

使用ISE和TACACS+配置设备管理的APIC

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[身份验证过程](#)

[APIC配置](#)

[ISE配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍将APIC与ISE集成以使用TACACS+协议进行管理员用户身份验证的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 应用策略基础设施控制器 (APIC)
- 身份服务引擎 (ISE)
- TACACS协议

使用的组件

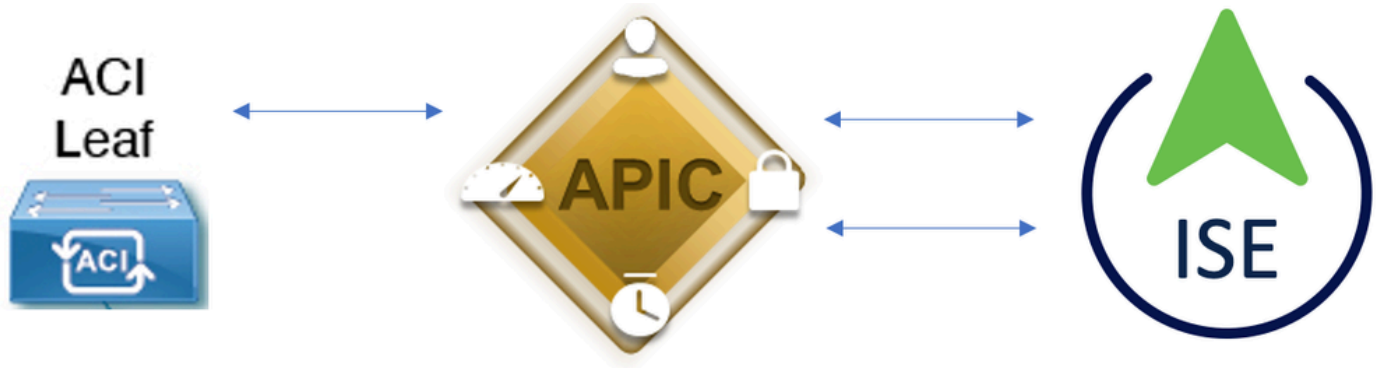
本文档中的信息基于以下软件和硬件版本：

- APIC版本4.2(7u)
- ISE版本3.2补丁1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



