



N-Partner

N-REPORTER

How to manage and set up
Windows Server Log with
NXLOG

V 1.1.3

Preface

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

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

Contents

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

1 Set up NxLog on Windows Server

1.1 Set up Windows Server 2003

1. Download NXLOG :

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

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

2. Install NXLOG :

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

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

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

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

Note :

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

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

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

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

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

nxlog_win2k3_all.conf :

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

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

```
## 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>
```

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

The environment of this example is a 64 bit system. Please choose " **define ROOT C:\Program Files (x86)\nxlog** " .

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

Setting as follows :

```

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
24       $EventID == 540 or $EventID == 551 or $EventID == 560 or $EventID == 612 or $EventID == 624 or $EventID == 626 or
25       $EventID == 627 or $EventID == 628 or $EventID == 629 or $EventID == 630 or $EventID == 631 or $EventID == 632 or
26       $EventID == 633 or $EventID == 634 or $EventID == 635 or $EventID == 636 or $EventID == 637 or $EventID == 638 or
27       $EventID == 641 or $EventID == 642 or $EventID == 645 or $EventID == 646 or $EventID == 647) { $SyslogFacilityValue
28         = 13; } \
29     else if ($SourceName == "Service Control Manager") { $SyslogFacilityValue = 13; } \
30     else if ($SourceName == /^MSSQL*/) { $SyslogFacilityValue = 18; } \
31     else \
32     { \
33       drop(); \
34     } \
35 </Input>
36
37 <Output out_eventlog>
38   Module om_udp
39   Host 192.168.2.64
40   Port 514
41   Exec $Message = string($EventID) + ": " + $Message;
42   Exec if ($EventType == 'ERROR' or $EventType == 'AUDIT_FAILURE') { $SyslogSeverityValue = 3; } \
43     else if ($EventType == 'WARNING') { $SyslogSeverityValue = 4; } \
44     else if ($EventType == 'INFO' or $EventType == 'AUDIT_SUCCESS') { $SyslogSeverityValue = 5; }
45   Exec to_syslog_bsd();
46 </Output>
47
48 <Route eventlog>
49   Path in_eventlog => out_eventlog
50 </Route>

```

5. Start NXLOG :

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

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

Enter command prompt :

```

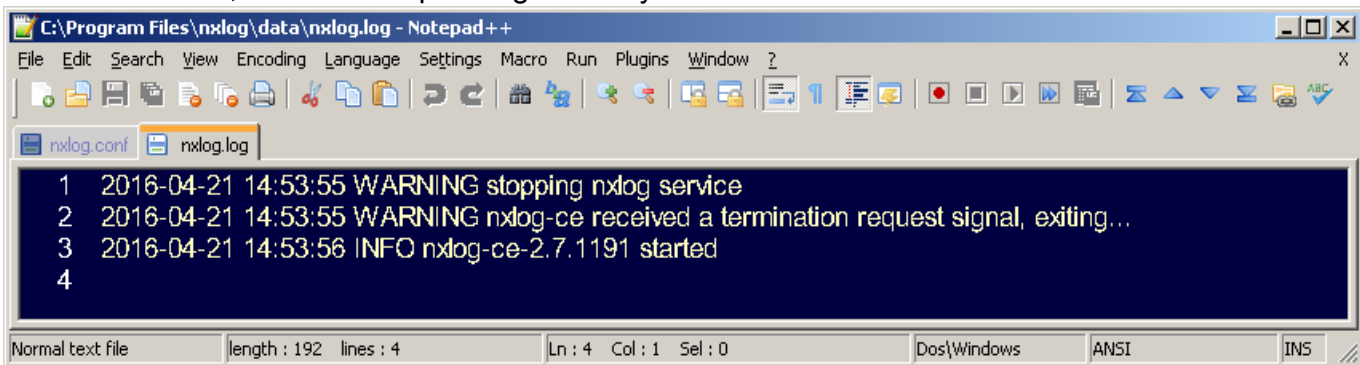
net stop nxlog
net start nxlog

```

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

6. Check whether does NXLOG runs normally :

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



```

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

```

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

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

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

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

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

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

1.2 Set up Windows Server 2008

1. Download NXLOG :

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

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

2. Install NXLOG :

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

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

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

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

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

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

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

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

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

nxlog_win2k8_all.conf :

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

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

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

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

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

Moduledir %ROOT%\modules
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>

```

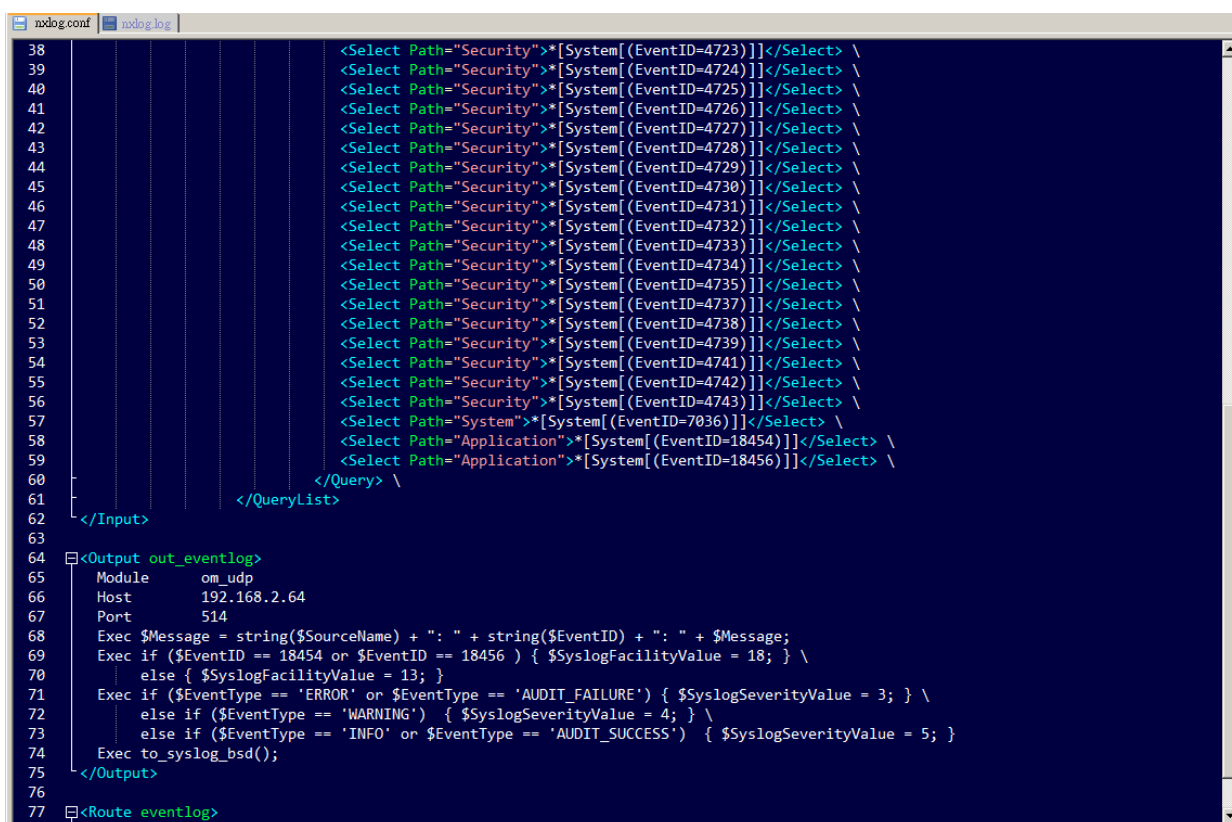
Please choose the correct install path of NXLOG about the green words .

The environment of this example is a 64 bit system. Please choose " **define ROOT C:\Program Files (x86)\nxlog** " .

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

Setting as follows :

5. Start NXLOG :



```

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>

```

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

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

Enter command prompt :

```

net stop nxlog
net start nxlog

```

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

6. Check whether does NXLOG runs normally :

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

```

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

```

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

1.3 Set up Windows Server 2012

1. Download NXLOG :

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

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

2. Install NXLOG :

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

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

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

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

Note :

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

Install NXLOG on 64 bit operating system at " C:\Program Files (x86)\nxlog\conf\nxlog.conf "

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

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

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

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

```
## 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>
```

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

The environment of this example is a 64 bit system. Please choose " **define ROOT C:\Program Files (x86)\nxlog** " .

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

Setting as follows :

```

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

```

3. Start NXLOG :

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

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

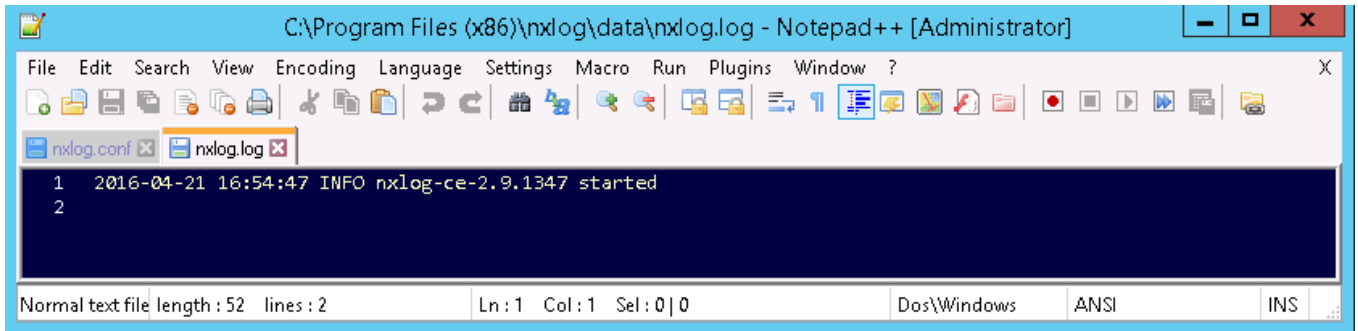
Under [Windows PowerShell] mode, input :

```

net stop nxlog
net start nxlog

```

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



The screenshot shows a Notepad++ window titled "C:\Program Files (x86)\nxlog\data\nxlog.log - Notepad++ [Administrator]". The window contains two tabs: "nxlog.conf" and "nxlog.log". The "nxlog.log" tab is active, displaying the following content:

```
1 2016-04-21 16:54:47 INFO nxlog-ce-2.9.1347 started
2
```

The status bar at the bottom indicates "Normal text file length : 52 lines : 2 Ln : 1 Col : 1 Sel : 0 | 0 Dos\Windows ANSI INS".

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

2 Windows 2003 Server Audit log Settings

This section introduces the local machine policy audit of Windows 2003 Server. The local machine here means it is an independent host, which does not belong to any network domain.

Mainly discuss the following two settings :

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

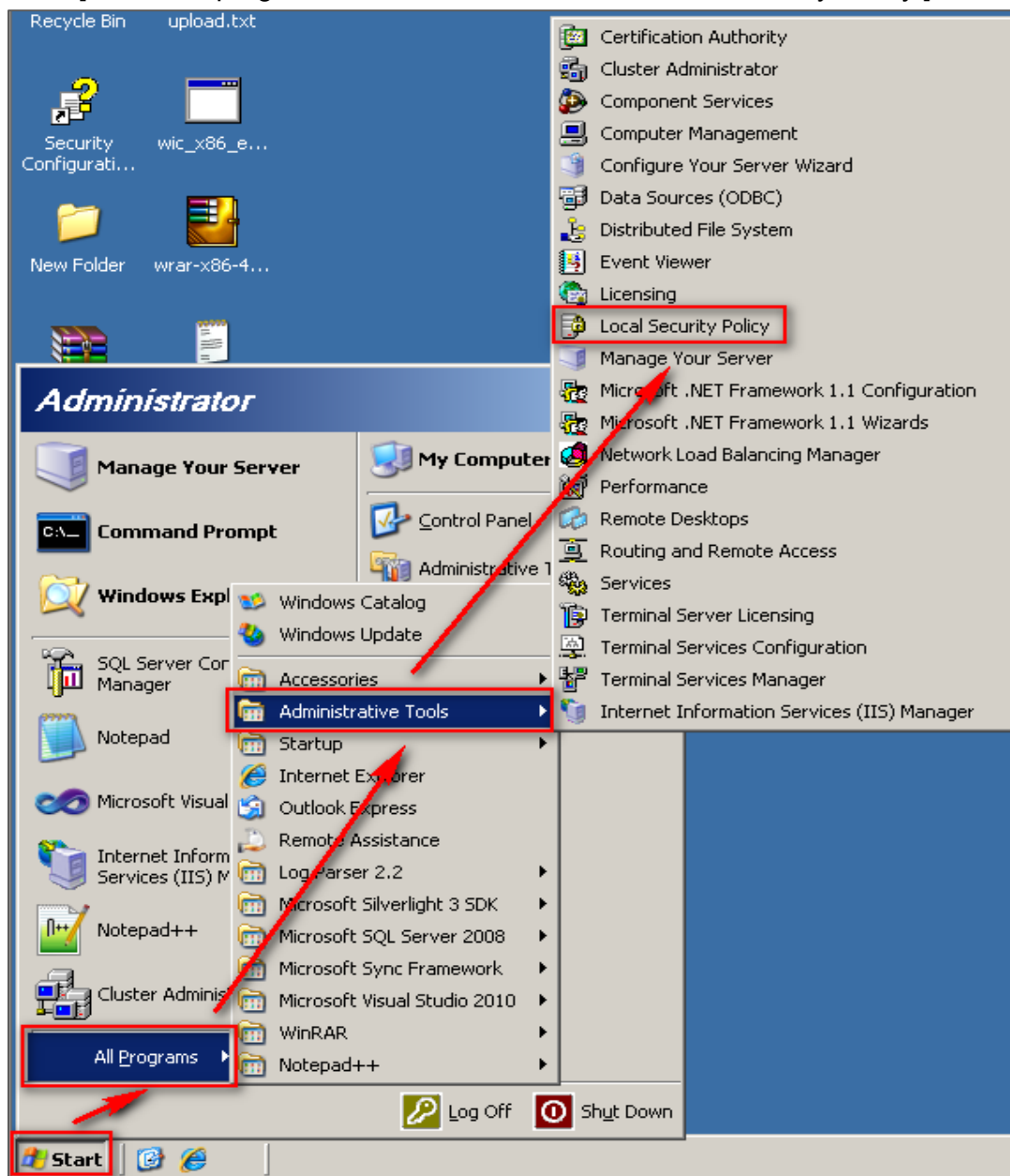
Please remember to download NXLOG, which may refer to section 1.

2.1 Setting up local machine audit policy

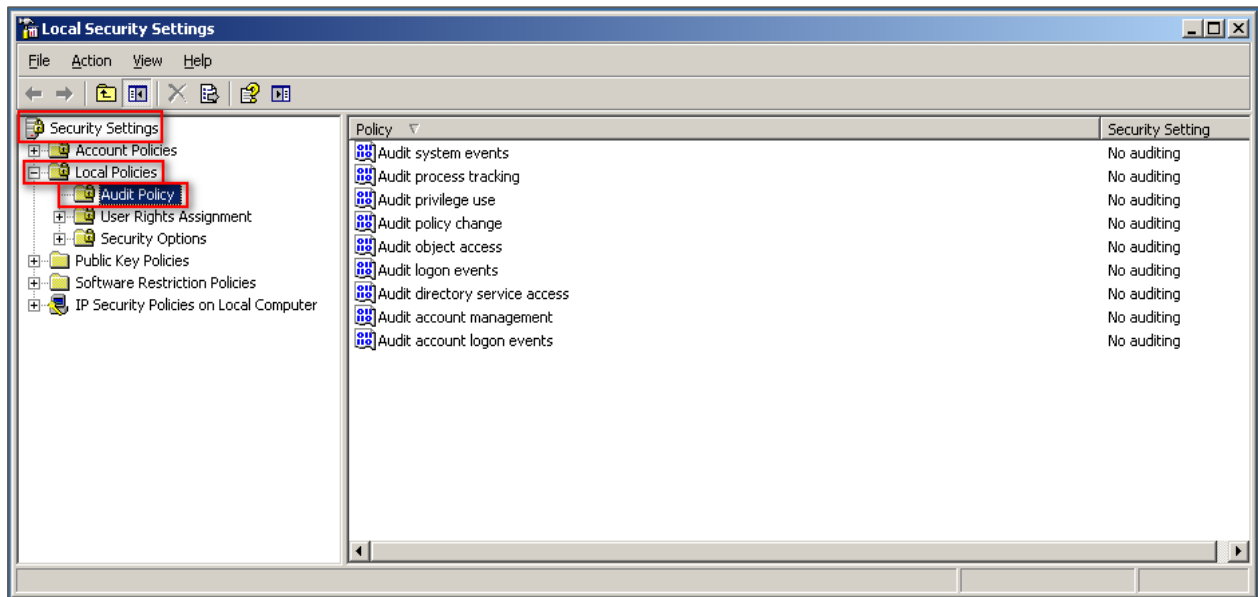
Set as follows :

1. Log in Windows 2003 Server as Administrator.

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



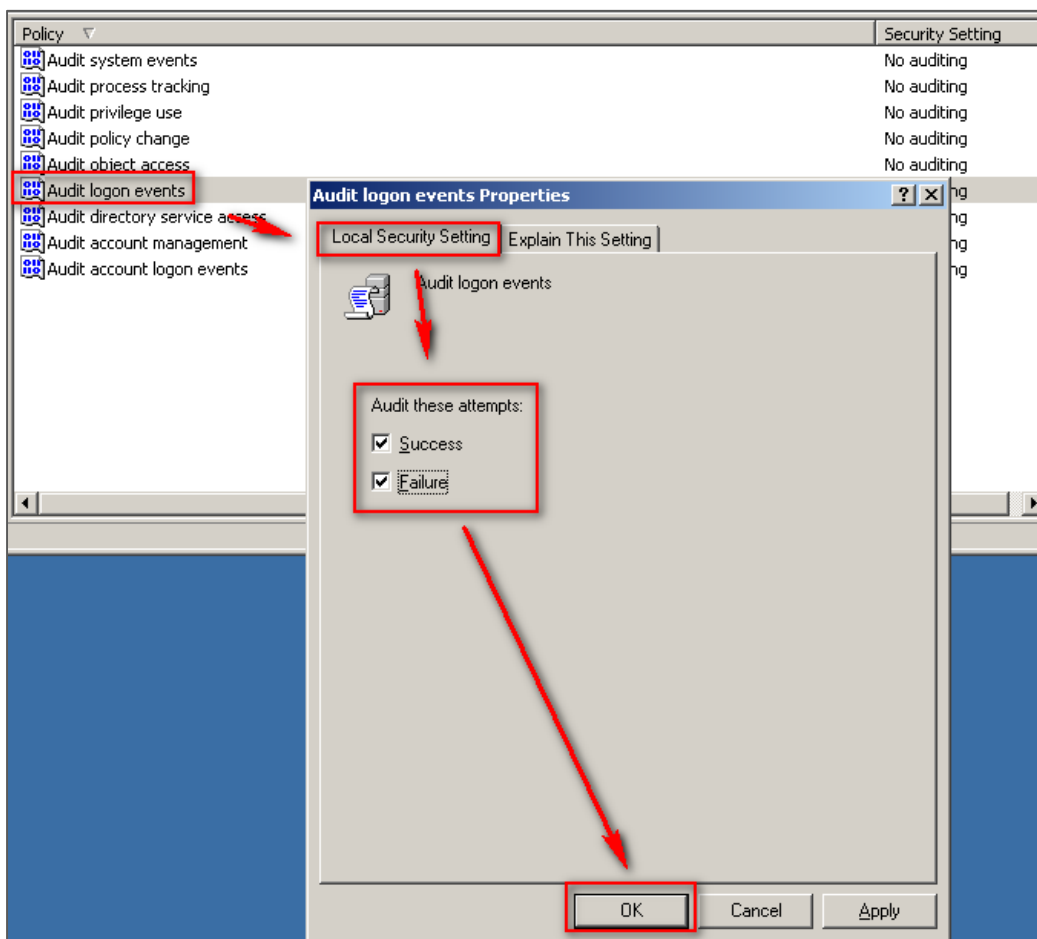
2. Click [Local Policies / Audit Policy]



3. Define the following policy set value :

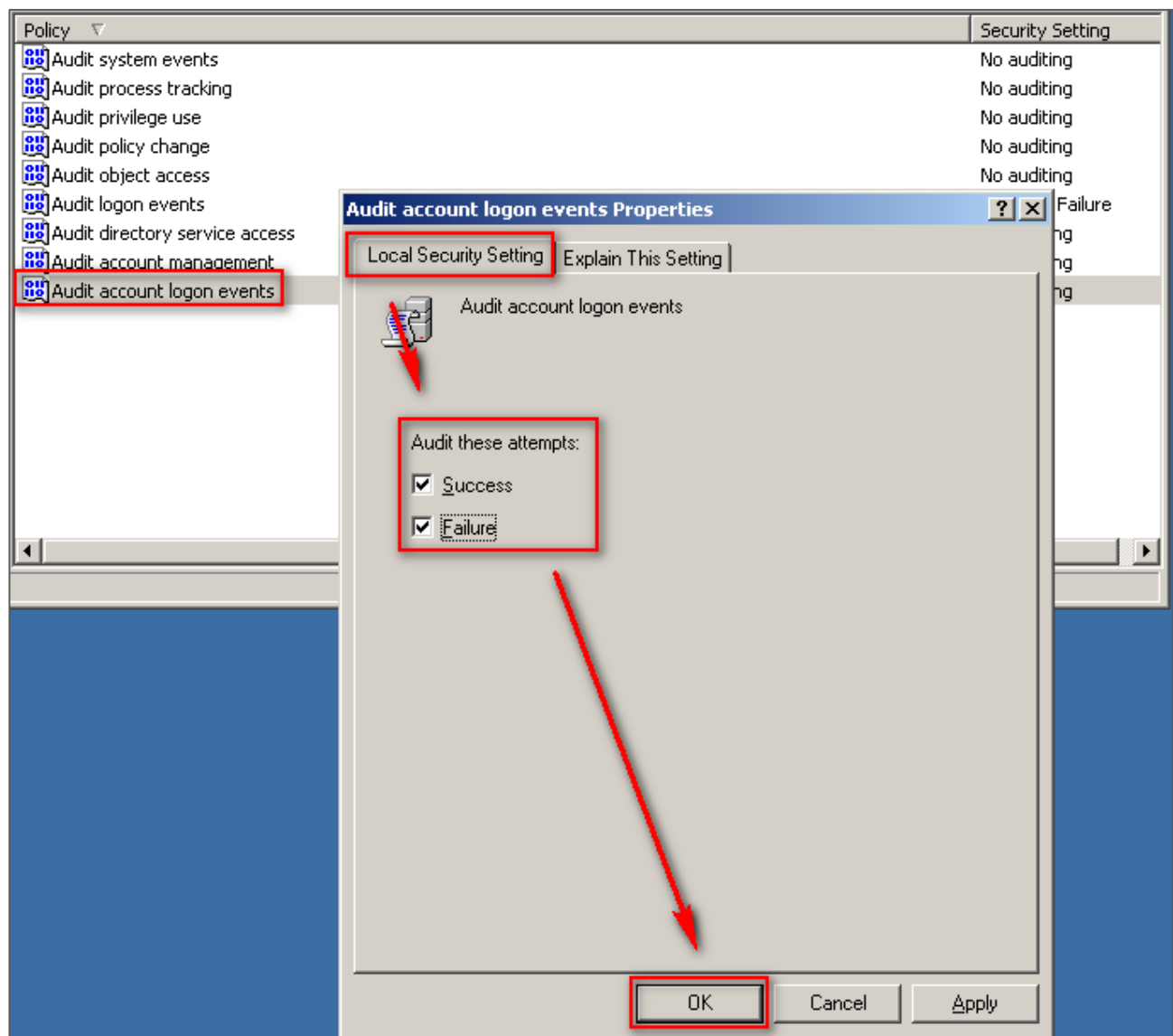
(1) Audit logon event :

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



(2) Audit account logon event :

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

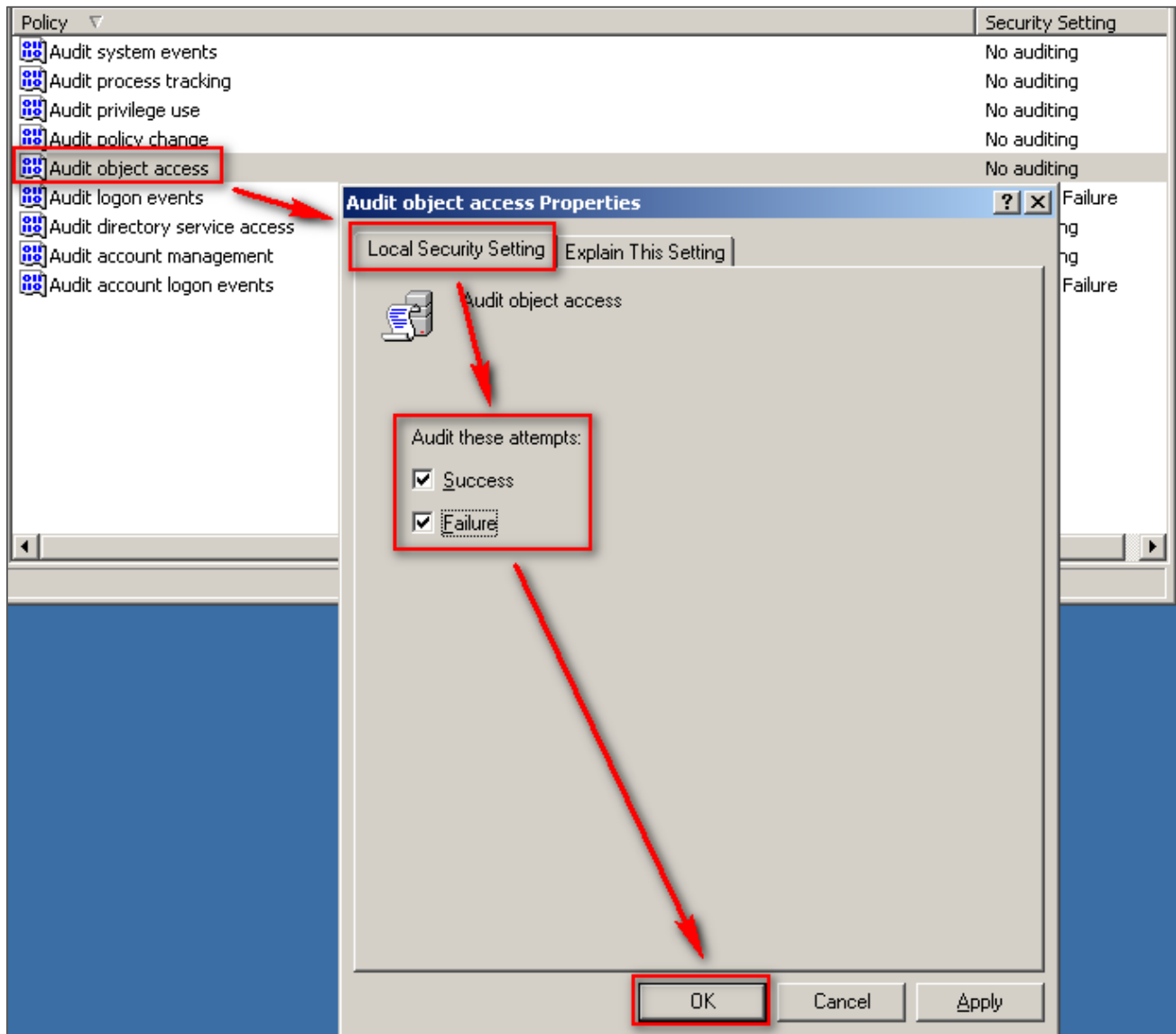


(3) Audit object access :

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

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

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



(4) Changing audit policy :

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

(5) Audit account management :

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

Note : If Windows 2003 Server does not run File server audit, we recommend not to audit object access, please skip steps 2.1(3) and 2.2, and only operate steps 2.1 (1), (2), (4), (5).

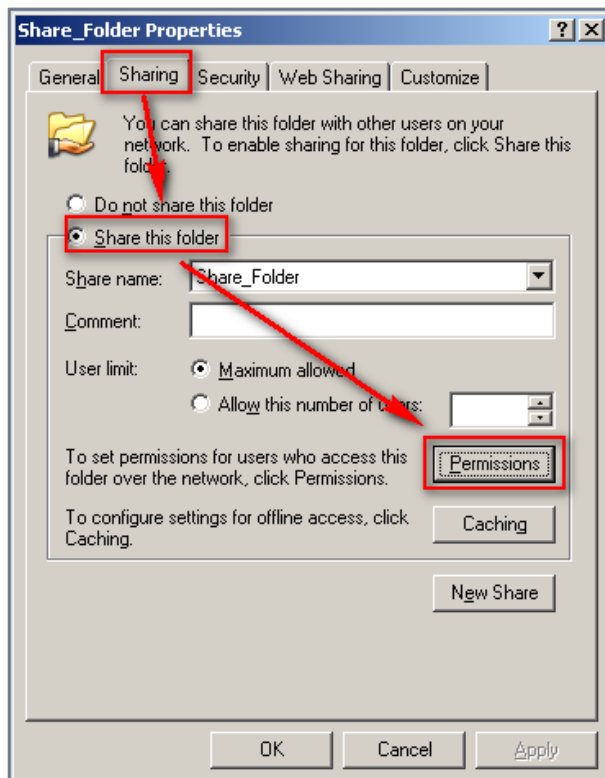
This will help Windows avoid auditing unnecessary Object access security events.

These unnecessary and redundant security events that are converted into syslog and sent to N-Reporter will reduce its performance.

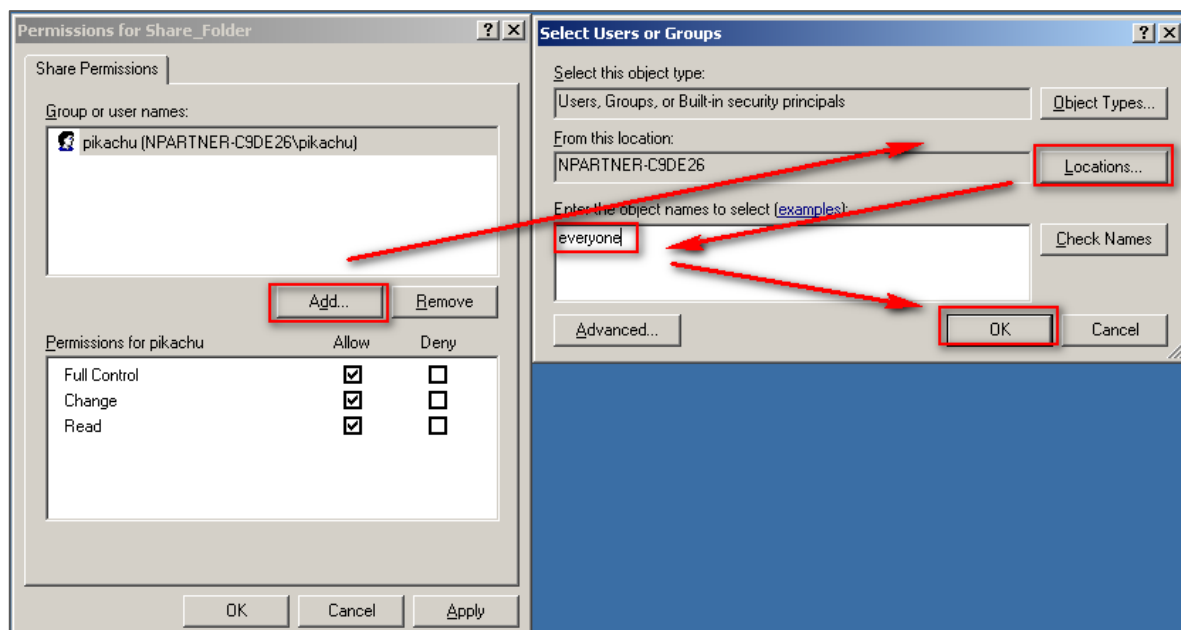
2.2 Setting up local shared folder authorization and audit policy

Set up as follows :

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

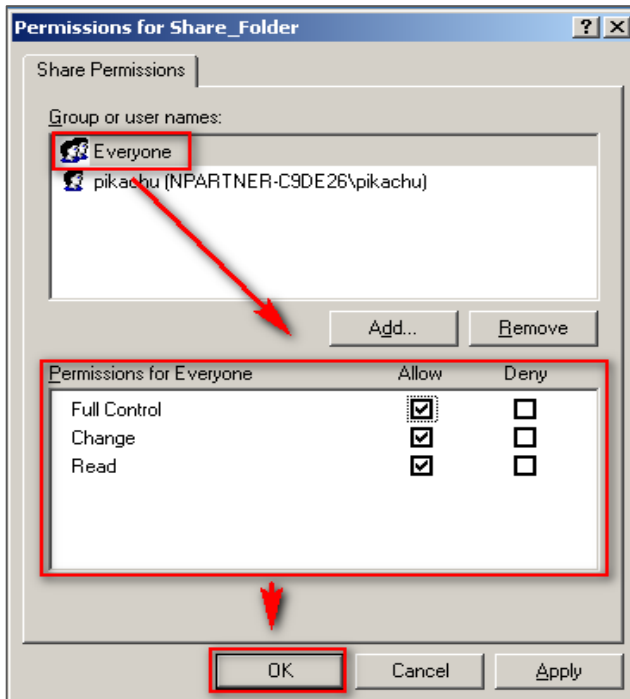


3. Set up user permission :
 - (1) Click [Add], to add a new user.
 - (2) Click [Locations], then choose the local computer name.
 - (3) Enter a user name account.
 - (4) Click [OK].



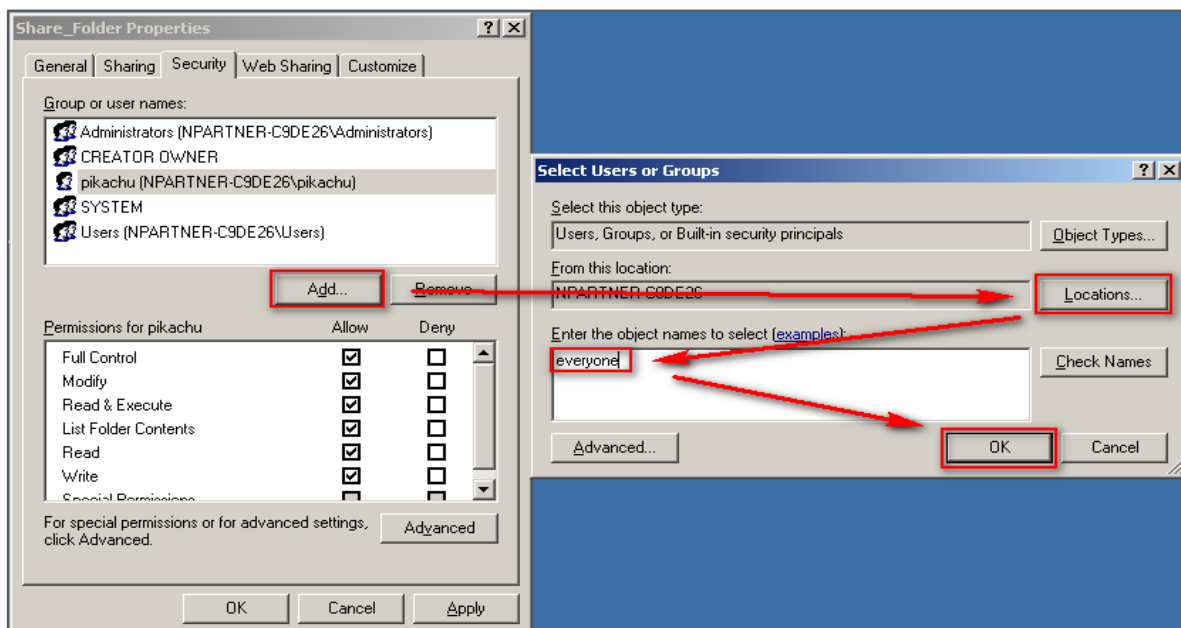
4. Set up user account privilege :

- (1) Choose a user account account.
- (2) Check [Full Control] and [Change] permissions.
- (3) Click [OK] .



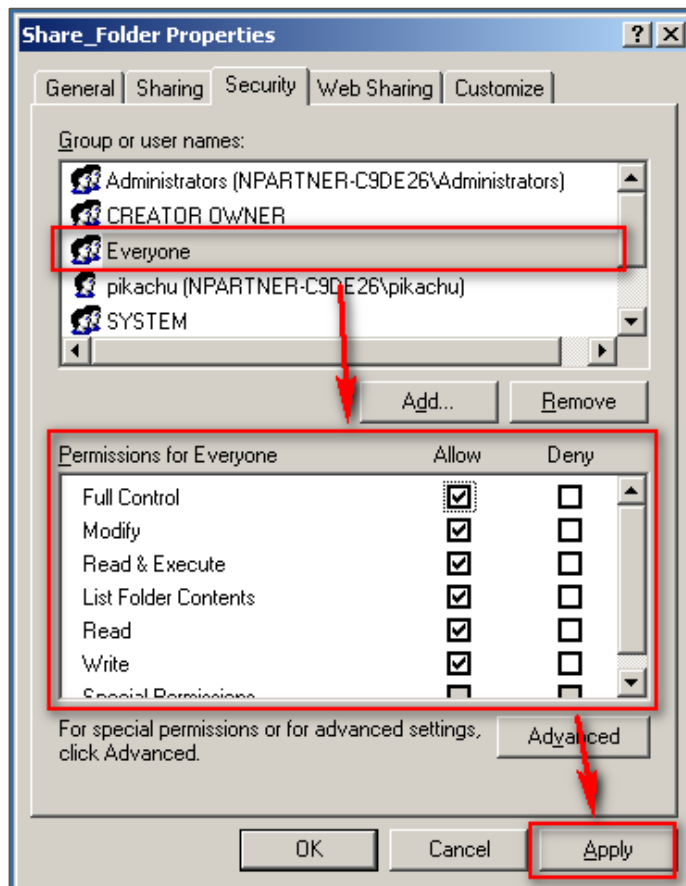
5. Security settings :

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



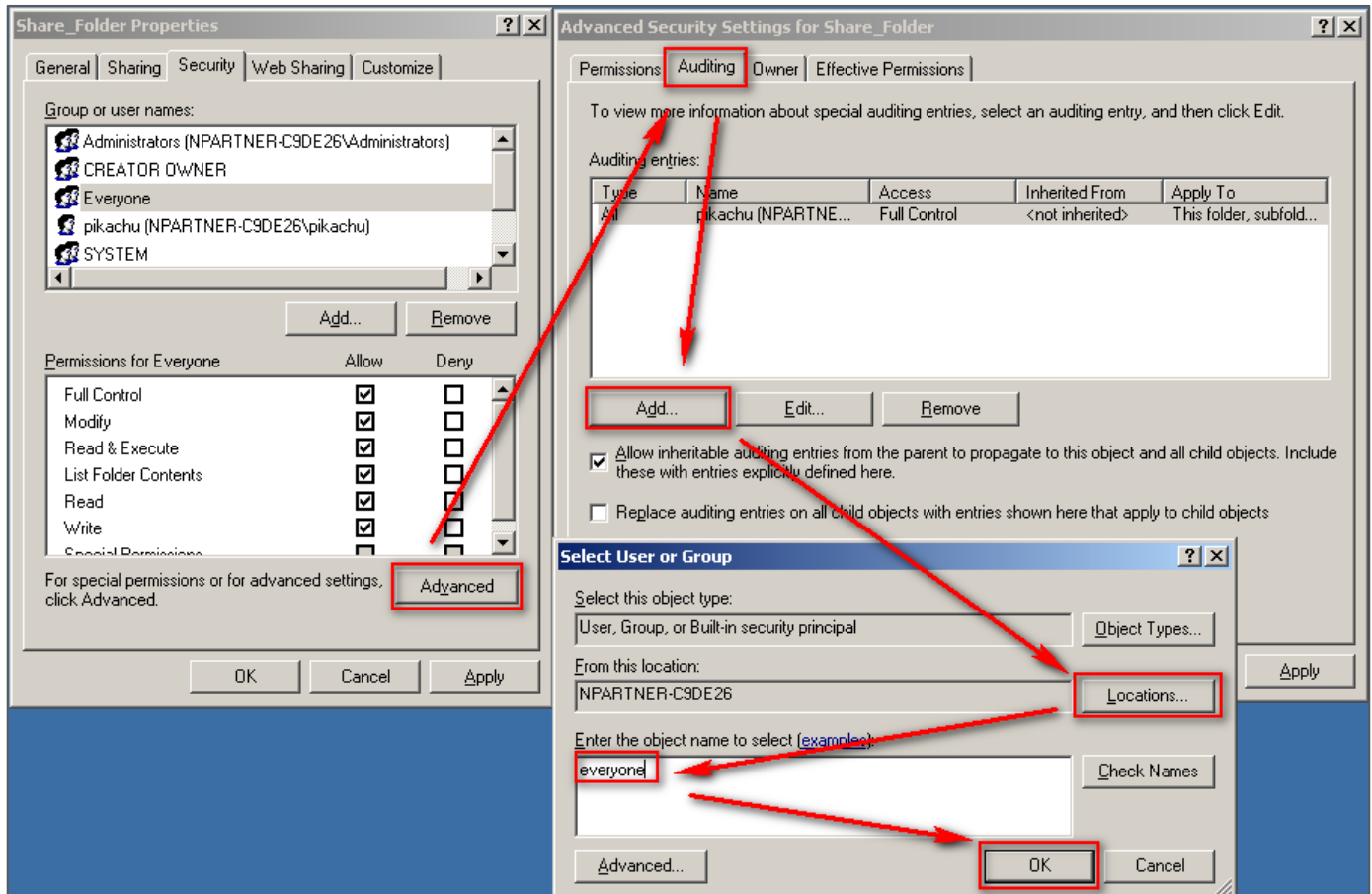
6. Set up user account privilege :

