



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
3.1 设置域用户登录注销的审核策略	25
3.2 设置共享文件夹权限与审核策略	30
4 Windows 2012 Active Directory Server 审核设置	40
4.1 设置域用户登录注销的审核策略	40
4.2 设定共享文件夹权限与审核策略	46
联络信息	47

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。

4. 下载 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 192.168.2.64
  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：

```

C:\Program Files\nxlog\conf\nxlog.conf - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 语言(L) 设置(T) 宏(M) 运行(R) 插件(P) 窗口(W) ?
nxlog.conf
2  L## online at http://nxlog.org/nxlog-docs/en/nxlog-reference-manual.html
3
4  ## Please set the ROOT to the folder your nxlog was installed into,
5  ## otherwise it will not start.
6
7  define ROOT C:\Program Files\nxlog
8  #define ROOT C:\Program Files (x86)\nxlog
9
10 ModuleDir %ROOT%\modules
11 CacheDir %ROOT%\data
12 Pidfile %ROOT%\data\nxlog.pid
13 SpoolDir %ROOT%\data
14 LogFile %ROOT%\data\nxlog.log
15
16 <Extension syslog>
17   Module xm_syslog
18 </Extension>
19 <Input in_eventlog>
20 # For windows 2003 and earlier use the following:
21   Module in_mseventlog
22   Exec parse_syslog_bsd(); \
23     if ($EventID == 672 or $EventID == 673 or $EventID == 675 or $EventID == 528 or $EventID == 529 or $EventID == 538 or $EventID == 540
24       or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or $EventID == 627 or $EventID == 628
25       or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or $EventID == 633 or $EventID == 634 or $EventID == 635
26       or $EventID == 636 or $EventID == 637 or $EventID == 638 or $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID == 646
27       or $EventID == 647) { $SyslogFacilityValue = 13; } \
28     else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
29     else if ($SourceName =~ /MSSQL*/) { $SyslogFacilityValue = 18; } \
30     else \
31       drop(); \
32 </Input>
33 <Output out_eventlog>
34   Module om_udp
35   Host 192.168.2.64
36   Port 514
37   Exec $Message = string($EventID) + " : " + $Message;
38   Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
39     else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
40     else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
41 </Output>
42 <Route eventlog>
43   Path in_eventlog => out_eventlog
44 </Route>
45
46 Perl source file      length: 2029  lines: 47  ln: 31  col: 1  sel: 0 | 0  DosWindows  UTF-8 w/o BOM  INS
    
```

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[运行方式], 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]。

6. 检查 NXLOG 是否正常启动：

检查 NXLOG 的 log 档 " 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 2003 设备时语系选择：

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 - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(O) 语言(L) 设置(T) 宏(M) 运行(R) 插件(P) 窗口(W) ?
nxlog.log
1  2014-10-29 18:01:14 WARNING received a system shutdown request
2  2014-10-29 18:01:14 WARNING stopping nxlog service
3  2014-10-29 18:01:14 WARNING nxlog-ce received a termination request signal, exiting...
4  2014-11-18 14:06:06 INFO nxlog-ce-2.8.1248 started
5
    
```

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 "。

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。

4. 下载 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:
  Module im_msvistalog
  ReadFromLast TRUE
  SavePos TRUE
  Query <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> \
          <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> \
    </Query> \
</QueryList>
</Input>
<Output out_eventlog>
    Module      om_udp
    Host        192.168.2.64
    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：


```

38 <Select Path="Security">*[System[(EventID=4723)]]</Select> \
39 <Select Path="Security">*[System[(EventID=4724)]]</Select> \
40 <Select Path="Security">*[System[(EventID=4725)]]</Select> \
41 <Select Path="Security">*[System[(EventID=4726)]]</Select> \
42 <Select Path="Security">*[System[(EventID=4727)]]</Select> \
43 <Select Path="Security">*[System[(EventID=4728)]]</Select> \
44 <Select Path="Security">*[System[(EventID=4729)]]</Select> \
45 <Select Path="Security">*[System[(EventID=4730)]]</Select> \
46 <Select Path="Security">*[System[(EventID=4731)]]</Select> \
47 <Select Path="Security">*[System[(EventID=4732)]]</Select> \
48 <Select Path="Security">*[System[(EventID=4733)]]</Select> \
49 <Select Path="Security">*[System[(EventID=4734)]]</Select> \
50 <Select Path="Security">*[System[(EventID=4735)]]</Select> \
51 <Select Path="Security">*[System[(EventID=4737)]]</Select> \
52 <Select Path="Security">*[System[(EventID=4738)]]</Select> \
53 <Select Path="Security">*[System[(EventID=4739)]]</Select> \
54 <Select Path="Security">*[System[(EventID=4741)]]</Select> \
55 <Select Path="Security">*[System[(EventID=4742)]]</Select> \
56 <Select Path="Security">*[System[(EventID=4743)]]</Select> \
57 <Select Path="System">*[System[(EventID=7036)]]</Select> \
58 <Select Path="Application">*[System[(EventID=18454)]]</Select> \
59 <Select Path="Application">*[System[(EventID=18456)]]</Select> \
60 </Query> \
61 </QueryList>
62 </Input>
63
64 <Output out_eventlog>
65   Module      om_udp
66   Host        192.168.2.64
67   Port        514
68   Exec $Message = string($SourceName) + " : " + string($EventID) + " : " + $Message;
69   Exec if ($EventID == 18454 or $EventID == 18456 ) { $SyslogFacilityValue = 18; } \
70     else { $SyslogFacilityValue = 13; }
71   Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
72     else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
73     else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
74   Exec to_syslog_bsd();
75 </Output>
76
77 <Route eventlog>

```

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. [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]。

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。

```

C:\Program Files\nxlog\data\nxlog.log - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(T) 宏(O) 运行(R) 插件(P) 窗口(W) ?
1 2014-10-22 16:57:51 WARNING nxlog-ce received a termination request signal, exiting...
2 2014-10-23 09:06:51 INFO nxlog-ce-2.8.1248 started
3 2014-10-23 09:38:10 WARNING received a system shutdown request
4 2014-10-23 09:38:10 WARNING stopping nxlog service
5 2014-10-23 09:38:10 WARNING nxlog-ce received a termination request signal, exiting...
6 2014-11-20 10:32:04 INFO nxlog-ce-2.8.1248 started
7

```

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。

4. 下载 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:
  Module im_msvistalog
  ReadFromLast TRUE
  SavePos TRUE
  Query <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> \
          <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> \
    </Query> \
</QueryList>

</Input>

<Output out_eventlog>
    Module    om_udp
    Host      192.168.2.64
    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：

```

25 <Query Id="0"> \
26 <Select Path="Security">*[System[(EventID=4768)]]</Select> \
27 <Select Path="Security">*[System[(EventID=4769)]]</Select> \
28 <Select Path="Security">*[System[(EventID=4771)]]</Select> \
29 <Select Path="Security">*[System[(EventID=4624)]]</Select> \
30 <Select Path="Security">*[System[(EventID=4625)]]</Select> \
31 <Select Path="Security">*[System[(EventID=4634)]]</Select> \
32 <Select Path="Security">*[System[(EventID=4647)]]</Select> \
33 <Select Path="Security">*[System[(EventID=4648)]]</Select> \
34 <Select Path="Security">*[System[(EventID=4656)]]</Select> \
35 <Select Path="Security">*[System[(EventID=4719)]]</Select> \
36 <Select Path="Security">*[System[(EventID=4720)]]</Select> \
37 <Select Path="Security">*[System[(EventID=4722)]]</Select> \
38 <Select Path="Security">*[System[(EventID=4723)]]</Select> \
39 <Select Path="Security">*[System[(EventID=4724)]]</Select> \
40 <Select Path="Security">*[System[(EventID=4725)]]</Select> \
41 <Select Path="Security">*[System[(EventID=4726)]]</Select> \
42 <Select Path="Security">*[System[(EventID=4727)]]</Select> \
43 <Select Path="Security">*[System[(EventID=4728)]]</Select> \
44 <Select Path="Security">*[System[(EventID=4729)]]</Select> \
45 <Select Path="Security">*[System[(EventID=4730)]]</Select> \
46 <Select Path="Security">*[System[(EventID=4731)]]</Select> \
47 <Select Path="Security">*[System[(EventID=4732)]]</Select> \
48 <Select Path="Security">*[System[(EventID=4733)]]</Select> \
49 <Select Path="Security">*[System[(EventID=4734)]]</Select> \
50 <Select Path="Security">*[System[(EventID=4735)]]</Select> \
51 <Select Path="Security">*[System[(EventID=4737)]]</Select> \
52 <Select Path="Security">*[System[(EventID=4738)]]</Select> \
53 <Select Path="Security">*[System[(EventID=4739)]]</Select> \
54 <Select Path="Security">*[System[(EventID=4741)]]</Select> \
55 <Select Path="Security">*[System[(EventID=4742)]]</Select> \
56 <Select Path="Security">*[System[(EventID=4743)]]</Select> \
57 <Select Path="System">*[System[(EventID=7036)]]</Select> \
58 <Select Path="Application">*[System[(EventID=18454)]]</Select> \
59 <Select Path="Application">*[System[(EventID=18456)]]</Select> \
60 </Query> \
61 </QueryList>
62 </Input>
63
64 <Output out_eventlog>
65     Module    om_udp
66     Host      192.168.2.64
67     Port      514
68     Exec $Message = string($SourceName) + " : " + string($EventID) + " : " + $Message;
69     Exec if ($EventID == 18454 or $EventID == 18456 ) { $SyslogFacilityValue = 18; } \
70         else { $SyslogFacilityValue = 13; }
71     Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
72         else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
73         else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
74     Exec to_syslog_bsd();
75 </Output>
76
77 <Route eventlog>
78     Path      in_eventlog => out_eventlog
79 </Route>
80

```

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]。

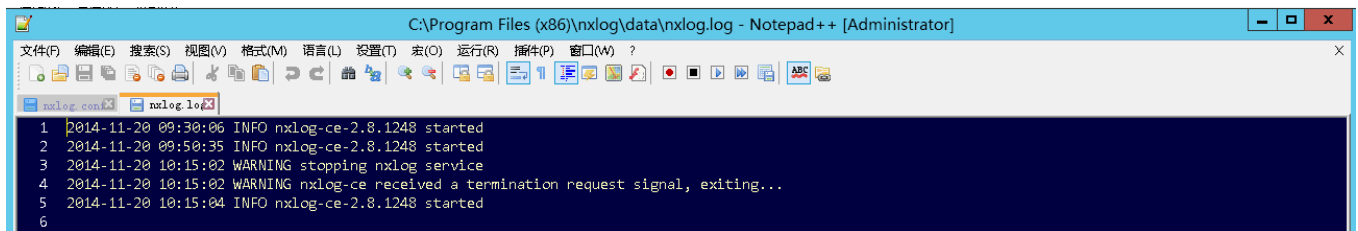
[Windows PowerShell]输入 :

```
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。



```
C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++ [Administrator]
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(T) 宏(O) 运行(R) 插件(P) 窗口(W) ?
nxlog.conf nxlog.log
1 2014-11-20 09:30:06 INFO nxlog-ce-2.8.1248 started
2 2014-11-20 09:50:35 INFO nxlog-ce-2.8.1248 started
3 2014-11-20 10:15:02 WARNING stopping nxlog service
4 2014-11-20 10:15:02 WARNING nxlog-ce received a termination request signal, exiting...
5 2014-11-20 10:15:04 INFO nxlog-ce-2.8.1248 started
6
```

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。

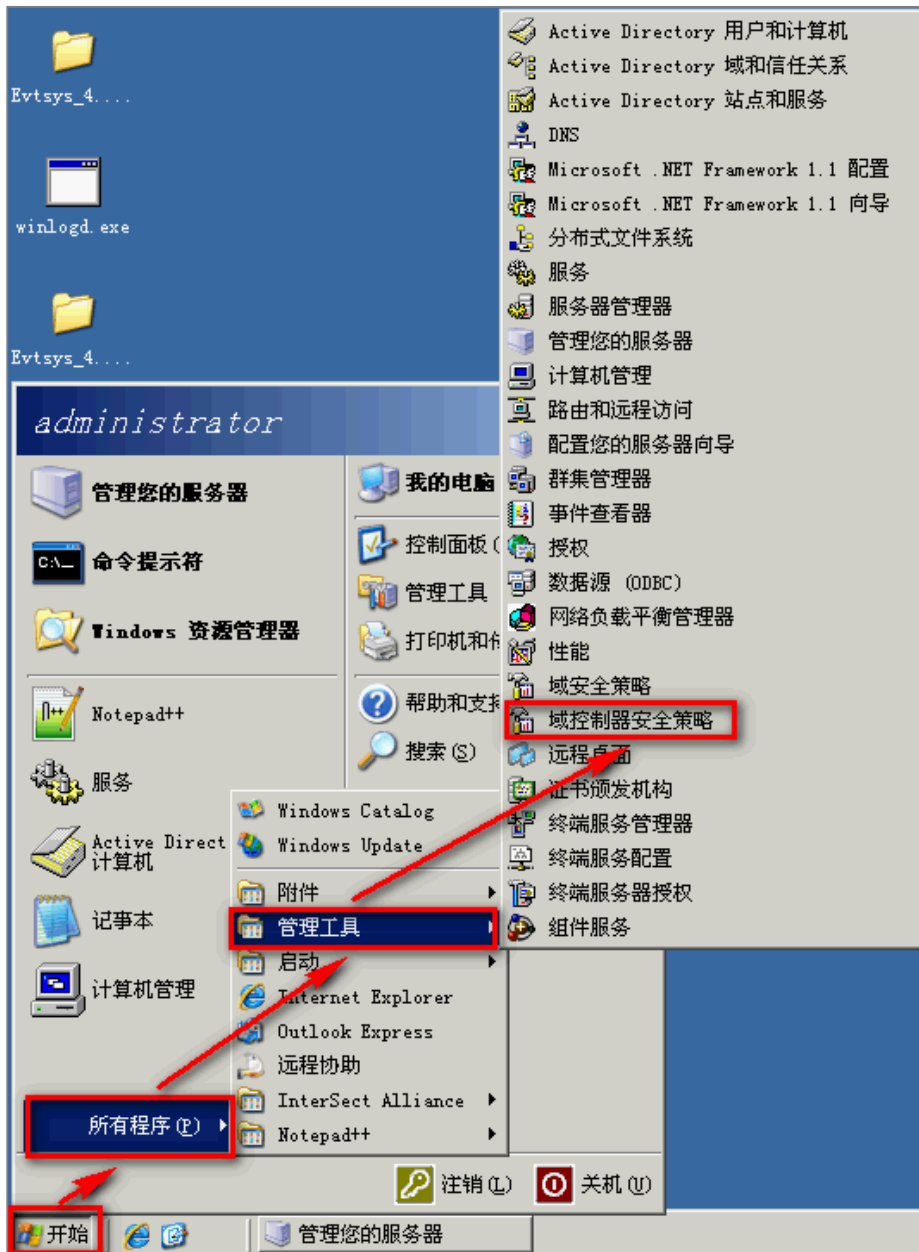
Windows 2003 AD Server 登录注销的审核策略和目录分享的审核策略，默认是关闭的。

请记住安装 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

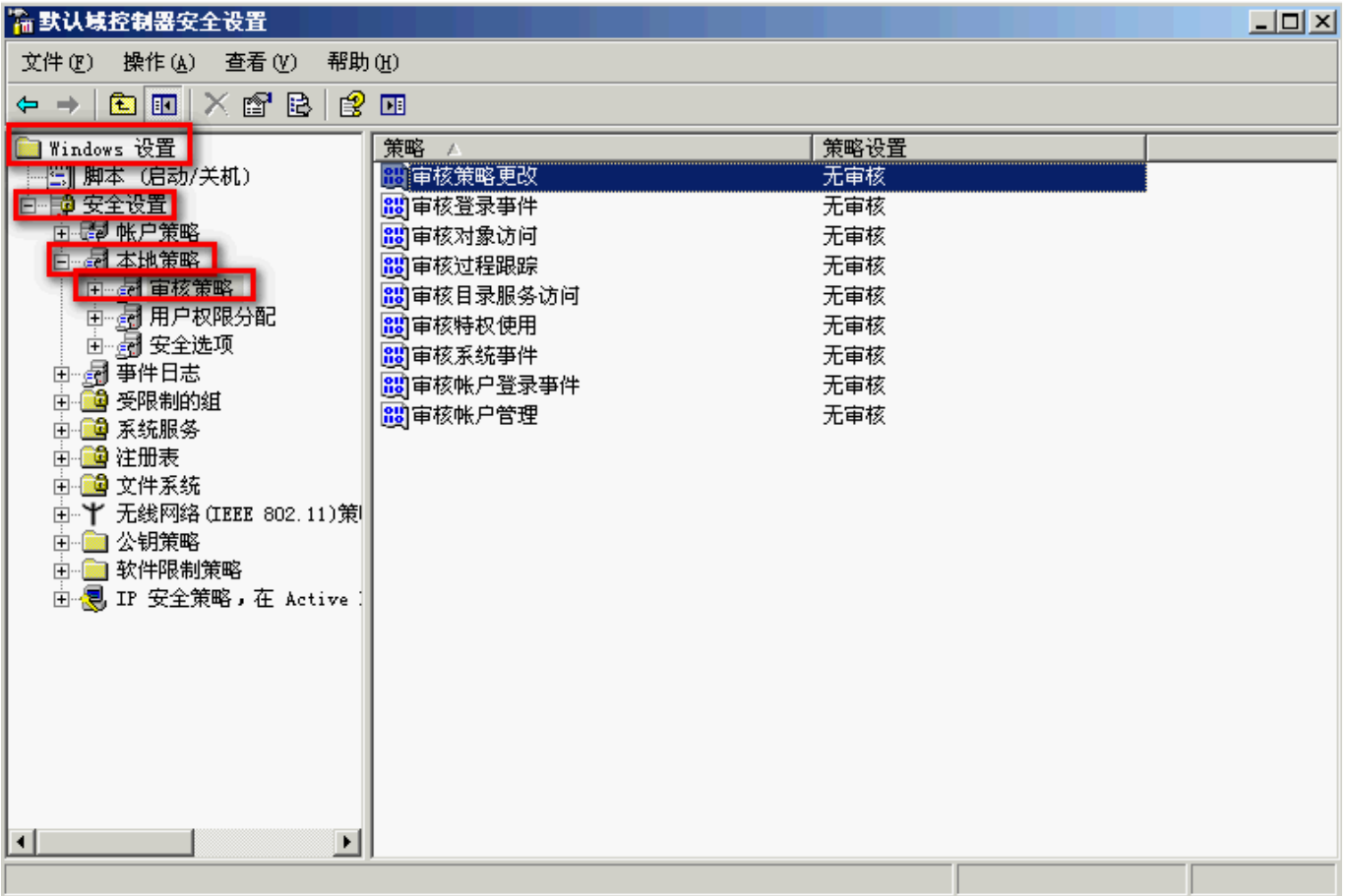
设置步骤如下：

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。

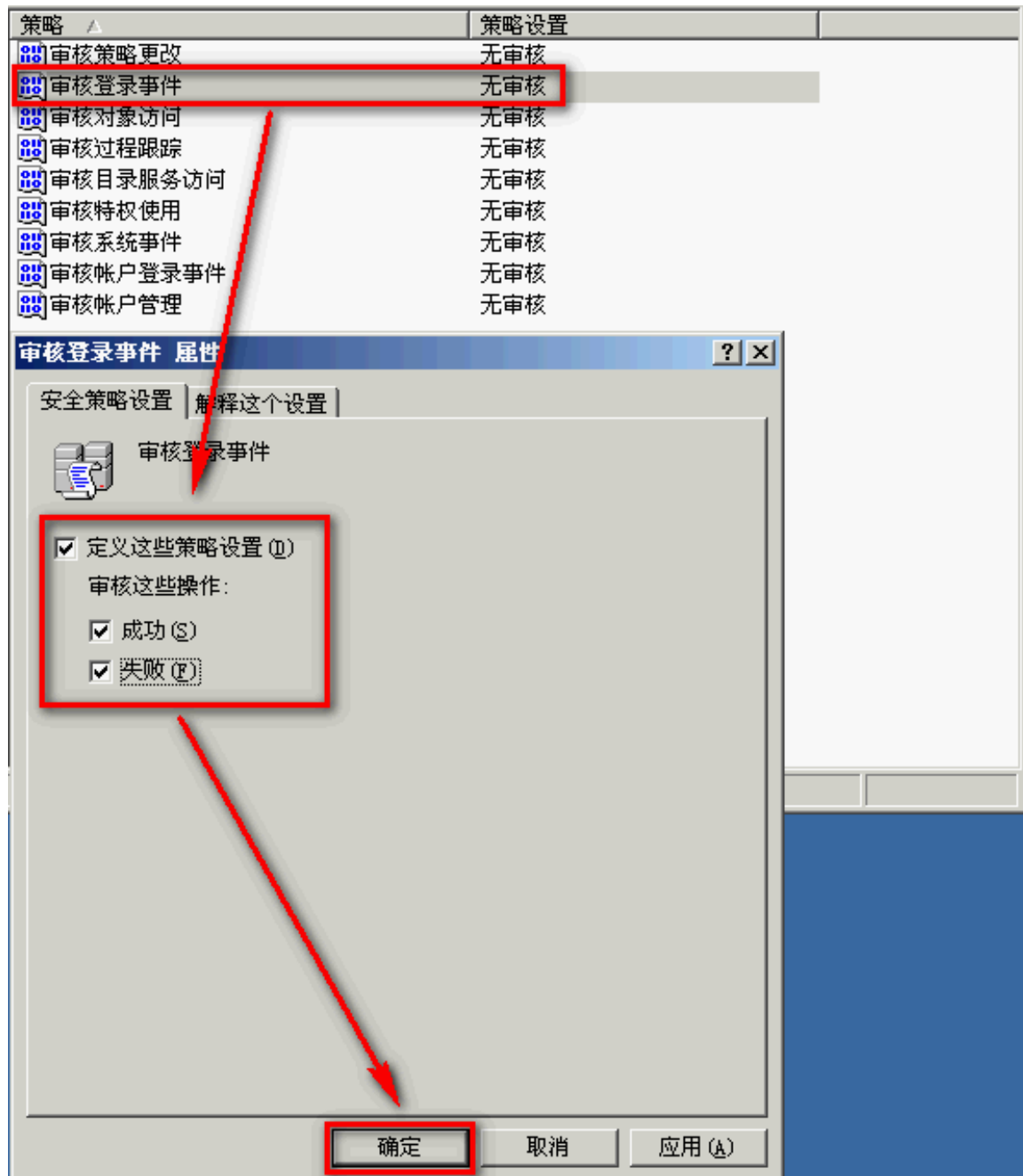
2. 点选 [Windows 设置 / 安全设置 / 本机策略 / 审核策略]。



