

Comprendre la commande AAA Authentication Login Default Local Group TACACS+

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit le comportement de la commande `aaa authentication login default local group tacacs+` sur un périphérique Cisco IOS®.

Conditions préalables

Exigences

Cisco recommande que :

- Le nouveau modèle `aaa` est activé sur le périphérique.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

Remarque : utilisez l'[analyseur CLI Cisco](#) du catalogue d'outils Cisco pour obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés ont accès aux informations et aux outils internes de Cisco.

Configurez ces commandes sur le périphérique en mode de configuration globale :

```
aaa new-model
aaa authentication login default local group tacacs+
```

Avec juste `aaa new model` configuré, l'authentification locale est appliquée à toutes les lignes et interfaces (à l'exception de la ligne de console `con 0`).

Ici, la liste de méthodes AAA est appliquée à toutes les tentatives de connexion sur toutes les lignes du périphérique, où la première base de données locale est vérifiée, puis si nécessaire, le serveur TACACS (Terminal Access Controller Access Control System) est essayé.

```
username cisco privilege 15 password 0 cisco
```

Base de données utilisateur locale :

```
tacacs-server host 10.20.220.141
tacacs-server key cisco
```

Le serveur TACACS est maintenant configuré.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

1. Activez **Debug TACACS** et **Debug AAA Authentication** sur le périphérique testé.

```
RUT#show debug
```

```
General OS:
```

```
  TACACS access control debugging is on
  AAA Authentication debugging is on
```

2. Exécutez une commande telnet sur le périphérique :

```
RUT#show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	10.197.235.96	YES	DHCP	up	up
Loopback0	192.168.1.2	YES	manual	up	up

```
RUT#telnet 192.168.1.2
```

```
Trying 192.168.1.2 ... Open
```

```
User Access Verification
```

```
Username: cisco
```

```
*Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
```

```
*Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list 'default'
```

```
Password:
```

```
RUT>
```

Vous remarquerez qu'il n'a pas essayé d'atteindre le serveur TACACS car le nom d'utilisateur `cisco` a été trouvé localement.

Maintenant, si vous essayez d'utiliser une information d'identification qui n'est pas configurée localement sur la boîte :

```
RUT#telnet 192.168.1.2
```

Trying 192.168.1.2 ... Open

User Access Verification

Username:

*Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f

*Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list 'default'

Username: **cisco1**

*Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing

*Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31

*Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)

***Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141**

*Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout

*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out

*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up

*Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet

% Authentication failed

Vous pouvez voir qu'il tente d'atteindre le serveur TACACS 10.20.220.141. Il s'agit d'un comportement par défaut attendu. Aucun nom d'utilisateur cisco1 n'est configuré sur le serveur TACACS, ce qui indique que l'authentification a échoué.

Si le périphérique dispose d'un journal d'authentification AAA dans le groupe par défaut tacacs+ local dans la configuration, sa première préférence est TACACS. Si le TACACS est accessible, mais qu'aucun utilisateur ne l'a configuré, il n'effectue pas de reprise et tente d'effectuer une recherche dans la base de données locale. Le message suivant s'affiche : **Authentication failed** .

Dépannage

Aucune information spécifique n'est actuellement disponible pour dépanner cette configuration.

Informations connexes

- [Configurer AAA de base sur un serveur d'accès](#)
- [Assistance technique et téléchargements Cisco](#)

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.