



Manage Windows AD Server Syslog V014 with NXLOG



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

Preface2
1. NXLog
1.1 Configure NXLOG in Windows Server AD
1.2 NXLog Configuration File Download7
1.2.1 For Windows 2003 or Its Earlier Versions7
1.2.1.1 Output Host Audit, Object Access, and Account
Management Event Logs7
1.2.1.2 Output All Event Logs8
1.2.2 For Windows 2008 or Its Later Versions9
1.2.2.1 Output Host Audit, Object Access, and Account
Management Event Logs9
1.2.2.2 Output All Event Logs for Applications, Security, and
System10
1.3 NXLog Configuration11
1.3.1 For Windows 2003 or Its Earlier Versions11
1.3.1.1 Output Host Audit, Object Access, and Account
Management Event Logs11
1.3.1.2 Output All Event Logs12
1.3.2 For Windows 2008 or Its Later Versions13
1.3.2.1 Output Host Audit, Object Access, and Account
Management Event Logs13
1.3.2.2 Output All Event Logs for Applications, Security, and
System15
1.4 NXLog Startup16
1.4.1 For Windows 2003 or Its Earlier Versions16
1.4.2 For Windows 2008 or Its Later Versions19
2. For Windows 2000
2.1 Domain22
2.1.1 Organizational Unit Setup22
2.1.2 Group Policy Settings25
2.2 Workgroup32
2.2.1 Audit Policy Settings
2.2.2 Event Log Settings
3. For Windows 2003
3.1 Domain
3.1.1 Organizational Unit Configuration39
3.1.2 Group Policy Settings42
3.2 Workgroup48
3.2.1 Audit Policy Settings48
3.2.2 Event Log Settings52
4. For Windows 200855
4.1 Domain55
4.1.1 Organizational Unit Setup55
4.1.2 Group Policy Settings

4.2 Workgroup	65
4.2.1 Audit Policy Settings	65
4.2.2 Event Log Settings	68
5. For Windows 2012	70
5.1 Domain	70
5.1.1 Organizational Unit Setup	70
5.1.2 Group Policy Settings	73
5.2 Workgroup	79
5.2.1 Audit Policy Settings	79
5.2.2 Event Log Settings	82
6. For Windows 2016	84
6.1 Domain	84
6.1.1 Organizational Unit Setup	84
6.1.2 Group Policy Settings	87
6.2 Workgroup	94
6.2.1 Audit Policy Settings	94
6.2.2 Event Log Settings	98
7. For Windows 2019	101
7.1 Domain	101
7.1.1 Organizational Unit Setup	101
7.1.2 Group Policy Settings	105
7.2 Workgroup	112
7.2.1 Audit Policy Settings	112
7.2.2 Event Log Settings	116
8. For Windows 2022	118
8.1 Domain	118
8.1.1 Organizational Unit Setup	118
8.1.2 Group Policy Settings	121
8.2 Workgroup	128
8.2.1 Audit Policy Settings	128
8.2.2 Event Log Settings	132
9. N-Reporter	135
10. Troubleshooting	142
10.1 Invoke-GPUpdate Error	142
10.2 NXLog Installation Issues	144
Contact	145



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: <u>https://docs.microsoft.com/zh-tw/windows-server/identity/ad-</u> <u>ds/plan/security-best-practices/audit-policy-recommendations</u>

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

Connect Windows Security Event: <u>https://docs.microsoft.com/zh-tw/azure/sentinel/connect-windows-</u> 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.xxx.msi; here, it's nxlog-ce-3.2.2329.msi.





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

					2	
NX	LOG PU	BLIC	LICE	NSE vi	1.0	Í
1. DEFI	NITIONS	ion 1.0 .	- - 44 - NTV			
LICENSE	, i.e. the terms	and con	ditions se	LOG PU t forth in t	his docume	ent;
"Software"	shall mean the media printed	source material	code and Is and "o	object co nline" or e	de form, a lectronic	11
documenta	tion. All such s	oftware	and mate	rials are r	eferred to	-
			7			

Click "Next."

NXLog-CE Setup				
Destination Folder Click Next to install to the defaul	lt folder or click C	hange to cho	oose another,	
Install NXLog-CE to:				
C:\Program Files\nxlog\				
Change				



Click "Install."



Click "Finish."





<2.2> Windows 2003

Click "nxlog-ce-3.2.2329.msi→Install→Finish."

援 NXLog-CE Setup	-		×
Ready to install NXLog-CE			
Click Install to begin the installation. Click Back to review or change ar installation settings. Click Cancel to exit the wizard.	ıy of you	r	
Back Install		Cano	el

<2.3> Windows 2000

Go to the old version website of NXLog CE at <u>https://sourceforge.net/projects/nxlog-ce/</u>. 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 \rightarrow 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: <u>http://www.npartner.com/download/tech/nxlog_Win2003Server.conf</u> C:\ > copy "C:\nxlog_Win2003Server.conf" "C:\Program Files\nxlog\conf\nxlog.conf" /y



If the operating system is 64-bit, modify the following setting in red part: "C:\Program Files

(x86)\nxlog\conf\nxlog.conf"

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



1.2.1.2 Output All Event Logs

(1) Click "Command Prompt."



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

configuration file

Download Link: <u>http://www.npartner.com/download/tech/nxlog_Win2003All.conf</u> 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'

 Administrator: Windows PowerShell

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



1.2.2.2 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'

Administrator: Windows PowerShell

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

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
                       %ROOT%\data\nxlog.pid
Pidfile
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 \text{ or } \text{EventID} = 626 \text{ or } \text{EventID} = 627 \text{ or } \text{EventID} = 628 \text{ or } \text{EventID} = 629 \text{ or } \text{EventID} = 630 \text{ or } \text{EventID} = 630 \text{ or } \text{EventID} = 629 \text{ or } \text{EvenI
$EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635 or $EventID ==
$$$ of $EventID == 637 of $EventID == 635 of $EventID == 635 of $EventID == 635 of $EventID == 635 of $EventID == 636 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
                                        %NCloud%
     Host
     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
           %ROOT%\data
SpoolDir
## 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
                TRUE
  SavePos
                <QueryList> \
  Query
    <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
           %ROOT%\data
SpoolDir
## 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%
             514
  Port
  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.



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





(4) Open NXLog Service

Please select "nxlog" and click \blacksquare .

🍇 Services							
Eile Action View	Help						
← → 💽 🚰 🤄) 🗟 😰 🖬 🕨 🔳 💷 🖦						
🦓 Services (Local)	🍇 Services (Local)						
	nxlog	Name 🔺	Description	Status	Startup Type	Log On As	
		Network DDE DSDM	Manages D		Disabled	Local System	
	Stop the service	Network Location A	Collects an	Started	Manual	Local System	
	Restart the service	Network Provisionin	Manages X		Manual	Local System	
		MANT I M Security Sup	Provides s		Manual	Local System	
	Description: This service is responsible for running the	nxlog 👘	This servic	Started	Automatic	Local System	
		Performance Logs	Collects pe		Automatic	Network S	
	INALOG agent, See www.nxlog.co.	Plug and Play	Enables a c	Started	Automatic	Local System	
		Portable Media Seri	Retrieves t		Manual	Local System	
		Print Spooler	Manages al	Started	Automatic	Local System	
		Protected Storage	Protects st	Started	Automatic	Local System	
		Remote Access Aut	Creates a		Manual	Local System	
		Remote Access Co	Creates a		Manual	Local System	
		Remote Desktop H	Manages a		Manual	Local System	
		Remote Procedure	Serves as t	Started	Automatic	Network S	
		Remote Procedure	Enables re		Manual	Network S	
		Remote Registry	Enables re	Started	Automatic	Local Service	
		Removable Storage	Manages a		Manual	Local System	
		Be Docultont Cot of Do	Enables a		Manual	Local Suctor	-
	Extended Standard	Stan Docultoot Cot of Do	Epoblec a		Manual	Local Suctor	

(5) Select "Automatic" of "Startup type" in "General."

eneral Log On	Recovery Dependencies
Service name:	nxlog
Display <u>n</u> ame:	NXLog
Description:	This service is responsible for running the NXLog agent. See www.nxlog.co.
Pat <u>h</u> to executat	ole:
"C:\Program File	s\nxlog\nxlog.exe" -c "C:\Program Files\nxlog\conf\nxlog
Startup typ <u>e</u> :	Automatic
Service status:	Started
Service status: <u>S</u> tart	Started
Service status: <u>S</u> tart You can specify from here	Started Stop Pause Ithe start parameters that apply when you start the service
Service status: <u>S</u> tart You can specify from here.	Started Stop Pause Resume the start parameters that apply when you start the service
Service status: <u>S</u> tart You can specify from here. Start para <u>m</u> eters	Started Stop Besume the start parameters that apply when you start the service



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

og Properties (Local C	omputer)	?
ieneral Log On Recove	עזי Dependencies	
Select the computer's resp	onse if this service fails.	
<u>F</u> irst failure:	Restart the Service	
<u>S</u> econd failure:	Restart the Service	-
S <u>u</u> bsequent failures:	Restart the Service	-
Reset fail c <u>o</u> unt after:	0 days	
Restart ser <u>v</u> ice after:	1 minutes	
Program:		1
ļ	Brow	Wse
<u>C</u> ommand line paramete	rs:	
F Append fail count to	end of command line (/fail=%1%)	
	<u>R</u> estart Computer Optio	ms
	OK Cancel	Apply



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' 🜌 Administrator: Windows PowerShell - 🗆 × PS C:\> Restart-Service -Name nxlog * PS C:igwedge Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType Name Status StartType nxlog Running PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log' 2024-04-12 15:39:05 WARNING no functional input modules! 2024-04-12 15:39:05 WARNING no routes defined! 2024-04-12 15:39:05 INFO nxlog-ce-3.2.2329 started 2024-04-12 16:31:38 WARNING stopping nxlog service 2024-04-12 16:31:38 WARNING nxlog-ce received a termination request signal, exiting... 2024-04-12 16:31:39 INFO nxlog-ce-3.2.2329 started PS C:>>

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





(4) Open NXLog Service

Please select "nxlog" and click 🔟.

🝳 Services							
File Action View	Help						
	nxlog Stop the service	Name A	Description Collects an This servic	Status Started Started	Startup Type Automatic	Log On As	
	Restart the service	Performance Count	This servic Enables re	Started	Automatic (D Manual	Local System Local Service	
	Description: This service is responsible for running the NXLog agent. See www.nxlog.co.	Performance Logs Plug and Play PnP-X IP Bus Enum Portable Device En Power	Enables a c The PnP-X Enforces g Manages p Loads files	Started Started Started	Manuar Automatic Disabled Manual Automatic	Local System Local System Local System Local System Local System	
	Extended / Standard /	Problem Reports an	This servic		Manual	Local System	<u> </u>

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

nxlog Properties (l	Local Computer)	×
General Log On	Recovery Dependencies	
Service name:	nxlog	
Display name:	nxlog	
Description:	This service is responsible for running the N agent. See www.nxlog.co.	XLog 🔺
Path to executable "C:\Program Files"	e: \nxlog\nxlog.exe'' -c ''C:\Program Files\nxlog	\conf\nxlog.
Startup type:	Automatic (Delayed Start)	_
Help me configure	e service startup options.	
Service status:	Started	
Start	Stop Pause	Resume
You can specify th from here. Start parameters:	he start parameters that apply when you start	the service
	OK Cancel	Apply



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

1040113.	
ïrst failure:	Restart the Service
econd failure:	Restart the Service
iubsequent failures:	Restart the Service
leset fail count after:	1 days
lestart service after:	1 minutes
Enable actions for sto	ops with errorsRestart Computer Options
	Browse
Command line parame	eters:



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."

New Object	- Organizal	tional Unit				×	
3	Create in:	npartner.local/					
N <u>a</u> me:							
Servers]	
				OK](Cancel	
			2.2		20 92		

(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."

