Configure AAA

This chapter describes the implementation of the administrative model of task-based authorization used to control user access in the software system.

Table 1: Feature History

Feature Name	Release Information	Feature Description
OC support for AAA user	Cisco IOS XR Release 7.3.2	This feature allows all authorized users on XR VM to access administration data on the router through NETCONF or gRPC interface, similar to accessing the CLI. This functionality works by internally mapping the task group of the user on XR VM to a predefined group on System Admin VM. Therefore, the NETCONF and gRPC users can access the administrative information on the router even if their user profiles do not exist on System Admin VM. Command added: • **aaa authorization (System Admin-VM)**

Understanding of AAA

User groups and task groups are configured through the software command set used for authentication, authorization and accounting (AAA) services. Authentication commands are used to verify the identity of a user or principal. Authorization commands are used to verify that an authenticated user (or principal) is granted permission to perform a specific task. Accounting commands are used for logging of sessions and to create an audit trail by recording certain user- or system-generated actions.

AAA is part of the software base package and is available by default.

To configure authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode.

Admin Access for NETCONF and gRPC

This feature allows all authorized users on XR VM to access administration data on the router through NETCONF or gRPC interface, similar to accessing the CLI. This functionality works by internally mapping the task group of the user on XR VM to a predefined group on System Admin VM. Therefore, the NETCONF and gRPC users can access the admin-related information on the router even if their user profiles do not exist on System Admin VM.

NETCONF is an XML-based protocol used over Secure Shell (SSH) transport to configure a network. Similarly, gRPC is an open-source remote procedure call framework. The client applications can use these protocols to request information from the router and make configuration changes to the router. Prior to Cisco IOS XR Software Release 7.3.2, users who use NETCONF, gRPC or any other configuration interface, other than CLI, to access the admin-related information on the router, had to belong to user groups that are configured on System Admin VM. Otherwise, the router would issue an UNAUTHORIZED access error message and deny access through that client interface.

By default, XR VM synchronizes only the first configured user to System Admin VM. If you delete the first user in XR VM, the system synchronizes the next user in the **root-lr** group (which is the highest privilege group in XR VM for Cisco IOS XR 64-bit platforms) to System Admin VM only if there are no other users configured in System Admin VM. The system does not automatically synchronize the subsequent users to System Admin VM. Therefore, in earlier releases, users whose profiles did not exist in System Admin VM were not able to perform any NETCONF or gRPC operations on System Admin VM.

From Cisco IOS XR Software Release 7.3.2, the system internally maps the users who are authorized on XR VM to System Admin VM of the router, based on the task table of the user on XR VM. With this feature, the NETCONF and gRPC users can access admin-related information on the router even if their user profiles do not exist on System Admin VM. By default, this feature is enabled.

User Profile Mapping from XR VM to System Admin VM

User privileges to execute commands and access data elements on the router are usually specified using certain command rules and data rules that are created and applied on the user groups.

When the internal process for AAA starts or when you create the first user, the system creates the following set of predefined groups, command rules and data rules in System Admin VM. These configurations are prepopulated to allow users of different groups (such as root-system, admin-r and aaa-r) in System Admin VM

You can use the **show running-configuration aaa** command to view the AAA configurations.

```
aaa authentication groups group aaa-r gid 100 users %%__system_user__%%
!
aaa authentication groups group admin-r gid 100 users %%__system_user__%%
!
aaa authentication groups group root-system gid 100 users "%%__system_user__%% "
!
aaa authorization cmdrules cmdrule 1 context * command * group root-system ops rx action
accept
!
aaa authorization cmdrules cmdrule 2 context * command "show running-config aaa" group aaa-r
```

```
ops rx action accept
!
aaa authorization cmdrules cmdrule 3 context * command "show tech-support aaa" group aaa-r
ops rx action accept
!
aaa authorization cmdrules cmdrule 4 context * command "show aaa" group aaa-r ops rx
action accept
!
aaa authorization cmdrules cmdrule 5 context * command show group admin-r ops rx action
accept
!
aaa authorization datarules datarule 1 namespace * context * keypath * group root-system
ops rwx action accept
!
aaa authorization datarules datarule 2 namespace * context * keypath /aaa group aaa-r ops
r action accept
!
aaa authorization datarules datarule 3 namespace * context * keypath /aaa group admin-r ops
rwx action reject
!
aaa authorization datarules datarule 4 namespace * context * keypath / group admin-r ops r
action accept
```

The admin CLI for the user works based on the above configurations. The root-system is the group with the highest privilege in System Admin VM. The admin-r group has only read and execute access to all data. The aaa-r group has access only to AAA data. With the introduction of the admin access feature for all users, the NETCONF and gRPC applications can also access the admin data based on the above rules and groups.

How to Allow Read Access to Administration Data for NETCONF and gRPC Clients

NETCONF and gRPC users access the administration data on the router through GET operations as defined by the respective protocols. To allow this read access to administration data for users belonging to admin-r group, you must configure a new command rule specifically for the NETCONF or gRPC client.

Configuration Example

```
Router#admin
sysadmin-vm:0_RP0#configure
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 6
sysadmin-vm:0_RP0(config-cmdrule-6)#context netconf
sysadmin-vm:0_RP0(config-cmdrule-6)#command get
sysadmin-vm:0_RP0(config-cmdrule-6)#group admin-r
sysadmin-vm:0_RP0(config-cmdrule-6)#ops rx
sysadmin-vm:0_RP0(config-cmdrule-6)#action accept
sysadmin-vm:0_RP0(config)#commit
```

Running Configuration

```
aaa authorization cmdrules cmdrule 6
context netconf
command get
group admin-r
ops rx
action accept
!
```