Konfigurieren von Radius-Authentifizierung und Fehlerbehebung für UCSM

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Konfiguration und Fehlerbehebung von Radius auf UCS Manager mit einem Windows Server 2022 Data Center beschrieben.

Voraussetzungen

- UCS Manager - 4.2(3o) oder höher
- Windows Server 2022-Rechenzentrum

Konfiguration auf Windows Server

Active Directory-Domänendienste installieren

Weitere Informationen finden Sie im Microsoft-Dokument - Installieren von AD DS mithilfe des Server Managers unter Windows Server 2022.

Erstellen des Active Directory-Benutzers (Anmeldekonto)

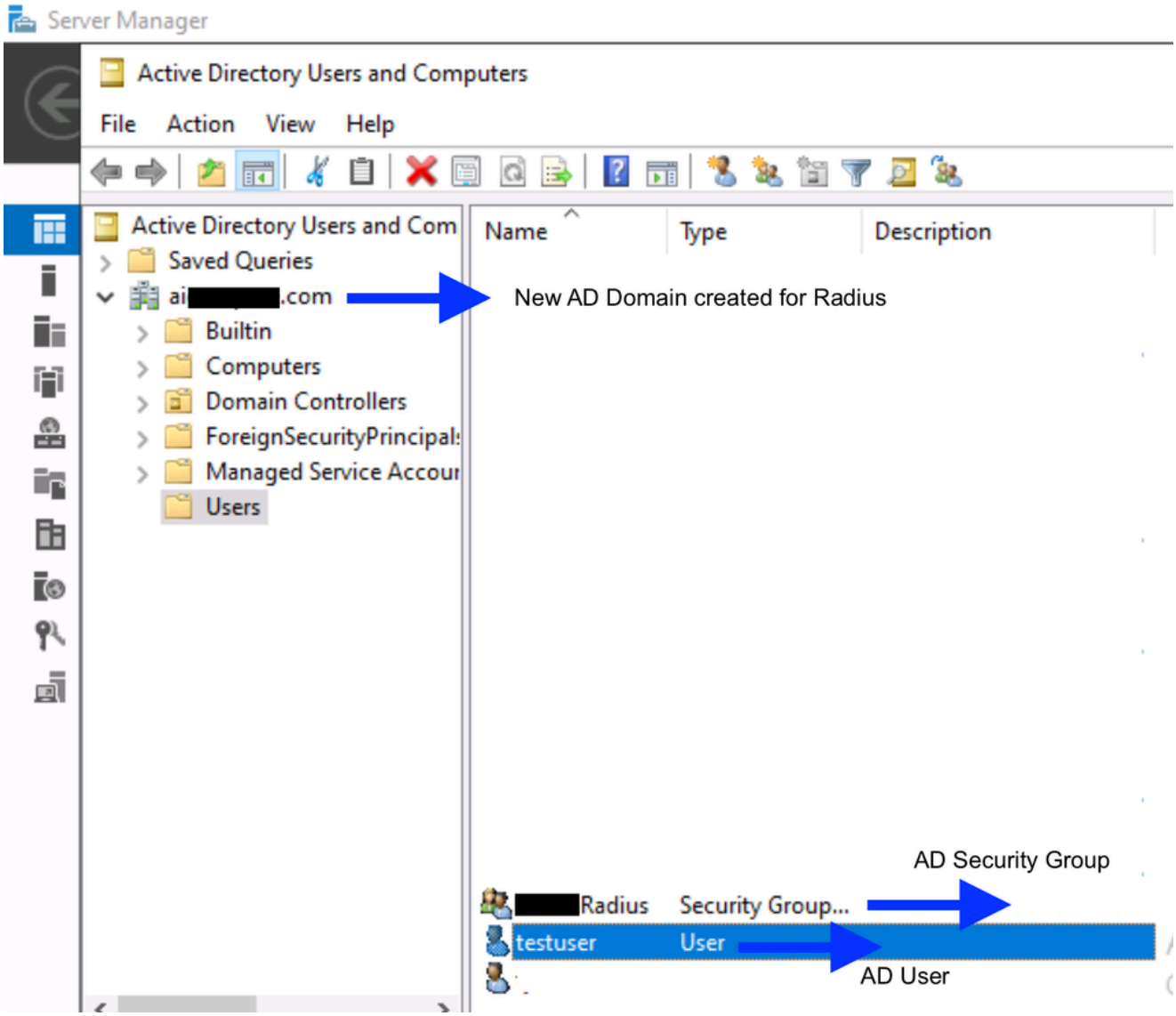
1. Öffnen Sie Server-Manager > Tools > Active Directory-Benutzer und -Computer.

