

Exemple de configuration TACACS+ dans Nexus 4005I

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configurations](#)

[Step-by-Step Instructions](#)

[Configuration CLI TACACS+](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer le système TACACS+ (Terminal Access Controller Access Control System) dans un commutateur de la gamme Nexus 4000. L'authentification TACACS+ varie légèrement dans la gamme Nexus 4000 par rapport à un commutateur Cisco Catalyst.

[Conditions préalables](#)

[Conditions requises](#)

Cisco recommande que vous ayez une connaissance de ce sujet : [Commandes de base NX-OS de la gamme Cisco Nexus 7000](#).

[Components Used](#)

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

- Commutateur Cisco Nexus 4005I
- Cisco Secure Access Control Server (ACS) 5.x

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Reportez-vous aux [Conventions des conseils techniques de Cisco](#) pour plus d'informations sur les conventions du document.

Configurations

L'exemple de configuration de cette section décrit comment configurer un commutateur Nexus 4005I et un serveur TACACS+.

Step-by-Step Instructions

Complétez ces étapes afin de configurer le commutateur Nexus et le serveur TACACS+ :

1. Activez la fonctionnalité de protocole TACACS+.L'adresse IP du serveur ACS doit être configurée avec la clé pré-partagée. S'il existe plusieurs serveurs ACS, les deux hôtes doivent être configurés.
2. Activez le concept AAA et le groupe de serveurs AAA.Dans cet exemple de configuration, le nom du groupe AAA est « ACS ».

Configuration CLI TACACS+

```
ASA
!--- Enable TACACS+ on the device. feature tacacs+
tacacs-server host 10.0.0.1 key 7 Cisco tacacs-server
host 10.0.0.2 key 7 Cisco tacacs-server directed-request
!--- Provide the name of your ACS server. aaa group
server tacacs+ ACS
!--- Mention the IP address of the tacacs-servers !---
referred to in the "tacacs-server host" command. server
10.0.0.1 server 10.0.0.2 !--- Telnet and ssh sessions.
aaa authentication login default group ACS local !---
Console sessions. aaa authentication login console group
ACS local !--- Accounting command. aaa accounting
default group ACS
```

Remarque : utilisez la même clé prépartagée « Cisco » dans le serveur ACS pour l'authentification entre le serveur Nexus 4000 et le serveur ACS.

Remarque : Si le serveur TACACS+ est en panne, vous pouvez revenir à l'authentification locale en configurant le nom d'utilisateur et le mot de passe dans le commutateur.

Le système d'exploitation Nexus n'utilise pas le concept de niveaux de *privilege* au lieu de cela, il utilise *des rôles*. Par défaut, vous êtes placé dans le rôle *opérateur réseau*. Si vous souhaitez qu'un utilisateur dispose d'autorisations complètes, vous devez les placer dans le rôle *admin-réseau*, et vous devez configurer le serveur TACACS pour qu'il désactive un attribut lorsque l'utilisateur se connecte. Pour TACACS+, vous renvoyez un attribut personnalisé TACACS avec une valeur de rôles=« roleA ». Pour un utilisateur à accès complet, vous utilisez : `cisco-av-pair*shell:rôles=« network-admin »`

```
cisco-av-pair*shell:roles="network-admin"(The * makes it optional)
```

```
shell:roles="network-admin"
```

Vérification

Utilisez les commandes de cette section afin de vérifier la configuration du serveur TACACS+ :

- **show tacacs-server** : affiche la configuration du serveur TACACS+.
- **show aaa authentication [login {error-enable | mschap}]** : affiche les informations d'authentification configurées.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Configuration de AAA](#)
- [Configuration de TACACS+](#)
- [Support et documentation techniques - Cisco Systems](#)