Configuración de la autenticación LDAP de ACI

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Configuraciones
Paso 1. Crear grupos/usuarios en Ubuntu phpLDAPadmin
Paso 2. Configuración de proveedores LDAP en APIC
Paso 3. Configurar reglas de mapa de grupo LDAP
Paso 4. Configuración de Mapas de Grupo LDAP
Paso 5. Configurar política de autenticación AAA
Verificación
Troubleshoot
Información Relacionada

Introducción

Este documento describe cómo configurar la autenticación del protocolo ligero de acceso a directorios (LDAP) de la infraestructura centrada en aplicaciones (ACI).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Política de autenticación, autorización y contabilidad (AAA) de ACI
- LDAP

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

Configurar

Esta sección describe cómo configurar APIC para integrarse con el servidor LDAP y utilizar LDAP como el método de autenticación predeterminado.

Configuraciones

Paso 1. Crear grupos/usuarios en Ubuntu phpLDAPadmin



Nota: Para configurar Ubuntu como un servidor LDAP, consulte el sitio web oficial de Ubuntu para obtener pautas completas. Si ya existe un servidor LDAP, comience por el paso 2.

En este documento, el DN base es dc=dclab,dc=com y dos usuarios (Usuario1 y Usuario2) pertenecen a Grupos (DCGroup).



Paso 2. Configuración de proveedores LDAP en APIC

En la barra de menús de APIC, desplácese hasta Admin > AAA > Authentication > LDAP > Providers como se muestra en la imagen.

Authentication							0
			AAA LDAP	RADIUS TACACS SAML	RSA	DUO (DAuth 2
				Providers LDAP Group M	ap Rules	LDAP Grou	p Maps
						0.	· %-
Host Name	Description	Port	SSL Enabled	Timeout (sec)			
10.124.3.6		389	False	30			
LDAP Provider - 10.1	124.3.6					08	5
				Policy	Faults	History	
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:							
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						

Enlazar DN: El DN de enlace es la credencial que está utilizando para autenticarse contra un LDAP. El APIC se autentica utilizando esta cuenta para consultar el directorio.

DN base: esta cadena la utiliza el APIC como punto de referencia para buscar e identificar entradas de usuario en el directorio.

Contraseña: Es la contraseña necesaria para el DN de enlace necesario para acceder al servidor LDAP, que se correlaciona con la contraseña establecida en el servidor LDAP.

Habilitar SSL: si utiliza una CA interna o un certificado autofirmado, debe elegir Permiso.

Filtro: La configuración de filtro predeterminada es cn=\$userid cuando el usuario se define como un objeto con un nombre común (CN), el filtro se utiliza para buscar los objetos dentro del DN base.

Atributo: el atributo se utiliza para determinar la pertenencia al grupo y los roles. ACI proporciona dos opciones aquí: memberOf y

CiscoAVPair.memberOf es un atributo RFC2307bis para identificar la pertenencia al grupo. Actualmente, OpenLDAP verifica RFC2307, por lo que title se utiliza en su lugar.

Grupo de terminales de administración (EPG): la conectividad con el servidor LDAP se consigue a través del EPG en banda o fuera de banda, en función del enfoque de administración de red elegido.

Paso 3. Configurar reglas de mapa de grupo LDAP

En la barra de menús, desplácese hasta Admin > AAA > Authentication > LDAP > LDAP Group Map Rules como se muestra en la imagen.

Authentication								0
					AAA LDAP	RADIUS TAC	ACS SAML RSA	DUO OAuth 2
						Providers	LDAP Group Map Rules	LDAP Group Maps
								0 ± %.
 Name 		Des	cription		Group DN			
LDAPGroupMapRule					cn=DCGroup.ou=Grou	ups,dc=dclab,dc=com		
LDAP Group Map	Rule - LDAPGroupMapRule			00				
				History				
				-oncy mistory				
Burner aller				0 • **				
Name: LOAP	PGroupMapRule							
Description: Opti	ional							
Group DN: cn=E	DCGroup.ou+Groups.dc+dclab.dc+co							
Security Domains:				0 +				
Nam	10	Access						
	Security Domain all	unita Delar						
	Role admin	WILEPTIN						
			Show Usage Close	Submit				

Los usuarios de DCGroup tienen privilegios de administrador. Por lo tanto, el DN de grupo está cn=DCGroup, ou=Groups, dc=dclab, dc=com. Aasignando el dominio de seguridad a All y asignando las funciones de admin con write privilege .

Paso 4. Configuración de Mapas de Grupo LDAP

En la barra de menús, desplácese hasta Admin > AAA > Authentication > LDAP > LDAP Group Maps como se muestra en la imagen.

LDAP Group Map - LDAPGroupMap
LDAP Group Map Rules LDAP Group Map Rules LDAP Group Map Rules LDAP Group Map Rules C 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
Name Description LDAPGroupMap LDAPGroupMap - LDAPGroupMap Policy History Properties Description Properties Description
+ Name Description LDAPGroupMap LDAPGroupMap → LDAPGroupMap Potecy History Properties Description: optional
LDAPGroupMap LDAPGroupMap
LDAP Group Map - LDAPGroupMap
LDAP Group Map - LDAPGroup Map
Properties Description: optional
Properties Descriptional
Properties Descriptional
Description: optional
Note: E +
solite LLAPCrocoManBale
toor uniquely new constraints and the constrai
Show Usage Close Submit

Cree un mapa de grupo LDAP que contenga las reglas de mapa de grupo LDAP creadas en el paso 2.

Paso 5. Configurar política de autenticación AAA

En la barra de menús, desplácese hasta Admin > AAA > Authentication > AAA > Policy > Create a login domaincomo se muestra en la imagen.

AAA LDAP RADUE RADUE RADA	Authentication										Q
Poperties Image: Section of the sec				AAA	LDAP	RADIUS	TACACS	SAML	RSA	DUO	OAuth 2
Properties Sanda and property in the initial initializa initial initializa initial initial initial initial in									Policy	Faults	History
Properties Interest and spip plots in the spin										0	± %-
Friendezieher Conside Autentering Reeme Instance Login Domain - LDAP Perceptries Reeme LOAP Properties Reeme LOAP Properties Reeme LOAP Description De	Properties Remote user login policy: No Login Use ICMP reachable true Default Authentication Realm: LDAP LDAP Login Domain: LDAP										2 ///
Conside Authentication Realm * Name tatua: Login Domain - LDAP Properties Name: LDAP Properties	Fallback Domain Availability: Always Available										
Name Description Realm Login Domain - LDAP Poperties Name: LDAP Poperties Name: LDAP Poperties Name: LDAP Poperties Name: LDAP Poperties Pope	Console Authentication Realm: Local										Q
Name Description Name Photory Name											1
Instact Logi Login Domain - LDAP Image: Comparison Properties image: Comparison Mane: Comparison image: Comparison Name: Comparison image: Comparison Name: Projecting image: Comparison Na	* Name	Description		Realm							Z
Login Domain - LDAP	failback			Local							
Properties Name: LOAP Description LOAP CompAnder Description LOAP CompAnder Description LOAP CompAnder Description LOAP CompAnder Description Tot243.6 1	Login Domain - LDAP		08	LUNP							
Properties Name: LDAP Bescription Auth Choice: CoscoMVP#r LDAPCroupMap LDAPCroupMap Providers: Providers: Name Providers: Total243.6 1			Policy History								
Properties Name: LDAP Regim: Re			0 ± %-								
Change Change Change Change	Properties Name: LDAP Priority Description Optional Auth Choice: LDAP Group Map: LDAP Group Map: LDAP Group Map: Name Providers: Name Providers: Name Name Name Name Name Name Name Name	2 + Description									

 $\label{eq:analytical} En \ la \ barra \ de \ men \ us \ des places \ hasta \ Admin > AAA > Authentication > AAA > Policy > Default \ Authentication \ como \ se \ muestra \ en \ la \ imagen.$

Authentication							Q
		ААА	LDAP RADIUS	TACACS SAT	IL RSA	DUO	OAuth 2
					Policy	Faults	History
						Ó	± %∗
Properties Renote user login policy; No Login Use ICMP reachable providers only Login CMP reachable providers only Login Console LDAP Login Domain; LDAP Console Authentication Realm; Local V	4						
							0
* Name	Description	Realm					+
fallback		Local					
LDAP		LDAP					

Cambie la autenticación predeterminada Realm a LDAP y seleccione LDAP Login Domain Created .

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

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

cisco APIC					User1 🔍	0	0	00
System Tenants Fabric Virtual Networking Admin Operations	Apps Integrations							
QuickStart Deshboard Controllers System Settings Smart Licensing Faults	History Config Zones Active Sessions Security							
System Health		Fault Co	ounts by Domain					
Zoom 1H 1D AIL		8	nowledged Faults		Hide Delegated Faults	0	0	0
	APIC		1DE		1	0	0	2
CO.LE	What's New in 5 2/75)				0	0	0	0
	mac shew in S.2(77)				0	0	0	1
	ACI Fabric Software UI Enhancements Onboard ACI fabrics to Nexus Cloud for inventory, Simplified workflows for fabric and access pol	olicies			1	0	0	0
	anomaly, and assurance information Migration to simplified workflows for fabric an access policies	nd	ot		0	0	0	0
	Gen2 CloudScale platforms • Enhanced ACI Fabric Setup				0	0	0	0
	Support Getting Started Explore				0	0	0	0
	Online Help What's new in 5.2(7f) Configuration Guides Troubleshooting Online Videos (YouTube'') Configuration Examples and	ples and			0	0	0	0
Nodes with Health ≤ 99	Documentation View All Tutorial Videos TechNotes		into bu Tumo					
 Name Pod ID 	Arro Communes		vision of the second se		Hide Delegated Faults			
			townedged Palans		0	0	٥	0
Tenerts with Uselik < 00	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 Set	itup	ations		0	0	0	0
lenants with Health # 99					0	0	0	1
* Name			tal		0	0	0	0
					1	0	0	1
			r Status					
			Jame	IP	Admin State Op Sta	erational Ite	Healt	h State
		1	apic1	10.0.0.1	In Service 🤷	aliable	Fully F	Sec.

Verifique que el usuario LDAP User1 inicie sesión en APIC correctamente con el rol de administrador y el privilegio de escritura.

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Cuando el usuario no existe en la base de datos LDAP:

		User ID			
APIC		Password			
Version 5.2(7f)		Domain		1	
ւլիւլիւ cisco	Login Error	ication DENIED Login	~		

Cuando la contraseña es incorrecta:

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

Cuando el servidor LDAP es inalcanzable:

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

Comandos para resolución de problemas:

<#root>

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

Si necesita más ayuda, póngase en contacto con Cisco TAC.

Información Relacionada

- <u>Guía de configuración de seguridad de Cisco APIC, versión 5.2(x)</u>
- <u>Soporte técnico y descargas de Cisco</u>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).