Comment affecter des niveaux de privilège avec TACACS+ et RADIUS

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Exemple](#)
[Configurations - Routeur](#)
[Configurations - Serveur](#)
[Informations connexes](#)

Introduction

Ce document explique comment modifier le niveau de privilège pour certaines commandes, et fournit à un exemple de configuration pour un routeur et des serveurs TACACS+ et RADIUS.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des niveaux de privilège sur un routeur.

Par défaut, il y a trois niveaux de privilèges sur le routeur :

- niveau de privilège 1 = non-privilégié (l'invite indique router>), niveau par défaut pour se connecter
- le niveau de privilège 15 = a favorisé (l'invite indique router#), niveau après être entré en mode activer
- le niveau de privilège 0 = rarement utilisé, mais inclut 5 commandes : **désactiver**, **activer**, **quitter**, **aide** et **déconnexion**

Des niveaux 2-14 ne sont pas utilisés dans la configuration par défaut, mais des commandes qui sont normalement au niveau 15 peuvent être configurées à une de ces niveaux, et les commandes qui sont normalement au niveau 1 peuvent être relevées à l'un de ces niveaux. Évidemment, ce modèle de Sécurité signifie une certaine gestion du routeur.

Pour déterminer le niveau de privilège en tant qu'utilisateur connecté, introduisez la commande de **montrer privilège**. Pour déterminer quelles commandes sont disponibles à un niveau de privilège

particulier pour la version du logiciel de Cisco IOS® que vous utilisez, saisissez **?** à la ligne de commande une fois connecté à ce niveau de privilège.

Remarque: Au lieu d'attribuer des niveaux de privilège, vous pouvez exécuter l'autorisation de commande si le serveur d'authentification prend en charge TACACS+. Le protocole RADIUS ne prend en charge pas l'autorisation de commande.

Composants utilisés

Les informations de ce document sont basées sur les versions de logiciel Cisco IOS 11.2 et ultérieures.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Exemple

Dans cet exemple, des commandes de **snmp-server** sont changées du niveau de privilège 15 (le routage par défaut) au niveau de privilège 7. **La commande ping** est relevée du niveau de privilège 1 au niveau 7. Quand l'utilisateur sept est authentifié, cet utilisateur est attribué le niveau de privilège 7 par le serveur, et le niveau de privilège actuel d'affiche le **privilège** « 7." L'utilisateur peut exécuter une commande ping et faire la configuration de snmp-server dans le mode de configuration. D'autres commandes de configuration ne sont pas disponibles.

Configurations - Routeur

Routeur - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Routeur - 11.3.3.T et versions ultérieures (jusqu'à 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Routeur - 12.0.5.T et versions ultérieures

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Configurations - Serveur

Cisco Secure NT TACACS+

Suivez ces étapes pour configurer le serveur.

1. Complétez le nom d'utilisateur et mot de passe.
2. Dans des paramètres de groupe, assurez-vous que shell/exec est coché et 7 saisi dans la case de niveau de privilège.

TACACS+ - Strophe dans le serveur gratuit

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco Secure UNIX TACACS+

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Cisco Secure NT RADIUS

Suivez ces étapes pour configurer le serveur.

1. Saisissez le nom d'utilisateur et mot de passe.
2. Dans les paramètres de groupe pour l'IETF, Service-type (attribut 6) = Nas-**Invite**
3. Dans la zone CiscoRADIUS, cochez **AV-Pair** et dans la zone rectangulaire dessous, saisissez **shell:priv-lvl=7**.

Cisco Secure UNIX RADIUS

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

C'est le fichier utilisateur pour le nom d'utilisateur « sept. »

Remarque: Le serveur doit prendre en charge Cisco av-pairs.

- mot de passe sept = **passwdxyz**
- Type de service = **Shell-User**
- cisco-avpair =shell:priv-lvl=7

Informations connexes

- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- TACACS+ dans la documentation d'IOS
- Page d'assistance TACACS+
- Page d'assistance Cisco Secure UNIX

- Cisco Secure ACS pour la page d'assistance de Windows
- Support technique - Cisco Systems