

Partner

RADIUS / LDAP

認證使用說明

V006

2022/04/25



版權聲明

N-Partner Technologies Co.版權所有。未經 N-Partner Technologies Co.書面許可，不得以任何形式仿製、拷貝、謄抄或轉譯本手冊的任何內容。由於產品一直在更新中， N-Partner Technologies Co. 保留不告知變動的權利。

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言	2
1. RADIUS 配置	4
1.1 Linux 版本	4
1.1.1 安裝 FreeRADIUS 套件	4
1.1.2 創建 Dictionary 文件	5
1.1.3 設定服務連線資訊.....	6
1.1.4 設定使用者認證帳號密碼.....	7
1.1.5 啟動 RADIUS 服務.....	8
2.1 Windows 版本	9
2.1.1 安裝 NPS 網路原則伺服器	9
2.1.2 設定 NPS 整合 AD 驗證	10
2.1.3 設定 RADIUS 用戶端	12
2.1.4 設定連線要求原則.....	14
2.1.5 設定網路原則.....	22
2.1.6 查看 AD 使用者.....	50
2. LDAP 配置	53
2.1 設定 Windows AD 帳戶資料.....	53
3. N-Cloud / N-Reporter 配置	57
3.1 RADIUS 設定	57
3.1.1 設定服務連線資訊.....	57
3.1.2 登入	58
3.2 LDAP 設定.....	59
3.2.1 設定服務連線資訊.....	59
3.2.2 登入	60
3.2.3 網頁後台更改帳戶權限	61

前言

本文件描述如何配置 RADIUS / LDAP 與 N-Cloud / N-Reporter 做 RADIUS / LDAP 認證。

N-Cloud / N-Reporter 版本 6.1.142

測試環境：

CentOS 8 / Debian 10 安裝 FreeRADIUS 套件。

Windows 2022 設定 NPS(RADIUS)。

Windows 2019 設定 Active Directory 帳戶。

A decorative frame consisting of two L-shaped brackets. The top-left bracket is orange and yellow, and the bottom-right bracket is green and blue. They are positioned around the chapter title text.

Chapter 1

RADIUS 配置



1. RADIUS 配置

1.1 Linux 版本

1.1.1 安裝 FreeRADIUS 套件

CentOS 8

(1) 安裝 FreeRADIUS 套件

```
# dnf -y install freeradius freeradius-utils
```

(2) 查看 FreeRADIUS 版本

```
# radiusd -v
```

```
[root@CentOS8 ~]# radiusd -v
radiusd: FreeRADIUS Version 3.0.20, for host x86_64-redhat-linux-gnu
FreeRADIUS Version 3.0.20
Copyright (C) 1999-2019 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYRIGHT
[root@CentOS8 ~]#
```

Debian 10

(1) 安裝 FreeRADIUS 套件

```
# apt -y install freeradius freeradius-utils
```

(2) 查看 FreeRADIUS 版本

```
# freeradius -v
```

```
root@debian10:~# freeradius -v
radiusd: FreeRADIUS Version 3.0.17, for host x86_64-pc-linux-gnu, built on Apr 22 2019 at 21:23:36
FreeRADIUS Version 3.0.17
Copyright (C) 1999-2017 The FreeRADIUS server project and contributors
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE
You may redistribute copies of FreeRADIUS under the terms of the
GNU General Public License
For more information about these matters, see the file named COPYRIGHT
```

1.1.2 創建 Dictionary 文件

(1) Dictionary 文件中，定義各廠商特有的參數名稱，與其對應的數值及型態，此參數名稱用於解析 RADIUS 封包中的參數並顯示於 Debug 模式或是 Log 檔中。

```
# vi /usr/share/freeradius/dictionary.npartner
# -*- text -*-
# Copyright (C) 2015 The FreeRADIUS Server project and contributors
#####
#
#       N-Partner attributes
#
#       $Id$
#####
VENDOR          N-Partner          39693
BEGIN-VENDOR    N-Partner

ATTRIBUTE       N-Partner-Domain   1      integer
ATTRIBUTE       N-Partner-Menu     2      integer
ATTRIBUTE       N-Partner-Email    3      string

END-VENDOR N-Partner
```

```
# -*- text -*-
# Copyright (C) 2015 The FreeRADIUS Server project and contributors
#####
#
#       N-Partner attributes
#
#       $Id$
#####
VENDOR          N-Partner          39693
BEGIN-VENDOR    N-Partner

ATTRIBUTE       N-Partner-Domain   1      integer
ATTRIBUTE       N-Partner-Menu     2      integer
ATTRIBUTE       N-Partner-Email    3      string

END-VENDOR N-Partner
```

(2) 編輯 dictionary 檔

CentOS 8

```
# vi /etc/raddb/dictionary
```

Debian 10

```
# vi /etc/freeradius/3.0/dictionary
```

(3) 檔案最下方新增載入 dictionary.npartner 文件

```
$INCLUDE /usr/share/freeradius/dictionary.npartner
```

1.1.3 設定服務連線資訊

請於檔案最下方定義 N-Cloud / N-Reporter 與 RADIUS server 連線時的共享密鑰 Secret Key · IP 為 N-Cloud / N-Reporter 對外 IP。

CentOS 8

```
# vi /etc/raddb/clients.conf
```

Debian 10

```
# vi /etc/freeradius/3.0/clients.conf
```

檔案最下方設定服務連線資訊

```
client n-reporter{  
    ipaddr = 192.168.8.4  
    secret = npartner  
    shortname = npartner  
}
```

```
client n-reporter{  
    ipaddr = 192.168.8.4  
    secret = npartner  
    shortname = npartner  
}
```

紅色文字部位請輸入 N-Cloud / N-Reporter 系統 IP address 和共享密鑰 Secret Key

1.1.4 設定使用者認證帳號密碼

請設定使用者於 RADIUS server 認證的帳號及密碼，並定義此使用者的領域管理 ID、選單樣版 ID、E-Mail，前兩者可於 N-Cloud / N-Reporter 的領域管理及使用者總表中查詢。

CentOS 8

```
# vi /etc/raddb/users
```

Debian 10

```
# vi /etc/freeradius/3.0/users
```

檔案最下方設定使用者認證帳號密碼

```
npartner Cleartext-Password := "npartner"  
    Reply-Message = "RADIUS npartner",  
    N-Partner-Domain = 1001,  
    N-Partner-Menu = 2,  
    N-Partner-Email = "npartner@npartner.local"
```

```
npartner Cleartext-Password := "npartner"  
    Reply-Message = "RADIUS npartner",  
    N-Partner-Domain = 1001,  
    N-Partner-Menu = 2,  
    N-Partner-Email = "npartner@npartner.local"
```

紅色文字部位請輸入認證帳號密碼和領域管理 ID(N-Partner-Domain)和選單樣版 ID(N-Partner-Menu)

1.1.5 啟動 RADIUS 服務

如 RADIUS 認證上有問題，可查詢 RADIUS Log 檔。

CentOS 8

(1) 啟動服務

```
# systemctl restart radiusd && systemctl status radiusd
```

```
[root@CentOS8 ~]# systemctl restart radiusd && systemctl status radiusd
● radiusd.service - FreeRADIUS high performance RADIUS server.
   Loaded: loaded (/usr/lib/systemd/system/radiusd.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2021-10-27 17:11:04 CST; 6ms ago
     Process: 6546 ExecStart=/usr/sbin/radiusd -d /etc/raddb (code=exited, status=0/SUCCESS)
     Process: 6542 ExecStartPre=/usr/sbin/radiusd -C (code=exited, status=0/SUCCESS)
     Process: 6533 ExecStartPre=/bin/sh /etc/raddb/certs/bootstrap (code=exited, status=0/SUCCESS)
     Process: 6532 ExecStartPre=/bin/chown -R radiusd.radiusd /var/run/radiusd (code=exited, status=0/SUCCESS)
   Main PID: 6548 (radiusd)
     Tasks: 6 (limit: 11514)
    Memory: 77.0M
     CGroup: /system.slice/radiusd.service
            └─6548 /usr/sbin/radiusd -d /etc/raddb

Oct 27 17:11:04 CentOS8.localdomain systemd[1]: Stopped FreeRADIUS high performance RADIUS server..
Oct 27 17:11:04 CentOS8.localdomain systemd[1]: Starting FreeRADIUS high performance RADIUS server...
Oct 27 17:11:04 CentOS8.localdomain sh[6533]: server.pem: OK
Oct 27 17:11:04 CentOS8.localdomain systemd[1]: Started FreeRADIUS high performance RADIUS server..
[root@CentOS8 ~]#
```

(2) 設定開機自動啟動 radiusd 服務

```
# systemctl enable radiusd
```

```
[root@CentOS8 ~]# systemctl enable radiusd
Created symlink /etc/systemd/system/multi-user.target.wants/radiusd.service → /usr/lib/systemd/system/radiusd.service.
[root@CentOS8 ~]#
```

(3) 查看 Log 檔

```
# tail /var/log/radius/radius.log
```

Debian 10

(1) 啟動服務

```
# systemctl restart freeradius && systemctl status freeradius
```

```
root@debian10:~# systemctl restart freeradius && systemctl status freeradius
● freeradius.service - FreeRADIUS multi-protocol policy server
   Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-07-20 03:31:57 EDT; 5ms ago
     Docs: man:radiusd(8)
           man:radiusd.conf(5)
           http://wiki.freeradius.org/
           http://networkradius.com/doc/
     Process: 775 ExecStartPre=/usr/sbin/freeradius $FREERADIUS_OPTIONS -Cxm -lstdout (code=exited, status=0/SUCCESS)
     Process: 777 ExecStart=/usr/sbin/freeradius $FREERADIUS_OPTIONS (code=exited, status=0/SUCCESS)
   Main PID: 779 (freeradius)
     Tasks: 6 (limit: 2354)
    Memory: 9.7M
     CGroup: /system.slice/freeradius.service
            └─779 /usr/sbin/freeradius

Jul 20 03:31:57 debian10 freeradius[775]: [/etc/freeradius/3.0/mods-config/attr_filter/access_reject]:ll Check item "Freeradius-Response-Delay-Usec" found in filter list for realm "
Jul 20 03:31:57 debian10 freeradius[775]: tls: Using cached TLS configuration from previous invocation
Jul 20 03:31:57 debian10 freeradius[775]: rlm_cache (cache_eap): Driver rlm_cache_rbtree (module rlm_cache_rbtree) loaded and linked
Jul 20 03:31:57 debian10 freeradius[775]: Ignoring "sql" (see raddb/mods-available/README.rst)
Jul 20 03:31:57 debian10 freeradius[775]: Ignoring "ldap" (see raddb/mods-available/README.rst)
Jul 20 03:31:57 debian10 freeradius[775]: # Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:331
Jul 20 03:31:57 debian10 freeradius[775]: radiusd: ### Skipping IP addresses and Ports ###
Jul 20 03:31:57 debian10 freeradius[775]: Configuration appears to be OK.
Jul 20 03:31:57 debian10 systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

(2) 設定開機自動啟動 freeradius 服務

```
# systemctl enable freeradius
```

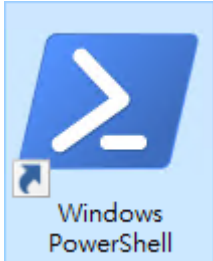
(3) 查看 Log 檔

```
# tail /var/log/freeradius/radius.log
```

2.1 Windows 版本

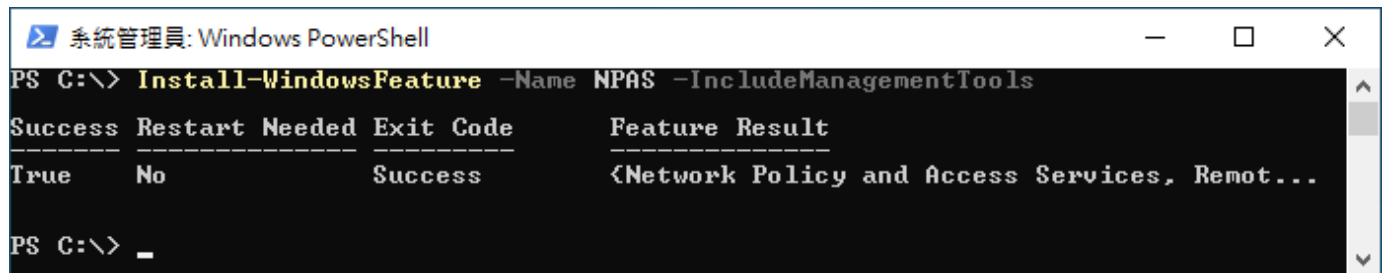
2.1.1 安裝 NPS 網路原則伺服器

(1) 開啟 [Windows PowerShell]



(2) 安裝 [網路原則伺服器]

