Configureer WLC met LDAP-verificatie voor 802.1x en Web-Autation WLAN's

Inhoud

Inleiding **Voorwaarden** Vereisten Gebruikte componenten Achtergrondinformatie Technische achtergrond Veelgestelde vragen Configureren WLAN's maken die afhankelijk zijn van LDAP-server om gebruikers te verifiëren via 802.1x Netwerkdiagram WLAN's maken die op LDAP-server vertrouwen om gebruikers te verifiëren via het interne WLCwebportal Netwerkdiagram Gebruik LDP-tool om LDAP te configureren en problemen op te lossen Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

In dit document wordt de procedure beschreven voor het configureren van een AireOS WLC om clients met een LDAP Server als gebruikersdatabase te authenticeren.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- Microsoft Windows-servers
- Active Directory

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

Cisco WLC-software 8.2.10.0

Microsoft Windows Server 2012 R2

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Technische achtergrond

- LDAP is een protocol dat wordt gebruikt voor de toegang tot directory servers.
- Directory servers zijn hiërarchische, object georiënteerde databases.
- Objecten worden georganiseerd in containers zoals Organisatorische Eenheden (OU), Groepen, of standaard Microsoft Containers als CN=Gebruikers.
- Het moeilijkste deel van deze opstelling is de LDAP serverparameters correct op WLC te vormen.

Voor gedetailleerdere informatie over deze concepten, raadpleegt u de sectie Inleiding van <u>Hoe u</u> <u>Wireless LAN Controller (WLC) kunt configureren voor LDAP-verificatie (Lichtgewicht Directory</u> <u>Access Protocol)</u>.

Veelgestelde vragen

• Welke gebruikersnaam moet worden gebruikt om te binden met de LDAP-server? Er zijn twee manieren om te binden tegen een LDAP-server, Anoniem of Geverifieerd (raadpleeg de sectie om het verschil tussen beide methoden te begrijpen).

Deze bind gebruikersnaam moet beheerdersrechten hebben om te kunnen vragen naar andere gebruikersnamen/wachtwoorden.

• Indien geverifieerd: is de bind gebruikersnaam binnen dezelfde container dan alle gebruikers? **Nee:** gebruik het hele pad. Voorbeeld:

CN=Administrator, CN=Domain Admins, CN=Gebruikers, DC=labm, DC=cisco, DC=com

Ja: gebruik alleen de gebruikersnaam. Voorbeeld:

Beheerder

• Wat als er gebruikers zijn in verschillende containers? Moeten alle betrokken draadloze LDAP-gebruikers in dezelfde container zitten?

Nee, een basis DN die alle benodigde containers bevat kan worden gespecificeerd.

• Welke eigenschappen moet de WLC zoeken?

WLC past het gespecificeerde Gebruikerskenmerk en het gespecificeerde objecttype aan.

Opmerking: sAMAccountName is hoofdlettergevoelig, maar persoon niet. Daarom zijn

sAMAccountName=RICARDO en sAMAccountName=ricardo hetzelfde en werkt dit, terwijl samaccountname=RICARDO en samaccountname=ricardo dit niet doen.

• Welke EAP-methoden kunnen worden gebruikt?

Alleen EAP-FAST, PEAP-GTC en EAP-TLS. Android, iOS en MacOS standaardapplicaties werken met Protected Extensible Verification Protocol (PEAP).

In Windows moet AnyConnect Network Access Manager (NAM) of de standaard Windowsaanvrager met Cisco:PEAP worden gebruikt voor ondersteunde draadloze adapters zoals in de afbeelding.