集成图

身份验证过程

第1步：使用管理员用户凭证登录APIC应用。

步骤2.身份验证过程触发并ISE在本地或通过Active Directory验证凭证。

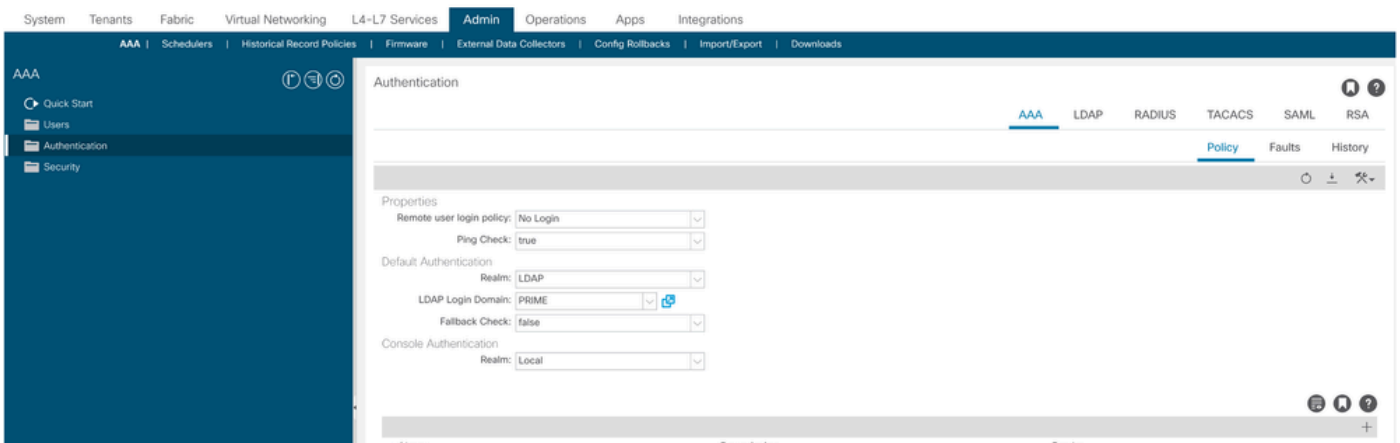
步骤3.身份验证成功后，ISE发送允许数据包以授权对APIC的访问。

步骤4. ISE显示成功的身份验证实时日志。

 注意：APIC将TACACS+配置复制到属于交换矩阵的枝叶交换机。

APIC配置

步骤1.导航到Admin > AAA > Authentication > AAA，然后选择+图标以创建新的登录域。



APIC登录管理员配置

步骤2.定义新登录域的名称和领域，然后单击+“提供程序”下的以便创建新的提供程序。

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
------	----------	-------------

APIC登录管理员

Providers:

Name	Priority	Description
<input type="text" value="select an option"/> <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>

Create TACACS+ Provider

APIC TACACS提供程序

步骤3.定义ISE IP地址或主机名，定义共享密钥，并选择管理终端策略组(EPG)。单击Submit以将TACACS+提供程序添加到登录管理员。

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol: CHAP MS-CHAP PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring: Disabled Enabled

APIC TACACS提供程序设置

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

TACACS提供程序视图

ISE 配置

步骤1. 导航到 **Administration > Network Resources > Network Device Groups**。在All Device Types下创建网络设备组。

☰ Cisco ISE

Network Devices **Network Device Groups** Network Device Profiles External

Network Device Groups

All Groups

Choose group ▾

↻ **Add** Duplicate Edit 🗑️ Trash 👁️ Show group members ⬇️ Import ⬆️ Export ▾ ☰

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▾ All Device Types	All Device Types
<input type="checkbox"/>	APIC	

ISE网络设备组

步骤2. 导航至 **Administration > Network Resources > Network Devices**。选择Add“定义APIC名称和IP地址”，在“设备类型和TACACS+”复选框下选择APIC，然后定义在APIC TACACS+提供程序配置中使用的密码。单击。Submit

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > APIC-LAB

Network Devices

Name

Description

IP Address * IP :

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret [Show](#) [Retire](#)

对枝叶交换机重复步骤1和步骤2。

步骤3.使用此链接上的说明将ISE与Active Directory集成；

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>。



注意：本文档包含内部用户和AD管理员组作为身份源，但测试是使用内部用户的身份源执行的。AD组的结果相同。

步骤4. (可选) 导航至 **Administration > Identity Management > Groups**。选择 **User Identity Groups** 并单击 **Add**。为只读管理员用户和管理员用户创建一组。

Identity Groups

EQ

< [List Icon] [Settings Icon]

- > Endpoint Identity Groups
- > **User Identity Groups**

User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/> APIC_RO	i
<input type="checkbox"/> APIC_RW	

身份组

步骤5. (可选) 导航至☰>Administration > Identity Management > Identity. 点击Add并创建一个用Read Only Admin户和Admin用户。将每个用户分配到步骤4中创建的每个组。

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/> Enabled	APIC_ROUser					APIC_RO
<input type="checkbox"/> Enabled	APIC_RWUser					APIC_RW

步骤6. 导航至☰>Administration > Identity Management > Identity Source Sequence。选择Add，定义名称，然后从列AD Join Points表选Internal Users择和身份源。选择Treat as if the user was not found and proceed to the next store in the sequenceAdvanced Search List Settings 下，然后单击Save。

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected
Internal Endpoints		iselab
Guest Users		Internal Users
All_AD_Join_Points		

Navigation buttons: > < >> << (between columns) and < > (within columns)

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

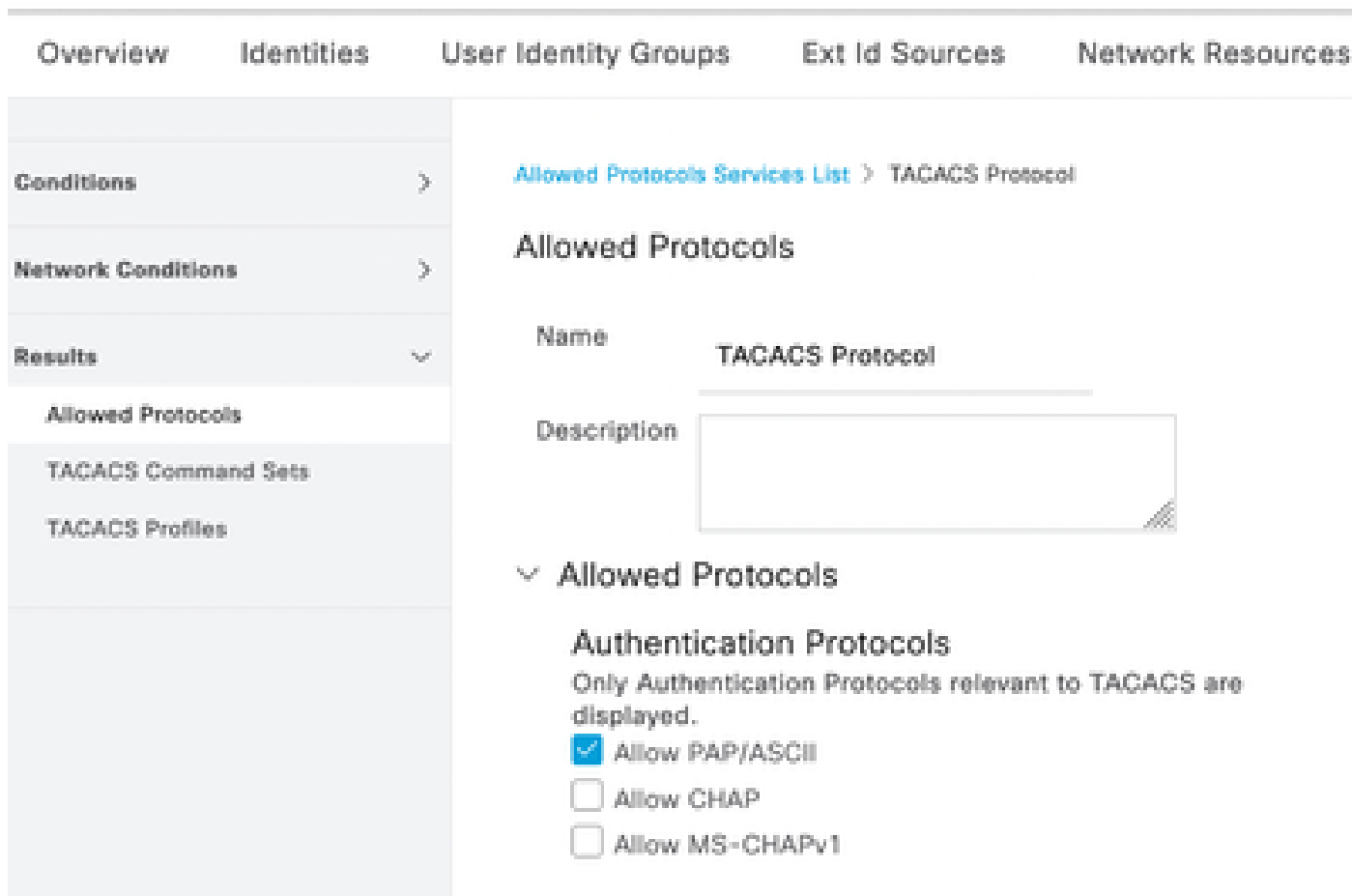
- Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
- Treat as if the user was not found and proceed to the next store in the sequence

身份源序列

7. 导航至 ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. 选择 Add, 定义名称

, 并取消选中Allow CHAP和Allow MS-CHAPv1 from Authentication protocol列表。选择Save。

☰ Cisco ISE



Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results ▾

Allowed Protocols

TACACS Command Sets

TACACS Profiles

Allowed Protocols Services List > TACACS Protocol

Allowed Protocols

Name TACACS Protocol

Description

▾ Allowed Protocols

Authentication Protocols

Only Authentication Protocols relevant to TACACS are displayed.

