为Windows 2008 NPS服务器配置RADIUS - WAAS AAA

目录

简介

本文档介绍在思科广域应用服务(WAAS)和Windows 2008 R2网络策略服务器(NPS)上配置远程身份验证拨入用户服务(RADIUS)的过程。

默认WAAS配置使用本地身份验证。Cisco WAAS支持RADIUS和终端访问控制器访问控制系统(TACACS+)，也用于身份验证、授权和记帐(AAA)。 本文档仅介绍一台设备的配置。但是，也可以在设备组下执行此操作。所有配置必须通过WAAS CM GUI应用。

Cisco Wide Area Application Services Configuration Guide(Cisco Wide Area Application Services配置指南)中的"Configuring Administrative Login Authentication， Authorization， and Accounting"一章中提供了常规WAAS AAA配置。

作者：思科TAC工程师Hamilan Gnanabaskaran。

由思科TAC工程师Sanaz Tayar编辑。

先决条件

要求

Cisco 建议您了解以下主题：

- WAAS 5.x或6.x
- Windows NPS服务器
- AAA - RADIUS

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco WAAS — 虚拟中央管理器(vCM)
- WAAS 6.2.3.b
- Windows 2008 NPS

本文档中的信息都是基于特定实验室环境中的设备编写的。用于本文的所有设备都始于默认配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

本文档也可与以下硬件和软件版本一起应用：

- vWAAS、ISR-WAAS和所有WAAS设备
- WAAS 5.x或WAAS 6.x
- WAAS作为中央管理器、应用加速器

> **注意：**APPNAV-XE不支持此配置。路由器AAA将配置推送到APPNAV-XE。

配置步骤

需要应用以下配置：

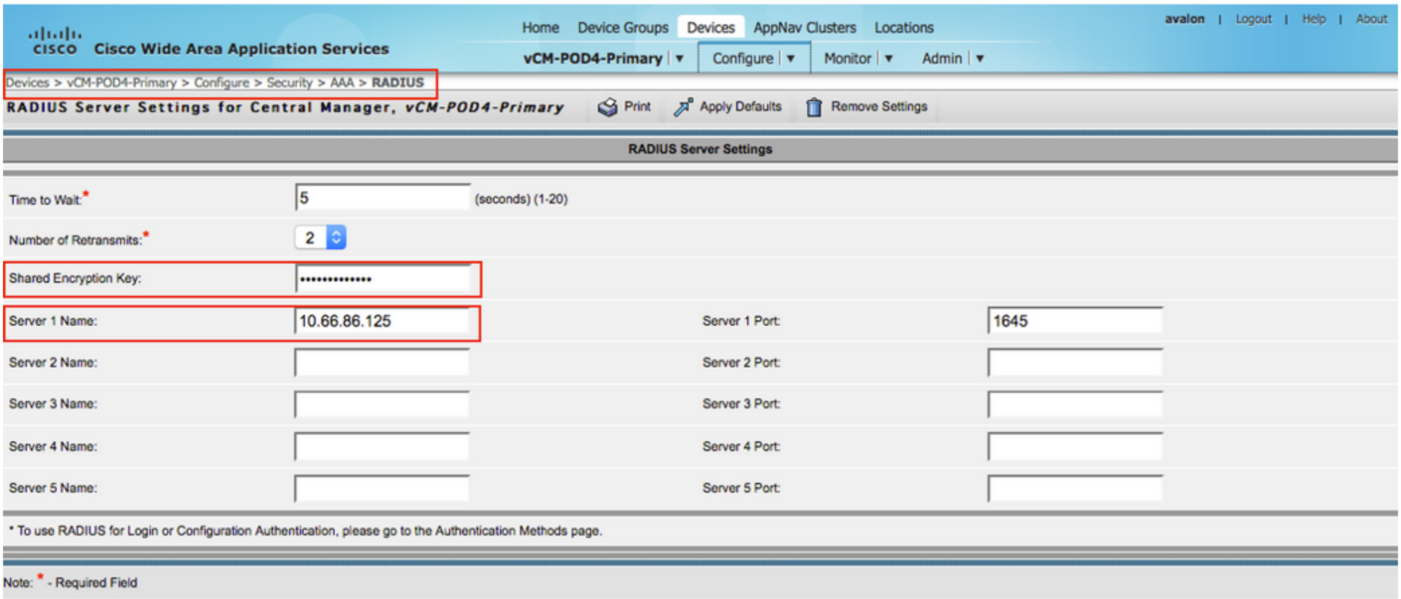
1. WAAS中央管理器
 1.1 AAA RADIUS配置
 1.2 AAA身份验证配置

2. Windows 2008 R2 - NPS服务器配置
 2.1 RADIUS客户端配置
 2.2网络策略配置

3. RADIUS用户帐户的WAAS CM配置

1. WAAS中央管理器

1.1在WAAS Central manager中，在Configure>Security>AAA>RADIUS下**创建RADIUS服务器。**



Devices > vCM-POD4-Primary > Configure > Security > AAA > RADIUS

RADIUS Server Settings for Central Manager, *vCM-POD4-Primary*

RADIUS Server Settings

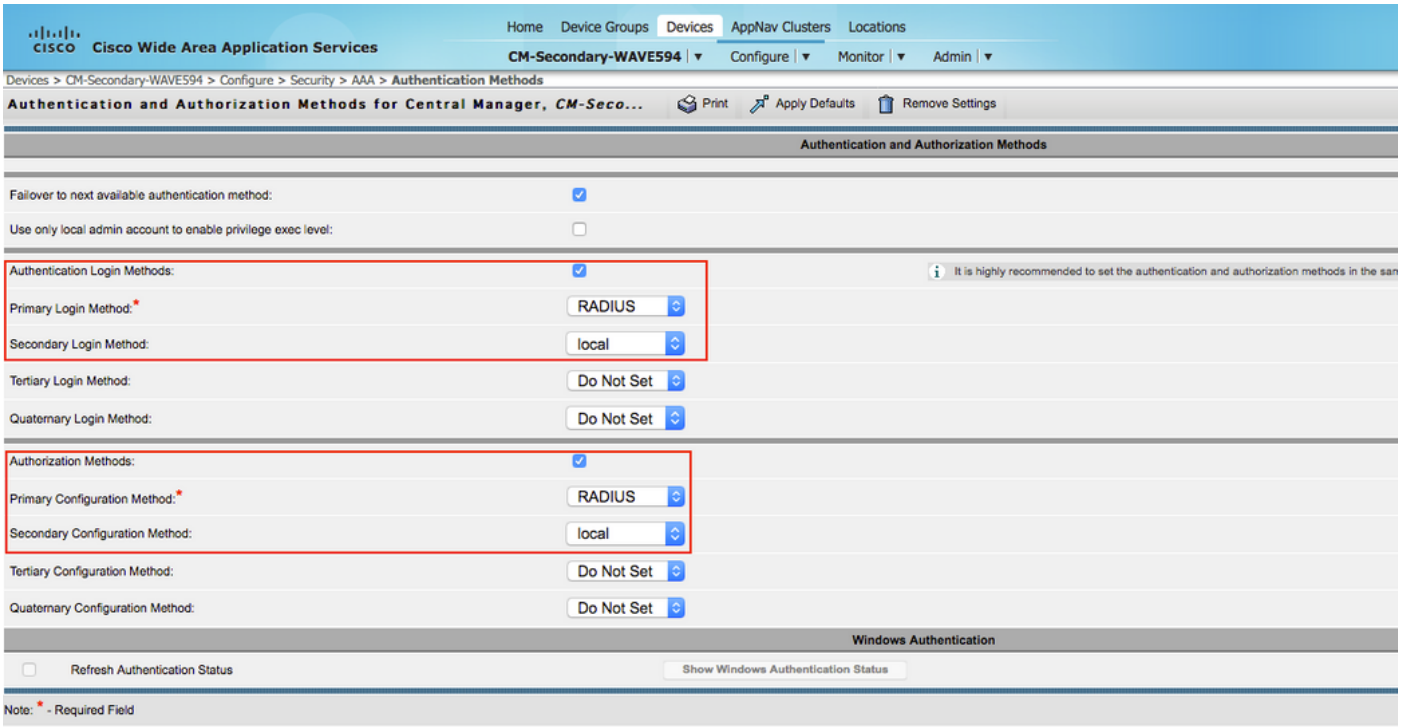
Time to Wait:*	5 (seconds) (1-20)		
Number of Retransmits:*	2		
Shared Encryption Key:	•••••••••••••		
Server 1 Name:	10.66.86.125	Server 1 Port:	1645
Server 2 Name:		Server 2 Port:	
Server 3 Name:		Server 3 Port:	
Server 4 Name:		Server 4 Port:	
Server 5 Name:		Server 5 Port:	

* To use RADIUS for Login or Configuration Authentication, please go to the Authentication Methods page.

Note: * - Required Field

1.2在Configure>Security>AAA>Authentication Methods下配置身份验证方法以反映RADIUS。

主身份验证方法被选为RADIUS，辅助身份验证方法被选为本地。因此，在RADIUS失败时，客户可以通过本地帐户登录。



Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authentication Methods

Authentication and Authorization Methods for Central Manager, *CM-Seco...*

Authentication and Authorization Methods

Failover to next available authentication method:	☑
Use only local admin account to enable privilege exec level:	□
Authentication Login Methods:	☑
Primary Login Method:*	RADIUS
Secondary Login Method:	local
Tertiary Login Method:	Do Not Set
Quaternary Login Method:	Do Not Set
Authorization Methods:	☑
Primary Configuration Method:*	RADIUS
Secondary Configuration Method:	local
Tertiary Configuration Method:	Do Not Set
Quaternary Configuration Method:	Do Not Set

It is highly recommended to set the authentication and authorization methods in the san

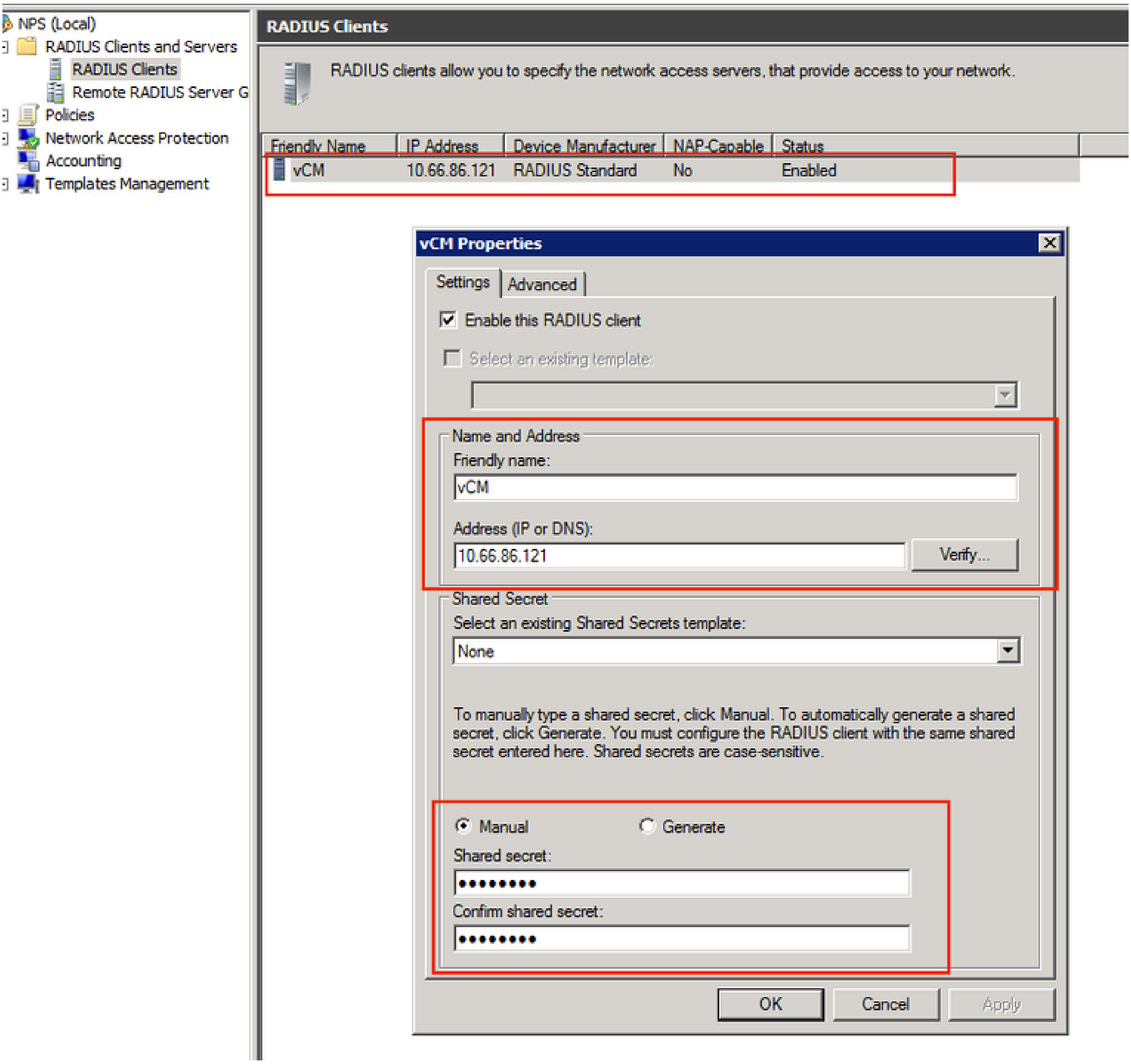
Windows Authentication

□ Refresh Authentication Status

Note: * - Required Field

2. Windows 2008 R2 - NPS服务器配置

2.1在Windows 2008 R2 - NPS服务器中，将WAAS设备IP创建为RADIUS客户端。



RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer	NAP-Capable	Status
vCM	10.66.86.121	RADIUS Standard	No	Enabled

vCM Properties

☑ Enable this RADIUS client

□ Select an existing template:

Name and Address

Friendly name: vCM

Address (IP or DNS): 10.66.86.121

Shared Secret

Select an existing Shared Secrets template: None

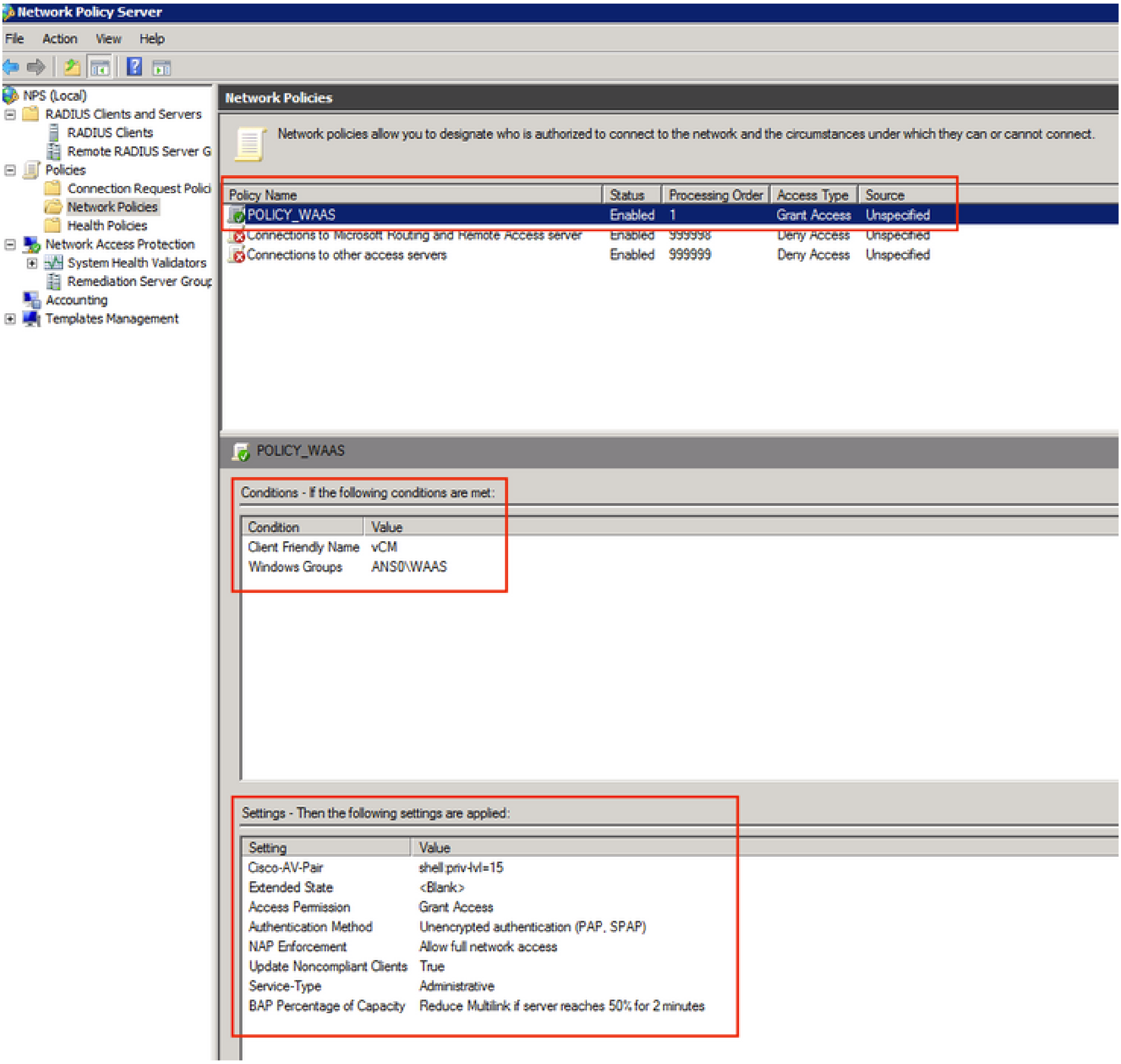
To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: ••••••••

Confirm shared secret: ••••••••

2.2在Windows 2008 R2 - NPS服务器中，创建网络策略以匹配WAAS设备并允许身份验证。



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
POLICY_WAAS	Enabled	1	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999998	Deny Access	Unspecified
Connections to other access servers	Enabled	999999	Deny Access	Unspecified

POLICY_WAAS

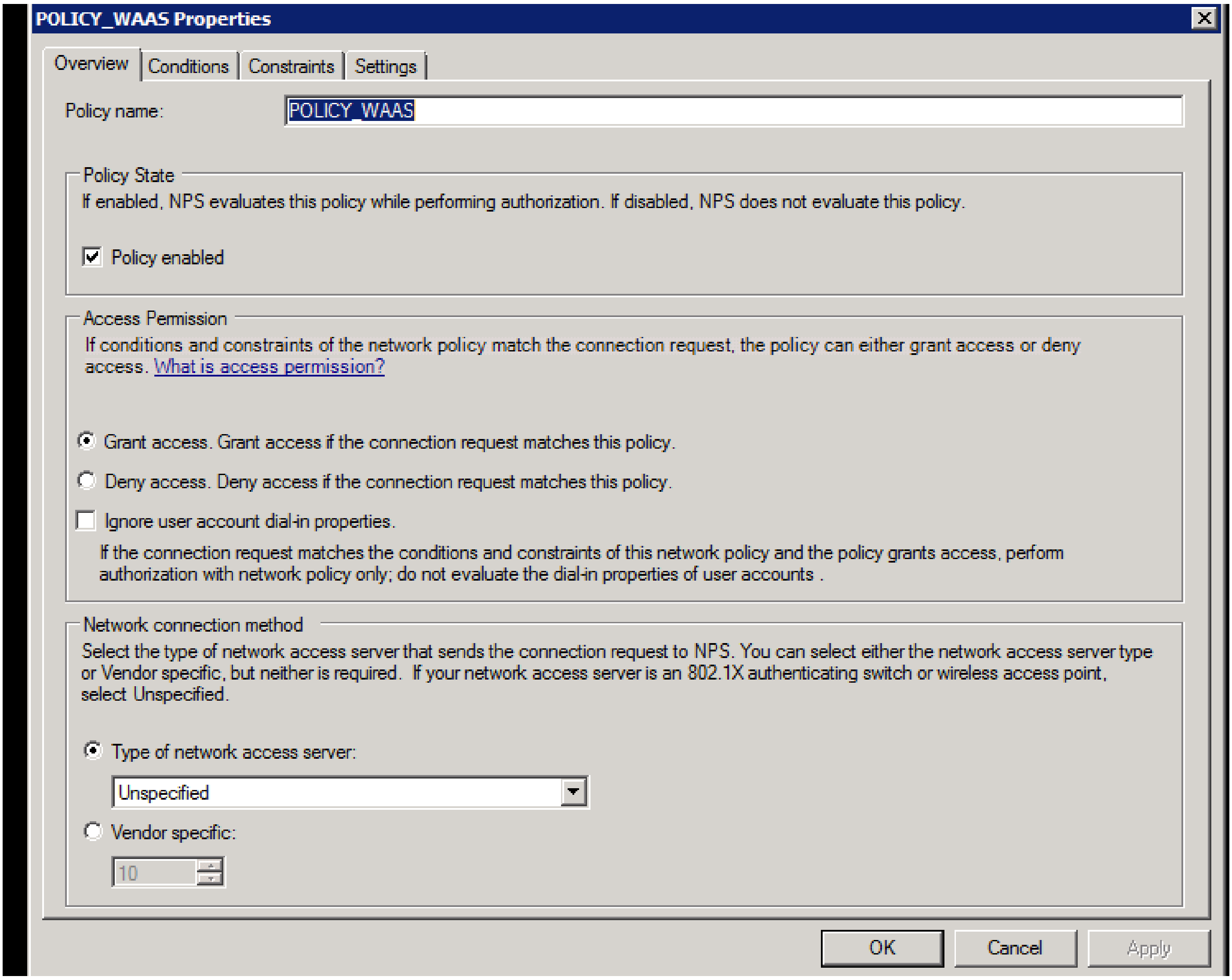
Conditions - If the following conditions are met:

Condition	Value
Client Friendly Name	vCM
Windows Groups	ANS0\WAAS

Settings - Then the following settings are applied:

Setting	Value
Cisco-AV-Pair	shell:priv-lvl=15
Extended State	<Blank>
Access Permission	Grant Access
Authentication Method	Unencrypted authentication (PAP, SPAP)
NAP Enforcement	Allow full network access
Update Noncompliant Clients	True
Service-Type	Administrative
BAP Percentage of Capacity	Reduce Multilink if server reaches 50% for 2 minutes

在实验室中，必须在NPS >Policies > Network Policy下选择这些参数。



Policy name: POLICY_WAAS

Policy State

If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☑ Policy enabled

Access Permission

If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. What is access permission?

● Grant access. Grant access if the connection request matches this policy.

○ Deny access. Deny access if the connection request matches this policy.

□ Ignore user account dial-in properties.

If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts .

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

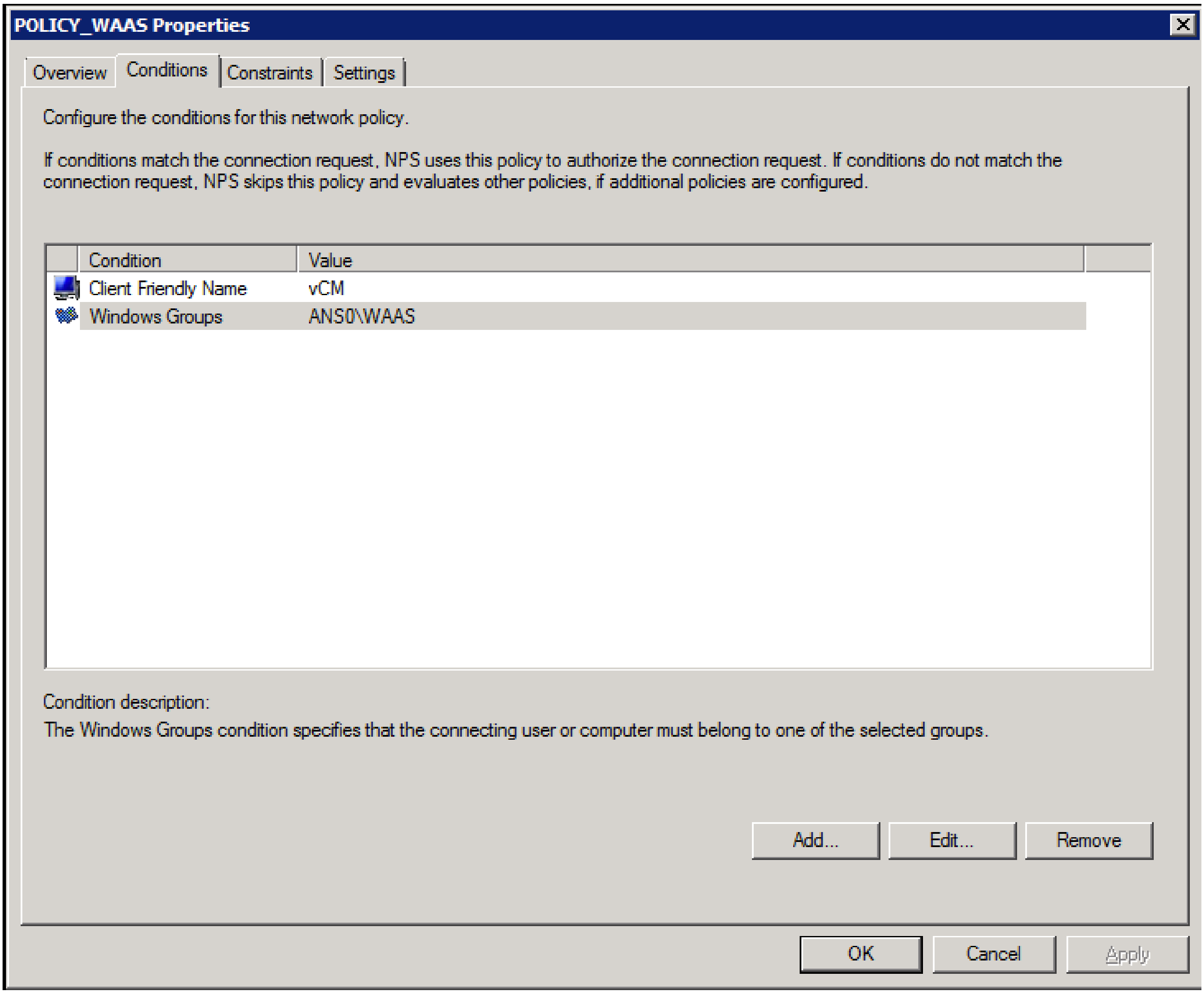
● Type of network access server:

Unspecified

○ Vendor specific:

10

条件可与Radius客户端友好名称匹配。其他方法可以使用，例如IP地址。



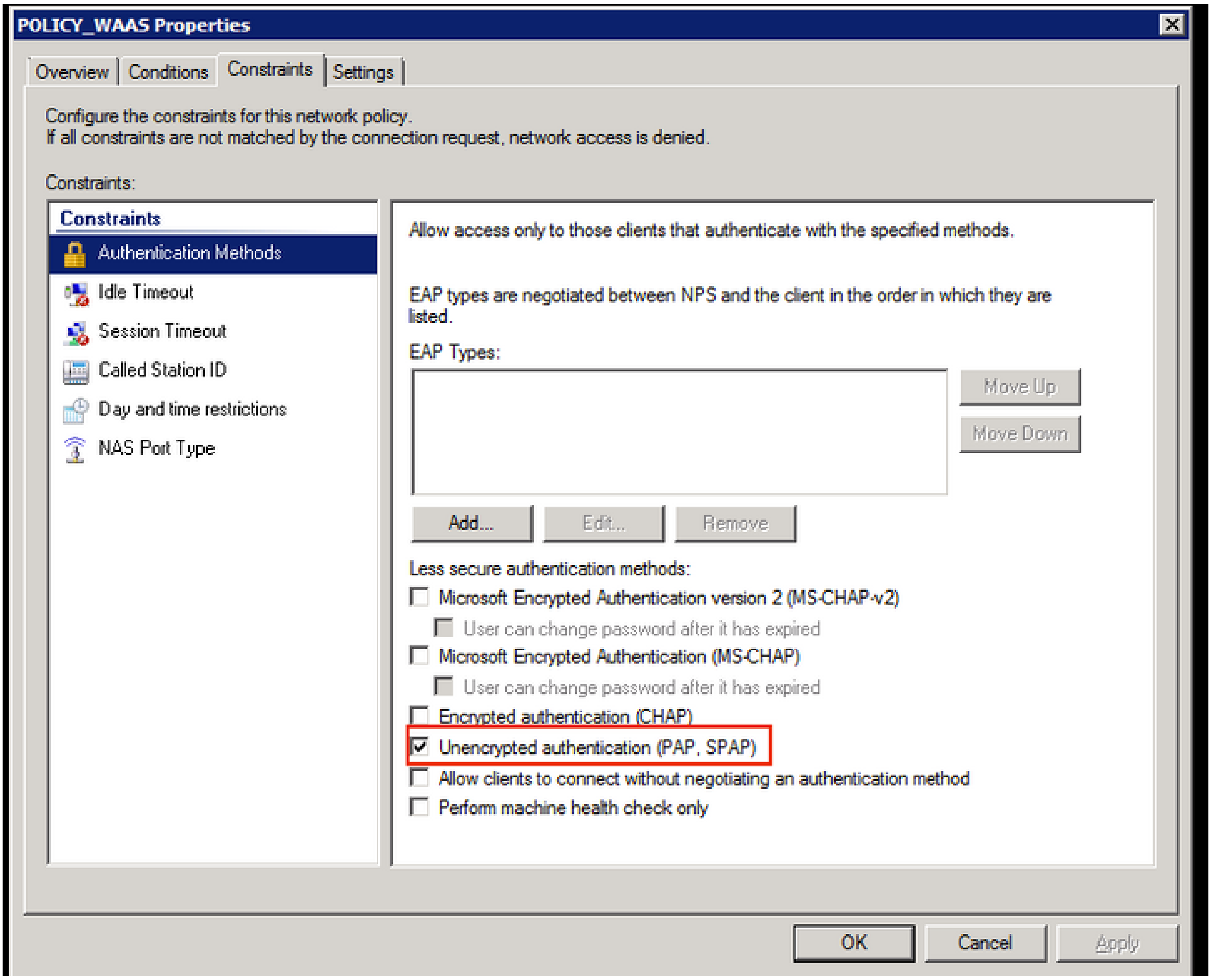
Configure the conditions for this network policy.

If conditions match the connection request, NPS uses this policy to authorize the connection request. If conditions do not match the connection request, NPS skips this policy and evaluates other policies, if additional policies are configured.

Condition	Value
Client Friendly Name	vCM
Windows Groups	ANS0\WAAS

Condition description:
The Windows Groups condition specifies that the connecting user or computer must belong to one of the selected groups.

身份验证方法，即未加密身份验证(PAP、SPAP)。



Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Less secure authentication methods:

□ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)

□ User can change password after it has expired

□ Microsoft Encrypted Authentication (MS-CHAP)

□ User can change password after it has expired

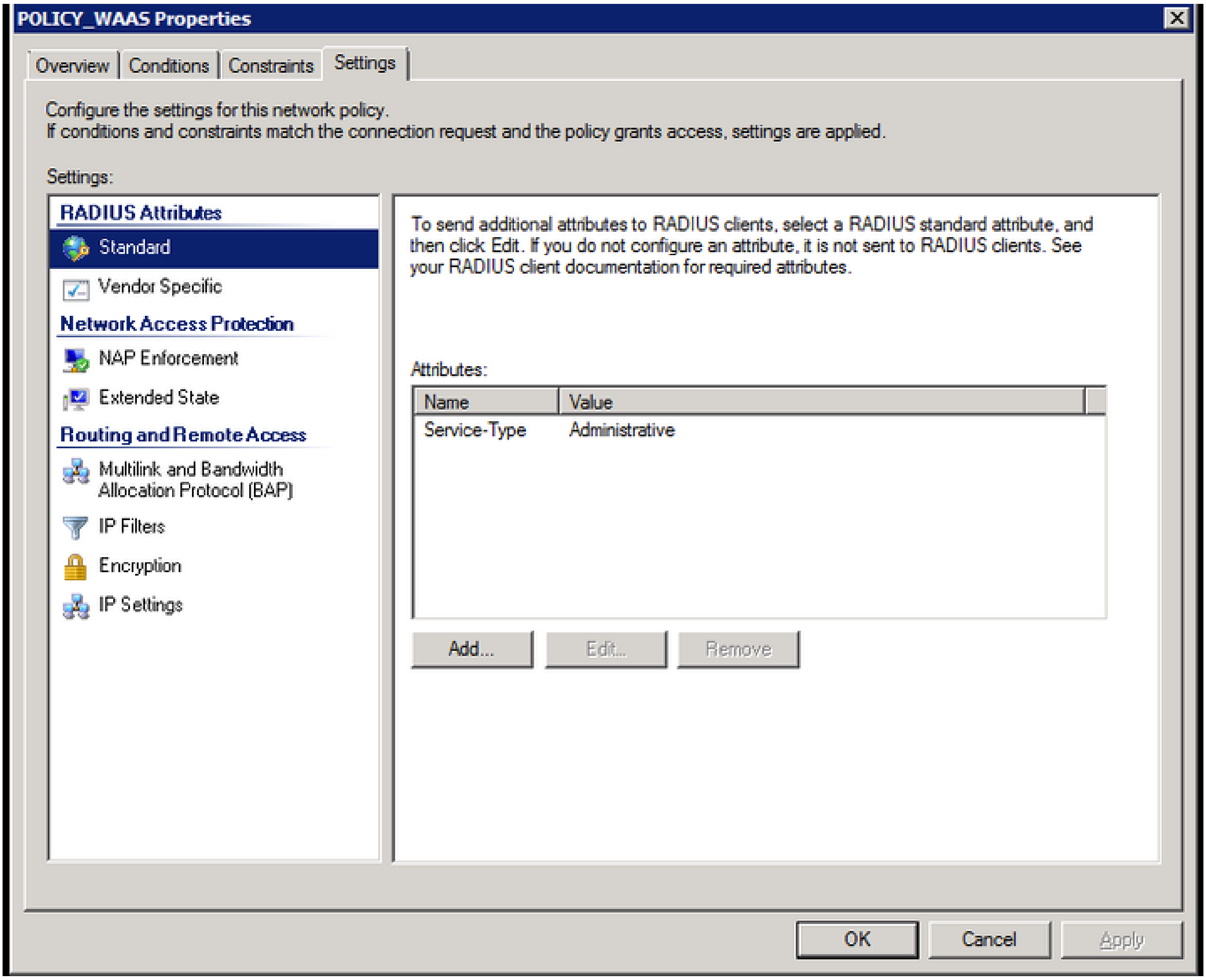
□ Encrypted authentication (CHAP)

☑ Unencrypted authentication (PAP, SPAP)

□ Allow clients to connect without negotiating an authentication method

□ Perform machine health check only

Service-Type（服务类型）作为Administrative（管理）。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

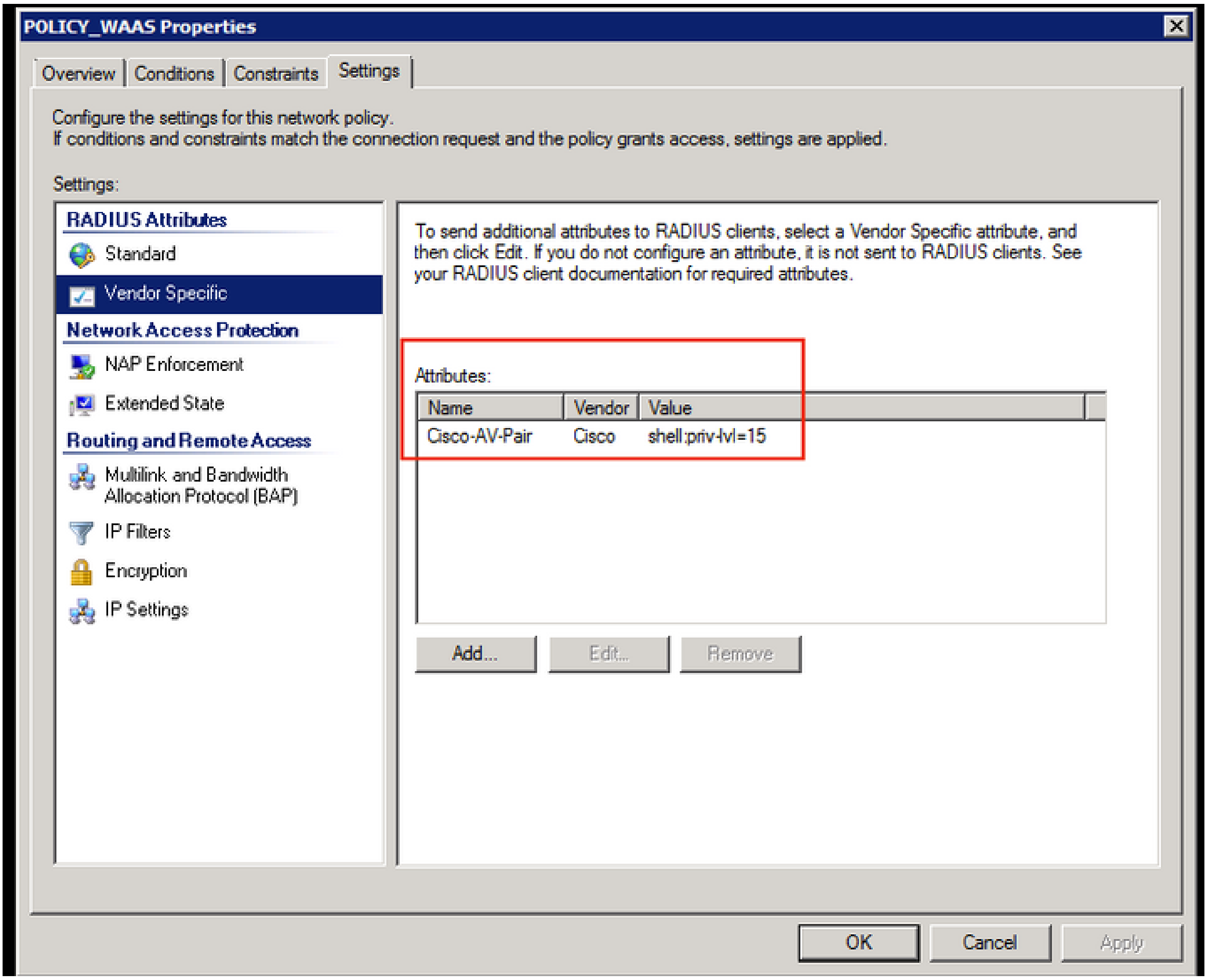
Settings:

To send additional attributes to RADIUS clients, select a RADIUS standard 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	Value
Service-Type	Administrative

供应商特定属性，作为Cisco-AV-Pair(Shell:priv-lvl=15)。



Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

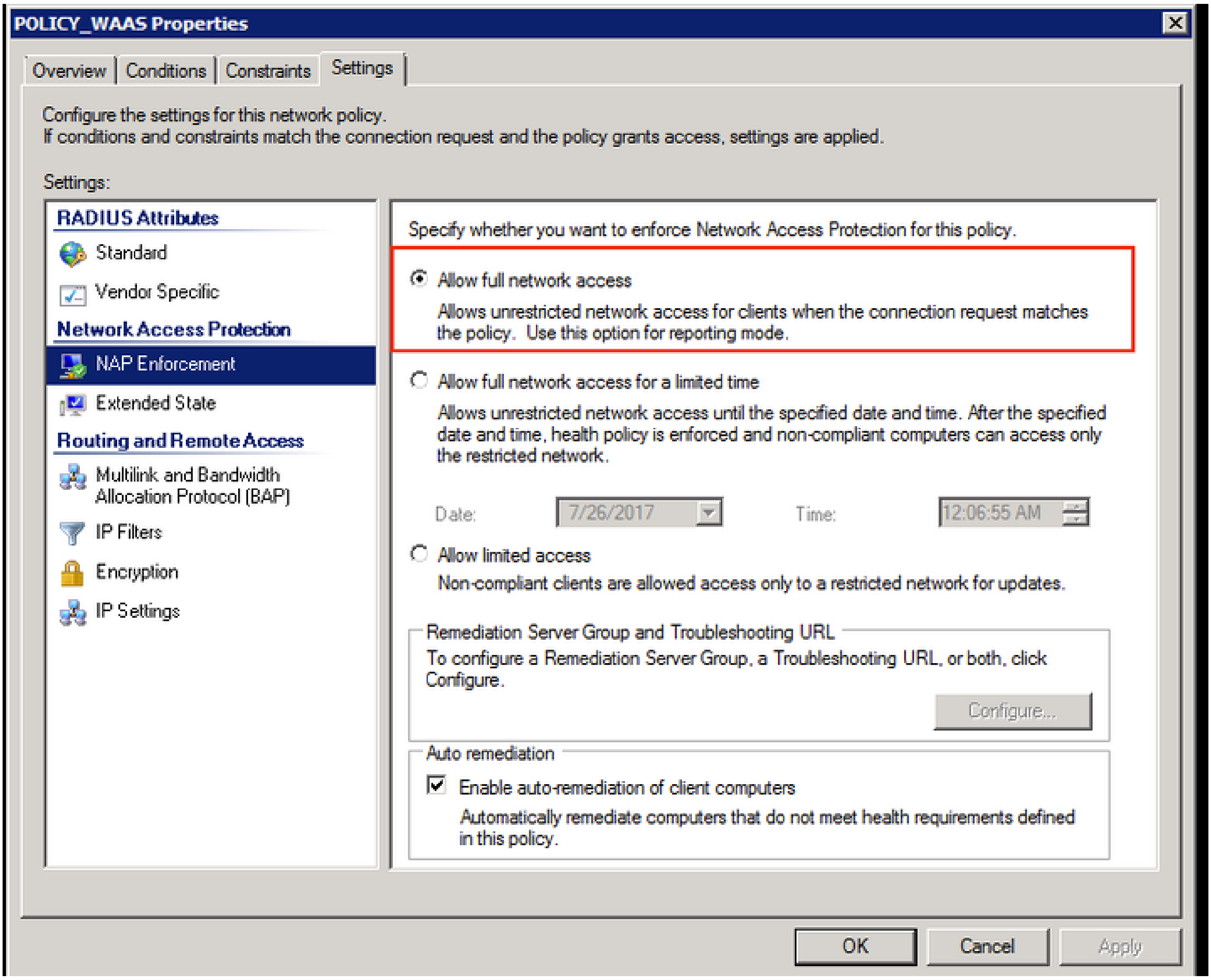
Settings:

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:priv-lvl=15

允许完全网络访问。



POLICY_WAAS Properties

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

Specify whether you want to enforce Network Access Protection for this policy.

● Allow full network access

Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.

○ Allow full network access for a limited time

Allows unrestricted network access until the specified date and time. After the specified date and time, health policy is enforced and non-compliant computers can access only the restricted network.

Date: 7/26/2017 Time: 12:06:55 AM

○ Allow limited access

Non-compliant clients are allowed access only to a restricted network for updates.

Remediation Server Group and Troubleshooting URL

To configure a Remediation Server Group, a Troubleshooting URL, or both, click Configure.

Auto remediation

☑ Enable auto-remediation of client computers

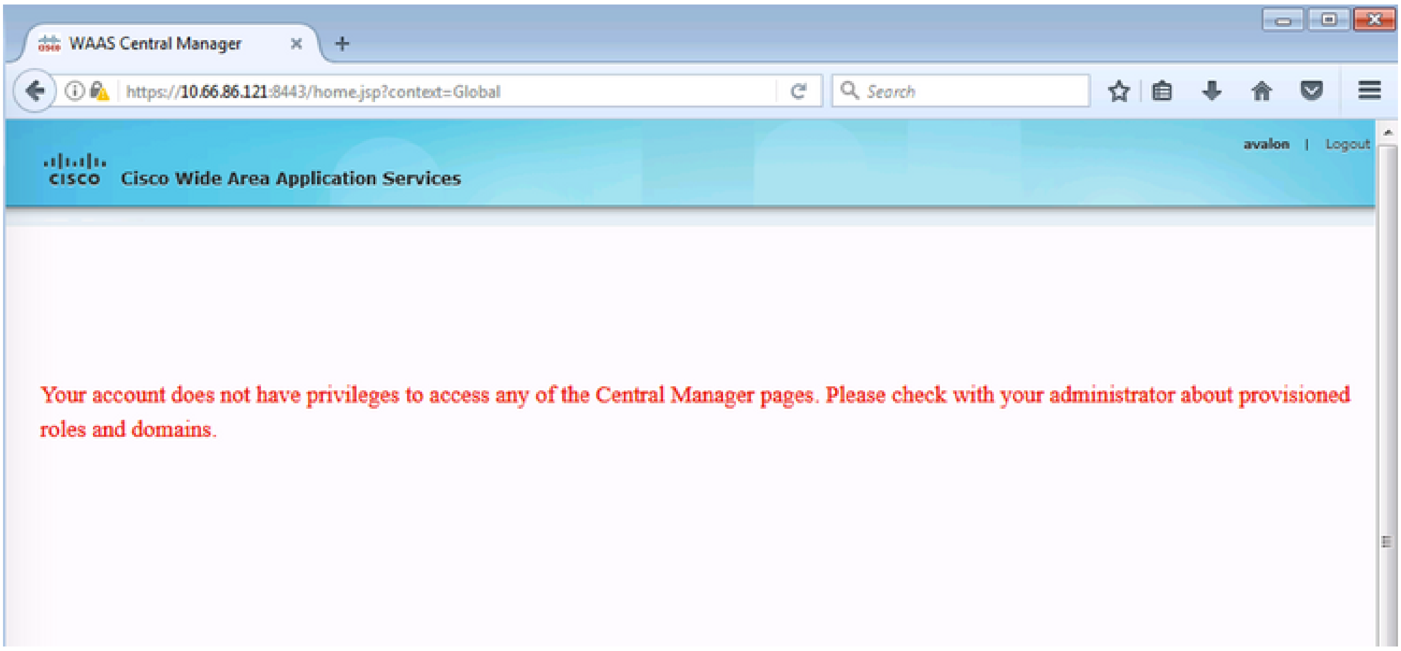
Automatically remediate computers that do not meet health requirements defined in this policy.

3. RADIUS用户帐户的WAAS CM配置

在RADIUS中配置权限级别为15或1的用户，不提供对WAAS CM GUI的访问。CMS数据库维护与外部AAA服务器分离的用户、角色和域列表。

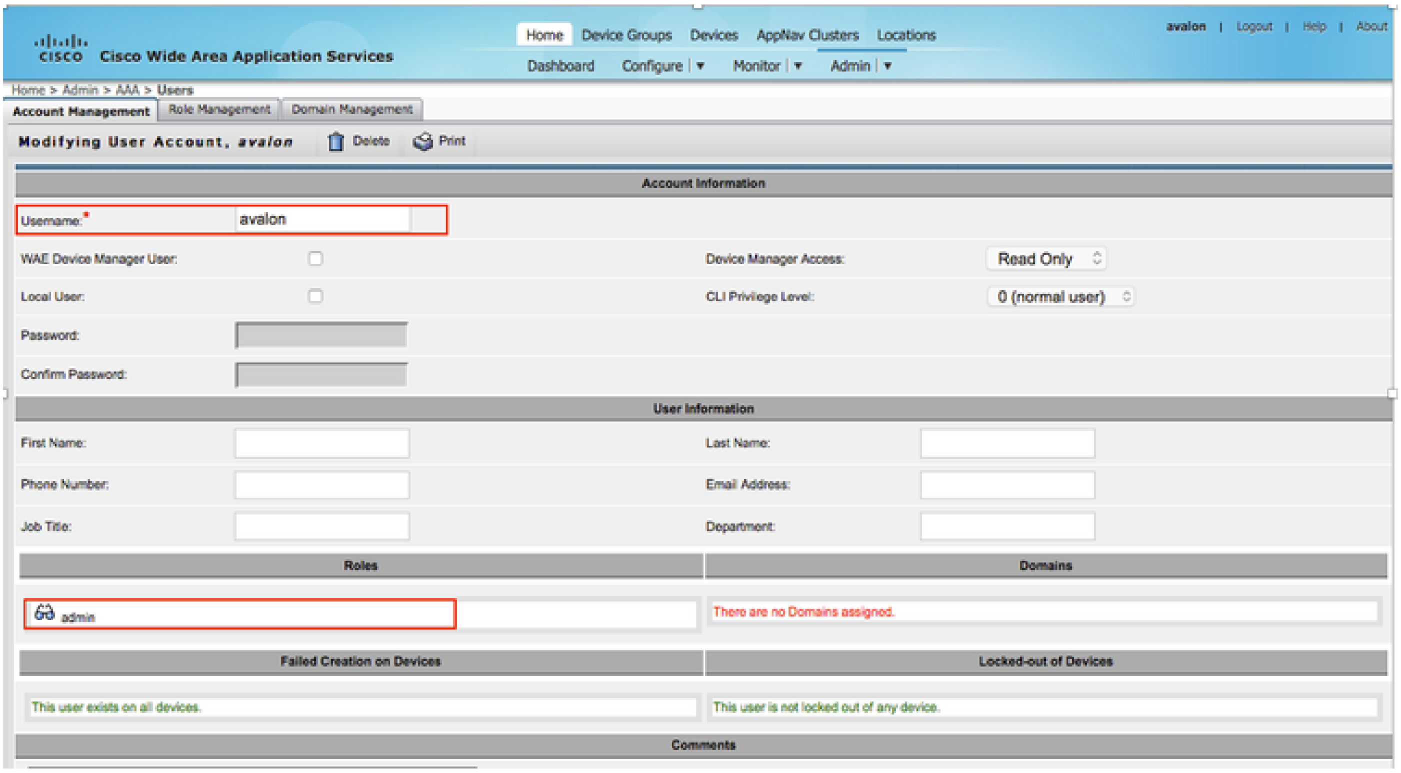
正确配置外部AAA服务器以验证用户身份后，必须配置CM GUI以为该用户提供在CM GUI内工作所需的角色和域。

如果RADIUS用户不在CM中的用户下，则当使用该用户登录GUI时，**您的帐户没有访问任何Central Manager页的权限。请咨询管理员，了解已调配的角色和域**。显示此按摩。


WAAS Central Manager
https://10.66.86.121:8443/home.jsp?context=Global
Search
Cisco Wide Area Application Services
avalon | Logout

Your account does not have privileges to access any of the Central Manager pages. Please check with your administrator about provisioned roles and domains.

在WAAS CM下配置本地用户名（无密码）。



Modifying User Account, avalon

Account Information

Username:*	avalon		
WAE Device Manager User:	□	Device Manager Access:	Read Only
Local User:	□	CLI Privilege Level:	0 (normal user)
Password:			
Confirm Password:			

User Information

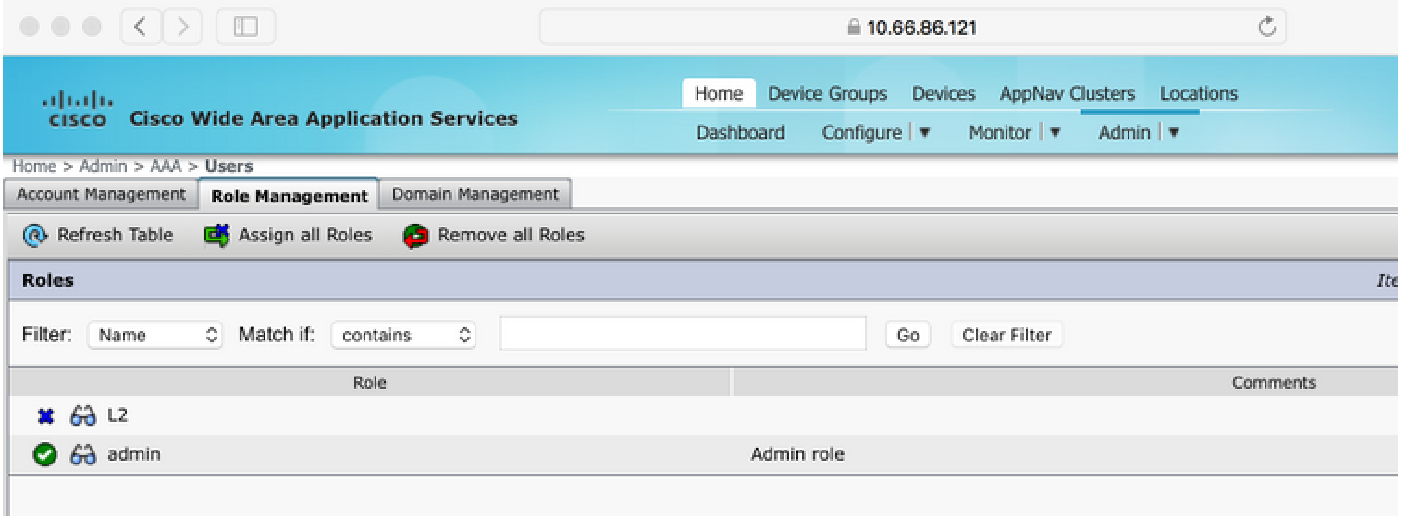
First Name:		Last Name:	
Phone Number:		Email Address:	
Job Title:		Department:	

Roles	Domains
admin	There are no Domains assigned.

Failed Creation on Devices	Locked-out of Devices
This user exists on all devices.	This user is not locked out of any device.

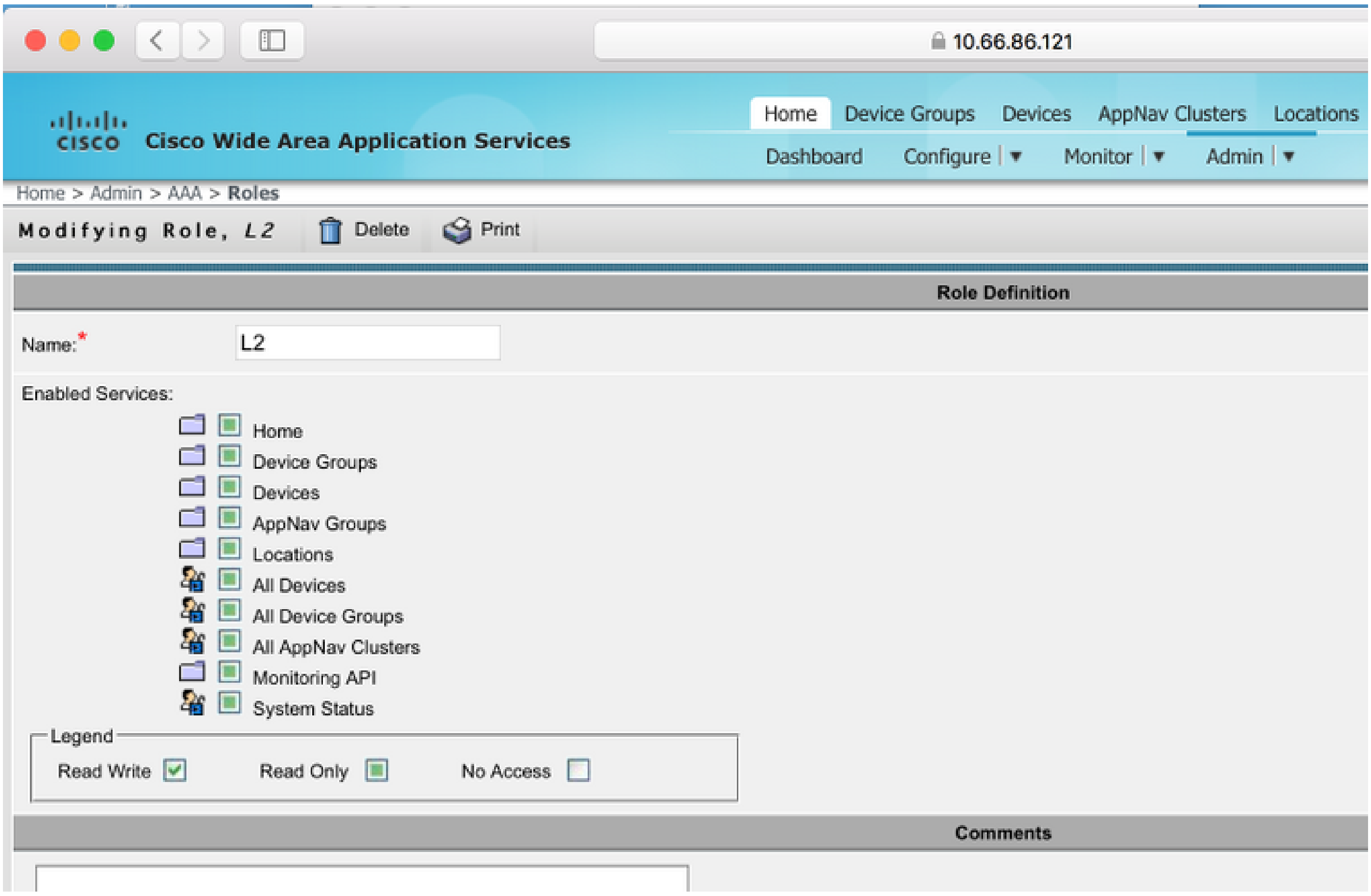
Comments

对于每个用户，用户名必须与角色管理下的正确角色绑定。



Role	Comments
✖ L2	
✓ admin	Admin role

如果用户需要具有只读访问权限或有限访问权限，可以在角色下配置。



Name:* L2

Enabled Services:

- ▣ Home
- ▣ Device Groups
- ▣ Devices
- ▣ AppNav Groups
- ▣ Locations
- ▣ All Devices
- ▣ All Device Groups
- ▣ All AppNav Clusters
- ▣ Monitoring API
- ▣ System Status

Legend

Read Write ☑ Read Only ▣ No Access □

确认

在WAAS设备中，此配置被推送。

```
radius-server key ****
radius-server host 10.66.86.125 auth-port 1645
!
身份验证登录本地启用辅助
身份验证登录RADIUS启用主
身份验证配置本地启用辅助
身份验证配置radius启用主
```

authentication fail-over server-unreachable

思科 CLI 分析器（仅适用于注册客户）支持某些 show 命令。要查看对 show 命令输出的分析，请使用思科 CLI 分析器。

- **authentication** — 配置身份验证

故障排除

本部分提供的信息可用于对配置进行故障排除。

- 检查Windows域日志
- #从**WAAS CM CLI**调试aaa授权

相关信息

- 在WAAS上配置RADIUS服务器身份验证设置
- 网络策略服务器适用于Windows Server 2008