

Configurar o APIC para administração de dispositivos com ISE e TACACS+

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Procedimento de autenticação](#)

[Configuração do APIC](#)

[Configuração do ISE](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve o procedimento para integrar o APIC ao ISE para autenticação de usuários administradores com o protocolo TACACS+.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Application Policy Infrastructure Controller (APIC)
- Identity services engine (ISE)
- protocolo TACACS

Componentes Utilizados

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

- APIC versão 4.2(7u)
- Patch 1 do ISE versão 3.2

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

Diagrama de Rede

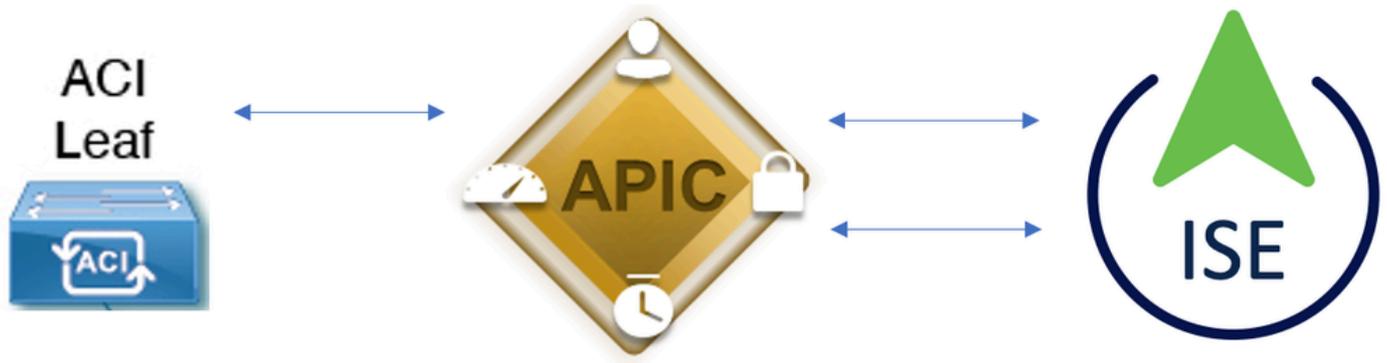


Diagrama de integração

Procedimento de autenticação

Etapa 1. Faça login no aplicativo APIC com as Credenciais de usuário do administrador.

Etapa 2. O processo de autenticação é acionado e o ISE valida as credenciais localmente ou por meio do Ative Directory.

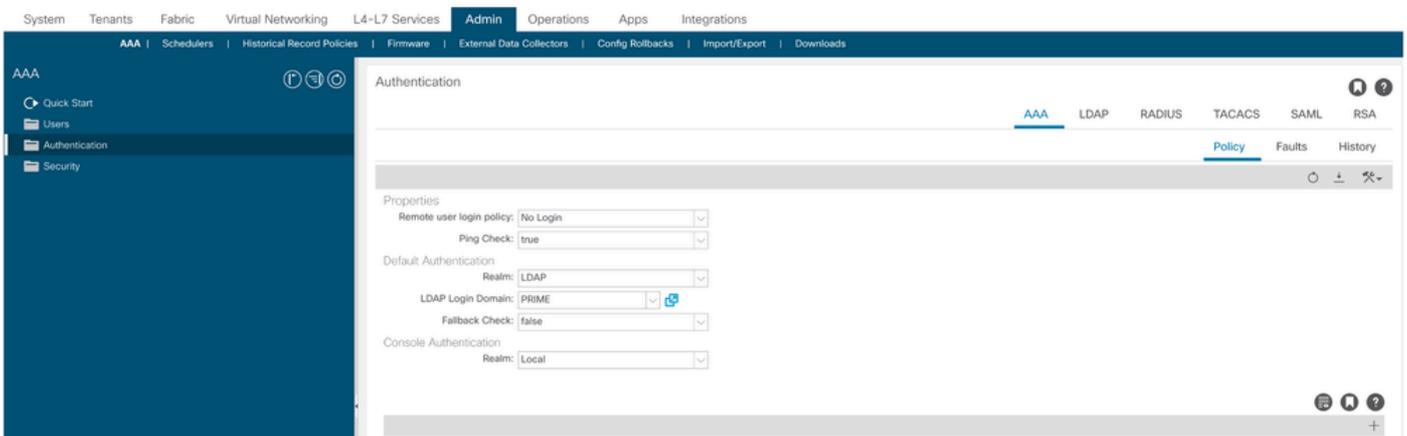
Etapa 3. Quando a autenticação for bem-sucedida, o ISE enviará um pacote de permissão para autorizar o acesso ao APIC.

Etapa 4. O ISE mostra um registro ativo de autenticação bem-sucedido.

 Note: O APIC replica a configuração TACACS+ em switches leaf que fazem parte da malha.

Configuração do APIC

Etapa 1. Navegue para **Admin > AAA > Authentication > AAA** e escolha o ícone **+** para criar um novo domínio de login.



Configuração de admin de login do APIC

Etapa 2. Defina um nome e um realm para o novo Domínio de Login e clique em Provedores para criar um novo provedor.

Create Login Domain



Name:

Realm:

Description:

Providers:

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

administrador de login do APIC

Providers:

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

Create TACACS+ Provider

Provedor APIC TACACS

Etapa 3. Defina o endereço IP ou o nome do host do ISE, defina um segredo compartilhado e escolha o EPG (Endpoint Policy Group) de gerenciamento. Clique para adicionar o provedor TACACS+ ao administrador de login.

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

Configurações do provedor APIC TACACS

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

Exibição do provedor TACACS

Configuração do ISE

Etapa 1. Navegue até  > Administração > Recursos de rede > Grupos de dispositivos de rede. Crie um grupo de dispositivos de rede em Todos os tipos de dispositivo.

 **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	

Grupos de dispositivos de rede do ISE

Etapa 2. Navegue até Administration > Network Resources > Network Devices. Escolha **Add** definir nome e endereço IP do APIC, escolha APIC em Tipo de dispositivo e caixa de seleção TACACS+ e defina a senha usada na configuração do provedor APIC TACACS+. Clique em **.Submit**

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](#)

Repita as etapas 1 e 2 para switches leaf.

Etapa 3. Use as instruções neste link para integrar o ISE com o Ative Directory;

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



Note: Este documento inclui usuários internos e grupos de administradores do AD como origens de identidade. No entanto, o teste é executado com a Origem de identidade dos usuários internos. O resultado é o mesmo para grupos do AD.

Etapa 4. (Opcional) Navegue até **☰** >Administration > Identity Management > Groups. Escolha **User Identity Groups** e clique em **Add**. Crie um grupo para usuários somente leitura Admin e usuários Admin.

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	

Grupo de Identidade

Etapa 5. (Opcional) Navegue até **≡**>Administration > Identity Management > Identity. Clique em **Add** e crie um Read Only Adminusuário e Adminusuário. Atribua cada usuário a cada grupo criado na Etapa 4.

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

Etapa 6. Navegue até **≡** >Administration > Identity Management > Identity Source Sequence. Escolha **Add**, defina um nome e escolha **AD Join Points** e **Internal Users** Origem da identidade na lista. Escolha **Treat as if the user was not found** and proceed to the next store in the sequence **emAdvanced Search List Settings** e clique em **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 ^ v (within columns)

∨ Advanced Search List Settings

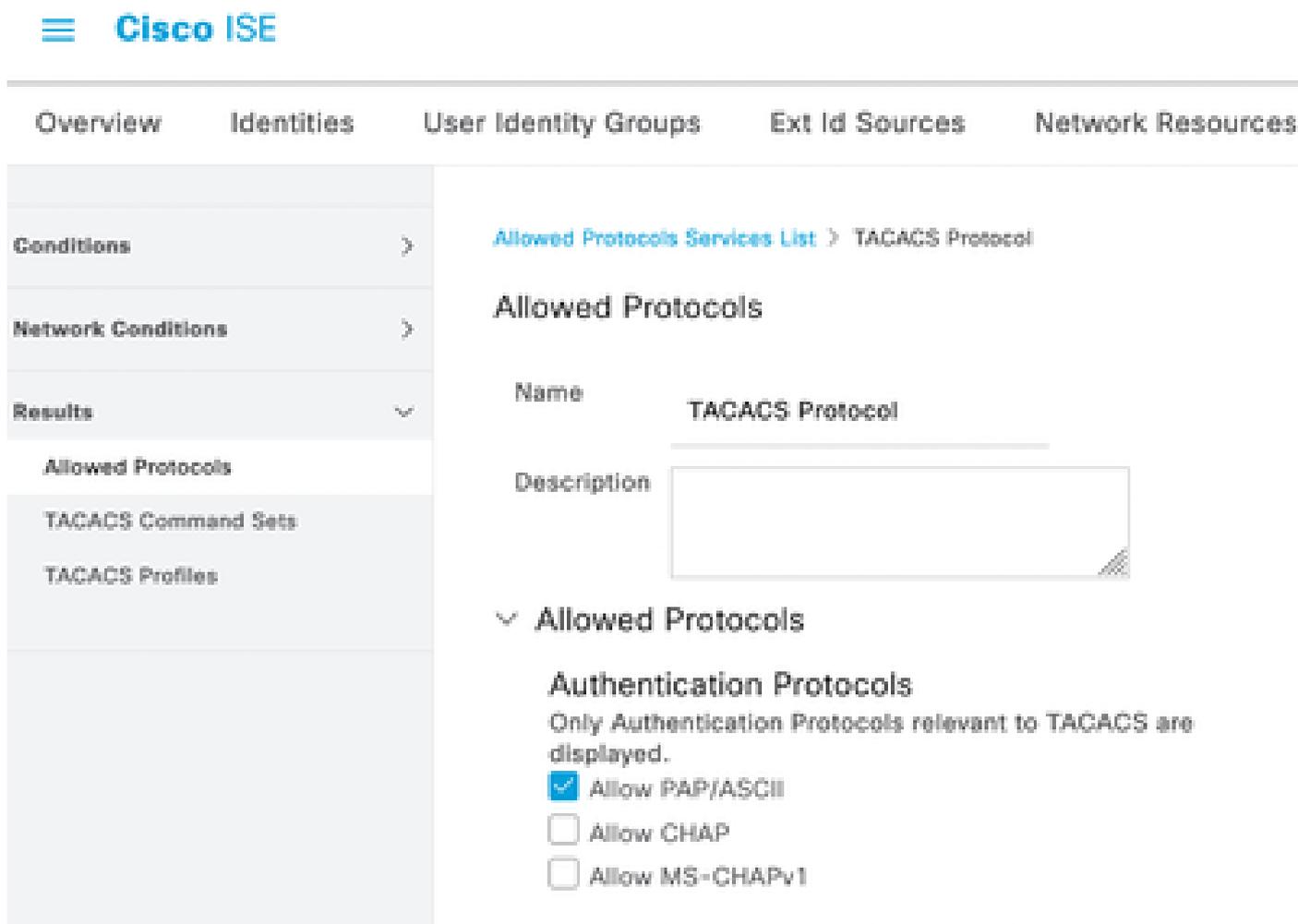
If a selected identity store cannot be accessed for authentication

- 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

Sequência de Origem da Identidade

7. Navegue até ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Selecionar

Adicionar, defina um nome e desmarque Permitir CHAP e Permitir MS-CHAPv1 da lista de protocolos de autenticação. Selecione Save.



Allowed Protocols Services List > TACACS Protocol

Allowed Protocols

Name: TACACS Protocol

Description:

Allowed Protocols

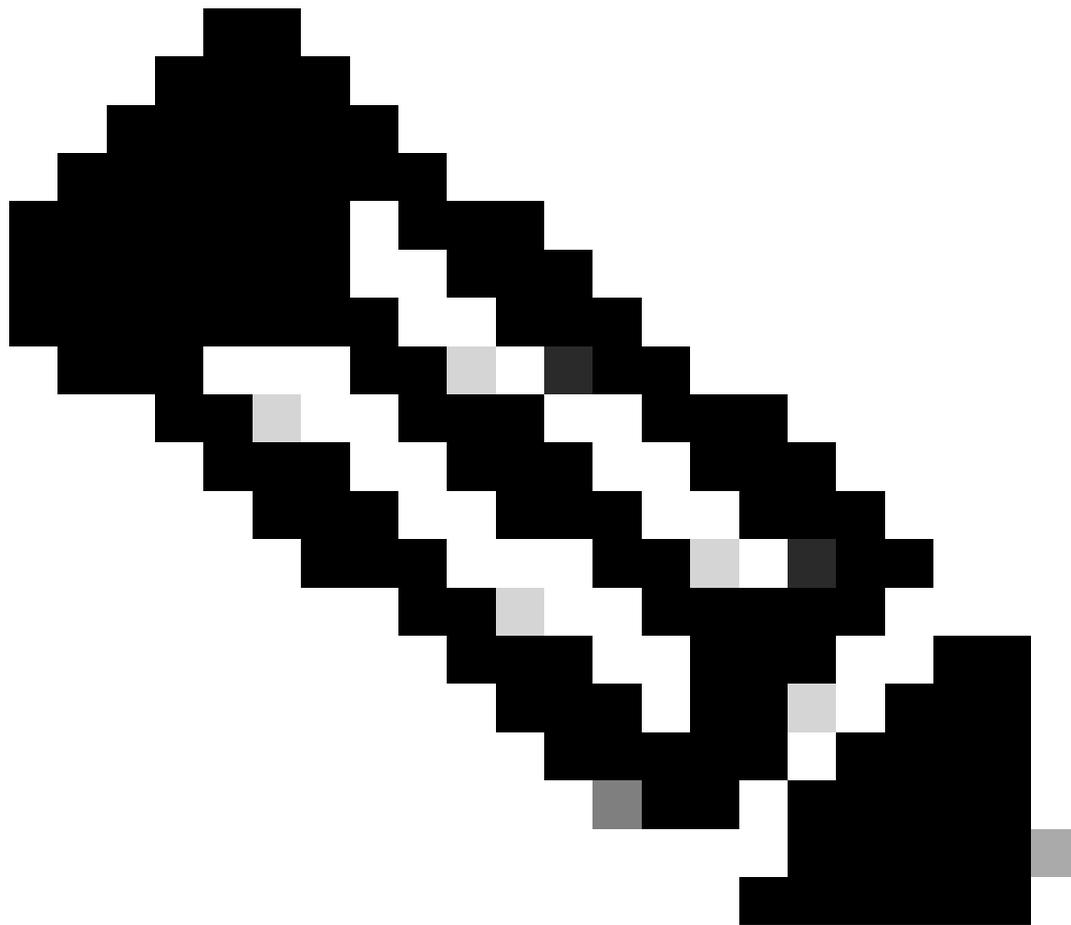
Authentication Protocols
Only Authentication Protocols relevant to TACACS are displayed.

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

TACACS Permitir protocolo

8. Navegue até  > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Clique adde crie dois perfis com base nos atributos da lista em Raw View. Clique em .Save

- Usuário Admin: `cisco-av-pair=shell:domains=all/admin/`
- Usuário administrador somente leitura: `cisco-av-pair=shell:domains=all/read-all`



Note: No caso de espaço ou caracteres adicionais, a fase de autorização falha.

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

Perfil TACACS

Overview Identities User Identity Groups Ext Id Sources Network Resources

TACACS Profiles

Refresh Add Duplicate Trash Edit

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

Perfis de administrador TACACS e de administrador somente leitura

Etapa 9. Navegue até **≡ >Work Centers > Device Administration > Device Admin Policy Set.** Crie um Novo Conjunto de Políticas, defina um nome e escolha o tipo de dispositivo APIC criado na Etapa 1. Escolha TACACS Protocol criado na Etapa 7. como Protocolo permitido e clique em Save.

Policy Sets Reset [Reset Policyset 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		

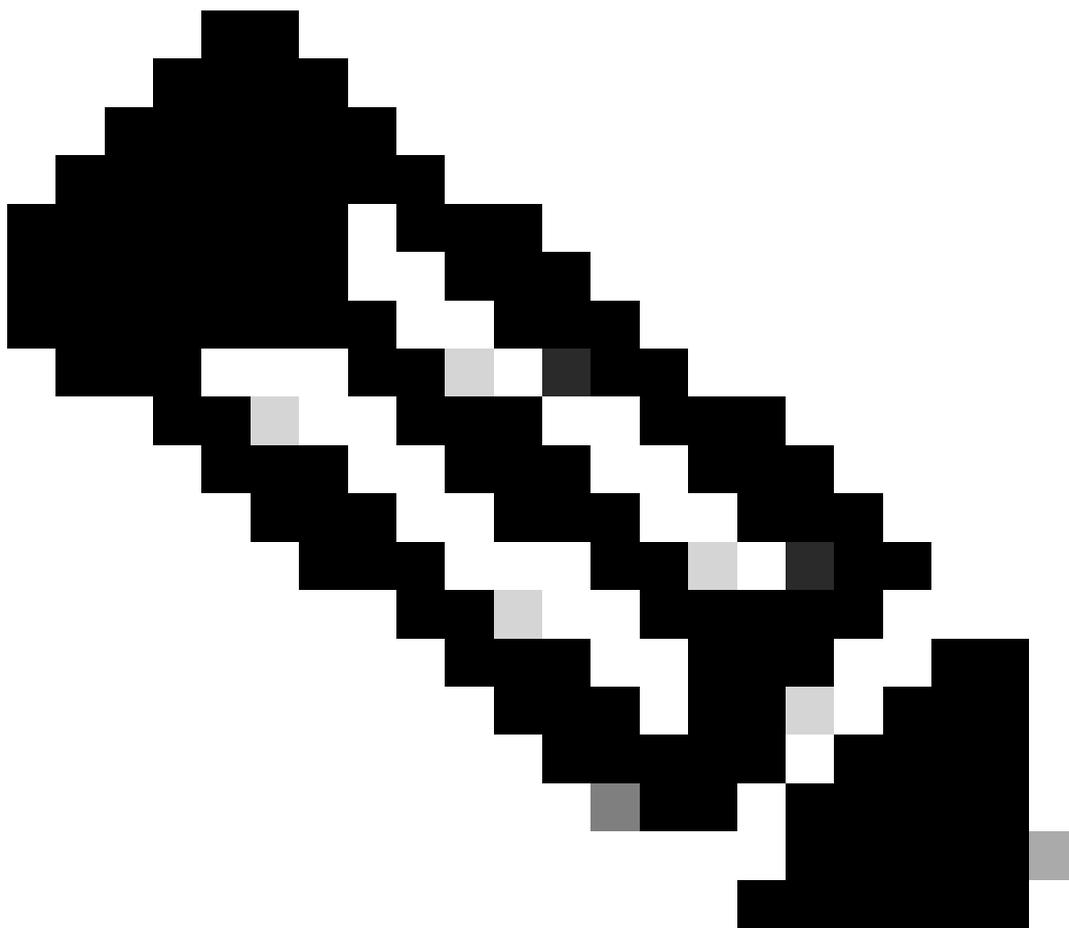
Conjunto de políticas TACACS

Etapa 10. Em newPolicy Set, clique na seta para a direita e crie uma política de autenticação. Defina um nome e escolha o endereço IP do dispositivo como a condição. Em seguida, escolha a Sequência de Origem da Identidade criada na Etapa 6.

Authentication Policy (2)

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

Política de autenticação



Note: O local ou outros atributos podem ser usados como uma condição de autenticação.

Etapa 11. Crie um perfil de Autorização para cada tipo de Usuário Admin, defina um nome e escolha um usuário interno e/ou grupo de usuários do AD como a condição. Condições adicionais, como APIC, podem ser usadas. Escolha o perfil de shell apropriado em cada política de autorização e clique em save.

Authorization Policy (3)

Status	Rule Name	Conditions	Results		
			Command Sets	Shell Profiles	Hits
ON	APIC Admin RO	AND Network Access Device IP Address EQUALS :188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO		APIC ReadOnly Profile	34
ON	APIC Admin User	AND Network Access Device IP Address EQUALS :188.21 OR IdentityGroup-Name EQUALS User Identity Groups:APIC_RW IsLab-ExternalGroups EQUALS cisco:lab/Bullin/Administrators		APIC ReadWrite Profile	16
ON	Default		DenyAllCommands	Deny All Shell Profile	0

Perfil de autorização TACACS

Verificar

Etapa 1. Fazer login na interface do usuário do APIC com credenciais de administrador do usuário. Escolha a opção TACACS na lista.

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

Login no APIC

Etapa 2. Verificar se o acesso na interface do usuário do APIC e se as políticas apropriadas foram aplicadas aos registros TACACS Live.

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](#)

Mensagem de boas-vindas do APIC

Repita as etapas 1 e 2 para usuários Administradores somente leitura.

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
×	▼		Identity	▼	Authentication Policy	Authorization Policy	Ise Node	Network Device N...
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	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+ Live Logs

Troubleshooting

Etapa 1. Navegue até ☰ >Operations > Troubleshoot > Debug Wizard. Escolha TACACSe clique em 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

Depurar Configuração do Perfil

Etapa 2. Escolha o nó que recebe o tráfego e clique em **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](#)

Depurar Seleção de Nós

Etapa 3. Execute um novo teste e faça o download dos logs em [Operations > Troubleshoot > Download logs](#) como mostrado:

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

Caso as depurações não mostrem informações de autenticação e autorização, valide isso:

1. O serviço Administração de dispositivos está habilitado no nó ISE.
2. O endereço IP correto do ISE foi adicionado à configuração do APIC.
3. Caso haja um firewall no meio, verifique se a porta 49 (TACACS) é permitida.

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.