Configuration et dépannage de l'authentification Radius sur UCSM

Table des matières

Introduction

Ce document décrit les étapes de configuration et de dépannage de Radius sur UCS Manager à l'aide d'un DataCenter Windows Server 2022.

Conditions préalables

- UCS Manager - 4.2(3o) ou supérieur
- DataCenter Windows Server 2022

Configuration sur Windows Server

Installer les services de domaine Active Directory

Consultez le document Microsoft - Installer AD DS à l'aide du Gestionnaire de serveur sur Windows Server 2022.

Créer l'utilisateur Active Directory (compte de connexion)

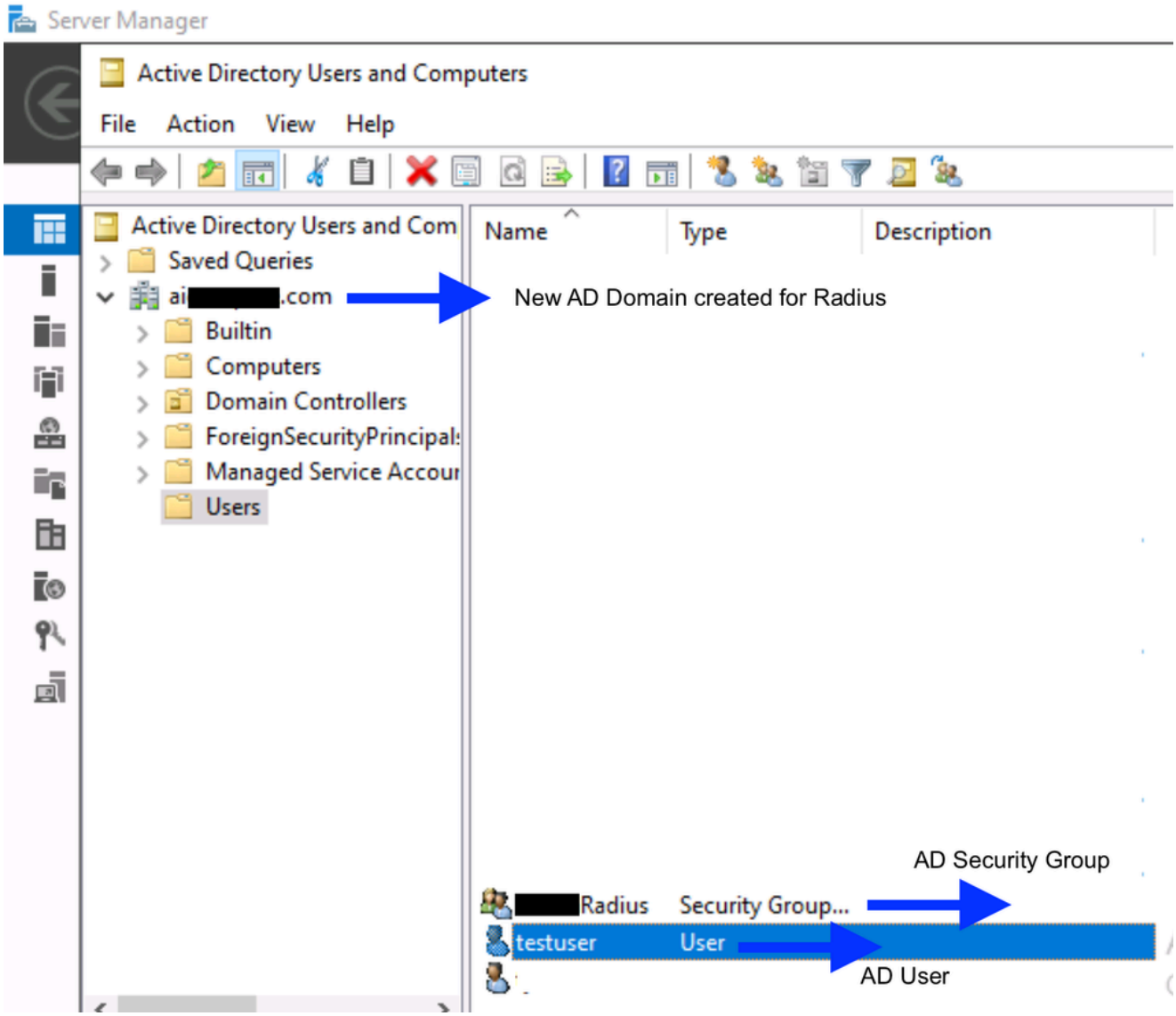
1. Ouvrez le Gestionnaire de serveur > Outils > Utilisateurs et ordinateurs Active Directory.

