ACILDAP認証の設定

```
内容

      はじめに

      前提条件

      要件

      使用するコンボーネント

      設定

      コンフィギュレーション

      ステップ1: Ubuntu phpLDAPadminでのグループ/ユーザの作成

      ステップ2: APICでのLDAPプロバイダーの設定

      ステップ3: LDAPグループマップルールの設定

      ステップ5: AAA認証ポリシーの設定

      アンフィシュート

      関連情報
```

はじめに

このドキュメントでは、アプリケーションセントリックインフラストラクチャ(ACI)のLightweight Directory Access Protocol(LDAP)認証を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ACI認証、許可、アカウンティング(AAA)ポリシー
- [LDAP]

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Application Policy Infrastructure Controller(APIC)/ $(- \vec{v} = 25.2(7f))$
- ・ Ubuntu 20.04とslapdおよびphpLDAPadmin

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

設定

このセクションでは、LDAPサーバと統合し、LDAPをデフォルトの認証方式として使用するよう にAPICを設定する方法について説明します。

コンフィギュレーション

ステップ1: Ubuntu phpLDAPadminでのグループ/ユーザの作成



注:UbuntuをLDAPサーバとして設定するには、Ubuntuの公式Webサイトで包括的なガイ ドラインを参照してください。既存のLDAPサーバがある場合は、ステップ2から始めま す。

このドキュメントでは、ベースDNはdc=dclab,dc=comで、2人のユーザ(User1とUser2)はグループ(DCGroup)に属しています。





ステップ2: APICでのLDAPプロバイダーの設定

APICメニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > Providersに移動します。

Authentication							Q
			AAA LDA	P RADIUS TACACS SAML	RSA	DUO	OAuth 2
				Providers LDAP Group Map	Rules	LDAP Grou	up Maps
						0	± %.
Host Name	Description	Port	SSL Enabled	Timeout (sec)			
10.124.3.6		389	False	30			
LDAP Provider - 10.1	124.3.6					06	3
				Policy	Enulte	History	
0.000				Poley	Tusma	i notory	
$\otimes \odot \odot \odot$					C	· · ×	*
Properties Host Name (or IP Address):	10.124.3.6						
Description	optional						
Port	389						
Bind DN:	cn+admin,dc+dclab,dc+com						
Base DN	cu=Users,dc=dclab,dc=com						
Password							
Confirm Password:							
Timeout (sec):	30						
Retries	1						
Enable SSL:							
Filter	cn+\$userid						
Attribute.	bbe						
SSL Certificate Validation Level	Permissive Strict						
Management EPG:	e default (Out-of-Band)						
Server Monitoring	Disabled Enabled						

バインドDN:バインドDNは、LDAPに対して認証するために使用するクレデンシャルです。APICは、このアカウントを使用して ディレクトリを照会することで認証を行います。

ベースDN:この文字列は、ディレクトリ内のユーザエントリを検索および識別するためのリファレンスポイントとしてAPICに採 用されます。

パスワード:これは、LDAPサーバにアクセスするために必要なバインドDNの必須パスワードであり、LDAPサーバに設定された パスワードと関連付けられます。

SSLの有効化:内部CAまたは自己署名証明書を使用する場合は、Permissiveを選択する必要があります。

Filter:デフォルトのフィルタ設定はcn=\$userid、ユーザが共通名(CN)を持つオブジェクトとして定義されている場合に、ベース DN内のオブジェクトを検索するために使用されます。 属性:属性は、グループメンバーシップとロールを決定するために使用されます。ここでは、ACIに2つのオプションが用意され ています。memberOfおよびCiscoAVPair.memberOf は、グループメンバーシップを識別するためのRFC2307bis属性です。現在、 OpenLDAPはRFC2307をチェックするため、代わりにtitle が使用されます。

管理エンドポイントグループ(EPG):LDAPサーバへの接続は、選択されたネットワーク管理アプローチに応じて、インバンドまた はアウトオブバンドのEPGを介して実現されます。

ステップ3:LDAPグループマップルールの設定

メニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > LDAP Group Map Rules に移動します。

	Q
	AAA LDAP RADIUS TACACS SAML RSA DUO OAuth 2
	Providers LDAP Group Map Rules LDAP Group Maps
	0 ± %.
Name Description	Group DN
LDAPGroupMapRule	cn=DCGroup.ou=Groups.dc=dclab.dc=com
LDAP Group Map Rule - LDAPGroupMapRule	
o ± %-	
Properties Name: LDAPCroupMapRule Description: Optional Group DH: Cn+DCGroup.ou-Groups.dc+dclab.dc+co	
security bomains O +	
Name Access	
Role admin writePriv	
Show Usage Close Submit	

