Configurez IOS-XE pour afficher le plein show running-config pour des utilisateurs avec les niveaux bas de privilège

Contenu

Introduction

Ce document décrit les étapes de configuration sur la façon dont afficher la pleine configuration en cours pour des utilisateurs ouverts une session au routeur avec les niveaux bas de privilège. Pour comprendre le problème et le contournement ci-dessous il est nécessaire de comprendre des niveaux de privilège. Les niveaux de privilège disponibles s'étendent de 0 à 15, et permettent à l'administrateur pour personnaliser quelles commandes sont disponibles à quel niveau de privilège. Par défaut, les trois niveaux de privilège sur un routeur sont :

- **Niveau 0** – Inclut seulement des commandes fondamentales (débronchement, enable, sortie, aide, et déconnexion)
- **Niveau 1** – Inclut toutes les commandes disponibles au mode de commande d'Exec de l'utilisateur
- **Niveau 15** – Inclut toutes les commandes disponibles au mode de commande de privileged exec

Les niveaux restants entre ces minimum et taux maxima sont non définis jusqu'à ce que l'administrateur leur affecte des commandes et/ou des utilisateurs. Par conséquent, l'administrateur peut assigner à des utilisateurs différents niveaux de privilège entre ces niveaux de privilège minimum et maximum pour séparer ce que les différents utilisateurs ont accès aussi. L'administrateur peut alors allouer des commandes individuelles (et de diverses autres options) à un niveau de privilège individuel de rendre ceci disponible pour n'importe quel utilisateur à ce niveau. Exemple :

```
Mot de passe P@ssw0rD1 du privilège 7 du nom d'utilisateur user1 de
Router(config)#
Show access-lists du niveau 7 d'exec privilégié de Router(config)#
```

Avec cette configuration, quand « user1 » connecté au routeur ils pourrait exécuter le « show access-lists » commande, et/ou toute autre chose activés à ce niveau de privilège. Toutefois les mêmes ne peuvent pas être dits pour ont activé la commande de « show running-config », comme sera discuté ci-dessous avec notre déclaration de problème.

Conditions préalables

Conditions requises

Une compréhension de base des niveaux de privilège de Cisco est exigée pour comprendre ce document, l'introduction ci-dessus devrait suffire pour expliquer la compréhension des niveaux de privilège qui est exigée.

Composants utilisés

Les composants utilisés pour les exemples de configuration dans ce document étaient des ASR1006.

Problème de configuration

En configurant différents niveaux d'accès au routeur pour différents utilisateurs, c'est une application courante pour qu'un administrateur réseau tente d'affecter certains utilisateurs pour avoir seulement accès « pour afficher » des commandes, et ne pas permettre d'accéder à n'importe quelle « configuration » commande. C'est une tâche simple pour la plupart des commandes show, comme vous pouvez accorder l'accès par la configuration simple selon ci-dessous :

```
Mot de passe testP@ssw0rD du privilège 10 de test_user de nom
d'utilisateur de Router(config)#
Exposition du niveau 10 d'exec privilégié de Router(config)#
Show running-config du niveau 10 d'exec privilégié de Router(config)#
```

Avec cet exemple de configuration, la deuxième ligne permettra au « test_user » pour avoir accès à une pléthore de commandes associées par exposition, qui ne sont normalement pas disponibles à ce niveau de privilège. Cependant, la commande show running-config est traitée différemment la plupart des commandes show. Même avec la troisième ligne de code exemple, « show running-config » omis/abrégé seulement sera affiché pour l'utilisateur en dépit de la commande étant spécifiée au niveau de privilège correct.

```
Vérification d'accès client

Nom d'utilisateur : test_user
Mot de passe :
Router#
Privilège de Router#show
Le niveau de privilège en cours est 10
Router#
Running-config de Router#show
Configuration de construction…

Configuration en cours : 121 octets
!
! Dernière modification de configuration à UTC Lun de 21:10:08 le 28
août 2017
!
```

```
boot-start-marker
boot-end-marker
!
!
!
extrémité

Router#
```

Comme vous pouvez voir cette sortie n'affiche aucune configuration, et ne serait pas utile à un utilisateur essayant de collecter des informations au sujet de la configuration du routeur. C'est parce que la commande show running-config affichera seulement toutes les commandes que l'utilisateur peut modifier à leur niveau de privilège en cours. Ceci est conçu comme configuration de sécurité pour empêcher l'utilisateur d'avoir accès aux commandes qui ont été configurées de au-dessus de leur niveau de privilège en cours. C'est une question en tentant de créer un utilisateur avec l'accès aux commandes show, en tant que « show running-config » est une commande standard pour que les ingénieurs collectent au commencement le pour le dépannage.

Solution et vérification de configuration

Comme solution à ce dilemme, il y a une autre version de la commande traditionnelle de passage d'exposition qui sautera cette limite de la commande.

```
Vue de show running-config de Router(config)# complètement
Vue de show running-config du niveau 10 d'exec privilégié de
Router(config)# complètement
```

L'ajout de la « vue complètement » à la commande, (et consécutivement au niveau de privilège de la commande de permettre l'accès client à la commande), permet maintenant à l'utilisateur pour ne visualiser le plein show running-config sans aucune commande omise.

```
Nom d'utilisateur : test_user
Mot de passe :
Router#
Privilège de Router#show
Le niveau de privilège en cours est 10
Router#
Vue de running-config de Router#show complètement

Configuration de construction…

Configuration en cours : 2664 octets
!
! Dernière modification de configuration à UTC Lun de 21:25:45 le 28
août 2017
!
version 15.4
les horodateurs de service mettent au point la milliseconde date-
heure
les horodateurs de service se connectent la milliseconde date-heure
aucun débronchement-noyau-noyau de coup de volée-keepalive de plate-
forme
```

```
!
routeur d'adresse Internet
!
boot-start-marker
boot system flash bootflash: packages.conf
boot system bootflash:asr1000rp1-adventerprisek9.03.13.06a.S.154-
3.S6a-ext.bin instantané
boot-end-marker
!
vrf definition Mgmt-intf
 !
 ipv4 d'address-family
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
<omitted> de mot de passe d'enable
!
aucun aaa new-model
!
aucun ip domain lookup
!
abonné templating
!
multilink bundle-name authentifié
!
spanning-tree extend system-id
!
mot de passe 0 testP@ssw0rD du privilège 10 de test_user de nom
d'utilisateur
!
Redondance
 sso de mode
!
cdp run
!
interface GigabitEthernet0/2/0
 aucun IP address
 arrêt
 negotiation auto
!
interface GigabitEthernet0/2/1
 aucun IP address
 arrêt
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 <omitted> d'IP address
 negotiation auto
 cdp enable
!
```

```
ND d'ip forward-protocol
!
contrôle-avion
!
!
vue de show running-config du niveau 10 d'exec privilégié
complètement
alias vue de show running-config de show running-config d'exécutif
complètement
!
ligne escroquerie 0
 stopbits 1
ligne 0 aux.
 exec-timeout 0 1
 aucun exécutif
 transport output aucun
 stopbits 1
line vty 0 4
gens du pays de procédure de connexion
!
extrémité
Router#
```

Toutefois ceci soulève alors la question, est-ce qu'en fournissant l'accès client à cette version de la commande, ceci ne soulève pas le risque de sécurité initial qui tentait d'être résolu en concevant une version omise ?

Comme contournement à la solution et pour assurer la cohérence dans une conception de réseau sécurisé, nous pouvons créer un pseudonyme pour l'utilisateur qui exécutera la version complète de la commande show running-config sans fournir l'accès/connaissance à l'utilisateur, comme affiché ci-dessous :

```
Vue de show running-config de show running-config d'exécutif de
Router(config)# alias complètement
```

Dans cet exemple le « show running-config » est le pseudonyme, et quand l'utilisateur est enregistré dans le routeur, ils peuvent alors écrire ce pseudonyme au lieu de la commande et recevoir la sortie prévue sans connaissance de la commande réelle qui est exécutée.

Conclusion

En conclusion, c'est juste un exemple de la façon avoir plus de contrôle en créant administrativement l'accès de privilège des utilisateurs aux différents niveaux. Il y a une pléthore d'options de créer de divers niveaux de privilège et d'accès à différentes commandes, et c'est un exemple de la façon s'assurer qu'un utilisateur « réservé à l'exposition » a toujours accès au plein running-config quand ils n'ont aucun accès à aucune commande de configuration.