2. Cliquez avec le bouton droit sur le domaine que vous avez créé Nouveau > Utilisateur.

3. Entrez le nom de connexion (Exemple - testuser), définissez un mot de passe, décochez L'utilisateur doit changer de mot de passe à la prochaine ouverture de session, et cochez Mot de passe n'expire jamais (pour un compte de service/administrateur) > Terminer (en fonction de vos exigences/stratégies de sécurité locales).

Créer un groupe de sécurité AD pour les administrateurs UCS

- Dans la même console, cliquez avec le bouton droit sur votre domaine Nouveau > Groupe (Exemple - testRadius, Sécurité). Ajoutez l'utilisateur AD testuser) à ce groupe.
- Ce nom de groupe correspond à ce que vous devrez mapper ultérieurement à un rôle UCS.

- 

Installer NPS (rôle RADIUS) et enregistrer NPS dans Active Directory

1. Accédez à Gestionnaire de serveur > Gérer > Ajouter des rôles et des fonctionnalités.

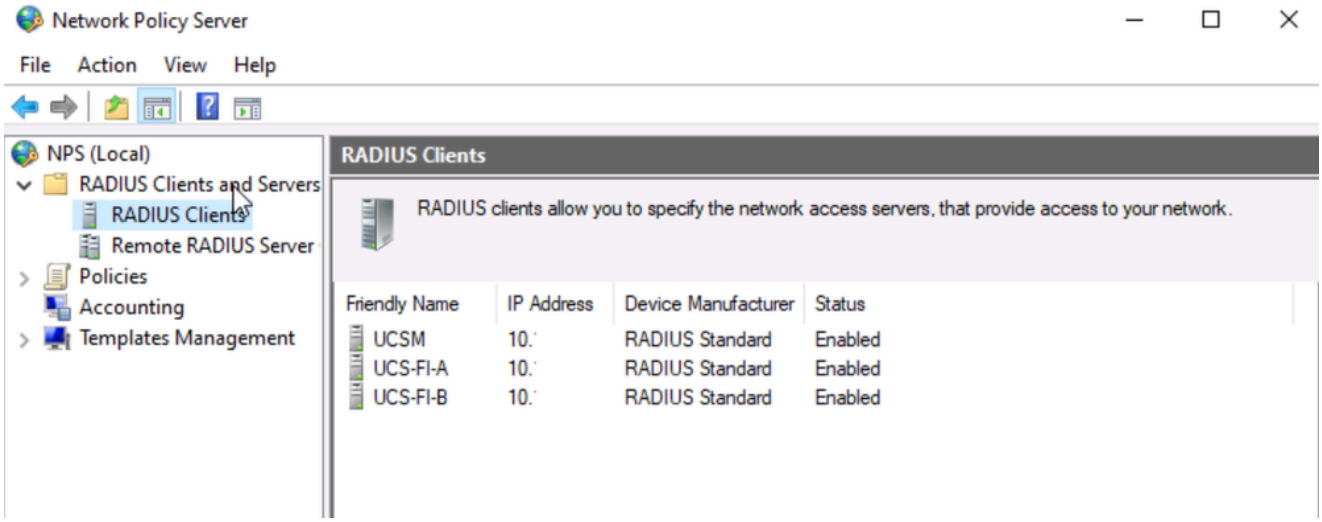
2. Sélectionnez Network Policy and Access Services > Exécutez l'Assistant pour installer le serveur NPS (Network Policy Server).

3. Ouvrez Outils > Serveur de stratégie réseau. Cliquez avec le bouton droit sur NPS (Local) > Register server in Active Directory > OK. Cela permet à NPS de lire l'appartenance d'un utilisateur/groupe AD.

Ajout des interconnexions de fabric UCS en tant que clients RADIUS

- Cela indique à NPS d'approuver les demandes UCSM. Dans NPS, développez RADIUS

Clients and Servers > RADIUS Clients. cliquez avec le bouton droit sur Nouveau.

- Fournir :
  - Nom convivial : Exemple - UCSM
  - Adresse (IP) : la PI de gestion de FI-A
  - Secret partagé : créez un secret fort et notez-le — vous devrez entrer cette chaîne exacte de secret partagé dans UCSM ultérieurement.
- Répétez l' pour Fabric Interconnect B et, si vous devez vous authentifier auprès du VIP du cluster, ajoutez cette adresse IP.
- 

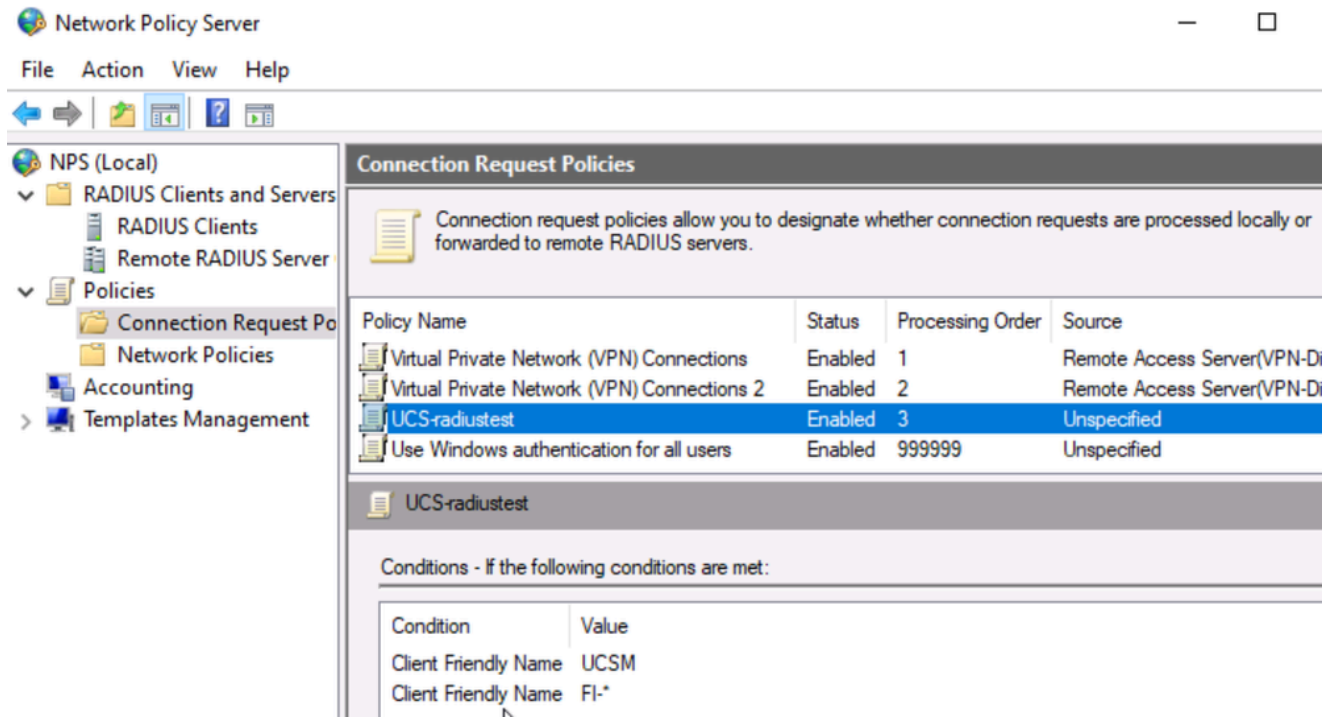
Clients Radius

Créer une stratégie de demande de connexion et une stratégie réseau (Autorisation et mappage de rôle)

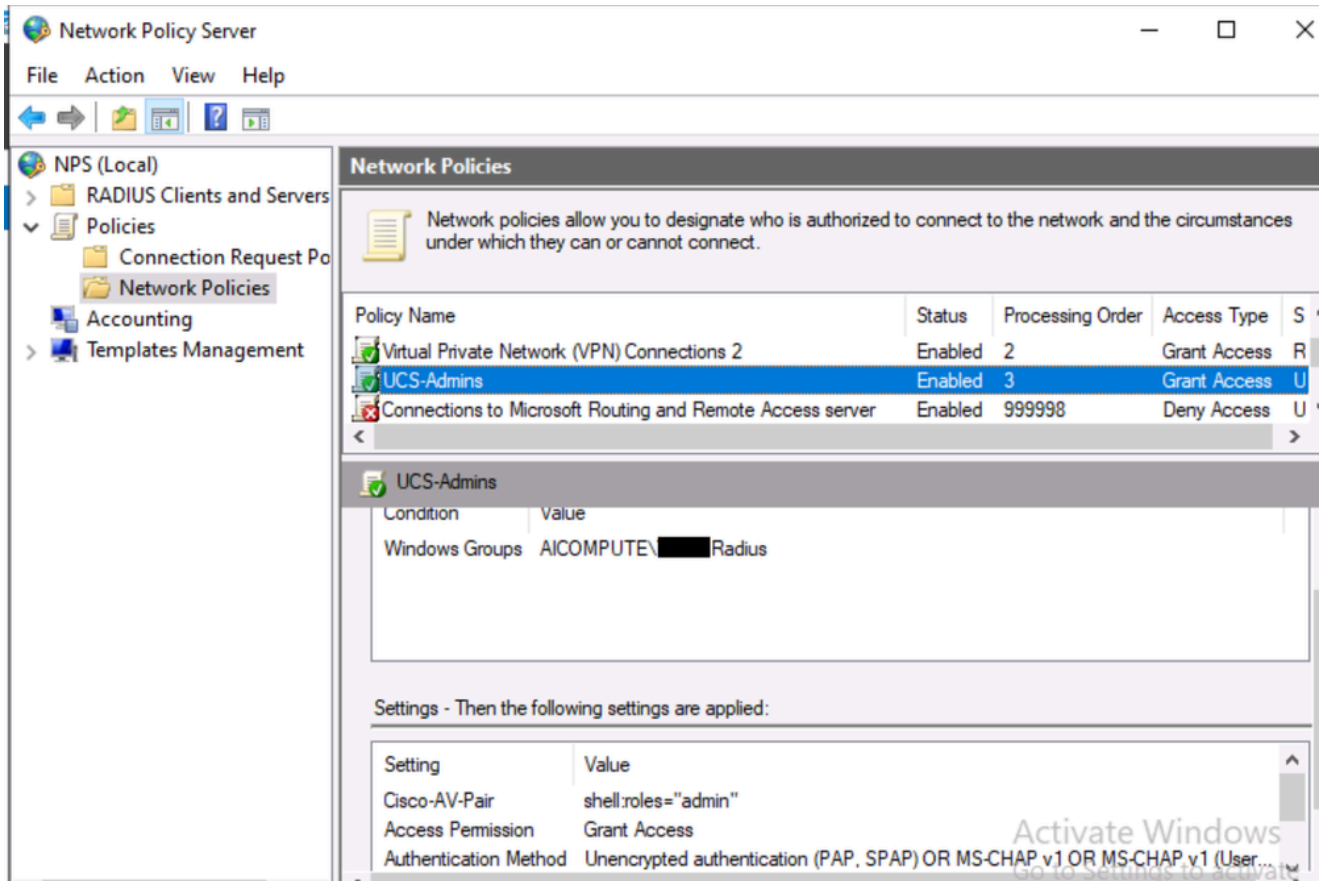
- Stratégies > Stratégies de demande de connexion > Nouveau > Nommez-le (Exemple - UCS-radiustest), ajoutez la condition « Nom convivial du client » qui lui permet de s'authentifier localement. Exemple : FI-* ou UCSM,
- Politiques > Politiques réseau > Nouveau > Nom de la politique
  - Modalités: ajouter des groupes Windows. Sélectionnez le groupe testRadius que vous avez créé à l'étape 3.
  - Autorisation d'accès : Accorder l'accès
  - Méthodes d'authentification : activer l'authentification non cryptée (PAP/SPAP) et/ou les méthodes utilisées par UCS. (UCS RADIUS utilise généralement le protocole PAP.)
- Configurer les paramètres > Attributs spécifiques au fournisseur (il s'agit de la partie clé qui mappe l'utilisateur AD à un rôle UCS) : Ajouter un attribut spécifique au fournisseur > Paire AV Cisco
  - Définissez la valeur sur la chaîne de rôle/paramètres régionaux UCS, Exemple - shell :

roles="admin" (Si vous ignorez cet attribut, l'utilisateur se connecte en lecture seule).

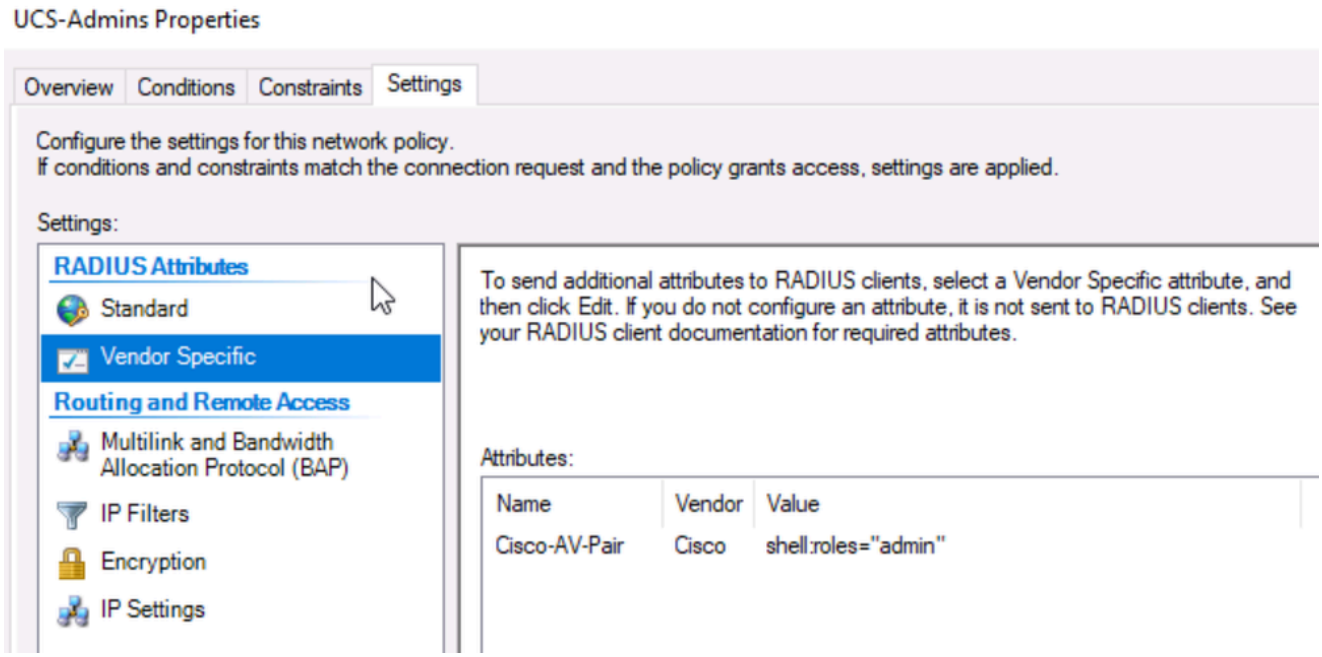
Stratégie de demande de connexion

- 

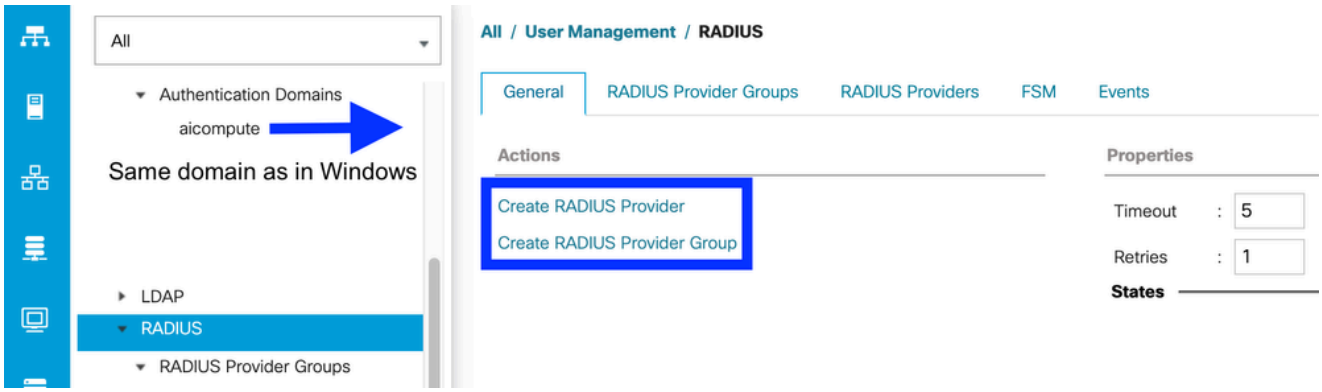
Politique de réseau

- 

Attribut spécifique au fournisseur

- 

Configuration sur UCSM

- 

Créer un fournisseur Radius et l'ajouter à un groupe de fournisseurs

1. Connectez-vous à l'interface utilisateur graphique d'UCS Manager et accédez à Admin > User Management > RADIUS.

2. Cliquez sur Create RADIUS Provider (l'option +/ Create) et renseignez :

- Nom d'hôte/FQDN ou IP : votre serveur NPS Windows.
- Clé : le secret partagé exact que vous avez défini à l'étape 5 de NPS.
