Configurazione del WLC con autenticazione LDAP per le WLAN 802.1x e Web-Auth

Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Premesse Contesto tecnico Domande frequenti Configurazione Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite 802.1x Esempio di rete Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite il portale Web WLC interno Esempio di rete Utilizzare Lo Strumento LDP Per Configurare E Risolvere I Problemi Relativi A LDAP Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

In questo documento viene descritta la procedura per configurare un WLC di AireOS in modo da autenticare i client con un server LDAP come database utenti.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server Microsoft Windows
- Active Directory

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

Software Cisco WLC 8.2.10.0

Microsoft Windows Server 2012 R2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Contesto tecnico

- LDAP è un protocollo utilizzato per accedere ai server delle directory.
- I server di directory sono database gerarchici orientati agli oggetti.
- Gli oggetti sono organizzati in contenitori, ad esempio Unità organizzative (OU, Organizational Units), Gruppi o Contenitori Microsoft predefiniti, come CN=Users.
- La parte più difficile di questa configurazione è configurare correttamente i parametri del server LDAP sul WLC.

Per informazioni più dettagliate su questi concetti, fare riferimento alla sezione Introduzione di <u>Come configurare Wireless LAN Controller (WLC) per l'autenticazione LDAP (Lightweight</u> <u>Directory Access Protocol)</u>.

Domande frequenti

• Quale nome utente deve essere utilizzato per il binding al server LDAP?

Esistono due modi per eseguire l'associazione a un server LDAP: Anonimo o Autenticato (fare riferimento a per comprendere la differenza tra entrambi i metodi).

Il nome utente associato deve disporre dei privilegi di amministratore per poter eseguire query per altri nomi utente/password.

• Se autenticato: il nome utente di binding si trova nello stesso contenitore di tutti gli utenti? No: utilizza l'intero percorso. Ad esempio:

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

Sì: utilizzare solo il nome utente. Ad esempio:

Amministratore

Cosa succede se gli utenti si trovano in contenitori diversi? Tutti gli utenti LDAP wireless interessati devono trovarsi nello stesso contenitore?

No, è possibile specificare un DN di base che includa tutti i contenitori necessari.

• Quali attributi deve cercare il WLC?

II WLC corrisponde all'attributo utente e al tipo di oggetto specificati.

Nota: sAMAccountName fa distinzione tra maiuscole e minuscole, ma person non lo fa.

Pertanto, **sAMAccountName=RICARDO** e **sAMAccountName=ricardo** sono gli stessi e funzionano, a differenza di **samaccountname=RICARDO** e **samaccountname=ricardo**.

• Quali metodi EAP (Extensible Authentication Protocol) è possibile utilizzare? Solo EAP-FAST, PEAP-GTC e EAP-TLS. I supplicant predefiniti Android, iOS e MacOS funzionano con PEAP (Protected Extensible Authentication Protocol).

Per Windows, è necessario usare Anyconnect Network Access Manager (NAM) o il supplicant predefinito di Windows con Cisco:PEAP sulle schede wireless supportate, come mostrato nell'immagine.

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

Nota: i <u>plug-in EAP di Cisco</u> per Windows includono una versione di Open Secure Socket Layer (OpenSSL 0.9.8k) su cui ha effetto l'ID bug Cisco <u>CSCva09670</u>, Cisco non prevede di rilasciare altre versioni dei plug-in EAP per Windows e consiglia ai clienti di utilizzare AnyConnect Secure Mobility Client.

Perché il WLC non trova gli utenti?

Impossibile autenticare gli utenti all'interno di un gruppo. Devono trovarsi all'interno di un contenitore predefinito (CN, Default Container) o di un'unità organizzativa (OU, Organizational Unit), come mostrato nell'immagine.

	Name	Туре	Description
<u>.</u>	SofiaLabGroup	Group	will not work
-0	SofiaLabOU	Organizational Unit	
	Users	Container	Default container for upgr

Configurazione

Esistono diversi scenari in cui è possibile utilizzare un server LDAP, sia con l'autenticazione 802.1x sia con l'autenticazione Web.

Per questa procedura, è necessario autenticare solo gli utenti all'interno di OU=SofiaLabOU.

Per informazioni su come utilizzare lo strumento Label Distribution Protocol (LDP), configurare e risolvere i problemi relativi a LDAP, consultare la <u>guida alla configurazione di LDAP nel WLC</u>.

Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite 802.1x

Esempio di rete

In questo scenario, il protocollo LDAP-dot1x della WLAN utilizza un server LDAP per autenticare gli utenti con l'uso di 802.1x.



È Carlo de C	Server Manager	_ 0 ×
€ Server Ma	lanager • Dashboard	- ② 🏹 Manage Took View Help
Dashboard	WELCOME TO SERVER MANAGER	Active Directory Administrative Center Active Directory Domains and Trusts Active Directory Lightweight Directory Services Setup Wizard
Local Server All Servers AD CS	1 Configure this local server	Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers
AD DS	2 Add roles and features	ADSI Edit Certification Authority Component Services
■ DNS ■ File and Storage Services ▷	3 Add other servers to manage whats new 4 Create a server group	Computer Management Defragment and Optimize Drives DHCP
∎o IIS ¶∿ NAP		DNS Event Viewer Group Policy Management

Create User: SofiaLab User1 Test User

Create User: SofiaLab U	er1 Test User		TASKS 🔻	SECTIONS 🔻
Account Account				() × 🔊
Organization Member Of Password Settings Profile Policy Silo Password: Confirm password: Confirm password: Confirm password: Confirm password: Confirm password: Confirm password: Confirm password: This object will	sofialab User1 Test User Sofialab User1 Test User Sofialab User1 Test User Sofialab User1 Test User Sofialab User1 Test User Sofialab User1 Test User Sofialab User1 Sofialab Sofiala	Account expire:		* * * * * * * * * * *

Create User: SofiaLab User1 Test User

Create User:	SofiaLab User1	Test User		TASKS 🔻 SECTI	IONS 🔻
Account	Account			0	
Organization Member Of Password Settings Profile Policy Silo	First name: Middle initials: Last name: Full name: User UPN logon: User SamAccountName Io Password: Confirm password: Create in: OU=SofiaLabOU, Protect from accidental Log on hour	SofiaLab User1 Test User SofiaLab User1 Test User Isbm DC=labm,DC=cisco,DC=com Chan deletion Log on to	Account expires: Account expires: Account expires: End of Password options: User1 Password options: Smart card is required for interactive log on Password never expires Buser cannot change password Encryption options: Other options: Other options:		•
	Organization			0	
	Member Of		Select Groups	(
	Filter Name SofiaLabGroup	Active Director Primary labm-SofiaLab	Select this object type: Groups or Built neoutly principals From this location: ightm: class.com Enter the object names to select (scamples): IsodaLabGroup Check Names	I	Add Remove
	This object will be addeed	d to the default Active Directory gro Password Settings Precedence	Advanced OK Cancel	Q) & ©

Passaggio 2. Creare un profilo EAP sul WLC con il metodo EAP desiderato (utilizzare PEAP).

،، ،،، ،، cısco		MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS		s Y M <u>A</u> NAGEMENT	a <u>v</u> e Configuratio C <u>O</u> MMANDS	on <u>P</u> ing HE <u>L</u> P	Logout <u>R</u> efres <u>F</u> EEDBACK
Security	^	Local EA	P Profile	is				Ne	2W	Apply
 ▼ AAA General ▼ RADIUS 		Profile Nar	ne		LEAP	EAP-FAST	EAP-TLS	PEAP		
Authentication Accounting Fallback DNS		Local-EAP-P	EAP		✓				0	
DAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies		LE/ EA/ EA/	AP P-FAST P-TLS AP	Server Server Server	Nothing PAK Certific	C C cate C	lient Userna lient Userna lient Certif lient Userna	me & Pass me & Pass icate me & Pass	word	
Ceneral General Profiles EAP-FAST Parameters Authentication Priority	,			1 Server			iicht üserna	me & F833	u	

Passaggio 3. Associare il WLC al server LDAP.

Suggerimento: se il nome utente di associazione non si trova nel DN della base utente, è necessario scrivere l'intero percorso all'utente **Admin** come mostrato nell'immagine. In caso contrario, è sufficiente immettere **Administrator**.

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	Save Configuration Ping	Logout <u>R</u> efre
Security	LDAP Servers > New						< Back	Apply
 AAA General RADJUS Authentication Accounting Fallback DNS TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP 	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 10.68.173.121 389 Authenticated V CN=Administrator,CN=Use CN=Administrator,CN=Use CM=Administrator,CN=Use CM=Administrator,CN=Use SAMAccountName Person Disabled V 2 seconds Enabled V	rs,DC=labm,DC=	Admin	priv	Vileges required here are we going to hat Attribute are we Message from webpage Message from webpage Warning: LDAP can only be used w EAP-TLS methods	look for use looking for ith EAP-FAST, PEAP-GTC ar	ers?
Local Policies Advanced							OK Can	icel

Passaggio 4. Impostare l'ordine di autenticazione su Solo utenti interni + LDAP o LDAP.

،، ،،، ،، cısco		MONITOR	<u>w</u> lans	CONTROLLER	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	CAL	Up Down]
 Local EAP General Profiles EAP-FAST Parameters Authentication Priority 						-	

Passaggio 5. Creare la WLAN LDAP-dot1x.

uluilu cisco	Monitor <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
WLANs	Current Filter: None [Change Filter] [Clear Filter] Create New V Go
Advanced	WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies

،، ،،، ،، cısco	Monitor Wlans Controller Wireless Security Management Commands Help Feedback
WLANs	WLANs > Edit 'LDAP-dot1x'
WLANS WLANS Advanced	General Security QoS Policy-Mapping Advanced Profile Name LDAP-dot1x
	Radio PolicyAllInterface/Interface Group(G)Vlan2562Multicast Vlan FeatureEnabledBroadcast SSIDEnabledNAS-IDnone

Passaggio 6. Impostare il metodo di protezione L2 su WPA2 + 802.1x e la protezione L3 su none (nessuno).

cisco		<u>W</u> LANs <u>C</u> ON	TROLLER W	VIRELESS	SECURITY	MANAGEN
WLANs	WLANs >	Edit 'LDA	P-dot1x'			
WLANs WLANs	General	Security	QoS Po	olicy-Mappi	ing Adv	anced
Advanced	Layer 2	Layer 3	AAA Serve	ers		
	Layer 2	2 Security 🕯 🛛 🛛	/PA+WPA2	~		
	Fast Tran	MA	C Filtering]		
	Fast Trans	ition 🗌				
	Protected	l Management	Disabled	\checkmark		
	WPA+WP	A2 Parameter	s			
	WPA Po	olicy Policy				
	WPA2	Encryption	AES			
	Authentic	ation Key Man	agement			
	ССКМ	. <u> </u>	nable			
	PSK	1X 🗆	nable			
	FT PSK		Enable			
	WPA gt	tk-randomize St	Di	isable 🗸		

Passaggio 7. Abilitare l'autenticazione EAP locale e assicurarsi che le opzioni Server di autenticazione e Server di accounting siano disabilitate e che LDAP sia abilitato.

،، ،،، ،، cısco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> OI	NTROLLER W <u>I</u> RELESS	<u>s</u> ecurity m <u>a</u>	NAGEMENT COMMANDS	HE <u>L</u> P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LD/	AP-dot1x'			
WLANS WLANS	General Security	QoS Policy-Mappi	ing Advance	ed	
Advanced	Layer 2 Layer 3	AAA Servers			
	Select AAA servers bel	ow to override use of defa	ult servers on th	is WLAN	
	Radius Servers				
	Radius Server Overw	rite interface 🗌 Enabled			
	Authentication Servers	Accounting Servers		E	AP Parameters
		Enabled	Enable	d	Enable
	Server 1	None	✓ None	\sim	
	Server 2	None	✓ None	\checkmark	
	Server 3	None	✓ None	\checkmark	
	Server 4	None	✓ None	\sim	
	Server 5	None	✓ None	\checkmark	
	Server 6	None	✓ None	\checkmark	
	Radius Server Account	ing			
	Interim Update				
	LDAP Servers				
	Server 1 IP:10.88.	173.121, 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	ority order for web-aut	h user		
	Not Used			Order Used For Authe	ntication
			>	LOCAL	Up
			<	RADIUS	Down

Tutte le altre impostazioni possono essere lasciate in posizione predefinita.

Note:

Utilizzate lo strumento LDP per confermare i parametri di configurazione. La base di ricerca non può essere un gruppo, ad esempio SofiaLabGroup. Se si tratta di un computer Windows, è necessario utilizzare PEAP-GTC o Cisco:PEAP anziché Microsoft:PEAP nel supplicant. Microsoft:PEAP funziona per impostazione predefinita con MacOS/iOS/Android.

Creazione di una WLAN basata sul server LDAP per autenticare gli utenti tramite il portale Web WLC interno

Esempio di rete

In questo scenario, il protocollo LDAP-Web della WLAN utilizza un server LDAP per autenticare gli utenti con il portale Web WLC interno.

LDAP Server



Assicurarsi che i passaggi da 1 a 4 siano stati eseguiti dall'esempio precedente. Da qui, la configurazione WLAN è impostata in modo diverso.

Passaggio 1. Creare un utente **User1** nel membro Server LDAP dell'OU SofiaLabOU e del Gruppo SofiaLabGroup.

Passaggio 2. Creare un profilo EAP sul WLC con il metodo EAP desiderato (utilizzare PEAP).

Passaggio 3. Associare il WLC al server LDAP.

Passaggio 4. Impostare l'ordine di autenticazione su Internal Users + LDAP.

Passaggio 5. Creare la WLAN LDAP-Web come mostrato nelle immagini.

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

iiliiilii cisco	Monitor Wlans Controll	.er 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	o'				
WLANS	General Security Qo	S Policy-Mapping Ad	lvanced			
Advanced	Profile Name Type SSID Status Security Policies	LDAP-Web WLAN LDAP-Web Contemporal Enabled [WPA2][Auth(802.1X)] (Modifications done under secu	rity tab will appear a	after applying th	e change	es.)
	Radio Policy Interface/Interface Group(G) Multicast Vlan Feature Broadcast SSID NAS-ID	Vlan2562 V Enabled Ø Enabled none				

Passaggio 6. Imposta sicurezza L2 su nessuna e sicurezza L3 su criteri Web -Autenticazionecome mostrato nelle immagini.

uluili. cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
 WLANs Mdvanced 	General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Layer 2 Security None MAC Filtering? Fast Transition Fast Transition

،،ا،،،ا،، 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 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

Passaggio 7. Impostare l'ordine di priorità dell'autenticazione per l'autenticazione Web per utilizzare LDAP e assicurarsi che le opzioni Server di autenticazione e Server di accounting siano disattivate.

ululu 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 WLANS	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				
	Authoptication Convers				
	Server 1 None V None V				
	Server 2 None None				
	Server 3 None None None None None None None None None None None None None None None None				
	Server 4 None Non				
	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				
	Authentication priority order for web-auth user				
	Not Used Order Used For Authentication				
	RADIUS A > LDAP A Up				
	< LOCAL Down				

Tutte le altre impostazioni possono essere lasciate in posizione predefinita.

Utilizzare Lo Strumento LDP Per Configurare E Risolvere I Problemi Relativi A LDAP

Passaggio 1. Aprire lo strumento LDP sul server LDAP o su un host con connettività (la porta TCP 389 deve essere consentita al server).



Passaggio 2. Passare a **Connessione > Binding**, accedere con un utente Admin e selezionare il pulsante di opzione **Binding con credenziali**.

<u>83</u>				
Con	nection	Browse	View	0
	Connec	t		
Bind Ctrl+B				
	Disconn	ect		
	New		Ctrl+N	
	Save			
	Save As			
	Exit			

	Bind ×			
User:	Administrator			
Password:	••••••			
Domain:				
Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)				
 Encrypt traffic after bind 				
Advanced Cancel OK				

Passaggio 3. Passare a Visualizza > Albero e selezionare OK nel DN di base.

Connection Browse View Options Utilities Help	X
Tree Ctrl+T	
Enterprise Configuration	
Status Bar	
Set Font Cancel	ОК

Passaggio 4. Espandere la struttura per visualizzare la struttura e cercare il DN della base di ricerca. È possibile utilizzare qualsiasi tipo di contenitore, ad eccezione dei gruppi. Può trattarsi dell'intero dominio, di un'unità organizzativa specifica o di un CN come CN=Users.



Passaggio 5. Espandere SofiaLabOU per vedere quali utenti si trovano al suo interno. È presente l'utente 1 creato in precedenza.



.ılı.ılı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Save Configuration Ping Logout Bel COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
 AAA General RADUS Authentication Accounting Fallback DNS TACACS+ LOAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority 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 ▼ 10.88.173.121 389 Authenticated ✓ (Cl=Administrator,CN=Users,DC=labm,DCe •••••••• 0U=SofiaLabOU,DC=labm,DC=cisco,DC=com sAMAccountName Person Disabled ✓ 2 seconds Enabled ✓	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

Passaggio 7. Gruppi come SofiaLabGroup non possono essere utilizzati come DN di ricerca. Espandere il gruppo e cercare gli utenti al suo interno, dove l'utente 1 creato in precedenza deve esserecome illustrato.

€ → Active	Directory Administ	rative Center 🔸 la	abm (local) 🕨				• 🗊 Manage Help	
Active Directory <	labm (local) (16)						Tasks	
E TE Overview SofialabOU Users Dynamic Access Control Authentication P Global Search	Filter Name Builtin Computers Domain Controllers Employees ForeignSecurityPrincipals Control	B B B Container Organizational Unit Container Organizational Unit Container	SofiaLabGro Group Managed By Member Of Members Password Settings	UD Group Group name: Group (SamAccountNam* Group type: Security O Security	SofiaLabGroup SofiaLabGroup Group scope: O Domain local	E-mail: Description:		
	Guests Infrastructure LostAndFound Managed Service Accounts NTDS Quotas Program Data	Organizational Unit infrastructureUpdate lostAndFound Container msDS-QuotaContainer Container	Password Settings Extensions	Extensions	Extensions N	tensions Obstruction Obstruction Universal Universal Managed By Member Of	rotes:	
	SofiaLabGroup	Group Organizational Unit Container msTPM-InformationObjectsC Container		Members Filter Name Sofialab User1 Test User	Active Directory Domain Services Folder labm-SofiaLabOU-SofiaLab User1 Test User		① ⑧ ○ Add Remove	
	E-mail: Managed by:		More Information				OK Cancel	

L'utente 1 era presente ma LDP non è stato in grado di trovarlo. Significa che il WLC non è in grado di eseguire questa operazione e per questo motivo i gruppi non sono supportati come DN della base di ricerca.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

```
(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	

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

```
(cisco-controller) >debug client <MAC Address>
(cisco-controller) >debug aaa ldap enable
(cisco-controller) >show ldap statistics
Server Index..... 1
Server statistics:
Initialized OK..... 0
Initialization failed..... 0
Initialization retries..... 0
Closed OK..... 0
Request statistics:
Received...... 0
Sent......0
OK..... 0
Success..... 0
Authentication failed..... 0
Server not found...... 0
No received attributes..... 0
No passed username..... 0
Not connected to server.....
Internal error..... 0
```

Informazioni correlate

- LDAP Guida alla configurazione di WLC 8.2
- <u>Configurazione di Wireless Lan Controller (WLC) per l'autenticazione LDAP (Lightweight</u> <u>Directory Access Protocol) - di Vinay Sharma</u>
- Esempio di configurazione dell'autenticazione Web tramite LDAP sui Wireless LAN Controller

<u>(WLC) - di Yahya Jaber e Ayman Alfares</u> • <u>Documentazione e supporto tecnico – Cisco Systems</u>

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).