2. Klicken Sie mit der rechten Maustaste auf Ihre erstellte Domäne Neu > Benutzer.

3. Geben Sie den Anmeldenamen ein (Beispiel - testuser), legen Sie ein Kennwort fest, deaktivieren Sie Benutzer muss Kennwort bei der nächsten Anmeldung ändern, und aktivieren Sie Kennwort läuft nie ab (für einen Service/Admin-Konto) > Beenden (abhängig von Ihren lokalen Sicherheitsanforderungen/-richtlinien).

Erstellen einer AD-Sicherheitsgruppe für UCS-Administratoren

- Klicken Sie in derselben Konsole mit der rechten Maustaste auf Ihre Domäne Neu > Gruppe (Beispiel - testRadius, Sicherheit). Fügen Sie den AD-Benutzer testuser) dieser Gruppe hinzu.
- Dieser Gruppenname muss später einer UCS-Rolle zugeordnet werden.

- 

NPS installieren (RADIUS-Rolle) und NPS in Active Directory registrieren

1. Navigieren Sie zu Server Manager > Verwalten > Rollen und Funktionen hinzufügen.

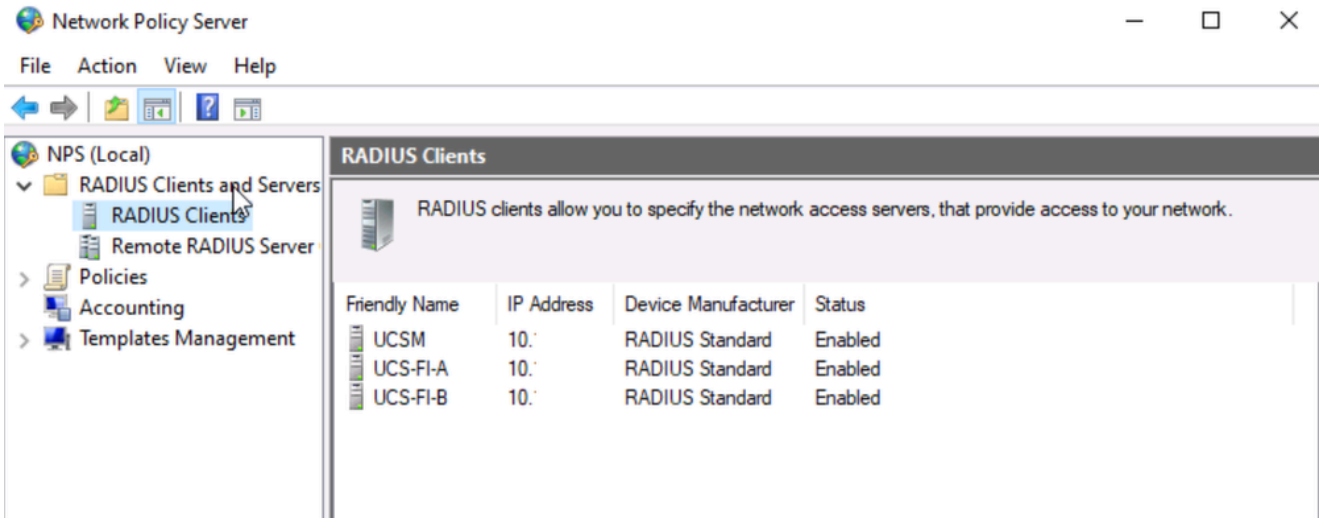
2. Wählen Sie Netzwerkrichtlinie und Zugriffsdienste > Assistenten abschließen, um den Netzwerkrichtlinienserver (NPS) zu installieren.

3. Öffnen Sie Tools > Network Policy Server. Klicken Sie mit der rechten Maustaste auf NPS (Lokal) > Server in Active Directory registrieren > OK. Dadurch kann NPS die AD-Benutzer-/Gruppenmitgliedschaft lesen.

Hinzufügen von UCS Fabric Interconnects als RADIUS-Clients

- Dadurch wird NPS angewiesen, Anforderungen von UCSM zu vertrauen. Erweitern Sie in

NPS die Option RADIUS Clients and Servers > RADIUS Clients (RADIUS-Clients und Server > RADIUS-Clients). Klicken Sie mit der rechten Maustaste auf Neu.

- Stellen Sie Folgendes bereit:
  - Anzeigename: Beispiel: UCSM
  - Adresse (IP): die Verwaltungs-IP von FI-A
  - Gemeinsamer Schlüssel: Erstellen Sie einen strengen Schlüssel, und notieren Sie sich diesen. Sie müssen diesen strengen Schlüssel zu einem späteren Zeitpunkt in UCSM eingeben.
- Wiederholen Sie den Vorgang für Fabric Interconnect B, und fügen Sie diese IP bei der Authentifizierung für die Cluster-VIP hinzu.
- 

Radius-Clients

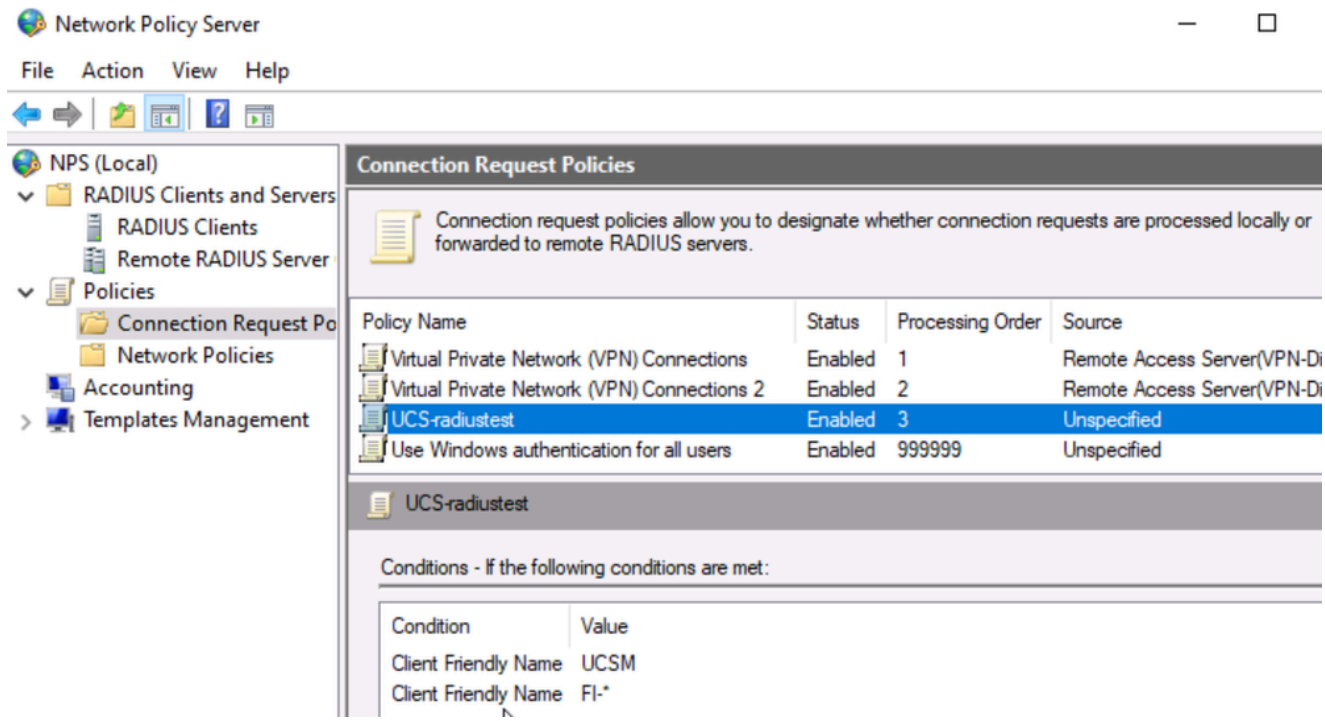
Erstellen einer Verbindungsanforderungsrichtlinie und einer Netzwerkrichtlinie (Autorisierung und Rollenzuordnung)

