Management Access for Aire OS WLC via Microsoft NPS

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Achtergrondinformatie Configuraties WLC-configuratie Microsoft NPS-configuratie Verifiëren Problemen oplossen

Inleiding

Dit document beschrijft hoe u beheerstoegang voor AireOS WLC GUI en CLI kunt configureren via de Microsoft Network Policy Server (NPS).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van draadloze beveiligingsoplossingen
- AAA en RADIUS-concepten
- Basiskennis van Microsoft Server 2012
- Installatie van Microsoft NPS en Active Directory (AD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardwareonderdelen.

- AireOS-controller (5520) op 8.8.120.0
- Microsoft Server 2012

Opmerking: Dit document is bedoeld om de lezers een voorbeeld te geven van de configuratie die op een Microsoft-server vereist is voor toegang tot het WLC-beheer. De Microsoft Windows serverconfiguratie die in dit document wordt gepresenteerd, is getest in het laboratorium en bleek te werken zoals verwacht. Als u problemen hebt met de configuratie, neemt u contact op met Microsoft voor ondersteuning. Het Cisco Technical Assistance Center (TAC) ondersteunt de Microsoft Windows-serverconfiguratie niet. U vindt

de installatie- en configuratiehandleidingen van Microsoft Windows 2012 in Microsoft Tech Net.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Wanneer de WLC CLI/GUI wordt benaderd, wordt de gebruiker gevraagd om de inloggegevens in te voeren. De geloofsbrieven kunnen tegen of een lokale gegevensbestand of een externe AAA server worden geverifieerd. In dit document wordt Microsoft NPS gebruikt als externe verificatieserver.

Configuraties

In dit voorbeeld worden twee gebruikers ingesteld op AAA (NPS), d.w.z. **loginuser** en **adminuser**. **loginuser** heeft alleen de read-only toegang terwijl **adminuser** volledige toegang krijgt.

WLC-configuratie

Stap 1. Voeg de RADIUS-server toe aan de controller. Navigeer naar **Security > RADIUS > Verificatie**. Klik op **New** om de server toe te voegen. Zorg ervoor dat de beheeroptie is ingeschakeld zodat deze server kan worden gebruikt voor beheertoegang, zoals in deze afbeelding wordt weergegeven.

cisco		<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	Sa EEEDB
Security	RADIUS	Authenti	ication Server	rs > Edit					
 AAA General RADIUS Authentication Accounting Access Control Lists Wireless Protection Policies Web Auth TrustSec Local Policies Umbrella 	Server In Server Ad Shared S Shared S Confirm S Key Wrap Apply Cis Apply Cis Port Num Server St Support f Server Til Network I Managem Tunnel Provi PAC Provi IPSec Cisco AC/	dex ddress{Ipv4 ecret Formi ecret Shared Secr co ISE Defa co ACA Def ber atus for CoA meout User sent sent net Retrans oxy a isioning	l/Ipv6) at ret ault settings ault settings	2 10.106.33.31 ASCII © (Designed for 1812 Enabled © 5 secon ✓ Enable 5 second Enable Enable Enable	e FIPS custom ds	ers and requires a k	ey wrap complia	nt RADIU	S server;
h Advanced									

Stap 2. Navigeer naar **security > prioriteitsopdracht > beheergebruiker**. Zorg ervoor dat de RADIUS is geselecteerd als een van de authenticatietypen.

MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Priority C	rder > N	lanagement l	Jser		
Authentic	ation				
Not I	Jsed		Order U	sed for Authe	entication
TACACS	5+	>		RADIUS	Up
		<		LUCAL	Down

Opmerking: Als RADIUS is geselecteerd als eerste prioriteit in de authenticatievolgorde, worden lokale geloofsbrieven alleen gebruikt voor authenticatie als de RADIUS-server onbereikbaar is. Als RADIUS als tweede prioriteit wordt geselecteerd, worden de RADIUS-referenties eerst geverifieerd via de lokale database en vervolgens gecontroleerd via de geconfigureerde RADIUS-servers.

Microsoft NPS-configuratie

Stap 1. Open de Microsoft NPS-server. Klik met de rechtermuisknop op RADIUS-clients. Klik op

New om de WLC als de RADIUS-client toe te voegen.

Voer de gewenste gegevens in. Zorg ervoor dat het gedeelde geheim hetzelfde is als dat welke is ingesteld op de controller terwijl de RADIUS-server wordt toegevoegd.

V	WLC Properties	×
 File Action View Help File Action View Help NPS (Local) ADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Policies Network Access Protection Accounting Templates Management 	WLC Properties ************************************	
< III >	OK Cancel Apply	Ц

Stap 2. Navigeer naar **beleid > Aanvraagbeleid**. Klik met de rechtermuisknop om een nieuw beleid toe te voegen, zoals in de afbeelding.

Stap 3. Onder het tabblad **Voorwaarden** selecteert u **NAS-identificator** als de nieuwe voorwaarde. Voer desgevraagd de hostnaam van de controller in als de waarde, zoals in de afbeelding.

	Cisco WLC Properties	x
Overview Conditions Set	ttings	
Configure the conditions for If conditions match the con connection request, NPS s	r this network policy. Infection request, NPS uses this policy to authorize the connection request. If conditions do not match the kips this policy and evaluates other policies, if additional policies are configured.	
Condition	Value	
NAS Identifier	Cisco-WLC	
Condition description: The NAS Identifier condition syntax to specify NAS name	n specifies a character string that is the name of the network access server (NAS). You can use pattern matching es.	
	Add Edit Remove]
	OK Cancel Appl	y

Stap 4. Navigeer naar **beleid > Netwerkbeleid**. Klik met de rechtermuisknop om een nieuw beleid toe te voegen. In dit voorbeeld wordt het beleid aangeduid als **Cisco WLC RW-**beleid wat impliceert dat het beleid wordt gebruikt om volledige (lezen-schrijven) toegang te bieden. Zorg ervoor dat het beleid is geconfigureerd zoals hier wordt getoond.

0	Cisco WLC RW Properties	x
File Action View Help File Action View Help Pile Pile Pile Pile Pile Pile Pile Pile Policies Policies Policies Policies Peleth Policies Pile Accounting Pile Pile Pile Pile Pile Pile Pile Pile	Cisco WLC RW Properties Verview Conditions Constraints Settings Policy name: Policy State F 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? Grant access. Grant access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy. Deny access. Deny access if the connection request matches this policy and the policy grants access. perform activation with network policy only: do not evaluate the dial-in properties of user accounts. Network connection method Select the type of network access server: Deny of network ac	
< III >	OK Cancel Apply	у

Stap 5. Onder het tabblad **Voorwaarden** klikt u op **Toevoegen**. Selecteer de **gebruikersgroepen** en klik op **Toevoegen**, zoals in de afbeelding.

Overview	Conditions	Constraints	Settings									
Configure	the condition	ns for this net	vork policy.									
If condition connection	ns match the n request, N	Connection r PS skips this	equest, NP colicy and e	S uses this po avaluates othe	olicy to authors of the second s	orize the con additional p	nection re olicies are	equest. If cor configured.	nditions d	o not match	n the	
					Select c	ondition						x
Select	a condition, a	and then click	Add.									
Group	s											^
	Windows The Windo groups. Machine	Groups ws Groups c Groups	ondition sp	ecifies that t	he connecti	ng user or c	omputer	must belong	to one o	f the select	ted	=
	The Machi User Gro The User (ne Groups co ps Groups condi	ndition sp tion specifi	ecifies that th	e connectir	ng computer ser must be	must bel long to or	ong to one o ne of the sele	f the sele	ected group	15.	
	Location The HCAP required to network ac	Groups Location Gro match this p cess servers	ups condit olicy. The (NASs). S	tion specifies HCAP protoc See your NAS	the Host C ol is used fi documenta	redential Au or communi ation before	thorizatio cation be using this	on Protocol (ween NPS a condition.	HCAP) Id and some	ocation gro third party	ups /	~
										Add	Cance	4
								Add	Б	dit	Remov	/e

Stap 6. Klik op **Add Group** in het dialoogvenster dat nu wordt weergegeven. In het venster **Select Group** die nu wordt weergegeven, selecteert u het gewenste **doeltype** en de gewenste **locatie**. Voer de gewenste objectnaam in, zoals in de afbeelding.

	Cisco WLC RW Properties)
Ov	User Groups 🗶	
C H	Specify the group membership required to match this policy. on request. If conditions do not match the	
	Groups sare configured.	x
		~
	iter must belong to one of the selected	Ξ
	Add Groups Remove : belong to one of the selected groups.	
	OK Cancel to one of the selected groups.	
	Select Group	
	Group Object Types Object Types Dcol (HCAP) location groups	
	From this location:	~
	wlanlsc.com Locations Add Cancel	
	Enter the object name to select (examples):	
	Domain Admins Check Names Edit Remove	,
	Advanced OK Cancel	

De conditie, indien correct toegevoegd, moet eruit zien zoals hier getoond wordt.

			Cisco WLC RW Properties
Overview	Conditions	Constraints	Settings
Configure If condition	the condition ons match the on request, N	ns for this network of the second sec	work policy. request, NPS uses this policy to authorize the connection request. If conditions do not match the policy and evaluates other policies, if additional policies are configured.
Cor	ndition	V	alue
🕌 Use	er Groups	W	/LANLSC\Domain Admins
Condition The User	description:	ition specifies	s that the connecting user must belong to one of the selected groups.
Condition The User	description : Groups cond	lition specifies	s that the connecting user must belong to one of the selected groups.

Opmerking: Wilt u te weten komen waar de locatie en de objectnaam zijn, dan opent u de actieve directory en zoekt u de gewenste gebruikersnaam. In dit voorbeeld bestaat **Domain Admins** uit gebruikers die volledige toegang krijgen. **beheerder** maakt deel uit van deze objectnaam.

	Ac	tive Directory Use	rs and Con	nputers			-	x
File Action View Help Active Directory Users and Com Active Directory Users and Com Saved Queries Wanlsc.com Builtin Computers Domain Controllers ForeignSecurityPrincipals Managed Service Accour Users	Admi Name Admi Admi Admi Admi Allow Anan AP US AR US AP US AC Contr AC Contr AC Contr AC Contr AC Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma A Doma	Remote control Member Of General Address Admin Use First name: Last name: Display name: Description: Office:	rs and Con Admin Us Remote D Dial-in Account er User Admin User	er Prope Desktop Sen Envir Profile	erties vices Profile onment Telephones	COM+ Sessions Organization		×
< III >	B Doma Doma Doma Emple Enter; Group Coup Login RAS a RAS a Read-	Office: Telephone number: E-mail: Web page:	K C	ancel	Apply	Other Other		

	Active	Directory	Users an	d Compute	ers	
File Action View Help		Admin Us	ser Prop	erties	?	x
Active Directory Users and Active Directory Users and Saved Queries Manlsc.com Builtin Computers Domain Controllers ForeignSecurityPrir Managed Service A Users	Remote control General Address Member Of Member of: Name Domain Admins	Remote Dial-In Dial-In Active Director wlanisc.com/	Desktop Ser Profile Envir ory Domain Users	vices Profile Telephones ronment	COM- Organizal Sessions	+ tion is r a rou rou rou rou rou rou rou rou rou rou
	Add Primary group: C	Remove Domain Admins There is n you have application	no need to c Macintosh ns.	hange Primary clients or POSID	group unless X-compliant	istr rou rou rou

Stap 7. Onder het tabblad **Beperkingen**, navigeer naar **Verificatiemethoden** en controleer of alleen **niet-versleutelde verificatie** is ingeschakeld.

	Cisco WLC RW Properties
Overview Conditions Constraints Setting Configure the constraints for this network pol If all constraints are not matched by the conr Constraints: Constraints	s lcy. nection request, network access is denied.
Authentication Methods Authentication Methods	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types: Move Up Move Down
	Add Edt Remove Less secure authentication methods:
	Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication method Perform machine health check only
	OK Cancel Apply

Stap 8. Onder het tabblad **Instellingen** navigeren naar **RADIUS-kenmerken > Standaard**. Klik op **Add** om een nieuwe eigenschap, **Service-type**, toe te voegen. Selecteer in het vervolgkeuzemenu de optie **Administratief** om volledige toegang te bieden tot de gebruikers die aan dit beleid zijn toegewezen. Klik op Toepassen om de wijzigingen op te slaan, zoals in de afbeelding wordt weergegeven.

COLLENS Offerhadees	Attaileute Information X	
Chardend	Attribute Information	andard attribute, and
Standard	Attribute name:	ADIUS Clients, See
Vendor Specific	Service-Type	
Network Access Protection	Attribute number:	
NAP Enforcement	0	
Extended State	Attribute format: Enumerator	
Routing and Remote Acc		
Multilink and Bandwid Allocation Protocol (B	Attribute Value: Commonly used for Dial-Up or VPN	
IP Filters	<pre></pre>	
Encryption	Commonly used for 802.1x	
R IP Settings	<none></none>	
	Others	
	Administrative	
	UK Cancel	

Opmerking: Als u alleen-lezen toegang wilt geven aan bepaalde gebruikers, selecteert u NAS-prompt in de vervolgkeuzelijst. In dit voorbeeld wordt een ander beleid met de naam **Cisco WLC RO** gecreëerd om alleen-lezen toegang te bieden aan gebruikers onder de objectnaam **Domain Gebruikers**.

	Cisco WLC RO Properties
Overview Conditions Constr	aints Settings
Configure the conditions for thi If conditions match the connec connection request, NPS skips	s network policy. tion request, NPS uses this policy to authorize the connection request. If conditions do not match the this policy and evaluates other policies, if additional policies are configured.
Condition	Value
all User Groups	WLANLSC\Domain Users
Condition description: The User Groups condition spe	ecifies that the connecting user must belong to one of the selected groups.
	OK Cancel Apply

	Cisco WLC RO Properties	x
Overview Conditions Constr	aints Settings	
Configure the settings for this r If conditions and constraints m Settings:	network policy. atch the connection request and the policy grants access, settings are applied.	
RADIUS Attributes	Attribute Information X and at the tea and	_
Standard	Attribute name: Service-Type	
Network Access Protection	Attribute number: 6	
Extended State	Attribute format: Enumerator	
Multilink and Bandwid Allocation Protocol (B	Attribute Value: O Commonly used for Dial-Up or VPN	
TP Filters	<pre></pre>	
Encryption	O Commonly used for 802.1x	
🔏 IP Settings	<pre></pre>	
	Others	
	NAS Prompt V	
	OK Cancel	
	OK Cancel	ply

Verifiëren

1. Wanneer inloggebruikersreferenties worden gebruikt, mag de gebruiker geen wijzigingen op de controller configureren.



me	tes	tr			
	WLAN				
	tes	t2			
		Enabled			
Policies					
					inges.)
	Autho	rization Failed. No su	fficient privileges		
cy					
Interface Gro					-
Vlan Feature				Close	
SSID	0	Lilabieu			
	nor	1e			
	olicies cy Interface Gro Vlan Feature : SSID	volicies volicies Cy Interface Groo Vian Feature SSID	WLAN test2 Enabled Policies Authorization Failed. No su Vian Feature SSID	WLAN test2 Enabled Policies Authorization Failed. No sufficient privileges Vian Feature SSID	volicies volicies cy Interface Gro Vian Feature SSID

Van **debug a allen toelaten**, kunt u zien dat de waarde van de eigenschap servicetype in autorisatie 7 is die aan NAS-prompt correspondeert.

```
*aaaQueueReader: Dec 07 22:20:14.664: 30:01:00:00:00:00 Successful transmission of
Authentication Packet (pktId 14) to 10.106.33.39:1812 from server queue 0, proxy state
30:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:20:14.664: 00000000: 01 0e 00 48 47 f8 f3 5c 58 46 98 ff 8e f8 20 7a
\dots HG. \backslash XF. . . . z
*aaaQueueReader: Dec 07 22:20:14.664: 00000010: f6 a1 f1 d1 01 0b 6c 6f 67 69 6e 75 73 65 72 02
.....loginuser.
*aaaQueueReader: Dec 07 22:20:14.664: 00000020: 12 c2 34 69 d8 72 fd 0c 85 aa af 5c bd 76 96 eb
...4i.r....\.v..
*aaaQueueReader: Dec 07 22:20:14.664: 00000030: 60 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43
....j$1..C
*aaaQueueReader: Dec 07 22:20:14.664: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC
:
*radiusTransportThread: Dec 07 22:20:14.668: 30:01:00:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (gid:0) with port:1812, pktId:14
*radiusTransportThread: Dec 07 22:20:14.668: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:20:14.668: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:20:14.668:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:20:14.668:
*radiusTransportThread: Dec 07 22:20:14.668: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:20:14.668: AVP[01] Service-
*radiusTransportThread: Dec 07 22:20:14.668: AVP[02]
Class.....DATA (44 bytes)
```

2. Wanneer de gebruikersreferenties worden gebruikt, moet de gebruiker volledige toegang hebben met **servicetype** waarde 6, hetgeen overeenkomt met **administratieve gegevens**.



```
*aaaQueueReader: Dec 07 22:14:27.439: AuthenticationRequest: 0x7fba240c2f00
*aaaQueueReader: Dec 07 22:14:27.439:
proxyState.....2E:01:00:00:00:00-00:00
*aaaQueueReader: Dec 07 22:14:27.439: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:14:27.439: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:14:27.439: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:14:27.439: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:14:27.442: 2e:01:00:00:00 Access-Accept received from
RADIUS server 10.106.33.39 (qid:0) with port:1812, pktId:13
*radiusTransportThread: Dec 07 22:14:27.442: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:14:27.442:
protocolUsed.....0x00000001
*radiusTransportThread: Dec 07 22:14:27.442:
proxyState.....2E:01:00:00:00:00-00:00
*radiusTransportThread: Dec 07 22:14:27.442: AVP[01] Service-
Type.....0x00000006 (6) (4 bytes)
*radiusTransportThread: Dec 07 22:14:27.442: AVP[02]
Class.....DATA (44 bytes)
```

Problemen oplossen

Om de toegang tot WLC van het probleemoplossingsbeheer door NPS te toegang hebben, **kan** de run **debug a.u.** opdracht uitvoeren.

1. De logbestanden waarin onjuiste referenties worden gebruikt, worden hier weergegeven.

*aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 Successful transmission of Authentication Packet (pktId 15) to 10.106.33.39:1812 from server queue 0, proxy state 32:01:00:00:00:00-00:00 *aaaQueueReader: Dec 07 22:36:39.753: 00000000: 01 0f 00 48 b7 e4 16 4d cc 78 05 32 26 4c ec 8dH....M.x.2&L... *aaaQueueReader: Dec 07 22:36:39.753: 00000010: c7 a0 5b 72 01 0b 6c 6f 67 69 6e 75 73 65 72 02 ..[r..loginuser. *aaaQueueReader: Dec 07 22:36:39.753: 00000020: 12 03 a7 37 d4 c0 16 13 fc 73 70 df 1f de e3 e47.....sp..... *aaaQueueReader: Dec 07 22:36:39.753: 00000030: 32 06 06 00 00 07 04 06 0a 6a 24 31 20 0b 43 2....j\$1..C *aaaQueueReader: Dec 07 22:36:39.753: 00000040: 69 73 63 6f 2d 57 4c 43 isco-WLC *aaaQueueReader: Dec 07 22:36:39.753: 32:01:00:00:00:00 User entry not found in the Local FileDB for the client. *radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Counted 0 AVPs (processed 20 bytes, left 0) *radiusTransportThread: Dec 07 22:36:39.763: 32:01:00:00:00:00 Access-Reject received from

2. De logboeken bij gebruik van het servicetype met een andere waarde dan **administratief** (waarde=6) of NAS-prompt (waarde=7) worden als volgt weergegeven. In dat geval, mislukt de inlognaam, zelfs als de verificatie lukt.

```
*aaaQueueReader: Dec 07 22:46:31.849: AuthenticationRequest: 0x7fba240c56a8
*aaaQueueReader: Dec 07 22:46:31.849:
*aaaQueueReader: Dec 07 22:46:31.849: Packet contains 5 AVPs:
*aaaQueueReader: Dec 07 22:46:31.849: AVP[01] User-Name......adminuser
(9 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[03] Service-
Type.....0x00000007 (7) (4 bytes)
*aaaQueueReader: Dec 07 22:46:31.849: AVP[04] Nas-Ip-
*aaaQueueReader: Dec 07 22:46:31.849: AVP[05] NAS-Identifier.....Cisco-WLC
(9 bytes)
:
:
*radiusTransportThread: Dec 07 22:46:31.853: AuthorizationResponse: 0xa3d3fb25a0
*radiusTransportThread: Dec 07 22:46:31.853: RadiusIndexSet(1), Index(1)
*radiusTransportThread: Dec 07 22:46:31.853: resultCode.....0
*radiusTransportThread: Dec 07 22:46:31.853:
protocolUsed.....0x0000001
*radiusTransportThread: Dec 07 22:46:31.853: Packet contains 2 AVPs:
*radiusTransportThread: Dec 07 22:46:31.853: AVP[01] Service-
Type.....0x00000001 (1) (4 bytes)
*radiusTransportThread: Dec 07 22:46:31.853: AVP[02]
Class.....DATA (44 bytes)
*emWeb: Dec 07 22:46:31.853: Authentication succeeded for adminuser
```