IOS-Berechtigungsstufen können keine vollständige laufende Konfiguration anzeigen

Inhalt

Einführung

In diesem Dokument wird erläutert, wie sich Berechtigungsebenen auf die Fähigkeit eines Benutzers auswirken, bestimmte Befehle auf einem Router auszuführen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Anzeigen der Router-Konfiguration

Wenn der Zugriff auf den Router anhand von Berechtigungsebenen konfiguriert wird, besteht ein häufiges Problem darin, dass die Befehle **show running** oder **write terminal** konfiguriert werden, die auf oder unter der Berechtigungsebene des Benutzers konfiguriert sind. Wenn der Benutzer den Befehl ausführt, scheint die Konfiguration leer zu sein. Das ist eigentlich beabsichtigt aus den folgenden Gründen:

- Der Befehl **write terminal** / **show running-config** zeigt eine leere Konfiguration. Dieser Befehl zeigt alle Befehle an, die der aktuelle Benutzer ändern kann (d. h. alle Befehle auf oder unter der aktuellen Berechtigungsebene des Benutzers). Aus Sicherheitsgründen sollte der Befehl keine Befehle über der aktuellen Berechtigungsebene des Benutzers anzeigen. In diesem Fall können Befehle wie **snmp-server community** verwendet werden, um die aktuelle Konfiguration des Routers zu ändern und vollständigen Zugriff auf den Router zu erhalten.
- Der Befehl **show config/show start-up config** zeigt eine vollständige Konfiguration, aber nicht die tatsächliche Konfiguration an. Stattdessen gibt der Befehl einfach den Inhalt des NVRAM aus, der zufällig die Konfiguration des Routers ist, wenn der Benutzer einen **Schreibspeicher** ausführt.

Berechtigungsstufen

Damit ein privilegierter Benutzer die gesamte Konfiguration im Arbeitsspeicher anzeigen kann, muss der Benutzer die Berechtigungen für alle Befehle ändern, die auf dem Router konfiguriert sind. Beispiel:

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local

username john privilege 9 password 0 doe
username six privilege 6 password 0 six
username poweruser privilege 15 password poweruser
username inout password inout
username inout privilege 15 autocommand show running

privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Um dieses Beispiel zu verstehen, müssen Sie die Berechtigungsebenen verstehen. Standardmäßig gibt es drei Befehlsstufen auf dem Router:

- Berechtigungsstufe 0 - Enthält die **Befehle disable**, **enable**, **exit**, **help** und **login.**
- Berechtigungsstufe 1 - Normale Ebene bei Telnet; enthält alle Befehle auf Benutzerebene in der `Router->`Eingabeaufforderung.
- Berechtigungsstufe 15 - Enthält alle Befehle auf Aktivierungsebene an der `Router#`-Eingabeaufforderung.

Befehle, die auf einer bestimmten Ebene in einem bestimmten Router verfügbar sind, können durch Eingabe eines Befehls gefunden werden**?** an der Router-Eingabeaufforderung. Befehle können zwischen Berechtigungsebenen verschoben werden, indem der Befehl **privilege** verwendet wird, wie im Beispiel veranschaulicht. In diesem Beispiel werden lokale Authentifizierung und Autorisierung dargestellt, die Befehle funktionieren jedoch ähnlich für die TACACS+- oder RADIUS-Authentifizierung und die Exec-Autorisierung (eine genauere Kontrolle des Routers kann durch Implementierung der TACACS+-Befehlsautorisierung mit einem Server erreicht werden.)

Weitere Details zu den Benutzern und Berechtigungsebenen, die im Beispiel dargestellt werden:

- Benutzer *6* kann den Befehl **show run** einbinden und ausführen, die resultierende

Konfiguration ist jedoch praktisch leer, da dieser Benutzer nichts konfigurieren kann (das **configure terminal** befindet sich auf Ebene 8 und nicht auf Ebene 6). Dem Benutzer ist es nicht gestattet, Benutzernamen und Kennwörter der anderen Benutzer anzuzeigen oder SNMP-Informationen (Simple Network Management Protocol) anzuzeigen.

- User *John* kann den Befehl **show run** einbinden und ausführen, sieht jedoch nur Befehle, die er konfigurieren kann (der **SNMP-server Community** Teil der Routerkonfiguration, da dieser Benutzer unser Netzwerkmanagement-Administrator ist). Er kann die **snmp-server-Community** konfigurieren, da **configure terminal** auf Ebene 8 (auf oder unter Ebene 9) liegt und die **snmp-server-Community** ein Level-8-Befehl ist. Dem Benutzer ist es nicht gestattet, Benutzernamen und Kennwörter der anderen Benutzer anzuzeigen, ihm wird jedoch die SNMP-Konfiguration vertraut.
- User *Inout* ist in der Lage, Telnet ein, und durch die Konfiguration für **automatische Befehlszeilenausgabe**, sieht die Konfiguration angezeigt, wird aber danach getrennt.
- User *poweruser* kann Telnet einbinden und den Befehl **show run** ausführen. Dieser Benutzer befindet sich auf Stufe 15 und kann alle Befehle anzeigen. Alle Befehle befinden sich auf oder unter Stufe 15. Benutzer auf dieser Ebene können auch Benutzernamen und Kennwörter anzeigen und steuern.

Zugehörige Informationen

- Command Lookup Tool **(nur registrierte Kunden)**
- IOS-Dokumentation für TACACS+ und RADIUS
- Support-Seite für TACACS/TACACS+
- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- Technischer Support - Cisco Systems