Configure AAA

This chapter describes the implementation of the administrative model of *task-based authorization* used to control user access in the software system. The major tasks required to implement task-based authorization involve configuring TACACS+ and RADIUS servers and groups.

About TACACS+

The Terminal Access Controller Access Control System Plus (TACACS+) application is designed to enhance the security of router or network access server by centralizing user validation. It uses AAA commands and can be enabled and configured on NCS 1014 for improved security. TACACS+ provides detailed accounting information and flexible administrative control over user access.

When TACACS+ server is configured and protocol is enabled on the node, the user credentials are authenticated through TACACS+ server. When the user attempts to log into the node, the username and password is forwarded to the configured TACACS+ servers and get authentication status. If the authentication fails through TACACS+ server, the credentials are sent to the node and are authenticated against the node. If the authentication fails against the node, the user is not allowed to log into the node.

Configure TACACS+ Server

Enabling the AAA accounting feature on a switch allows it to track the network services that users are accessing and the amount of network resources they are using. The switch then sends this user activity data to the TACACS+ security server in the form of accounting records. Each record contains attribute-value pairs and is saved on the security server for analysis. This data can be used for network management, client billing, or auditing purposes.

To configure TACACS+ server, perform these steps:

Procedure

Step 1 **configure**

Example:

```
RP/0/0RP0RSP0/CPU0:KEPLER_PSB(config)# configure
```

Enters mode.

Step 2 **aaa accounting exec** *default* **start-stop tacacs+**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)#aaa accounting exec default start-stop group TACACS_ALL
```

Enables TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end.

Step 3 **aaa accounting commands** *default* **start-stop tacacs+**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)#aaa accounting exec default start-stop group TACACS_ALL
```

Defines a default command accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level commands with a stop-only restriction.

Configure TACACS+ Server Groups

Configuring NCS 1014 to use AAA server groups provides a way to group existing server hosts. This allows you to select a subset of the configured server hosts and use them for a particular service. 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.

You can enter one or more **server** commands. The **server** command specifies the hostname or IP address of an external TACACS+ server. Once configured, this server group can be referenced from the AAA method lists (used while configuring authentication, authorization, or accounting).

To configure TACACS+ server groups, perform these steps:

Before you begin

For successful configuration, the external server should be accessible at the time of configuration. When configuring the same IP address for global configuration, server-private parameters are required.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB# configure
```

Enters global configuration XR Config mode.

Step 2 **aaa group server tacacs+** *group-name*

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)# aaa group server tacacs+ tacgroup1
```

Creates an AAA server-group and enters server group subconfiguration mode.

Step 3 **server-private** { *ip-address in IPv4 or IPv6 format*} [**port** *port-number*]

Example:

```
 Router(config-sg-tacacs+)# server-private 10.1.1.1 port 49 key a_secret
```

Configures the IP address of the private TACACS+ server for the group server.

Note
- You can configure a maximum of 10 TACACS+ private servers in a server group.
- If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

Step 4 **key** *string*

Example:

```
 RP/0/RP0/CPU0:ios(config-sg-tacacs+)# key 7 08984B1A4D0C19157A5F57
```

Specifies the authentication and encryption key that is used between the router and the TACACS+ daemon running on the TACACS+ server. If no key string is specified, the global value is used.

Step 5 **timeout** *seconds*

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config-sg-tacacs-private)# timeout 4
```

Configures the timeout value that sets the length of time the authentication, authorization, and accounting (AAA) server waits to receive a response from the TACACS+ server.

Step 6 Repeat steps 3 to 5 for every private server to be added to the server group.

Step 7 **aaa authorization** {**exec**}{**default**} **group** *group-name* **local**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config-sg-tacacs-private)#aaa authorization exec default group
TACACS_ALL local
```

Configures certificate-based authentication for users configured in the TACACS+ server or server groups.

Step 8 **aaa authentication**{**login**}{**default**} **group** *group-name* **local**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config-sg-tacacs-private)#aaa authentication login default group
TACACS_ALL local
```

Specifies the default method list for authentication, and also enables authentication for console in global configuration mode.

Step 9 Use the **commit** or **end** command.

Step 10 (Optional) **show tacacs server-groups**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB# show tacacs server-groups
```

Displays information about each TACACS+ server group configured in the system.

About RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system that provides security against unauthorized access in distributed client/server networks. In Cisco's implementation, RADIUS clients operate on Cisco NCS 1014 and send requests for authentication and accounting to a central RADIUS server that contains all user authentication and network service access information.

Cisco's AAA security paradigm supports RADIUS, which can be used alongside other security protocols like TACACS+, Kerberos, and local username lookup.

Configure RADIUS Server Groups

You can enter one or more **server** commands. The **server** command specifies the hostname or IP address of an external RADIUS server along with port numbers. When configured, this server group can be referenced from the AAA method lists (used while configuring authentication, authorization, or accounting).

You can configure a maximum of 30 servers and private servers each per RADIUS server group. To configure RADIUS server groups, perform these tasks:

Before you begin

Ensure that the external server is accessible at the time of configuration.

Procedure

Step 1 **configure**

Example:

```
RP/0/RP0/CPU0:hostname# configure
```

Enters mode.

Step 2 **aaa group server radius** *group-name*

Example:

```
RP/0/RP0/CPU0(config)# aaa group server radius radgroup1
```

Groups different server hosts into distinct lists and enters the server group configuration mode.

Step 3 **radius-server** {*ip-address*}

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)# radius-server host 192.168.20.0
```

Specifies the hostname or IP address of the RADIUS server host.

Step 4 **auth-port** *port-number*

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)#auth-port 1812
```

Specifies the User Datagram Protocol (UDP) destination port for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.

Step 5 **acct-port** *port-number*

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config)# acct-port 1813
```

Specifies the UDP destination port for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.

Step 6 **key** *string*

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config-radius-host)#key 7 08984B1A4D0C19157A5F57
```

Specifies the authentication and encryption key used between the router and the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used.

The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the **radius-server host** command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Step 7 Repeat steps 4 to 6 for every external radius server to be added to the server group.

—

Step 8 **aaa authentication** {**login**} {**default**} **group** *group-name* **local**

Example:

```
RP/0/RP0/CPU0:KEPLER_PSB(config-radius-host)#aaa authentication login default group radius
 local
```

Specifies the default method list for authentication, and also enables authentication for console in global configuration mode.

Step 9 Use the **commit** or **end** command.

Step 10 **show radius server-groups** [*group-name* [**detail**]]

Example:

```
 RP/0/0RP0RSP0/CPU0:router:hostname# show radius server-groups
```

(Optional) Displays information about each RADIUS server group that is configured in the system.