N-Partner

N-REPORTER

如何使用 NXLOG 管理配置 Windows Server AD 日誌

V 009 (繁體)

2018/10/18

前言

本文件描述 N-Reporter 使用者如何使用 Open Source 工具 NXLOG 管理配置 Windows Server AD 2003/2008/2012/2016 的日誌(Event log)，將事件(Event)轉成 syslog，再轉發到 N-Reporter 做正規化、稽核與分析。本文件配置的環境分別為 Windows Server 2003 AD、Windows Server 2008 AD、Windows Server 2012 AD、Windows2016 AD。

NXLOG 適用於記錄大量事件的環境。Windows Server 日誌(Event log)每秒最大記錄速率超過 700 筆，請使用 NXLOG 的配置方式。

文件章節如下：

1 安裝設定 Windows Server AD 環境中的 NXLog

1.1 For Windows Server 2003 AD

1. **下載 NXLOG：**

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

   請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi，本例為下載 nxlog-ce-2.9.1716.msi。

2. **安裝 NXLOG：**

   請全程以具有 **系統管理員(Administrator)** 的帳號權限身分登入系統並操作相關步驟。(否則可能會因權限不足的問題導致設定無作用)

   滑鼠雙點 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式安裝步驟。

3. **下載設定 Windows 2003 的 NXLOG 配置檔 nxlog_win2k3.conf：**

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

   開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 的 NXLOG 配置檔, 將上面的 URL 上的 nxlog_win2k3.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 檔案中的參數設定後存檔。

   註 1： 預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog，會過濾大部分非必要的 Eventlog 雜訊，減輕 NXLOG 程式對 Windows AD 主機效能的負擔。

   註 2：32 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "

   64 位元 OS 的 NXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

4. **下載設定 Windows 2003 的 NXLOG 配置檔 nxlog_win2k3_all.conf (輸出全部的 Eventlog)**

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

   N-Reporter 提供**法規報表**統計 Windows AD 所有 Eventlog。使用者若是需要 Windows AD 的法規報表，請將 nxlog_win2k3_all.conf 檔案裡的設定內容複製, 然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 的參數設定後存檔。

   此設定將會輸出所有 Windows AD 的 Eventlog。

   請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

   若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重，請使用上述章節 nxlog_win2k3.conf 的配置檔 for Windows 2003.

```
## 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
```

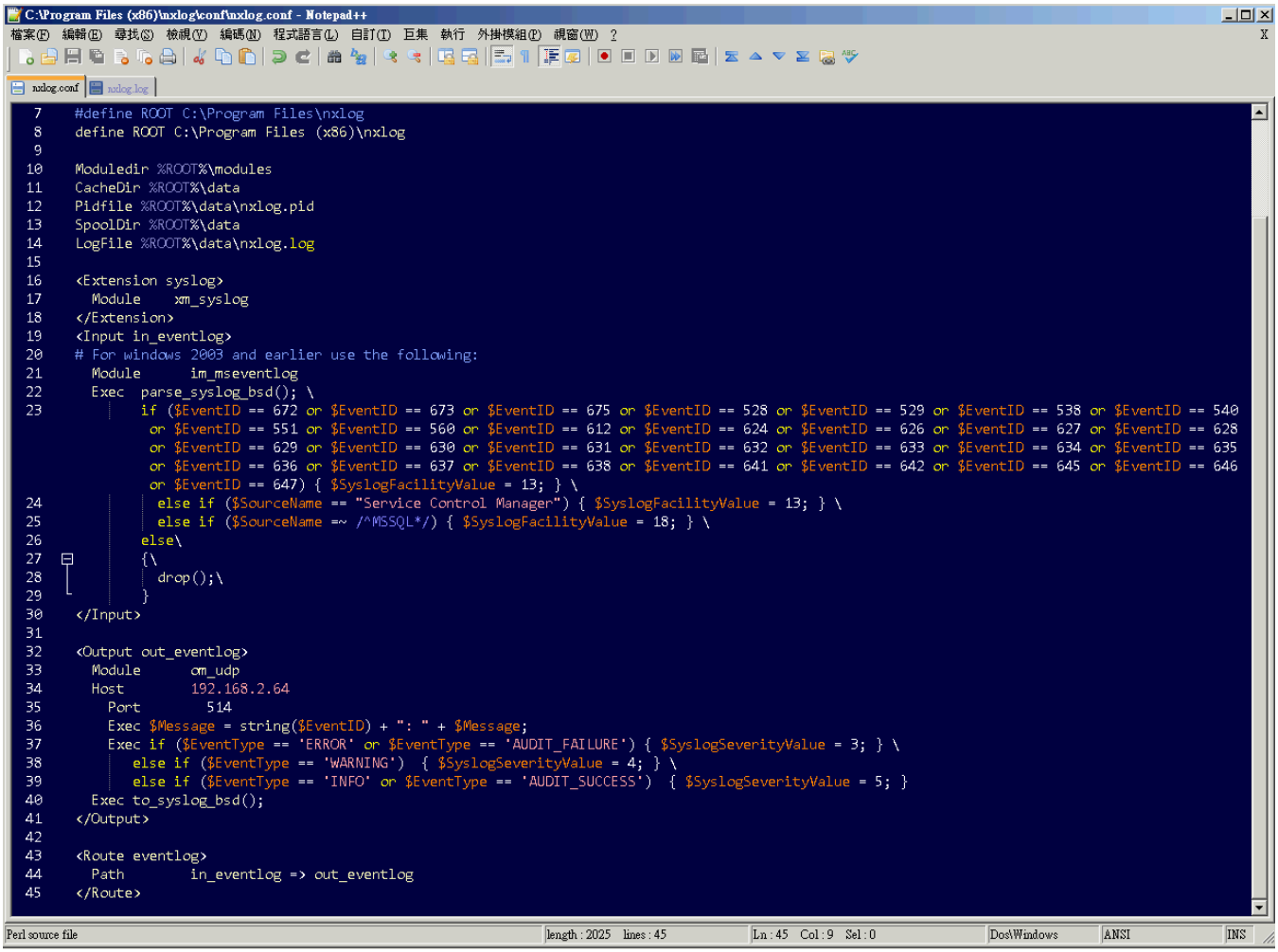
```
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
LogFile %ROOT%\data\nxlog.log

<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>
```

綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑，

本文件範例環境為 64 位元 OS 系統，選擇 " define ROOT C:\Program Files (x86)\nxlog " 。

紅色文字部位請輸入 N-Reporter 機器 IP，本文件範例為輸入 " 192.168.2.64 " 。

設定範例如下圖：



5. 啟動 NXLOG 程式：

a. 以系統管理員身份執行[命令提示字元]啟動 NXLOG：

[開始]→[所有程式]→[應用附屬程式] → [命令提示字元]，滑鼠右鍵點[命令提示字元]，選擇 [以系統管理員身分執行]。

命令提示字元輸入：

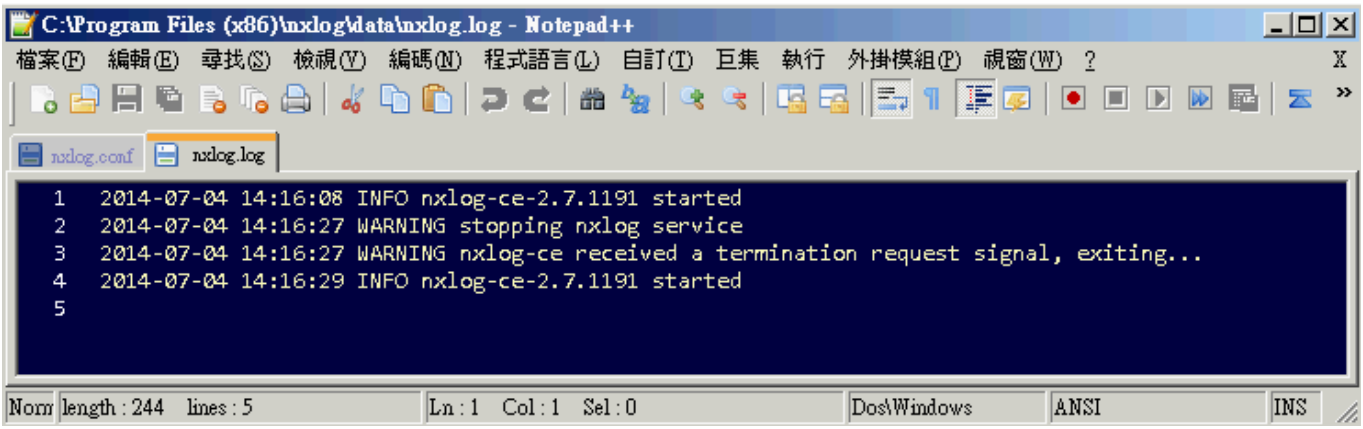
```
net stop nxlog
net start nxlog
#會看到以下訊息
The nxlog service is starting.
The nxlog service was started successfully.
```

b. [開始] →[所有程式]→[系統管理工具]→[服務] →找到[nxlog]，右鍵點服務[nxlog]，點選[啟動]或[重新啟動]。

6. 檢查 NXLOG 是否正常啟動：

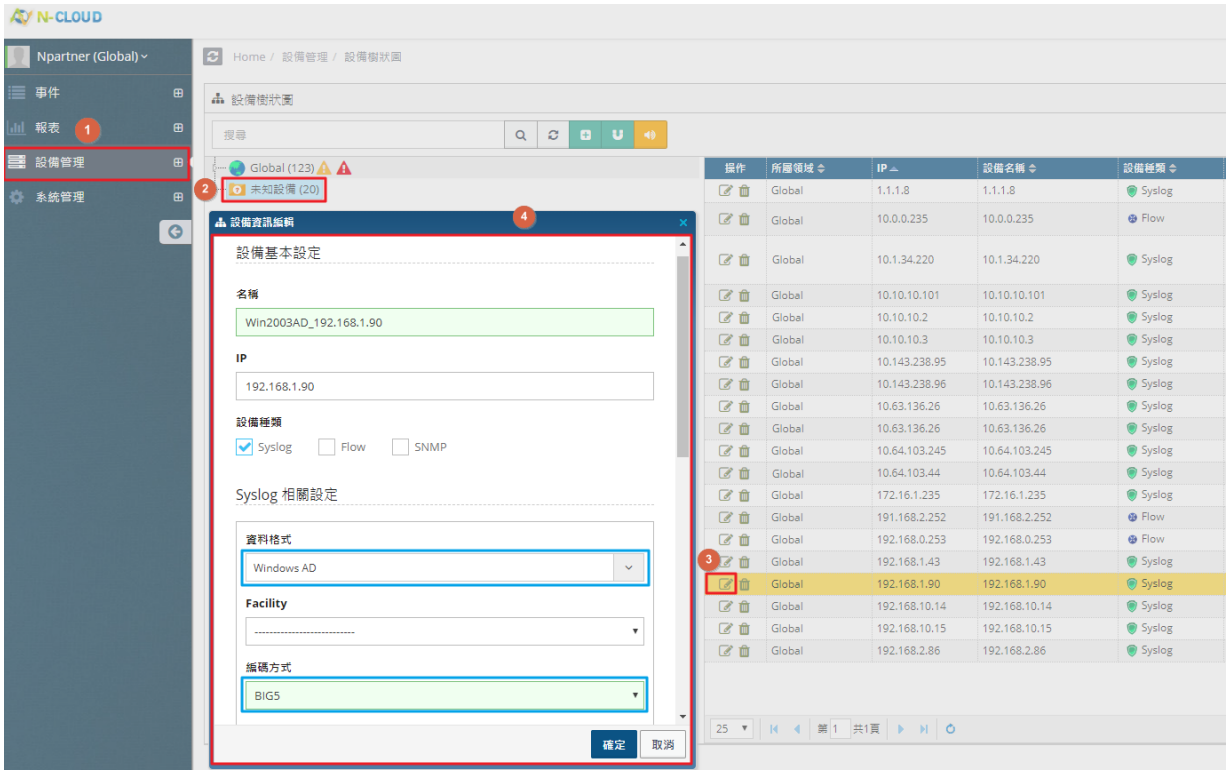
開啟檢查 NXLOG 的 log 檔，檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log "

若沒有顯示 Error 的訊息，表示正常啟動。



7. 新增 Windows Server 2003 AD Syslog 設備時，資料格式請選擇 [Windows AD]

註： 因 NXLOG 沒有 Eventlog to Syslog Utility 將事件編碼轉成 UTF8 編碼的功能，所以新增 Windows Server 2003 AD 設備時請注意語系選擇，避免出現亂碼。



8. 語系選擇：

OS Windows Server 2003 AD 繁體版 請選擇[BIG5]編碼。

OS Windows Server 2003 AD 簡體版 請選擇[GB2312]編碼。

OS Windows Server 2003 AD 英文版 請選擇[UTF8]編碼。

1.2 For Windows Server 2008 AD

1. **下載 NXLOG：**

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

   請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi，本例為下載 nxlog-ce-2.9.1716.msi。

2. **安裝 NXLOG：**

   請全程以具有 **系統管理員(Administrator)** 的帳號權限身分登入系統並操作相關步驟。(否則可能會因權限不足的問題導致設定無作用)

   滑鼠雙點 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式安裝步驟。

3. **下載設定 Windows 2008 NXLOG 配置檔 nxlog_win2k8.conf：**

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

   開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 NXLOG 配置檔，將上面的 URL 上的 nxlog_win2k8.conf 裡的設定內容複製，然後貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 檔案中的參數設定後存檔。

   註 1： 預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog，會過濾大部分非必要的 Eventlog 雜訊，減輕 NXLOG 程式對 Windows AD 主機效能的負擔。

   註 2：32 位元 OS NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "
   64 位元 OSNXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。

4. **下載設定 Windows 2008 的 NXLOG 配置檔 nxlog_win2k8_all.conf (輸出全部 Eventlog)**

   前往 URL：http://www.npartnertech.com/download/tech/nxlog_win2k8_all.conf

   N-Reporter 提供**法規報表**統計 Windows AD 所有 Eventlog。使用者若是需要 Windows AD 的法規報表，請將 nxlog_win2k8_all.conf 檔案裡的設定內容複製，然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 的參數設定後存檔。

   此設定將會輸出所有 Windows AD 的 Eventlog。

   請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

   若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重，請使用上述章節 nxlog_win2k8.conf 的配置檔 for Windows 2008.

```
## 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=1100)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4769)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4768)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4771)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4616)]]</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=4740)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4741)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4742)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4743)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4744)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4745)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4748)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4749)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4750)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4753)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4754)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4755)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4756)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4758)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4759)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4760)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4763)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4764)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4767)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4778)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4783)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4800)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4801)]]</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>
```

綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑

本文件範例環境為 64 位元 OS 系統，選擇 " define ROOT C:\Program Files (x86)\nxlog " 。

紅色文字部位請輸入 N-Reporter 機器 IP，本文件範例為輸入 " 192.168.2.64 " 。

設定範例如下圖：

nxlog.conf | nxlog.log

```
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. 啟動 NXLOG 程式：

a. 以系統管理員身份執行[命令提示字元]啟動 NXLOG：

[開始]→[所有程式]→[應用附屬程式] → [命令提示字元]，滑鼠右鍵點[命令提示字元]，選擇 [以系統管理員身分執行]。

命令提示字元輸入：

```
net stop nxlog
net start nxlog
```

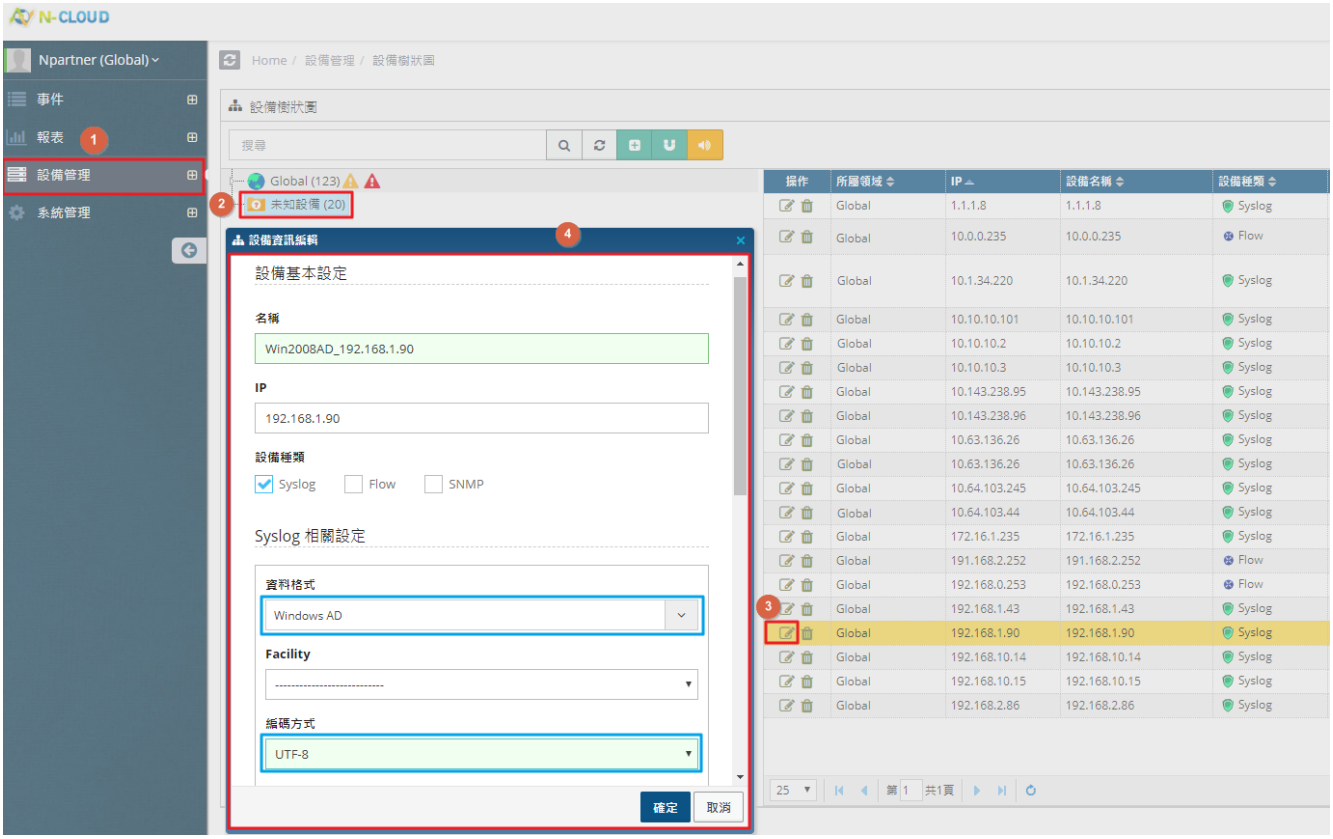
```
#會看到以下訊息
The nxlog service is starting.
The nxlog service was started successfully.
```

b. [開始] →[所有程式]→[系統管理工具]→[服務] →找到[nxlog]，右鍵點服務[nxlog]，點[啟動]或[重新啟動]。

6. 檢查 NXLOG 是否正常啟動：

開啟檢查 NXLOG 的 log 檔，檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log "
若沒有顯示 Error 的訊息，表示正常啟動。

7. 新增 Windows Server 2008 AD Syslog 設備時，資料格式請選擇 [Windows AD]。



1.3 For Windows Server 2012 AD

1. **下載 NXLOG：**

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

   請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi，本例為下載 nxlog-ce-2.9.1716.msi。

2. **安裝 NXLOG：**

   請全程以具有 **系統管理員(Administrator)** 的帳號權限身分登入系統並操作相關步驟。(否則可能會因權限不足的問題導致設定無作用)

   滑鼠雙點 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式安裝步驟。

3. **下載設定 Windows 2012 NXLOG 配置檔 nxlog_win2012.conf：**

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

   開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 NXLOG 配置檔，將上面的 URL 上的 nxlog_win2k3.conf 檔案裡的設定內容複製，然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 檔案中的參數設定後存檔。

   註 1：預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog，會過濾大部分非必要的 Eventlog 雜訊，減輕 NXLOG 程式對 Windows AD 主機效能的負擔。

   註 2：32 位元 OS NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "

   64 位元 OS NXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

4. **下載設定 Windows 2012 的 NXLOG nxlog_win2012_all.conf (輸出全部 Eventlog)**

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

   N-Reporter 提供**法規報表**統計 Windows AD 所有 Eventlog。使用者若是需要 Windows AD 的法規報表，請將 nxlog_win2012_all.conf 裡的設定內容複製，然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 的參數設定後存檔。

   此設定將會輸出所有 Windows AD 的 Eventlog。

   請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

   若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重，請使用上述章節 nxlog_win2012.conf 的配置檔 for Windows 2012.

```
## 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=1100)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4769)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4768)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4771)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4616)]]</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=4740)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4741)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4742)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4743)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4744)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4745)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4748)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4749)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4750)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4753)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4754)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4755)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4756)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4758)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4759)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4760)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4763)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4764)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4767)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4778)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4783)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4800)]]</Select> \
                                                <Select Path="Security">*[System[(EventID=4801)]]</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>
```

綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑

本文件範例環境為 64 位元 OS 系統，選擇 " define ROOT C:\Program Files (x86)\nxlog " 。

紅色文字部位請輸入 N-Reporter 機器 IP，本文件範例為輸入 " 192.168.2.64 " 。

設定範例如下圖：

nxlog.conf | nxlog.log

```
                    <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>
```

5. 啟動 NXLOG 程式：

a. 以系統管理員身份執行[命令提示字元] 啟動 NXLOG：

[開始]→[所有程式]→[應用附屬程式] → [命令提示字元]，滑鼠右鍵點[命令提示字元]，點選[以系統管理員身分執行]。

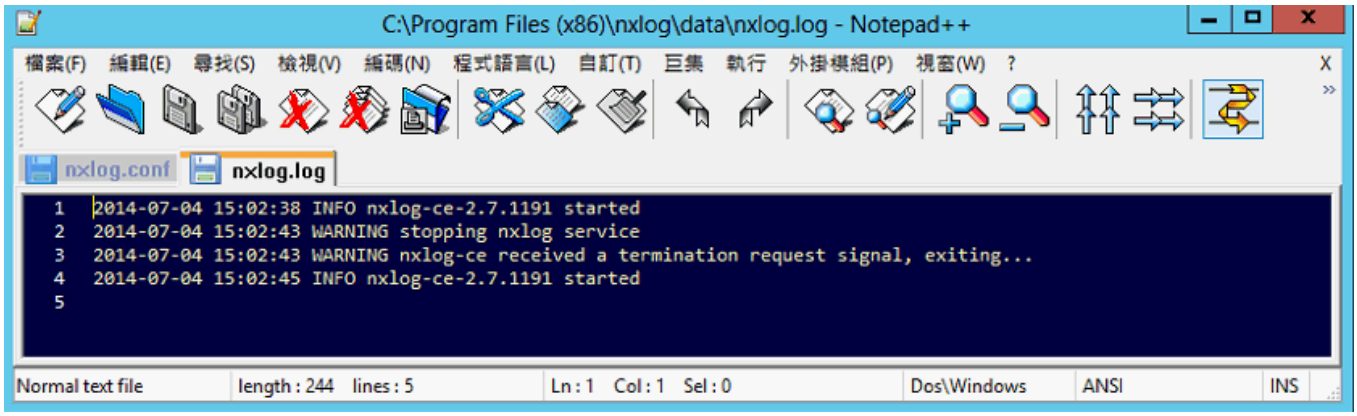
[Windows PowerShell]輸入：

```
net stop nxlog
net start nxlog
#會看到以下訊息
nxlog 服務正在啟動.
nxlog 服務已經啟動成功.
```

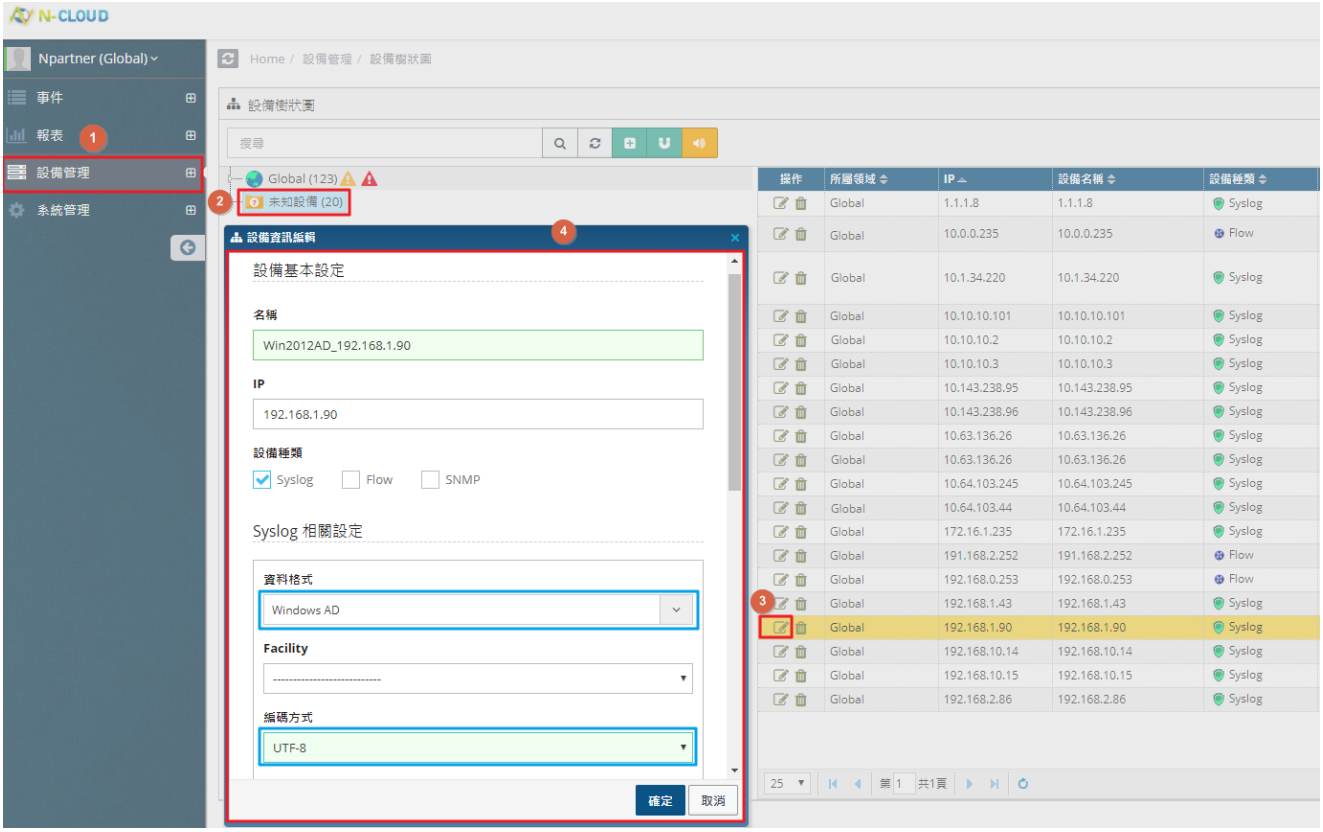
b. [開始] →[所有程式]→[系統管理工具]→[服務] →找到[nxlog]，右鍵點服務[nxlog]，點選[啟動]或[重新啟動]。

6. 檢查 NXLOG 是否正常啟動：

開啟檢查 NXLOG 的 log 檔，檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log "
若沒有顯示 Error 的訊息，表示正常啟動。



7. 新增 Windows Server 2012 AD Syslog 設備時，資料格式請選擇 [Windows AD]。



1.4 For Windows Server 2016 AD

1. **下載 NXLOG：**

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

   請下載網頁中提供的最新版 nxlog-ce-x.x.xxxx.msi，本例為下載 nxlog-ce-2.9.1716.msi。

2. **安裝 NXLOG：**

   請全程以具有 **系統管理員(Administrator)** 的帳號權限身分登入系統並操作相關步驟。(否則可能會因權限不足的問題導致設定無作用)

   滑鼠雙點 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式安裝步驟。

3. **下載設定 Windows 2016 NXLOG 配置檔 nxlog_win2016.conf：**

   前往 URL：http://www.npartnertech.com/download/tech/nxlog_win2016.conf

   開啟並編輯此檔案路徑 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 NXLOG 配置檔，將上面的 URL 上的 nxlog_win2016.conf 裡的設定內容複製，然後貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 檔案中的參數設定後存檔。

   註 1：預設建議使用者採用此設定檔. 此設定只輸出主機稽核、物件存取、帳戶管理等 Eventlog，會過濾大部分非必要的 Eventlog 雜訊，減輕 NXLOG 程式對 Windows AD 主機效能的負擔。

   註 2：32 位元 OS NXLOG 安裝路徑在 " C:\Program Files\nxlog\conf\nxlog.conf "
   64 位元 OSNXLOG 安裝路徑在 " C:\Program Files (x86)\nxlog\conf\nxlog.conf " 。

4. **下載設定 Windows 2016 的 NXLOG 配置檔 nxlog_win2016_all.conf (輸出全部 Eventlog)**

   前往 URL：http://www.npartnertech.com/download/tech/nxlog_win2016_all.conf

   N-Reporter 提供**法規報表**統計 Windows AD 所有 Eventlog。使用者若是需要 Windows AD 的法規報表，請將 nxlog_win2016_all.conf 檔案裡的設定內容複製，然後將其貼上並覆蓋 C:\Program Files (x86)\nxlog\conf\nxlog.conf " 路徑中的 nxlog.conf 的參數設定後存檔。

   此設定將會輸出所有 Windows AD 的 Eventlog。

   請注意!! 此設定檔會需要 Windows AD 主機配備較高的硬體效能來執行 NXLOG。

   若主機硬體效能不足或 Nxlog 處理程序的資源使用的 Loading 太重，請使用上述章節 nxlog_win2016.conf 的配置檔 for Windows 2016.

