

Partner

Manage Windows AD Server

Syslog

with NXLOG

V014

2024/08/21



Copyright Declaration

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

Registered Trademark

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

Contents

Preface	2	4.2 Workgroup.....	65
1. NXLog	3	4.2.1 Audit Policy Settings	65
1.1 Configure NXLOG in Windows Server AD	3	4.2.2 Event Log Settings.....	68
1.2 NXLog Configuration File Download.....	7	5. For Windows 2012	70
1.2.1 For Windows 2003 or Its Earlier Versions	7	5.1 Domain	70
1.2.1.1 Output Host Audit, Object Access, and Account Management Event Logs	7	5.1.1 Organizational Unit Setup	70
1.2.1.2 Output All Event Logs	8	5.1.2 Group Policy Settings.....	73
1.2.2 For Windows 2008 or Its Later Versions.....	9	5.2 Workgroup.....	79
1.2.2.1 Output Host Audit, Object Access, and Account Management Event Logs	9	5.2.1 Audit Policy Settings	79
1.2.2.2 Output All Event Logs for Applications, Security, and System	10	5.2.2 Event Log Settings.....	82
1.3 NXLog Configuration.....	11	6. For Windows 2016	84
1.3.1 For Windows 2003 or Its Earlier Versions	11	6.1 Domain	84
1.3.1.1 Output Host Audit, Object Access, and Account Management Event Logs	11	6.1.1 Organizational Unit Setup	84
1.3.1.2 Output All Event Logs	12	6.1.2 Group Policy Settings.....	87
1.3.2 For Windows 2008 or Its Later Versions.....	13	6.2 Workgroup.....	94
1.3.2.1 Output Host Audit, Object Access, and Account Management Event Logs	13	6.2.1 Audit Policy Settings	94
1.3.2.2 Output All Event Logs for Applications, Security, and System	15	6.2.2 Event Log Settings.....	98
1.4 NXLog Startup.....	16	7. For Windows 2019	101
1.4.1 For Windows 2003 or Its Earlier Versions	16	7.1 Domain	101
1.4.2 For Windows 2008 or Its Later Versions.....	19	7.1.1 Organizational Unit Setup	101
2. For Windows 2000	22	7.1.2 Group Policy Settings.....	105
2.1 Domain	22	7.2 Workgroup.....	112
2.1.1 Organizational Unit Setup	22	7.2.1 Audit Policy Settings	112
2.1.2 Group Policy Settings.....	25	7.2.2 Event Log Settings.....	116
2.2 Workgroup.....	32	8. For Windows 2022	118
2.2.1 Audit Policy Settings	32	8.1 Domain	118
2.2.2 Event Log Settings	36	8.1.1 Organizational Unit Setup	118
3. For Windows 2003	39	8.1.2 Group Policy Settings.....	121
3.1 Domain	39	8.2 Workgroup.....	128
3.1.1 Organizational Unit Configuration.....	39	8.2.1 Audit Policy Settings	128
3.1.2 Group Policy Settings.....	42	8.2.2 Event Log Settings.....	132
3.2 Workgroup.....	48	9. N-Reporter	135
3.2.1 Audit Policy Settings	48	10. Troubleshooting	142
3.2.2 Event Log Settings	52	10.1 Invoke-GPUdate Error	142
4. For Windows 2008	55	10.2 NXLog Installation Issues	144
4.1 Domain	55	Contact	145
4.1.1 Organizational Unit Setup	55		
4.1.2 Group Policy Settings.....	58		

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>

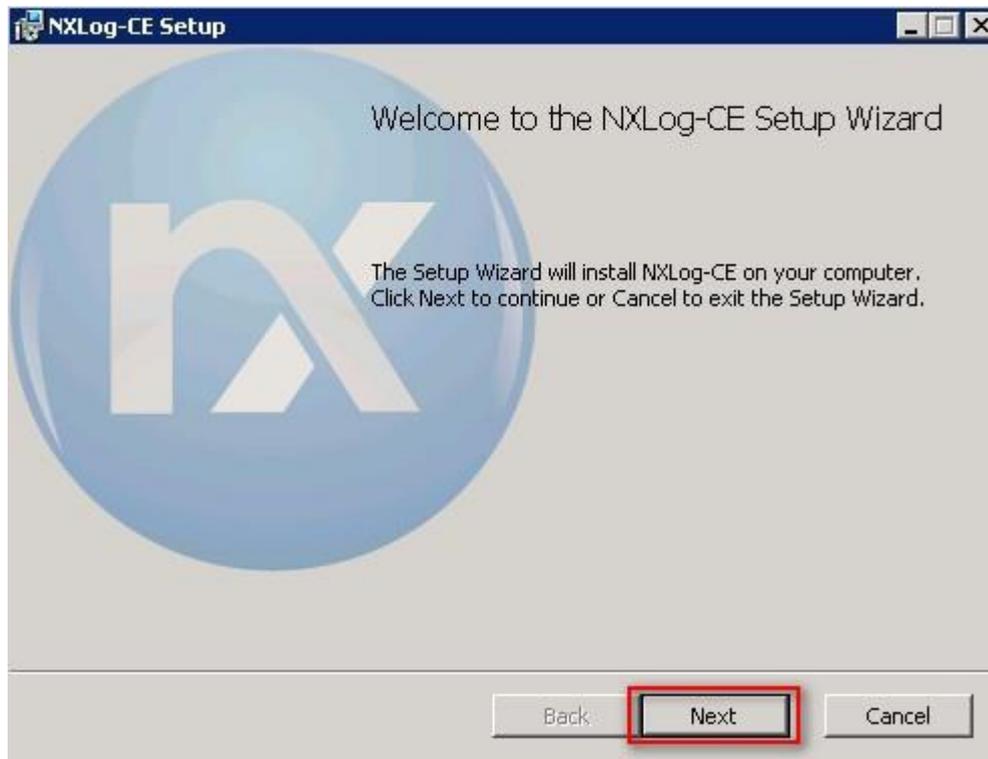
Download the latest nxlog-ce-x.x.xxxx.msi; here, it's nxlog-ce-3.2.2329.msi.



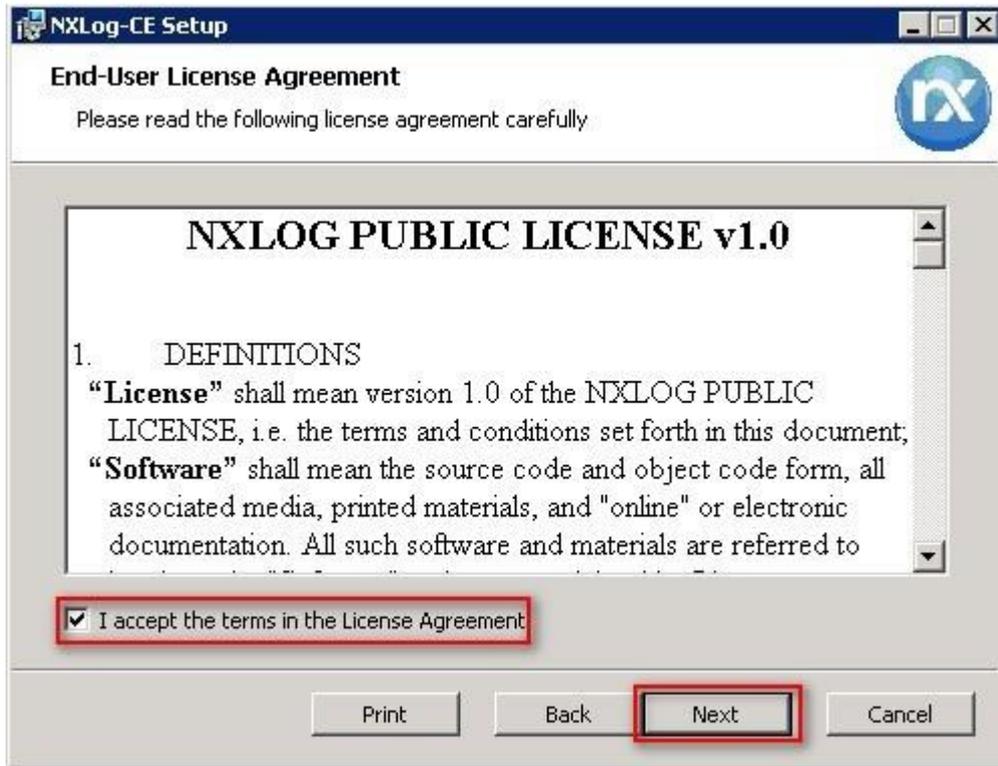
(2) Install NXLOG

<2.1> Windows 2008 or later operating systems

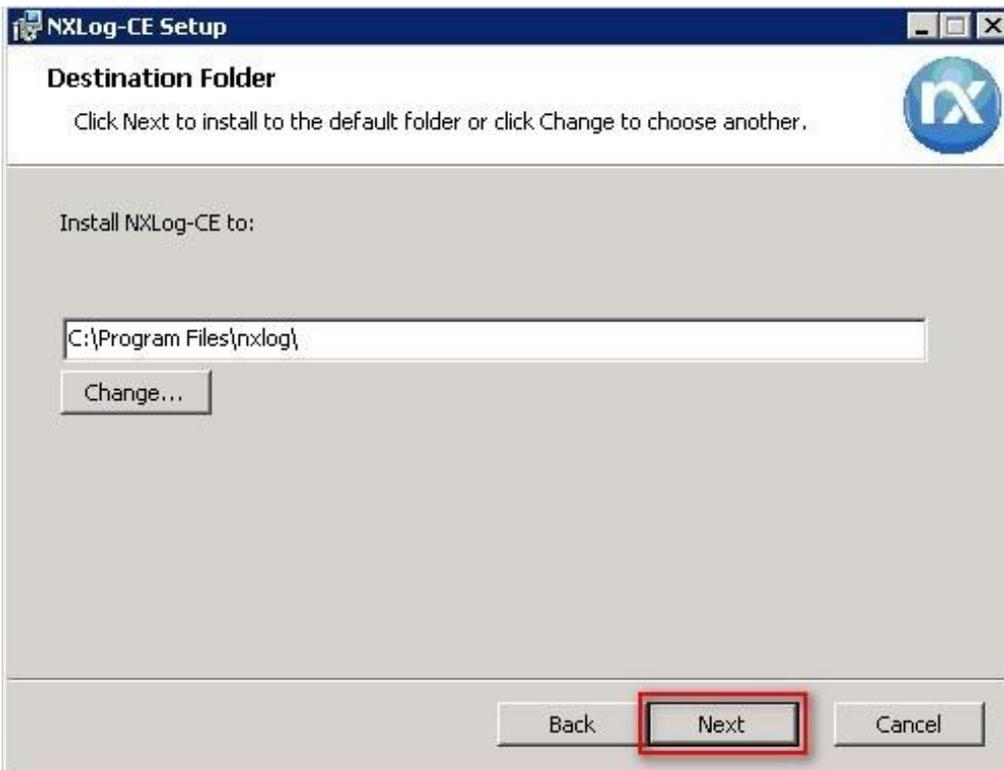
Click "nxlog-ce-3.2.2329.msi → Next."



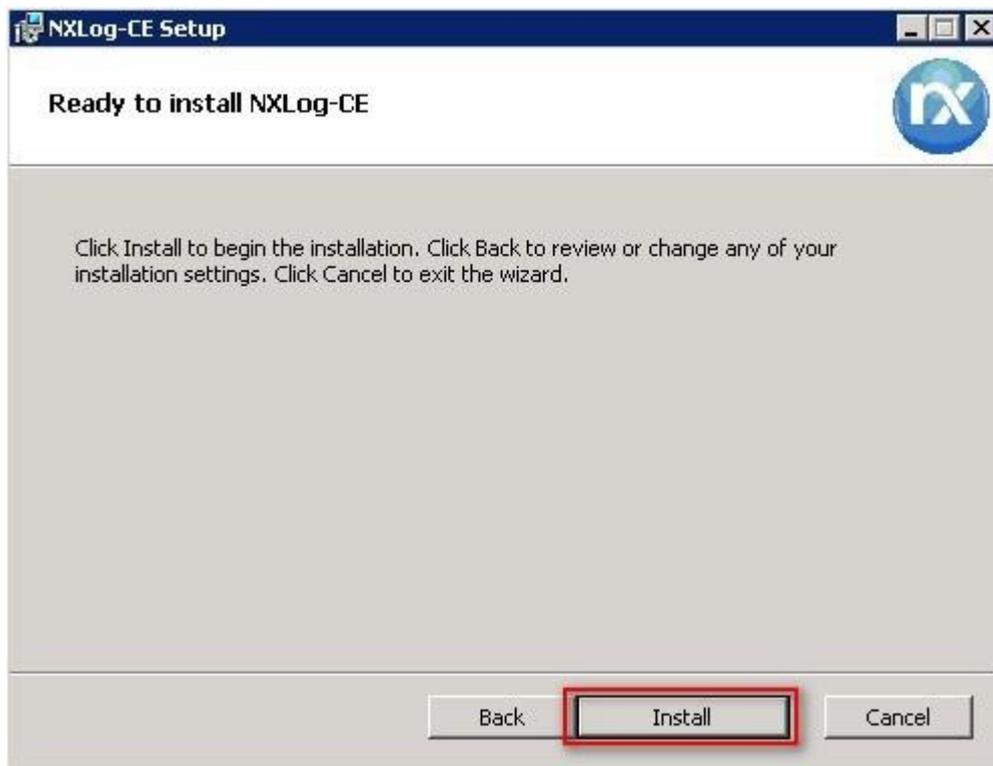
Check "I accept the terms in the License Agreement" and click "Next."



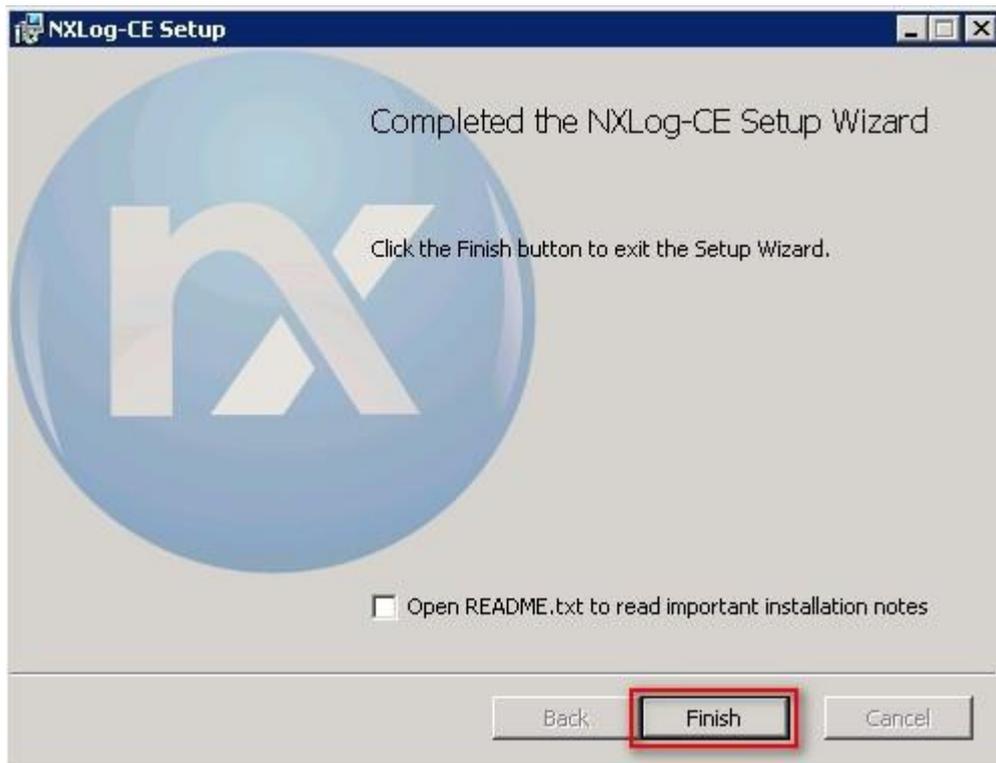
Click "Next."



Click "Install."

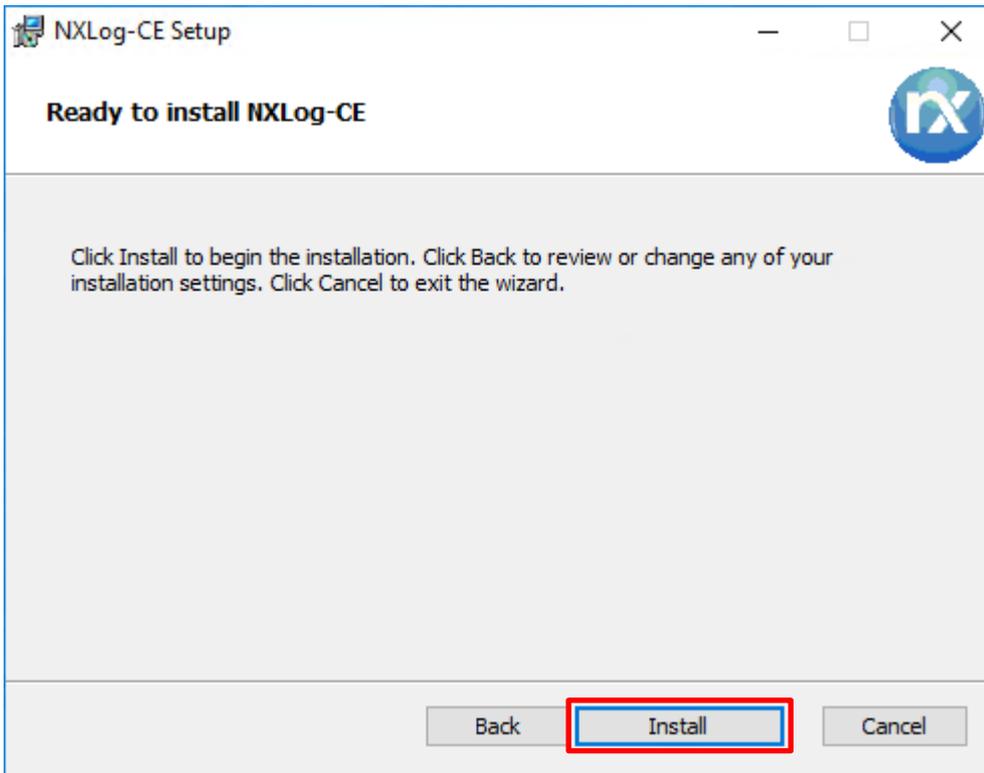


Click "Finish."



<2.2> Windows 2003

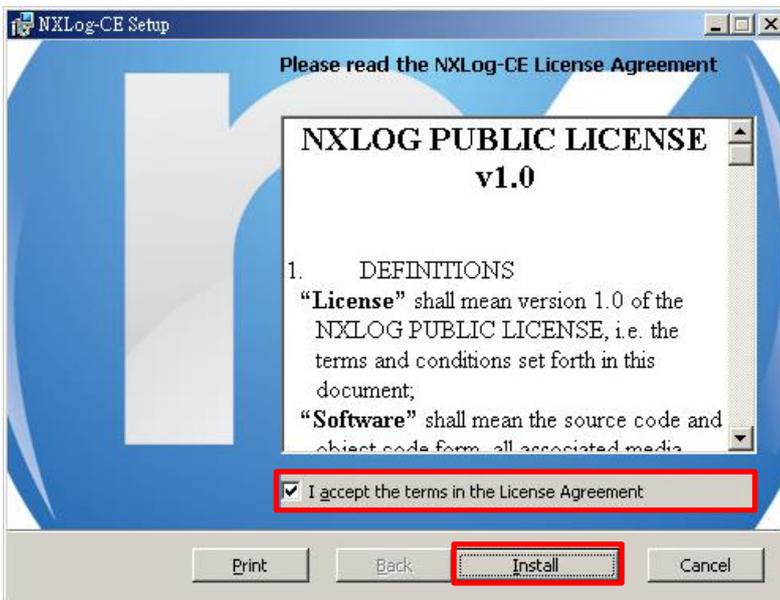
Click “nxlog-ce-3.2.2329.msi→Install→Finish.”



<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.”

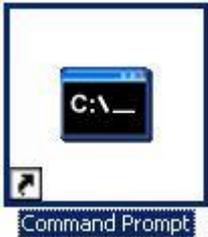


1.2 NXLog Configuration File Download

1.2.1 For Windows 2003 or Its Earlier Versions

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

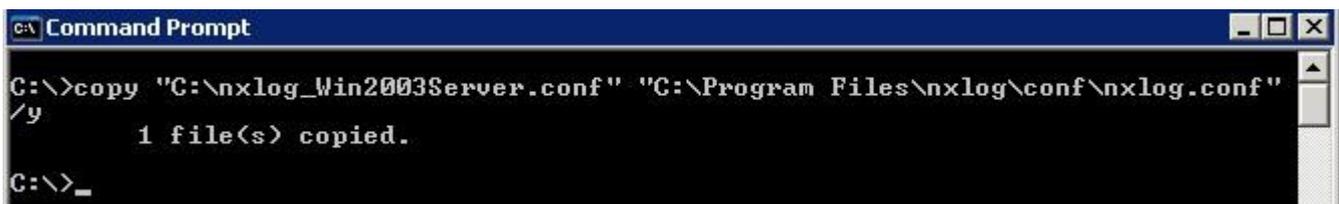
(1) Click "Command Prompt."



(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
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command prompt shows the following text:

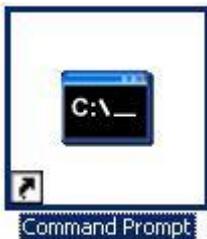
```
C:\>copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y
1 file(s) copied.
C:\>_
```

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

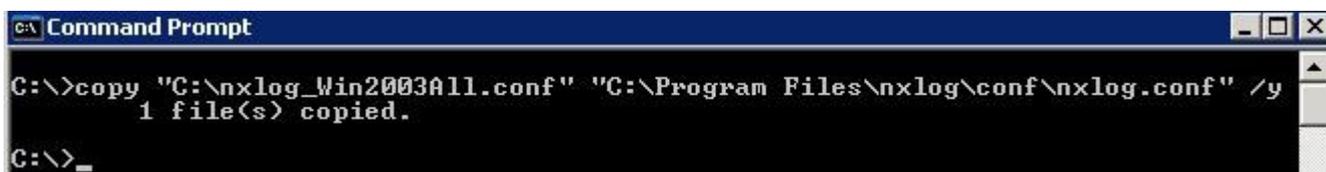
(1) Click "Command Prompt."



(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'
```

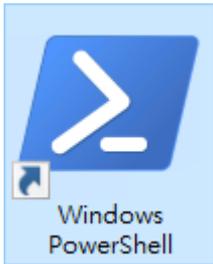


If the operating system is 64-bit, modify the following setting in red part: 'C:\Program Files (x86)\nxlog\conf\nxlog.conf'

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
```

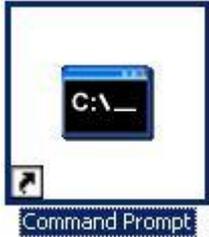
If the operating system is 64-bit, please change the setting to the following:

```
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"
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command prompt shows the following text:

```
C:\>net start nxlog  
The nxlog service is starting.  
The nxlog service was started successfully.  
  
C:\>type "C:\Program Files\nxlog\data\nxlog.log"  
2024-04-12 15:29:02 WARNING no functional input modules!  
2024-04-12 15:29:02 WARNING no routes defined!  
2024-04-12 15:29:02 INFO nxlog-ce-3.2.2329 started  
2024-04-12 16:13:50 WARNING stopping nxlog service  
2024-04-12 16:13:50 WARNING nxlog-ce received a termination request signal, exiting...  
2024-04-12 16:13:57 INFO nxlog-ce-3.2.2329 started  
C:\>_
```

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

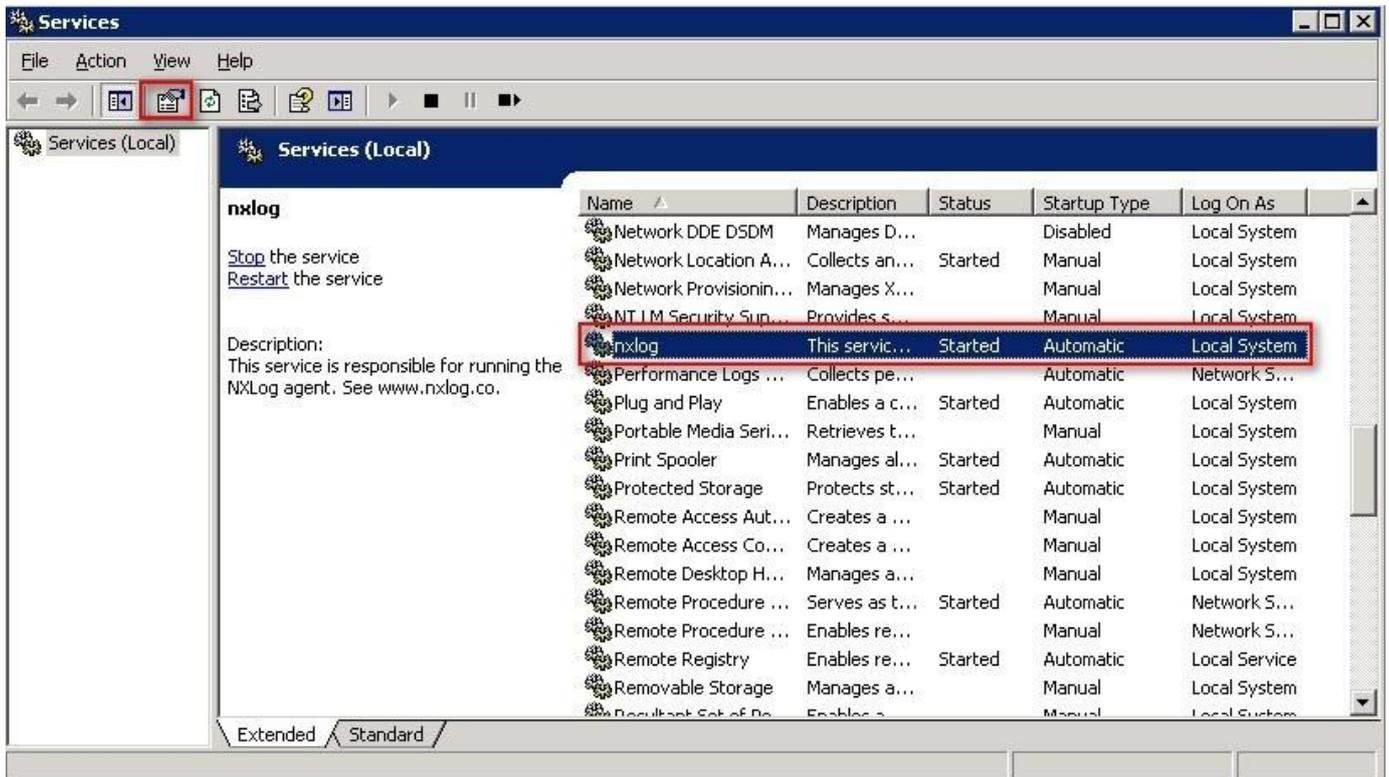
```
C:\> Services.msc
```

A screenshot of a Windows Command Prompt window. The title bar reads 'C:\ Command Prompt'. The command prompt shows the following text:

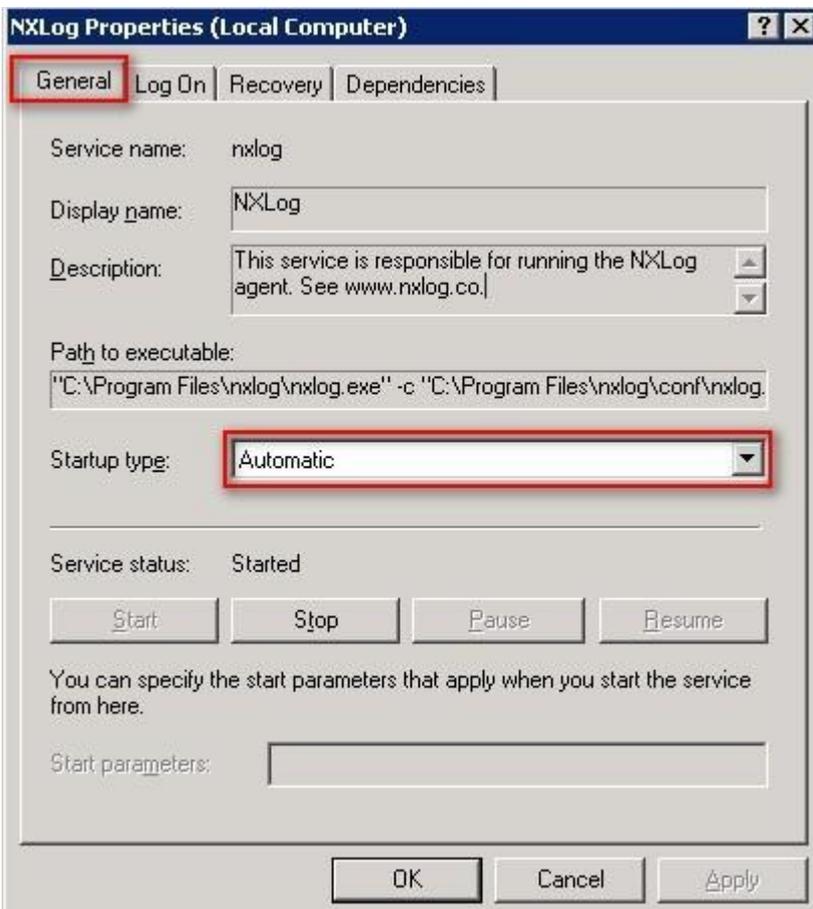
```
C:\>Services.msc  
C:\>_
```

(4) Open NXLog Service

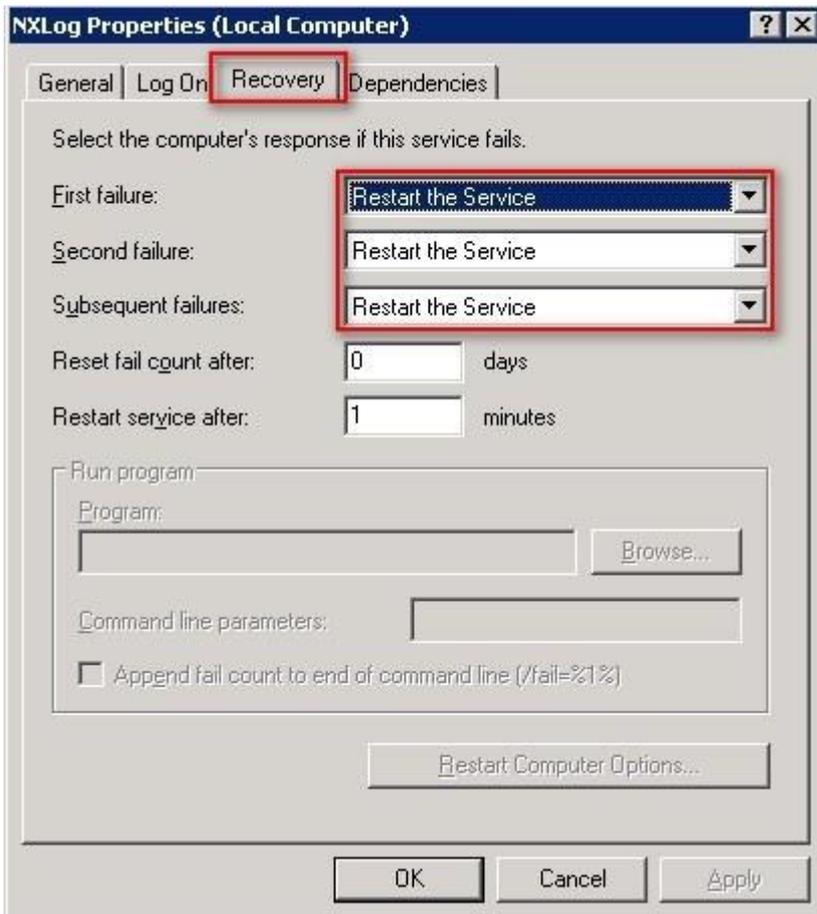
Please select "nxlog" and click  .



(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'
```

A screenshot of an Administrator Windows PowerShell terminal window. The terminal shows the execution of three commands: 'Restart-Service -Name nxlog', 'Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType', and 'Get-Content 'C:\Program Files\nxlog\data\nxlog.log''. The output of the second command is a table with columns 'Name', 'Status', and 'StartType'. The 'nxlog' service is shown as 'Running'. The output of the third command shows log entries with timestamps and messages such as 'WARNING no functional input modules!', 'WARNING no routes defined!', 'INFO nxlog-ce-3.2.2329 started', 'WARNING stopping nxlog service', 'WARNING nxlog-ce received a termination request signal. exiting...', and 'INFO nxlog-ce-3.2.2329 started'.

Name	Status	StartType
nxlog	Running	

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

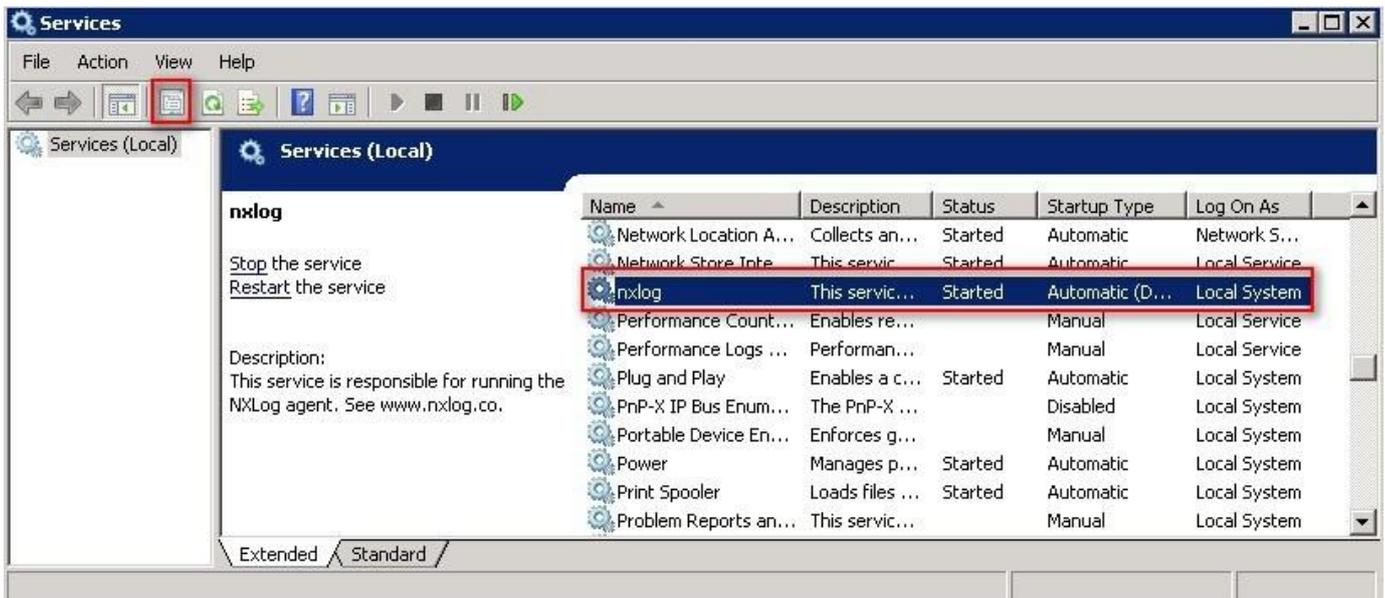
```
PS C:\> Services.msc
```

A screenshot of an Administrator Windows PowerShell terminal window. The terminal shows the execution of the command 'Services.msc'.

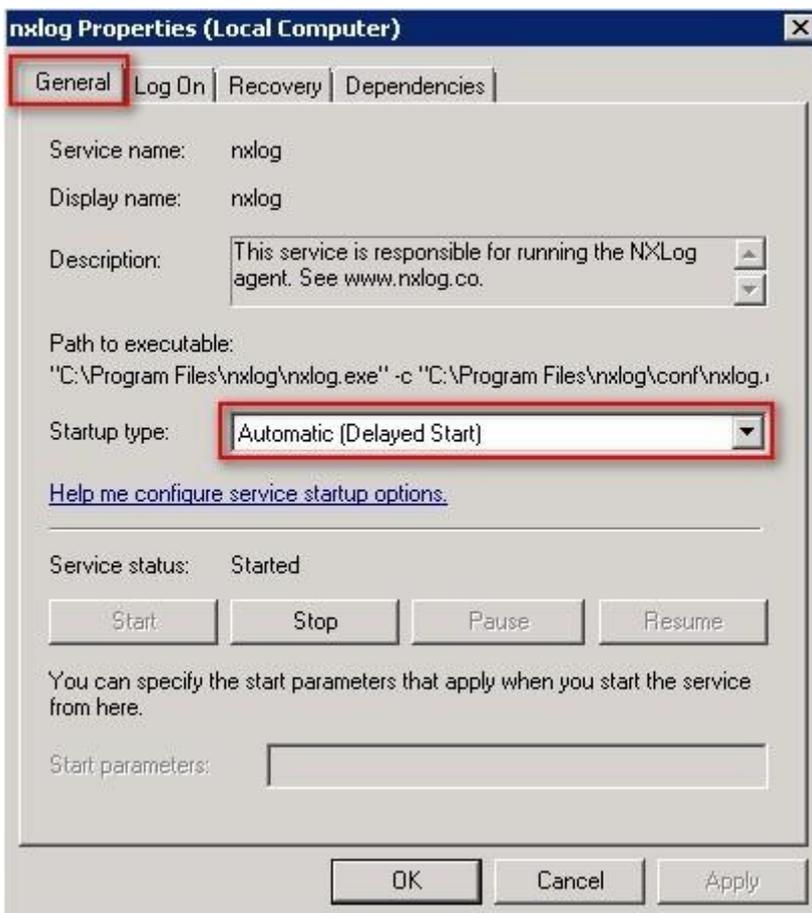
```
PS C:\> Services.msc
PS C:\>
```

(4) Open NXLog Service

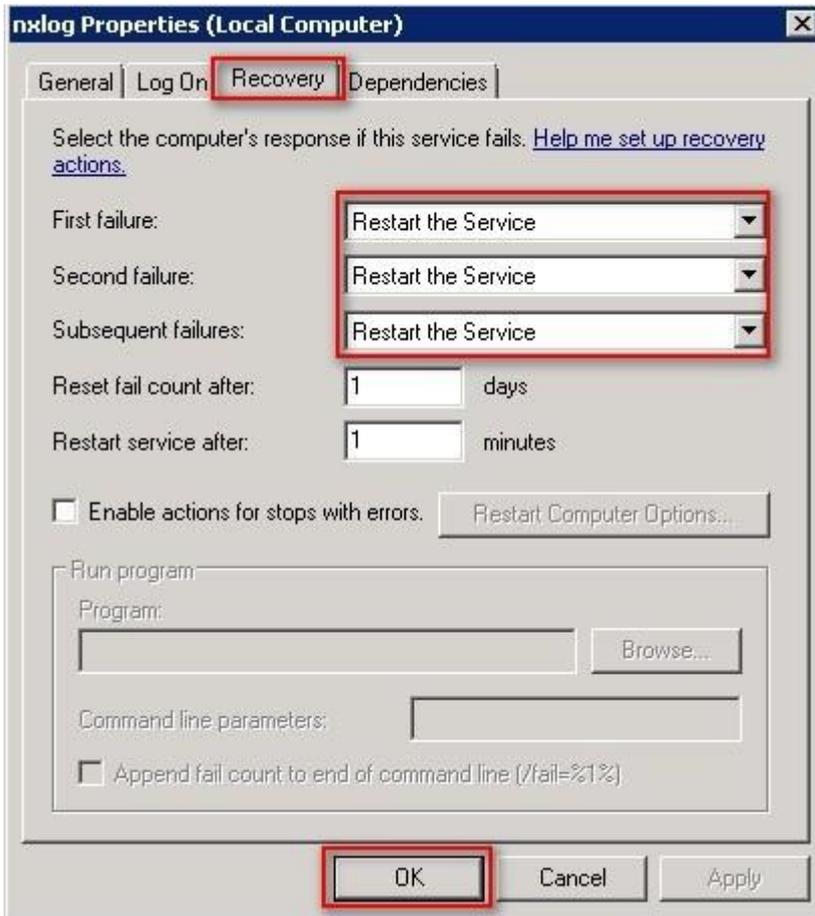
Please select “nxlog” and click .



(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

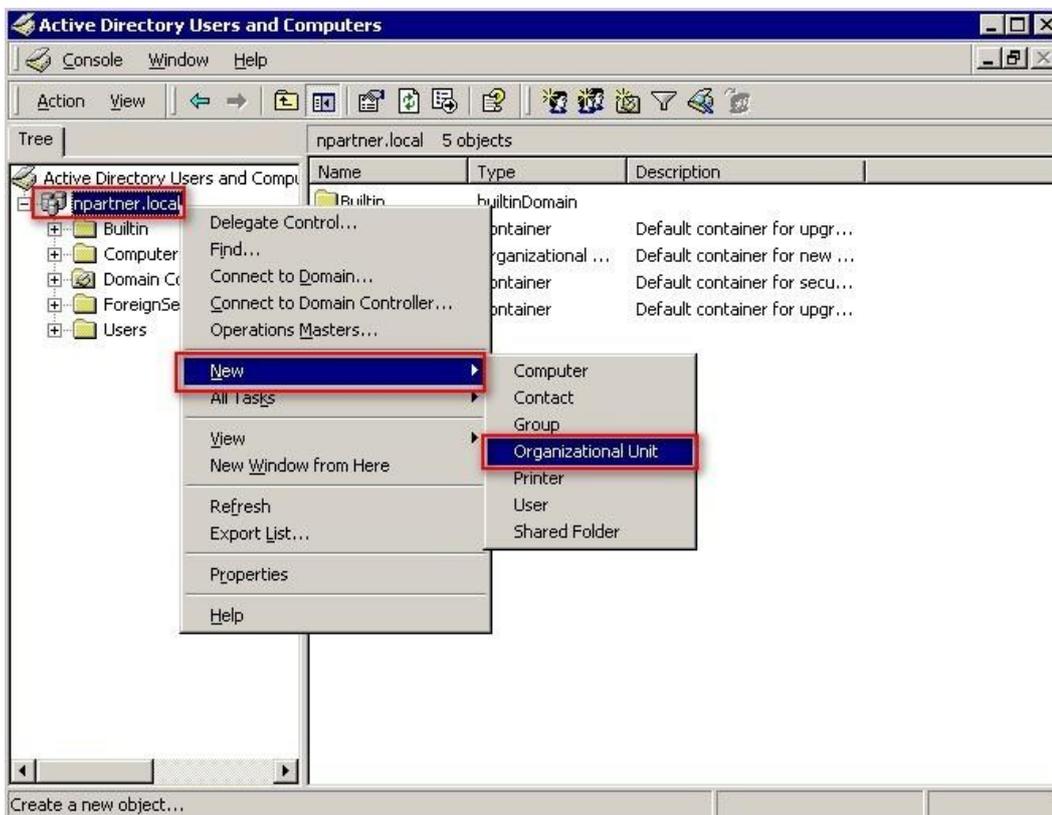
2.1.1 Organizational Unit Setup

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



(2) Add Your Organizational Unit

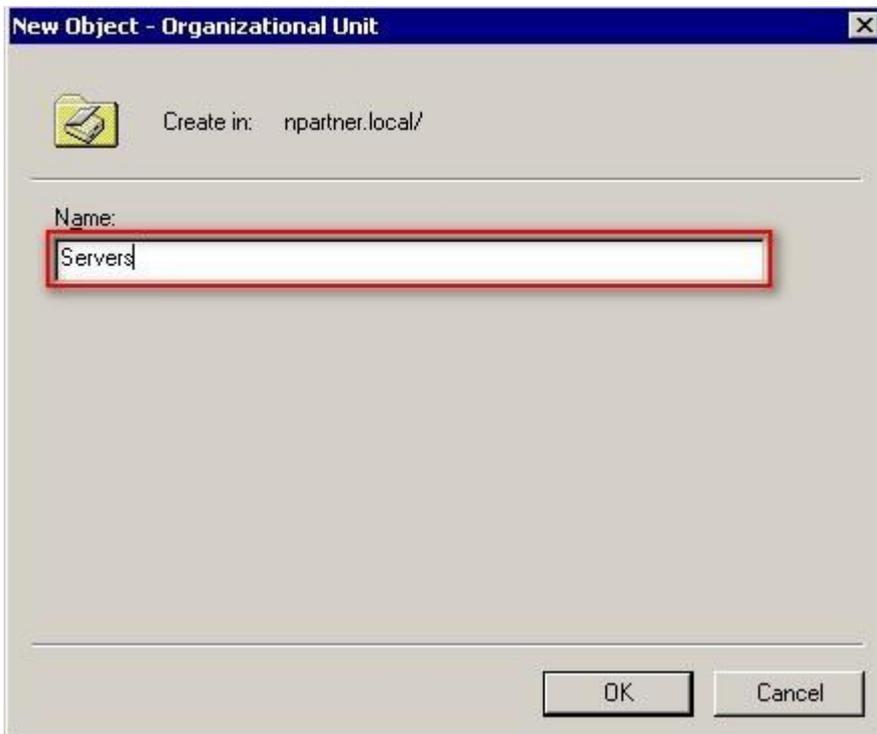
Right-click on your “Domain Name,” (in this example, it is “npartner.local”), select “New” and click “Organizational Unit.”



(3) Name Your Organizational Unit

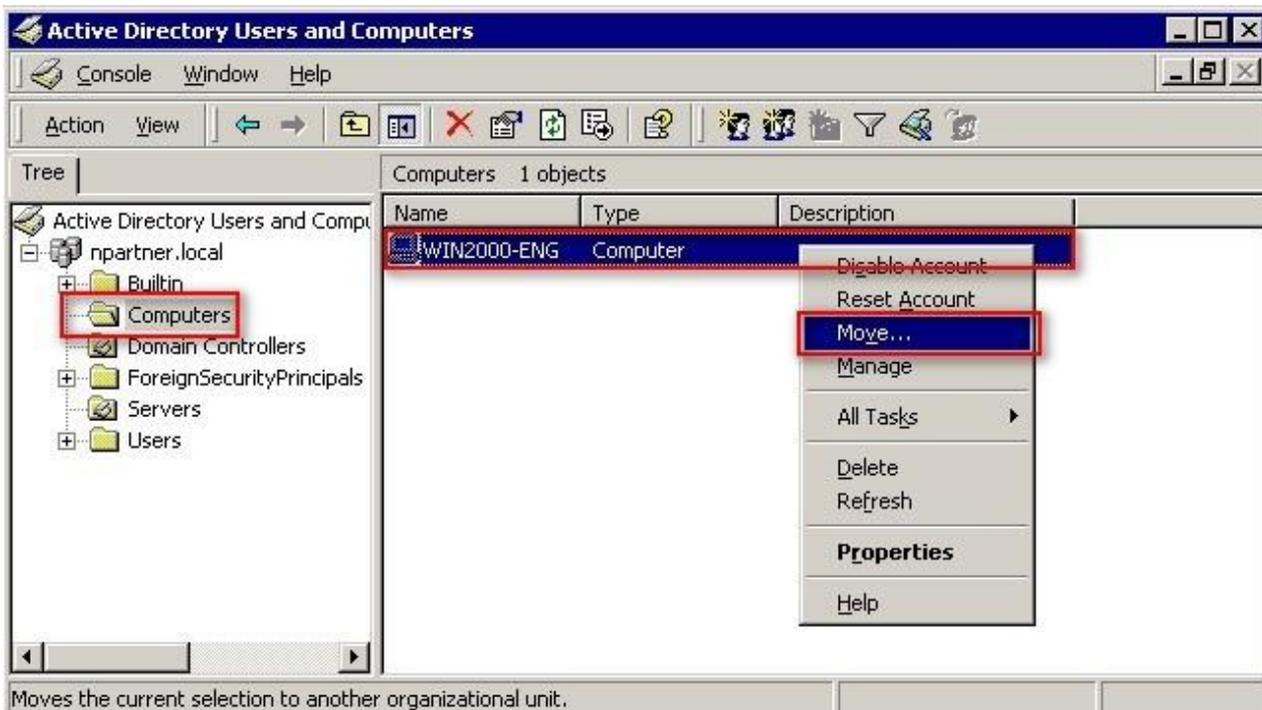
Enter your "Organizational Unit Name," (In this example, it is "Servers.")

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



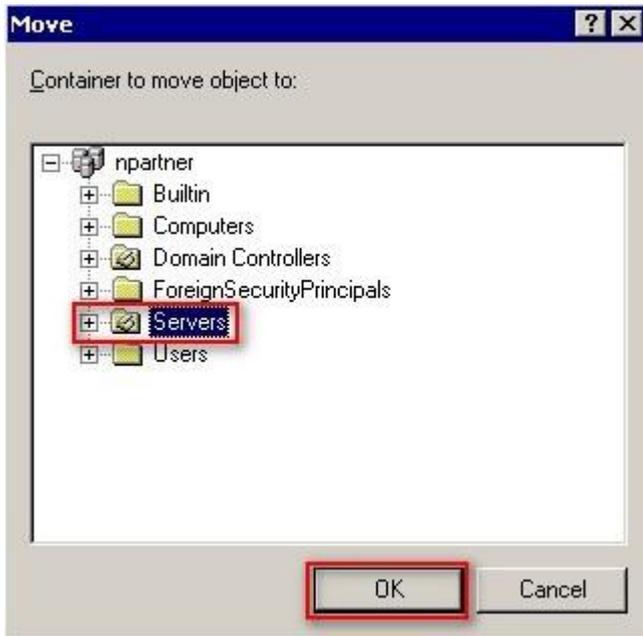
(4) Move Your Server to New Organizational Unit

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."



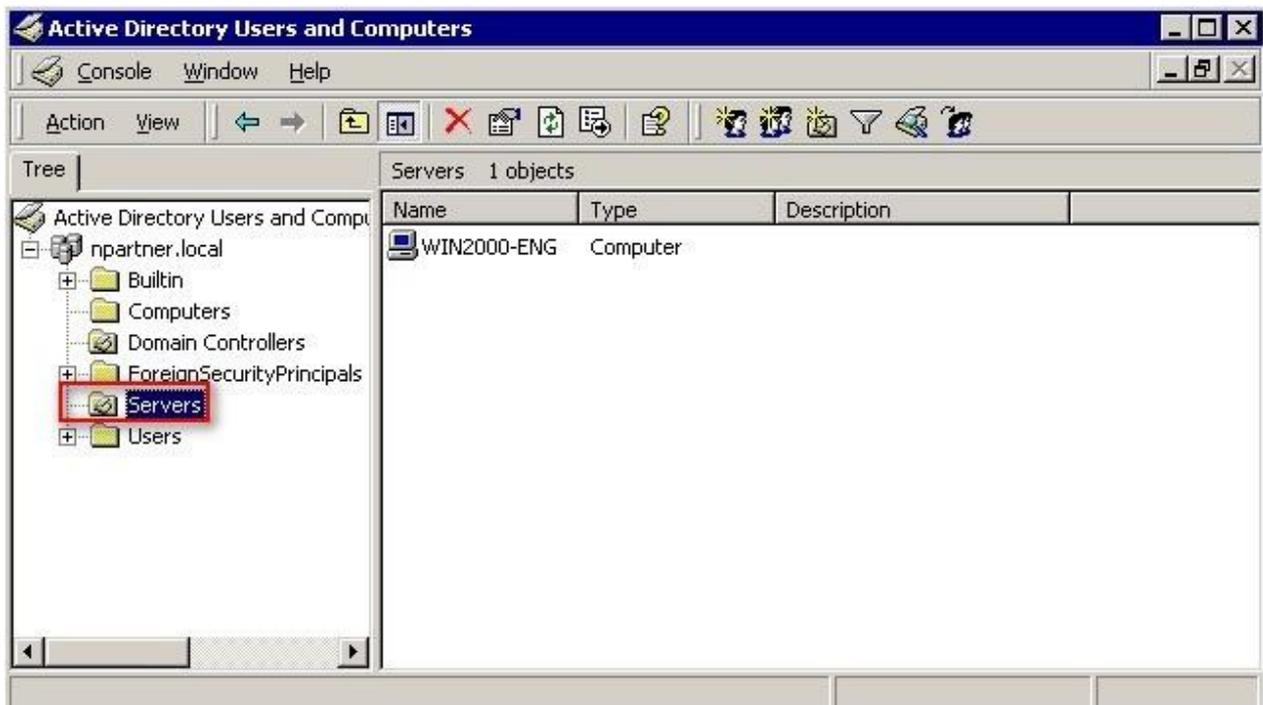
(5) Select Your Organizational Unit

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.

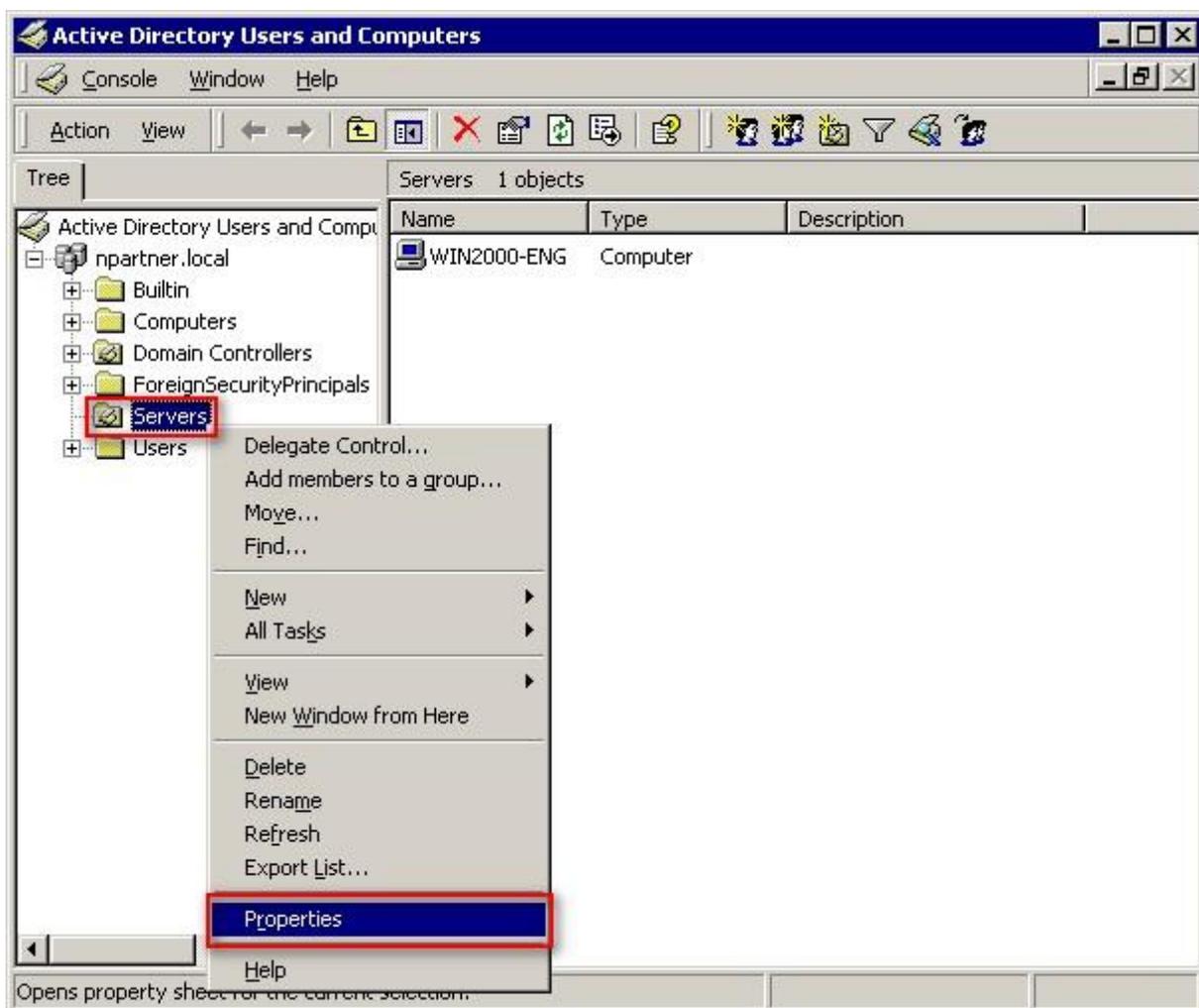


2.1.2 Group Policy Settings

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

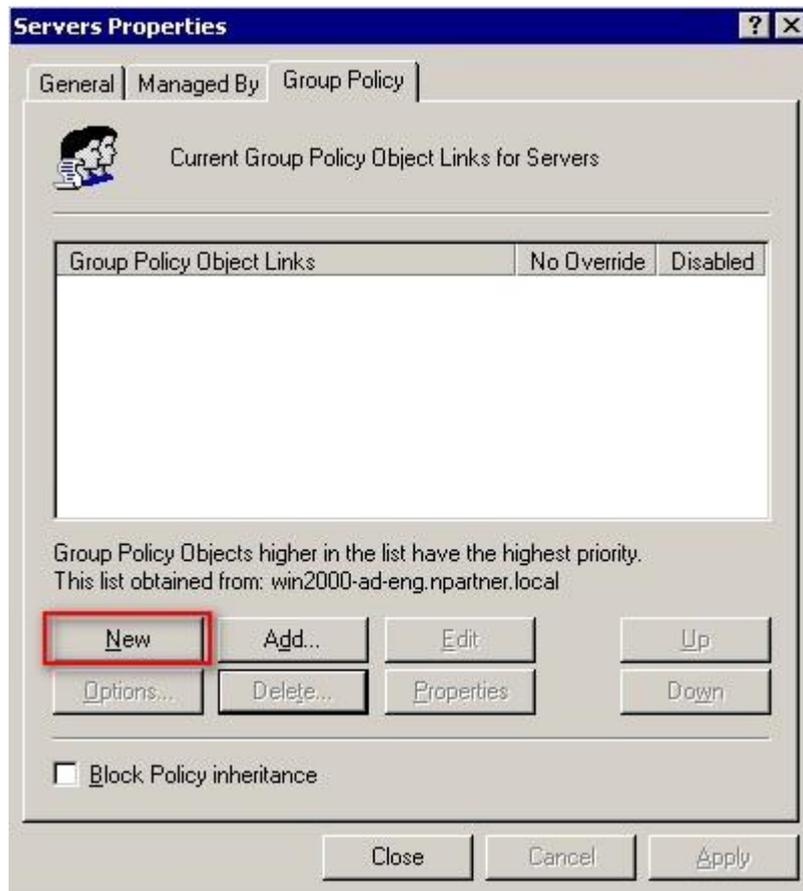


(2) Select your organizational unit (the example here is “Servers”) and right-click on “Properties.”



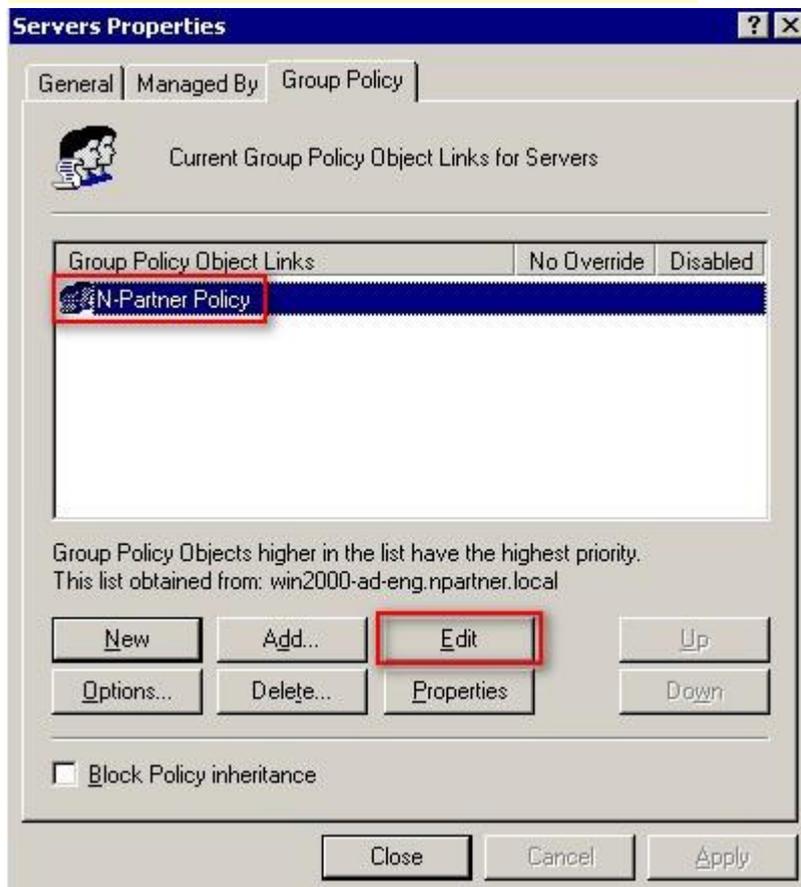
(3) Enter Your Group Policy Object Name

Click on the "Group Policy" page and click "New."



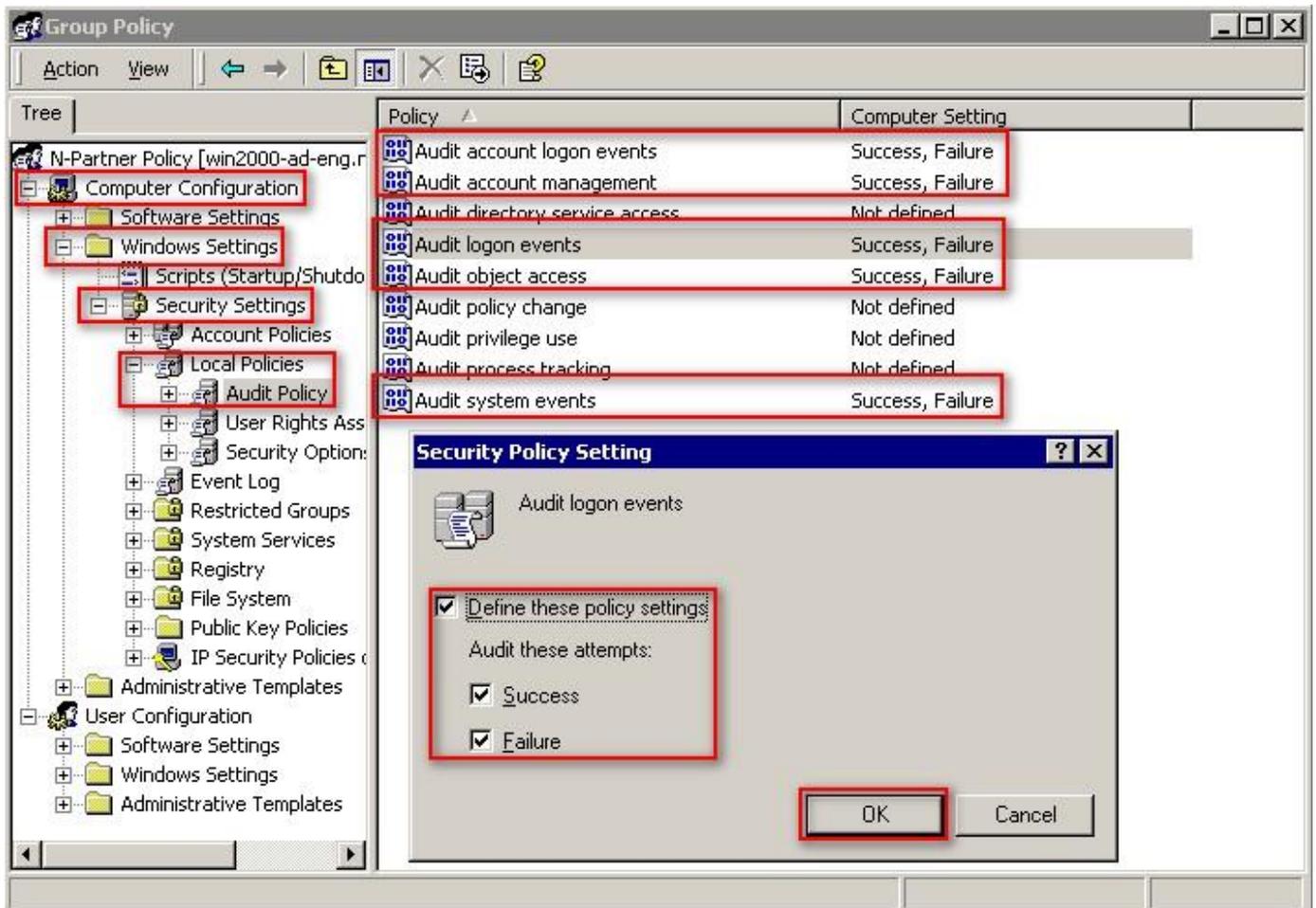
(4) Name Your Group Policy Object

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.”



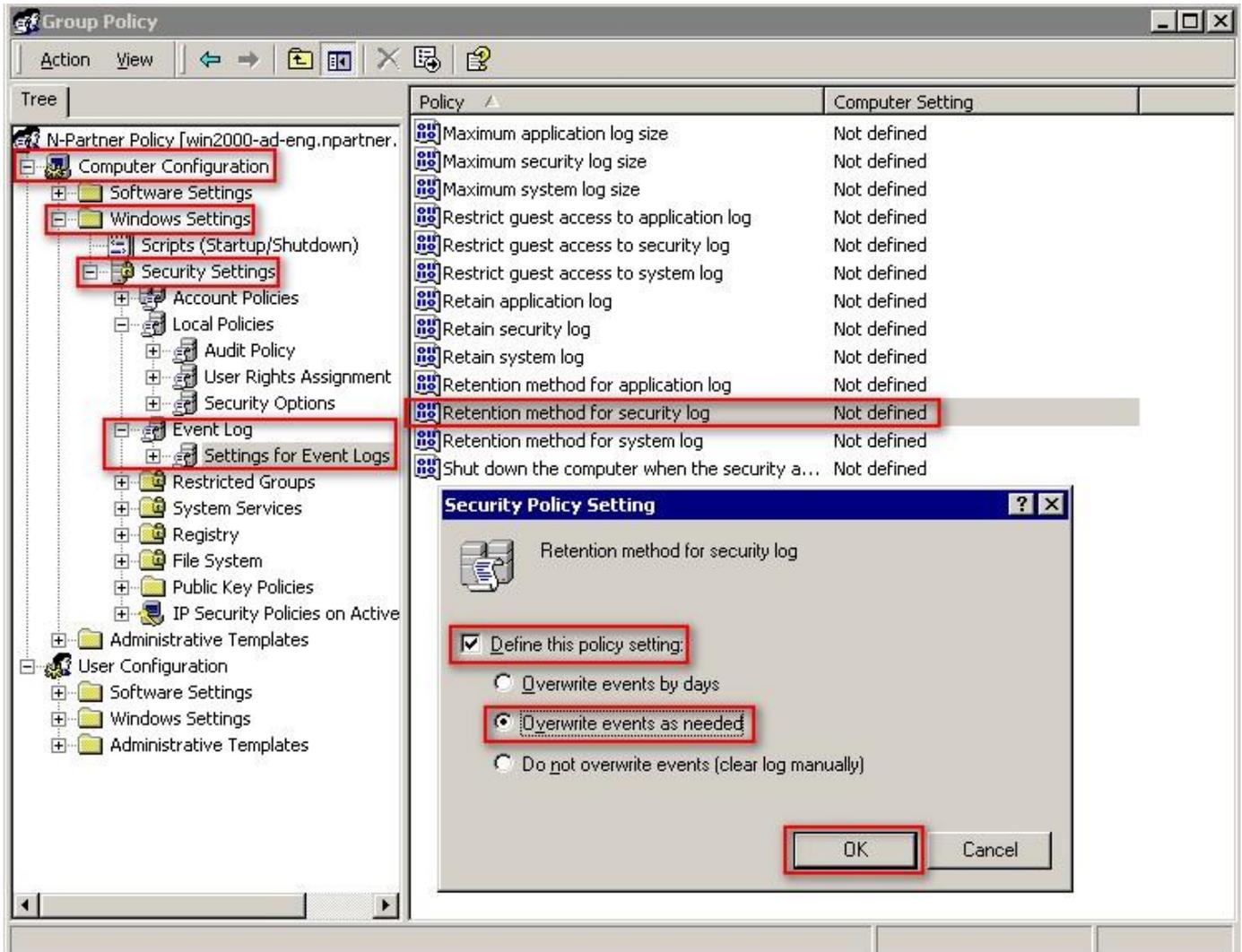
(5) Local Group Policies: Audit Policy

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

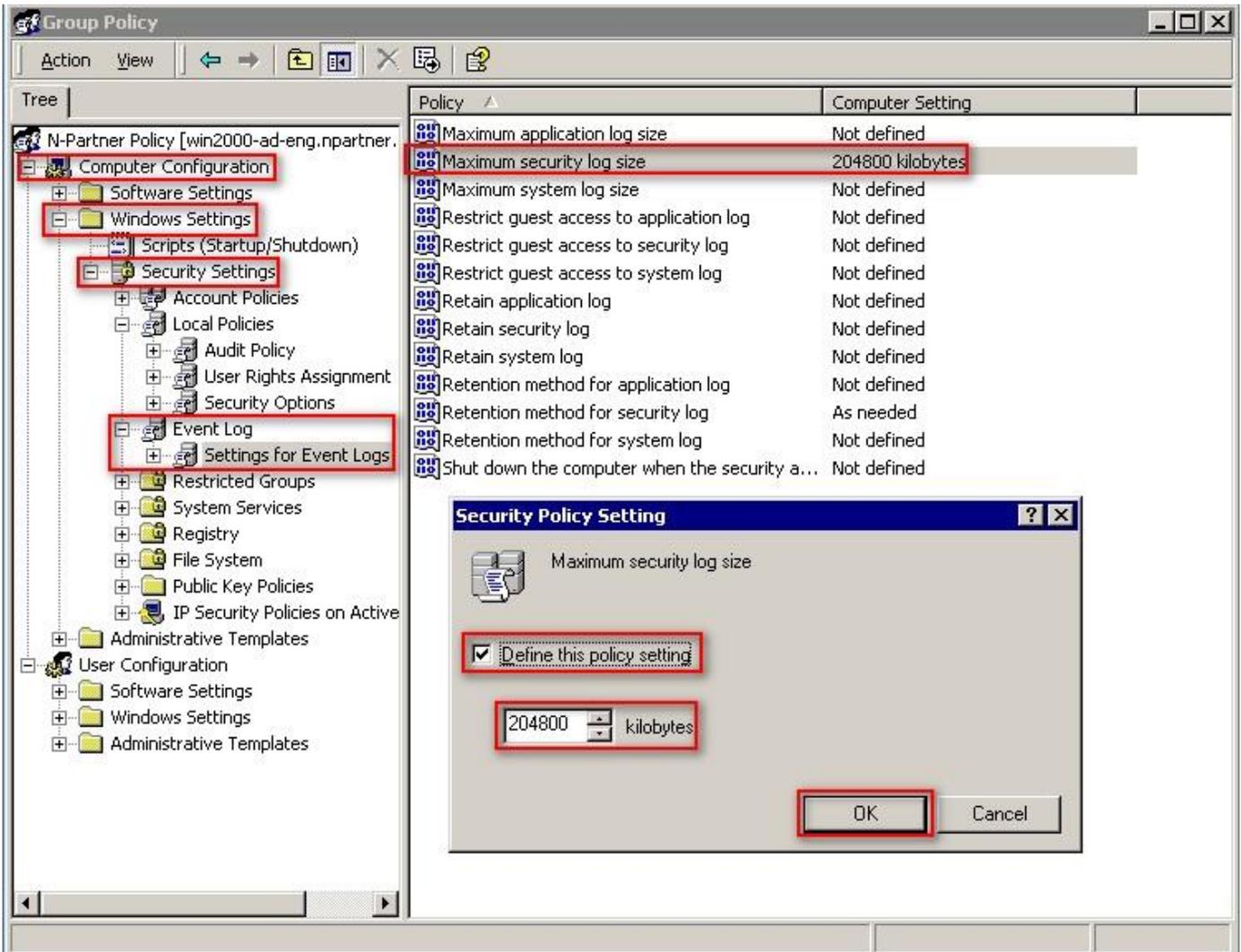
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Event Log” -> “Settings for Event Log Settings” -> Click on “Retention method for security log” -> And check “Define this policy setting”: -> Select “Overwrite events as needed” -> Click “OK.”



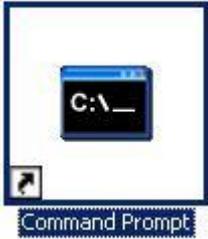
(7) Event Logs: Maximum Size of Security Log

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
```

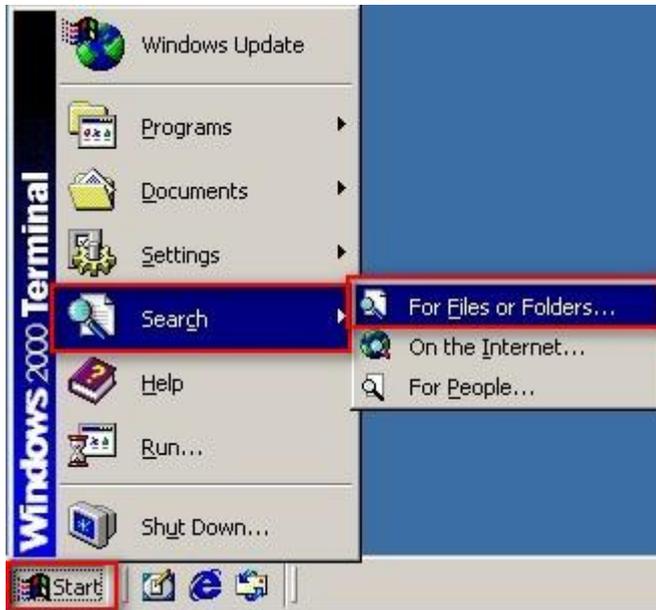


2.2 Workgroup

2.2.1 Audit Policy Settings

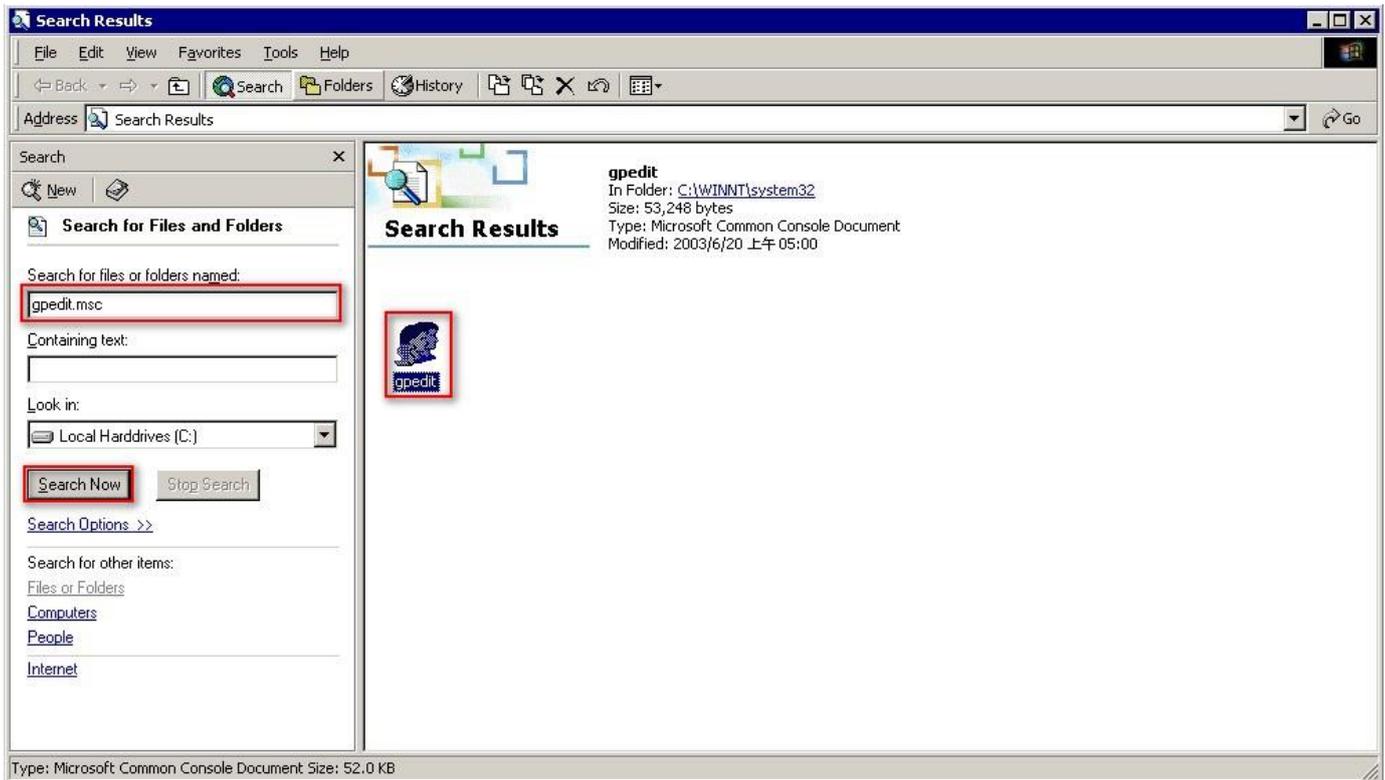
(1) Search

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.”

The screenshot shows the Group Policy console with the following table of settings:

Policy	Local Setting	Effective Setting
Audit account logon events	Success, Failure	No auditing
Audit account management	Success, Failure	No auditing
Audit directory service access	No auditing	No auditing
Audit logon events	Success, Failure	No auditing
Audit object access	Success, Failure	No auditing
Audit policy change	No auditing	No auditing
Audit privilege use	No auditing	No auditing
Audit process tracking	No auditing	No auditing
Audit system events	Success, Failure	No auditing

The dialog box titled "Local Security Policy Setting" for "Audit logon events" shows the following configuration:

- Effective policy setting: No auditing
- Local policy setting:
 - Audit these attempts:
 - Success
 - Failure

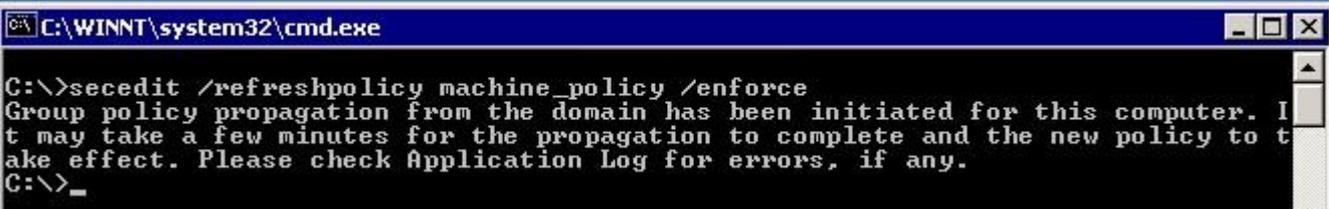
Buttons for "OK" and "Cancel" are visible at the bottom of the dialog box.

(4) Open “Command Prompt.”



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

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



```
C:\WINNT\system32\cmd.exe
C:\>secedit /refreshpolicy machine_policy /enforce
Group policy propagation from the domain has been initiated for this computer. I
t may take a few minutes for the propagation to complete and the new policy to t
ake effect. Please check Application Log for errors, if any.
C:\>_
```

2.2.2 Event Log Settings

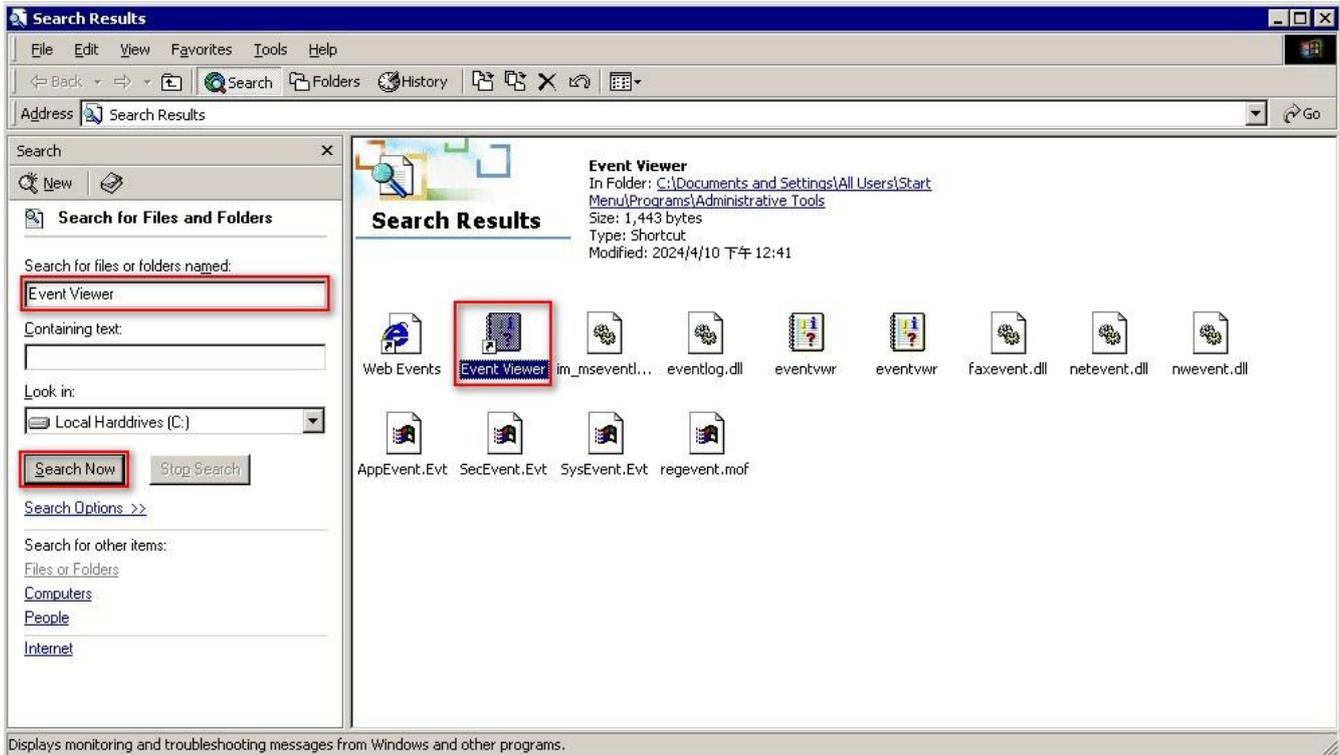
(1) Open "Search"

Click on "Start" -> "Search" -> "For Files or Folders."



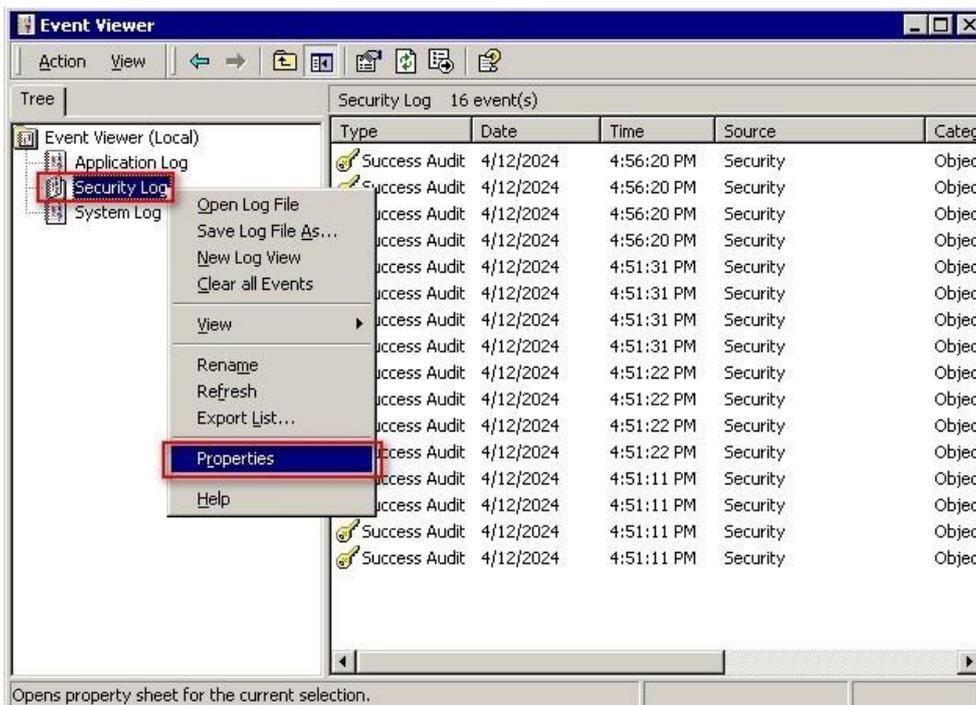
(2) Search for "Event Viewer"

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



(3) Edit Security Log

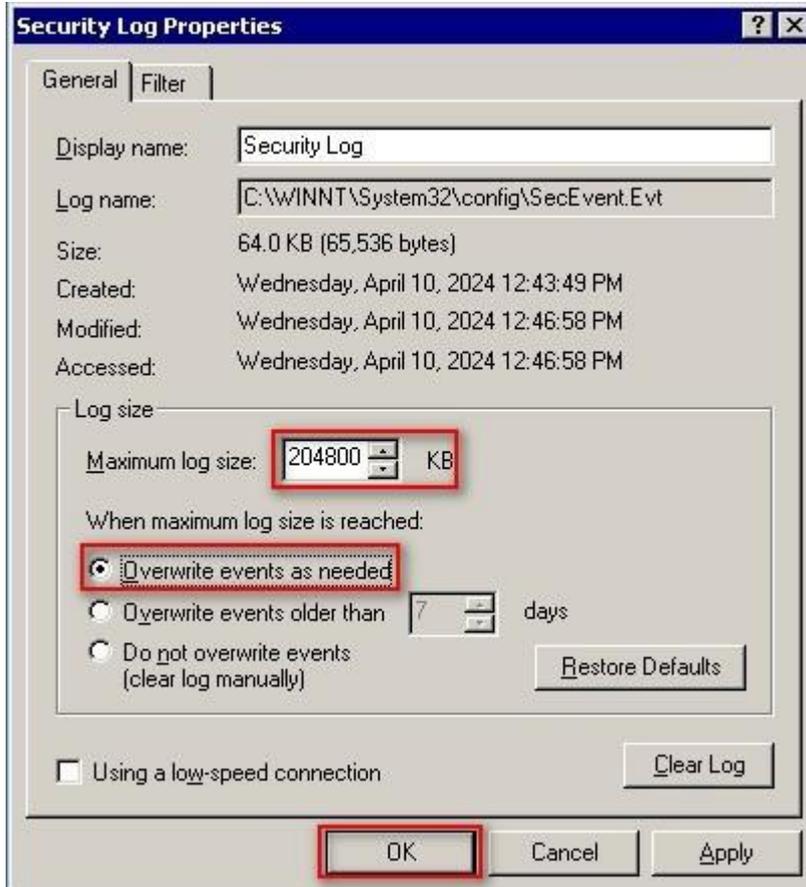
Right-click on "Security Log" -> And click on "Properties."



(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

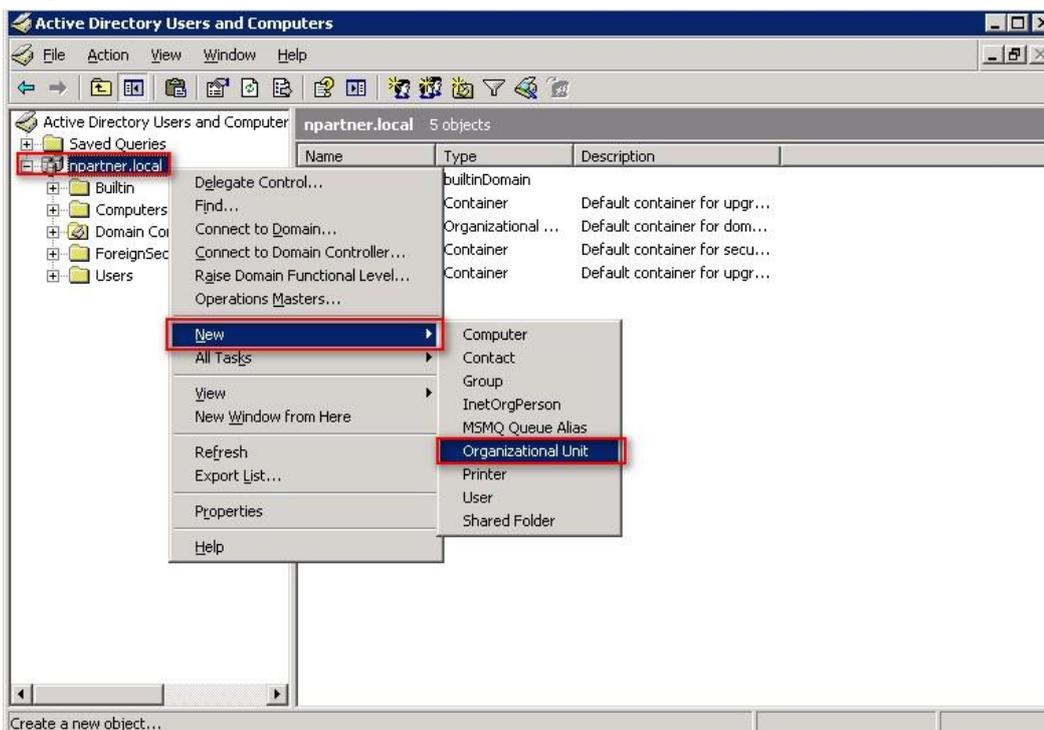
3.1.1 Organizational Unit Configuration

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



(2) Add Organizational Unit

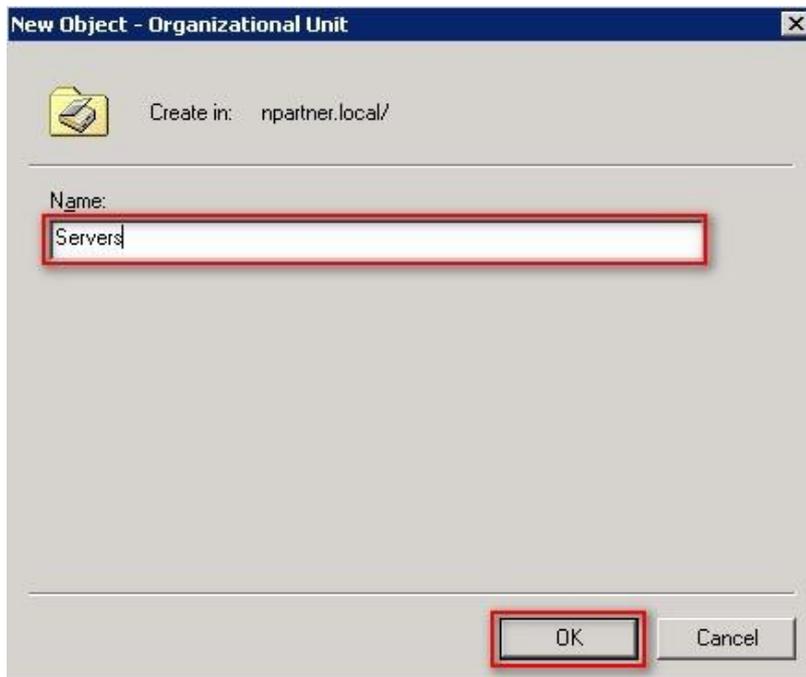
Right-click on your “Domain Name,” (in this example, it is “[npartner.local](#)”), select “New” and click “Organizational Unit.”



(3) Name Your Organizational Unit

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

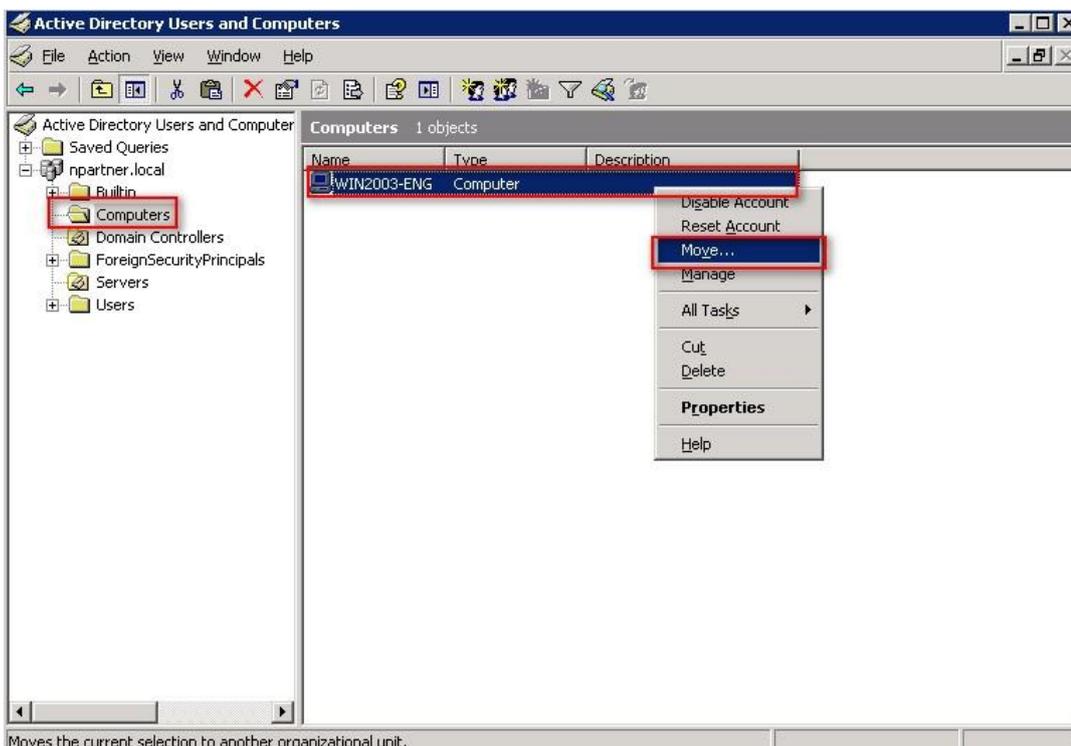
Note: Please create your organizational unit name according to the actual environment and click "OK."



(4) Move Your Server to New Organizational Unit

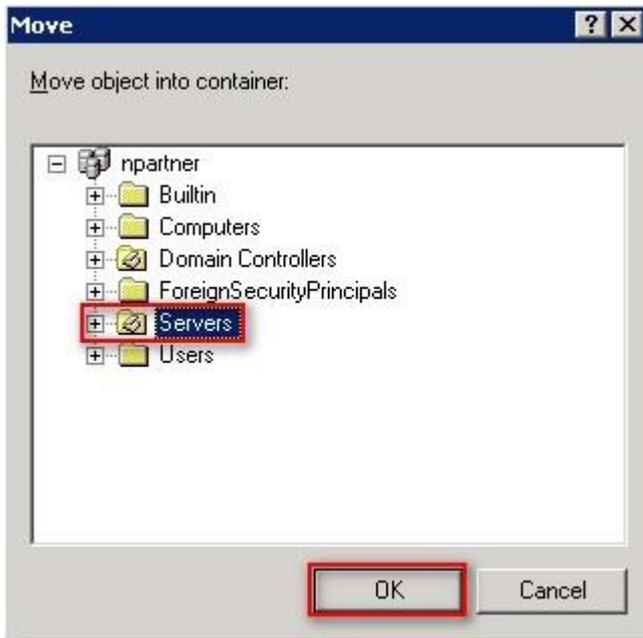
Select your organizational unit (the example here is "Computers") -> Right-click on the "WIN2003-ENG"

server · Note: Please select the Windows Server host based on actual environment -> Click "Move."



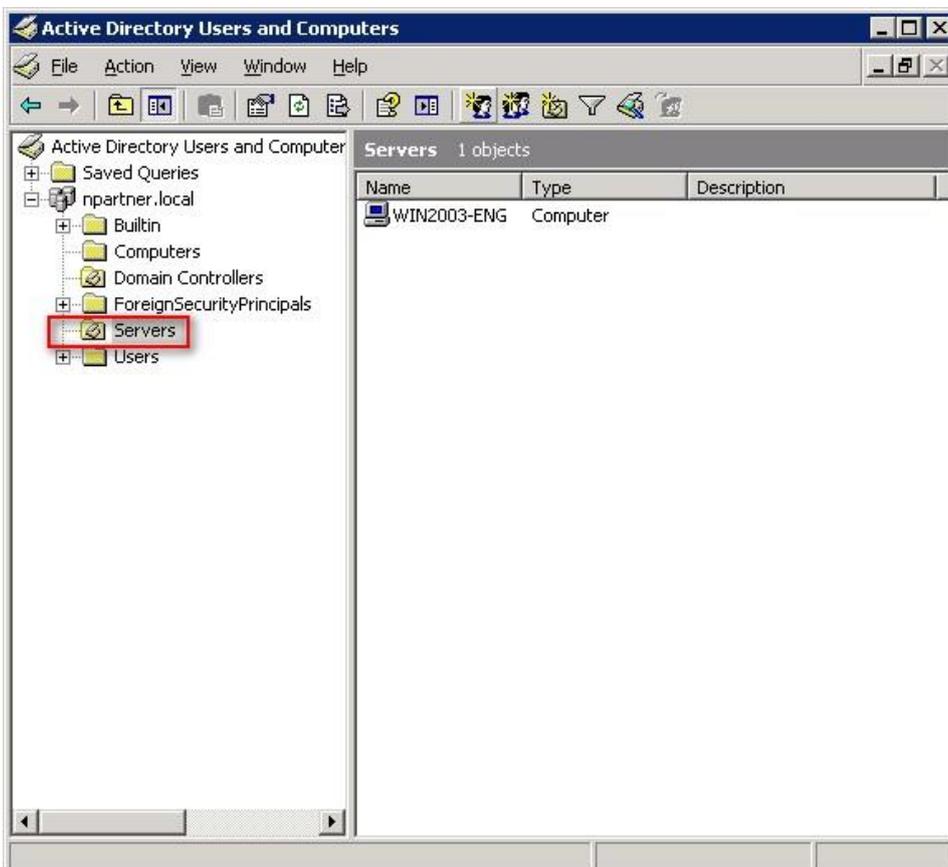
(5) Select Your Organizational Unit

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.

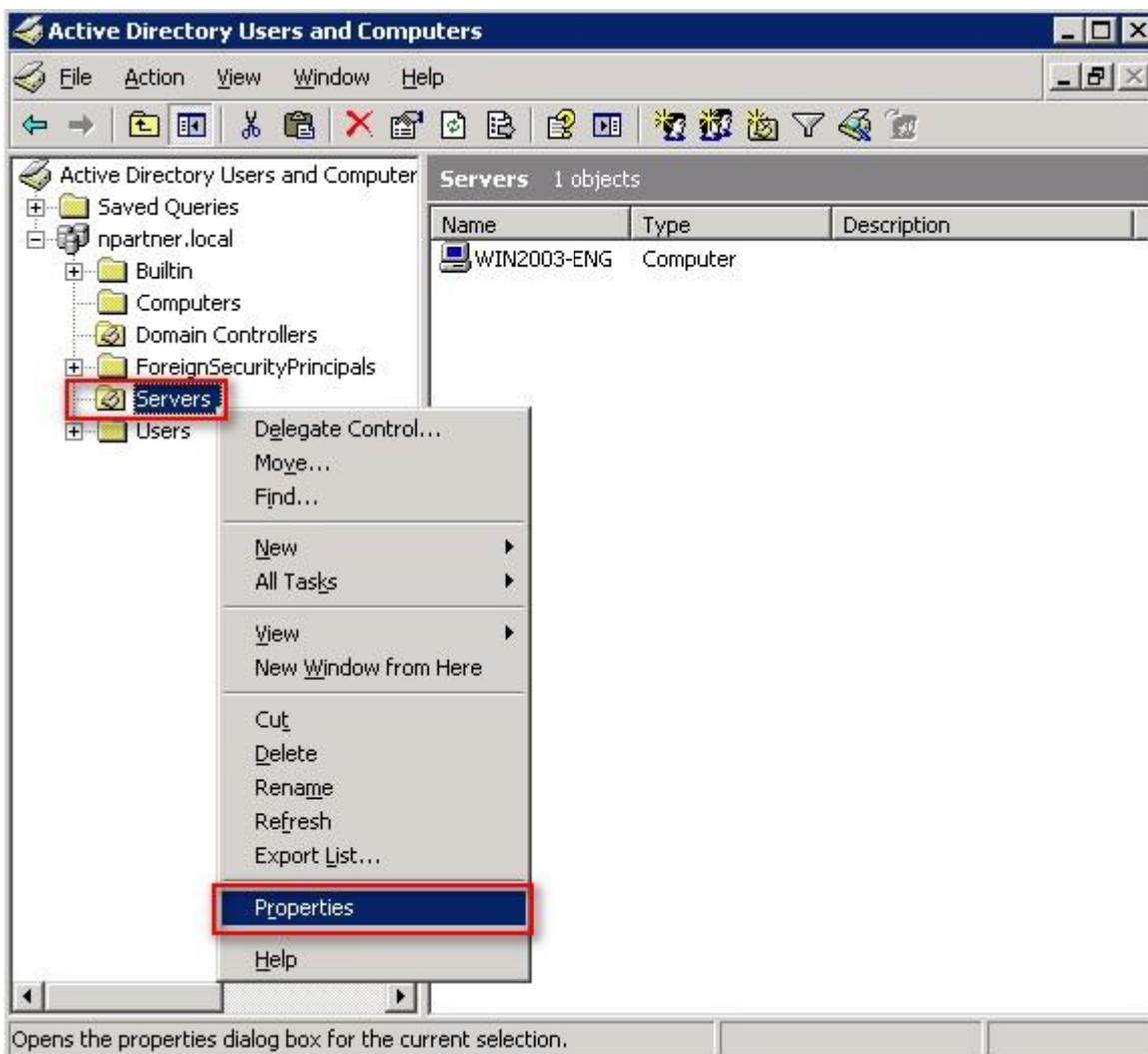


3.1.2 Group Policy Settings

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

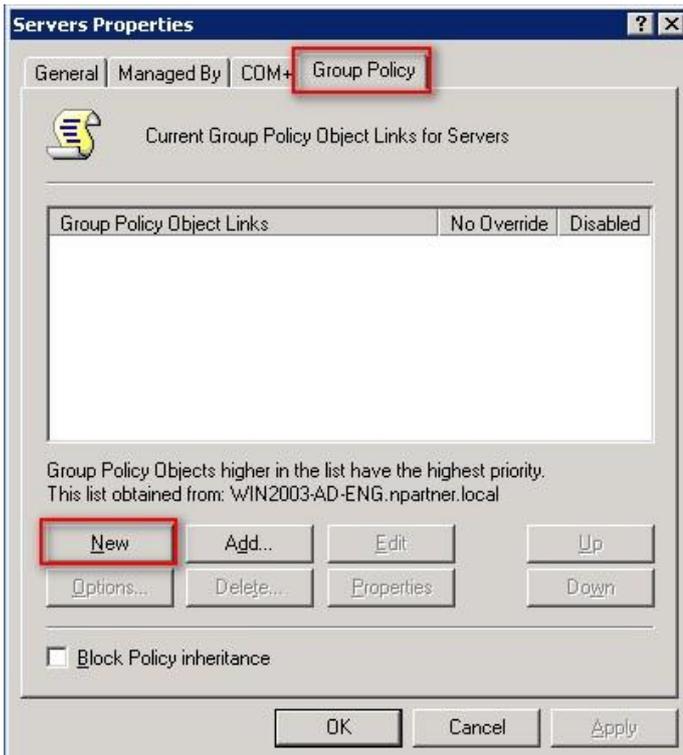


(2) Select your organizational unit (the example here is “Servers”) and right-click on “Properties.”



(3) Enter Your Group Policy Object Name

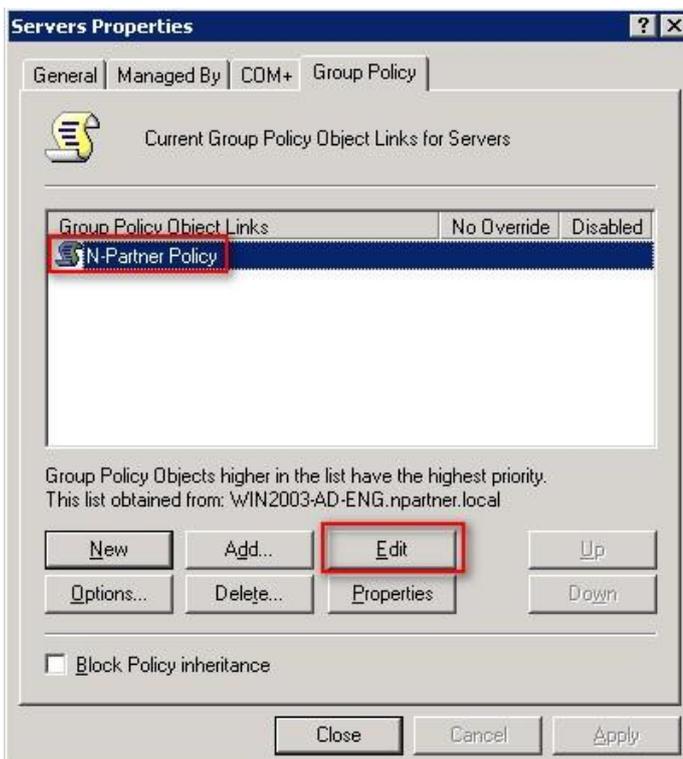
Click on the “Group Policy” page and click “New.”



(4) Edit Your Group Policy Object

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

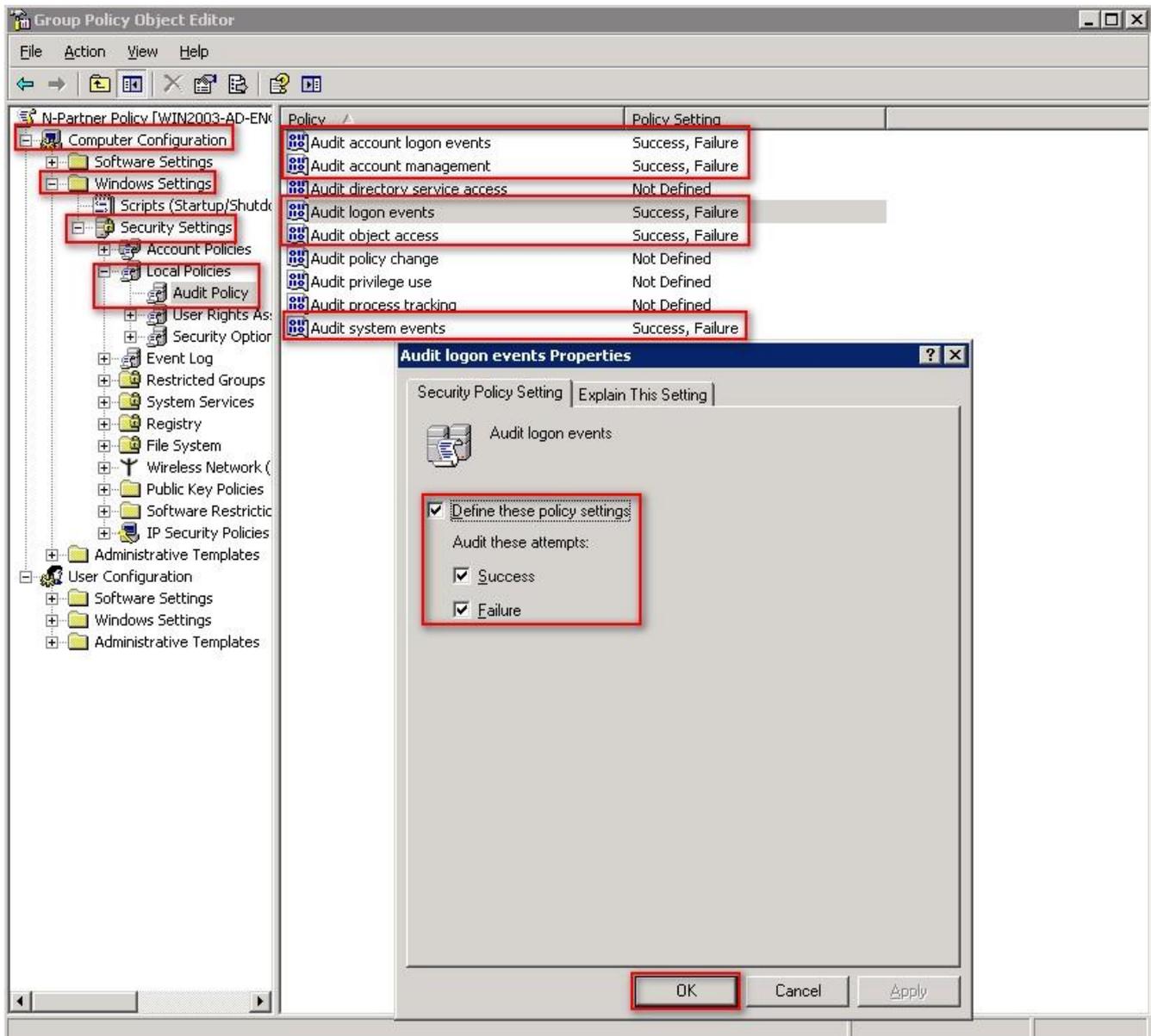
Note: Please create your group object name based on the actual environment -> Click “Edit.”



(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”:

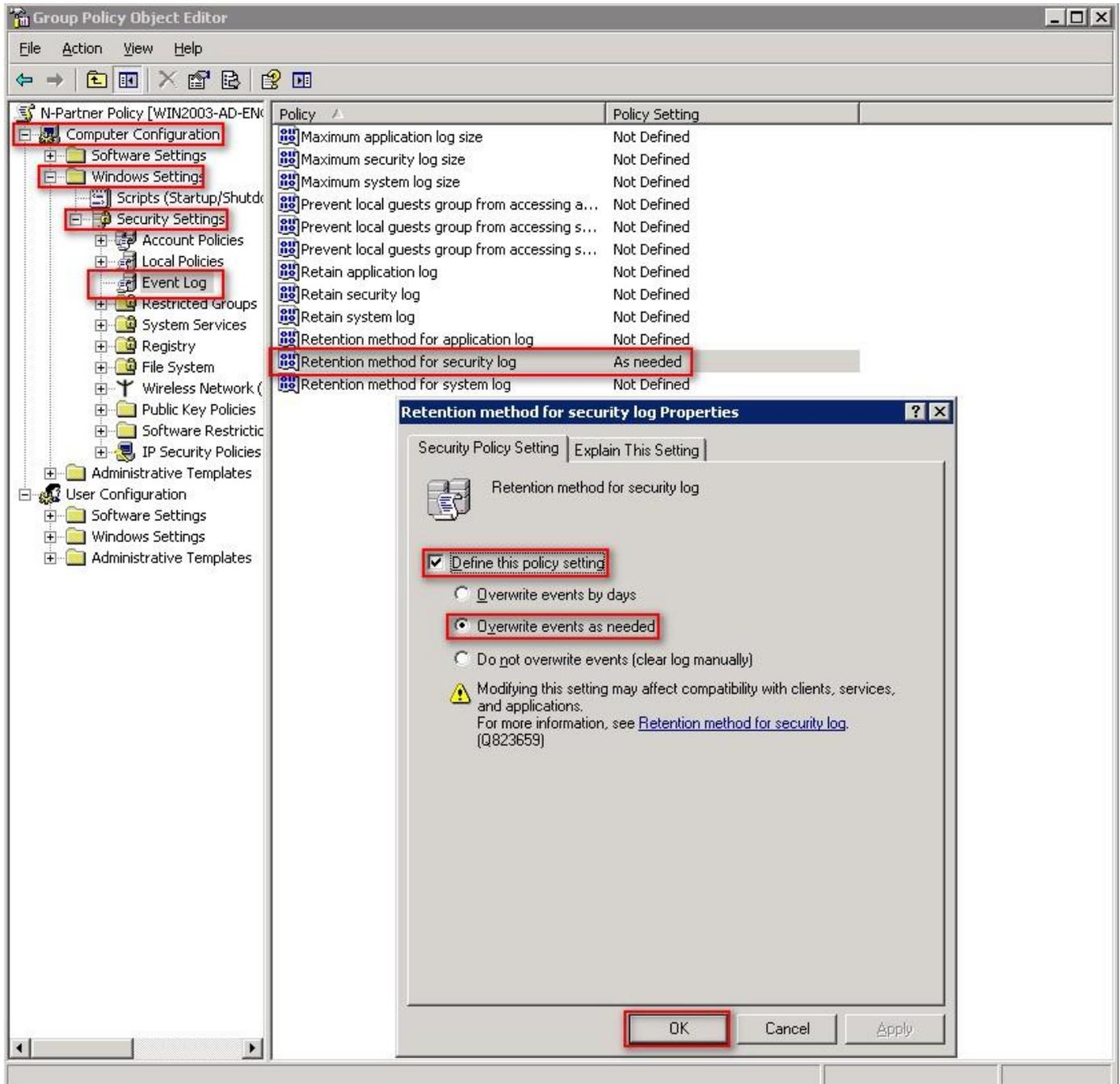
Success, Failure. -> Click “OK.”



(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].

The screenshot displays the Group Policy Object Editor window. The left-hand tree view shows the navigation path: Computer Configuration > Windows Settings > Security Settings > Event Log. The right-hand pane lists various policy settings, with 'Maximum security log size' selected and its value set to '204800 kilobytes'. A dialog box titled 'Maximum security log size Properties' is open in the foreground, showing the 'Define this policy setting' checkbox checked and the value '204800 kilobytes' entered in the text box. A warning message is visible below the text box, stating: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see [Maximum security log size](#). (Q823659)'. The 'OK' button is highlighted with a red box.

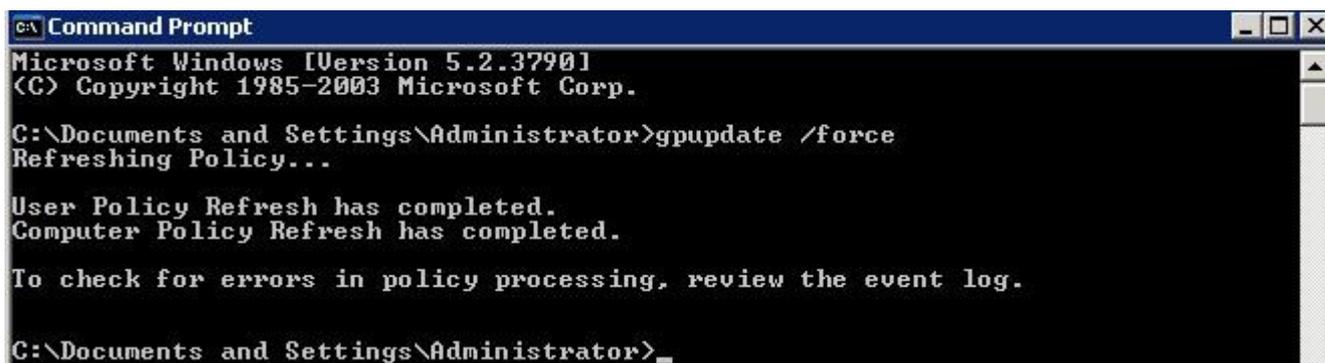
Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	204800 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing a...	Not Defined
Prevent local guests group from accessing s...	Not Defined
Prevent local guests group from accessing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

(8) Open "Command Prompt" on your Windows Server.



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

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

A screenshot of a Windows Command Prompt window. The title bar reads 'c:\ Command Prompt'. The text inside the window shows the execution of the 'gpupdate /force' command. The output indicates that the user and computer policies have been refreshed successfully. The prompt is now at 'C:\Documents and Settings\Administrator>_'.

