

Configurez l'authentification de la perfection 3.1 TACACS contre ISE 2.x

Contenu

[Introduction](#)

[Conditions requises](#)

[Configurez](#)

[Configuration principale](#)

[Configuration ISE](#)

[Dépannez](#)

Introduction

Ce document décrit comment configurer l'infrastructure principale pour authentifier par l'intermédiaire de TACACS avec ISE 2.x.

Conditions requises

Cisco recommande que vous ayez une connaissance de base de ces thèmes :

- Cisco Identity Services Engine (ISE)
- Infrastructure principale

Configurez

Cisco Prime Network Control System 3.1

Engine 2.0 de gestion d'identité de Cisco ou plus tard.

(Note : ISE prend en charge seulement TACACS commençant par la version 2.0, cependant il est possible de configurer la perfection utiliser Radius. La perfection inclut la liste d'attributs RADIUS en plus de TACACS si vous préféreriez utiliser Radius, avec une version plus ancienne d'ISE ou d'une solution de tiers.)

Configuration principale

Navigiate à l'écran suivant : Gestion/utilisateurs, rôles et AAA d'utilisateurs comme vu ci-dessous.

Une fois que là, sélectionnent l'onglet de serveurs TACACS+, puis sélectionnez l'option de serveur de l'ajouter TACACS+ dans le coin supérieur droit et choisi allez.

Sur l'écran suivant la configuration de l'entrée de serveur TACACS est disponible (ceci devra être faite pour chaque serveur TACACS individuel)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address
 DNS Name
 * Port
 Shared Secret Format
 * Shared Secret
 * Confirm Shared Secret
 * Retransmit Timeout (secs)
 * Retries
 Authentication Type
 Local Interface IP

Save Cancel

Voici que vous devrez introduire l'adresse IP ou l'adresse DNS du serveur, aussi bien que la clé secrète partagée. Veuillez également noter l'IP d'interface locale que vous voudriez utiliser, comme cette même adresse IP doit être utilisée pour le client d'AAA dans ISE plus tard.

Afin de se terminer la configuration sur la perfection. Vous devrez activer TACACS sous la gestion/utilisateurs/utilisateurs, les rôles et l'AAA sous l'onglet de configurations de mode d'AAA.

(Note : Il est recommandé pour vérifier le retour d'enable à l'option locale, avec SEULEMENT en aucune réponse de serveur ou en fonction l'aucune option de réponse ou de panne, particulièrement tout en testant la configuration)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

AAA Mode Settings

AAA Mode Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respon:

Save

Configuration ISE

Configurez la perfection en tant que client d'AAA sur ISE aux centres de travail/à gestion de périphérique/aux ressources de réseau/aux périphériques de réseau/ajoutez

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration

Overview Identities User Identity Groups Ext Id Sources Network Resources Network Device Groups Policy Elements Device Admin Policy Sets Reports Settings

Network Devices

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices

Selected 0 | Total 0

Edit Add Duplicate Import Export Generate PAC Delete Show All

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

Écrivez les informations pour le serveur principal. Les attributs exigés que vous devez inclure sont nom, adresse IP, sélectionnent l'option pour TACACS et le secret partagé. Vous pouvez supplémentaire souhaiter ajouter un type de périphérique, spécifiquement pour la perfection, afin d'utiliser plus tard comme condition pour la règle d'autorisation ou d'autres informations, toutefois c'est facultative.

Network Devices List > New Network Device

Network Devices

Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

Créez alors un résultat de profil TACACS pour envoyer les attributs requis d'ISE pour amorcer, pour fournir le niveau d'accès correct. Naviguez vers des centres de travail/résultats de stratégie/profils de Tacacs et sélectionnez l'option d'ajouter.

Identity Services Engine

Home > Operations > Policy > Guest Access > Administration > Work Centers

TrustSec > Device Administration

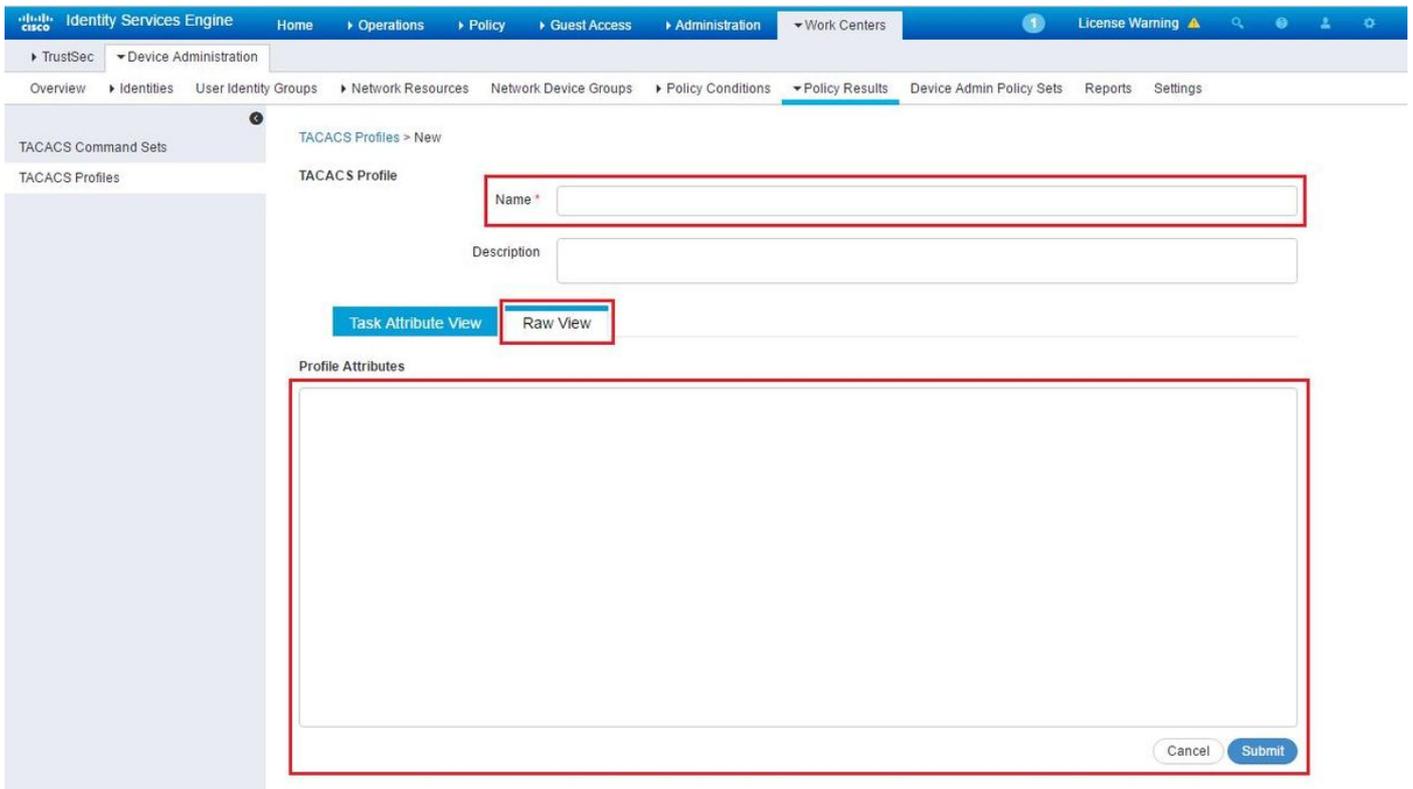
Overview > Identities > User Identity Groups > Network Resources > Network Device Groups > Policy Conditions > Policy Results > Device Admin Policy Sets > Reports > Settings

TACACS Profiles

Rows/Page 6 / 1 / 1 Go 6 Total Rows

Name	Description
------	-------------

Configurez le nom, et employez l'option crue de vue afin d'écrire les attributs sous la case d'attributs de profil. Les attributs proviendront le serveur d'amorce lui-même.



Obtenez les attributs sous la gestion/utilisateurs d'utilisateurs, les rôles et l'écran d'AAA, et sélectionnez l'onglet de groupes d'utilisateurs. Voici que vous sélectionnez le niveau du groupe de l'accès que vous souhaitez fournir. Dans cet admin d'exemple l'accès est fourni en sélectionnant la liste des tâches appropriée du côté gauche.

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		Task List
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
User Groups	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

Copiez tous les attributs personnalisés TACACS.

- AAA Mode Settings
- Active Sessions
- Change Password
- Local Password Policy
- RADIUS Servers
- SSO Server Settings
- SSO Servers
- TACACS+ Servers
- User Groups**
- Users

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point
Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point
Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click here.

Collez- alors les dans la section brute de vue du profil sur ISE.

The screenshot shows the 'TACACS Profile' configuration page in Cisco ISE. The 'Name' field is set to 'Prime'. The 'Raw View' tab is active, displaying the following task attributes:

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Les attributs personnalisés virtuels de domaine sont obligatoires. Les informations de Racine-domaine peuvent être trouvées sous la gestion principale -> les domaines virtuels.

The screenshot shows the 'Virtual Domains' configuration page in Cisco Prime Infrastructure. The 'Name' field is set to 'ROOT-DOMAIN' and the 'Description' field is also set to 'ROOT-DOMAIN'. The 'Time Zone' is set to '-- Select Time Zone --'. A red box highlights the 'Name' and 'Description' fields.

Le nom du domaine virtuel principal doit être ajouté comme nom de domaine de l'attribut **virtual-domain0="virtual** »

TACACS Profiles > Prime Access

TACACS Profile

Name: Prime Access

Description:

Task Attribute View | **Raw View**

Profile Attributes

```
task162=Monitor Mobility Devices
task163=Context Aware Reports
task164=Voice Diagnostics
task165=Configure Choke Points
task166=RRM Dashboard
task167=Swim Delete
task168=Theme Changer Access
task169=Import Policy Update
task170=Design Endpoint Site Association Access
task171=Planning Mode
task172=Pick and Unpick Alerts
task173=Configure Menu Access
task174=Ack and Unack Security Index Issues
task175=Ack and Unack Alerts
task176=Auto Provisioning
virtual-domain0=ROOT-DOMAIN
```

Cancel Save

Une fois que cela est fait tous vous devez faire doit créer une règle d'assigner le profil de shell créé dans l'étape précédente, dans le cadre des centres de travail/de la stratégie d'admin gestion de périphérique/périphérique place

(Note : Les « conditions » varieront selon le déploiement, toutefois vous pouvez utiliser le « type de périphérique » spécifiquement pour une perfection ou un type différent de filtre tel que l'adresse IP de la perfection, en tant qu'une de « conditionne » de sorte que cette règle filtre correctement des demandes)

Policy Sets

Search policy names & descriptions.

Summary of Policies

Global Exceptions

Default

Save Order Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

Authentication Policy

Default Rule (if no match) : Allow Protocols : Default Device Admin and use : Internal Users

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Prime Rule	if DEVICE Device Type EQUALS All Device Types#Prime	then PermitAll AND	Prime
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s) Deny All Shell Profile	

En ce moment la configuration devrait être complète.

Dépannez

Si cette configuration est infructueuse et si le local tombent de retour option était enable sur la perfection, vous pouvez forcer un basculer d'ISE, en retirant l'adresse IP de la perfection. Ceci fera ne pas répondre et forcer ISE l'utilisation des qualifications locales. Si le retour local est configuré pour être exécuté sur une anomalie, les comptes locaux fonctionneront et permettront d'accéder toujours au client.

S'ISE affiche une authentification réussie et apparie la règle correcte cependant la perfection rejette toujours la demande que vous pouvez souhaiter pour vérifier une deuxième fois les attributs êtes configuré correctement dans le profil et aucun attribut supplémentaire n'est envoyé.