

# 10. Windows Log

LibreNMS

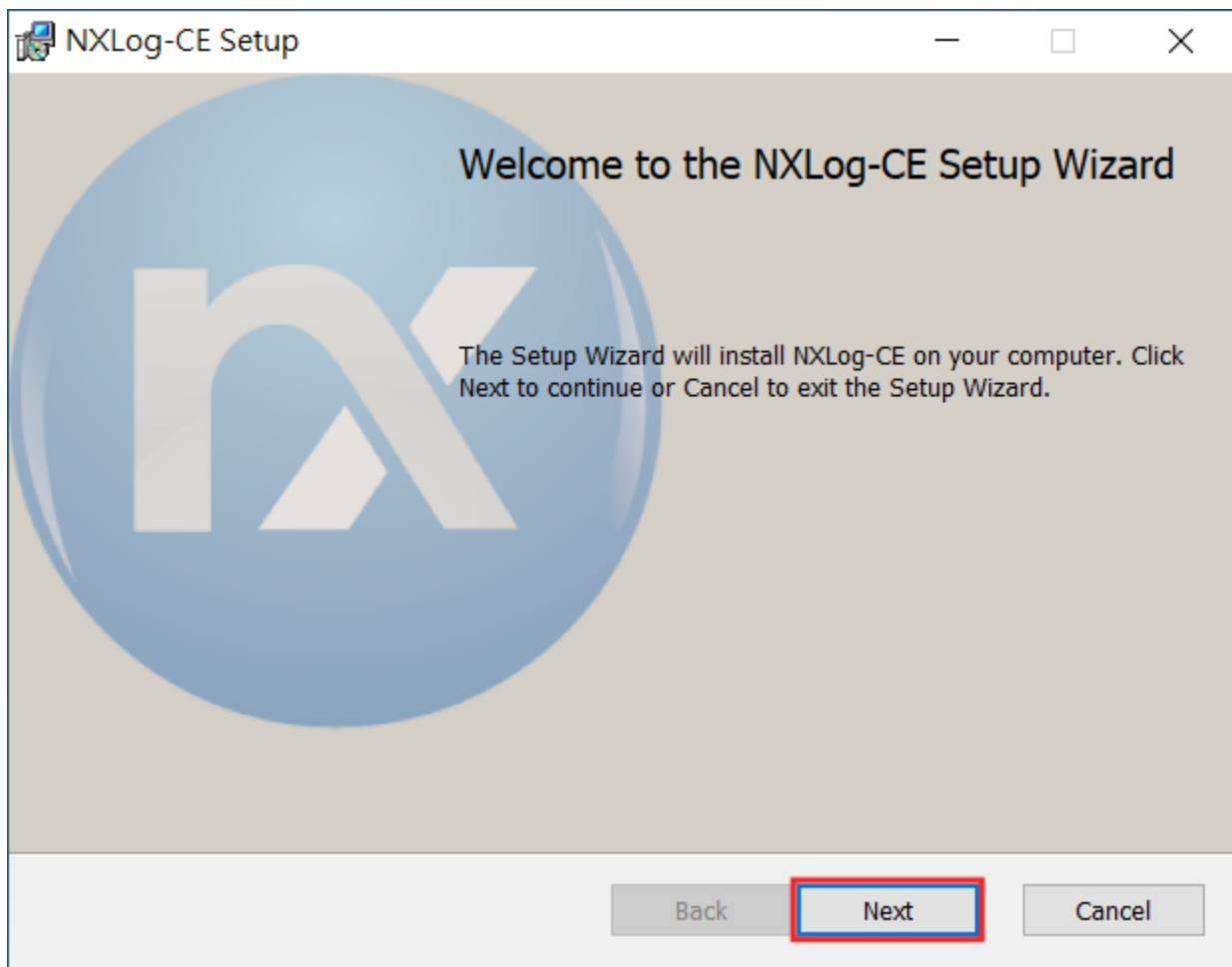
NXLog

[NXLog Community Edition](#)

