Cisco IOS-Router: Konfigurationsbeispiel für HTTP-Verbindungen: Lokale, TACACS+- und RADIUS-Authentifizierung

Inhalt

Einführung

Dieses Dokument zeigt, wie die lokale, TACACS+- und RADIUS-Authentifizierung der HTTP-Verbindung konfiguriert wird. Einige relevante Debugbefehle werden ebenfalls bereitgestellt.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und

Hardwareversionen.

- Cisco IOS® Software-Versionen 11.2 oder höher
- Hardware, die diese Softwareänderungen unterstützt

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Hintergrundtheorie

In der Cisco IOS® Softwareversion 11.2 wurde eine Funktion zum Verwalten des Routers über HTTP hinzugefügt. Der Abschnitt "Befehle des Cisco IOS-Webbrowsers" in der Befehlsreferenz zu den Cisco IOS-Konfigurationsgrundlagen enthält folgende Informationen zu dieser Funktion.

"Mit dem Befehl **ip http authentication** können Sie eine bestimmte Authentifizierungsmethode für HTTP-Serverbenutzer angeben. Der HTTP-Server verwendet die Methode enable password, um einen Benutzer auf der Berechtigungsebene 15 zu authentifizieren. Mit dem Befehl **ip http authentication** können Sie jetzt die HTTP-Serverbenutzerauthentifizierung "enable", "local", "TACACS" oder "Authentication, Authorization, Accounting (AAA) angeben."

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

In diesem Dokument werden die unten angegebenen Konfigurationen verwendet.

- Konfigurieren der lokalen Authentifizierung für HTTP-Serverbenutzer
- Konfigurieren der TACACS+-Authentifizierung für HTTP-Serverbenutzer
- Konfigurieren der RADIUS-Authentifizierung für HTTP-Serverbenutzer

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Konfigurieren der lokalen Authentifizierung für HTTP-Serverbenutzer