- Policies > Connection Request Policies > New > Name it (Beispiel - UCS-radiustest): Fügen Sie die Bedingung für "Client Friendly Name" hinzu, die eine lokale Authentifizierung ermöglicht. Beispiele: FI-* oder UCSM,
- Richtlinien > Netzwerkrichtlinien > Neu > Name der Richtlinie
  - Bedingungen: Windows-Gruppen hinzufügen. Wählen Sie die Gruppe testRadius aus, die Sie in Schritt 3 durchgeführt haben.
  - Zugriffsberechtigung: Zugriff gewähren
  - Authentifizierungsmethoden: Aktivieren Sie die unverschlüsselte Authentifizierung (PAP/SPAP) und/oder die vom UCS verwendeten Methoden. (UCS RADIUS verwendet in der Regel PAP.)
- Konfigurieren Sie Einstellungen > Herstellerspezifische Attribute (dies ist der

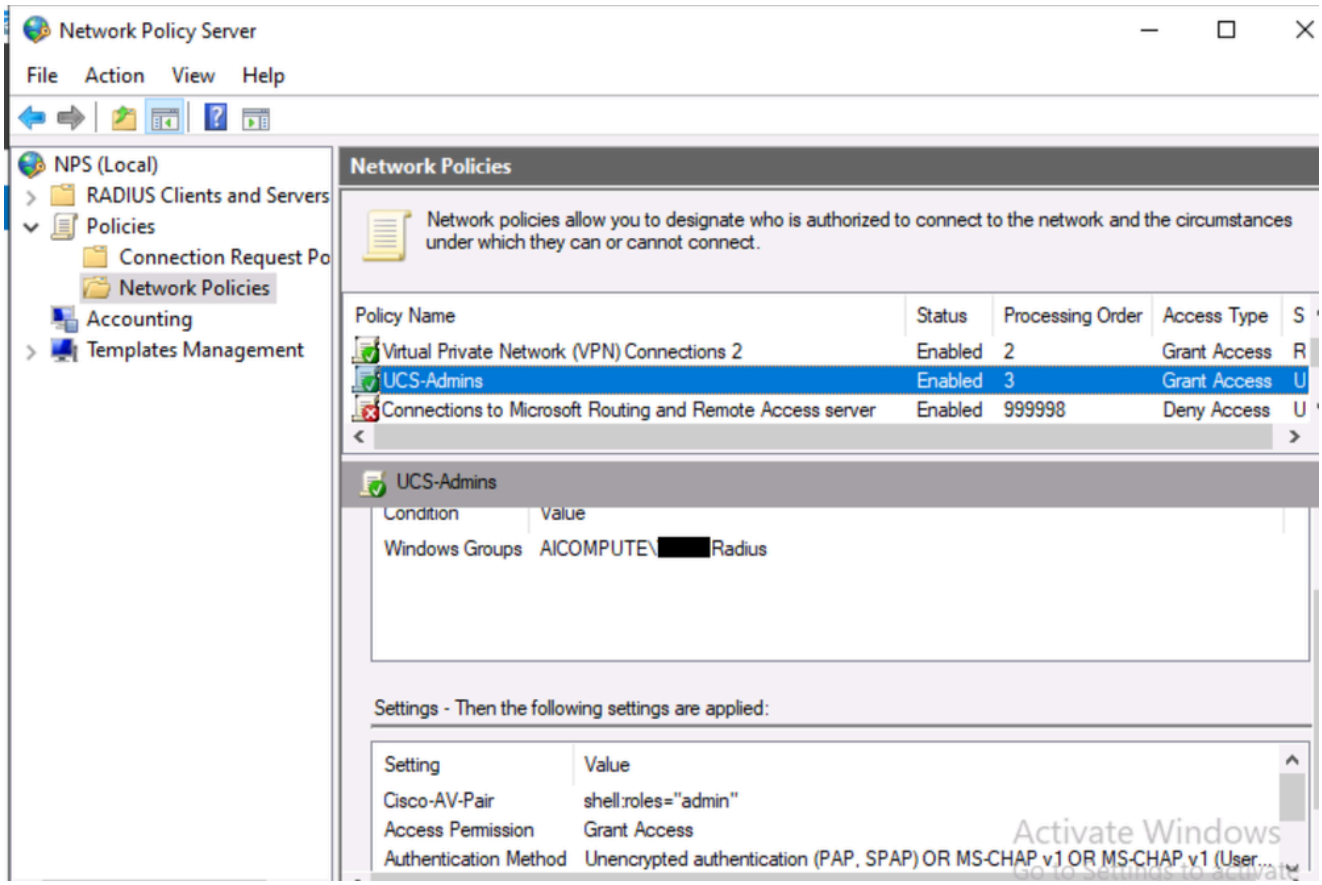
Hauptbestandteil, der den AD-Benutzer einer UCS-Rolle zuordnet): Herstellerspezifisches Attribut hinzufügen > Cisco AV-Pair

- Legen Sie den Wert auf die UCS-Rollen-/Gebietsschemazeichenfolge fest. Beispiel: shell:roles="admin" (Wenn Sie dieses Attribut überspringen, meldet sich der Benutzer schreibgeschützt an).

