

N- Partner N-REPORTER

How to manage and set up Windows Server Log with NXLOG V 1.1.3



(01-01-03-017) 2015/06/23



Preface

This document introduces how can N-Reporter users use Open Source NXLOG to manage and set up Windows Server 2003/2008/2012 Eventlog. Convert Event to syslog, then send it to N-Reporter for normalization, audit and analysis. The environment of this document is Windows Server 2003, Windows Server 2008 and Windows Server 2012.

N-Reporter provides two kinds of configuration file for converting Event into syslog, Eventlog to Syslog Utility and NXLOG. NXLOG has better performance when processing great amount of events. When the Windows Server Eventlog recording rate is over 700 pcs/sec, please use the NXLOG config document.

Contents

1	Set up NxLog on Windows Server			
	1.1	Set up Windows Server 2003	2	
	1.2	Set up Windows Server 2008	5	
	1.3	Set up Windows Server 2012	8	
2	Wind	dows 2003 Server Audit log Settings	12	
	2.1	Setting up local machine audit policy	12	
	2.2	Setting up local shared folder authorization and audit policy	.16	
3	Wind	dows 2008 Server Audit log Settings	25	
	3.1	Setting up local login audit policy	25	
	3.2	Setting up local shared folder authorization and audit policy	.30	
4	Wind	dows 2012 Server Audit log Setting	43	
	4.1	Setting up local login audit policy	.43	
	4.2	Setting up local shared folder authorization and audit policy	.46	

1 Set up NxLog on Windows Server 1.1 Set up Windows Server 2003

1. Download NXLOG :

Go to URL: http://nxlog.org/products/nxlog-community-edition/download

Download the latest version: nxlog-ce-x.x.xxxx.msi. Here we use: nxlog-ce-2.9.1347.msi.

2. Install NXLOG :

Double click: nxlog-ce-2.9.1347.msi, then click [Install], start installing.

3. Download Windows 2003 NXLOG config file: nxlog_win2k3.conf :

Go to URL: http://www.npartnertech.com/download/tech/nxlog_win2k3.conf

Edit NXLOG config file " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

Note :

Install NXLOG on 32 bit operating system at " C:\Program Files\nxlog\conf\nxlog.conf " Install NXLOG on 64 bit operating system at " C:\Program Files

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

Paste nxlog_win2k3.conf over nxlog.conf. This setting only output eventlogs, such as console audit, object access and account management. It filters out most of noise messages to reduce the loading that NXLOG produced on Windows Server. When the Windows Server Eventlog recording rate is over 700 pcs/sec, please use nxlog_win2k3.conf setting.

4. Download Windows 2003 NXLOG to output all of the eventlog config file nxlog_win2k3_all.conf :

Go to URL : http://www.npartnertech.com/download/tech/nxlog_win2k3_all.conf

N-Reporter provides legislation reports to calculate all the Windows Server eventlog. If the user needs Windows Server legislation reports, please paste nxlog_win2k3_all.conf over nxlog.conf. This setting enables all the eventlog output. It requires better hardware performance of Windows Server to run NXLOG.

🐼 NHReporter

This is a sample configuration file. See the nxlog reference manual about the

```
## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
## Please set the ROOT to the folder your nxlog was installed into,
## otherwise it will not start.
#define ROOT C:\Program Files\nxlog
define ROOT C:\Program Files (x86)\nxlog
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log
<Extension syslog>
  Module
             xm_syslog
</Extension>
<Input in_eventlog>
# For windows 2003 and earlier use the following:
  Module
               im_mseventlog
  Exec parse_syslog_bsd(); \
        if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID
== 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID
== 628 or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID
== 635 or $EventID == 636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID
== 646 or $EventID == 647) { $SyslogFacilityValue = 13; } \
            else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
            else if ($SourceName =~ /^MSSQL*/) { $SyslogFacilityValue = 18; } \
        else\
        {\
          drop();\
        }
</Input>
<Output out_eventlog>
  Module
               om_udp
  Host
      Port
                  514
      Exec $Message = string($EventID) + ": " + $Message;
      Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
       else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
         else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
  Exec to_syslog_bsd();
</Output>
<Route eventlog>
  Path
               in_eventlog => out_eventlog
</Route>
```

Please choose the correct install path of NXLOG about the green words.

The environment of this example is a 64 bit system. Please choose " define ROOT C:\Program Files

(x86)\nxlog " •

Please enter N-Reporter IP about the red words, here we enter " 192.168.2.64 " .

Setting as follows :



5. Start NXLOG :

Step a : Start NXLOG by using [Command Prompt] or Step b : Start NXLOG on [Services] •

a. Click [Start] → [All programs] → [Accessories] → Right click [Command Prompt] →
 Click [Run as administrator], run as system administrator.

Enter command prompt :

net stop nxlog	
net start nxlog	
Click [Start] > [All programs] > [Administrative Teels] > [Services] right click [

b. Click [Start] → [All programs] → [Administrative Tools] → [Services], right click [nxlog] →
 Click [Start] or [Restart] ∘

6. Check whether does NXLOG runs normally :

Check the log file of NXLOG "C:\Program Files (x86)\nxlog\data\nxlog.log". If it does not show Error, means it is operating normally.

🔐 C:\Program Files\nxlog\data\nxlog.log - Notepad++ _ 🗆 🗡 File Edit Search View Encoding Language Settings Macro Run Plugins Window ? 🔚 nxlog.conf 😑 nxlog.log 2016-04-21 14:53:55 WARNING stopping nxlog service 2 2016-04-21 14:53:55 WARNING nxlog-ce received a termination request signal, exiting... 3 2016-04-21 14:53:56 INFO nxlog-ce-2.7.1191 started 4 Normal text file length : 192 lines : 4 Ln:4 Col:1 Sel:0 Dos\Windows ANSI INS |

7. While adding Windows Server 2003 device on the N-Reporter :

For Windows Server 2003 Traditional Chinese version, please choose [BIG5] code.

For Windows Server 2003 Simplified Chinese version, please choose [GB2312] code.

For Windows Server 2003 English version, please choose [UTF8] code.

Note: Since NXLOG is not able to convert event code into UTF8 code (Eventlog to Syslog Utility), please pay attention to the language system choice to avoid garbled.

 While adding Windows Server 2003 device on the N-Reporter, please choose " (13) log audit " for Facility.

1.2 Set up Windows Server 2008

1. Download NXLOG :

Go to URL http://nxlog.org/products/nxlog-community-edition/download

Download the latest version: nxlog-ce-x.x.xxxx.msi. Here we use: nxlog-ce-2.9.1347.msi °

2. Install NXLOG :

Double click: nxlog-ce-2.9.1347.msi, then click [Install], start installing.

