N-Cloud 設定 SOP

- Windows IIS Log 設定
- Linux syslog 設定
- NXLog 安裝常見問題

目錄

Windows IIS Log 設定

- NXLog 安裝與設定
- Internet Information Services (IIS) 設定

Linux syslog 轉發設定

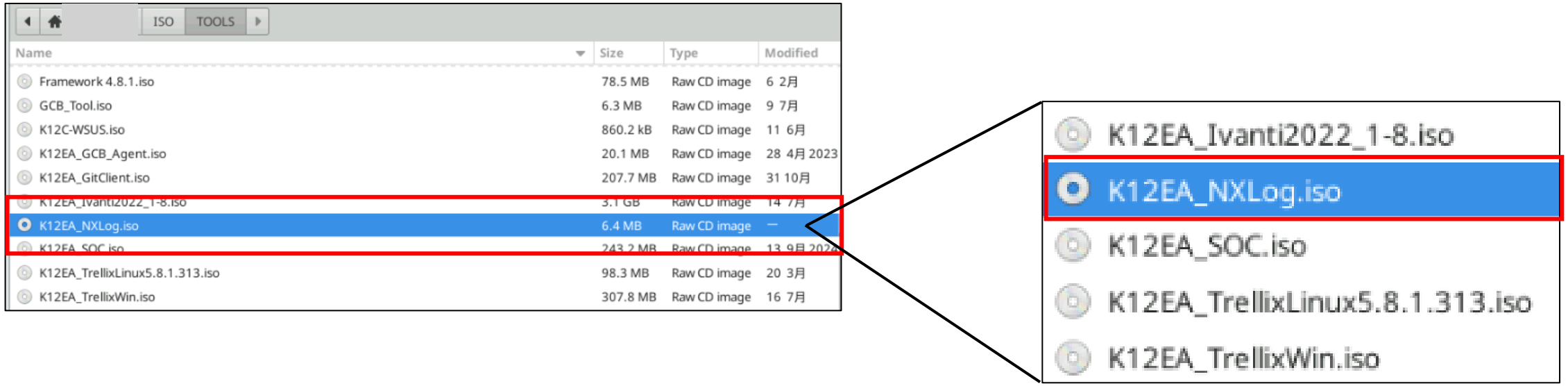
- 設定rsyslog轉發

NXLog 安裝

- 此為Agent全安裝的環境
- 適用 Windows 2019 & Windows 2022 作業系統

NXLog 安裝

- 掛載**K12EA_NXLog.iso**檔 (ISO > TOOLS)

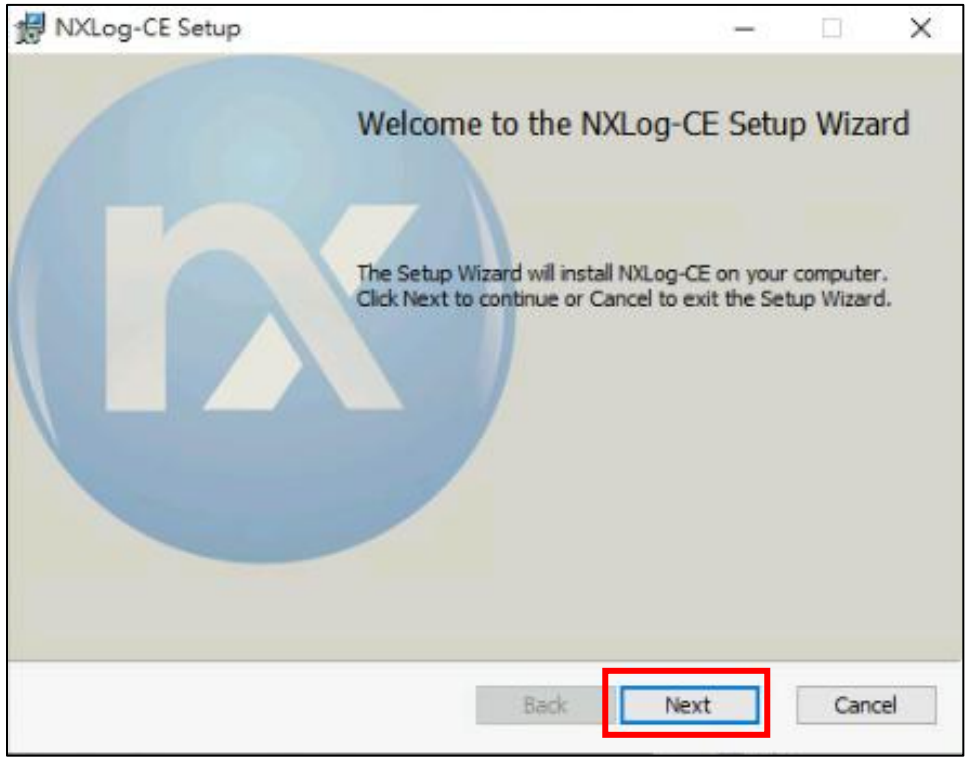


NXLog 安裝

- 點擊執行 **nxlog-ce-3.2.2329** 安裝檔

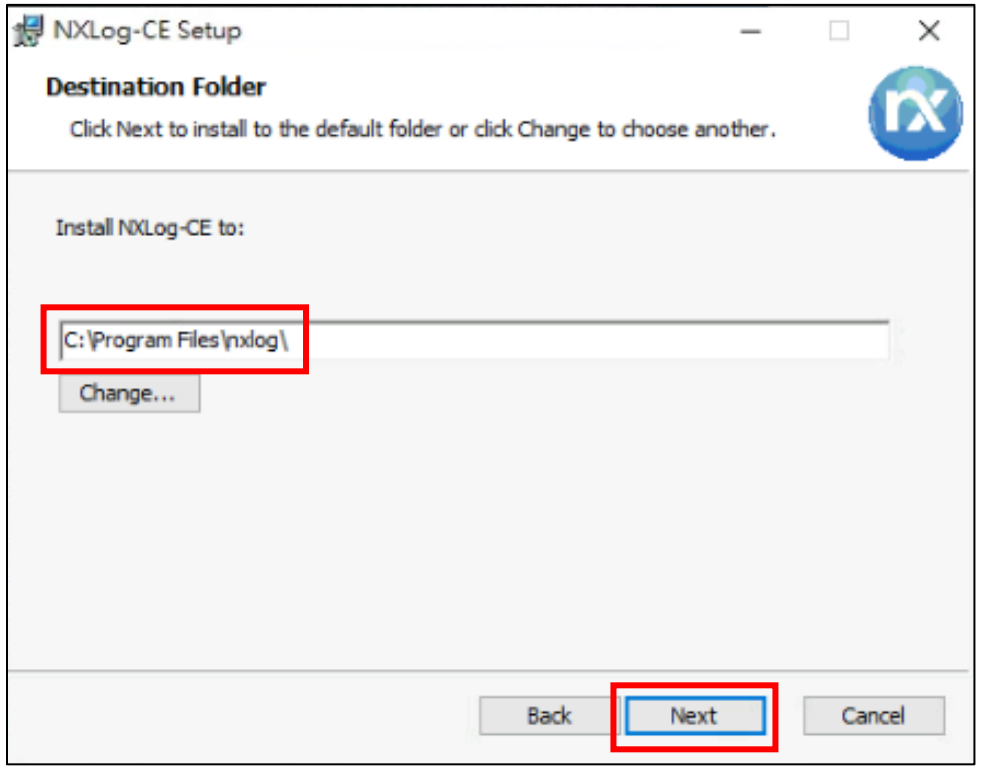
NXLog 安裝

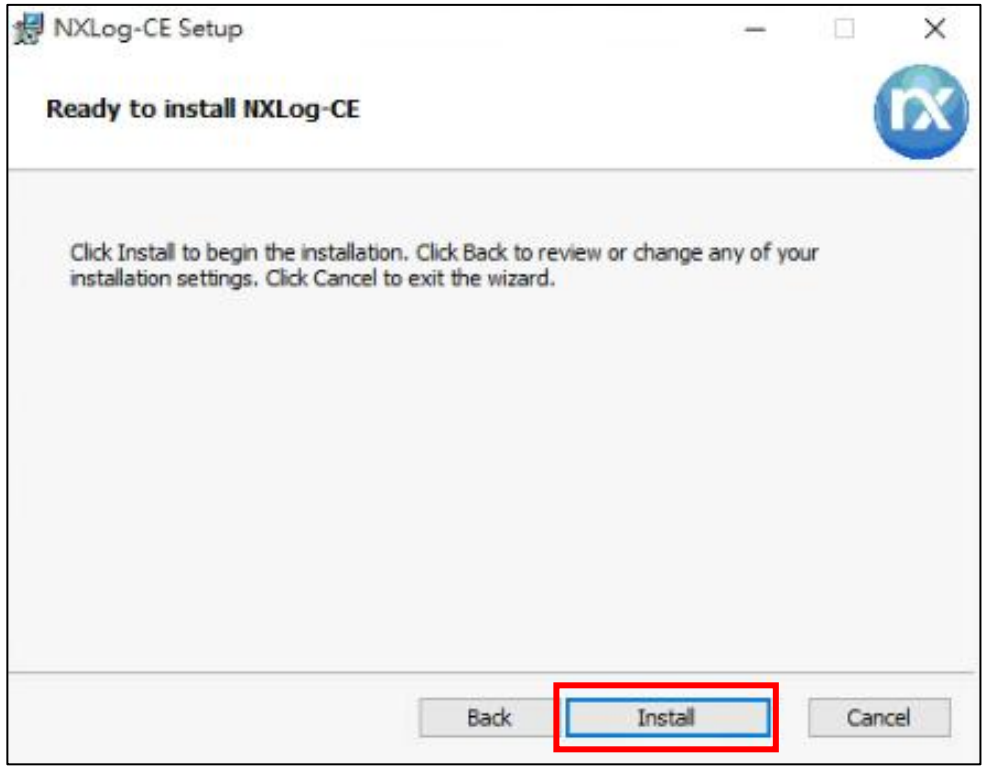
1. 點擊 [nxlog-ce-3.2.2329.msi] -> 按 [Next].
2. 勾選 [I accept the terms in the License Agreement], 按 [Next] .



NXLog 安裝

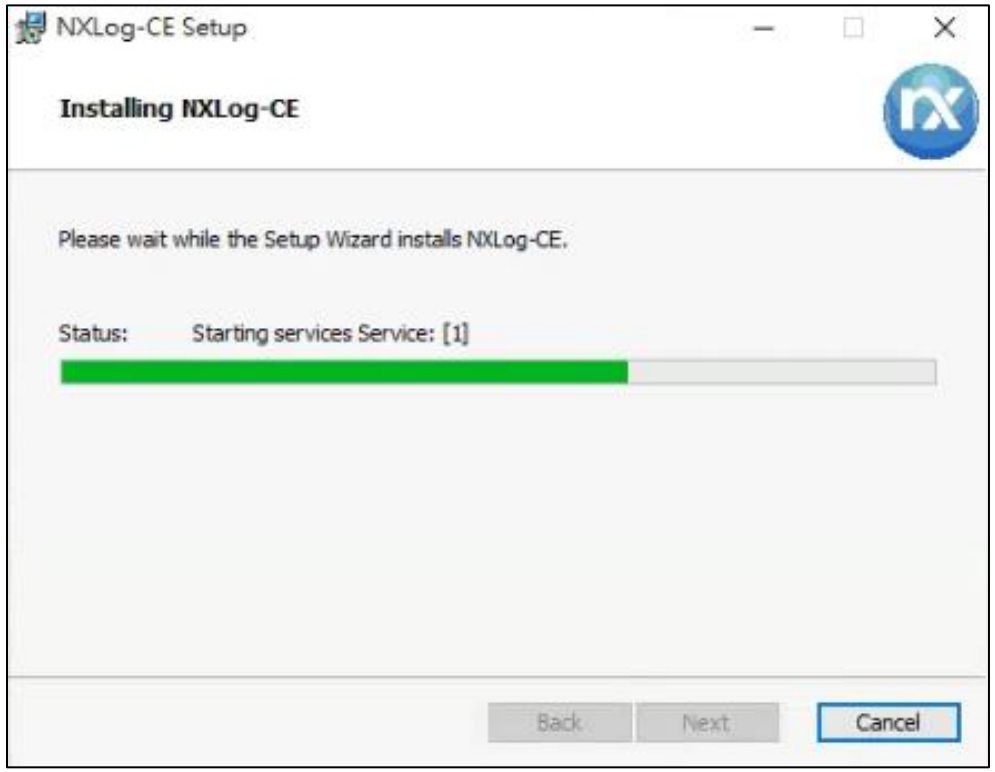
1. 按 [Next]. (預設安裝路徑為 C:\Program Files\nxlog\)
2. 按 [Install].

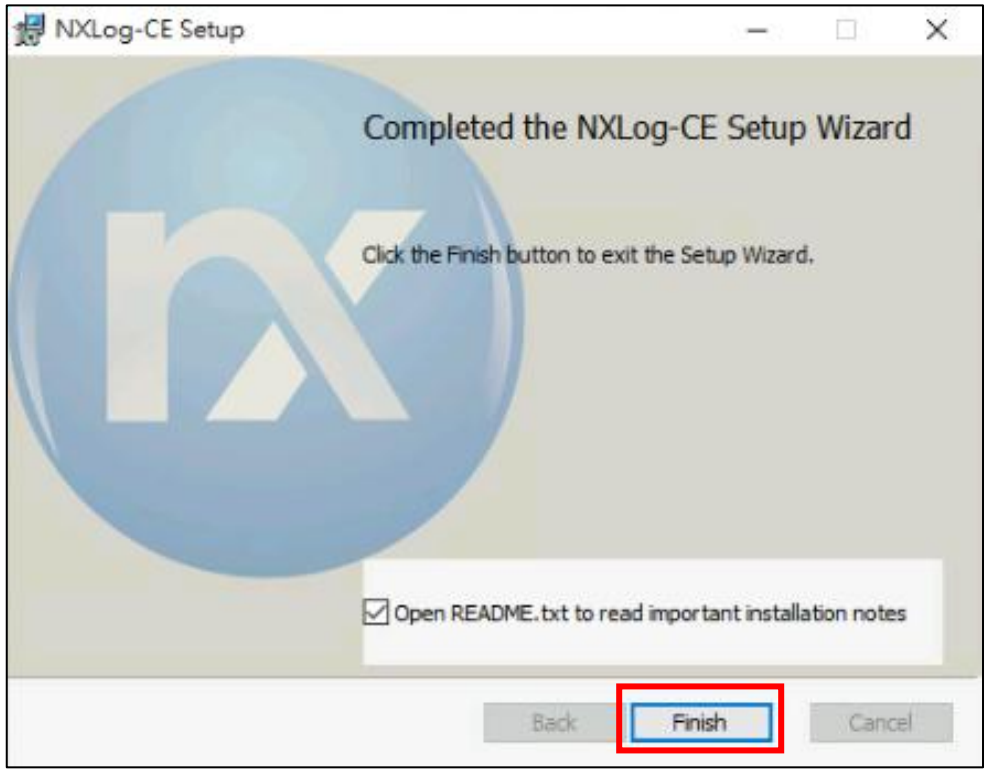




NXLog 安裝

- 按 [Finish]





NXLog 設定檔

- 適用 Windows 2019 & Windows 2022 作業系統

NXLog 設定檔

- 複製 K12EA_NXLog.iso檔裡的 **nxlog.conf**

NXLog 設定檔

- 進入 C:\Program Files\nxlog\conf裡，並貼上 **nxlog.conf** 設定檔

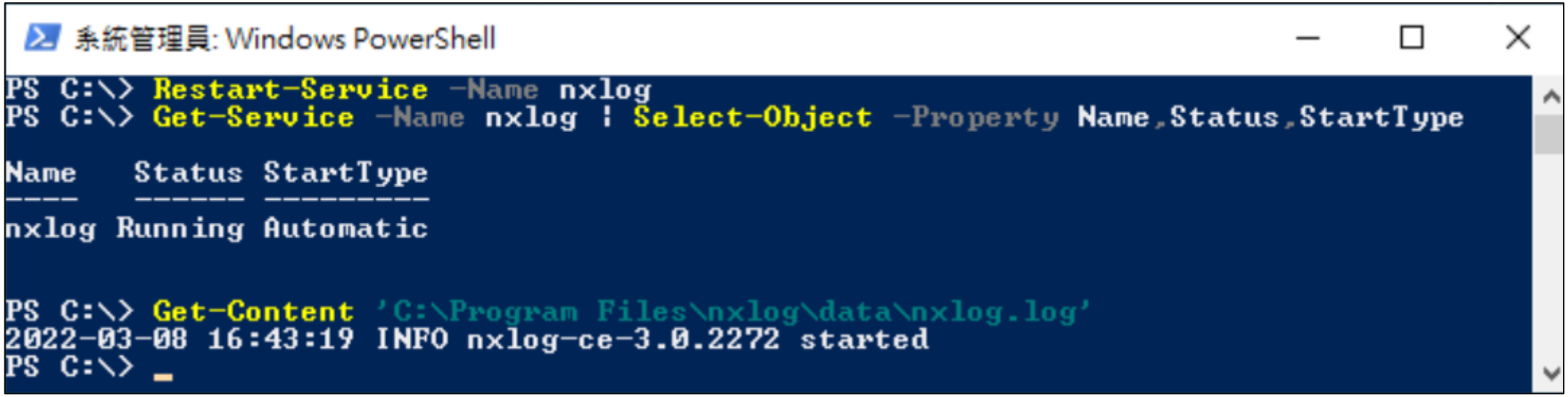
NXLog 啟動服務

- 適用 Windows 2019 & Windows 2022 作業系統

NXLog 啟動服務 (方法一)

- 開啟 [Windows PowerShell]
- 重新啟動 NXLog 服務，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息

```
PS C:\> Restart-Service -Name nxlog
PS C:\> Get-Service -Name nxlog | Select-Object -Property Name,Status,StartType
PS C:\> Get-Content 'C:\Program Files\nxlog\data\nxlog.log'
```

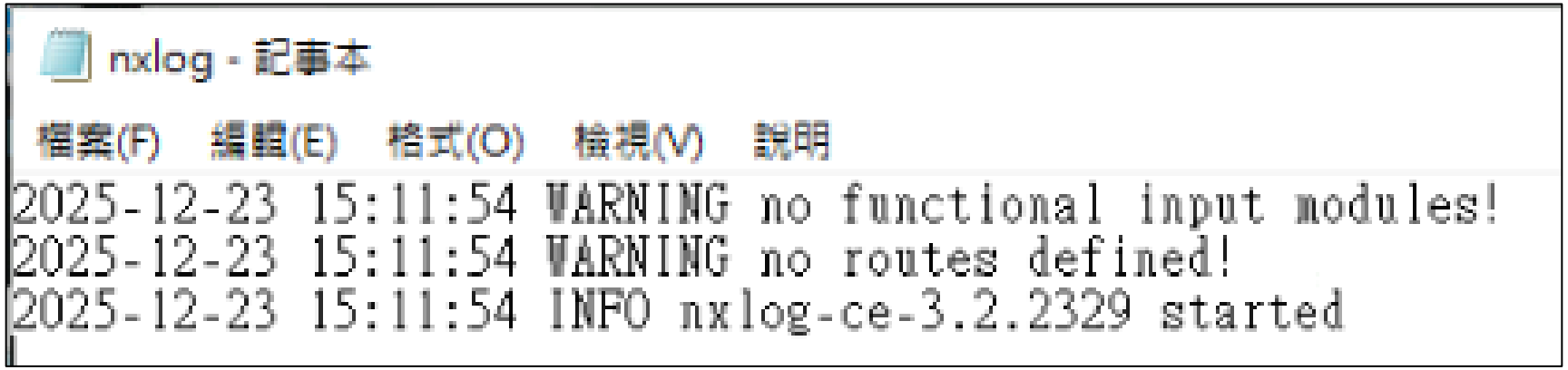


NXLog 啟動服務 (方法二)

- 也可以透過服務程式，找到nxlog服務，並且重新啟動

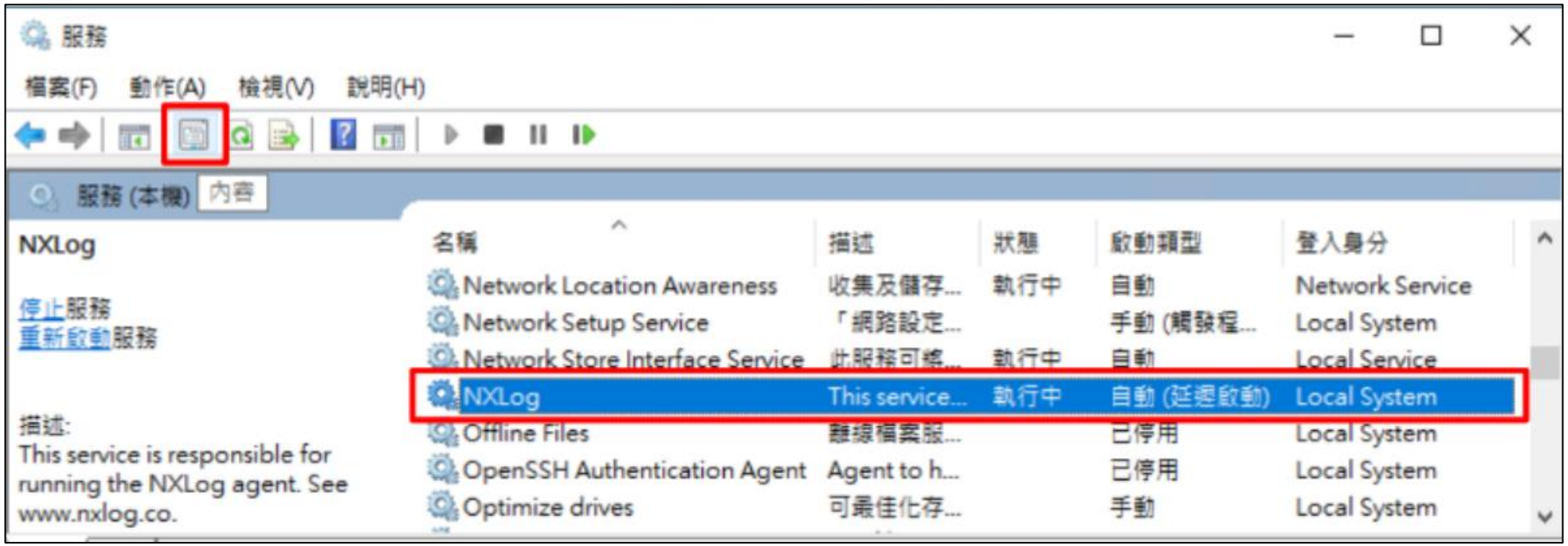
NXLog 啟動服務 (方法二)

- 重新啟動 NXLog 服務後，檢查 NXLog 服務和確認 NXLog 沒有錯誤訊息



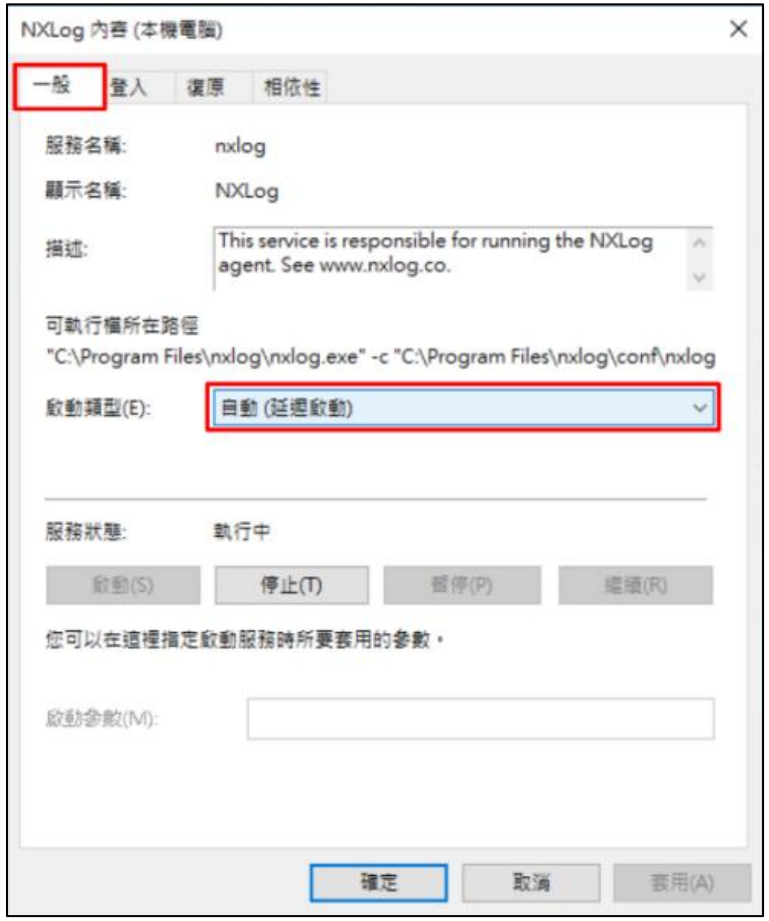
NXLog 啟動服務

- 開啟 NXLog 服務內容，選擇 [NXLog] -> 點選 [內容]



NXLog 啟動服務

- [一般] 頁面
- 啟動類型: [自動 (延遲啟動)]



NXLog 啟動服務

- [復原] 頁籤
- 第一次失敗時: [重新啟動服務]

  第二次失敗時: [重新啟動服務]

  後續失敗時: [重新啟動服務]
- 按 [確定]

Internet Information Services (IIS) 設定

適用有安裝IIS設定的 WebServer

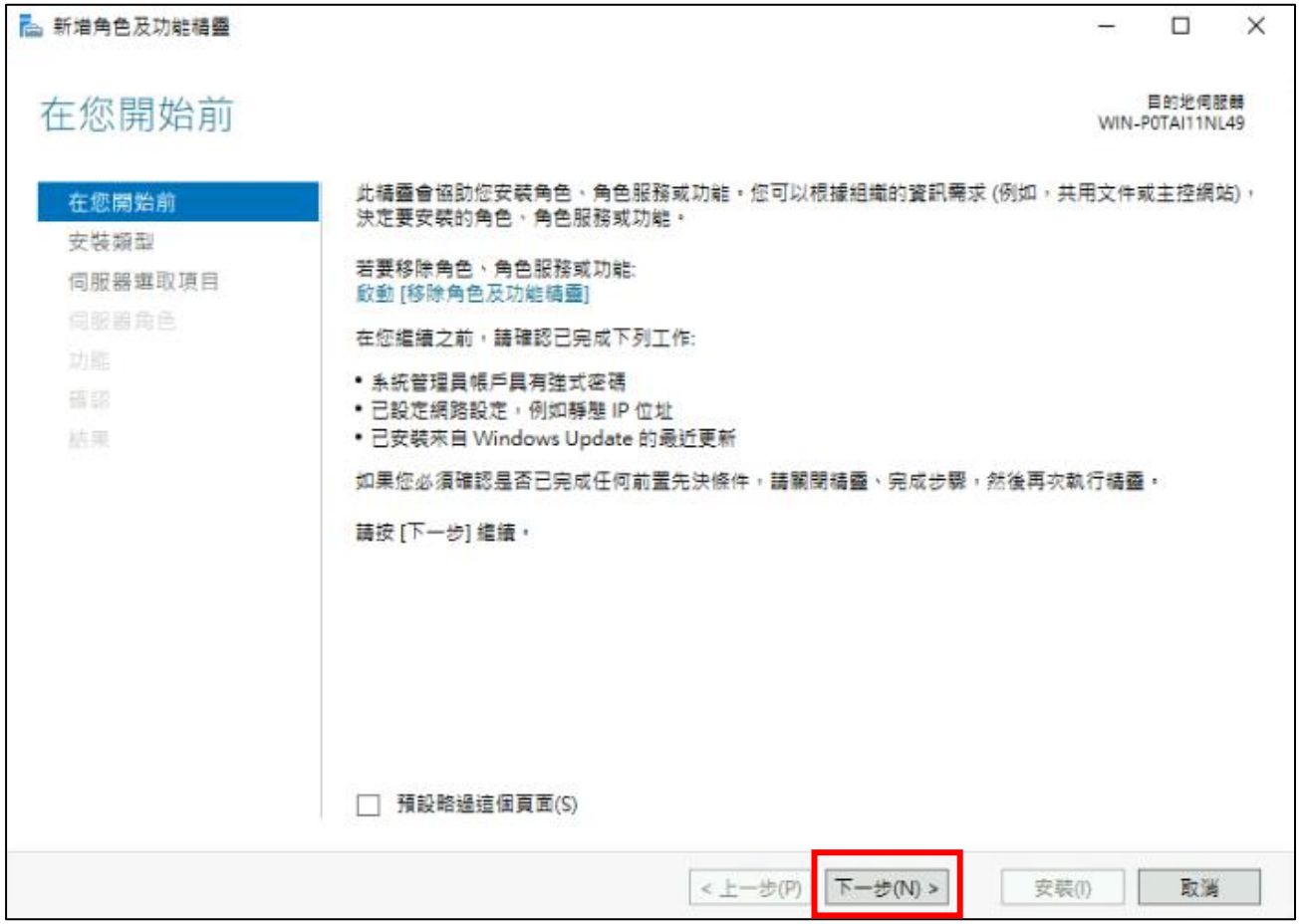
(若沒有安裝IIS可跳過此步驟)

Internet Information Services (IIS) 設定

- 打開控制台，並點選”**開啟或關閉Windows 功能**”

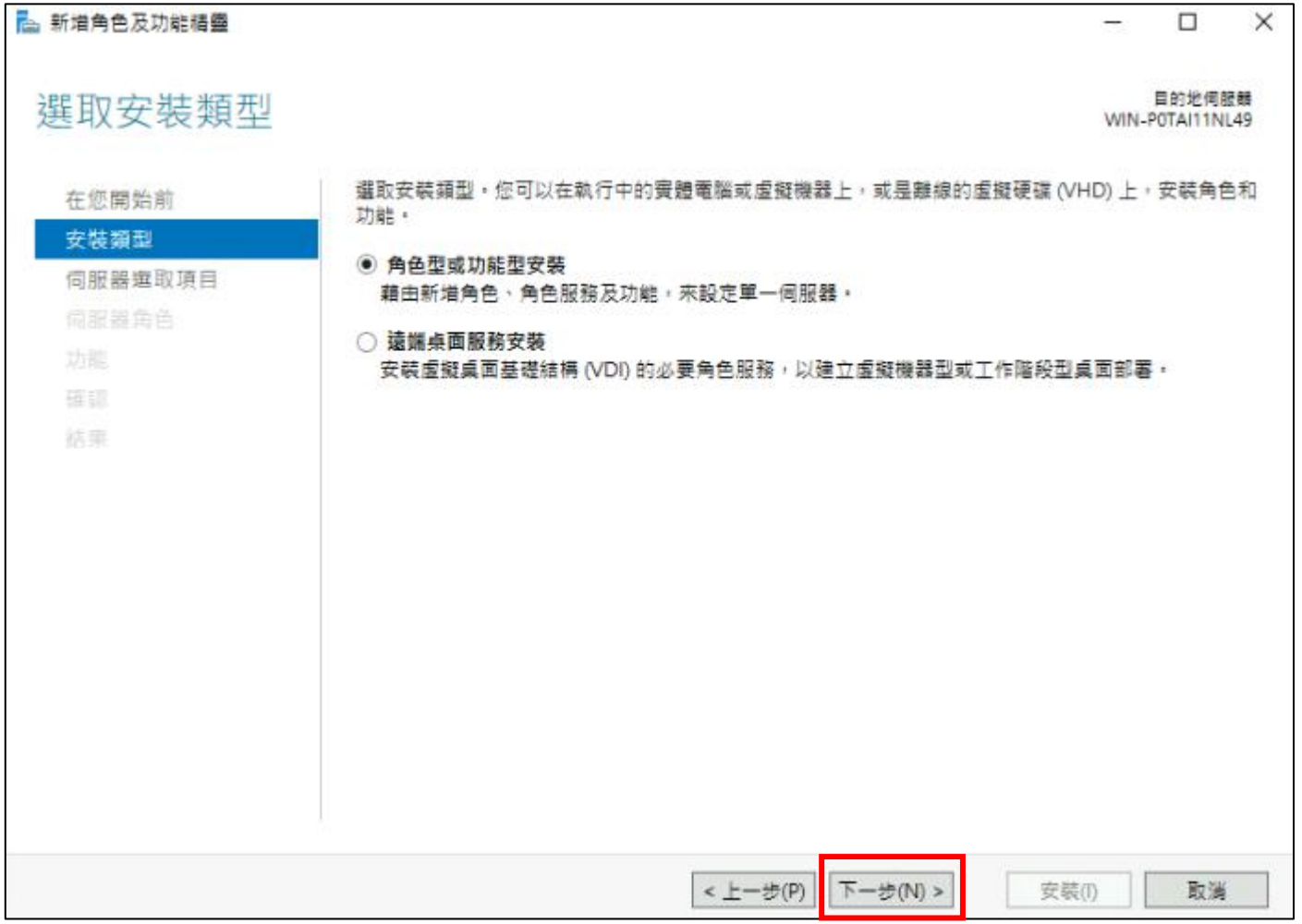
Internet Information Services (IIS) 設定

- 進入新增角色及功能精靈頁面
- 點擊”下一步”



