



RBFS Installation and Licensing

Version 25.2.1, 23 April 2024

Table of Contents

| | |
|---|----|
| 1. RBFS Installation Overview | 1 |
| 1.1. Understanding RBFS Release Versioning | 2 |
| 1.2. Understanding the RBFS Image Formats | 2 |
| 1.3. Downloading the RBFS Image | 3 |
| 1.4. Installation Modes | 3 |
| 1.5. Self-Service Portal Sign-Up / Sign-In | 4 |
| 1.5.1. Using the Self-Service Portal | 5 |
| 2. RBFS Image Download | 6 |
| 2.1. Generating a Client Certificate | 6 |
| 2.1.1. About the RtBrick APT Tool (rtb-apt) | 7 |
| 2.1.2. Installing the rtb-apt Tool | 7 |
| 2.1.3. Generating a TLS Client Certificate | 8 |
| 2.2. Uploading the Client Certificate to the Self-Service Portal | 9 |
| 2.3. Obtaining Approval and verification of the Client Certificate | 10 |
| 2.4. Identifying and Activating the Image Repository | 11 |
| 2.4.1. Finding the Image Repositories | 11 |
| 2.4.2. Activating an Image Repository | 11 |
| 2.4.3. Verifying the Active Repositories | 12 |
| 2.5. Installing the rtb-image Tool and Verifying Access to Image Stores | 12 |
| 2.5.1. Installing the rtbrick-imgstore Package | 12 |
| 2.5.2. Verifying Access (Authentication) to Image Stores | 13 |
| 2.6. Downloading the ONL Image | 14 |
| 2.6.1. Updating the Local Cached Copy of the Remote Image Store | 15 |
| 2.6.2. Finding the ONL Image | 15 |
| 2.6.3. Pulling the ONL Image | 16 |
| 2.6.4. Displaying the Location of the Downloaded Image | 18 |
| 3. RBFS Manual Installation | 19 |
| 3.1. Prerequisites for Manual Installation | 19 |
| 3.2. Installing RBFS Using a USB Thumb Drive | 19 |
| 3.2.1. Prerequisites | 20 |
| 3.2.2. Installation Procedure | 20 |
| 3.2.3. Manual Configuration of the Management Interface IP | 21 |

| | |
|--|----|
| 3.3. Installing over the Network | 21 |
| 3.3.1. Prerequisites | 22 |
| 3.3.2. Installation Procedure | 22 |
| 3.4. Upgrading RBFS | 24 |
| 3.4.1. Guidelines | 24 |
| 3.4.2. Upgrading RBFS Using a Thumb Drive | 25 |
| 3.4.3. Upgrading RBFS over the Network | 27 |
| 4. RBFS Automated Installation (ZTP) | 29 |
| 4.1. Overview | 29 |
| 4.2. ZTP Workflow | 29 |
| 4.2.1. ZTP Process | 30 |
| 4.3. DHCP Service | 33 |
| 4.4. HTTP Service (Management Server) | 34 |
| 4.4.1. ZTP installation | 34 |
| 4.4.2. ZTP configuration | 36 |
| 4.4.3. ZTP APIs | 37 |
| 4.5. Control Daemon | 37 |
| 4.5.1. Trigger the ZTP process | 37 |
| 4.5.2. Trigger the reinstall | 38 |
| 4.5.3. Trigger Firmware Update | 38 |
| 4.5.4. Management Server URL Discovery | 38 |
| 4.5.5. Request configurations | 39 |
| 4.5.6. Business Events | 39 |
| 4.5.7. Overall Process Flow | 39 |
| 4.6. References | 41 |
| 5. RBFS Licensing | 43 |
| 5.1. Overview | 43 |
| 5.2. Obtaining or Extending Licenses | 43 |
| 5.3. Managing Licenses via Self-Service Portal | 43 |
| 5.3.1. Accessing the license key | 43 |
| 5.3.2. Working with the license list view | 44 |
| 5.3.3. Requesting a new license | 45 |
| 5.3.4. Renewing an existing license | 46 |
| 5.4. Installing a License | 46 |

| | |
|--|----|
| 5.5. Installing Multiple Licenses | 47 |
| 5.6. Viewing the installed license | 47 |
| 5.7. Deleting a License | 48 |
| 5.8. License Expiry..... | 48 |
| 5.8.1. License Validation | 48 |

1. RBFS Installation Overview

RBFS software images are available in the RtBrick Image Store, allowing users to download and install the images for specific roles on supported hardware platforms. All the latest versions of RBFS software images are available in the RtBrick image store. For a complete list of the supported hardware platforms, see [Supported Platforms](#) section of the Platform Guide.



Access to Image Store and Debian package repositories on [/https://releases.rtbrick.com/](https://releases.rtbrick.com/) is restricted through the use of TLS mutual authentication with TLS client certificates.

It is essential to familiarize with the components listed below before beginning the [RBFS Image Download](#) process.

- **RtBrick Image Store:** RBFS software images are stored in the RtBrick Image Store and can be downloaded after meeting licensing requirements.

