特権レベルの低いユーザに対して完全なshow running-configを表示するようにIOS-XEを設定します

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定の問題](#)
[設定ソリューションと検証](#)
[結論](#)

概要

このドキュメントでは、低い特権レベルでルータにログインしたユーザの完全な実行コンフィギュレーションを表示する手順について説明します。次の問題と回避策を理解するには、特権レベルを理解する必要があります。 使用可能な特権レベルの範囲は0 ~ 15で、管理者はどの特権レベルで使用可能なコマンドをカスタマイズできます。デフォルトでは、ルータの3つの特権レベルは次のとおりです。

- **レベル0**：基本コマンド(disable、enable、exit、help、logout)だけが含まれます。
- **レベル1**：ユーザEXECコマンドモードで使用可能なすべてのコマンドが含まれます
- **レベル15**：特権EXECコマンドモードで使用可能なすべてのコマンドが含まれます

管理者がコマンドやユーザを割り当てるまで、これらの最小レベルと最大レベルの間の残りのレベルは未定義です。したがって、管理者は、これらの最小権限レベルと最大権限レベルの間でユーザに異なる権限レベルを割り当て、アクセスできるユーザを区別できます。管理者は、個々のコマンド（およびその他のさまざまなオプション）を個々の特権レベルに割り当て、このレベルの任意のユーザに対して利用可能にすることができます。以下に、いくつかの例を示します。

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

この設定では、ルータに「user1」が接続されると、「show access-lists」コマンドを実行したり、その特権レベルで有効になっている他のコマンドを実行したりできます。ただし、この問題の説明で後述するように、「show running-config」コマンドを有効にしても同じことは言えません。

前提条件

要件

このドキュメントを理解するには、シスコの特権レベルに関する基本的な知識が必要です。上記の概要では、必要な特権レベルに関する理解を説明できます。

使用するコンポーネント

このドキュメントの設定例に使用するコンポーネントは、ASR1006です。

設定の問題

異なるユーザに対してルータに異なるアクセスレベルを設定する場合、ネットワーク管理者は特定のユーザに「show」コマンドへのアクセス権だけを割り当て、どの「configuration」コマンドにもアクセス権を与えないようにするのが一般的なアプリケーションです。これは、次に示すように簡単な設定でアクセスを許可できるため、ほとんどのshowコマンドの簡単な作業です。

```
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
```

この設定例では、2行目で「test_user」が多数のshow relatedコマンドにアクセスできます。これらのコマンドは通常、この特権レベルでは使用できません。ただし、show running-configコマンドは、ほとんどのshowコマンドとは異なる方法で扱われます。例コードの3行目でも、コマンドが正しい特権レベルで指定されているにもかかわらず、ユーザに対して省略または省略された「show running-config」だけが表示されます。

```
User Access Verification

:test_user

Router#
 Router#show privilege
 10
 Router#
 Router#show running-config
Building configuration...

Current configuration :121
 !
 !201782821:10:08 UTC(GMT)
 !
 boot-start-marker
 boot-end-marker
 !
 !
 !


Router#
```

この出力は設定を示していないため、ルータの設定に関する情報を収集しようとするユーザには役立ちません。これは、show running-configコマンドでは、ユーザが現在の特権レベルで変更できるすべてのコマンドが表示されるためです。これは、ユーザが現在の特権レベルを超えて設定されたコマンドにアクセスできないように、セキュリティ設定として設計されています。show running-configはエンジニアがトラブルシューティング時に最初に収集する標準コマンドであるため、showコマンドにアクセスできるユーザを作成しようとすると、これは問題になります。

設定ソリューションと検証

このジレンマに対する解決策として、コマンドのこの制限を回避する従来のshow runコマンドの別のバージョンがあります。

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

コマンドに「view full」が追加され (そしてコマンドの特権レベルがユーザにコマンドへのアクセスを許可します) 、コマンドを省略せずに完全なshow running-configを表示できるようになりました。

```
:test_user

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

Building configuration...

Current configuration :2664 bytes
 !
 !201782821:25:45 UTC(GMT)
 !
 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 <>
 !
 no aaa new-model
 !
```

```
 no ip domain lookup
 !

 !
 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
  IP
  shutdown
  negotiation auto
 !
 interface GigabitEthernet0/2/1
  IP
  shutdown
  negotiation auto
 !
 interface GigabitEthernet0
  vrf forwarding Mgmt-intf
  ip address <>
  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
 !

 Router#
```

ただし、このコマンドのこのバージョンへのアクセスをユーザに提供することで、省略したバー

ジョンを設計することで解決しようとする初期セキュリティリスクが高まらないという問題は発生しますか。

このソリューションの回避策として、セキュアなネットワーク設計の一貫性を確保するために、ユーザにアクセスや知識を提供せずにshow running-configコマンドの完全なバージョンを実行するユーザのエイリアスを次のように作成できます。

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

この例では、「show-running-config」はエイリアス名です。ユーザがルータにログインすると、コマンドの代わりにエイリアス名を入力し、実際に実行されているコマンドを知らなくても、期待される出力を受け取ることができます。

結論

結論として、これは、異なるレベルでユーザ特権アクセスを管理上で作成する際に、より詳細な制御を行う方法の一例にすぎません。さまざまな特権レベルを作成し、さまざまなコマンドにアクセスするためのオプションが多数あります。これは、「show-only」ユーザが設定コマンドにアクセスできない場合でも、完全なrunning-configにアクセスできるようにする方法の例です。