

Configurer l'authentification externe sur Catalyst Center à l'aide de Windows Server

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Stratégie de rôle Admin](#)

[Politique de rôle Observateur](#)

[Activer l'authentification externe](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer l'authentification externe dans Cisco DNA Center à l'aide de Network Policy Server (NPS) dans Windows Server en tant que RADIUS.

Conditions préalables

Exigences

Connaissances de base sur :

- Utilisateurs et rôles de Cisco DNA Center
- Serveur de stratégie réseau Windows Server, RADIUS et Active Directory

Composants utilisés

- Cisco DNA Center 2.3.5.x
- Microsoft Windows Server Version 2019 agissant comme contrôleur de domaine, serveur DNS, NPS et Active Directory

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.



Remarque : le centre d'assistance technique Cisco (TAC) ne fournit pas d'assistance technique pour Microsoft Windows Server. Si vous rencontrez des problèmes avec la configuration de Microsoft Windows Server, contactez le support technique de Microsoft pour obtenir une assistance technique.

Configurer

Stratégie de rôle Admin

1. Cliquez sur dans le menu Démarrer de Windows et recherchez NPS. Sélectionnez ensuite Network Policy Server :

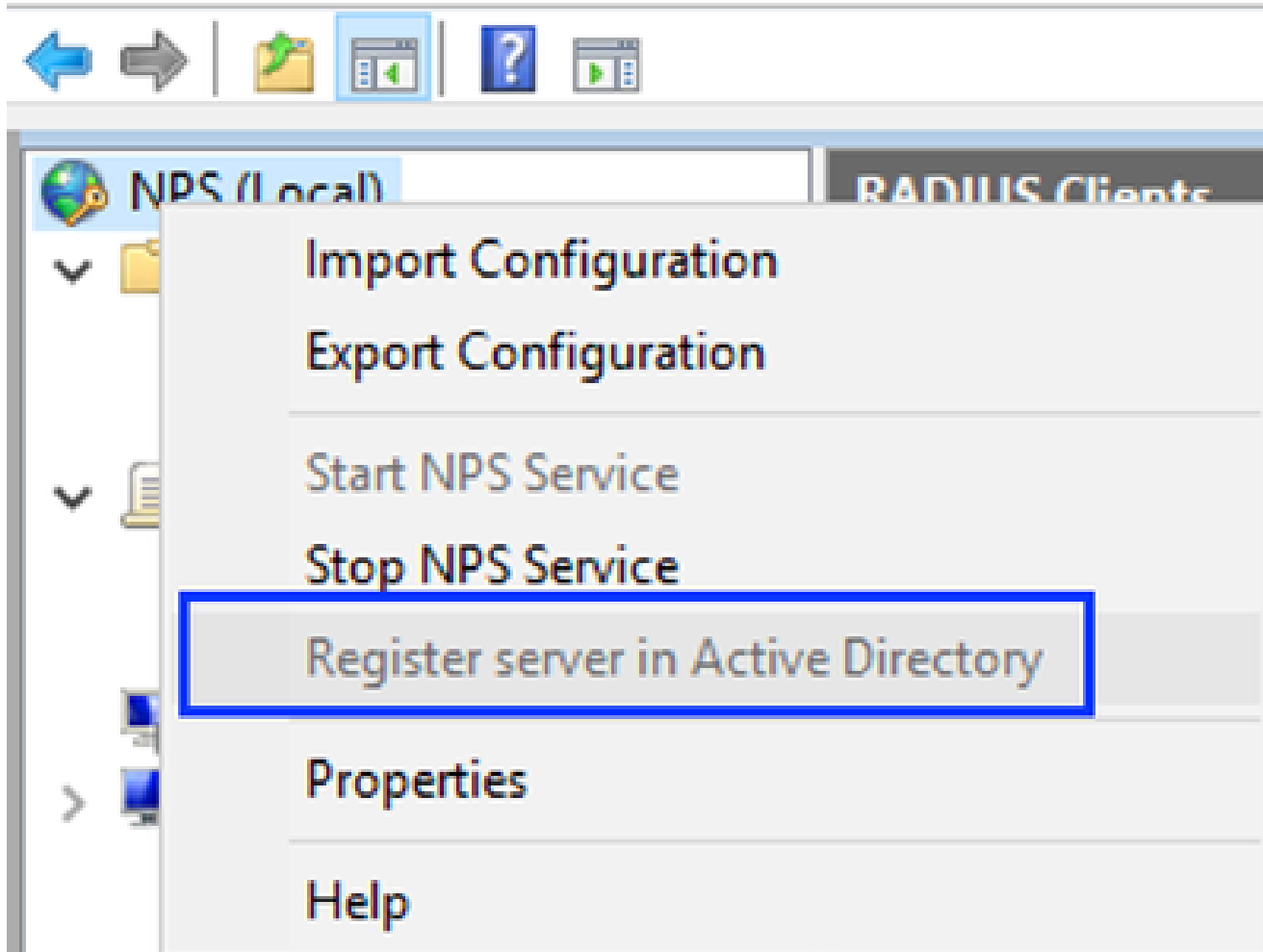


Network Policy Server

Desktop app

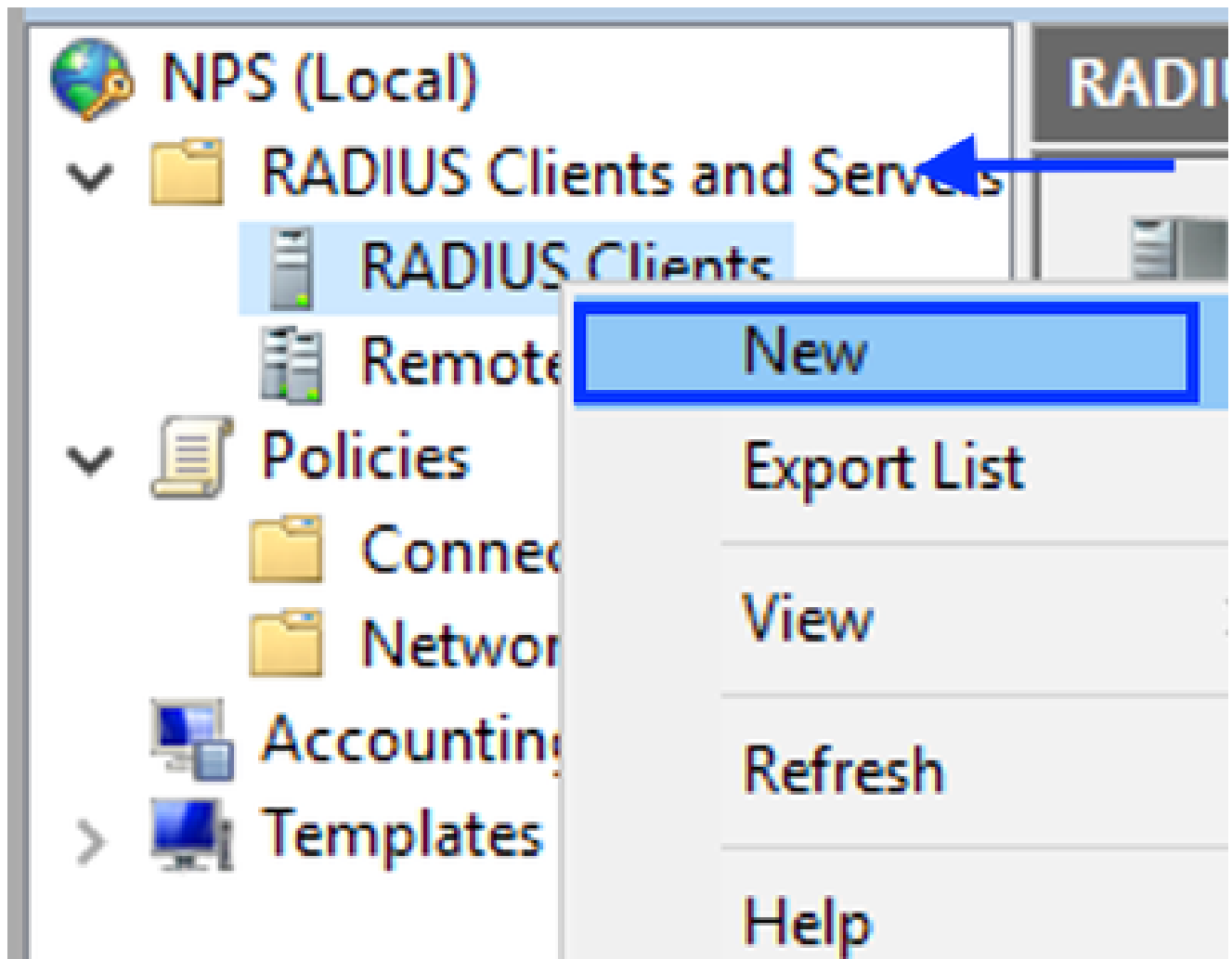
Network Policy Server

File Action View Help



Service de stratégie réseau Windows

3. Cliquez sur OK deux fois.
4. Développez Clients et serveurs RADIUS, cliquez avec le bouton droit sur Clients RADIUS, puis sélectionnez Nouveau :



