

Konfigurieren von RADIUS mit Livingston Server

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Authentifizierung](#)

[Hinzufügen von Buchhaltung](#)

[Testdateien](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument soll dem erstmaligen RADIUS-Benutzer bei der Einrichtung und beim Debuggen einer RADIUS-Konfiguration auf einem Livingston RADIUS-Server behilflich sein. Die Beschreibung der Cisco IOS® RADIUS-Funktionen ist nicht vollständig. Livingston-Dokumentation ist auf der Lucent Technologies-Website verfügbar.

Die Router-Konfiguration ist unabhängig vom verwendeten Server identisch. Cisco bietet im Handel erhältlichen RADIUS-Code in Ciscos NA, Ciscos UNIX oder Cisco Access Registrar an.

Diese Router-Konfiguration wurde auf einem Router entwickelt, auf dem die Cisco IOS Software, Version 11.3.3, ausgeführt wird. Version 12.0.5.T und höher verwendet **Gruppenradius** anstelle des **Radius**, sodass Anweisungen wie **ein Standardradius für die Authentifizierungs-Anmeldung** als **standardmäßiger Gruppenradius für die Authentifizierungsanmeldung** angezeigt werden können.

Weitere Informationen zu RADIUS-[Routerbefehlen](#) finden Sie in der Cisco IOS-Dokumentation zu den [RADIUS-Informationen](#).

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 unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Authentifizierung

Gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Sie RADIUS-Code auf dem UNIX-Server kompiliert haben. Bei den Serverkonfigurationen wird davon ausgegangen, dass Sie den Livingston RADIUS-Servercode verwenden. Die Routerkonfigurationen müssen mit anderen Servercodes verwendet werden, die Serverkonfigurationen unterscheiden sich jedoch voneinander. Der Code, radiusd, muss als root ausgeführt werden.
2. Der Livingston RADIUS-Code enthält drei Beispieldateien, die für Ihr System angepasst werden müssen: clients.beispiel, users.example und dictionary. Diese werden in der Regel im radardb-Verzeichnis gefunden. Sie können diese Dateien oder die Benutzer- und Clientdateien am Ende dieses Dokuments ändern. Alle drei Dateien müssen in einem Arbeitsverzeichnis gespeichert werden. Stellen Sie sicher, dass der RADIUS-Server mit den drei Dateien startet:

```
radiusd -x -d (directory_containing_3_files)
```

Fehler beim Start müssen auf den Bildschirm oder die Datei directory_contains_3_files_logfile ausgegeben werden. Überprüfen Sie, ob RADIUS über ein anderes Serverfenster gestartet wurde:

```
ps -aux | grep radiusd  
(or ps -ef | grep radiusd)
```

Sie sehen zwei radikale Prozesse.

3. Radius-Prozess beenden:

```
kill -9 highest_radiusd_pid
```

4. Konfigurieren Sie auf dem Konsolenport des Routers RADIUS. Wechseln Sie in den Aktivierungsmodus, und geben Sie **configure terminal** vor dem Befehlssatz ein. Diese Syntax stellt sicher, dass Sie zunächst nicht vom Router ausgeschlossen sind, da RADIUS auf dem Server nicht ausgeführt wird:

```
!--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" are !--- names of lists, and the methods listed on the same !--- lines are the methods in the order to be tried. As !--- used here, if authentication fails due to the radiusd !--- not being started, the enable password will be !--- accepted because it is in each list. aaa authentication login default radius enable aaa authentication login linmethod radius enable aaa authentication login vtymethod radius enable aaa authentication login conmethod radius enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address. radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server: radius-server key cisco line con 0 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 password whatever flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication vtymethod
```

5. Lassen Sie sich beim Einchecken über den Konsolenport am Router angemeldet, um sicherzustellen, dass Sie weiterhin über Telnet auf den Router zugreifen können, bevor Sie fortfahren. Da radiusd nicht ausgeführt wird, muss das enable-Kennwort mit jeder Benutzer-

ID akzeptiert werden. **Vorsicht:** Lassen Sie die Konsolenport-Sitzung aktiv, und bleiben Sie im Aktivierungsmodus. Stellen Sie sicher, dass für diese Sitzung keine Zeitüberschreitung auftritt. Schließen Sie sich nicht selbst ab, während Sie Konfigurationsänderungen vornehmen. Führen Sie die folgenden Befehle aus, um die Interaktion zwischen Server und Router am Router anzuzeigen:

```
terminal monitor
debug aaa authentication
```

6. Starten Sie als Root RADIUS auf dem Server:

```
radiusd -x -d (directory_containing_3_files)
```

Fehler beim Start werden auf den Bildschirm oder die Datei `directory_contains_3_files_logfile` ausgegeben. Stellen Sie sicher, dass RADIUS von einem anderen Serverfenster gestartet wurde:

```
Ps -aux | grep radiusd
(or Ps -ef | grep radiusd)
```

Sie müssen zwei radikale Prozesse sehen.

7. Telnet-Benutzer (vty) müssen sich jetzt über RADIUS authentifizieren. Beim Debuggen auf Router und Server, Schritte 5 und 6, Telnet in den Router von einem anderen Teil des Netzwerks. Der Router gibt eine Eingabeaufforderung für Benutzername und Kennwort aus, auf die Sie antworten:

```
ciscoursr (username from users file)
ciscopas (password from users file)
```

Beobachten Sie den Server und den Router, wo Sie die RADIUS-Interaktion sehen müssen, z. B. was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.

8. Wenn Sie auch möchten, dass die Benutzer über RADIUS authentifizieren, um in den Aktivierungsmodus zu wechseln, stellen Sie sicher, dass Ihre Konsolenport-Sitzung noch aktiv ist, und fügen Sie diesen Befehl zum Router hinzu.

```
!--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS not running. aaa authentication enable default radius enable
```

9. Benutzer müssen nun über RADIUS **aktiviert werden**. Wenn die Fehlerbehebung für Router und Server durchgeführt wird, führen Sie die Schritte 5 und 6 Telnet von einem anderen Teil des Netzwerks in den Router ein. Der Router muss eine Eingabeaufforderung für Benutzername und Kennwort erstellen, auf die Sie antworten:

```
ciscoursr (username from users file)
ciscopas (password from users file)
```

Wenn Sie in den Aktivierungsmodus wechseln, sendet der Router den Benutzernamen `$enable15$` und fordert ein Kennwort an, auf das Sie antworten:

```
shared
```

Beobachten Sie den Server und den Router, wo Sie die RADIUS-Interaktion sehen müssen, z. B. was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.

10. Überprüfen Sie, ob die Benutzer des Konsolenports über RADIUS authentifiziert werden, indem Sie eine Telnet-Sitzung zum Router einrichten, der über RADIUS authentifiziert werden muss. Bleiben Sie im Router- und Aktivierungsmodus, bis Sie sich über den Konsolenport beim Router anmelden, sich über den Konsolenport von der ursprünglichen Verbindung zum Router abmelden und dann wieder eine Verbindung zum Konsolenport herstellen können. Die Konsolen-Port-Authentifizierung für die Anmeldung und die Aktivierung durch die Verwendung von Benutzer-IDs und Kennwörtern in Schritt 9 muss jetzt über RADIUS erfolgen.

11. Während Sie entweder über eine Telnet-Sitzung oder den Konsolen-Port verbunden bleiben

und die Fehlerbehebung am Router und Server stattfindet, stellen Sie in den Schritten 5 und 6 eine Modemverbindung zu Leitung 1 her. Line-Benutzer müssen sich jetzt anmelden und über RADIUS aktivieren. Der Router muss eine Eingabeaufforderung für Benutzername und Kennwort erstellen, auf die Sie antworten:

```
ciscoursr (username from users file)
ciscopas (password from users file)
```

Wenn Sie in den Aktivierungsmodus wechseln, sendet der Router den Benutzernamen \$enable15\$ und fordert ein Kennwort an, auf das Sie antworten:

```
shared
```

Beobachten Sie den Server und den Router, wo Sie die RADIUS-Interaktion sehen müssen, z. B. was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.

Hinzufügen von Buchhaltung

Die Rechnungslegung ist optional.

1. Die Abrechnung findet nur nach Konfiguration im Router statt. Aktivieren Sie die Accounting-Funktion im Router wie in diesem Beispiel:

```
aaa accounting exec default start-stop radius
aaa accounting connection default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```

2. Starten Sie RADIUS auf dem Server mit der Accounting-Option:

```
Start RADIUS on the server with the accounting option:
```

3. So zeigen Sie die Interaktion zwischen Server und Router am Router an:

```
terminal monitor
debug aaa accounting
```

4. Greifen Sie auf den Router zu, während Sie die Interaktion zwischen Server und Router über das Debuggen beobachten, und überprüfen Sie dann das Accounting-Verzeichnis auf Protokolldateien.

Testdateien

Dies ist die Testdatei für Benutzer:

```
ciscoursr      Password = "ciscopas"
               User-Service-Type = Login-User,
               Login-Host = 1.2.3.4,
               Login-Service = Telnet
```

```
$enable15$    Password = "shared"
               User-Service-Type = Shell-User
```

Dies ist die Testdatei des Clients:

```
# 1.2.3.4 is the ip address of the client router and cisco is the key
1.2.3.4        cisco
```

Zugehörige Informationen

- [RADIUS \(Remote Authentication Dial-In User Service\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)