

N-Partner N-REPORTER

如何使用 NXLOG 管理配置 Windows AD Server 日志 V 1.1.3 (简体)



前言

本文件描述 N-Reporter 用户如何使用 Open Source 工具 NXLOG 管理配置 Windows AD Server 2003/2008/2012 的日志(Eventlog),将事件(Event)转成 syslog,再转发到 N-Reporter 做正规化、审核与分析。本文件配置的环境分别为 Windows Server 2003、Windows Server 2008、Windows Server 2012。

N-Reporter 同时提供 Eventlog to Syslog Utility 和 NXLOG 两种将事件(Event)转 syslog 的配置文件, 其中 NXLOG 拥有较佳的效能,适用于记录大量事件的环境。当 Windows AD Server 所有日志(Eventlog) 每秒最大记录速率超过 700 笔,请选用本文 NXLOG 的配置文件。

文件章节如下:

1	配置 Windows Server	2
	1.1 配置 Windows Server 2003	2
	1.2 配置 Windows Server 2008	5
	1.3 配置 Windows Server 2012	9
2	Windows 2003 Active Directory Server 审核设置	13
	2.1 设置域用户登录注销的审核策略	13
	2.2 设置共享文件夹权限与审核策略	16
3	Windows 2008 Active Directory Server 审核设置	25
3	Windows 2008 Active Directory Server 审核设置	25 25
3	Windows 2008 Active Directory Server 申核设置 3.1 设置域用户登录注销的审核策略 3.2 设置共享文件夹权限与审核策略	25 25 30
3	Windows 2008 Active Directory Server 审核设置 3.1 设置域用户登录注销的审核策略 3.2 设置共享文件夹权限与审核策略 Windows 2012 Active Directory Server 审核设置	25 25 30 40
3	Windows 2008 Active Directory Server 审核设置 3.1 设置域用户登录注销的审核策略 3.2 设置共享文件夹权限与审核策略 Windows 2012 Active Directory Server 审核设置 4.1 设置域用户登录注销的审核策略	25 25 30 40
4	Windows 2008 Active Directory Server 审核设置 3.1 设置域用户登录注销的审核策略 3.2 设置共享文件夹权限与审核策略 Windows 2012 Active Directory Server 审核设置 4.1 设置域用户登录注销的审核策略 4.2 设定共享文件夹权限与审核策略	25 25 30 40 40 46

1 配置 Windows Server

1.1 配置 Windows Server 2003

1. 下载 NXLOG:

浏览 URL http://nxlog.org/products/nxlog-community-edition/download 下载最新版 nxlog-ce-x.x.xxxx.msi,本例下载 nxlog-ce-2.9.1347.msi。

2. 安装 NXLOG:

鼠标双点 nxlog-ce-2.9.1347.msi, 左点[Install], 执行安装。

3. 下载 Windows 2003 NXLOG 配置文件 nxlog_win2k3.conf:

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

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

注:32 位操作系统 NXLOG 安装在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位操作系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2k3.conf 设定贴上并覆盖 nxlog.conf 设定。此设定只输出主机登录、对象访问、帐户管理等 eventlog,过滤大部分噪声,减少 NXLOG 对 Windows AD 效能的负担。Windows AD 的 eventlog 每秒写入笔数超过 700 笔,建议使用 nxlog_win2k3.conf 设定。

F载 Windows 2003 NXLOG 输出全部 eventlog 配置文件 nxlog_win2k3_all.conf:
浏览 URL: http://www.npartnertech.com/download/tech/nxlog_win2k3_all.conf
N-Reporter 提供法规报表统计 Windows AD 所有 eventlog。用户若是需 Windows AD 的法规报表,
请将 nxlog_win2k3_all.conf 设定贴上并覆盖 nxlog.conf 设定。此设定会输出所有 eventlog,Windows
AD 需要较高的效能跑 NXLOG。

(接下页)

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>

绿色部位请选择 NXLOG 正确的安装路径,

本例环境为 32 位系统选择 " define ROOT C:\Program Files\nxlog " 。

红色部位输入 N-Reporter IP,本例输入 "192.168.2.64 "。

配置范例如下:



以系统管理员身分执行。

命令提示符输入:

net stop nxlog

net start nxlog

b. [开始]→[所有程序]→[管理工具]→[服务],右点服务[nxlog],左点[启动]或[重新启动]。

检查 NXLOG 是否正常启动: 6.

检查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log ", 没有显示 Error 的信息, 表示正常启动。

新增 Windows Server 2003 设备时语系选择: 7.

Windows Server 2003 繁体版请选择[BIG5]编码。

Windows Server 2003 简体版请选择[GB2312]编码。

Windows Server 2003 英文版请选择[UTF8]编码。

🞬 C:\Program Files\nxlog\data\nxlog.log - Hotepad++ 文件(12)编辑(12)搜索(2)视图(12)格式(14)语言(12)设置(12)宏(12)运行(18)插件(12)窗口(14)2) 🗄 🗏 🛍 🔥 🕞 🖌 🛍 🚺 🗩 C 📾 🋬 🔍 🖫 🔂 🖬 🔚 1 🏋 🐼 🔊 🖉 🖉 🖉

📄 nxlog. con🖾 📄 nxlog. logX

2014-10-29 18:01:14 WARNING received a system shutdown request 2014-10-29 18:01:14 WARNING stopping nxlog service 2014-10-29 18:01:14 WARNING nxlog-ce received a termination request signal, exiting... 2014-11-18 14:06:06 INFO nxlog-ce-2.8.1248 started

- 注: 因 NXLOG 没有 Eventlog to Syslog Utility 将事件编码转成 UTF8 编码的功能,所以新增 Windows Server 2003 设备时请注意语系选择,避免出现乱码。
- 8. 新增 Windows Server 2003 设备时 Facility 请选择 " (13) log audit " 。

<u>_ | ×</u>

1.2 配置 Windows Server 2008

1. 下载 NXLOG:

浏览 URL http://nxlog.org/products/nxlog-community-edition/download 下载最新版 nxlog-ce-x.x.xxxx.msi,本例下载 nxlog-ce-2.9.1347.msi。

2. 安装 NXLOG:

鼠标双点 nxlog-ce-2.9.1347.msi, 左点[Install], 执行安装。

3. 下载 Windows 2008 NXLOG 配置文件 nxlog_win2k8.conf:

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

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

注:32 位操作系统 NXLOG 安装在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位操作系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2k8.conf 设定贴上并覆盖 nxlog.conf 设定。此设定只输出主机登录、对象访问、帐户管理等 eventlog,过滤大部分噪声,减少 NXLOG 对 Windows AD 效能的负担。Windows AD 的 eventlog 每秒写入笔数超过 700 笔,建议使用 nxlog_win2k8.conf 设定。

F载 Windows 2008 NXLOG 输出全部 eventlog 配置文件 nxlog_win2k8_all.conf:
 浏览 URL: http://www.npartnertech.com/download/tech/nxlog_win2k8_all.conf

N-Reporter 提供法规报表统计 Windows AD 所有 eventlog。用户若是需 Windows AD 的法规报表, 请将 nxlog_win2k8_all.conf 设定贴上并覆盖 nxlog.conf 设定。此设定会输出所有 eventlog, Windows AD 需要较高的效能跑 NXLOG。

(接下页)

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:

Moduleim_msvistalogReadFromLast TRUESavePosTRUEQuery<QueryList> \

<Query 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> \
<pre><select path="Security">*[System[(EventID=4741)]]</select> \</pre>

```
<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> \
                                      </Query> \
                       </QueryList>
</Input>
<Output out_eventlog>
  Module
              om_udp
 Host
  Port
             514
  Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
 Exec if ($EventID == 18454 or $EventID == 18456 ) { $SyslogFacilityValue = 18; } \
      else { $SyslogFacilityValue = 13; }
 Exec if ($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>
绿色部位请选择 NXLOG 正确的安装路径,
```

本例环境为 64 位系统选择 " define ROOT C:\Program Files (x86)\nxlog " 。

红色部位输入 N-Reporter IP,本例输入 "192.168.2.64 "。

配置范例如下:

```
如何使用 NXLOG 管理配置 Windows AD Server 日志
```



5. 启动 NXLOG:

步骤 a:利用[命令提示符]启动 NXLOG 或 步骤 b:[服务]启动 NXLOG。

a. [开始]→[所有程序]→[附件],鼠标右点[命令提示符],左点[以系统管理员身分执行]。

命令提示符输入:

	net stop nxlog
	net start nxlog
b.	

6. 检查 NXLOG 是否正常启动:

检查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log ",没有显示 Error 的信息,表示正常启动。



7. 新增 Windows Server 2008 设备时 Facility 请选择 " (13) log audit "。

1.3 配置 Windows Server 2012

1. 下载 NXLOG:

浏览 URL http://nxlog.org/products/nxlog-community-edition/download 下载最新版 nxlog-ce-x.x.xxxx.msi,本例下载 nxlog-ce-2.9.1347.msi。

2. 安装 NXLOG:

鼠标双点 nxlog-ce-2.9.1347.msi, 左点[Install], 执行安装。

3. 下载 Windows 2012 NXLOG 配置文件 nxlog_win2012.conf:

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

编辑 NXLOG 配置文件 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " :

注:32 位操作系统 NXLOG 安装在 " C:\Program Files\nxlog\conf\nxlog.conf "

64 位操作系统 NXLOG 安装在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

将 nxlog_win2012.conf 设定贴上并覆盖 nxlog.conf 设定。此设定只输出主机登录、对象访问、帐户 管理等 eventlog,过滤大部分噪声,减少 NXLOG 对 Windows AD 效能的负担。Windows AD 的 eventlog 每秒写入笔数超过 700 笔,建议使用 nxlog_win2012.conf 设定。

F载 Windows 2012 NXLOG 输出全部 eventlog 配置文件 nxlog_win2012_all.conf : 浏览 URL : http://www.npartnertech.com/download/tech/nxlog_win2012_all.conf
N-Reporter 提供法规报表统计 Windows AD 所有 eventlog。用户若是需 Windows AD 的法规报表, 请将 nxlog_win2012_all.conf 设定贴上并覆盖 nxlog.conf 设定。此设定会输出所有 eventlog, Windows AD 需要较高的效能跑 NXLOG。

(接下页)

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:

Moduleim_msvistalogReadFromLast TRUESavePosTRUEQuery<QueryList> \

<Query Id="0"> \

<select< td=""><td>Path="Security">*[System[(EventID=4768)]] \</td></select<>	Path="Security">*[System[(EventID=4768)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4769)]] \</td></select<>	Path="Security">*[System[(EventID=4769)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4771)]] \</td></select<>	Path="Security">*[System[(EventID=4771)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4624)]] \</td></select<>	Path="Security">*[System[(EventID=4624)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4625)]] \</td></select<>	Path="Security">*[System[(EventID=4625)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4634)]] \</td></select<>	Path="Security">*[System[(EventID=4634)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4647)]] \</td></select<>	Path="Security">*[System[(EventID=4647)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4648)]] \</td></select<>	Path="Security">*[System[(EventID=4648)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4656)]] \</td></select<>	Path="Security">*[System[(EventID=4656)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4719)]] \</td></select<>	Path="Security">*[System[(EventID=4719)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4720)]] \</td></select<>	Path="Security">*[System[(EventID=4720)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4722)]] \</td></select<>	Path="Security">*[System[(EventID=4722)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4723)]] \</td></select<>	Path="Security">*[System[(EventID=4723)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4724)]] \</td></select<>	Path="Security">*[System[(EventID=4724)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4725)]] \</td></select<>	Path="Security">*[System[(EventID=4725)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4726)]] \</td></select<>	Path="Security">*[System[(EventID=4726)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4727)]] \</td></select<>	Path="Security">*[System[(EventID=4727)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4728)]] \</td></select<>	Path="Security">*[System[(EventID=4728)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4729)]] \</td></select<>	Path="Security">*[System[(EventID=4729)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4730)]] \</td></select<>	Path="Security">*[System[(EventID=4730)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4731)]] \</td></select<>	Path="Security">*[System[(EventID=4731)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4732)]] \</td></select<>	Path="Security">*[System[(EventID=4732)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4733)]] \</td></select<>	Path="Security">*[System[(EventID=4733)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4734)]] \</td></select<>	Path="Security">*[System[(EventID=4734)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4735)]] \</td></select<>	Path="Security">*[System[(EventID=4735)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4737)]] \</td></select<>	Path="Security">*[System[(EventID=4737)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4738)]] \</td></select<>	Path="Security">*[System[(EventID=4738)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4739)]] \</td></select<>	Path="Security">*[System[(EventID=4739)]] \
<select< td=""><td>Path="Security">*[System[(EventID=4741)]] \</td></select<>	Path="Security">*[System[(EventID=4741)]] \

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

```
<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> \
                                       </Query> \
                        </QueryList>
</Input>
<Output out_eventlog>
 Module
              om_udp
 Host
 Port
              514
 Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
 Exec if ($EventID == 18454 or $EventID == 18456 ) { $SyslogFacilityValue = 18; } \
       else { $SyslogFacilityValue = 13; }
 Exec if ($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>
```

绿色部位请选择 NXLOG 正确的安装路径,

本例环境为 64 位系统选择 " define ROOT C:\Program Files (x86)\nxlog " 。

红色部位输入 N-Reporter IP,本例输入 "192.168.2.64 "。

配置范例如下:



5. 启动 NXLOG:

步骤 a: 利用[Windows PowerShell]启动 NXLOG 或 步骤 b: [服务]启动 NXLOG。

a. 鼠标左点[开始],鼠标右点[Windows PowerShell],左点[以管理员身分运行]。

[Windows PowerShell]输入:

net stop nxlog			
net start nxlog			

b. 鼠标左点[开始]→[管理工具]→[服务], 右点服务[nxlog], 左点[启动]或[重新启动]。

6. 检查 NXLOG 是否正常启动:

检查 NXLOG 的 log 檔 " C:\Program Files (x86)\nxlog\data\nxlog.log ",没有显示 Error 的信息,表 示正常启动。



7. 新增 Windows Server 2012 设备时 Facility 请选择 " (13) log audit "。

2 Windows 2003 Active Directory Server 审核设置

本章节主要说明以下操作设置:

1.设置域用户登录注销的审核策略。2.设置共享文件夹权限与审核策略。 Windows 2003 AD Server 登录注销的审核策略和目录分享的审核策略,默认是关闭的。 请记得安装 NXLOG,详细请参阅第一章节。

2.1 设置域用户登录注销的审核策略

设置步骤如下:

1. 以管理员 Administrator 登入 Windows 2003 AD Server(域控制站)。点选 [开始 / 所有程序 / 管理

工具 / 域控制器安全策略]。



注:域安全策略(Default Domain Policy)为设定域上所有对象(Object),而域控制器安全策略 (Default Domain Controllers Policy) 为设定所有域控制站(Domain Controllers/Windows AD)。 建议两者安全审核策略设定一致。

2. 点选 [Windows 设置 / 安全设置 / 本机策略 / 审核策略]。

🚡 默认域控制器安全设置			
文件(E) 操作(A) 查看(V) 帮助	(H)		
← → 🗈 🖪 🗙 😭 😫	N E		
🦲 Windows 设置	策略 ∠	策略设置	
	間审核策略更改	无审核	
□-□ 安全设置	副审核登录事件	无审核	
	間审核对象访问	无审核	
	2011年初初日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	大軍核	
南		大軍核	
田 國 安全选项	週 申核特权使用 	二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、	
□… 🛃 事件日志		二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、二、	
🖻 🤷 受限制的組	1000年後帙广立永争住 1000年核帐户管理	一方中位	
□ 🛄 系统服务		九甲板	
□ □ □ □ 注册表			
□□□□ 1 元或网络(ILLE 002.11)束(□□□□□ 公钼管略			
田 🛃 IP 安全策略,在 Active:			
-			
	l		

- 3. 定义下列的原则设置值:
 - (1) 审核登录事件:

双击 [审核登录事件],勾选 [定义这些策略设置],再勾选 [成功]及 [失败], 设置完成后按 [确定]。



(2) 审核账户登录事件:

双击 [审核账户登录事件],勾选 [定义这些策略设置],再勾选 [成功]及 [失败], 设置完成后按 [确定]。

(3) 审核对象访问:

双击 [审核对象访问], 勾选 [定义这些策略设置], 再勾选 [成功] 及 [失败], 设置完成后按 [确定]。

成功:若欲审核成功事件的 Log , 请勾选 [成功] 复选框。 失败:若欲审核失败事件的 Log , 请勾选 [失败] 复选框。

- (4) 审核策略更改:
 双击 [审核策略更改],勾选 [定义这些策略设置],再勾选 [成功]及[失败],
 设置完成后按 [确定]。
- (5) 审核账户管理:
 双击 [审核账户管理],勾选 [定义这些策略设置],再勾选 [成功]及[失败],
 设置完成后按 [确定]。

注:若 Windows 2003 Active Directory Server 不做文件服务器审核(File server audit),建议不审核 对象访问,请直接跳过 2.1 中(3)与 2.2 的设置,只需完成 2.1 中的(1)、(2)、(4)、(5)步骤的设置,以避 免 Windows 审核多余的对象访问(Object access)审核的安全事件。此多余且事件冗长的安全事件转成 syslog 后发送给 N-Reporter 接收,会影响效能(performance)。

2.2 设置共享文件夹权限与审核策略

设置步骤如下:

- 1. 在欲共享的文件夹上点击鼠标右键,点选[属性]。
- 2. 点选 [共享] 索引卷标, 圈选 [共享此文件夹]。点选 [权限]。

share_f	older 📠	性	? ×
常规	共享	安全 自定义	
	您可以 该文件 不共享此3 共享此34	与网络上的其他用户共享该文件夹。 夹,请单击"共享此文件夹"。 【件夹 (2)	要共享
共享	名(H):	share_folder	-
注释	€(C):		
用户	数限制:	 ● 允许最多用户 (M) ● 允许的用户数量 (W): 	
要为权限	通过网络 ,请单击	访问该文件夹的用户设置 权限 "权限"。	e
要配 存"	置脱机访 。	问的设置,请单击"缓 缓存	G
		新建共	<u>\$@</u>
		确定 取消	应用 (<u>A</u>)

3. 使用者设置:

- (1) 点选 [添加], 来添加一用户。本例输入 Everyone 审核所有用户。
- (2) 点选 [位置] , 选择域。
- (3) 输入域用户账号。
- (4) 设置完成后按 [确定]。

选择用户、计算机或组	<u>?</u> ×	share_folder 的权限		<u>l</u> ×
选择对象类型 (5):		共享权限		4
用户、组或内置安全主体	对象类型 (0)	组或用户名称 (G):		
查找位置 (E):				
NPWin2k3chs.local	位置(L)			
輸入对象名称来选择(示例)(图):				
everyone	检查名称 (C)			
	·		添加(0) 册除(R)	11
		权限		1
3 我的电脑		更改		
日本 1997年1997年1997年1997年1997年1997年1997年1997		读取		
				_
洋細信息 ジ				
			11	
		确定		

- 4. 设置用户权力:
 - (1) 点选域用户账号。
 - (2) 勾选允许 [完全控制]及 [更改]权限。
 - (3) 设置完成后按 [确定]。

且或用户名称(G):		
	添加 @)	删除(图)
iveryone 的权限 (£) 完全控制 更改 读取	允许	

17 Copyright © All rights are reserved by N-Partner Technologies C

- 5. 安全性设置:
 - (1) 点选 [安全性]索引卷标。
 - (2) 点选 [添加], 来添加一用户。本例输入 Everyone 审核所有用户。
 - (3) 点选 [位置], 选择域。
 - (4) 输入用户账号。
 - (5) 设置完成后按 [确定]。

hare_folder 屈性		? ×	选择用户、计算机或组	<u>? ×</u>
常规 共享 安全 自定	义]		选择对象类型 (S):	
组或用户名称(G):			用户、组或内置安全主体	
Administrators (NPWIN2)	3CHS\Administ	rators)	查找位置 (E):	
CREATOR OWNER			NPWin2k3chs.local	位置(L)
SYSTEM	·s)		· 输入对象名称来选择(<u>示例</u>) (2): everyone	检查名称 (C)
Administrators 的权限 (P) 完全控制	添加@) 允许	册除 ® 拒绝	高级(4)	确定 取消
修改 读取和运行 列出文件夹目录	2			
读取 写入 ##9065#078	× ×			
特别权限或高级设置,请单击	"高级"。	高级 (V)		
		 应用(<u>A</u>)		

- 6. 设置用户权力:
 - (1) 点选用戶账号。
 - (2) 勾选允许 [完全控制] 权限, 以取得所有权限。
 - (3) 设置完成后按 [应用]。

Administrators (NPM	'IN2K3CHS\Administ:	rators)
CREATOR OWNER		
SYSTEM		
🕵 Users (NPWIN2K3CHS)	Users)	
	添加@)	删除(医)
Everyone 的权限(P)	允许	拒绝
完全控制		
修改 法即和进行		
列出文件夹目录		H
读取		- E - I
写入		
	自士 "吕松"。	宣体の

7. 高级安全设置:

- (1) 点选 [高级]。
- (2) 点选 [审核] 索引卷标。
- (3) 点选 [添加]。
- (4) 点选 [位置] , 选择域。
- (5) 输入用户账号。本例输入 Everyone 审核所有用户。
- (6) 设置完成后按 [确定]。

are_folder 雇性		? :	× shar	e_folder	的高级安全设计	Ë.			?
常规 共享 安全	自定义		权利	し 审核	所有者有刻	汝权限			
组或用户名称 (G):			要	查看有关特	殊审核项目的详	细信息,请选择一个	╰审核项目,然后单	击"编辑"。	
Administrators (NP)	/IN2K3CHS\Adminis	strators)	_审	"核项目(T):					
Everyone				类型	名称	访问	继承于	应用于	
SYSTEM									
🕵 Users (NPWIN2K3CHS)	(Users)								
	添加(2)	删除(E)							
Everyone 的权限(P)		 拒绝							
完全控制				添加(0)	编辑化) 冊除係	1		
修改 遠即和法行					_				
列出文件夹目录				允许父项的	的继承审核项目化	传播到该对象和所有-	子对象。包括那些花	至此明确定义的	项目(A)。
读取				用在此显示	市的那些可以应用	用到子对象的项目替付	代所有子对象的审构	亥项目 (Ľ)	
特别权限或高级设置,请单	单击"高级"。	高级 (V)	_#	一步了解审	核。				
确注	定 取消	应用(A)	1				确定	取消	应用(2)
			选择用	1户、计算;	机或组			<u>?</u> ×	
			选择	对象类型 (S):				
			用户	^D 、组或内置	安全主体		对象:	类型 (0)	
			查找	位置(2):					
			NPW	in2k3chs.10	ocal		位:	置①	
			输入	要选择的对	象名称 (例如) (图	<u>E</u>):			
			eve	ryone			检查	查名称(C)	
			-	E&R (A)	f		確定	ETT NEW	
				USS (A)			WHAE	40,415	

8. 审核项目设置:

勾选所有审核项目的 [成功] 及 [失败], 设置完成后按 [确定]。

3称(M): Everyone		更改(C)	•••
亚用到 @): 该文件夹,子文件:	夹及文件	20-11-20	-
5问(5):	成功	失败	
元主江制 遍历文件夹/运行文件 列出文件夹/读取数据 读取加展属性 创建文件/写入数据 创建文件夹/附加数据 写入属性 写入扩展属性 删除子文件夹及文件 删除 读取权限	ত ত ত ত ত ত ত ত ত		

9. 在高级安全设置完成后,点选[确定]。

, Everyone TETIERS (NEWERRARD) (ALITY)	型	<u>名称</u>		继承于 	
	ЧН	Thet Ante	76 ± 31 m3	VINER/PAD	
			2 0.1 1 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0		
	etin (n	(编号 (四)	印度の		
<u>加 (1)</u> 編輯 (2) 删除 (2)	於加位) 编辑 (E)			
加四)] 编辑 (E) 删除 (E)	添加位) 编辑 (2)			
加四) 編輯 ④ 删除 函) 许父项的继承审核项目传播到该对象和所有子对象。包括那些在此明确定义的项目	参加回 允许父) 编辑 (E) :项的继承审核项目作	」	 ^Z 对象。包括那些石	E此明确定义的项目(A
加四) 編輯 (E) 删除 (E) 许父项的继承审核项目传播到该对象和所有子对象。包括那些在此明确定义的项目	を加つ 允许父) 编辑 (E) 项的继承审核项目 f	删除 (B) 传播到该对象和所有于	 ² 对象。包括那些在	E此明确定义的项目(A
	≌加00 ℃许父 日本 ሥ) 编辑 (2) 项的继承审核项目在	删除 (B) 传播到该对象和所有于	】 ² 对象。包括那些在	E此明确定义的项目(A

10. 在分享文件夹设置完成后,点选[确定]。

常规	共享	安全	自知	EX			
组或用	1户名称(G):					
A SE	dministr	ators	(NPWIN2	K3CHS	Administ	rators)	
20	REATOR (WNER					
E E	veryone						
S S	YSTEM						
1	sers (M)	WIN2K3	CHS\Vs	ers)			
1							
				添加	(D)	删除®)
Every	one 的权	限(2)			允许	拒绝	
完全	È控制						
修改	文						
读明	如石运行						
列出	出文件夹制	录					
读明	又						
写)	1				\checkmark		-
	0654078					—	-
特别和	(股或高级	以设置,	请甲击	" 局级'	• (高级(2))
		-	120.121		41414000	NERT ANT IN	1.1

11. 点选 [开始 / 所有程序 / 管理工具 / 计算机管理]。

		S	Active Directory 用户和计算机
		SB	Active Directory 域和信任关系
		5	Active Directory 站点和服务
		2	DNS
			Microsoft .NET Framework 1.1 配置
		验	Microsoft .NET Framework 1.1 向导
		Ŀs	分布式文件系统
		1	服务
		1	服务器管理器
		1	管理您的服务器
administrator		9	计算机管理
administrator		Đ	路由和远程访问
一 善用你的更发现	💭 我的电脑	9	配置您的服务器向导
● 日庄25印象分音	5	-	群集管理器
人名坦兰 茨	🛃 控制面板(事件查看器
GA- 即考定不付	1 会理了目	ē	授权
(C2)	- BHTH	8	数据源 (ODBC)
Indows 员福吉建备	打印机和布		网络负载平衡管理器
		T	性能
记事本	1 帮助和支持	-	域安全策略
		-	域控制器安全策略
Active Directory 用尸和 计質机		(Ch)	远程桌面
	(<u>a)</u> (<u>a</u>)	m	证书颁发机构
₩ Tindows Windows	s Catalog	帮	终端服务管理器
🕛 🍪 Windows	s Update	高	终端服务配置
🚦 事件查看器 📄 附件	,	而	终端服务器授权
	. ,	0	组件服务
域安全策略 局动	•	r i	
	et Explorer		
/ 写字板 🛐 Outlool	Express		
	њ		
所有程序 (E) A Tatars	ect Allianca 🕨		
the second second second		1	
	∠ 2 注销(L))	◯ 关机 (1)
創开始 🖉 🙆 📄			

12. 点选 [系统工具/共享文件夹/共享]。

昌 计算机管理					
🗐 文件 (E) 操作 (A) 查看 (V) 1	窗口(11) 帮助(11)				_ B ×
	1 📖				
📃 计算机管理(本地)	共享名 🛆	文件夹路径	类型	# 客户	端连接
日 🌇 系统工具	R ADMIN\$	C:\WINDOWS	Windows	0	
由	C\$	C:\	Windows	0	
	JIPC\$		Windows	0	
	NETLOGON	C:\WINDOWS\SYSV	Windows	0	
	Share_folder	C:\share_folder	Windows	0	
 ● 一個 性能日志和警报 ● 设备管理器 ● ● 存储 ● ● 可移动存储 ● ● 可移动存储 ● ● 磁盘碎片整理程序 ● 磁盘管理 ● ● 服务和应用程序 	SISVOL	C: \WINDOWS\SISV	Windows	U	
	 				Þ

13. 双击该分享文件夹, 点选 [共享权限]索引卷标。 点选用户账号, 勾选允许 [完全控制]、[更改] 及 [读取]权限, 设置完成后按 [确定]。

三 计算机管理					<
① 文件 (2) 操作 (A) 查看 (V) ③	窗口(\r) 帮助(\r)			_ 8 ×	:
	2				
📕 计算机管理(本地)	共享名 /	文件夹路径	类型	# 客户端连接	T
京 派 系统工具	admin\$	C:\WINDOWS	Windows	0	
💿 🗐 事件查看器	😡 C\$	C:X	Windows	0	
日 😝 共享文件夹	IPC\$		Windows	0	
	NETLOGON	C:\WINDOWS\SYSV	Windows	0	
	🜏 share_folder	C:\share_folder	Windows	0	
四、网 性能日素和整据	SYSVOL	C:\WINDOWS\SYSV	Windows	0	
□ 301 注船口芯相自10	-1	24+		21 21	
□ 圖 存储	suare_torder H	6LE			
□ 🔐 可移动存储	常规 发布	共享权限 安全			
磁盘碎片整理程序	射武田中夕称(c) ·			
	2H34/11/ -01/01 (<u>v</u>).			
出 38 服务和应用程序	1 Lveryone				
	T .		添加(四)		a
l	L Everyone 的权	限(2)	允许	拒绝	-
)	完全控制				
	更改			H	
	读取			H H	
			To Sile		
				<u>巡用(A)</u>	

3 Windows 2008 Active Directory Server 审核设置

本章节主要说明以下操作设置:

1.设置域用户登录注销的审核策略。2.设置共享文件夹权限与审核策略。 Windows 2008 AD Server 登录注销的审核策略和目录分享的审核策略,默认是关闭的。 请记得安装 NXLOG,详细请参阅第一章节。

3.1 设置域用户登录注销的审核策略

设置步骤如下:

以管理员 Administrator 登录 Windows 2008 AD Server(域控制站)。开启组策略管理。
 点选[开始 / 运行]。

输入:gpmc.msc,完成后按[确定]。

 □ 命令提示符 □ 記事本 			💦 下载并安装更新(I)	检查更 已安装
🧭 Internet Explorer	administrator	3	自定义此服务器	
本地安全策略	文档 		[]] 添加角色(A)	角色:
Active Directory 用户和计算 机	计算机 网络		添加功能(F)	功能:
 第件查看器 通 事件查看器 通 组件服务 ● 所有程序 搜索程序和文件 	控制面板 设备和打印机 管理工具 → 帮助和支持 运行 注销 →	ビルAID Windd 文件夹 打开(O): gpmd 愛 使	ows 将根据您所输入的名称,为您打开相应。 文档或 Internet 资源。 c.msc 通用管理权限创建此任务。 确定 取消	
🎝 开始 👪 ⊿ 📜 🧃				

2. 点选 [林/域/win2008chs.local / Default Domain Controllers Policy]。



注:此步骤展开域(Domain),出现 [默认域安全策略(Default Domain Policy)];展开域控制站(Domain Controllers),出现 [默认域控制站安全策略(Default Domain Controllers Policy)]。

3. 在 Default Domain Controllers Policy 点击鼠标右键, 点选[编辑]。



注: Default Domain Policy 为设定域上所有对象 (Object), 而 Default Domain Controllers Policy 为 设定所有域控置站(Domain Controllers/Windows AD)。建议两者安全审核策略设定一致。 4. 点选 [计算机配置/策略/Windows 设置/安全设置/本地策略/审核策略]。

』 组策略管理编辑器		
文件(F) 操作(A) 查看(V) 帮助(H)		
🗇 🔿 🙎 💼 😖 👔 🖬	n	
Pefault Domain Controllers Policy [WIN2K8▲ 计算机配置 使我件设置 使了我件设置 使了我件设置 使了我件设置 使了我名解析策略 使为名解析策略 使为全设置 使了我名解析策略 使为全设置 使了我名解析策略 使于我的人们的一个意味 使于我的人们的一个意味 使用户权限分配 使用户权限分配 使用户权限分配 使用户权限分配 使用户权限分配 使限制的组 使限制的组 使派统服务	 → 第 第 第 市核 校長 市核 中核 中 市 市 市 市 市 市 市 市 ボ ボ<th>策略设置 无审核 无审核</th>	策略设置 无审核 无审核

- 5. 定义下列的策略设置值:
 - (1) 审核登录事件:

双击 [审核登录事件], 勾选 [定义这些策略设置], 再勾选 [成功] 及 [失败],





(2) 审核账户登录事件:

双击 [审核账户登录事件], 勾选 [定义这些策略设置], 再勾选 [成功] 及 [失败], 设置 完成后按 [确定]。



(3) 审核对象访问:

双击 [审核对象访问], 勾选 [定义这些策略设置], 再勾选 [成功] 及 [失败], 设置完成 后按 [确定]。



(4) 审核策略更改:

双击 [审核策略更改],勾选 [定义这些策略设置],再勾选 [成功] 及 [失败],设置完成后 按 [确定]。

(5) 审核账户管理:

双击 [审核账户管理],勾选 [定义这些策略设置],再勾选 [成功]及 [失败],设置完成后按 [确定]。

注:若 Windows 2008 Active Directory Server 不做文件服务器审核(File server audit),建议不审核 对象访问,请直接跳过 3.1 中(3)与 3.2 的设置,只需完成 3.1 的(1)、(2) 、(4) 、(5)步骤的设置,以避免 Windows 审核多余的对象访问(Object access)审核的安全事件。此多余且事件冗长的安全事件转成 syslog 后发送给 N-Reporter 接收,会影响效能(performance)。

3.2 设置共享文件夹权限与审核策略

设置步骤如下:

- 1. 在欲共享的文件夹上点击鼠标右键,点选[属性]。
- 2. 点选[共享]索引卷标,圈选[共享]。

一网络文件和文	Z件夹共享 re folder	
→ 不共 网络路径 00	·	
不共享 世 (3)	1	
- 高级共享		
设置自定义相 项。	又限,创建多个共享,并设置其	其他高级共享选
💡 高级技	共享(0)	

3. 在文件共享设置中,点下拉选单至[查找用户]。

1	
Evenyone	
查找用户	
👗 Administrator	读取/写入 ▼
Administrators	所有有

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

4. 用户设置:

- (1) 点选 [位置] , 选择域。
- (2) 输入域用户账号。本例输入 Everyone 审核所有用户。
- (3) 设置完成后按 [确定]。

选择用户或组		<u>? ×</u>
选择此对象类型(S):		
用户、组或内置安全主体		对象类型(0)
查找位置(F):		
win2008chs.local		位置(L)
输入对象名称来选择(示例)(图):		11 I.
everyone		检查名称(C)
高级(A)	确定	取消

5. 点选 [共享]。

	★ 添加(A)	
名称 《 Administrator	权限级别 法取/写) ▼	
Administrator	所有者	
Everyone	读取 ▼	

6. 等待共享设置完成后,再按[完成]。

🧊 文件共享	×
G 🗷 文件共享	
您的文件夹已共享。	
可通过电子邮件向某个人发送到这些共享项的链接,或将链接复制并粘贴到其他程序中。	
各个项目	E
share_folder \\WIN2K8ADCHS\share_folder	
显示该计算机上的所有网络共享。	
	完成 (0)

7. 安全设置:

- (1) 点选 [安全] 索引卷标。
- (2) 点选用户名,本例输入 Everyone 审核所有用户。
- (3) 点选 [编辑]。

组或用户名(G):		
STSTEM		
& Administrator		
Administrators (WIN2	2008CHS\Administra	tors)
要更改权限,请单击"编辑	" ·	扁辑(E)
Everyone 的权限(P)	允许	拒绝
完全控制		-
修改		
读取和执行	~	
	1	
列出又1年夹内谷	1.0	
列出又件夹内谷 读取	~	

- 8. 设置用户权力:
 - (1) 点选用户名,本例输入 Everyone 审核所有用户。
 - (2) 勾选允许 [完全控制]权限,以取得所有权限。
 - (3) 设置完成后按 [确定]。

时象名称: C:\share_	folder		
目或用户名(G); 			
SYSTEM			
Administrator (WI)	N2008CHS\Ad	lministr	ators)
	添加	ወ)	删除(R)
veryone 的权限(P)	添加	@) 允许	删除 (B) 拒绝
veryone 的权限(P) 完全控制	<u>添加</u>	@) 允许 ☑	删除 (B.) 拒绝
veryone 的权限(P) 完全控制 修改 读取和执行	<u>添加</u>	(D) 允许 又又又	删除 (R) 拒绝
veryone 的权限(F) 完全控制 修改 读取和执行 列出文件夹内容	<u>添加</u>	^(D) 允许 又又又又	删除 (B) 拒绝

- 9. 高级安全设置:
 - (1) 点选 [高级]。
 - (2) 点选 [审核] 索引卷标。
 - (3) 点选 [编辑]。
 - (4) 点选 [添加]。
 - (5) 点选 [位置], 选择域。
 - (6) 输入用户账号,本例输入 Everyone 审核所有用户。
 - (7) 设置完成后按 [确定]。

