遠端桌面連線設定指引

東海大學 圖書暨資訊處

TUNGHAI 東海大學圖書暨資訊處
OFFICE OF LIBRARY AND INFORMATION SERVICES, TUNGHAI UNIVERSITY

前言

本文件適合的對象

如果您負責管理Windows伺服器或是配合的協助廠商需要透過遠端桌面管理Windows伺服器主機，則您可以參考本文件做遠端桌面的相關設定及加強遠端桌面的連線安全性。

但我們不建議在一般的行政辦公電腦上面開啟遠端桌面服務，未來我們也有可能針對全校的遠端桌面服務做出網路連線上的限制，所以請盡可能不要在您的個人電腦上面開啟遠端桌面服務，以避免造成個人資訊安全上面的危害。

★・取消遠端桌面服務可考本文件第四頁的說明。

Agenda

如何啟用Windows 遠端桌面

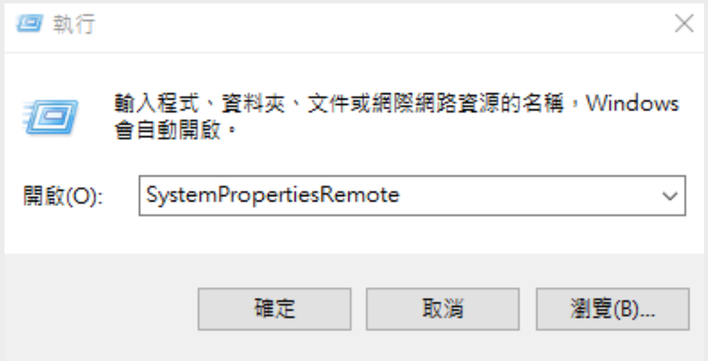
如何設定遠端桌面之防火牆

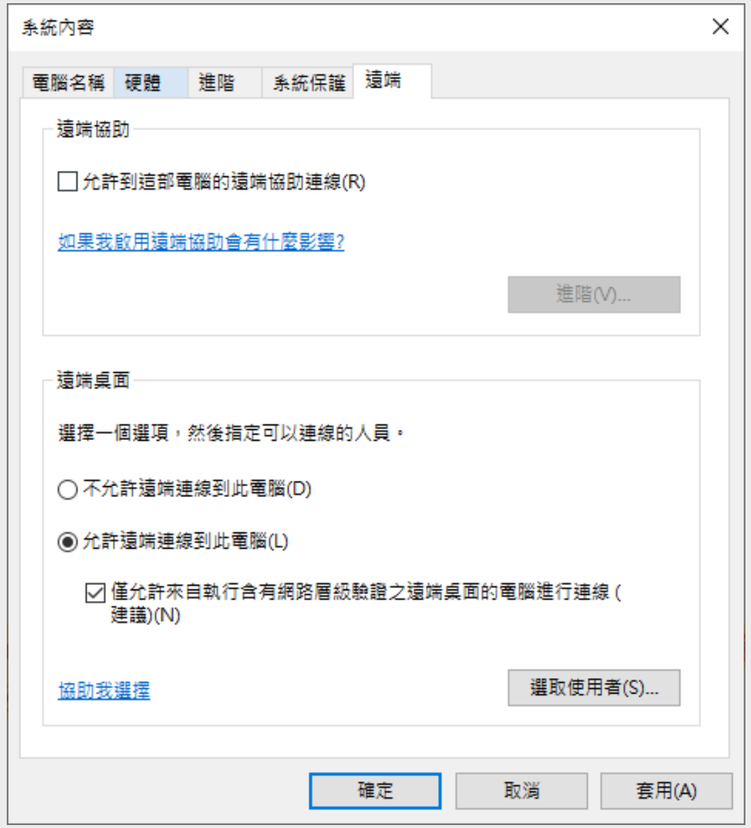
如何查看遠端桌面連線紀錄

如何啟用及取消Windows 遠端桌面

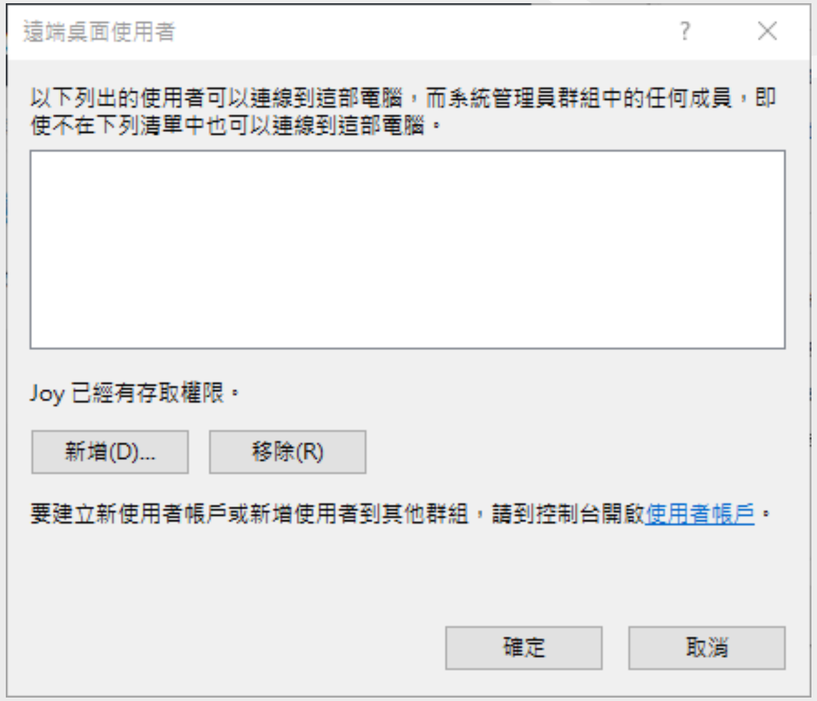
1、請用鍵盤快速鍵 ⊞ + R
叫出執行後輸入：

SystemPropertiesRemote





☆．如您要取消遠端桌面服務，請在這裡選擇「不允許連接到此電腦」。



啟用遠端桌面連線後，預設會讓系統管理員可以連線登入，如主機上有其他帳號，也可另外新增。

更改遠端桌面的連線服務Port

更改遠端桌面連接埠號碼能有效提升遠端存取的安全性。駭客常攻擊已知的預設3389埠號,改用非標準埠號可大幅增加他們猜測正確埠號的難度。此外，許多駭客自動掃描工具也會鎖定3389埠號進行入侵，改用其他埠號能有效迴避這類攻擊行為。

1、直接在開始功能表找到PowerShell，並選擇「以系統管理員身分執行」

2、輸入以下指令更改預設的連線埠號(33900數字為示範用)

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'PortNumber' -Value 33900
```

3、檢查目前的設定

```
get-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -Name 'PortNumber'
```

```
PortNumber     : 33900
PSPath         : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\Cur
PSParentPath   : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\Cur
PSChildName    : RDP-Tcp
PSDrive        : HKLM
PSProvider     : Microsoft.PowerShell.Core\Registry
```

設定遠端桌面之防火牆

預設在啟用遠端桌面後，Windows會自動設定內建的防火牆規則，但由於我們在前面更改了遠端桌面的連線服務埠後，預設的規則並不會自動修正，故我們仍須自行手動修改規則。

(我們不建議開放任意來源IP連線，故以下範例為僅設定單一來源IP允許連線，個人家用IP或廠商連線IP請自行查閱)

1、直接在開始功能表找到PowerShell，並選擇「以系統管理員身分執行」

2、輸入以下指令新增防火牆規則

(參數如下說明，請自行修改為自已要的)

