

AAA Server Group

This document includes the following sections:

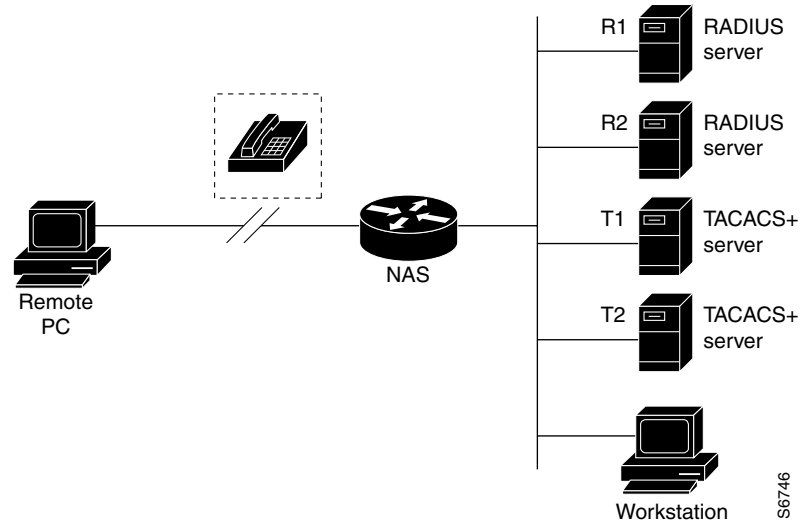
- Feature Overview on page 1
- Supported Platforms on page 2
- Supported Standards, MIBs and RFCs on page 2
- Configuration Tasks on page 3
- Configuration Examples on page 4
- Command Reference on page 4
- Glossary on page 18

Feature Overview

The AAA server-group feature introduces a way to group existing server hosts. The feature allows you to select a subset of the configured server hosts and use them for a particular service.

A server-group is a list of server hosts of a particular type. Currently supported server-host types are Remote Authentication Dial In User Service (RADIUS) server hosts and Terminal Access Controller Access Control System Plus (TACACS+) server hosts. A server-group is used in conjunction with a global server-host list. The server-group lists the IP addresses of the selected server hosts. Figure 1 shows a typical AAA network configuration: R1 and R2 are RADIUS server hosts, and T1 and T2 are TACACS+ server hosts.

Figure 1 Typical AAA Network Configuration



Benefits

The AAA server-group feature allows customers to define a distinct list of server hosts and apply this list to relevant applications. The AAA server-group feature is also backward compatible; this feature works on releases earlier than Cisco IOS Release 12.0(5)T.

Related Documents

- *Security Configuration Guide*
- *Security Command Reference*

Restrictions

The AAA server-group feature works only when the server hosts in a group are the same type: RADIUS or TACACS+.

Supported Platforms

AAA is part of the core IOS; therefore, the AAA server-group feature is supported on all platforms using Cisco IOS Release 12.0(5)T.

Supported Standards, MIBs and RFCs

Standards

None

MIBs

No new or modified MIBs are supported by this feature.

For descriptions of supported MIBs and how to use MIBs, see the Cisco MIB web site on CCO at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

RFCs

None

Configuration Tasks

Perform the following tasks to configure AAA server-groups:

- Configuring AAA Server Groups (Required)
- Verifying AAA Server Groups

Configuring AAA Server Groups

Note The server host configuration has precedence over any server-group configuration, which in turn has precedence over any system-global configuration that exists.

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

Step	Command	Purpose
1	Router(config)# aaa new-model	Enables AAA globally.
2	Router(config)# radius-server host <i>ip-address</i> <i>key</i> or Router(config)# tacacs-server host <i>ip-address</i> <i>key</i>	Specifies and defines the IP address of the server host before configuring the AAA server-group.
3	Router(config-if)# aaa group server { radius tacacs+ } <i>group-name</i>	Defines the AAA server-group with a group name.

After you define the server group with a group name, enter the following commands to enable AAA authentication, AAA authorization, and AAA accounting:

Command	Purpose
Router(config-if)# aaa authentication login default group [<i>group-name</i> radius tacacs]	Creates local authentication.
Router(config-if)# aaa authentication ppp default group [<i>group-name</i> radius tacacs]	Enables local authentication.
Router(config-if)# aaa authorization default group [<i>group-name</i> radius tacacs]	Creates an authorization method list for the server-group.
Router(config-if)# aaa accounting default network group [<i>group-name</i> radius tacacs]	Enables accounting for the server-group.

Verifying AAA Server Groups

Embedded error messages guide you to configure the server-group feature correctly. Therefore, no verification steps are needed.

Configuration Examples

A server-group is uniquely identified by its name. It is important to select the correct server host type because the method-list definition identifies the server host types by name.

A configuration example for an AAA server group is as follows:

```
Router(config)# aaa group server {tacacs+ | radius} group-name
Router(config-sg radius)# server 1.1.1.1
Router(config-sg radius)# server 2.2.2.2
Router(config-sg radius)# server 3.3.3.3
Router(config)# end
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 *Security Command Reference*.

New Commands

- **aaa group server**
- **server**

Modified Commands

- **aaa accounting**
- **aaa authentication login**
- **aaa authorization**

aaa group server

To group different server hosts into distinct lists and distinct methods, enter the **aaa group server** global configuration command. To remove a server group from the configuration list, enter the **no** form of this command.

```
aaa group server { tacacs+ | radius } group-name
no aaa group server { tacacs+ | radius } group-name
```

Syntax Description

tacacs+	Use only the TACACS+ server hosts.
radius	Use only the RADIUS server hosts.
<i>group-name</i>	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The AAA server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A server group is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A server group is used in conjunction with a global server host list. The server group lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of an AAA server-group:

```
Router(config) aaa group server { tacacs+ | radius } group-name
  Router(config-sg radius) server 1.1.1.1
  Router(config-sg radius) server 2.2.2.2
  Router(config-sg radius) server 3.3.3.3
Router(config) end
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict network access to a user.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies and defines the IP address of the RADIUS server host before configuring an AAA server-group.
tacacs-server host	Specifies and defines the IP address of the TACACS+ server host before configuring an AAA server-group.

aaa accounting

To enable AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, enter the **aaa accounting** global configuration command. To disable accounting, enter the **no** form of this command.

```
aaa accounting {system | network | exec | connection | commands level} {default | list-name}
  {start-stop | wait-start | stop-only | none} [group group-name]
no aaa accounting {system | network | exec | commands level} [group group-name]
```

Syntax Description

system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP NCPs, and AppleTalk Remote Access (ARA).
exec	Runs accounting for an EXEC session (user shells). This keyword could return user profile information, such as autocommand information.
connection	Provides information about all outbound connections made from the network access server, such as Telnet, local-area transport (LAT), TN3270, packet assembler/disassembler (PAD), and rlogin.
commands	Runs accounting for all commands at the specified privilege level.
<i>level</i>	Specifies the command level to track for accounting. Valid entries are 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of accounting methods.
start-stop	Sends a start-accounting notice at the beginning of a requested process and a stop-accounting notice at the end of a process. The start-accounting record is sent in the background. The requested user process begins regardless whether the start-accounting notice was received by the accounting server.
wait-start	As in start-stop , sends both a start and a stop-accounting notice to the accounting server. However, if you use the wait-start keyword, the requested user service does not begin until the start-accounting notice is acknowledged. A stop-accounting notice also is sent.
stop-only	Sends a stop-accounting notice at the end of the requested user process.
none	Disables accounting services on the specified line or interface.
group	(Optional) Group of servers.
<i>group-name</i>	(Optional) Character string used to name the group of accounting methods.

Defaults

AAA accounting is disabled. If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	The group keyword was added.

Usage Guidelines

Enter the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 1 AAA Accounting Method Keywords

Keyword	Description
<i>group name</i> radius	Uses RADIUS to provide accounting service.
<i>group name</i> tacacs+	Uses TACACS+ to provide accounting services.

Cisco IOS software supports the following two methods for accounting:

- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting AV pairs and is stored on the security server.

Method lists for accounting define the way accounting is performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as RADIUS or TACACS+) and *method* identifies the method(s) tried in the given sequence.

