AAA Commands

To use these commands in System Admin VM, you must be in a user group associated with appropriate command rules and data rules. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

- aaa authentication, page 2
- aaa authentication login group tacacs , page 4
- aaa authorization, page 5
- aaa authorization commands group tacacs , page 7
- aaa disaster-recovery, page 8
- aaa accounting commands group tacacs , page 9
- confdConfig aaa authOrder , page 10
- confdConfig aaa authorization callback enabled , page 11
- confdConfig aaa authorization enabled , page 12
- confdConfig aaa externalAuthentication enabled , page 13
- confdConfig aaa externalAuthentication executable , page 14
- show tacacs-server request , page 15
- show tacacs-server trace , page 16
- show aaa, page 17
- tacacs-server host, page 18
- tacacs-server key, page 19
- tacacs-server timeout, page 20

aaa authentication

To create users and user-groups for the System Admin VM, use the **aaa authentication** command in the System Admin Config mode. To delete users and user-groups, use the **no** form of this command.

aaa authentication {**groups group** *group-name* [**gid | users**]| **users user** *user-name* [**gid| homedir| password| ssh_keydir| uid**]}

Syntax Description

groups	Configures access groups.
group	Specifies a group.
group-name	Name of the group.
gid	Specifies a numeric value.
users	Configures users.
user	Specifies a user.
user-name	Name of the user.
homedir	Specifies an alphanumeric value.
password	Specifies a password for user authentication.
ssh_keydir	Specifies an alphanumeric value.
uid	Specifies a numeric value.

Command Default

None

Command Modes

System Admin Config

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Examples

This example shows how to create a new user- user1:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)# aaa authentication users user user1 gid 20 homedir dir password
 pwd ssh_keydir dir uid 10
```

This example shows how to create a new group- group1:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)# aaa authentication groups group group1 gid 10 users user1
```

aaa authentication login group tacacs

To enable remote authentication support using TACACS+ protocol, use the **aaa authentication login group tacacs** command. To disable remote authentication , use the **no** form of this command.

aaa authentication login group tacacs

This command has no keywords or arguments.

Command Default

AAA authentication is disabled.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command is introduced.

Examples

The following example shows how to use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authentication login group tacacs
```

aaa authorization

To create command rules and data rules for authorization, use the **aaa authorization** command in the System Admin Config mode. To delete the command rules and data rules, use the **no** form of this command.

aaa authorization {**cmdrules cmdrule** [*integer* | **range** *integer*] [**action | command| context | group| ops**]| **datarules datarule** [*integer* | **range** *integer*] [**action| context | group| keypath| namespace| ops**]}

Syntax Description

cmdrules	Configures command rules.
cmdrule *integer*	Specifies the command rule number. The *integer* value ranges from 1 to 2,147,483,647. **Note** Numbers between 1 and 1000 are reserved for internal use. Specify an integer value that is greater than 1000.
range *integer*	Specifies the range of the command rules or data rules to be configured. The *integer* value ranges from 1 to 2,147,483,647.
action	Specifies whether the users are permitted or refrained from performing the operation specified for the **ops** keyword.
command	Specifies the command to which the command rule applies to. The command should be entered within double-quotes.
context	Specifies which type of connection the command rule or data rule applies to. The connection type can be netconf, cli, or xml.
group	Specifies the group to which the command rule or data rule applies to.
ops	Specifies whether the user has read, execute, or read and execute permission for the command.
datarules	Configures data rules.
datarule *integer*	Specifies the data rule number. The *integer* value ranges from 1 to 2,147,483,647. **Note** Numbers between 1 and 1000 are reserved for internal use. Specify an integer value that is greater than 1000.
keypath	Specifies the keypath of the data element. If you enter an asterisk '*' for keypath, it indicates that the command rule is applicable to all the configuration data.
namespace	Enter asterisk "*" to indicate that the data rule is applicable for all namespace values.

Command Default

None

Command Modes System Admin Config

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Examples This example shows how to create a command rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 10 action accept command "show
 platform" context cli group group1 ops rx
```

This example shows how to create a data rule:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)#aaa authorization datarules datarule 20 action accept context cli
 group group10 keypath * namespace * ops rwx
```

aaa authorization commands group tacacs

To enable remote authorization support using TACACS+ protocol, use the **aaa authorization commands group tacacs** command. To disable authorization for a function, use the **no** form of this command.

aaa authorization command group {**tacacs**| **none**}

Syntax Description

tacacs	Specifies that authorization has to be performed using TACACS+ protocol.
none	(Optional) Specifies that no authorization has to be performed.

Command Default

Authorization is disabled for all actions.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command is introduced.

Examples

The following example shows how to use this command to specify that TACACS+ authorization has to be performed:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authorization commands group tacacs
```

