

AAA Server Groups

Configuring a device to use authentication, authorization, and accounting (AAA) server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics. This feature module describes how to configure AAA server groups and the deadtimer.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- Information About AAA Server Groups, on page 1
- How to Configure AAA Server Groups, on page 2
- Configuration Examples for AAA Server Groups, on page 5
- Additional References, on page 6
- Feature Information for AAA Server Groups, on page 7

Information About AAA Server Groups

AAA Server Groups

Configuring the device to use AAA server groups provides a way to group existing server hosts. Grouping existing server hosts allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts.

Server groups can also include multiple host entries for the same server, as long as each entry has a unique identifier. The combination of an IP address and a UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to different UDP ports on a server at the same IP address. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry that is configured acts as a failover backup to the first one. If the first host entry fails to provide accounting services, the network access server tries the second host entry configured

on the same device for accounting services. (The RADIUS host entries are tried in the order in which they are configured.)

AAA Server Groups with a Deadtimer

After you configure a server host with a server name, you can use the **deadtime** command to configure each server per server group. Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics.

Configuring deadtime is not limited to a global configuration. A separate timer is attached to each server host in every server group. Therefore, when a server is found to be unresponsive after numerous retransmissions and timeouts, the server is assumed to be dead. The timers attached to each server host in all server groups are triggered. In essence, the timers are checked and subsequent requests to a server (once it is assumed to be dead) are directed to alternate timers, if configured. When the network access server receives a reply from the server, it checks and stops all configured timers (if running) for that server in all server groups.

If the timer has expired, the server to which the timer is attached is assumed to be alive. This becomes the only server that can be tried for later AAA requests using the server groups to which the timer belongs.



Note Because one server has different timers and might have different deadtime values configured in the server groups, the same server might, in the future, have different states (dead and alive) at the same time.



Note To change the state of a server, you must start and stop all configured timers in all server groups.

The size of the server group will be slightly increased because of the addition of new timers and the deadtime attribute. The overall impact of the structure depends on the number and size of the server groups and how the servers are shared among server groups in a specific configuration.

How to Configure AAA Server Groups

Configuring AAA Server Groups

To define a server host with a server group name, enter the following commands in global configuration mode. The listed server must exist in global configuration mode.

Before you begin

Each server in the group must be defined previously using the **radius-server host** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*

4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server** *server-name* **Example:** `Device(config)# radius server rad1`	Specifies the name for the RADIUS server.
Step 4	**aaa group server** {**radius** | **tacacs+**} *group-name* **Example:** `Device(config)# aaa group server radius group1`	Defines the AAA server group with a group name. • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the device in server group RADIUS configuration mode.
Step 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Device(config-sg-radius)# server 172.16.1.1 acct-port 1616`	Associates a particular RADIUS server with the defined server group. • Each security server is identified by its IP address and UDP port number. • Repeat this step for each RADIUS server in the AAA server group.
Step 6	**end** **Example:** `Device(config-sg-radius)# end`	Exits server group RADIUS configuration mode and returns to privileged EXEC mode.

Configuring AAA Server Groups with a Deadtimer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa group server radius** *group* **Example:** `Device(config)# aaa group server radius group1`	Defines a RADIUS type server group and enters server group RADIUS configuration mode.
Step 4	**deadtime** *minutes* **Example:** `Device(config-sg-radius)# deadtime 1`	Configures and defines a deadtime value in minutes. **Note** Local server group deadtime overrides the global configuration. If the deadtime vlaue is omitted from the local server group configuration, it is inherited from the primary list.
Step 5	**end** **Example:** `Device(config-sg-radius)# end`	Exits the server group RADIUS configuration mode and returns to the privileged EXEC mode.

Configuration Examples for AAA Server Groups

Examples: AAA Server Groups

The following example shows how to create server group radgroup1 with three different RADIUS server members, each using the default authentication port (1645) and accounting port (1646):

```
aaa group server radius radgroup1
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

The following example shows how to create server group radgroup2 with three RADIUS server members, each with the same IP address but with unique authentication and accounting ports:

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

Example: Multiple RADIUS Server Entries Using AAA Server Groups

The following example shows how to configure the network access server to recognize two different RADIUS server groups. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one. Each group is individually configured for the deadtime; the deadtime for group 1 is one minute, and the deadtime for group 2 is two minutes.

Note In cases where both global commands and **server** commands are used, the **server** command takes precedence over the global command.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
```

```
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Cisco IOS Master Command List, All Releases*
AAA and RADIUS commands	*Cisco IOS Security Command Reference*
RADIUS attributes	*RADIUS Attributes Configuration Guide* (part of the Securing User Services Configuration Library)
AAA	*Authentication, Authorization, and Accounting Configuration Guide* (part of the Securing User Services Configuration Library)
L2TP, VPN, or VPDN	*Dial Technologies Configuration Guide* and *VPDN Configuration Guide*
Modem configuration and management	*Dial Technologies Configuration Guide*
RADIUS port identification for PPP	*Wide-Area Networking Configuration Guide*

RFCs

RFC	Title
RFC 2138	*Remote Authentication Dial-In User Service (RADIUS)*
RFC 2139	*RADIUS Accounting*
RFC 2865	*RADIUS*
RFC 2867	*RADIUS Accounting Modifications for Tunnel Protocol Support*
RFC 2868	*RADIUS Attributes for Tunnel Protocol Support*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for AAA Server Groups

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for AAA Server Groups

Feature Name	Releases	Feature Information
AAA Server Group		Configuring the device to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. A server group is used with a global server-host list. The server group lists the IP addresses of the selected server hosts. • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller • Catalyst 3650 Series Switches The following commands were introduced or modified: **aaa group server radius**, **aaa group server tacacs+**, and **server** (RADIUS).
AAA Server Group Enhancements		AAA Server Group Enhancements enables the full configuration of a server in a server group. • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller • Catalyst 3650 Series Switches

Feature Name	Releases	Feature Information
AAA Server Group Deadtimer		Configuring deadtime within a server group allows you to direct AAA traffic to separate groups of servers that have different operational characteristics. • Catalyst 3850 Series Switches • Cisco 5760 Wireless LAN Controller • Catalyst 3650 Series Switches The following commands were introduced or modified: **deadtime**.