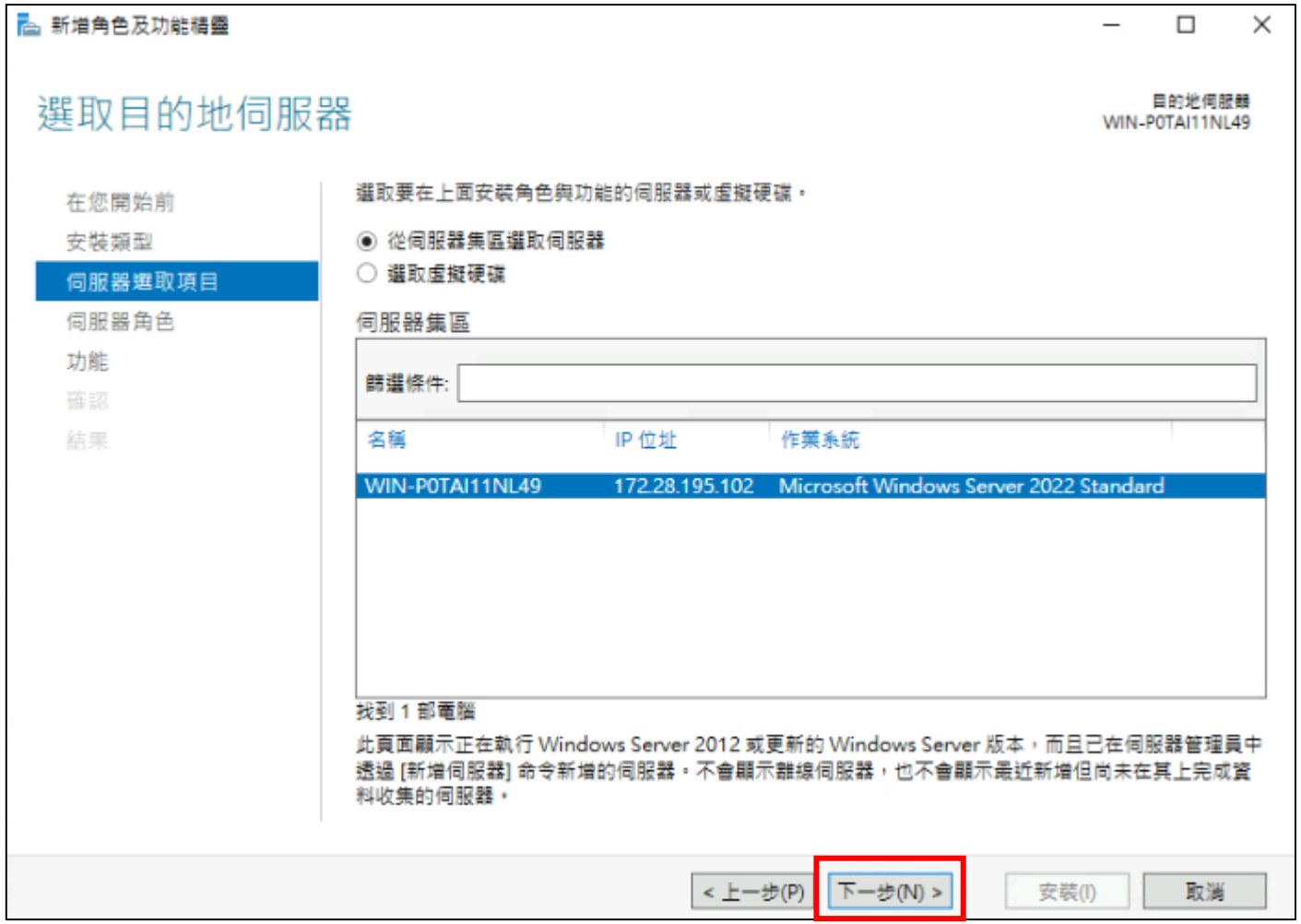
Internet Information Services (IIS) 設定

- 點擊”下一步”



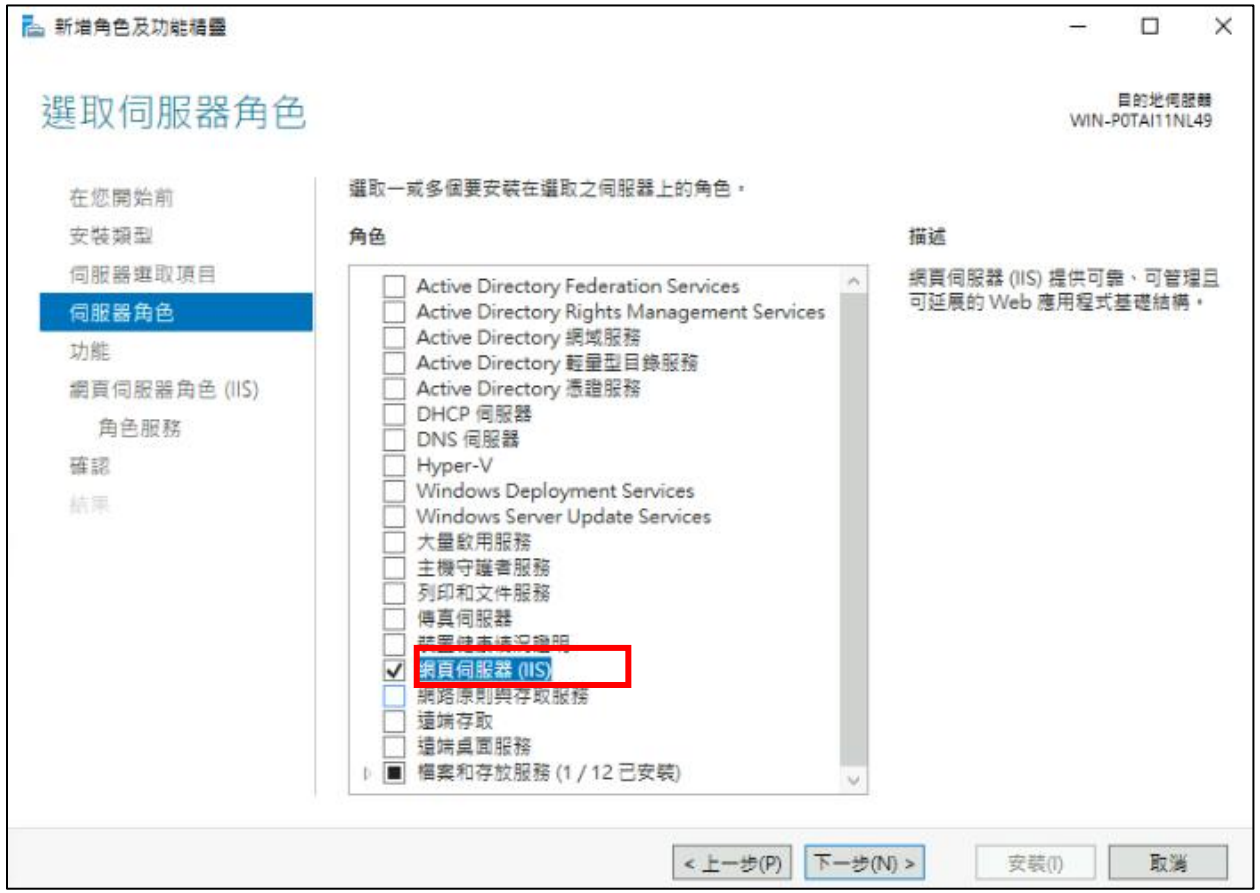
Internet Information Services (IIS) 設定

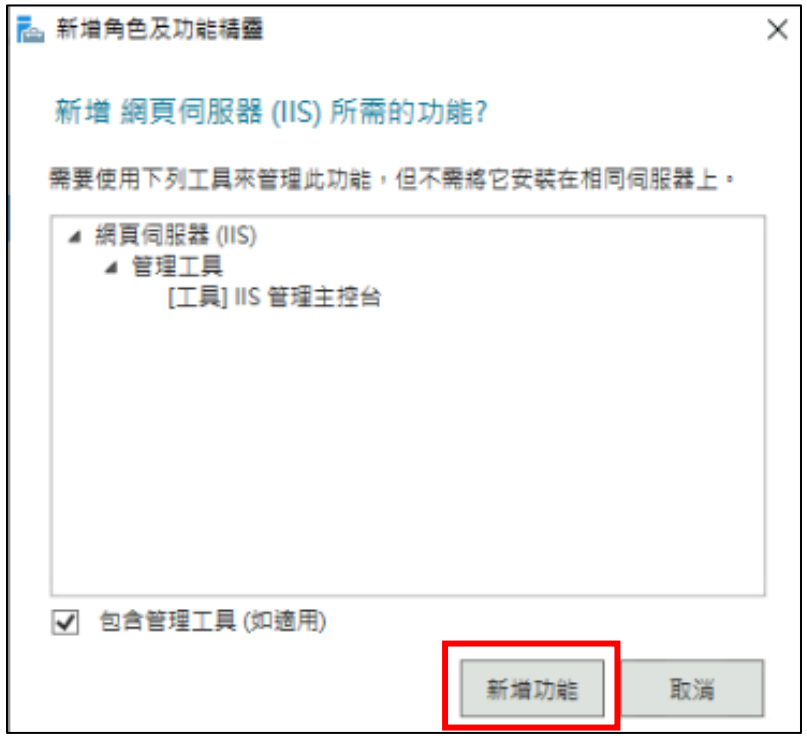
- 點擊”下一步”



Internet Information Services (IIS) 設定

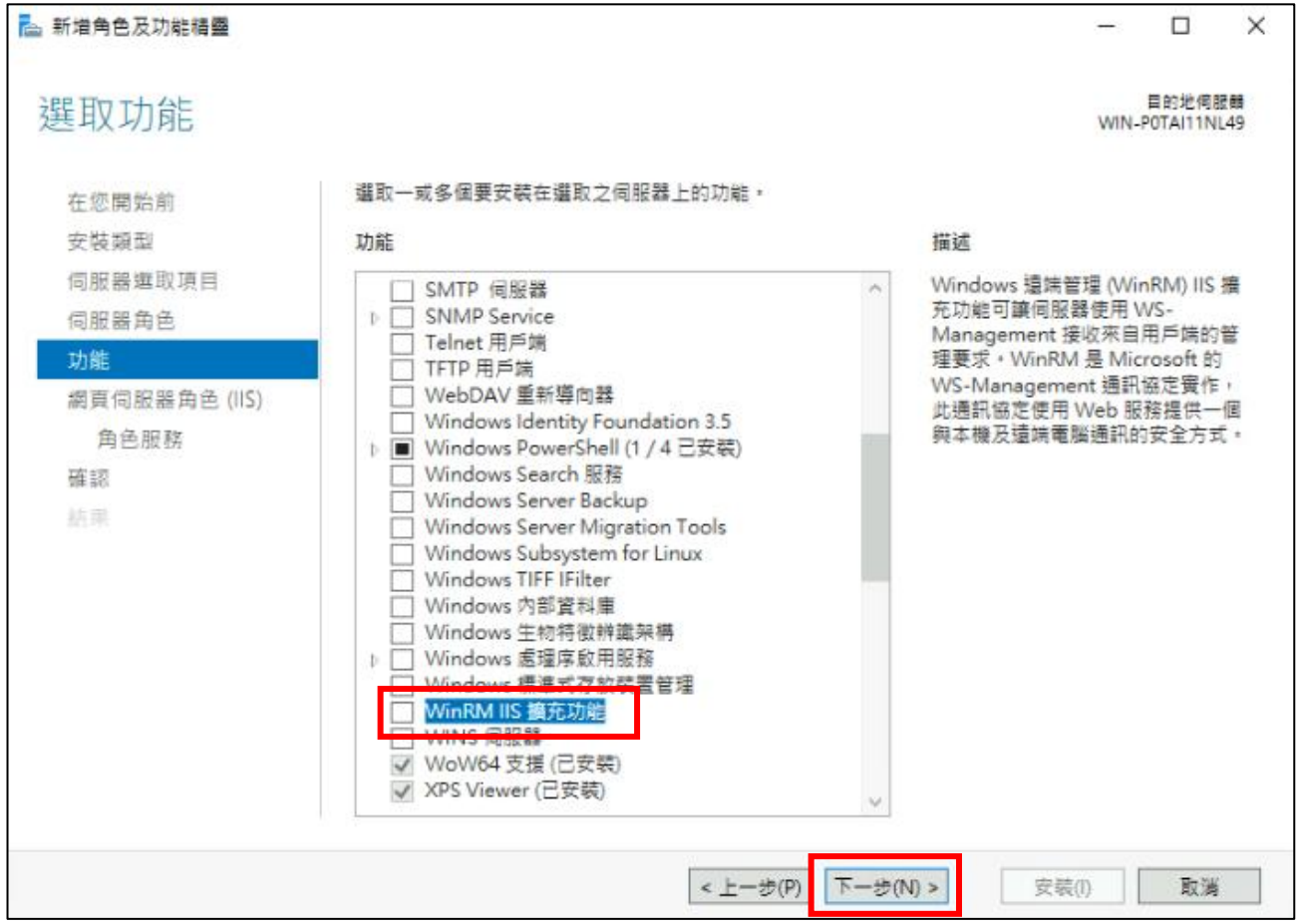
- 在角色欄位裡，勾選”網頁伺服器(IIS)“





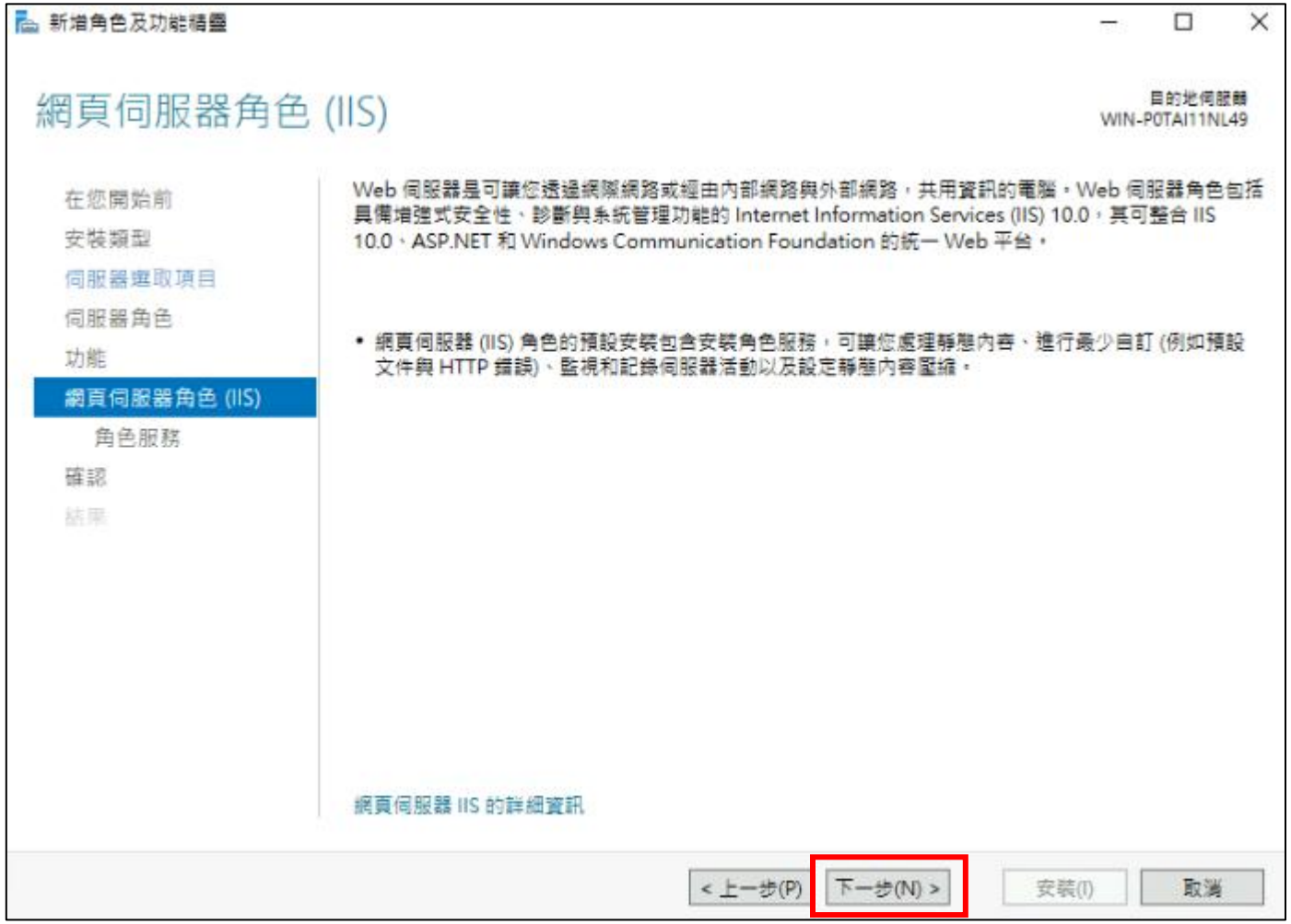
Internet Information Services (IIS) 設定

- 選擇”WinRM IIS 擴充功能”
- 點擊”下一步”



Internet Information Services (IIS) 設定

- 點擊”下一步”



Internet Information Services (IIS) 設定

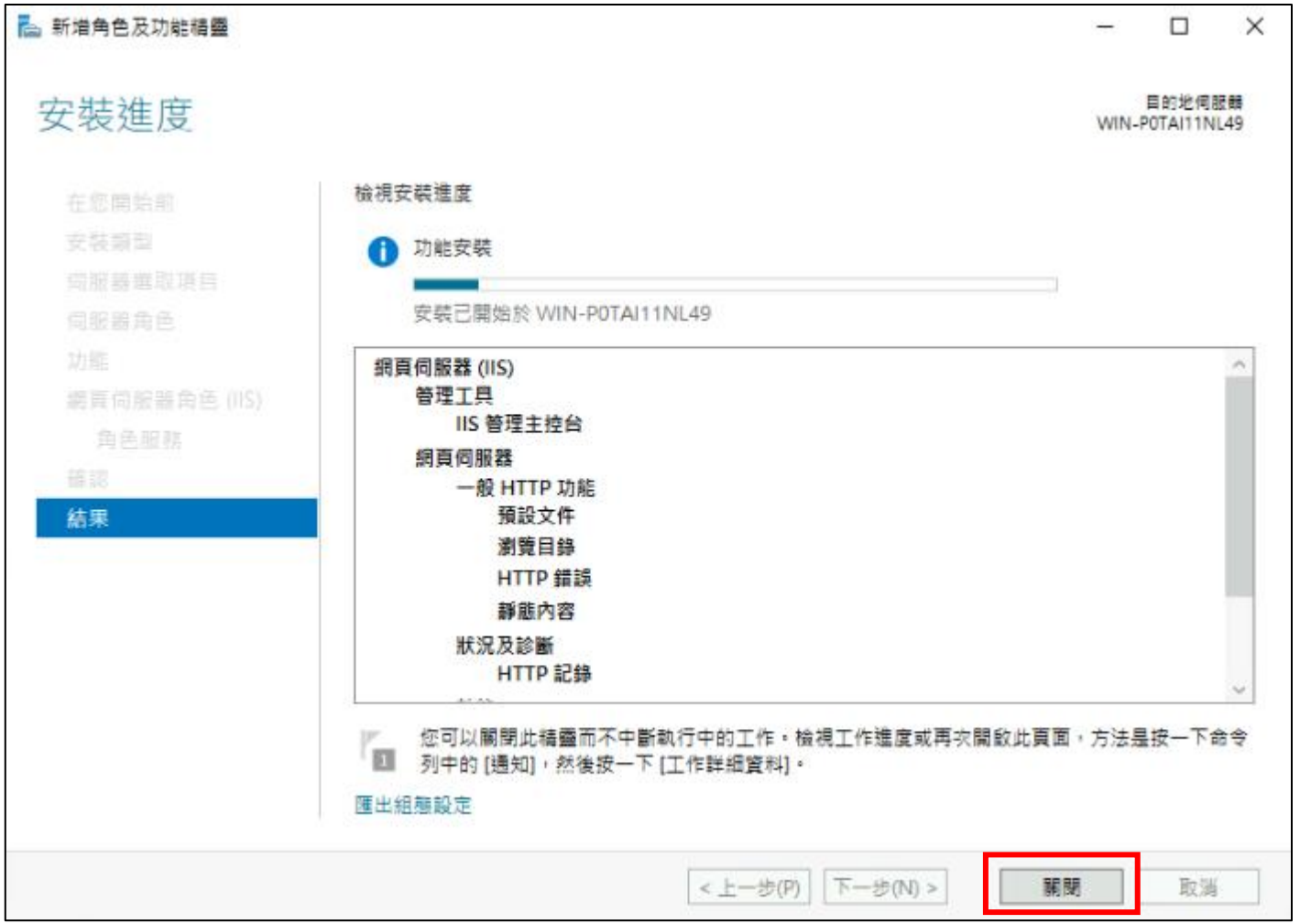
- 點擊”下一步”

Internet Information Services (IIS) 設定

- 點擊”安裝”

Internet Information Services (IIS) 設定

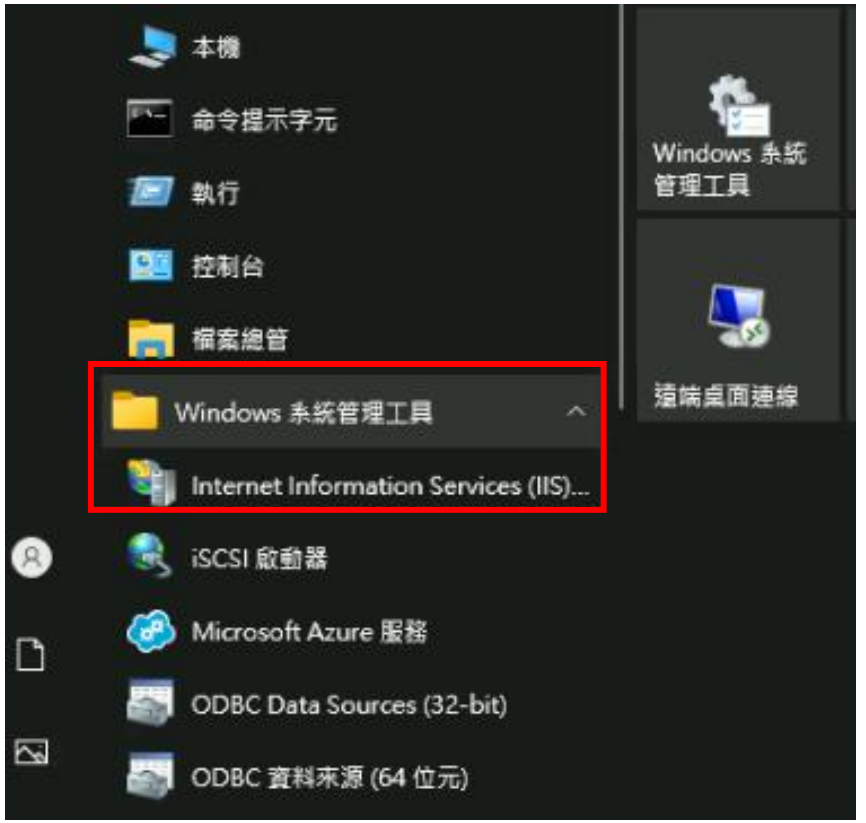
- 點擊”關閉”



Internet Information Services (IIS) 設定

- 點擊圖示或是打開Windows系統管理工具

  找到Internet Information Services (IIS) 管理員

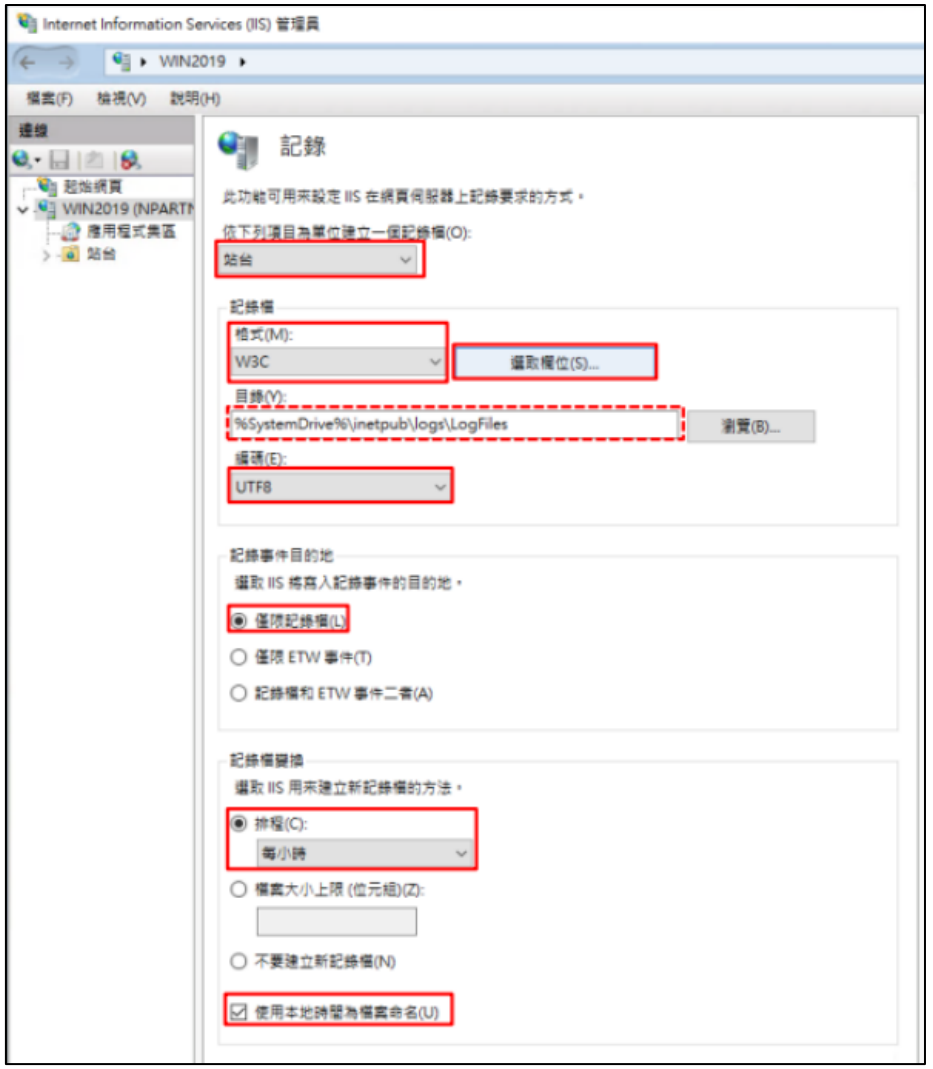


Internet Information Services (IIS) 設定

- 選擇 [IIS Server] -> 點選 [記錄]

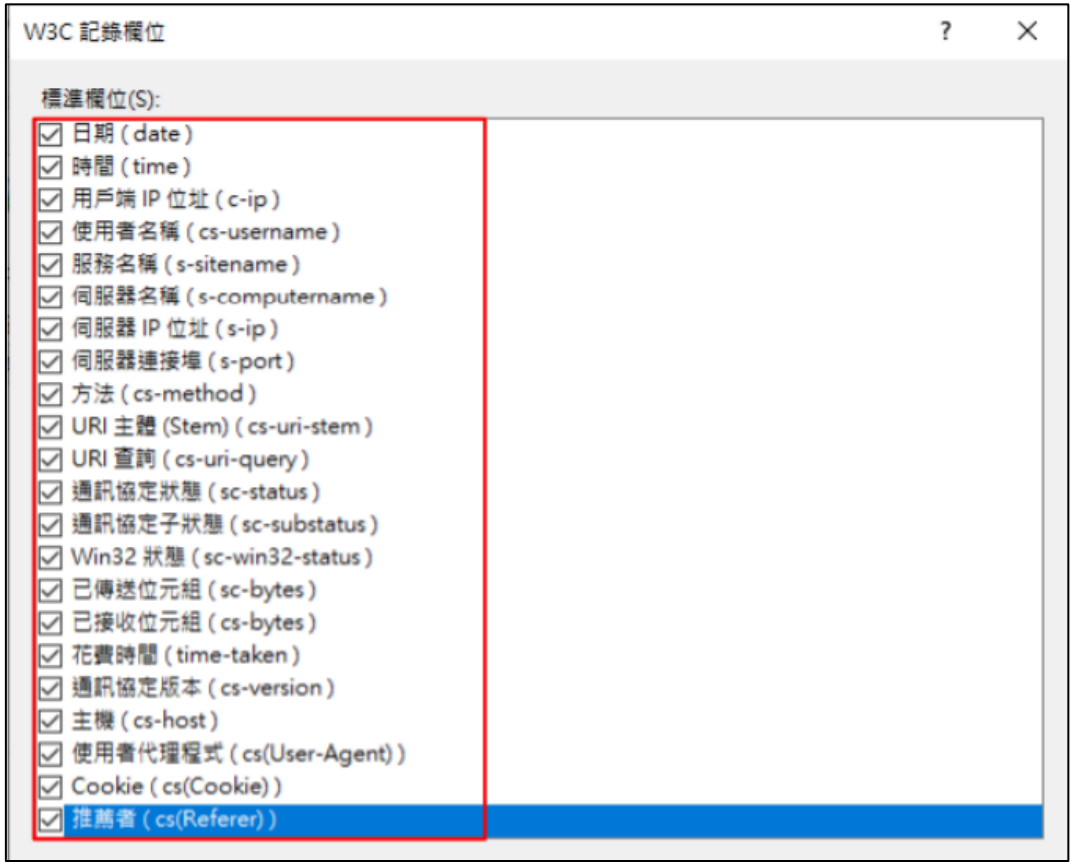
Internet Information Services (IIS) 設定

- 選擇依下列項目為單位建立一個記錄檔: [站台]
- 記錄檔格式: [W3C]
- 目錄: %SystemDrive%\inetpub\logs\LogFiles
- 編碼: [UTF-8]
- 記錄事件目的地: [僅限記錄檔]
- 排程: [每小時]
- 勾選 [使用本地時間為檔案命名]
- 按下 [選取欄位]



