Configurar a autenticação LDAP da ACI

Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Configurações
Etapa 1. Criar grupos/usuários no Ubuntu phpLDAPadmin
Etapa 2. Configurar provedores LDAP no APIC
Etapa 3. Configurar regras de mapa de grupo LDAP
Etapa 4. Configurar mapas de grupo LDAP
Etapa 5. Configurar a Política de Autenticação AAA
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve como configurar a autenticação do Lightweight Diretory Access Protocol (LDAP) da Application Centric Infrastructure (ACI).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Política de AAA (Authentication, Authorization, and Accounting) da ACI
- LDAP

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Esta seção descreve como configurar o APIC para integrar com o servidor LDAP e usar LDAP como o método de autenticação padrão.

Configurações





Observação: para configurar o Ubuntu como um servidor LDAP, consulte o site oficial do Ubuntu para obter diretrizes abrangentes. Se houver um servidor LDAP existente, comece com a Etapa 2.

Neste documento, o DN base é dc=dclab,dc=com e dois usuários (Usuário1 e Usuário2) pertencem a Grupos (DCGroup).



Etapa 2. Configurar provedores LDAP no APIC

Na barra de menus do APIC, navegue até Admin > AAA > Authentication > LDAP > Providers conforme mostrado na imagem.

Authentication											Q
				AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
						Prov	iders LD/	AP Group Map	Rules	LDAP G	oup Maps
										0	÷ %-
Host Name	Description	Port	SSL Enabled				Timeout	(sec)			
10.124.3.6		389	False				30				
LDAP Provider - 10.1	124.3.6									0	0
								Deter	Faulte		
								Policy	Paults	Histo	У
0 0 0									C) ± :	×-
Properties	10124.2.6										
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										
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										

DN de vinculação: o DN de vinculação é a credencial que você está usando para se autenticar em um LDAP. O APIC autentica usando essa conta para consultar o diretório.

DN base: essa sequência de caracteres é empregada pelo APIC como um ponto de referência para pesquisar e identificar entradas de usuário no diretório.

Senha: Esta é a senha necessária para o DN de vinculação necessário para acessar o servidor LDAP, correlacionando-se com a senha estabelecida em seu servidor LDAP.

Habilitar SSL: se você usar uma CA interna ou um certificado autoassinado, escolha Permissivo.

Filtro: A definição de filtro default é cn=\$userid quando o usuário é definido como um objeto com um nome comum (CN), o filtro é usado para procurar os objetos dentro do DN de Base.

Atributo: O atributo é usado para determinar a associação de grupo e as funções. A ACI oferece duas opções aqui: memberOf e CiscoAVPair.memberOf é um atributo RFC2307bis para identificar a associação de grupo. Atualmente, o OpenLDAP verifica o RFC2307, portanto title é usado.

Grupo de endpoint de gerenciamento (EPG): a conectividade com o servidor LDAP é obtida por meio do EPG dentro da banda ou fora da banda, dependendo da abordagem de gerenciamento de rede escolhida.

Etapa 3. Configurar regras de mapa de grupo LDAP

Na barra de menus, navegue até Admin > AAA > Authentication > LDAP > LDAP Group Map Rules conforme mostrado na imagem.

Authentication				0
			AAA LDAP RADIUS TACACS SAML RSA DUO	OAuth 2
			Providers LDAP Group Map Rules LDAP	Group Maps
) ± %-
* Name	Description		Group DN	
LDAPGroupMapRule			cn=DCGroup.ou=Groups.dc=dclab.dc=com	
LDAP Group Map Rule - LDAPGroupMapRule		00		
		Policy History		
		0 ± %.		
Properties Name: LDAPGroupMapRule Description: Optional Group DN: concOncern our Downey description description				
Security Domains:		0 +		
Name	Access	0		
Security Domain all				
Role admin	writePriv			
	Show Usage C	554 Coonsil		

Os usuários no DCGroup têm privilégios de administrador. Portanto, o DN do grupo está cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aatribuindo o domínio de segurança a All e alocando as funções de admin com write privilege .

Etapa 4. Configurar mapas de grupo LDAP

Na barra de menus, navegue até Admin > AAA > Authentication > LDAP > LDAP Group Maps conforme mostrado na imagem.

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								

Crie um mapa de grupo LDAP que contenha regras de mapa de grupo LDAP criadas na Etapa 2.

Etapa 5. Configurar a Política de Autenticação AAA

Na barra de menus, navegue até Admin > AAA > Authentication > AAA > Policy > Create a login domainconforme mostrado na imagem.

Authentication										G
			AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
								Policy	Faults	History
									0	± %-
Properties Remote user login policy: No Login Use (CMP reachable true providers only: Default Authentication Realm: LDAP LDAP Login Domain: LDAP Fallback Domain Availability: Always Available										
Console Authentication Realm: Local										Q
* Name	Description		Realm							51
falback			Local							
Login Domain - LDAP		00	LDAP							
Eogin Donialit EDA		Policy History								
		Policy History								
Properties Name: LDAP Read::: [LDAP Description: Optional Auth Choice: CiscoM/Pair LdapOrroupMap LDAP Group Map: [LDAPGroupMap Providers: Name Piority 10.124.3.6 1	C + Description									
	Show Usage	Close Submit						Re	set	Submit

Na barra de menus, navegue até Admin > AAA > Authentication > AAA > Policy > Default Authentication conforme mostrado na imagem.

Authentication											Q
			AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth :	z
								Policy	Faults	History	1
									Ó	+ %	÷
Properties Remote user login policy; No Login Use (CMP reachable provides only; Crue provides only; CluAP Default Authentication Realm; LDAP Authon Realm; LDAP Fatback Coman Availability; Aways Available Console Authentication											
nouni Luva										(D +
 Name 	Description		Realm								
fallback			Local								
LDAP			LDAP								

Altere a autenticaçãoRealm padrão para LDAP e selecione LDAP Login Domain created.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

	User ID	
	User1	
AFIC	Password	
Version 5.2(7f)	•••••	
	Domain	
սիսիս	LDAP \checkmark	
cisco	Login	

cisco APIC					User1 🔍	00	0	00
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations							
decoment (Damaged) company (System Denings) company (Feed)	unitary county to use of second second							
System Health		Fault C	ounts by Domain					
Zoom TH 10 AI		ø	nowledged Faults		Hide Delegated Faults	0	٥	0
	APIC		IDE		1	0	0	2
autopa	What's New in 5.2(7f)				0	0	0	0
Ne					0	0	0	1
NC.	ACI Fabric Software UI Enhancements UI Enhancements Simplified workflows for fabric and access p	olicies				0	0	1
	anomaly, and assurance information Migration to simplified workflows for fabric a simplified migration from Gent News switches to	ind	et.		0	ò	0	0
	Gen2 CloudScale platforms • Enhanced ACI Fabric Setup				0	0	0	0
	Support Getting Started Explore				0	ō	ō	0
	Online Help What's new in 5.2(7!) 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		~	~
	It looks like this is your first time logging into APIC. Let's go through some of	-	ations			•	•	-
Tenants with Health ≠ 99	the basics to get you up and running.	arop			0	0	0	1
- Name			Iste		0	0	0	0
			1		1	ō	ō	1
			r Status					
			Jame	IP	Admin State Op Sta	erational ite	Healt	h State
		1	apic1	10.0.0.1	In Service	alatia	Fully F	it .

Verifique se o usuárioUser1 LDAP faz login no APIC com êxito com função de administrador e privilégio de gravação.

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Quando o usuário não existir no banco de dados LDAP:

			User ID			
	APIC		Password			
1 1	Version 5.2(7f)		•••••		1	
	ւլիւվի. cisco	Login Error	ication DENIED Login	~		
			ĸ			

Quando a senha estiver incorreta:

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

Quando o servidor LDAP estiver inacessível:

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

Comandos para Troubleshooting:

<#root>

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

Se precisar de mais ajuda, entre em contato com o Cisco TAC.

Informações Relacionadas

- <u>Guia de configuração de segurança do Cisco APIC, versão 5.2(x)</u>
- Suporte técnico e downloads da Cisco

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.