نيوكت Windows 2008 NPS -WAAS AAA

تايوتحملا

<u>قمدق ملا</u> <u>قمدق ملا</u> <u>قمدخت سملا تاب طتملا</u> <u>تاب طتملا</u> <u>تاب طتملا</u> <u>تاب طتملا</u> <u>قمدخت سملاً تانوكملاً</u> <u>مداخلاً تانوكت الملح</u> <u>مداخلاً تيوكت الملح</u> <u>مداخلاً تيوكت الملح</u> <u>قم حت الملح</u> <u>قم حت الملح</u> <u>مداخالاً فاشكت سا</u>

ةمدقملا

(RADIUS) ديعبلا مدختسملا لاصتا بلط ةقداصم ةمدخ نيوكت ءارجإ دنتسملا اذه فصي و Cisco Wide Area Application Services (WAAS) و Windows 2008 R2 Network Policy Server (NPS).

مكحتلا ماظن Cisco WAAS معدي .ةيلحملا ةقداصملا يضارتفالا WAAS نيوكت مدختسي ةقداصملل اضيأ (+TACACS) ةيفرطلا ةطحملا ىلإ لوصولا مكحت ةدحو ىلإ لوصولا يف نكمي ،كلذ عمو .طقف دحاو زاهج نيوكت دنتسملا اذه يطغي .(AAA) ةبساحملاو ضيوفتلاو مدختسملا ةهجاو ربع نيوكتلا عيمج قيبطت بجي .ةزهجألا ةعومجم نمض اضيأ كلذب مايقلا قيموسرلا

<u>نم ةعساولا تاقىبطتلا تامدخ نىوكت لىلد</u> يف WAAS AAA ماعلا نىيوكتلا ريفوت متي ماعلا نيوكتلا ريفوت متي <u>Cisco</u> قراد المخدلا ليجست ققداصم نيوكت لصفلا نمض.

Cisco TAC. سدنهم ،ناراكسابانغ ناليماه لمعلا اذه يف مهاس

.Cisco نم TAC سدنهم ،رايط زناس اهريرحتب ماق

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- WAAS 5.x وأ 6.x
- Windows NPS مداخ •
- AAA RADIUS

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست:

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

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. ديق كتكبش تناك اذإ .يضارتفا نيوكتب دنتسملا اذه يف ةمدختسملا قزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا.

ةلصلا تاذ تاجتنملا

:ةغيص ةيجمربو زاهج اذه عم ةقيثو اذه قيبطت اضيأ نكمي

- WAAS ةزهجأ عيمجو ISR-WAAS و •
- WAAS 5.x وأ WAAS 6.x
- قيبطت عرسم ،يزكرم ريدمك WAAS •

ىلإ نيوكتلا عفدب AAA ەجوملا موقي .نيوكتلا اذە APPNAV-XE معدي ال :**ةظحال م** APPNAV-XE.

نيوكتلا تاوطخ

:يلاتلا نيوكتلا قيبطت مزلي

- ةكرشل يزكرملا ريدملا 1 WAAS ةكرشل يزكرمل AAA RADIUS 1.1 نيوكت 1.2 AAA
- 2. ليغشتلا ماظن ربع مداخلا ةئيەت Windows 2008 R2 ليغشتلا ماظن .2 1.2 ءالمع نيوكت 2.1 RADIUS 2.2 ةكبشلا جەن نيوكت
- RADIUS يمدختسم تاباسحل WAAS CM نيوكت .3

WAAS ةكرشل يزكرملا ريدملا - 1

.AAA>RADIUS مداخ قلخي يزكرملا WAAS ريدم يف 1.1 مداخ قلخي يزكرمل AAA>RADIUS ريدم يف

cisco Wide Area Applica	tion Services	Home Devic	ce Groups De Primary 🔻	vices AppNav	Clusters Locatio	ons Admin ∣ ▼	avalon Logout Help About
Devices > vCM-POD4-Primary > Configure > Sec	urity > AAA > RADIUS				1		
RADIUS Server Settings for Cent	ral Manager, vCM-P	OD4-Primary	Print 🎢	Apply Defaults	Remove Setting	js	
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							

العرب مق 1.2 قرط<AAA<טוחألا<טפטיי הישט אין אפטיי א **ו ה פטרוס ארו**.

