Working with Multiple AAA Servers

Introduction

The use of AAA services (Authentication, Authorization, and Accounting) allows for several methods of controlling and recording access to AOS-based devices. The two methods of achieving this result involve either RADIUS or TACACS+ servers. This guide will specifically cover the configuration of multiple servers, and define the proper methods for utilizing them.

Device Administration Considerations

The use of multiple AAA servers is only configurable via the Command Line Interface (CLI). If this type of configuration is utilized, the AAA configuration should not be manipulated in the Graphical User Interface (GUI), as it can result in potentially invalid configurations that would lockout some or all users from authenticating to the appropriate source, or even any source in some cases, thereby potentially either blocking or providing unrestricted access to the service(s) the user(s) are attempting to reach.

Command Line Configuration

Defining Individual Servers

Each server must be defined globally with its associated Pre-Shared Key. This configuration statement will be referenced and matched by the server group to determine the appropriate Pre-Shared Key to use with that server, and any other optional parameters that might be required.

```
radius-server host <RADIUS Server IP> key <Pre-Shared Key>
!
tacacs-server host <TACACS+ Server IP> key <Pre-Shared Key>
```

Defining Server Groups

The next step is to define the server groups. The servers are typically grouped by desired order of use or desired type of authentication. Examples of such types are Device Administration, Wireless Client Authentication, Port-Authentication, and VPN Client Authentication.

There is not a limit to the number of groups that can be configured. Each server can be in its own group and the same server can be referenced by multiple groups. Servers are utilized in a top-down fashion; the group will only fail-over to the next server if the previous server cannot be contacted.

The purpose of the groupings is to allow for varied methods of authentication. Two examples of configuring the same authentication method in multiple ways are shown:

```
radius-server host 1.1.1.1 key adtran
radius-server host 2.2.2.2 key adtran
!
aaa group server radius Server1
  server 1.1.1.1
aaa group server radius Server2
  server 2.2.2.2
aaa group server radius Server2-1
  server 2.2.2.2
  server 1.1.1.1
!
aaa authentication login Example-1 group Server2 group Server1
!
aaa authentication login Example-2 group Server2-1
```

The previous example displays the Server2 being utilized first to demonstrate the top-down order of servers is based upon the order of entry and not on any other metric. The example demonstrates that server 1.1.1.1 will not be moved to the top of the list upon entry; it will maintain its original position.

Both the “Example-1” and “Example-2” methods will accomplish the same result. However, the “Example-1” method would allow for a TACACS+ server to be used after Server2 but before Server1. The groups are divided into RADIUS and TACACS+ types, so a TACACS+ server cannot exist in the same group as a RADIUS server.

Apply Authentication Methods to Services

The defined login method lists are applied in the manner appropriate to the service in question. Please refer to the appropriate document to determine the required settings for the service in question.

An example is shown for SSH login:

```
line ssh 0 4
  login authentication Example-1
```

Configuring the RADIUS/TACACS+ Server

The RADIUS/TACACS+ server settings will depend upon the type of AAA service in use on the network. Please refer to the appropriate document to determine the required settings for the service in question.

Troubleshooting

This section will describe the relevant debug procedures involved when determining any issues with the AAA, RADIUS, or TACACS+ configuration. The commands that will be used are:

- debug aaa
- debug radius
- debug tacacs+

A failed communication with RADIUS “Server2” and subsequent successful fallback authentication to RADIUS “Server1” would be similar to the following:

```
AAA: New Session on portal 'SSH 1 (<Client IP>:<Port>)'.
AAA: Session using AUTHENTICATION list 'Example-1'.
RADIUS AUTHENTICATION: Sending packet to 2.2.2.2 (1812).
RADIUS AUTHENTICATION: Waiting on response from server
RADIUS AUTHENTICATION: Receive timed out
RADIUS AUTHENTICATION: Marking server 2.2.2.2 (1812) (1813) as
     dead.
RADIUS AUTHENTICATION: Failed to get response from server(s).
AAA: No answer from the RADIUS server(s).
RADIUS AUTHENTICATION: Sending packet to 1.1.1.1 (1812).
RADIUS AUTHENTICATION: Waiting on response from server
RADIUS AUTHENTICATION: Receiving from RADIUS socket
RADIUS AUTHENTICATION: Response received from server (1.1.1.1)
RADIUS AUTHENTICATION: Received response from 1.1.1.1.
AAA: RADIUS authentication passed.
```

DISCLAIMER

ADTRAN provides the foregoing application description solely for the reader's consideration and study, and without any representation or suggestion that the foregoing application is or may be free from claims of third parties for infringement of intellectual property rights, including but not limited to, direct and contributory infringement as well as for active inducement to infringe. In addition, the reader's attention is drawn to the following disclaimer with regard to the reader's use of the foregoing material in products and/or systems. That is:

ADTRAN SPECIFICALLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ADTRAN BE LIABLE FOR ANY LOSS OR DAMAGE, AND FOR PERSONAL INJURY, INCLUDING BUT NOT LIMITED TO, COMPENSATORY, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGES.