

Configuración de APIC para la administración de dispositivos con ISE y TACACS+

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Procedimiento de autenticación](#)

[Configuración de APIC](#)

[Configuración de ISE](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe el procedimiento para integrar APIC con ISE para la autenticación de usuarios administradores con el protocolo TACACS+.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de infraestructura de política de aplicación (APIC)
- Identity Services Engine (ISE)
- protocolo TACACS

Componentes Utilizados

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

- APIC versión 4.2(7u)
- Parche 1 de ISE versión 3.2

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

Diagrama de la red



Diagrama de integración


Procedimiento de autenticación

Paso 1. Inicie sesión en la aplicación APIC con las credenciales del usuario administrador.


Paso 2. El proceso de autenticación se activa e ISE valida las credenciales localmente o a través de Active Directory.

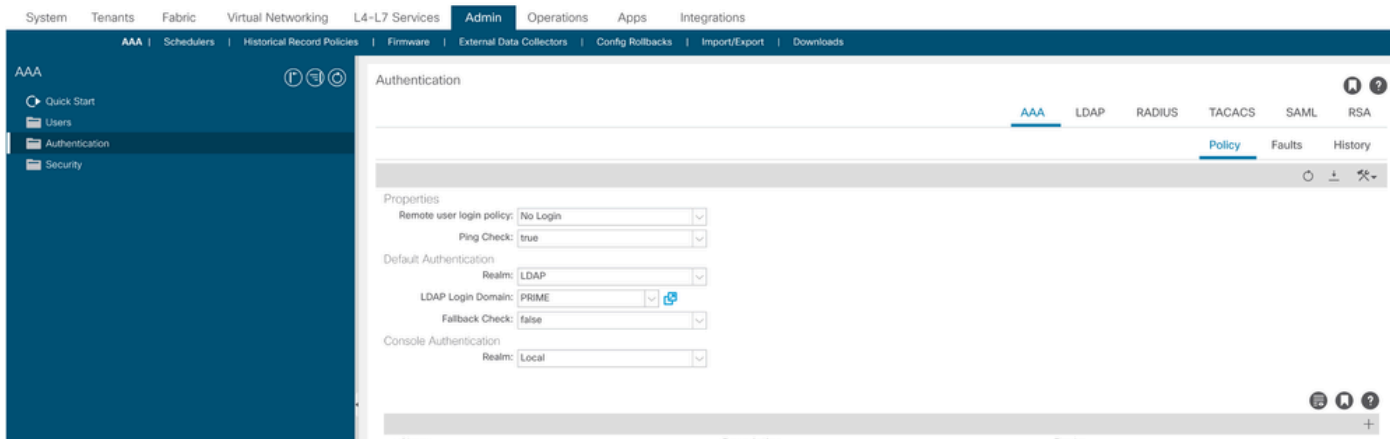
Paso 3. Una vez que la autenticación es satisfactoria, ISE envía un paquete de permiso para autorizar el acceso al APIC.

Paso 4. ISE muestra un registro en directo de autenticación correcta.

 Nota: APIC replica la configuración de TACACS+ en switches de hoja que forman parte del fabric.

Configuración de APIC

Paso 1. Navegue hasta `Admin > AAA > Authentication > AAA` y seleccione  para crear un nuevo dominio de conexión.



Configuración de administración de inicio de sesión APIC

Paso 2. Defina un nombre y un rango para el nuevo dominio de inicio de sesión y haga clic+bajo Proveedores para crear un nuevo proveedor.

Create Login Domain

Name:

Realm:

Description:

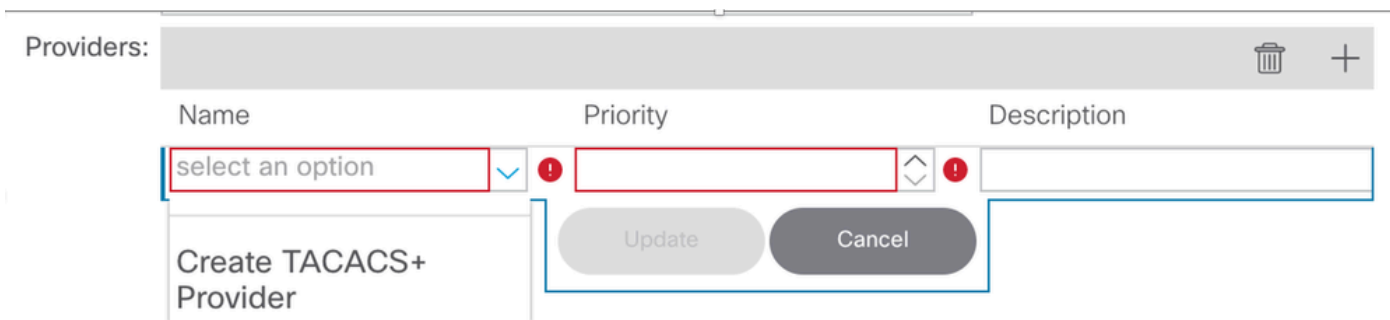
Providers: 🗑️ +

Name	Priority	Description

Cancel

Submit

administrador de inicio de sesión APIC



Proveedor TACACS de APIC

Paso 3. Defina la dirección IP o el nombre de host de ISE, defina un secreto compartido y

seleccione la gestión Grupo de políticas de terminales (EPG). Haga clic **Submit** para agregar el proveedor TACACS+ al login admin.

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol:

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring:

Cancel **Submit**

Configuración del proveedor TACACS de APIC

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

Cancel **Submit**

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

vista de proveedor TACACS

Configuración de ISE

Paso 1. Navegue hasta **Administration > Network Resources > Network Device Groups**. Cree un grupo de dispositivos de red en Todos los tipos de dispositivos.

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 red ISE

Paso 2. Desplácese hasta **Administration > Network Resources > Network Devices**. Elija **Add** defina APIC Name and IP address, elija APIC bajo Device Type y la casilla de verificación TACACS+, y defina la contraseña utilizada en la configuración del proveedor APIC TACACS+. Haga clic en **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 el paso 1 y el paso 2 para los modificadores de hoja.

Paso 3. Utilice las instrucciones de este enlace para integrar ISE con Active Directory;

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



Nota: Este documento incluye usuarios internos y grupos de administradores de AD como orígenes de identidad; sin embargo, la prueba se realiza con el origen de identidad de los usuarios internos. El resultado es el mismo para los grupos AD.

Paso 4. (Opcional) Desplácese hasta **☰** >Administration > Identity Management > Groups. Elija **User Identity Groups** y haga clic en **Add**. Cree un grupo para usuarios administradores de solo lectura y usuarios administradores.

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	
<input type="checkbox"/>	APIC_RW	

Grupo de identidad

Paso 5. (Opcional) Navegue hasta ☰ > Administration > Identity Management > Identity. Haga clic Addy cree un Read Only Adminusuario y unAdminusuario. Asigne cada usuario a cada grupo creado en el paso 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

Paso 6. Vaya a ☰ > Administration > Identity Management > Identity Source Sequence. ElijaAdd, defina un nombre y elijaAD Join Pointsy Origen deInternal Usersidentidad en la lista. ElijaTreat as if the user was not found and proceed to the next store in the sequencebajoAdvanced Search List Settingsy haga clic enSave.

∨ 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

Secuencia de origen de identidad

7. Navegue hasta ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Select Add,

defina un nombre y desmarque Allow CHAP y Allow MS-CHAPv1 de la lista de protocolos de autenticación. Seleccione Guardar.

≡ Cisco ISE

Overview Identities User Identity Groups Ext Id Sources Network Resources

Conditions >

Network Conditions >

Results v

Allowed Protocols

TACACS Command Sets

TACACS Profiles

[Allowed Protocols Services List](#) > TACACS Protocol

Allowed Protocols

Name: TACACS Protocol

Description:

Allowed Protocols

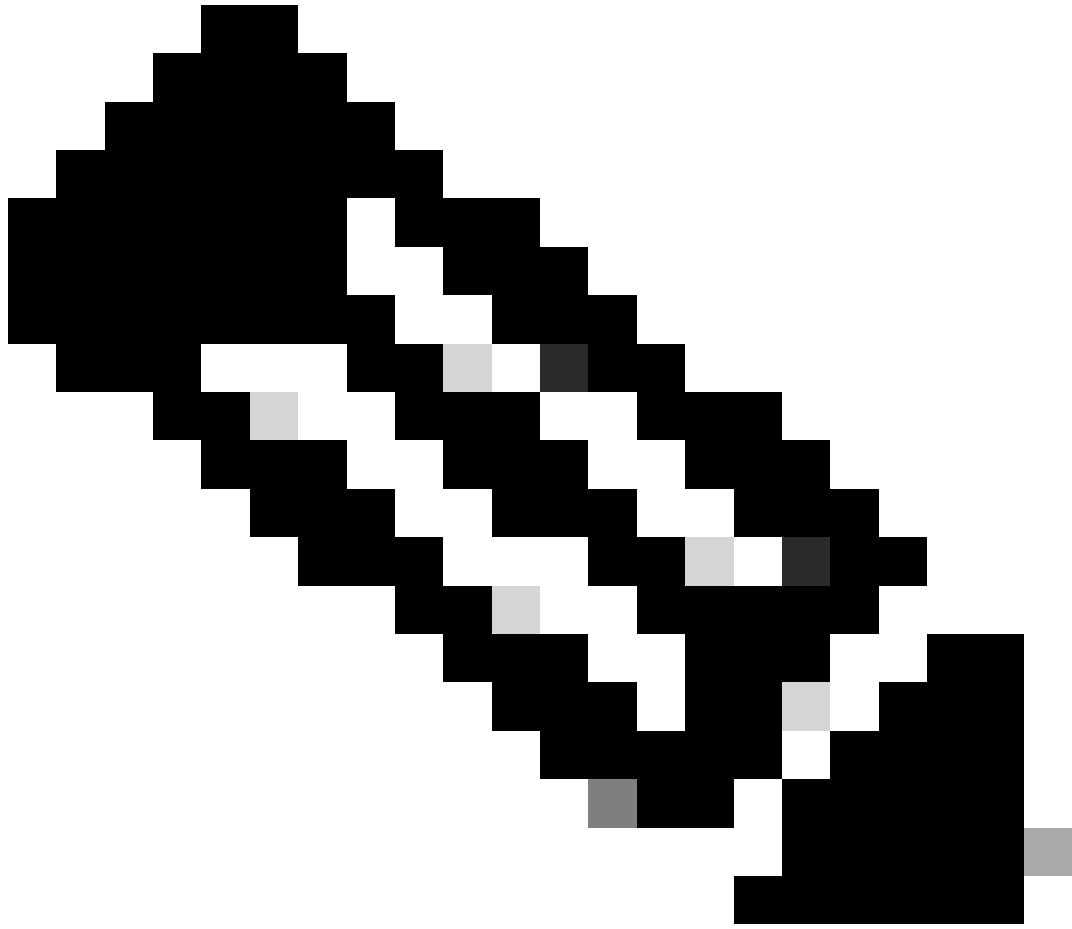
Authentication Protocols
Only Authentication Protocols relevant to TACACS are displayed.

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

Protocolo TACACS Allow

8. Acceda a **≡** >Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Haga clic en **yadd** cree dos perfiles basados en los atributos de la lista de **Raw View**. Haga clic en **Save**.

- Usuario administrador: `cisco-av-pair=shell:domains=all/admin/`
- Usuario administrador de solo lectura: `cisco-av-pair=shell:domains=all/read-all`



Nota: En caso de espacios o caracteres adicionales, la fase de autorización falla.

- 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

Perfil TACACS

- 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	

Perfiles de administración de TACACS y de administración de solo lectura

Paso 9. Desplácese hasta >Work Centers > Device Administration > Device Admin Policy Set. Cree un nuevo juego de políticas, defina un nombre y elija el tipo de dispositivo APIC creado en el paso 1. Seleccione TACACS Protocol creado en el paso 7. como protocolo permitido y haga clic en 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		

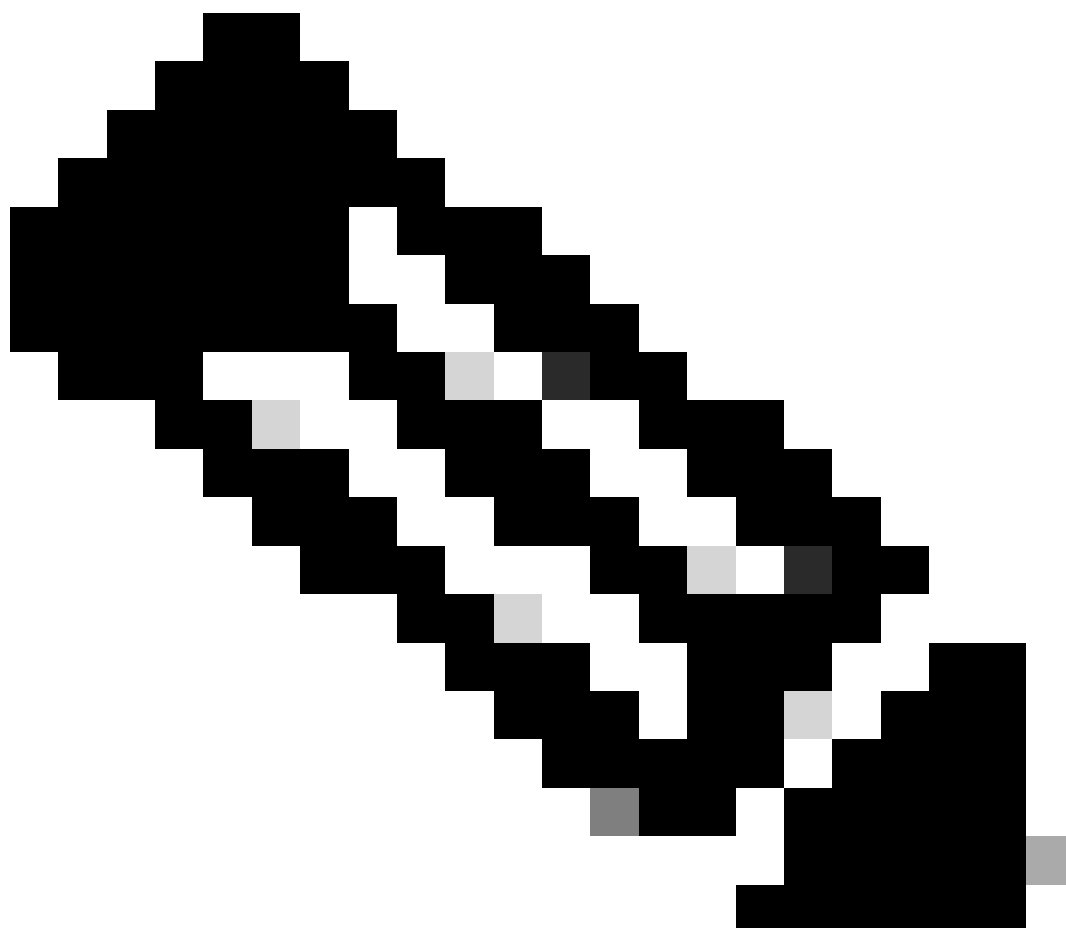
Conjunto de políticas TACACS

Paso 10. En nuevo Policy Set, haga clic en la flecha derecha y cree una política de autenticación. Defina un nombre y elija la dirección IP del dispositivo como condición. A continuación, seleccione la secuencia de origen de identidad creada en el paso 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 autenticación



Nota: La ubicación u otros atributos se pueden utilizar como condición de autenticación.

Paso 11. Cree un perfil de autorización para cada tipo de usuario administrador, defina un nombre y elija un usuario interno y/o un grupo de usuarios AD como condición. Se pueden utilizar condiciones adicionales como APIC. Elija el perfil de shell adecuado en cada política de autorización y haga clic en 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 OR Network Access Device IP Address EQUALS :188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RW Iselab-ExternalGroups EQUALS cisco:lab/Bullin/Administrators		APIC ReadWrite Profile	16
ON	Default		DenyAllCommands	Deny All Shell Profile	0

Perfil de autorización TACACS

Verificación

Paso 1. Inicie sesión en la interfaz de usuario de APIC con credenciales de administrador de usuarios. Elija la opción TACACS de la lista.

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

Inicio de sesión en APIC

Paso 2. Verifique el acceso en la interfaz de usuario de APIC y se aplican las políticas adecuadas en los registros de 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](#)

mensaje de bienvenida de APIC

Repita los pasos 1 y 2 para los usuarios administradores de sólo lectura.

☰ 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)

Registros en directo de TACACS+

Troubleshoot

Paso 1. Vaya a ☰ >Operations > Troubleshoot > Debug Wizard. Elija TACACSy haga clic en 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

Configuración del perfil de depuración

Paso 2. Elija el nodo que recibe el tráfico y haga clic en **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](#)

Selección de nodos de depuración

Paso 3. Realice una nueva prueba y descargue los registros en `Operations > Troubleshoot > Download logs` como se muestra:

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

En caso de que los debugs no muestren información de autenticación y autorización, valide esto:

1. El servicio Device Administration está habilitado en el nodo ISE.
2. Se ha agregado la dirección IP de ISE correcta a la configuración de APIC.
3. En caso de que haya un firewall en el medio, verifique que el puerto 49 (TACACS) esté permitido.

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).