

UCSMでのRADIUS認証の設定およびトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[Windows Serverでの設定](#)

[Active Directoryドメインサービスのインストール](#)

[Active Directoryユーザ（ログインアカウント）の作成](#)

[UCS管理者用のADセキュリティグループの作成](#)

[NPS（RADIUSロール）をインストールし、NPSをActive Directoryに登録する](#)

[UCSファブリックインターコネクトをRADIUSクライアントとして追加する](#)

[接続要求ポリシーとネットワークポリシーの作成（承認と役割のマッピング）](#)

[接続要求ポリシー](#)

[ネットワークポリシー](#)

[ベンダー固有の属性](#)

[UCSMでの設定](#)

[RADIUSプロバイダーの作成とプロバイダーグループへの追加](#)

[認証ドメインの作成](#)

[確認](#)

[Windows Serverから：ファイアウォール/ポートの確認](#)

[UCSMからのテストログイン](#)

[Radius認証のトラブルシューティング](#)

[Windows Serverから](#)

[UCSM CLIから](#)

[関連情報](#)

はじめに

このドキュメントでは、Windows Server 2022 DataCenterを使用してUCS ManagerでRADIUSを設定およびトラブルシューティングする手順について説明します。

前提条件

- UCS Manager - 4.2(3o)以降
- Windows Server 2022データセンター

Windows Serverでの設定

Active Directoryドメインサービスのインストール

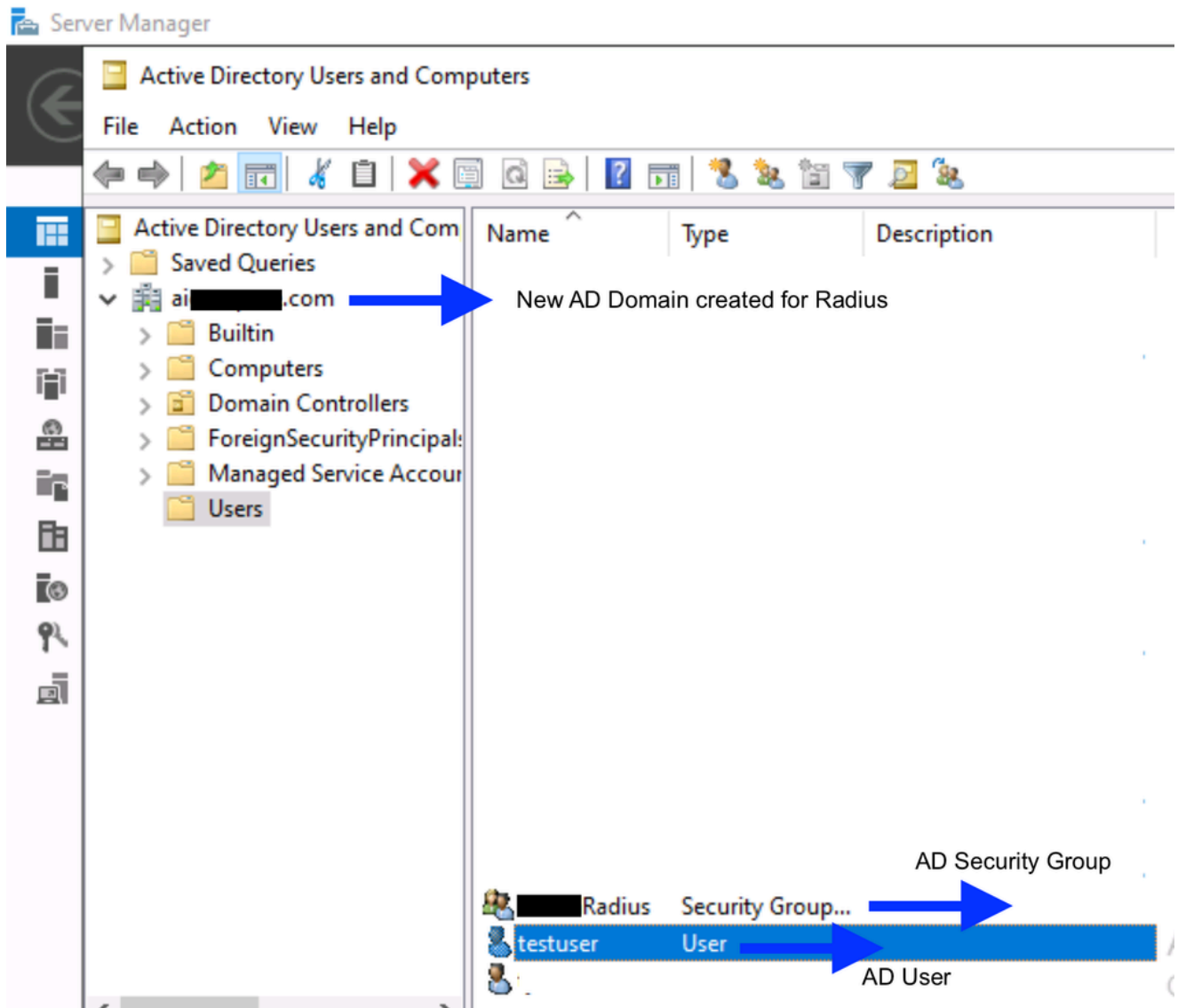
Microsoftのドキュメント「Windows Server 2022のサーバマネージャを使用したAD DSのインストール」を参照してください。