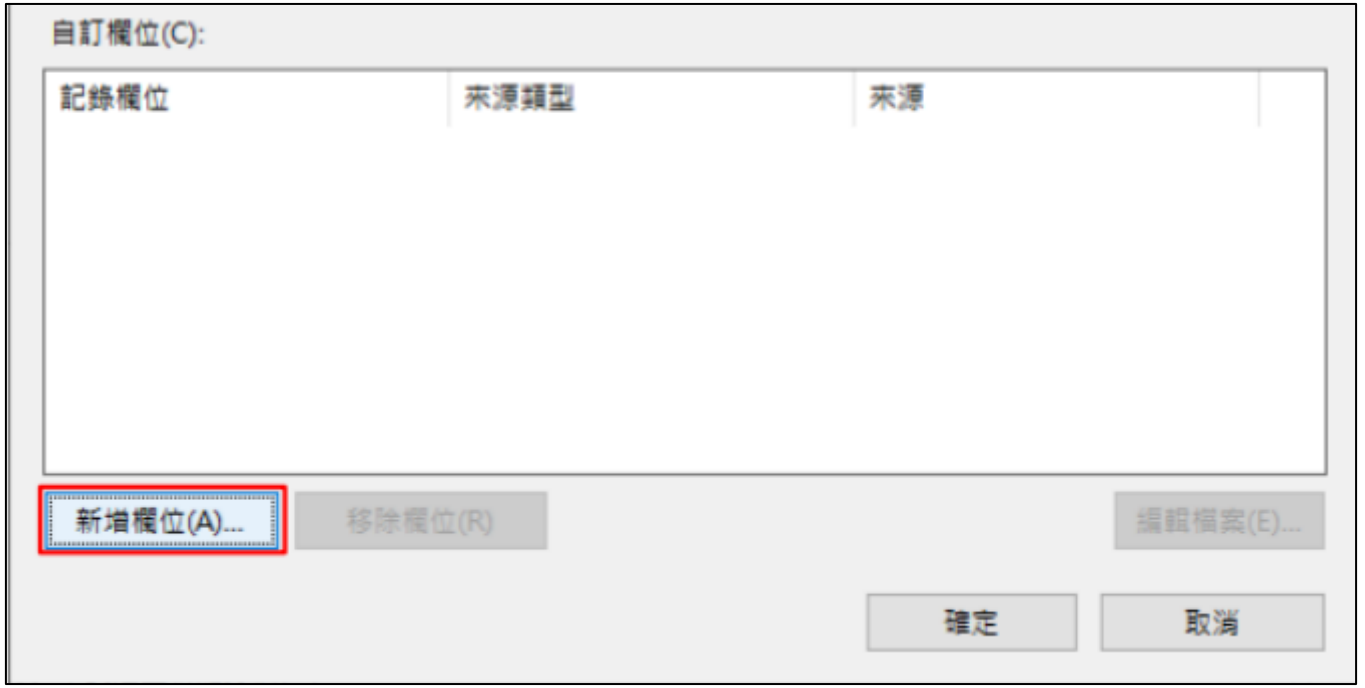
Internet Information Services (IIS) 設定

- 勾選 [日期 (date)]、[時間 (time)]、[用戶端 IP 位址 (c-ip)]、[使用者名稱 (cs-username)]、[服務名稱 (s-sitename)]、[伺服器名稱 (s-computername)]、[伺服器 IP 位址 (s-ip)]、[伺服器連接埠 (s-port)]、[方法 (cs-method)]、[URI 主體(csuri-stem)]、[URI 查詢 (cs-uri-query)]、[通訊協定狀態 (sc-status)]、[通訊協定子狀態 (sc-substatus)]、[Win32 狀態 (scwin32-status)]、[傳送位元組 (sc-bytes)]、[接收位元組 (cs-bytes)]、[花費時間 (time-taken)]、[通訊協定版本(csversion)]、[主機 (cs-host)]、[使用者代理 (cs(User-Agent))]、[Cookie(cs(Cookie))]、[推薦者 (cs(Referer))]



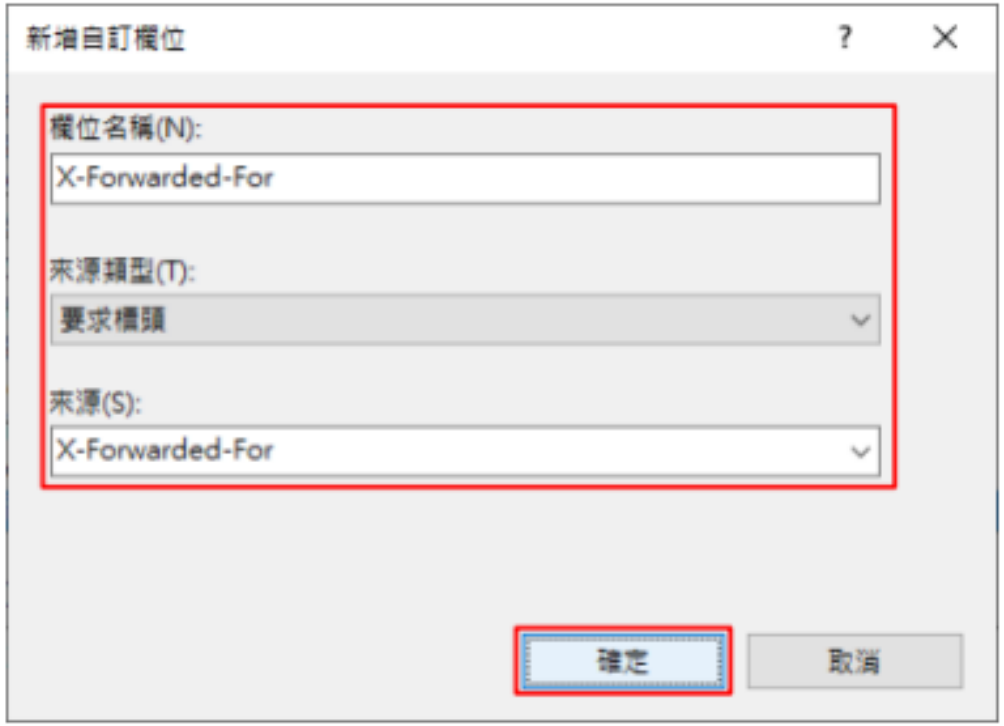
Internet Information Services (IIS) 設定

- 按下 [Add Field(新增欄位)]



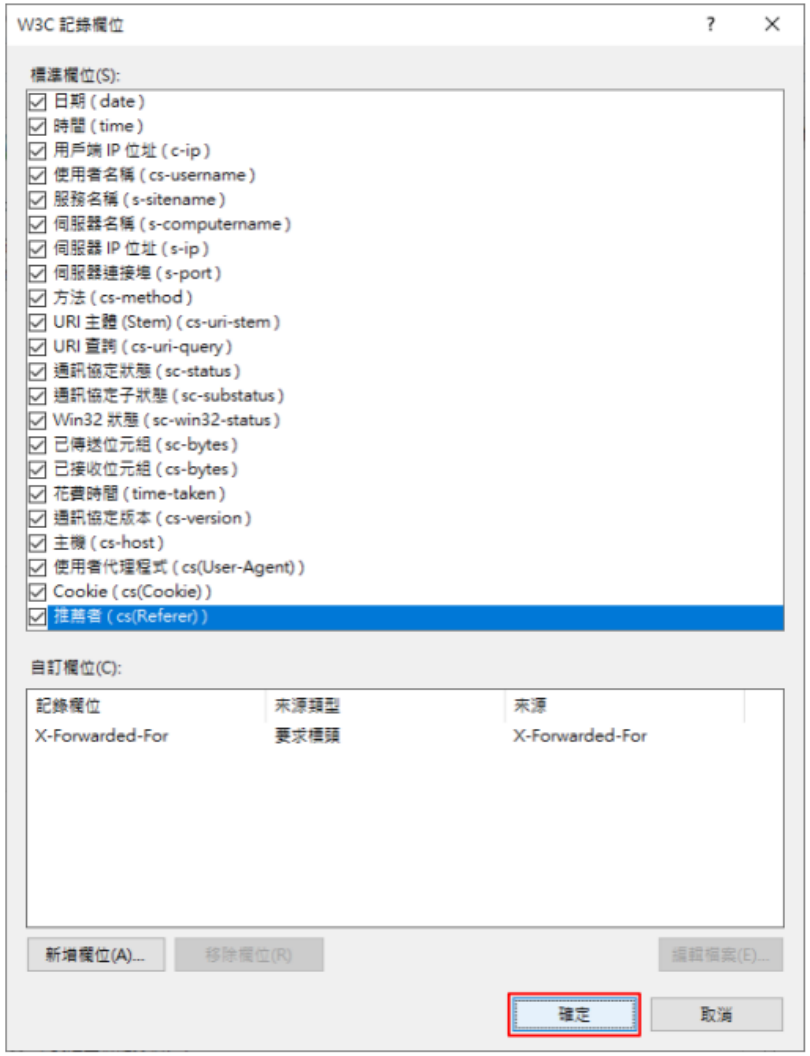
Internet Information Services (IIS) 設定

- 輸入欄位名稱: X-Forwarded-For
- 選擇來源類型: [Request Header(要求標頭)]
- 輸入來源: X-Forwarded-For
- 按下 [確定]



Internet Information Services (IIS) 設定

- 按下 [確定]