2 Console Window Help				
	📧 🗡 🖭 🕼			
Tree	Computers 1 obje	ects		
🎻 Active Directory Users and Compt	Name	Туре	Description	
🖻 🗊 npartner.local	WIN2000-ENG	Computer	Digable Account	
			Reset Account	
Domain Controllers			Мо <u>ч</u> е	
🗄 🛅 ForeignSecurityPrincipals			Manage	
Servers			All Tas <u>k</u> s 🕨 🕨	
			Delete	
			Refresh	
			P <u>r</u> operties	
			Help	
	45			



(5) Select Your Organizational Unit

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

love			? >
<u>C</u> ontainer to move o	bject to:		
Program Computer Program Computer	ters 1 Controllers SecurityPrinc	sipals	
		ОК	Cancel

(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"

🐗 Active Directory Users and Co	mputers			
🛛 🎻 Console 🛛 <u>W</u> indow Help				_8×
📙 Action View 🗍 🖙 🔶 主	💽 🗙 😭	🔁 🗟 😫 🛛	10 10 10 V 4 10	
Tree	Servers 1 obj	ects		
Active Directory Users and Compt		Type	Description	
Image reparties local Event in the second				

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."

literative Directory Users and	Computers			_ 🗆 ×
] 🌍 Console 🛛 Window Help				<u>_8×</u>
] Action ⊻iew] ← → 🤁	🗅 📧 🗙 😭 🖸	B 2 1	1 🖥 💩 🖓 🍕 🙆	
Tree	Servers 1 objects	5		
Active Directory Users and Com Active Directory Users and Com Builtin Computers Domain Controllers ForeignSecurityPrincipal	s Name	Type Computer	Description	
	ntrol rs to a group			
<u>N</u> ew All Tas <u>k</u> s	*			
<u>V</u> iew New <u>W</u> indov	v from Here			
Delete Rena <u>m</u> e Refresh Export List				
Properties				
Opens property she ct for the carter	ic selection.			



(3) Enter Your Group Policy Object Name

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

	-5			?
General Manag	ed By Group Po	olicy		
Cur	rent Group Policy	Object Links for S	ervers	
Group Policy 0)bject Links	N	o Override	Disabled
Group Policy Ob	ients higher in the	a list have the high	ast prioritu	
Group Policy Ob This list obtained	ojects higher in the d from: win2000-a	e list have the high d-eng.npartner.loc	est priority. al	
Group Policy Ob This list obtained <u>N</u> ew	ejects higher in the d from: win2000-a A <u>d</u> d	e list have the high d-eng.npartner.loc	est priority. al	Шр



(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."

		ст. Объеми (м. н. с.	C	
Currer	nt Group Policy	UDJect Links for	Servers	
Group Policy Ob	iect Links		No Override	Disabled
N-Partner Pol	су			
Group Policy Obje	cts higher in the	: list have the hi	ghest priority.	
Group Policy Obje This list obtained f	cts higher in the rom: win2000-a	e list have the hi d-eng.npartner.l	ghest priority. ocal	
Group Policy Obje This list obtained f	cts higher in the rom: win 2000-a A <u>d</u> d	e list have the hi d-eng.npartner.l	ghest priority. ocal	<u>Шр</u>
Group Policy Obje This list obtained f <u>N</u> ew	cts higher in the rom: win2000-a A <u>d</u> d Dele <u>t</u> e	e list have the hi d-eng.npartner.l <u>E</u> dit <u>P</u> roperties	ghest priority. ocal	Uр Do <u>w</u> n
Group Policy Obje This list obtained f <u>N</u> ew <u>Options</u>	cts higher in the rom: win2000-a Add Dele <u>t</u> e	e list have the hi d-eng.npartner.l <u>E</u> dit <u>P</u> roperties	ghest priority. ocal	<u>U</u> р Do <u>w</u> n



(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."

🚮 Group Policy			- U ×
📙 Action View	🖸 X 🖫 🔗		
Tree	Policy 🛆	Computer Setting	
 N-Partner Policy [win2000-ad-eng.r Computer Configuration Software Settings Scripts (Startup/Shutdo Security Settings Account Policies Local Policies Local Policies Mult Policy Security Option: Security Log 	Image: Construction of the second	Success, Failure Success, Failure Not defined Success, Failure Not defined Not defined Success, Failure	
Restricted Groups System Services System Services Registry Prile System Public Key Policies Proble Key Policies Probl	Audit logon events Image: Define these policy settings Audit these attempts: Image: Define these policy settings Audit these policy settings <	OK Cancel	



(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].

🚮 Group Policy		<u>_</u> _×
Action View ⇐ → 🔁 💽 🗙	E 2	
Tree	Policy A	Computer Setting
Repartner Policy [win2000-ad-eng.npartner.	Maximum application log size	Not defined
Computer Configuration	Maximum security log size	204800 kilobytes
	Maximum system log size	Not defined
E- Windows Settings	Restrict guest access to application log	Not defined
Scripts (Startup/Shutdown)	Restrict guest access to security log	Not defined
🖻 🚽 😼 Security Settings	Restrict guest access to system log	Not defined
🕀 🥩 Account Policies	Betain application log	Not defined
E - 🛃 Local Policies	Betain security log	Not defined
🕀 🔁 Audit Policy	🕮 Retain system log	Not defined
🕒 🚮 User Rights Assignment	Betention method for application log	Not defined
Security Options	Retention method for security log	As needed
	BRetention method for system log	Not defined
E Settings for Event Logs	BShut down the computer when the security a	Not defined
Benistry	Security Policy Setting	? ×
	Maximum securitu log size	
😥 🗐 IP Security Policies on Active		
Administrative Templates		
🖻 👧 User Configuration	Define this policy setting	
E Software Settings	the second se	
🗄 💼 Windows Settings	204800 - kilobutes	
🗄 🛅 Administrative Templates	Kilobytes	
2800.00		
	F	
	L	
	-	



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



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

C:\> secedit /refreshpolicy machine_policy /enforce





2.2 Workgroup

2.2.1 Audit Policy Settings

(1) Search

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





(2) Search for Group Policy

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





(3) Local Group Policies: Audit Policies

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



(4) Open "Command Prompt."




