# **Configurer l'authentification LDAP ACI**

## Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Configurations
Étape 1. Créer des groupes/utilisateurs sur Ubuntu phpLDAPadmin
Étape 2. Configuration des fournisseurs LDAP sur APIC
Étape 3. Configurer les règles de mappage de groupe LDAP
Étape 4. Configurer les mappages de groupe LDAP
Étape 5. Configurer la stratégie d'authentification AAA
Vérifier
Dépannage
Informations connexes

## Introduction

Ce document décrit comment configurer l'authentification LDAP (Lightweight Directory Access Protocol) de l'infrastructure axée sur les applications (ACI).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Politique AAA (Authentication, Authorization, and Accounting) de l'ACI
- LDAP

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur Cisco APIC (Application Policy Infrastructure Controller) version 5.2(7f)
- Ubuntu 20.04 avec slapd et phpLDAPadmin

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configurer

Cette section décrit comment configurer le contrôleur APIC afin de l'intégrer au serveur LDAP et utiliser LDAP comme méthode d'authentification par défaut.

### Configurations

Étape 1. Créer des groupes/utilisateurs sur Ubuntu phpLDAPadmin



Remarque : Pour configurer Ubuntu en tant que serveur LDAP, reportez-vous au site Web officiel d'Ubuntu pour obtenir des instructions détaillées. S'il existe un serveur LDAP, commencez à l'étape 2.

Dans ce document, le DN de base est dc=dclab,dc=com et deux utilisateurs (User1 et User2) appartiennent à des groupes (DCGroup).



Étape 2. Configuration des fournisseurs LDAP sur APIC

Dans la barre de menus du module APIC, accédez à commeAdmin > AAA > Authentication > LDAP > Providers indiqué dans l'image.

Authentication							0
			AAA LDAP	RADIUS TACACS SAML	RSA	DUO	OAuth 2
				Providers LDAP Group M	ap Rules	LDAP Gr	bup Maps
						0	÷ %-
Host Name	Description	Port	SSL Enabled	Timeout (sec)			
10.124.3.6		389	False	30			
LDAP Provider - 10.1	124.3.6					Q	
				Policy	Faults	Histor	
					-		
					C	) <u>-</u> 7	<.
Host Name (or IP Address):	10.124.3.6						
Description	optional						
Port	389						
Bind DN:	cn+admin,dc+dclab,dc+com						
Base DN:	ou=Users,dc=dclab,dc=com						
Password:							
Contirm Password:							
Datriac	30						
Enable SSL:							
Filter	cn+\$userid						
Attribute:	title						
SSL Certificate Validation Level:	Permissive Strict						
Management EPG:	default (Out-of-Band) 🗸 😫						
Server Monitoring:	Disabled Enabled						

Bind DN : le DN de liaison est les informations d'identification que vous utilisez pour vous authentifier auprès d'un LDAP. Le contrôleur APIC s'authentifie à l'aide de ce compte pour interroger le répertoire.

Base DN : cette chaîne est utilisée par le contrôleur APIC comme point de référence pour la recherche et l'identification des entrées utilisateur dans le répertoire.

Password : mot de passe requis pour le DN de liaison nécessaire pour accéder au serveur LDAP, en corrélation avec le mot de passe établi sur votre serveur LDAP.

Enable SSL : si vous utilisez une autorité de certification interne ou un certificat auto-signé, vous devez choisir Permissive.

Filtre : le paramètre de filtre par défaut est cn=\$userid lorsque l'utilisateur est défini en tant qu'objet avec un nom commun (CN), le filtre est utilisé pour rechercher les objets dans le DN de base. Attribut : l'attribut est utilisé pour déterminer l'appartenance au groupe et les rôles. L'ACI offre deux options ici : memberOf et CiscoAVPair.memberOf est un attribut RFC2307bis afin d'identifier l'appartenance au groupe. Actuellement, OpenLDAP vérifie RFC2307, donc title est utilisé à la place.

Groupe de terminaux de gestion (EPG) : la connectivité au serveur LDAP est assurée par le groupe de terminaux de gestion (EPG) intrabande ou hors bande, en fonction de l'approche de gestion du réseau choisie.

Étape 3. Configurer les règles de mappage de groupe LDAP

Dans la barre de menus, accédez à Admin > AAA > Authentication > LDAP > LDAP Group Map Rules comme indiqué dans l'image.

Authentication		0
		AAA LDAP RADIUS TACACS SAML RSA DUO OAuth 2
		Providers LDAP Group Map Rules LDAP Group Maps
		0 ± %.
* Name	Description	Group DN
LDAPGroupMapRule		cn+DCGroup,ou+Groups,dc+dclab,dc+com
LDAP Group Map Rule - LDAPGroupMapRule	Po	C C
		0 ± **-
Properties Name: L0APOroupMapRule Description: optional Group DN: cn+DCGroup,oe+Groups,dc+dclab,dc+co Societh Domains		
Name	Access	0 +
Security Domain all	110000	
Role admin	writePriv	
	Show Usage Close	Submit

Les utilisateurs de DCGroup disposent de privilèges d'administrateur. Par conséquent, le DN du groupe cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aattribue le domaine de sécurité à All et alloue les rôles de admin avec write privilege .

Étape 4. Configurer les mappages de groupe LDAP

Dans la barre de menus, accédez à Admin > AAA > Authentication > LDAP > LDAP Group Maps comme indiqué dans l'image.

