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

# 内容

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

### 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、『<u>Cisco Wide Area Application Services設定ガイド』の「</u> <u>管理ログイン認証、許可、アカウンティングの設定」</u>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
- 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。

cisco Cisco Wide Area Applica	tion Services	Home	Device Groups	Devices AppNa Configure	v Clusters Locati	ions Admin   🔻	avalon   Logout   Help   About
Devices > vCM-POD4-Primary > Configure > Sec	urity > AAA > RADIUS				-		
RADIUS Server Settings for Cent	ral Manager, vCM-F	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:		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.							
kote: * - Required Field							

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。

cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations CM-Secondary-WAVE594 V Configure V Monitor V Admin V
Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authentica	ition Methods
Authentication and Authorization Methods for Centra	I Manager, CM-Seco 🥸 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 sar
Primary Login Method:*	RADIUS
Secondary Login Method:	local 🗘
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。

NPS (Local)	DADUIC Charles
RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server G Policies	RADIUS clients allow you to specify the network access servers, that provide access to your network.
Network Access Protection	Friendly Name IP Address Device Manufacturer NAP-Capable Status
Accounting	vCM 10.66.86.121 RADIUS Standard No Enabled
	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 Verify
	C 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     C Generate     Shared secret:
	••••••
	Confirm shared secret:
	••••••
	OK Cancel Apply

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。

Network Policy Server							
File Action View Help							
(=							
NPS (Local)	Network Policies						
E RADIUS Clients and Servers							
RADIUS Clients	Network policies allow yo	u to designate who is authorized t	o connect t	to the network and t	he circumstance	s under which the	ey can or cannot connect.
Remote RADIUS Server G							
In Policies	a j Policies						1
Connection Request Polici	Policy Name		Status	Processing Order	Access Type	Source	
Wetwork Policies	POLICY_WAAS		Enabled	1	Grant Access	Unspecified	
Realth Polices	Connections to Microsoft Hout	ng and Hemote Access server	Enabled	aaaaas	Deny Access	Unspecified	
System Health Validators	Connections to other access s	ervers	Enabled	999999	Deny Access	Unspecified	
Remediation Server Group							
Accounting							
Implates Management							
			_				
	POLICY_WAAS						
	Conditions - If the following cond	ditions are met:					
	Condition						
	Cleat Eteady Name VCM						
	Wiedewe Groupe ANS/01	MAAS					
	Windows Groups ANSON	VAR3					
	1						
	Settings - Then the following set	tings are applied:					
	Catting	Value					
	Geographic Ciego AV/ Pair	value shall not y bits 15					
	Extended State	Allerty AVIE 10					
	Access Participa	Grant Accase					
	A theotication Method	Linencented a theotication /DAD	CDAD)				
	NAP Enforcement	Allow full petwork appage	, SPAP)				
	Ladata Naccampliant Conto	Taue					
	Section Time	Administrative					
	PAP Personal and Connector	Partice Multiple & engine reacher	E01/ (m- 2	min das			
	over reicentage or capacity	neudce mutuink if server reaches	5 30 % TOP 2	ina futes			
	4						

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**。

LICY_WAAS Properties					
Overview Conditions Constraints Settings					
Policy name: POLICY_WAAS					
Policy State If enabled, NPS evaluates this policy while performing au	thorization. If disabled. N	IPS does not e	valuate this poli	cv.	
Policy enabled					
Access Permission					
If conditions and constraints of the network policy mat access What is access permission?	tch the connection requ	est, the policy	can either gran	t access or deny	t
access. <u>I mario acceso pormosion.</u>					
<ul> <li>Grant access. Grant access if the connection request</li> </ul>	matches this policy.				
C 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 netwo	k policy and th	e policy grants a	access, perform	
authorization with network policy only; do not evaluate	the dial-in properties of i	iser accounts .			
Network connection method	N N				
or Vendor specific, but neither is required. If your network	connection request to N k access server is an 80	2.1X authentic	elect eitner the r ating switch or v	vireless access se	erver type bint,
select Unspecified.					
• Type of network access server:					
Unspecified	•				
C Vendor specific:					
10 -					
·					
			ОК	Cancel	Apply

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。

POLICY_W	AAS Properties	s	×
Overview	Conditions Co	onstraints Settings	
Configur	n the conditions fo	arthis potwork policy	
coningui	e trie conditions to	or this network policy.	
If conditi connect	ions match the co ion request. NPS :	onnection request, NPS uses this policy to authorize the connection request. If conditions do not match the skips this policy and evaluates other policies, if additional policies are configured.	
	andition	Value	_
	ient Friendly Name	e vCM	
w 🐝	indows Groups	ANSO/WAAS	
Condition	n description:		
The Win	ndows Groups con	ndition specifies that the connecting user or computer must belong to one of the selected aroups.	
		······································	
		Add Edit Bemo	vell
			<u> </u>
		OK Cancel	Apply

非暗号化認証(PAP、SPAP)としての認証方式。

POLICY_WAAS Properties	×
Overview Conditions Constraints Setting	s
Configure the constraints for this network pol If all constraints are not matched by the conr Constraints:	icy. nection request, network access is denied.
Constraints Authentication Methods	Allow access only to those clients that authenticate with the specified methods.
nt Idle Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed.
Called Station ID	Move Up
Day and time restrictions     AS Port Type	Move Down
	Add Edit 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)     Unencrypted authentication (PAP, SPAP)
	Allow clients to connect without negotiating an authentication method
,	,
	OK Cancel Apply

Service-Type as Administrative.

POLICY_WAAS Properties		×
Overview Conditions Constraints Settings	1	
Configure the settings for this network policy. If conditions and constraints match the connect Settings: RADIUS Attributes	tion request and the policy grants access, settings are applied.	
Standard  Vendor Specific  Network Access Protection  NAP Enforcement	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:	-
Extended State	Name Value	-
Routing and Remote Access         Multilink and Bandwidth Allocation Protocol (BAP)         IP Filters         Encryption         IP Settings	Service-Type Administrative Administrative Add Edit Remove	
	OK Cancel	Apply

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

POLICY_WAAS Properties		×
Overview Conditions Constraints Setting	s	
Configure the settings for this network policy. If conditions and constraints match the conn Settings:	ection request and the policy grants access, settings are applied.	
RADIUS Attributes     Standard     Zendor 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)		
🔒 Encryption 🚜 IP Settings		
	Add Edit Remove	
	OK Cancel Apply	

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 Central Manager	× +						<b>×</b>
( Inttps://10.66.86.121:84	43/home.jsp?context=Global	C Q. Search	☆自	÷	A	◙	≡
cisco Cisco Wide Area A	pplication Services				avalon	I Lo	gout
Your account does not hav roles and domains.	re privileges to access any of the Cent	ral Manager pages. Please check with your ad	ministrator a	bout	provis	sione	d
							н

### WAAS CMでのローカルユーザ名のパスワードなしの設定。

Lisco Cisco Wide Are	a Application Services	Home Device Groups D Dashboard Configure	v Monitor   v Admin   v	ons	avalon   Logout   Help   About	
Account Management Role Ma	nagement Domain Management					
Modifying User Accoun	t, avalon 📋 Delete 🥁 Print					
		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		
A 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						

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。

$\bullet \bullet \bullet \langle \rangle$		€ 10.66.86.121	Ċ
alialia cisco Cisco (	Wide Area Application Services	Home Device Groups Devices AppNav Clusters L Dashboard Configure    Monitor    Admin	ocations
Home > Admin > AAA >	Users		
Account Management	Role Management Domain Management		
Refresh Table	🗳 Assign all Roles 🛛 👩 Remove all Roles		
Roles			It
Filter: Name	♦ Match if: contains ♦	Go Clear Filter	
	Role		Comments
¥ 60 L2			
🕗 🔂 admin		Admin role	

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。

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

# 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

<u>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。</u>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
- <u>ネットワークポリシーサーバはWindows Server 2008に適用されます</u>