

使用Windows Server在Catalyst Center上配置外部身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[管理員角色策略](#)

[觀察者角色策略](#)

[啟用外部身份驗證](#)

[驗證](#)

簡介

本文檔介紹如何在Cisco DNA Center中使用Windows Server中的網路策略伺服器(NPS)作為RADIUS配置外部身份驗證。

必要條件

需求

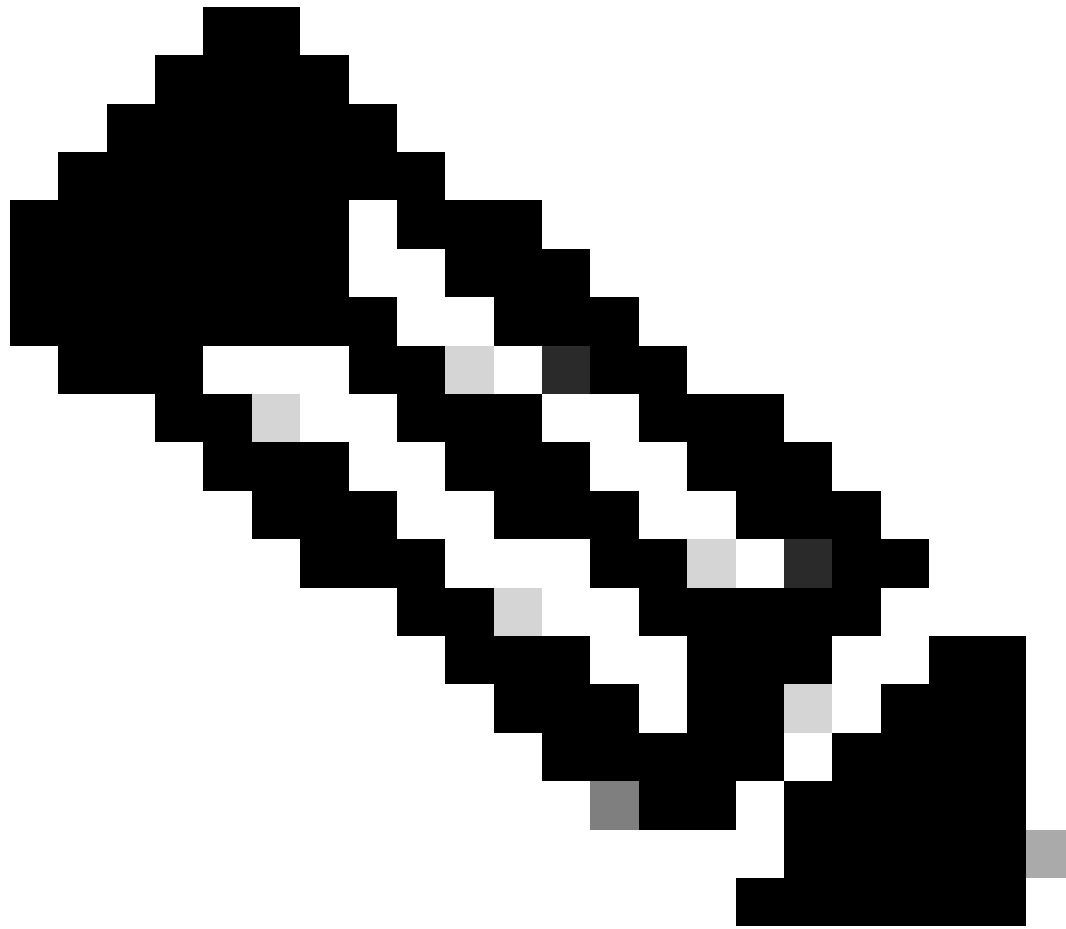
基本知識：

- Cisco DNA Center使用者和角色
- Windows Server網路策略伺服器、RADIUS和Active Directory

採用元件

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server 2019版充當域控制器、DNS伺服器、NPS和Active Directory

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。



注意：思科技術支援中心(TAC)不向Microsoft Windows Server提供技術支援。如果Microsoft Windows Server配置遇到問題，請與Microsoft支援部門聯絡以獲得技術支援。

設定

管理員角色策略

1. 按一下Windows Start選單並搜尋NPS。然後選擇Network Policy Server：

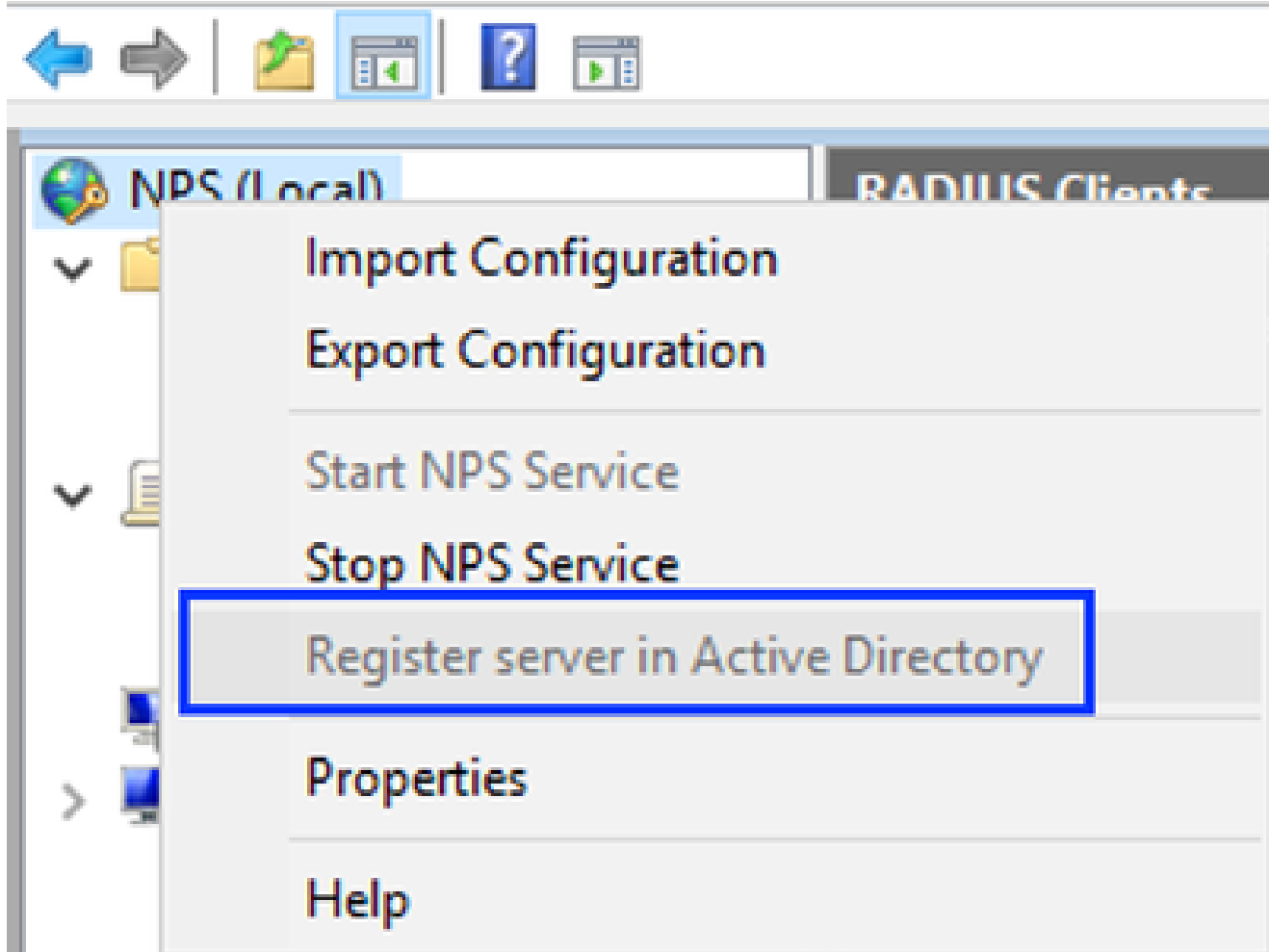


Network Policy Server

Desktop app

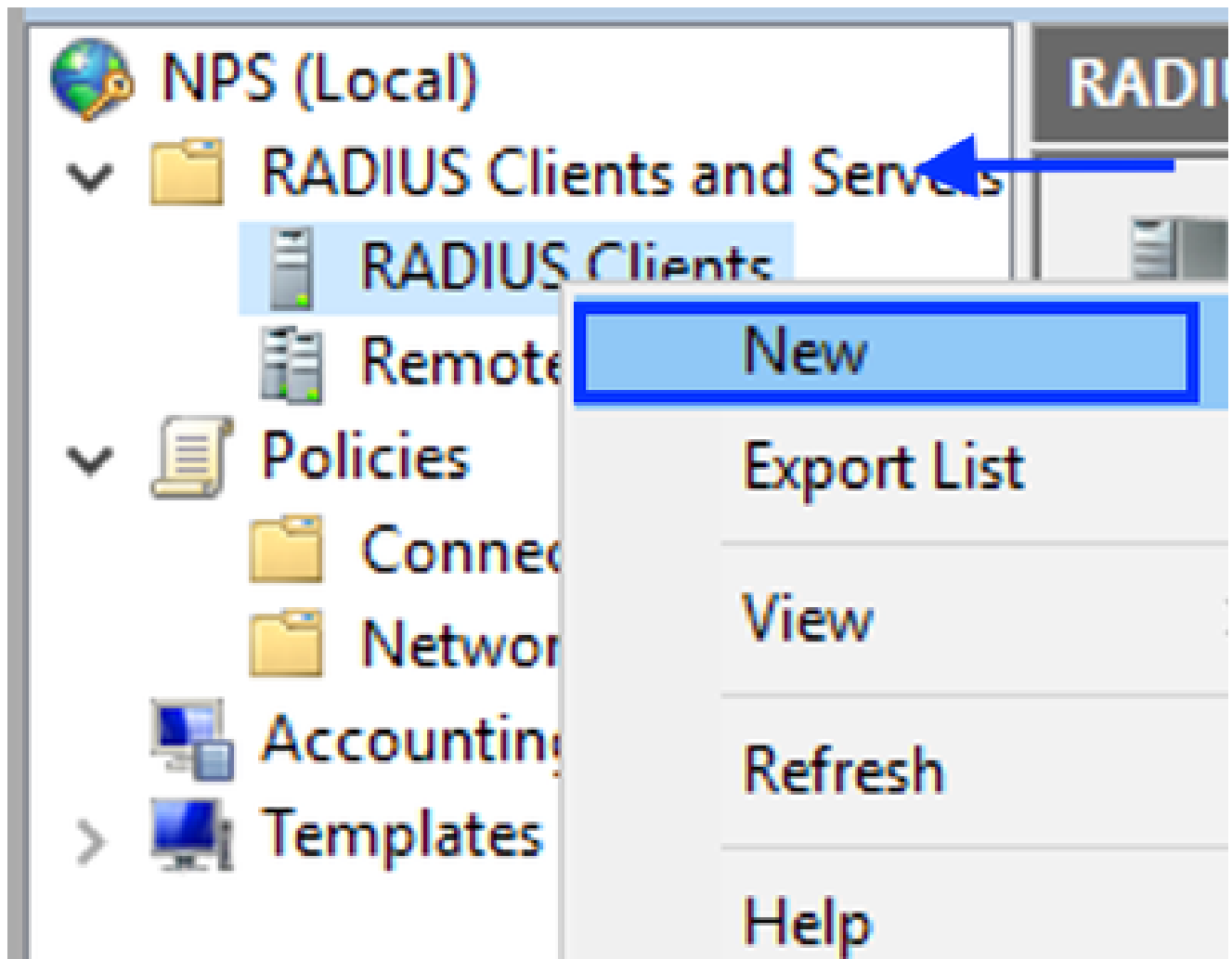
Network Policy Server

File Action View Help



Windows網路策略服務

3. 按一下OK兩次。
4. 展開RADIUS Clients and Servers，按一下右鍵RADIUS Clients，然後選擇New：



增加RADIUS客戶端

5. 輸入友好名稱、Cisco DNA Center管理IP地址和共用金鑰（以後可以使用）：

DNAC Properties X

Settings **Advanced**

Enable this RADIUS client

Select an existing template:

Name and Address

Friendly name:
DNAC

Address (IP or DNS):
10.88.244.160 Verify...

Shared Secret

Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

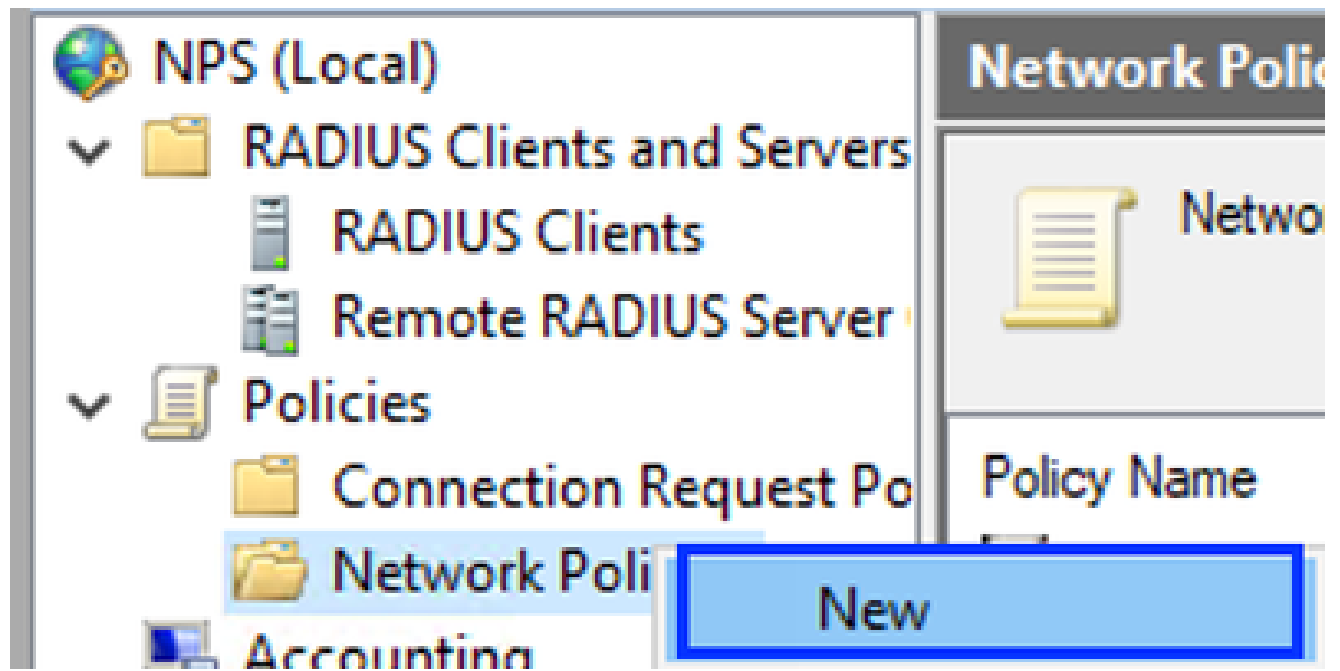
Shared secret:
●●●●●●●●

Confirm shared secret:
●●●●●●●●

OK Cancel Apply

Radius客戶端配置

6. 按一下OK儲存它。
7. 展開策略，按一下右鍵網路策略並選擇新建：



增加新網路策略

8. 為規則輸入策略名稱，然後按一下Next：



Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:
DNAC-Admin-Policy

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

Type of network access server:
Unspecified

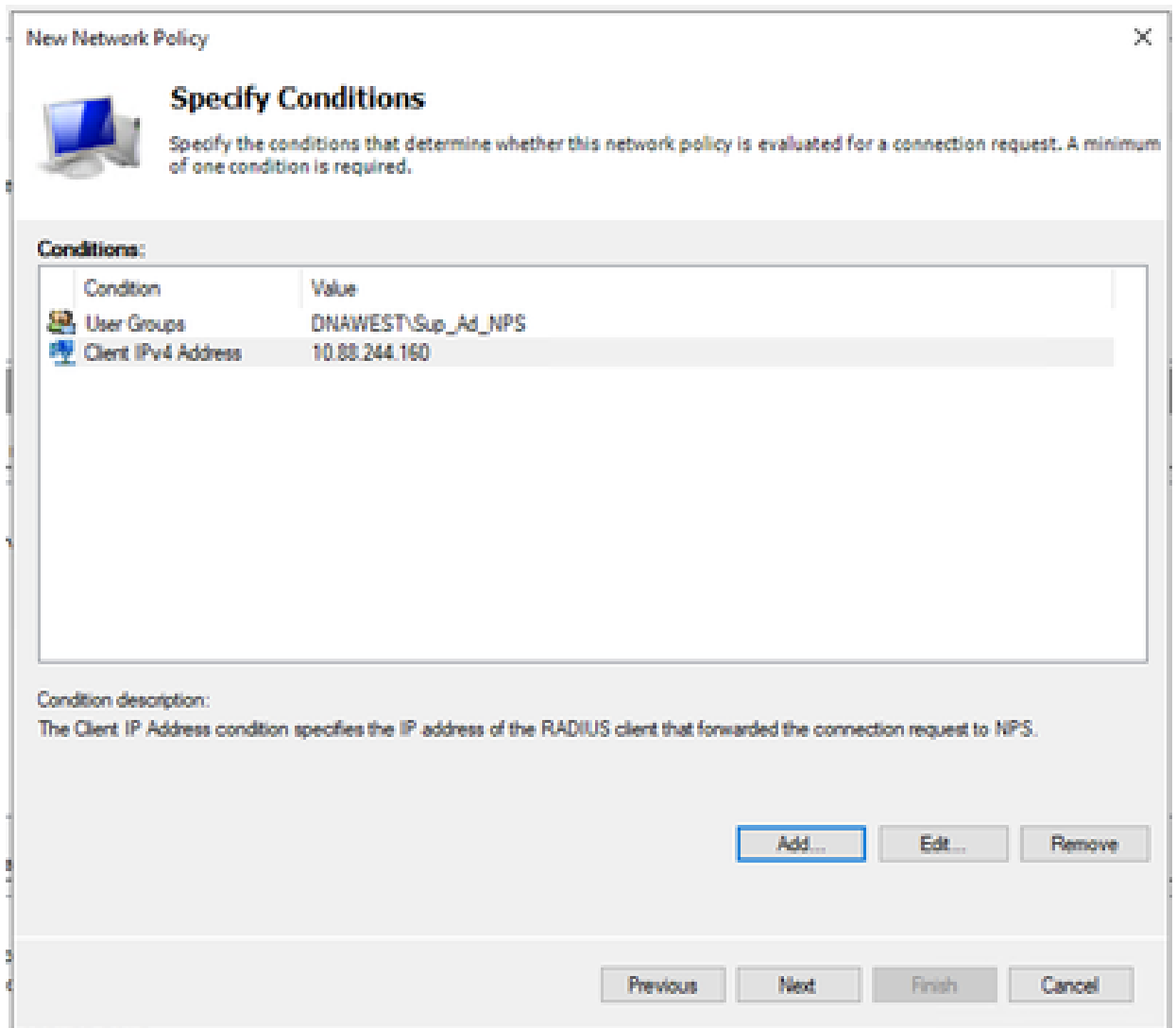
Vendor specific:
10

Previous Next Finish Cancel

策略名稱

9. 要允許特定域組，請增加以下兩個條件並按一下Next：


- User Group -增加您在Cisco DNA Center上可以具有管理員角色的域組（例如，使用 Sup_Ad_NPS組）。
- ClientIPv4Address -增加您的Cisco DNA Center管理IP地址。



政策條件

10. 選擇已授予訪問許可權，然後按一下下一步：

New Network Policy ✕



Specify Access Permission

Configure whether you want to grant network access or deny network access if the connection request matches this policy.

Access granted
Grant access if client connection attempts match the conditions of this policy.

Access denied
Deny access if client connection attempts match the conditions of this policy.

Access is determined by User Dial-in properties (which override NPS policy)
Grant or deny access according to user dial-in properties if client connection attempts match the conditions of this policy.

Previous Next Finish Cancel

使用授予的訪問許可權

11. 僅選擇Unencrypted authentication (PAP , SPAP) :



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Move Up

Move Down

Add...

Edit...

Remove

Less secure authentication methods:

- Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - User can change password after it has expired
- Microsoft Encrypted Authentication (MS-CHAP)
 - User can change password after it has expired
- Encrypted authentication (CHAP)
- Unencrypted authentication (PAP, SPAP)
- Allow clients to connect without negotiating an authentication method.

Previous

Next

Finish

Cancel

選取未加密的驗證

12. 由於使用了預設值，請選擇Next：



Configure Constraints

Constraints are additional parameters of the network policy that are required to match the connection request. If a constraint is not matched by the connection request, NPS automatically rejects the request. Constraints are optional; if you do not want to configure constraints, click Next.

Configure the constraints for this network policy.

If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Specify the maximum time in minutes that the server can remain idle before the connection is disconnected

