Chapter 21

Check User Accounts and Permissions

This chapter describes how to check user accounts and permissions. (See Table 45.)

Table 45: Checklist for Checking User Accounts and Permissions

Check User Accounts and Permissions Tasks	Command or Action
Understand User Accounts and Permissions on page 248	
Check Users Logged In To a Router on page 248	show system users
Check for Users in Configuration Mode on page 249	[edit] status
Check the Commands That Users Are Entering on page 250	
1. Configure the Log File for Tracking CLI Commands on page 250	[edit] edit system syslog edit file *filename* set interactive-commands info show commit
2. Display the Configured Log File on page 251	[edit system syslog] run show log *filename*
Log a User Out of the Router on page 252	request system logout *username*
Check When the Last Configuration Change Occurred on page 253	
1. Configure Configuration Change Tracking on page 253	[edit] edit system syslog edit file *filename* set change-log info show commit
2. Display the Configured Log File on page 254	[edit system syslog] run show log *filename*
Force a Message to Logged-In User Terminals on page 255	request message all message "*text*" request message message "*text*" user *username*
Check RADIUS Server Connectivity on page 256	[edit system] show run ping *IP-address*

Understand User Accounts and Permissions

JUNOS software can be configured to support any number of user accounts. Each user account has an access level for which you can define the login name and, optionally, information that identifies the user. After you create an account, the software creates a home directory in the file system for the user.

In this chapter, it is assumed that user accounts and permissions are configured on the router. For more detailed information about creating a user account and configuring permissions, see the *JUNOS Network Management Configuration Guide*.

Check Users Logged In To a Router

Purpose You may need to take note of the users currently logged in to a router.

Action To list all users who are currently logged in to a router, enter the following JUNOS command-line interface (CLI) operational mode command:

```
user@host> show system users
```

Sample Output

```
user@host> show system users
1:49PM PDT up 6:44, 3 users, load averages: 0.00, 0.00, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
jgchan   p0       big.company.net              1:36PM     12 -csh (csh)
user   p1       pink.company.net             1:49PM      - -cli (cli)
blue     p2       level5.company.net               2:30PM      - -cli
```

What It Means The sample output lists information about the users who are currently logged in to a router. There are three users, one of whom has not recently accessed the router. Two of the users are running the CLI, and one is working from the UNIX-level shell (csh). Figure 45 lists and describes the fields in the output of the show system users command.

Table 46: Description of Output Fields for the show system users Command

Field	Description
time and up	Current time, in the local time zone, and how long the router has been operational.
users	Number of users logged in to the router.
load averages	Load averages for the last 1 minute, 5 minutes, and 15 minutes.
USER	Username.
TTY	Terminal through which the user is logged in.
FROM	System from which the user is logged in. A hyphen indicates that the user is logged in through the console.
LOGIN@	Time when the user logged in.
IDLE	How long the user has been idle.
WHAT	Processes that the user is running.

Check for Users in Configuration Mode

Purpose Before you change the configuration or commit a candidate configuration, it is a good idea to check for users in configuration mode.

Action To display users currently editing the configuration, follow these steps:

1. To enter configuration mode, type the following command:

   ```
   user@host> edit
   ```

   For example:

   ```
   user@host> edit
   Entering configuration mode
   ```

2. Enter the following configuration mode command:

   ```
   [edit]
   user@host# status
   ```

   For example:

```
user@host> show system users
4:58PM PST up 5 days,  9:52, 5 users, load averages: 0.01, 0.01, 0.00
USER     TTY      FROM                              LOGIN@  IDLE WHAT
mwazna   p0       bigpunk.juniper.net             4:58PM      - -cli (cli)
jgchan   p1       bigpunk.juniper.net             2:25PM   2:32 -csh (csh)
jgchan   p2       bigpunk.juniper.net             2:35PM   2:18 cli
taffy    p3       bigpunk.juniper.net             3:28PM      5 -cli (cli)
tmauro   p4        bigpunk.juniper.net              4:16PM     37 cli
```

What It Means The sample output lists the users who are currently logged in to the router. Five users are logged in to the router, with one user logged in twice, jgchan. Each user is logged in through a different terminal (TTY—p0, p1, p2, p3, and p4) from the system bigpunk.juniper.net. A hyphen in the FROM field indicates that the user logged in through the console.

Additional information includes the time when the user logged in (LOGIN), the amount of time the user is not active on the router (IDLE), and the processes that the user is running (WHAT). In this example, the users are running the command-line interface (cli) and the UNIX-level shell (csh).

Check the Commands That Users Are Entering

Purpose A common set of operations you can check is when users log in to the router and the CLI commands they issue.

Steps To Take To check the commands that users are entering, follow these steps:

1. Configure the Log File for Tracking CLI Commands on page 250
2. Display the Configured Log File on page 251

Step 1: Configure the Log File for Tracking CLI Commands

Action To configure the log file for tracking CLI commands, follow these steps:

1. In configuration mode, go to the following hierarchy level:

   ```
   [edit]
   user@host# edit system syslog
   ```

2. Configure the log file:

   ```
   [edit system syslog]
   user@host# edit file filename
   ```

   For example:

   ```
   [edit system syslog]
   user@host# edit file cli-commands
   ```

3. Configure the interactive-commands facility and severity level:

   ```
   [edit system syslog filename]
   user@host# set interactive-commands info
   ```

4. Verify the configuration:

   ```
   [edit system syslog]
   user@host# show
   file cli-commands {
       interactive-commands info;
   }
   ```

5. Commit the configuration:

   ```
   user@host# commit
   ```

What It Means The configuration example shows that the log file cli-commands is configured with the interactive-commands facility at the info severity level. Table 47 lists and describes the severity levels.

Table 47: Severity Levels

Severity Level	Description
info	Log all top-level CLI commands, including the configure command, and all configuration mode commands.
notice	Log the configuration mode commands rollback and commit.
warning	Log when any software process restarts.

Step 2: Display the Configured Log File

Action To display the log file in configuration mode, enter the following command:

```
[edit system syslog]
user@host# run show log filename
```

For example:

```
[edit system syslog]
user@host# run show log cli-commands
```

Sample Output

```
[edit system syslog]
user@host# run show log cli-commands
Sep 16 11:24:25  nut mgd[3442]: UI_COMMIT_PROGRESS: commit: signaling 'Syslog
daemon', pid 2457, signal 1, status 0
Sep 16 11:24:25  nut mgd[3442]: UI_COMMIT_PROGRESS: commit: signaling 'SNMP
daemon', pid 2592, signal 31, status 0
Sep 16 11:28:36  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'run
show log cli-commands '
Sep 16 11:30:39  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'run
show log security '
Sep 16 11:31:26  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'run
show log messages '
Sep 16 11:41:21  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'edit
file cli-commands '
Sep 16 11:41:25  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'show
'
Sep 16 11:44:57  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'set
interactive-commands info '
Sep 16 14:32:15  nut mgd[3442]: UI_CMDLINE_READ_LINE: User 'user', command 'run
show log cli-commands '
```

What It Means The sample output shows the CLI commands that were entered since the log file was configured.

Log a User Out of the Router

Purpose Disconnect a user session when that session does not terminate after the user logs out.

Action To log a user out of all terminal sessions on a router, enter the following JUNOS CLI operational mode command:

user@host> **request system logout** *username*

Sample Output

```
user@host> show system users
10:07PM  up 13 days,  1:25, 2 users, load averages: 0.17, 0.05, 0.02
USER     TTY      FROM                              LOGIN@  IDLE WHAT
harry    p0       hpot-lt.cmpy.net                 10:07PM     - -cli (cl
wizard   p1       hpot-lt.cmpy.net                 10:06PM     - -cli (cl

user@host> request system logout user harry

user@host> show system users
10:07PM  up 13 days,  1:25, 1 user, load averages: 0.24, 0.06, 0.02
USER     TTY      FROM                              LOGIN@  IDLE WHAT
wizard   p1       hpot-lt.cmpy.net                 10:06PM     - -cli (cl
```

What It Means The sample output for the first show system users command shows there were two users on the router, harry and wizard. The request system logout user command was issued to log out user harry. Because there is no output to indicate that harry was logged out, the show system users command was issued again to verify that user harry was actually logged out of the router.

Check When the Last Configuration Change Occurred

Purpose When a problem occurs on a router, it is a good idea to check when the last configuration change was made because it may have had some influence on the problem.

Action To check when the last configuration change occurred, follow these steps:

1. Configure Configuration Change Tracking on page 253
2. Display the Configured Log File on page 254

Step 1: Configure Configuration Change Tracking

Action To configure this type of logging, follow these steps:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@host# edit system syslog
```

2. Configure the log file:

```
[edit system syslog]
user@host# edit file filename
```

For example:

```
[edit system syslog]
user@host# edit file mw-configuration-changes
```

3. Configure the change-log facility and severity level:

```
[edit system syslog filename]
user@host# set change-log info
```

4. Verify the configuration:

```
[edit system syslog]
user@host# show
file mw-configuration-changes {
    change-log info;
}
```

5. Commit the configuration:

```
user@host# commit
```

Step 2: Display the Configured Log File

Action To display the log file in configuration mode, enter the following command:

```
[edit system syslog]
user@host# run show log filename
```

For example:

```
[edit system syslog]
user@host# run show log mw-configuration-changes
```

Sample Output

```
[edit system syslog]
user@host# run show log mw-configuration-changes
Sep 17 07:03:22  nut mgd[7793]: UI_CFG_AUDIT_OTHER: User 'root' override:
/config/juniper.conf
Sep 17 07:07:21  nut mgd[2751]: UI_CFG_AUDIT_OTHER: User 'root' set: [interfaces
lo0 unit 0 family inet address 127.0.0.1/32]
Sep 17 07:07:21  nut mgd[2751]: UI_CFG_AUDIT_SET: User 'root' set: [system
domain-name] "englab.company.net" -> "englab.company.net"
Sep 17 07:07:21  nut mgd[2751]: UI_CFG_AUDIT_OTHER: User 'root' set: [system
name-server 172.17.28.101]
Sep 17 07:07:22  nut mgd[2751]: UI_CFG_AUDIT_OTHER: User 'root' set: [system
domain-search] "englab.company.net"
Sep 17 07:07:22  nut mgd[2751]: UI_CFG_AUDIT_OTHER: User 'root' set: [system
domain-search] "company.net"
Sep 17 07:07:22  nut mgd[2751]: UI_CFG_AUDIT_OTHER: User 'root' set: [system
domain-search] "jnpr.net"
```

What It Means The sample output shows the contents of the log file and that the last configuration change was on September 17 at 07:07:22.

Force a Message to Logged-In User Terminals

Purpose You have a scheduled maintenance window or have other important information to convey to users logged in to the router.

Action To force a message to the terminals of logged-in users, enter the following JUNOS CLI operational mode command:

user@host> **request message all message** *"text"*

Sample Output

```
user@host> request message all message "This is an experiment, please be
patient"

Broadcast Message from user@host
        (/dev/ttyp0) at 10:50 PDT...

This is an experiment, please be patient

user@host> request message message "Maintenance window in 10 minutes" user maria
Message from user@host on ttyp0 at 20:27 ...
Maintenance window in 10 minutes
EOF
```

What It Means The sample output shows that the message "This is an experiment, please be patient" was sent to the consoles of all logged-in users, and the message "Maintenance window in 10 minutes" was sent to the console of the logged-in user, maria. For more detailed information about this command, see the *JUNOS Network Management Configuration Guide.*

Syntax

request message all message "*text*"

request message message "*text*" (terminal terminal-name | user user-name)

Check RADIUS Server Connectivity

Purpose It is important to check connectivity to the RADIUS server when attempting to diagnose an authentication problem.

Action To ensure that you can ping the RADIUS server, follow these steps:

1. In configuration mode, go to the following hierarchy level:

```
[edit]
user@host# edit system
```

2. Determine the IP address of the RADIUS server:

```
[edit system]
user@host# show
```

For example:

```
[edit system]
user@host# show
host-name nut;
domain-name englab.company.net;
[...Output truncated...]
radius-server {
    10.10.10.5 {
        secret "$9$14bhIM-VYJGDX7-w2gUD"; # SECRET-DATA
        timeout 5;
        retry 3;
    }
    10.10.10.240 {
        secret "$9$hMKrMXwYoDik-VwgaJHk"; # SECRET-DATA
        timeout 5;
        retry 3;
    }
}
[...Output truncated...]
```

3. Ping the IP address of the RADIUS server:

   user@host# **run ping** *IP address*

   For example:

```
user@host# run ping 10.10.10.5
PING 10.10.10.5 (10.10.10.5): 56 data bytes
64 bytes from 10.10.10.5: icmp_seq=0 ttl=254 time=0.402 ms
64 bytes from 10.10.10.5: icmp_seq=1 ttl=254 time=0.279 ms
64 bytes from 10.10.10.5: icmp_seq=2 ttl=254 time=0.292 ms
64 bytes from 10.10.10.5: icmp_seq=3 ttl=254 time=0.283 ms
64 bytes from 10.10.10.5: icmp_seq=4 ttl=254 time=0.283 ms
^C
— 10.10.10.5 ping statistics —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.271/0.295/0.402/0.036 ms
```

What It Means The sample output shows that the RADIUS server is connected and that the connection is running at a reasonable speed.