Named accounting method lists are specific to the indicated type of accounting. To create a method list to provide accounting information for ARA (network) sessions, enter the **arap** keyword. To create a method list to provide accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times, enter the **exec** keyword. To create a method list to provide accounting information about specific, individual EXEC commands associated with a specific privilege level, enter the **commands** keyword. To create a method list to provide accounting information about all outbound connections made from the network access server, enter the **connection** keyword.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting notice at the end of the process. For even more accounting control, you can include the **wait-start** keyword, which ensures that the start accounting notice is received by the RADIUS or TACACS+ server before granting the process request from the user. Accounting is only stored on the RADIUS or TACACS+ server. The **none** keyword disables accounting services for the specified line or interface.

When **aaa accounting** is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server.

For a list of supported RADIUS accounting attributes, refer to the “RADIUS Attributes” appendix in the *Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the “TACACS+ Attribute-Value Pairs” appendix in the *Security Configuration Guide*.

Examples

The following example shows a default commands accounting method list defined, where command accounting services are provided by a TACACS+ security server, and are set for privilege level 15 commands with a stop-only restriction.

```
aaa accounting commands 15 default stop-only tacacs+
```

Related Commands

Command	Description
aaa authentication	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict a network access to a user.
aaa new-model	Enables the AAA access control model.

aaa authentication login

To set AAA authentication at login, enter the **aaa authentication login** global configuration command. To disable AAA authentication, enter the **no** form of this command.

```
aaa authentication login {default | list-name} group group-name  
no aaa authentication login {default | list-name} [group group-name | method1 method2]
```

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
<i>list-name</i>	Character string used to name the list of authentication methods activated when a user logs in.
<i>method</i>	AAA authentication method that uses at least one of the keywords described in Table 2.
group	Group of servers.
<i>group-name</i>	Character string used to name the group of servers for authentication when a user logs in.

Defaults

If the **default** list is not set, only the local user database is checked, which has the same effect as the following command:

```
aaa authentication login default local
```

Note On the console, login will succeed without any authentication checks if **default** is not set.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	The group keyword was added.

Usage Guidelines

Enter the default and optional list names that you create with the **aaa authentication login** command with the **login authentication** command.

Create a list by entering the **aaa authentication list-name method** command for a particular protocol, where *list-name* is any character string used to name this list (such as *MIS-access*). The *method* argument identifies the list of methods that the authentication algorithm tries in the given sequence. Method keywords are described in Table 2.

To create a default list that is used if no list is assigned to a line, enter the **login authentication** command with the *default* argument followed by the methods you want to use in default situations.

Use the additional methods of authentication only if the previous method returns an error—not if it fails. To ensure that the authentication succeeds even if all methods return an error, specify **none** as the final method in the command line.

If you do not set authentication specifically for a line, the default is to deny access and no authentication is performed. To display currently configured lists of authentication methods, enter the **more system:running-config** command.

Table 2 AAA Authentication Login Methods

Keyword	Description
enable	Uses the enable password for authentication.
krb5	Uses Kerberos 5 for authentication.
line	Uses the line password for authentication.
local	Uses the local username database for authentication.
none	Uses no authentication.
<i>group-name</i> radius	Uses RADIUS authentication.
<i>group-name</i> tacacs+	Uses TACACS+ authentication.
krb5-telnet	Uses the Kerberos 5 Telnet authentication protocol when using Telnet to connect to the router.

Examples

The following example shows an AAA authentication list created called *MIS-access*. This authentication first tries to contact a TACACS+ server. If no server is found, TACACS+ returns an error and AAA tries to use the enable password. If this attempt also returns an error (because no **enable** password is configured on the server), the user is allowed access with no authentication:

```
aaa authentication login MIS-access tacacs+ enable none
```

The following example shows the same list created, but it is set as the default list that is used for all login authentications if no other list is specified:

```
aaa authentication login default tacacs+ enable none
```

The following example shows the authentication set at login to use the Kerberos 5 Telnet authentication protocol when Telnet is used to connect to the router:

```
aaa authentication login default KRB5-TELNET krb5
```

Related Commands

Command	Description
aaa authentication local-override	Configures the Cisco IOS software to check the local user database for authentication before attempting another form of authentication.
aaa new-model	Enables the AAA access control model.
login authentication	Enables AAA authentication for logins.

