

Configurar o IOS-XE para exibir o comando show running-config completo para usuários com baixos níveis de privilégio

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema de configuração](#)

[Solução de configuração e verificação](#)

[Conclusão](#)

Introduction

Este documento descreve as etapas de configuração sobre como exibir a configuração de execução completa para usuários conectados ao roteador com níveis de privilégio baixos. Para entender o problema abaixo e a solução alternativa, é necessário entender os níveis de privilégio. Os níveis de privilégio disponíveis variam de 0 a 15 e permitem que o administrador personalize os comandos disponíveis em qual nível de privilégio. Por padrão, os três níveis de privilégio em um roteador são:

- **Nível 0** - Inclui apenas comandos básicos (desabilitar, habilitar, sair, ajudar e fazer logoff)
- **Nível 1** - Inclui todos os comandos disponíveis no modo de comando EXEC do usuário
- **Nível 15** - Inclui todos os comandos disponíveis no modo de comando EXEC privilegiado

Os níveis restantes entre esses níveis mínimo e máximo são indefinidos até que o administrador atribua comandos e/ou usuários a eles. Portanto, o administrador pode atribuir níveis de privilégio diferentes aos usuários entre esses níveis de privilégio mínimo e máximo para separar o que os diferentes usuários têm acesso. O administrador pode então alocar comandos individuais (e várias outras opções) a um nível de privilégio individual para disponibilizá-los para qualquer usuário nesse nível. Por exemplo:

```
Router(config)# nome de usuário usuário1 privilégio 7 senha P@ssw0rD1
Router(config)# privilégio exec nível 7 show access-lists
```

Com essa configuração, quando 'user1' estiver conectado ao roteador, eles poderão executar o comando 'show access-lists' e/ou qualquer outra opção habilitada nesse nível de privilégio. No entanto, o mesmo não pode ser dito para o comando 'show running-config' ativado, como será discutido abaixo com nossa declaração de problema.

Prerequisites

Requirements

Uma compreensão básica dos níveis de privilégio da cisco é necessária para entender este documento, a introdução acima deve ser suficiente para explicar a compreensão dos níveis de privilégio necessários.

Componentes Utilizados

Os componentes usados para os exemplos de configuração neste documento foram um ASR1006.

Problema de configuração

Ao configurar diferentes níveis de acesso ao roteador para diferentes usuários, é um aplicativo comum para um administrador de rede tentar atribuir determinados usuários para terem acesso apenas aos comandos 'show' e não fornecer acesso a nenhum comando 'configuration'. Esta é uma tarefa simples para a maioria dos comandos show, pois você pode conceder acesso por meio de configuração simples, conforme abaixo:

```
Router(config)# nome de usuário test_user privilege 10 password
testP@ssw0rD
Router(config)# privilégio exec nível 10 show
Router(config)# privilégio exec nível 10 show running-config
```

Com esta configuração de exemplo, a segunda linha permitirá que o 'test_user' tenha acesso a uma variedade de comandos show related, que normalmente não estão disponíveis neste nível de privilégio. No entanto, o comando show running-config é tratado diferentemente da maioria dos comandos show. Mesmo com a terceira linha do código de exemplo, somente um 'show running-config' omitido/abreviado será exibido para o usuário, apesar do comando ser especificado no nível de privilégio correto.

Verificação de acesso do usuário

```
Nome de usuário: test_user
```

```
Senha:
```

```
Roteador#
```

```
Roteador#mostrar privilégio
```

```
O nível de privilégio atual é 10
```

```
Roteador#
```

```
Router#show running-config
```

```
Criando configuração...
```

```
Configuração atual: 121 bytes
```

```
!
```

```
! Última alteração de configuração às 21:10:08 UTC Seg 28 de agosto
de 2017
```

```
!
```

```
boot-start-marcador
```

```
boot-end-flag
```

```
!
```

```
!
```

```
!
```

```
fim
```

```
Roteador#
```

Como você pode ver, essa saída não mostra nenhuma configuração e não seria útil para um usuário tentando coletar informações sobre a configuração do roteador. Isso ocorre porque o comando `show running-config` exibirá apenas todos os comandos que o usuário pode modificar em seu nível de privilégio atual. Isso é projetado como uma configuração de segurança para impedir que o usuário tenha acesso a comandos que foram configurados acima de seu nível de privilégio atual. Esse é um problema ao tentar criar um usuário com acesso aos comandos `show`, pois `"show running-config"` é um comando padrão que os engenheiros devem coletar inicialmente ao solucionar problemas.

Solução de configuração e verificação

Como solução para esse dilema, há outra versão do comando tradicional `show run` que ignorará essa limitação do comando.

```
Router(config)# show running-config view full
Router(config)# privilégio exec nível 10 show running-config view
full
```

A adição de `"view full"` ao comando (e, por sua vez, o nível de privilégio do comando para permitir o acesso do usuário ao comando) agora permite que o usuário veja o comando `show running-config` completo sem nenhum comando omitido.

```
Nome de usuário: test_user
Senha:
Roteador#
Roteador#mostrar privilégio
O nível de privilégio atual é 10
Roteador#
Router#show running-config view full
```

Criando configuração...

```
Configuração atual: 2664 bytes
!
! Última alteração de configuração às 21:25:45 UTC Seg 28 de agosto
de 2017
!
versão 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname Roteador
!
boot-start-marcador
boot system flash bootflash:packages.conf
boot system flash bootflash:asr1000rp1-
adventerprise9.03.13.06a.S.154-3.S6a-ext.bin
boot-end-flag
!
```

```
vrf definição 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
!
modelo de assinante
!
multilink bundle-name authenticated
!
spanning-tree extended system-id
!
username test_user privilege 10 password 0 testP@ssw0rD
!
redundância
modo sso
!
cdp run
!
interface GigabitEthernet0/2/0
no ip address
fechamento
autonegociação
!
interface GigabitEthernet0/2/1
no ip address
fechamento
autonegociação
!
interface GigabitEthernet0
vrf forwarding Mgmt-intf
endereço IP <omitted>
autonegociação
cdp enable
!
ip forward-protocol nd
!
plano de controle
!
!
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
!
fim
Roteador#
```

No entanto, isso levanta a questão, ao fornecer ao usuário acesso a essa versão do comando, isso não levanta o risco inicial de segurança que estava tentando ser resolvido com o projeto de uma versão omitida?

Como uma solução alternativa para a solução e para garantir a consistência em um projeto de rede seguro, podemos criar um alias para o usuário que executará a versão completa do comando `show running-config` sem fornecer acesso/conhecimento ao usuário, como mostrado abaixo:

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

Neste exemplo, "show-running-config" é o nome do alias e, quando o usuário está conectado ao roteador, ele pode então inserir esse nome de alias em vez do comando e receber a saída esperada sem saber do comando real que está sendo executado.

Conclusão

Para concluir, este é apenas um exemplo de como ter mais controle ao criar administrativamente acesso de privilégio de usuário em diferentes níveis. Há uma variedade de opções para criar vários níveis de privilégio e acesso a diferentes comandos, e este é um exemplo de como garantir que um usuário 'show-only' ainda tenha acesso à configuração atual completa quando não tem acesso a nenhum comando de configuração.