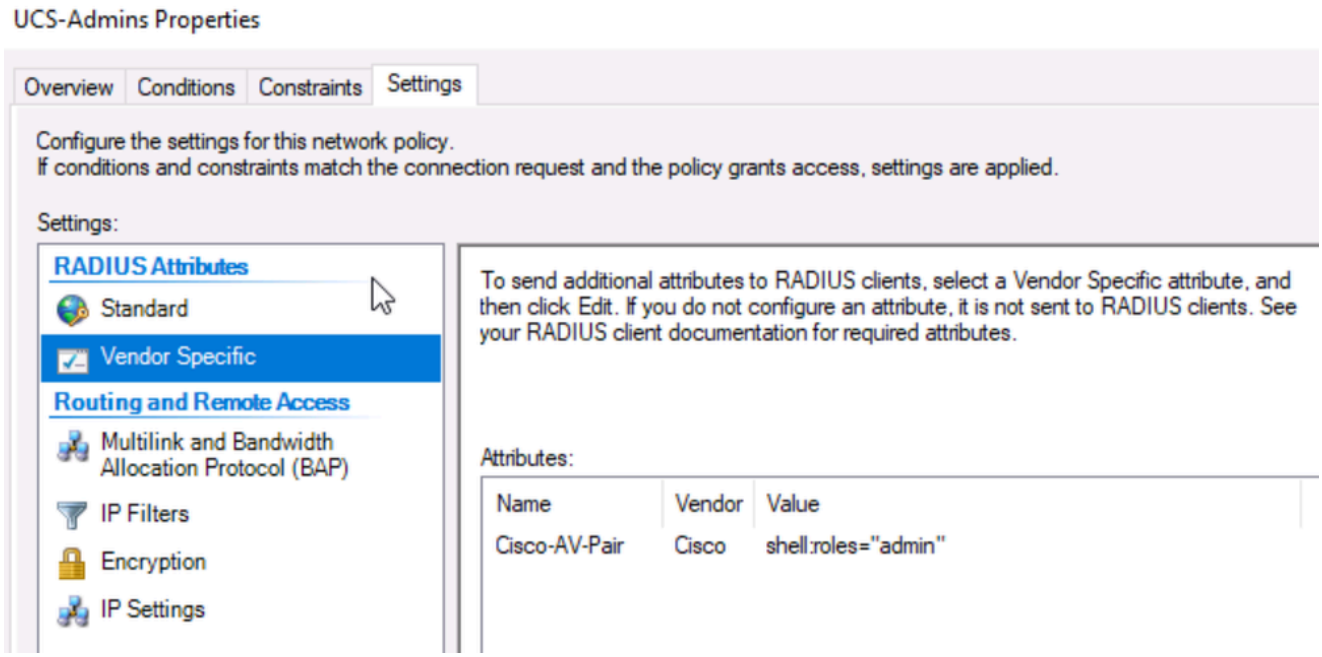
Verbindungsanforderungsrichtlinie

- 

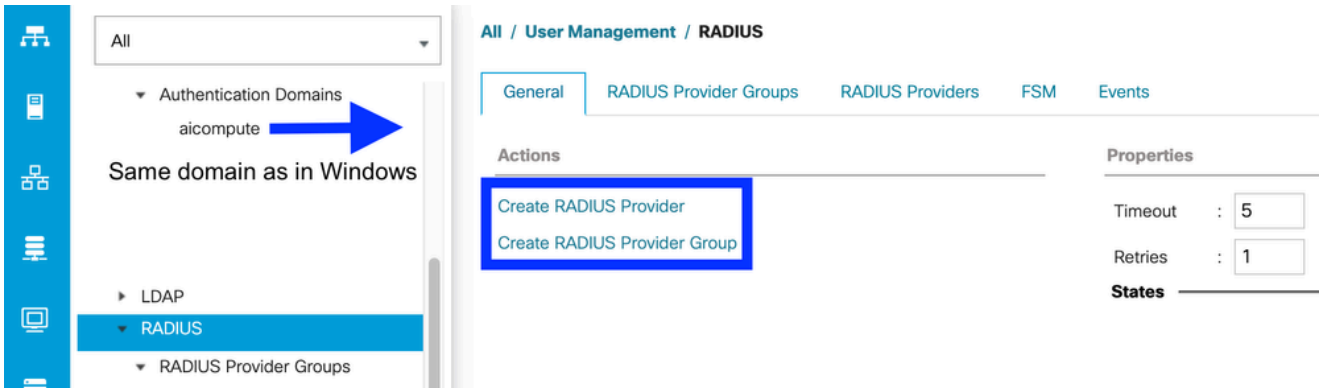
Netzwerkrichtlinie

- 

Herstellerspezifisches Attribut

- 

Konfiguration auf UCSM

- 

Erstellen eines Radius-Anbieters und Hinzufügen zu einer Anbietergruppe

1. Melden Sie sich bei der UCS Manager-GUI an, und navigieren Sie zu Admin > User Management > RADIUS (Admin > Benutzerverwaltung > RADIUS).

2. Klicken Sie auf Create RADIUS Provider (die Option +/ Create) und füllen Sie:

- Hostname/FQDN oder IP: Windows NPS-Server.
- Wichtigste: den genauen Shared Secret, den Sie in Schritt 5 des NPS festgelegt haben.
- Autorisierungs-Port: 1812 (muss mit NPS übereinstimmen)
- Timeout/Wiederholungen: belassen die Standardeinstellung auf "Start".

3. Erstellen Sie unter Admin > User Management > RADIUS eine Provider Group (Example - RADIUS-Grp), und fügen Sie den Provider von einer früheren Seite hinzu.

Erstellen einer Authentifizierungsdomäne

Das ist der Teil, der alles zusammenhält.

1. Navigieren Sie zu Admin > User Management > Authentication > Authentication Domains (Verwaltung > Benutzerverwaltung > Authentifizierung > Authentifizierungsdomänen).

2. Klicken Sie auf Create a Domain (Domäne erstellen) (Beispiel: RADIUS - Domänenname sollte mit der in NPS erstellten Domäne übereinstimmen).

