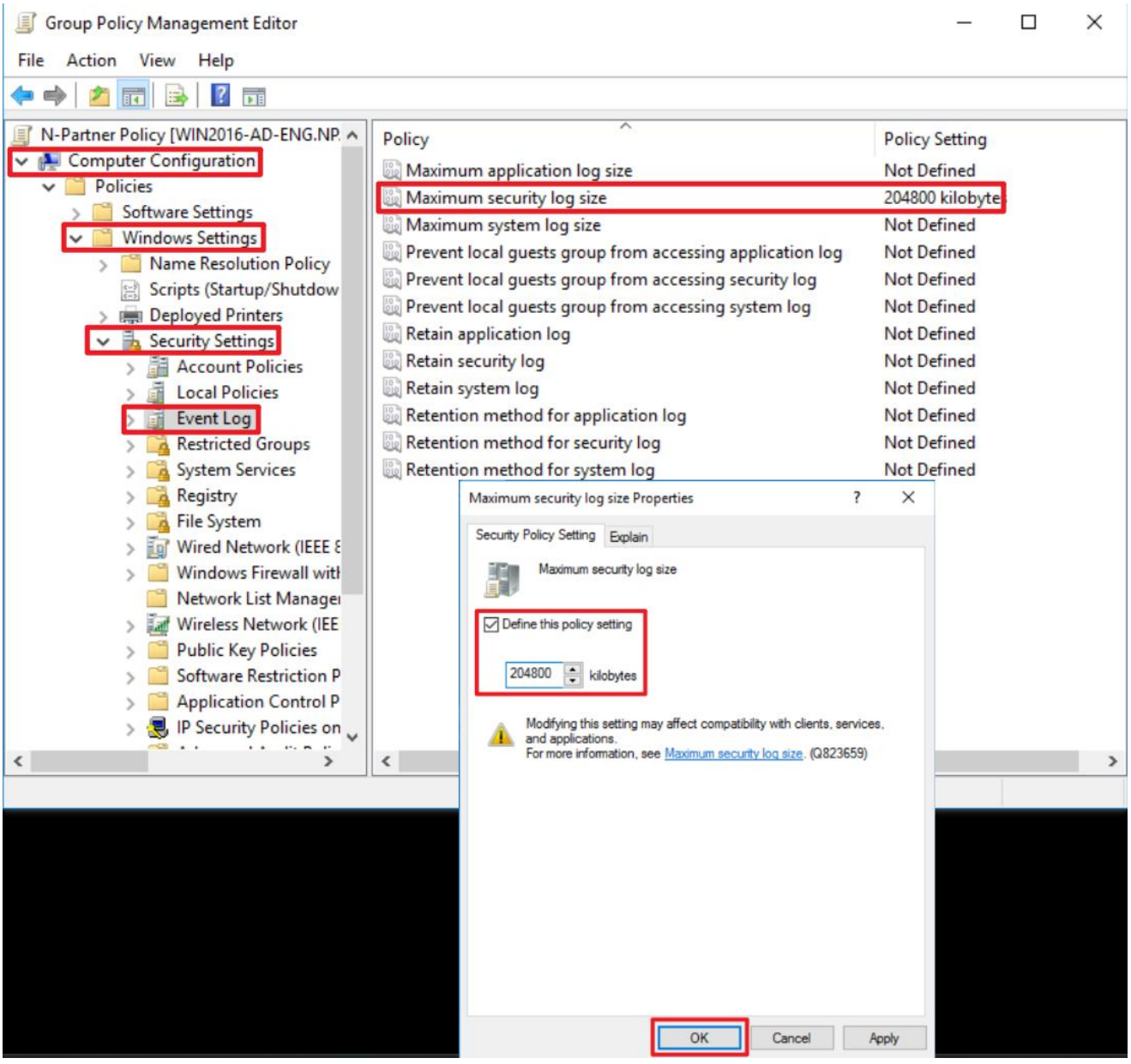
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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

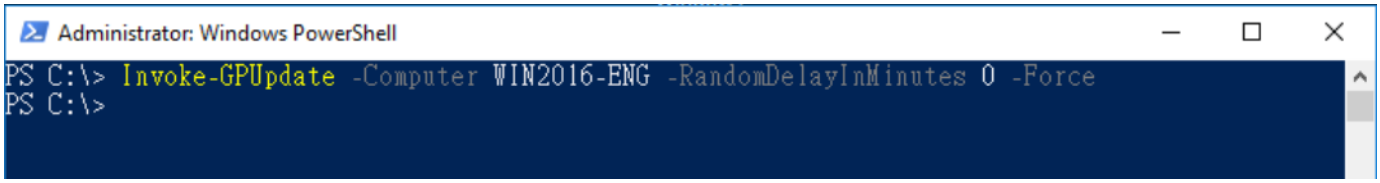
Note: Please adjust the number based on the actual environment. → click “OK.”



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

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

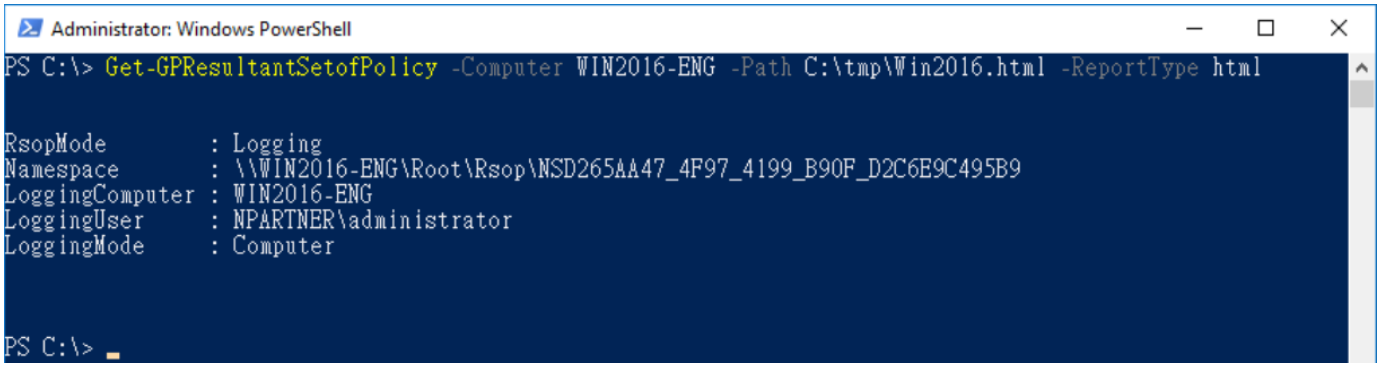
```
PS C:\> Invoke-GPUpdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
```



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

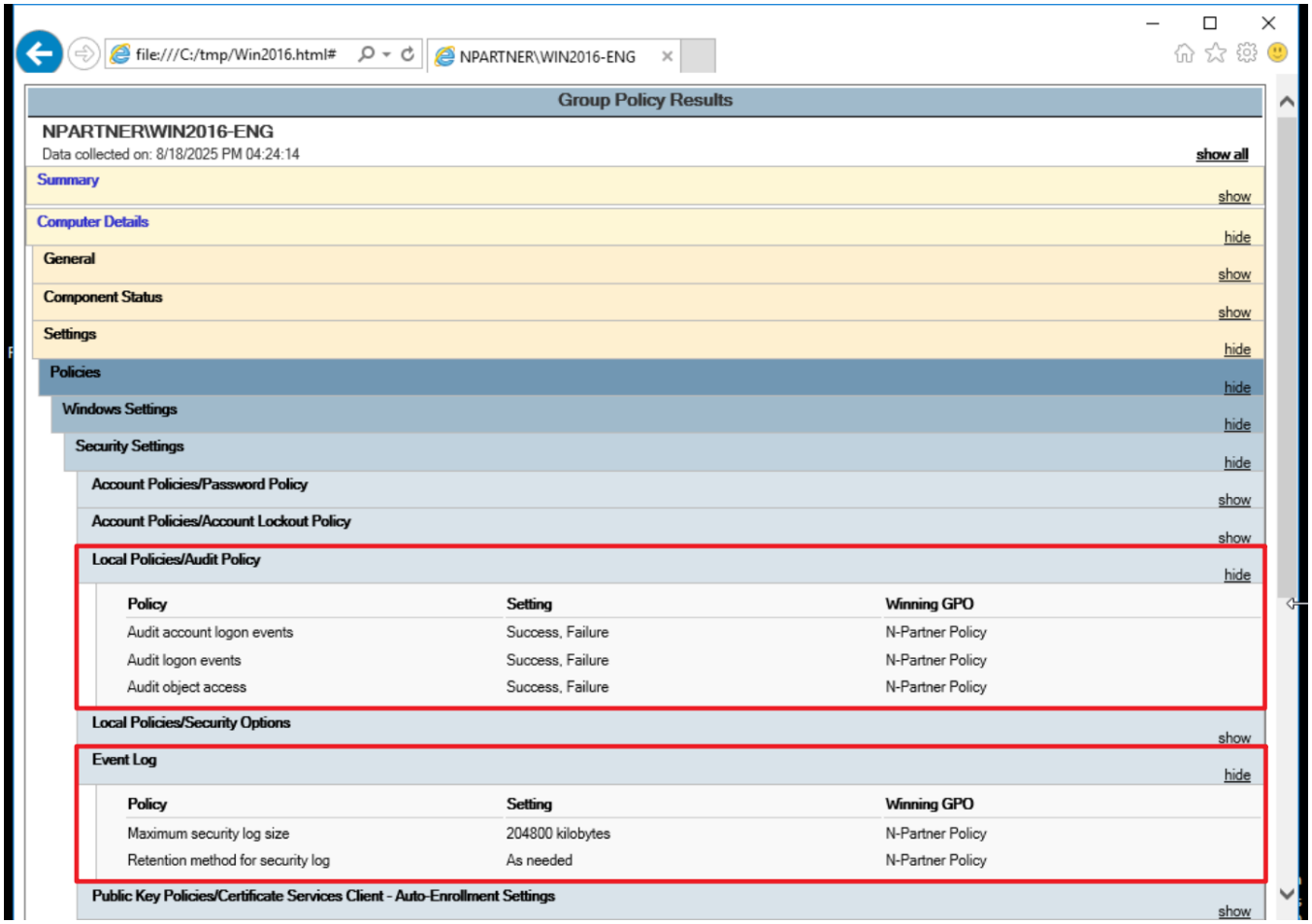
(10) Enter the command below to generate server group policy report.

```
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.

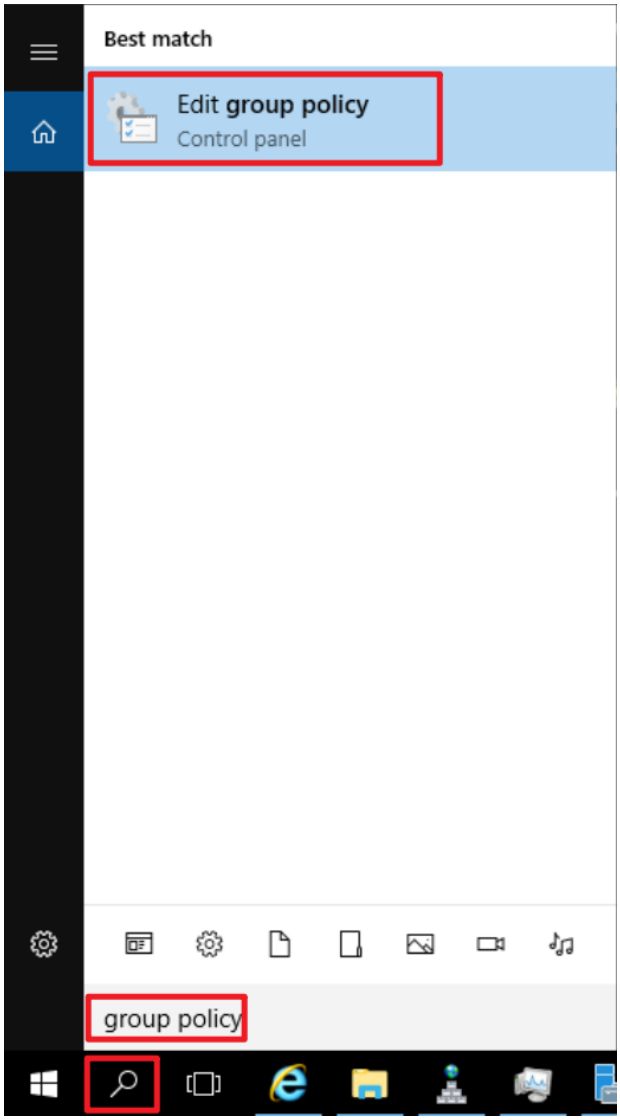


6.2 Workgroup

6.2.1 Audit Policy Configuration

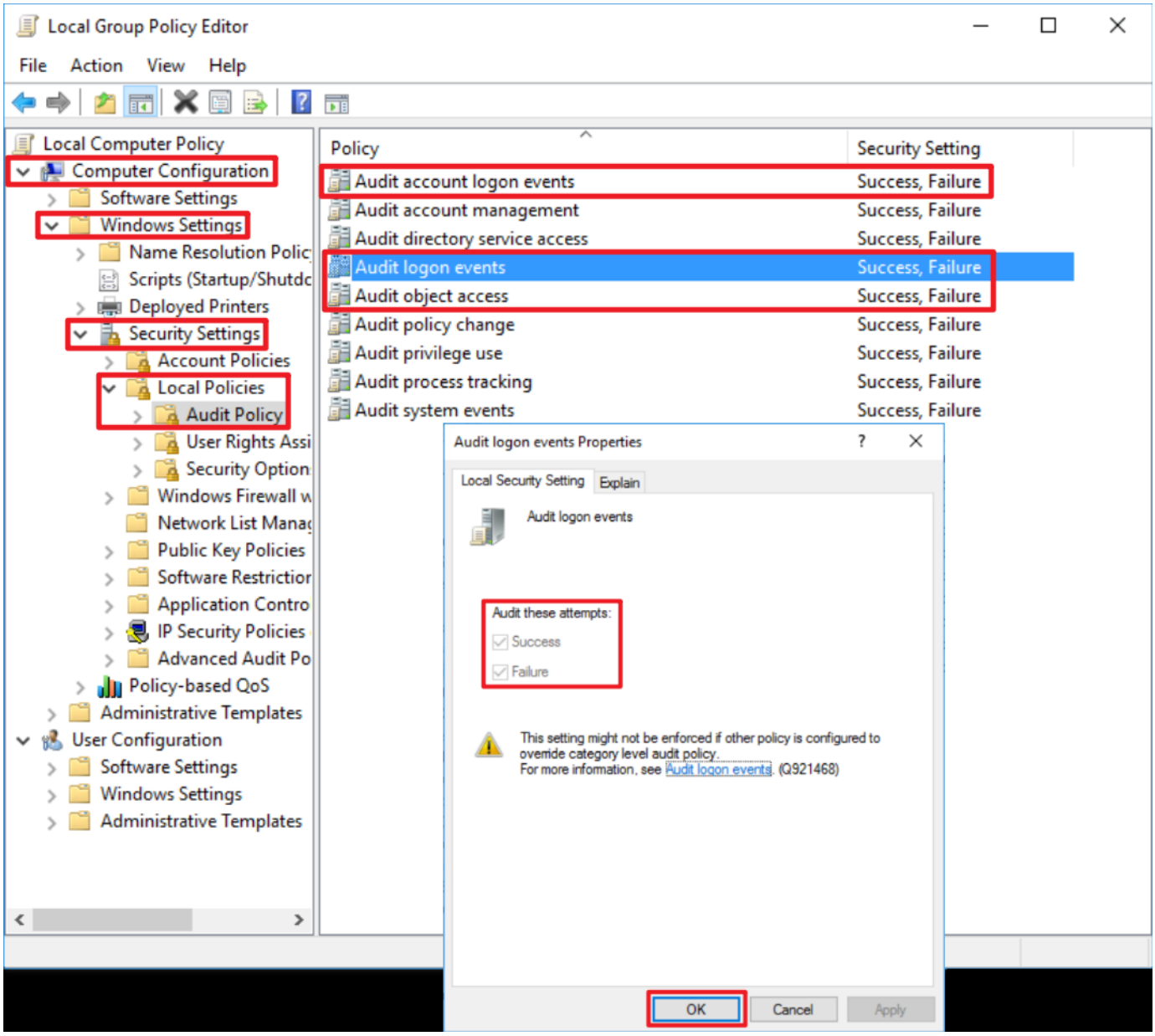
(1) Open Local Group Policy Editor

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



(2) Local Group Policies: Audit Policy

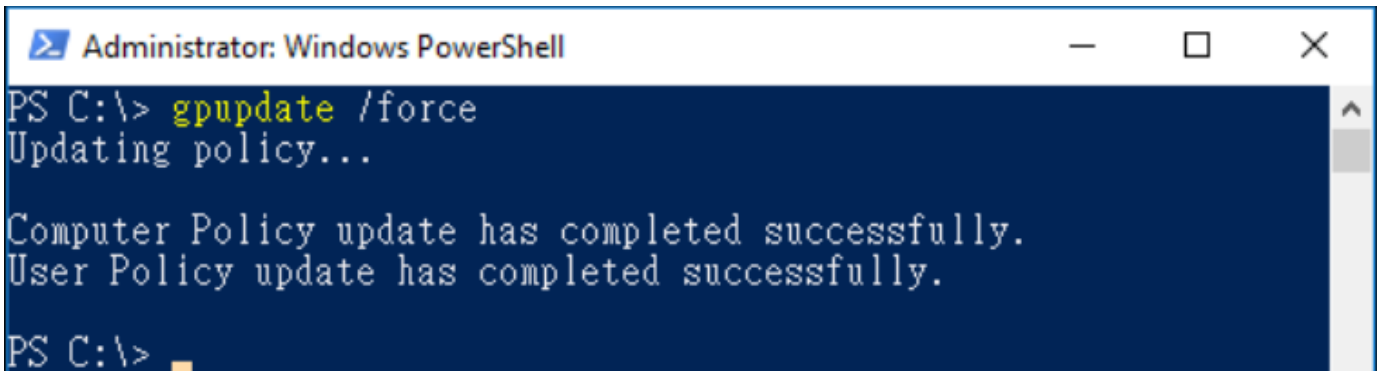
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”

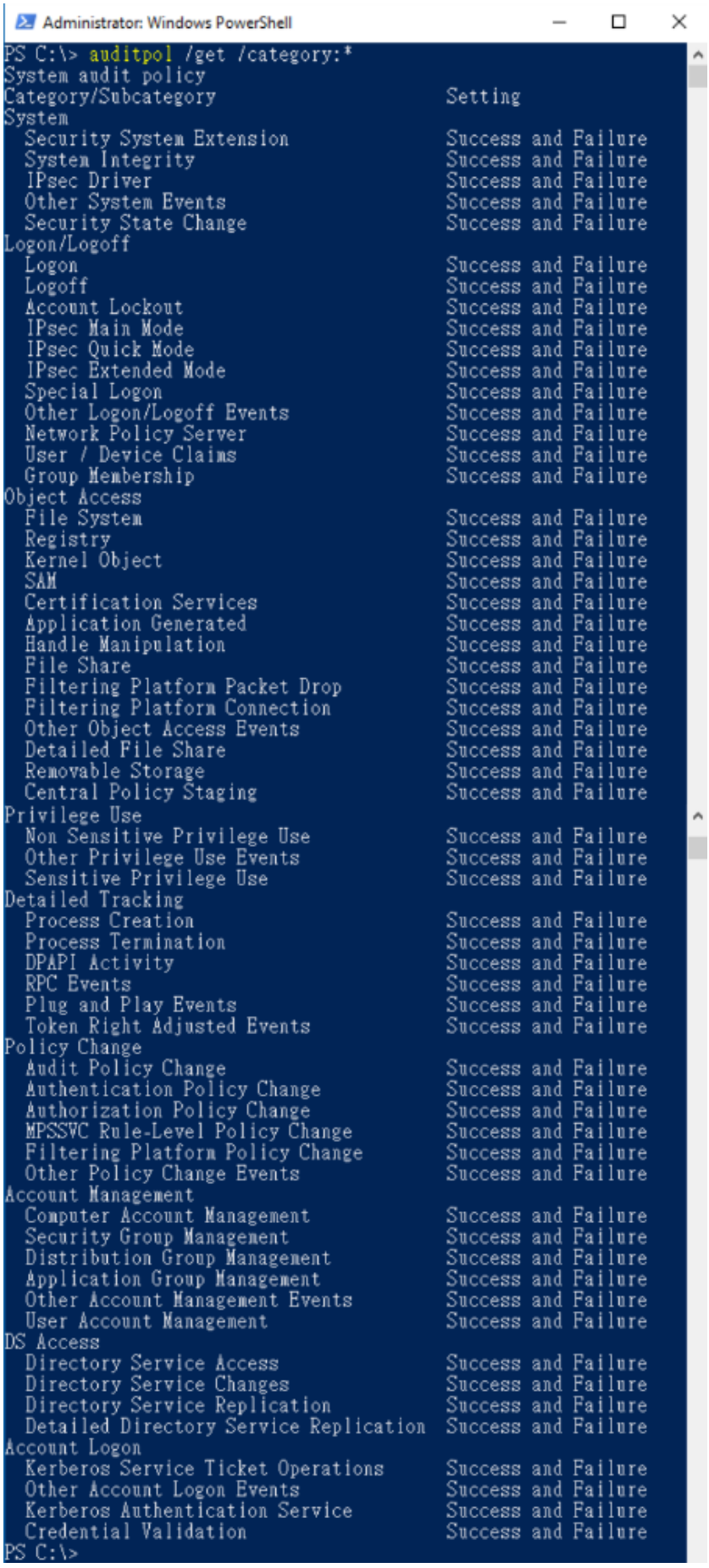
(4) Enter the command below to refresh group policy.

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



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

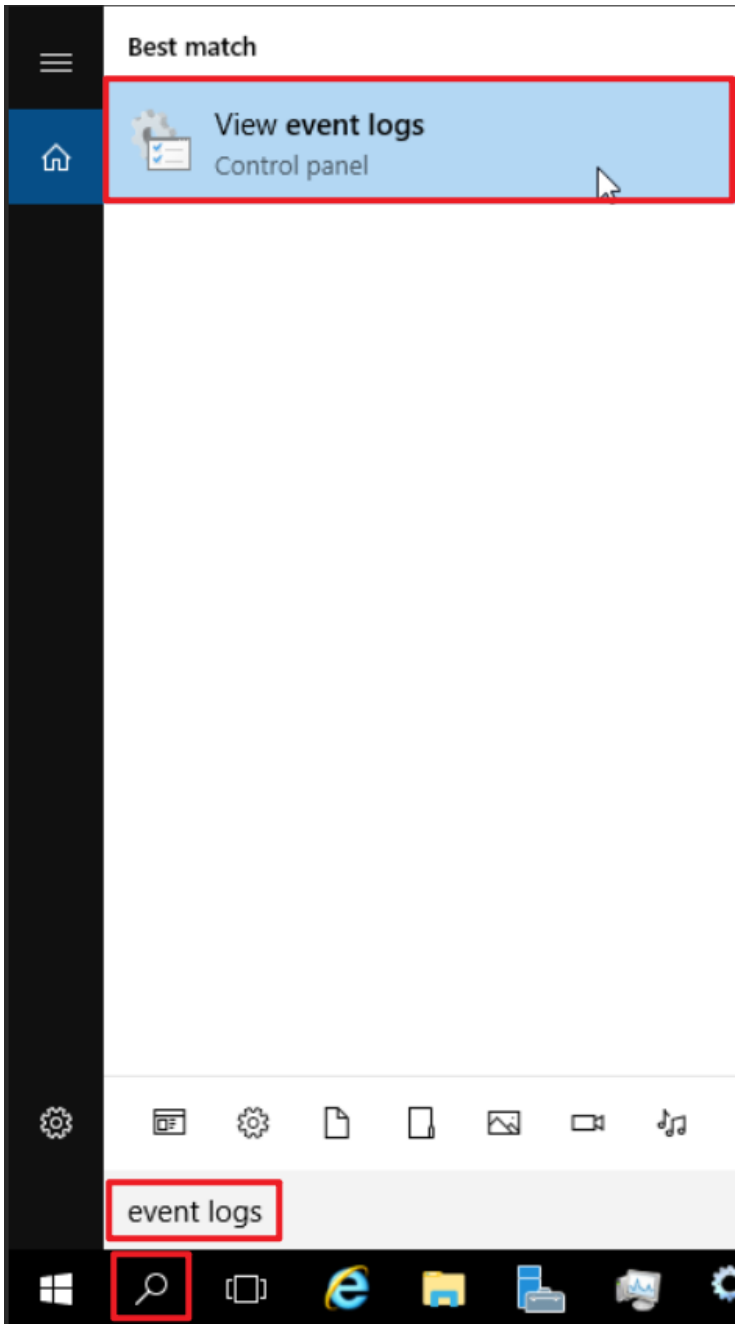
```
PS C: \> auditpol /get /category:*
```



6.2.2 Event Log Settings

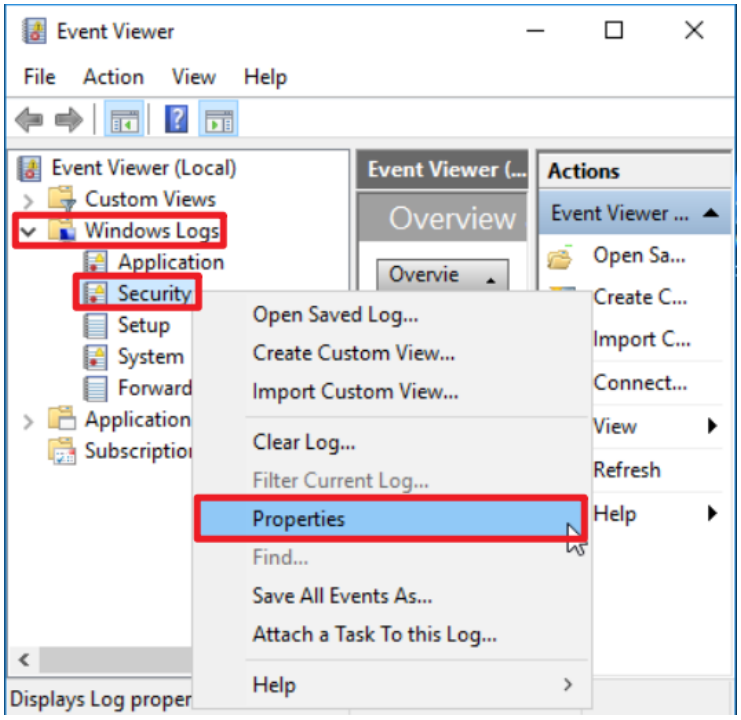
(1) Search for “Event Viewer”

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.”

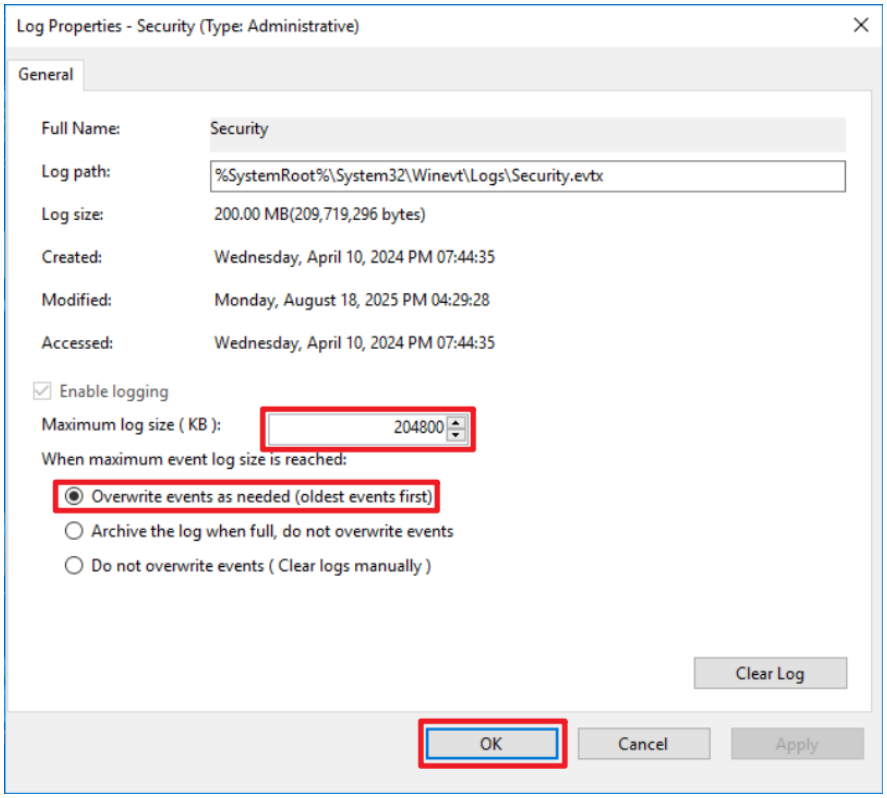


(3) Configure Security Log

Enter maximum log file size: 204800 KB

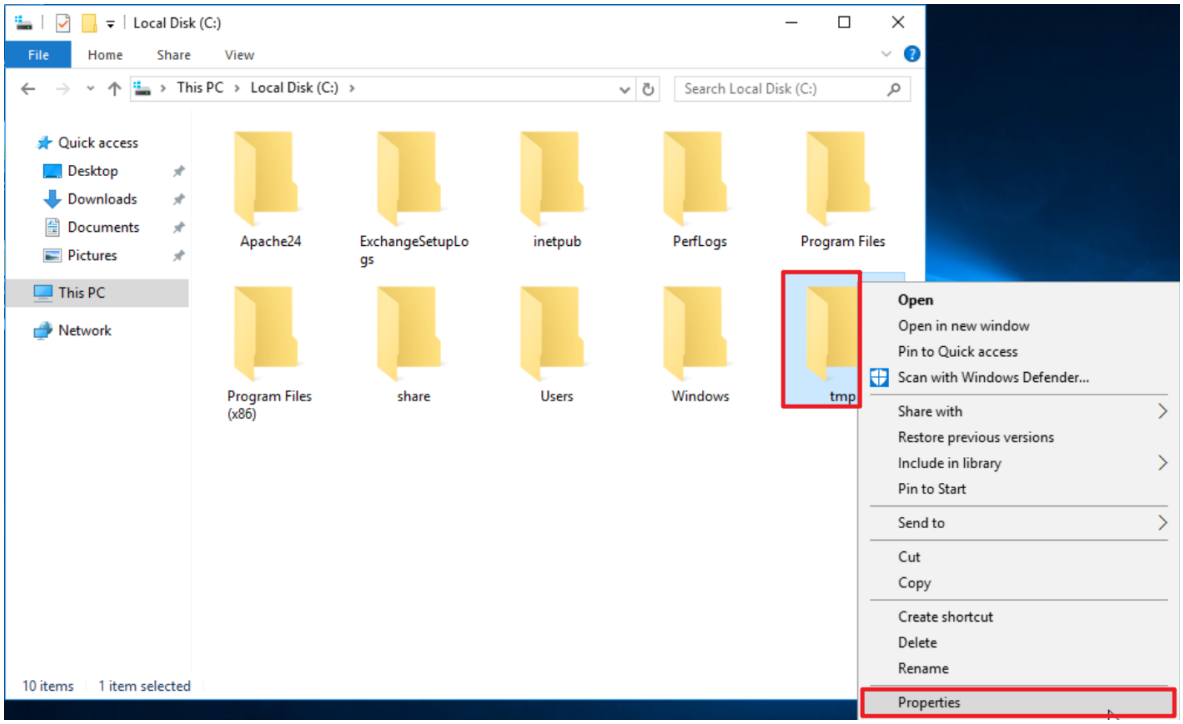
Note: Please adjust the number according to the actual environment.

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

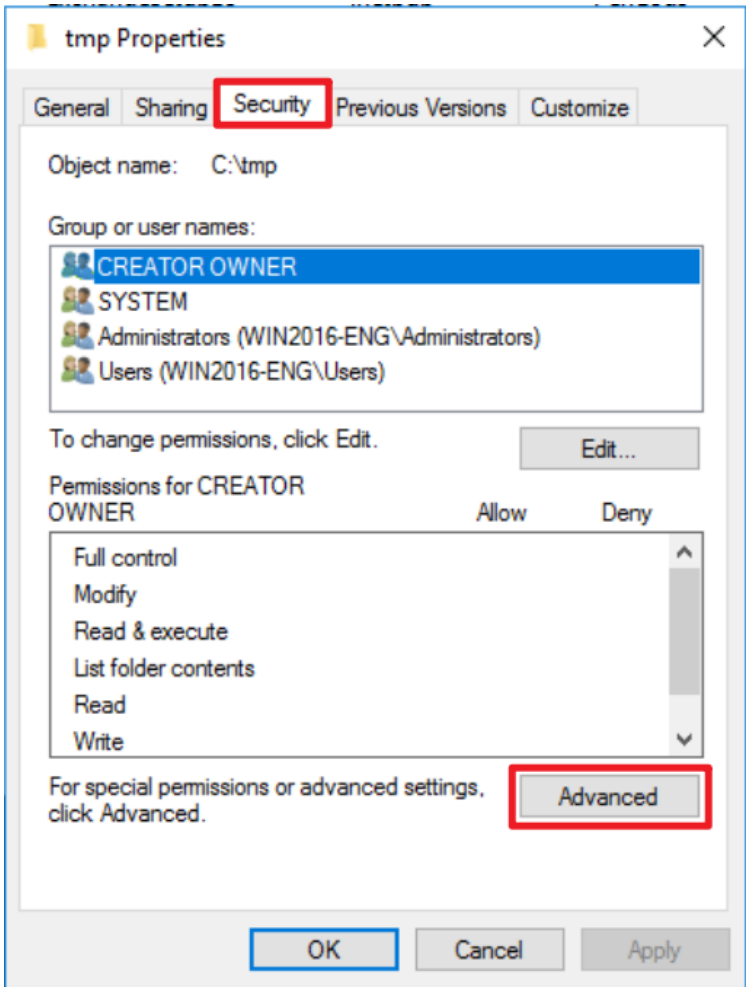


6.3 Folder Audit Configuration

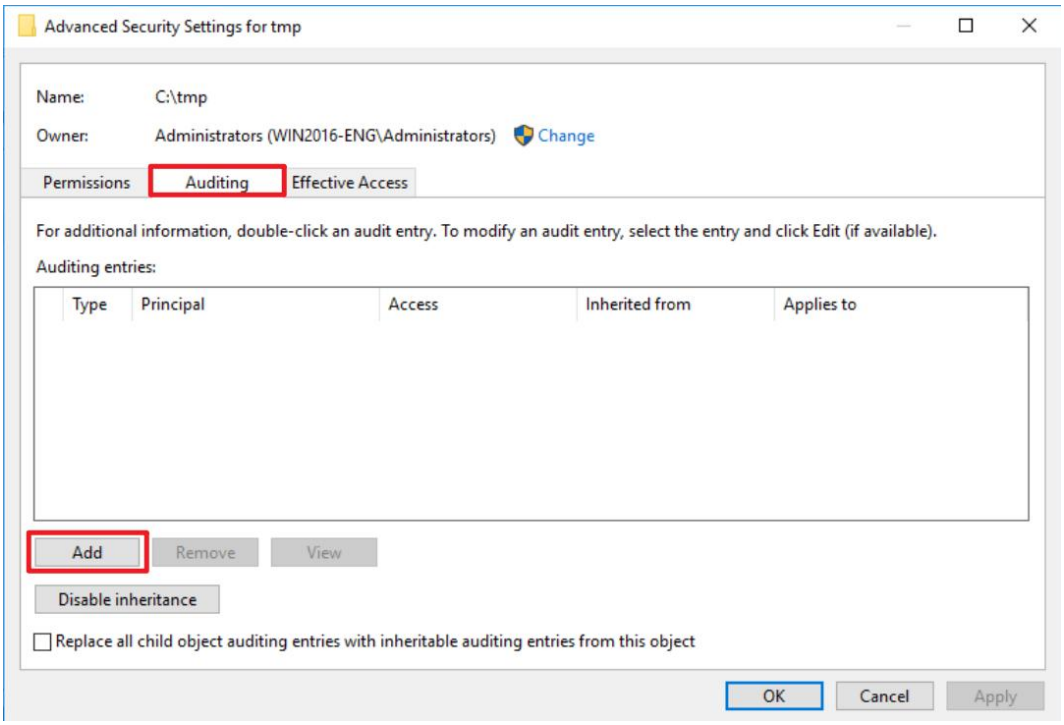
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



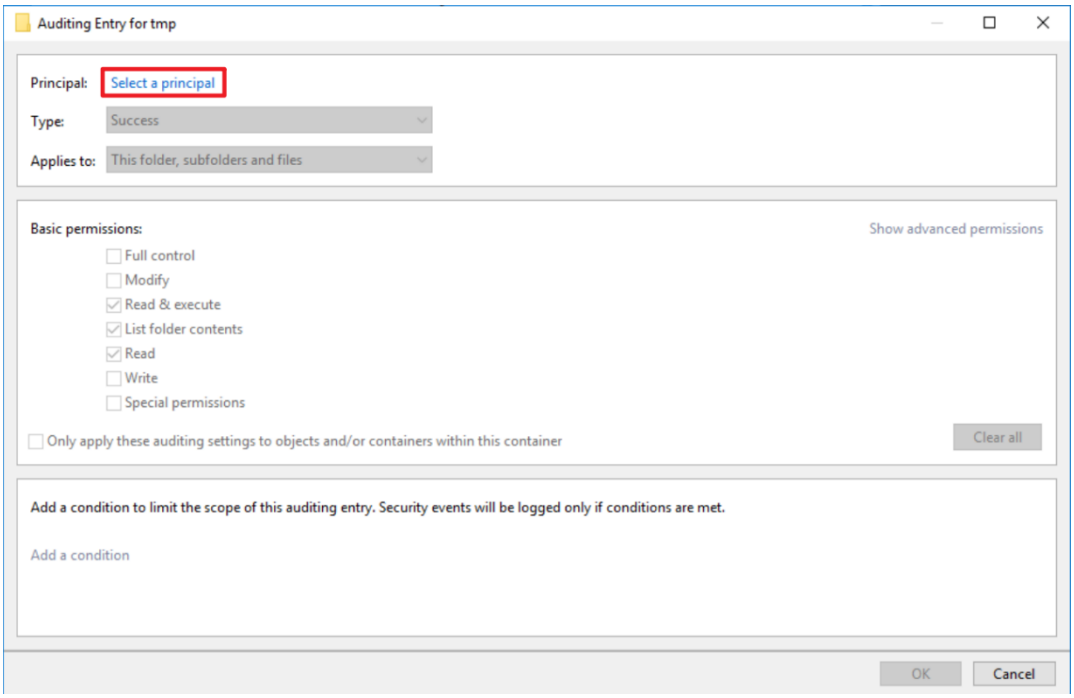
(2) Go to the “Security” tab → click “Advanced.”



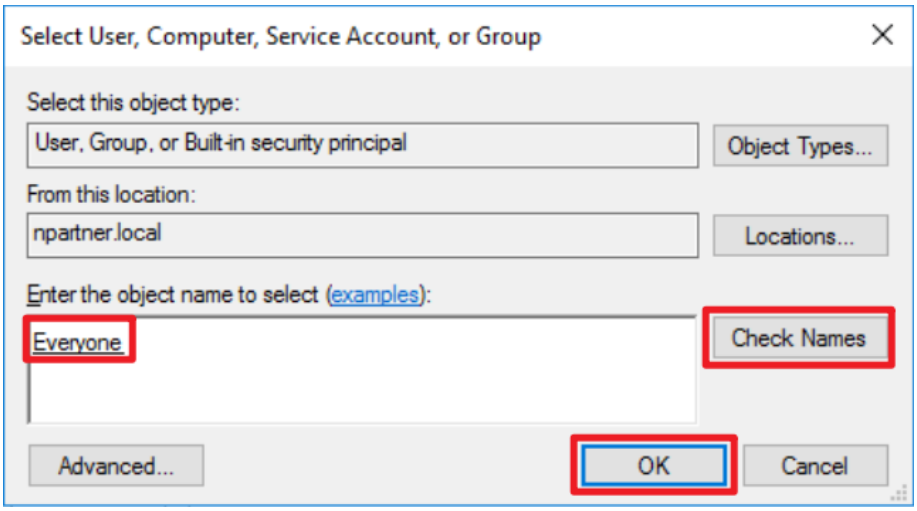
(3) Open the “Auditing” tab → click “Add.”



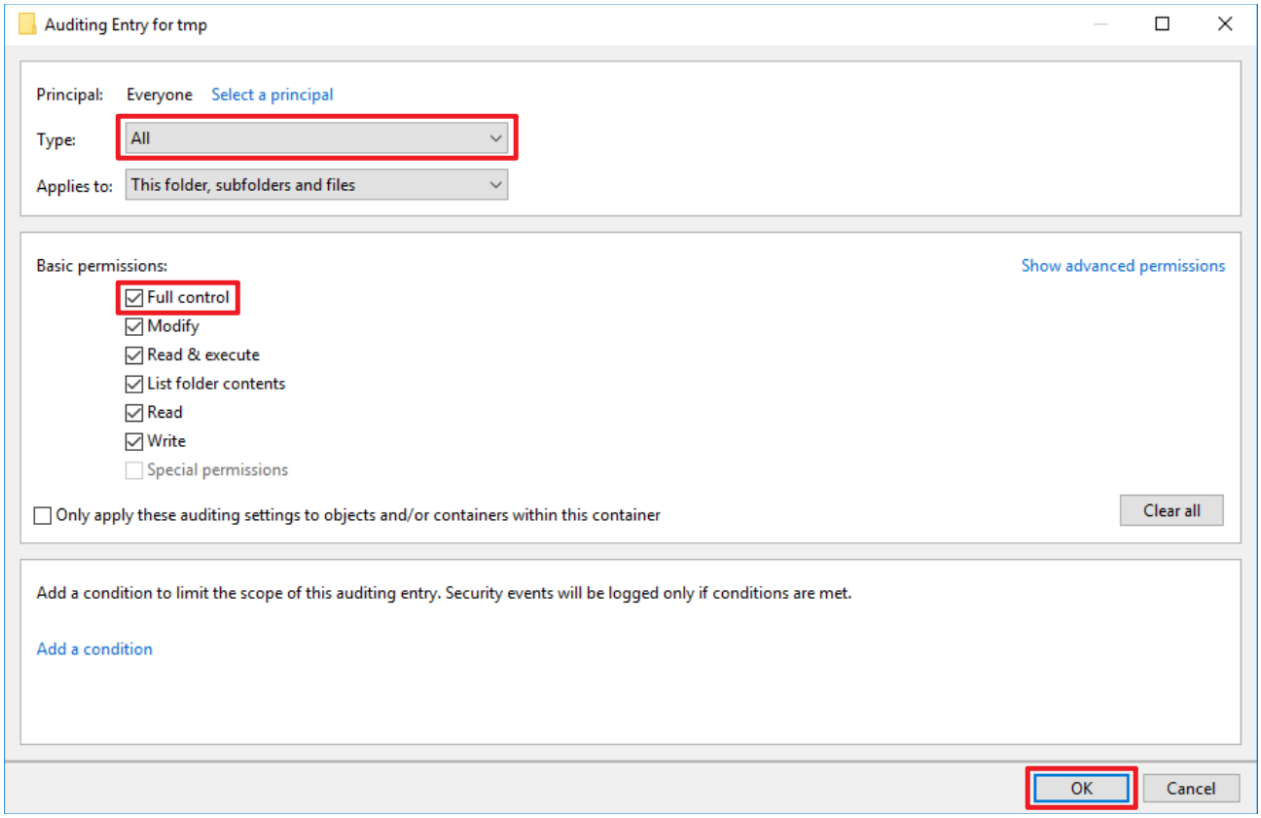
(4) Click “Select a principal.”



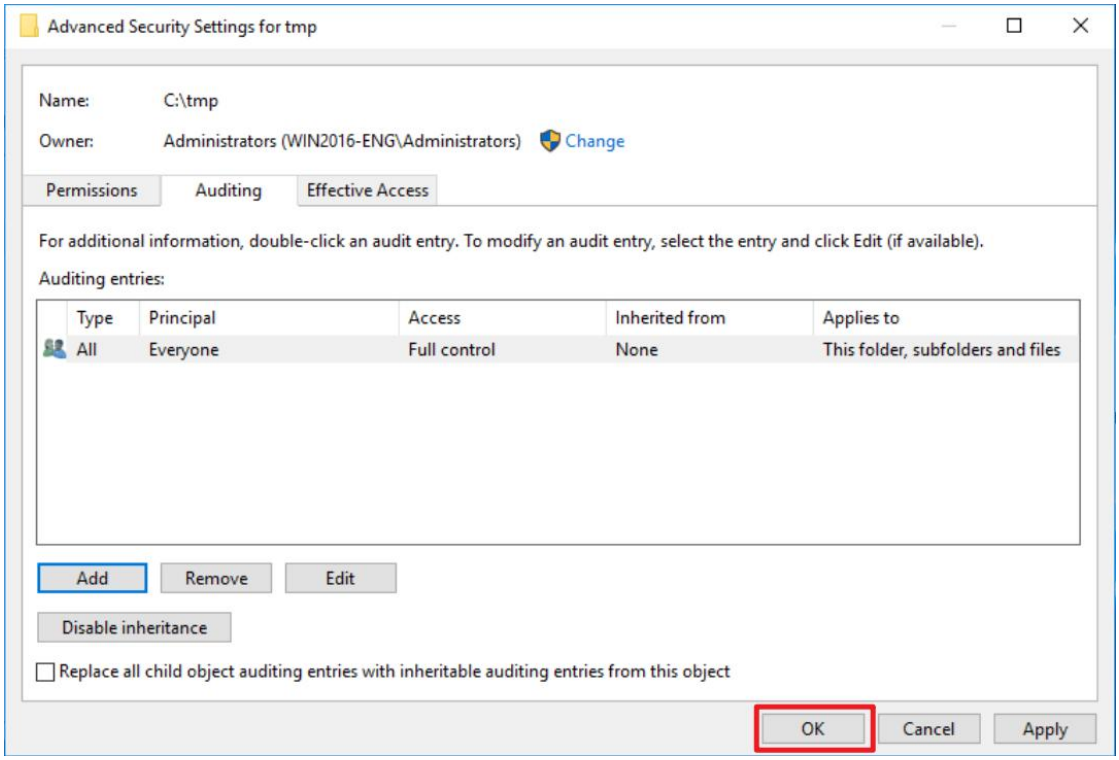
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



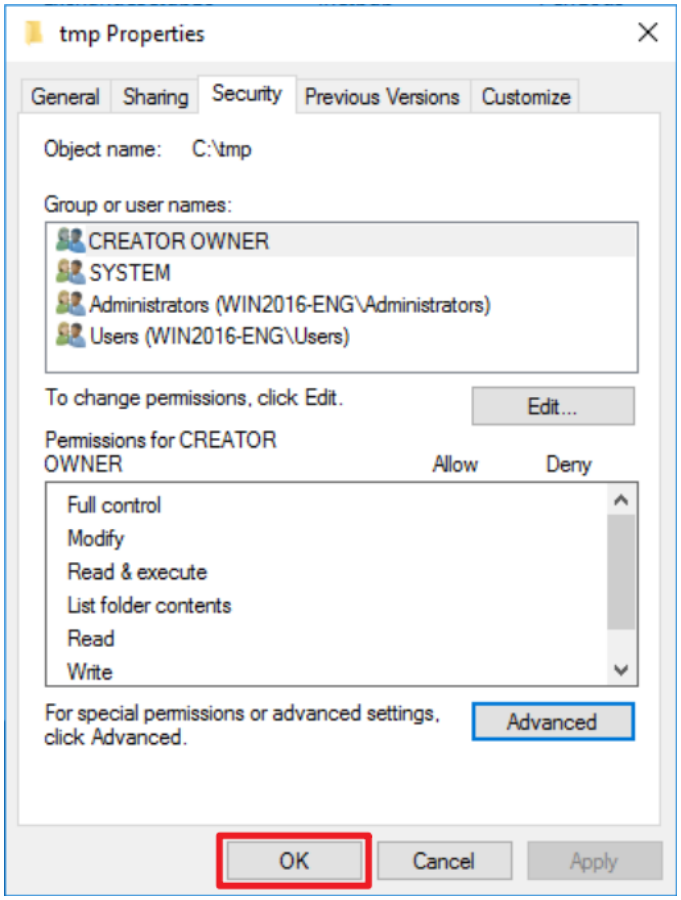
(6) Select “All” in type → enable “Full Control” → click “OK.”



(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.

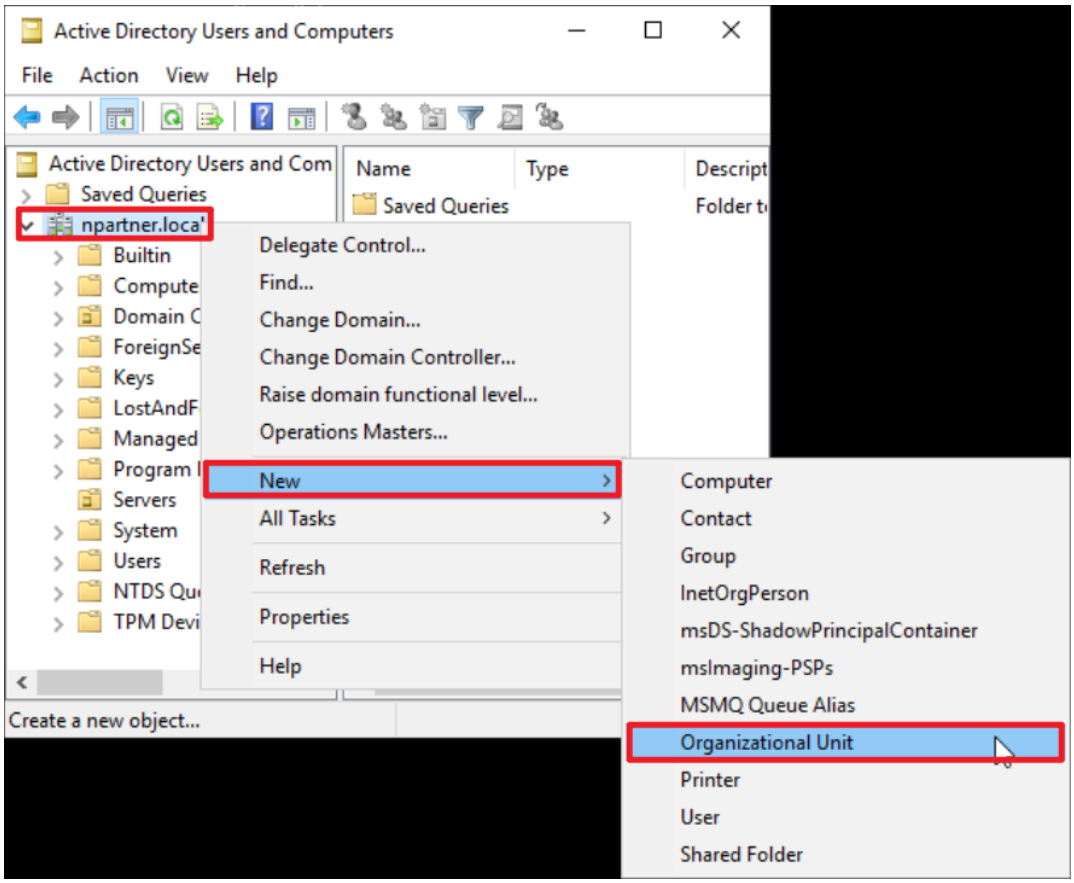
The following sections describe the configuration methods for Domain and Workgroup environments.

7.1.1 Organizational Unit (OU) Configuration

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

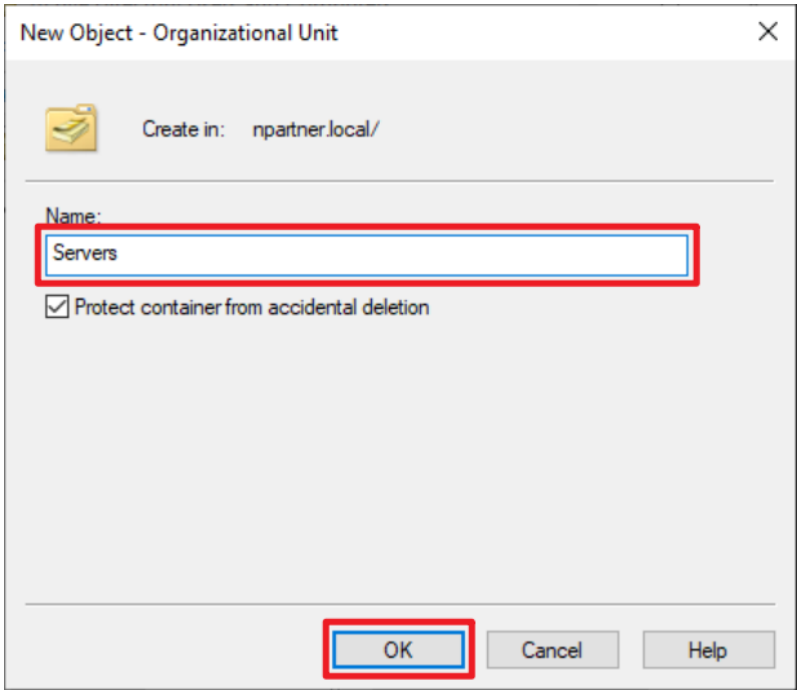
(2) Add an Organizational Unit

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



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

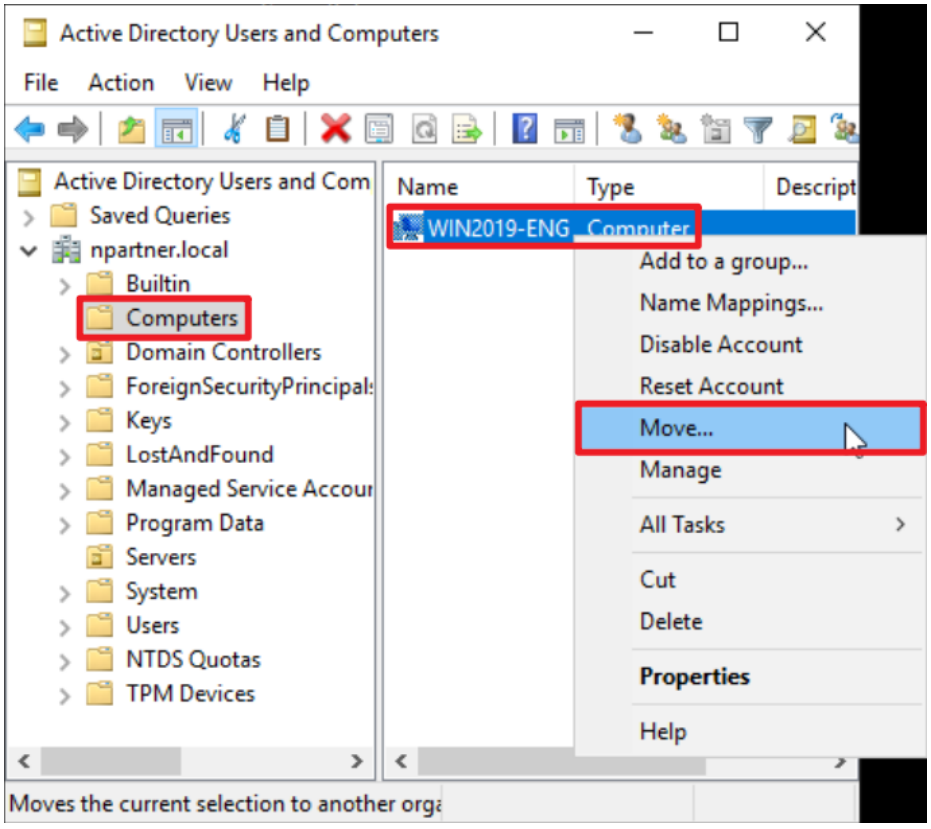
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

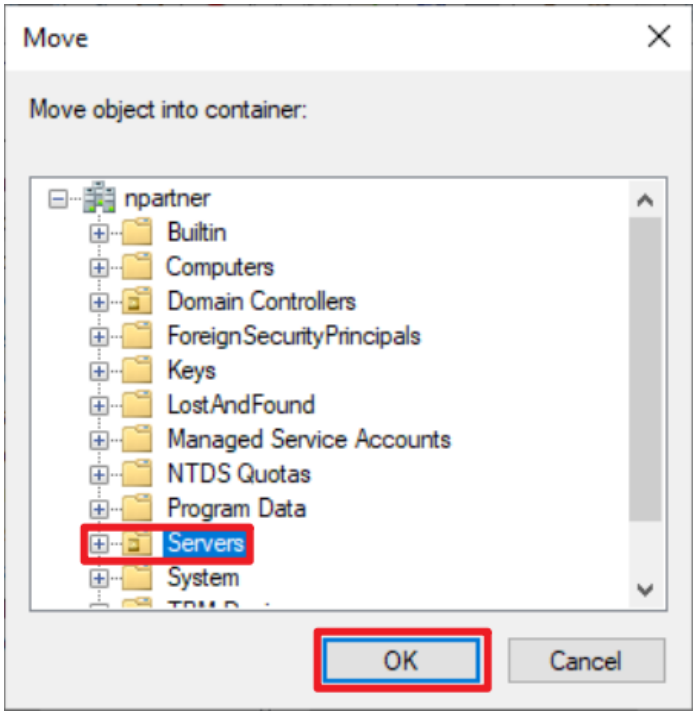
Select the “Computers” organizational unit (OU) → right-click on the “WIN2019-ENG” server.