🚺 share_folder 属性 📃	🕌 share_fold	er 的高级安全	全设置				x	
常规 共享 安全 以前的版本 自定义	权限 审核	所有者有	i效权限					ndows Server 20 Icenter
对象名称: C:\share_folder	若要查看某个	权限项目的详细	细信息,请双击该 ^I	页目。若要修改	权限,请单击"更	改权限"。		
组或用户名(6):	对象名称:	C:\share f	Folder					
& Everyone	()]() 宙核项目(T))							搜索 本地磁盘 (C
Administrator	类型	名称]	继承于			
& Administrators (WIN2008CHS\Administrators)								
要更改权限,请单击"编辑"。 编辑 (E)							1	
Everyone 的权限(F) 允许 拒绝								
完全控制 イ -								
▶ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1								
→ 列出文件夹内容 ✓	に自想の	1						
	5冊4章 (27							
有关特殊权限或高级设置,请单击"高高级(V)。	▶ 包括可从	刻了象的父项组	撬的审核项目(I)					
	常按时每注读	的画动目江ル	, 	Mar Marine Marine	harder alle also	-P./n		
▶ Share_folder 的高级女主反立			<u> </u>	达洋用尸、オ	具机、服労幣尸	兴 祖		
				选择此对象突	型(S): 回罟安全主体			対象米刑の)
要宣看或编辑申核项目的详细信息,请选择该项目开里击"编辑"	0			查找位置 (F):				X13X X 1 0 /
对象名称: C:\share_folder				win2008chs.	local			位置 (L)
审核项目(I):				, 输入要选择的	[]]象名称(<u>例如</u>)(<u>E</u>):	-	
	進承于	<u> 应用于</u>		everyone				检查名称(C)
				「古切(い)	1	_	72-	1 1 1
					·		明定	
添加 @) 编辑 @) 删除 (R)								
☑ 包括可从该对象的父项继承的审核项目 (I)								
□ 使用可从此对象继承的审核项目替换所有后代上现有的所有可	继承审核项目(P)							* EUm
								X [4](C)
里核系系加回时要求是什么?								
	确定	取消	应用(A)					

10. 审核项目设置:

勾选所有审核项目的 [成功] 及 [失败], 设置完成后按 [确定]。

名称(M): Everyone 应用到(0): 此文件夹、子文件夹和)	文件	更改(C).	
访问(S):	成功	失败	
元全控制 遍历文件夹/执行文件 列出文件夹/读取数据 读取属性 创建文件/写入数据 创建文件夹/附加数据 写入属性 写入扩展属性 删除子文件夹及文件 删除			
□ 仅将这些审核项目应用到此容器 象和/或容器(T) 管理审核	中的对	全部清除	(L)

11. 在高级安全设置配置完成后,点选[确定]。

减项目 (1):			
类型	名称	访问	继承于	应用于
全部	Everyone	完全控制	〈不是继承的〉	此文件夹、子文件
添加面)	(编辑 (7)			
添加(0)	编辑(E)			

核项目 (T)	1:			
た しょう	名称	访问	继承于	应用于
EaP	Tveryone	元主控制	《小走地序印》》	

12. 在分享文件夹设置完成后,点选[确定]。

组或用户名 (G & Everyone & SYSTEM & Administ:): rator		
Administ: 要更改权限,	rators (WIN2O 清单击"编辑"	08CHS\Administr	ators) 编辑(E)
Everyone 的权	2限(P)	允许	拒绝
完全控制		~	
修改		~	
读取和执行		~	
列出文件夹	内容	~	
读取		~	
<u>写入</u>		1	
右 半時难扣阻:	动 直纸设置,语	「 宮" 上前	宣纪(1/)



14. 点选 [系统工具/共享文件夹/共享]。

🛃 计算机管理					
文件(F) 操作(A) 查看(V)	帮助(H)				
🗢 🔿 🖄 📅 🛛 🔤 🛛	3				
🌉 计算机管理(本地)	- 共享名 🔺	文件夹路径	类型	# 客户端连接	
🖸 🖹 系统工具	admin\$	C:\Windows	Windows	0	Remote Admin
🖽 🕑 任务计划程序	50 C\$	C:\	Windows	0	Default share
田 副 事件查看器	1PC\$		Windows	0	Remote IPC
	🛛 📆 NETLOGON	C:\Windows\SYSVOL\sysvol\win20	Windows	0	Logon server s
82 开写	👔 share_folder	C:\share_folder	Windows	0	
281 云话 262 打开文件	SYSVOL	C:\Windows\SYSVOL\sysvol	Windows	0	Logon server s
표 🔕 性能					
🚔 设备管理器					
■ ■ 「 「 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■					
由 📷 服为和应用柱序					
					•

15. 双击该分享文件夹,点选[共享权限]索引卷标。点选用户账号,本例选择 Everyone 审核所有用 户。勾选允许[完全控制]、[更改]及[读取]权限,设置完成后按[确定]。

共享名 ▲	文件夹路径	类型	# 客户端连接	
ADMIN\$	C:\Windows	Windows	0	Remote Admin
500C\$	C:\	Windows	0	Default share
IPC\$		Windows	0	Remote IPC
netlogon	C:\Windows\SYSVOL\sysvol\win20	Windows	0	Logon server s
就 share_folder	C:\share_folder	Windows	0	
፼ SYSVOL shar 常規	C:\Windows\SYSVOL\sysvol e_folder 属性 现 发布 共享权限 安全	Windows		Logon server s
	i或用户名(G): Everyone Administrators (WIN2008CHS\Admini	istrators)		
	<u>流</u>	加0)		
E	veryone 的权限(P)	允许	拒绝	
	完全控制 更改 读取			
	" <u>解访问控制和权限</u> 确定	取消	应用 (A)	
-				

4 Windows 2012 Active Directory Server 审核设置

本章节主要说明以下操作设置:

1.设置域用户登录注销的审核策略。2.设置共享文件夹权限与审核策略。

Windows 2012 AD Server 登录注销的审核策略和目录分享的审核策略,默认是关闭的。

请记得安装 NXLOG , 详细请参阅第一章节。

4.1 设置域用户登录注销的审核策略

配置步骤如下:

 以管理员 administrator 登入 Windows 2012 AD Server(域控制站)。鼠标左点[开始],右点 [Windows PowerShell],左点[Run as Administrator]。

输入:gpmc.msc,完成后按[Enter],开启[组策略管理]。

Σ	Administrator: Windows PowerShell	_ D X
Windows PowerShell Copyright (C) 2012 Microsoft Corporation.	All rights reserved.	^
PS C:\Users\Administrator> gpmc.msc PS C:\Users\Administrator> _		

- 2. 点选 [林 / 域 / npartnertech.com / Domain Controllers / Default Domain Controllers Policy]。
- 3. 鼠标右点[Default Domain Controllers Policy], 点选[编辑], 开启[组策略管理编辑器]。

<u>s</u>	组策略管理	
🔜 文件(F) 操作(A) 查看(V) 窗口(W) 帮助(H	0	_ - ×
🗢 🔿 🙍 🔣 🖬		
🔜 组策略管理	Default Domain Controllers Policy	у
⊿ A 林: npartnertech.com	作用域 详细信息 设置 委派	
⊿ ∰ npartnertech.com	鐵接	
🗐 Default Domain Policy	在此位置内显示链接(L): npartnertech	ch.com v
a 🗊 Domain Controllers	下列站点、域和组织单位链接到此 GPO(T):	
▶ 📑 组第略对象	位置 强制	日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日
▷ 📑 WMI 筛选器	III Domain Controllers 否	是 npartnertech.com/Domain Controll
▷ [፴] Starter GPO ▷ [語 就占		
2 组 第 略建模		
民 组 策略结 果		
	< III	۱ ک
	此 GPO 内的设置只应用于下列组、用户和计算机(S):	
	名称	
	& Authenticated Users	
	添加(D) 删除(R)	属性(P)
	│ ▼TI 筛选	
	此 GPO 链接到下列 WMI 筛选器(W):	
<		✔ 打开(0)
	,	

注:此步骤展开域(Domain),出现 [默认域安全策略(Default Domain Policy)]; 展开域控制站 (Domain Controllers),出现 [默认域控制站安全策略(Default Domain Controllers Policy)]。 如何使用 NXLOG 管理配置 Windows AD Server 日志

4. 点选 [计算器配置 / 策略 / Windows 设置 / 安全设置 / 本地策略 / 审核策略]。



注 : Default Domain Policy 为设定域上所有对象 (Object), 而 Default Domain Controllers Policy 为

设定所有域控置站(Domain Controllers/Windows AD)。建议两者安全审核策略设定一致。

- 5. 定义下列的策略设定值:
 - (1) 审核登录事件(Audit logon events):

双击 [审核登录事件],勾选 [定义这些策略设置],再勾选 [成功]及 [失败],设定完成后按 [确定]。



(2) 审核账户登录事件(Audit account logon events):

双击 [审核账户登录事件], 勾选 [定义这些策略设置], 再勾选[成功] 及 [失败], 设定完成后按 [确定]。



- (3) 审核对象访问(Audit object access):
 双击[审核对象访问],勾选[定义这些策略设置],再勾选[成功]及[失败],
 设定完成后按[确定]。
- (4) 审核策略更改(Audit policy change):
 双击[审核策略更改],勾选[定义这些策略设置],再勾选[成功]及[失败],
 设定完成后按[确定]。
- (5) 审核账户管理(Audit account management):
 双击[审核账户管理],勾选[定义这些策略设置],再勾选[成功]及[失败],
 设定完成后按[确定]。

注:若 Windows 2012 Active Directory Server 不做文件服务器稽核(File server audit),建议不审核 对象访问,请直接跳过 4.1 中(3)与 4.2 的设置,只需完成 4.1 的(1)、(2) 、(4) 、(5)步骤的设定,以避免 Windows 审核多余的对象访问(Object access)的安全事件。此多余且事件冗长的安全事件转成 syslog 后发送给 N-Reporter 接收,会影响效能(performance)。

4.2 设定共享文件夹权限与审核策略

设定步骤如下:

1. 点选 [服务器管理器 / 文件和储存服务 / 共享 / 任务 / 新建共享...]。



- 2. 选择配置文件,鼠标左点 [SMB 共享-快速],左点 [下一步]。
- 3. 共享位置勾选[键入自定义路径],本例输入 " C:\share_folder ", 左点[下一步]。
- 4. 输入共享名称,本例输入 "share_folder ",左点 [下一步]。
- 5. 其他设置勾选 [启用基于存取的枚举], 左点 [下一步]。
- 6. 权限点选 [自定义权限... / 审核 / 添加] 。

2	新建共享向导	_	D X	
指定控制访问的机	又限			
选择配置文件 共享位置 共享名称	对共享上文件的访问权限,是结合使用文件夹权限、共 共享权限:所有人都完全控制 文件夹权限(F):	:享权限以及中心访问策略(可选)而设	置的。	
其他设置 权限 确认 结果	类型 主体 访问 允许 CREATOR OWNER 完全控制 允许 BUILTIN\Users 特殊 允许 BUILTIN\Users 技取和执行 允许 BUILTIN\Administrators 完全控制 允许 NT AUTHORITY\SYSTEM 完全控制 自定义权限(C) 日 日	应用于 仅子文件夹和文件 此文件夹和子文件夹 此文件夹、子文件夹及其中包含的 此文件夹、子文件夹及其中包含的 此文件夹、子文件夹及其中包含的	1文件 1文件 1文件	
),	share_folder的高级安	全设置		_ 🗆 X
名称: C:\share_folder 所有者: Administrators (N 权限 共享 有关其他信息,请双击审核项目 审核项目:	PARTINERTECH∖Administrators)更改(C) 审核 有效访问 :若要修改审核项目,请选择该项目并单击"编辑"(约	미果可用) •		
美型 主体 添加(D) 删除(R) 禁用继承(I) 一	查看(\/) 直看(\/)	▶ ■ ■ ■	7	
山波用可不成对象级承的审核,	《山台·坎州方丁八·多时甲依坝日(F)	74. 1	÷	K ROBAN
		明7	AE (1927)	8 <u>M</u> H(A)

7. 左点 [选择主体], 如果欲审核所有用户, 对象名称输入 " everyone " , 左点 [确定] 。

X.	share_folder 的审核项目		_ □ X
主体: 选择主体	选择用户、计算机、服务帐户或组	? ×	
类型: 成功 ✓ 应用于: 此文件夹、子文件夹和文件 ✓	选择此对象类型(S): 用户、组或内置安全主体	对象类型(O)	
基本权限:	查找位置(F): npartnertech.com	位置(L)	显示高级权限
 □ 完全控制 □ 修改 □ 读取和执行 	输入要选择的对象名称(例如)(E):	检查名称(C)	
	高级(A) 确定	取消	公如注注
□ 仅将这些审核设置应用到此容器中的对象和/或容器(T)			全部清除

8. 类型下拉选 [全部] ,基本权限勾选 [完全控制] ,左点 [确定]。

🖡 share_folder 的审核项目	_ □ X
主体: Everyone 选择主体 类型: 全部	
 基本权限: ダ完全控制 ダ修改 ダ该取和执行 ダ列出文件夹内容 ダ支取 マラ入 特殊权限 	显示高级权限
□ 仅将这些审核设置应用到此容器中的对象和/或容器(T) 添加条件以限制此审核项目的范围。仅当满足条件时才记录安全事件	全部清除
添加条件(D)	
确须	取消

9. 等待设定完成后,左点 [确定]。左点 [下一步]。左点 [创建]完成设定。

连络信息

N-Partner 公司连络方式: TEL: +886-4-23752865 FAX: +886-4-23757458 有关技术问题请洽: Email: support@npartnertech.com Skype : support@npartnertech.com 有关业务相关问题请洽: Email: sales@npartnertech.com

