将IOS-XE配置为为具有低权限级别的用户显示完整的show running-config

目录

简介

本文档介绍如何为以低权限级别登录路由器的用户显示完整运行配置的配置步骤。要了解以下问题和解决方法，必须了解权限级别。 可用权限级别范围为0到15，允许管理员自定义哪些命令可在哪些权限级别使用。默认情况下，路由器的三个权限级别是：

- **级别0** — 仅包括基本命令（禁用、启用、退出、帮助和注销）
- **第1级** — 包括用户EXEC命令模式下可用的所有命令
- **15级** — 包括特权EXEC命令模式下可用的所有命令

在这些最低级别和最高级别之间的其余级别在管理员为它们分配命令和/或用户之前是未定义的。因此，管理员可以在这些最小和最大权限级别之间为用户分配不同的权限级别，以区分不同用户也具有哪些访问权限。然后，管理员可以将单个命令（以及各种其他选项）分配到单个权限级别，以便此级别上的任何用户都可以使用。例如：

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

使用此配置时，当“user1”连接到路由器时，他们将能够运行“show access-lists”命令和/或在该权限级别启用的任何其他命令。但是，对于启用“show running-config”命令，不能同样如此，下面将与我们的问题陈述一起讨论。

先决条件

要求

要了解本文档，必须基本了解思科权限级别，上述介绍应足以说明对所需权限级别的了解。

使用的组件

本文档中用于配置示例的组件是ASR1006。

配置问题

当为不同用户配置不同的路由器访问级别时，网络管理员通常会尝试将某些用户分配为仅具有“show”命令访问权限，而不提供对任何“configuration”命令的访问权限。对于大多数show命令而言，这是一项简单任务，因为您可以通过如下简单配置授予访问权限：

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

使用此示例配置时，第二行将允许“test_user”访问大量与show相关的命令，这些命令通常在此权限级别不可用。但是，show running-config命令与大多数show命令的处理方式不同。即使使用示例代码的第三行，也只会为用户显示省略/缩写的“show running-config”，尽管命令在正确的权限级别指定。

```
usernametest_user

Router#
 Router#show privilege
 10
 Router#
 Router#show running-config
…

121 bytes
 !
 !201782821:10:08 UTC
 !
 boot-start-marker
 boot-end-marker
 !
 !
 !


Router#
```

如您所见，此输出不显示任何配置，对于尝试收集有关路由器配置信息的用户来说，也无济于事。这是因为show running-config命令只显示用户可在当前权限级别修改的所有命令。此配置设计为安全配置，以防止用户访问从其当前权限级别以上配置的命令。这是尝试创建具有show命令访问权限的用户时出现的问题，因为“show running-config”是工程师在进行故障排除时最初收集的标准命令。

配置解决方案和验证

为了解决这一难题，传统show run命令的另一个版本将绕过该命令的限制。

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

在命令中添加“view full”（以及允许用户访问该命令的命令的权限级别）后，用户现在可以在不省略任何命令的情况下查看完整的show running-config。

```
usernametest_user

Router#
 Router#show privilege
 10
 Router#
 Router#show running-config view full

…

2664 bytes
 !
 !201782821:25:45 UTC
 !
 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
 !
 vrfMgmt-intf
  !
  address-family ipv4
  exit-address-family
  !
 address-family ipv6
  exit-address-family
 !
 enable password <>
 !
 no aaa new-model
 !
 no ip domain lookup
 !

 !

 !
 spanning-tree extend system-id
 !
 username test_user privilege 10 password 0 testP@ssw0rD
!
 redundancy
  SSO
 !
 CDP
```

```
!
interface GigabitEthernet0/2/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/1
 no ip address
 shutdown
 negotiation auto
!
GigabitEthernet0
 vrfMgmt-intf
 ip address <>
 negotiation auto
 cdp enable
!
ip forward-protocol nd
!

!
!
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

 stopbits 1
line vty 0 4
login local
!

Router#
```

但是，这确实会提出一个问题，即通过向用户提供对此版本命令的访问，这是否不会增加通过设计省略版本来尝试解决的初始安全风险？

作为解决方案的解决方法并确保安全网络设计的一致性，我们可以为用户创建别名，该别名将运行show running-config命令的完整版本，而不向用户提供访问/知识，如下所示：

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

在本例中，“show-running-config”是别名，当用户登录路由器时，他们可以输入此别名而不是命令，并在不知道实际运行的命令的情况下接收预期输出。

结论

总之，这只是管理性创建不同级别的用户权限访问时如何拥有更多控制权的一个示例。创建不同权限级别和访问不同命令的选项太多，这是如何确保“show-only”用户在无法访问任何配置命令时仍有权访问完整的running-config的示例。