- (1) Choose the user account.
- (2) Check [Full Control] permissions.
- (3) Click [Apply].



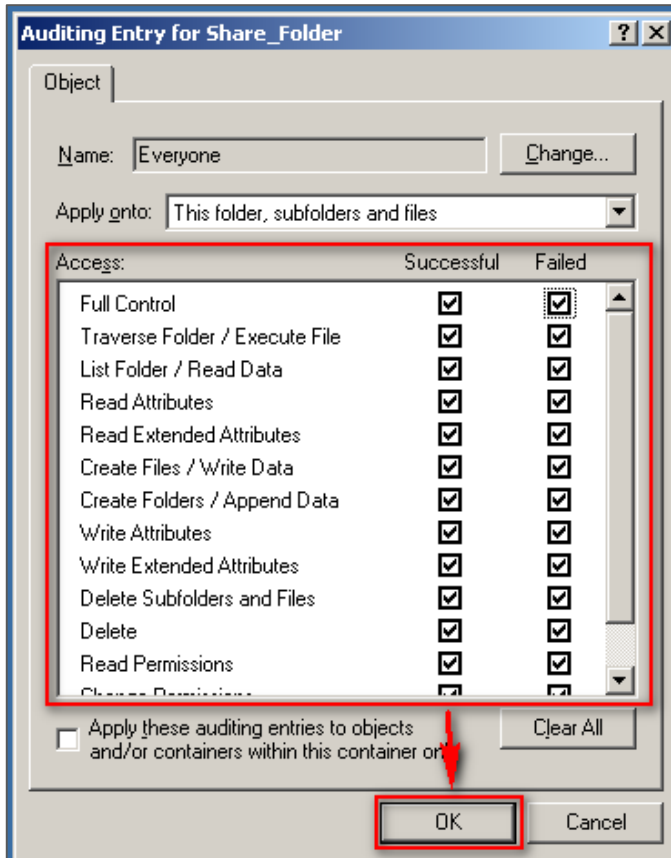
7. Advanced security settings :

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

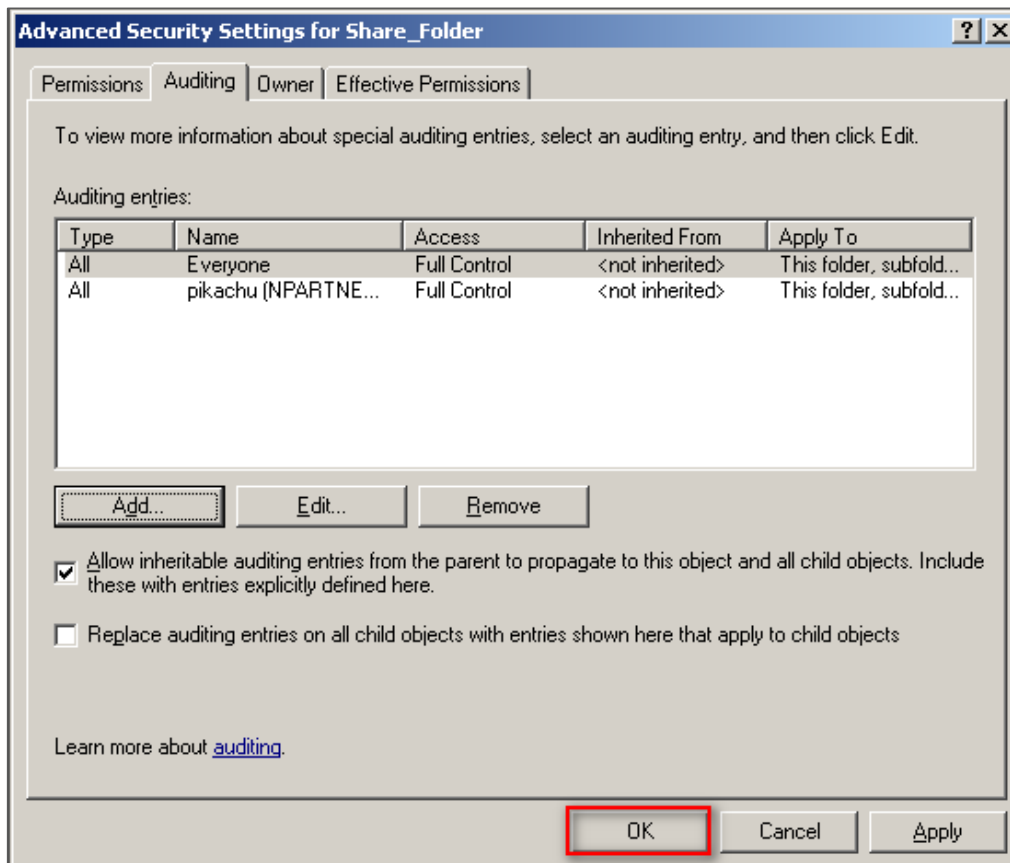


8. Audit entry settings :

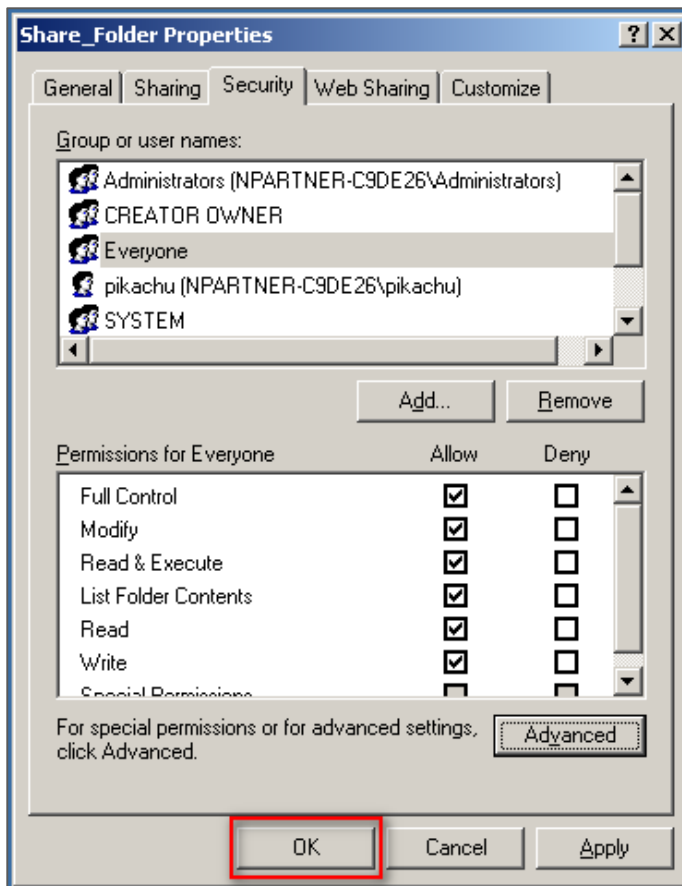
Check [Successful] and [Failed] of all the entries, then click [OK].



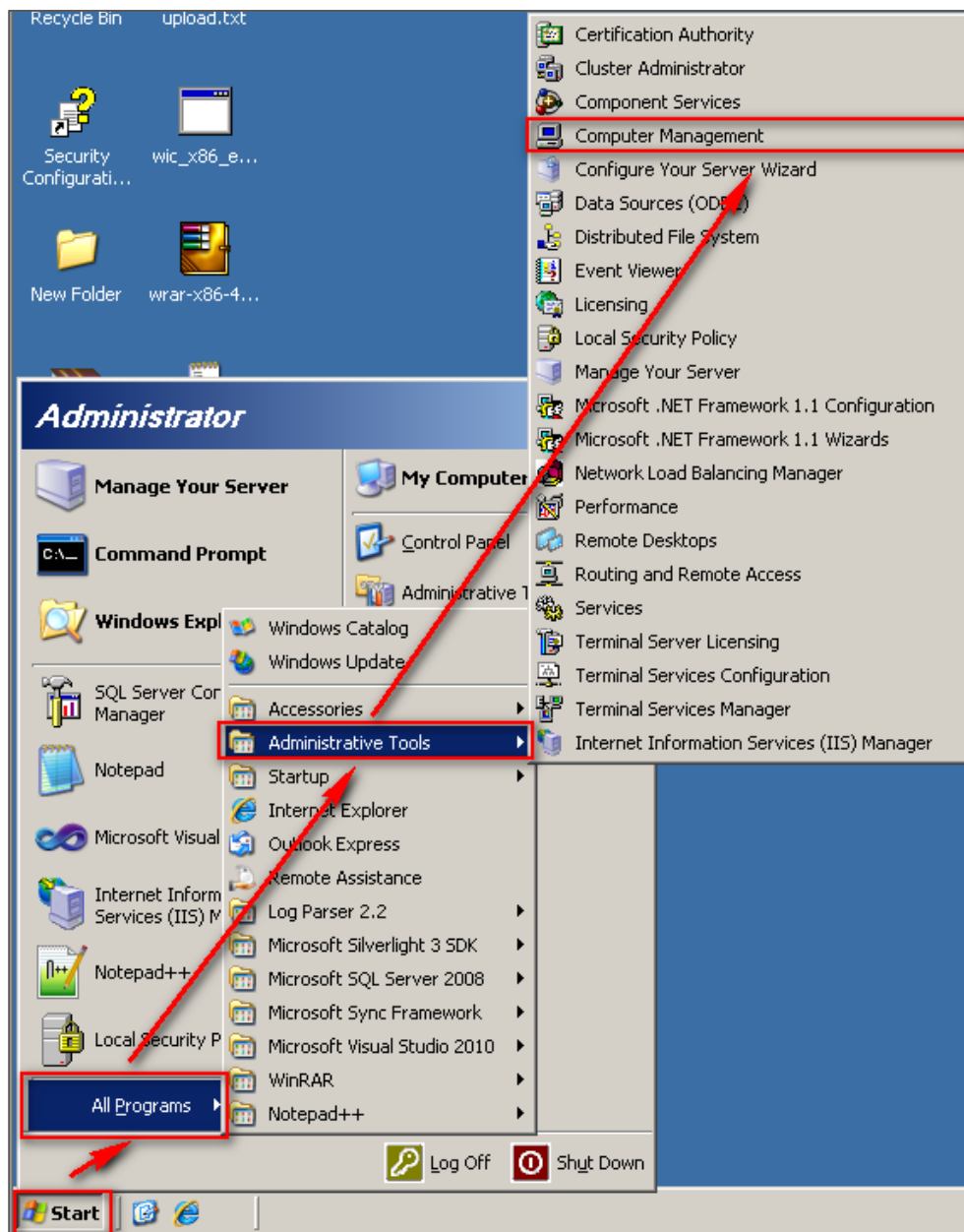
9. After completing advanced security settings. click [OK] .



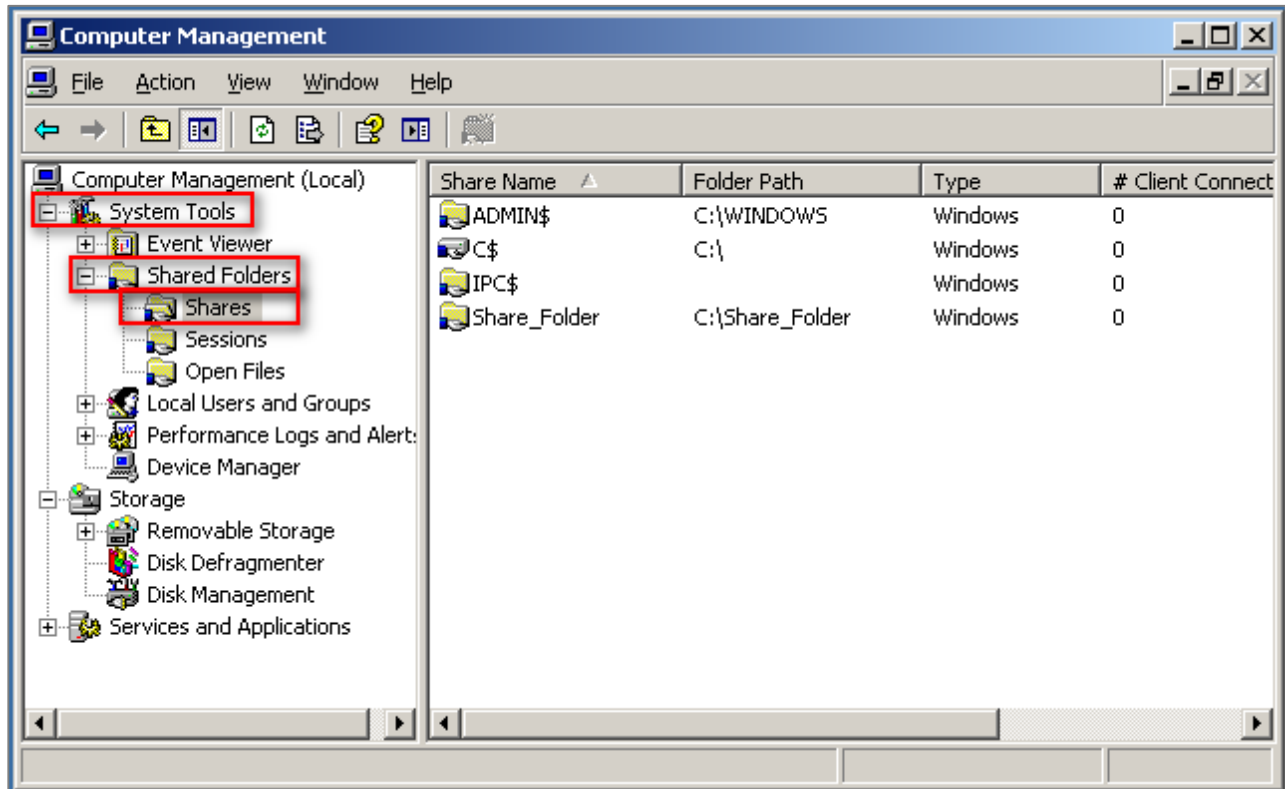
10. After completing shared folders settings, click [OK] .



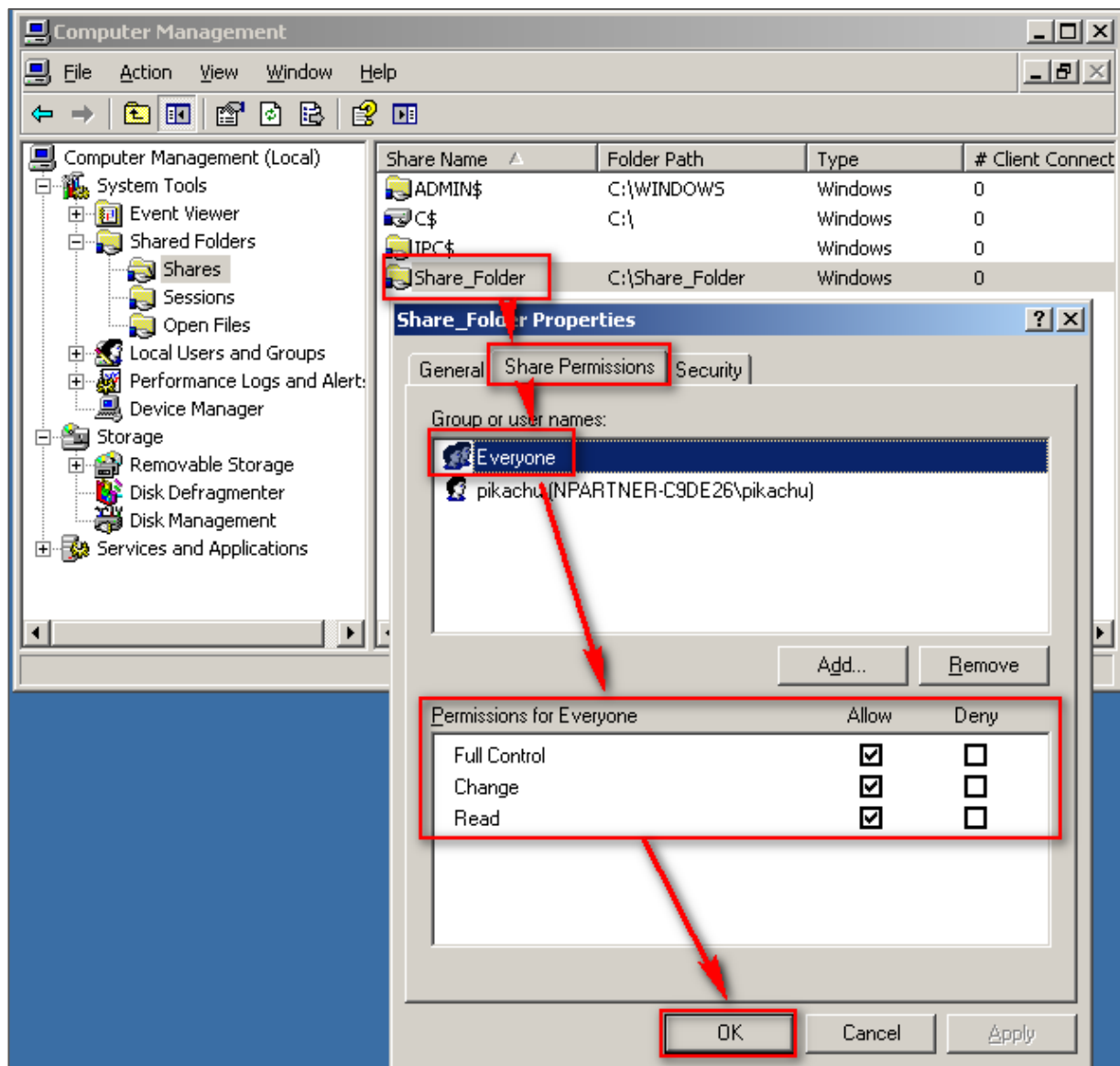
11. Click [Start / All Programs / Administrative Tools / Computer Management].



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



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



3 Windows 2008 Server Audit log Settings

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

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

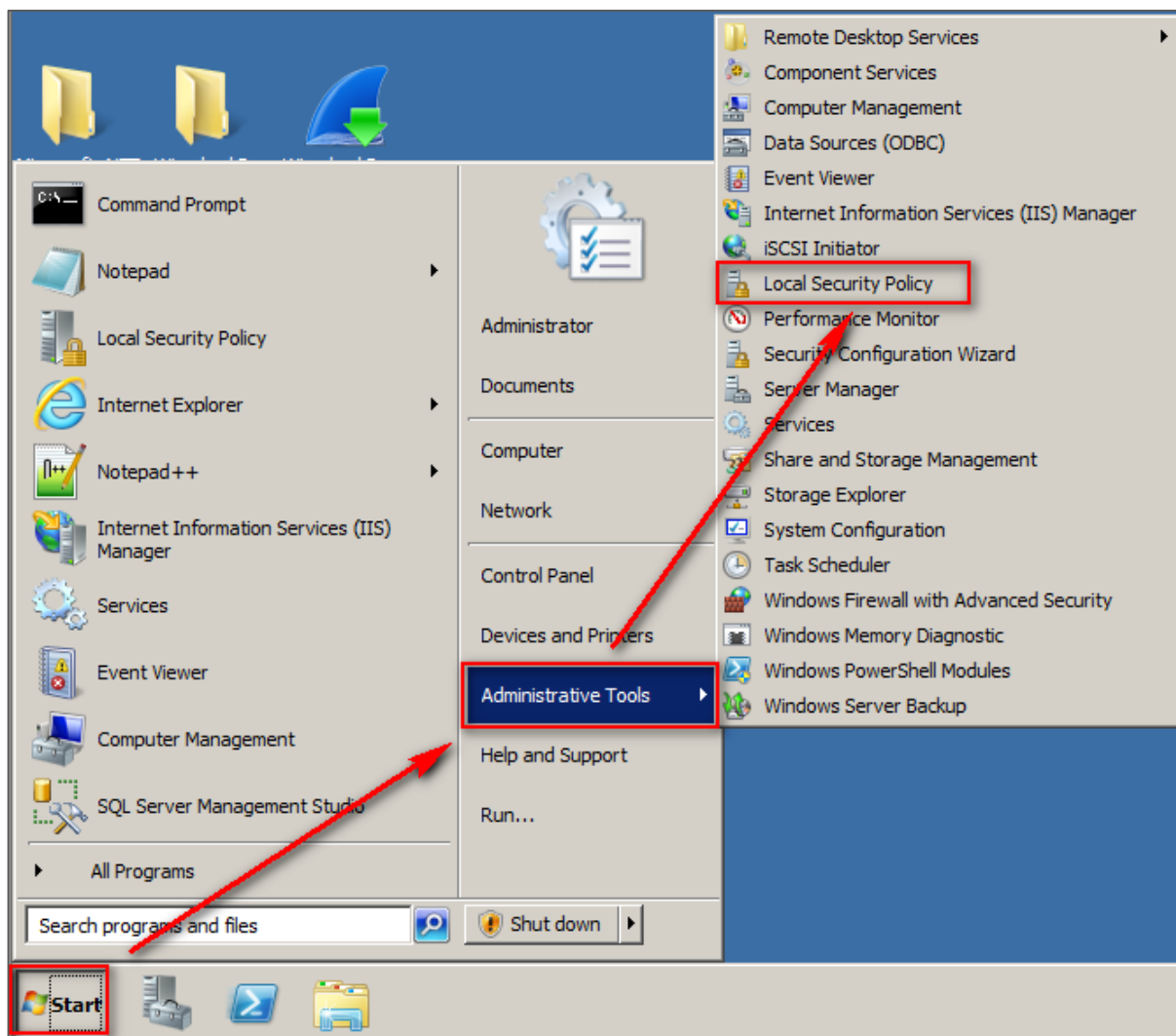
Please remember to download NXLOG, which may refer to section 1.

3.1 Setting up local login audit policy

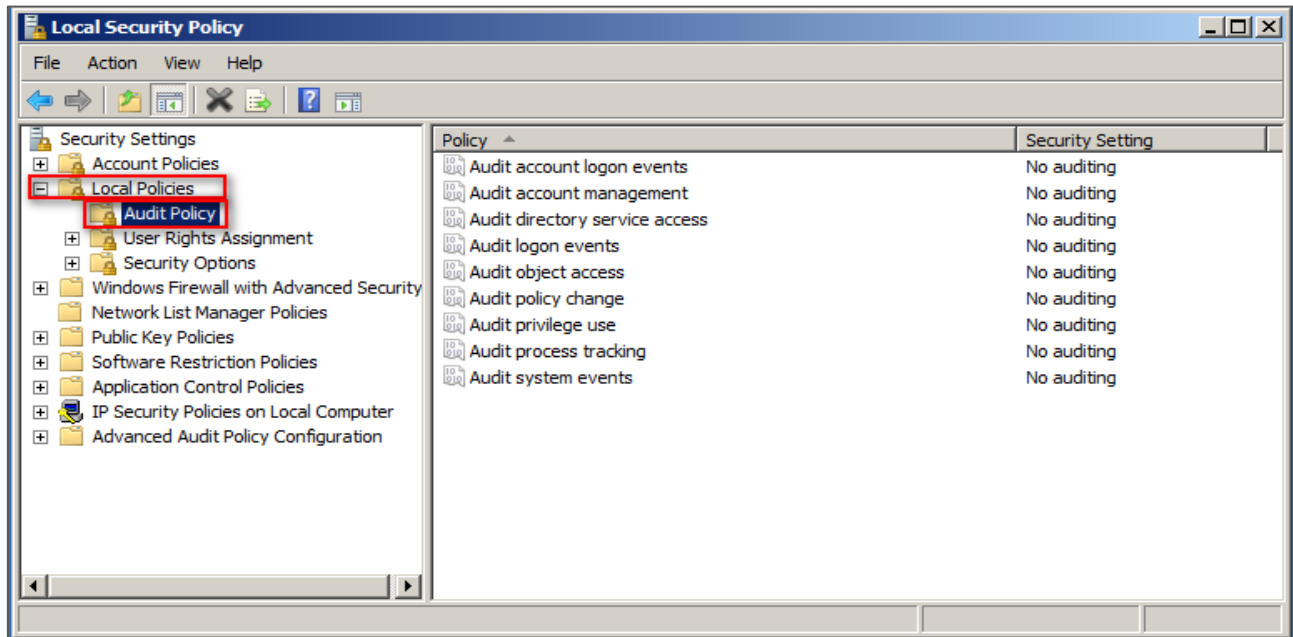
Set as follows :

1. Log in Windows 2008 Server as Administrator.

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



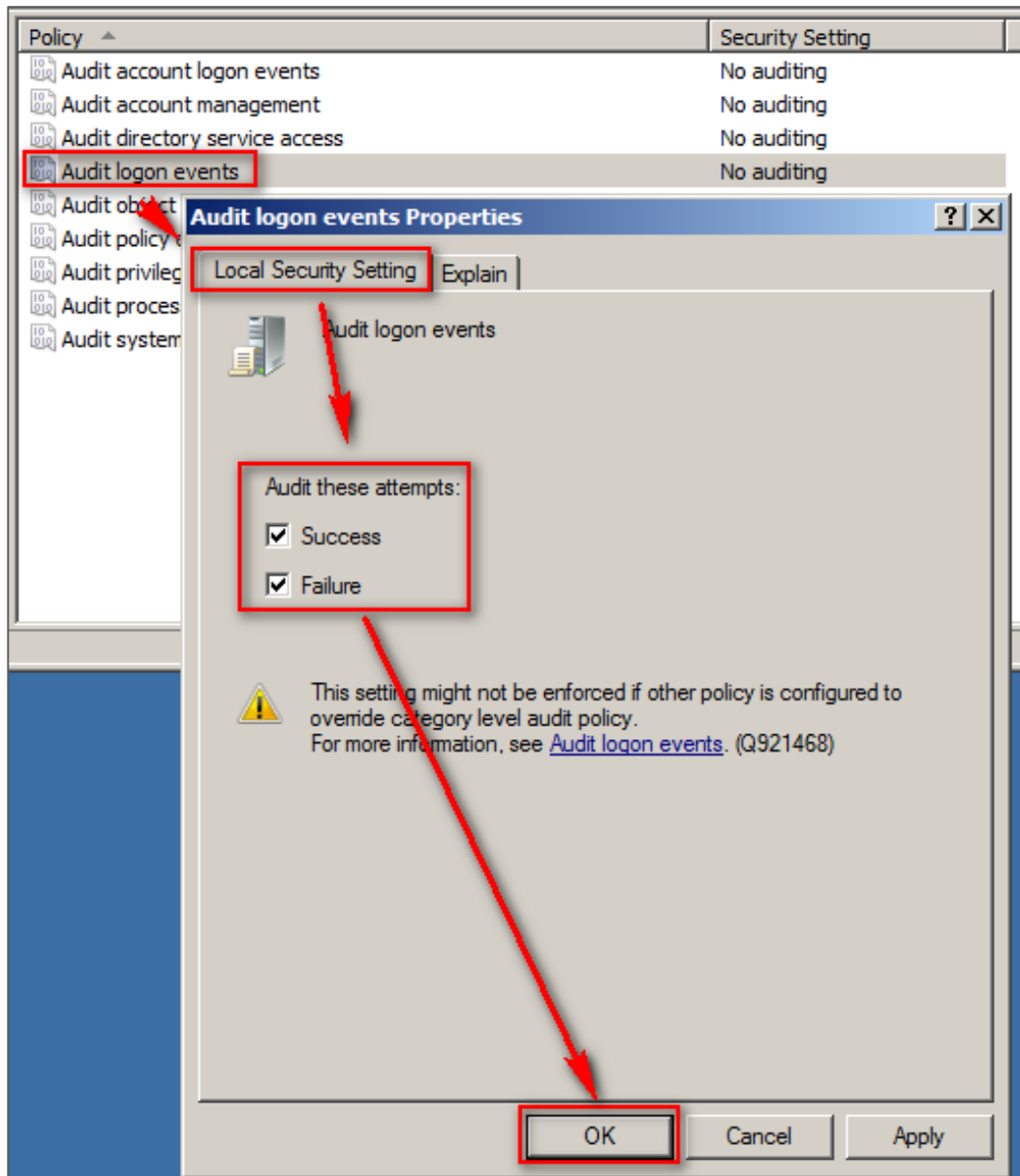
2. Click [Local Policies / Audit Policy] °



3. Define the following policy set value :

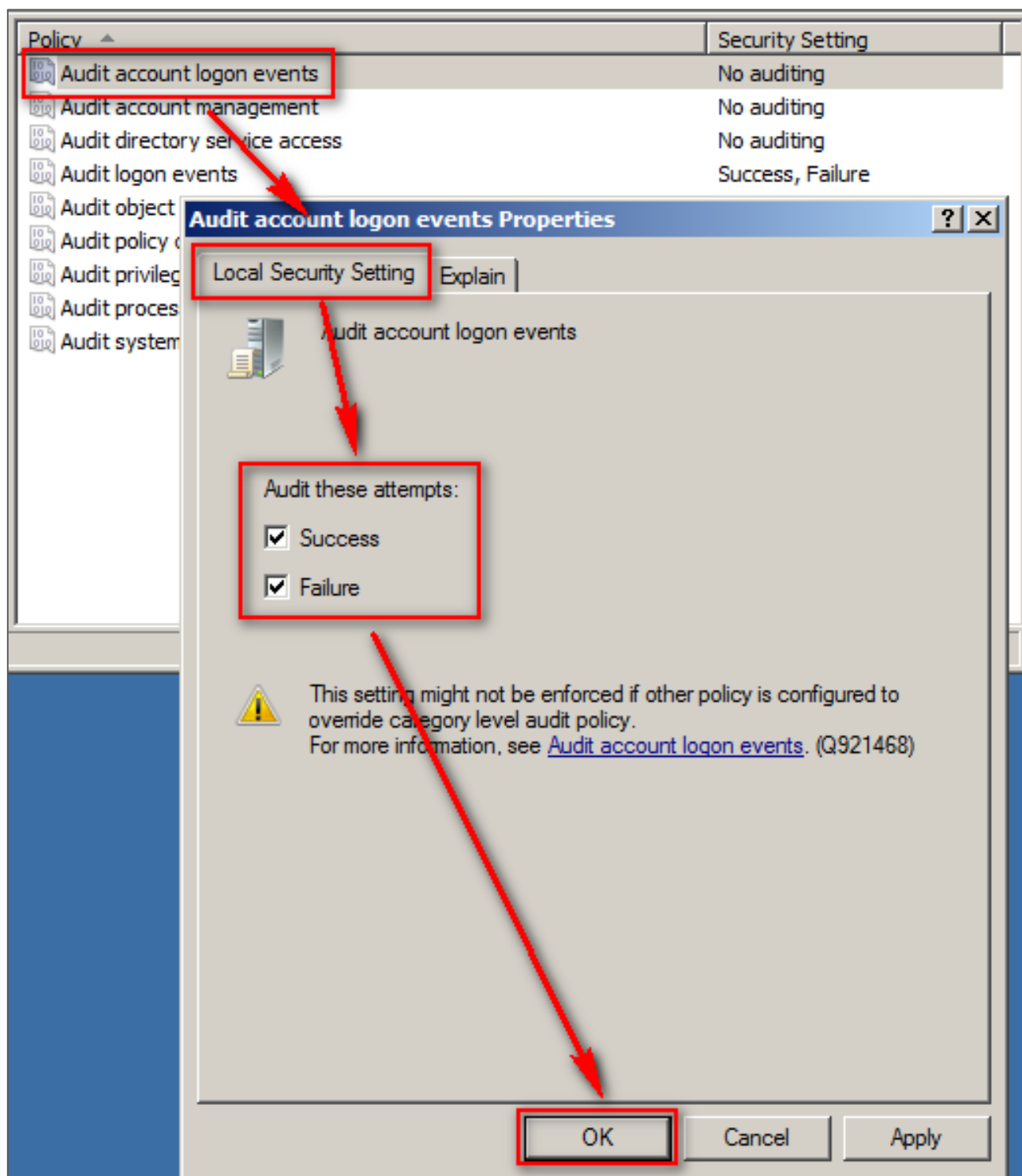
(1) Audit logon event :

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



(2) Audit account logon event :

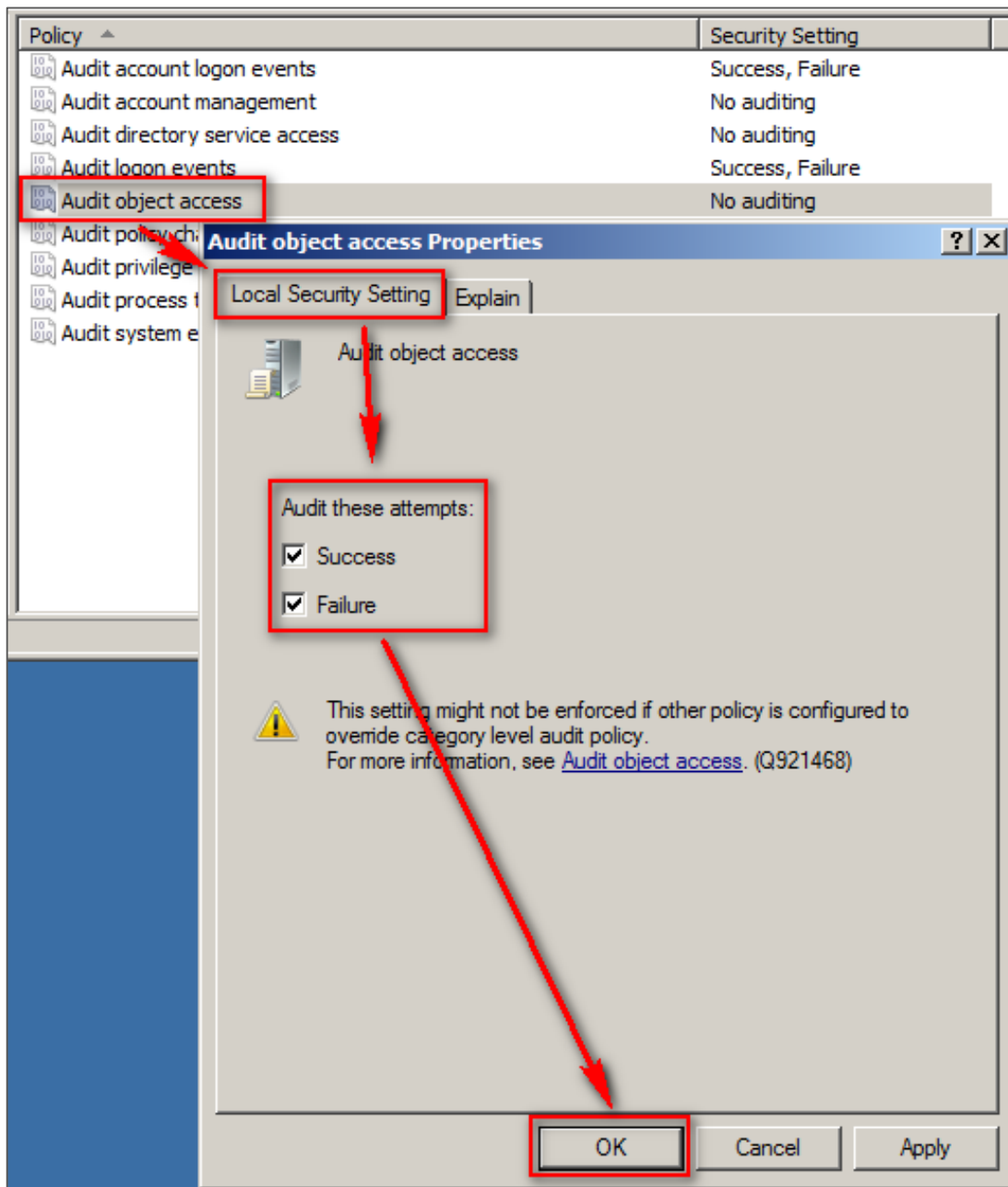
Double click [Audit logon events], check [Success] and [Failure], then click [OK].



(3) Audit object access :

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

(4) Changing audit policy :



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

(5) Audit account management :

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

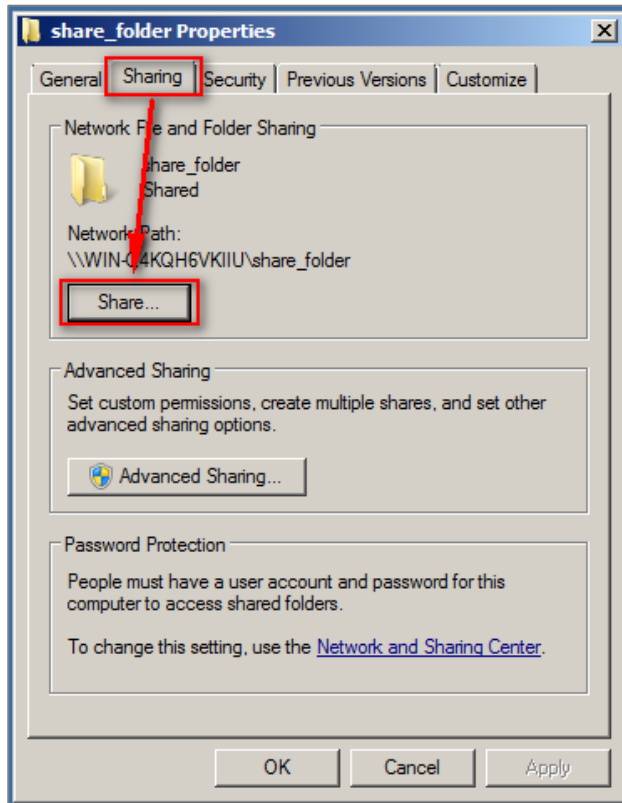
Note : If Windows 2008 Server does not run File server audit, we recommend not to audit object access, please skip steps 3.1(3) and 3.2, and only operate steps 3.1 (1), (2), (4), (5). This will help Windows avoid auditing unnecessary Object access security events. These unnecessary and redundant security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

sent to N-Reporter will reduce its performance.

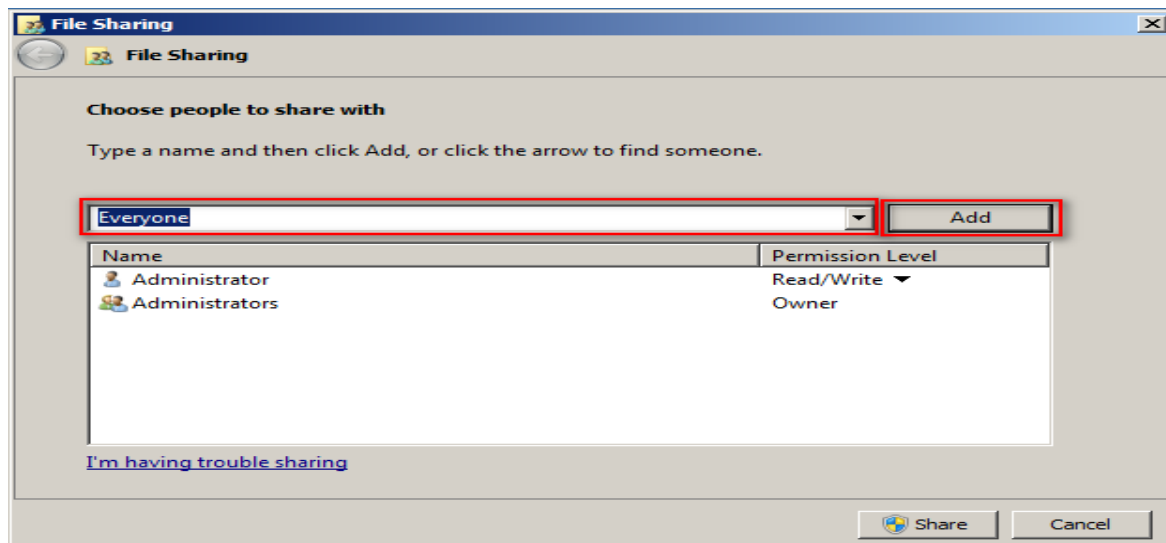
3.2 Setting up local shared folder authorization and audit policy

Set as follows :

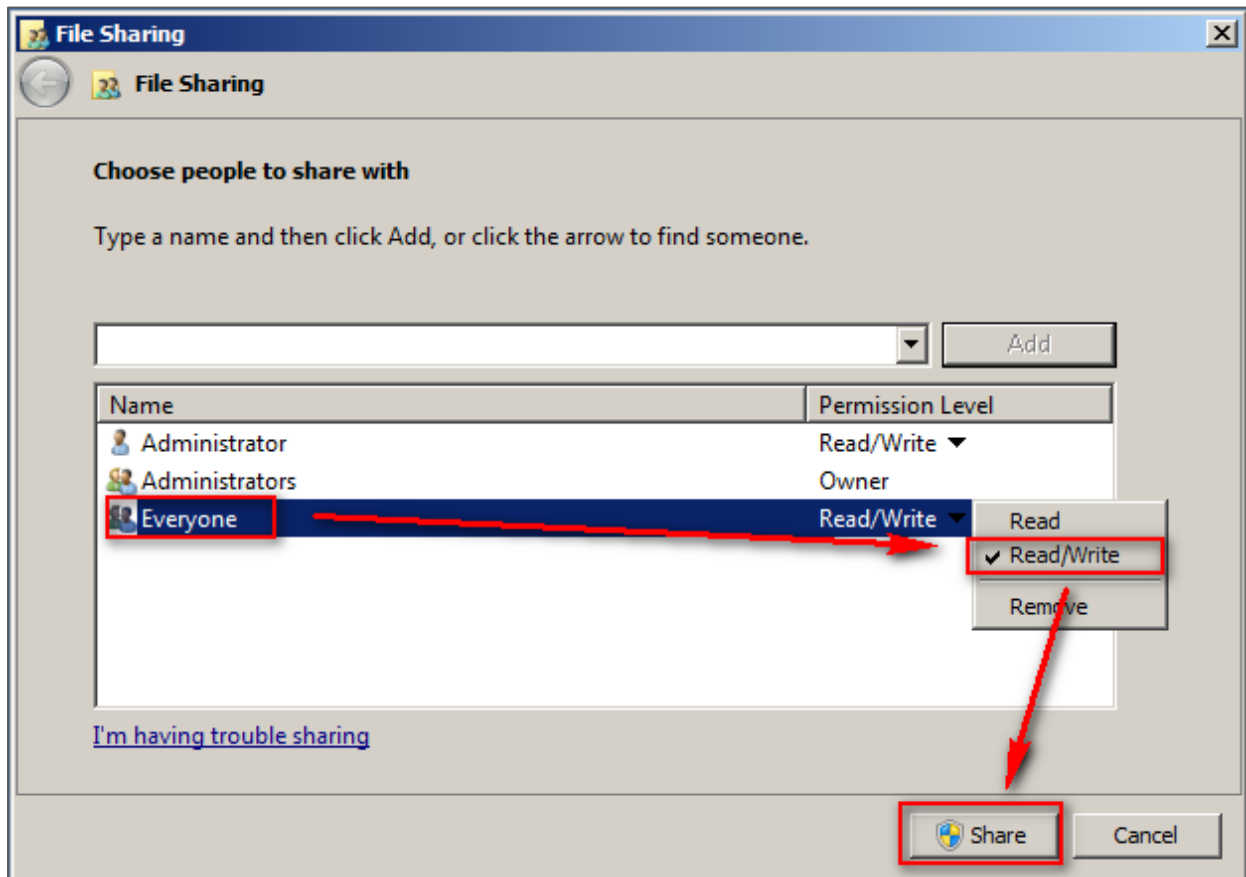
1. Right click the folder you want to share, click [Properties].
2. Click [Sharing], then click [Share].

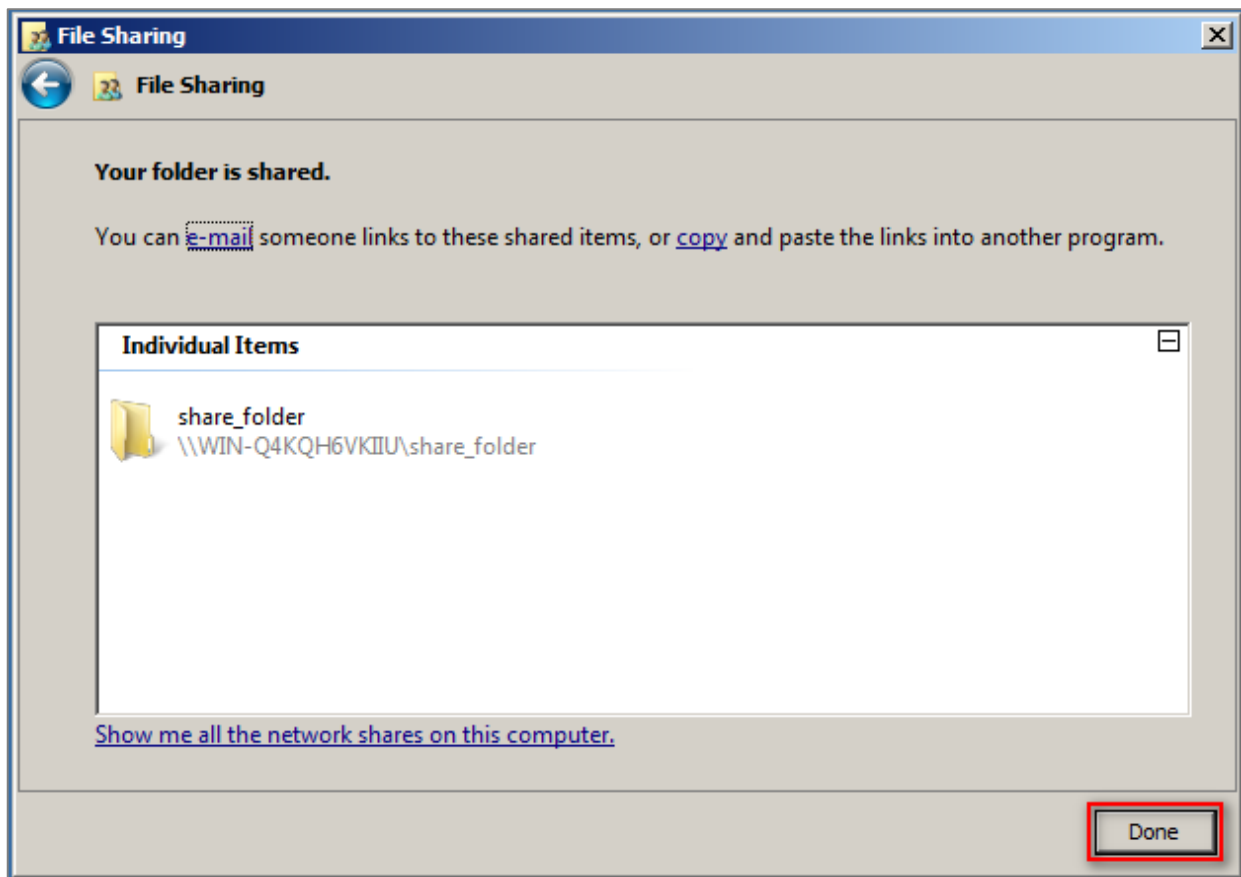


3. In share permissions settings, open the menu and choose an existing user account, then click [Add].



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

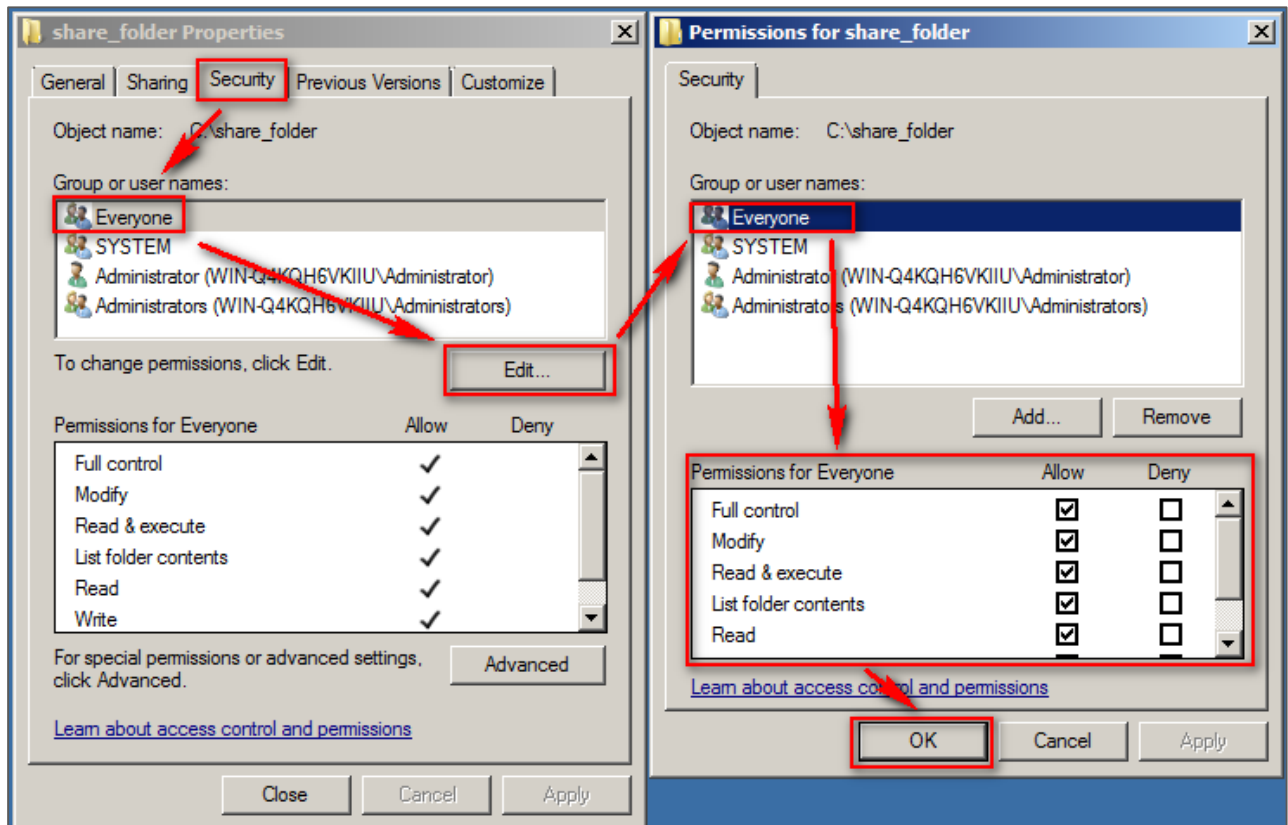




4. When you complete setting, click [OK].

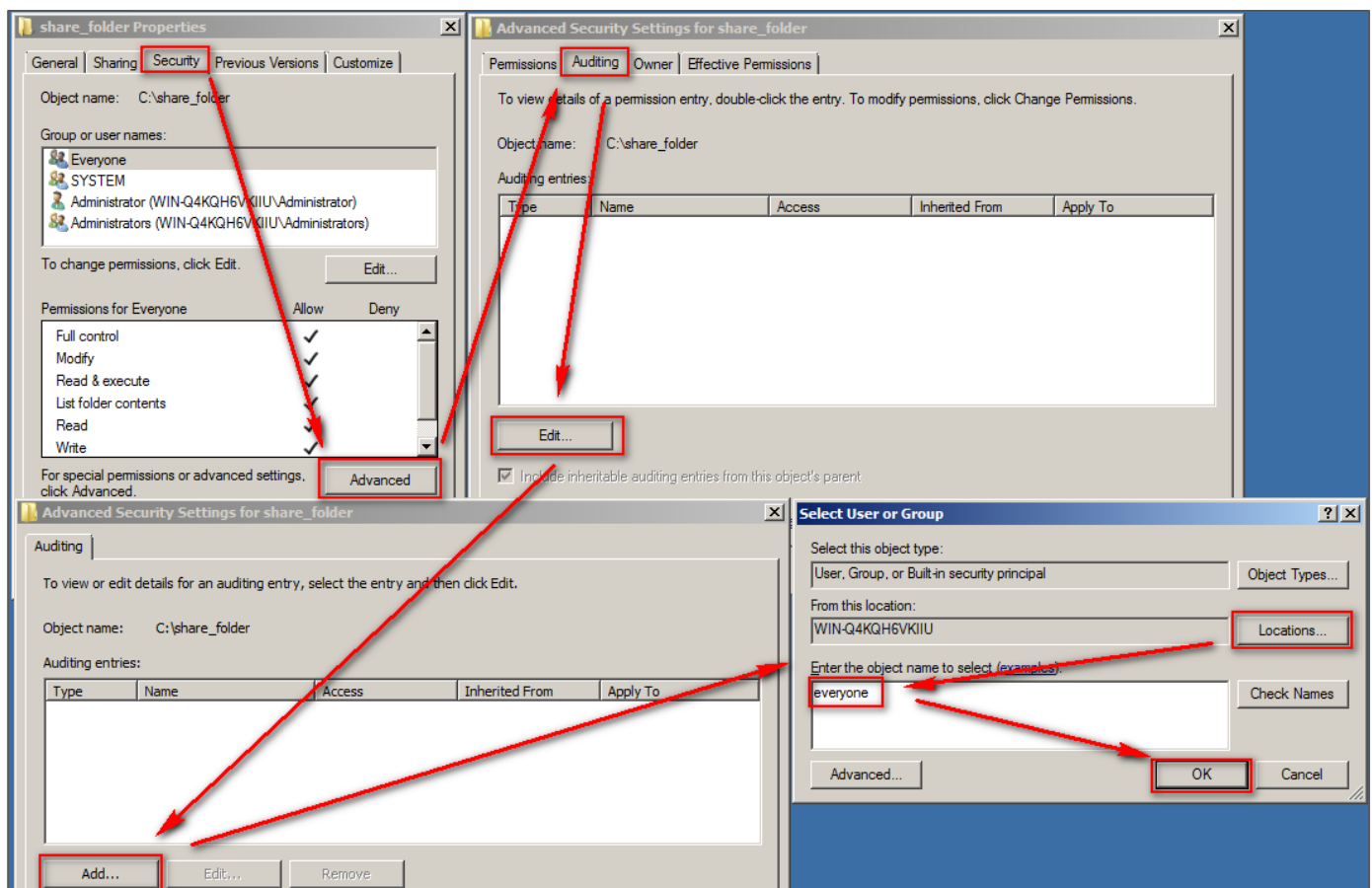
5. Security settings :

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



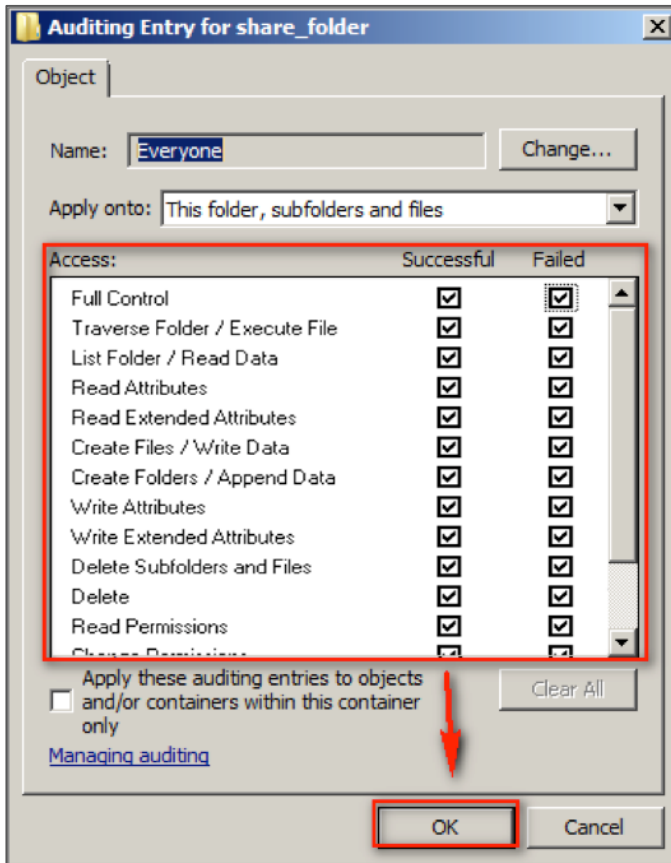
6. Advanced security settings :

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

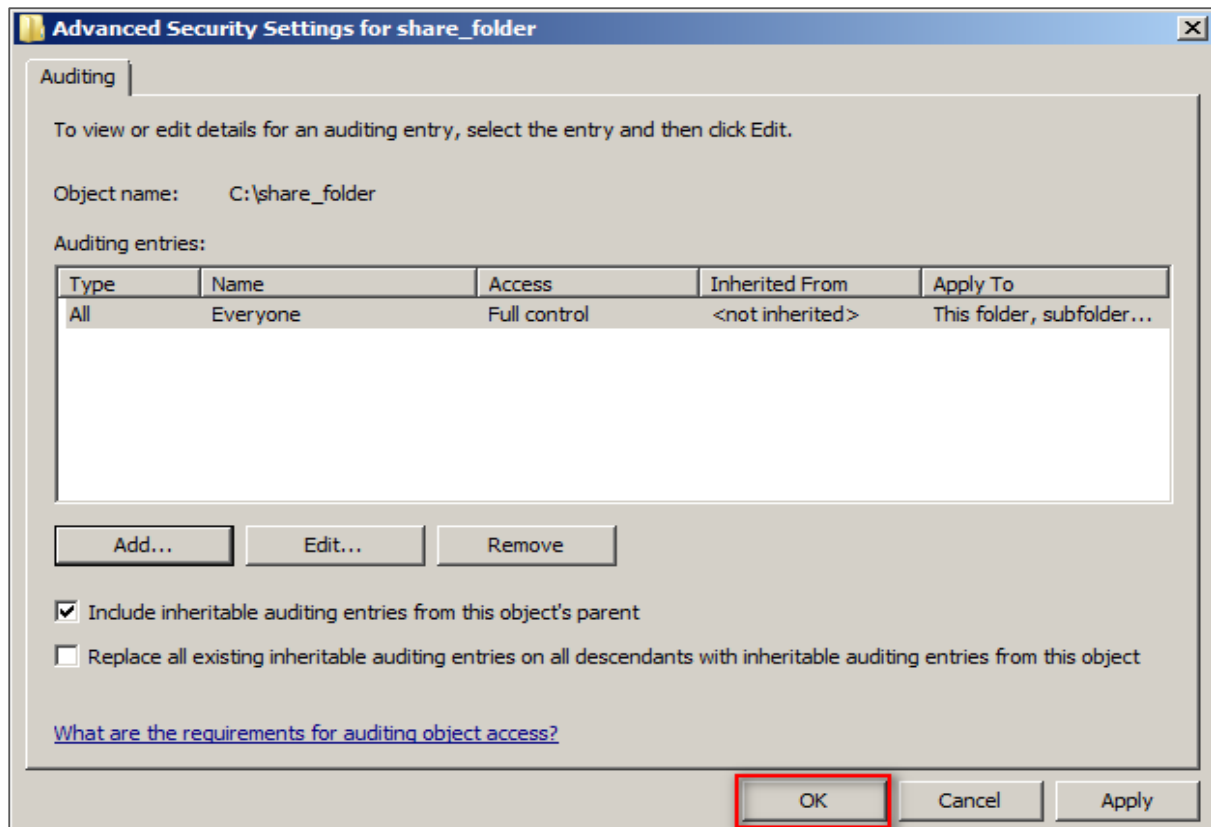


7. Audit entry settings :

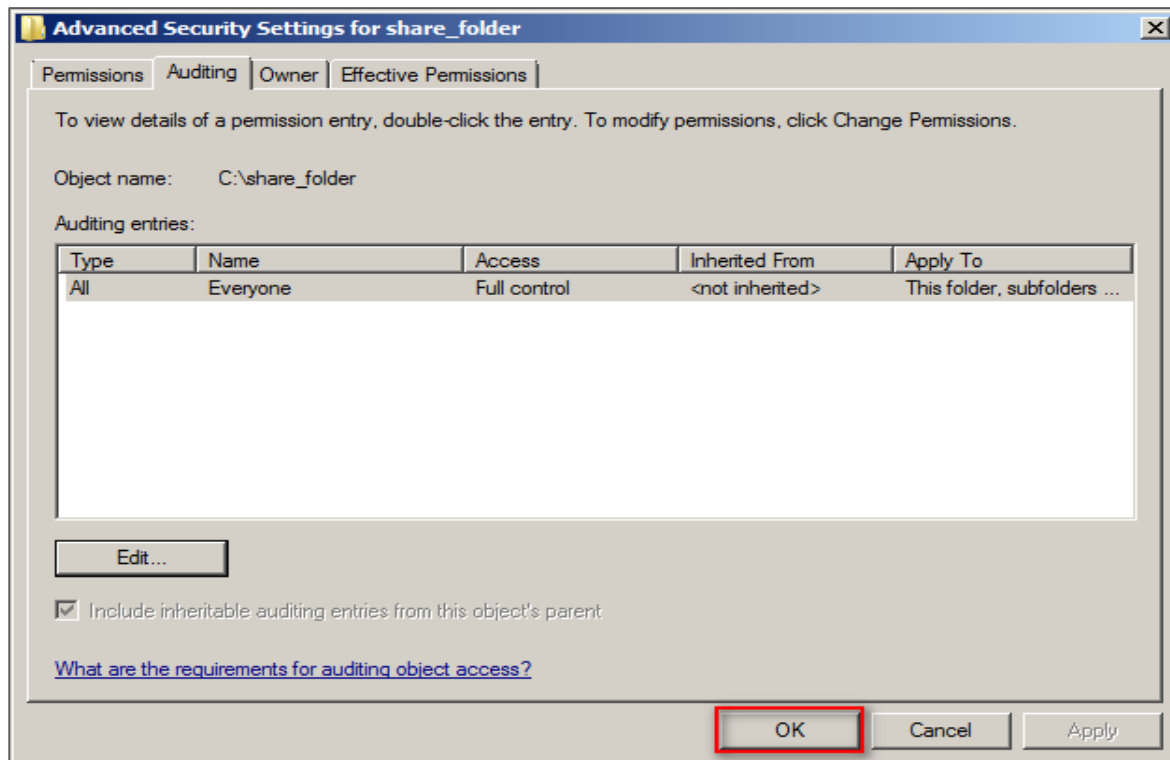
Check [Success] and [Failure] of all the entries, then click [OK].



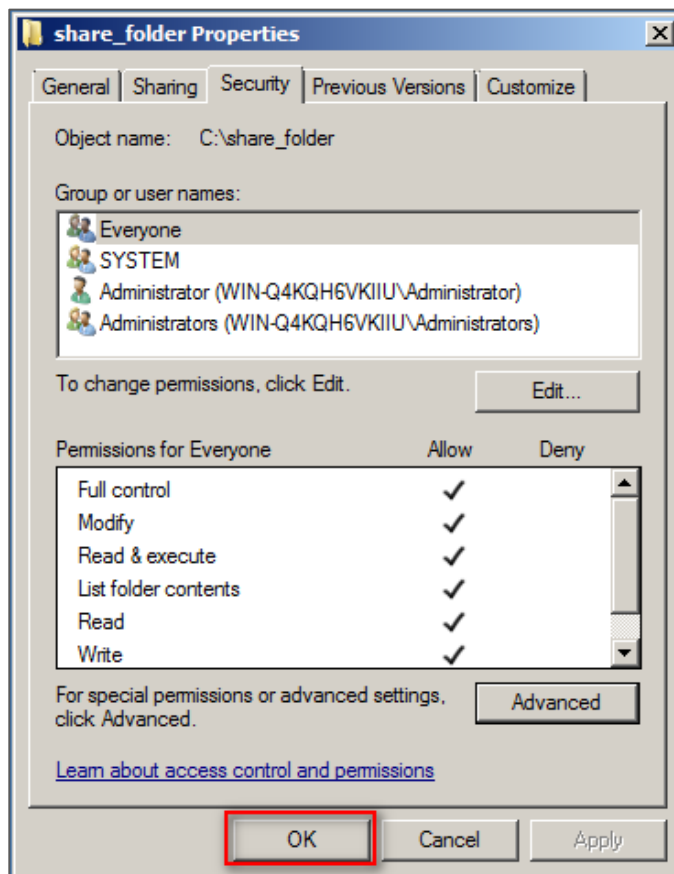
8. After completing advanced security settings, click [OK].



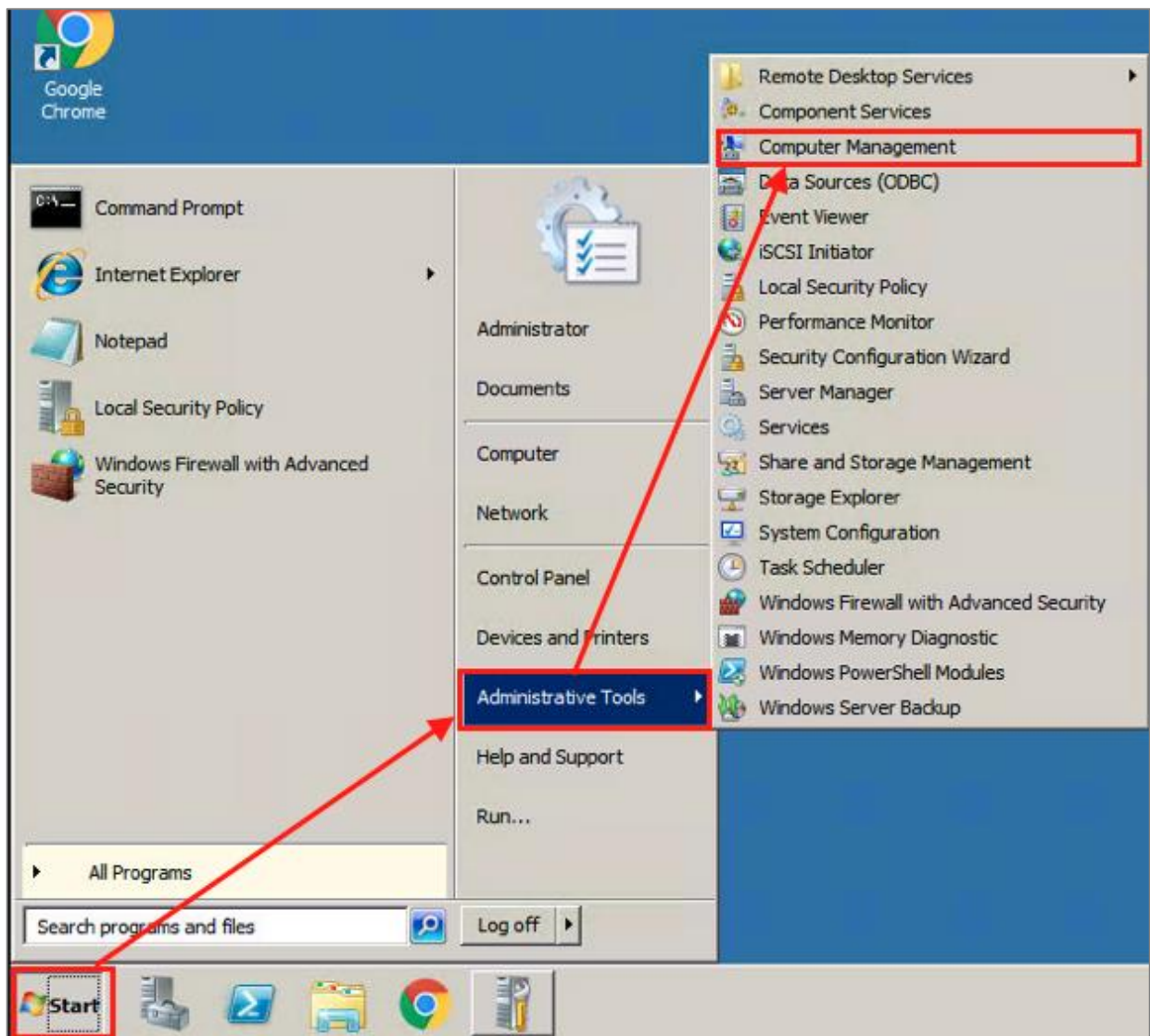
9. After completing shared folders settings, click [OK].



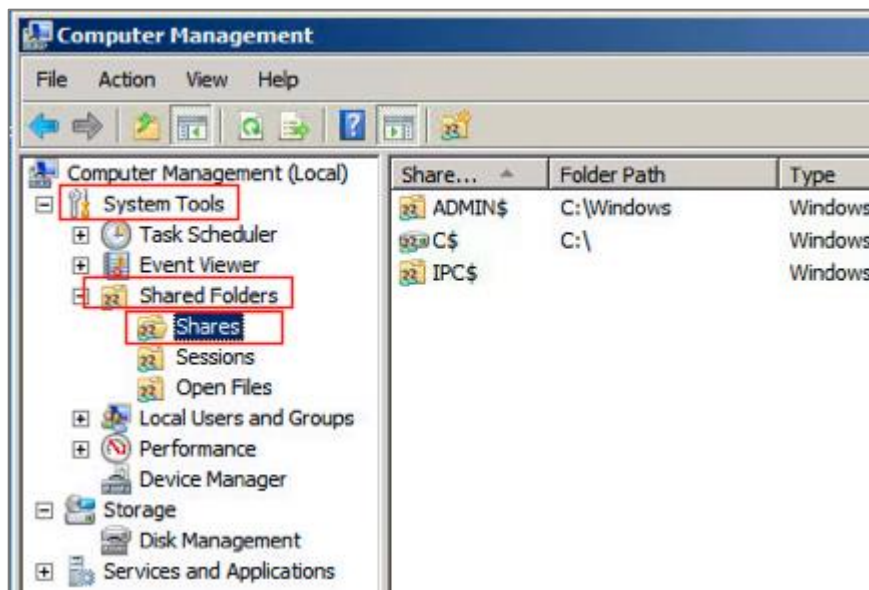
10. After completing shared folders settings, click [OK].



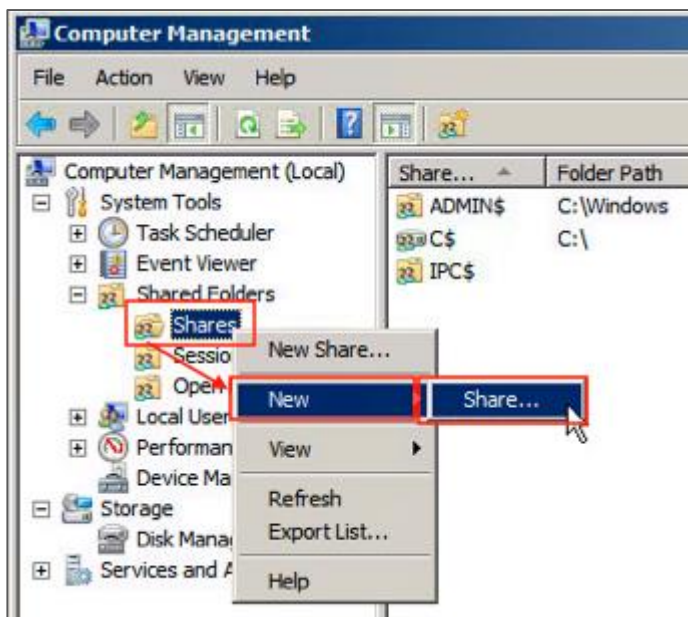
11. Click [Start / Administrative Tools / Computer Management].



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



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

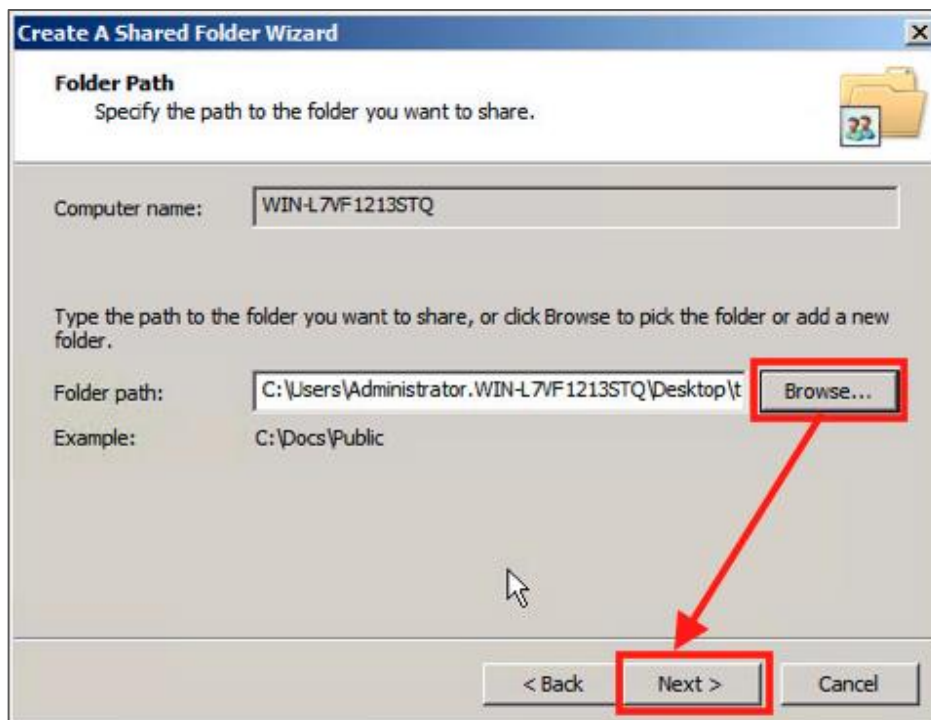


14. New share wizard settings :

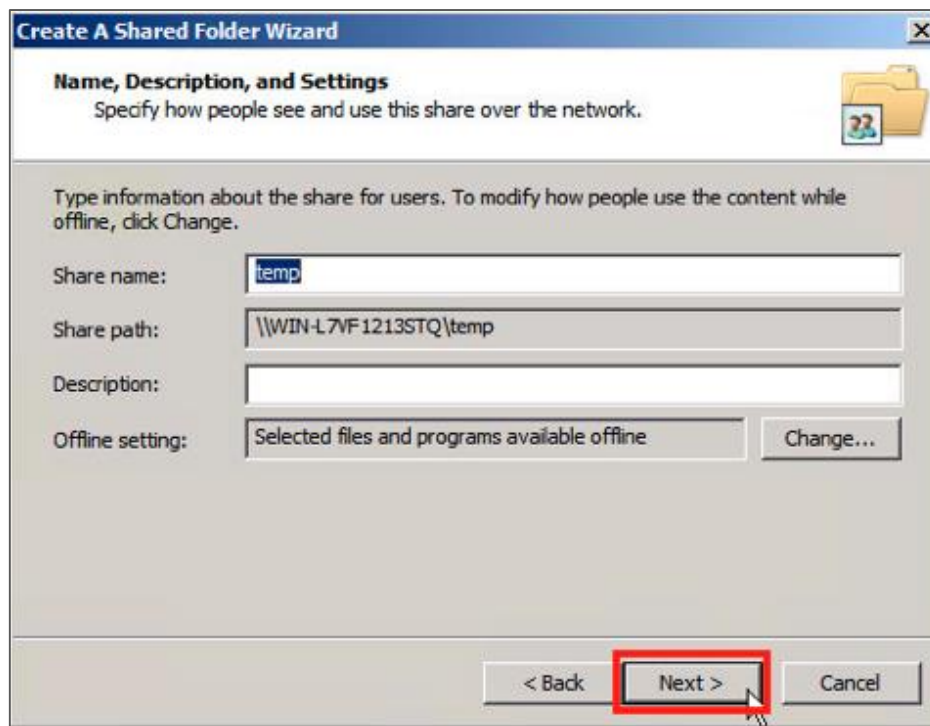
(1) Click [Next].



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



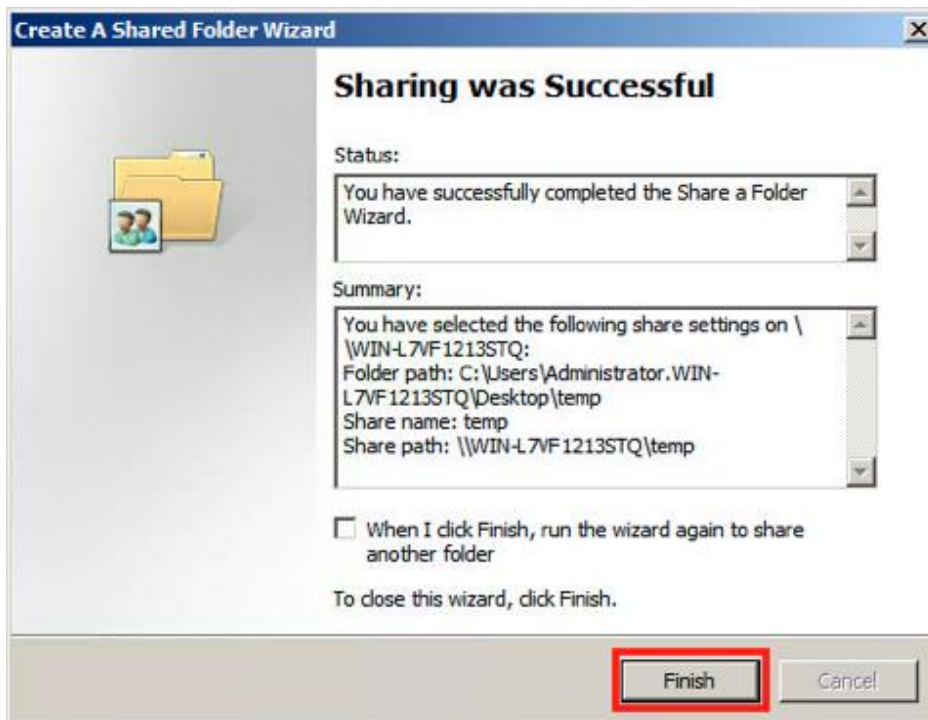
(3) Click [Next].



(4) Click [Finish].

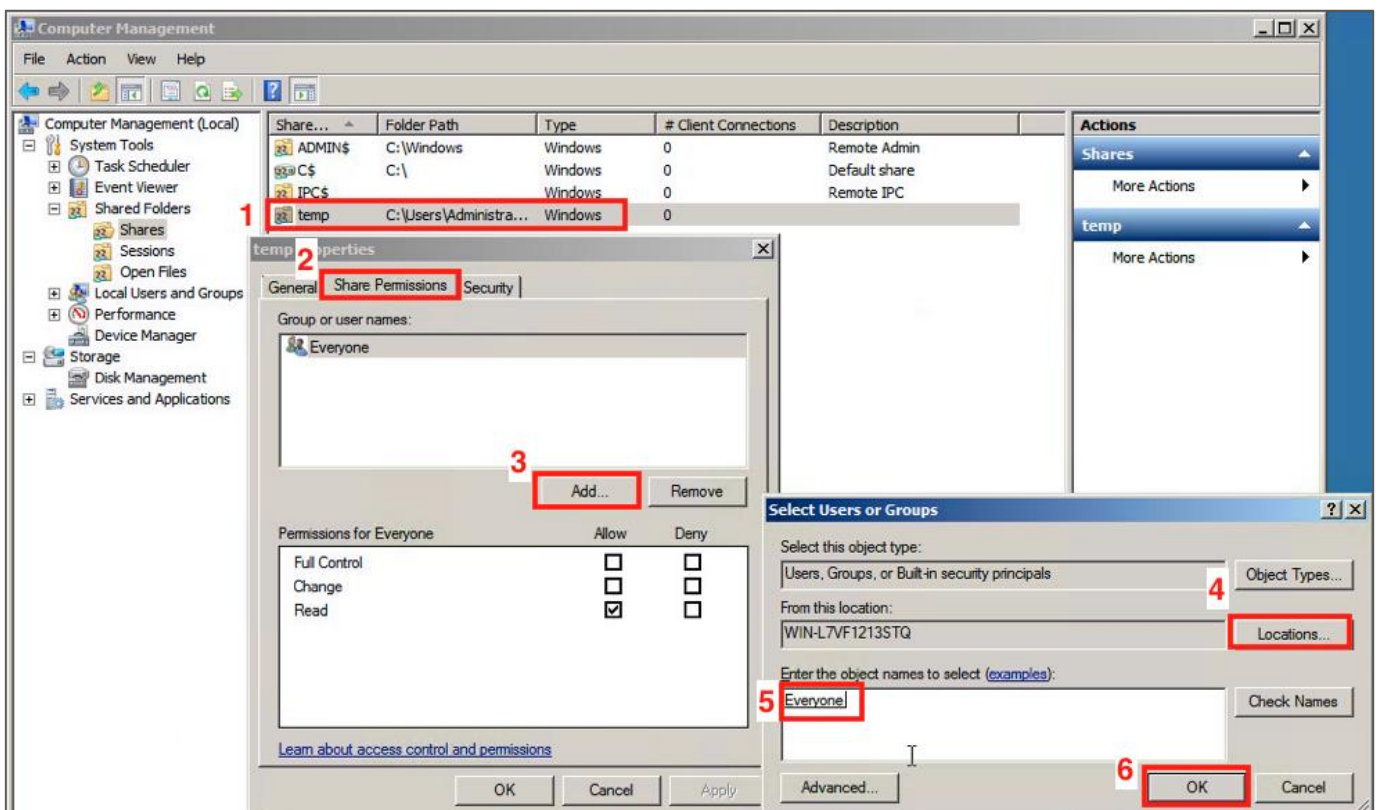


(5) Click [Finish].



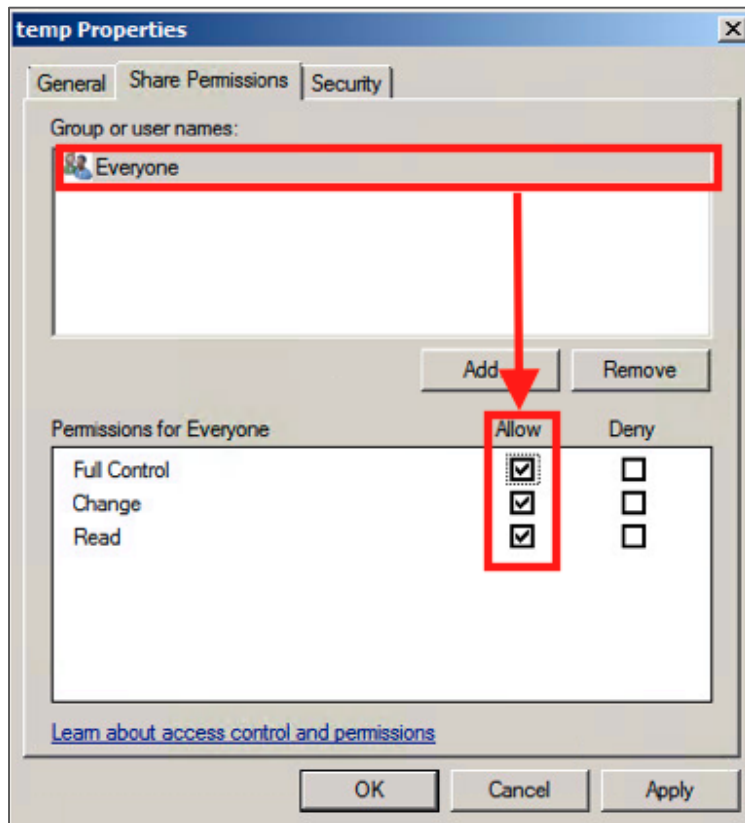
