為具有低許可權級別的使用者配置完全運行配置

目錄

簡介

本文檔介紹為低許可權級別的使用者顯示完整運行配置的配置過程。

必要條件

需求

要理解本檔案，必須具備對思科許可權級別的基本理解，背景資訊足以解釋對所需許可權級別的理解。

採用元件

本文檔中用於配置示例的元件是ASR1006，但所有Cisco IOS®或Cisco IOS XE裝置的工作方式都類似。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文描述如何顯示以低許可權級別登入到路由器的使用者的完整運行配置的配置步驟。要瞭解下一個問題和解決方法，必須瞭解許可權級別。 可用的許可權級別範圍為0到15，並允許管理員自定義哪些命令在哪些許可權級別可用。預設情況下，路由器上的三個許可權層級為：

- 級別0 — 僅包括基本命令（禁用、啟用、退出、幫助和註銷）
- 第1級 — 包括使用者EXEC命令模式下可用的所有命令
- 第15級 — 包括在特權EXEC命令模式下可用的所有命令

在管理員將命令和/或使用者分配給它們之前，這些最小和最大級別之間的剩餘級別是未定義的。因此，管理員可以為使用者分配不同許可權級別，這些許可權級別介於最小許可權級別和最大許可權級別之間，以分隔不同使用者也具有訪問許可權的內容。然後，管理員可以將單個命令（和各種其他選項）分配給單個許可權級別，以使此級別的任何使用者都可以使用它。舉例來說：

```
Router(config)# username user1 privilege 7 password P@sswOrD1
Router(config)# privilege exec level 7 show access-lists
```

透過此組態，使用者1連線到路由器時，可以執行 show access-lists 命令和/或在該許可權級別啟用的任何其它內容。但是，對於啟用 show running-config 命令，稍後將在problem語句中討論。

組態問題

為不同使用者配置不同的路由器訪問級別時，網路管理員通常會將某些使用者分配為僅有權訪問 show 命令，不提供對任何 configuration 指令。對大多數人來說，這是個簡單的任務 show 命令，因為您可以通過簡單配置授予訪問許可權，如下所示：

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

使用此示例配置，第二行可以允許 test_user 訪問過多的show相關命令，這些命令通常在此許可權級別不可用。但是， show running-config 命令的處理方式與大多數show命令不同。即使使用示例代碼的第3行，也僅有一個省略/縮寫 show running-config 顯示為使用者，儘管命令是在正確的許可權級別指定的。

```
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#
```

您可以看到，此輸出未顯示任何配置，對試圖收集路由器配置資訊的使用者沒有幫助。這是因為 show running-config 命令顯示使用者能夠在其當前許可權級別修改的所有命令。這是設計為安全配置，防止使用者從其當前許可權級別訪問以前配置的命令。當嘗試建立具有show命令訪問許可權的使用者時，會出現此問題，例如 show running-config 是工程師進行故障排除時最初收集的標準命令。

組態解決方案和驗證

作為這一困境的解決之道，中國還有另一種傳統 show run 命令來繞過命令的此限制。

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

新增 view full 現在，對命令（並反過來允許使用者訪問命令的許可權級別），允許使用者檢視完整的 show running-config 沒有任何省略的命令。

```
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@sswOrD
!
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#
```

但是，這確實會引發問題，通過向使用者提供此版本命令的訪問許可權，這是否不會引起試圖通過設計省略版本來解決的初始安全風險？

作為解決方案的一種變通方法，為確保安全網路設計的一致性，您可以為運行完整版本的使用者建立一個別名， show running-config 命令而不向使用者提供訪問/知識，如下所示：

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

在本示例中， show running-config 是別名，當使用者登入到路由器時，他們可輸入此別名而不是命令，並在不知道正在運行的實際命令的情況下接收預期輸出。

註：從16.X版本開始，根據平台的不同，還需要使用命令(config)#file privilege <level>向檔案新增許可權。

結論

總之，這只是管理性建立不同級別的使用者許可權訪問時如何擁有更多控制的一個示例。建立各種許可權級別以及訪問不同命令的選項眾多，以下示例說明了如何確保show only使用者在無權訪問任何配置命令時仍然能夠訪問完整運行配置。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。