Active Directoryユーザ（ログインアカウント）の作成

1. Server Manager > Tools > Active Directory Users and Computersの順に開きます。
2. 作成したドメインを右クリック[新規] > [ユーザ]の順に選択します。
3. ログイン名（例：testuser）を入力し、パスワードを設定します。次にUser must change password at next logonをオフにし、Password never expires（サービス/管理者アカウント用）>Finish（ローカルのセキュリティ要件/ポリシーに従います）にチェックマークを入れます。

UCS管理者用のADセキュリティグループの作成

- 同じコンソールで、ドメインを右クリックし、New > Group (Example - testRadius, Security)の順に選択します。ADユーザtestuser)をこのグループに追加します。
- このグループ名は、後でUCSロールにマッピングする必要があります。



NPS（RADIUS役割）をインストールし、NPSをActive Directoryに登録する

1. [サーバーマネージャー] > [管理] > [役割と機能の追加] に移動します。
2. Network Policy and Access Services > Complete the wizard to install Network Policy Server (NPS)の順に選択します。
3. Tools > Network Policy Serverの順に開きます。NPS (Local) > Register server in Active Directory > OKの順に右クリックします。これにより、NPSはADユーザー/グループメンバーシップを読み取ることができます。

UCSファブリックインターコネクトをRADIUSクライアントとして追加する

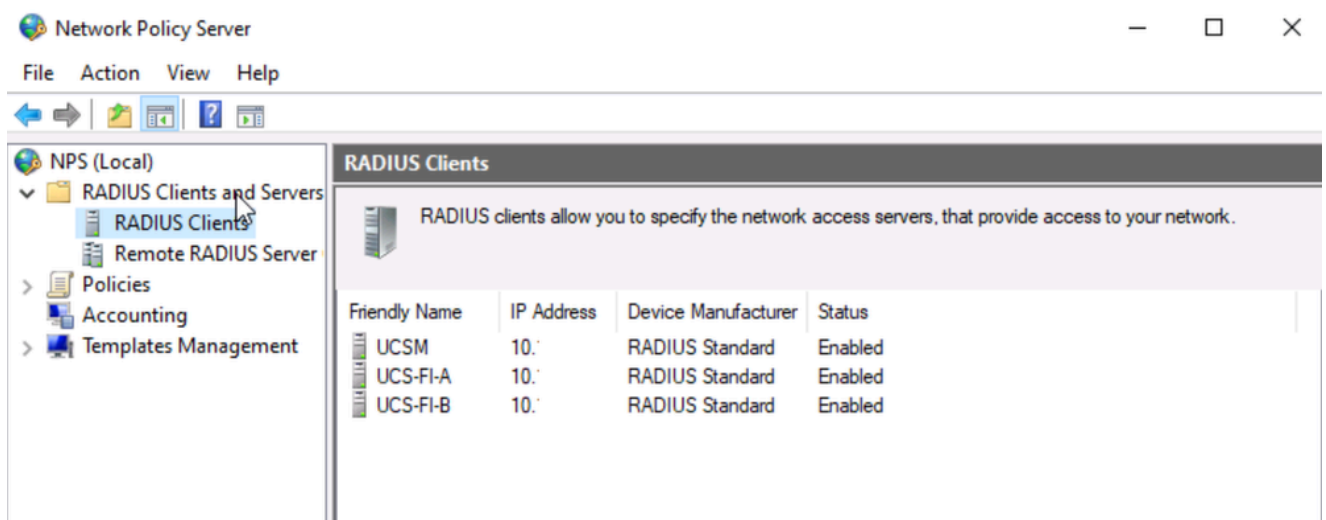
- これにより、NPSはUCSMからの要求を信頼します。NPSで、RADIUS Clients and Servers

> RADIUS Clientsの順に展開します。Newを右クリックします。

• 次を提供：

- フレンドリ名：例：UCSM
- アドレス(IP):FI-Aの管理IP
- 共有秘密：強力な秘密を作成して書き留めます。この共有秘密の文字列は、後でUCSMに正確に入力します。

