Configuration de RADIUS pour Windows 2008 NPS Server - WAAS AAA

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configuration Steps
1. Gestionnaire central WAAS
2. Windows 2008 R2 - Configuration du serveur NPS
3. Configuration WAAS CM pour les comptes d'utilisateurs RADIUS
Vérification
<u>Dépannage</u>
Informations connexes

Introduction

Ce document décrit la procédure de configuration RADIUS (Remote Authentication Dial-In User Service) sur Cisco Wide Area Application Services (WAAS) et Windows 2008 R2 Network Policy Server (NPS).

La configuration WAAS par défaut utilise l'authentification locale. Cisco WAAS prend également en charge RADIUS et le système de contrôle d'accès du contrôleur d'accès aux terminaux (TACACS+) pour l'authentification, l'autorisation et la comptabilité (AAA). Ce document couvre la configuration d'un seul périphérique. Cependant, cela peut également être fait sous le groupe de périphériques. Toute la configuration doit être appliquée via l'interface utilisateur graphique WAAS CM.

La configuration générale de WAAS AAA est fournie dans le <u>Guide de configuration de Cisco</u> <u>Wide Area Application Services</u> sous le chapitre Configuration de l'authentification de connexion administrative, de l'autorisation et de la comptabilité.

Contribution de Hamilan Gnanabaskaran, Ingénieur du centre d'assistance technique Cisco.

Édité par Sanaz Tayyar, Ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WAAS 5.x ou 6.x
- Serveur NPS Windows
- AAA RADIUS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

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

The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont démarré avec une configuration par défaut. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Produits connexes

Ce document peut également être appliqué avec les versions matérielles et logicielles suivantes :

- vWAAS, ISR-WAAS et tous les appareils WAAS
- WAAS 5.x ou WAAS 6.x
- WAAS en tant que gestionnaire central, accélérateur d'applications

Remarque : APPNAV-XE ne prend pas en charge cette configuration. Le routeur AAA transmet la configuration à APPNAV-XE.

Configuration Steps

Ces configurations doivent être appliquées :

- 1. Gestionnaire central WAAS
 - 1.1 Configuration AAA RADIUS
 - 1.2 Configuration de l'authentification AAA
- 2. Windows 2008 R2 Configuration du serveur NPS
 - 2.1 Configuration des clients RADIUS
 - 2.2 Configuration de la stratégie réseau
- 3. Configuration WAAS CM pour les comptes d'utilisateurs RADIUS
- 1. Gestionnaire central WAAS

1.1 Dans le Gestionnaire central WAAS, crée le serveur RADIUS sous Configure>Security>AAA>RADIUS.

cisco Cisco Wide Area Applicat	tion Services	Home Device Groups	Devices AppNav Clusters Locations Configure ▼ Monitor ▼ Admir	. ▼	avalon Logout Help About
Devices > vCM-POD4-Primary > Configure > Sec RADIUS Server Settings for Cent	urity > AAA > RADIUS ral Manager, vCM-POD	4-Primary 🌍 Print 👔	Apply Defaults 🍵 Remove Settings		
		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 Configurez la méthode d'authentification pour refléter RADIUS sous Configure>Security>AAA>Authentication Methods.

La méthode d'authentification principale est RADIUS et la méthode d'authentification secondaire est locale. Ainsi, en cas de panne RADIUS, le client peut se connecter via un compte local.

CISCO Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations CM-Secondary-WAVE594 Configure Monitor Admin
Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authenti Authentication and Authorization Methods for Centr	cation Methods ral Manager, CM-Seco 🤹 Print 🖉 Apply Defaults 👔 Remove Settings
	Authentication and Authorization Methods
Failover to next available authentication method:	٥
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 📀
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 - Configuration du serveur NPS

2.1 Dans le serveur Windows 2008 R2 - NPS, créez l'adresse IP du périphérique WAAS en tant que client RADIUS.

Policies Network Access Protection Accounting Methods Management	Friendly Name IP Address Device Manufacturer NAP-Capable Status vCM 10.66.86.121 RADIUS Standard No Enabled	
	vCH 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 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: OK Cancel Apply	

2.2 Dans le serveur Windows 2008 R2 - NPS, créez une stratégie réseau correspondant aux périphériques WAAS et autorisez l'authentification.



Dans les travaux pratiques, ces paramètres doivent être sélectionnés sous NPS >Policies>Network Policy.

ICY_WAAS Proper		
erview Conditions	Constraints Settings	
olicy name:	POLICY_WAAS	
Policy State	uates this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
Policy enabled		
Access Permission		
If conditions and co access. What is ac	nstraints of the network policy match the connection request, the policy can either grant a cess permission?	access or deny
Grant access. Gr	int access if the connection request matches this policy.	
C Deny access. De	ny access if the connection request matches this policy.	
🗌 Ignore user acco	int dial-in properties.	
If the connection authorization with	equest matches the conditions and constraints of this network policy and the policy grants acc network policy only; do not evaluate the dial-in properties of user accounts .	cess, perform
Network connection	method	
Select the type of no or Vendor specific, b select Unspecified.	twork access server that sends the connection request to NPS. You can select either the net ut neither is required. If your network access server is an 802.1X authenticating switch or wire	work access server type eless access point,
 Type of network 	access server:	
Unspecified		
C Vendor specific:		
10 *		
		Creat Land
	OK	Cancel App

La condition peut être mise en correspondance avec le nom convivial du client Radius. D'autres méthodes peuvent être utilisées, telles que l'adresse IP.