```
## 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/7/8/2012/2012R2/2016 and latter use the following:
   Module          im_msvistalog
   ReadFromLast TRUE
   SavePos         TRUE
   Query        <QueryList> \
                                                <Query Id="0"> \
                                                        <Select Path="Security">*[System[(EventID=1100)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4769)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4768)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4771)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4616)]]</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=4740)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4741)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4742)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4743)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4744)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4745)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4748)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4749)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4750)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4753)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4754)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4755)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4756)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4758)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4759)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4760)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4763)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4764)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4767)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4778)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4783)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4800)]]</Select> \
                                                        <Select Path="Security">*[System[(EventID=4801)]]</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>
```

綠色文字部位請依 OS 環境為 32 位元或 64 位元選擇 NXLOG 正確的安裝路徑

本文件範例環境為 64 位元 OS 系統，選擇 " define ROOT C:\Program Files (x86)\nxlog " 。

紅色文字部位請輸入 N-Reporter 機器 IP，本文件範例為輸入 " 192.168.2.64 " 。

設定範例如下圖：

nxlog.conf | nxlog.log

```
65                                  <Select Path="Security">*[System[(EventID=4753)]]</Select> \
66                                  <Select Path="Security">*[System[(EventID=4754)]]</Select> \
67                                  <Select Path="Security">*[System[(EventID=4755)]]</Select> \
68                                  <Select Path="Security">*[System[(EventID=4756)]]</Select> \
69                                  <Select Path="Security">*[System[(EventID=4758)]]</Select> \
70                                  <Select Path="Security">*[System[(EventID=4759)]]</Select> \
71                                  <Select Path="Security">*[System[(EventID=4760)]]</Select> \
72                                  <Select Path="Security">*[System[(EventID=4763)]]</Select> \
73                                  <Select Path="Security">*[System[(EventID=4764)]]</Select> \
74                                  <Select Path="Security">*[System[(EventID=4767)]]</Select> \
75                                  <Select Path="Security">*[System[(EventID=4778)]]</Select> \
76                                  <Select Path="Security">*[System[(EventID=4783)]]</Select> \
77                                  <Select Path="Security">*[System[(EventID=4800)]]</Select> \
78                                  <Select Path="Security">*[System[(EventID=4801)]]</Select> \
79                                  <Select Path="System">*[System[(EventID=7036)]]</Select> \
80                                  <Select Path="Application">*[System[(EventID=18454)]]</Select> \
81                                  <Select Path="Application">*[System[(EventID=18456)]]</Select> \
82                              </Query> \
83                      </QueryList>
84    </Input>
85
86  <Output out_eventlog>
87     Module       om_udp
88     Host         192.168.2.64
89     Port         514
90     Exec $Message = string($SourceName) + ": " + string($EventID) + ": " + $Message;
91     Exec if ($EventID == 18454 or $EventID == 18456 ) { $SyslogFacilityValue = 18; } \
92           else { $SyslogFacilityValue = 13; }
93     Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
94           else if ($EventType == 'WARNING')   { $SyslogSeverityValue = 4; } \
95           else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS')   { $SyslogSeverityValue = 5; }
96     Exec to_syslog_bsd();
97    </Output>
98
99  <Route eventlog>
100    Path         in_eventlog => out_eventlog
101   </Route>
```

5. 啟動 NXLOG 程式：

a. 以系統管理員身份執行[命令提示字元]啟動 NXLOG：

[開始]→[所有程式]→[應用附屬程式] → [命令提示字元]，滑鼠右鍵點[命令提示字元]，選擇 [以系統管理員身分執行]。

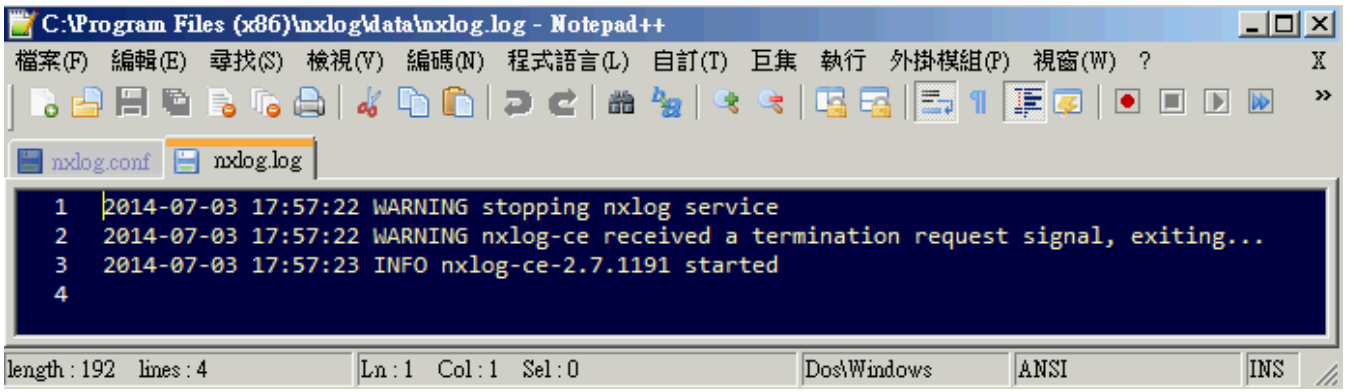
命令提示字元輸入：

