配置Windows 2008 NPS伺服器的RADIUS - WAAS AAA

目錄

簡介 必要條件 需求 採用元件 配置步驟 1. WAAS中央管理器 2. Windows 2008 R2 -NPS伺服器配置 3.為RADIUS使用者帳戶配置WAAS CM 驗證 疑難排解 相關資訊

簡介

本檔案介紹在Cisco廣域應用程式服務(WAAS)和Windows 2008 R2網路原則伺服器(NPS)上設定遠 端驗證撥入使用者服務(RADIUS)的程式。

預設WAAS配置使用本地身份驗證。Cisco WAAS還支援RADIUS和終端訪問控制器訪問控制系統 (TACACS+)進行身份驗證、授權和記帳(AAA)。 本文檔僅介紹一台裝置的配置。但是,這也可以在 裝置組下完成。所有配置必須通過WAAS CM GUI應用。

一般WAAS AAA配置在<u>Cisco廣域應用服務配置指南</u>配置管理登入身份驗證、授權和記帳一章下提 供。

作者:Hamilan Gnanabaskaran,思科TAC工程師。

由Cisco TAC工程師Sanaz Tayyar編輯。

必要條件

需求

思科建議您瞭解以下主題:

- WAAS 5.x或6.x
- Windows NPS伺服器
- AAA RADIUS

採用元件

本文中的資訊係根據以下軟體和硬體版本:

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從預設組態來啟動 。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

相關產品

本檔案也適用於以下硬體和軟體版本:

- vWAAS、ISR-WAAS和所有WAAS裝置
- WAAS 5.x或WAAS 6.x
- •WAAS作為應用程式加速器的中央管理器

附註:APPNAV-XE不支援此配置。路由器AAA將配置推送到APPNAV-XE。

配置步驟

需要應用以下配置:

- 1. WAAS中央管理器
- 1.1 AAA RADIUS配置
- 1.2 AAA身份驗證配置
- 2. Windows 2008 R2 NPS伺服器配置 2.1 RADIUS客戶端配置 2.2網路策略配置

3.為RADIUS使用者帳戶配置WAAS CM

1. WAAS中央管理器

1.1在WAAS Central manager中,在Configure>Security>AAA>RADIUS下建立RADIUS伺服器。

داندان داندو Cisco Wide Area Applicat	tion Services	Home	Device Groups	Devices AppNa	v Clusters Locat	ions	avalon Logout Help About
Devices Nuclid DOD4 Primary N Configure N Ser		VCM-PC	0D4-Primary	Configure	Monitor V	Admin 🔻	
PADULS Server Settings for Cent		POD4-Primary	Print	2 Anoly Defaults	TRAMOVA Setti	0.05	
KADIOS SEIVEI SELLINGS TOI CEIL	Tal Mallager, VCM-		V	A Apply Dolution			
			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下配置身份驗證方法以反映RADIUS。

選擇主要身份驗證方法作為RADIUS,選擇輔助身份驗證方法作為本地。因此,發生RADIUS故障時 ,客戶可透過本機帳戶登入。

CISCO Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations CM-Secondary-WAVE594 v Configure v Monitor v Admin v
Authentication and Authorization Methods for Central N	Manager, CM-Seco SPrint Z ^a Apply Defaults 1 Remove Settings
	Authentication and Authorization Methods
Failover to next available authentication method:	
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:	
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伺服器配置

2.1在Windows 2008 R2 - NPS伺服器中,建立WAAS裝置IP作為RADIUS客戶端。

NPS (Local)	RADIUS Clients
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.
3 Setwork Access Protection	Friendly Name IP Address Device Manufacturer NAP-Capable Status
Accounting	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 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 C Generate
	Shared secret:
	••••••
	Confirm shared secret:
	•••••
	OK Cancel Apply

