Configurazione e risoluzione dei problemi di autenticazione Radius su UCSM

Sommario

Introduzione

In questo documento viene descritto come configurare e risolvere i problemi relativi a Radius in UCS Manager utilizzando un data center di Windows Server 2022.

Prerequisiti

- UCS Manager - 4.2(3o) o versione successiva
- Windows Server 2022 DataCenter

Configurazione su Windows Server

Installare Servizi di dominio Active Directory

Fare riferimento al documento Microsoft - Installare Servizi di dominio Active Directory utilizzando Server Manager in Windows Server 2022.

Crea utente di Active Directory (account di accesso)

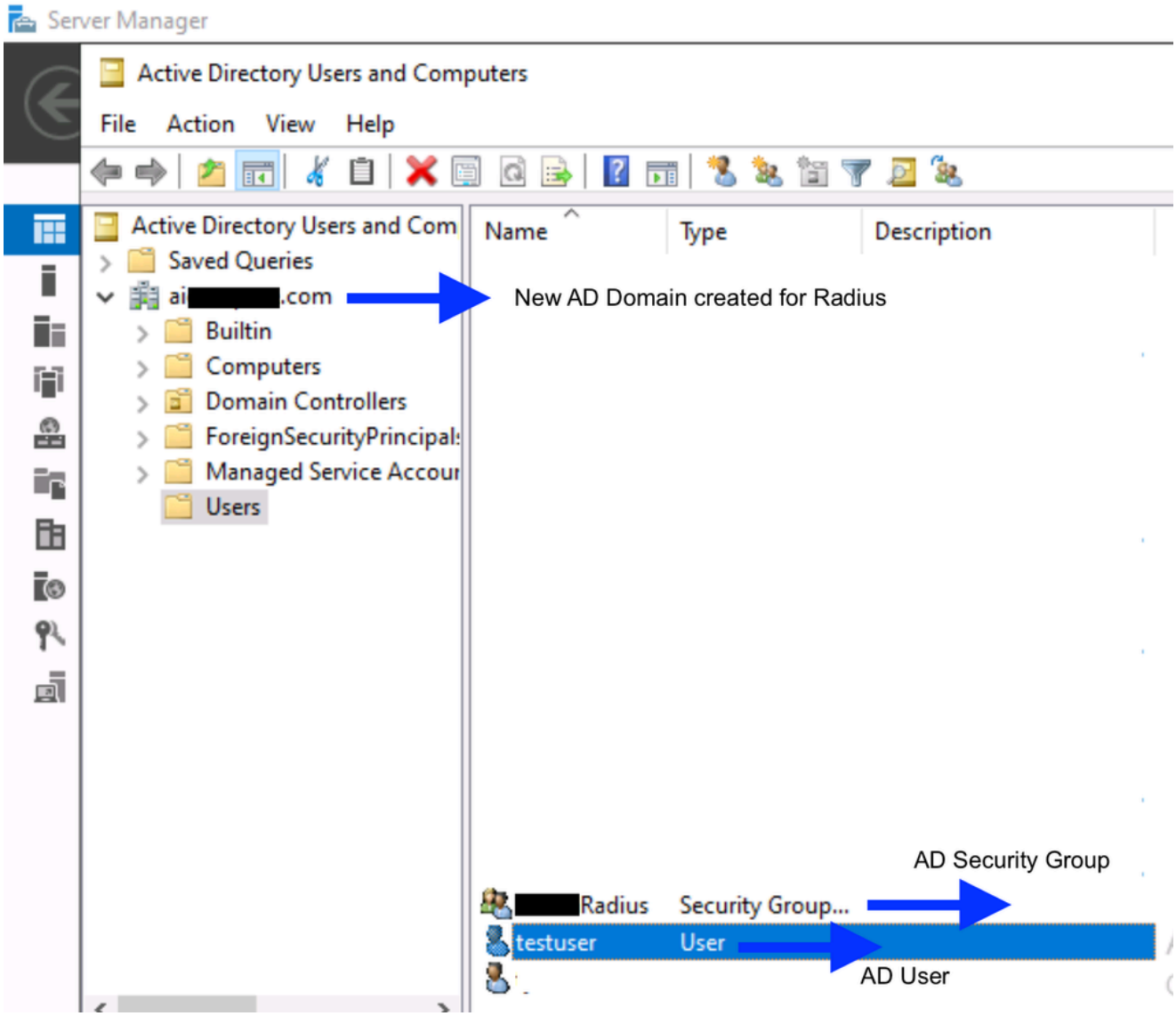
1. Aprire Server Manager > Strumenti > Utenti e computer di Active Directory.

