FreeRADIUS für Administratorzugriff auf Cisco IOS - Konfigurationsbeispiel

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Konfigurieren eines Switches für die Authentifizierung und Autorisierung](#)
[Konfiguration von FreeRADIUS](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die RADIUS-Authentifizierung auf Cisco IOS®-Switches mit einem RADIUS-Server eines Drittanbieters (FreeRADIUS) konfigurieren. In diesem Beispiel wird die direkte Platzierung eines Benutzers im Modus "Privileg 15" bei der Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass der Cisco Switch in FreeRADIUS als Client definiert ist, dessen IP-Adresse und derselbe geheime Schlüssel in FreeRADIUS und dem Switch definiert sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FreeRADIUS
- Cisco IOS Version 12.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Konfigurieren eines Switches für die Authentifizierung und Autorisierung

1. Geben Sie Folgendes ein, um auf dem Switch einen lokalen Benutzer mit vollständigen Berechtigungen für den Fallback-Zugriff zu erstellen:

   ```
   Switch(config)#username admin privilege 15 password 0 cisco123!
   ```
2. Um AAA zu aktivieren, geben Sie Folgendes ein:

   ```
   switch(config)# aaa new-model
   ```
3. Geben Sie Folgendes ein, um die IP-Adresse des RADIUS-Servers sowie den Schlüssel anzugeben:

   ```
   switch# configure terminal
   switch(config)#radius-server host 172.16.71.146 auth-port 1645 acct-port 1646
   switch(config)#radius-server key hello123
   ```

   Hinweis: Der Schlüssel muss mit dem auf dem RADIUS-Server für den Switch konfigurierten gemeinsamen geheimen Schlüssel übereinstimmen.
4. Um die Verfügbarkeit des RADIUS-Servers zu testen, geben Sie den Befehl **test aaa ein**:

   ```
   switch# test aaa server Radius 172.16.71.146 user1 Ur2Gd2BH
   ```

   Die Testauthentifizierung schlägt fehl, und der Server wird abgelehnt, da er noch nicht konfiguriert ist. Es wird jedoch bestätigt, dass der Server selbst erreichbar ist.
5. Geben Sie Folgendes ein, um die Anmeldeauthentifizierungen so zu konfigurieren, dass sie auf lokale Benutzer zurückgreifen, wenn RADIUS nicht erreichbar ist:

   ```
   switch(config)#aaa authentication login default group radius local
   ```
6. Geben Sie Folgendes ein, um die Autorisierung für eine Berechtigungsstufe von 15 zu konfigurieren, solange ein Benutzer authentifiziert wird:

   ```
   switch(config)#aaa authorization exec default group radius if-authenticated
   ```

Konfiguration von FreeRADIUS

Client auf dem FreeRADIUS-Server definieren

1. Geben Sie Folgendes ein, um zum Konfigurationsverzeichnis zu navigieren:

   ```
   # cd /etc/freeradius
   ```
2. Geben Sie Folgendes ein, um die Datei **clients.conf** zu bearbeiten:

   ```
   # sudo nano clients.conf
   ```

3. Geben Sie Folgendes ein, um jedes durch den Hostnamen identifizierte Gerät (Router/Switch) hinzuzufügen und den richtigen gemeinsamen geheimen Schlüssel einzufügen:

```
client 192.168.1.1 {
secret = secretkey
nastype = cisco
shortname = switch
}
```

4. Um die Benutzerdatei zu bearbeiten, geben Sie Folgendes ein:

```
# sudo nano users
```

5. Fügen Sie jeden Benutzer hinzu, der auf das Gerät zugreifen darf. In diesem Beispiel wird die Cisco IOS-Berechtigungsstufe 15 für den Benutzer "cisco" festgelegt.

```
cisco Cleartext-Password := "password"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=15"
```

6. Um FreeRADIUS neu zu starten, geben Sie Folgendes ein:

```
# sudo /etc/init.d/freeradius restart
```

7. Um die STANDARD-Benutzergruppe in der Benutzerdatei zu ändern und allen Benutzern, die Mitglieder von cisco-rw sind, die Berechtigungsstufe 15 zuzuweisen, geben Sie Folgendes ein:

```
DEFAULT Group == cisco-rw, Auth-Type = System
Service-Type = NAS-Prompt-User,
cisco-avpair :="shell:priv-lvl=15"
```

8. Sie können weitere Benutzer auf verschiedenen Berechtigungsebenen nach Bedarf in der Datei FreeRADIUS users hinzufügen. Dieser Benutzer (life) erhält beispielsweise die Stufe 3 (Systemwartung):

```
sudo nano/etc/freeradius/users

life Cleartext-Password := "testing"
Service-Type = NAS-Prompt-User,
Cisco-AVPair = "shell:priv-lvl=3"

Restart the FreeRADIUS service:
sudo /etc/init.d/freeradius restart
```

Hinweis: Die Konfiguration in diesem Dokument basiert auf FreeRADIUS unter Ubuntu 12.04 LTE und 13.04.

Überprüfung

Verwenden Sie folgende Befehle, um die Konfiguration des Switches zu überprüfen:

```
switch# show  run | in radius       (Show the radius configuration)
switch# show run | in aaa           (Show the running AAA configuration)
switch# show startup-config Radius  (Show the startup AAA configuration in
start-up configuration)
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- FreeRADIUS
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.