```
PS C:\> Install-WindowsFeature -Name NPAS -IncludeManagementTools
```

A screenshot of a Windows PowerShell window titled "系統管理員: Windows PowerShell". The window shows the execution of the command `Install-WindowsFeature -Name NPAS -IncludeManagementTools`. The output is a table with the following content:

Success	Restart Needed	Exit Code	Feature Result
True	No	Success	<Network Policy and Access Services, Remot...

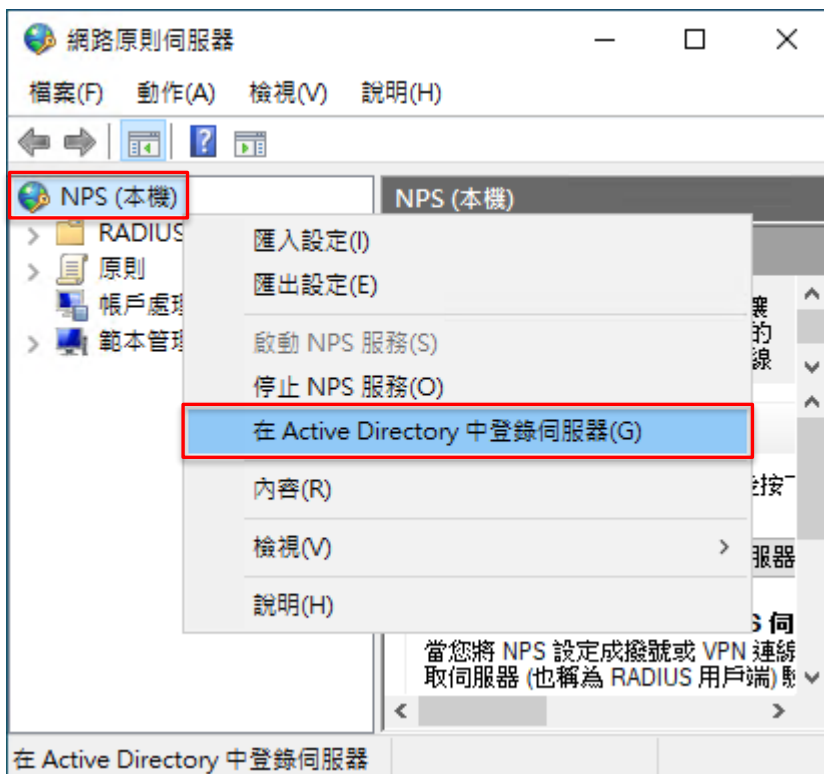
The window also shows the prompt `PS C:\> _` at the bottom.

2.1.2 設定 NPS 整合 AD 驗證

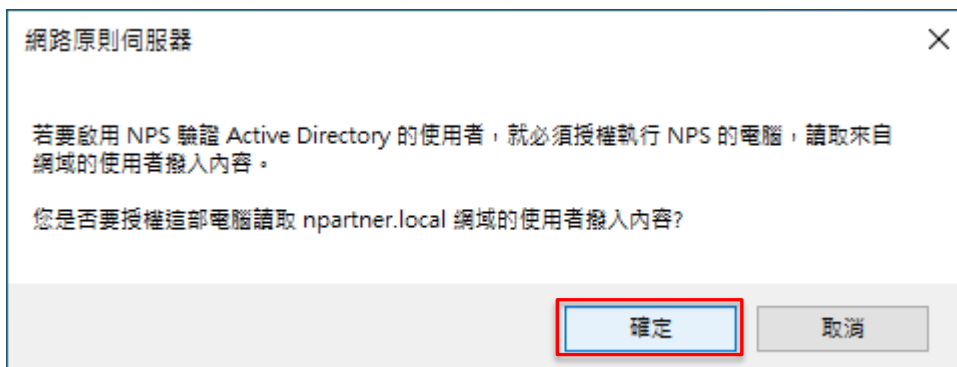
(1) 開啟 [網路原則伺服器]



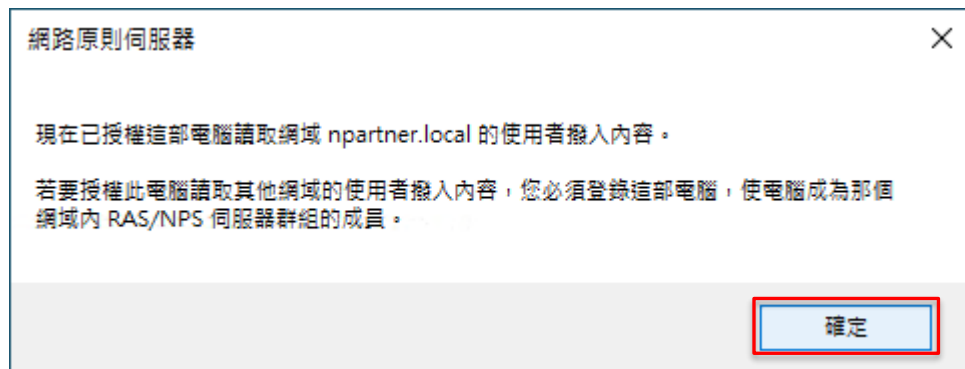
(2) 將 NPS 整合 AD 帳號做為驗證使用； [NPS (本機)] 按滑鼠右鍵 -> 點選 [在 Active Directory 中登錄伺服器]



(3) 授權 NPS 電腦讀取網域的使用者，按 [確定]

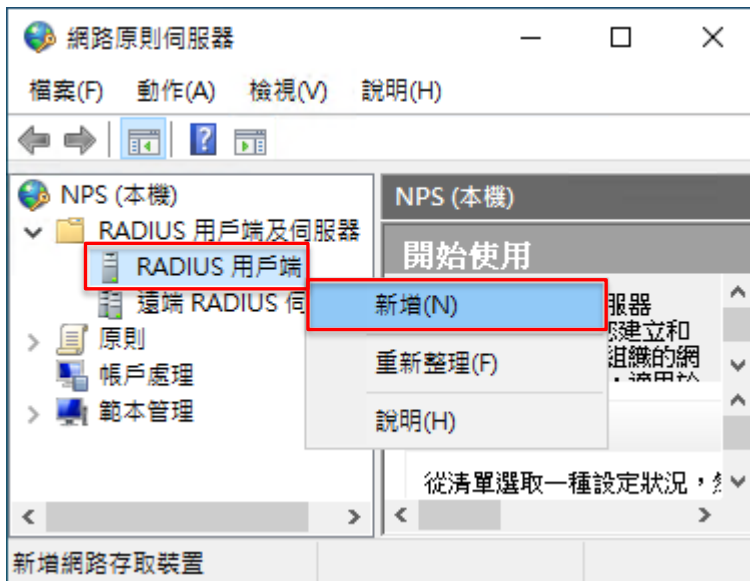


(4) 授權 NPS 電腦成為網域內的 RAS/NPS 伺服器成員，按 [確定]



2.1.3 設定 RADIUS 用戶端

(1) 展開 [RADIUS] 用戶端及伺服器 -> 在 [RADIUS 用戶端] 按滑鼠右鍵 -> 點選 [新增]



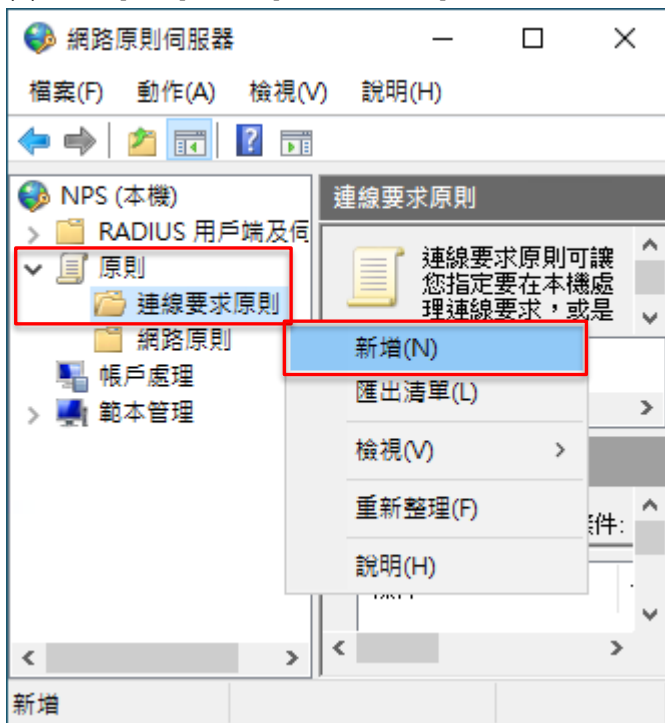
(2) 勾選 [啟用此 RADIUS 用戶端] -> 輸入名稱 · 本例 N-Cloud 註：請依客戶環境設定 -> 輸入 N-Cloud/N-Reporter 位址 · 本例 192.168.8.53 註：請依客戶環境設定 -> 輸入 共用密碼 Secret Key 註：請依客戶環境設定 -> 按 [確定]

(3) 點選 [RADIUS 用戶端] -> 顯示 [RADIUS 用戶端] 訊息

好記的名稱	IP 位址	裝置製造商	狀態
N-Cloud	192.168.8.53	RADIUS Standard	啟用


2.1.4 設定連線要求原則

(1) 展開 [原則] -> 在 [連線要求原則] 按滑鼠右鍵 -> 點選 [新增]



(2) 輸入 原則名稱，本例 N-Cloud 註：請依客戶環境設定 -> 按 [下一步]

新增連線要求原則 ×

 **指定連線要求原則名稱及連線類型**
您可以指定連線要求原則的名稱，以及原則套用的連線類型。

原則名稱(A):
N-Cloud

網路連線方法
選取傳送連線要求給 NPS 的網路存取伺服器類型。您可以選取網路存取伺服器類型或廠商特定，但兩者都不是必要資訊。若您的網路存取伺服器是 802.1X 驗證交換器或無線存取點，請選取 [未指定]。

網路存取伺服器類型(S):
未指定

廠商特定(V):
10

上一步(P) 下一步(N) 完成(F) 取消

(3) 按 [新增]

新增連線要求原則

 **指定條件**
指定條件來判定是否已為連線要求評估這個連線要求原則。至少要有一個條件。

條件(C):

條件	值
----	---

條件描述:


新增(D)... 編輯(E)... 移除(R)

上一步(P) 下一步(N) 完成(F) 取消


(4) 選擇 [好記的用戶端名稱] -> 按 [新增]


選取條件


選取條件，然後按一下 [新增]。


 **日期和時間限制**
[日期和時間限制] 可指定允許和不允許連線嘗試的日期和時間。這些限制是以 NPS 伺服器所在的時區為主。

RADIUS 用戶端內容

 **發出呼叫的工作站識別碼**
發出呼叫的工作站識別碼條件指定存取用戶端撥出的網路存取伺服器電話號碼。

 **好記的用戶端名稱**
好記的用戶端名稱條件指定轉寄連線要求給 NPS 的 RADIUS 用戶端名稱。

 **用戶端 IP v4 位址**
用戶端 IP 位址條件指定轉寄連線要求給 NPS 的 RADIUS 用戶端 IP 位址。

 **用戶端 IP v6 位址**
用戶端 IP v6 位址條件指定轉寄連線要求給 NPS 的 RADIUS 用戶端 IP v6 位址。

新增(D)... 取消

(5) 輸入 用戶端名稱，本例 N-Cloud 註：請依客戶環境設定 -> 按 [確定]

好記的用戶端名稱 ×

指定好記的 RADIUS 用戶端名稱。您可以使用模式比對語法(S)

N-Cloud

確定 取消

(6) 按 [下一步]

新增連線要求原則 ×

 **指定條件**
指定條件來判定是否已為連線要求評估這個連線要求原則。至少要有一個條件。

條件(C):

條件	值
 好記的用戶端名稱	N-Cloud


條件描述:

新增(D)... 編輯(E)... 移除(R)

上一步(P) **下一步(N)** 完成(F) 取消


(7) 按 [下一步]

新增連線要求原則 ×

 **指定轉寄連線要求**
連線要求可以由本機伺服器驗證，或是轉寄給遠端 RADIUS 伺服器群組的 RADIUS 伺服器。

如果原則條件符合連線要求時，便會套用這些設定。

設定(S):

轉寄連線要求	指定要在本機處理連線要求、轉寄到遠端 RADIUS 伺服器進行驗證，或是未經驗證就接受。
→ 驗證	
 帳戶處理	

驗證這個伺服器上的要求(U)
 轉送要求到下列遠端 RADIUS 伺服器群組進行驗證(R):
 <尚未設定> 新增(W)...
 不確認認證即接受使用者(C)

上一步(P) 下一步(N) 完成(F) 取消

(8) 按 [下一步]

新增連線要求原則 ×

 **指定驗證方法**
設定所需的一或多種驗證方法，讓連線要求符合這個原則。對於 EAP 驗證，您必須設定 EAP 類型。

覆寫網路原則驗證設定(O)
使用這些驗證設定，而不要使用網路原則中的限制及驗證設定。

EAP 類型是以列出的順序，依序在 NPS 和用戶端之間交涉。


EAP 類型(T):

較不安全的驗證方法:

- Microsoft 加密驗證版本 2 (MS-CHAP-v2)(V)
 - 使用者在密碼到期後可以變更密碼(H)
- Microsoft 加密驗證 (MS-CHAP)(Y)
 - 使用者在密碼到期後可以變更密碼(X)
- 加密驗證 (CHAP)(C)
- 未加密驗證 (PAP, SPAP)(S)
- 允許用戶端沒有交涉驗證方法仍然可以連線(L)



(9) 按 [下一步]

新增連線要求原則 ✕

 **設定設定值**
如果原則的所有連線要求原則條件都符合，NPS 就會將設定套用到連線要求。

設定這個網路原則的設定。
如果條件符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

指定領域名稱	選取要套用下列規則的屬性。規則會根據它們出現在清單中的順序來處理。																		
 屬性	屬性(B): <input type="text" value="Called-Station-Id"/>																		
RADIUS 屬性	規則(L):																		
 標準	<table border="1"><thead><tr><th>尋找</th><th>取代為</th><th></th></tr></thead><tbody><tr><td> </td><td> </td><td><input type="button" value="新增(D)"/></td></tr><tr><td> </td><td> </td><td><input type="button" value="編輯(E)"/></td></tr><tr><td> </td><td> </td><td><input type="button" value="移除(R)"/></td></tr><tr><td> </td><td> </td><td><input type="button" value="上移(U)"/></td></tr><tr><td> </td><td> </td><td><input type="button" value="下移(V)"/></td></tr></tbody></table>	尋找	取代為				<input type="button" value="新增(D)"/>			<input type="button" value="編輯(E)"/>			<input type="button" value="移除(R)"/>			<input type="button" value="上移(U)"/>			<input type="button" value="下移(V)"/>
尋找	取代為																		
		<input type="button" value="新增(D)"/>																	
		<input type="button" value="編輯(E)"/>																	
		<input type="button" value="移除(R)"/>																	
		<input type="button" value="上移(U)"/>																	
		<input type="button" value="下移(V)"/>																	
<input checked="" type="checkbox"/> 廠商特定																			

(10) 按 [完成]

新增連線要求原則 ×

 **正在完成連線要求原則精靈**

您已成功建立下列連線要求原則:

N-Cloud

原則條件:

條件	值
好記的用戶端名稱	N-Cloud

原則設定:

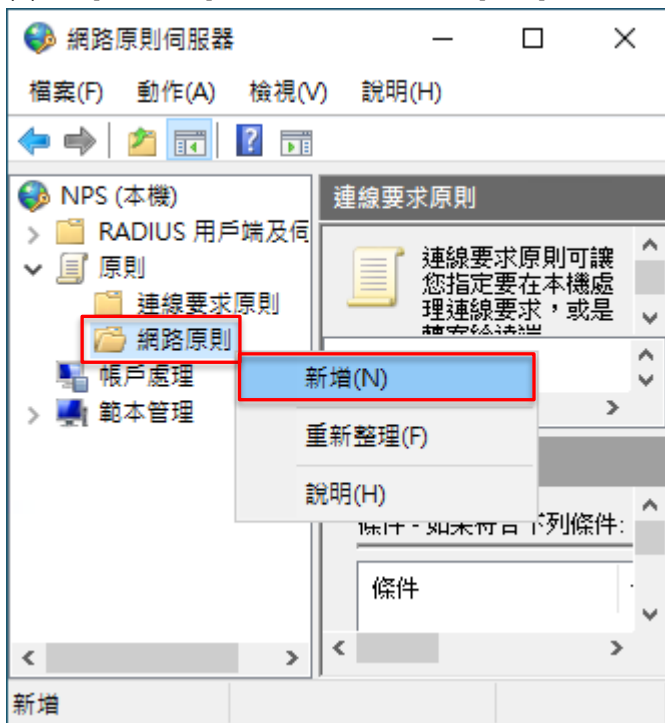
條件	值
驗證提供者	本機電腦

要關閉這個精靈，請按一下 [完成]。

上一步(P) 下一步(N) 完成(F) 取消


2.1.5 設定網路原則

(1) 在 [網路原則] 按滑鼠右鍵 -> 點選 [新增]



(2) 輸入 原則名稱，本例 N-Cloud 註：請依客戶環境設定 -> 按 [下一步]

新增網路原則 ×

 **指定網路原則名稱及連線類型**
您可以指定網路原則的名稱，以及要套用原則的連線類型。

原則名稱(A):
N-Cloud

網路連線方法
選取傳送連線要求給 NPS 的網路存取伺服器類型。您可以選取網路存取伺服器類型或廠商特定，但兩者都不是必要資訊。若您的網路存取伺服器是 802.1X 驗證交換器或無線存取點，請選取 [未指定]。

網路存取伺服器類型(S):
未指定

廠商特定(V):
10

上一步(P) 下一步(N) 完成(F) 取消

(3) 按 [新增] 使用者群組

新增網路原則 ×

 **指定條件**
指定條件來判定是否已為連線要求評估這個網路原則。最少要有一個條件。

條件(C):

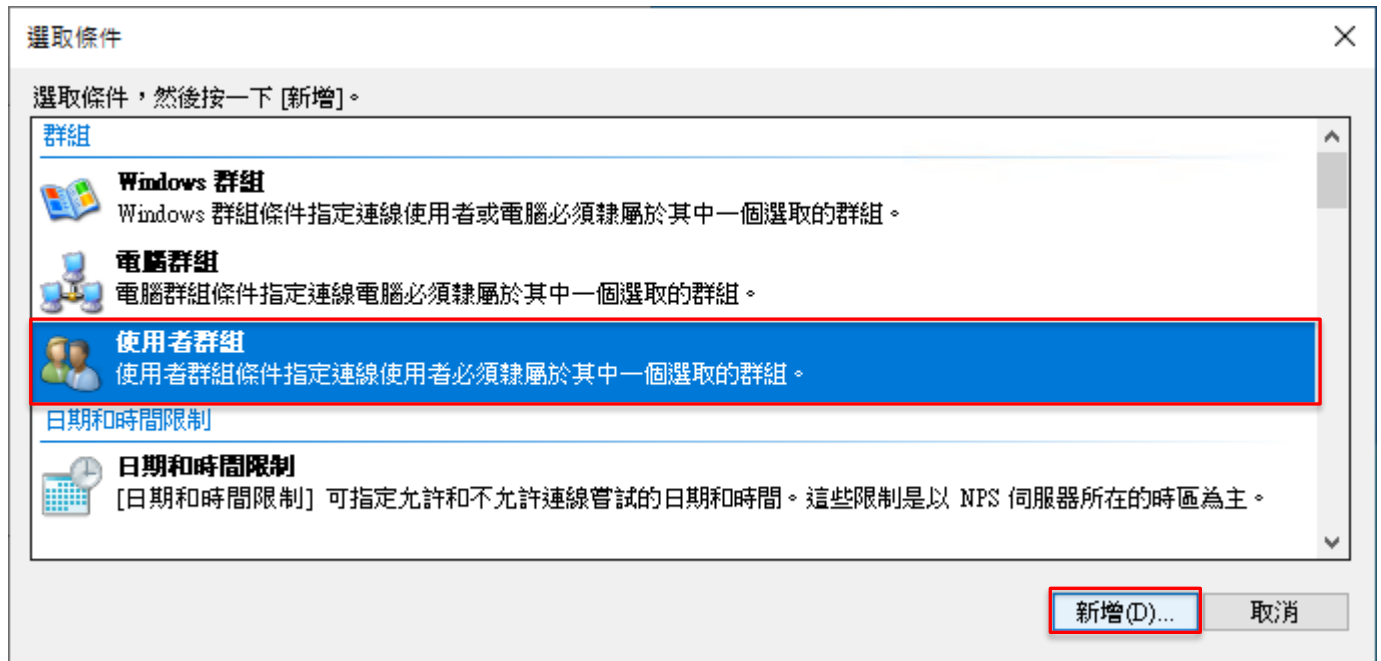
條件	值
----	---

條件描述:

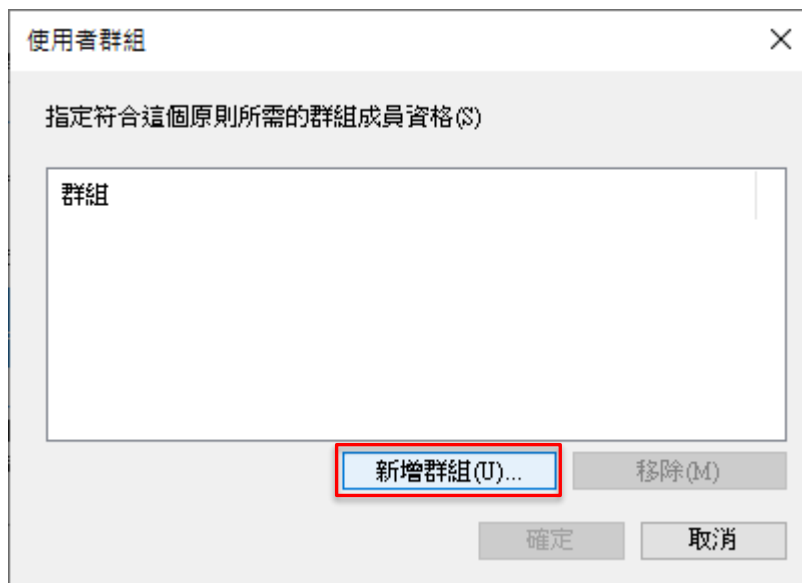
新增(D)... 編輯(E)... 移除(R)

上一步(P) 下一步(N) 完成(F) 取消

(4) 選擇 [使用者群組] -> 按 [新增]



(5) 按 [新增群組]



(6) 輸入使用者群組名稱，本例 N-Cloud 註：請依客戶環境設定 -> 按 [檢查名稱] -> 按 [確定]

選取群組

選取這個物件類型(S):

群組 物件類型(O)...

從這個位置(F):

npartner.local 位置(L)...

請輸入物件名稱來選取 (範例)(E):

N-Cloud 檢查名稱(C)

進階(A)... 確定 取消

(7) 按 [確定]

使用者群組

指定符合這個原則所需的群組成員資格(S)

群組


NPARTNER\N-Cloud

新增群組(U)... 移除(M)


確定 取消

(8) 按 [新增] 好記的用戶端名稱

新增網路原則 ×

 **指定條件**
指定條件來判定是否已為連線要求評估這個網路原則。最少要有一個條件。

條件 (C):

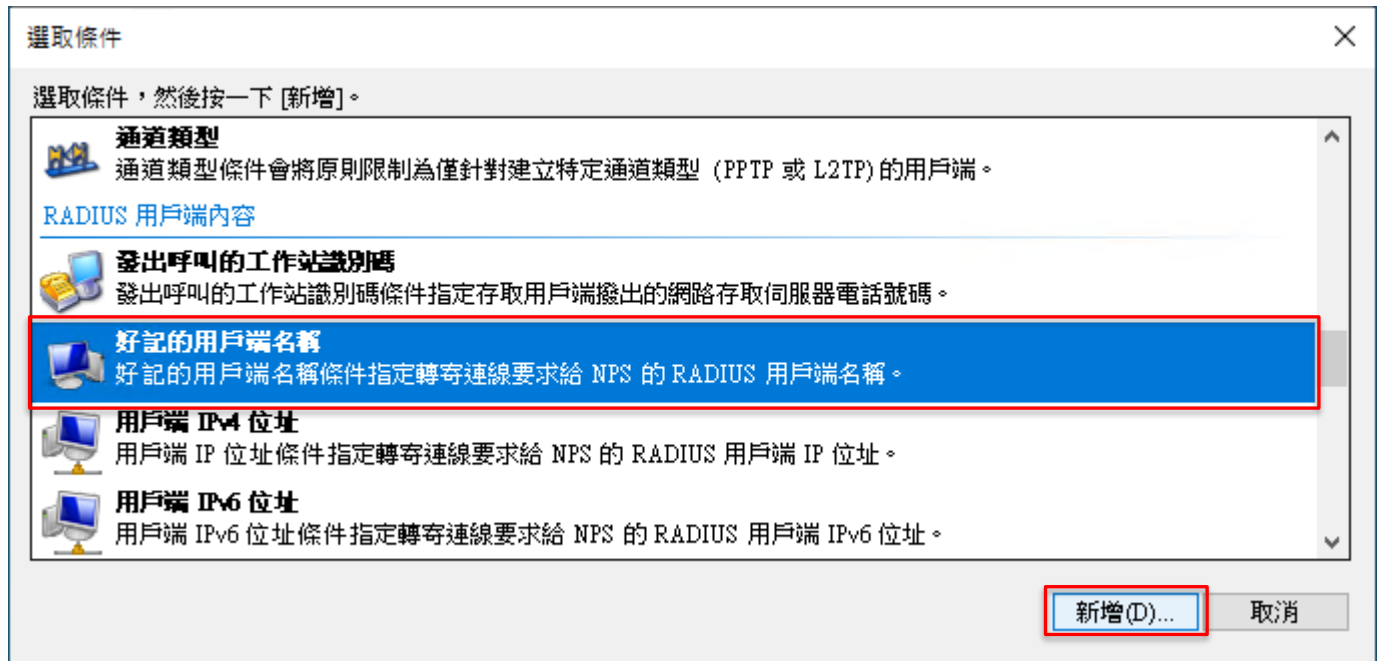
條件	值
 使用者群組	NPARTNER\W-Cloud

條件描述:
使用者群組條件指定連線使用者必須隸屬於其中一個選取的群組。

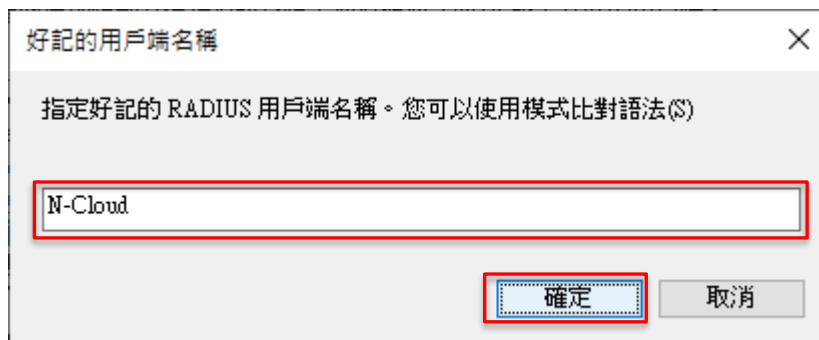
新增 (D)... 編輯 (E)... 移除 (R)

上一步 (P) 下一步 (N) 完成 (F) 取消

(9) 選擇 [好記的用戶端名稱] -> 按 [新增]



(10) 輸入好記的 RADIUS 用戶端名稱，本例 N-Cloud 註：請參照第 2.1.3 章節設定 -> 按 [確定]



(11) 按 [下一步]

新增網路原則

指定條件

指定條件來判定是否已為連線要求評估這個網路原則。最少要有一個條件。

條件 (C):

條件	值
使用者群組	NPARTNER\W-Cloud
好記的用戶端名稱	N-Cloud


條件描述:
好記的用戶端名稱條件指定轉寄連線要求給 NPS 的 RADIUS 用戶端名稱。

新增 (D)... 編輯 (E)... 移除 (R)

上一步 (P) **下一步 (N)** 完成 (F) 取消

(12) 按 [下一步]

