Les niveaux de privilège IOS ne peuvent pas voir la configuration complète d'exécution

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Conventions
Afficher la configuration du routeur
Niveaux de privilège
Informations connexes

Introduction

Ce document explique comment les niveaux de privilège affectent la capacité d'un utilisateur d'exécuter certaines commandes sur un routeur.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Afficher la configuration du routeur

Lorsque l'accès au routeur est configuré par niveaux de privilège, un problème courant est que les commandes **show running ou write terminal sont configurées au niveau de privilège de l'utilisateur ou plus bas.** Lorsque l'utilisateur exécute la commande, la configuration paraît vide. C'est en fait conçu comme ça pour les raisons suivantes :

- La commande **write terminal/show running-config affiche une configuration vide.** Cette

commande affiche toutes les commandes que l'utilisateur actuel est en mesure de modifier (autrement dit, toutes les commandes au niveau de privilège actuel de l'utilisateur ou plus bas). La commande ne devrait pas afficher les commandes au-dessus du niveau de privilège actuel de l'utilisateur pour des considérations de sécurité. Si c'était le cas, des commandes telles que **snmp-server community pourraient être utilisées pour modifier la configuration actuelle du routeur et obtenir l'accès complet au routeur.**

- La commande **show config/show start-up config affiche une configuration complète, mais n'affiche pas vraiment la configuration réelle.** Plutôt, la commande affiche simplement le contenu du NVRAM, qui se trouve à être la configuration du routeur au moment où l'utilisateur fait un **write memory**.

Niveaux de privilège

Pour permettre à un utilisateur privilégié de visionner la totalité de la configuration en mémoire, l'utilisateur doit modifier les privilèges pour toutes les commandes qui sont configurées sur le routeur. Exemple :

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Afin de comprendre cet exemple, il est nécessaire de comprendre les niveaux de privilège. Par défaut, il existe trois niveaux de commande sur le routeur :

- niveau de privilège 0 — Comprend les commandes disable (désactiver)**, enable (activer), exit (quitter), help (aide), et logout (déconnexion).**
- niveau de privilège 1 — niveau normal sur Telnet; comprend toutes les commandes user-level (niveau de l'utilisateur) pour l'invite `router>`.
- niveau de privilège 15 — Comprend toutes les commandes enable-level (niveau d'activation) pour l'invite router#.

Vous trouverez les commandes disponibles pour un niveau particulier dans un routeur particulier en tapant **?** dans l'invite du routeur. Les commandes peuvent être déplacées entre les niveaux de privilège en utilisant la commande **privilege (privilège), comme illustré dans l'exemple.** Alors que cet exemple montre l'authentification et l'autorisation locales, les commandes fonctionnent d'une façon semblable pour l'authentification TACACS+ ou RADIUS et l'autorisation exec (on peut obtenir plus de granularité dans la gestion du routeur avec la mise en œuvre de l'autorisation des commandes TACACS+ avec un serveur.)

Des détails supplémentaires sur les utilisateurs et les niveaux de privilège présentés dans l'exemple :

- L'utilisateur *six est en mesure de se connecter par Telnet et exécuter la commande* **show run, mais la configuration obtenue est pratiquement vide puisque l'utilisateur ne peut rien configurer (la configuration du terminal est au niveau 8, pas au niveau 6).** L'utilisateur n'est pas autorisé à voir les noms d'utilisateur et les mots de passe des autres utilisateurs, ou à consulter les renseignements du protocole SNMP (Simple Network Management Protocol).
- L'utilisateur *john est en mesure de se connecter par Telnet et exécuter la commande* **show run, mais ne voit que les commandes qu'il peut configurer (snmp-server community (communauté du serveur SNMP), qui fait partie de la configuration du routeur, puisque cet utilisateur est notre administrateur de gestion de réseau).** Il peut configurer **snmp-server community puisque la configuration du terminal est au niveau 8 (au niveau 9 ou plus bas), et que la commande snmp-server community est une commande de niveau 8.** L'utilisateur n'est pas autorisé à voir les noms d'utilisateur et les mots de passe des autres utilisateurs, mais la configuration SNMP lui est confiée.
- L'utilisateur *inout est en mesure de se connecter par Telnet et, en vertu d'être configuré pour la commande* **autocommand show running**, peut voir la configuration affichée, mais se fait déconnecter par la suite.
- L'utilisateur *poweruser est en mesure de se connecter par Telnet et d'exécuter la commande***showrun.** Cet utilisateur est au niveau 15, et est en mesure de voir toutes les commandes. Toutes les commandes sont au niveau 15 ou plus bas; les utilisateurs à ce niveau peuvent aussi voir et contrôler les noms d'utilisateur et les mots de passe.

Informations connexes

- Command Lookup Tool (clients enregistrés uniquement)
- Documentation IOS pour TACACS+ et RADIUS
- Page de support TACACS/TACACS+
- Page d'assistance RADIUS
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems