# Konfigurieren von RADIUS für Windows 2008 NPS-Server - WAAS AAA

### Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konfigurationsschritte 1. WAAS Central Manager 2. Windows 2008 R2 - NPS-Serverkonfiguration 3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten Überprüfung Fehlerbehebung Zugehörige Informationen

# Einführung

In diesem Dokument wird das Verfahren der RADIUS-Konfiguration (Remote Authentication Dial-In User Service) für Cisco Wide Area Application Services (WAAS) und Windows 2008 R2 Network Policy Server (NPS) beschrieben.

Die WAAS-Standardkonfiguration verwendet die lokale Authentifizierung. Cisco WAAS unterstützt RADIUS und Terminal Access Controller Access Control System (TACACS+) auch für Authentication, Authorization, and Accounting (AAA). Dieses Dokument behandelt die Konfiguration nur für ein Gerät. Dies kann jedoch auch unter "Device Group" (Gerätegruppe) erfolgen. Alle Konfigurationen müssen über die grafische Benutzeroberfläche von WAAS CM angewendet werden.

Eine allgemeine WAAS-AAA-Konfiguration finden Sie im <u>Cisco Wide Area Application Services</u> <u>Configuration Guide</u> unter Configuring Administrative Login Authentication, Authorization, and Accounting.

Unterstützt von Hamilan Gnanabaskaran, Cisco TAC Engineer.

Bearbeitet von Sanaz Tayyar, Cisco TAC Engineer.

### Voraussetzungen

#### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- WAAS 5.x oder 6.x
- Windows NPS-Server

• AAA - RADIUS

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer Standardkonfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen angewendet werden:

- vWAAS, ISR-WAAS und alle WAAS-Appliances
- WAAS 5.x oder WAAS 6.x
- WAAS als Central Manager, Application Accelerator

**Hinweis**: APPNAV-XE unterstützt diese Konfiguration nicht. Router AAA leitet die Konfiguration an APPNAV-XE weiter.

### Konfigurationsschritte

Diese Konfiguration muss angewendet werden:

- 1. WAAS Central Manager
  - 1.1 AAA RADIUS-Konfiguration
  - 1.2 Konfiguration der AAA-Authentifizierung
- 2. Windows 2008 R2 NPS-Serverkonfiguration
  - 2.1 Konfiguration von RADIUS-Clients
  - 2.2 Netzwerkrichtlinienkonfiguration
- 3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten

#### 1. WAAS Central Manager

1.1 In WAAS Central Manager erstellt der RADIUS-Server unter **Konfigurieren > Sicherheit > AAA>RADIUS**.

cisco Wide Area Applicat	tion Services	Home I	Device Groups	Devices AppNar Configure   🔻	v Clusters Locati Monitor   🔻	ions Admin   🔻		avalon   Logout	Help   About
Devices > vCM-POD4-Primary > Configure > Sec	urity > AAA > RADIUS								
RADIUS Server Settings for Cent	ral Manager, <i>vCM</i> -P	OD4-Primary	S Print	Apply Defaults	Remove Settin	ngs			
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:		16	645		
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	Note: * - Required Field								

1.2 Konfigurieren Sie die Authentifizierungsmethode, um RADIUS unter **Konfigurieren > Sicherheit > AAA > Authentifizierungsmethoden** widerzuspiegeln.

Die Methode für die primäre Authentifizierung wird als RADIUS und die sekundäre Authentifizierungsmethode als lokal ausgewählt. Im Falle eines RADIUS-Fehlers kann sich der Kunde über ein lokales Konto anmelden.

(1)(1) CISCO Cisco Wide Area Application Services	Home     Device     AppNav Clusters     Locations       CM-Secondary-WAVE594 <ul> <li>Configure</li> <li>V</li> <li>Monitor</li> <li>I</li> <li>Admin</li> <li>I</li> <li>Admin</li> <li>I</li> <li>I</li></ul>
Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authentica Authentication and Authorization Methods for Centra	رtion Methods ا Manager, <i>CM-Seco</i> 🎯 Print 🔊 Apply Defaults 📋 Remove Settings
	Authentication and Authorization Methods
Failover to next available authentication method:	0
Use only local admin account to enable privilege exec level:	
Authentication Login Methods:	i It is highly recommended to set the authentication and authorization methods in the sa
Primary Login Method:*	RADIUS
Secondary Login Method:	local ᅌ
Tertiary Login Method:	Do Not Set
Quaternary Login Method:	Do Not Set 🗘
Authorization Methods:	0
Primary Configuration Method:*	RADIUS
Secondary Configuration Method:	local 🗘
Tertiary Configuration Method:	Do Not Set 👂
Quaternary Configuration Method:	Do Not Set
	Windows Authentication
Refresh Authentication Status	Show Windows Authentication Status
Note: * - Required Field	