```
c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
Refreshing Policy...

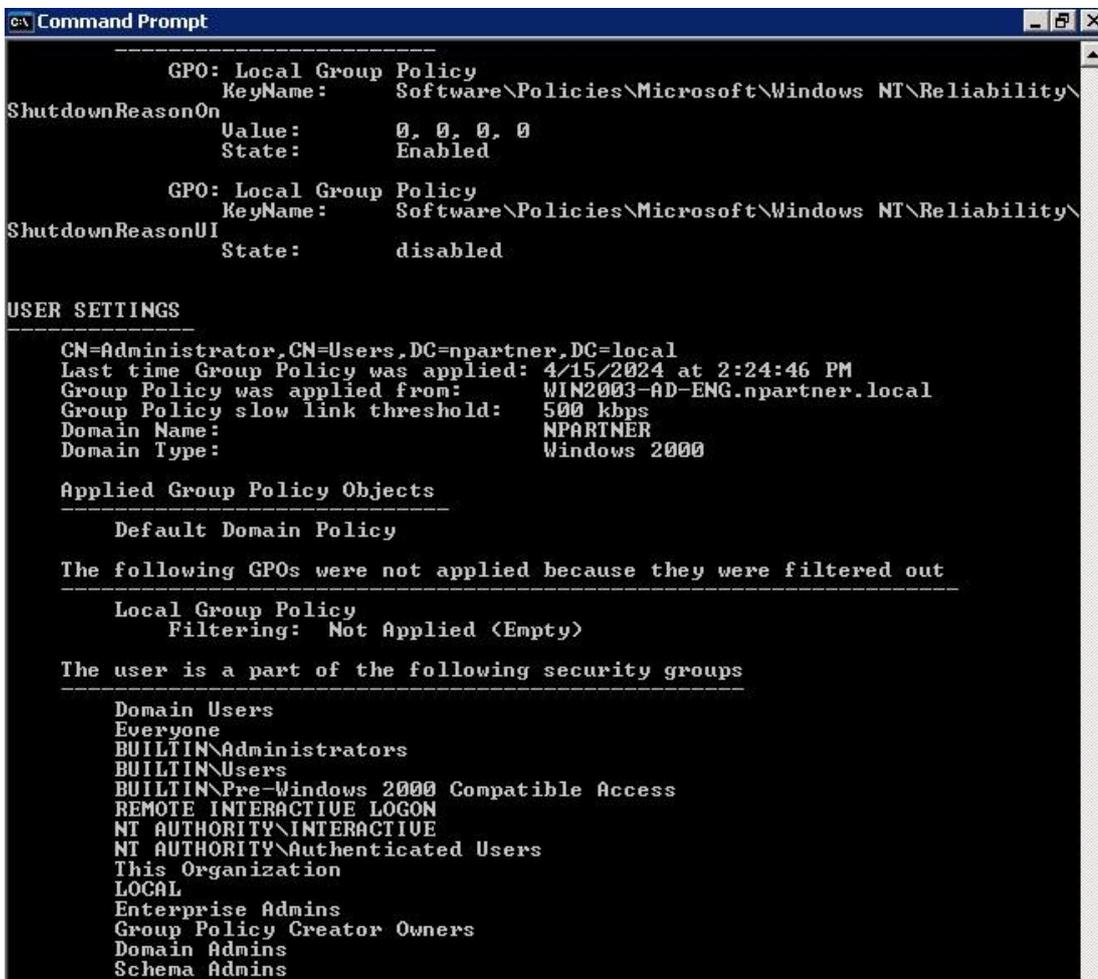
User Policy Refresh has completed.
Computer Policy Refresh has completed.

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

C:\Documents and Settings\Administrator>_
```

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

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

A screenshot of a Windows Command Prompt window showing the output of the 'gpresult /v' command. The output is formatted with dashes and includes details about local group policies, user settings, and applied group policy objects. The user is identified as 'CN=Administrator,CN=Users,DC=npartner,DC=local'.

```
c:\ Command Prompt
-----
GPO: Local Group Policy
KeyName: Software\Policies\Microsoft\Windows NT\Reliability\
ShutdownReasonOn
Value: 0, 0, 0, 0
State: Enabled

GPO: Local Group Policy
KeyName: Software\Policies\Microsoft\Windows NT\Reliability\
ShutdownReasonUI
State: disabled

USER SETTINGS
-----
CN=Administrator,CN=Users,DC=npartner,DC=local
Last time Group Policy was applied: 4/15/2024 at 2:24:46 PM
Group Policy was applied from: WIN2003-AD-ENG.npartner.local
Group Policy slow link threshold: 500 kbps
Domain Name: NPARTNER
Domain Type: Windows 2000

Applied Group Policy Objects
-----
Default Domain Policy

The following GPOs were not applied because they were filtered out
-----
Local Group Policy
Filtering: Not Applied (Empty)

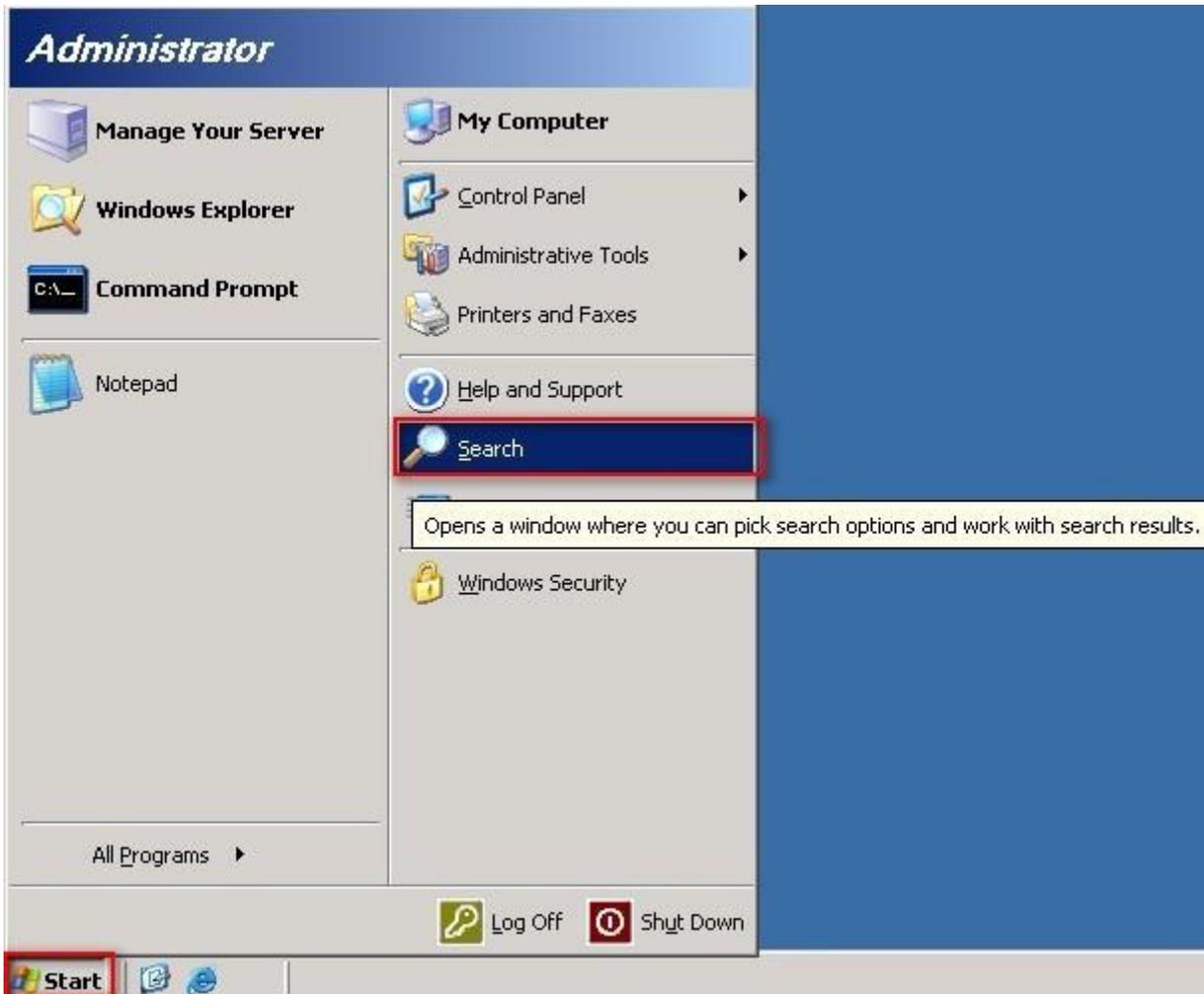
The user is a part of the following security groups
-----
Domain Users
Everyone
BUILTIN\Administrators
BUILTIN\Users
BUILTIN\Pre-Windows 2000 Compatible Access
REMOTE INTERACTIVE LOGON
NT AUTHORITY\INTERACTIVE
NT AUTHORITY\Authenticated Users
This Organization
LOCAL
Enterprise Admins
Group Policy Creator Owners
Domain Admins
Schema Admins
```

3.2 Workgroup

3.2.1 Audit Policy Settings

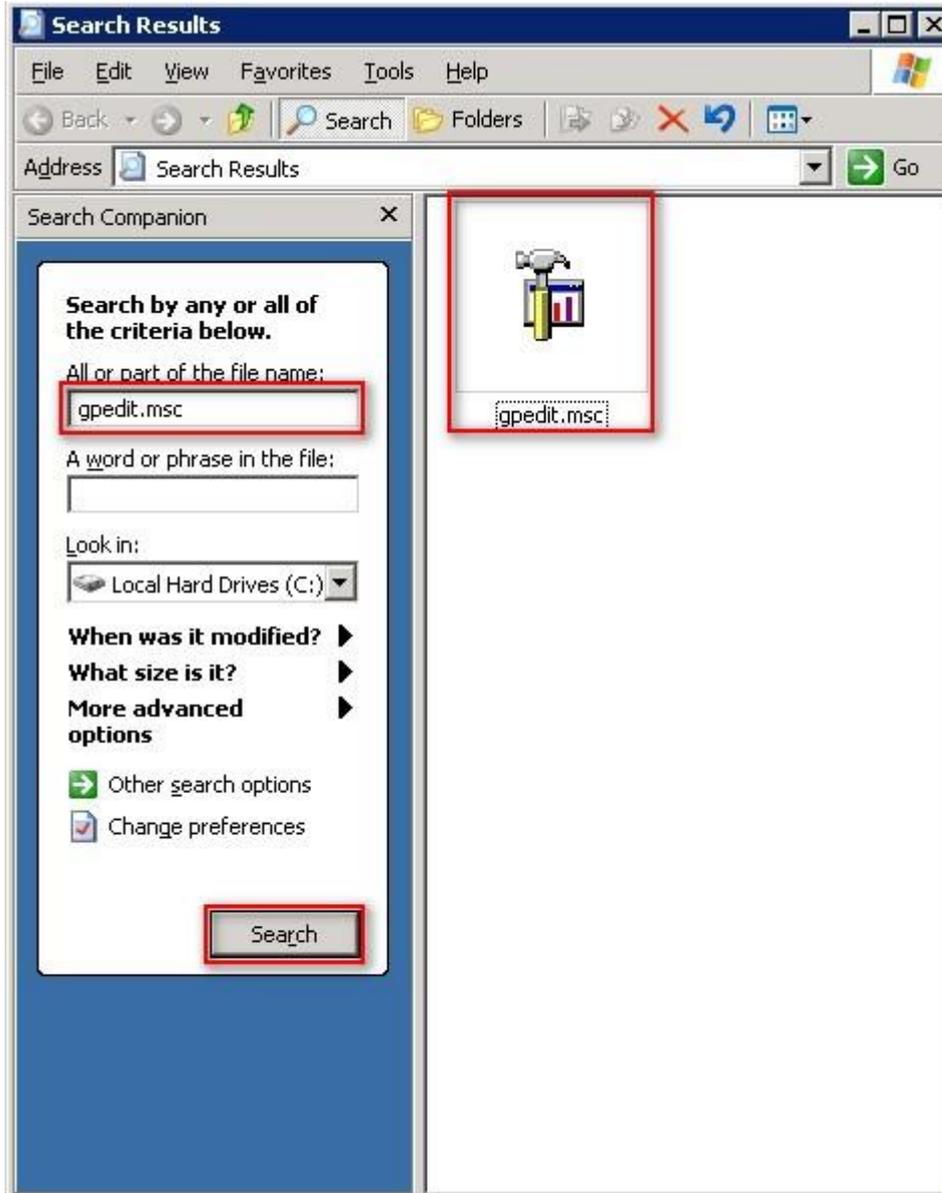
(1) Open Search

Click on "Start" -> "Search."



(2) Search for Group Policy

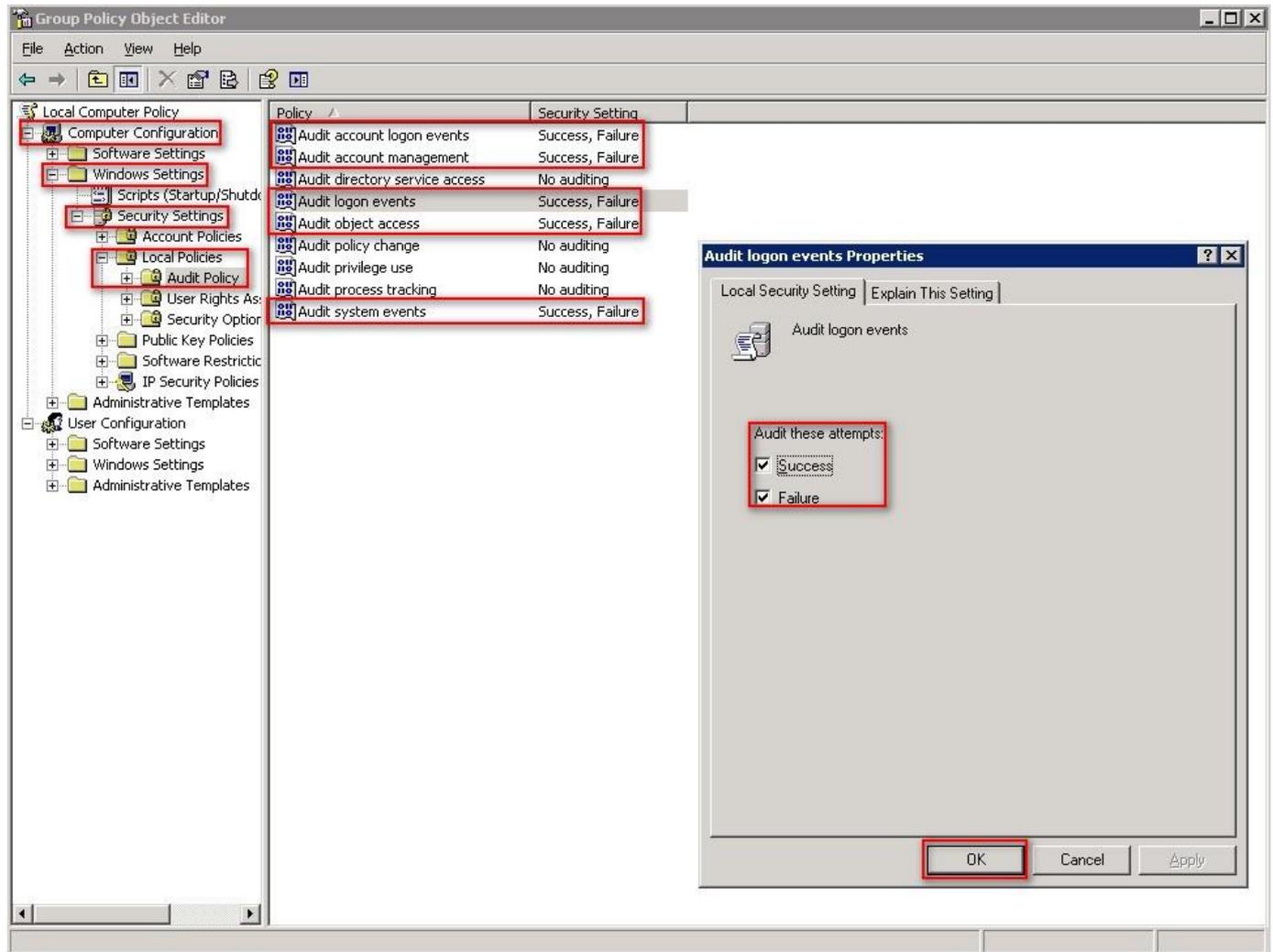
Enter "gpedit.msc" -> And click "Search" -> Click on "gpedit" in the search results.



(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
```



```
c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>gpupdate /force
Refreshing Policy...

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

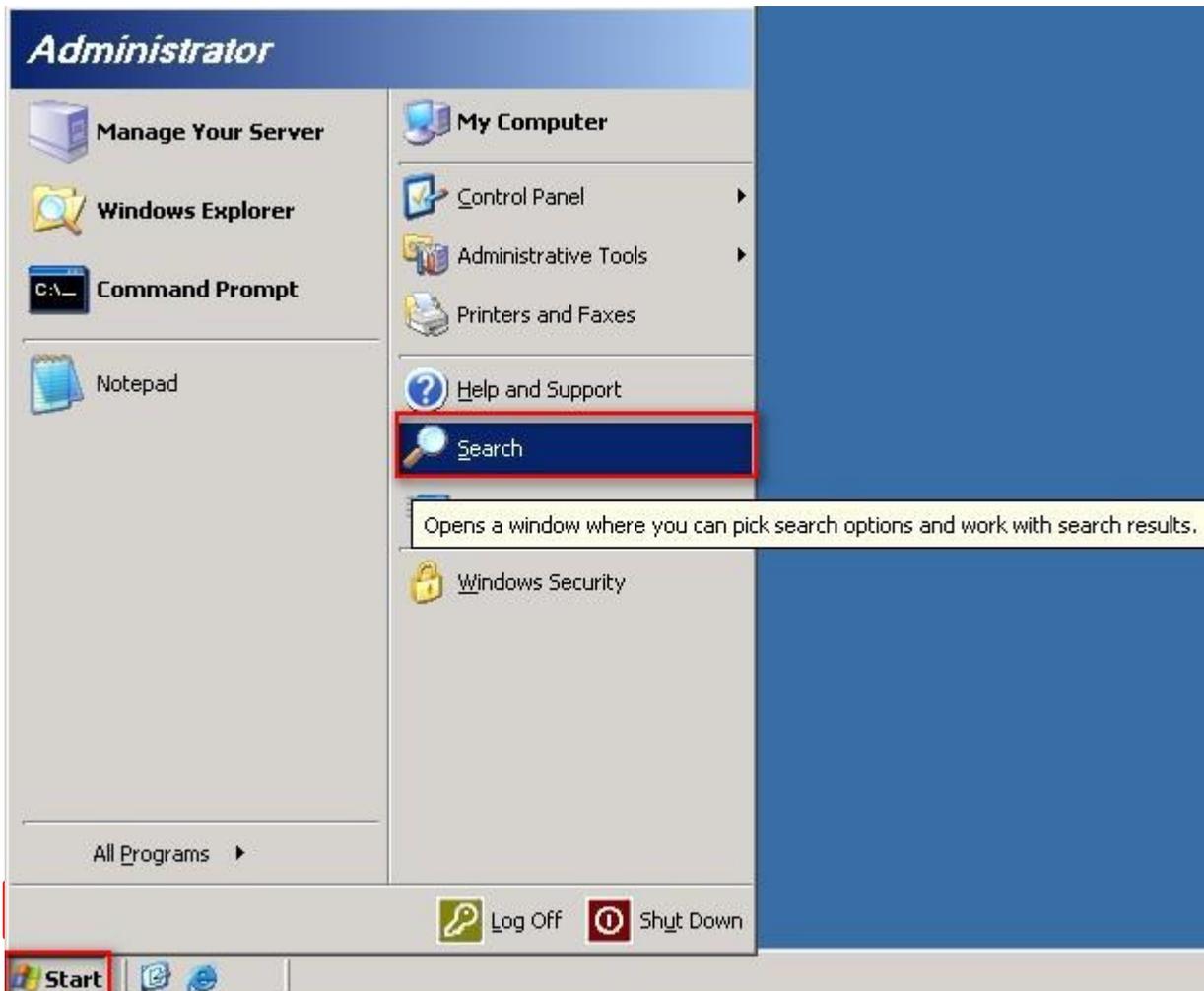
To check for errors in policy processing, review the event log.

C:\Documents and Settings\Administrator>
```

3.2.2 Event Log Settings

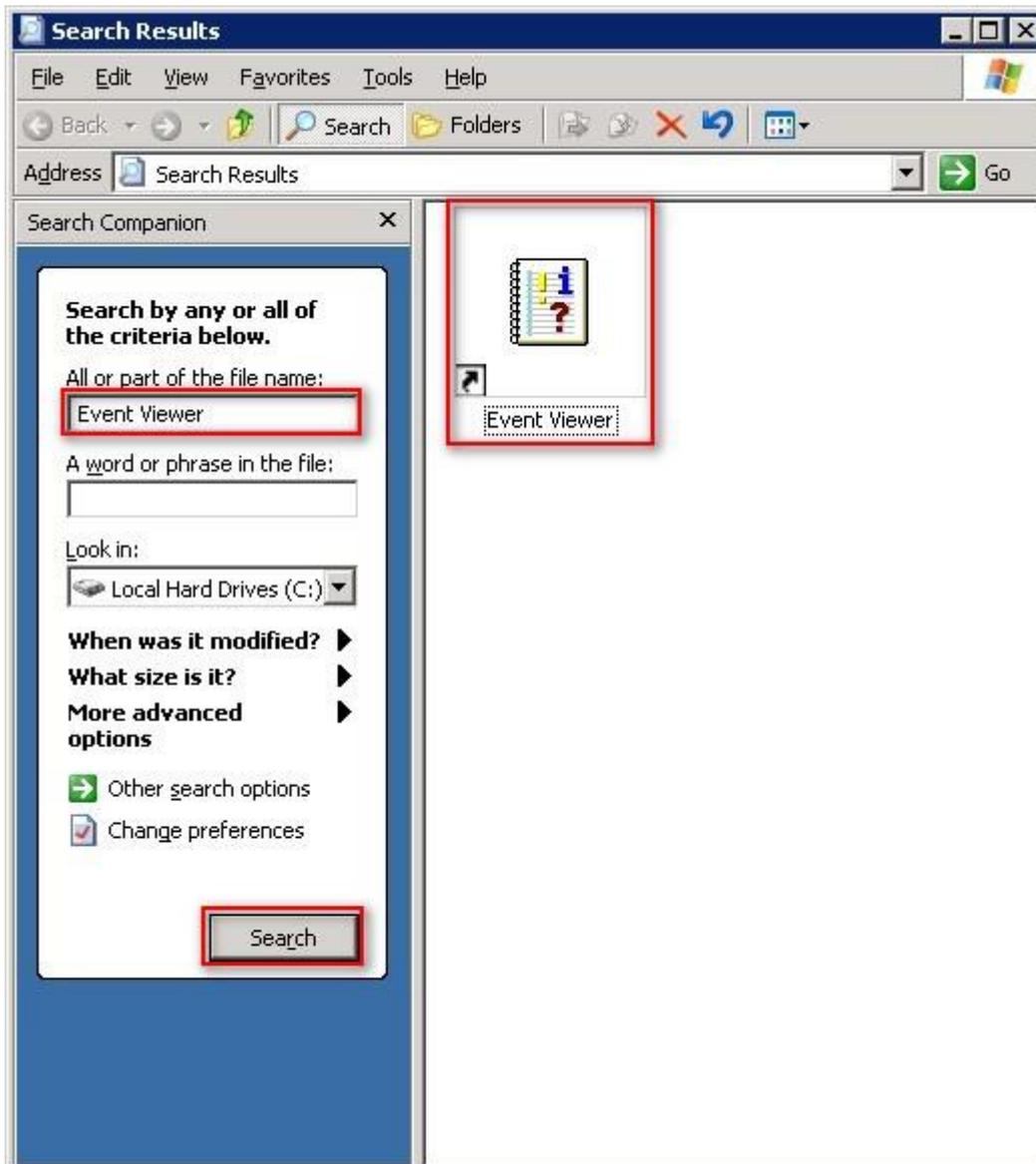
(1) Open "Search."

Click on "Start" -> "Search."



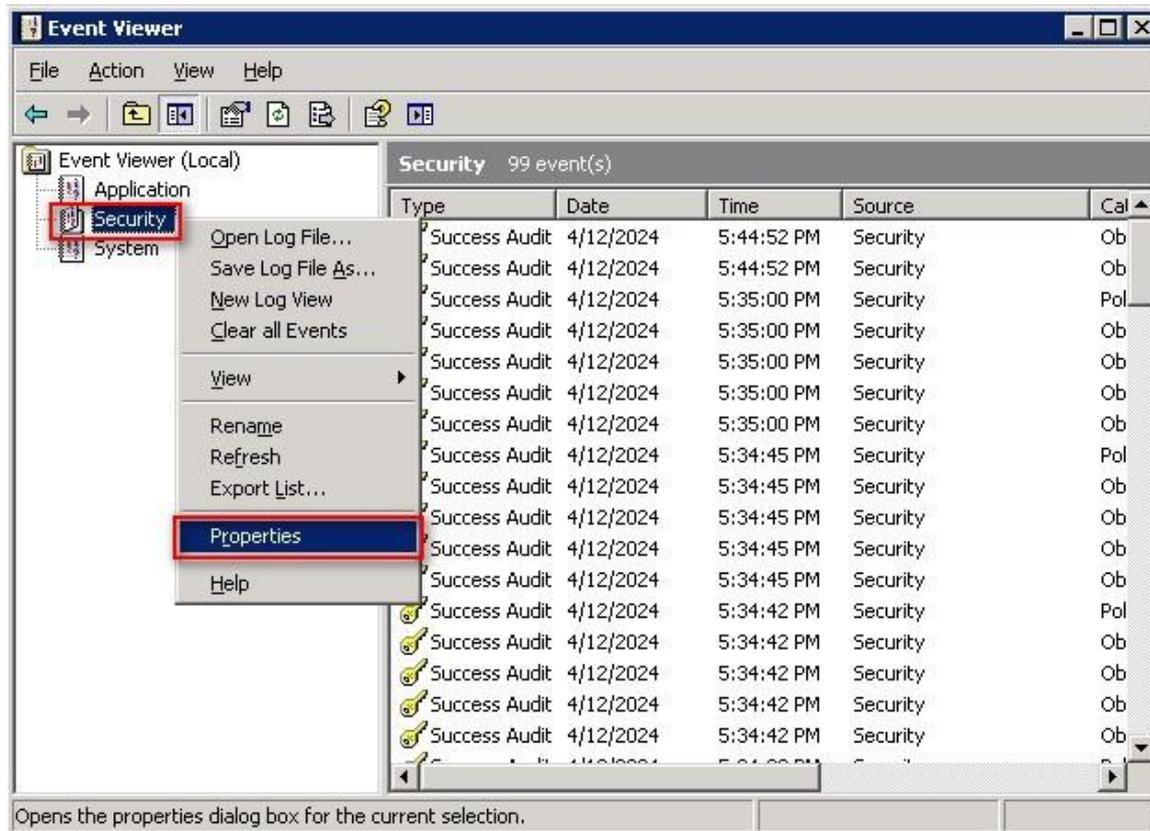
(2) Search for “Event Viewer”

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."

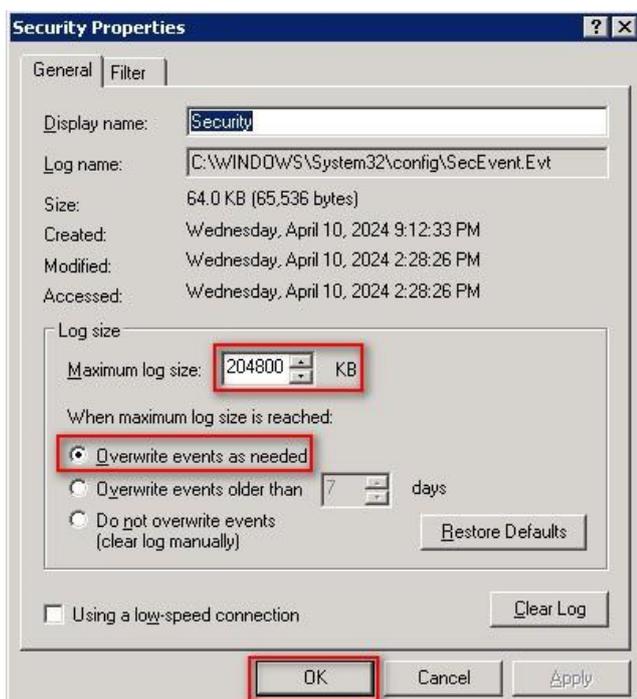


(4) Configure Security Log

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

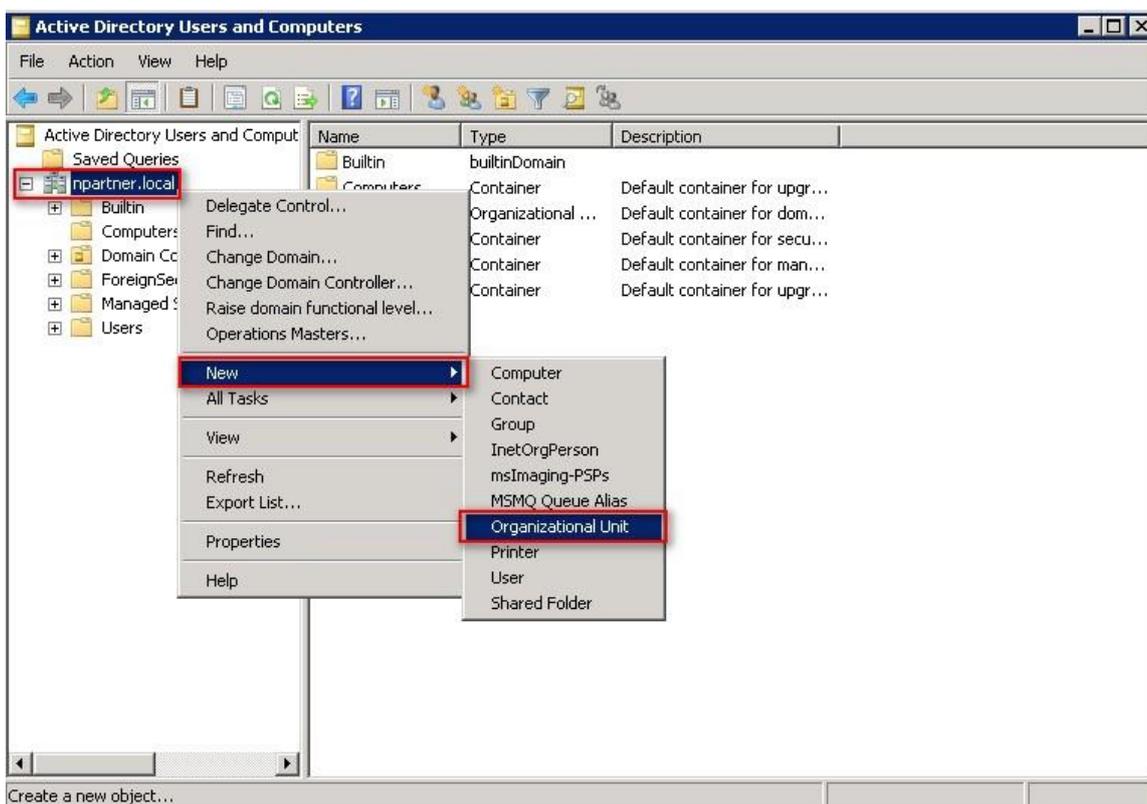
4.1.1 Organizational Unit Setup

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



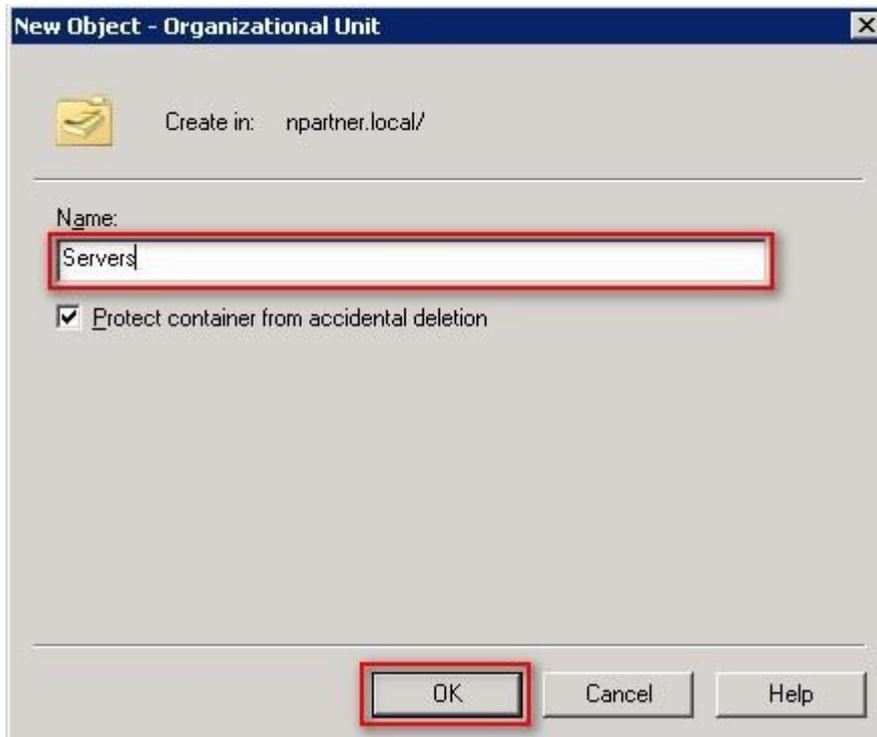
(2) Add Your Organizational Unit

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



(3) Name Your Organizational Unit

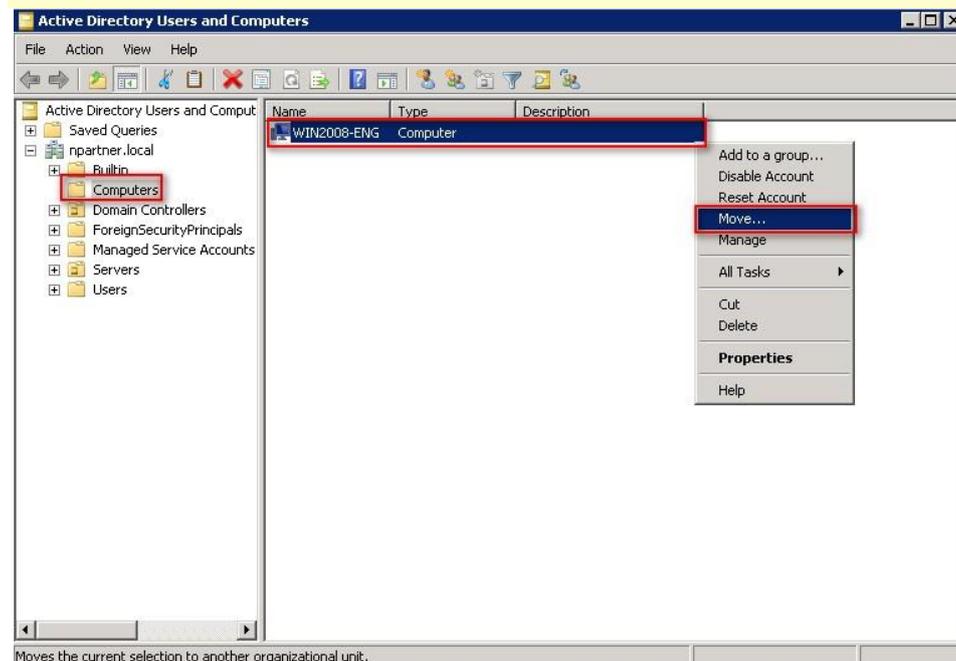
Enter your "Organizational Unit Name," (In this example, it is "Servers") Note: Please create the organizational unit name based on the client's environment. -> Click "OK."



(4) Move Your Server to New Organizational Unit

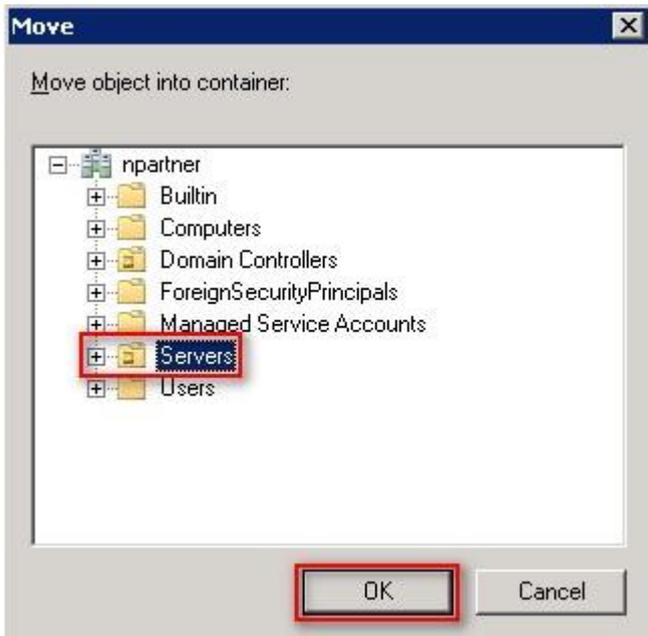
Select your organizational unit from the original folder (the example here is "Computers") -> Right-click on the "WIN2008-ENG" server.

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



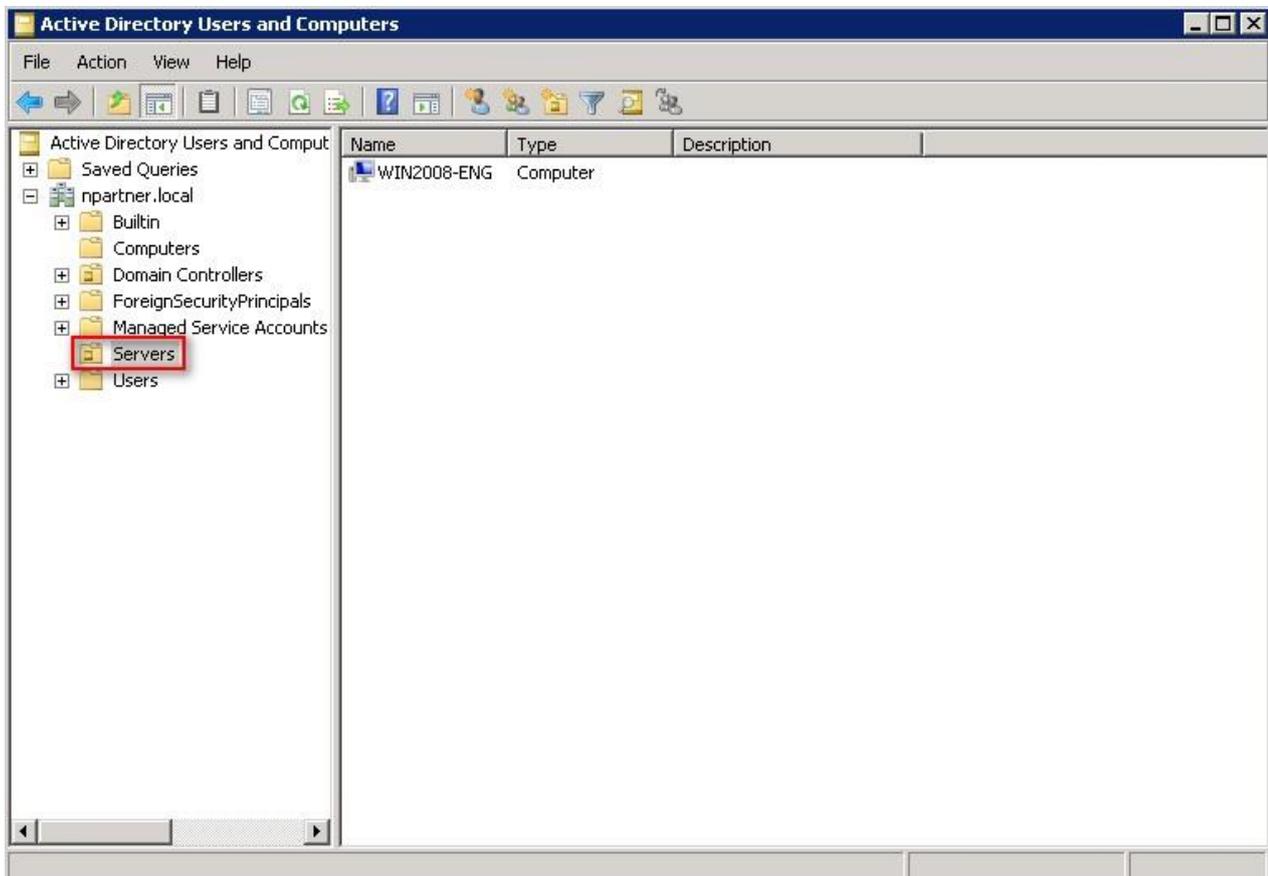
(5) Select Your New Organizational Unit

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.

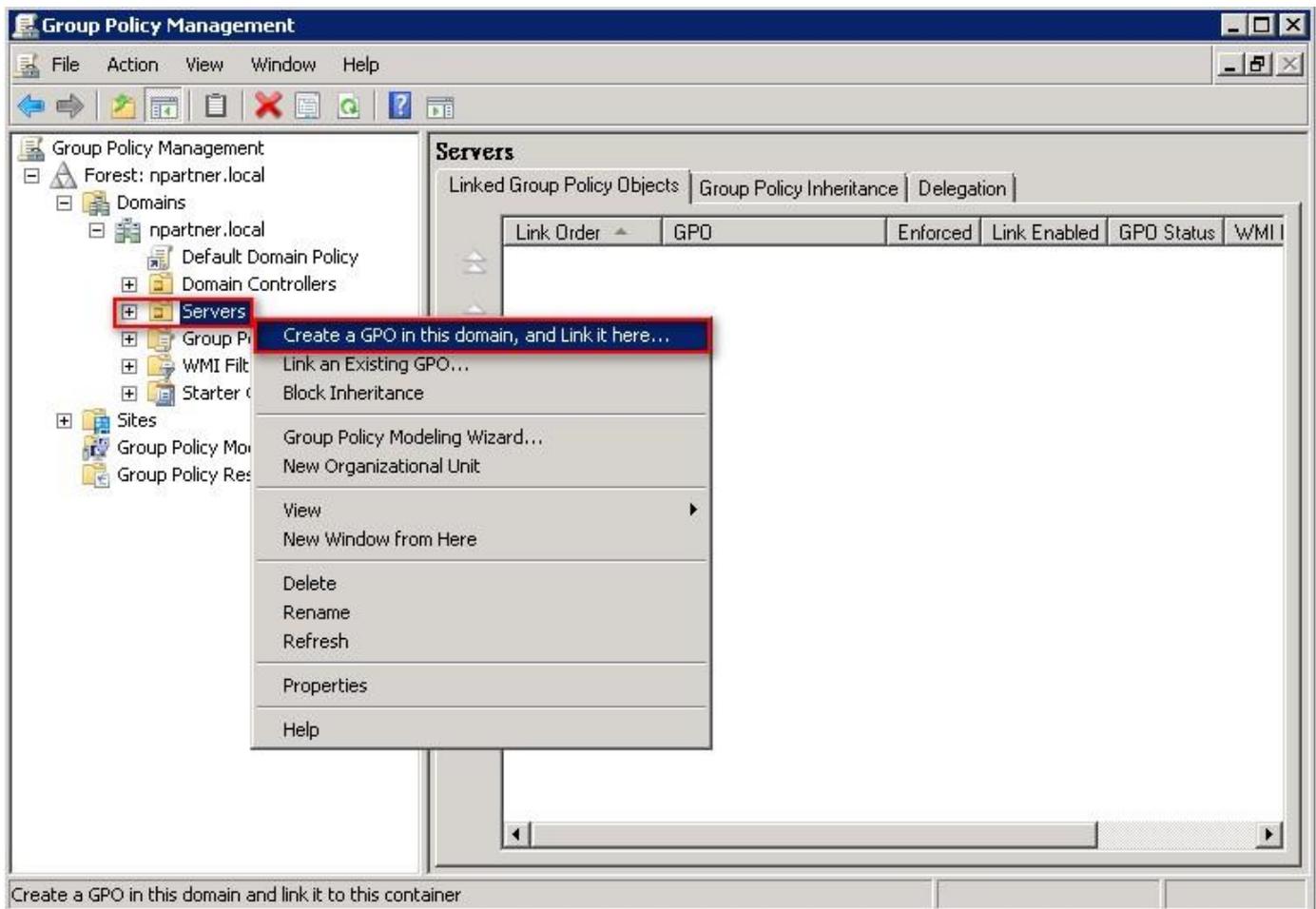


4.1.2 Group Policy Settings

(1) Open “Group Policy Management.”



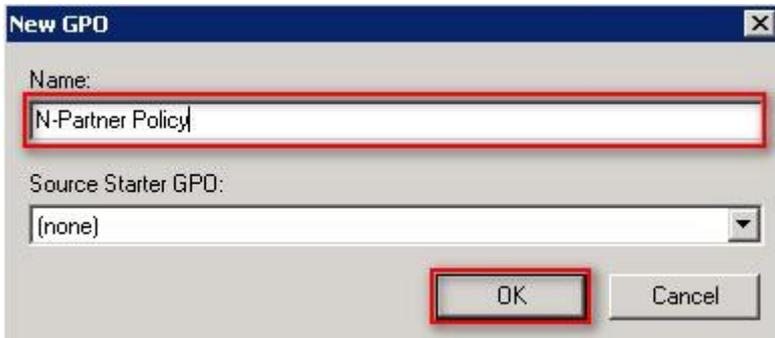
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

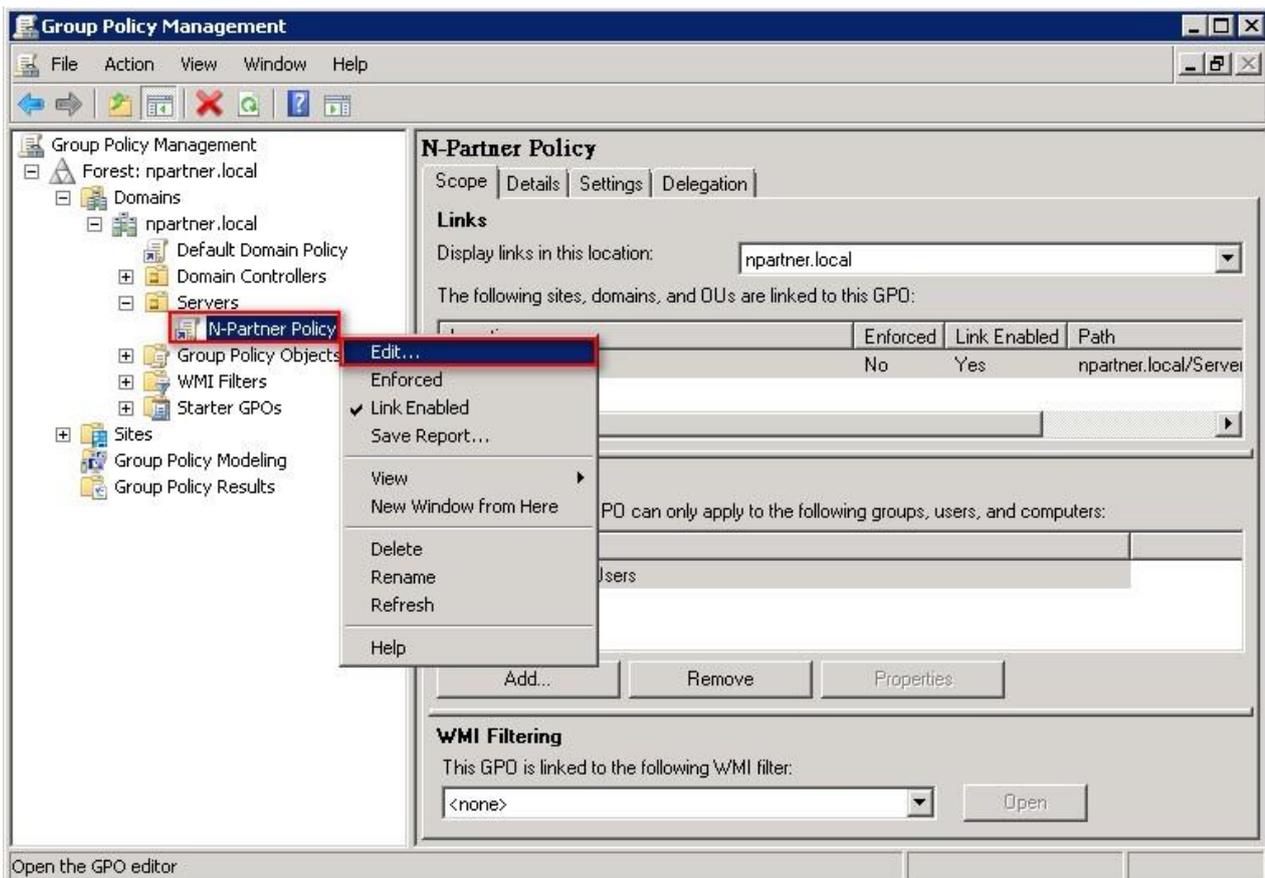
Enter your group policy object name (the example here is “N-Partner Policy”).

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



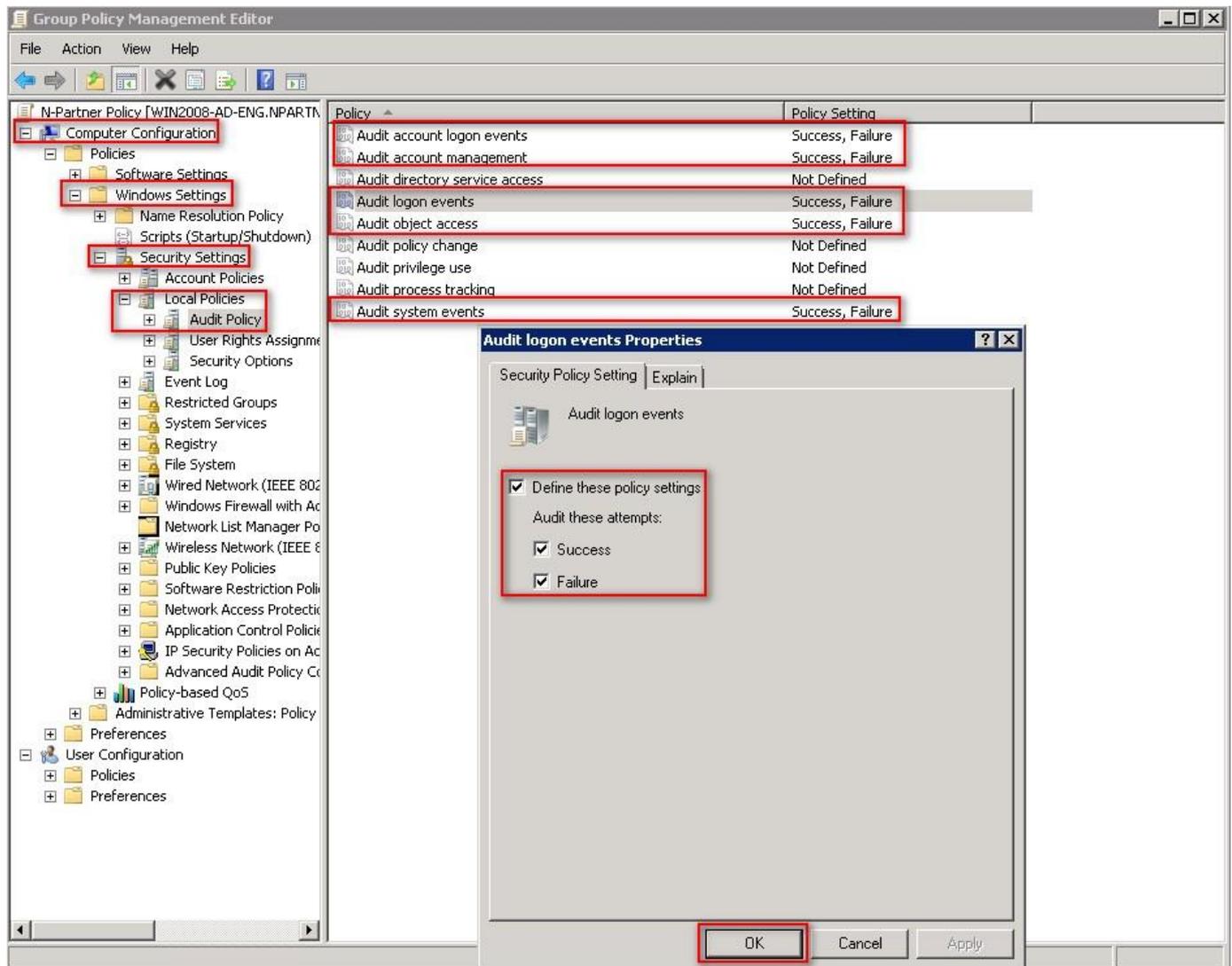
(4) Edit Your Group Policy Object

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

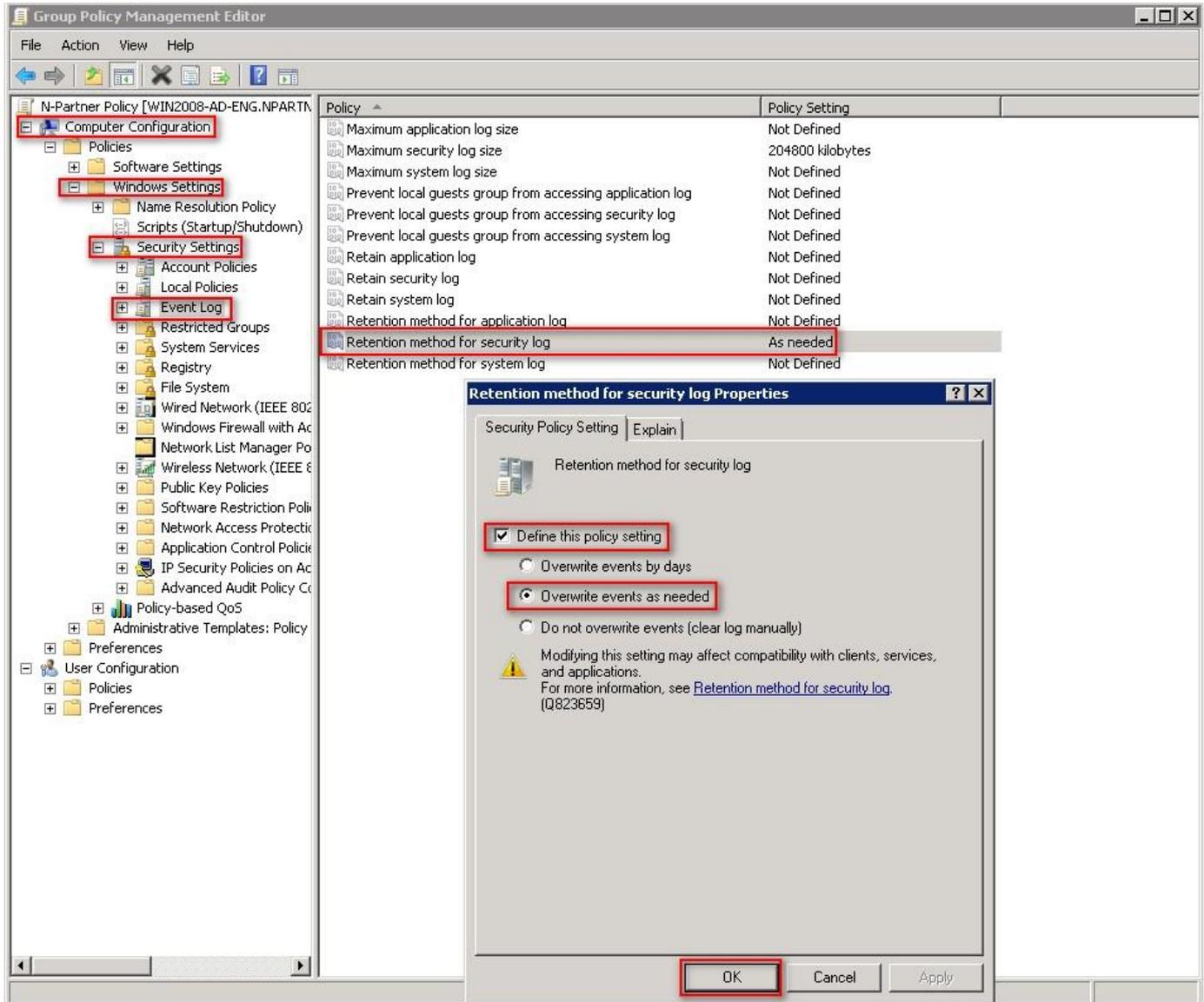
Note: Please adjust the number based on the actual environment. -> Click [OK].

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

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

(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
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

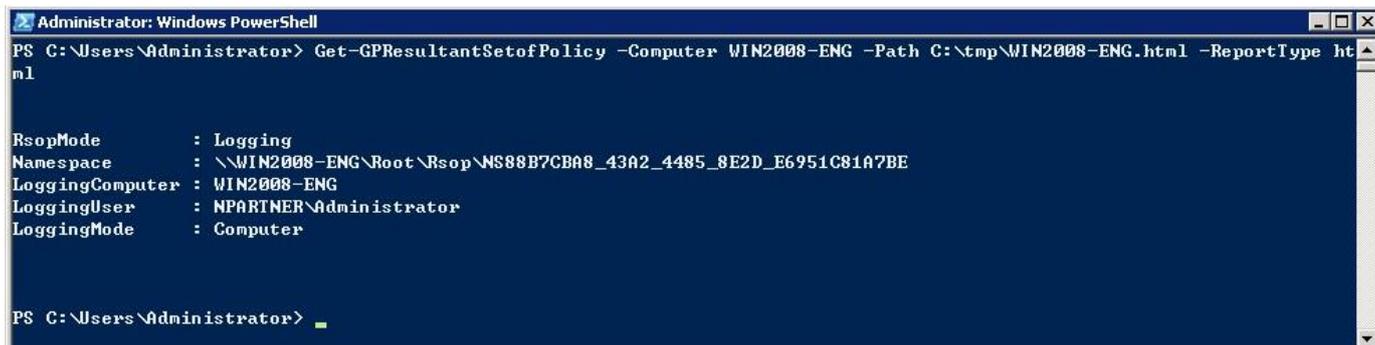
PS C:\Users\Administrator> gpupdate /force
Updating Policy...

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

PS C:\Users\Administrator> _
```

(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
```



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-GPResultantSetofPolicy -Computer WIN2008-ENG -Path C:\tmp\WIN2008-ENG.html -ReportType ht
ml

RsopMode       : Logging
Namespace     : \\WIN2008-ENG\Root\Rsop\NS88B7CBA8_43A2_4485_8E2D_E6951C81A7BE
LoggingComputer : WIN2008-ENG
LoggingUser    : NPARTNER\Administrator
LoggingMode    : Computer

PS C:\Users\Administrator> _
```

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.

The screenshot shows a web browser window displaying a report titled "Computer Configuration". The report is organized into several sections, each containing a table of policy settings. The sections visible are:

- Account Policies/Password Policy**

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
- Account Policies/Account Lockout Policy**

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
- Local Policies/Audit Policy**

Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
- Local Policies/Security Options**

Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy

4.2 Workgroup

4.2.1 Audit Policy Settings

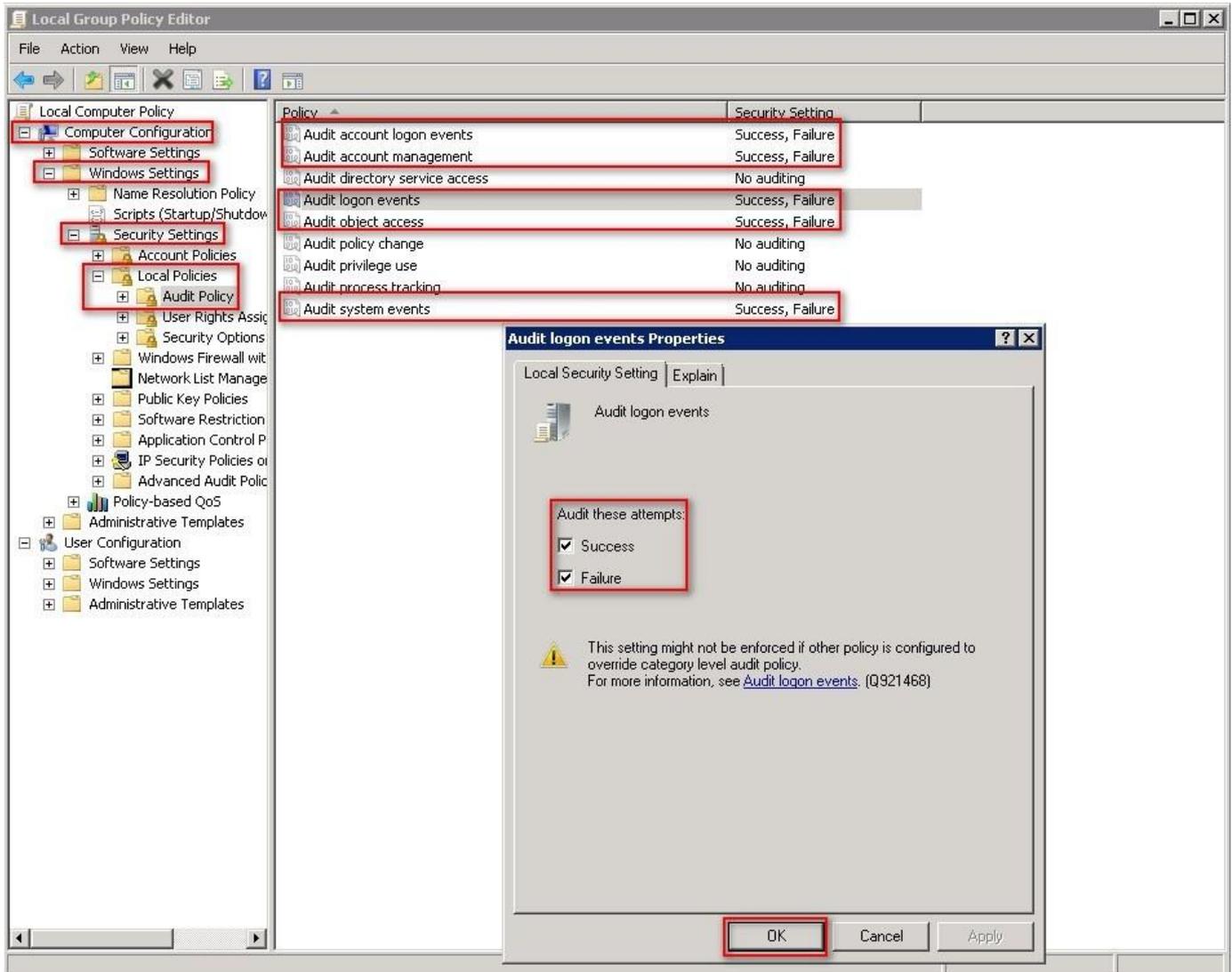
(1) Open Local Group Policy Editor

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.”

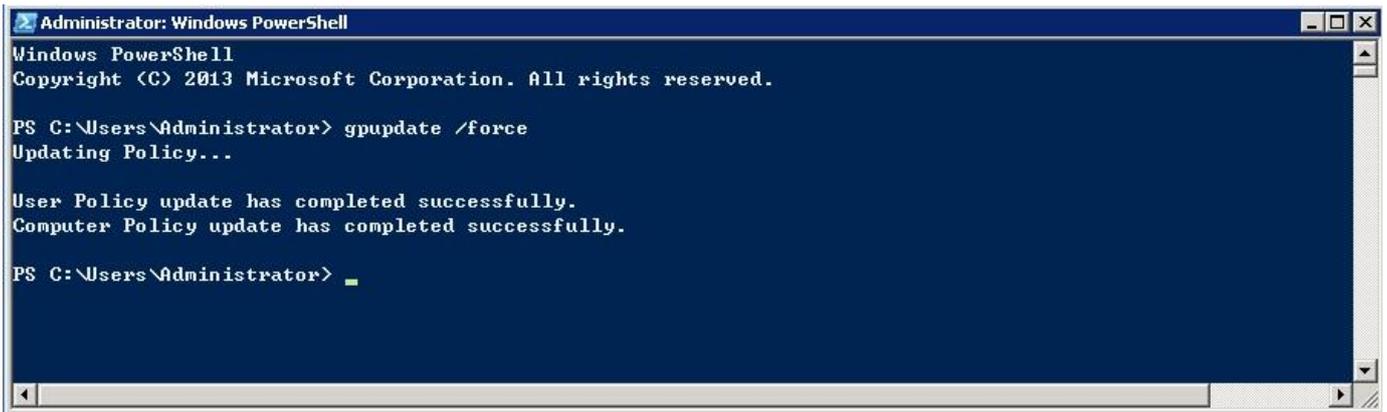


(3) Open “Windows PowerShell.”



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

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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

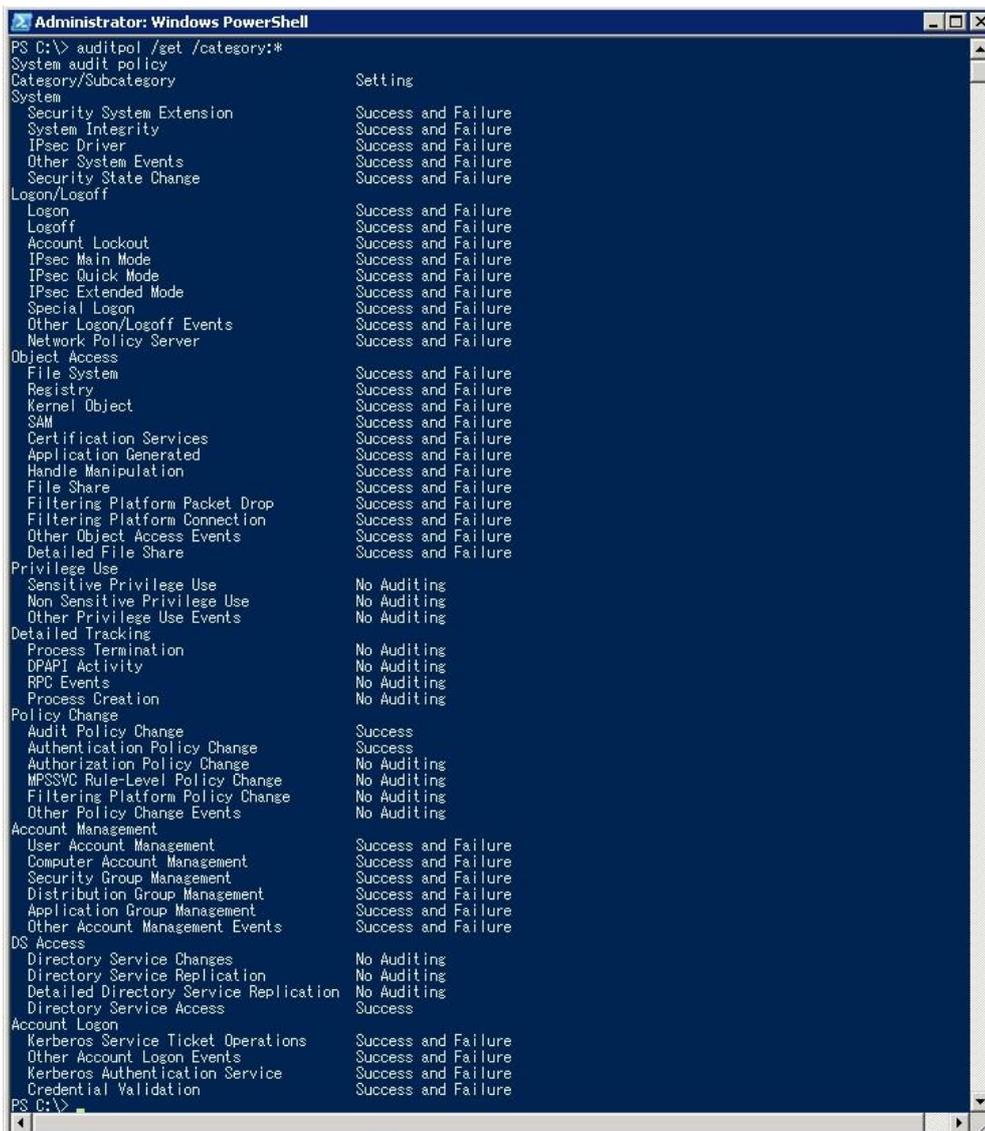
PS C:\Users\Administrator> gpupdate /force
Updating Policy...

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

PS C:\Users\Administrator> _
```

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

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

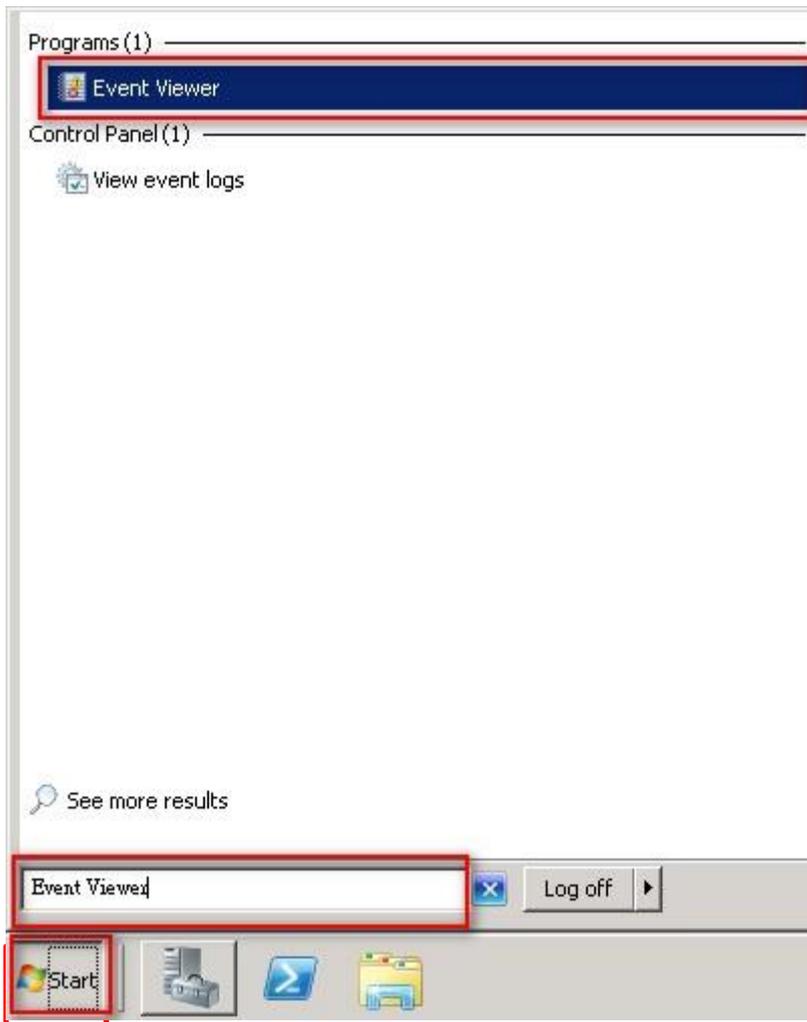


```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System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

4.2.2 Event Log Settings

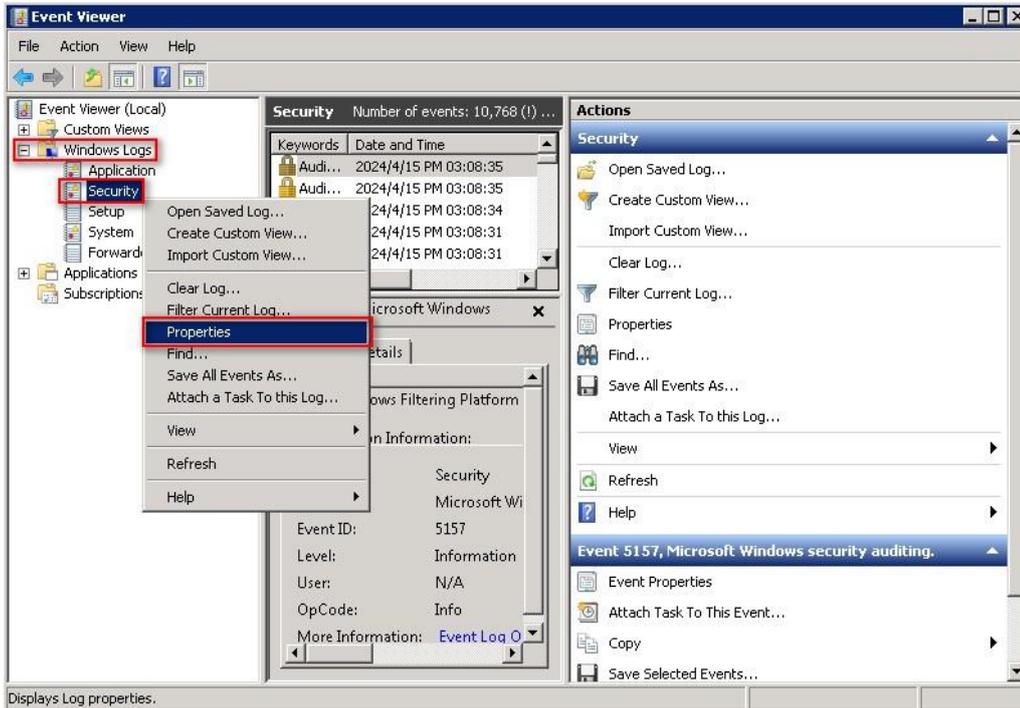
(1) Search for “Event Viewer”

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.”

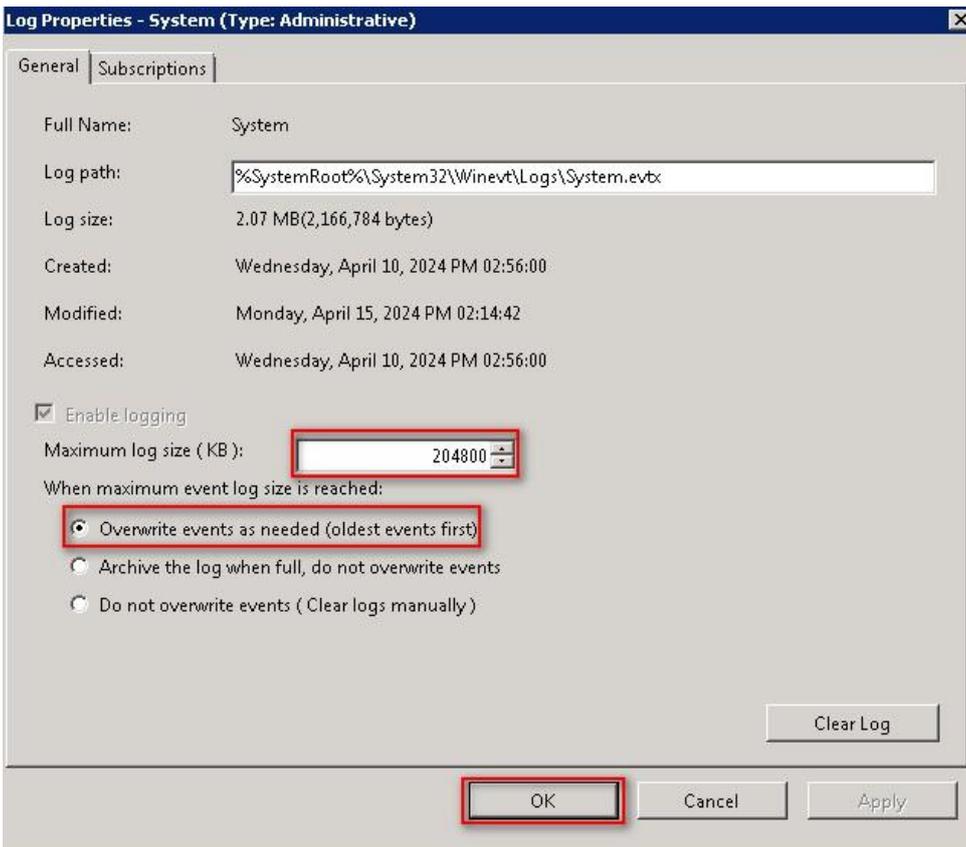


(3) Configure Security Log

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 Recommendation link](#) provided in preface for detailed explanations.

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

5.1 Domain

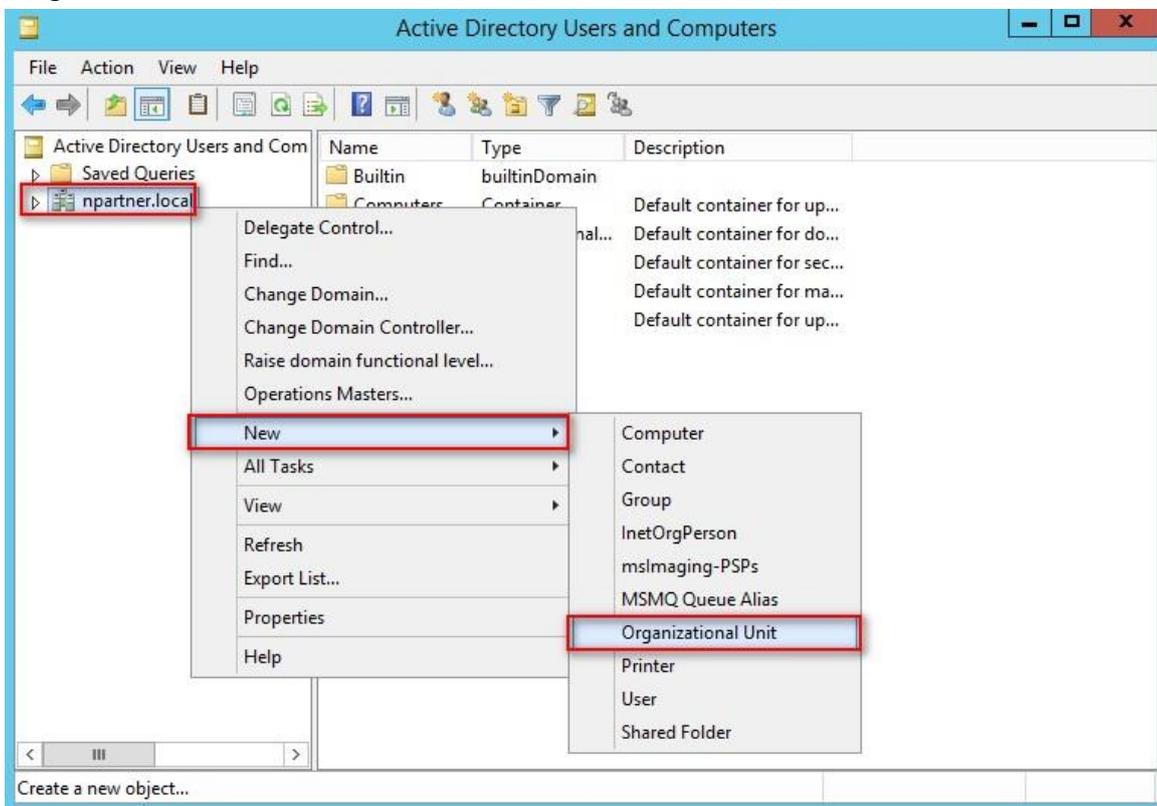
5.1.1 Organizational Unit Setup

(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.”

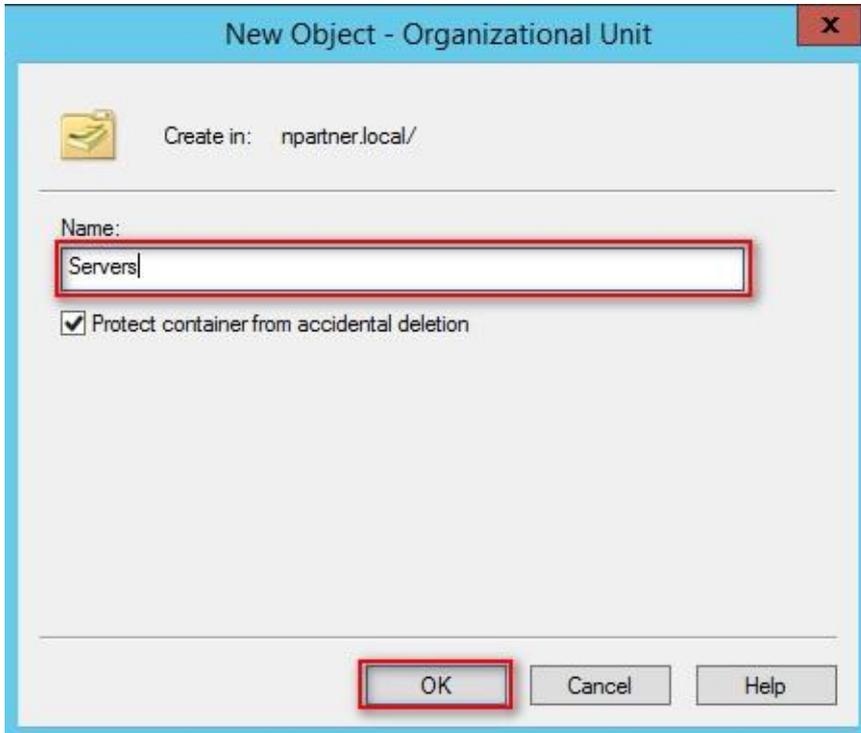


(3) Name Your Organizational Unit

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

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

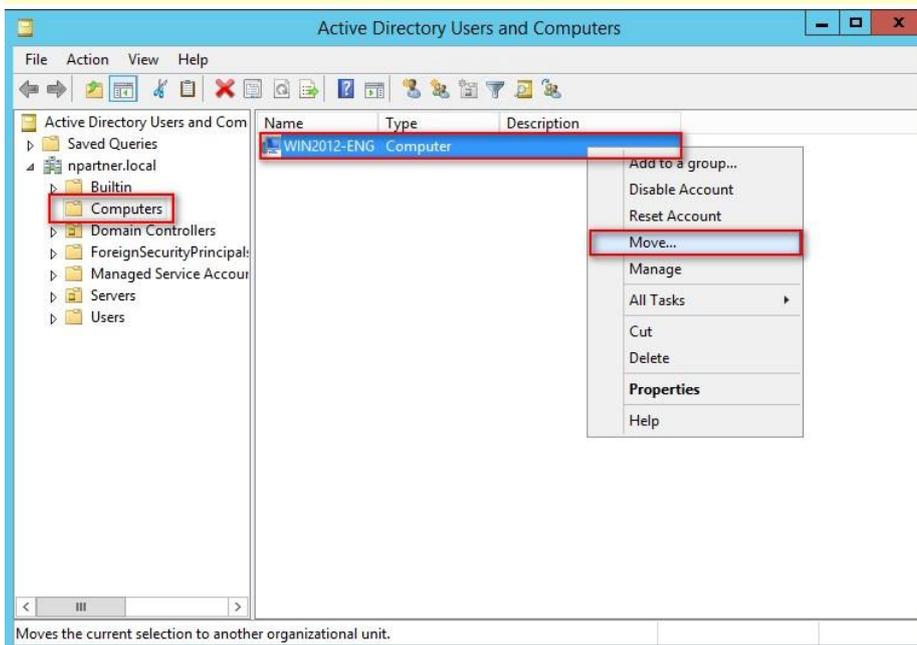
-> and click "OK."



(4) Move Your Server to New Organizational Unit

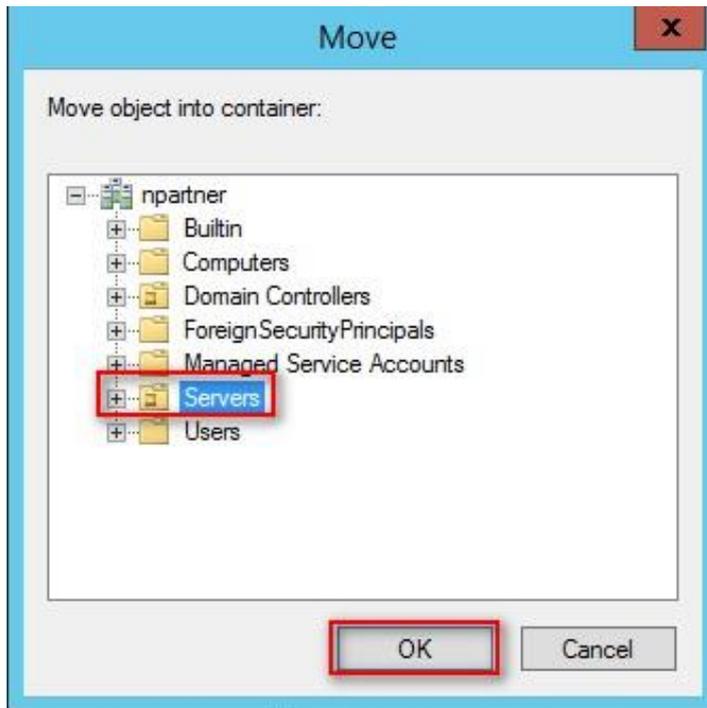
Select your organizational unit (the example here is "Computers") -> Right-click on the "WIN2012-ENG" server.

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



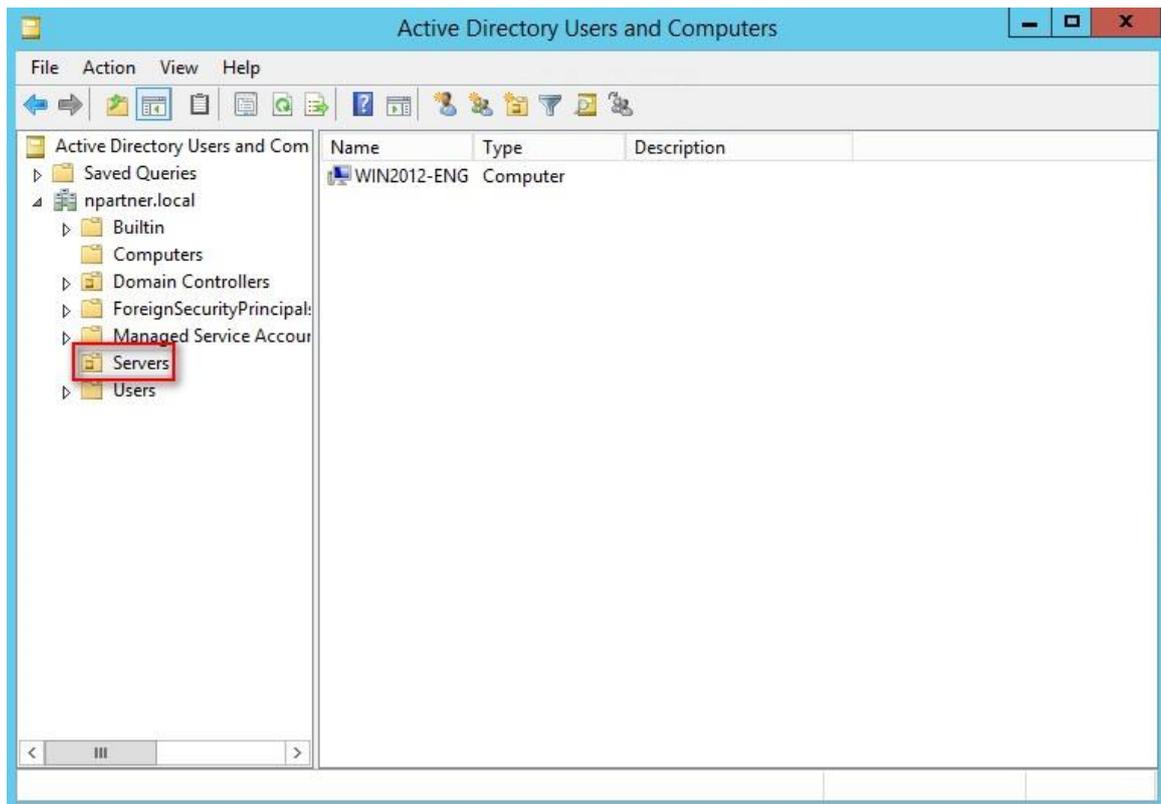
(5) Select Your Organizational Unit

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.

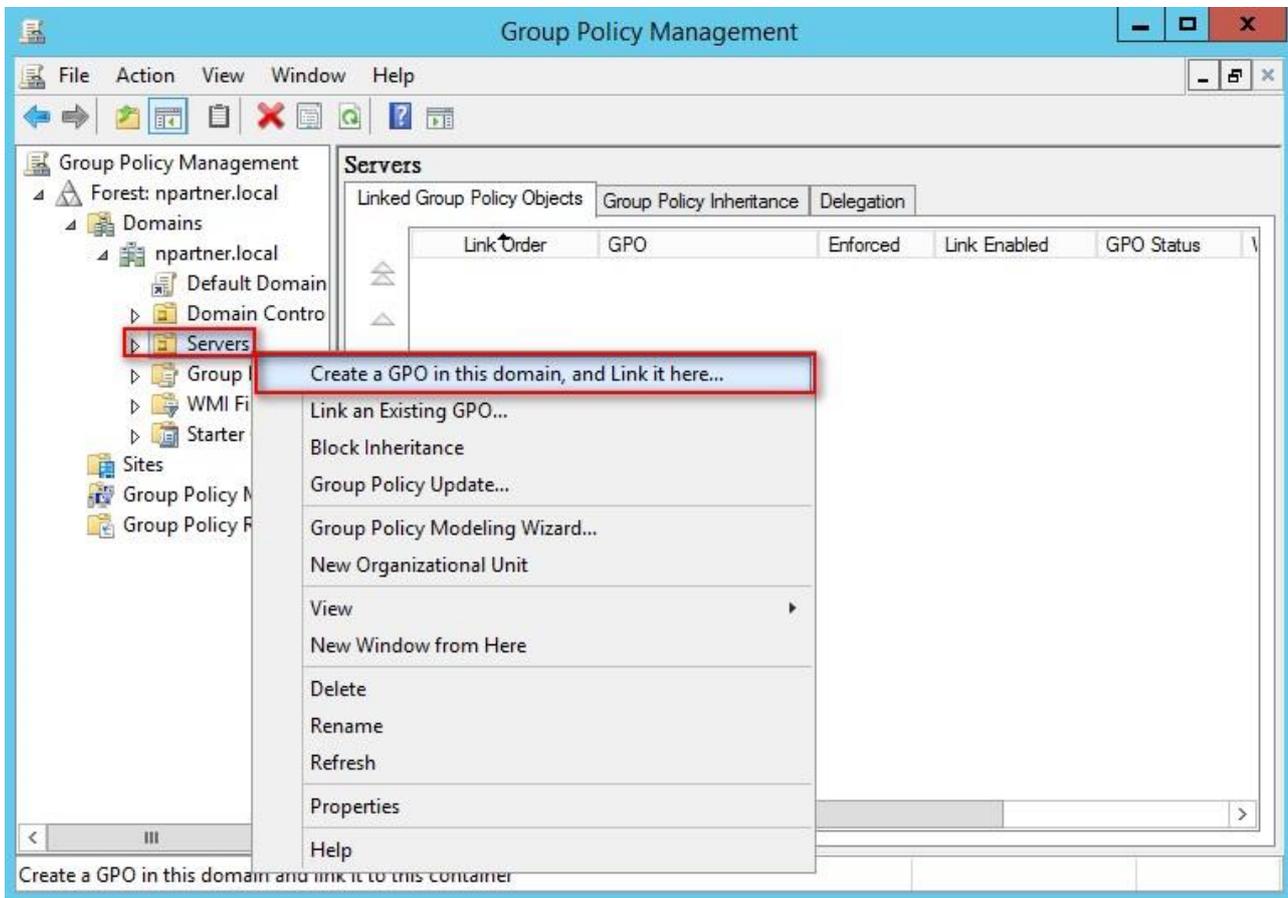


5.1.2 Group Policy Settings

(1) Open “Group Policy Management.”



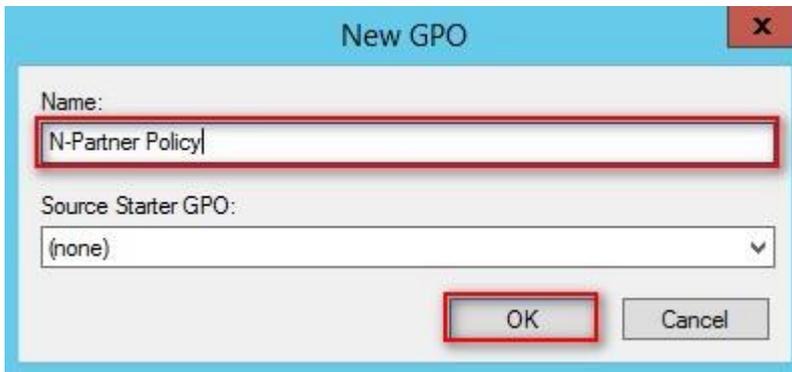
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

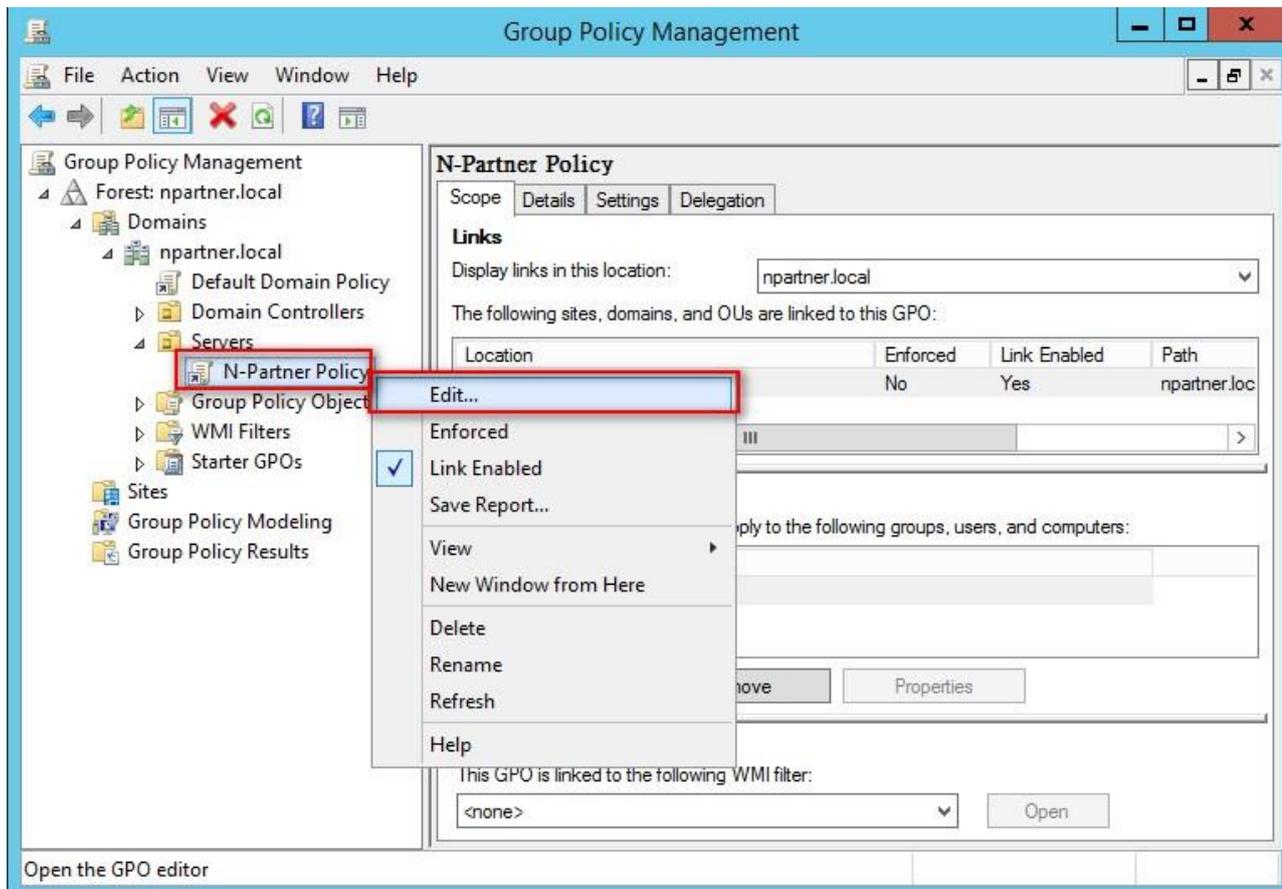
Enter your group policy object name (the example here is “N-Partner Policy”).

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



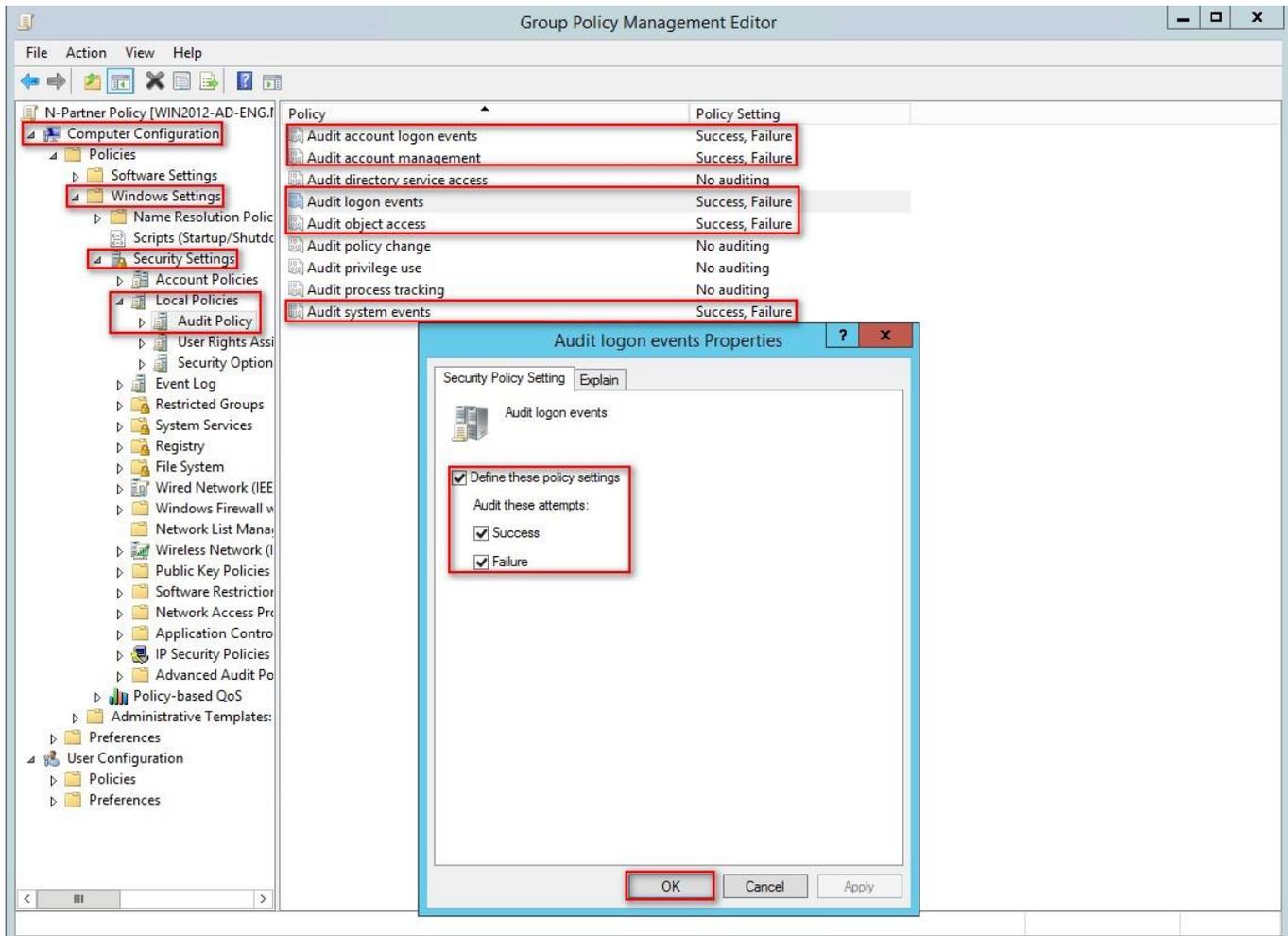
(4) Edit Your Group Policy Object

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.”

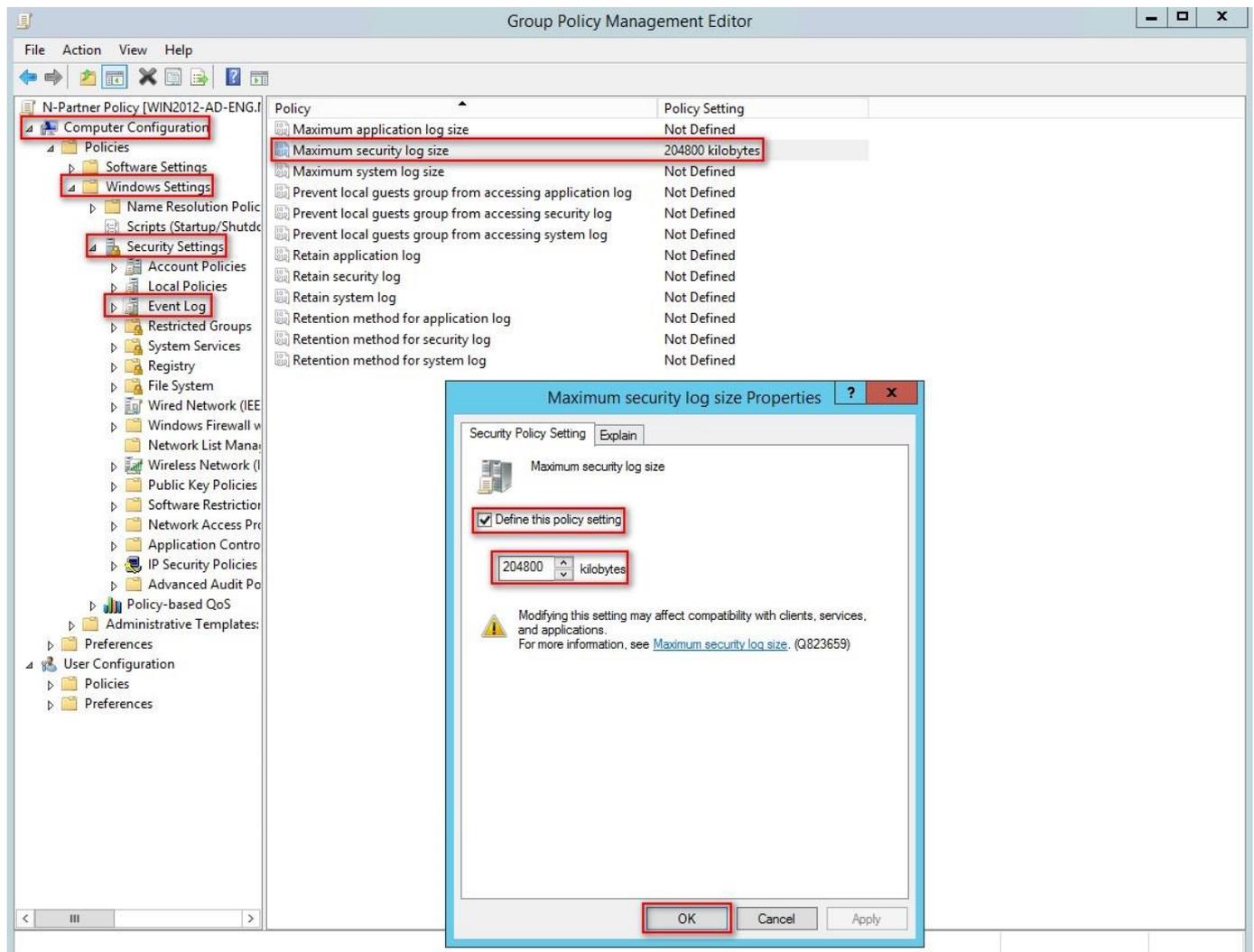


(6) Event Logs: Maximum Size of Security Log

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

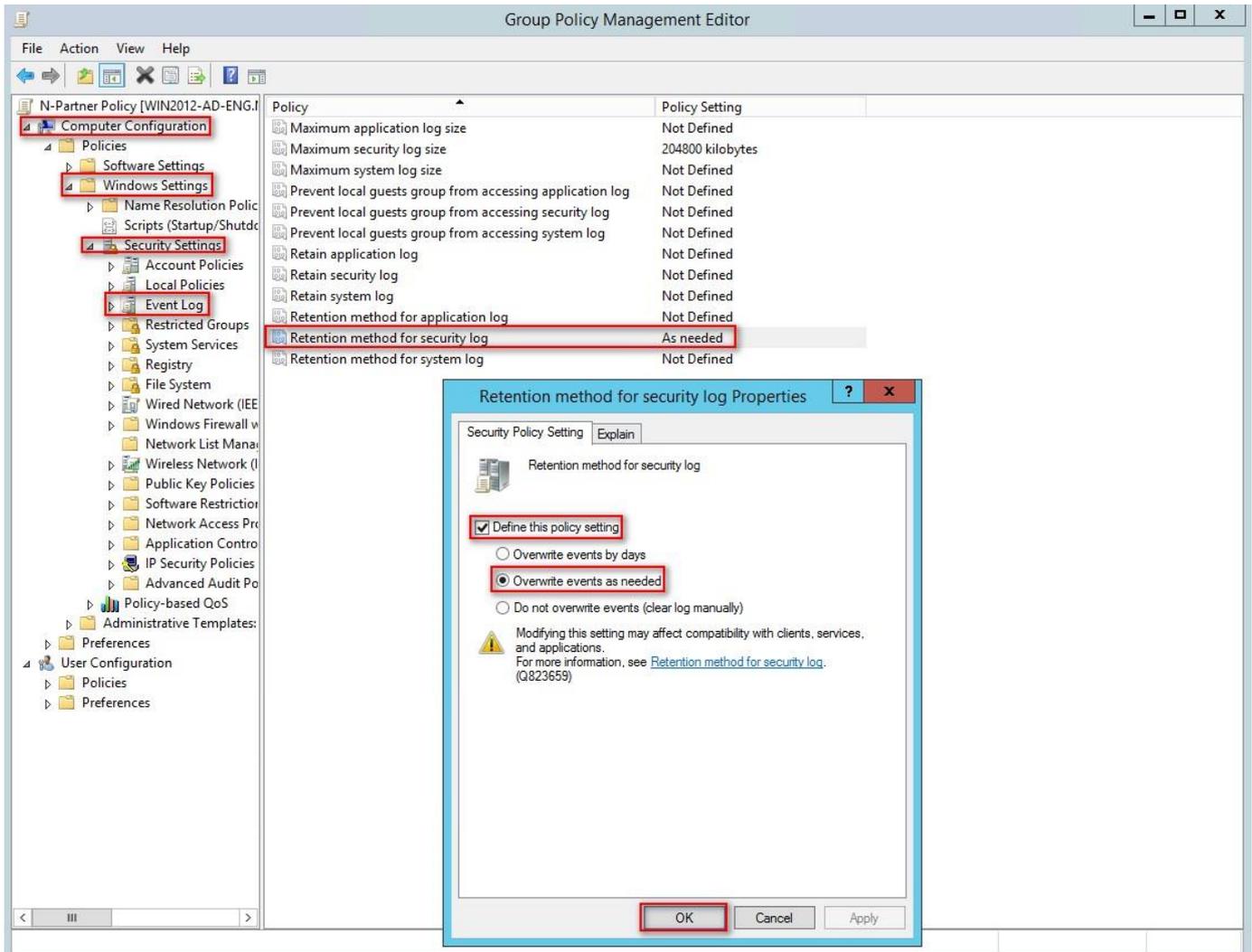
And click on “Maximum security log size” -> Check “Define this policy setting” -> Enter 204800 KB

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.

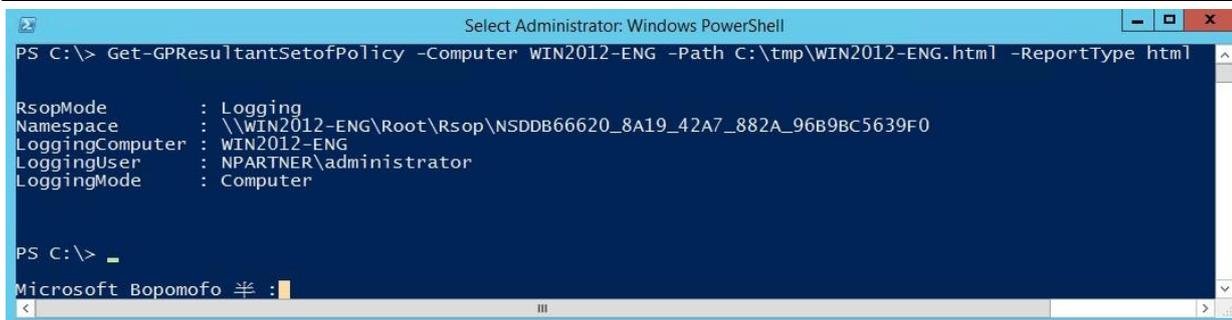
```
PS C:\> Invoke-GPUdate -Computer WIN2012-ENG -RandomDelayInMinutes 0 -Force
```



Please enter your Windows Server hostname in red text.

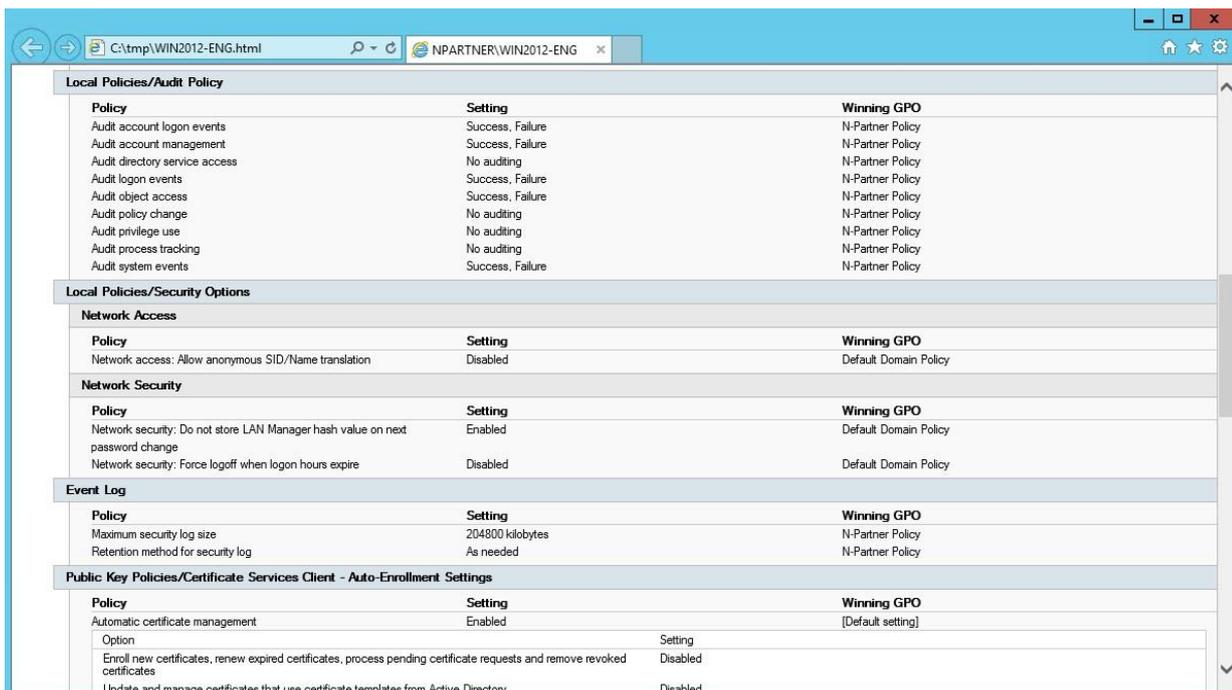
(10) Enter the command below to generate a report on Windows server group policy at the AD domain server.

```
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

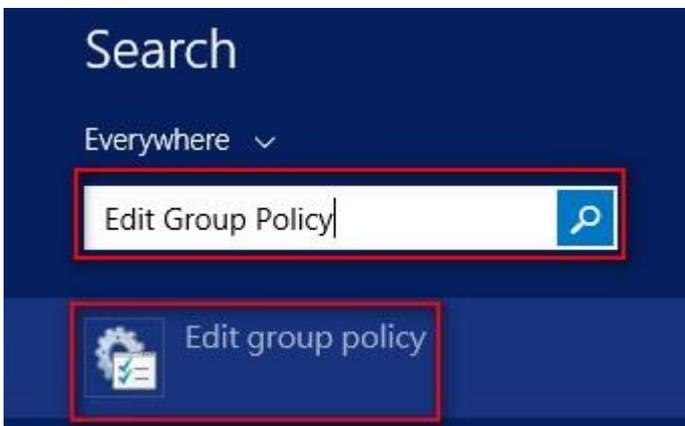
5.2.1 Audit Policy Settings

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



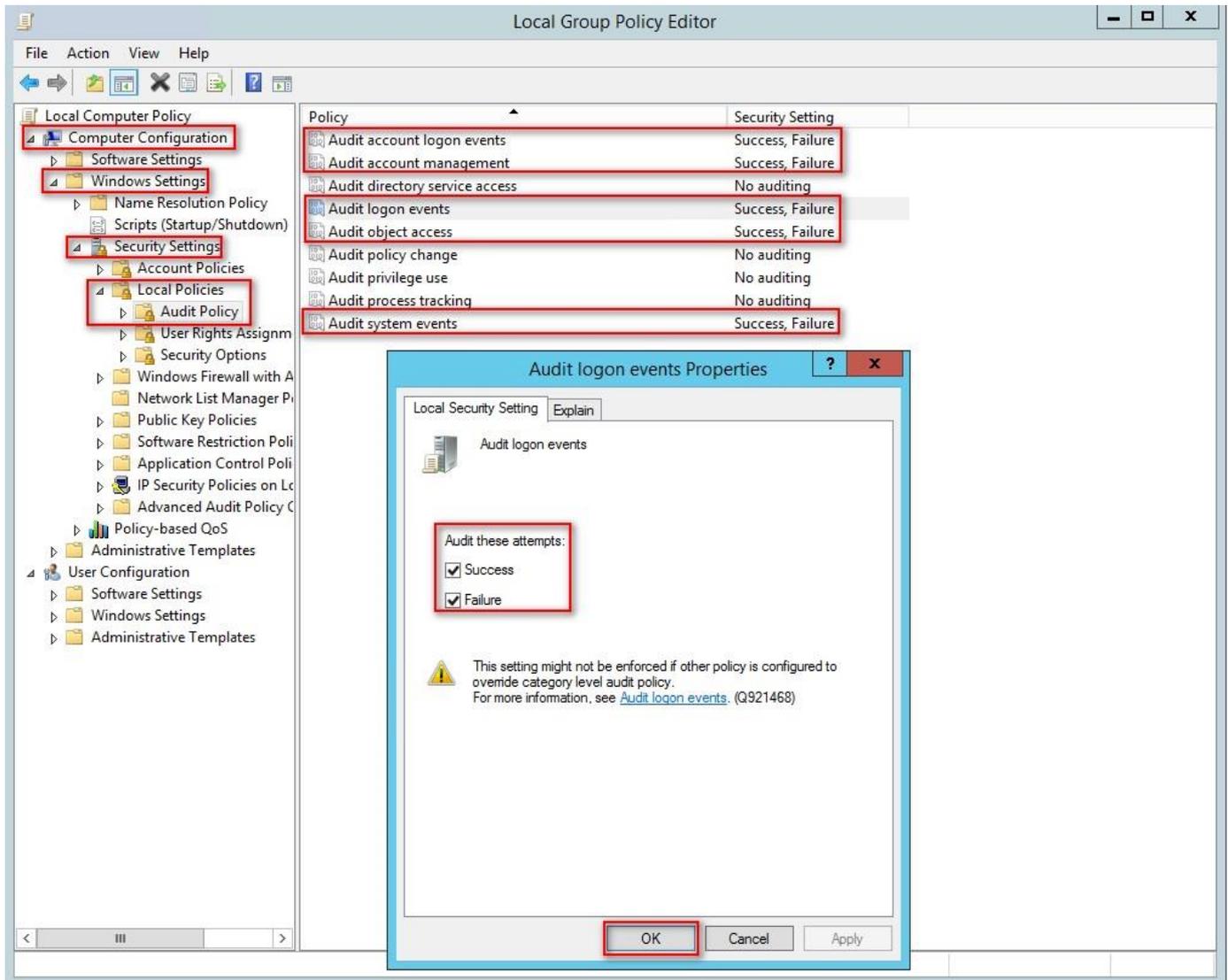
(2) Search for “Group Policy Object Editor”

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
```



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> gpupdate /force
Updating policy...

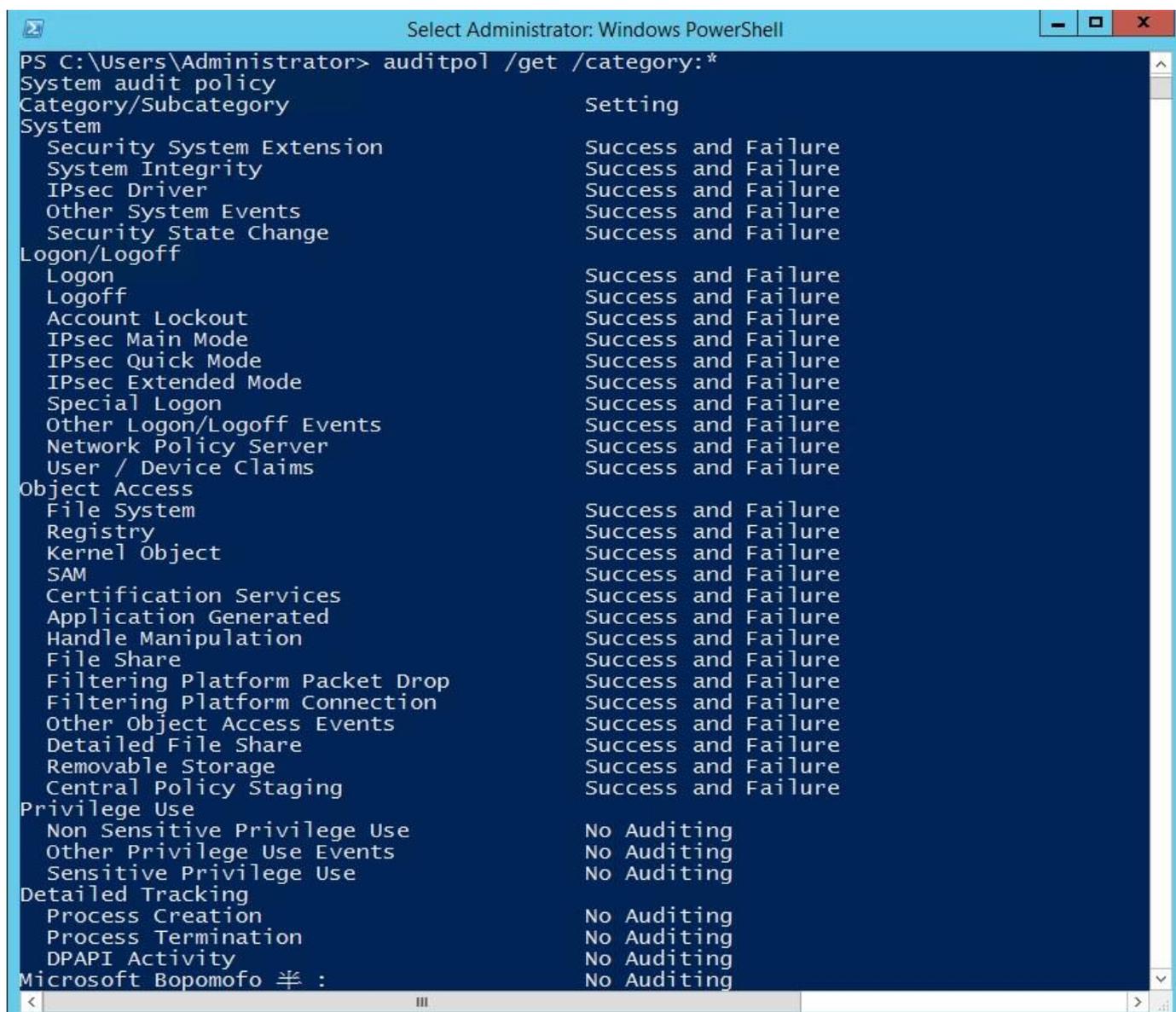
Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\Administrator> _

Microsoft Bopomofo 半 :
```

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

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



```
Select Administrator: Windows PowerShell
PS C:\Users\Administrator> auditpol /get /category:*
System audit policy
Category/Subcategory          Setting
System
  Security System Extension    Success and Failure
  System Integrity             Success and Failure
  IPsec Driver                 Success and Failure
  Other System Events          Success and Failure
  Security State Change        Success and Failure
Logon/Logoff
  Logon                        Success and Failure
  Logoff                       Success and Failure
  Account Lockout              Success and Failure
  IPsec Main Mode              Success and Failure
  IPsec Quick Mode             Success and Failure
  IPsec Extended Mode          Success and Failure
  Special Logon                Success and Failure
  Other Logon/Logoff Events     Success and Failure
  Network Policy Server        Success and Failure
  User / Device Claims         Success and Failure
Object Access
  File System                  Success and Failure
  Registry                     Success and Failure
  Kernel Object                Success and Failure
  SAM                          Success and Failure
  Certification Services       Success and Failure
  Application Generated         Success and Failure
  Handle Manipulation           Success and Failure
  File Share                    Success and Failure
  Filtering Platform Packet Drop Success and Failure
  Filtering Platform Connection Success and Failure
  Other Object Access Events    Success and Failure
  Detailed File Share           Success and Failure
  Removable Storage            Success and Failure
  Central Policy Staging        Success and Failure
Privilege Use
  Non Sensitive Privilege Use   No Auditing
  Other Privilege Use Events    No Auditing
  Sensitive Privilege Use       No Auditing
Detailed Tracking
  Process Creation              No Auditing
  Process Termination           No Auditing
  DPAPI Activity                No Auditing
Microsoft Bopomofo 半 :
```

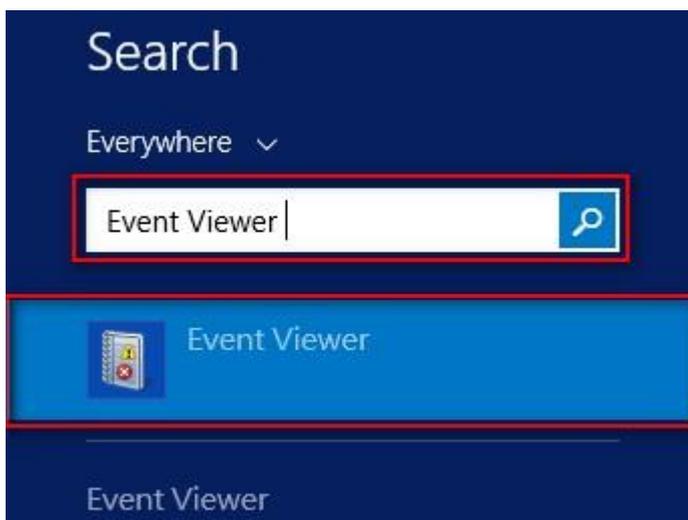
5.2.2 Event Log Settings

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



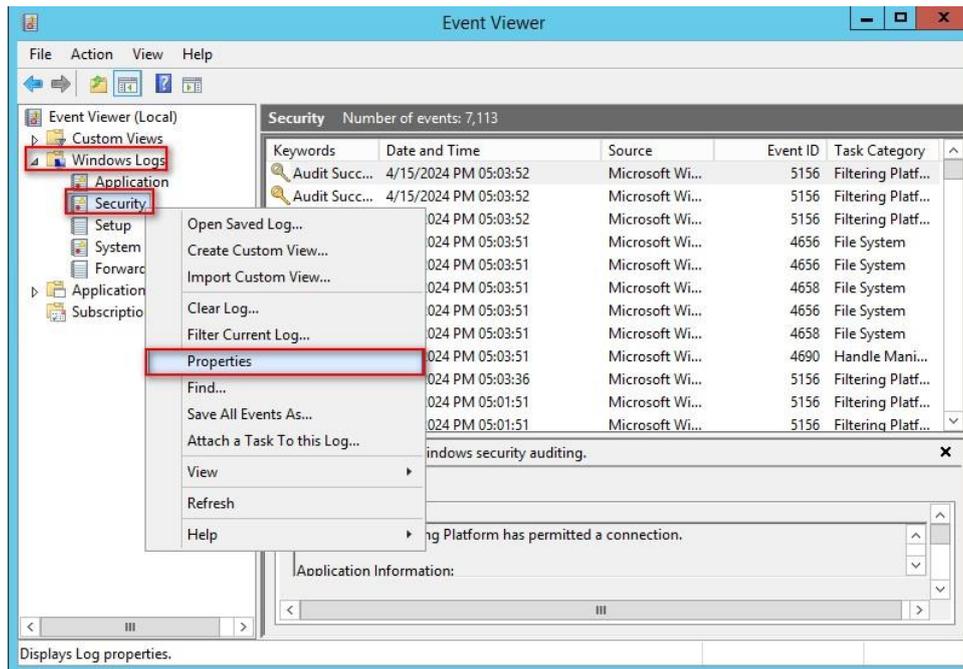
(2) Search for “Group Policy Object Editor”

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.”

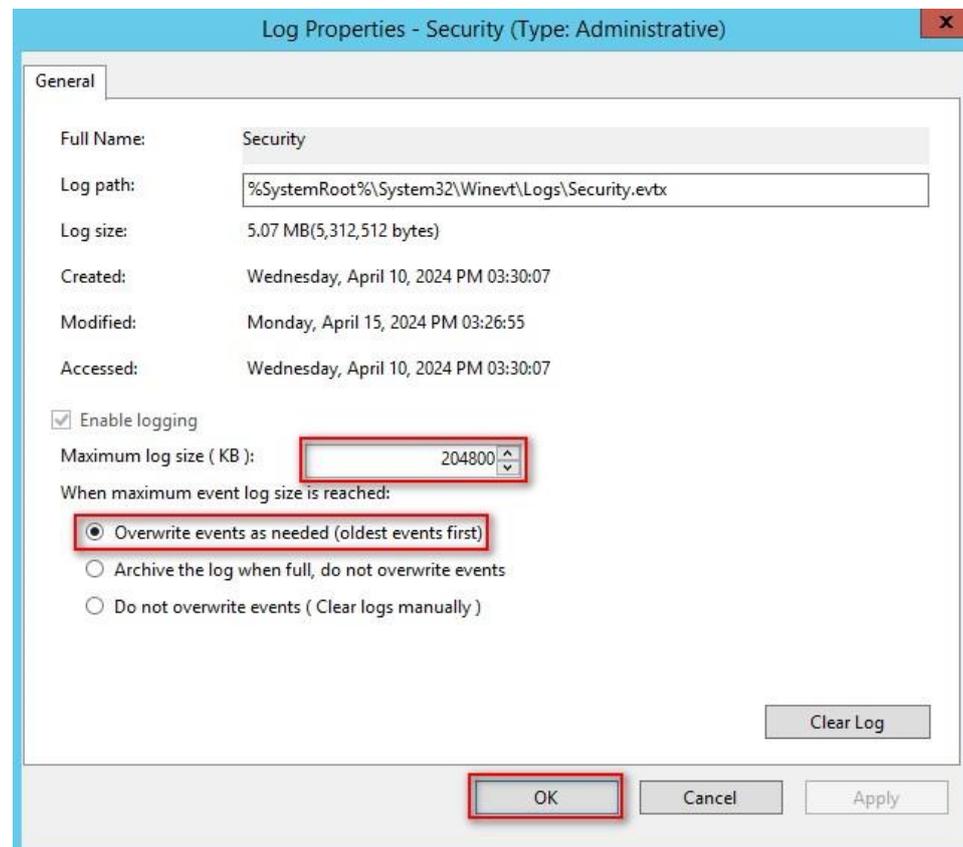


(4) Configure Security Log

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 Recommendation link provided in preface for detailed explanations.