15. Shared folder administrator settings :

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



16. Share permissions settings :

Choose the user account, check to allow [Full Control], [Change] and [Read] permissions, then click [OK] .



4 Windows 2012 Server Audit log Setting

This section mainly discuss the following two settings :

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

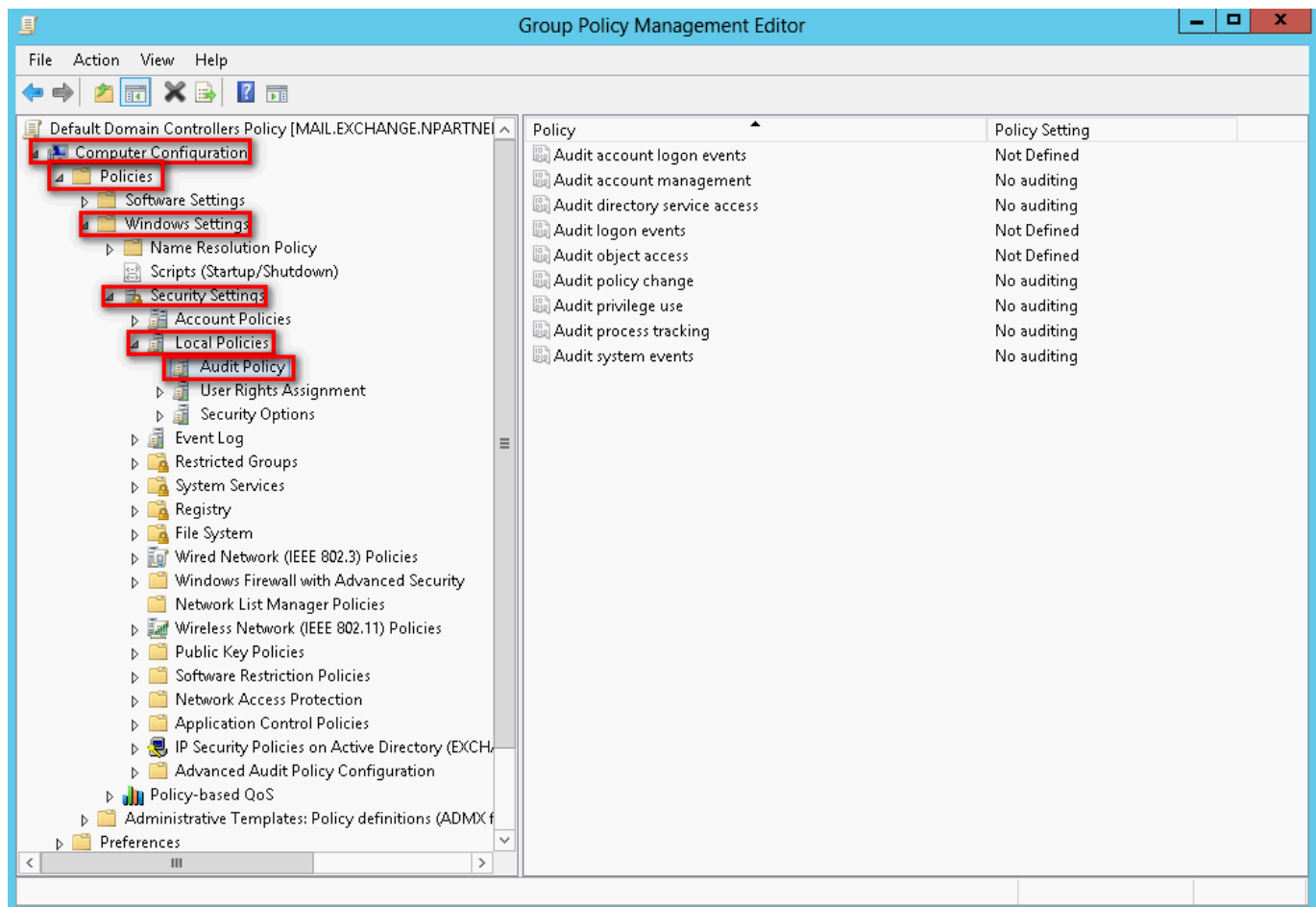
The default setting about Windows 2012 Server audit and share folder policy is off.

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

4.1 Setting up local login audit policy

Set as follows :

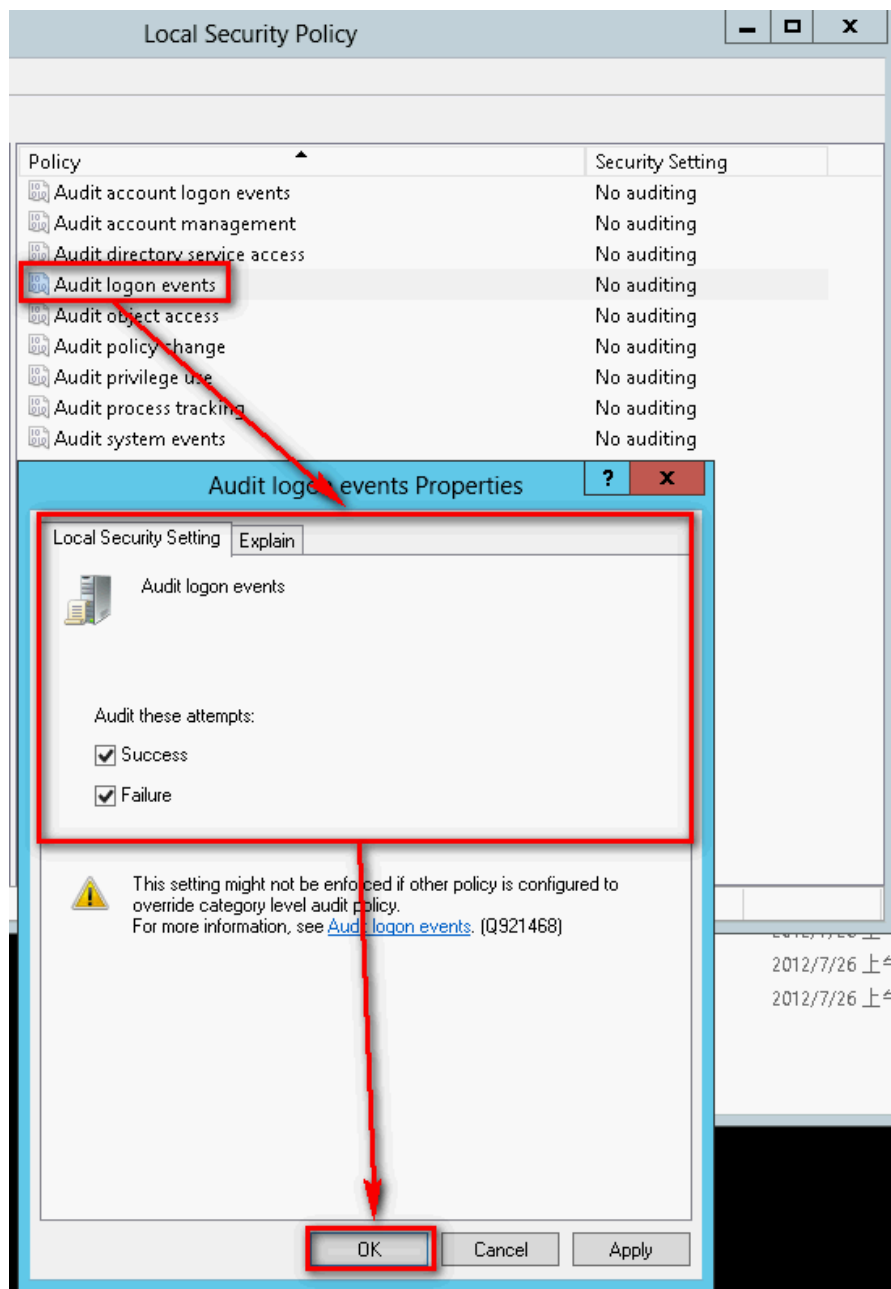
1. Log in Windows 2012 Server as Administrator, click [Start / Administrative Tools / Local Security Policy], extend [Local Security Policy].
2. Click[Security Settings / Local Policies / Audit Policy] °



3. Define the following policy set value :

(1) Audit logon events :

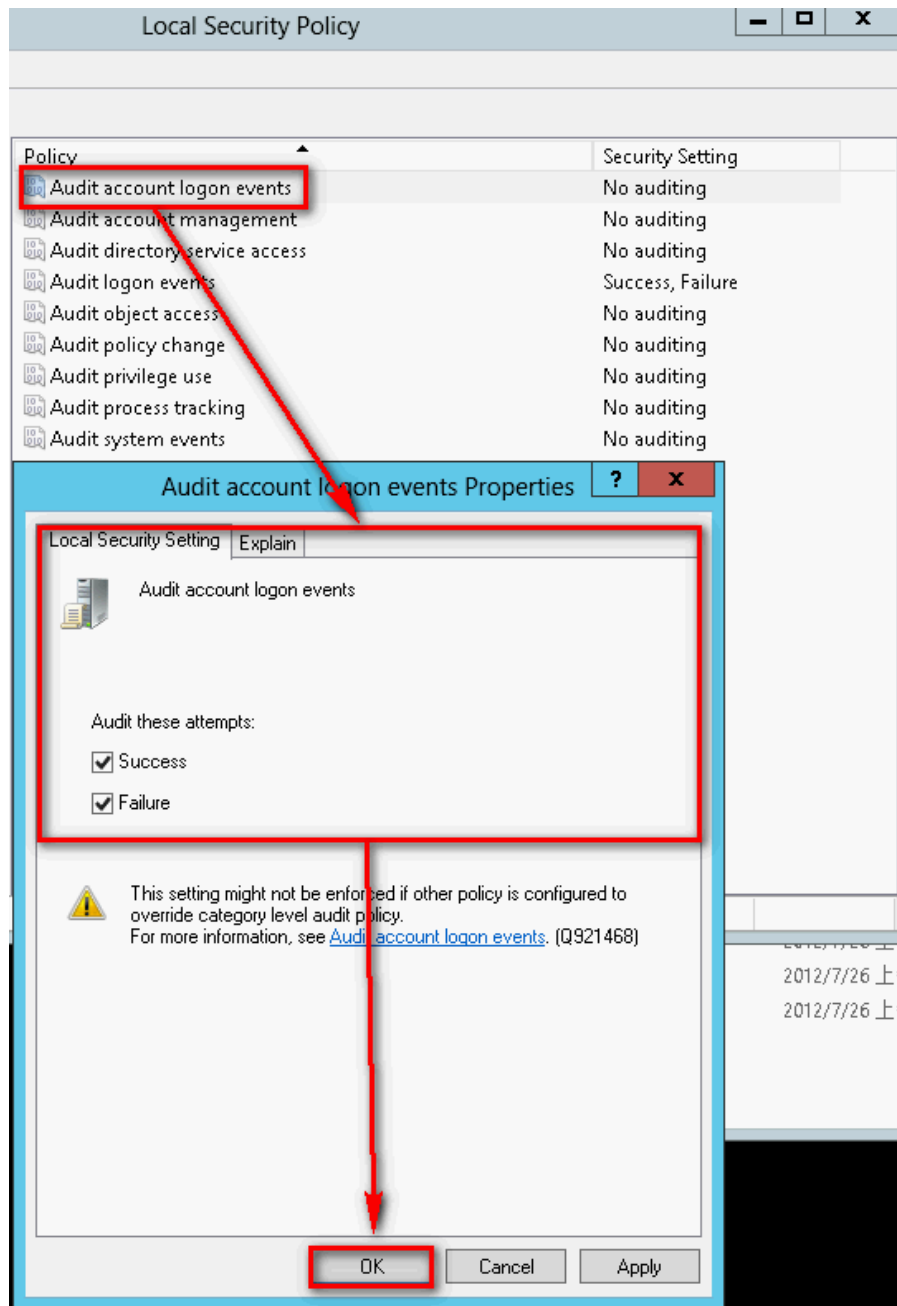
Double click [Audit logon events], check [Success] and [Failure], then click [OK].



(2) Audit account logon events :

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

(3) Audit object access :



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

(4) Audit policy change :

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

(5) Audit account management :

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

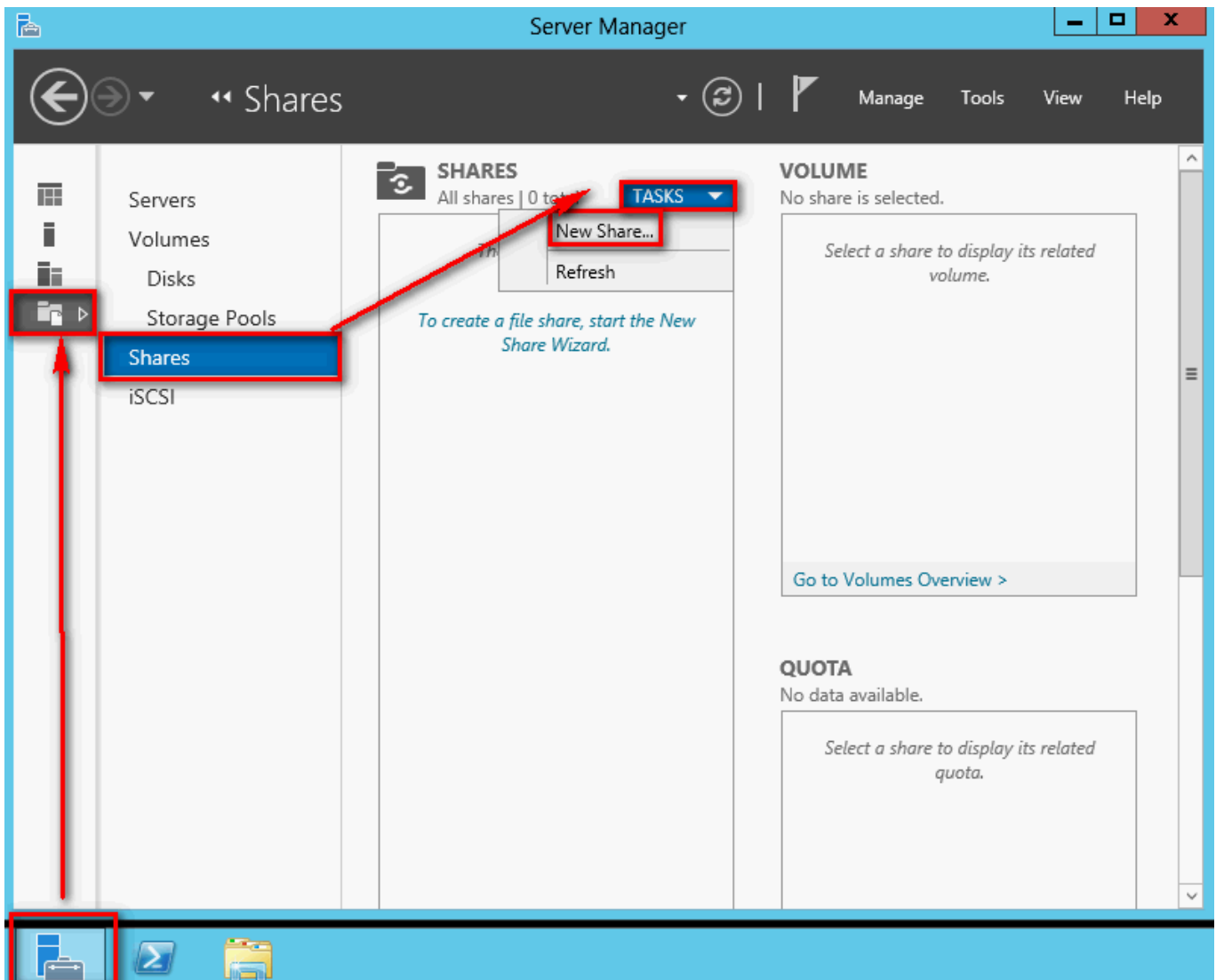
Note : If Windows 2012 Server does not run File server audit, we recommend not to audit object access, please skip steps 4.1(3) and 4.2, and only operate steps 4.1 (1), (2), (4), (5). This will help Windows avoid auditing unnecessary Object access security events. These unnecessary and redundant security events that are converted into syslog and

sent to N-Reporter will reduce its performance.

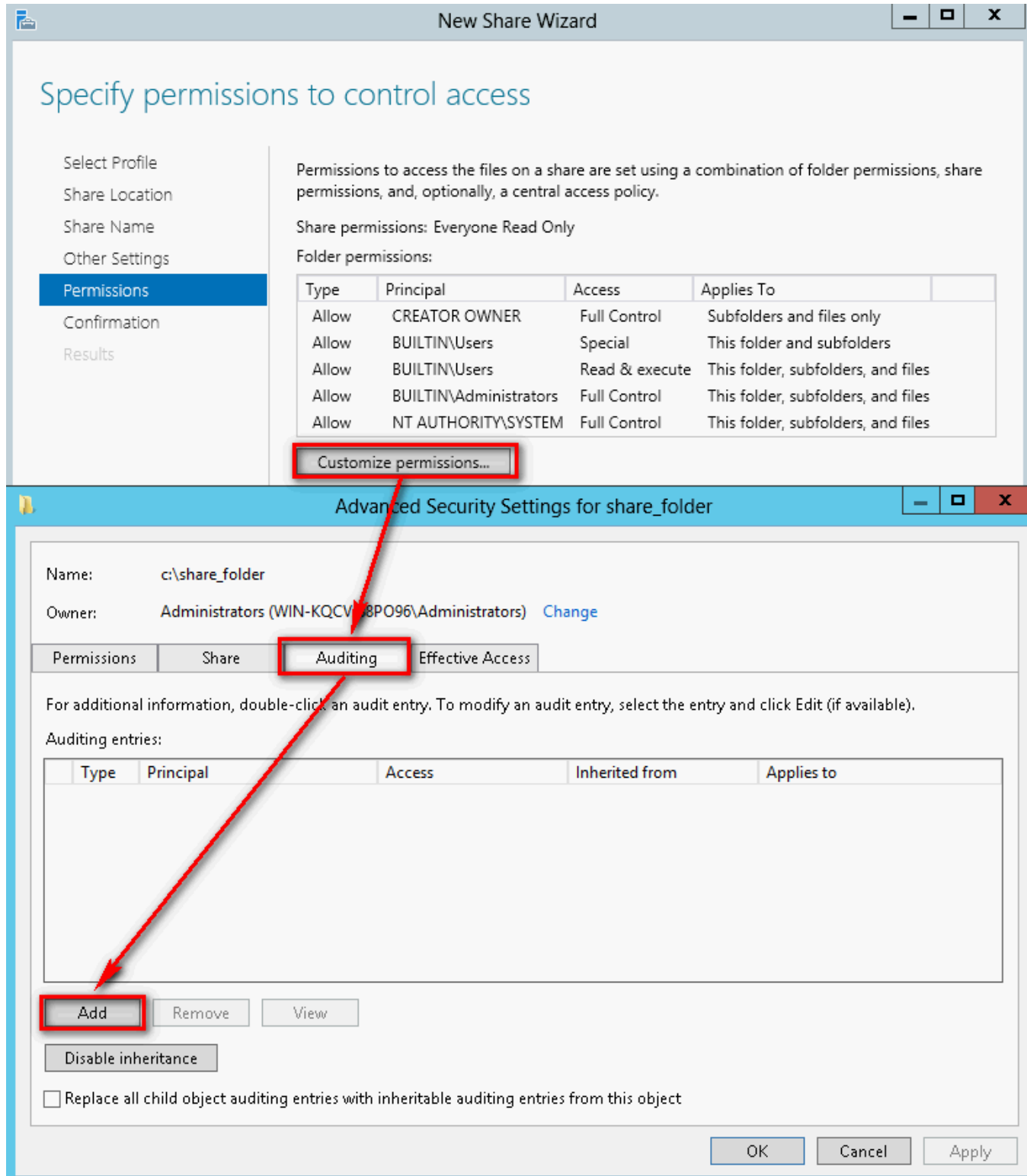
4.2 Setting up local shared folder authorization and audit policy

Set as follows :

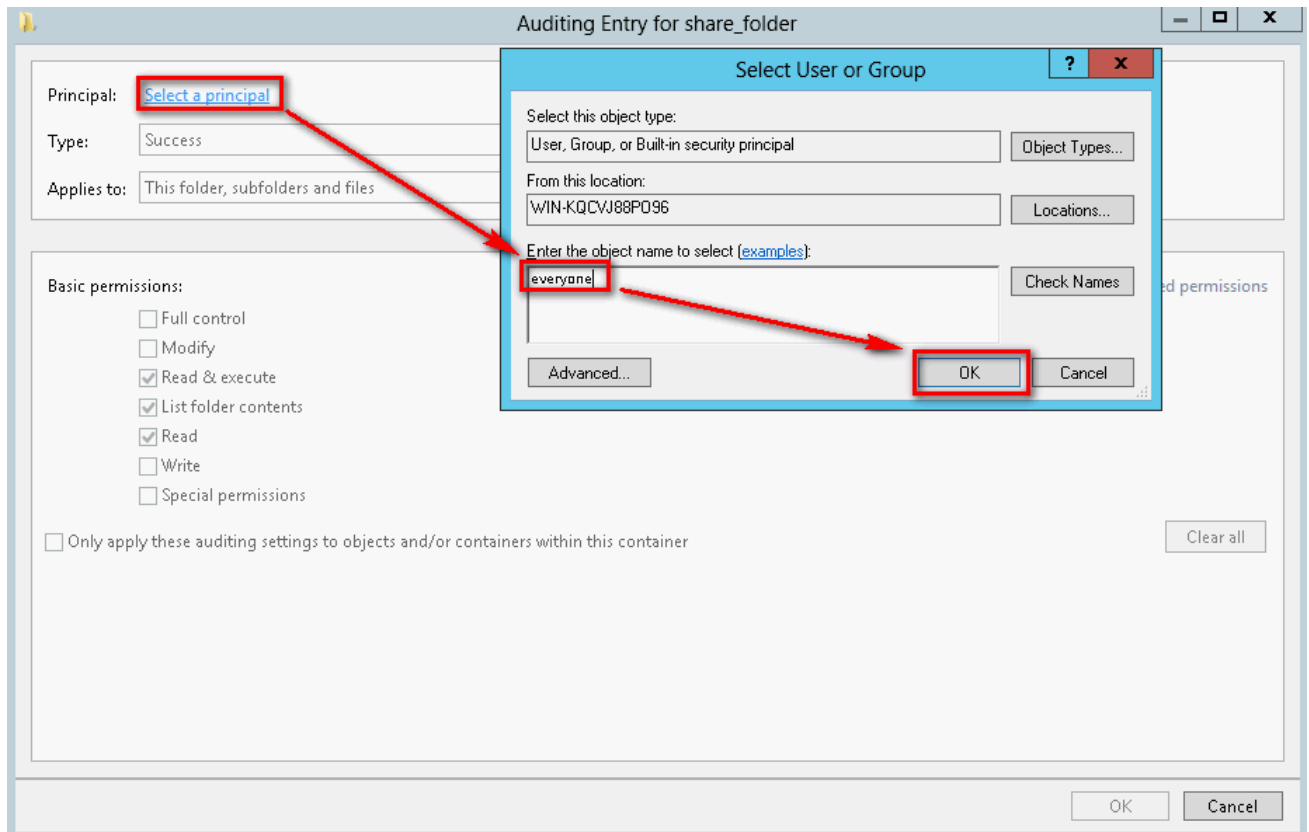
1. Click [Server Manager / File and Storage Services / Shares / TASKS / New Share...].



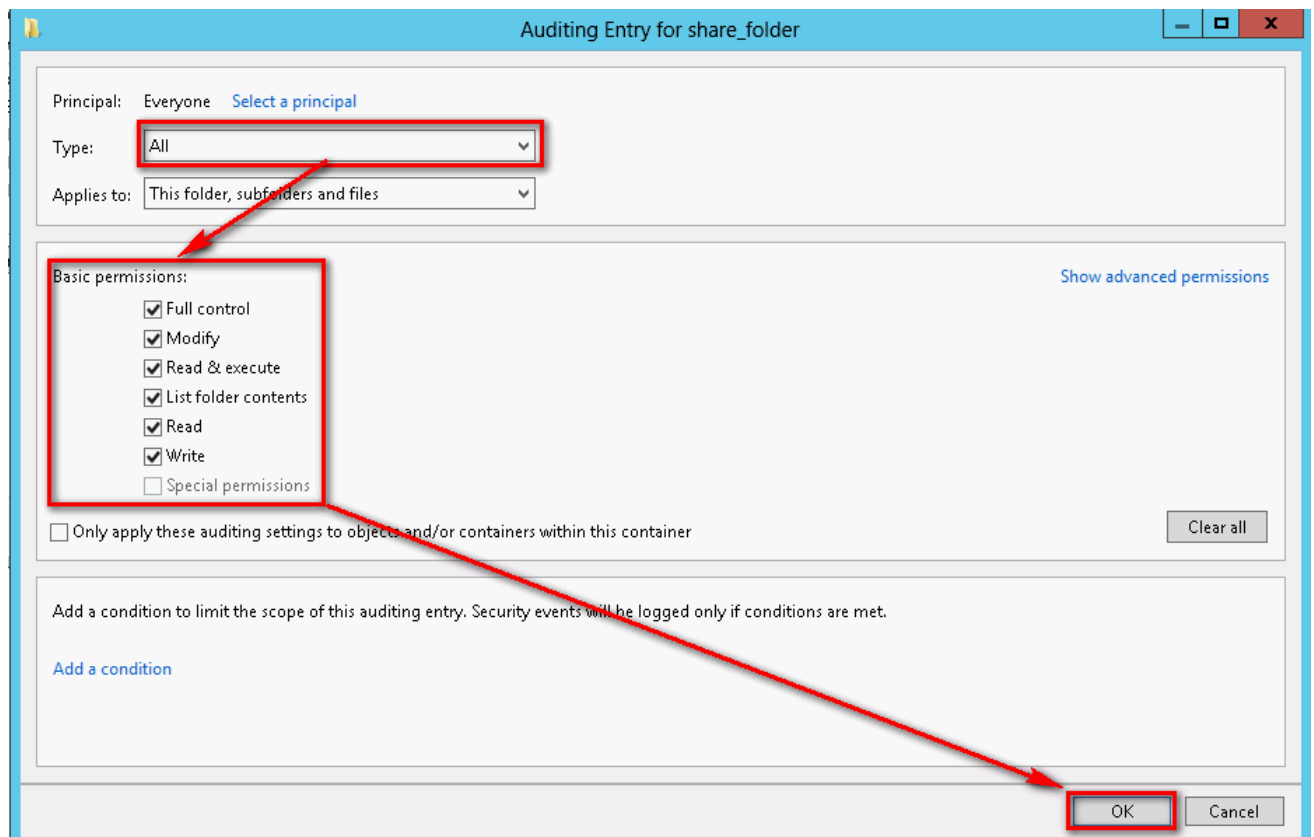
2. Click [SMB Share - Quick] → [Next].
3. Click [Type a custom path]. In this example we use " C:\share_folder " , then click [Next].
4. Enter share name, then click [Next].
5. Check [Enable access-based enumeration], click [Next].
6. Click [Customize permissions... / Auditing / Add].



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



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



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

Contact Information

N-Partner Company :

TEL: +886-4-23752865

FAX: +886-4-23757458

Technical Support :

Email: support@npartnertech.com

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

Sales Information :

Email: sales@npartnertech.com

