



N-Partner

N-REPORTER

如何使用 NXLOG 管理配置
Windows Server 日誌

V 005 (繁體)

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 2003/2008/2012 的日誌(Eventlog) , 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、Windows Server 2008、Windows Server 2012。

NXLOG 適用於記錄大量事件的環境。當 Windows Server 日誌(Eventlog)每秒最大記錄速率超過 700 筆 , 請選用本文件介紹的 NXLOG 的配置方式。

本章節內容如下

1	安裝設定 Windows Server 環境中的 NXLog	2
1.1	For Windows Server 2003	2
1.2	For Windows Server 2008	5
1.3	For Windows Server 2012	8
2	Windows 2003 Server 稽核設定	12
2.1	設定本機登入登出的稽核原則	12
2.2	設定本機共享資料夾權限與稽核原則	16
3	Windows 2008 Server 稽核設定	25
3.1	設定本機登入登出的稽核原則	25
3.2	設定本機共享資料夾權限與稽核原則	30
4	Windows 2012 Server 稽核設定	43
4.1	設定本機登入登出的稽核原則	43
4.2	設定共享資料夾權限與稽核原則	47
5	將設備加入系統及 Syslog 資料格式及 Facility 的設定.....	53
	連絡資訊	54

1 安裝設定 Windows Server 環境中的 NXLog

1.1 For Windows Server 2003

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 :

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi · 點選[Install] · 執行 NXLog 程式後續的安裝步驟 。

3. 下載設定 Windows 2003 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 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 Server 所有 Eventlog 。

使用者若是需要 Windows Server 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 Server 的 Eventlog, 此設定檔會需要 Windows Server 主機配備較高的硬體效能來執行 NXLOG 。

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

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

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

```
Moduledir %ROOT%\modules
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：

```

C:\Program Files (x86)\nxlog\conf\nxlog.conf - Notepad++
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(I) 巨集 執行 外掛模組(P) 視窗(W) ?
nxlog.conf nxlog.log
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 im_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     { \
32         drop(); \
33     }
34 </Input>
35
36 <Output out_eventlog>
37 Module om_udp
38 Host 192.168.2.64
39 Port 514
40 Exec $Message = string($EventID) + " : " + $Message;
41 Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
42     else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
43     else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
44 Exec to_syslog_bsd();
45 </Output>
46
47 <Route eventlog>
48 Path in_eventlog => out_eventlog
49 </Route>
Perl source file length: 2025 lines: 45 Ln: 45 Col: 9 Sel: 0 DosWindows ANSI INS
    
```

5. 啟動 NXLOG：

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
    
```

b. 或是從[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 " 若沒顯示 Error 的訊息，表示正常啟動。

```

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(I) 巨集 執行 外掛模組(P) 視窗(W) ?
nxlog.conf nxlog.log
1 2014-07-04 14:16:08 INFO nxlog-ce-2.7.1191 started
2 2014-07-04 14:16:27 WARNING stopping nxlog service
3 2014-07-04 14:16:27 WARNING nxlog-ce received a termination request signal, exiting...
4 2014-07-04 14:16:29 INFO nxlog-ce-2.7.1191 started
5
Norm length: 244 lines: 5 Ln: 1 Col: 1 Sel: 0 DosWindows ANSI INS
    
```

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

註：因 NXLOG 沒有將事件編碼轉成 UTF8 編碼的功能，所以新增 Windows Server 2003 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 繁體版 請選擇[BIG5]編碼。

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

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

1.2 For Windows Server 2008

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：

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式後續的安裝步驟。

3. 下載 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 " 的 NXLOG 配置檔，將上面的 URL 上的 nxlog_win2k8.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 2008 的 NXLOG 配置檔 nxlog_win2k8_all.conf(輸出全部的 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 Server 所有 Eventlog。使用者若是需要 Windows Server 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 Server 的 Eventlog，此設定檔會需要 Windows Server 主機配備較高的硬體效能來執行 NXLOG。

```

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

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

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

Moduledir %ROOT%\modules
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>

```

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：

```

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 </QueryList> \
61 </Input>
62
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：

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

```

b. 或是從[開始]→[所有程式]→[系統管理工具]→[服務]，右點服務[nxlog]，左點[啟動]或[重新啟動]。

6. 檢查 NXLOG 是否正常啟動：

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

```

C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++
檔案(F) 編輯(E) 尋找(S) 檢視(V) 編碼(N) 程式語言(L) 自訂(T) 巨集 執行 外掛模組(P) 視窗(W) ?
nxlog.conf nxlog.log
1 2014-07-03 17:57:22 WARNING stopping nxlog service
2 2014-07-03 17:57:22 WARNING nxlog-ce received a termination request signal, exiting...
3 2014-07-03 17:57:23 INFO nxlog-ce-2.7.1191 started
4
length: 192 lines: 4 Ln: 1 Col: 1 Sel: 0 Dos\Windows ANSI INS

```

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

1.3 For Windows Server 2012

3. 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。

4. 安裝 NXLOG :

滑鼠雙點剛下載的 nxlog-ce-2.9.1716.msi，點選[Install]，執行 NXLog 程式後續的安裝步驟。

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 " 的 NXLOG 配置檔，將上面的 URL 上的 nxlog_win2012.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 2012 的 NXLOG 配置檔 nxlog_win2012_all.conf (輸出全部的 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 Server 所有 Eventlog。使用者若是需要 Windows Server 的法規報表，請將 nxlog_win2012_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 Server 的 Eventlog，此設定檔會需要 Windows Server 主機配備較高的硬體效能來執行 NXLOG。

```

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

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

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

Moduledir %ROOT%\modules
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>

```

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：

```

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. 啟動 NXLOG：

- a. 滑鼠左點[開始]，滑鼠右點[Windows PowerShell]，左點[以系統管理員身分執行]。
[Windows PowerShell]輸入：

```

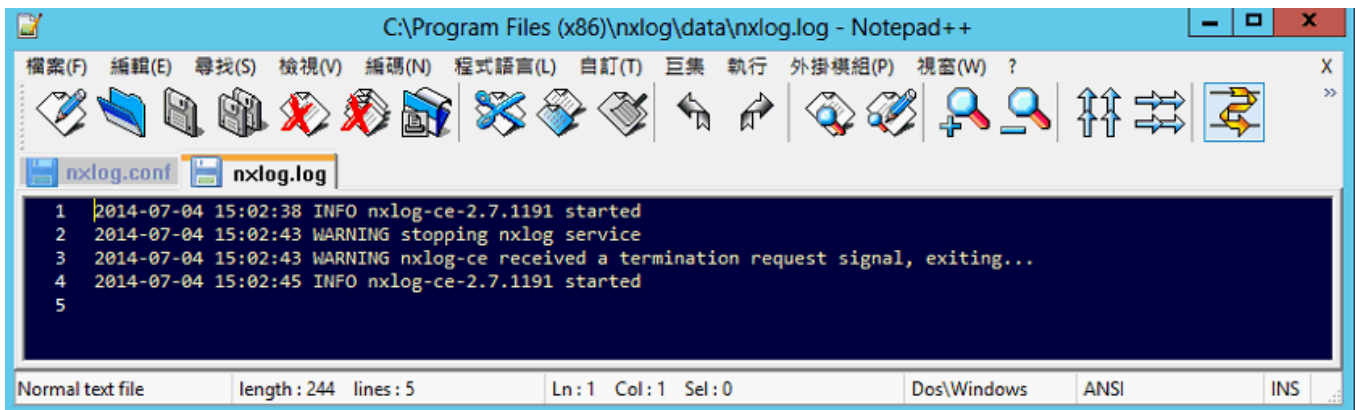
net stop nxlog
net start nxlog

```

- b. 或是從 [開始]→[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。