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

C:\> secedit /refreshpolicy machine_policy /enforce

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:\>_
```



- 🗆 X

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.

💐 Search Results								- 🗆 ×
Eile Edit View Favorites Tools Help								-
Back + + + E Search Brolde	rs 🔇 History 📴 🔁 🗙	n .						
Address 🔊 Search Results							•	∂ Go
Search X								
C New 🥔		In Folder: <u>C:\Documents a</u>	nd Settings\All	Users\Start				
Search for Files and Folders	Search Results	Menu\Programs\Administra Size: 1,443 bytes - Type: Shortcut	ative Tools					
Search for files or folders named:		Modified: 2024/4/10 下午 1	.2:41					
Event Viewer								
Containing text:	🔿 📕 📗	&]	2	2	\$	\$	*	
	Web Events Event Viewer in	m_mseventl eventlog.dll	eventvwr	eventvwr	faxevent.dll	netevent.dll	nwevent.dll	
Look in:								
🖃 Local Harddrives (C:)								
Stop Search	AppEvent.Evt SecEvent.Evt S	5ysEvent.Evt regevent.mof						
Search Options >>								
Search for other items:								
Files or Folders								
Lomputers								
Internet								
Displays monitoring and troubleshooting messages fr	om Windows and other programs.							11.

(3) Edit Security Log

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

📲 Event Viewer						_ 🗆 ×
Action View	⇔ → 🗈 🖪		B			
Tree		Security Log 16	event(s)			
Event Viewer (Loca	al)	Туре	Date	Time	Source	Categ
Application Log	Qpen Log File Save Log File As. New Log View Clear all Events View Rename Refresh Export List Properties Help	Success Audit cuccess Audit uccess Audit	4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024 4/12/2024	4:56:20 PM 4:56:20 PM 4:56:20 PM 4:56:20 PM 4:51:31 PM 4:51:31 PM 4:51:31 PM 4:51:32 PM 4:51:22 PM 4:51:22 PM 4:51:22 PM 4:51:11 PM	Security Security Security Security Security Security Security Security Security Security Security Security Security Security	Object Object Object Object Object Object Object Object Object Object
		Success Audit	4/12/2024	4:51:11 PM	Security	Objec



(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."

ieneral Filter	1
Display name:	Security Log
Log name:	C:\WINNT\System32\config\SecEvent.Evt
Size:	64.0 KB (65,536 bytes)
Created:	Wednesday, April 10, 2024 12:43:49 PM
Modified:	Wednesday, April 10, 2024 12:46:58 PM
Accessed:	Wednesday, April 10, 2024 12:46:58 PM
When maxim	num log size is reached:



3. For Windows 2003

Windows Audit Policy Settings

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

⅔ 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."

🐗 Active Directory U	sers and Computers			_ 🗆 ×
Sile Action View	v <u>W</u> indow <u>H</u> elp			_ 8 ×
⇔ → € 🖪 🛱	1 🖻 🖻 😫 📝 🚺 🧖	1 10 7 4 1		
Active Directory Use	rs and Computer popartner local	5 objects		
E Saved Queries	Namo	Tupe	Description	
Compartner/local Densition Dens	Delegate Control Find Connect to Domain Connect to Domain Controller Raise Domain Functional Level Operations Masters	builtinDomain Container Organizational Container Container	Default container for upgr Default container for dom Default container for secu Default container for upgr	
	New I All Tas <u>k</u> s I Yiew I New Window from Here	Computer Contact Group InetOrgPerson MSMO Queue A	lias	
	Re <u>f</u> resh Export <u>L</u> ist	Organizational L Printer	Jnit	
	Properties	User Shared Folder		
	Help	1		
	×	_		
Create a new object				



(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	- Organizal	tional Unit		×
Ø	Create in:	npartner.local/		
N <u>a</u> me: Servers				
			ОК	Cancel

(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."

1ove		? ×
Move object into	ntainer:	
Porter Porter	iters n Controllers nSecurityPrincipals	
	ОК	Cancel

(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."

merar i manay	ed By COM+ G	iroup Policy	
E Cur	rent Group Policy (Dbject Links for Serv	ers
Group Policy (Dbject Links	No()verride Disable
iroup Policy Ob	jects higher in the	list have the highest	priority.
iroup Policy OL his list obtained <u>N</u> ew	ojects higher in the d from: WIN2003-4 A <u>d</u> d	list have the highest AD-ENG.npartner.loc Edit	priority. al <u>⊔</u> p

(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			?
General Manage	ed By COM+	Group Policy		
Curr	ent Group Policy	Object Links for Se	rvers	
Group Policy O	I <mark>biect Links</mark>	N	o Override	Disabled
N-Partner F	Policy			
Group Policy Ob This list obtained <u>N</u> ew	jects higher in the from: WIN2003+ Add	list have the highe AD-ENG.npartner.lr	est priority. ocal	Шр
Group Policy Ob This list obtained New Options	jects higher in the I from: WIN2003+/ Add Delete	list have the highe AD-ENG.npartner.lr <u>E</u> dit <u>P</u> roperties	est priority. local	<u>Ш</u> р Do <u>w</u> n
Group Policy Ob This list obtained New Options	jects higher in the from: WIN2003- Add Delete inheritance	list have the highe AD-ENG.npartner.k <u>E</u> dit <u>P</u> roperties	est priority. bocal	<u>U</u> р Do <u>w</u> n



(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."

🚡 Group Policy Object Editor			
Eile Action View Help			
N-Partner Policy [WIN2003-AD-EN] Computer Configuration Software Settings Windows Settings Scripts (Startup/Shutch Scripts (Startup/Shutch Account Policies Account Policies Restricted Groups Registry Registry Software Restriction Software Settings Registry Software Restriction Software Settings Software Restriction Software Settings Windows Settings Administrative Templates	ation log size ity log size m log size uests group from accessing a uests group from accessing s on log log og od for application log od for security log od for security log od for system log Retention method for secu Security Policy Setting Expl Color Policy Setting Expl Color Policy Setting Color verwrite events by Color verwrite events as Color overwrite events as Color overwrite events as Color overwrite events and applications. For more information (Q823659)	Policy Setting Not Defined As needed ain This Setting for security log days needed ents (clear log manually) g may affect compatibility with clients, serv , see Retention method for security log.	ices.
		OK Cancel	Apply
			J



(7) Event Logs: Maximum Size of Security Log

Expand folder "Computer Configuration" -> "Windows Settings" -> "Security Settings" -> "Event Log" ->

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

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





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



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



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





3.2 Workgroup

3.2.1 Audit Policy Settings

(1) Open Search

Click on "Start" -> "Search."

Administrator		
Manage Your Server	My Computer	
Windows Explorer	Administrative Tools	
Notepad	 <u>H</u> elp and Support	
	Opens a window where you can pic	k search options and work with search results.
All <u>P</u> rograms	-	
👔 Start 🛛 😰 🙈	Log Off 🚺 Shut Down	



(2) Search for Group Policy

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





(3) Local Group Policies: Audit Policies

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



(4) Open "Command Prompt."





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

C:\> gpupdate /force





3.2.2 Event Log Settings

(1) Open "Search."

Click on "Start" -> "Search."





(2) Search for "Event Viewer"

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





(3) Edit Security Log

Right-click on	"Security"	' -> And	click on	"Properties"
Night-Chek On	Jecunty	-> Anu	CHCK OH	Froperties.

📑 Event Viewer						
File Action Vi	ew <u>H</u> elp					
⇐ ⇒ 🗈 💽	🗗 🖻 😫 😫					
Event Viewer (I	Local)	Security 99 ev	ent(s)			
Application		Туре	Date	Time	Source	Cal 🔺
Security	Open Log File	Success Audit	4/12/2024	5:44:52 PM	Security	Ob
Bystein	Save Log File <u>A</u> s	Success Audit	4/12/2024	5:44:52 PM	Security	оь
	New Log View	Success Audit	4/12/2024	5:35:00 PM	Security	Pol
	⊆lear all Events	Success Audit	4/12/2024	5:35:00 PM	Security	ОЬ
		Success Audit	4/12/2024	5:35:00 PM	Security	ОЬ
	Tiem	Success Audit	4/12/2024	5:35:00 PM	Security	ОЬ
	Rena <u>m</u> e	Success Audit	4/12/2024	5:35:00 PM	Security	ОЬ
	Refresh	Success Audit	4/12/2024	5:34:45 PM	Security	Pol
	Export List	² Success Audit	4/12/2024	5:34:45 PM	Security	ОЬ
		Success Audit	4/12/2024	5:34:45 PM	Security	ОЬ
	Properties	Success Audit	4/12/2024	5:34:45 PM	Security	ОЬ
	Help	Success Audit	4/12/2024	5:34:45 PM	Security	ОЬ
-		Success Audit	4/12/2024	5:34:42 PM	Security	Pol
		Success Audit	4/12/2024	5:34:42 PM	Security	ОЬ
		Success Audit	4/12/2024	5:34:42 PM	Security	ОЬ
		of Success Audit	4/12/2024	5:34:42 PM	Security	ОЬ
		Success Audit	4/12/2024	5:34:42 PM	Security	Ob _1
		- · ·	414.01000.4			Ì
Opens the propertie	es dialog box for the cu	urrent selection.		j.		

(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.

⅔ 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."

File Action View Help Image: Second S	0 🗈 🛛 🖬 🔧	8. 🛅 🔻 🖂 🖇		
 Active Directory Users and 	🗐 🤷 😹 🛛 🗊 🔧	9. 🛅 🔻 🖂 🕄	2	
Active Directory Users and			3	
Saved Queries partner.local Builtin Computers Domain Cc ForeignSec Managed S Rai Users Opp	d Comput Name Builtin egate Control d ange Domain se domain functional level erations Masters	Type builtinDomain Container Organizational Container Container Container	Description Default container for upgr Default container for dom Default container for secu Default container for man Default container for upgr	
Nex All View Ref Exp Pro Hel	M A Tasks Ta	Computer Contact Group InetOrgPerson msImaging-PSPs MSMQ Queue Ali Organizational U Printer User Shared Folder	as	



(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."

w Object -	Organizationa	al Unit		
3	Create in: np/	artner.local/		
N <u>a</u> me:				_
Servers				
Protect	container from a	accidental deletion		_
			Coursel 1	Liele

(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."

love	×
Move object into container:	
Inpartner Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accounts Servers Users	
ОК	Cancel

(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."

New GPO	
Name:	
N-Partner Policy	
Source Starter GPO:	
(none)	×
	OK Cancel

(4) Edit Your Group Policy Object

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

File Action View Window Help Forest: npartner.local Forest: npartner.local Default Domain Policy Bomain Controllers Default Domain Controllers Servers Display links in this location: Inpartner.local Display links in this location: Inpartner.local Image: Servers Will Filters Stater Group Policy Objects Enforced Will Filters Stater Group Sites Vink Enabled Save Report Stater Save Report	🛃 Group Policy Management					
Image: Stress of the stress	😹 File Action View Window Help					_B×
Group Policy Management Group Policy Management Forest: npartner.local Default Domain Policy Default Domain Policy Group Policy Objects Group Policy Objects Forest: npartner.local Default Domain Policy Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Forest: npartner Policy Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Forest: npartner Policy Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Forest: npartner.local Forest: npartner.local Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Forest: npartner.local/Server Sites Save Report	🗇 🔿 🖄 📰 💥 🧟 🛛 🖬					
Group Policy Modeling	Group Policy Management Forest: npartner.local Domains Default Domain Policy Domain Controllers Servers N-Partner Policy WMI Filters Sites Sites Sites Group Policy Modeling View	N-Partner Policy Scope Details S Links Display links in this The following sites, ced nabled Report	tettings Delegation location: npartne domains, and OUs are links	er.local ed to this GPO: Enforced No	Link Enabled Yes	Path npartner.local/Server
Group Policy Results New Window from Here PO can only apply to the following groups, users, and computers: Delete Image: Comparison of the following groups, users, and computers: Rename Image: Comparison of the following groups, users, and computers: Refresh Image: Comparison of the following groups, users, and computers:	Group Policy Results	Window from Here e me ish	PD can only apply to the Jsers	following groups, u	users, and comp	
Help Add Remove Properties WMI Filtering This GPO is linked to the following WMI filter: (none>	Help	Add WMI Filtering This GP0 is linked <none></none>	to the following WMI filter:	Propertie	open	



(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].

📕 Group Policy Management Editor			×
File Action View Help			
🗢 🔿 🙍 📷 💥 🖻 😼 🚺 🖬			
N-Partner Policy [WIN2008-AD-ENG.NPARTN	Policy 🔺	Policy Setting	1
🖻 🞥 Computer Configuration	Maximum application log size	Not Defined	
E Policies	Maximum security log size	204800 kilobytes	
Software Settings	Maximum system log size	Not Defined	
Windows Settings	📓 Prevent local guests group from accessing application log	Not Defined	
Seriets (Startup/Shutdown)	Revent local guests group from accessing security log	Not Defined	
Scripts (Startup) Shacdowny	Revent local guests group from accessing system log	Not Defined	
E Account Policies	Retain application log	Not Defined	
E Local Policies	Retain security log	Not Defined	
🕀 📻 Event Log	📓 Retain system log	Not Defined	
🛨 📴 Restricted Groups	Retention method for application log	Not Defined	
🕀 📴 System Services	Retention method for security log	As needed	
🕀 📴 Registry	Retention method for system log	Not Defined	
🕀 📴 File System	Maximum security log size Propert	ies ? 🗙	
∰ Wired Network (IEEE 802			
Windows Firewall with Act	Security Policy Setting Explain		
Network List Manager Po	Maximum securitu log size		
Contraction Police			
🛨 🧮 Network Access Protectic	Define this policy setting		
표 🧮 Application Control Policie			
표 🌏 IP Security Policies on Ac	204000 1		
🕀 🚞 Advanced Audit Policy Co			
🕀 🍿 Policy-based QoS			
🕀 🧰 Administrative Templates: Policy	Modifying this setting may affe	ect compatibility with clients, services,	
Preferences	A and applications.	······	
E 15 User Configuration	For more information, see <u>Ma</u>	ximum security log size. (U823659)	
		OK Cancel Apply	
1			



(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."

📕 Group Policy Management Editor			_ 🗆 🗙
File Action View Help			
🗢 🔿 🞽 📅 💥 🖹 😹 🚺 🖬			
Image: Account view rep Image: Account view rep Image: Account Policy (WIN2008-AD-ENG.NPARTIN Image: Policy (WIN2008-AD-ENG.NPARTIN Image: Policy (Statup/Shutdown) Image: Policy (Statup/Shutdown)	Policy Imaximum application log size Maximum security log size Maximum system log size Prevent local guests group from accessing application log Prevent local guests group from accessing system log Retain application log Retain security log Retain security log Retain security log Retain security log Retain system log Retention method for security log Retention method for security log Retention method for system log Security Policy Setting Explain Explain Retention method for system log Security Policy Setting Retention method for system log Coverwrite events by days Define this policy setting Overwrite events as needed Do not overwrite events log Modifying this setting may af and applications. For more information, see Ret (J823659)	Policy Setting Not Defined 204800 kilobytes Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined As needed Not Defined As needed Not Defined 1 Properties	
		OK Cancel Annly	

(8) Open "Windows PowerShell" on your Windows server.





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



(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 : \\WIN2008-ENG\Root\Rsop\NS88B7CBA8_43A2_4485_8E2D_E6951C81A7BE Namespace LoggingComputer : WIN2008-ENG : NPARTNER\Administrator LoggingUser LoggingMode : Computer <u>PS</u> 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

RTNER\WIN2008-ENG - Internet Explorer		
🖉 🖉 C:\tmp\WIN2008-ENG.html 🛛 🔎 💽 🍕	NPARTNER\WIN2008-ENG ×	ŵ
No data available.		
puter Configuration		
ides		
Vindows 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		
Policy	Setting	Winning GPO
Network access: Allow anonymous SID/Name translation	Disabled	Default Domain Policy
Network Security		



4.2 Workgroup

4.2.1 Audit Policy Settings

(1) Open Local Group Policy Editor

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





(2) Local Group Policies: Audit Policy

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



(3) Open "Windows PowerShell."





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

PS C:\> gpupdate /force



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

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

PS C:3/ auditpol /stt/category:* System audit policy Settem suff version Success and Failure System Success and Failure System Fuencial Internation Success and Failure System System Fuencial Success and Failure System System Fuencial Success and Failure Discurity State Ohange Success and Failure Discust Lockout Success and Failure Phese Nain Mode Success and Failure Discust Lockout Success and Failure Discust Access Success and Failure	🗷 Administrator: Windows PowerShell		_ 🗆 🗙
System Audit Policy System fully System Extension System System Fully Sys	PS C:\> auditpol /get /category:*		
Source of Source Source Sources and Failure Source Interrity Sources and Failure Source Source Sources and Failure Deterrison Events Sources and Failure Deterrison Deterison Deterison Deterrison Deterrison Deterrison Deterrison Det	System audit policy Category(Subcategory	Setting	
Security System Extension Success and Failure System Internity Success and Failure Inter System Events Success and Failure Learn/Losoff Success and Failure Learn/Losoff Success and Failure Learn/Losoff Success and Failure Learn/Losoff Success and Failure Here Guick Mode Success and Failure Bestin Loson Here Success File System Success and Failure Here Guick Mode Success and Failure Here Guick Mode Success and Failure Here Guick Mode Success and Failure Here Success File System Success and Failure Here Here Here Here Success and Failure Here Here Here Here Here Success and Failure Here Here Here Here Here Here Here Here	System	occerns	
System Integrity Bace Diriver Contacts and Failure Security Site Contacts and Failure Security Site Contacts and Failure Security Site Contacts and Failure Logoff Logo Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logoff Logo Logoff Logoff Logoff Logo Logoff Log	Security System Extension	Success and Failure	
Other System Success and Failure Logon/Logoff Success and Failure Logon/Logoff Success and Failure Logon/Logoff Success and Failure Logon/Logoff Success and Failure Prescutive/Logon/Logoff Success and Failure Prescutive/Logon/Logoff Success and Failure Prescutive/Logon/Logoff Success and Failure Prescutive/Logon/Logoff Success and Failure Dilet Accest Success and Failure Prescutive/Logon/Logoff Success and Failure Dilet Accest Success and Failure Prescutive/Logon/Logoff Success and Failure Dilet Accest Success and Failure File System Success and Failure Failure Success and Failure Success and Failure Success and Failure Failure Success and Failure Success and Failure Success and Failure Suc	System Integrity IPsec Driver	Success and Failure Success and Failure	
Security State Change Success and Failure Logon/Logit Logon/Logit Success and Failure House Link Mode Success and Failure House Link Mode Success and Failure Prace Link Mode Success and Failure Prace Link Mode Success and Failure Prace Link Mode Success and Failure Beet Logon Other Logon/Logoff Events Success and Failure Other Logon/Logoff Events Success and Failure Hetwork Folloy Server Success and Failure Other Logon/Logoff Events Success and Failure Hetwork Folloy Server Success and Failure Hetwork Folloy Server File State File Sta	Other System Events	Success and Failure	
Logon/Logonf Logon/Logonf Logon/Logonf Hocount Lookouth Prese Built Mode Prese Built Mode Prese Built Mode Prese Built Mode Success and Fail Ure Prese Built Mode Success and Fail Ure Prese Built Mode Success and Fail Ure Differ Logon/Logonf Events Nuccess and Fail Ure Differ Logon/Logonf Events Success and Fail Ure Metwork Policy Server Success and Fail Ure Prese Built Mode Disct Access File System Hetwork Policy Server Success and Fail Ure Hetwork Policy Server Success and Fail Ure Faile System Handle Manipulation File System File Share File Share Success and Fail Ure Success and Fail Ure Success and Fail Ure File Share File Share Success and Fail Ure File Share File Share File Share Success and Fail Ure File Share File Share Success and Fail Ure Success and Fail Ure File Share File Share Success and Fail Ure Success and Fail Ure File Share Success and Fail Ure File Share Success and Fail Ure Success and Fail	Security State Change	Success and Failure	
Ution Subcess and Failure IPace Duikk Mode Subcess and Failure Uter Logon/Doorf Events Subcess and Failure Dist. Access Subcess and Failure Dist. Access Subcess and Failure Restry Subcess and Failure Prist. Subcess and Failure Restry Subcess and Failure Prist. Subcess and Failure File Share Subcess and Failure File	Logon/Logoff	Surgers and Failling	
Account Lockout Success and Failure Pase Main Mode Success and Failure Pase Extended Mode Success and Failure Sterial Logon Success and Failure Wetwork Folloy Server Dist Access Test Extense Remain Conserver Success and Failure Dist Access Test Extense Remain Conserver Success and Failure Success and Failure Certification Services Success and Failure Success and Failure Certification Services Success and Failure Success and Failure Certification Services Success and Failure Success and Failure File Share File Share File Share Fritering Platform Packet Drop Success and Failure Success and Failure Success and Failure Success and Failure File Share Fritering Platform Packet Drop Success and Failure File Share Fritering Platform Success and Failure Success and Failure Success and Failure Success and Failure Success and Failure Fritering Platform Success and Failure Success and Failure Fritering Platform Success and Failure Success and Failure Success and Failure Success and Failure Fritering Platform Success and Failure Success and F	Logoff	Success and Failure	
IPsec Duick Mode Success and Failure IPsec Extended Mode Success and Failure Secial Logon Success and Failure Other Logon/Logoff Events Success and Failure Direit Access Success and Failure Application Services Success and Failure Application Generated Success and Failure Fillers Park Success and Failure Fillers Platforn Connection Success and Failure Fillering Platforn Connection Success and Failure Privilege Use No Auditing Protess Creation No Auditing Protess Creation No Auditing Process Creation	Account Lockout	Success and Failure	
Interect Work Mode Interection of Events Strenge Locan Methods Mode Strenge Locan Methods Mole Strenge Locan Methods Mole Methods Mole	IPsec Main Mode	Success and Failure	
Special Loom Success and Failure Other Loom/Looff Events Success and Failure Network Folicy Server Success and Failure File System Success and Failure Reistry Success and Failure SM Success and Failure Certification Generated Success and Failure SM Success and Failure Certification Generated Success and Failure Hendle Manipulstion Success and Failure File Share Success and Failure Protess Events Success and Failure Detailed Faile Share Success and Failure Protess Creation No Auditing PDAPI Action Folicy Change Success Audit Policy Change Success Author Strip Change No Auditing Protess Creation No Auditing Pual action Folicy Change <td< td=""><td>IPsec Wilck Mode IPsec Extended Mode</td><td>Success and Failure</td><td></td></td<>	IPsec Wilck Mode IPsec Extended Mode	Success and Failure	
Other Logon/Logoff Events Success and Failure Object Access Success and Failure Registry Success and Failure Resistry Success and Failure SAM Success and Failure Application Generated Success and Failure Hendle Manipulation Success and Failure Other Object Access Success and Failure Filtering Platform Connection Success and Failure Other Object Access Events Success and Failure Provise Filter Filtering Platform Connection Success and Failure Provise Filter Filtering Platform Connection Success and Failure Provise Filter Filtering Platform Connection Success and Failure Provise Filtering Platform Success and Failure Success and Failure Provise Filtering Platform Success and Failure Success and Failure Provise Filtering Platform Success and Failure Success and Failure Provise Filtering Platform Platfore No Auditing	Special Logon	Success and Failure	
Mettorik Folicy Server Success and Failure File System Success and Failure Resistry Success and Failure Method Success and Failure Method Success and Failure Method Success and Failure Method Success and Failure Application Services Success and Failure Application Generated Success and Failure Hondle Manipulation Success and Failure File Fing Platform Packet Drop Success and Failure Priviles Success and Failure Other Object Access Events Success and Failure Detailed Tracking Success and Failure Process Itermination No Auditing Process Creation No Auditing </td <td>Other Logon/Logoff Events</td> <td>Success and Failure</td> <td></td>	Other Logon/Logoff Events	Success and Failure	
File System Success and Failure Registry Success and Failure SAM Success and Failure Operation Generated Success and Failure Handle Manipulation Success and Failure Handle Manipulation Success and Failure File Share Success and Failure Filtering Platform Connection Success and Failure Filtering Platform Connection Success and Failure Detailed File Share Success and Failure Sensitive Privilege Use No Auditing Non Sensitive Privilege Use No Auditing Process Tranination No Auditing Process Traning No Auditing Distroicy Change No Auditing <td>Network Policy Server</td> <td>Success and Failure</td> <td></td>	Network Policy Server	Success and Failure	
Resistry Success and Failure SMM Success and Failure SMM Success and Failure Application Generated Success and Failure Hendle Manipulation Success and Failure File Share Success and Failure File Share Success and Failure Filtering Platform Packet Drop Success and Failure Other Object Access Events Success and Failure Detailed File Share Success and Failure Detailed File Share Success and Failure Provess Termination No Auditing Other Object Charges No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Mit Policy Change No Auditing MSSYOR Nule-Level Policy Change No Auditing MMSSYOR Policy Change Events No Auditing Obmet Policy Change Events No Auditing MSSYOR Syor Rule-Level Policy Change No Auditing MSSYOR Syor Rule-Level Policy Change No Auditing Nouccess and Failure Obmet Policy Change Sand Failure <td>File System</td> <td>Success and Failure</td> <td></td>	File System	Success and Failure	
Kernel Ubject Success and Failure SMM Success and Failure Certification Services Success and Failure Application Generated Success and Failure Filleshare Success and Failure Filleshare Success and Failure Filtering Platform Connection Success and Failure Detailed File Share Success and Failure Privilege Use Success and Failure Sensitive Privilege Use No Auditing Other Privilege Use Events No Auditing Detailed Tracking No Auditing Process Tremination No Auditing Process Treation No Auditing Process Treation No Auditing Price Use Success Authentication Policy Change No Auditing MtSNC Rule-Level Policy Change No Auditing Other Prolicy Change Events No Auditing Computer Account Management Success and Failure Obstribution Group Management Success and Failure Success and Failure Success and Failure Security Group Management	Registry	Success and Failure	
Definition Decess and Failure Application Generated Success and Failure Handle Manipulation Success and Failure File Share Success and Failure File Share Success and Failure Filering Platforn Packet Drop Success and Failure Filering Platforn Connection Success and Failure Other Object Access Events Success and Failure Detailed File Share No Auditing Own Sensitive Privilege Use No Auditing Other Object Versities No Auditing Other Privilege Use No Auditing Process Termination No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing MCOmpter Policy Change Success Authorization Policy Change No Auditing Mesount Management Success and Failure Obscrut Management Success and Failure Ob	Kernel Ubject	Success and Failure Success and Failure	
Application Generated Success and Failure Hendle Mnipulation Success and Failure File Share Success and Failure Filtering Platform Packet Drop Success and Failure Detailed File Share Success and Failure Privilege Use No Auditing Non Sansitive Privilege Use No Auditing Process Fermination No Auditing Process Fermination No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Authorization Policy Change Success and Failure Authorization Policy Change No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Authorization Policy Change No Auditing Change No Auditing Diterct	Certification Services	Success and Failure	
Hendle Manipulation Success and Failure File Share Success and Failure Filtering Platform Packet Drop Success and Failure Other Object Access Events Success and Failure Detailed File Share Success and Failure Privilege Use No Auditing Sensitive Privilege Use No Auditing Other Privilege Use Events No Auditing Process Termination No Auditing Process Creation No Auditing Process Creation No Auditing Policy Change Success Authentication Policy Change No Auditing Philes Change Success Authentication Policy Change No Auditing Process Creation No Auditing Philes Change No Auditing Policy Change No Auditing MSSNC Rule-Level Policy Change No Auditing MSSNC Rule-Level Policy Change No Auditing User Account Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing </td <td>Application Generated</td> <td>Success and Failure</td> <td></td>	Application Generated	Success and Failure	
Filtering Platform Packet Drop Success and Failure Filtering Platform Connection Success and Failure Dther Object Access Events Success and Failure Detailed File Share Success and Failure Privilege Use No Auditing Sensitive Privilege Use No Auditing Detailed File Share No Auditing Detailed Fracking No Auditing Process Termination No Auditing Process Creation No Auditing Policy Change Success Authentication Policy Change Success Authentication Policy Change No Auditing Process Creation No Auditing User Account Management Success and Failure Other Policy Change Sent No Auditing Discriburd Management <td>Handle Manipulation</td> <td>Success and Failure</td> <td></td>	Handle Manipulation	Success and Failure	
Filtering Platform Connection Success and Failure Other Object Access Events Success and Failure Privilege Use Success and Failure Sensitive Privilege Use No Auditing Other Privilege Use No Auditing Other Privilege Use No Auditing Detailed Tracking No Auditing Process Formination No Auditing Process Creation Policy Change No Auditing MMSSVC Rule-Level Policy Change No Auditing Other Prolicy Change No Auditing Other Prolicy Change No Auditing Process Creation No Auditing MMSSVC Rule-Level Policy Change No Auditing Other Policy Change Events No Auditing Directory Service Changeent Success and Failure Disectority Group Management Success and Failure Disectory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Success	Filtering Platform Packet Drop	Success and Failure	
Other Object Access Events Success and Failure Detailed File Share Success and Failure Privilege Use No Auditing Other Privilege Use Events No Auditing Detailed Tracking Process Termination Process Termination No Auditing Process Termination No Auditing Process Termination No Auditing Process Creation No Auditing Other Account Management Success and Failure	Filtering Platform Connection	Success and Failure	
Detailed File Share Success and Failure Sensitive Privilege Use No Auditing Other Privilege Use No Auditing Detailed Tracking No Auditing Process Termination No Auditing Process Termination No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Process Creation No Auditing Audit Policy Change Success Authentication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Computer Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Replication No Audit	Other Object Access Events	Success and Failure	
Sensitive Privilege Use No Auditing Non Sensitive Privilege Use No Auditing Other Privilege Use Events No Auditing Process Termination No Auditing DPAPI Activity No Auditing Process Creation No Auditing Process Creation No Auditing Policy Change Success Authentication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Other Policy Change Events No Auditing Tiltering Platform Policy Change No Auditing Other Policy Change Events No Auditing User Account Management Success and Failure Distribution Group Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Changes Success and Failure Directory Service Replication No Auditing Directory Service Replication Success and Failure Directory Service Replication Success and Failure Directory Service Replication Success and Failure Directory Service Replication Success and Failure Other Account Logon Events Success and Failure Success and Failure	Privileze lise	Success and Fallure	
