Windows 2008 NPSサーバ用RADIUSの設定 – WAAS AAA

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定手順](#)
[1. WAAS Central Manager](#)
[2. Windows 2008 R2 - NPSサーバーの構成](#)
[3. RADIUSユーザアカウントのWAAS CM設定](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Wide Area Application Services(WAAS)およびWindows 2008 R2 Network Policy Server(NPS)でのリモート認証ダイヤルインユーザサービス(RADIUS)の設定手順について説明します。

デフォルトのWAAS設定では、ローカル認証が使用されます。Cisco WAASは、RADIUSおよびTerminal Access Controller Access-Control System(TACACS+)をAuthentication, Authorization, and Accounting（AAA；認証、認可、アカウンティング）にもサポートしています。 このドキュメントでは、1つのデバイスのみの設定について説明します。ただし、これはデバイスグループでも実行できます。すべての設定は、WAAS CM GUIを介して適用する必要があります。

一般的なWAAS AAA設定については、『Cisco Wide Area Application Services設定ガイド』の「管理ログイン認証、許可、アカウンティングの設定」の章を参照してください。

著者：Cisco TACエンジニア、Hamilan Gnanabaskaran

編集：Sanaz Tayyar、Cisco TACエンジニア

前提条件

要件

次の項目に関する知識があることが推奨されます。

- WAAS 5.xまたは6.x
- Windows NPSサーバー
- AAA:RADIUS

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco WAAS - Virtual Central Manager(vCM)
- WAAS 6.2.3.b
- Windows 2008 NPS

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のハードウェアおよびソフトウェアのバージョンにも適用できます。

- vWAAS、ISR-WAAS、およびすべてのWAASアプライアンス
- WAAS 5.xまたはWAAS 6.x
- WAAS as Central Manager、アプリケーションアクセラレータ

注：APPNAV-XEはこの設定をサポートしていません。ルータAAAは設定をAPPNAV-XEにプッシュします。

設定手順

次の設定を適用する必要があります。

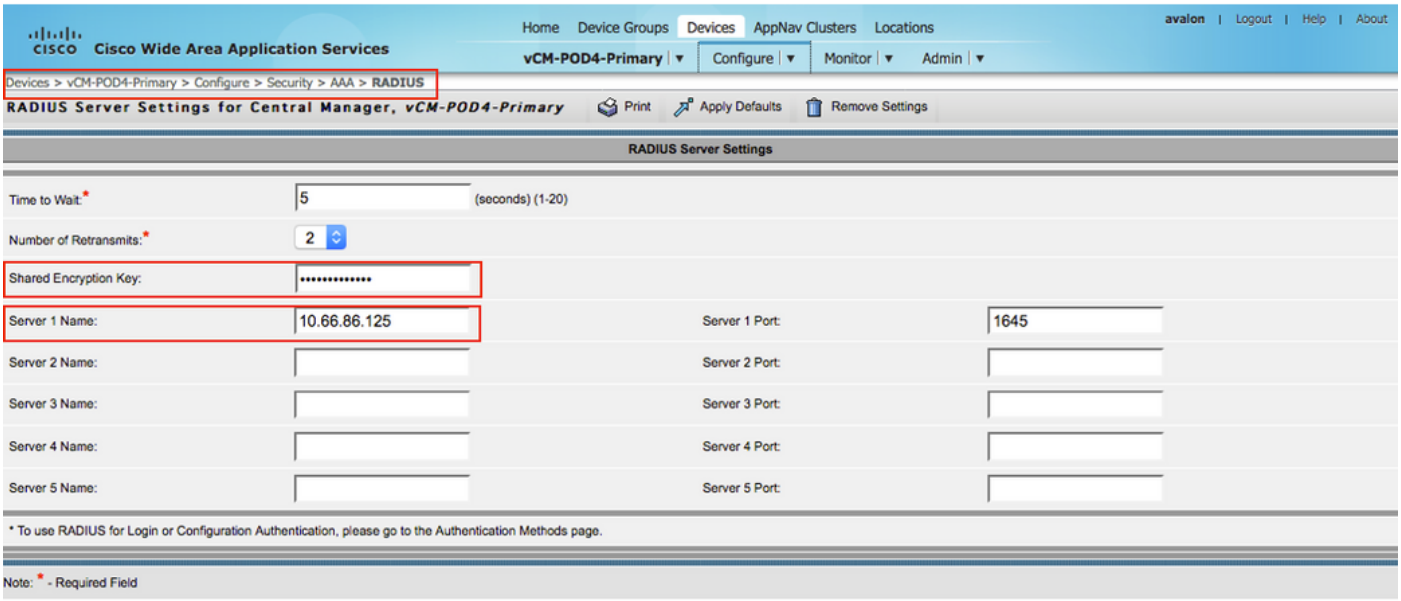
1. WAAS Central Manager
  1.1 AAA RADIUSの設定
  1.2 AAA認証の設定