Disconnect after the maximum idle time

Previous

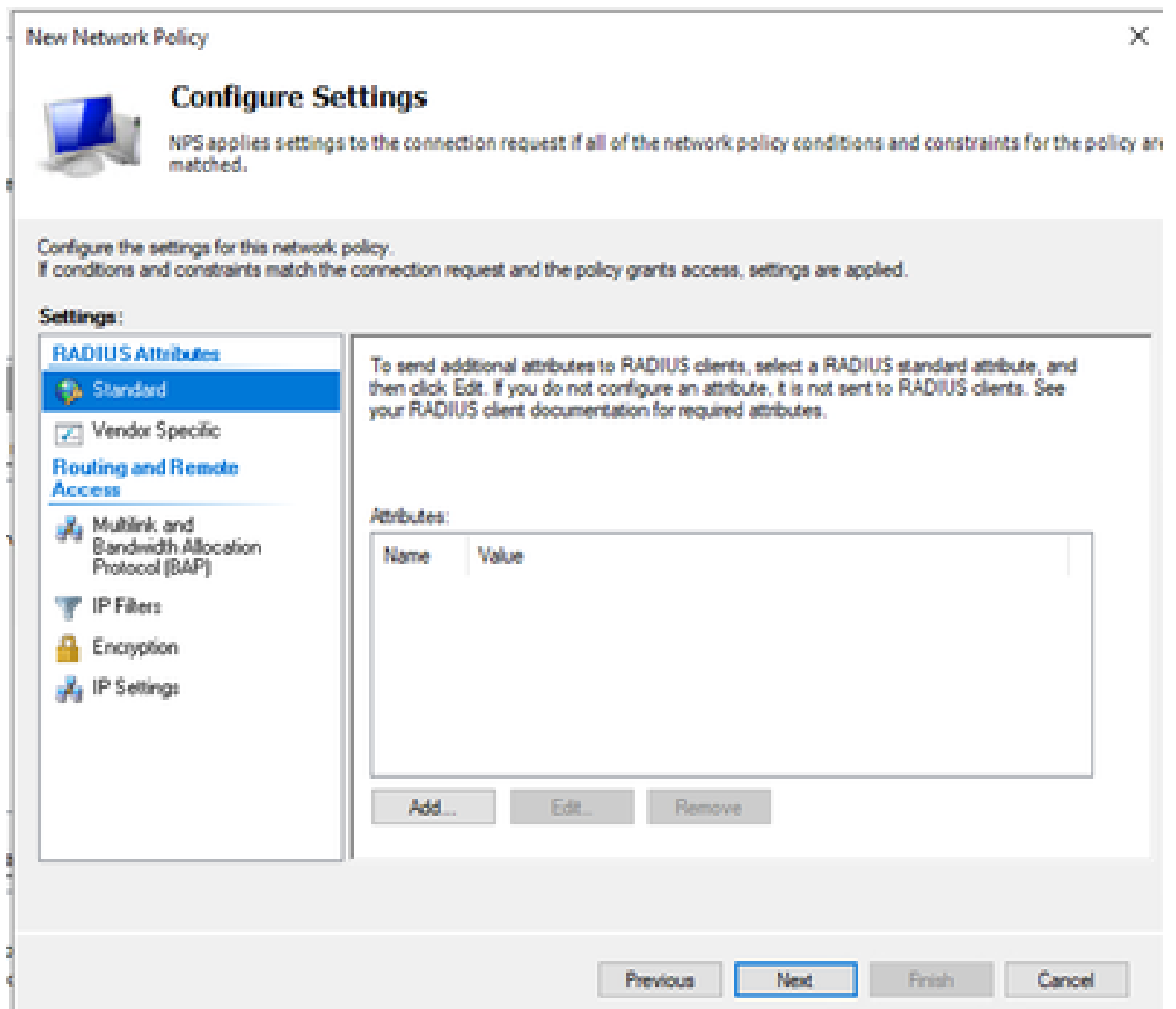
Next

Finish

Cancel

配置約束窗口

13. 移除標準屬性：



定義要使用的屬性

14. 在RADIUS屬性上，選擇Vendor Specific，然後按一下Add，選擇Cisco作為供應商，然後按一下Add：

Add Vendor Specific Attribute



To add an attribute to the settings, select the attribute, and then click Add.

To add a Vendor Specific attribute that is not listed, select Custom, and then click Add.

Vendor:

Disco

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add...

Close

增加Cisco AV對

15. 按一下Add，寫入Role=SUPER-ADMIN-ROLE，然後按一下OK兩次：



Configure Settings

NPS applies settings to the connection request if **all** of the network policy conditions and constraints for the policy are matched.

Configure the settings for this network policy.

If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

Standard

Vendor Specific

Routing and Remote Access

Multilink and Bandwidth Allocation Protocol (BAP)

IP Filters

Encryption

IP Settings

To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Cisco-AV-Pair	Cisco	Role=SUPER-ADMIN-ROLE

Add...

Edit...

Remove

Previous

Next

Finish

Cancel

增加了Cisco AV對屬性

16. 選擇關閉，然後選擇下一步。
17. 檢查策略設定，然後選擇Finish儲存策略。



Completing New Network Policy

You have successfully created the following network policy:

DNAC-Admin-Policy

Policy conditions:

Condition	Value
User Groups	DNAWEST\Sup_Ad_NPS
Client IPv4 Address	10.88.244.160

Policy settings:

Condition	Value
Authentication Method	Encryption authentication (CHAP)
Access Permission	Grant Access
Ignore User Dial-In Properties	False
Cisco-AV-Pair	Role=SUPER-ADMIN-ROLE

To close this wizard, click Finish.