3. Download Windows 2008 NXLOG config file nxlog_win2k8.conf :

Go to URL: http://www.npartnertech.com/download/tech/nxlog_win2k8.conf

Edit NXLOG configuration file " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

Install NXLOG on 32 bit operating system at " C:\Program Files\nxlog\conf\nxlog.conf "

Install NXLOG on 64 bit operating system at " C:\Program Files

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

Paste nxlog_win2k8.conf over nxlog.conf. This setting only output eventlogs, such as console audit, object access and account management. It filters out most of noise (miscellaneous) messages to reduce the loading that NXLOG produced on Windows Server. When the Windows Server Eventlog recording rate is over 700 pcs/sec, please use nxlog_win2k8.conf setting.

4. Download Windows 2008 NXLOG to output all of the eventlog config file nxlog_win2k8_all.conf :

Go to URL : http://www.npartnertech.com/download/tech/nxlog_win2k3_all.conf

N-Reporter provides legislation reports to calculate all the Windows Server eventlog. If the user needs Windows Server legislation reports, please paste nxlog_win2k8_all.conf over nxlog.conf. This setting enables all the eventlog output. It requires better performance of Windows Server to run NXLOG.

## This is a sample configuration file. See the nxlog reference manual about the ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html				
## Please set the ROOT to the folder your nxlog was installed into, ## otherwise it will not start.				
#define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog				
Moduledir %ROOT%\modules				
Pidfile %ROOT% (data\nxlog.pid				
SpoolDir %ROOT%\data				
LogFile %ROOT%\data\nxlog.log				
<extension syslog=""></extension>				
Module xm_syslog				
<pre><input in_eventiog=""/> # Ear windows 2008/wists/7/8/2012/2012/2 and latter use the following:</pre>				
Module im msvistalog				
ReadFromLast TRUE				
SavePos IRUE				
<0uery <0ueryList>1				
<pre></pre>				
<select path="Security">*[System[(EventID=4769)]]</select> \				
<select path="Security">*[System[(EventID=4771)]]</select> \				
<select path="Security">*[System[(EventID=4624)]]</select> \				
<select path="Security">*[System[(EventID=4625)]]</select> \				
<pre><select path="security">[System](EventID=4634)]/<select> \ <select path="security">[System](EventID=4634)]/<select> \ </select></select></select></select></pre>				
<select path="Security">*[System](EventID=4648)]]</select> \				
<pre><select path="Security">*[System[(EventID=4656)]]</select></pre>				
<select path="Security">*[System[(EventID=4719)]]</select> \				
<select path="Security">*[System[(EventID=4720)]]</select> \				
<select path="Security">*[System](EventID=4722)]]</select> \				
<select path="Security">*[System[(EventID=4723)]]</select> \				
<select path="Security">*[System[(EventID=4724)]]</select> \				
<select path="Security">"[System](EventID=4726)]]</select> \ <select path="Security">*[System](EventID=4726)]]</select> \				
<select path="Security">*[System](EventiD=4725)]]</select> \				
<select path="Security">*[System](EventID=4728)]]</select> \				
<select path="Security">*[System[(EventID=4729)]]</select> \				
<select path="Security">*[System[(EventID=4730)]]</select> \				
<select path="Security">*[System[(EventID=4731)]]</select> \				
<select path="Security">*[System[(EventID=4732)]]</select> \				
<select path="Security">[System](EventID=4734)]</select> \ <select path="Security">*[System](EventID=4734)]</select> \				
<select path="Security">*[System](EventID=4735)]]</select>				
<select path="Security">*[System[(EventID=4737)]]</select> \				
<select path="Security">*[System[(EventID=4738)]]</select> \				
<select path="Security">*[System](EventID=4739)]]</select> \				
<select path="Security">*[System[(EventID=4741)]]</select> \				
<select path="Security">*[System](EventID=4742)]]</select> \ <select path="Security">*[System](EventID=4742)]</select> \				
<pre><select path="System">*[System[(EventD=4743)]</select> \</pre>				
<select path="Application">*[System[(EventID=18454)]]</select> \				
<select path="Application">*[System[(EventID=18456)]]</select> \				
\				
<quitaut eventlog="" out=""></quitaut>				
Module om_udp				
Host 102 168 2 64				

Port 514



Please choose the correct install path of NXLOG about the green words .

The environment of this example is a 64 bit system. Please choose " define ROOT C:\Program Files

(x86)\nxlog " •

Please enter N-Reporter IP about the red words , here we enter " 192.168.2.64 " .

Setting as follows :

5. Start NXLOG :

😑 nxlog.	golgobu 📑 Inte						
38	<pre><select path="Security">*[System[(EventID=4723)]]</select> \</pre>						
39	<pre><select path="Security">*[System[(EventID=4724)]]</select> \</pre>						
40	<pre><select path="Security">*[System[(EventID=4725)]]</select> \</pre>						
41	<pre><select path="Security">*[System[(EventID=4726)]]</select> \</pre>						
42	<pre><select path="Security">*[System[(EventID=4727)]]</select> \</pre>						
43	<pre><select path="Security">*[System[(EventID=4728)]]</select> \</pre>						
44	<pre><select path="Security">*[System[(EventID=4729)]]</select> \</pre>						
45	<pre><select path="Security">*[System[(EventID=4730)]]</select> \</pre>						
46	<pre><select path="Security">*[System[(EventID=4731)]]</select> \</pre>						
47	<pre><select path="Security">*[System[(EventID=4732)]]</select> \</pre>						
48	<pre><select path="Security">*[System[(EventID=4733)]]</select> \</pre>						
49	<pre><select path="Security">*[System[(EventID=4734)]]</select> \</pre>						
50	<pre><select path="Security">*[System[(EventID=4735)]]</select> \</pre>						
51	<pre><select path="Security">*[System[(EventID=4737)]]</select> \</pre>						
52	<pre><select path="Security">*[System[(EventID=4738)]]</select> \</pre>						
53	<pre><select path="Security">*[System[(EventID=4739)]]</select> \</pre>						
54	<pre><select path="Security">*[System[(EventID=4741)]]</select> \</pre>						
55	<pre><select path="Security">*System[(EventID=4742)]]</select> \</pre>						
56	<pre><select path="Security">*[System[(EventID=4743)]]</select> \</pre>						
5/	<pre><select path="System">*[System[(EventID=/036)]]</select> \</pre>						
58	<pre><select path="Application">*System[[EventID=18454]]]</select> \</pre>						
59	<pre><select path="Application">*[System[(tventID=18456)]]</select> \</pre>						
60	<pre></pre>						
61	VT View (VueryList)						
62							
63							
64	acourput out_eventiogs						
60							
60	NOST 122.100.2.04						
69	rore 514						
60	Exec \$Message = string(\$SourceName) + ": " + string(\$Eventlu) + ": " + \$Message;						
70	<pre>Exec if (\$EventID == 18494 or \$EventID == 18496) { \$>ysiogFacilityvalue = 18; } \</pre>						
71	0 else { \$>ystograciiityvalue = 1; } Ever if (ferupting = - 'EPROP() on ferupting == 'AUDIT EATLURE') / (SurlarSavanitu/alug = 3; })						
72	$\frac{1}{2} = \frac{1}{2} \left[\frac{1}{2} \left(\frac{1}{2} \right) \left(\frac{1}{2} \right)$						
73	$\frac{1}{2} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} = \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \left\{ \frac{1}{2} \right\} = \frac{1}{2} \left\{ 1$						
74							
75	0/</td						
76							
77	77 ⊖ <route eventlog=""></route>						
,							