Non Sensitive Privilese Use No Auditing Other Privilese Use Events No Auditing Process Termination No Auditing DPAPI Activity No Auditing RPC Events No Auditing Process Creation No Auditing Policy Change Success Authorization Policy Change No Auditing MFSSVC Rule-Level Policy Change No Auditing Filtering Platform Policy Change No Auditing Other Privilese Use No Auditing Policy Change No Auditing MfSSVC Rule-Level Policy Change No Auditing Filtering Platform Policy Change No Auditing Other Policy Change Events No Auditing Account Management Success and Failure Computer Account Management Success and Failure Obscription Group Management Success and Failure Other Account Management Events Success and Failure Of Access No Auditing Directory Service Replication No Auditing Directory Service Reprications Success and F	Sensitive Privilege Use	No Auditing	
Uther Privilege Use Events No Auditing Detailed Tracking No Auditing Process Termination No Auditing DPAP1 Activity No Auditing Process Creation No Auditing Process Creation No Auditing Policy Change Success Audit Policy Change No Auditing Authorization Policy Change No Auditing MSSVC Rule-Level Policy Change No Auditing Dither Policy Change Events No Auditing Other Policy Change Events No Auditing Deter Policy Group Management Success and Failure Security Group Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication	Non Sensitive Privilege Use	No Auditing	
Dock The Process Termination No Auditing DPAPI Activity No Auditing Process Creation No Auditing Policy Change Success Authentication Policy Change Success Authentication Policy Change No Auditing Process Creation No Auditing Policy Change Success Authentication Policy Change No Auditing Pristering Platform Policy Change No Auditing Pristering Platform Policy Change No Auditing Other Policy Change Events No Auditing Other Policy Change Events No Auditing Other Policy Change Events No Auditing Other Account Management Success and Failure User Account Management Success and Failure Discribution Group Management Success and Failure Other Account Management Events Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Access Success and Failure Other Account Logon Events Success and Failure	Uther Privilege Use Events Detailed Tracking	No Auditing	
DPAPI Activity No Auditing RPC Events No Auditing Process Creation No Auditing Policy Change Success Audit Policy Change Success Authentication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Other Policy Change No Auditing User Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Directory Service Changes No Auditing Directory Service Replication Success and Failure Other Account Logon Events Success and Failure Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure <td>Process Termination</td> <td>No Auditing</td> <td></td>	Process Termination	No Auditing	
RPC Events No Auditing Process Creation No Auditing Policy Change Success Autherlication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Process Rule-Level Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Recount Management Success and Failure Computer Account Management Success and Failure Security Group Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Other Account Logon Success and Failure Other Account Logon Events Su	DPAPI Activity	No Auditing	
Audit Policy Change Success Authentication Policy Change Success Authentication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Tiltering Platform Policy Change No Auditing Other Policy Change Events No Auditing Other Policy Change Events No Auditing User Account Management Success and Failure Descurity Group Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Access Success and Failure Other Account Logon Kerberos Success and Failure Other Account Logon Service Service Ticket Operations Success and Failure Rerberos Authentication Service Success and Failure Success and Failu	RPC Events Presence Creation	No Auditing No Auditing	
Audit Policy Change Success Authon Ication Policy Change No Auditing Mthorization Policy Change No Auditing MFSSVC Rule-Level Policy Change No Auditing Dther Policy Change Events No Auditing Other Policy Change Events No Auditing User Account Management Success and Failure Discription Group Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Access Success and Failure Other Account Logon Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Retberos Authentication Success and Failure	Policy Change	NO HOUTCHIS	
Authentication Policy Change Success Authentication Policy Change No Auditing MPSSVC Rule-Level Policy Change No Auditing Filtering Platform Policy Change No Auditing Other Policy Change Events No Auditing User Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Replication Success and Failure Other Account Logon Kocess Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Success and Failure Su	Audit Policy Change	Success	
Addrift 2atroin Policy Change No Addrifting MRSSNC Rule-Level Policy Change No Auditing Filtering Platform Policy Change No Auditing Other Policy Change Events No Auditing Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Credential Validation Success and Failure	Authentication Policy Change		
Filtering Platform Policy Change No Auditing Other Policy Change Events No Auditing Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Replication No Auditing Directory Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Success and Failure	MPSSVC Rule-Level Policy Change	No Auditing	
Other Policy Change Events No Auditing Account Management Success and Failure Computer Account Management Success and Failure Distribution Group Management Success and Failure Distribution Group Management Success and Failure Other Account Management Success and Failure Other Account Management Success and Failure Other Account Management Events Success and Failure Other Account Management Events Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Access Success and Failure Account Logon Kerberos Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Success and Failure Other Account Logon Events Success and Failure Success and Failure Other Account Logon Events Success and Failure Success and Failure Retberos Authentication Service Success and Failure Success and Failure PS C:\> Success and Failure Success and Failure	Filtering Platform Policy Change	No Auditing	
Account Management Success and Failure Computer Account Management Success and Failure Security Group Management Success and Failure Distribution Group Management Success and Failure Other Account Management Events Success and Failure Directory Service Changes No Auditing Directory Service Replication No Auditing Directory Service Access Success and Failure Other Account Logon Kerberication Success and Failure Directory Service Replication Success and Failure Directory Service Access Success Account Logon Kerberos Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Sterberos Authentication Service Success and Failure Service Jailed Directory Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Success and Failure	Other Policy Change Events	No Auditing	
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 Directory Service Changes No Auditing Directory Service Replication No Auditing Detailed Directory Service Replication No Auditing Detailed Directory Service Replication Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Credential Validation Success and Failure	User 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 Directory Service Changes No Auditing Directory Service Replication No Auditing Detailed Directory Service Replication No Auditing Directory Service Access Success and Failure Other Account Logon Events Success and Failure Other Account Logon Events Success and Failure Credential Validation Success and Failure	Computer Account Management	Success and Failure	
Distribution uroup Management Success and Failure Application Group Management Success and Failure Other Account Management Events Success and Failure Directory Service Changes No Auditing 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 Other Account Logon Events Success and Failure Credential Validation Success and Failure PS C:>-	Security Group Management	Success and Failure	
Attributed Success and Failure Other Account Management Events Success and Failure DS Access Directory Service Replication Directory Service Replication No Auditing Directory Service Access Success and Failure Kerberos Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Credential Validation Success and Failure PS C:\> Success and Failure	Application Group Management	Success and Failure	
DS Access Directory Service Changes No Auditing Directory Service Replication No Auditing Detailed Directory Service Replication No Auditing Directory Service Access Account Logon Kerberos Service Ticket Operations Success and Failure Other Account Logon Events Success and Failure Rerberos Authentication Service Success and Failure Credential Validation Success and Failure	Other Account Management Events	Success and Failure	
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 Credential Validation Success and Failure PS C:V-	DS Access	10 A 10 10 10	
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	Directory Service Unanges Directory Service Replication	No Auditing No Auditing	
Directory Service Access Success Account Logon Events Success and Failure Other Account Logon Events Success and Failure Kerberos Authentication Service Success and Failure Credential Validation Success and Failure PS C:/>	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:\>	Directory Service Access	Success	
Other Acount Logon Events Success and Failure Kerberos Authentication Service Success and Failure Credential Validation Success and Failure PS C:/>= Success and Failure	Account Logon Kerbaros Service Ticket Operations	Success and Failure	
Kerberos Authentication Service Success and Failure Credential Validation Success and Failure PS C:\>	Other Account Logon Events	Success and Failure	
Credential Validation Success and Failure PS C:>	Kerberos Authentication Service	Success and Failure	
	Credential Validation	Success and Failure	T



4.2.2 Event Log Settings

(1) Search for "Event Viewer"

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

vrograms(1)			
🛃 Event Viewer			
Iontrol Panel (1)			
🤠 View event logs			
🔎 See more results			
Zvent Viewer	×	Log off	



(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 - Syst	em (Type: Administrative) 🛛 🛛 🔀
General Subscriptio	ns
Full Name:	System
Log path:	%SystemRoot%\System32\Winevt\Logs\System.evtx
Log size:	2.07 MB(2,166,784 bytes)
Created:	Wednesday, April 10, 2024 PM 02:56:00
Modified:	Monday, April 15, 2024 PM 02:14:42
Accessed:	Wednesday, April 10, 2024 PM 02:56:00
 Enable logging Maximum log size When maximum e Overwrite e Overwrite e Archive the Do not ove 	: (KB): 204800 == event log size is reached: events as needed (oldest events first) e log when full, do not overwrite events rwrite events (Clear logs manually)
	Clear Log
	OK Cancel Apply



5. For Windows 2012

Windows Audit Policy Settings

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

⅔ 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

Active Directory Users and Computers				
File Action View Help		k 🛅 🍸 🗾 🕄	R	
Active Directory Users and Com Saved Queries Builtin builtinDu Computers Delegate Control Find Change Domain Change Domain Controller Raise domain functional level Operations Masters New All Tasks View Refresh Export List Properties		Type builtinDomain Container nal	Description Default container for up Default container for do Default container for sec Default container for ma Default container for up	
		• •	Computer Contact Group InetOrgPerson msImaging-PSPs MSMQ Queue Alias Organizational Unit	
< III > Create a new object			Printer User Shared Folder	

"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 "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."

Move
Move object into container:
OK Cancel

(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."

Ŷ
OK Cancel

(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."

E.	Group Policy Manag	ement			- 🗆 X
📓 File Action View Window Help	1				_ 8 ×
File Action View Window Help Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Image: Servers Ima	N-Partner Policy Scope Details Settings Delegation Links Display links in this location: The following sites, domains, and O Location Edit Enforced Link Enabled Save Report View New Window from Here	ation npartner.loca US are linked to t	I his GPO: Enforced No	Link Enabled Yes	Path npartner.loc
	Delete Rename Refresh Help This GPO is linked to the following <none></none>	iove	Properties	Open	
Open the GPO editor					



(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.



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.



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.

2 C:\tmp\WIN2012-ENG.html	NPARTNER\WIN2012-ENG ×			6
Local Policies/Audit Policy				
Policy	Setting		Winning GPO	
Audit account logon events	Success, Failure		N-Partner Policy	
Audit account management	Success, Failure		N-Partner Policy	
Audit directory service access	No auditing		N-Partner Policy	
Audit logon events	Success, Failure		N-Partner Policy	
Audit object access	Success, Failure		N-Partner Policy	
Audit policy change	No auditing		N-Partner Policy	
Audit privilege use	No auditing		N-Partner Policy	
Audit process tracking	No auditing		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	
Network Security				
Policy	Setting		Winning GPO	
Network security: Do not store LAN Manager hash value on next password change	Enabled		Default Domain Policy	
Network security: Force logoff when logon hours expire	Disabled		Default Domain Policy	
Event Log				
Policy	Setting		Winning GPO	
Maximum security log size	204800 kilobytes		N-Partner Policy	
Retention method for security log	As needed		N-Partner Policy	
Public Key Policies/Certificate Services Client - Auto-Enrollmen	t Settings			
Policy	Setting		Winning GPO	
Automatic certificate management	Enabled		[Default setting]	
Option		Setting		
Enroll new certificates, renew expired certificates, process pending of certificates	ertificate requests and remove revoked	Disabled		
Indate and manage certificates that use certificate templates from A	ctive Directory	Disphlad		



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.



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

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

Ð	Select Administrator: Windows PowerShell	- 🗆 X
PS C:\Users\Administrator> au	uditpol /get /category:*	×
System audit policy		
Category/Subcategory	Setting	
System	Success and Enilume	
System Integrity	Success and Failure	
TPsec 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	
Other Logon /Logoff Events	Success and Failure	
Network Policy Server	Success and Failure	
User / Device Claims	Success and Failure	
Object Access	Success and rarrare	
File System	Success and Failure	
Registry	Success and Failure	
Kernel Óbject	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 Connect	ion 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	e No Auditing	
Other Privilege Use Events	No Auditing	
Sensitive Privilege Use	No Auditing	
Detailed Tracking		
Process Creation	No Auditing	
Process Termination	No Auditing	
Microsoft Bonomofo *	No Auditing	
		3
		1.7.01040

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."

			Event Viewer			_ 0	x
File Action View	Help						
(† †) 🖄 🖬 🛛							
📳 Event Viewer (Loca	l) Security	Number of	events: 7,113				
Custom Views	Keywords	Date	and Time	Source	Event ID	Task Category	^
Application	Audit S	Succ 4/15	/2024 PM 05:03:52	Microsoft Wi	5156	Filtering Platf	
Security	🔍 Audit S	Succ 4/15	/2024 PM 05:03:52	Microsoft Wi	5156	Filtering Platf	
Setup	Open Saved Log		024 PM 05:03:52	Microsoft Wi	5156	Filtering Platf	
System	Create Custom View		024 PM 05:03:51	Microsoft Wi	4656	File System	
Forward	Import Curtom View		024 PM 05:03:51	Microsoft Wi	4656	File System	
Application	Import Custom view		024 PM 05:03:51	Microsoft Wi	4658	File System	
🚰 Subscriptio	Clear Log		024 PM 05:03:51	Microsoft Wi	4656	File System	
	Filter Current Log		024 PM 05:03:51	Microsoft Wi	4658	File System	
	Properties		024 PM 05:03:51	Microsoft Wi	4690	Handle Mani	
	Find		024 PM 05:03:36	Microsoft Wi	5156	Filtering Platf	
	Save All Events As		024 PM 05:01:51	Microsoft Wi	5156	Filtering Platf	_
	Attach a Tack To this L		024 PM 05:01:51	Microsoft Wi	5156	Filtering Platf	
	Attach a Task To this Lo	·g	indows security auditi	ng.			×
	View	+					
	Refresh					1	
	Help		ng Platform has permi	tted a connection.			<u> </u>
	oilaaA	ation Inform	nation:			~	_
							~
< 111	>			m			
Displays Log 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."
```