3. Set Realm = RADIUS.

4. Weisen Sie die von Ihnen erstellte Anbietergruppe (RADIUS-Grp) zu, und speichern Sie.

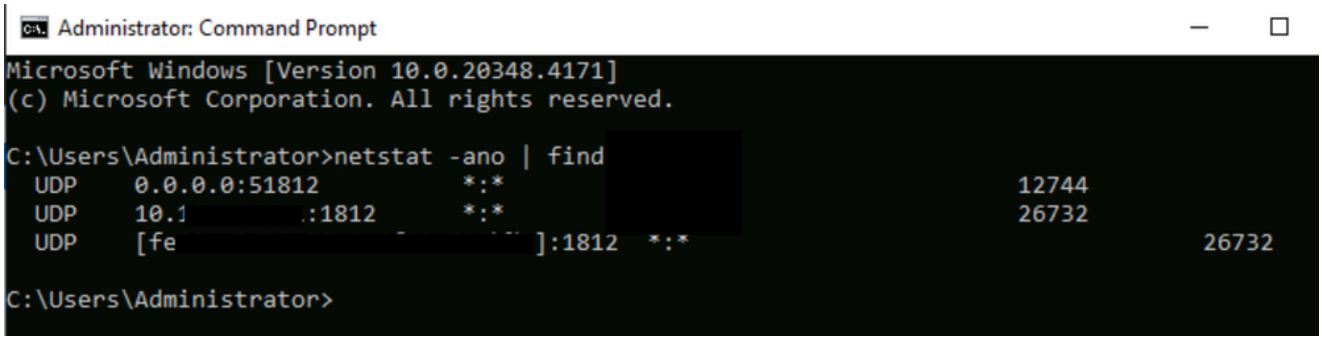
Überprüfung

Von Windows Server - Firewall/Ports bestätigen

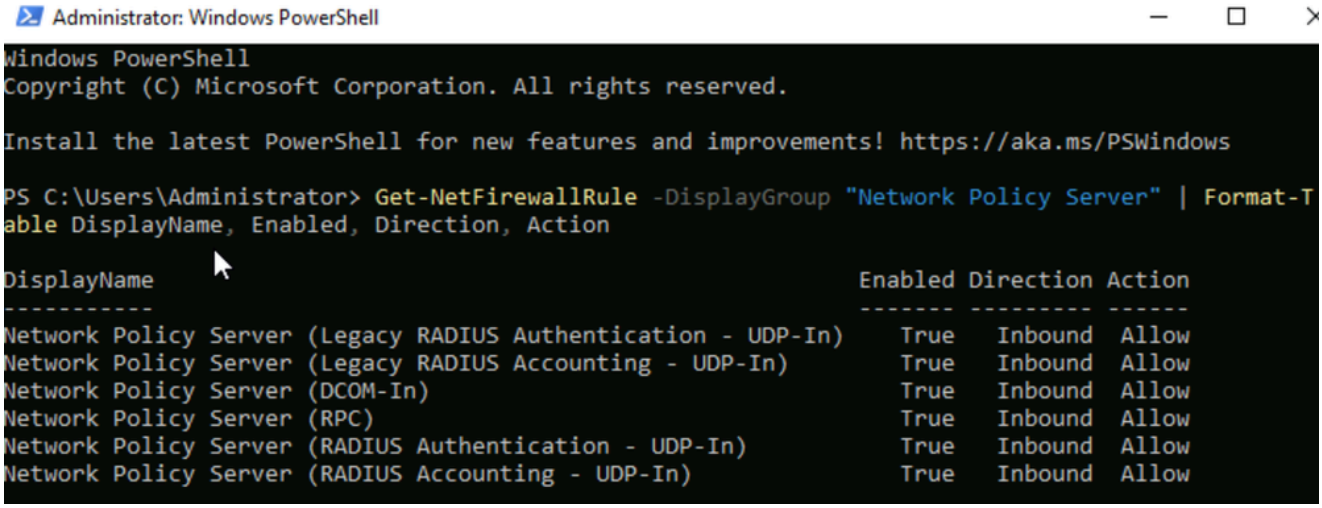
Die RADIUS-Authentifizierung verwendet den UDP-Port 1812 (und die Abrechnung 1813). Stellen Sie sicher, dass die Windows-Firewall und alle Netzwerk-Firewalls diese von den FI-Mgmt-IPs zulassen.