Step a : Start NXLOG by using [Command Prompt] or Step b : Start NXLOG on [Services].

a. Click [Start] → [All programs] → [Accessories] → Right click [Command Prompt] →
 Click [Run as administrator], run as system administrator °

Enter command prompt :

net stop nxlog net start nxlog

- b. Click [Start] → [All programs] → [Administrative Tools] → [Services], right click [nxlog] → Click [Start] or [Restart].
- 6. Check whether does NXLOG runs normally :

Check the log file of NXLOG "C:\Program Files (x86)\nxlog\data\nxlog.log". If it does not show Error, means it is operating normally $^\circ$

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++ [Administrator]	C					
File Edit Search View Encoding Language Settings Macro Run Plugins Window ? 🕞 🚔 🖫 🛸 🕞 🕞 🚔 🐇 🛍 🛍 ⊅ 🛋 🏘 🍢 🍳 👒 📴 🚍 🚍 🗊 ỹ 🎉 🖾 🖉 💷 🕨 💷 🕨 🔤 🤯	Х					
🔚 nxlog.conf 🔚 nxlog.log						
 2014-07-03 17:57:22 WARNING stopping nxlog service 2014-07-03 17:57:22 WARNING nxlog-ce received a termination request signal, exiting 2014-07-03 17:57:23 INFO nxlog-ce-2.7.1191 started 						

 While adding Windows Server 2008 device on the N-Reporter , please choose " (13) log audit " for Facility.

1.3 Set up Windows Server 2012

1. Download NXLOG :

Go to URL: http://nxlog.org/products/nxlog-community-edition/download

Download the latest version: nxlog-ce-x.x.xxxx.msi. Here we use: nxlog-ce-2.9.1347.msi.

2. Install NXLOG :

Double click nxlog-ce-2.9.1347.msi, then click [Install], start installing.

3. Download Windows 2012 NXLOG config file nxlog_win2012.conf :

Go to URL : http://www.npartnertech.com/download/tech/nxlog_win2012.conf

Edit NXLOG config file " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

Note :

Install NXLOG on 32 bit operating system at " C:\Program Files\nxlog\conf\nxlog.conf " Install NXLOG on 64 bit operating system at " C:\Program Files

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

Paste nxlog_win2012.conf over nxlog.conf. This setting only output eventlogs, such as local policy audit, object access and account management. It filters out most of noise messages to reduce the loading that NXLOG produced on Windows Server. When the Windows Server Eventlog recording rate is over 700 pcs/sec, please use nxlog_win2012.conf setting.

4. Download Windows 2012NXLOG to output all of the eventlog configuration file nxlog_win2k12_all.conf :

Go to URL : http://www.npartnertech.com/download/tech/nxlog_win2012_all.conf

N-Reporter provides legislation reports to calculate all the Windows Server eventlog. If the user needs Windows Server legislation reports, please paste nxlog_win2012_all.conf over nxlog.conf. This setting enables all the eventlog output. It requires better performance of Windows Server to run NXLOG.

🐼 NHReporter

This is a sample configuration file. See the nxlog reference manual about the ## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html

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

#define ROOT C:\Program Files\nxlog define ROOT C:\Program Files (x86)\nxlog

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

<Extension syslog> Module xm_syslog </Extension> <Input in_eventlog> # For windows 2008/vista/7/8/2012/2012r2 and latter use the following: Module im_msvistalog ReadFromLast TRUE SavePos TRUE Query <QueryList> \

<qu< th=""><th>uery Id="0"> \</th></qu<>	uery Id="0"> \
	<select path="Security">*[System[(EventID=4768)]]</select> \
	<select path="Security">*[System[(EventID=4769)]]</select> \
	<select path="Security">*[System[(EventID=4771)]]</select> \
	<select path="Security">*[System[(EventID=4624)]]</select> \
	<select path="Security">*[System[(EventID=4625)]]</select> \
	<select path="Security">*[System[(EventID=4634)]]</select> \
	<select path="Security">*[System[(EventID=4647)]]</select> \
	<select path="Security">*[System[(EventID=4648)]]</select> \
	<select path="Security">*[System[(EventID=4656)]]</select> \
	<select path="Security">*[System[(EventID=4719)]]</select> \
	<select path="Security">*[System[(EventID=4720)]]</select> \
	<select path="Security">*[System[(EventID=4722)]]</select> \
	<select path="Security">*[System[(EventID=4723)]]</select> \
	<select path="Security">*[System[(EventID=4724)]]</select> \
	<select path="Security">*[System[(EventID=4725)]]</select> \
	<select path="Security">*[System[(EventID=4726)]]</select> \
	<select path="Security">*[System[(EventID=4727)]]</select> \
	<select path="Security">*[System[(EventID=4728)]]</select> \
	<select path="Security">*[System[(EventID=4729)]]</select> \
	<select path="Security">*[System[(EventID=4730)]]</select> \
	<select path="Security">*[System[(EventID=4731)]]</select> \
	<select path="Security">*[System[(EventID=4732)]]</select> \
	<select path="Security">*[System[(EventID=4733)]]</select> \
	<select path="Security">*[System[(EventID=4734)]]</select> \
	<select path="Security">*[System[(EventID=4735)]]</select> \
	<select path="Security">*[System[(EventID=4737)]]</select> \
	<select path="Security">*[System[(EventID=4738)]]</select> \
	<select path="Security">*[System[(EventID=4739)]]</select> \
	<select path="Security">*[System[(EventID=4741)]]</select> \
	<select path="Security">*[System[(EventID=4742)]]</select> \
	<select path="Security">*[System[(EventID=4743)]]</select> \
	<select path="System">*[System[(EventID=7036)]]</select> \
	<select path="Application">*[System[(EventID=18454)]]</select>
	<select path="Application">*[System[(EventID=18456)]]</select>
<td>uery> \</td>	uery> \

<Route eventlog> Path in_eventlog => out_eventlog </Route> s ۱

Please choose the correct install path of NXLOG about the green words.