• Fabric Interconnect Bについても同じ手順を繰り返し、クラスタVIPに対して認証する場合は、そのIPも追加します。

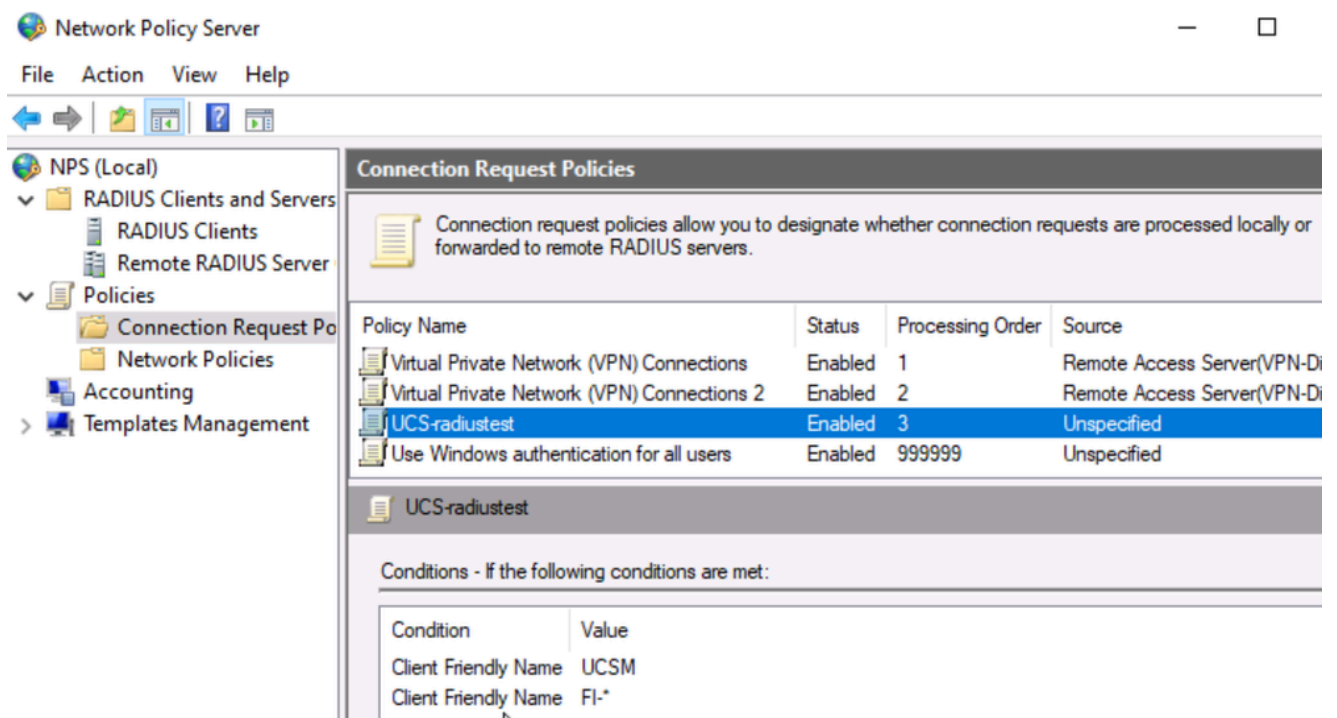


Radiusクライアント

接続要求ポリシーとネットワークポリシーの作成（許可と役割のマッピング）

- Policies > Connection Request Policies > New > Name it (Example - UCS-radiustest)の順に選択し、ローカルでの認証を可能にする「Client Friendly Name」の条件を追加します。例：FI-*またはUCSM、
- Policies > Network Policies > New > Policy name
 - 条件：Windowsグループを追加します。ステップ3で作成したtestRadiusグループを選択します。
 - アクセス権：アクセス権の付与
 - 認証方式：非暗号化認証(PAP/SPAP)を有効にするか、UCSで使用する方式を有効にします。（UCS RADIUSでは一般的にPAPが使用されます）。
- Configure Settings > Vendor Specific Attributes（これはADユーザをUCSロールにマッピングする重要な部分です）:Vendor-Specific attributeの追加> Cisco AV-Pair
 - 値をUCSロール/ロケール文字列に設定します（例：shell:roles="admin"）（この属性をスキップすると、ユーザは読み取り専用としてログインします）。

