EPower Graylog

EPower Graylog

1. Graylog

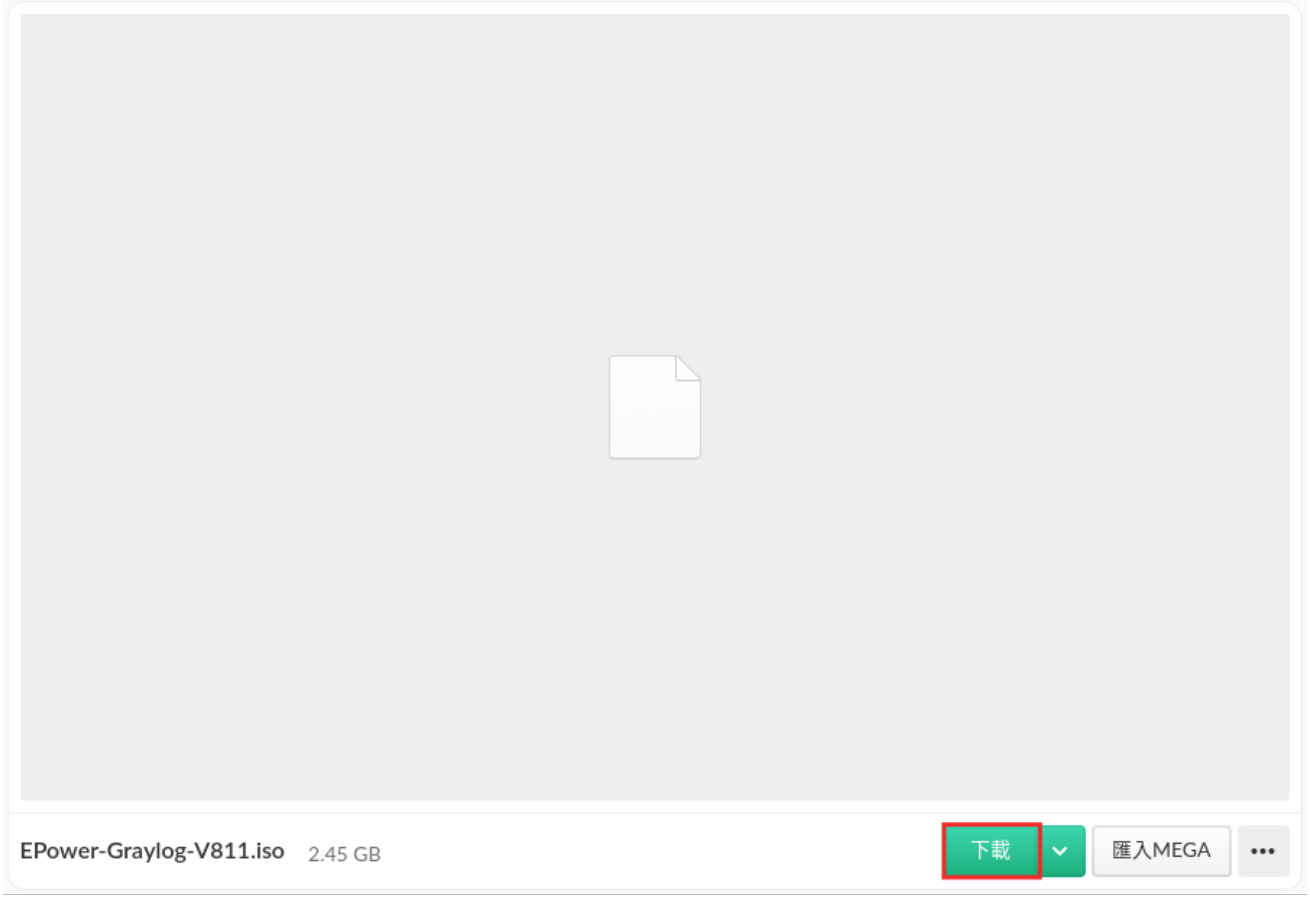
EPower-Graylog-V811.iso

※USB ※

---

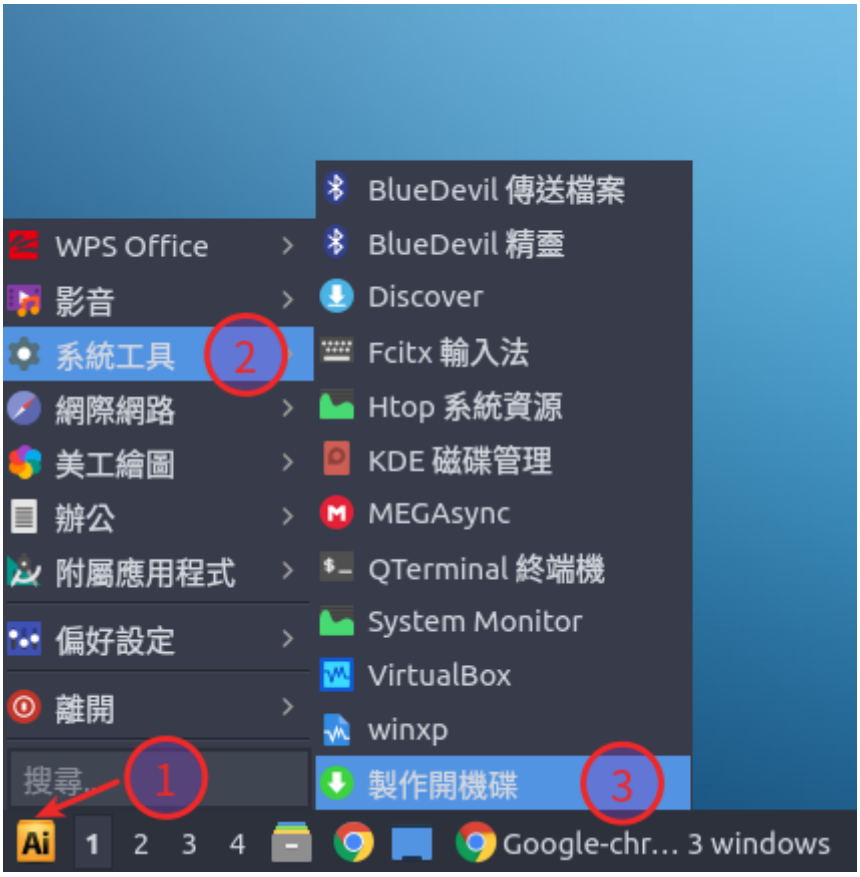
1. iso

EPower-Graylog-V811.iso

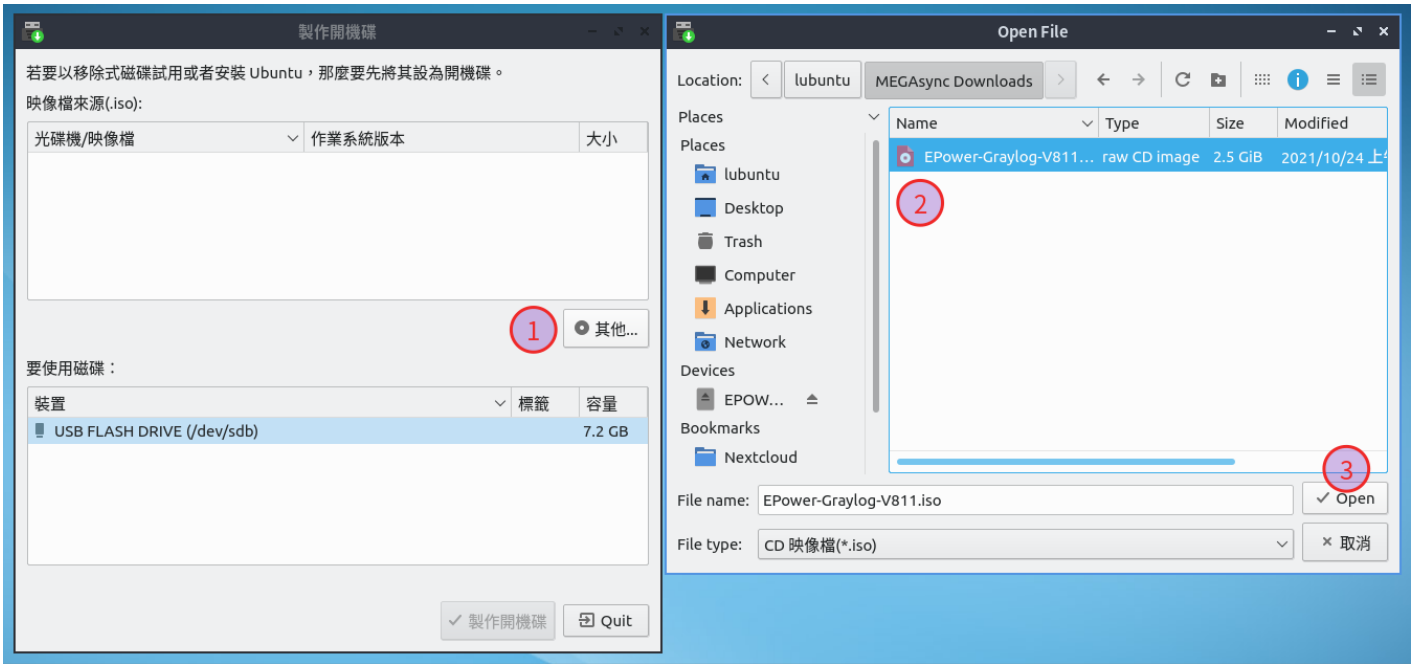


2.

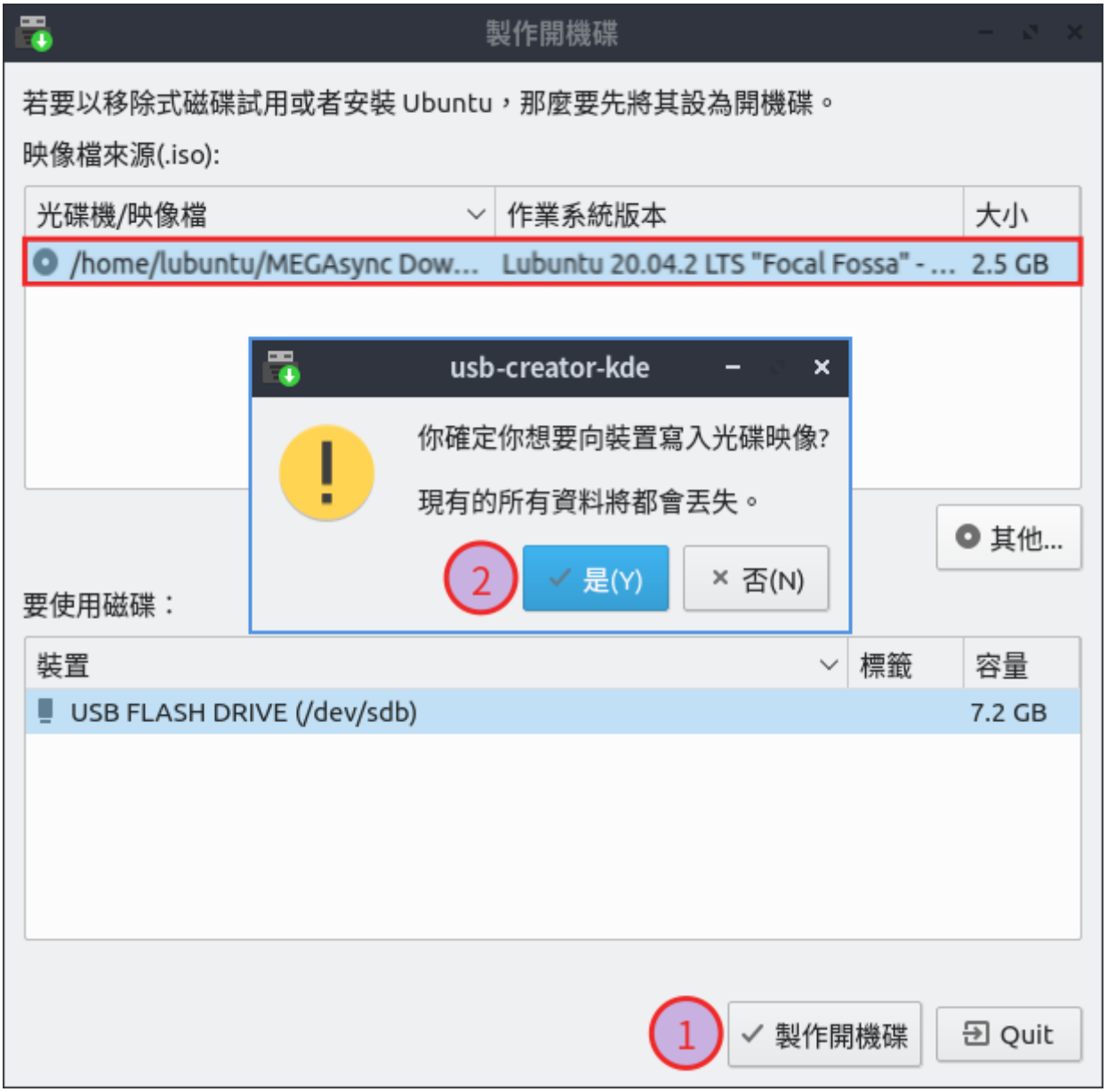
- Ai➔ ➔


BlueDevil 傳送檔案
BlueDevil 精靈
Discover
Fcitx 輸入法
Htop 系統資源
KDE 磁碟管理
MEGAsync
QTerminal 終端機
System Monitor
VirtualBox
winxp
製作開機碟
WPS Office
影音
系統工具
網際網路
美工繪圖
辦公
附屬應用程式
偏好設定
離開
搜尋...
1
2
3
Google-chr... 3 windows

- → → Open


製作開機碟
若要以移除式磁碟試用或者安裝 Ubuntu，那麼要先將其設為開機碟。
映像檔來源(.iso):
光碟機/映像檔
作業系統版本
大小
其他...
要使用磁碟：
裝置
標籤
容量
USB FLASH DRIVE (/dev/sdb)
7.2 GB
製作開機碟
Quit
Open File
Location:
lubuntu
MEGAsync Downloads
Places
Desktop
Trash
Computer
Applications
Network
Devices
EPOW...
Bookmarks
Nextcloud
Name
Type
Size
Modified
EPower-Graylog-V811...
raw CD image
2.5 GiB
File name:
EPower-Graylog-V811.iso
File type:
CD 映像檔(*.iso)
Open
取消
1
2
3

- " "→


製作開機碟
若要以移除式磁碟試用或者安裝 Ubuntu，那麼要先將其設為開機碟。
映像檔來源(.iso):
光碟機/映像檔
作業系統版本
大小
/home/lubuntu/MEGAsync Dow...
Lubuntu 20.04.2 LTS "Focal Fossa" - ...
2.5 GB
usb-creator-kde
你確定你想要向裝置寫入光碟映像?
現有的所有資料將都會丟失。
2
是(Y)
否(N)
其他...
要使用磁碟：
裝置
標籤
容量
USB FLASH DRIVE (/dev/sdb)
7.2 GB
1
製作開機碟
Quit


安裝中
正在寫入磁碟映像檔...
8%
取消

2. Graylog

Graylog

※ Graylog ※

---

1. Graylog

EPSR

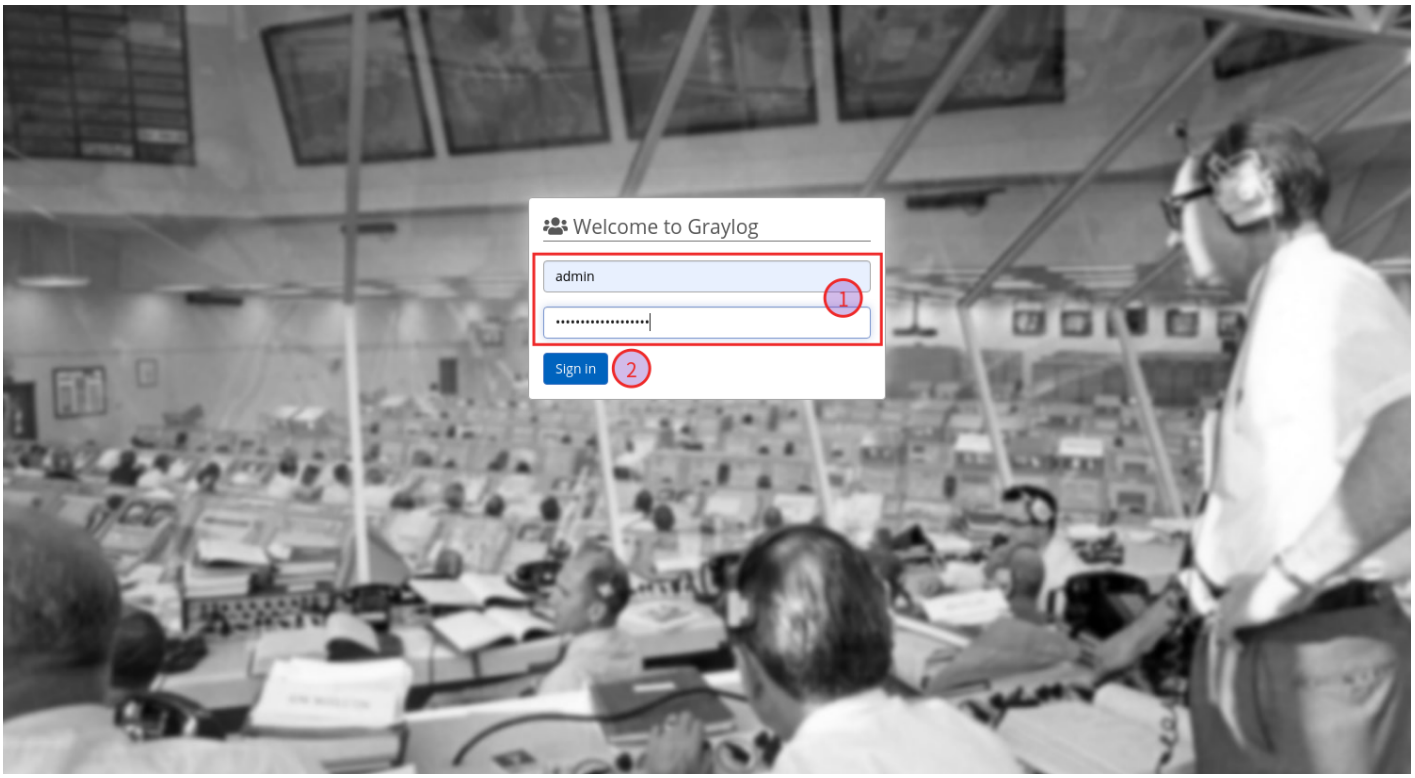
Power

3. Graylog

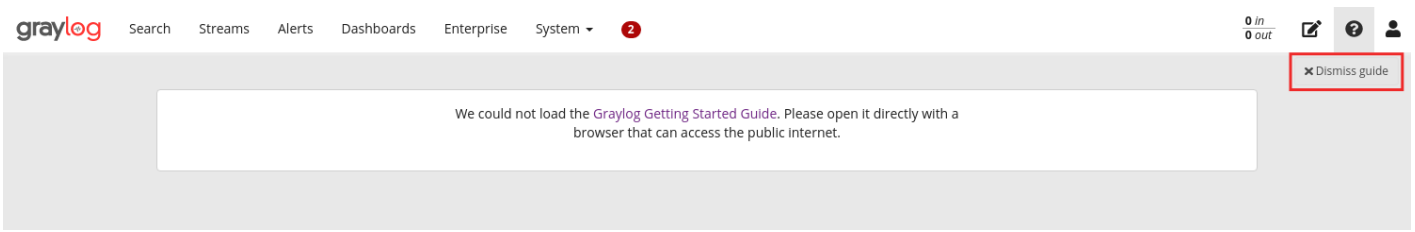
https:// Graylog IP :9000 Graylog

1.

Username Password Sign in



Graylog Dissmiss guide

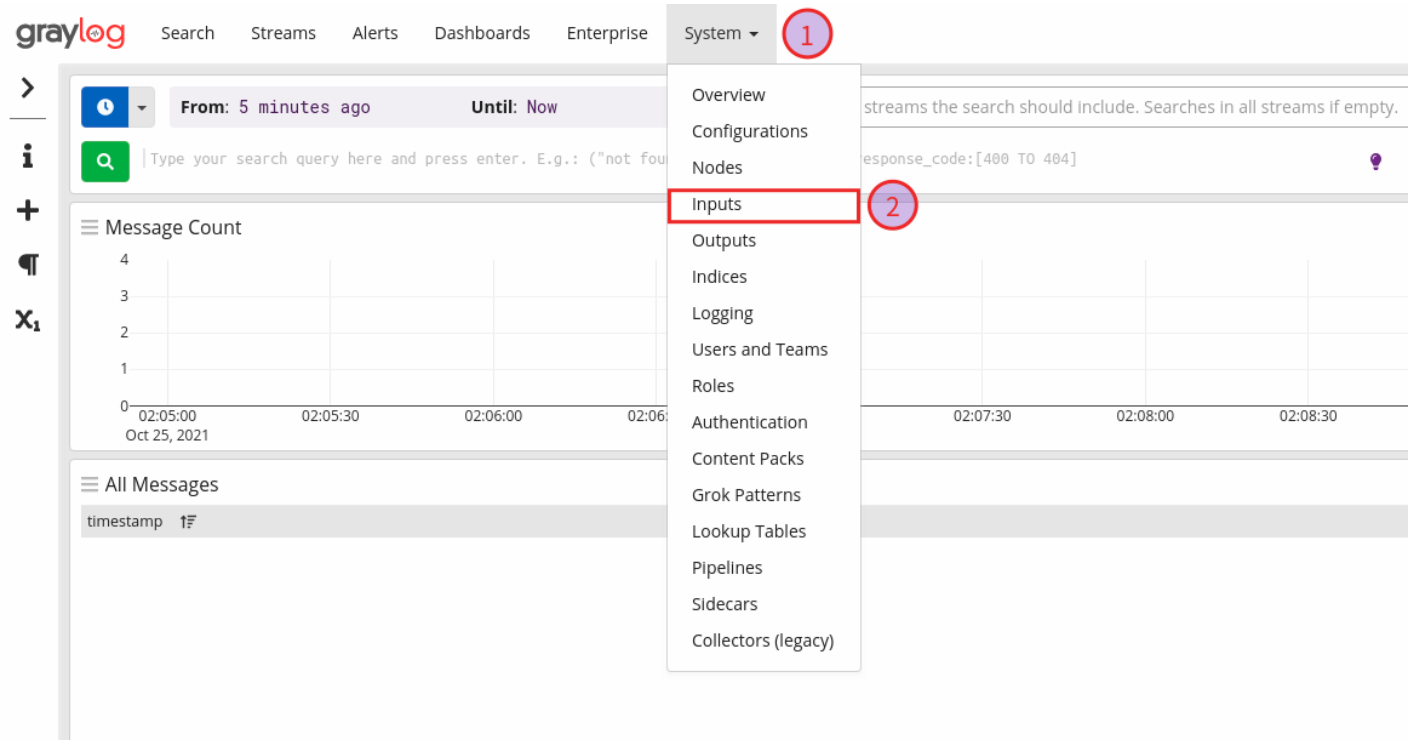


Linux

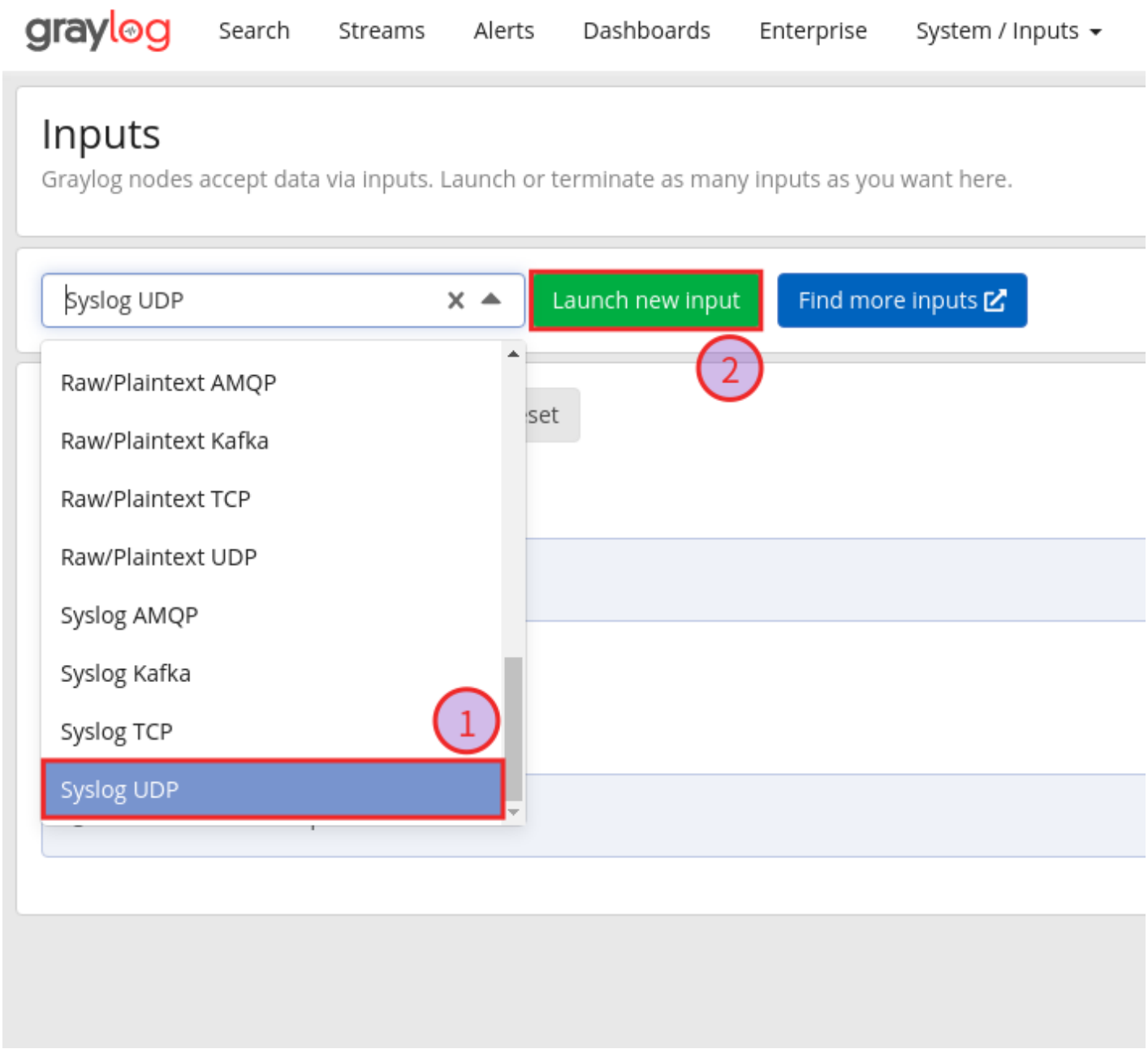
Windows

2. Input

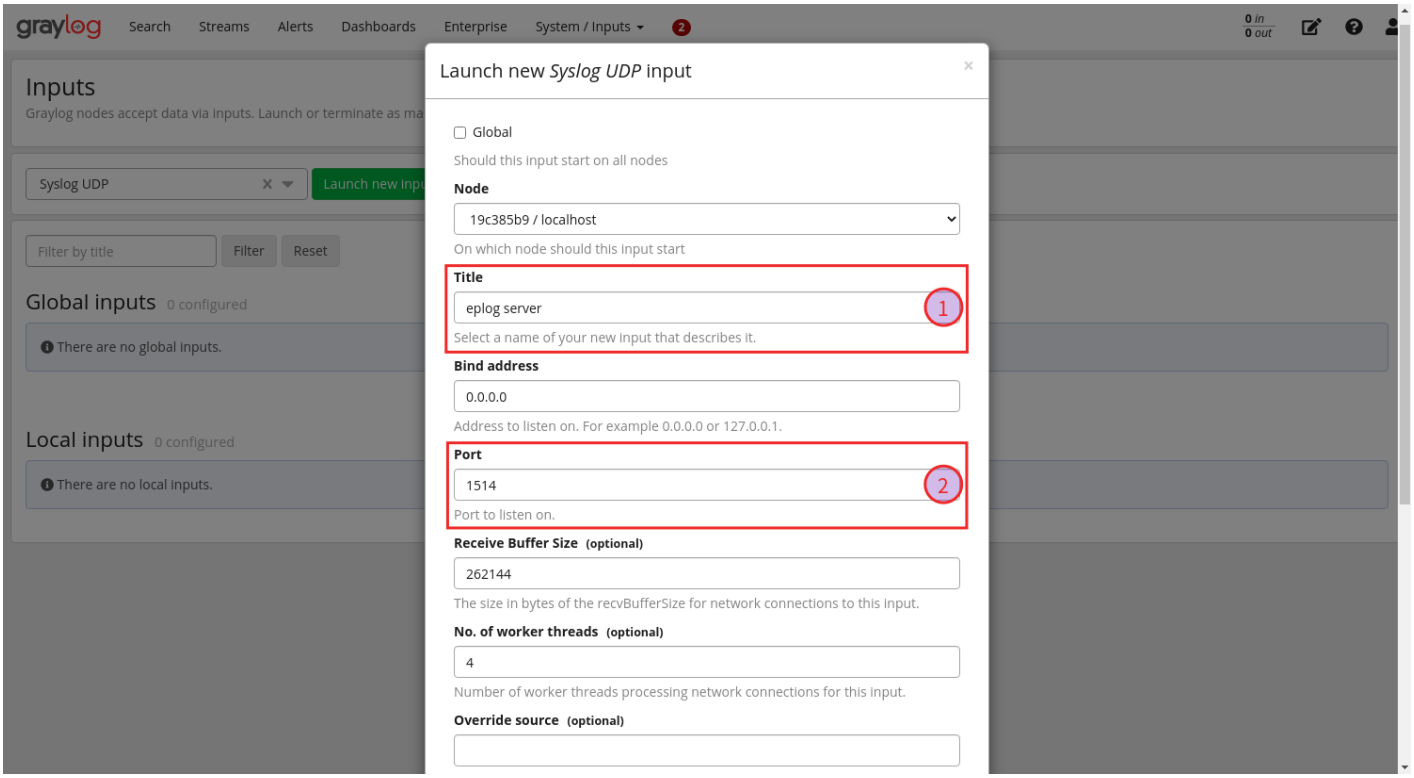
- System➔Inputs



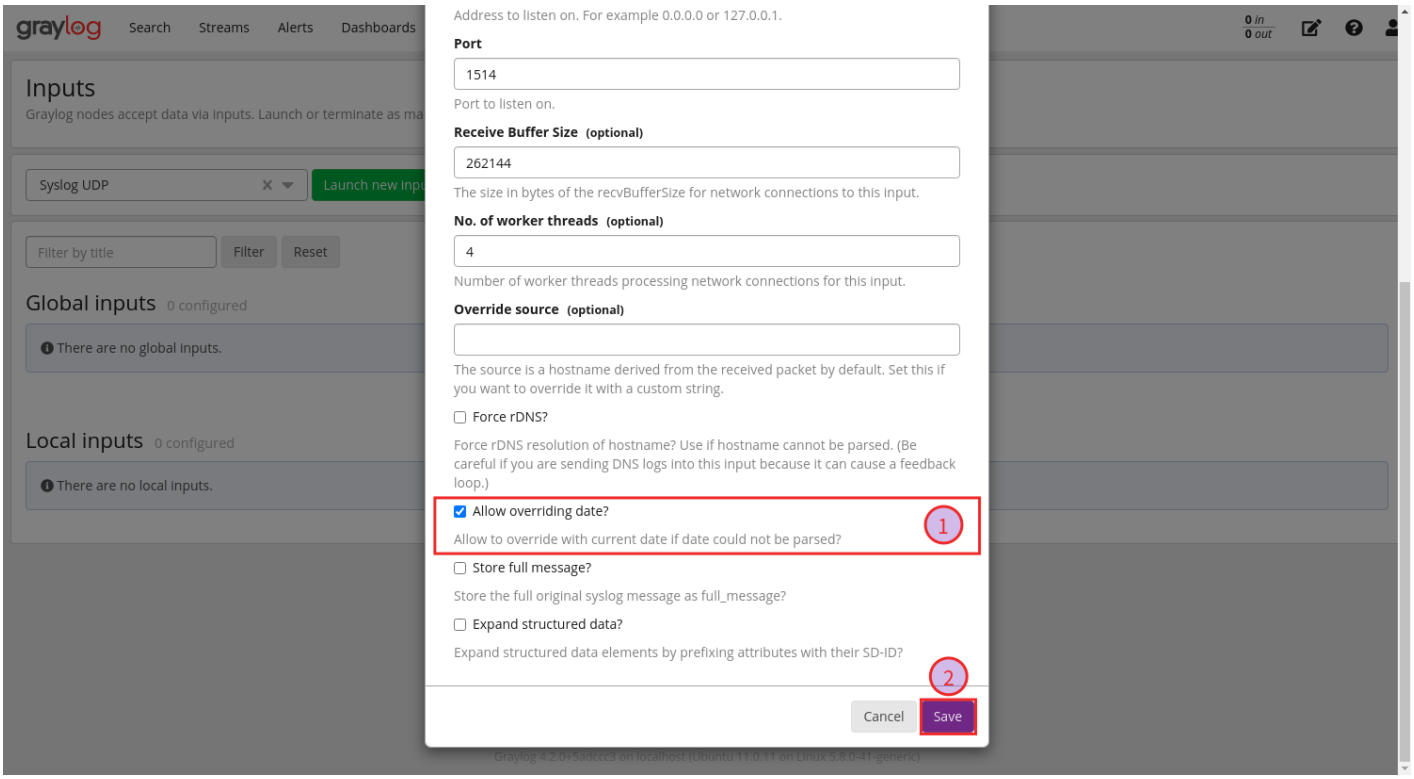
- Input Syslog UDP Launch new input
- Windows "Windows Syslog" "WIndows Graylog"



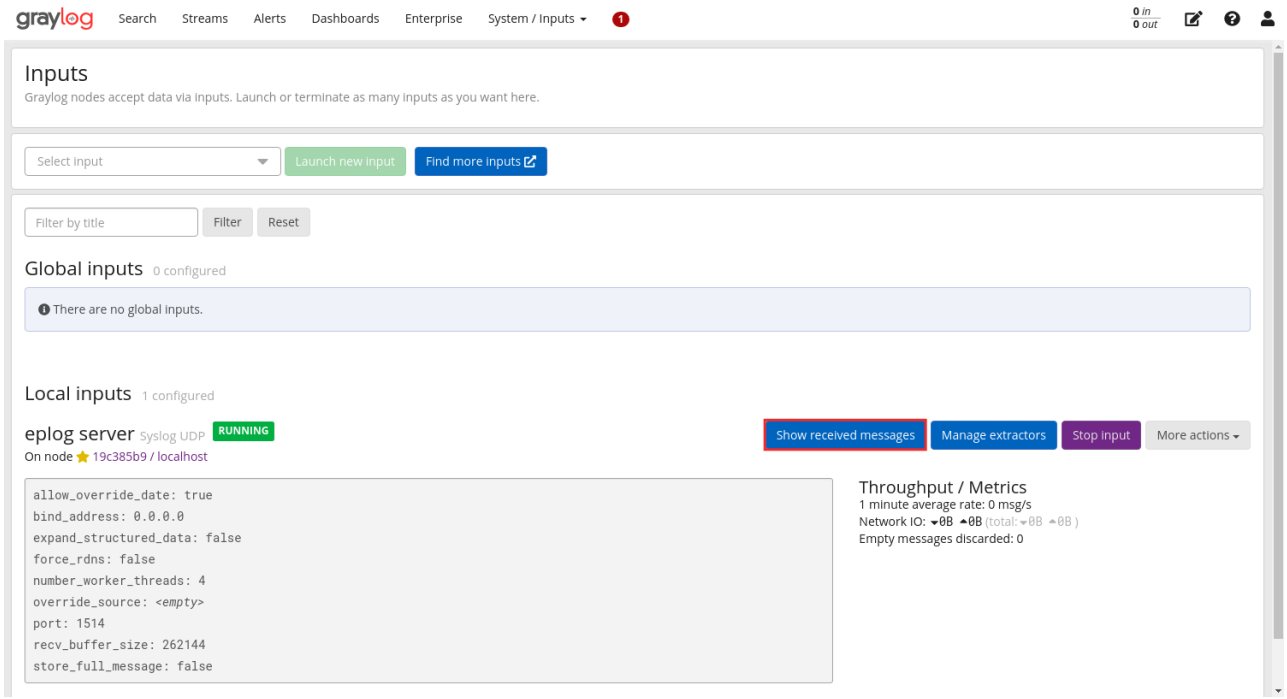
- Title Port
- Windows Port "Windows Syslog" "WIndows Graylog"



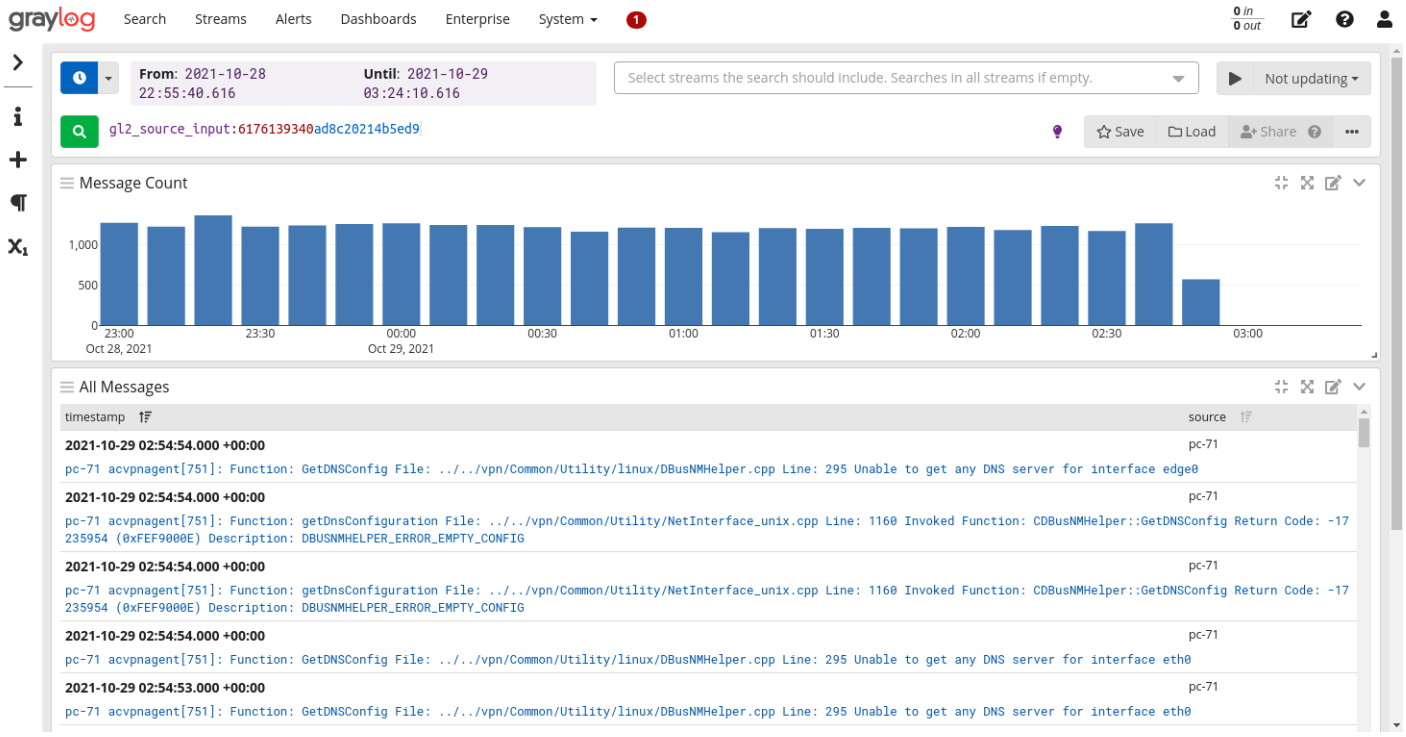
- Allow overriding date Save



- Input Show received messages



- Input



4. NXLog Windows

Graylog NXLog

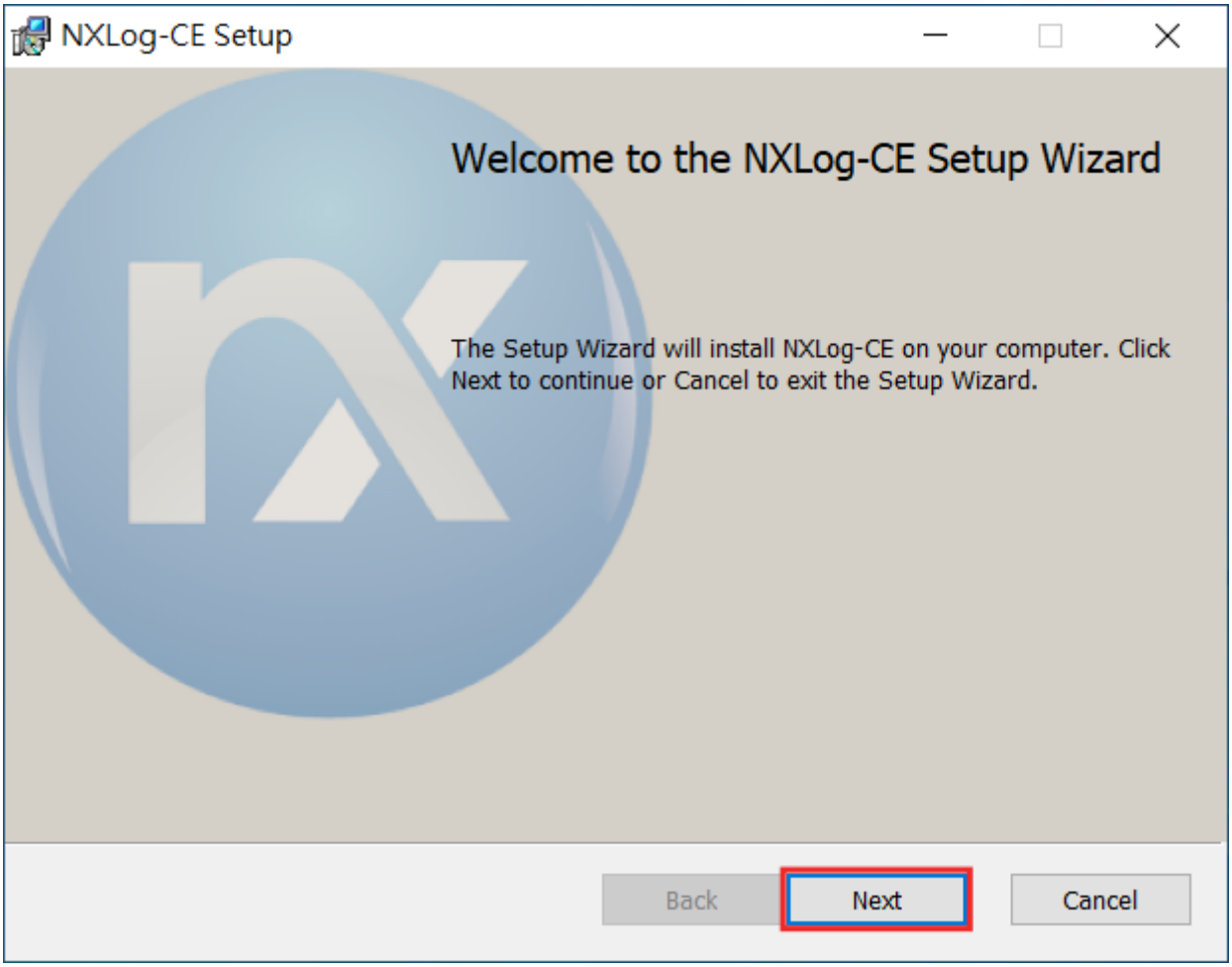
NXLog Community Edition

---

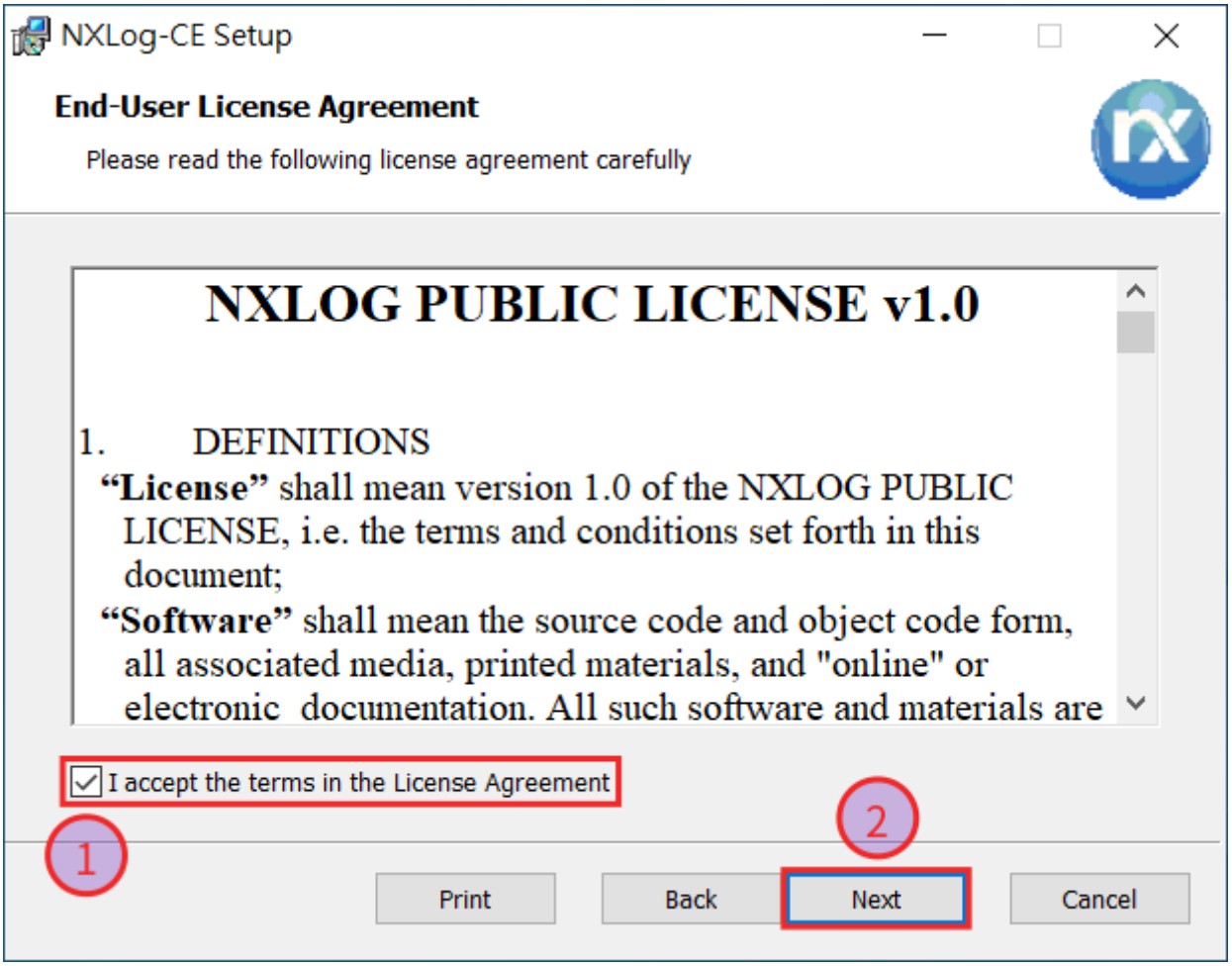
1. NXLog

   nxlog-ce-2.11.2190.msi

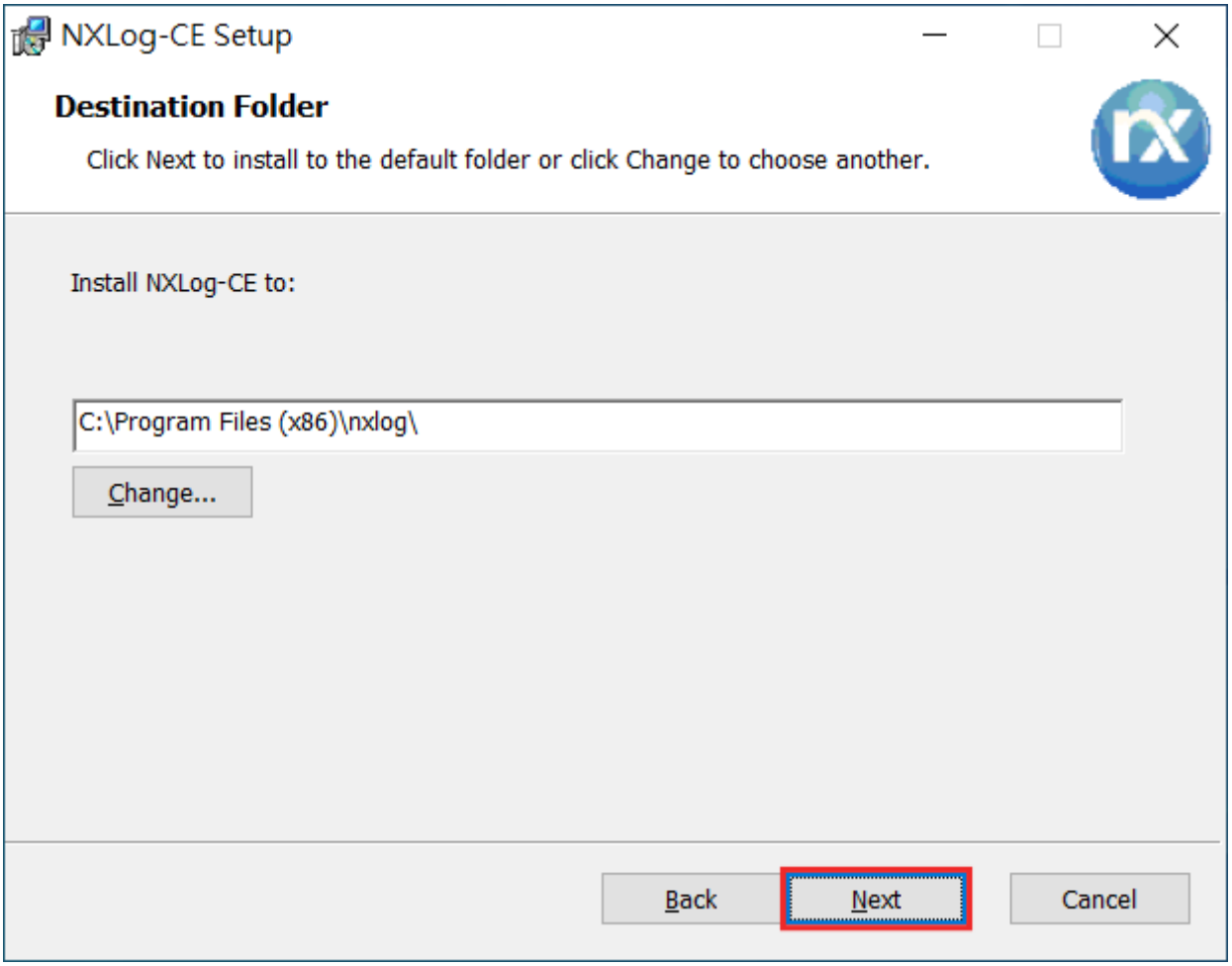
- Next



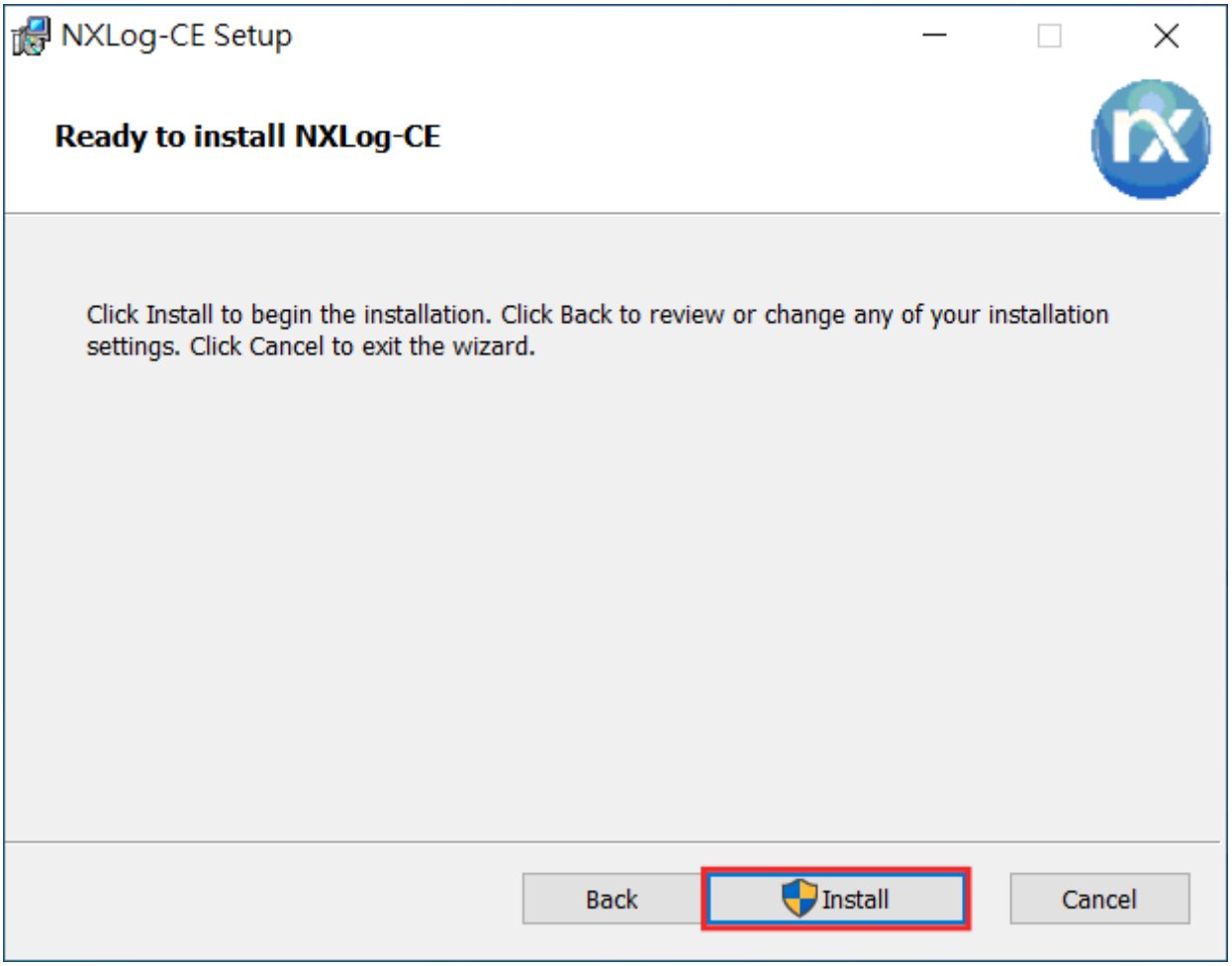
- I accept the terms in the License Agreement→ Next


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

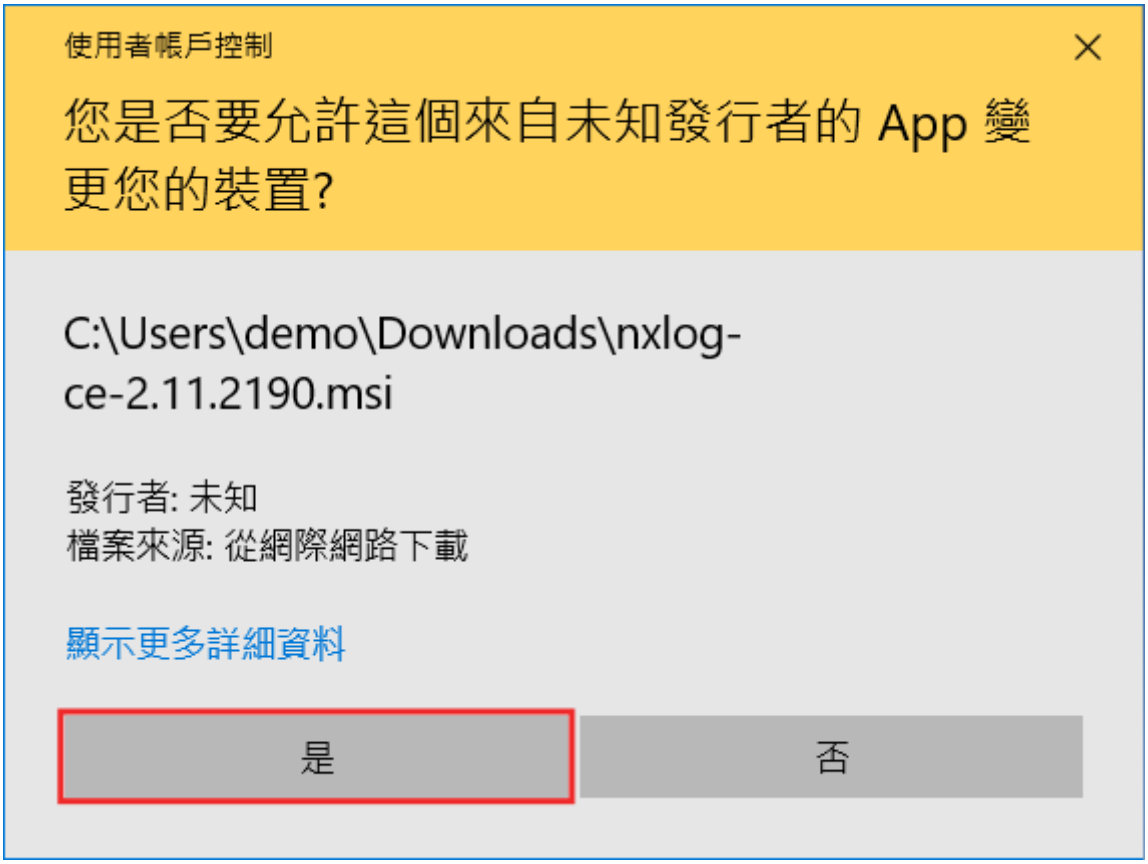
- Next


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

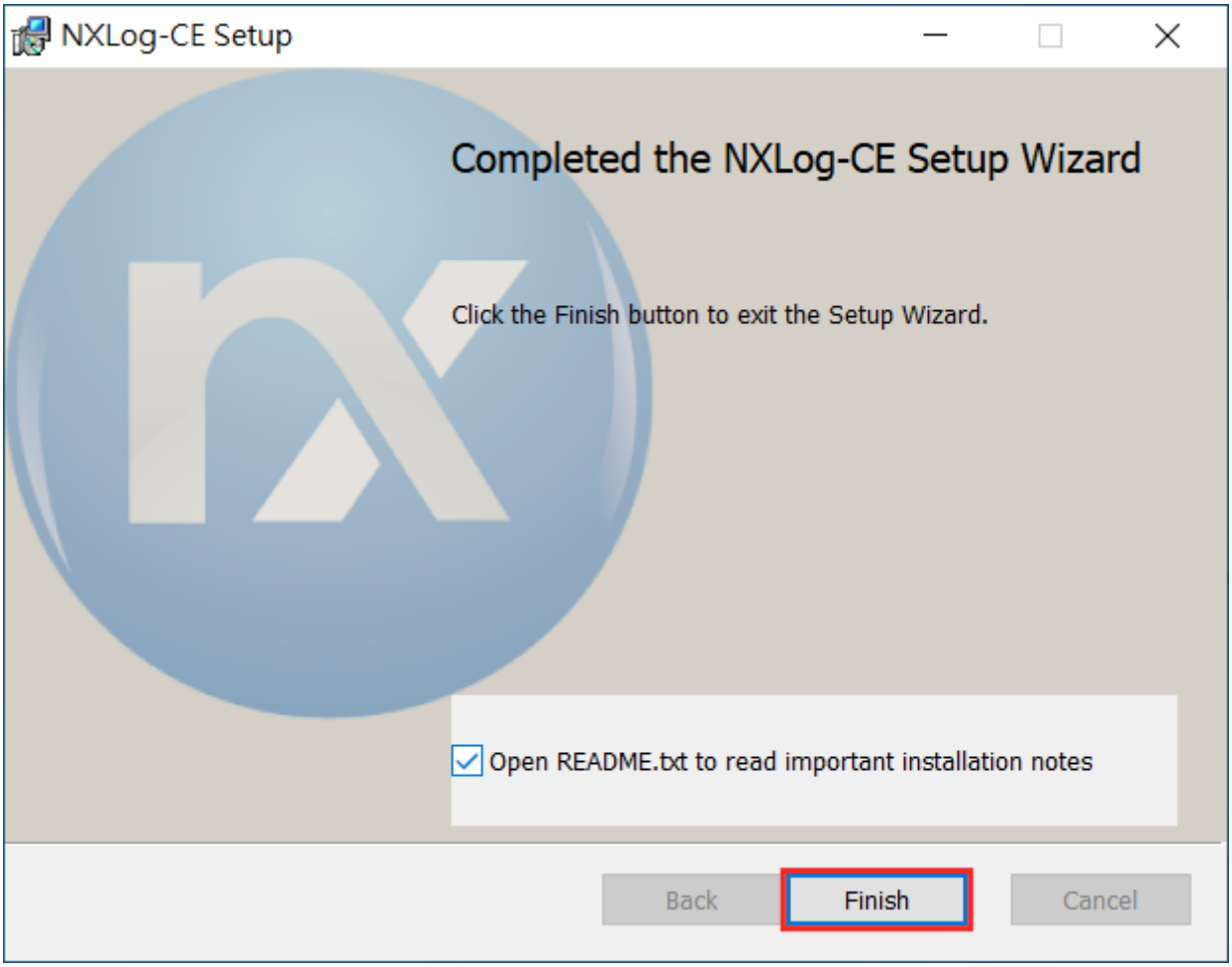
- Install


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

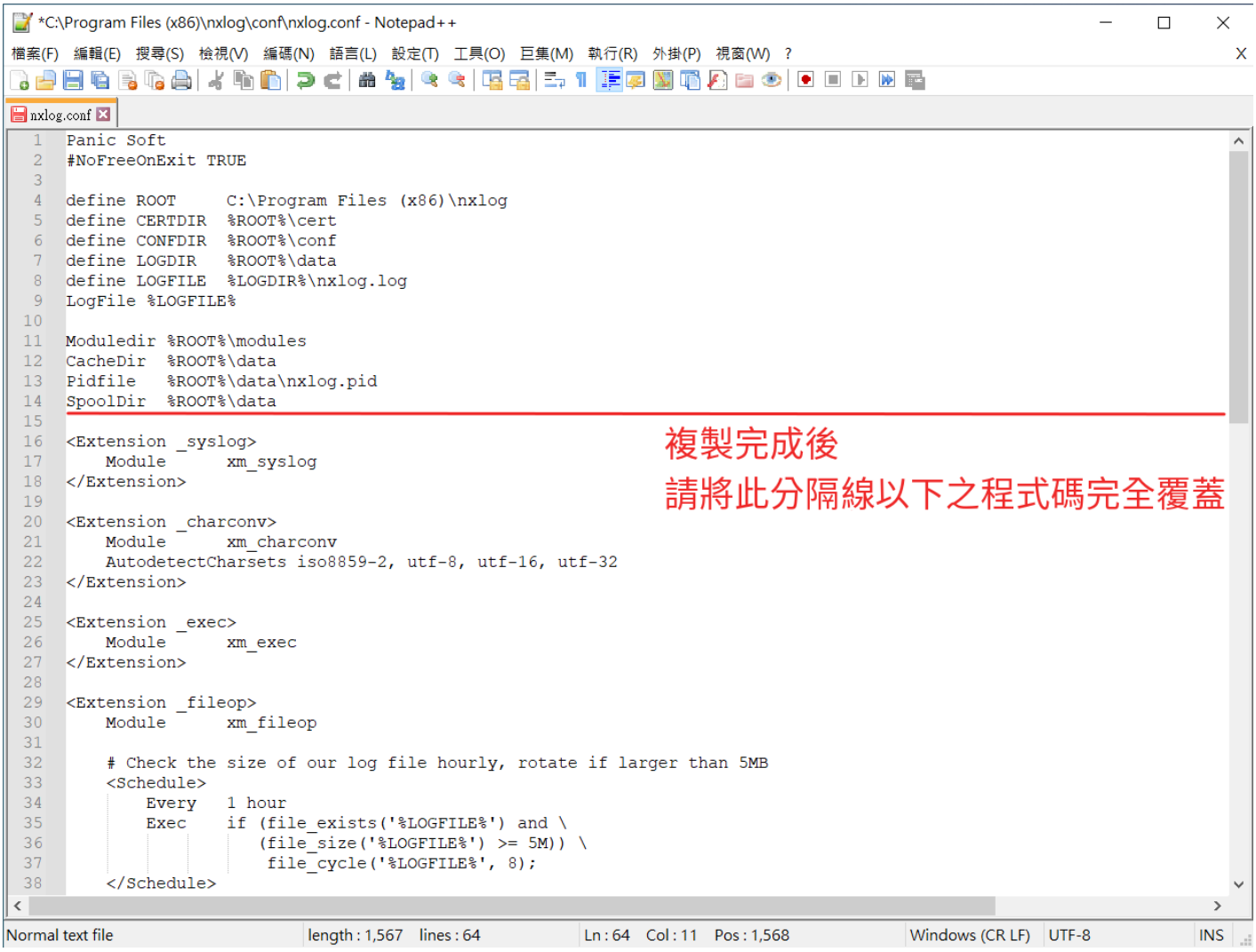
※notepad++ ※

- 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>
```

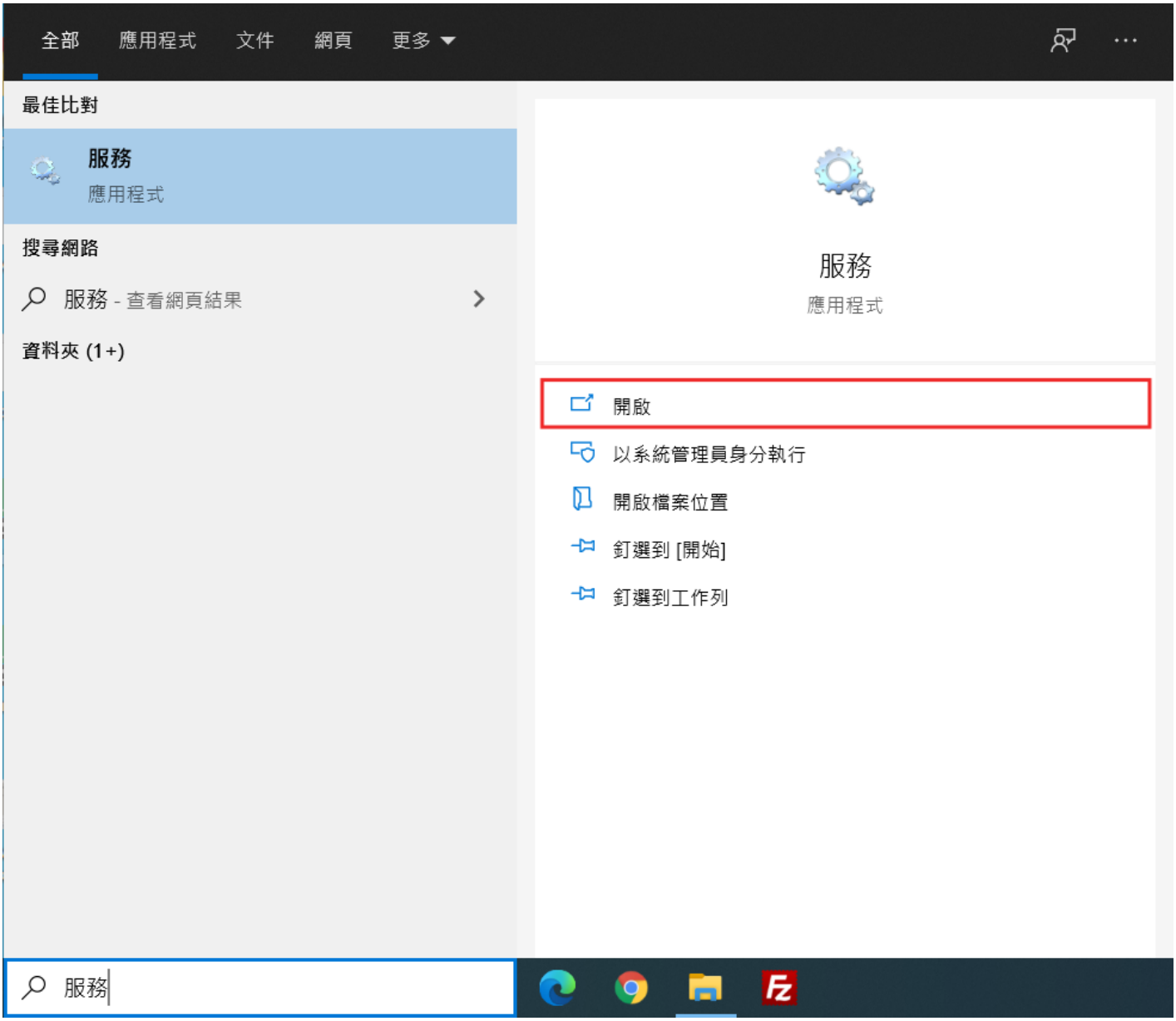
- WIndows Graylog

```
<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>
```

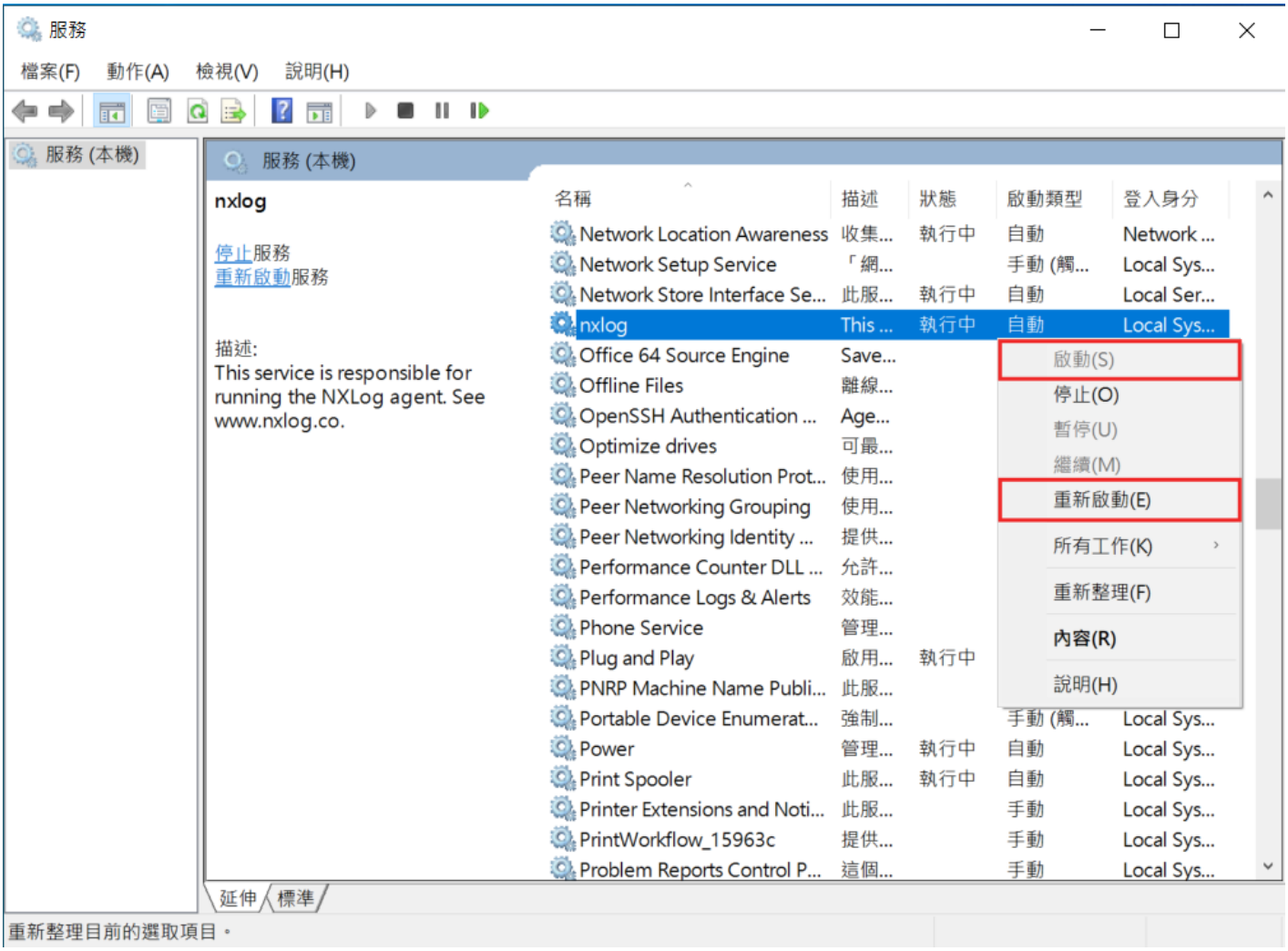

*C:\Program Files (x86)\nxlog\conf\nxlog.conf - Notepad++
檔案(F) 編輯(E) 搜尋(S) 檢視(V) 編碼(N) 語言(L) 設定(T) 工具(O) 巨集(M) 執行(R) 外掛(P) 視窗(W) ?
nxlog.conf
Panic Soft
#NoFreeOnExit TRUE
define ROOT C:\Program Files (x86)\nxlog
define CERTDIR %ROOT%\cert
define CONFDIR %ROOT%\conf
define LOGDIR %ROOT%\data
define 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


服務
檔案(F) 動作(A) 檢視(V) 說明(H)
服務 (本機)
服務 (本機)
nxlog
停止服務
重新啟動服務
描述:
This service is responsible for running the NXLog agent. See www.nxlog.co.
名稱 描述 狀態 啟動類型 登入身分
Network Location Awareness 收集... 執行中 自動 Network ...
Network Setup Service 「網... 手動 (觸... Local Sys...
Network Store Interface Se... 此服... 執行中 自動 Local Ser...
nxlog This ... 執行中 自動 Local Sys...
Office 64 Source Engine Save...
Offline Files 離線...
OpenSSH Authentication ... Age...
Optimize drives 可最...
