Configureer IOS-XE om volledige show-in-run-configuratie voor gebruikers met lage prioriteitsniveaus weer te geven

Inhoud

Inleiding

Dit document beschrijft de configuratiestappen in de manier om de volledige actieve configuratie voor gebruikers die aan de router met lage voorkeursniveaus inloggen, weer te geven. Om het onderstaande probleem te begrijpen en om te werken is het nodig om de voorkeursniveaus te begrijpen. De beschikbare voorrechten variëren van 0 tot 15, en staan de beheerder toe om aan te passen welke opdrachten op welk niveau van het voorrecht beschikbaar zijn. Standaard zijn de drie prioriteitsniveaus op een router:

- **Niveau 0** - omvat alleen basisopdrachten (uitschakelen, inschakelen, afsluiten, helpen en uitloggen)
- **Niveau 1** - Omvat alle opdrachten die beschikbaar zijn in de User EXEC-opdrachtmodus
- **Niveau 15** - Omvat alle opdrachten die beschikbaar zijn in de bevoorrechte EXEC-opdrachtmodus

De resterende niveaus tussen deze minimum en maximum niveaus zijn niet gedefinieerd totdat de beheerder opdrachten en/of gebruikers aan deze niveaus heeft toegewezen. Daarom kan de beheerder verschillende voorkeursniveaus tussen deze minimum en maximum bevoorrechtingsniveaus toewijzen om te scheiden wat verschillende gebruikers ook hebben. De beheerder kan dan individuele opdrachten (en verschillende andere opties) aan een individueel voorkeursniveau toewijzen om dit voor elke gebruiker op dit niveau beschikbaar te maken. Bijvoorbeeld:

```
Router (fig)# gebruikersnaam1 privilege 7 wachtwoord P@ssw0rD1
Router (fig)# voorkeursniveau 7 toont toegangslijsten
```

Met deze configuratie zouden "user1" verbonden met de router de opdracht "show access-lists" kunnen uitvoeren en/of andere mogelijkheden die op dat prioriteitsniveau zijn ingeschakeld. Dit kan echter niet worden gezegd voor de opdracht "show-run-alle-opstellers", zoals hieronder met onze probleemverklaring zal worden besproken.

Voorwaarden

Vereisten

Om dit document te kunnen begrijpen, is een fundamenteel begrip van de voorrechten van Cisco vereist. De bovenstaande inleiding moet volstaan om het begrip van de voorrechten te verklaren dat vereist is.

Gebruikte componenten

De onderdelen die werden gebruikt voor de configuratievoorbeelden in dit document waren een ASR1006.

Configuratieprobleem

Bij het configureren van verschillende toegangsniveaus voor de router voor verschillende gebruikers, is het een algemene toepassing voor een netwerkbeheerder om te proberen bepaalde gebruikers alleen toegang te geven tot 'show'-opdrachten, en geen toegang te bieden tot ‘configuratie’-opdrachten. Dit is een eenvoudige taak voor de meeste showopdrachten, aangezien u toegang kunt verlenen door middel van een eenvoudige configuratie zoals hieronder wordt beschreven:

```
Router (configuratie)# gebruikersnaam test_user privilege 10
wachtwoord testP@ssw0rD
Router (configuratie)# voorkeursniveau 10 tonen
Router (configuratie)# bevoorrecht niveau 10 tonen in werking
stellen-configuratie
```

Met deze voorbeeldconfiguratie zal de tweede lijn de ‘test_user' toegang geven tot een overvloed aan met show samenhangende opdrachten, die normaal niet beschikbaar zijn op dit voorkeursniveau. Nochtans, wordt het show in werking stellen-enig bevel verschillend behandeld aan de meeste showopdrachten. Zelfs met de derde regel van voorbeeldcode, zal slechts een weggelaten/afgekort "show run-run-fig" voor de gebruiker worden weergegeven ondanks dat de opdracht op het juiste niveau van de voorrechten wordt gespecificeerd.

```
Verificatie van gebruikerstoegang

Username: test_gebruiker
 Wachtwoord:
Router#
 Routerprivilege#show
 Huidige voorkeursniveau is 10
 Router#
 Router#show-in werking stellen-configuratie
Configuratie gebouw....

Huidige configuratie: 121 bytes
 !
 ! Laatste wijziging van de configuratie om 21:10:08 UTC maandag 28
augustus 2017
 !
 markeerstift
 markeerstift
```

```
 !
 !
 !
 einde

Router#
```

Zoals u kunt zien deze uitvoer toont geen configuratie, en zou niet behulpzaam aan een gebruiker zijn die informatie over de configuratie van de router probeert te verzamelen. Dit is omdat het tonen in werking stellen-enig bevel slechts alle opdrachten zal tonen die de gebruiker op hun huidige bevoorrechtingsniveau kan aanpassen. Dit is ontworpen als een beveiligingsconfiguratie om te voorkomen dat de gebruiker toegang heeft tot opdrachten die zijn geconfigureerd boven hun huidige voorkeursniveau. Dit is een probleem wanneer het probeert om een gebruiker met toegang tot tonen bevelen te creëren, zoals het "tonen in werking stellen-configuratie" een standaardbevel voor ingenieurs is om aanvankelijk te verzamelen wanneer het oplossen van problemen.