#### 2. Windows 2008 R2 - NPS-Serverkonfiguration

2.1 Erstellen Sie im Windows 2008 R2 - NPS-Server die WAAS-Geräte-IP als RADIUS-Client.

NPS (Local)	PADTIIS Clients
RADIUS Clients and Servers	
RADIUS Clients	RADIUS clients allow you to specify the network access servers, that provide access to your network.
👸 Remote RADIUS Server G	
Policies	
Network Access Protection	Friendly Name IP Address Device Manufacturer NAP-Capable Status
Accounting	vCM 10.66.86.121 RADIUS Standard No Enabled
. Templates Management	
	vCM Properties
	Settings Advanced
	Enable this RADIUS client
	Select an existing template:
	Name and Address
	Friendly name:
	VCM
	Address (IP or DNS):
	10.66.86.121 Venity
	Shared Secret
	Select an existing Shared Secrets template:
	None
	_
	To manually type a shared executionic Manual. To a temptically expected a shared
	secret, click Generate. You must configure the RADIUS client with the same shared
	secret entered here. Shared secrets are case-sensitive.
	C Manual C Generate
	Chand accent
	Configuration of a second second
	OK Cancel Apply

2.2 Erstellen Sie im Windows 2008 R2 - NPS-Server eine Netzwerkrichtlinie, die den WAAS-Geräten entspricht und eine Authentifizierung zulässt.

Metwork Policy Server							
File Action View Help							
(= ->   2 🖬 🛛 🖬							
NPS (Local)	Network Policies						
RADIUS Clients and Servers							
RADIUS Clients	<ul> <li>Network policies allow you</li> </ul>	u to designate who is authorized to	o connect t	o the network and t	ne circumstance	is under which the	ey can or cannot connect.
Policies	-						
Connection Request Polici	Policy Name		Status	Processing Order	Access Type	Source	
Network Policies	POLICY WAAS		Enabled	1	Grant Access	Unspecified	
Health Policies	Connections to Microsoft Houtin	ng and Hemote Access server	Enabled	333338	Deny Access	Unspecified	
System Health Validators	Connections to other access se	rvers	Enabled	999999	Deny Access	Unspecified	
Remediation Server Group							
Not Accounting							
🗉 💐 Templates Management							
	POLICY_WAAS						
	Conditions . If the following cond	itione are mat-					
	Conductors - It are following cond	itions are met.					
	Condition Value						
	Client Friendly Name vCM						
	Windows Groups ANSU\V	IAAS					
	L						
	1						
	Settinge . Then the following set	inne are anotad					
	Settings - mentale following set	angs are appreu.					
	Setting	Value					
	Cisco-AV-Pair	shell:priv-lvl=15					
	Extended State	<blank></blank>					
	Access Permission	Urant Access	CDAD)				
	NAP Enforcement	Allow full network access	, SPAP)				
	Update Noncompliant Clients	True					
	Service-Type	Administrative					
	BAP Percentage of Capacity	Reduce Multilink if server reacher	s 50% for 2	minutes			

Im LAB müssen diese Parameter unter NPS > Policies > Network Policy (NPS > Richtlinien > Netzwerkrichtlinie) ausgewählt werden.

ICY_WAAS Prope	ties							
verview Conditions	Constraints Se	ttings						
Policy name:	POLICY_W	AAS						
Policy State If enabled, NPS eva	luates this policy v	while performing a	authorization. If	disabled, NPS	does not e	valuate this pol	icy.	
Policy enabled								
Access Permission	onstraints of the r	etwork policy m	atch the conne	ection request,	the policy	can either gra	nt access or der	ιу
		-						
• Grant access. G	ant access if the c	onnection reque	st matches this	policy.				
C Deny access. De	ny access if the c	onnection reque	st matches this	policy.				
🗌 Ignore user acco	unt dial-in propertie	es.						
If the connection authorization with	equest matches to network policy on	he conditions and ly; do not evalua	d constraints of te the dial-in pro	this network po operties of user	olicy and th accounts	e policy grants	access, perform	
Network connection	method							
Select the type of n or Vendor specific, I select Unspecified.	twork access ser ut neither is requir	ver that sends th ed. If your netwo	e connection re ork access serv	equest to NPS. veris an 802.1X	You can se ( authentic	elect either the ating switch or	network access wireless access	server type point,
• Type of network	access server:							
Unspecified			•					
C Vendor specific								
10 🚊								

Bedingung kann mit Radius Client Friendly Name abgeglichen werden. Es können andere Methoden verwendet werden, z. B. die IP-Adresse.

POLICY	_WAAS Properties		×
Overv	iew Conditions Constra	raints Settings	
			1
Conf	igure the conditions for this	is network policy.	
If con	nditions match the connect vection request NPS skips	ction request, NPS uses this policy to authorize the connection request. If conditions do not match the	
Conin	icetion request, nr 5 stips	s and policy and evaluates only policies, in additional policies are configured.	
	Condition	Meha	— I
		Value	
	Client Friendly Name	VCM	
	Windows Groups	ANS0\WAAS	
Cond	lition description:		
The	Windows Groups conditior	on specifies that the connecting user or computer must belong to one of the selected groups.	
		Add Edit Remo	ve
		OK Cancel	Apply

Authentifizierungsmethoden als unverschlüsselte Authentifizierung (PAP, SPAP).

POLICY_WAAS Properties	×
Overview Conditions Constraints Setting	s
Configure the constraints for this network poli If all constraints are not matched by the conn	cy. ection request, network access is denied.
Constraints  Constraints  Authentication Methods  Session Timeout  Called Station ID	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: Move Up
Pay and time restrictions	Add       Edt       Remove         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)         User can change password after it has expired         Encrypted authentication (PAP, SPAP)         Allow clients to connect without negotiating an authentication method         Perform machine health check only
	OK Cancel Apply

Servicetyp als "Verwaltung".

infigure the settings for this network policy conditions and constraints match the con ettings:	y. nection request and the policy grants access, settings are applied.
RADIUS Attributes Standard Vendor Specific Network Access Protection NAP Enforcement	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.
Extended State	Attributes:
Routing and Remote Access	Service-Type Administrative
Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Encryption R IP Settings	Add Edit Remove

Herstellerspezifisches Attribut als Cisco-AV-Paar (Shell:priv-lvl=15).

POLICY_WAAS Properties		×
Overview Conditions Constraints Setting	js	
Configure the settings for this network policy If conditions and constraints match the conr Settings:	, nection request and the policy grants access, settings are applied.	_
Standard      Vendor Specific      Network Access Protection	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.	
NAP Enforcement	Attributes:	
🕎 Extended State	Name Vendor Value	
Routing and Remote Access	Cisco-AV-Pair Cisco shell:priv-lvl=15	
Multilink and Bandwidth Allocation Protocol (BAP) IP Filters Encryption References		
	Add Edit Remove	
	OK Cancel Apply	

Vollständigen Netzwerkzugriff zulassen.

Configure the settings for this network policy. f conditions and constraints match the conne Settings:	ection request and the policy grants access, settings are applied.
Standard     Vendor Specific     Network Access Protection	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.
<ul> <li>NAP Enforcement</li> <li>Extended State</li> <li>Routing and Remote Access</li> <li>Multilink and Bandwidth Allocation Protocol (BAP)</li> <li>IP Filters</li> <li>Encryption</li> <li>IP Settings</li> </ul>	<ul> <li>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</li> <li>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         Muto remediation         Fenable auto-remediation of client computers         Automatically remediate computers that do not meet health requirements defined         </li> </ul>

#### 3. WAAS CM-Konfiguration für RADIUS-Benutzerkonten

Wenn Sie einen Benutzer in RADIUS mit der Berechtigungsstufe 15 oder 1 konfigurieren, ist der Zugriff auf die grafische Benutzeroberfläche von WAAS CM nicht möglich. Die CMS-Datenbank verwaltet eine Liste von Benutzern, Rollen und Domänen, die vom externen AAA-Server getrennt sind.

Nach der korrekten Konfiguration des externen AAA-Servers für die Benutzerauthentifizierung muss die CM-GUI so konfiguriert werden, dass diesem Benutzer die Rollen und Domänen zugewiesen werden, die für die Arbeit in der CM-GUI erforderlich sind.

Wenn sich der RADIUS-Benutzer nicht im CM unter dem Benutzer befindet, hat Ihr Konto keine Berechtigungen für den Zugriff auf eine der Seiten des zentralen Managers, wenn Sie sich bei diesem Benutzer in der GUI anmelden. Bitte erkundigen Sie sich bei Ihrem Administrator nach den bereitgestellten Rollen und Domänen. Diese Massage wird angezeigt.

wAAS Central Manager	× +					
( I A https://10.66.86.12	1:8443/home.jsp?context=Global	C <sup>e</sup> Q, Search	☆自	+ -	r 🛡	≡
alialia cisco Cisco Wide Are	a Application Services			a	valon	Logout
Your account does not I	nave privileges to access any of the Centr	ral Manager pages. Please check with your	administrator al	bout p	rovisio	ned
roles and domains.						
						н

#### Konfiguration eines lokalen Benutzernamens unter WAAS CM ohne Kennwort.

ahaha		Home Device Groups	Devices AppNav Clusters Lo	cations	avalon   Logout   Help   About		
CISCO Cisco Wide Are	a Application Services	Dashboard Configure	▼ Monitor   ▼ Admin   ▼				
Home > Admin > AAA > Users	Domain Management						
Account Hanagement	angenere de Deine de Deine						
Modifying User Account	t, avaion						
		Account	Information				
Usemame:*	avalon						
WAE Device Manager User:			Device Manager Access:	Read Only 0			
Local User:	•		CLI Privilege Level:	0 (normal user)			
Password:							
Confirm Password:							
·		User In	formation				
First Name:			Last Name:				
Phone Number:			Email Address:				
Job Title:			Department:				
Roles			Domains				
L (1)			These are an Demains and see				
00 admin			mere are no comains assigned.				
	Failed Creation on Devices			Locked-out of Devices			
This user exists on all devices.	This user exists on all devices.			y device.			
Comments							

Benutzername muss für jeden Benutzer mit den richtigen Rollen unter Rollenverwaltung verknüpft werden.

$\bullet \bullet \bullet \checkmark \land$		⋒ 10.66.86.121	Ċ
cisco Cisco Wide	e Area Application Services	Home Device Groups Devices AppNav Clus Dashboard Configure    Monitor	ters Locations
Home > Admin > AAA > Users			
Account Management Rol	e Management Domain Management		
🔞 Refresh Table 📑 Assign all Roles 👩 Remove all Roles			
Roles			Ite
Filter: Name 0	Match if: contains	Go Clear Filter	
	Role		Comments
🗙 🔂 L2			
🕗 🔂 admin		Admin role	

Wenn der Benutzer nur Lesezugriff oder eingeschränkten Zugriff benötigt, kann dies unter Rollen konfiguriert werden.

	€ 10.66.86.121		
CISCO Cisco Wide Area Application Service	Home         Device Groups         Devices         AppNav Clusters         Locations           s         Dashboard         Configure   ▼         Monitor   ▼         Admin   ▼		
Home > Admin > AAA > Roles       Modifying Role, L2     In Delete       In Delete     In Print			
	Role Definition		
Name:* L2			
Enabled Services:			
	Comments		

# Überprüfung

Auf den WAAS-Geräten wird diese Konfiguration weitergeleitet.

```
Radius-Server-Schlüssel ****
RADIUS-Server-Host 10,66,86.125 Authentifizierungsport 1645
!
Authentifizierung Anmeldung lokal aktivieren sekundäre
Authentifizierungs-Anmelderadius aktiviert primär
Authentifizierung Konfiguration lokal aktivieren sekundäre
```

Der <u>Cisco CLI Analyzer</u> (nur <u>registrierte</u> Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

• Authentifizierung: Authentifizierung konfigurieren

# Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

- Überprüfen Sie die Windows-Domänenprotokolle
- #debugaa-Autorisierung von der WAAS CM-CLI

## Zugehörige Informationen

- Konfigurieren der Authentifizierungseinstellungen des RADIUS-Servers in WAAS
- Network Policy Server gilt für Windows Server 2008