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

6.1 Domain

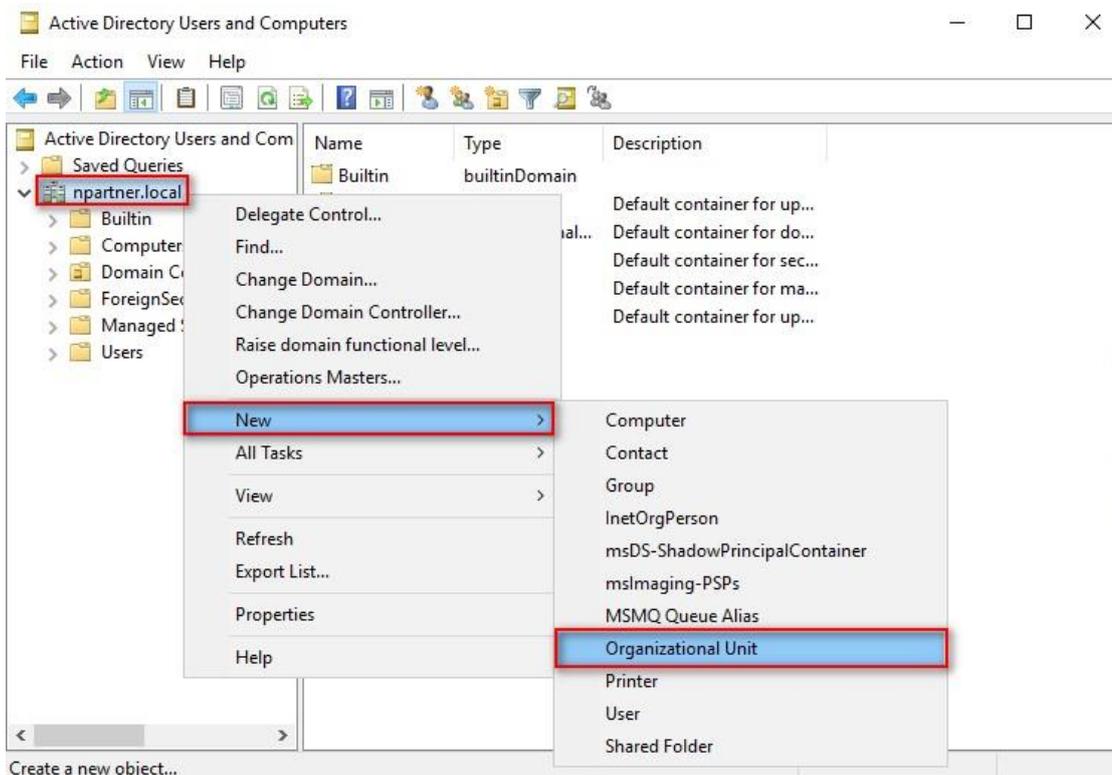
6.1.1 Organizational Unit Setup

(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.”

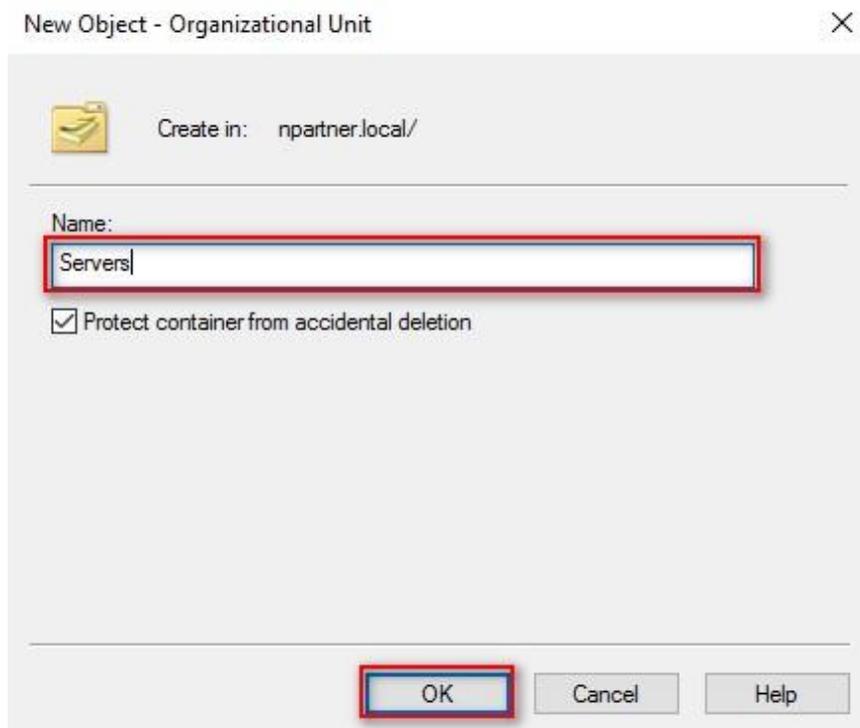


(3) Name Your Organizational Unit

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

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

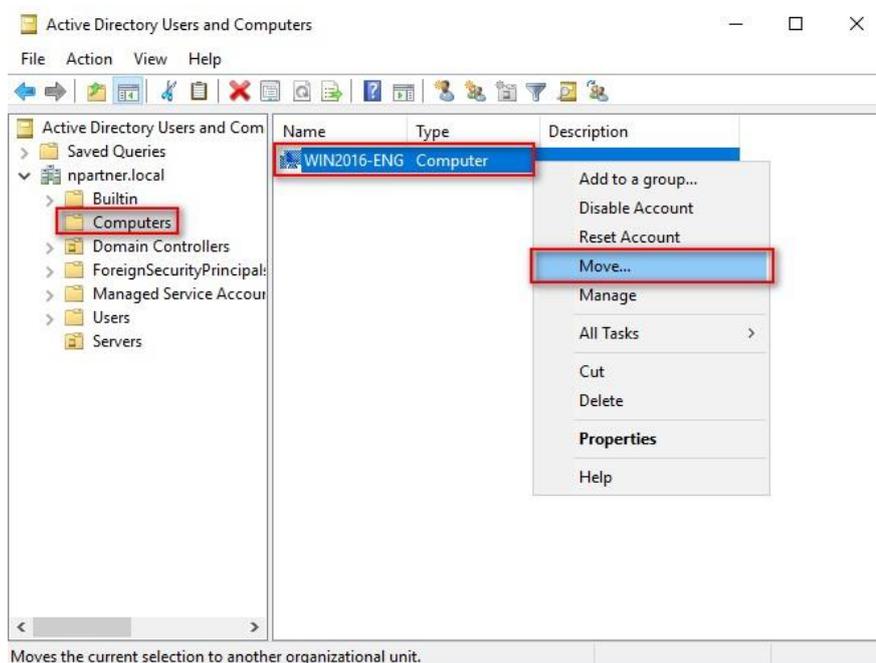
-> and click "OK."



(4) Move Your Server to New Organizational Unit

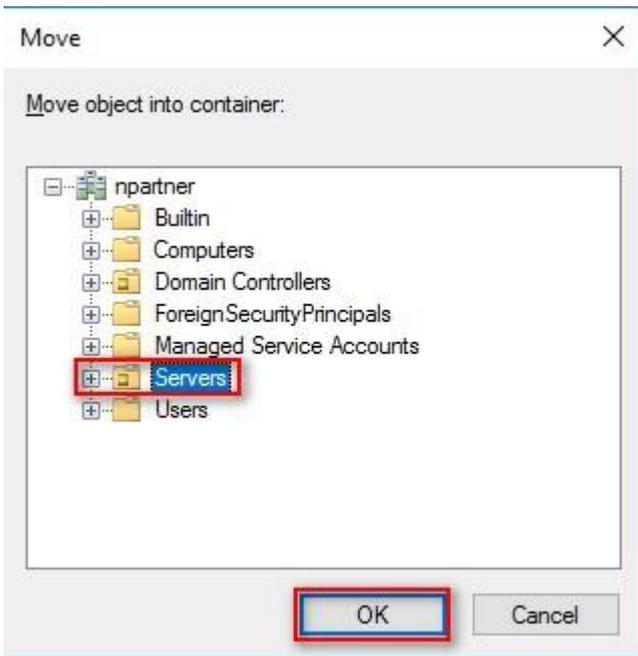
Select your organizational unit (the example here is "Computers") -> Right-click on the "WIN2016-ENG" server.

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



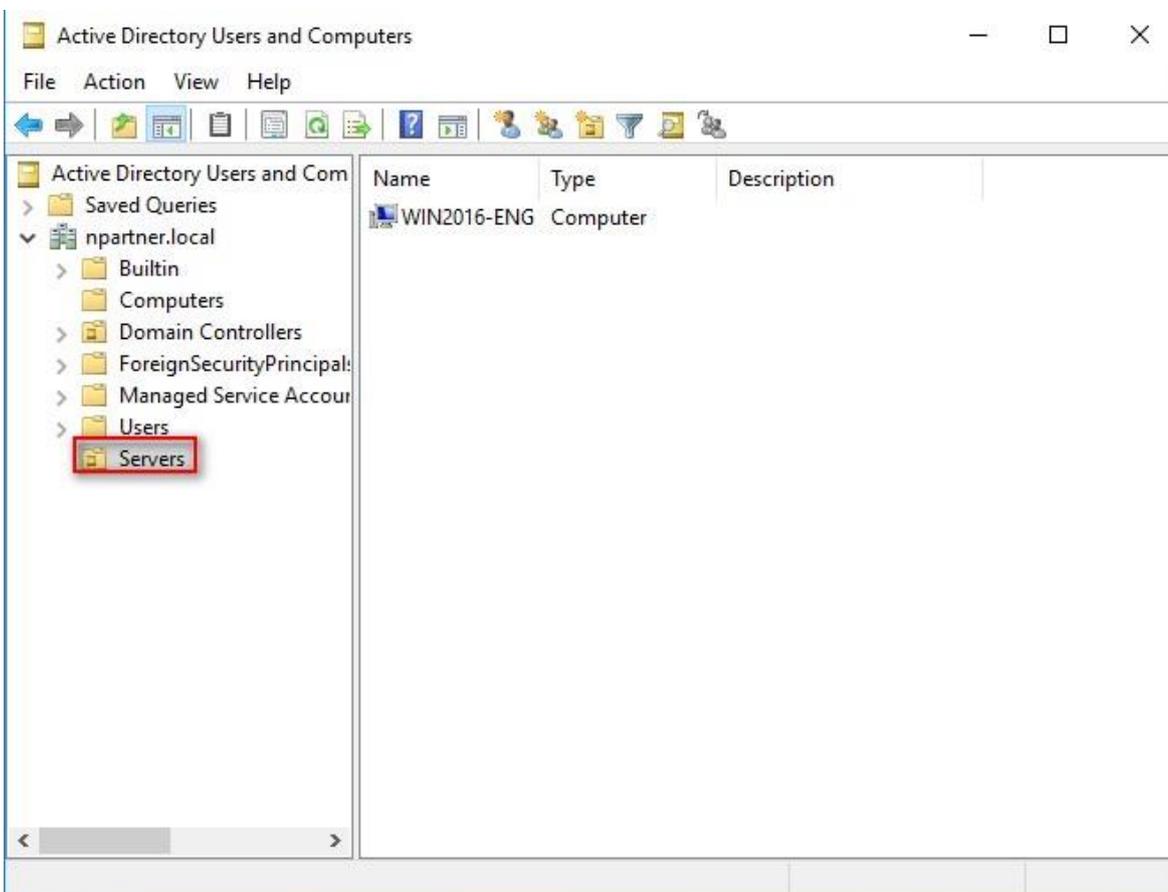
(5) Select Your Organizational Unit

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.

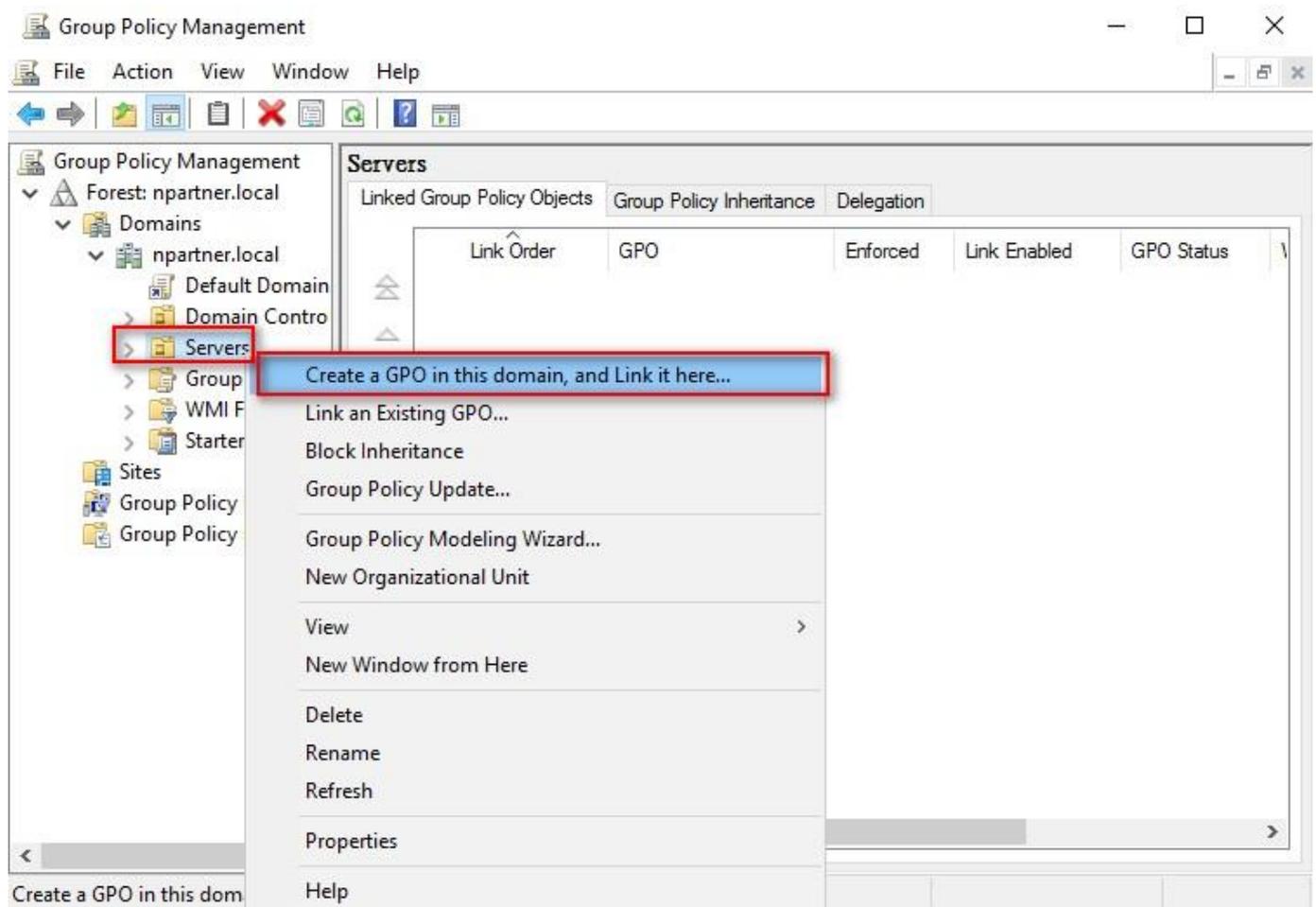


6.1.2 Group Policy Settings

(1) Open “Group Policy Management.”



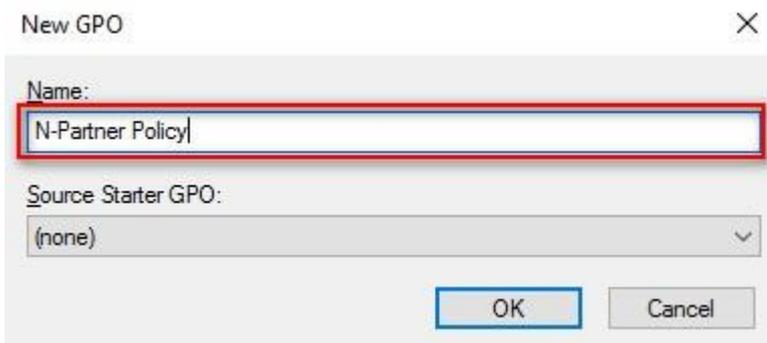
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

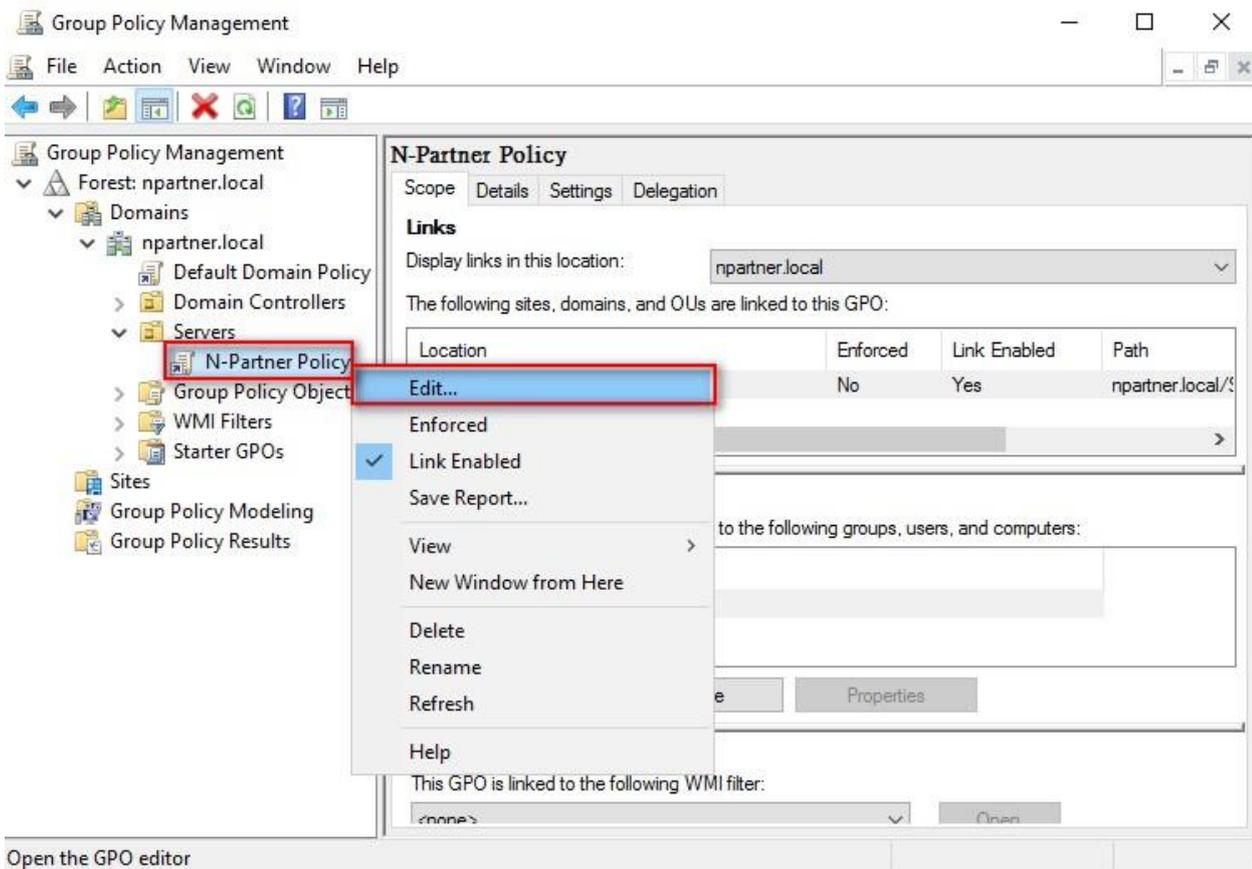
Enter your group policy object name (the example here is “N-Partner Policy”).

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



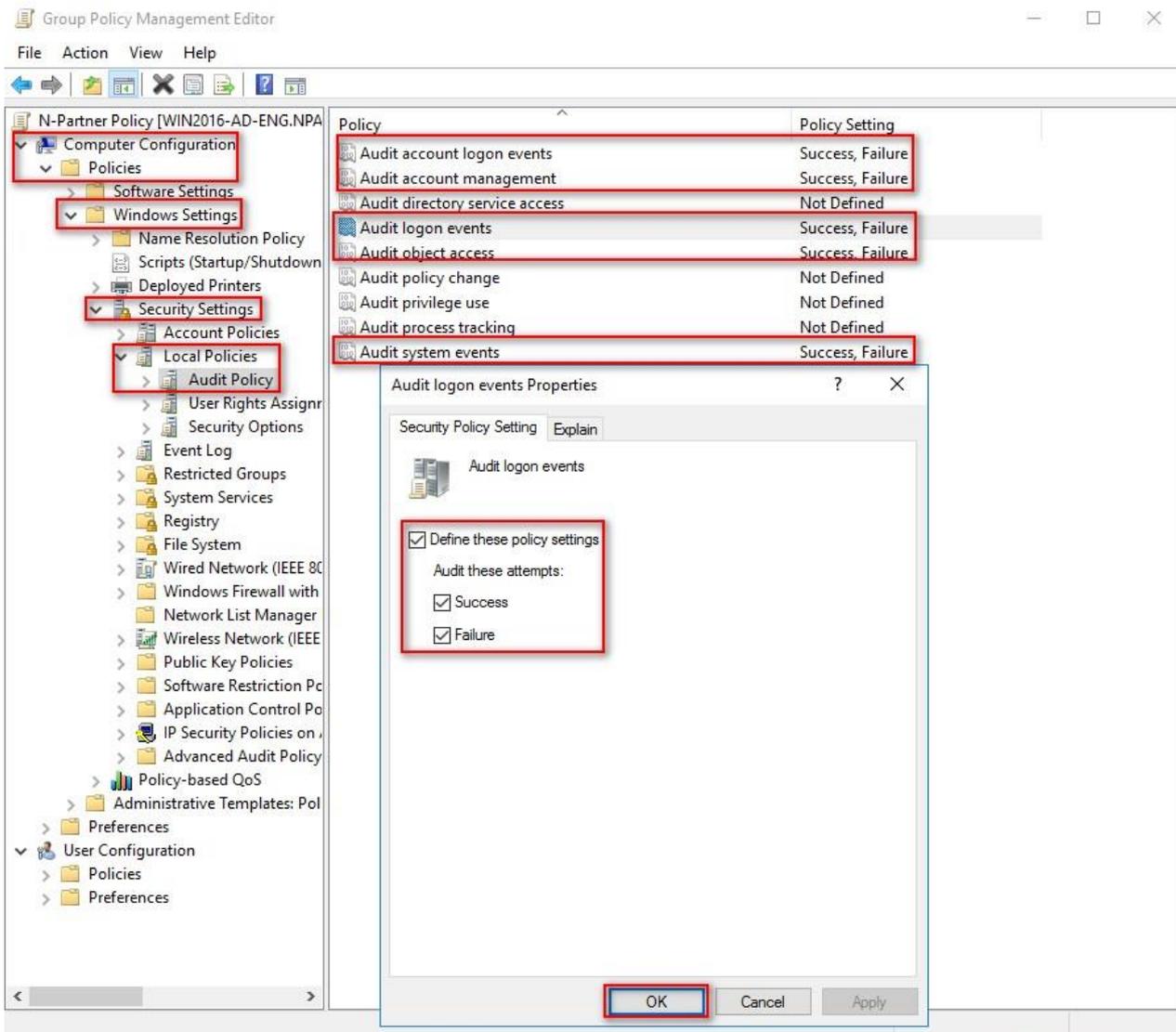
(4) Edit Your Group Policy Object

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

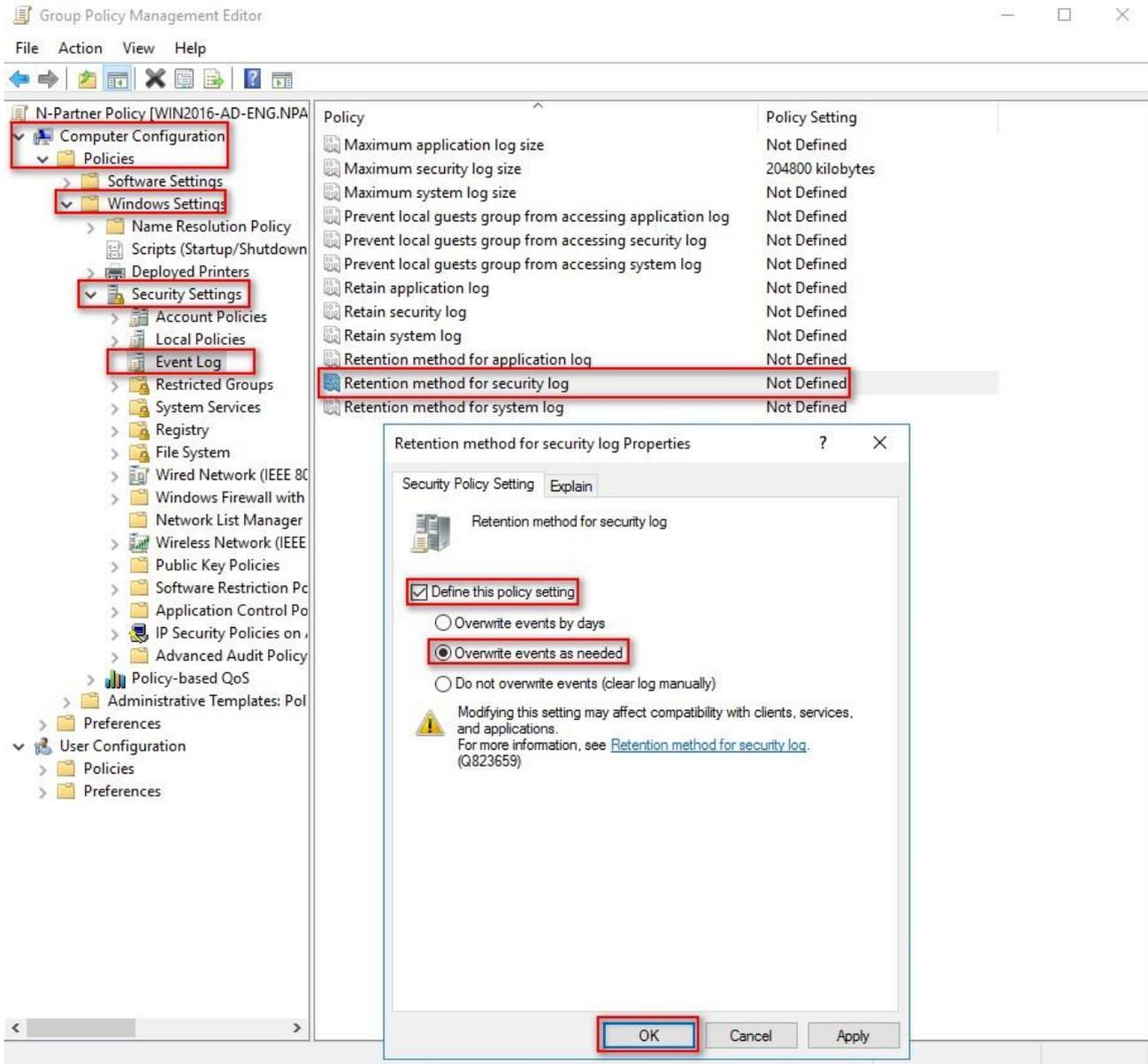
Note: Please adjust the number based on the actual environment. -> Click [OK].

The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows the tree structure: Computer Configuration > Windows Settings > Security Settings > Event Log. The 'Maximum security log size' policy is selected and highlighted in the main pane. A red box highlights the '204800 kilobytes' value in the policy list. A secondary dialog box titled 'Maximum security log size Properties' is open, showing the 'Define this policy setting' checkbox checked and the value '204800 kilobytes' entered in the text field. A red box highlights the 'OK' button at the bottom of this dialog. A warning message is visible in the dialog: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see [Maximum security log size](#). (Q823659)'. The background table lists other policies such as 'Maximum application log size', 'Maximum system log size', and various retention methods, all currently set to 'Not Defined'.

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

(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.”

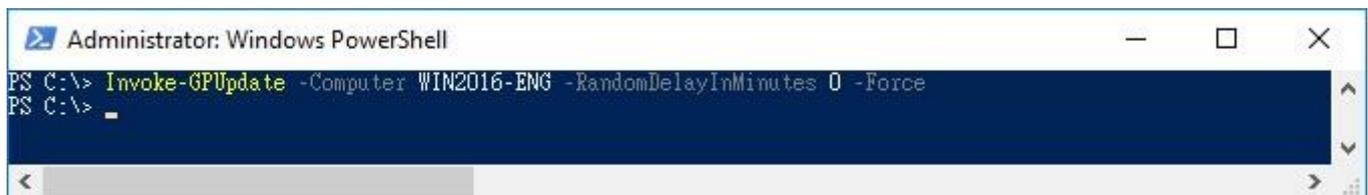


(8) Open “Windows PowerShell” on your Windows server.



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

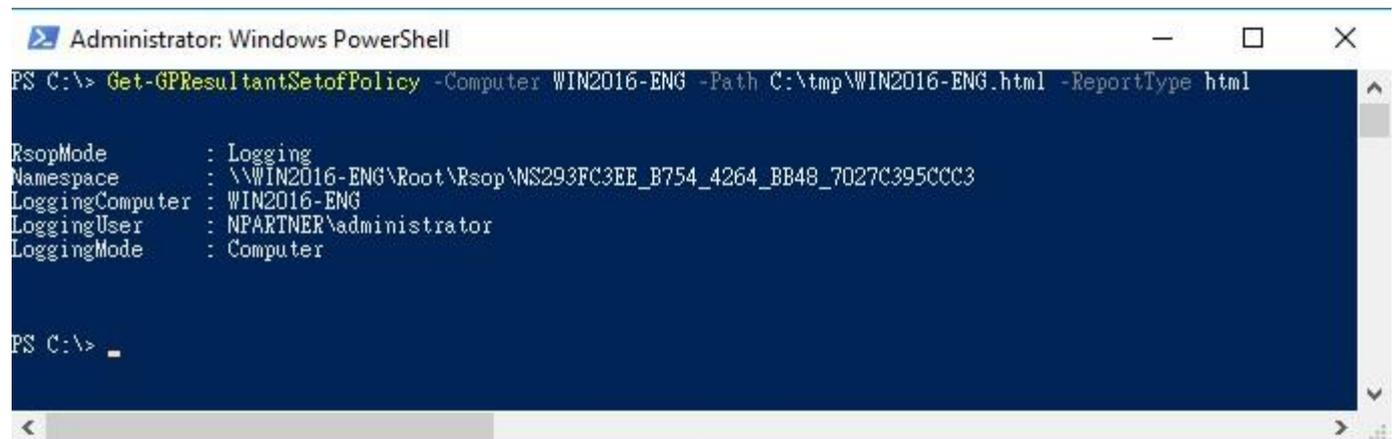
```
PS C:\> Invoke-GPUdate -Computer WIN2016-ENG -RandomDelayInMinutes 0 -Force
```



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.

The screenshot shows a web browser window with the address bar displaying 'C:\tmp\WIN2016-ENG.html' and 'NPARTNER\WIN2016-ENG'. The page content is as follows:

Domain: npartner.local
Site: Default-First-Site-Name
Organizational Unit: npartner.local/Servers
Security Group Membership: show

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	738 Millisecond(s)	4/16/2024 AM 11:40:12	View Log
Registry	Success	16 Millisecond(s)	4/16/2024 AM 11:40:12	View Log
Security	Success	313 Millisecond(s)	4/16/2024 AM 11:40:12	View Log

Settings

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy

Account Policies/Account Lockout Policy

Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy

Local Policies/Audit Policy

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

Local Policies/Security Options

Network Access

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.”

The screenshot shows the Local Group Policy Editor window. The left pane shows the tree view with the following folders expanded: Computer Configuration, Windows Settings, Security Settings, and Local Policies. The 'Audit Policy' folder is selected. The right pane shows a list of policies with their corresponding security settings:

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

The 'Audit logon events Properties' dialog box is open, showing the 'Local Security Setting' tab. The 'Audit logon events' icon is displayed. Below it, the 'Audit these attempts:' section has two checked checkboxes: 'Success' and 'Failure'. A warning icon and text are visible at the bottom of the dialog:

Warning: This setting might not be enforced if other policy is configured to override category level audit policy. For more information, see [Audit logon events](#). (Q921468)

The 'OK' button is highlighted with a red box.

(3) Open “Windows PowerShell.”



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

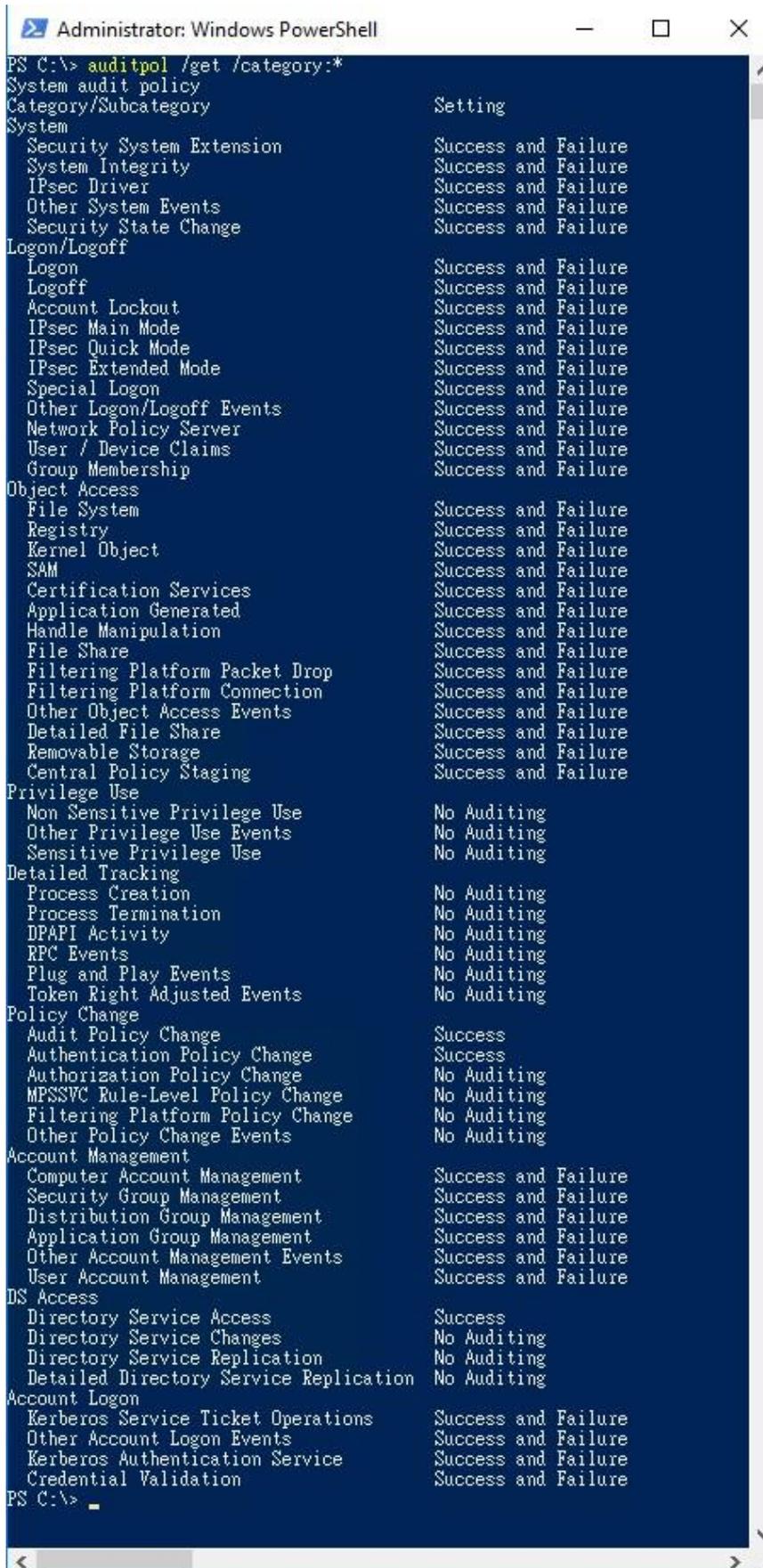
```
PS C:\> gpupdate /force
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The command prompt shows "PS C:\> gpupdate /force" with the output "Updating policy...". Below that, it says "Computer Policy update has completed successfully." and "User Policy update has completed successfully." The prompt then shows "PS C:\> _" with a cursor. The terminal has a dark blue background and a scroll bar on the right side.

```
Administrator: Windows PowerShell  
PS C:\> gpupdate /force  
Updating policy...  
Computer Policy update has completed successfully.  
User Policy update has completed successfully.  
PS C:\> _
```

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

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

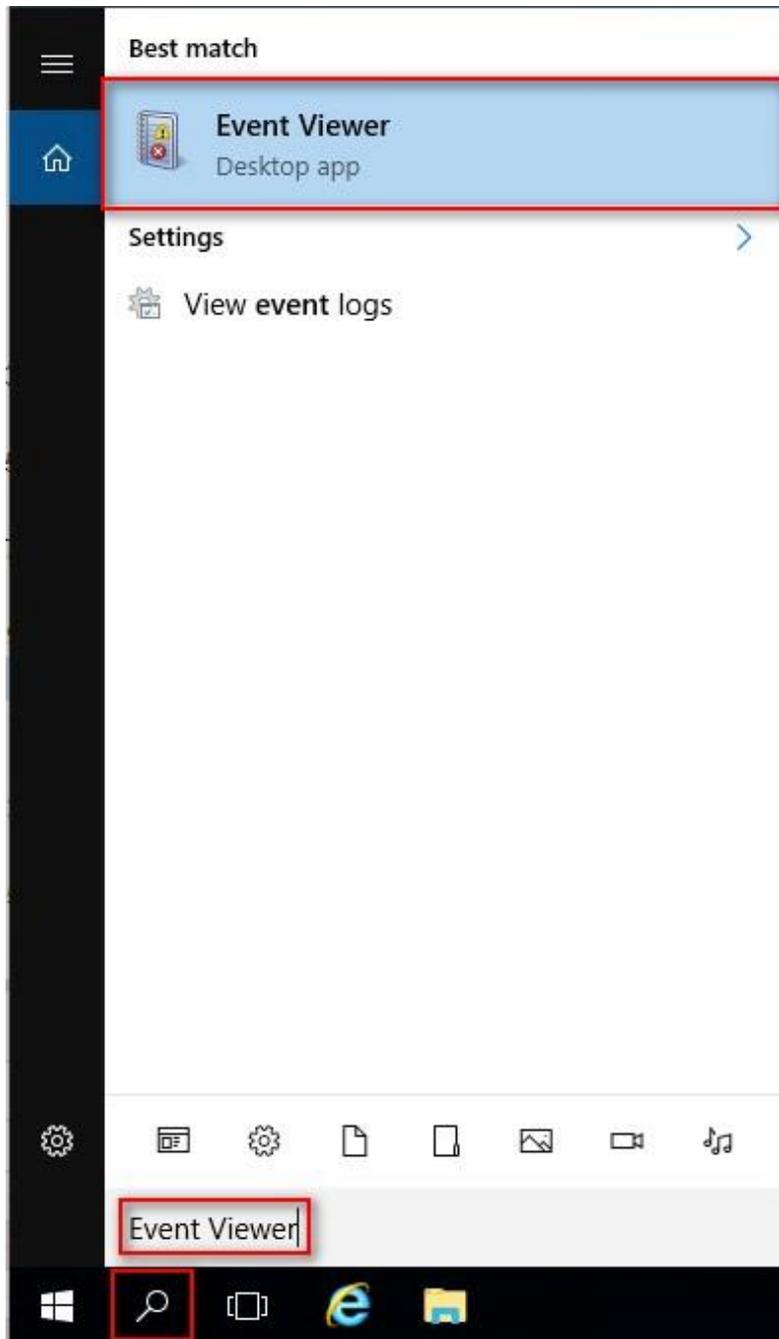


```
Administrator: Windows PowerShell
PS C:\> auditpol /get /category:*
System audit policy
Category/Subcategory      Setting
System
Security System Extension  Success and Failure
System Integrity           Success and Failure
IPsec Driver               Success and Failure
Other System Events       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

6.2.2 Event Log Settings

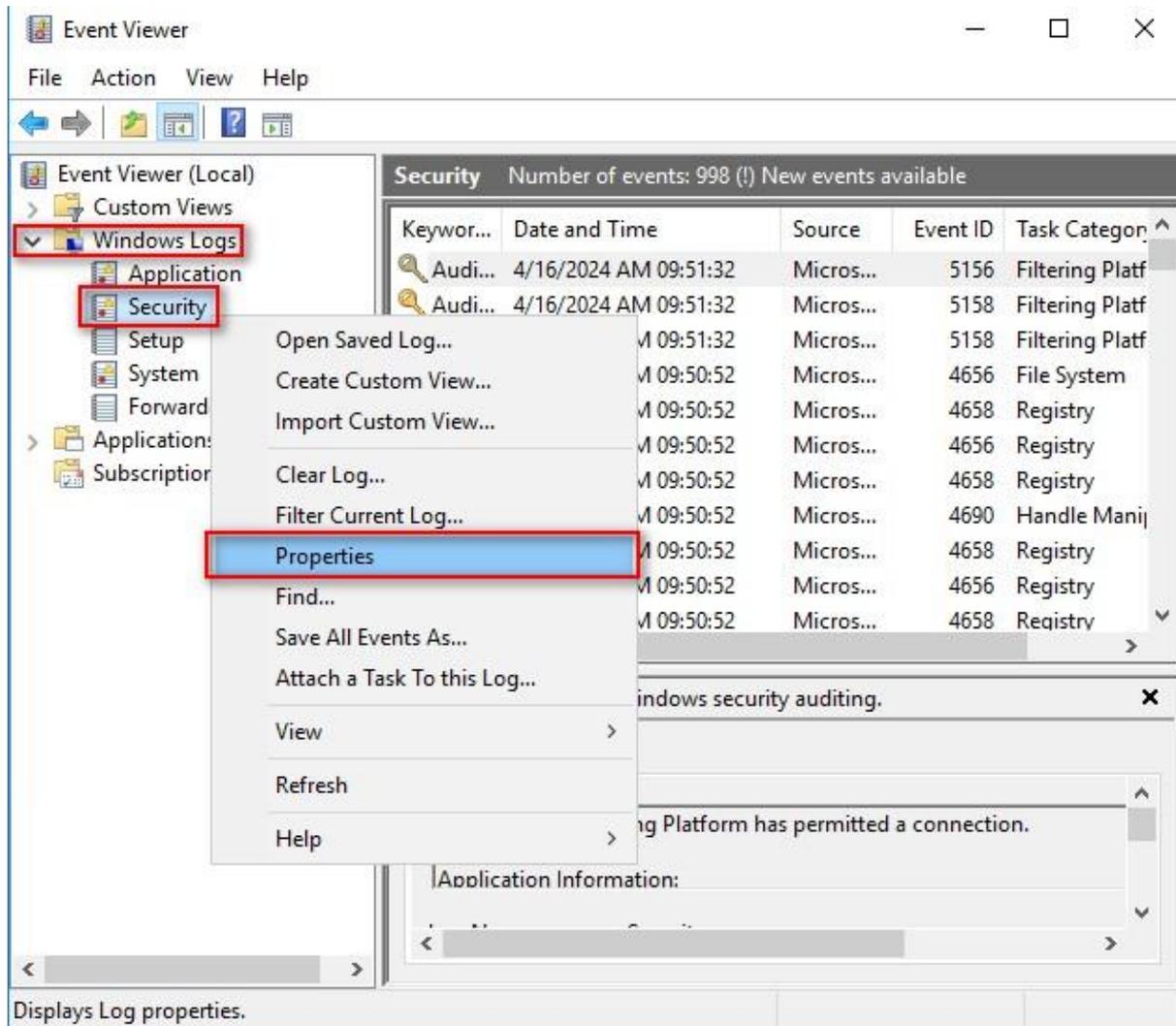
(1) Search for “Group Policy Object Editor”

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."

Log Properties - Security (Type: Administrative) X

General

Full Name: Security

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

Log size: 1.07 MB(1,118,208 bytes)

Created: Wednesday, April 10, 2024 PM 07:44:35

Modified: Tuesday, April 16, 2024 AM 09:32:14

Accessed: Wednesday, April 10, 2024 PM 07:44:35

Enable logging

Maximum log size (KB): 204800

When maximum event log size is reached:

Overwrite events as needed (oldest events first)

Archive the log when full, do not overwrite events

Do not overwrite events (Clear logs manually)

Clear Log

OK Cancel Apply

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

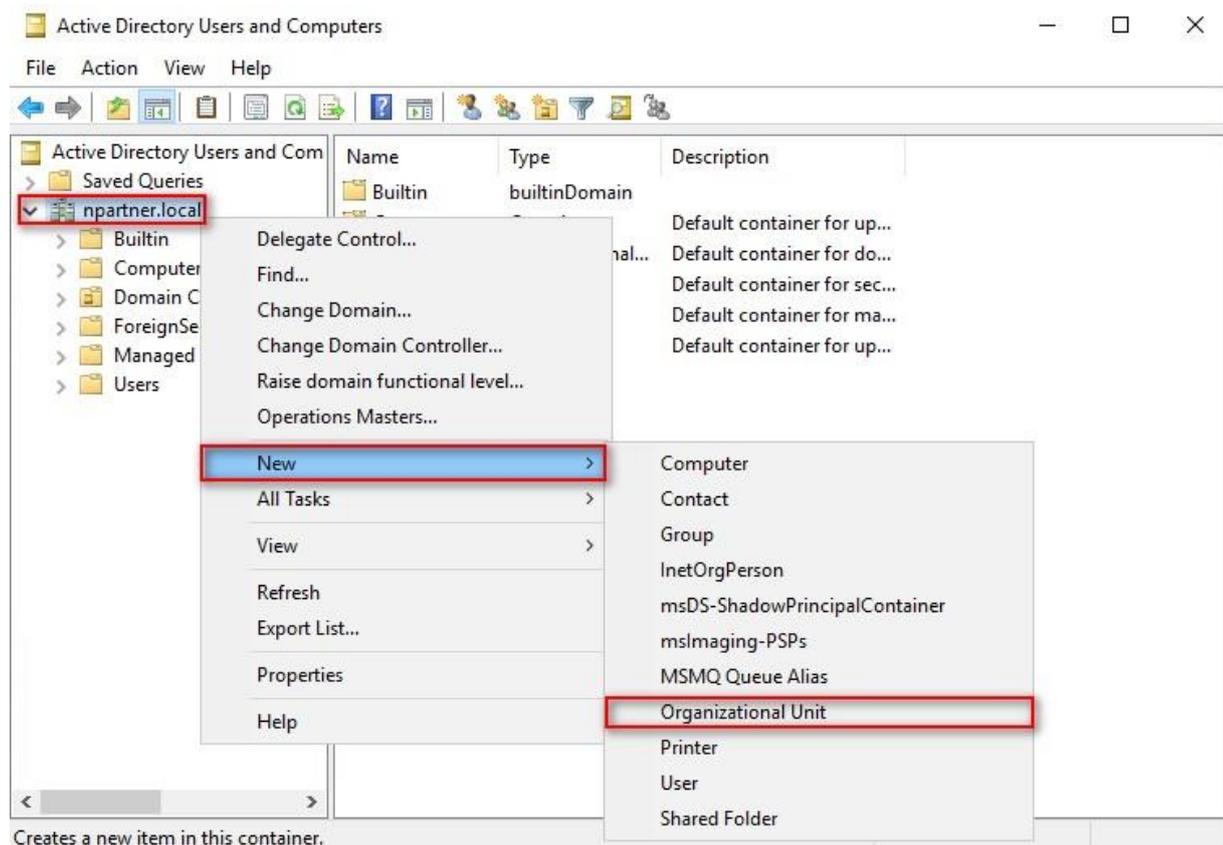
7.1.1 Organizational Unit Setup

(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.”

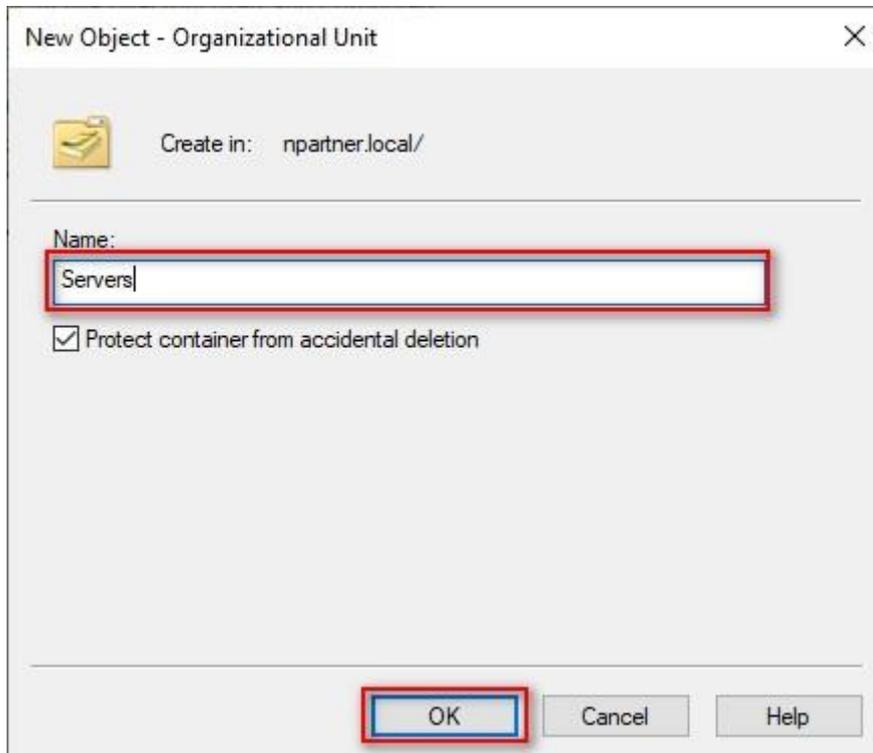


(3) Name Your Organizational Unit

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."



New Object - Organizational Unit

Create in: npartner.local/

Name:
Servers

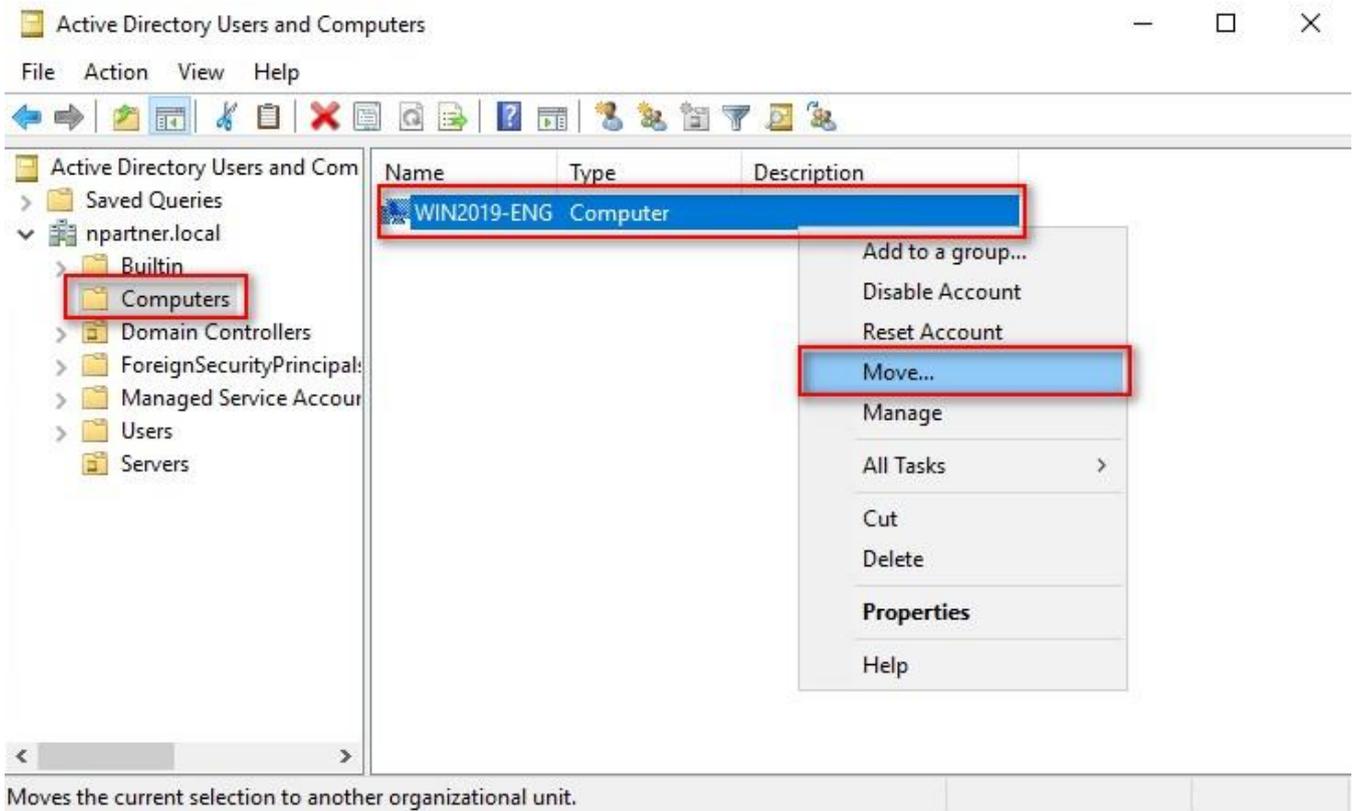
Protect container from accidental deletion

OK Cancel Help

(4) Move Your Server to New Organizational Unit

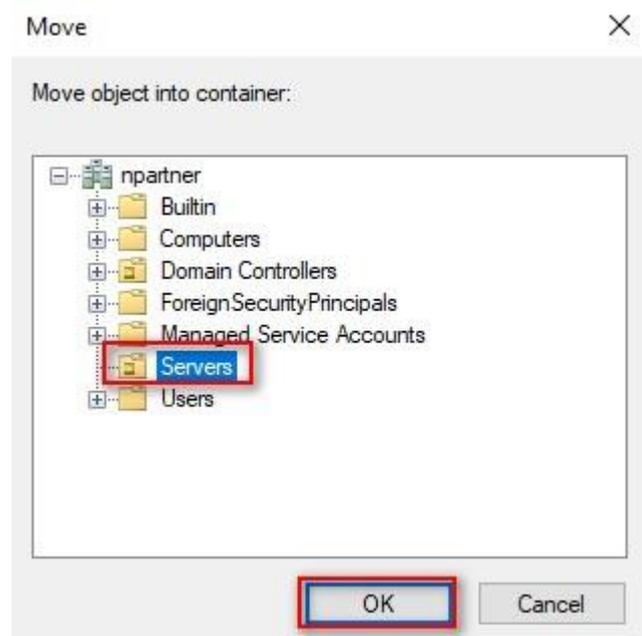
Select your organizational unit (the example here is “Computers”) -> Right-click on the “WIN2019-ENG” server.

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



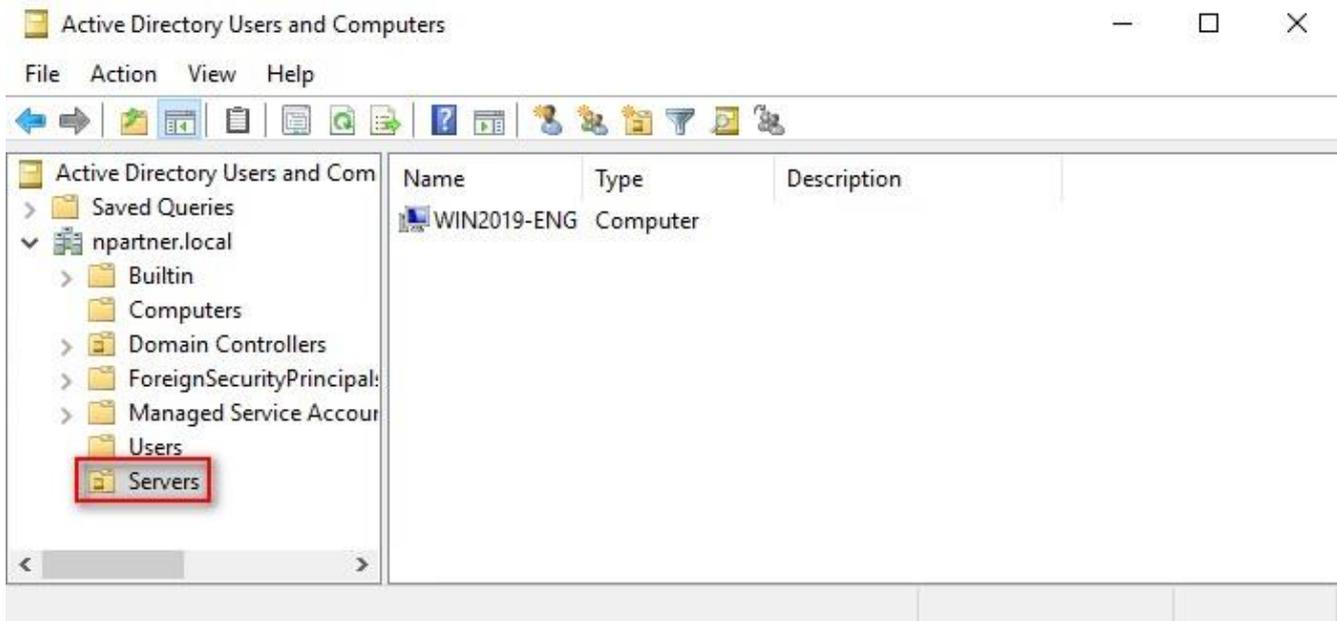
(5) Select Your Organizational Unit

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.

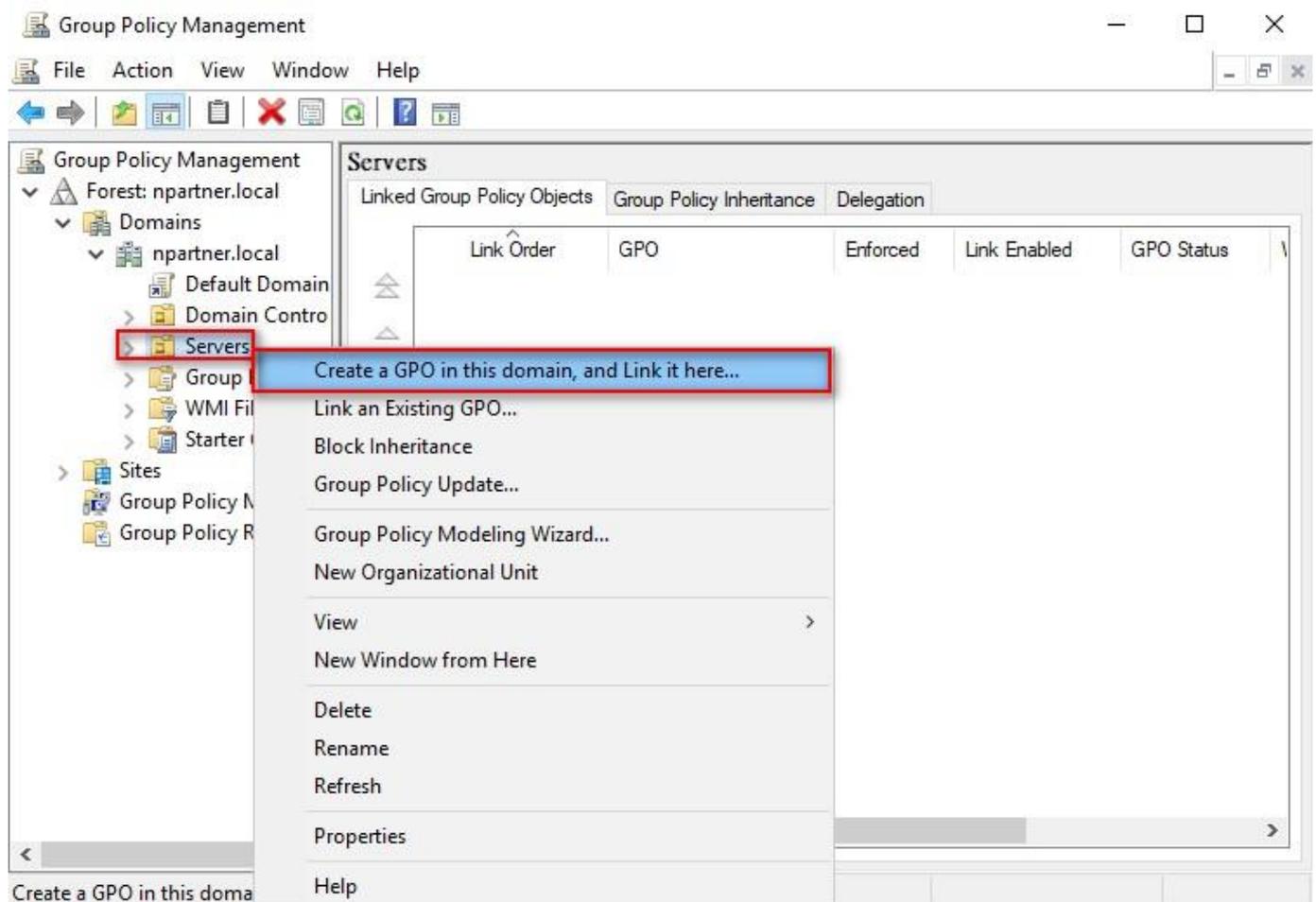


7.1.2 Group Policy Settings

(1) Open “Group Policy Management.”



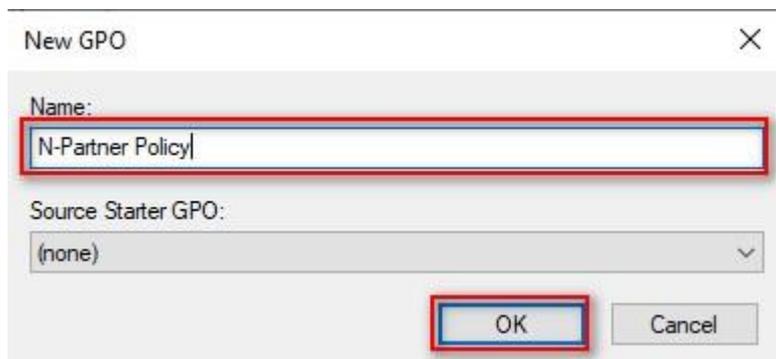
(2) Select your organizational unit (the example here is “Servers”) and right-click on “Create a GPO in this domain and Link it here...”.



(3) Name Your Group Policy Object

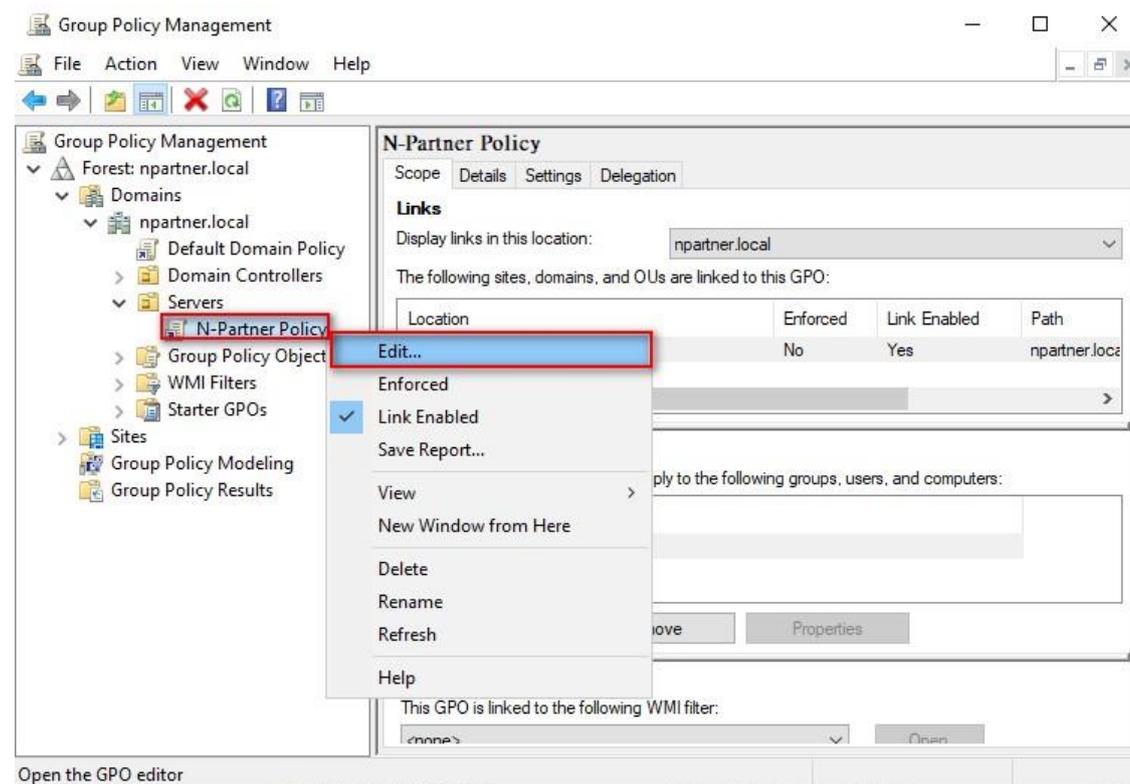
Enter your group policy object name (the example here is “N-Partner Policy”).

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



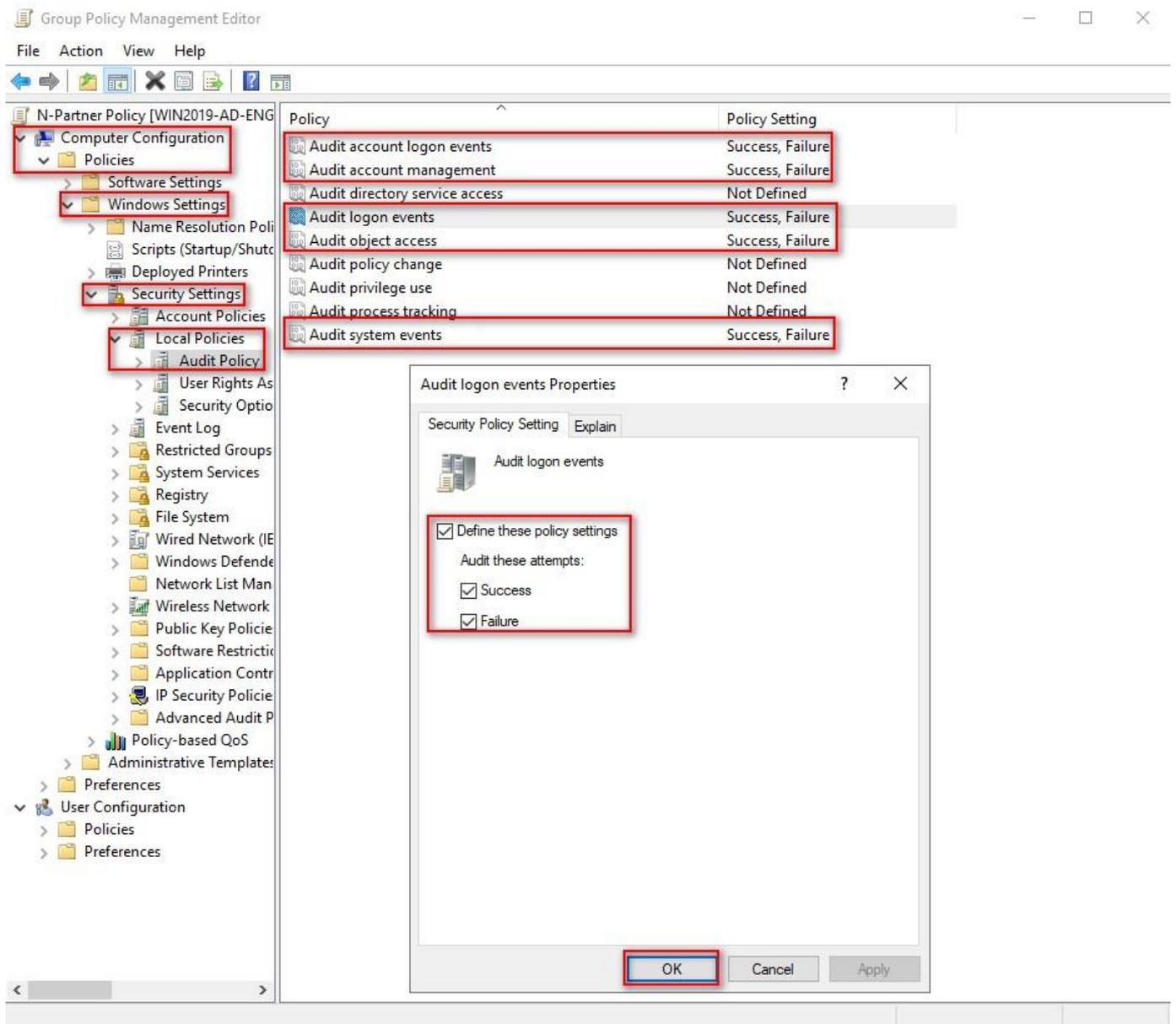
(4) Edit Your Group Policy Object

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.”

The screenshot displays the Group Policy Management Editor interface. The left-hand navigation pane shows the tree structure: Computer Configuration > Policies > Windows Settings > Security Settings > Event Log. The right-hand pane shows a list of policies, with 'Maximum security log size' selected and its value set to '204800 kilobytes'. A 'Maximum security log size Properties' dialog box is open in the foreground, showing the 'Define this policy setting' checkbox checked and the value '204800 kilobytes' entered in the spin box. A warning message is visible: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see [Maximum security log size. \(Q823659\)](#)'. The 'OK' button is highlighted at the bottom of the dialog.

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

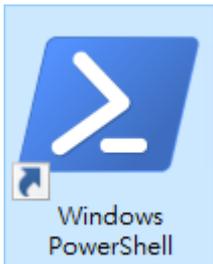
(7) Event Logs: Retention Method for Security Log

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.”

The screenshot shows the Group Policy Management Editor window. The left-hand navigation pane is expanded to show the following path: Computer Configuration > Policies > Windows Settings > Security Settings > Event Log. The 'Retention method for security log' policy is selected and highlighted in the main pane. The 'Policy Setting' column shows it is currently 'As needed'. A 'Retention method for security log Properties' dialog box is open in the foreground. In this dialog, the 'Define this policy setting' checkbox is checked. Underneath, the 'Overwrite events as needed' radio button is selected. A warning icon and text are visible at the bottom of the dialog, stating: 'Modifying this setting may affect compatibility with clients, services, and applications. For more information, see [Retention method for security log](#). (Q823659)'. The 'OK' button at the bottom of the dialog is highlighted with a red box.

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

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



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

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

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Invoke-GPUdate -Computer WIN2019-ENG -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt `PS C:\>` is visible before and after the command. The terminal background is dark blue with white text.

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
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Get-GPResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\WIN2019-ENG.html -ReportType html` being entered and executed. The output of the command is displayed as follows:
`RsopMode : Logging`
`Namespace : \\WIN2019-ENG\Root\Rsop\ANS078FF8A1_B7F8_4F26_BD37_83CFD10A9A31`
`LoggingComputer : WIN2019-ENG`
`LoggingUser : NPARTNER\administrator`
`LoggingMode : Computer`
The prompt `PS C:\>` is visible before and after the command. The terminal background is dark blue with white text.

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.

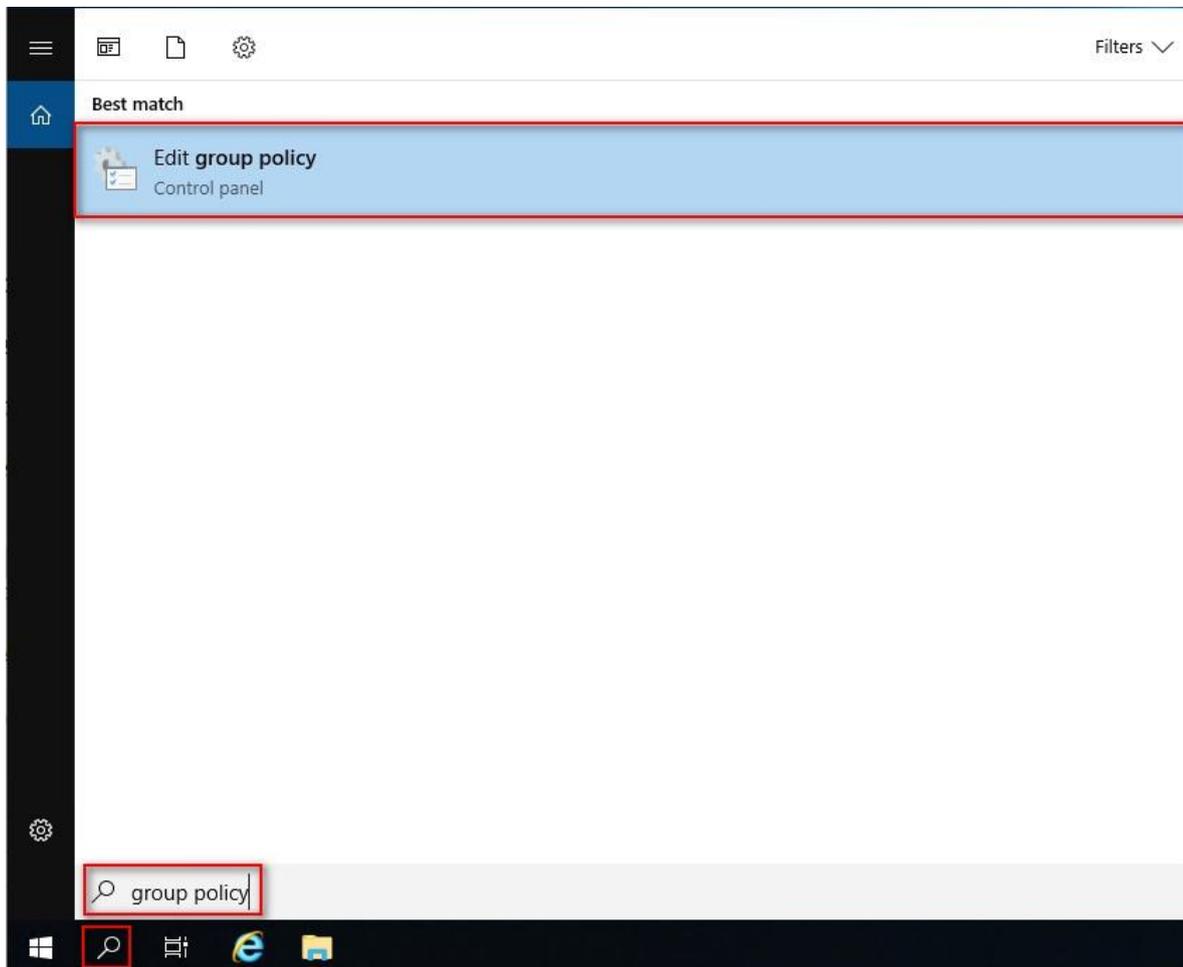
Security Settings		
Account Policies/Password Policy		
Policy	Setting	Winning GPO
Enforce password history	24 passwords remembered	Default Domain Policy
Maximum password age	42 days	Default Domain Policy
Minimum password age	1 days	Default Domain Policy
Minimum password length	7 characters	Default Domain Policy
Password must meet complexity requirements	Enabled	Default Domain Policy
Store passwords using reversible encryption	Disabled	Default Domain Policy
Account Policies/Account Lockout Policy		
Policy	Setting	Winning GPO
Account lockout threshold	0 invalid logon attempts	Default Domain Policy
Local Policies/Audit Policy		
Policy	Setting	Winning GPO
Audit account logon events	Success, Failure	N-Partner Policy
Audit account management	Success, Failure	N-Partner Policy
Audit logon events	Success, Failure	N-Partner Policy
Audit object access	Success, Failure	N-Partner Policy
Audit system events	Success, Failure	N-Partner Policy
Local Policies/Security Options		
Network Access		
Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain 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

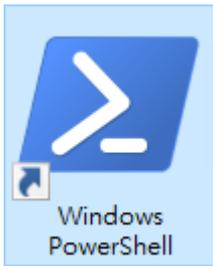
Expand folder “Computer Configuration” -> “Windows Settings” -> “Security Settings” -> “Local Policies” -> “Audit Policy” -> And click on “Audit account logon events,” “Audit account management,” “Audit logon events,” “Audit object access,” and “Audit system events,” items -> Check “Audit these attempts”: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

The screenshot shows the Local Group Policy Editor window. The left-hand tree view is expanded to 'Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Audit Policy'. Several policies are highlighted with red boxes:

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Success, Failure
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	Success, Failure

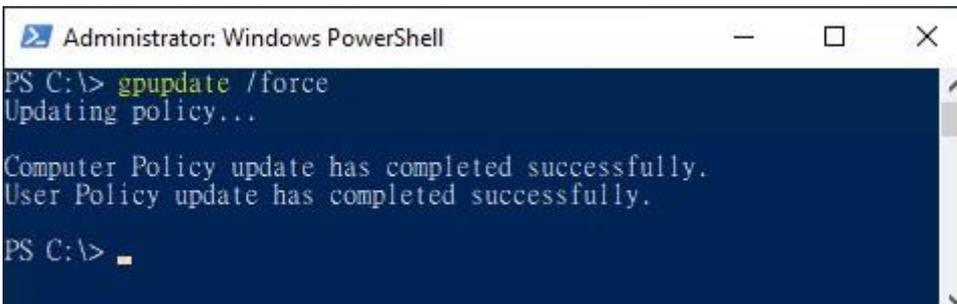
The 'Audit logon events Properties' dialog box is open, showing the 'Local Security Setting' tab. The 'Audit these attempts' section has both 'Success' and 'Failure' checked. A warning message at the bottom states: 'This setting might not be enforced if other policy is configured to override category level audit policy. For more information, see [Audit logon events](#). (Q921468)'. The 'OK' button is highlighted with a red box.

(3) Open "Windows PowerShell."



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

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

A screenshot of a Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The terminal content shows the command `gpupdate /force` being entered and executed. The output indicates that the policy update was successful for both the computer and the user.

```
Administrator: Windows PowerShell
PS C:\> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\> █
```

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

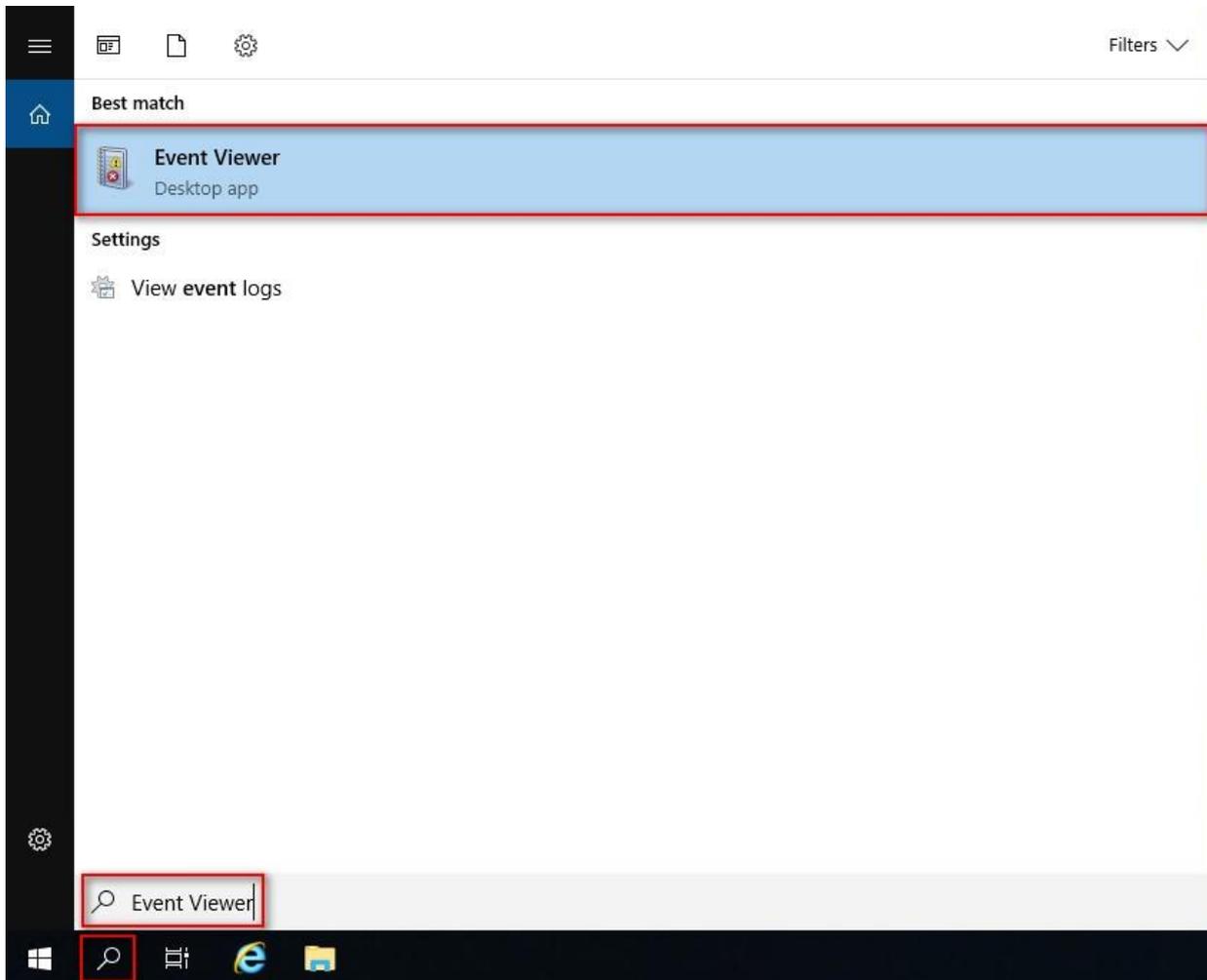
```
PS C:\> auditpol /get /category:*
```

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

7.2.2 Event Log Settings

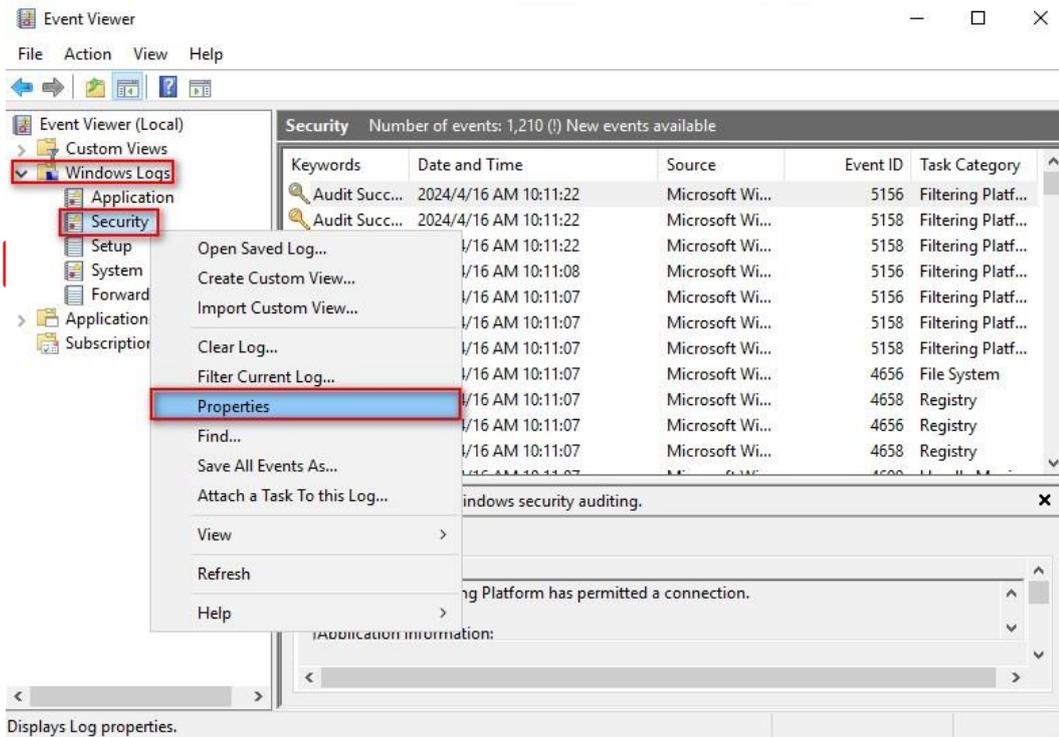
(1) Search for “Group Policy Object Editor”

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.”

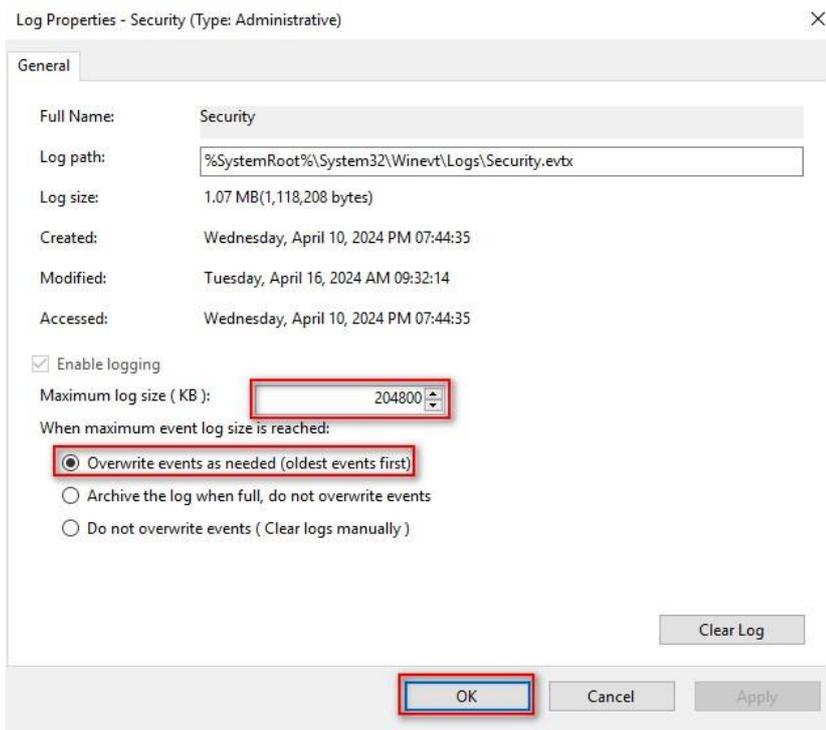


(3) Configure Security Log

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 Recommendation](#) link provided in preface for detailed explanations.

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

8.1 Domain

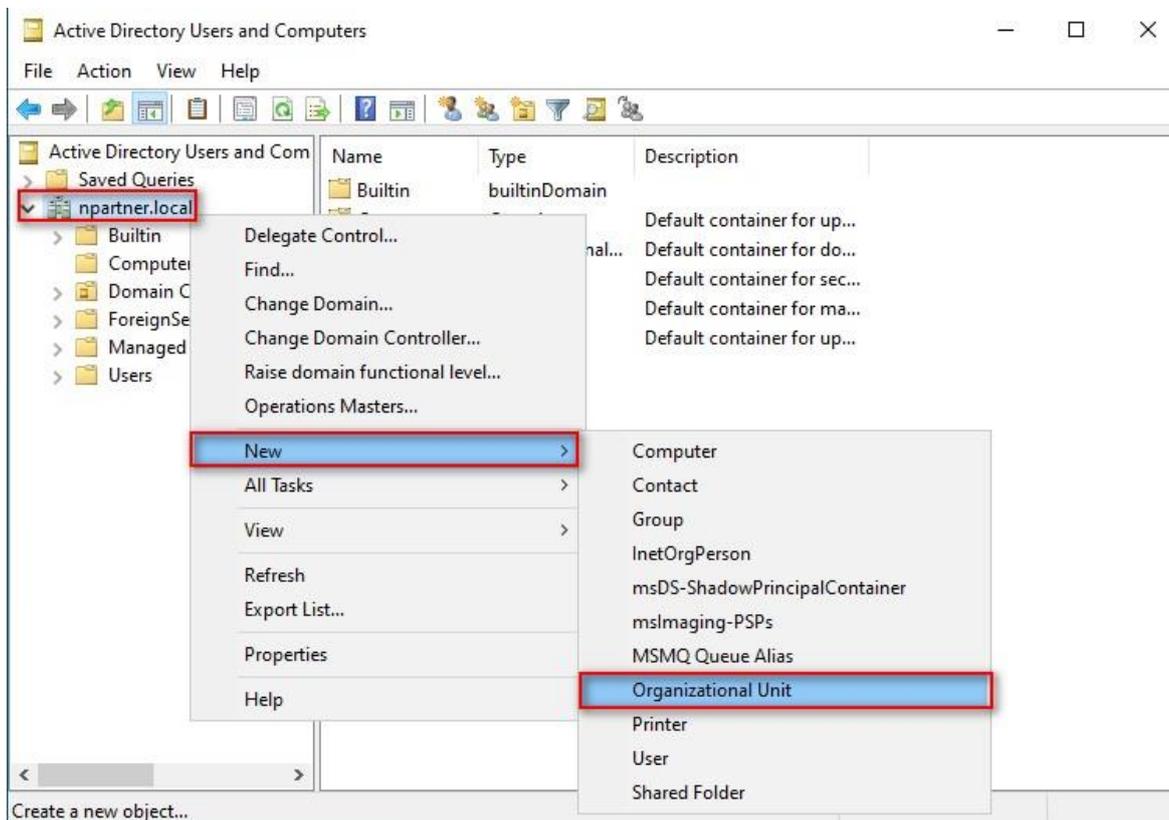
8.1.1 Organizational Unit Setup

(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.”

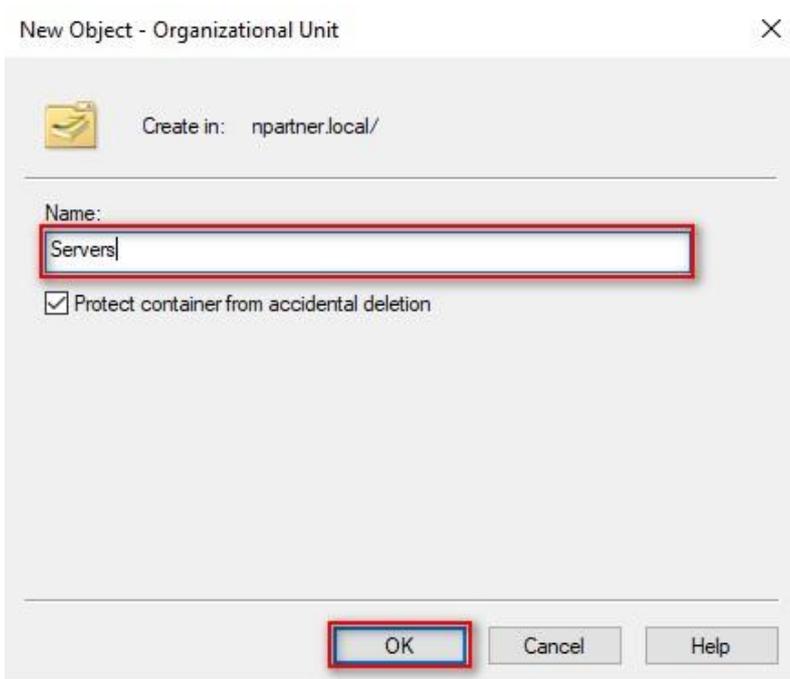


(3) Name Your Organizational Unit

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

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

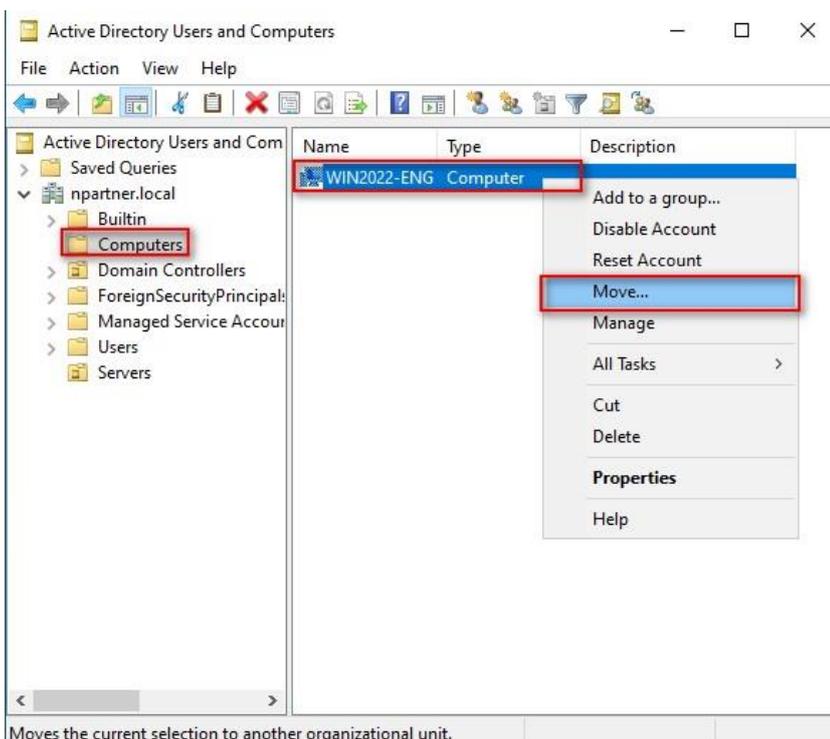
-> and click "OK."



(4) Move Your Server to New Organizational Unit

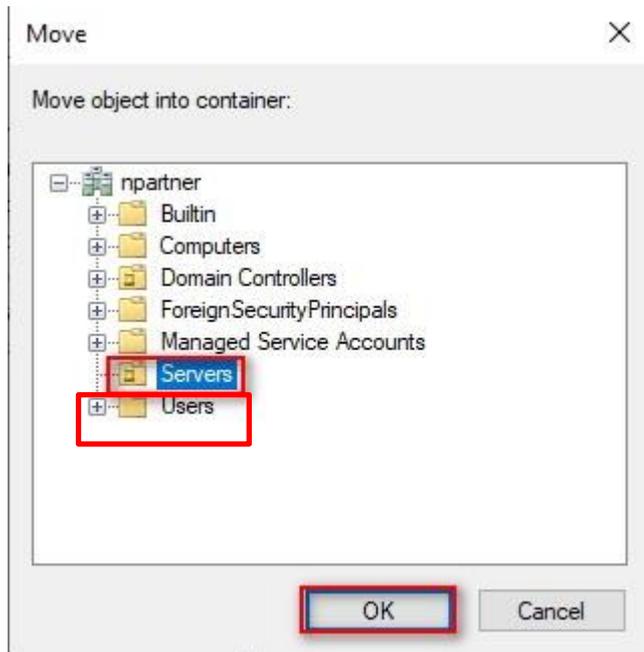
Select your organizational unit (the example here is "Computers") -> Right-click on the "WIN2022-ENG" server.

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



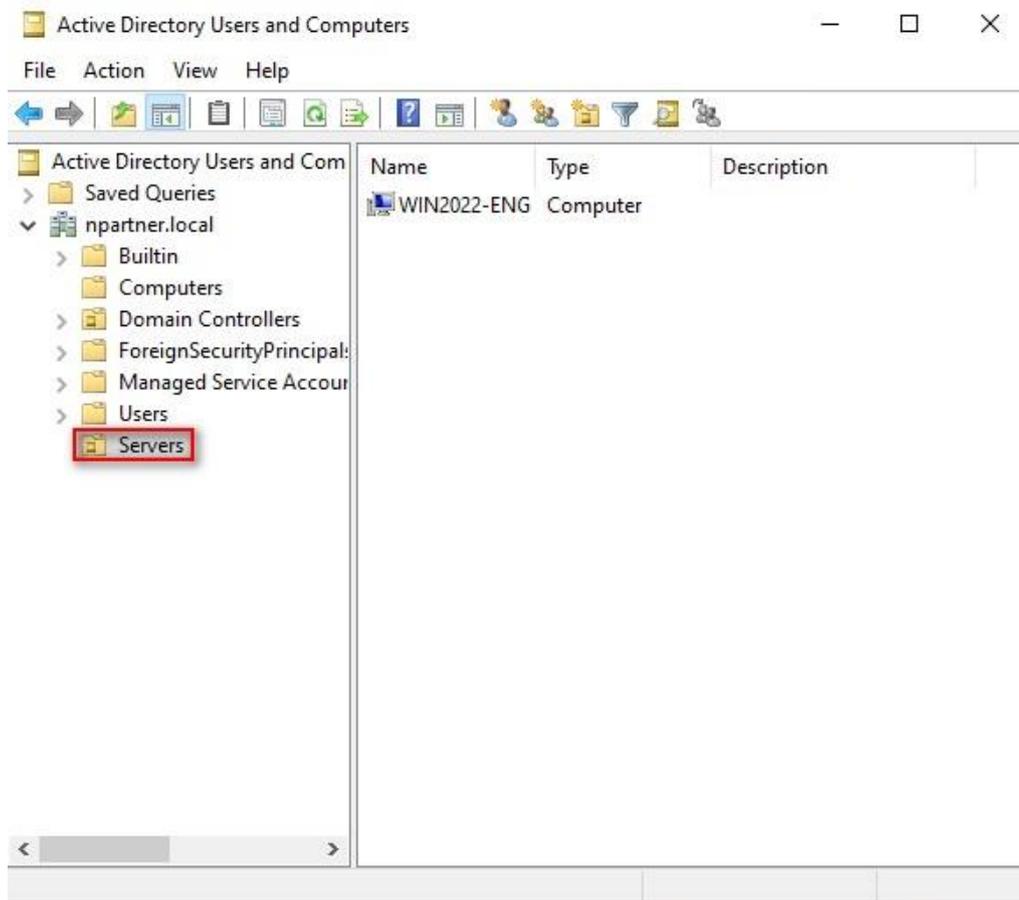
(5) Select Your Organizational Unit

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.