2.2在Windows 2008 R2 - NPS伺服器中,建立與WAAS裝置匹配的網路策略並允許身份驗證。

Network Policy Server							
File Action View Help							
(=							
NPS (Local)	Network Policies						
RADIUS Clients and Servers							
RADIUS Clients	Network policies allow yo	u to designate who is authorized to	o connect t	to the network and t	he circumstance	s under which the	ey can or cannot connect.
Remote RADIUS Server G							
Polices							1
Connection Request Polici	Policy Name		Status	Processing Order	Access Type	Source	
Westwork Policies	POLICY_WAAS		Enabled	1	Grant Access	Unspecified	
Realth Polices	Connections to Microsoft Hout	ng and Hemote Access server	Enabled	333338	Deny Access	Unspecified	
System Health Validators	Connections to other access s	ervers	Enabled	999999	Deny Access	Unspecified	
Remediation Server Group							
Accounting							
Templates Management							
			_				
	POLICY_WAAS						
	Conditions - If the following cond	ditions are met:					
	Condition						
	Cleat Eleady Name VCM						
	Wedawa Grauna ANS/01	MAAS					
	Windows Groups ANSON	NA63					
	1						
	Settings - Then the following set	ttings are applied:					
	Come	Makia					
	Cieco AV Pair	value shall not y hd=15					
	Extended Sinte	Allenks					
	Access Participa	Const Assess					
	A theotication Method	Linencented a theotication /DAD	CDAD)				
	NAP Enforcement	Allow full estimate accessor	, SPAP)				
	Lindate Naccompliant Classic	Taue					
	Section Time	Administration					
	BAR Respectance of Canacity	Partice Middle frequences and	50% fee 2	minu data			
	over Percentage or Capacity	neudce mutanik if server reaches	5 30 % for 2	ina luces			
	4						

在實驗室中,必須在NPS >Policies>Network Policy下選擇這些引數。

rerview Conditions Constraints Settings olicy name: FOLCY_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? G Grant access. Grant access of the connection request matches this policy. Deny access. Deny access if the connection request 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 contraints 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: Vhapeofied. G Type of network access server: Unspecified G Vendor specific: 10		
olicy name: FOLCY_WAAS Policy State if enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy. If enabled 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? 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? If and access. Grant access if the connection request matches this policy. In provide the connection request matches this policy. In provide the connection request matches this policy. Ingore user account dial in properties. If the connection nequest 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 is an 802.1X authenticating switch or wireless access point, select Unspecified. Image: Type of network access server: Unspecified Unspecified Image: Type of network access server: Unspecified Image: Type of network access server: Unspecified Image: Type of net	straints Settings	
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. <u>What is access permission?</u> Grant access. Grant access if the connection request matches this policy. Dery 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 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: Unspecified Vendor specific: 10 Vendor specific:	POLICY_WAAS	
Policy State		
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? If 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 point, select Unspecified. Type of network access server: Unspecified Vendor specific: Image: Content in the image of the server is an 802.1X authenticating switch or wireless access point, select Unspecified. Or work access server: Unspecified Or work access server:	this policy while performing authorization. If disabled, NPS does not evaluate this policy.	
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 to r Vendor specified. Type of network access server: Unspecified Vendor specific: To		
 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 is an 802.1X authenticating switch or wireless access point, select Unspecified. Type of network access server: Unspecified Vendor specific: Image: 	ints of the network policy match the connection request, the policy can either grant access or deny permission?	,
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 to r 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	cess if the connection request matches this policy. cess if the connection request matches this policy.	
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 to 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	lin properties.	
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 is 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 2	t matches the conditions and constraints of this network policy and the policy grants access, perform rk policy only; do not evaluate the dial-in properties of user accounts .	
Select the type of network access server that sends the connection request to NPS. You can select either the network access server 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 2 0 0 0 0 0 0 0 0 0 0 0 0	od	
Type of network access server: Unspecified Vendor specific: 10 10	access server that sends the connection request to NPS. You can select either the network access set ther is required. If your network access server is an 802.1X authenticating switch or wireless access po	erver type bint,
Vendor specific:	ss server:	
		
	OK Carcel	Ann

條件可以與Radius使用者端友好名稱相匹配。也可以使用其它方法,例如IP地址。

POLICY_W	AAS Propertie	25	×
Overview	Conditions C	Constraints Settings	
Continue	n the conditions f	for this network policy	
Conligun	e the conditions i	for this network policy.	
lf conditi connecti	ions match the co ion request. NPS	onnection request, NPS uses this policy to authorize the connection request. If conditions do not match the S skips this policy and evaluates other policies, if additional policies are configured.	
		· · · · · · · · · · · · · · · · · · ·	
	odition	Value	
	ent Friendly Nam		
	indows Groups		
	indows circups		
Condition	n description:		
The Win	ndows Groups co	ndition specifies that the connecting user or computer must belong to one of the selected groups.	
		Add Eda Dom	
		OK Cancel	Apply

驗證方法為非加密驗證(PAP、SPAP)。

POLICY_WAAS Properties	×
Overview Conditions Constraints Setting	ja j
Configure the constraints for this network po If all constraints are not matched by the con Constraints:	licy. nection request, network access is denied.
Constraints Authentication Methods	Allow access only to those clients that authenticate with the specified methods.
5 Idle Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:
Called Station ID Called Station ID Day and time restrictions NAS Port Tupo	Move Up Move Down
A MAS FOIL Type	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
	Perform machine health check only
	OK Cancel Apply

Service-Type(管理)。

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

Cisco-AV-Pair形式的供應商特定屬性(Shell:priv-lvl=15)。

POLICY_WAAS Properties		×
Overview Conditions Constraints Setting	35	
Configure the settings for this network policy If conditions and constraints match the conn Settings: BADIUS Attributes	ection 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.	
S 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 All Encryption		
💑 IP Settings		
	Add Edit Remove	
	OK Cancel Apply	

允許完全網路訪問。

POLICY_WAAS Properties	×
POLICY_WAAS Properties Overview Conditions Constraints Settings Configure the settings for this network policy. If conditions and constraints match the connerse Settings: Settings: RADIUS Attributes Standard	s ection request and the policy grants access, settings are applied. Specify whether you want to enforce Network Access Protection for this policy.
Vendor Specific Network Access Protection	 Allow full network access Allows unrestricted network access for clients when the connection request matches the policy. Use this option for reporting mode.
Image: NAP Enforcement Image: Extended State Routing and Remote Access Image: Extended State Image: Extended State	 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 Finable auto-remediation of client computers Automatically remediate computers that do not meet health requirements defined in this policy.
	OK Cancel Apply

3.為RADIUS使用者帳戶配置WAAS CM

在RADIUS中為使用者配置許可權級別15或1,不提供對WAAS CM GUI的訪問。CMS資料庫維護獨 立於外部AAA伺服器的使用者、角色和域清單。

在對外部AAA伺服器進行正確配置以驗證使用者之後,必須配置CM GUI,以便為使用者在CM GUI中工作提供必要的角色和域。

如果RADIUS使用者不在CM under user下,則使用該使用者登入GUI時,您的帳戶沒有訪問任何 Central Manager頁面的許可權。請向您的管理員諮詢已設定的角色和域。將顯示此消息。

👬 WAAS Central Manager	× +) 🗙
🗲 🛈 🛍 https://10.66.86.17	1:8443/home.jsp?context=Global	C Q. Search	☆自	∔		≡
cisco Cisco Wide Are	a Application Services			ava	kon L	ogout
Your account does not	have privileges to access any of the Centr	ral Manager pages. Please check with you	r administrator al	oout pro	vision	ed
Tores and domains.						

在WAAS CM下配置本地使用者名稱,無需密碼。

(1)(1) CISCO Cisco Wide Area Application Services		Hama Davies Course 1	- Analise Chattan	Laurian	avalon Logout Help About			
		Porthand Configure	Aevices Appivav Clusters	Locations				
Home & Admin & AMA & House		Dashboard Configure	Monitor Admir	1				
Account Management Role Man	nagement Domain Management							
Modifying User Account	t, avalon 📋 Delete 🤮 Print							
Account Information								
Usemame:*	Usemame:* avaion							
WAE Device Manager User:			Device Manager Access:	Read Only 0				
Local User:	0		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 is not locked out of any device.					
Comments								

對於每個使用者,使用者名稱必須與角色管理下的正確角色繫結。

	10.66.86.121	Ċ
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		Ite
Filter: Name Match if: contains	Go Clear Filter	
Role		Comments
¥ 6∂ L2		
A admin	Admin role	

如果使用者需要具有只讀訪問許可權或受限訪問許可權,可以在角色下配置該許可權。

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



在WAAS裝置中推送此配置。

radius-server key **** radius-server host 10.66.86.125 auth-port 1645 ! authentication login local enable secondary 驗證登入radius enable primary

身份驗證配置local enable secondary

身份驗證配置radius enable primary

<u>Cisco CLI Analyzer(僅供已註冊客戶使用)支援某些</u> **show 指令。**使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

• authentication — 配置身份驗證

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

- 檢查Windows域日誌
- #debug aaa authorization from WAAS CM CLI

相關資訊

- 在WAAS上配置RADIUS伺服器身份驗證設定
- 網路策略伺服器適用於Windows Server 2008