

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurations](#)

[Instructions pas à pas](#)

[Configuration TACACS+ CLI](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

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

[Conditions préalables](#)

[Conditions requises](#)

Cisco recommande que vous ayez la connaissance de ce thème : [Commandes de principes fondamentaux de la gamme 7000 NX-OS de Cisco Nexus](#).

[Composants utilisés](#)

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

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

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Conventions](#)

Référez-vous au [Conventions relatives aux conseils techniques Cisco](#) pour les informations sur des conventions de document.

Configurations

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

Instructions pas à pas

Terminez-vous ces étapes afin de configurer le commutateur de Nexus et le serveur TACACS+ :

1. Caractéristique de protocole de l'enable TACACS+.L'adresse IP du serveur ACS doit être configurée avec la clé pré-partagée. S'il y a plus d'un serveur ACS, les deux hôtes doivent être configurés.
2. Activez le concept d'AAA et le Groupe de serveurs AAA.Dans cet exemple de configuration, le nom du nom de groupe d'AAA est « ACS. »

Configuration TACACS+ CLI

ASA
<pre>!--- Enable TACACS+ on the device.feature tacacs+ tacacs-server host 10.0.0.1 key 7 Ciscotacacs-server host 10.0.0.2 key 7 Ciscotacacs-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</pre>

Remarque: Utilisez la même clé pré-partagée « Cisco » dans le serveur ACS pour l'authentification entre la gamme 4000 de Nexus et le serveur ACS.

Remarque: Si le serveur TACACS+ est en panne, vous pouvez tomber de nouveau à authentifiez localement en configurant le nom d'utilisateur et le mot de passe dans le commutateur.

Le système d'exploitation de Nexus n'utilise pas le concept des niveaux de *privilège* à la place qu'il utilise des *rôles*. Par défaut vous êtes placé dans le rôle d'*opérateur réseau*. Si vous voulez qu'un utilisateur ait de pleines autorisations, vous devez les placer dans le rôle de *réseau-admin*, et vous devez configurer le serveur TACACS pour abaisser un attribut quand l'utilisateur ouvre une session. Pour TACACS+, vous passez de retour un attribut personnalisé TACACS avec une valeur de `roles= " roleA »`. Pour un utilisateur d'accès complet, vous utilisez : `cisco-av-pair*shell : roles= " réseau-admin »`

```
!--- Enable TACACS+ on the device.feature tacacs+ tacacs-server host 10.0.0.1 key 7 Ciscotacacs-
server host 10.0.0.2 key 7 Ciscotacacs-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!--- Enable TACACS+ on the device.feature tacacs+ tacacs-server host 10.0.0.1 key 7
Ciscotacacs-server host 10.0.0.2 key 7 Ciscotacacs-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
```

Vérifiez

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

- **show tacacs-server** ? Affiche la configuration du serveur TACACS+.
- **show aaa authentication [procédure de connexion {erreur-enable | mschap}]** ? Les affichages ont configuré les informations d'authentification.

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** .

Dépannez

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

Informations connexes

- [Configurer l'AAA](#)
- [Configurer TACACS+](#)
- [Support et documentation techniques - Cisco Systems](#)