4. NXLog Windows

Graylog NXLog

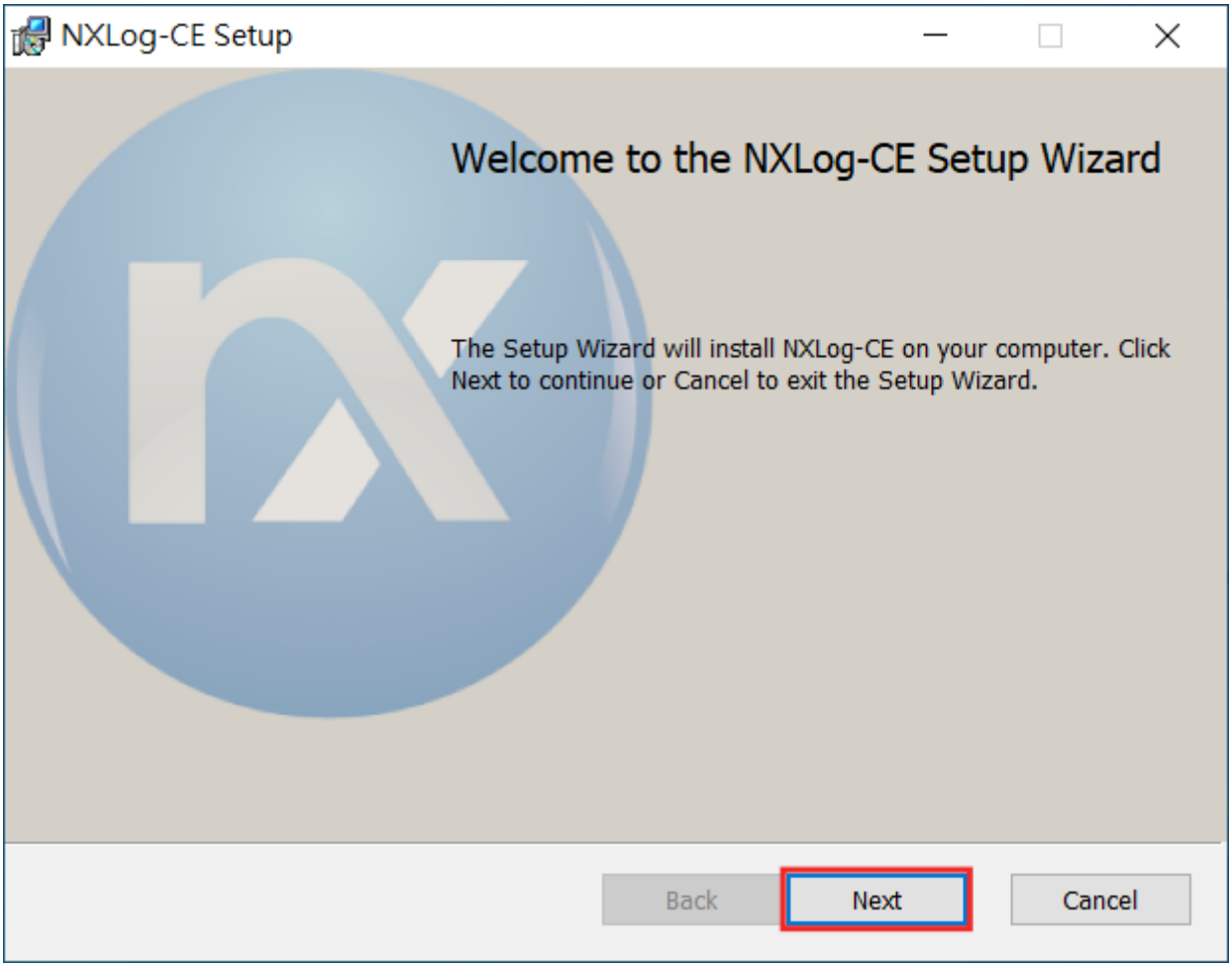
NXLog Community Edition

---

