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)**

AAA services

Authentication, authorization, and accounting (AAA) is a security service framework that

- verifies the identity of a user or principal,
- verifies that an authenticated user or principal has permission to perform a specific task, and

- logs sessions and records user-generated or system-generated actions for audit trails.

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

Login authentication command

To configure AAA authentication at login, use the **aaa authentication login** command in global configuration mode.

Admin access for NETCONF and gRPC clients

Admin access for NETCONF and gRPC clients is a system capability that

- maps the task group of an authorized user on the XR virtual machine to a predefined group on the System Admin VM,
- allows NETCONF and gRPC users to access administration information on the router, and
- is enabled by default from Cisco IOS XR Software Release 7.3.2.

NETCONF is an XML-based protocol that uses Secure Shell transport to configure a network. gRPC is an open-source remote procedure call framework.

Administration access before Release 7.3.2

Before Cisco IOS XR Software Release 7.3.2, users who used NETCONF, gRPC, or another configuration interface other than the command-line interface (CLI) to access administration information had to belong to user groups configured on the System Admin VM. Otherwise, the router denied access through the client interface with an UNAUTHORIZED access error message.

By default, the XR VM synchronizes only the first configured user to the System Admin VM. If you delete this first user in the XR VM, the system synchronizes the next user in the **root-lr** group to the System Admin VM only when there are no other users configured in the System Admin VM. Subsequent users are not automatically synchronized to the System Admin VM

Administration access from Release 7.3.2

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

User profile mapping from XR VM to System Admin VM

User profile mapping is an AAA behavior that

- uses predefined groups, command rules, and data rules in the System Admin VM,
- allows users from different System Admin VM groups to access permitted command and data scopes, and
- supports administration data access for NETCONF and gRPC applications based on those groups and rules.

The system creates the predefined groups, command rules, and data rules when the internal AAA process starts or when you create the first user.

Predefined group access

The predefined groups provide these access levels:

- **root-system**: Has the highest privilege in the System Admin VM.
- **admin-r**: Has read and execute access to all data.
- **aaa-r**: Has access only to AAA data.

With the admin access feature, NETCONF and gRPC applications can access administration data that is determined by these rules and groups.

Predefined AAA configuration example

Use the **show running-configuration aaa** command to view the AAA configuration.

```
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
```

Allow read access to administration data for NETCONF and gRPC clients

Create a command rule when users in the **admin-r** group must read administration data through NETCONF or gRPC clients.

NETCONF and gRPC users access administration data on the router through GET operations as defined by each protocol. Configure a command rule if the client context requires read access.

Before you begin

Ensure that the user group exists and that you can access the System Admin configuration mode.

Procedure

Step 1 Enter the system admin configuration mode.

Example:

```
admin
configure
```

Step 2 Use the **aaa authorization cmdrules cmdrule 6** command to create command rule 6.

Example:

```
aaa authorization cmdrules cmdrule 6
```

Step 3 Use the **context netconf** command to set the client context for the command rule.

Example:

```
context netconf
```

This example uses the NETCONF context. Use the context that matches the client type requiring read access.

Step 4 Use the **command get** command to allow the GET operation.

Example:

```
command get
```

Step 5 Use the **group admin-r** command to apply the command rule to the **admin-r** group.

Example:

```
group admin-r
```

Step 6 Use the **ops rx** command to set the operation permissions to read and execute.

Example:

```
ops rx
```

Step 7 Use the **action accept** command to accept requests that match the command rule.

Example:

```
action accept
```

Step 8 Commit the configuration.

Example:

```
commit
```

The command rule allows users in the **admin-r** group to read administration data for the configured client context.

The running configuration includes this command rule:

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

What to do next

Use the **show running-configuration aaa** command to verify the command rule.