```
net stop nxlog
net start nxlog
#會看到以下訊息
The nxlog service is starting.
The nxlog service was started successfully.
```

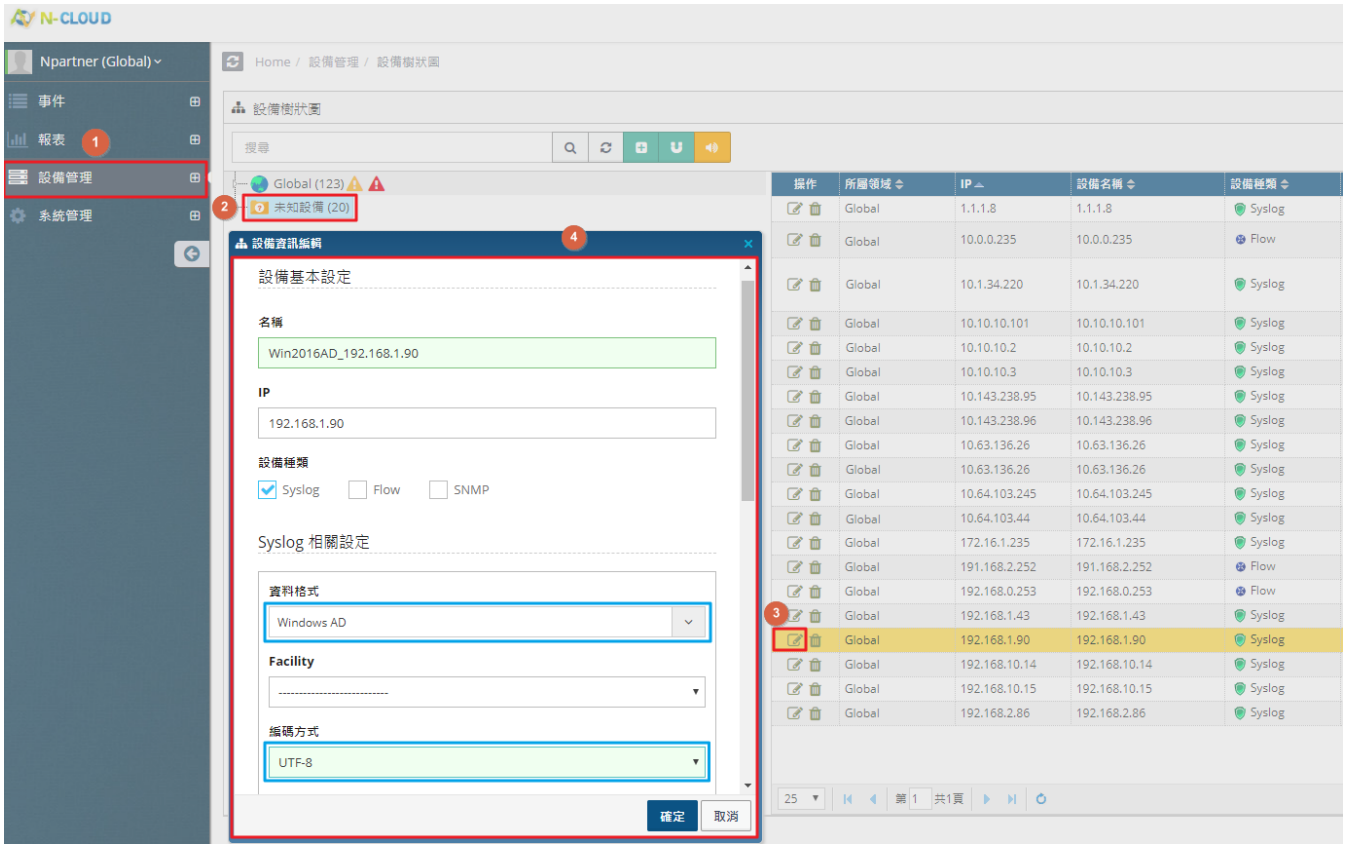
b. [開始] →[所有程式]→[系統管理工具]→[服務] →找到[nxlog]，右鍵點服務[nxlog]，點[啟動]或[重新啟動]。

6. 檢查 NXLOG 是否正常啟動：

開啟檢查 NXLOG 的 log 檔，檔案路徑為 " C:\Program Files (x86)\nxlog\data\nxlog.log "
若沒有顯示 Error 的訊息，表示正常啟動。



7. 新增 Windows Server 2016 AD Syslog 設備時，資料格式請選擇 [Windows AD]。



2 Windows 2003 Active Directory Server 稽核設定

本章節主要說明以下操作設定：

1.設定網域使用者登入登出的稽核原則。2.設定共享資料夾權限與稽核原則。

Windows 2003 AD Server 登入登出的稽核原則和目錄分享的稽核原則，預設是關閉的。

安裝 NXLOG 的步驟，詳細請參閱第一章節。

2.1設定 Windows 2003 AD Server 網域使用者登入登出的稽核原則

設定步驟如下：

1. 以**全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分**登入 Windows 2003 AD Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用)

點選 [開始 / 所有程式 / 系統管理工具 / 網域控制站安全性原則]。

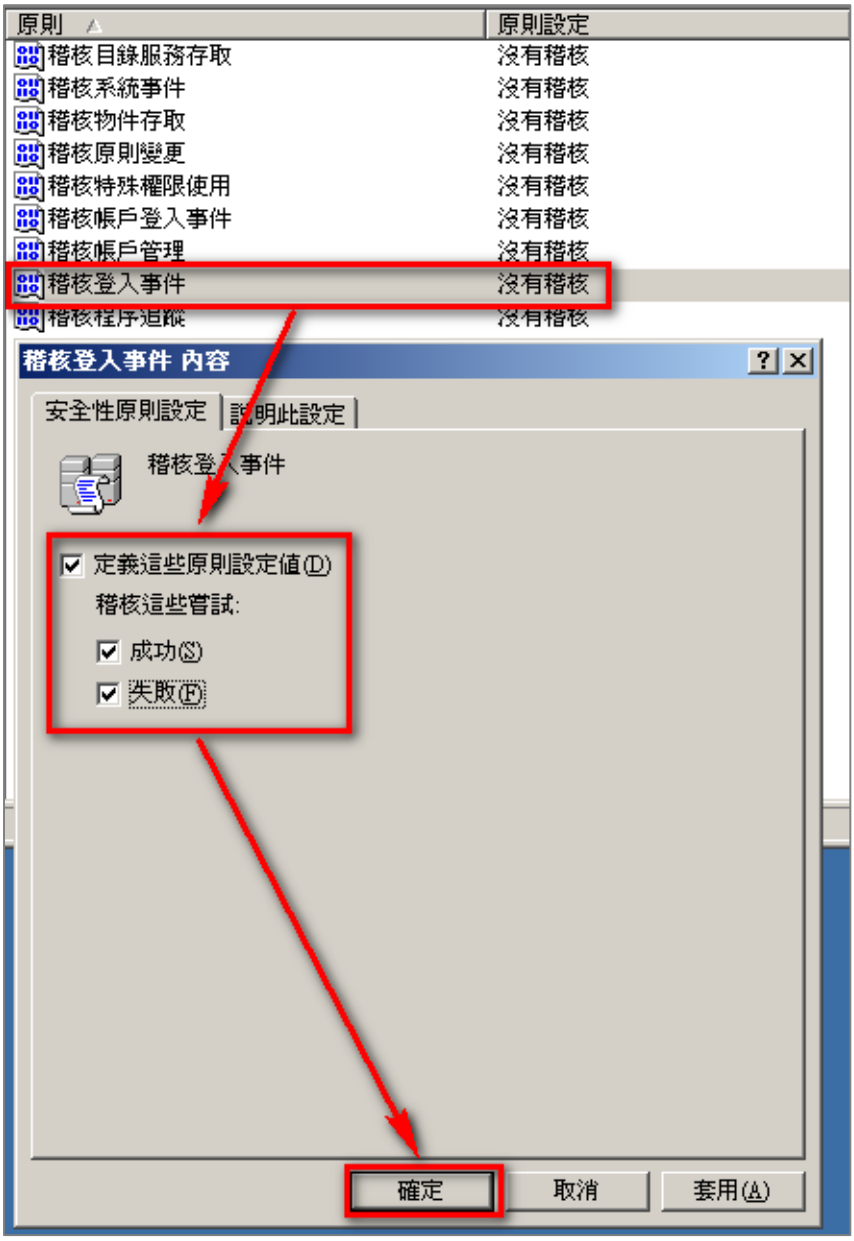
註：[系統管理工具]裡的[網域安全性原則]為設定整個網域裡的所有物件(所有使用者與電腦) ，而網域控制站安全性原則為設定所有網域控制站(Domain Controllers)。建議將此兩種安全性稽核原則設定為一致。

2. 前往 [Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]。

3. 定義下列的原則設定值：

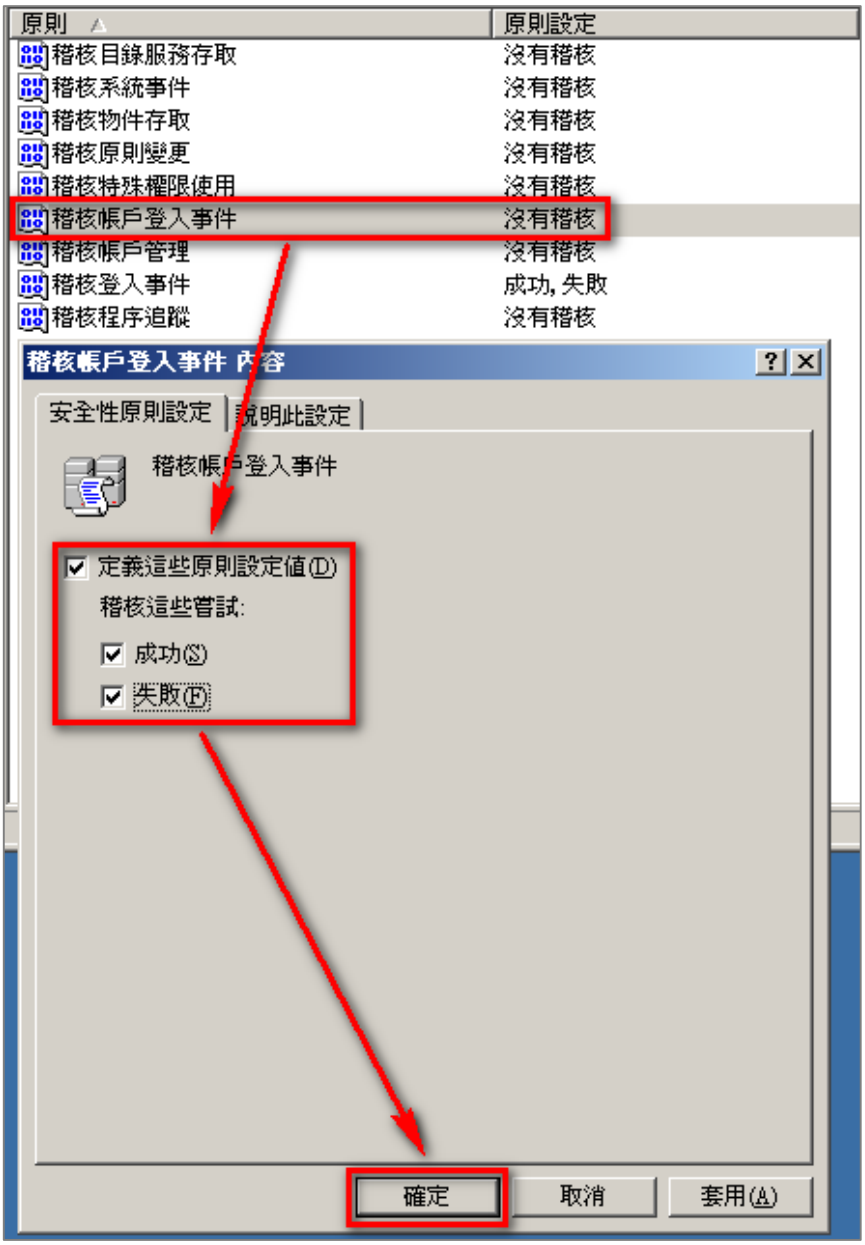
(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(2) 稽核帳戶登入事件：

滑鼠雙擊 [稽核帳戶登入事件]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核物件存取：

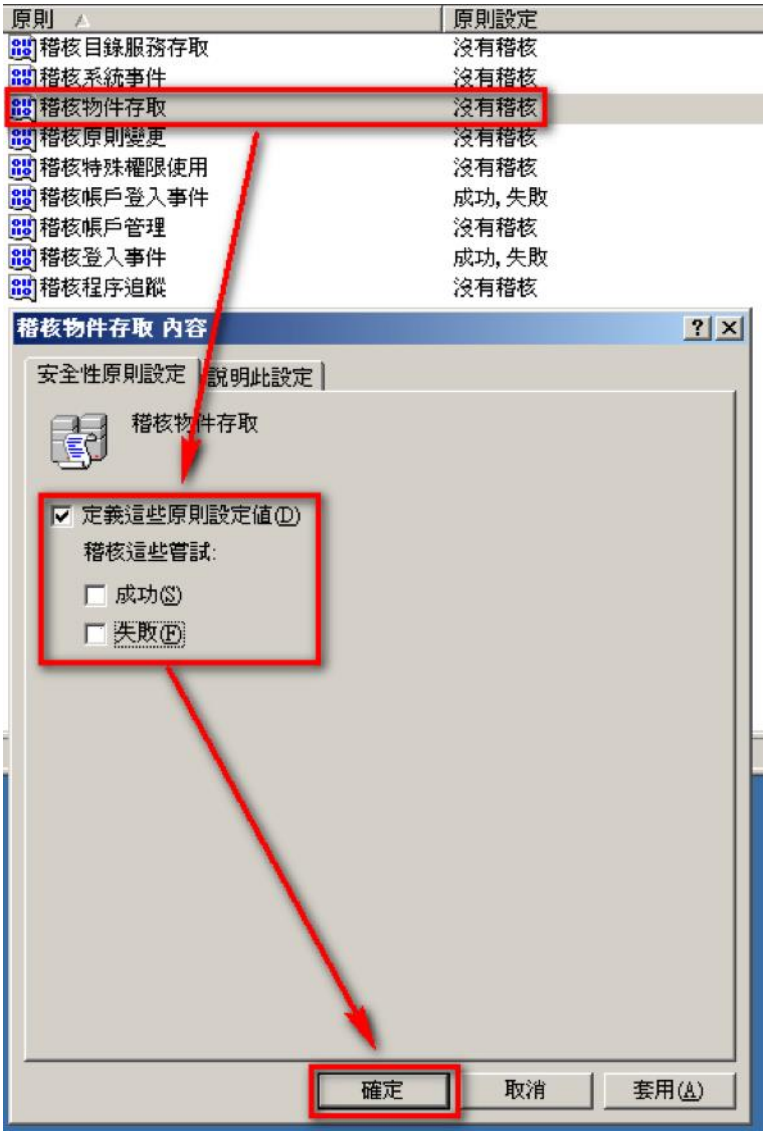
滑鼠雙擊 [稽核物件存取]，勾選 [定義這些原則設定值]

成功：若欲稽核成功事件的 Log，請勾選 [成功] 核取方塊。

失敗：若欲稽核失敗事件的 Log，請勾選 [失敗] 核取方塊。

設定完成後按 [確定]。

註：若 Windows 2003 Active Directory Server 不做檔案伺服器稽核 (File server audit)，建議不要勾選成功與失敗的設定值，僅需勾[定義這些原則設定值] 即可. 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter，會影響主機的運作效能。



(4) 稽核原則變更：

滑鼠雙擊 [稽核原則變更]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

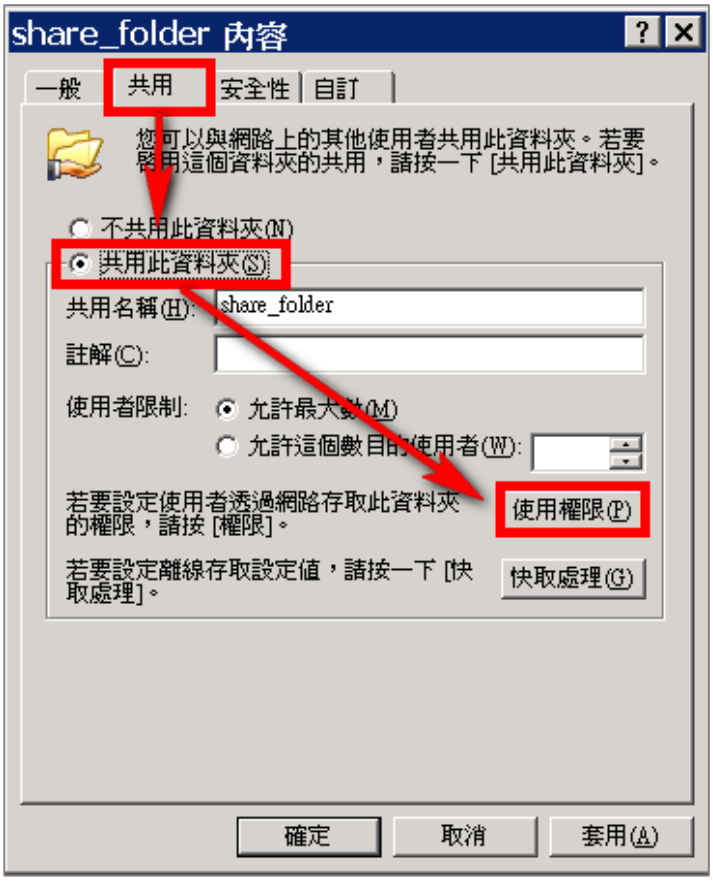
(5) 稽核帳戶管理：

滑鼠雙擊 [稽核帳戶管理]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

2.2設定共享資料夾權限與稽核原則

設定步驟如下：

1. 在欲共用的資料夾上點擊滑鼠右鍵，點選 [內容]。
2. 點選 [共用] 索引標籤，點選 [共用此資料夾]。點選 [使用權限]。



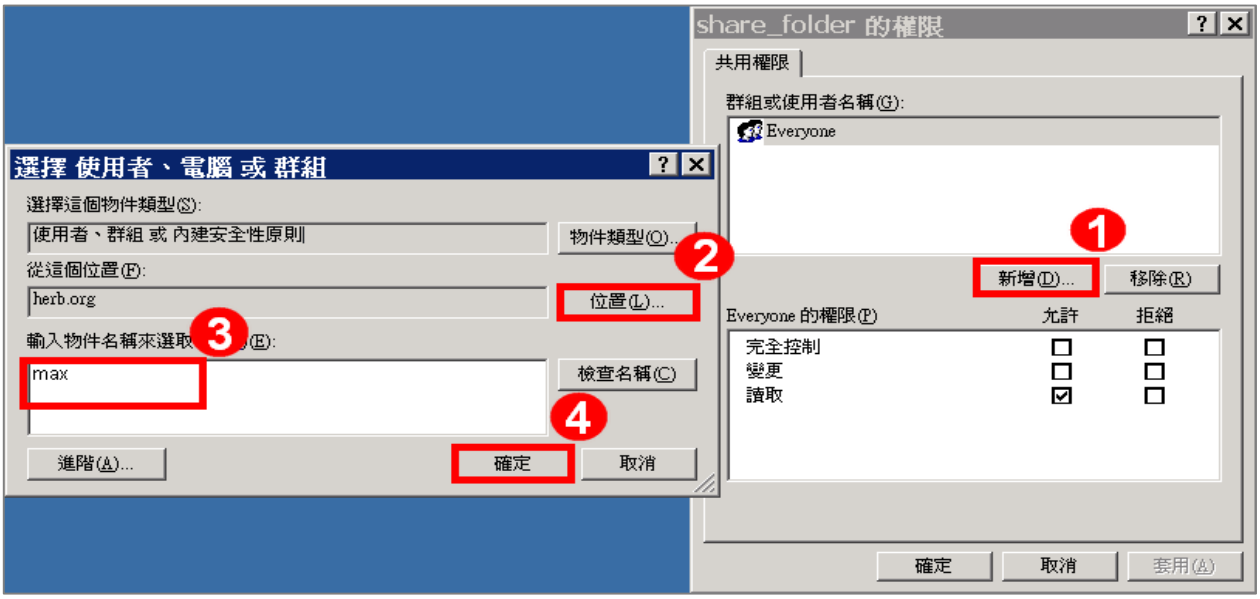
3. 使用者權限設定：

(1) 點選 [新增]，來新增一使用者。

(2) 若要選擇其他網域，可點選 [位置]。

(3) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

(4) 若網域使用者帳號存在的話，按 [確定] 完成設定。

