K through L

- key (config-radius-server), page 2
- key (TACACS+), page 5
- key-hash, page 7
- load-balance (server-group), page 8

key (config-radius-server)

To specify the authentication and encryption key for all RADIUS communications between the device and the RADIUS server, use the **key** command in RADIUS server configuration mode. To remove the configured key, use the **no** form of this command.

key {**0** *string* | **6** *string* | **7** *string*} *string*

no key

Syntax Description

0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an advanced encryption scheme (AES) encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to specify the host with IP address 192.0.2.2 as the RADIUS server and set rad123 as the encryption key:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key rad123
```

The following example shows how to set the authentication and encryption key to anykey. The keyword 7 specifies that a hidden key follows.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key 7 anykey
```

After you save your configuration and use the **show running-config** command, an encrypted key is displayed as follows:

```
Device> enable
Device# show running-config

radius server myserver
  address ipv4 192.0.2.2
  key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
password encryption aes	Enables a type 6 encrypted preshared key.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

Command	Description
show running-config	Displays the current configuration of your routing device.

key (TACACS+)

To configure the per-server encryption key on the TACACS+ server, use the **key** command in TACACS+ server configuration mode. To remove the per-server encryption key, use the **no** form of this command.

key [**0** | **6** | **7**] *key-string*

no key [**0** | **6** | **7**] *key-string*

Syntax Description

0	(Optional) Specifies that an unencrypted key follows.
6	(Optional) Specifies that an advanced encryption scheme (AES) encrypted key follows.
7	(Optional) Specifies that a hidden key follows.
key-string	The unencrypted shared key.

Command Default

No TACACS+ encryption key is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added.

Usage Guidelines

The **key** command allows you to configure a per-server encryption key.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to specify an unencrypted shared key named “key1”:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# key 0 key1
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

key-hash

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) key type and name, use the **key-hash**command in SSH public key configuration mode. To remove the SSH RSA Rivest, Shamir, and Adleman (RSA) public key, use the **no** form of this command.

key-hash *key-type key-name*

no key-hash [*key-type key-name*]

Syntax Description

key-type key-name	The SSH RSA public key type and name.

Command Default

SSH key type and name are not specified.

Command Modes

SSH public key configuration (conf-ssh-pubkey-user)

Command History

Release	Modification
12.2(33)SRA	This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.

Usage Guidelines

The key type must be **ssh-rsa** for configuration of private-public key pairs. You can use a hashing software to compute the hash of the public key string or you can copy the hash value from another Cisco IOS router. Using the **key-string** command is the preferred method for entering the public key data for the first time.

Examples

The following example shows how to specify the SSH key type and name:

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-hash ssh-rsa key1
Router(conf-ssh-pubkey-user))# exit
Router(config-pubkey)# exit
Router(config)# exit
```

Related Commands

Command	Description
key-string	Specifies the SSH RSA public key of the remote peer.

load-balance (server-group)

To enable RADIUS server load balancing for a named RADIUS server group, use the load-balance command in server group configuration mode. To disable named RADIUS server load balancing, use the **no** form of this command.

load-balance method least-outstanding [**batch-size** *number*] **[ignore-preferred-server]**

no load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1-2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single authentication, authorization, and accounting (AAA) session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Default

If this command is not configured, named RADIUS server load balancing will not occur.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.

Examples

The following shows the relevant RADIUS configuration:

```
Router# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp**command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the start-stop keyword.

Examples

The debug output below shows the selection of a preferred server and the processing of requests for the configuration above.

```
Router#
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers
RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
Router#
```

The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS load balancing.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
test aaa group	Tests RADIUS load balancing server response manually.