2. Fare clic con il pulsante destro del mouse sul dominio creato Nuovo > Utente.

3. Inserire il nome di accesso (Esempio - testuser), impostare una password, deselezionare Cambiamento obbligatorio password all'accesso successivo, e selezionare Nessuna scadenza password (per un account di servizio/amministratore) > Fine (in base ai requisiti/criteri di protezione locali).

Crea un gruppo di sicurezza Active Directory per gli amministratori UCS

- Nella stessa console fare clic con il pulsante destro del mouse sul dominio Nuovo > Gruppo (Esempio - testRadius, Sicurezza). Aggiungere l'utente AD testuser) a questo gruppo.
- Questo nome di gruppo è il nome da associare in seguito a un ruolo UCS.

- 

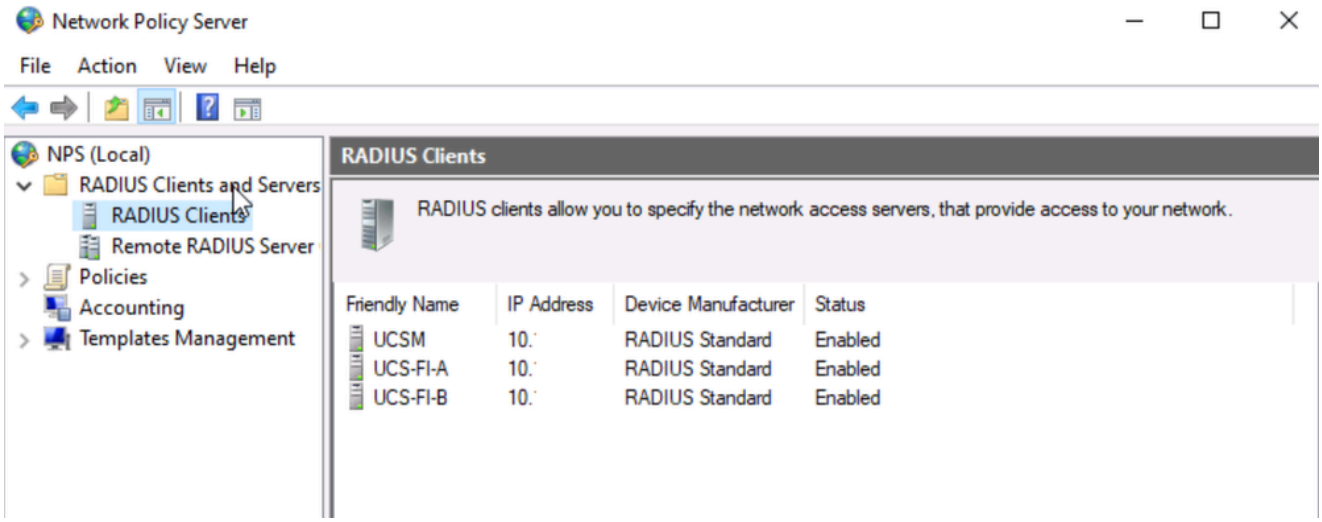
Installare Server dei criteri di rete (ruolo RADIUS) e registrare Server dei criteri di rete in Active Directory

1. Passare a Server Manager > Gestisci > Aggiungi ruoli e funzionalità.

2. Selezionare Servizi di accesso e criteri di rete > Completare la procedura guidata per installare Server dei criteri di rete.

3. Aprire Strumenti > Network Policy Server. Fare clic con il pulsante destro del mouse su Server dei criteri di rete (locale) > Registra server in Active Directory > OK. In questo modo Server dei criteri di rete è in grado di leggere l'appartenenza di utenti/gruppi AD.

Aggiungere le interconnessioni fabric UCS come client RADIUS

- In questo modo Server dei criteri di rete considera attendibili le richieste provenienti da UCSM. In Server dei criteri di rete espandere Client e server RADIUS > Client RADIUS. fare clic con il pulsante destro del mouse su Nuovo.
- Fornire:
    - Nome: Esempio - UCSM
    - Indirizzo (IP): IP di gestione di FI-A
    - Segreto condiviso: creare un segreto sicuro e annotarlo — sarà necessario immettere questa stringa segreta condivisa in UCSM in un secondo momento.
- Ripetere l'operazione per Fabric Interconnect B e, se si desidera eseguire l'autenticazione con il VIP del cluster, aggiungere anche tale IP.
- 

Client Radius

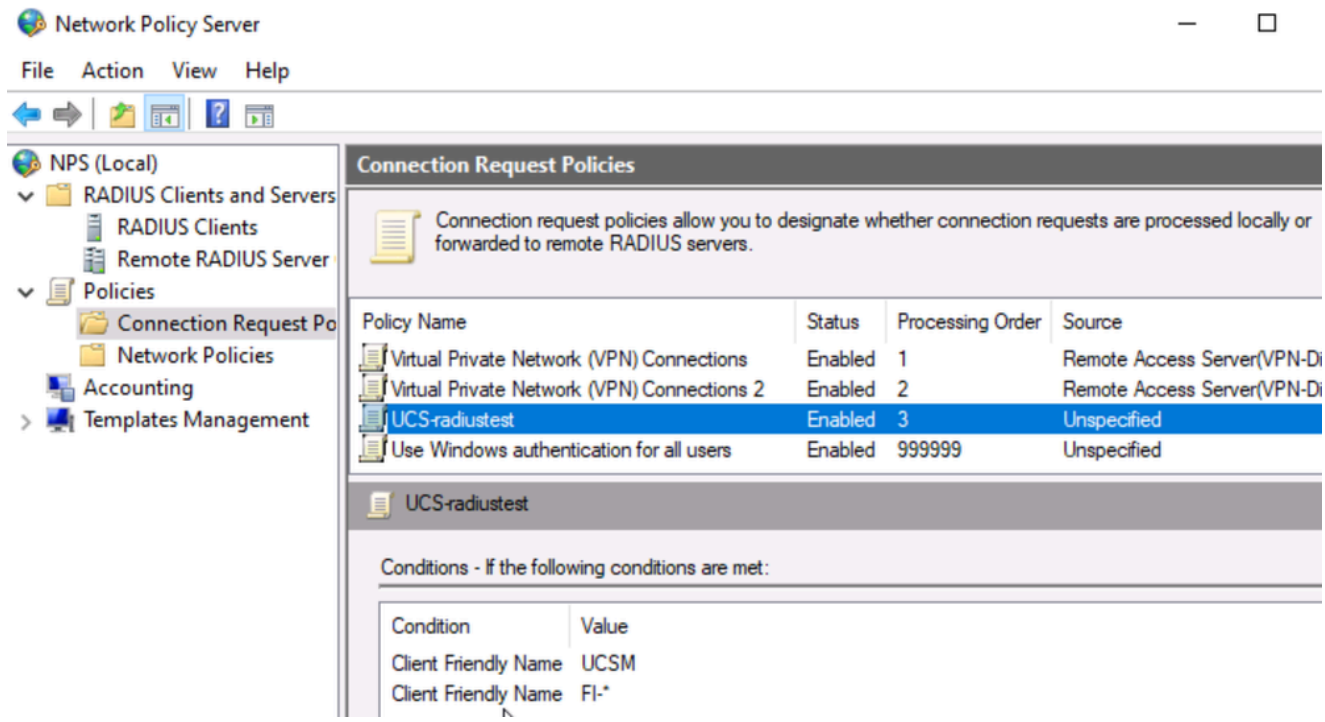
Creare un criterio di richiesta di connessione e un criterio di rete (autorizzazione e mapping dei ruoli)