1. Bestätigen Sie, dass der NPS/Radius-Dienst über den netstat -ano abhört. | findstr 1812 Befehl.

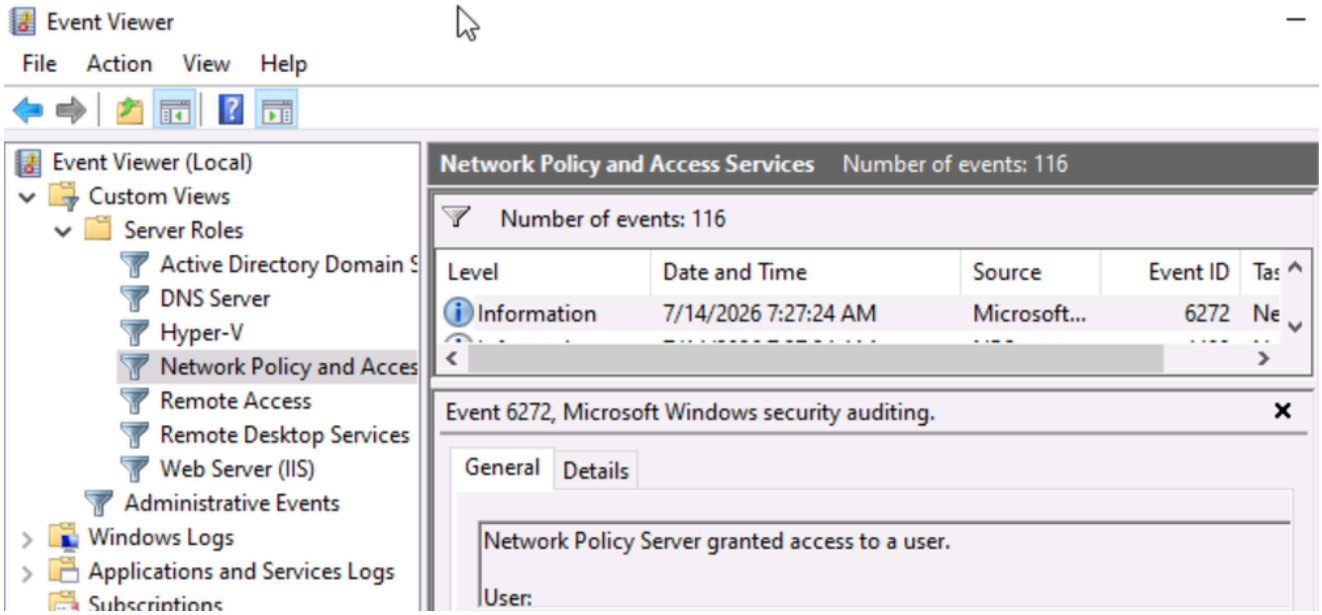
- (Sie sehen eine Leitung mit UDP und *:1812 (oder den Server IP:1812). Dadurch wird bestätigt, dass der NPS/RADIUS-Dienst aktiv auf Verbindungen wartet.
- Wenn nichts angezeigt wird, konnte der NPS nicht ausgeführt werden. Aktivieren Sie dazu Services > Network Policy Server (IAS) is Started.)