Local-EAP Wireless Netw	vork Properties
Connection Security	
Security type: Encryption type:	WPA2-Enterprise AES
Choose a network aut	hentication method:
Cisco: PEAP Microsoft: Smart Card Microsoft: Protected B Cisco: LEAP Cisco: PEAP Cisco: EAP-FAST Intel: EAP-FAST Intel: EAP-SIM Intel: EAP-TTLS Intel: EAP-AKA Advanced settings	Settings does not work! works!
	OK Cancel

Opmerking: De <u>Cisco EAP plug-ins</u> voor Windows bevatten een versie van Open Secure Socket Layer (OpenSSL 0.9.8k) die wordt beïnvloed door Cisco bug-id <u>CSC09670</u>, Cisco is niet van plan om meer releases van de EAP plug-ins voor Windows uit te geven en raadt klanten aan in plaats daarvan de AnyConnect Secure Mobility Client te gebruiken.

• Waarom kan de WLC geen gebruikers vinden?

Gebruikers binnen een groep kunnen niet worden geverifieerd. Ze moeten zich in een Default Container (CN) of een Organisatorische Eenheid (OU) bevinden zoals getoond in de afbeelding.

	Name	Туре	Description
<u>_</u>	SofiaLabGroup	Group	will not work
20	SofiaLabOU	Organizational Unit	
	Users	Container	Default container for upgr

Configureren

Er zijn verschillende scenario's waarin een LDAP-server kan worden gebruikt, met 802.1x-verificatie of webverificatie.

Voor deze procedure, slechts moeten de gebruikers binnen OU=SofiaLabOU worden voor authentiek verklaard.

Raadpleeg de <u>WLC LDAP Configuration Guide</u> voor informatie over het gebruik van LDAP (Label Distribution Protocol), het configureren en oplossen van problemen.

WLAN's maken die afhankelijk zijn van LDAP-server om gebruikers te verifiëren via 802.1x

Netwerkdiagram

In dit scenario maakt WLAN LDAP-dot1x gebruik van een LDAP-server om de gebruikers te verifiëren met het gebruik van 802.1x.



Stap 1. Maak een gebruiker **Gebruiker1** in het LDAP Server lid van SofiaLabOU en SofiaLabGroup.

<u>1</u>	Server Manager	_ 0 <u>×</u>
Server Ma	anager • Dashboard	
Dashboard	WELCOME TO SERVER MANAGER	Active Directory Domains and Trusts Active Directory Lightweight Directory Services Setup Wizard Active Directory Module for Windows PowerShell
All Servers	1 Configure this local server	Active Directory Sites and Services Active Directory Users and Computers ADSI Fela
留 AD DS 日 AD LDS 算 DHCP	Quick start 2 Add roles and features	Certification Authority Component Services
B DNS ■ File and Storage Services ▷	3 Add other servers to manage WHATS NEW 4 Create a server group	Defragment and Optimize Drives DHCP
∎ø IIS ¶∿ NAP		Event Viewer Group Policy Management

TASKS 🔻 SECTIONS 🔻

TASKS 🔻 SECTIONS 🔻

Create User: SofiaLab User1 Test User

Account	Account		() × ()
Organization	First name: SofiaLab User1	Account expires: Never	
Member Of	Middle initials:	O End of	
Password Settings	Last name: Test User	Paraword options	
Profile	Full name: * SofiaLab User1 Test User	User must change password at next log on	-
Policy	User OVN logon:	O Other password options	
Silo	Use SamAccountivame o Jaom	Smart card is required for interactive log on	
3110	Password:	User cannot change password	
	Confirm password:	Encryption options:	•
	Create in: DC=labm,DC=cisco,DC=com Change	Other options:	•
	Find in this column Find in this column		
	Domain Controllers		
	Employees		<u> </u>
	Guets		000
	N In LostAndFound		(?) (\$) (\$)
	Managed Service Accos >		
	Im NTDS Quotas		
	III Program Data		Add
	f ^{rei} SofiaLabOU		Remove
	System 🕨 🗸		
	This object will be added to the default Active Directory accurs		

Create User: SofiaLab User1 Test User

Account	Account	0.80	
Organization Member Of Password Settings Profile Policy Silo	First name: SofiaLab User1 Middle initials: Test User Last name: Test User User UPN logon: SofiaLab User1 Test User User SamAccountName Io Iabm Password: Iabm Confirm password: Create in: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com C Protect from accidental deletion Log on hours Log on to	♥ • \★ [User1	Account expires:
	Organization		?⊗⊙
	Member Of	Select Groups	× () & ⊙
	Filter P Name Active Director Primary SofiaLabGroup Jabm-SofiaLab	Select this object type: Groups or Built in security principals Prom this location: Iabm cisco.com Enter the object names to select (<u>scarcelest</u>): Select.abGroup One	z Types Add astons Remove
	This object will be added to the default Active Directory Directly Associated Password Settings Name Precedence	gro Advanced OK	Cancel 0 ® ©

Stap 2. Maak een EAP-profiel bij de WLC met de gewenste EAP-methode (gebruik PEAP).

ahaha							5	Sa <u>v</u> e Configuratio	n <u>P</u> ing	Logout <u>R</u> efree
cisco		MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURIT	TY MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	FEEDBACK
Security	^	Local EA	P Profile	is				Ne	w	Apply
General		Profile Na	me		LEAP	EAP-FAST	EAP-TLS	PEAP		
Authentication		Local-EAP-P	PEAP					✓		
Accounting Fallback		Local-EAP-L	.EAP		✓					
Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP General Profiles		LE EA PE	AP P-FAST P-TLS AP	Server Server Server Server	Nothing PAK Certific Certific	((cate (cate (Client Userna Client Userna Client Certif Client Userna	ume & Pass ume & Pass ficate ume & Pass	word word word	
EAP-FAST Parameters Authentication Priority	,									

Stap 3. Bind de WLC met de LDAP Server.

Tip: Als de bind Gebruikersnaam niet in de User Base-ISDN staat, moet u het gehele pad naar de **Admin-**gebruiker schrijven zoals in de afbeelding. Anders kunt u eenvoudig **Administrator** invoeren.

Security LDAP Servers > New < Back	uluilu cisco
VAA Server Index (Priority) 1 < General Server IP Address 10.88.173.121 Authentication Port Number 389 Fallback Simple Bind Lauthenticated DNS Bind Username CN=Administrator,CN=Users,DC=labm,DC= Local Net Users Bind Password Internet	Security
Disabled Clients User Base DN OU=SofiaLabOU_DC=labm_DC=cisco_DC=com Where are we going to look for user AP Policies User Atribute SAMAccountName What Attribute are we looking for? Password Policies User Object Type Person What Attribute are we looking for? Priority Order Secure Mode(via TLS) Disabled V Secure Mode(via TLS) Certificate Server Timeout 2 seconds Access Control Enable Server Status Enabled V Wireless Protection Policies V Message from webpage Wireless Protection Policies Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods Maccal Policies Advanced OK	 AAA General RADIUS Authentication Accounting Falback DNS TACACS+ LOAP LOCAI Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Access Control Lists Weieless Protection Policies Web Auth TrustSec SXP Local Policies Advanced

Stap 4. Stel de verificatievolgorde in op alleen Interne Gebruikers + LDAP of LDAP.

،، ،،، ،، cısco		MONITOR	<u>w</u> lans	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u>
Security	^	Priority C	rder > L	ocal-Auth			
 AAA General RADIUS Authentication 		User Cred	lentials				
Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies		Not Used	>	Order Used F	or Authentica	Up Down]
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 						-	

Stap 5. Maak de LDAP-dot1x WLAN aan.

uluili. cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
WLANs	WLANs								
WLANs	Current Fi	ter: No	ne [<u>Char</u>	oge Filter] [Clea	r Filter]		Cr	eate New	✓ Go
Advanced	WLAN	ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies	5		

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'LDAP-dot1x'
 WLANS Advanced 	General Security QoS Policy-Mapping Advanced Profile Name LDAP-dot1x Type WLAN SSID LDAP-dot1x Status Inabled Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.) Radio Policy All Interface/Interface Group(G) Van2562 Multicast VIan Feature Enabled Broadcast SSID Enabled
	NAS-ID none

Stap 6. Stel de L2 beveiligingsmethode in op WPA2 + 802.1x en stel L3 beveiliging in op nul.

cisco	MONITOR	<u>W</u> LANs <u>C</u> ON	ITROLLER V	WIRELESS	SECURITY	MANAGEN
WLANs	WLANs >	Edit 'LDA	P-dot1x'			
WLANs WLANs	General	Security	QoS P	olicy-Mapp	oing Ad	vanced
Advanced	Layer 2	Layer 3	AAA Serv	vers		
	Layer	2 Security 🕯 🛛	VPA+WPA2	~]	
	Fast Tra	nsition	C Filtering			
	Fast Trans	sition				
	PRE	d Management	Disabled	4 🗸		
	WPA+W	PA2 Parameter	s			
	WPA P	Policy	✓			
	WPA2	Encryption	✓ AES			
	802.1	X V E	inable			
	CCKM		nable			
	FT 80	2.1X	Enable			
	FT PSI	K	Enable			
	14	, and the state of the state of	D	isable 🗸		

Stap 7. Schakel lokale EAP-verificatie in en zorg ervoor dat de opties voor verificatieservers en accountingservers worden uitgeschakeld en dat LDAP is ingeschakeld.

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> OP	NTROLLER W <u>I</u> RELESS	<u>s</u> ecurity m <u>a</u> na	GEMENT C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LD/	AP-dot1x'			
WLANS WLANS	General Security	QoS Policy-Mappi	ng Advanced		
Advanced	Layer 2 Layer 3	AAA Servers			
	Select AAA servers bel	ow to override use of defai	ult servers on this \	WLAN	
	Radius Servers				
	Radius Server Overwr	ite interface 🗌 Enabled			
	Authentication Servers	Accounting Servers		E	AP Parameters
		Enabled	Enabled		Enable
	Server 1	None	✓ None	\sim	
	Server 2	None	✓ None	\checkmark	
	Server 3	None	✓ None	\checkmark	
	Server 4	None	✓ None	\checkmark	
	Server 5	None	✓ None	\checkmark	
	Server 6	None	✓ None	\checkmark	
	Radius Server Account	ing			
	Interim Update				
	LDAP Servers				
	Server 1 IP:10.88.1	73.121, Port:389 🗸			
	Server 2 None	~			
	Server 3 None	~			
	Local EAP Authenticati	on			
	Local EAP Authenticat	ion 🗹 Enabled			
	EAP Profile Name	Local-EAP-PEAP V			
	Authentication prio	rity order for web-auth	1 user		
	Not Used			Order Used For Authe	ntication
			>	LOCAL	Up
			<	RADIUS	Down
				,	

Alle andere instellingen kunnen standaard ingeschakeld worden.

Opmerkingen:

Gebruik het LDP-gereedschap om de configuratieparameters te bevestigen. De Zoekbasis kan geen Groep zijn (zoals SofiaLabGroup). PEAP-GTC of Cisco:PEAP moeten worden gebruikt in plaats van Microsoft:PEAP bij de aanvrager als het een Windows-machine is. Microsoft:PEAP werkt standaard met MacOS/iOS/Android.

WLAN's maken die op LDAP-server vertrouwen om gebruikers te verifiëren via het interne WLC-webportal

Netwerkdiagram

In dit scenario maakt WLAN LDAP-Web gebruik van een LDAP-server om de gebruikers te verifiëren met de interne WLC Web Portal.

LDAP Server



Verzeker Stappen 1. door Stappen 4. zijn genomen van het vorige voorbeeld. Van daaruit wordt de WLAN-configuratie anders ingesteld.

Stap 1. Maak een gebruiker **Gebruiker1** in het LDAP Server lid van de OU SofiaLabOU en de Groep SofiaLabGroup.

Stap 2. Maak een EAP-profiel bij de WLC met de gewenste EAP-methode (gebruik PEAP).

Stap 3. Bind de WLC met de LDAP Server.

Stap 4. Stel de verificatievolgorde in op Interne gebruikers + LDAP.

Stap 5. Maak het LDAP-Web WLAN zoals in de afbeeldingen wordt getoond.

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANS
WLANs	Current Filter: None [Change Filter] [Clear Filter] Create New V Go
Advanced	UKLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
 WLANS Mdvanced 	General Security QoS Policy-Mapping Advanced Profile Name LDAP-Web Type WLAN SSID LDAP-Web Status Image: Comparison of the security Policies Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio PolicyAllInterface/Interface Group(G)Vlan2562Multicast Vlan FeatureEnabledBroadcast SSIDImabledNAS-IDnone

Stap 6. L2-beveiliging op nul en L3-beveiliging op webbeleid instellen - verificatiezoals in de afbeeldingen wordt getoond.

cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER W <u>I</u> RELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
 WLANs Advanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security None T MAC Filtering? T Fast Transition Fast Transition

،،۱۱،،۱۱، cısco	Monitor Wlans Controller Wireless Security Management Commands Help Feedback
WLANs	WLANs > Edit 'LDAP-Web'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security 1 Web Policy V Authentication Passthrough Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure 10 Preauthentication ACL IPv4 None VIPv6 None VWebAuth FlexAcl None V Sleeping Client Enable Over-ride Global Config 20 Enable Web Auth type Internal V

Stap 7. Stel de prioriteitsvolgorde voor de verificatie voor web-auth in om LDAP te gebruiken en zorg ervoor dat de opties voor de verificatieservers en de accountingservers zijn uitgeschakeld.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'LDAP-Web'	
VLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN RADIUS Servers RADIUS Server Overwrite interface Enabled	
	Authentication Servers Accounting Servers	
	Server 1 None	
	Server 2 None V None V	
	Server 3 None V None V	
	Server 4 None V None V	
	Server 5 None None	
	Server 6 None V None V	
	RADIUS Server Accounting	
	Interim Update	
	LDAP Servers	
	Server 1 IP:10.88.173.121, Port:389 V	
	Server 2 None	
	Server 3 None T	
	Local EAP Authentication	
	Local EAP Authentication Enabled	
	Authentication priority order for web-auth user	
	Not Used Order Used For Authentication RADIUS A > LDAP Up	
	T C Down	

Alle andere instellingen kunnen standaard ingeschakeld worden.

Gebruik LDP-tool om LDAP te configureren en problemen op te lossen

Stap 1. Open het LDP-gereedschap op de LDAP-server of op een host met connectiviteit (poort TCP 389 moet aan de server zijn toegestaan).



Stap 2. Navigeer naar **Verbinding > Bind,** log in met een beheerder gebruiker en selecteer **Bind met referenties** keuzerondje.

User: Password: Password: Domain: Bind Domain: Bind type Bind as o Bind as o Bind with Save Save As Evit		
Bind Ctrl+B Disconnect Bind type Disconnect Bind as a New Ctrl+N Save Save Save As Save Encrypt		User:
Bind Ctrl+B Disconnect Bind type New Ctrl+N Save Simple bill Save As Image: Save As	Onnection Browse View	w Ol Password:
Disconnect ○ Bind as of Order New Ctrl+N Save ○ Simple bind with Save As ✓ Encrypt	Bind Ctrl+B	+B Bind type
New Ctrl+N Save ○ Simple bi Save As ○ Advance	Disconnect	O Bind a
Save Save As Advance	New Ctrl+N	•N Simple
Encrypt	Save Save As	O Advar
	Exit	✓ Encry;

Stap 3. Navigeer naar **Beeld > Boom** en selecteer **OK** in de basis-DN.

						Idap)://V	/IN-4BD4NV0J3NK.Iabm.cisco.com/DC=Iabm,DC=cisco,DC=com
Connection B	Browse	View	Options	Utilities	Help			Tree View
			Tree			Ctrl+T		
			Enterprise (Configurat	ion			B . DV .
		\checkmark	Status Bar					BaseDN:
			Set Font					Cancel OK
							1	

Stap 4. Breid de structuur uit om de structuur te bekijken en te zoeken naar de zoekbasis DN. Bedenk dat het elk containertype kan zijn, behalve Groepen. Het kan het hele domein zijn, een specifieke OU of een CN zoals CN=User.



Stap 5. Breid de SofiaLabOU uit om te zien welke gebruikers er in zitten. Er is de Gebruiker1 die eerder is gemaakt.



ာင်း Cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Save Configuration Bing Logout Ret COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
 AAA General RADIUS Authentication Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Poriority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Local Policies Advanced 	Server Index (Priority) Server IP Address Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base DN User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1 V 10.88.173.121 289 Authenticated V (CN=Administrator,CN=Users,DC=labm,DC= 	Admin privileges required Where are we going to look for users? What Attribute are we looking for? Message from webpage Warning: LDAP can only be used with EAP-FAST, PEAP-GTC and EAP-TLS methods OK Cancel

Stap 7. Groepen zoals SofiaLabGroup kunnen niet worden gebruikt als een zoekopdracht-DN. Breid de groep uit en zoek naar de gebruikers erin, waar de eerder gemaakte Gebruiker1 moet zijnzoals getoond.

E - Active	e Directory Admini	strative Center • la	abm (local) 🕨				- 🗭 Manage Help
Active Directory <	labm (local) (16)						Tasks
Coverview Cover	Filter Filter Filter Filter Name Builtin Computers Domain Controllers Employees ForeignSecurityPrincipals Guests Infrastructure LostAndFound Managed Service Account	P (II) (II) (II) (II) (II) (II) (III) (IIII) (III) (IIII) (III) (I	SofiaLabGro Group Managed By Member Of Members Password Settings Extensions	UP Group name: * Sofia Group (SamAccountNam.* Sofia Group ype: © Security Distribution Protect from accidental deletion Managed By	LabGroup LabGroup Group scope: O Domain local Global Universal	E-mail: Description: Notes:	
	Program Data	msDS-QuotaContainer		Member Of			? ≋ ⊙
	SofiaLabGroup Group Group SofiaLabGroup Group System Container TPM Devices msTPM-InformationObjectsC Users Container SofiaLabGroup		Members Filter Name Activ Sofialab User1 Test User labor	P e Directory Domain Services Folder SofiaLabOU-SofiaLab User1 Test User		⑦ ⊗ ⊙ Add Remove	
	E-mail: Managed by:		 More Information 				OK Cancel

Gebruiker1 was er maar LDP kon het niet vinden. Het betekent dat de WLC niet in staat is om het ook te doen en dat is de reden waarom Groepen niet worden ondersteund als een Search Base DN.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

```
(cisco-controller) > show ldap summary
```

--- ----- -----

1 10.88.173.121 389 Yes No

(cisco-controller) >show ldap 1

Server Index	1
Address	10.88.173.121
Port	389
Server State	Enabled
User DN	OU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute	sAMAccountName
User Type	Person
Retransmit Timeout	2 seconds
Secure (via TLS)	Disabled
Bind Method	Authenticated
Bind Username	CN=Administrator,CN=Domain
Admins,CN=Users,DC=labm,DC=cisco,DC=com	

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

(cisco-controller) >debug client <mac address=""></mac>	
(cisco-controller) >debug aaa ldap enable	
(cisco-controller) >show ldap statistics	
Server Index Server statistics:	. 1
Initialized OK	С
Initialization failed	С
Initialization retries (С
Closed OK	С
Request statistics:	
Received	С
Sent	С
OK	С
Success	С
Authentication failed	С
Server not found	С
No received attributes	С
No passed username	0
Not connected to server	0
Internal error	n N
Detriog	n
NELTTED	J

Gerelateerde informatie

- LDAP WLC 8.2 configuratiehandleiding
- Hoe te om Draadloze LAN Controller (WLC) voor Lichtgewicht Directory Access Protocol (LDAP) verificatie te configureren - door Vinay Sharma
- Webverificatie met LDAP op configuratievoorbeeld van draadloze LAN-controllers (WLCs) door Yahya Jaber en Ayman Alfare

• <u>Technische ondersteuning en documentatie – Cisco Systems</u>

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.