```
New-NetFirewallRule -DisplayName "自訂義遠端桌面連線規則" -Direction Inbound -Protocol TCP -LocalPort 33900 -Action Allow -Profile Any -RemoteAddress 100.100.100.100
```

這條指令的各個參數解釋如下：

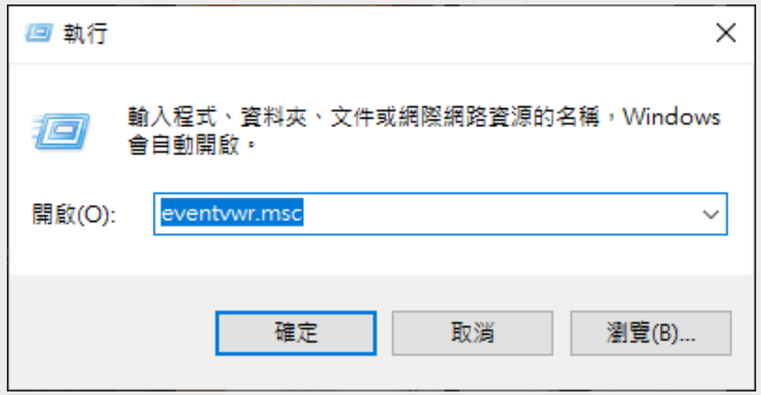
- DisplayName 是防火牆規則的顯示名稱。
- Direction 指定規則的方向，設定為 Inbound
- Protocol 指定規則適用的協定，使用 TCP
- LocalPort 指定本機端口，設定為 33900
- Action 設定為 Allow，表示允許通過
- Profile 設定為 Any，表示此規則適用於所有的防火牆設定檔
- RemoteAddress 指定允許連入的遠端 IP 地址。

檢查遠端桌面連線紀錄

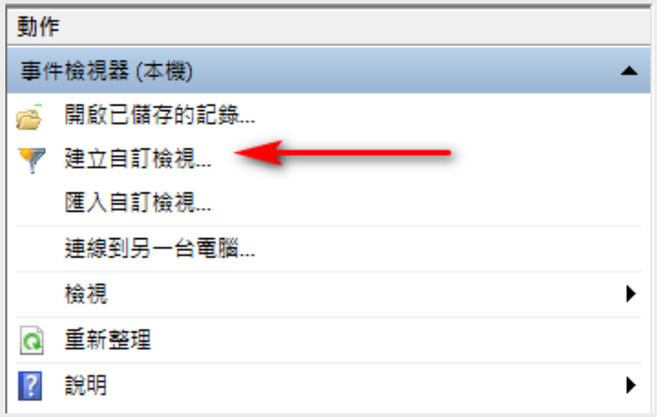
定期檢查主機的遠端桌面連線紀錄有助於防止和發現未經授權的連線，確保只有授權的來源和使用者能夠進行遠端連線，提高主機系統的安全性。這能夠及時採取防範措施，保護敏感資料和系統免受未授權存取的風險。

1、請用鍵盤快速鍵 ⊞ + R 叫出執行後輸入：

