Exemple de configuration de l'intégration ACS version 5.x avec WAAS

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Configurer ACS Configuration sur le WAAS Vérifier Dépannage

Introduction

Ce document décrit comment configurer l'intégration de Cisco Wide Area Application Services (WAAS) avec Cisco Access Control Server (ACS) Version 5.x . Lorsqu'ils sont configurés conformément aux étapes de ce document, les utilisateurs peuvent s'authentifier auprès de WAAS avec des informations d'identification TACACS+ via ACS.

Conditions préalables

Exigences

There are no specific requirements for this document.

Composants utilisés

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

- Cisco Secure ACS version 5.x
- Cisco WAAS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Configurer ACS

 Afin de définir un client AAA sur ACS Version 5.x, naviguez à Ressources réseau > Périphériques réseau et clients AAA. Configurez le client AAA avec un nom descriptif, une adresse IP unique et une clé secrète partagée pour TACACS+.

+ 😚 My Workspace	Network Resources > Netw	ork Devices and AAA Clients > Create		
Network Resources Network Device Groups Location Device Type	o Name: WAA: Description: test / Network Device Grou	S AA dient Ips		
Default Network Device External Proxy Servers OCSP Services	Location Device Type	All Locations All Device Types	Select Select	
Busers and identity Stores Solution Policy Elements	IP Address	ress 🔿 IP Subrets 🔿 IP Rance(s)		Authentication Options TACACS+
Carlos Policies Monitoring and Reports	• IP: 1.1.1.1			Shared Secret disco Hide
 System Administration 				Egacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support RADIUS
				Shared Secret Show Show CoAport 1700 Enable KeyWrap Key Encryption Key: Message Authenticator Code Key: Key Input Format ASCII © HEXADECIMAL

2. Afin de définir un profil Shell, naviguez vers Éléments de stratégie > Autorisations et autorisations > Administration de périphérique > Profils Shell. Dans cet exemple, un nouveau profil shell appelé WAAS_Attribute est configuré. Cet attribut personnalisé est envoyé au WAAS, ce qui lui permet de déduire quel groupe d'utilisateurs est le groupe d'administrateurs. Configurez ces attributs personnalisés :

L'attribut est waas_rbac_groups.La configuration requise est facultative afin qu'elle ne perturbe aucun autre périphérique.La valeur est le nom du groupe auquel un accès administratif doit être attribué (Groupe de

test).				
+ 🖓 My Workspace	Policy Elements > Authoriza	tion and Permissions > Device Ad	ninistration > Shell Profiles > Edit: "WAAS_Attri	bute"
By Network Resources By Users and Identity Stores	General Commo	n Tasks Custom Attributes		
Policy Elements	Common Tasks Attri	butes		
Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access Device Administration Shell Profiles Organization	Aftribute Manually Entered	Regultement	Value	·
Named Permission Objects	Attribute	Requirement	Value	
Access Policies	waas_rbac_groups	Optional	Test_Group	÷
Image: System Administration				
				-
	Add A Edi	tV Replace A Delete	Bulk Edit	

3. Afin de définir un jeu de commandes pour autoriser toutes les commandes, naviguez vers Policy Elements > Authorization and Permissions > Device Administration > Command Sets. Modifiez le jeu de commandes Permit_All.Si vous cochez la case Autoriser une commande qui ne figure pas dans le tableau ci-dessous, l'utilisateur bénéficie de privilèges complets.

► 💮 My Workspace	Policy Elements > Aut	horization and Permissions > D	evice Administration	> Command Sets > Edit: "permital"		
A) Network Resources	General					
Users and Identity Stores						
+ 🥱 Policy Elements	Name:	Permit_All				
	Description:					
Date and Time						
Custom	2 Permit source	ommand that is not in the to	ble below			
 Network Conditions Authorization and Resminsterio 						
Network Access	Grant	Command	4	Arguments		
 Device Administration 					~	
Shell Profiles						
Command Sets						
 Named Permission Objects 						$ \ge $
Access Policies						<u> </u>
Monitoring and Reports						$[$ \ge $]$
🔸 🍓 System Administration						
					-	
	Add A	Edit V Replace A	Delete			

Remarque : comme cet exemple utilise TACACS, le service par défaut sélectionné est **default device admin**.

4. Afin de pointer l'identité vers la source d'identité correcte, naviguez vers Access Policies > Access Services > Default Device Admin > Identity. Si l'utilisateur existe dans la base de données ACS locale, sélectionnez Internal Users. Si l'utilisateur existe dans Active Directory, sélectionnez le magasin d'identités configuré (AD1 dans cet exemple).

