Konfigurieren Sie die ACI-LDAP-Authentifizierung

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konfigurieren
Konfigurationen
Schritt 1: Erstellen von Gruppen/Benutzern unter Ubuntu phpLDAPadmin
Schritt 2: LDAP-Anbieter auf dem APIC konfigurieren
Schritt 3: LDAP-Gruppenzuordnungsregeln konfigurieren
Schritt 4: LDAP-Gruppenzuordnungen konfigurieren
Schritt 5: AAA-Authentifizierungsrichtlinie konfigurieren
Überprüfung
Fehlerbehebung
Zugehörige Informationen

Einleitung

In diesem Dokument wird die Konfiguration der ACI-Authentifizierung (Application Centric Infrastructure) und LDAP-Authentifizierung (Lightweight Directory Access Protocol) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ACI-AAA-Richtlinie (Authentication, Authorization und Accounting)
- LDAP

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Application Policy Infrastructure Controller (APIC) Version 5.2(7f)
- Ubuntu 20.04 mit slapd und phpLDAPadmin

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie den APIC konfigurieren, um ihn in den LDAP-Server zu integrieren und LDAP als Standardauthentifizierungsmethode zu verwenden.

Konfigurationen

Schritt 1: Erstellen von Gruppen/Benutzern unter Ubuntu phpLDAPadmin



Hinweis: Um Ubuntu als LDAP-Server zu konfigurieren, finden Sie umfassende Richtlinien auf der offiziellen Ubuntu-Website. Wenn bereits ein LDAP-Server vorhanden ist, beginnen Sie mit Schritt 2. In diesem Dokument ist die Basis-DN gleich, dc=dclab,dc=com und zwei Benutzer (User1 und User2) gehören zu Gruppen (DCGroup).

≡ php ⊢≡LDAP ⊨ #admin	
Home Purge caches Show Cache	
My LDAP Server My LDA	E Outhenticate to server Successfully logged into server.

Schritt 2: LDAP-Anbieter auf dem APIC konfigurieren

Navigieren Sie in der APIC-Menüleiste wie im Bild dargestellt zuAdmin > AAA > Authentication > LDAP > Providers.

Authentication												0
				AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OA	ith 2
						Provi	ders LD	AP Group Map	Rules	LDAP	Group N	taps
											0 ±	×
Host Name	Description	Port	SSL Enabled				Timeout	(sec)				
10.124.3.6		389	False				30					
LDAP Provider - 10.1	24.3.6									0	00	
								Dollars	Enulte			
								Policy	rauns	ma	nory	
0 0 0 0									(⇒ ±	**-	
Properties	10.124.2.6											
Description:	optional											
Port:	389											
Bind DN:	cn+admin,dc+dclab,dc+com											
Base DN:	ou=Users,dc=dclab,dc=com											
Password:												
Confirm Password:												
Timeout (sec):	30 0											
Retries:	1											
Enable SSL:												
Filter:	cn+\$userid											
Attribute.	bbe											
SSL Certificate Validation Level:	Permissive Strict											
Management EPG:	default (Out-of-Band)											
Server Monitoring:	Disabled Enabled											

Bind-DN: Die Bind-DN sind die Anmeldeinformationen, die Sie für die Authentifizierung gegenüber einem LDAP verwenden. Der APIC authentifiziert sich mithilfe dieses Kontos, um das Verzeichnis abzufragen.

Basis-DN: Diese Zeichenfolge wird vom APIC als Bezugspunkt für die Suche und Identifizierung von Benutzereinträgen im Verzeichnis verwendet.

Kennwort: Dies ist das erforderliche Kennwort für die Bind-DN, die für den Zugriff auf den LDAP-Server erforderlich ist und mit dem auf Ihrem LDAP-Server eingerichteten Kennwort korreliert.

SSL aktivieren: Wenn Sie eine interne Zertifizierungsstelle oder ein selbstsigniertes Zertifikat verwenden, müssen Sie Zulässig auswählen.

Filter: Die Standardfiltereinstellung ist, cn=\$userid wenn der Benutzer als Objekt mit einem gemeinsamen Namen (CN) definiert ist, wird der Filter verwendet, um nach den Objekten innerhalb der Basis-DN zu suchen.

Attribut: Ein Attribut wird verwendet, um die Gruppenmitgliedschaft und die Gruppenrollen zu bestimmen. Die ACI bietet hier zwei Optionen: memberOf und CiscoAVPair.memberOf ist ein RFC2307bis-Attribut zur Identifizierung der Gruppenmitgliedschaft. Derzeit überprüft OpenLDAP RFC2307, title wird also stattdessen verwendet.

Management-Endpunktgruppe (EPG): Die Verbindung zum LDAP-Server wird je nach gewähltem Netzwerkmanagement-Ansatz entweder über die In-Band- oder die Out-of-Band-EPG hergestellt.

Schritt 3: LDAP-Gruppenzuordnungsregeln konfigurieren

Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > LDAP > LDAP Group Map Rules wie im Bild dargestellt.

Authentication												Q
					AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
							Prov	iders L	DAP Group Ma	p Rules	LDAP Gr	oup Maps
								_			0	± %.
 Name 		Description			Group	DN						
LDAPGroupMapRule					cn=DC0	roup,ou=Grou	ps,dc=dclab,d	c=com				
LDAP Group M	ap Rule - LDAPGroupMapRule			00								
			Policy	History								
			Ó	± %-								
Properties Name: Description: Group DN:	LDAPGroupMapRule optional cn=DCGroup,ou=Group6,dc=dclab,dc=co											
Security Domains:				0 +								
	Name	Access		-								
	 Security Domain all 											
	Role admin	writePriv										
		Show U	sage Close									

Benutzer in der DCGroup haben Administratorrechte. Aus diesem Grund weist die Gruppen-DN der Sicherheitsdomäne zu, cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aund weist dieser All die Rollen von admin mit write privilege zu.

Schritt 4: LDAP-Gruppenzuordnungen konfigurieren

Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > LDAP > LDAP Group Maps wie im Bild dargestellt.

Authentication									0
		AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
				Provi	ders LD	AP Group Ma	p Rules	LDAP Gr	oup Maps
								0	± %.
* Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	00								
	Policy History								
	0 ± %-								
Properties									
Description: optional									
Hures:	U +								
LDAPGroupMacRule									
Con- di Ogenation de									
	Show Usage Close Submit								

Erstellen Sie eine LDAP-Gruppenzuordnung mit den in Schritt 2 erstellten LDAP-Gruppenzuordnungsregeln.

Schritt 5: AAA-Authentifizierungsrichtlinie konfigurieren

Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > AAA > Policy > Create a login domainwie im Bild dargestellt.

Authentication														C
							AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
												Policy	Faults	History
													0	± %-
Properties														
Remote user login policy: No Lo	ogin													
Use ICMP reachable true														
Default Authentication														
Realm: LDAP														
LDAP Login Domain: LDAP														
Fallback Domain Availability: Alway	ys Available													
Realm: Local														
														Q
														+
 Name 			Di	escription			Realm							Z
fallback							Local							1
Login Domain - LDA	١P					08	LDAP							
					Policy	History								
					0	+ %-								
Properties					Ť									
Name: LDAP														
						- 11								
Description: 0	ptional					- 11								
						- 11								
Auth Choice:	CiscoAVPair LdapGr	oupMap				- 11								
LDAP Group Map: L	DAPGroupMap	V 🗗				- 11								
Providers:				2 +		- 11								
1	Name	 Priority 	Description			- 11								
1	10.124.3.6	1												
				Show Usa	ige Close							De		Cubmit
												Re	Set	Suumi

Navigieren Sie in der Menüleiste zu, Admin > AAA > Authentication > AAA > Policy > Default Authentication wie im Bild dargestellt.

Authentication													0
					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											
													2
												-	F.
 Name 		C	Description		Realm								
fallback					Local								
LDAP					LDAP								

Ändern Sie die Standardauthentifizierung Realm in LDAP, und wählen Sie LDAP Login Domain erstellt aus.

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

	User ID	
APIC	User1 Password	
Version 5.2(7f)	•••••	
، ۱۱، ۱۱، cisco	Domain LDAP ~	

cisco APIC				User1 Q	00	0	0 0
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations						
Concent Destances Connounces (apprendictings) and toconsing (Peories)	uasion, I considironae I vicina Sapanua I Samunik						
System Health		Fault Counts	s by Domain				
Zoom TH ID AI		S rowle	edged Faults	Hide Delegated Fault	° 💿	0	0
	APIC	1DE		1	0	0	2
score	What's New in 5.2(7f)			0	0	0	0
Ne	Mit Exhele Pathware III Exhancemente			0	0	0	0
	Onboard ACI fabrics to Nexus Cloud for inventory, Onboard ACI fabrics to Nexus Cloud for inventory, Simplified workflows for fabric and access points	olicies		1	0	0	1
	anomaly, and assurance information Simplified migration from Gen1 Nexus switches to access policies	nd		0	0	0	0
	Gen2 CloudScale platforms Enhanced ACI Fabric Setup			0	0	0	0
	Support Getting Started Explore			0	0	o	0
	Online Help What's new in 5.2(7f) Configuration Guides Troubleshooting Online Videos (YouTube'') Configuration Examples and			0	0	0	0
Nodes with Health ≤ 99	Documentation View All Tutorial Videos TechNotes	nte	by Type				
Name Pod ID	APRO CONTINUES	inca	a by Type				
			eogeo Faans	0	0	٥	0
7	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 Se	tup stion	15	0	0	0	0
Ienants with Health # 99		_		0	0	0	1
 Name 		hate		0	0	0	0
		1		1	0	0	1
		r St	tatus				
		Jame	ip IP	Admin State Or	verational	Health	State
				St	ate		
		1 apic1	10.0.0.1	In Service	valable	Fully Fi	R

Vergewissern Sie sich, dass sich der LDAP-Benutzer User1 erfolgreich mit der Admin-Rolle und den Schreibberechtigungen im APIC anmeldet.

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Wenn der Benutzer nicht in der LDAP-Datenbank vorhanden ist:

			User ID			
	APIC		Password			
	Version 5.2(7f)		Domain		1	
1	 cisco	Login Error		~		
			K Login			
		4		-/		

Wenn das Kennwort falsch ist:

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

Wenn der LDAP-Server nicht erreichbar ist:

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

Befehle für die Fehlerbehebung:

<#root>

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

Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an das Cisco TAC.

Zugehörige Informationen

- <u>Cisco APIC Security Konfigurationsleitfaden, Version 5.2(x)</u>
- <u>Technischer Support und Downloads von Cisco</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.