Local User Management

Version 20.11.1.2, 23 December 2020

Registered Address	Support	Sales
26, Kingston Terrace, Princeton, New Jersey 08540, United States		
		+91 80 4850 5445
http://www.rtbrick.com	support@rtbrick.com	sales@rtbrick.com

Table of Contents

1. Local User Management

Local User Management enables you to create, manage, and secure the Linux local users and groups through the RBFS configuration. This enables you to manage users and groups in the following environments:

- In the RBFS container only for the virtual platform
- In the RBFS container and on the ONL host for the hardware platforms

1.1. Supported Hardware

The Local User Management is supported on the following hardware:

- Broadcom Qumran-MX

2. Configuring Local user management

2.1. Create New Users

The new users created through local user management will always have a primary group with the same name and ID of the created user. The new user's ID will be allocated within the range of 3000 and 3999.

To create a new user, enter the following command:

set system user <name>

Command arguments

<name>	User name

Example

```
root@rtbrick: cfg> set system user user1
```

You cannot use usernames such as root, wheel, admin, sudo or any of the SMP Linux pre-configured users and groups such as supervisor, operator, reader. Also, a username cannot start with "rtbrick_". If a Linux user with the same username already exists but has an ID outside of the 3000-3999 range then the user creation through the RBFS configuration will fail.

2.2. Assigning Roles to Users

A "role" is an RBFS RBAC construct and it is mapped to a Linux group. and the list of user roles from the RBFS configuration becomes the list of additional Linux groups that the Linux user belongs to. You can assign "roles" to new users. The supervisor, operator, and reader are the pre-defined and pre-configured roles both in Linux and RBFS.

When a user is configured in RBFS under "system users", RBFS/confd validates that the list of user roles only contain roles that are pre-defined or that are configured under "system authorization".

Do not create role names that start with "rtbrick_". Similarly, the following role names are unacceptable:

- root
- wheel
- admin
- sudo

Linux pre-configured users and groups

User Name	Group Name	Privilege
supervisor	supervisor	level 15
operator	operator	level 7-14
reader	reader	level 0-6

For the above-mentioned three users it is possible to change shell, encrypted_password and ssh_keys but nothing else.

To assign a role to a new user, enter the following command:

set system user <name> **role** <role1>

set system user <name> **role** <role2>

Command arguments

<name>	User name
<roles>	Roles of the user (not the primary role)

Example

```
root@rtbrick: cfg> set system user user1 role operator
```

2.3. Configuring Authentication for a New User

Password hashing is used to verify the integrity of your password. If a user is present in the configuration but “encrypted password” is not present, it is considered that the password authentication is disabled for that specified user.

This is also the way to disable password authentication for any of the pre-defined supervisor, operator and reader users, for example by adding a “system users supervisor” configuration section without any “encrypted password” thus causing password authentication for the supervisor user to be disabled.

Even if “encrypted password” is not present, you can still have SSH public keys configured to be able to authenticate.

To create an encrypted password, enter the following command:

```
mkpasswd --method=SHA-512
```

- For supervisor, reader, operator roles, it is possible to change shell, password-hash and ssh-pub-keys.
- To generate an valid encrypted password, use the "mkpasswd --method=SHA-512" command.

To configure authentication using an encrypted-password, enter the following command:

set system user <name> **encrypted-password** <pwd>

set system user <name> **ssh-pub-key** <key1>

Command arguments

<name>	User name
<pwd>	Password string
<key1>	public keys of a user. You can specify multiple ssh-pub-keys.

The password string provided as part of the RBFS configuration needs to be a compatible encrypted password string as defined by the shadow manual page: https://manpages.debian.org/buster/passwd/shadow.5.en.html and by the crypt https://manpages.debian.org/buster/manpages-dev/crypt.3.en.html.

Example

```
root@rtbrick: cfg> set system user user1 password-hash d1ae8a702adedf1243

root@rtbrick: cfg> set system user user1 ssh-pub-key ssh-ed25519
```

2.4. Setting the User Shell

RBFS validates that the shell is one of the following 3 valid options:

- /usr/sbin/nologin
- /bin/bash
- /usr/local/bin/cli

To configure user shell, enter the following command:

set system user <name> **bds-map** <shell>

Command arguments

<name>	User name
<shell>	Name of the shell

Example

```
root@rtbrick: cfg> set system user user1 bds-map bds_test_li
```

2.5. Specifying the Display Name for User Names

The display name allows you to specify a preferred name so that you can easily identify the user. You can change your display name by entering the following command:

set system user <name> **display-name** <display_name>

Command arguments

<name>	User name
<display_name>	Display name to easily identify the user

Example

```
set system user user1 display-name primeuser
```

2.6. Enabling or disabling CLI access

You can control a user's access to the CLI. By default, users will have access to the CLI.

set system user <name> **no-cli-access** < **true** | **false** >

Command arguments

<name>	User name
<true | false>	When the no-cli-access is set to true, the user's access to the CLI is disabled. When the no-cli-access is set to false, the user will be able access the CLI.

Example

```
set system user user1 no-cli-access false
```