Configuratieoplossing en -verificatie

Als oplossing voor dit dilemma, is er een andere versie van de traditionele show run opdracht die deze beperking van de opdracht zal omzeilen.

```
Router (configuratie)# tonen in werking stellen-configuratiemening
volledig
 Router (configuratie)# bevoorrecht niveau 10 tonen in werking
stellen-configuratiemening volledig
```

De toevoeging van ‘view full’ aan het bevel, (en op het voorrecht niveau van het bevel om de gebruiker toegang tot het bevel toe te staan), staat nu de gebruiker toe om de volledige show in werking stellen-in werking stellen-configuratie zonder om het even welke gemiste bevelen te bekijken.

```
Username: test_gebruiker
 Wachtwoord:
Router#
 Routerprivilege#show
 Huidige voorkeursniveau is 10
 Router#
 De router#show in werking stellen-configuratie bekijken volledig

Configuratie gebouw....

Huidige configuratie: 2664 bytes
 !
 ! Laatste wijziging uit de configuratie, 12:25:45 UTC-maaltijd 28
aug. 2017
 !
 versie 15.4
 Service timepostzegels debug msec
 Service timestamps log datetime msec
 geen platform punt-keeplevi-blokkering
 !
```

```
 hostname-router
 !
 markeerstift
 flitser van het laars systeem:pakketten.conf
 flitser van het laars systeem:asr1000rp1-
adventerprisek9.03.13.06a.S.154-3.S6a-ext.bin
 markeerstift
 !
 vrf-definitie Mgmt-intf
  !
  adresfamilie ipv4
  exit-adresfamilie
  !
 adresfamilie ipv6
  exit-adresfamilie
 !
 Wachtwoord invoeren <weggelaten>
 !
 geen nieuw model
 !
 geen ip - domeinraadpleging
 !
 abonnee-templatie
 !
 gewaarmerkte multilink-gebundelnaam
 !
 in-boom-extender systeem-id
 !
 gebruikersnaam test_user privilege 10 wachtwoord 0 testP@ssw0rD
!
 redundantie
  mode sso
 !
 cdp-run
 !
 interface Gigabit Ethernet0/2/0
  geen ip-adres
  sluiting
  onderhandelings-auto
 !
 interface Gigabit Ethernet0/2/1
  geen ip-adres
  sluiting
  onderhandelings-auto
 !
 interface voor Gigabit Ethernet0
  Vrf-verzending Mgmt-intf
  IP-adres <weggelaten>
  onderhandelings-auto
  cdp mogelijk
 !
 ip-voorwaartse protocol en
 !
```

```
 besturingsplane
 !
 !
 bevoorrecht exec niveau 10 tonen in werking stellen-beslist mening
volledig
 alias exec show-run-configuratie show run-OP-bestand-configuratie-
weergave in zijn geheel
 !
 lijn pictogram 0
  stopzetting 1
 lijn 0
  vrijstelling 0 1
  geen uitzondering
  vervoersoutput geen
  stopzetting 1
 lijn vty 0 4
 aanmelding lokaal
 !
 einde
 Router#
```

Maar dit roept dan de vraag op, door de gebruiker toegang te geven tot deze versie van de opdracht, leidt dit niet tot het eerste veiligheidsrisico dat werd opgelost door het ontwerpen van een weggelaten versie?

Als een oplossing en om consistentie in een veilig netwerkontwerp te verzekeren, kunnen we een alias voor de gebruiker maken die de volledige versie van het show in werking stellen-in werking stellen-enig bevel zonder toegang/kennis aan de gebruiker, zoals hieronder getoond wordt.

```
Router (enig)# alias exec show-run-software-in werking stellen-
configuratie tonen de in werking gestelde-configuratie weergave
```

In dit voorbeeld is de "show-run-Configuratie" de naam van het alias, en wanneer de gebruiker in de router is aangemeld, kunnen zij dan deze naam van het alias invoeren in plaats van de opdracht en de verwachte uitvoer ontvangen zonder kennis van de eigenlijke opdracht die wordt uitgevoerd.

Conclusie

Tot slot is dit slechts één voorbeeld van hoe je meer controle kunt krijgen wanneer je op verschillende niveaus administratieve toegang creëert tot gebruikersrechten. Er zijn een overvloed aan opties om verschillende bevoorrechtingsniveaus en toegang tot verschillende opdrachten te creëren, en dit is een voorbeeld van hoe te verzekeren een "show-only" gebruiker nog toegang tot het volledige in werking stellen-configuratie heeft wanneer zij geen toegang tot om het even welke configuratiebevelen hebben.