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]。



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]。



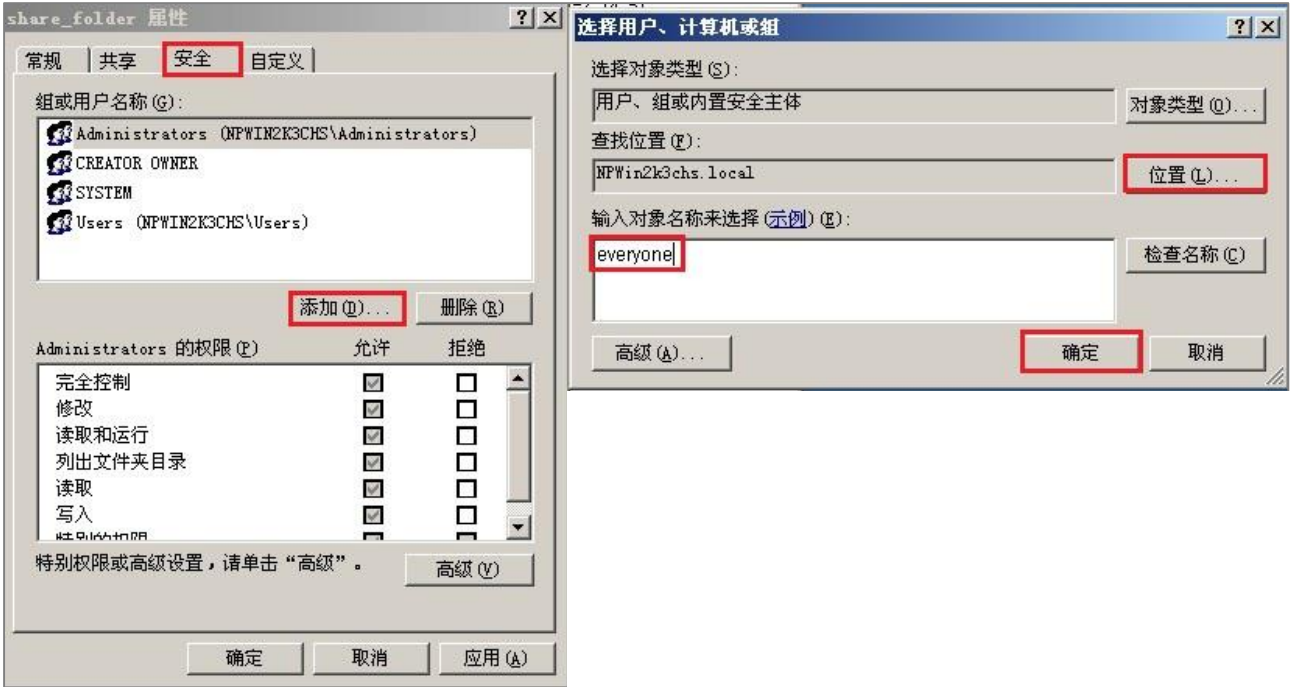
4. 设置用户权力：

- (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]。



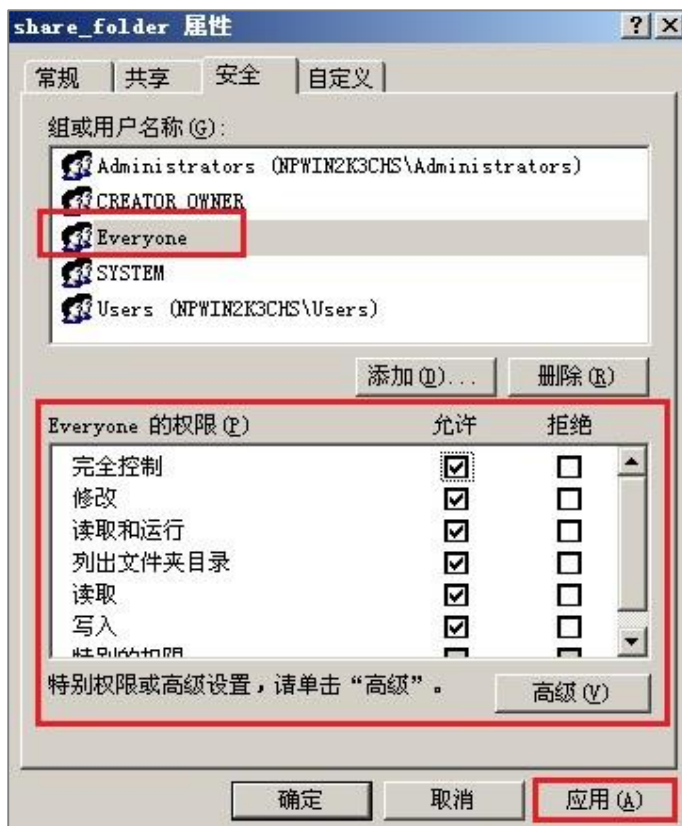
5. 安全性设置：

- (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]。



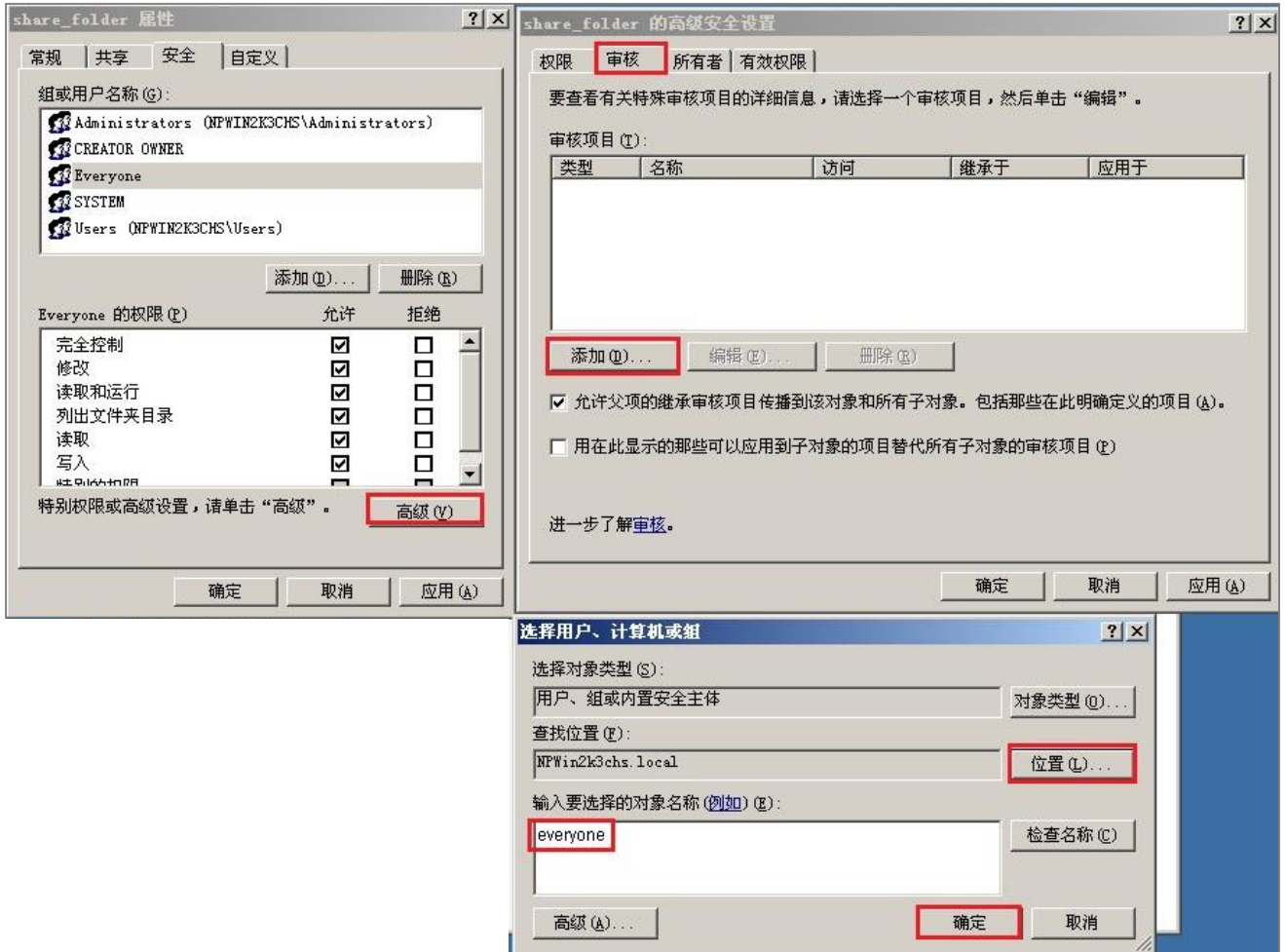
6. 设置用户权力：

- (1) 点选用户账号。
- (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]。



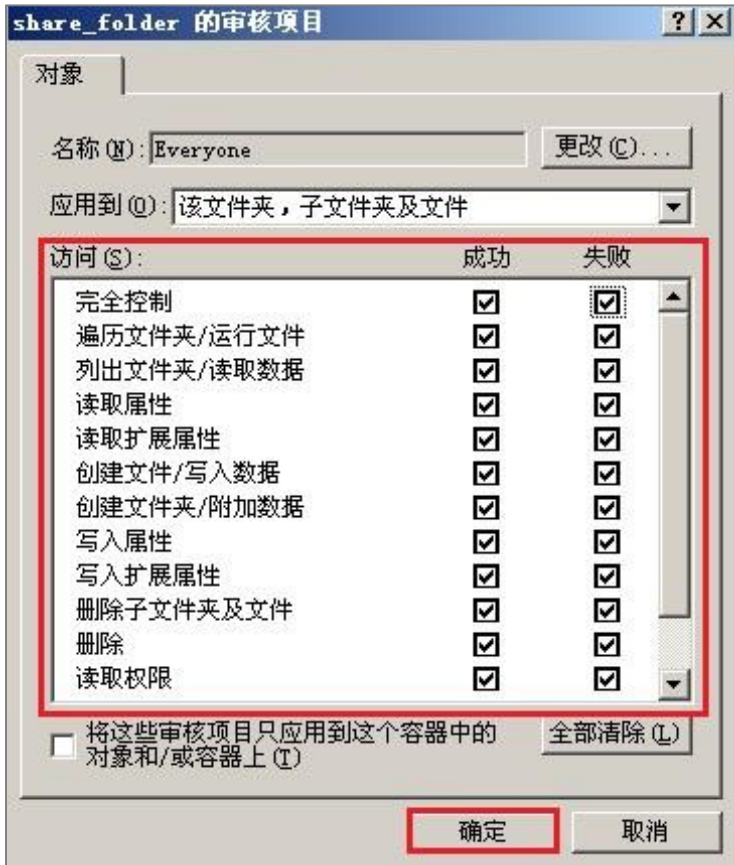
7. 高级安全设置：

- (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]。

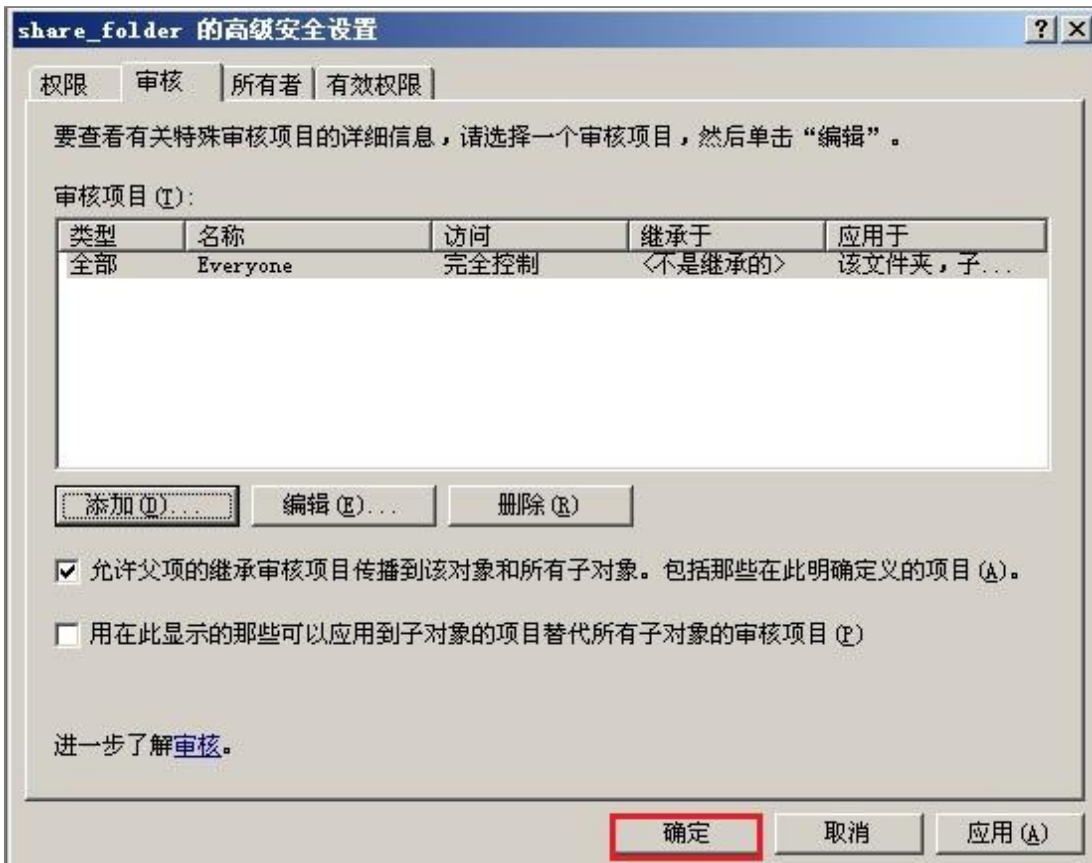


8. 审核项目设置：

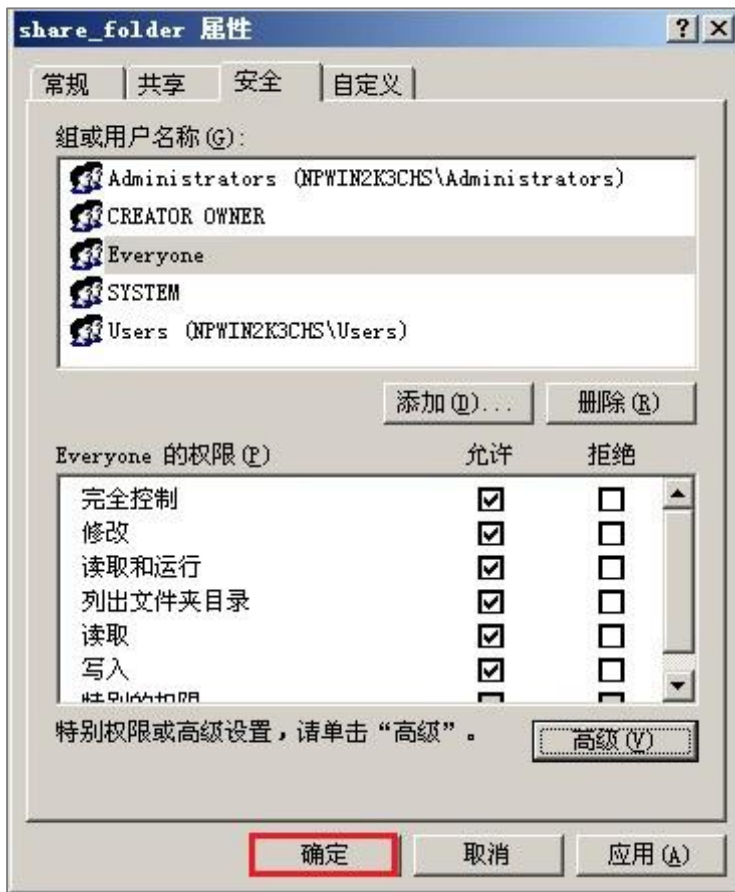
勾选所有审核项目的 [成功] 及 [失败]，设置完成后按 [确定]。



9. 在高级安全设置完成后，点选 [确定]。



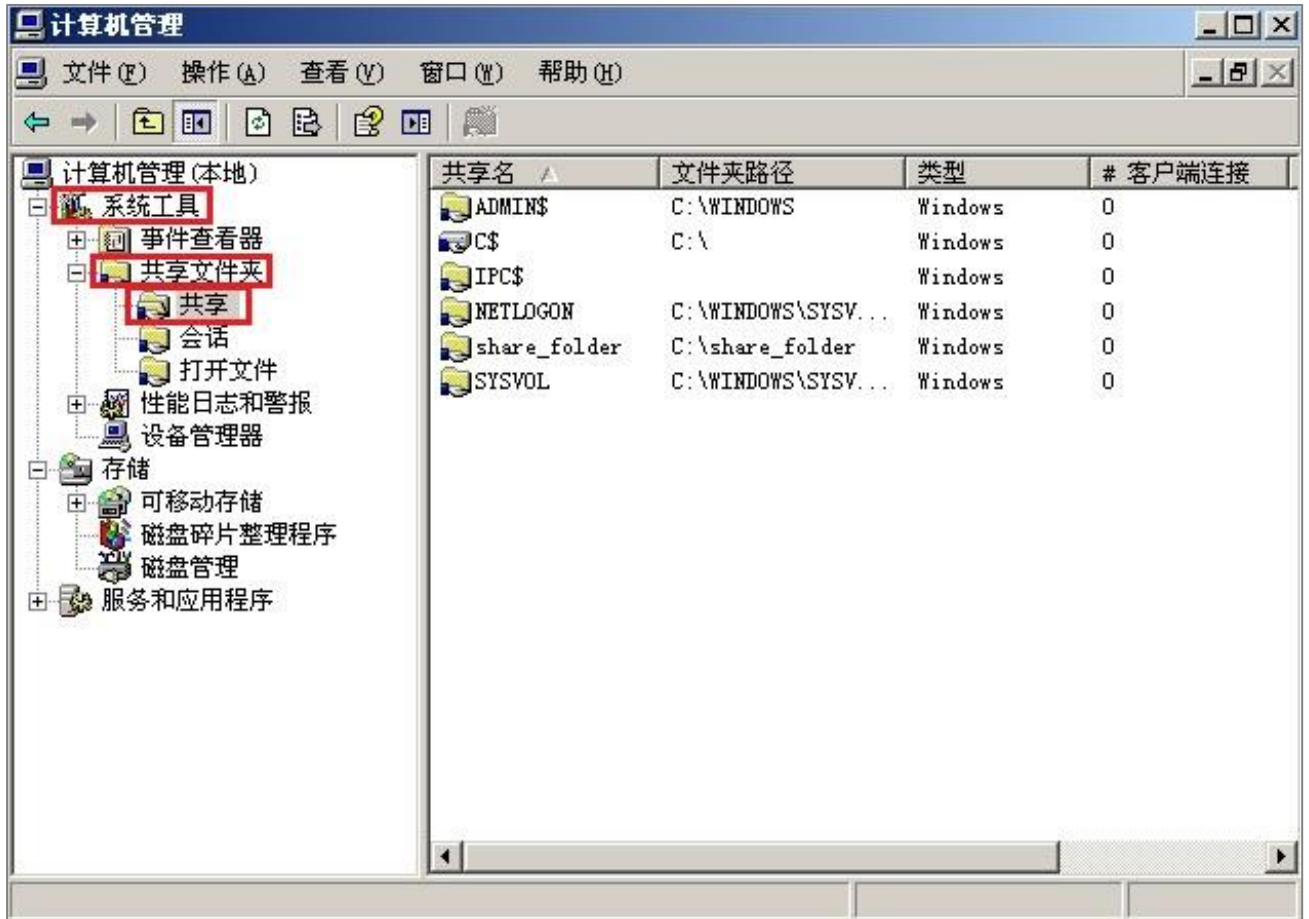
10. 在分享文件夹设置完成后，点选 [确定]。



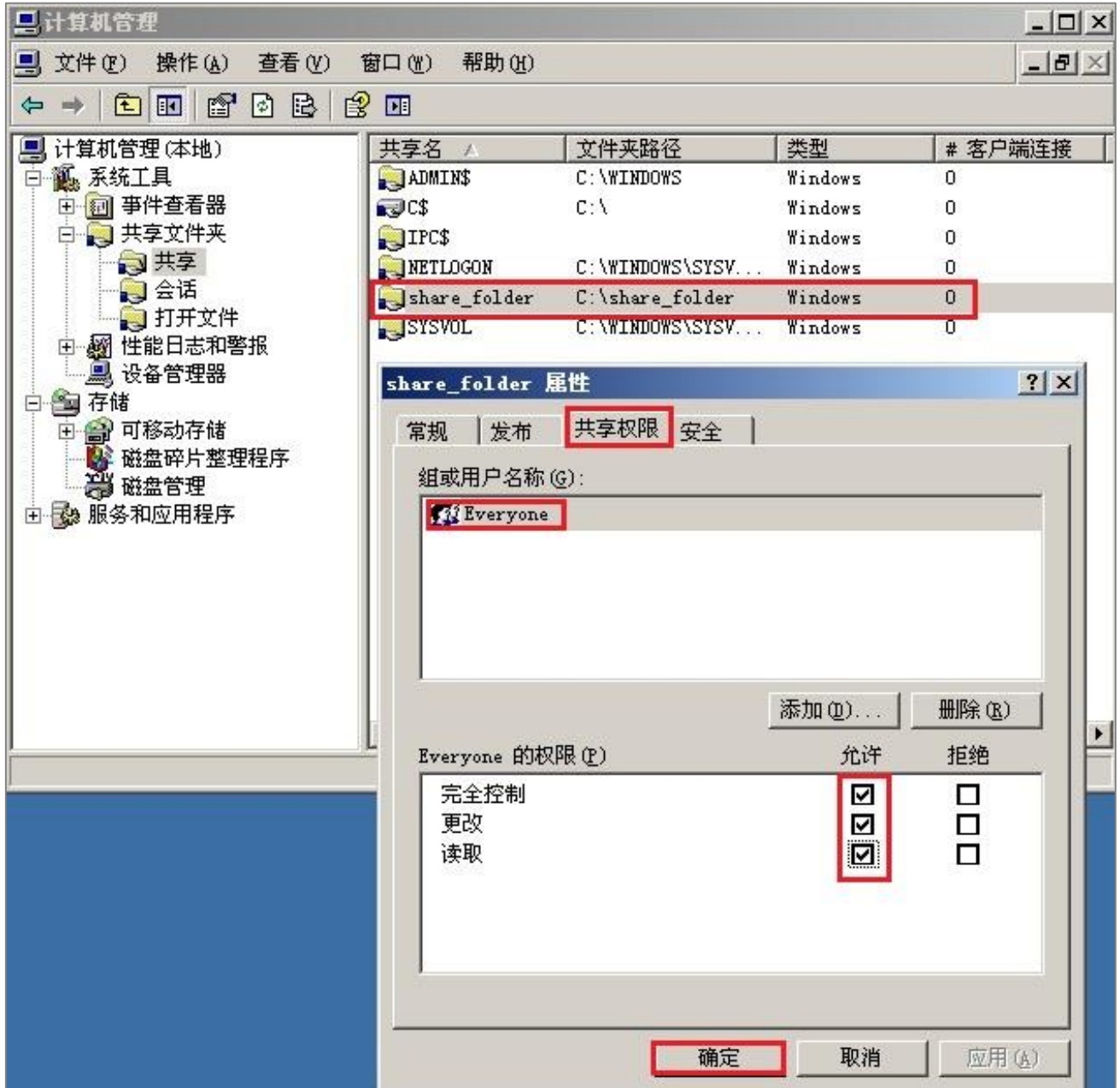
11. 点选 [开始 / 所有程序 / 管理工具 / 计算机管理]。



12. 点选 [系统工具 / 共享文件夹 / 共享]。



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]。



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。

请记住安装 NXLOG，详细请参阅第一章节。

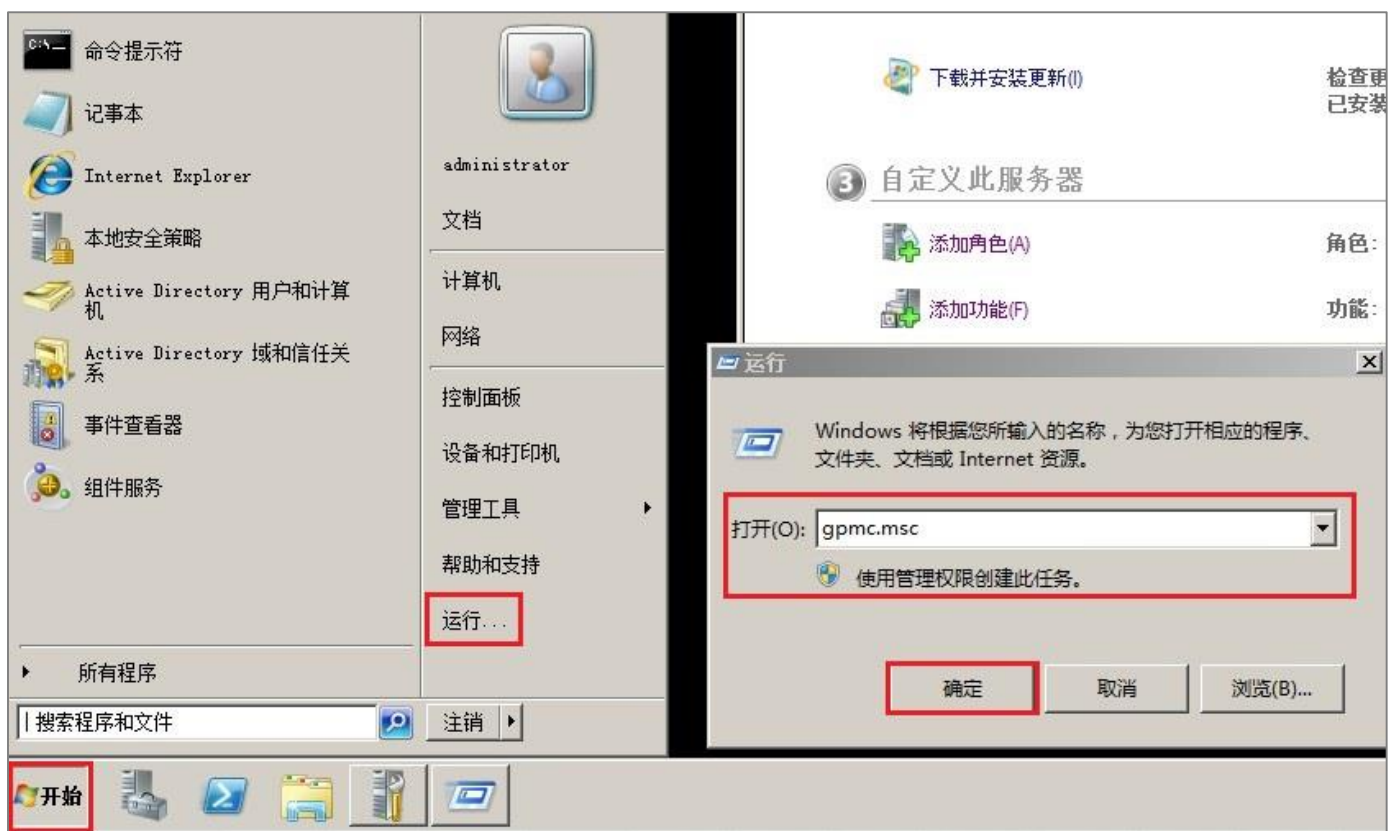
3.1 设置域用户登录注销的审核策略

设置步骤如下：

- 1. 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]。



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



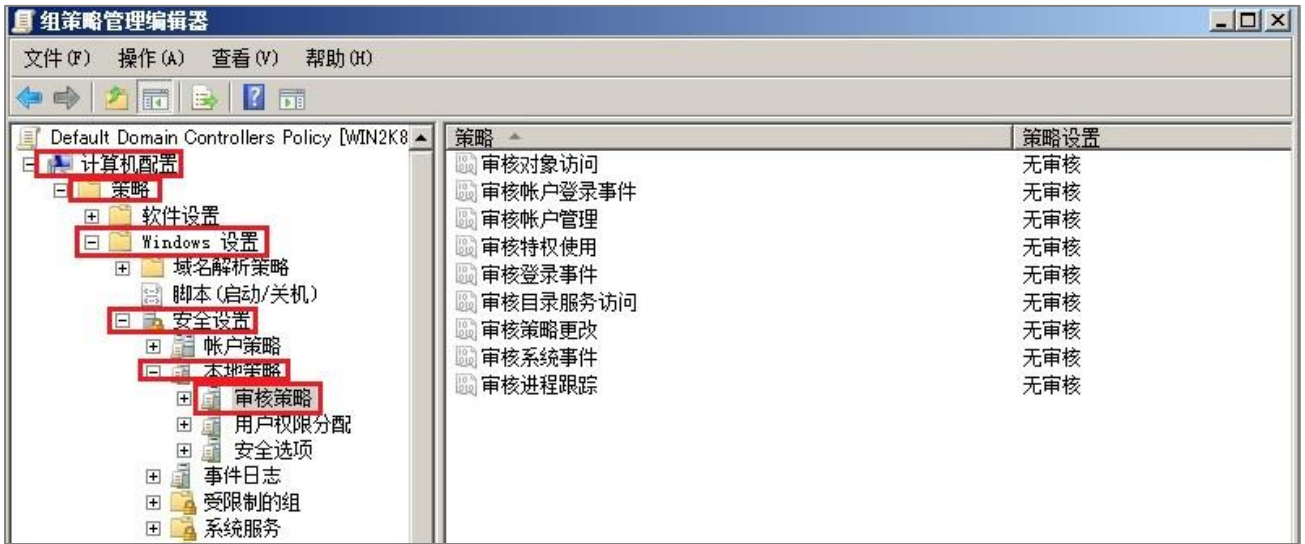
注 :此步骤展开域(Domain) ,出现 [默认域安全策略(Default Domain Policy)] ;展开域控制站(Domain Controllers) , 出现 [默认域控制站安全策略(Default Domain Controllers Policy)]。