- Führen Sie in Windows PowerShell den folgenden Befehl aus:
  - Get-NetFirewallRule -DisplayGroup "Network Policy Server" | Format-Table DisplayName, Enabled, Direction, Action.



- In der Windows-Ereignisanzeige:
  - Benutzerdefinierte Ansichten > Serverrollen > Netzwerkrichtlinie und Zugriffsdienste > Pakete erreichen uns.



Testanmeldung über UCSM

1. Melden Sie sich ab, und melden Sie sich an, indem Sie das Dropdown-Menü Domain (Domäne) entsprechend der erstellten Radius-Domäne auswählen.

2. Benutzerkennwort konfigurieren. (Weitere Informationen finden Sie unter Windows-Konfiguration - Schritt 2).

- Wenn die Anmeldung funktioniert und Sie über Administratorberechtigungen verfügen, ist die Cisco AV-Pair-Zuordnung (Windows-Konfiguration, Schritt 6) richtig.

Fehlerbehebung für RADIUS-Authentifizierung

Von Windows Server

1. Führen Sie diese Befehle in Powershell zur Paketerfassung aus:

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

2. Melden Sie sich über UCSM an, und stoppen Sie die Erfassung mithilfe der folgenden Befehle:

- Pktmon-Stopp
- pktmon etl2pcap C:\radius_capture.etl -o C:\radius_capture.pcap

3. Öffnen Sie radius_capture.pcap in Wireshark: RADIUS > Attributwertpaare > bestätigen Message-Authenticator (oder Attribut 80) ist vorhanden. Dies impliziert, dass NPS die Antwort unterzeichnet.

Von UCSM CLI

Wenn pktmon unter Windows gleichzeitig über UCSM CLI ausgeführt wird,

1. ausgeführt:

- Anschließen von NX
- Terminalmonitor
- debug radius all

2. versuchen, nach dem Starten des Debuggens eine UCSM-Anmeldung durchzuführen.

Eine erfolgreiche Anmeldung sieht ähnlich aus wie 2026 Jul 3 09:54:02.917044 radius:Verified Message Authenticator in response from: 10.xxx.xx.xx

- Wenn Pakete gesendet und empfangen werden, die Anmeldung aber mit dem Nachrichtenauthentifizierer fehlschlägt, ist dies wahrscheinlich falsch. In der Debug-Ausgabe impliziert dies, dass der Port und die Erreichbarkeit in Ordnung sind.
  - Versuchen Sie, den gemeinsamen geheimen Schlüssel im Windows NPS-Server und den UCSM-Schlüssel erneut zu konfigurieren (diese müssen genau übereinstimmen).
  - Wenn das Problem weiterhin besteht, während wir uns nach der Neukonfiguration anmelden, könnte ein bekannter Cisco Bug mit der ID CSCwm80801 auftreten: Benutzer können sich mit Radius nach dem Microsoft-Patch KB5040434, der ein Upgrade auf eine erwähnte feste Version erfordert, nicht mehr bei UCSM anmelden.

Zugehörige Informationen

- Cisco UCS Manager Administration Management Guide 4.2 - Remote-Authentifizierung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.