

低い特権レベルを持つユーザ向けの完全な show running-config を表示するために IOS XE を設定して下さい

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[コンフィギュレーションに関する問題](#)

[設定 ソリューションおよび確認](#)

[結論](#)

概要

この資料は方法のコンフィギュレーションのステップを低い特権レベルが付いているルータにログオンされるユーザ向けの完全な実行コンフィギュレーションを表示する記述したものです。下記の問題および回避策を理解するために特権レベルを理解することは必要です。利用可能な特権レベルは 0 から 15 までどんな特権レベルか及び、管理者がどんなコマンドが利用できるかカスタマイズすることを可能にします。デフォルトで、ルータの 3 つの特権レベルは次のとおりです:

- レベル 0 – includes 基本的なコマンドだけ (デイセーブル、イネーブル、終了、ヘルプおよびログアウト)
- レベル 1 – ユーザ EXEC コマンド モードで利用可能なすべてのコマンドが含まれています
- レベル 15 – Privileged exec コマンド モードで利用可能なすべてのコマンドが含まれています

管理者がそれらにコマンドやユーザを割り当てるまでこれらの最小の間の残りのレベルおよび最高レベルは未定義です。従って、管理者はユーザに異なるユーザーはアクセスできるもの分けるためにこれらの最小および最大特権レベルの間の異なる特権レベルを指定できます。管理者は個々の特権レベルにこれをあらゆるユーザ向けに使用できるようにこのレベルでするそれから個々のコマンド (および他のいろいろなオプションを) 割り当てることができます。次に、例を示します。

```
Routerconfig# user1 7 P@ssw0rD1
Routerconfig# exec 7 show access-lists
```

この設定 ルータに接続された「user1」が「show access-lists」コマンドを実行できるおよび/またはその特権レベルで有効にされて何か他のもの場合の。同じがどんなに有効にした「show running-config」コマンドをののために言うことができなくても、問題文と後で説明されているように。

前提条件

要件

cisco 特権レベルの基本的な知識が上の概要必要となる特権レベルの知識を説明することを足る必要がありますこの資料を理解するために必要となります。

使用するコンポーネント

この資料内の設定例のために使用したコンポーネントは ASR1006 でした。

コンフィギュレーションに関する問題

異なるアクセスレベルを異なるユーザー向けのルータに設定するとき、それは「コマンド示すためにアクセスできるようにただ一定のユーザを割り当てるように試みるネットワーク管理者のための一般的なアプリケーション」でありとアクセスをあらゆる「を設定」に提供しないために命じます。これは下記にによって簡単なコンフィギュレーションによってアクセスを認めることができるように、ほとんどの show コマンドのための単純なタスクです:

```
Routerconfig# test_user 10 testP@ssw0rD
Routerconfig# exec 10
Routerconfig# exec 10 show running-config
```

この設定例によって、第 2 行は「test_user が」茄多にの普通この特権レベルで利用可能ではない関連のコマンドを示すのをアクセスできるようにします。ただし、show running-config コマンドはほとんどの show コマンド別様に扱われます。コード例の第 3 行と、ただ省略された/短縮された「show running-config は」正しい特権レベルで規定される コマンドにもかかわらずユーザー向けに表示する。

```
User Access Verification

test_user

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

121
!
! 21:10:08 UTC 2017 8 28
!
boot-start-marker
boot-end-marker
!
!
end

Router#
```

見ることができるようにこの出力は設定を示さないし、ルータの設定についての情報を収集することを試みているユーザに有用ではないものです。これはユーザは現在の特権レベルで修正することだけ show running-config コマンドがコマンドすべてを表示するという理由によります。これはセキュリティとコンフィギュレーションとして設計されていますアクセスできることを現在の特権レベルの上でから設定されたコマンドにユーザによってが防ぐように。これは解決するとき「show running-config」として show コマンドにアクセスでユーザを、作成するように試みるとき問題です最初に集まるエンジニアのための標準 コマンドです。

設定 ソリューションおよび確認

このジレンマへのソリューションとして、コマンドのこの制限をバイパスする従来の show run コマンドのもう一つのバージョンがあります。

```
Routerconfig# show running-config
Routerconfig# exec 10 show running-config
```

コマンドにユーザアクセスを許可するコマンドのコマンド、（および次々と特権レベルへの「十分のビュー」の付加は）、今ユーザが省略されたコマンドなしで完全な show running-config を表示することを可能にします。

```
test_user

Router#
Router#show
10
Router#
Router#show running-config

Building configuration...

2664
!
! 21:25:45 UTC 2017 8 28
!
15.4
service timestamps debug datetime msec
service timestamps log datetime msec

!
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 Mgmt-intf
!
address-family ipv4
exit-address-family
!
```

```
address-family ipv6
exit-address-family
!
<omitted>
!
no aaa new-model
!
no ip domain lookup
!

!
multilink bundle-name
!
spanning-tree extend system-id
!
test_user 10 0 testP@ssw0rD
!
redundancy
sso
!
cdp run
!
GigabitEthernet0/2/0
no ip address
shutdown
negotiation auto
!
GigabitEthernet0/2/1
no ip address
shutdown
negotiation auto
!
GigabitEthernet0
VRF Mgmt-intf
IP <omitted>
negotiation auto
cdp enable
!
ip forward-protocol nd
!
control-plane
!
!
exec 10 show running-config
exec show running-config show running-config
!
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#
```

これがそれから質問をどんなに上げても、コマンドのこのバージョンへユーザアクセスを提供することによって、これは省略されたバージョンの設計によって解決するように試みていた最初のセキュリティリスクを上げませんか。

ソリューションへの対応策としてセキュア ネットワーク設計の一貫性を確認するために、下記に示されているようにユーザへアクセス/知識を提供しないで show running-config コマンドの完全なバージョンを実行するユーザ向けのエイリアスを、作成し、：

```
Routerconfig# exec show running-config show running-config
```

この例では「show running-config は」エイリアス名前であり、ユーザがルータ ログイン される時、それらはコマンドの代わりにそしてこのエイリアス名前を入力し、実行されている実際のコマンドのナレッジなしで期待された 出力を表示されることが出来ます。

結論

結論として、これは異なるレベルで管理上ユーザー特権アクセスを作成するとき方法のちょうど1つの例より多くの制御を持つです。さまざまな特権レベルを作成し、異なるコマンドにアクセスするオプションの拮多があり「示だけ」ユーザを確認するあらゆる設定コマンドにアクセスがないときこれは完全な running-config に方法の例今でもアクセスできますです。