Previous

Next

Finish

Cancel

策略摘要

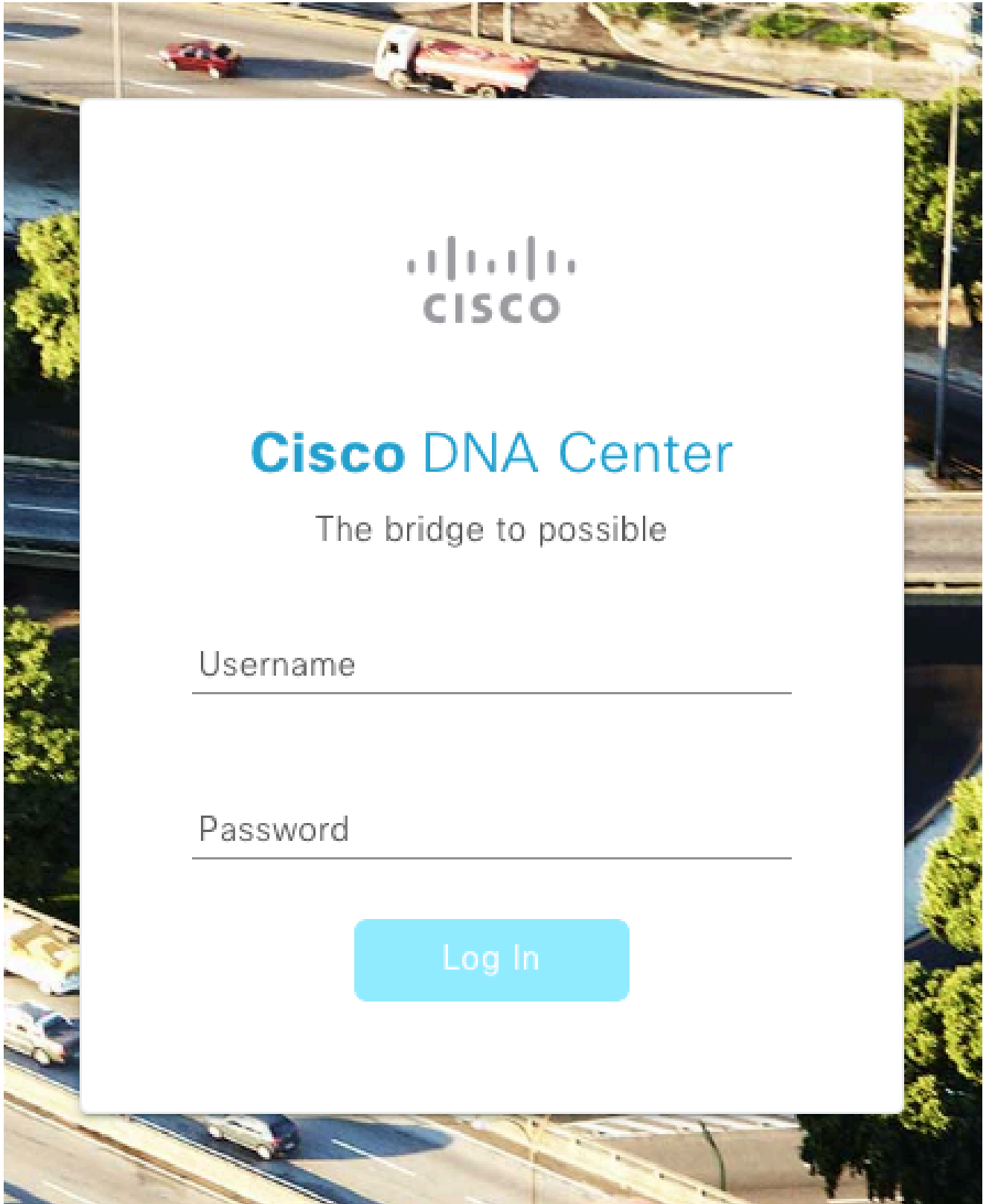
觀察者角色策略。

1. 按一下Windows Start選單並搜尋NPS。然後選擇Network Policy Server。
2. 從左側的導航面板中，按一下右鍵NPS (Local) 選項，然後選擇Register server in Active Directory。
3. 按一下OK兩次。
4. 展開RADIUS Clients and Servers，按一下右鍵RADIUS Clients，然後選擇New。
5. 輸入友好名稱、Cisco DNA Center管理IP地址和共用金鑰（以後可以使用）。
6. 按一下OK儲存它。
7. 展開策略，按一下右鍵網路策略，然後選擇新建。
8. 為規則輸入策略名稱，然後按一下Next。
9. 要允許特定域組，需要增加這兩個條件並選擇Next。

- User Group -增加您的域組，以便在Cisco DNA Center上分配觀察者角色（本示例使用Observer_NPS組）。
 - ClientIPv4Address -增加您的Cisco DNA Center管理IP。
10. 選擇授予訪問許可權，然後選擇下一步。
 11. 僅選擇Unencrypted authentication (PAP, SPAP)。
 12. 由於使用了預設值，請選擇Next。
 13. 移除標準屬性。
 14. 在RADIUS屬性上，選擇Vendor Specific，然後按一下Add，選擇Cisco作為供應商，然後按一下Add。
 15. 選擇Add，寫入ROLE=OBSERVER-ROLE，然後兩次選擇OK。
 16. 選擇關閉，然後選擇下一步。
 17. 檢查策略設定，然後選擇Finish儲存策略。

啟用外部身份驗證

1. 在Web瀏覽器中打開Cisco DNA Center Graphical User Interface (GUI)，然後使用管理員特權帳戶登入：



Cisco DNA Center登入頁面

2. 導航到選單>系統>設定> 身份驗證和策略伺服器，然後選擇增加> AAA：

Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

[+ Add ^](#) [↑ Export](#)

AAA	Protocol
ISE	RADIUS_TACACS

新增Windows Server

3. 鍵入您的Windows Server IP地址和前面步驟中使用的共用金鑰，然後按一下Save：

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. 驗證您的Windows Server狀態為Active：

10.88.244.148

RADIUS

AAA

ACTIVE



Windows Server摘要

5. 導航到選單 > 系統 > 使用者和角色 > 外部身份驗證，然後選擇您的AAA伺服器：

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

Update

Windows Server作為AAA伺服器

6. 鍵入Cisco-AVPair作為AAA屬性，然後按一下Update：

✓ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

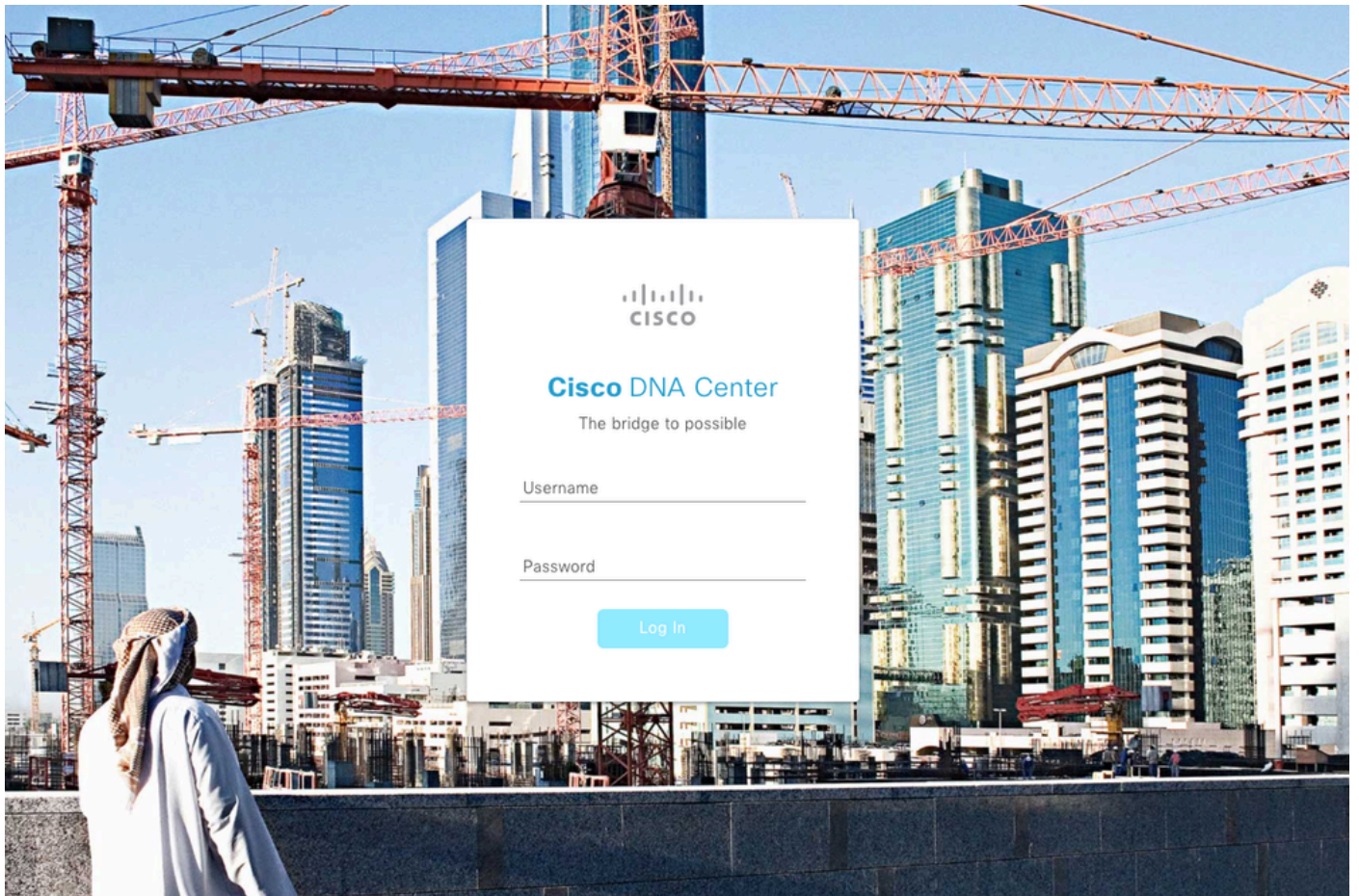
外部使用者上的AV對

7. 按一下Enable External User 覈取方塊以啟用外部身份驗證：

Enable External User 

驗證

您可以在Web瀏覽器中打開Cisco DNA Center圖形使用者介面(GUI)，然後使用在Windows Server中配置的外部使用者登入，以驗證可以使用外部身份驗證成功登入。



Cisco DNA Center 登入頁面

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。