Configura autenticazione LDAP ACI

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Configurazione
Configurazioni
Passaggio 1. Crea gruppi/utenti su Ubuntu phpLDAPadmin
Passaggio 2. Configurare i provider LDAP su APIC
Passaggio 3. Configura regole mapping gruppi LDAP
Passaggio 4. Configura mapping gruppi LDAP
Passaggio 5. Configura criterio di autenticazione AAA
Verifica
Risoluzione dei problemi
Informazioni correlate

Introduzione

In questo documento viene descritto come configurare l'autenticazione LDAP (Lightweight Directory Access Protocol) di ACI (Application Centric Infrastructure).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Policy ACI di autenticazione, autorizzazione e accounting (AAA)
- LDAP

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Application Policy Infrastructure Controller (APIC) versione 5.2(7f)
- Ubuntu 20.04 con slapd e phpLDAPadmin

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.

Configurazione

In questa sezione viene descritto come configurare APIC in modo da integrarlo con il server LDAP e utilizzare LDAP come metodo di autenticazione predefinito.

Configurazioni

Passaggio 1. Crea gruppi/utenti su Ubuntu phpLDAPadmin



Nota: per configurare Ubuntu come server LDAP, consultare il sito ufficiale di Ubuntu per le linee guida complete. Se è presente un server LDAP esistente, iniziare con il passo 2.

In questo documento, il DN di base è dc=dclab,dc=com e due utenti (Utente1 e Utente2) appartengono a Gruppi (DCGroup).



Passaggio 2. Configurare i provider LDAP su APIC

Sulla barra dei menu APIC, spostarsi suAdmin > AAA > Authentication > LDAP > Providers come mostrato nell'immagine.

Authentication							0
			AAA LDA	P RADIUS TACACS SAML	RSA	DUO	OAuth 2
				Providers LDAP Group I	Map Rules	LDAP Gr	oup Maps
						0	+ 56-
Host Name	Description	Port	SSL Enabled	Timeout (sec)		0	- ///
10.124.3.6		389	False	30			
LDAD Provider - 101	2426					0	
LDAP PIOVIDEI - 10.1	24.5.0					0	
				Polic	/ Faults	Histor	У
					() ± 1	t-
Properties							
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:							
Contrim Password:							
Detries:	30						
Founda SSI 1							
Filter:	cn+\$userid						
Attribute:	title						
SSL Certificate Validation Level:	Permissive Strict						
Management EPG:	default (Out-of-Band)						
Senar Monitorion	Disabled Enabled						
Server Monitoring:	Enabled Enabled						

DN di binding: il DN di binding è la credenziale utilizzata per l'autenticazione in base a un LDAP. APIC esegue l'autenticazione utilizzando questo account per eseguire query sulla directory.

DN di base: questa stringa viene utilizzata dall'APIC come punto di riferimento per la ricerca e l'identificazione delle voci utente all'interno della directory.

Password: la password richiesta per il DN di binding necessaria per accedere al server LDAP, correlata alla password impostata sul server LDAP.

Abilita SSL: se si utilizza una CA interna o un certificato autofirmato, è necessario scegliere Permissivo.

Filtro: l'impostazione predefinita del filtro è cn=\$userid quando l'utente è definito come un oggetto con un nome comune (CN), il filtro viene utilizzato per cercare gli oggetti all'interno del DN di base.

Attributo: l'attributo viene utilizzato per determinare l'appartenenza al gruppo e i ruoli. ACI fornisce due opzioni qui: memberOf e CiscoAVPair.memberOf è un attributo RFC2307bis per identificare l'appartenenza al gruppo. Attualmente, OpenLDAP controlla RFC2307, quindi title viene utilizzato.

Management Endpoint Group (EPG): la connettività al server LDAP viene ottenuta tramite EPG in-band o out-of-band, a seconda dell'approccio di gestione della rete scelto.

Passaggio 3. Configura regole mapping gruppi LDAP

Sulla barra dei menu, passare a Admin > AAA > Authentication > LDAP > LDAP Group Map Rules come mostrato nell'immagine.

Name Description 0 LDAP Group Map Rule ~ LDAPGroupMapRule 0 LDAP Group Map Rule ~ LDAPGroupMapRule 0 Description 0 ± %- Properties0 ± %-	للمه LDAP RADIUS TACACS SAML RSA DUO OAuth 2 Providers LDAP Group Map Rules LDAP Group Maps DO ± %× Proup DN n=DCGroup, gu=Groups, dc=ddab, dc=com
Name Description 0 LDAPOroupMapRule Description 0 LDAPOroupMapRule Policy History O ± %	Providers LDAP Group Map Rules LDAP Group Maps © ± %- proup DN n=DCGroup,ou=Groups,dc=dclab,dc=com
Name Description 0 LOAPOroupMapRule Description LDAP Group Map Rule - LDAPGroupMapRule Policy History O ± % Properties	ი ± ჯ. n=DCGroup,ou=Groups,dc=ecom
Name Description 0 LOAPOroupMapRule O LDAP Group Map Rule - LDAPGroupMapRule O Policy History O	iroup DN n=DCGroup,ou=Groups,dc=dclab,dc=com
LDAPOrougMagRule CONTRACTION OF A CONTRACT O	un=DCOroug, ou=Orouge, dic=dclab, dic= com
LDAP Group Map Rule - LDAPGroupMapRule	
Policy History ○ ± %-	
O ± %. Properties	
Properties	
Name: LDARGioupMapilie Descriptor: Optional	
Group DN: cn+DCGroup,eu+Groups,dc+dclab,dc+co	
Security Domains: O +	
Name Access	
Security Domain all	
Nos admini analysis Show Usage Close Subtract	

Gli utenti in DCGroup dispongono di privilegi di amministratore. Il DN gruppo cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aassegna pertanto il dominio di protezione a All e alloca i ruoli di admin con write privilege .

Passaggio 4. Configura mapping gruppi LDAP

Sulla barra dei menu, passare a Admin > AAA > Authentication > LDAP > LDAP Group Maps come mostrato nell'immagine.

Authentication									0
		AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
				Provi	ders LD	AP Group Map	Rules	LDAP Grou	ip Maps
								0	± %.
* Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	00								
	Policy History								
	0 ± %-								
Properties									
Description: optional	*								
D. Jac	· · ·								
Name									
LDAPGroupMapRule									
	Show Usage Close Submit								

Creare una mappa di gruppo LDAP che contenga le regole della mappa di gruppo LDAP create nel passo 2.

Passaggio 5. Configura criterio di autenticazione AAA

$Sulla \ barra \ dei \ menu, \ passare \ a \ Admin > AAA > Authentication > AAA > Policy > Create \ a \ login \ domain come \ mostrato \ nell'immagine.$

Authentication									C
			AAA	LDAP RAD	NUS TACACS	SAML	RSA	DUO	OAuth 2
							Policy	Faults	History
								0	+ %-
Properties								0	- ///
Remote user login policy: No Login									
Use ICMP reachable true									
Default Authentication									
Realm: LDAP									
LDAP Login Domain: LDAP 🗸									
Fallback Domain Availability: Always Available									
Console Authentication									
Nearric Local									
									0
									+
* Name	Description		Realm						5
fallback			Local						~
Login Domain - LDAD		0.0	LDAP						
Login Domain - LDAP		00							
		Policy History							
		0 ± %-							
Properties									
Name: LDAP		· · · · · ·							
Description: optional									
Auth Choice: CiscoAVPair LdapGroupMap									
LDAP Group Map: LDAPGroupMap 🗸 🛃									
Providers:	≅ +								
Name A Prior	ity Description								
10.124.3.6 1									
	Show Lisana	Close Subwar					_		
	chiow Usage						R	iset	Submit

Sulla barra dei menu, passare a Admin > AAA > Authentication > AAA > Policy > Default Authentication come mostrato nell'immagine.

Authentication							Q
		AAA	LDAP RADIU	S TACACS	SAML RSA	DUO	OAuth 2
					Policy	Faults	History
						0	± %-
Properties Remote user login policy: No Login Use ECMP reactable providers only Realm: LDAP Login Domain LDAP Login Domain LDAP Login Domain Console Authentication Realm: Cocal	4						
							0
* Name	Description	Realm					
fallback		Local					
LDAP		LDAP					

Cambiare l'autenticazione predefinita Realm in LDAP e selezionare LDAP Login Domain creato.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

	User ID	
APIC	User1 Password	
Version 5.2(7f)	•••••	
۰۱ ۱۰۱ ۱۰ cisco	Domain LDAP ~	

diale APIC					User1 🔍	00	0	00
System Tenants Fabric Virtual Networking Admin Operations QuickStart Deshboard Controllers System Settings Smart Licensing Faults	Apps Integrations History Config Zones Active Sessions Security							
System Health		Fa	ult Counts by Domain					
Zoom TH 1D All			Nowledged Faults		Hide Delegated Faults	0	0	0
	APIC		10E		1	0	0	2
score	What's New in 5.2(7f)				0	0	0	0
No	ACI Fabric Software UI Enhancement • Onboard ACI fabrics to Nexus Cloud for Inventory. • Simplified w	s orkflows for fabric and access policies			0	0	0	0
	anomaly, and assurance information • Migration to Simplified migration from Gen1 Nexus switches to access polic	simplified workflows for fabric and ies	nt		0	0	0	0
	Gen2 CloudScale platforms Enhanced ACI Fabric Se	CI Fabric Setup			0	0	0	0
	Support Getting Started Online Help What's new in 5.2(77) Traveline Methods (March 1997)	Explore Configuration Guides			0	0	0	0
Nodes with Health ≤ 99	Documentation View All Tutorial Videos	TechNotes APIC Communities	nts by Type					
Training Training		rowledged Faults		Hide Delegated Faults		~	~	
	It looks like this is your first time logging into APIC. Let's go through some of the basics to get you up and pupping.	Start ACI Fabric Setup	ations		0	0	0	•
renants with Health \$ 99	and second to first has the environment.				0	0	0	1
			1		1	0	ò	1
			r Status					
			lame	IP	Admin State Op	erational	Health	h State
		1	apic1	10.0.0.1	In Service	alatia	Fully Fi	e

Verificare che l'utente LDAP User1 esegua correttamente l'accesso ad APIC con il ruolo di amministratore e il privilegio di scrittura.

Risoluzione dei problemi

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

Se l'utente non esiste nel database LDAP:

					User ID		
			APIC		Password		
	1		Version 5.2(7f)		•••••		
	ւվուվո cisco	Login Error	cation DENIED Login	~			
				0	K		

Se la password è errata:

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

Quando il server LDAP non è raggiungibile:

		User ID		
APIC		Password		
Version 5.2(7f)	•••••		1
	Login Error	8		
սիսիս	LDAP/AD failed to bind	to any servers	~	
CISCO	ОК	Login		
/			1	

Comandi per la risoluzione dei problemi:

<#root>

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

Per ulteriore assistenza, contattare Cisco TAC.

Informazioni correlate

- <u>Guida alla configurazione della sicurezza di Cisco APIC, versione 5.2(x)</u>
- Supporto tecnico Cisco e download

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).