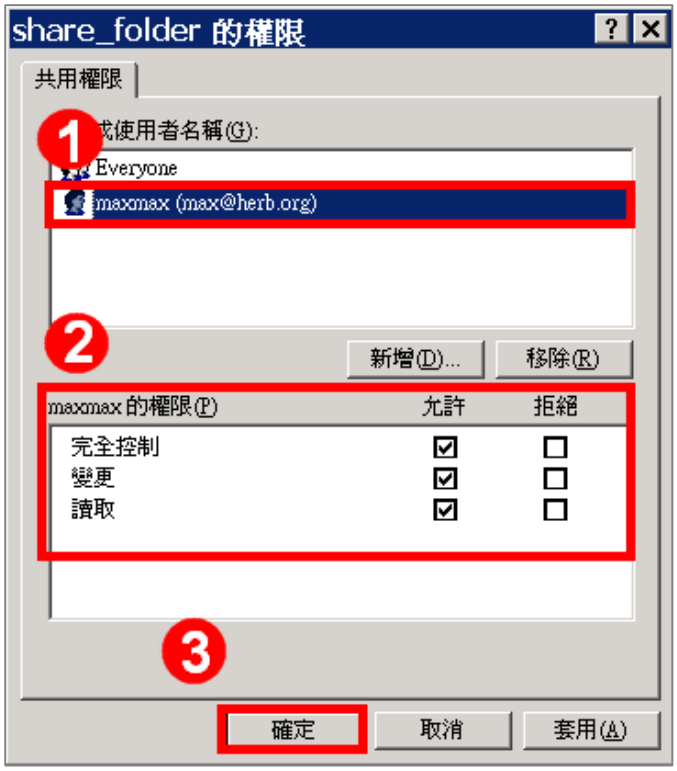


4. 設定使用者權限：

(1) 點選網域使用者帳號。

(2) 勾選允許 [完全控制] 及 [變更] 權限。

(3) 設定完成後按 [確定]。



5. 安全性設定：

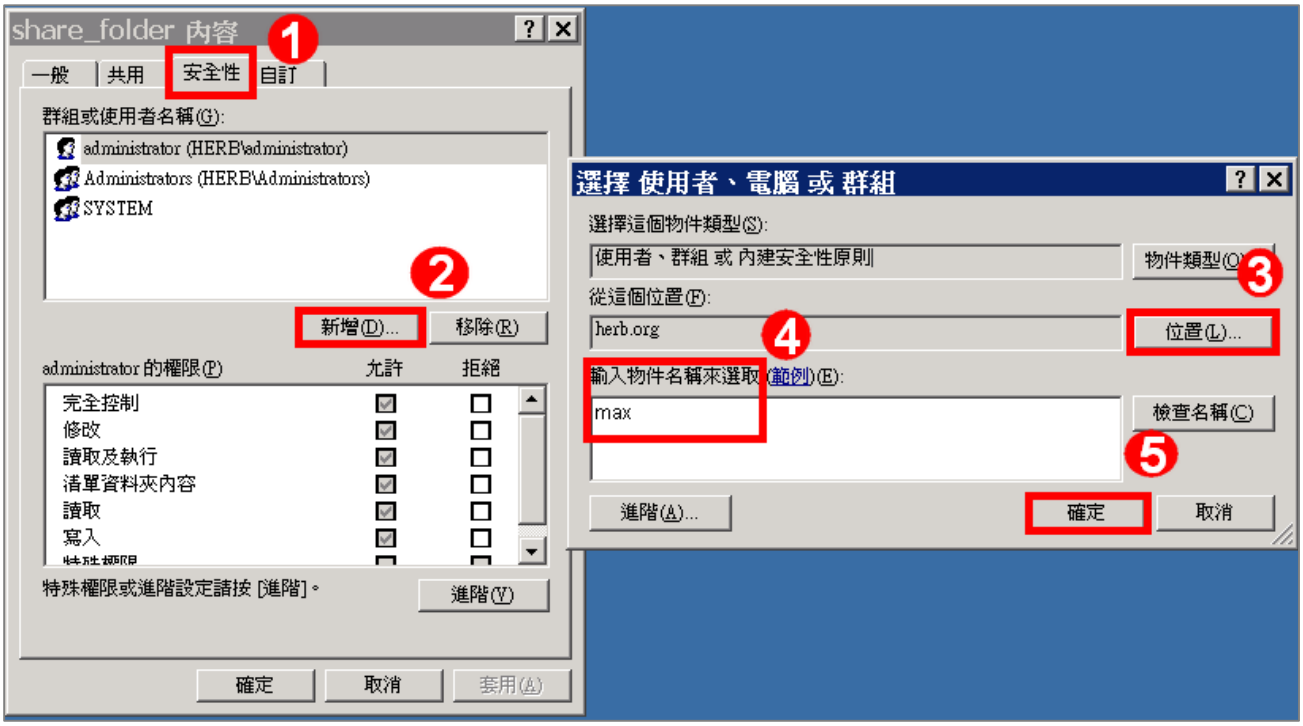
(1) 點選 [安全性] 索引標籤。

(2) 點選 [新增]，來新增一使用者。

(3) 若要選擇其他網域，可點選 [位置]。

(4) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

(5) 若網域使用者帳號存在的話，按 [確定] 完成設定。

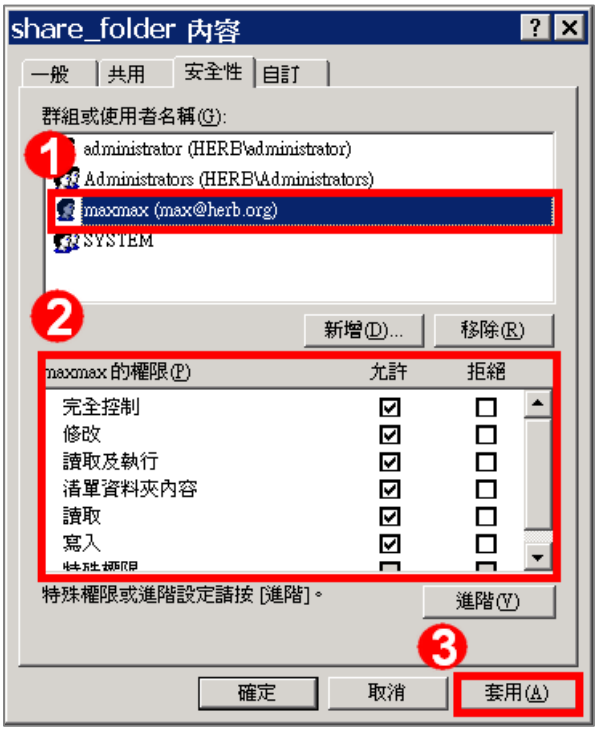


6. 設定使用者權限：

(1) 點選要設定的使用者帳號。

(2) 勾選允許 [完全控制] 權限，以取得所有權限。

(3) 按 [套用]及[確定]，完成設定。



7. 進階安全性設定：

(1) 點選 [進階]。

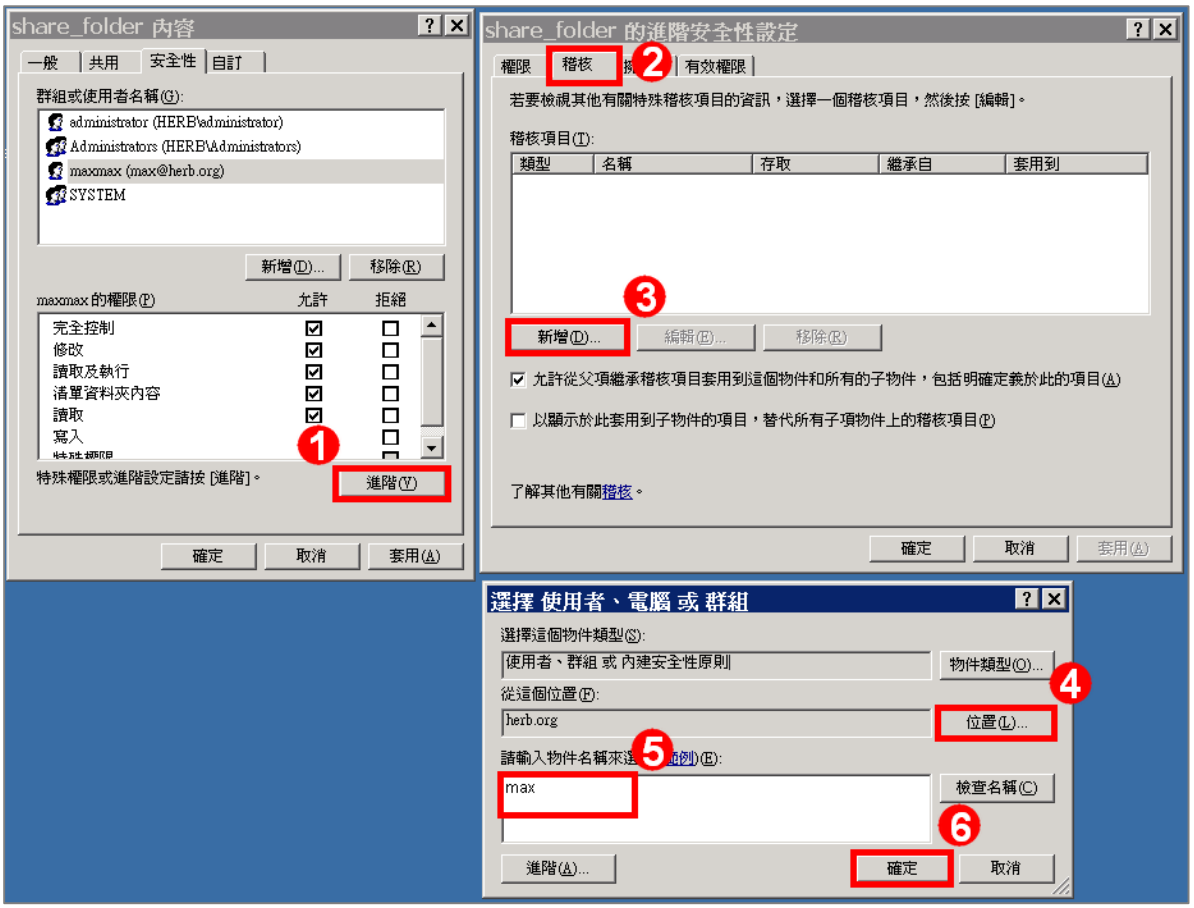
(2) 點選 [稽核] 索引標籤。

(3) 點選 [新增]，來新增一使用者。

(4) 若要選擇其他網域，可點選 [位置]。

(5) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

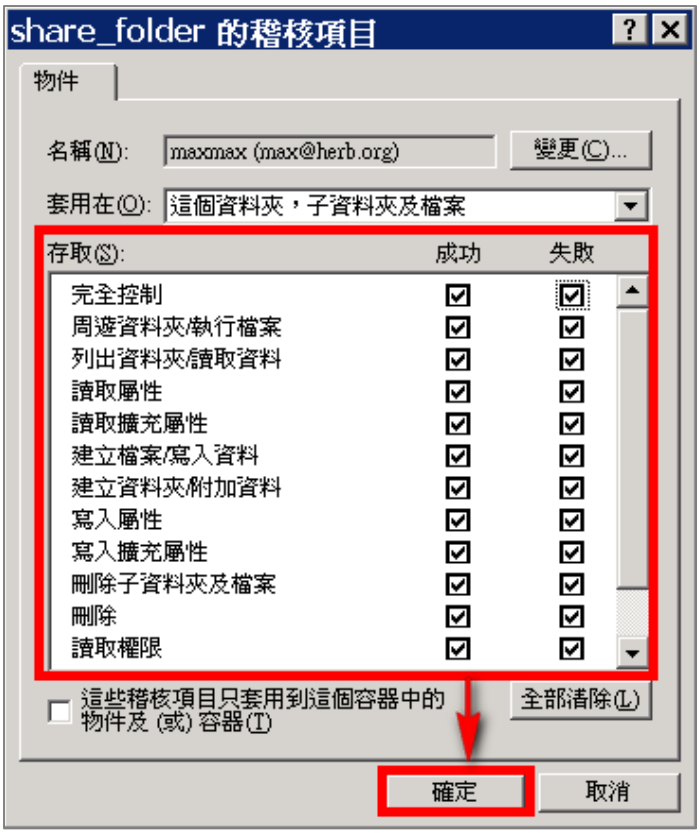
(6) 若網域使用者帳號存在的話，按 [確定] 完成設定。



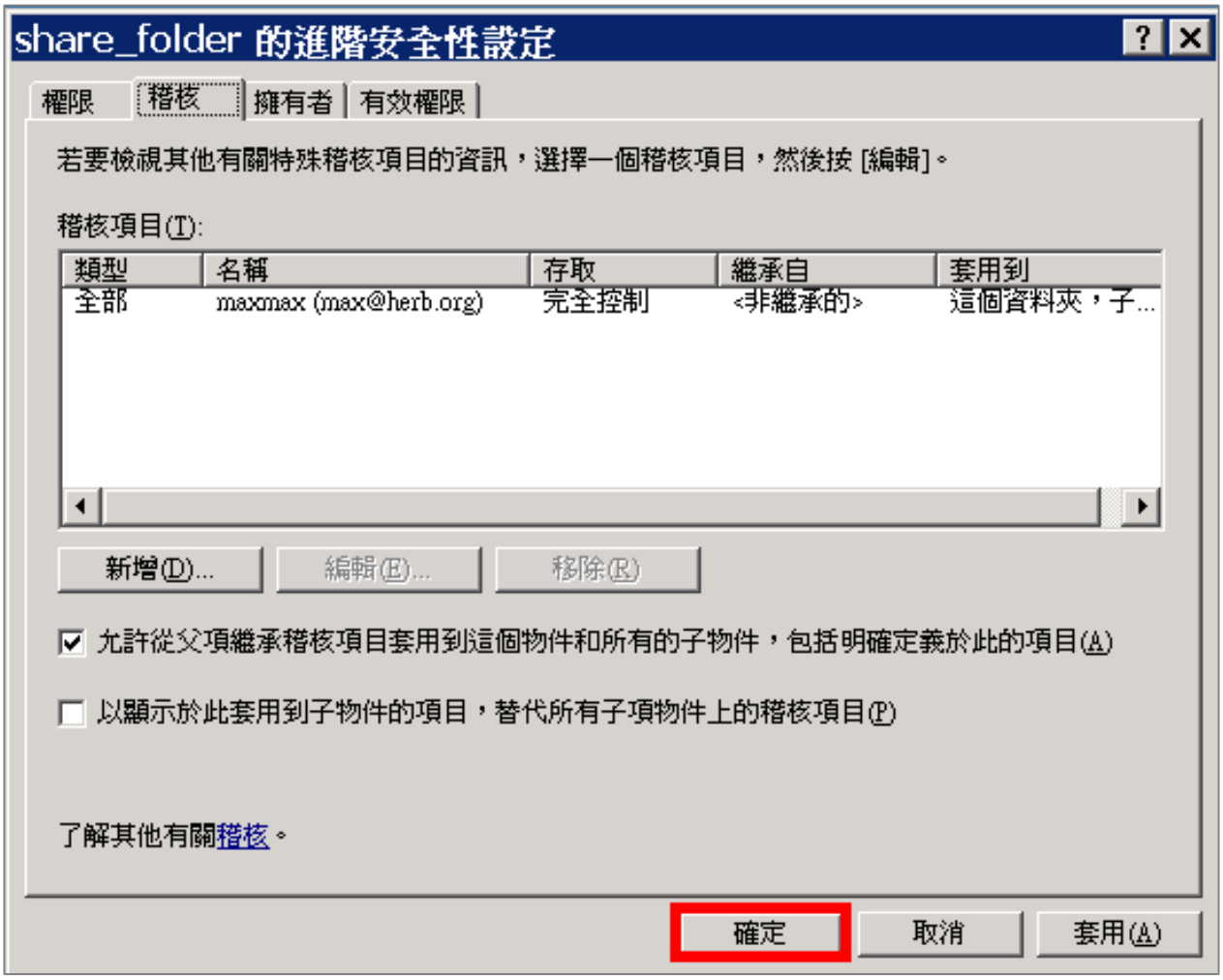
8. 稽核項目設定：

點選並編輯稽核項目清單內所要的稽核項目

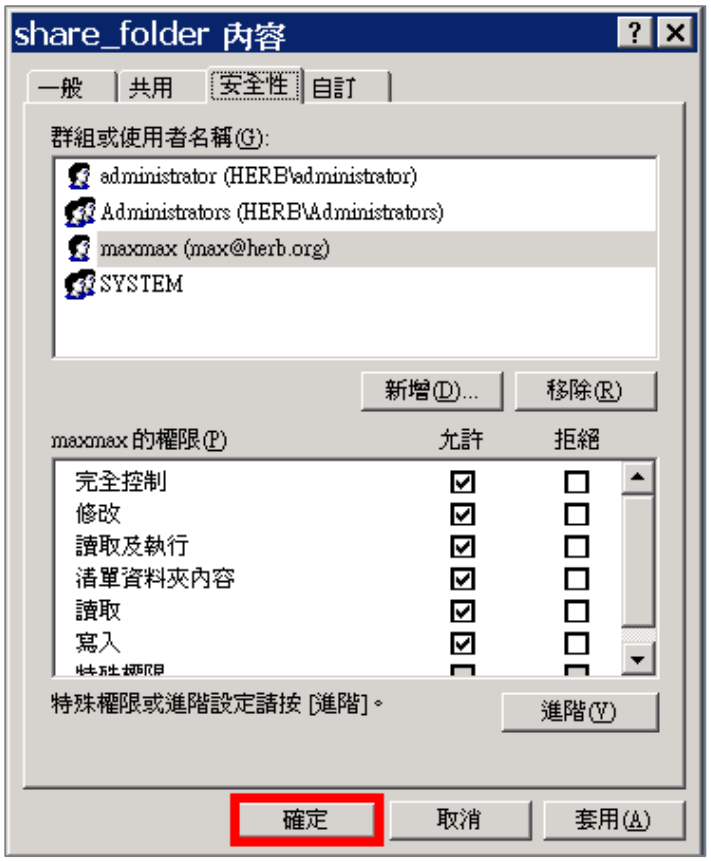
勾選該稽核項目的 [成功] 及 [失敗]的項目，設定完成後按 [確定]。



9. 在進階安全性設定完成後，點選 [確定]。

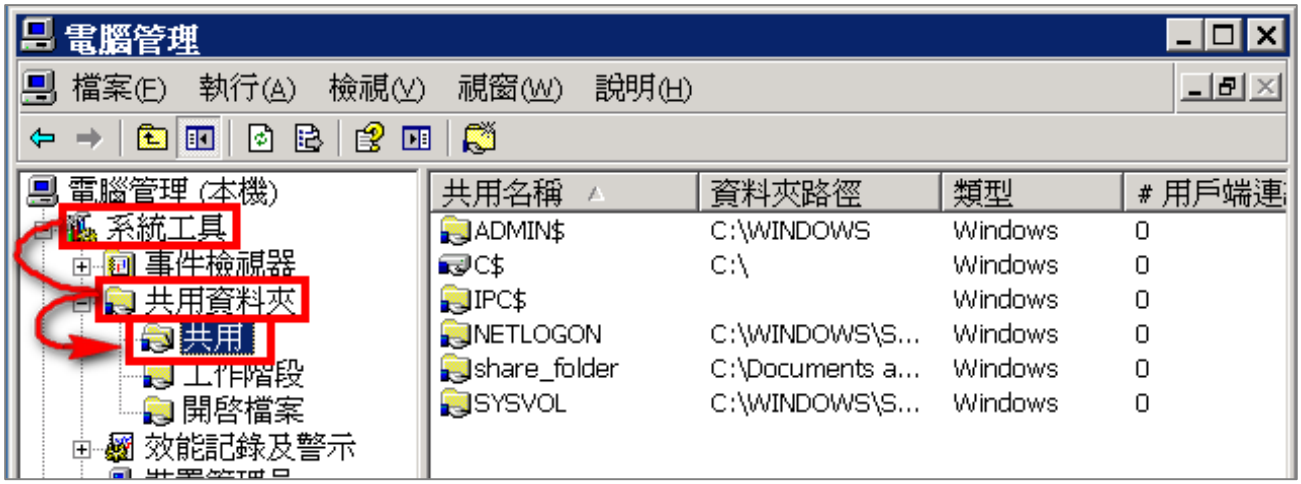


在分享資料夾設定完成後，點選 [確定]。

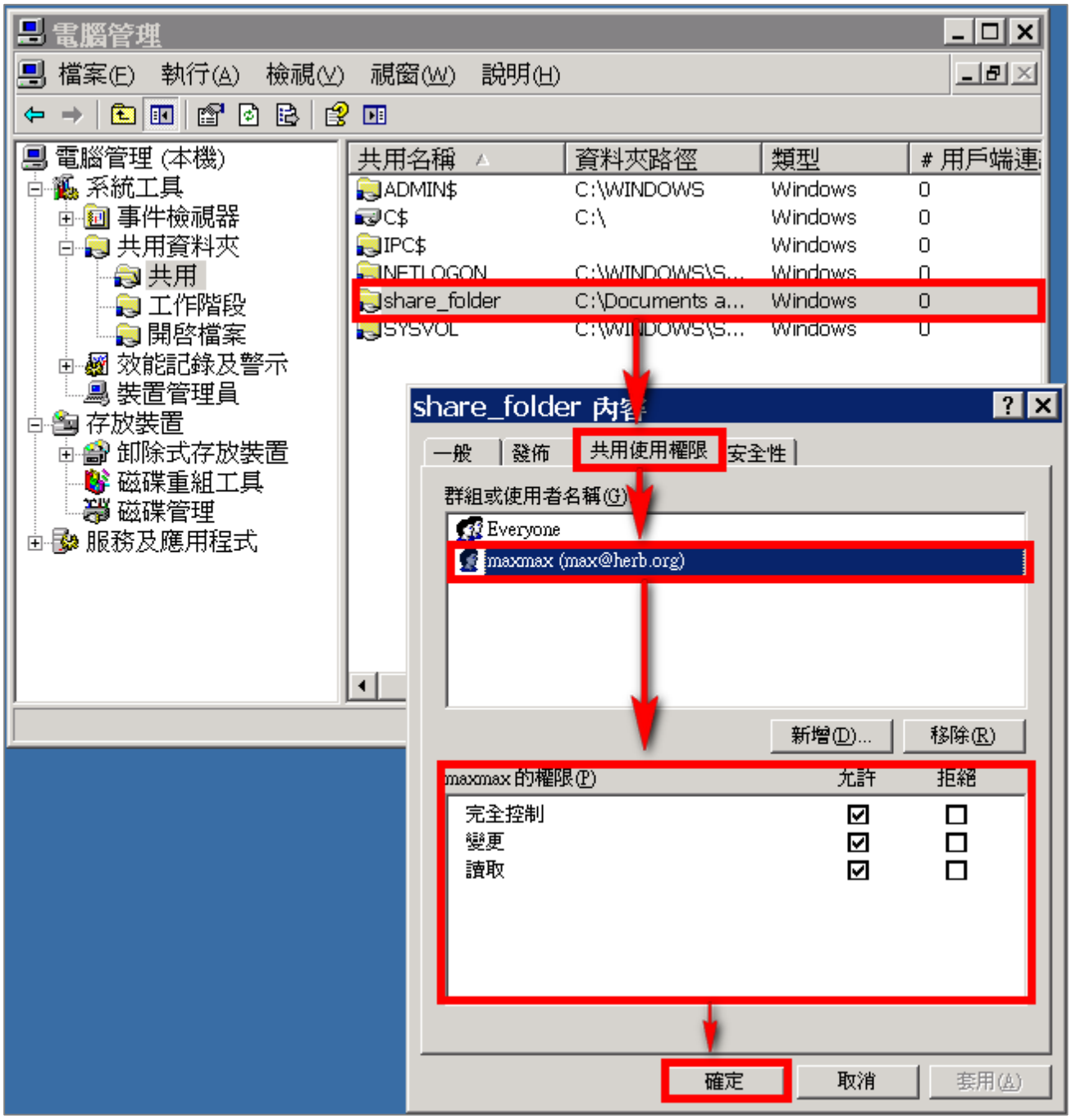


10. 點選 [開始功能表 / 所有程式 / 系統管理工具 / 電腦管理]。

11. 點選 [系統工具 / 共用資料夾 / 共用]。



12. 滑鼠左鍵雙擊被設定分享的分享資料夾，點選 [共用使用權限] 索引標籤。點選使用者名稱，勾選允許 [完全控制]、[變更] 及 [讀取] 權限，設定完成後按 [確定]。



3 Windows 2008 Active Directory Server 稽核設定

本章節主要說明以下操作設定：

1.設定網域使用者登入登出的稽核原則。2.設定共享資料夾權限與稽核原則。

Windows 2008 AD Server 登入登出的稽核原則和目錄分享的稽核原則，預設是關閉的。

安裝 NXLOG 的步驟，詳細請參閱第一章節。

3.1設定網域使用者登入登出的稽核原則

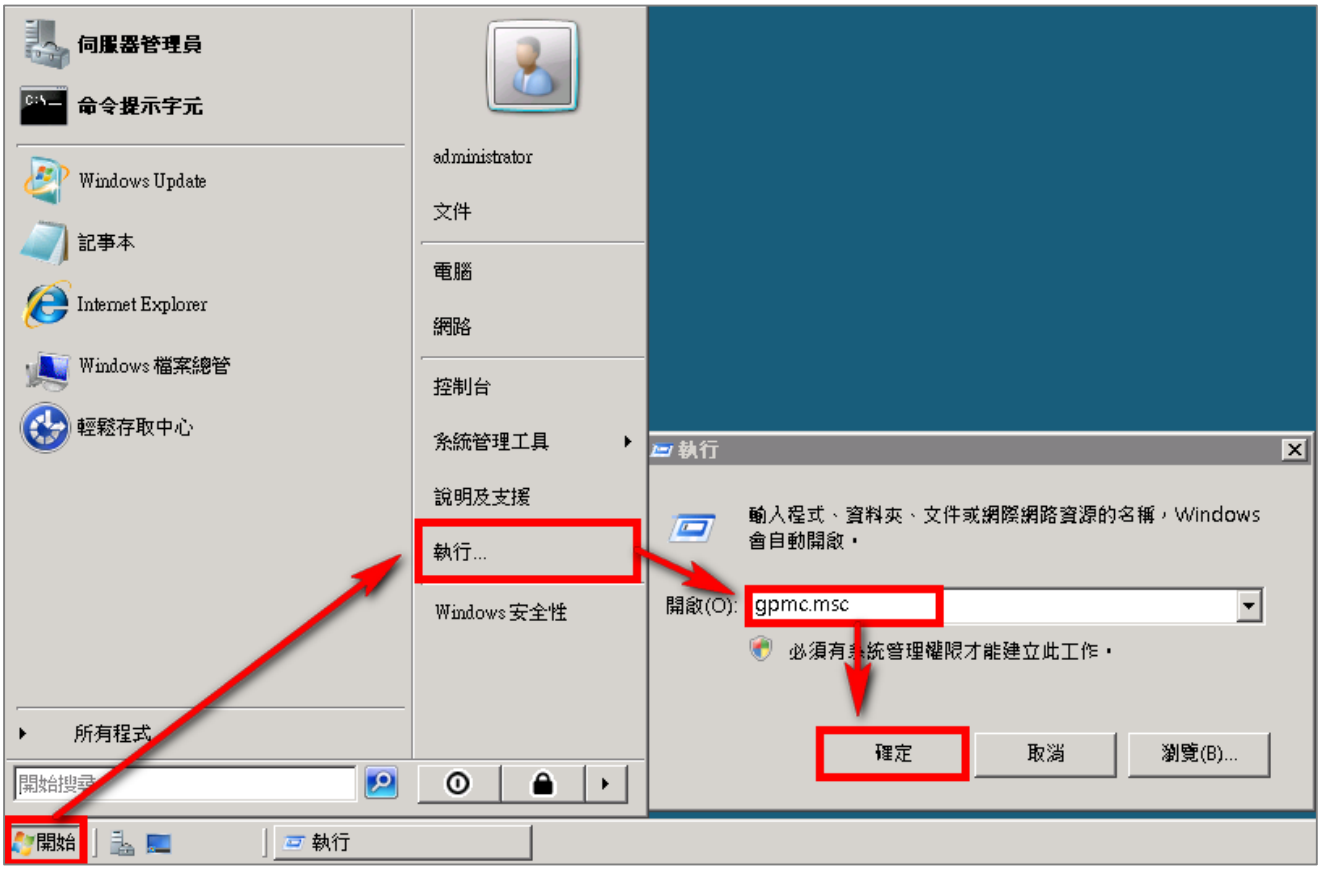
設定步驟如下：

1. 以**全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分**登入 Windows 2008 AD Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用)

   開啟群組原則管理。

   點選[開始功能表 / 執行]。

   輸入：**gpmc.msc** ，完成後按 [確定]。



註: 若出現"Windows 找不到'gpmc.msc' "的訊息，請依下面步驟安裝 群組原則管理 (gpmc)

1. 以系統管理員身分開啟命令提示字元。

2. 在命令提示字元，輸入 ServerManagerCmd -install gpmc。

3. 安裝完成時請關閉命令提示字元。

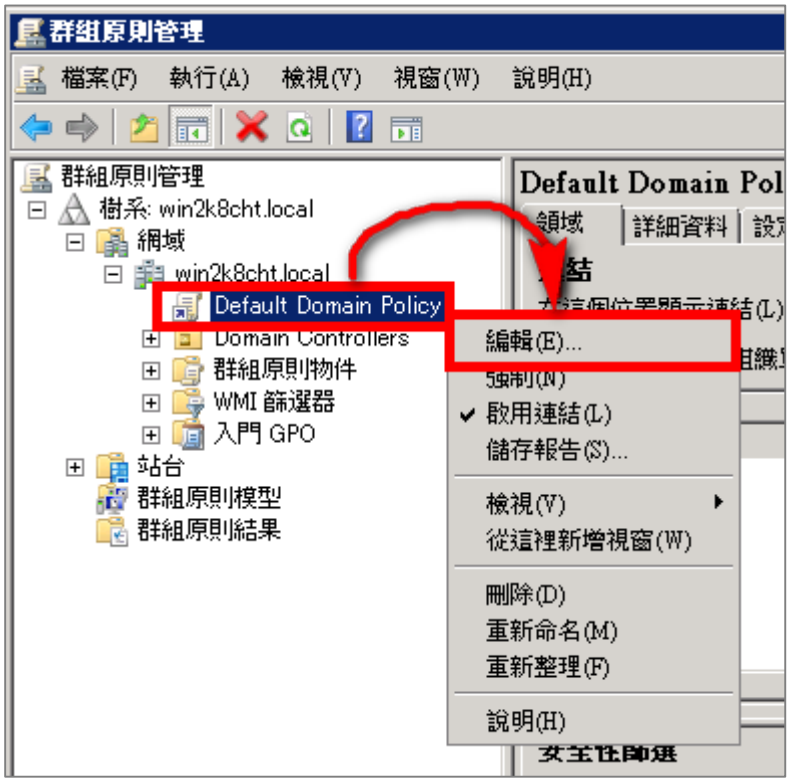
2. 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / win2k8cht.local / Default Domain Policy]。

註：此步驟展開 網域，會有 [Default Domain Policy] (預設網域安全性原則)；

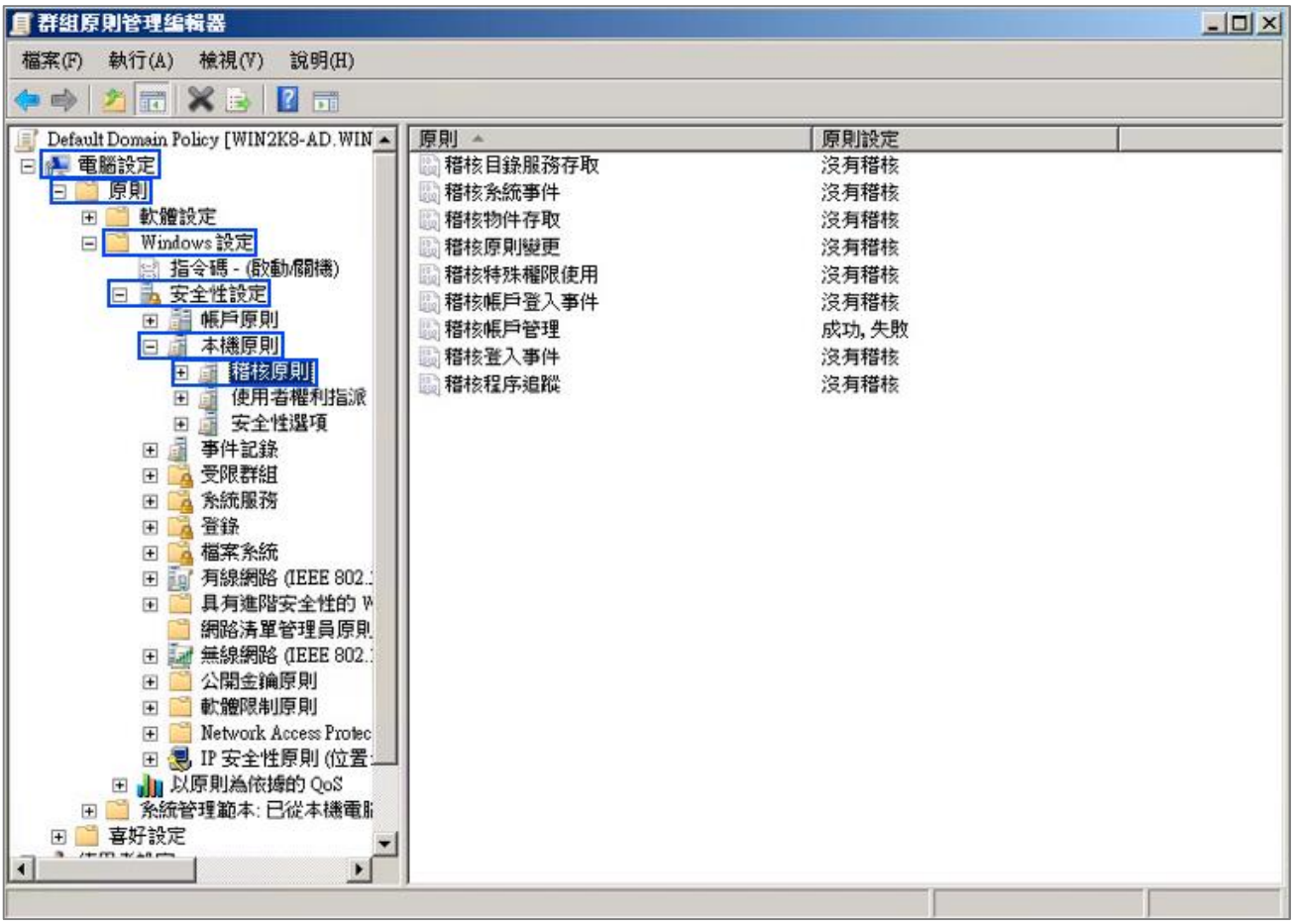
另外展開 Domain Controllers(網域控制站)，會有 [Default Domain Controllers Policy] (預設網域控制站安全性原則)。

