Beheben von TACACS-Authentifizierungsproblemen

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Behebung von TACACS-Authentifizierungsproblemen bei Cisco IOS®/Cisco IOS-XE-Routern und -Switches beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in diesen Themen verfügen:

- Konfiguration der Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA) auf Cisco Geräten
- TACACS-Konfiguration

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 kennen.

Funktionsweise von TACACS

Das TACACS+-Protokoll verwendet das Transmission Control Protocol (TCP) als Transportprotokoll mit der Zielportnummer 49. Wenn der Router eine Anmeldeanforderung empfängt, stellt er eine TCP-Verbindung mit dem TACACS-Server her, wobei dem Benutzer eine Aufforderung zur Eingabe des Benutzernamens angezeigt wird. Wenn der Benutzer den Benutzernamen eingibt, kommuniziert der Router erneut mit dem TACACS-Server, um die Kennwortaufforderung zu erhalten. Sobald der Benutzer das Kennwort eingegeben hat, sendet der Router diese Informationen erneut an den TACACS-Server. Der TACACS-Server überprüft die Anmeldeinformationen des Benutzers und sendet eine Antwort an den Router zurück. Das Ergebnis einer AAA-Sitzung kann wie folgt aussehen:

PASS: Wenn Sie authentifiziert sind, beginnt der Dienst nur, wenn auf dem Router eine AAA-Autorisierung

konfiguriert ist. Zu diesem Zeitpunkt beginnt die Autorisierungsphase.

FEHLER: Wenn Sie die Authentifizierung nicht bestanden haben, können Sie weiteren Zugriff verweigern oder aufgefordert werden, die Anmeldesequenz erneut zu versuchen. Das hängt vom TACACS+-Daemon ab. Auf diese Weise können Sie die für den Benutzer im TACACS-Server konfigurierten Richtlinien überprüfen, wenn Sie vom Server ein FAIL erhalten.

FEHLER: Dies weist auf einen Fehler bei der Authentifizierung hin. Dies kann entweder am Daemon oder in der Netzwerkverbindung zwischen dem Daemon und dem Router erfolgen. Wenn eine ERROR-Antwort empfangen wird, versucht der Router in der Regel, den Benutzer auf eine alternative Methode zu authentifizieren.

Dies ist die grundlegende Konfiguration von AAA und TACACS auf einem Cisco Router.

```
aaa new-model

aaa authentication log in default group tacacs+ local

aaa authorization exec default group tacacs+ local

!

tacacs server prod

address ipv4 10.106.60.182

key cisco123

!

ip tacacs source-interface Gig 0/0
```

Fehlerbehebung bei TACACS-Problemen

Schritt 1:

Überprüfen Sie die Verbindung zum TACACS-Server mit einem Telnet auf Port 49 vom Router mit der entsprechenden Quellschnittstelle. Falls der Router keine Verbindung zum TACACS-Server an Port 49 herstellen kann, kann es eine Firewall oder eine Zugriffsliste geben, die den Datenverkehr blockiert.

```
Router#telnet 10.106.60.182 49
Trying 10.106.60.182, 49 ... Open
```

Schritt 2:

Vergewissern Sie sich, dass der AAA-Client auf dem TACACS-Server ordnungsgemäß mit der richtigen IP-Adresse und dem gemeinsamen geheimen Schlüssel konfiguriert ist. Wenn der Router über mehrere ausgehende Schnittstellen verfügt, wird empfohlen, die TACACS-Quellschnittstelle mit diesem Befehl zu konfigurieren. Sie können die Schnittstelle, deren IP-Adresse auf dem TACACS-Server als Client-IP-Adresse konfiguriert ist, als TACACS-Quellschnittstelle auf dem Router konfigurieren.

```
Router(config)#ip tacacs source-interface Gig 0/0
```

Schritt 3:

Überprüfen Sie, ob sich die TACACS-Quellschnittstelle in einer Virtual Routing and Forwarding (VRF) befindet. Falls sich die Schnittstelle auf einer VRF-Instanz befindet, können Sie die VRF-Informationen unter der AAA-Servergruppe konfigurieren. Informationen zur Konfiguration von VRF-kompatiblen TACACS finden Sie im TACACS-Konfigurationsleitfaden.

Schritt 4:

Test aaa durchführen und überprüfen, ob wir die richtige Antwort vom Server erhalten

```
Router#test aaa  group tacacs+ cisco cisco legacy
Sending password
User successfully authenticated
```

Schritt 5:

Wenn Test aaa fehlschlägt, aktivieren Sie diese Debugs zusammen, um die Transaktionen zwischen dem Router und dem TACACS-Server zu analysieren und die Ursache zu identifizieren.

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

Dies ist eine Beispielausgabe für das Debuggen in einem Arbeitsszenario:

```
*Apr  6 13:32:50.462: AAA/BIND(00000054): Bind i/f
*Apr  6 13:32:50.462: AAA/AUTHEN/LOGIN (00000054): Pick method list 'default'
*Apr  6 13:32:50.462: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:50.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:50.462: TPLUS: processing authentication start request id 84
*Apr  6 13:32:50.462: TPLUS: Authentication start packet created for 84()
*Apr  6 13:32:50.462: TPLUS: Using server 10.106.60.182
*Apr  6 13:32:50.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:50.466: TPLUS(00000054)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 43 bytes data)
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:50.466: TPLUS(00000054)/0/READ: read entire 55 bytes response
```

```
*Apr  6 13:32:50.466: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:50.466: TPLUS: Received authen response status GET_USER (7)
*Apr  6 13:32:53.242: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:53.242: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:53.242: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:53.242: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE/10882BBC: Started 5 sec timeout
*Apr  6 13:32:53.242: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:53.246: TPLUS(00000054)/0/READ: read entire 28 bytes response
*Apr  6 13:32:53.246: TPLUS(00000054)/0/10882BBC: Processing the reply packet
*Apr  6 13:32:53.246: TPLUS: Received authen response status GET_PASSWORD (8)
*Apr  6 13:32:54.454: TPLUS: Queuing AAA Authentication request 84 for processing
*Apr  6 13:32:54.454: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:54.454: TPLUS: processing authentication continue request id 84
*Apr  6 13:32:54.454: TPLUS: Authentication continue packet generated for 84
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE/2432818: Started 5 sec timeout
*Apr  6 13:32:54.454: TPLUS(00000054)/0/WRITE: wrote entire 22 bytes request
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.458: TPLUS(00000054)/0/READ: read entire 18 bytes response
*Apr  6 13:32:54.458: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.458: TPLUS: Received authen response status PASS (2)
*Apr  6 13:32:54.462: AAA/AUTHOR (0x54): Pick method list 'default'
*Apr  6 13:32:54.462: TPLUS: Queuing AAA Authorization request 84 for processing
*Apr  6 13:32:54.462: TPLUS(00000054) log in timer started 1020 sec timeout
*Apr  6 13:32:54.462: TPLUS: processing authorization request id 84
*Apr  6 13:32:54.462: TPLUS: Protocol set to None .....Skipping
*Apr  6 13:32:54.462: TPLUS: Sending AV service=shell
*Apr  6 13:32:54.462: TPLUS: Sending AV cmd*
*Apr  6 13:32:54.462: TPLUS: Authorization request created for 84(cisco)
*Apr  6 13:32:54.462: TPLUS: using previously set server 10.106.60.182 from group tacacs+
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT/2432818: Started 5 sec timeout
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: socket event 2
*Apr  6 13:32:54.462: TPLUS(00000054)/0/NB_WAIT: wrote entire 62 bytes request
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.462: TPLUS(00000054)/0/READ: Would block while reading
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 12 header bytes (expect 18 bytes data)
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: socket event 1
*Apr  6 13:32:54.470: TPLUS(00000054)/0/READ: read entire 30 bytes response
*Apr  6 13:32:54.470: TPLUS(00000054)/0/2432818: Processing the reply packet
*Apr  6 13:32:54.470: TPLUS: Processed AV priv-lvl=15
*Apr  6 13:32:54.470: TPLUS: received authorization response for 84: PASS
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV cmd=
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): processing AV priv-lvl=15
*Apr  6 13:32:54.470: AAA/AUTHOR/EXEC(00000054): Authorization successful
```

Dies ist ein Beispiel für eine Debugausgabe vom Router, wenn der TACACS-Server mit einem falschen vorinstallierten Schlüssel konfiguriert wurde.

```
*Apr  6 13:35:07.826: AAA/BIND(00000055): Bind i/f
*Apr  6 13:35:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*Apr  6 13:35:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*Apr  6 13:35:07.826: TPLUS(00000055) log in timer started 1020 sec timeout
```

```
*Apr  6 13:35:07.826: TPLUS: processing authentication start request id 85
*Apr  6 13:35:07.826: TPLUS: Authentication start packet created for 85()
*Apr  6 13:35:07.826: TPLUS: Using server 10.106.60.182
*Apr  6 13:35:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*Apr  6 13:35:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.830: TPLUS(00000055)/0/READ: Would block while reading
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: socket event 1
*Apr  6 13:35:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*Apr  6 13:35:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*Apr  6 13:35:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*Apr  6 13:35:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

Zugehörige Informationen

- TACACS-Konfiguration auf Cisco IOS
- Technischer Support und Dokumentation für Cisco Systeme

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.