The environment of this example is a 64 bit system. Please choose " define ROOT C:\Program Files

(x86)\nxlog ".

Please enter N-Reporter IP about the red words, here we enter " 192.168.2.64 " .

Setting as follows :

😑 nxiog	g.conr 🔤	😑 nxiog.iog 🖬				
25	白		<pre><ouerv id="0"> \</ouerv></pre>			
26	Т		<pre><select_path="security">*[System[(EventTD=4768)]] \</select_path="security"></pre>			
27			<pre>cfalect Dath="Security" *[System[(CountID-1760)]]/(cleat))</pre>			
21			(sleet path scority / [system[(tventro-473)]](sleet)			
28			<pre><select path="Security">*[system[(eventD=4771)]]</select> \</pre>			
29			<pre><select path="Security">*[System[(EventID=4624)]]</select> \</pre>			
30			<pre><select path="Security">*[System[(EventID=4625)]]</select> \</pre>			
31			<pre><select path="Security">*[System[(EventID=4634)]]</select> \</pre>			
32			<pre><select path="Security">*[System[(EventID=4647)]]</select> \</pre>			
33			<pre><select path="Security">*[System[(EventID=4648)]]</select> \</pre>			
34			Select Path-"Security"'*[System[(EventTD-4656)]]/(Select))			
36			(clear bath "Security" (System (Control 470))]; Screet)			
35			collect Path= Security >[[system[(tventib=4719)]](select) (
36			<pre><select path="Security">*[System[(EventID=4720)]]</select> \</pre>			
37			<pre><select path="Security">*[System[(EventID=4722)]]</select> \</pre>			
38			<pre><select path="Security">*[System[(EventID=4723)]]</select> \</pre>			
39			<pre><select path="Security">*[System[(EventID=4724)]]</select> \</pre>			
40			<pre><select path="Security">*[System[(EventID=4725)]]</select> \</pre>			
41			<pre><select path="Security">*[System[(EventTD=4726)]]</select> \</pre>			
42			<pre>cSelect Path="Security"**[System[(EventTD=4727)]]</pre> (Select)			
45			Colort Dath-"Security" (System[(ContD-4729)]](Select)			
45			(Select Ath-Security / System (Control-720)])(Select)			
44			<pre><select %[system[(eventid="4/29)]]</pre" path="Security"></select></pre>			
45			<pre><select path="Security">*[System[(EventID=4730)]]</select> \</pre>			
46			<pre><select path="Security">*[System[(EventID=4731)]]</select> \</pre>			
47			<pre><select path="Security">*[System[(EventID=4732)]]</select> \</pre>			
48			<pre><select path="Security">*[System[(EventID=4733)]]</select> \</pre>			
49			<pre><select path="Security">*[System[(EventID=4734)]]</select>)</pre>			
50			<pre><select path="Security">*[System[(EventTD=4735)]]</select> \</pre>			
51			Select Dath-"Security" (System[(CountID-1737)]]/(Select)			
51			(clear bath Scould's (system(territe (37))); (clear)			
22			<pre>cselect Path= Security > [system[(eventib=4756)]](select) (</pre>			
53			<pre><select path="Security">*[System[(EventID=4739)]]</select> \</pre>			
54			<pre><select path="Security">*[System[(EventID=4741)]]</select> \</pre>			
55			<pre><select path="Security">*[System[(EventID=4742)]]</select> \</pre>			
56			<pre><select path="Security">*[System[(EventID=4743)]]</select> \</pre>			
57			<pre><select path="System">*[System[(EventID=7036)]]</select></pre> /Select> \			
58			<pre><select path="Annlication">*[System[(EventID=18454)]]</select> \</pre>			
50			<pre>cSelect Path="Application">*[System[(FuentID=18456)]]/(Select))</pre>			
60						
60			Signal Antonio Signal S			
61			<pre>/QueryList></pre>			
62	_⊢ <td>out></td> <td></td>	out>				
63						
64	- <out< td=""><td>out out_ev</td><td>entlog></td></out<>	out out_ev	entlog>			
65	Mod	dule	om udp			
66	Hos	st	192.168.2.64			
67	Por	Port 514				
68	Exe	Figure 1 Wassage = string(\$SourceName) + ", " + string(\$FuentTD) + ", " + \$Massage,				
69	Exe	er if (tew	$ \begin{array}{c} \text{entry} = 18454 \text{ or } \{\text{EventTD} = 18456 \} \\ \left\{ \frac{1}{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} \sqrt{2} $			
70	LXC		Social Statistical Statistics (Social Statist			
70	- E m	Else { \$29510graclityValue = 13; }				
/1	EXE	Exec if (\$EventType == 'ERROR' or \$EventType == 'AUDIT_FAILURE') { \$SyslogSeverityValue = 3; } \				
72	else if (\$EventType == 'WARNING') { \$SyslogSeverityValue = 4; } \					
73	<pre>else if (\$EventType == 'INFO' or \$EventType == 'AUDIT_SUCCESS') { \$SyslogSeverityValue = 5; }</pre>					
74	Exec to_syslog_bsd();					
75	-					
76						
77	Execute eventlog>					
78	Path in eventlog => out eventlog					
79						
80	<) (O					
2						
			111 2			

3. Start NXLOG :

Step a : Start NXLOG by using [Command Prompt] or Step b : Start NXLOG on [Services].

a. Click [Start] → [Windows PowerShell] → Click [Run as administrator], run as system administrator].

Under [Windows PowerShell] mode, input :

net stop nxlog			
net start nxlog			

- b. Click [Start] → [All programs] → [Administrative Tools] → [Services], right click [nxlog] → Click [Start] or [Restart].
- Check whether does NXLOG runs normally : Check the log file of NXLOG "C:\Program Files (x86)\nxlog\data\nxlog.log". If it does not show Error, means it is operating normally.