DCGroup内のユーザーは管理者権限を持ちます。したがって、グループDNはセキュリティドメインをcn=DCGroup, ou=Groups, dc=dclab, dc=com. A割り当てAll、adminwrite privilegeとの役割を割り当てます。

ステップ4:LDAPグループマップの設定

メニューバーで、図に示すようにAdmin > AAA > Authentication > LDAP > LDAP Group Maps に移動します。

Authentication									Q
		AAA	LDAP	RADIUS	TACAC	S SAN	IL RSA	DUO	OAuth 2
				Prov	viders	LDAP Grou	p Map Rules	LDAP	Froup Maps
								() ± %-
* Name	Description								
LDAPGroupMap									
LDAP Group Map - LDAPGroupMap	00								
	Policy History								
	0 + %-								
Properties	0 = 7.0								
Description: optional									
Rules:	± +								
Name									
LDAPGroupMapRule									
	Show Usage Close Submit								

ステップ2で作成したLDAPグループマップルールを含むLDAPグループマップを作成します。

ステップ 5: AAA認証ポリシーの設定

メニューバーで、図に示すようにAdmin > AAA > Authentication > AAA > Policy > Create a login domainに移動します。

Authentication				
			AAA LDAP F	ADIUS TACACS SAML RSA DUO OAuth 2
				Policy Faults History
				0 ± *
Properties				
Remote user login policy: No Login 🗸				
Use ICMP reachable true v				
Default Authentication				
I DAR Login Domain: LDAR				
Fallback Domain Availability: Always Available				
Console Authentication				
Realm: Local 🗸				
Name	Description		Realm	51
falback			Local	K
Logia Demois al DAD			LDAP	
Login Domain - LDAP		00		
		Policy History		
		0 ± %-		
Properties				
Name: LDAP		<u>^</u>		
Description ontional				
Description. Optionial				
Auth Chaises Clisco MiDair I den Crouch Ian				
LOAD Group Mary L DAD Group Mary				
Providers:	· +			
Name Priority	Description			
10.124.3.6 1				
		_		
		*		
	Show Henne	Close		
	Silow Usage			Reset Submit

メニューバーで、図に示すようにAdmin > AAA > Authentication > AAA > Policy > Default Authentication に移動します。

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					

デフォルトの認証RealmをLDAPに変更し、「LDAP Login Domain created」を選択します。

確認

ここでは、設定が正常に機能しているかどうかを確認します。

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

International APIC			User1 🕲 🕥 🖏	
ystem Tenants Fabric Virtual Networking Admin Operation	s Apps Integrations			
uckStart Deenboard Controllers System Settings Smart Licensing Fa	its History Contig Zones Active Sessions Security			
ystem Health		Fault Counts by Domain		
Zoom 1H 1D All		S howledged Faults	Hide Delegated Faults	0 0
	S APIC	30F	1 0	0 2
score	What's New in 5.2(7f)		0 0	0 0
	NC ACI Fabric Software UI Enhancements		0 0	0 0
	Onboard ACI fabrics to Nexus Cloud for inventory, Simplified workflows for fabric and a Micratice to clean@filed.updfiled.execution	rccess policies	1 0	0 1
	Simplified migration from Gen1 Nexus switches to	nt	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 Examp	s ples and	0 0	0 0
odes with Health 5 99	Documentation View All Tutorial Videos TechNotes APIC Communities	nts by Type		
Name Poditu		valetaet Earlis	Hide Delevated Exuits	
			O O	0 0
enants 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 F	Fabric Setup ations	0 0	0 0
hans with Health # 99			0 0	0 1
- Name		14.04	0 0	0 0
			1 0	0 1
		r Status		
		Jame IP	Admin State Operational State	Health State
		1 apic1 10.0	.0.1 In Service Available	Fully Fit

LDAPユーザがUser1、管理者ロールと書き込み権限を使用してAPICに正常にログインできることを確認します。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

ユーザがLDAPデータベースに存在しない場合:

			User ID			
	APIC		Password			
11	Version 5.2(7f)		Domain		1	
	ւլիւվի, cisco	Login Error		~		
			K			

パスワードが正しくない場合:

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

LDAPサーバに到達できない場合:

APIC		User ID Password		
Version 5.2(7f) ۱۱ ۱۰۱ ۱۰ داsco	Ogin Error	D any servers	1	1
	- 5			

トラブルシューティング コマンド:

<#root>

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

さらにサポートが必要な場合は、Cisco TACまでお問い合わせください。

- <u>Cisco APICセキュリティ設定ガイド、リリース5.2(x)</u>
- <u>シスコのテクニカルサポートとダウンロード</u>

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。