- Criteri > Criteri di richiesta di connessione > Nuovo > Assegna nome (Esempio - UCS-radiustest), aggiungi la condizione per 'Nome descrittivo client' che consente l'autenticazione locale. Ad esempio: FI-* o UCSM,
- Criteri > Criteri di rete > Nuovo > Nome criterio
    - Condizioni: aggiungere gruppi di Windows. Selezionare il gruppo testRadius creato nel passaggio 3.
    - Autorizzazione di accesso: Concedi accesso
    - Metodi di autenticazione: abilitare l'autenticazione non crittografata (PAP/SPAP) e/o i metodi utilizzati da UCS. (UCS RADIUS in genere utilizza PAP.)
- Configurare Impostazioni > Attributi specifici del fornitore (questa è la parte chiave che mappa l'utente AD a un ruolo UCS): Aggiungi un attributo specifico del fornitore > Cisco AV-

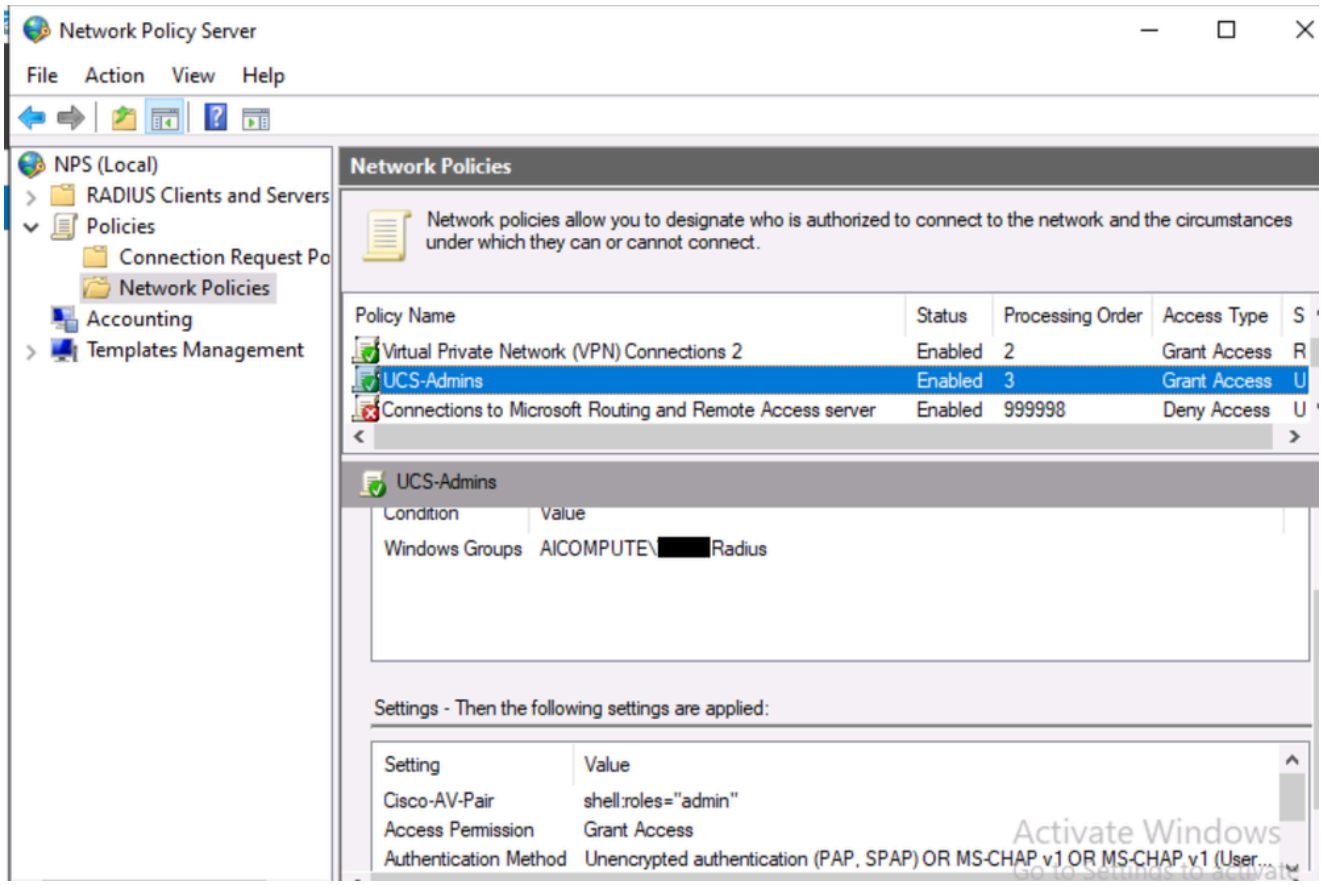
Pair

- Impostare il valore sulla stringa delle impostazioni locali/del ruolo UCS, Esempio - shell:roles="admin" (se si ignora questo attributo, l'utente accede in sola lettura).

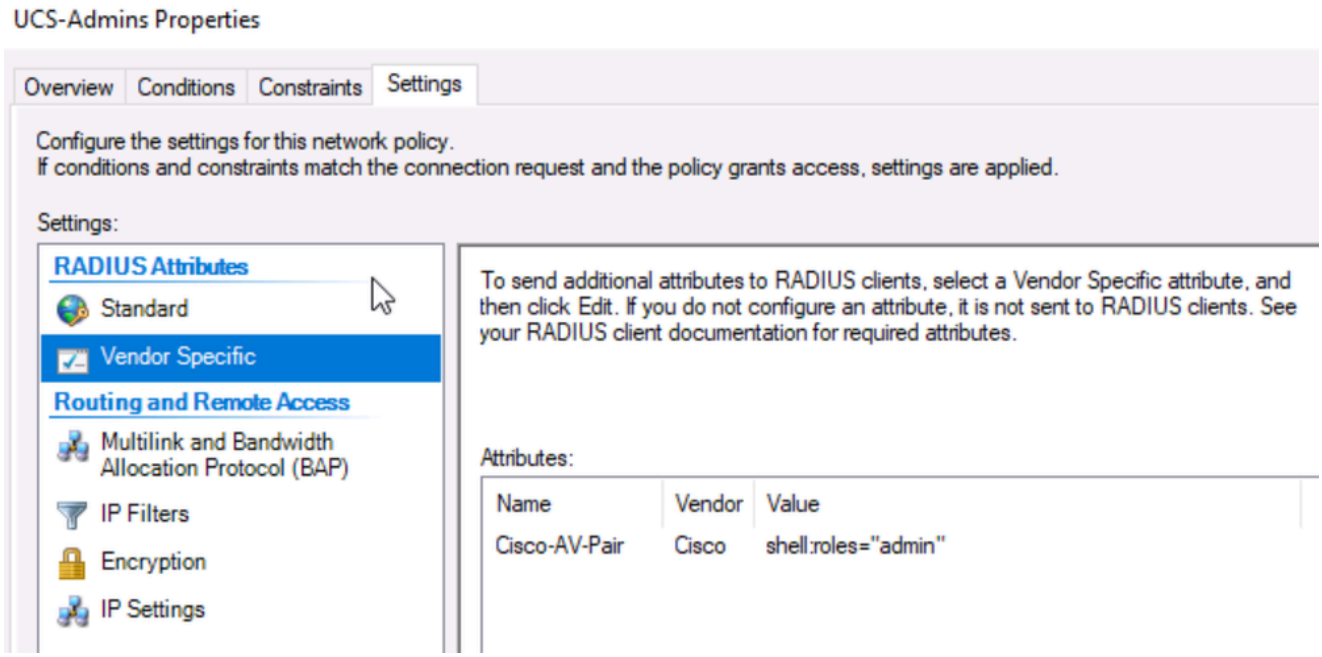
Criterio di richiesta di connessione

- 

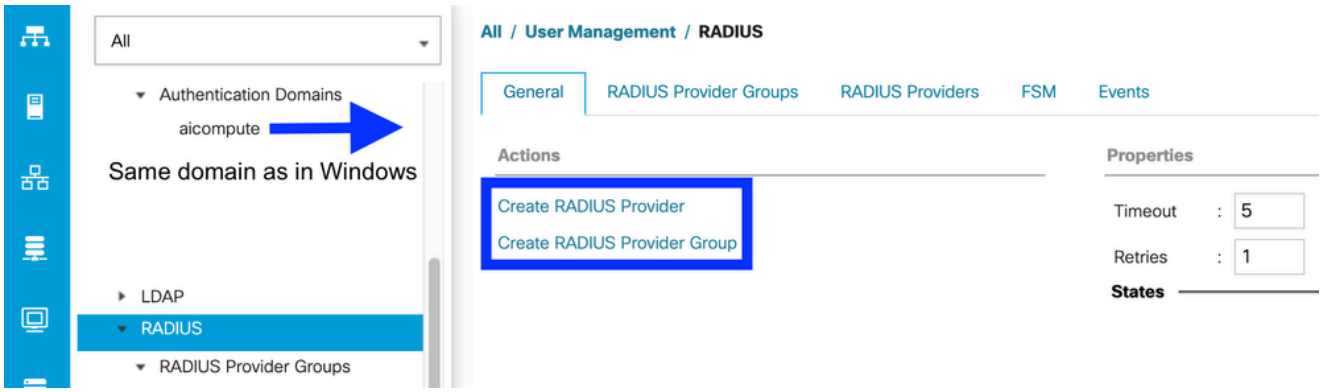
Criteri di rete

- 

Attributo specifico del fornitore

- 

Configurazione su UCSM

- 

Creare un provider Radius e aggiungerlo a un gruppo di provider

1. Accedere alla GUI di UCS Manager e selezionare Admin > User Management > RADIUS.

2. Fare clic su Create RADIUS Provider (l'opzione +/ Create) e immettere:

- Nome host/FQDN o IP: Server dei criteri di rete Windows.
- Chiave: il segreto condiviso impostato esattamente nel passaggio 5 di Server dei criteri di rete.
- Porta di autorizzazione: 1812 (deve corrispondere a Server dei criteri di rete)
- Timeout/Tentativi: lasciare avviate le impostazioni predefinite.

3. In Admin >User Management > RADIUS, creare un gruppo di provider (Esempio - RADIUS-Grp) e aggiungere il provider della versione precedente.

Crea un dominio di autenticazione

Questo è il pezzo che lega il tutto.

1. Passare a Amministrazione > Gestione utenti > Autenticazione > Domini di autenticazione.

2. Fare clic su Crea dominio (Esempio - RADIUS - il nome del dominio deve corrispondere al dominio creato in Server dei criteri di rete).

3. Impostare Realm = RADIUS.

4. Assegnare il gruppo di provider creato (RADIUS-Grp) e salvare.

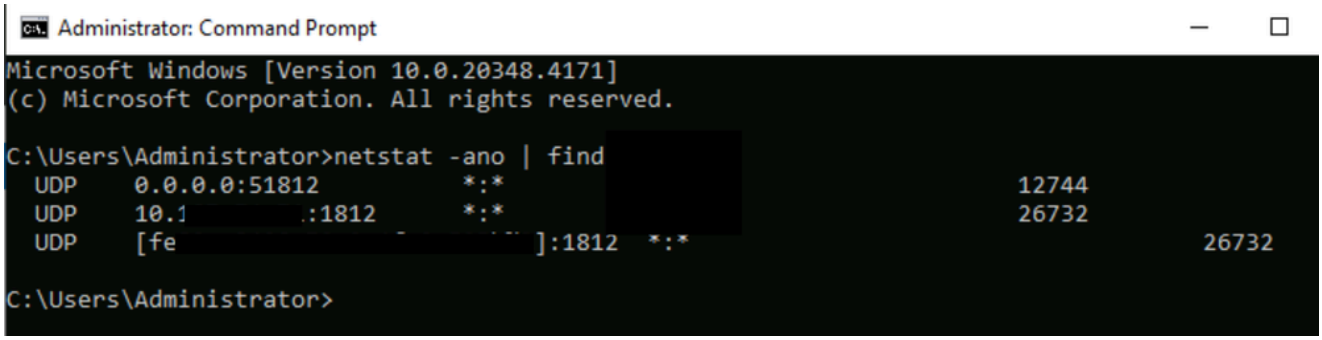
Verifica

Da Windows Server - Conferma firewall/porte

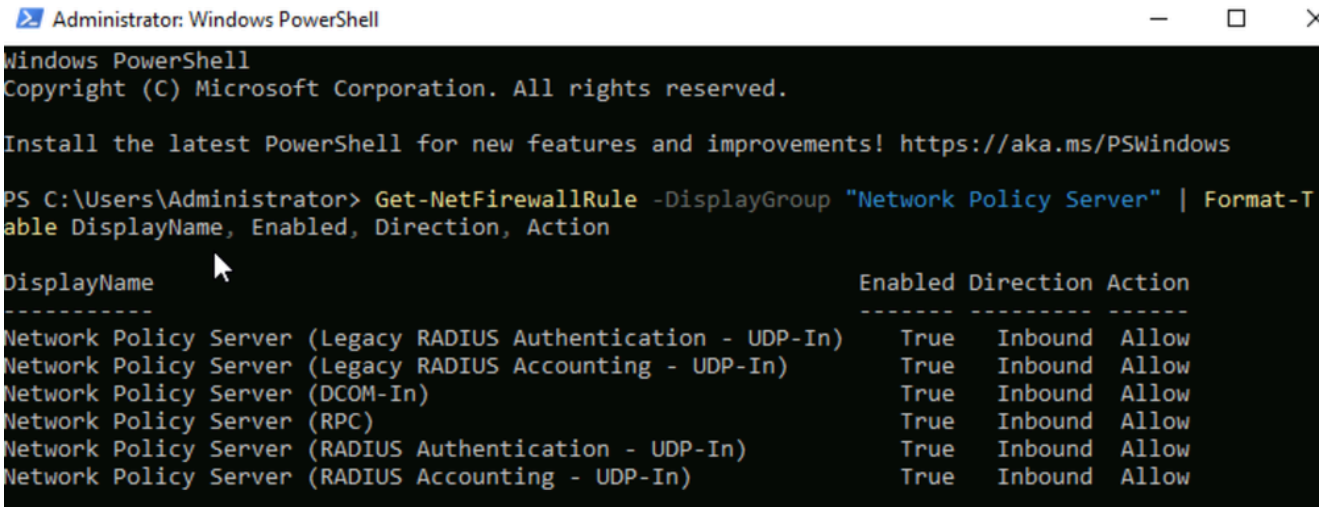
L'autenticazione RADIUS utilizza la porta UDP 1812 (e l'accounting 1813). Verificare che Windows Firewall e i firewall di rete consentano l'accesso da IP di gestione dei file system.

1. Conferma che il servizio NPS/Radius è in ascolto tramite netstat -ano | findstr 1812.

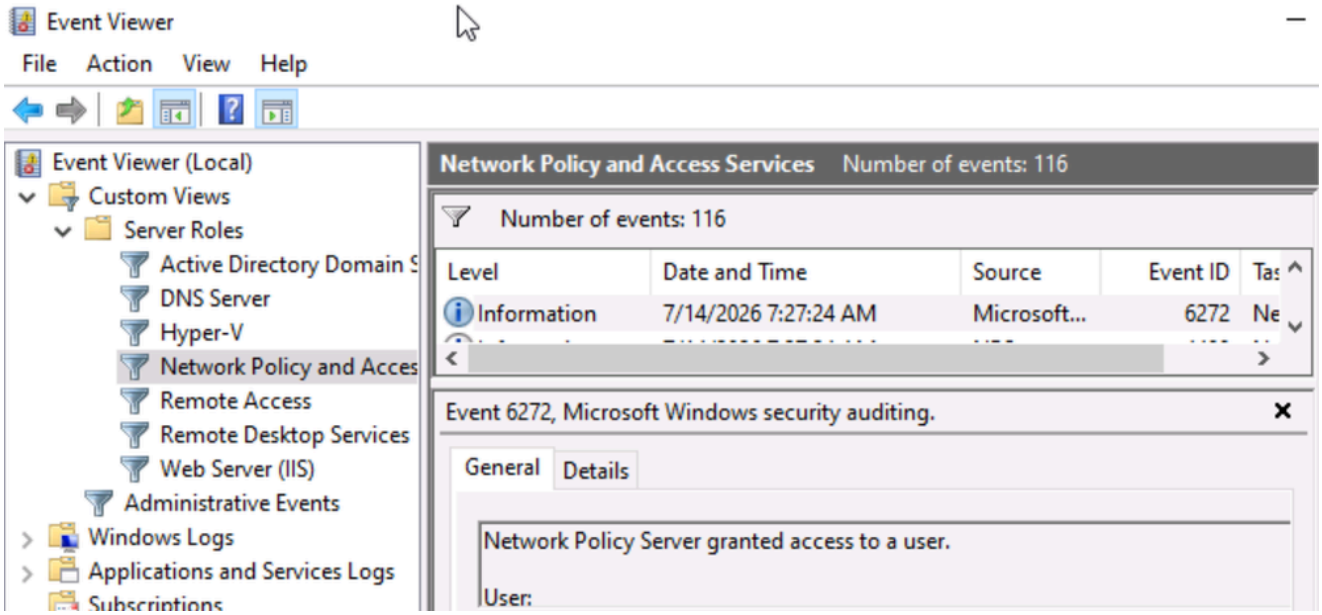
- (La linea deve essere visualizzata con UDP e *:1812 (o il server IP:1812). Ciò conferma che il servizio Server dei criteri di rete/RADIUS è in ascolto.
- Se non viene visualizzato nulla, Server dei criteri di rete non è in esecuzione. Selezionare Servizi > Server dei criteri di rete avviato.)



- In Windows Powershell eseguire il comando:
  - Get-NetFirewallRule -DisplayGroup "Server dei criteri di rete" | Format-Table DisplayName, Enabled, Direction, Action.



- Nel Visualizzatore eventi di Windows:
  - Visualizzazioni personalizzate > Ruoli server > Servizi di accesso e criteri di rete > I pacchetti stanno per raggiungere.



Test dell'accesso da UCSM

1. Disconnettersi e accedere scegliendo l'elenco a discesa Dominio in base al dominio Radius creato.

2. Configurare la password utente. (consultare il passaggio 2 della configurazione di Windows).

- Se l'accesso funziona e si ottengono i privilegi di amministratore, la mappatura della coppia AV di Cisco (passaggio 6 della configurazione di Windows) è corretta.

Risoluzione dei problemi di autenticazione Radius

Da Windows Server

1. Eseguire questi comandi in Powershell per l'acquisizione dei pacchetti:

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

2. Avviare l'accesso da UCSM e interrompere l'acquisizione utilizzando i comandi:

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

3. Aprire radius_capture.pcap in Wireshark: RADIUS > Coppie di valori attributo > conferma autenticazione messaggio (o attributo 80). Ciò implica che il Server dei criteri di rete sta firmando la risposta.

Da CLI UCSM

Quando si esegue pktmon su Windows, contemporaneamente dalla CLI di UCSM,

1. lanciare:

- connetti nxos
- monitor del terminale
- debug radius all

2. tentare un accesso UCSM dopo l'avvio del debug.

Un login riuscito sembra simile a 2026 lug 3 09:54:02.917044 radius:Verified Message Authenticator in risposta da: 10.xxx.xx.xx.

- Se i pacchetti vengono inviati e ricevuti ma l'accesso non riesce con l'autenticatore del messaggio, è probabile che non sia corretto. Nell'output del debug - ciò implica che la porta e la raggiungibilità sono corrette.
  - Provare a riconfigurare il segreto condiviso nel Server dei criteri di rete di Windows e la chiave UCSM (è necessario che corrispondano esattamente).
  - Se il problema persiste durante l'accesso dopo la riconfigurazione, è possibile che venga riscontrato un ID bug Cisco noto CSCwm80801: L'utente non può accedere a UCSM utilizzando Radius dopo che la patch KB5040434 di Microsoft ha richiesto un aggiornamento a una versione fissa menzionata.

Informazioni correlate

- Cisco UCS Manager Administration Management Guide 4.2 - Autenticazione remota

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).