Peer Name Resolution Prot... 使用...
Peer Networking Grouping 使用...
Peer Networking Identity ... 提供...
Performance Counter DLL ... 允許...
Performance Logs & Alerts 效能...
Phone Service 管理...
Plug and Play 啟用... 執行中
PNRP Machine Name Publi... 此服...
Portable Device Enumerat... 強制... 手動 (觸... Local Sys...
Power 管理... 執行中 自動 Local Sys...
Print Spooler 此服... 執行中 自動 Local Sys...
Printer Extensions and Noti... 此服... 手動 Local Sys...
PrintWorkflow_15963c 提供... 手動 Local Sys...
Problem Reports Control P... 這個... 手動 Local Sys...
啟動(S)
停止(O)
暫停(U)
繼續(M)
重新啟動(E)
所有工作(K)
重新整理(F)
內容(R)
說明(H)
延伸 標準
重新整理目前的選取項目。

Graylog

5. NXLog Linux

Linux Syslog rsyslog.conf

NXLog Community Edition syslog

---

1. rsyslog.conf

```
lubuntu@pc-71:~$ sudo bash
root@pc-71:/home/lubuntu# vi /etc/rsyslog.conf
```

---

2. rsyslog.conf

```
#################
#### MODULES ####
#################
module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability
# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")
# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")
# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")
###########################
#### GLOBAL DIRECTIVES ####
###########################
#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

*.* @192.168.31.16:1514
```

Esc :wq

3. rsyslog

```
root@pc-71:/home/lubuntu# /etc/init.d/rsyslog restart
```

Graylog