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++ [Administrator]	_ 0	x				
File Edit Search View Encoding Language Settings Macro Run Plugins Window ? 🕞 🗁 🔚 🖻 🕞 🕞 🚔 🐇 🛍 🖺 ગ 🛋 🕍 🌸 🔍 🤏 🕞 📴 🚍 🗐 플 🇊 🖉 🖾 🏂 💷 💽 💌 🕨 💌 🕨 🕬 👘 👘 👘 👘 👘 👘 👘 👘 🖉		X J	:			
1 2016-04-21 16:54:47 INFO nxlog-ce-2.9.1347 started 2						
Normal text file_length : 52_lines : 2Ln : 1_Col : 1_Sel : 0 0Dos\WindowsANSI		INS				

 While adding Windows Server 2012 device on the N-Reporter, please choose " (13) log audit " for Facility.

2 Windows 2003 Server Audit log Settings

This section introduces the local machine policy audit of Windows 2003 Server. The local machine

here means it is an independent host, which does not belong to any network domain °

Mainly discuss the following two settings :

- 1. Setting up local machine audit policy ·
- 2. Setting up local machine shared folder authorization and audit policy ·

Please remember to download NXLOG, which may refer to section 1.

2.1 Setting up local machine audit policy

Set as follows :

1. Log in Windows 2003 Server as Administrator •

Click [Start / All programs / Administrative Tools / Local Security Policy].



2. Click [Local Policies / Audit Policy]

🚡 Local Security Settings							
Eile Action Yiew Help							
Security Settings	Policy V	Secu	rity Setting				
🕀 🧧 Account Policies	Audit system events	No a	uditing				
E Gal Policies	Audit process tracking	No a	uditing				
Audit Policy	Audit privilege use	No a	uditing				
User Rights Assignment	Audit policy change	No a	uditing				
	Audit object access	No a	uditing				
Goftware Restriction Policies	Audit logon events	Noa	uditing				
🗄 👼 IP Security Policies on Local Computer	Audit directory service access	Noa	uditing				
	Audit account management	No a No a	ualting uditing				
		NU a	aalang				
	<u> </u>						

- 3. Define the following policy set value :
 - (1) Audit logon event :

Double click [Audit logon events], check [Success] and [Failure], then click [OK].



(2) Audit account logon event :

Double click [Audit logon events], check [Success] and [Failure], then click [OK] °



(3) Audit object access :

Double click [Audit object access], check [Success] and [Failure], then click [OK] °

Success: If you need the Log of success events, please check [Success].

Failure: If you need the Log of failed events, please check [Failure].



- (4) Changing audit policy : Double click [Audit policy change], check [Define these policy settings], check (choose) [Success] and [Failure], then click [OK].
- (5) Audit account management :
 Double click [Audit account management], click [Define these policy settings], check [Success] and [Failure], then click [OK] °

Note : If Windows 2003 Server does not run File server audit, we recommend not to audit object access, please skip steps 2.1(3) and 2.2, and only operate steps 2.1 (1), (2), (4), (5). This will help Windows avoid auditing unnecessary Object access security events. These unnecessary and redundant security events that are converted into syslog and sent to N-Reporter will reduce its performance.

2.2 Setting up local shared folder authorization and audit policy

Set up as follows :

- 1. Right click the folder you want to share, click [Properties].
- 2. Click [Sharing], check [Share this folder]. Click [Permissions] °

Share_Folder Proper	ties		? ×
General Sharing S	ecurity Web Sł	naring Customiz	e
You can si net vork. T foldet.	hare this folder wi Fo enable sharing	th other users on I for this folder, cli	your ck Share this
○ Do <u>n</u> ot share t ○ <u>S</u> hare this fold	his folder er		
S <u>h</u> are name: 🍗	hare_Folder		•
Comment:			
User limit: 💽	Maximum allow	4	
0	Allo <u>w</u> this numb	er of up rs:	•
To set permissions folder over the net	for users who ac work, click Permi	cess this Ee	rmissions
To configure settin Caching.	ngs for offline acc	ess, click(Caching
		Ng	ew Share
	ОК	Cancel	Apply

- 3. Set up user permission :
 - (1) Click [Add], to add a new user.
 - (2) Click [Locations], then choose the local computer name.
 - (3) Enter a user name account.
 - (4) Click [OK].

Permissions for Share_Folder	Select Users or Groups	<u>? ×</u>
Share Permissions Group or user names: pikachu (NPARTNER-C9DE26\pikachu) Add., Remove	Select this object type: Users, Groups, or Built-in security principals From this location: NPARTNER-C9DE26 Epter the object names to select (examples) everyone	Dbject Types
Permissions for pikachu Allow Deny Full Control 🖉 🔲 Change 🖉 🔲 Read 🗹	Advanced	Cancel
OK Cancel Apply		

- 4. Set up user account privilege :
 - (1) Choose a user account account.
 - (2) Check [Full Control] and [Change] permissions.
 - (3) Click [OK] °

Permissions for Share_Folder		? ×
Share Permissions		
Group or user names:		
🕵 Everyone		
😰 pikaohu (NPARTNER-C9DE:	26\pikachu)	
	Add	Bemove
	<u> </u>	
Permissions for Everyone	Allow	Deny
Permissions for Everyone Full Control	Allow	
Permissions for Everyone Full Control Change		
Permissions for Everyone Full Control Change Read	Allow	
Permissions for Everyone Full Control Change Read	Allow V V V	

- 5. Security settings :
 - (1) Click [Security].
 - (2) Click [Add], to add a new user.
 - (3) Click [Locations], then choose the local computer name.
 - (4) Enter a user account.
 - (5) Click [OK].



- 6. Set up user account privilege :
 - (1) Choose the user account.
 - (2) Check [Full Control] permissions.
 - (3) Click [Apply].

Share_Folder Properties		? ×
General Sharing Security Web	Sharing Custon	nize
<u>G</u> roup or user names:		
Administrators (NPARTNER-C CBEATOB OW/NEB	9DE26\Administ	rators) 🔺
Everyone		
🙎 pikachu (NPARTNER-C9DE2 🕵 SYSTEM	26\pikachu)	
<u> </u>	A <u>d</u> d	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Full Control Modify	NG	
Head & Execute		H
Read		E II
Write		
Coocial Permissions		
click Advanced.	iceu settings, 	Advanced
OK	Cancel	

- 7. Advanced security settings :
 - (1) Click [Advanced].
 - (2) Click [Auditing].
 - (3) Click [Add].
 - (4) Click [Locations], then choose the local computer name.
 - (5) Enter the user name account.
 - (6) Click [OK].



8. Audit entry settings :

Check [Successful] and [Failed] of all the entries, then click [OK].