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



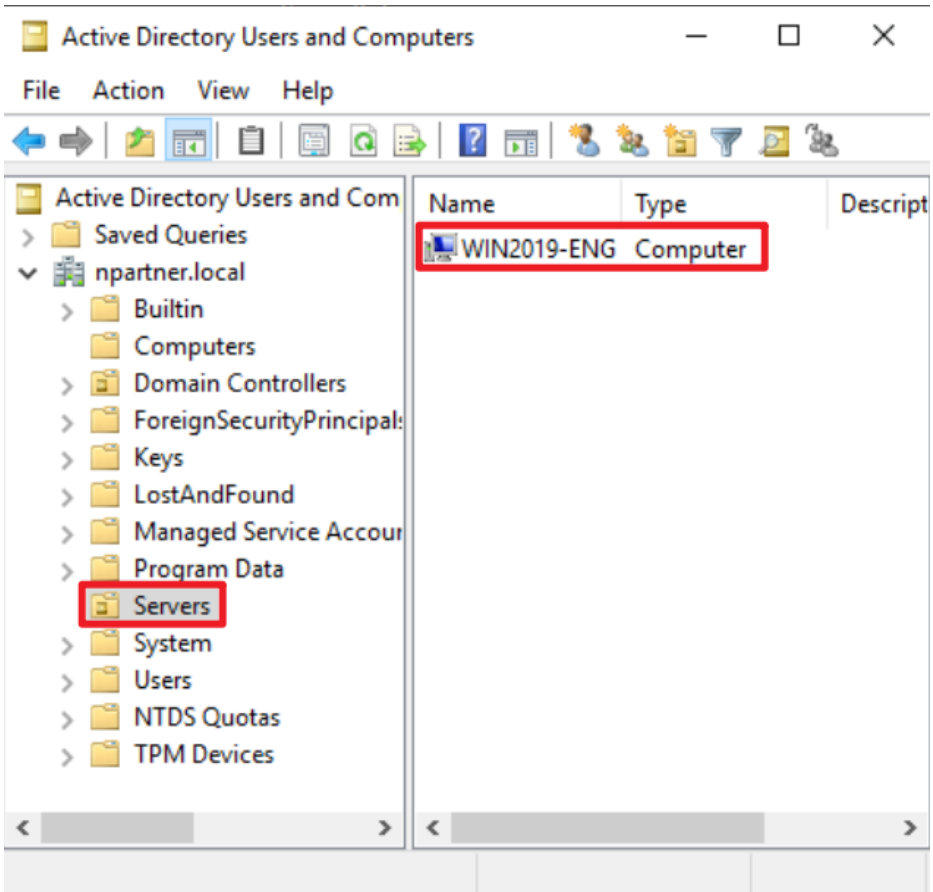
(5) Select your Organizational Unit:

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.

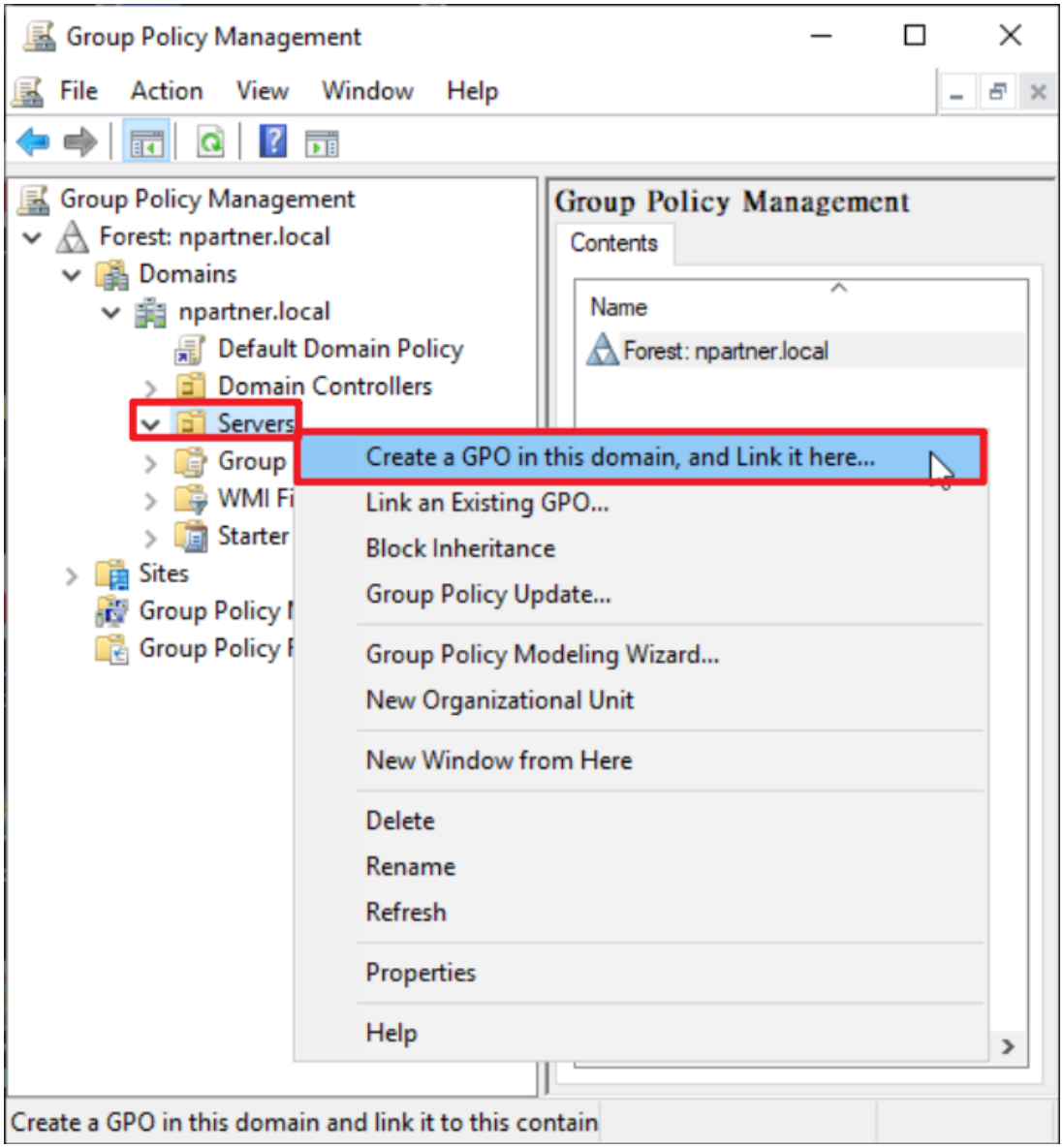


7.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

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

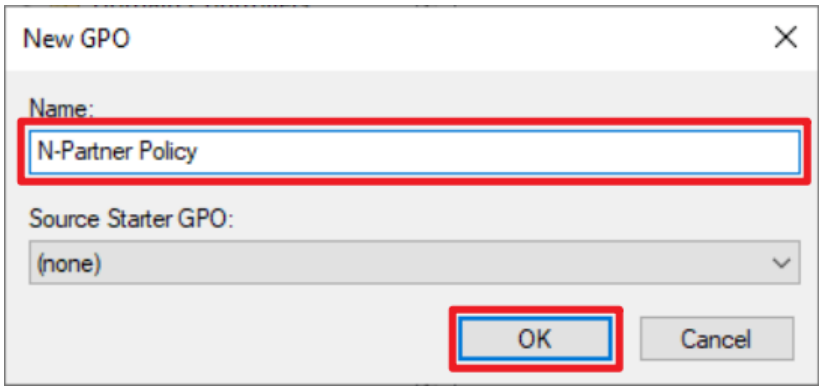
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Enter your Group Policy Object

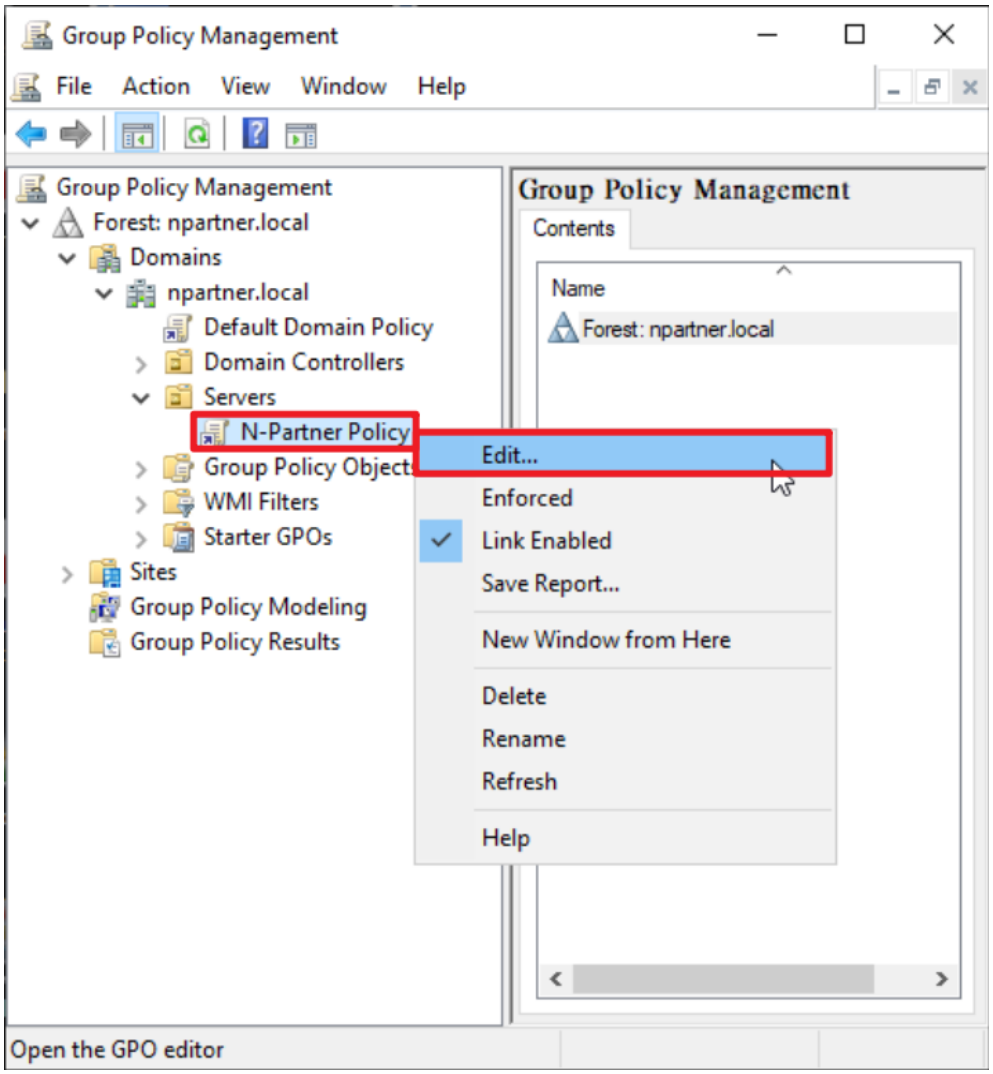
Enter your Group Policy Object name. (in this example, it is “N-Partner Policy”)

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



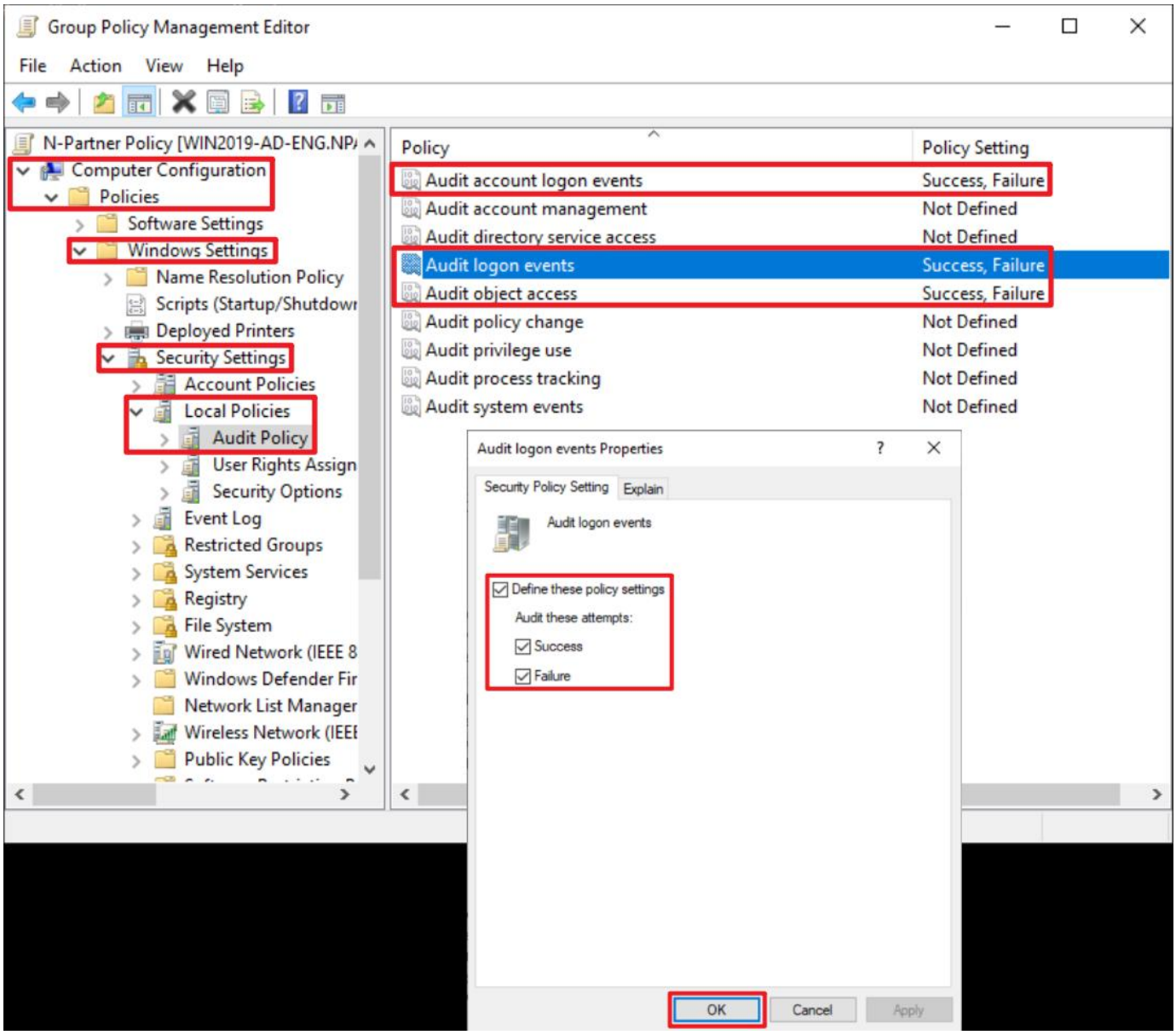
(4) Edit your Group Policy Object

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



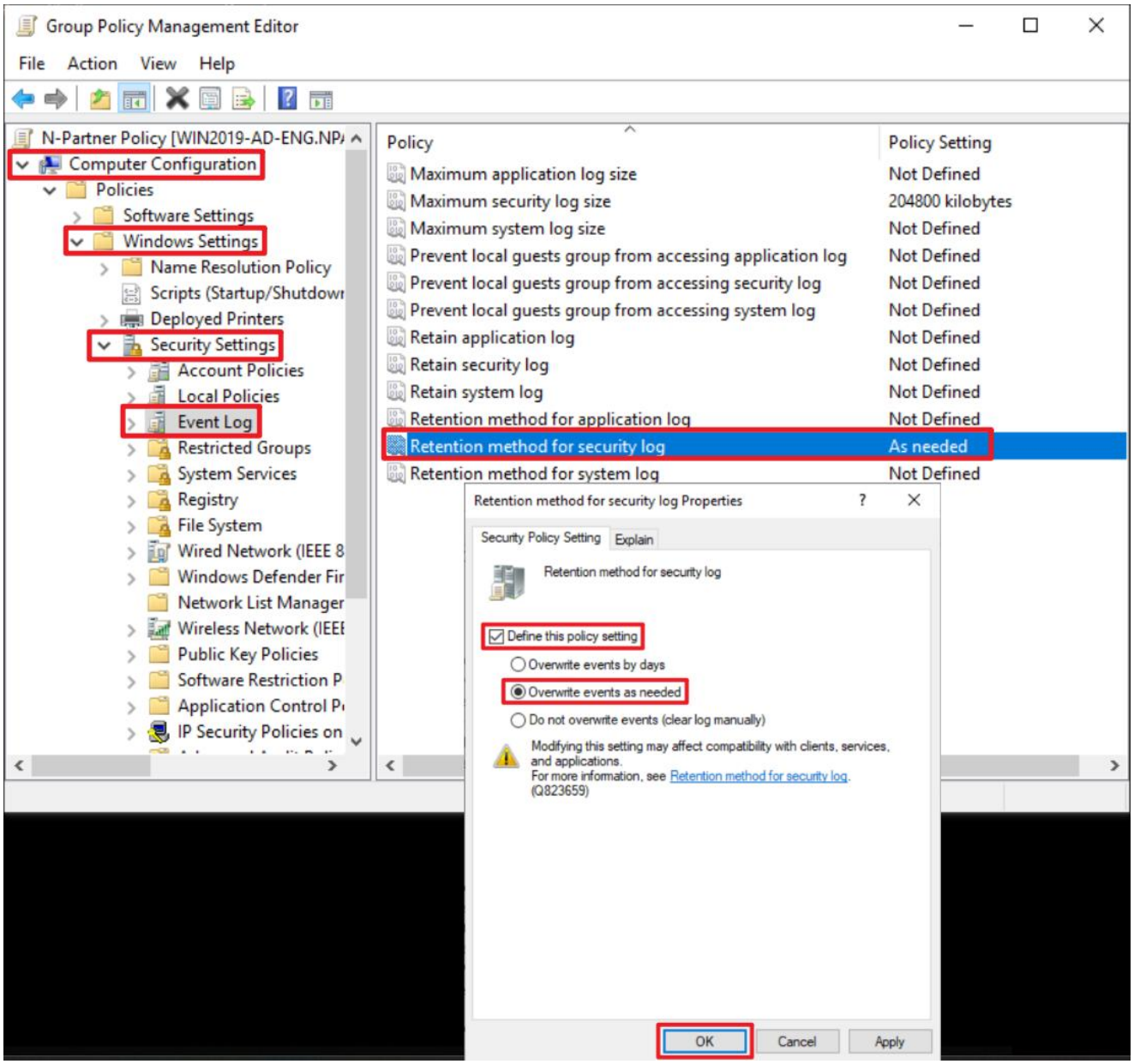
(5) Local Group Policies: Audit Policy

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

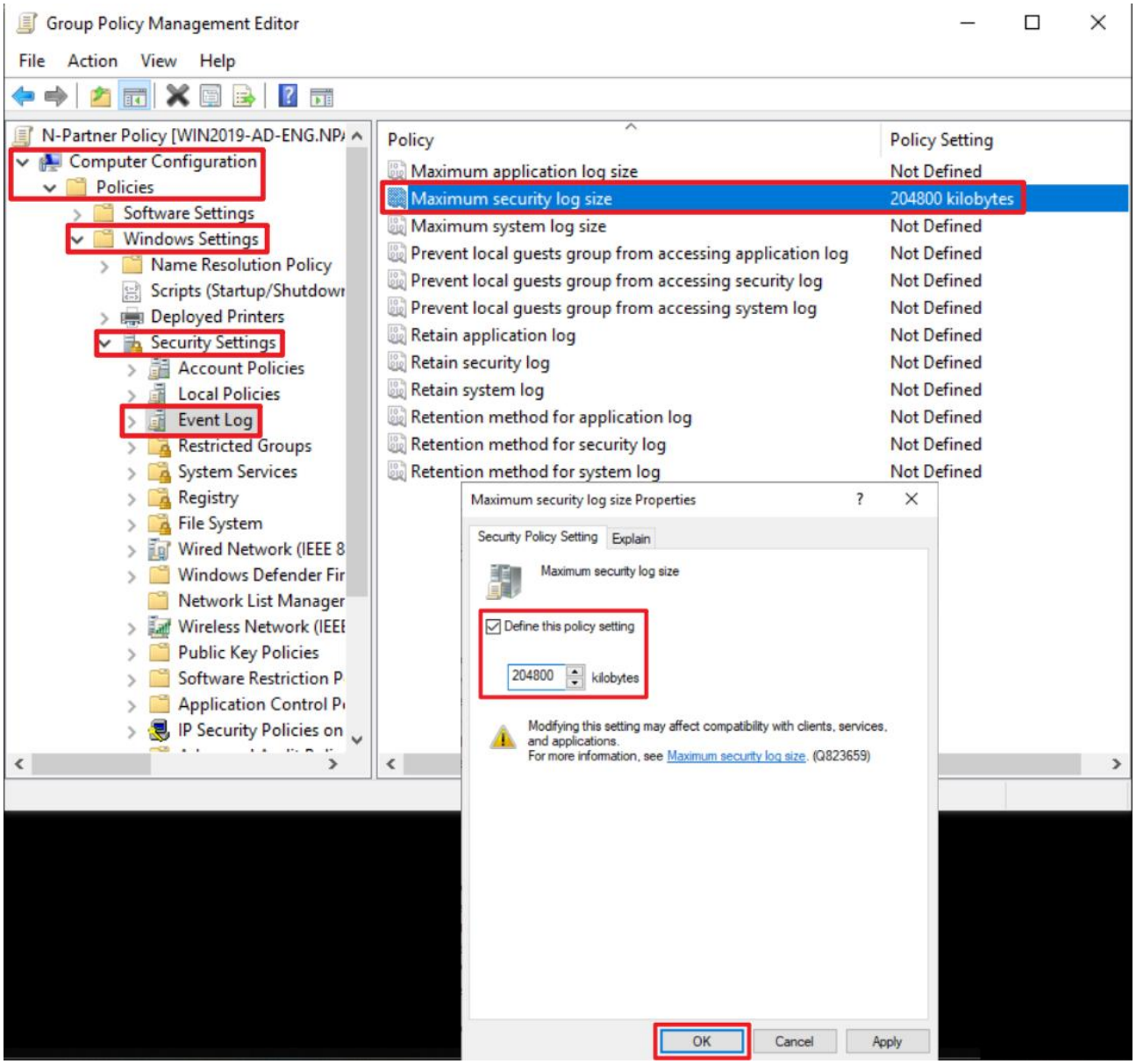
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

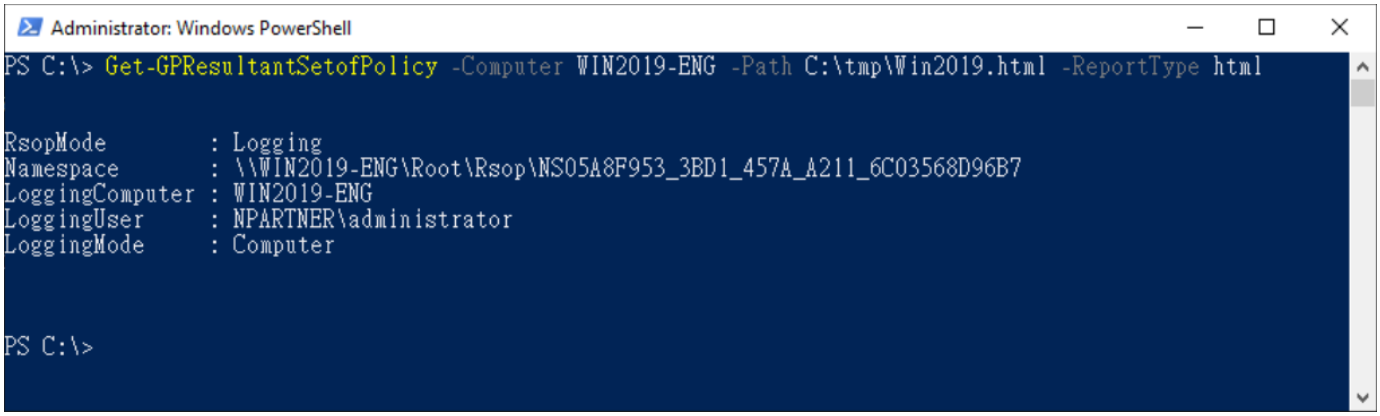
(9) Enter the command below to refresh group policy.

```
PS C:\> Invoke-GPUpdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force
```

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

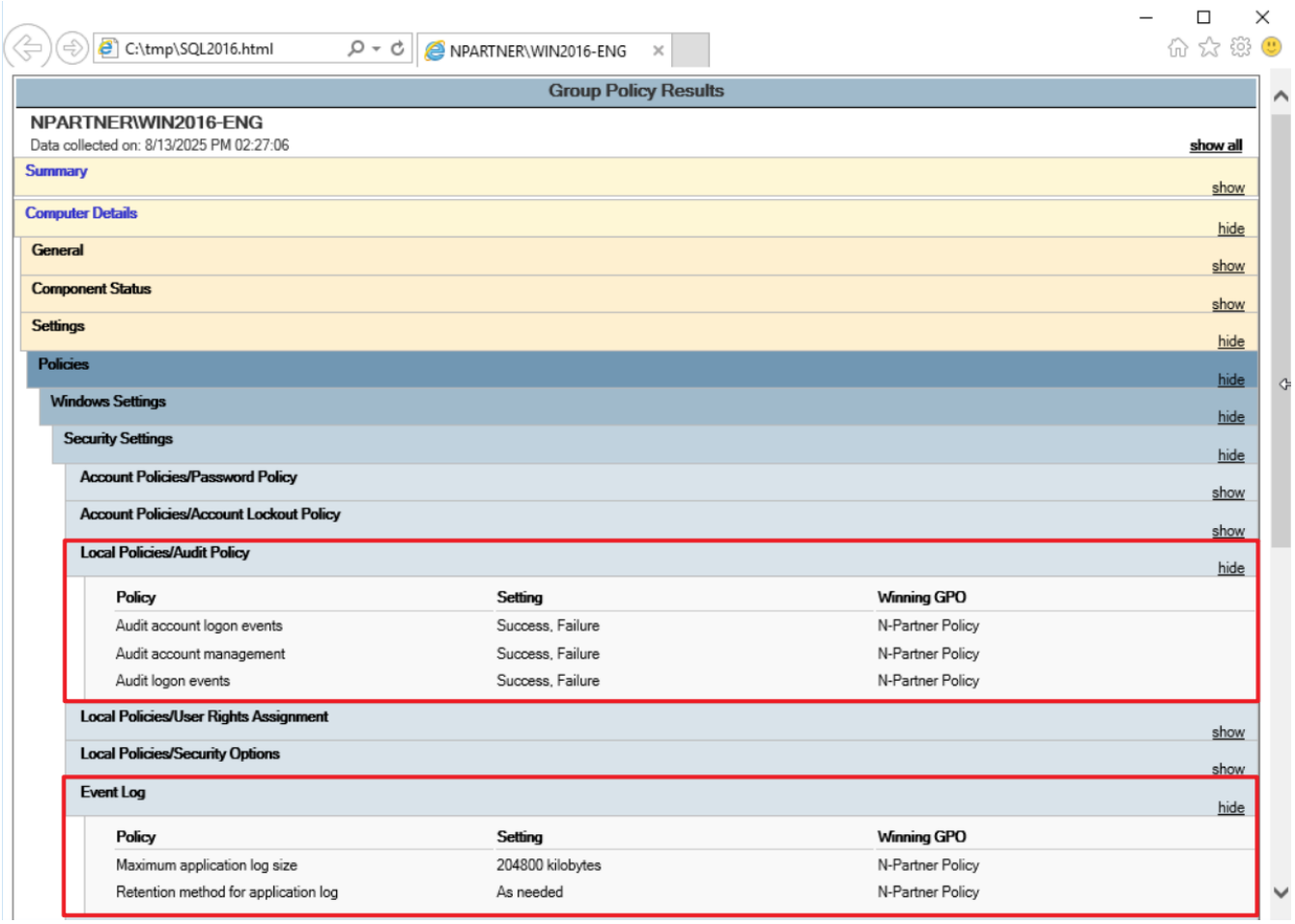
(10) Enter the command below to generate server group policy report.

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

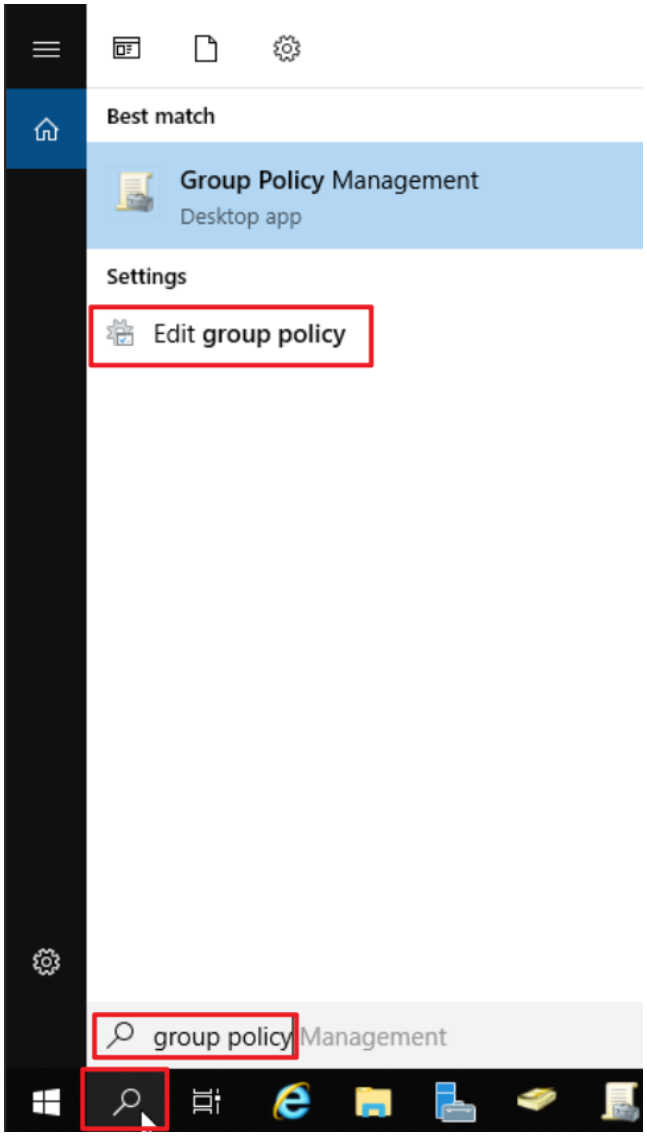


7.2 Workgroup

7.2.1 Audit Policy Configuration

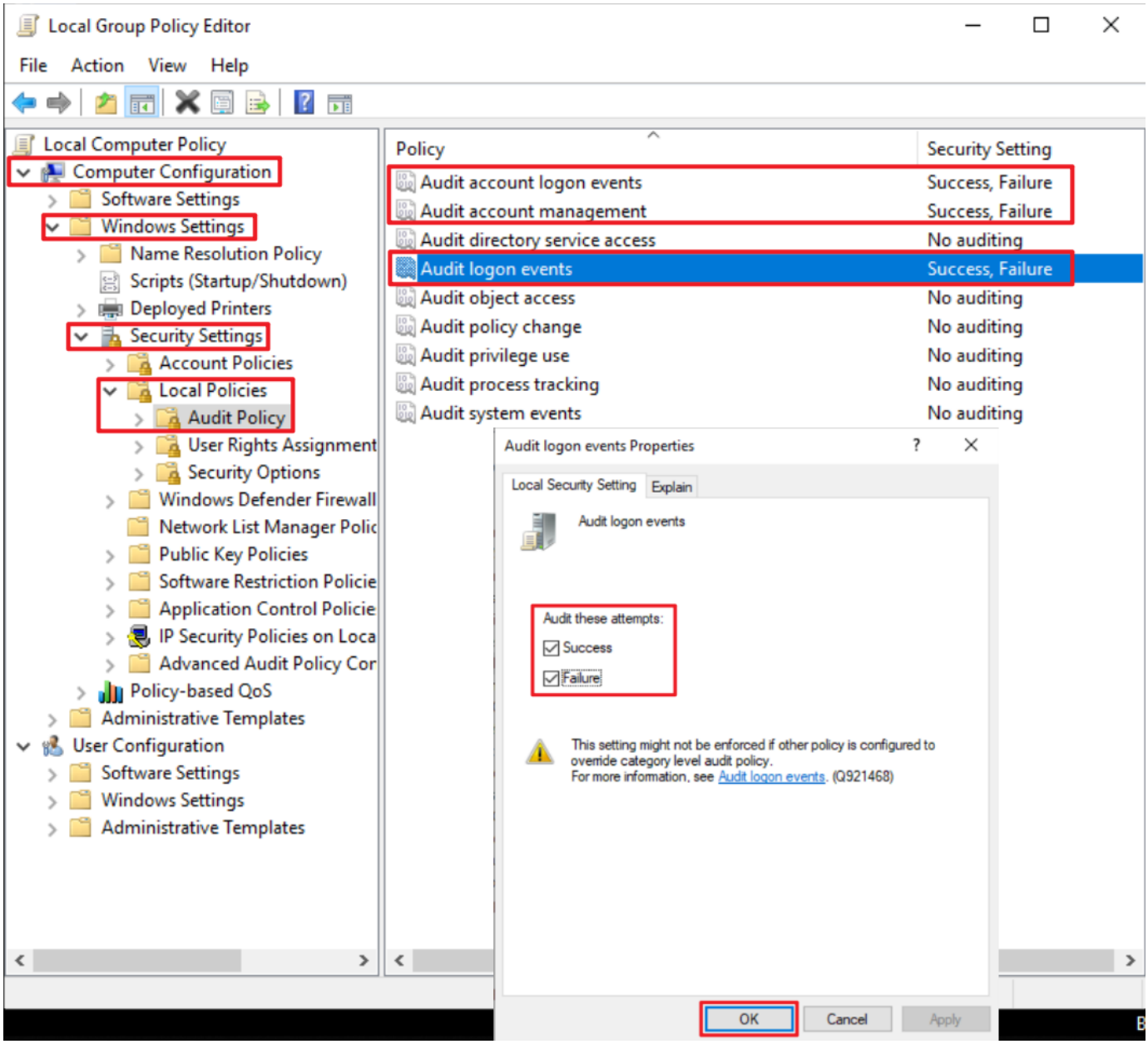
(1) Open Local Group Policy Editor

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



(2) Local Group Policies: Audit Policy

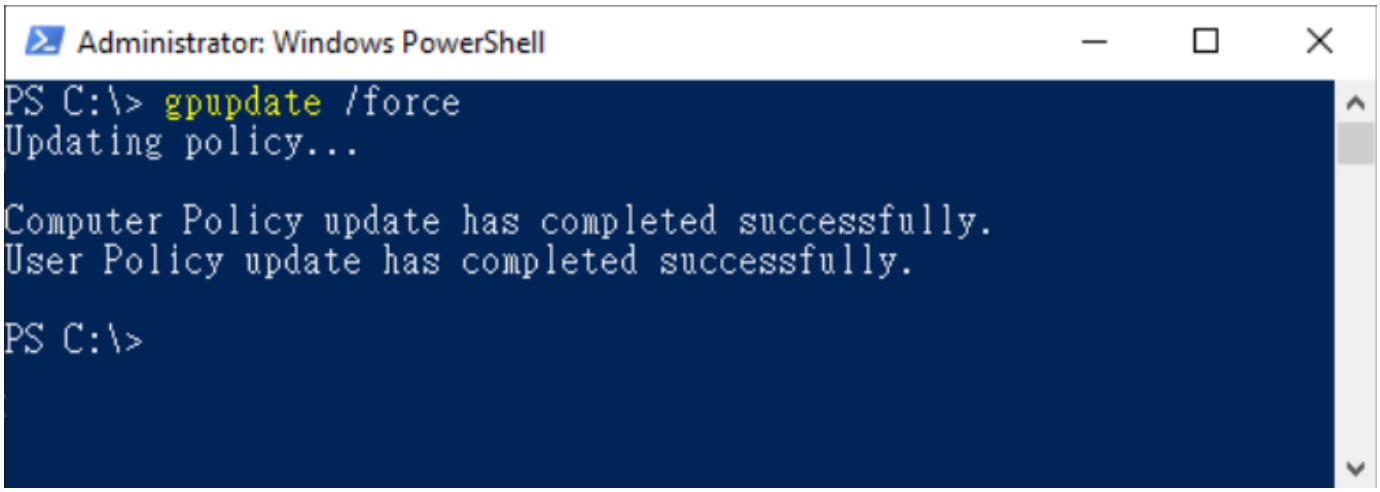
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events” and “Audit logon events” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”

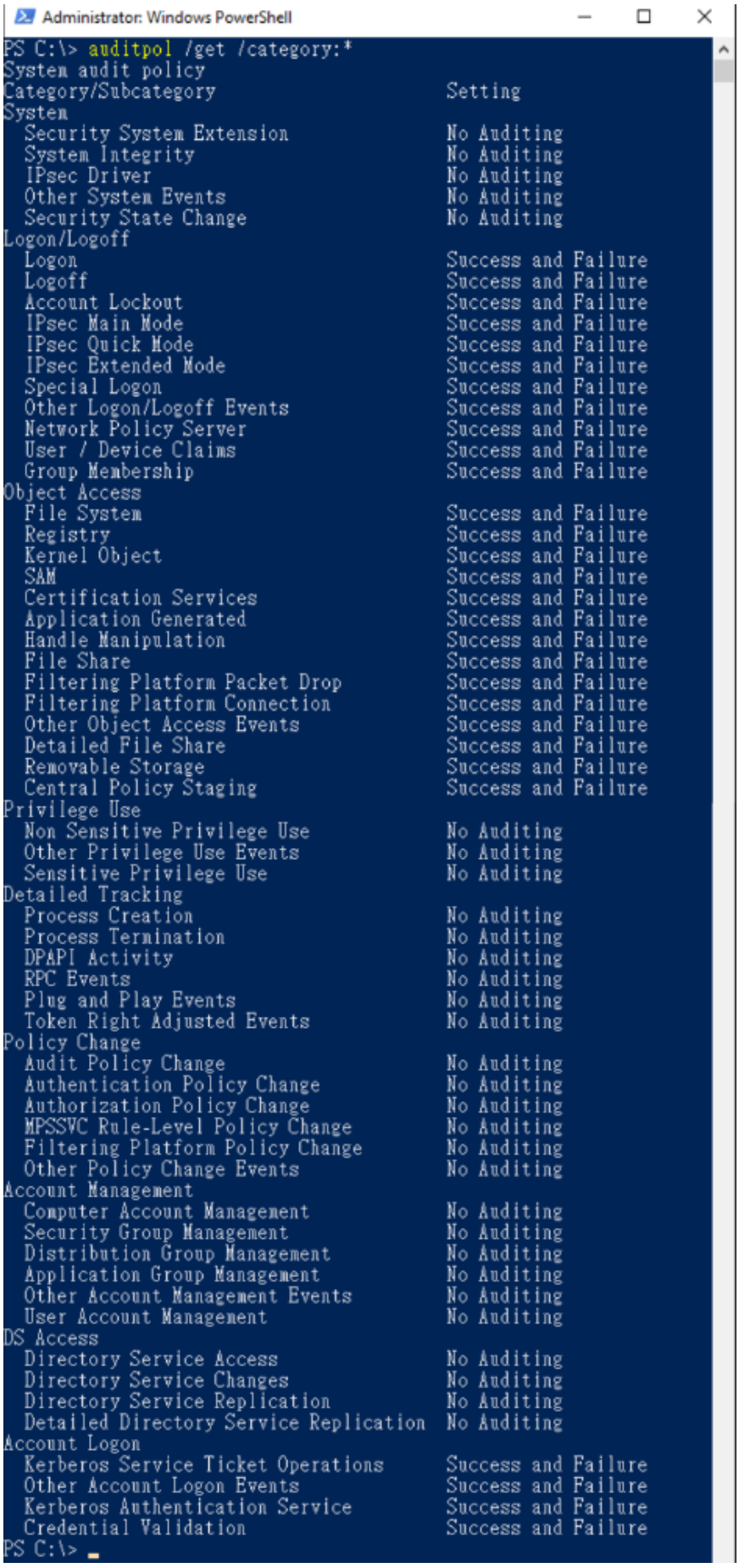
(4) Enter the command below to refresh group policy.

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



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

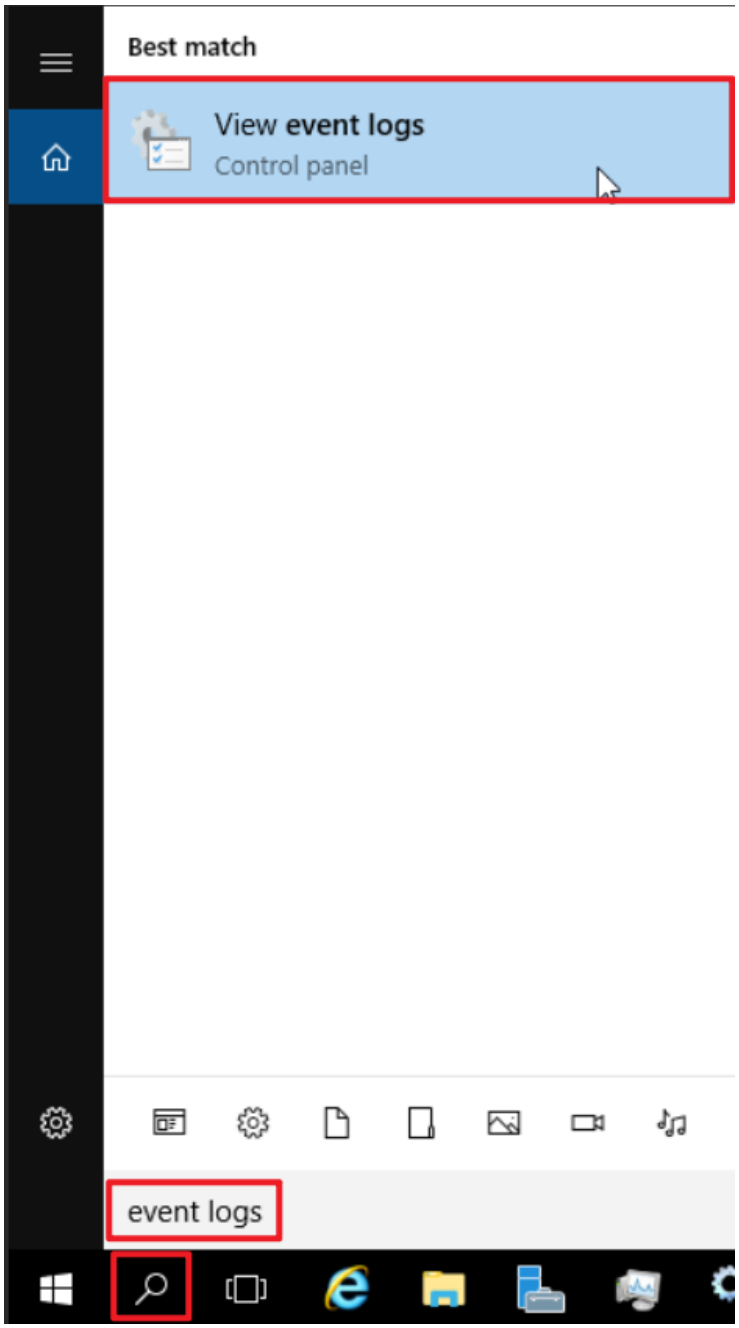
```
PS C: \> auditpol /get /category:*
```



7.2.2 Event Log Settings

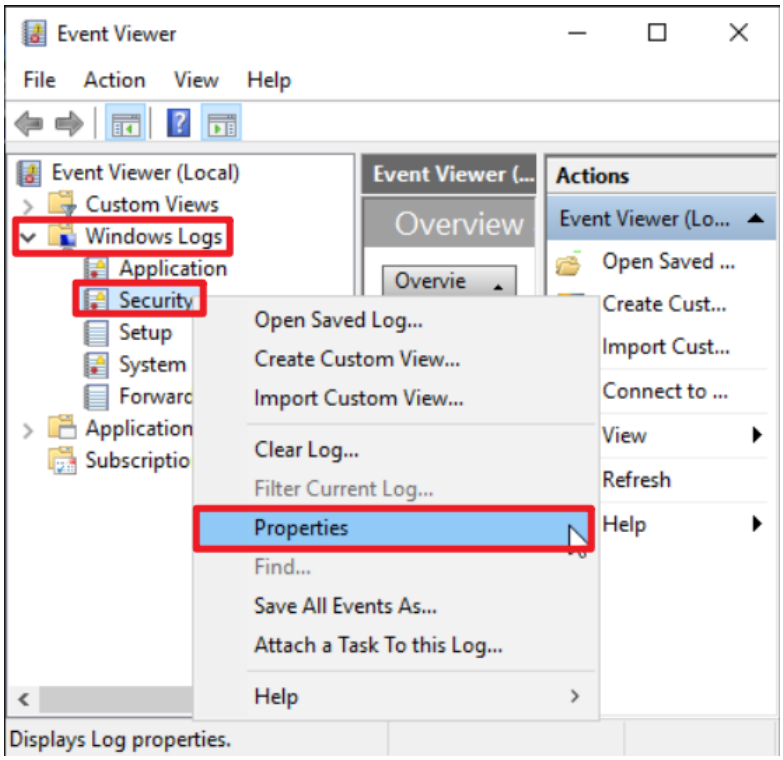
(1) Search for “Event Viewer”

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.”

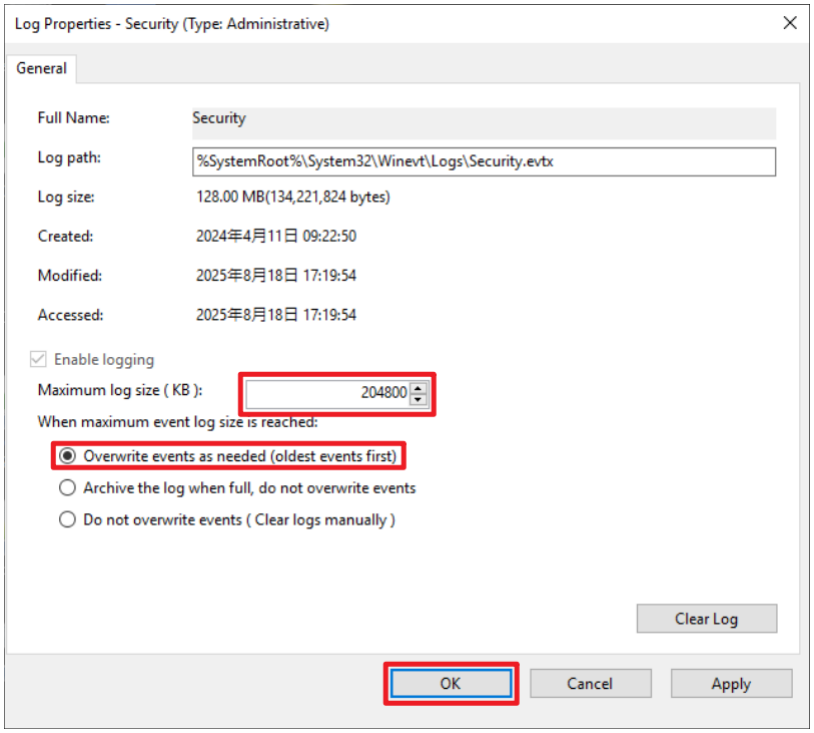


(3) Configure Security Log

Enter maximum log file size: 204800 KB

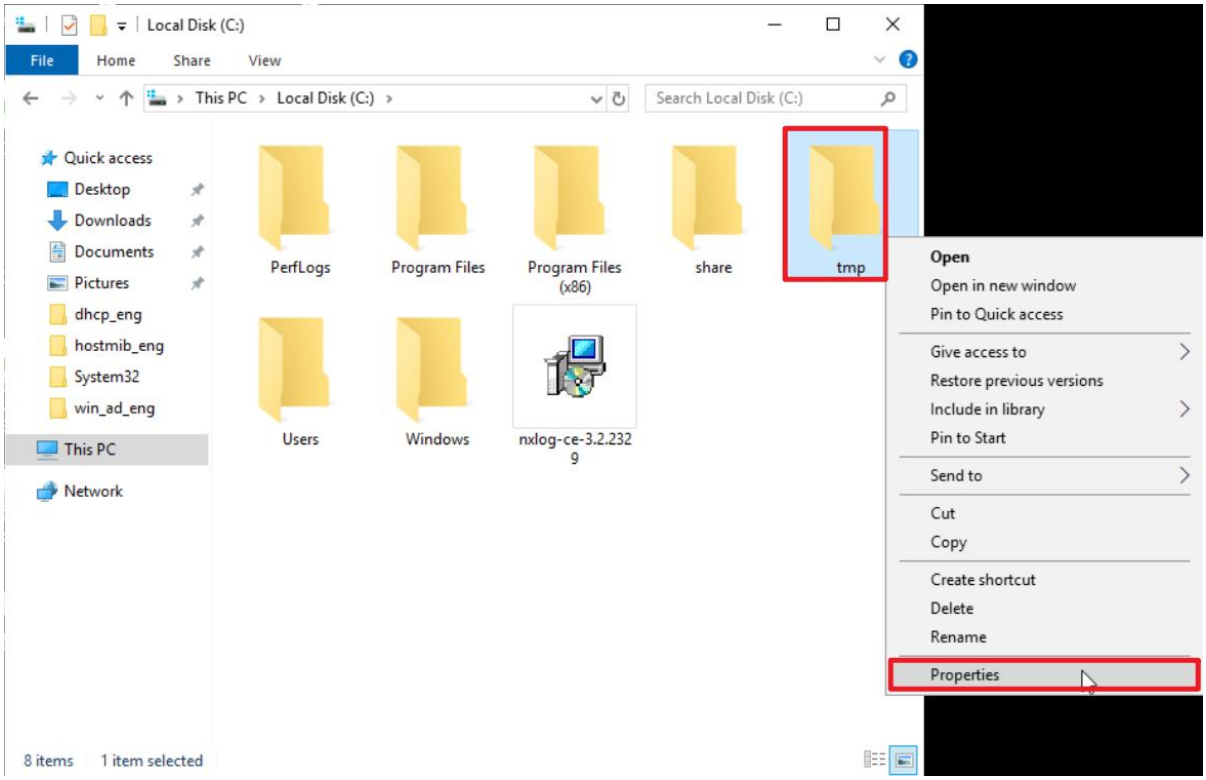
Note: Please adjust the number according to the actual environment.

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

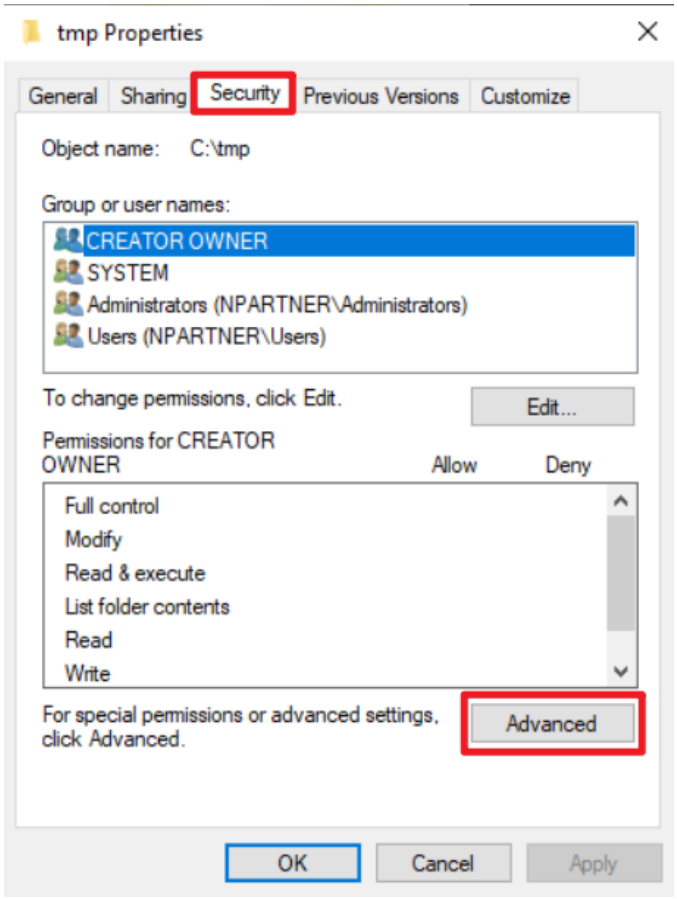


7.3 Folder Audit Configuration

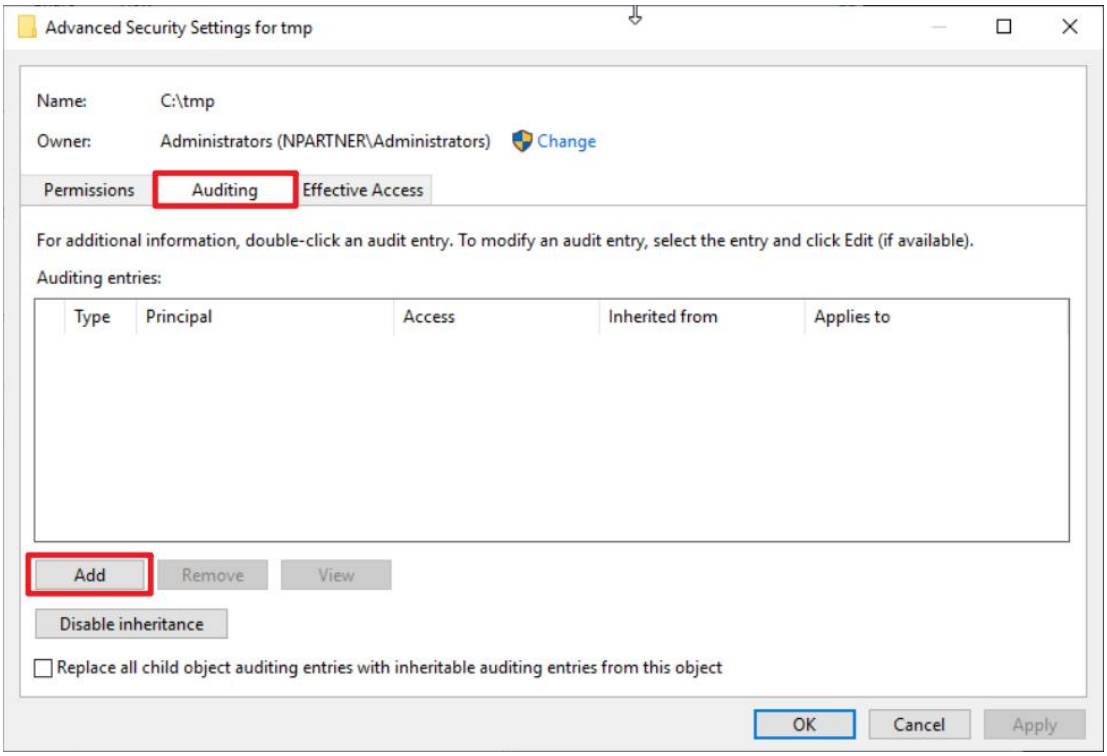
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



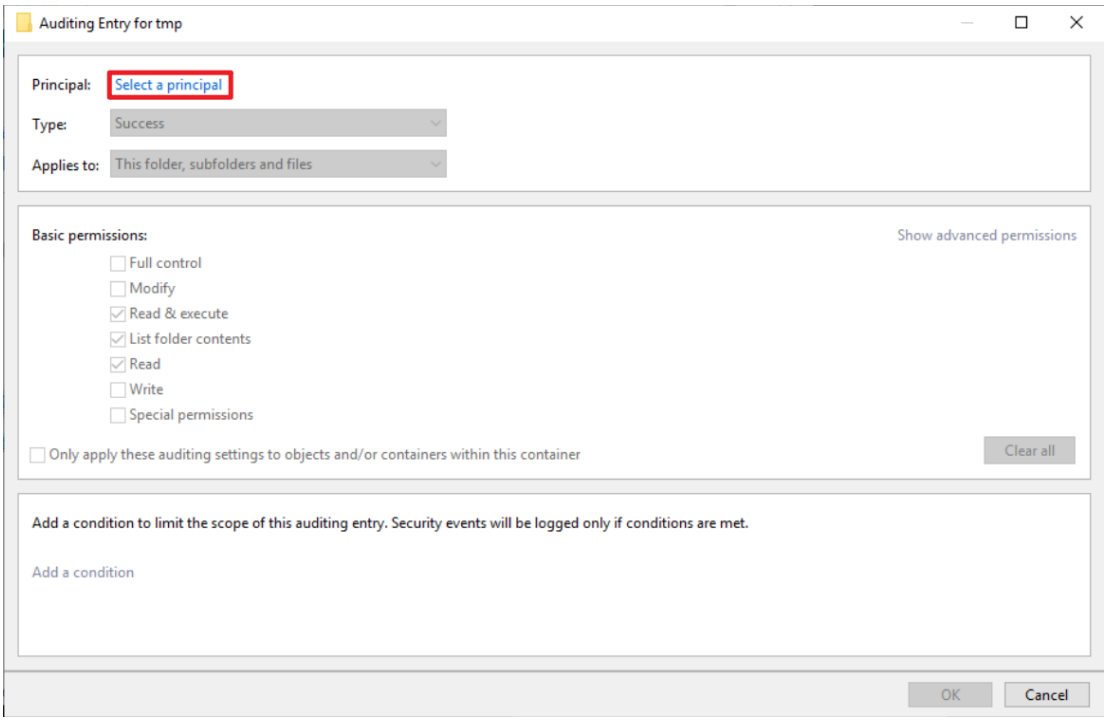
(2) Go to the “Security” tab → click “Advanced.”



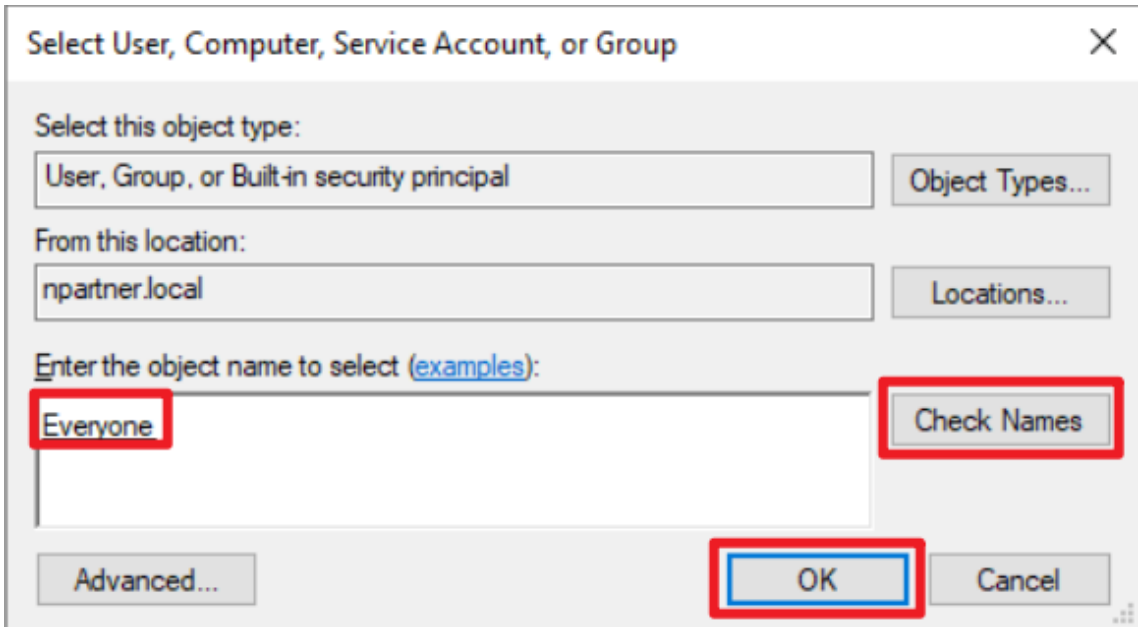
(3) Open the “Auditing” tab → click “Add.”



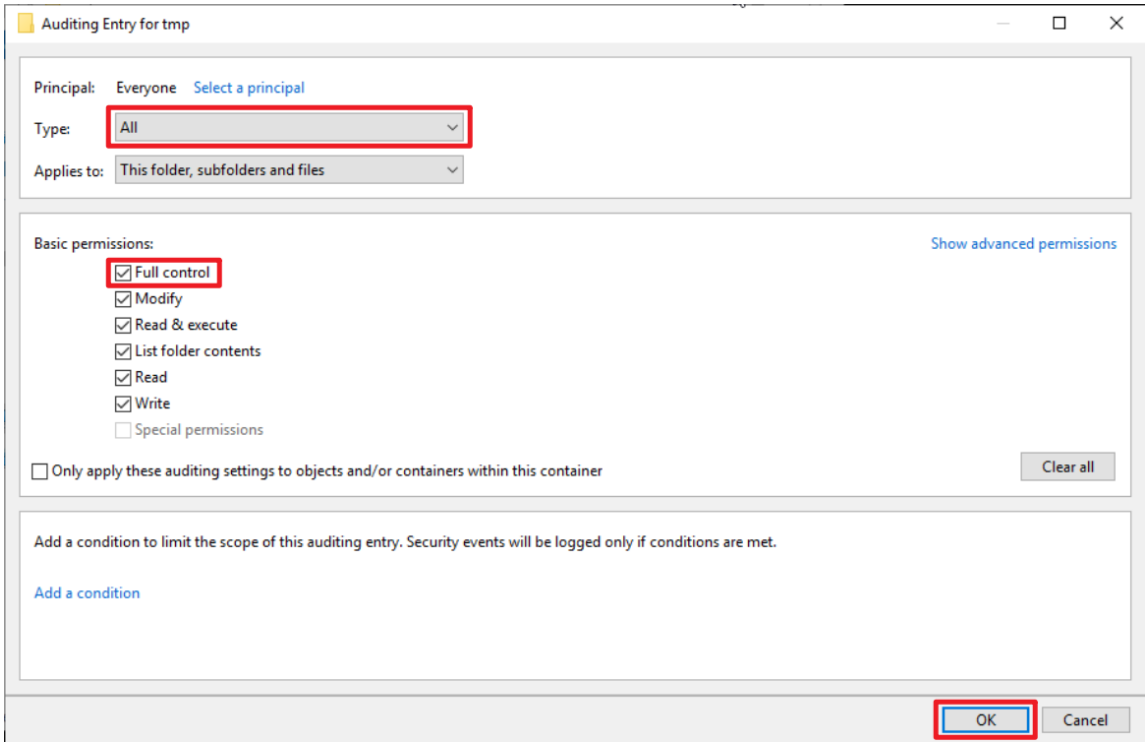
(4) Click “Select a principal.”



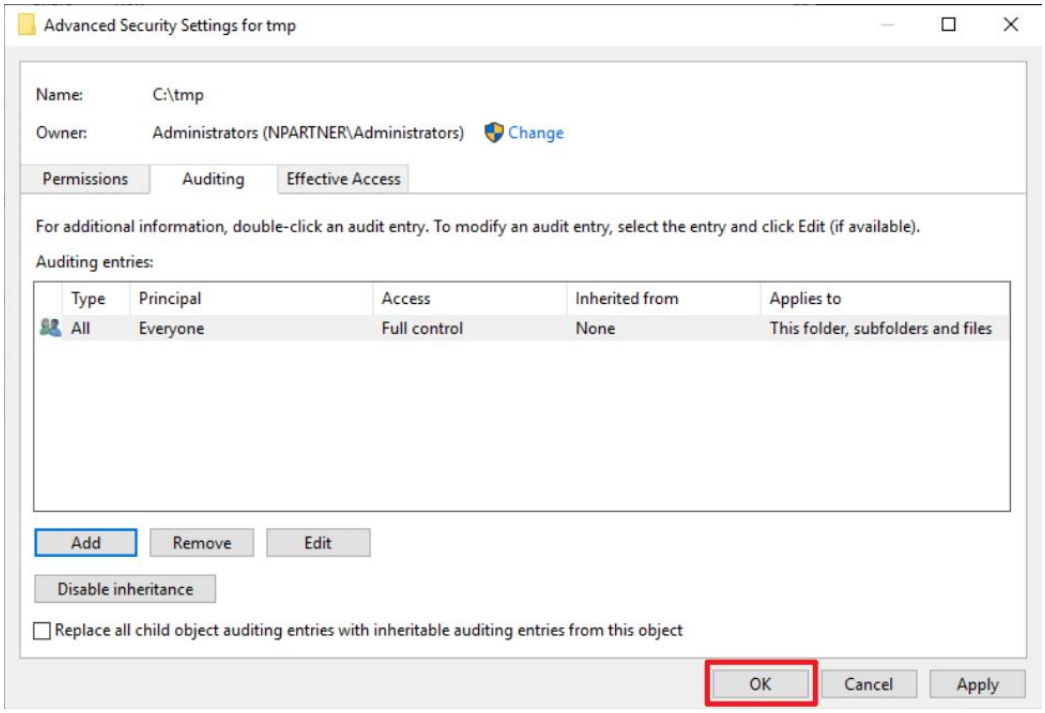
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



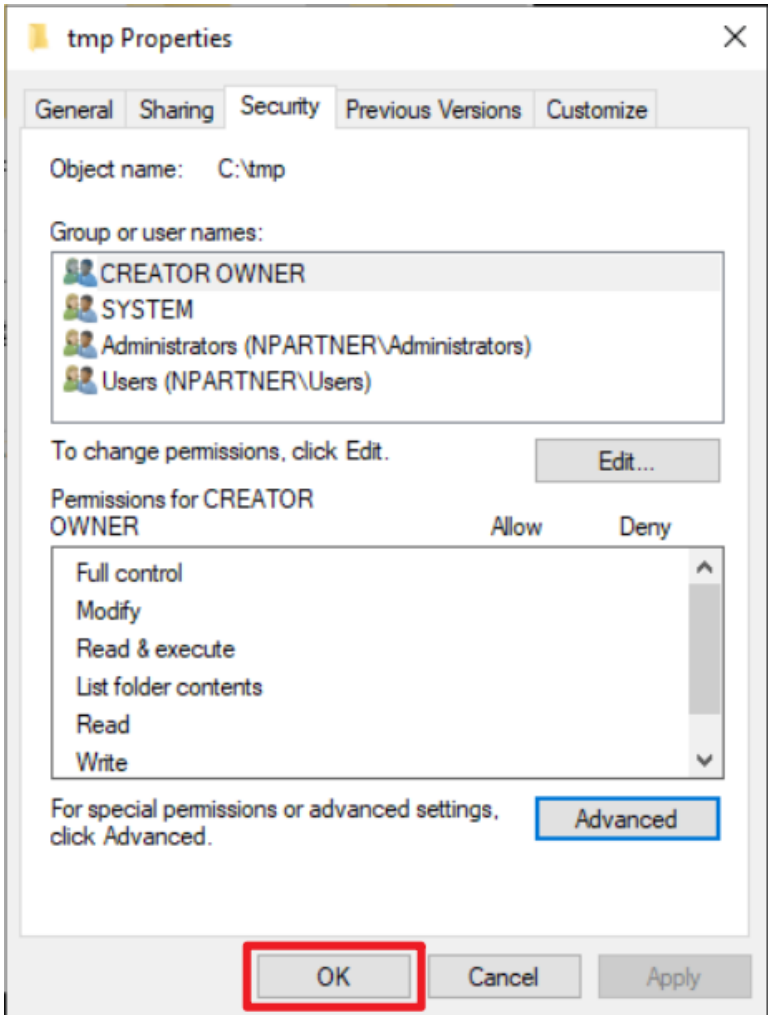
(6) Select “All” in type → enable “Full Control” → click “OK.”



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



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



8. Windows Server 2022

8.1 Domain

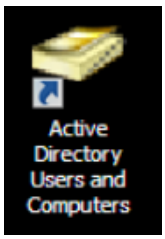
Windows Audit Policy Configuration:

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.

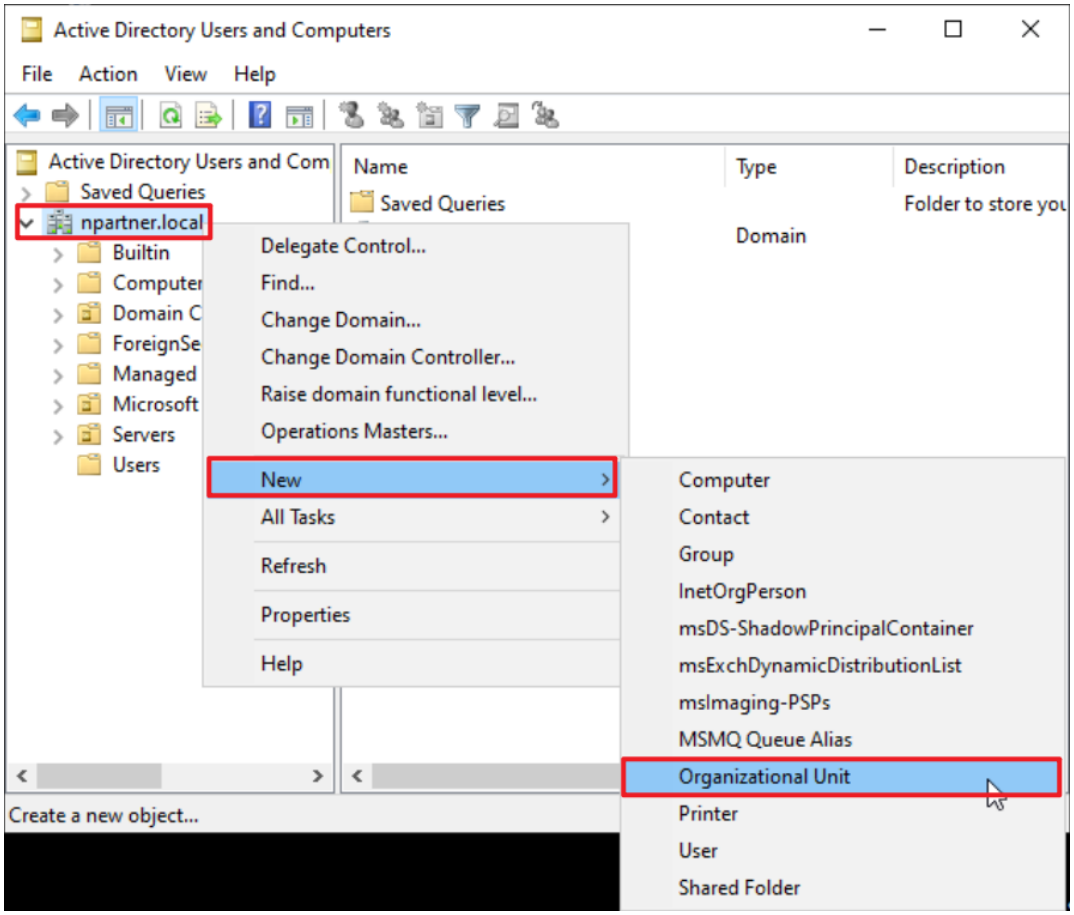
8.1.1 Organizational Unit (OU) Configuration

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



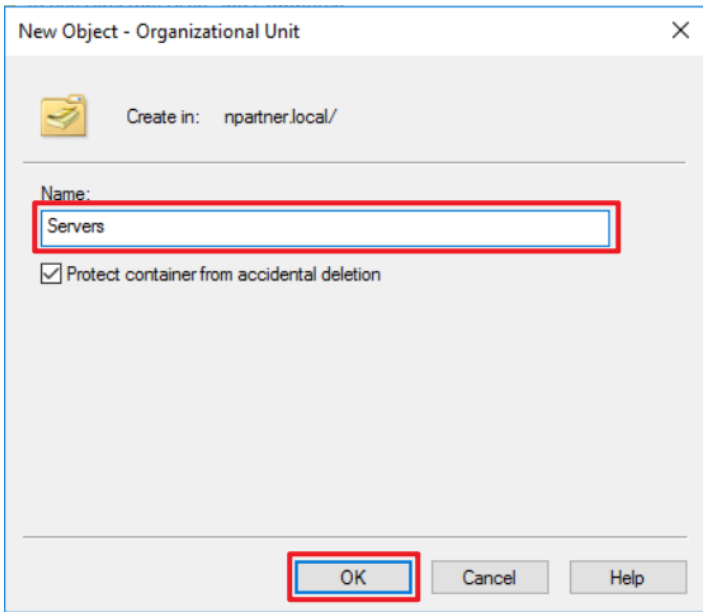
(2) Add an Organizational Unit

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



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

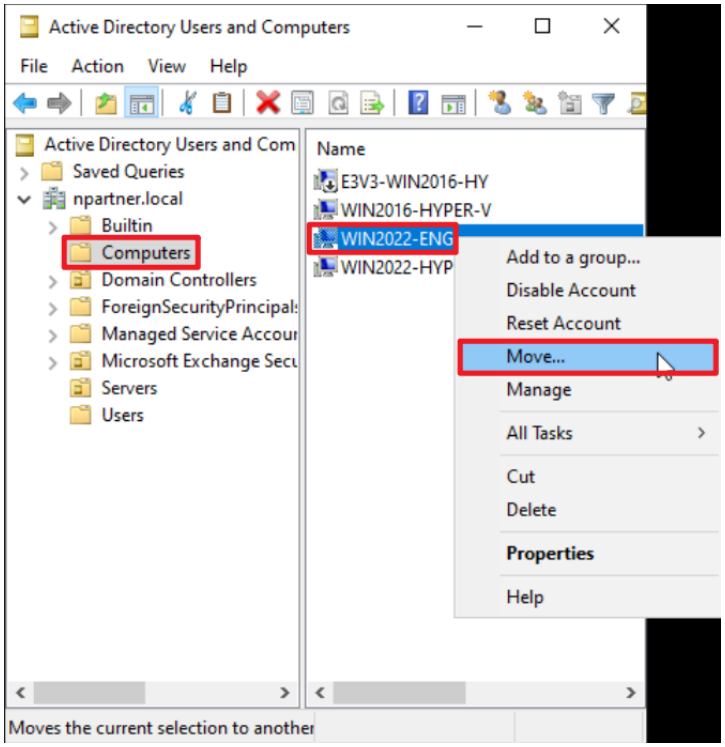
Note: Please create the organizational unit name according to the actual environment. → click “OK.”



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

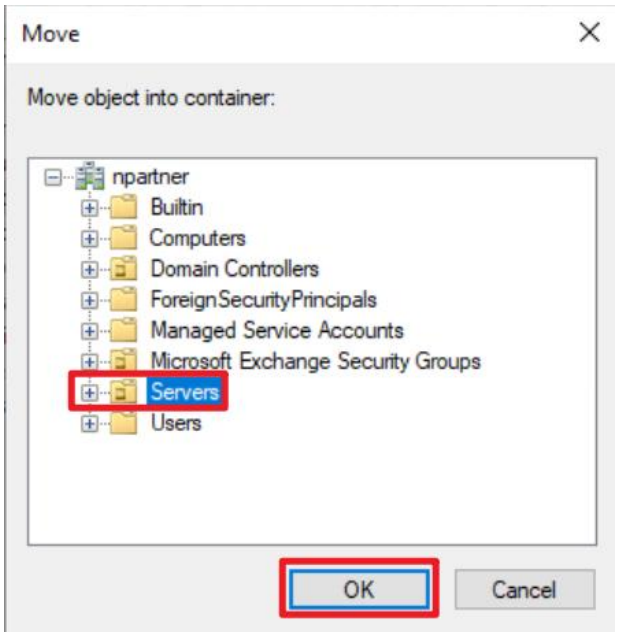
Select your organizational unit in “Domain Controllers” -> Right-click on the “WIN2022-ENG” server.

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



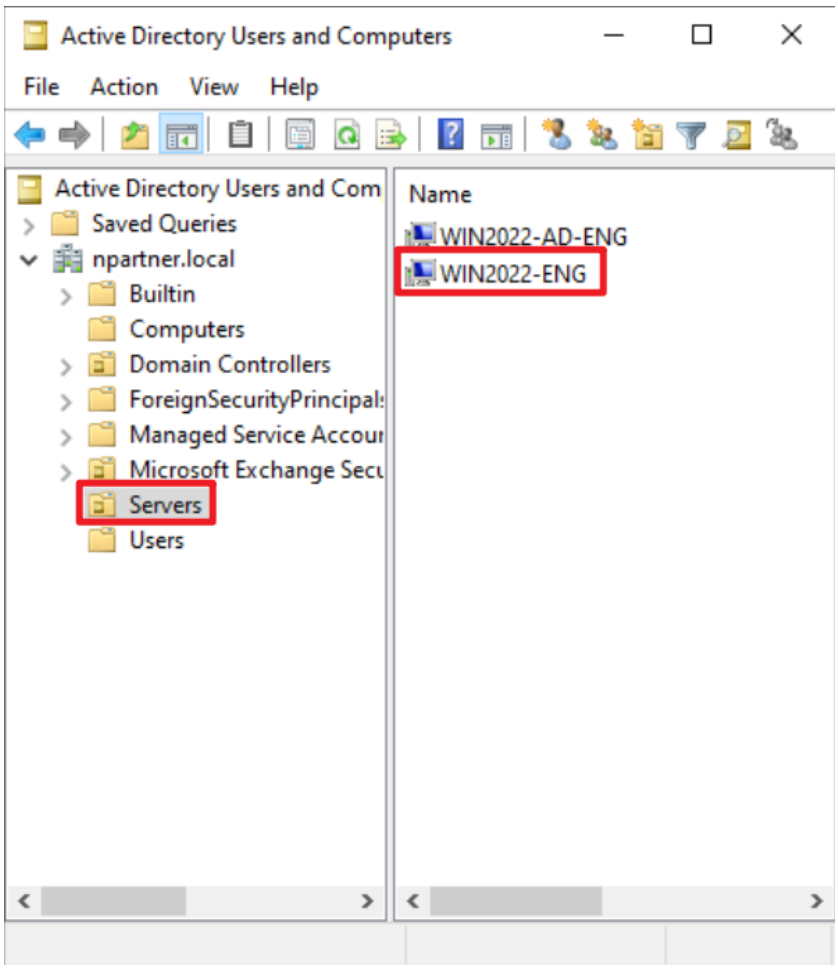
(5) Select your Organizational Unit:

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.

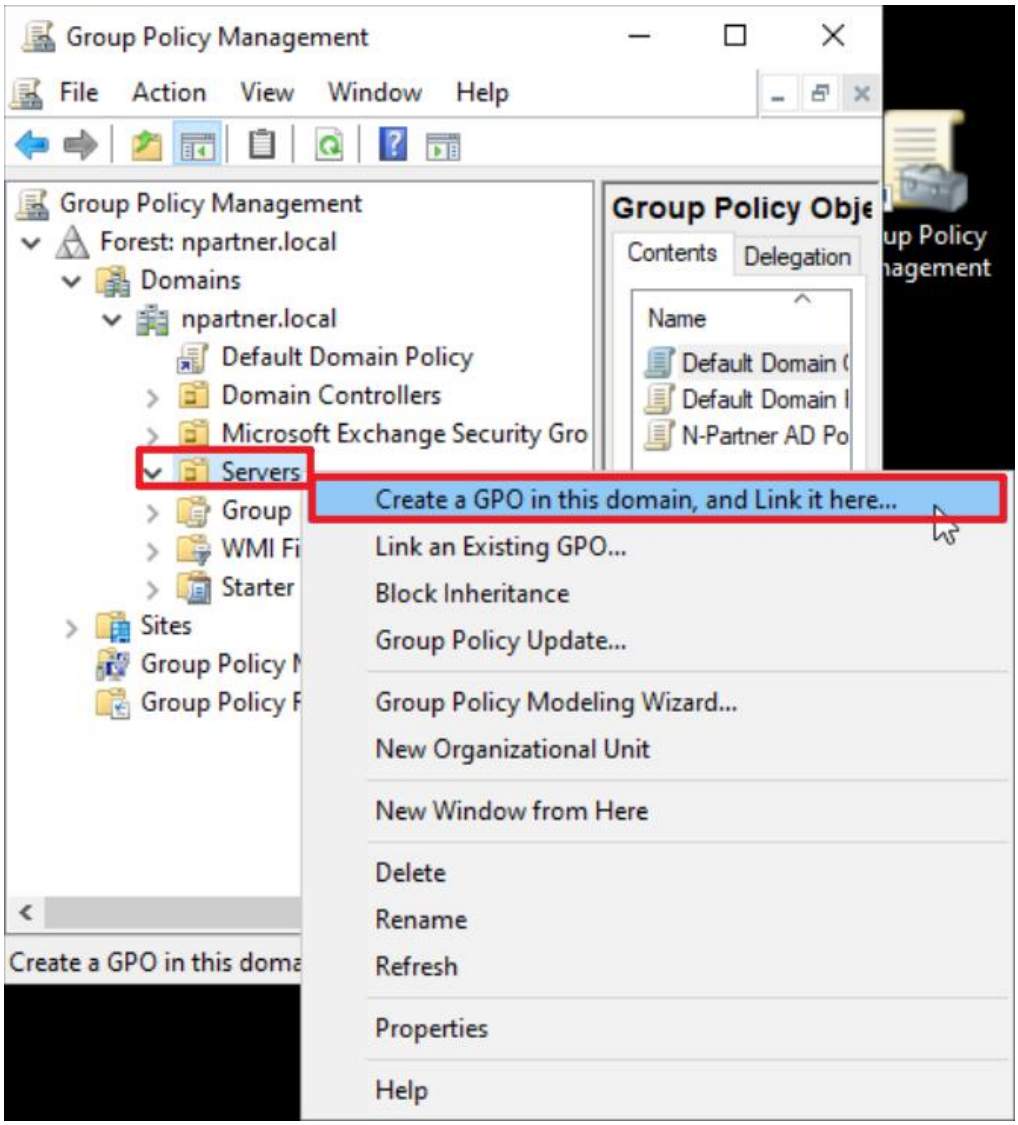


8.1.2 Group Policy Settings

(1) Click “Group Policy Management.”

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

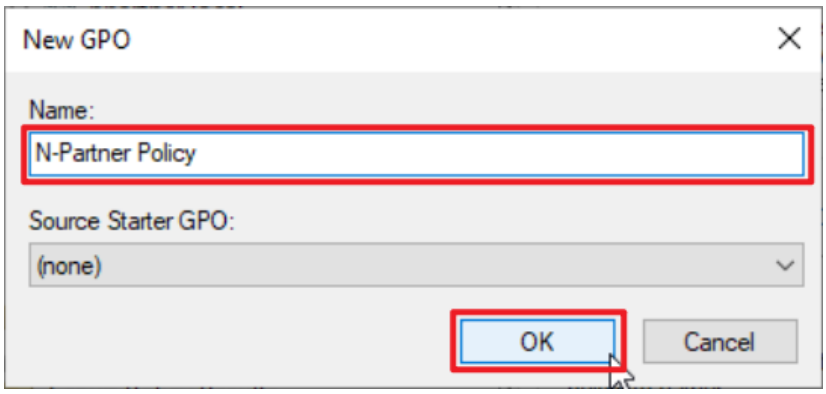
Right-click the [Servers] organizational unit → select “Create a GPO in this domain, and Link it here...”