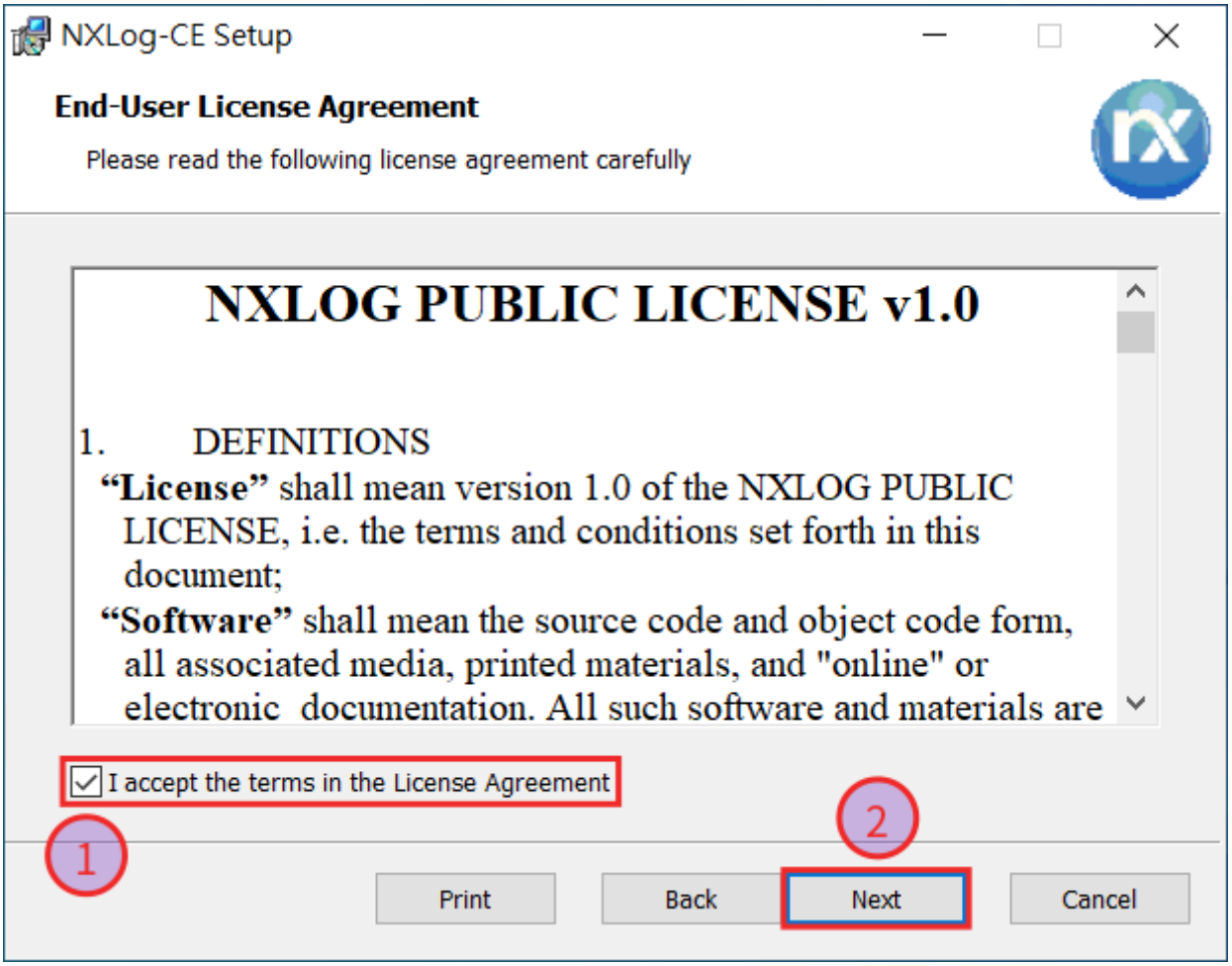
1. NXLog

   nxlog-ce-2.11.2190.msi

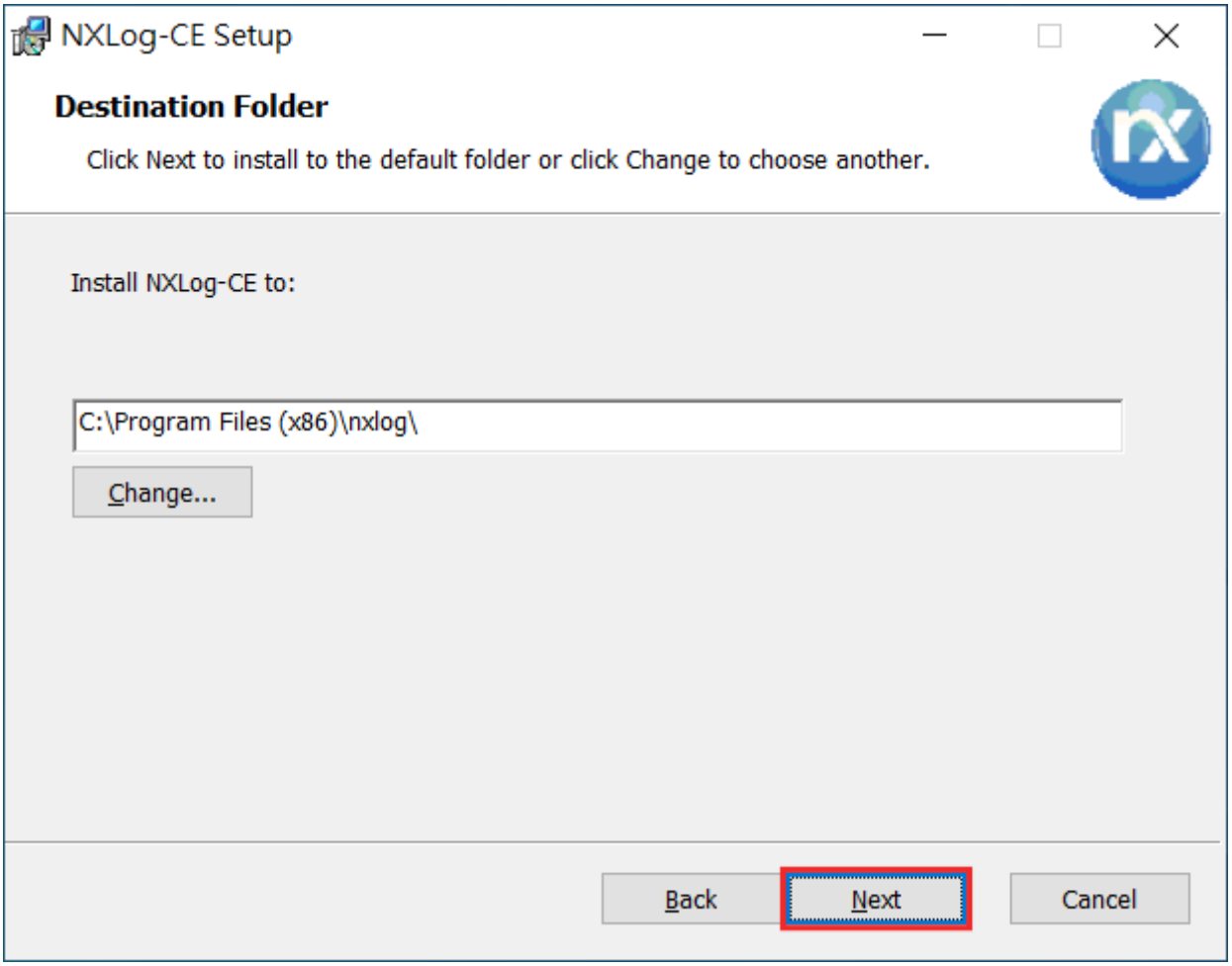
