ACI LDAP-verificatie configureren

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Configureren Configuraties Stap 1. Groepen/gebruikers maken op Ubuntu phpLDAPadmin Stap 2. LDAP-providers op APIC configureren Stap 3. Regels voor LDAP-groepstoewijzing configureren Stap 4. LDAP-groepkaarten configureren Stap 5. AAA-verificatiebeleid configureren Stap 5. AAA-verificatiebeleid configureren

Inleiding

Gerelateerde informatie

Dit document beschrijft hoe u LDAP-verificatie (Application Centric Infrastructure) (ACI) kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ACI-beleid voor verificatie, autorisatie en accounting (AAA)
- LDAP

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Application Policy Infrastructure Controller-controller (APIC) versie 5.2(7f)
- Ubuntu 20.04 met slip en phpLDAPadmin

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.

Configureren

In dit deel wordt beschreven hoe APIC kan worden geconfigureerd om met de LDAP-server te integreren en LDAP als de standaardverificatiemethode te gebruiken.

Configuraties

Stap 1. Groepen/gebruikers maken op Ubuntu phpLDAPadmin



Opmerking: Raadpleeg de officiële Ubuntu-website voor uitgebreide richtlijnen om Ubuntu als LDAP-server te configureren. Als er een bestaande LDAP-server is, start dan met Stap 2.

In dit document, basis-DN is dc=dclab,dc=com en twee gebruikers (Gebruiker1 en Gebruiker2) behoren tot Groepen (DCGroup).





Stap 2. LDAP-providers op APIC configureren

$Navigeer \ in \ de \ APIC-menubalk \ naar \ Admin > AAA > Authentication > LDAP > Providers \ zoals \ in \ de \ afbeelding.$

Authentication						0
			AAA LDAP	RADIUS TACACS SAML	RSA DUO OA	uth 2
				Providers LDAP Group M	Map Rules LDAP Group N	Maps
					⊙ ±	*
Host Name	Description	Port	SSL Enabled	Timeout (sec)		
10.124.3.6		389	False	30		
LDAP Provider - 10.1	124.3.6				00	
				Policy	Faults History	
					0 ± %.	
Properties						
Host Name (or IP Address):	10.124.3.6					
Description	optional					
Port.	389 U					
Rase DN	ound isers deardelab deacom					
Password						
Confirm Password:						
Timeout (sec):	30					
Retries	1					
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: De bind DN is de geloofsbrieven u gebruikt om tegen een LDAP voor authentiek te verklaren. APIC verifieert het gebruiken van deze rekening om de folder te vragen.

Base-DN: Deze string wordt door de APIC gebruikt als een referentiepunt voor het zoeken en identificeren van gebruikerangen in de directory.

Wachtwoord: Dit is het vereiste wachtwoord voor de bind DN noodzakelijk om tot de server LDAP toegang te hebben, correlerend met het wachtwoord dat op uw server LDAP wordt gevestigd.

SSL inschakelen: Als u een intern CA of een zelfondertekend certificaat gebruikt, moet u Permissive kiezen.

Filter: De standaardinstelling van het filter is cn=\$userid wanneer de gebruiker is gedefinieerd als een object met een algemene naam (CN), de filter wordt gebruikt om te zoeken naar de objecten in de Base-DN.

Attribuut: Attribute wordt gebruikt om groepslidmaatschap en rollen te bepalen. ACI biedt hier twee opties: memberOf en

CiscoAVPair.memberOf is een RFC2307bis attribuut om groepslidmaatschap te identificeren. Op dit moment controleert OpenLDAP RFC2307, dus title wordt deze gebruikt.

Management endpoint group (EPG): Connectiviteit met de LDAP-server wordt bereikt via de In-band of Out-of-band EPG, afhankelijk van de gekozen netwerkbeheerbenadering.

Stap 3. Regels voor LDAP-groepstoewijzing configureren

Navigeer in de menubalk naar Admin > AAA > Authentication > LDAP > LDAP Group Map Rules zoals in de afbeelding.

Authentication											Q
					AAA	LDAP	RADIUS T	ACACS	SAML	RSA DUO	OAuth 2
							Providers	LDAP	Group Map	Rules LDA	P Group Maps
											0 ± %.
 Name 		Descrip	tion		Group	p DN					
LDAPGroupMapRule					cn=D0	CGroup,ou=Grou	ups,dc=dclab,dc=co	n			
LDAP Group M	ap Rule - LDAPGroupMapRu	le	Policy	O O History							
			Ċ	± %-							
Properties Name: Description: Group DN:	LDAPCroupMapRule Optional cn=DCGroup.ou=Groups.dc=dclab.dc=co										
Security Domains:				0 +							
	Security Domain all	PECESS									
	Role admin	writePriv									
			Show Usage Close								

Gebruikers in DCGroup hebben beheerdersrechten. Daarom cn=DCGroup, ou=Groups, dc=dclab, dc=com. Awijst de Groep DN het veiligheidsdomein aan All toe en wijst de rollen van admin met toe write privilege.

Stap 4. LDAP-groepkaarten configureren

Navigeer in de menubalk naar Admin > AAA > Authentication > LDAP > LDAP Group Maps zoals in de afbeelding.

Authentication									G
		AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
				Prov	ders LD	AP Group Map	Rules	LDAP Gro	up Maps
								0	± %.
* Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	00								
	Policy History								
	0 ± %.								
Properties									
Description: optional	-								
Rufes:	÷								
Name									
LDAPGroupMapRule									
	*								
	Show Usage Close Stidmit								

Maak een LDAP Group Map die LDAP Group Map-regels bevat die in Stap 2 zijn gemaakt.

Stap 5. AAA-verificatiebeleid configureren

Navigeer in de menubalk naar Admin > AAA > Authentication > AAA > Policy > Create a login domainzoals in de afbeelding.

Authentication										C
			A	AA LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
								Policy	Faults	History
							-		0	+ 40-
Properties									0	- ^*
Remote user login policy: No Login										
Use ICMP reachable true										
Default Authentication										
Realm: LDAP										
LDAP Login Domain: LDAP										
Console Authentication										
Realm: Local										
										-
										Q
• Mana	Description		De	alm						1
- Name fallback	Description		lo lo	val						N
Innorth			LO	MP						
Login Domain - LDAP										
		Policy History								
		○ ± %-								
Properties										
Name: LDAP		î.								
Rearry LDAP										
Description: Optional										
And Only Characterity I des Councilies										
Auth Choice: Cisconvear Lasporoupwap										
DAPGroupMap	~ +									
Name Priority	Description									
10.124.3.6 1										
		*								
	Chaustin	Church								
	Show Osage	Chuse Submit						Res	et	Submit

Navigeer in de menubalk naar Admin > AAA > Authentication > AAA > Policy > Default Authentication zoals in de afbeelding.

Authentication													o
					AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2	1
										Policy	Faults	History	t
											Ó	± %	w
Properties Remote user login policy: Use ICMP reachable providers only: Default Authentication Reatm: : LDAP Login Domain: Fallback Domain Availability: Console Authentication Reatm:	No Login v true v LDAP v LDAP v LDAP v LDAP v LOAP v Local v Local v	4											
													3
												-	F.
 Name 		D	Description		Realm								
fallback					Local								
LDAP					LDAP								

Wijzing de standaardverificatie Realm in LDAP en selecteer LDAP Login Domain aangemaakt.

Verifiëren

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

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

disco APIC					User1 🔇	0	0	00
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations							
Quoksart Desnooerd Contolers System Settings Smart Licensing Paulis	History Consig.cones Active Sessions Security							
System Health		Fault Co	ounts by Domain					
Zoom IH ID AIL		8	nowledged Faults		Hide Delegated Faults	0	0	0
	S APIC		1DE		1	0	0	2
a o	What's New in 5 2(7f)				0	0	0	0
	that show in s.E(77)				0	0	0	1
N	ACI Fabric Software Onboard ACI fabrics to Nexus Cloud for Inventory, Simplified workflows for fabric and access poli	licies			0	0	0	0
	anomaly, and assurance information • Migration to simplified workflows for fabric and Simplified migration from Gent News switches to success policies	d	et.		0	0	0	0
	Gen2 CloudScale platforms • Enhanced ACI Fabric Setup				0	0	0	0
	Support Getting Started Explore				0	ò	0	0
	Online Help What's new in 5.2(7f) Configuration Guides				0	0	0	0
Nodes with Health ≤ 99	Documentation View All Tutorial Videos TechNotes							
Name Pod ID	APIC Communities	ints by Type						
			nowledged Faults		Hide Delegated Faults			0
	It looks like this is your first time logging into APIC. Let's go through some of Start ACI Eable Set	10	ations			0	0	
Tenants with Health ≤ 99	the basics to get you up and running.	-			0	0	0	1
 Name 			Iste		0	0	0	0
					1	0	0	1
			r Status					
			Jame	IP	Admin State Op Sta	erational ite	Health	n State
		1	apic1	10.0.0.1	In Service 🧧	alatia	Fully F	it .

Controleer dat de LDAP-gebruiker User1 zich met succes aanmeldt bij APIC met de beheerdersrol en schrijfrechten.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Wanneer de gebruiker niet in de LDAP-database bestaat:

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

Als het wachtwoord niet correct is:

APIC Version 5.2(7f) Login Error Uluit Cisco	User ID Password eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee

Wanneer de LDAP-server onbereikbaar is:

APIC		User ID	
 Version 5.2(7f)	•••••	
ւվուլը cisco	Login Error LDAP/AD failed to bind	to any servers	1

Opdrachten voor troubleshooting:

<#root>

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

Als u meer hulp nodig hebt, neem dan contact op met Cisco TAC.

Gerelateerde informatie

- <u>Cisco APIC-configuratiehandleiding voor beveiliging, release 5.2(x)</u>
- <u>Cisco Technical Support en downloads</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.