- Allow PAP/ASCII
- Allow CHAP
- Allow MS-CHAPv1

TACACS允许协议

8. 定位至☰>Work Centers > Device Administration > Policy Elements > Results > TACACS Profile。 点击add并根据下方的列表上的属性创建两个配置文件Raw View。 单击。 Save

- 管理员用户 : cisco-av-pair=shell:domains=all/admin/
- 只读管理员用户 : cisco-av-pair=shell:domains=all/read-all



注意：如果出现空格或其他字符，授权阶段将失败。

- Conditions >
- Network Conditions >
- Results
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles**

TACACS Profiles > APIC ReadWrite Profile

TACACS Profile

Name
APIC ReadWrite Profile

Description

Task Attribute View **Raw View**

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

Cancel Save

TACACS配置文件

- Overview
- Identities**
- User Identity Groups
- Ext Id Sources
- Network Resources

TACACS Profiles

↻
Add
Duplicate
Trash ▼
Edit

	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

TACACS管理员和只读管理员配置文件

步骤9. 导航到 > Work Centers > Device Administration > Device Admin Policy Set。创建新的策略集，定义名称，并选择在步骤1中创建的设备类APIC型。选择在步骤7中创建TACACS Protocol的。作为允许的协议，然后单击 Save。

Policy Sets

Reset [Reset Polycyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	APIC		DEVICE-Device Type EQUALS All Device Types#APIC	TACACS Protocol	55		

TACACS策略集

步骤10. 在new下单Policy Set击向右箭头并>创建身份验证策略。定义名称并选择设备IP地址作为条件。然后选择在第6步中创建的Identity Source Sequence。

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
●	APIC Authentication Policy	Network Access-Device IP Address EQUALS 188.21	APIC_ISS	55	

验证策略

注意：位置或其他属性可用作身份验证条件。

步骤11.为每个管理员用户类型创建授权配置文件，定义名称，并选择内部用户和/或AD用户组作为条件。可以使用其他条件，例如APIC。在每个授权策略上选择适当的外壳配置文件，然后点击 Save。

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
●	APIC Admin RO	AND Network Access Device IP Address EQUALS 192.168.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO	APIC ReadOnly Profile			34	⚙️
●	APIC Admin User	AND OR Network Access Device IP Address EQUALS 192.168.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS ciscoise.lab/Bullfin/Administrators	APIC ReadWrite Profile			18	⚙️
●	Default		Deny All Commands		Deny All Shell Profile	0	⚙️

TACACS授权配置文件

验证

步骤1.使用用户管理员凭证登录APIC UI。从列表中选择TACACS选项。

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

APIC登录

步骤2.验证APIC UI上的访问以及对TACACS Live日志应用了正确的策略。

Welcome to APIC

What's new in version 4.2(7u)



New Features

- Floating L3out
 - Docker EE (Kubernetes) container integration
 - L4-L7 Services support in vPod
 - Backup PBR destination
 - Support for 64 Remote Leaf pairs
- UI Enhancements:
 - User-defined UI banner
 - First Time Setup wizard
 - Simplified L3Out creation
 - EPG to leafs deployment view

[View Release Notes](#)

Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC欢迎消息

对只读管理员用户重复步骤1和2。

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...	Authentication Policy	Authorization Policy	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

TACACS+实时日志

故障排除

步骤1. 导航到☰ > Operations > Troubleshoot > Debug Wizard。选择TACACS并单击 Debug Nodes。

Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

调试配置文件配置

步骤2.选择接收流量的节点并点击Save。

Diagnostic Tools Download Logs **Debug Wizard**

Debug Profile Configuration




Debug Log Configuration

Debug Profile Configuration > Debug Nodes

Debug Nodes

Selected profile **TACACS**

Choose on which ISE nodes you want to enable this profile.

 Filter  

<input type="checkbox"/>	Host Name	Persona	Role
<input checked="" type="checkbox"/>	PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/>	SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

[Cancel](#) [Save](#)

调节点选择

步骤3.执行新测试并下载下方的日志，Operations > Troubleshoot > Download logs 如下所示：

AcsLogs, 2023-04-20 22:17:16, 866, DEBUG, 0x7f93cab7700, cntx=0004699242, sesn=PAN32/469596415/70, CPMSession

如果调试不显示身份验证和授权信息，请验证以下内容：

1. 设备管理服务在ISE节点上启用。
2. 已将正确的ISE IP地址添加到APIC配置。
3. 如果防火墙位于中间，请验证是否允许端口49(TACACS)。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。