Configurer une configuration complète pour les utilisateurs ayant des niveaux de privilège faibles

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Problème de configuration

Solution de configuration et vérification

Conclusion

Informations connexes

Introduction

Ce document décrit le processus de configuration pour afficher la configuration en cours complète pour les utilisateurs avec des niveaux de privilège faibles.

Conditions préalables

Exigences

Une compréhension de base des niveaux de privilège Cisco est requise pour comprendre ce document. Les renseignements généraux suffisent à expliquer la compréhension des niveaux de privilège requis.

Composants utilisés

Les composants utilisés pour les exemples de configuration dans ce document étaient un ASR1006, mais tout périphérique Cisco IOS® ou Cisco IOS XE fonctionne de la même manière.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Ce document décrit les étapes de configuration sur la façon d'afficher la configuration en cours complète pour les utilisateurs connectés au routeur avec des niveaux de privilège faibles. Pour comprendre le problème suivant et la solution de contournement, il est nécessaire de comprendre

les niveaux de privilège. Les niveaux de privilège disponibles sont compris entre 0 et 15 et permettent à l'administrateur de personnaliser les commandes disponibles pour chaque niveau de privilège. Par défaut, les trois niveaux de privilège d'un routeur sont les suivants :

- Niveau 0 : inclut uniquement les commandes de base (désactiver, activer, quitter, aide et déconnexion)
- Niveau 1 : inclut toutes les commandes disponibles en mode d'exécution utilisateur
- Niveau 15 - Inclut toutes les commandes disponibles en mode privilégié

Les niveaux restants entre ces niveaux minimum et maximum ne sont pas définis tant que l'administrateur ne leur a pas attribué de commandes et/ou d'utilisateurs. Par conséquent, l'administrateur peut attribuer aux utilisateurs différents niveaux de privilèges entre ces niveaux minimum et maximum pour séparer les différents utilisateurs auxquels ils ont accès. L'administrateur peut ensuite attribuer des commandes individuelles (et diverses autres options) à un niveau de privilège individuel pour le rendre disponible à tout utilisateur à ce niveau. Exemple :

```
Router(config)# username user1 privilege 7 password P@ssw0rD1
Router(config)# privilege exec level 7 show access-lists
```

Avec cette configuration, lorsque l'utilisateur 1 se connecte au routeur, il peut exécuter la commande, `show access-lists` et/ou tout autre élément activé à ce niveau de privilège. Cependant, il n'en va pas de même pour la commande enabled`show running-config` , comme nous le verrons plus loin dans l'énoncé du problème.

Problème de configuration

Lors de la configuration de différents niveaux d'accès au routeur pour différents utilisateurs, il est courant qu'un administrateur réseau tente d'attribuer à certains utilisateurs l'accès à des `show` commandes uniquement, et qu'il n'accorde l'accès à aucune `configuration` commande. Il s'agit d'une tâche simple pour la plupart des `show` commandes, car vous pouvez accorder l'accès par le biais d'une configuration simple, comme indiqué ci-dessous :

```
Router(config)# username test_user privilege 10 password testP@ssw0rD
Router(config)# privilege exec level 10 show
Router(config)# privilege exec level 10 show running-config
```

Avec cet exemple de configuration, la deuxième ligne peut permettre au `test_user` d'accéder à une pléthore de commandes show associées, qui ne sont normalement pas disponibles à ce niveau de privilège. Cependant, la commande est traitée différemment de la plupart des `show running-config` commandes show. Même avec la troisième ligne de l'exemple de code, seul un caractère omis/abrégé `show running-config` est affiché pour l'utilisateur, bien que la commande soit spécifiée au niveau de privilège correct.

```
User Access Verification

Username: test_user
 Password:
 Router#
 Router#show privilege
 Current privilege level is 10
 Router#
 Router#show running-config
 Building configuration...

Current configuration : 121 bytes
 !
 ! Last configuration change at 21:10:08 UTC Mon Aug 28 2017
 !
 boot-start-marker
 boot-end-marker
 !
 !
 !
 end

Router#
```

Comme vous pouvez le voir, ce résultat n'affiche aucune configuration et ne serait pas utile à un utilisateur qui tente de collecter des informations sur la configuration du routeur. En effet, la `show running-config` commande affiche toutes les commandes que l'utilisateur peut modifier à son niveau de privilège actuel. Cette configuration est conçue comme une configuration de sécurité pour empêcher l'utilisateur d'avoir accès à des commandes qui ont été configurées précédemment à partir de leur niveau de privilège actuel. Il s'agit d'un problème lors de la tentative de création d'un utilisateur ayant accès aux commandes show, comme c'`show running-config`est le cas d'une commande standard que les ingénieurs doivent collecter initialement lors du dépannage.

Solution de configuration et vérification

Pour résoudre ce dilemme, il existe une autre version de la commande traditionnelle `show run` qui contourne cette limitation de la commande.

```
Router(config)# show running-config view full
 Router(config)# privilege exec level 10 show running-config view full
```

L'ajout de `view full` à la commande (et à son tour le niveau de privilège de la commande pour permettre à l'utilisateur d'accéder à la commande), permet maintenant à l'utilisateur d'afficher l'intégralité de la commande `show running-config` sans aucune commande omise.

```
Username: test_user
 Password:
```

```
Router#
Router#show privilege
Current privilege level is 10
Router#
Router#show running-config view full

Building configuration...

Current configuration : 2664 bytes
!
! Last configuration change at 21:25:45 UTC Mon Aug 28 2017
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot system flash bootflash:packages.conf
boot system flash bootflash:asr1000rp1-adventerprisek9.03.13.06a.S.154-3.S6a-ext.bin
boot-end-marker
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password <omitted>
!
no aaa new-model
!
no ip domain lookup
!
subscriber templating
!
multilink bundle-name authenticated
!
spanning-tree extend system-id
!
username test_user privilege 10 password 0 testP@ssw0rD
!
redundancy
 mode sso
!
cdp run
!
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
```

```
 vrf forwarding Mgmt-intf
 ip address <omitted>
 negotiation auto
 cdp enable
!
ip forward-protocol nd
!
control-plane
!
!
privilege exec level 10 show running-config view full
alias exec show-running-config show running-config view full
!
line con 0
 stopbits 1
line aux 0
 exec-timeout 0 1
 no exec
 transport output none
 stopbits 1
line vty 0 4
login local
!
end
Router#
```

Cependant, cela soulève la question suivante : en fournissant à l'utilisateur l'accès à cette version de la commande, cela ne soulève-t-il pas le risque de sécurité initial qui tentait d'être résolu en concevant une version omise ?

Pour contourner la solution et garantir la cohérence d'une conception de réseau sécurisée, vous pouvez créer un alias pour l'utilisateur qui exécute la version complète de la show running-config commande sans fournir d'accès/de connaissances à l'utilisateur, comme illustré ci-dessous :

```
Router(config)# alias exec show-running-config show running-config view full
```

Dans cet exemple, le show running-config est le nom d'alias et lorsque l'utilisateur est connecté au routeur, il peut entrer ce nom d'alias au lieu de la commande et recevoir le résultat attendu sans connaître la commande en cours d'exécution.



Remarque : À partir de la version 16.X, selon la plate-forme, il est également nécessaire d'ajouter des autorisations aux fichiers à l'aide de la commande (config)#file privilege <level>.

Conclusion

En conclusion, ce n'est qu'un exemple de la façon d'avoir plus de contrôle lors de la création administrative d'un accès avec privilège utilisateur à différents niveaux. Il existe une multitude

d'options pour créer différents niveaux de privilèges et accéder à différentes commandes, et c'est un exemple de la façon de s'assurer qu'un utilisateur show only a toujours accès à la configuration en cours complète lorsqu'il n'a pas accès aux commandes de configuration.

Informations connexes

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.