- Next



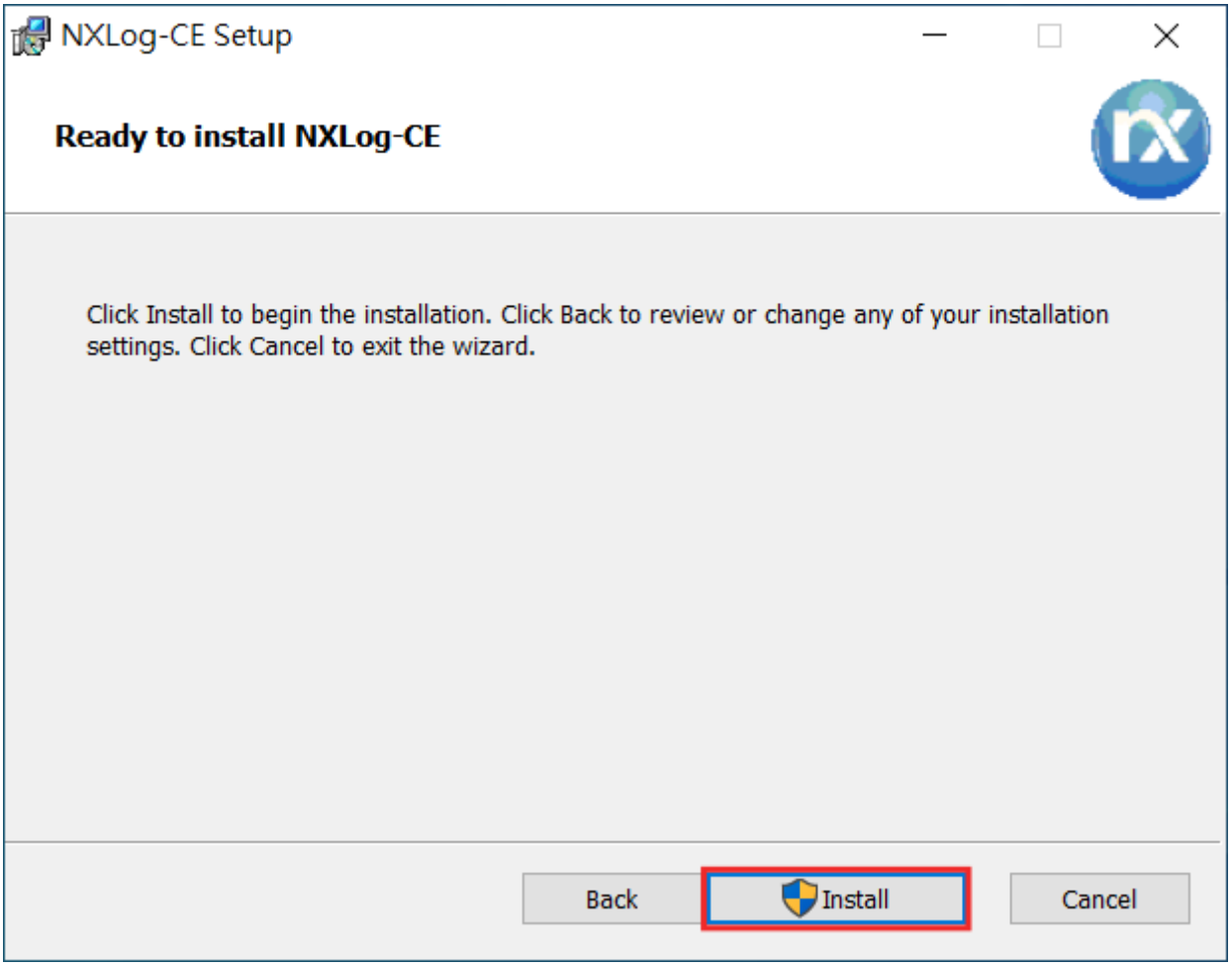
- I accept the terms in the License Agreement→ Next


NXLog-CE Setup
End-User License Agreement
Please read the following license agreement carefully
NXLOG PUBLIC LICENSE v1.0
1. DEFINITIONS
"License" shall mean version 1.0 of the NXLOG PUBLIC LICENSE, i.e. the terms and conditions set forth in this document;
"Software" shall mean the source code and object code form, all associated media, printed materials, and "online" or electronic documentation. All such software and materials are
I accept the terms in the License Agreement
1
2
Print
Back
Next
Cancel

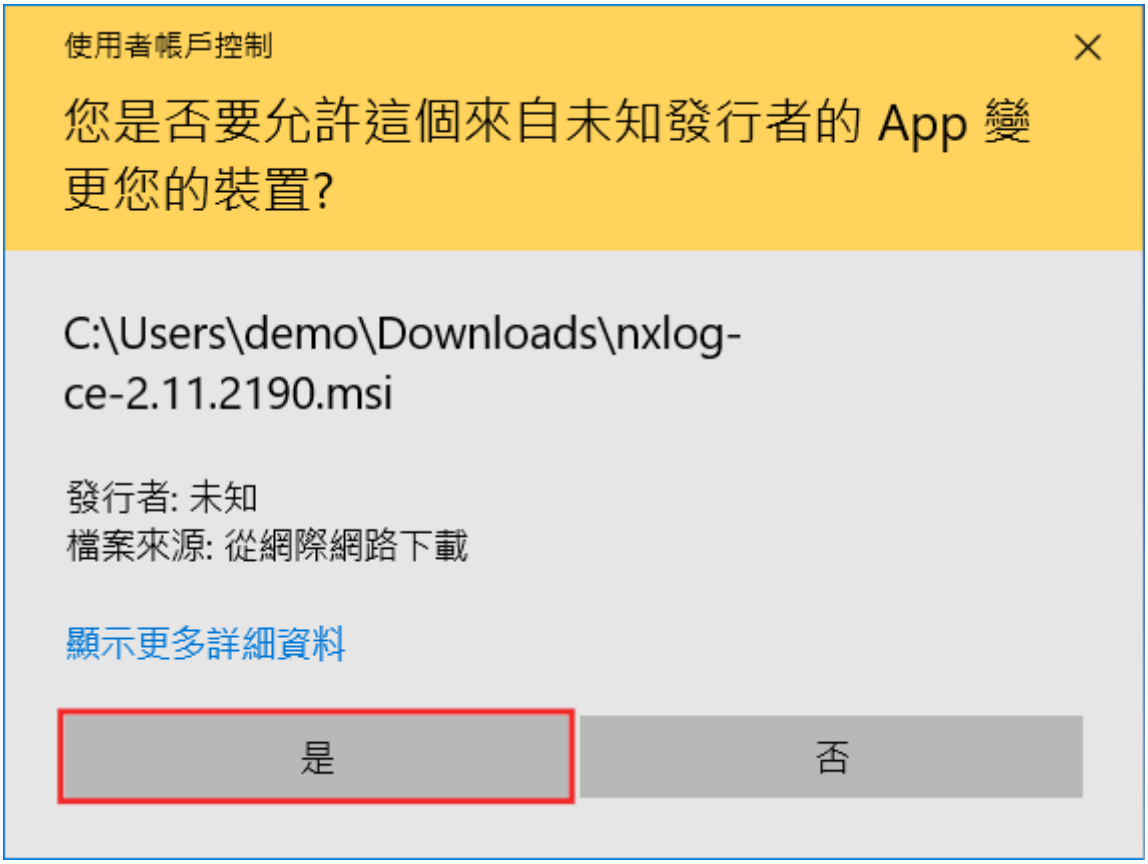
- Next


NXLog-CE Setup
Destination Folder
Click Next to install to the default folder or click Change to choose another.
Install NXLog-CE to:
C:\Program Files (x86)\nxlog\
Change...
Back
Next
Cancel

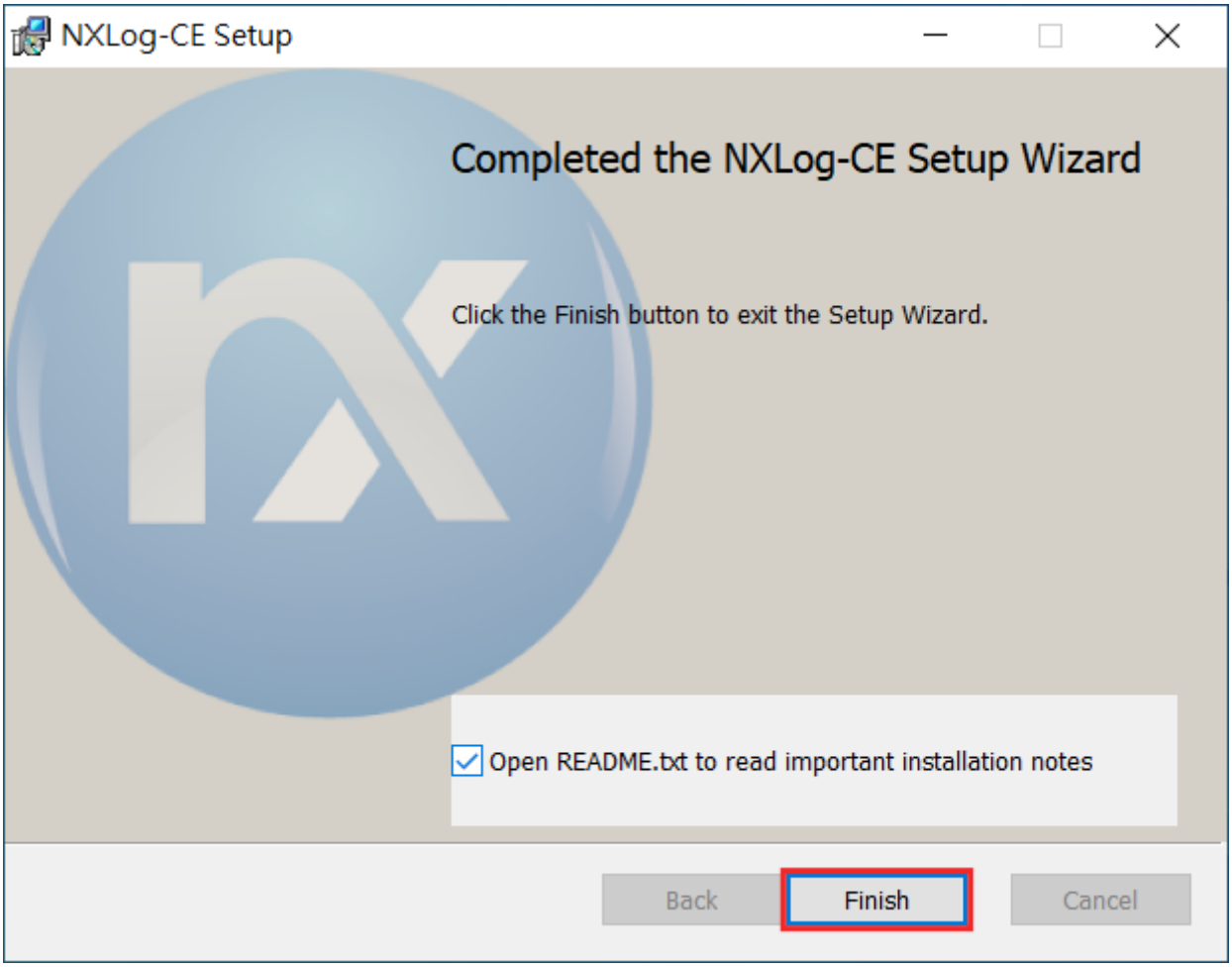
- Install


NXLog-CE Setup
Ready to install NXLog-CE
Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Back
Install
Cancel

