

Configurer l'authentification TACACS+ sur CIMC avec le serveur ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configuration côté serveur TACACS+ pour association de privilèges](#)

[Configuration requise pour ISE](#)

[Configuration TACACS+ sur CIMC](#)

[Vérification](#)

[Vérification de la configuration à partir de l'interface de ligne de commande dans CIMC](#)

[Dépannage](#)

[Dépannage ISE](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration de l'authentification TACACS+ (Terminal Access Controller Access Control System Plus) sur le contrôleur de gestion intégré Cisco (CIMC).

TACACS+ est généralement utilisé pour authentifier les périphériques réseau avec un serveur central. Depuis la version 4.1(3b), Cisco IMC prend en charge l'authentification TACACS+. La prise en charge de TACACS+ sur CIMC facilite la gestion de plusieurs comptes d'utilisateurs ayant accès au périphérique. Cette fonctionnalité permet de modifier régulièrement les informations d'identification de l'utilisateur et de gérer les comptes utilisateur à distance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Integrated Management Controller (CIMC)
- Terminal Access Controller Access Control System Plus (TACACS+)

Components Used

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

- UCSC-C220-M4S

- Version CIMC : 4.1(3b)
- Cisco Identity Services Engine (ISE) version 3.0.0.458

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.

Configuration

Configuration côté serveur TACACS+ pour association de privilèges

Le niveau de privilège de l'utilisateur est calculé en fonction de la valeur **cisco-av-pair** configurée pour cet utilisateur. Une **paire cisco-av** doit être créée sur le serveur TACACS+ pour et les utilisateurs ne peuvent pas utiliser d'attributs TACACS+ par défaut. Les trois syntaxes indiquées ci-dessous sont prises en charge pour l'attribut **cisco-av-pair**

Pour le privilège **admin** :

```
cisco-av-pair=shell:roles="admin"
```

Pour le privilège **utilisateur** :

```
cisco-av-pair=shell:roles="user"
```

Pour les privilèges **en lecture seule** :

```
cisco-av-pair=shell:roles="read-only"
```

Pour prendre en charge d'autres périphériques, si d'autres rôles doivent être ajoutés, ils peuvent être ajoutés avec une virgule comme séparateur. Par exemple, UCSM prend en charge **aaa**, de sorte que **shell:rôles= " admin, aaa "** peut être configuré et CIMC accepte ce format.

Note: Si **cisco-av-pair** n'est pas configuré sur le serveur TACACS+, alors un utilisateur avec ce serveur a un privilège **en lecture seule**.

Configuration requise pour ISE

L'adresse IP de gestion du serveur doit être autorisée sur les périphériques réseau ISE.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration · Network Resources'. Below this, there are several tabs for different configuration areas: 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' tab is selected, and the main content area displays a table of network devices. The table has columns for 'Name', 'IP/Mask', 'Profile Name', 'Location', 'Type', and 'Description'. A red box highlights the first row, which contains the following data: Name: CIMC_4.1b, IP/Mask: 10.31.123.2, Profile Name: Cisco, Location: All Locations, Type: All Device Types, and Description: (empty).

Name	IP/Mask	Profile Name	Location	Type	Description
CIMC_4.1b	10.31.123.2	Cisco	All Locations	All Device Types	
Prime Test	10.201.222	Cisco	All Locations	All Device Types	

Mot de passe secret partagé à saisir sur CIMC.

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server

Network Devices

Default Device

Device Security Settings

Network Devices List > CIMC_4.1b

Network Devices

* Name Description IP Address / * Device Profile Model Name Software Version

* Network Device Group

Location IPSEC Device Type TEST

Shared Secret

Cisc0123

Profil Shell avec attribut **cisco-av-pair** avec autorisations admin.

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

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

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

+ Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles+ admin*

Configuration TACACS+ sur CIMC

Étape 1. Accédez à **Admin > User Management > TACACS+**

Étape 2. Cochez la case pour activer **TACACS+**

Étape 3. Un nouveau serveur peut être ajouté à l'une des 6 lignes spécifiées dans le tableau. Cliquez sur la ligne ou sélectionnez-la et cliquez sur le bouton **modifier** en haut du tableau, comme illustré dans cette image.

TACACS+ Properties

Enabled: 1 ←

Fallback only on no connectivity:

Timeout (for each server): (5 - 30 Seconds)

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key
<input type="radio"/> 1			
<input type="radio"/> 2			
<input type="radio"/> 3			
<input type="radio"/> 4			
<input type="radio"/> 5			
<input type="radio"/> 6			

Note: Dans le cas où un utilisateur a activé la fonctionnalité de secours TACACS+ sur aucune option de connectivité, CIMC impose que la première priorité d'authentification doit toujours être définie sur TACACS+, sinon la configuration de secours pourrait devenir inpertinente.

Étape 4. Complétez l'adresse IP ou le nom d'hôte, le port et la clé de serveur/secret partagé et **enregistrez** la configuration.

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key	Confirm Server Key
1	<input type="text" value="10.31.126.220"/>	<input type="text" value="49"/>	<input type="text" value="....."/>	<input type="text" value="....."/>
2				
3				
4				
5				

Save | Cancel

Cisco IMC prend en charge jusqu'à six serveurs distants TACACS+. Une fois qu'un utilisateur est authentifié avec succès, le nom d'utilisateur est ajouté à (TACACS+).



Refresh | ? | i

Ceci est également affiché dans la Gestion des sessions

Sessions

Selected 0 / Total 1 ⚙

Terminate Session				
	Session ID	User Name	IP Address	Session Type
<input type="checkbox"/>	81	tacacs_user (TACACS+)	10.24.92.202	webgui

Vérification

- Un maximum de 6 serveurs TACACS+ peut être configuré sur le CIMC.
- La clé secrète associée au serveur peut comporter jusqu'à 64 caractères.
- Le délai d'attente peut être configuré entre 5 et 30 secondes (ce qui équivaut à 180 secondes maximum pour être conforme à LDAP).
- Si un serveur TACACS+ doit utiliser le nom de service pour créer la **paire cisco-av**, les utilisateurs doivent utiliser **Se connecter** comme nom de service.
- Aucune prise en charge du sébaste pour modifier les configurations.

Vérification de la configuration à partir de l'interface de ligne de commande dans CIMC

- Vérifiez si TACACS+ est activé.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- Vérifiez les détails de configuration par serveur.

```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: *****
Server Port: 49
```

Dépannage

- Assurez-vous que l'adresse IP du serveur TACACS+ est accessible à partir du CIMC et que le port est configuré correctement.
- Assurez-vous que la **paire cisco-av** est correctement configurée sur le serveur TACACS+.
- Vérifiez si le serveur TACACS+ est accessible (IP et port).
- Assurez-vous que la clé ou les informations d'identification secrètes correspondent à celles configurées sur le serveur TACACS+.
- Si vous pouvez vous connecter avec TACACS+ mais que vous disposez uniquement

d'autorisations **en lecture seule**, vérifiez si cisco-av-pair a la syntaxe correcte sur le serveur TACACS+.

Dépannage ISE

- Vérifiez les journaux Tacacs Live pour l'une des tentatives d'authentification. Le statut doit être **Pass**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ise30baaamex/408819883/155352
Message Text	Device-Administration: Session Authorization succeeded
Username	tacacs_user
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Shell Profile	Test_Shell
Matched Command Set	
Command From Device	

- Vérifiez que l'attribut **cisco-av-pair** correct est configuré pour la réponse.

Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

Informations connexes

- [Authentication TACACS+ Cisco UCS-C](#)
- [Support et documentation techniques - Cisco Systems](#)
- [Configurer ISE 2.0 : Authentification et autorisation de commande IOS TACACS+ basées sur l'appartenance au groupe AD](#)