建議將此兩種安全性稽核原則設定為一致

3. 在 Default Domain Policy 點擊滑鼠右鍵，點選 [編輯]。



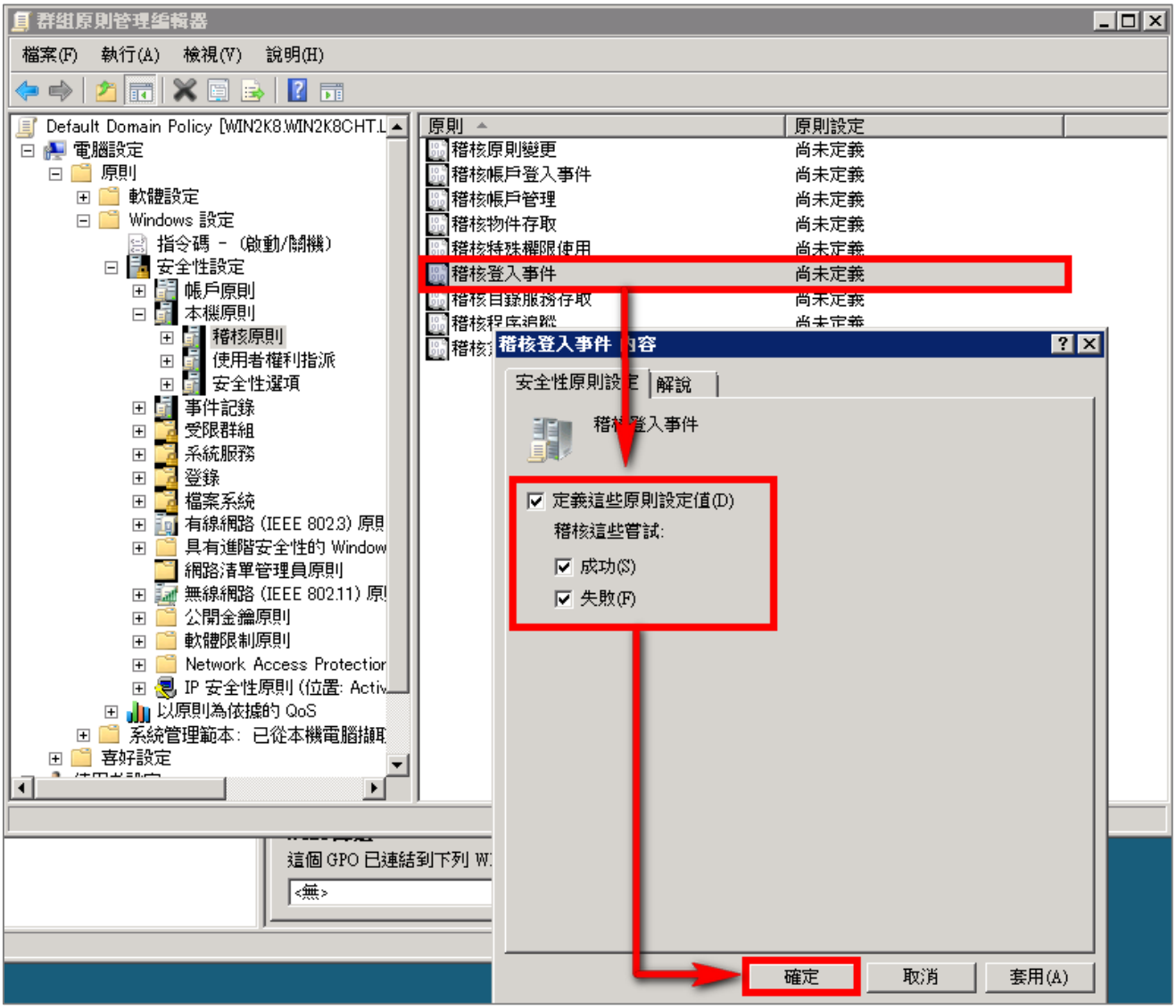
4. 展開 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 點選 稽核原則]。



5. 定義下列的原則設定值：

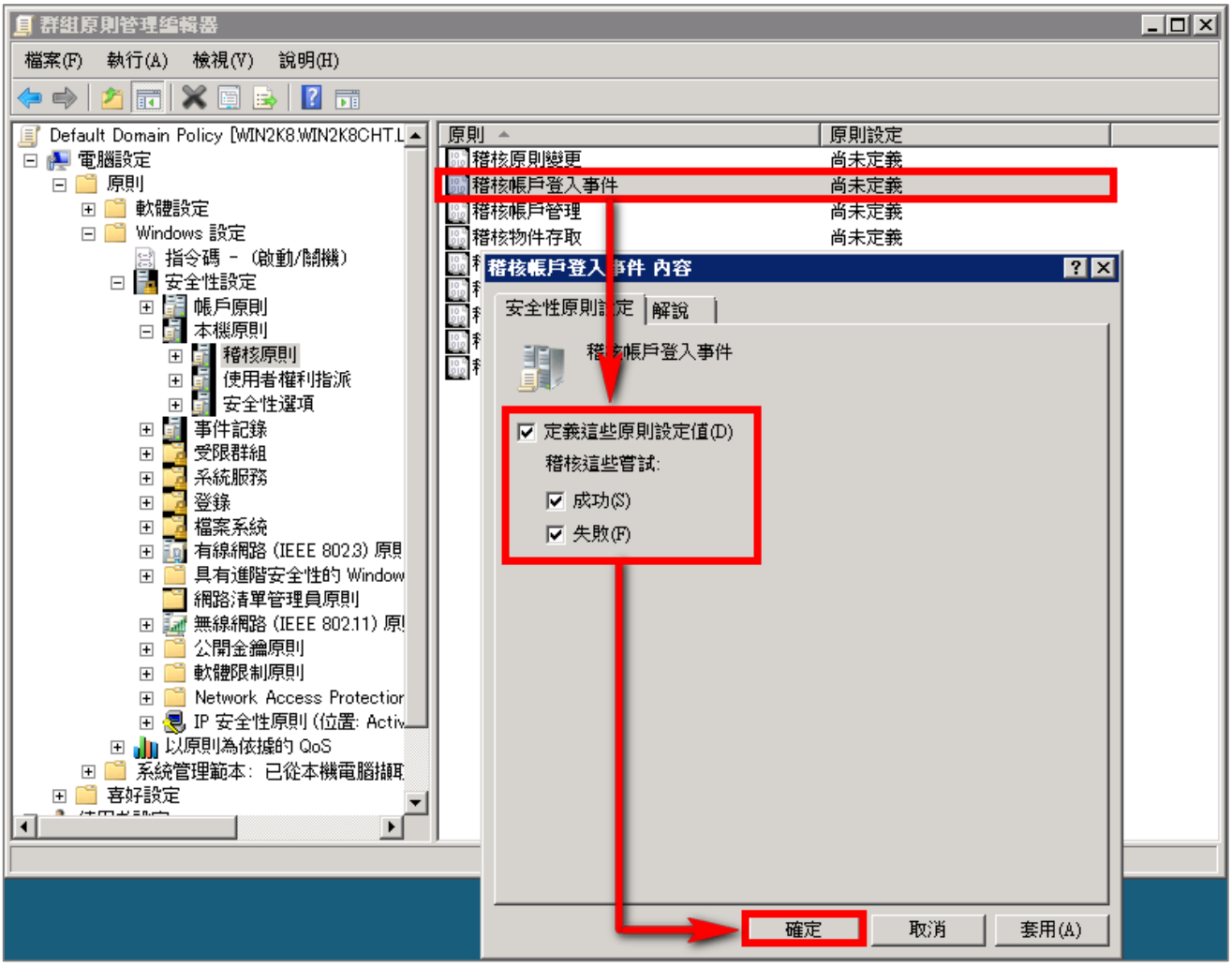
(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(2) 稽核帳戶登入事件：

滑鼠雙擊 [稽核帳戶登入事件]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核物件存取：

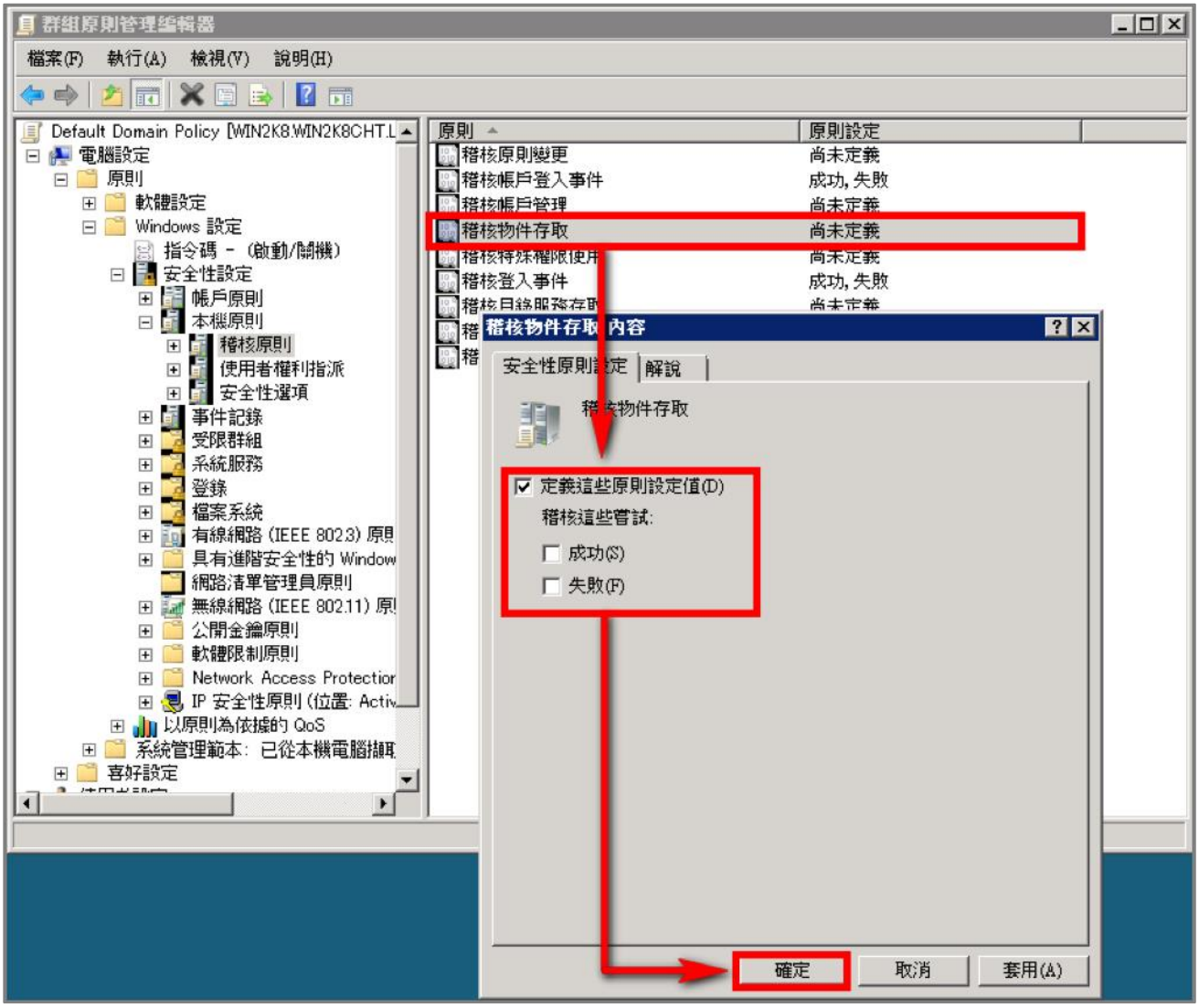
滑鼠雙擊 [稽核物件存取]，勾選 [定義這些原則設定值]

成功：若欲稽核成功事件的 Log，請勾選 [成功] 核取方塊。

失敗：若欲稽核失敗事件的 Log，請勾選 [失敗] 核取方塊。

設定完成後按 [確定]。

註：若 Windows 2008 Active Directory Server 不做檔案伺服器稽核 (File server audit)，建議不要勾選成功與失敗的設定值，僅需勾選[定義這些原則設定值] 即可. 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter，會影響主機的運作效能



(4) 稽核原則變更：

滑鼠雙擊 [稽核原則變更]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

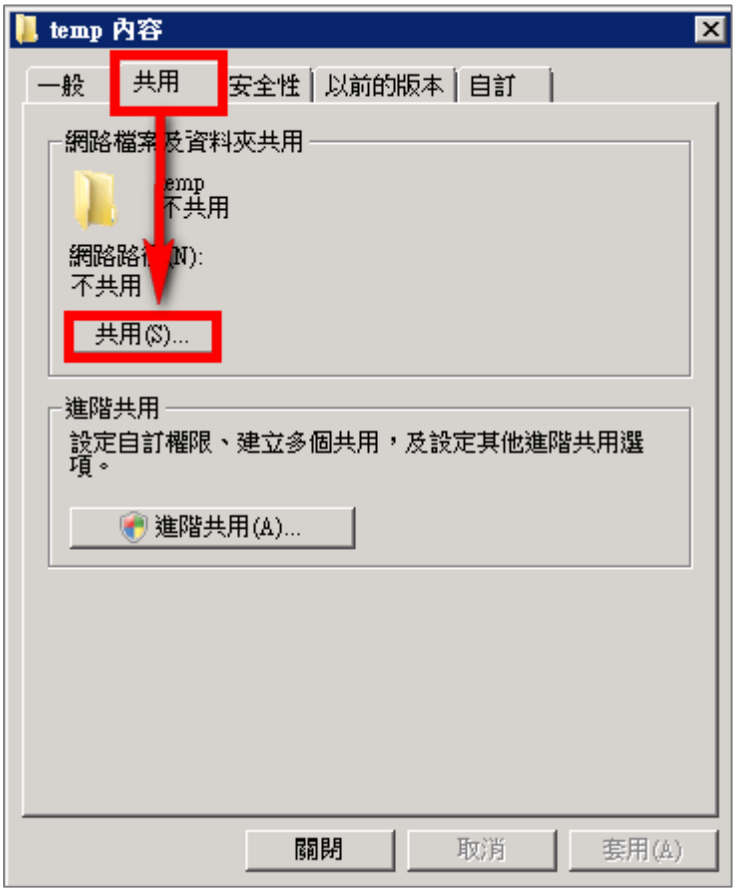
(5) 稽核帳戶管理：

滑鼠雙擊 [稽核帳戶管理]，勾選 [定義這些原則設定值]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

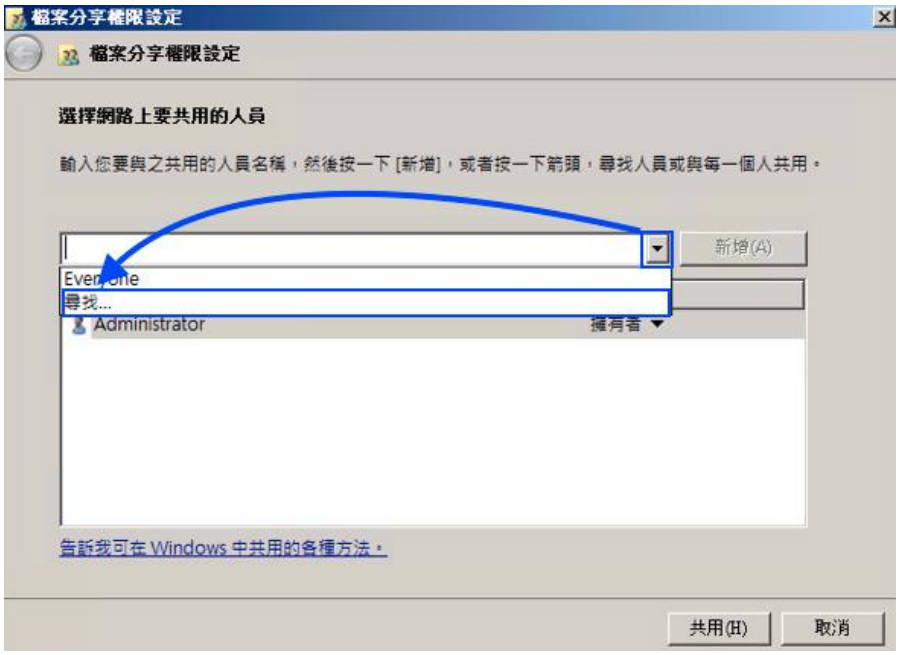
3.2設定共享資料夾權限與稽核原則

設定步驟如下：

1. 在欲共用的資料夾上點擊滑鼠右鍵，點選 [內容]。
2. 點選 [共用] 索引標籤，點選 [共用]。



3. 在檔案分享權限設定中，點下拉選單至 [尋找]。

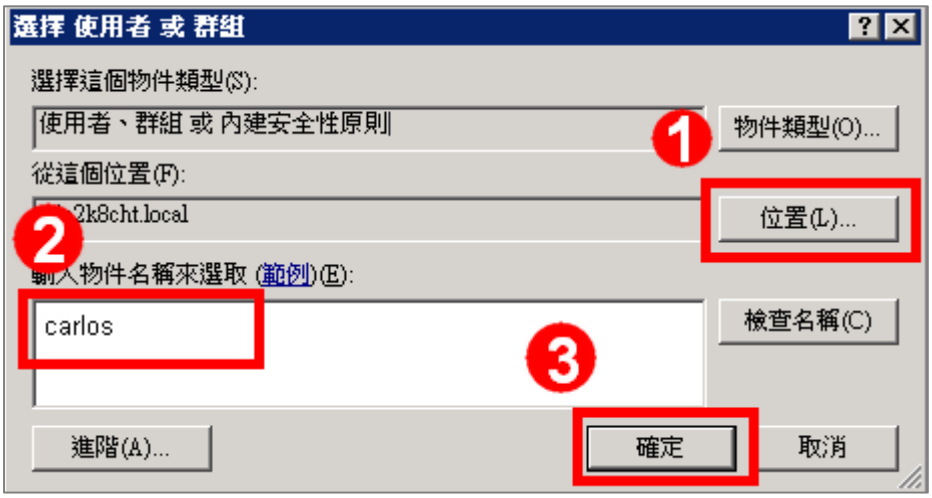


4. 使用者設定：

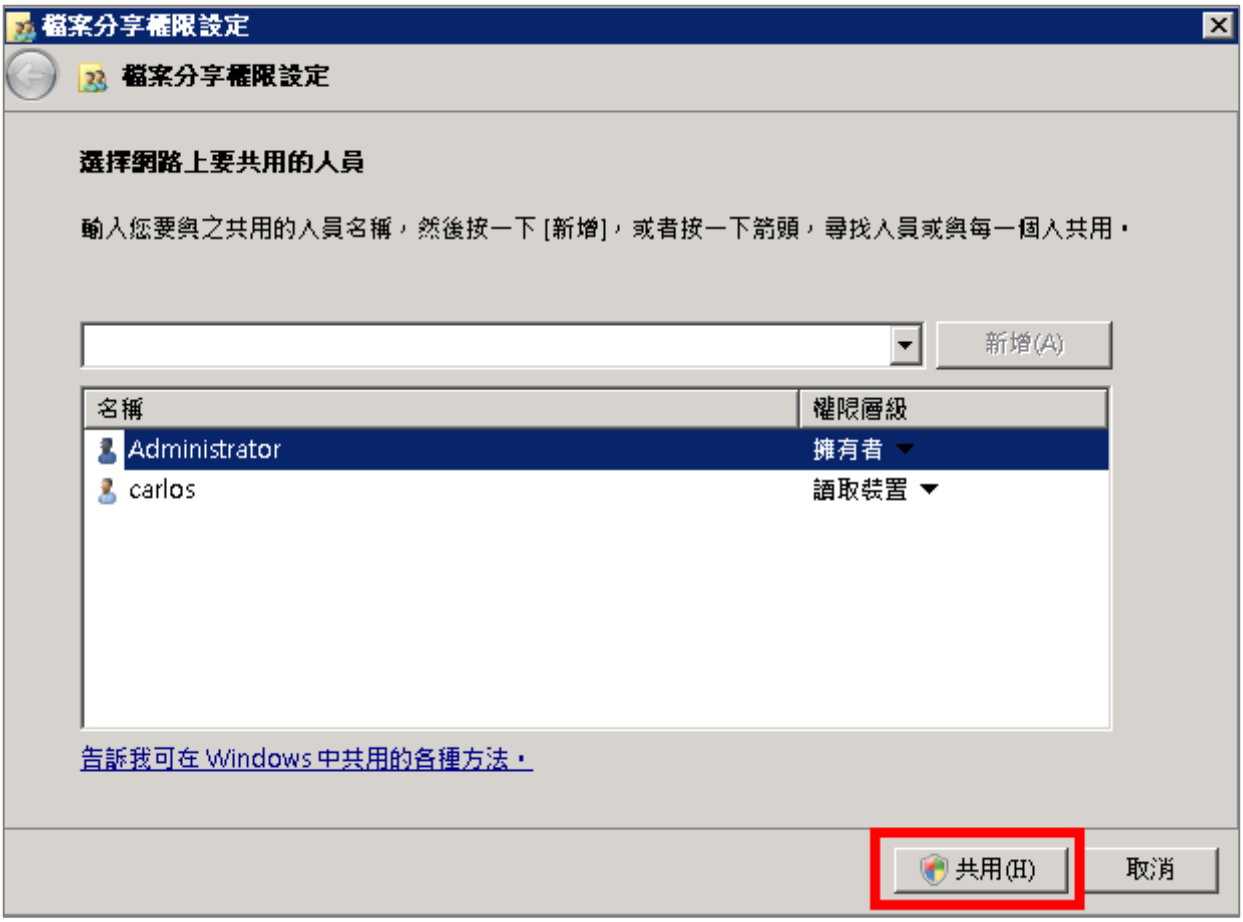
(1) 若要選擇其他網域，可點選 [位置]。

(2) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

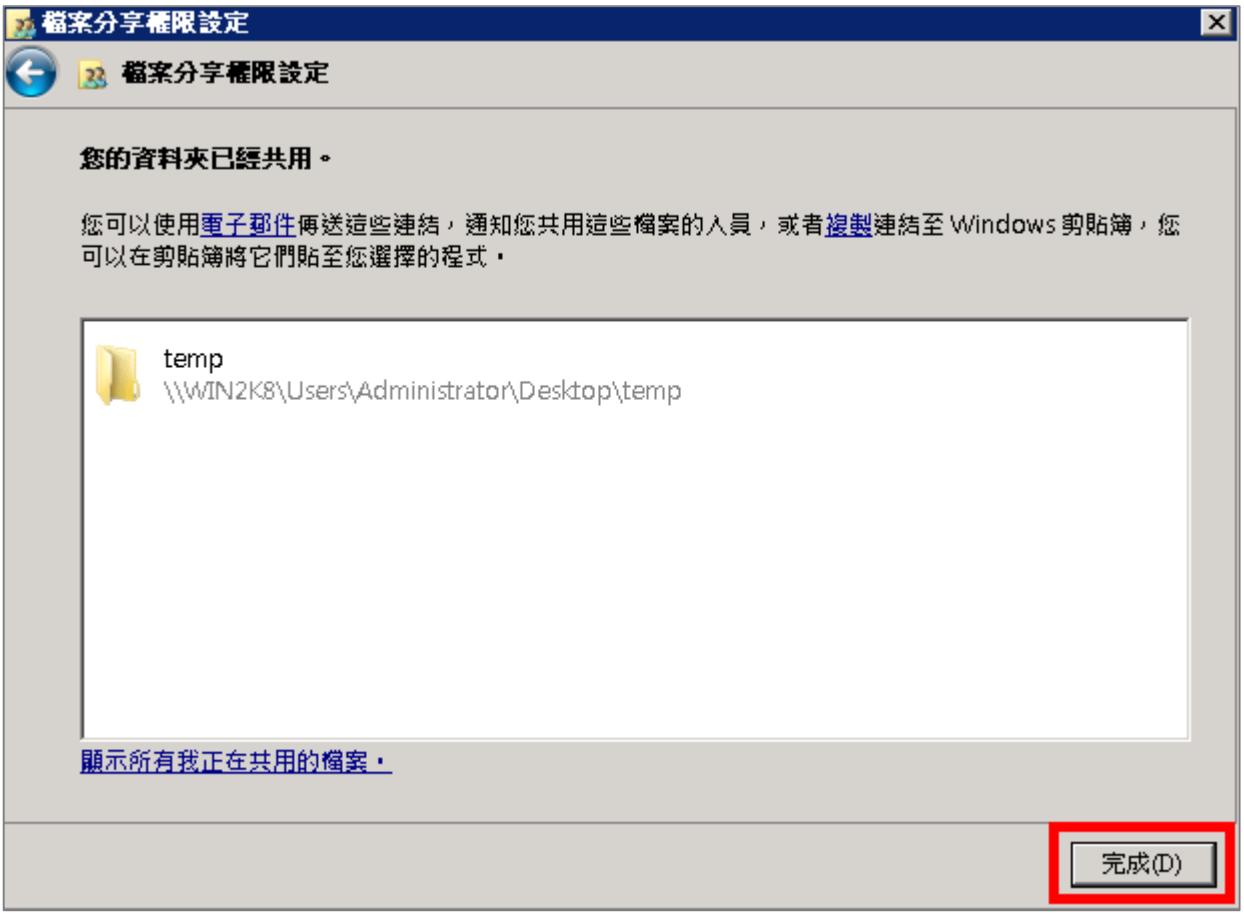
(3) 若網域使用者帳號存在的話，按 [確定] 完成設定。



5. 點選 [共用]。



6. 等待共用設定完成後，再按 [完成]。



7. 安全性設定：

(1) 點選 [安全性] 索引標籤。

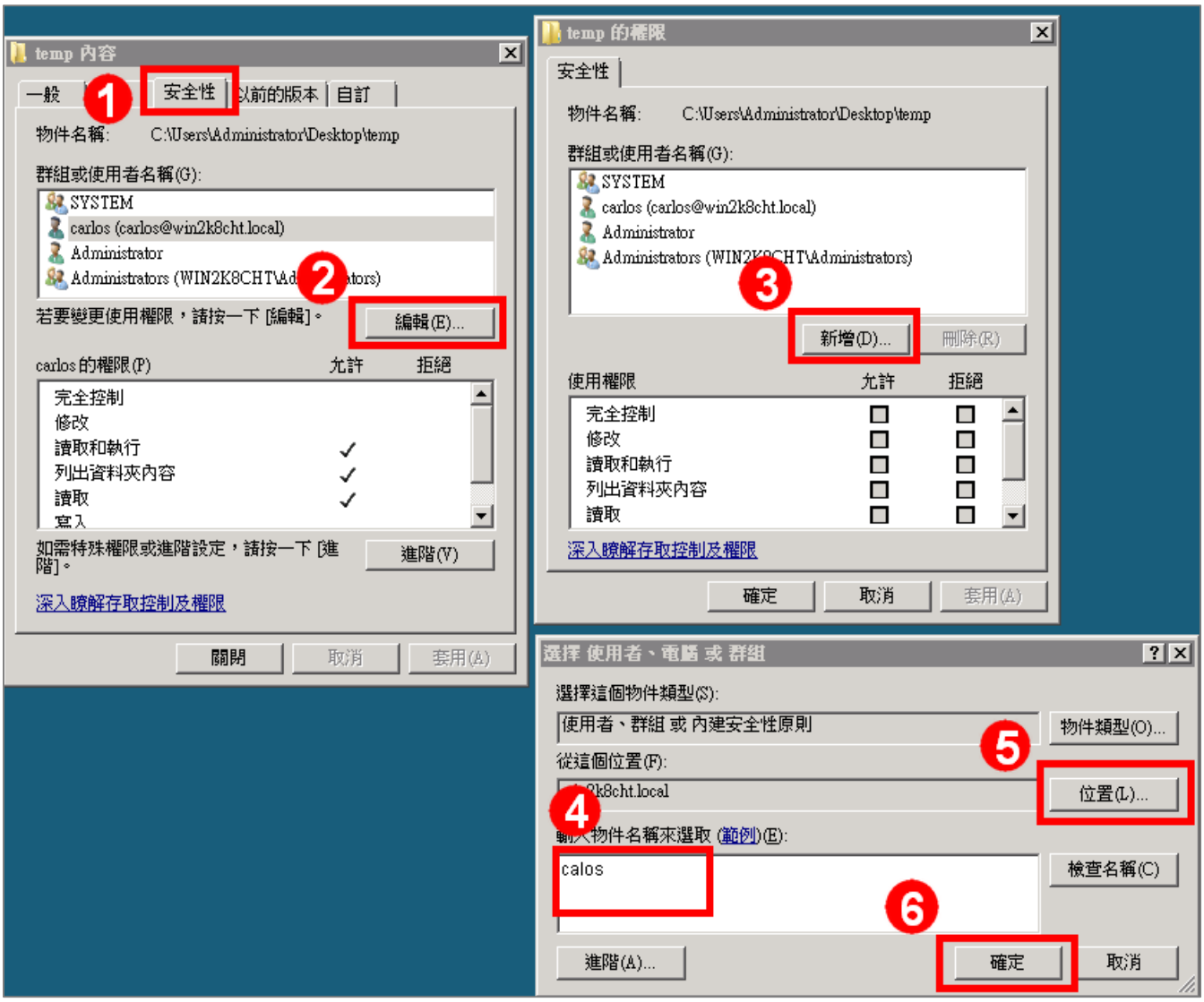
(2) 點選 [編輯]。

(3) 點選 [新增]。

(4) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

(5) 若要選擇其他網域，可點選 [位置]。

(6) 設定完成後按 [確定]。

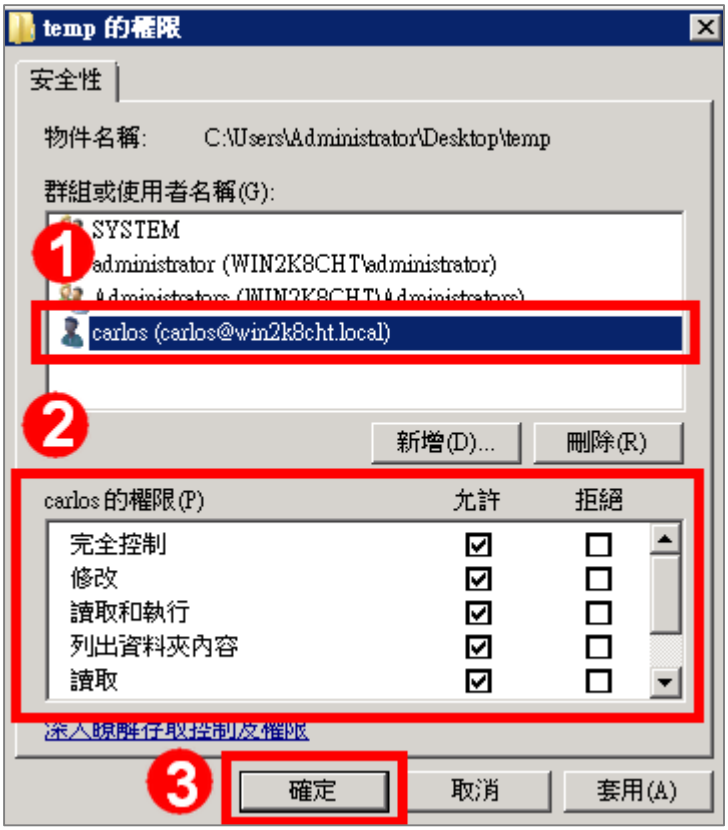


8. 設定使用者權限：

(1) 點選新增的使用者帳號。

(2) 勾選允許 [完全控制] 權限，以取得所有權限。

(3) 設定完成後按 [確定]。



9. 進階安全性設定：

(1) 點選 [進階]。

(2) 點選 [稽核] 索引標籤。

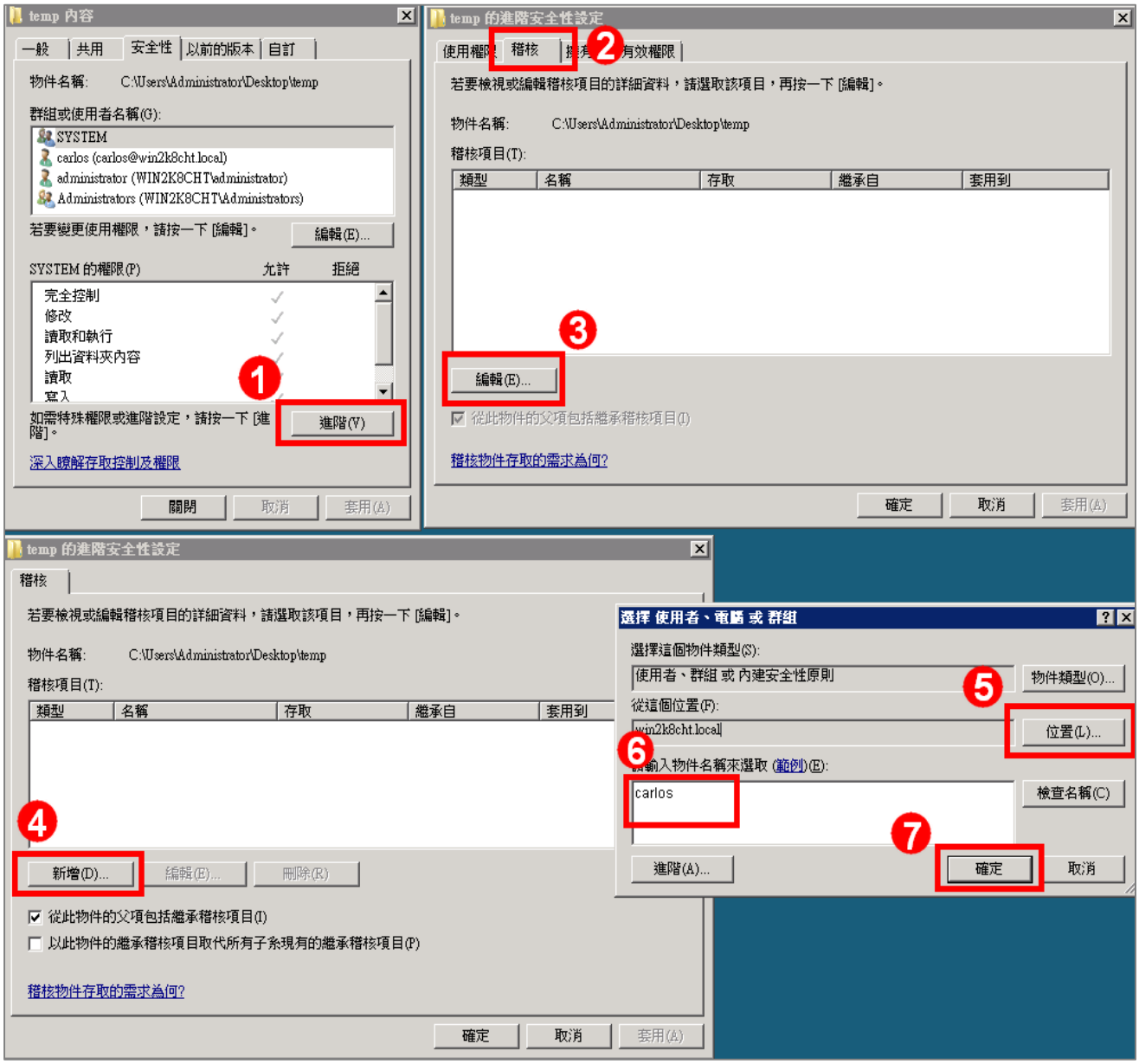
(3) 點選 [編輯]。

(4) 點選 [新增]，來新增一使用者。

(5) 若要選擇其他網域，可點選 [位置]。

(6) 可於此空白處直接輸入已知的網域使用者帳號後，按[檢查名稱]檢查存不存在。

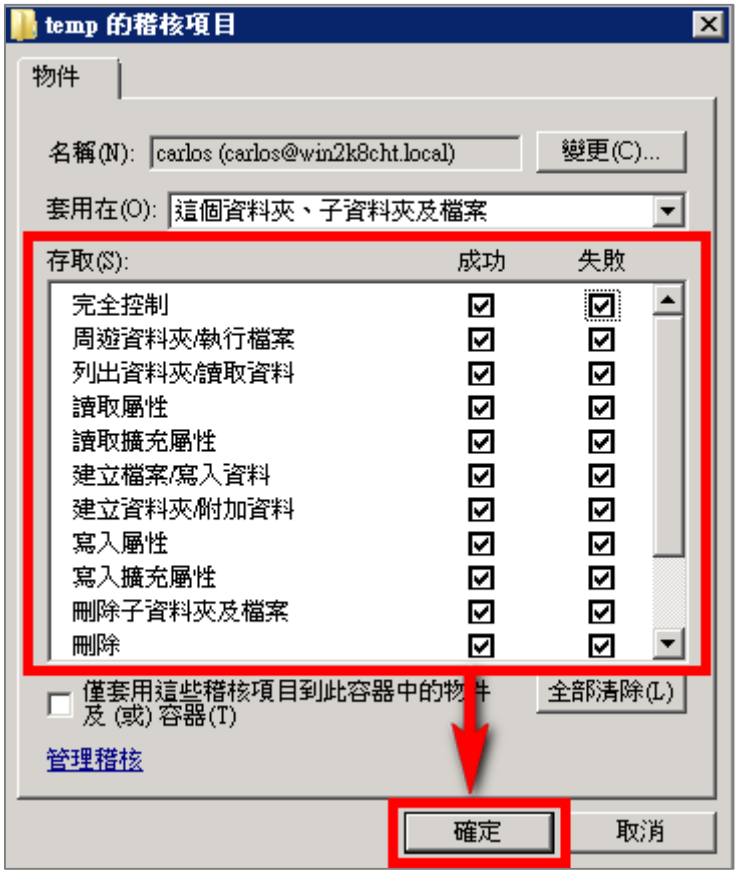
(7) 設定完成後按 [確定]。



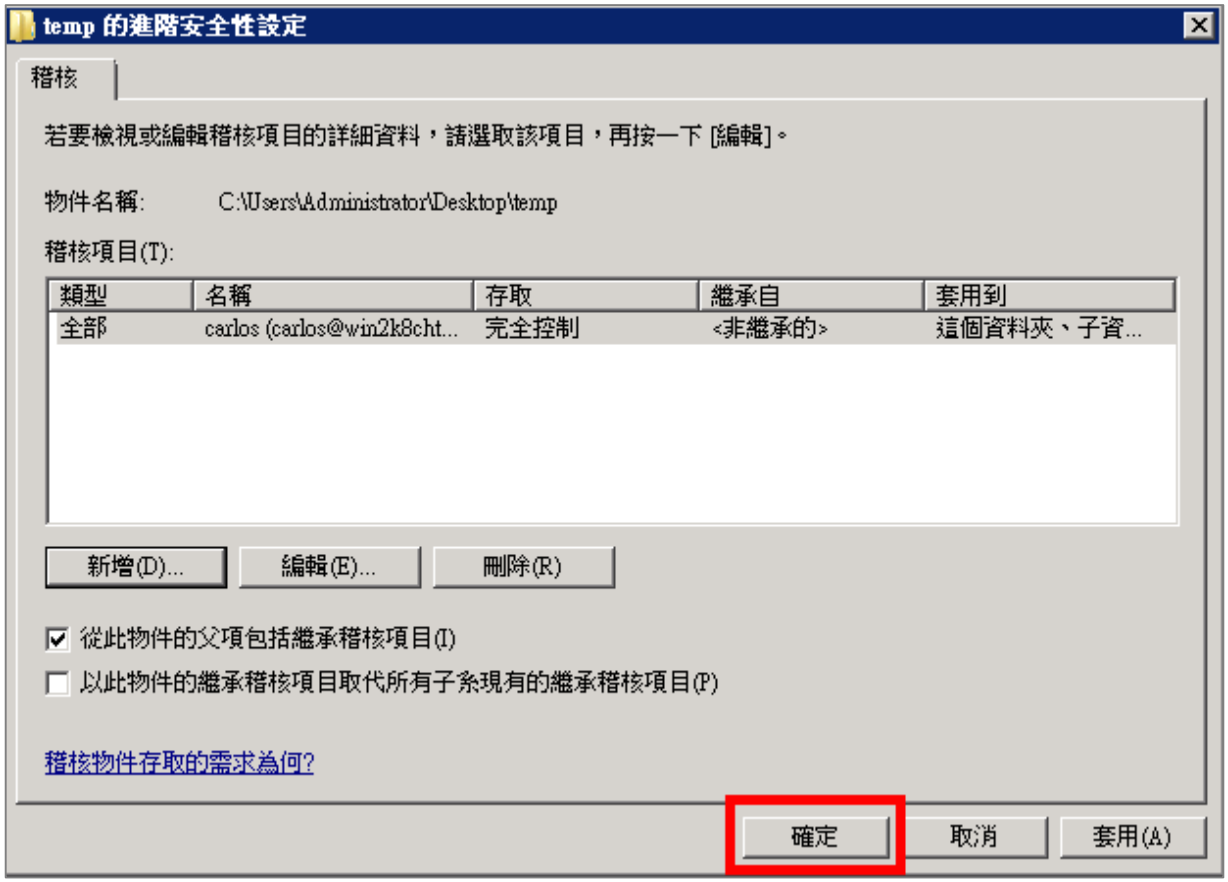
10. 稽核項目設定：

    點選並編輯稽核項目清單內所要的稽核項目

