# 为 802.1x 和 Web-Auth WLAN 配置具备 LDAP 身份验证的 WLC

# 目录

简介 <u>先决条件</u> 要求 使用的组件 背景信息 技术背景 常见问题 配置 创建依赖LDAP服务器通过802.1x对用户进行身份验证的WLAN 网络图 创建依赖LDAP服务器通过内部WLC Web门户对用户进行身份验证的WLAN 网络图 使用LDP工具对LDAP进行配置和故障排除 验证 故障排除 相关信息

# 简介

本文档介绍配置AireOS WLC以使用LDAP服务器作为用户数据库对客户端进行身份验证的过程。

# 先决条件

要求

建议掌握下列主题的相关知识:

- Microsoft Windows服务器
- Active Directory

# 使用的组件

本文档中的信息基于以下软件版本:

- 思科WLC软件8.2.110.0
- Microsoft Windows Server 2012 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 背景信息

## 技术背景

•LDAP是用于访问目录服务器的协议。

- •目录服务器是分层的、面向对象的数据库。
- 对象以CN=Users形式组织到容器中,例如组织单位(OU)、组或默认Microsoft容器。
- 此设置最难的部分是在WLC上正确配置LDAP服务器参数。

有关这些概念的更多详细信息,请参阅<u>如何为轻量级目录访问协议(LDAP)身份验证配置无线局域网</u> 控制器(WLC)的简介部分。

#### 常见问题

•必须使用什么用户名与LDAP服务器绑定?

有两种方法可以与LDAP服务器绑定,即Anonymous或Authenticated(为了了解两种方法之间的区 别,请参阅)。

此绑定用户名需要具有管理员权限,才能查询其他用户名/密码。

•如果经过身份验证:绑定用户名是否与所有用户位于同一容器中? **不:使**用整个路径。例如:

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

**是:仅**使用用户名。例如:

#### 管理员

•如果用户位于不同的容器中怎么办?所有涉及的无线LDAP用户是否需要位于同一容器中? 否,可以指定包含所需所有容器的基本DN。

• WLC必须查找哪些属性?

WLC与指定的用户属性和对象类型匹配。

**注意:sAMAccountName**区分大小写,但person不区分大小写。因此 ,sAMAccountName=RICARDO和sAMAccountName=ricardo相同,并且工作正常,而 samaccountname=RICARDO和samaccountname=ricardo则不同。

• 可以使用哪种可扩展身份验证协议(EAP)方法?

仅EAP-FAST、PEAP-GTC和EAP-TLS。Android、iOS和MacOS默认请求方使用受保护的可扩展 身份验证协议(PEAP)。

对于Windows,必须在支持的无线适配器上使用Anyconnect网络访问管理器(NAM)或带有 Cisco:PEAP的默认Windows请求方,如图所示。

Local-EAP Wireless Netw	ork Properties
Connection Security	
Security type: Encryption type:	WPA2-Enterprise
Choose a network aut	hentication method:
Cisco: PEAP	<ul> <li>Settings</li> </ul>
Microsoft: Smart Card Microsoft: Protected E Cisco: LEAP	AP (PEAP) does not work!
Cisco: EAP-FAST Intel: EAP-SIM Intel: EAP-TTLS Intel: EAP-AKA	works:
Advanced settings	
	OK Cancel

注意:<u>Cisco EAP Plug-ins</u> for Windows包括受Cisco bug ID <u>CSCva09670</u>影响的开放安全套 接字层(OpenSSL 0.9.8k)版本,思科不计划发布任何其他版本的Windows EAP插件,并建议 客户改用AnyConnect安全移动客户端。

•为什么WLC找不到用户?

无法对组内的用户进行身份验证。它们需要位于默认容器(CN)或组织单位(OU)内,如图所示。

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

配置

有多种不同的方案可以采用LDAP服务器,包括802.1x身份验证或Web身份验证。

对于此过程,仅必须对OU=SofiaLabOU内的用户进行身份验证。

要了解如何使用Label Distribution Protocol(LDP)工具、配置并对LDAP进行故障排除,请参阅<u>WLC</u> LDAP配置指南。

## 创建依赖LDAP服务器通过802.1x对用户进行身份验证的WLAN

#### 网络图

在此方案中,WLAN LDAP-dot1x使用LDAP服务器使用802.1x对用户进行身份验证。



#### 步骤1:在SofiaLabOU和SofiaLabGroup的LDAP服务器成员中创建用户User1。



Create User:	SofiaLab User1	fest User		TASKS 🔻 SECTIONS 🔻		
Account	Account	Account				
Organization Member Of Password Settings Profile Policy Silo	First name: Middle initials: Last name: Full name: User UPN logon: Use SamAccountName own Password: Confirm password: Create in: DC alabam DC= cis Find in this column	SofiaLab User1 Test User SofiaLab User1 Test User SofiaLab User1 Test User SofiaLab User1  Test User SofiaLab User1  Test User	Account expires:	÷		
	d	ForeignSecurityPrincipa		?≈⊙		
	N	Guests LostAndFound		280		
	This object will be added	Managed Service Acco		Add Remove		

#### Create User: SofiaLab User1 Test User

Create User:	SofiaLab User1	Test User		TASKS 🔻	SECTIONS 🔻
Account	Account				•
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	SofiaLab User1 Test User SofiaLab User1 Test User Iabm DC=labm,DC=cisco,DC=com_Chan; deletion	Account expires:		•
	Log on hours	Log on to			
	Organization				? 🗙 👽
	Member Of		Select Groups		?× •
	Filter Name SofiaLabGroup	Active Director Primary Jabm-SofiaLab	Select this object type: Groups of Built in seculty principals From this location: Bither disco com Enter the object names to select ( <u>complete</u> ) Enter the object names to select ( <u>complete</u> ) Enter the object names to select ( <u>complete</u> ) Enter the object names to select ( <u>complete</u> )		Add Remove
	This object will be addee	I to the default Active Directory gro			
	Directly Associated	Password Settings	Advanced OK Cancel		• •
	Name	Precedence			Assign

# 第二步:使用所需的EAP方法在WLC上创建EAP配置文件(使用PEAP)。

،،۱۱،،۱۱، cısco	<u>M</u> ONITOR <u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	s: M <u>A</u> NAGEMENT	a <u>v</u> e Configuration     C <u>O</u> MMANDS HE	<u>Ping Logout R</u> efres <u>L</u> P <u>F</u> EEDBACK
Security	Local EAP Profile	95				New	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> </ul>	Profile Name Local-EAP-PEAP Local-EAP-LEAP			EAP-FAST	EAP-TLS	PEAP ✓ □ ✓	]
<ul> <li>TACACS+ LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul>	LEAP EAP-FAST EAP-TLS PFAP	Server   Server   Server	Nothing PAK Certific	C1:   C1: ate   C1: ate   C1:	ient Userna ient Userna ient Certif	me & Passwor me & Passwor icate me & Passwor	d d
Local EAP     General     Profiles     EAP-FAST Parameters     Authentication Priority	FEAP	l server		ate   CI.	tent Userna	ine a rasswor	u

**提示**:如果绑定用户名不在用户基础DN中,则必须将整个路径写入管理员用户,如图所示。 否则,您只需输入Administrator。

uluilu cisco	MONITOR WLANS CONTROLLER	W <u>i</u> reless <u>s</u> ecurity m <u>a</u> nagement	Saye Configuration Ping Logout Befr COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>DNS</li> </ul> </li> <li>TACACS+         <ul> <li>LOAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> </ul> </li> <li>Certificate</li> <li>Access Control         <ul> <li>Lists</li> <li>Wireless Protection             <ul> <li>Policies</li> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Local Policies</li> <li>Advanced</li> </ul> </li> </ul></li></ul>	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         389       ■         Authenticated ♥       ■         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

第四步:将Authentication Order设置为Internal Users + LDAP或仅LDAP。



## 第五步:创建LDAP-dot1x WLAN。

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

iiliiilii cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'LDAP-dot1x'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Profile Name       LDAP-dot1x         Type       WLAN         SSID       LDAP-dot1x         Status       ✓ Enabled         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 SSIDImage: EnabledNAS-IDnone