aaa authorization

To set parameters that restrict a network access to a user, enter the **aaa authorization** global configuration command. To disable authorization for a function, enter the **no** form of this command.

```
aaa authorization {network | exec | commands level | reverse-access} {default | list-name}
group group-name
no aaa authorization {network | exec | commands level | reverse-access} [group group-name
| method1 method2]
```

Syntax Description

network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP NCPs, and AppleTalk Remote Access (ARA).
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility could return user profile information, such as autocommand information.
commands	Runs authorization for all commands at the specified privilege level.
<i>level</i>	Specifies the command level that should be authorized. Valid entries are 0 through 15.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
default	Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
<i>list-name</i>	Character string used to name the list of authorization methods.
<i>method1</i> [<i>method2...</i>]	AAA authorization method that uses one of the keywords listed in Table 3.
group	Group of servers.
<i>group-name</i>	Character string used to name the group of authorization methods.

Defaults

Authorization is disabled for all actions (equivalent to the method keyword **none**). If the **aaa authorization** command for a particular authorization type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place.

Command Modes

Global configuration

Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	The group keyword was added.

Usage Guidelines

Enter the **aaa authorization** command to enable authorization and to create named method lists that define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways authorization is performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+) in sequence. Method lists enable you to designate one or more security protocol to be used for authorization; thus it ensures a backup system if the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Enter the **aaa authorization** command to create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Table 3 AAA Authorization Methods

Keyword	Description
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.
local	Uses the local username database for authorization.
<i>group-name</i> radius	Uses RADIUS to get authorization information.
<i>group-name</i> tacacs+	Requests authorization information from the TACACS+ server.
krb5-instance	Uses the instance defined by the kerberos instance map command.

Method lists are specific to the type of authorization being requested. AAA supports four different types of authorization:

- Network—Applies to network connections. This method can include a PPP, SLIP, or ARA connection.
- EXEC—Applies to the attributes associated with a user EXEC terminal session.
- Commands—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- Reverse Access—Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The **authorization** command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS+ daemon as part of the authorization process. The daemon can perform one of the following actions:

- Accept the request as is
- Make changes to the request
- Refuse the request and refuse authorization

For a list of supported RADIUS attributes, refer to the “RADIUS Attributes” appendix in the *Security Configuration Guide*. For a list of supported TACACS+ AV pairs, refer to the “TACACS+ Attribute-Value Pairs” appendix in the *Security Configuration Guide*.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands are not included in the privilege level command set.

Examples

The following example shows a network authorization method list defined and named scoobee, which specifies that RADIUS authorization is used on serial lines using PPP. If the RADIUS server fails to respond, then local network authorization is performed:

```
aaa authorization network scoobee radius local
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when RADIUS or TACACS+ is used.
aaa authentication	Sets AAA authentication at login.
aaa new-model	Enables the AAA access control model.

server

To configure the IP address of the RADIUS server, enter the **server** AAA server-group command. To remove the IP address of the RADIUS server, enter the **no** form of this command.

```
server ip-address
no server ip-address
```

Syntax Description

ip-address IP address of the selected server.

Defaults

None

Command Modes

AAA server-group sub-mode.

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Enter the **server** command to specify the IP address of the RADIUS server. Also configure a matching **radius-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default group g1
Router(config)# aaa group server radius g1
    Router(config-sg radius)# server 1.0.0.1
    Router(config-sg radius)# server 2.0.0.1
Router(config)# radius-server host 1.0.0.1 auth-port 1000 acct-port 1001...
Router(config)# radius-server host 1.0.0.1 auth-port 1645 acct-port 1646...
Router(config)# radius-server host 2.0.0.1 auth-port 1645 acct-port 1646...
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa server group	Groups different servers hosts into distinct lists and distinct methods.
radius-server host	Specifies and defines the IP address of the RADIUS server host before configuring an AAA server-group.

Glossary

AV pairs—attribute-value pairs.

NAS—network access server.

RADIUS—Remote Access Dial-In User Service.

TACACS+—Terminal Access Controller Access Control System Plus.