- Port d'autorisation : 1812 (doit correspondre à NPS)
- Délai d'attente/tentatives : conservez les valeurs par défaut pour démarrer.

3. Sous Admin > User Management > RADIUS, créez un groupe de fournisseurs (Exemple - RADIUS-Grp) et ajoutez le fournisseur de la version précédente.

Créer un domaine d'authentification

C'est le morceau qui relie tout.

1. Accédez à Admin > User Management > Authentication > Authentication Domains.

2. Cliquez sur Create a Domain (Exemple - RADIUS - nom de domaine recommandé pour être identique au domaine créé dans NPS).

3. Définir le domaine = RADIUS.

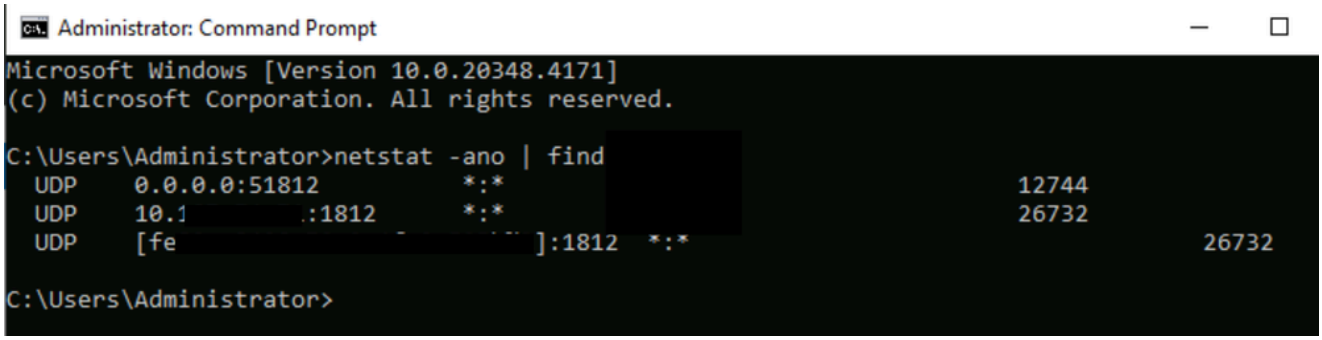
4. Affectez le groupe de fournisseurs que vous avez créé (RADIUS-Grp) et enregistrez.

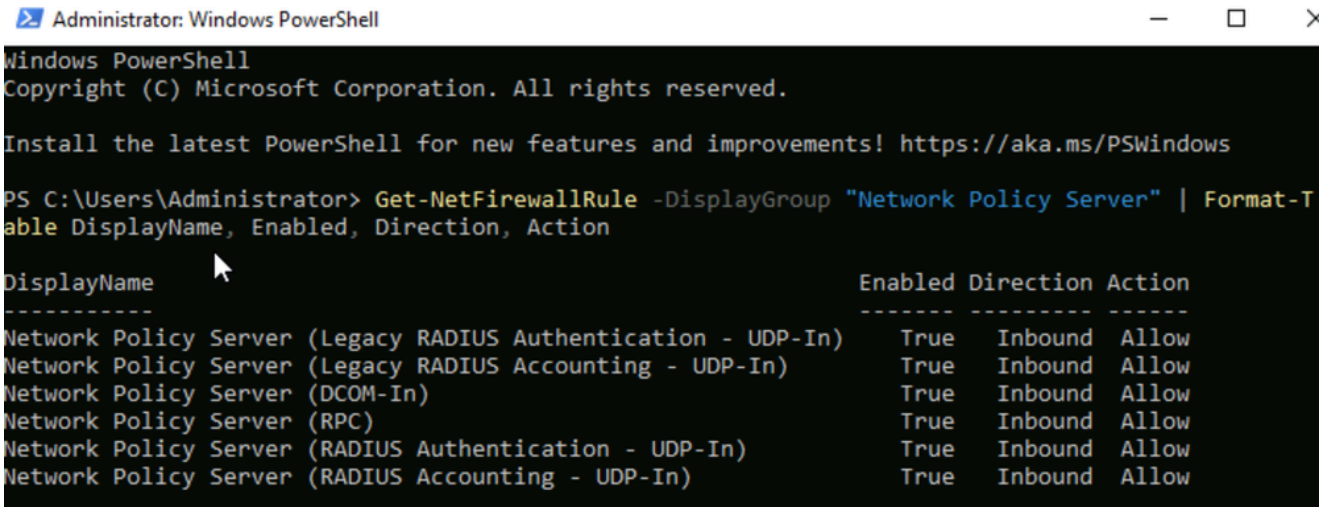
Vérifier

À partir de Windows Server - Confirmer le pare-feu / les ports

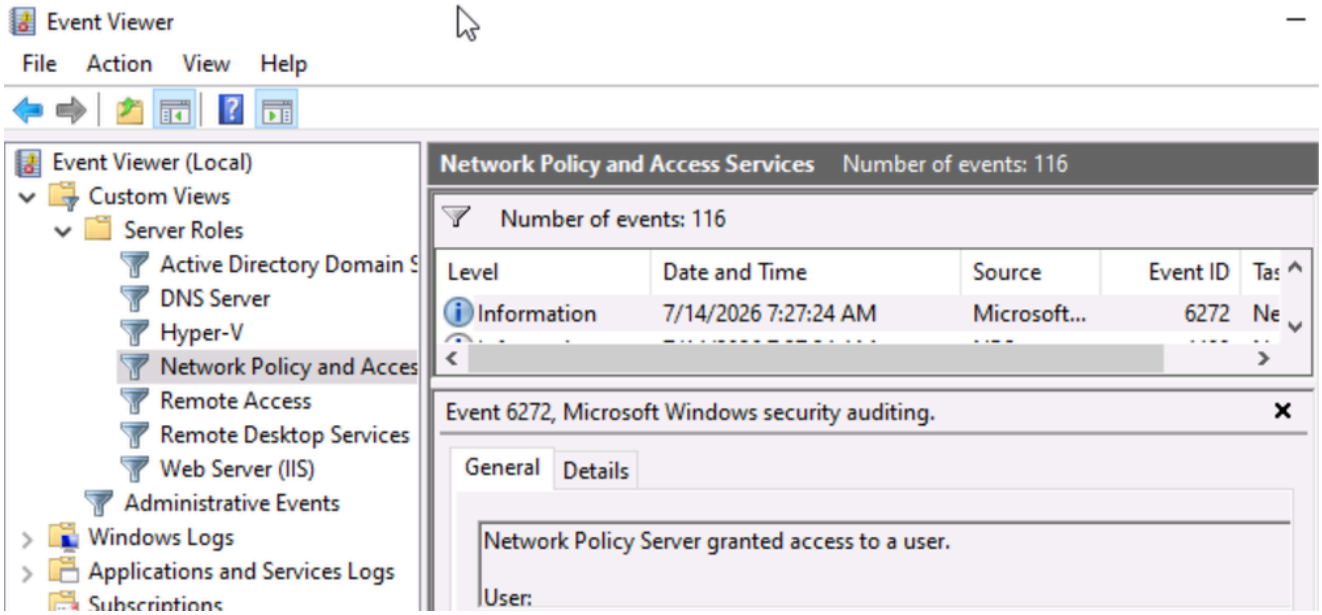
L'authentification RADIUS utilise le port UDP 1812 (et la comptabilité 1813). Assurez-vous que le pare-feu Windows et tout pare-feu réseau les autorisent à partir des adresses IP de gestion FI.

1. Confirmez que le service NPS / Radius écoute via netstat -ano | findstr 1812.

- (Vous voyez une ligne avec UDP et *:1812 (ou l'adresse IP du serveur : 1812). Cela confirme que le service NPS/RADIUS écoute activement.
- Si rien ne s'affiche, NPS ne peut pas être en cours d'exécution — cochez Services > Network Policy Server (IAS) is Started.)
- 

- Sous Windows Powershell, exécutez la commande :
  - Get-NetFirewallRule -DisplayGroup "Serveur de stratégie réseau" | Format-Table DisplayName, Enabled, Direction, Action.
- 

- Dans l'Observateur d'événements Windows :
  - Vues personnalisées > Rôles du serveur > Services de stratégie et d'accès réseau > Les paquets sont accessibles.



Tester la connexion depuis UCSM

1. Déconnectez-vous et connectez-vous en choisissant la liste déroulante Domain selon le domaine Radius créé.

2. Configurez le mot de passe utilisateur. (Reportez-vous à l'étape 2 de la configuration Windows).

- Si la connexion fonctionne et que vous atterrissez avec des privilèges d'administrateur, le mappage de la paire AV Cisco (étape 6 de la configuration Windows) est correct.

Dépannage de l'authentification Radius

Depuis Windows Server

1. Exécutez ces commandes dans Powershell pour la capture de paquets :

- pktmon filter add -p 1812
- pktmon start —capture —pkt-size 0 -f C:\radius_capture.etl

2. Lancez la connexion à partir d'UCSM et arrêtez la capture à l'aide des commandes :

- arrêt pktmon
- pktmon etl2pcap C:\radius_capture.etl -o C:\radius_capture.pcap

3. Ouvrez radius_capture.pcap dans Wireshark : RADIUS > Attribute Value Pairs > confirm Message-Authenticator (ou attribute 80). Cela signifie que NPS signe la réponse.

À partir de UCSM CLI

Lors de l'exécution de pktmon sous Windows, simultanément à partir de l'interface UCSM CLI,

1. exécutez la commande :

- connecter nxos
- moniteur de terminal
- debug radius all

2. tenter une connexion UCSM après avoir initié le débogage.

Une connexion réussie ressemble à 2026 Jul 3 09:54:02.917044 radius:Verified Message Authenticator en réponse de : 10.xxx.xx.xx.

- Si des paquets sont envoyés et reçus mais que la connexion échoue avec l'authentificateur de message, c'est probablement incorrect. dans la sortie de débogage - cela implique que le port et l'accessibilité sont corrects.
  - Essayez à nouveau de reconfigurer le secret partagé dans le serveur NPS Windows et la clé UCSM (ceux-ci doivent correspondre exactement).
  - Si le problème persiste lors de la connexion après la reconfiguration, nous pourrions rencontrer un bogue Cisco connu ID CSCwm80801 : L'utilisateur ne peut pas se connecter à UCSM à l'aide de Radius après le correctif Microsoft KB5040434 nécessitant une mise à niveau vers une version fixe mentionnée.

Informations connexes

- Guide d'administration de Cisco UCS Manager 4.2 - Authentification à distance

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.