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

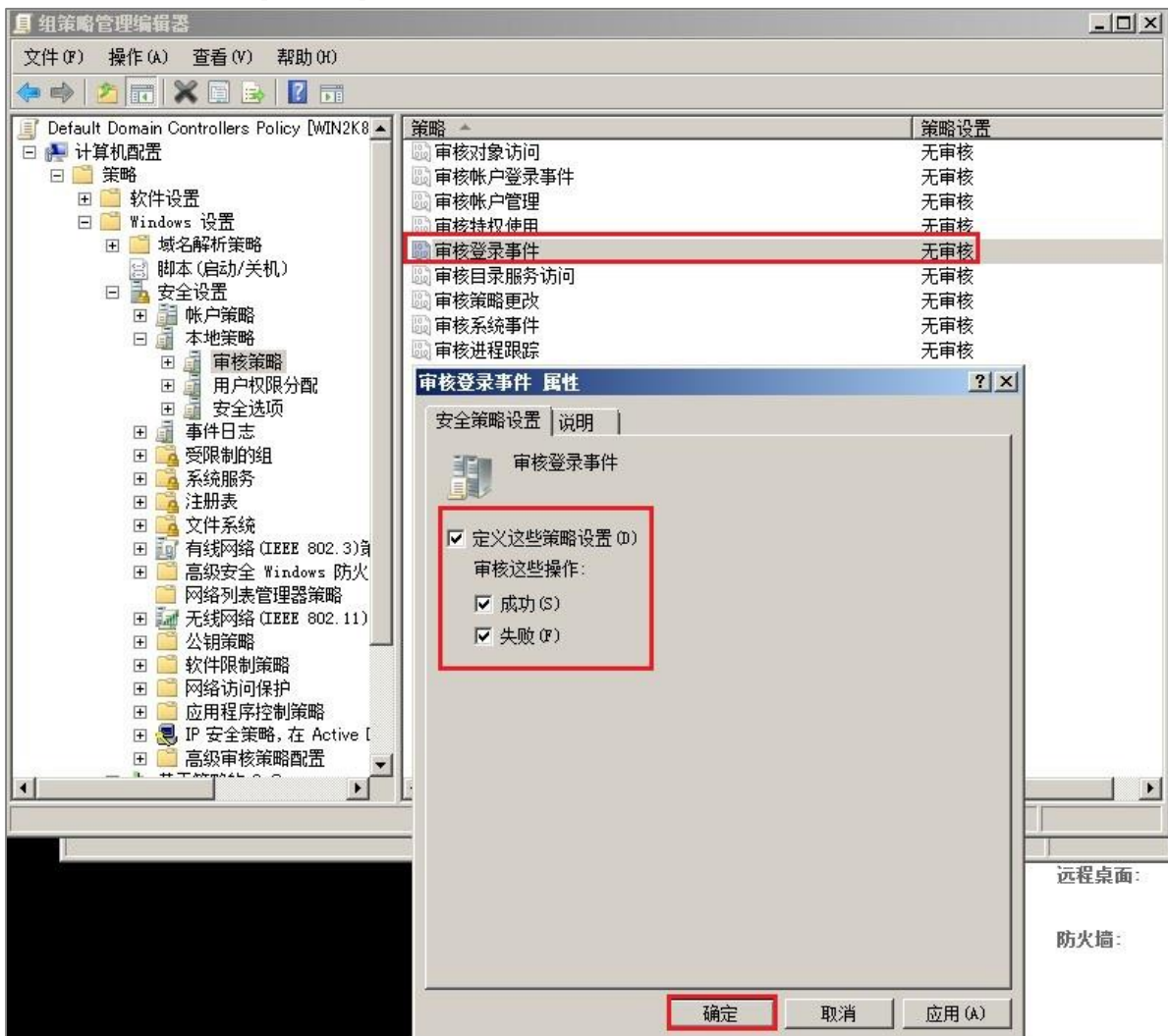
4. 点选 [计算机配置/策略/Windows 设置/安全设置/本地策略/审核策略]。



5. 定义下列的策略设置值：

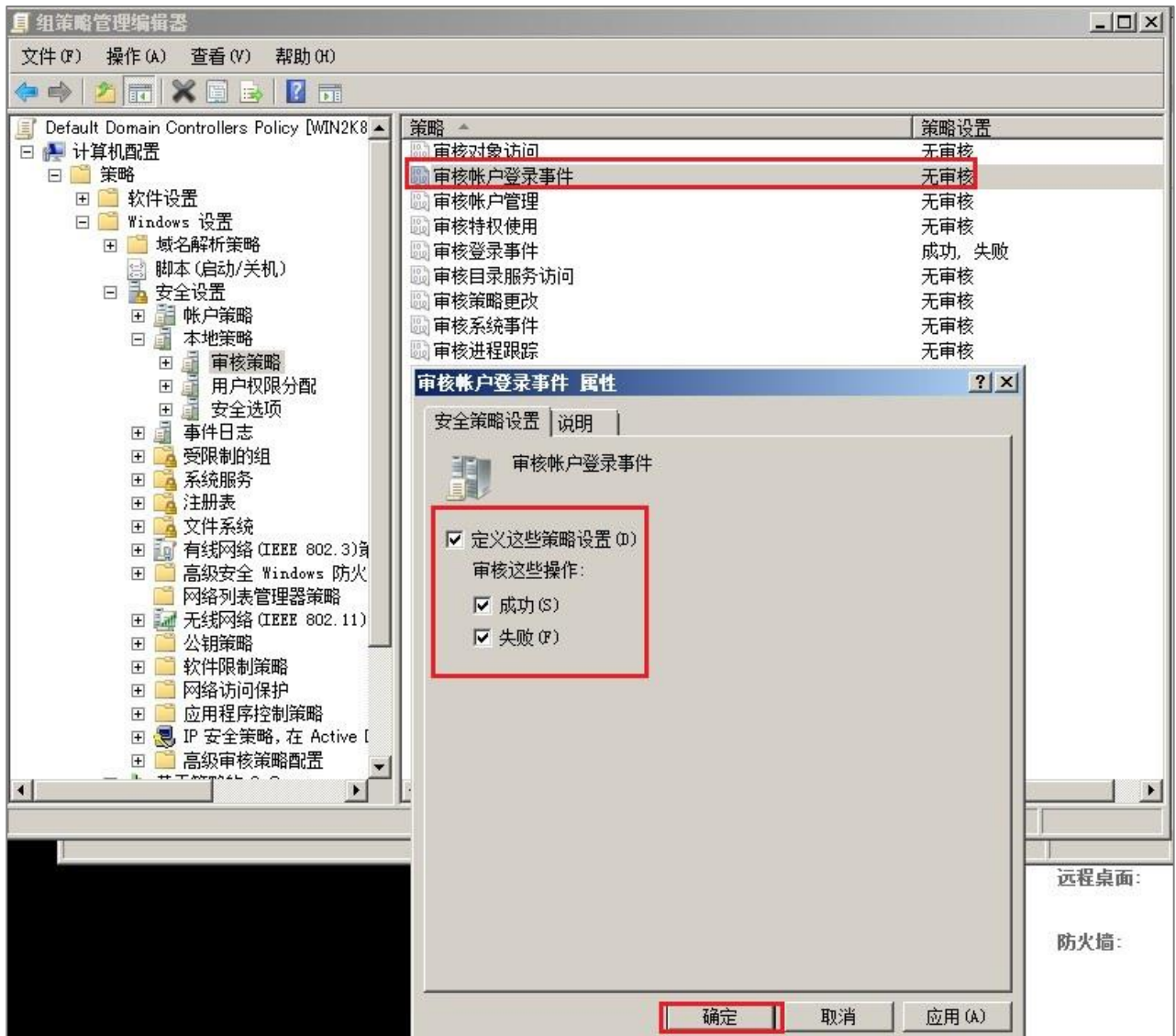
(1) 审核登录事件：

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]，设置完成后按 [确定]。



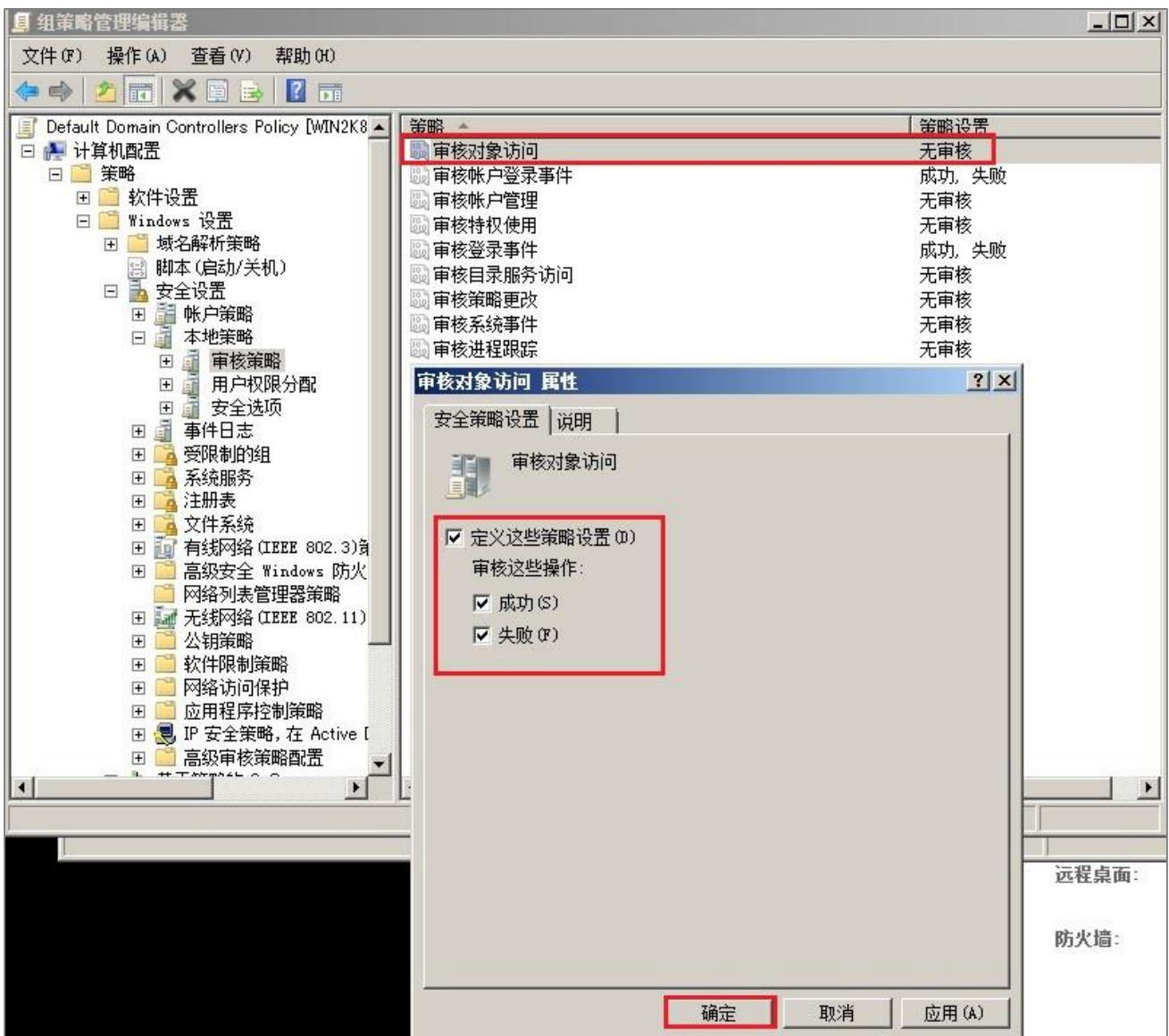
(2) 审核账户登录事件：

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]。



(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：

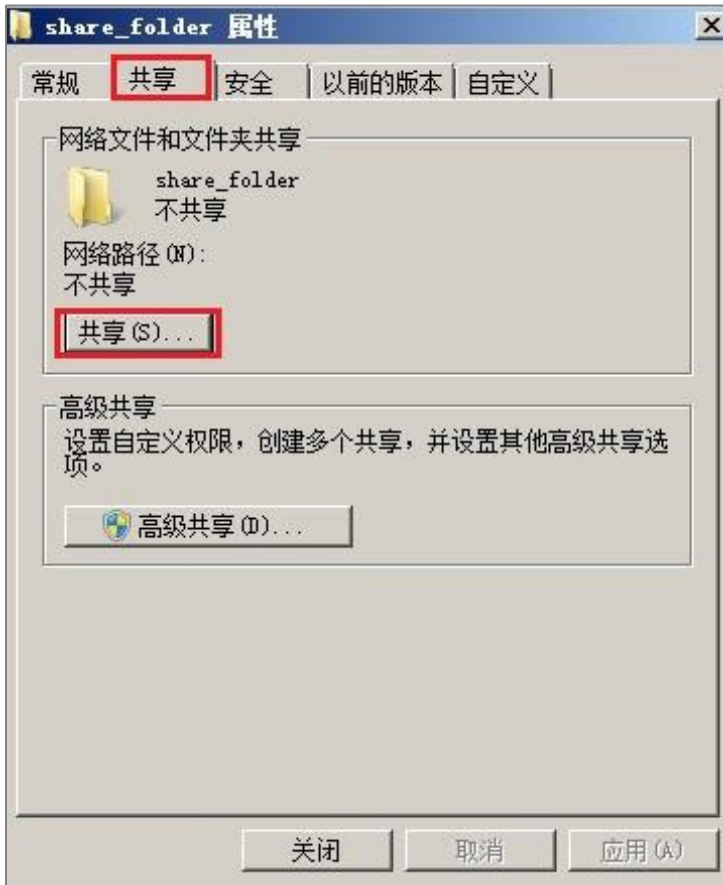
双击 [审核账户管理]，勾选 [定义这些策略设置]，再勾选 [成功] 及 [失败]，设置完成后按 [确定]。