- Router-Konfigurationen
- Benutzerergebnisse

Router-Konfigurationen

Lokale Authentifizierung mit Cisco IOS Software Version 11.2
`!--- This is the part of the configuration related to local authentication. ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three password three username four privilege 7 password four`

```
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

Lokale Authentifizierung mit Cisco IOS Software Releases 11.3.3.T oder höher

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Benutzerergebnisse

Diese Ergebnisse gelten für die Benutzer in den vorherigen Routerkonfigurationen.

- **Benutzer 1**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.# eingegeben wird.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer wird nach der Anmeldung aktiviert (die **Berechtigung show** lautet 15).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.
- **Benutzer 3**Der Benutzer kann die Webautorisierung nicht durchführen, da er über keine Berechtigungsebene verfügt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer befindet sich nach der Anmeldung im nicht aktivierten Modus (die **Berechtigung "show"** lautet 1).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.
- **Benutzer 4**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.#/level/7/exec eingegeben wird.Es werden Befehle der Stufe 1 plus der Befehl **clear line** der Stufe 7 angezeigt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Benutzer befindet sich nach der Anmeldung auf der Berechtigungsebene 7 (**Berechtigung anzeigen** ist 7).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.

Konfigurieren der TACACS+-Authentifizierung für HTTP-Serverbenutzer

Router-Konfigurationen

Authentifizierung mit Cisco IOS Software Version 11.2

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Authentifizierung mit Cisco IOS Software-Versionen 11.3.3.T bis 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Authentifizierung mit Cisco IOS Software-Versionen 12.0.5.T und höher

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Benutzerergebnisse

Die folgenden Ergebnisse gelten für die Benutzer in den unten stehenden Serverkonfigurationen.

- **Benutzer 1**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.# eingegeben wird.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer wird nach der Anmeldung aktiviert (die **Berechtigung show** lautet 15).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.
- **Benutzer 2**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.# eingegeben wird.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer wird nach der Anmeldung aktiviert (die **Berechtigung show** lautet 15).Wenn dem Router eine Befehlsautorisierung hinzugefügt wird, schlägt der Benutzer alle Befehle fehl, da die Serverkonfiguration sie nicht autorisiert.
- **Benutzer 3**Der Benutzer kann die Webautorisierung nicht durchführen, da er über keine Berechtigungsebene verfügt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer befindet

sich nach der Anmeldung im nicht aktivierten Modus (die **Berechtigung "show"** lautet 1).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.

- **Benutzer 4**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.#/level/7/exec eingegeben wird.Es werden Befehle der Stufe 1 plus der Befehl **clear line** der Stufe 7 angezeigt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Benutzer befindet sich nach der Anmeldung auf der Berechtigungsebene 7 (**Berechtigung anzeigen** ist 7).Wenn dem Router die Befehlsautorisierung hinzugefügt wird, ist der Benutzer bei allen Befehlen weiterhin erfolgreich.

Konfiguration des Freeware Daemon-Servers

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Cisco Secure ACS für UNIX-Serverkonfiguration

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
```

```
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

[Cisco Secure ACS für die Konfiguration von Windows-Servern]

Benutzer 1 in Gruppe 1

- GruppeneinstellungenCheck **Shell (Exec)**.Aktivieren Sie **privilege level=15**.Aktivieren Sie **Standarddienste (nicht definierte Dienste)**.**Hinweis:** Wenn diese Option nicht angezeigt wird, gehen Sie zu **Schnittstellenkonfiguration**, wählen Sie **TACACS+** und anschließend **Erweiterte Konfigurationsoptionen**. Wählen Sie **Display enable default (undefined) service** configuration aus.
- BenutzereinstellungenKennwort der Datenbank, Geben Sie das Kennwort ein, und bestätigen Sie es im oberen Bereich.

Benutzer 2 in Gruppe 2

- GruppeneinstellungenCheck **Shell (Exec)**.Aktivieren Sie **privilege level=15**.Aktivieren Sie keine **Standarddienste (nicht definierte Dienste)**.
- BenutzereinstellungenKennwort der Datenbank, Geben Sie das Kennwort ein, und bestätigen Sie es im oberen Bereich.

Benutzer 3 in Gruppe 3

- GruppeneinstellungenCheck **Shell (Exec)**.Lassen Sie **die Berechtigungsebene** leer.Aktivieren Sie **Standarddienste (nicht definierte Dienste)**.**Hinweis:** Wenn diese Option nicht angezeigt wird, gehen Sie zu **Schnittstellenkonfiguration**, wählen Sie **TACACS+** und anschließend **Erweiterte Konfigurationsoptionen**. Wählen Sie **Display enable default (undefined) service** configuration aus.
- BenutzereinstellungenKennwort der Datenbank, Geben Sie das Kennwort ein, und bestätigen Sie es im oberen Bereich.

Benutzer 4 in Gruppe 4

- GruppeneinstellungenCheck **Shell (Exec)**.Aktivieren Sie **privilege level=7**.Aktivieren Sie **Standarddienste (nicht definierte Dienste)**.**Hinweis:** Wenn diese Option nicht angezeigt wird, gehen Sie zu **Schnittstellenkonfiguration**, wählen Sie **TACACS+** und anschließend **Erweiterte Konfigurationsoptionen**. Wählen Sie **Display enable default (undefined) service** configuration aus.
- BenutzereinstellungenKennwort der Datenbank, Geben Sie das Kennwort ein, und bestätigen Sie es im oberen Bereich.

Konfigurieren der RADIUS-Authentifizierung für HTTP-Serverbenutzer

Router-Konfigurationen

Authentifizierung mit Cisco IOS Software Version 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Authentifizierung mit Cisco IOS Software-Versionen 11.3.3.T bis 12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Authentifizierung mit Cisco IOS Software-Versionen 12.0.5.T und höher

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Benutzerergebnisse

Die folgenden Ergebnisse gelten für die Benutzer in den unten stehenden Serverkonfigurationen.

- **Benutzer 1**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.# eingegeben wird.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer wird nach der Anmeldung aktiviert (die **Berechtigung show** lautet 15).
- **Benutzer 3**Der Benutzer kann die Webautorisierung nicht durchführen, da er über keine Berechtigungsebene verfügt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Der Benutzer befindet sich nach der Anmeldung im nicht aktivierten Modus (die **Berechtigung "show"** lautet 1).
- **Benutzer 4**Der Benutzer übergibt die Webautorisierung, wenn die URL als http://#.#.#.#/level/7/exec eingegeben wird.Es werden Befehle der Stufe 1 plus der Befehl **clear line** der Stufe 7 angezeigt.Nach der Verbindung von Telnet mit dem Router kann der Benutzer alle Befehle nach der Anmeldeauthentifizierung ausführen.Benutzer befindet sich nach der Anmeldung auf der Berechtigungsebene 7 (**Berechtigung anzeigen** ist 7).

RADIUS-Konfiguration auf Server, die Cisco AV-Paare unterstützt

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Cisco Secure ACS für UNIX-Serverkonfiguration

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
```

```
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Cisco Secure ACS für die Konfiguration von Windows-Servern

- Benutzer = ein, Servicetyp (Attribut 6) = Verwaltung
- Benutzer = drei, Servicetyp (Attribut 6) = Anmeldung
- Benutzer = vier, Servicetyp (Attribut 6) = Anmeldung, aktivieren Sie das Kontrollkästchen Cisco AV-Paare, und geben Sie shell:priv-lvl=7 ein.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Die folgenden Befehle sind für das Debuggen der HTTP-Authentifizierung hilfreich. Sie werden auf dem Router ausgegeben.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **Terminalmonitor** - Zeigt Ausgaben für Debug-Befehle und Systemfehlermeldungen für das aktuelle Terminal und die aktuelle Sitzung an.
- **debug aaa authentication**: Zeigt Informationen zur AAA/TACACS+-Authentifizierung an.
- **debug aaa autorization** - Zeigt Informationen zur AAA/TACACS+-Autorisierung an.
- **Debugradius** - Zeigt detaillierte Debuginformationen an, die RADIUS zugeordnet sind.
- **debug tacacs** - Zeigt Informationen an, die TACACS zugeordnet sind.

- **debug ip http authentication** - Verwenden Sie diesen Befehl, um HTTP-Authentifizierungsprobleme zu beheben. Zeigt die Authentifizierungsmethode an, mit der der Router versucht hat, und authentifizierungsspezifische Statusmeldungen.

Zugehörige Informationen

- Support-Seite für Cisco TACACS+-Zugriffssoftware
- RADIUS-Support-Seite
- Support-Seite für Cisco Secure ACS für Windows
- Support-Seite für Cisco Secure ACS für UNIX
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems