Configure Full Running Config for Users with Low Privilege Levels

Contents

Introduction

This document describes the configuration process to display the full running configuration for users with low privilege levels.

Prerequisites

Requirements

A basic understanding of Cisco privilege levels is required to understand this document, the Background Information suffices to explain the understanding of required privilege levels.

Components Used

The components used for the configuration examples within this document was an ASR1006 but any Cisco IOS® or Cisco IOS XE device works similar.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes the configuration steps on how to display the full running configuration for users logged in to the router with low privilege levels. To understand the next problem and workaround it is necessary to understand privilege levels. The available privilege levels range from 0 to 15, and allow the administrator to customise what commands are available at what privilege level. By default, the three privilege levels on a router are:

- **Level 0** – Includes only basic commands (disable, enable, exit, help, and log out)
- **Level 1** – Includes all commands available at the User EXEC command mode

- **Level 15** – Includes all commands available at the Privileged EXEC command mode

The remaining levels in between these minimum and maximum levels are undefined until the administrator assigns commands and/or users to them. Therefore, the administrator can assign users different privilege levels in between these minimum and maximum privilege levels to separate what different users have access too. The administrator can then allocate individual commands (and various other options) to an individual privilege level to make this available for any user at this level. For example:

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

With this configuration, when user1 connected to the router they would be able to run the show access-lists command, and/or anything else enabled at that privilege level. However the same cannot be said for enabled the show running-config command, as is discussed later in the problem statement.

Configuration Problem

When configuring different access levels to the router for different users, it is a common application for a network administrator to attempt to assign certain users to only have access to show commands, and not provide access to any configuration commands. This is a simple task for most show commands, as you can grant access through a simple configuration as per this:

```
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
```

With this example configuration, the second line can allow the test_user to have access to a plethora of show related commands, which are normally not available at this privilege level. However, the show running-config command is treated differently to most show commands. Even with the third line of example code, only an omitted/abbreviated show running-config is displayed for the user despite the command being specified at the correct privilege level.

```
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#
```

As you can see this output does not show any configuration, and would not be helpful to a user trying to collect information about the configuration of the router. This is because the show running-config command displays all of the commands that the user is able to modify at their current privilege level. This is designed as a security configuration to prevent the user from having access to commands that have been configured previously from their current privilege level. This is an issue when attempting to create a user with access to show commands, as show running-config is a standard command for engineers to initially collect when troubleshooting.

Configuration Solution and Verification

As a solution to this dilemma, there is another version of the traditional show run command that bypasses this limitation of the command.

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

The addition of view full to the command, (and in turn the privilege level of the command to allow the user access to the command), now allows the user to view the full show running-config without any omitted commands.

```
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#
```

However this does then raise the question, by providing the user access to this version of the command, does this not raise the initial security risk that was attempting to be solved by designing an omitted version?

As a workaround to the solution and to ensure consistency in a secure network design, you can create an alias for the user that runs the full version of the show running-config command without providing access/knowledge to the user, as shown here:

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

In this example the show running-config is the alias name, and when the user is logged into the router, they can then enter this alias name instead of the command and receive the expected output without knowledge of the actual command that is being run.

Note: From 16.X version, depending on the platform it is also required to add permissions to the files using the command **(config)#file privilege <level>**.

Conclusion

In conclusion, this is just one example of how to have more control when administratively creating user privilege access at different levels. There are a plethora of options to create various privilege levels and access to different commands, and this is an example of how to ensure a show only user still has access to the full running config when they have no access to any configuration commands.

Related Information

- Cisco Technical Support & Downloads