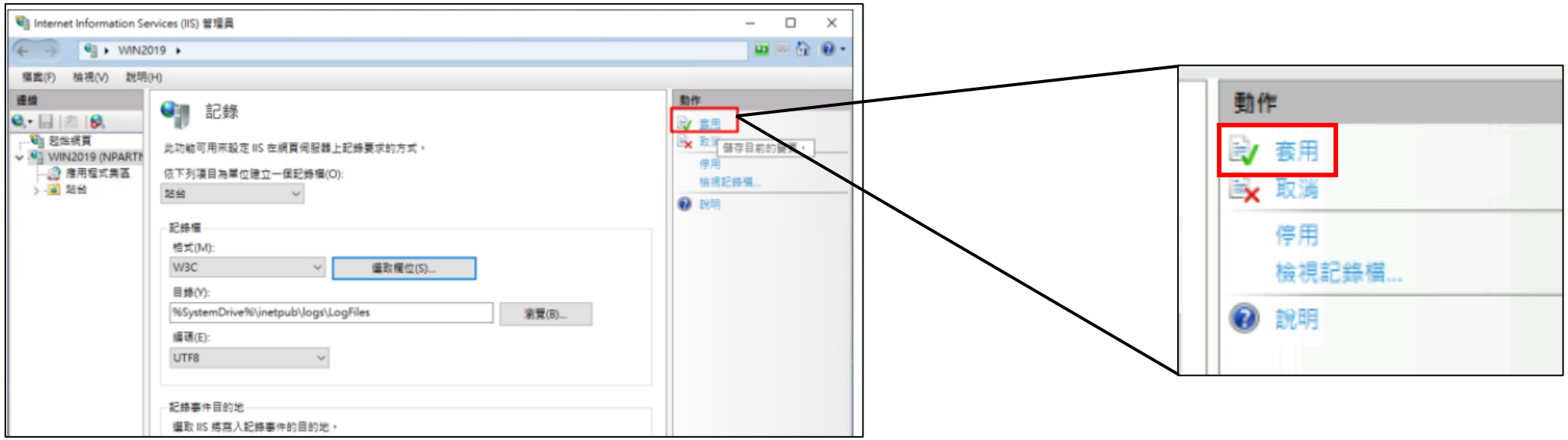


Internet Information Services (IIS) 設定

- 檢查設定是否正確無誤

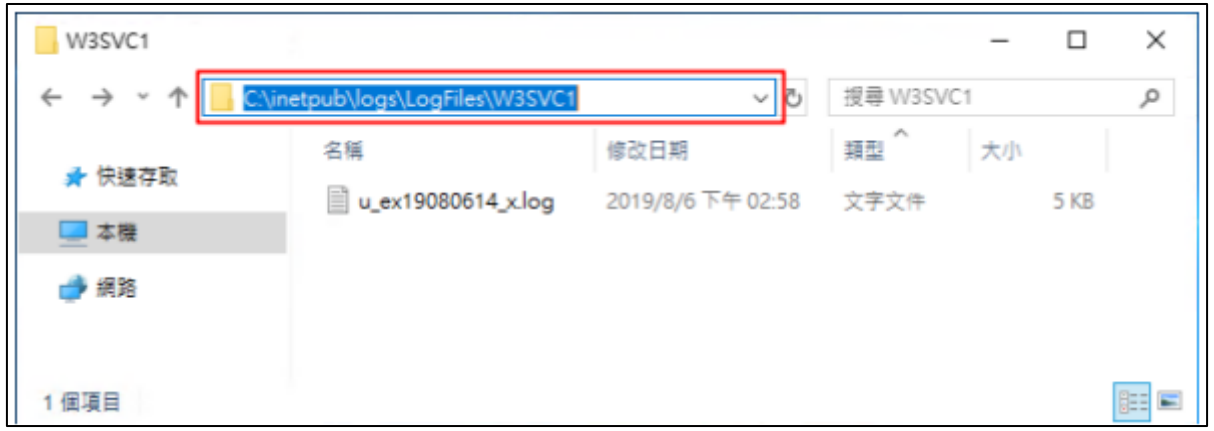
Internet Information Services (IIS) 設定

- 按下 [套用]



Internet Information Services (IIS) 設定

- 確認 [C:\Inetpub\logs\LogFiles\W3SVC1] 資料夾 IIS log 檔案: ex*.log



Linux syslog 轉發設定

- 適用 CentOS / Rocky / Redhat / Ubuntu
- 設定 rsyslog 轉發

Linux syslog 轉發設定

在/etc/rsyslog.d目錄底下，新增**110-forward.conf** 的設定檔

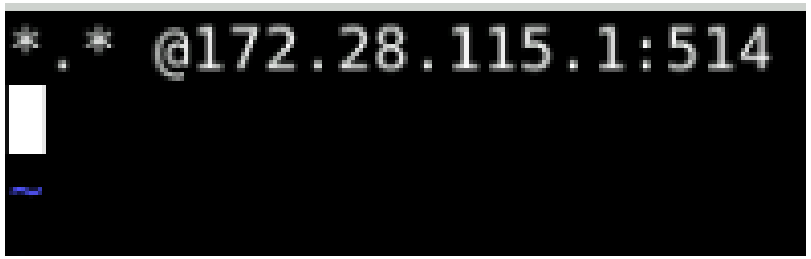
 # vim /etc/rsyslog.d/110-forward.conf

```
[root@CentOS9Kadm kadm]# vim /etc/rsyslog.d/110-forward.conf
[root@CentOS9Kadm kadm]#
```

Linux syslog 轉發設定

- 在設定檔 **110-forward.conf** 新增以下內容:

***.* @172.28.115.1:514**



- 新增完成後，儲存離開。

若使用者需要TCP 設定，可參考以下語法設定:

***.* @@172.28.115.1:514**

Linux syslog 轉發設定 (CentOS / Rocky / Redhat)

防火牆開放 514 port，並套用後查看防火牆列表 **(此指OS防火牆)**

 # firewall-cmd --add-port=514/udp --permanent

 # firewall-cmd --reload

 # firewall-cmd --list-ports

```
[root@CentOS9Kadm kadm]# firewall-cmd --list-ports
514/udp
```

Linux syslog 轉發設定 (Ubuntu)

防火牆開放 514 port，並套用後查看防火牆列表

 # sudo ufw allow 514/udp

 # sudo ufw status

Linux syslog 轉發設定

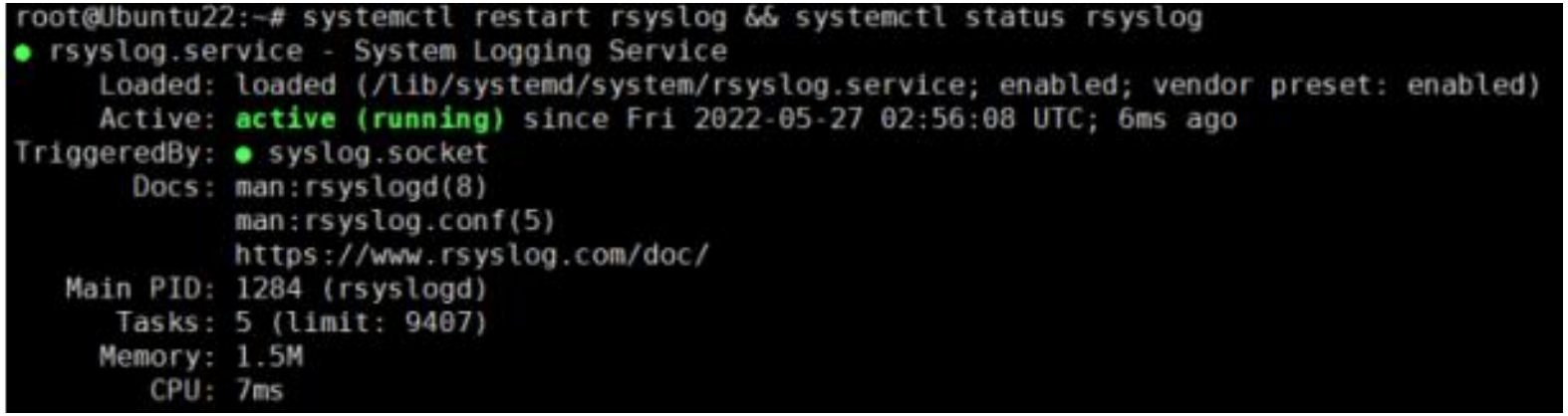
- SElinux 設定(啟用NIS相關存取，放寬 SElinux policy 限制)
- **此設定適用於預設開啟 SELinux 者 (CentOS / Rocky / Redhat)**
- **若 Ubuntu 有開啟 SELinux，也須做 SELinux 放寬限制設定**

 # setsebool -P nis_enabled 1

Linux syslog 轉發設定

重新啟動 rsyslog 服務和確認服務正常

 # systemctl restart rsyslog && systemctl status rsyslog



N-Cloud 設定完成

- Windows IIS Log 設定
- Linux syslog 設定

NXLog 安裝常見問題

測試方法及解決步驟**供參考**

常見問題 1

- 測試Linux環境拋送syslog是否正常，可輸入以下指令測試。

 # sudo tcpdump -i any port 514

- 若有看到 ”**本機的IP > 172.28.115.1**” 相關的資訊，
  代表有成功將syslog轉發至N-Cloud。(需等待一下)

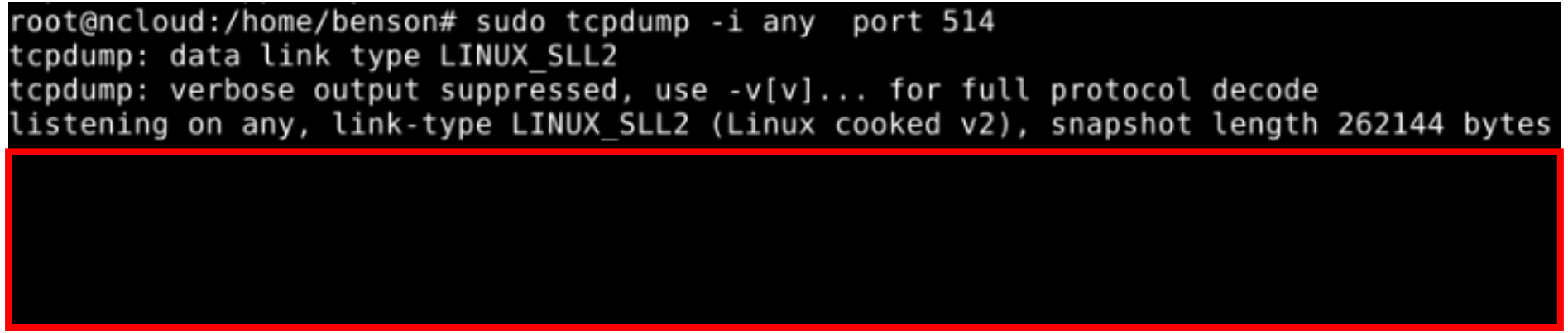
```
root@ncloud:/home/benson# sudo tcpdump -i any port 514
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
15:20:23.586182 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 112
15:20:23.586210 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 108
15:20:23.586222 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 113
15:20:23.586398 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 102
15:20:23.586700 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 125
15:20:23.587140 ens33 Out IP 172.28.195.107.60038 > 172.28.115.1.syslog: SYSLOG local6.notice, length: 104
```

(成功轉發)

常見問題 2

- 若未看到 ”**本機IP > 172.28.115.1**”相關資訊，可參考以下方法測試

1. 可以檢查防火牆狀態及設置內容
2. 若有啟用SELinux者，須放寬限制設定



(轉發未成功-無Log資訊)

常見問題 3

- 在測試Linux轉發Log時，若syslog的訊息量不多，可以嘗試發送以下測試指令，主動觸發 syslog 拋送。

  # logger “SYSLOG TEST”

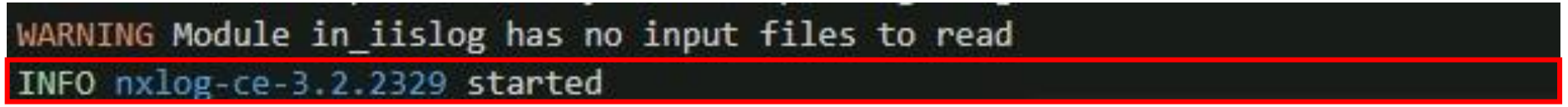
常見問題 4

- 安裝 Windows機器檢查Log時，若是沒有設定IIS服務的主機，可能會出現下列紅框內的提醒訊息，此為正常現象!

```
WARNING stopping nxlog service
WARNING nxlog-ce received a termination request signal, exiting...
ERROR failed to open directory: C:\inetpub\logs\LogFiles\: 系統找不到指定的路徑。
WARNING Module in_iislog has no input files to read
INFO nxlog-ce-3.2.2329 started
```

常見問題 5

- 在 Windows機器上完成NXLog安裝，在Log中主要檢查nxlog是否能正常啟動! (如紅框內訊息)



- 若無法正常啟動NXLog服務，可參考以下步驟排查錯誤。

  建議重新載入NXLog套件、重新套用設定檔，並重新啟動服務。