رايتخإ متيو RADIUS ةقداصم بولسأ هرابتعاب يساسألا ةقداصملا بولسأ رايتخإ متيو ليمعل نكمي ،RADIUS لشف ةلاح يف ،كلذل .يلحم بولسأك ةيوناثلا ةقداصملا بولسأ يلحم باسح ربع لوخدلا ليجست.

ululu CISCO Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Locations
Devices > CM-Secondary-WAVE594 > Configure > Security > AAA > Authent	consecundary-wavesse v consigure v Monitor v Aurinit v
Authentication and Authorization Methods for Cent	ral Manager, CM-Seco 🤪 Print 🎤 Apply Defaults 📋 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. مداخلا نيوكت Windows 2008 R2 -NPS

.RADIUS ليمعك WAAS زاهجل IP ءاشنإب مق ،NPS مداخ - Windows 2008 R2 يف 2.1

NPS (Local)	RADIUS Clients	
RADIUS Clients and Servers	RADIUS clients allow you to specify the network access servers, that provide access to your network.	
Remote RADIUS Server G		
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:	
	JVCM	
	Address (IP or DNS):	
	10.66.86.121 Venty	
	Shared Secret	
	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	
	Confirm shared secret:	
	OK Cancel Apply	

يف 2.2 Windows 2008 R2 - هداخ مق Windows 2008 R2 يف Windows قزهجأ ةقباطمل ةكبش ةسايس ءاشنإب مق Windows مداخ ةقداصملاب حامسلاو.

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	connect t	to the network and t	he circumstance	s under which the	ey can or cannot connect.
Remote RADIUS Server G							
Connection Request Polici	Polices						1
Network Policies	Policy Name		Status	Processing Order	Access Type	Source	
Health Policies	POLICY_WAAS		Enabled	1	Grant Access	Unspecified	
Network Access Protection	Connections to Microsoft Hout	ng and Hemote Access server	Enabled	333339	Deny Access	Unspecified	
System Health Validators	Connections to other access s	civeis	Enabled	333333	Deny Access	Unspecified	
Remediation Server Group							
Accounting							
🖭 🜉 Templates Management							
			_				
	POLICY_WAAS						
	Conditions - If the following con	ditions are met:					
	Condition Value						
	Client Friendly Name vCM						
	Windows Groups ANSO\\	NAAS					
	1						
	Settings - Then the following set	tings are applied:					
	Setting	Value					
	Cisco-AV-Pair	shell:priv-lvl=15					
	Extended State	<blank></blank>					
	Access Permission	Grant Access					
	Authentication Method	Unencrypted authentication (PAP	, SPAP)				
	NAP Enforcement	Allow full network access	-				
	Update Noncompliant Clients	True					
	Service-Type	Administrative					
	BAP Percentage of Capacity	Reduce Multilink if server reaches	50% for 2	minutes			

.**ةكبشلا جەن<تاسايسلا< NPS** نمض تاملعملا ەذە دىدحت بجي لمعملا يف

LICY_WAAS Proper	ties						
verview Conditions	Constraints Setting	s					
Policy name:	POLICY_WAAS						
Policy State	luates this policy while	performing authorizatio	n. If disabled, NPS do	oes not eva	luate this poli	cy.	
Policy enabled							
Access Permission If conditions and co access. What is ac	onstraints of the netwo cess permission?	ork policy match the c	onnection request, th	ne policy ca	n either gran	t access or deny	/
 Grant access. Gr Deny access. De 	ant access if the conn	ection request matches ection request matches	this policy. this policy.				
Ignore user acco	unt dial-in properties.						
If the connection authorization with	equest matches the c network policy only; d	onditions and constrain o not evaluate the dial-i	ts of this network polic n properties of user ac	icy and the p iccounts .	oolicy grants a	access, perform	
Network connection	method						
Select the type of ne or Vendor specific, b select Unspecified.	twork access server t ut neither is required.	hat sends the connecti If your network access	on request to NPS. Yo server is an 802.1X a	'ou can sele authenticatir	ct either the r ng switch or v	network access so vireless access po	erver type pint,
• Type of network	access server:						
Unspecified		•					
O Vendor specific:							
10 +							
					ок	Cancel	Applu