(3) Edit your Group Policy Object

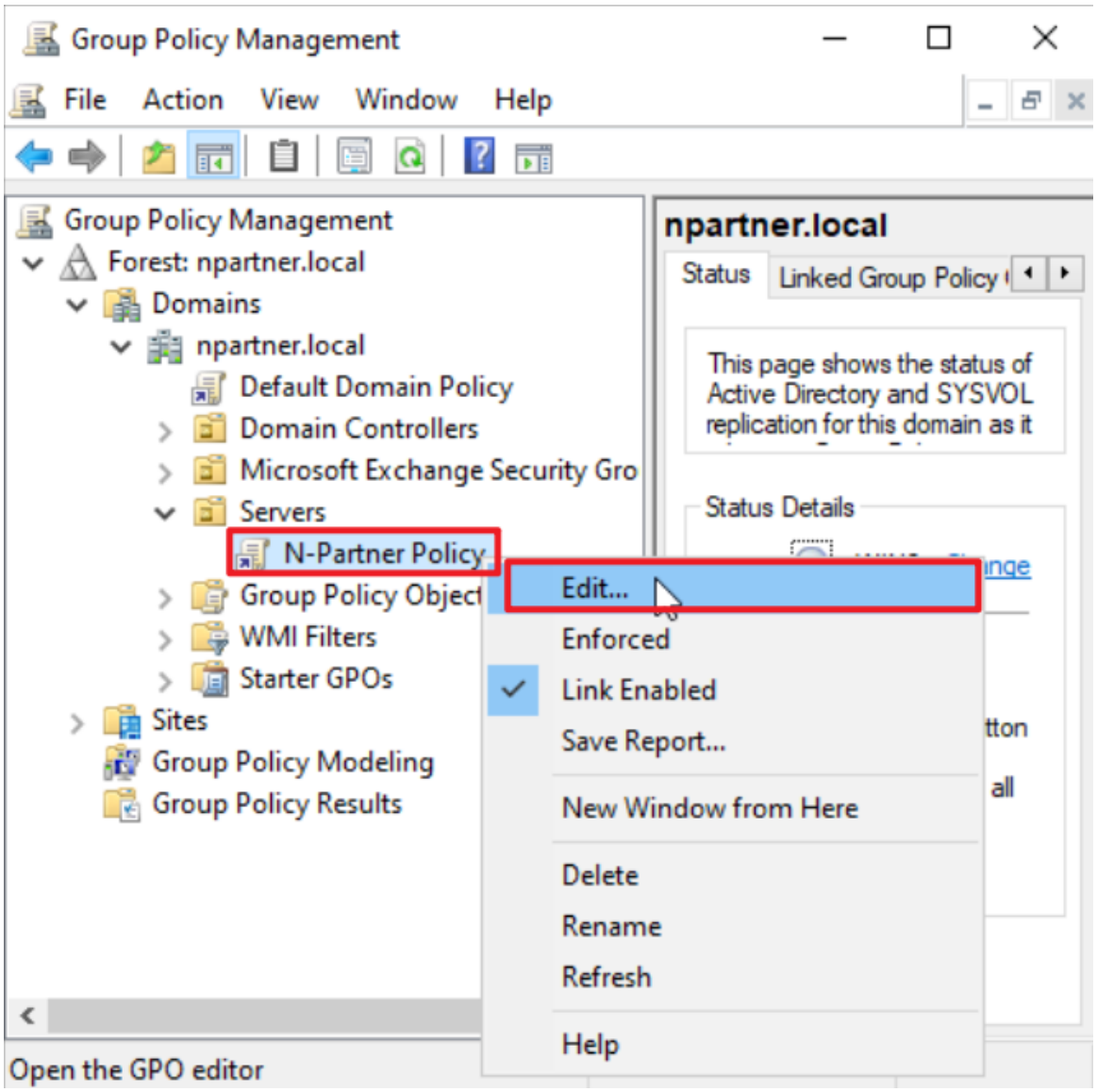
Enter your Group Policy Object name. (in this example, it is "N-Partner Policy")

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



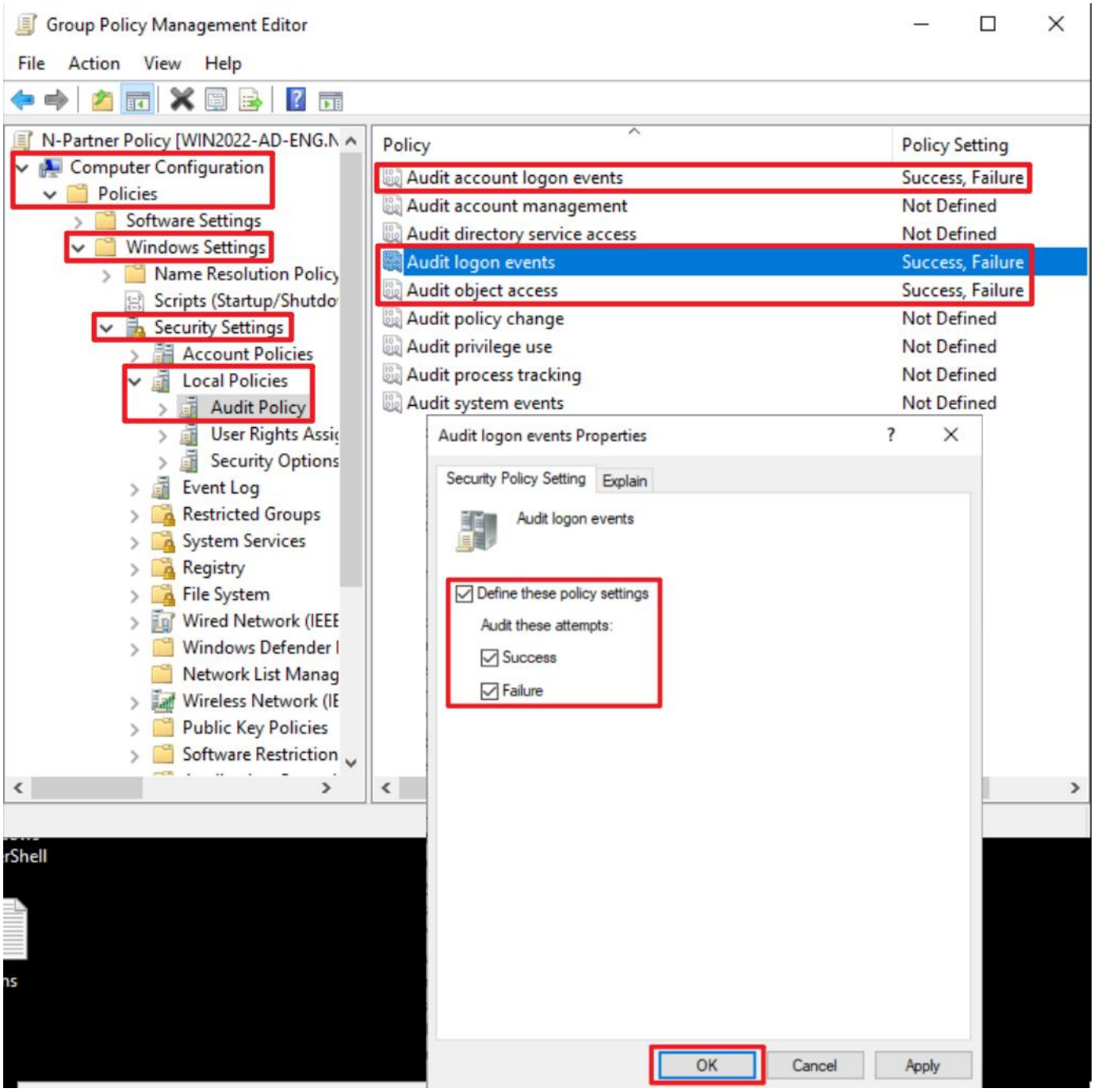
(4) Edit your Group Policy Object

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



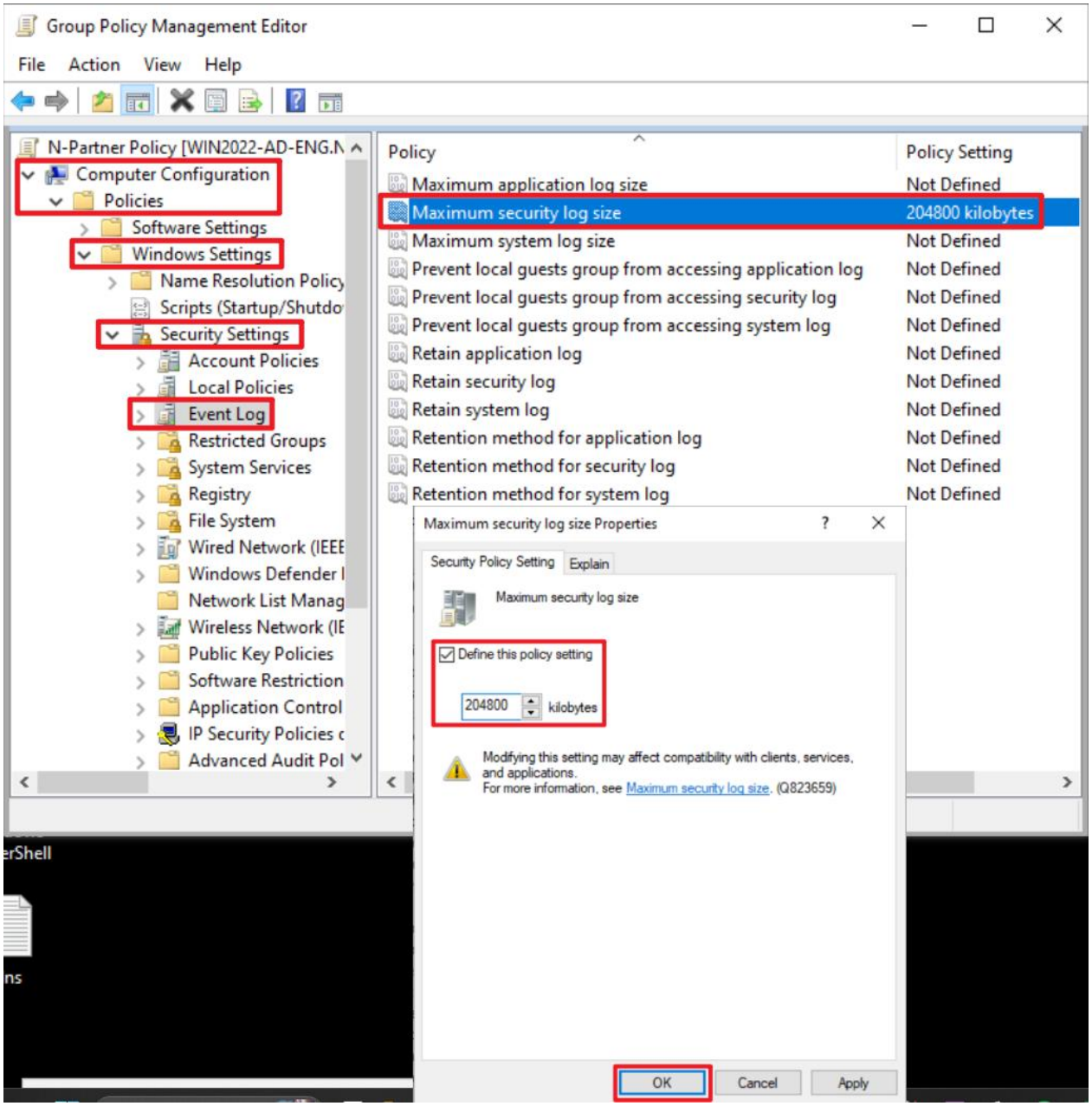
(5) Local Group Policies: Audit Policy

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

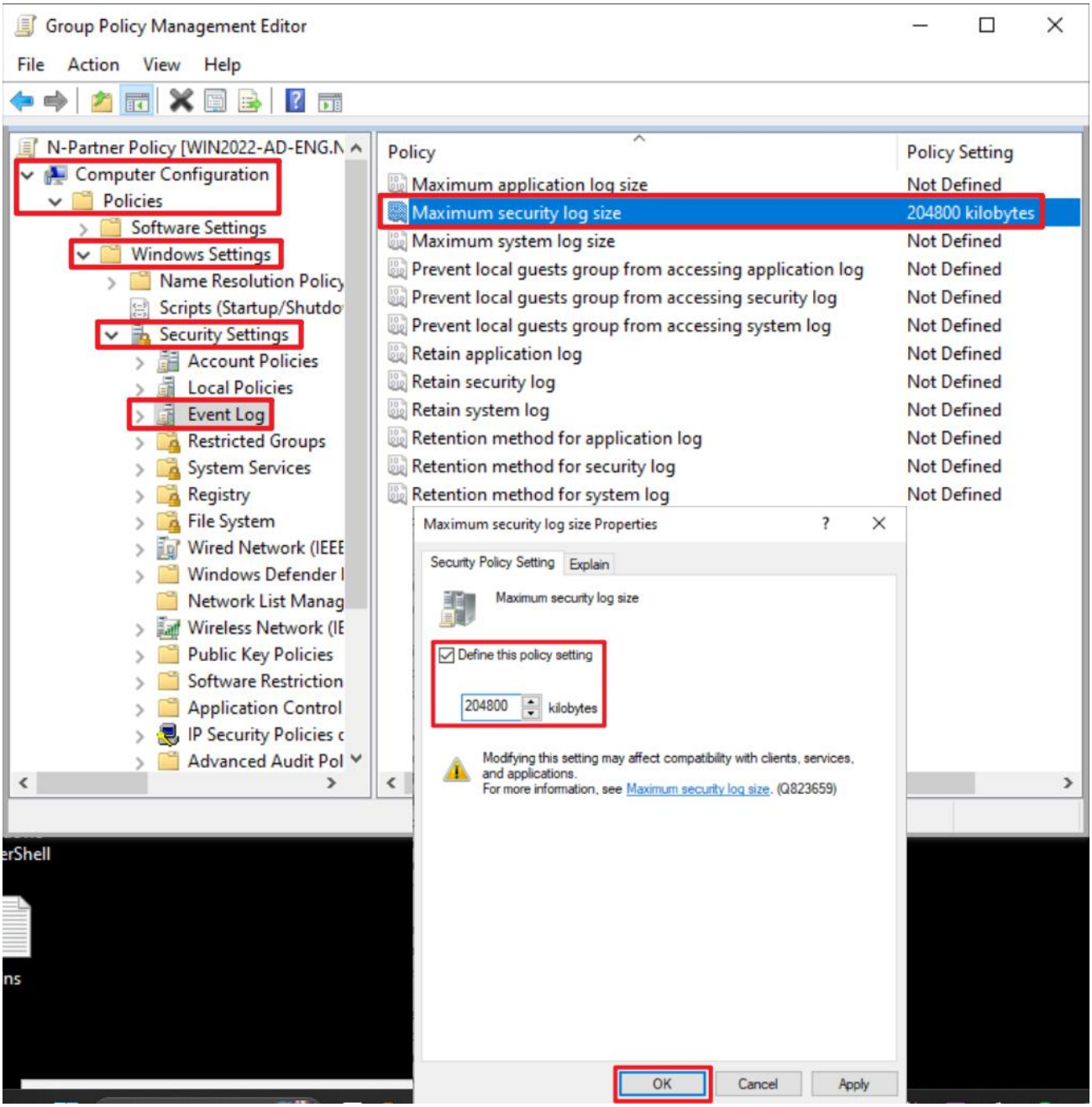
Expand “Computer Configuration” → “Policies” → “Windows Settings” → “Security Settings” → “Event Log” → select “Retention method for security log” → check “Define this policy setting” → select “Overwrite events as needed” → click “OK.”



(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.”

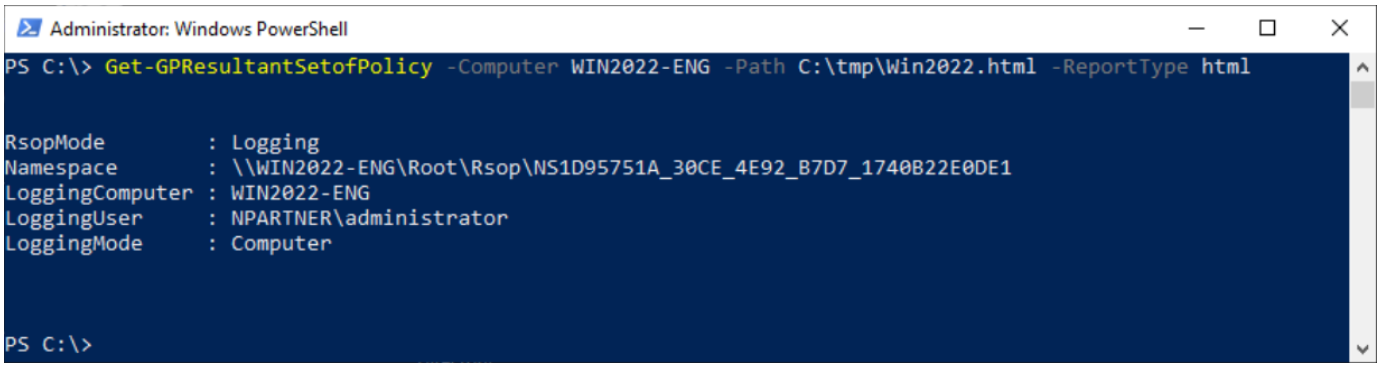
(9) Enter the command below to refresh group policy.

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

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

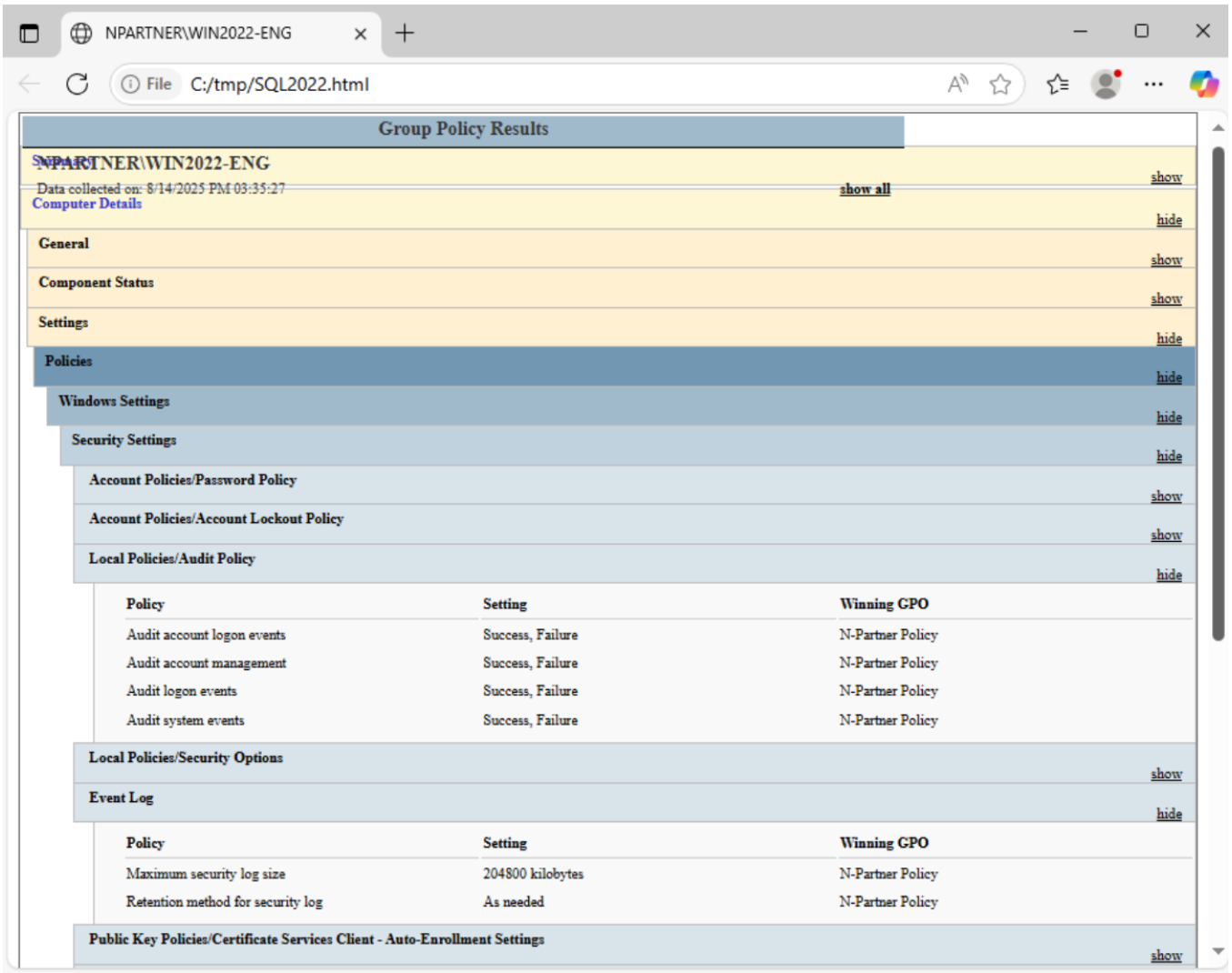
(10) Enter the command below to generate server group policy report.

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

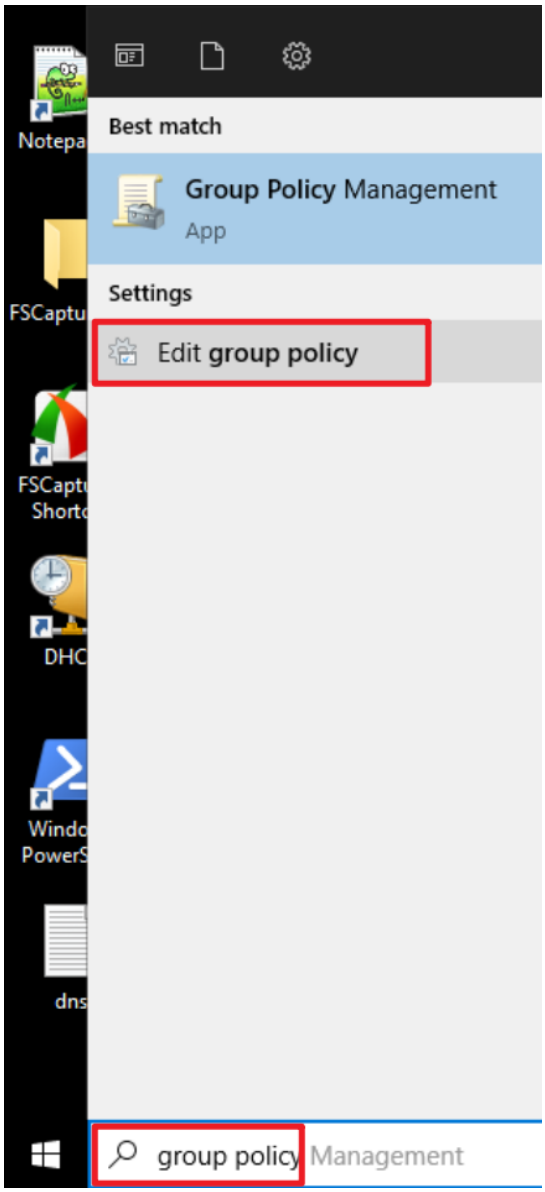


8.2 Workgroup

8.2.1 Audit Policy Configuration

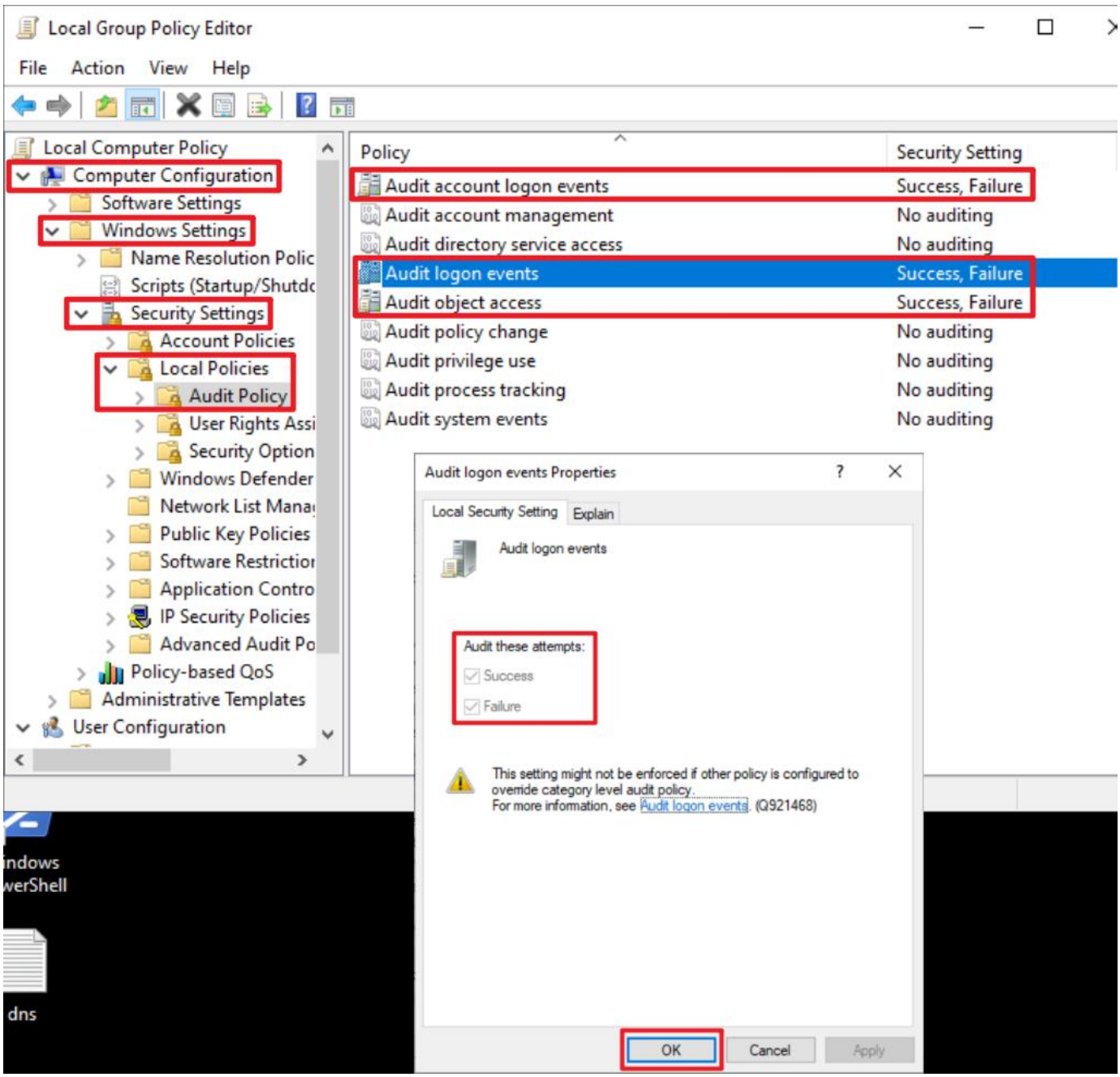
(1) Open Local Group Policy Editor

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



(2) Local Group Policies: Audit Policy

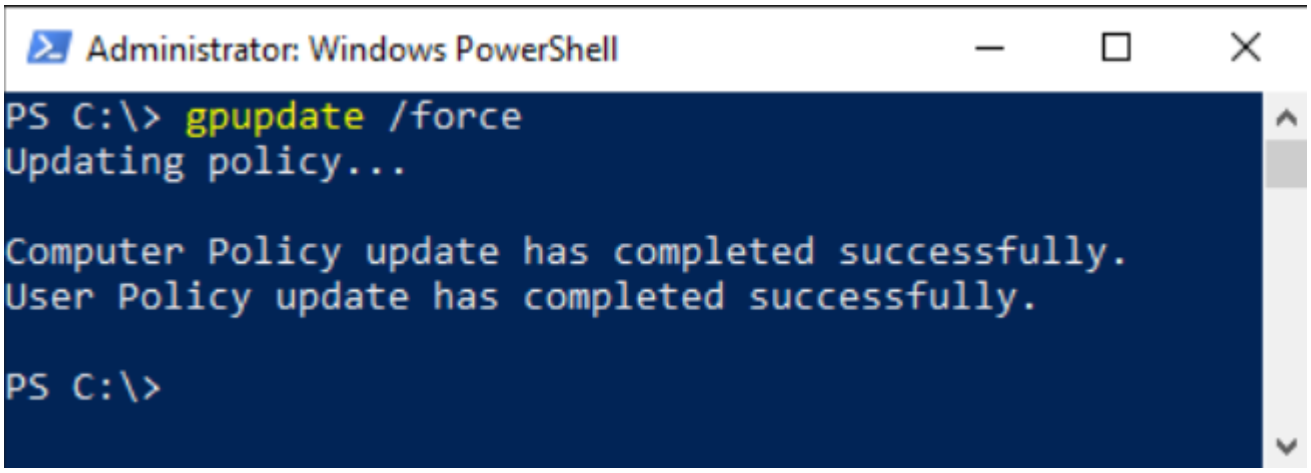
Expand folder “Computer Configuration” → “Windows Settings” → “Security Settings” -> “Local Policies” → “Audit Policy.” And click on “Audit account logon events,” “Audit logon events” and “Audit object access” items → check “Define these policy settings”: Success, Failure. → click “OK.”



(3) Open “Windows PowerShell.”

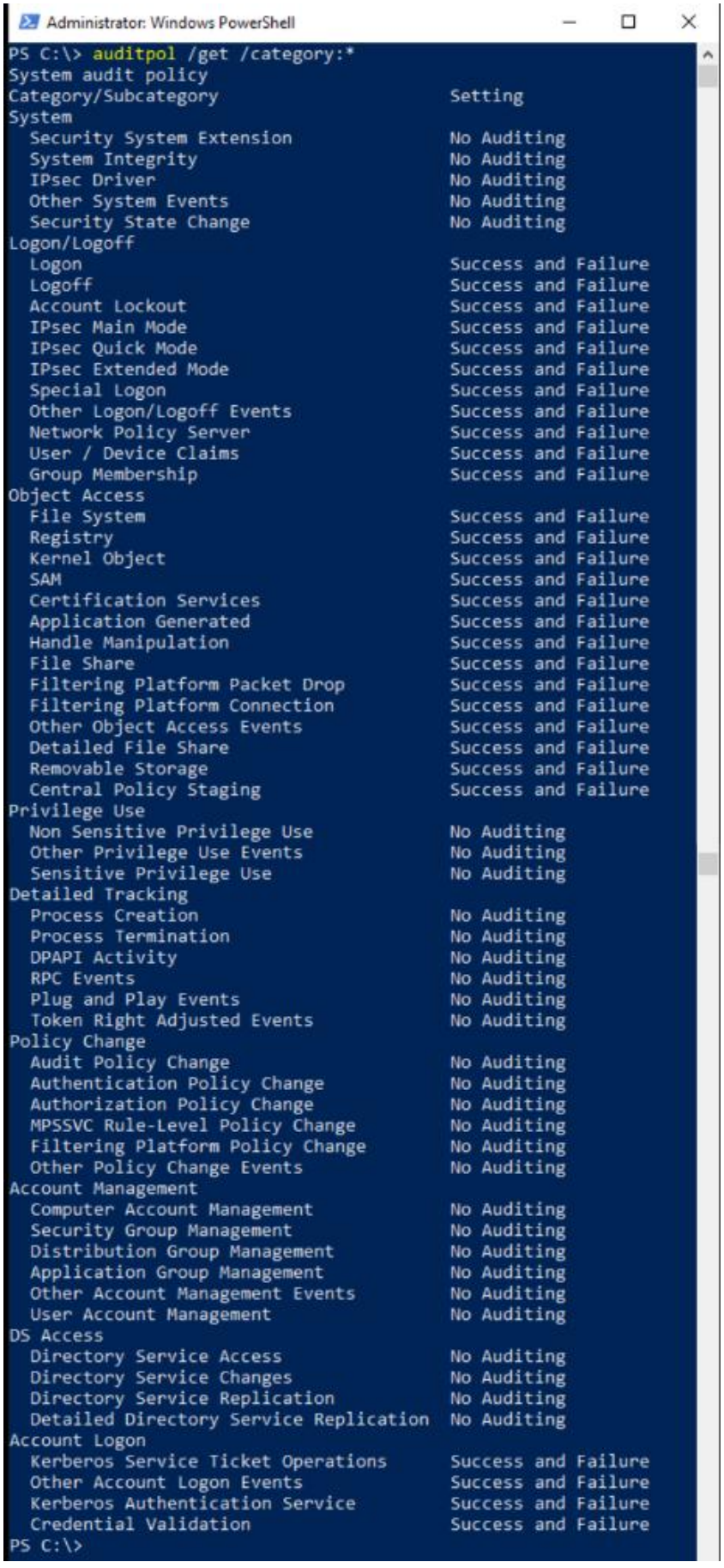
(4) Enter the command below to refresh group policy.