POLICY_WAAS Properties		×
Overview Conditions Constraint	s Settings	
Configure the conditions for this p	etwork policy	
Conligure the conditions for this fr	etwork policy.	
If conditions match the connectio connection request, NPS skips th	n request, NPS uses this policy to authorize the connection request. If conditions do not match the is policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
Client Friendly Name	vCM	
🐝 Windows Groups	ANS0\WAAS	
o		
Condition description:	where the second s	
The Windows Groups condition s	pecifies that the connecting user or computer must belong to one of the selected groups.	
		nove
	OK Cancel	Applu
		CPPV

Méthodes d'authentification en tant qu'authentification non cryptée (PAP, SPAP).

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: Constraints	Allow access only to those clients that authenticate with the specified methods.
Authentication Methods Joint Session Timeout Called Station ID	EAP types are negotiated between NPS and the client in the order in which they are listed.
Day and time restrictions NAS Port Type	Move Up Move Down
	Add Edit Remove Less secure authentication methods:
	Over 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
	OK Cancel Apply

Service-Type en tant que Administrative.

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

Attribut spécifique au fournisseur en tant que Cisco-AV-Pair (Shell : priv-lvl=15).

POLICY_WAAS Properties		×
Overview Conditions Constraints Settings		
Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the connerse Settings: RADIUS Attributes Image: Constraints Settings: Standard Image: Constraints Image: Vendor Specific Network Access Protection Image: Constraints Image: NAP Enforcement Image: Extended State Routing and Remote Access Image: Routing and Remote Access Image: Allocation Protocol (BAP)	Attributes: Name Vendor Value Cisco-AV-Pair Cisco shell:priv-tvl=15	are applied. lect a Vendor Specific attribute, and it is not sent to RADIUS clients. See ibutes.
IP Filters	Add Edit Remove	
	[OK Cancel Applu
	l	

Autoriser un accès réseau complet.

POLICY_WAAS Properties		×
POLICY_WAAS Properties Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the connel Settings: Settings: RADIUS Attributes Settings: Wendor Specific Network Access Protection NAP Enforcement Settended State Routing and Remote Access Settings Multilink and Bandwidth Allocation Protocol (BAP) IP Filters	 ction request and the policy grants access, settings are applied. 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: <u>7/26/2017</u> Time: <u>12:06:55 AM</u> 	X
 IP Filters Encryption IP Settings 	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. Configure.	
	Auto remediation Enable auto-remediation of client computers Automatically remediate computers that do not meet health requirements defined in this policy.	
-	OK Cancel Apply	

3. Configuration WAAS CM pour les comptes d'utilisateurs RADIUS

Configurez un utilisateur dans RADIUS avec le niveau de privilège 15 ou 1, ne fournit pas l'accès à l'interface utilisateur graphique de WAAS CM. La base de données CMS tient à jour une liste d'utilisateurs, de rôles et de domaines distincts du serveur AAA externe.

Une fois que le serveur AAA externe a été correctement configuré pour authentifier un utilisateur, l'interface utilisateur graphique de CM doit être configurée pour donner à cet utilisateur les rôles et domaines nécessaires pour fonctionner dans l'interface utilisateur graphique de CM.

Si l'utilisateur RADIUS ne se trouve pas dans le CM sous utilisateur, lorsque vous vous connectez à l'interface utilisateur avec cet utilisateur, votre compte ne dispose pas des privilèges d'accès aux pages du Gestionnaire central. Contactez votre administrateur pour en savoir plus sur les rôles et les domaines provisionnés. Ce massage s'affiche.



Configuration du nom d'utilisateur local sous WAAS CM sans mot de passe.

cisco Wide Area Application Services		Home Device Groups	Devices AppNav Clusters	Locations	avalon Logout Help About		
		Dashboard Configure	Monitor Admir	1			
Home > Admin > AAA > Users							
Account Management Role Ma	nagement Domain Management						
Modifying User Accoun	Modifying User Account, 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			
60 admin There are no Domains assigned.							
	Failed Creation on Devices Locked-out of Devices						
This user exists on all devices.	This user exists on all devices. This user is not locked out of any device.						
Comments							

Le nom d'utilisateur doit être lié avec les rôles appropriés sous Gestion des rôles pour chaque utilisateur.

$\bullet \bullet \bullet \checkmark \square$		€ 10.66.86.121	Ċ
cisco Cisco Wide Ar	ea Application Services	Home Device Groups Devices AppNav Cli Dashboard Configure Monitor	Admin 🔻
Home > Admin > AAA > Users	Domain Management		
Refresh Table	gn all Roles 😰 Remove all Roles		
Roles			Ite
Filter: Name O Mate	ch if: contains	Go Clear Filter	
	Role		Comments
🗱 60 L2			
A admin		Admin role	

Si l'utilisateur a besoin d'un accès en lecture seule ou d'un accès limité, vous pouvez le configurer sous rôles.

	€ 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	
Mourrying Kore, 22 Denote Strant	
	Role Definition
Name:* L2	
Enabled Services:	
	Comments

Vérification

Dans les périphériques WAAS, cette configuration est diffusée.

```
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 basculement de l'authentification serveur inaccessible

Certaines commandes d'affichage (« show ») sont offertes par l'outil « Cisco CLI Analyzer » réservé aux clients inscrits. Utilisez cet outil pour obtenir une analyse des rapports produits par ces commandes.

• authentication - Configurer l'authentification

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- · Vérifiez les journaux de domaine Windows
- #debug aaa authorization from WAAS CM CLI

Informations connexes

- <u>Configuration des paramètres d'authentification du serveur RADIUS sur WAAS</u>
- Network Policy Server s'applique à Windows Server 2008

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.