تنك عيطتسي ةقيرط رخآ .RADIUS ليمعل فولأملا مسالا عم طرشلا قباطت نكمي .ناونع لـثم تـلمعتسا

POLICY_WA	AAS Properties		×
Overview	Conditions Constra	aints Settings	
Cartan			
Configure	the conditions for this	s network policy.	
If conditio	ons match the connect on request NPS skips	ction request, NPS uses this policy to authorize the connection request. If conditions do not match the s this policy and evaluates other policies, if additional policies are configured.	
Connocat	intequeer, ni e erape		
	- Int	Mala	_
	ndition	Value	_
El Clie	nt Friendly Name	VCM	
🔰 🗰 Win	ndows Groups	ANS0\WAAS	
Condition	description:		
The Wind	lowe Groupe condition	a propriet that the connecting upper or computer must belong to one of the selected groups	
The wind	lows Groups condition	n specilies that the connecting user of computer must belong to one of the selected groups.	
			_
		Add Edit Hemove	
			_
		OK Cancel Ar	oply

.(PAP، SPAP) ةرفشم ريغ ةقداصمك ةقداصملا بيلاسأ

POLICY_WAAS Properties	×
Overview Conditions Constraints Setting	s
Configure the constraints for this network po If all constraints are not matched by the con	icy. nection request, network access is denied.
Constraints:	
Authentication Methods	Allow access only to those clients that authenticate with the specified methods.
Idle Timeout	EAP types are negotiated between NPS and the client in the order in which they are listed.
Called Station ID	EAP Types:
Called Station 10	Move Up
Day and time restrictions	Move Down
MAS Port Type	
	Add Edit Remove
	Less secure authentication methods:
	Incrosoft Encrypted Authentication Version 2 (MS-CHAP-V2) Iser 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

يرادإك ةمدخلا عون.

POLICY_WAAS Properties	E E E E E E E E E E E E E E E E E E E
Overview Conditions Constraints Setting	s
Configure the settings for this network policy. If conditions and constraints match the connection Settings: RADIUS Attributes	ection 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 Remote Access IP Settings	Add Edit Remove
	OK Cancel Apply

ك دروملاب صاخ ةمس Cisco-AV-PAIR (Shell:priv-lvl=15).

POLICY_WAAS Properties		×
Overview Conditions Constraints Setting	3	
Configure the settings for this network policy If conditions and constraints match the conn 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:	
j፼ 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 IP Settings		
	Add Edit Remove	
	OK Cancel Apply	

ةكبشلا ىلإ لماكلا لوصولاب حامسلا.



RADIUS يمدختسم تاباسحل WAAS CM نيوكت .3

يف لمعتسم تلكش WAAS CM GUI. ىلإ لوصولاا دوزي ال ،1 وأ 15 ىوتسم زايتما عم RADIUS يف لمعتسم تلكش AAA مداخ نع ةلصفنملا تالاجملاو راودألاو نيمدختسملا ةمئاقب CMS تانايب ةدعاق ظفتحت يچراخلا.

