Zuweisen von Berechtigungsebenen mit TACACS+ und RADIUS

Inhalt

Einführung

In diesem Dokument wird erläutert, wie die Berechtigungsebene für bestimmte Befehle geändert wird. Außerdem wird ein Beispiel mit Teilen von Beispielkonfigurationen für einen Router sowie TACACS+- und RADIUS-Server bereitgestellt.

Voraussetzungen

Anforderungen

Leser dieses Dokuments sollten über Kenntnisse der Berechtigungsebenen eines Routers verfügen.

Standardmäßig gibt es drei Berechtigungsebenen für den Router.

- Berechtigungsstufe 1 = nicht privilegiert (Eingabeaufforderung ist `router>`), die Standardstufe für die Anmeldung
- Berechtigungsstufe 15 = privilegiert (Eingabeaufforderung ist `router#`), die Ebene nach dem Aktivieren
- Berechtigungsstufe 0 = selten verwendet, beinhaltet jedoch 5 Befehle: **Deaktivieren**, **Aktivieren**, **Beenden**, **Hilfe** und **Abmelden**

Die Ebenen 2-14 werden in einer Standardkonfiguration nicht verwendet, Befehle, die normalerweise auf Ebene 15 liegen, können jedoch auf eine dieser Ebenen reduziert werden, und Befehle, die normalerweise auf Ebene 1 sind, können auf eine dieser Ebenen verschoben werden. Offensichtlich beinhaltet dieses Sicherheitsmodell eine gewisse Administration auf dem Router.

Um die Berechtigungsstufe als angemeldeter Benutzer festzulegen, geben Sie den Befehl **show**

privilege ein. Um zu bestimmen, welche Befehle auf einer bestimmten Berechtigungsebene für die von Ihnen verwendete Version der Cisco IOS®-Software verfügbar sind, geben Sie einen ein. auf der Befehlszeile, wenn Sie sich auf dieser Berechtigungsebene angemeldet haben.

Hinweis: Anstatt Berechtigungen zuzuweisen, können Sie eine Befehlsautorisierung durchführen, wenn der Authentifizierungsserver TACACS+ unterstützt. Das RADIUS-Protokoll unterstützt keine Befehlsautorisierung.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco IOS Software Releases 11.2 und höher.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

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

Beispiel

In diesem Beispiel werden **snmp-server-**Befehle von der Berechtigungsebene 15 (der Standardwert) in die Berechtigungsebene 7 verschoben. Der **Ping-**Befehl wird von der Berechtigungsebene 1 in die Berechtigungsebene 7 verschoben. Wenn Benutzer 7 authentifiziert wird, wird diesem Benutzer vom Server die Berechtigungsstufe 7 zugewiesen, und der Befehl **show privilege** (Aktuelle Berechtigungsstufe ist 7) wird angezeigt. Der Benutzer kann im Konfigurationsmodus Ping-Signale senden und eine SNMP-Serverkonfiguration vornehmen. Andere Konfigurationsbefehle sind nicht verfügbar.

Konfigurationen - Router

Router - 11.2

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router: 11.3.3.T und höher (bis 12.0.5.T)

```
aaa new-model
aaa authentication login default tacacs+|radius local
aaa authorization exec default tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Router - 12.0.5.T und höher

```
aaa new-model
aaa authentication login default group tacacs+|radius local
aaa authorization exec default group tacacs+|radius local
username backup privilege 7 password 0 backup
tacacs-server host 171.68.118.101
tacacs-server key cisco
radius-server host 171.68.118.101
radius-server key cisco
privilege configure level 7 snmp-server host
privilege configure level 7 snmp-server enable
privilege configure level 7 snmp-server
privilege exec level 7 ping
privilege exec level 7 configure terminal
privilege exec level 7 configure
```

Konfigurationen - Server

Cisco Secure NT TACACS+

Führen Sie diese Schritte aus, um den Server zu konfigurieren.

1. Geben Sie den Benutzernamen und das Kennwort ein.
2. Stellen Sie sicher, dass unter Gruppeneinstellungen shell/exec aktiviert ist und dass 7 in das Feld Berechtigungsebene eingegeben wurde.

TACACS+ - Stanza in Freeware Server

```
Stanza in TACACS+ freeware:
user = seven {
login = cleartext seven
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure UNIX TACACS+

```
user = seven {
password = clear "seven"
service = shell {
set priv-lvl = 7
}
}
```

Cisco Secure NT RADIUS

Führen Sie diese Schritte aus, um den Server zu konfigurieren.

1. Geben Sie den Benutzernamen und das Kennwort ein.
2. In den Gruppeneinstellungen für IETF, Servicetyp (Attribut 6) = **NAS-Prompt**
3. Aktivieren Sie im Bereich CiscoRADIUS das Kontrollkästchen **AV-Pair**, und geben Sie im rechteckigen Feld darunter **shell:priv-lvl=7** ein.

Cisco Secure UNIX RADIUS

```
user = seven{
radius=Cisco {
check_items= {
2="seven"
}
reply_attributes= {
6=7
9,1="shell:priv-lvl=7"
}
}
}
```

Dies ist die Benutzerdatei für den Benutzernamen "sieben".

Hinweis: Der Server muss Cisco AV-Paare unterstützen.

- Sieben Kennwort = **passwdxyz**
- Servicetyp = **Shell-User**
- cisco-avpair =**shell:priv-lvl=7**

Zugehörige Informationen

- RADIUS-Support-Seite
- Anforderungen für Kommentare (RFCs)
- TACACS+ in der IOS-Dokumentation
- Support-Seite für TACACS+
- Support-Seite für Cisco Secure UNIX
- Support-Seite für Cisco Secure ACS für Windows
- Technischer Support - Cisco Systems