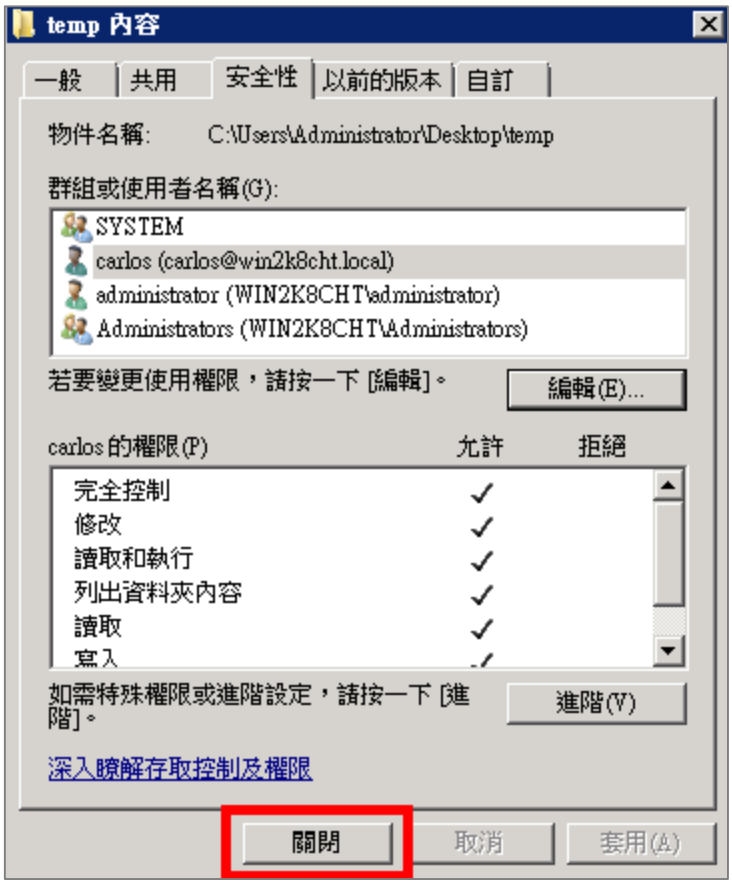
    勾選該稽核項目的 [成功] 及 [失敗]的項目，設定完成後按 [確定]。



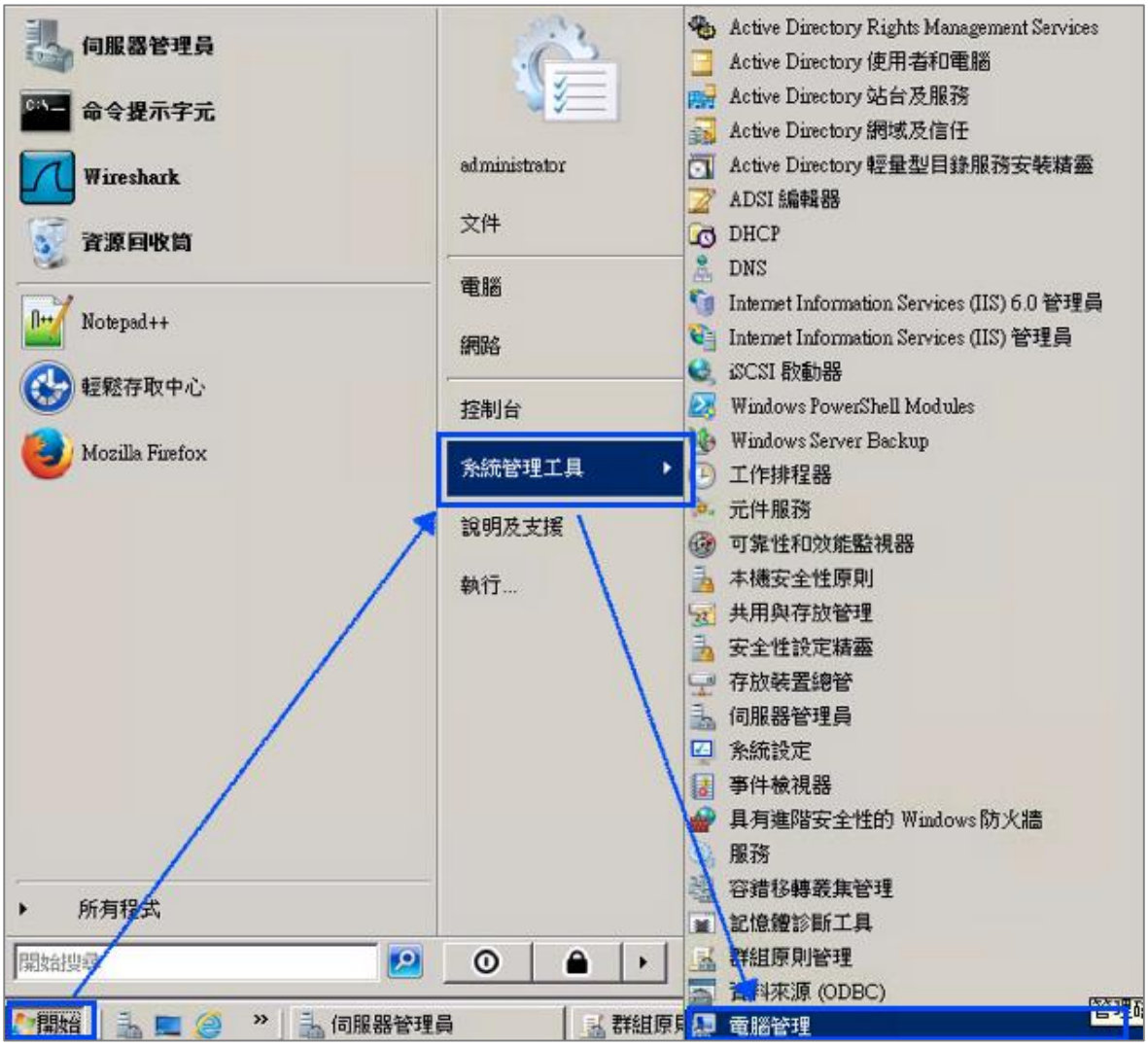
11. 在進階安全性設定完成後，點選 [確定]。



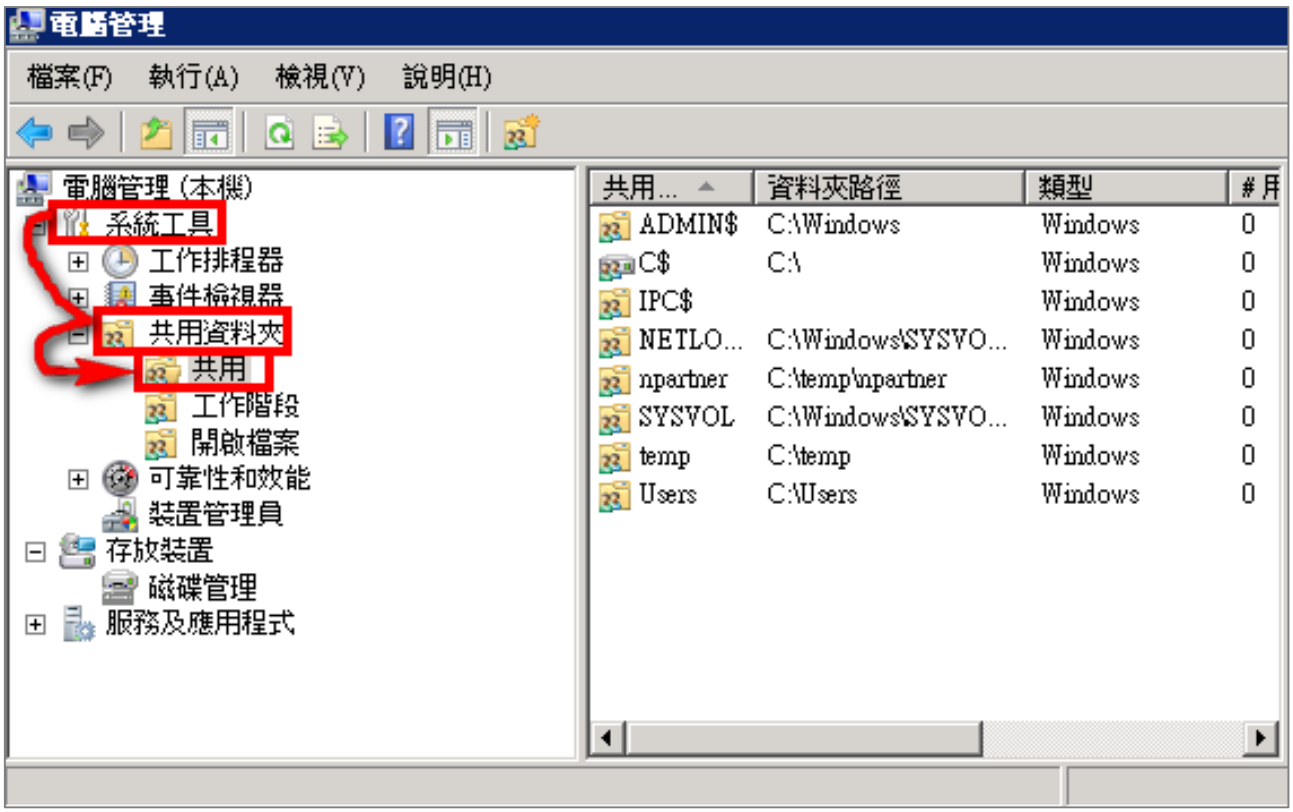
12. 在分享資料夾設定完成後，點選 [關閉]。



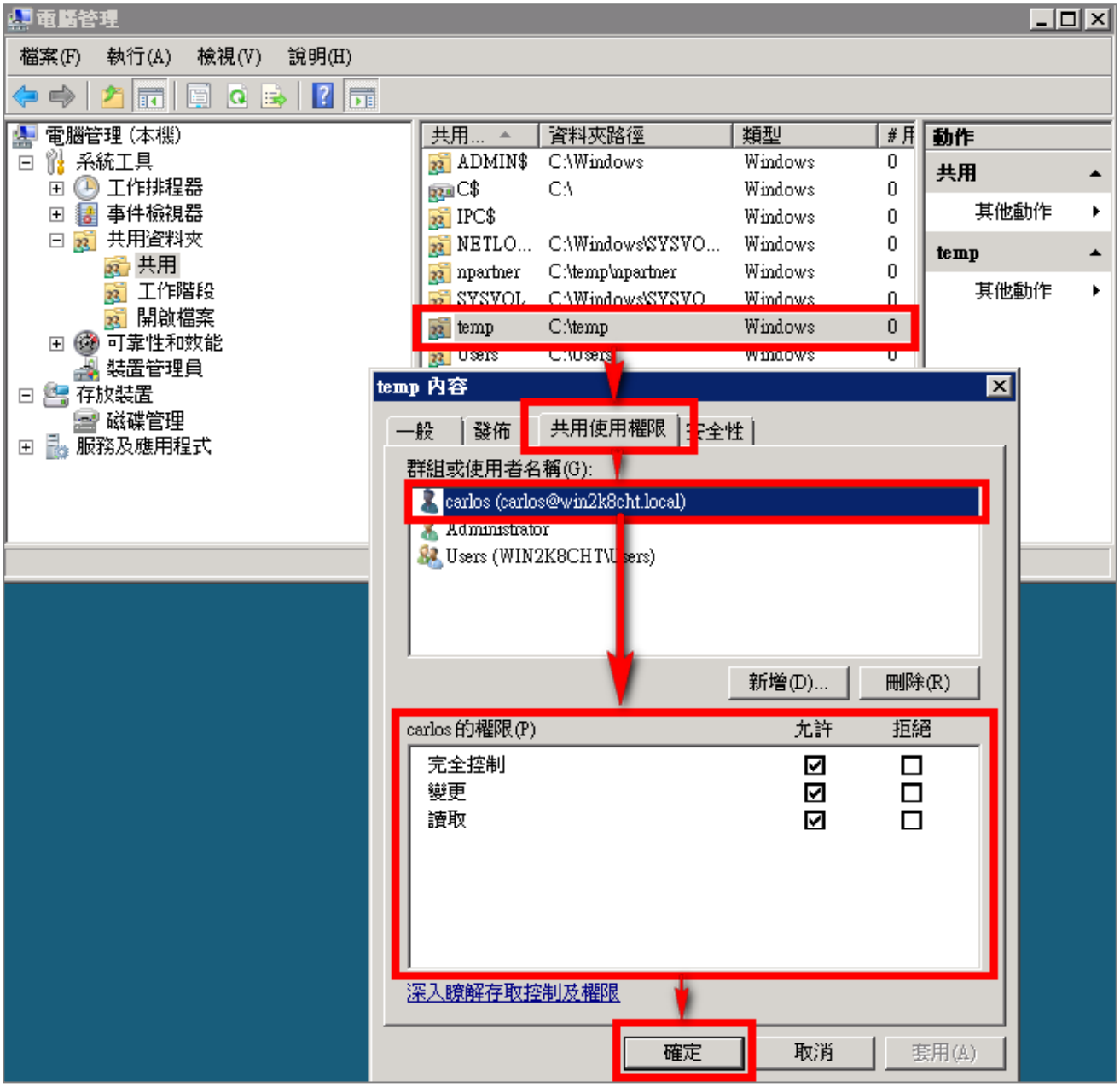
13. 點選 [開始功能表 / 系統管理工具 / 電腦管理]。



14. 點選 [系統工具 / 共用資料夾 / 共用]。



15. 滑鼠左鍵雙擊被設定分享的分享資料夾，點選 [共用使用權限] 索引標籤。點選使用者名稱，勾選允許 [完全控制]、[變更] 及 [讀取] 權限，設定完成後按 [確定]。



4 Windows 2012 Active Directory Server 稽核設定

本章節主要說明以下操作設定：

1.設定網域使用者登入登出的稽核原則。2.設定共享資料夾權限與稽核原則。

Windows 2012 AD Server 登入登出的稽核原則和目錄分享的稽核原則，預設是關閉的。

安裝 NXLOG 的步驟，詳細請參閱第一章節。

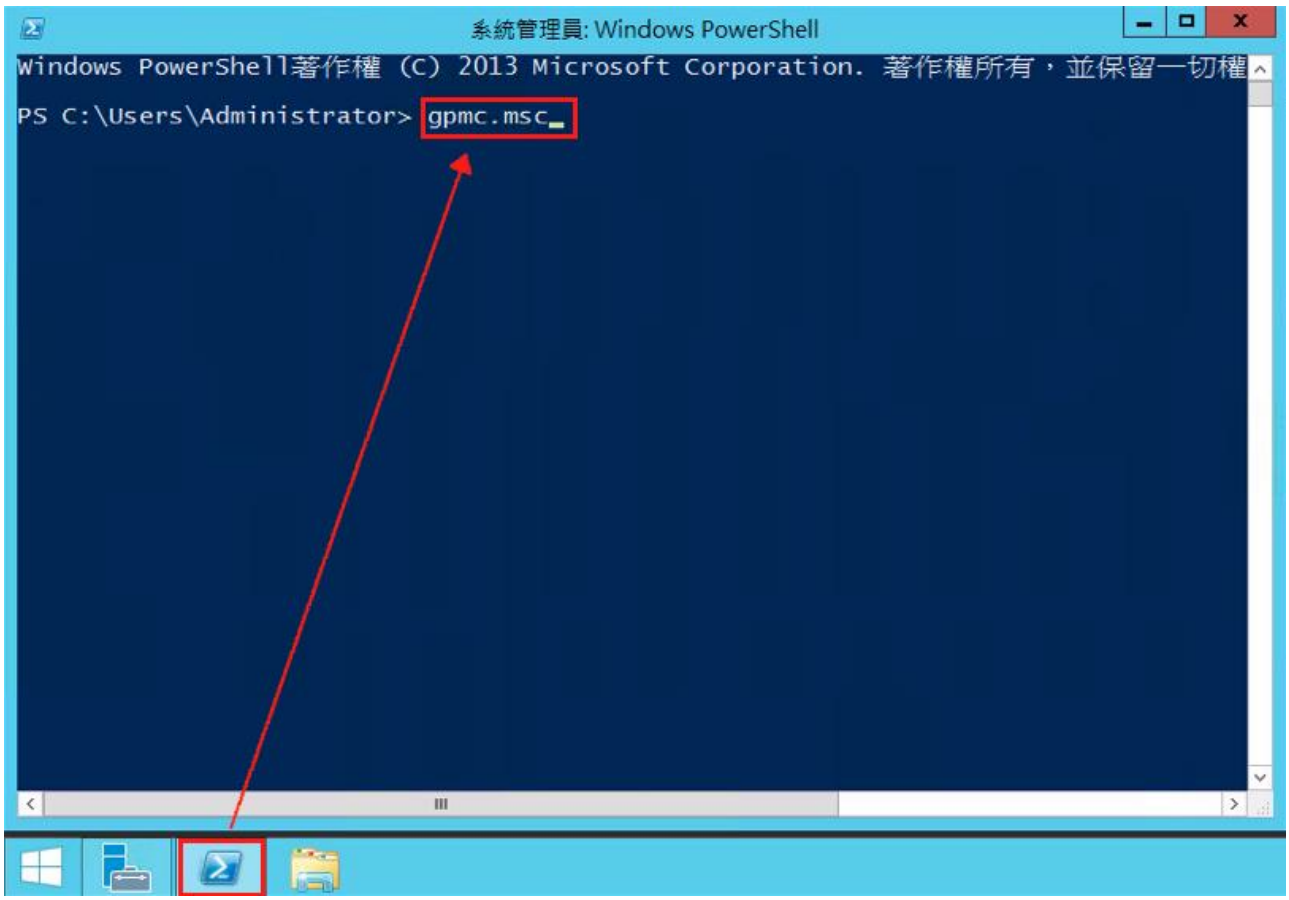
4.1設定網域使用者登入登出的稽核原則

設定步驟如下：

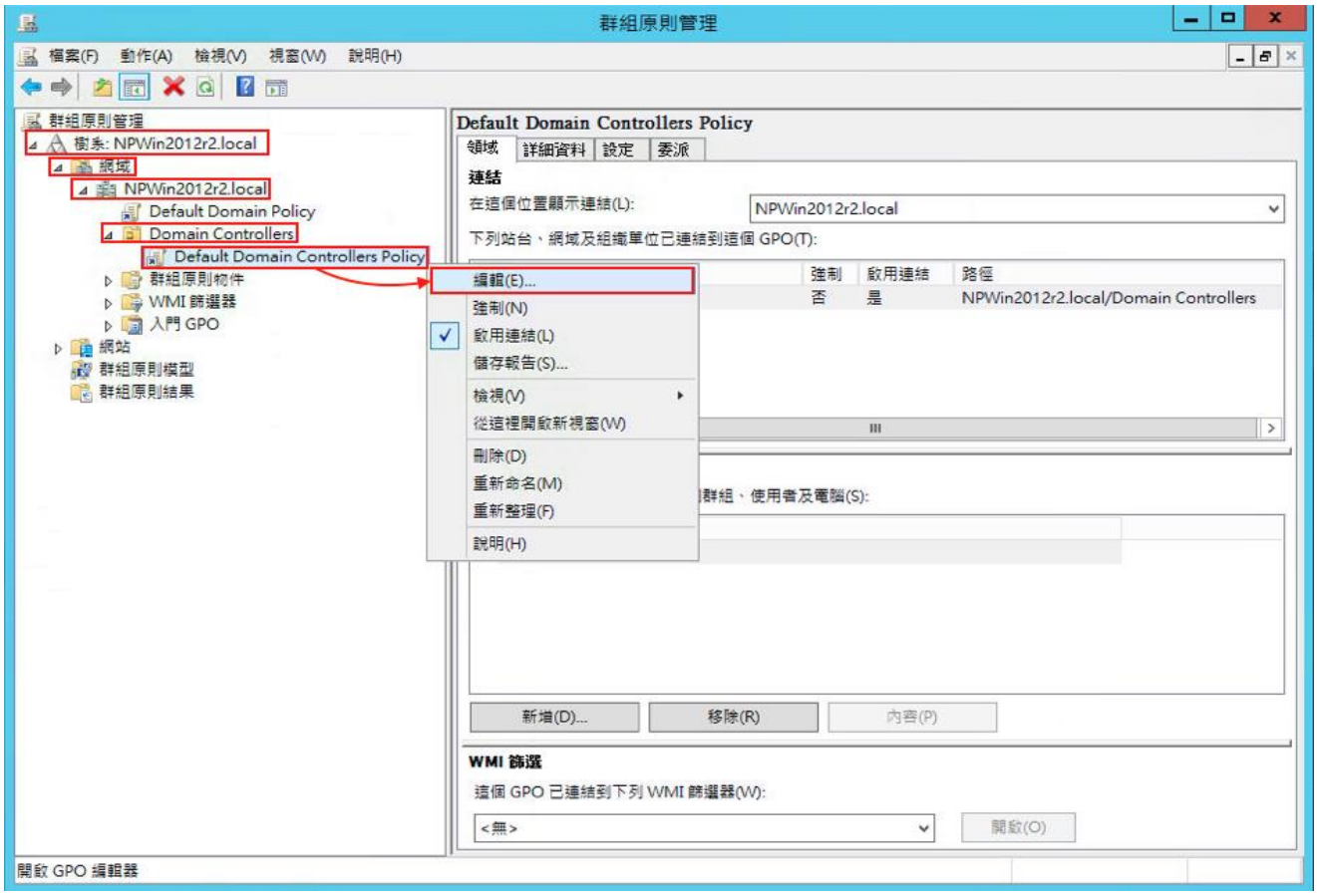
1. 以**全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分**登入 Windows 2012 Active Directory Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用)

   開啟群組原則管理:

   點選[Windows PowerShell]，輸入：**gpmc.msc** ，完成後按 [Enter]



2. 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / NPWin2012r2.local / Domain Controllers / Default Domain Controllers Policy]。
3. 滑鼠右鍵點選[Default Domain Controllers Policy]，按 [編輯]，開啟[群組原則管理編輯器]。

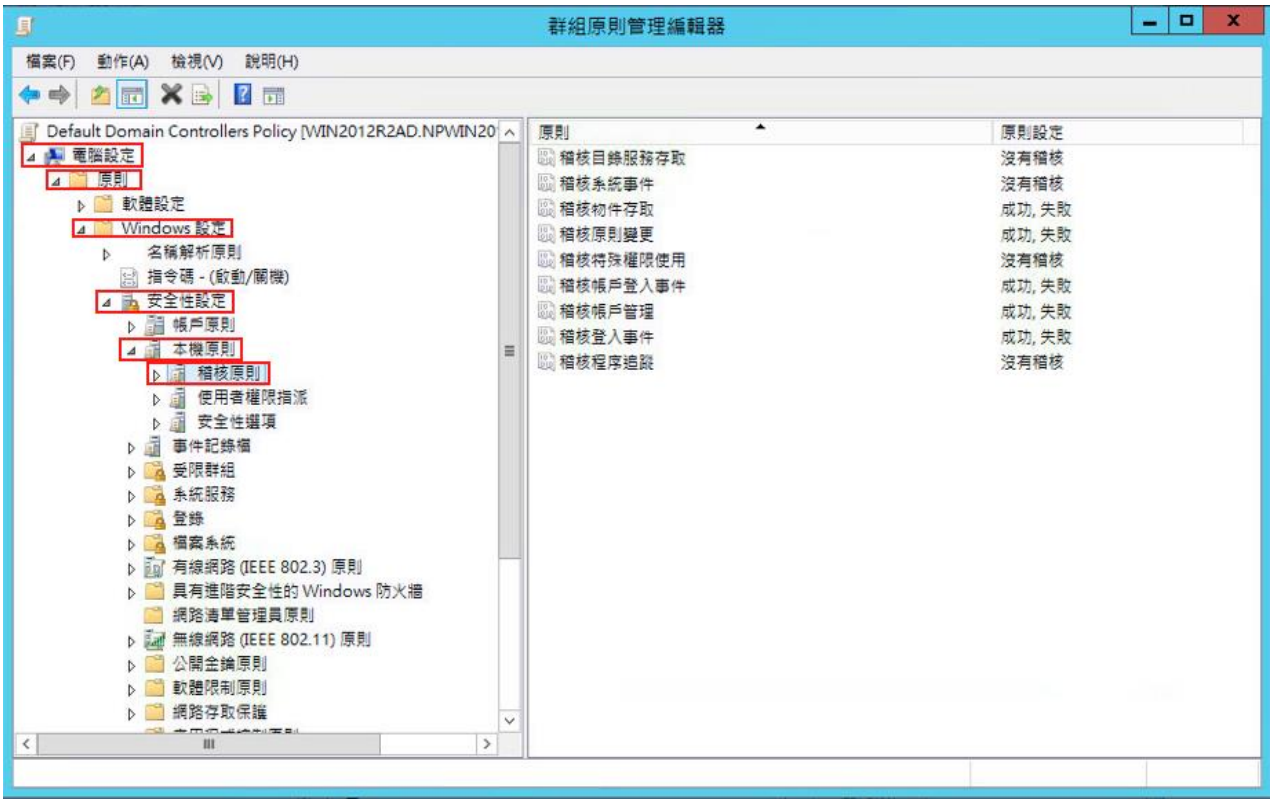


註：此步驟展開 網域，會有 [Default Domain Policy] (預設網域安全性原則)；

另外展開 Domain Controllers(網域控制站)，會有 [Default Domain Controllers Policy] (預設網域控制站安全性原則)。

建議將此兩種安全性稽核原則設定為一致

4. 點選 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]

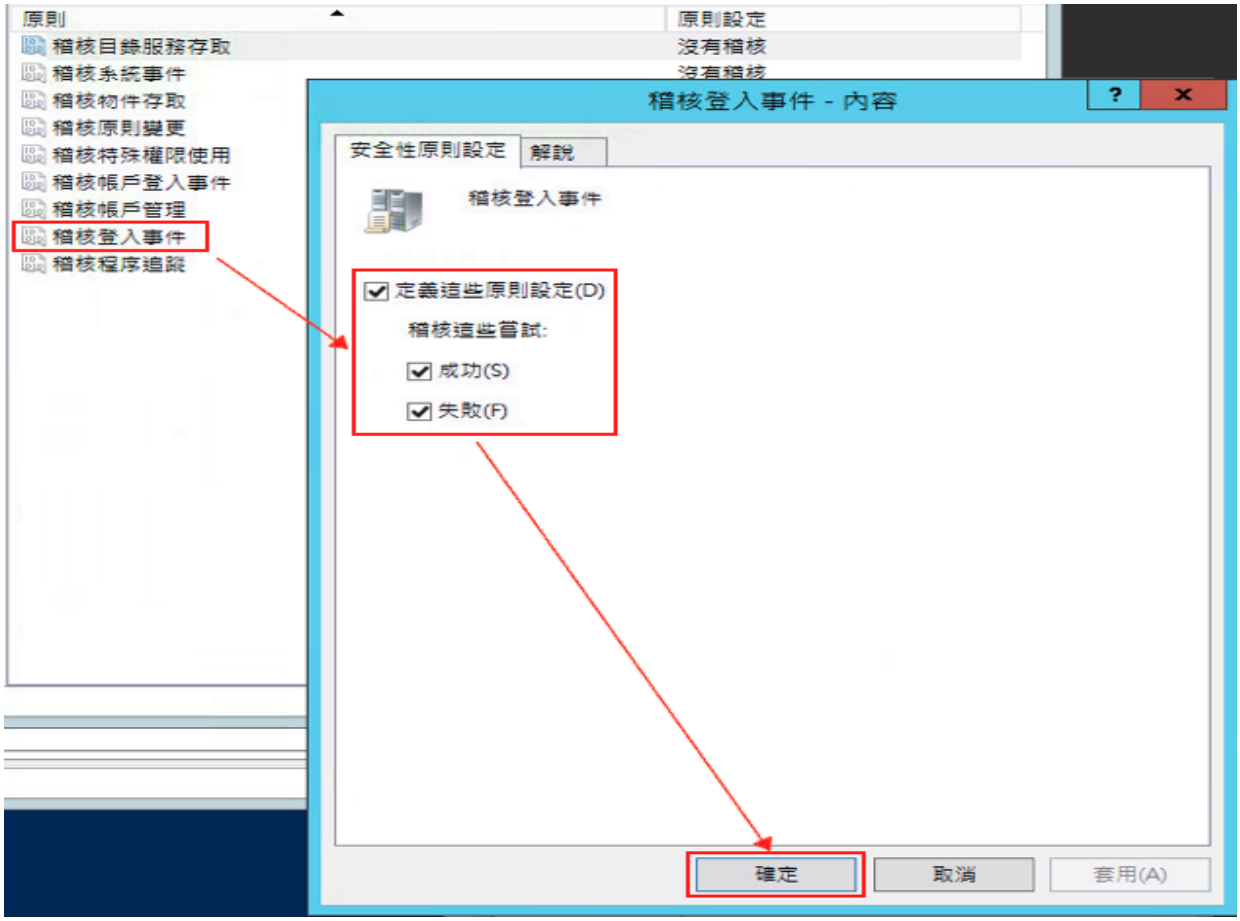


5. 定義下列的原則設定值：

(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [定義這些原則設定]，

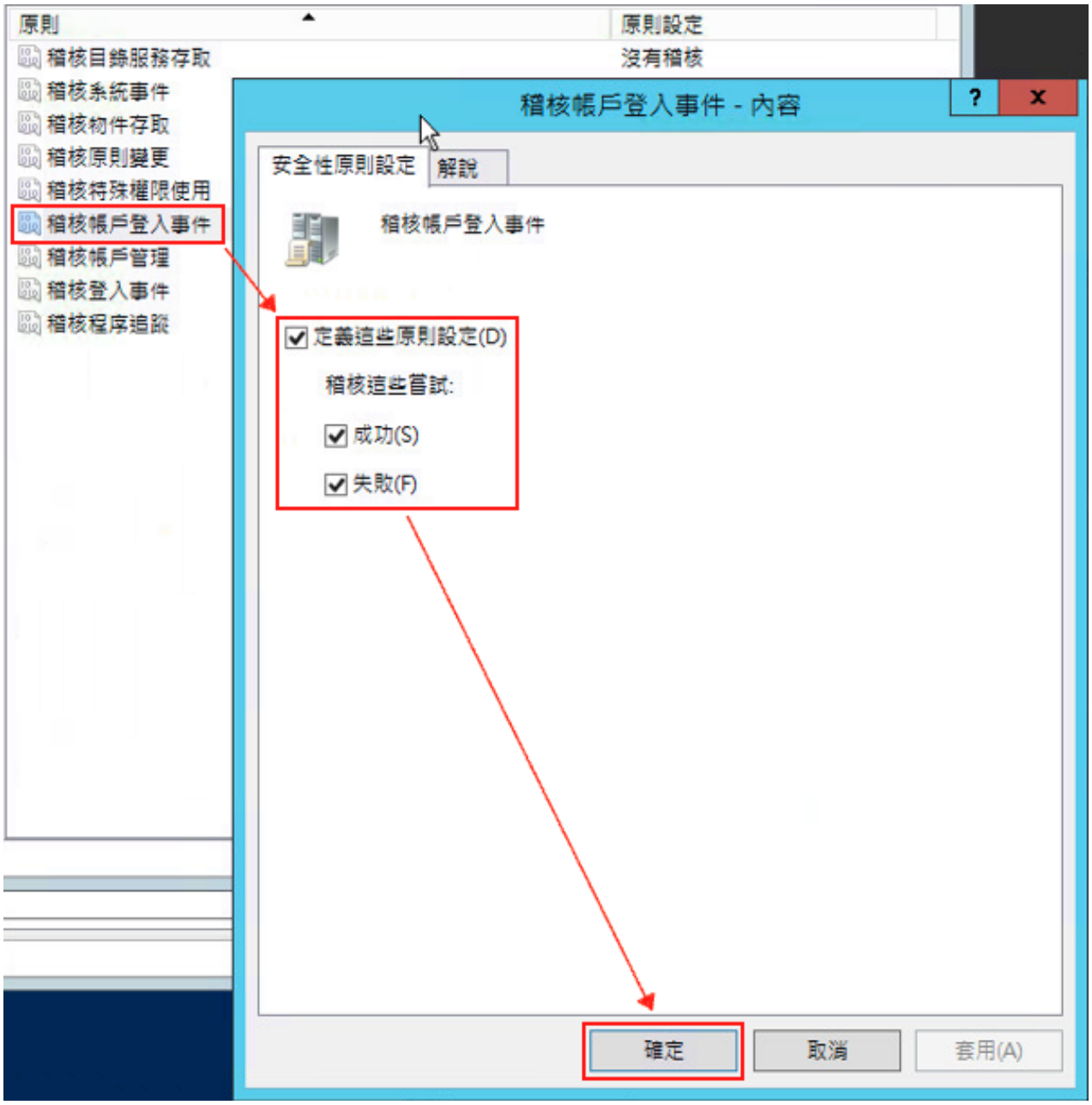
再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(2) 稽核帳戶登入事件：

滑鼠雙擊 [稽核帳戶登入事件]，勾選 [定義這些原則設定]，

再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核原則變更：

雙擊 [稽核原則變更]，勾選 [定義這些原則設定]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

(4) 稽核帳戶管理：

雙擊 [稽核帳戶管理]，勾選 [定義這些原則設定]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

(5) 稽核物件存取：

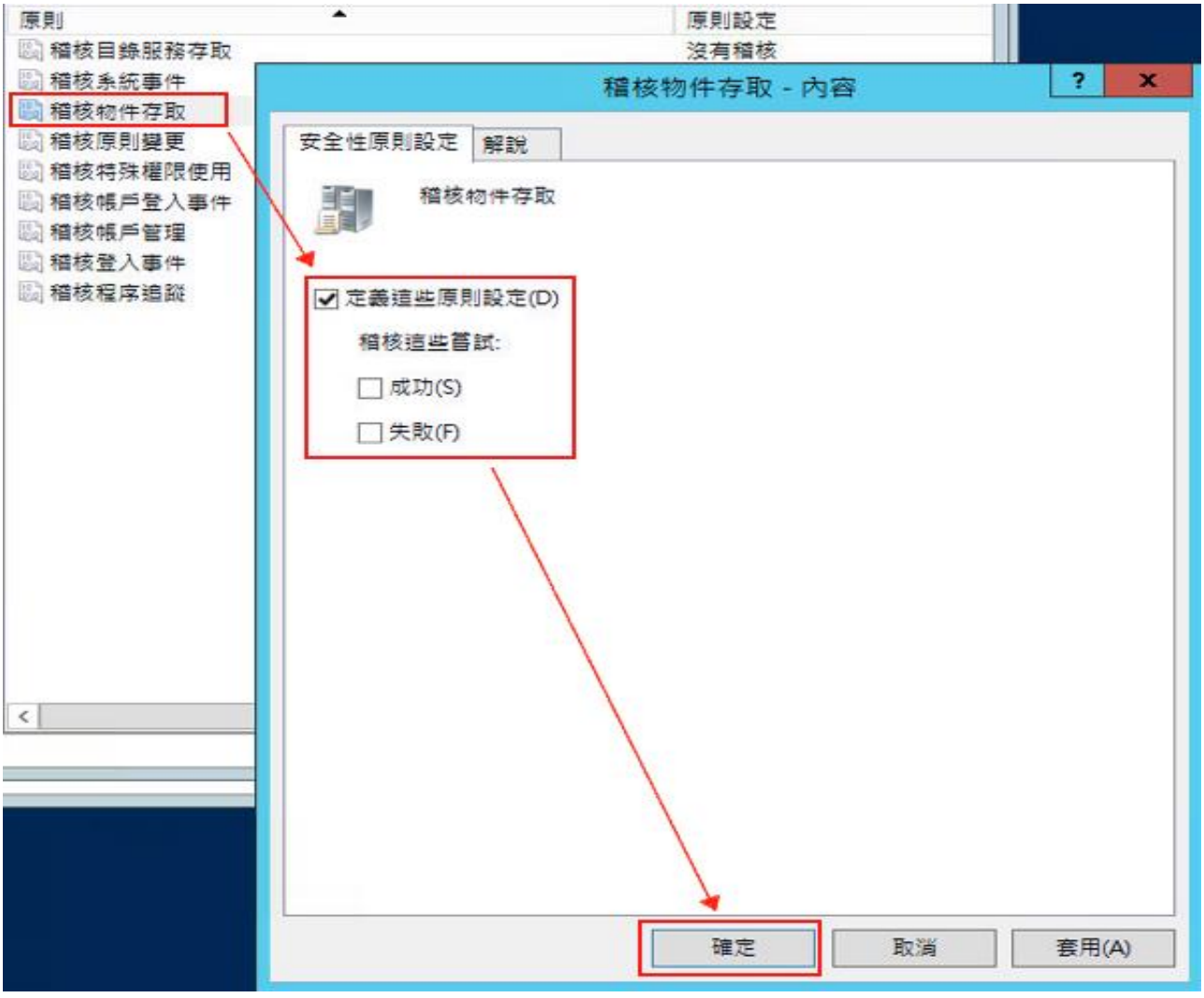
滑鼠雙擊 [稽核物件存取]，勾選 [定義這些原則設定]。

成功：若欲稽核成功事件的 Log，請勾選 [成功] 核取方塊。

失敗：若欲稽核失敗事件的 Log，請勾選 [失敗] 核取方塊。

設定完成後按 [確定]