Auditing Entry for Share_Folder		<u>?</u> ×
Ubject Name: Everyone Apply onto: This folder, subfolders a	nd files	<u>C</u> hange ▼
Access: Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions	Successful V V V V V V V V V V V V V	Failed
Apply these auditing entries to obj and/or containers within this cont	ects ainer on	Clear All
	OK	Cancel

9. After completing advanced security settings. click [OK] °

Ad	vanced Sec	curity Settings for Share	e_Folder	Advanced Security Settings for Share_Folder				
F	Permissions Auditing Owner Effective Permissions							
	To view mo	re information about special	auditing entries, selec	st an auditing entry, a	and then click Edit.			
	Auditing ont	riee:						
	Additing eng	nes.		4	1	_		
	Туре	Name	Access	Inherited From	Apply To			
	All	Everyone	Full Control	<not inherited=""></not>	This folder, subfold	i		
	All	pikachu (NPARTNE	Full Control	<not inherited=""></not>	This folder, subfold	i		
	I					_		
	Add.	<u>E</u> dit	<u>R</u> emove					
	— Allow in	heritable auditing entries from	o the parent to propar	- Tate to this object an	d all child objects. In	Jude		
	these w	ith entries explicitly defined h	iere.			51000		
	E Benlace	a auditing entries on all child	objects with entries s	hown here that apply	uto child objects			
	I nepiace	e additing critics of all crilia	objects with entries s	почитнете спасарру	to crilid objects			
		1						
	Learn more	about <u>auditing</u> .						
-								
			L	OK	Cancel <u>A</u> p	ply		

10. After completing shared folders settings, click [OK] $\ensuremath{^\circ}$

Share_Folder Properties		? ×
General Sharing Security We	b Sharing Custo	mize
<u>G</u> roup or user names:		
Administrators (NPARTNER	-C9DE26\Adminis	trators) 🔺
CREATOR OWNER		
Everyone		
🧕 📓 pikachu (NPARTNER-C9DI	E26\pikachu)	
SYSTEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for Everyone	Allow	Deny
Full Control		
Modify	\checkmark	
Read & Execute	\checkmark	
List Folder Contents	\checkmark	
Read		
Write		
Coocial Pormissions		
For special permissions or for adv click Advanced.	anced settings,	Advanced
ОК	Cancel	

11. Click [Start / All Programs / Administrative Tools / Computer Management].



12. Click [System Tools / Shared Folders / Shares] $^{\circ}$

📮 Computer Management				
🗐 File Action View Window H	lelp			_ 8 ×
	1 📖			
Computer Management (Local)	Share Name 🔺	Folder Path	Туре	# Client Connect
E System Tools	admin\$	C:\WINDOWS	Windows	0
	₽ C\$	C:/	Windows	0
Shared Folders	Regirec\$		Windows	0
Shares	💫 Share_Folder	C:\Share_Folder	Windows	0
Eucal Osers and Groups				
🕀 🎒 Removable Storage				
Disk Defragmenter				
📲 Disk Management				
🗄 🚱 Services and Applications				
_				
	•			►

13. Double click the [shared folder], then click [Share Permissions]. Choose the user name account, and check to allow [Full Control], [Change] and [Read] permissions, then click [OK].



3 Windows 2008 Server Audit log Settings

This section introduces the local audit policy of Windows 2008 Server. The local computer here means it is an independent host, which does not belong to any network domain. Here we mainly discuss the following two settings :

- 1. Setting up local login audit policy.
- 2. Setting up local shared folder authorization and audit policy.

Please remember to download NXLOG, which may refer to section 1.

3.1 Setting up local login audit policy

Set as follows :

1. Log in Windows 2008 Server as Administrator.

Click [Start / Administrative Tools / Local Security Policy].



2. Click [Local Policies / Audit Policy] ·



- 3. Define the following policy set value :
 - (1) Audit logon event :

Double click [Audit logon events], check [Success] and [Failure], then click [OK].



(2) Audit account logon event :

Double click [Audit logon events], check [Success] and [Failure], then click [OK].



(3) Audit object access :

Double click [Audit object access], check [Success] and [Failure], then click [OK] °

(4) Changing audit policy :



Double click [Audit policy change], check [Define these policy settings], check [Success] and [Failure], then click [OK].

(5) Audit account management :

Double click [Audit account management], check [Define these policy settings], check [Success] and [Failure], then click [OK].

Note : If Windows 2008 Server does not run File server audit, we recommend not to audit object access, please skip steps 3.1(3) and 3.2, and only operate steps 3.1 (1), (2), (4), (5). This will help Windows avoid auditing unnecessary Object access security events.

These unnecessary and redundant security events that are converted into syslog and

sent to N-Reporter will reduce its performance.

3.2 Setting up local shared folder authorization and audit policy

Set as follows :

- 1. Right click the folder you want to share, click [Properties].
- 2. Click [Sharing], then click [Share].

🔋 share_folder Properties	×			
General Sharing Security Previous Versions Customize				
Network Fie and Folder Sharing				
Shared				
Network Path: \\WIN-CL4KQH6VKIIU\share_folder				
Share				
Advanced Sharing				
Set custom permissions, create multiple shares, and set other advanced sharing options.				
G Advanced Sharing				
Password Protection				
People must have a user account and password for this computer to access shared folders.				
To change this setting, use the <u>Network and Sharing Center</u> .				
OK Cancel Apply				

3. In share permissions settings, open the menu and choose an existing user account, then click [Add].



Change its [Permission Level] to [Read/Write], then Click [Share].

👩 Fil	2 Sharing			×
\bigcirc	🔉 File Sharing			
	Choose people to share with Type a name and then click Add, or click the arrow to find someone			
		•	Add	
	Name	Permission L	evel	
	& Administrator	Read/Write	-	
	Administrators	Owner		
	Everyone	Read/Write	Read	
			✓ Read/Write	
			Remove	
	I'm having trouble sharing		1	
			Share Cancel	



4. When you complete setting, click [OK].

- 5. Security settings :
 - (1) Click [Security].
 - (2) Choose the user account.
 - (3) Click [Edit].
 - (4) Check to allow [Full Control] permission to have all the authorizations.
 - (5) Click [OK].

