Introduction

This document describes the steps to troubleshoot Terminal Access Controller Access-Control System Authentication (TACACS) issues on Cisco IOS/IOS-XE routers and switches.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- Authentication, Authorization and Accounting (AAA) configuration on Cisco devices
- TACACS configuration

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

How TACACS works

TACACS+ protocol uses Transmission Control Protocol (TCP) as the transport protocol with destination port number 49. When the Router receives a login request, it establishes a TCP connection with the TACACS server, post which a username prompt is displayed to the user. When the user enters the username, the Router again communicates with the TACACS server for the password prompt. Once the user enters the password, the Router send this information to the TACACS server again. The TACACS server verifies the user credentials and sends a response back to the Router. The result of a AAA session can be any of these:

PASS: When you are authenticated the service begins only if AAA authorization is configured on the router. The authorization phase begins at this time.

FAIL: When you have failed the authentication. You might be denied further access or be
prompted to retry the login sequence, depending on the TACACS+ daemon. In this, you may need to check the policies configured for the user in TACACS server, if you receive a FAIL from the server.

ERROR: It indicates an error occurred during authentication. This can be either at the daemon or in the network connection between the daemon and the router. If an ERROR response is received, the router typically tries to use an alternative method to authenticate the user.

These are the basic configuration of AAA and TACACS on a Cisco Router

**Troubleshoot TACACS Issues**

**Step 1.** Verify the connectivity to the TACACS server with a **telnet** on port 49 from the router with appropriate source interface. In case the router is not able to connect to the TACACS server on Port 49, there might be some firewall or access list blocking the traffic.

**Step 2.** Verify that the AAA Client is properly configured on the TACACS server with the correct IP address and the shared secret key. If the Router has multiple outgoing interfaces, it is suggested to configure the TACACS source interface by using the following command. You may need to configure the interface, of which the IP address is configured as client IP address on TACACS server, as the TACACS source interface on Router.

**Step 3.** Verify if the TACACS source interface is on a Virtual Routing and Forwarding (VRF). In case the interface is on a VRF, you may need to configure the VRF information under the AAA server group. Refer link for configuration of VRF aware TACACS.

**Step 4.** Perform **test aaa** and verify that we are receiving the correct response from the Server.

**Step 5.** If **test aaa** fails, enable these debugs together to analyse the transactions between the Router and the TACACS server to identify the root cause.

This is a sample debug output in a working scenario:

This is a sample debug output from the Router, when the TACACS server is configured with a wrong pre shared key

**Related Information**

- [TACACS Configuration on Cisco IOS](#)
- [Technical Support & Documentation - Cisco Systems](#)