第六步:将L2安全方法设置为WPA2+802.1x,并将L3安全设置为none。

cisco	MONITOR	<u>W</u> LANs <u>C</u> ON	ITROLLER	WIRELESS	SECURITY	MANAGEN
WLANs	WLANs >	Edit 'LDA	P-dot1x'			
WLANs     WLANs	General	Security	QoS	Policy-Map	ping Ad	vanced
Advanced	Layer 2	Layer 3	AAA Ser	vers	1	
	Layer	MA	AC Filterings		]	
	Fast Tran	sition				
	Protecte	d Management	Frame			
	WPA+W	PA2 Parameter	Disable	ed 💙		
	WPA P	Policy				
	WPA2	Encryption	AES			
	Authenti	cation Key Mar	nagement			
	802.13 CCKM	X Ve	inable			
	PSK		nable			
	FT 802	2.1X	Enable			
	FT PS	K 🗌	Enable			
	WPA g 14	tk-randomize St	tate [	Disable 🗸		

步骤 7.启用本地EAP身份验证,并确保已禁用Authentication Servers和Accounting Servers选项并 启用LDAP。

uluili. cisco	<u>M</u> onitor <u>W</u> lans (	ONTROLLER WIRELE	ss <u>s</u> ecurity	M <u>A</u> NAGEMENT C <u>O</u> MMAND	S HE <u>L</u> P <u>F</u> EEDBACK				
WLANs	WLANs > Edit 'L	DAP-dot1x'							
WLANS WLANS	General Securit	y QoS Policy-	Mapping Adva	nced					
Advanced	Layer 2 Layer	3 AAA Servers							
	Select AAA servers	below to override use o	f default servers on	this WLAN					
	Radius Servers								
	Radius Server Ove	rwrite interface 🛛 Ena	bled						
	Authentication Serv	ers Accounting Server	s		EAP Parameters				
		Enabled	Enal	bled	Enable				
	Server 1	None	✓ None	~					
	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 Accou	inting							
	Interim Update								
	LDAP Servers								
	Server 1 IP:10.8	18.173.121, Port:389 🗸							
	Server 2 None	~							
	Server 3 None	~							
	Local EAP Authentic	ation							
	Local EAP Authenti	cation 🗹 Enabled							
	EAP Profile Name	Local-EAP-PEAP	$\sim$						
	Authentication p	riority order for wel	o-auth user						
	Not Us	ed		Order Used For Aut	hentication				
			>	LOCAL	Up				
			<	LDAP	Down				

所有其	他设置都可以保留为默认值。
<b>沪</b> 依 把 女 N	<b>注意:</b> 使用LDP工具确认配置参数。 搜索基础不能是组(如SofiaLabGroup)。 □果是Windows计算机,则必须在请求方使用PEAP-GTC或Cisco:PEAP,而不是 /icrosoft:PEAP。Microsoft:PEAP默认情况下适用于MacOS/iOS/Android。

# 创建依赖LDAP服务器通过内部WLC Web门户对用户进行身份验证的WLAN

## 网络图

在此方案中,WLAN LDAP-Web使用LDAP服务器通过内部WLC Web门户对用户进行身份验证。

# LDAP Server



确保已在上一个示例中执行了步骤1.到步骤4.。WLAN配置从此处设置的方式不同。

步骤1:在OU SofiaLabOU和组SofiaLabGroup的LDAP服务器成员中创建用户User1。

第二步:使用所需的EAP方法在WLC上创建EAP配置文件(使用PEAP)。

第三步:将WLC与LDAP服务器绑定。

第四步:将Authentication Order设置为Internal Users + LDAP。

第五步:创建LDAP-Web WLAN,如图所示。



iiliilii cisco	<u>M</u> onitor <u>w</u> lans <u>c</u> ontroll	er w <u>i</u> reless <u>s</u> ecurity	M <u>a</u> nagement C	C <u>o</u> mmands he <u>l</u> i	p <u>f</u> eedback
WLANs	WLANs > Edit 'LDAP-Web				
WLANS	General Security Qo	S Policy-Mapping Adva	anced		
Advanced	Profile Name Type SSID Status Security Policies Radio Policy Interface Group(G)	LDAP-Web WLAN LDAP-Web C Enabled [WPA2][Auth(802.1X)] (Modifications done under security All Vlan2562	y tab will appear afte	er applying the chan	iges.)
	Multicast Vlan Feature Broadcast SSID NAS-ID	<ul> <li>■ Enabled</li> <li>✓ Enabled</li> <li>none</li> </ul>			

第六步:将L2 Security设置为none,将L3 Security设置为Web Policy - Authentication如图所示。

uluulu 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 HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'LDAP-Web'
<ul> <li>WLANs</li> <li>Mdvanced</li> </ul>	General       Security       QoS       Policy-Mapping       Advanced         Layer 2       Layer 3       AAA Servers         Layer 2       Security       None       T         MAC       Filtering       T         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 IPv6 None WebAuth FlexAcl None Sleeping Client Enable Over-ride Global Config 20 Enable Web Auth type Internal

步骤 7. 将Web-auth的身份验证优先级顺序设置为使用LDAP,并确保已禁用Authentication Servers和Accounting Servers选项。

ດປາດປາດ 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'
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
	Enabled Enabled
	Server 1 None V None V
	Server 2 None  V None  V
	Server 3 None   None
	Server 4 None V None V
	Server 5 None V None V
	Interim Update
	LDAP Servers
	Server 1 [IP:10.88.173.121, Port:389
	Server 2 None
	Local FAR Authentication
	Local EAP Authentication Enabled
	Authentication priority order for web-auth ucor
	Not Used Order Used For Authentication
	RADIUS A Vp
	V COCAL V Down

## 使用LDP工具对LDAP进行配置和故障排除

步骤1:在LDAP服务器或具有连接性的主机上打开LDP工具(必须允许到服务器的端口TCP 389)。



第二步: 导航到Connection > Bind,使用Admin用户登录,然后选择Bind with credentials单选按钮

裔			
Connection	Browse	View	0
Connect	t		
Bind		Ctrl+B	
Disconn	ect		
New		Ctrl+N	
Save			
Save As			
Exit			

0

	Bind
User:	Administrator
Password:	•••••
Domain:	
Bind type Bind as cu Bind with Simple bin Advanced	rrently logged on user credentials d (DIGEST)
<ul> <li>Encrypt tr</li> </ul>	affic after bind
Advanced	Cancel OK

## 第三步:导航到View > Tree,然后在基本DN中选择OK。

12000			_			ldap	://\	/IN-4BD4NV0J3NK.Iabm.cisco.com/DC=Iabm,DC=cisco,DC=com
Connection	Browse	View	Options	Utilities	Help			Tree Man
			Tree			Ctrl+T		Tree View
			Enterprise (	Configurat	ion			
		$\checkmark$	Status Bar					BaseDN:
			Set Font					Cancel OK

第四步:展开树以查看结构并查找Search Base DN。请考虑它可以是除"组"之外的任何容器类型。 它可以是整个域、特定OU或类似CN=Users的CN。



## 第五步:展开SofiaLabOU以查看其中的用户。这是之前创建的User1。

1 Idap://WIN-4BD	4NV0J3NK.labm.cisco.com/DC=labm,DC=cisco,DC=com	_		x
Connection Browse View Options Utilities Help				
■ DC=labm,DC=cisco,DC=com     ON=Builtin,DC=labm,DC=cisco,DC=com     ON=Computers,DC=labm,DC=cisco,DC=com     OU=Domain Controllers,DC=labm,DC=cisco,DC=com     OU=Employees,DC=labm,DC=cisco,DC=com     OU=Guests,DC=labm,DC=cisco,DC=com     ON=lnfrastructure,DC=labm,DC=cisco,DC=com     ON=LostAndFound,DC=labm,DC=cisco,DC=com     ON=Nanaged Service Accounts,DC=labm,DC=cisco,DC=com     ON=Yorgam Data,DC=labm,DC=cisco,DC=com     OU=SofiaLabGroup,DC=labm,DC=cisco,DC=com     OU=SofiaLabGU,DC=labm,DC=cisco,DC=com     ON=System,DL=labm,DC=cisco,DC=com     ON=System,DL=labm,DL=cisco,DL=labm,DL=labm,DL=cisco,DL=labm,DL=labm,DL=cisco,DL=com     ON=System,DL=labm,DL=cisco,DL=com	Expanding base 'OU=SofiaLabOU,DC=labm,DC=cisco,DC=com' Getting 1 entries: Dr: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com; distinguishedName: OU=SofiaLabOU,DC=labm,DC=cisco,DC=com; dSCorePropagationData (2): 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); 0x0 = ( ); instanceType: 0x4 = (WRITE ); name: SofiaLabOU; objectClass (2): 10p; organizational-Unit,CN=Schema,CN=Configuration,DC=labm,DC=cisco,DC=com; objectClass (2): 10p; organizational-Unit, objectClass (2): 10p; organizational-Unit,CN=Schema,CN=Configuration,DC=labm,DC=cisco,DC=com; objectClass (2): 10p; organizational-Unit, ou: SofiaLabOU; uSNChanged: 45117; uSNCreated: 45116; whenChanged: 8/10/2016 4:22:39 PM Central Daylight Time (Mexico); whenCreated: 4510/2016 4:22:39 PM Central Daylight Time (Mexico); bit to the tot user; codelPage: 0; country/Claber 200; country/Claber 200; country/Cla			Ш
< III >				~
Ready		NU	M	