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)。

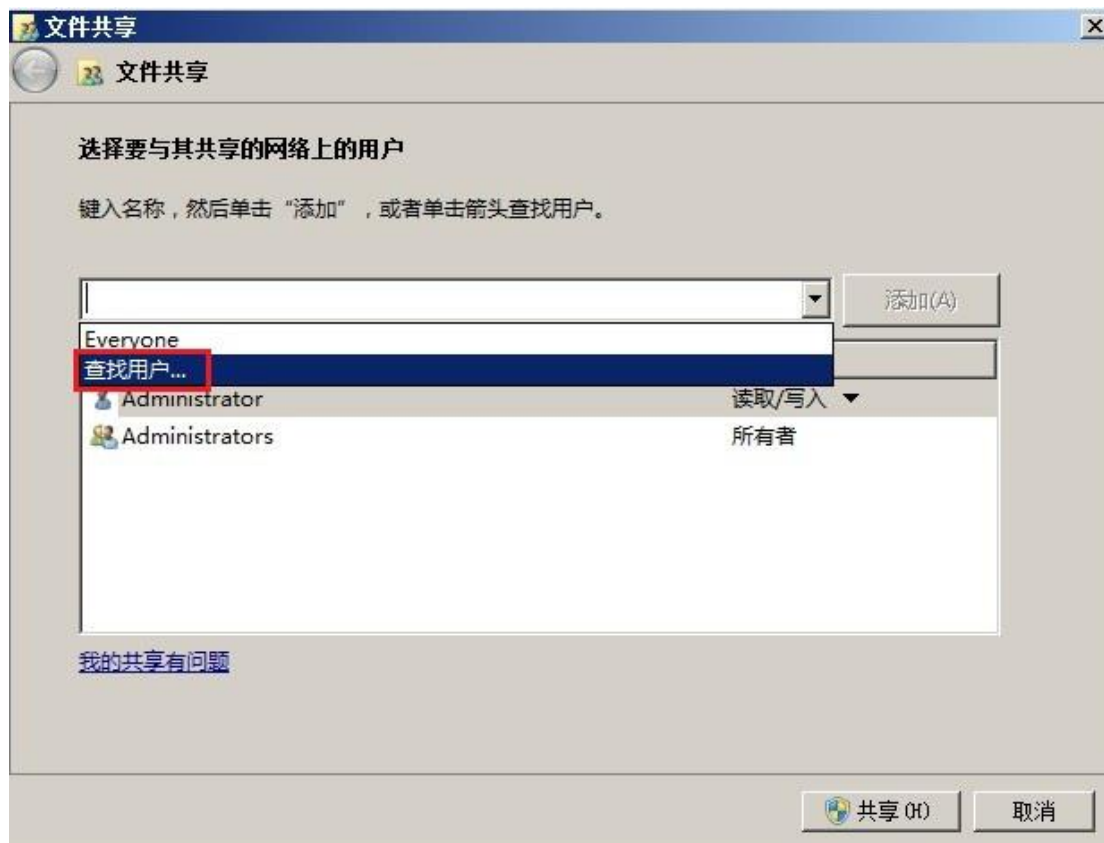
3.2 设置共享文件夹权限与审核策略

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]。



3. 在文件共享设置中，点下拉选单至 [查找用户]。



4. 用户设置：

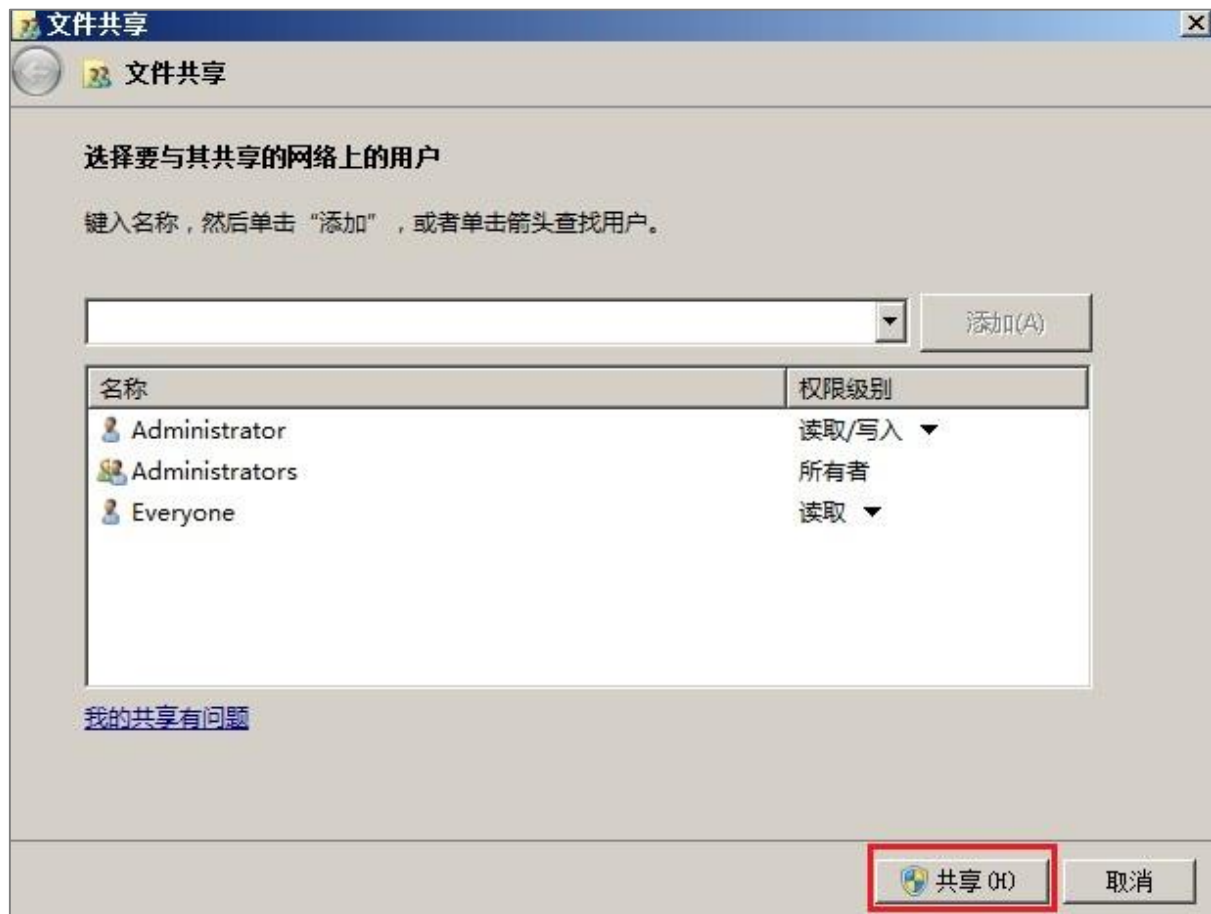
(1) 点选 [位置]，选择域。

(2) 输入域用户账号。本例输入 Everyone 审核所有用户。

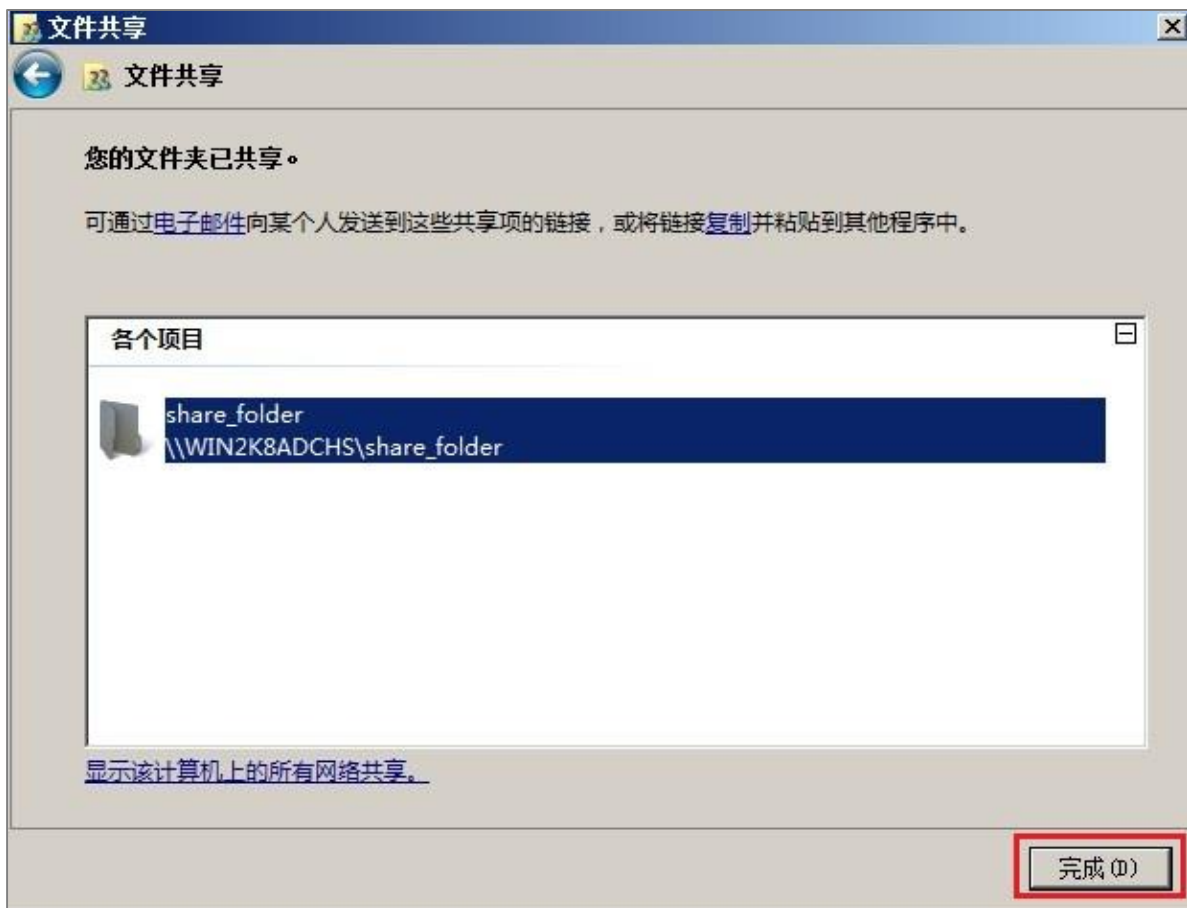
(3) 设置完成后按 [确定]。



5. 点选 [共享]。

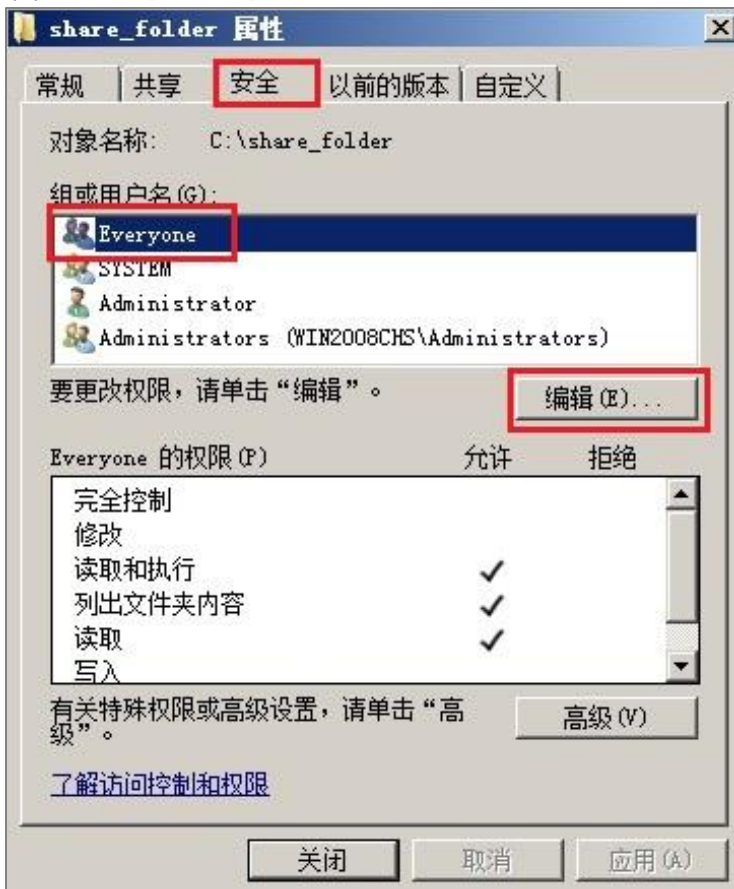


6. 等待共享设置完成后，再按 [完成]。



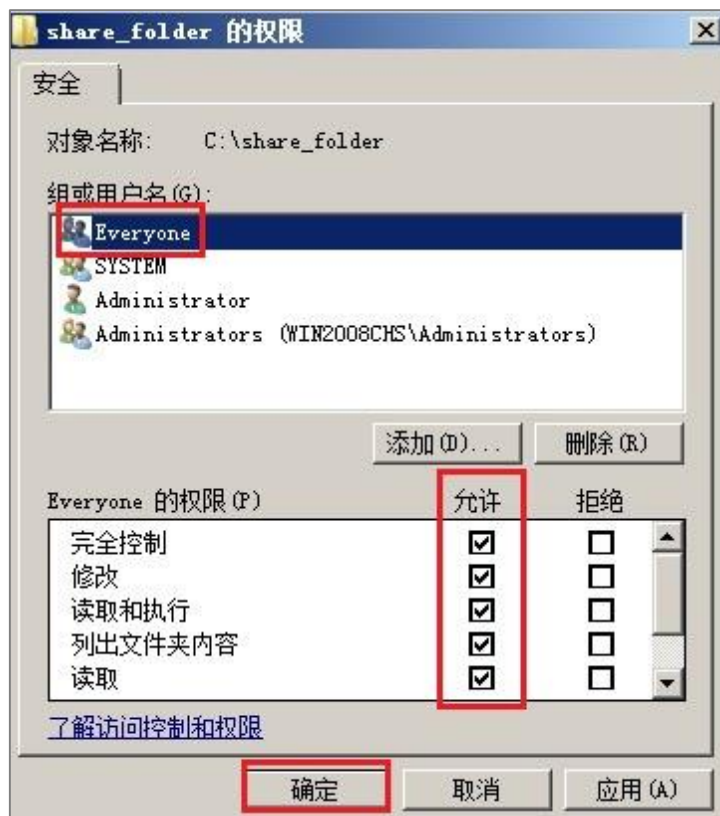
7. 安全设置：

- (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]。



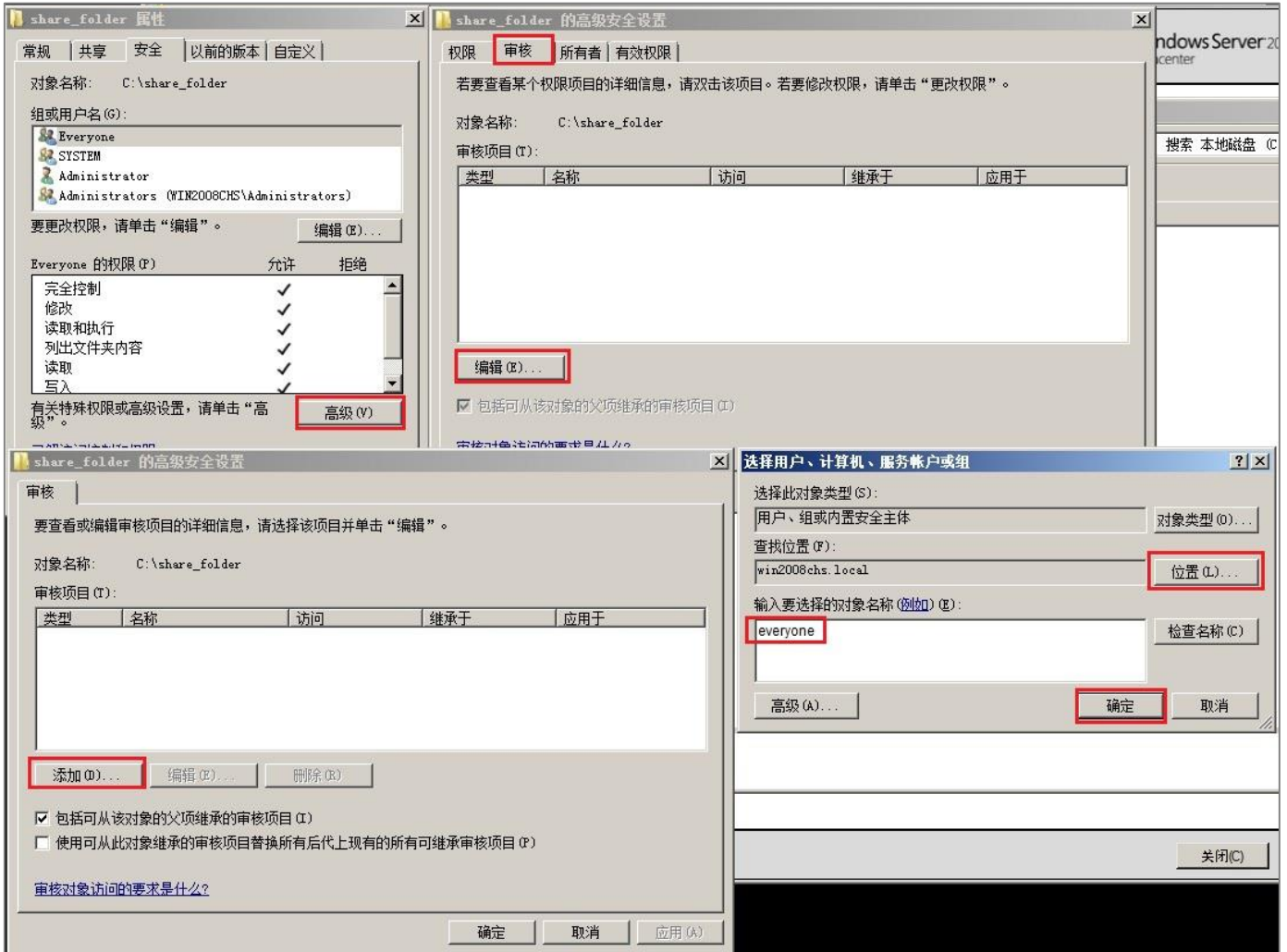
8. 设置用户权力：

- (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]。



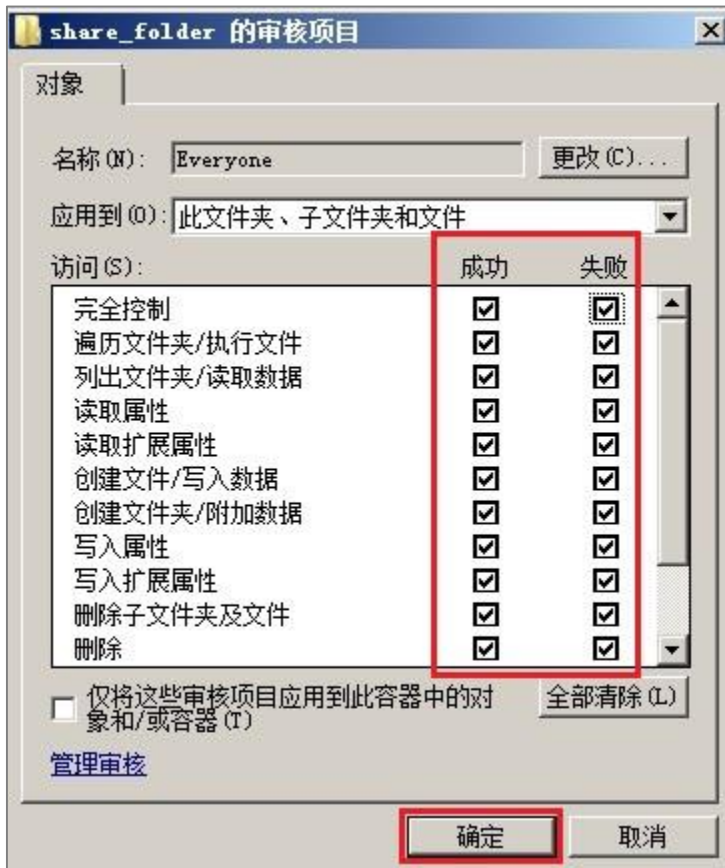
9. 高级安全设置：