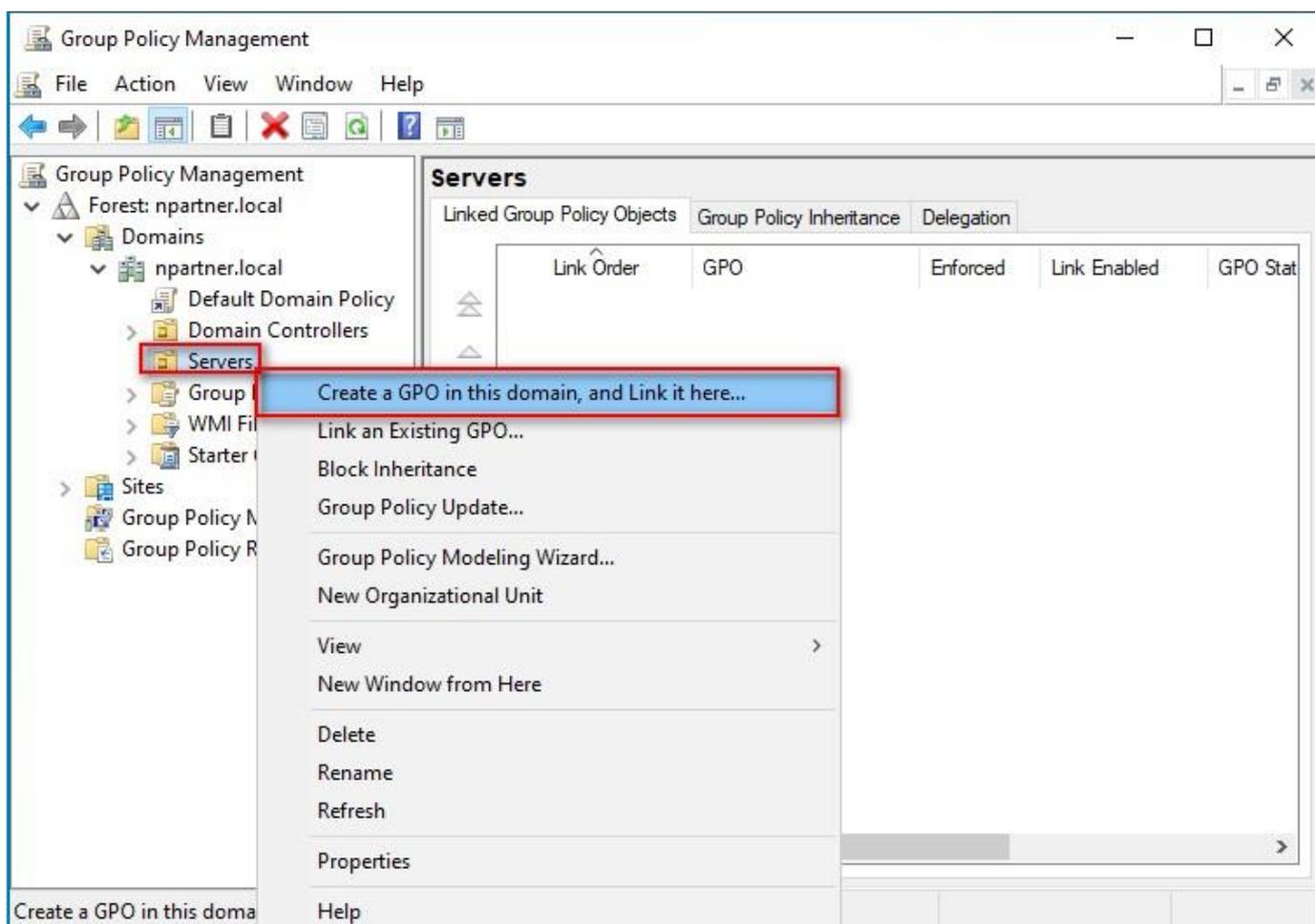


8.1.2 Group Policy Settings

(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

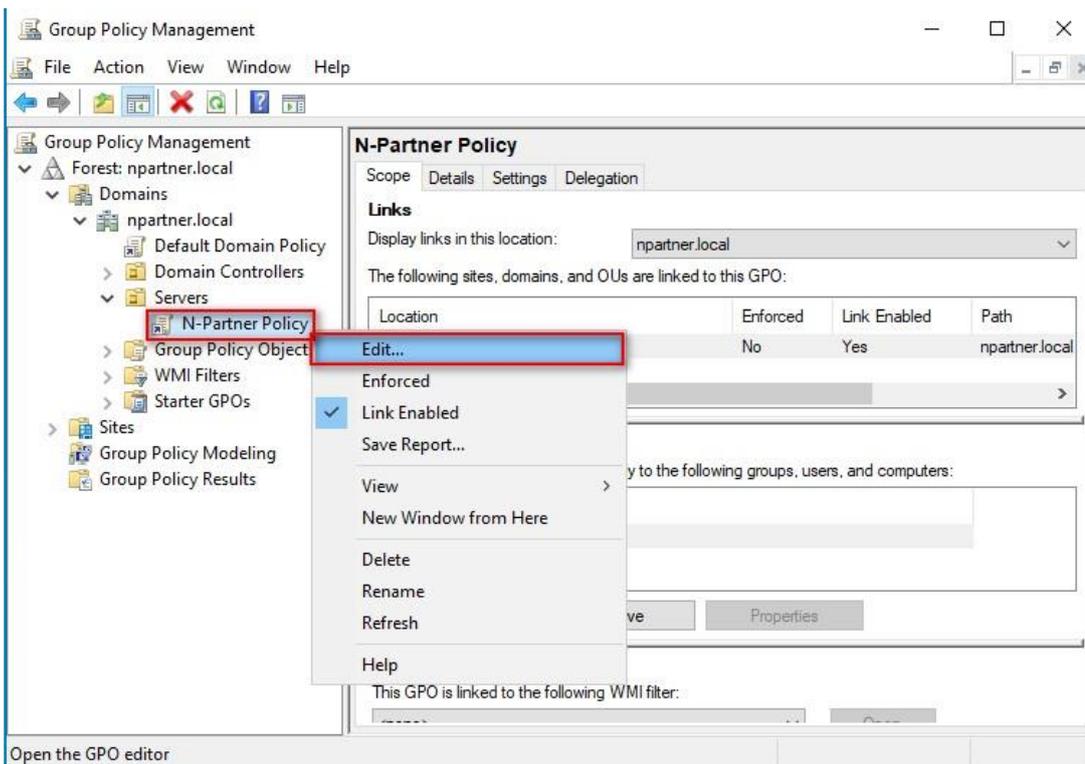
Enter your group policy object name (the example here is “N-Partner Policy”).

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



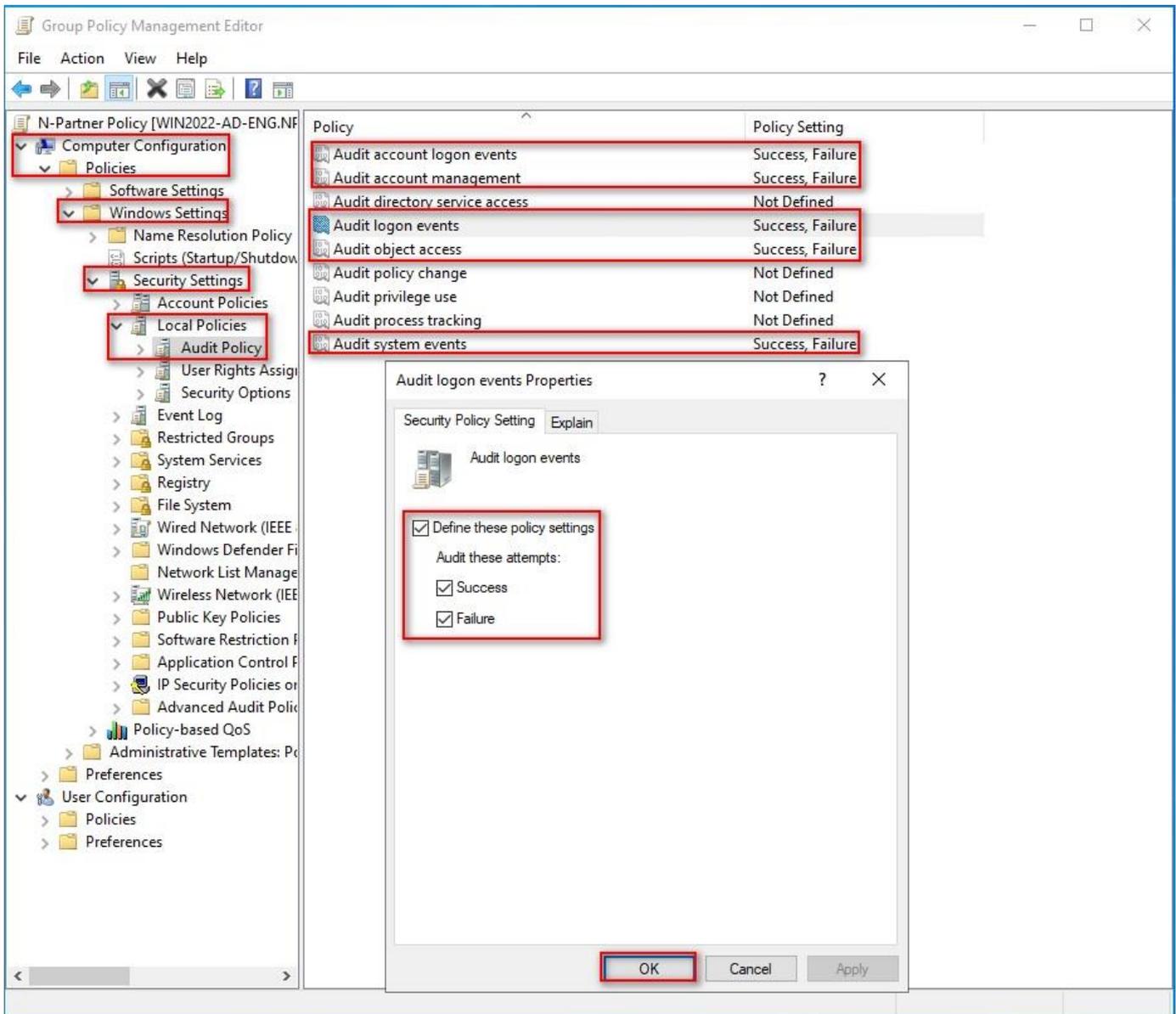
(4) Edit Your Group Policy Object

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

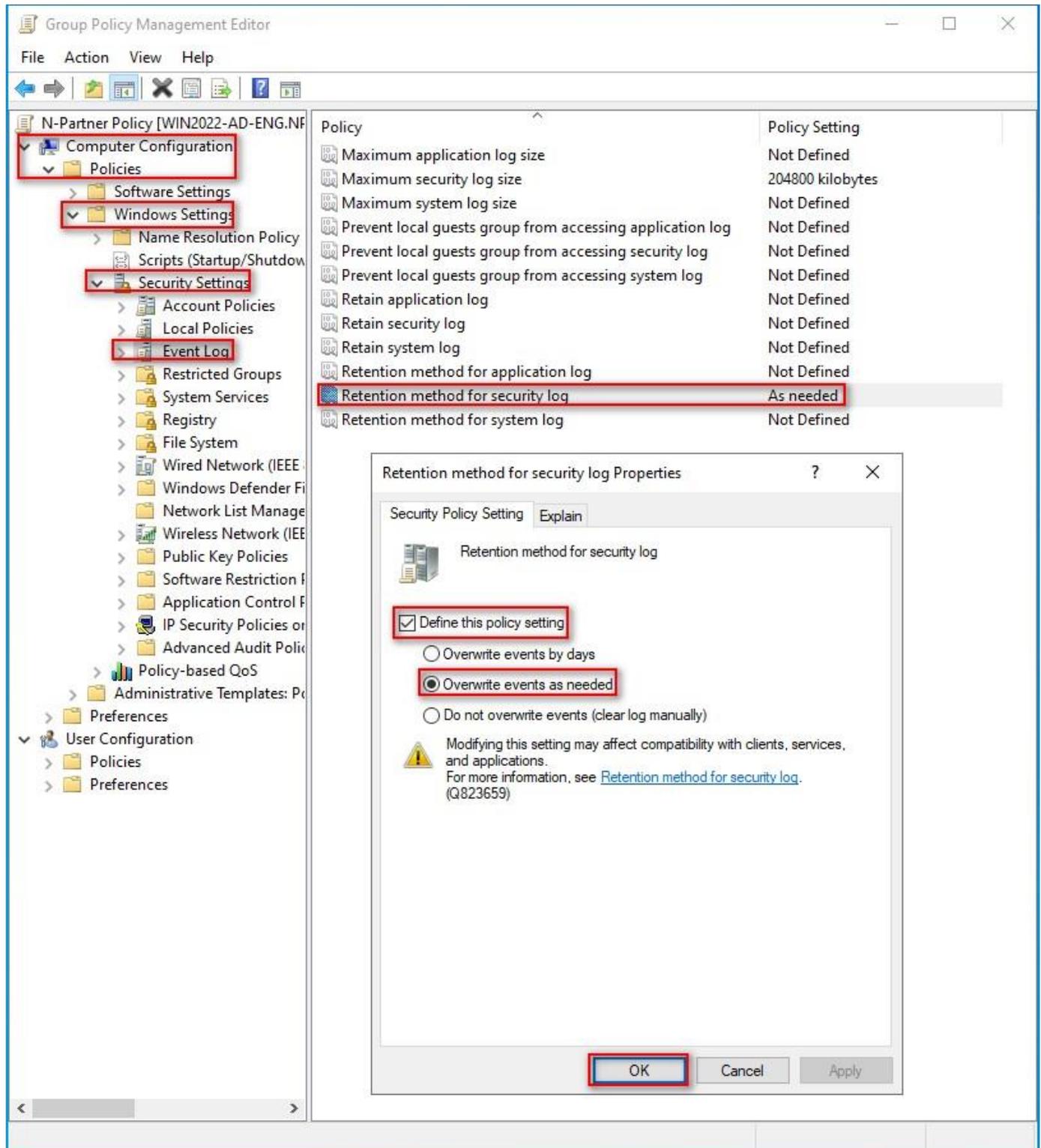
Note: Please adjust the number based on the actual environment. -> Click “OK.”

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

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

(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-GPUdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Invoke-GPUdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force` being entered and executed. The prompt `PS C:\>` is visible before and after the command. The terminal background is dark blue with white text.

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
```

A screenshot of a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal shows the command `Get-GPResultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\WIN2022-ENG.html -ReportType html` being entered and executed. The output is displayed as follows:
`RsopMode : Logging`
`Namespace : \\WIN2022-ENG\Root\Rsop\NSE7835E87_F6F9_4870_ADA9_618106FB1B0C`
`LoggingComputer : WIN2022-ENG`
`LoggingUser : NPARTNER\administrator`
`LoggingMode : Computer`
The prompt `PS C:\>` is visible before and after the command. The terminal background is dark blue with white text.

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.

Group Policy Results

NPARTNER\WIN2022-ENG

Data collected on: 4/16/2024 PM 02:20:06 [show all](#) [hide](#)

During last **computer policy** refresh on 4/16/2024 PM 02:18:29

- No Errors Detected
- A fast link was detected [More information...](#)

No data available.

Computer Details [hide](#)

General [hide](#)

Computer name	NPARTNER\WIN2022-ENG
Domain	npartner.local
Site	Default-First-Site-Name
Organizational Unit	npartner.local/Servers
Security Group Membership	show

Component Status [show](#)

Settings [hide](#)

Policies [hide](#)

- Windows Settings** [hide](#)
- Security Settings** [show](#)
- Administrative Templates** [show](#)

Group Policy Objects [hide](#)

Applied GPOs [hide](#)

Default Domain Policy [{31B2F340-016D-11D2-945F-00C04FB984F9}]	show
Local Group Policy [LocalGPO]	show
N-Partner Policy [{044DAB72-77DD-4B98-AAC6-4BFC6C313C62}]	show

Denied GPOs [hide](#)

WMI Filters [hide](#)

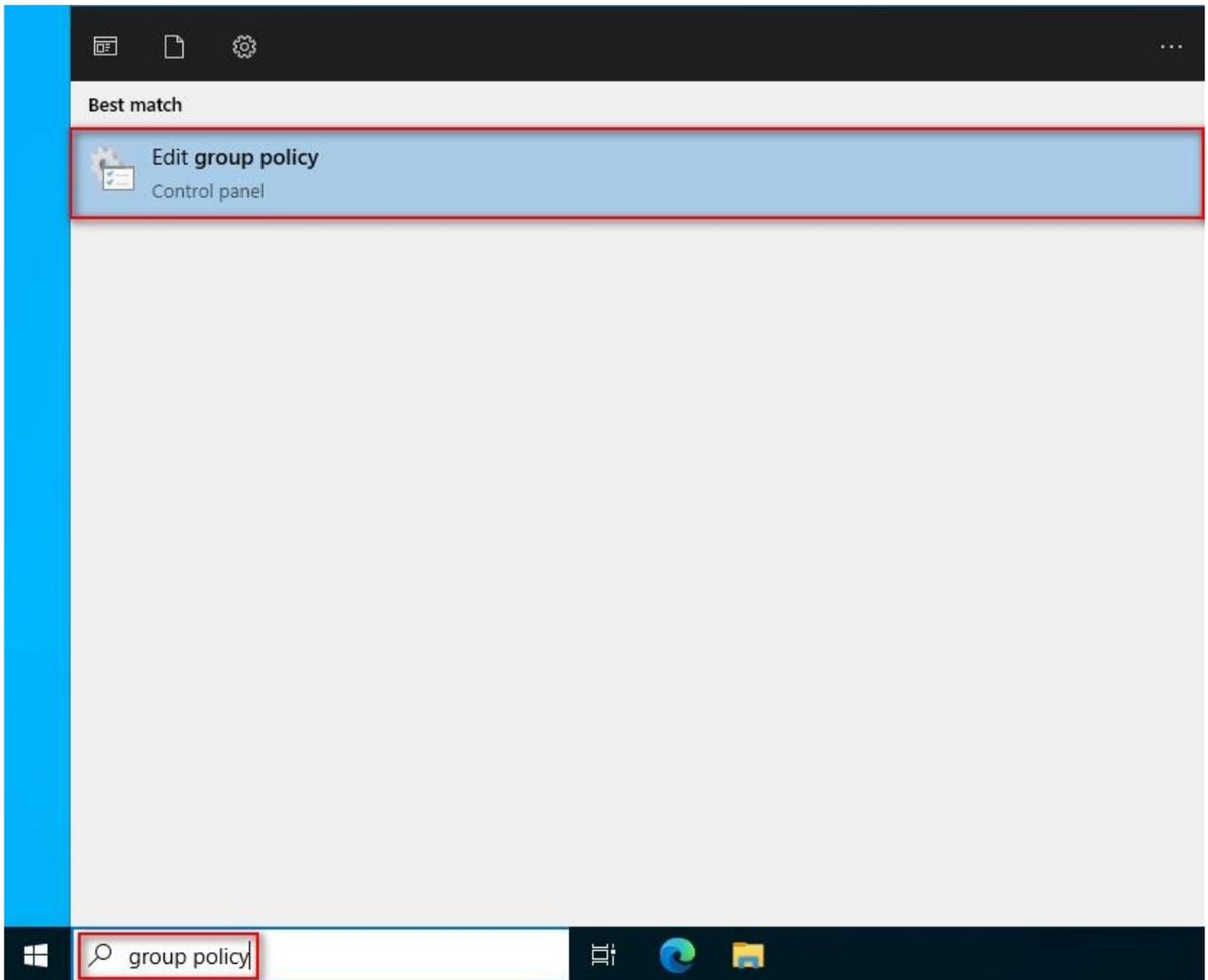
Name	Value	Reference GPO(s)
------	-------	------------------

8.2 Workgroup

8.2.1 Audit Policy Settings

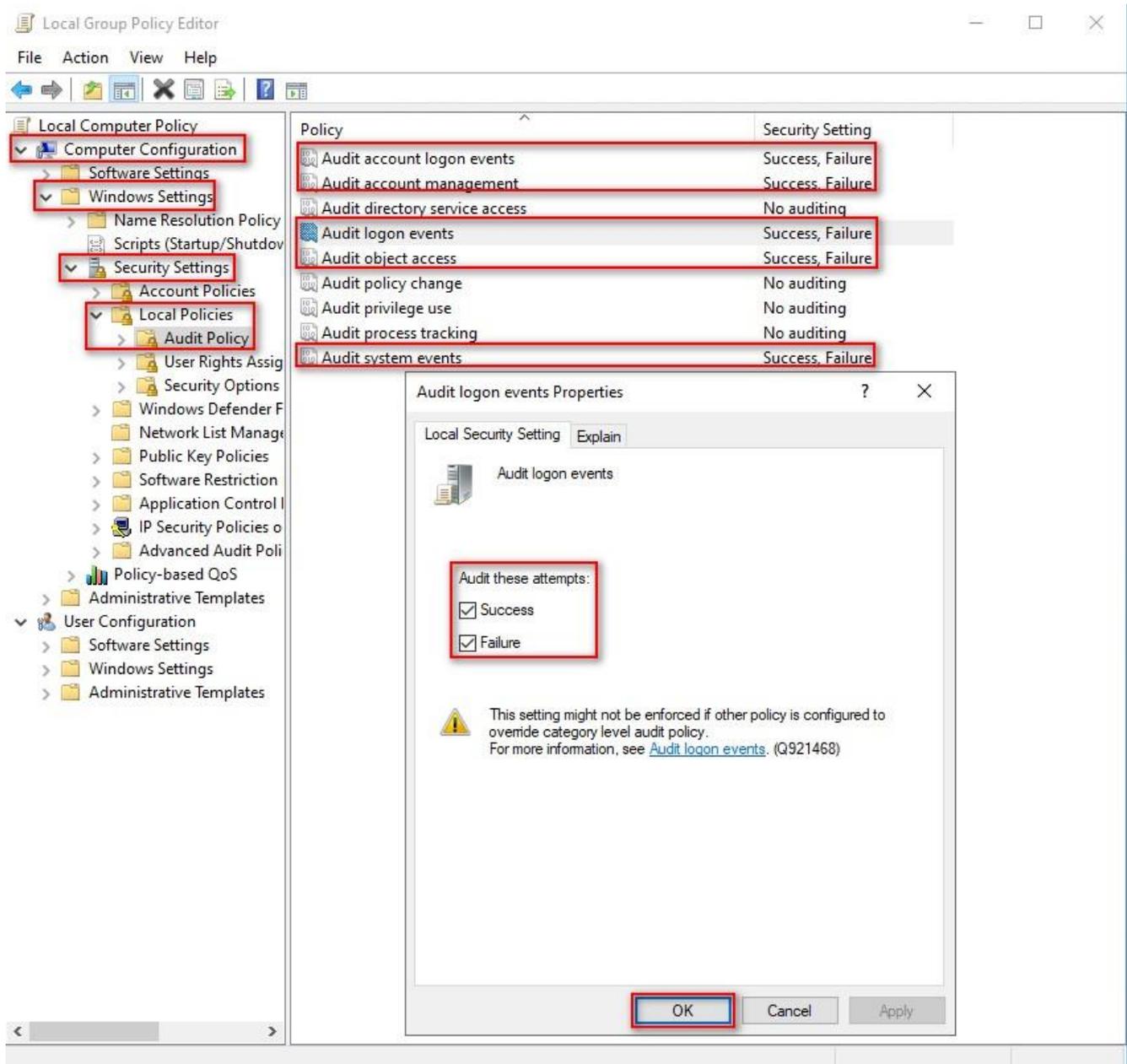
(1) Edit Your Group Policy Object

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

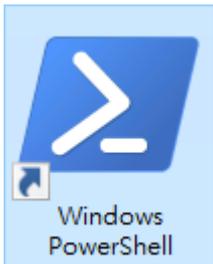


(2) Local Group Policies: Audit Policy

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
```

A screenshot of a Windows PowerShell terminal window. The title bar reads "Administrator: Windows PowerShell". The terminal content shows the command "gpupdate /force" being entered and executed. The output is "Updating policy...", followed by "Computer Policy update has completed successfully." and "User Policy update has completed successfully." The prompt "PS C:\>" is followed by a cursor and a space character.

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

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

PS C:\> _
```

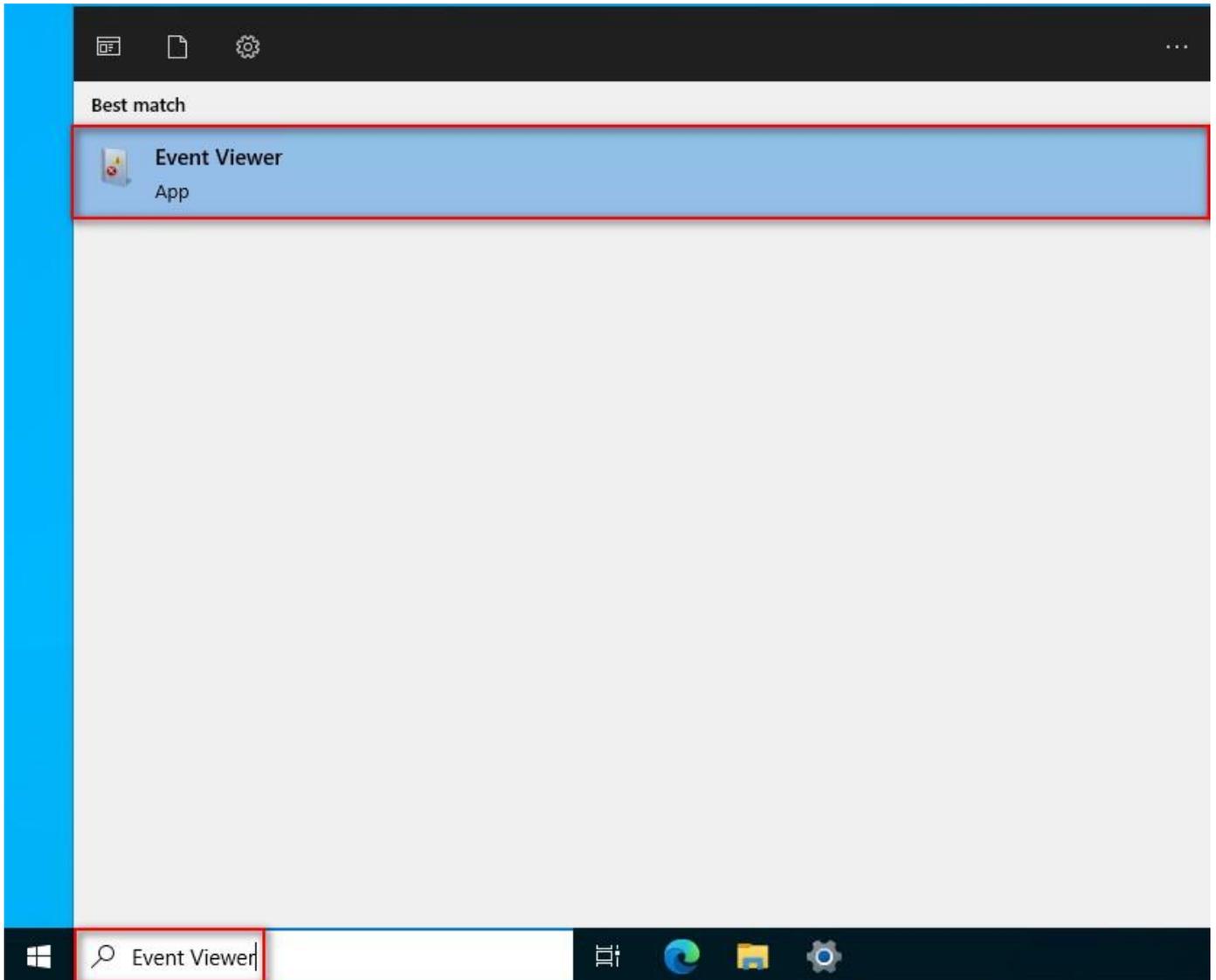
(5) Enter the command to view group policy applied status.

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

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

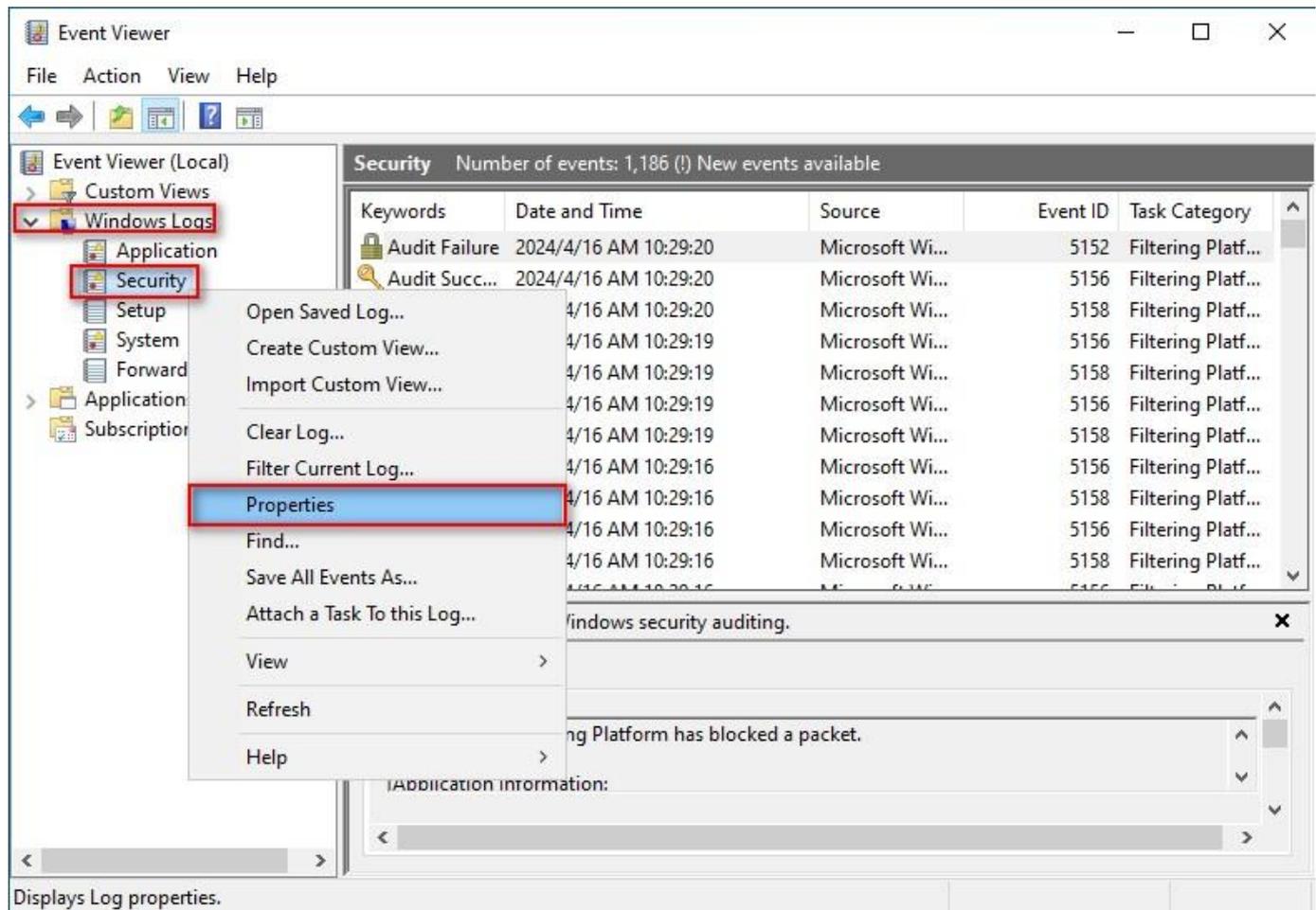
8.2.2 Event Log Settings

(1) 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."

Log Properties - Security (Type: Administrative) ✕

General

Full Name: Security

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

Log size: 1.07 MB(1,118,208 bytes)

Created: Wednesday, April 10, 2024 PM 07:44:35

Modified: Tuesday, April 16, 2024 AM 09:32:14

Accessed: Wednesday, April 10, 2024 PM 07:44:35

Enable logging

Maximum log size (KB):

When maximum event log size is reached:

Overwrite events as needed (oldest events first)

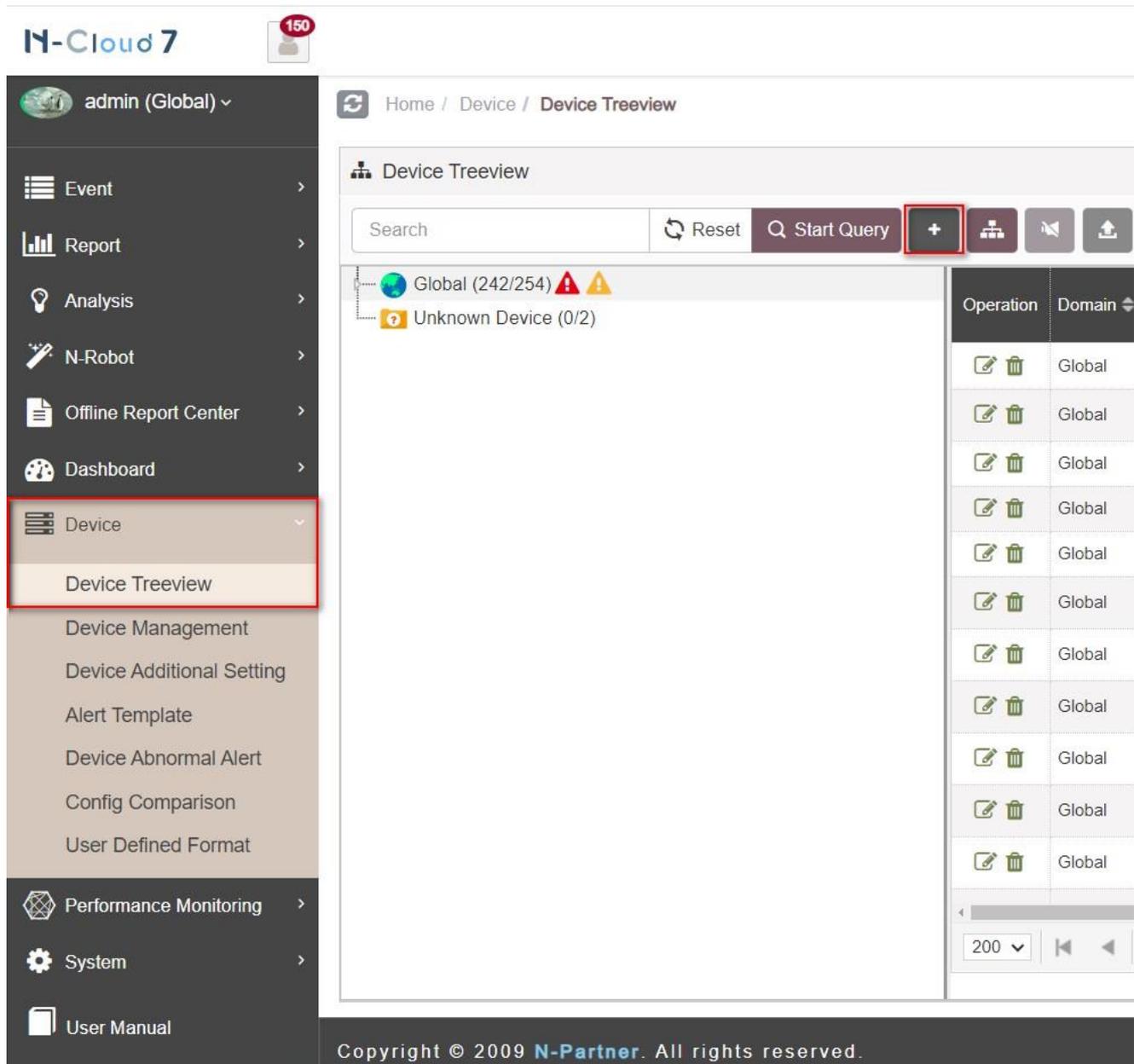
Archive the log when full, do not overwrite events

Do not overwrite events (Clear logs manually)

9. N-Reporter

(1) Add a Windows Server Device:

Click "Device" -> "Device Treeview" -> And click "Add."



Copyright © 2009 N-Partner. All rights reserved.

(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.”

Add Device - Basic Setting

Basic Setting

Machine Name *
Win2022 ENG 192.168.14.84

IP *
192.168.14.84

Domain *
Global

Syslog Data Type ⓘ
Windows

User Defined Syslog Format ⓘ
Please select ...

SNMP Model ⓘ
Please select ...

Web Monitor ⓘ
 Activate Page Monitoring

Previous **Next** Cancel

Click "Next."

Add Device - SNMP Setting

SNMP Setting

SNMP IP

Version

V2C

Read Community

public

Write Community

SNMP Timeout(sec)

5

Encoding

UTF-8

Device (Interface and Partition) Searched Timeout (Sec)

120

SNMP V3

Previous **Next** Cancel

Click "Next."

Add Device - Syslog Setting

Syslog Setting

Facility ⓘ

Encoding

UTF-8

Syslog Normalized Data Retention Days (Max) ⓘ

Raw Data Kept and Replied

- Raw Data Kept
- Raw data format is adopted while Syslog relaying is activated in Threshold Report.
- The source IP will be kept in normalized data relaying

Previous **Next** Cancel

Click "Next."

Add Device - Monitor & Alert

Alert Template ^

ICMP Alert Template

Please select ... v

Device Alert Template

Please select ... v

Process Alert Template

Please select ... v

User Defined OID Template

NTP Template

Please select ... v

Monitor and Connection Test v

Alert Notification Setting v

Alert Detail Configuration v

Previous **Next** Cancel

Click "Next."

Add Device - Other

Other ^

Device Icon 

Host v

Latitude and Longitude

atitude, longitude

Receive Status

Activated Disabled

Device Sharing 

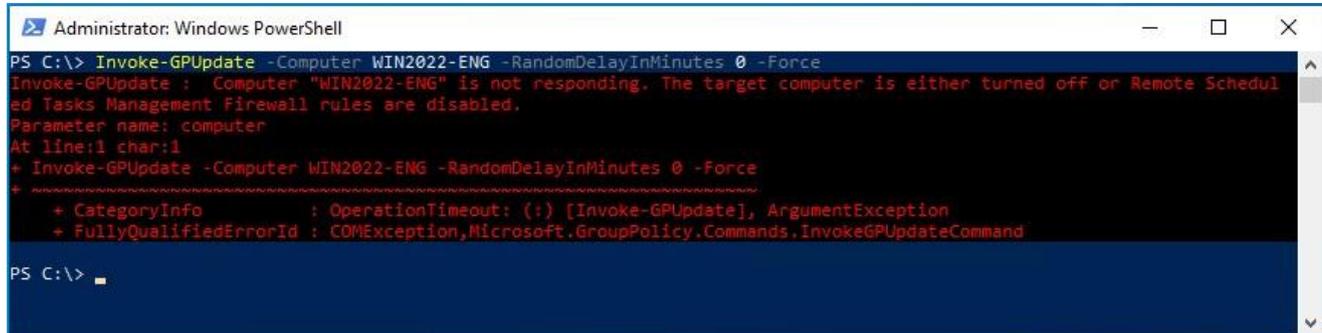
Device Sharing

Previous **Next** Cancel

10. Troubleshooting

10.1 Invoke-GPUUpdate Error

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



```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
Invoke-GPUUpdate : Computer "WIN2022-ENG" is not responding. The target computer is either turned off or Remote Scheduled Tasks Management firewall rules are disabled.
Parameter name: computer
At line:1 char:1
+ Invoke-GPUUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
+ ~~~~~
+ CategoryInfo          : OperationTimeout: (:) [Invoke-GPUUpdate], ArgumentException
+ FullyQualifiedErrorId : COMException,Microsoft.GroupPolicy.Commands.InvokeGPUUpdateCommand

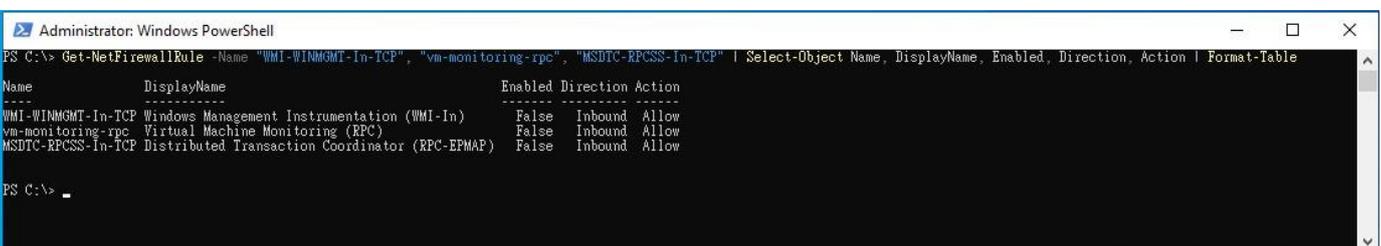
PS C:\>
```

(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
```

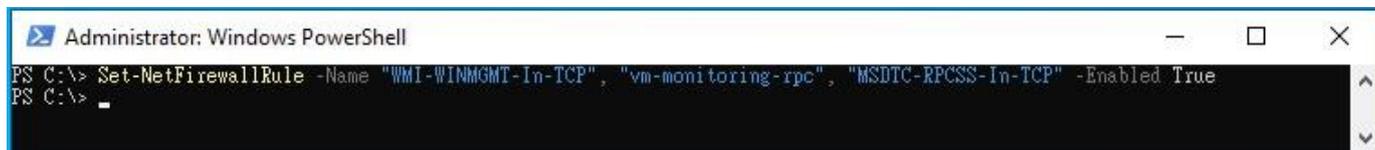


```
Administrator: Windows PowerShell
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
Name                DisplayName          Enabled Direction Action
-----
WMI-WINMGMT-In-TCP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

PS C:\>
```

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

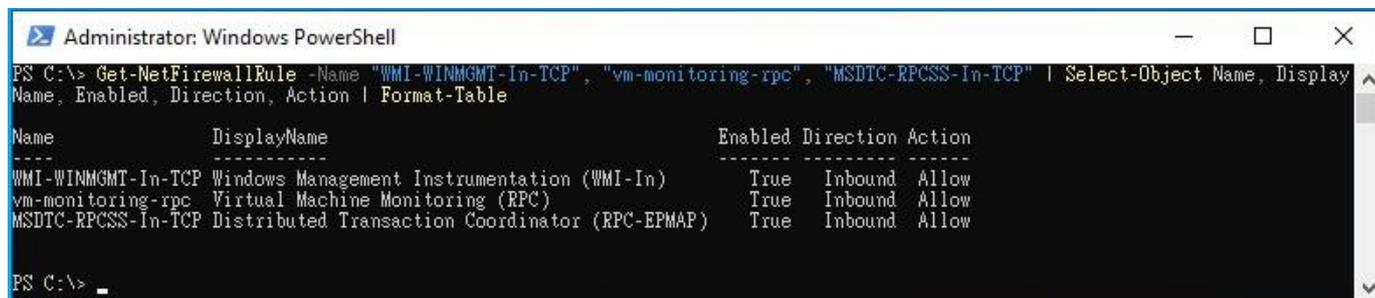
```
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" -Enabled True
```



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

(5) Enter the 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
```

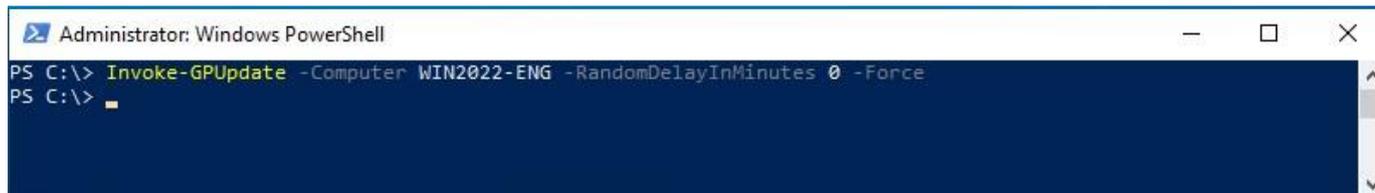


```
Administrator: Windows PowerShell
PS C:\> Get-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" | Select-Object Name, DisplayName, Enabled, Direction, Action | Format-Table
Name                DisplayName          Enabled Direction Action
-----
WMI-WINMGMT-In-TCP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

PS C:\> _
```

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

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

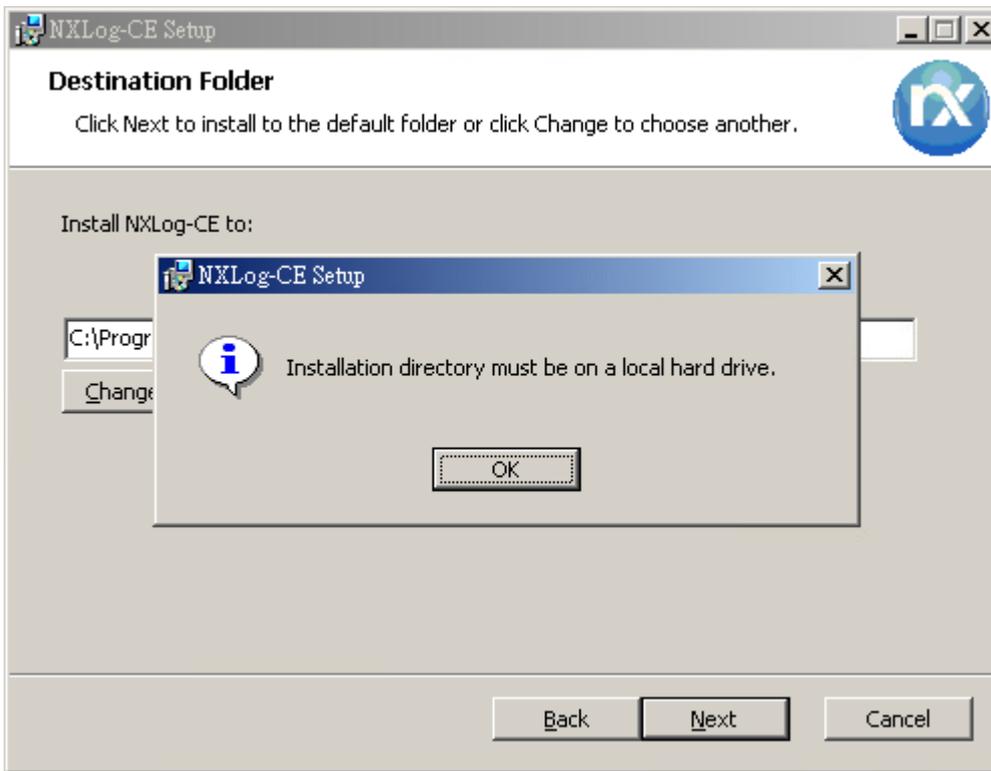


```
Administrator: Windows PowerShell
PS C:\> Invoke-GPUdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force
PS C:\> _
```

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

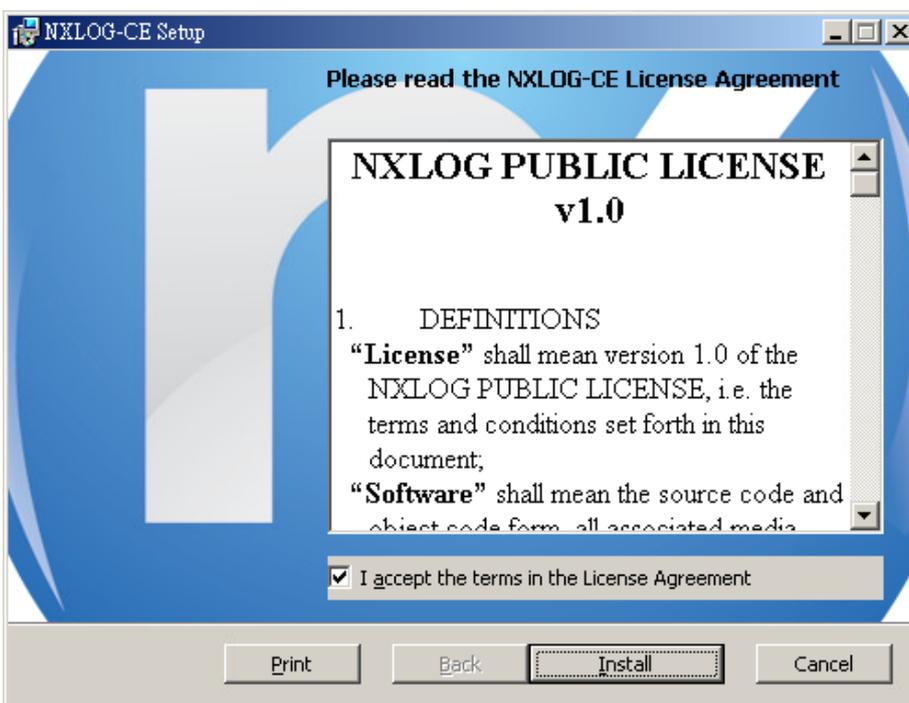
10.2 NXLog Installation Issues

(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