🔋 share_folder Properties 🗙	Permissions for share_folder	×
General Sharing Security Previous Versions Customize	Security	
Object name:	Object name: C:\share_folder	
Group or user names:	Group or user names:	
SYSTEM Administrator (WIN-Q4KQH6VKIIU\Administrator)	Administrato (WIN-Q4KQH6VKIIU\Administrator)	
& Administrators (WIN-Q4KQH6vKUU\Administrators)	Administrato s (WIN-Q4KQH6VKIIU\Administrators)	
To change permissions, click Edit.		
Permissions for Everyone Allow Deny	AddRemove	
Full control 🗸 🔺	Permissions for Everyone Allow Deny	1
Modify 🗸	Full control	
Read & execute 🗸		
List folder contents	Read & execute	
Head V	List folder contents	
Vvnte 🗸 💆	Read 🗹 🗖 🖵	
For special permissions or advanced settings, Advanced	Leam about access could and permissions	1
Leam about access control and permissions	OK Cancel Apply	
Close Cancel Apply		

- 6. Advanced security settings :
 - (1) Click [Security].
 - (2) Click [Advanced].
 - (3) Click [Auditing].
 - (4) Click [Edit].
 - (5) Click [Add].
 - (6) Click [Locations], then choose the local computer name.
 - (7) Enter the user name account.
 - (8) Click [OK].



7. Audit entry settings :

Check [Success] and [Failure] of all the entries, then click [OK].

Auditing Entry for share_folder		2
Name: Everyone		Change
Apply onto: This folder, subfolders	and files	•
Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions	Succession Succession	
Apply these auditing entries to ol and/or containers within this con only <u>Managing auditing</u>	bjects tainer	Clear All
	ОК	Cancel

8. After completing advanced security settings, click [OK].

Advanced S	ecurity Settings for share	e_folder			×
Auditing					
To view or ed	lit details for an auditing entry	, select the entry and the	n click Edit.		
Object pamer	Culaboro foldor				
Object name:	C: gnare_rolder				
Auditing entri	es:	[The start From	Annels To	
All	Everyone	Full control	<pre> Innerited From <not inherited=""></not></pre>	This folder, subfolder	1
				,,	
		- 1			
Add	Edit	Remove			
✓ Include in	heritable auditing entries from	n this object's parent			
Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object					
What are the	requirements for auditing ob	ject access?			
			ОК	Cancel Apply	

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

9. After completing shared folders settings, click [OK].

	Advanced Se	curity Settings for share	_folder			×	
ſ	Permissions Au	uditing Owner Effective Per	missions				
	To view details	of a permission entry, double-	click the entry. To modify	permissions, click Cha	nge Permissions.		
	Object name:	C:\share_folder					
	Auditing entries						
	Туре	Name	Access	Inherited From	Apply To	1	
	All	Everyone	Full control	<not inherited=""></not>	This folder, subfolders		
	, Edit						
	☑ Include inheritable auditing entries from this object's parent						
	What are the requirements for auditing object access?						
				ОК	Cancel Apply		

10. After completing shared folders settings, click [OK].

📕 share_folder Proper	rties	×
General Sharing Secu	urity Previous Versions	Customize
Object name: C:\sha	re_folder	
Group or user names:		
Administrator (WIN	I-Q4KQH6VKIIU\Administr	ator)
Administrators (WI	N-Q4KQH6VKIIU\Administ	rators)
To change permissions,	, click Edit.	Edit
	_	
Permissions for Everyon	ie Allow	Deny
Full control	~	
Mar differ		
woary	~	
Read & execute	~ ~	
Read & execute		
Read & execute List folder contents Read		
Read & execute List folder contents Read Write	* * * * *	-
Read & execute List folder contents Read Write	or advanced settings.	▼ Advanced
Read & execute List folder contents Read Write For special permissions click Advanced.	or advanced settings,	▼ Advanced
For special permissions click Advanced.	or advanced settings,	▼ Advanced
For special permissions click Advanced.	or advanced settings,	Advanced
For special permissions click Advanced.	or advanced settings,	Advanced

11. Click [Start / Administrative Tools / Computer Management].

Google Chrome		Remote Desktop Services Component Services Computer Management
 Command Prompt Internet Explorer Notepad Local Security Policy Windows Firewall with Advanced Security 	Administrator Documents Computer Network Control Panel Devices and trinters	 Data Sources (ODBC) Ivent Viewer ISCSI Initiator Local Security Policy Performance Monitor Security Configuration Wizard Server Manager Services Share and Storage Management Storage Explorer System Configuration Task Scheduler Windows Firewall with Advanced Security Windows PowerShell Modules Windows Server Backup
All Programs Search programs and files	Help and Support Run Log off	
Astart 🝶 ⊿ 🚞 🌍		

12. Click [System Tools / Shared Folders / Shares].



13. Right click [Shares], then click [New] / [Share].



- 14. New share wizard settings :
 - (1) Click [Next].

Create A Shared Folder W	izard	×
23	Welcome to the Create A Shared Folder Wizard This wizard helps you share a computer folder so that it can be accessed by people on other computers in your network or workgroup. Windows Firewall will be set up to allow this folder to be shared with other computers. Please read how this may impact Windows Firewall and the security of your computer. Learn more about Windows Firewall	
	Click Next to continue.	

(2) Click [Browse] to choose the sharing path, then click [Next].

ate A Shared Fol	der Wizard
Folder Path Specify the pa	th to the folder you want to share.
Computer name:	WIN-L7VF1213STQ
Type the path to the folder.	e folder you want to share, or click Browse to pick the folder or add a new
Folder path:	C:\Users\Administrator.WIN-L7VF1213STQ\Desktop\t Browse
Example:	C:\Pocs\Public
	R
	< Back Next > Cancel

(3) Click [Next].

Name, Descripti Specify how p	on, and Settings eople see and use this share over the network.	33
Type information a offline, dick Chang	bout the share for users. To modify how people use the e.	e content while
Share name:	temp	
Share path:	\\WIN-L7VF1213STQ\temp	
Description:		
Offline setting:	Selected files and programs available offline	Change

(4) Click [Finish].

Permissions let you control who can se have.	e the folder and the level of access they	33
Set the kind of permissions you want for th	e shared folder.	
All users have read-only access		
C Administrators have full access; othe	er users have read-only access	
C Administrators have full access; othe	er users have n <u>o</u> access	
C <u>C</u> ustomize permissions		
Custom		
By default, only share permissions are set of permissions to this folder or objects within the permissions on the Security tab to apply sp	on this folder. To control local access the folder, dick Custom and then modify ecific permissions on the folder.	the

(5) Click [Finish].

	Sharing was Successful
-	Status:
33	You have successfully completed the Share a Folder Wizard.
	Summary:
	You have selected the following share settings on \ \WIN-L7VF1213STQ: Folder path: C:\Users\Administrator.WIN- L7VF1213STQ\Desktop\temp Share name: temp Share path: \\WIN-L7VF1213STQ\temp
	When I dick Finish, run the wizard again to share another folder
	To dose this wizard, dick Finish.

- 15. Shared folder administrator settings :
 - (1) Double click the shared folder.
 - (2) Click [Share Permissions].
 - (3) Click [Add].
 - (4) Click [Location], then choose the local computer name.
 - (5) Enter the administrator account.
 - (6) Click [OK].



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

16. Share permissions settings :

Choose the user account, check to allow [Full Control], [Change] and [Read] permissions, then click [OK] $^{\circ}$

emp Pro	perties			
General	Share Permissio	ons Security		
Group	or user names:			
Se Ev	/eryone			
1			Add	Remove
				Tichiove
Permiss	ions for Everyon	e	Allow	Deny
Full	Control			
Bear	ige I			
Leam a	bout access cor	trol and permission	<u>s</u>	
		ОК	Cancel	Anoly
			Carloor	1 1000

4 Windows 2012 Server Audit log Setting

This section mainly discuss the following two settings :

1. Setting up local login audit policy.

2. Setting up local shared folder authorization and audit policy.

The default setting about Windows 2012 Server audit and share folder policy is off.

Please remember to install NXLOG, which may refer to section 1.

4.1 Setting up local login audit policy

Set as follows :

- Log in Windows 2012 Server as Administrator, click [Start / Administrative Tools / Local Security Policy], extend [Local Security Policy].
- 2. Click[Security Settings / Local Policies / Audit Policy] °



- 3. Define the following policy set value :
 - (1) Audit logon events :

Double click [Audit logon events], check [Success] and [Failure], then click [OK].

Local Security Policy	-		x
· · · · · · · · · · · · · · · · · · ·			
Policy A Security Sett	ing		
Audit account logon events No auditing			
Audit account management No auditing			
Audit directory service access No auditing			
Audit logon events No auditing			
Audit object access No auditing			
Audit policy hange No auditing			
Madit privilege use No auditing			
We Audit process tracking No auditing			
No auditing			
Audit loge events Properties ? X			
Local Security Setting Evolution			
Audit logon events			
Audit these attempts:			
✓ Success			
Le Esilve			
This setting might not be enforced if other policy is configured to			
override category level audit policy.			
For more momation, see <u>Add hogon events</u> . (Q321466)			
		2012/	7/26上
		2012/	7/26上

(2) Audit account logon events :

Double click [Audit account logon events], check [Success] and [Failure], then click [OK].

(3) Audit object access :



Double click [Audit object access], check [Success] and [Failure], then click [OK].

(4) Audit policy change :

Double click [Audit policy change], check [Success] and [Failure], then click [OK].

(5) Audit account management :

Double click [Audit account management], check [Success] and [Failure], then click [OK]. Note : If Windows 2012 Server does not run File server audit, we recommend not to audit object access, please skip steps 4.1(3) and 4.2, and only operate steps 4.1 (1), (2), (4), (5). This will help Windows avoid auditing unnecessary Object access security events. These unnecessary and redundant security events that are converted into syslog and sent to N-Reporter will reduce its performance.

4.2 Setting up local shared folder authorization and audit policy

Set as follows :

1. Click [Server Manager / File and Storage Services / Shares / TASKS / New Share...].

b		Server Manager		. <mark>0</mark> X
E	🔊 🔹 📢 Shares	- ②	Manage Tools View	v Help
	Servers Volumes Disks Storage Pools Shares iSCSI	SHARES All shares 0 tot New Share Refresh To create a file share, start the New Share Wizard.	OLUME o share is selected. Select a share to display its relatively volume. Go to Volumes Overview > VUOTA o data available. Select a share to display its relating up to a share to a share to display its relating up to a share to a shar	ed ~

🔊 NReporter

- 2. Click [SMB Share Quick] \rightarrow [Next].
- 3. Click [Type a custom path]. In this example we use "C:\share_folder ", then click [Next].
- 4. Enter share name, then click [Next].
- 5. Check [Enable access-based enumeration], click [Next].
- 6. Click [Customize permissions... / Auditing / Add].

A	New Share Wi	zard			x
Specify permission	ns to control access				
Select Profile Share Location Share Name Other Settings	Permissions to access the files on a sh permissions, and, optionally, a central Share permissions: Everyone Read Or Folder permissions:	are are set using a access policy. Ily	combination of folder perm	iissions, sha	re
Permissions Confirmation Results	Type Principal Allow CREATOR OWNER Allow BUILTIN\Users Allow BUILTIN\Users Allow BUILTIN\Administrators Allow NT AUTHORITY\SYSTEM Customize permissions	Access Full Control Special Read & execute Full Control Full Control	Applies To Subfolders and files only This folder and subfolders This folder, subfolders, an This folder, subfolders, an This folder, subfolders, an	; d files d files d files	
r	Advanced Security Setting	s for share_fold	er	_ □	x
Name: c:\share_folder Owner: Administrators (Permissions Share For additional information, doub Auditing entries:	WIN-KQCV 8PO96\Administrators) Cr Auditing Effective Access de-click an audit entry. To modify an aud	iange it entry, select the e	entry and click Edit (if availal	ole).	
Type Principal	Access	Inherited from	Applies to		
Disable inheritance					
Replace all child object audition	ng entries with inheritable auditing entrie	s from this object			
			OK Cancel	Ap	ply

7. Click [Select a principal]. If you want to audit all the administrators, please enter the object name " everyone " . Click [OK].

λ.		Auditing Entry for share_folder		_ D X
		Select User or Group	? X	
Principal:	Select a principal	Select this object type:		
Type:	Success	User, Group, or Built-in security principal	Object Types	
Applies to:	This folder, subfolders and files	From this location:		
		WIN-KQCVJ88P096	Locations	
		Enter the object name to select (<u>examples</u>):		
Basic perm	issions:	everyane	Check Names	d permissions
· ·	Full control			
	 □ Modify			
	📝 Read & execute	Advanced OK	Cancel	
	List folder contents			
	Read			
	Write			
	Special permissions			
🗌 Only app	oly these auditing settings to objects and/or contai	iners within this container		Clear all
			OK	Cancel

8. Type: Choose [All], then check [Full control]. Click [OK].

Auditing Entry for share_folder	_ D ×
Principal: Everyone Select a principal Type: All Applies to: This folder, subforders and files	
Basic permissions:	Show advanced permissions
 ✓ Read & execute ✓ List folder contents ✓ Read ✓ Write 	
Special permissions Only apply these auditing settings to objects and/or containers within this container	Clear all
Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.	
	OK Cancel

9. After completing the auditing settings, click [OK]. Then, click [Next]. Finally, click [Create] to complete the settings.

Contact Information N-Partner Company : TEL: +886-4-23752865 FAX: +886-4-23757458 Technical Support : Email: support@npartnertech.com Skype : support@npartnertech.com Sales Information : Email: sales@npartnertech.com