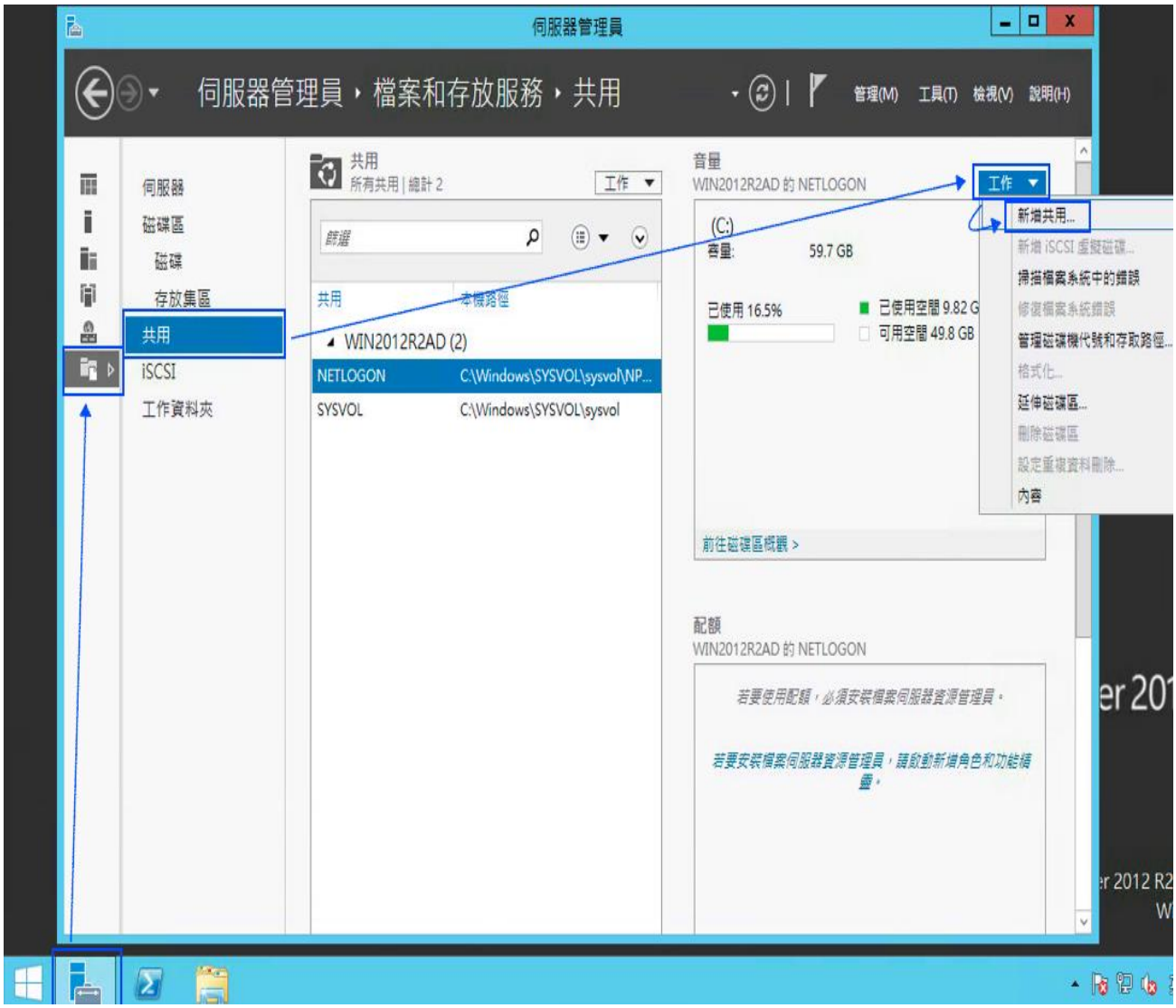
註：若 Windows 2012 Active Directory Server 不做檔案伺服器稽核(File server audit)，建議不要勾選成功與失敗的設定值，僅需勾[定義這些原則設定值]即可. 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter，會影響主機的運作效能。



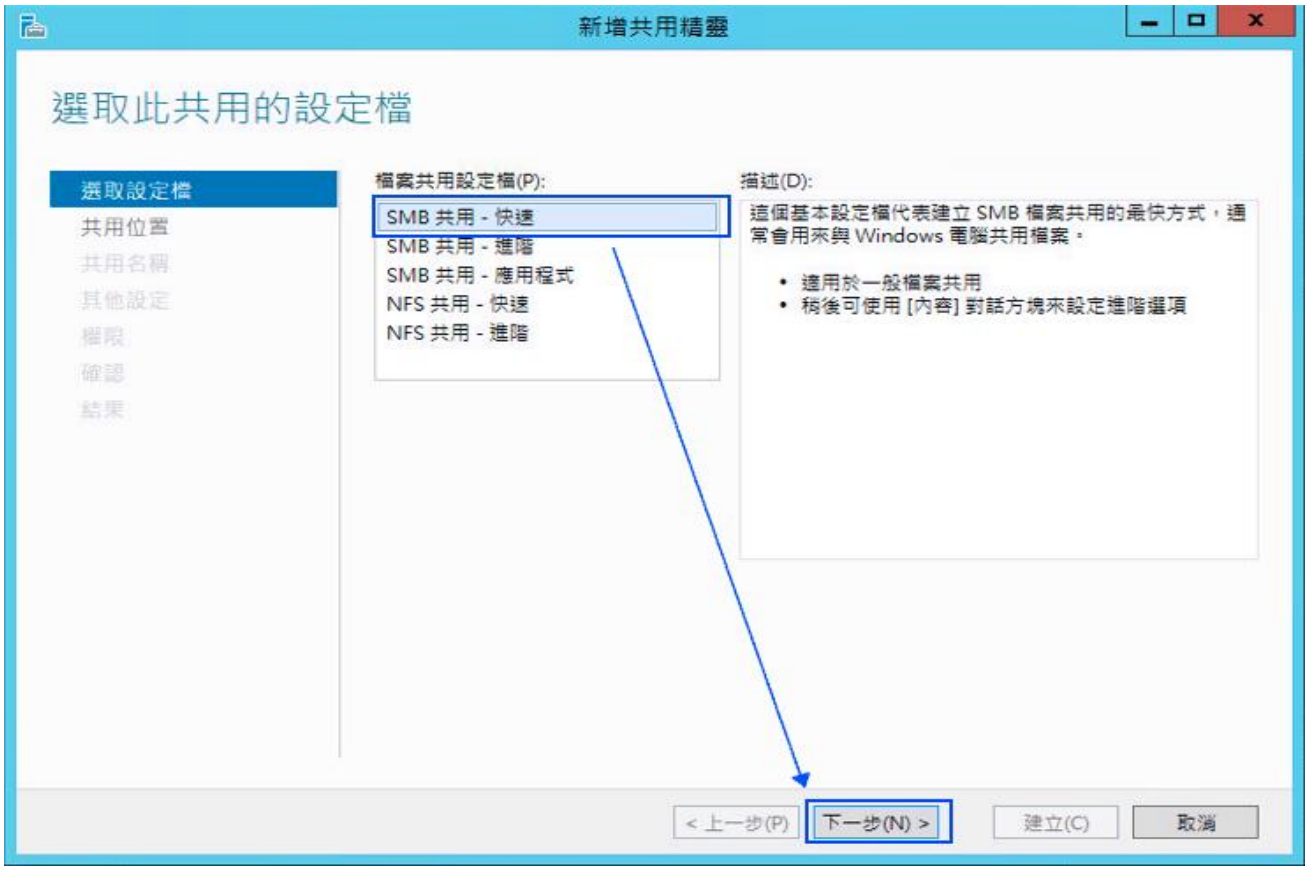
4.2設定共享資料夾權限與稽核原則

設定步驟如下：

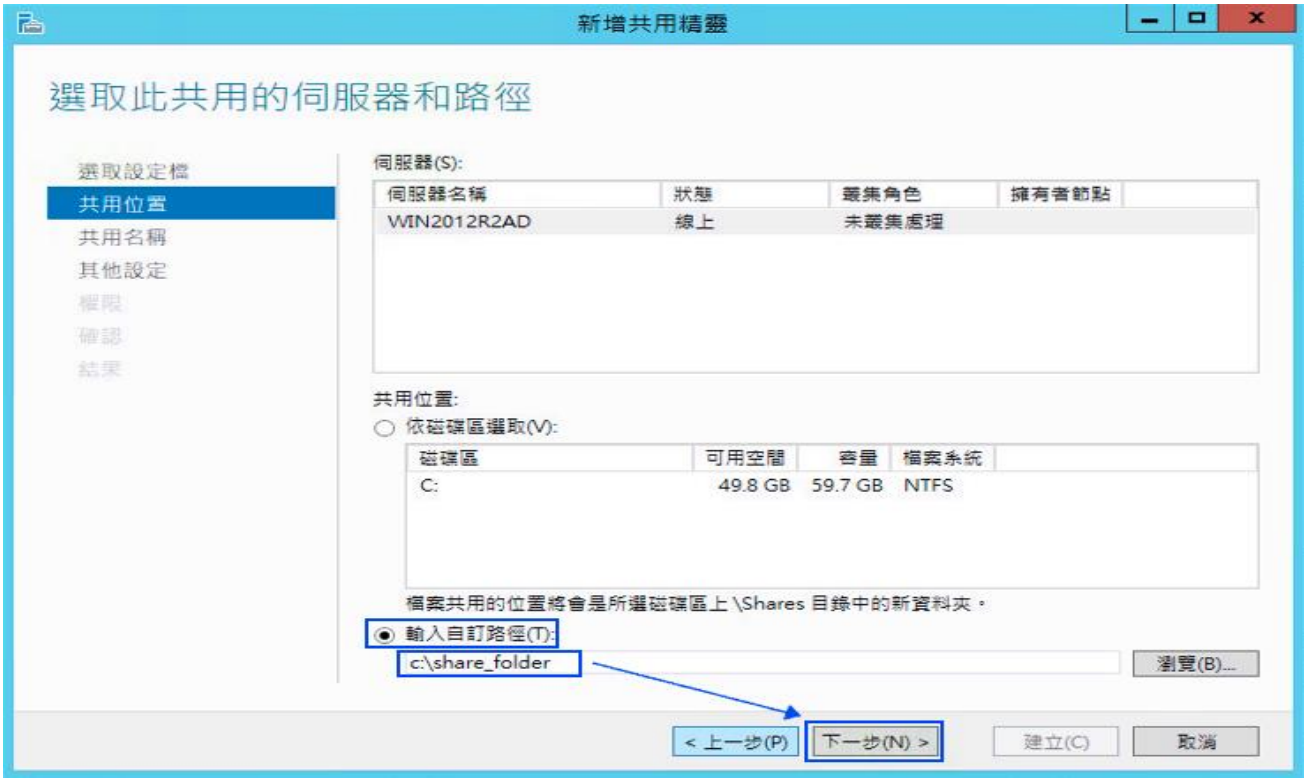
1. 點選 [伺服器管理員 / 檔案和存放服務 / 共用 / 工作 / 新增共用...], 開啟 新增共用精靈。



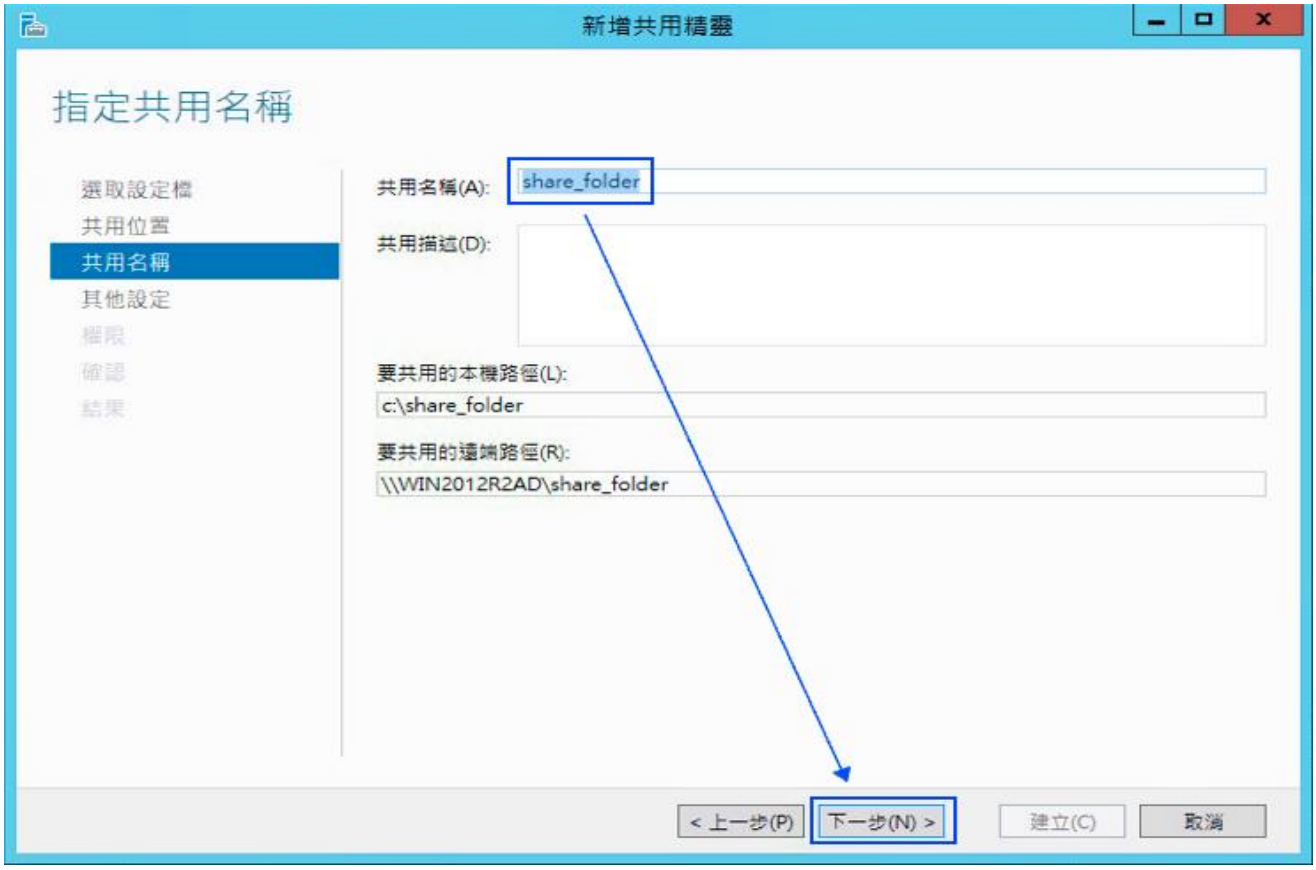
2. 滑鼠左點 [SMB 共用-快速] ，左點 [下一步]。



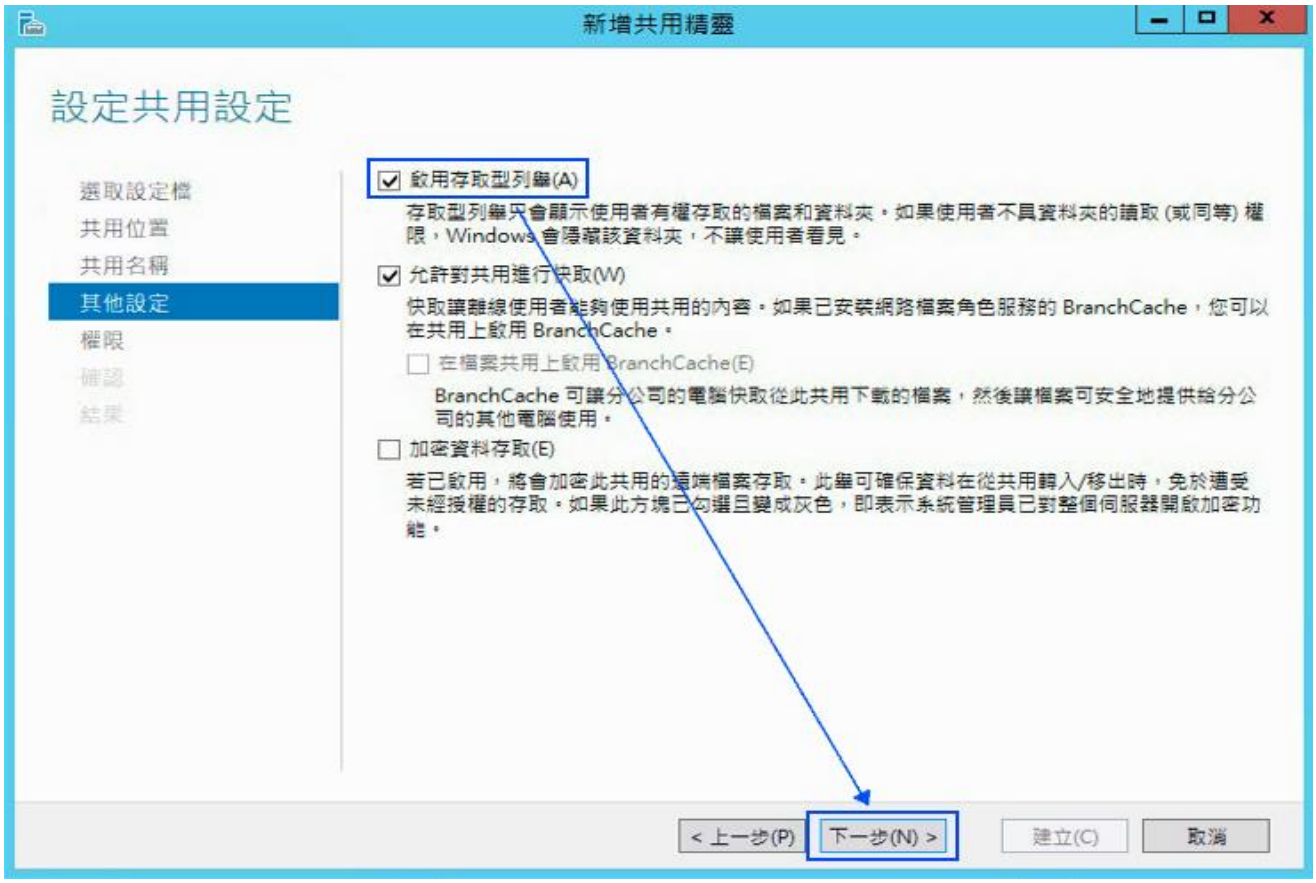
3. 左點 [輸入自訂路徑]，本例為輸入 " C:\share_folder " ，左點 [下一步]。



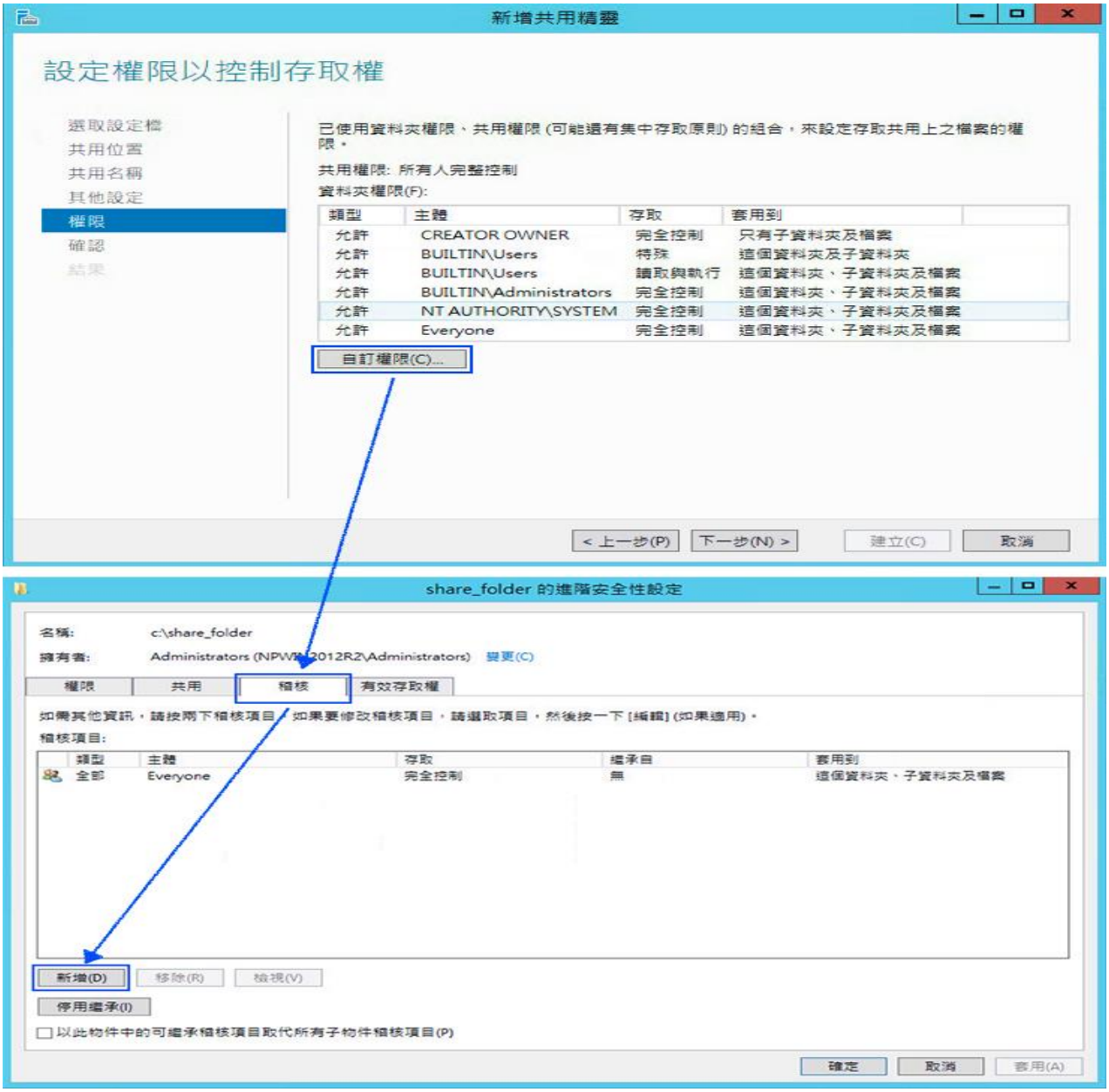
4. 在 共用名稱 欄位輸入所要共用的資料夾的名稱, 本例為輸入[share_folder]，然後按 [下一步] 。



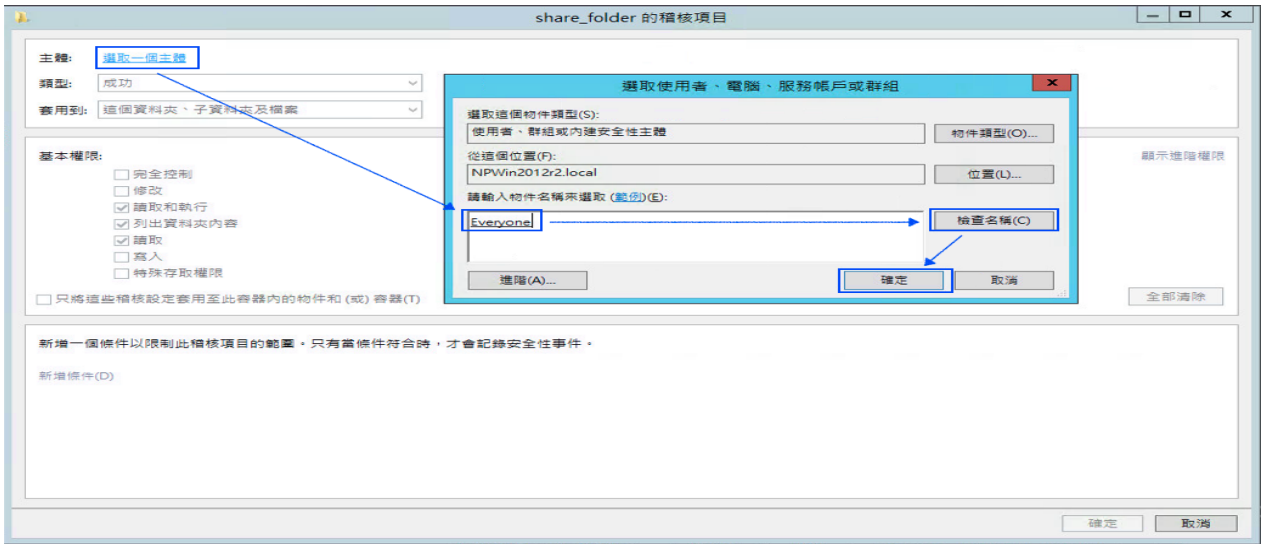
5. 勾選 [啟用存取型列舉]，左點 [下一步] 。



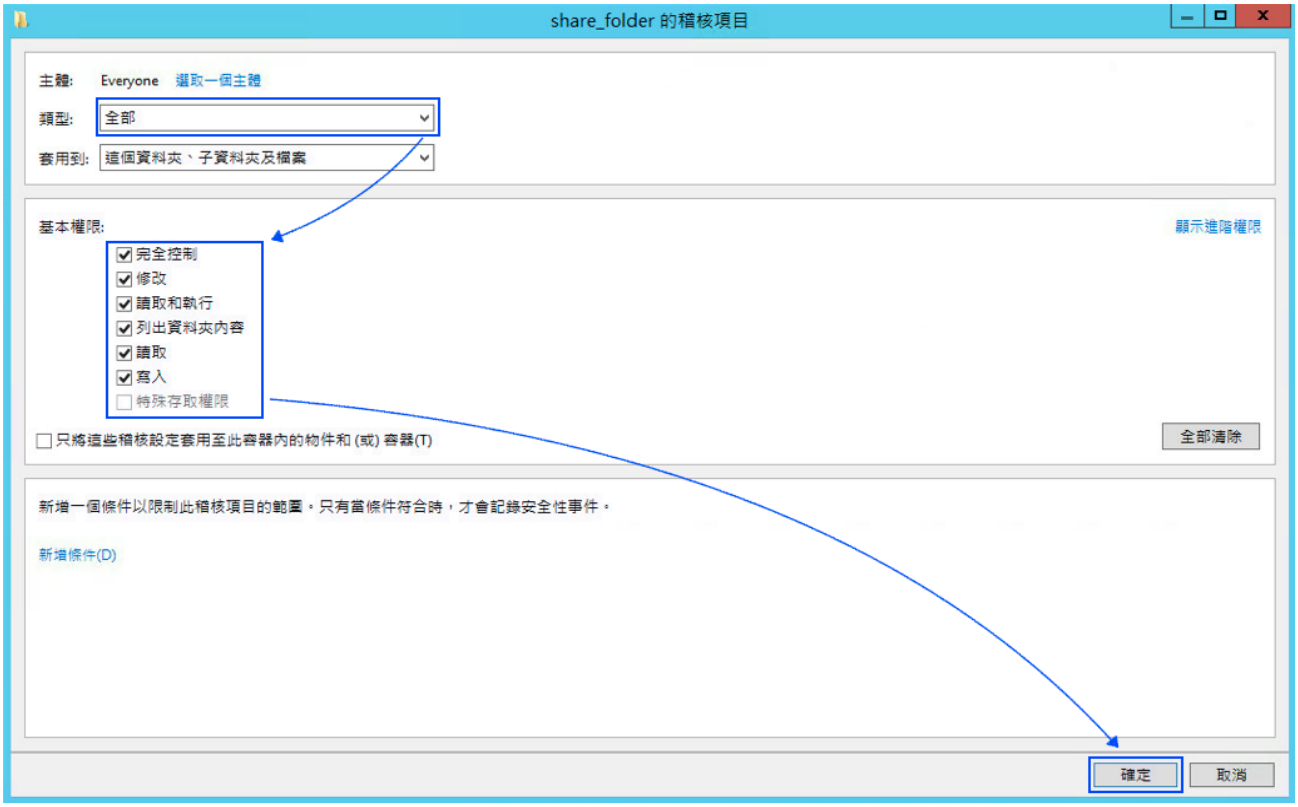
6. 點選 [自訂權限... / 稽核 / 新增] 。



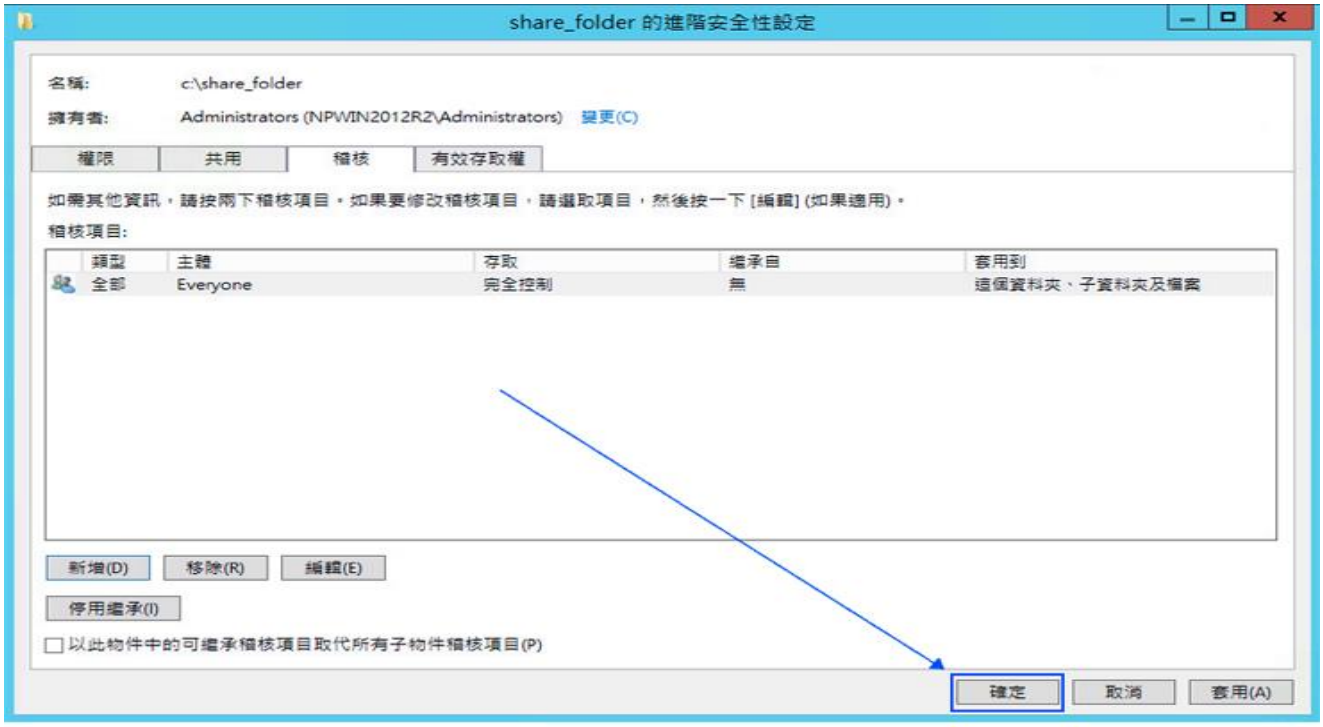
7. 左點 [選取一個主體]，如果欲稽核所有使用者，在物件名稱欄位的空白處輸入 " everyone " 後，點選檢查名稱，按 [確定] 。**(註 ： 若要選擇其他網域, 可點選 [位置])**

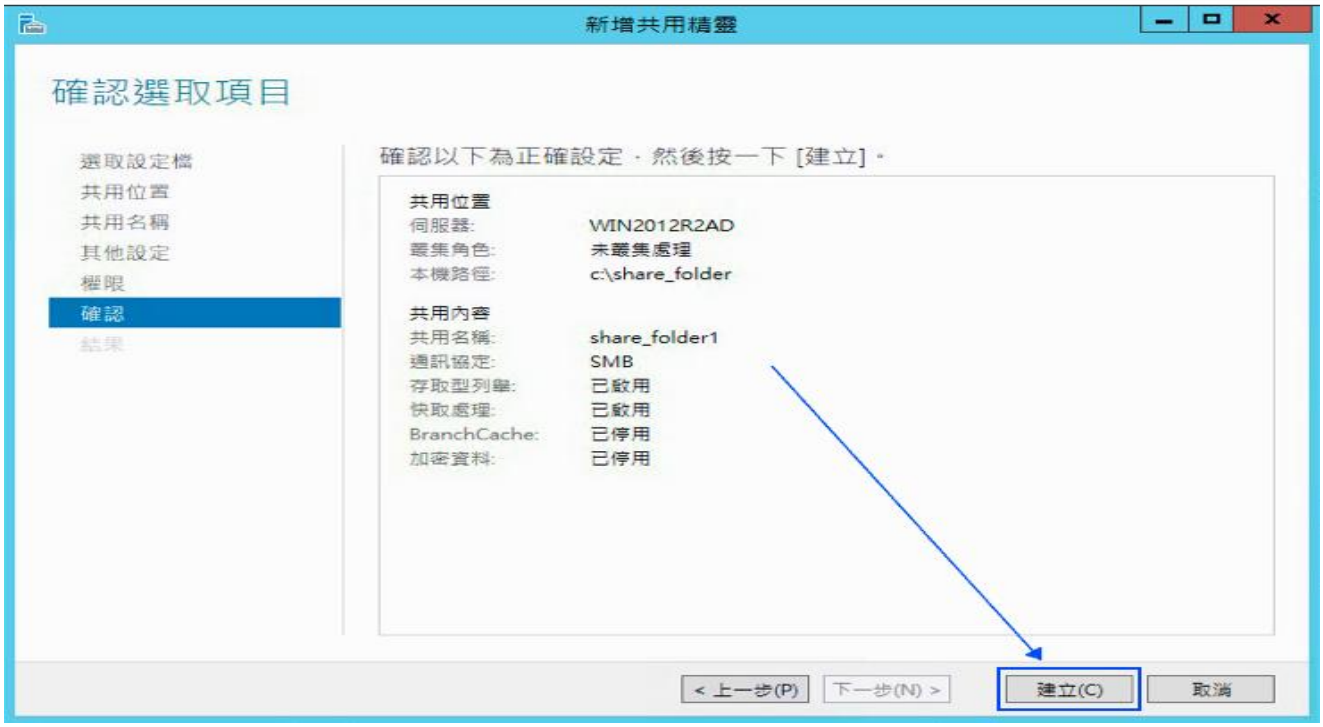


8. 類型 下拉選 [全部] ，基本權限勾選 [完全控制] ，然後按左點 [確定] 。



9. 若稽核設定完成後，按 [確定]。按 [下一步] 。按 [建立] / [關閉], 完成設定。





5 Windows 2016 Active Directory Server 稽核設定

本章節主要說明以下操作設定：

1.設定網域使用者登入登出的稽核原則。2.設定共享資料夾權限與稽核原則。

Windows 2016 AD Server 登入登出的稽核原則和目錄分享的稽核原則，預設是關閉的。

安裝 NXLOG 的步驟，詳細請參閱第一章節。

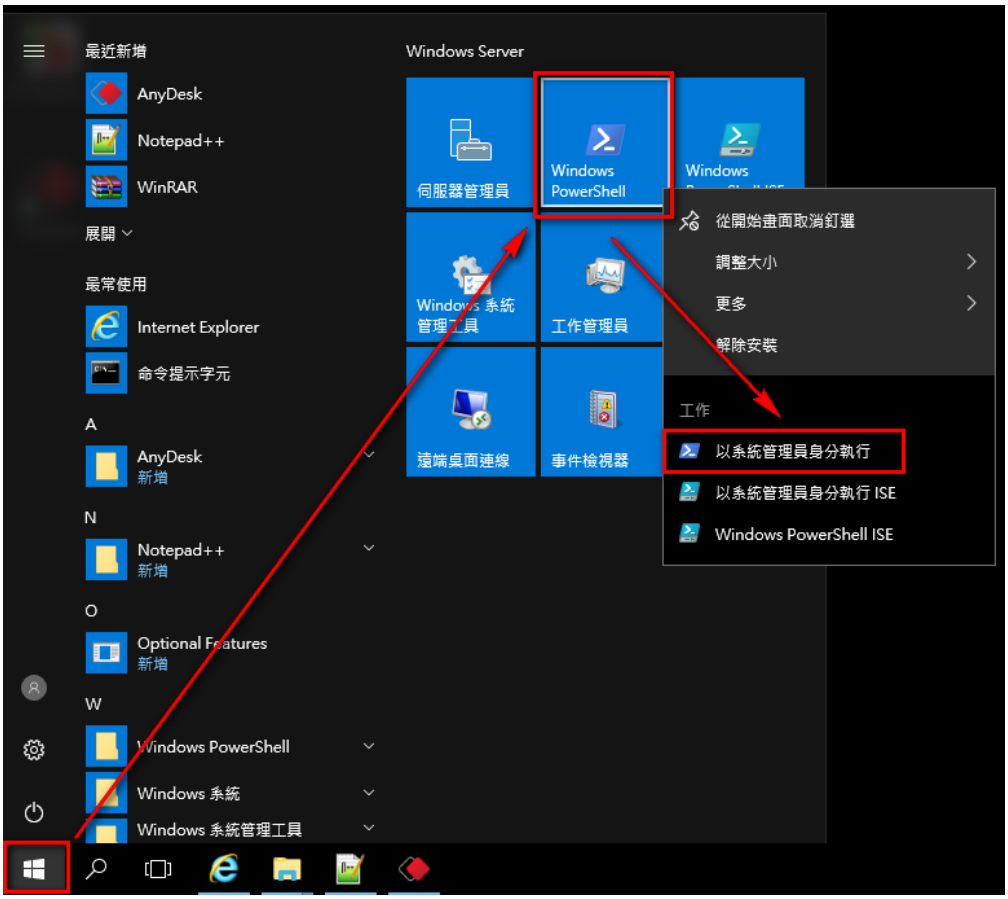
5.1設定網域使用者登入登出的稽核原則

設定步驟如下：

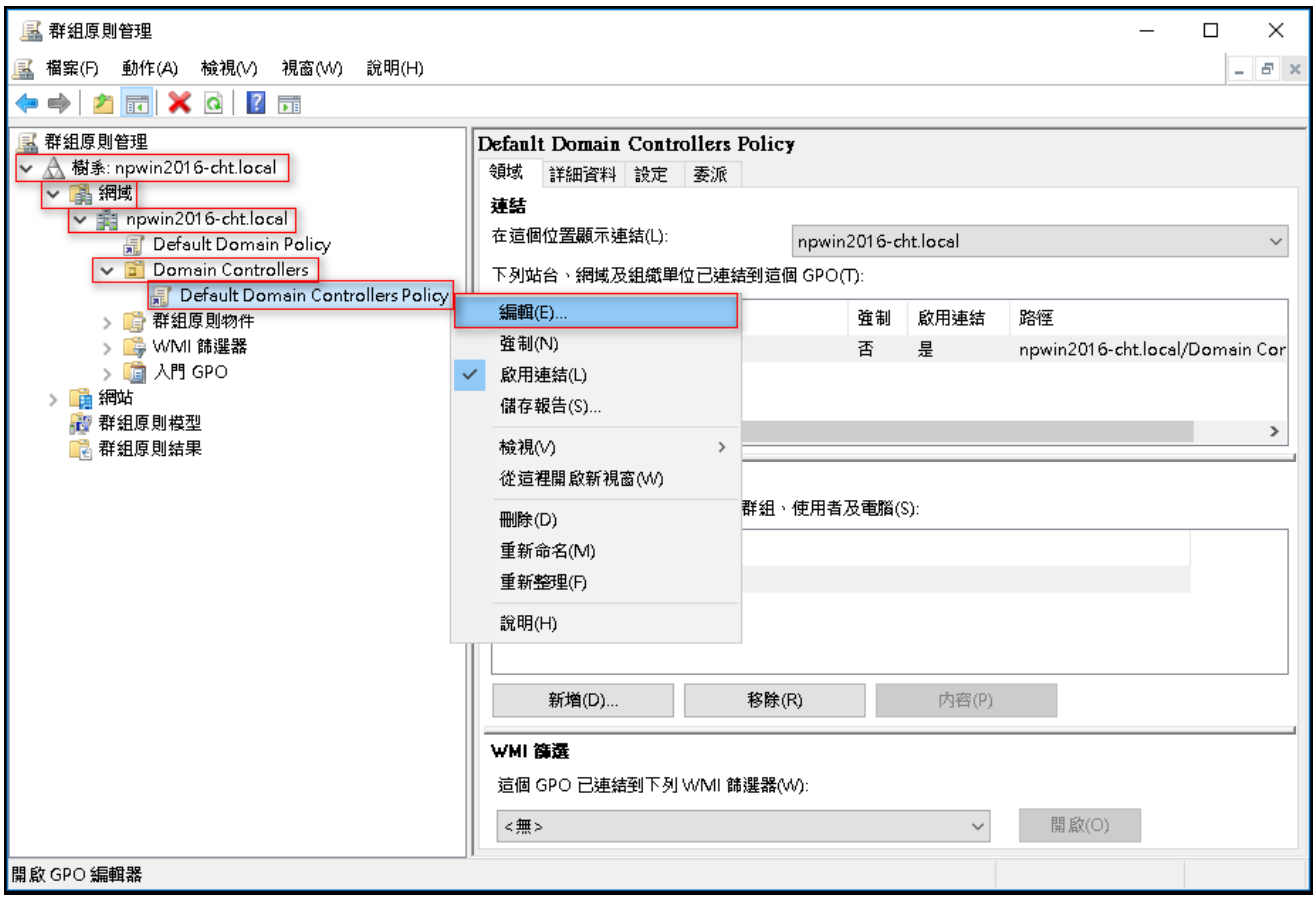
1. 以**全程以 系統管理員權限的 Administrator 或是具有 Domain Admin 的帳號權限身分**登入 Windows 2016 Active Directory Server(網域控制站)。(否則可能會因權限不足的問題導致設定無作用)

   開啟[群組原則管理]:

   滑鼠左點[開始]，右點[Windows PowerShell]，左點[以系統管理員身分執行]。輸入：**gpmc.msc** ，完成後按 [Enter]



2. 以本文件為例子(實際情況請依使用者的環境做調整), 點選 [樹系 / 網域 / npwin2016-cht.local / Domain Controllers / Default Domain Controllers Policy]。
3. 滑鼠右鍵點選[Default Domain Controllers Policy]，按 [編輯]，開啟[群組原則管理編輯器]。

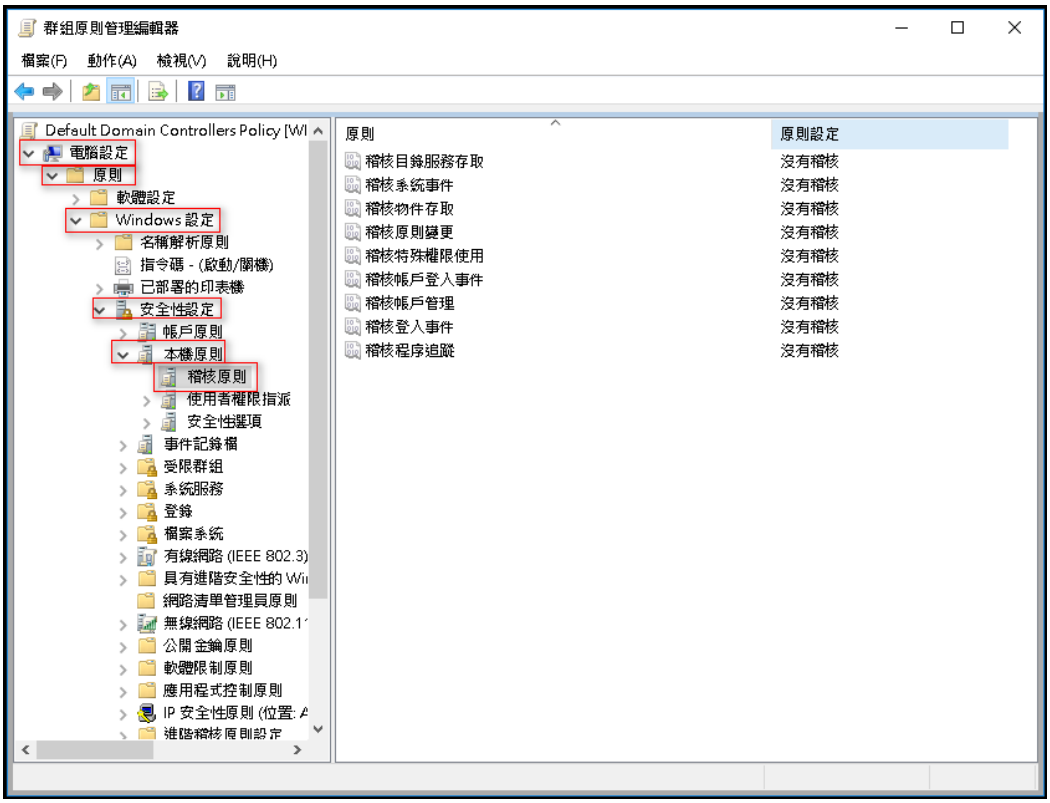


註：此步驟展開 網域，會有 [Default Domain Policy] (預設網域安全性原則)；

另外展開 Domain Controllers(網域控制站)，會有 [Default Domain Controllers Policy] (預設網域控制站安全性原則)。

建議將此兩種安全性稽核原則設定為一致

4. 點選 [電腦設定 / 原則 / Windows 設定 / 安全性設定 / 本機原則 / 稽核原則]