	Log Properties - Security (Type: Administrative)
General	
Full Name:	Security
Log path:	%SystemRoot%\System32\Winevt\Logs\Security.evtx
Log size:	5.07 MB(5,312,512 bytes)
Created:	Wednesday, April 10, 2024 PM 03:30:07
Modified:	Monday, April 15, 2024 PM 03:26:55
Accessed:	Wednesday, April 10, 2024 PM 03:30:07
Enable logging Maximum log siz When maximum Overwrite Archive th O not ov	g ze (KB): 204800 event log size is reached: events as needed (oldest events first) ne log when full, do not overwrite events rerwrite events (Clear logs manually) Clear Log
	OK Cancel Apply



6. For Windows 2016

Windows Audit Policy Settings

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

⅔ 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."

w Object - Organiza	itional Unit	
Create in:	npartner.local/	
Name:		_
Servers		
Protect container fr	rom accidental deletion	
Protect container fi	rom accidental deletion	
Protect container fi	rom accidental deletion	
Protect container fi	rom accidental deletion	
Protect container fi	rom accidental deletion	

(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."

⊡…∰ npartner ⊕… <mark>∭</mark> Builtin			
	s ontrollers :curityPrincipals Service Account	ts	
🕀 🚺 Users			

(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."

<u>Name:</u> N-Partner Policy	
Source Starter GPO:	

(4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is "N-Partner Policy") and click

elp				- 5
N-Partner Policy Scope Details Settings Delegati Links Display links in this location: The following sites, domains, and OU	on npartner.k Is are linked	ocal to this GPO:		~
Location		Enforced	Link Enabled	Path
Edit		No	Yes	npartner.local/{
Enforced Link Enabled Save Report	to the foll	owing groups, us	ers, and computers:	>
New Window from Here				
Delete Rename Refresh	e	Properties		
Help				
This GPO is linked to the following W	/MI filter:			
	elp N-Partner Policy Scope Details Scope Details Display links in this location: The following sites, domains, and OU Location Enforced Link Enabled Save Report View New Window from Here Delete Rename Refresh Help This GPO is linked to the following W	N-Partner Policy Scope Details Settings Display links in this location: npartner.k The following sites, domains, and OUs are linked Location Edit Enforced Link Enabled Save Report View New Window from Here Delete Rename Refresh Help This GPO is linked to the following WMI filter:	elp N-Partner Policy Scope Details Settings Delegation Links Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Location Enforced Enforced Link Enabled Save Report View New Window from Here Delete Rename Refresh Help This GPO is linked to the following WMI filter:	elp N-Partner Policy Scope Details Settings Display links in this location: npartner.local The following sites, domains, and OUs are linked to this GPO: Location Enforced Link Enabled Save Report View New Window from Here Delete Rename Refresh Help This GPO is linked to the following WMI filter:



(5) Local Group Policies: Audit Policy

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





(6) Event Logs: Maximum Size of Security Log

Expand folder "Computer Configuration" -> "Windows Settings" -> "Security Settings" -> "Event Log" ->

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

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





(7) Event Logs: Retention Method for Security Log

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

Group Policy Management Editor			- 🗆 X
File Action View Help			
🗢 🤿 🙍 📆 🗙 🗊 🛃 🖬			
 N-Partner Policy [WIN2016-AD-ENG.NPA Computer Configuration Policies Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown Deployed Printers Security Settings Account Policies Local Policies Local Policies Event Log Restricted Groups System Services Registry File System Wired Network (IEEE 80 Windows Firewall with Network List Manager Wireless Network (IEEE Public Key Policies Software Restriction Pc Advanced Audit Policy Molicy-based QoS Preferences Wiref Configuration Policies Preferences Preferences Preferences 	Policy Maximum application log size Maximum security log size Maximum system log size Prevent local guests group from accessing application log Prevent local guests group from accessing security log Prevent local guests group from accessing system log Retain application log Retain system log Retention method for application log Retention method for security log Retention method for security log Properties Retention method for security log Properties Retention method for security log Prevent local guests group from accessing application log Retention method for security log Retention method for security log Properties Netwrite events by days Overwrite events as needed Do not overwrite events (clear log manually) Modifying this setting may affect compatibility with and applications. For more information, see Retention method for security log region (a) 23659)	Policy Setting Not Defined 204800 kilobytes Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined r Clients, services, ecurity log.	
< >	ОК Са	ncel Apply	



(8) Open "Windows PowerShell" on your Windows server.



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

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

Administrator: Windows PowerShell

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

S C:\> _

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 Administrator: Windows PowerShell PS C:\> Get-GPResultantSetofPolicy -Computer WIN2016-ENG -Path C:\tmp\WIN2016-ENG.html -ReportType html RsopMode Logging Server: NNANESpace VWIN2016-ENG\Root\Rsop\NS293FC3EE_B754_4264_BB48_7027C395CCC3 LoggingComputer NNARTNER\administrator LoggingMode Computer S C:\> _

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.

Domain		npartn	er.local	
Site		Defau	t-First-Site-Name	
Organizational Unit		npartn	er.local/Servers	
Security Group Membership		show		
nent 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
5				
s				
lows Settings				
curity Settings				
Account Policies/Password Policy				
Policy		Setting	Winning GPO	
Enforce password history		24 passwords remembered	Default Domain P	blicy
Maximum password age		42 days	Default Domain Pe	blicy
Minimum password age		1 days	Default Domain P	plicy
Minimum password length		7 characters	Default Domain P	blicy
Password must meet complexity req	uirements	Enabled	Default Domain P	blicy
Store passwords using reversible en	cryption	Disabled	Default Domain P	blicy
Account Policies/Account Lockout Policy				
Policy		Setting	Winning GPO	
Account lockout threshold		0 invalid logon attempts	Default Domain Po	olicy
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	



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."

Local Group Policy Editor		— 🗆 🗙
File Action View Help		
 Local Computer Policy Computer Configuration Software Settings Windows Settings Name Resolution Policy Scripts (Startup/Shutdown) 	Policy See Q Audit account logon events Su Q Audit account management Su Q Audit directory service access No Q Audit logon events Su	curity Setting iccess, Failure o auditing iccess, Failure
 Deployed Printers Security Settings Account Policies Local Policies Audit Policy 	Audit object access Su Audit policy change No Audit privilege use No Audit process tracking No Audit system events Su	ccess, Failure o auditing o auditing o auditing uccess, Failure
 Guser Rights Assignment Security Options Windows Firewall with Advantion Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies Advanced Audit Policy Config Policy-based QoS Administrative Templates Software Settings Windows Settings Administrative Templates 	Audit logon events Properties Local Security Setting Explain Image: Audit logon events Audit logon events Image: Audit these attempts: Image: Success Image: Failure Image: This setting might not be enforced if other override category level audit policy. For more information, see Audit logon events Image: This setting might not be enforced if other override category level audit policy. For more information, see Audit logon events	Policy is configured to nts. (Q921468)



(3) Open "Windows PowerShell."



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

PS C: \> gpupdate /force		
🛃 Administrator: Windows PowerShell	_2	×
PS C:\> <mark>gpupdate</mark> /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		<u>_</u> 2	X
PS C:\> auditpol /get /category:*			~
System audit policy Category/Subcategory	Setting		
System		1941 - 1944 -	
Security System Extension System Integrity	Success and	Failure	
IPsec Driver	Success and	Failure	
Other System Events	Success and	Failure	
Logon/Logoff	Success and	rallule	
Logon	Success and	Failure	
Account Lockout	Success and	Failure	
IPsec Main Mode	Success and	Failure	
IPsec Extended Mode	Success and	Failure	
Special Logon	Success and	Failure	
Network Policy Server	Success and	Failure	
User / Device Claims	Success and	Failure	
Object Access	Success and	rallure	
File System	Success and	Failure	
Kernel Object	Success and Success and	Failure	
SAM	Success and	Failure	
Certification Services Application Generated	Success and Success and	Failure	
Handle Manipulation	Success and	Failure	
File Share Filtering Platform Packet Dron	Success and Success and	Failure	
Filtering Platform Connection	Success and	Failure	
Other Object Access Events Detailed File Share	Success and	Failure	
Removable Storage	Success and	Failure	
Central Policy Staging Privilege Use	Success and	Failure	
Non Sensitive Privilege Use	No Auditing		
Other Privilege Use Events Sensitive Privilege Use	No Auditing		
Detailed Tracking	no naarorng		
Process Creation Process Termination	No Auditing		
DPAPI Activity	No Auditing		
RPC Events Plug and Play Events	No Auditing		
Token Right Adjusted Events	No Auditing		
Policy Change	Success		
Authentication Policy Change	Success		
Authorization Policy Change	No Auditing		
Filtering Platform Policy Change	No Auditing		
Other Policy Change Events	No Auditing		
Computer Account Management	Success and	Failure	
Security Group Management	Success and	Failure	
Application Group Management	Success and	Failure	
Other Account Management Events	Success and	Failure	
DS Access	Success and	railuie	
Directory Service Access	Success		
Directory Service Changes Directory Service Replication	No Auditing		
Detailed Directory Service Replication	No Auditing		
Kerberos Service Ticket Operations	Success and	Failure	
Other Account Logon Events	Success and	Failure	
Credential Validation	Success and 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.