-


使用者帳戶控制
您是否要允許這個來自未知發行者的 App 變更您的裝置?
C:\Users\demo\Downloads\nxlog-ce-2.11.2190.msi
發行者: 未知
檔案來源: 從網際網路下載
顯示更多詳細資料
是
否

- Finish



2. nxlog.conf

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

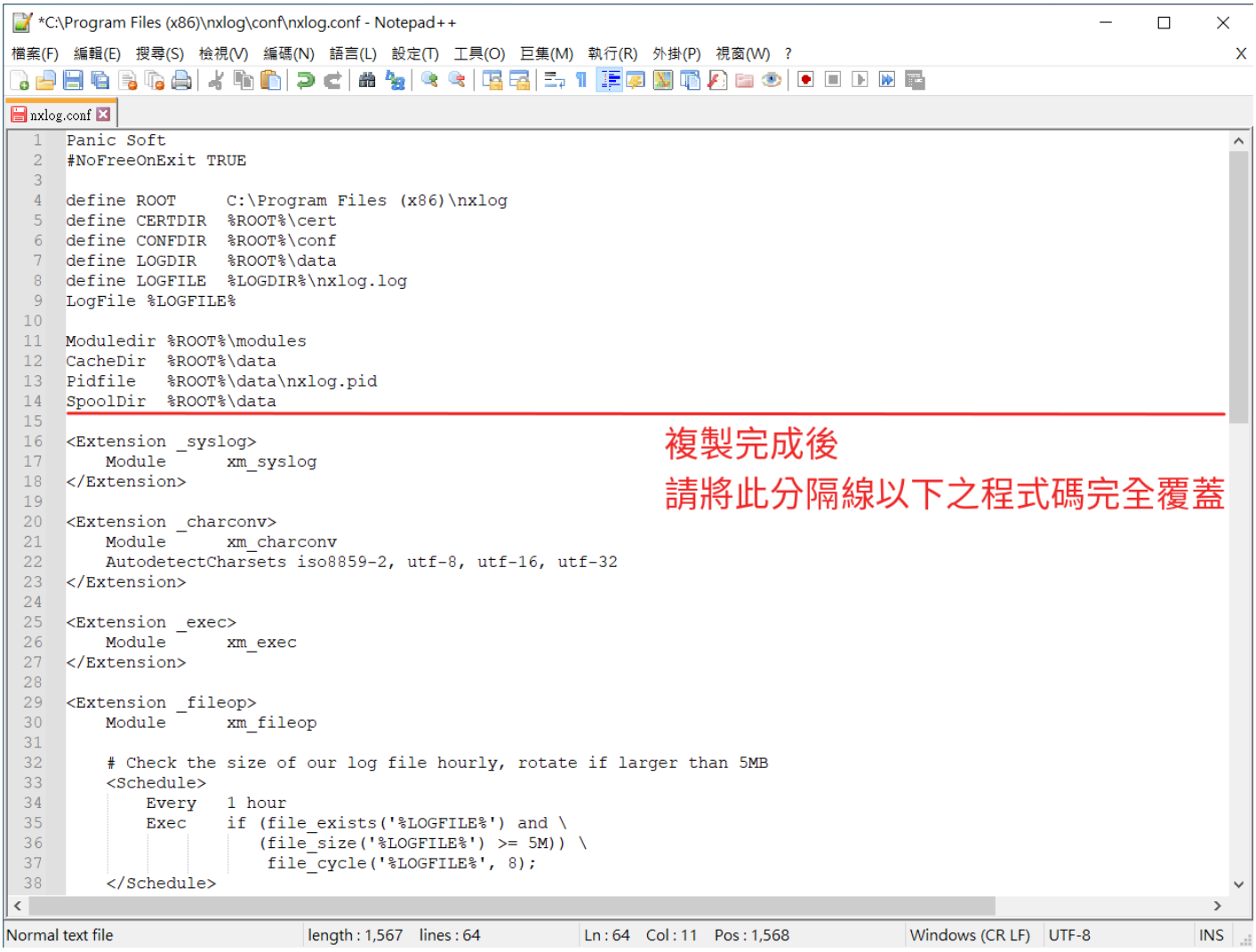
※notepad++ ※

- 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 [redacted]Gra
        Port 514
        Exec to_syslog_snare();
</Output>

<Route 1>
        Path in => out
</Route>
```

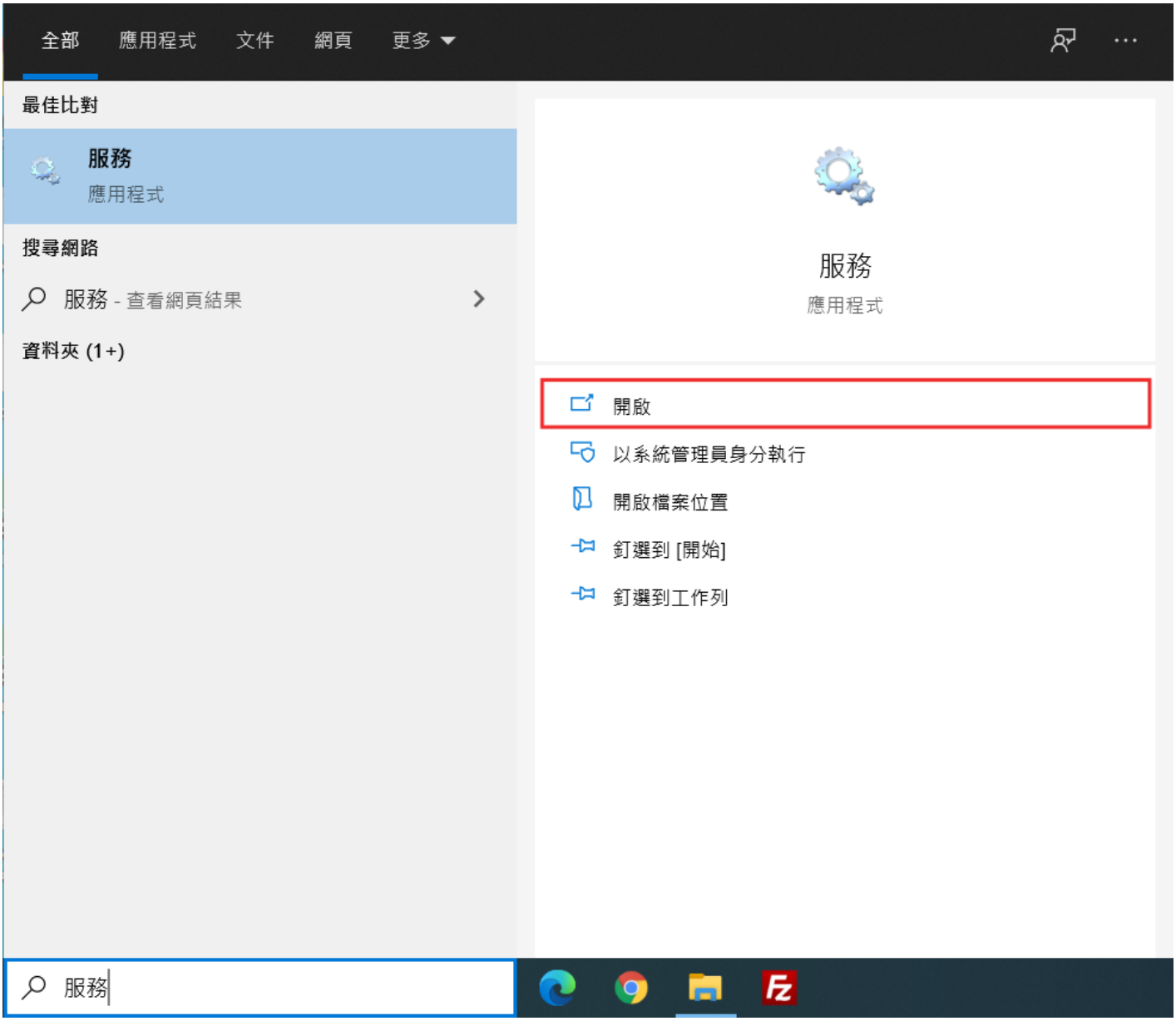
- WIndows Graylog

```
<Extension _syslog>
	Module xm_gelf
</Extension>

<Input in>
	# Vista (  )		im_msvistalog
	Module im_msvistalog

	# 2003 (  )		im_mseventlog
	# Module im_mseventlog
</Input>

<Output out>
	Module om_udp
	Host [redacted]Gra
	Port 12201
	OutputType GELF
</Output>

<Route 1>
	Path in => out
</Route>
```

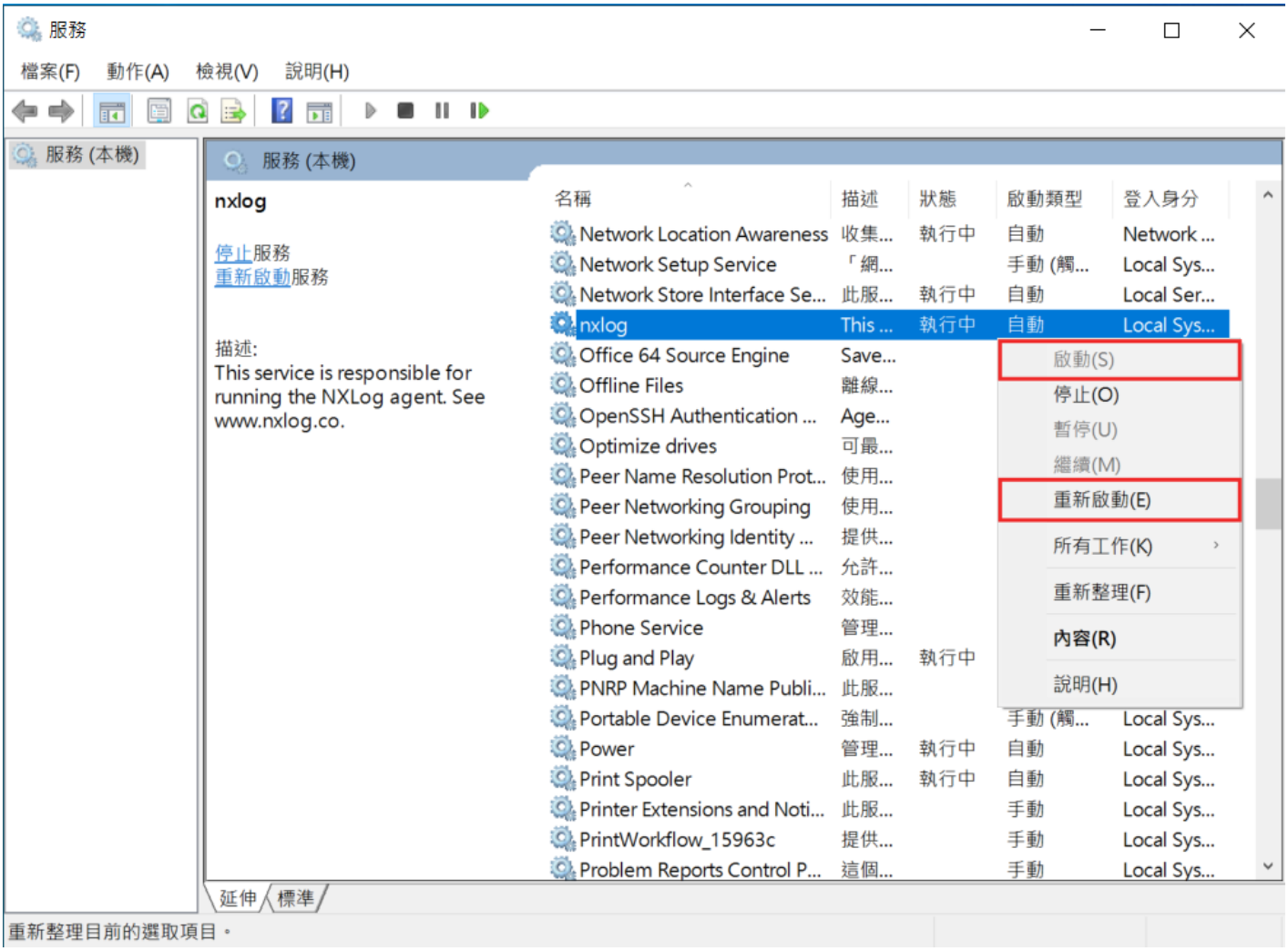

*C:\Program Files (x86)\nxlog\conf\nxlog.conf - Notepad++
檔案(F) 編輯(E) 搜尋(S) 檢視(V) 編碼(N) 語言(L) 設定(T) 工具(O) 巨集(M) 執行(R) 外掛(P) 視窗(W) ?
nxlog.conf
Panic Soft
#NoFreeOnExit TRUE
define ROOT C:\Program Files (x86)\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define LOGFILE %LOGDIR%\nxlog.log
LogFile %LOGFILE%
Moduledir %ROOT%\modules
CacheDir %ROOT%\data
Pidfile %ROOT%\data\nxlog.pid
SpoolDir %ROOT%\data
<Extension _syslog>
Module xm_syslog
</Extension>
<Extension _charconv>
Module xm_charconv
AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
</Extension>
<Extension _exec>
Module xm_exec
</Extension>
<Extension _fileop>
Module xm_fileop
Check the size of our log file hourly, rotate if larger than 5MB
<Schedule>
Every 1 hour
Exec if (file_exists('%LOGFILE%') and \
(file_size('%LOGFILE%') >= 5M)) \
file_cycle('%LOGFILE%', 8);
</Schedule>
複製完成後
請將此分隔線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

- " "


全部
應用程式
文件
網頁
更多
最佳比對
服務
應用程式
搜尋網路
服務 - 查看網頁結果
資料夾 (1+)
服務
應用程式
開啟
以系統管理員身分執行
開啟檔案位置
釘選到 [開始]
釘選到工作列
服務

- nxlog



Graylog

Revision #38
Created 26 October 2021 00:41:46 by Epower
Updated 26 November 2021 07:24:11 by Epower