

Konfigurieren Sie IOS-XE so, dass vollständige show running-config für Benutzer mit eingeschränkten Berechtigungen angezeigt wird

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsproblem](#)

[Konfigurationslösung und -überprüfung](#)

[Schlussfolgerung](#)

Einführung

In diesem Dokument werden die Konfigurationsschritte zur Anzeige der vollständigen Konfiguration für Benutzer beschrieben, die beim Router angemeldet sind und über geringe Berechtigungen verfügen. Um das folgende Problem zu verstehen und eine Problemumgehung zu ermöglichen, müssen Sie die Berechtigungsebenen verstehen. Die verfügbaren Berechtigungsebenen liegen zwischen 0 und 15 und ermöglichen dem Administrator, die verfügbaren Befehle auf welcher Berechtigungsebene festzulegen. Die drei Berechtigungsebenen eines Routers sind standardmäßig:

- **Stufe 0** - Enthält nur grundlegende Befehle (Deaktivieren, Aktivieren, Beenden, Hilfe und Abmelden)
- **Stufe 1** - Enthält alle Befehle, die im Benutzer-EXEC-Befehlsmodus verfügbar sind
- **Stufe 15** - Enthält alle Befehle, die im privilegierten EXEC-Befehlsmodus verfügbar sind

Die verbleibenden Ebenen zwischen diesen Mindest- und Höchstwerten sind nicht definiert, bis der Administrator ihnen Befehle und/oder Benutzer zuweist. Daher kann der Administrator Benutzern verschiedene Berechtigungsebenen zwischen diesen minimalen und maximalen Berechtigungsebenen zuweisen, um zu trennen, auf welche Benutzer Zugriff haben. Der Administrator kann dann einzelne Befehle (und verschiedene andere Optionen) einer individuellen Berechtigungsebene zuweisen, um diese für jeden Benutzer auf dieser Ebene verfügbar zu machen. Beispiel:

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

Wenn "user1" mit dem Router verbunden ist, kann mit dieser Konfiguration der Befehl "show access-lists" und/oder alles andere ausgeführt werden, was auf dieser Berechtigungsebene aktiviert ist. Dasselbe kann jedoch nicht für die Aktivierung des Befehls "show running-config" gesagt werden, wie im Folgenden mit unserer Problembeschreibung erläutert wird.

Voraussetzungen

Anforderungen

Um dieses Dokument verstehen zu können, ist ein grundlegendes Verständnis der Cisco Berechtigungsebenen erforderlich. Die obige Einführung sollte ausreichen, um das Verständnis der erforderlichen Berechtigungsebenen zu erklären.

Verwendete Komponenten

Die in diesem Dokument für die Konfigurationsbeispiele verwendeten Komponenten waren ASR1006.

Konfigurationsproblem

Bei der Konfiguration verschiedener Zugriffsebenen für den Router für unterschiedliche Benutzer ist es für Netzwerkadministratoren üblich, bestimmten Benutzern nur Zugriff auf Befehle der Anzeigefunktion zu gewähren, nicht jedoch auf Befehle der Konfigurationsoptionen. Dies ist eine einfache Aufgabe für die meisten Anzeigebefehle, da Sie den Zugriff wie unten beschrieben über eine einfache Konfiguration gewähren können:

```
Router(config)# username test_user privilege 10 password testP@ssw0rD
Router(config)# privilege exec Level 10 wird angezeigt
Router(config)# privilege exec-Ebene 10 show running-config
```

Bei dieser Beispielkonfiguration ermöglicht die zweite Zeile dem "test_user" Zugriff auf eine Fülle von Befehlen, die in der Regel auf dieser Berechtigungsebene nicht verfügbar sind. Der Befehl show running-config wird jedoch anders behandelt als die meisten show-Befehle. Selbst bei der dritten Zeile Beispielcode wird für den Benutzer nur eine auswegige/abgekürzte "show running-config" angezeigt, obwohl der Befehl auf der richtigen Berechtigungsebene angegeben wurde.

Überprüfung des Benutzerzugriffs

```
Benutzername: Test_Benutzer
Kennwort:
Router#
Router#show-Berechtigung
Die aktuelle Berechtigungsstufe ist 10.
Router#
Router#show running-config
Konfiguration erstellen...
```

```
Aktuelle Konfiguration: 121 Byte
!
! Letzte Konfigurationsänderung am 28. August 2017 um 21:10:08 Uhr
UTC Mo.
!
Startmarker
Bootendmarker
!
!
!
Ende
```

```
Router#
```

Wie Sie sehen, zeigt diese Ausgabe keine Konfiguration an und wäre für einen Benutzer, der versucht, Informationen über die Konfiguration des Routers zu erfassen, nicht hilfreich. Dies liegt daran, dass der Befehl `show running-config` nur alle Befehle anzeigt, die der Benutzer auf der aktuellen Berechtigungsebene ändern kann. Diese Konfiguration dient als Sicherheitskonfiguration, um zu verhindern, dass Benutzer auf Befehle zugreifen können, die über der aktuellen Berechtigungsstufe konfiguriert wurden. Dies ist ein Problem, wenn versucht wird, einen Benutzer mit Zugriff auf Befehle zu erstellen, da `"show running-config"` ein Standardbefehl ist, den Techniker bei der Fehlerbehebung zunächst erfassen müssen.

Konfigurationslösung und -überprüfung

Als Lösung für dieses Dilemma gibt es eine andere Version des herkömmlichen Befehls `show run`, die diese Einschränkung des Befehls umgeht.

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

Durch die Hinzufügung von `"view full"` zum Befehl (und damit auch der Berechtigungsebene des Befehls, der dem Benutzer Zugriff auf den Befehl gewährt) kann der Benutzer jetzt die vollständige `show running-config` ohne ausgelassene Befehle anzeigen.

```
Benutzername: Test_Benutzer
Kennwort:
Router#
Router#show-Berechtigung
Die aktuelle Berechtigungsstufe ist 10.
Router#
Router#show running-config view full
```

Konfiguration erstellen...

```
Aktuelle Konfiguration: 2664 Byte
!
! Letzte Konfigurationsänderung am 28. August 2017 um 21:25:45 Uhr
UTC Mo.
!
Version 15.4
Dienstzeitstempel Debugdatetime msec
Dienstzeitstempel Protokolldateizeit ms
no platform punt-keepalive disable-kernel-core
!
Hostname-Router
!
Startmarker
Flash-Bootflash des Bootsystems: packages.conf
boot system flash bootflash:asr1000rp1-
adventerprisek9.03.13.06a.S.154-3.S6a-ext.bin
Bootendmarker
!
```

```
VRF-Definition Mgmt-intf
!
  Adressfamilie IPv4
  Exitadresse-Familie
!
address-family IPv6
  Exitadresse-Familie
!
enable password <ausgelassen>
!
kein neues Modell
!
Keine IP-Domänensuche
!
Teilnehmervorlage
!
Bündelname authentifiziert
!
Spanning-Tree Extended System-ID
!
username test_user privilege 10 password 0 testP@ssw0rD
!
Redundanz
  Mode-Sup
!
CDP-Ausführung
!
interface GigabitEthernet0/2/0
  keine IP-Adresse
  Herunterfahren
  Verhandlungsauto
!
interface GigabitEthernet0/2/1
  keine IP-Adresse
  Herunterfahren
  Verhandlungsauto
!
interface GigabitEthernet0
  VRF-Forwarding Mgmt-intf
  ip address <ausgelassen>
  Verhandlungsauto
  cdp enable
!
ip forward-Protokoll und
!
Kontrollebene
!
!
privilege exec Level 10 show running-config view full
alias exec show running-config show running-config view full
!
Line con 0
  Stopp 1
```

```
Linie aux 0
  exec-Timeout 0 1
  keine Ausnahme
  Transportleistung keine
  Stopp 1
Line Vity 0 4
Anmelden lokal
!
Ende
Router#
```

Dies wirft jedoch die Frage auf, ob dies durch die Bereitstellung des Benutzerzugriffs auf diese Befehlsversion das anfängliche Sicherheitsrisiko, das durch das Entwerfen einer ausgeweggenommenen Version behoben werden sollte, nicht erhöht?

Als Problemumgehung zur Lösung und zur Gewährleistung der Konsistenz in einem sicheren Netzwerkdesign können wir einen Alias für den Benutzer erstellen, der die Vollversion des Befehls `show running-config` ausführt, ohne dem Benutzer Zugriff/Informationen bereitzustellen, wie im Folgenden gezeigt:

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

In diesem Beispiel ist die "show-running-config" der Aliasname. Wenn der Benutzer beim Router angemeldet ist, kann er diesen Aliasnamen anstelle des Befehls eingeben und die erwartete Ausgabe erhalten, ohne dass er Kenntnis von dem tatsächlich ausgeführten Befehl hat.

Schlussfolgerung

Zusammenfassend lässt sich feststellen, dass dies nur ein Beispiel dafür ist, wie Sie bei der administrativen Erstellung von Benutzerberechtigungszugriffen auf verschiedenen Ebenen mehr Kontrolle haben. Es gibt eine Vielzahl von Optionen zum Erstellen verschiedener Berechtigungsebenen und zum Zugriff auf verschiedene Befehle. Dies ist ein Beispiel dafür, wie sichergestellt werden kann, dass ein Benutzer nur "anzeigen" weiterhin Zugriff auf die vollständige Ausführungskonfiguration hat, wenn er keinen Zugriff auf Konfigurationsbefehle hat.