```

1 2014-07-04 15:02:38 INFO nxlog-ce-2.7.1191 started
2 2014-07-04 15:02:43 WARNING stopping nxlog service
3 2014-07-04 15:02:43 WARNING nxlog-ce received a termination request signal, exiting...
4 2014-07-04 15:02:45 INFO nxlog-ce-2.7.1191 started
5

```

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

2 Windows 2003 Server 稽核設定

本章節說明的 Windows 2003 Server 本機稽核原則，這裡的本機是指該主機為獨立主機，並不屬於任何的網域。

主要說明以下操作設定：

1. 設定本機登入登出的稽核原則。
2. 設定本機共享資料夾權限與稽核原則。

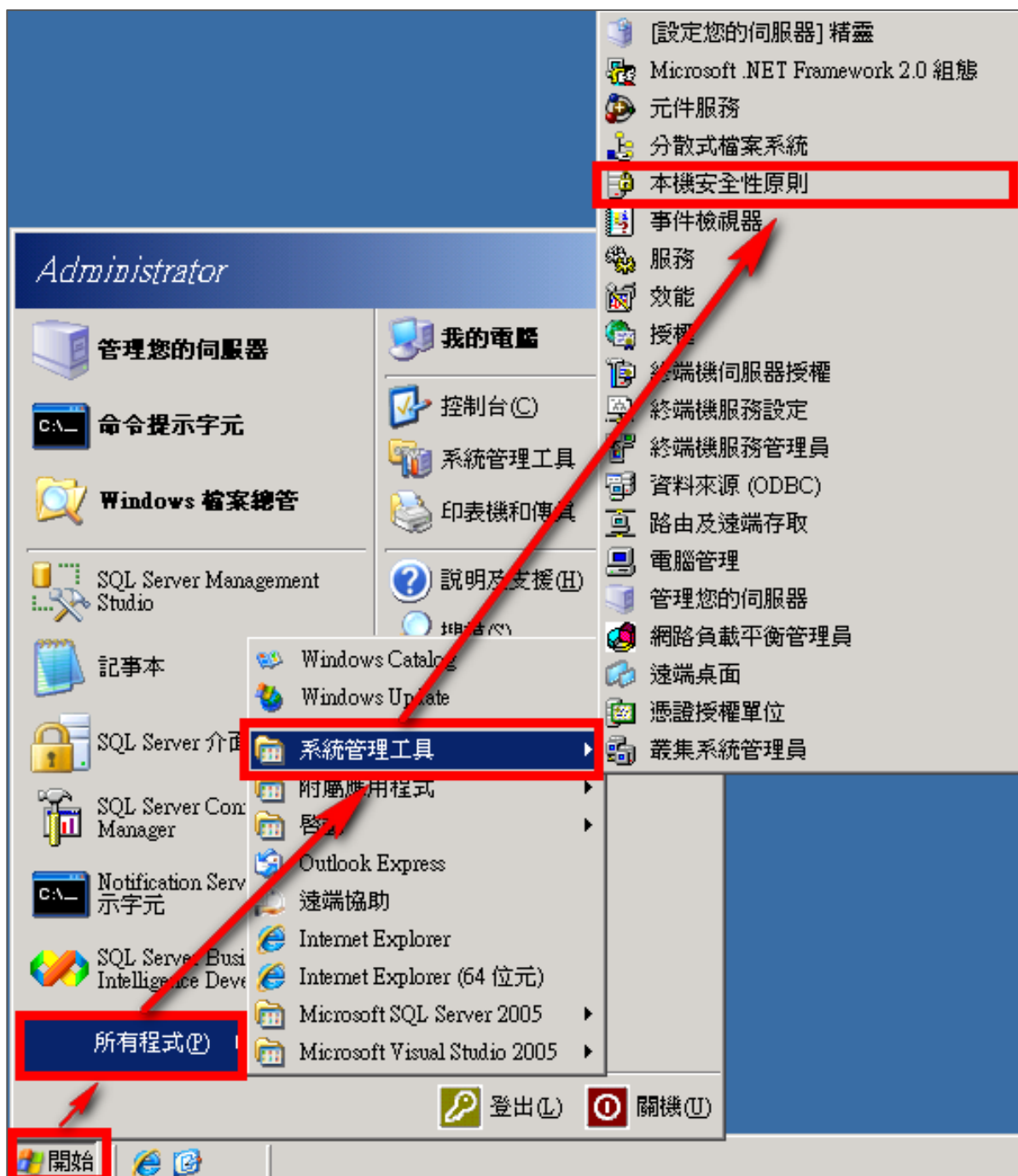
安裝 NXLOG 的步驟，詳細請參閱第一章節。

2.1 設定本機登入登出的稽核原則

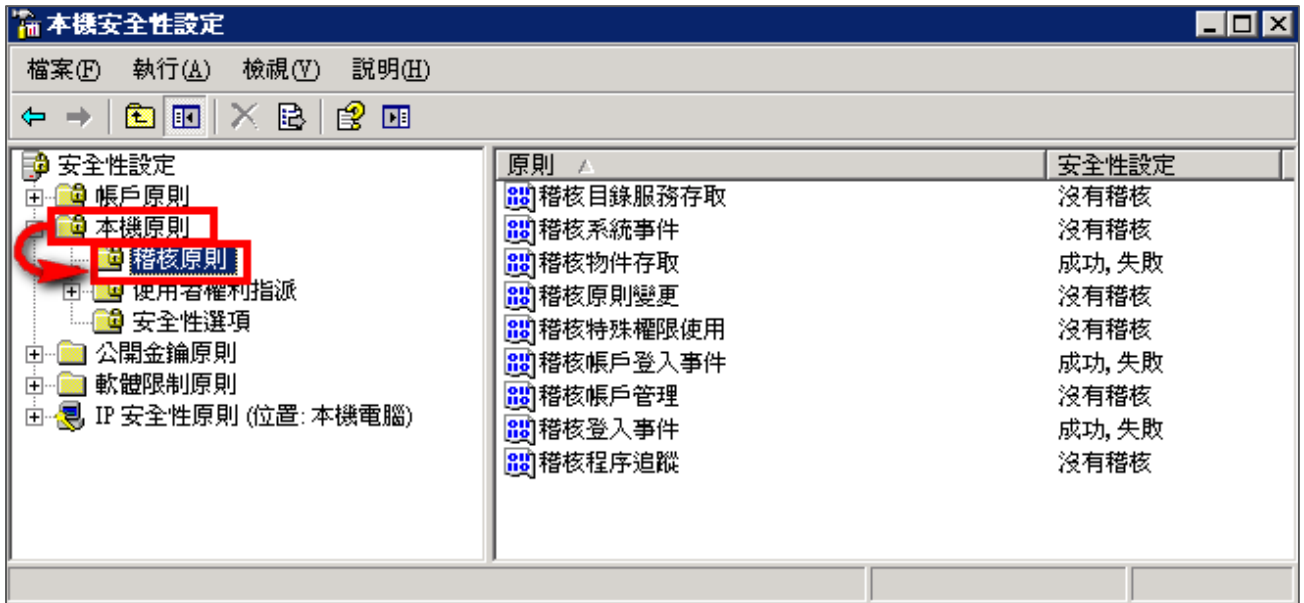
設定步驟如下：

1. 以系統管理員權限的 Administrator 登入 Windows 2003 Server。

點選 [開始功能表 / 所有程式 / 系統管理工具 / 本機安全性原則]。



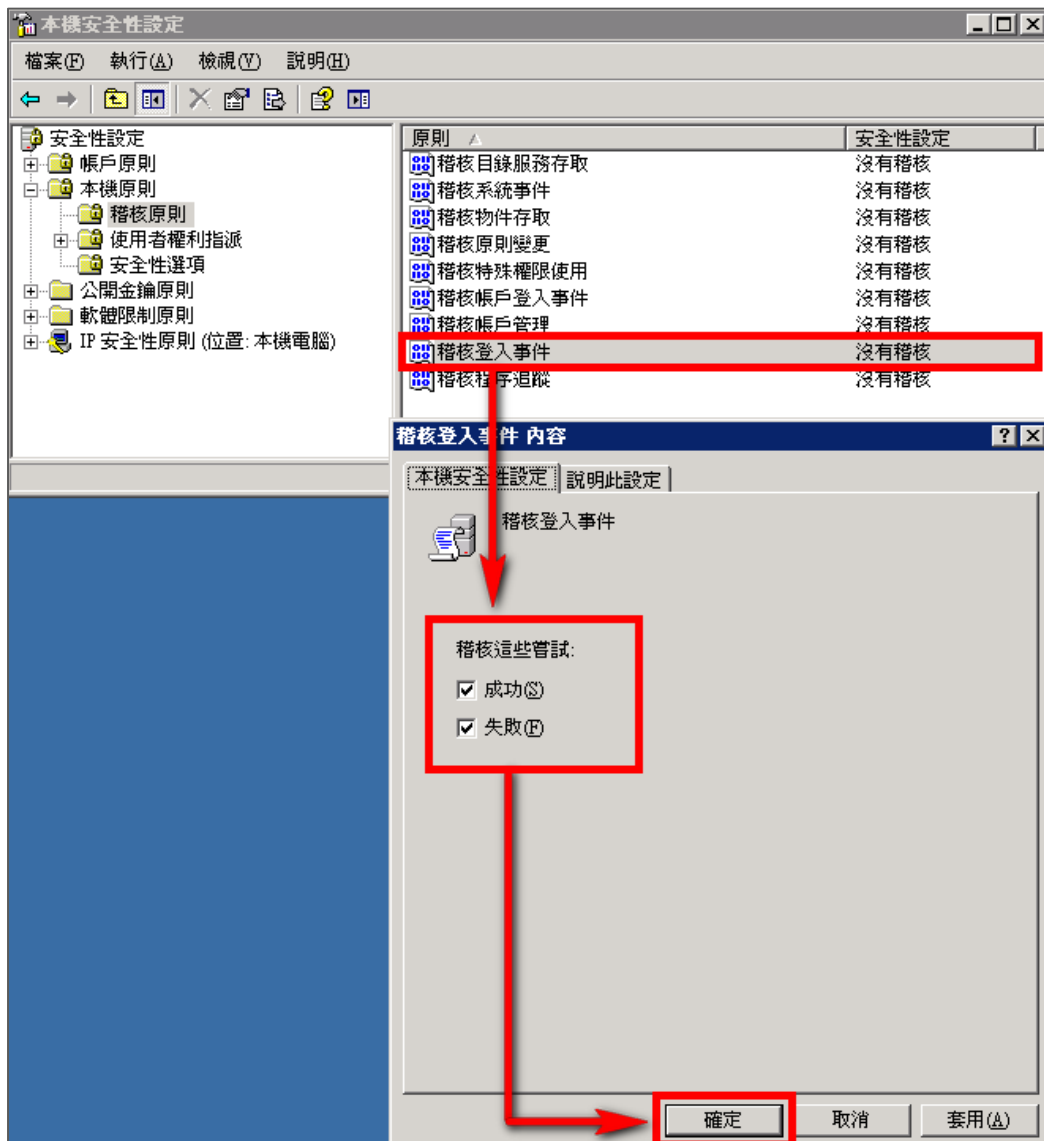
2. 前往 [本機原則 / 稽核原則]



3. 定義下列的原則設定值：

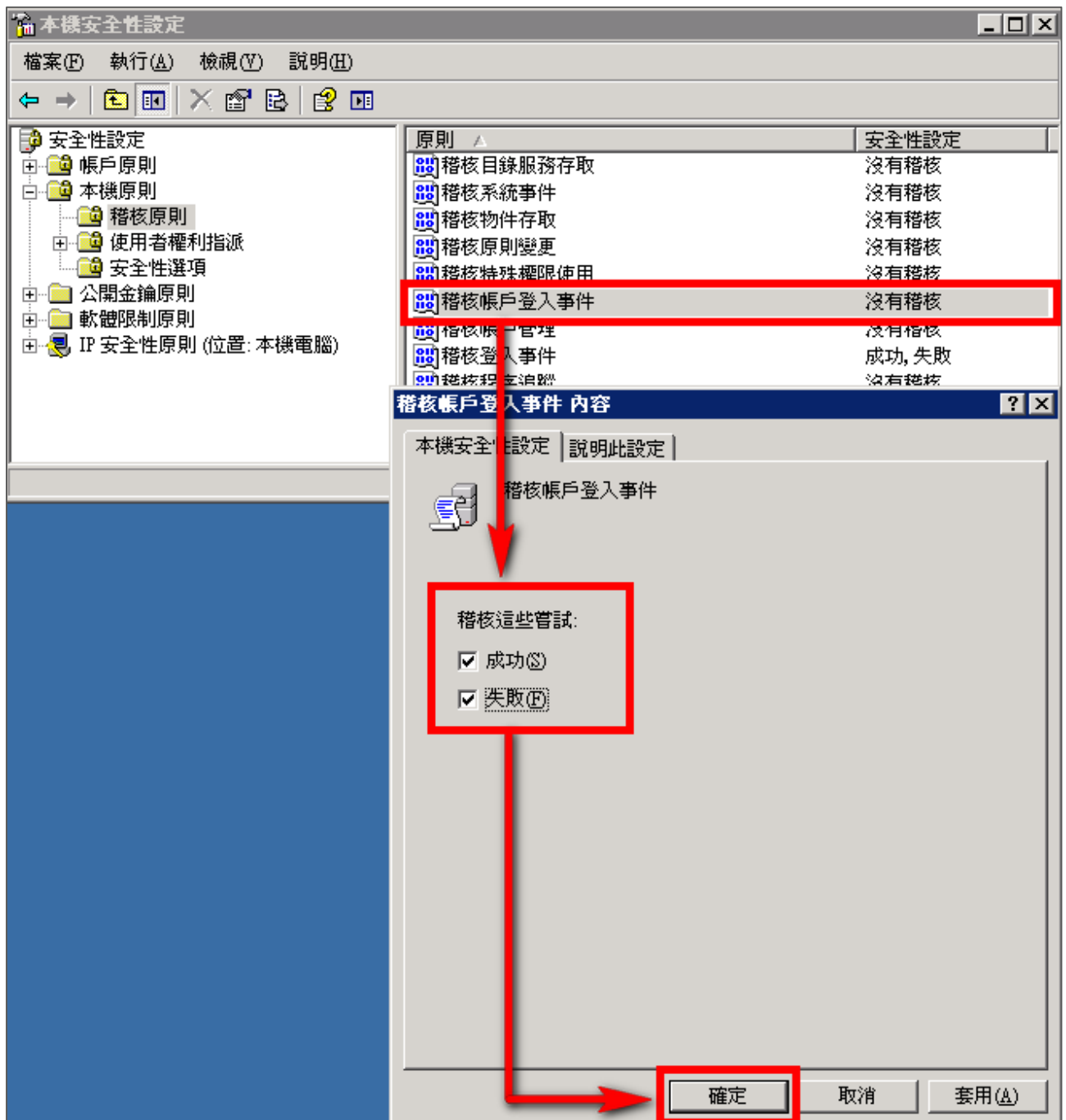
(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [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 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核物件存取：

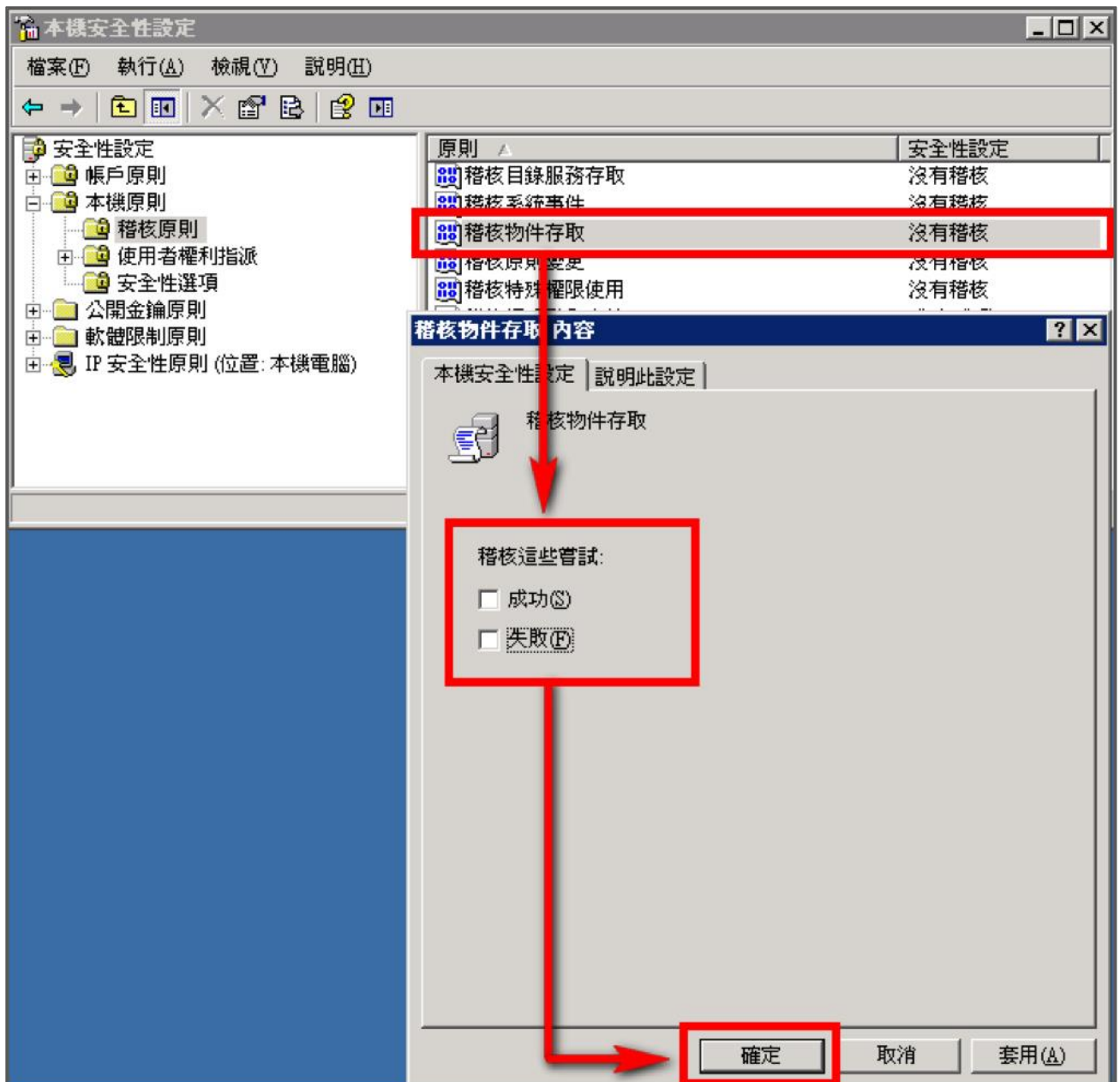
滑鼠雙擊 [稽核物件存取]