Authentication									0
		AAA	LDAP	RADIUS	TACACS	SAML	RSA D	UO OAuth	2
				Provid	ers LDAI	P Group Map I	Rules L	DAP Group Maj	ps
								0 ± :	%-
^ Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	00								
	Policy History								
	0 ± %.								
Properties									
Description: optional									
Nules:	U +								
LDAPGroupMapRule									
	Show Usage Close Submit								

Créez un mappage de groupe LDAP contenant les règles de mappage de groupe LDAP créées à l'étape 2.

Étape 5. Configurer la stratégie d'authentification AAA

Dans la barre de menus, accédez à Admin > AAA > Authentication > AA	AA > Policy >	Create a login domaincomme	indiqué dans l'image.
---	---------------	----------------------------	-----------------------

Authentication								Q
	AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
						Policy	Faults	History
							0	± %-
Properties Remote user login policy: [No Login  UbsectMP reachable [rough]								
providers only: Low P								
LDAP Login Domain: LDAP								
Falback Domain Availability: Always Available								
Console Authentication								
Hearn: Local								
								0
								1
Name Description	Realm							Z
falback	Local							
Login Domain - LDAP	LDAP							
Policy Histo	у							
0 ± 1	K-							
Properties								
Name: LDAP								
Description: Optional								
besugnes. optioner								
Auth Choice: Clisco/WPair LdspGroupMap								
LDAP Group Map: LDAP Group Map								
Providers: 🕆 +								
Name Priority Description								
10.124.3.6 1								
Show Usage Close Submit						Res	set	Submit

Dans la barre de menus, accédez à Admin > AAA > Authentication > AAA > Policy > Default Authentication comme indiqué dans l'image.

Authentication												Q
					AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
										Policy	Faults	History
											Ó	± %-
Properties Remote user login policy: Use ICMP reachable providers only: Default Authentication Realm: LDAP Login Domain: Fallback Domain Avalability: Console Authentication Realm:	No Login v true v LDAP v LDAP v LANP v Always Available v Local v	4										
												0
												+
<ul> <li>Name</li> </ul>			Description		Realm							
fallback					Local							
LDAP					LDAP							

Remplacez l'authentification par défaut Realm par LDAP et sélectionnez LDAP Login Domain créé.

#### Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

	User ID	
APIC	User1 Password	
Version 5.2(7f)	•••••	
າປານປານ cisco	Domain LDAP ~	

cisco APIC				User1	90%	0	00
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations						
Contrary Upship	united in country and the control of the country	Fault C	aunte hu Damain		-		
Zoom 1H 1D All		Padit Co	vowledged Faults	Hide Delegated Fax	its	~	0
	APIC		IDE	1	0	0	2
0.005	What's New in 5.2(7f)			0	0	0	0
Nc	ACI Fabric Software UI Enhancements			0	0	0	0
	Onboard ACI fabrics to Nexus Cloud for Inventory, anomaly, and assurance information     Simplified workflows for Migration to simplified	or fabric and access policies workflows for fabric and		1	0	0	1
	Simplified migration from Gen1 Nexus switches to access policies     Gen2 CloudScale platforms     Enhanced ACI Fabric Si	Setup	nt	0	0	0	0
	Sunnast Catting Started Evalue			0	0	0	0
	Online Help What's new in 5.2(7f) Configu	uration Guides		0	0	0	0
Nodes with Health = 99	Troubleshooting Online Videos (YouTube'') Configuration Examples and Documentation View All Tutorial Videos TechNotes	otes					
- Name Pod ID	APIC Communities		ints by Type	Hide Delegated Fa	Hide Delegated Faults		
			Anna Ogeo Faana	0	0	٥	0
Tenants with Health ≤ 99	It looks like this is your first time logging into APIC. Let's go through some of the basics to get you up and running.	Start ACI Fabric Setup	ations	0	0	0	0
- Name			stal	0	0	0	1
				1	0	0	1
			r Status				
			Jame	IP Admin State	/perational itate	Healt	h State
		1	apic1	10.0.0.1 In Service	Available	Fully F	a

Vérifiez que l'utilisateur LDAP se connecteUser1 au contrôleur APIC avec le rôle admin et le privilège d'écriture.

#### Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Lorsque l'utilisateur n'existe pas dans la base de données LDAP :

			User ID			
	APIC		Password			
1 1	Version 5.2(7f)		Domain		1	
	ւլիւլիւ cisco	Login Error	cation DENIED Login	~		
			ĸ			

Lorsque le mot de passe est incorrect :

APIC Version 5.2(7f) Login Error Uluit LDAP/AD Server Denied au	User ID Password eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

#### Lorsque le serveur LDAP est inaccessible :

APIC	Us Pa	ser ID		
Version 5.2(7f) ۱۱/۱۰۱/۱۰ دisco	Ogin Error DAP/AD failed to bind to an	y servers	1	1
	- 3- 11			

Dépannage des commandes:

#### <#root>

apic1# moquery -c aaaLdapProvider Total Objects shown: 1 # aaa.LdapProvider name : 10.124.3.6 SSLValida

Si vous avez besoin d'aide, contactez le TAC Cisco.

Informations connexes

- <u>Guide de configuration de la sécurité Cisco APIC, version 5.2(x)</u>
- <u>Assistance technique de Cisco et téléchargements</u>

### À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.