My Workspace My Workspace Morkspace Users and Identity Stores Policy Elements	Access Policies > Access Services > Default Device Admin > Identity Single result selection Identity Source: Internal Users Select
Access Policies Access Services Service Selection Rules	Cisco Secure ACS - Mozilla Firefox
O Default Device Admin Identity Authorization O Default Network Access Identity	Filter: Match if: Go Name Description Co Co
Authorization V EAP access Identity Authorization	AD1 CN Username Predefined Certificate Authentication Profile DenyAccess
Max User Session Policy Monitoring and Reports	Internal Hosts Internal Users
 System Administration 	IN Page 1 of 1 P Page 1 Page 1 of 1 P Page 1

5. Afin de créer une règle d'autorisation, naviguez vers Access Policies > Access Services >

Default Device Admin > Authorization. Créez une nouvelle stratégie d'autorisation appelée **Autorisation WAAS**. Cette commande recherche les requêtes de WAAS. Dans cet exemple, l'adresse IP du périphérique est utilisée comme condition. Toutefois, cette configuration peut être modifiée en fonction des exigences de déploiement. Appliquez le profil de shell et les jeux de commandes configurés aux étapes 2 et 3 de cette section.

🔸 💮 My Workspace	Access Policies > Access Services > Default Device Admin > Authorization
→ 30 Network Resources	Standard Policy F
Users and identity Stores	Device Administra 102 168 26 52 https://102 168 26 52/accadmin/PoliceInputAction.do
Policy Elements	
🔹 🏭 Access Policies	Filter: Status
★ Access Services E Service Selection Rules	Statu Statu Name: Waas Authorization Status: Enabled - O
O Default Device Admin	Noda
Authorization • O Default Network Access	The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.
Identity	Conditions
✓ ZA EAP access	NDG:Location: -ANY-
Identity	NDG:Device Type: -ANV-
Authorization Max User Session Policy	Device IP Address: = + 1.1.1.1
Monitoring and Reports	Results
 Restern Administration 	Shell Profile: V/AAS_Athibute Select
	PermLAI *
	Create • Duplicate • Edt Delete A Nove to

Configuration sur le WAAS

 Afin de définir un serveur TACACS+, naviguez vers Devices > <Central Manager System Name> > Configure > Security > AAA > TACACS+. Configurez l'adresse IP du serveur ACS et la clé pré-partagée.

	TAPAPS: Server Settions				
		1050	Con server senargs		
Jse ASCII Password Authentication:	×.				
ime to Welt."	5	(seconds) (1-20)			
kanber of Retransmits.*	2 (1-3)				
iecurity Word:					
rimary Server.			Primary Server Port	49	
econdary Server:	<u> </u>		Secondary Server Port	49	
fertiary Server:			Tertiary Server Port		

2. Afin de modifier les méthodes d'authentification et d'autorisation, accédez à Devices > <Central Manager System Name> > Configure > Security > AAA > Authentication Methods. Dans cette capture d'écran, la méthode de connexion principale est configurée pour local et la méthode secondaire est configurée pour TACACS+.

Authentication and Authorization Methods	for Central Manager, pi-wave	S Print	Apply Defaults	Remove Settings
	Authentie	cation and	Authorization Metho	ds
Failover to next available authentication method:	V			
Authentication Login Methods:	V		i It is highly recor	nmended to set the autho
Primary Login Method:*	local			
Secondary Login Method:	TACACS+			
Tertiary Login Method:	Do Not Set			
Guaternary Login Method:	Do Not Set			
Authorization Methodis:	V			
Primary Configuration Method:*	local			
Secondary Configuration Method:	TACACS+			
Tertiary Configuration Method:	Do Not Set			
Quaternary Configuration Method:	Do Not Set			

3. Accédez à **Home > Admin > AAA > User Groups** afin d'ajouter le nom de groupe qui correspond à l'attribut personnalisé **Value** (voir l'étape 2 dans la section **Configure ACS**) dans WAAS.

Home > Admin > AAA > User Groups		
Creating New User Group 🗳 Print		
		User Group Information
Name:*	Test_Group]
		Comments
Group name matching a Shell profile on A	cs //	
Note: * - Required Field		

 4. Attribuez ce groupe (Test_Group) aux droits de niveau admin dans l'onglet Accueil > Admin > AAA > Gestion des rôles des groupes d'utilisateurs. Le rôle admin sur le Gestionnaire central est préconfiguré.

External User Group Management	Role Management	Domain Management	
🔞 Refresh Table 🛛 🥶 Assign al	l Roles 🛛 😰 Remov	e all Roles	
Roles			
Filter: Name 💌 Match if	like 💌		Go Clear Filter
	Role		
🔿 😂 admin			Admin role

Vérifier

Tentative de connexion à WAAS avec les informations d'identification TACACS+. Si tout est configuré correctement, vous disposez d'un droit d'accès.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

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.