

Configurer APIC pour l'administration des périphériques avec ISE et TACACS+

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Procédure D'Authentification](#)

[Configuration APIC](#)

[Configuration ISE](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit la procédure pour intégrer APIC avec ISE pour l'authentification des utilisateurs administrateurs avec le protocole TACACS+.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Contrôleur des infrastructures des politiques relatives aux applications (APIC)
- Moteur du service de vérification des identités (ISE)
- protocole TACACS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- APIC version 4.2(7u)
- ISE version 3.2 Patch 1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau



Diagramme D'Intégration


Procédure D'Authentification

Étape 1. Connectez-vous à l'application APIC avec les informations d'identification utilisateur Admin.

Étape 2. Le processus d'authentification déclenche et ISE valide les informations d'identification localement ou via Active Directory.

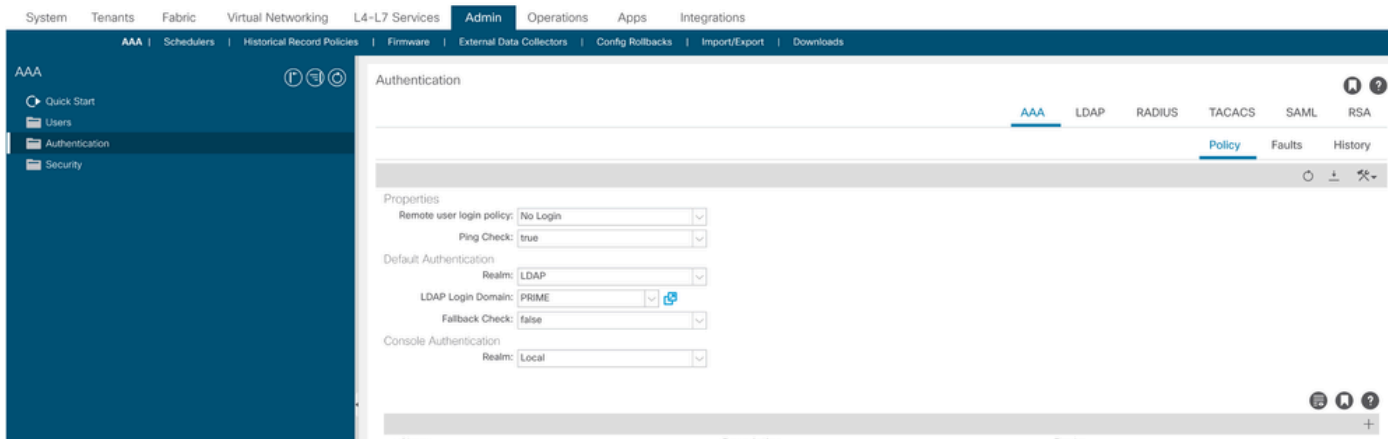
Étape 3. Une fois l'authentification réussie, ISE envoie un paquet d'autorisation pour autoriser l'accès au contrôleur APIC.

Étape 4. ISE affiche un journal en direct d'authentification réussi.

 Remarque : Le contrôleur APIC réplique la configuration TACACS+ sur les commutateurs Leaf qui font partie du fabric.

Configuration APIC

Étape 1. Naviguez jusqu'à Admin > AAA > Authentication > AAA et choisissez l'icône afin de créer un nouveau domaine de connexion.



Configuration admin de connexion APIC

Étape 2. Définissez un nom et un domaine pour le nouveau domaine de connexion et cliquez sur **Providers** afin de créer un nouveau fournisseur.

Create Login Domain

Name:

Realm:

Description:

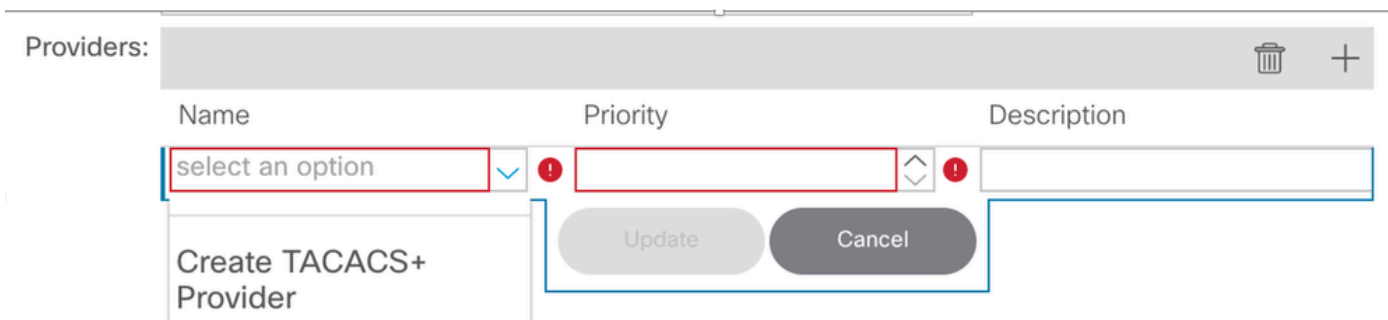
Providers: 🗑️ +

Name	Priority	Description

Cancel

Submit

Administrateur de connexion APIC



Fournisseur TACACS APIC

Étape 3 : définition de l'adresse IP ISE ou du nom d'hôte, définition d'un secret partagé et

sélection du groupe de stratégie de point de terminaison (EPG) de gestion Cliquez pour Submit ajouter TACACS+ Provider à login admin.

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol:

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring:

Paramètres du fournisseur TACACS APIC

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

Vue Fournisseur TACACS

Configuration ISE

Étape 1. Accédez à  Administration > Network Resources > Network Device Groups. Créez un groupe de périphériques réseau sous Tous les types de périphériques.

 **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	

Groupes de périphériques réseau ISE

Étape 2. Accédez à Administration > Network Resources > Network Devices. Choisissez **Add** define APIC Name and IP address, choisissez APIC sous Device Type et TACACS+ case à cocher, et définissez le mot de passe utilisé sur la configuration du fournisseur APIC TACACS+. Cliquez sur **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

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

RADIUS Authentication Settings

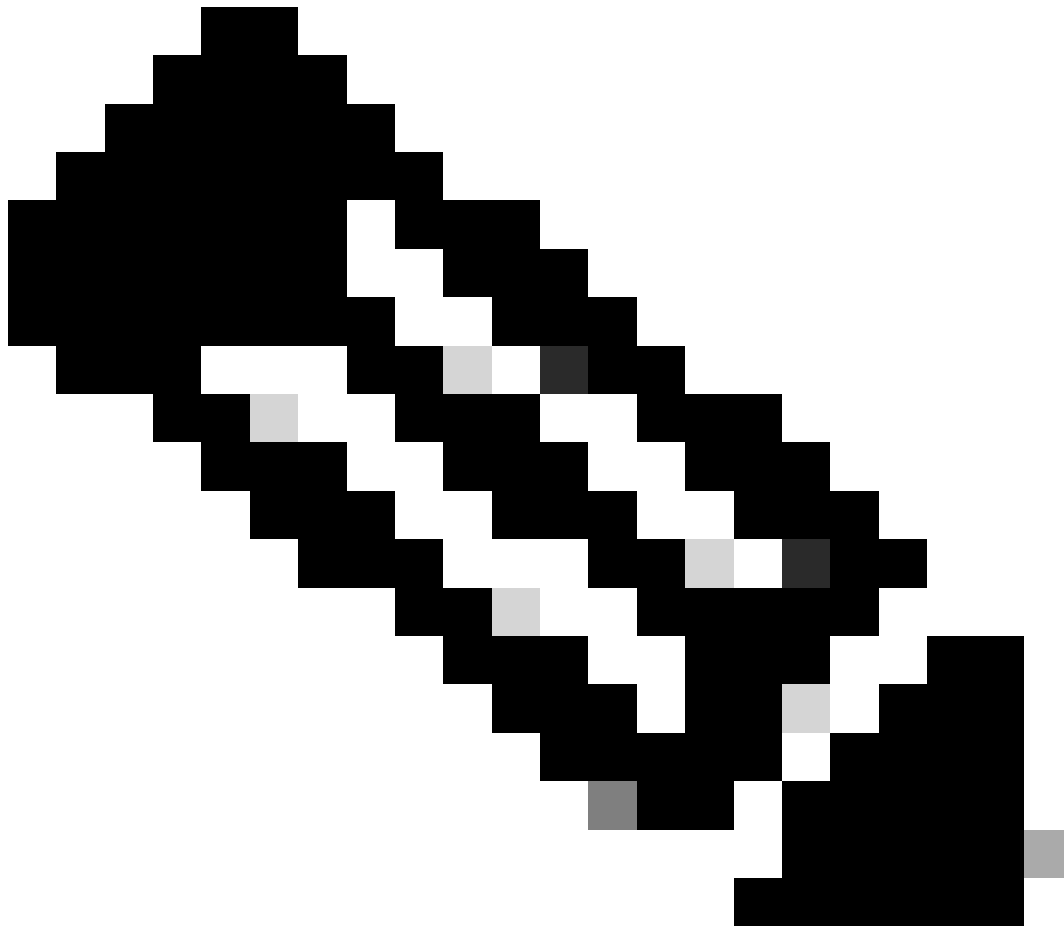
TACACS Authentication Settings

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

Répétez les étapes 1 et 2 pour les commutateurs Leaf.

Étape 3. Utilisez les instructions sur ce lien afin d'intégrer ISE avec 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>.



Remarque : Ce document inclut des utilisateurs internes et des groupes d'administrateurs AD en tant que sources d'identité. Toutefois, le test est effectué avec la source d'identité des utilisateurs internes. Le résultat est le même pour les groupes AD.

Étape 4. (Facultatif) Accédez à **☰**>Administration > Identity Management > Groups. Sélectionnez **User Identity Groups** et cliquez sur **Add**. Créez un groupe pour les utilisateurs Admin en lecture seule et les utilisateurs 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	
<input type="checkbox"/>	APIC_RW	

Groupe d'identité

Étape 5. (Facultatif) Accédez à ☰ > Administration > Identity Management > Identity. Cliquez sur Add et créez un Read Only Admin utilisateur et un Admin utilisateur. Attribuez chaque utilisateur à chaque groupe créé à l'étape 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

Étape 6. Accédez à ☰ > Administration > Identity Management > Identity Source Sequence. Choisissez Add, définissez un nom, puis choisissez AD Join Points et Internal Users Source d'identité dans la liste. Choisissez Treat as if the user was not found and proceed to the next store in the sequence SOUS Advanced Search List Settings et cliquez sur 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

Séquence source d'identité

7. Accédez à ☰ > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Sélectionnez

Ajouter, définissez un nom et décochez Autoriser CHAP et Autoriser MS-CHAPv1 dans la liste des protocoles d'authentification. Sélectionnez Enregistrer.

☰ Cisco ISE

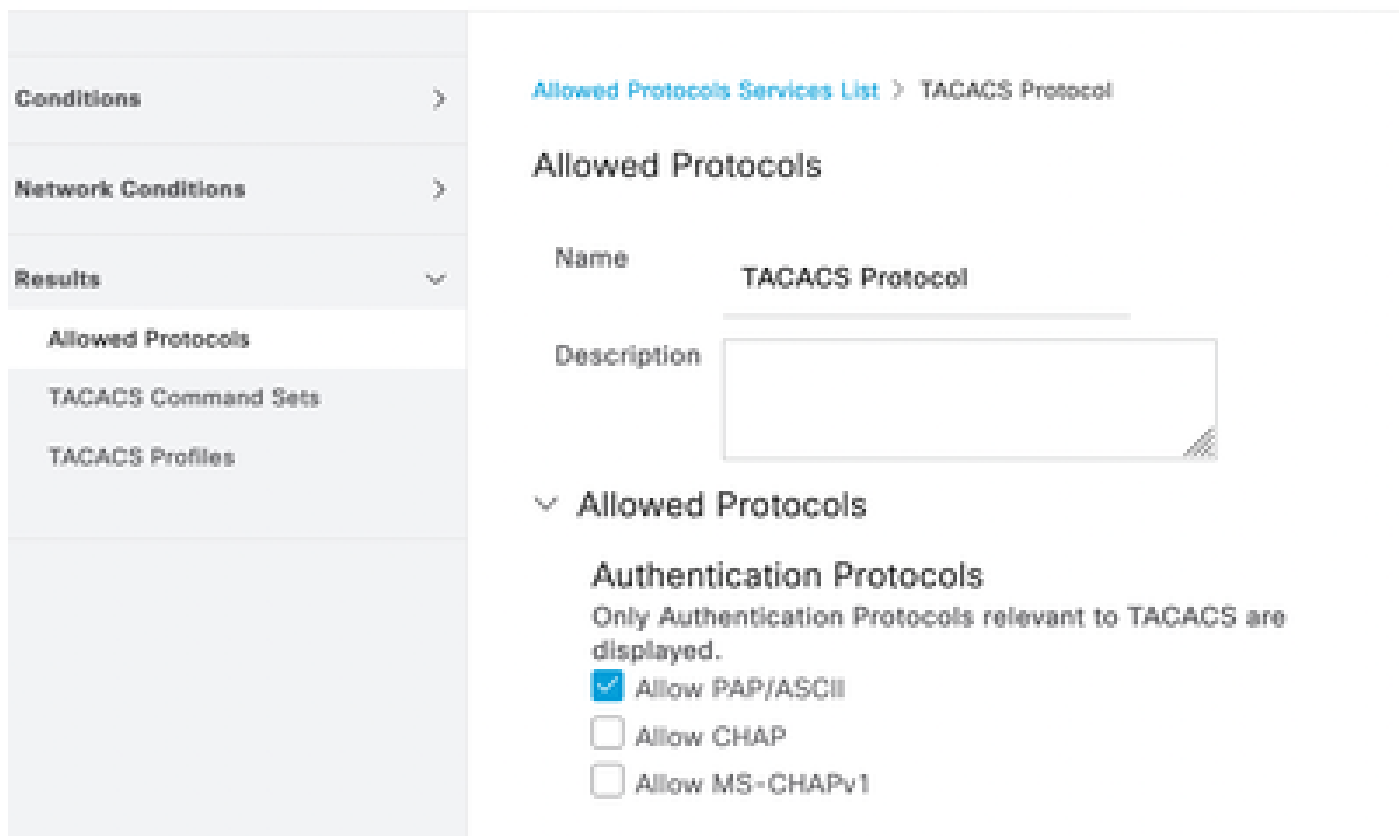
Overview

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

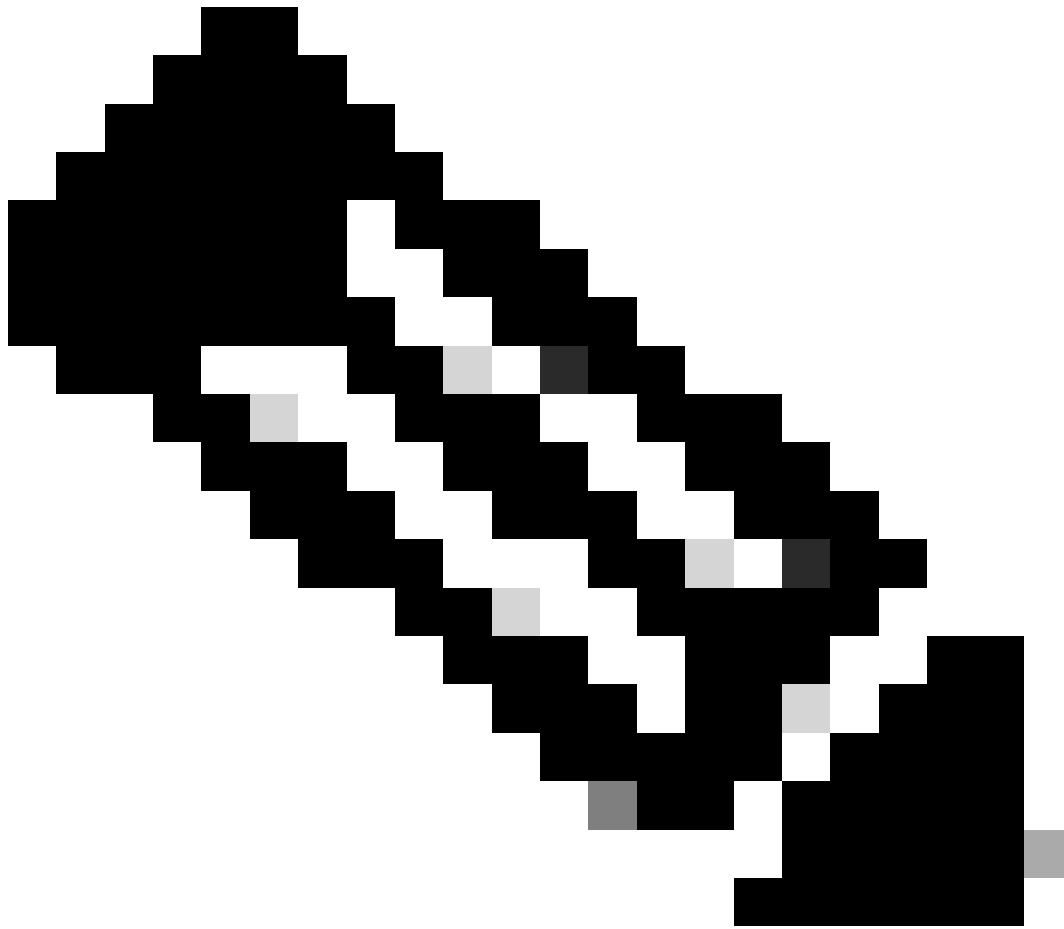
Only Authentication Protocols relevant to TACACS are displayed.

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

Protocole TACACS Allow

8. Accédez à ☰ > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Cliquez sur **add** et créez deux profils en fonction des attributs de la liste située sous **Raw View**. Cliquez sur **Save**.

- Utilisateur admin : `cisco-av-pair=shell:domains=all/admin/`
- Utilisateur admin en lecture seule : `cisco-av-pair=shell:domains=all/read-all`



Remarque : En cas d'espace ou de caractères supplémentaires, la phase d'autorisation échoue.

- 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

Profil 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	

Profil admin TACACS et admin en lecture seule

Étape 9. Accédez à > Work Centers > Device Administration > Device Admin Policy Set. Créez un nouvel ensemble de stratégies, définissez un nom et choisissez le type de périphérique APIC créé à l'étape 1. Choisissez TACACS Protocol créé à l'étape 7. comme protocole autorisé, puis cliquez sur 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		

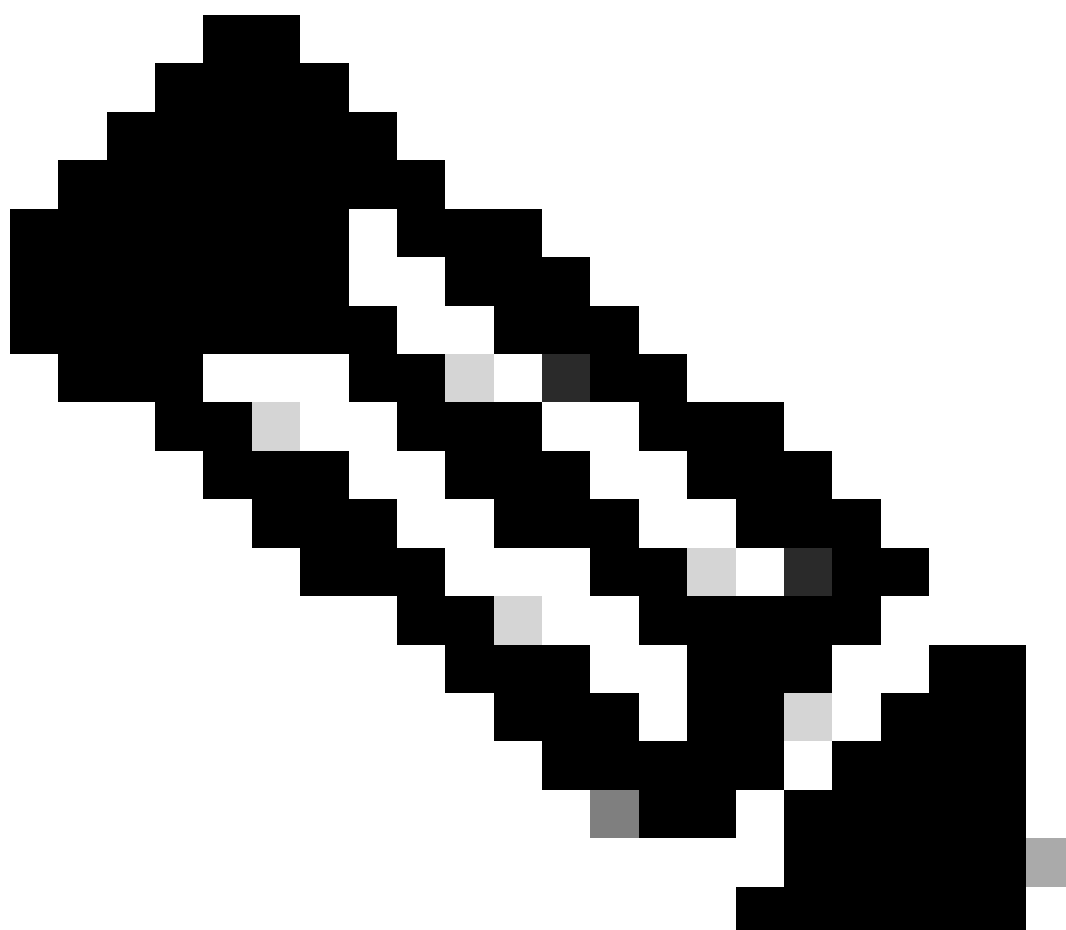
Ensemble de politiques TACACS

Étape 10. Sous newPolicy Set, cliquez sur la flèche droite et créez une stratégie d'authentification. Définissez un nom et choisissez l'adresse IP du périphérique comme condition. Sélectionnez ensuite la séquence source d'identité créée à l'étape 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

Stratégie d'authentification



Remarque : L'emplacement ou d'autres attributs peuvent être utilisés comme condition d'authentification.

Étape 11. Créez un profil d'autorisation pour chaque type d'utilisateur Admin, définissez un nom et choisissez un utilisateur interne et/ou un groupe d'utilisateurs AD comme condition. D'autres conditions, telles qu'un APIC, peuvent être utilisées. Sélectionnez le profil d'environnement approprié pour chaque stratégie d'autorisation et cliquez sur 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 .188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO	APIC ReadOnly Profile			34	⚙️
●	APIC Admin User	AND OR Network Access Device IP Address EQUALS .188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RW IsExternalGroups EQUALS cisco:lab/Bullfin/Administrators	APIC ReadWrite Profile			18	⚙️
●	Default		DenyAllCommands		Deny All Shell Profile	0	⚙️

Profil d'autorisation TACACS

Vérifier

Étape 1. Connectez-vous à l'interface utilisateur APIC avec les informations d'identification administrateur utilisateur. Sélectionnez l'option TACACS dans la liste.

APIC
Version 4.2(7u)
CISCO

User ID
APIC_ROUser

Password
.....

Domain
S_TACACS

Login

Connexion APIC

Étape 2 : vérification de l'accès à l'interface utilisateur APIC et application des stratégies appropriées aux journaux 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](#)

Message de bienvenue APIC

Répétez les étapes 1 et 2 pour les utilisateurs Admin en lecture seule.

☰ 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)





Journaux TACACS+ en direct

Dépannage

Étape 1. Accédez à ☰ > Operations > Troubleshoot > Debug Wizard. Sélectionnez TACACS et cliquez sur 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

Configuration du profil de débogage

Étape 2. Choisissez le noeud qui reçoit le trafic et cliquez sur **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](#)

Sélection des noeuds de débogage

Étape 3. Effectuez un nouveau test et téléchargez les journaux sous `Operations > Troubleshoot > Download logs` comme indiqué :

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

Si les débogages n'affichent pas les informations d'authentification et d'autorisation, validez ceci :

1. Le service d'administration des périphériques est activé sur le noeud ISE.
2. L'adresse IP ISE correcte a été ajoutée à la configuration APIC.
3. Si un pare-feu se trouve au milieu, vérifiez que le port 49 (TACACS) est autorisé.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.