接続要求ポリシー



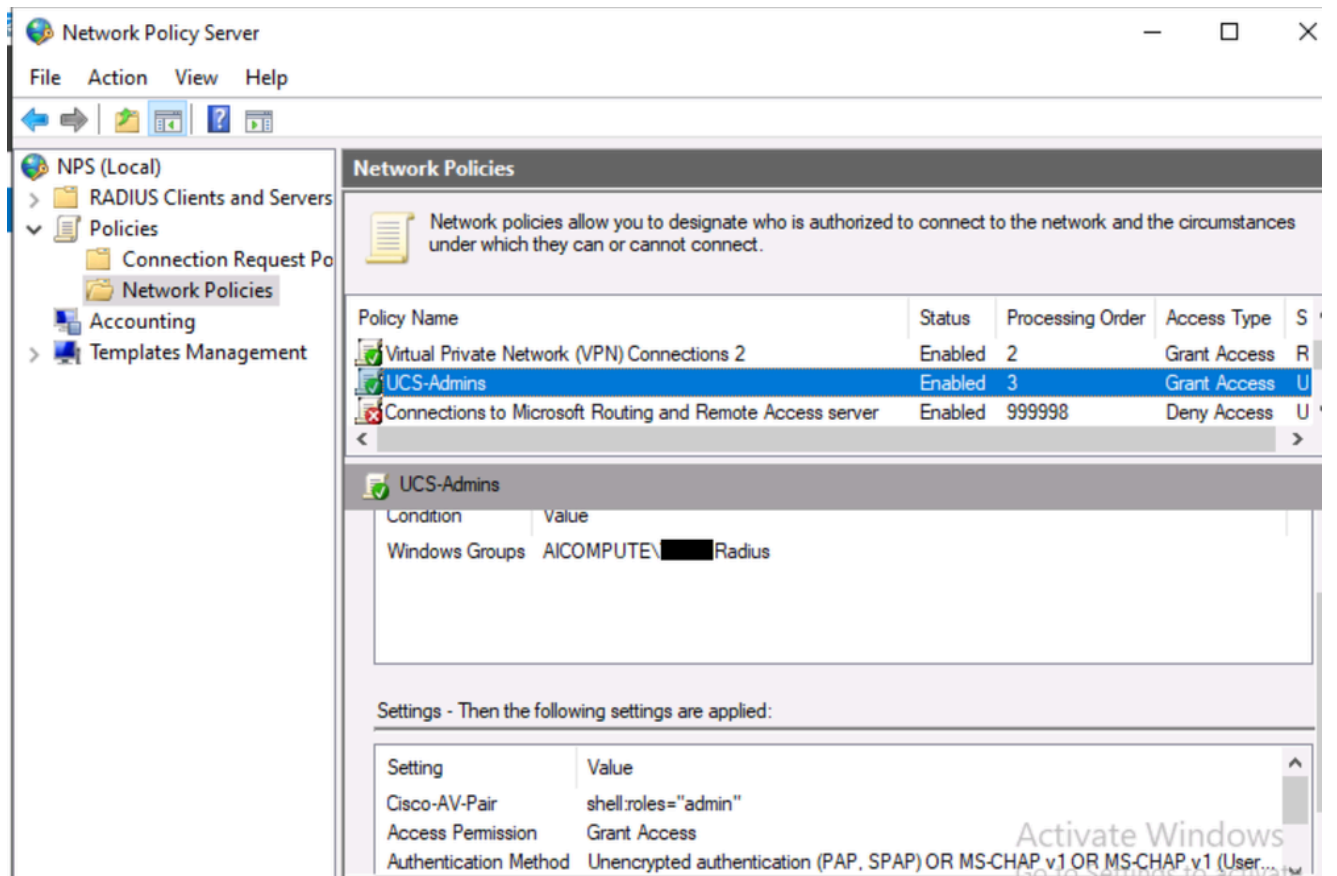
The screenshot shows the Network Policy Server (NPS) console. The left pane shows the tree structure: NPS (Local) > Policies > Connection Request Policies. The right pane displays the 'Connection Request Policies' table.

Policy Name	Status	Processing Order	Source
Virtual Private Network (VPN) Connections	Enabled	1	Remote Access Server(VPN-Di
Virtual Private Network (VPN) Connections 2	Enabled	2	Remote Access Server(VPN-Di
UCS-radiustest	Enabled	3	Unspecified
Use Windows authentication for all users	Enabled	999999	Unspecified

Below the table, the 'UCS-radiustest' policy is selected, showing its conditions:

Condition	Value
Client Friendly Name	UCSM
Client Friendly Name	FI*

ネットワークポリシー



The screenshot shows the Network Policy Server (NPS) console. The left pane shows the tree structure: NPS (Local) > Policies > Network Policies. The right pane displays the 'Network Policies' table.

Policy Name	Status	Processing Order	Access Type	S
Virtual Private Network (VPN) Connections 2	Enabled	2	Grant Access	R
UCS-Admins	Enabled	3	Grant Access	U
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	U

Below the table, the 'UCS-Admins' policy is selected, showing its settings:

Setting	Value
Cisco-AV-Pair	shell:roles="admin"
Access Permission	Grant Access
Authentication Method	Unencrypted authentication (PAP, SPAP) OR MS-CHAP v1 OR MS-CHAP v1 (User...

ベンダー固有の属性

UCS-Admins Properties

Overview Conditions Constraints **Settings**

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	shell:roles="admin"

UCSMでの設定

All

Authentication Domains

aicompute →

Same domain as in Windows

LDAP

RADIUS

RADIUS Provider Groups

All / User Management / RADIUS

General RADIUS Provider Groups RADIUS Providers FSM Events

Actions

Create RADIUS Provider

Create RADIUS Provider Group

Properties

Timeout : 5

Retries : 1

States

RADIUSプロバイダーの作成とプロバイダーグループへの追加

1. UCS ManagerのGUIにログインし、Admin > User Management > RADIUSの順に選択します。
2. Create RADIUS Provider (+/ Create オプション) をクリックし、次のように入力します。
 - ホスト名/FQDNまたはIP: Windows NPSサーバー。
 - Key:NPSステップ5で設定した共有秘密と完全に一致する共有秘密。
 - 認証ポート:1812 (NPSと一致する必要あり)

- Timeout / Retries : デフォルトをstartのままにします。

3. Admin > User Management > RADIUSで、プロバイダーグループ (例 : RADIUS-Grp) を作成し、以前の手順で作成したプロバイダーを追加します。

認証ドメインの作成

これはそれらすべてを結び付ける部分です。

1.Admin > User Management > Authentication > Authentication Domainsの順に移動します。

2. Create a Domainをクリックします (例 : RADIUS – ドメイン名はNPSで作成されたドメインと同じにすることを推奨) 。

3. Realm = RADIUSを設定します。

4. 作成したプロバイダーグループ(RADIUS-Grp)を割り当てて保存します。

確認

Windows Serverから : ファイアウォール/ポートの確認

RADIUS認証はUDPポート1812 (およびアカウンティング1813) を使用します。 Windowsファイアウォールとすべてのネットワークファイアウォールで、Firewall IPからこれらが許可されていることを確認します。

1. netstat -ano | findstr 1812 コマンドを使用して、NPS / Radiusサービスがリッスンしていることを確認します。

- (UDPと*:1812 (またはサーバIP:1812) の行が表示されます。 これにより、NPS/RADIUSサービスがアクティブにリッスンしていることが確認されます。
- 何も表示されない場合は、NPS could not be running — Services > Network Policy Server (IAS) is Startedにチェックマークを入れます)。

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.4171]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat -ano | find
UDP    0.0.0.0:51812      *:*                12744
UDP    10.1.1.1:1812     *:*                26732
UDP    [fe80::...]:1812  *:*                26732

C:\Users\Administrator>
```

- Windows Powershellで、次のコマンドを実行します。
 - Get-NetFirewallRule -DisplayGroup "Network Policy Server" | Format-Table DisplayName, Enabled, Direction, Actionです。

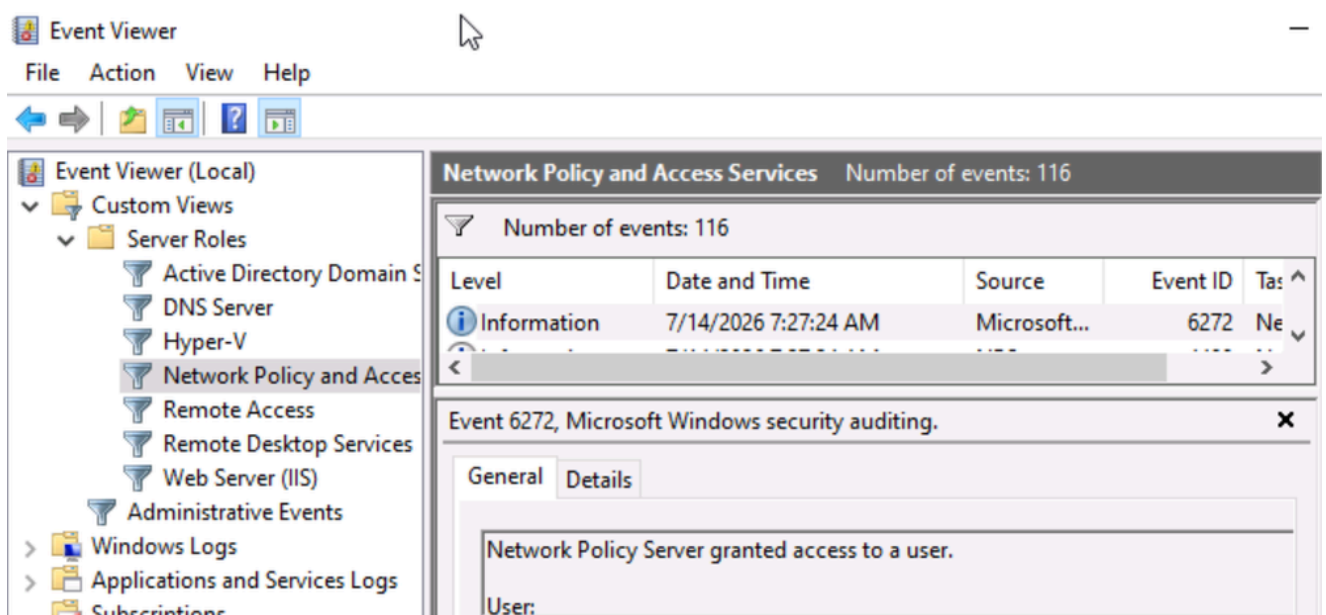
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Get-NetFirewallRule -DisplayGroup "Network Policy Server" | Format-Table DisplayName, Enabled, Direction, Action

DisplayName                                     Enabled Direction Action
-----
Network Policy Server (Legacy RADIUS Authentication - UDP-In) True      Inbound Allow
Network Policy Server (Legacy RADIUS Accounting - UDP-In) True      Inbound Allow
Network Policy Server (DCOM-In) True      Inbound Allow
Network Policy Server (RPC) True      Inbound Allow
Network Policy Server (RADIUS Authentication - UDP-In) True      Inbound Allow
Network Policy Server (RADIUS Accounting - UDP-In) True      Inbound Allow
```

- Windows Event Viewer(IEV)で、
 - カスタムビュー>サーバの役割>ネットワークポリシーとアクセスサービス>パケットが到達しています。



UCSMからのテストログイン

1. ログアウトし、作成したRADIUSドメインに従ってDomainドロップダウンを選択してログインします。
 2. ユーザパスワードを設定します。（「Windows設定ステップ2」を参照）。
- ログインが成功し、admin権限が付与された場合は、Cisco AV-Pairマッピング（Windows設定ステップ6）が正しく行われます。

Radius認証のトラブルシューティング

Windows Serverから

1. Powershellでパケットキャプチャ用に次のコマンドを実行します。
- `pktmonフィルタadd -p 1812`
 - `pktmon start —capture —pkt-size 0 -f C:\radius_capture.etl`
2. UCSMからログインを開始し、次のコマンドを使用してキャプチャを停止します。
- `pktmon停止`
 - `pktmon etl2pcap C:\radius_capture.etl -o C:\radius_capture.pcap`
3. Wiresharkでradius_capture.pcapを開きます。RADIUS > Attribute Value Pairs（属性80）が存在することを確認します（または属性80）。これは、NPSが応答に署名していることを意味します。

UCSM CLIから

Windowsでpktmonを実行すると同時に、UCSM CLIから

1. 次を実行します。
- NXOSの接続
 - 端末モニタ
 - `debug radius all`

2. デバッグを開始した後、UCSMログインを試行します。

ログインに成功すると、「2026 Jul 3 09:54:02.917044 radius:Verified Message Authenticator in response from: 10.xxx.xx.xx」のようなメッセージが表示されます。

- パケットが送受信されても、ログインが失敗し、「message authenticator is probably incorrect.」というメッセージが表示される場合、デバッグ出力では、ポートと到達可能性に問題がないことを意味しています。
 - Windows NPSサーバとUCSMキーの共有秘密を再度設定します（完全に一致させる必要があります）。
 - 再設定後にログインしても問題が解決しない場合、既知のCisco Bug ID CSCwm80801（登録ユーザ専用）「Microsoft/パッチKB5040434で前述の修正済みリリースへのアップグレードが必要になった後で、Radiusを使用してUCSMにログインできない」に該当する可能性があります。

関連情報

- [Cisco UCS Manager Administration Managementガイド4.2 – リモート認証](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。