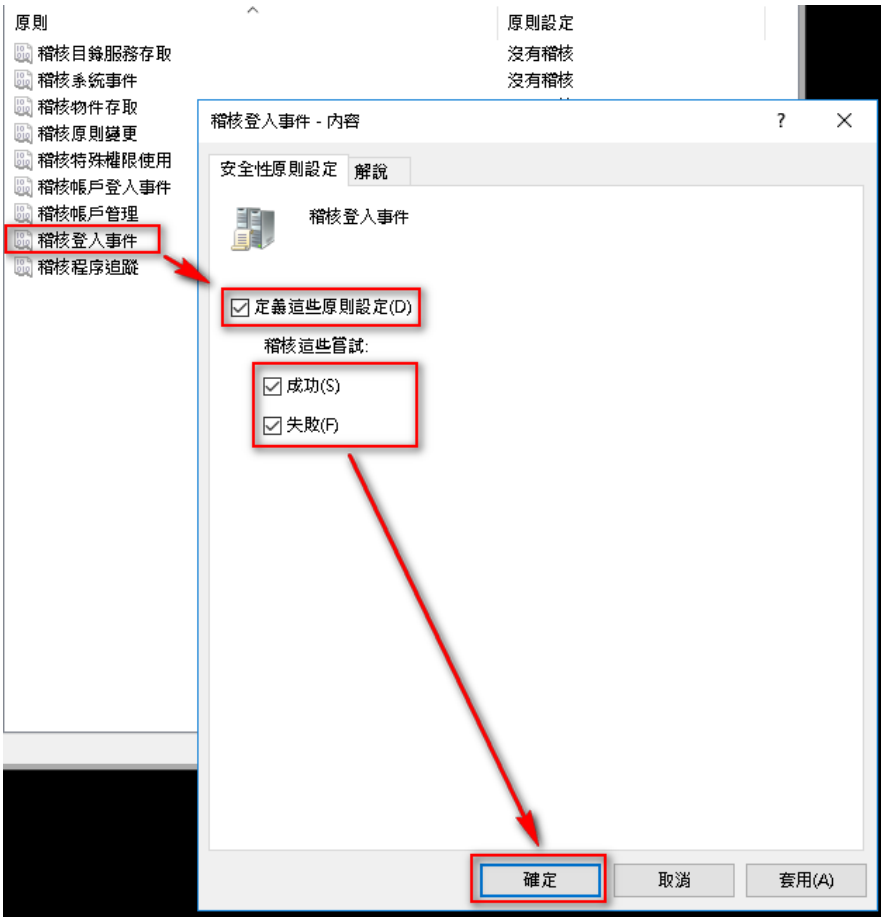


5. 定義下列的原則設定值：

(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [定義這些原則設定]，

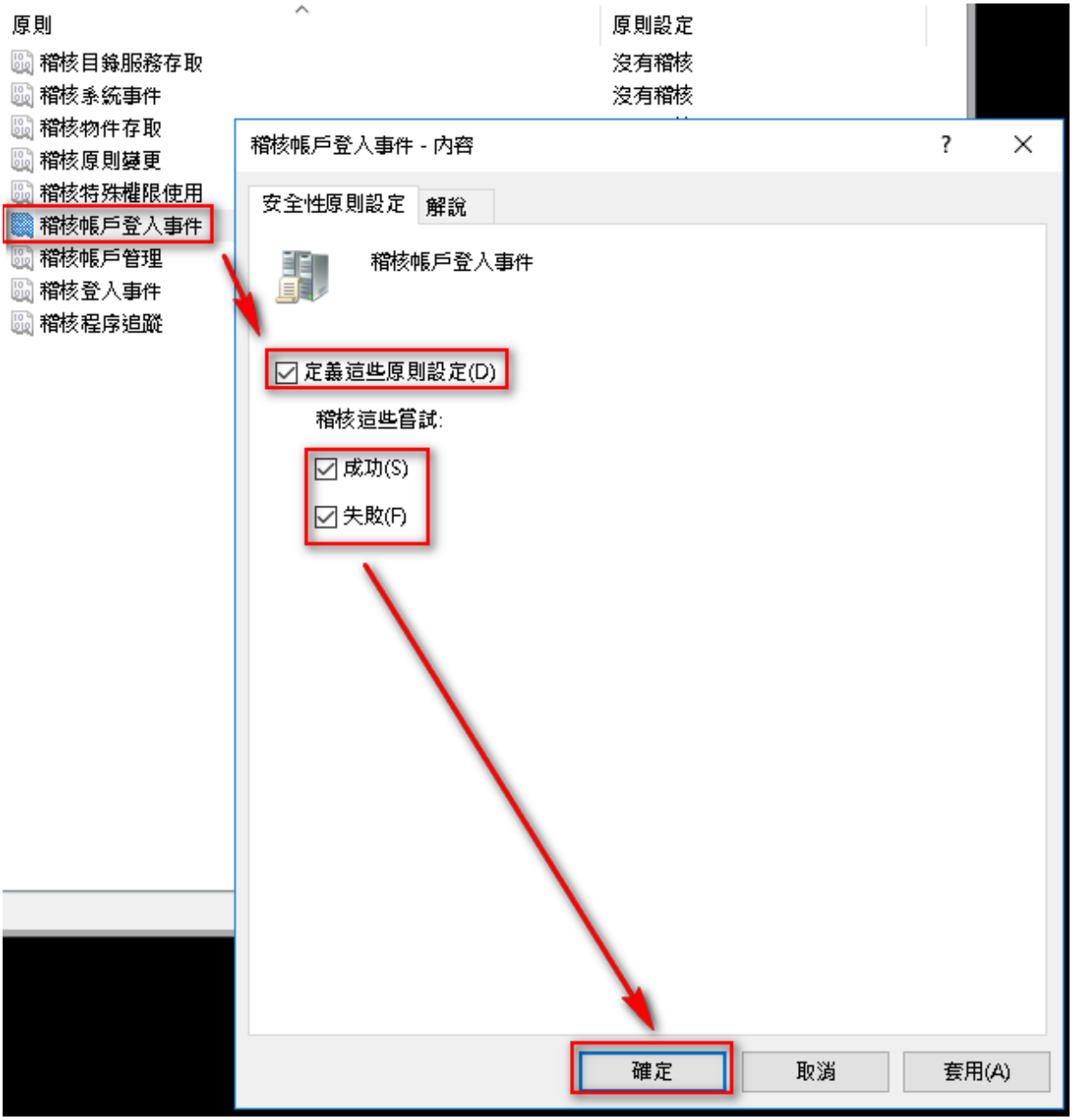
再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(2) 稽核帳戶登入事件：

滑鼠雙擊 [稽核帳戶登入事件]，勾選 [定義這些原則設定]，

再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核原則變更：

雙擊 [稽核原則變更]，勾選 [定義這些原則設定]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

(4) 稽核帳戶管理：

雙擊 [稽核帳戶管理]，勾選 [定義這些原則設定]，再勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

(5) 稽核物件存取：

滑鼠雙擊 [稽核物件存取]，勾選 [定義這些原則設定]。

成功：若欲稽核成功事件的 Log，請勾選 [成功] 核取方塊。

失敗：若欲稽核失敗事件的 Log，請勾選 [失敗] 核取方塊。

設定完成後按 [確定]

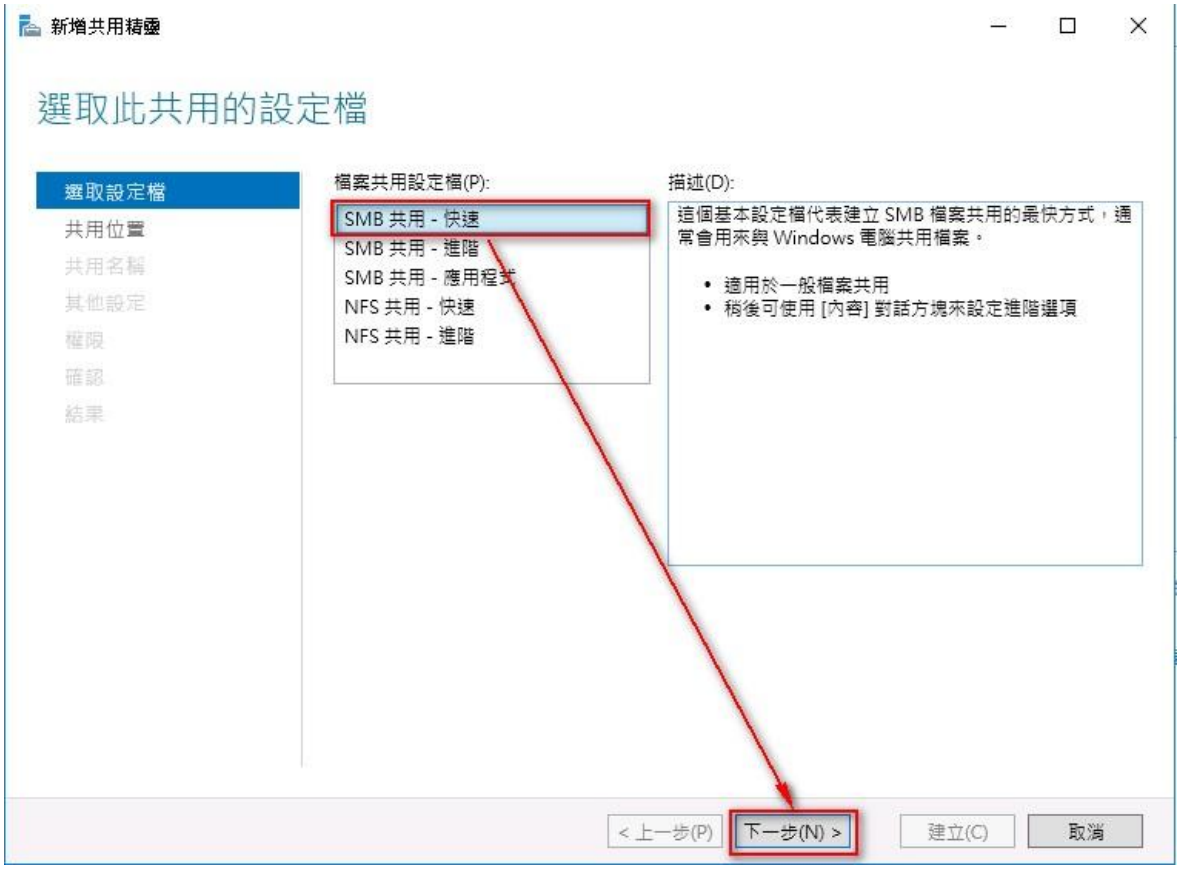
註：若 Windows 2016 Active Directory Server 不做檔案伺服器稽核(File server audit)，建議不要勾選成功與失敗的設定值，僅需勾[定義這些原則設定值]即可. 以避免 Windows 稽核多餘且冗長的物件存取事件然後轉換成 syslog 後發送給 N-Reporter，會影響主機的運作效能。

5.2設定共享資料夾權限與稽核原則

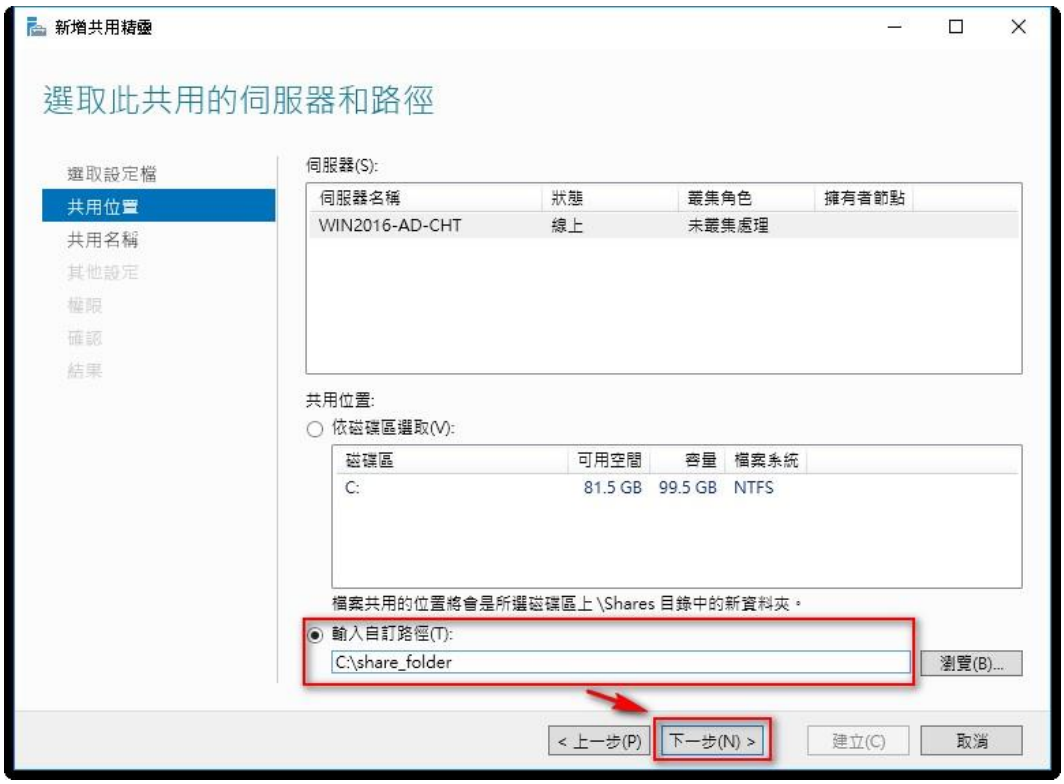
設定步驟如下：

1. 點選 [伺服器管理員 / 檔案和存放服務 / 共用 / 工作 / 新增共用...], 開啟 新增共用精靈。

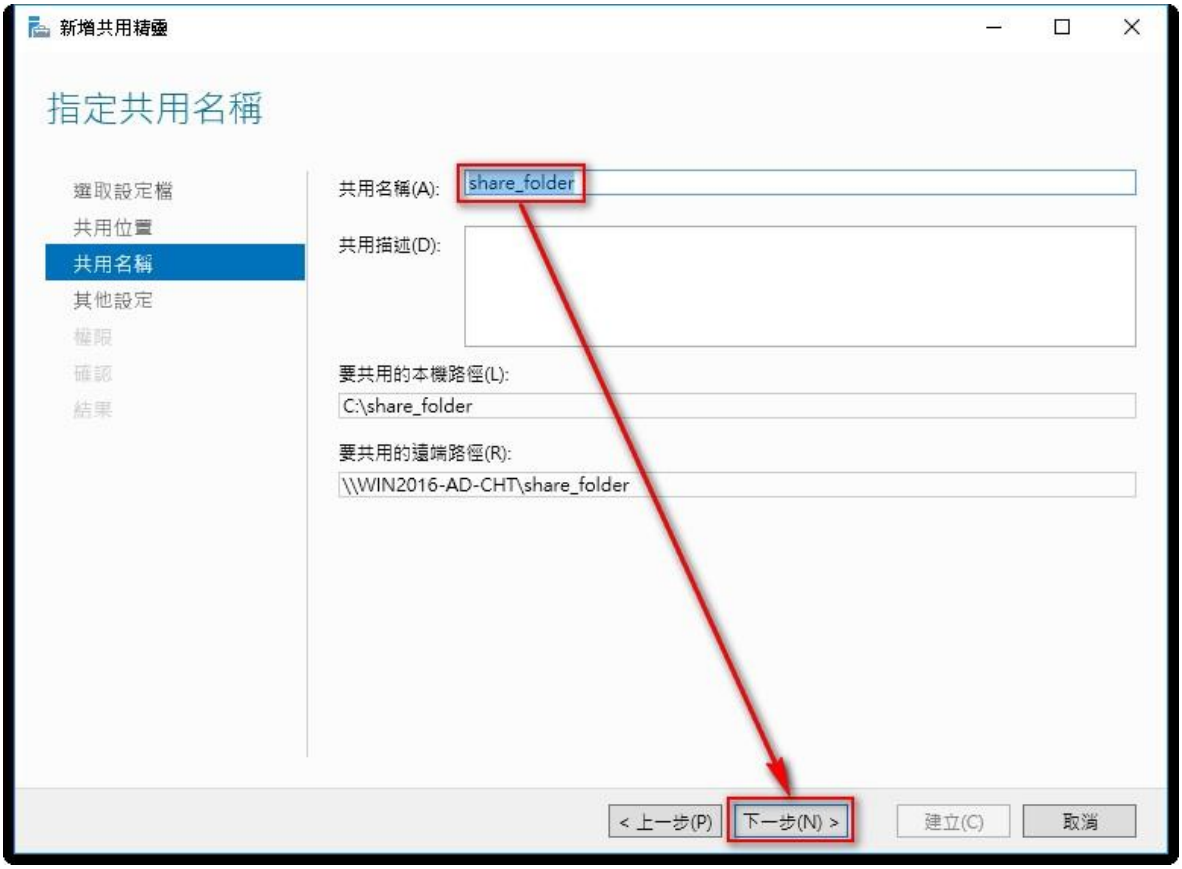
2. 滑鼠左點 [SMB 共用-快速] ，左點 [下一步]。



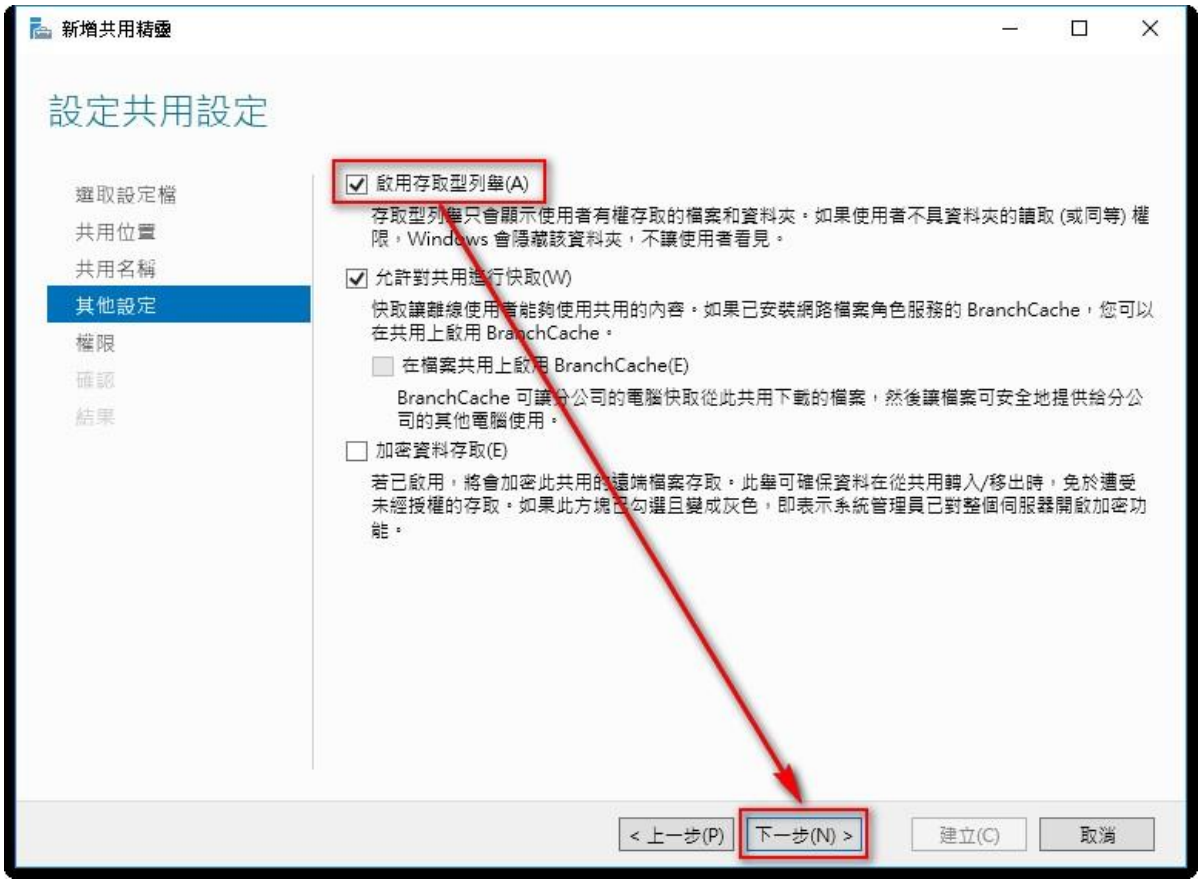
3. 左點 [輸入自訂路徑]，本例為輸入 " C:\share_folder " ，左點 [下一步]。



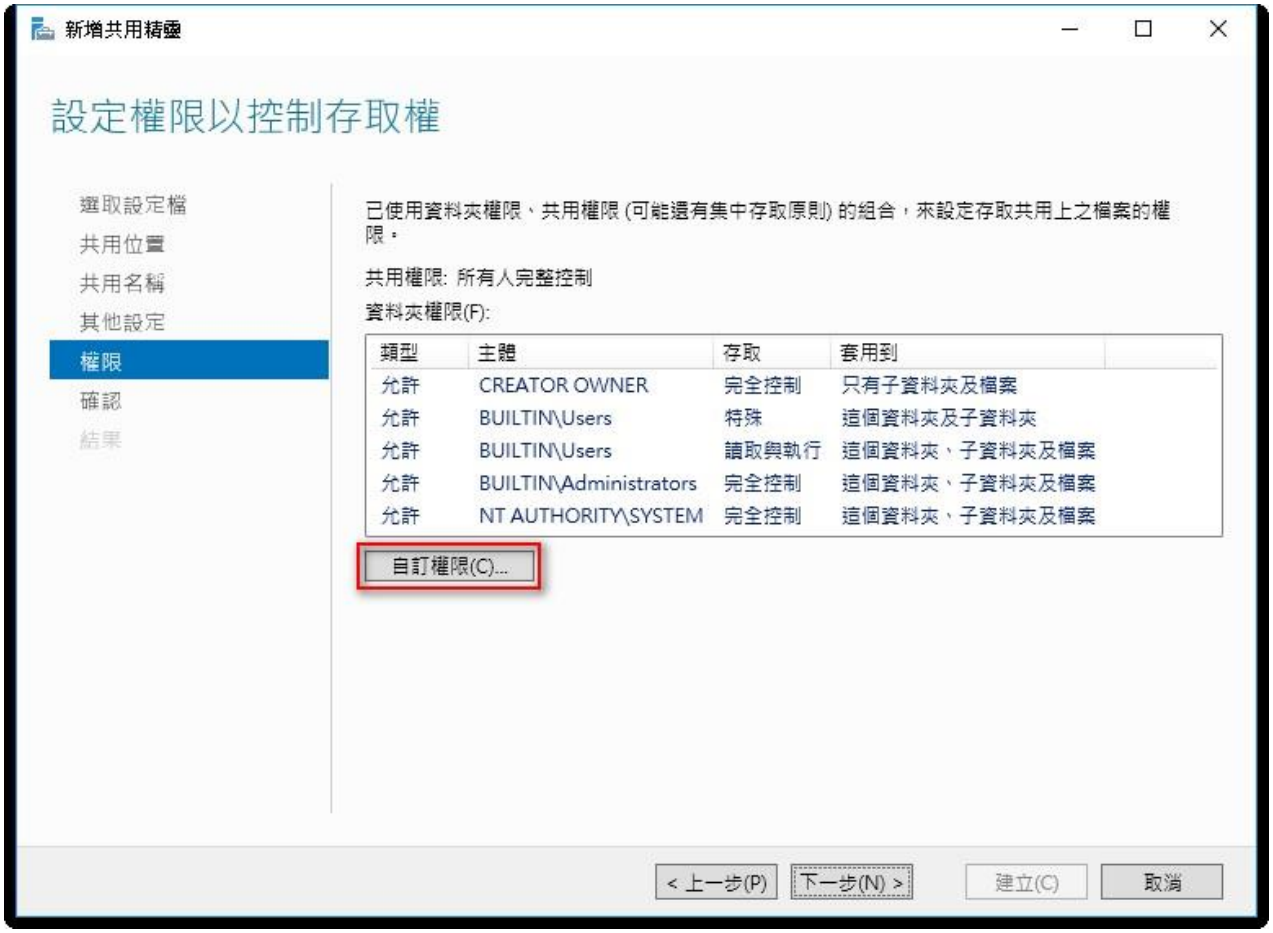
4. 在 共用名稱 欄位輸入所要共用的資料夾的名稱，本例為輸入[share_folder]，然後按 [下一步] 。

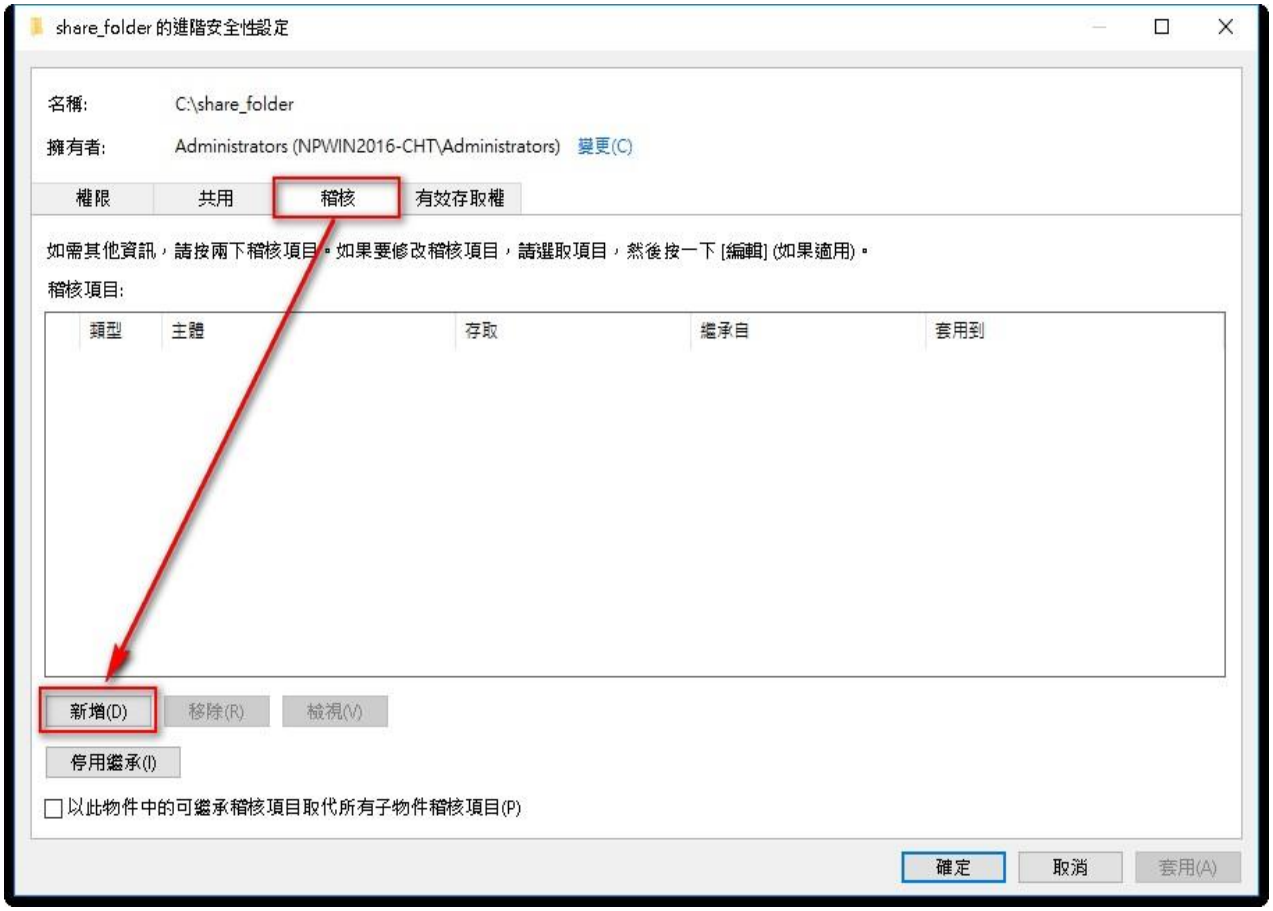


5. 勾選 [啟用存取型列舉]，左點 [下一步] 。

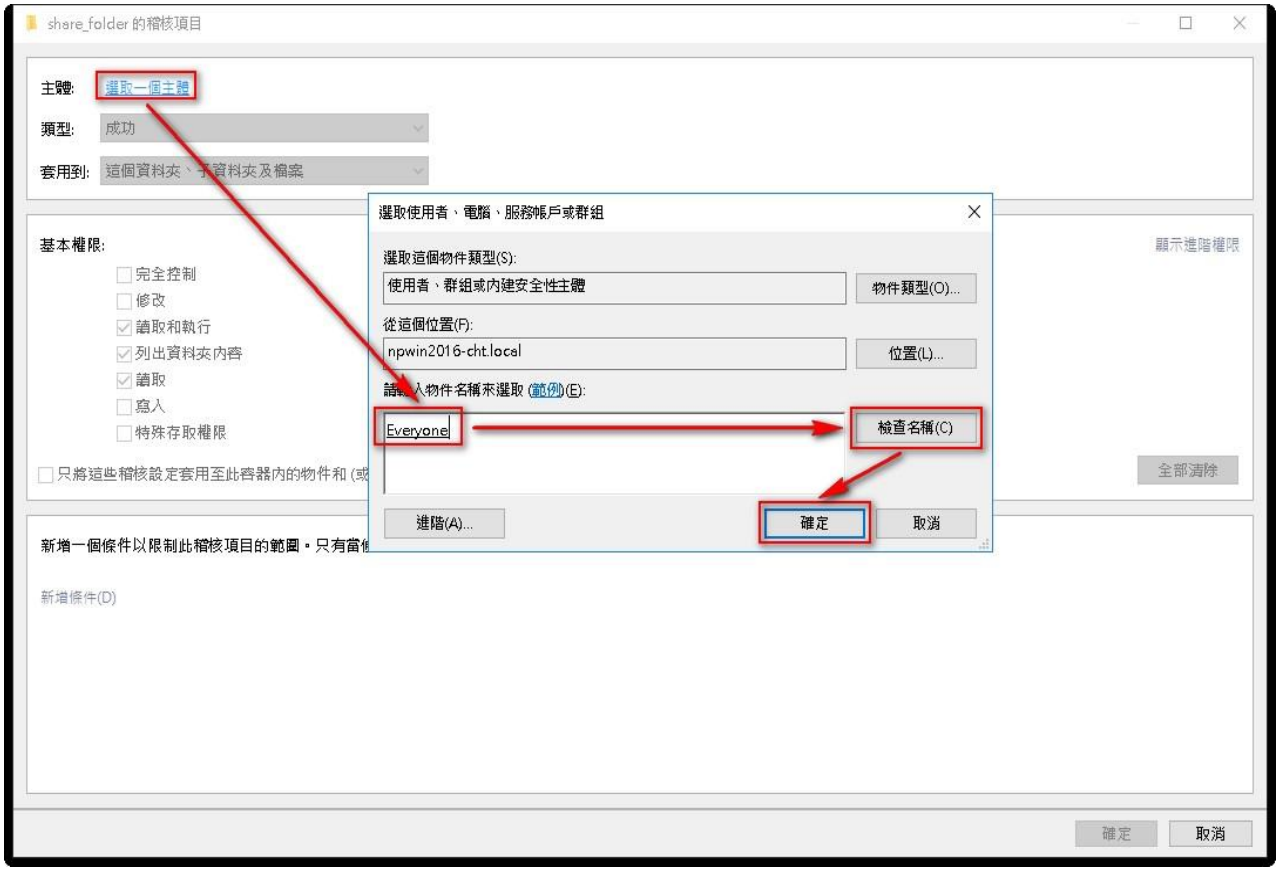


6. 點選 [自訂權限... / 稽核 / 新增] 。



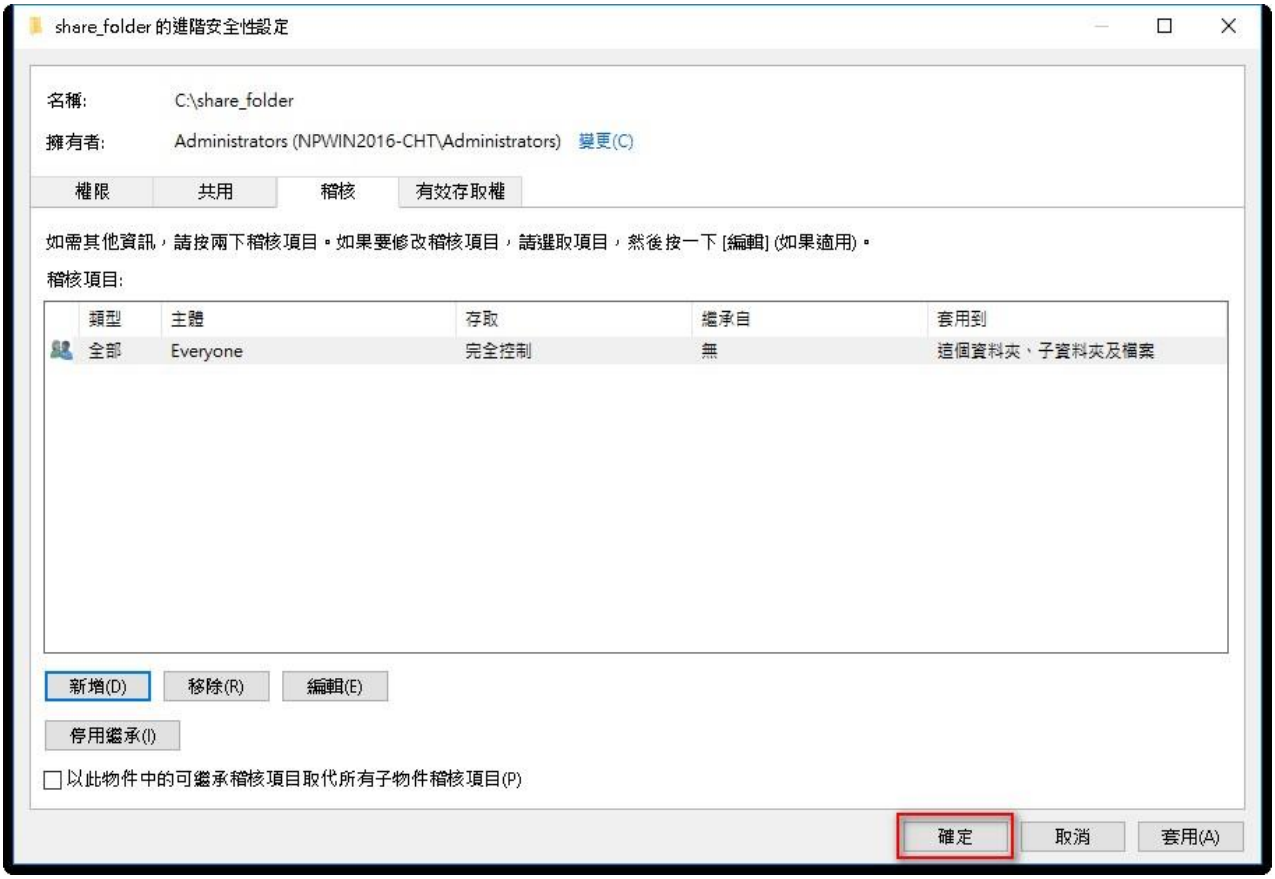


7. 左點 [選取一個主體]，如果欲稽核所有使用者，在物件名稱欄位的空白處輸入 " everyone " 後，點選檢查名稱，按 [確定] 。**(註 ： 若要選擇其他網域, 可點選 [位置])**



8. 類型 下拉選 [全部] ，基本權限勾選 [完全控制] ，然後按左點 [確定] 。

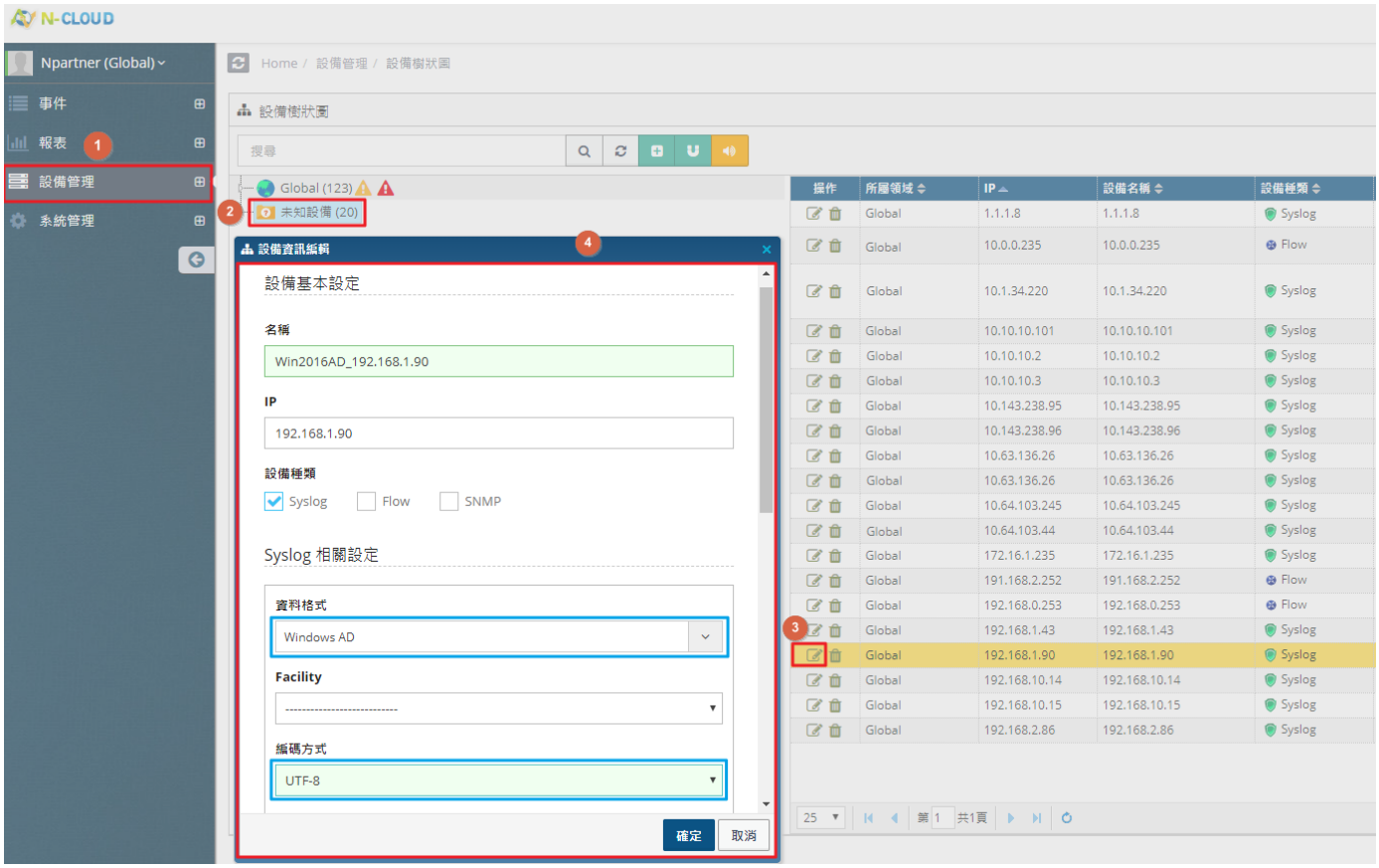
9. 若稽核設定完成後，按 [確定]。按 [下一步] 。按 [建立] / [關閉], 完成設定。



6 將設備加入系統及 Syslog 資料格式及 Facility 的設定

(1) 登入 N-Reporter / N-Cloud 系統

(2) 滑鼠點選[設備管理 / 設備樹狀圖 / 未知設備的編輯圖示]，在 IP 欄位中應該能看見此台的設備的 IP。請輸入一個方便記憶的設備名稱，接著在[資料格式]下拉選單中選擇 {Windows AD}，勾選[啟動接收]，按下[確定] ，即完成設備的系統新增程序



連絡資訊

N-Partner 公司連絡方式：

TEL: +886-4-23752865

FAX: +886-4-23757458

有關技術問題請洽：

Email: support@npartnertech.com

Skype：support@npartnertech.com

有關業務相關問題請洽：

Email: sales@npartnertech.com