TACACS 인증 문제 해결

목차

소개

이 문서에서는 Cisco IOS®/Cisco IOS-XE 라우터 및 스위치에서 TACACS 인증 문제를 해결하는 단계를 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 기본 지식을 갖춘 것을 권장합니다.

- Cisco 디바이스의 AAA(Authentication, Authorization and Accounting) 컨피그레이션
- TACACS 컨피그레이션

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

TACACS 작동 방식

TACACS+ 프로토콜은 TCP(Transmission Control Protocol)를 목적지 포트 번호 49의 전송 프로토콜로 사용합니다. 라우터가 로그인 요청을 수신하면 TACACS 서버와의 TCP 연결을 설정하고, 여기에 사용자 이름 프롬프트가 표시됩니다. 사용자가 사용자 이름을 입력하면 라우터는 비밀번호 프롬프트를 위해 TACACS 서버와 다시 통신합니다. 사용자가 비밀번호를 입력하면 라우터는 이 정보를 TACACS 서버에 다시 전송합니다. TACACS 서버는 사용자 자격 증명을 확인하고 응답을 라우터로 다시 전송합니다. AAA 세션의 결과는 다음 중 하나일 수 있습니다.

PASS: 인증되면 라우터에 AAA 권한 부여가 구성된 경우에만 서비스가 시작됩니다. 이 시점에서 권

한 부여 단계가 시작됩니다.

FAIL: 인증에 실패한 경우 추가 액세스가 거부되거나 로그인을 다시 시도하라는 메시지가 표시될 수 있습니다. TACACS+ 데몬에 따라 달라집니다. 이 단계에서는 서버에서 FAIL을 수신하는 경우 TACACS 서버의 사용자에 대해 구성된 정책을 확인할 수 있습니다

ERROR: 인증 중에 오류가 발생했음을 나타냅니다. 이는 데몬에서 또는 데몬과 라우터 간의 네트워크 연결에서 발생할 수 있습니다. ERROR 응답이 수신되면 라우터는 일반적으로 사용자를 인증하기 위해 대체 방법을 사용하려고 시도합니다.

Cisco 라우터에서 AAA 및 TACACS의 기본 컨피그레이션입니다

```
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
```

TACACS 문제 해결

1단계.

적절한 소스 인터페이스를 사용하는 라우터에서 포트 49의 텔넷을 사용하여 TACACS 서버에 대한 연결을 확인합니다. 라우터가 포트 49의 TACACS 서버에 연결할 수 없는 경우, 트래픽을 차단하는 일부 방화벽 또는 액세스 목록이 있을 수 있습니다.

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

2단계.

AAA 클라이언트가 올바른 IP 주소 및 공유 비밀 키를 사용하여 TACACS 서버에 올바르게 구성되어 있는지 확인합니다. 라우터에 여러 발신 인터페이스가 있는 경우 이 명령을 사용하여 TACACS 소스 인터페이스를 구성하는 것이 좋습니다. IP 주소가 TACACS 서버의 클라이언트 IP 주소로 구성

된 인터페이스를 라우터의 TACACS 소스 인터페이스로 구성할 수 있습니다

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

3단계.

TACACS 소스 인터페이스가 VRF(Virtual Routing and Forwarding)에 있는지 확인합니다. 인터페이스가 VRF에 있는 경우 AAA 서버 그룹 아래에서 VRF 정보를 구성할 수 있습니다. VRF 인식 TACACS 컨피그레이션은 TACACS 컨피그레이션 가이드를 참조하십시오.

4단계.

aaa 테스트를 수행하고 서버에서 올바른 응답을 받는지 확인합니다.

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

5단계.

aaa 테스트가 실패할 경우 라우터와 TACACS 서버 간의 트랜잭션을 분석하여 근본 원인을 파악하기 위해 이러한 디버그를 함께 활성화합니다.

```
debug aaa authentication

debug aaa authorization

debug tacacs

debug ip tcp transaction
```

작업 시나리오의 샘플 디버그 출력입니다.

```
*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
```

TACACS 서버가 잘못된 사전 공유 키로 구성된 경우 라우터의 샘플 디버그 출력입니다.

```
*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).
```

관련 정보

- Cisco IOS의 TACACS 컨피그레이션
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.