

Grundlegendes zum Befehl AAA Authentication Login Default Local Group TACACS+

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Verhalten des Befehls `aaa authentication login default local group tacacs+` auf einem Cisco IOS[®]-Gerät beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt Folgendes:

- Das **neue aaa-Modell** wird auf dem Gerät aktiviert.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

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 Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfigurieren

Hinweis: Verwenden Sie den [Cisco CLI Analyzer](#) aus dem Cisco Tool Catalog, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten. Nur registrierte Cisco Benutzer haben Zugriff auf interne Tools und Informationen von Cisco.

Konfigurieren Sie diese Befehle auf dem Gerät im globalen Konfigurationsmodus:

```
aaa new-model
aaa authentication login default local group tacacs+
```

Mit nur `aaa new model` konfiguriert wurde, wird die lokale Authentifizierung auf alle Leitungen und Schnittstellen angewendet (mit Ausnahme der Konsolenleitung `line con 0`).

Hier wird die AAA-Methodenliste auf alle Anmeldeversuche in allen Zeilen des Geräts angewendet, wobei zuerst die lokale Datenbank und dann ggf. der TACACS-Server (Terminal Access Controller Access Control System) überprüft wird.

```
username cisco privilege 15 password 0 cisco
```

Lokale Benutzerdatenbank:

```
tacacs-server host 10.20.220.141
tacacs-server key cisco
```

Der TACACS-Server ist jetzt konfiguriert.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

1. Aktivieren Sie **Debug TACACS** und **Debug AAA Authentication** auf dem zu testenden Gerät.

```
RUT#show debug
General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
```

2. Führen Sie ein Telnet auf dem Gerät aus:

```
RUT#show ip interface brief | exclude unassigned
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/1          10.197.235.96   YES DHCP    up          up
Loopback0                 192.168.1.2     YES manual  up          up
```

```
RUT#telnet 192.168.1.2
Trying 192.168.1.2 ... Open
```

User Access Verification

```
Username: cisco
*Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
*Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list 'default'
Password:
```

```
RUT>
```

Es wurde nicht versucht, den TACACS-Server zu erreichen, da der Benutzername `cisco` lokal gefunden wurde.

Wenn Sie nun versuchen, eine Anmeldeinformation zu verwenden, die nicht lokal auf dem Gerät konfiguriert ist, führen Sie Folgendes aus:

```
RUT#telnet 192.168.1.2
Trying 192.168.1.2 ... Open
```

User Access Verification

Username:

```
*Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f
*Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list 'default'
Username: cisco1
*Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing
*Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31
*Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)
*Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141
*Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up
*Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet
% Authentication failed
```

Sie können sehen, dass er versucht, den TACACS-Server 10.20.220.141 zu erreichen. Es handelt sich um ein erwartetes Standardverhalten. Auf dem TACACS-Server ist kein Benutzername cisco1 konfiguriert, daher wird als Authentifizierung fehlgeschlagen angezeigt.

Wenn das Gerät über ein AAA-Authentifizierungsprotokoll in der Standardgruppe tacacs+ local in der Konfiguration verfügt, lautet seine erste Voreinstellung TACACS. Wenn das TACACS-Gerät erreichbar ist, aber kein Benutzer es konfiguriert hat, wird kein Fallback ausgeführt, und es wird versucht, in der lokalen Datenbank zu suchen. Es wird die Meldung angezeigt, **Authentication failed (Authentifizierung fehlgeschlagen)**.

Fehlerbehebung

Es sind derzeit keine spezifischen Informationen zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

- [Konfigurieren von grundlegendem AAA auf einem Zugriffsserver](#)
- [Technischer Support und Downloads von Cisco](#)

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.