مداخ نيوكت دعب مدختسم ةقداصمل حيحص لكشب يجراخلا AAA مداخ نيوكت دعب قيرورضلا تالاجملاو راودألا مدختسملا كلذ حنمل CM ب ةصاخلا (GUI) ةيموسرلا مدختسملا ميموسرلا مدختسما مدختسما (CM) قيموسرلا مدختسما القيا مداف المعال

لا سيل نا RADIUS لا مون ترك ال CM لا يف لمعتسم GUI كا سيل نا OT لا عن ال المعتسم GUI كا ال عم كلذ نم ققحتلا عاجرلا .ةحفص ريدملا نم يأ ذفني نأ تازايتما كباسح ىقلتي ال كيلدتلا اذه ضرع متي .ةدوزملا تاقاطنلاو راودالا لوح لوؤسملا.

wAAS Central Manager ×	+						×
(Inttps://10.66.86.121:844	3/home.jsp?context=Global	C Q Search	☆自	÷	A		≡
սիսիս cisco Cisco Wide Area Ap	plication Services				avalon	Log	out
Your account does not have	privileges to access any of the Central N	Manager pages. Please check with you	r administrator a	ibout	provis	ioned	
roles and domains.							
							- 10

رورم ةملك نودب WAAS CM تحت يلحملا مدختسملا مسا نيوكت.

Home > Admin > AAA > Users Account Management Role Ma	Pa Application Services	Home Device Groups D Dashboard Configure	Pevices AppNav Clusters Locat Monitor Admin	tions	avalon Logout Help About	
Usemame:* avaion						
WAE Device Manager User:	0		Device Manager Access:	Read Only 0		
Local User:			CLI Privilege Level:	0 (normal user) 0		
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.		Con	This user is not locked out of any de	evice.		

مدختسم لكل راودألا ةرادإ نمض ةحيحصلا راودألاب مدختسملا مسا طبتري نأ بجي.

	€ 10.66.86.121	Ċ
CISCO Cisco Wide Area Application Services	Home Device Groups Devices AppNav Clusters Dashboard Configure Monitor Admin	Locations
Home > Admin > AAA > Users		
Account Management Role Management Domain Management		
🔞 Refresh Table 🛛 🗃 Assign all Roles 👩 Remove all Roles		
Roles		Ite
Filter: Name O Match if: contains O	Go Clear Filter	
Role		Comments
# 60 L2		
S & admin	Admin role	

نمض اذه نيوكت نكمي ،دودحم لوصو وأ طقف ةءارقلل لوصو ىلإ ةجاحب مدختسملا ناك اذا راودأ.

	€ 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 The Delete Print	
	Role Definition
Name:* L2	
Enabled Services:	
	Comments

ققحتلا

نيوكتلا اذه عفد متي ،WAAS ةزهجأ يف.

```
مداخ حاتفم مداخ حاتفم مداخ حاتفم AADIUS 10.66.86.125 ذفنم 1645 ذفنم 1645 المداخ فيضم مداخ فيضم
!
ايلحم ةقداصملا لوخد ليجستل يوناث نيكمت
يساسألا لوخدلا ليجست رطق فصن نيكمت نم ققحتلا
يوناثلا ةقداصملل يلحملا نيوكتلا نيكمت
```

يساسألا نكمي ةقداصملا نيوكت عاعش ميلإ لوصولا رذعتي يذلا-مداخلا ربع ةقداصملا لشف

ر<u>ماوأ (طقف نيلجسملا</u> <u>ءالمعلل) (Cisco CLI Analyzer نم رماوأل رطس ةمجاو للحم) Cisco CLI Analyzer</u> معدي show مدختسا **.قنيعم** Cisco CLI Analyzer (ليلحم) نم رماوأل رطس قمجاو للحم) دفت في مع رمألا جَرخُمل show.

ةقداصملا نيوكت -**ةقداصملا •**

اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي.

- Windows لاجم تالجس نم ققحت •
- #debug aaa نم ليوختلا WAAS CM CLI

ةلص تاذ تامولعم

- <u>WAAS ىلع RADIUS مداخ ةقداصم تادادعاٍ نيوكت</u> •
- <u>Windows Server 2008 ىلع ةكبشلا جەن مداخ قىيبطت متى</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما