N-Partner

Manage Windows AD Server Syslog with NXLOG

V014

2024/08/21

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 user can use open source tool, NXLOG, to manage Windows AD Server 2000/2003/2008/2012/2016/2019/2022 log (eventlog), transfer events to Syslog, and then forward them to N-Reporter for normalization, audit, and analysis.

The environments in the document are Windows Server 2000 AD, Windows Server 2003 AD, Windows Server 2008 AD, Windows Server 2012 AD, Windows Server 2016 AD, Windows Server 2019 AD and Windows Server 2022 AD.

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

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

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

Note: This document serves only as a reference for configuring log output. It is recommended that you still contact the manufacturer of the device or software for assistance with setting up log output.

1. NXLog

1.1 Configure NXLOG in Windows Server AD

(1) Download NXLOG CE (Community Edition)

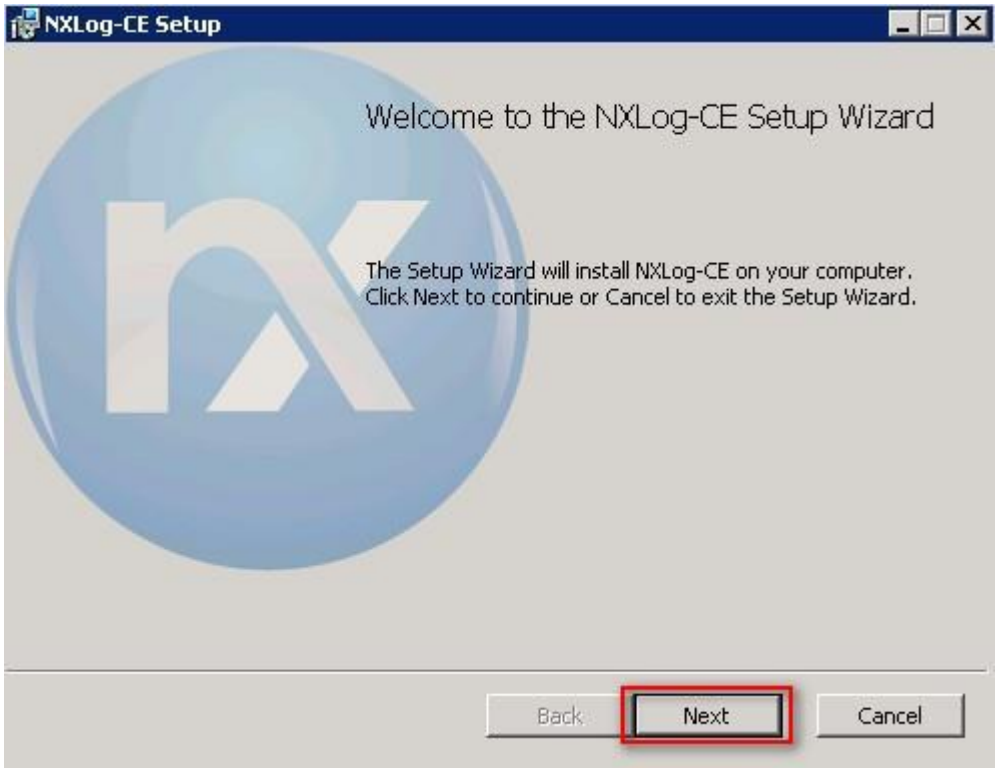
Go to URL: https://nxlog.co/products/nxlog-community-edition/download

Download the latest nxlog-ce-x.x.xxxx.msi; here, it's nxlog-ce-3.2.2329.msi.

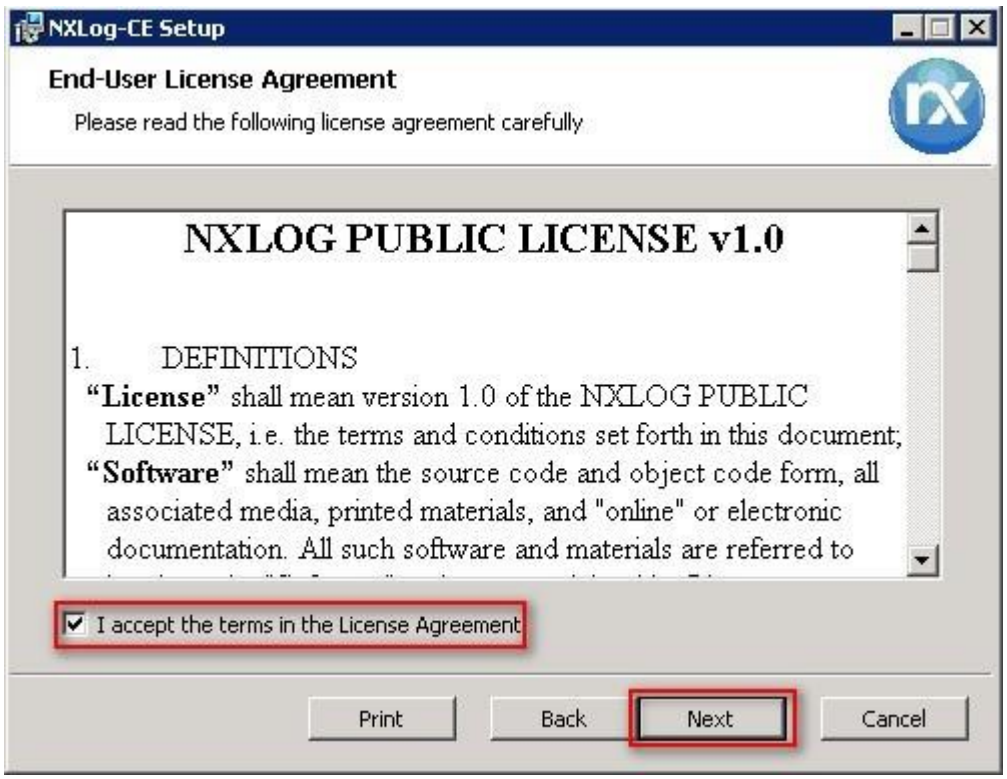
(2) Install NXLOG

<2.1> Windows 2008 or later operating systems

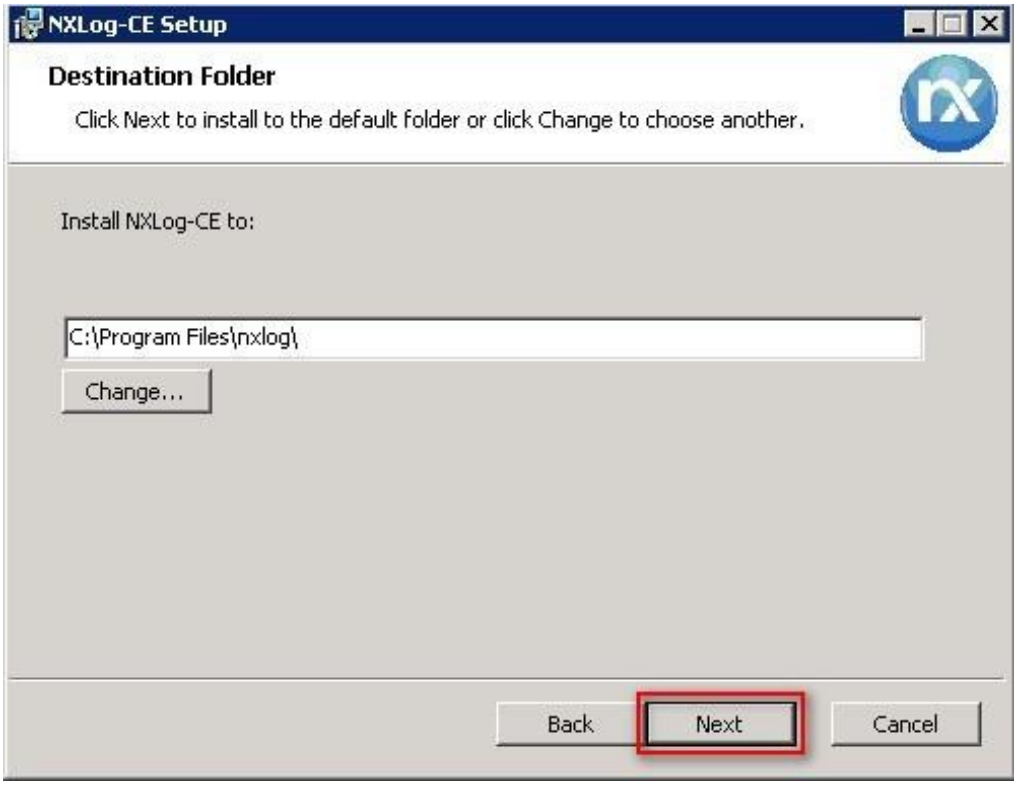
Click "nxlog-ce-3.2.2329.msi → Next."



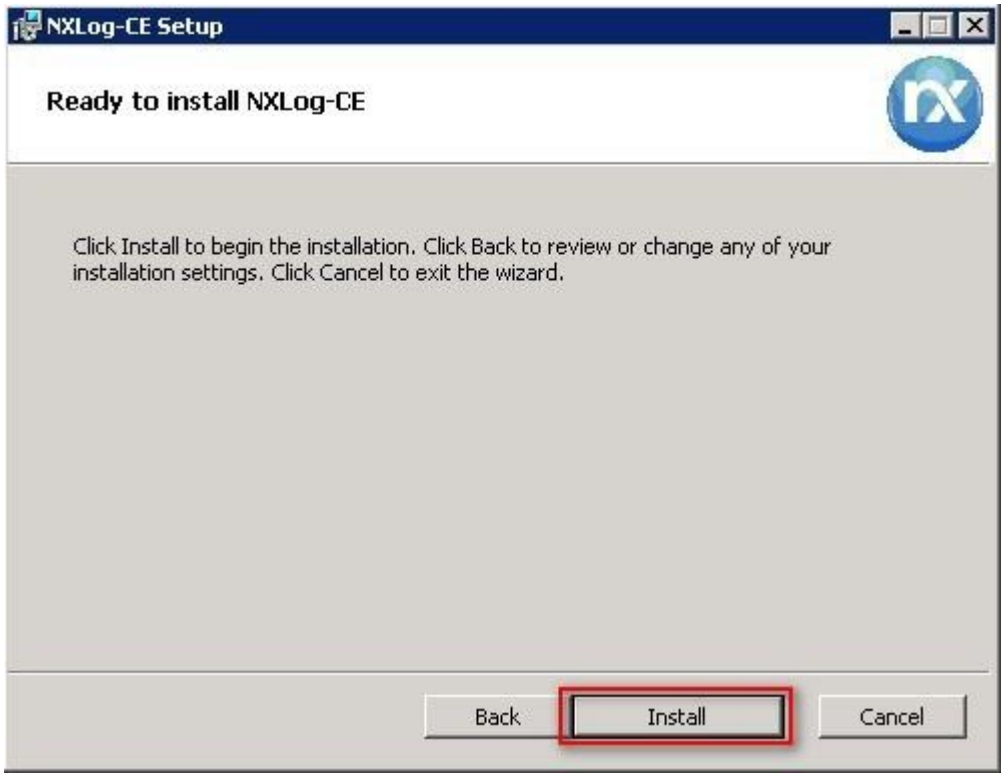
Check “I accept the terms in the License Agreement” and click “Next.”



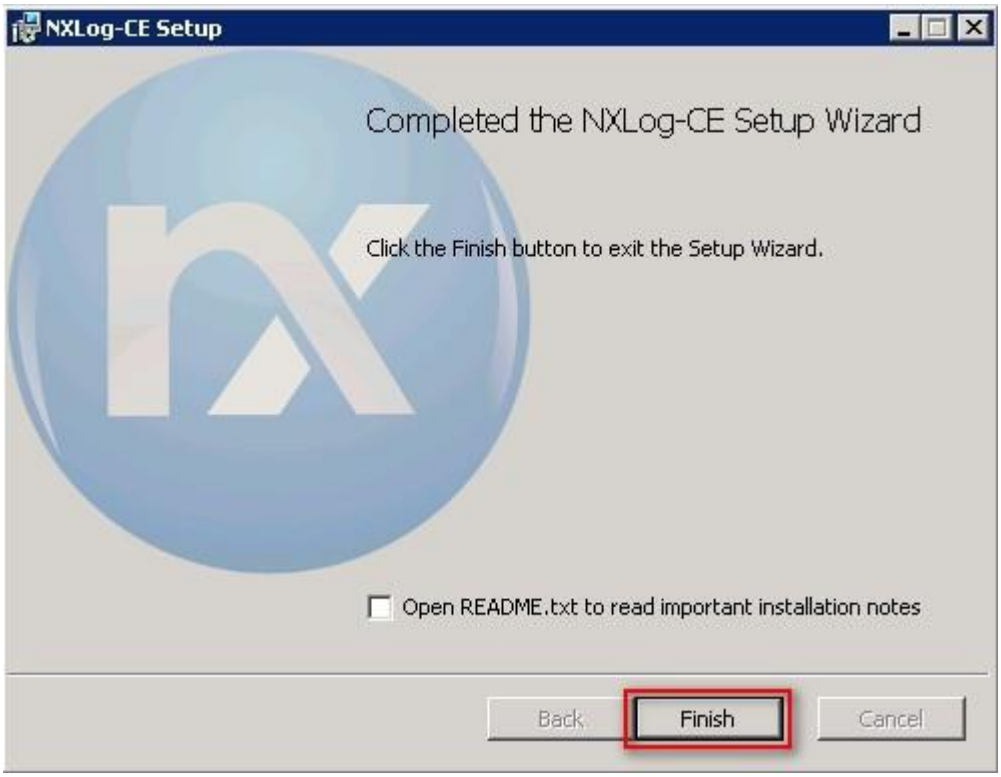
Click “Next.”



Click “Install.”

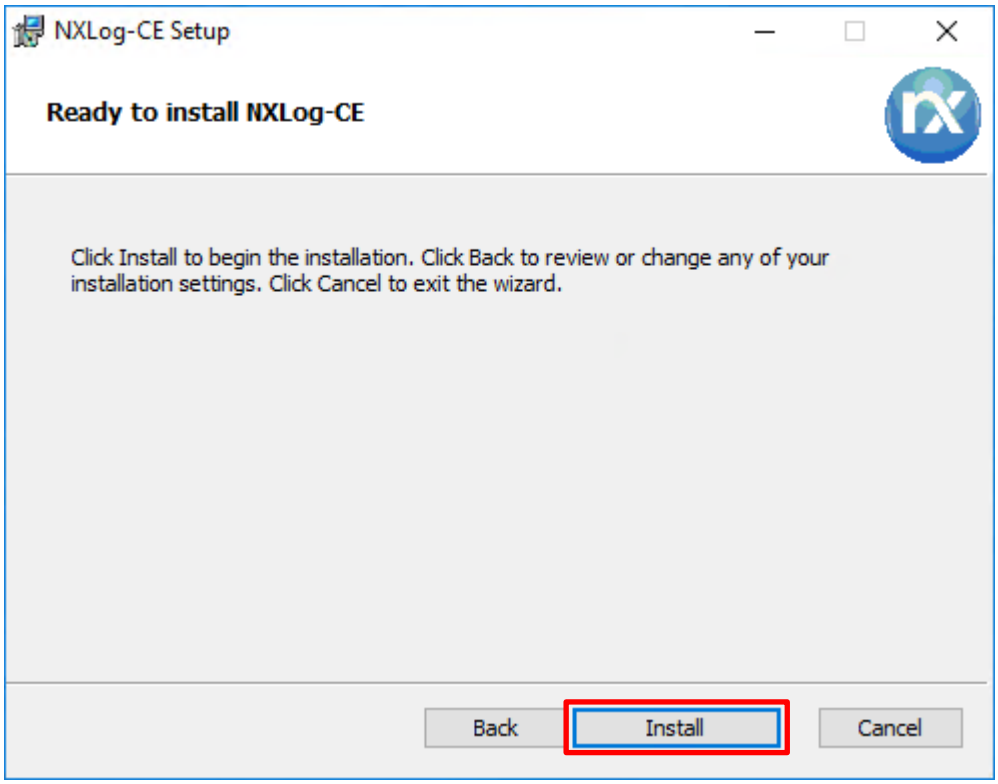


Click “Finish.”



<2.2> Windows 2003

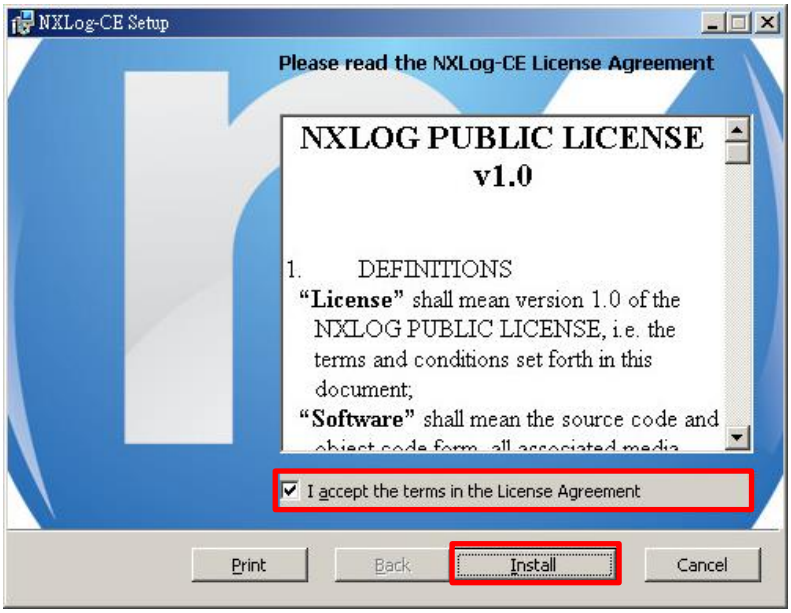
Click “nxlog-ce-3.2.2329.msi→Install→Finish.”



<2.3> Windows 2000

Go to the old version website of NXLog CE at https://sourceforge.net/projects/nxlog-ce/ . Click on “See All Activity” on the left side, then download NXLOG CE version that supports Windows 2000, which is nxlog-ce-2.8.1248.msi here.

Click “nxlog-ce-2.8.1248.msi” and check “I accept the terms in the License Agreement” then click “Install→ Finish.”

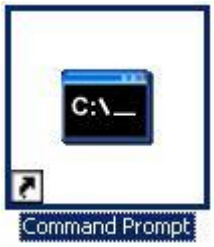


1.2 NXLog Configuration File Download

1.2.1 For Windows 2003 or Its Earlier Versions

1.2.1.1 Output Host Audit, Object Access, and Account Management Event Logs

(1) Click “Command Prompt.”



(2) Download NXLog Windows 2003 configuration file and overwrite the Windows system NXLog configuration file.

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

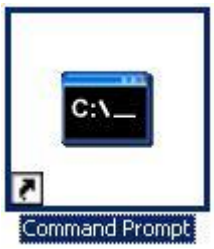
```
C:\ > copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
```

If the operating system is 64-bit, modify the following setting in red part: "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

Note: It is recommended to use this default setting. This configuration file only outputs event logs such as host audit, object access, and account management, thus reducing the burden on Windows Server performance.

1.2.1.2 Output All Event Logs

(1) Click “Command Prompt.”



(2) Download NXLog Windows 2003 configuration file and overwrite the Windows system NXLog configuration file

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

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

If the operating system is 64-bit, modify the following setting in red part: "C:\Program Files (x86)\nxlog\conf\nxlog.conf"

Note: This configuration file outputs all Windows event logs.

1.2.2 For Windows 2008 or Its Later Versions

1.2.2.1 Output Host Audit, Object Access, and Account Management Event Logs

(1) Click “Windows Powershell.”

(2) Download NXLog Windows 2008 configuration file and overwrite the Windows system NXLog configuration file

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

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

If the operating system is 64-bit, modify the following setting in red part: 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

Note: It is recommended to use this default setting. This configuration file only outputs event logs such as host audit, object access, and account management, thus reducing the burden on Windows Server performance.

1.2.2.2 Output All Event Logs for Applications, Security, and System

(1) Click “Windows PowerShell.”

(2) Download NXLog Windows 2008 configuration file and overwrite the Windows system NXLog configuration file.

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

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

If the operating system is 64-bit, modify the following setting in red part: 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

Note: This configuration file outputs all event logs for Windows applications, security, and system.

1.3 NXLog Configuration

1.3.1 For Windows 2003 or Its Earlier Versions

1.3.1.1 Output Host Audit, Object Access, and Account Management Event Logs

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

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

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

## Windows Server 2000 - 2003 Event Log use the following:
<Input in_eventlog>
   Module            im_mseventlog
   ReadFromLast TRUE
   SavePos           TRUE
   Exec    parse_syslog_bsd(); \
      if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or
$EventID == 538 or $EventID == 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID ==
624 or $EventID == 626 or $EventID == 627 or $EventID == 628 or $EventID == 629 or $EventID == 630 or
$EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635 or $EventID ==
636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 644 or
$EventID == 645 or $EventID == 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
      else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
      else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
      else\
      {\
         drop();\
      }
</Input>

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

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

Enter N-Reporter system IP address in blue part.

```
define NCloud      192.168.3.50
```

If the operating system is 64-bit, please change the setting to the following:

```
define ROOT        C:\Program Files\nxlog
```

1.3.1.2 Output All Event Logs

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

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

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

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

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

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

Enter N-Reporter system IP address in blue part.

```
define NCloud      192.168.3.50
```

If the operating system is 64-bit, please change the setting to the following:

```
define ROOT        C:\Program Files\nxlog
```

1.3.2 For Windows 2008 or Its Later Versions

1.3.2.1 Output Host Audit, Object Access, and Account Management Event Logs

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

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

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

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

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

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

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

Enter N-Reporter system IP address in blue part:

```
define NCloud      192.168.3.50
```

If the operating system is 64-bit, please change the setting to the following:

```
define ROOT        C:\Program Files\nxlog
```

1.3.2.2 Output All Event Logs for Applications, Security, and System

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

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

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

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

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

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

Enter N-Reporter system IP address in blue part:

```
define NCloud      192.168.3.50
```

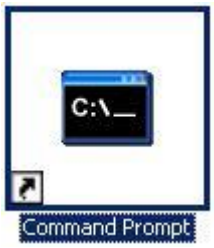
If the operating system is 64-bit, please change the setting to the following:

```
define ROOT        C:\Program Files\nxlog
```

1.4 NXLog Startup

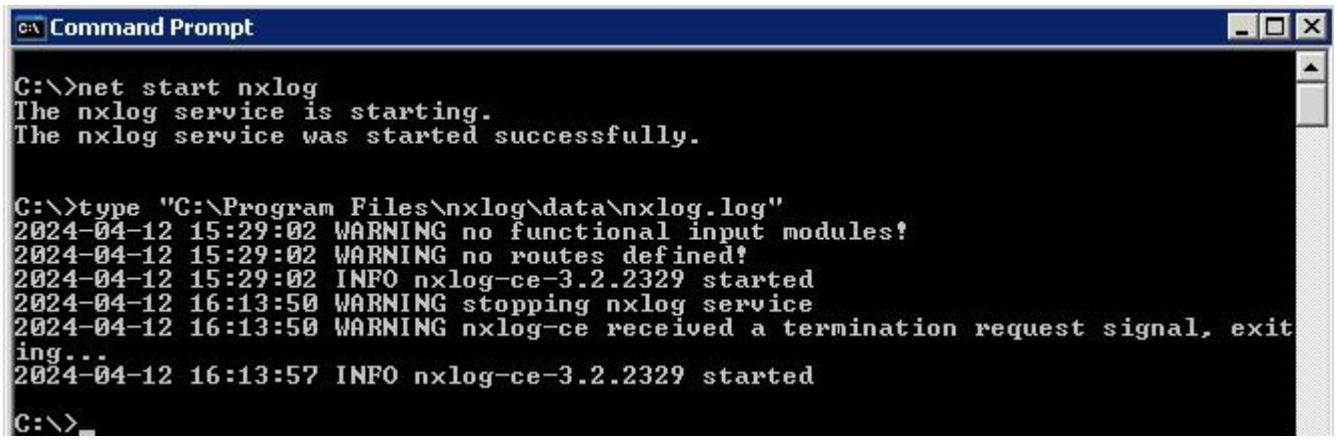
1.4.1 For Windows 2003 or Its Earlier Versions

(1) Click “Command Prompt.”



(2) Start NXLog and verify that there are no error messages from NXLog.

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

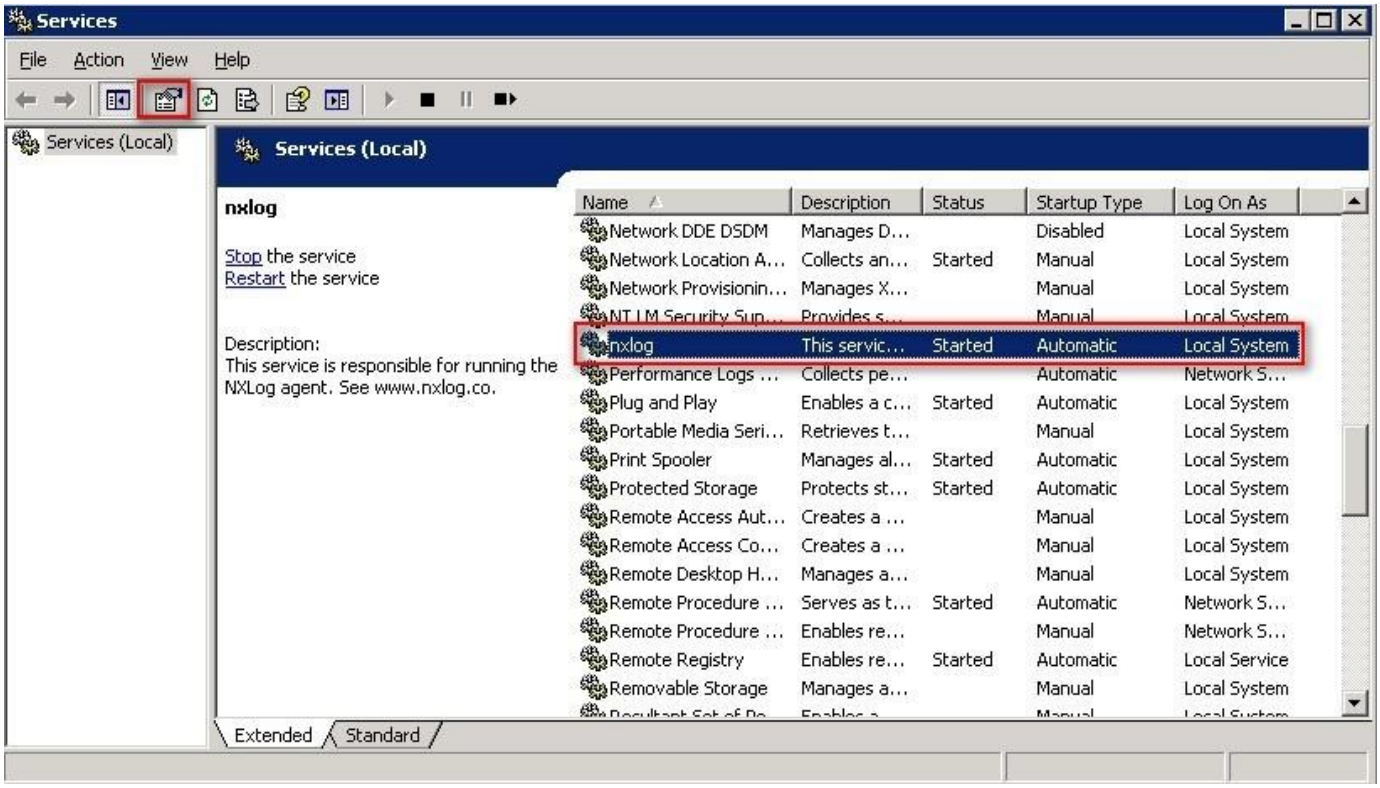


(3) Enter the following blue part to enable the service.

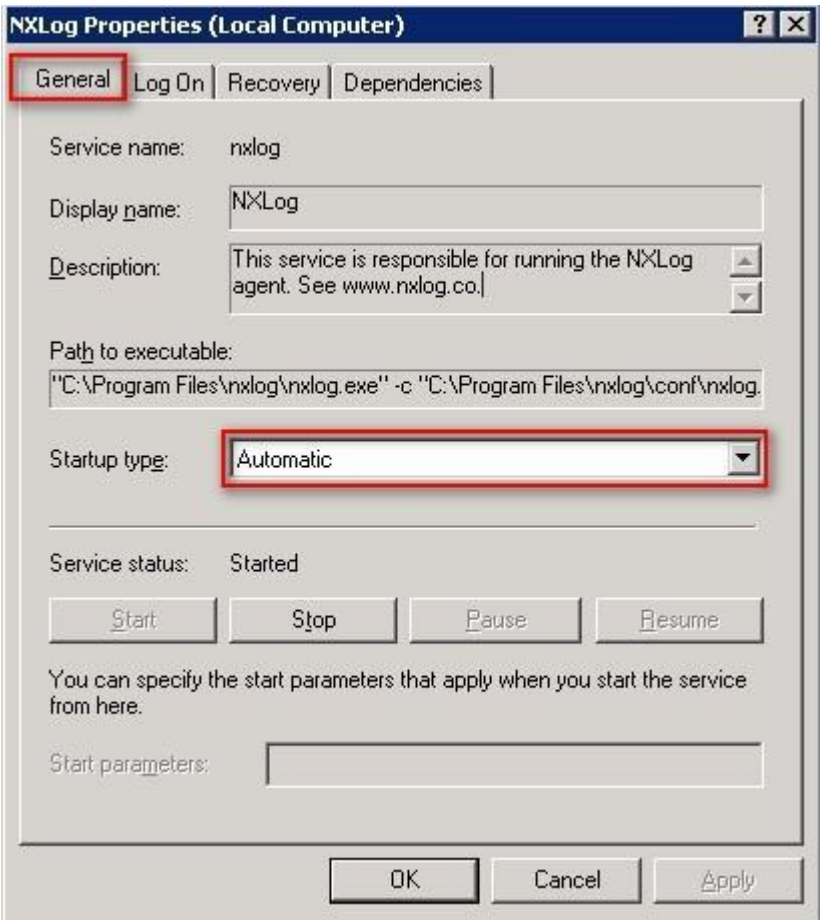
```
C:\> Services.msc
```

(4) Open NXLog Service

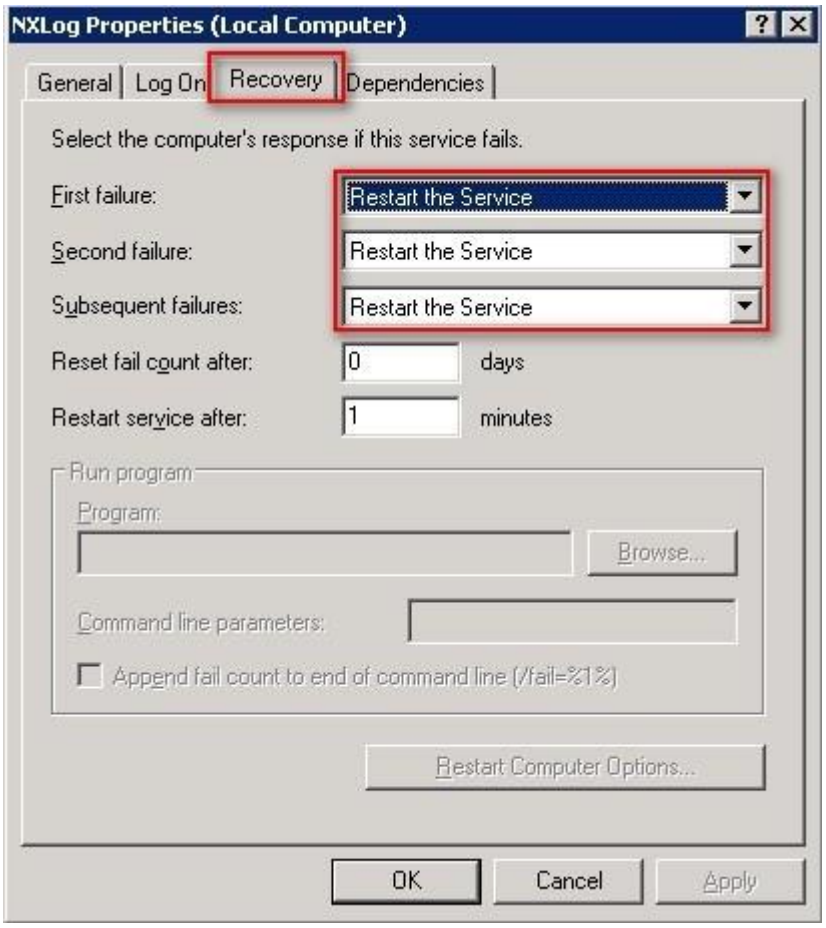
Please select “nxlog” and click  .



(5) Select “Automatic” of “Startup type” in “General.”



(6) Select “Restart the Service” of “First, Second and Subsequent Failures” in “Recovery” and click “OK”



1.4.2 For Windows 2008 or Its Later Versions

(1) Click “Windows PowerShell.”

(2) Restart NXLog and check for any errors.

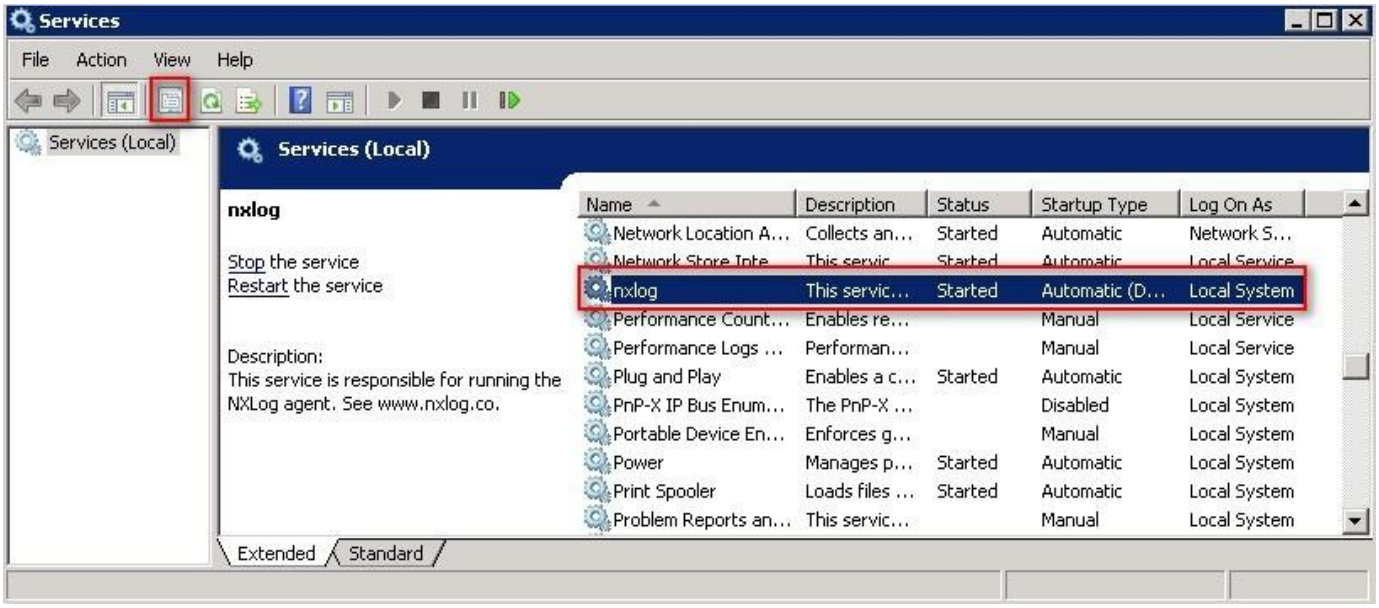
```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```

(3) Enter the following blue part to enable the service.

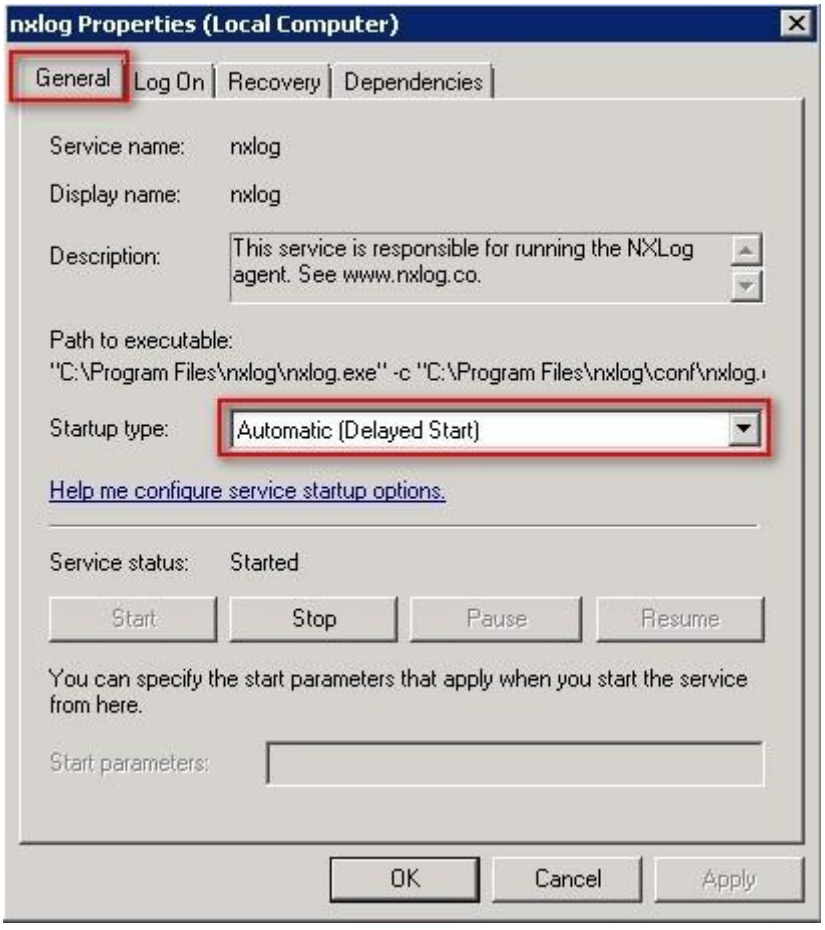
```
PS C:\> Services.msc
```

(4) Open NXLog Service

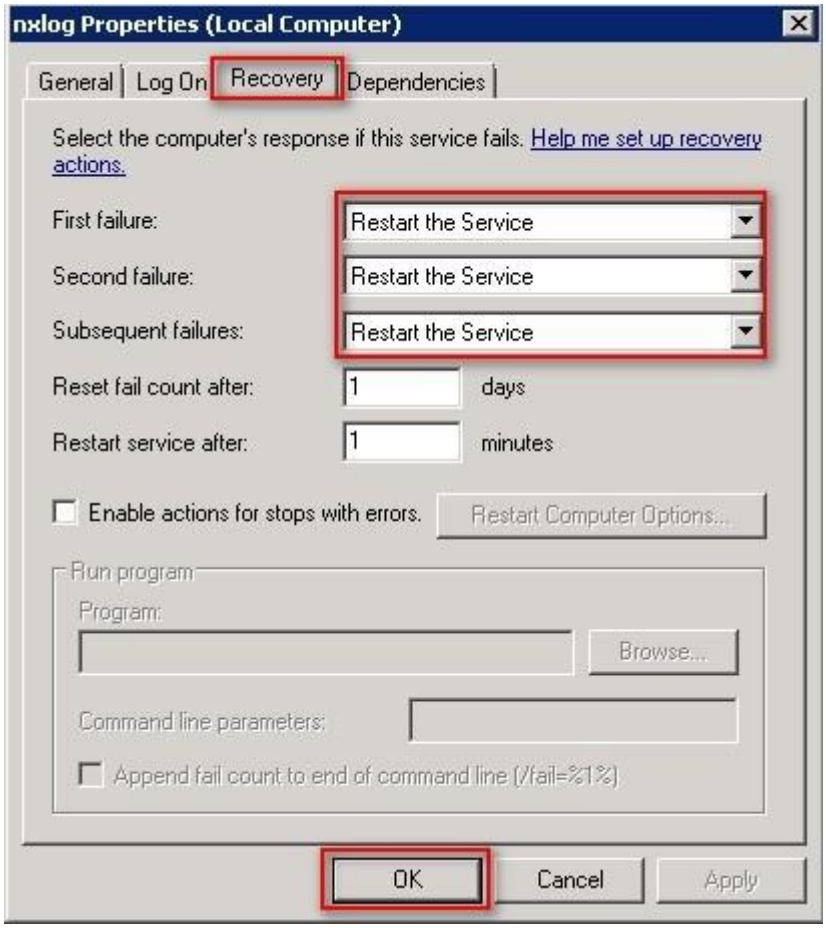
Please select “nxlog” and click  .



(5) Select “Automatic (Delayed Start)” of “Startup type” in “General.”



(6) Select “Restart the Service” of “First, Second and Subsequent Failures” in “Recovery” and click “OK.”



2. For Windows 2000

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendation” link provided in “preface” for detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

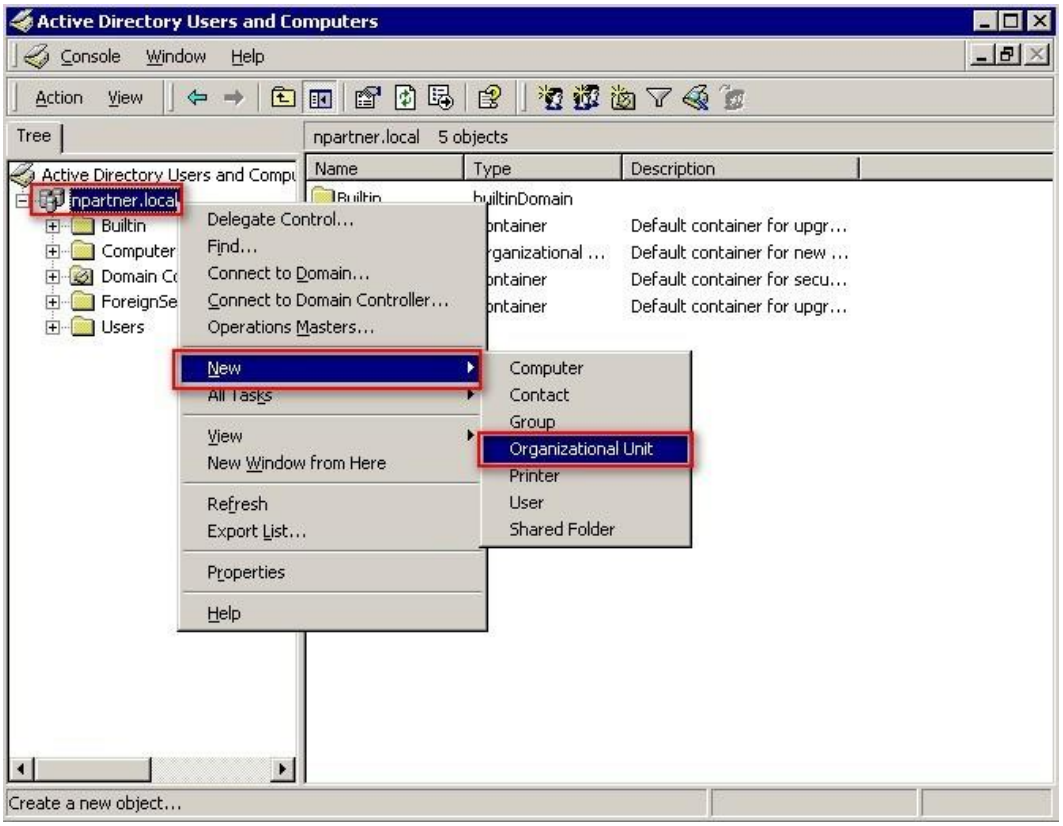
2.1 Domain

2.1.1 Organizational Unit Setup

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

(2) Add Your Organizational Unit

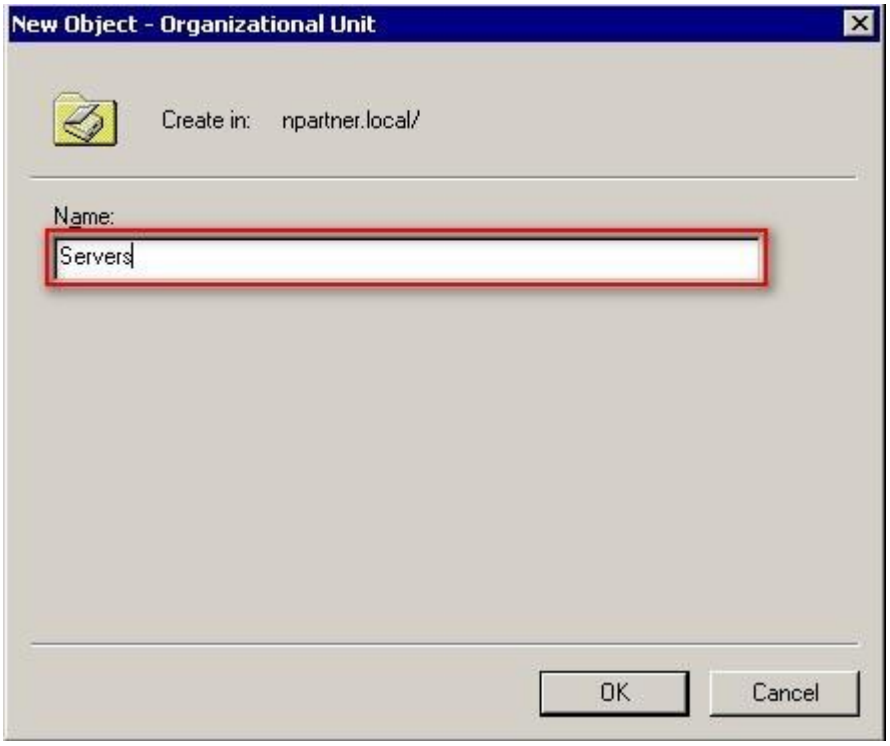
Right-click on your “Domain Name,” (in this example, it is “npartner.local), select “New” and click “Organizational Unit.”



(3) Name Your Organizational Unit

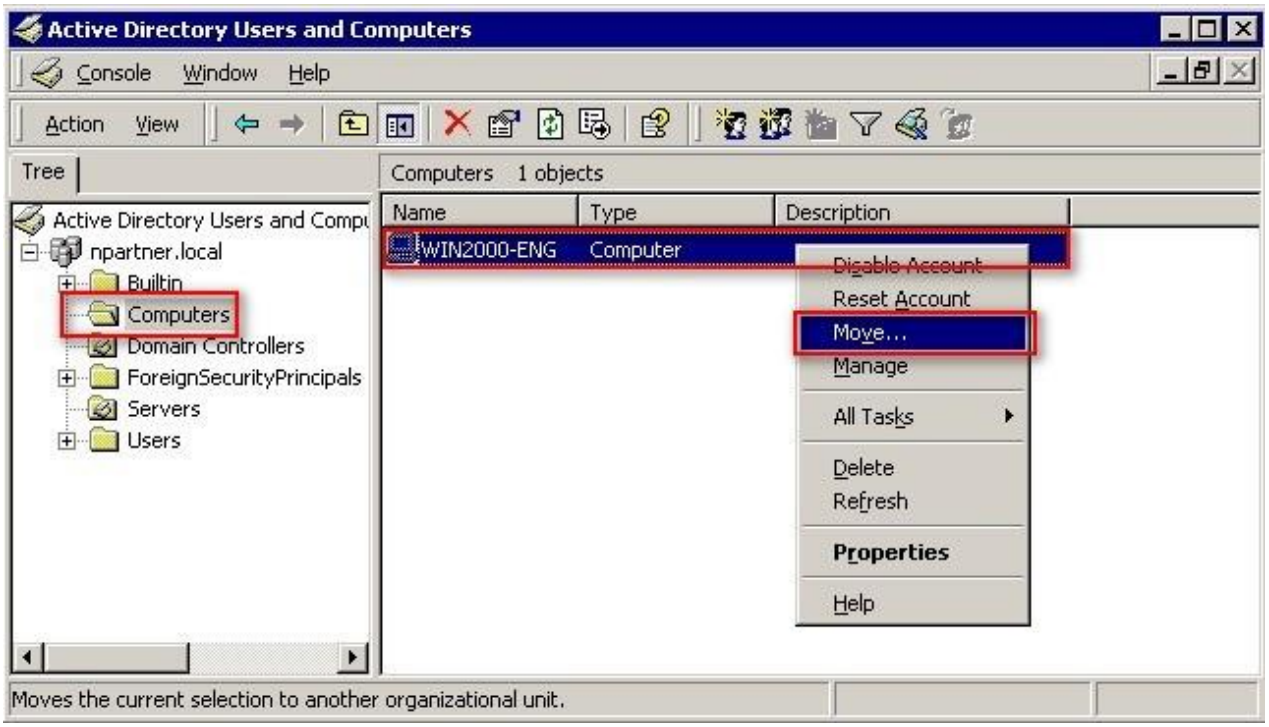
Enter your “Organizational Unit Name,” (In this example, it is “Servers.”)

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



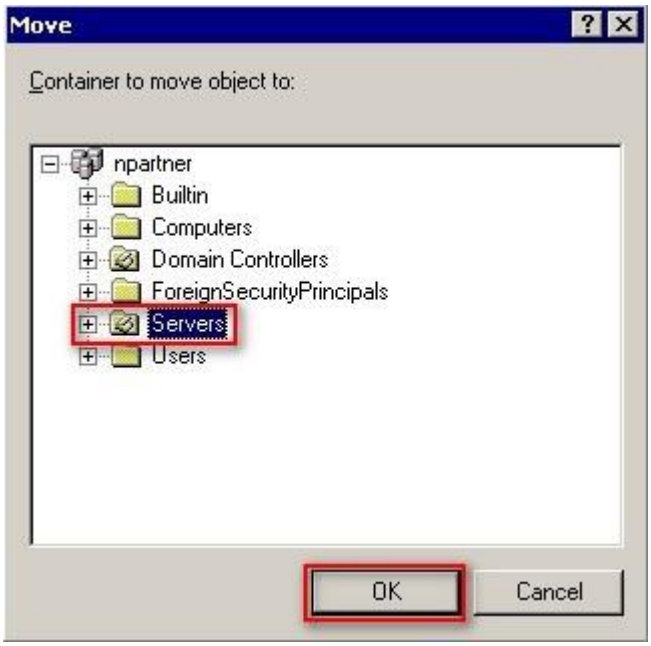
(4) Move Your Server to New Organizational Unit

Select your organizational unit(the example here is “Computers”) -> Right-click on the “WIN2000-ENG” server.Note: Please select the Windows Server host based on actual environment -> Click “Move.”



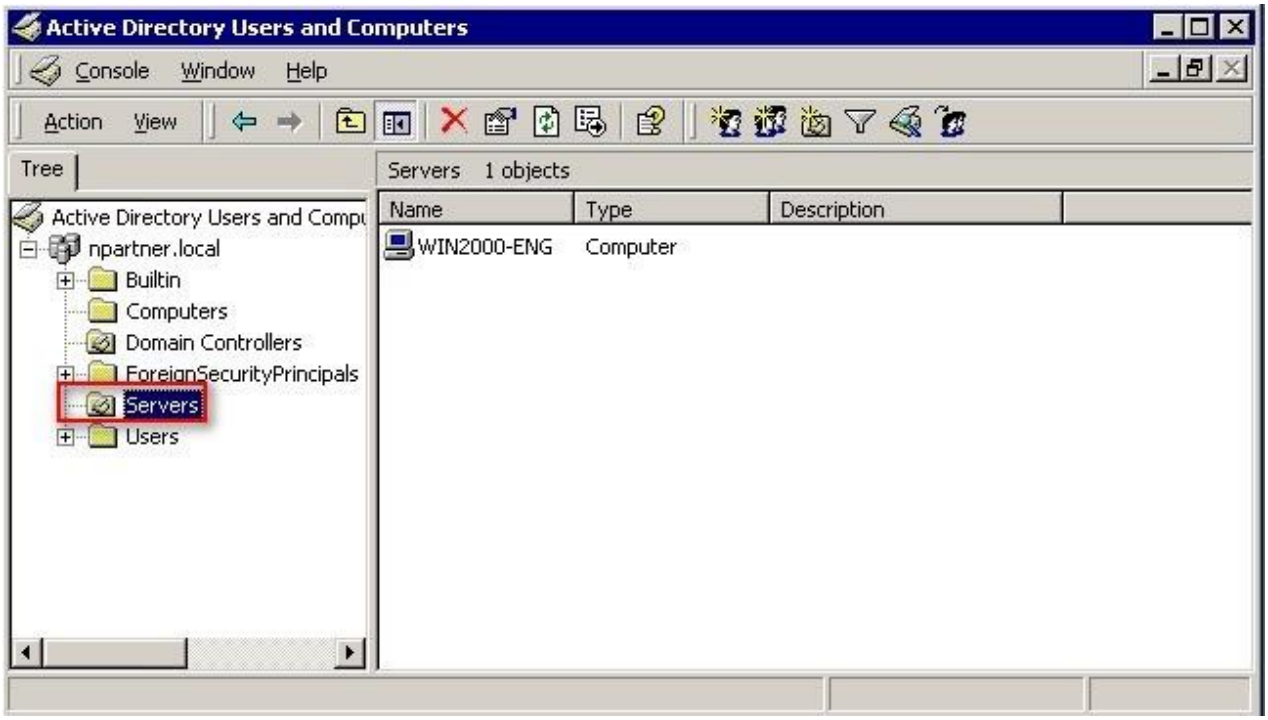
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

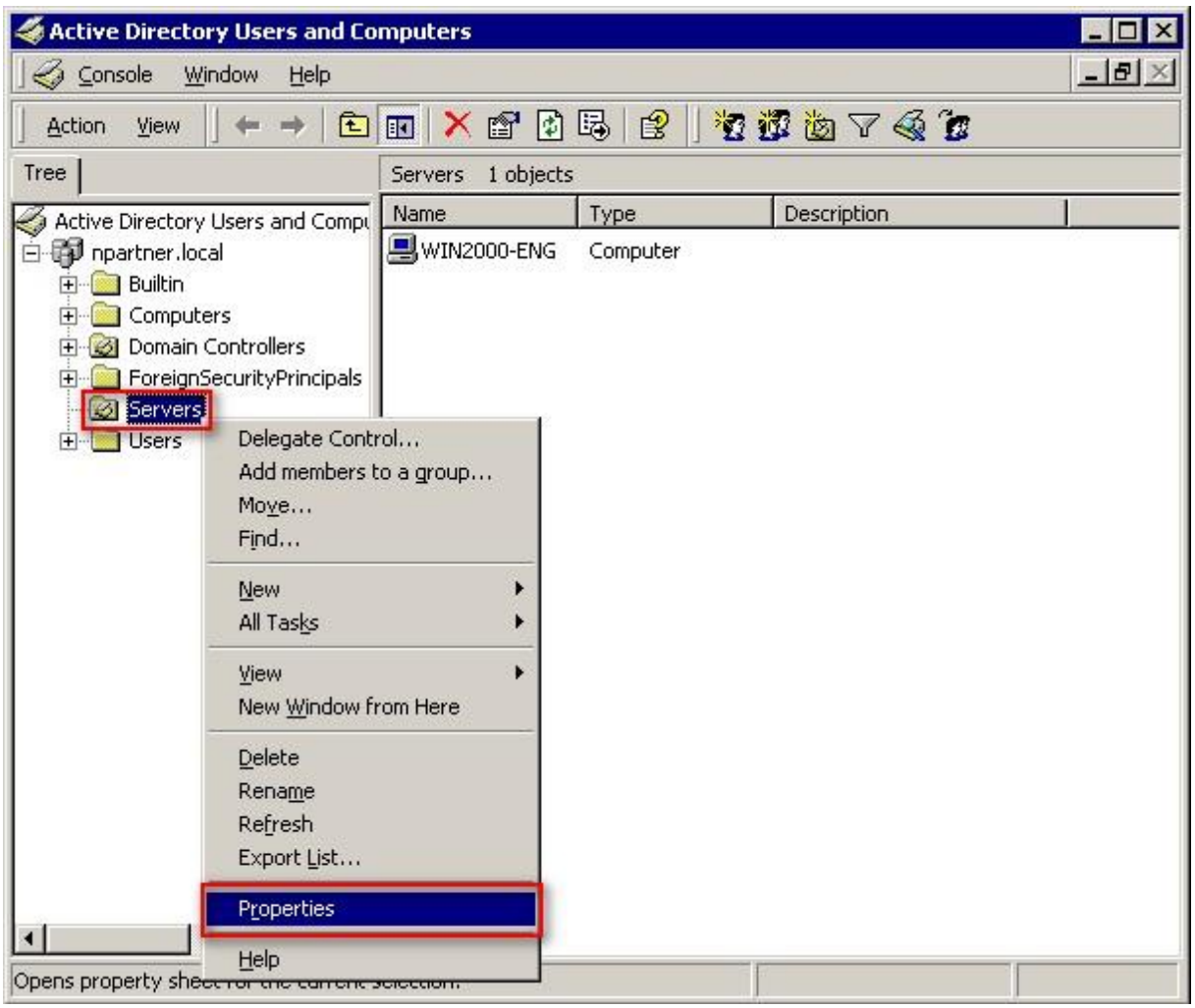
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2000-ENG” server has been moved.



2.1.2 Group Policy Settings

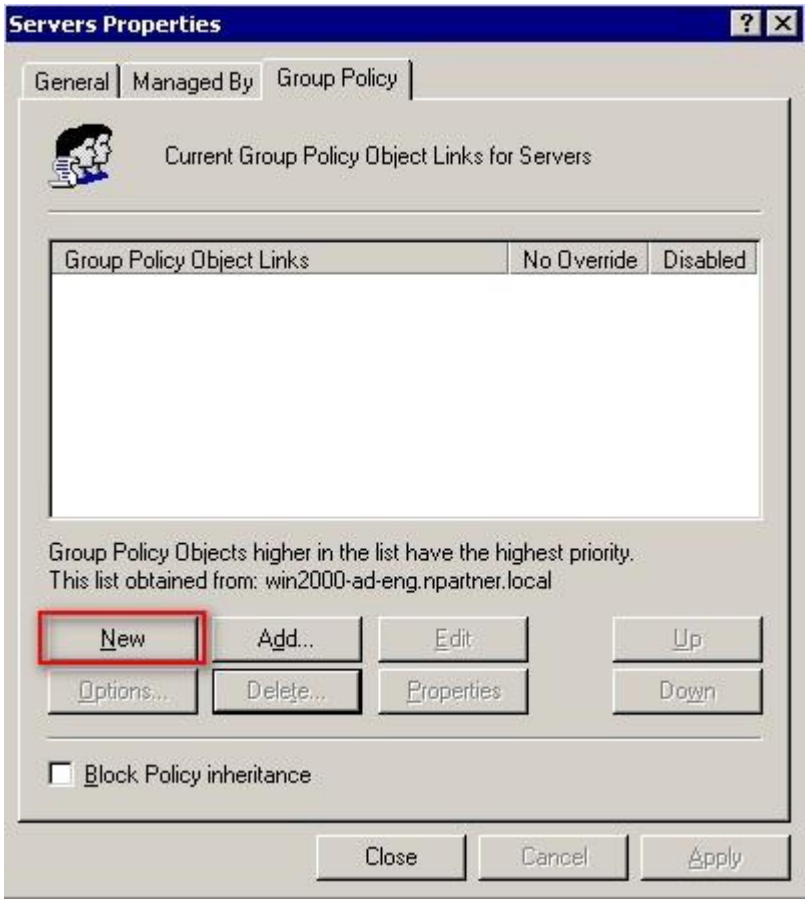
(1) Open “Active Directory Users and Computers.”

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



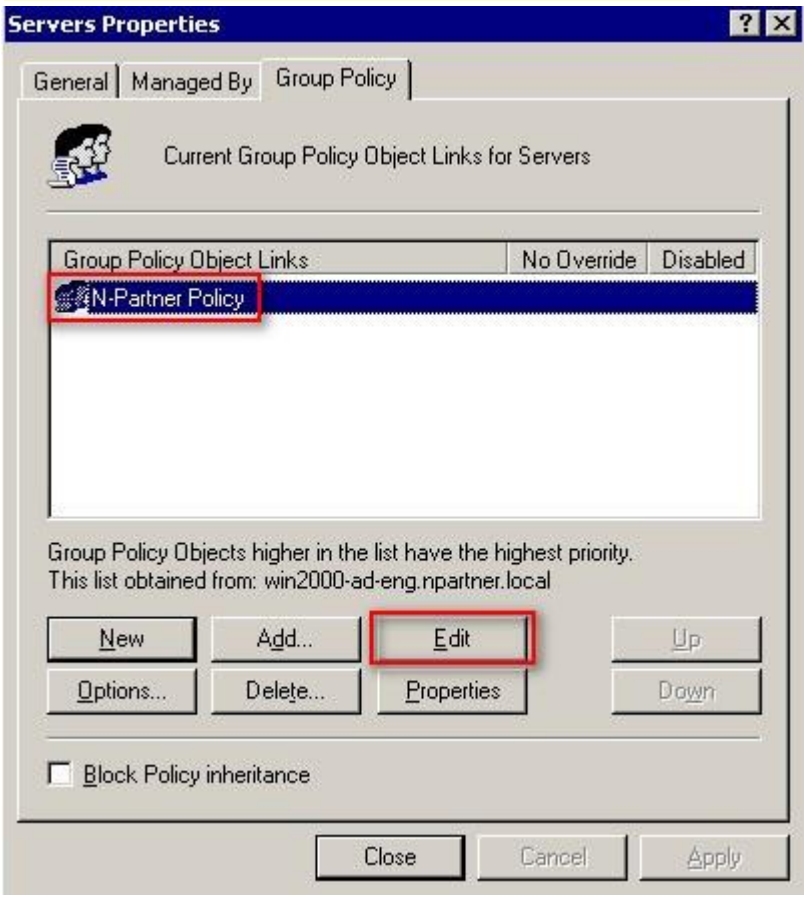
(3) Enter Your Group Policy Object Name

Click on the “Group Policy” page and click “New.”



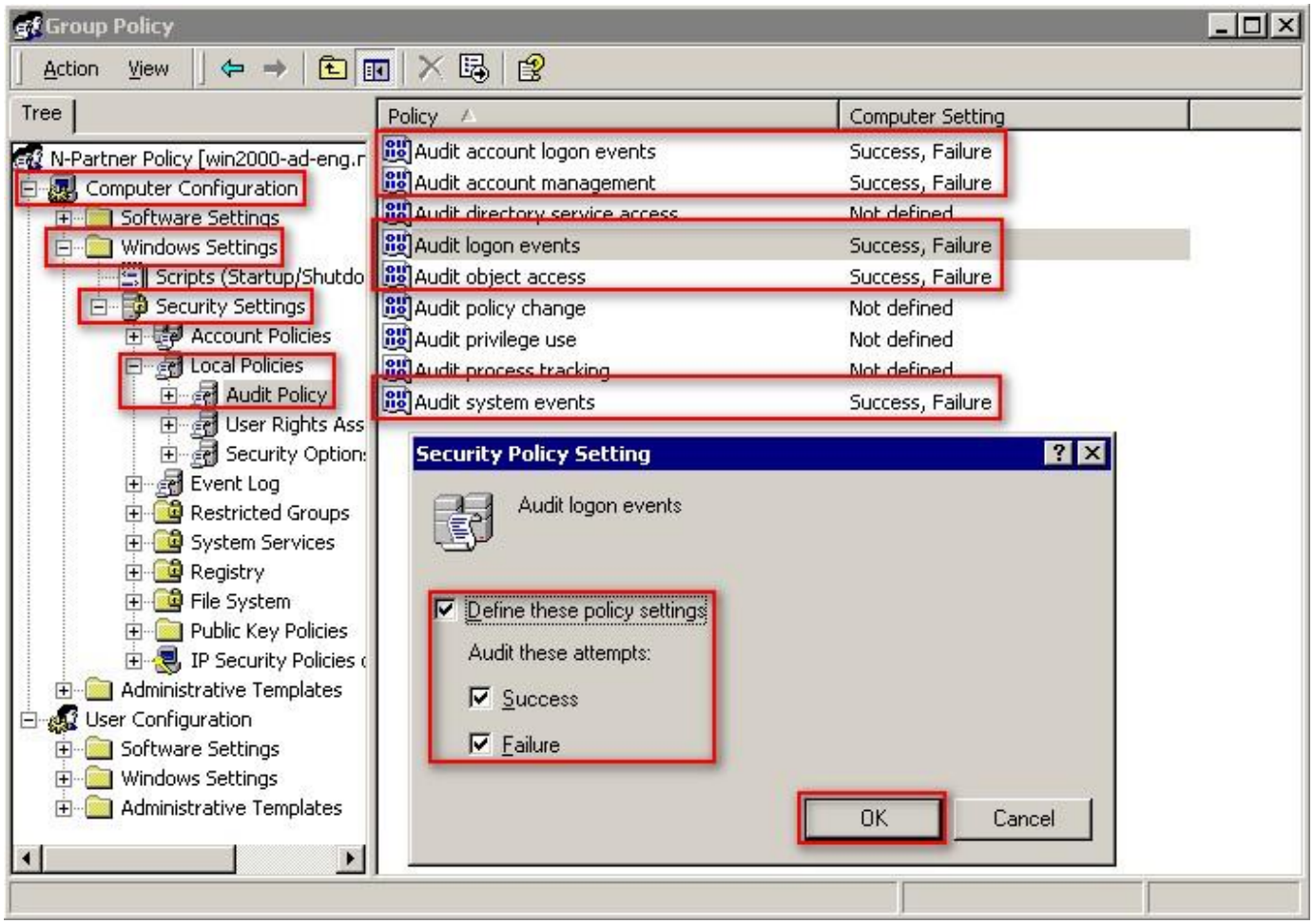
(4) Name Your Group Policy Object

Enter your group policy object name (the example here is “N-Partner Policy”) Note: Please create your group object name based on the actual environment -> Click “Edit.”



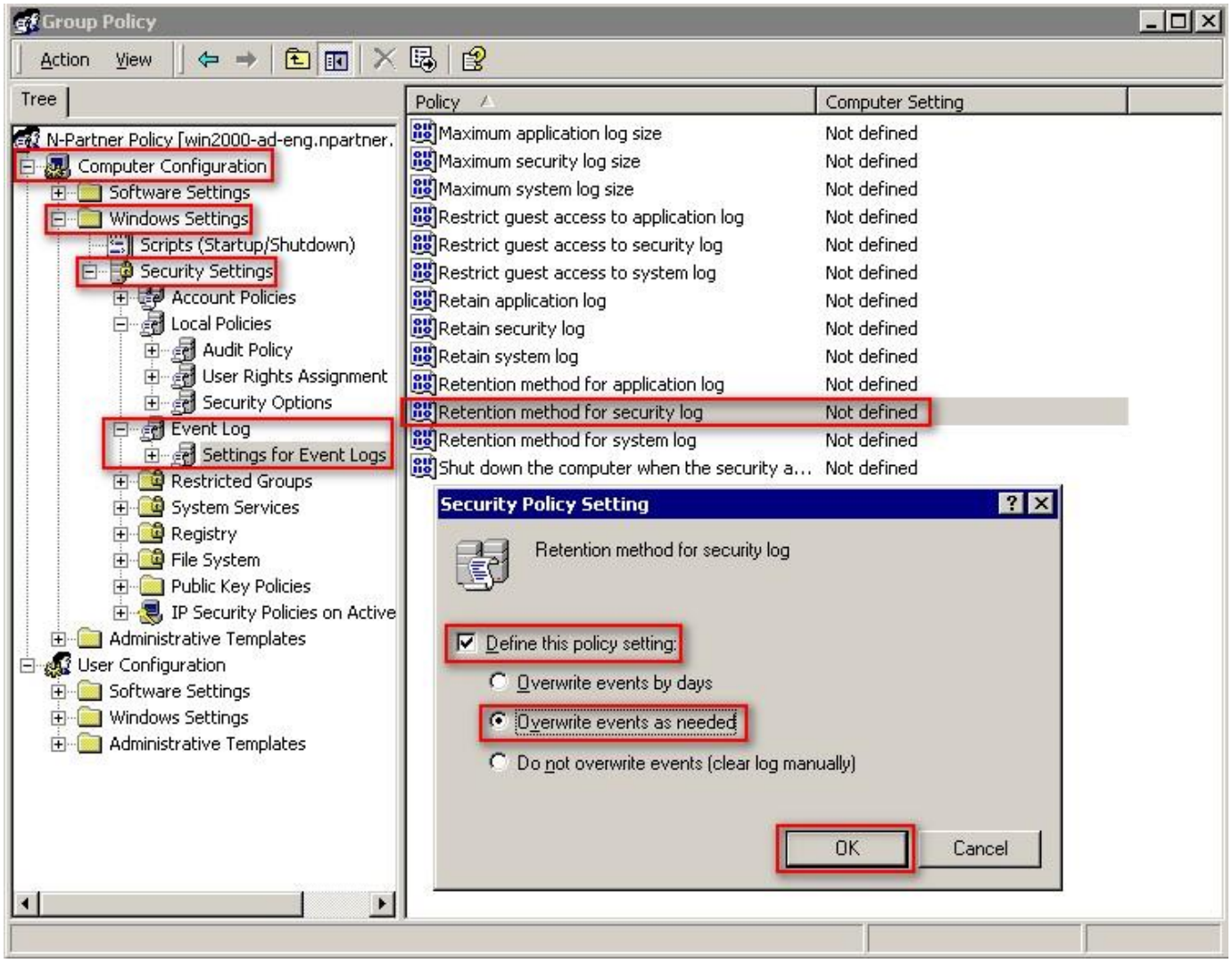
(5) Local Group Policies: Audit Policy

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



(6) Event Logs: Retention Method for Security Log

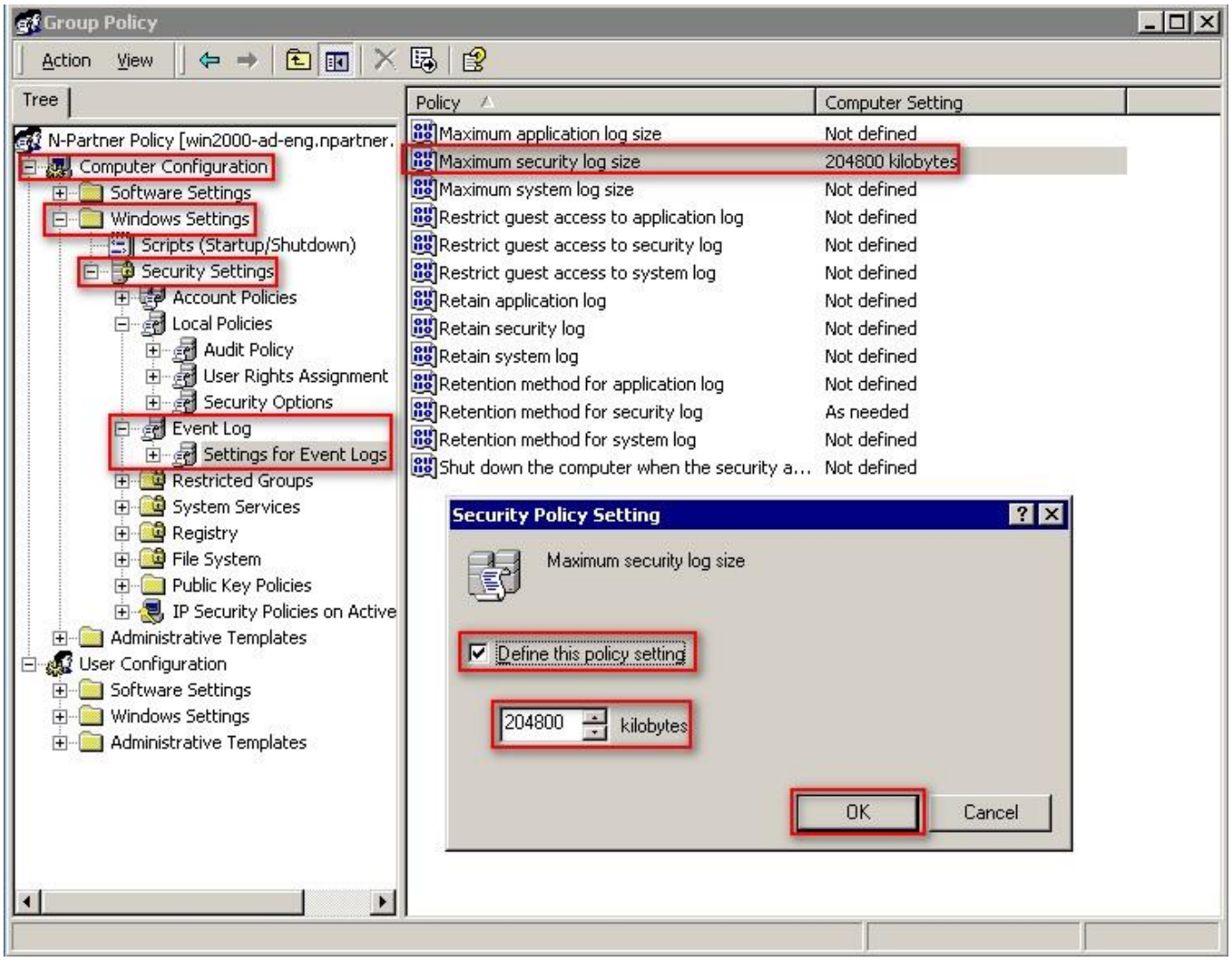
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting”: -> Select “Overwrite events as needed” -> Click “OK.”



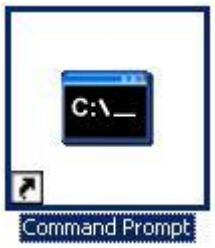
(7) Event Logs: Maximum Size of Security Log

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

Note: Please adjust the number based on the actual environment -> Click [OK].



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



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

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

2.2 Workgroup

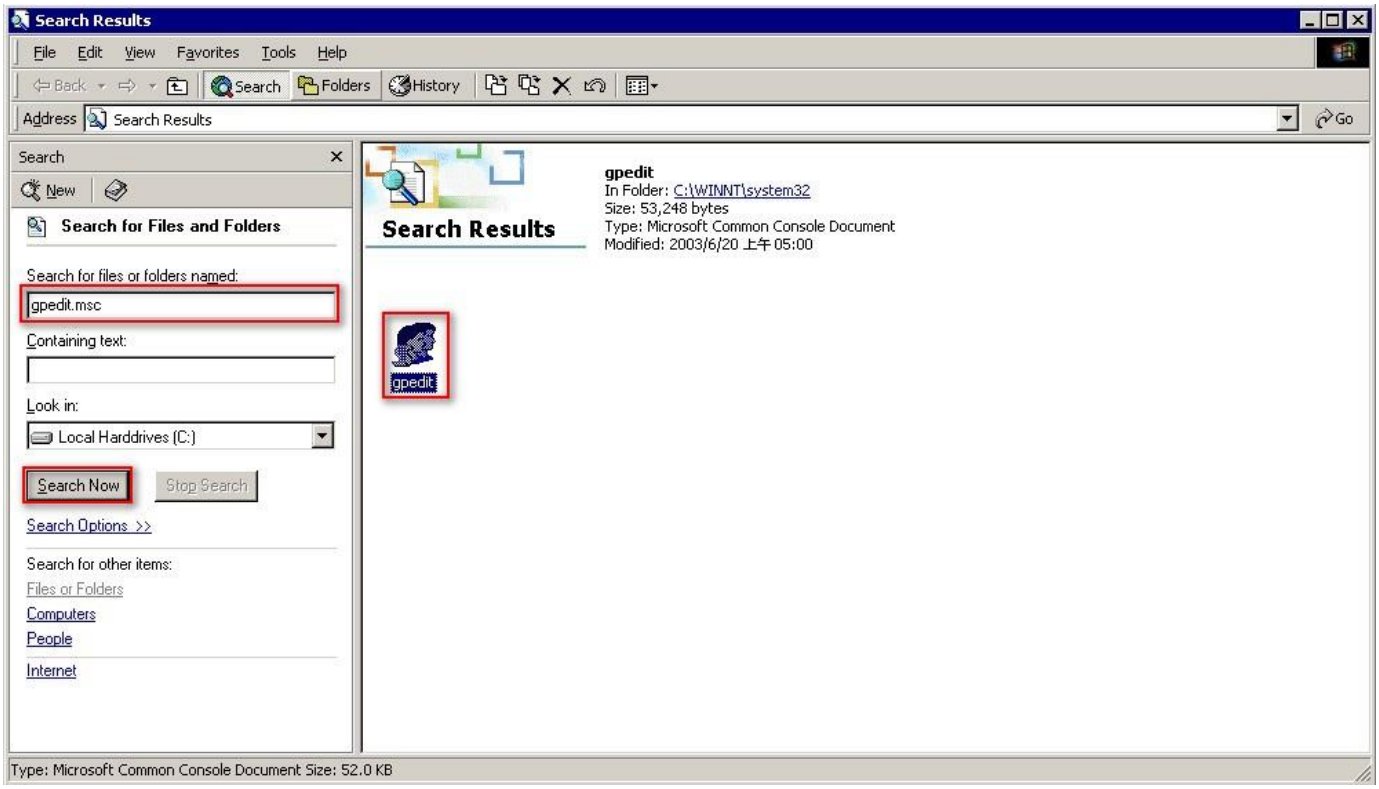
2.2.1 Audit Policy Settings

(1) Search

Click on “Start” -> “Search” -> “For Files or Folders.”

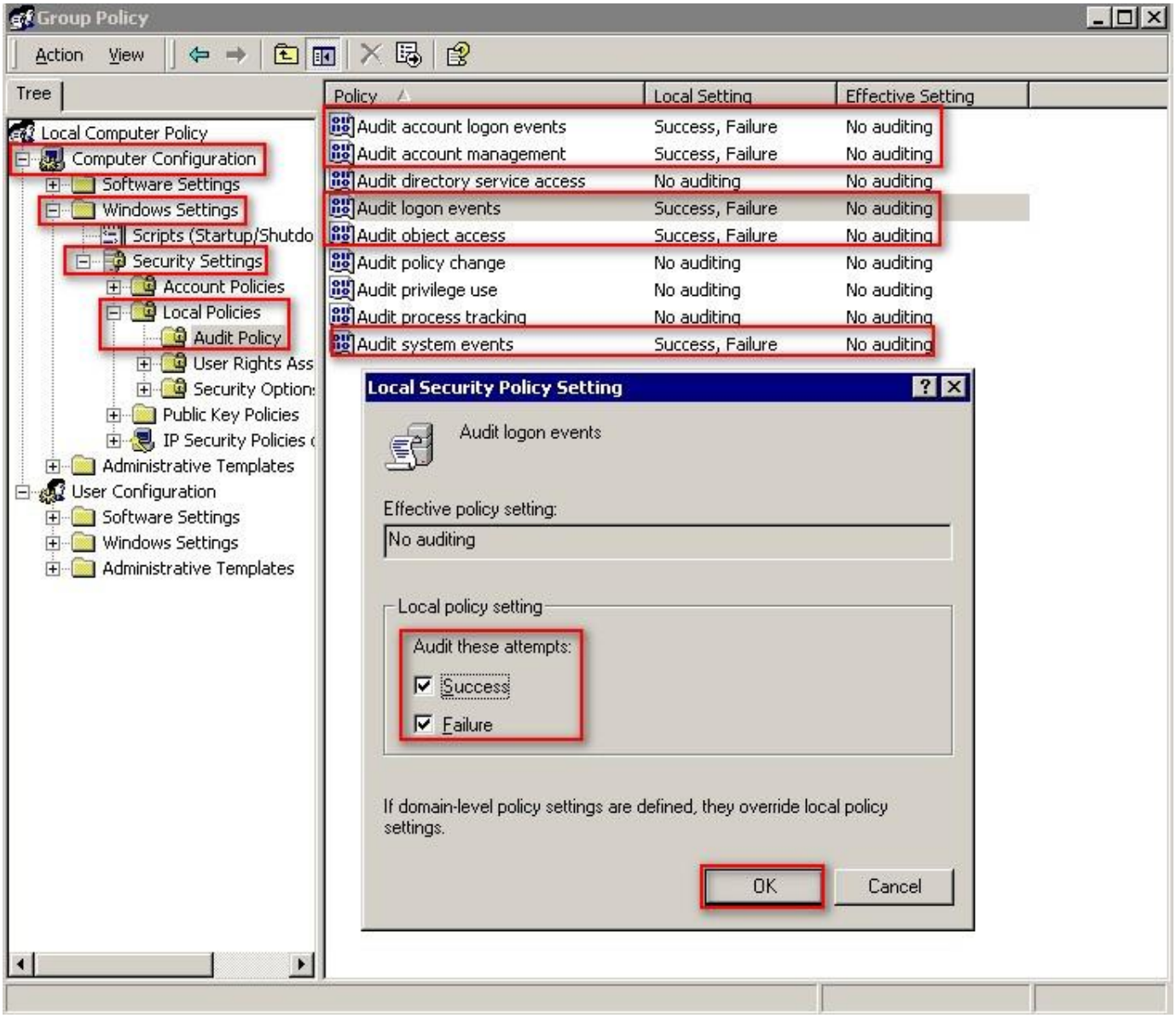
(2) Search for Group Policy

Enter “gpedit.msc” -> And click “Search Now” -> Click on “gpedit” in the search results.

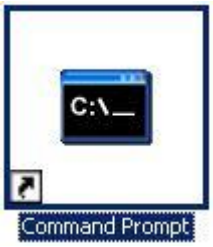


(3) Local Group Policies: Audit Policies

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: “Success” & “Failure” -> Click “OK.”

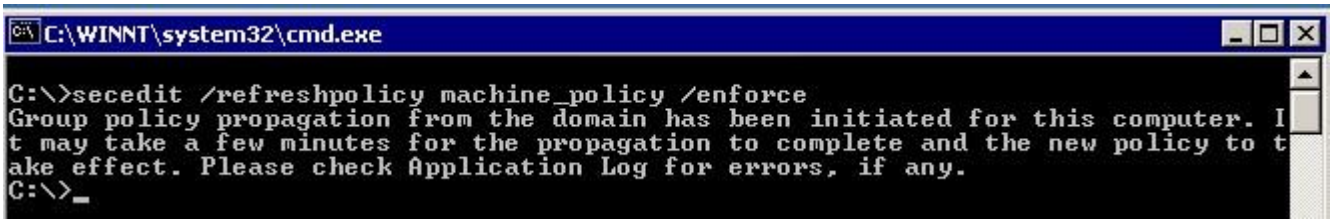


(4) Open “Command Prompt.”



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

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



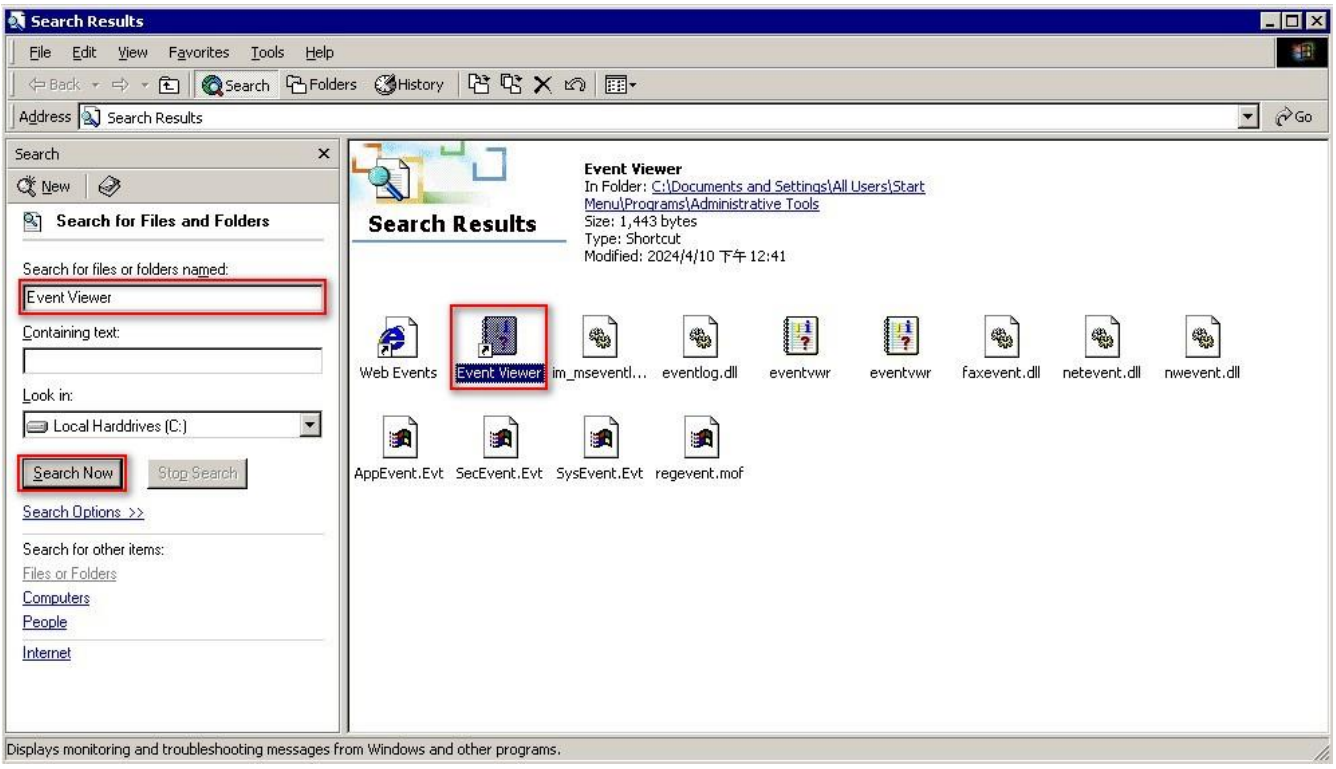
2.2.2 Event Log Settings

(1) Open “Search”

Click on “Start” -> “Search” -> “For Files or Folders.”

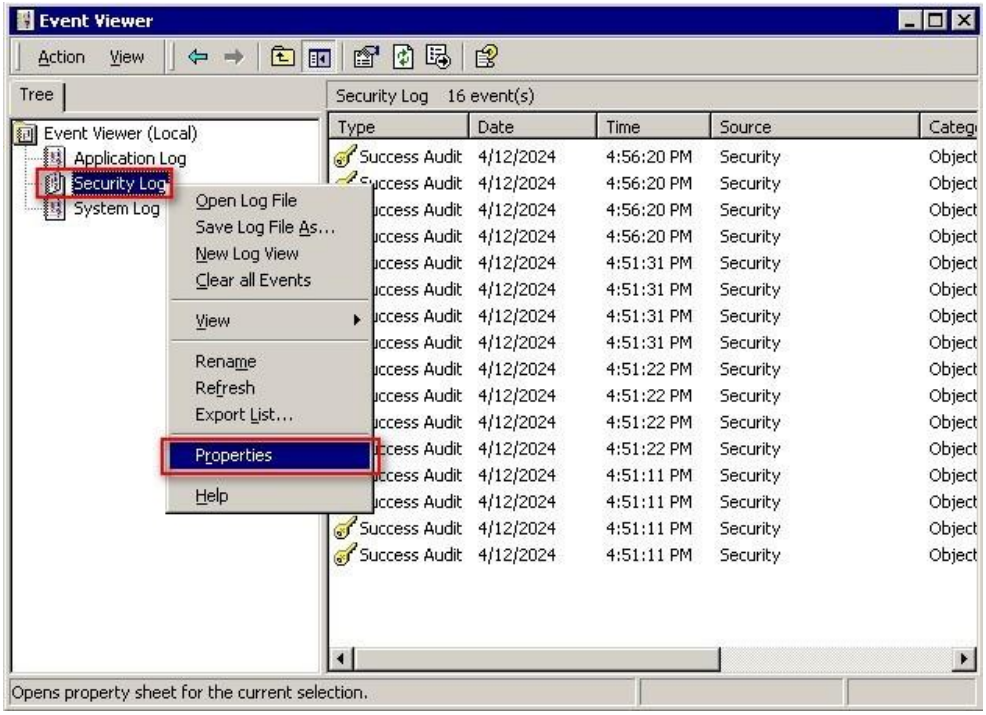
(2) Search for “Event Viewer”

Enter “Event Viewer” -> And click “Search Now” -> Click on “Event Viewer” in the search results.



(3) Edit Security Log

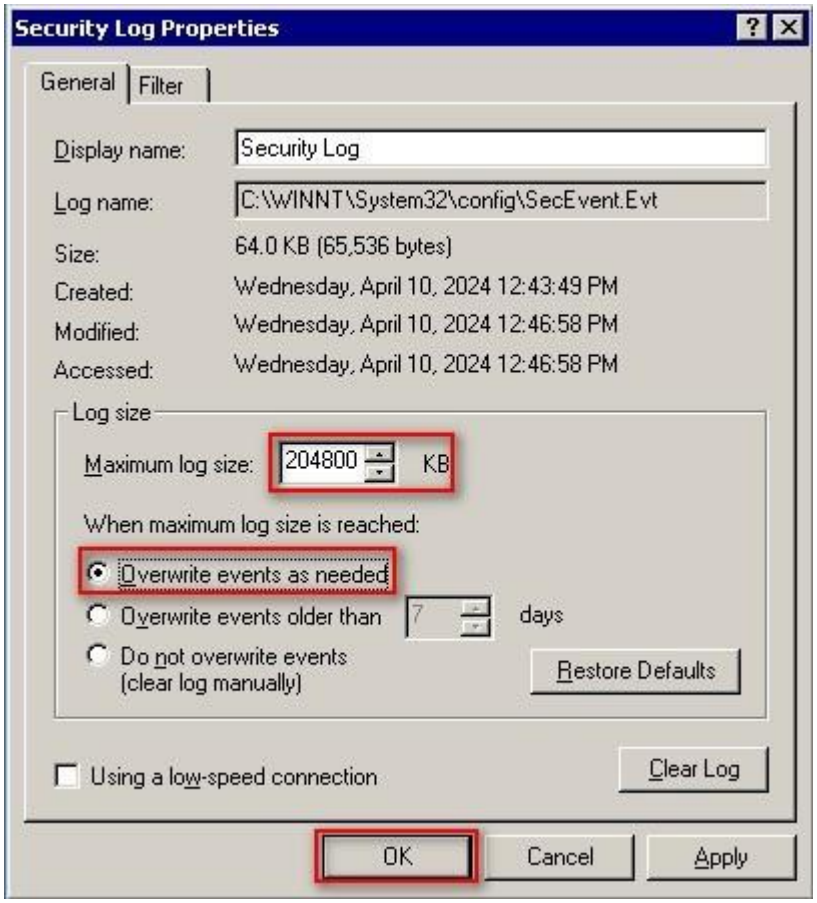
Right-click on “Security Log” -> And click on “Properties.”



(4) 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. For Windows 2003

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendation” link provided in “preface” for detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

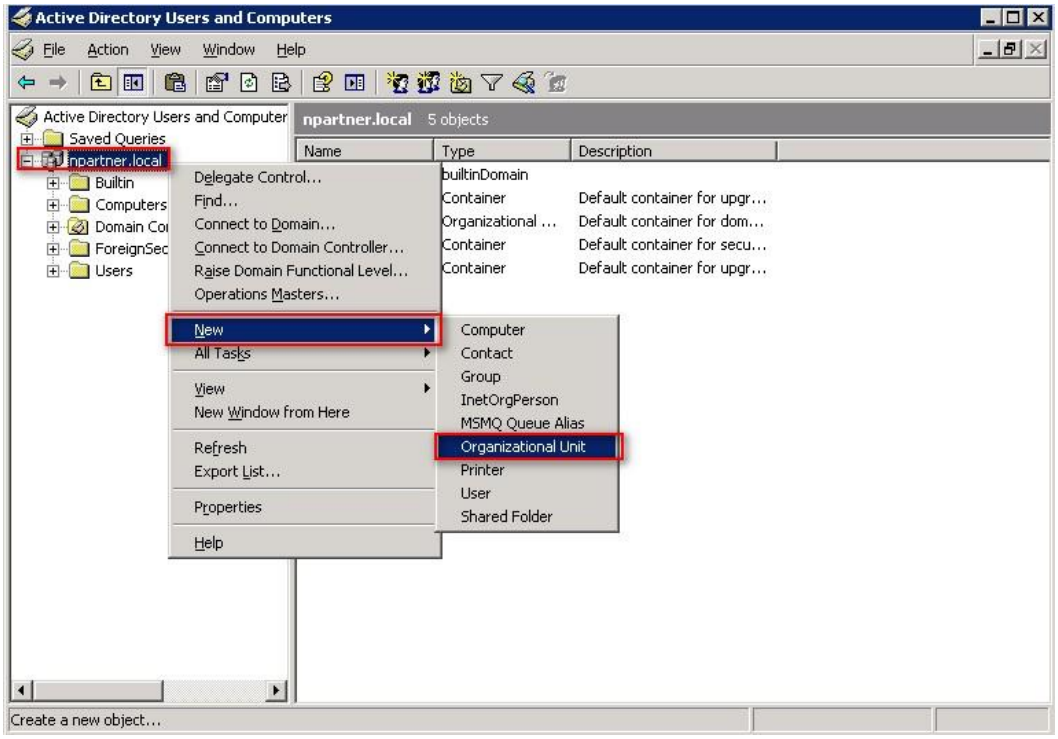
3.1 Domain

3.1.1 Organizational Unit Configuration

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

(2) Add Organizational Unit

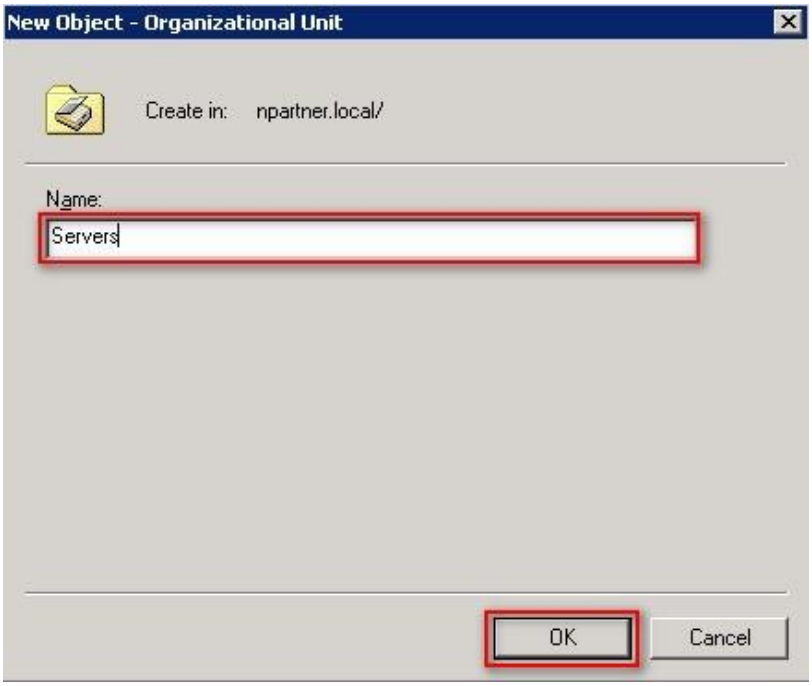
Right-click on your “Domain Name,” (in this example, it is “npartner.local), select “New” and click “Organizational Unit.”



(3) Name Your Organizational Unit

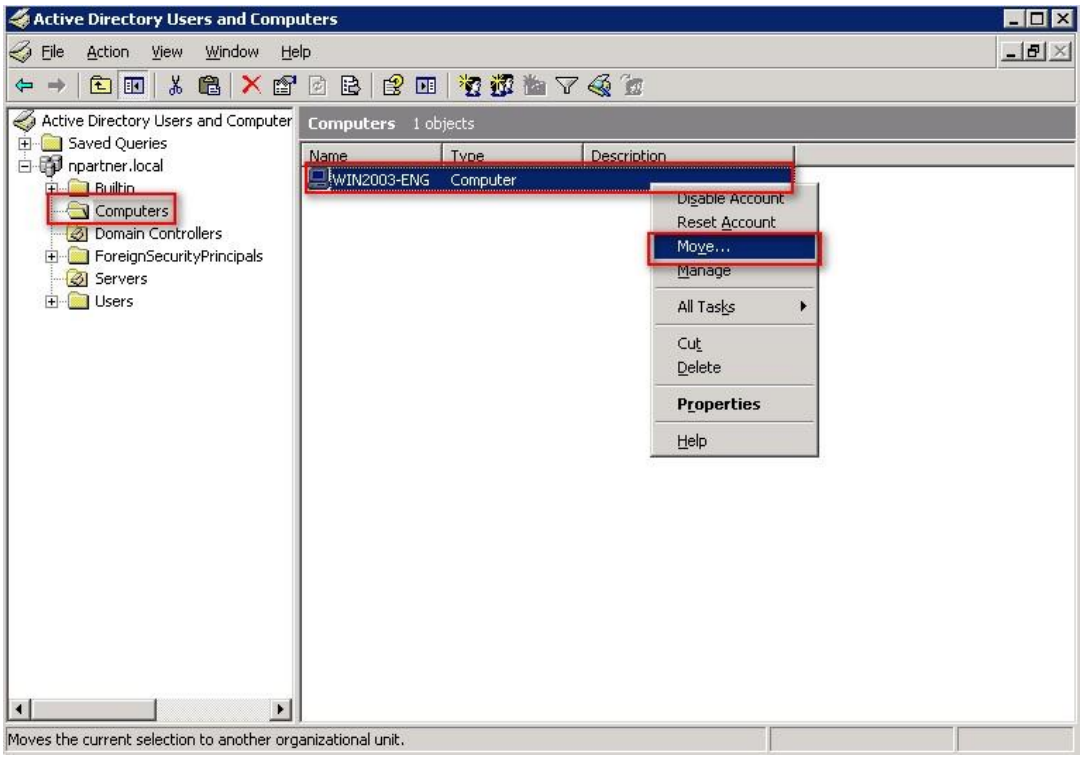
Enter your “Organizational Unit Name,” (In this example, it is “Servers”)

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



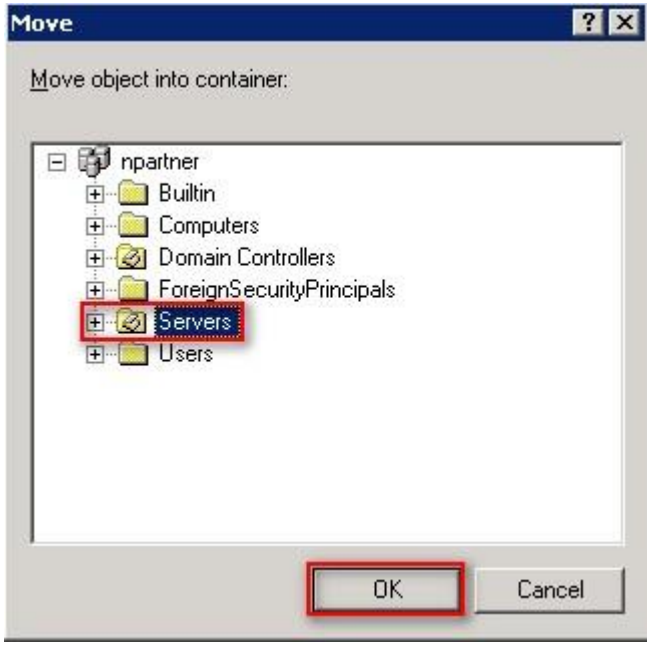
(4) Move Your Server to New Organizational Unit

Select your organizational unit(the example here is “Computers”) -> Right-click on the “WIN2003-ENG” server，Note: Please select the Windows Server host based on actual environment -> Click “Move.”



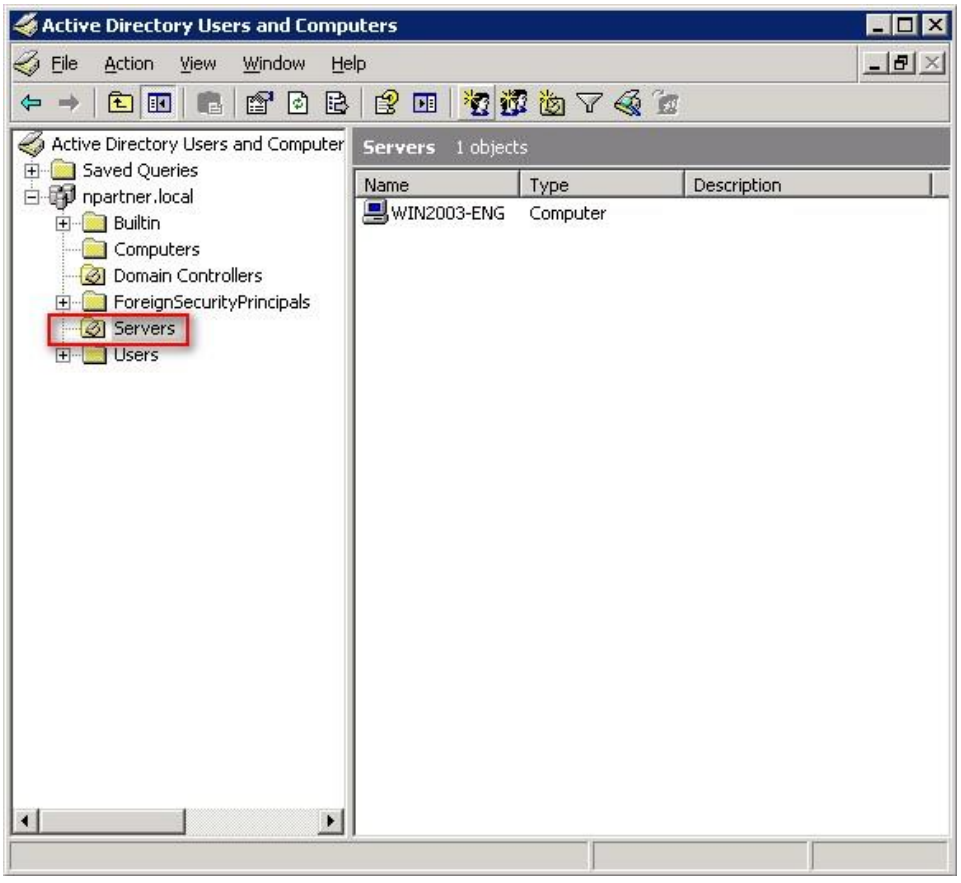
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

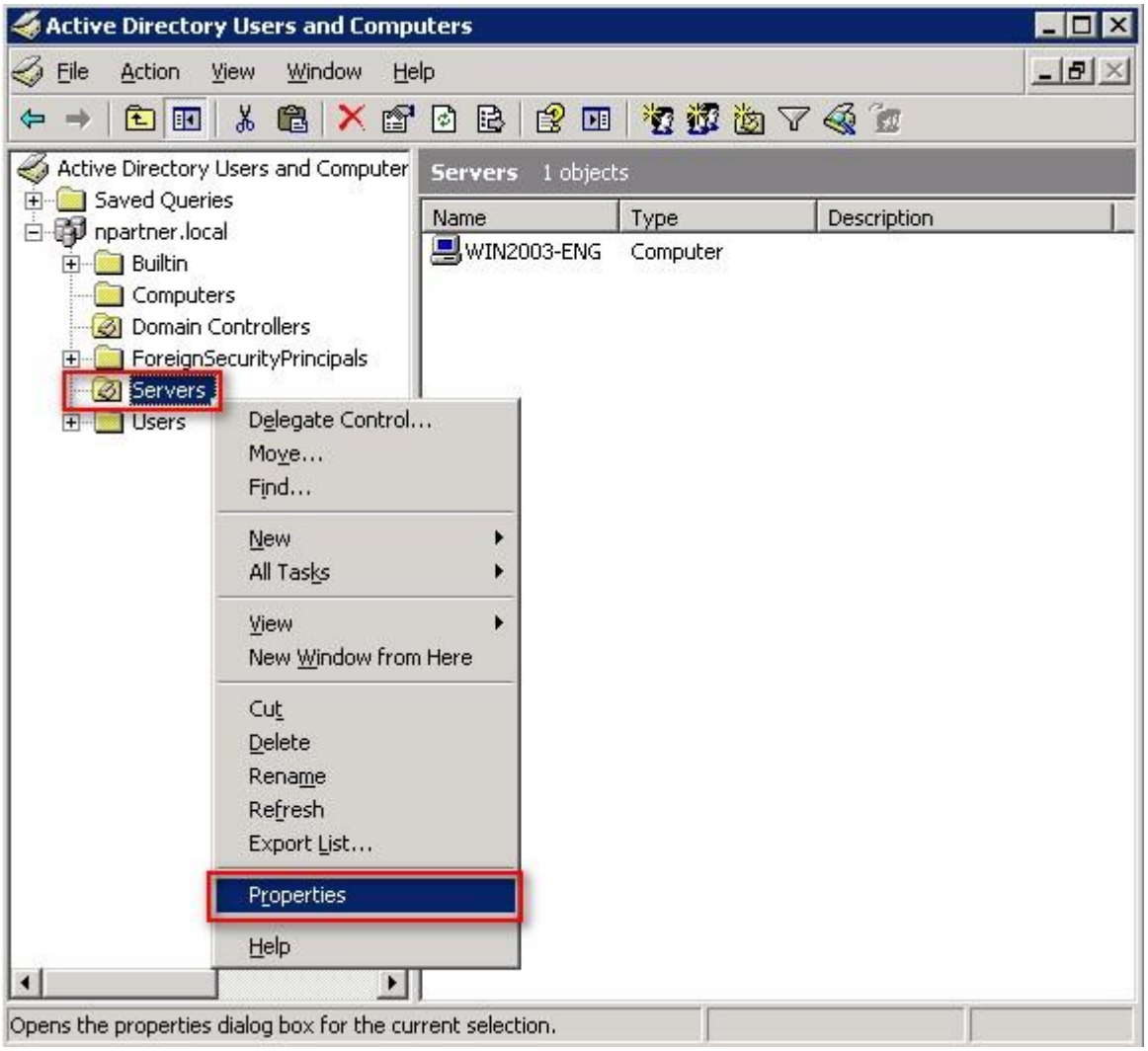
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2003-ENG” server has been moved.



3.1.2 Group Policy Settings

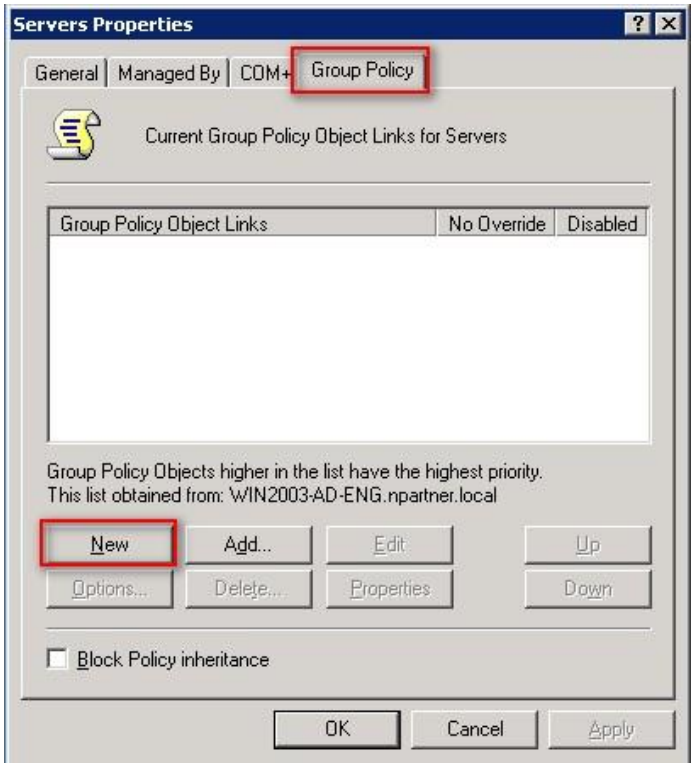
(1) Open “Active Directory Users and Computers.”

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



(3) Enter Your Group Policy Object Name

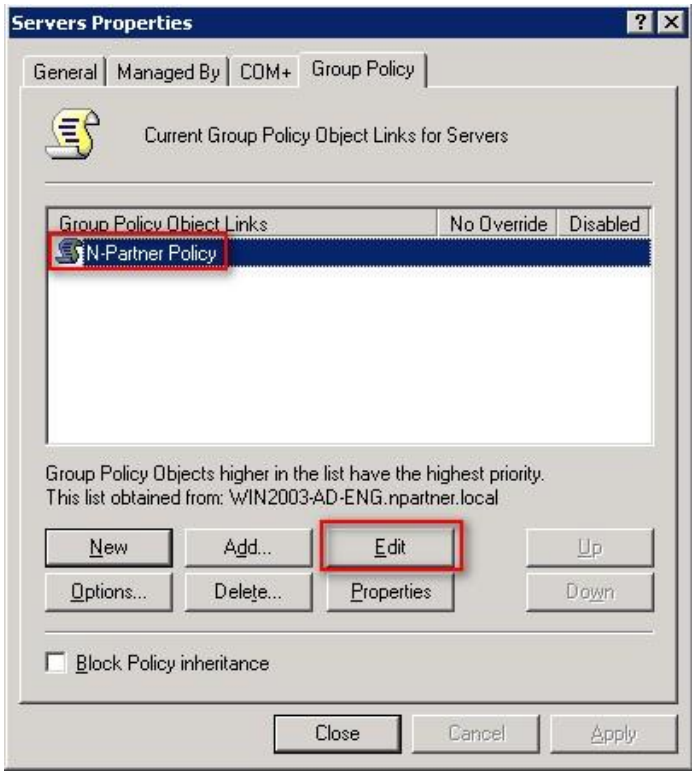
Click on the “Group Policy” page and click “New.”



(4) Edit Your Group Policy Object

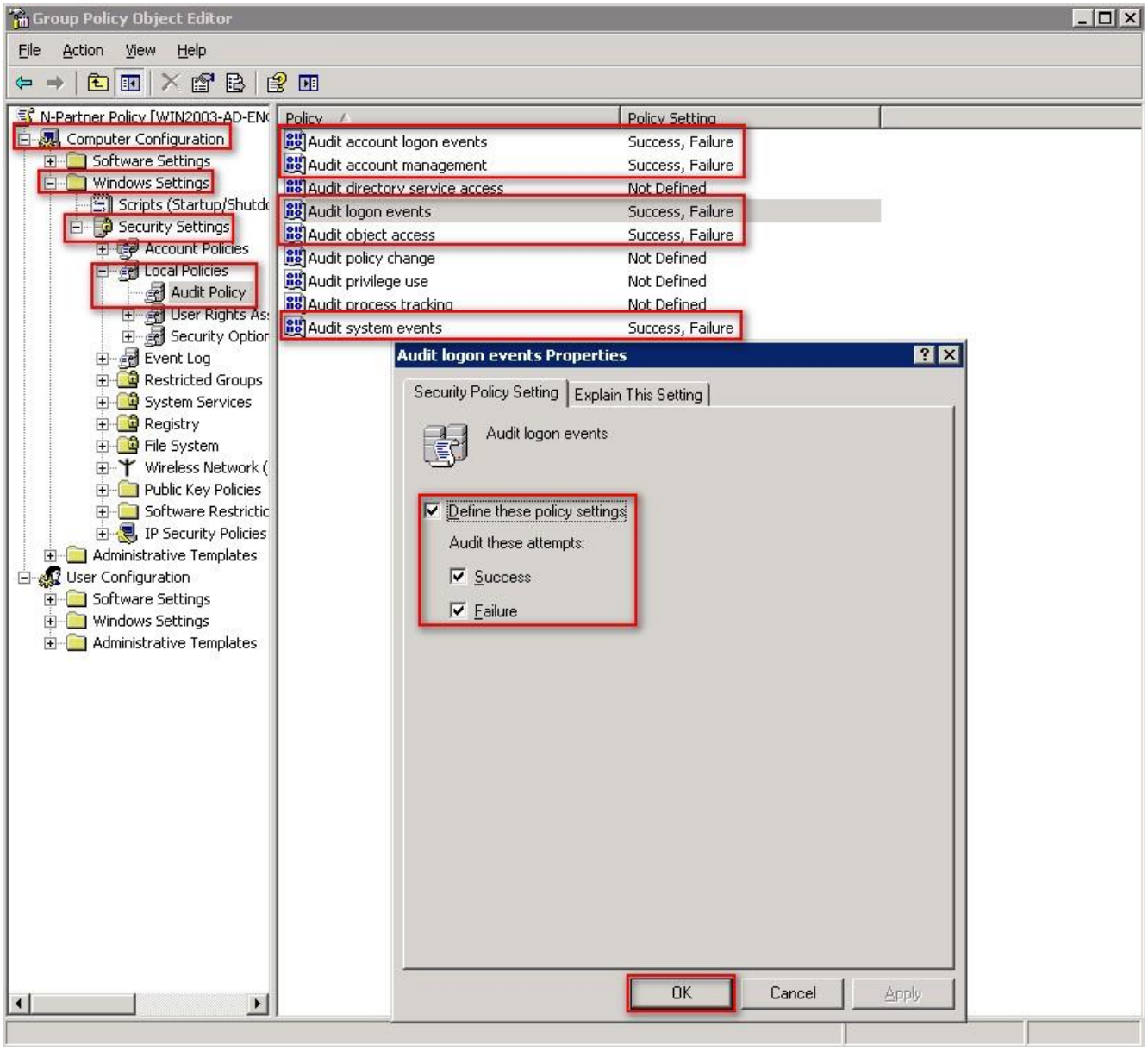
Enter your group policy object name (the example here is N-Partner Policy)

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



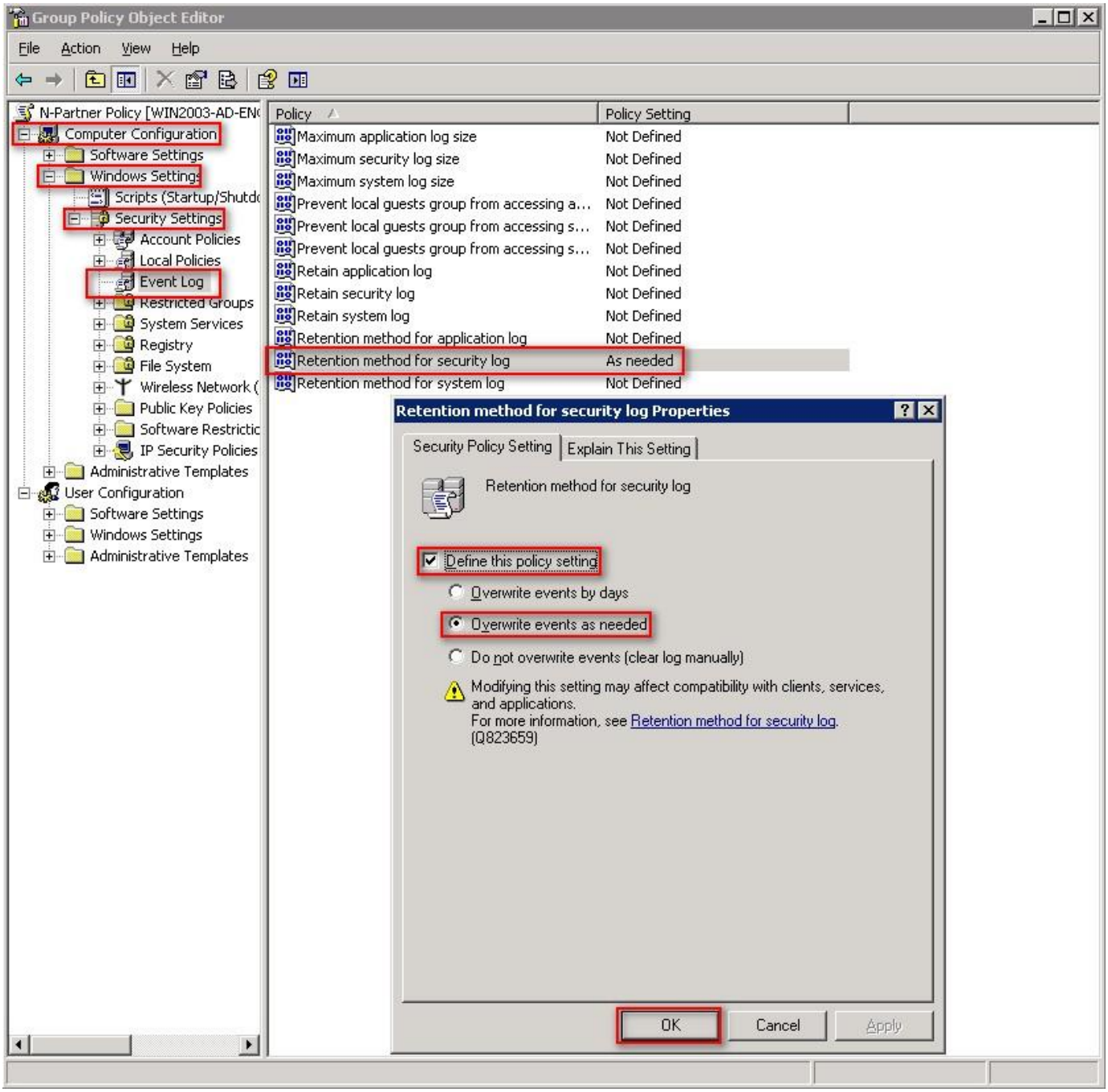
(5) Local Group Policies: Audit Policy

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



(6) Event Logs: Retention Method for Security Log

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

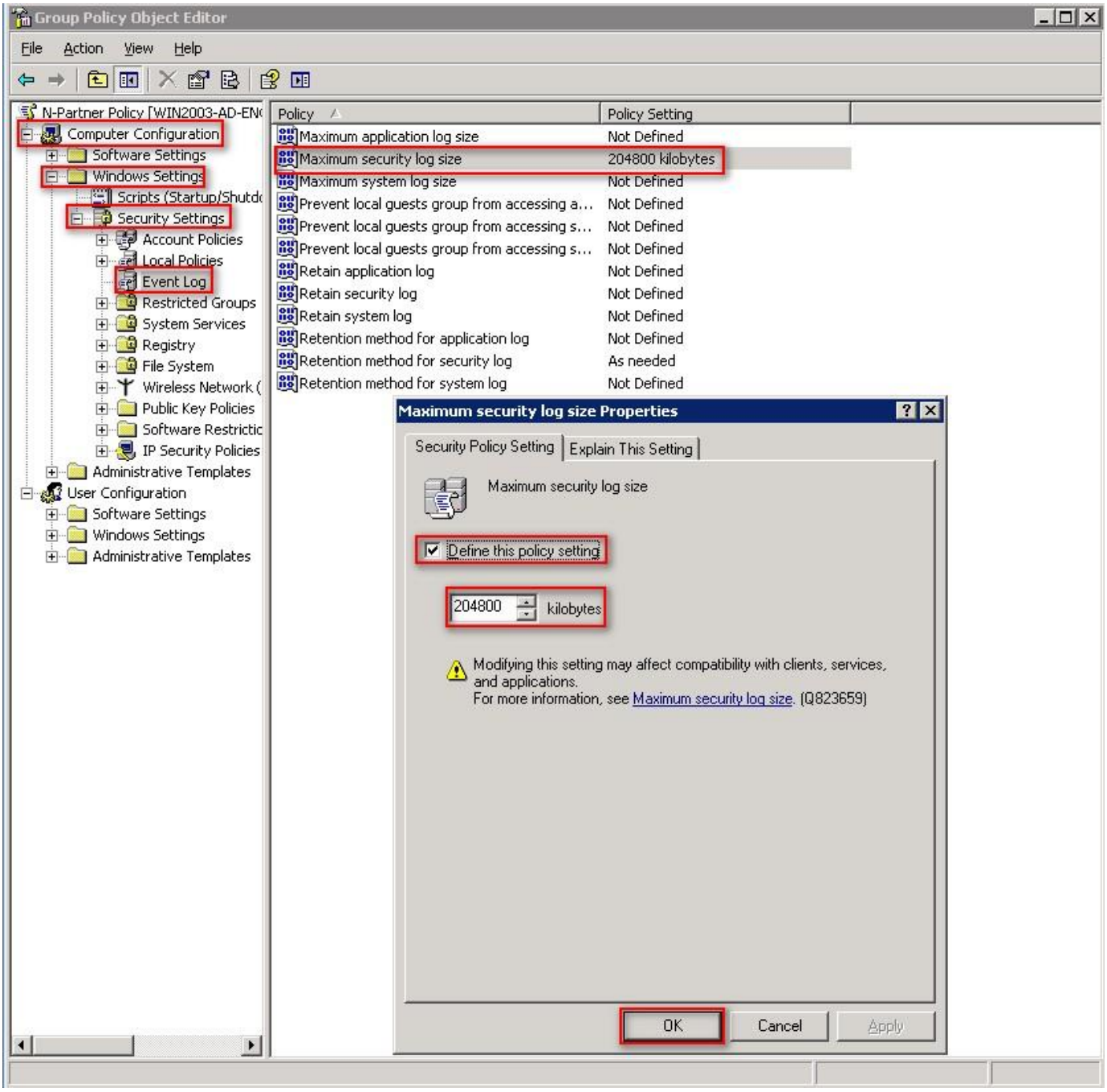


(7) Event Logs: Maximum Size of Security Log

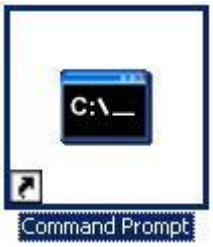
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” ->

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].

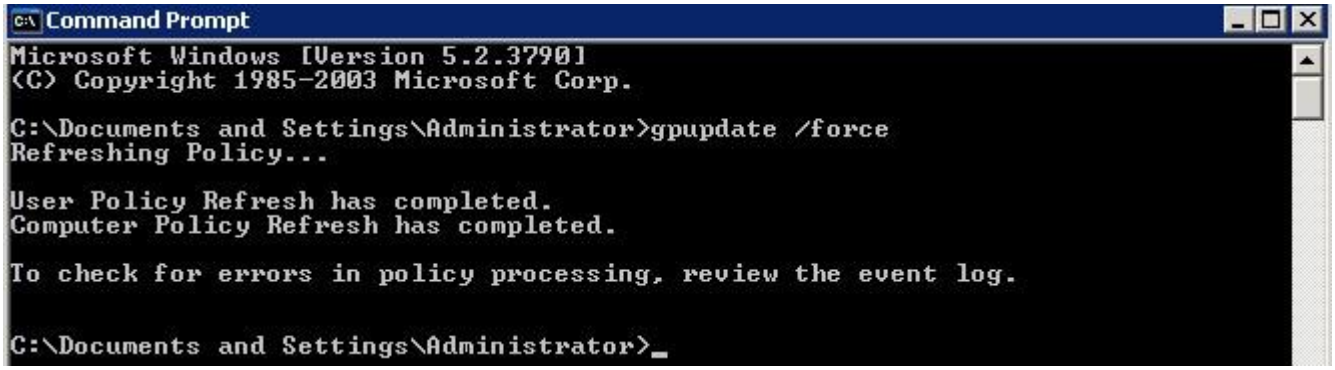


(8) Open “Command Prompt” on your Windows Server.



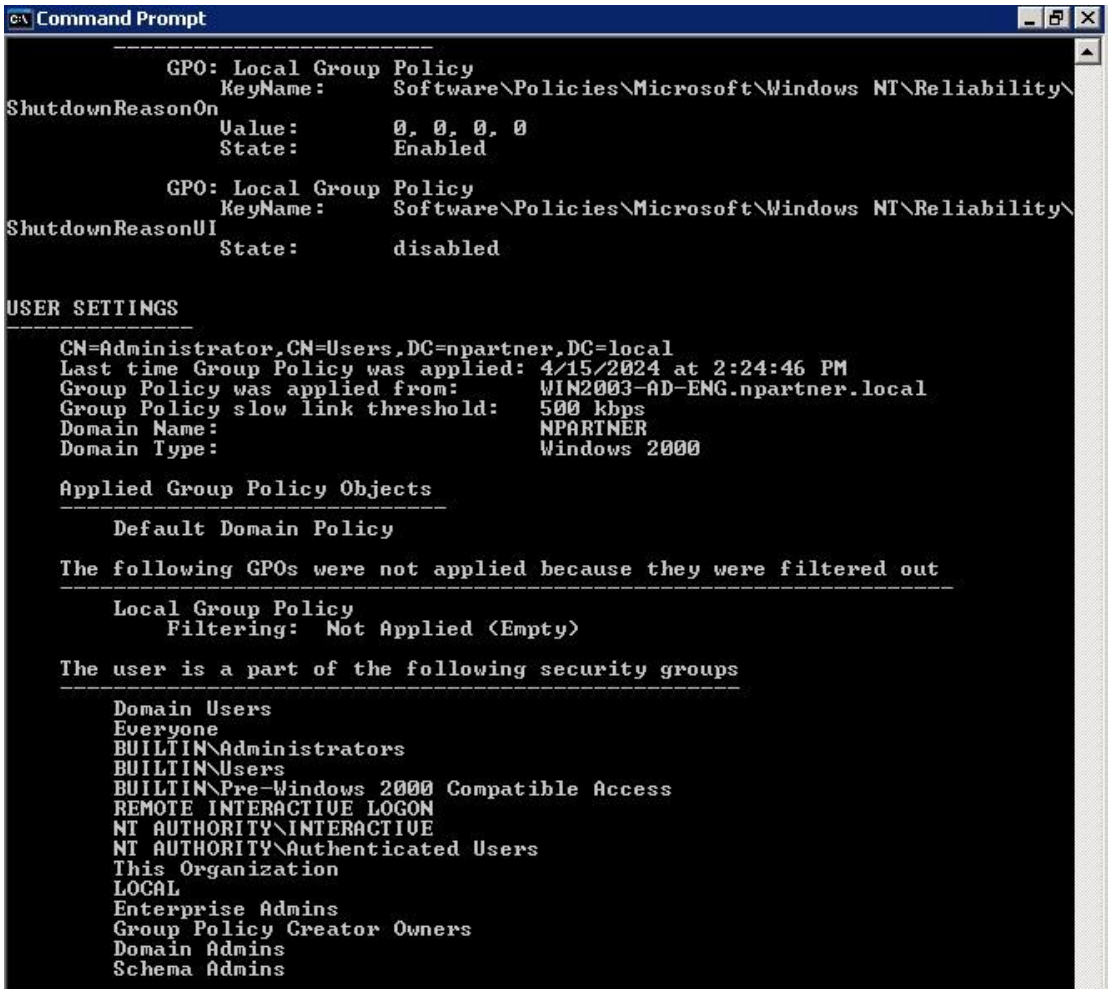
(9) Enter the command below to refresh group policy.

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



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

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

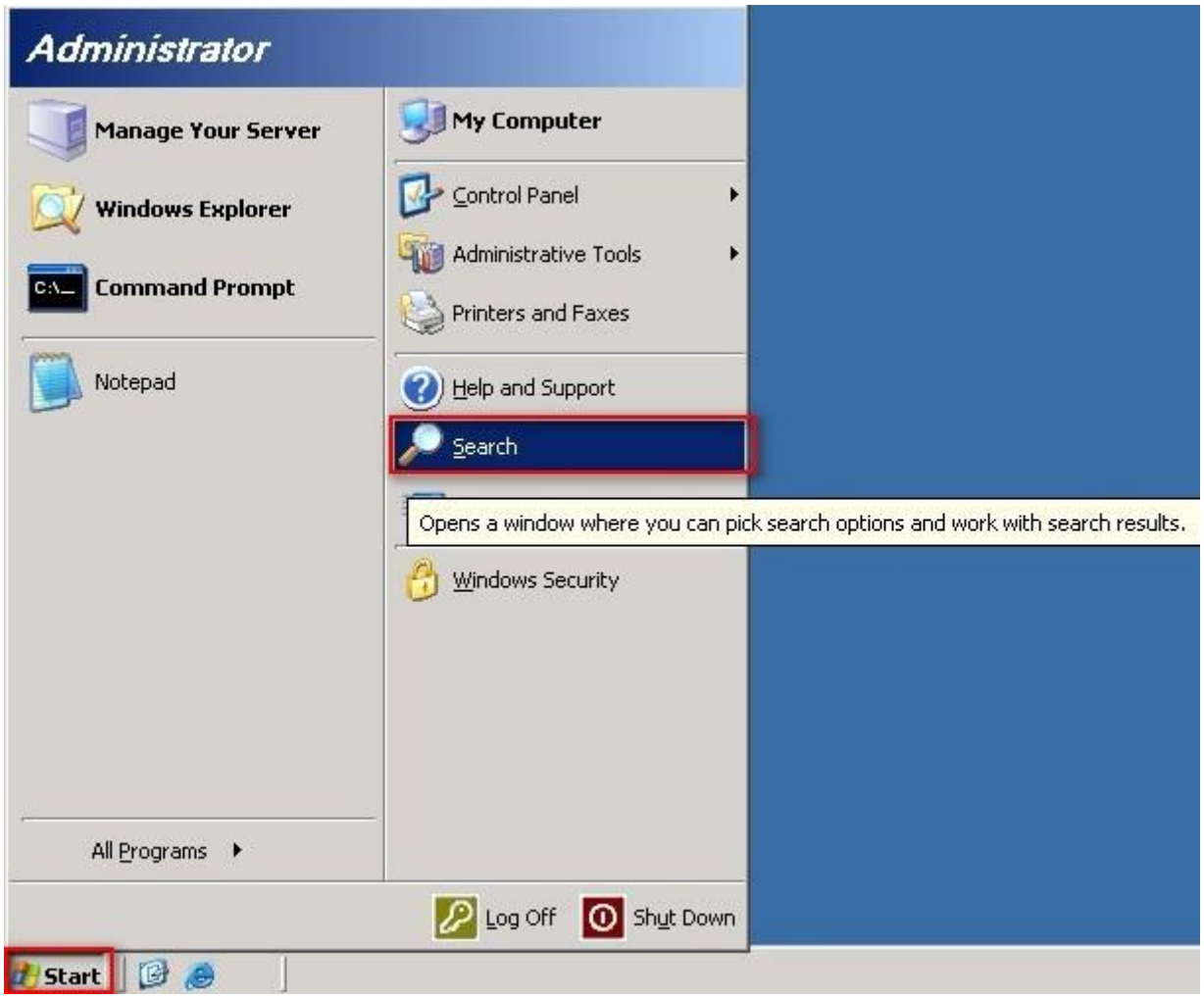


3.2 Workgroup

3.2.1 Audit Policy Settings

(1) Open Search

Click on “Start” -> “Search.”

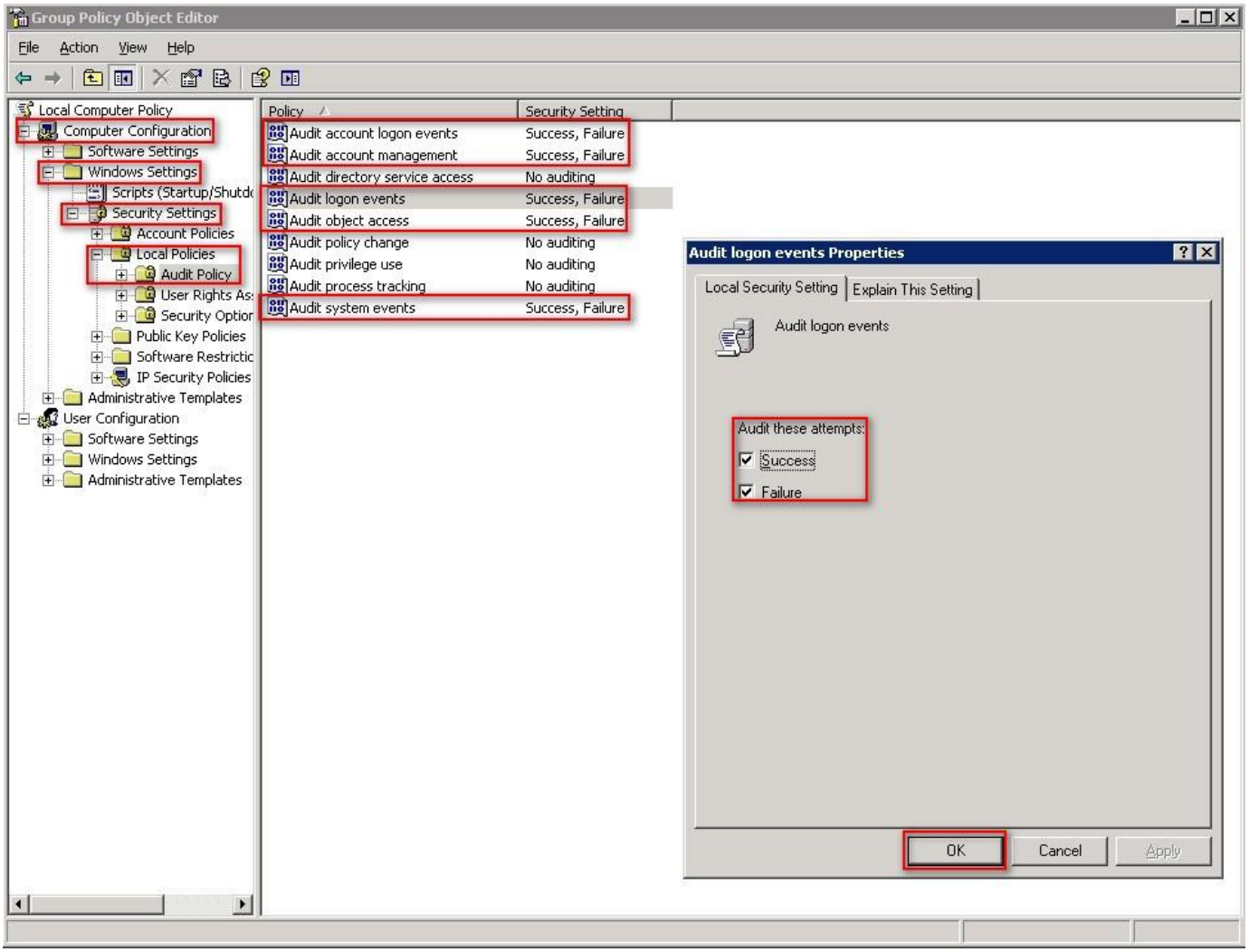


(2) Search for Group Policy

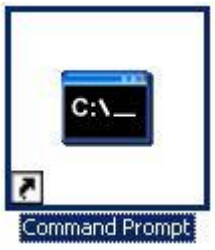
Enter “gpedit.msc” -> And click “Search” -> Click on “gpedit” in the search results.

(3) Local Group Policies: Audit Policies

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: “Success” & “Failure” -> Click “OK.”



(4) Open “Command Prompt.”



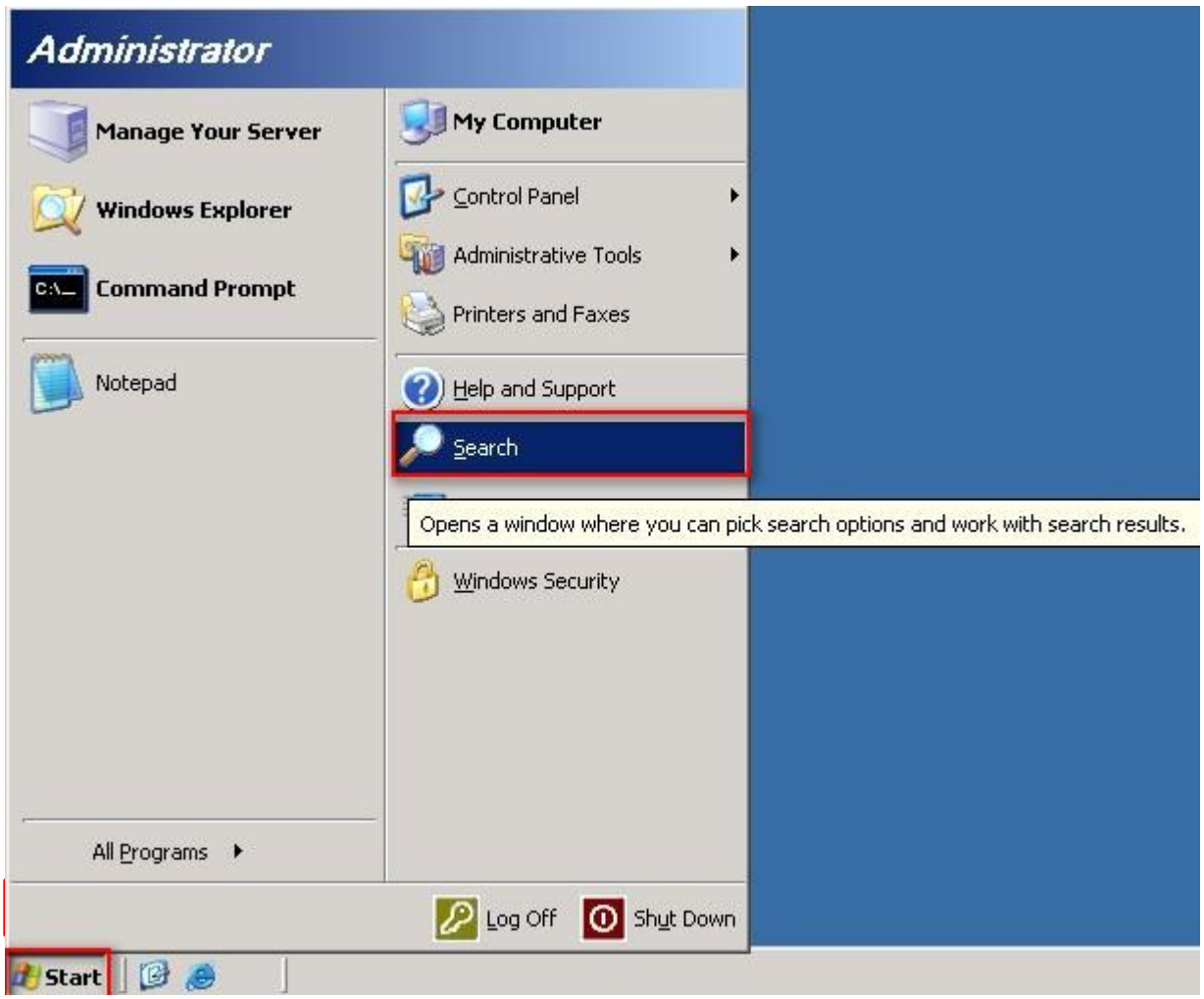
(5) Enter the command below to refresh group policy.

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

3.2.2 Event Log Settings

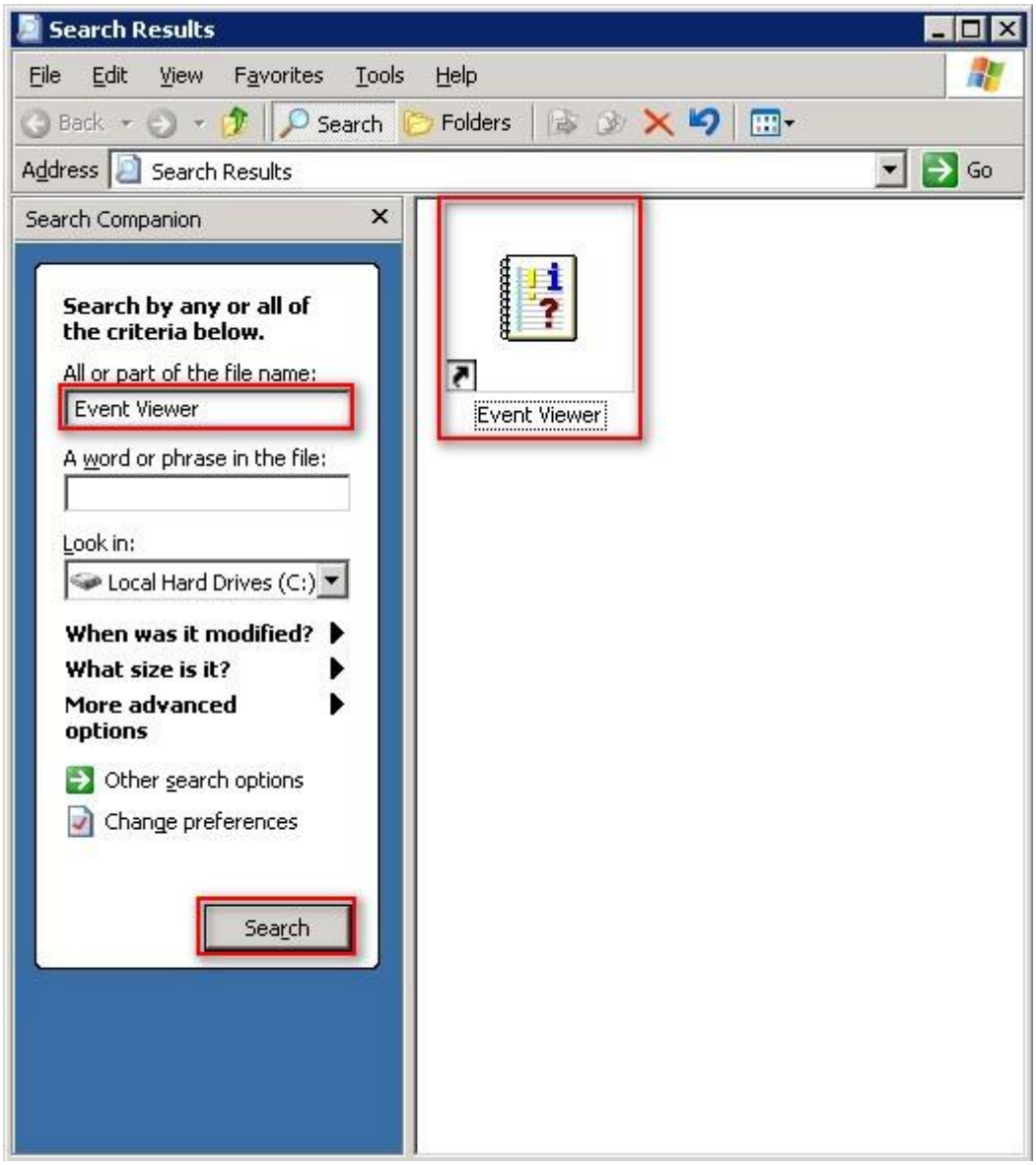
(1) Open “Search.”

Click on “Start” -> “Search.”



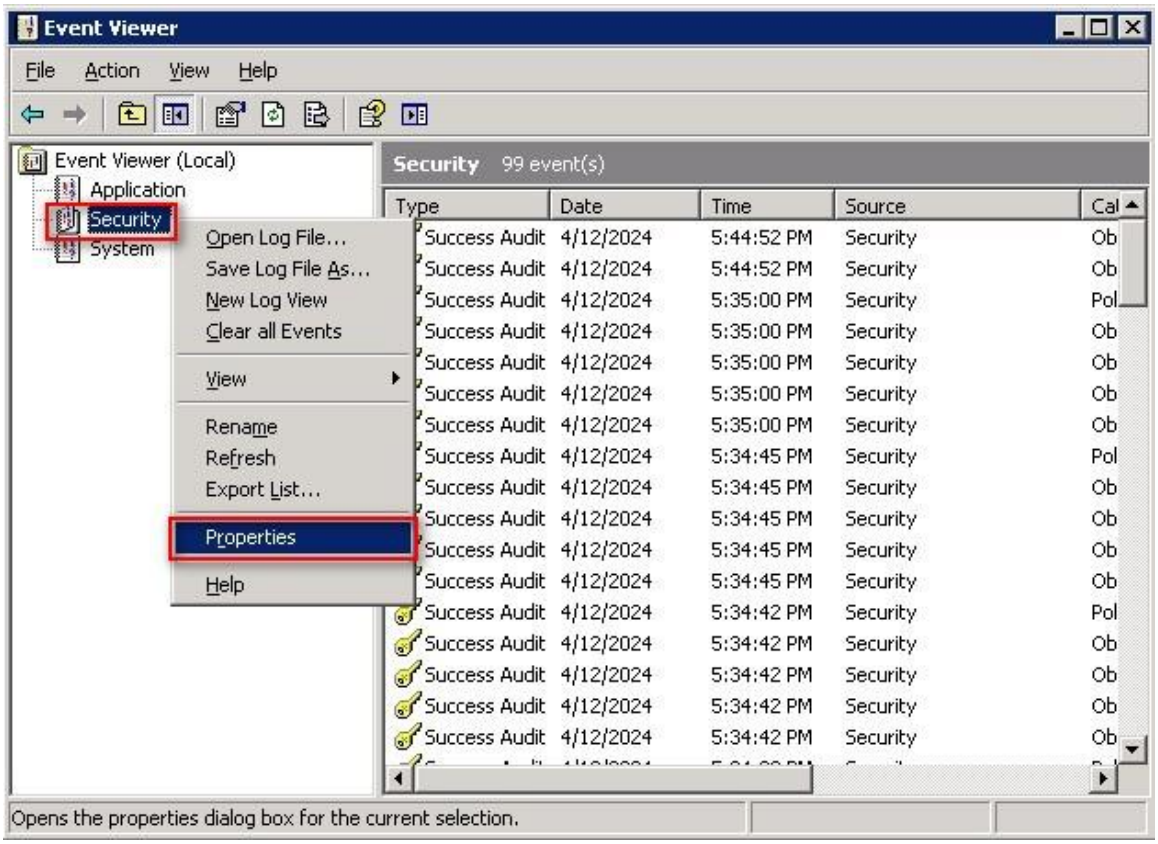
(2) Search for “Event Viewer”

Enter “Event Viewer” -> And click “Search Now” -> Click on “Event Viewer” in the search results.



(3) Edit Security Log

Right-click on “Security” -> And click on “Properties.”

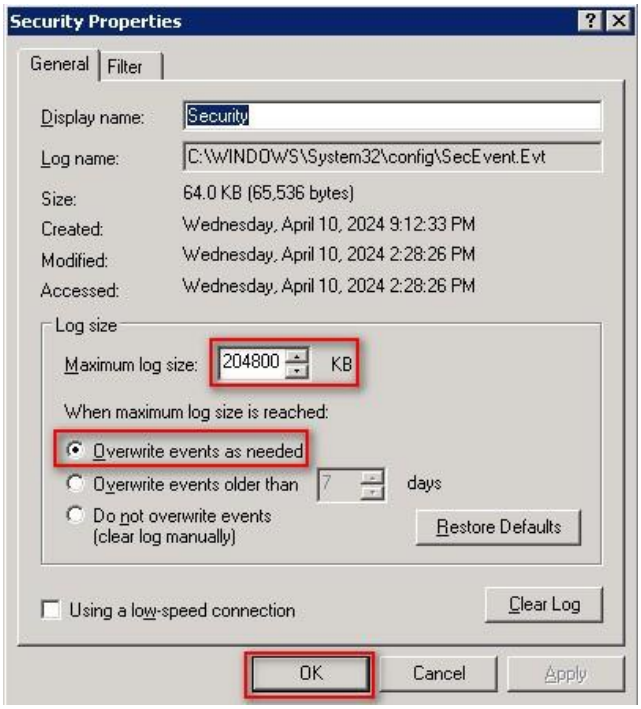


(4) Configure Security Log

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.”



4. For Windows 2008

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendation” link provided in “preface” for detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

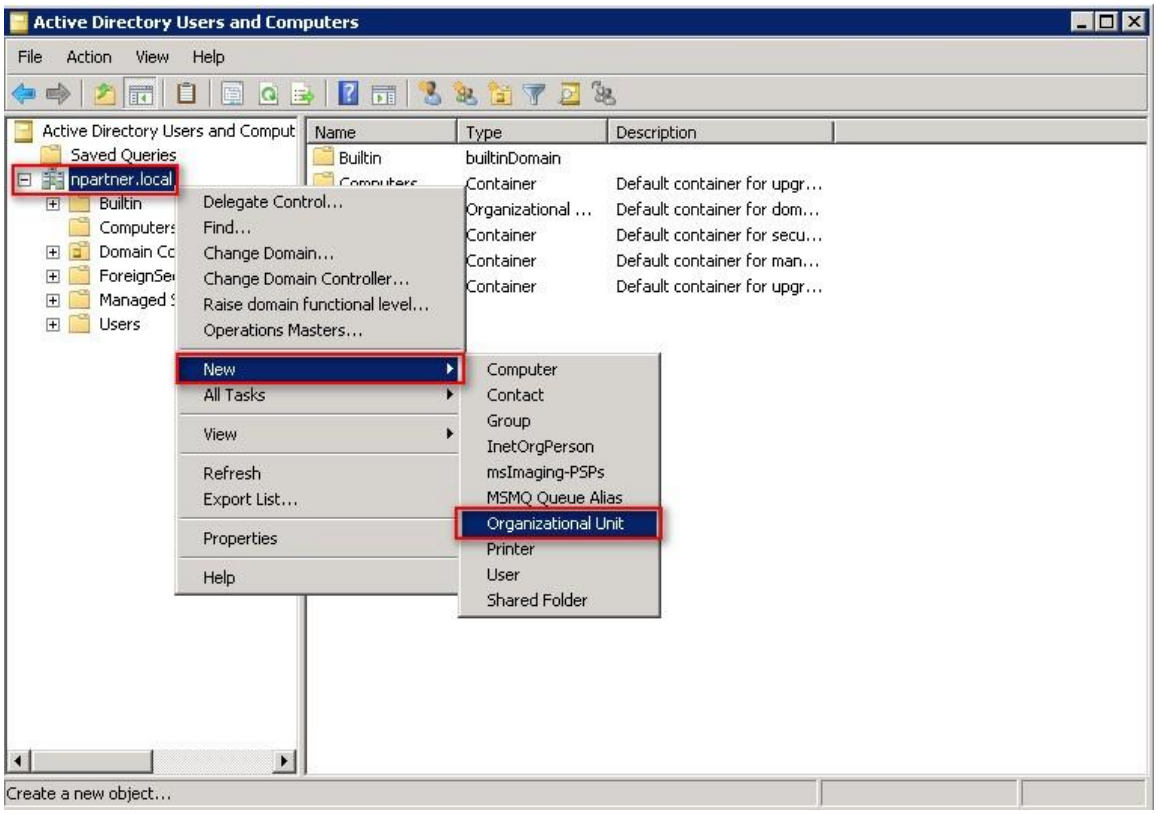
4.1 Domain

4.1.1 Organizational Unit Setup

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

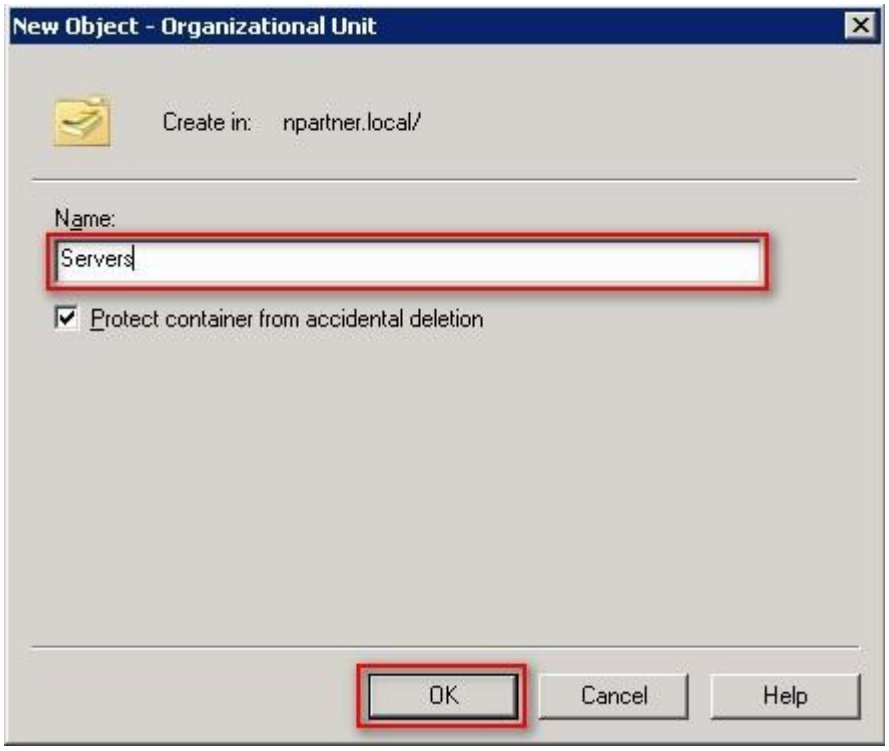
(2) Add Your Organizational Unit

Right-click on your “Domain Name” (In this example, it is “npartner.local”), select “New” and click “Organizational Unit.”



(3) Name Your Organizational Unit

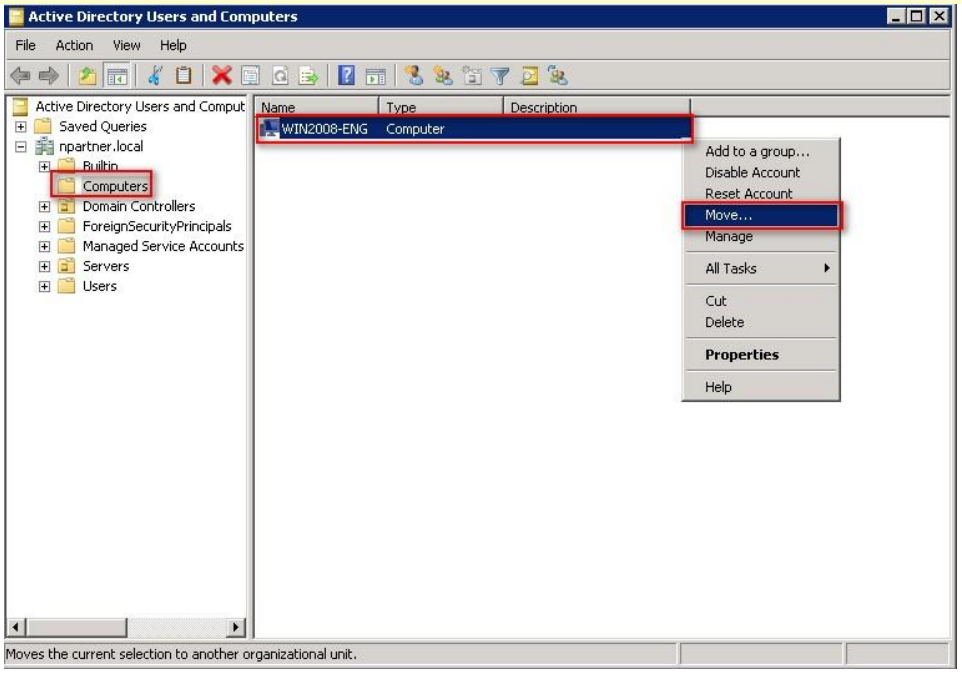
Enter your “Organizational Unit Name,” (In this example, it is “Servers”) Note: Please create the organizational unit name based on the client's environment. -> Click “OK.”



(4) Move Your Server to New Organizational Unit

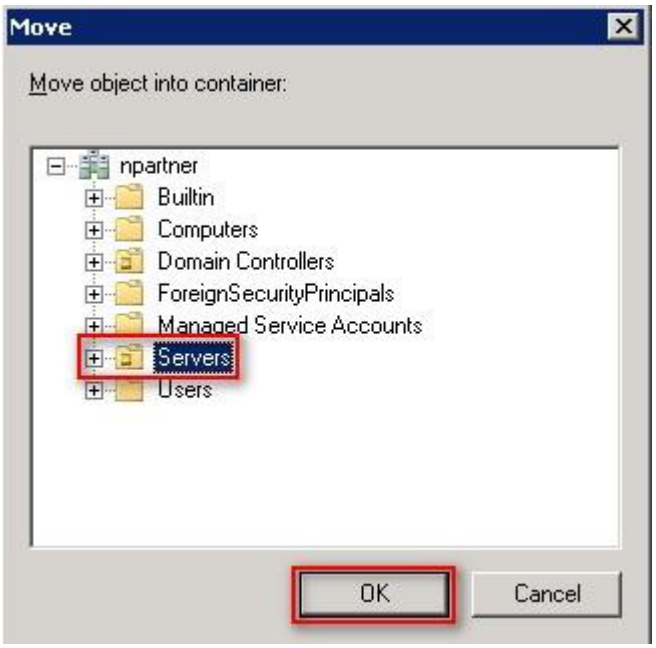
Select your organizational unit from the original folder (the example here is “Computers”) -> Right-click on the “WIN2008-ENG” server.

Note: Please select the Windows server host based on actual environment. -> Click “Move.”



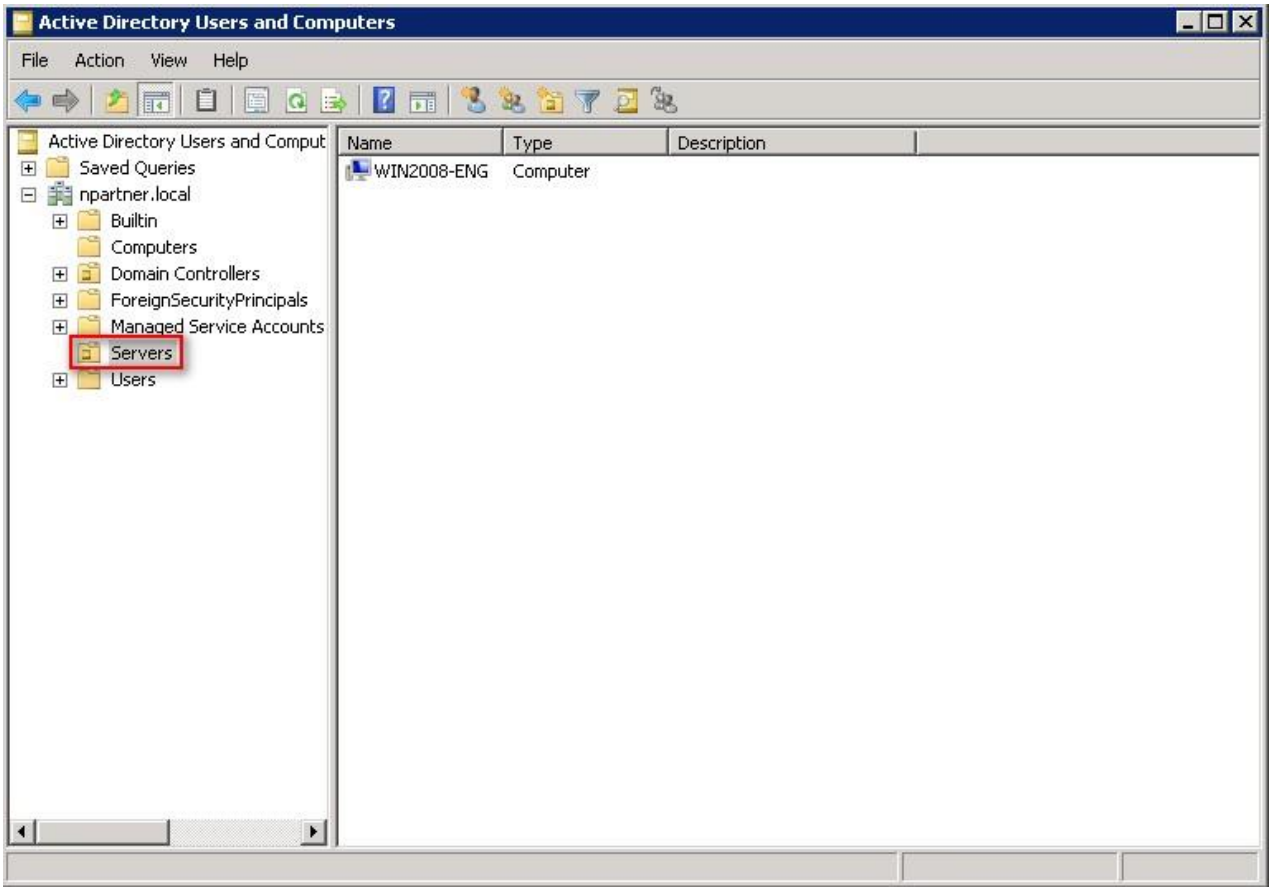
(5) Select Your New Organizational Unit

Select your organizational unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

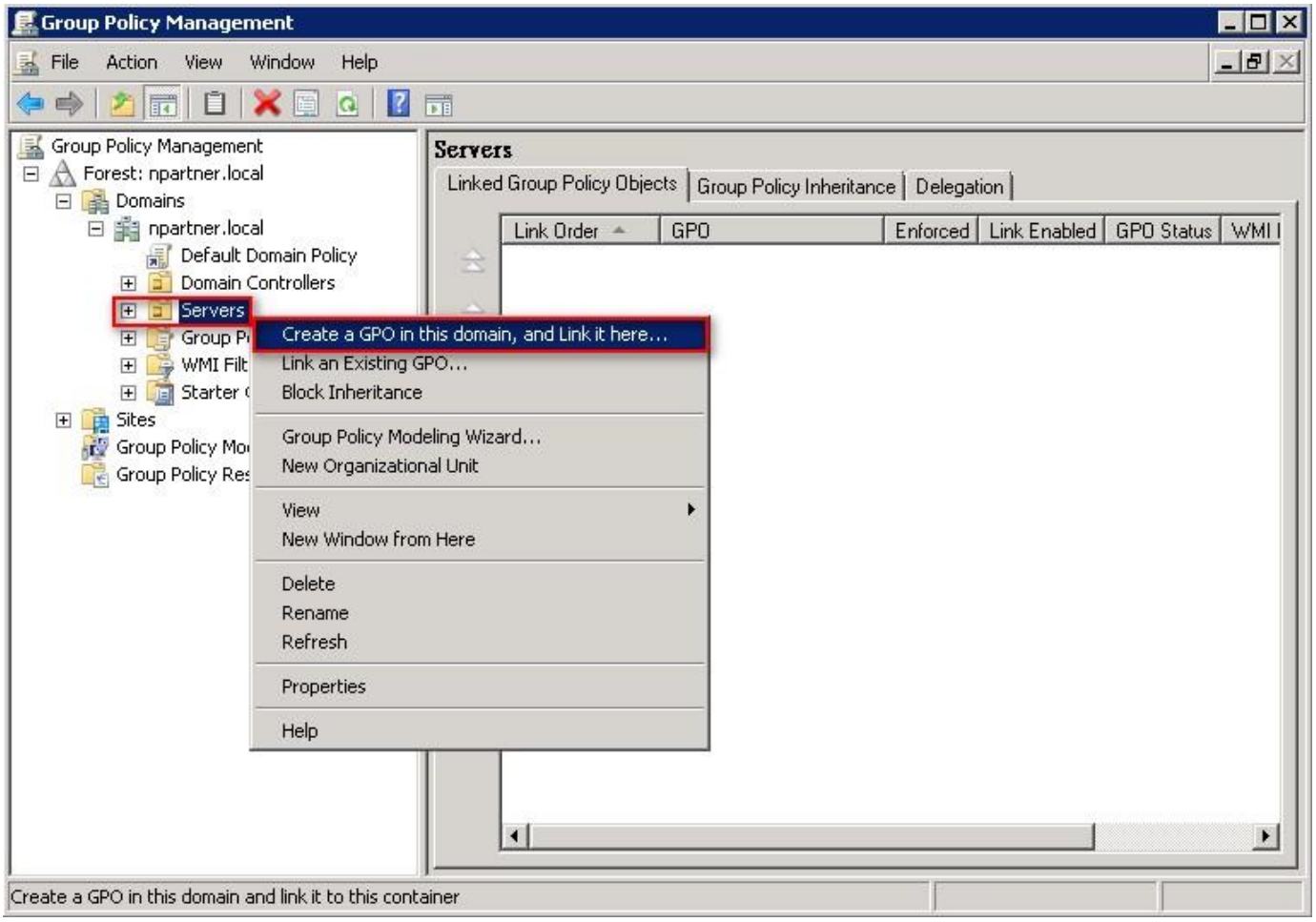
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2008-ENG” server has been moved.



4.1.2 Group Policy Settings

(1) Open “Group Policy Management.”

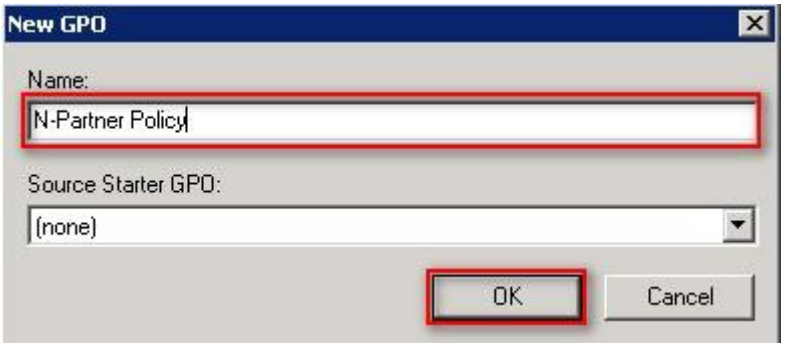
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

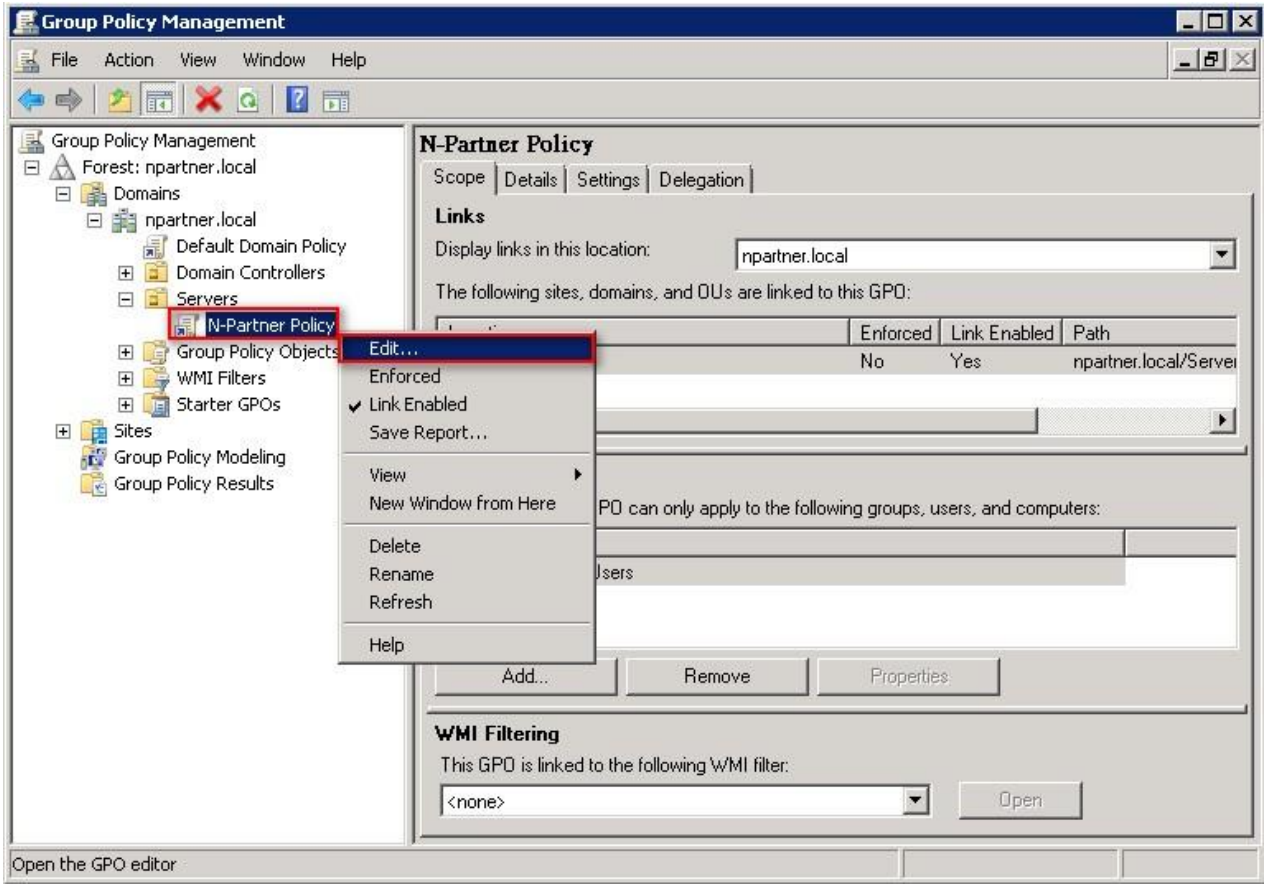
Enter your group policy object name (the example here is “N-Partner Policy”).

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



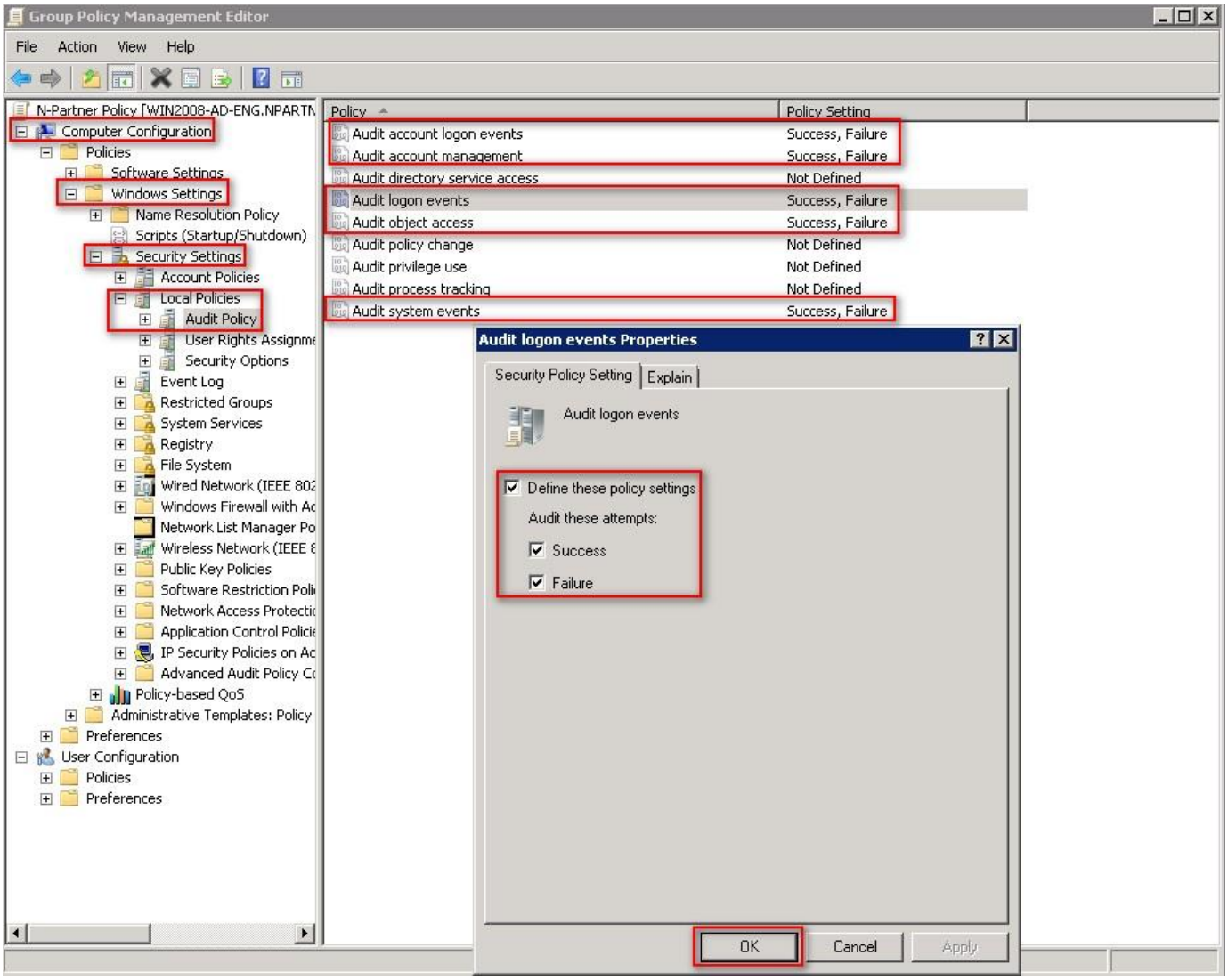
(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is N-Partner Policy) and click “Edit.”



(5) Local Group Policies: Audit Policy

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

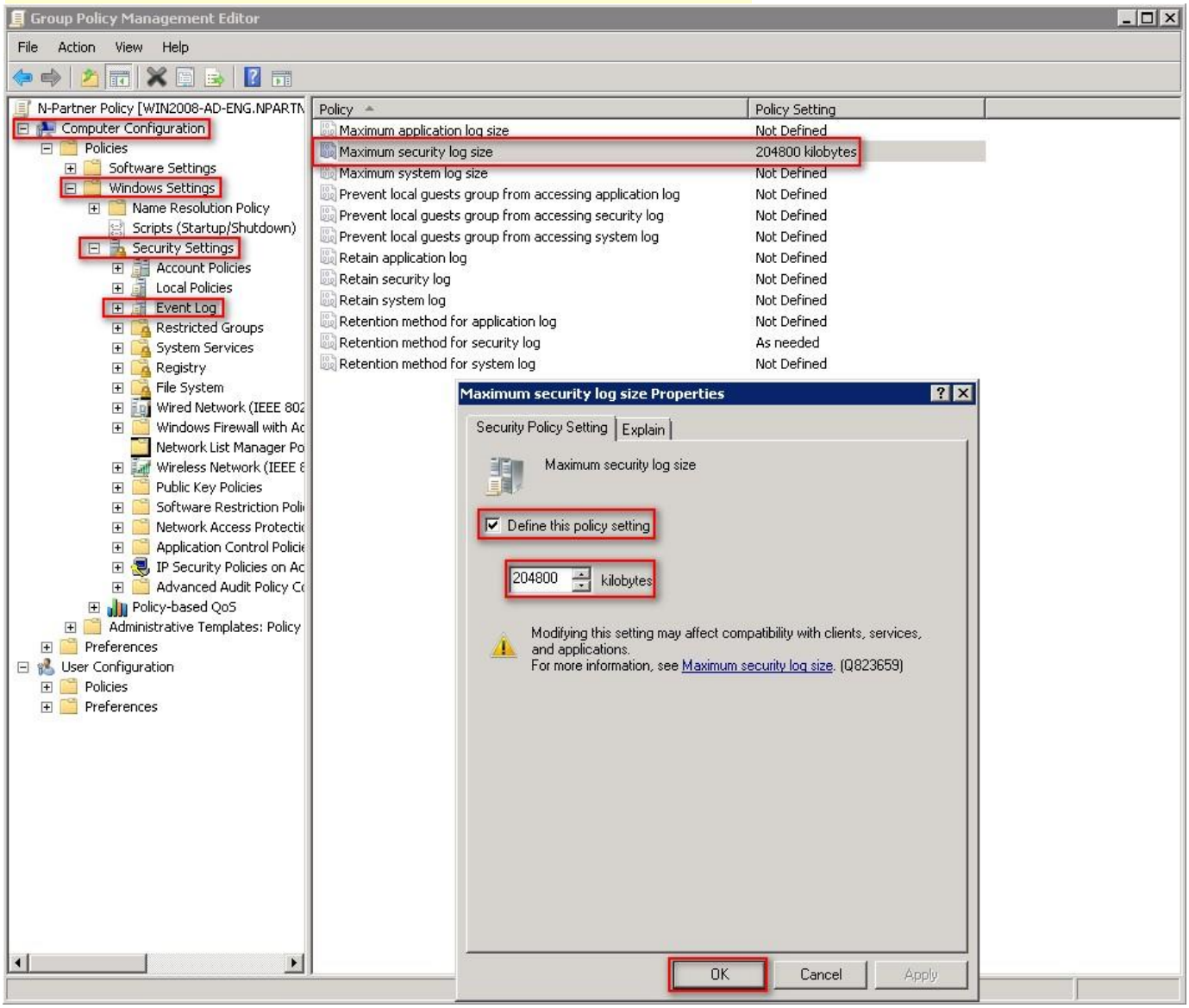


(6) Event Logs: Maximum Size of Security Log

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

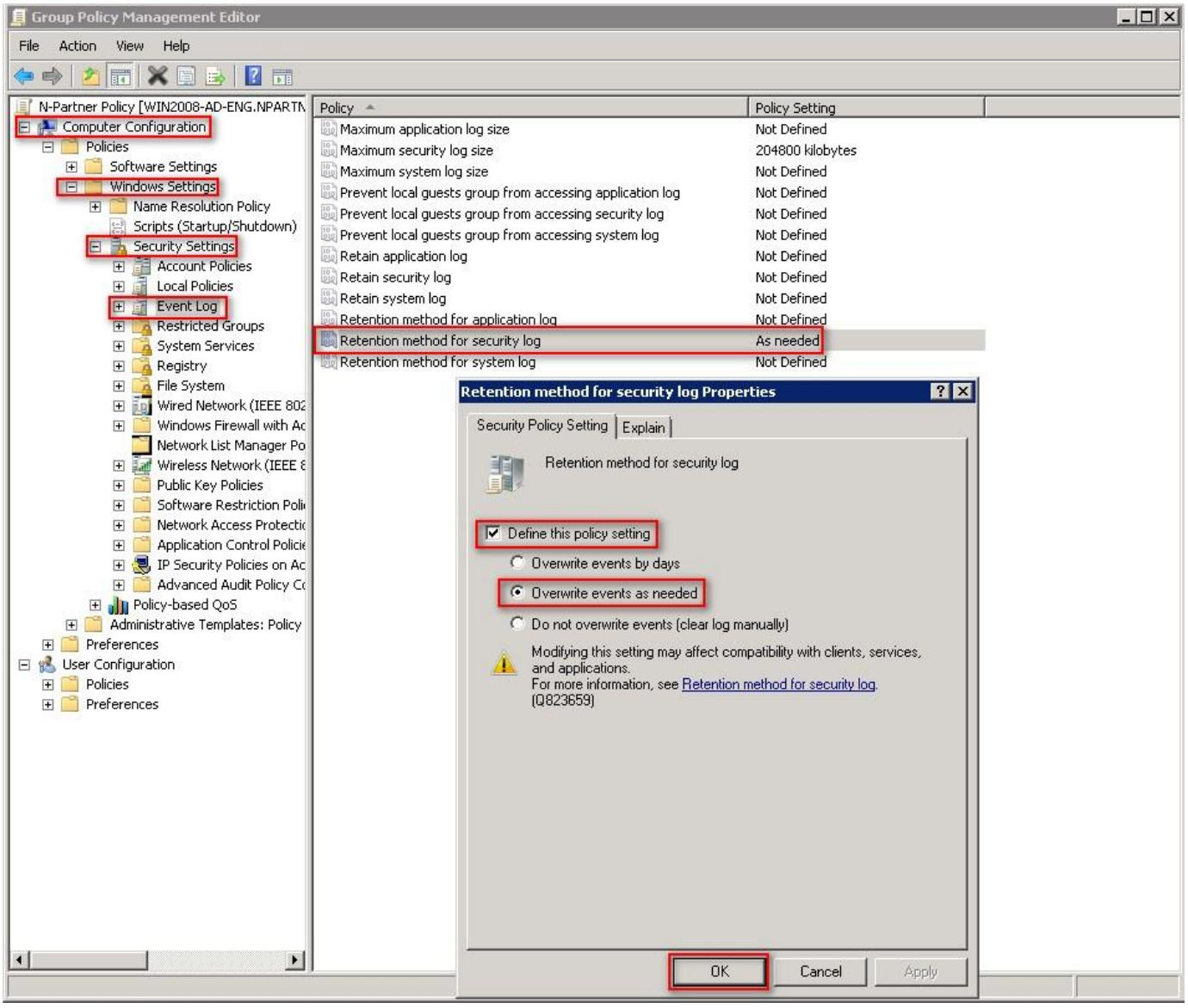
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click [OK].



(7) Event Logs: Retention Method for Security Log

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



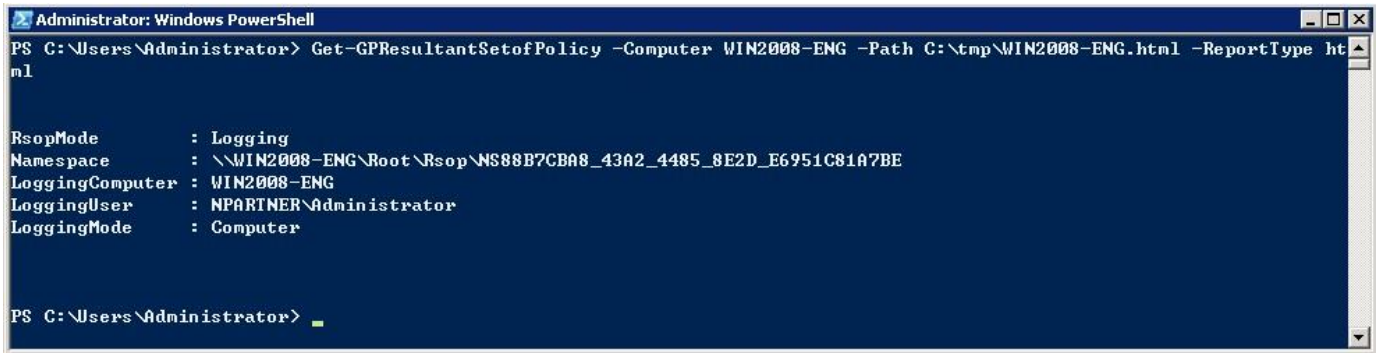
(8) Open “Windows PowerShell” on your Windows server.

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

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

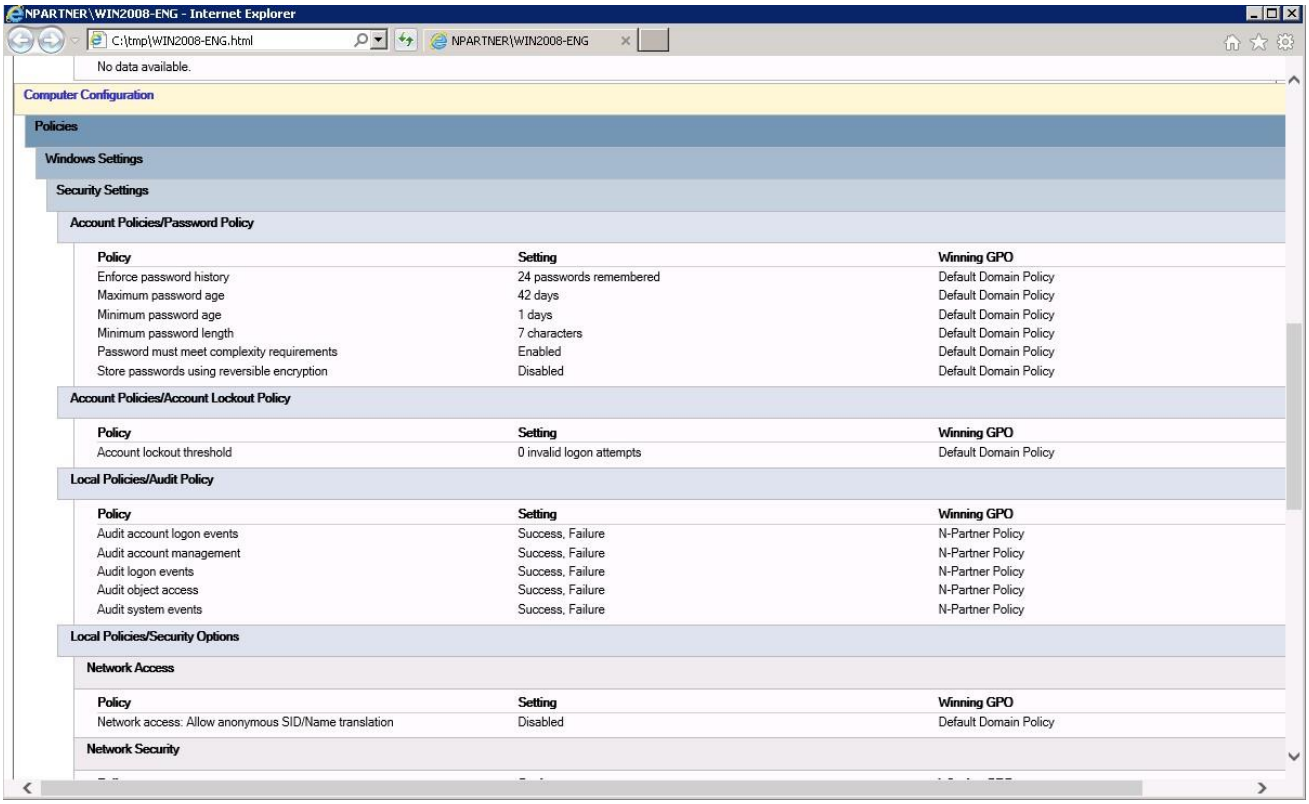
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2008-ENG -Path C:\tmp\WIN2008-ENG.html -ReportType html
```



Please enter your Windows server hostname and the folder path including the file name in red text.

(11) Open your report. -> Confirm your Windows server hostname. -> Apply the N-Partner Policy Group Policy.



4.2 Workgroup

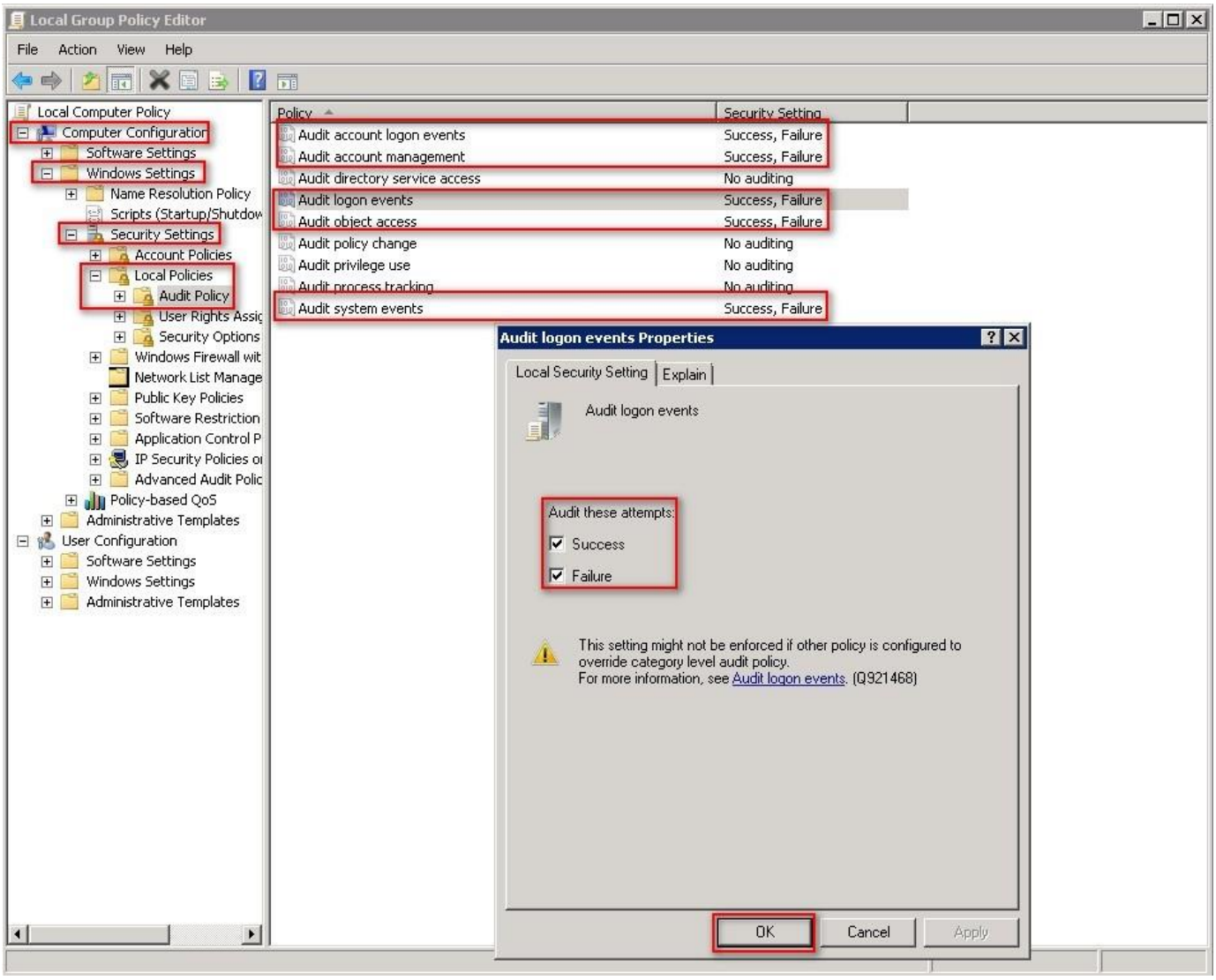
4.2.1 Audit Policy Settings

(1) Open Local Group Policy Editor

Click on “Start” -> Enter “edit group policy” to search -> Click on “Edit Group Policy.

(2) Local Group Policies: Audit Policy

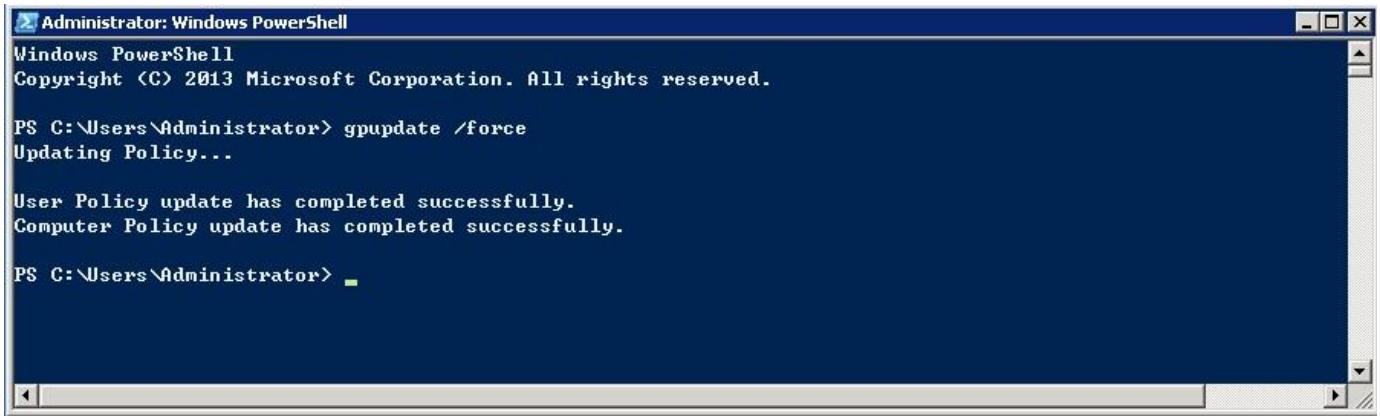
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Define these policy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



(3) Open “Windows PowerShell.”

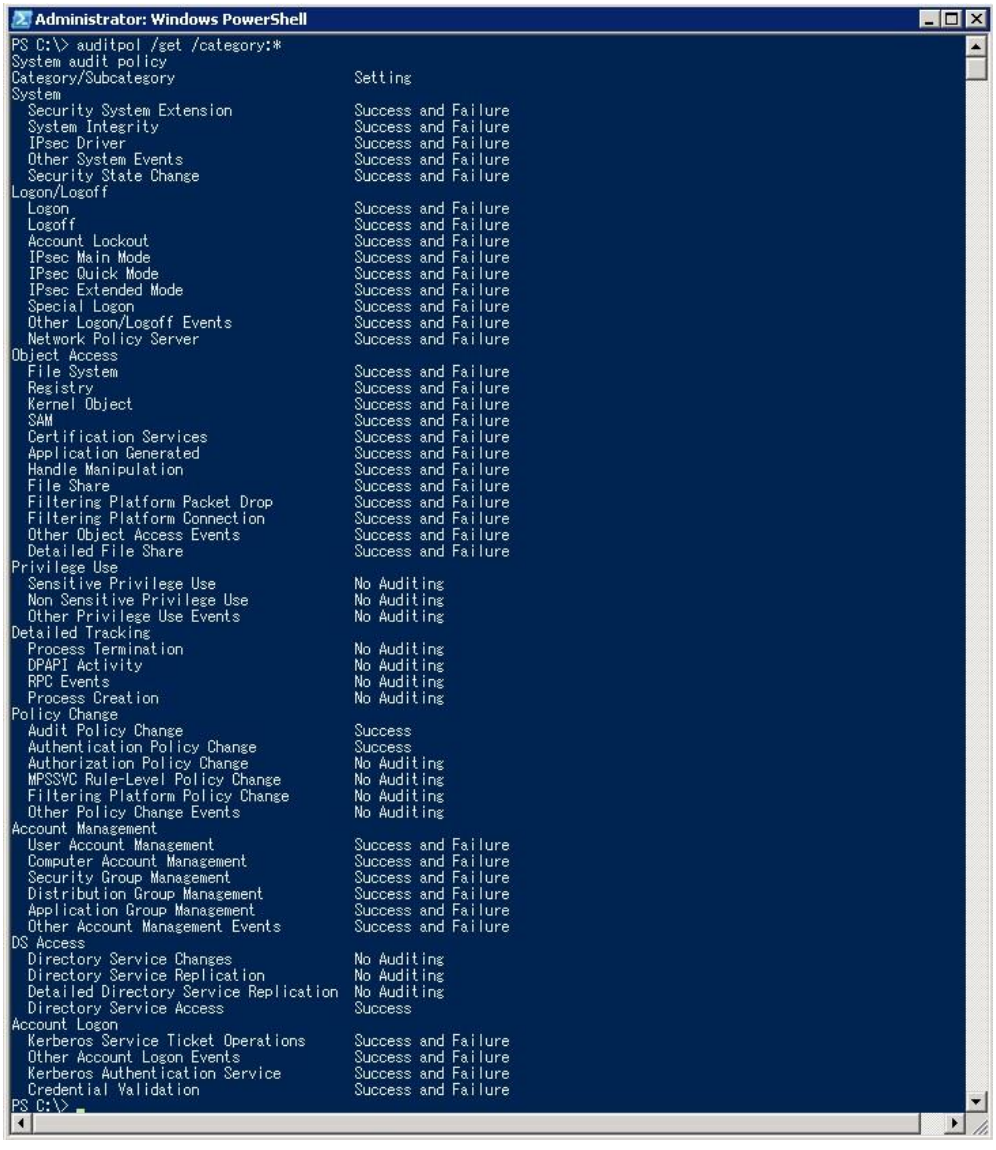
(4) Enter the command below to refresh group policy.

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



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

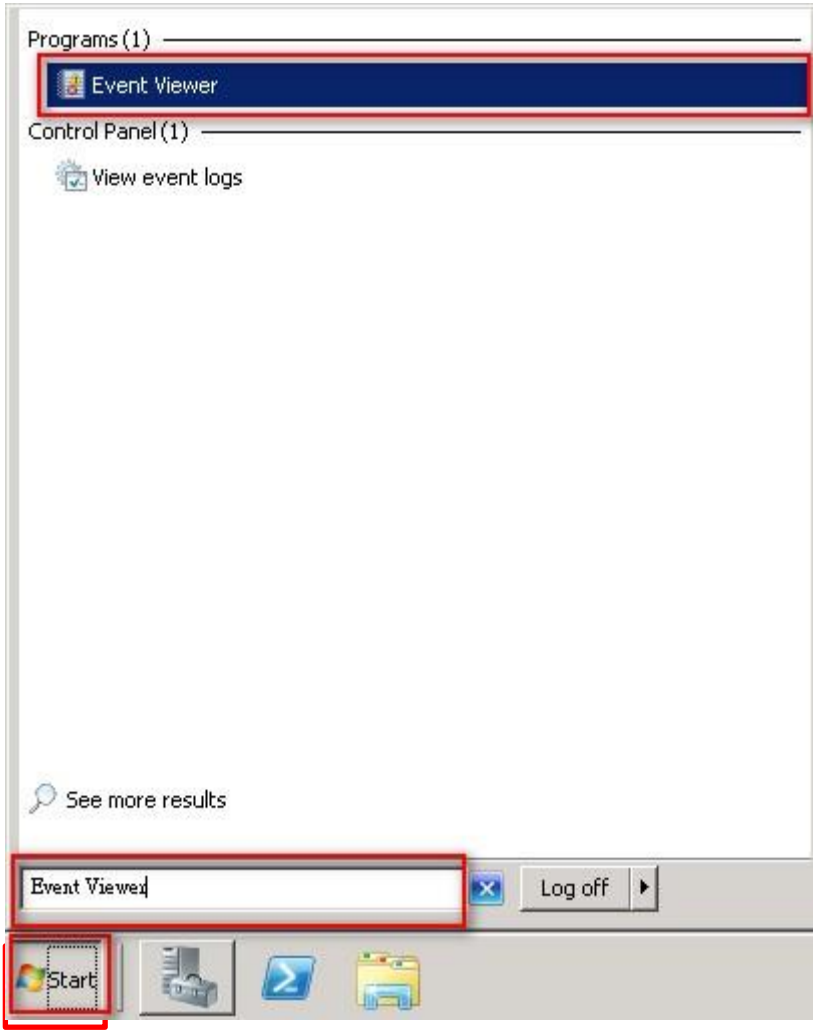
```
PS C: \> auditpol /get /category:*
```



4.2.2 Event Log Settings

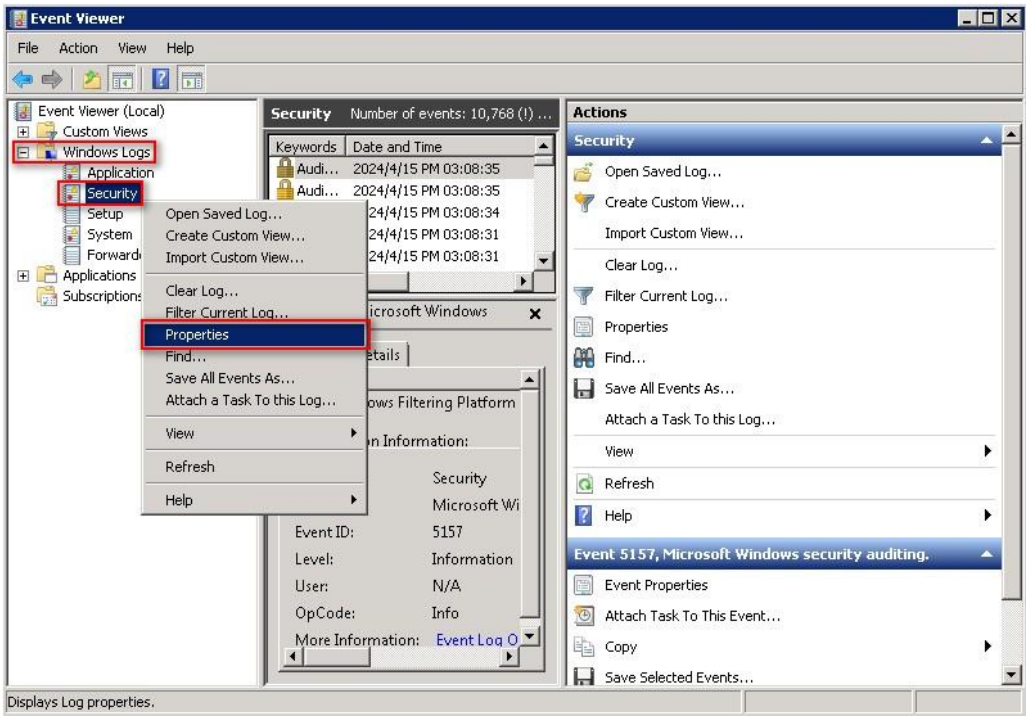
(1) Search for “Event Viewer”

Enter “Event Viewer” to search -> Click on “Event Viewer” in the search results.



(2) Edit Security Log

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

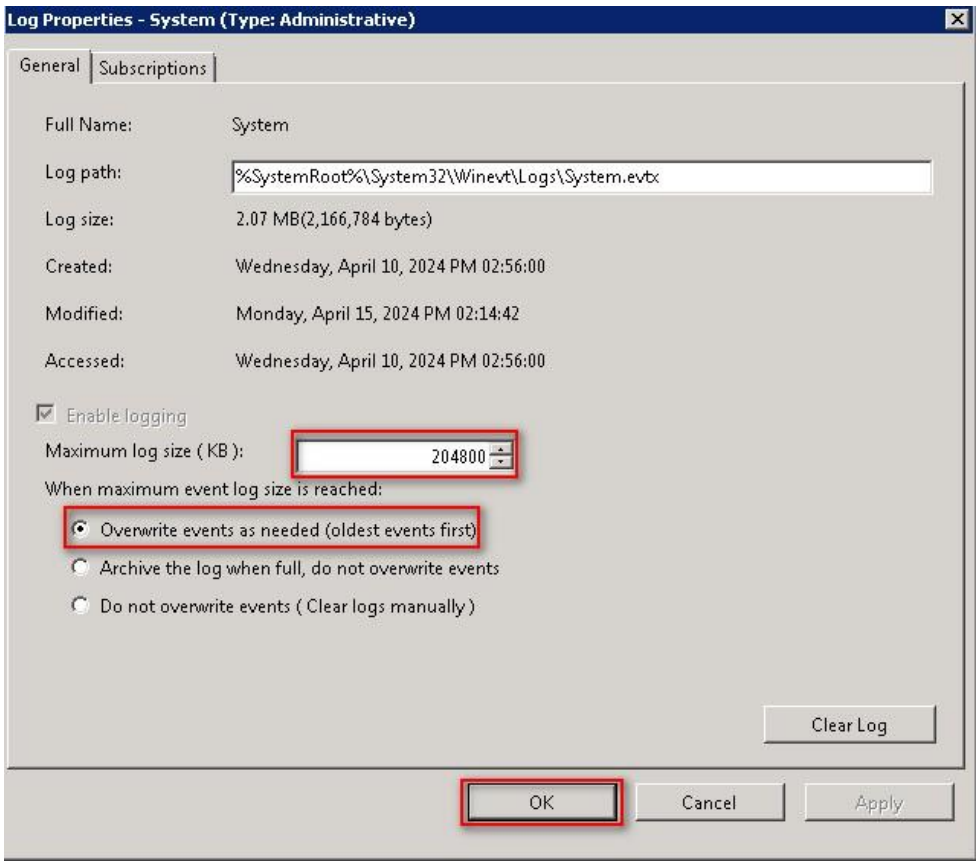


(3) Configure Security Log

Enter maximum log file size: 204800 KB

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

-> Click on “Overwrite events as needed” -> Click “OK.”



5. For Windows 2012

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendationlink provided in prefacefor detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

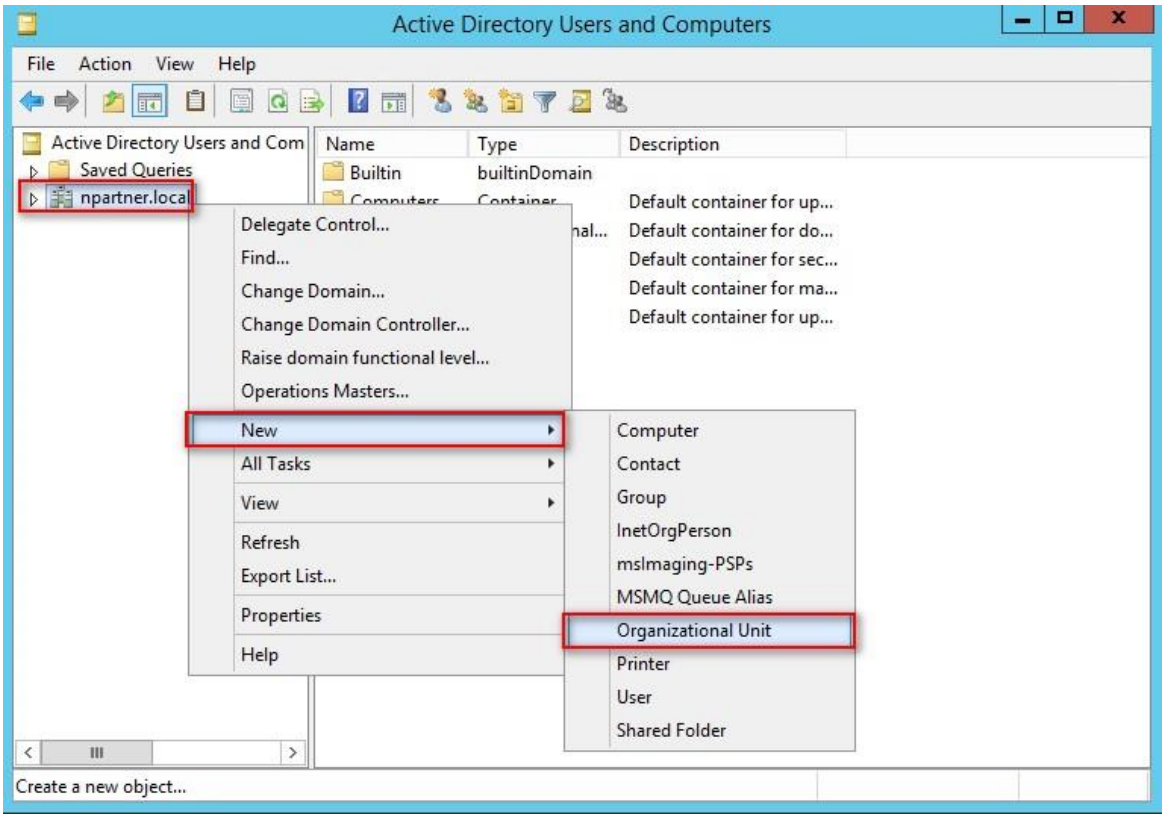
5.1 Domain

5.1.1 Organizational Unit Setup

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

(2) Add Your Organizational Unit

Right-click on your “Domain Name,” (in this example, it is “npartner.local), select “New” and click “Organizational Unit.”

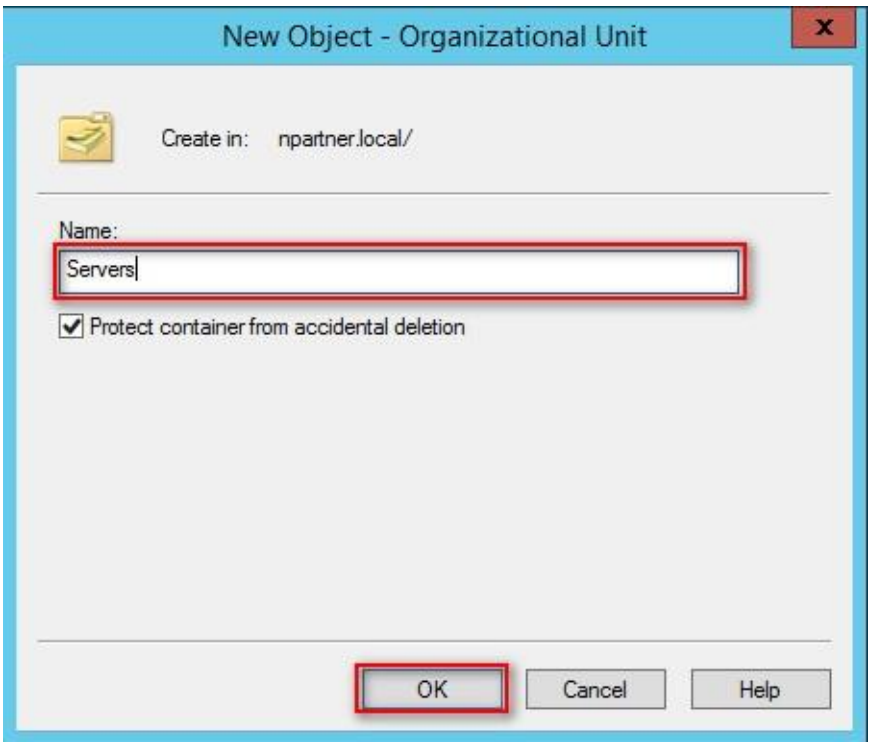


(3) Name Your Organizational Unit

Enter your “Organizational Unit Name,” (in this example, it is “Servers”)

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

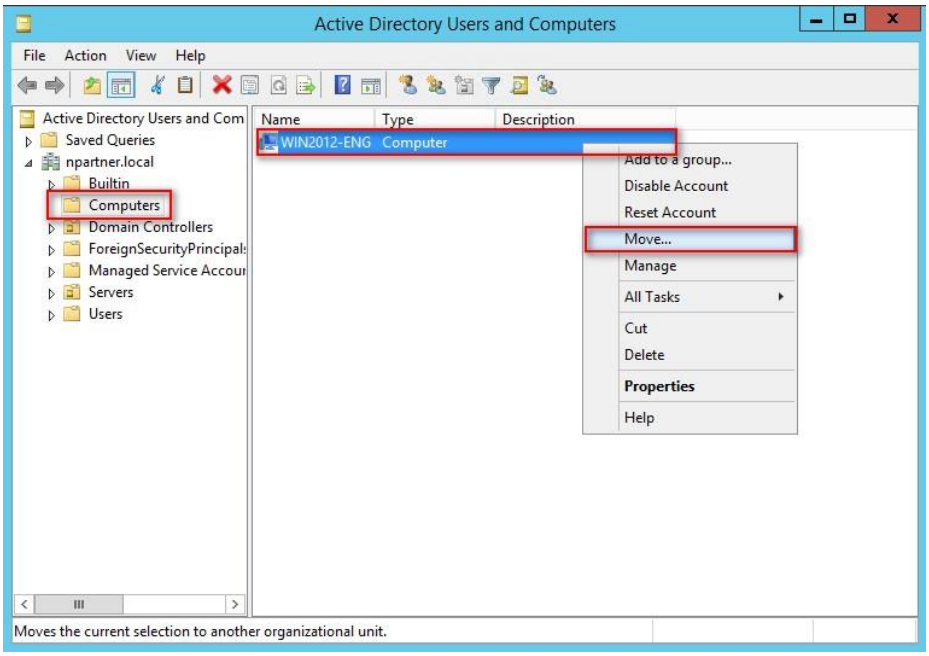
-> and click “OK.”



(4) Move Your Server to New Organizational Unit

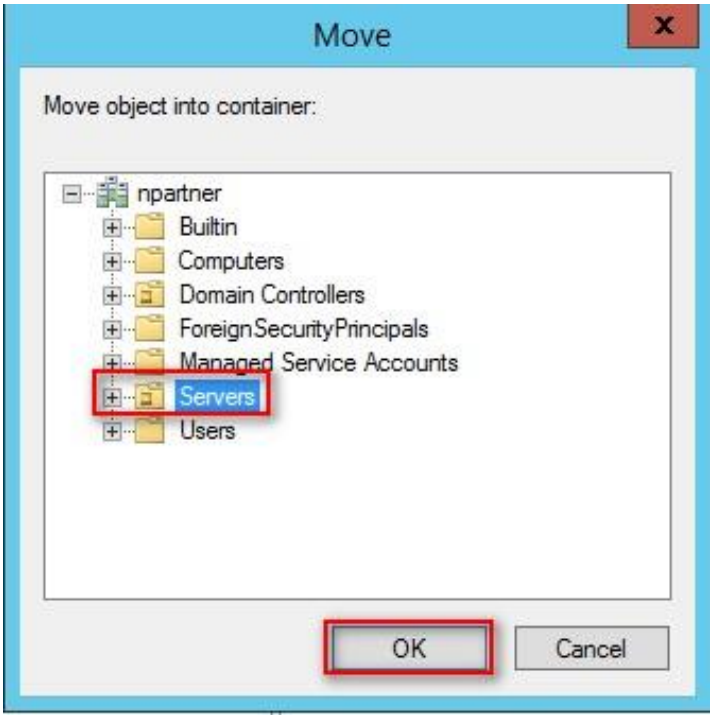
Select your organizational unit (the example here is “Computers”) -> Right-click on the “WIN2012-ENG” server.

Note: Please select the Windows Server host based on actual environment .-> Click “Move.”



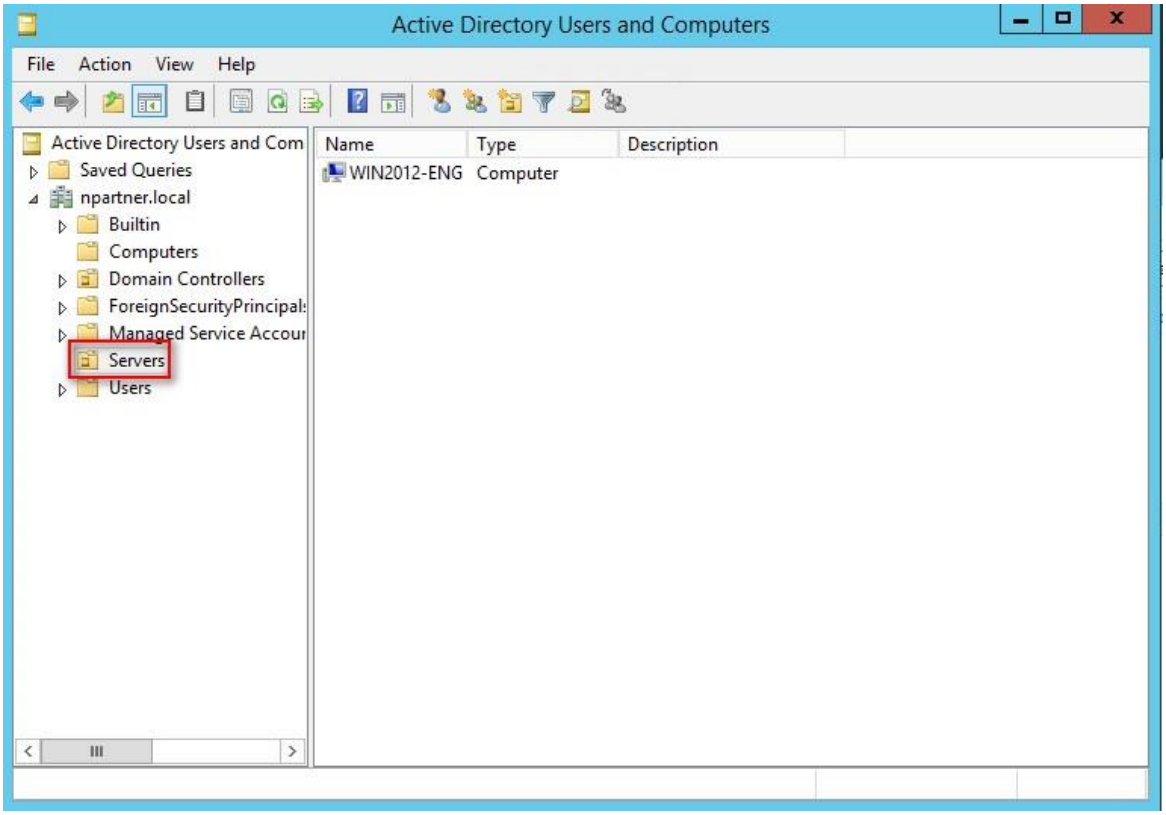
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

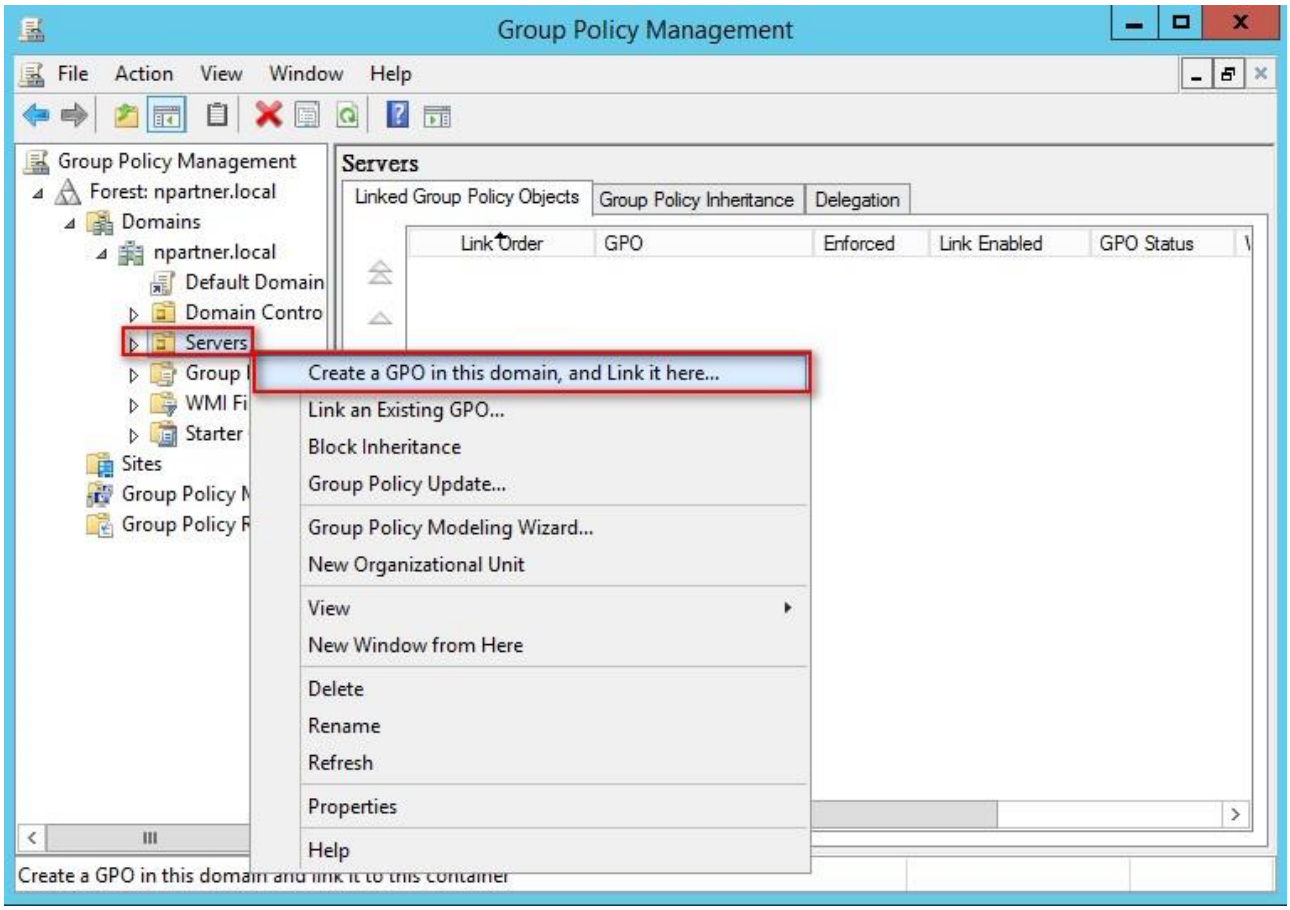
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2012-ENG” server has been moved.



5.1.2 Group Policy Settings

(1) Open “Group Policy Management.”

(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



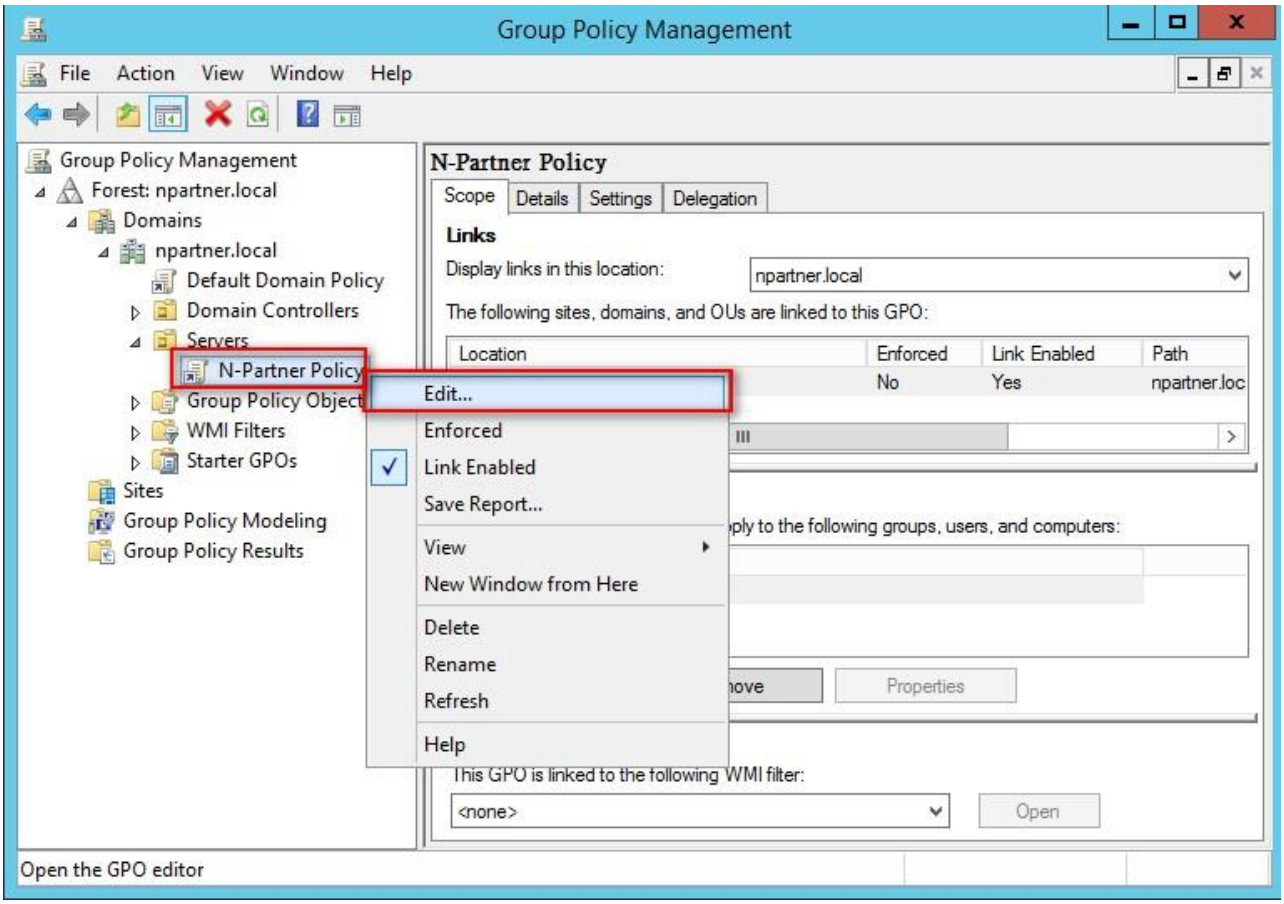
(3) Name Your Group Policy Object

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

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

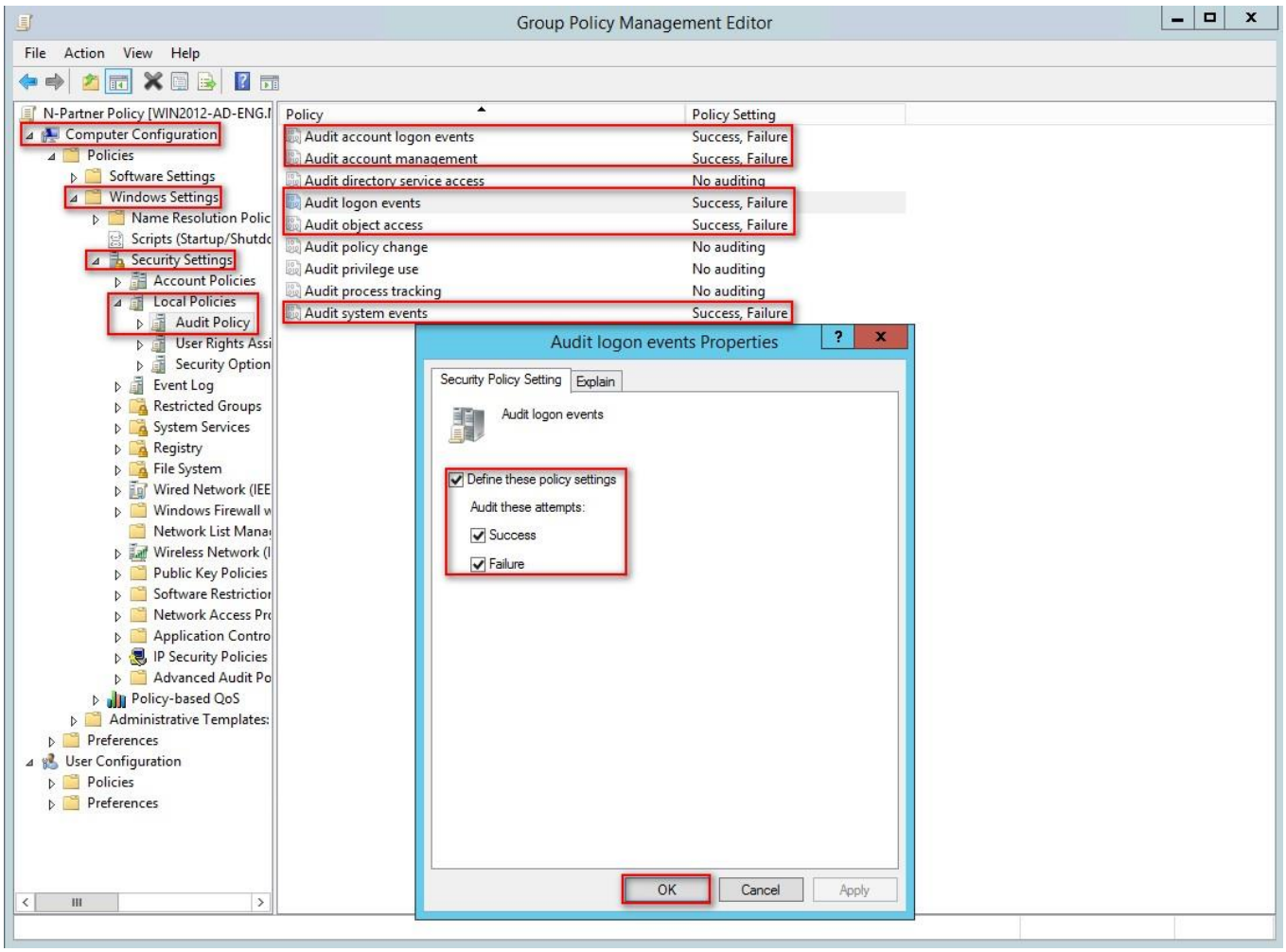
(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is “N-Partner Policy”) and click “Edit.”



(5) Local Group Policies: Audit Policy

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

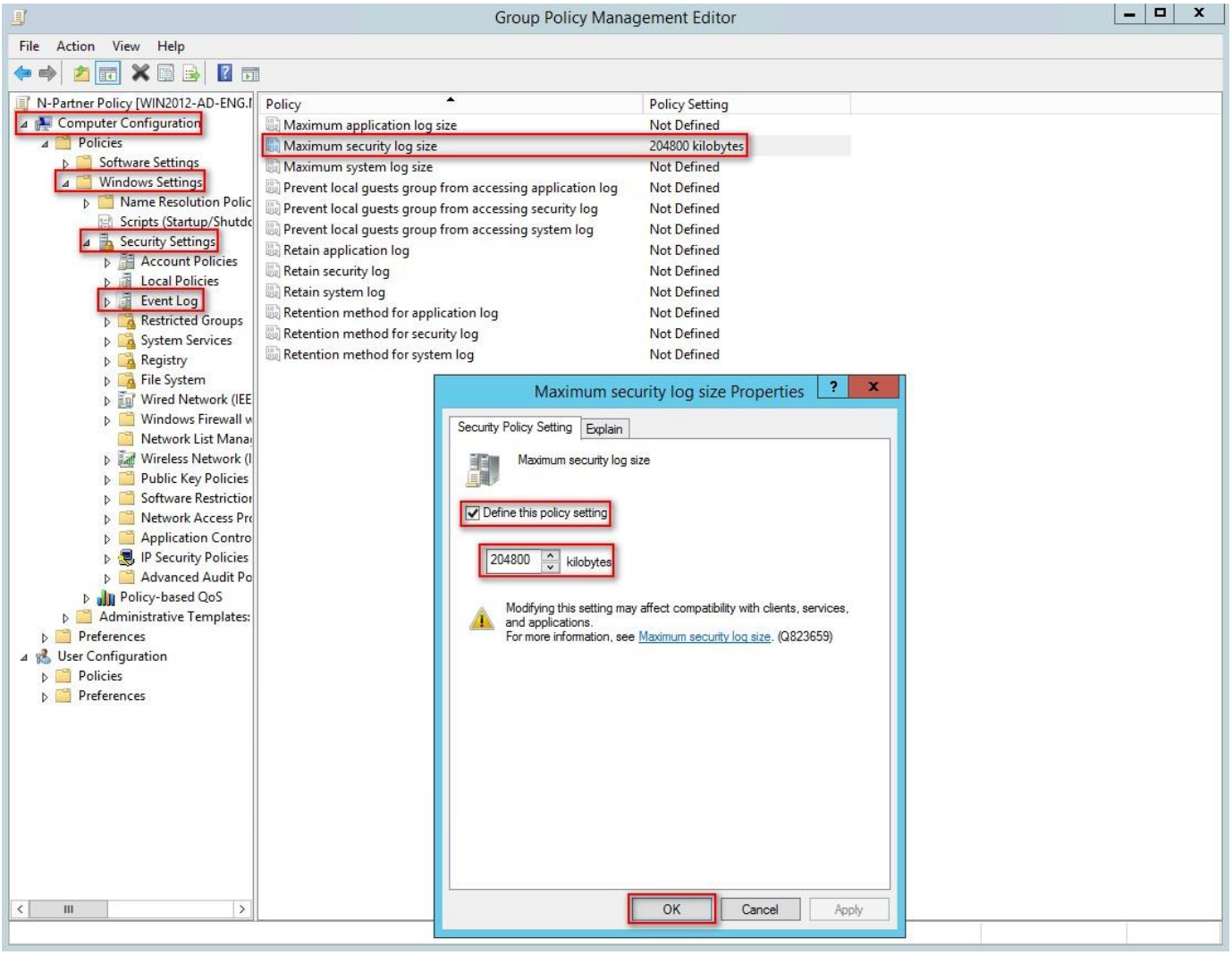


(6) Event Logs: Maximum Size of Security Log

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

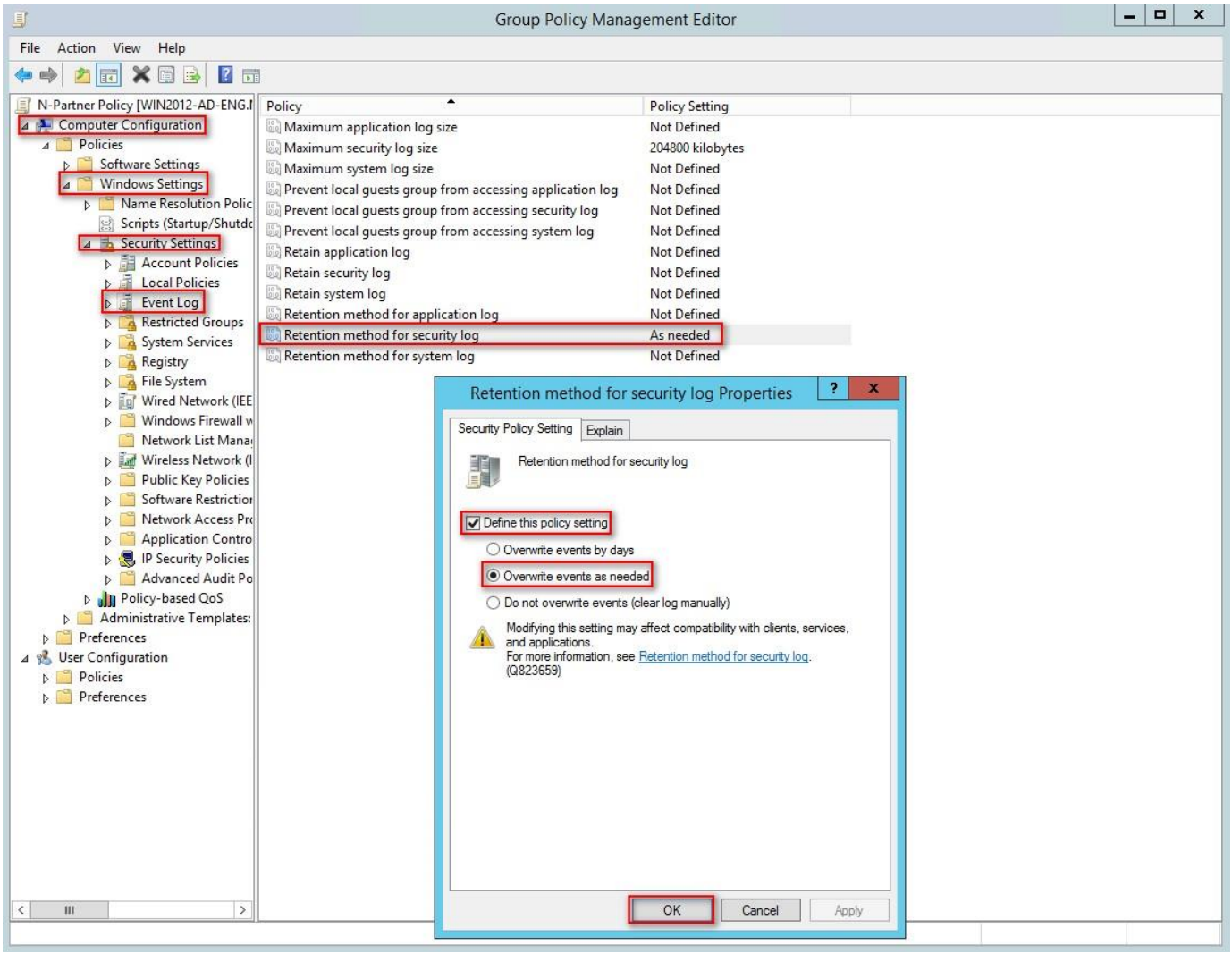
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click [OK].



(7) Event Logs: Retention Method for Security Log

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



(8) Open “Windows PowerShell” on your Windows server.