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



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

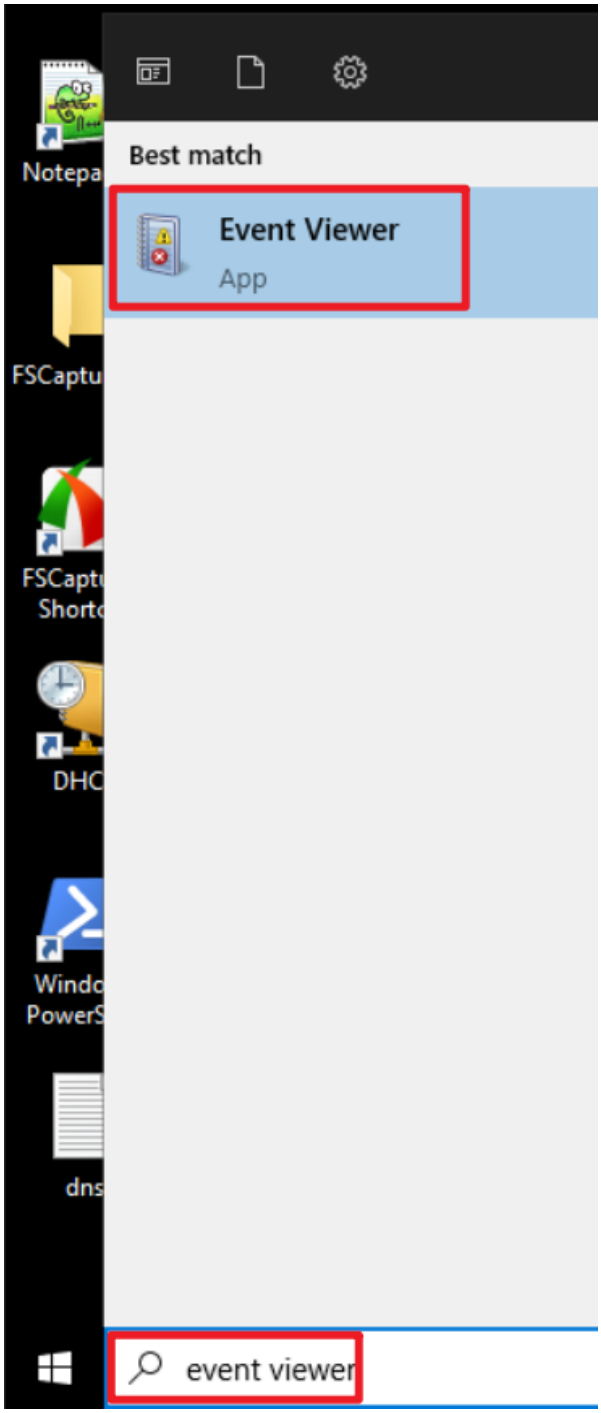
```
PS C: \> auditpol /get /category:*
```



8.2.2 Event Log Settings

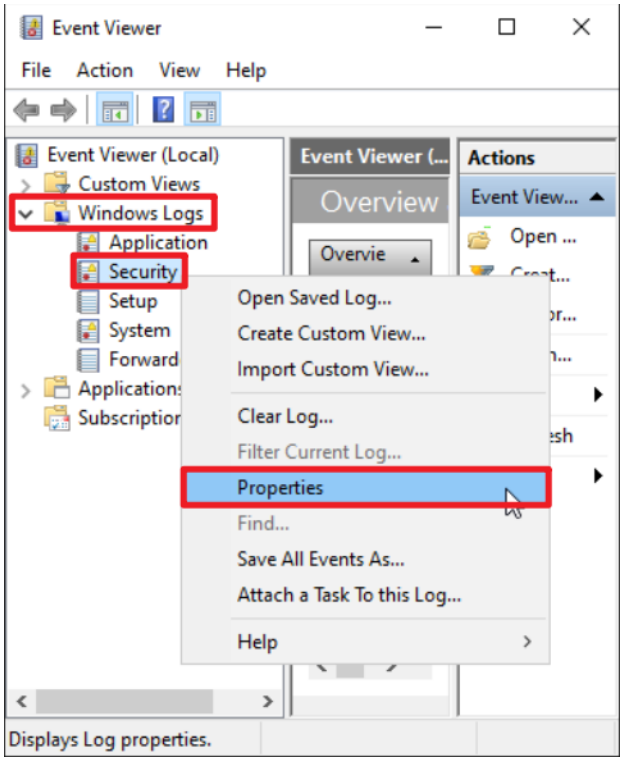
(1) Search for “Event Viewer”

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.”

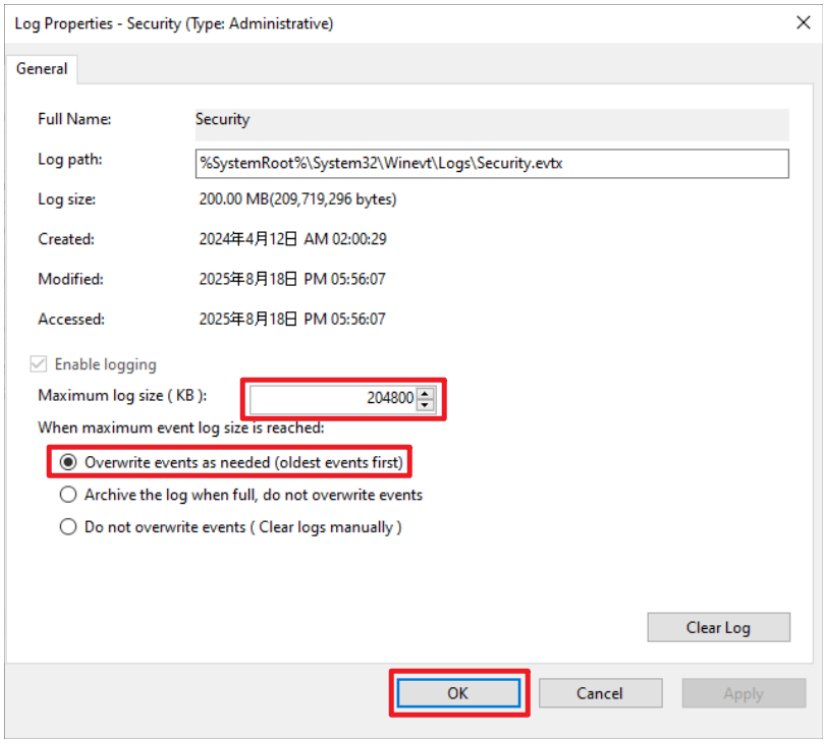


(3) Configure Security Log

Enter maximum log file size: 204800 KB

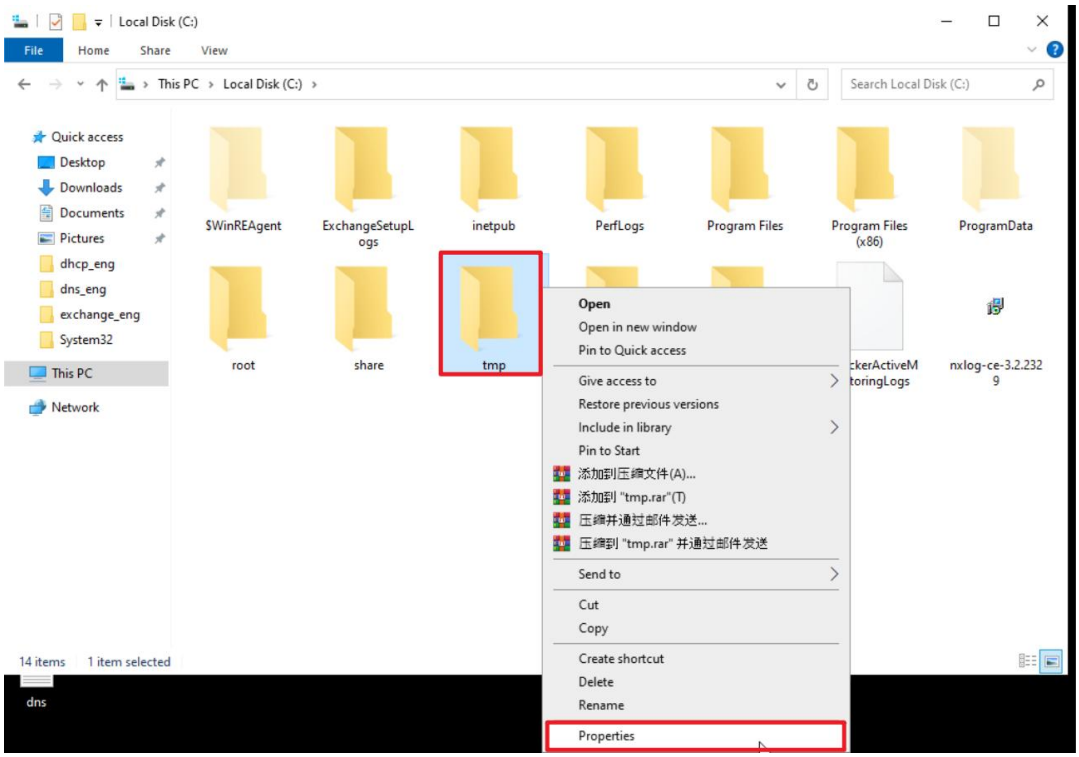
Note: Please adjust the number according to the actual environment.

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

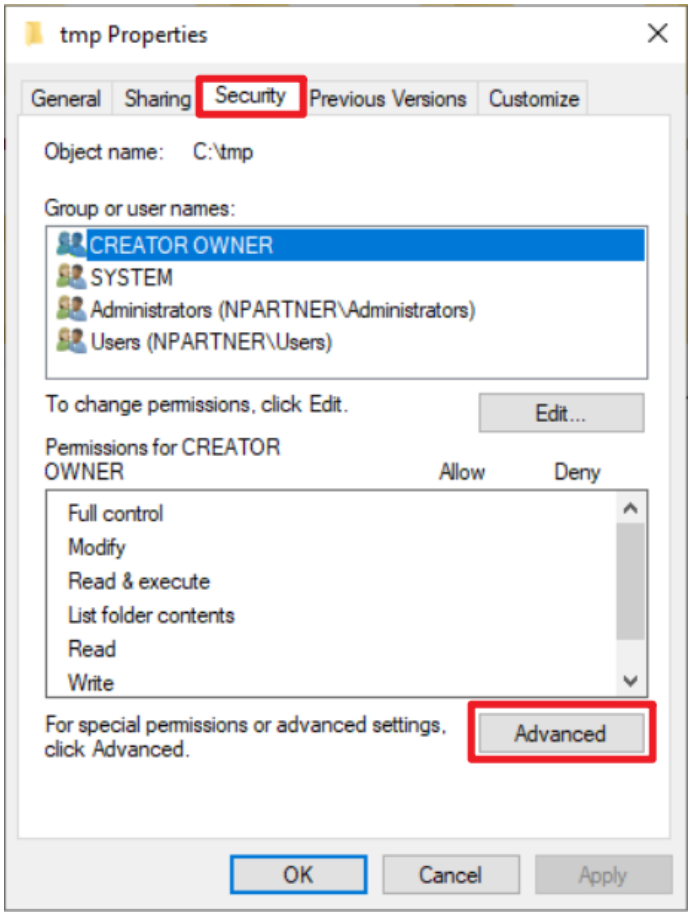


8.3 Folder Audit Configuration

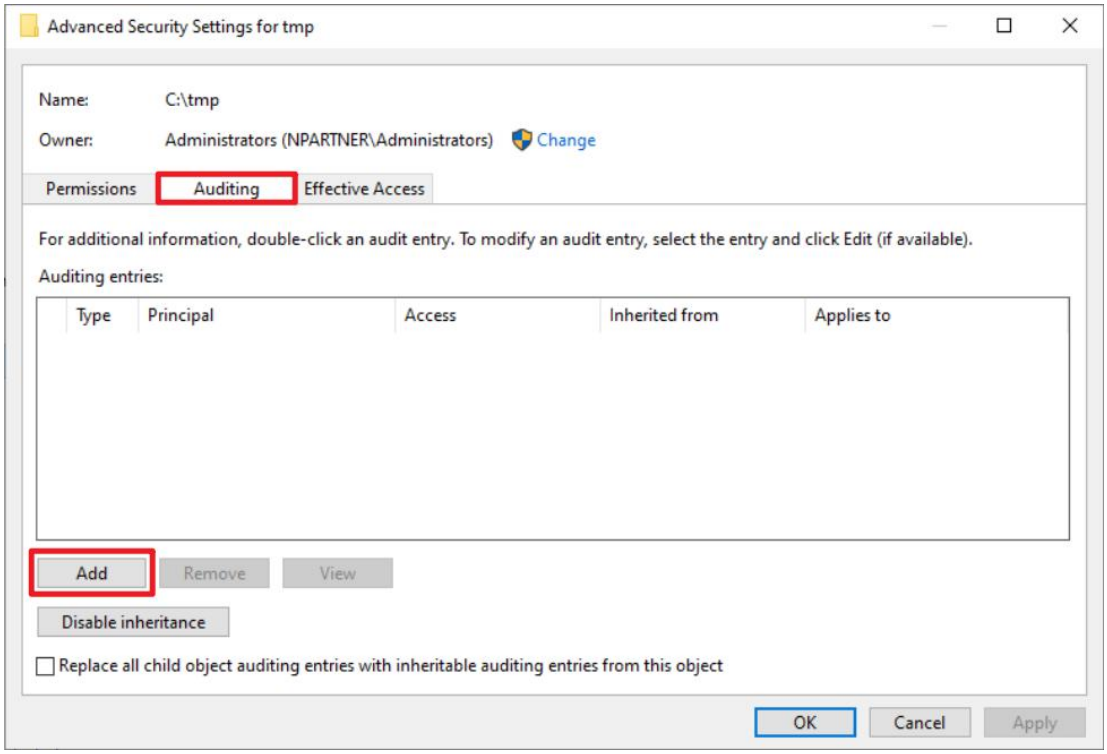
(1) Right-click the target folder to be audited (the example here is tmp) → select “Properties.”



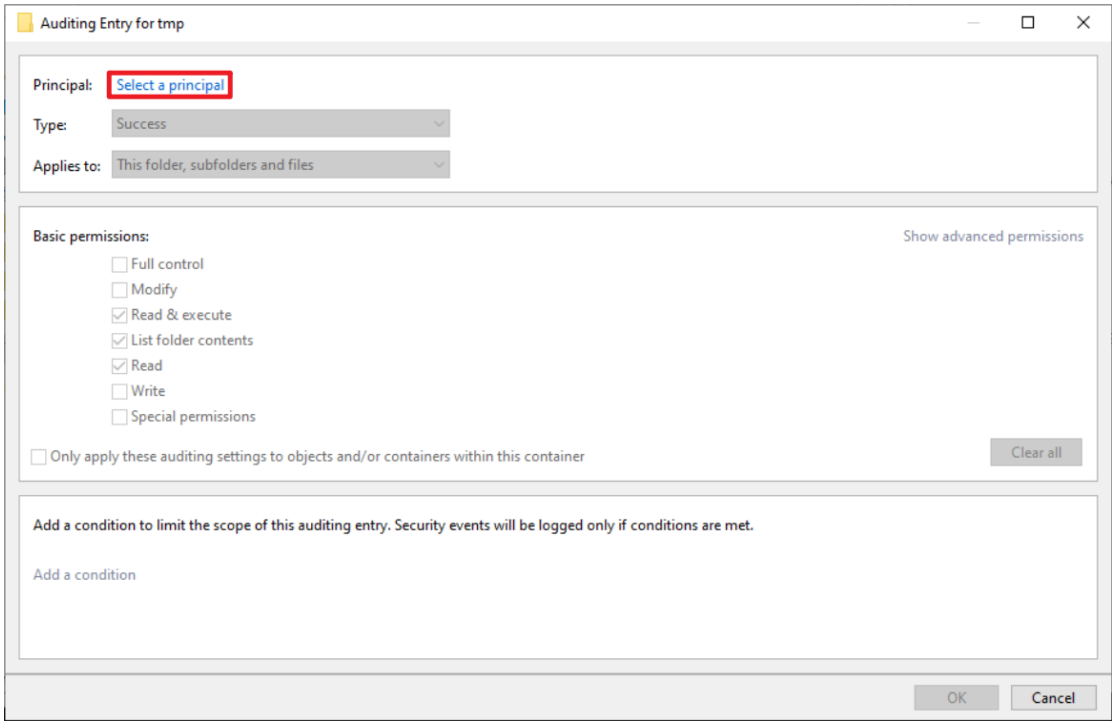
(2) Go to the “Security” tab → click “Advanced.”



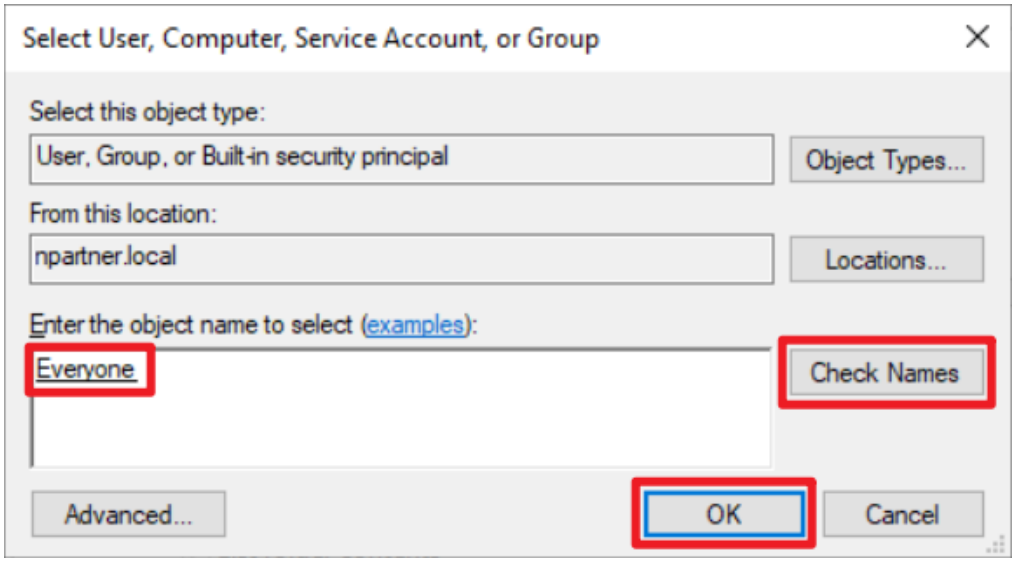
(3) Open the “Auditing” tab → click “Add.”



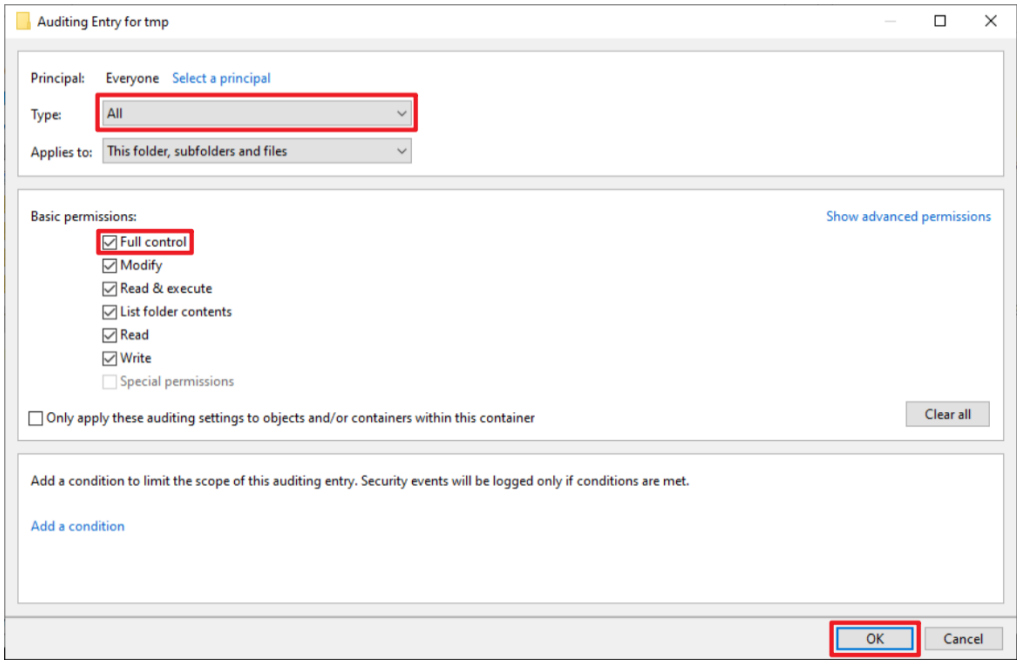
(4) Click “Select a principal.”



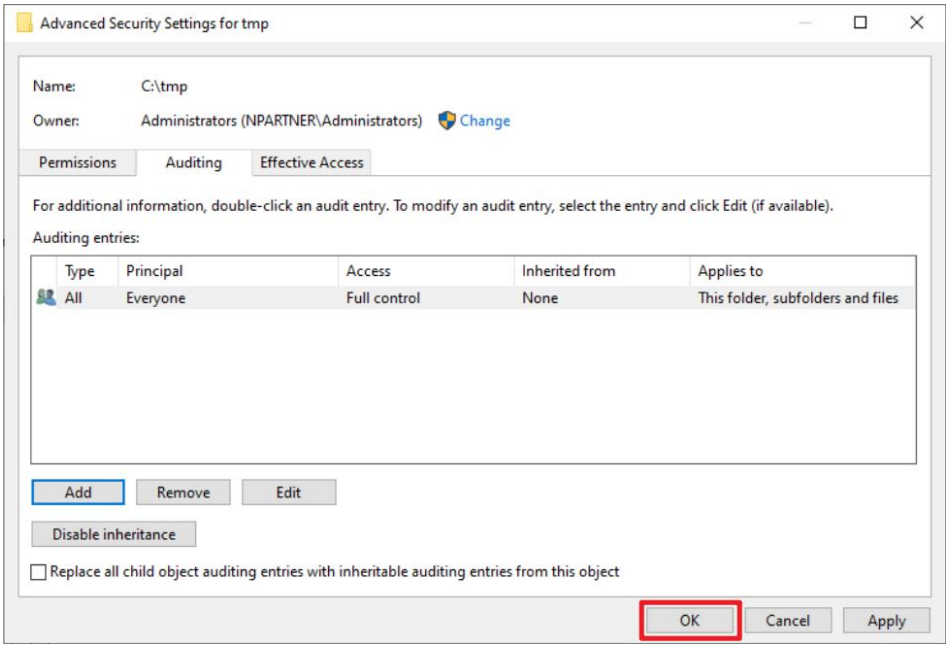
(5) In the object name field, enter “Everyone” to audit all users → click “Check Names” → click “OK.”



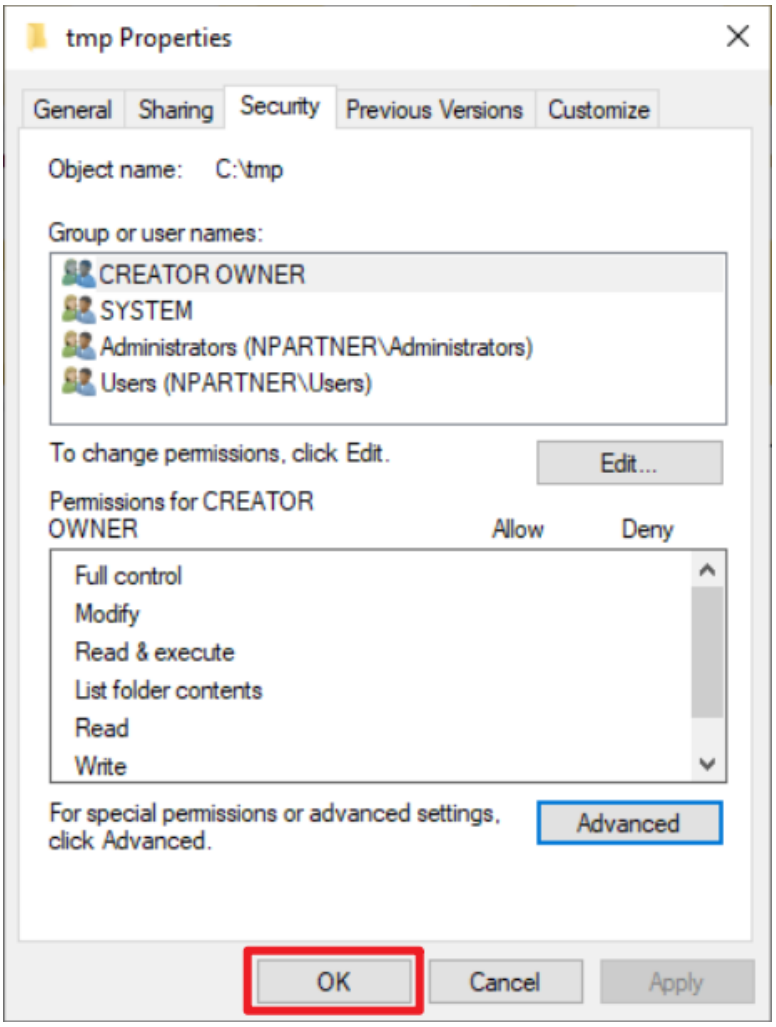
(6) Select “All” in type → enable “Full Control” → click “OK.”



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



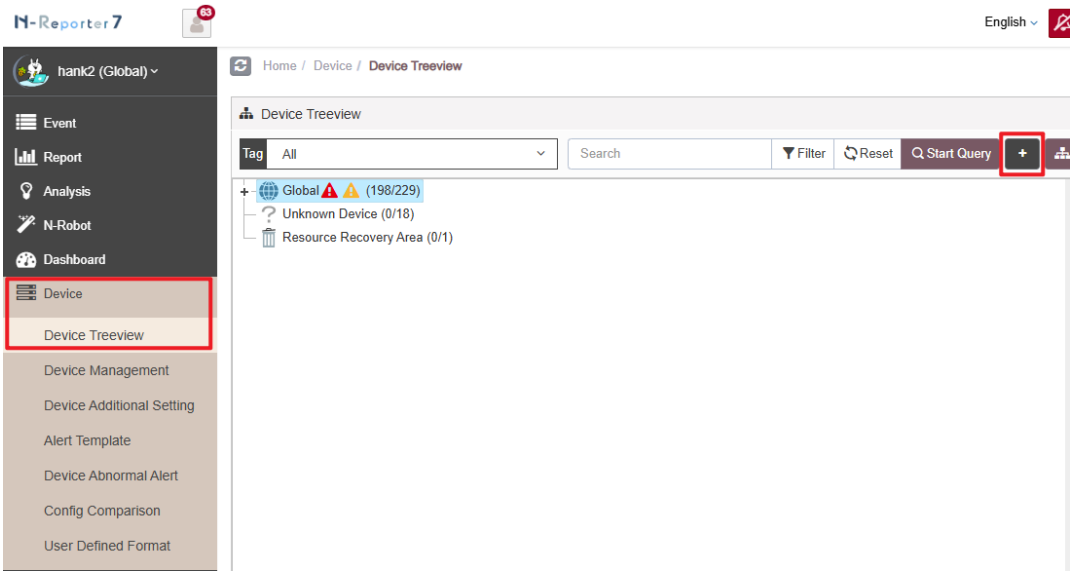
(8) Click “OK” again to confirm and close.



9. N-Reporter

(1) Add a Windows WINDOWS FILE device:

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



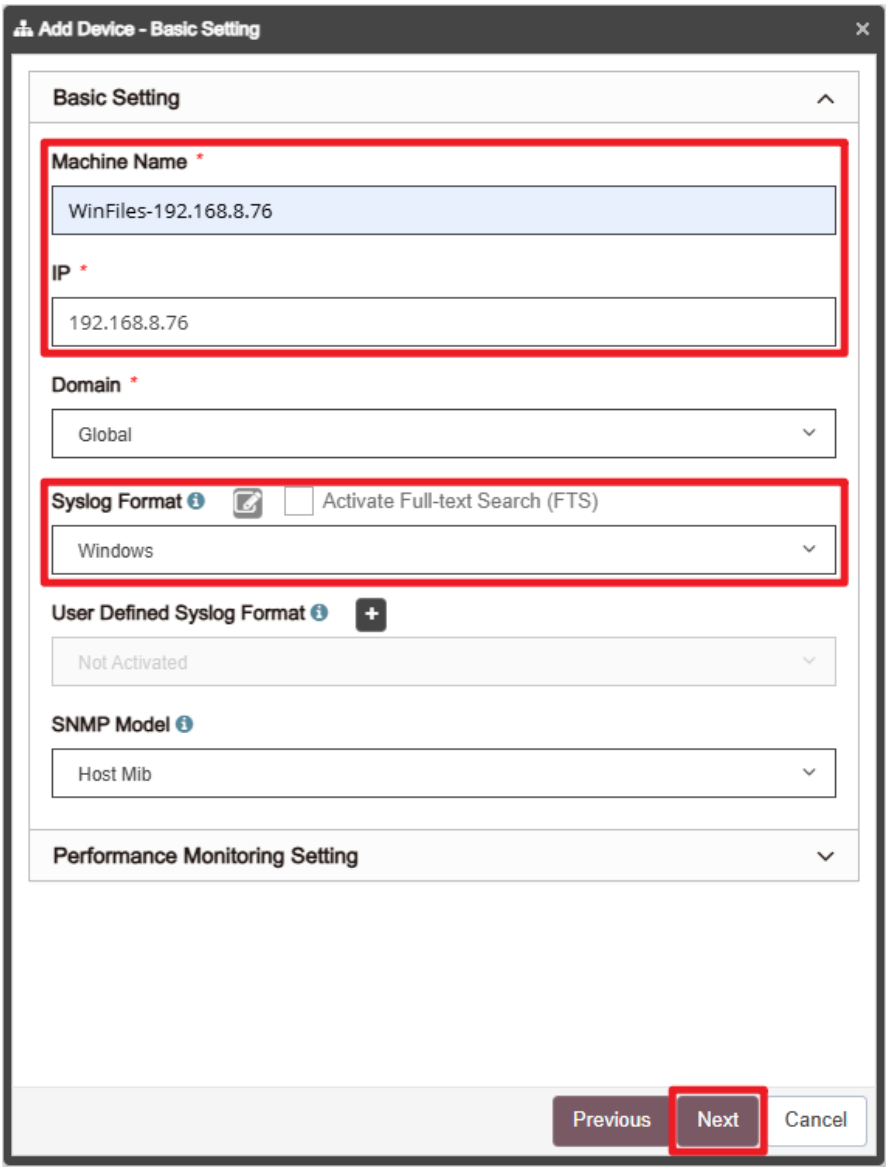
(2) Select the device type:

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

9.1 For Windows Server 2003 or earlier

(1) Basic Device Settings:

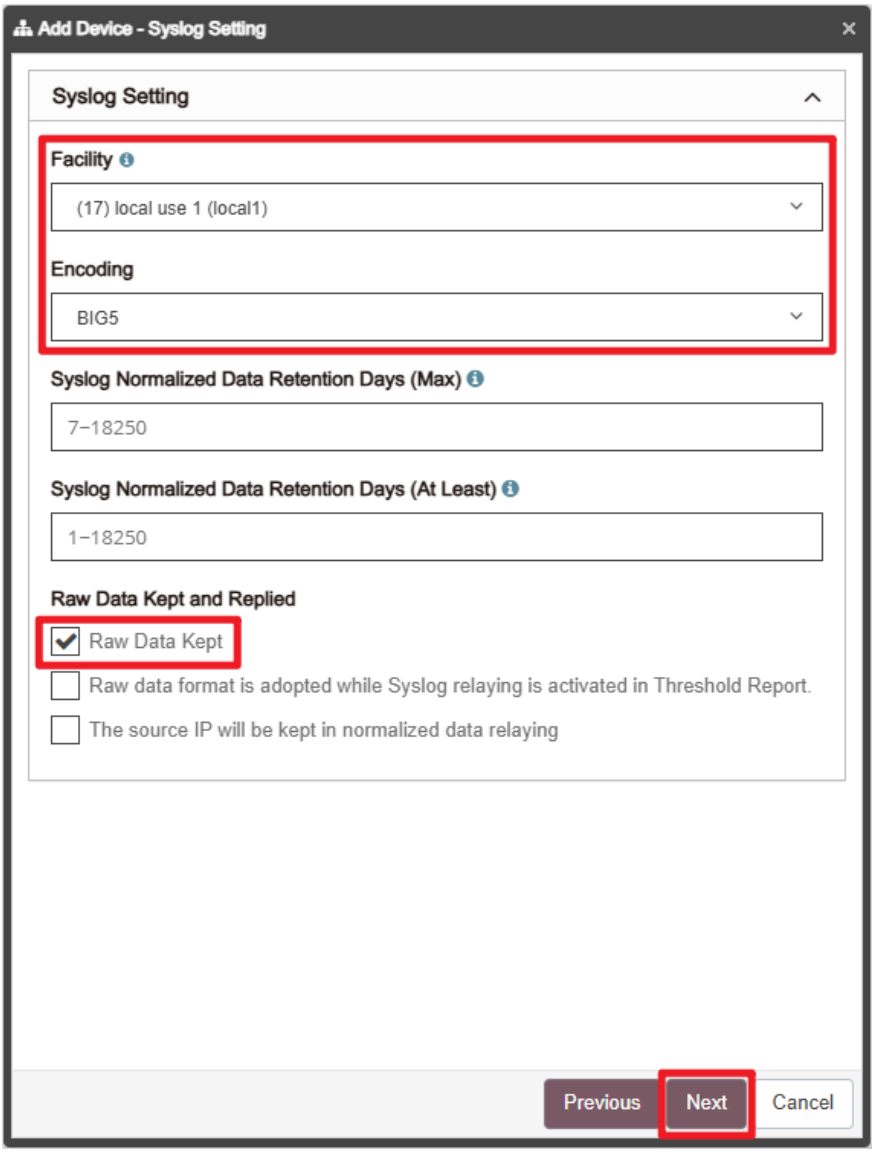
Enter the device name and IP address → For Syslog Data Format, select “Windows” → click “Next.”



(2) Syslog Settings

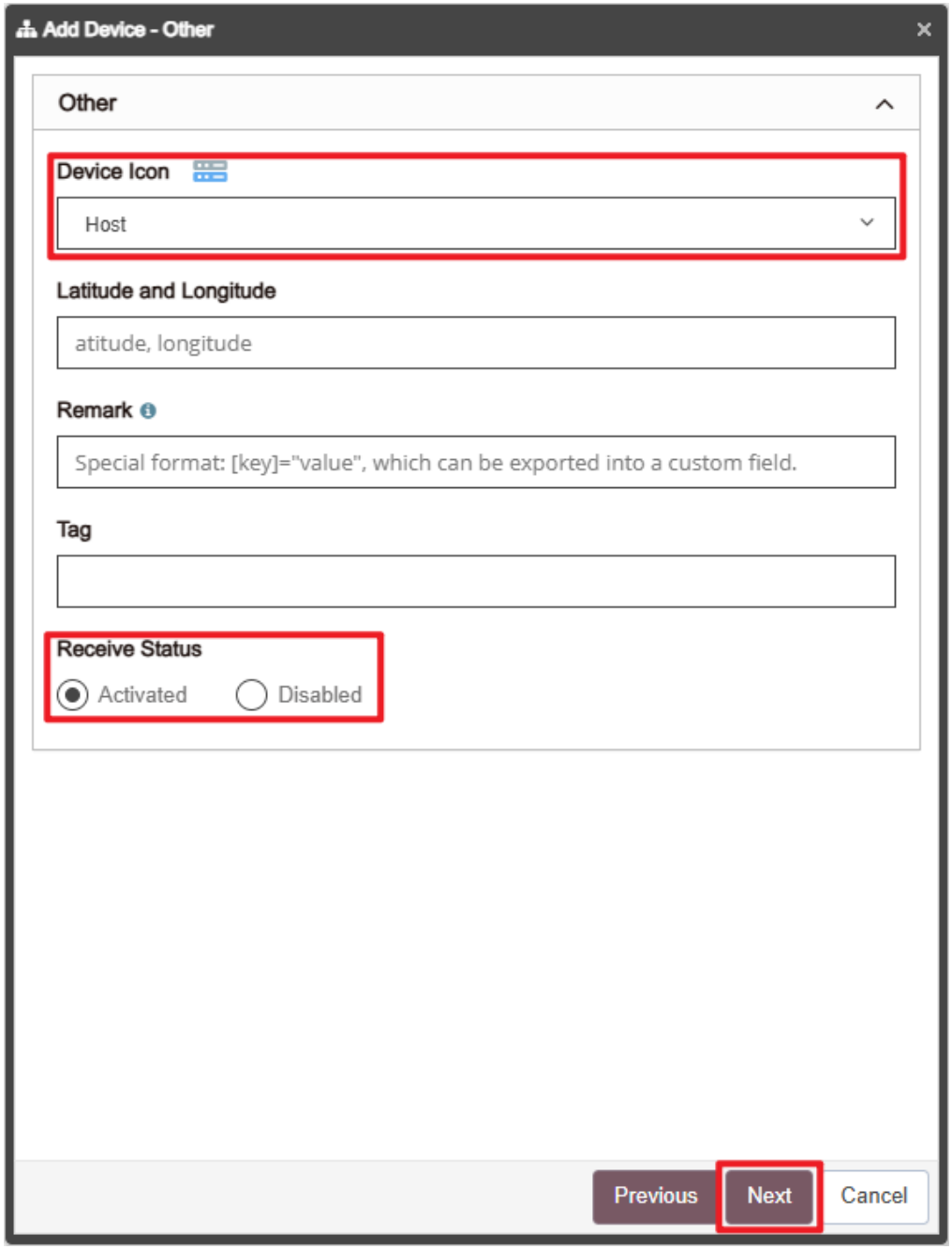
Set “Facility” to “(18) local use 2 (local2)” and “Encoding” to “BIG5” → click “Next.”

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

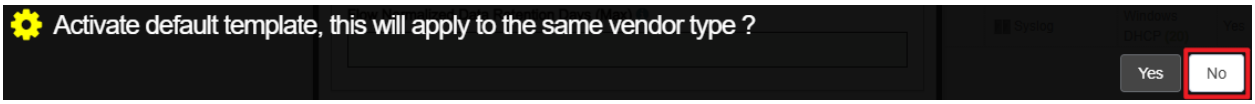


(3) Others

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



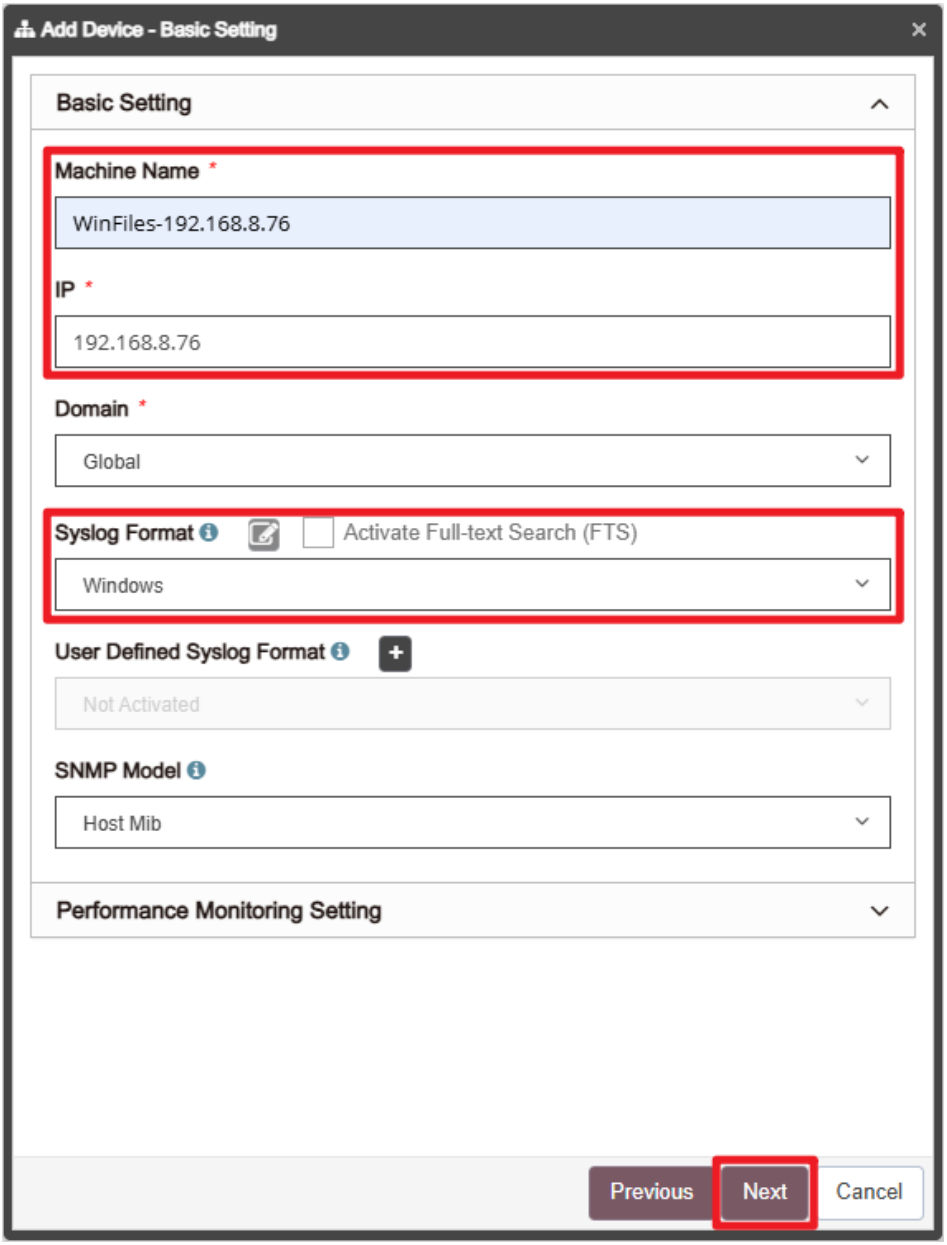
Activate default templates for devices of the same vendor type, click “No.”



9.2 For Windows 2008 or later

(1) Device Basic Settings

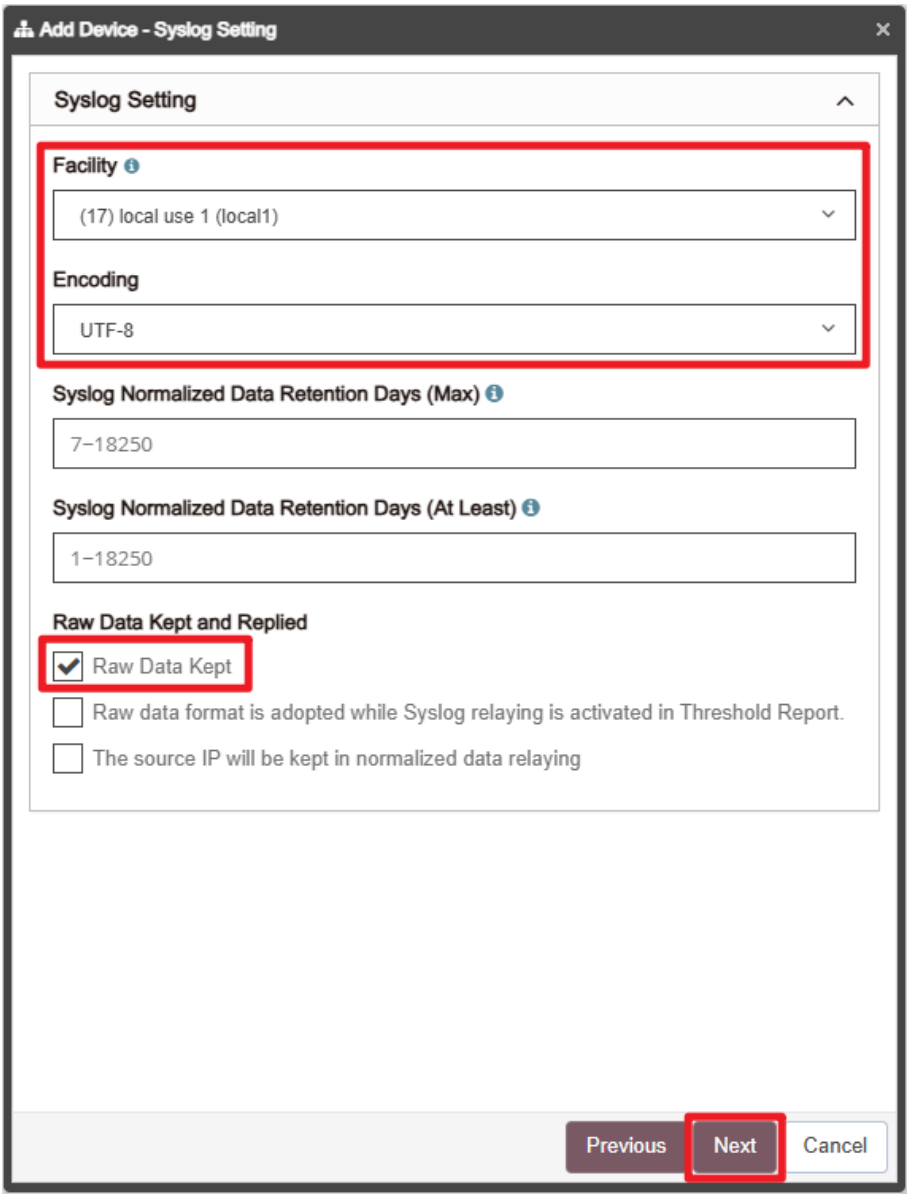
Enter the device name and IP → Select “Windows” for the Syslog data format → Click “Next.”



(2) Syslog Settings

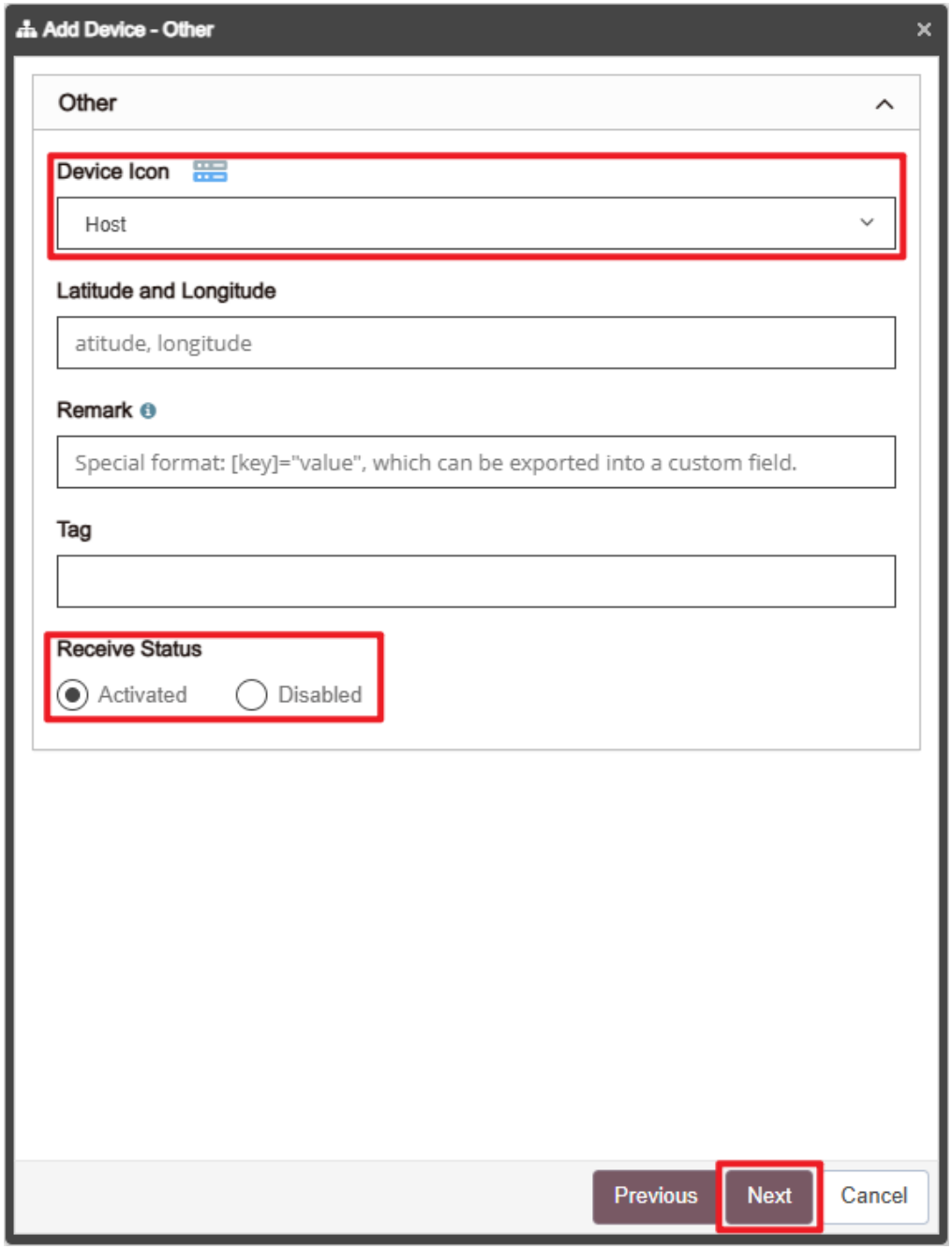
Set “Facility” to “(17) local use 1 (local1)” and “Encoding” to “UTF-8” → click “Next.”

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

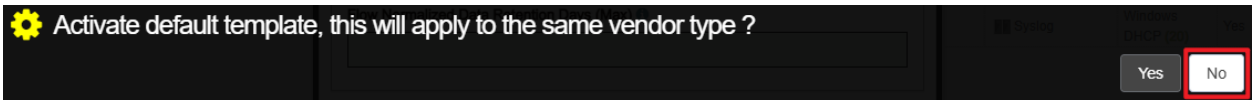


(3) Others

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



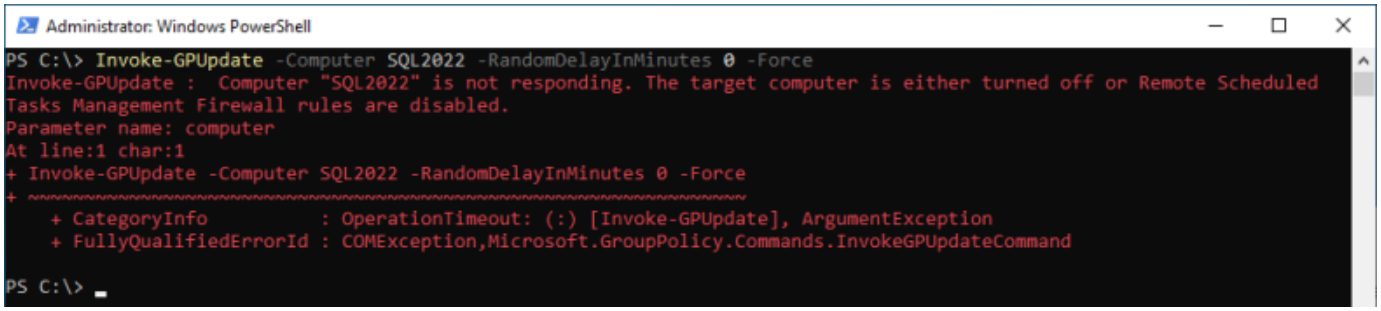
Activate default templates for devices of the same vendor type, click “No.”



10. Troubleshooting

10.1 Invoke-GPUpdate Error

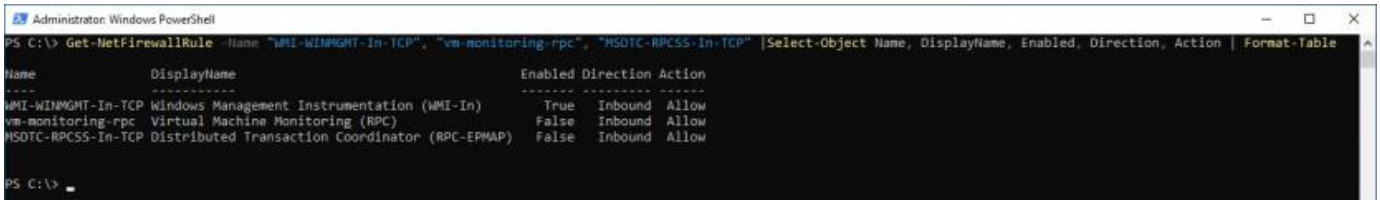
(1) On the server, run Invoke-GPUpdate to update the Windows Server Group Policy. An error message may appear.



(2) On the Windows Server, open “Windows PowerShell.”

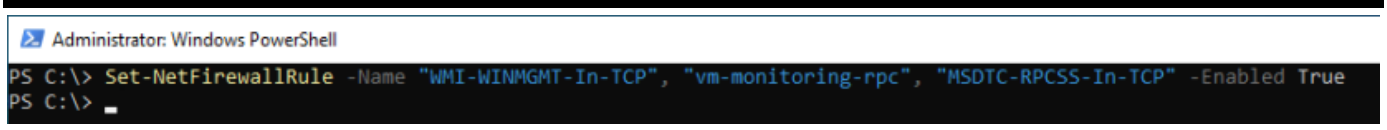
(3) Enter the following command to check the Windows Firewall rules for **WMI-WINMGMT-In-TCP, vm-monitoring-rpc, MSDTC-RPCSS-In-TCP:**

```
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
```



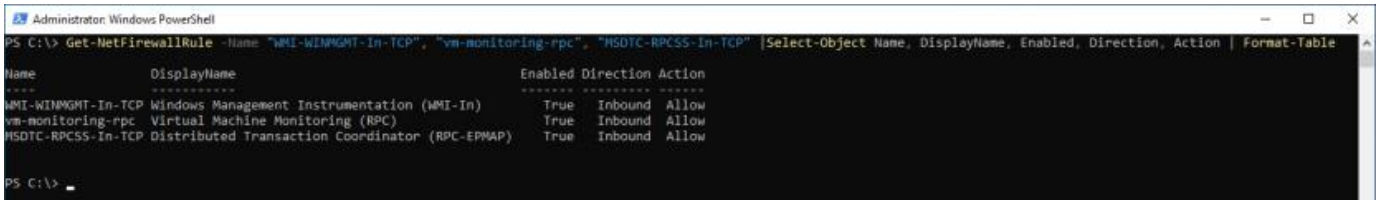
(4) Enter the following command to enable the Windows Firewall rules **WMI-WINMGMT-In-TCP**, **vm-monitoring-rpc**, and **MSDTC-RPCSS-In-TCP**:

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



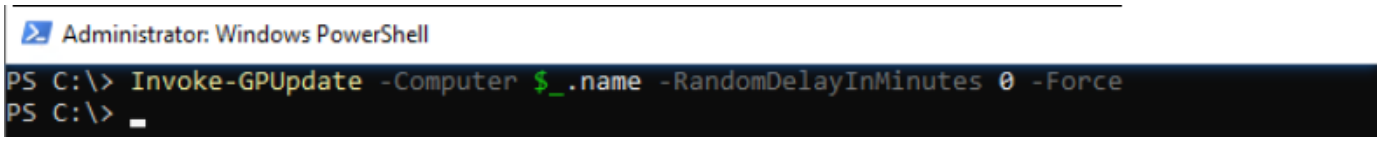
(5) Enter the following command to verify the Windows Firewall rules **WMI-WINMGMT-In-TCP, vm-monitoring-rpc, MSDTC-RPCSS-In-TCP** again:

```
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
```



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

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



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