Understanding an AAA Authentication Command on a Cisco IOS Device

Contents

Introduction

Prerequisites

Requirements

Components Used

Configure

Verify

Troubleshoot

Related Information

Introduction

This document describes the behavior of the **aaa authentication login default local group tacacs+** command on a Cisco IOS® device.

Prerequisites

Requirements

Cisco recommends that:

- The **aaa new-model** is enabled on the device.

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, ensure that you understand the potential impact of any command.

Configure

Note: Use the Cisco CLI Analyzer from the Cisco Tool Catalog in order to obtain more information on the commands used in this section. Only registered Cisco users have access to internal Cisco tools and information.

Configure these commands on the device in global configuration mode:

```
aaa new-model
aaa authentication login default local group tacacs+
```

With just aaa new model configured, local authentication is applied to all lines and interfaces (except console line **line con 0**).

Here the AAA method list is applied on all log in attempts on all lines of the device, where first local database is checked and then if required, Terminal Access Controller Access Control System (TACACS) server is tried.

```
username cisco privilege 15 password 0 cisco
```

Local user database:

```
tacacs-server host 10.20.220.141
tacacs-server key cisco
```

The TACACS server is now configured.

Verify

Use this section to confirm that your configuration works properly.

1. Enable **Debug TACACS** and **Debug AAA Authentication** on the device under test.

<#root>

```
RUT#

show debug

 General OS:

TACACS access control debugging is on


   AAA Authentication debugging is on
```

2. Perform a telnet on the device:

<#root>

```
RUT#

show ip interface brief | exclude unassigned
```

```
 Interface                  IP-Address      OK? Method Status                Protocol
 FastEthernet0/1            10.197.235.96   YES DHCP   up                    up
 Loopback0                  192.168.1.2     YES manual up                    up
```

<#root>

```
RUT#

telnet 192.168.1.2


 Trying 192.168.1.2 ... Open

 User Access Verification

 Username:

cisco


 *Jul 23 09:34:37.023: AAA/BIND(0000001E): Bind i/f
 *Jul 23 09:34:37.023: AAA/AUTHEN/LOGIN (0000001E): Pick method list '

default

'
 Password:

 RUT>
```

You notice that it did not try to reach the TACACS server as username cisco was found locally.

Now, if you try to use a credential that is not configured locally on the box:

<#root>

```
RUT#

telnet 192.168.1.2


 Trying 192.168.1.2 ... Open

 User Access Verification

 Username:
 *Jul 23 09:36:01.099: AAA/BIND(0000001F): Bind i/f
 *Jul 23 09:36:01.099: AAA/AUTHEN/LOGIN (0000001F): Pick method list '

default

'
 Username:

cisco1


 *Jul 23 09:36:11.095: TPLUS: Queuing AAA Authentication request 31 for processing
 *Jul 23 09:36:11.095: TPLUS: processing authentication start request id 31
 *Jul 23 09:36:11.095: TPLUS: Authentication start packet created for 31(cisco1)

*Jul 23 09:36:11.095: TPLUS: Using server 10.20.220.141


 *Jul 23 09:36:11.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: Started 5 sec timeout
 *Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out
 *Jul 23 09:36:16.095: TPLUS(0000001F)/0/NB_WAIT/47A14C34: timed out, clean up
 *Jul 23 09:36:16.095: TPLUS(0000001F)/0/47A14C34: Processing the reply packet

% Authentication failed
```

You can see that it tries to reach the TACACS server 10.20.220.141. It is an expected default behavior. There is no username cisco1 configured on the TACACS server, hence, the result is **Authentication failed**.

If the device has **aaa authentication login default group tacacs+ local** in the configuration, its first preference is TACACS. If the TACACS is reachable, but no user has been configured on it, it does not fallback and try to search in the local database. Instead, It displays the message, **Authentication failed** .

Troubleshoot

There is currently no specific information available to troubleshoot this configuration.

Related Information

- Configure Basic AAA on an Access Server
- Cisco Technical Support & Downloads