ı. cısco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY MANAGEMENT	Sage Configuration Ping Logout Bel COMMANDS HELP FEEDBACK
Security	LDAP Servers > New		< Back Apply
<ul> <li>AAA</li> <li>General</li> <li>RADUS</li> <li>Authentication</li> <li>Accounting</li> <li>Falback</li> <li>DNS</li> <li>TACACS+</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> <li>Password Policies</li> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control</li> <li>Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Local Policies</li> <li>Advanced</li> </ul>	Server Index (Priority) Server IP Address Port Number Simple Bind Bind Username Bind Password Confirm Bind Password User Base ON User Attribute User Object Type Secure Mode(via TLS) Server Timeout Enable Server Status	1     Image: Constraint of the second s	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

步骤 7.SofiaLabGroup等组不能用作搜索DN。展开组并查找组内的用户,其中之前创建的User1必 须是如所示.

€ → Active	Directory Administrative Center •	abm (local) •	▼ ②   Manage Help
Active Directory  Active  Active Directory   Coverview  SofialabOU Users  Dynamic Access Control  Authentication  Global Search	Directory Administrative Center         Iabm (local) (16)         Filter       P       B       ●       ●         Builtin       builtinDomain       Container         Computers       Organizational Unit       Employees       Organizational Unit         ForeignSecurityPrincipals       Container       Guests       Organizational Unit         Infrastructure       InfrastructureUpdate       IostAndFound       IostAndFound         Managed Service Accounts       Container       Container         Program Data       Container       SofialabSroup       Group         SofialabCou       Granizational Unit       System       Container         TPM Devices       msTPM-InformationObjecti       Users       Container	SofiaLabGroup         Group         Managed By         Member Of         Members         Password Settings         Extensions         Extensions         Managed By         Member Of         Members         Password Settings         Extensions         Extensions         Member Of         Member Of         Member Of         Member Of         Member Of         Member Of         Member S         Sofialab User Test User         Liber Sofialab Out-Sofialab Out-Sofialab User Test User	Tasks
	SofiaLabGroup E-mail:	More Information	OK Cancel

User1曾在那里,但LDP找不到它。这意味着WLC无法同样执行此操作,因此不支持将组用作搜索库DN。

# 验证

使用本部分可确认配置能否正常运行。

(cisco-controller) > show ldap summary

Idx Server Address Port Enabled Secure

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

1 10.88.173.121 389 Yes No

#### (cisco-controller) > show ldap 1

Server Index 1	
Address 10	0.88.173.121
Port	89
Server State Er	Inabled
User DN OU	DU=SofiaLabOU,DC=labm,DC=cisco,DC=com
User Attribute sA	AMAccountName
User Type Pe	Person
Retransmit Timeout 2	seconds
Secure (via TLS) Di	Disabled
Bind Method Au	authenticated
Bind Username CN	N=Administrator,CN=Domain
Admins,CN=Users,DC=labm,DC=cisco,DC=com	

# 故障排除

## 本部分提供的信息可用于对配置进行故障排除。

(cisco-controller) >debug client <mac address=""></mac>
(cisco-controller) >debug aaa ldap enable
(cisco-controller) >show ldap statistics
Server Index
Initialized OK0
Initialization failed0
Initialization retries0
Closed OK 0
Request statistics:
Received
Sent0
ок0
Success0
Authentication failed 0
Server not found 0
No received attributes 0
No passed username 0
Not connected to server 0
Internal error 0
Retries

# 相关信息

- <u>LDAP WLC 8.2配置指南</u>
- <u>如何为轻量级目录访问协议(LDAP)身份验证配置无线局域网控制器(WLC)- Vinay Sharma</u>
- <u>在无线局域网控制器(WLC)上使用LDAP的Web身份验证配置示例 Yahya Jaber和Ayman</u> <u>Alfares</u>
- <u>技术支持和文档 Cisco Systems</u>

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。