Konfigurieren von grundlegendem AAA auf einem Zugriffsserver

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie AAA (Authentication, Authorization, and Accounting) auf einem Cisco Router mit Radius- oder TACACS+-Protokollen konfiguriert wird.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Hauptproduktreihe der Cisco IOS®-Software, Version 12.

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.

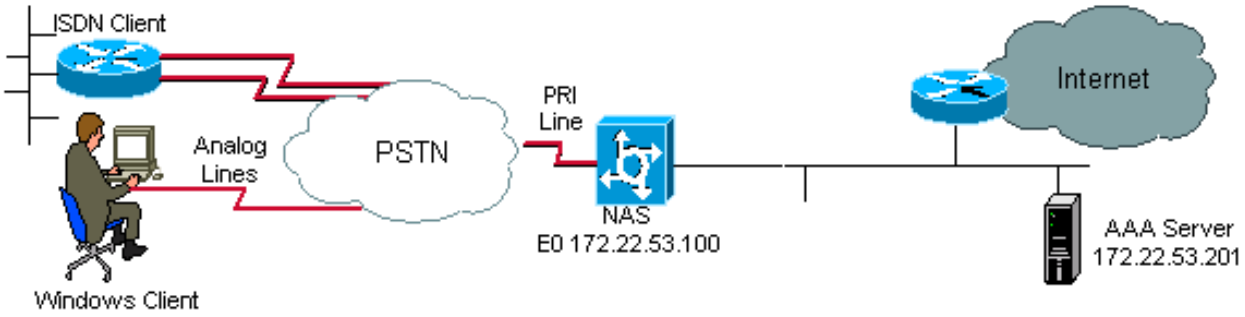
Hintergrundinformationen

In diesem Dokument wird erläutert, wie AAA (Authentication, Authorization, and Accounting) auf einem Cisco Router mit Radius- oder TACACS+-Protokollen konfiguriert wird. Ziel dieses Dokuments ist es nicht, alle AAA-Funktionen abzudecken, sondern die wichtigsten Befehle zu erklären und einige Beispiele und Richtlinien bereitzustellen.

> **Anmerkung:** Lesen Sie den Abschnitt zur allgemeinen AAA-Konfiguration, bevor Sie mit der Cisco IOS-Konfiguration fortfahren. Andernfalls kann es zu Fehlkonfigurationen und anschließenden Sperrungen kommen.

Weitere Informationen finden Sie unter Konfigurationsleitfaden für Authentifizierung, Autorisierung und Abrechnung.

Netzwerkdiagramm



Netzwerkdiagramm

Allgemeine AAA-Konfiguration

AAA aktivieren

Zur Aktivierung von AAA müssen Sie den Befehl **aaa new-model in der globalen Konfiguration konfigurieren.**

> **Anmerkung:** Bis zur Aktivierung dieses Befehls werden alle anderen AAA-Befehle ausgeblendet.

> **Warnung:** Mit dem Befehl **aaa new-model** wird sofort die lokale Authentifizierung auf alle Leitungen und Schnittstellen angewendet (mit Ausnahme der Konsolenleitung **line con 0**). Wenn nach dem Aktivieren dieses Befehls eine Telnet-Sitzung mit dem Router geöffnet wird (oder wenn eine Verbindung aufgrund eines Zeitüberschreitens erneut hergestellt werden muss), muss der Benutzer mit der lokalen Datenbank des Routers authentifiziert werden. Es wird empfohlen, vor dem Starten der AAA-Konfiguration auf dem Zugriffsserver einen Benutzernamen und ein Kennwort zu definieren, damit Sie nicht vom Router ausgeschlossen werden. Siehe nächstes Codebeispiel.

```
Router(config)#username xxx password yyy
```

> **Tipp:** Bevor Sie die AAA-Befehle konfigurieren, `save` Ihre Konfiguration ändern. Sie können `save` die Konfiguration erst erneut durchführen, nachdem Sie Ihre AAA-Konfiguration abgeschlossen haben (und sich davon überzeugt haben, dass sie ordnungsgemäß funktioniert). Dadurch können Sie sich von unerwarteten Aussperrungen erholen, da Sie jede Änderung mit einem Neuladen des Routers rückgängig machen können.

Geben Sie den externen AAA-Server an.

Definieren Sie in der globalen Konfiguration das mit AAA verwendete Sicherheitsprotokoll (Radius, TACACS+). Wenn Sie keines dieser beiden Protokolle verwenden möchten, können Sie die lokale Datenbank auf dem Router verwenden.

Wenn Sie TACACS+ verwenden, verwenden Sie den Befehl **tacacs-server host <IP-Adresse des AAA-Servers> <key>.**

Wenn Sie Radius verwenden, verwenden Sie den Befehl **radius-server host <IP-Adresse des**

AAA-Servers> <key>.

AAA-Serverkonfiguration

Konfigurieren Sie auf dem AAA-Server die folgenden Parameter:

- Den Namen des Zugriffsservers.
- Die IP-Adresse, die der Zugriffsserver für die Kommunikation mit dem AAA-Server verwendet.**Anmerkung:** Wenn sich beide Geräte im gleichen Ethernet-Netzwerk befinden, verwendet der Zugriffsserver beim Senden des AAA-Pakets standardmäßig die IP-Adresse, die auf der Ethernet-Schnittstelle definiert ist. Dies ist wichtig, wenn der Router über mehrere Schnittstellen (und damit mehrere Adressen) verfügt.
- Denselben Schlüssel **<key>** , der im Zugriffsserver konfiguriert ist.**Anmerkung:** Beim Schlüssel wird die Groß-/Kleinschreibung beachtet.
- Das vom Zugriffsserver verwendete Protokoll (TACACS+ oder Radius).

Die genaue Vorgehensweise zum Konfigurieren der vorherigen Parameter finden Sie in der Dokumentation des AAA-Servers. Wenn der AAA-Server nicht richtig konfiguriert ist, können AAA-Anforderungen vom NAS-Gerät ignoriert werden, und die Verbindung kann fehlschlagen.

Der AAA-Server muss vom Zugriffserver aus über IP erreichbar sein (führen Sie einen **Ping-Test durch, um die Netzwerkverbindungen zu überprüfen).**

Authentifizierungskonfiguration

Durch die Authentifizierung werden Benutzer überprüft, bevor diese Zugriff auf das Netzwerk und die Netzwerkservices erhalten (die bei der Autorisierung überprüft werden).

Gehen Sie wie folgt vor, um die AAA-Authentifizierung zu konfigurieren:

1. Definieren Sie zunächst eine benannte Liste mit Authentifizierungsmethoden (im globalen Konfigurationsmodus).
2. Wenden Sie diese Liste auf eine oder mehrere Schnittstellen an (im Schnittstellenkonfigurationsmodus).

Die einzige Ausnahme ist die Standardmethodenliste (die **default** heißt). Die Standardmethodenliste wird automatisch auf alle Schnittstellen angewendet, mit Ausnahme derer, für die eine benannte Methodenliste explizit definiert ist. Eine definierte Methodenliste überschreibt die Standardmethodenliste.

In diesen Authentifizierungsbeispielen wird die Radius-, Anmelde- und PPP-Authentifizierung (Point-to-Point Protocol) verwendet, um Konzepte wie Methoden und benannte Listen zu erläutern. In allen Beispielen kann TACACS+ für Radius oder eine lokale Authentifizierung verwendet werden.

Die Cisco IOS-Software verwendet die erste aufgeführte Methode zur Authentifizierung von Benutzern. Wenn diese Methode fehlschlägt (angezeigt durch ERROR), wählt die Cisco IOS-Software die nächste in der Methodenliste aufgeführte Authentifizierungsmethode aus. Dieser Prozess wird fortgesetzt, bis die Kommunikation mit einer aufgelisteten Authentifizierungsmethode erfolgreich ist oder alle in der Methodenliste definierten Methoden ausgeschöpft sind.

Es ist wichtig zu beachten, dass die Cisco IOS-Software die Authentifizierung mit der nächsten

aufgelisteten Authentifizierungsmethode nur vornimmt, wenn die vorherige Methode nicht reagiert. Wenn die Authentifizierung zu einem beliebigen Zeitpunkt in diesem Zyklus fehlschlägt, d. h. wenn die Antworten des AAA-Servers oder der lokalen Benutzernamendatenbank den Benutzerzugriff verweigern (was durch einen FAIL-Fehler angezeigt wird), wird der Authentifizierungsprozess beendet, und es werden keine anderen Authentifizierungsmethoden versucht.

Zur Ermöglichung einer Benutzerauthentifizierung müssen Sie den Benutzernamen und das Kennwort auf dem AAA-Server konfigurieren.

Anmeldeauthentifizierung

Sie können den Befehl **aaa authentication login verwenden, um Benutzer zu authentifizieren, die Exec-Zugriff auf den Zugriffsserver (tty, vty, console und aux) wünschen.**

Beispiel 1: Zugriff auf Führungskräfte mit Radius und dann lokal

```
Router(config)#aaa authentication login default group radius local
```

Im vorherigen Befehl:

- Die benannte Liste ist die Standardliste (Standard).
- Es gibt zwei Authentifizierungsmethoden (Gruppenradius und lokal).

Alle Benutzer werden mit dem Radius-Server authentifiziert (die erste Methode). Wenn der Radius-Server nicht reagiert, wird die lokale Router-Datenbank verwendet (die zweite Methode). Definieren Sie für die lokale Authentifizierung den Benutzernamen und das Kennwort:

```
Router(config)#username xxx password yyy
```

Da der Standard-Login-Befehl **aaa authentication** verwendet wird, wird die Anmeldeauthentifizierung automatisch für alle Anmeldeverbindungen (z. B. tty, vty, console und aux) angewendet.

> **Anmerkung:** Der Server (Radius oder TACACS+) kann nicht auf eine vom Zugriffsserver gesendete **AAA-Authentifizierungsanfrage** antworten, wenn keine IP-Verbindung besteht, wenn der Zugriffsserver auf dem AAA-Server nicht richtig definiert ist oder wenn der AAA-Server auf dem Zugriffsserver nicht richtig definiert ist.

> **Anmerkung:** Wenn Sie das vorherige Beispiel ohne **lokales** Schlüsselwort verwenden, lautet das Ergebnis:

```
Router(config)#aaa authentication login default group radius
```

> **Anmerkung:** Wenn der AAA-Server nicht auf die Authentifizierungsanfrage antwortet, schlägt die Authentifizierung fehl (da der Router keine andere Möglichkeit hat, es zu versuchen).

> **Anmerkung:** Das **group**-Schlüsselwort bietet eine Möglichkeit, aktuelle Serverhosts zu gruppieren. Mit dieser Funktion kann der Benutzer eine Teilmenge der konfigurierten Server-

Hosts auswählen und für einen bestimmten Service verwenden.

Beispiel 2: Konsolenzugriff mit Leitungskennwort

Erweitern Sie die Konfiguration aus Beispiel 1, sodass die Konsolenanmeldung nur durch das Kennwort authentifiziert wird, das auf line con 0 festgelegt ist.

Die Liste KONSOLE wird definiert und dann auf "line con 0" angewendet.

Konfiguration:

```
Router(config)#aaa authentication login CONSOLE line
```

Im vorherigen Befehl:

- die benannte Liste lautet KONSOLE.
- es gibt nur ein Authentifizierungsverfahren (Leitung).

Wenn eine benannte Liste (in diesem Beispiel CONSOLE) erstellt wird, muss sie auf eine Zeile oder Schnittstelle angewendet werden, bevor sie ausgeführt wird. Dies geschieht mithilfe des login authentication command:

```
Router(config)#line con 0
Router(config-line)#exec-timeout 0 0
Router(config-line)#password cisco
Router(config-line)#login authentication CONSOLE
```

Die CONSOLE-Liste überschreibt die **Standardmethodenliste** für line con 0. Nach dieser Konfiguration für line con 0 müssen Sie das Kennwort **cisco** eingeben, um Konsolenzugriff zu erhalten. Die Standardliste wird weiterhin für tty, vty und aux verwendet.

> **Anmerkung:** Um den Konsolenzugriff durch einen lokalen Benutzernamen und ein lokales Kennwort zu authentifizieren, verwenden Sie das folgende Codebeispiel:

```
Router(config)#aaa authentication login CONSOLE local
```

In diesem Fall müssen ein Benutzername und ein Kennwort in der lokalen Datenbank des Routers konfiguriert werden. Die Liste muss auch auf die Leitung oder Schnittstelle angewendet werden.

> **Anmerkung:** Um keine Authentifizierung zu erhalten, verwenden Sie das nächste Codebeispiel:

```
Router(config)#aaa authentication login CONSOLE none
```

In diesem Fall gibt es keine Authentifizierung für den Zugriff auf die Konsole. Die Liste muss auch auf die Leitung oder Schnittstelle angewendet werden.

Beispiel 3: Aktivierungsmodus für Zugriff mit externem AAA-Server

Sie können eine Authentifizierung ausgeben, um in den Aktivierungsmodus zu gelangen (Berechtigung 15).

Konfiguration:

```
Router(config)#aaa authentication enable default group radius enable
```

Nur das Passwort kann angefordert werden, der Benutzername ist $enab15$. Daher muss auf dem AAA-Server der Benutzername $enab15$ definiert werden.

Wenn der Radius-Server nicht antwortet, muss ggf. das lokal auf dem Router konfigurierte enable-Kennwort eingegeben werden.

PPP-Authentifizierung

Der Befehl **aaa authentication ppp wird verwendet, um eine PPP-Verbindung zu authentifizieren.** Es wird in der Regel zur Authentifizierung von ISDN oder analogen Remote-Benutzern verwendet, die über einen Zugriffsserver auf das Internet oder eine Zentrale zugreifen möchten.

Beispiel 1: Zentrale PPP-Authentifizierungsmethode für alle Benutzer

Der Zugriffsserver verfügt über eine ISDN-Schnittstelle, die für die Annahme von PPP-Einwahlclients konfiguriert ist. Wir verwenden eine **Wählerdrehgruppe 0**, die Konfiguration kann jedoch über die Hauptschnittstelle oder die Wählprofilschnittstelle erfolgen.

Konfiguration:

```
Router(config)#aaa authentication ppp default group radius local
```

Dieser Befehl authentifiziert alle PPP-Benutzer mit Radius. Wenn der Radius-Server nicht antwortet, wird die lokale Datenbank verwendet.

Beispiel 2: PPP-Authentifizierung für eine bestimmte Liste

Um eine benannte Liste anstelle der Standardliste zu verwenden, konfigurieren Sie die folgenden Befehle:

```
Router(config)#aaa authentication ppp ISDN_USER group radius

Router(config)#interface dialer 0
Router(config-if)#ppp authentication chap ISDN_USER
```

In diesem Beispiel lautet die Liste ISDN_USER und die Methode ist Radius.

Beispiel 3: PPP wird in der Zeichenmodus-Sitzung gestartet

Der Zugriffsserver verfügt über eine interne Modemkarte (Mica, Microcom oder Next Port). Es wird davon ausgegangen, dass **aaa authentication login-** und **aaa authentication ppp**-Befehle konfiguriert sind.

Greift ein Modembenutzer zuerst mit einer exec-Sitzung im Zeichenmodus auf den Router zu (z. B. mit Terminal Window nach dem Wählen), wird der Benutzer über eine tty-Leitung authentifiziert. Um in eine Sitzung im Paketmodus zu starten, müssen Benutzer **ppp default oder ppp eingeben.** Da die PPP-Authentifizierung explizit konfiguriert wird (mit **aaa authentication ppp), wird der Benutzer erneut auf PPP-Ebene authentifiziert.**

Um diese zweite Authentifizierung zu vermeiden, verwenden Sie das Schlüsselwort **if-need**:

```
Router(config)#aaa authentication login default group radius local
Router(config)#aaa authentication ppp default group radius local if-needed
```

> **Anmerkung:** Wenn der Client eine PPP-Sitzung direkt startet, wird die PPP-Authentifizierung direkt durchgeführt, da kein Anmeldezugriff auf den Zugriffsserver besteht.

Autorisierung konfigurieren

Autorisierung ist der Prozess, mit dem Sie steuern können, was ein Benutzer tun kann.

Für die AAA-Authentifizierung gelten die gleichen Regeln wie für die AAA-Autorisierung:

1. Definieren Sie zunächst eine benannte Liste mit Autorisierungsmethoden.
2. Wenden Sie diese Liste dann auf eine oder mehrere Schnittstellen an (mit Ausnahme der Standardmethodenliste).
3. Die erste aufgelistete Methode wird verwendet. Wenn sie nicht reagiert, wird die zweite verwendet, und so weiter.

Methodenlisten sind für den angeforderten Autorisierungstyp spezifisch. Im Mittelpunkt dieses Dokuments stehen die Autorisierungstypen Exec und Network.

Weitere Informationen zu den anderen Autorisierungsarten finden Sie im Cisco IOS Security Configuration Guide .

Exec-Autorisierung

Mit dem Befehl **aaa authorization exec wird festgelegt, ob der Benutzer eine EXEC-Shell ausführen darf.** Diese Funktion kann Benutzerprofilinformationen wie Informationen zu automatischen Befehlen, Leerlaufzeitüberschreitung, Sitzungszeitüberschreitung, Zugriffslisten und Berechtigungen sowie andere benutzerspezifische Faktoren zurückgeben.

Die Exec-Autorisierung wird nur über vty- und tty-Verbindungen ausgeführt.

Im nächsten Beispiel wird Radius verwendet.

Beispiel 1: Dieselben Exec-Authentifizierungsmethoden für alle Benutzer

Bei Authentifizierung mit:

```
Router(config)#aaa authentication login default group radius local
```

Alle Benutzer, die sich beim Zugriffsserver anmelden möchten, müssen über Radius (erste Methode) oder die lokale Datenbank (zweite Methode) autorisiert werden.

Konfiguration:

```
Router(config)#aaa authorization exec default group radius local
```

> **Anmerkung:** Auf dem AAA-Server muss Service-Type=1 (Anmeldung) ausgewählt werden.

> **Anmerkung:** Wenn bei diesem Beispiel das **lokale** Schlüsselwort nicht enthalten ist und der AAA-Server nicht reagiert, ist die Autorisierung daher nicht möglich, und die Verbindung kann fehlschlagen.

> **Anmerkung:** In den nächsten Beispielen 2 und 3 müssen Sie keine Befehle zum Router hinzufügen. Sie müssen nur das Profil auf dem Zugriffsserver konfigurieren.

Beispiel 2: Zuweisung der Exec-Privilegstufen vom AAA-Server

Konfigurieren Sie auf Basis von Beispiel 1 das nächste Cisco AV-Paar auf dem AAA-Server, sodass sich ein Benutzer beim Zugriffsserver anmelden und direkt in den Aktivierungsmodus wechseln kann:

```
shell:priv-lvl=15
```

Der Benutzer kann nun direkt in den Aktivierungsmodus wechseln.

> **Anmerkung:** Wenn die erste Methode nicht reagiert, wird die lokale Datenbank verwendet. Der Benutzer kann jedoch nicht direkt in den privilegierten Modus wechseln, sondern muss den Befehl enable eingeben und das Kennwort **enable eingeben**.

Beispiel 3: Zuweisen eines Leerlaufzeitlimits vom AAA-Server

Verwenden Sie das IETF Radius-Attribut 28, um eine Leerlaufzeitüberschreitung zu konfigurieren (sodass die Sitzung getrennt wird, wenn nach der Leerlaufzeitüberschreitung kein Datenverkehr mehr besteht): Idle-Timeout (Leerlaufzeit) im Benutzerprofil.

Netzwerkautorisierung

Die Fehlermeldung **aaa authorization network** -Befehl wird die Autorisierung für alle netzwerkbezogenen Serviceanforderungen wie PPP, SLIP und ARAP ausgeführt. Dieser Abschnitt konzentriert sich auf PPP, das am häufigsten verwendet wird.

Der AAA-Server überprüft, ob eine PPP-Sitzung durch den Client zulässig ist. Darüber hinaus können PPP-Optionen vom Client angefordert werden: Callback, Komprimierung, IP-Adresse usw. Diese Optionen müssen im Benutzerprofil auf dem AAA-Server konfiguriert werden. Darüber hinaus kann das AAA-Profil für einen bestimmten Client Leerlauf-Timeout, Zugriffslisten und andere benutzerspezifische Attribute enthalten, die von der Cisco IOS-Software heruntergeladen und für diesen Client angewendet werden können.

Die folgenden Beispiele zeigen die Autorisierung mit Radius.

Beispiel 1: Dieselben Netzwerkautorisierungsmethoden für alle Benutzer

Der Zugriffsserver wird verwendet, um PPP-Einwahlverbindungen zu akzeptieren.

Benutzer werden authentifiziert (wie zuvor konfiguriert) mit:

```
Router(config)#aaa authentication ppp default group radius local
```

Verwenden Sie den nächsten Befehl, um die Benutzer zu autorisieren:

```
Router(config)#aaa authorization network default group radius local
```

> **Anmerkung:** Konfigurieren Sie auf dem AAA-Server Folgendes: **Service-Type=7** (gerahmt) und **Framed-Protocol=PPP**.

Beispiel 2: Benutzerspezifische Attribute anwenden

Sie können den AAA-Server verwenden, um benutzerspezifische Attribute wie IP-Adresse, Rückrufnummer, Timeout-Wert für Leerlauf beim Wählvorgang oder Zugriffsliste usw. zuzuweisen. Bei einer solchen Implementierung lädt der NAS die entsprechenden Attribute aus dem Benutzerprofil des AAA-Servers herunter.

Beispiel 3: PPP-Autorisierung mit einer bestimmten Liste

Ähnlich wie bei der Authentifizierung sollten Sie einen Listennamen anstelle des Standardnamens konfigurieren:

```
Router(config)#aaa authorization network ISDN_USER group radius local
```

Wenden Sie diese Liste dann auf die Schnittstelle an:

```
Router(config)#interface dialer 0
Router(config-if)#ppp authorization ISDN_USER
```

Kontoführungskonfiguration

Mit der AAA-Accounting-Funktion können Sie die von Benutzern aufgerufenen Services und die von ihnen genutzten Netzwerkressourcen verfolgen.

Für die AAA-Abrechnung gelten die gleichen Regeln wie für Authentifizierung und Autorisierung:

1. Sie müssen zunächst eine benannte Liste von Abrechnungsmethoden definieren.
2. Wenden Sie diese Liste dann auf eine oder mehrere Schnittstellen an (mit Ausnahme der Standardmethodenliste).
3. Die erste aufgelistete Methode wird verwendet, wenn keine Reaktion erfolgt, wird die zweite verwendet usw.

- Die Netzwerkabrechnung bietet Informationen für alle PPP-, Slip- und AppleTalk Remote Access Protocol (ARAP)-Sitzungen: Paketanzahl, Oktettanzahl, Sitzungszeit, Start- und Stoppzeit.
- Exec Accounting enthält Informationen über EXEC-Terminalsitzungen (z. B. eine Telnet-Sitzung) des Netzwerkzugriffsservers: Sitzungszeit, Start- und Stoppzeit.

Im nächsten Beispiel wird erläutert, wie Informationen an den AAA-Server gesendet werden können.

Beispiele für die Konfiguration der Buchhaltung

Beispiel 1: Buchungsdatensätze generieren und anhalten

Für jede Einwahl-PPP-Sitzung werden nach der Authentifizierung des Clients und nach der Trennung mit dem Schlüsselwort **start-stop** Kontoinformationen an den AAA-Server gesendet.

```
Router(config)#aaa accounting network default start-stop group radius local
```

Beispiel 2: Nur Buchungsdatensätze generieren und anhalten

Wenn Kontoinformationen erst gesendet werden müssen, nachdem die Verbindung eines Clients getrennt wurde, verwenden Sie das Schlüsselwort **stop,** und konfigurieren Sie die nächste Zeile:

```
Router(config)#aaa accounting network default stop group radius local
```

Beispiel 3: Generieren von Ressourceneinträgen für Authentifizierungs- und Verhandlungsfehler

Bis zu diesem Zeitpunkt bietet die AAA-Abrechnung Unterstützung für Start- und Stoppdatensätze für Anrufe, die die Benutzerauthentifizierung bestanden haben.

Wenn die Authentifizierung oder PPP-Aushandlung fehlschlägt, ist kein Authentifizierungsdatensatz vorhanden.

Die Lösung ist die Verwendung eines Stoppdatensatzes für die Abrechnung bei einem AAA-Ressourcenausfall:

```
Router(config)#aaa accounting send stop-record authentication failure
```

Ein Stoppdatensatz wird an den AAA-Server gesendet.

Beispiel 4: Vollständige Ressourcenerfassung aktivieren

Zur Aktivierung der vollständigen Ressourcenabrechnung, die sowohl einen Startdatensatz bei der Anrufeinrichtung als auch einen Stoppdatensatz bei Anrufbeendigung generiert, müssen Sie Folgendes konfigurieren:

```
Router(config)#aaa accounting resource start-stop
```

Dieser Befehl wurde in Cisco IOS-Software Version 12.1(3)T eingeführt.

Mit diesem Befehl verfolgt ein Start-/Stoppdatensatz für den Anrufaufbau und die Anruftrennung den Fortschritt der Ressourcenverbindung zum Gerät. Ein separater Start-/Stoppdatensatz für die Abrechnung zur Benutzerauthentifizierung verfolgt den Fortschritt der Benutzerverwaltung. Diese beiden Datensätze sind mit einer eindeutigen Sitzungs-ID für den Anruf verknüpft.

Zugehörige Informationen

- Technischer Support – Cisco Systems

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.