- (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]。



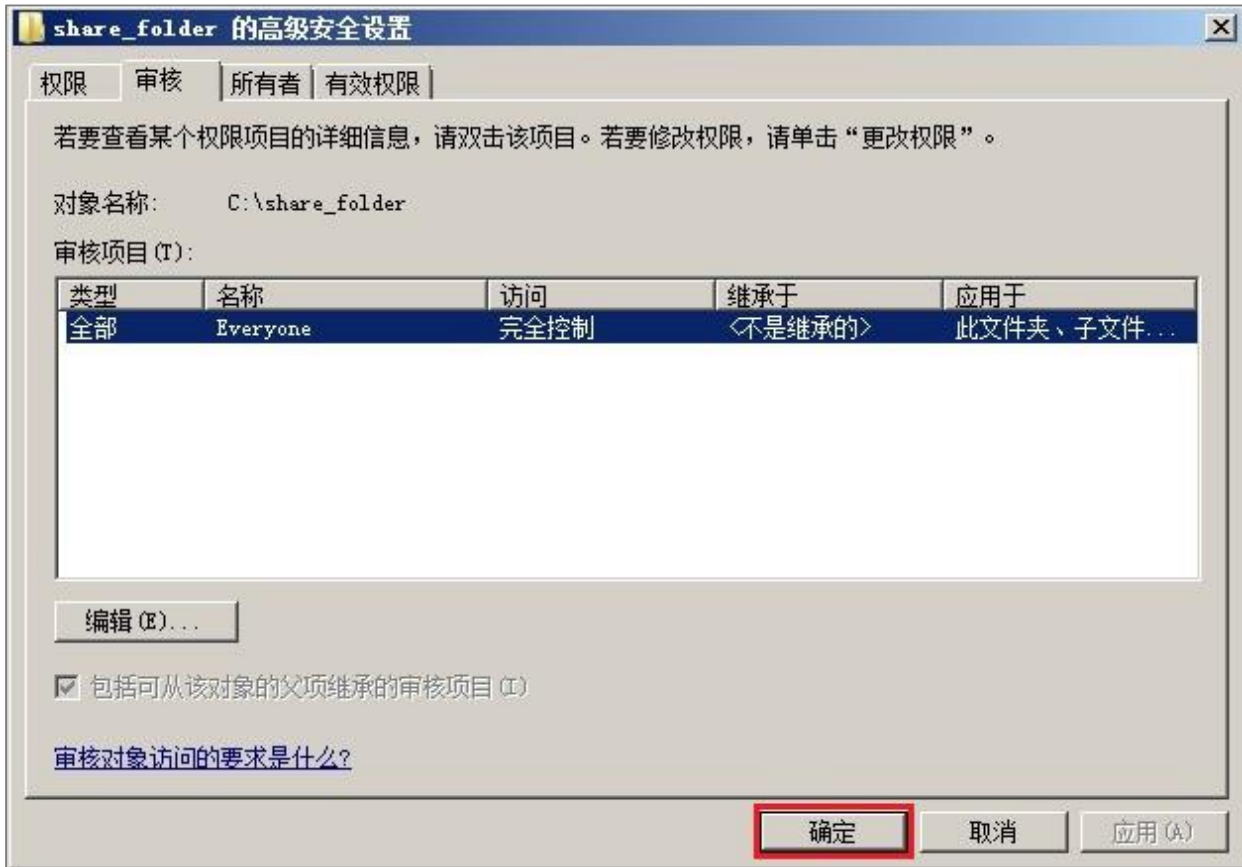
10. 审核项目设置：

勾选所有审核项目的 [成功] 及 [失败]，设置完成后按 [确定]。

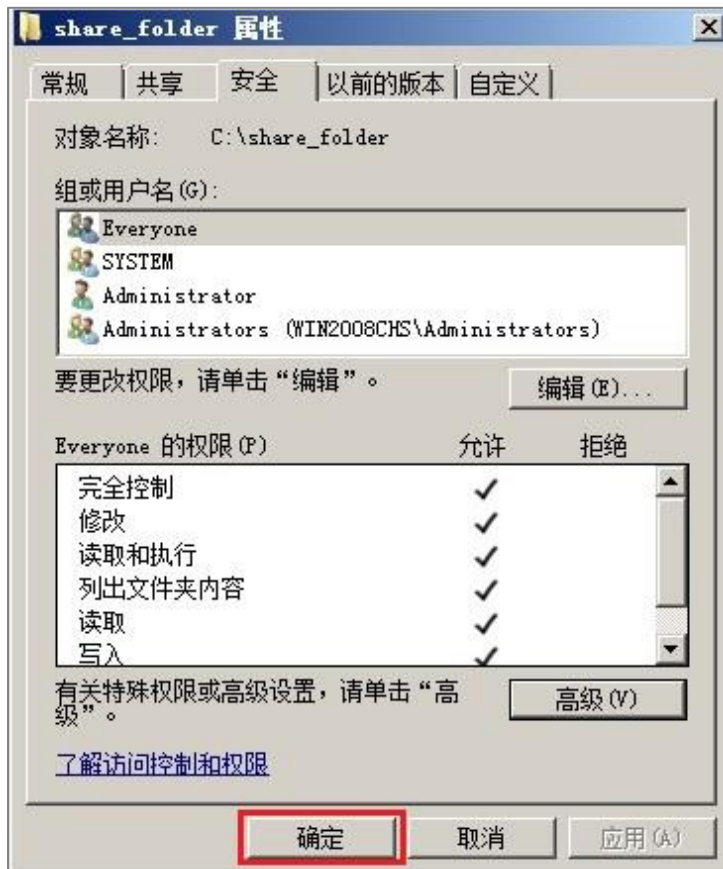


11. 在高级安全设置配置完成后，点选 [确定]。

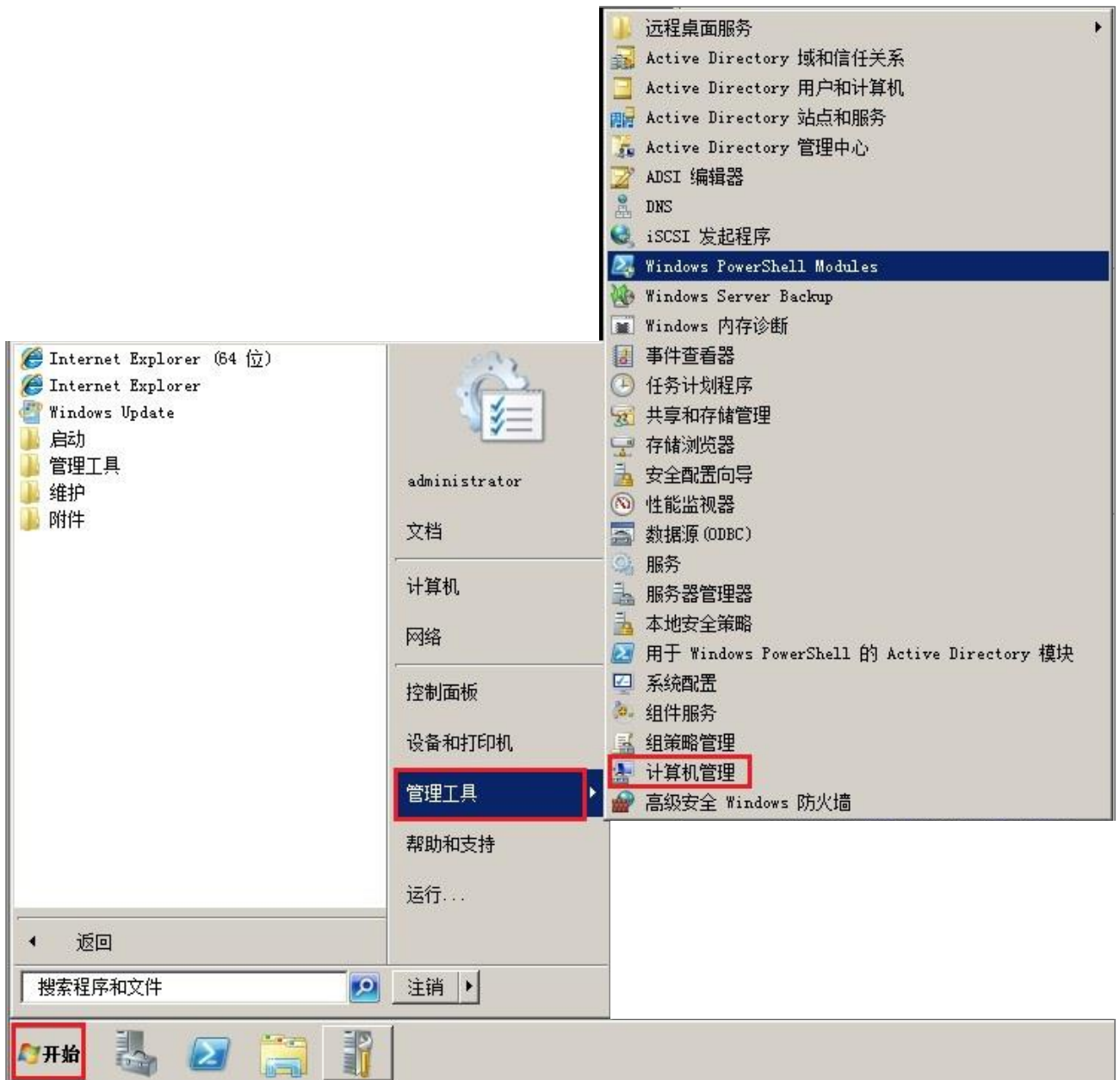




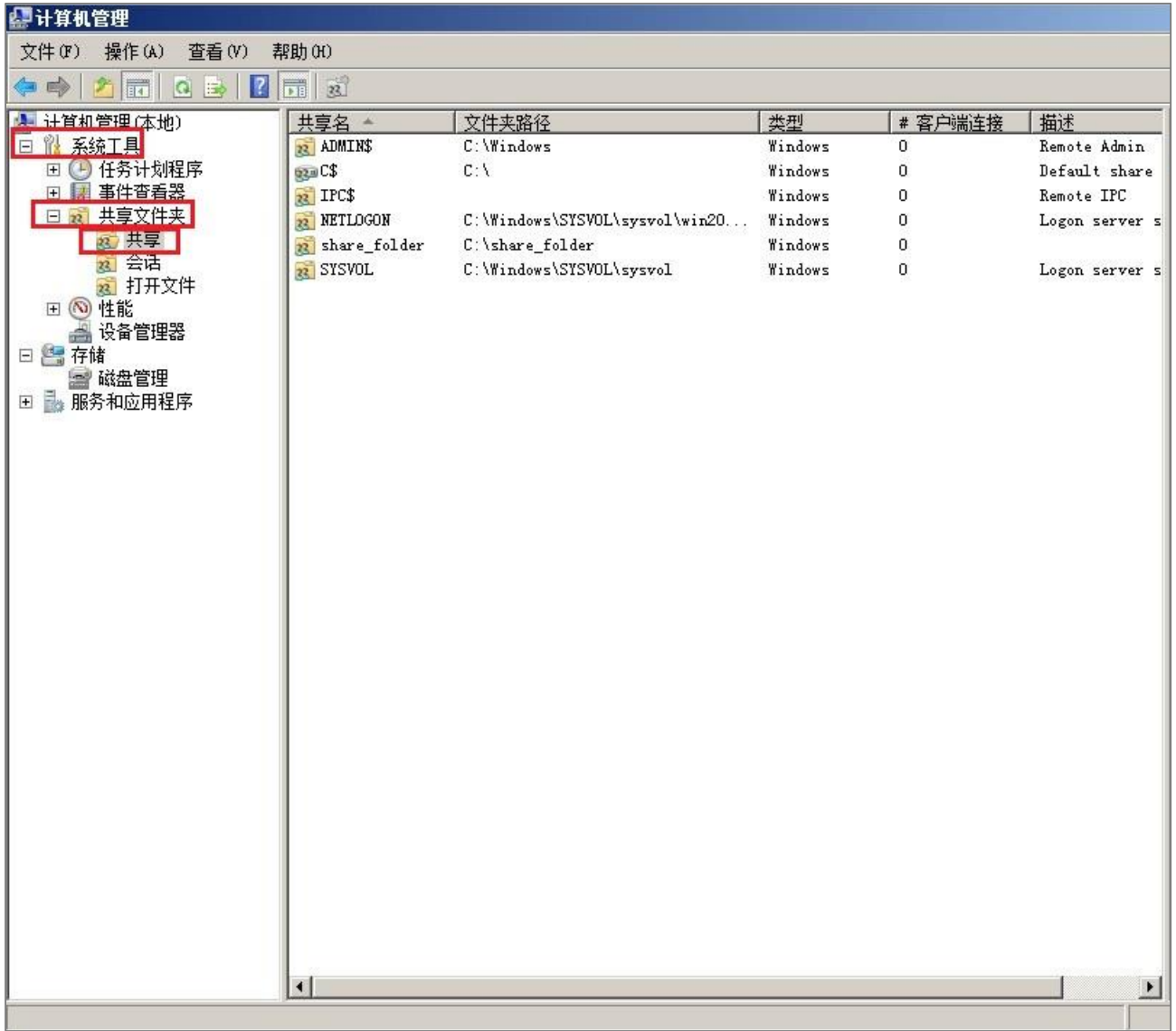
12. 在分享文件夹设置完成后，点选 [确定]。



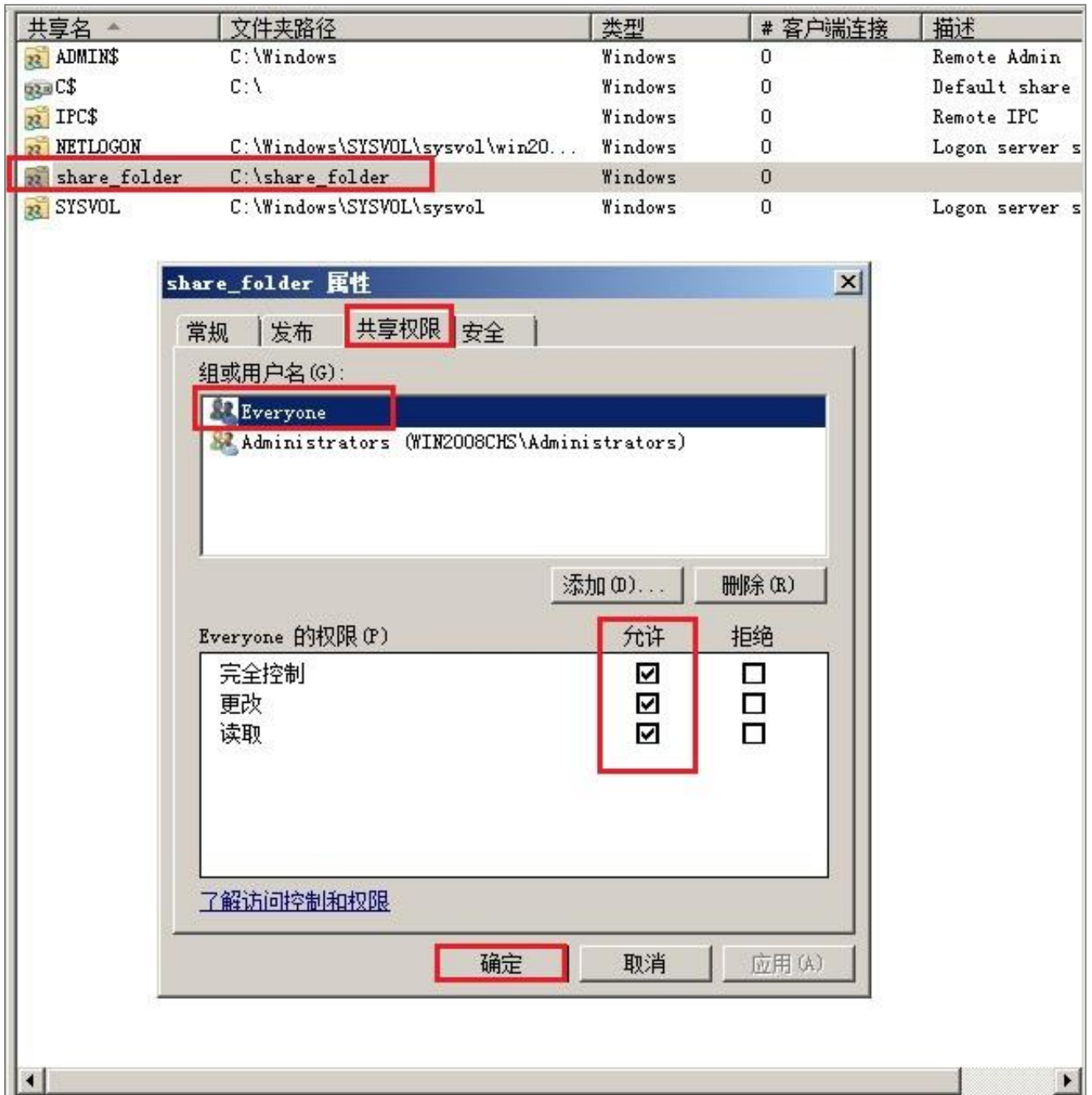
13. 点选 [开始/管理工具/计算机管理]。



14. 点选 [系统工具/共享文件夹/共享]。



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]。



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。

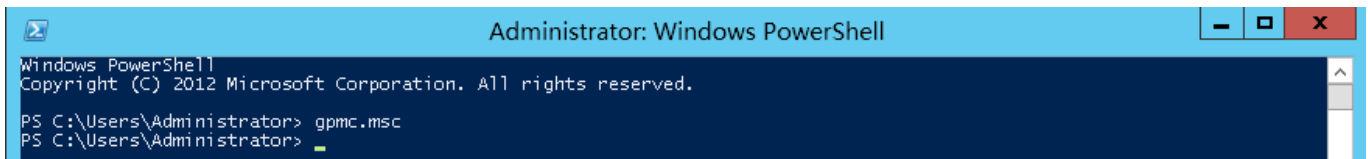
请记住安装 NXLOG ，详细请参阅第一章。

4.1 设置域用户登录注销的审核策略

配置步骤如下：

1. 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]。

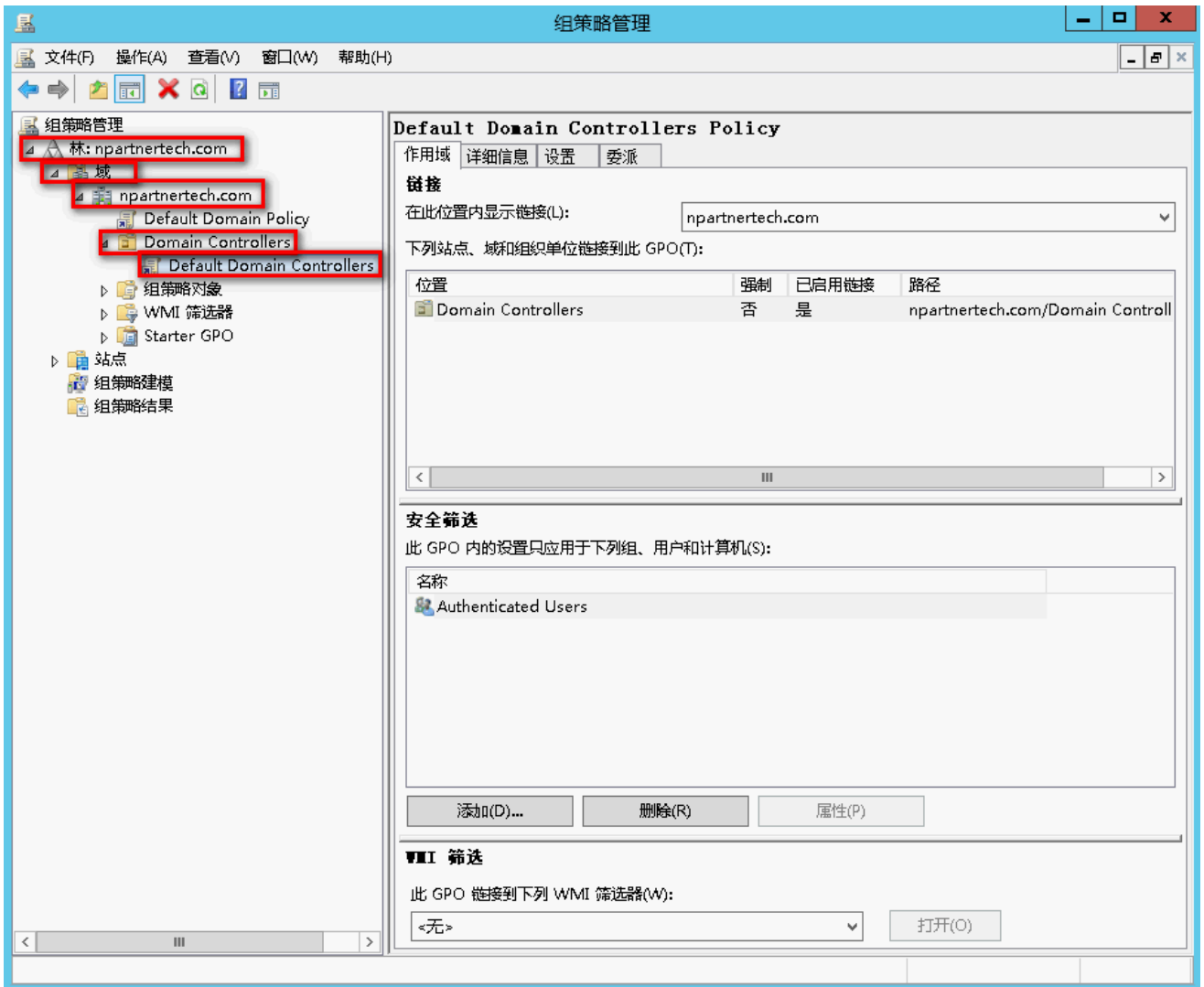
输入：**gpmmc.msc** ，完成后按 [Enter]，开启[组策略管理]。



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

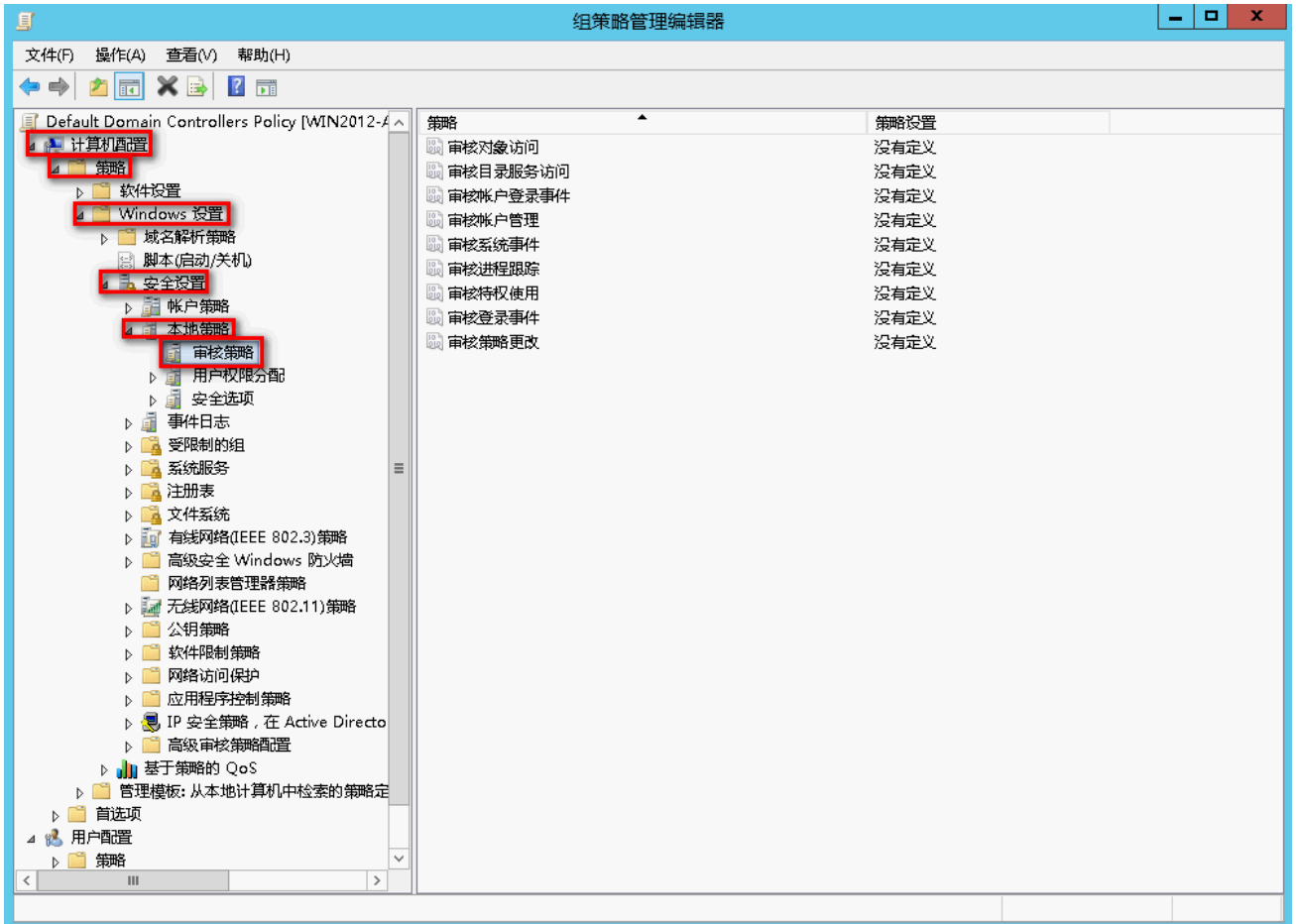
PS C:\Users\Administrator> gpmmc.msc
PS C:\Users\Administrator> _
```

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]。



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)]。

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]。

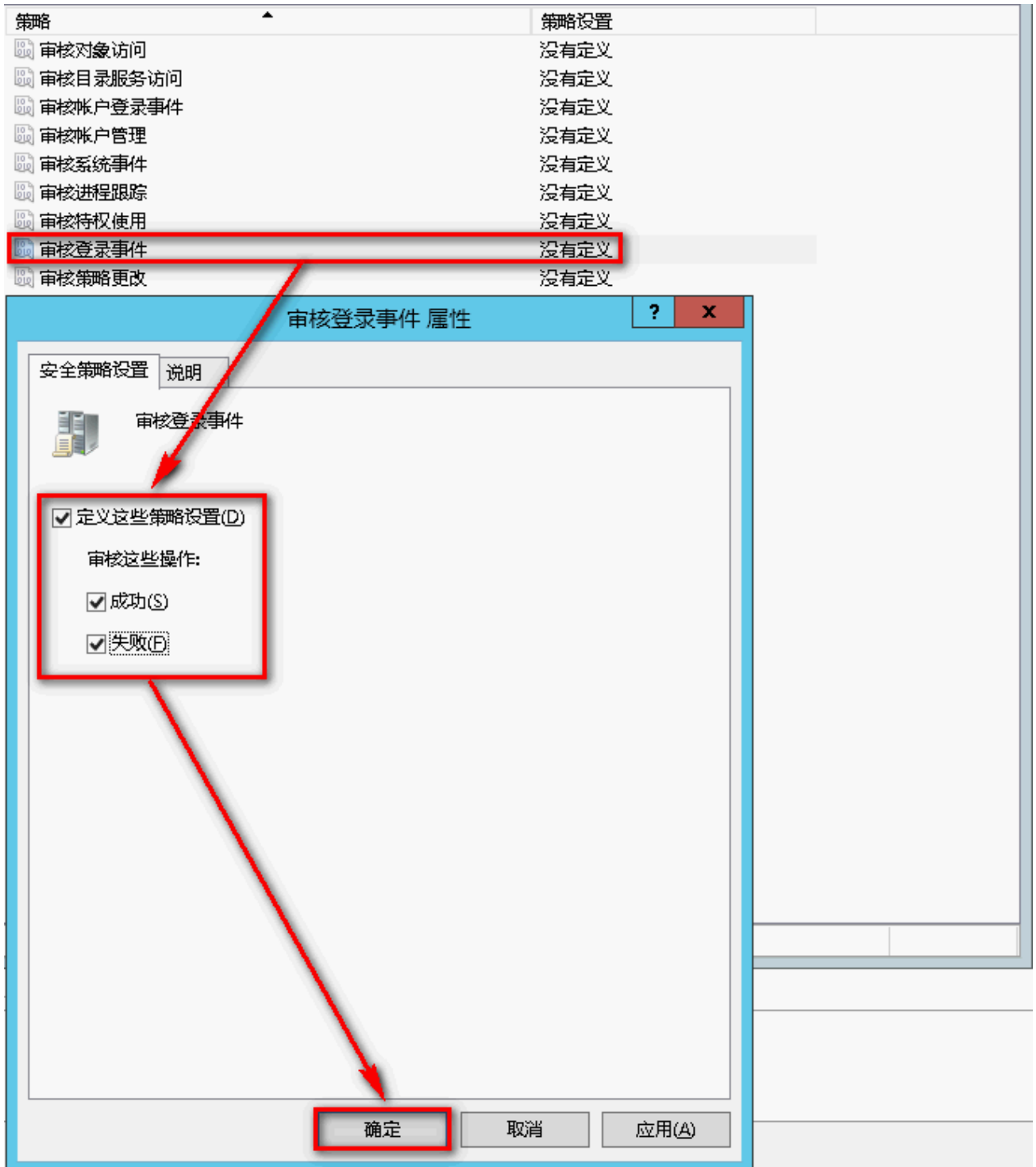


注：Default Domain Policy 为设定域上所有对象 (Object)，而 Default Domain Controllers Policy 为设定所有域控置站(Domain Controllers/Windows AD)。建议两者安全审核策略设定一致。

5. 定义下列的策略设定值：

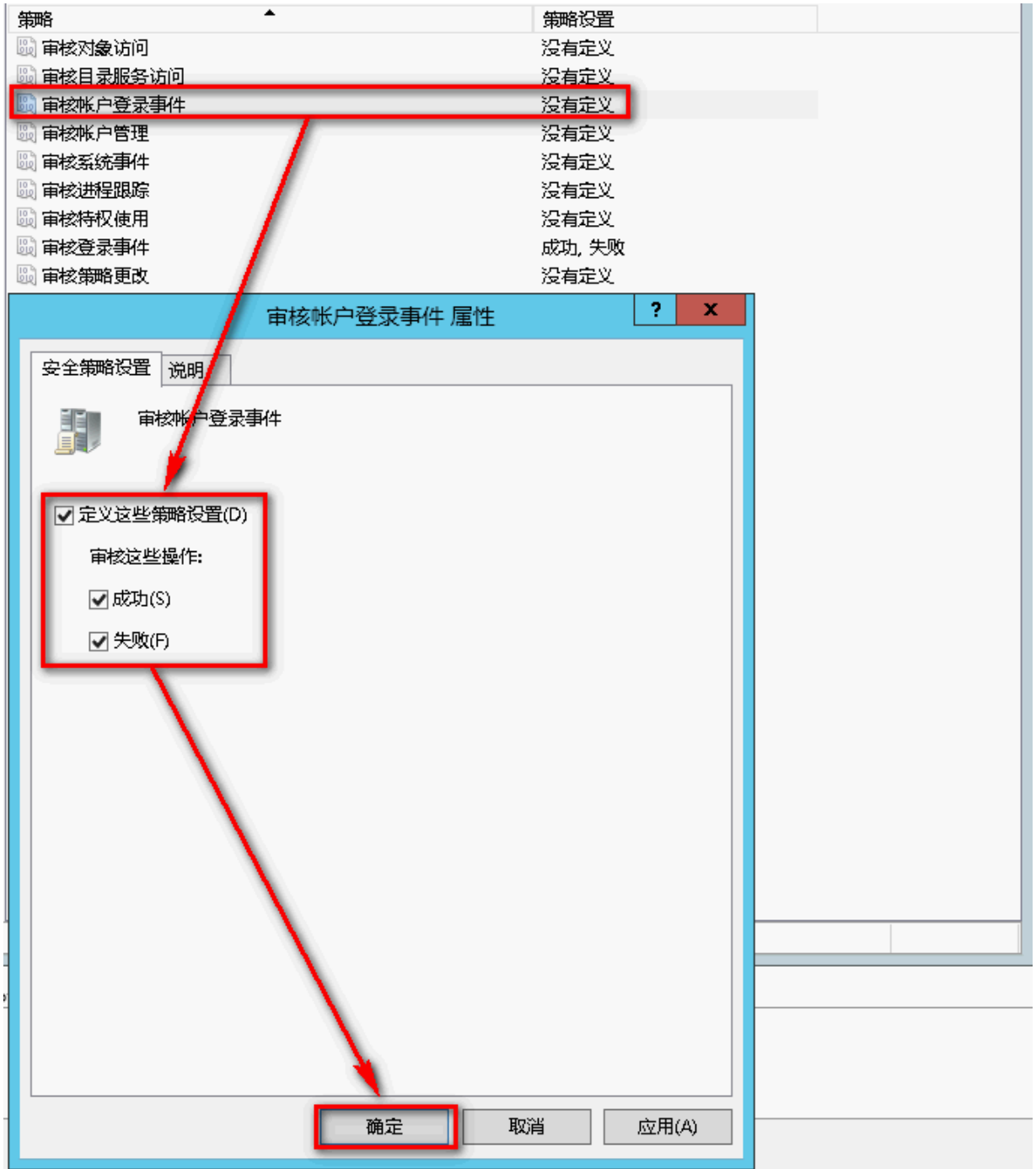
(1) 审核登录事件(Audit logon events)：

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) :

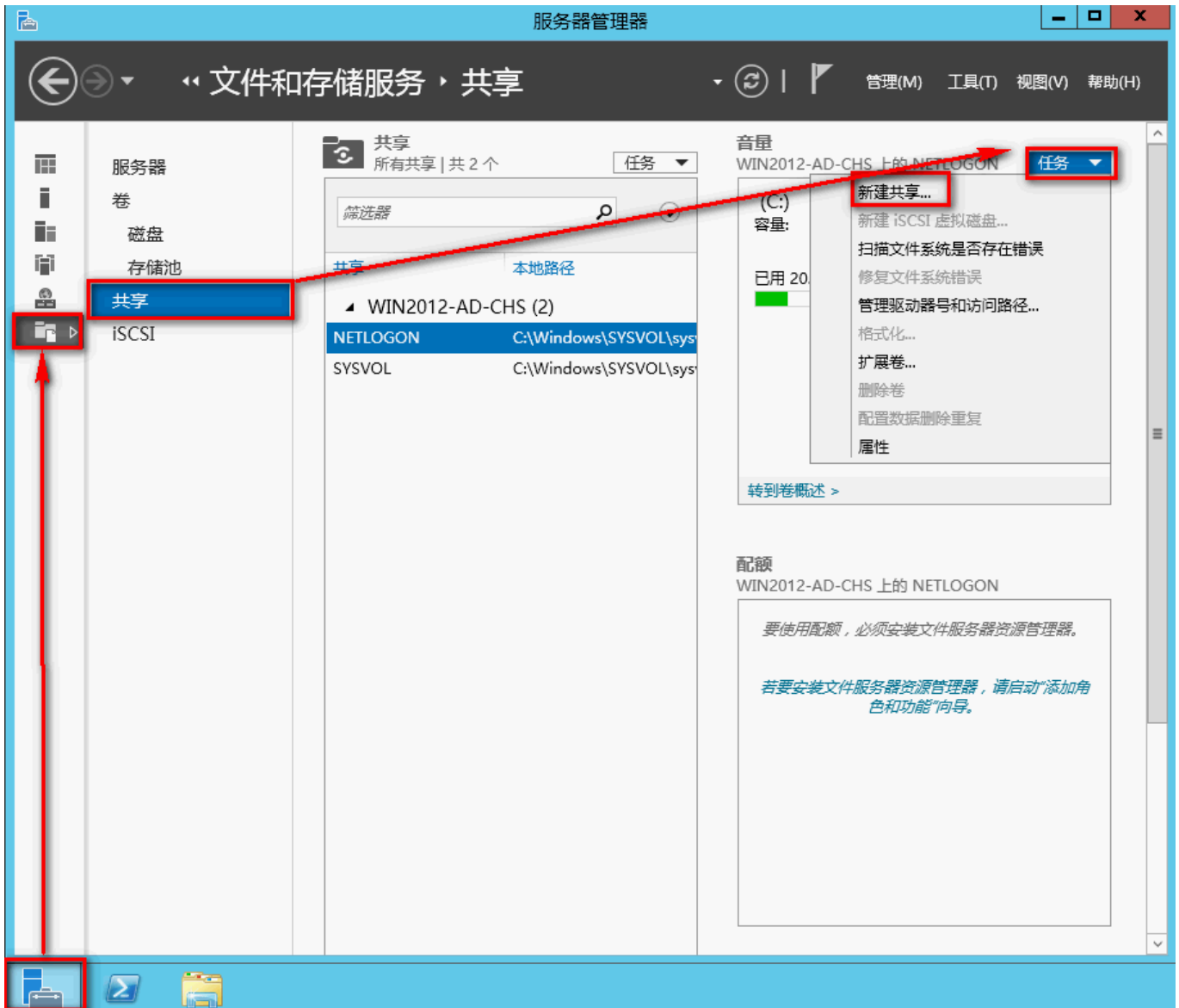
双击 [审核账户管理], 勾选 [定义这些策略设置], 再勾选 [成功] 及 [失败], 设定完成后按 [确定]。

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)。

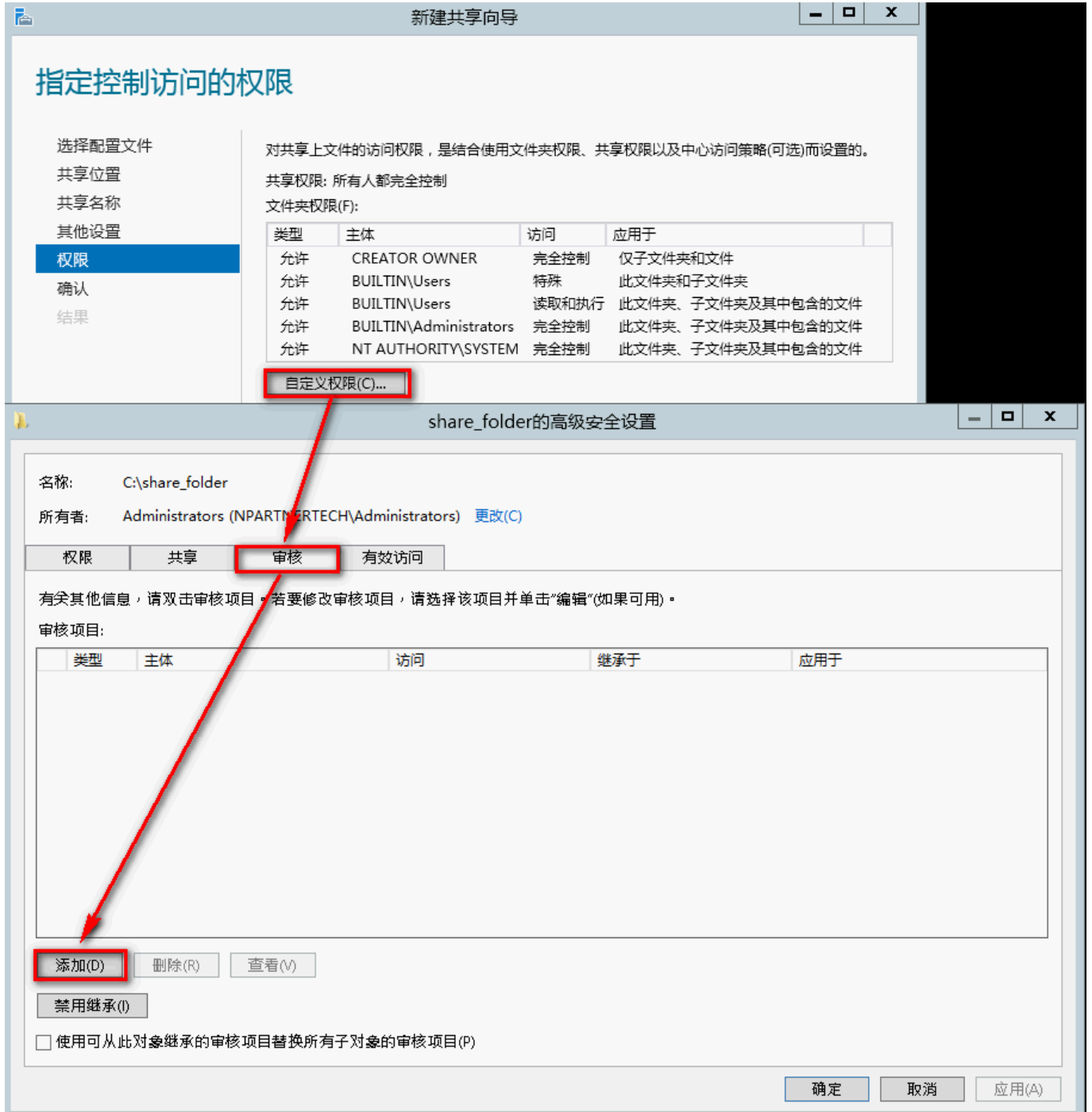
4.2 设定共享文件夹权限与审核策略

设定步骤如下：

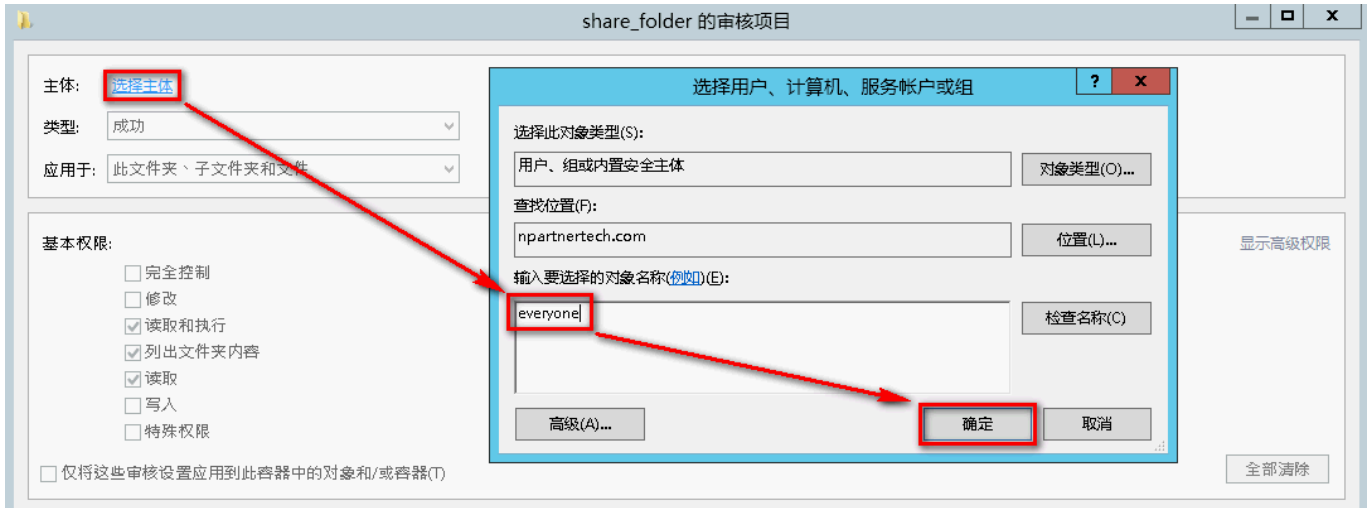
1. 点选 [服务器管理器 / 文件和储存服务 / 共享 / 任务 / 新建共享...]。



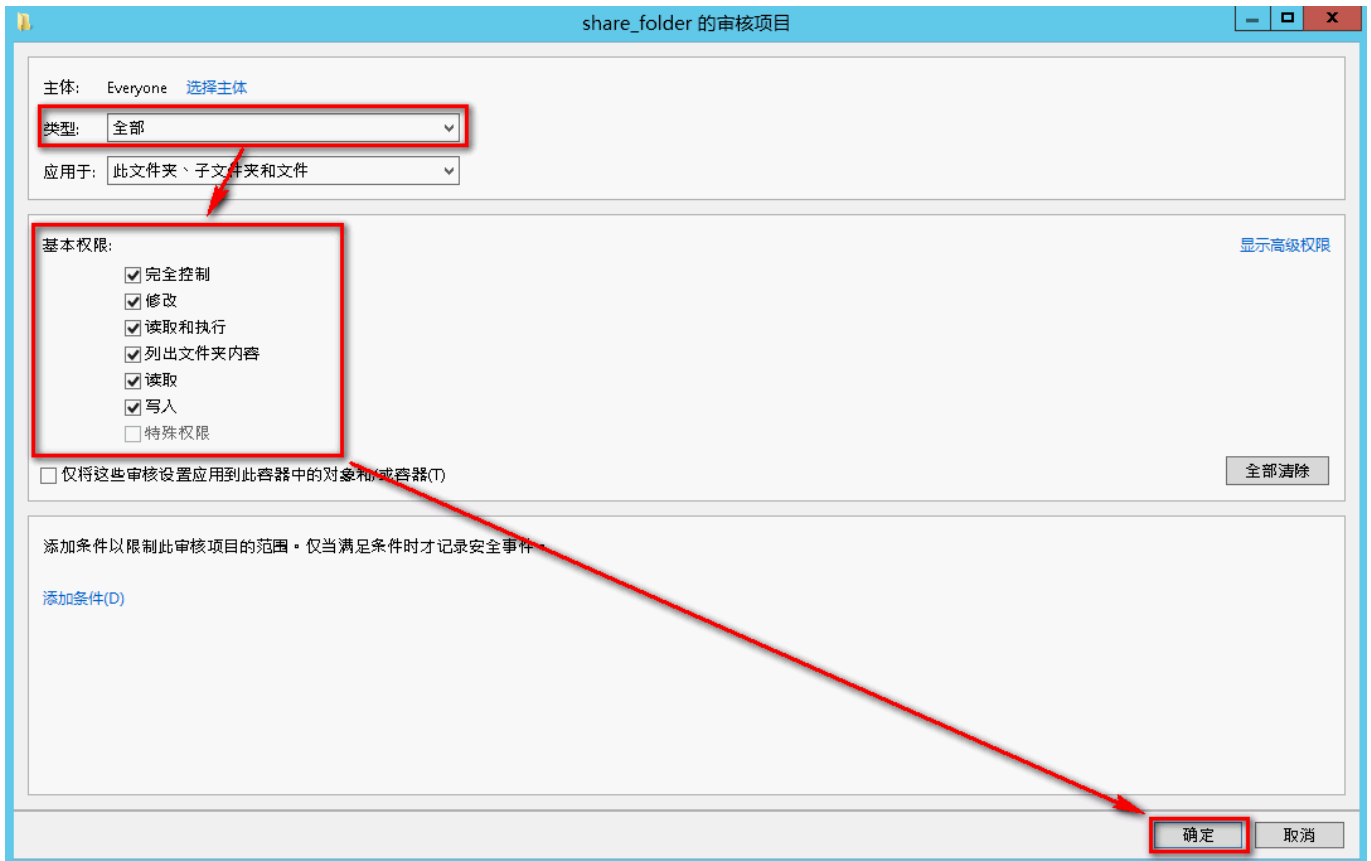
2. 选择配置文件，鼠标左点 [SMB 共享- 快速] ，左点 [下一步]。
3. 共享位置勾选[键入自定义路径] ，本例输入 " C:\share_folder " ，左点[下一步]。
4. 输入共享名称，本例输入 " share_folder " ，左点 [下一步] 。
5. 其他设置勾选 [启用基于存取的枚举] ，左点 [下一步] 。
6. 权限点选 [自定义权限... / 审核 / 添加] 。



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] 。



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



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。

联络信息

N-Partner 公司联络方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有关技术问题请洽：

Email: support@npartnertech.com

Skype : [support@npartnertech.com](https://www.skype.com/people/support@npartnertech.com)

有关业务相关问题请洽：

Email: sales@npartnertech.com