新增網路原則 ×

 **指定存取權限**
設定連線要求符合這個原則時，應該授與或是拒絕網路存取。

授與存取權(A)
如果用戶端連線嘗試符合此原則的條件，便授與存取權。

拒絕存取(D)
如果用戶端連線嘗試符合此原則的條件，便拒絕存取。

存取權是由使用者撥入內容 (會覆寫 NPS 原則) 決定(S)
如果用戶端連線嘗試符合此原則的條件，便根據使用者撥入內容授與或拒絕存取。

(13) 勾選 [加密驗證 (CHAP)] 和 [未加密驗證 (PAP · SPAP)] -> 按 [下一步]

新增網路原則

設定驗證方法

設定所需的一或多種驗證方法，讓連線要求符合這個原則。對於 EAP 驗證，您必須設定 EAP 類型。

EAP 類型是以列出的順序，依序在 NPS 和用戶端之間交涉。

EAP 類型(T):

新增(D)... 編輯(E)... 移除(R)

較不安全的驗證方法:

- Microsoft 加密驗證版本 2 (MS-CHAP-v2)(V)
 - 使用者在密碼到期後可以變更密碼(H)
- Microsoft 加密驗證 (MS-CHAP)(Y)
 - 使用者在密碼到期後可以變更密碼(X)
- 加密驗證 (CHAP)(C)
- 未加密驗證 (PAP · SPAP)(S)
- 允許用戶端沒有交涉驗證方法仍然可以連線(L)

上移(U) 下移(W)

上一步(P) **下一步(N)** 完成(F) 取消

(14) 按 [否] 不檢視說明

連線要求原則

i 您已選取一或多個不安全的驗證方法。如果您要確保遠端存取、原則及網域等級的每個通訊協定全都正確設定，請依照 [說明] 的逐步程序來進行。

您要檢視 [說明] 的相關主題嗎?

是(Y) **否(N)**

(15) 選擇 [NAS 連接埠類型] -> 按 [下一步]

新增網路原則

設定限制

限制是比對連線要求所需的其他網路原則參數。如果連線要求和限制不相符，NPS 就會自動拒絕該要求。限制是選用項目，如果您不想要設定限制，請按 [下一步]。

設定這個網路原則的限制。
如果連線要求不符合所有限制，便會拒絕網路存取。

限制(S):

限制

- 閒置逾時
- 工作階段逾時
- 被呼叫的工作站識別碼
- 日期和時間限制
- NAS 連接埠類型**

指定符合這個原則所需的存取媒體類型(F)

一般撥號及 VPN 通道類型(D)

- ISDN Sync
- 非對稱式 (Modem)
- 虛擬 (VPN)
- 對稱式 (T1 Line)

一般 802.1X 連線通道類型(X)

- FDDI
- 乙太網路
- 無線 - IEEE 802.11
- 權杖環

其他(T)

- ADSL-CAP - 非對稱式 DSL 無載波振幅相位調變
- ADSL-DMT - 非對稱式 DSL 離散多音頻

上一步(P) **下一步(N)** 完成(F) 取消

(16) 選擇 [標準] -> 按 [新增]



(17) 選擇 [Reply-Message] -> 按 [新增]

新增標準 RADIUS 屬性

若要新增屬性到設定中，請選取該屬性，然後按 [新增]。
若要新增自訂或預先定義的廠商特定屬性，請關閉此對話方塊，選取 [廠商特定]，然後按一下 [新增]。

存取類型(T):
全部

屬性(B):

- 名稱
- Login-TCP-Port
- NAS-Port-Id
- Reply-Message
- Service-Type
- Termination-Action
- Tunnel-Assignment-ID

描述:
指定當驗證要求被接受或拒絕時，顯示給使用者的訊息。

新增(A)... 關閉(C)

(18) 按 [新增]

屬性資訊

屬性名稱:
Reply-Message

屬性號碼:
18

屬性格式:
String

屬性值(T):

廠商	值
----	---

新增(A)...
編輯(E)...
移除(R)
上移(U)
下移(D)

確定 取消

(19) 輸入 屬性值 : RADIUS npartner -> 按 [確定]

屬性資訊

屬性名稱:
Reply-Message

屬性號碼:
18

屬性格式:
String

屬性值(A):
RADIUS npartner

確定 取消

(20) 按 [確定]

屬性資訊

屬性名稱:
Reply-Message

屬性號碼:
18

屬性格式:
String

屬性值(T):

廠商	值
RADIUS Standard	RADIUS npartner

新增(A)...
編輯(E)...
移除(R)
上移(U)
下移(D)

確定 取消

(21) 按 [關閉]

新增標準 RADIUS 屬性

若要新增屬性到設定中，請選取該屬性，然後按 [新增]。
若要新增自訂或預先定義的廠商特定屬性，請關閉此對話方塊，選取 [廠商特定]，然後按一下 [新增]。

存取類型(T):
全部

屬性(B):

名稱
Login-TCP-Port
NAS-Port-Id
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID

描述:
指定當驗證要求被接受或拒絕時，顯示給使用者的訊息。

新增(A)... 關閉(C)

(22) 移除 [Framed-Protocol: PPP] 和 [Service-Type: Framed]

新增網路原則

設定設定值

如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。

設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

- RADIUS 屬性**
 - 標準
 - 廠商特定
- 路由及遠端存取**
 - 多重連結與頻寬配置通訊協定 (BAP)
 - IP 篩選器
 - 加密
 - IP 設定

若要傳送其他屬性給 RADIUS 用戶端，請選取 RADIUS 標準屬性，然後按一下 [編輯]。如果您沒有設定屬性，就不會傳送給 RADIUS 用戶端。請參閱 RADIUS 用戶端文件以取得所需屬性的資訊。

屬性(T):

名稱	值
Framed-Protocol	PPP
Service-Type	Framed
Reply-Message	RADIUS npartner

新增(D)... 編輯(E)... 移除(R)

上一步(P) 下一步(N) 完成(F) 取消

(23) 顯示 [Framed-Protocol: PPP] 和 [Service-Type: Framed] 移除完成

新增網路原則

設定設定值

如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。

設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

- RADIUS 屬性**
 - 標準
 - 廠商特定
- 路由及遠端存取**
 - 多重連結與頻寬配置通訊協定 (BAP)
 - IP 篩選器
 - 加密
 - IP 設定

若要傳送其他屬性給 RADIUS 用戶端，請選取 RADIUS 標準屬性，然後按一下 [編輯]。如果您沒有設定屬性，就不會傳送給 RADIUS 用戶端。請參閱 RADIUS 用戶端文件以取得所需屬性的資訊。

屬性(T):

名稱	值
Reply-Message	RADIUS npartner

新增(D)... 編輯(E)... 移除(R)

上一步(P) **下一步(N)** 完成(F) 取消

(24) 選擇 [廠商特定] -> 按 [新增]

新增網路原則

設定設定值

如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。

設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

- RADIUS 屬性
 - 標準
 - 廠商特定**
- 路由及遠端存取
 - 多重連結與頻寬配置通訊協定 (BAP)
 - IP 篩選器
 - 加密
 - IP 設定

若要傳送其他屬性給 RADIUS 用戶端，請選取一個廠商特定屬性，然後按一下 [編輯]。如果您沒有設定屬性，就不會傳送給 RADIUS 用戶端。請參閱 RADIUS 用戶端文件以取得所需屬性的資訊。

屬性(T):

名稱	廠商	值
----	----	---

新增(D)... 編輯(E)... 移除(R)

上一步(P) 下一步(N) 完成(F) 取消

(25) 選擇 廠商 [自訂] 和 [Vendor-Specific] -> 按 [新增]

新增廠商特定屬性

若要新增屬性到設定中，請選取該屬性，然後按 [新增]。

若要新增未列出的廠商特定屬性，請選取 [自訂]，然後按一下 [新增]。

廠商(V):
自訂

屬性(B):

名稱	廠商
Allowed-Certificate-OID	RADIUS Standard
Generate-Class-Attribute	RADIUS Standard
Generate-Session-Timeout	RADIUS Standard
Saved-Machine-HealthCheck-Only	RADIUS Standard
Tunnel-Tag	RADIUS Standard
Vendor-Specific	RADIUS Standard

描述:
指定專屬 NAS 功能的支援。

新增(A)... 關閉(C)

(26) 按 [新增] 設定 N-Partner-Domain ID

屬性資訊

屬性名稱:
Vendor-Specific

屬性號碼:
26

屬性格式:
OctetString

屬性值(T):

廠商	值
----	---

新增(A)...
編輯(E)...
移除(R)
上移(U)
下移(D)

確定 取消

(27) 點選 [輸入廠商代碼] -> 輸入 39693 -> 點選 [是·符合] -> 按 [設定屬性]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是, 符合(Y)

否, 不符合(N)

設定屬性(A)...

確定 取消

(28) 輸入 廠商指定的屬性號碼: 1 註: 此為 N-Cloud/N-Reporter 領域管理(Domain) 編號 -> 選擇 屬性格式: [十進位] -> 輸入 屬性值: 1001 註: 此為 N-Cloud/N-Reporter 領域管理(Domain) ID · 請依客戶環境設定 -> 按 [確定]

設定 VSA (RFC 相容)

廠商指定的屬性號碼(V):
1

屬性格式(A):
十進位

屬性值(B):
1001

確定 取消

(29) 按 [確定]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是，符合(Y)

否，不符合(N)

設定屬性(A)...

確定 取消

(30) 按 [新增] 設定 N-Partner-Menu ID

屬性資訊

屬性名稱:
Vendor-Specific

屬性號碼:
26

屬性格式:
OctetString

屬性值(T):

廠商	值
廠商代碼: 39693	1001

新增(A)...

編輯(E)...

移除(R)

上移(U)

下移(D)

確定 取消

(31) 點選 [輸入廠商代碼] -> 輸入 39693 -> 點選 [是·符合] -> 按 [設定屬性]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是, 符合(Y)

否, 不符合(N)

設定屬性(A)...

確定 取消

(32) 輸入 廠商指定的屬性號碼: 1 註: 此為 N-Cloud/N-Reporter 選單樣版(Menu) 編號 -> 選擇 屬性格式: [十進位] -> 輸入 屬性值: 2 註: 此為 N-Cloud/N-Reporter 選單樣版(Menu) ID, 請依客戶環境設定 -> 按 [確定]

設定 VSA (RFC 相容)

廠商指定的屬性號碼(V):
2

屬性格式(A):
十進位

屬性值(B):
2

確定 取消

(33) 按 [確定]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是，符合(Y)

否，不符合(N)

設定屬性(A)...

確定 取消

(34) 按 [新增] 設定 N-Partner-Email

屬性資訊

屬性名稱:
Vendor-Specific

屬性號碼:
26

屬性格式:
OctetString

屬性值(T):

廠商	值
廠商代碼: 39693	1001
廠商代碼: 39693	2

新增(A)...

編輯(E)...

移除(R)

上移(U)

下移(D)

確定 取消

(35) 點選 [輸入廠商代碼] -> 輸入 39693 -> 點選 [是，符合] -> 按 [設定屬性]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是，符合(Y)

否，不符合(N)

設定屬性(A)...

確定 取消

(36) 輸入 廠商指定的屬性號碼: 3 -> 選擇 屬性格式: [字串] -> 輸入 屬性值: 本例 npartner@npartner.local 請依客
戶環境設定 -> 按 [確定]

設定 VSA (RFC 相容)

廠商指定的屬性號碼(V):
3

屬性格式(A):
字串

屬性值(B):
npartner@npartner.local

確定 取消

(37) 按 [確定]

廠商特定的屬性資訊

屬性名稱(T):
廠商特定

請指定網路存取伺服器廠商。

從清單選取(S): RADIUS Standard

輸入廠商代碼(E): 39693

指定屬性是否符合廠商特定屬性的 RADIUS RFC 規格。

是，符合(Y)

否，不符合(N)

設定屬性(A)...

確定 取消

(38) 按 [確定]

屬性資訊

屬性名稱:
Vendor-Specific

屬性號碼:
26

屬性格式:
OctetString

屬性值(T):

廠商	值
廠商代碼: 39693	1001
廠商代碼: 39693	2
廠商代碼: 39693	npartner@npartner.local

新增(A)...

編輯(E)...

移除(R)

上移(U)

下移(D)

確定 取消

(39) 按 [關閉]

新增廠商特定屬性 ×

若要新增屬性到設定中，請選取該屬性，然後按 [新增]。

若要新增未列出的廠商特定屬性，請選取 [自訂]，然後按一下 [新增]。

廠商(V):
自訂 ▼

屬性(B):

名稱	廠商
Allowed-Certificate-OID	RADIUS Standard
Generate-Class-Attribute	RADIUS Standard
Generate-Session-Timeout	RADIUS Standard
Saved-Machine-HealthCheck-Only	RADIUS Standard
Tunnel-Tag	RADIUS Standard
Vendor-Specific	RADIUS Standard

描述:
指定專屬 NAS 功能的支援。

(40) 按 [下一步]

新增網路原則

設定設定值

如果符合原則的全部網路原則條件及限制，NPS 就會對連線要求套用設定。

設定這個網路原則的設定。
如果條件及限制符合連線要求，而且該原則授與存取權，則會套用設定。

設定(S):

- RADIUS 屬性
 - 標準
 - 廠商特定
- 路由及遠端存取
 - 多重連結與頻寬配置通訊協定 (BAP)
 - IP 篩選器
 - 加密
 - IP 設定

若要傳送其他屬性給 RADIUS 用戶端，請選取一個廠商特定屬性，然後按一下 [編輯]。如果您沒有設定屬性，就不會傳送給 RADIUS 用戶端。請參閱 RADIUS 用戶端文件以取得所需屬性的資訊。

屬性(T):

名稱	廠商	值
Vendor-Specific	RADIUS Standard	1001, 2, npartner@npartner.local

新增(D)... 編輯(E)... 移除(R)

上一步(P) **下一步(N)** 完成(F) 取消

(41) 檢視 原則條件 和 原則設定 -> 按 [完成]

新增網路原則 ×

 **正在完成新增網路原則**

您已成功建立下列網路原則:

N-Cloud

原則條件:

條件	值
使用者群組	NPARTNER\N-Cloud
好記的用戶端名稱	N-Cloud

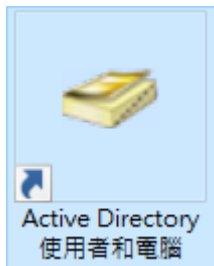
原則設定:

條件	值
驗證方法	未加密驗證 (PAP, SPAP) 或 加密驗證 (CHAP) 或 MS-CHAP v1 或 MS-CHAP v1 (使用者可在密碼...
存取權限	授與存取權
略過使用者撥入內容	False
Reply-Message	RADIUS npartner
Vendor-Specific	1001, 2, npartner@npartner.local

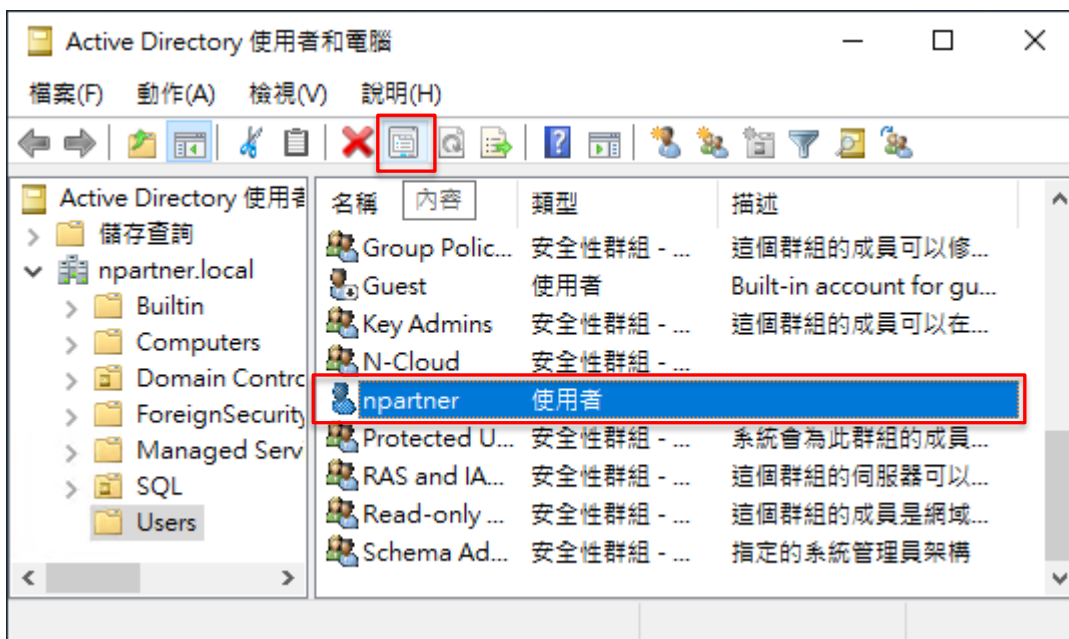
要關閉這個精靈，請按一下 [完成]。

2.1.6 查看 AD 使用者

(1) 在 Windows AD 伺服器 -> 開啟 [Active Directory 使用者和電腦]



(2) 選取 NPS 伺服器驗證使用者群組的使用者帳號，本例 npartner 帳號 註：請依客戶環境 -> 按 [內容]



(3) 在 [帳戶] 頁面；確認 未勾選 [使用者必須在下次登入時變更密碼]

npartner - 內容

環境	工作階段	遠端控制	遠端桌面服務設定檔	COM+			
一般	位址	帳戶	設定檔	電話	組織	隸屬於	撥入

使用者登入名稱(U):
npartner @npartner.local

使用者登入名稱 (Windows 2000 前版)(W):
NPARTNER\ npartner

登入時段(L)... 登入到(T)...

解除鎖定帳戶(N)

帳戶選項(O):

- 使用者必須在下次登入時變更密碼
- 使用者不能變更密碼
- 密碼永久有效
- 使用可還原的加密來存放密碼

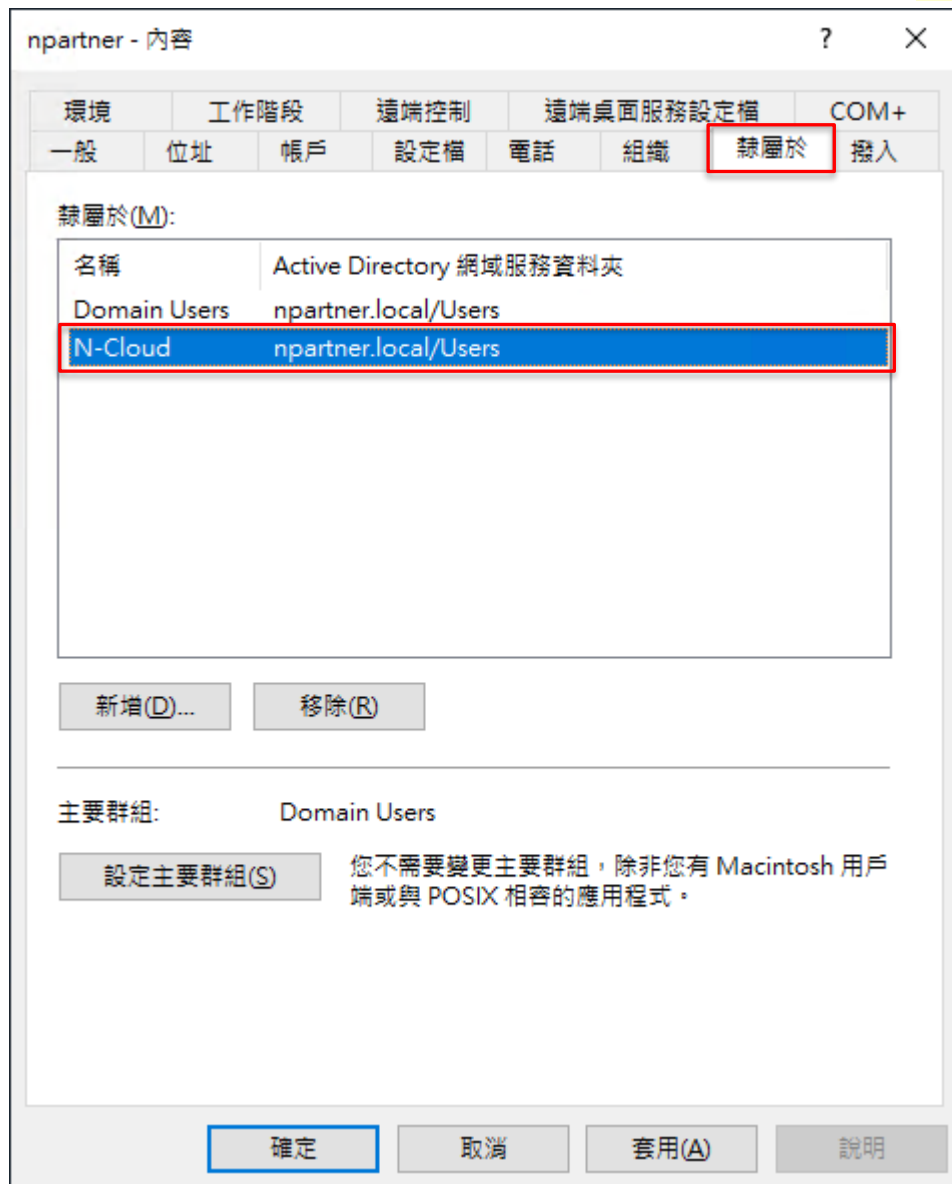
帳戶到期日

無(N)

到期日(E): 2022年 5月25日

確定 取消 套用(A) 說明

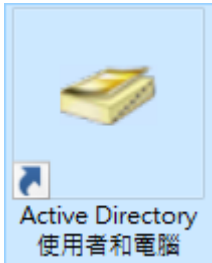
(4) 在 [隸屬於] 頁面；確認有 NPS 伺服器驗證使用者群組，本例 N-Cloud 註：請依客戶環境




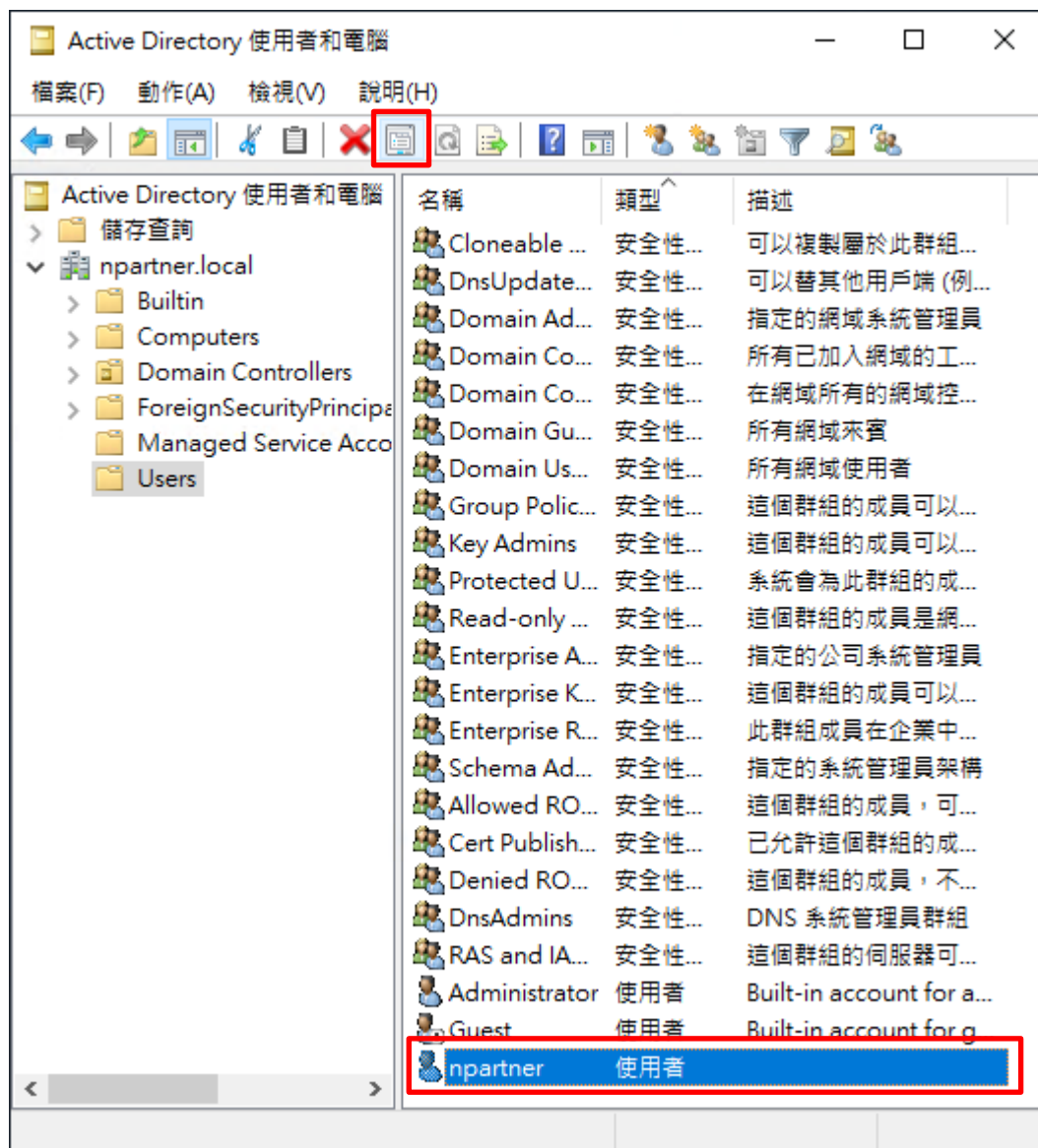
2. LDAP 配置

2.1 設定 Windows AD 帳戶資料

(1) 開啟 Active Directory 使用者和電腦



(2) 選取 AD 帳戶 -> 內容 



(3) [一般] 頁面: 確認 [電子郵件]

npartner - 內容 ? X

環境	工作階段	遠端控制	遠端桌面服務設定檔	COM+			
一般	位址	帳戶	設定檔	電話	組織	隸屬於	撥入

 npartner

姓氏(L):

名字(F): 英文縮寫(I):

顯示名稱(S):

描述(D):

辦公室(C):

電話號碼(T):

電子郵件(M):

網頁(W):

(4) [電話] 頁面: 在 [附註] 輸入 領域管理 ID 和選單樣版 ID -> [確定] (重要)

The screenshot shows a dialog box titled 'npartner - 內容'. It has several tabs: '環境', '工作階段', '遠端控制', '遠端桌面服務設定檔', and 'COM+'. Under '遠端控制', the '電話' tab is selected. Below the tabs, there are input fields for phone numbers: '住家(M):', '呼叫器(P):', '行動電話(B):', '傳真(F):', and 'IP 電話(I):'. Each field has a corresponding '其他(O...)', '其他(T...)', '其他(H...)', '其他(E...)', and '其他(R...)' button. Below these fields is a text area for '附註(N):' containing the text 'ncloud:group_id=1001,menu_id=2'. At the bottom, there are buttons for '確定', '取消', '套用(A)', and '說明'. The '確定' button is highlighted with a red box.

務必以 `ncloud:group_id=參數,menu_id=參數` 格式

Note : group_id : 領域 id

Menu_id : 選單樣板 id(後台)

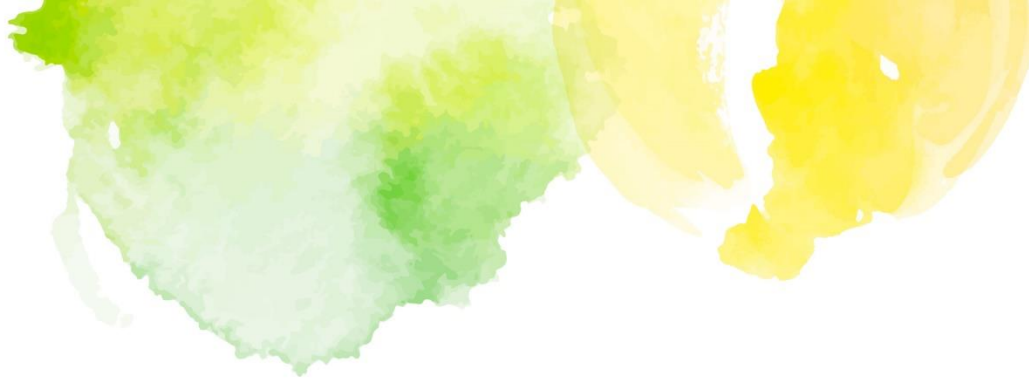
(5) 查看 AD 帳戶資訊