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 Server 不做檔案伺服器稽核(File server audit)，建議不要勾選此稽核物件存取的成功與失敗的設定值，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 [成功] 及 [失敗]，設定完成後按 [確定]。

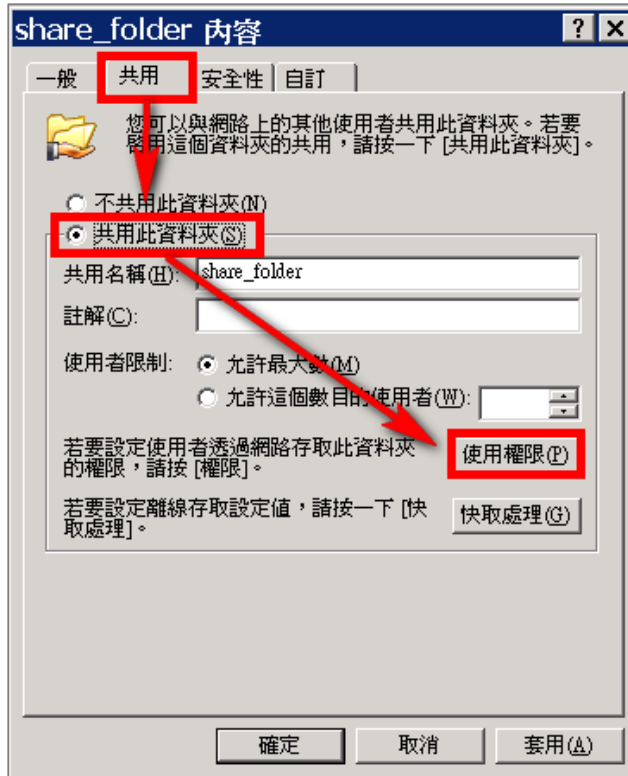
(5) 稽核帳戶管理：

滑鼠雙擊 [稽核帳戶管理]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

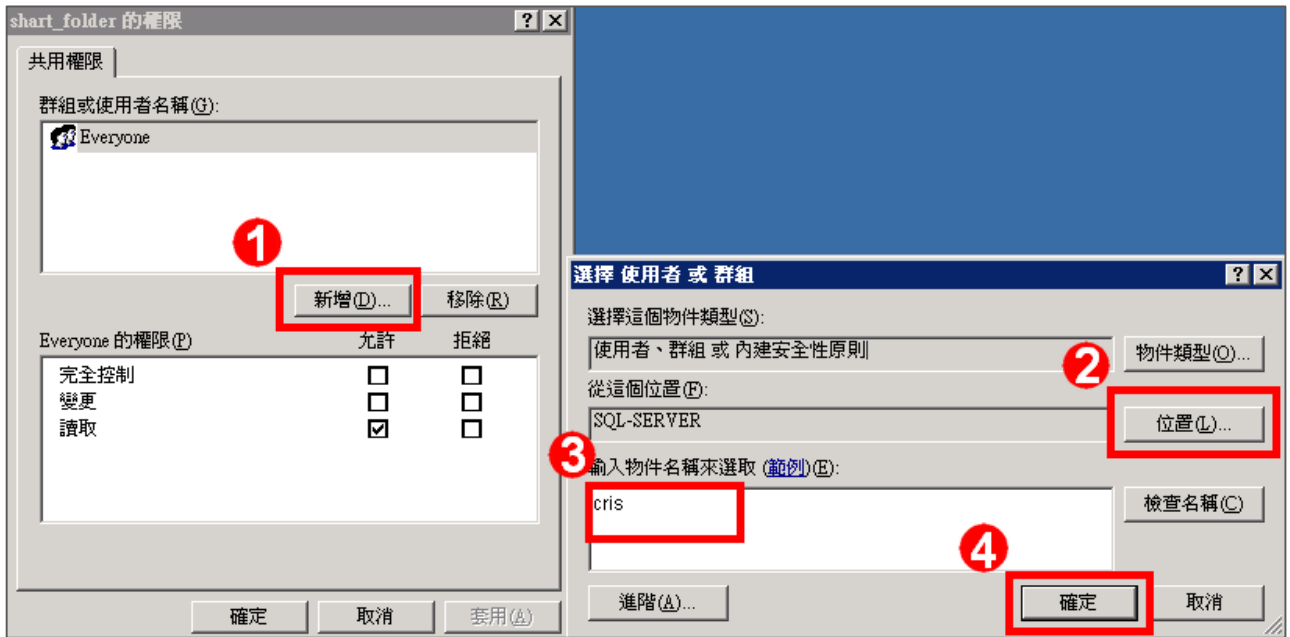
2.2 設定本機共享資料夾權限與稽核原則

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]。

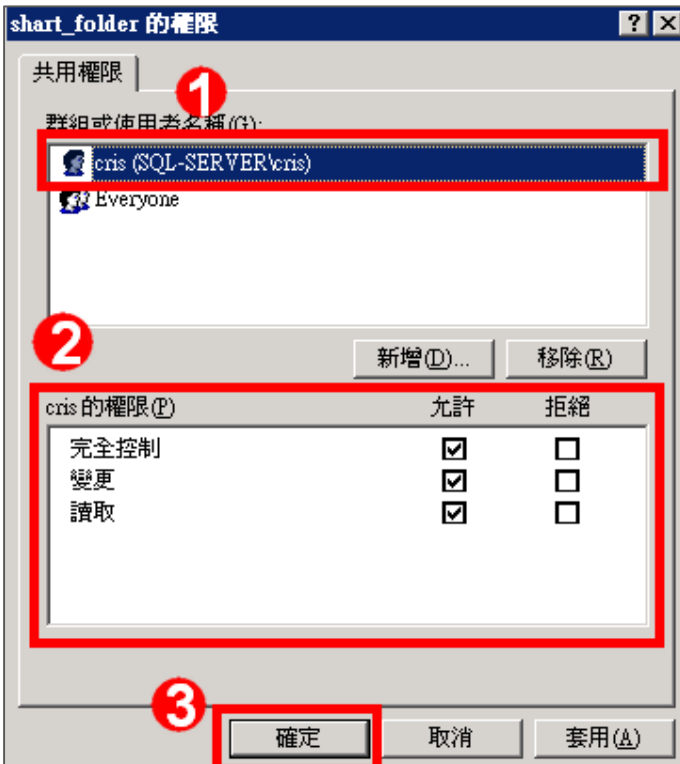


3. 使用者設定：
 - (1) 點選 [新增]，來新增一使用者。
 - (2) 若要選擇其他電腦名稱，可點選 [位置]，選擇其他電腦名稱。
 - (3) 可於此空白處直接輸入已知的使用者帳號後，按 [檢查名稱] 檢查存不存在。
 - (4) 若使用者帳號存在的話，按 [確定] 完成設定。



4. 設定使用者權限：

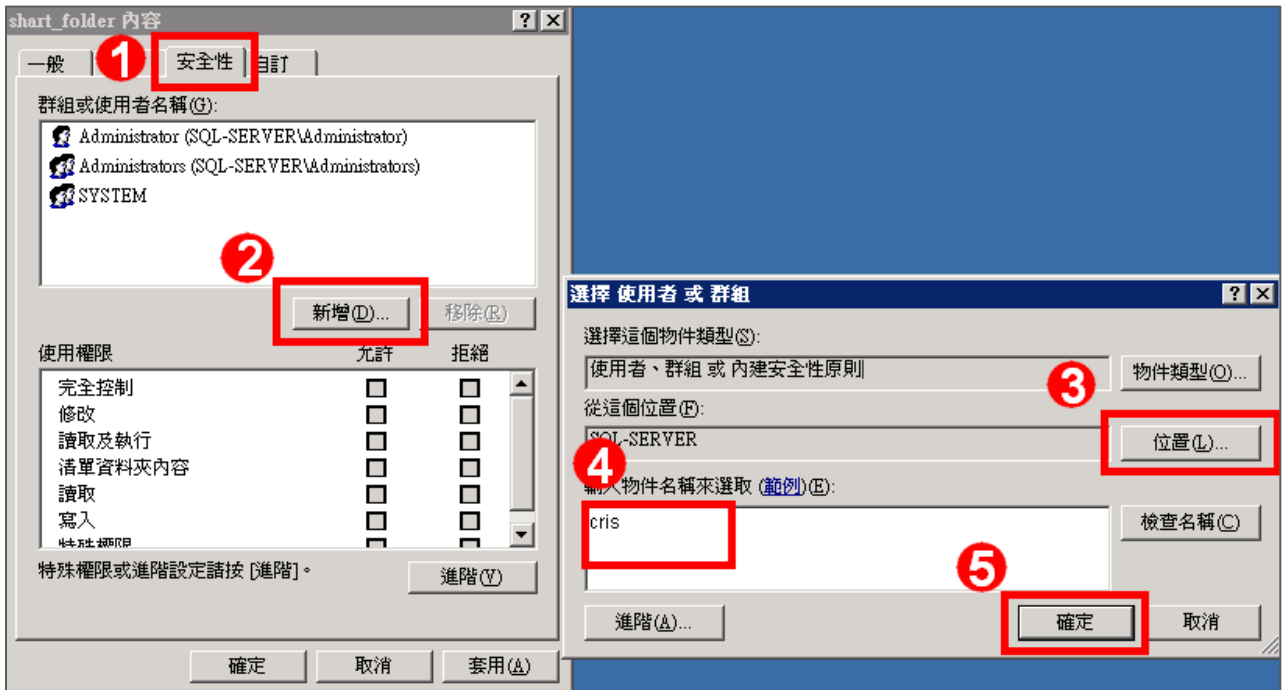
- (1) 點選使用者帳號。
- (2) 勾選允許 [完全控制] 及 [變更] 權限。
- (3) 設定完成後按 [確定]。



5. 安全性設定：

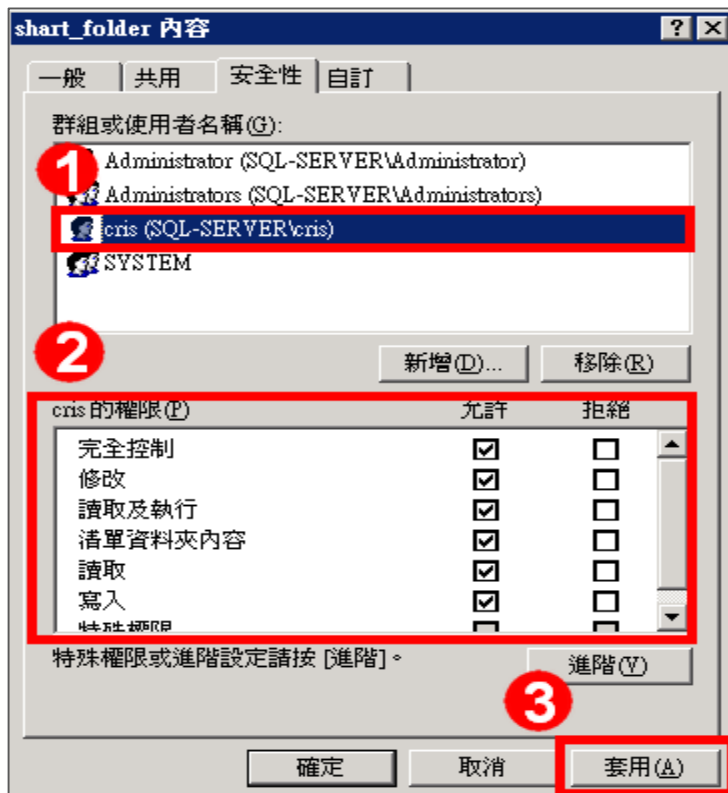
- (1) 點選 [安全性] 索引標籤。
- (2) 點選 [新增]，來新增一使用者。
- (3) 若要選擇其他電腦名稱，可點選 [位置]，選擇其他電腦名稱。
- (4) 可於此空白處直接輸入已知的使用者帳號後，按 [檢查名稱] 檢查存不存在。

(5) 若使用者帳號存在的話，按 [確定] 完成設定。



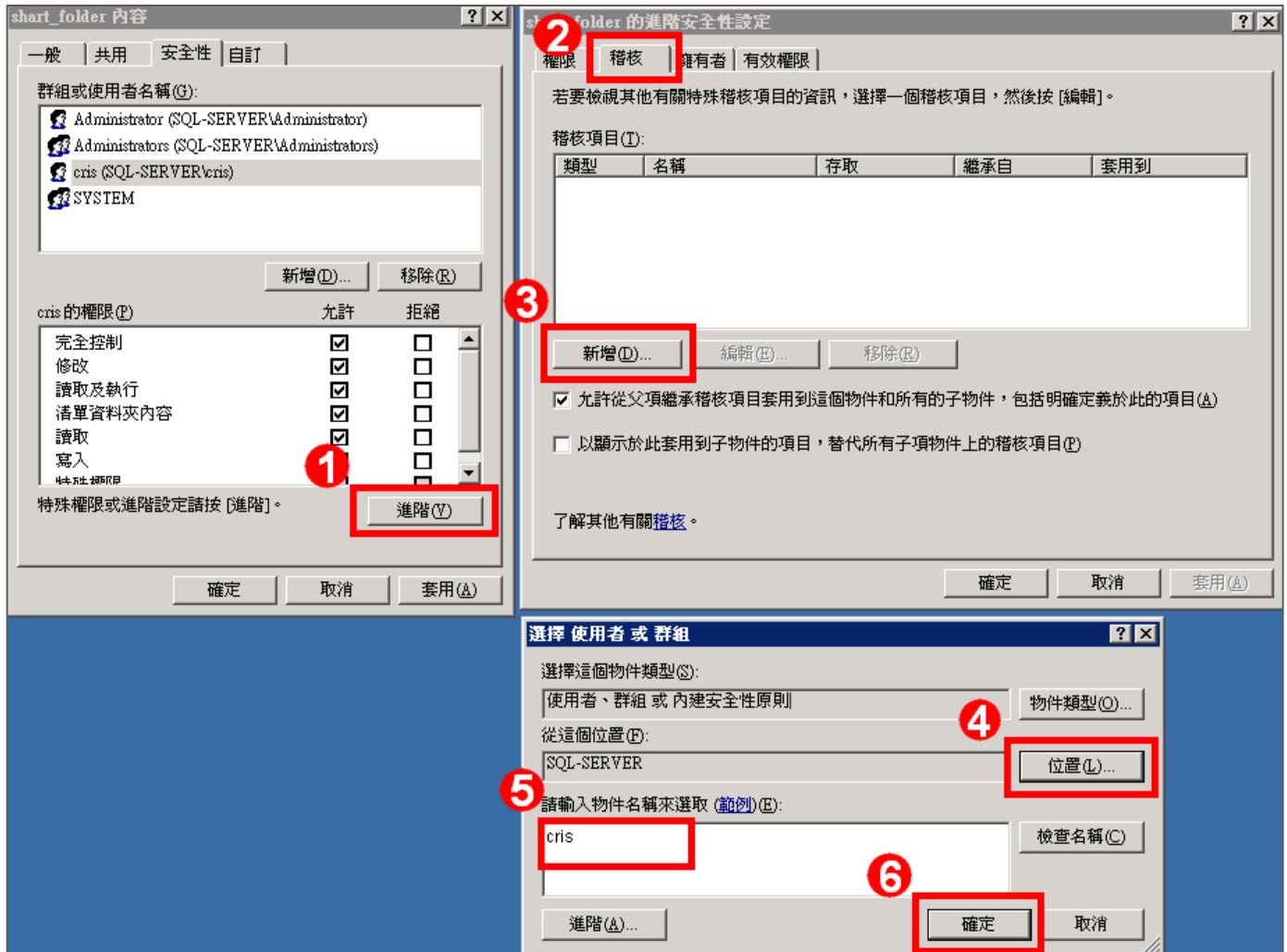
6. 設定使用者權限：

- (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 [套用]。



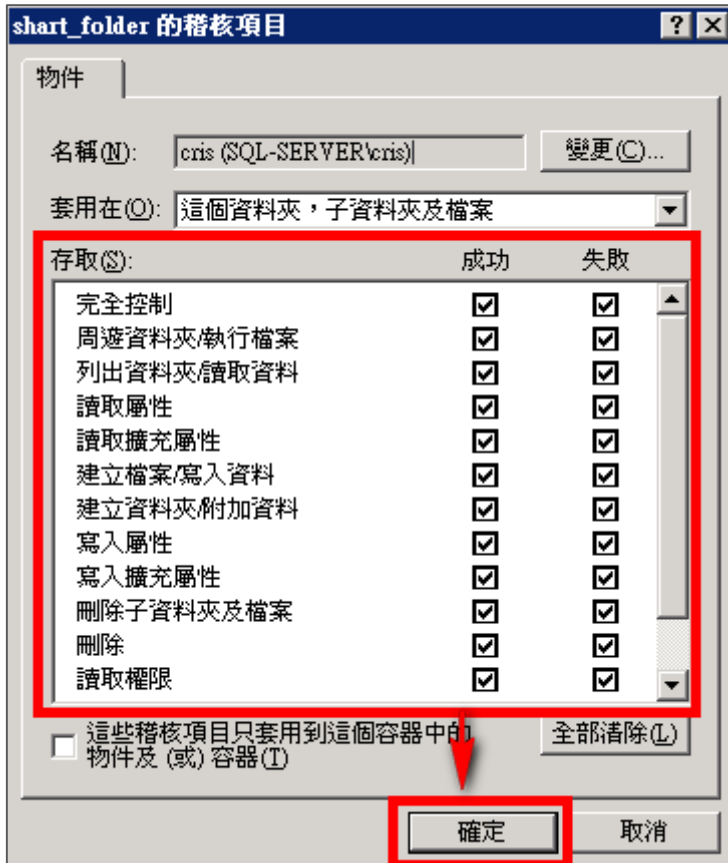
7. 進階安全性設定：

- (1) 點選 [進階]。
- (2) 點選 [稽核] 索引標籤。
- (3) 點選 [新增]。
- (4) 若要選擇其他電腦名稱，可點選 [位置]，選擇其他電腦名稱。
- (5) 可於此空白處直接輸入已知的使用者帳號後，按[檢查名稱]檢查存不存在。
- (6) 若使用者帳號存在的話，按 [確定] 完成設定。

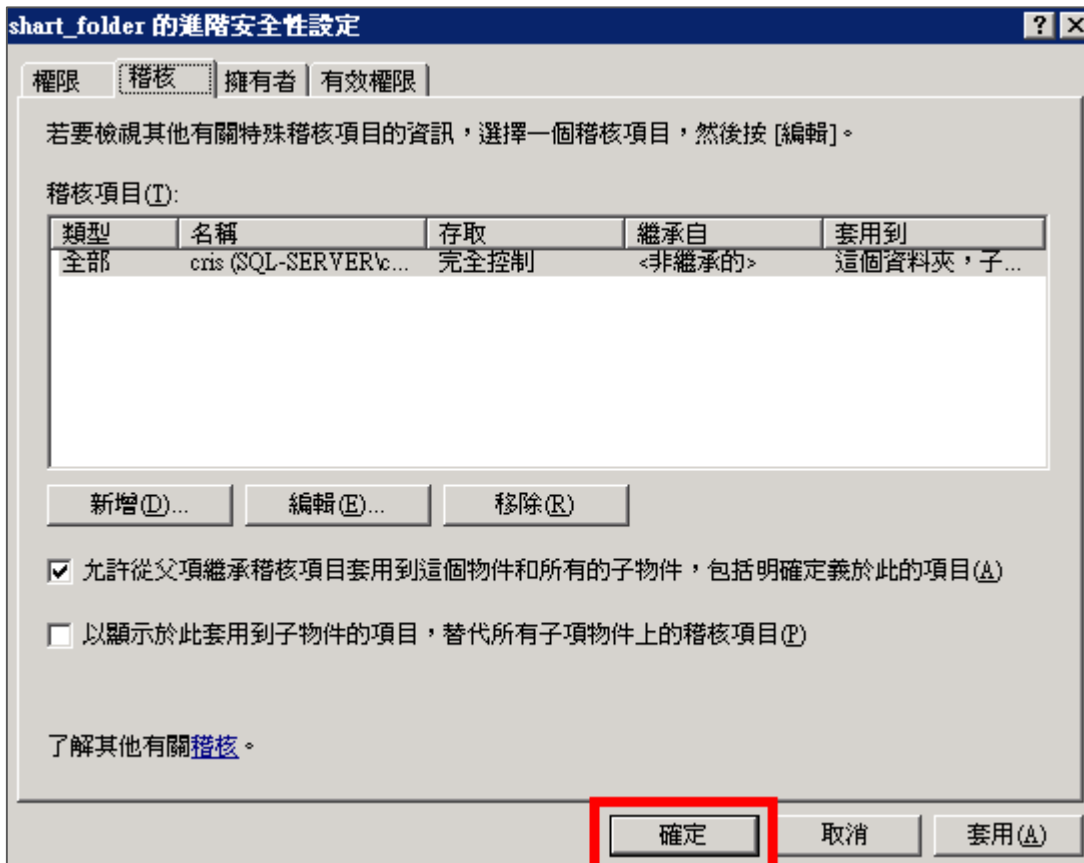


8. 稽核項目設定：

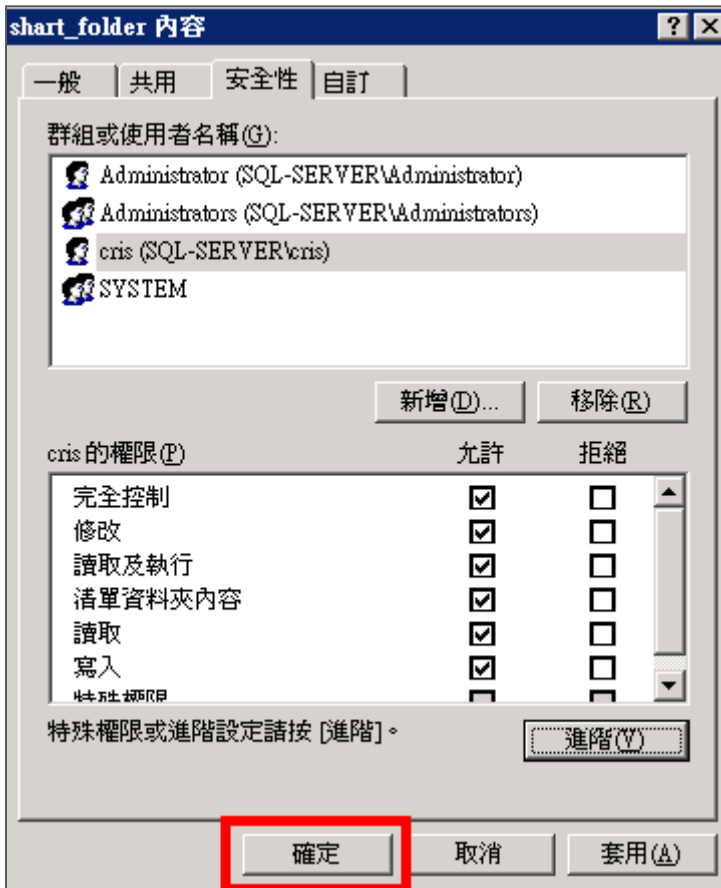
勾選所有稽核項目的 [成功] 及 [失敗] 的項目，設定完成後按 [確定]。



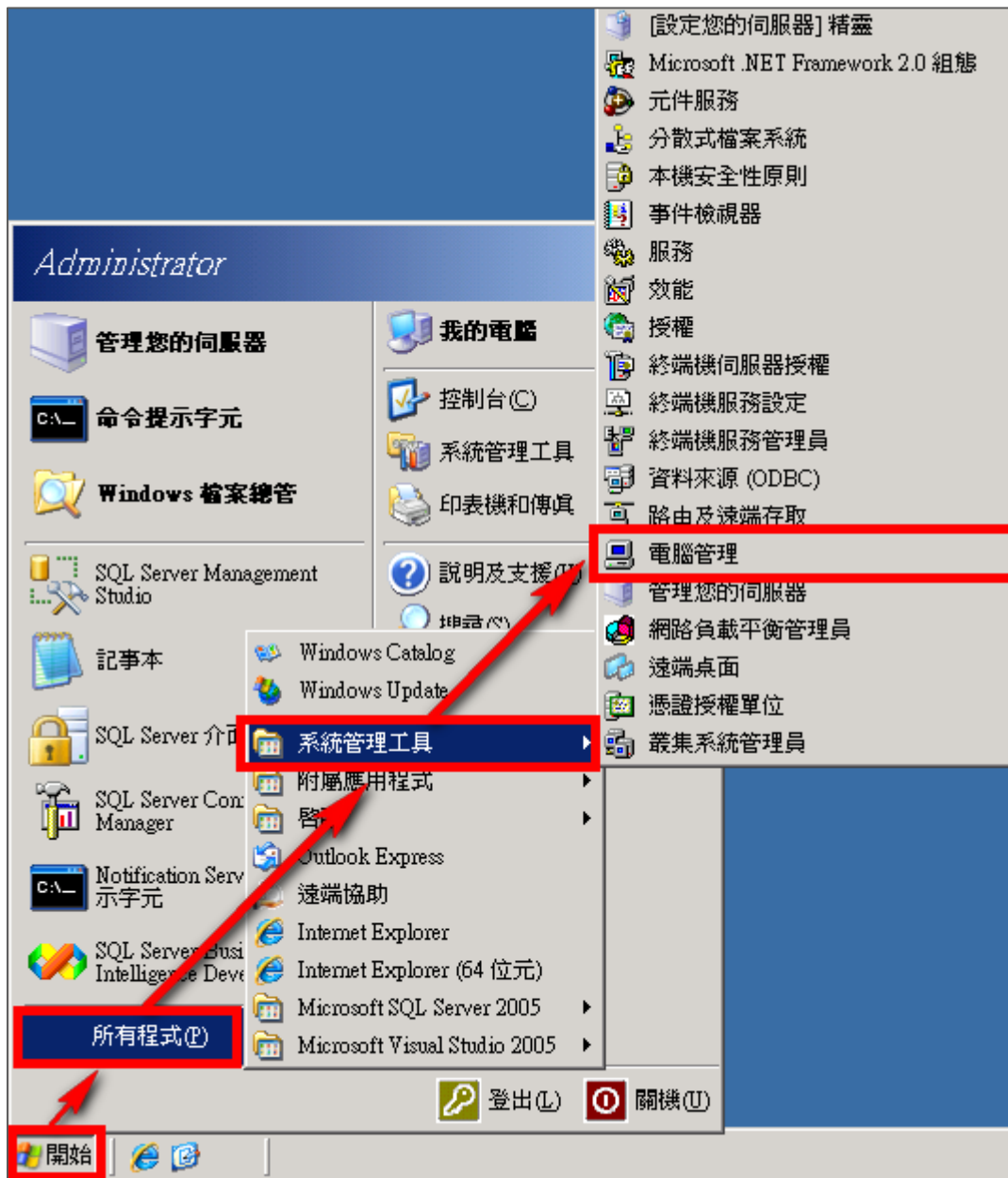
9. 在進階安全性設定完成後，點選 [確定]。



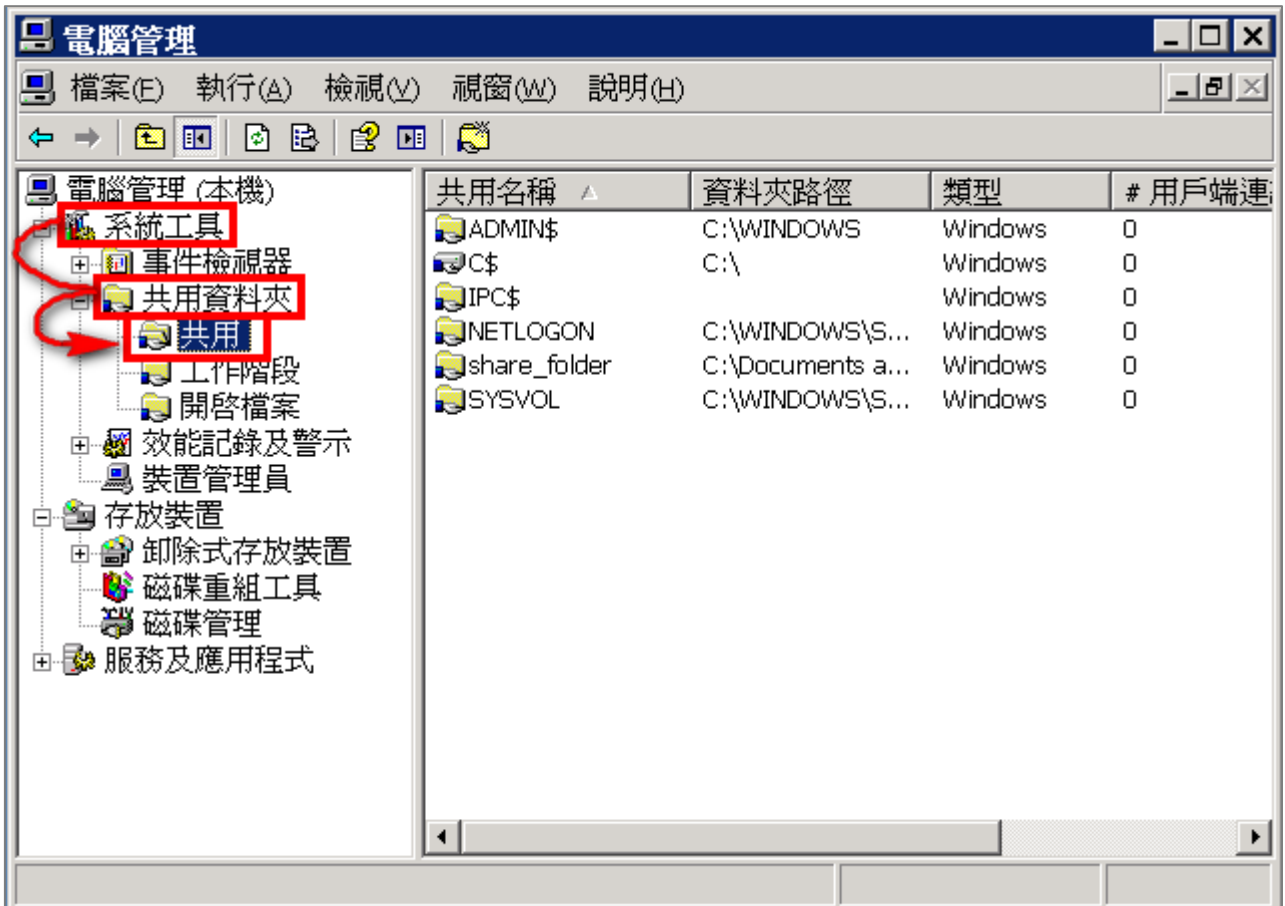
10. 在分享資料夾設定完成後，點選 [確定]。



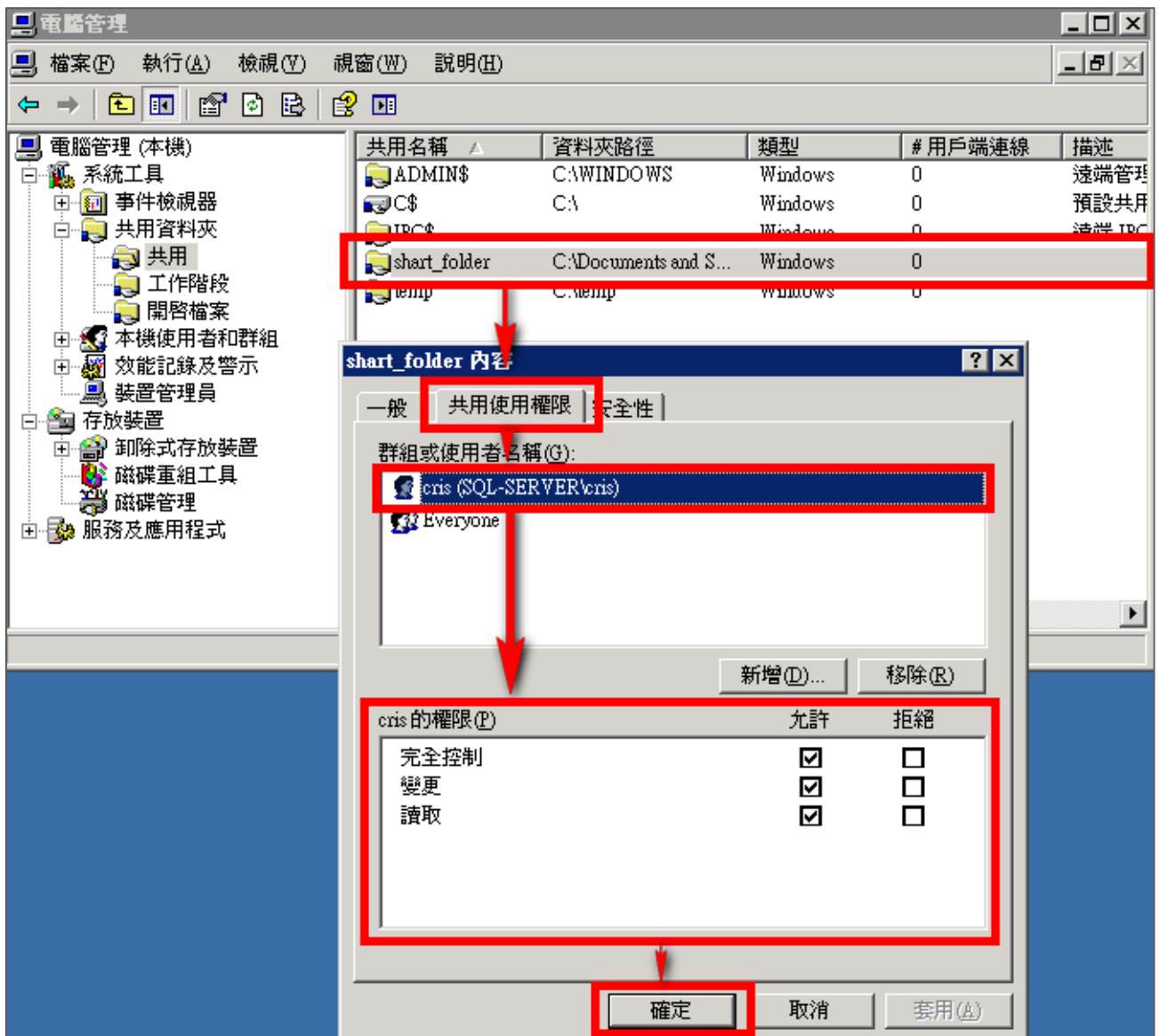
11. 點選 [開始功能表 / 所有程式 / 系統管理工具 / 電腦管理]。



12. 點選 [系統工具 / 共用資料夾 / 共用]。



13. 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 Server 稽核設定

本章節說明的 Windows 2008 Server 本機稽核原則，這裡的本機是指該主機為獨立主機，並不屬於任何的網域。

主要說明以下操作設定：

1. 設定本機登入登出的稽核原則。
2. 設定本機共享資料夾權限與稽核原則。

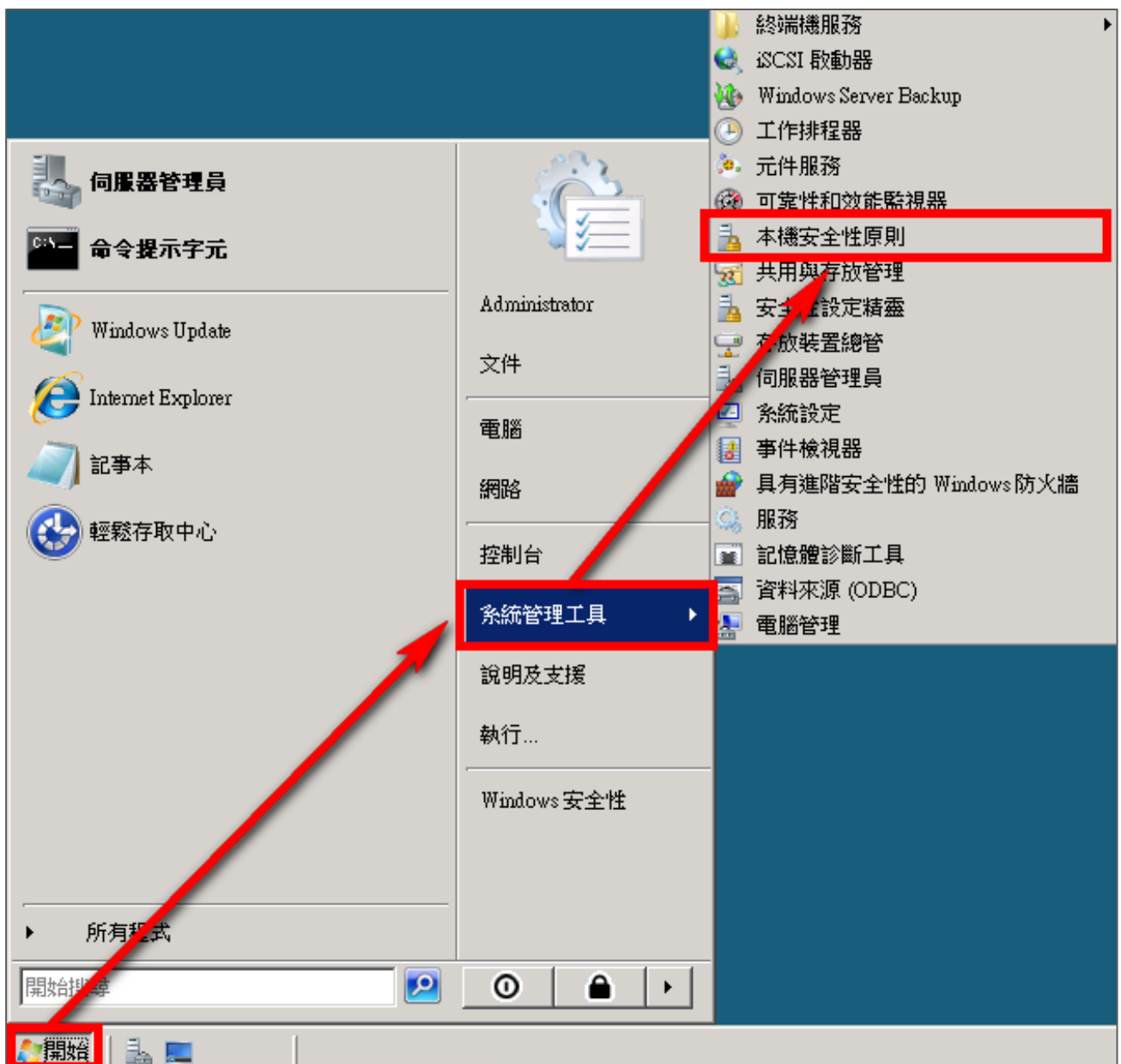
安裝 NXLOG 的步驟，詳細請參閱第一章節。

3.1 設定本機登入登出的稽核原則

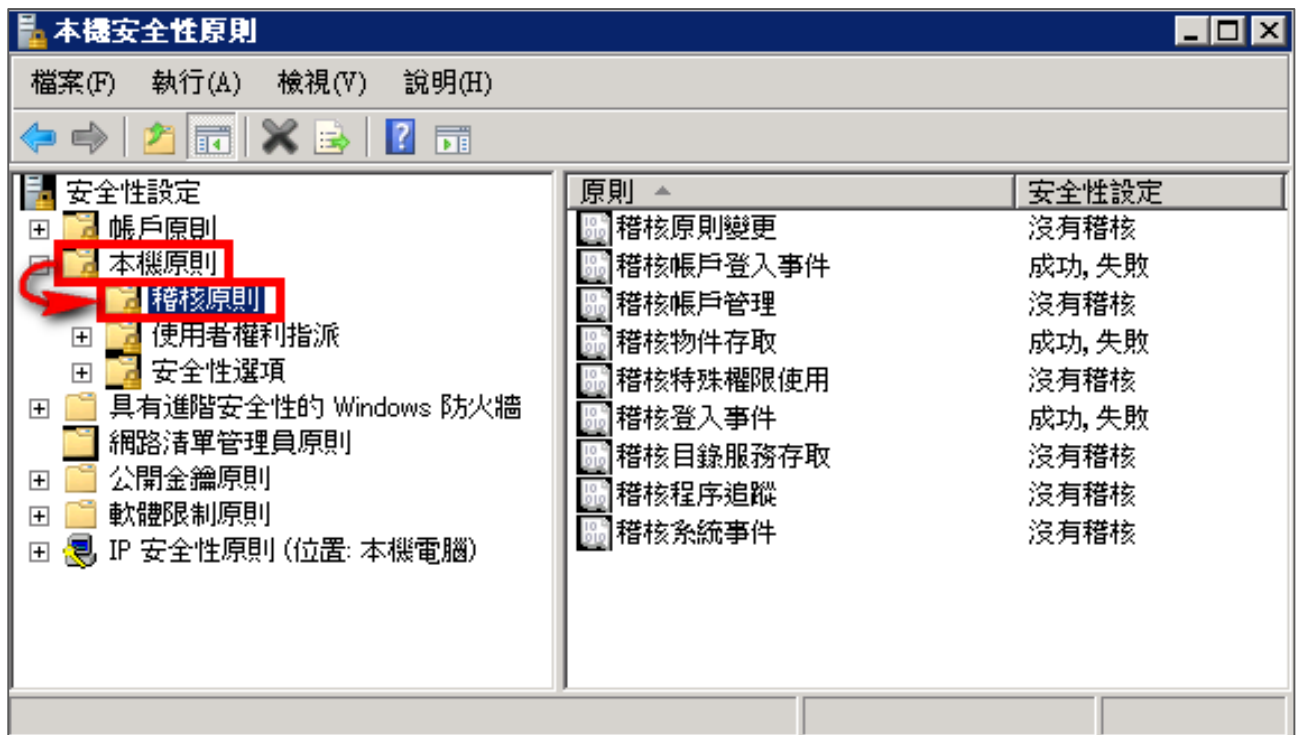
設定步驟如下：

1. 以系統管理員權限的 Administrator 登入 Windows 2008 Server。

點選 [開始功能表 / 系統管理工具 / 本機安全性原則]。



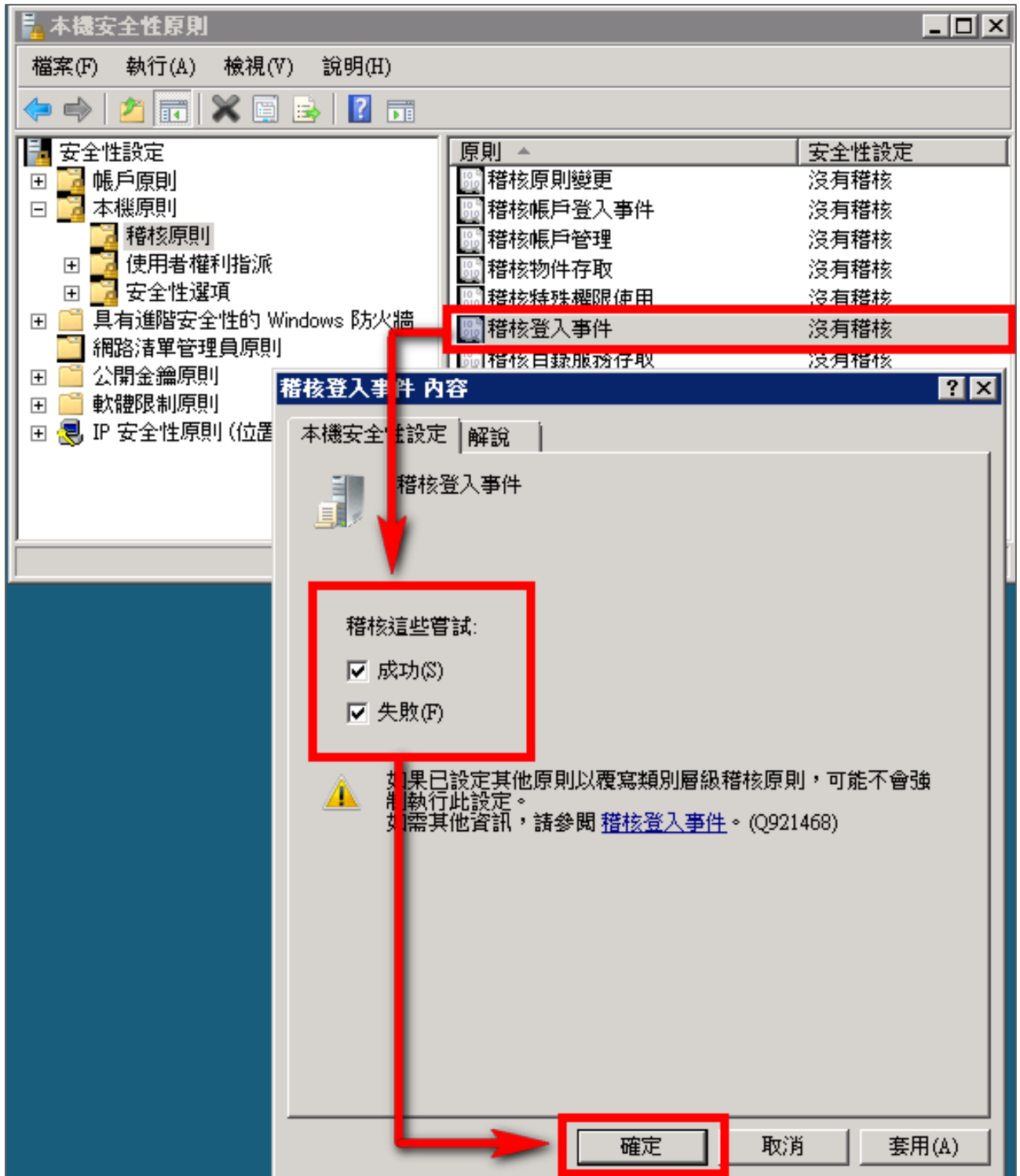
2. 前往 [本機原則 / 稽核原則]。



3. 定義下列的原則設定值：

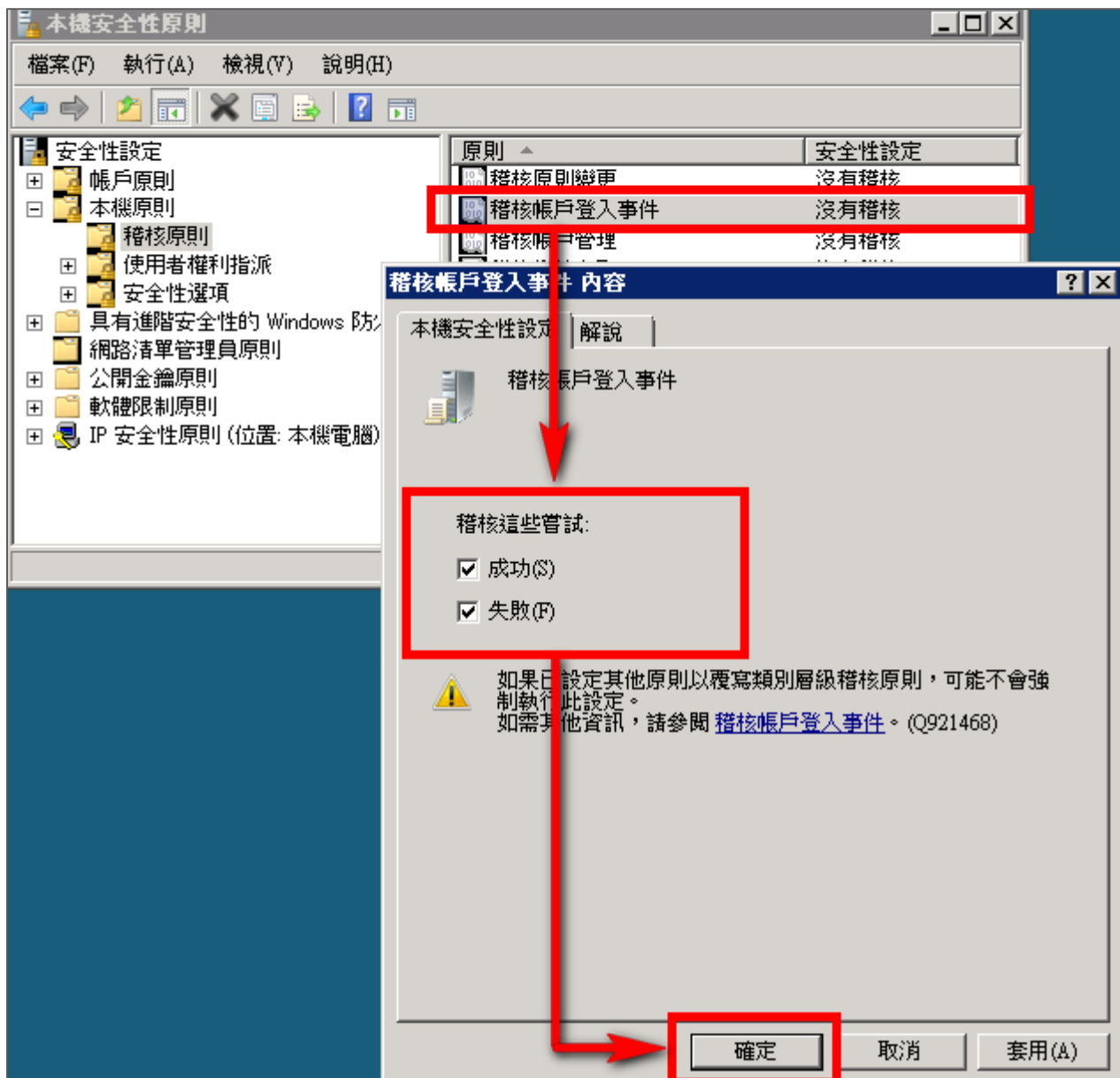
(1) 稽核登入事件：

滑鼠雙擊 [稽核登入事件]，勾選 [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 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核物件存取：

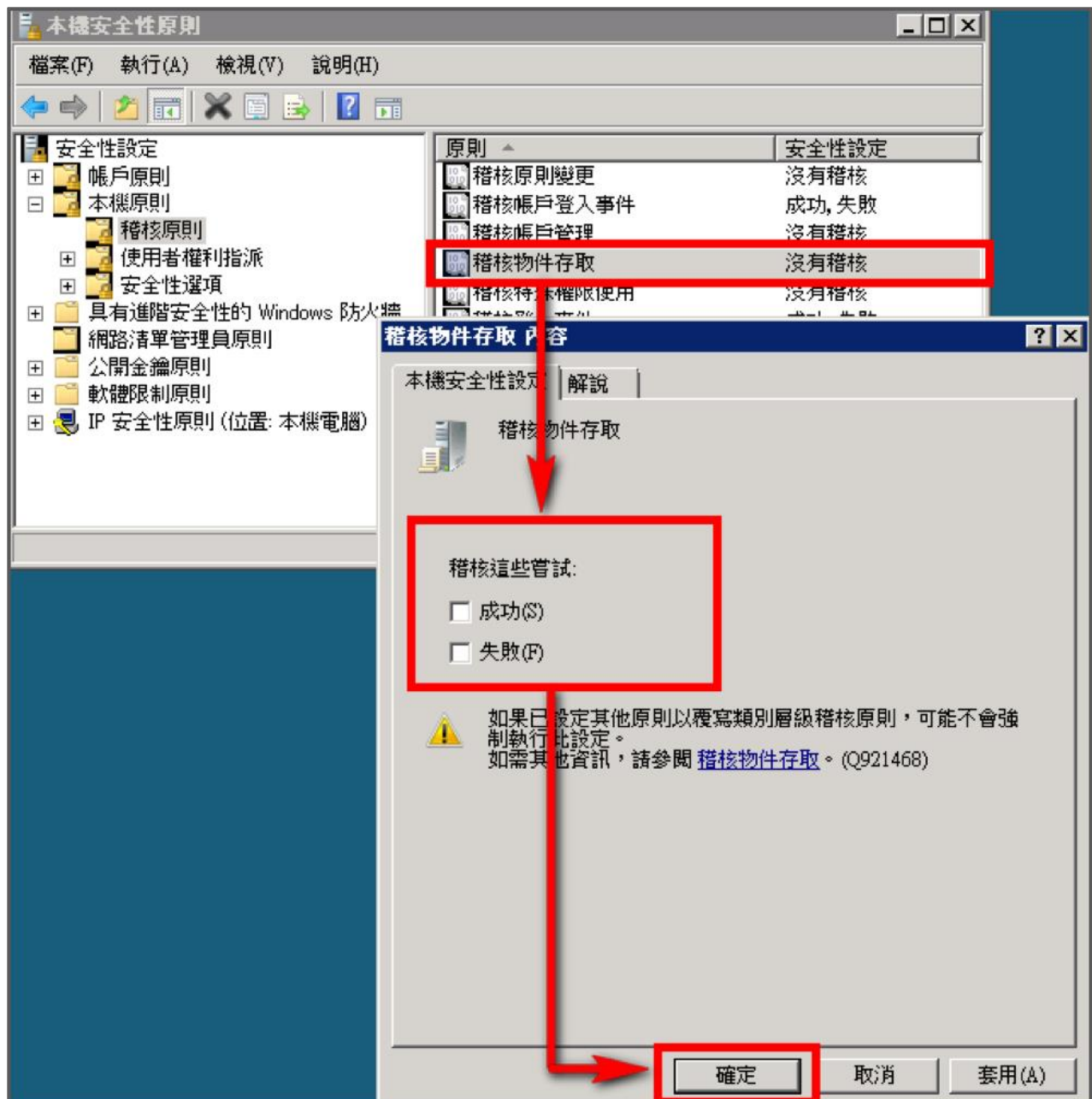
滑鼠雙擊 [稽核物件存取]

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 Server 不做檔案伺服器稽核(File server audit)，建議不要勾選此稽核物件存取的成功與失敗的設定值，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 [成功] 及 [失敗]，設定完成後按 [確定]。

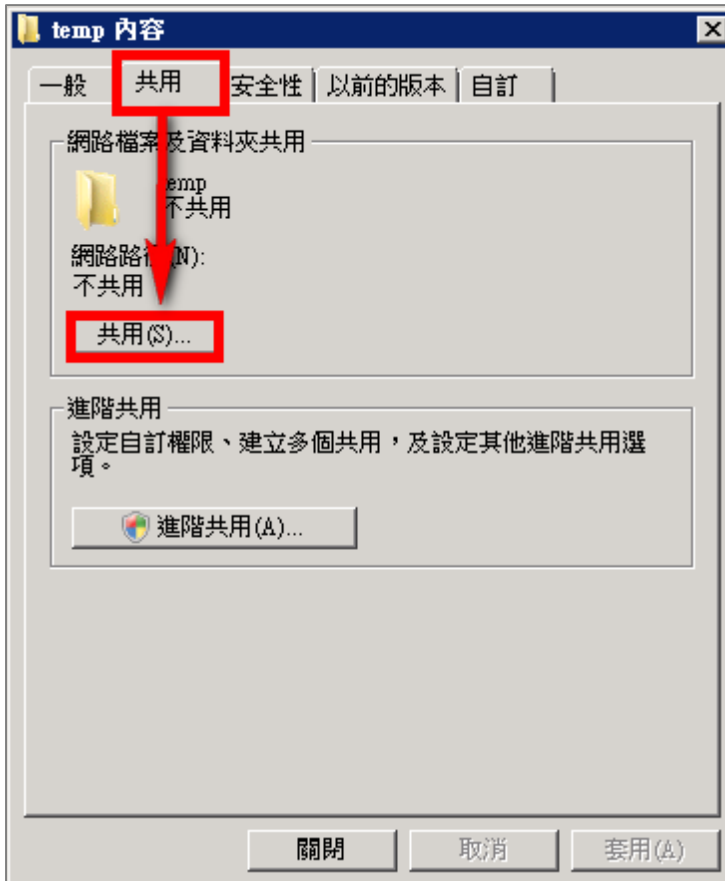
(5) 稽核帳戶管理：

滑鼠雙擊 [稽核帳戶管理]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

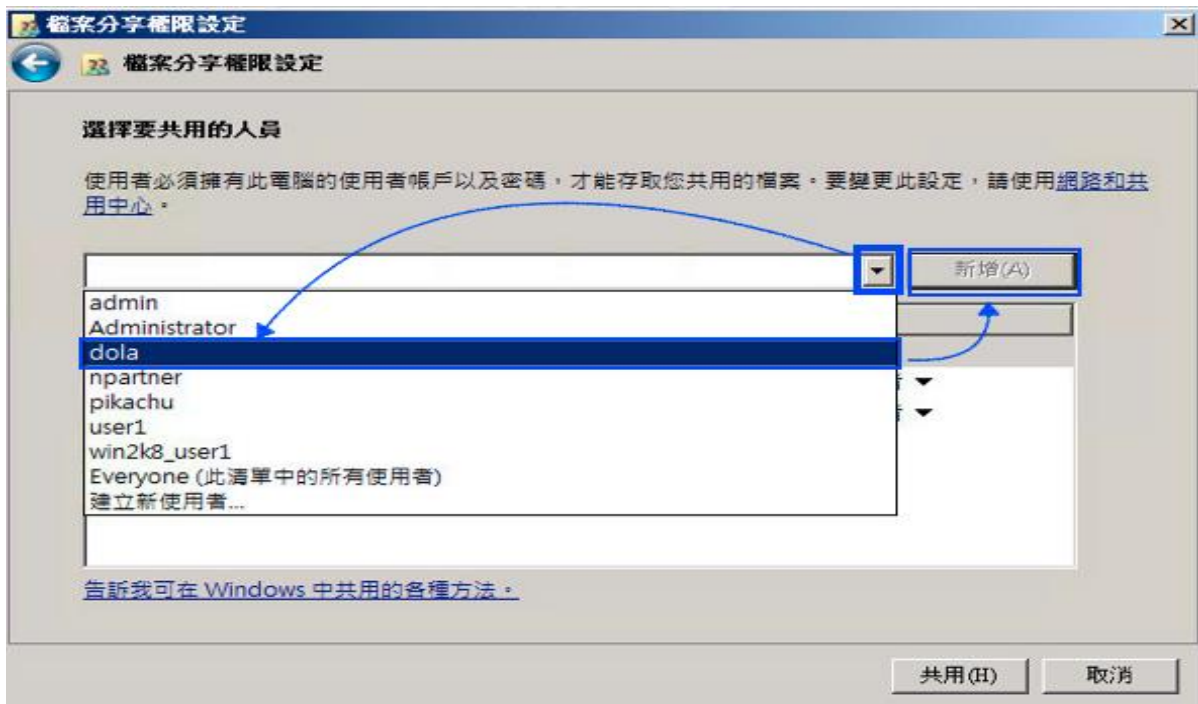
3.2 設定本機共享資料夾權限與稽核原則

設定步驟如下：

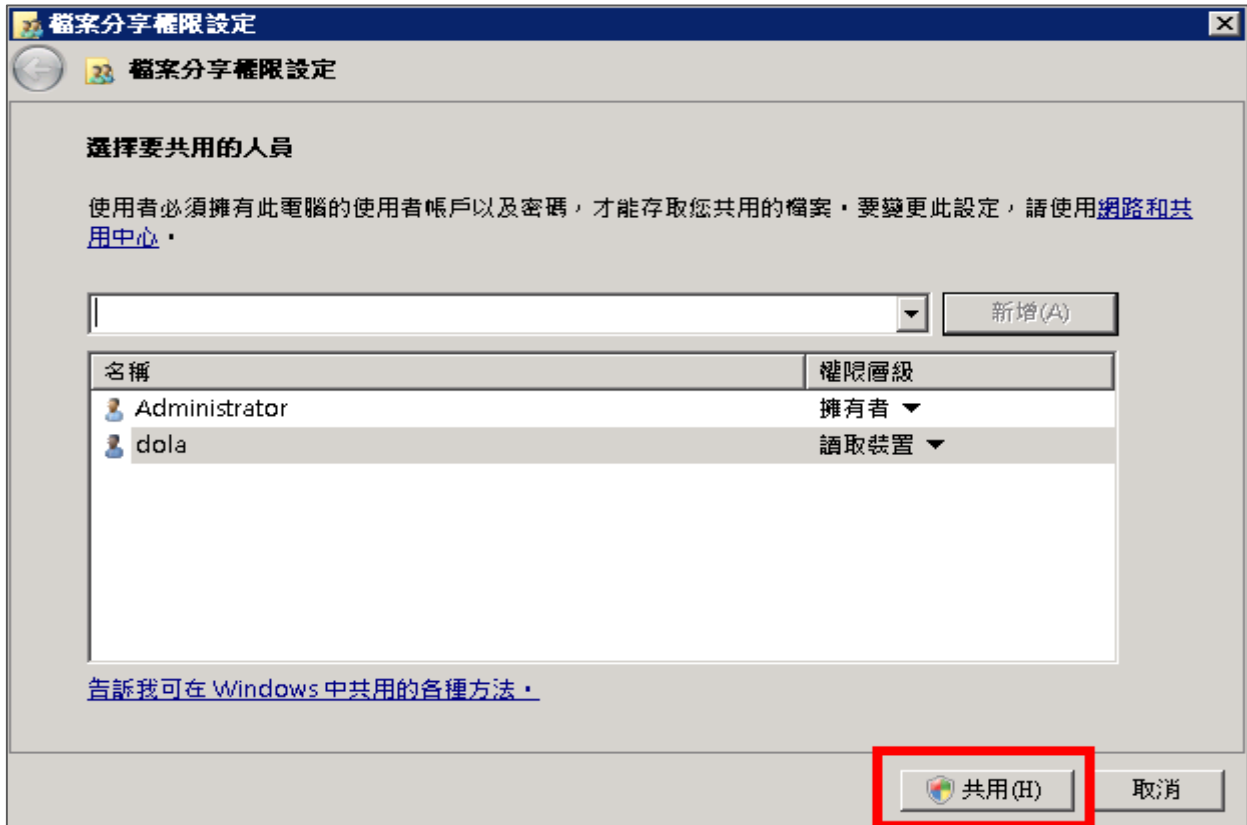
1. 在欲共用的資料夾上點擊滑鼠右鍵，點選 [內容]。
2. 點選 [共用] 索引標籤，點選 [共用]。



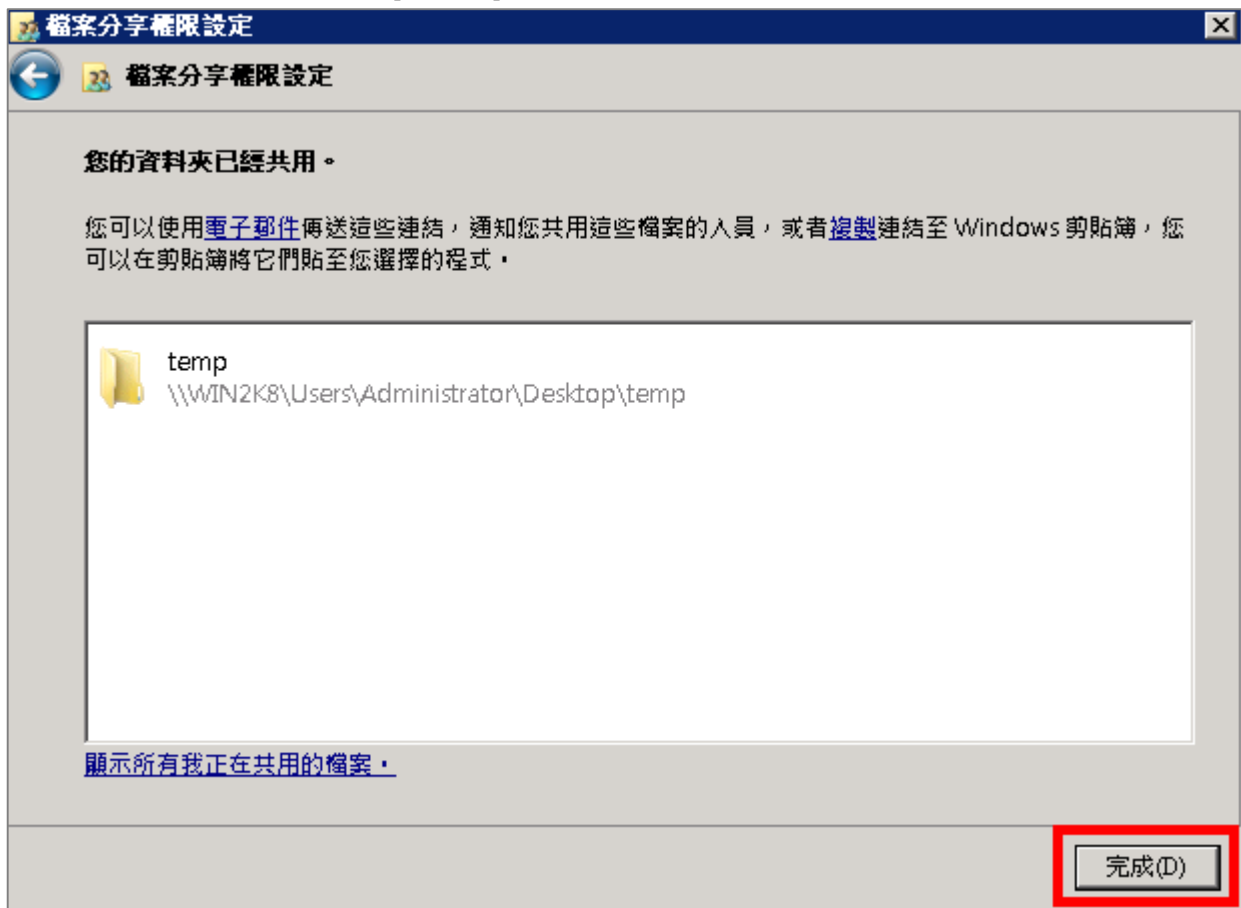
- 在檔案分享權限設定中，點下拉選單，選擇一位此電腦中已建立的使用者帳戶後，此文件例子為選擇 dola，選擇完使用者帳戶後點選 [新增]。



- 點選 [共用]。

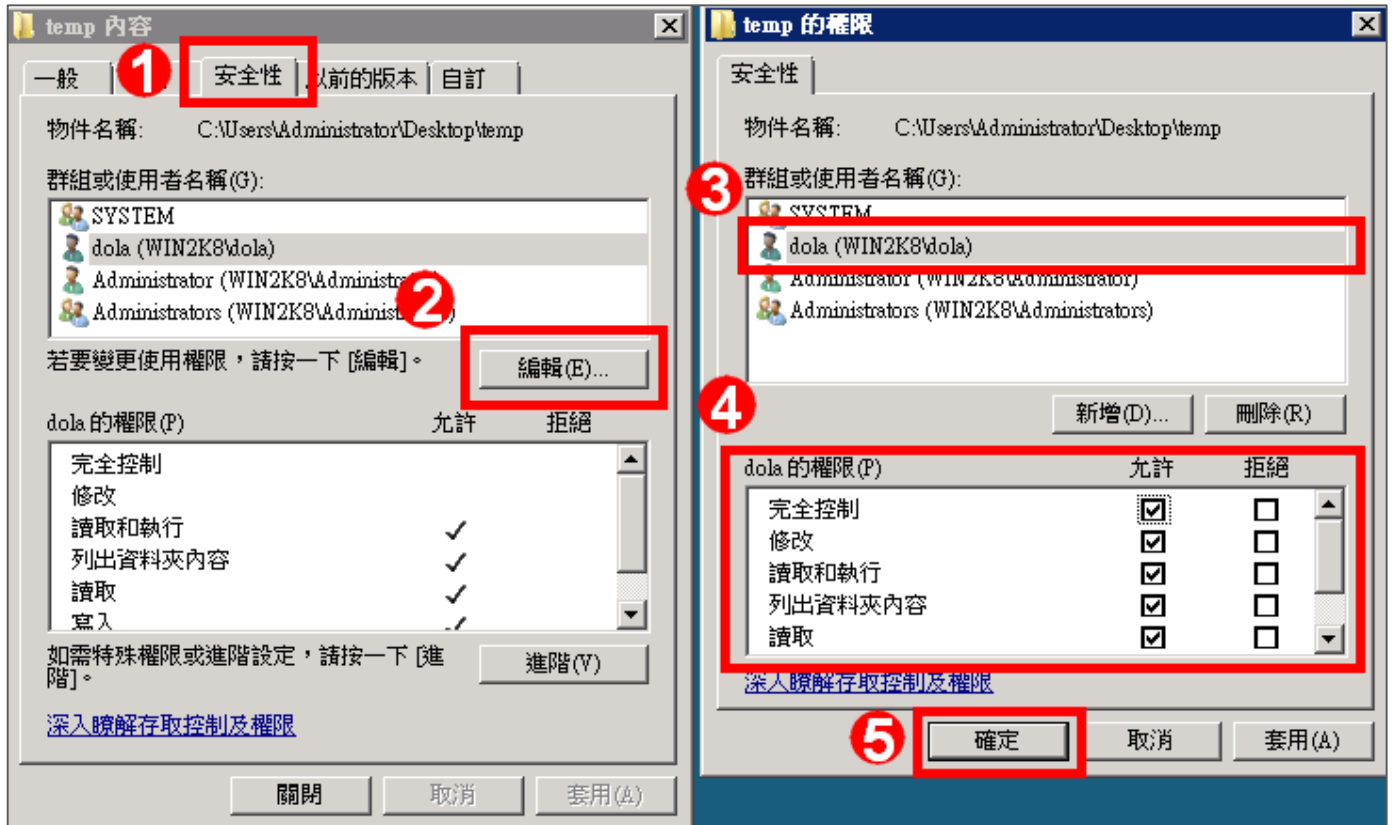


5. 等待共用設定完成後，再按 [完成]。



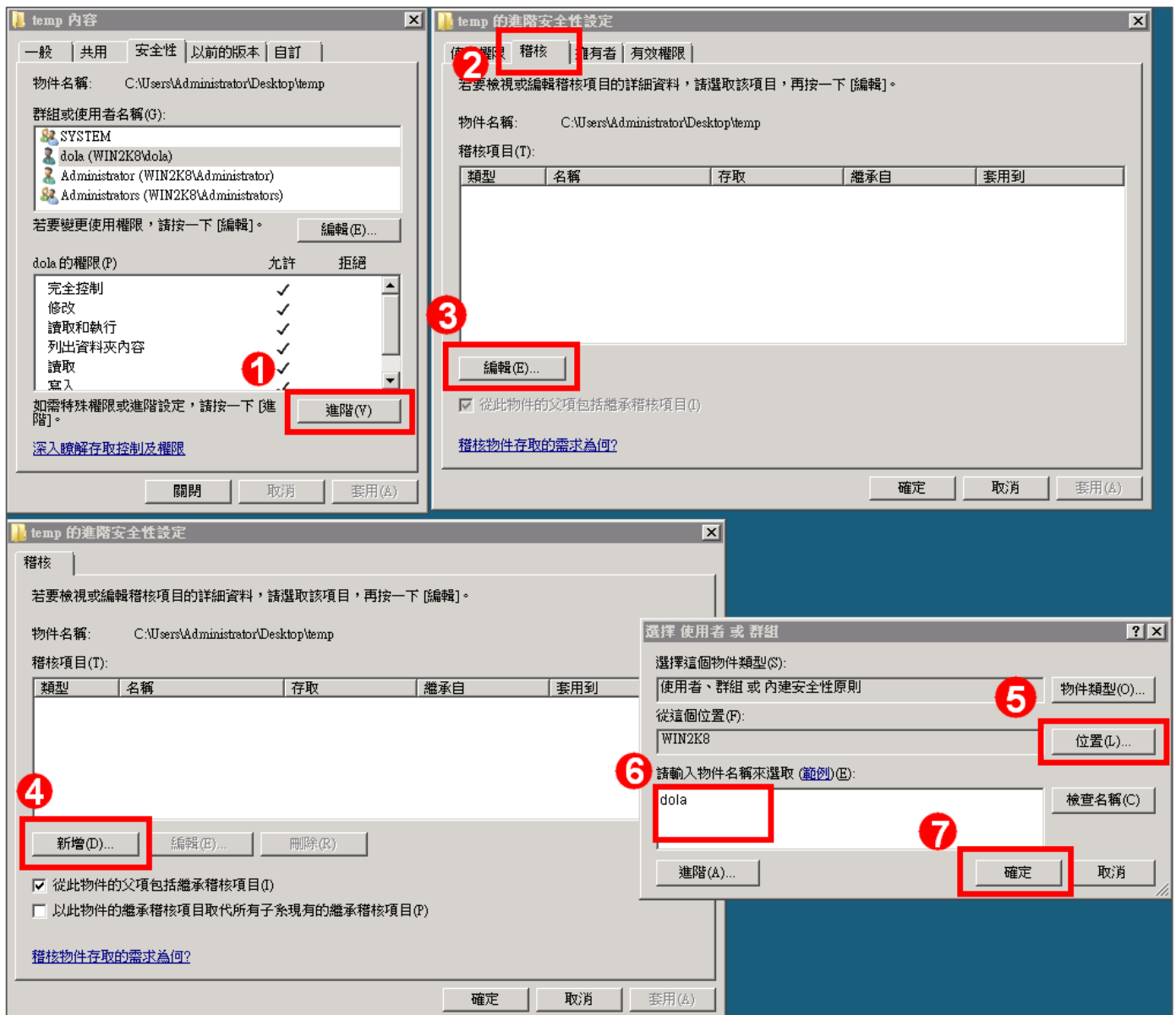
6. 安全性設定：

- (1) 點選 [安全性] 索引標籤。
- (2) 點選 [編輯]。
- (3) 選擇使用者。
- (4) 勾選允許 [完全控制] 權限，以取得所有權限。
- (5) 設定完成後按 [確定]。



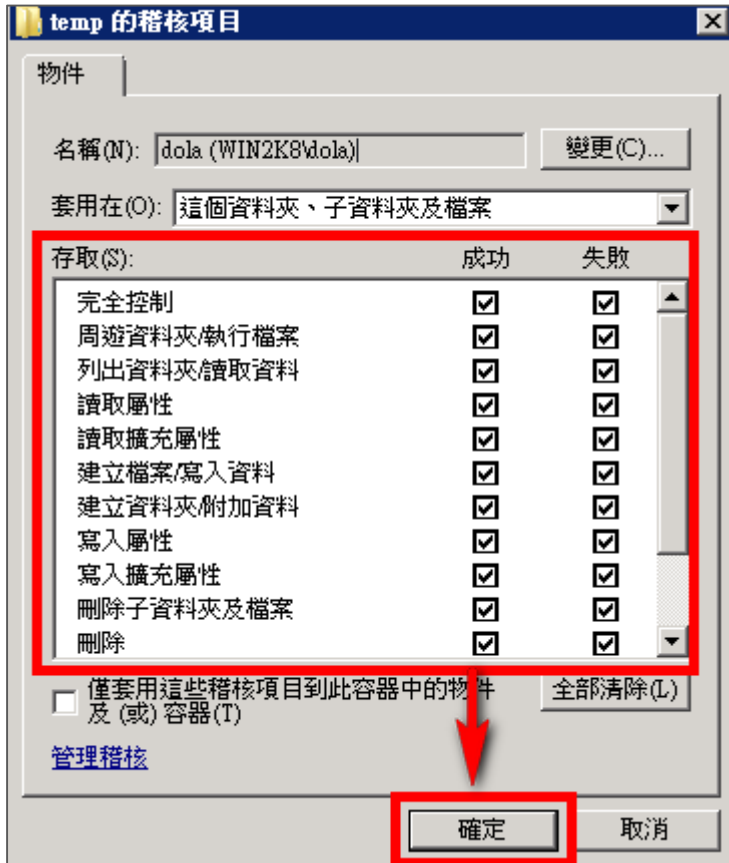
7. 進階安全性設定：

- (1) 點選 [進階]。
- (2) 點選 [稽核] 索引標籤。
- (3) 點選 [編輯]。
- (4) 點選 [新增]。
- (5) 若要選擇其他電腦名稱，可點選 [位置]，選擇其他電腦名稱。
- (6) 可於此空白處直接輸入已知的使用者帳號後，按[檢查名稱]檢查存不存在。
- (7) 設定完成後按 [確定]。

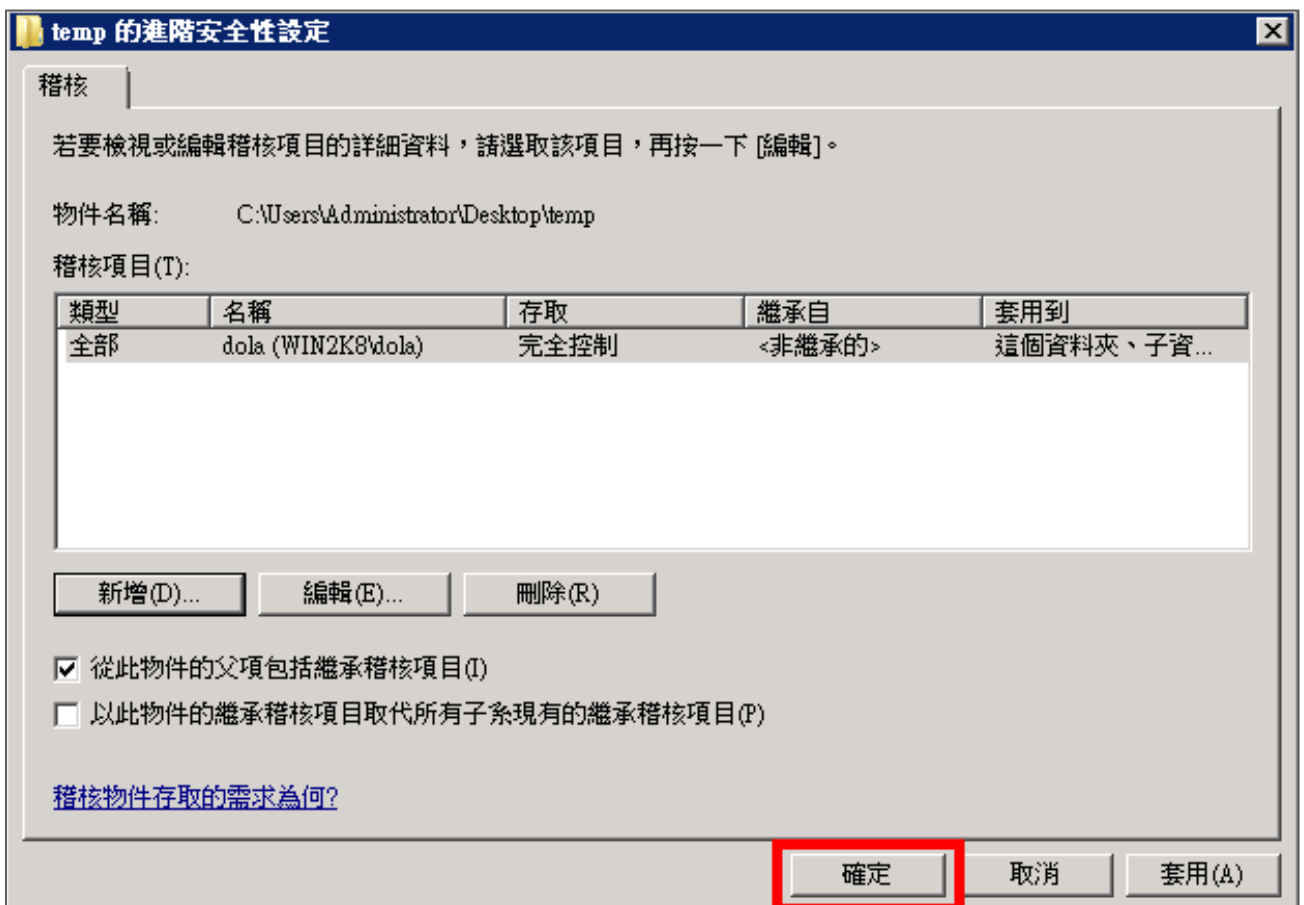


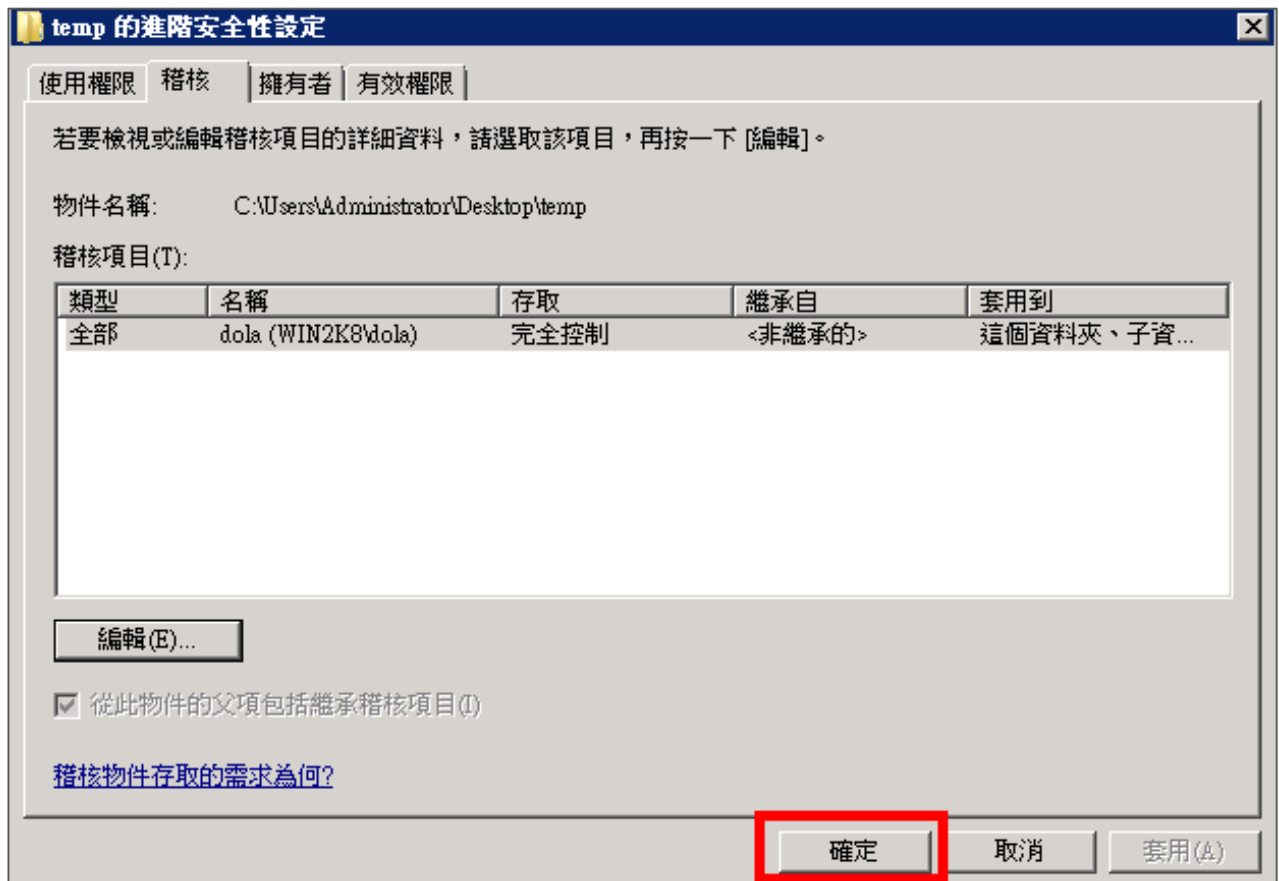
8. 稽核項目設定：

勾選所有稽核項目的 [成功] 及 [失敗]，設定完成後按 [確定]。

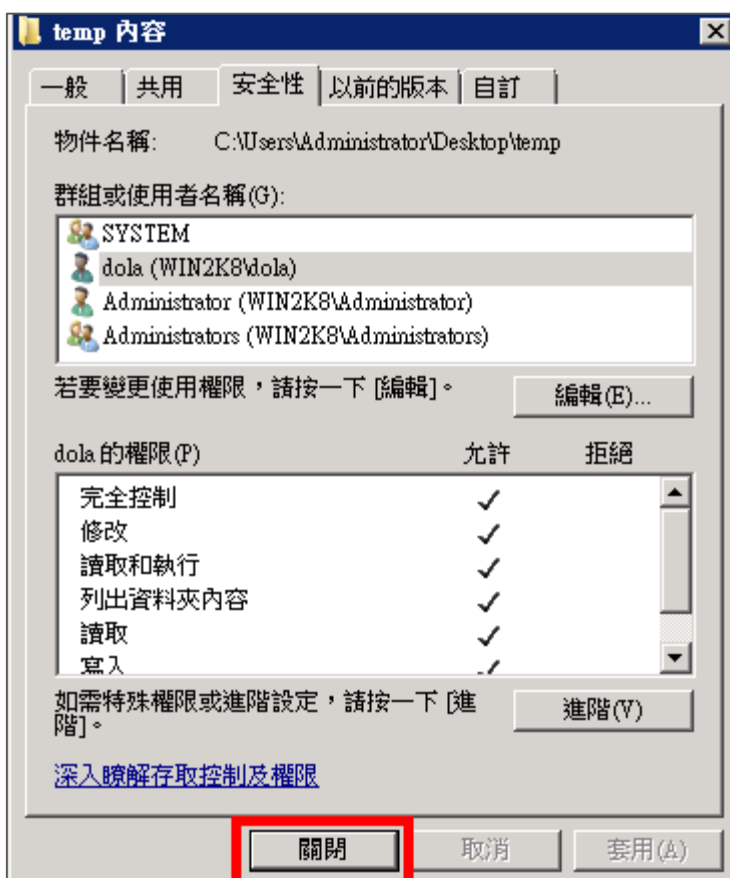


9. 在進階安全性設定完成後，點選 [確定]。

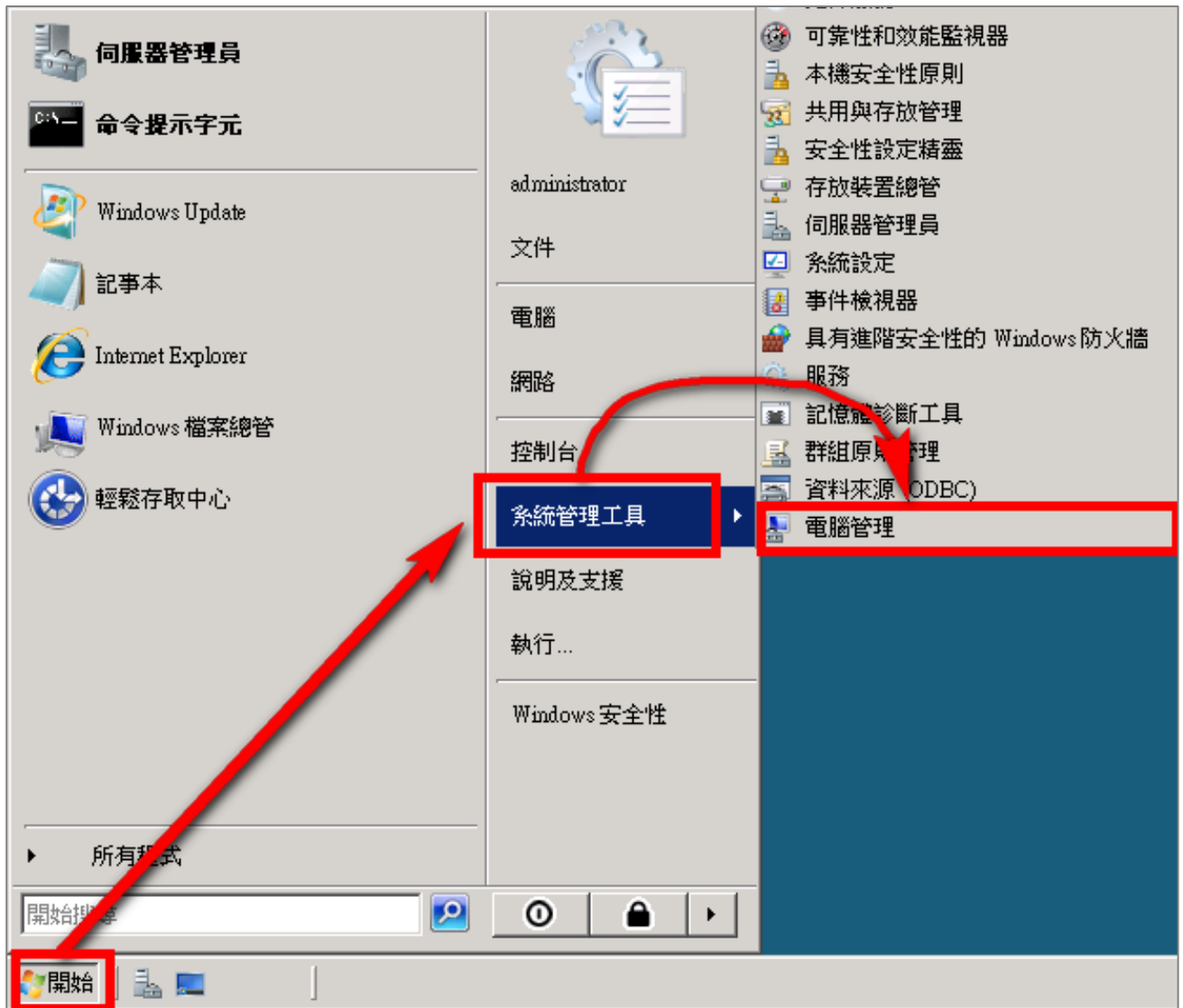




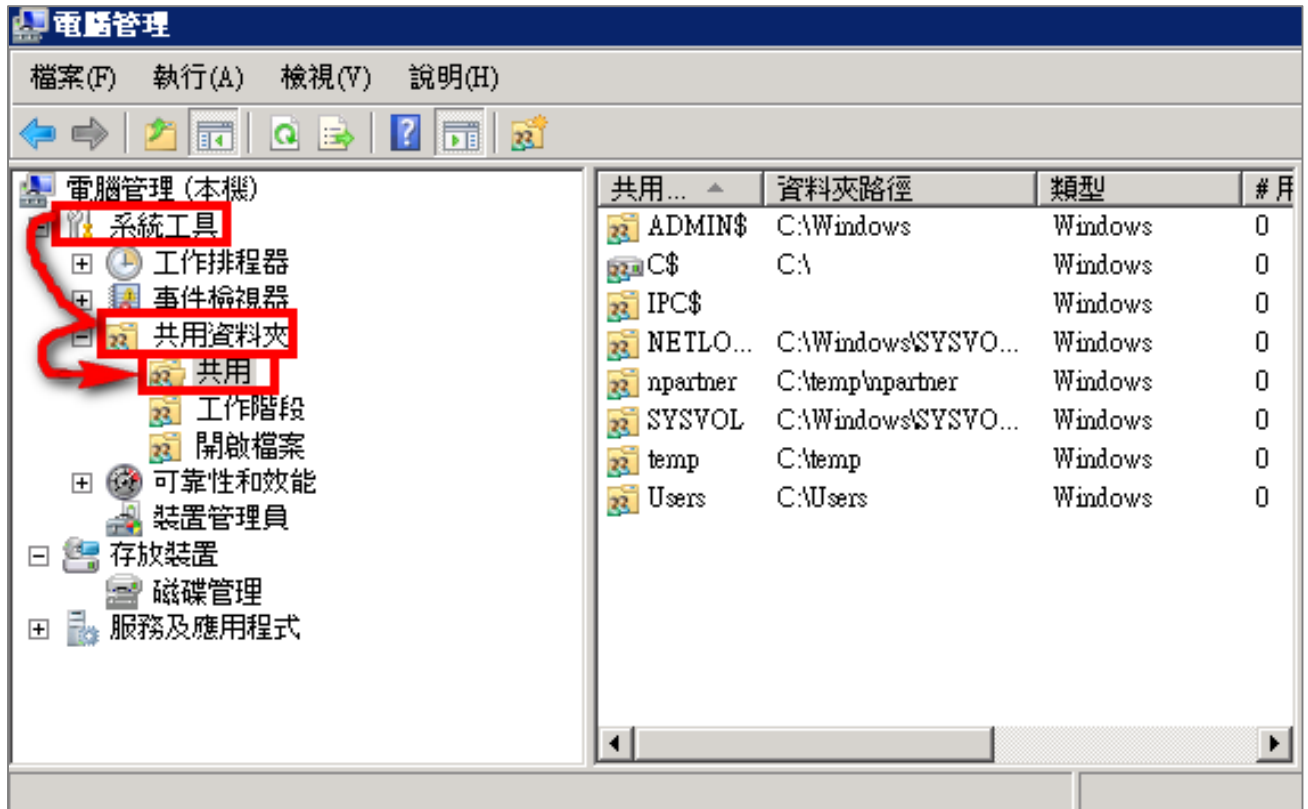
10. 在分享資料夾設定完成後，點選 [關閉]。



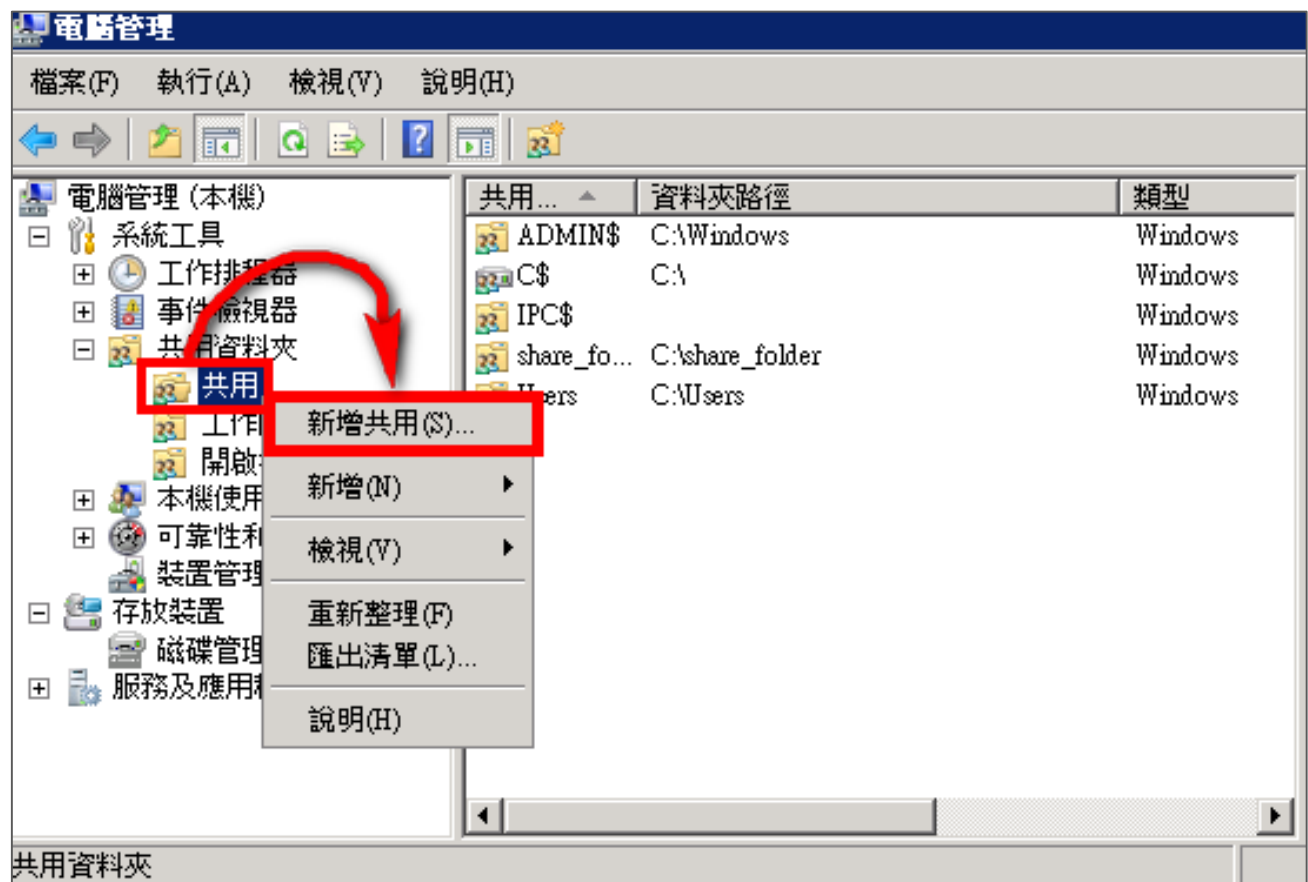
11. 點選 [開始功能表 / 系統管理工具 / 電腦管理]。



12. 點選 [系統工具 / 共用資料夾 / 共用]。



13. 在 [共用] 點擊滑鼠右鍵，點選 [新增共用]。

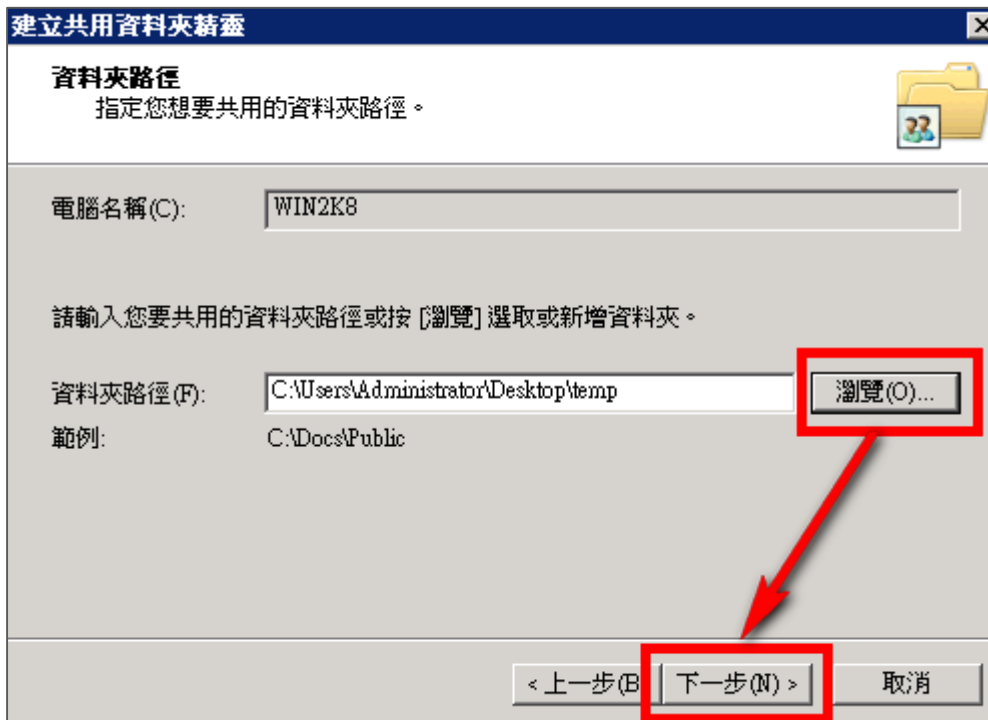


14. 建立共用資料夾精靈：

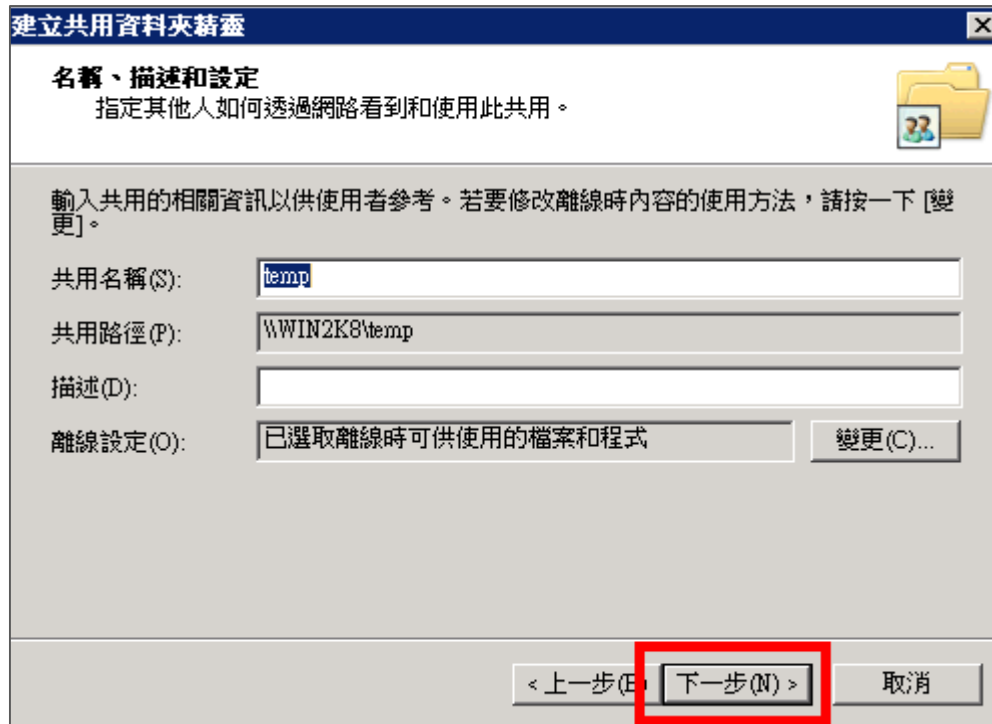
(1) 點選 [下一步]。



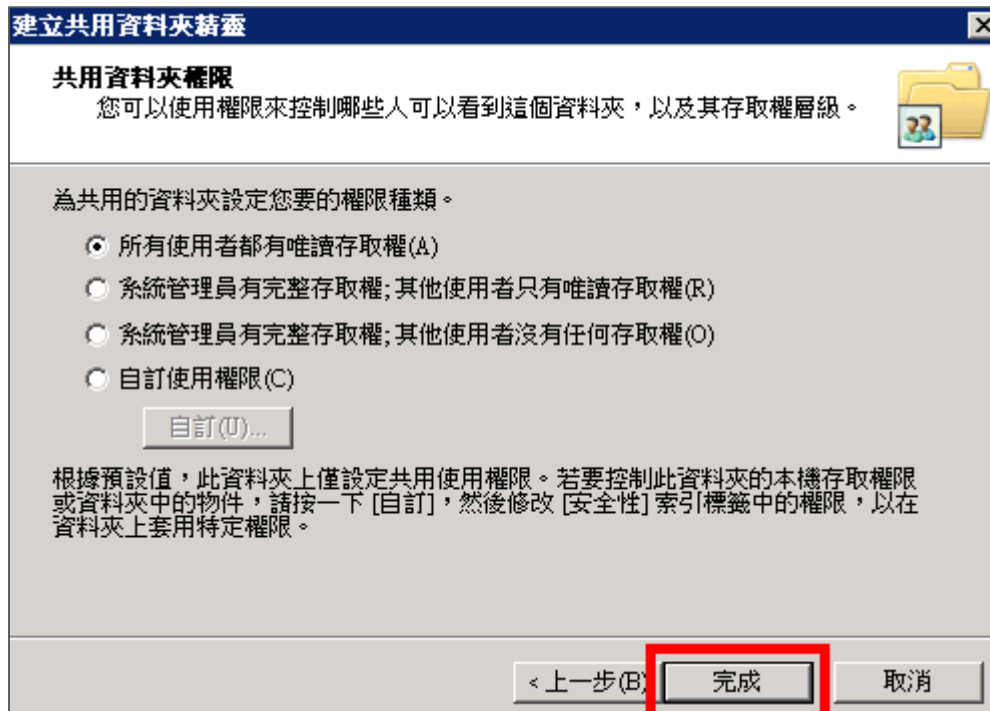
(2) 按 [瀏覽] 指定欲共用資料夾的檔案路徑，完成後按 [下一步]。



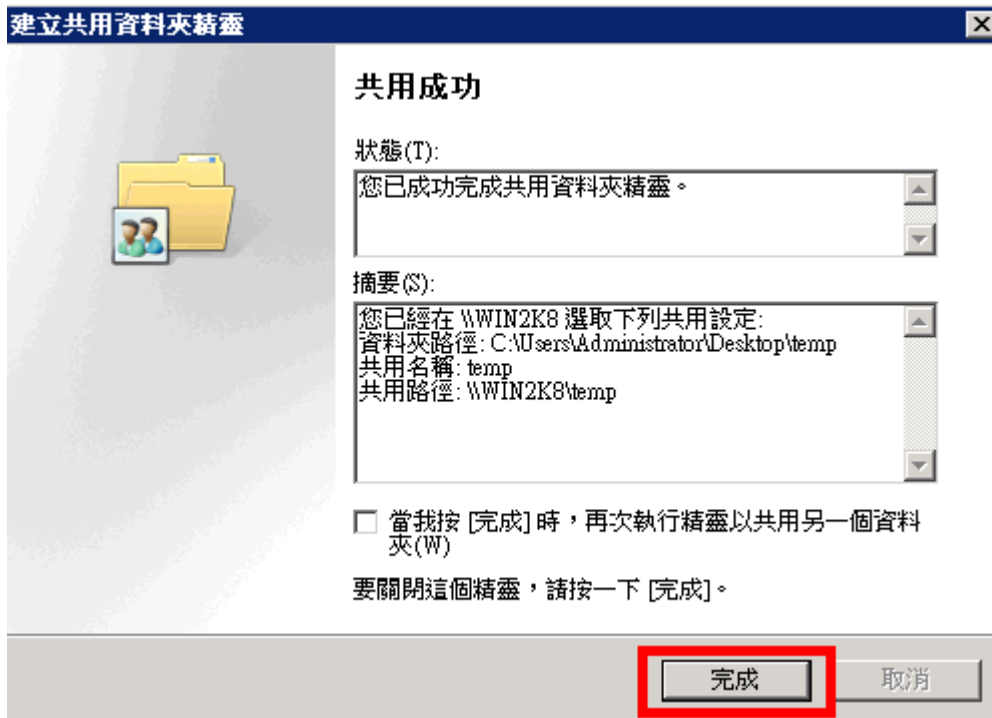
(3) 點選 [下一步]。



(4) 點選 [完成]。

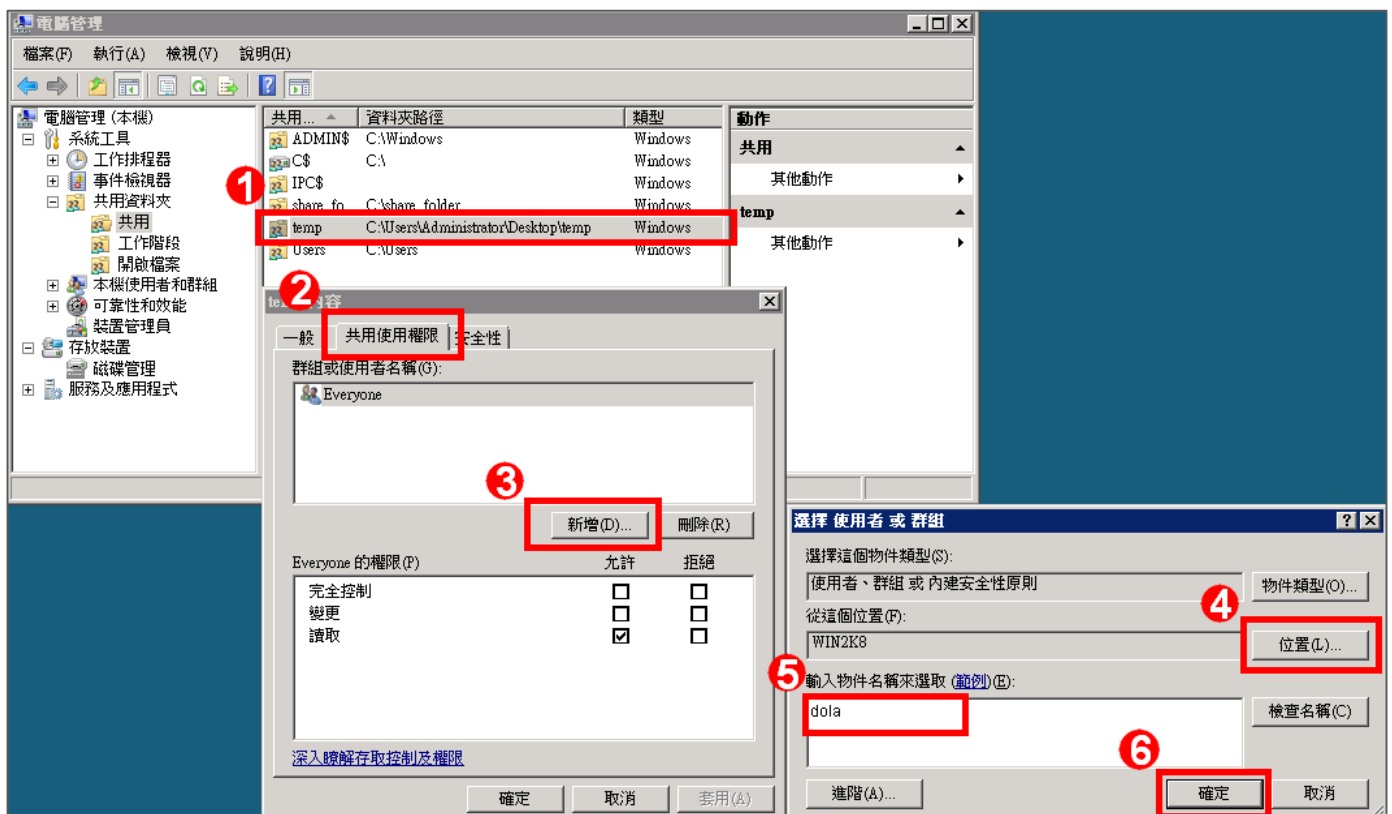


(5) 點選 [完成]。



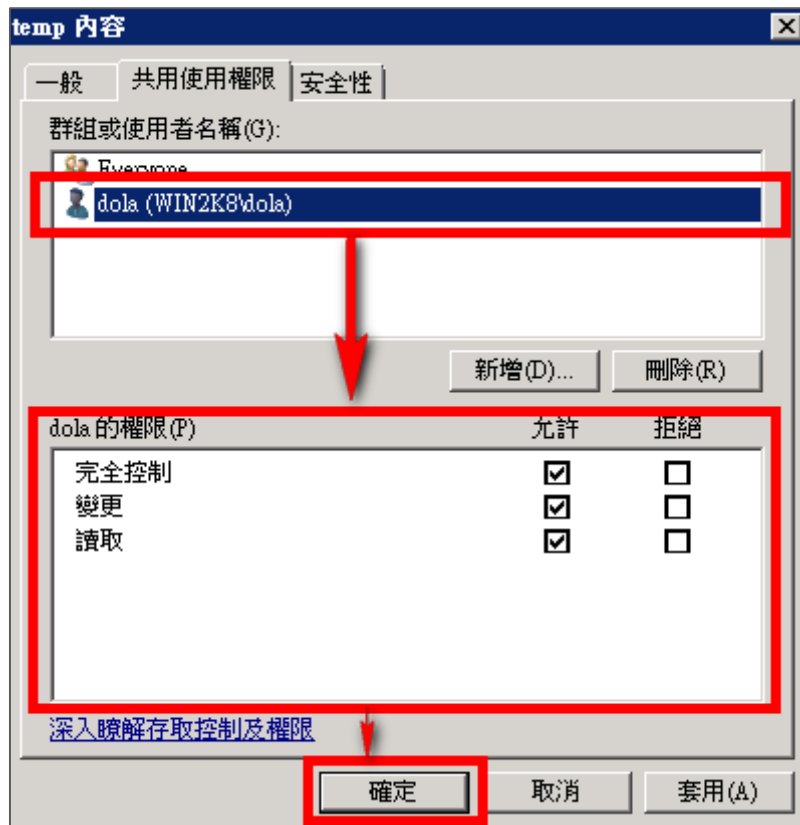
15. 設定共用資料夾使用者：

- (1) 滑鼠雙擊分享的資料夾。
- (2) 點選 [共用使用權限] 索引標籤。
- (3) 點選 [新增]。
- (4) 若要選擇其他電腦名稱, 可點選 [位置]，選擇其他電腦名稱。
- (5) 可於此空白處直接輸入已知的使用者帳號後, 按[檢查名稱]檢查存不存在。
- (6) 設定完成後按 [確定]。



16. 設定共用使用權限：

點選使用者帳號，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 Server 稽核設定

