ACI LDAP 인증 구성

목차

소개

이 문서에서는 ACI(Application Centric Infrastructure) LDAP(Lightweight Directory Access Protocol) 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ACI AAA(Authentication, Authorization, and Accounting) 정책
- LDAP

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco APIC(Application Policy Infrastructure Controller) 버전 5.2(7f)
- Ubuntu 20.04(slapd 및 phpLDAPadmin 사용)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 섹션에서는 LDAP 서버와 통합하고 기본 인증 방법으로 LDAP를 사용하기 위해 APIC를 구성하 는 방법에 대해 설명합니다.

설정

1단계. Ubuntu phpLDAPadmin에서 그룹/사용자 생성



참고: Ubuntu를 LDAP 서버로 구성하려면 공식 Ubuntu 웹 사이트에서 종합적인 지침을 참 조하십시오. 기존 LDAP 서버가 있는 경우 2단계로 시작합니다.

이 문서에서 기본 DN은dc=dclab,dc=com 이며 두 사용자(User1 및 User2)가 그룹(DCGroup)에 속합니다.





2단계. APIC에서 LDAP 제공자 구성

APIC 메뉴 모음에서 그림과 같이 로Admin > AAA > Authentication > LDAP > Providers 이동합니다.

Authentication					Q
			AAA LDAI	P RADIUS TACACS SAM	L RSA DUO OAuth 2
				Providers LDAP Group	Map Rules LDAP Group Maps
					0 + %-
Host Name	Description	Port	SSL Enabled	Timeout (sec)	
10.124.3.6		389	False	30	
LDAP Provider - 10.	.124.3.6			Pol	icy Faults History
					0 ± %-
Properties Host Name (or IP Address) Description Biol DM Base DM Passwor Confirm Passwor Confirm Passwor Timeout (ec) Retrie Enable SS Enable SS Fite SSL Certificate Validation Leve Management EPO Server Monitoring	i: 10.124.3.6 fc fc fc i: 0.124.3.6 fc fc <td></td> <td></td> <td></td> <td></td>				

바인드 DN: 바인드 DN은 LDAP에 대해 인증하기 위해 사용 중인 자격 증명입니다. APIC는 이 계정을 사용하여 디렉터리를 쿼리합니다.

Base DN: 이 문자열은 APIC에서 디렉토리 내의 사용자 항목을 검색하고 식별하기 위한 참조 지점으로 사용됩니다.

비밀번호: LDAP 서버에 액세스하는 데 필요한 바인드 DN의 필수 비밀번호이며, LDAP 서버에 설정된 비밀번호와 상관관계가 있습니다.

SSL 활성화: 내부 CA 또는 자체 서명 인증서를 사용하는 경우 허용을 선택해야 합니다.

필터: 기본 필터 설정은 사용자를 CN(Common Name)의 개체로 정의할 때 필터를 사용하여 기본 DN 내에서 개체를 찾는 것입니다 cn=\$userid.

속성: 속성은 그룹 멤버십 및 역할을 결정하는 데 사용됩니다. ACI는 여기에 두 가지 옵션을 제공합니다. memberOf CiscoAVPair.memberOf

은 그룹 멤버십을 식별하기 위한 RFC2307bis 특성입니다. 현재 OpenLDAP는 RFC2307을 확인하므로 title 대신 사용됩니다.

EPG(Management Endpoint Group): 선택한 네트워크 관리 방식에 따라 대역 내(In-band) 또는 대역 외(Out-of-band) EPG를 통해 LDAP 서버에 연결합니다.

3단계. LDAP 그룹 맵 규칙 구성

메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > LDAP > LDAP Group Map Rules 대로 이동합니다.

Authentication												Q
					AAA	LDAP	RADIUS	TACACS	SAML	RSA E	000 0	Auth 2
							Provider	s LDA	P Group Ma	p Rules	DAP Grou	p Maps
											0 :	. %-
▲ Name		Description			Group	DN						
LDAPGroupMapRule					cn=D0	CGroup,ou=Gro	ups,dc=dclab,dc=c	em -				
LDAP Group M	lap Rule - LDAPGroupMapRule		Policy	N & History								
			Ó	± %-								
Properties Name Description Group DN	LDAPGroupAupBule optional en=DCGroup.ou+Groups.de=dclab.de=co											
Security Domains				0 +								
	Name	Access										
	Role admin	writePriv										
		Show U	Usage Close									

DCGroup의 사용자는 관리자 권한을 갖습니다. 따라서 그룹 DN은 cn=DCGroup, ou=Groups, dc=dclab, dc=com. A에 대한 역할을 All할 당하도록 보안 도메인을admin write privilege지정합니다.

4단계. LDAP 그룹 맵 구성

메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > LDAP > LDAP Group Maps 대로 이동합니다.

Authentication									0
		AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
				Prov	iders L	DAP Group Ma	p Rules	LDAP G	roup Maps
								0	± %-
^ Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	08								
	Policy History								
	0 ± %-								
Properties									
Description: optional									
Rufes:	* +								
Name									
LDAPGroupMapRule									
•									
	*								
	Show Usage Close Subjille								

2단계에서 생성한 LDAP 그룹 맵 규칙을 포함하는 LDAP 그룹 맵을 생성합니다.

5단계. AAA 인증 정책 구성

메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > AAA > Policy > Create a login domain대로 이동합니다.

Authentication										C
				AAA LD	AP RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
								Dolicy	Enulte	History
								roacy	rouits	1 46
Dreparties									0	- X*
Remote user login policy: No Login										
Use ICMP reachable true										
Default Authentication										
Realm: LDAP										
LDAP Login Domain: LDAP	S 🖉									
Fallback Domain Availability: Always Available										
Console Authentication										
Contraction of the second seco										
										0
										+
 Name 		Description		Realm						N
fallback				Local						-
Login Domain - LDAP			00	LDAP						
			Policy History							
			() + K							
Properties			0 - ^+							
Name: LDAP			×							
Description: Optional										
Auth Choice: ClscoAVPair	LdapGroupMap									
LDAP Group Map: LDAPGroupMap	 C 									
Providers:		≅ +								
Name	 Priority 	Description								
10.124.3.6	1									
		Show Usage	Close Submit					_		_
								Re	set	Submit

메뉴 모음에서 이미지에 표시된 Admin > AAA > Authentication > AAA > Policy > Default Authentication 대로 이동합니다.

Authentication							Q
			LDAP RADIUS	TACACS SA	ML RSA	DUO	OAuth 2
					Policy	Faults	History
						Ó	± %-
Properties Remote user login policy: No Login Use ICMP reachable providers only Imue Default Authentication Ream: LDAP Login Domini: LDAP Falback Domain Analability: Always Available Console Authentication Ream: Ream: Local	4						
							Q
							+
* Name	Description	Realm					
fallback		Local					
LDAP		LDAP					

기본 인증을 LDAPRealm로 변경하고 created를 LDAP Login Domain 선택합니다.

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

	User ID	
	User1	
APIC	Password	
Version 5.2(7f)	••••••	
	Domain	
սիսիս	LDAP ~	1
CISCO	Login	

dialo APIC			User1	00	}0	00
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations					
Quokstart Deinboard Contoers System settings Smart Loensing Paul	I History Contrigizones Active Sessions Security					
System Health		Fault Counts by Domain				
Zoom TH 1D AI		owledged Faults	Hide Delegated	Faults	٥	0
	S APIC	106	1	0	0	2
au oo	What's New in 5.2(7f)		¢	0	0	0
-	Ne		0	0	0	1
	ACI Fabric Software UI Enhancements UI Enhancements Simplified workflows for fabric and access p	policies		0	0	1
	anomaly, and assurance information Simplified migration from Gen1 Nexus switches to access policies	and		0	0	Ó
	Gen2 CloudScale platforms Enhanced ACI Fabric Setup		c	0	0	0
	Support Getting Started Explore		0	0	0	0
	Online Help What's new in 5.2(7I) Configuration Guides Troubleshooting Online Videos (YouTube") Configuration Examples and		c	0	0	0
Nodes with Health ≤ 99	Documentation View All Tutorial Videos APIC Communities	and a first Transm				
 Name Pod ID 		ints by Type		Lists Delegated Facility		
		- Nemeogeo Fasica	C 100 000 000	0	٥	0
T	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 S	Setup	0	0	0	0
lenants with Health # 99			0	0	0	1
* Name		vtal	c	0	0	0
			1	0	0	1
		r Status				
		Jame	IP Admin State	Operational State	Healt	th State
		1 apic1	10.0.0.1 In Service	Available	Fully I	Fit

LDAP 사용자가 관리자 역할User1 및 쓰기 권한으로 APIC에 성공적으로 로그인했는지 확인합니다.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

사용자가 LDAP 데이터베이스에 없는 경우:

			User ID			
	APIC		Password			
1 1	Version 5.2(7f)		•••••		1	
			Domain			
	 cisco	Login Error	×	×		
		AAA Server Authenti	cation DENIED Login	n		
		•	ĸ			
		19				

암호가 올바르지 않은 경우:

APIC Version 5.2(7f)	User ID Password
Login Error LDAP/AD Server Denied a	authentication

LDAP 서버에 연결할 수 없는 경우:

		User ID		
APIC		Password		
 Version 5.2(71	F)	•••••		
	Login Error		1	
າປານປາ cisco	LDAP/AD failed to bind	Login		
	1.5			

문제 해결 명령:

<#root>

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

추가 지원이 필요한 경우 Cisco TAC에 문의하십시오.

관련 정보

- <u>Cisco APIC 보안 컨피그레이션 가이드, 릴리스 5.2(x)</u>
- <u>Cisco 기술 지원 및 다운로드</u>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.