```
eventvwr.msc
```

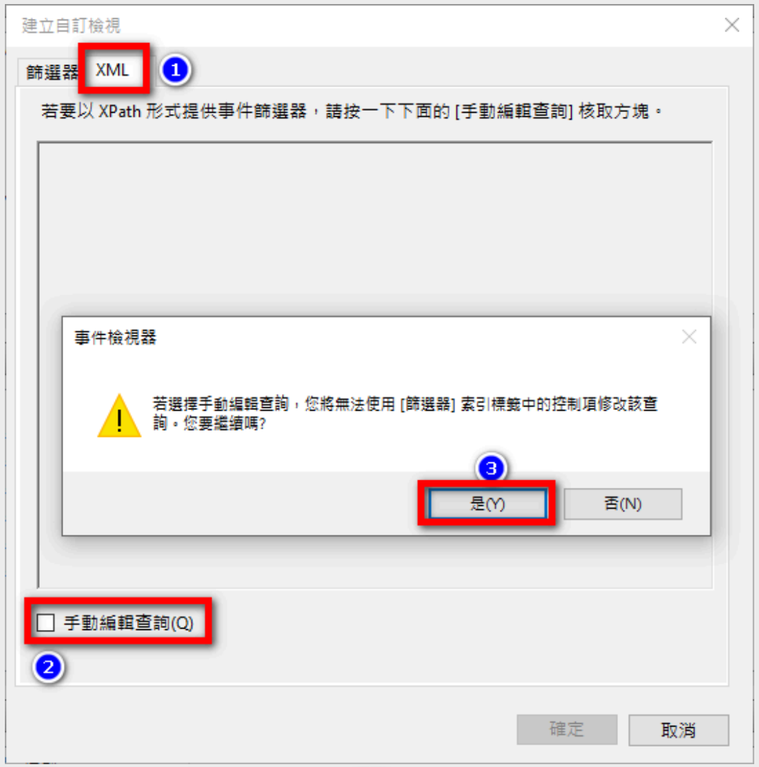


2、建立一個自訂檢視（專門查看遠端桌面連線紀錄用）



3、設定自訂檢視

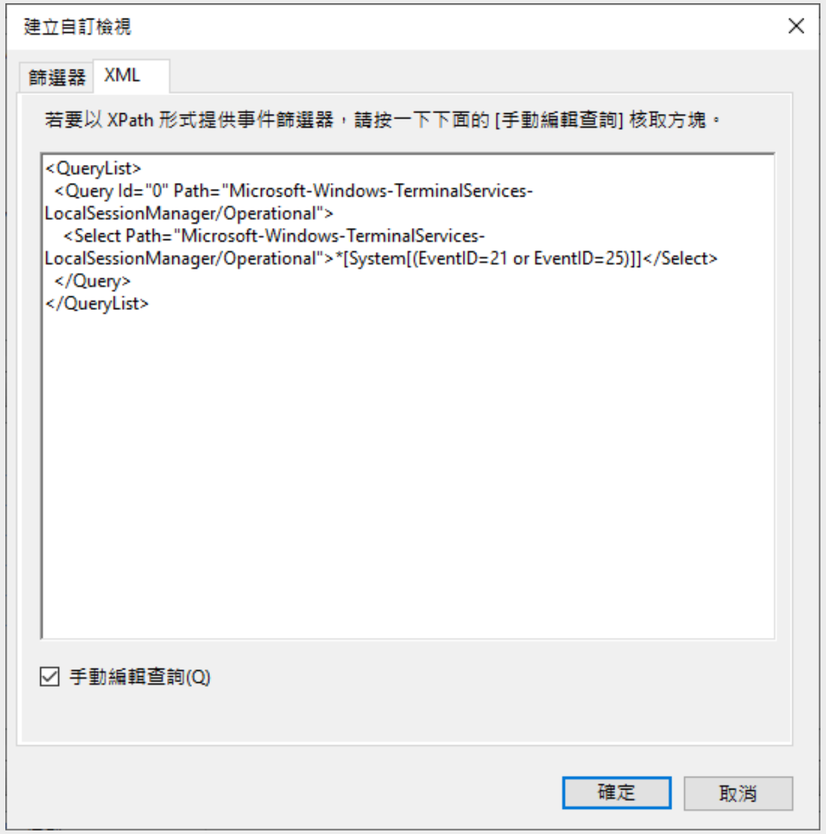
切換到「XML」頁籤，並勾選手動編輯查詢



事件檢視-自訂檢視XML內容

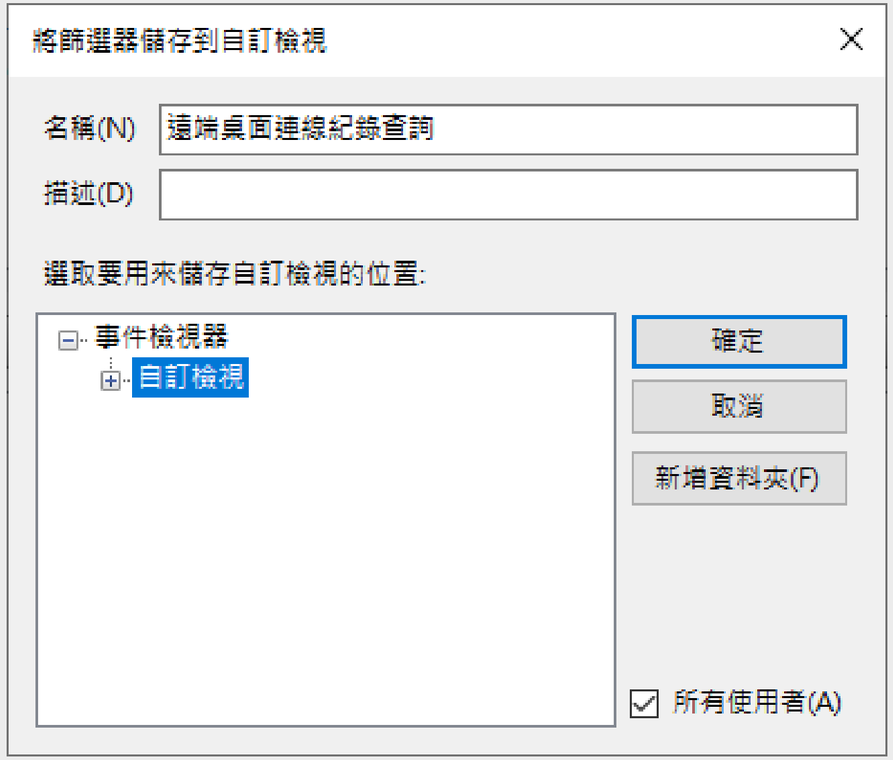
貼上如下XML設定：

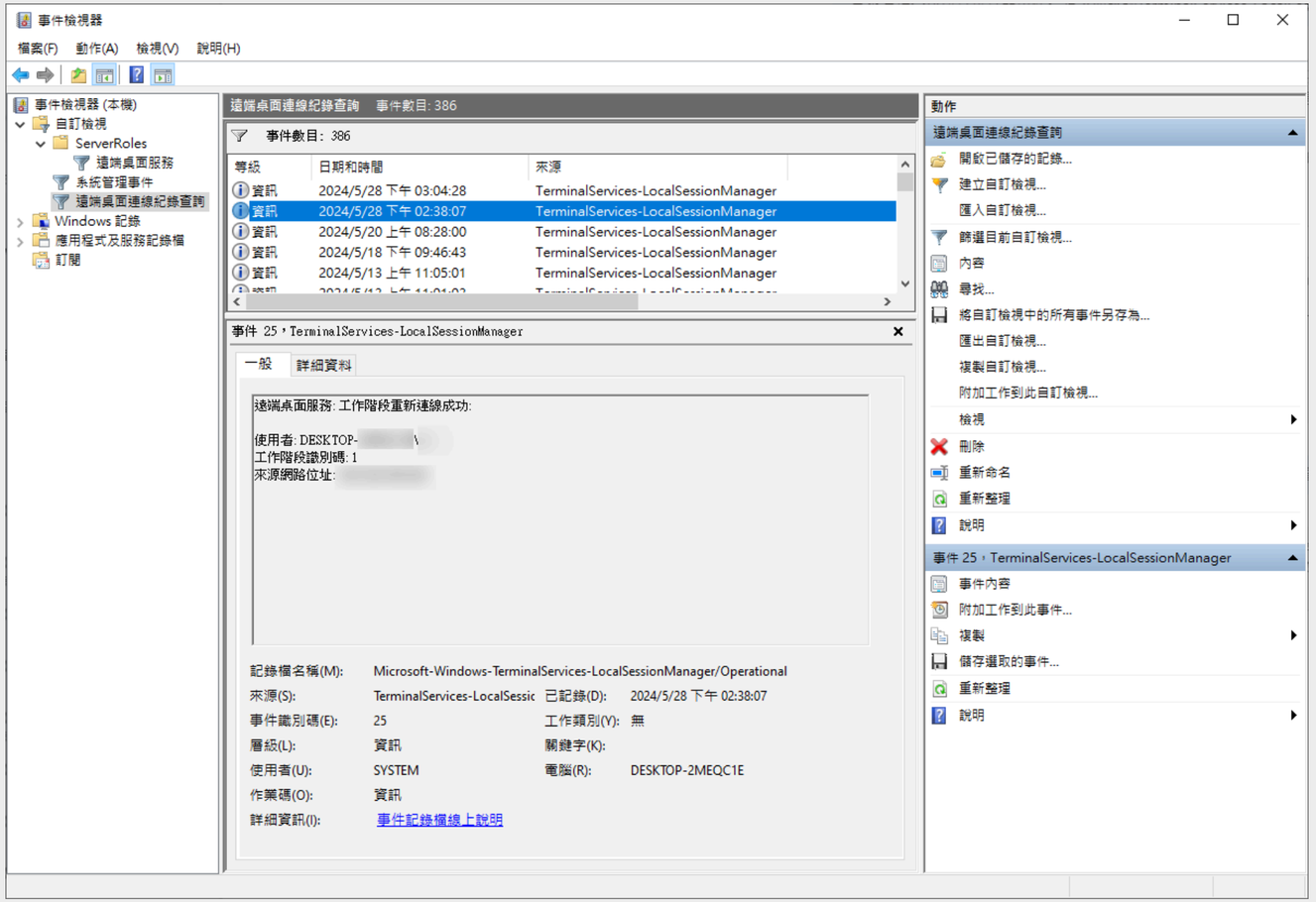
```
<QueryList>
  <Query Id="0" Path="Microsoft-Windows-TerminalServices-LocalSessionManager/Operational">
    <Select Path="Microsoft-Windows-TerminalServices-LocalSessionManager/Operational">*[System[(EventID=21 or EventID=25)]]</Select>
  </Query>
</QueryList>
```



事件檢視-自訂檢視XML內容

給予自訂檢視一個「名稱」後按下確定，後續就可以在事件檢視器中的自訂檢視查看遠端桌面連線紀錄。





THANK YOU

東海大學圖書暨資訊處
OFFICE OF LIBRARY AND INFORMATION SERVICES,
TUNGHAI UNIVERSITY