Ajouter un client RADIUS

5. Saisissez le nom convivial, l'adresse IP de gestion de Cisco DNA Center et un secret partagé (ceci peut être utilisé ultérieurement) :

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

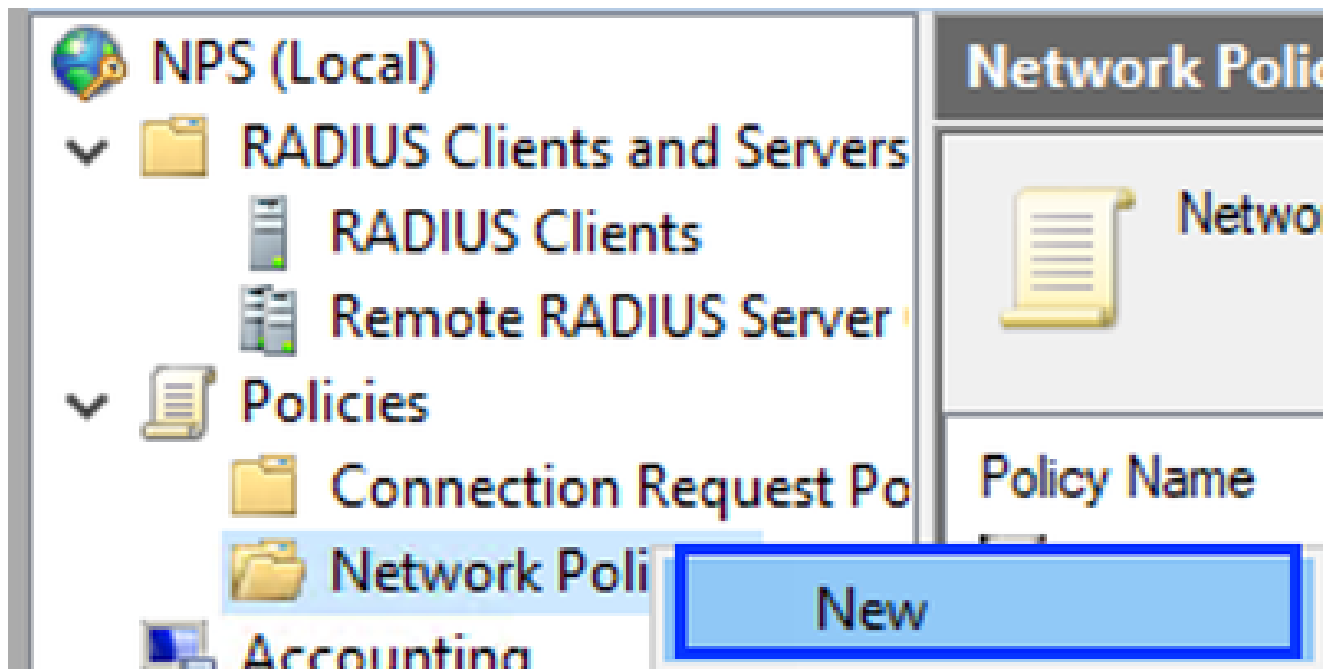
Shared secret:
●●●●●●●●

Confirm shared secret:
●●●●●●●●

OK Cancel Apply

Configuration du client Radius

6. Cliquez sur OK pour l'enregistrer.
7. Développez Stratégies, cliquez avec le bouton droit sur Stratégies réseau et sélectionnez Nouveau :



Ajouter une nouvelle politique de réseau

8. Entrez un nom de stratégie pour la règle et cliquez sur Suivant :



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:

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.

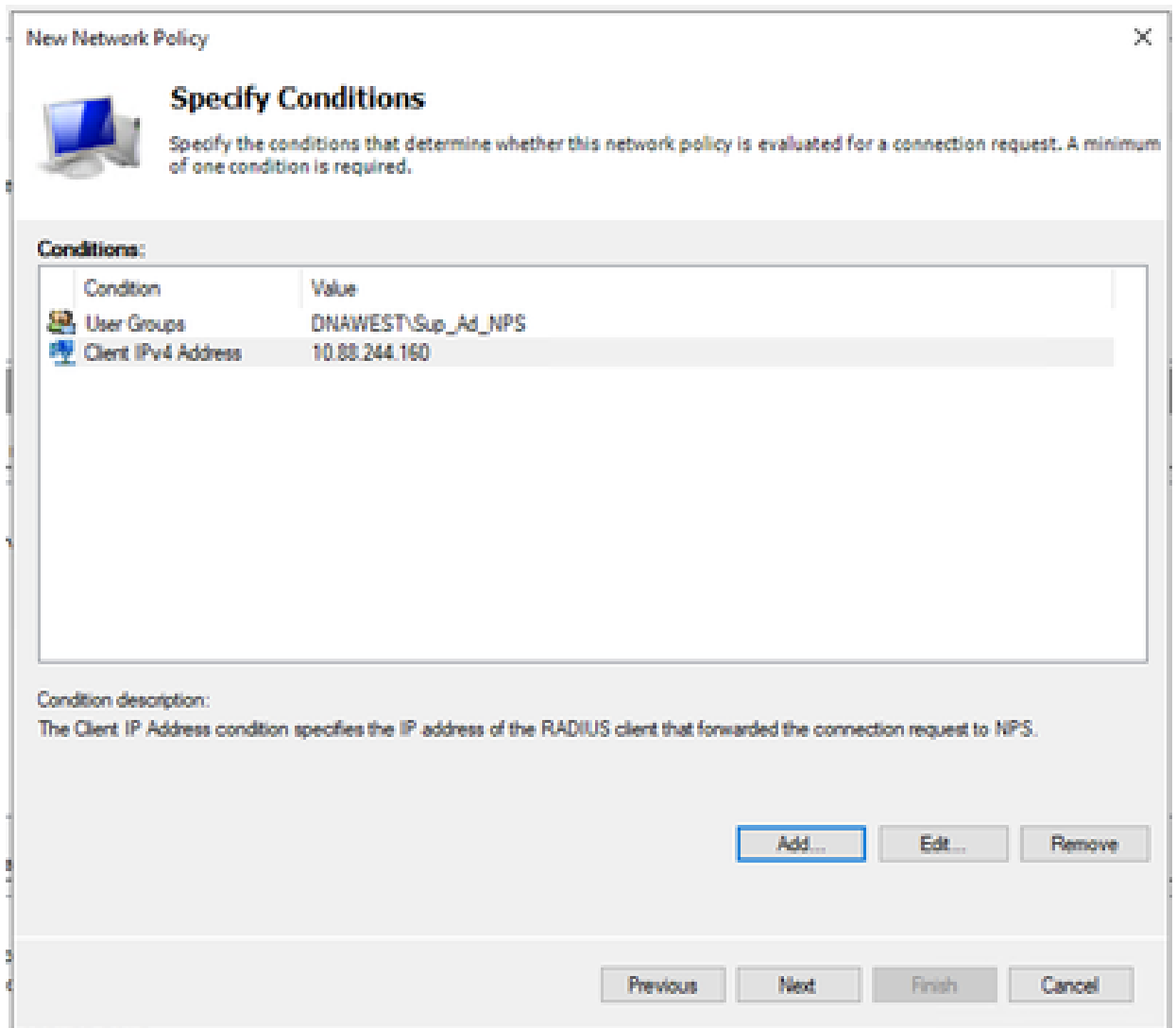
Type of network access server:

Vendor specific:

Nom de stratégie

9. Pour autoriser un groupe de domaines spécifique, ajoutez ces deux conditions et cliquez sur Suivant :


- Groupe d'utilisateurs - Ajoutez votre groupe de domaines pouvant avoir un rôle d'administrateur sur Cisco DNA Center (pour cet exemple, le groupe Sup_Ad_NPS est utilisé).
- ClientIPv4Address : ajoutez votre adresse IP de gestion Cisco DNA Center.



Conditions de stratégie

10. Sélectionnez Accès accordé et cliquez sur Suivant :

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

Utiliser l'accès accordé

11. Sélectionnez uniquement Authentication non chiffrée (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

Sélectionnez Authentification non chiffrée

12. Sélectionnez Next puisque les valeurs par défaut sont utilisées :



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

1

Previous

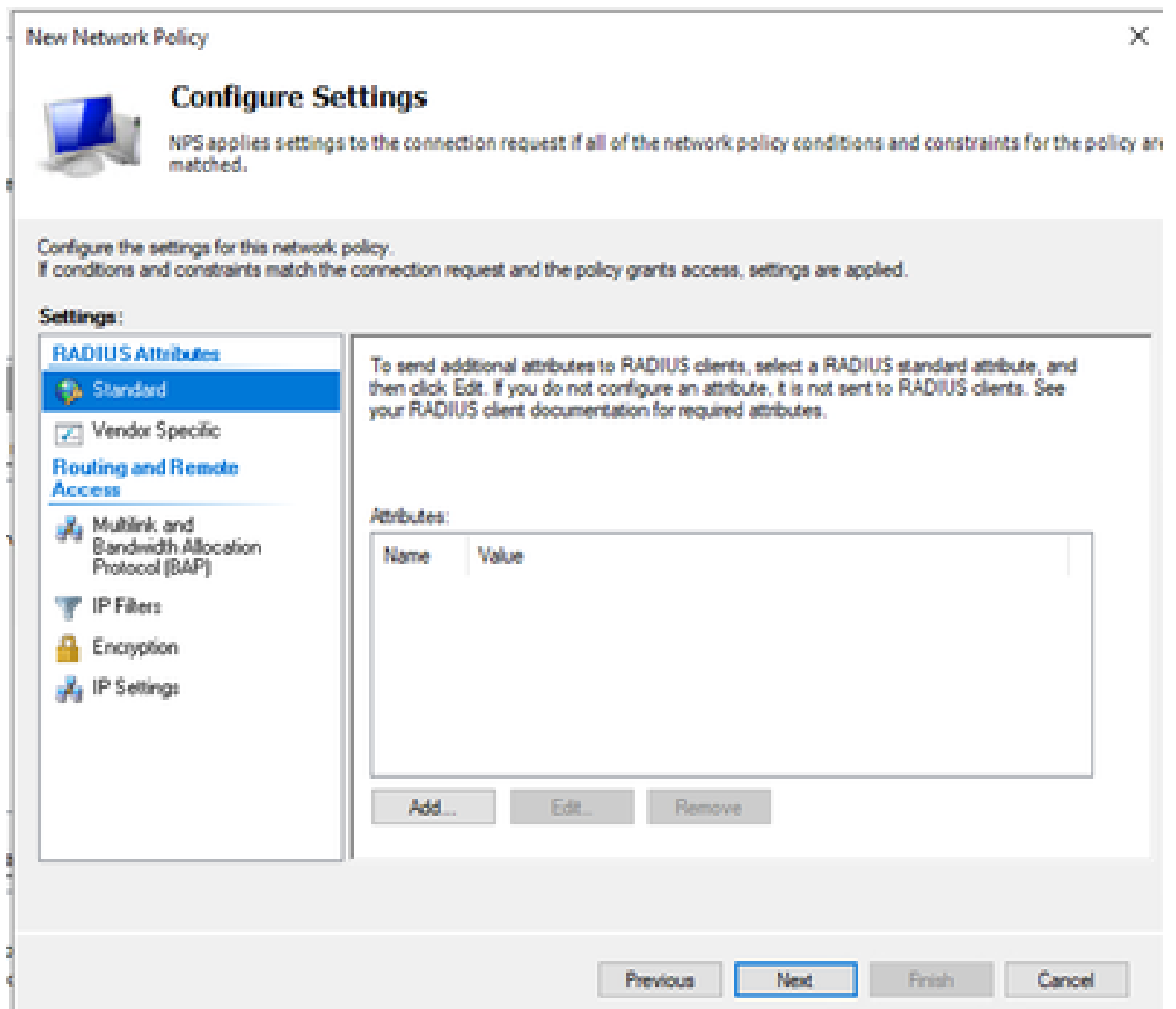
Next

Finish

Cancel

Fenêtre Configurer la contrainte

13. Supprimer les attributs standard :



Définir les attributs à utiliser

14. Dans RADIUS Attributes, sélectionnez Vendor Specific, puis cliquez sur Add, sélectionnez Cisco as a Vendor, et cliquez sur 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:

Attributes:

Name	Vendor
Cisco-AV-Pair	Cisco

Description:

Specifies the Cisco AV Pair VSA.

Add...

Close

Ajouter une paire AV Cisco

15. Cliquez sur Add, écrivez Role=SUPER-ADMIN-ROLE et cliquez sur OK deux fois :



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

Attribut de paire AV Cisco ajouté

16. Sélectionnez Fermer, puis Suivant.

17. Vérifiez vos paramètres de stratégie et sélectionnez Terminer pour l'enregistrer.



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

Récapitulatif des stratégies

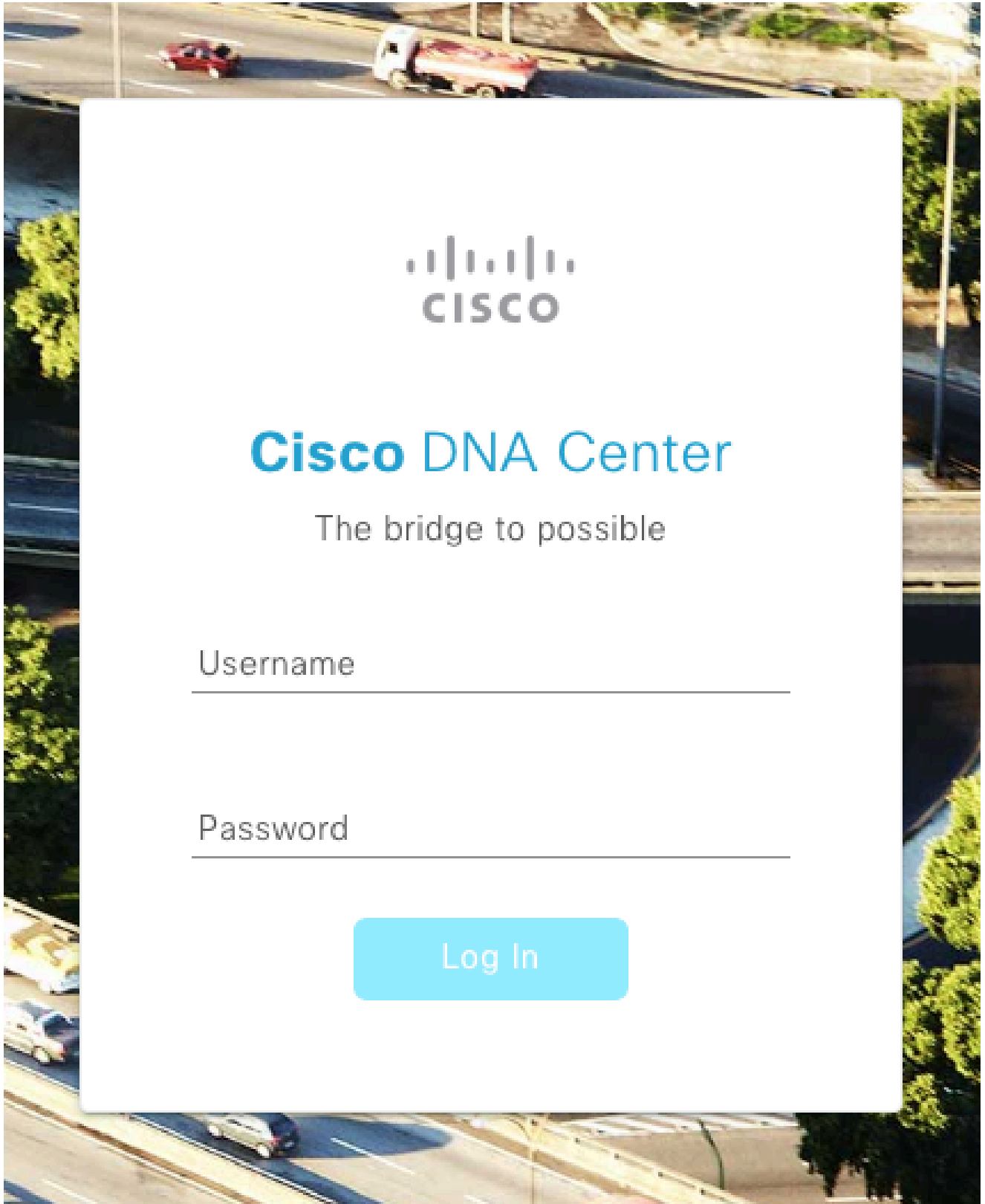
Politique de rôle Observateur.

1. Cliquez sur dans le menu Démarrer de Windows et recherchez NPS. Sélectionnez ensuite Network Policy Server.
2. Dans le volet de navigation sur le côté gauche, effectuez un clic droit dans l'option NPS (Local) et sélectionnez Register server in Active Directory.
3. Cliquez sur OK deux fois.
4. Développez RADIUS Clients and Servers, cliquez avec le bouton droit sur RADIUS Clients, puis sélectionnez New.
5. Saisissez un nom convivial, l'adresse IP de gestion de Cisco DNA Center et un secret partagé (ceci peut être utilisé ultérieurement).
6. Cliquez sur OK pour l'enregistrer.

7. Développez Stratégies, cliquez avec le bouton droit sur Stratégies réseau, puis sélectionnez Nouveau.
8. Entrez un nom de stratégie pour la règle et cliquez sur Next.
9. Pour autoriser un groupe de domaines spécifique, vous devez ajouter ces deux conditions et sélectionner Next.
 - Groupe d'utilisateurs - Ajoutez votre groupe de domaines afin d'attribuer un rôle d'observateur sur Cisco DNA Center (Pour cet exemple, le groupe Observer_NPS est utilisé).
 - ClientIPv4Address : ajoutez votre adresse IP de gestion Cisco DNA Center.
10. Sélectionnez Accès accordé, puis Suivant.
11. Sélectionnez uniquement Authentification non cryptée (PAP, SPAP).
12. Sélectionnez Next puisque les valeurs par défaut sont utilisées.
13. Supprimez les attributs Standard.
14. Dans Attributs RADIUS, sélectionnez Vendor Specific, puis cliquez sur Add, sélectionnez Cisco as a Vendor, et cliquez sur Add.
15. Sélectionnez Add, write ROLE=OBSERVER-ROLE, et OK deux fois.
16. Sélectionnez Fermer, puis Suivant.
17. Vérifiez vos paramètres de stratégie et sélectionnez Terminer pour l'enregistrer.

Activer l'authentification externe

1. Ouvrez l'interface utilisateur graphique de Cisco DNA Center dans un navigateur Web et connectez-vous à l'aide d'un compte d'administrateur privilégié :



Page de connexion à Cisco DNA Center

2. Accédez à Menu > System > Setting > Authentication and Policy Servers et sélectionnez Add > 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	4.189 RADIUS_TACACS

Ajouter un serveur Windows

3. Tapez votre adresse IP Windows Server et le secret partagé utilisé dans les étapes précédentes et cliquez sur Save :

Add AAA server



Server IP Address*

10.88.244.148

Shared Secret*

.....|

[SHOW](#)



Advanced Settings

Cancel

Save

4. Vérifiez que votre état Windows Server est Actif :

10.88.244.148

RADIUS

AAA

ACTIVE



Résumé de Windows Server

5. Accédez à Menu > System > Users & Roles > External Authentication et sélectionnez votre serveur AAA :

▼ AAA Server(s)

Primary AAA Server

IP Address

10.88.244.148

Shared Secret

[Info](#)

[View Advanced Settings](#)

Update

Windows Server comme serveur AAA

6. Tapez Cisco-AVPair comme attribut AAA et cliquez sur Update:

✓ AAA Attribute

AAA Attribute

Cisco-AVPair

Reset to Default

Update

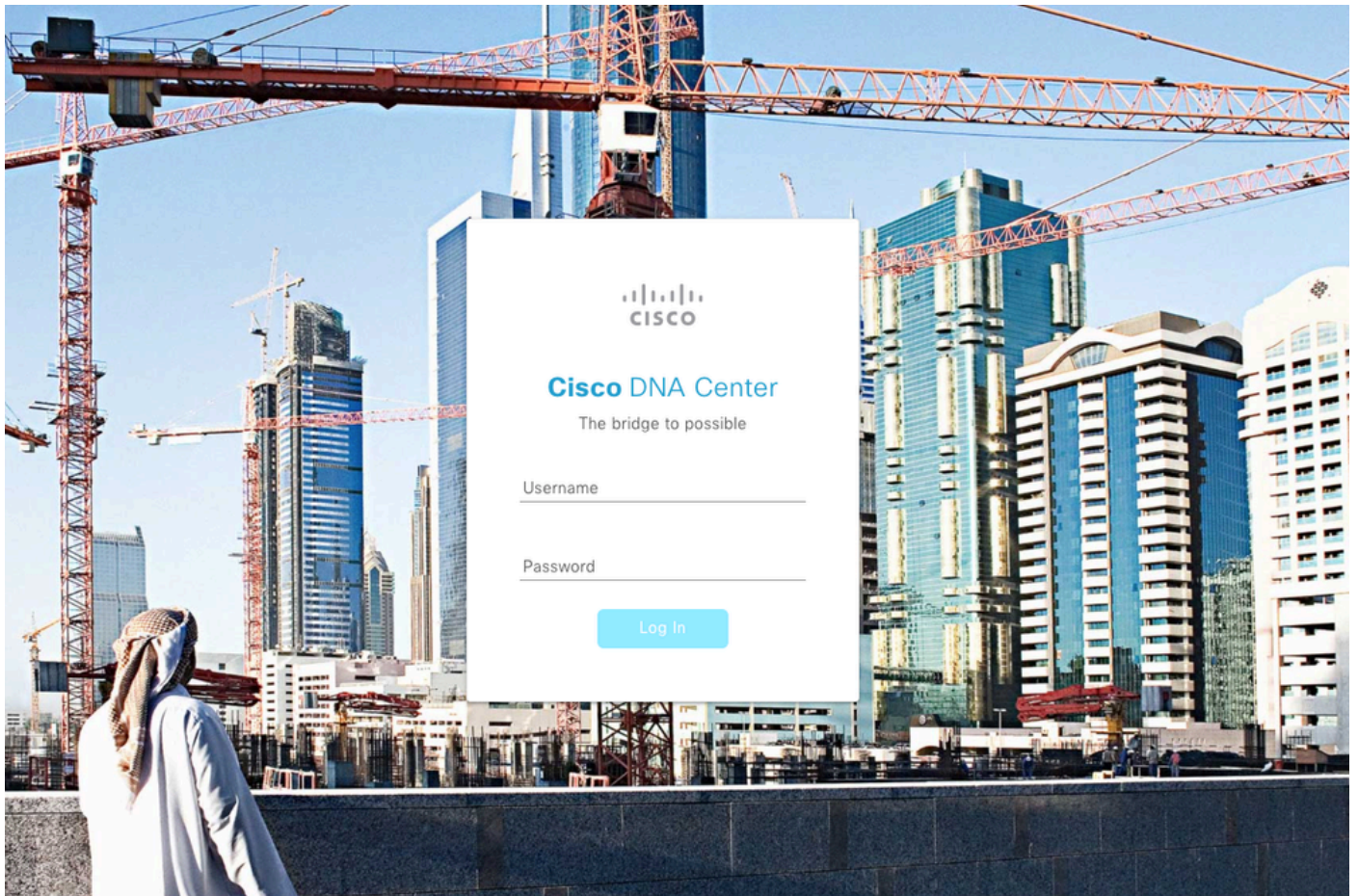
Paire AV sur utilisateur externe

7. Cochez la case Enable External User pour activer l'authentification externe :

Enable External User 

Vérifier

Vous pouvez ouvrir l'interface utilisateur graphique (GUI) de Cisco DNA Center dans un navigateur Web et vous connecter avec un utilisateur externe configuré dans le serveur Windows pour valider que vous pouvez vous connecter avec succès à l'aide de l'authentification externe.



Page de connexion à Cisco DNA Center

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.