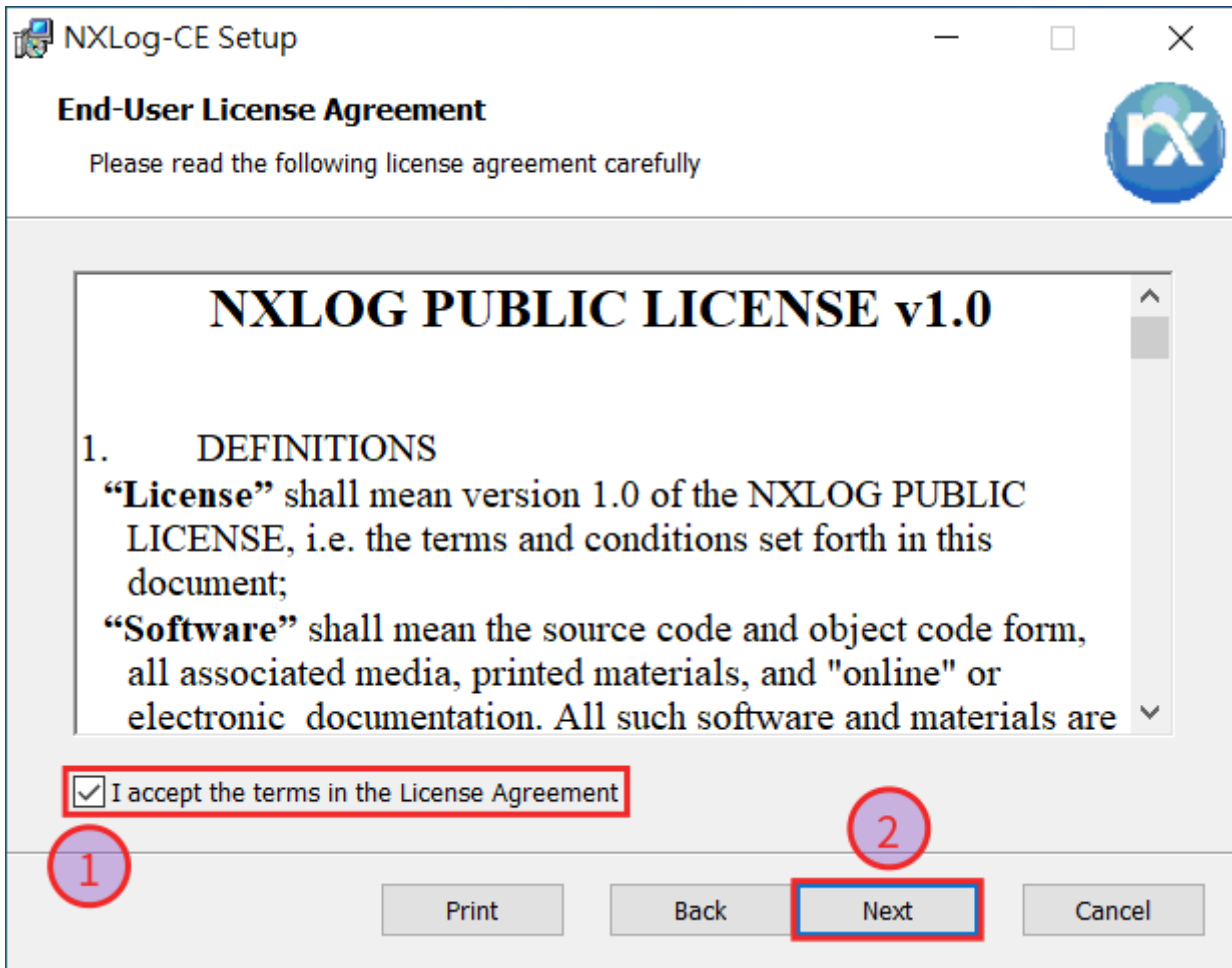
---

1. NXLog  
nxlog-ce-2.11.2190.msi

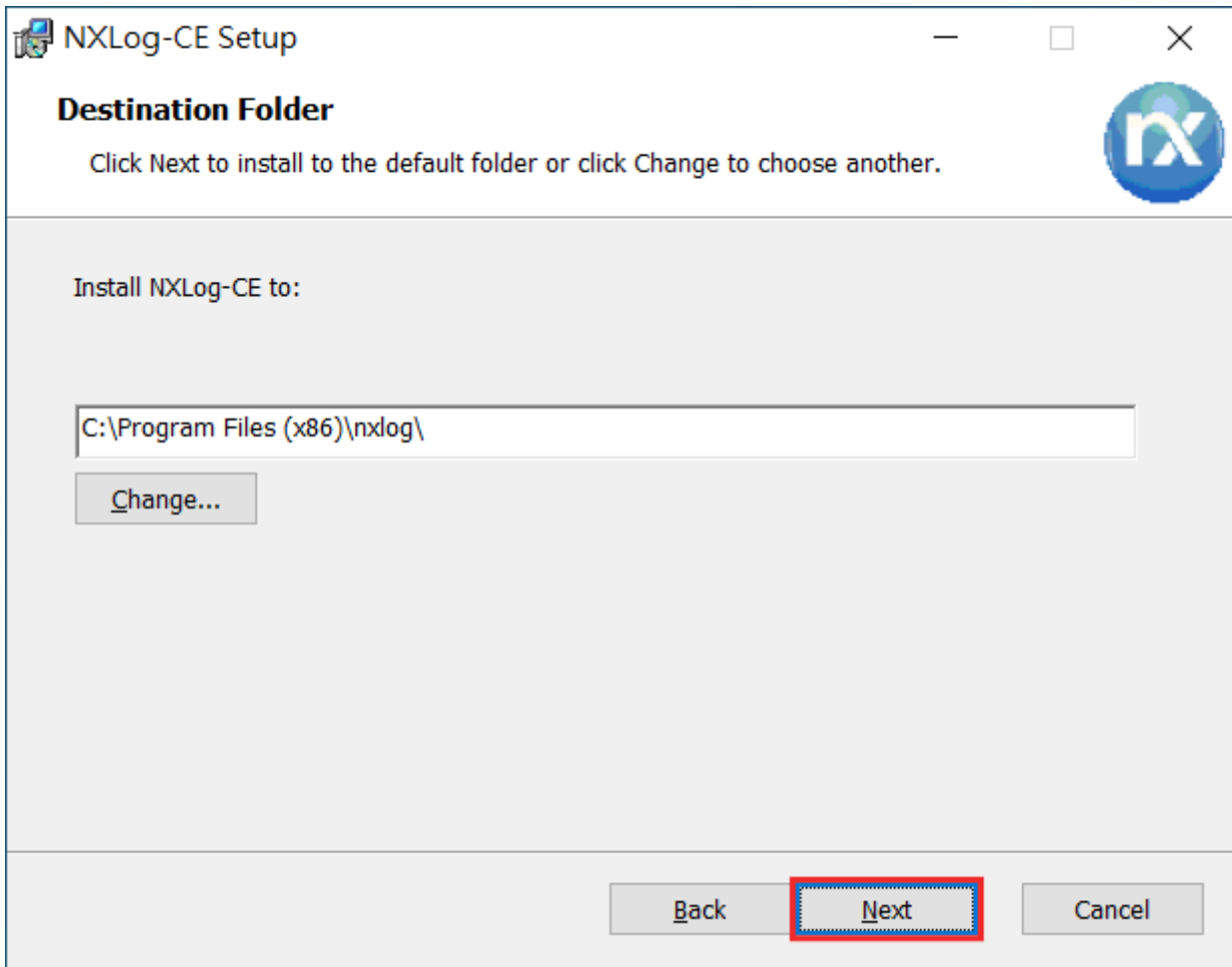
- Next



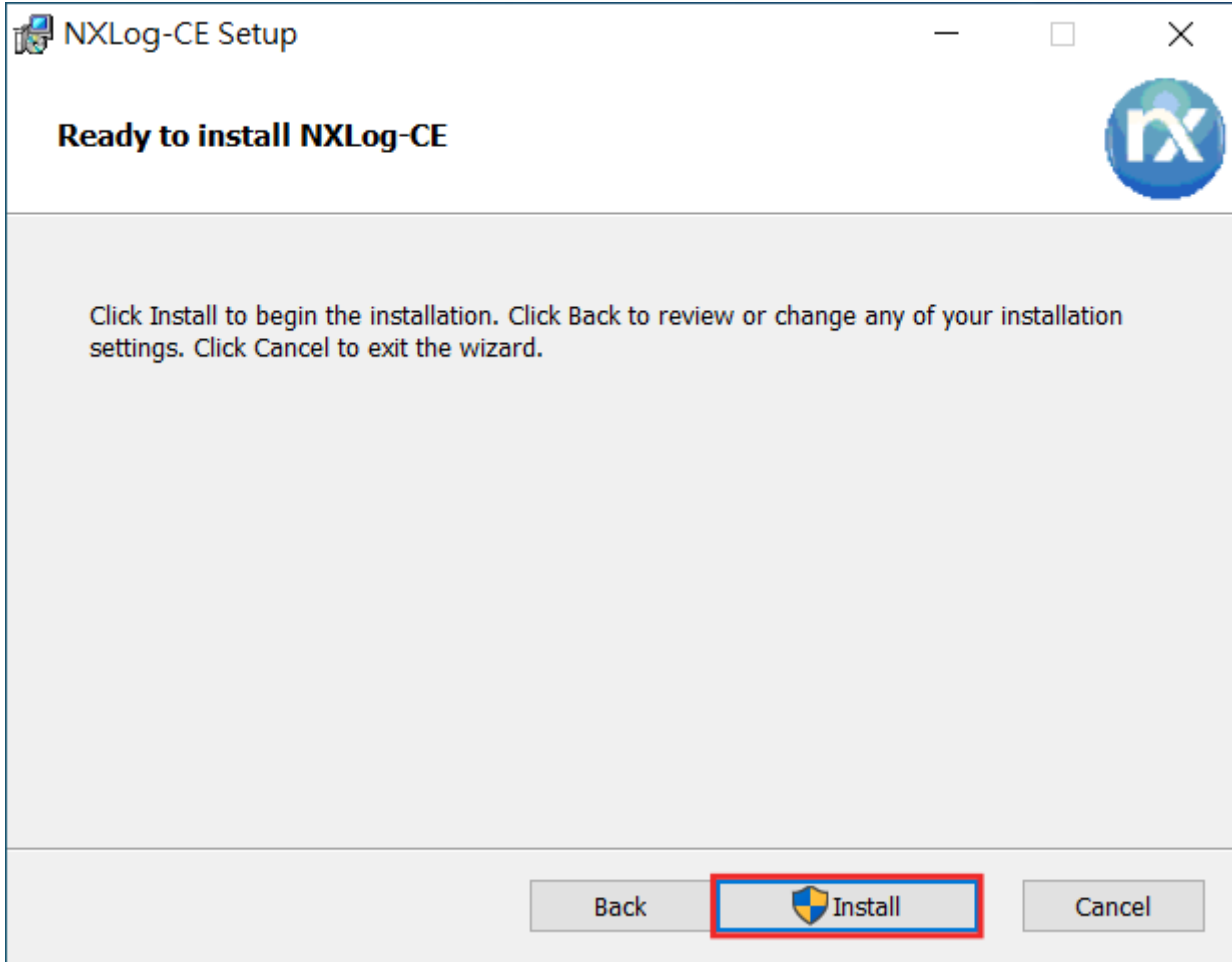
- I accept the terms in the License Agreement→ Next



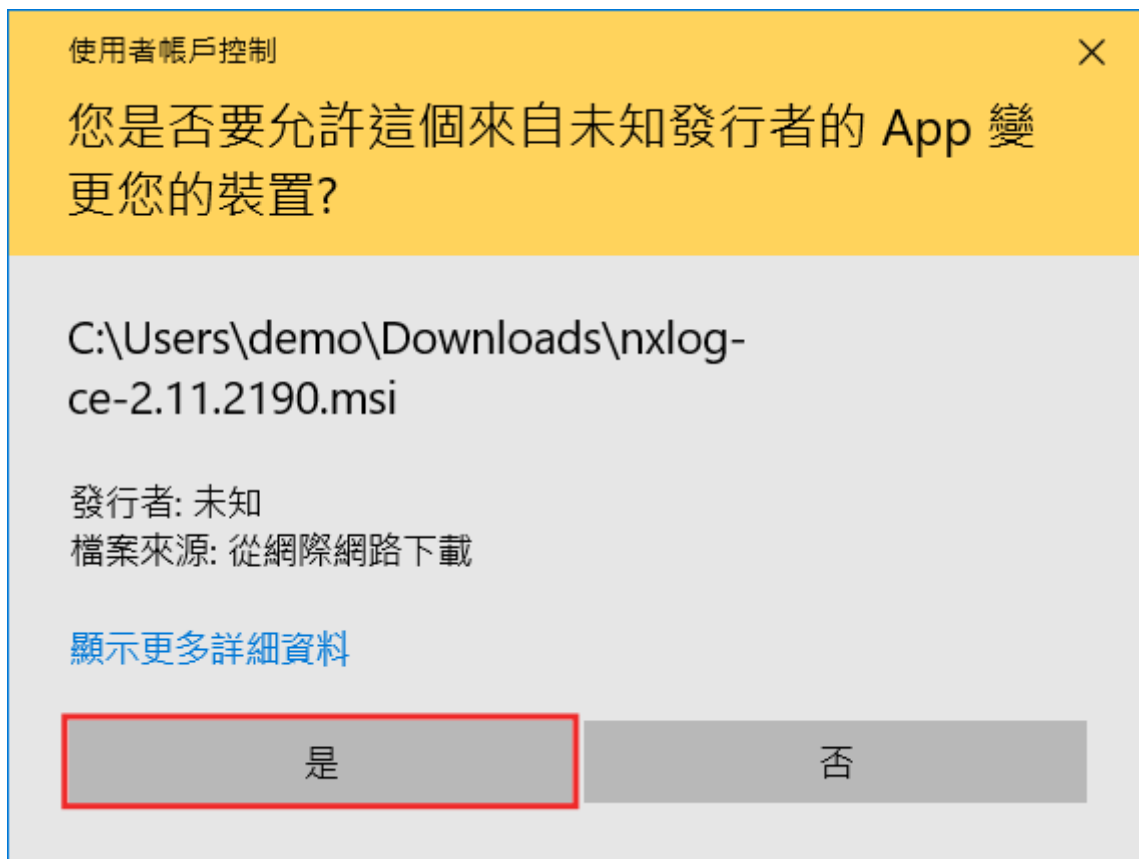
- Next



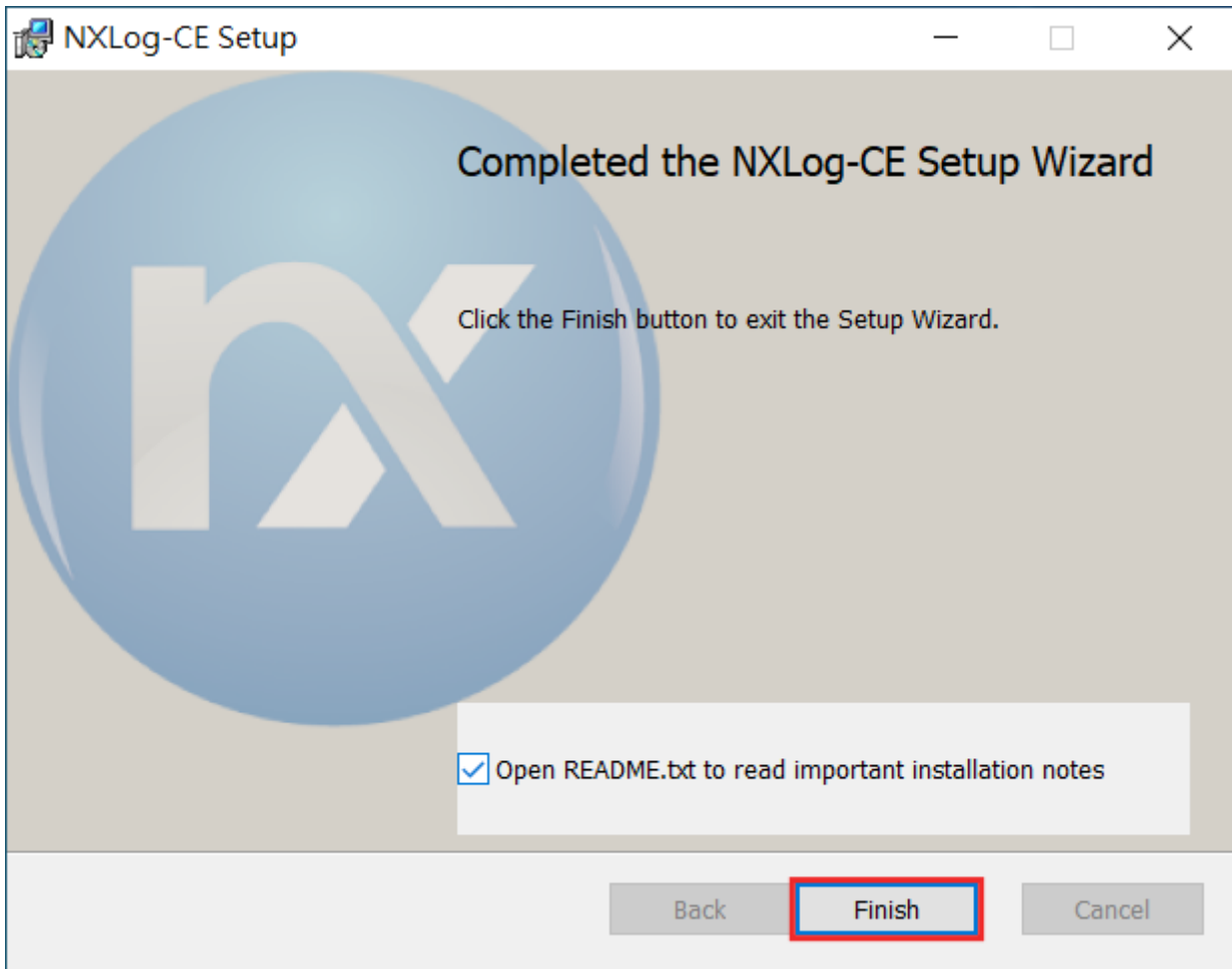
- Install



•



- Finish



---

2. nxlog.conf

c:\Program Files (x86)\nxlog\conf      nxlog.conf

※notepad++

※

- Windows Syslog

<Extension \_syslog>

Module xm\_syslog

</Extension>

<Input in>

# Vista ( ) im\_msvistalog

Module im\_msvistalog

# 2003 ( ) im\_mseventlog

# Module im\_mseventlog

</Input>

<Output out>

Module om\_udp

Host Libre

Port 514

Exec to\_syslog\_snare();

</Output>

<Route 1>

Path in => out

</Route>

\*C:\Program Files (x86)\nxlog\conf\nxlog.conf - Notepad++

檔案(F) 編輯(E) 搜尋(S) 檢視(V) 編碼(N) 語言(L) 設定(T) 工具(O) 巨集(M) 執行(R) 外掛(P) 視窗(W) ?

nxlog.conf

```
1 Panic Soft
2 #NoFreeOnExit TRUE
3
4 define ROOT      C:\Program Files (x86)\nxlog
5 define CERTDIR   %ROOT%\cert
6 define CONFDIR   %ROOT%\conf
7 define LOGDIR    %ROOT%\data
8 define LOGFILE   %LOGDIR%\nxlog.log
9 LogFile %LOGFILE%
10
11 Moduledir %ROOT%\modules
12 CacheDir  %ROOT%\data
13 Pidfile   %ROOT%\data\nxlog.pid
14 SpoolDir  %ROOT%\data
15
16 <Extension _syslog>
17     Module      xm_syslog
18 </Extension>
19
20 <Extension _charconv>
21     Module      xm_charconv
22     AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
23 </Extension>
24
25 <Extension _exec>
26     Module      xm_exec
27 </Extension>
28
29 <Extension _fileop>
30     Module      xm_fileop
31
32     # Check the size of our log file hourly, rotate if larger than 5MB
33     <Schedule>
34         Every    1 hour
35         Exec      if (file_exists('%LOGFILE%') and \
36                     (file_size('%LOGFILE%') >= 5M)) \
37                     file_cycle('%LOGFILE%', 8);
38     </Schedule>
```

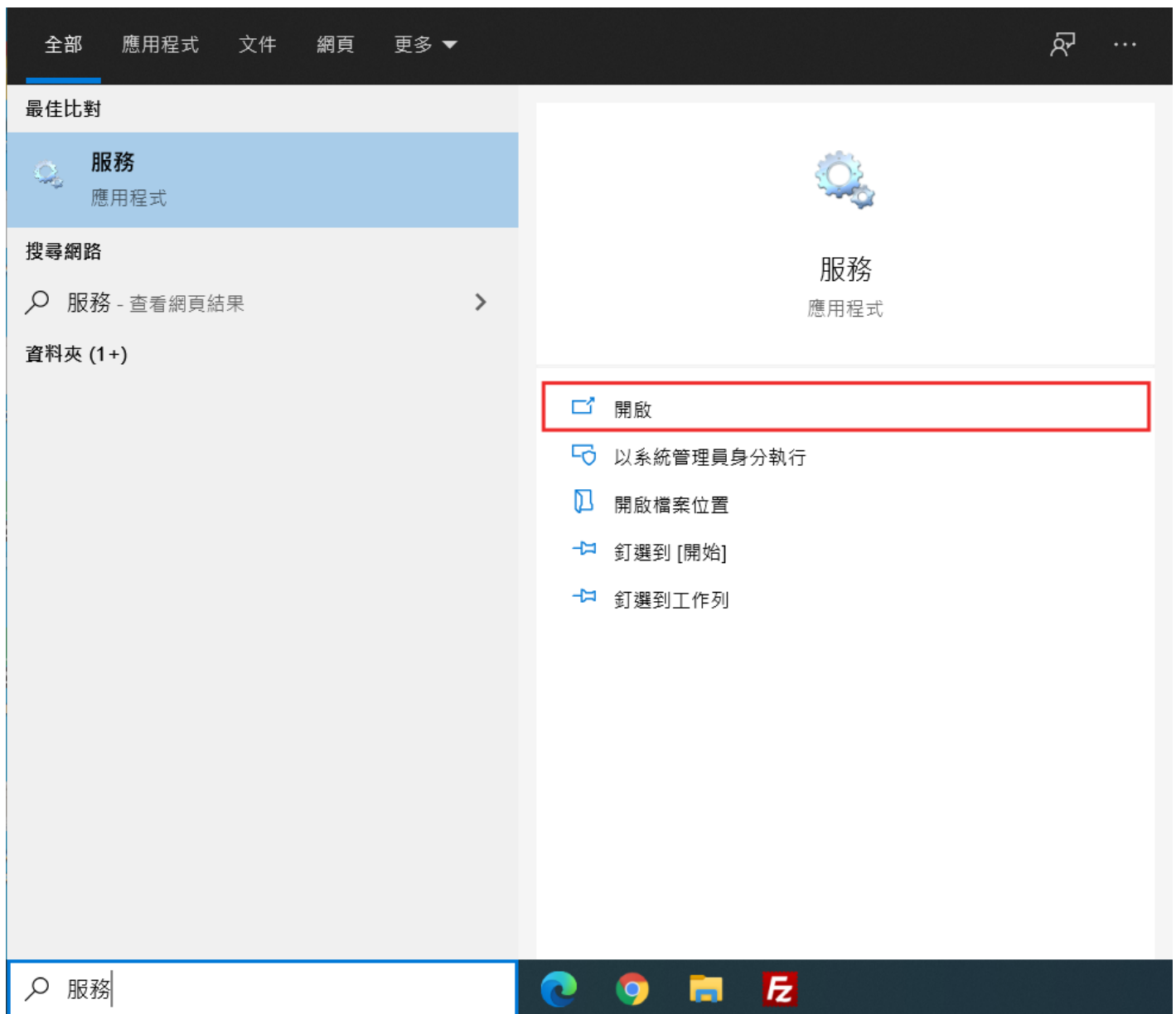
複製完成後  
請將此分隔現以下之程式碼完全覆蓋

Normal text file | length: 1,567 lines: 64 | Ln: 64 Col: 11 Pos: 1,568 | Windows (CR LF) UTF-8 INS

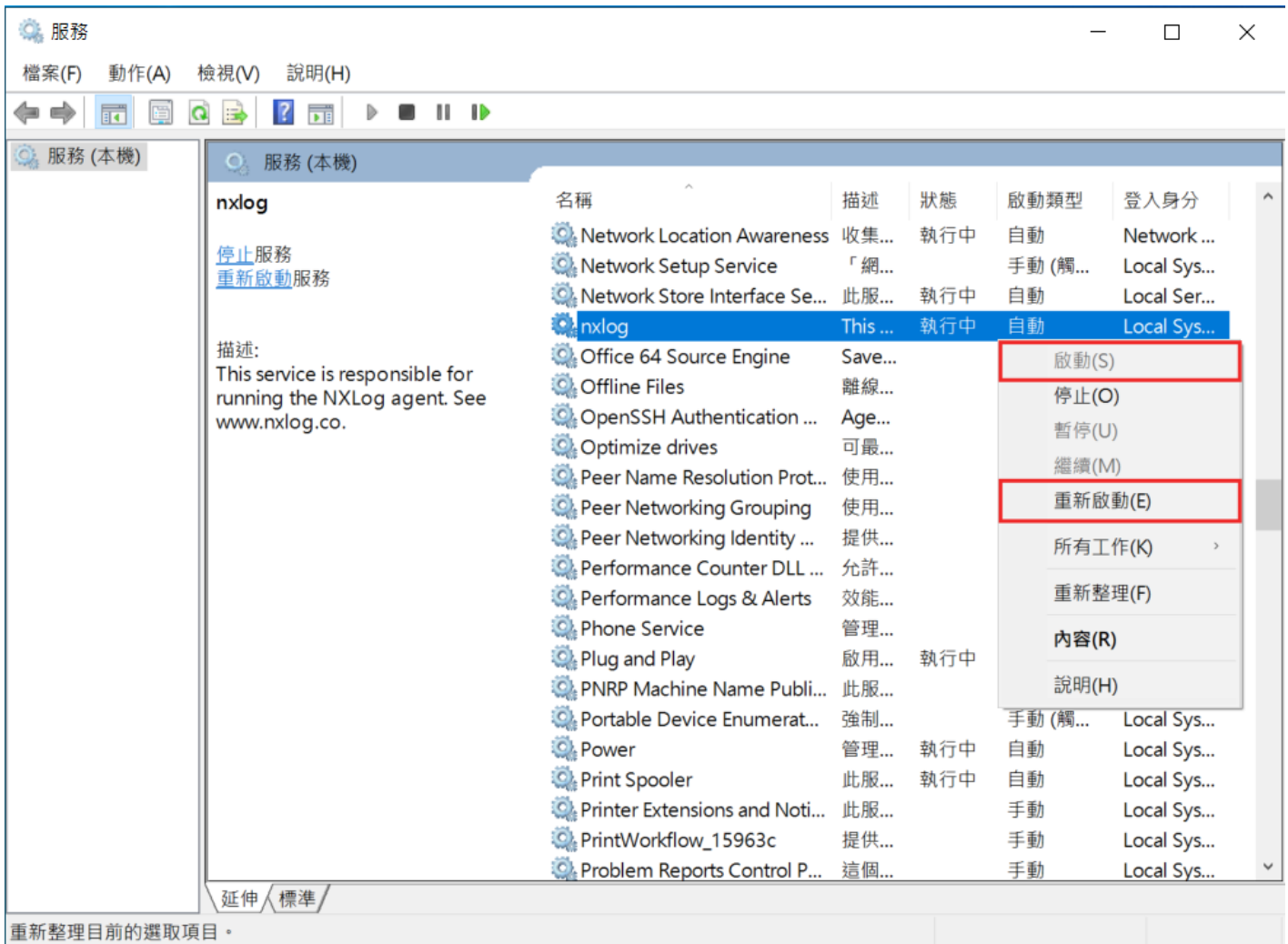
### 3. NXLog

- " "





- nxlog



## LibreNMS

Syslog

192.168.31.19x

All Programs

All Priorities

2021-11-25 14:55

2021-11-26 14:55

Filter

Q

Search

↺

50

≡

Timestamp	Level	Hostname	Program	Message	Priority
2021-11-26 14:51:27	info	192.168.31.19	MSWINEVENTLOG\011\011SYSTEM\011	Nov 26 14:51:12 2021\0117036\011Service Control Manager\011N\A\011N\A\011Information\011love-PC\011N\A\011\011Multimedia Class Scheduler 服務已進入 停止 狀態。 \0113379	info
2021-11-26 14:50:55	info	192.168.31.19	MSWINEVENTLOG\011\011SYSTEM\011	Nov 26 14:50:39 2021\0117036\011Service Control Manager\011N\A\011N\A\011Information\011love-PC\011N\A\011\011WinHTTP Web Proxy Auto-Discovery Service 服務已進入 停止 狀態。 \0113378	info

«

<

1

>

»

Showing 1 to 2 of 2 entries