本章節主要說明以下操作設定：

1. 設定本機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。

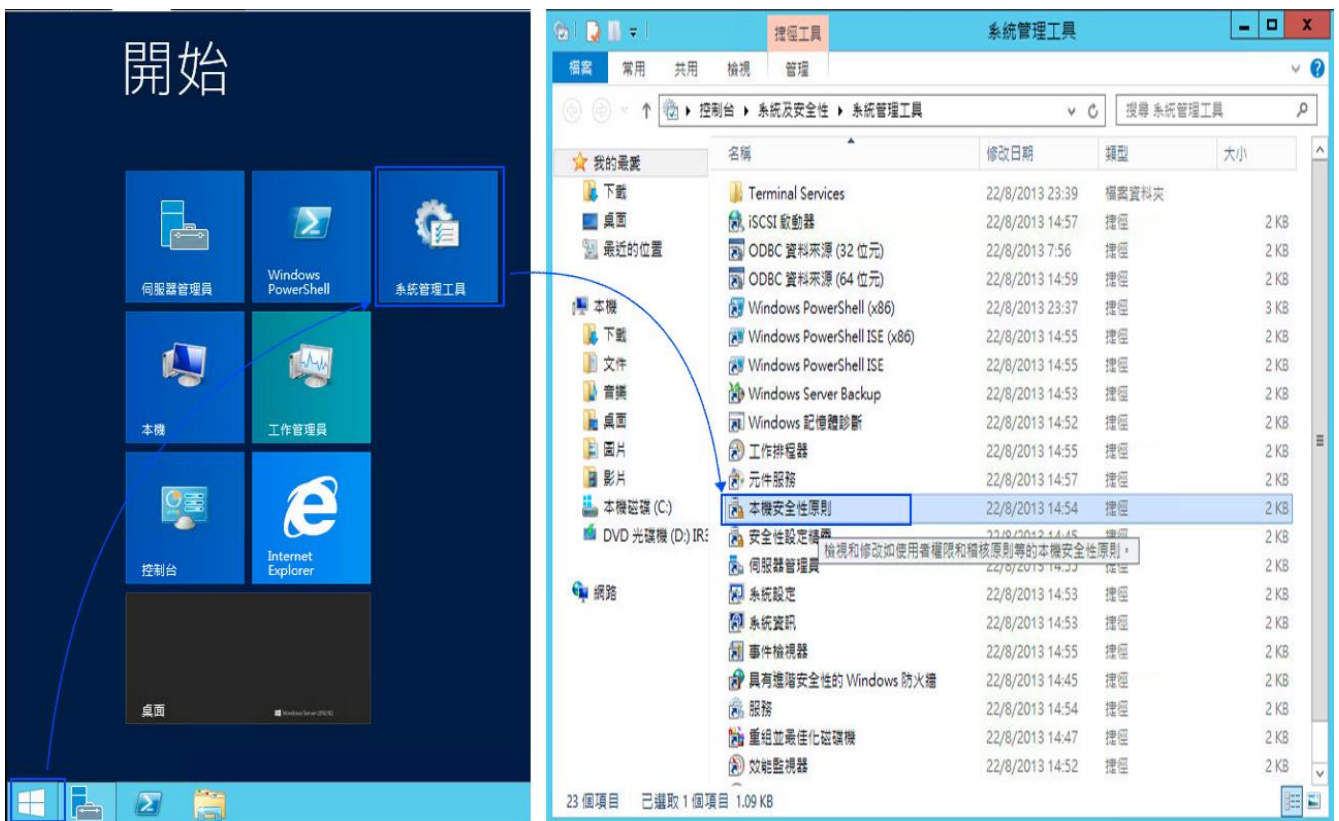
Windows 2012 Server 登入登出的稽核原則和目錄分享的稽核原則，預設是關閉的。

安裝 NXLOG 的步驟，詳細請參閱第一章節。

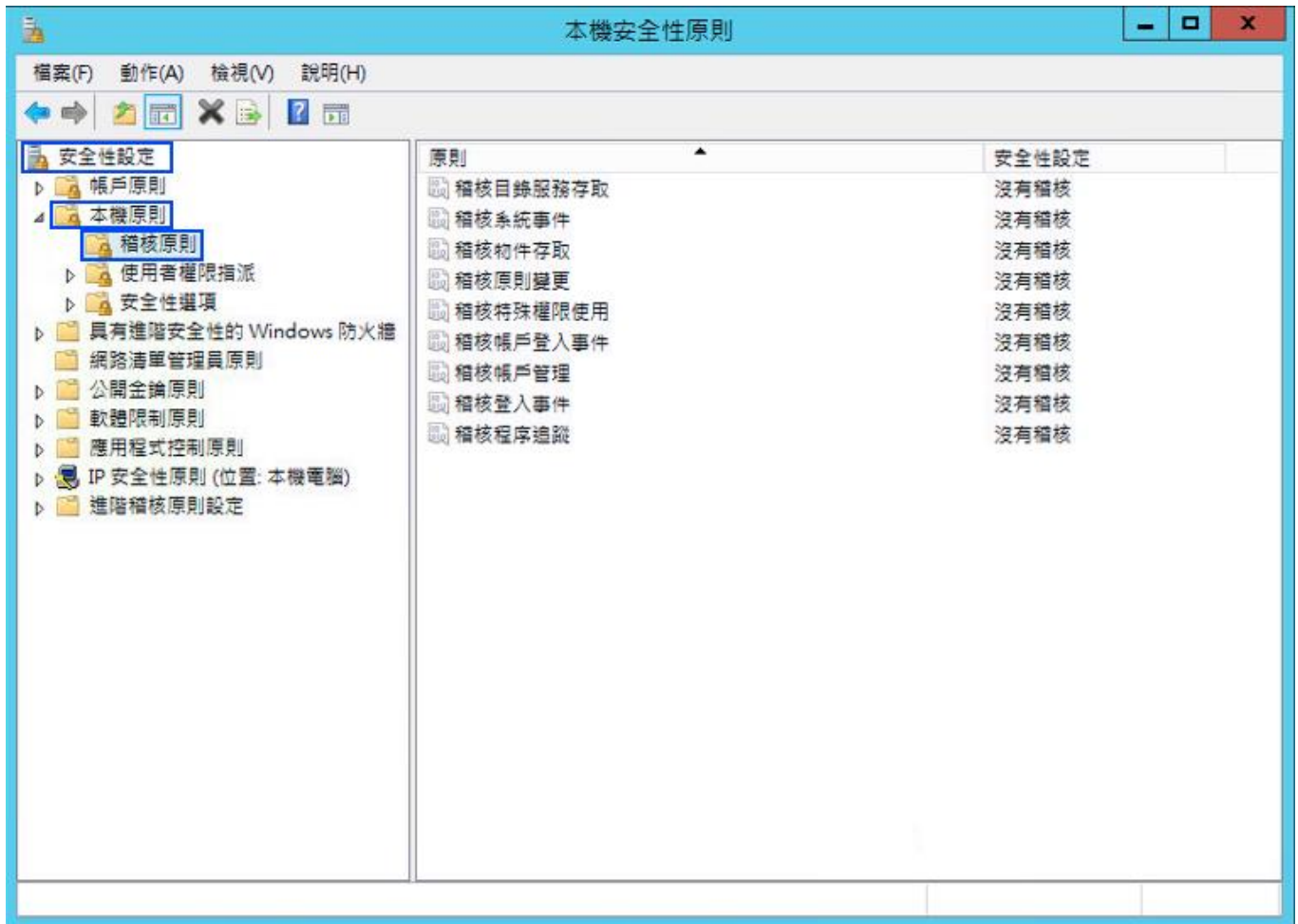
4.1 設定本機登入登出的稽核原則

設定步驟如下：

1. 以系統管理員權限的帳戶 administrator 登入 Windows 2012 Server。點選[開始 / 系統管理工具 / 本機安全性原則]，滑鼠點兩下開啟 [本機安全性原則(Local Security Policy)]。



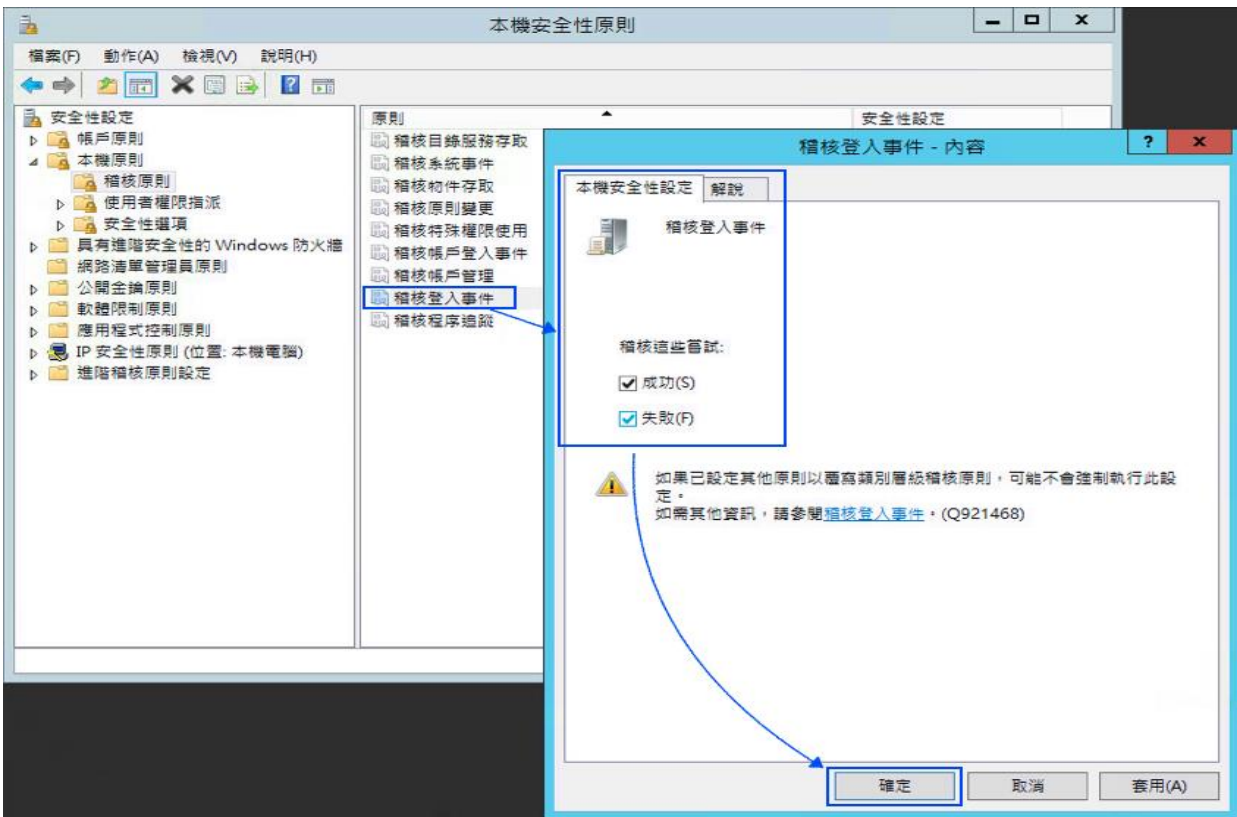
2. 點選 [安全性設定 / 本機原則 / 稽核原則]。



3. 定義下列的原則設定值：

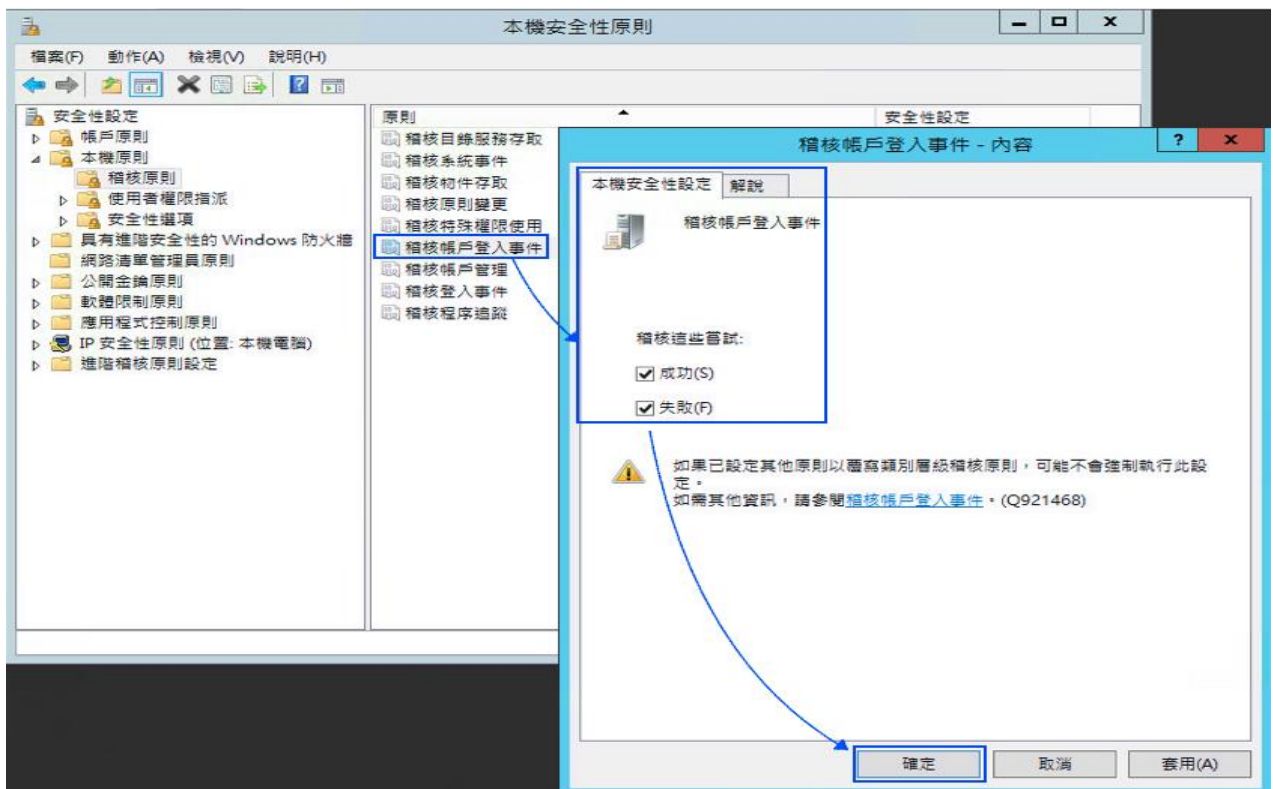
(1) 稽核登入事件(Audit logon events)：

滑鼠雙擊 [稽核登入事件]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(2) 稽核帳戶登入事件(Audit account logon events)：

滑鼠雙擊 [稽核帳戶登入事件]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。



(3) 稽核物件存取(Audit object access) :

滑鼠雙擊 [稽核物件存取]

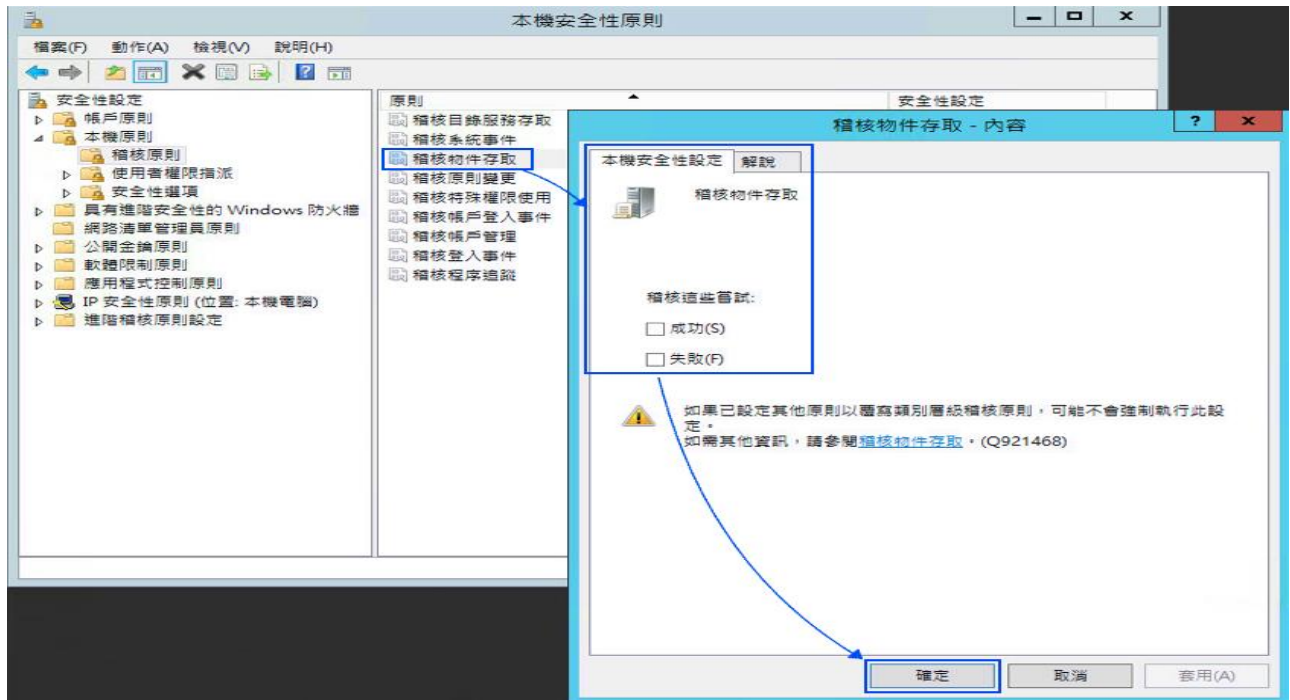
成功：若欲稽核成功事件的 Log，請勾選 [成功] 核取方塊。

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 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，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(Audit policy change) :

滑鼠雙擊 [稽核原則變更]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

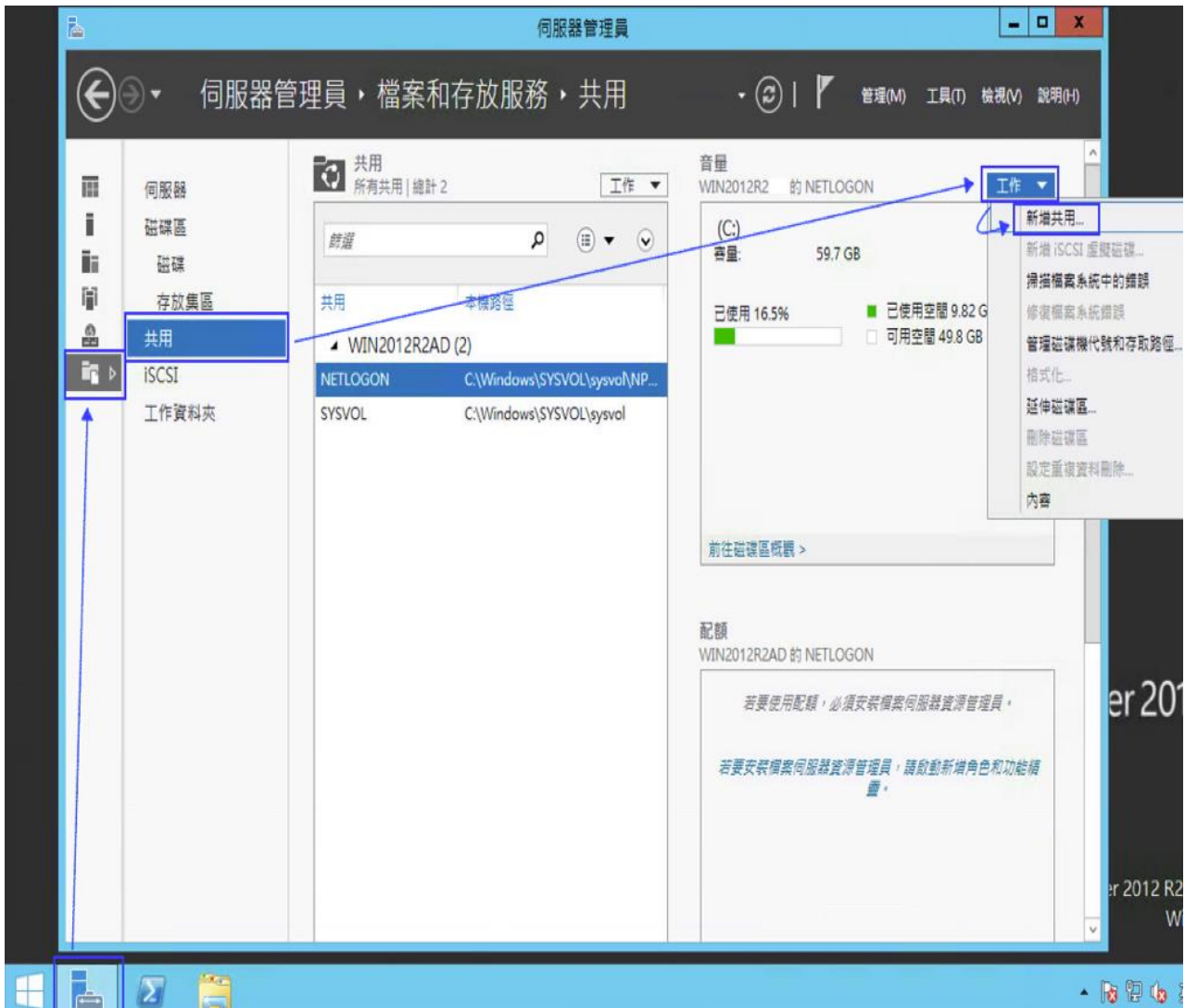
(5) 稽核帳戶管理(Audit account management) :

雙擊 [稽核帳戶管理]，勾選 [成功] 及 [失敗]，設定完成後按 [確定]。

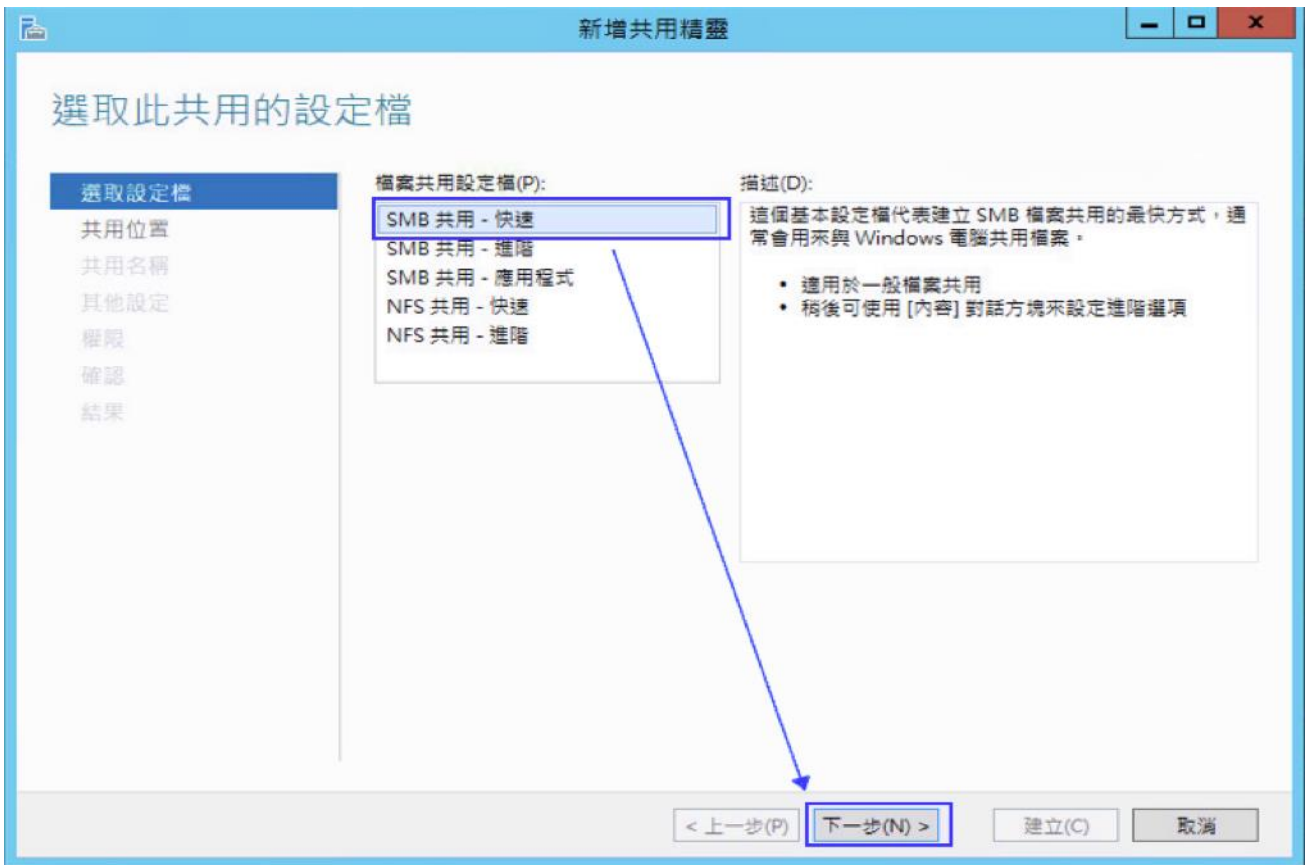
4.2 設定共享資料夾權限與稽核原則

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...]。



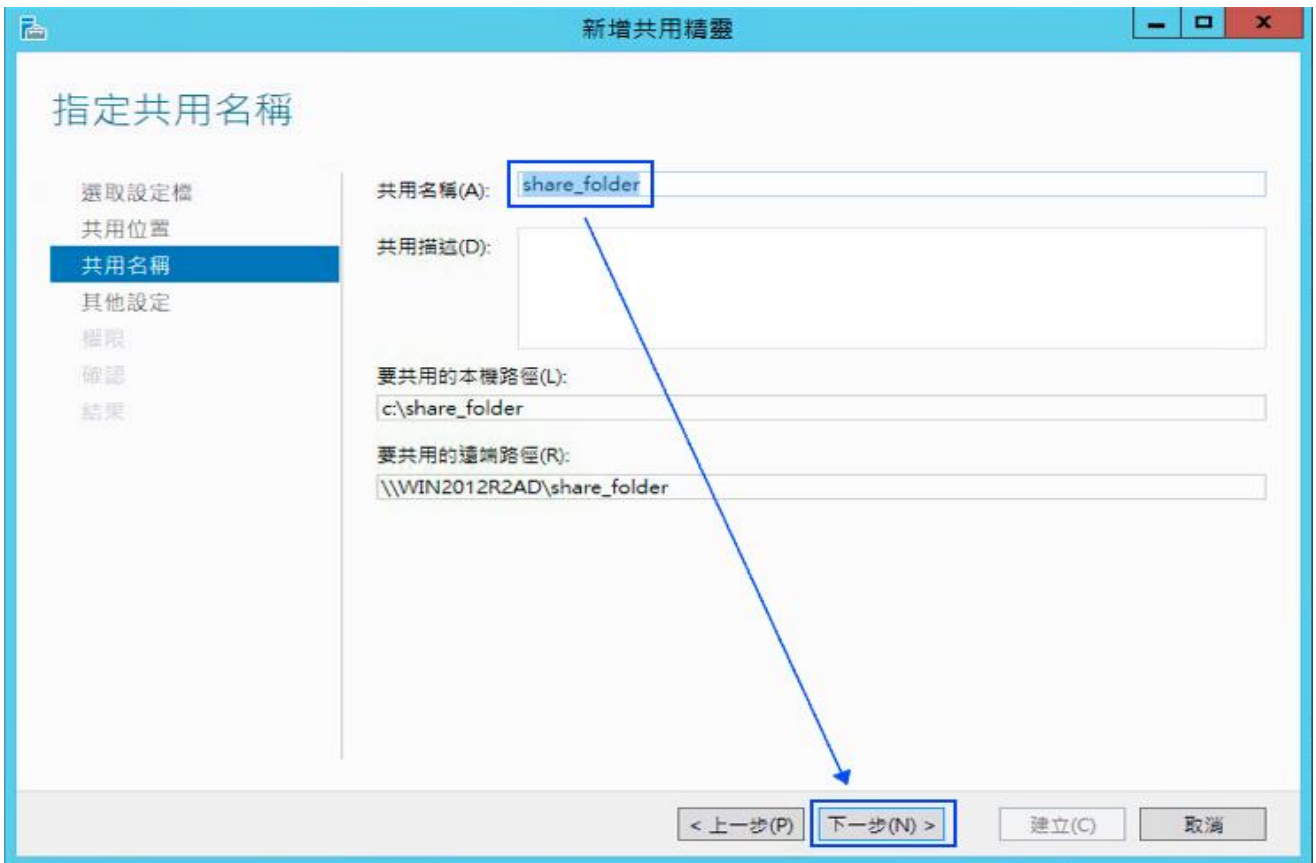
2. 滑鼠左點 [SMB 共用 – 快速] ，點選 [下一步] 。



3. 點選[輸入自訂路徑] ，本例輸入 " C:\share_folder " ，點選[下一步] 。



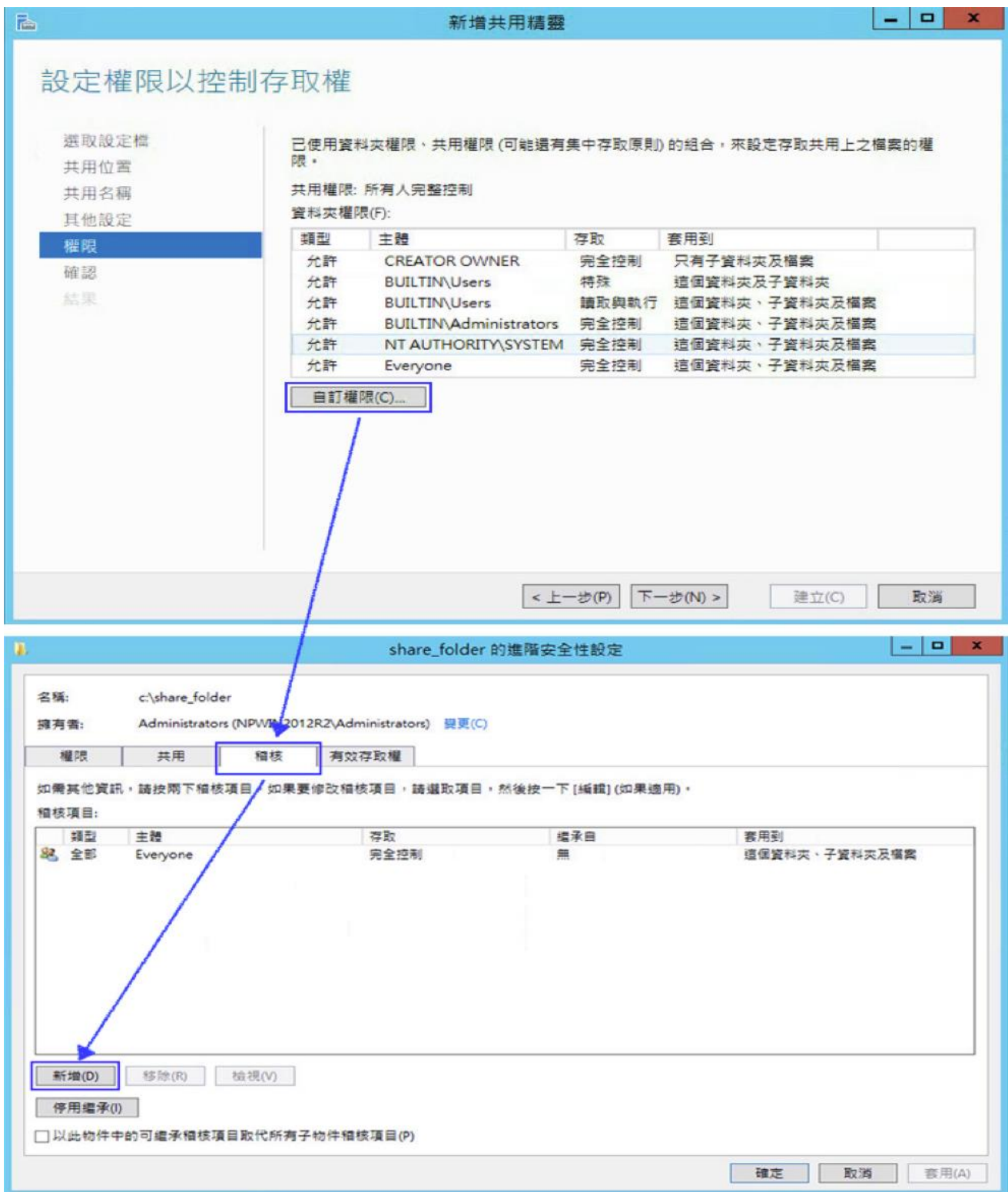
- 在 共用名稱 欄位輸入所要共用的資料夾的名稱，本例為輸入[share_folder]，然後按[下一步]。



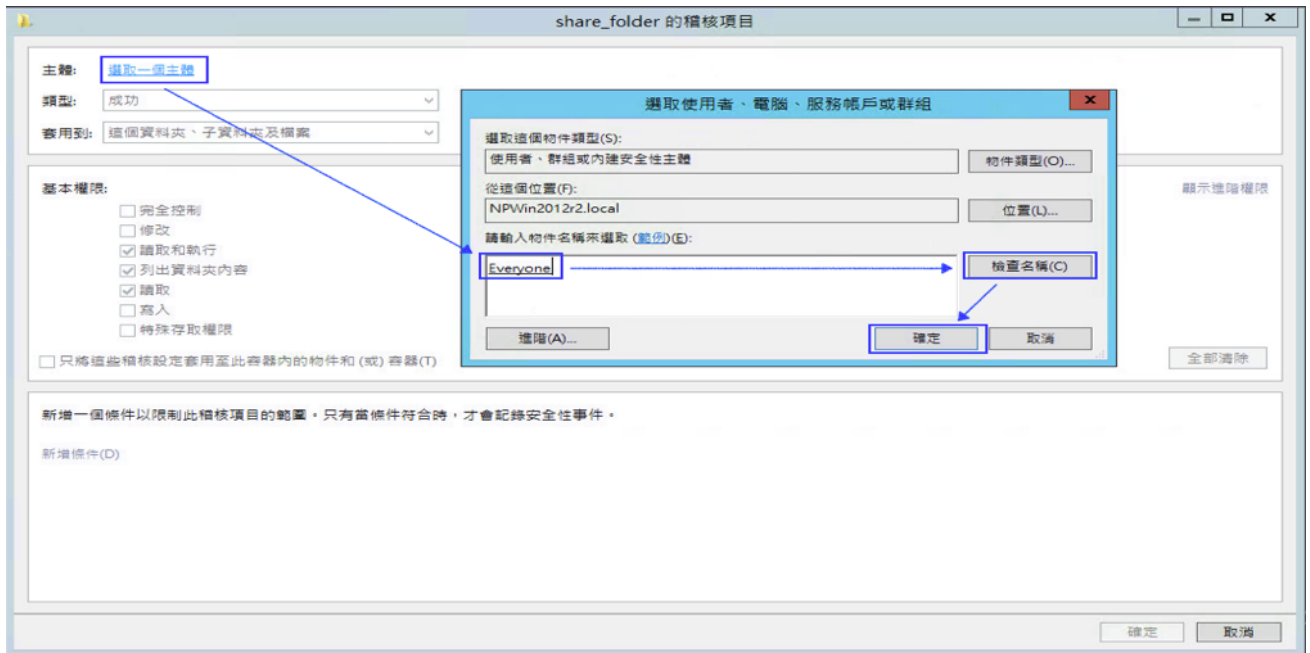
- 勾選 [啟用存取型列舉]，點選[下一步]。



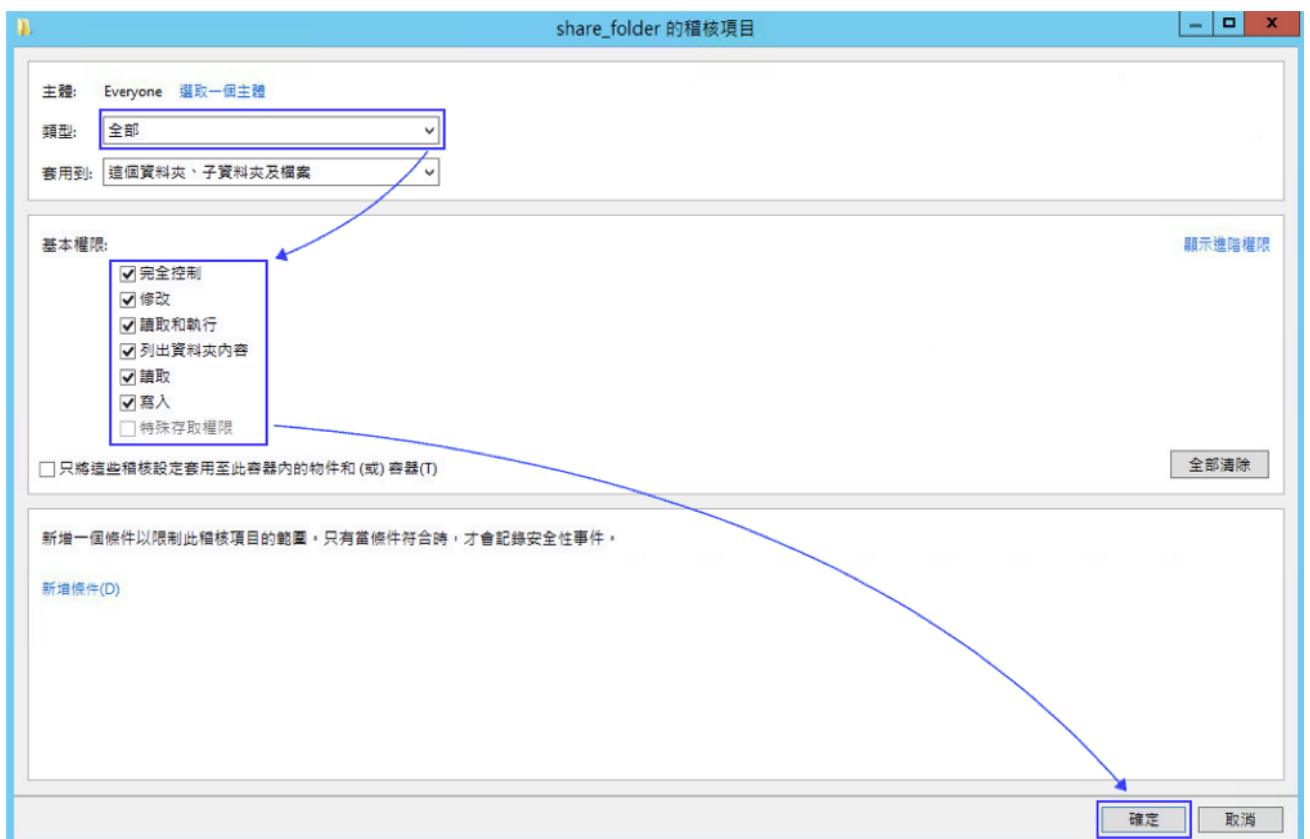
6. 點選 [自訂權限... / 稽核 / 新增]。



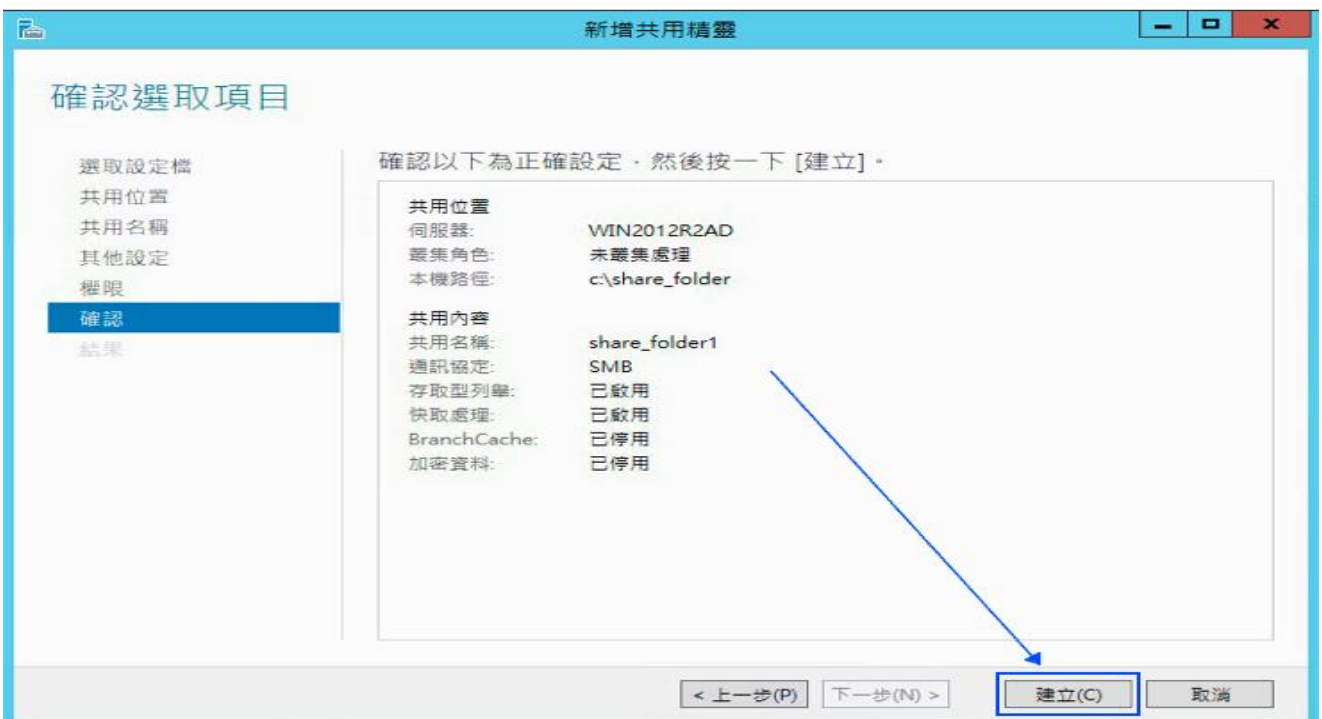
7. 左點 [選取一個主體]，如果欲稽核所有使用者，在物件名稱欄位的空白處輸入 " everyone " 後，點選檢查名稱，按 [確定]。



8. 類型 下拉選 [全部]，基本權限勾選 [完全控制]，然後按點 [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 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 / Syslog 設備]



- (3) 滑鼠點選 [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]下拉選單中依設備的類型選擇{Windows}，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](https://www.skype.com/join/support@npartnertech.com)

有關業務相關問題請洽：

Email: sales@npartnertech.com

