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

Contenu

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.

Composants utilisés

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

Conventions

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

Visualisez la configuration de routeur

Quand l'accès au routeur est configuré par des niveaux de privilège, un problème courant est que l'**exécution d'exposition** ou les commandes de **write terminal** sont configurées à ou en dessous du niveau de privilège de l'utilisateur. Quand l'utilisateur exécute la commande, la configuration semble être vide. C'est réellement par conception pour ces raisons :

- **La write terminal/commande show running-config** affiche une configuration vide. Cette commande affiche toutes les commandes que l'utilisateur courant peut modifier (en d'autres termes, toutes les commandes à ou en dessous du niveau de privilège en cours de l'utilisateur). La commande ne devrait pas afficher des commandes au-dessus du niveau de privilège en cours de l'utilisateur en raison des considérations liées à la sécurité. Si oui, des commandes telles que le **snmp-server community** ont pu être utilisées pour modifier la configuration en cours du routeur et pour gagner l'accès complet au routeur.
- La commande **de démarrage de show config/config d'exposition** affiche une configuration complète, mais n'affiche pas vraiment la configuration réelle. Au lieu de cela, la commande imprime simplement le contenu de NVRAM, qui s'avère justement être la configuration du routeur alors que l'utilisateur fait une **write memory**.

Niveaux de privilège

Pour permettre à un utilisateur privilégié de visualiser la configuration entière dans la mémoire, les besoins de l'utilisateur de modifier des 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
```

Pour comprendre cet exemple, il est nécessaire de comprendre des niveaux de privilège. Par défaut, il y a trois niveaux commande sur le routeur :

- niveau de privilège 0 — Inclut le **débronchement**, l'**enable**, la **sortie**, l'**aide**, et les commandes de **déconnexion**.
- niveau de privilège 1 — Niveau normal sur le telnet ; inclut toutes les commandes de niveau utilisateur à la demande de `router>`.
- niveau de privilège 15 — Inclut toutes les commandes niveau de l'enable à la demande de `router#`.

Des commandes disponibles à un niveau particulier dans un routeur particulier peuvent être trouvées en tapant a **?** à la demande de routeur. Des commandes peuvent être déplacées entre les niveaux de privilège à l'aide de la commande de **privilège**, comme illustré dans l'exemple. Tandis que cet exemple affiche l'authentification locale et l'autorisation, les commandes fonctionnent pareillement pour l'authentification TACACS+ ou de RAYON et l'autorisation EXEC (plus de finesse aux commandes du routeur peut être réalisée avec l'implémentation de l'autorisation de commande TACACS+ avec un serveur.)

Les détails supplémentaires aux utilisateurs et aux niveaux de privilège se sont présentés dans l'exemple :

- L'utilisateur *six* peut au telnet dedans et exécute la commande de **passage d'exposition**, mais la configuration en résultant est pratiquement vide parce que cet utilisateur ne peut configurer rien (la **configure terminal** est au niveau 8, pas au niveau 6). On ne permet pas à l'l'utilisateur pour voir des noms d'utilisateur et mot de passe des autres utilisateurs, ou pour voir les informations de Protocole SNMP (Simple Network Management Protocol).
- L'utilisateur *John* peut au telnet dedans et exécute la commande de **passage d'exposition**, mais voit seulement les commandes qu'il peut configurer (la pièce du **snmp-server community de la** configuration de routeur, puisque cet utilisateur est notre administrateur de Gestion de réseau). Il peut configurer le **snmp-server community** parce que la **configure terminal** est au niveau 8 (à ou en dessous du niveau 9), et du **snmp-server community** est une commande du niveau 8. L'utilisateur n'est pas permis pour voir des noms d'utilisateur et mot de passe des autres utilisateurs, mais il est de confiance avec la configuration SNMP.
- *L'inout d'*utilisateur peut au telnet dedans, et, en vertu d'être configuré pour l'**exécution d'exposition d'autocommand**, voit la configuration affichée mais est déconnecté ensuite.
- *Le poweruser d'*utilisateur peut au telnet dedans et exécute la commande de **passage d'exposition**. Cet utilisateur peut au niveau 15, et est voir toutes les commandes. Toutes les commandes sont à ou en dessous du niveau 15 ; les utilisateurs à ce niveau peuvent également visualiser et contrôler des noms d'utilisateur et mot de passe.

Informations connexes

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