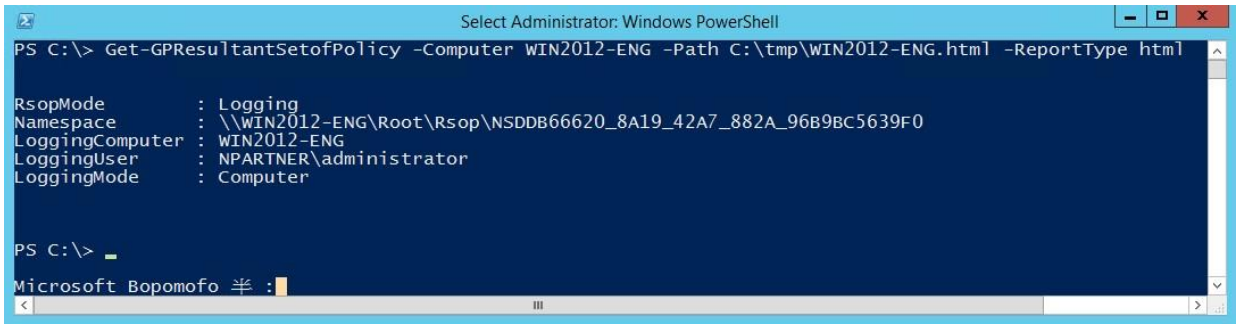
(9) Enter the command below to refresh group policy.

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

Please enter your Windows Server hostname in red text.

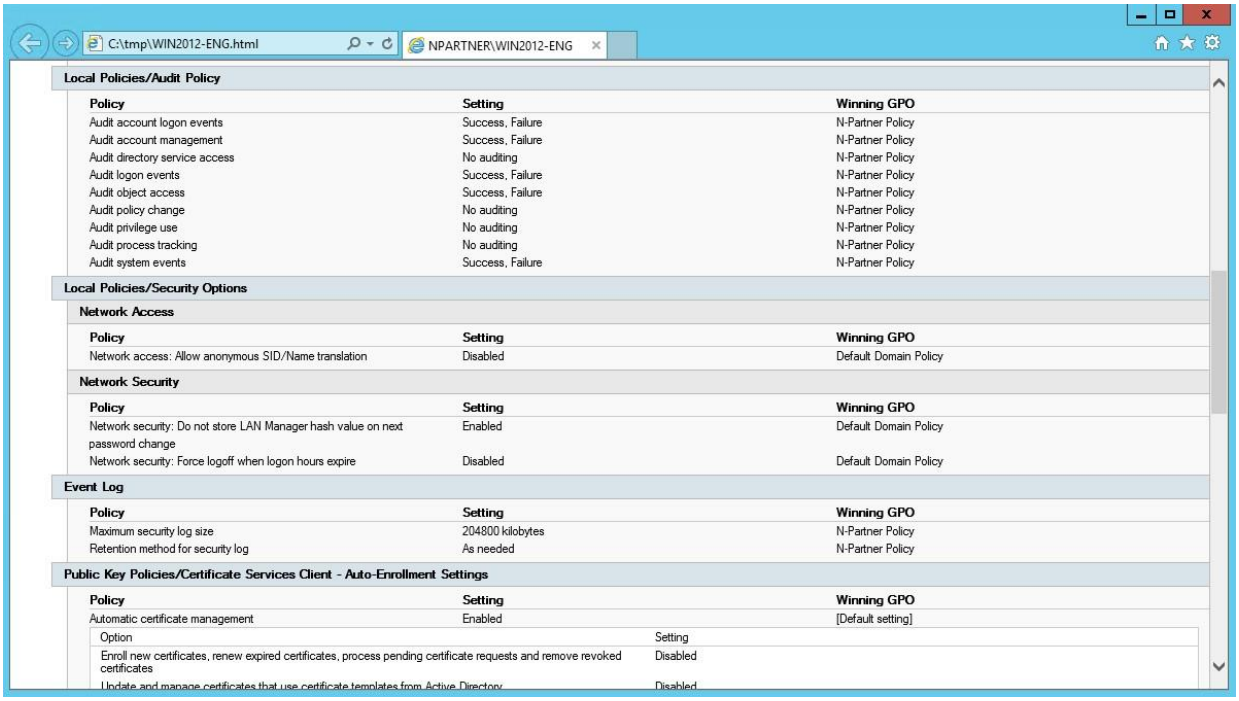
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

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



Please enter your Windows server hostname and the folder path including the file name in red text.

(11) Open your report. -> Confirm your Windows server hostname. -> Apply the N-Partner Policy Group Policy.



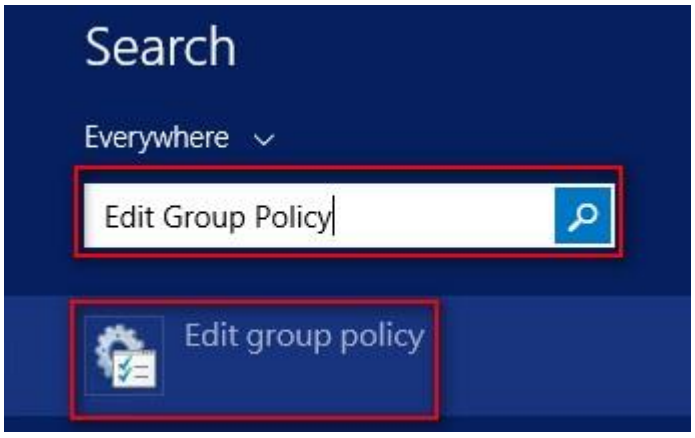
5.2 Workgroup

5.2.1 Audit Policy Settings

(1) Move the cursor to the bottom right corner and click on “Search.”

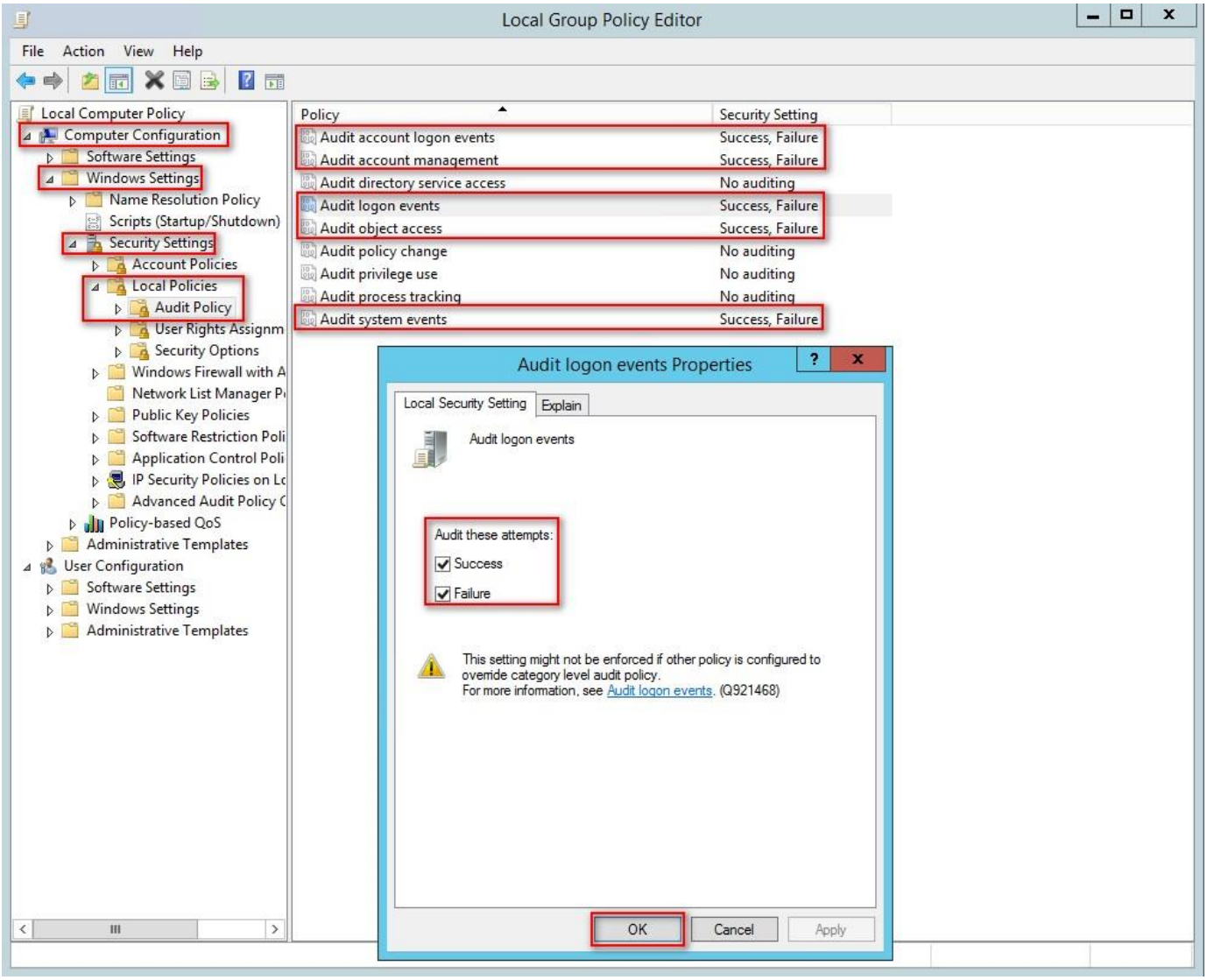
(2) Search for “Group Policy Object Editor”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy.”



(3) Local Group Policies: Audit Policies

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: “Success” & “Failure” -> Click “OK.”



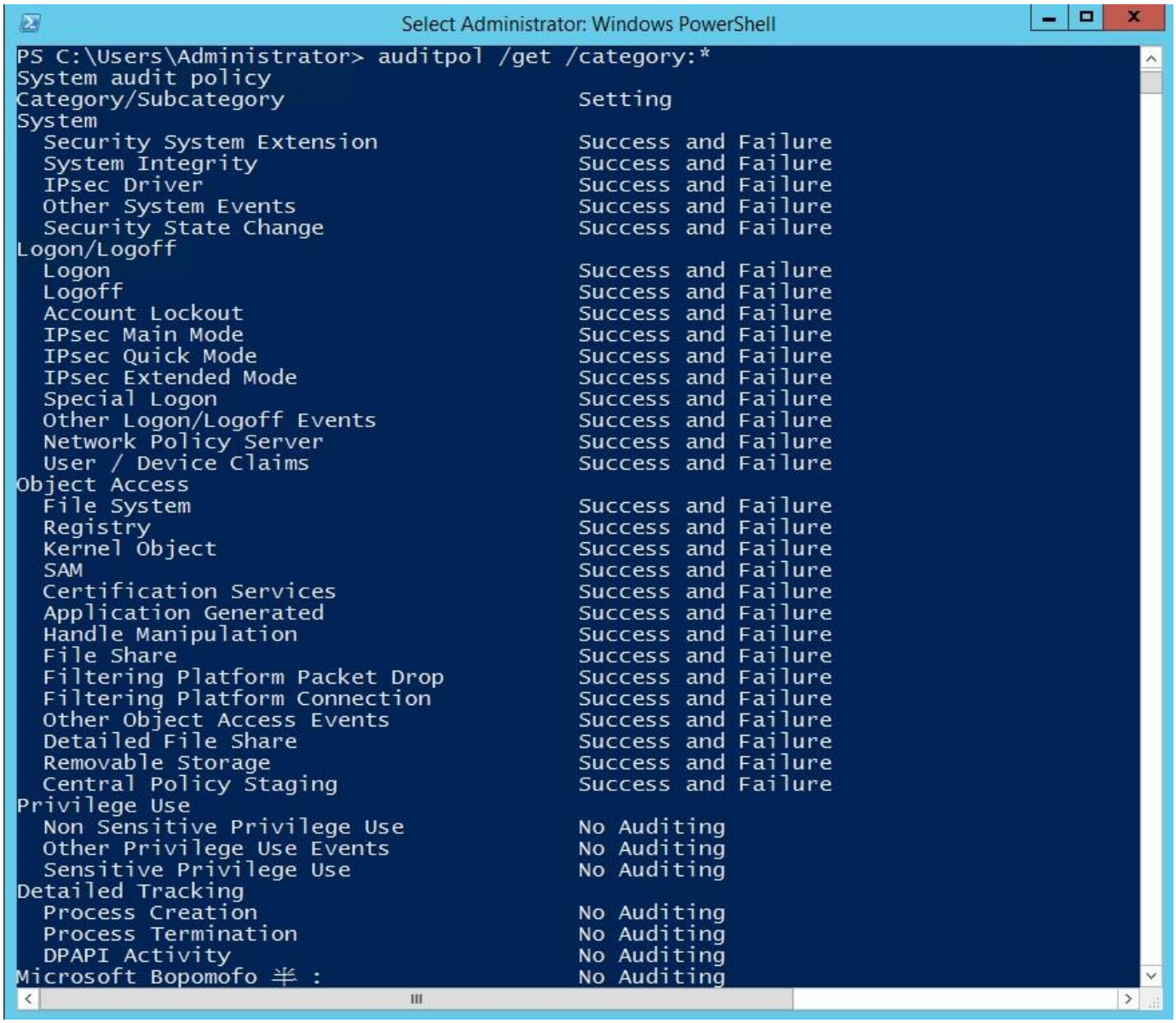
(4) Open “Windows PowerShell.”

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

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

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

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

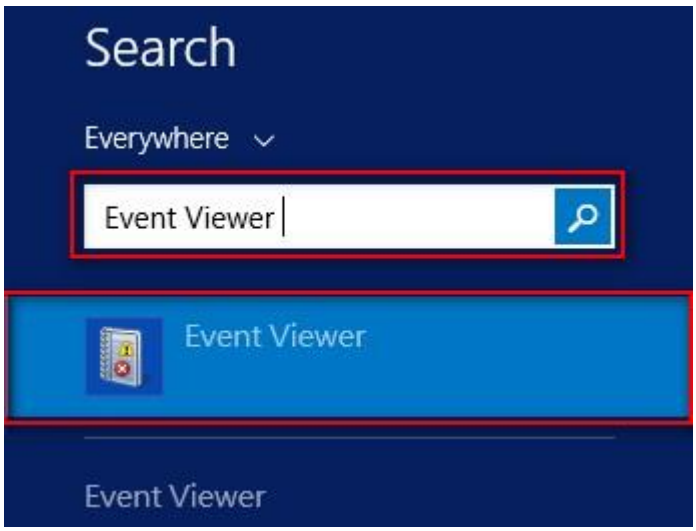


5.2.2 Event Log Settings

(1) Move the cursor to the bottom right corner and click on “Search.”

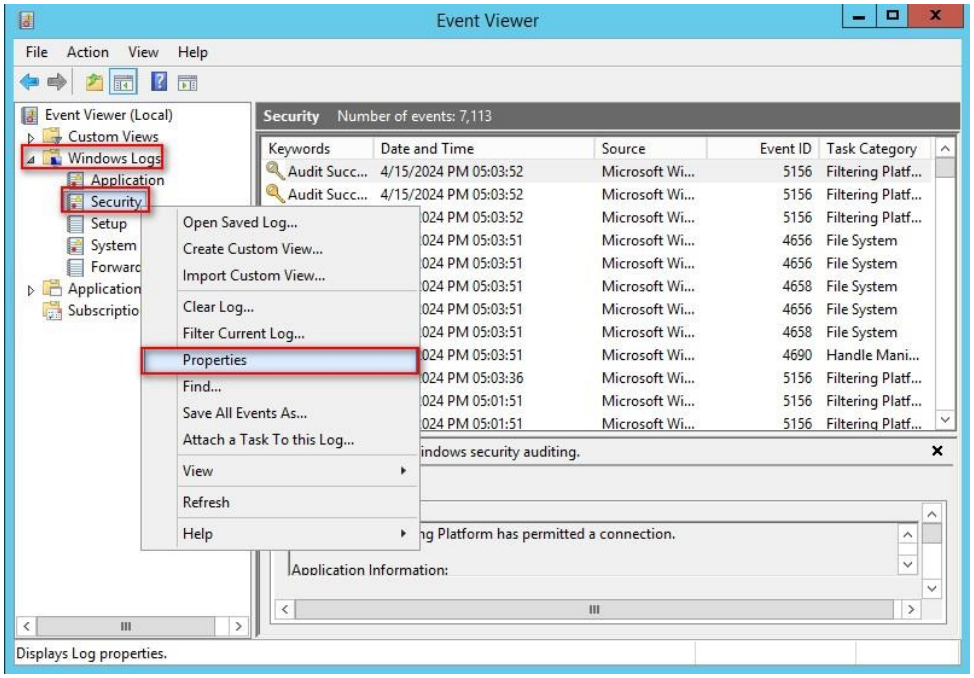
(2) Search for “Group Policy Object Editor”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy.



(3) Edit Security Log

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

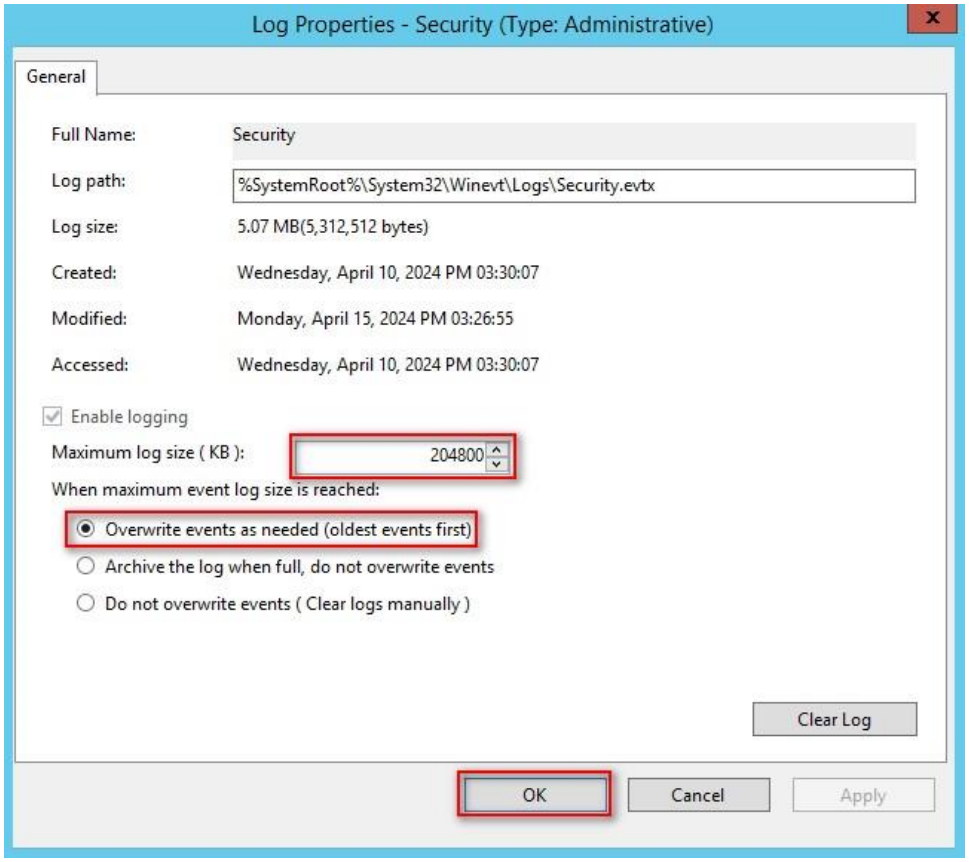


(4) Configure Security Log

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.”



6. For Windows 2016

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendationlink provided in prefacefor detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

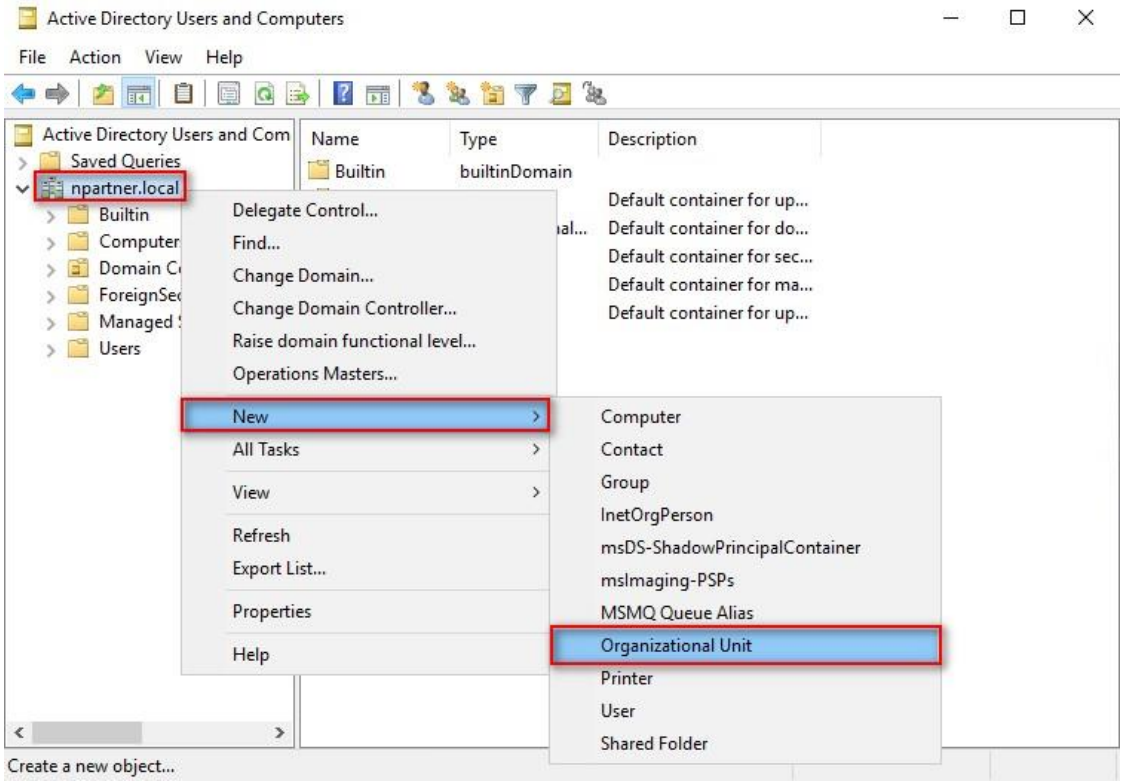
6.1 Domain

6.1.1 Organizational Unit Setup

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

(2) Add Your Organizational Unit

Right-click on your “Domain Name,” (in this example, it is “npartner.local), select “New” and click “Organizational Unit.”

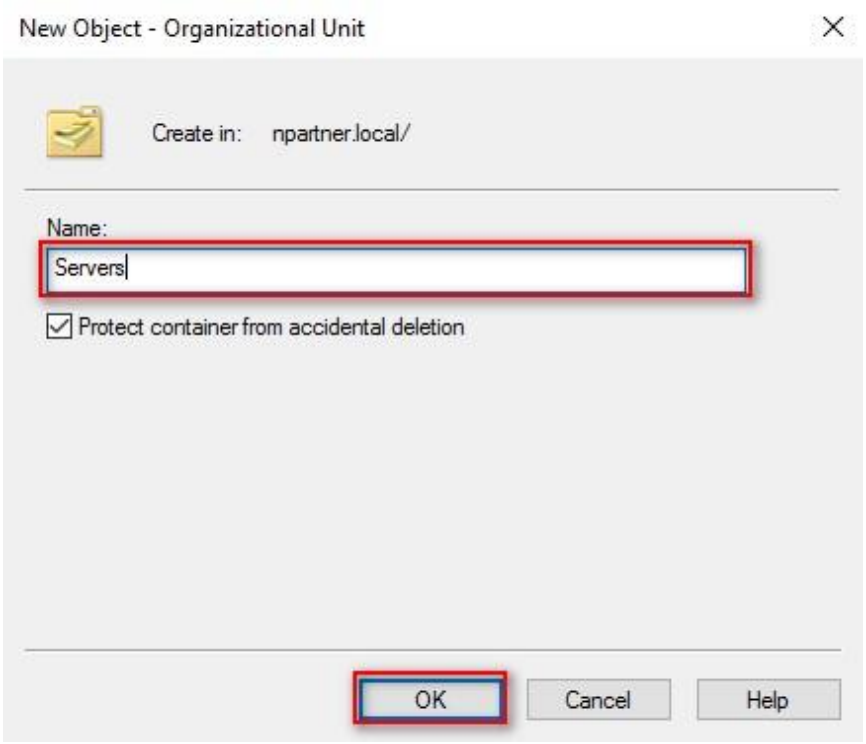


(3) Name Your Organizational Unit

Enter your “Organizational Unit Name,” (in this example, it is “Servers”)

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

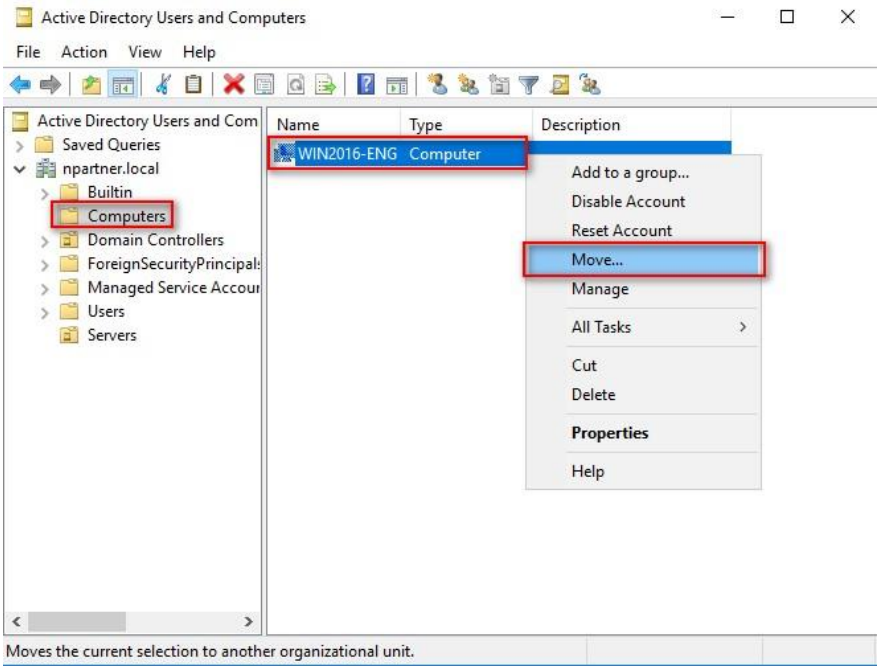
-> and click “OK.”



(4) Move Your Server to New Organizational Unit

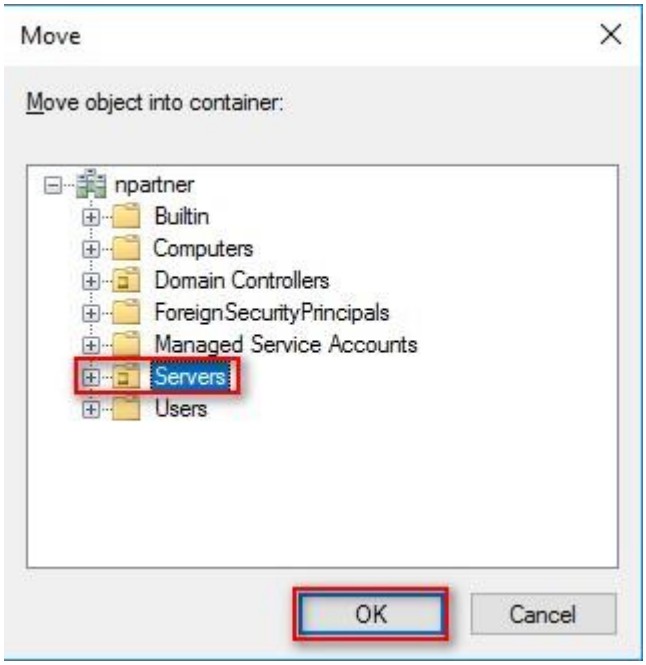
Select your organizational unit (the example here is “Computers”) -> Right-click on the “WIN2016-ENG” server.

Note: Please select the Windows Server host based on actual environment. -> Click “Move.”



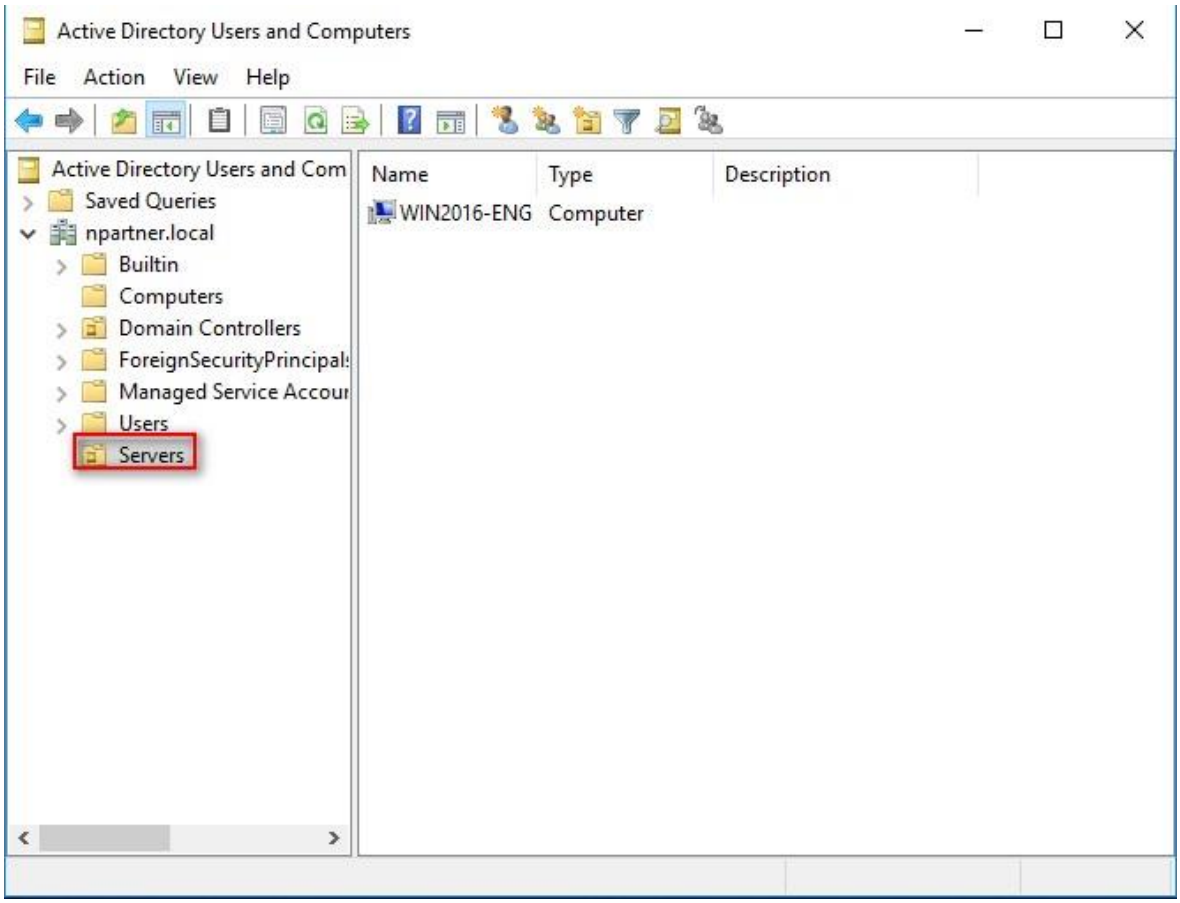
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

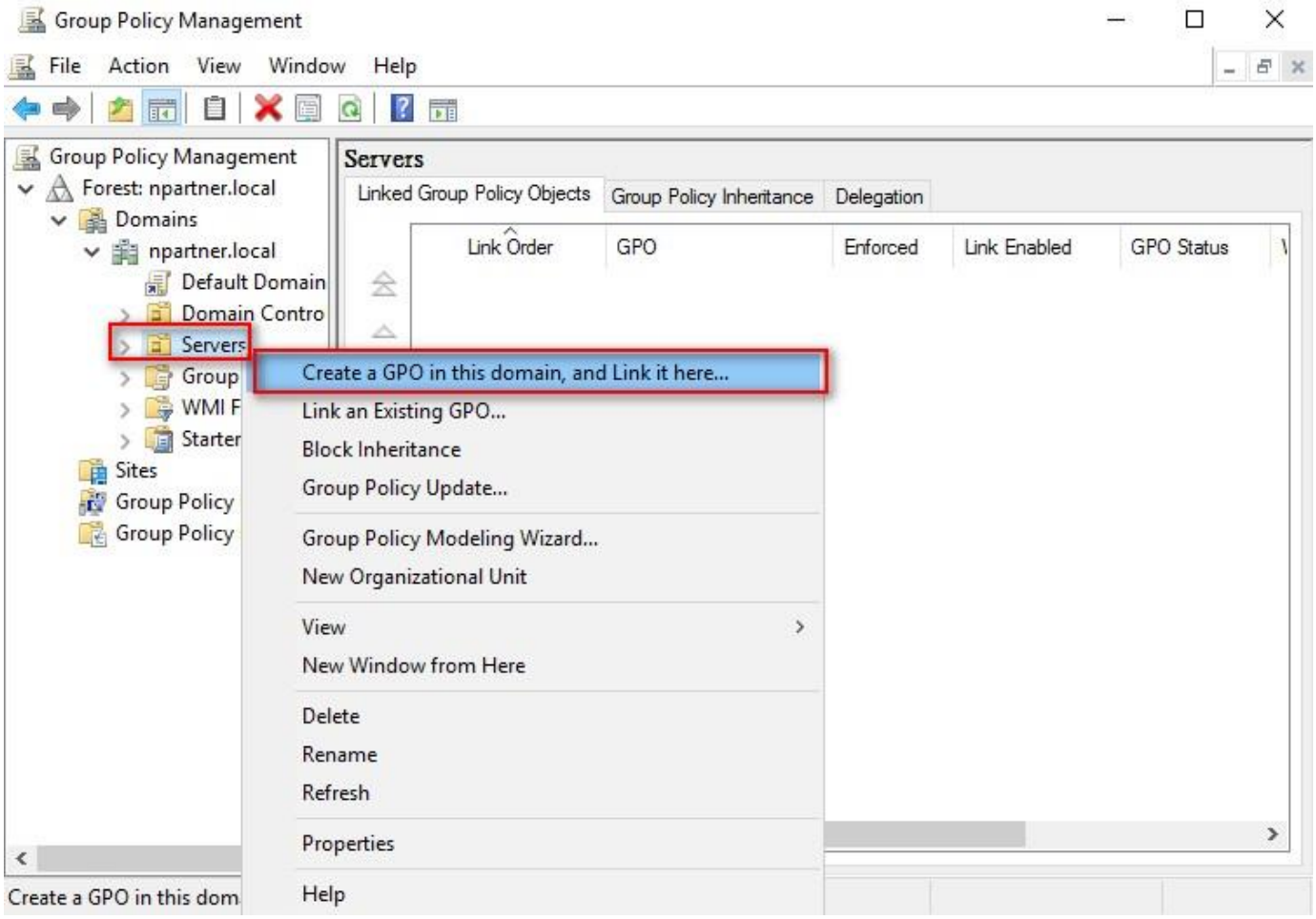
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2016-ENG” server has been moved.



6.1.2 Group Policy Settings

(1) Open “Group Policy Management.”

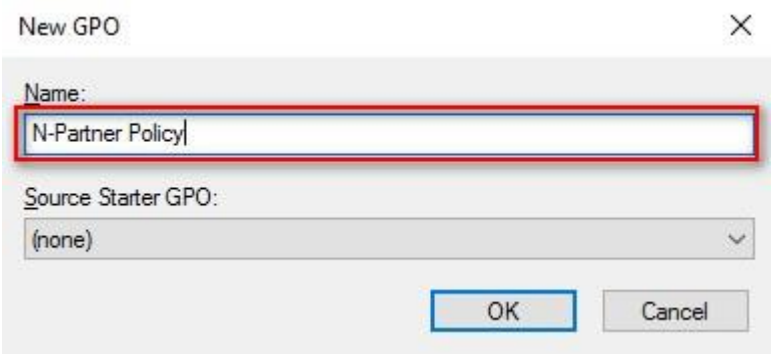
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

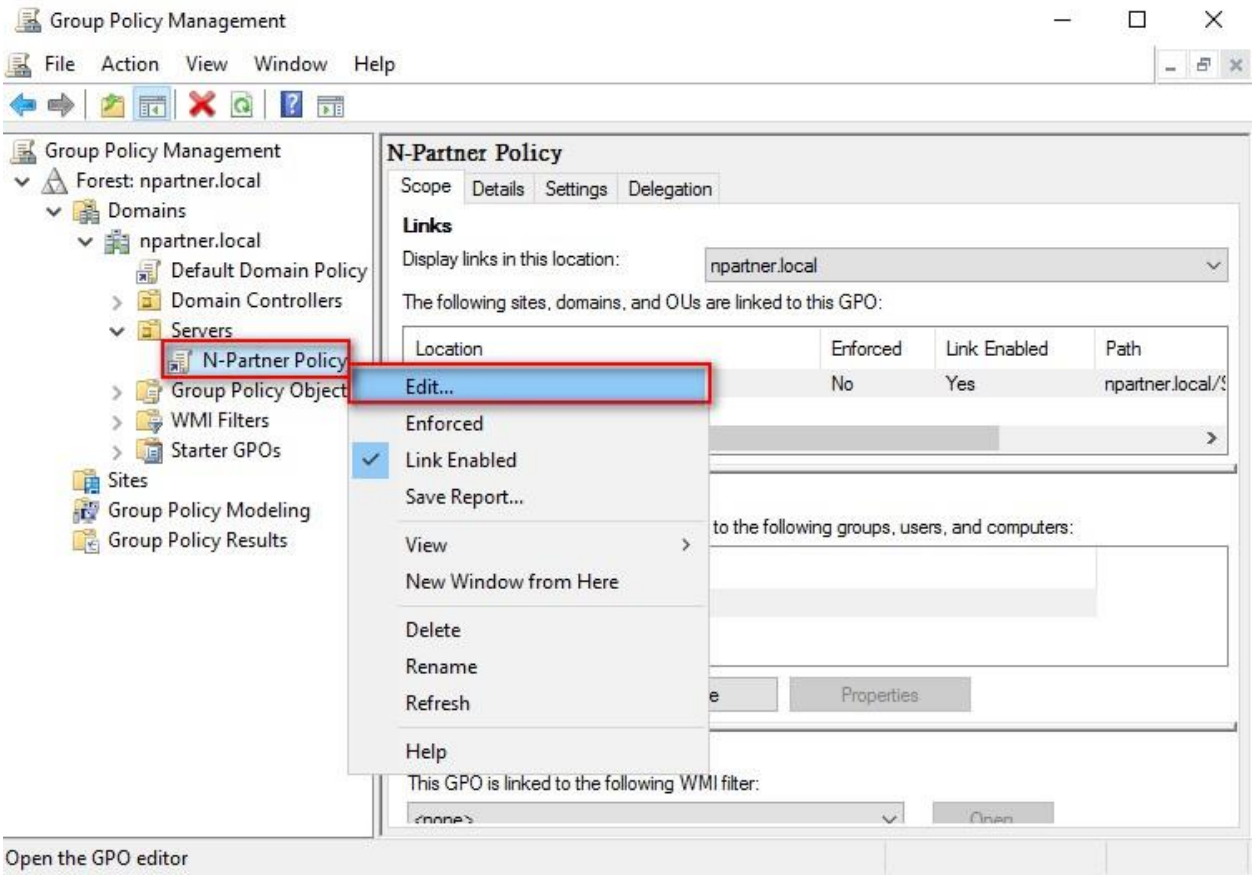
Enter your group policy object name (the example here is “N-Partner Policy”).

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



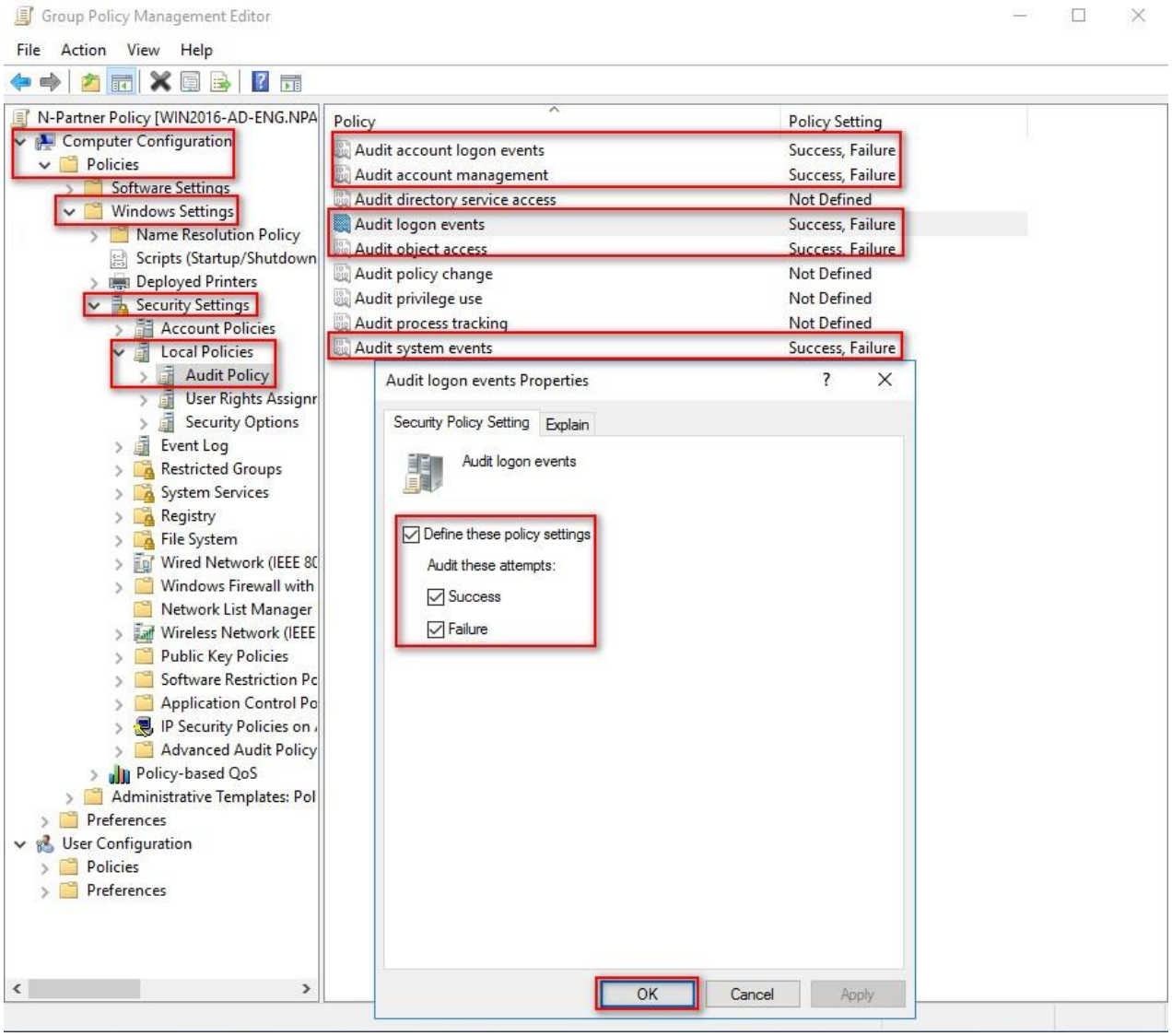
(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is “N-Partner Policy”) and click “Edit.”



(5) Local Group Policies: Audit Policy

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

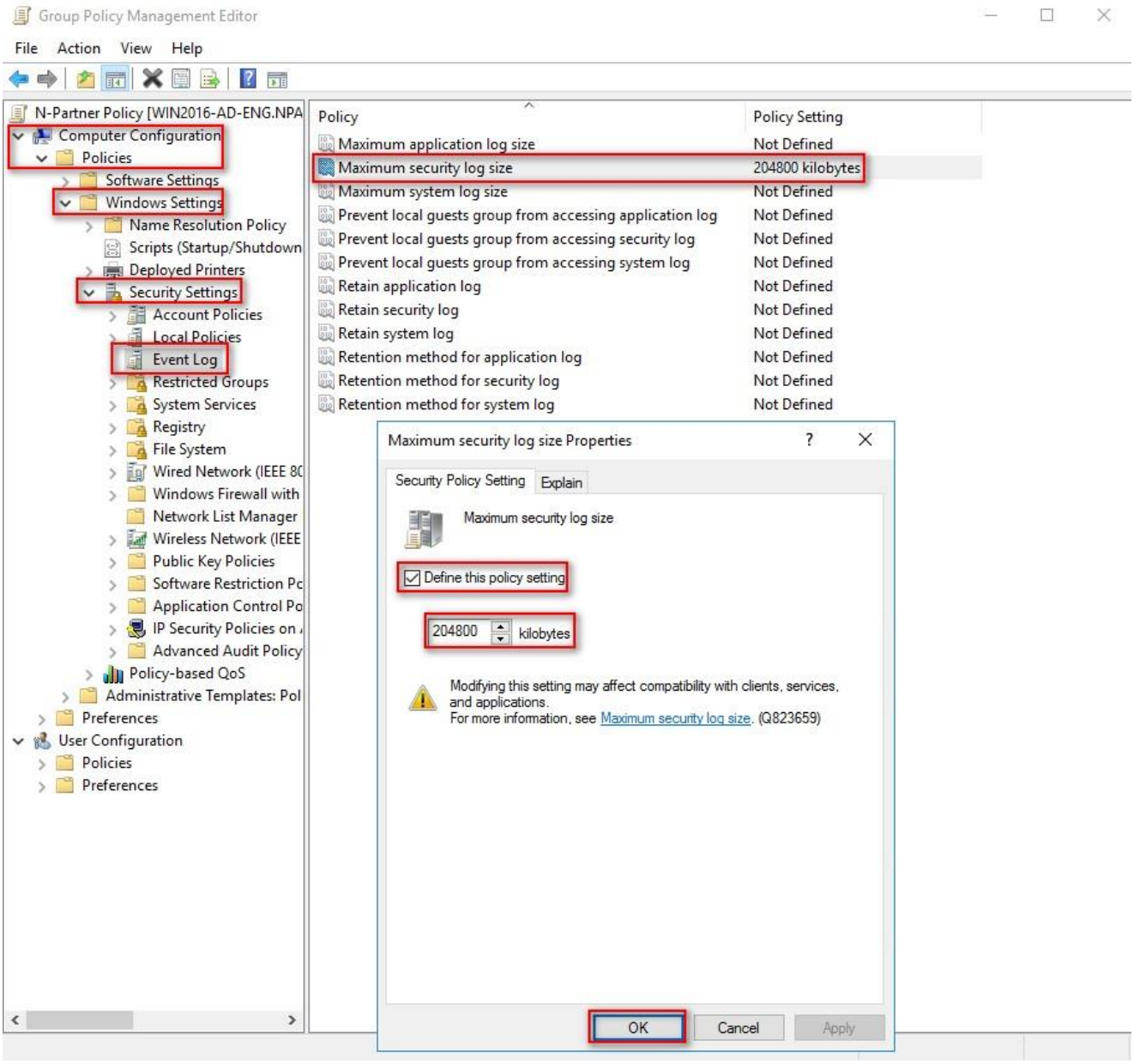


(6) Event Logs: Maximum Size of Security Log

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

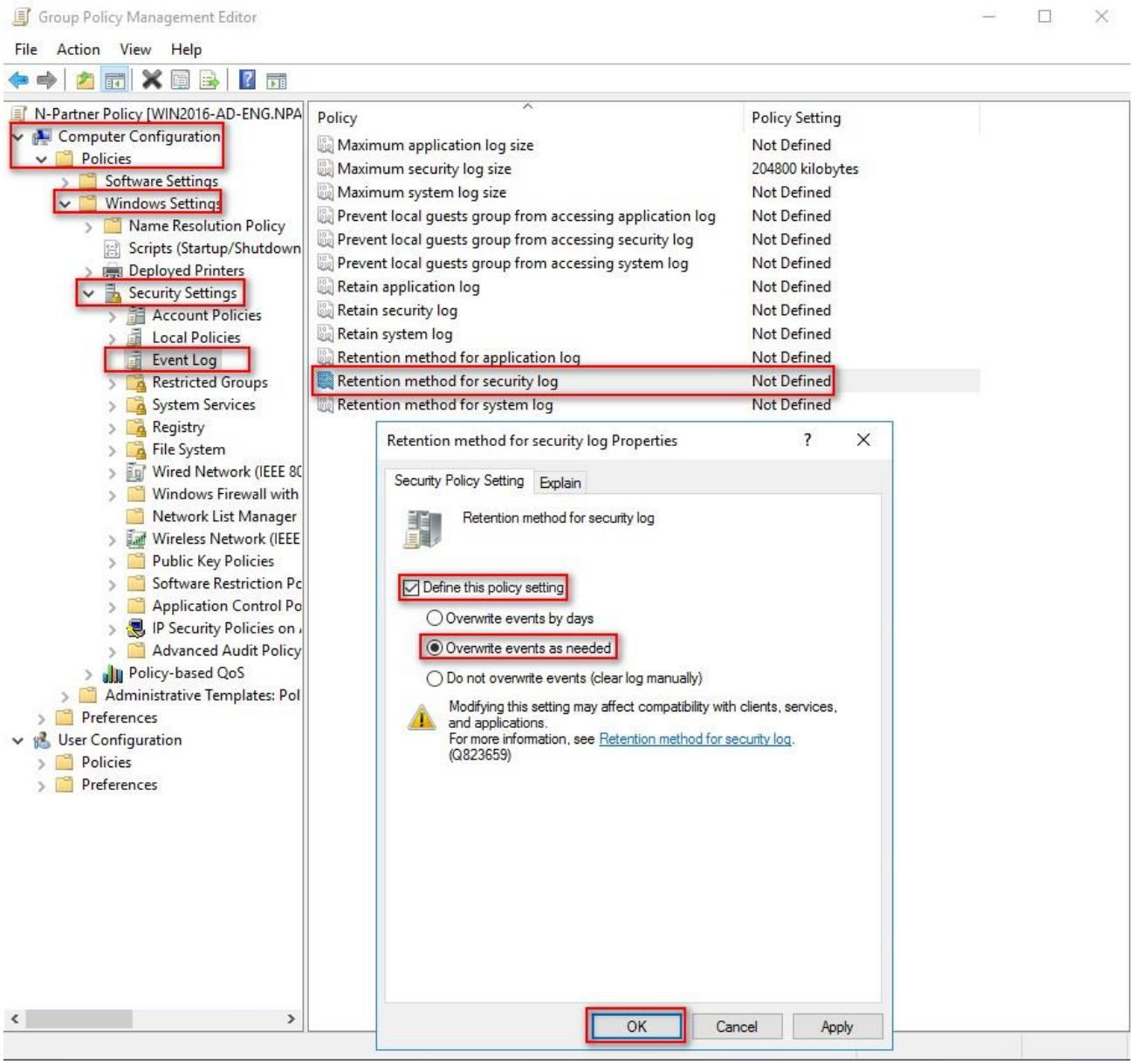
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

Note: Please adjust the number based on the actual environment. -> Click [OK].

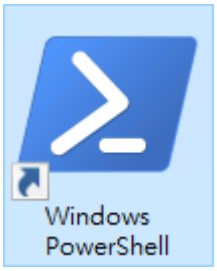


(7) Event Logs: Retention Method for Security Log

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

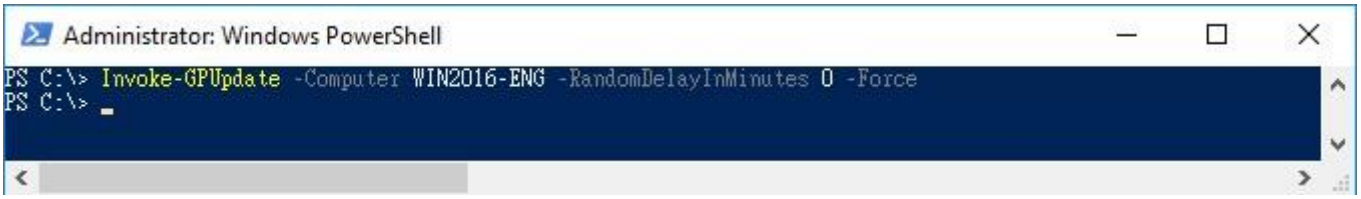


(8) Open “Windows PowerShell” on your Windows server.



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

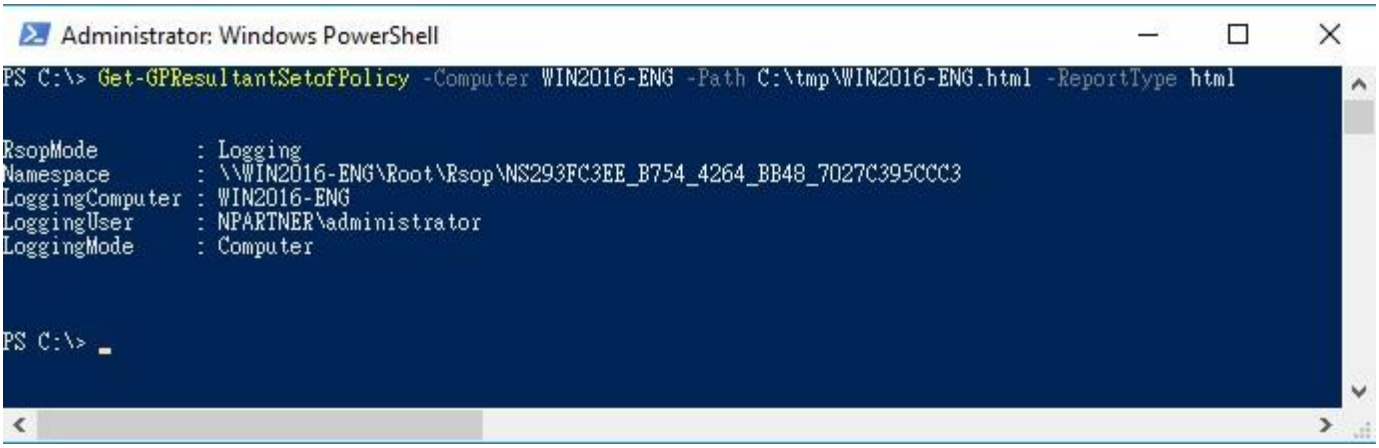
```
PS C:\> Invoke-GPUpdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
```



Please enter your Windows server hostname in red text.

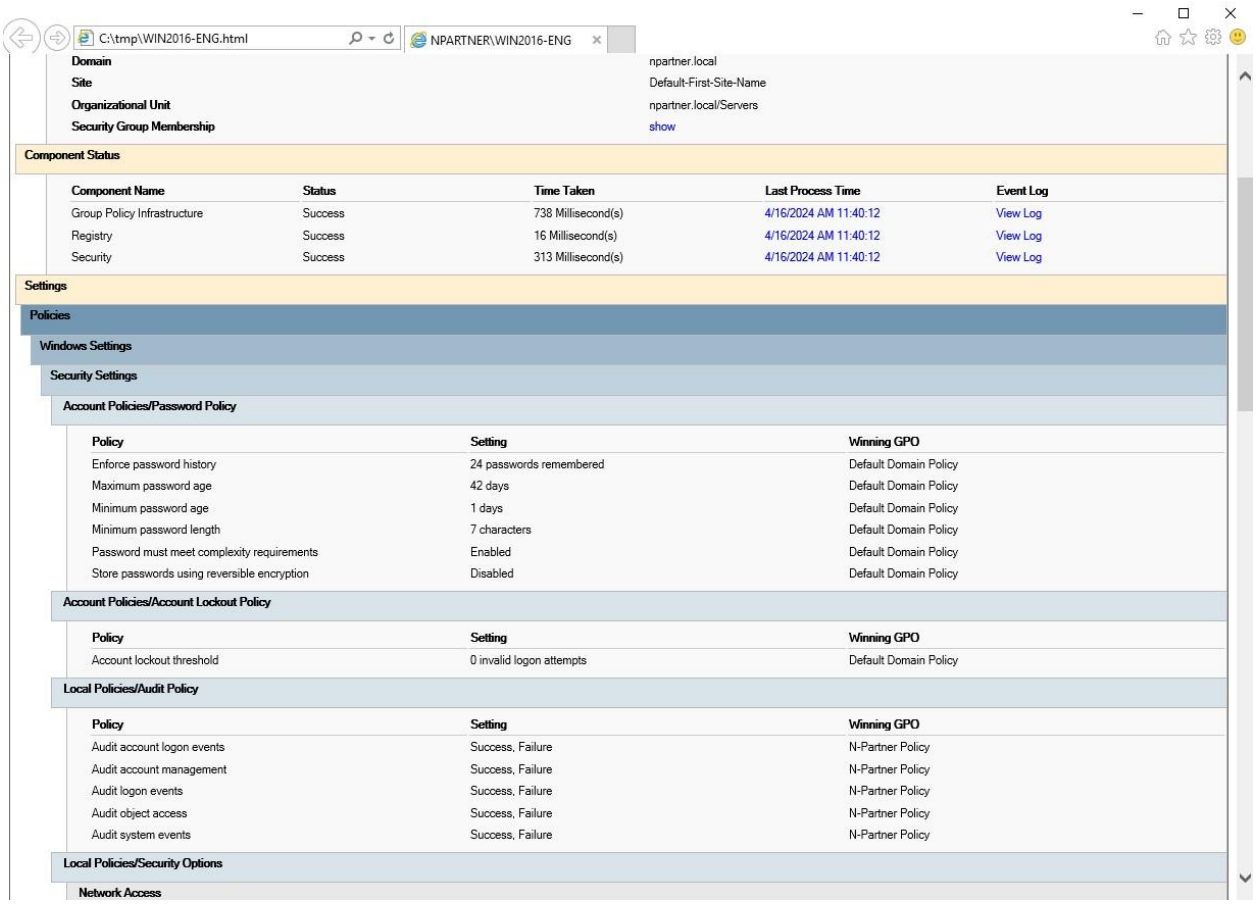
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

```
PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-ENG -Path C:\tmp\WIN2016-ENG.html -ReportType html
```



Please enter your Windows server hostname and the folder path including the file name in red text.

(11) Open your report. -> Confirm your Windows server hostname. -> Apply the N-Partner Policy Group Policy.

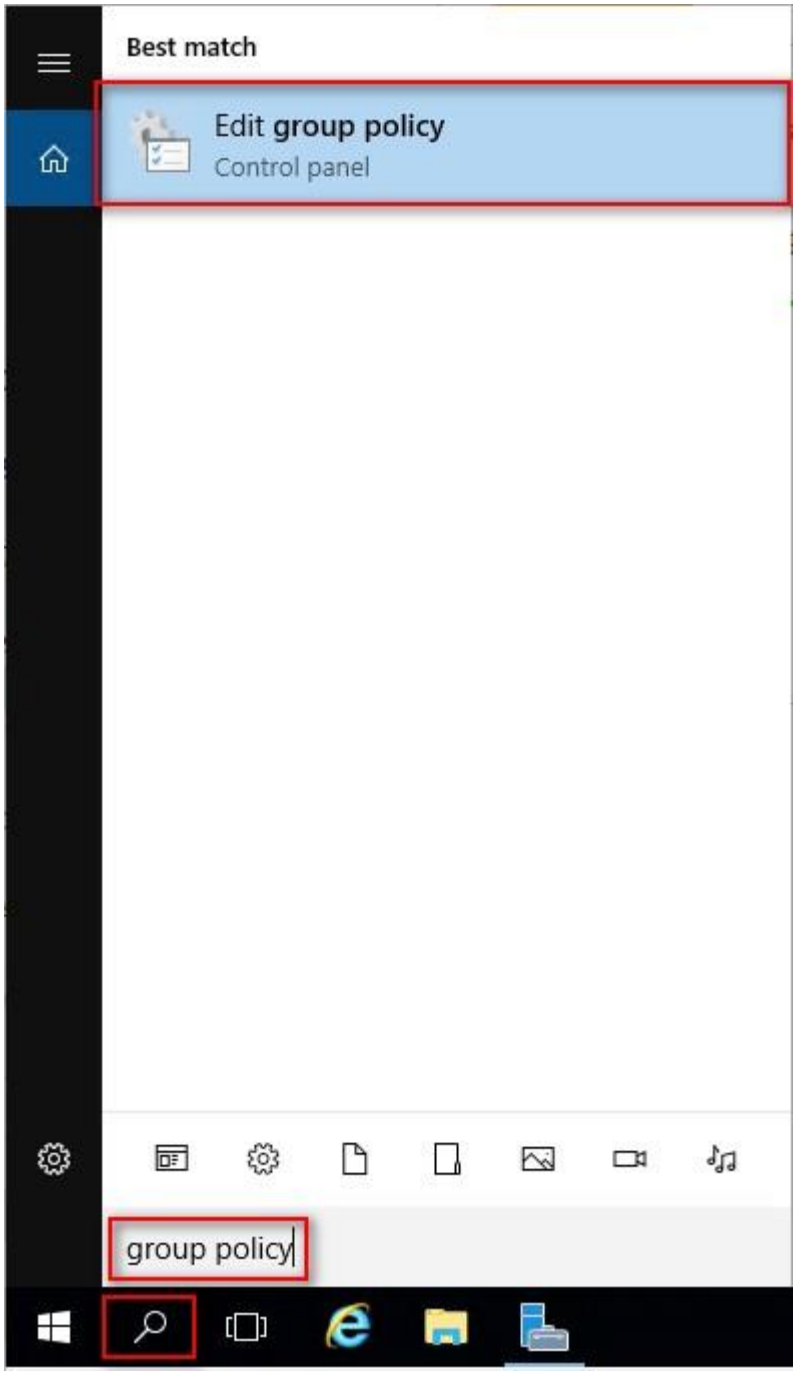


6.2 Workgroup

6.2.1 Audit Policy Settings

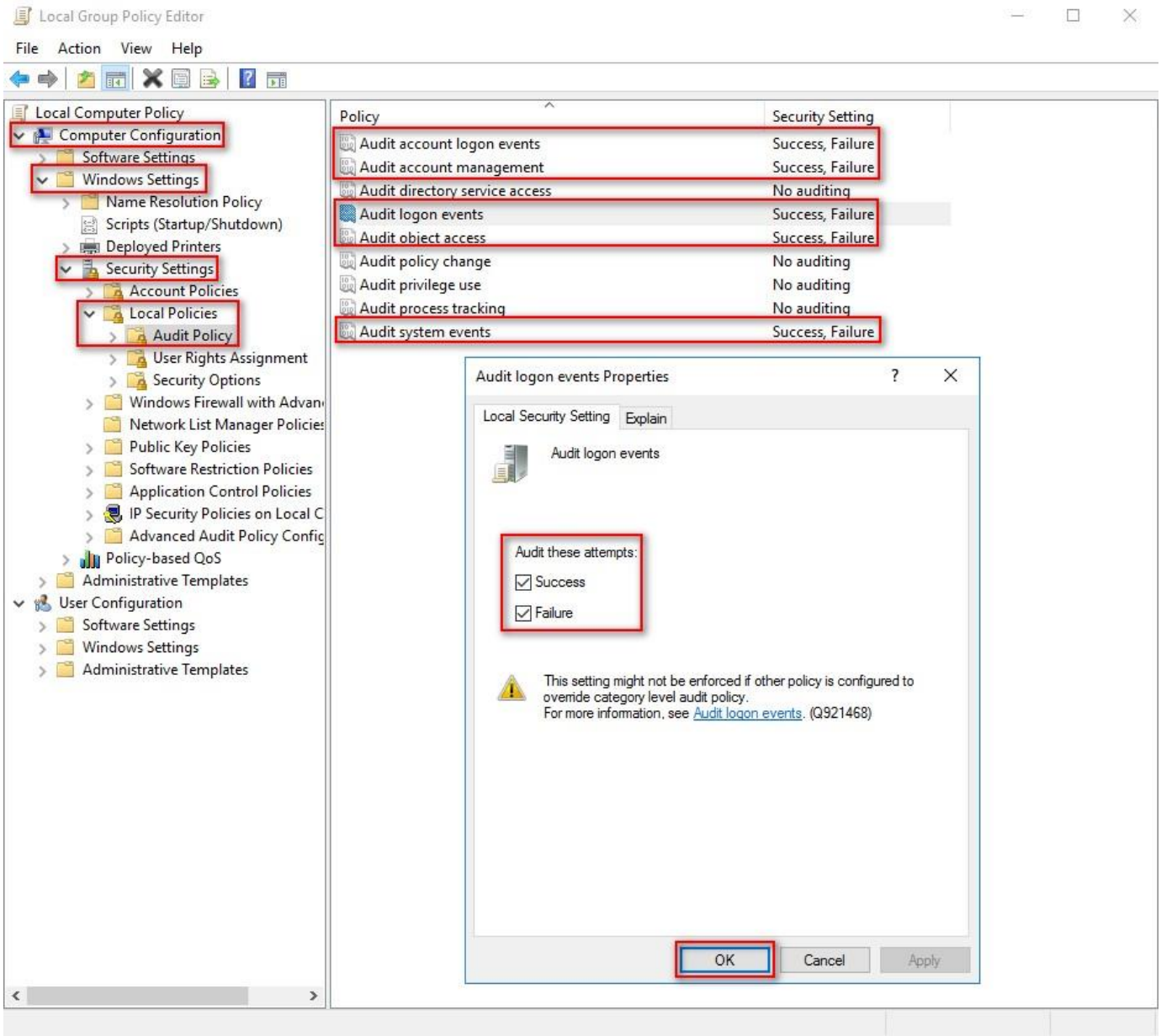
(1) Search for “Group Policy Object Editor.”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy” in the search results.

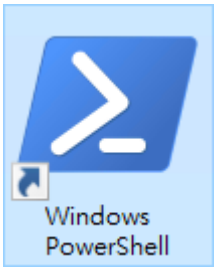


(2) Local Group Policies: Audit Policies

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: “Success” & “Failure” -> Click “OK.”



(3) Open “Windows PowerShell.”

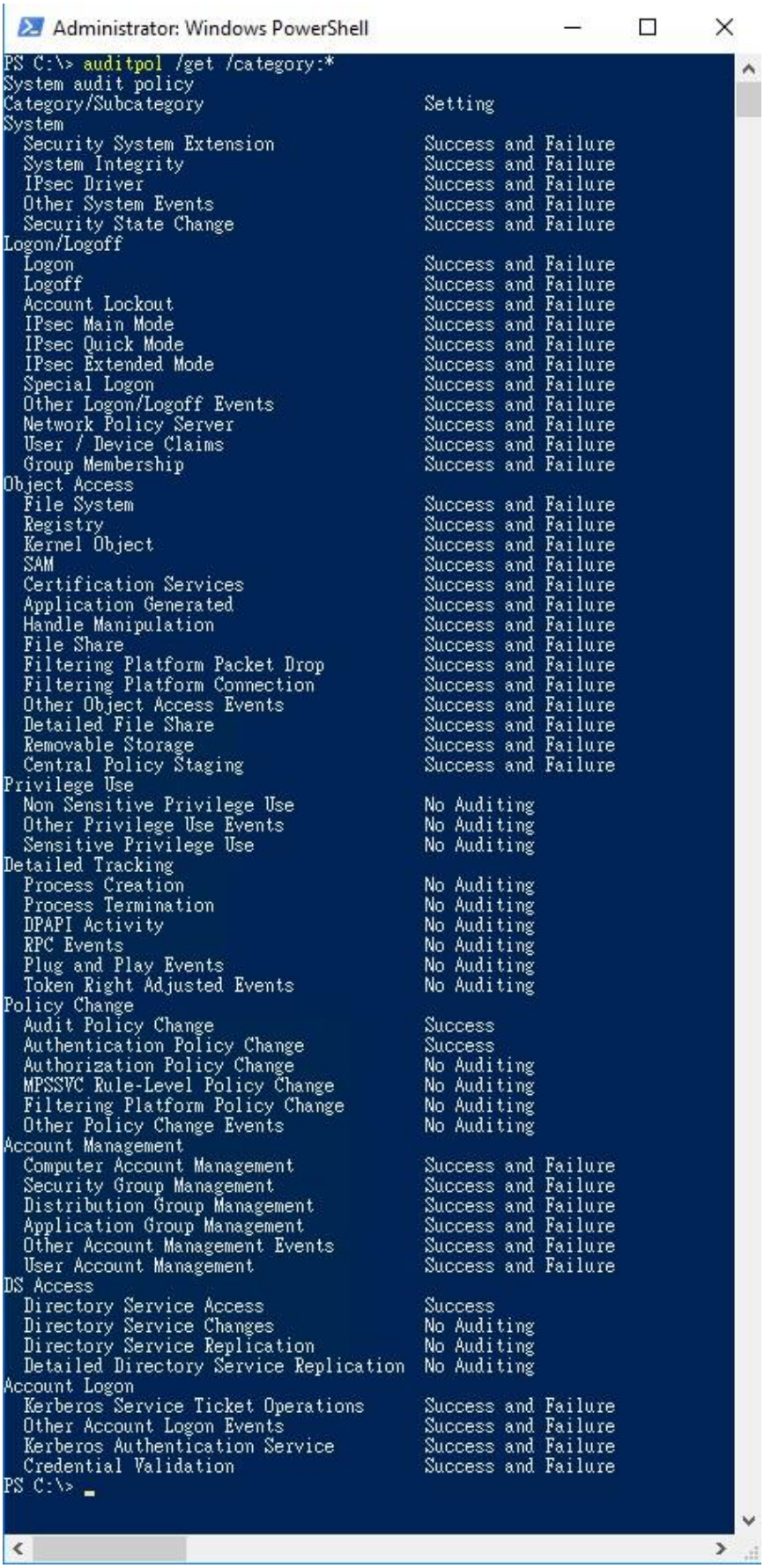


(4) Enter the command below to refresh group policy.

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

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

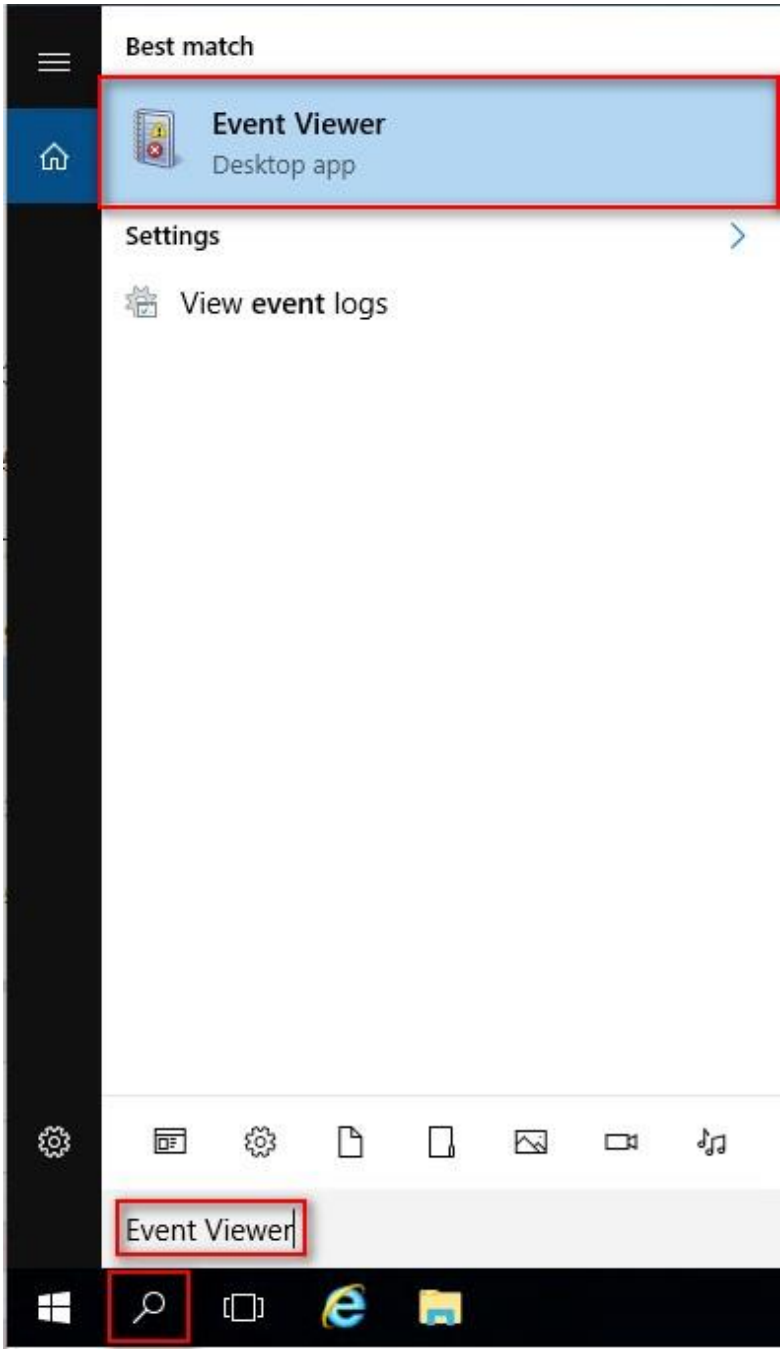
```
PS C: \> auditpol /get /category:*
```



6.2.2 Event Log Settings

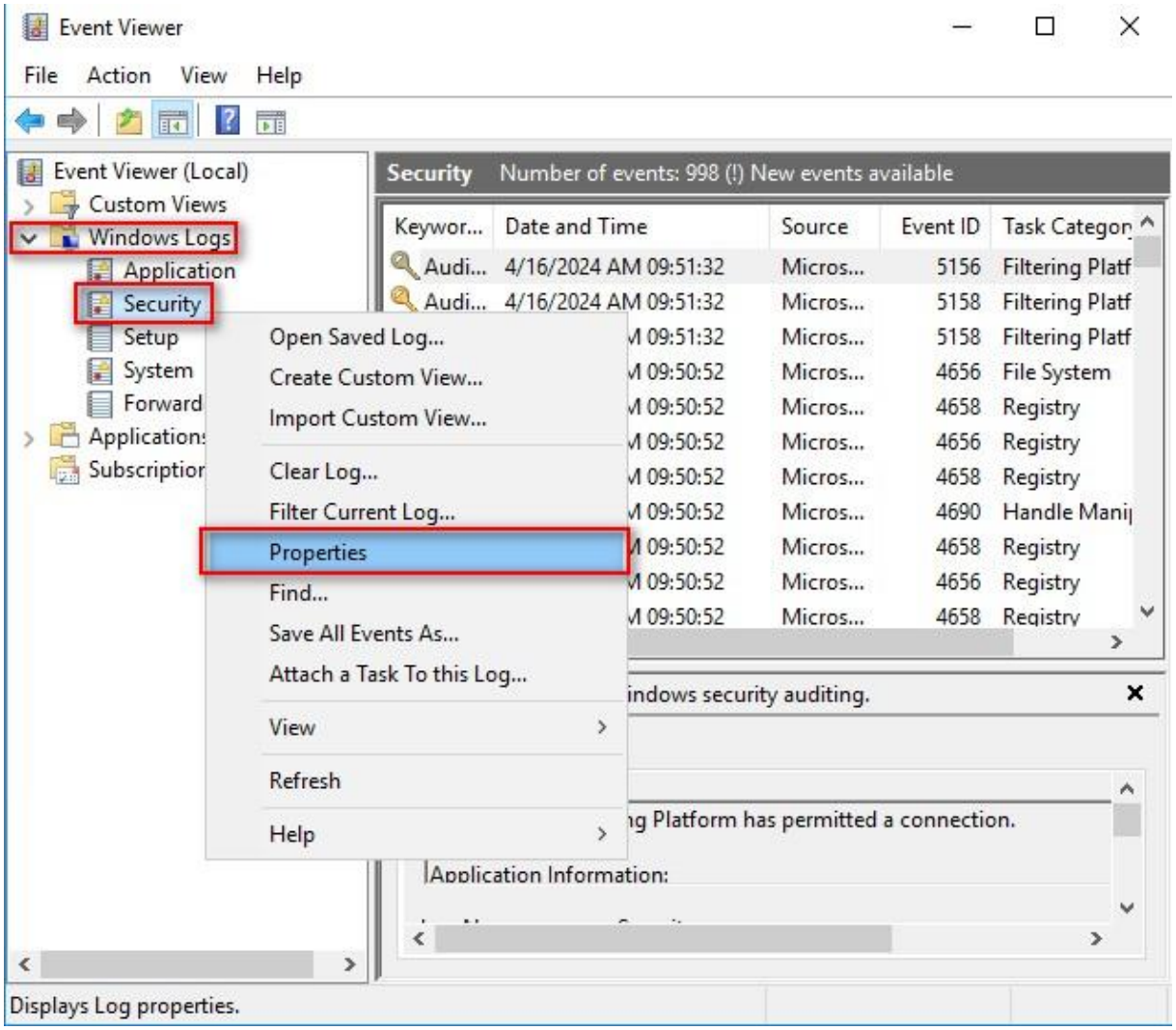
(1) Search for “Group Policy Object Editor”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy.



(2) Edit Security Log

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

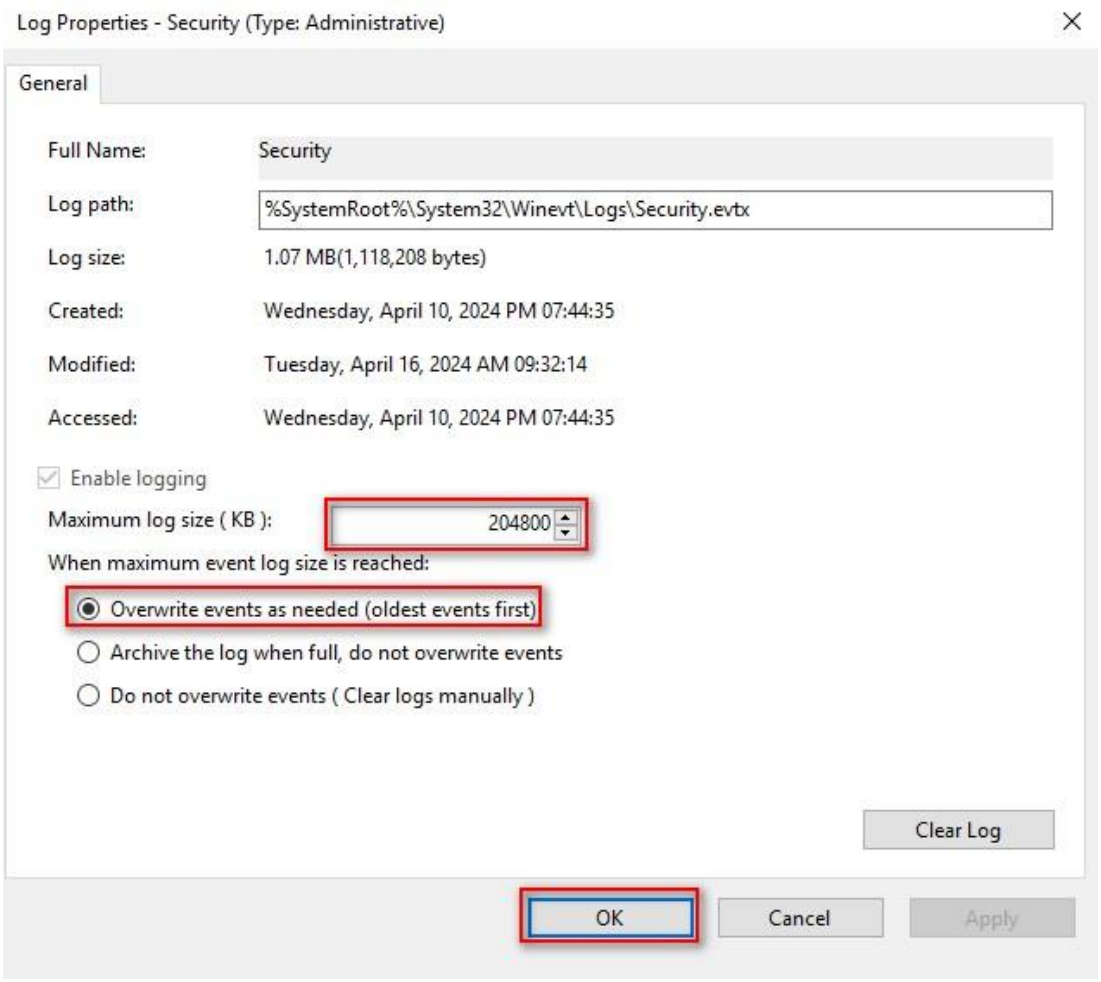


(3) Configure Security Log

Enter maximum log file size: 204800 KB

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

-> Click on “Overwrite events as needed” -> Click “OK.”



7. For Windows 2019

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendation” link provided in “preface” for detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

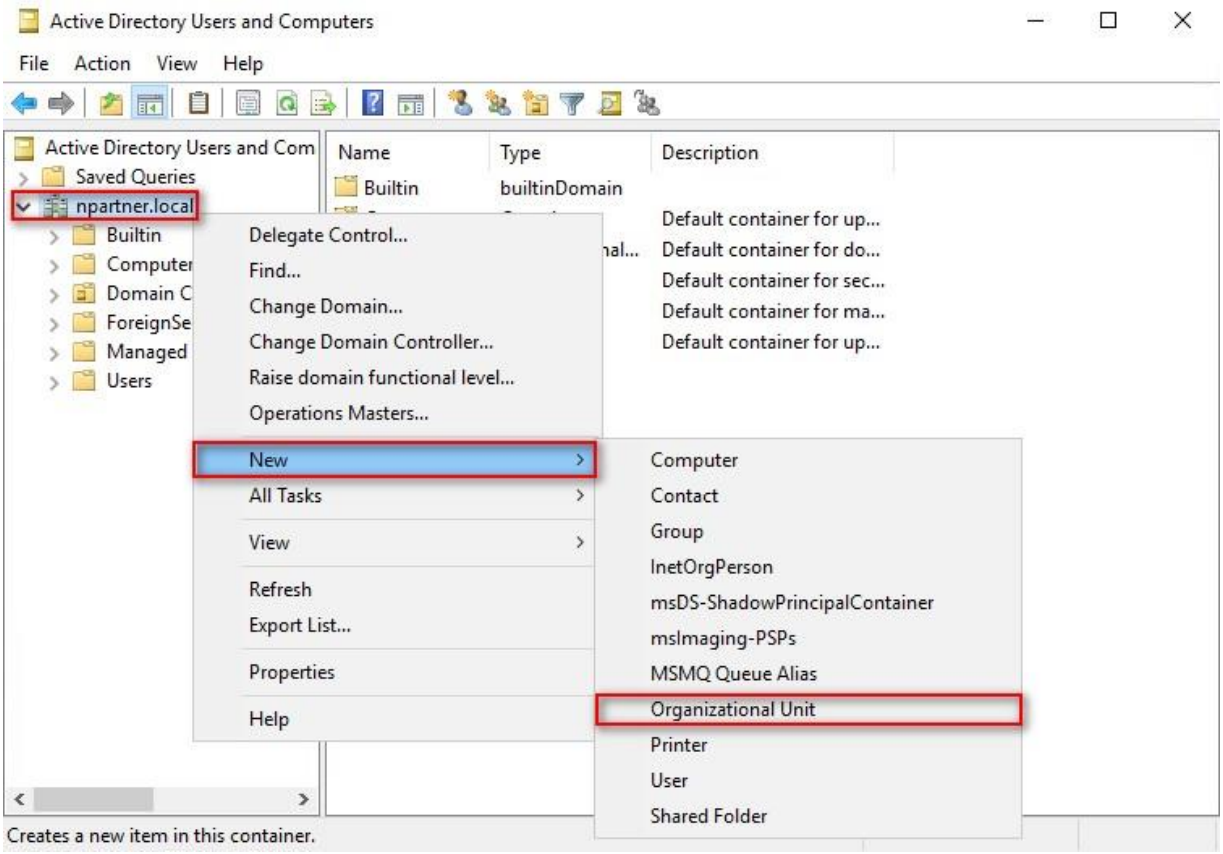
7.1 Domain

7.1.1 Organizational Unit Setup

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

(2) Add Your Organizational Unit

Right-click on your “Domain Name,” (in this example, it is “npartner.local), select “New” and click “Organizational Unit.”

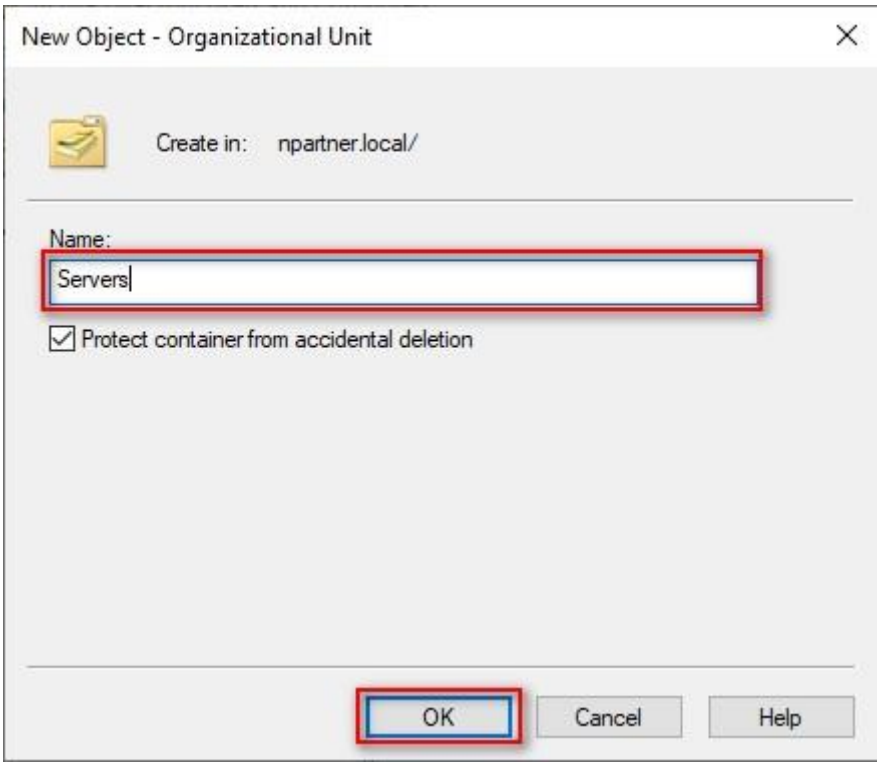


(3) Name Your Organizational Unit

Enter your “Organizational Unit Name,” (in this example, it is “Servers”)

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

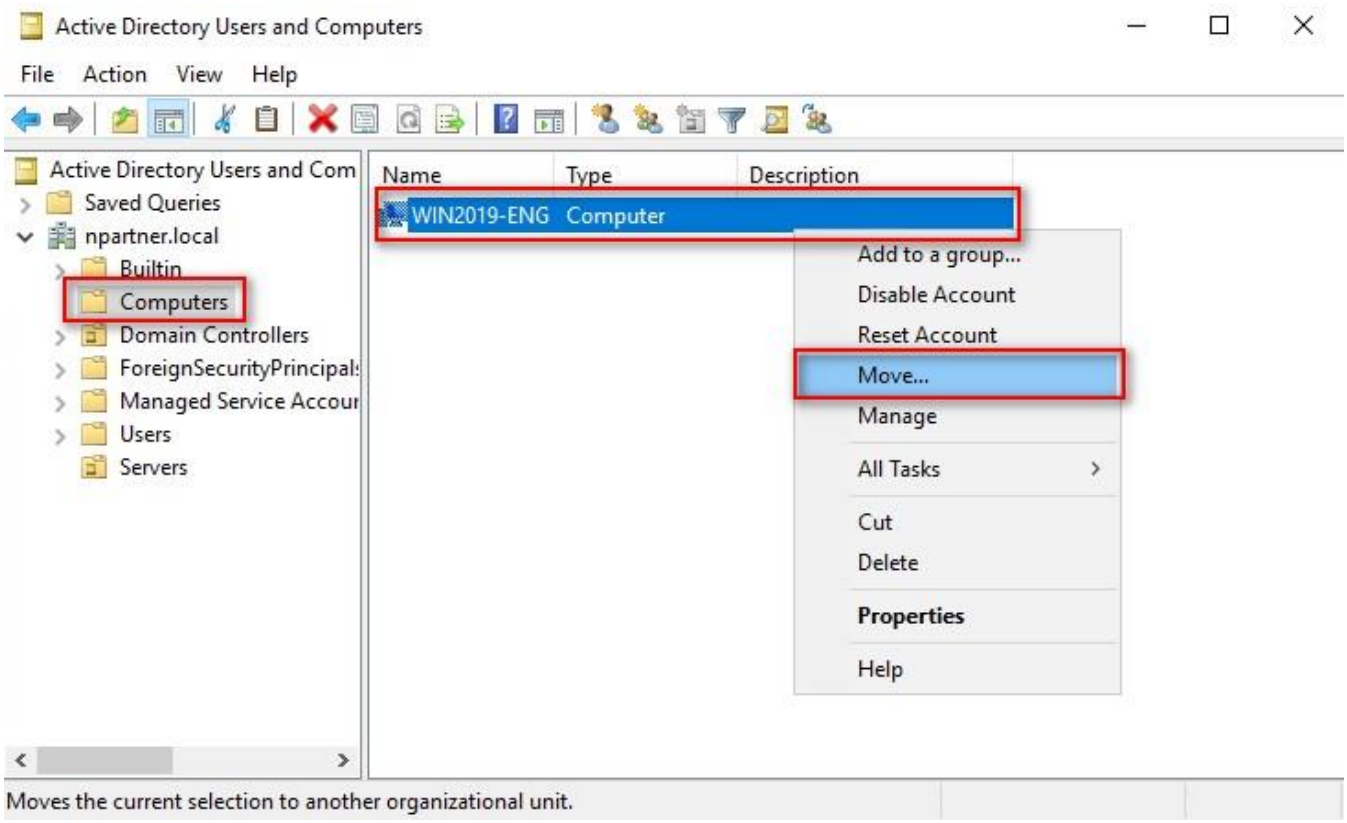
-> and click “OK.”



(4) Move Your Server to New Organizational Unit

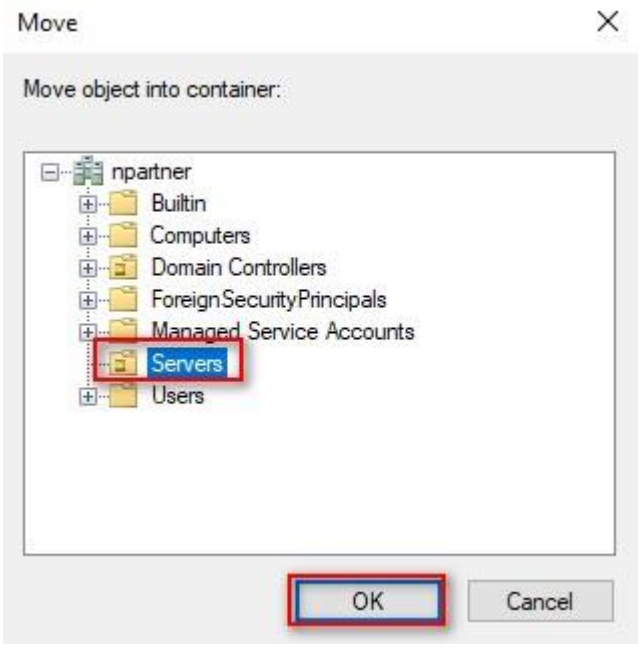
Select your organizational unit (the example here is “Computers”) -> Right-click on the “WIN2019-ENG” server.

Note: Please select the Windows Server host based on actual environment. -> Click “Move.”



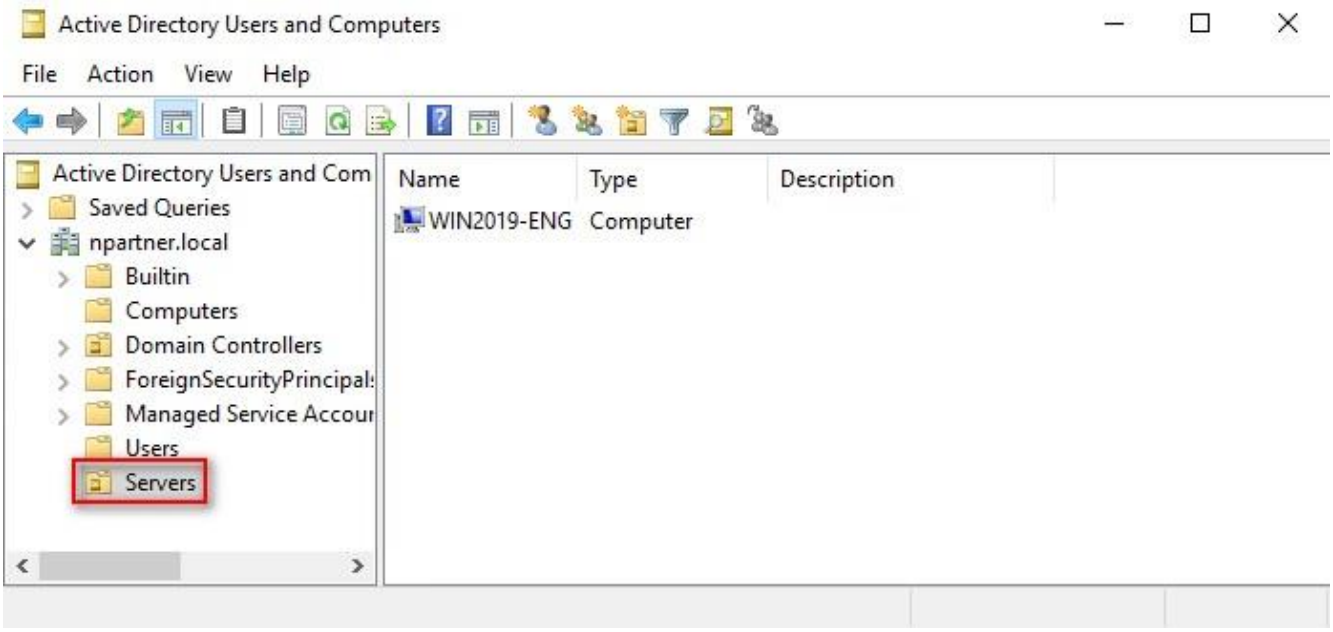
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

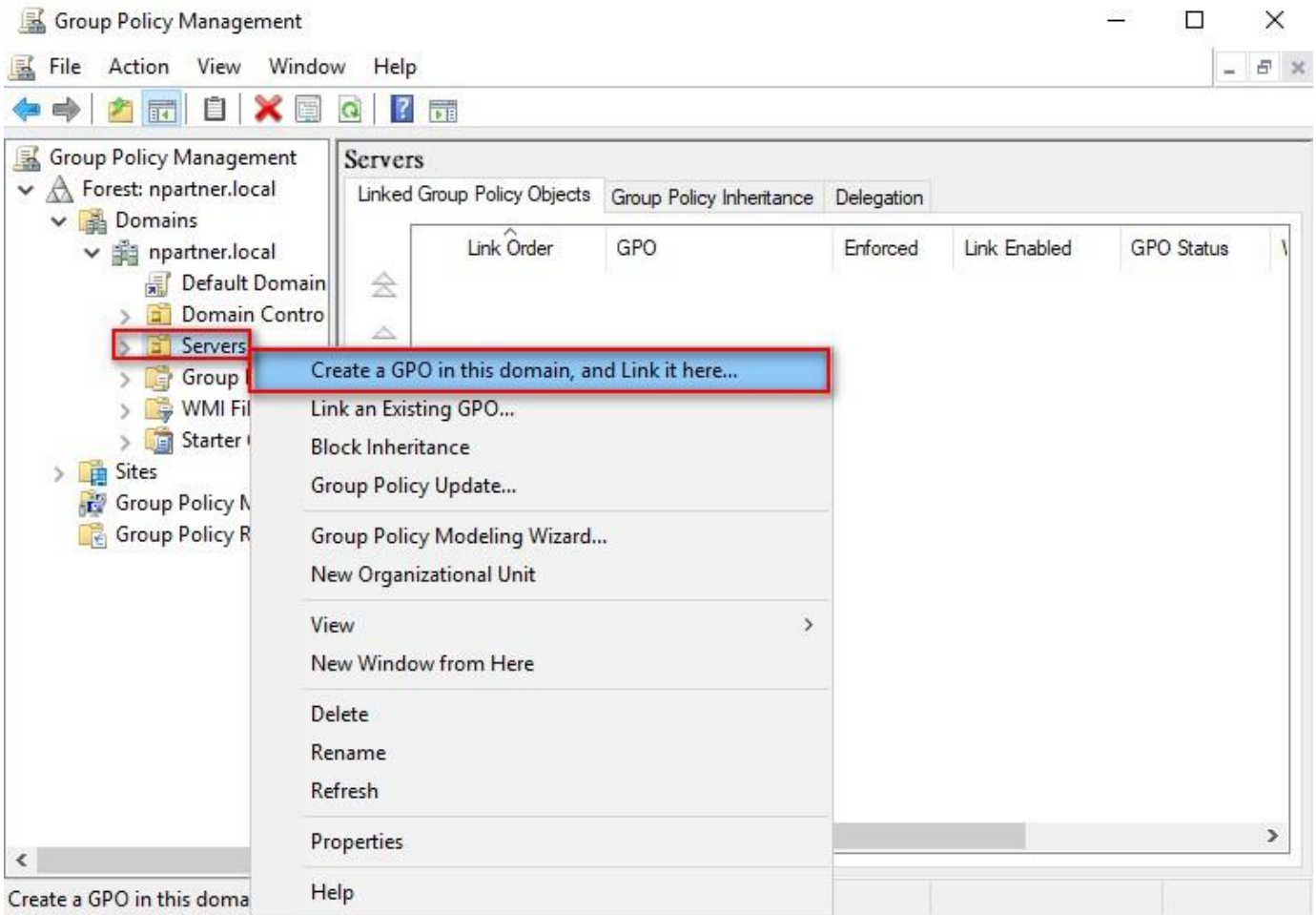
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2019-ENG” server has been moved.



7.1.2 Group Policy Settings

(1) Open “Group Policy Management.”

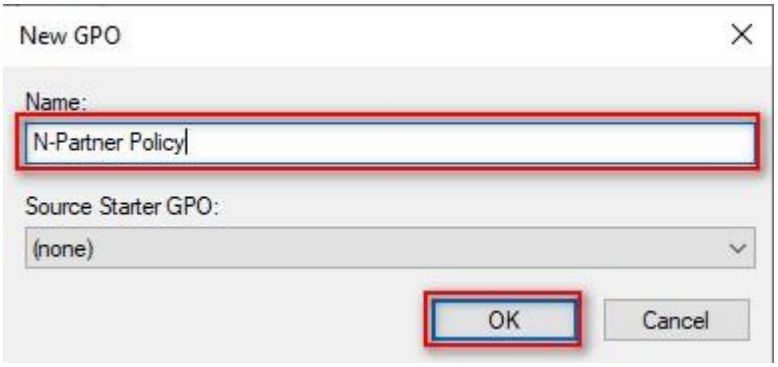
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

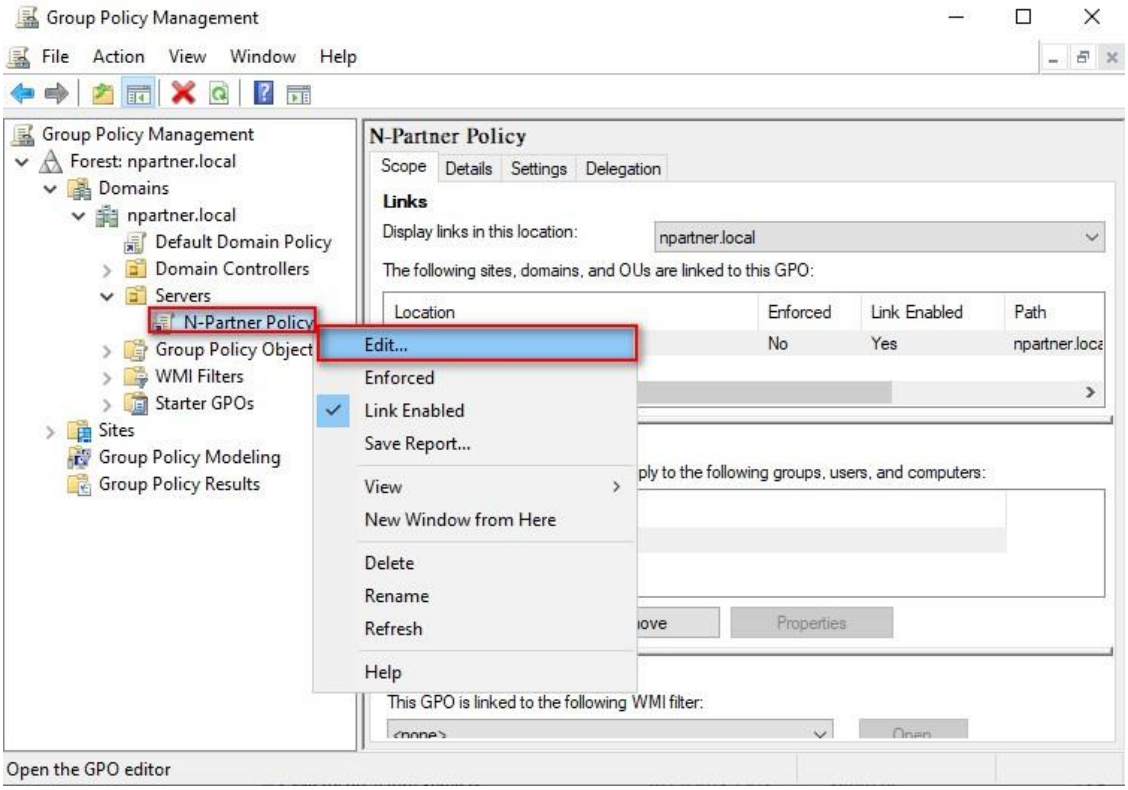
Enter your group policy object name (the example here is “N-Partner Policy”).

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



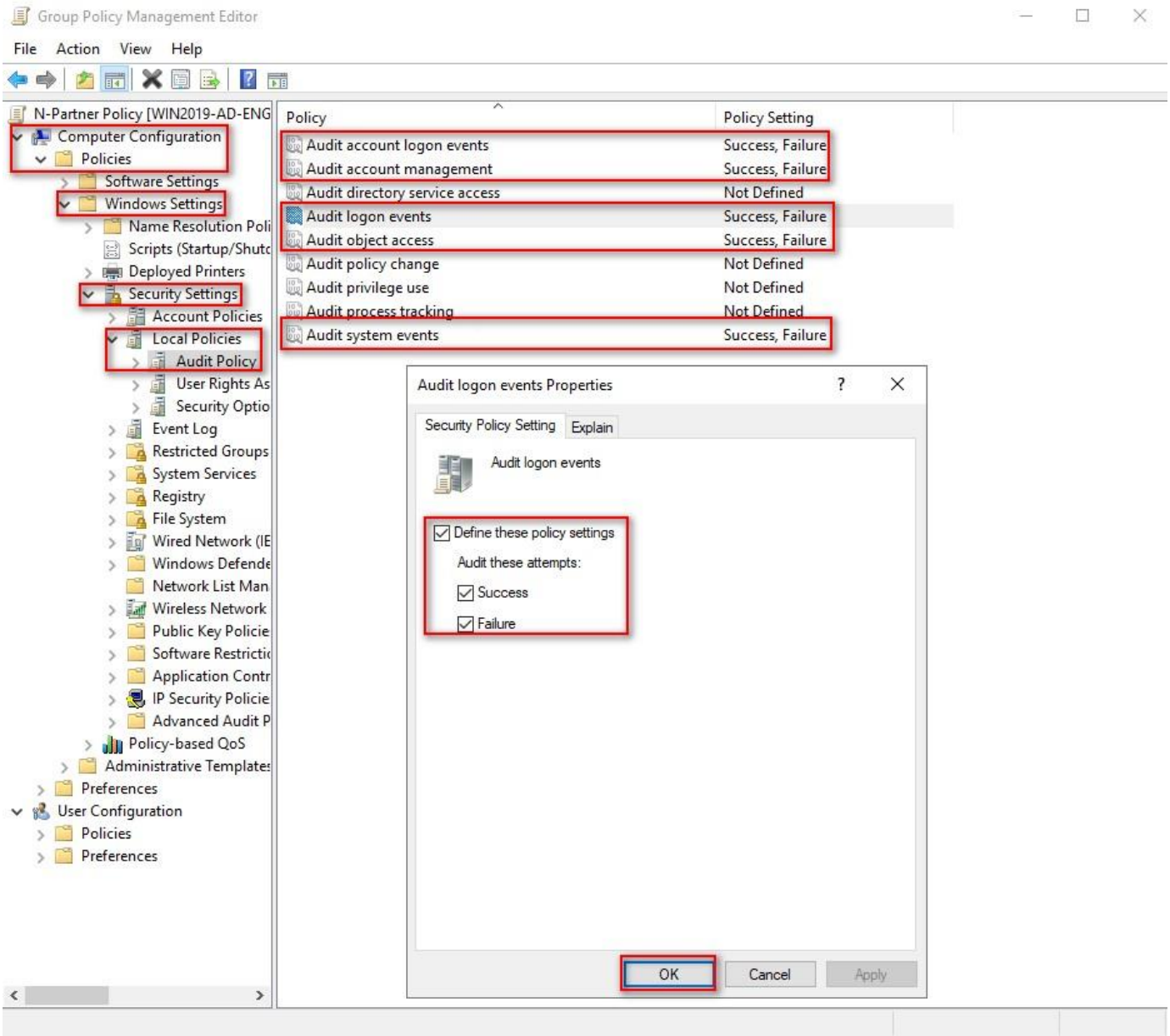
(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is “N-Partner Policy”) and click “Edit.”



(5) Local Group Policies: Audit Policy

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

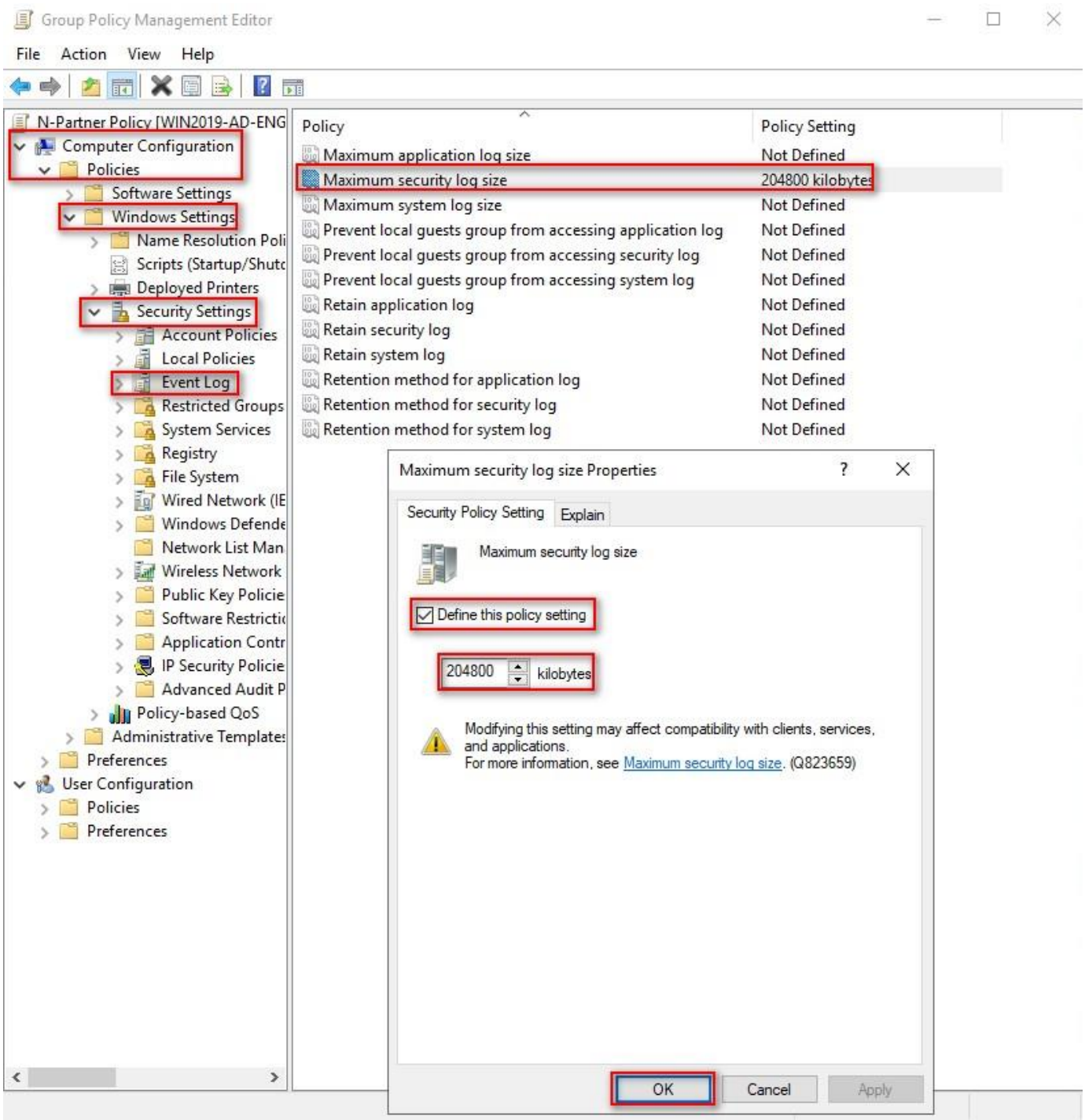


(6) Event Logs: Maximum Size of Security Log

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

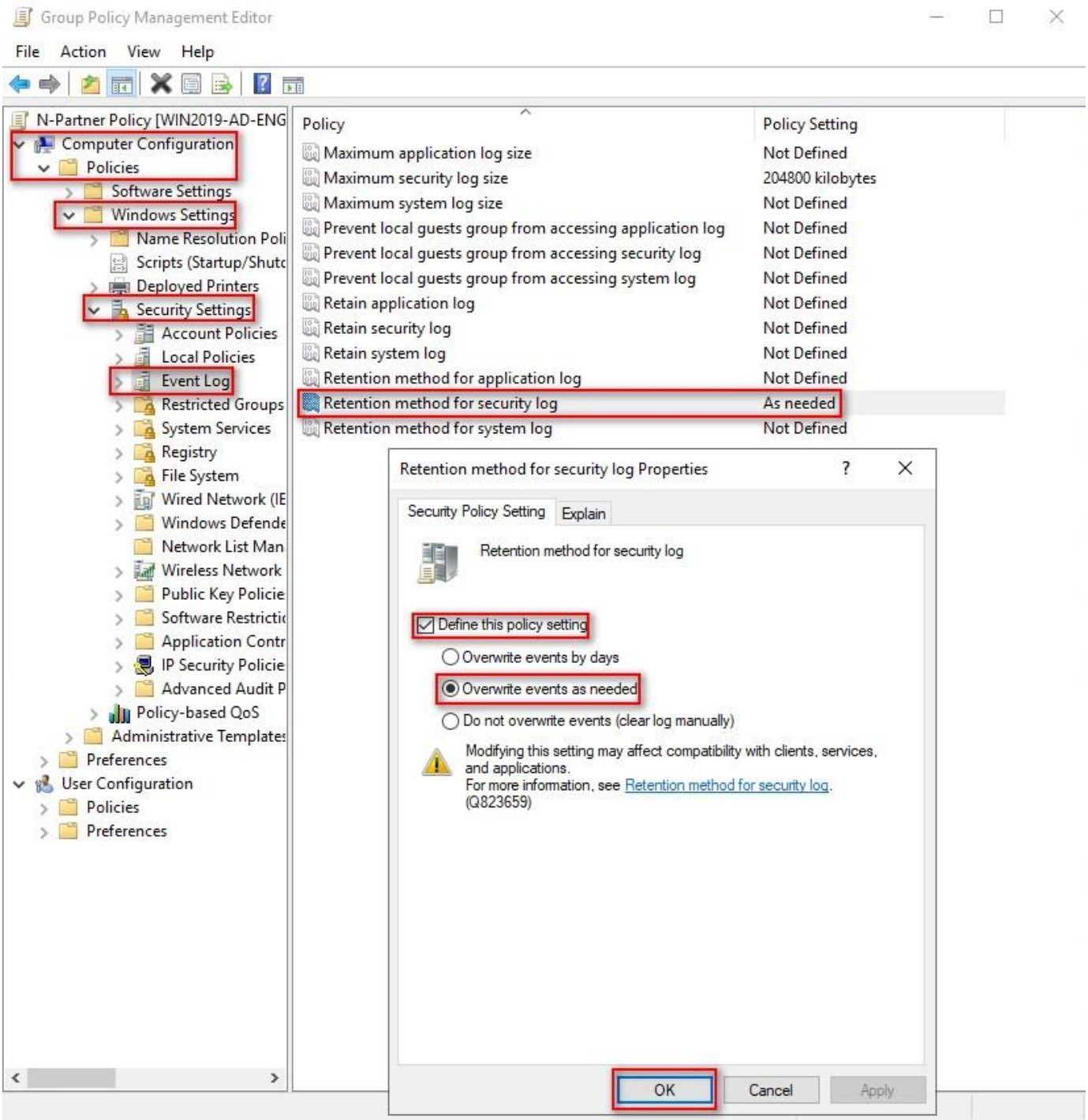
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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



(7) Event Logs: Retention Method for Security Log

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



(8) Open “Windows PowerShell” on your Windows server.

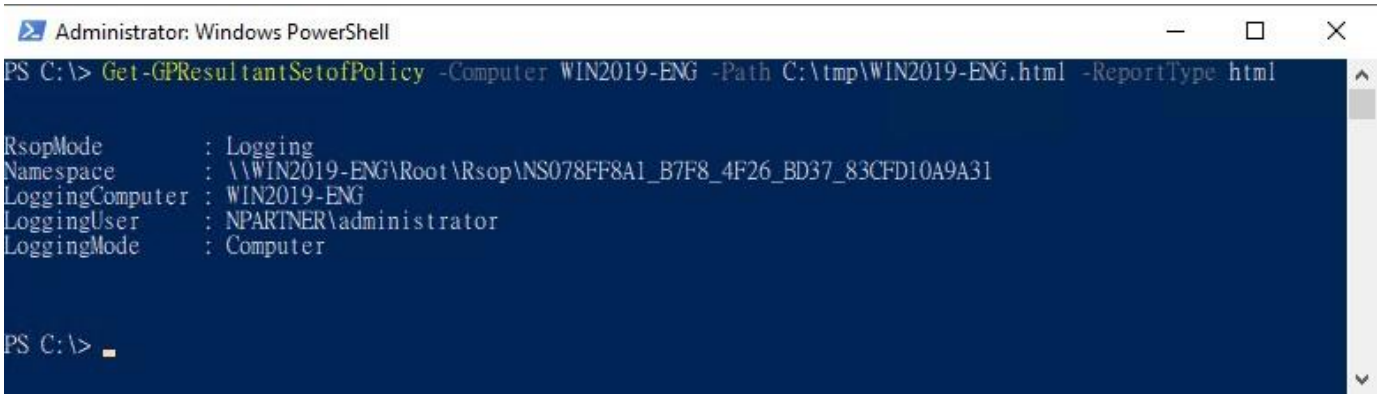
(9) Enter the command below to refresh group policy.

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

Please enter your Windows server hostname in red text.

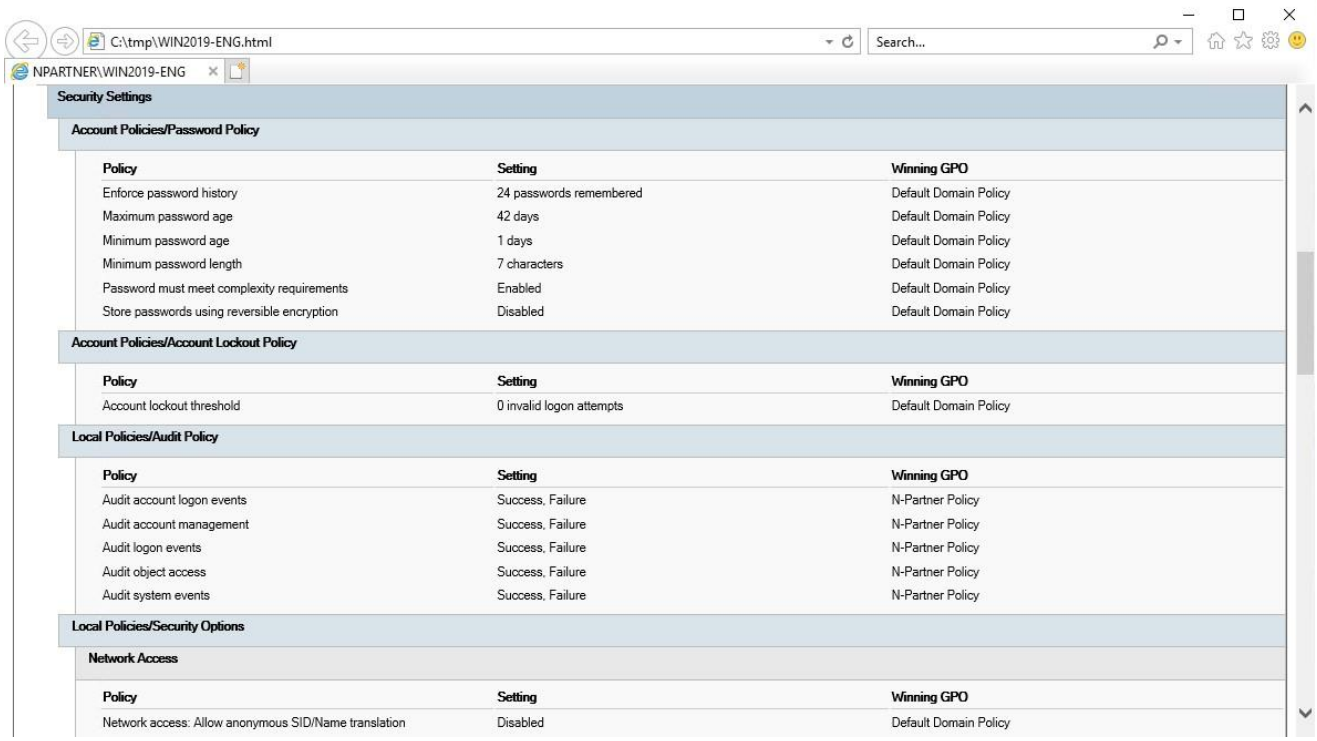
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

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



Please enter your Windows server hostname and the folder path including the file name in red text.

(11) Open your report. -> Confirm your Windows server hostname. -> Apply the N-Partner Policy Group Policy.

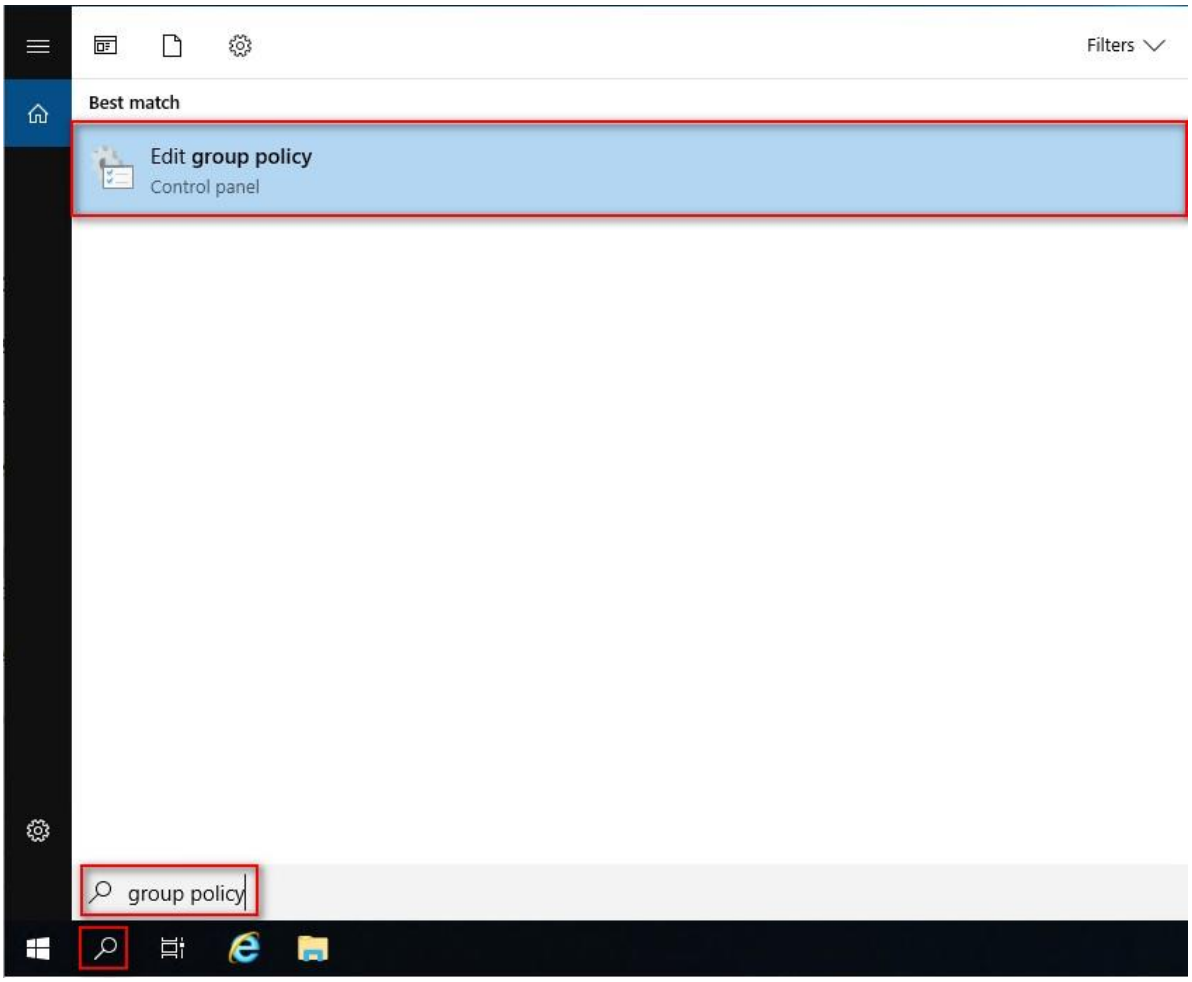


7.2 Workgroup

7.2.1 Audit Policy Settings

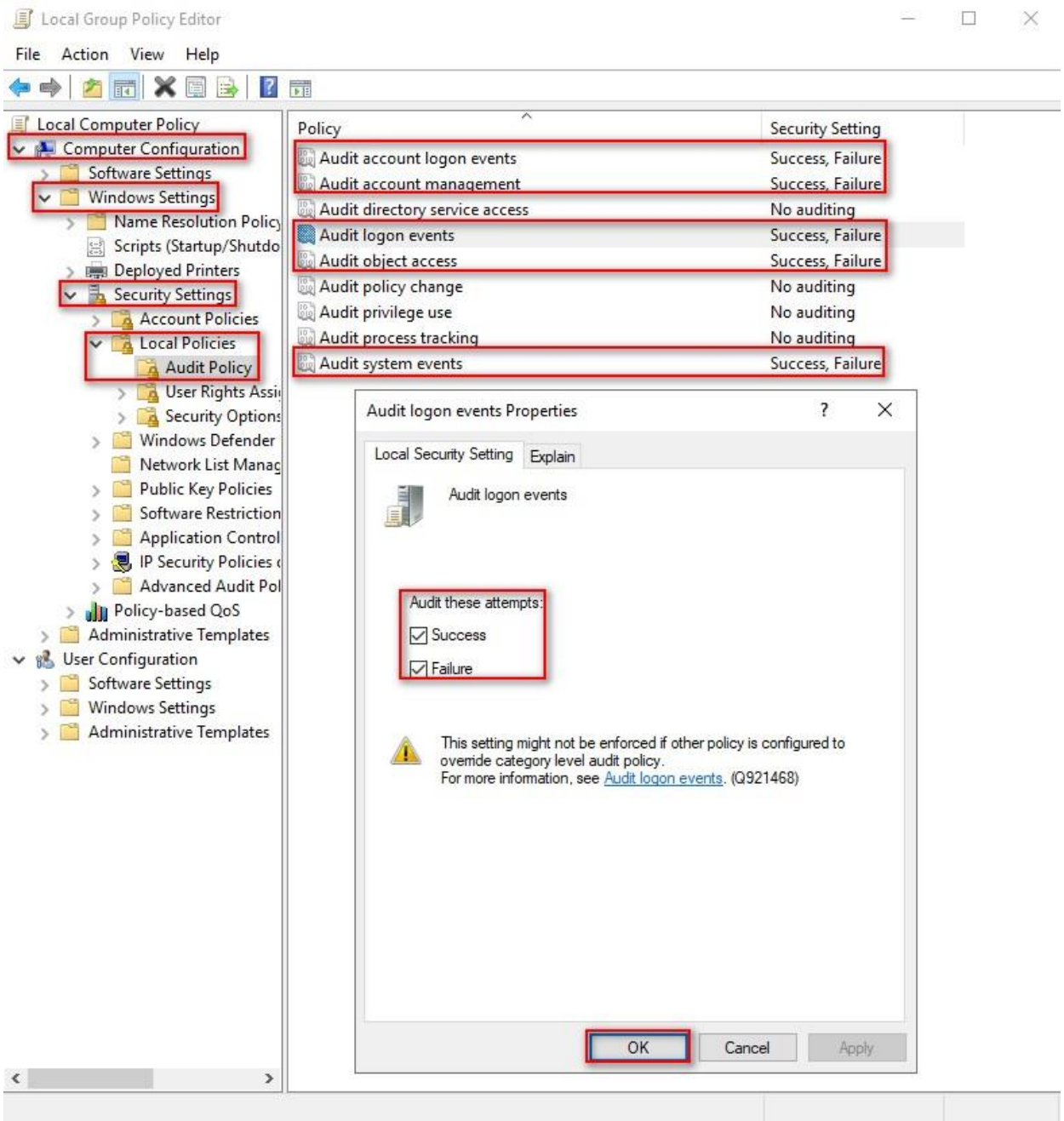
(1) Search for “Group Policy Object Editor”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy” in the search results.



(2) Local Group Policies: Audit Policies

Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: “Success” & “Failure” -> Click “OK.”



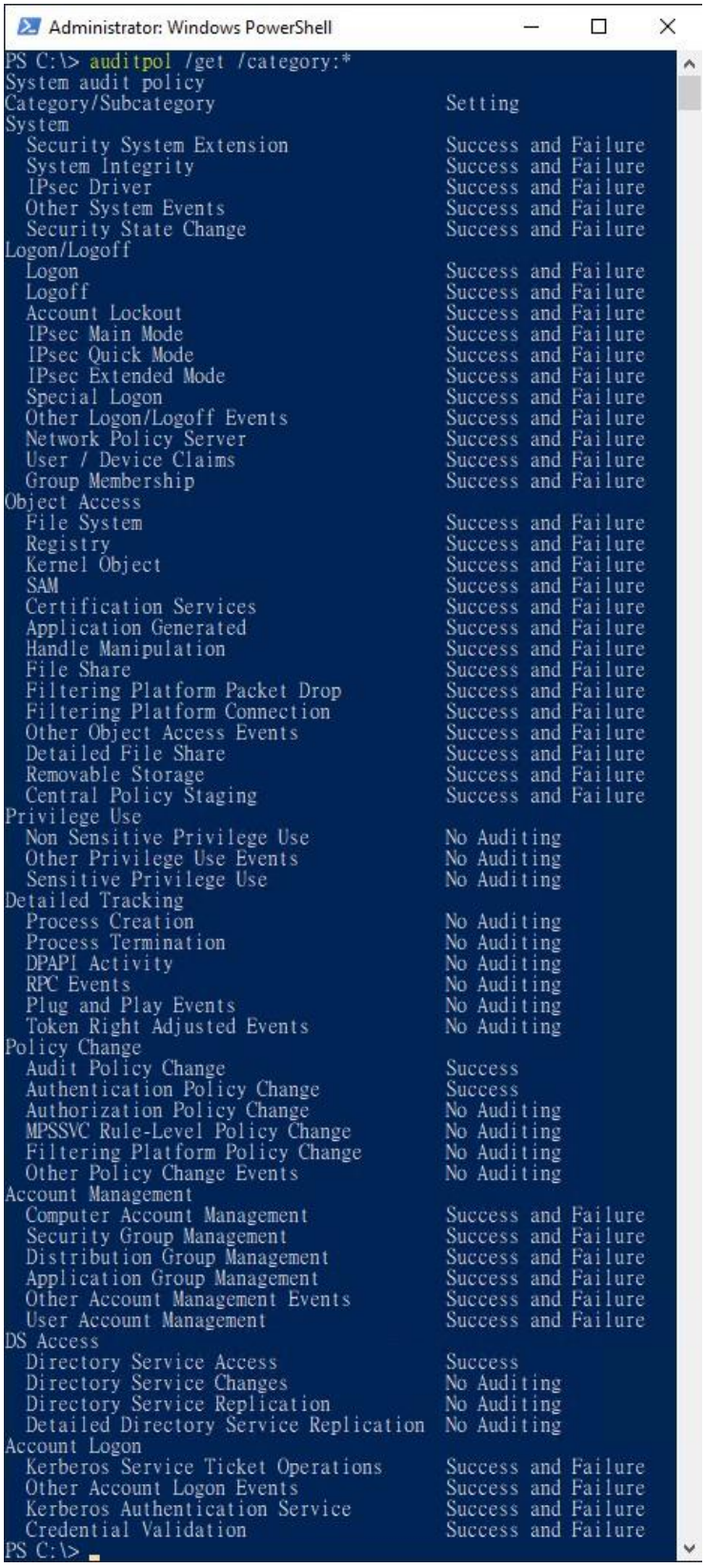
(3) Open “Windows PowerShell.”

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

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

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

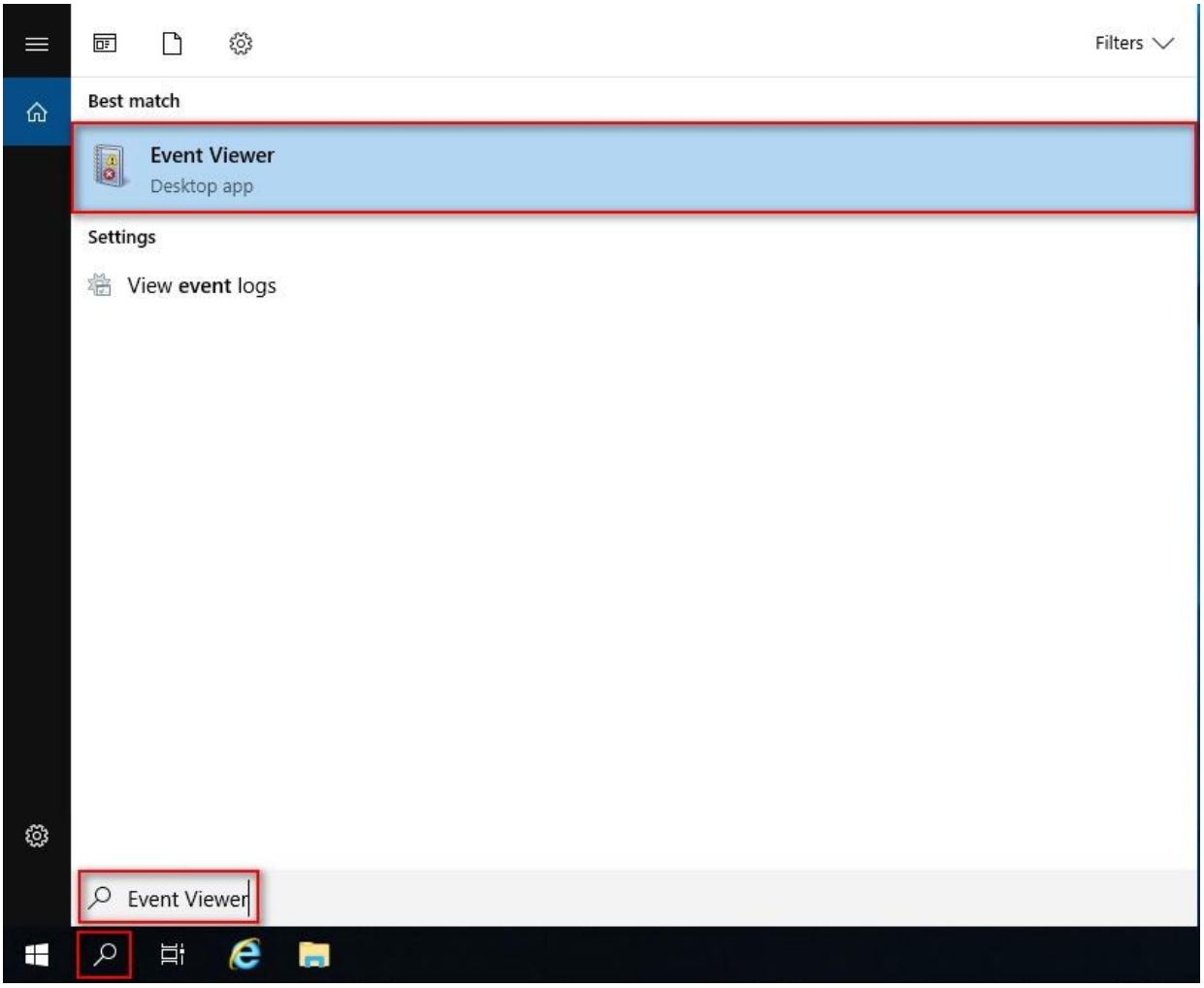
```
PS C: \> auditpol /get /category:*
```



7.2.2 Event Log Settings

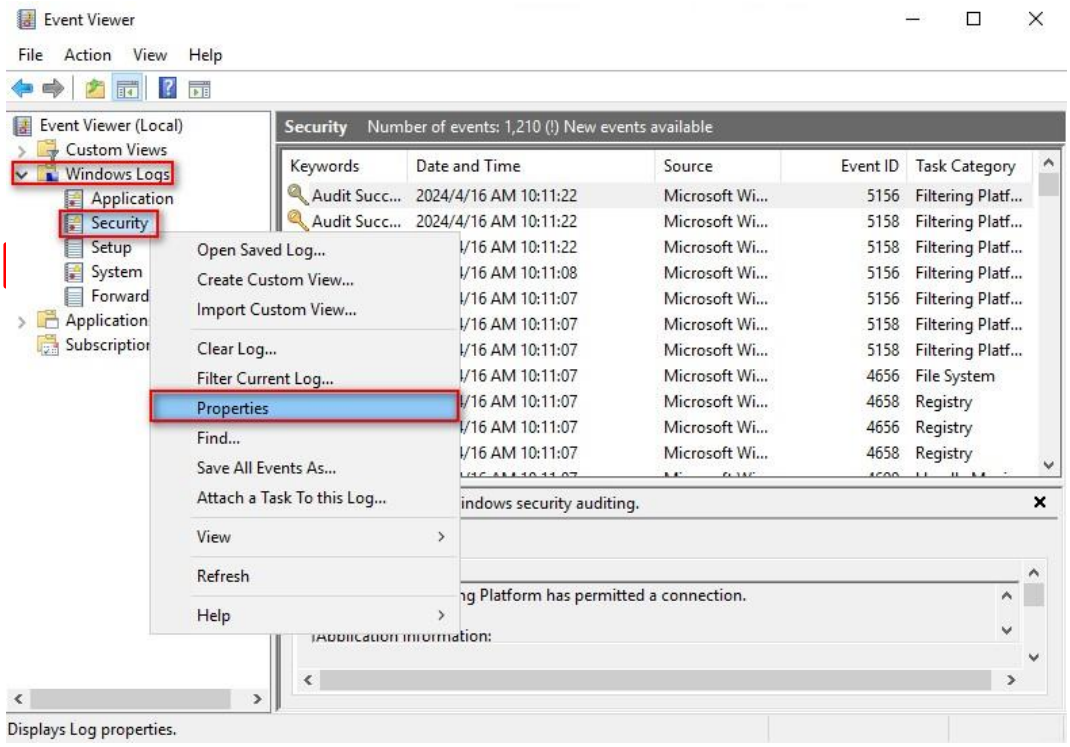
(1) Search for “Group Policy Object Editor”

Enter “Edit Group Policy” to search. -> Click on “Edit Group Policy.



(2) Edit Security Log

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

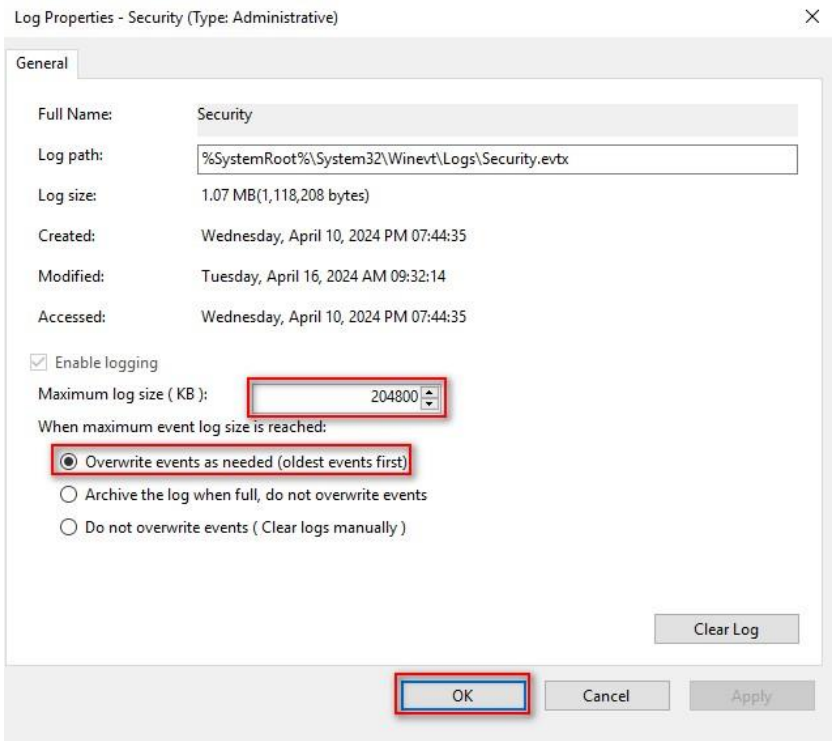


(3) Configure Security Log

Enter maximum log file size: 204800 KB

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

-> Click on “Overwrite events as needed” -> Click “OK.”



8. For Windows 2022

Windows Audit Policy Settings

Please refer to the “Audit Policy Recommendationlink provided in prefacefor detailed explanations.

※ Below are the settings for both domain and workgroup configurations.

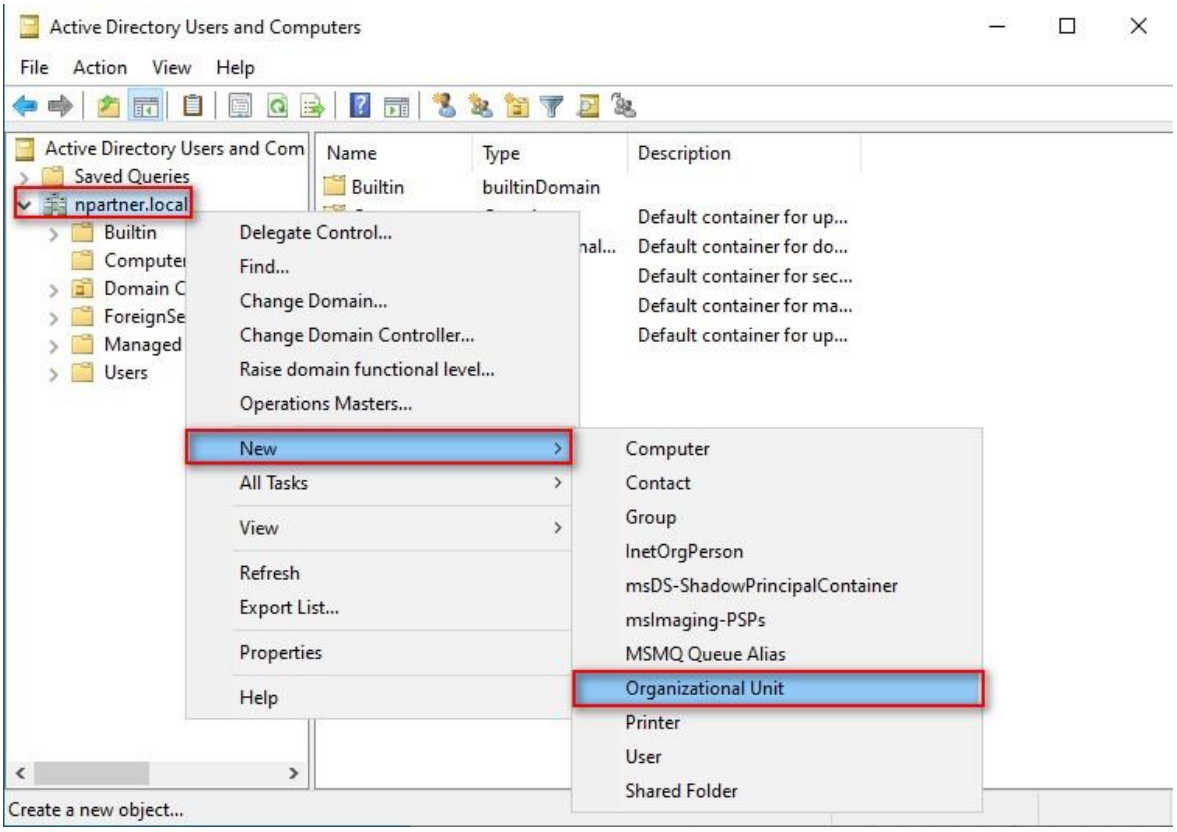
8.1 Domain

8.1.1 Organizational Unit Setup

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

(2) Add Your Organizational Unit

Right-click on your “Domain Name,” (in this example, it is “npartner.local”), select “New” and click “Organizational Unit.”

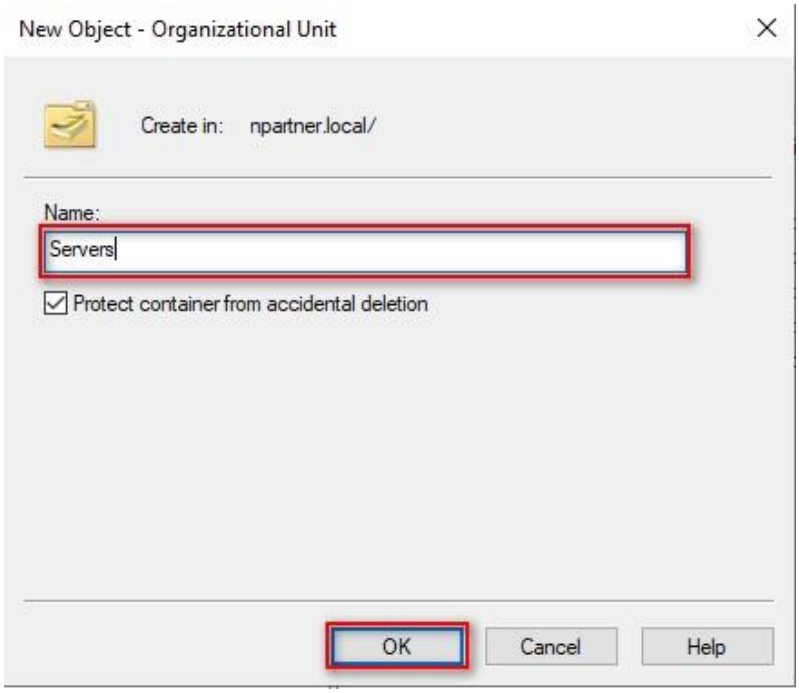


(3) Name Your Organizational Unit

Enter your “Organizational Unit Name,” (in this example, it is “Servers”)

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

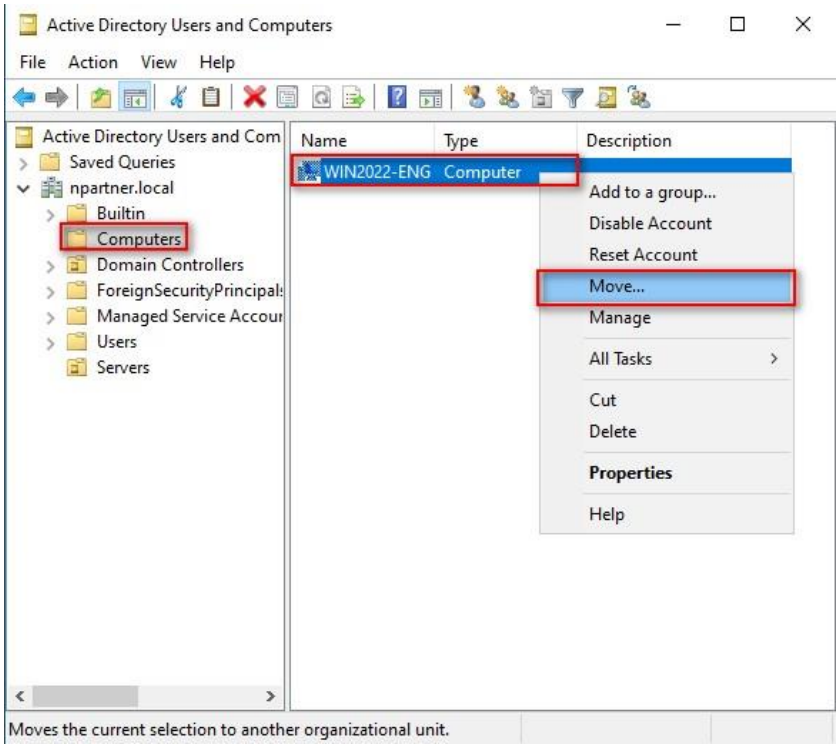
-> and click “OK.”



(4) Move Your Server to New Organizational Unit

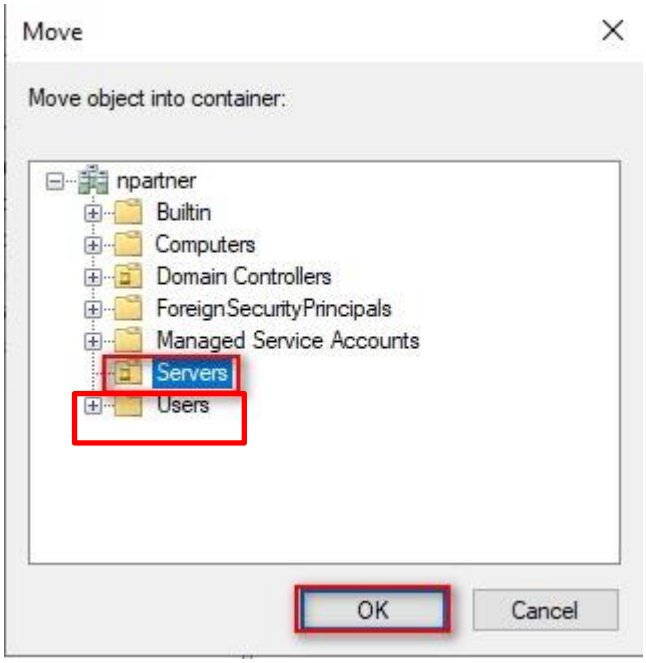
Select your organizational unit (the example here is “Computers”) -> Right-click on the “WIN2022-ENG” server.

Note: Please select the Windows Server host based on actual environment. -> Click “Move.”



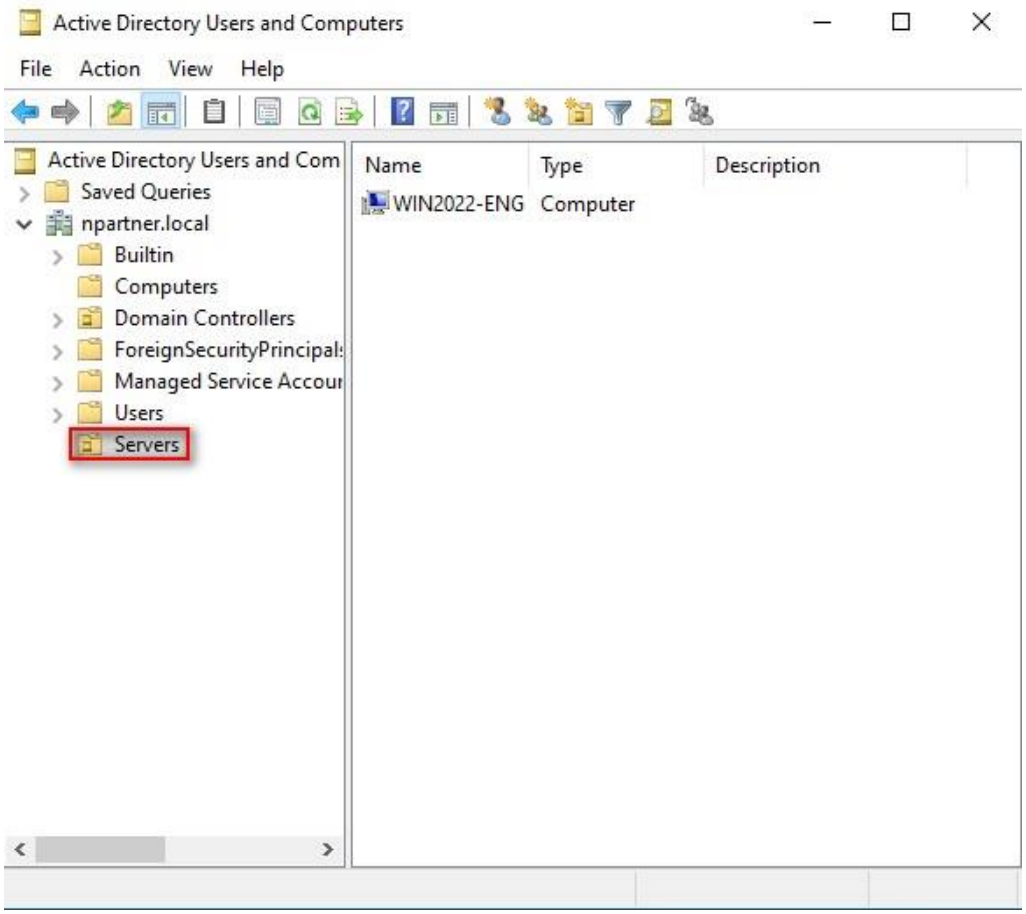
(5) Select Your Organizational Unit

Select your organization unit (the example here is “Servers”) -> Click “OK.”



(6) Confirm Your Server Has Been Moved to the New Organizational Unit

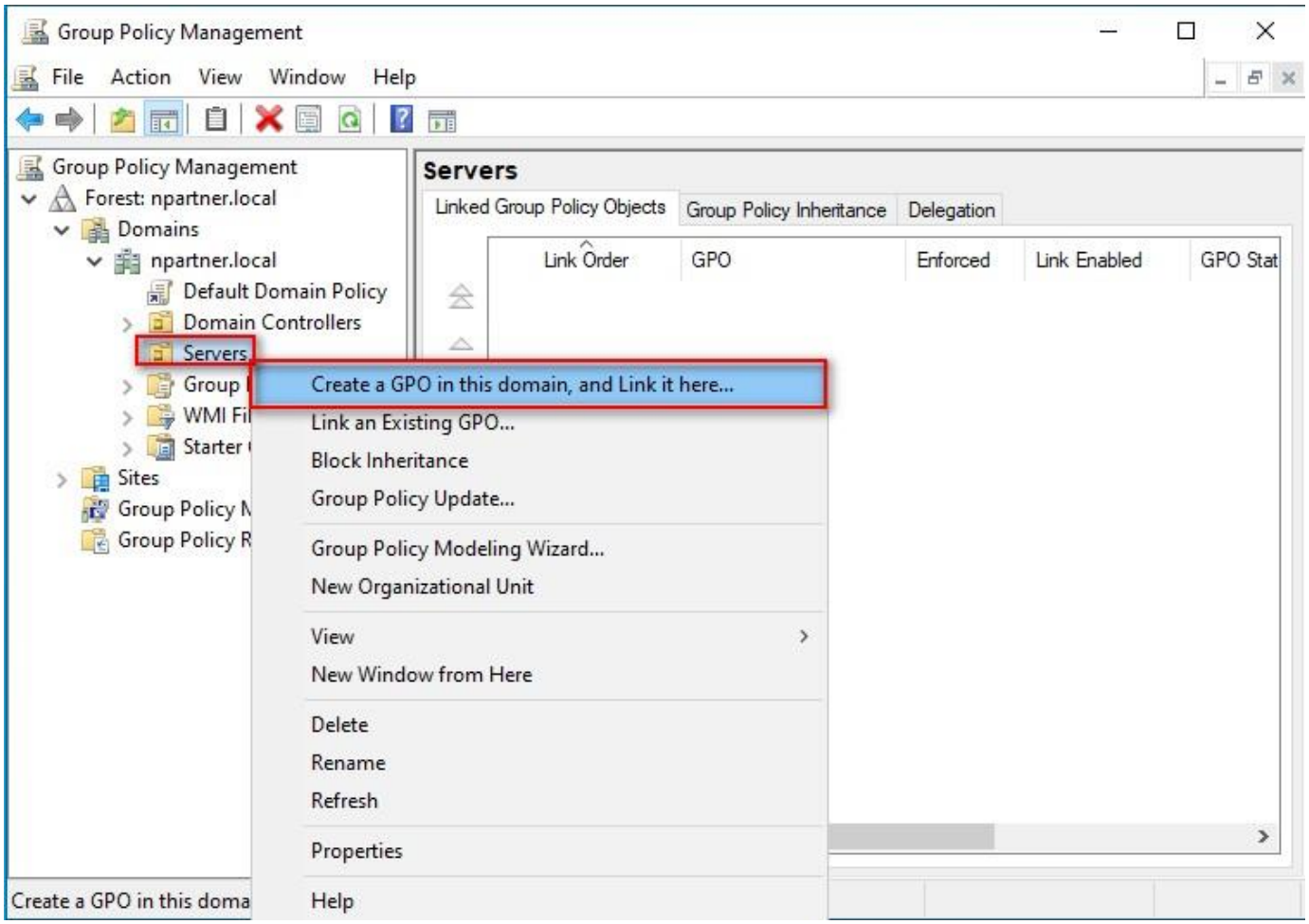
Click on your organizational unit (the example here is “Servers”) to confirm that the “WIN2022-ENG” server has been moved.



8.1.2 Group Policy Settings

(1) Open “Group Policy Management.”

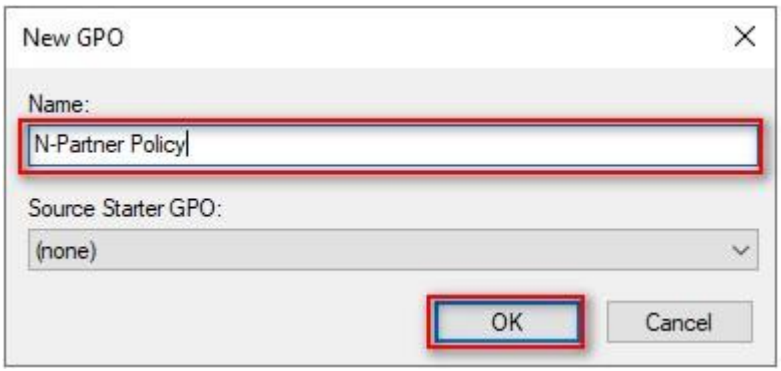
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

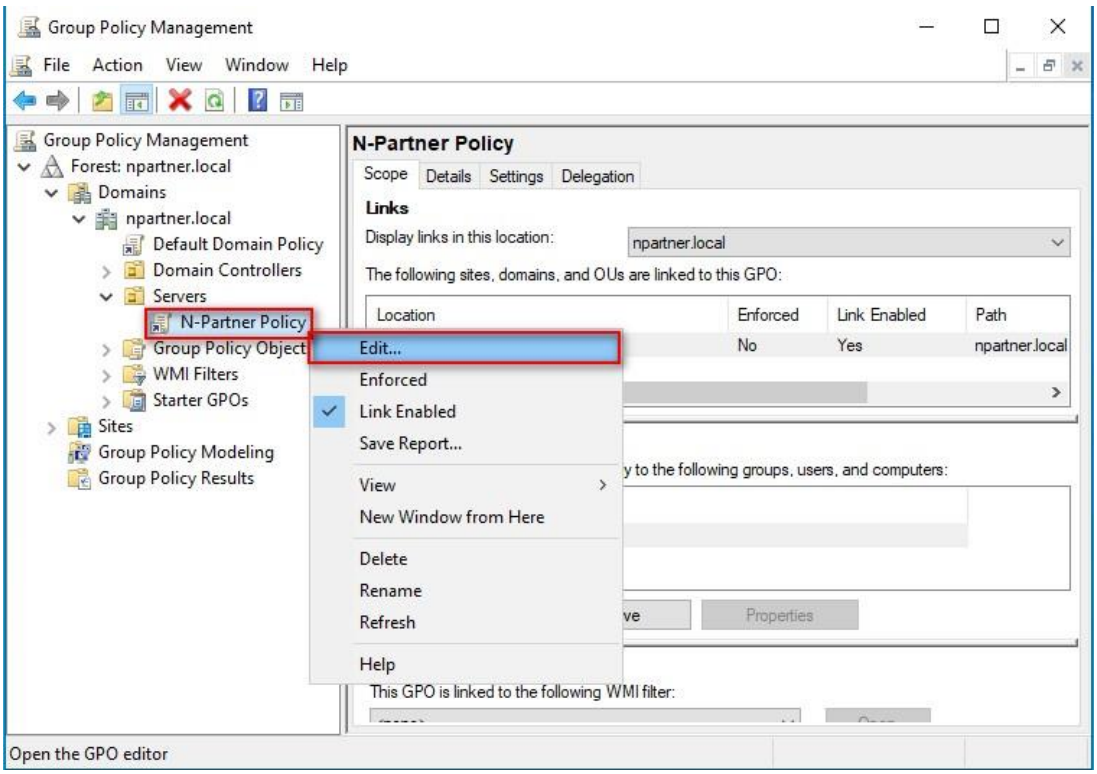
Enter your group policy object name (the example here is “N-Partner Policy”).

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



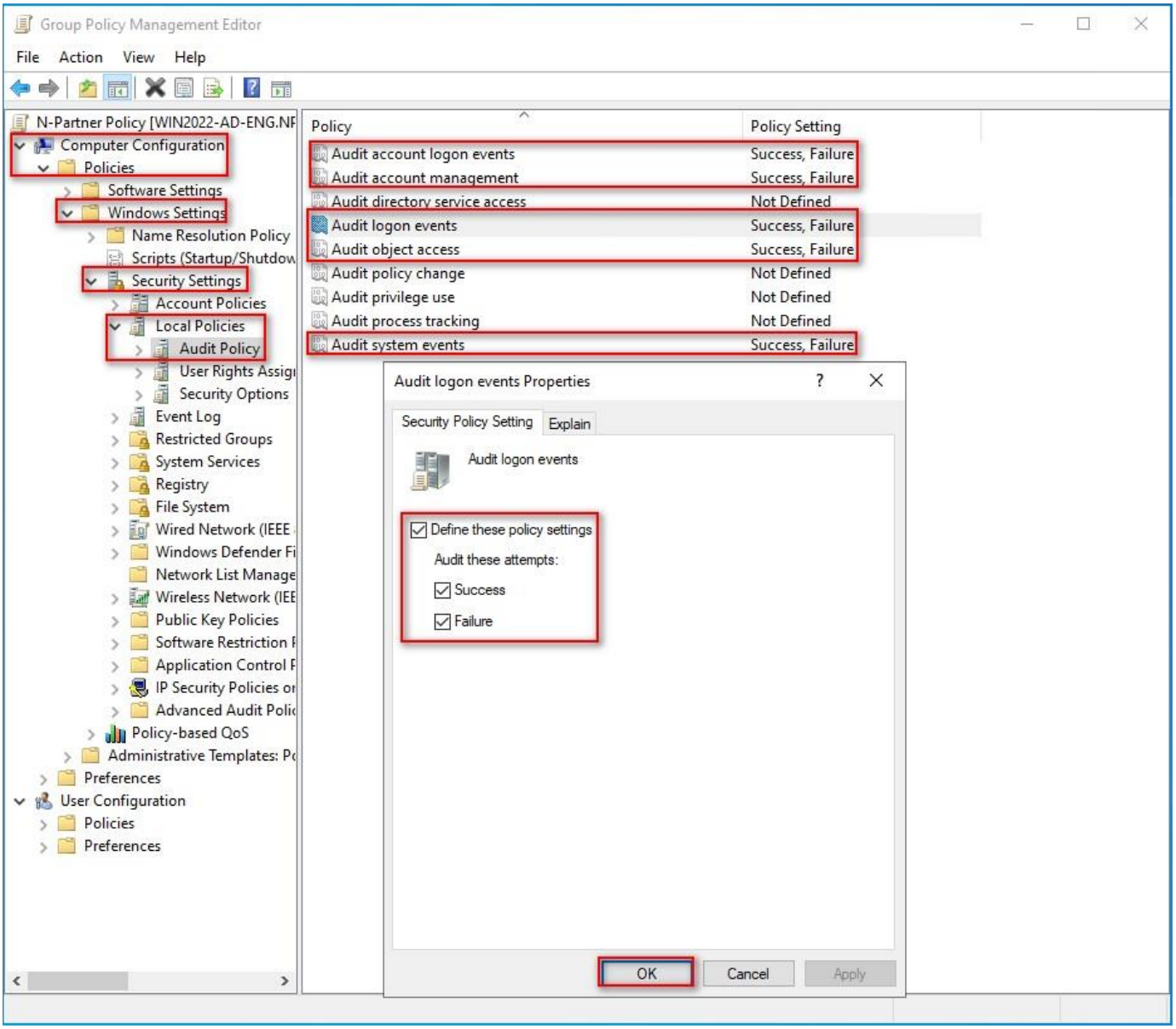
(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is “N-Partner Policy”) and click “Edit.”



(5) Local Group Policies: Audit Policy

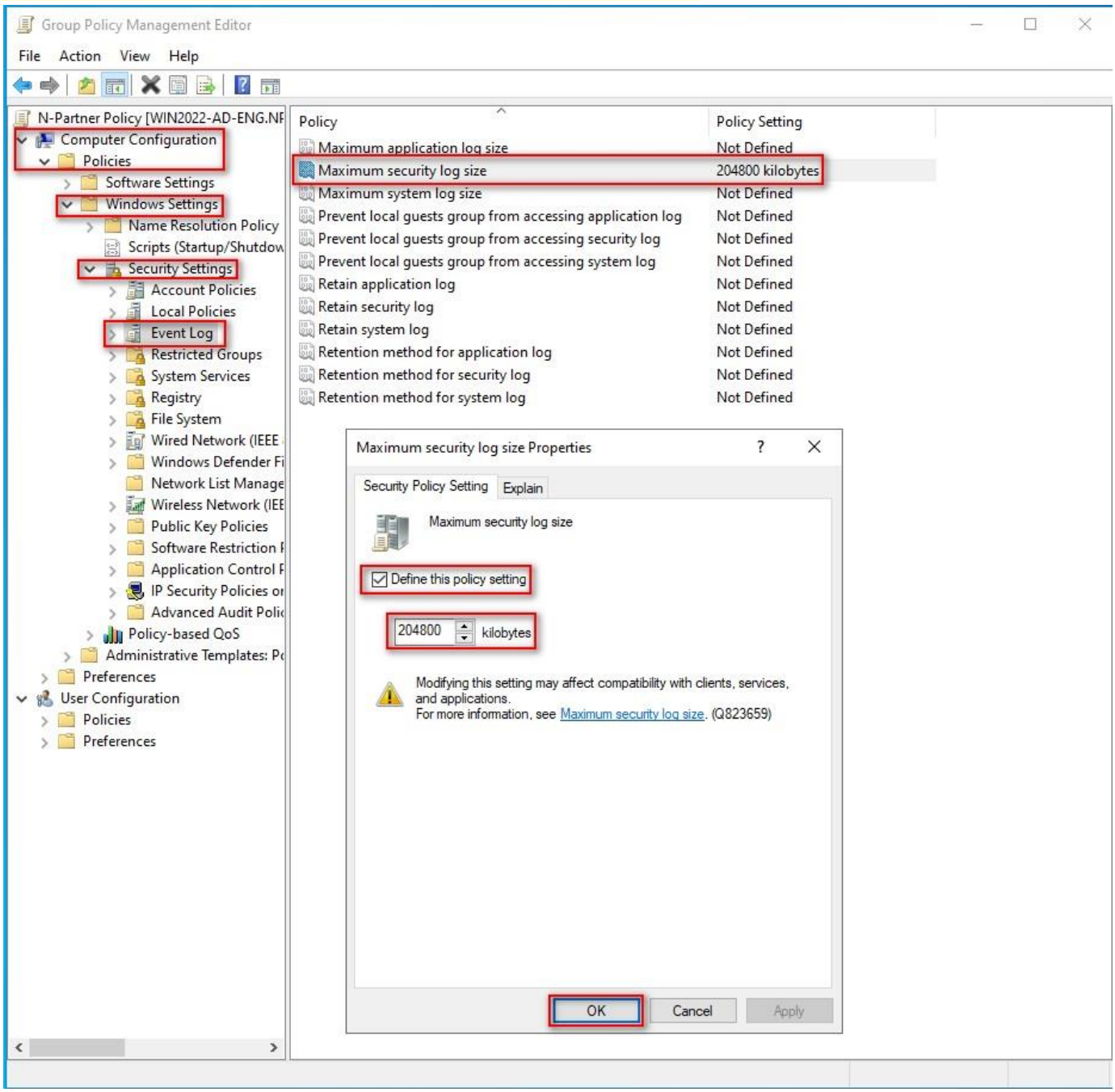
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Local Policies”-> “Audit Policy.” And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Define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



(6) Event Logs: Maximum Size of Security Log

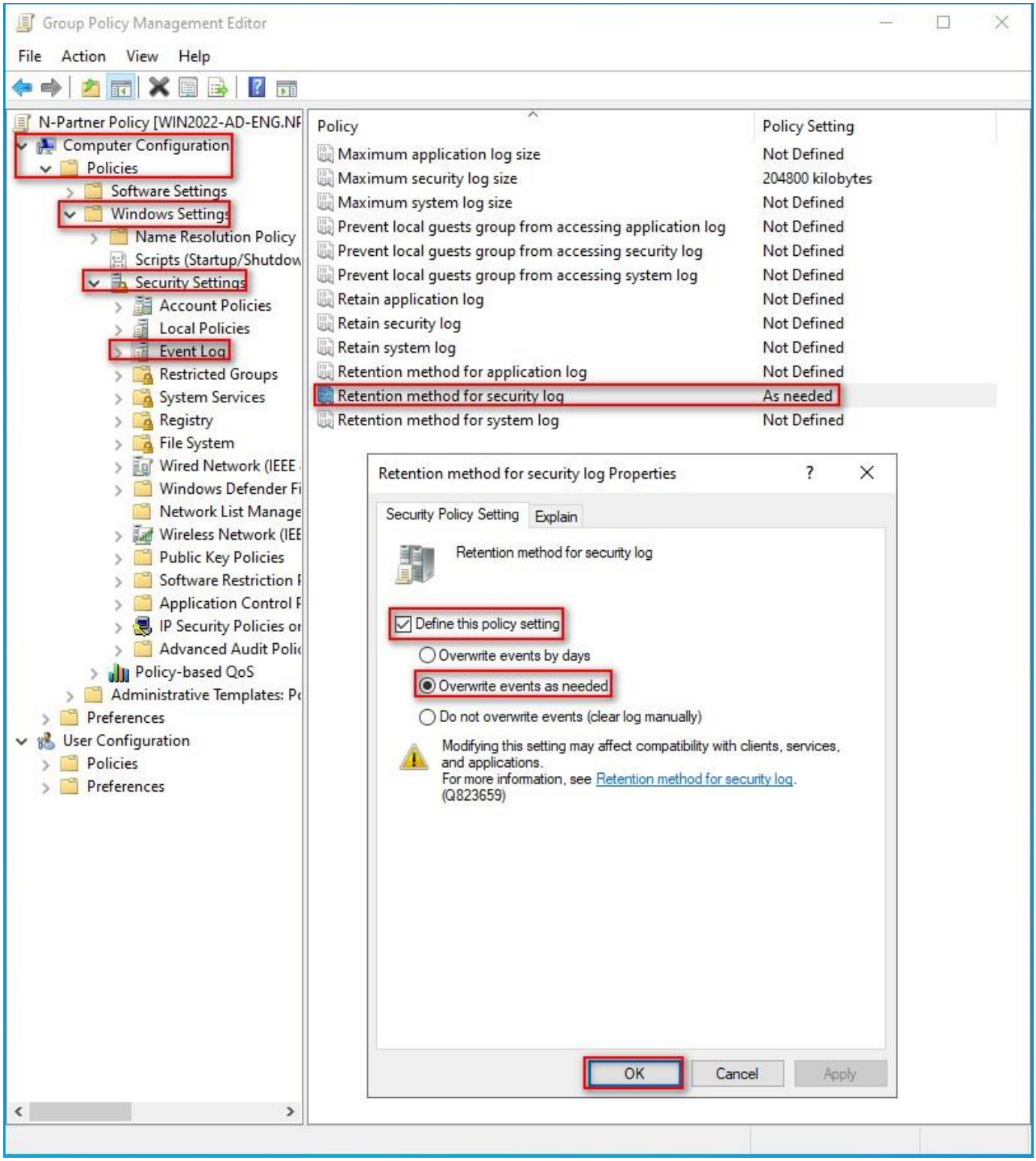
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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



(7) Event Logs: Retention Method for Security Log

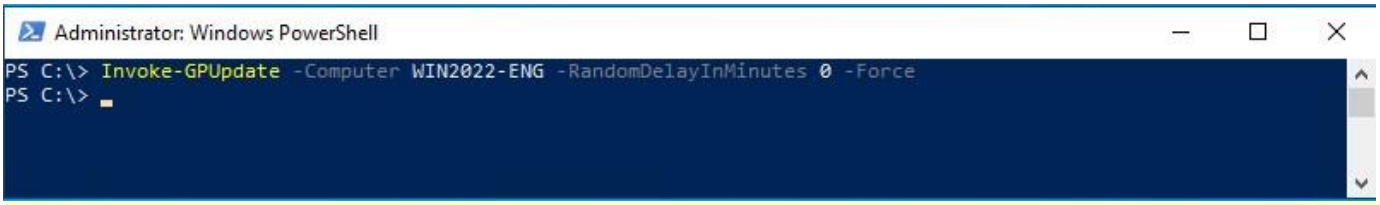
Expand folder “Computer Configuration” -> “Policies” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> Click on “Retention method for security log” -> Check “Define this policy setting”: -> And select “Overwrite events as needed” -> Click “OK.”



(8) Open “Windows PowerShell” on your Windows server.

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

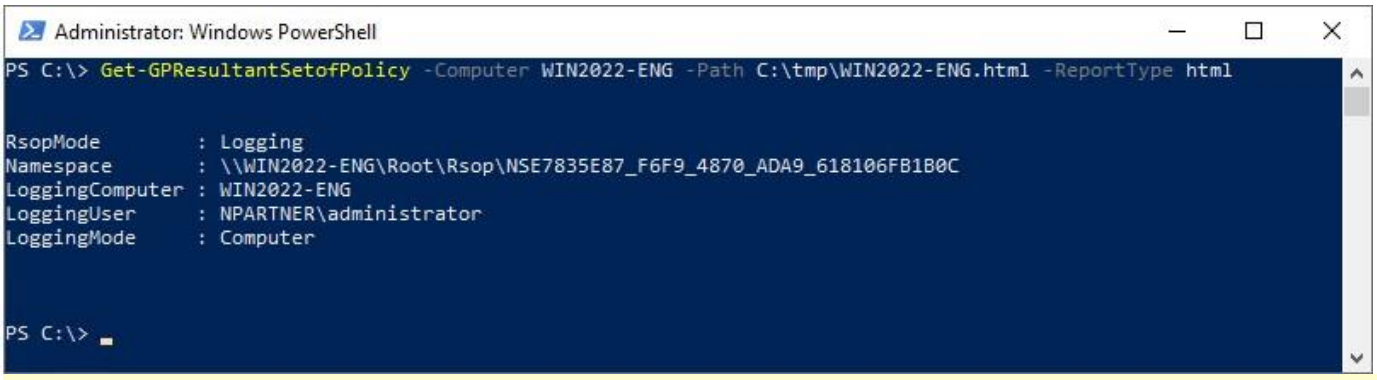
```
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
```



Please enter your Windows server hostname in red text.

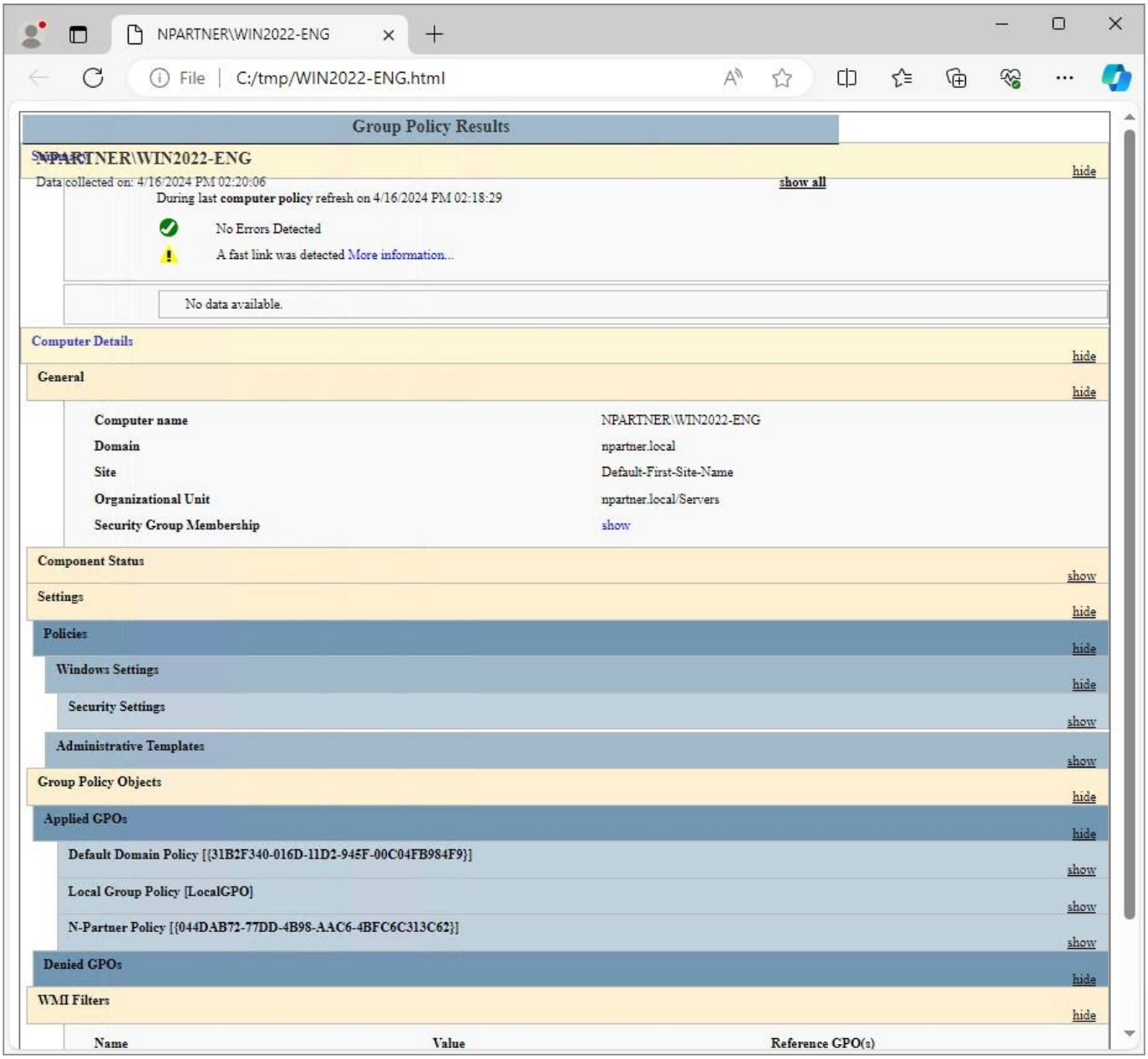
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

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



Please enter your Windows server hostname and the folder path including the file name in red text.

(11) Open your report. -> Confirm your Windows server hostname. -> Apply the N-Partner Policy Group Policy.

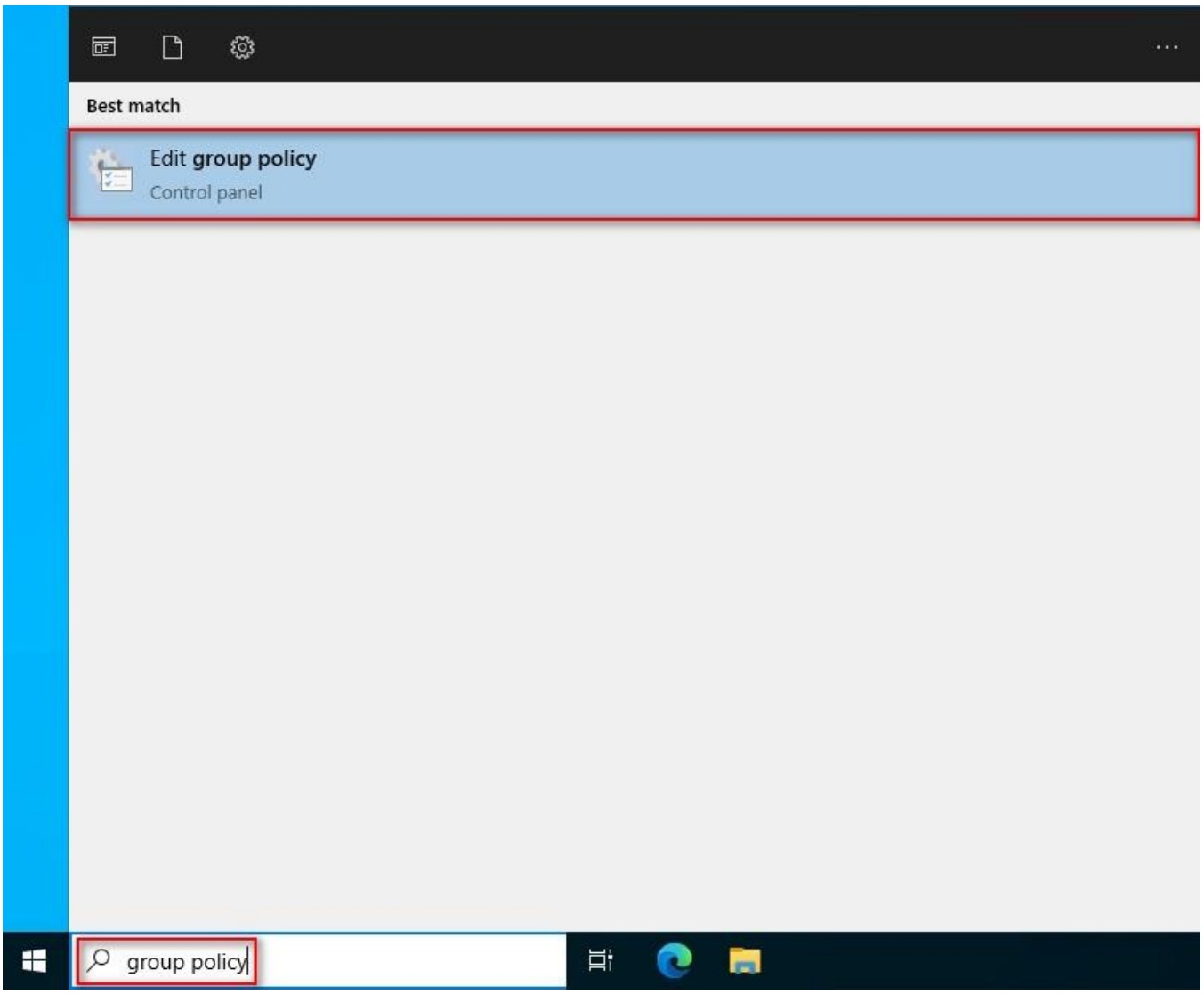


8.2 Workgroup

8.2.1 Audit Policy Settings

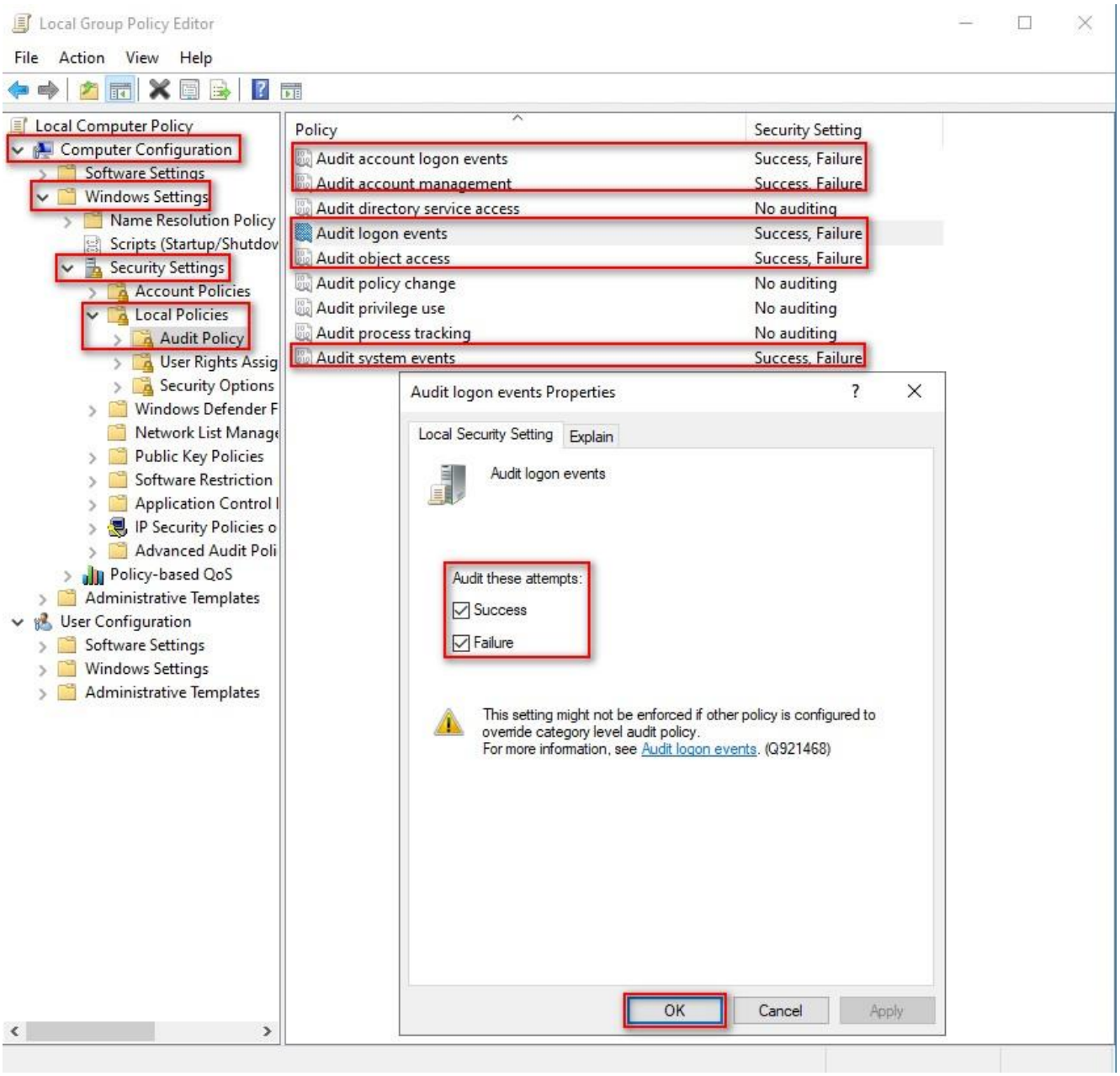
(1) Edit Your Group Policy Object

Select  and right-click your group policy object name (the example here is “N-Partner Policy”) and click “Edit.”



(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 account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Define these policy settings”: Success, Failure. -> Click “OK.”



(3) Open “Windows PowerShell” on your Windows server.

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

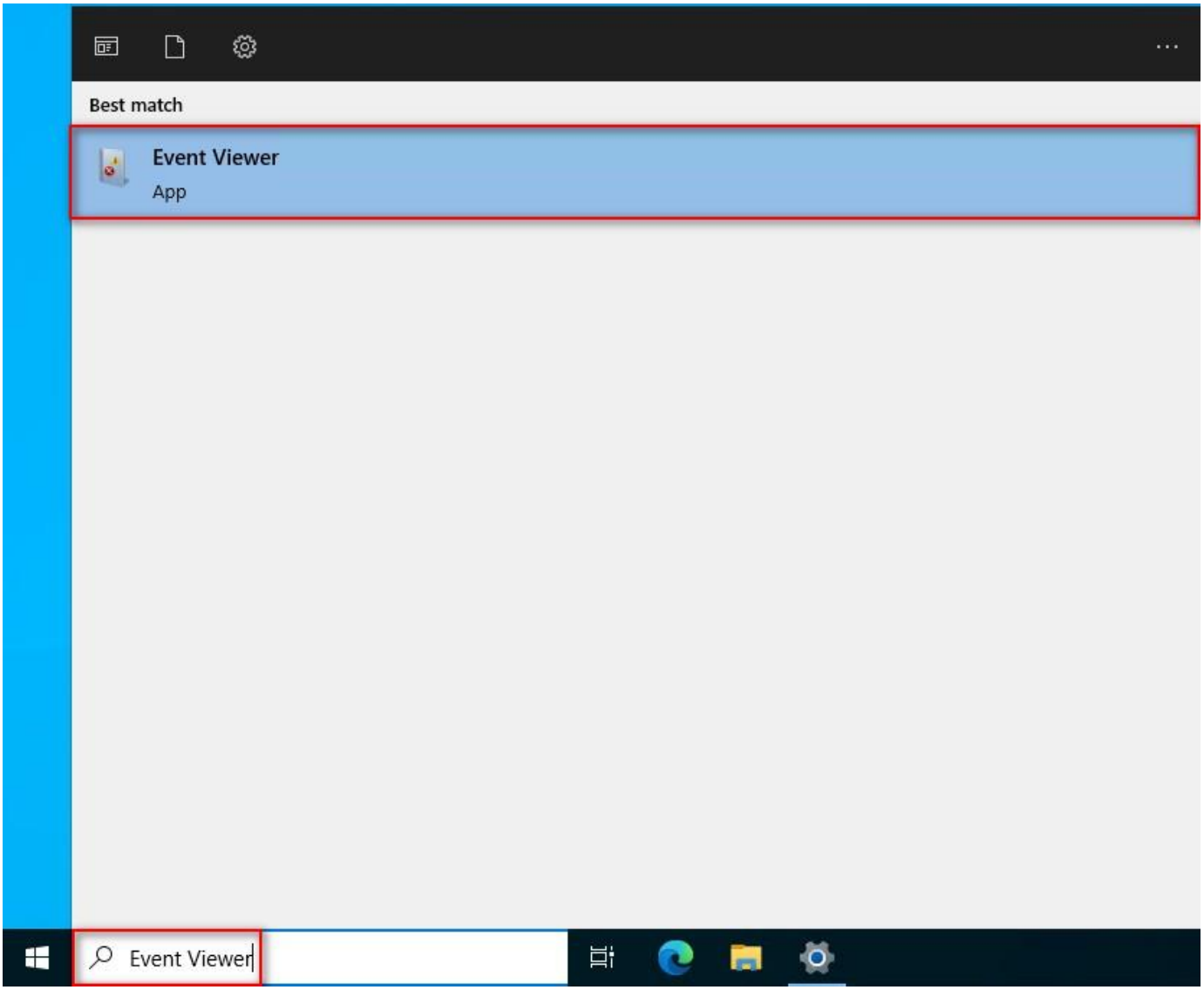
```
PS C: \> gpupdate /force
```

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

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

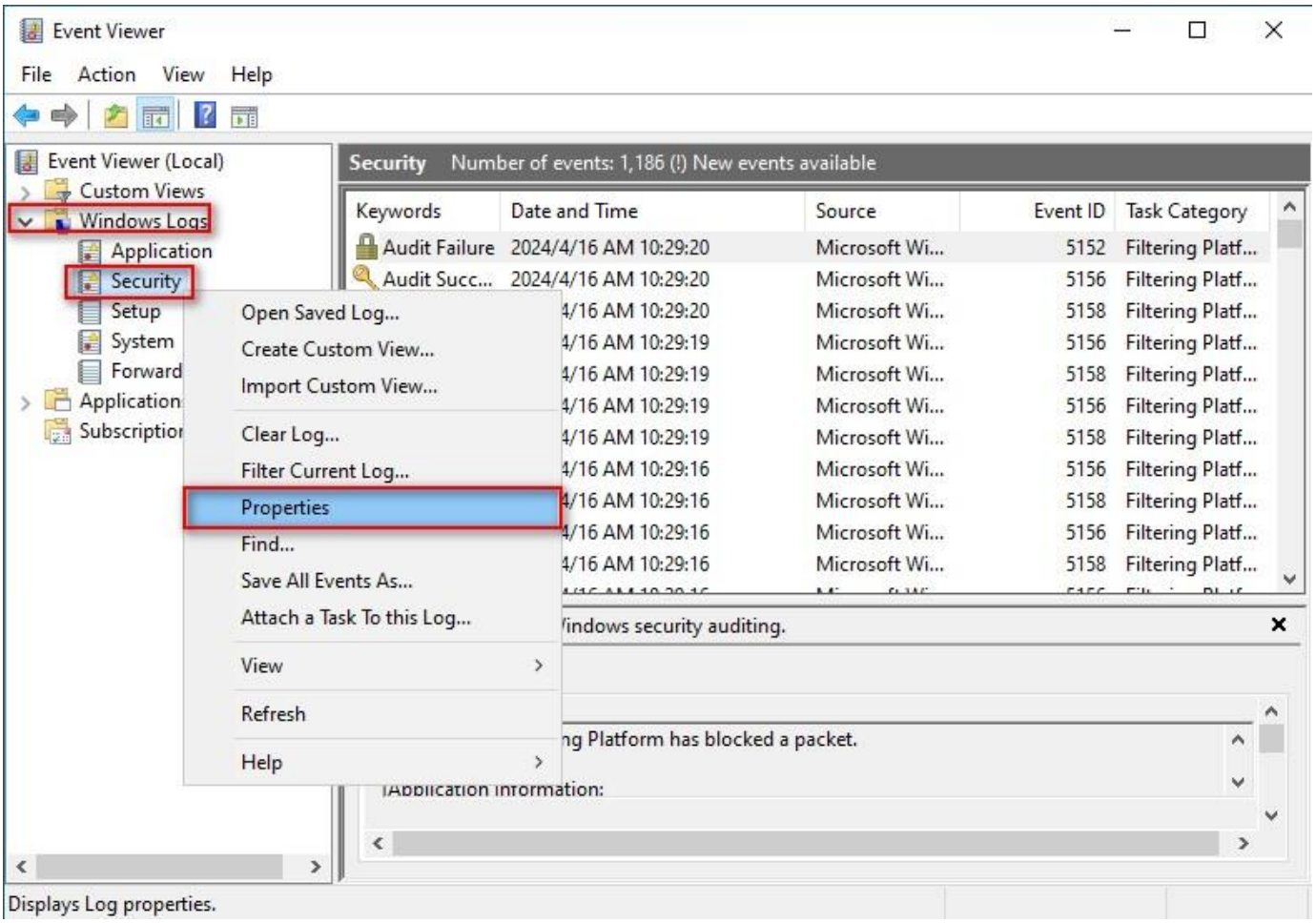
8.2.2 Event Log Settings

(1) Enter “Event Viewer” to search. -> Click on “Event Viewer.”



(2) Edit Security Log

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

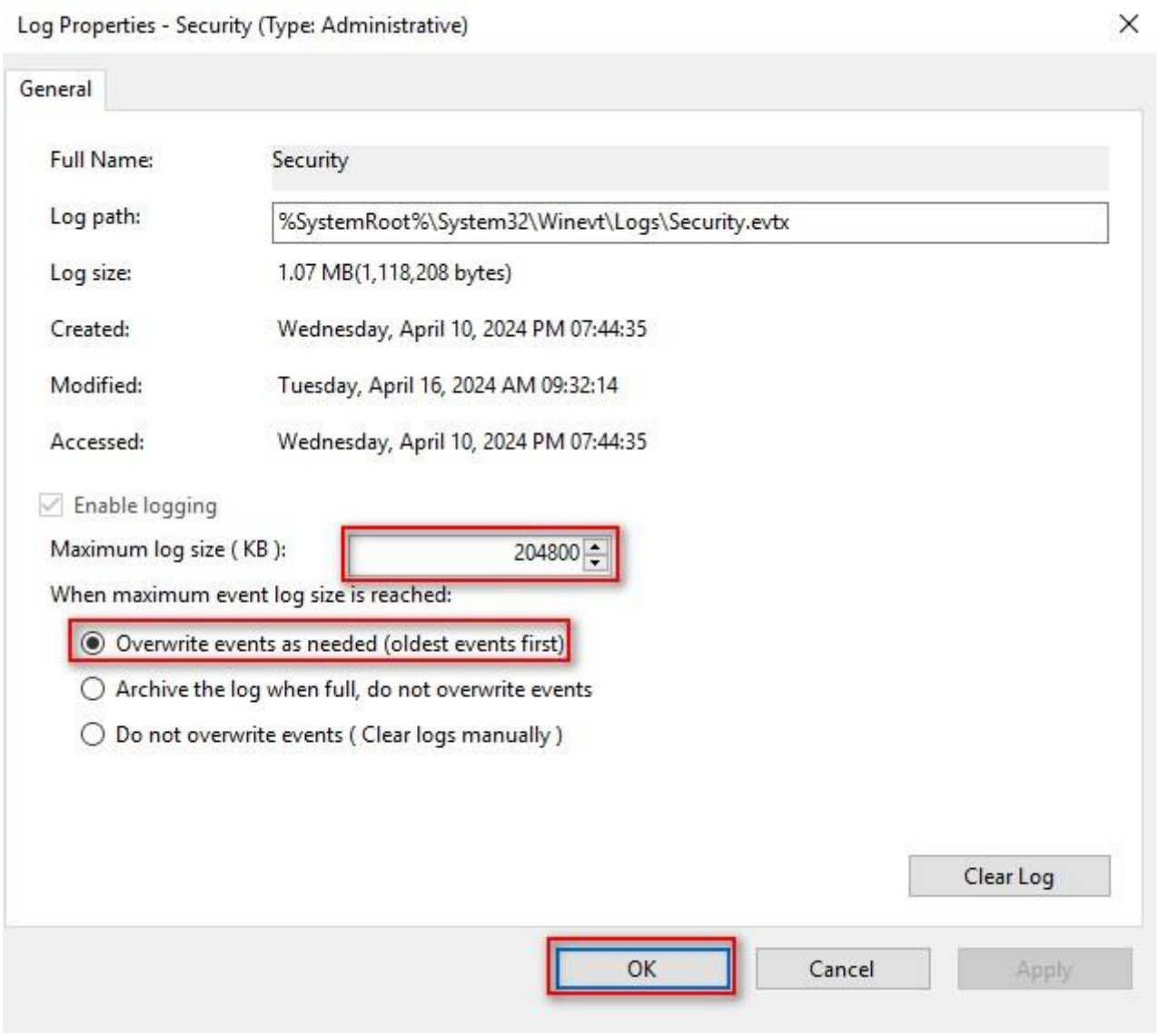


(3) Configure Security Log

Enter maximum log file size: 204800 KB

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

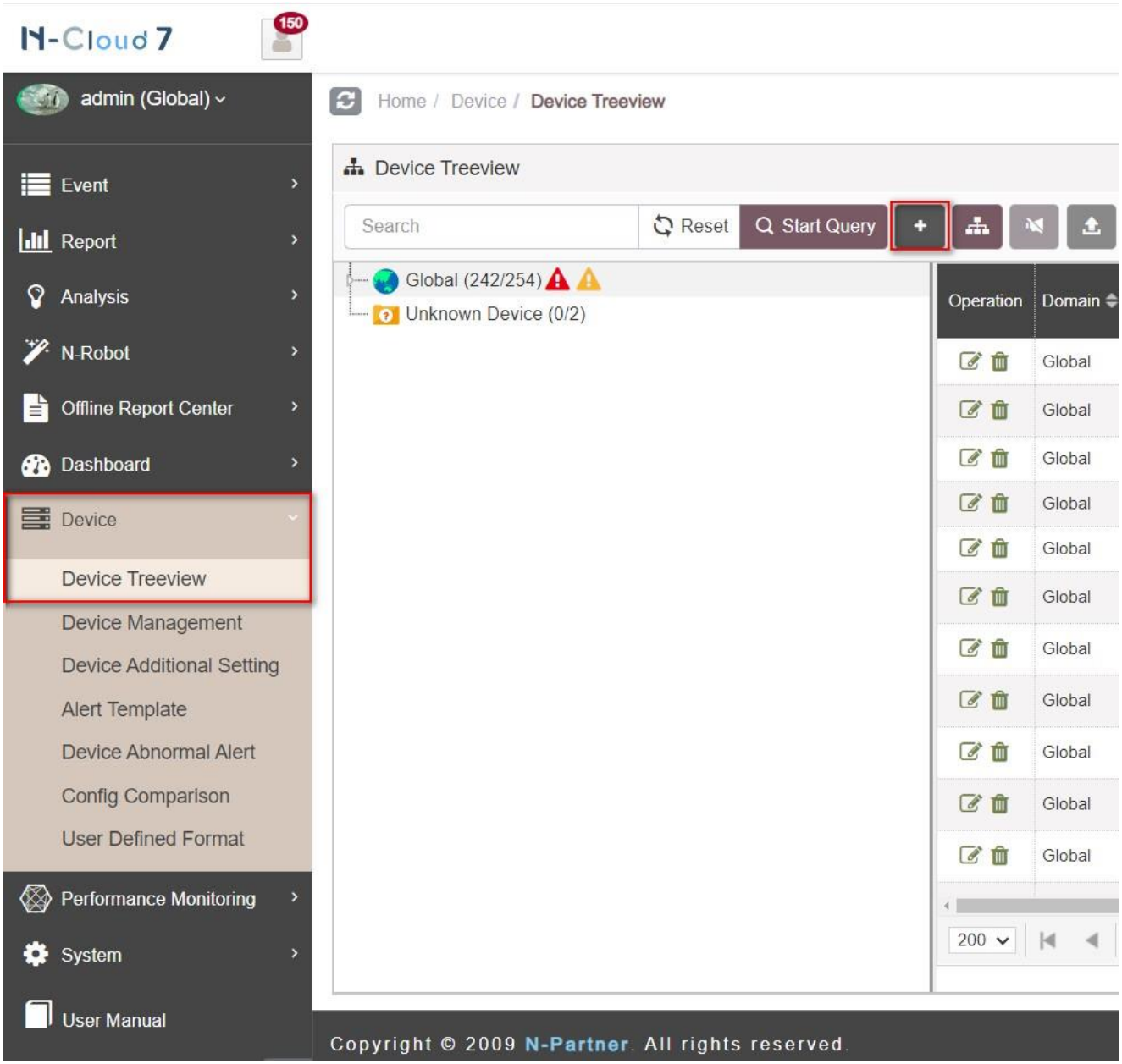
-> Click on “Overwrite events as needed” -> Click “OK.”



9. N-Reporter

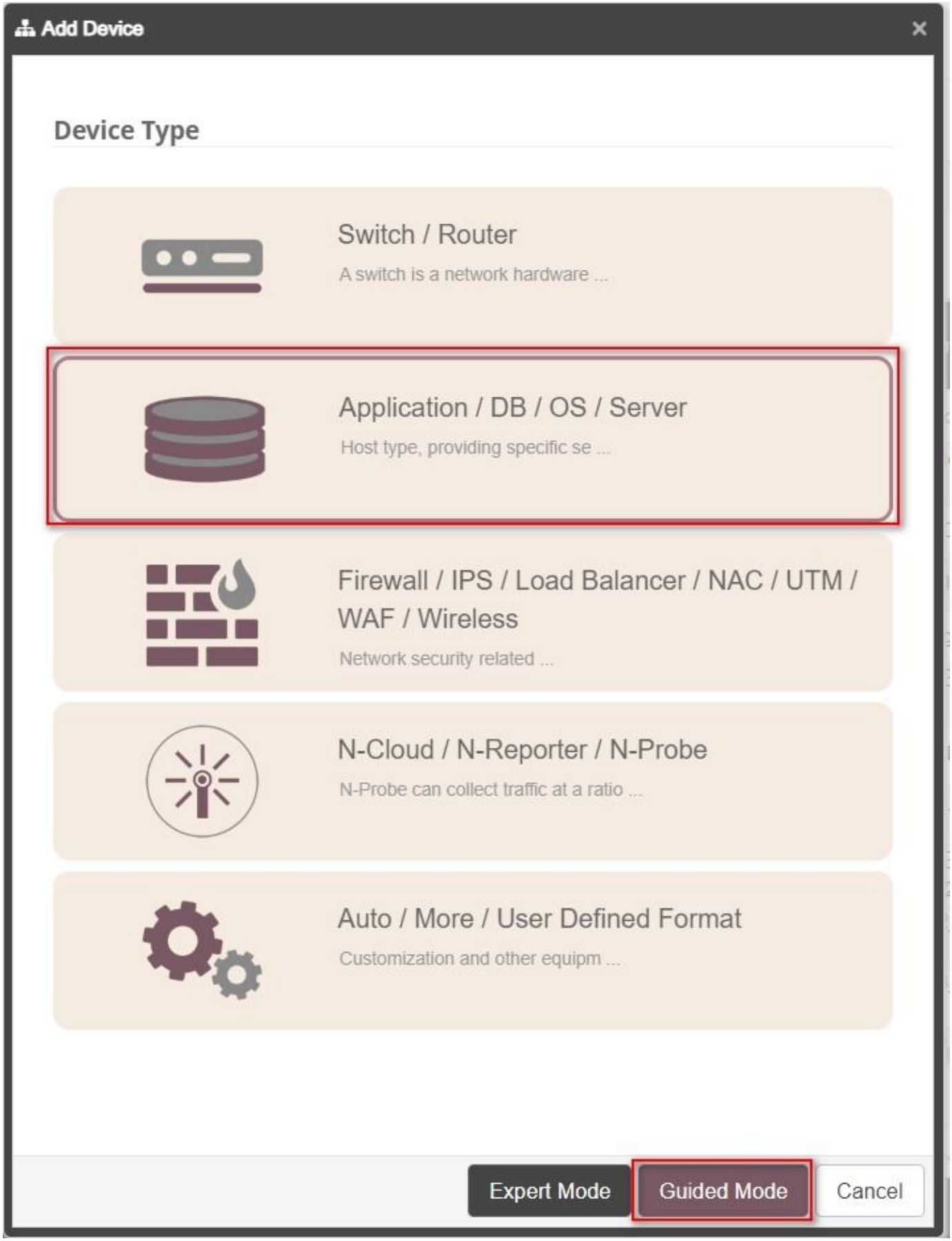
(1) Add a Windows Server Device:

Click “Device” -> “Device Treeview” -> And click “Add.”

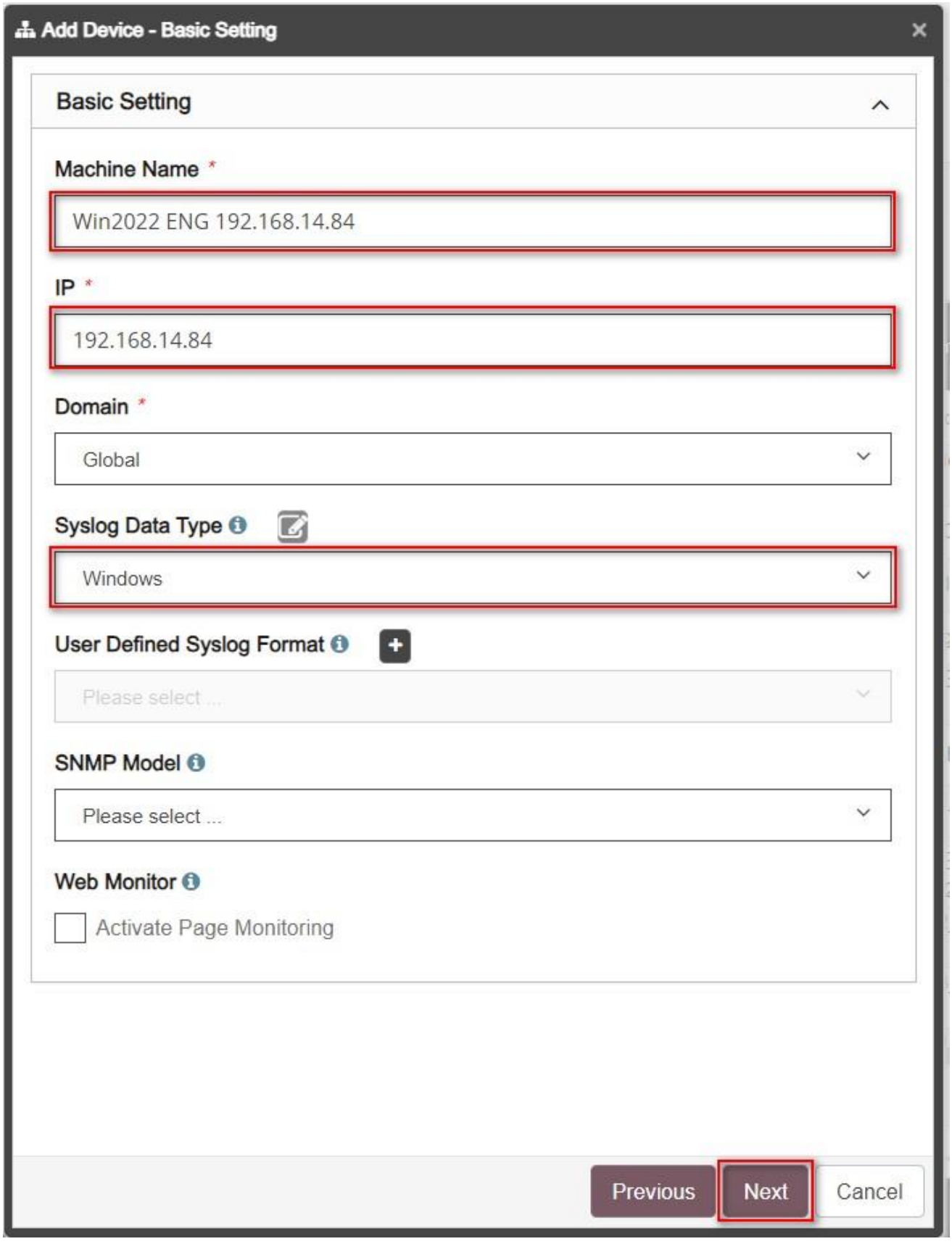


(2) Set the Device Type for your Windows Server Device:

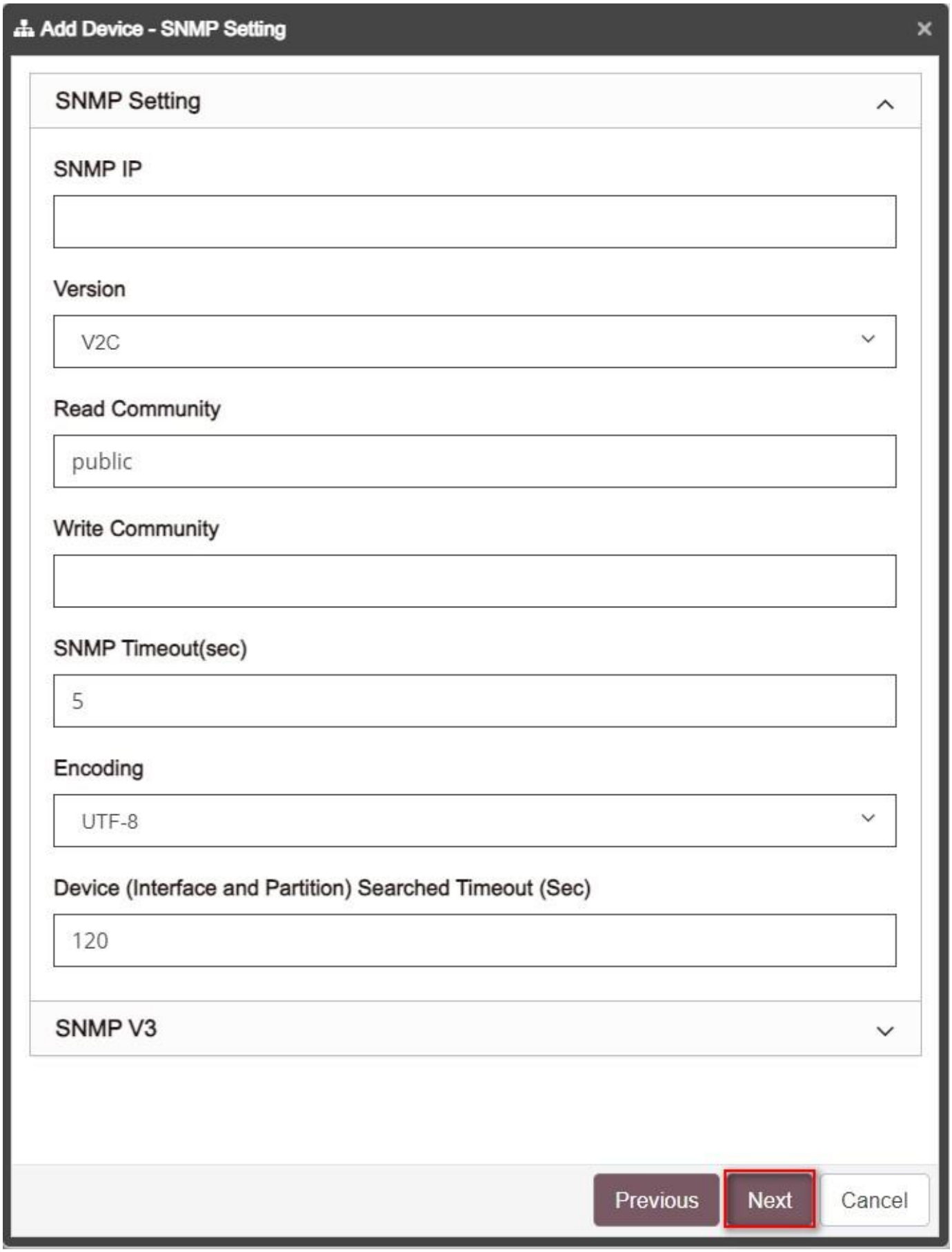
Click “Application / DB / OS / Server,” then click “Guided Mode.”



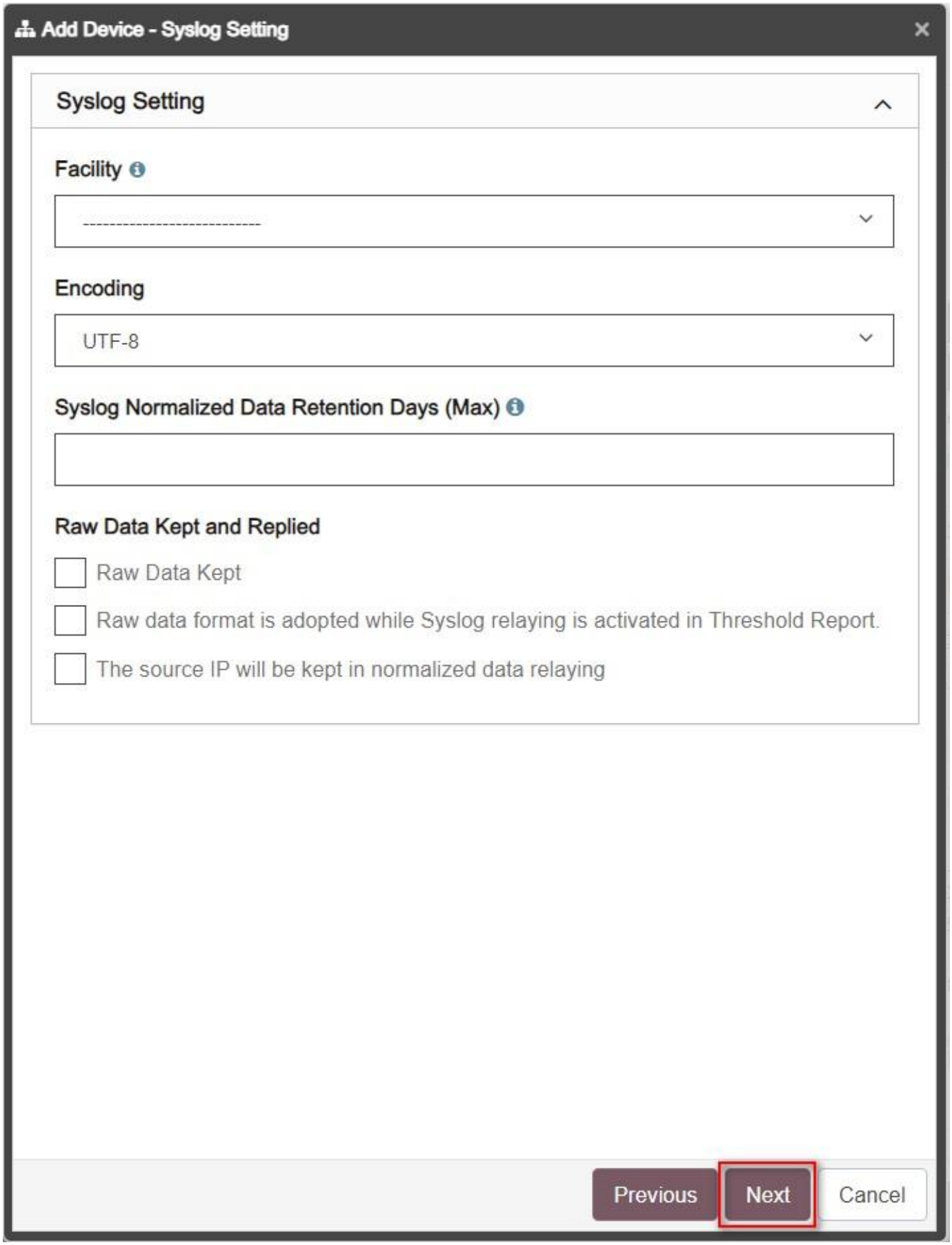
(3) Enter your device name and IP. Select “Windows or Windows (Raw)” for “Syslog Data Type.” -> And click “Next.”



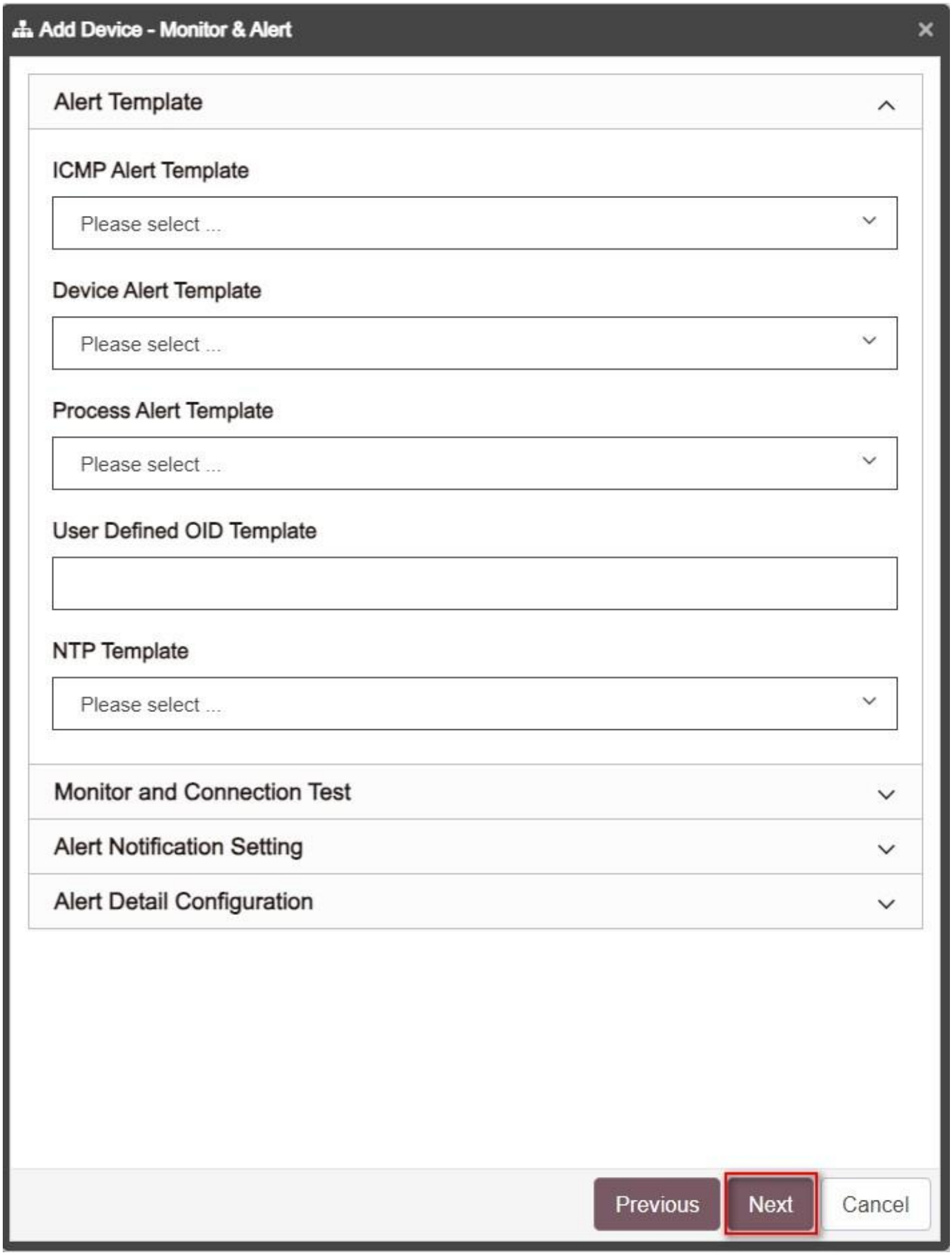
Click “Next.”



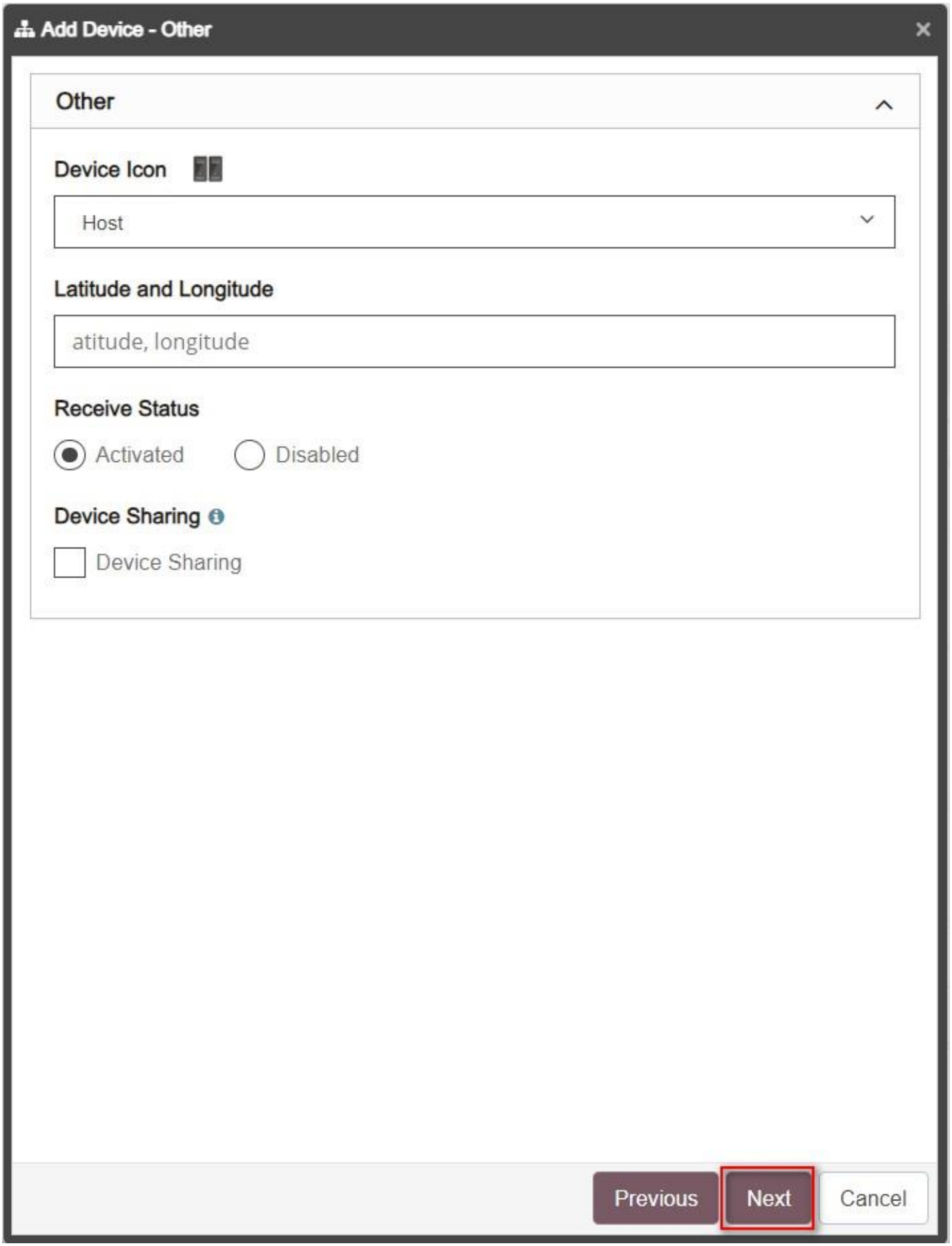
Click “Next.”



Click “Next.”



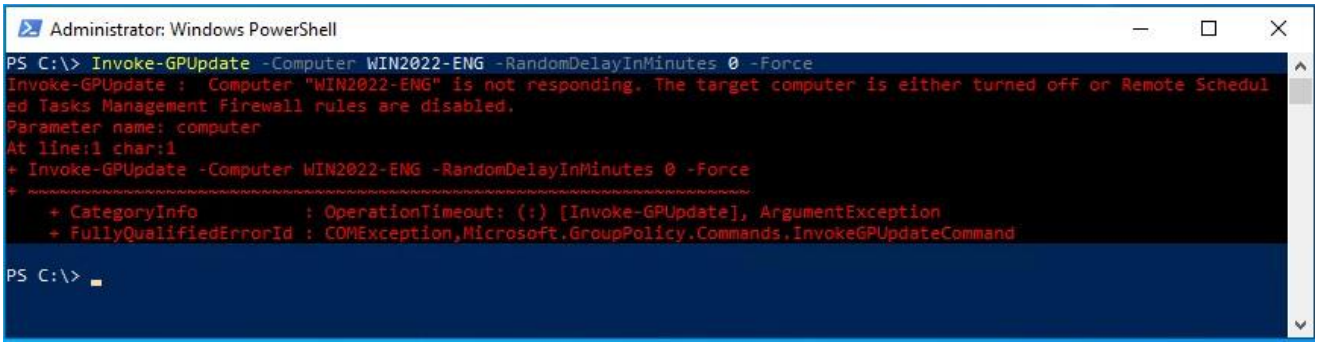
Click “Next.”



10. Troubleshooting

10.1 Invoke-GPUpdate Error

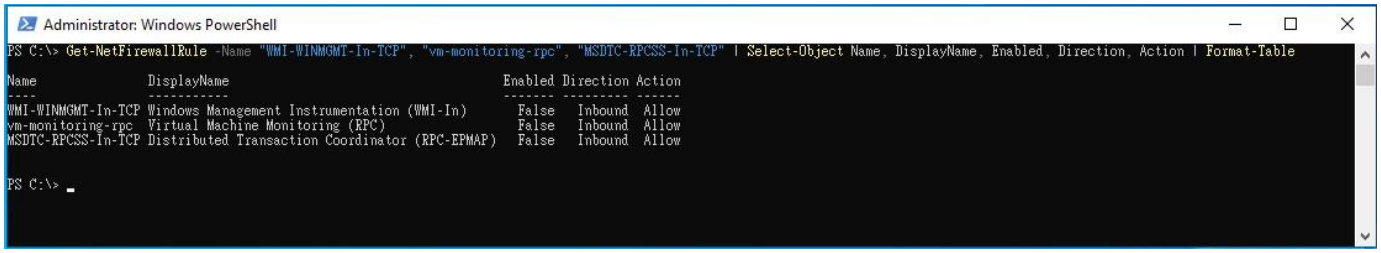
(1) On AD Domain server -> Run “Invoke-GPUpdate” to update Windows Server Group Policies, but an error message appears.



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

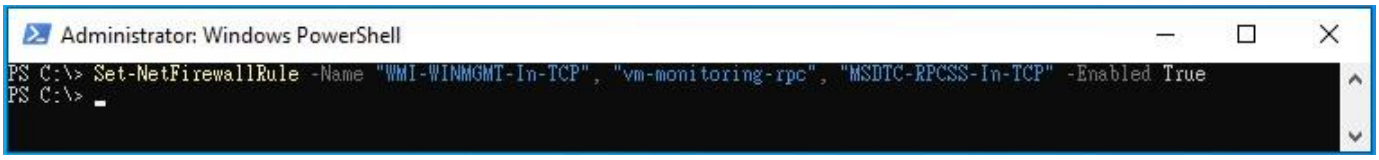
(3) Enter the command below to check the Windows Firewall rules for “WMI-WINMGMT-In-TCP, vm-monitoring-rpc, and MSDTC-RPCSS-In-TCP.”

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



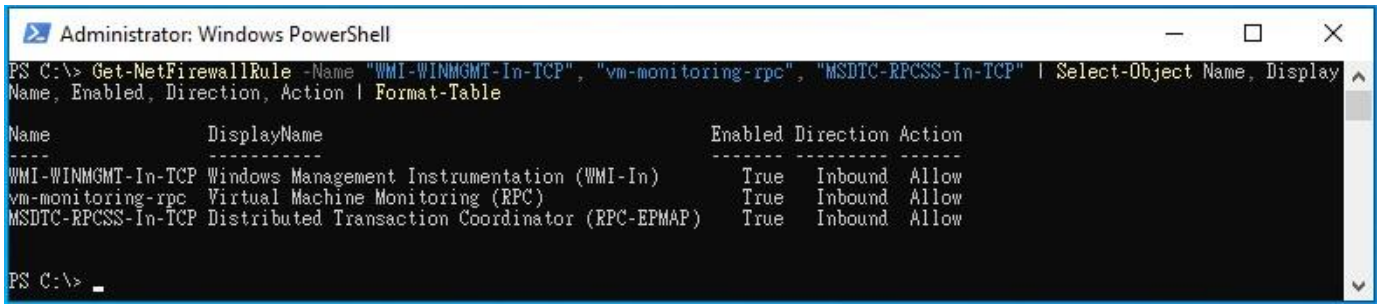
(4) Enter the command below to check the Windows Firewall rules for “WMI-WINMGMT-In-TCP, vm-monitoring-rpc, and MSDTC-RPCSS-In-TCP.

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



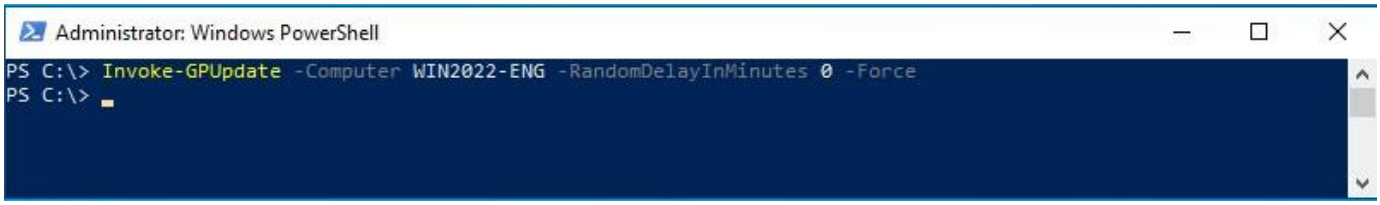
(5) Enter the command below to view the Windows Firewall rules for “WMI-WINMGMT-In-TCP, vm-monitoring-rpc, and MSDTC-RPCSS-In-TCP.”

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



(6) On the AD Domain server -> Enter the command below to update Windows Server Group Policies.

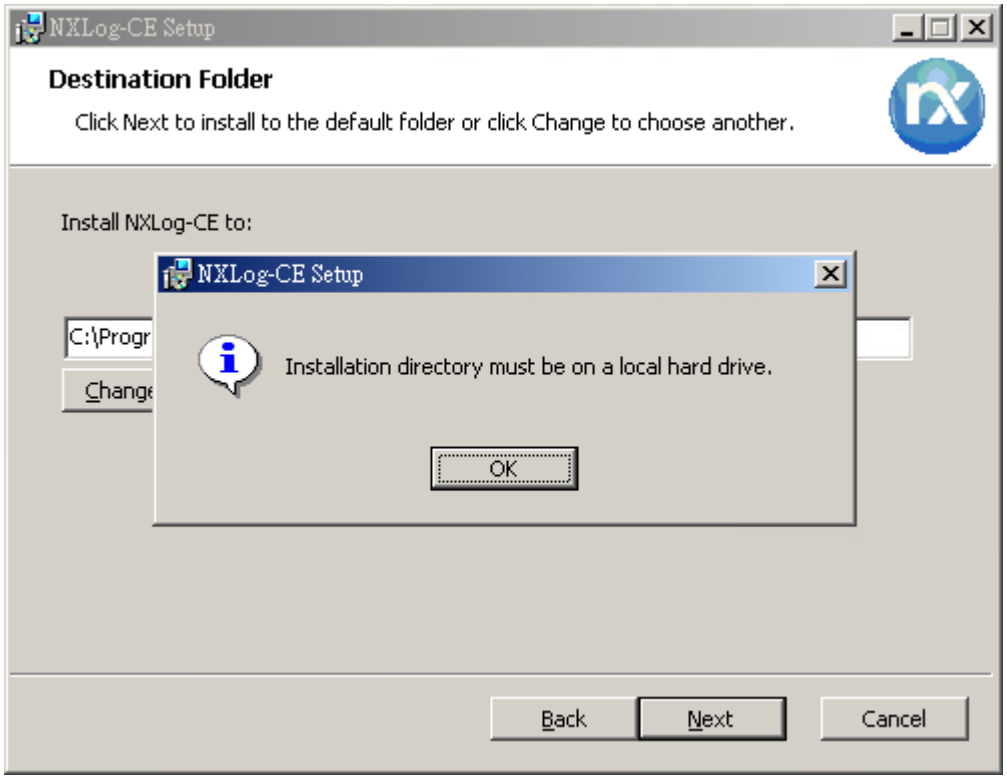
```
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
```



Please enter your Windows Server server name in the red text.

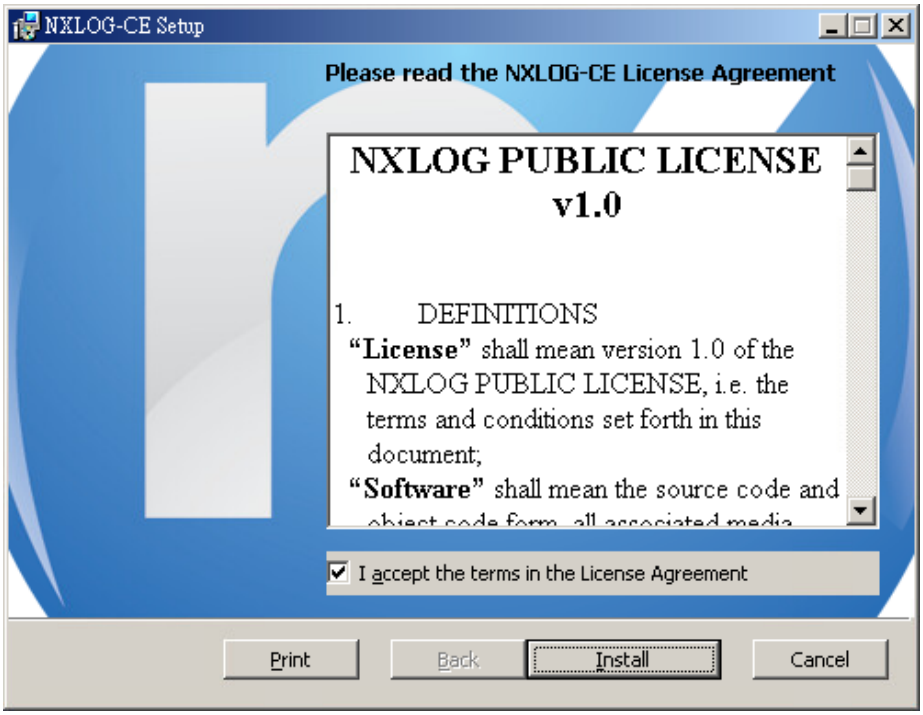
10.2 NXLog Installation Issues

(1) Installing NXLog (3.2.2329) and click “OK” after the system shows “Installation directory must be on a local hard drive.”



(2) To install a previous version of NXLog:

Click “nxlog-ce-3.2.2329.msi” -> Check “I accept the terms in the License Agreement” -> And click “Install” and then “Finish.”



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