2. Windows 2008 R2 - NPSサーバー構成
  2.1 RADIUSクライアントの設定
  2.2ネットワークポリシーの設定

3. RADIUSユーザアカウントのWAAS CM設定

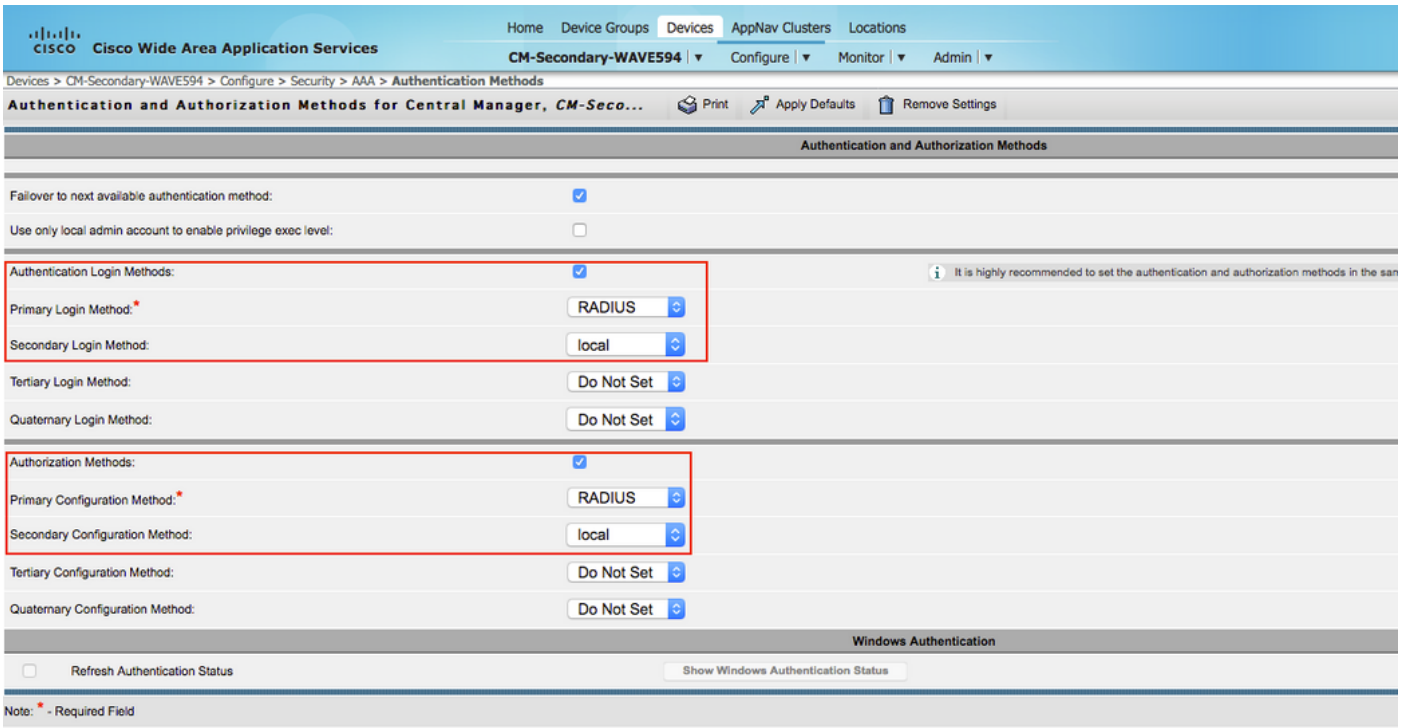
1. WAAS Central Manager

1.1 WAAS Central Managerで、**[Configure] > [Security] > [AAA] > [RADIUS]**の下にRADIUSサーバを作成します。



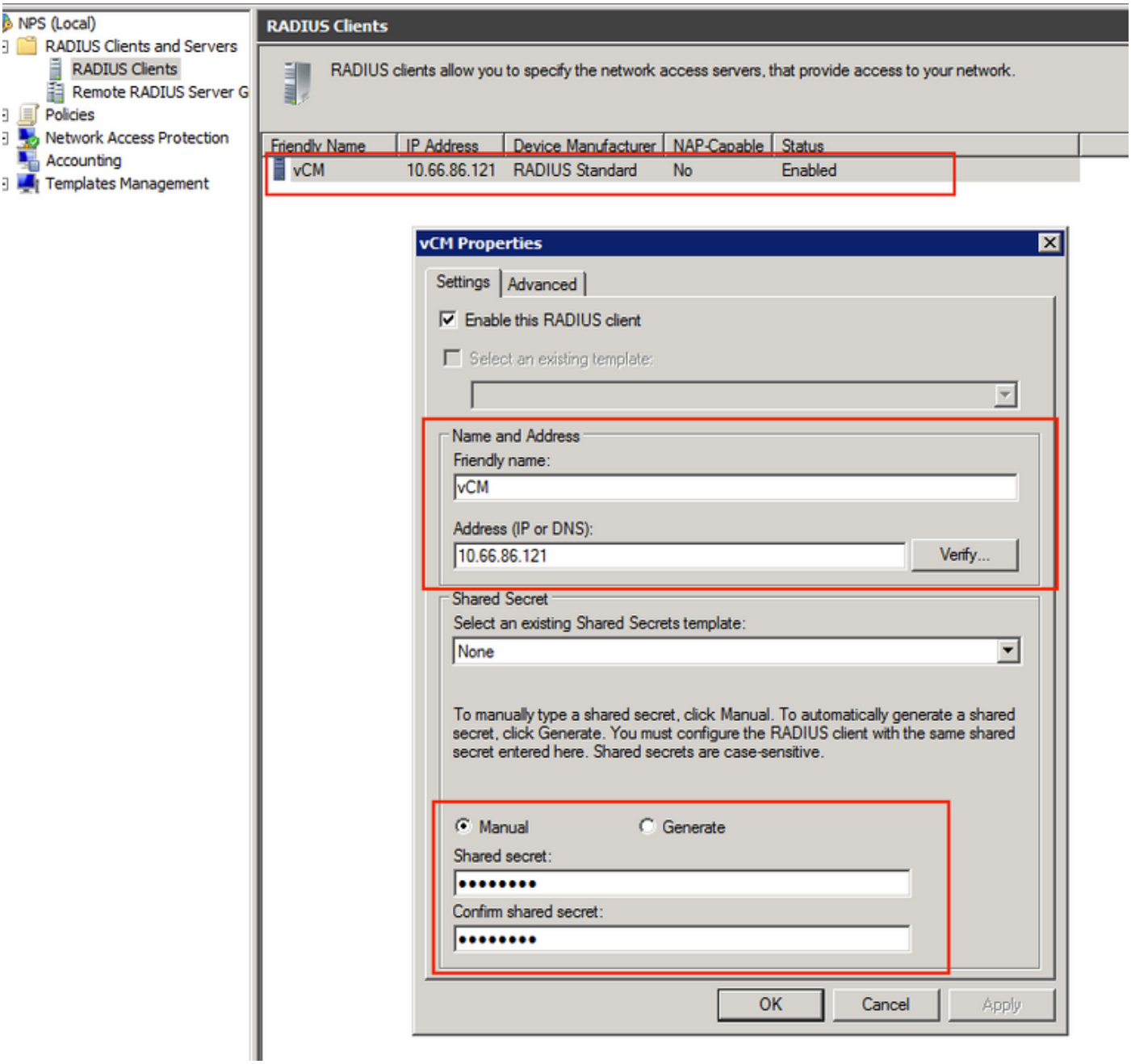
1.2 [Configure] > [Security] > [AAA] > [Authentication Methods]で、RADIUSを反映するように認証方式を設定します。

プライマリ認証方式はRADIUSとして選択され、セカンダリ認証方式はローカルとして選択されます。したがって、RADIUS障害が発生した場合は、顧客はローカルアカウントを使用してログインできます。

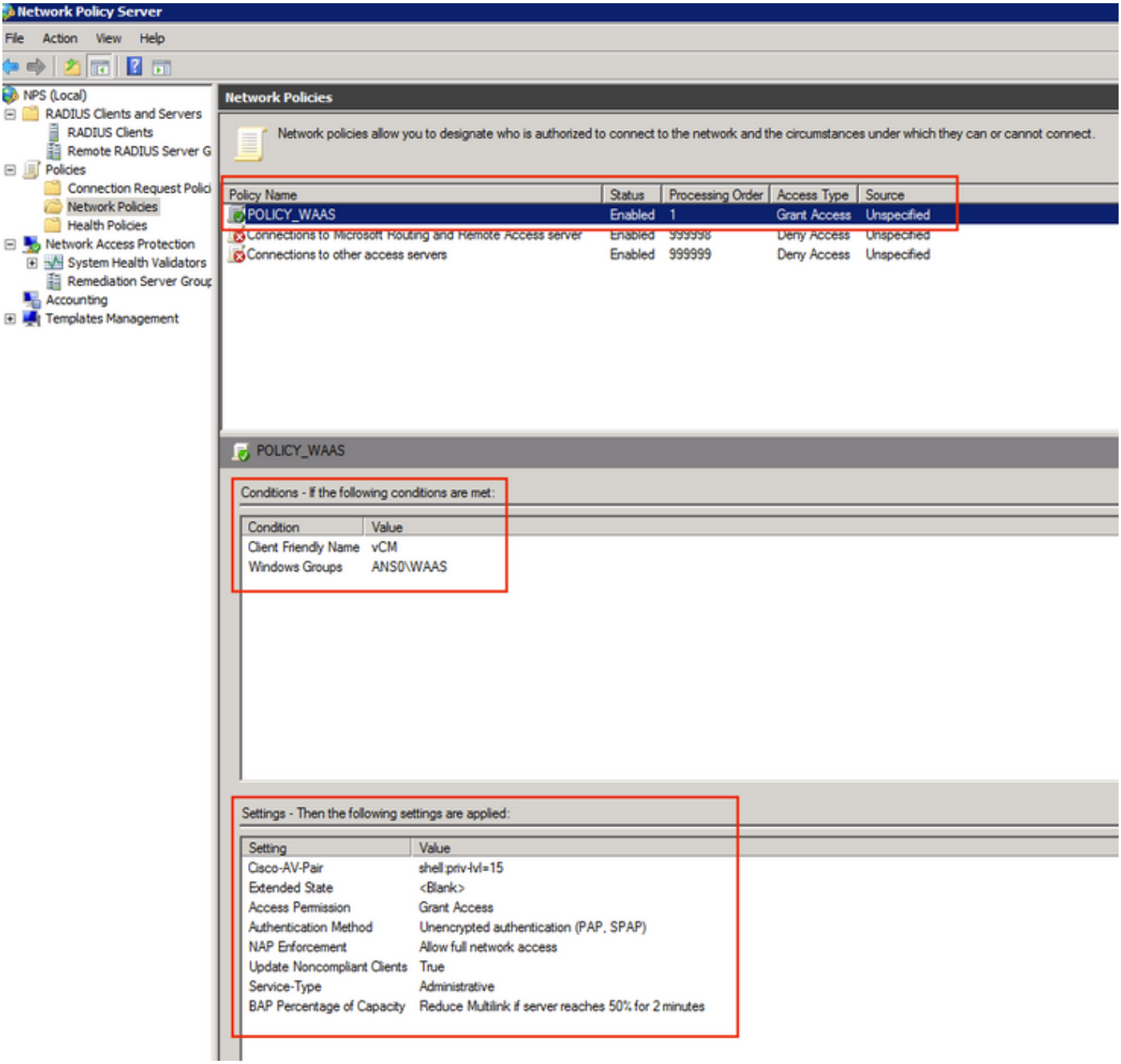


2. Windows 2008 R2 - NPSサーバーの構成

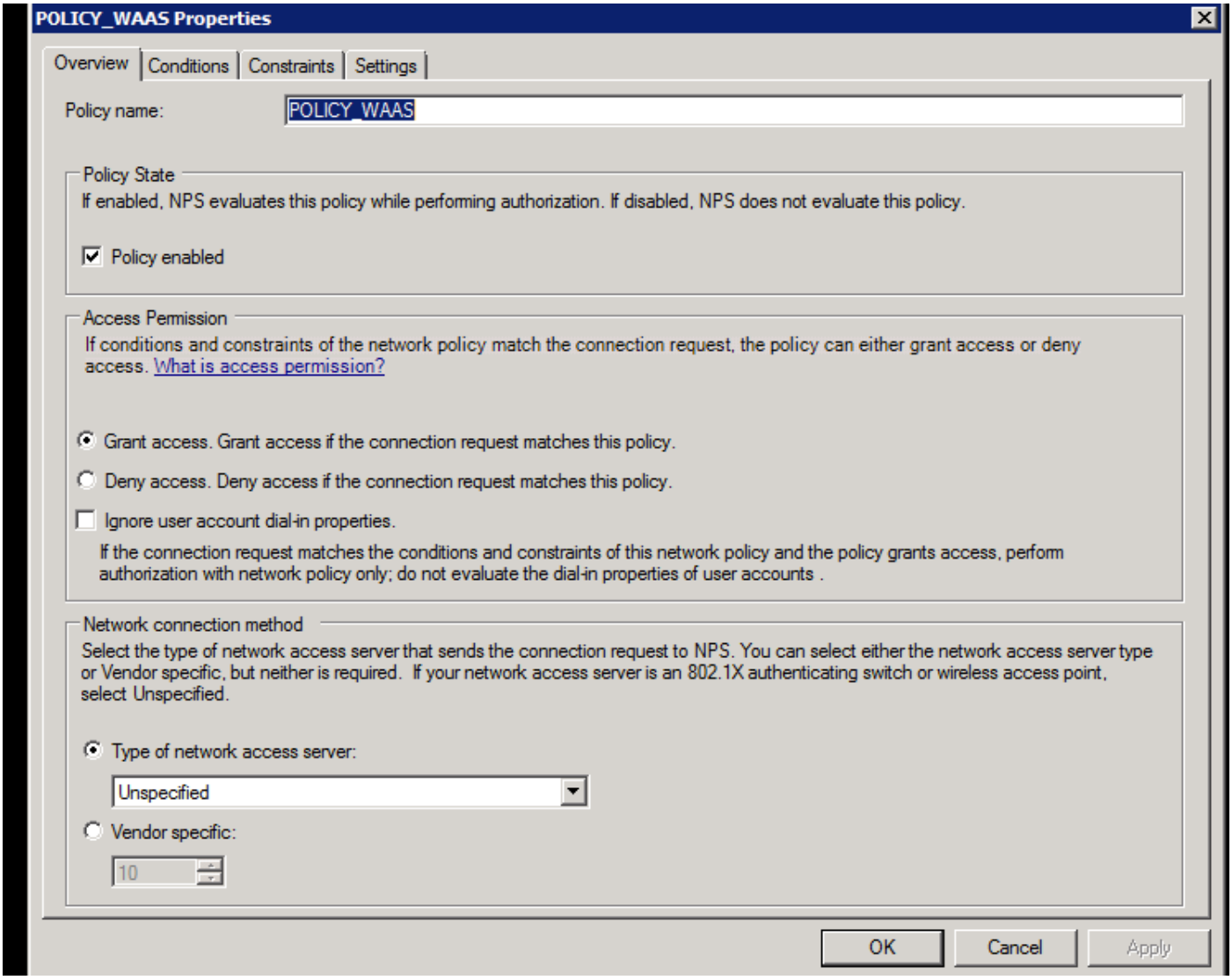
2.1 Windows 2008 R2 - NPSサーバで、RADIUSクライアントとしてWAASデバイスIPを作成します。



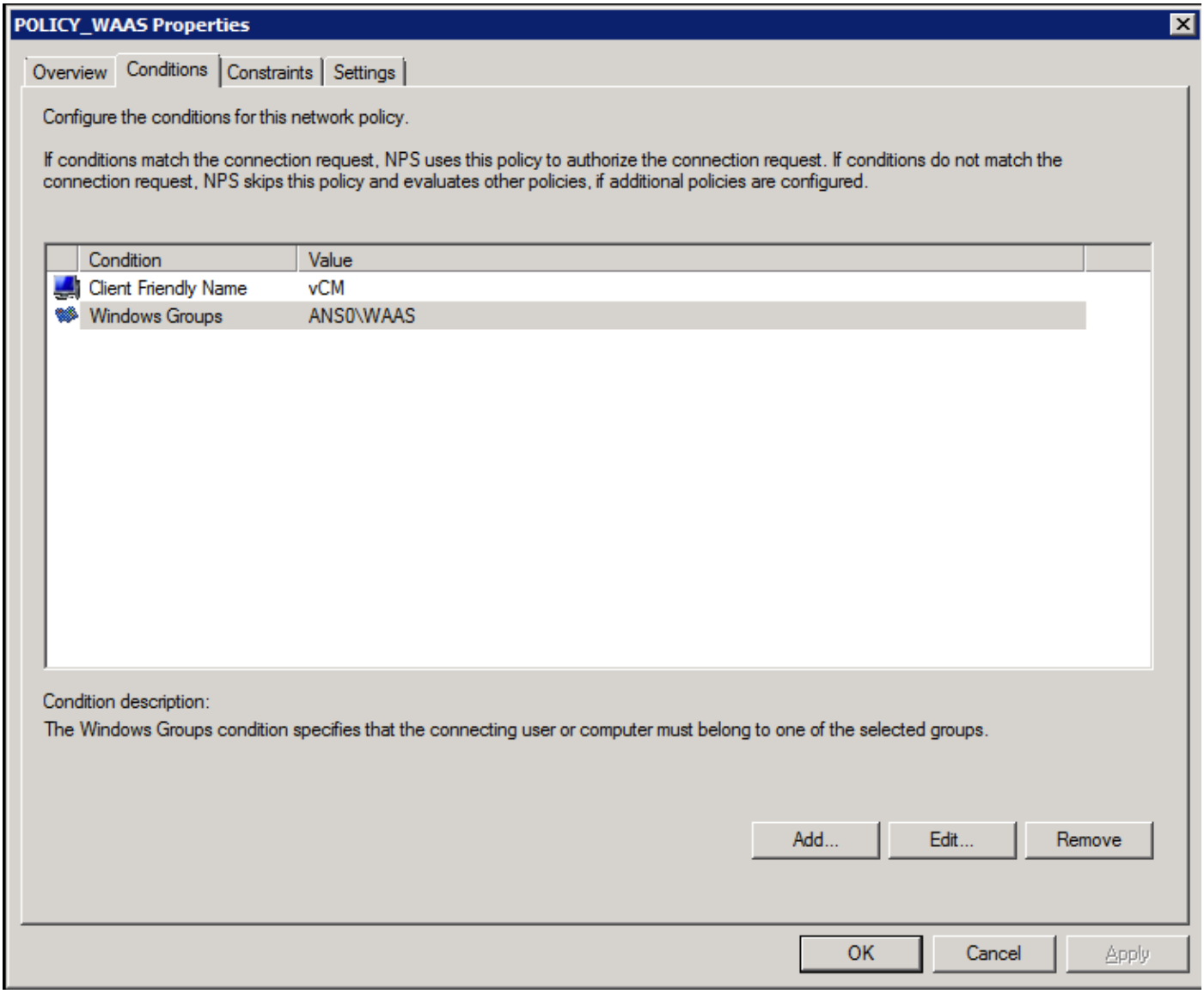
2.2 Windows 2008 R2 - NPSサーバで、WAASデバイスと一致し、認証を許可するネットワークポリシーを作成します。



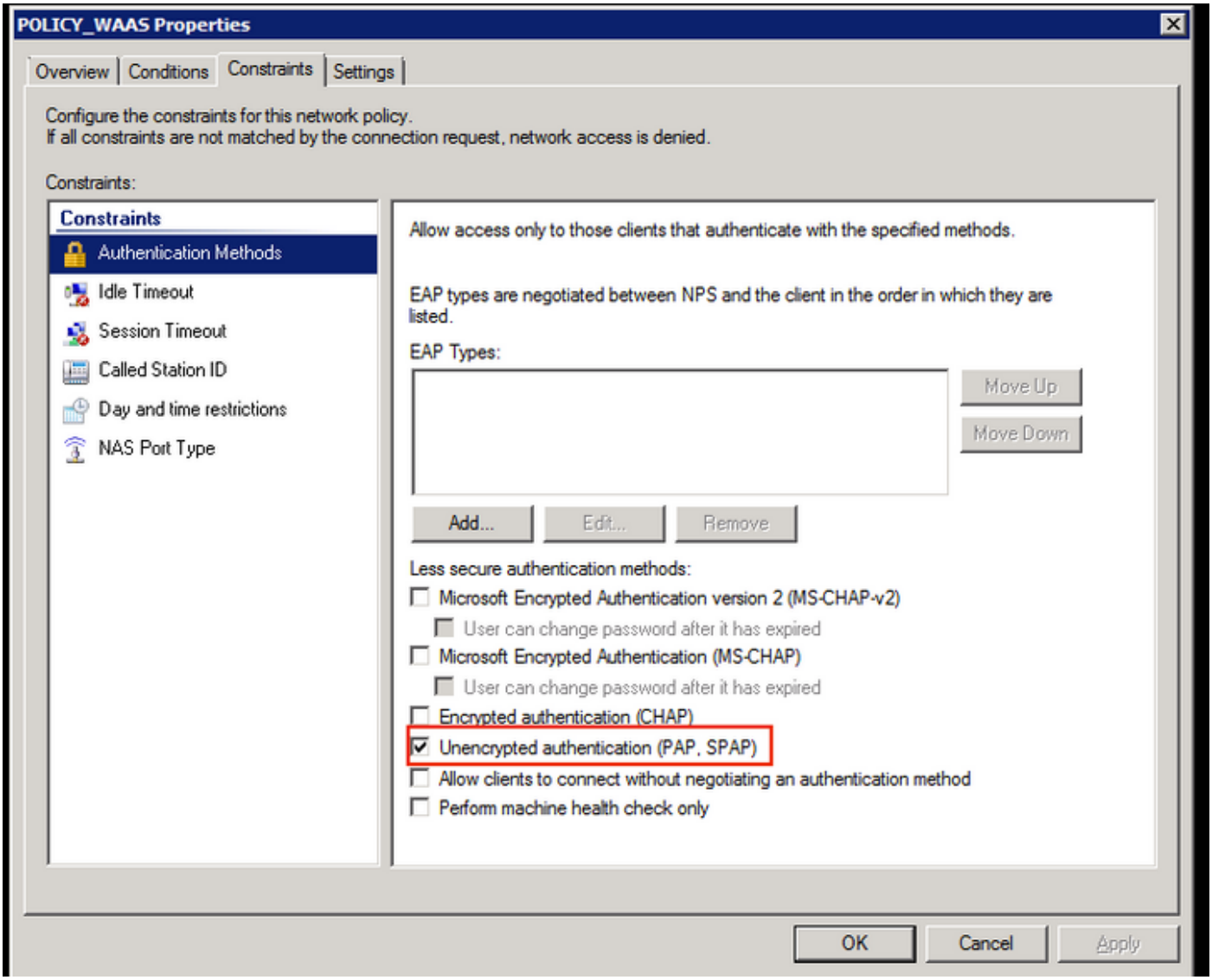
ラボでは、[NPS] > [ポリシー] > [ネットワークポリシー]で**これらのパラメータを選択する必要があります。**



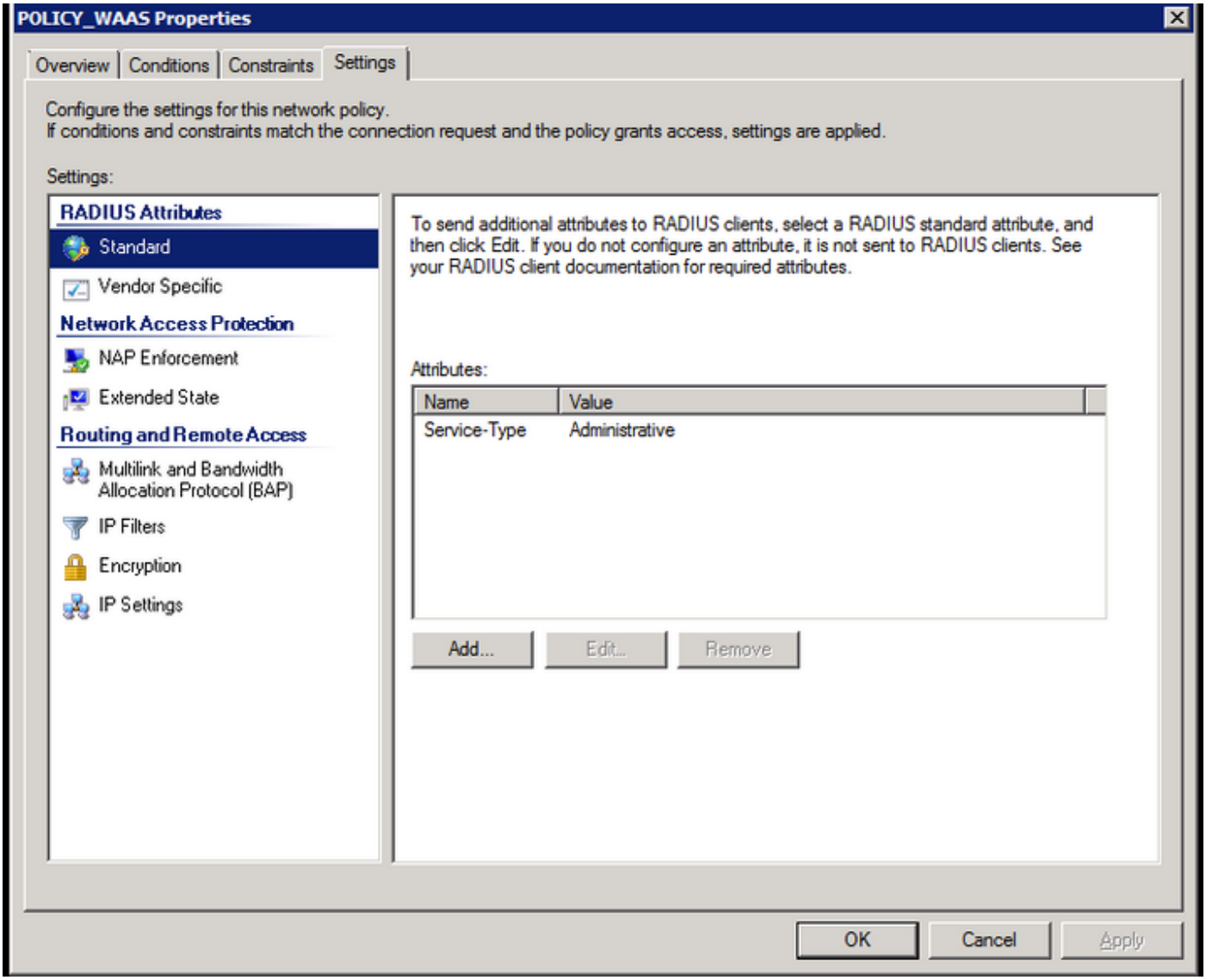
条件はRADIUSクライアントフレンドリ名と一致します。IPアドレスなどの他の方法も使用できます。



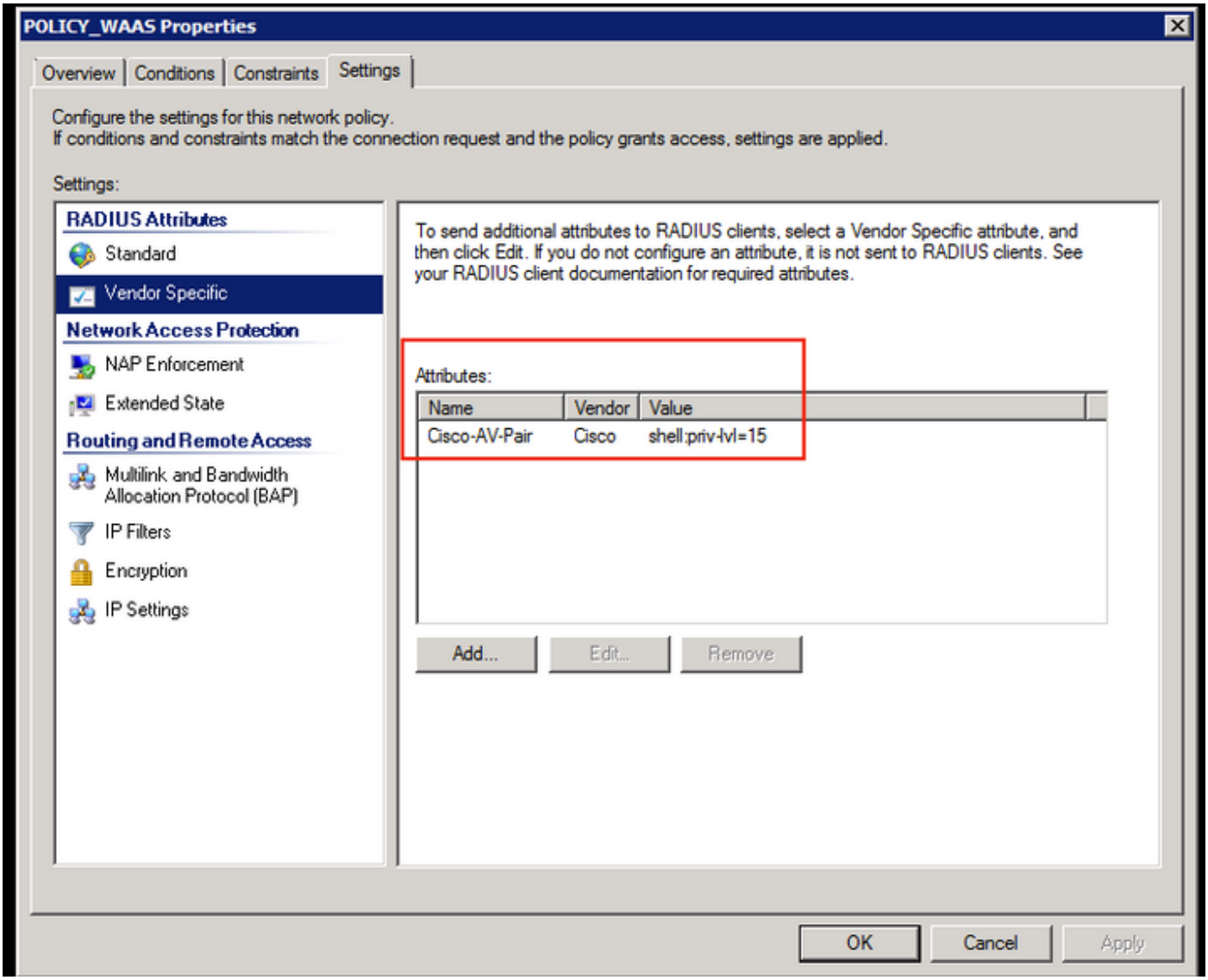
非暗号化認証(PAP、SPAP)としての認証方式。



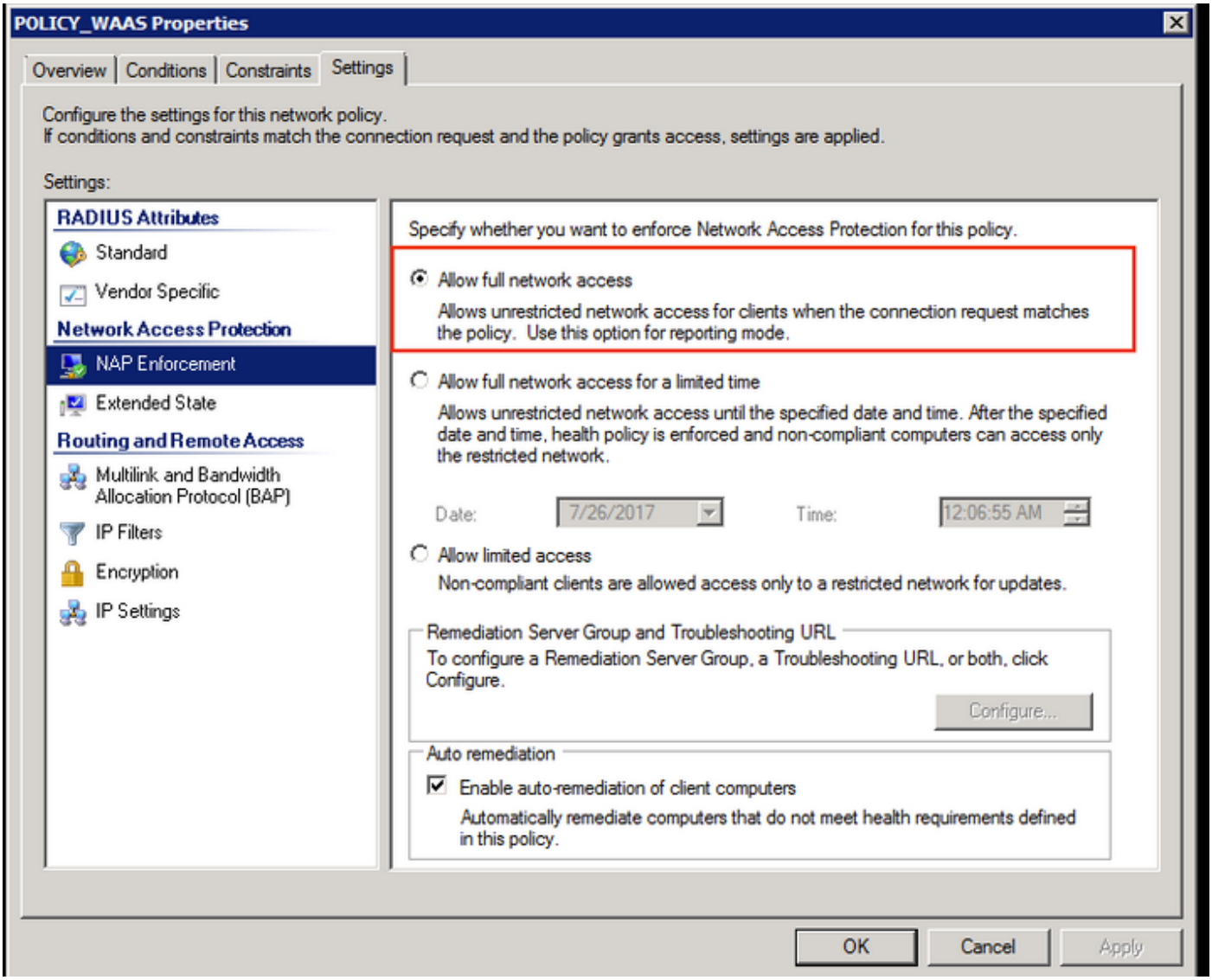
Service-Type as Administrative。



Cisco-AV-Pairとしてのベンダー固有属性(Shell:priv-lvl=15)。



フルネットワークアクセスを許可します。

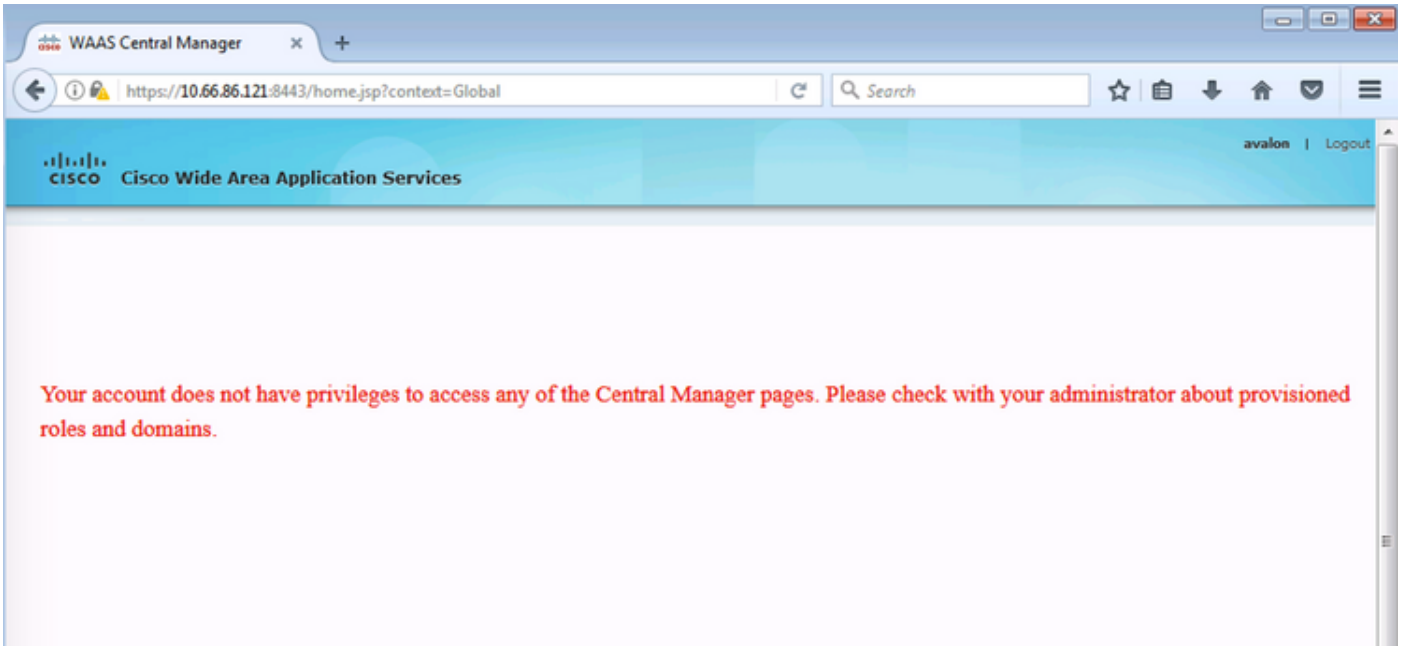


3. RADIUSユーザアカウントのWAAS CM設定

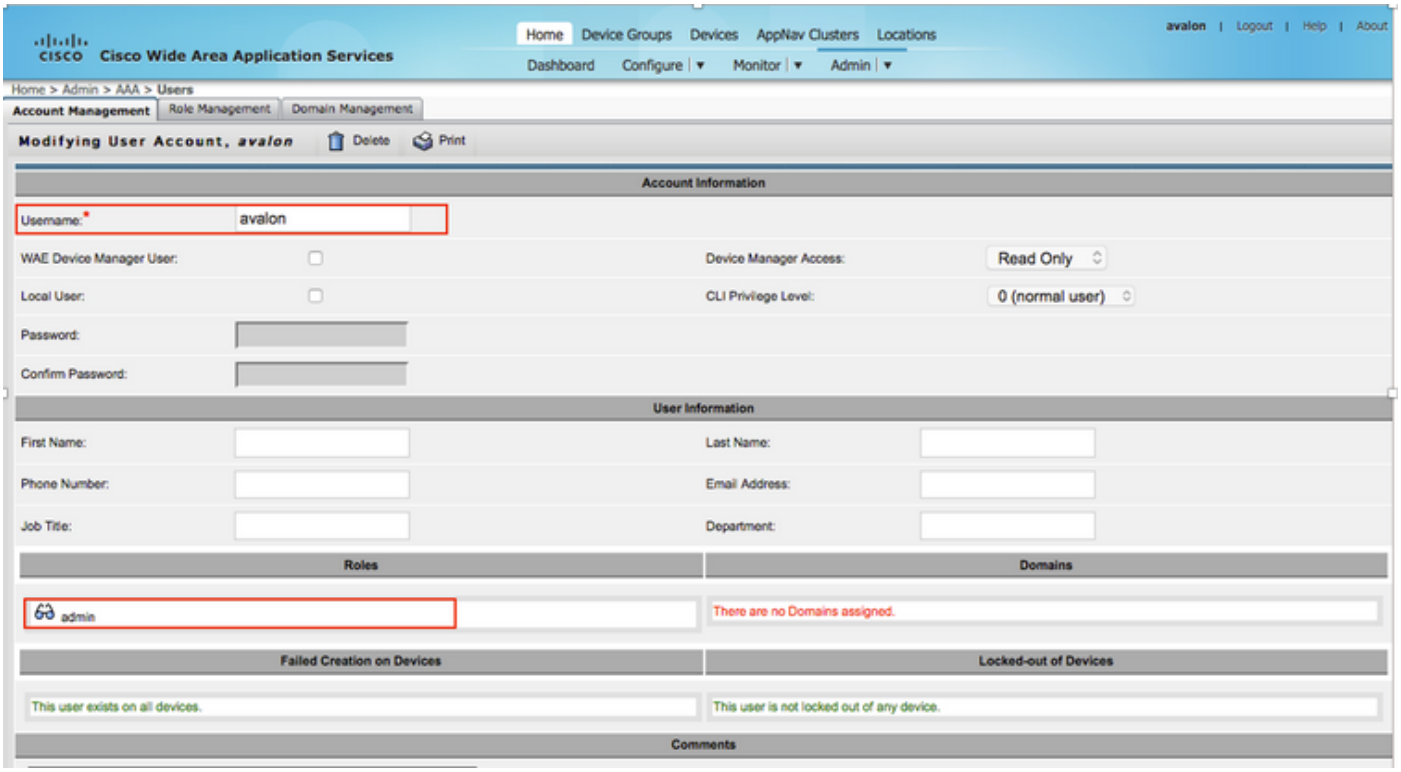
RADIUSで特権レベル15または1を使用してユーザを設定しても、WAAS CM GUIへのアクセスは提供されません。CMSデータベースには、外部AAAサーバとは別に、ユーザ、ロール、およびドメインのリストが保持されます。

ユーザを認証するために外部AAAサーバを正しく設定した後、CM GUIで動作するために必要なロールとドメインをユーザに与えるように、CM GUIを設定する必要があります。

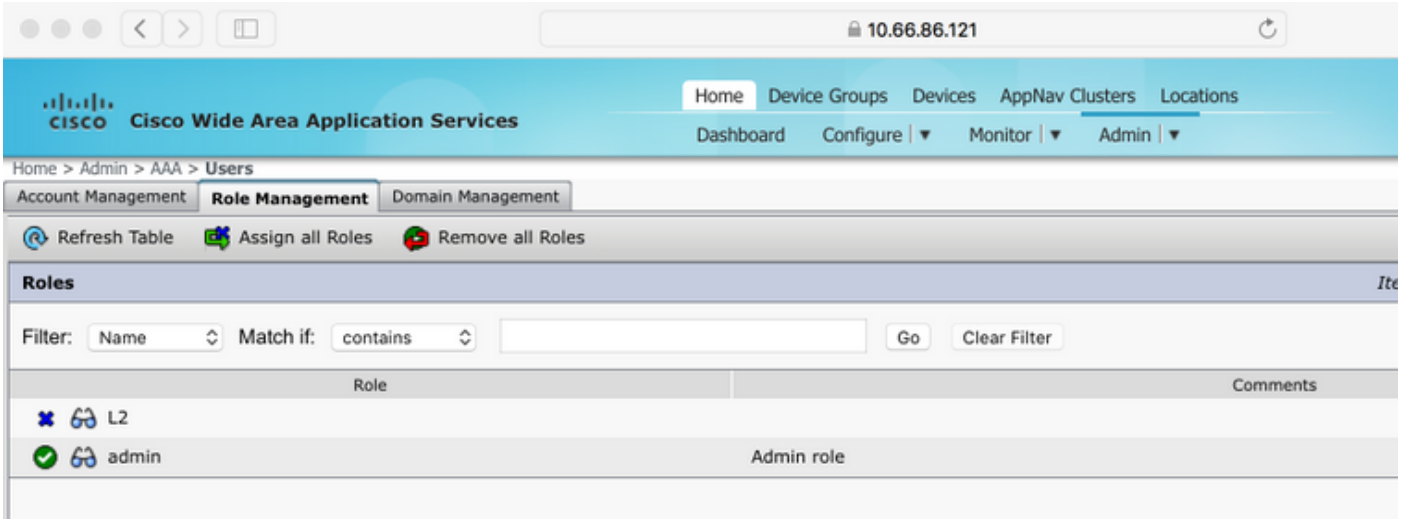
RADIUSユーザーがユーザーの下のCMに存在しない場合、そのユーザーを使用してGUIにログインするとき**は、アカウントにCentral Managerページへのアクセス権限がありません。プロビジョニングされた役割とドメインについては、管理者に確認してください。**このマッサージが表示されます。



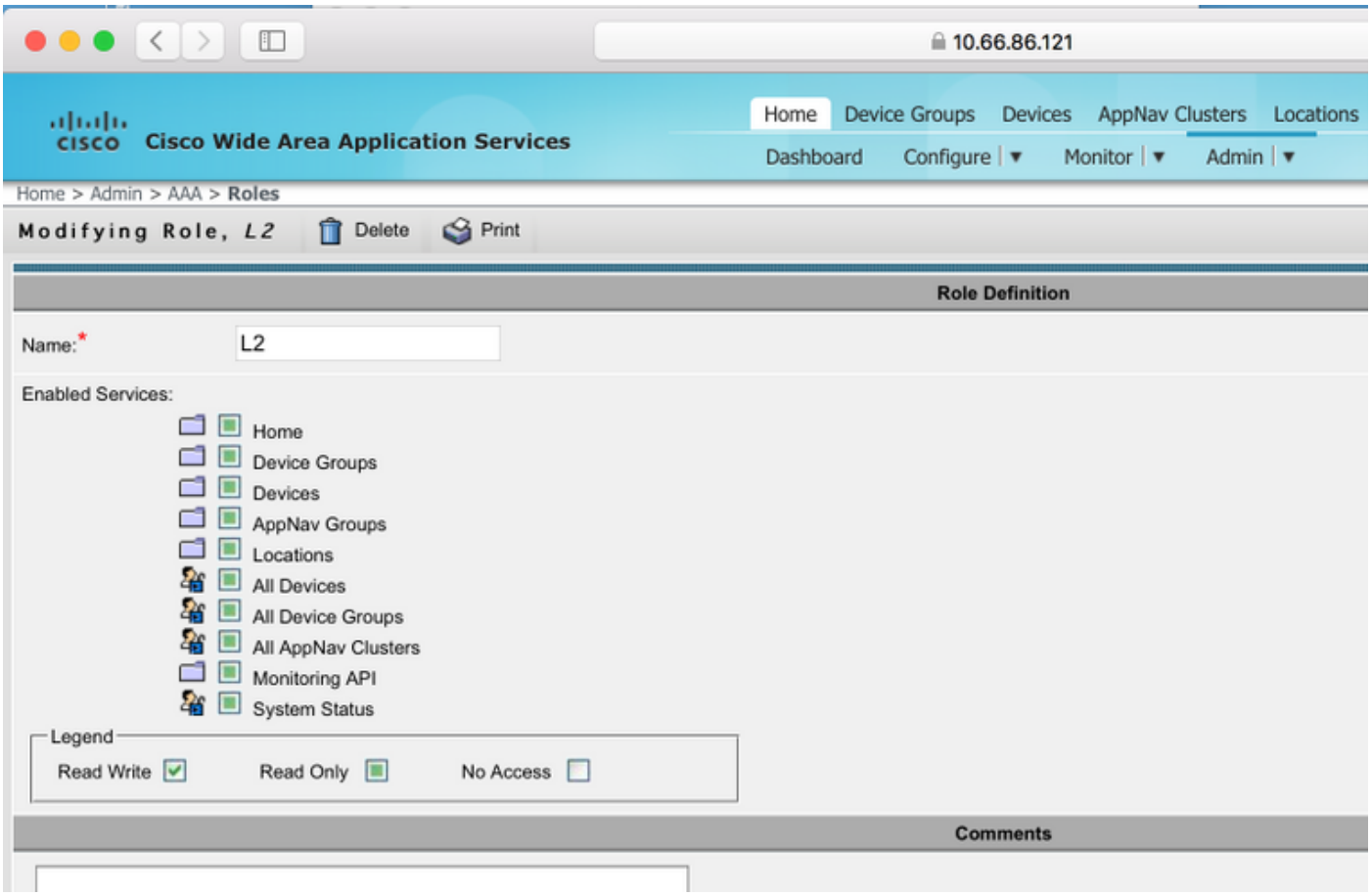
WAAS CMでのローカルユーザ名のパスワードなしの設定。



ユーザ名は、各ユーザの[Role Management]で適切なロールとバインドする必要があります。



ユーザに読み取り専用アクセスまたは制限付きアクセス権が必要な場合は、ロールの下でこれを設定できます。



確認

WAASデバイスでは、この設定がプッシュされます。

```
radius-server key ****
radius-server host 10.66.86.125 auth-port 1645
!
authentication login local enable secondary
authentication login radius enable primary
authentication configuration local enable secondary
```

authentication configuration radius enable primary
authentication fail-over server-unreachable

Cisco CLI アナライザ (登録ユーザ専用) は、特定の show コマンドをサポートします。show コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

- **authentication**：認証の設定

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

- Windowsドメインログを確認します
- **#debug aaa authorization** from WAAS CM CLI

関連情報

- WAASでのRADIUSサーバ認証設定
- ネットワークポリシーサーバはWindows Server 2008に適用されます