Examples

The following example shows how to use this command to specify that no authorization should be performed:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authorization commands group none
```

Examples

The following example shows how to use this command to specify that first TACACS+ authorization has to be performed and if it fails, no authorization should be performed:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa authorization commands group tacacs none
```

aaa disaster-recovery

To configure a disaster-recovery user and password, use the **aaa disaster-recovery** command in the System Admin Config mode. To delete the disaster-recovery user and password, use the **no** form of this command.

aaa disaster-recovery username *username* **password** *password*

Syntax Description

username	Configures the username for the disaster-recovery user.
username	Specifies the username for the disaster-recovery user.
password	Configures the password for the disaster-recovery user.
password	Password for the disaster-recovery user.

Command Default

None

Command Modes

System Admin Config

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

Only an already existing user can be specified as a disaster-recovery user.

Examples

This example shows how to configure a disaster-recovery user:

```
sysadmin-vm:0_RP0#config
sysadmin-vm:0_RP0(config)## aaa disaster-recovery username root user1 password pwd
```

aaa accounting commands group tacacs

To enable remote accounting support using TACACS+ protocol, use the **aaa accounting commands group tacacs** command. To disable remote accounting , use the **no** form of this command.

aaa accounting commands group tacacs

This command has no keywords or arguments.

Command Default

Authorization is disabled for all actions (equivalent to the method **none** keyword).

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how to use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# aaa accounting commands group tacacs
```

confdConfig aaa authOrder

To specify an order of authentication for AAA systems, use the **confdConfig aaa authOrder**command.

confdConfig aaa authOrder {**externalAuthentication**| **localAuthentication**}

Syntax Description

externalAuthentication	Specifies that external authentication should be performed based on the configured executable.
localAuthentication	Specifies that local authentication should be performed.

Command Default

By default the user is authenticated by using local authentication methods.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how to define external authentication as the primary authentication mechanism:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# confdConfig aaa authOrder externalAuthentication
localAuthentication
```

confdConfig aaa authorization callback enabled

To enable application callbacks for authorization, use the **confdConfig aaa authorization callback enabled**command.

confdConfig aaa authorization callback enabled

This command has no keywords or arguments.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# confdConfig aaa authorization callback enabled
```

confdConfig aaa authorization enabled

To enable external authorization, use the **confdConfig aaa authorization enabled**command.

confdConfig aaa authorization enabled

This command has no keywords or arguments.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# confdConfig aaa authorization enabled
```

confdConfig aaa externalAuthentication enabled

To enable external authentication, use the **confdConfig aaa externalAuthentication enabled**command. To disable external authentication, use the **no** form of the command.

confdConfig aaa externalAuthentication enabled

This command has no keywords or arguments.

Command Default

By default the user is authenticated by using external authentication method.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how to use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# confdConfig aaa externalAuthentication enabled
```

confdConfig aaa externalAuthentication executable

To enable external authentication using an executable configured on the local host, use the **confdConfig aaa externalAuthentication enabled**command.

confdConfig aaa externalAuthentication enabled *chvrf 0 /opt/cisco/calvados/bin/calvados_login_aaa_proxy*

Syntax Description

chvrf 0 /opt/cisco/calvados/bin/calvados_login_aaa_proxy	File name and path of the executable configured on the local host that is used to enable external authentication.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Examples

The following example shows how use this command:

```
sysadmin-vm:0_RP0# configure
sysadmin-vm:0_RP0(config)# confdConfig aaa externalAuthentication executable  chvrf 0
/opt/cisco/calvados/bin/calvados_login_aaa_proxy
```

show tacacs-server request

To display information of send/receive/pending request information of TACACS+ servers, use the **show tacacs-server request** command in the System Admin EXEC mode.

show tacacs-server request

This command has no keywords or arguments.

Command Default None

Command Modes System Admin EXEC

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines This command is used for diagnostics purpose only.

Examples The following example shows the output of the **show tacacs-server request** command:

```
sysadmin-vm:0_RP0#show tacacs-server request

sysadmin-vm:0_RP0# tacacs-server requests ipv4 1.1.1.1 59
Server: 1.1.1.1/59 opens=0 closes=0 aborts=0 errors=0
        packets in=0 packets out=0 family=IPv4
```

show tacacs-server trace

To display TACACS+ server and client process information, use the **show tacacs-server trace** command in the System Admin EXEC mode.

show tacacs-server trace location *[all|node-id]*

Syntax Description

location*all* |*node-id*	Specifies the target location. The *node-id* argument is expressed in the *rack*/*slot* notation. The *all*argument displays trace details of all the TACACS+ servers and client processes.

Command Default

None

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

This command is used for diagnostics purpose only.

Examples

The following example shows the output of the **show tacacs-server trace location*node-id*** command:

```
sysadmin-vm:0_RP0#show tacacs-server trace location 0/RP0
```

Examples

The following example shows the output of the **show tacacs-server trace location *all*** command:

```
sysadmin-vm:0_RP0#show tacacs-server trace location all
```

show aaa

To display information about a privileged user and aaa trace details, use the **show aaa** command in System Admin EXEC mode.

show aaa {**privileged-access** | **trace** {**login** | **sync**} **location** *node-id*}

Syntax Description

privileged-access	Displays access data.
trace	Displays the trace data.
login	Displays login trace.
sync	Displays aaa sync trace.
location *node-id*	Specifies the target location. The *node-id* argument is expressed in the *rack*/*slot* notation.

Command Default

None

Command Modes

System Admin EXEC

Command History

Release	Modification
Release 5.0.0	This command was introduced.

Usage Guidelines

The **show aaa privileged-access** command displays information about the first user, current disaster-recovery user, who accessed the disaster-recovery account, and when was it last accessed.

The **show aaa trace** command is used only for diagnostics.

Examples

This example shows how to view privileged access user details:

```
sysadmin-vm:0_RP0#show aaa privileged-access
Fri Aug  30 10:27:24.170 UTC

Privileged-user, shell access and disaster-recovery user information
  Last access to shell via disaster-recovery account : None
  Privileged-user                                    : root
  Privileged-user attributes changed via admin CLI   : Yes
  Current disaster-recovery user                     : root
```

tacacs-server host

To specify a TACACS+ server and TCP port number, use the **tacacs-server host** command. To delete the specified name or address, use the **no** form of this command.

tacacs-server host host-name *port number*

Syntax Description

host *ipaddress or host-name*	Host or domain name or IP address of the TACACS+ server.
port-number	Specifies a server port number. Valid port numbers range from 1 to 65535.

Command Default

No TACACS+ host is specified.

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can use multiple **tacacs-server host** commands to specify additional hosts. Cisco IOS XR software searches for hosts in the order in which you specify them.

Examples

The following example shows how to specify a TACACS+ host with the IP address 209.165.200.226:

```
sysadmin-vm:0_RP0(config)# tacacs-server host 209.165.200.226
sysadmin-vm:0_RP0(config-tacacs-host)#
```

The following example shows that the default values from the **tacacs-server host** command are displayed from the **show run** command:

```
sysadmin-vm:0_RP0# show run

Building configuration...
!! Last configuration change at 13:51:56 UTC Mon Nov 14 2005 by lab
!
tacacs-server host 209.165.200.226 port 49
 timeout 5
!
```

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the router and the TACACS+ daemon, use the **tacacs-server key** command. To disable the key, use the **no** form of this command.

tacacs-server key {*clear-text-key*}

Syntax Description

clear-text-key	Specifies an unencrypted (cleartext) shared key.

Command Default

None

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The key name entered must match the key used on the TACACS+ daemon. The key name applies to all servers that have no individual keys specified. All leading spaces are ignored; spaces within and after the key are not. 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.

The key name is valid only when the following guidelines are followed:

The TACACS server key is used only if no key is configured for an individual TACACS server. Keys configured for an individual TACACS server always override this global key configuration.

Examples

The following example sets the authentication and encryption key to key1:

```
sysadmin-vm:0_RP0(config)# tacacs-server key key1
```

tacacs-server timeout

To set the interval that the server waits for a server host to reply, use the **tacacs-server timeout** command. To restore the default, use the **no** form of this command.

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

Syntax Description

seconds	Integer that specifies the timeout interval (in seconds) from 1 to 1000.

Command Default

5 seconds

Command Modes

System Admin Config

Command History

Release	Modification
Release 6.1.2	This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The TACACS+ server timeout is used only if no timeout is configured for an individual TACACS+ server. Timeout intervals configured for an individual TACACS+ server always override this global timeout configuration.

Examples

The following example shows the interval timer being changed to 10 seconds:

```
RP/0/RP0/CPU0:router(config)# tacacs-server timeout 10
```