Konfigurieren eines Cisco Routers mit TACACS+-Authentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie einen Cisco Router für die Authentifizierung mit TACACS+ konfigurieren, das unter UNIX ausgeführt wird. TACACS+ bietet nicht so viele Funktionen wie das kommerziell verfügbare Cisco Secure ACS für Windows oder Cisco Secure ACS UNIX.

Die zuvor von Cisco Systems bereitgestellte TACACS+-Software wurde eingestellt und wird von Cisco Systems nicht mehr unterstützt.

Heute können Sie viele verfügbare Freeware-Versionen von TACACS+ finden, wenn Sie in Ihrer Internet-Suchmaschine nach "TACACS+ Freeware" suchen. Cisco empfiehlt keine spezielle Implementierung von TACACS+-Freeware.

Der Cisco Secure Access Control Server (ACS) kann über reguläre Vertriebs- und Vertriebskanäle von Cisco weltweit erworben werden. Cisco Secure ACS für Windows umfasst alle erforderlichen Komponenten für eine unabhängige Installation auf einer Microsoft Windows-Workstation. Die Cisco Secure ACS Solution Engine wird mit einer vorinstallierten Cisco Secure ACS-Softwarelizenz geliefert. Besuchen Sie die Cisco Bestellseite (nur registrierte Kunden), um eine Bestellung aufzugeben.

Hinweis: Sie benötigen ein CCO-Konto mit einem zugehörigen Servicevertrag, um die 90-Tage-Testversion für Cisco Secure ACS für Windows zu erhalten.

Die Router-Konfiguration in diesem Dokument wurde auf einem Router entwickelt, auf dem die Cisco IOS® Software, Version 11.3.3, ausgeführt wird. Cisco IOS Software Release 12.0.5.T und höher verwenden **Gruppentakacs+** anstelle von **tacacs+**, sodass Anweisungen wie **aaa authentication login default tacacs+ aktiviert** als **aaaa authentication login default group tacacs+**

enable erscheinen.

Weitere vollständige Informationen zu Routerbefehlen finden Sie in der Cisco IOS Software-Dokumentation.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco IOS Software-Version 11.3.3 und der Cisco IOS-Softwareversion 12.0.5.T und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

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 TACACS+ (TAC+)-Code auf dem UNIX-Server kompiliert haben.Bei den Serverkonfigurationen wird davon ausgegangen, dass Sie den Cisco TAC+-Servercode verwenden. Die Routerkonfigurationen sollten unabhängig davon funktionieren, ob der Servercode Cisco Server-Code ist. TAC+ muss als Root ausgeführt werden. su auf root, wenn nötig.
2. Kopieren Sie die test_file am Ende dieses Dokuments, platzieren Sie sie auf dem TAC+-Server, und nennen Sie sie **test_file**.Stellen Sie sicher, dass der **tac_plus_ausführbare** Daemon mit **test_file** beginnt. In diesem Befehl überprüft die **-P-**Option die Kompilierungsfehler, startet jedoch den Daemon nicht:
   ```
   tac_plus_executable -P -C test_file
   ```
   Möglicherweise sehen Sie den Inhalt von test_file, scrollen Sie das Fenster nach unten, aber Sie sollten keine Meldungen wie `Datei nicht finden können`, `Klartext erwartet - gefundener Klartext` oder `unerwarteter Aufstrich`. Wenn Fehler auftreten, überprüfen Sie die Pfade zu test_file, überprüfen Sie die Eingabe erneut, und testen Sie erneut, bevor Sie fortfahren.
3. Konfigurieren Sie TAC+ auf dem Router.Wechseln Sie **in den Aktivierungsmodus**, und geben Sie **configure terminal** vor dem Befehlssatz ein. Diese Befehlssyntax stellt sicher, dass Sie anfangs nicht vom Router ausgeschlossen sind, sofern die **ausführbare Datei "tac_plus_**nicht ausgeführt wird:

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of
authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---
tac_plus_executable not being started, the !--- enable password is accepted because !--- it
is in each list.

   !
   aaa authentication login linmethod tacacs+ enable
   aaa authentication login vtymethod tacacs+ enable
   aaa authentication login conmethod tacacs+ enable
   !
   !--- Point the router to the server, where #.#.#.# !--- is the server IP address. !
tacacs-server host #.#.#.# 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
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
```

4. Stellen Sie sicher, dass Sie weiterhin über Telnet und den Konsolenport auf den Router zugreifen können, bevor Sie fortfahren. Da die **tac_plus_ausführbare Datei** nicht ausgeführt wird, sollte das **enable-**Kennwort akzeptiert werden.**Hinweis:** Lassen Sie die Konsolenport-Sitzung aktiv, und bleiben Sie im Aktivierungsmodus. Diese Sitzung sollte nicht abgebrochen werden. Der Zugriff auf den Router ist zu diesem Zeitpunkt beschränkt. Sie müssen Konfigurationsänderungen vornehmen können, ohne sich selbst zu sperren.Führen Sie die folgenden Befehle aus, um die Interaktion zwischen Server und Router am Router anzuzeigen:
   ```
   terminal monitor
     debug aaa authentication
   ```
5. Starten Sie als Root TAC+ auf dem Server:
   ```
   tac_plus_executable -C test_file -d 16
   ```
6. Stellen Sie sicher, dass TAC+ gestartet wurde:
   ```
   ps -aux | grep tac_plus_executable
   ```
   oder
   ```
   ps -ef | grep tac_plus_executable
   ```
   Wenn TAC+ nicht startet, ist es normalerweise ein Problem mit der Syntax in der test_file. Kehren Sie zu Schritt 1 zurück, um dies zu korrigieren.
7. Geben Sie **tail -f /var/tmp/tac_plus.log** ein, um die Router-zu-Server-Interaktion auf dem Server anzuzeigen.**Hinweis:** Die `-d 16`-Option in Schritt 5 sendet die Ausgabe aller Transaktionen an /var/tmp/tac_plus.log.
8. Telnet-Benutzer (VTY) müssen sich jetzt über TAC+ authentifizieren.Wenn die Fehlersuche am Router und am Server (Schritte 4 und 7) durchgeführt wird, Telnet von einem anderen Teil des Netzwerks in den Router eindringen.Der Router gibt eine Eingabeaufforderung für Benutzername und Kennwort aus, auf die Sie antworten:
   ```
   'authenuser'   (username from test_file)
   'admin'   (password from test_file)
   ```
   Der Benutzer `authenuser` befindet sich in der Gruppe `admin`, die über das Kennwort `admin` verfügt.Beobachten Sie den Server und den Router, wo Sie die TAC+-Interaktion sehen können - das, was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.
9. Wenn Sie auch möchten, dass sich Ihre Benutzer über TAC+ 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 TAC+ !--- then enable password if TAC+ does
```

```
not run. aaa authentication enable default tacacs+ enable
```

Benutzer müssen jetzt über TAC+ aktivieren.

10. Wenn die Fehlersuche am Router und am Server (Schritte 4 und 7) durchgeführt wird, Telnet von einem anderen Teil des Netzwerks in den Router eindringen. Der Router gibt eine Eingabeaufforderung für Benutzername und Kennwort aus, auf die Sie antworten:

    ```
    'authenuser'   (username from test_file)
    'admin'   (password from test_file)
    ```

    Wenn Sie in den Aktivierungsmodus wechseln, fordert der Router ein Kennwort an, auf das Sie antworten:

    ```
    'cisco'  ($enable$ password from test_file)
    ```

    Beobachten Sie den Server und den Router, wo Sie die TAC+-Interaktion sehen sollten - was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.
11. Schalten Sie den TAC+-Prozess auf dem Server aus, während Sie weiterhin mit dem Konsolenport verbunden sind, um sicherzustellen, dass Ihre Benutzer weiterhin auf den Router zugreifen können, wenn das TAC+ nicht verfügbar ist:

    ```
    ps -aux | grep tac_plus_executable
    ```

    oder

    ```
    ps -ef | grep tac_plus_executable)
      kill -9 pid_of_tac_plus_executable
    ```

    Wiederholen Sie das Telnet, und aktivieren Sie den vorherigen Schritt. Der Router erkennt dann, dass der TAC+-Prozess nicht reagiert, und ermöglicht es Benutzern, sich anzumelden und mit den Standardkennwörtern zu aktivieren.
12. Überprüfen Sie, ob Ihre Konsolenport-Benutzer über TAC+ authentifiziert wurden. Rufen Sie dazu den TAC+-Server (Schritte 5 und 6) erneut auf, und richten Sie eine Telnet-Sitzung zum Router ein (die sich über TAC+ authentifizieren sollte).Bleiben Sie über Telnet mit dem Router im Aktivierungsmodus verbunden, bis Sie sich über den Konsolenport sicher beim Router anmelden können.Melden Sie sich über den Konsolenport von der ursprünglichen Verbindung zum Router ab, und stellen Sie dann wieder eine Verbindung zum Konsolenport her. Die Konsolenport-Authentifizierung zur Anmeldung und Aktivierung mithilfe von Benutzer-IDs und Kennwörtern (siehe Schritt 10) sollte jetzt über TAC+ erfolgen.
13. Während Sie entweder über eine Telnet-Sitzung oder den Konsolen-Port verbunden bleiben und die Fehlerbehebung am Router und Server (Schritte 4 und 7) ausgeführt wird, stellen Sie eine Modemverbindung zu Leitung 1 her.Line-Benutzer müssen sich jetzt anmelden und über TAC+ aktivieren.Der Router gibt eine Eingabeaufforderung für Benutzername und Kennwort aus, auf die Sie antworten:

    ```
    'authenuser'   (username from test_file)
    'admin'   (password from test_file)
    ```

    Wenn Sie in den Aktivierungsmodus wechseln, fordert der Router ein Kennwort an.Antwort:

    ```
    'cisco'   ($enable$ password from test_file)
    ```

    Beobachten Sie den Server und den Router, wo Sie die TAC+-Interaktion sehen - was wo, Antworten, Anfragen usw. gesendet wird. Korrigieren Sie alle Probleme, bevor Sie fortfahren.Benutzer müssen jetzt über TAC+ aktivieren.

Autorisierung hinzufügen

Das Hinzufügen einer Autorisierung ist optional.

Standardmäßig gibt es drei Befehlsstufen auf dem Router:

- Berechtigungsstufe 0, einschließlich Deaktivierung, Aktivierung, Beenden, Hilfe und Abmelden
- Berechtigungsstufe 1 - Normalstufe auf einem Telnet - Eingabeaufforderung sagt `Router>`
- Berechtigungsstufe 15 - Aktivierungsstufe - Eingabeaufforderung sagt `Router#`

Da die verfügbaren Befehle vom IOS-Feature-Set, der Version von Cisco IOS, dem Router-Modell usw. abhängen, gibt es keine umfassende Liste aller Befehle der Ebenen 1 und 15. **show ipx route** ist beispielsweise nicht in einem nur IP-basierten Feature-Set vorhanden, **show ip nat trans** ist nicht in Cisco IOS Software Release 10.2.x enthalten, da NAT zu diesem Zeitpunkt nicht eingeführt wurde und **show environment** in Routermodellen ohne Stromversorgung und Temperaturüberwachung nicht vorhanden ist. Befehle, die auf einer bestimmten Ebene auf einem bestimmten Router verfügbar sind, können bei der Eingabe eines Befehls gefunden werden**?** an der Eingabeaufforderung im Router, wenn auf dieser Berechtigungsebene.

Die Konsolenport-Autorisierung wurde erst als Funktion hinzugefügt, wenn die Cisco Bug-ID CSCdi82030 (nur registrierte Kunden) implementiert wurde. Die Konsolen-Port-Autorisierung ist standardmäßig deaktiviert, um die Wahrscheinlichkeit zu verringern, dass Sie versehentlich vom Router ausgeschlossen werden. Wenn ein Benutzer über die Konsole physischen Zugriff auf den Router hat, ist die Konsolenport-Autorisierung nicht sehr effektiv. Die Konsolen-Port-Autorisierung kann jedoch unter Zeile `con 0` aktiviert werden, und zwar in dem Bild, dass die Cisco Bug-ID CSCdi82030 (nur registrierte Kunden) mit dem folgenden Befehl implementiert wurde:

```
authorization exec default|WORD
```

1. Der Router kann so konfiguriert werden, dass Befehle über TAC+ auf allen oder einigen Ebenen autorisiert werden.Diese Router-Konfiguration ermöglicht es allen Benutzern, eine Berechtigung für jeden Befehl auf dem Server einzurichten. Hier autorisieren wir alle Befehle über TAC+, aber wenn der Server ausgefallen ist, ist keine Autorisierung erforderlich.
   ```
   aaa authorization commands 1 default tacacs+ none
     aaa authorization commands 15 default tacacs+ none
   ```
2. Während der TAC+-Server ausgeführt wird, Telnet mit Benutzer-ID **authenuser**.Da authenuser in test_file über den Standardwert service = permit verfügt, sollte dieser Benutzer in der Lage sein, alle Funktionen auszuführen.Wechseln Sie im Router in den **Aktivierungsmodus**, und aktivieren Sie das Autorisierungsdebuggen:
   ```
   terminal monitor
     debug aaa authorization
   ```
3. Telnet mit Benutzer-ID-**Autorisierer** und Kennwort-**Operator in den** Router.Dieser Benutzer kann die beiden show-Befehle **traceroute** und **Logout** nicht ausführen (siehe test_file).Beobachten Sie den Server und den Router, wo Sie die TAC+-Interaktion sehen sollten (was wo, Antworten, Anfragen usw. gesendet wird). Korrigieren Sie alle Probleme, bevor Sie fortfahren.
4. Wenn Sie einen Benutzer für einen automatischen Befehl konfigurieren möchten, entfernen Sie den ausgehenden Benutzertransient in der test_file, und setzen Sie ein gültiges IP-Adressziel anstelle des #.#.#.#.#.#.Beenden und starten Sie den TAC+ Server.Auf dem Router:
   ```
   aaa authorization exec default tacacs+
   ```
   Telnet zum Router mit **transienten** Benutzerdaten und **transienten** Kennwörtern. Die **Telnet #.#.#.#** wird ausgeführt, und der Benutzer transient wird an den anderen Standort gesendet.

Accounting hinzufügen

Die Rechnungslegung ist optional.

Der Verweis auf die Accounting-Datei befindet sich in test_file - accounting file = /var/log/tac.log. Die Abrechnung erfolgt jedoch nur, wenn sie im Router konfiguriert wurde (vorausgesetzt, der Router führt eine Version der Cisco IOS-Software später als 11.0 aus).

1. Aktivieren Sie Accounting im Router:
   ```
   aaa accounting exec default start-stop tacacs+
     aaa accounting connection default start-stop tacacs+
     aaa accounting network default start-stop tacacs+
     aaa accounting system default start-stop tacacs+
   ```
   Hinweis: Bei einigen Versionen erfolgt die AAA-Abrechnung nicht auf Befehlsebene. Eine Problemumgehung besteht in der Verwendung der Befehlsautorisierung und der Protokollierung des Vorfalls in der Accounting-Datei. (Siehe Cisco Bug ID CSCdi44140.) Wenn Sie ein Bild verwenden, in dem dieses feste System verwendet wird [Cisco IOS Software Releases 11.2(1.3)F, 11.2(1.2), 11.1(6.3), 11.1(6.3)AA01, 11.1(6.3)CA, können Sie ab dem 24. September 1997 auch "enable-CA" Buchführung.
2. Wenn TAC+ auf dem Server ausgeführt wird, geben Sie den folgenden Befehl auf dem Server ein, um die Einträge anzuzeigen, die in die Abrechnungsdatei gehen:
   ```
   tail -f /var/log/tac.log
   ```
   Melden Sie sich dann beim und vom Router, Telnet vom Router usw. an. Geben Sie ggf. auf dem Router Folgendes ein:
   ```
   terminal monitor
     debug aaa accounting
   ```

Testdatei

```
- - - - - - - (cut here) - - - - - - -

# Set up accounting file if enabling accounting on NAS
accounting file = /var/log/tac.log

# Enable password setup for everyone:
user = $enable$ {
        login = cleartext "cisco"
        }

# Group listings must be first:
group = admin {
# Users in group 'admin' have cleartext password
        login = cleartext "admin"
        expires = "Dec 31 1999"
}

group = operators {
# Users in group 'operators' have cleartext password
        login = cleartext "operator"
        expires = "Dec 31 1999"
}

group = transients {
# Users in group 'transient' have cleartext password
        login = cleartext "transient"
        expires = "Dec 31 1999"
}

# This user is a member of group 'admin' & uses that group's password to log in.
#  The $enable$ password is used to enter enable mode.  The user can perform all commands.
 user = authenuser {
```

```
        default service = permit
        member = admin
        }

# This user is limitted in allowed commands when aaa authorization is enabled:
 user = telnet {
        login = cleartext "telnet"
        cmd = telnet {
        permit .*
        }
        cmd = logout {
        permit .*
        }
        }

# user = transient {
#       member = transients
#       service = exec {
        # When transient logs on to the NAS, he's immediately
        # zipped to another site
#       autocmd = "telnet #.#.#.#"
#       }
#       }

# This user is a member of group 'operators'
# & uses that group's password to log in
 user = authenuser {
        member = operators
# Since this user does not have 'default service = permit' when command
# authorization through TACACS+ is on at the router, this user's commands
# are limited to:
        cmd = show {
        permit ver
        permit ip
        }
        cmd = traceroute {
        permit .*
        }
        cmd = logout {
        permit .*
        }
}
- - - - (end cut here) - - - -
```

Hinweis: Diese Fehlermeldung wird generiert, wenn Ihr TACACS-Server nicht erreichbar ist: `%AAAA-3-DROPACCTSNDFAIL: Abrechnungsdatensatz verloren,Senden an Server fehlgeschlagen: Systemstart.` Überprüfen Sie, ob der TACACS+-Server betriebsbereit ist.

Zugehörige Informationen

- TACACS+ für die Sicherheit des Netzwerkzugriffs für einen Benutzer
- Terminal Access Controller Access Control System (TACACS+)
- Cisco Secure Access Control Server für Windows
- Technischer Support und Dokumentation - Cisco Systems