```
PS C:\> Get-ADUser npartner -Properties * | Select-Object  
DisplayName,UserPrincipalName,DistinguishedName,EmailAddress,mail,info
```

The screenshot shows a Windows PowerShell terminal window with the following output:

```
PS C:\> Get-ADUser npartner -Properties * | Select-Object DisplayName,UserPrincipalName,DistinguishedName,EmailAddress,mail,info  
DisplayName : npartner  
UserPrincipalName : npartner@npartner.local  
DistinguishedName : CN=npartner,CN=Users,DC=npartner,DC=local  
EmailAddress : npartner@npartner.local  
mail : npartner@npartner.local  
info : ncloud:group_id=1001,menu_id=2  
PS C:\> _
```

紅色文字部位請依客戶環境輸入 Windows AD 帳戶



Chapter 3

N-Cloud / N-Reporter 配置



3. N-Cloud / N-Reporter 配置

3.1 RADIUS 設定

3.1.1 設定服務連線資訊

使用具前台管理權限的使用者登入 N-Cloud / N-Reporter，在 [系統管理] -> [偏好設定] -> [系統管理] -> [Radius / LDAP] 中，勾選 [啟動 Radius 認證]，並設定 Radius IP 和共享密鑰 Secret key 和測試登入帳號及密碼按 [Radius 測試]，顯示 "測試成功"，按 [儲存設定] 則此後登入即可用 Radius 帳戶登入。

The screenshot displays the N-Cloud / N-Reporter configuration interface. A green notification banner at the top right reads "Radius 測試成功" (Radius Test Successful). The left sidebar shows the navigation menu with "系統管理" (System Management) and "偏好設定" (Preferences) highlighted. The main content area is titled "Home / 系統管理 / 偏好設定" and contains several tabs: "密碼策略", "Radius / LDAP", "登錄設定", "系統名稱", "系統所在區域", and "檔案簽章". The "Radius / LDAP" tab is active, showing the following configuration options:

- 啟動 Radius 認證
- Radius IP: 192.168.8.186
- Secret key:
- 測試登入帳號: npartner
- 測試登入密碼: npartner

Below these settings, there are options for LDAP configuration:

- 啟動 LDAP 認證
- LDAP IP: 192.168.8.183
- LDAP BaseDN: CN=Users,DC=npartner,DC=local
- 測試登入帳號: [Empty field]
- 測試登入密碼: [Empty field]

At the bottom right, there are three buttons: "Radius 測試", "LDAP 測試", and "儲存設定" (Save Settings). The "儲存設定" button is highlighted with a red box.

Copyright © 2009 N-Partner. All rights reserved. 上次登錄時間 © 2021-10-27 16:13:18

3.1.2 登入

(1) 若輸入預設帳戶 "admin" 或 "superuser" 則走一般登入流程，不跟 RADIUS server 連線。

若輸入其他帳號登入，則會向 RADIUS server 做認證，取得回傳的使用者參數，當帳號不存在於 N-Cloud / N-Reporter 系統中，則自動根據回傳的使用者參數新增一個使用者。

登入畫面按鈕顯示 Radius Login



N-CLOUD

npartner

.....

Radius Login

[Forgot password?](#)

© 2009 N-Partner, inc. All rights reserved.

3.2 LDAP 設定

3.2.1 設定服務連線資訊

使用具前台管理權限的使用者登入 N-Cloud / N-Reporter，在 [系統管理] -> [偏好設定] -> [系統管理] -> [Radius / LDAP] 中，勾選 [啟動 LDAP 認證]，並設定 LDAP IP 和 LDAP BaseDN 和測試登入帳號及密碼按 [LDAP 測試]，顯示 "測試成功"，按 [儲存設定] 則此後登入即可用 LDAP 帳戶登入。

The screenshot displays the N-Cloud web interface for LDAP configuration. The sidebar on the left shows the navigation menu with '系統管理' (System Management) and '偏好設定' (Preferences) highlighted. The main content area is titled 'Home / 系統管理 / 偏好設定' and contains the 'Radius / LDAP' configuration section. The 'Radius / LDAP' section includes a checkbox for '啟動 Radius 認證' (which is unchecked), and fields for 'Radius IP', 'Secret key', '測試登入帳號' (test login username), and '測試登入密碼' (test login password). Below this, the 'LDAP' section is highlighted with a red box, showing '啟動 LDAP 認證' checked, 'LDAP IP' (192.168.8.183), 'LDAP BaseDN' (CN=Users,DC=npartner,DC=local), and test login fields for 'npartner'. At the bottom of the configuration area, there are three buttons: 'Radius 測試', 'LDAP 測試' (highlighted with a red box), and '儲存設定' (Save Settings). A green notification banner at the top right of the interface displays 'LDAP 測試成功' (LDAP Test Successful).

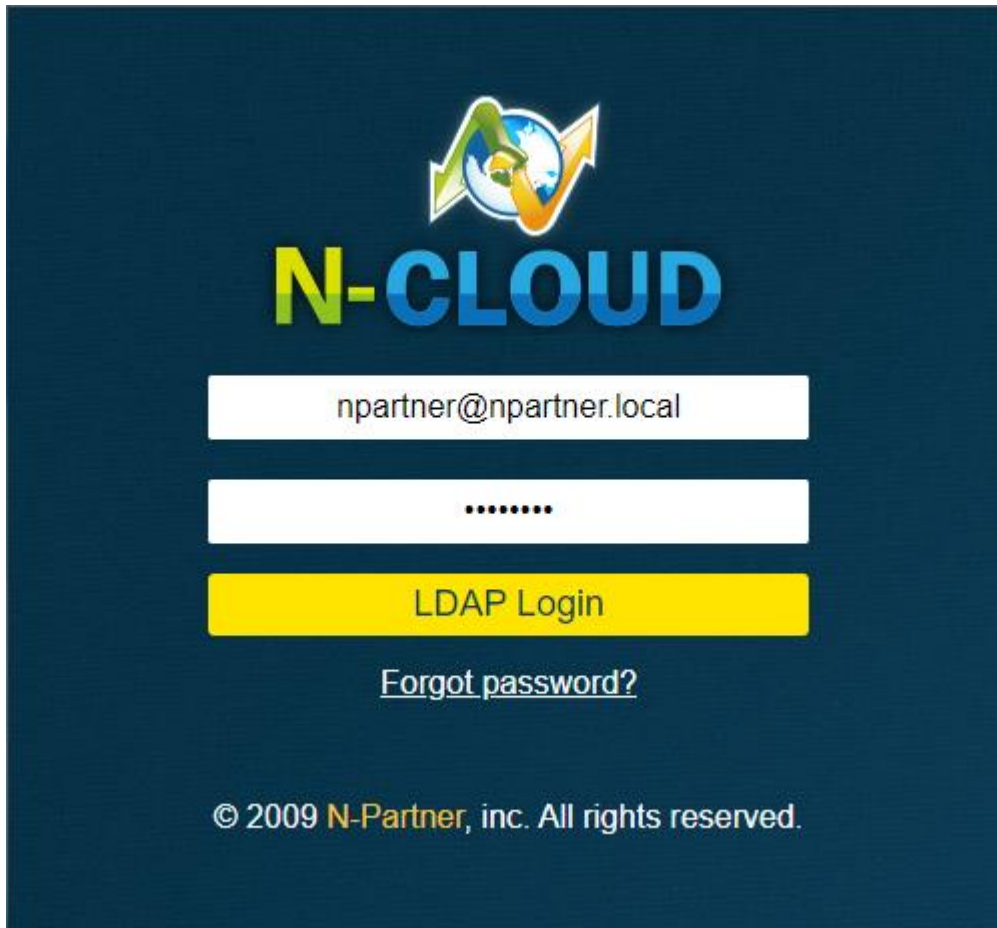
Copyright © 2009 N-Partner. All rights reserved. 上次登錄時間 © 2021-10-27 16:13:18

3.2.2 登入

(1) 若輸入預設帳戶 "admin" 或 "superuser" 則走一般登入流程，不跟 LDAP server 連線。

若輸入其他帳號登入，則會向 LDAP server 做認證，取得回傳的使用者參數

登入畫面按鈕顯示 LDAP Login -> 輸入 AD 帳戶 UserPrincipalName 和密碼



N-CLOUD

npartner@npartner.local

.....

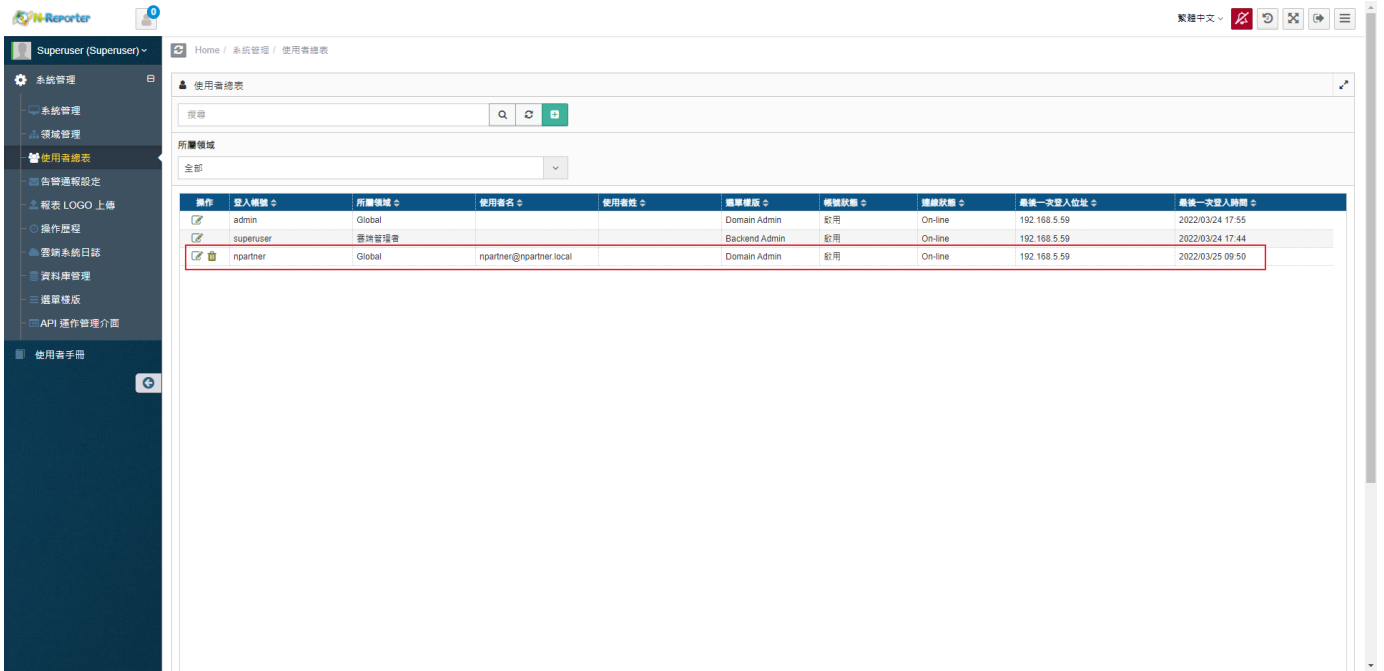
LDAP Login


[Forgot password?](#)

© 2009 N-Partner, inc. All rights reserved.

3.2.3 網頁後台更改帳戶權限

(1) 帳戶登入網頁後，即可在網頁後台[系統管理] -> [使用者總表] 查看到該帳戶。



(2) 在網頁後台[系統管理] -> [使用者總表] -> 選擇帳戶 ->  -> [選單樣版] 調整帳戶權限。





Tel / 04-23752865 Fax / 04-23757458
業務詢問 / sales@npartnertech.com
技術詢問 / support@npartnertech.com