=	Best match
ŵ	Event Viewer Desktop app
	Settings >
	着 View event logs
ŝ	
	Event Viewer
Ŧ	P III

(2) Edit Security Log

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

Event Viewer				—		×
File Action View	Help					
🗢 🧼 🖄 📰 🛛	ÞĒ					
Event Viewer (Local)	Security Number	of events: 998 (!)	New events a	vailable		
> Custom Views	Keywor Date an	d Time	Source	Event ID	Task Catego	on ^
Application	Q Audi 4/16/20	24 AM 09:51:32	Micros	5156	Filtering Pla	tf
Security	🛛 🔍 Audi 4/16/20	24 AM 09:51:32	Micros	5158	Filtering Pla	tf
Setup	Open Saved Log	v1 09:51:32	Micros	5158	Filtering Pla	tf
🛃 System	Create Custom View	A 09:50:52	Micros	4656	File System	
Forward	Import Custom View	A 09:50:52	Micros	4658	Registry	
> 💾 Application:	import custom view	vi 09:50:52	Micros	4656	Registry	
📑 Subscriptior	Clear Log	v1 09:50:52	Micros	4658	Registry	
	Filter Current Log	v1 09:50:52	Micros	4690	Handle Mar	nij
	Properties	1 09:50:52	Micros	4658	Registry	
	Find	/1 09:50:52	Micros	4656	Registry	
	Save All Events As	v1 09:50:52	Micros	4658	Registry	~
		-			3	>
	Attach a Task To this Log	indows secur	ity auditing.			×
	View	>				
	Refresh					^
	Help	> ig Platform h	as permitted	a connectio	on.	
	Application Info	ormation:			>	~
<	>					
isplays Log 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 Prop	erties - Sec	urity (Type:	Administrative)
Logitop	crucs see	unity (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
When maximum Overwrite O Archive th	event log size is reached: events as needed (oldest events first) e log when full, do not overwrite events
	Clear Log
	OK Cancel Apply



X

7. For Windows 2019

Windows Audit Policy Settings

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

⅔ 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."



Copyright © All rights are reserved by N-Partner Technologies Co

(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."

w Obje	ct - Organiza	itional Unit			
Nº	Create in:	npartner.loo	cal/		
Jame:					
Servers					
					_
Prote	ct container f	rom accidenta	al deletion		
Prote	et container f	rom accidenta	al deletion		
Prote	et container fi	rom accidenta	al deletion		
✓ Prote	ct container fi	rom accidenta	al deletion		
Prote	ct container fi	rom accidenta	al deletion		
Prote	ct container fi	rom accidenta	al deletion		



(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."

📃 Active Directory Users and Computers File Action View Help Þ 🛶 🛛 🚈 📊 🦧 🖹 🛛 🔀 ன 🖉 📷 🗌		×
Active Directory Users and Com Name Ty Saved Queries		
Builtin Computers Domain Controllers	Add to a group Disable Account Reset Account	
Service Accourty Managed Service Accourty Managed Service Accourty	Move Manage	
Servers	All Tasks > Cut	
	Properties	
	Help	
>		

Moves the current selection to another organizational unit.

(5) Select Your Organizational Unit

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

⊡ ∰ np ⊕ <mark>6</mark>	artner Builtin		
÷	Computers		
÷	Domain Contr	rollers	
	Foreign Secur	ityPrincipals	
1	Servers	VICE ACCOUNTS	
+	Users		



(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.

Active Directory Users and Comp	outers			<u>000</u> 5	×
File Action View Help					
🗢 🏟 🚈 📊 📋 🖌 🗔	8 🖬 💈	🐮 👕 🍸 🖻	(B)		
Active Directory Users and Com Saved Queries Enpartner.local Builtin Computers Domain Controllers Computers Managed Service Accour Servers	Name	Type Computer	Description		
۲ ک					



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...".

Group Policy Management	dow Help				- 0	× æ×
🥌 🔿 🖄 💼 🖬 🖄						
Group Policy Management • A Forest: npartner.local • A Domains	Scrvers Linked Group Policy Objects	Group Policy Inheritance	Delegation		The contraction of the	
 impartner.local imp	Ink Order Link Order Create a GPO in this domain, an Link an Existing GPO Block Inheritance Group Policy Update Group Policy Modeling Wizard New Organizational Unit	GPO nd Link it here	Enforced	Link Enabled	GPO Status	X
V N D	View New Window from Here Delete Rename	>				
4	Refresh Properties		-			>
Create a GPO in this doma	Help					



(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."

New GPO	×
Name:	
N-Partner Policy	
Source Starter GPO:	
(none)	~
	OK Cancel

(4) Edit Your Group Policy Object

"Edit."

Select and right-click your group policy object name (the example here is "N-Partner Policy") and click

🚡 File Action View Window He Þ 🔿 🙋 📆 🔀 🗔 🔽 🛒	lp				- 8
Group Policy Management Construction Group Policy Management Construction Forest: npartner.local Default Domain Policy Default Domain Policy Servers Construction Group Policy Object Starter GPOs Sites Group Policy Modeling Group Policy Results	N-Partner Policy Scope Details Settings Delegation Links Display links in this location: npartner The following sites, domains, and OUs are linke Location		ner.local ked to this GPO: Enforced Link Enabled		
	Edit Enforced Link Enabled		No	Yes	npartner.loca
	Save Report View > New Window from Here	ply to the following groups, users, and computers:			
	Delete Rename Refresh	iove	Properties		
	Help				
	This GPO is linked to the following to	VV MII Tilter:		Open	


(5) Local Group Policies: Audit Policy

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





(6) Event Logs: Maximum Size of Security Log

Expand folder "Computer Configuration" -> "Windows Settings" -> "Security Settings" -> "Event Log" ->

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

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





(7) Event Logs: Retention Method for Security Log

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





(8) Open "Windows PowerShell" on your Windows server.



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

PS C:\> Invoke-GPUpdate -Computer WIN2019-ENG -RandomDelayInMinutes (O -Force	
Z Administrator: Windows PowerShell	W <u></u>	×
PS C:\> Invoke-GPUpdate -Computer WIN2019-ENG -RandomDelayInMinutes PS C:\> _	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-GP	ResultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\WIN2019-EN	IG.html -Re	portTyp	e html
Z Administrator:	Windows PowerShell	(<u>198</u> 7),		×
PS C: \> Get-GPR	esultantSetofPolicy -Computer WIN2019-ENG -Path C:\tmp\WIN2019-ENG.html	-ReportType	html	^
RsopMode Namespace LoggingComputer LoggingUser LoggingMode	: Logging : \\WIN2019-ENG\Root\Rsop\NS078FF8A1_B7F8_4F26_BD37_83CFD10A9A31 : WIN2019-ENG : NPARINER\administrator : Computer			
PS C:\> _				~

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.

C:\tmp\WIN2019-ENG.html	- C	Search ・ ク・ 分 だ
INER\WIN2019-ENG ×		
ecurity 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
Naturalization Allow sees may a 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.

		Filters \checkmark
ŵ	Best match	
	Edit group policy Control panel	
ŝ		
~~~		



#### (2) Local Group Policies: Audit Policies

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



#### (3) Open "Windows PowerShell."



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





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

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

Z Administrator: Windows PowerShell	(223)		×
PS C:\> auditpol /get /category:*			^
Category/Subcategory	Setting		
System Security System Extension	Success and	Failure	
System Integrity	Success and	Failure	
IPsec Driver Other System Events	Success and	Failure	
Security State Change	Success and	Failure	
Logon/Logoff	e	P-11	
Logon	Success and	Failure	
Account Lockout	Success and	Failure	
IPsec Main Mode	Success and	Failure	
IPsec Extended Mode	Success and	Failure	
Special Logon	Success and	Failure	
Other Logon/Logoff Events	Success and	Failure	ł.
User / Device Claims	Success and	Failure	
Group Membership	Success and	Failure	
Object Access File Swetzm	Suggara and	Failure	
Registry	Success and	Failure	
Kernel Óbject	Success and	Failure	
SAM Contification Servines	Success and	Failure	ł.
Application Generated	Success and	Failure	
Handle Manipulation	Success and	Failure	
File Share	Success and	Failure	ł.
Filtering Platform Connection	Success and	Failure	
Other Object Access Events	Success and	Failure	
Detailed File Share	Success and	Failure	ł.
Central Policy Staging	Success and	Failure	
Privilege Use			
Non Sensitive Privilege Use	No Auditing		
Sensitive Privilege Use	No Auditing		
Detailed Tracking			
Process Creation	No Auditing		
DPAPI Activity	No Auditing		
RPC Events	No Auditing		
Plug and Play Events Token Right Adjusted Events	No Auditing		
Policy Change	No Auditing		
Audit Policy Change	Success		
Authentication Policy Change	Success No Auditing		
MPSSVC Rule-Level Policy Change	No Auditing		
Filtering Platform Policy Change	No Auditing		
Other Policy Change Events	No Auditing		
Computer Account Management	Success and	Failure	
Security Group Management	Success and	Failure	
Application Group Management	Success and	Failure	
Other Account Management Events	Success and	Failure	
User Account Management	Success and	Failure	
Directory Service Access	Success		
Directory Service Changes	No Auditing		
Directory Service Replication	No Auditing		
Account Logon	NO AUditing		
Kerberos Service Ticket Operations	Success and	Failure	
Other Account Logon Events	Success and	Failure	
Credential Validation	Success and	Failure	
PS C:\> _	Success and	Tarraro	~



#### 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."

Event Viewer (Loca	l) Security Num	ber of events: 1,210 (!) New ev	ents available		
Windows Logs	Keywords	Date and Time	Source	Event ID	Task Category
Application	🔍 Audit Succ	2024/4/16 AM 10:11:22	Microsoft Wi	5156	Filtering Platf
Security	📕 🔍 Audit Succ	2024/4/16 AM 10:11:22	Microsoft Wi	5158	Filtering Platf
Setup	Open Saved Log	1/16 AM 10:11:22	Microsoft Wi	5158	Filtering Platf
📔 System	Create Custom View	I/16 AM 10:11:08	Microsoft Wi	5156	Filtering Platf
Forward	Import Custom View	I/16 AM 10:11:07	Microsoft Wi	5156	Filtering Platf
Application	import custom news	1/16 AM 10:11:07	Microsoft Wi	5158	Filtering Platf
Caracteristics Subscription	Clear Log	I/16 AM 10:11:07	Microsoft Wi	5158	Filtering Platf
	Filter Current Log	1/16 AM 10:11:07	Microsoft Wi	4656	File System
	Properties	1/16 AM 10:11:07	Microsoft Wi	4658	Registry
-	Find	1/16 AM 10:11:07	Microsoft Wi	4656	Registry
	Save All Events As	I/16 AM 10:11:07	Microsoft Wi	4658	Registry
	Save All Events As	UNC ALA 10 11 07	N.C. 70 M.C.	4000	
	Attach a Task To this Log	indows security auditi	ng.		
	View	>			
	Refresh				
	Hale	ng Platform has permi	tted a connection.		^
	Ticip	· · ·			

#### (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."

eneral	
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
When maximum Overwrite Archive th	event log size is reached: events as needed (oldest events first) ne log when full, do not overwrite events
() Do not ov	erwrite events ( Clear logs manually )



# 8. For Windows 2022

Windows Audit Policy Settings

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

⅔ 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."

lew Obje	ct - Organizational Unit	×
1	Create in: npartner.local/	
Name: Servers	3	_
Prote	ect 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 "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."

love objec	partner
	Builtin Computers Domain Controllers Foreign SecurityPrincipals Managed Service Accounts Servers Users
	OK Cance

(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."

New GPO	
Name:	
N-Partner Policy	
Source Starter GPO:	
(none)	
	OK Cancel

#### (4) Edit Your Group Policy Object

Select and right-click your group policy object name (the example here is "N-Partner Policy") and click

📓 Group Policy Management 📓 File Action View Window Hel	p				
🔶 🧼 🖄 📰 💥 🙆 🛛 🖬					
Group Policy Management ✓ A Forest: npartner.local ✓ B Domains ✓ A npartner.local ∬ Default Domain Policy → B Domain Controllers	N-Partner Policy Scope Details Settings Delegat Links Display links in this location: The following sites, domains, and OU	ion npartner.k	ocal to this GPO:		~
<ul> <li>Servers</li> <li>N-Partner Policy</li> <li>Group Policy Object</li> <li>WMI Filters</li> <li>Starter GPOs</li> <li>Sites</li> <li>Group Policy Modeling</li> <li>Group Policy Results</li> </ul>	Edit Enforced		Enforced No	Link Enabled Yes	Path npartner.local
	Save Report View > New Window from Here	y to the follo	owing groups, us	ers, and computers:	
	Delete Rename Refresh	ve	Properties		
	Help This GPO is linked to the following V	VMI filter:		0	



(5) Local Group Policies: Audit Policy

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





(6) Event Logs: Maximum Size of Security Log

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

#### 204800 KB

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



(7) Event Logs: Retention Method for Security Log

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





(8) Open "Windows PowerShell" on your Windows server.



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

PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force		
Administrator: Windows PowerShell	(5778)	×
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force PS C:\> _		^
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.

🛃 Administrator:	Windows PowerShell			$\times$
PS C:\> Get-GPR	esultantSetofPolicy -Computer WIN2022-ENG -Path C:\tmp\WIN2022-ENG.html -Report	Type htm	1	^
RsopMode Namespace LoggingComputer LoggingUser LoggingMode	: Logging : \\WIN2022-ENG\Root\Rsop\NSE7835E87_F6F9_4870_ADA9_618106FB1B0C : WIN2022-ENG : NPARTNER\administrator : Computer			
PS C:\> _				

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.

	× +						-		×
← C ③ File   C:/tmp/WIN20	22-ENG.html	Aø	습	CD	לַ≡	Ē	<b>%</b>		Ø
	Group Policy Results								
NPARTNER\WIN2022-ENG								hide	
Data collected on: 4/16/2024 PM 02:20:06 During last computer policy refres	h on 4/16/2024 PM 02:18:29		show al	1				110	
No Errors Detected A fast link was detected	More information								
No data available.									
Computer Details								hid	
General								hide	
Computer name Domain		NPARTNER/WIN2022-ENG	3						
Site		Default-First-Site-Name							
Organizational Unit		npartner.local/Servers							
Security Group Membership		show							
Component Status								shov	y.
Settings								hide	-
Policies								hid	
Windows Settings								hid	
Security Settings								1	
Administrative Templates								snov	<u>×</u>
Group Policy Objects								shov	<u>v</u>
Applied GPOs								hide	1
Default Domain Policy [{31B2F340-016D-11D2-9	45F-00C04FB984F9}]							hide	2
Local Group Policy [LocalGPO]								shov	<u>r</u>
N-Partner Policy [{044DAB72-77DD-4B98-AACt	5-4BFC6C313C62}]							shov	<u>-</u>
Denied GPOs								snov	2
WMI Filters								hid	
Neme	Value		Reference	- CPO/-	N.			Hu	



# 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."

	Best match
	Edit group policy Control panel
H	🔎 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" on your Windows server.



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





# (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 .	a	P 11	
Security System Extension System Integrity	Success and	Failure	
IPsec Driver	Success and	Failure	
Other System Events	Success and	Failure	
Security State Change	Success and	Failure	
Logon/Logoff	d	P 1	
Logon	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 Other Leven/Levenff Eucente	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	
Kegistry Vernel 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 Filtering Platform Packet Dyon	Success and	Failure	
Filtering Flatform 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	
Mon Sensitive Privilere Nee	No Auditing		
Ather Privilege Use Events	No Auditing		
Sensitive Privilege Use	No Auditing		
Detailed Tracking	an assau		
Process Creation	No Auditing		
Process Termination	No Auditing		
PPC Events	No Auditing		
Plug and Play Events	No Auditing		
Token Right Ádjusted Events	No Auditing		
Policy Change	1		
Audit Folicy Change	Success		
Authentication Folicy Change	No Auditing		
MPSSVC Rule-Level Policy Change	No Auditing		
Filtering Platform Policy Change	No Auditing		
Other Policy Change Events	No Auditing		
Account Management	d	F 1	
Computer Account 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	
Do Access Directory Service Access	Success		
Directory Service Changes	No Auditing		
Directory Service Replication	No Auditing		
Detailed Directory Service Replication	No Auditing		
Account Logon	S	F- : 1	
Actions Service licket Uperations	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."

Ē	D	Ö								
Best n	natch									
0	Event \ App	/iewe	r							
		_								
, Р E	vent Vie	wer			Ц	0	-	Ø		



#### (2) Edit Security Log

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

Event Viewer (Loca	B Security Numb	er of events: 1 196 /l) New ev	entr available		_	
Custom Views	security Number	er of events: 1,100 (:) New ev				
📔 Windows Logs	Keywords	Date and Time	Source	Event ID	Task Category	
Application	Audit Failure	2024/4/16 AM 10:29:20	Microsoft Wi	5152	Filtering Platf	
Security	📕 🔍 Audit Succ	2024/4/16 AM 10:29:20	Microsoft Wi	5156	Filtering Platf	
Setup	Open Saved Log	4/16 AM 10:29:20	Microsoft Wi	5158	Filtering Platf	
🛃 System	Create Custom View	4/16 AM 10:29:19	Microsoft Wi	5156	Filtering Platf	
Forward	Import Custom View	4/16 AM 10:29:19	Microsoft Wi	5158	Filtering Platf	
Application	import custom richini	4/16 AM 10:29:19	Microsoft Wi	5156	Filtering Platf	
📑 Subscription	Clear Log	4/16 AM 10:29:19	Microsoft Wi	5158	Filtering Platf	
	Filter Current Log	4/16 AM 10:29:16	Microsoft Wi	5156	Filtering Platf	
	Properties	4/16 AM 10:29:16	Microsoft Wi	5158	Filtering Platf	
	Find	4/16 AM 10:29:16	Microsoft Wi	5156	Filtering Platf	
	Sava All Events As	4/16 AM 10:29:16	Microsoft Wi	5158	Filtering Platf	
	Save All Events As	LICALLIN 20.10	Nr our	. CAFC	E16 1 01 07	-
	Attach a lask lo this Log	/indows security auditi	ng.			
	View	>				
	Refresh					Ī
	Heln	ng Platform has blocke	d a packet.		^	
	Ticip					



# (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						
Maximum log s When maximur	ize ( KB ): 204800 ਦ n event log size is reached: e events as needed (oldest events first)						
O Archive	the log when full, do not overwrite events						
O Do not o	verwrite events ( Clear logs manually ) Clear Log						
	OK Cancel Apply						



X

# 9. N-Reporter

(1) Add a Windows Server Device:

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





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

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





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

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 1	
Please select	~
Web Monitor (1)	47 f.
Activate Page Monitoring	
Previous	Cancel



Add Device - SNMP Setting			×
SNMP Setting			^
SNMP IP			
Version			
V2C			~
Read Community			
public			
Write Community			10
SNMP Timeout(sec)			
5			13
Encoding			
UTF-8			~
Device (Interface and Partition) Searched Timeout (Se	ec)		
120	29		
SNMP V3			~
	Previous	Next	Cancel



Add Device - Syslog Setting			
Syslog Setting			^
Facility 0			
			~
Encoding			
UTF-8			~
Syslog Normalized Data Retention Days (Max) (1)			
Raw Data Kept and Replied			
Raw Data Kept			
Raw data format is adopted while Syslog relaying	is activated in 1	Threshold I	Report.
The source IP will be kept in normalized data relay	/ing		
	Previous	Next	Cancel



Add Device - Monitor & Alert			×
Alert Template			^
ICMP Alert Template			
Please select			~
Device Alert Template			
Please select			~
Process Alert Template			
Please select			~
User Defined OID Template			
NTP Template			
Please select			~
Monitor and Connection Test			~
Alert Notification Setting			~
Alert Detail Configuration			~
	Previous	Next	Cancel



Add Device - Other	×
Other	^
Device Icon	
Host	~
Latitude and Longitude	
atitude, longitude	
Receive Status	
Activated      Disabled	
Device Sharing ()	
Device Sharing	
Pre	vious Next Cancel



# **10. Troubleshooting**

# 10.1 Invoke-GPUpdate Error

(1) On AD Domain server -> Run "Invoke-GPUpdate" to update Windows Server Group Policies, but an

#### error message appears.



(2) Open "Windows PowerShell" on Windows Server.



(3) Enter the command below to check the Windows Firewall rules for "WMI-WINMGMT-In-TCP, vm-

#### monitoring-rpc, and MSDTC-RPCSS-In-TCP."


(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", "MS Enabled True	SDTC-RPCSS	S-In-TC	P" -
💹 Administrator: Windows PowerShell			×
PS C:\> Set-NetFirewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitoring-rpc", "MSDTC-RPCSS-In-TCP" PS C:\> _	-Enabled True		<b>^</b>

## (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-Net Select-Object Na	FirewallRule -Name "WMI-WINMGMT-In-T ame, DisplayName, Enabled, Direction, Act	⁻ CP", "v tion   Fo	m-monito ormat-Tab	ring-rpc", "M le	ISDTC-RPC	SS-Ir	n-TCF	D"
Administrator:	Windows PowerShell				77			×
PS C:\> Get-NetFir Name, Enabled, Dir	ewallRule -Name "WMI-WINMGMT-In-TCP", "vm-monitc ection, Action   Format-Table	ring-rpc	", "MSDTC-J	PCSS-In-TCP"	Select-Objec	t Name	e, Disj	play 🔨
Name	DisplayName	Enabled	Direction	Action				
WMI-WINMGMT-In-TCP vm-monitoring-rpc MSDTC-RPCSS-In-TCP	Windows Management Instrumentation (WMI-In) Virtual Machine Monitoring (RPC) Distributed Transaction Coordinator (RPC-EPMAP)	True True True	Inbound Inbound Inbound	Allow Allow Allow				

#### PS C:\> _

(6) On the AD Domain server -> Enter the command below to update Windows Server Group Policies. PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force

Administrator: Windows PowerShell	(5772)	×
PS C:\> Invoke-GPUpdate -Computer WIN2022-ENG -RandomDelayInMinutes 0 -Force PS C:\> _		1
		<b>v</b>

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."

🛃 NXLog-CE Setup	
<b>Destination Folder</b> Click Next to install to the default folder or click Change to choose another.	
Install NXLog-CE to:	X
C:\Progr Installation directory must be on a local hard drive.	
ОК]	
<u>B</u> ack <u>N</u> ext	Cancel

(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"







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