Image stores containing the RBFS ONL installer images are published on [/https://releases.rtbrick.com/](https://releases.rtbrick.com/) and updated when new image versions are available.

The `rtb-image` command (CLI tool) provided by the `rtbrick-imgstore` package is used to interact with "image stores".

- **RBFS ONL Image:** The RBFS software (NOS) available on the RtBrick Image Store is provided as the RBFS ONL installer image for installation on qualified OCP-compliant switches.
- **RtBrick Tools:** In addition to RBFS software, other RtBrick software tools are delivered in Debian package format compatible with Ubuntu. Currently, the only supported Ubuntu release is 22.04 LTS (Jammy). The software delivered as Debian packages includes a set of CLI tools and/or daemons designed to facilitate working with RBFS containers and the RBFS API. Debian package repositories containing these packages are available at [/https://releases.rtbrick.com/](https://releases.rtbrick.com/) and are updated whenever a new version becomes available.
- **ONIE:** The Open Network Install Environment (ONIE) comes pre-installed on OCP-compliant switches. The ONIE environment is used for installing the RBFS ONL installer image. It provides an environment for installing the RBFS software to run on those switches. For more details about ONIE, please see

<https://opencomputeproject.github.io/onie/>.

1.1. Understanding RBFS Release Versioning

An RBFS release can be defined as a set of software packages (currently, in the Debian package format). However, it is delivered as an image, either a container (LXC/LXD) image or as a complete ONL installation image. The ONL installation image may or may not contain a container image pre-installed in it. An image can be defined as the archived root file system of a Linux OS installation with the needed software packages pre-installed and with a default configuration. In the current context, the terms 'RBFS release' and 'image' are used interchangeably.

RBFS uses the following versioning format:

`<year>.<release>.<minor>[.<fix>][-<label>]`

Examples:

24.3.1

24.3.1.1

24.3.1-candidate.6

In the version example 24.3.1, the first number, "24," represents the year 2024. The second number, "3," indicates the release version, where "1" corresponds to the first release of the year, and this number will be incremented with each subsequent release. The third number, "1," denotes the minor release, which will also be incremented with each future minor release.

RtBrick also uses a four-number versioning format, represented as 24.3.1.1. In this format, the fourth number indicates the bug-fix release. Bug-fix releases are delivered only when necessary and are based on an existing RBFS release, such as 24.3.1. The bug-fix release numbers will also be incremented with each subsequent minor release.

Candidate releases will use a label such as "candidate.6", which will be incremented with each subsequent candidate release.

1.2. Understanding the RBFS Image Formats

RtBrick images delivered through the RtBrick Image Store and the [rtb-image](#) utility

have the following attributes:

- **format**: This is the file format in which the image is packaged and archived. The available format is **onl-installer**.
- **role**: The role inside a network of the device which will be running the image. For example, **multiservice-edge** signifies the full BNG functionality on a single image.
- **platform**: Identifies the hardware platform in which the image can run. For example, **q2a** signifies the switch ASIC Broadcom Qumran-2A.
- **model**: Identifies the hardware model. For example, **s9510-28dc** signifies the hardware model UfiSpace S9510-28DC.
- **ver-range**: Identifies the image version. For example, 24.8.1 signifies the RBFS release 24.8.1.

RtBrick images intended to be installed on supported hardware devices contain **format**, **platform**, and **model** set accordingly to the specific switching hardware.



You can see this using **sudo rtb-image list** command and look for the **Format** column.

1.3. Downloading the RBFS Image

Before you start the installation process, download the RBFS ONL image. For details on downloading the RBFS ONL image, see the **RBFS Image Download** section.

1.4. Installation Modes

After downloading the RBFS software image, you can install it in any of the following modes:

1. **RBFS Manual Installation**: In this mode, you install RBFS ONL installer on a new switch without manually using the ONIE install environment. For detailed step-by-step instructions on the manual installation process, see section **RBFS Manual Installation**.
2. **RBFS Automated Installation**: In this mode, you install RBFS on a new switch by using Zero Touch Provisioning (ZTP). For detailed step-by-step instructions on the automated installation process, see section **RBFS Automated**

Installation (Zero Touch Provisioning).

1.5. Self-Service Portal Sign-Up / Sign-In

RtBrick customers use the self-service portal to request access to the RBFS image download servers and request RBFS licenses. Every user of the Self-Service portal is associated with a specific organization, which is determined by the domain of their company email address. For example, all users with an email address under the domain @rtbrick.com are affiliated with RtBrick. If your email domain is not registered with RtBrick, please contact RtBrick Support for assistance.

The Self-Service portal uses OpenID/Connect to delegate user authentication to third-party authorization services. These authorization services ensure the secure storage of user credentials and provide additional security measures, including two-factor authentication and account recovery options for users who may have forgotten their passwords.

The portal supports three authentication service providers:

- GitHub
- Google
- Microsoft

When a user logs into the portal for the first time, their membership is created. The member will be assigned to an organization based on the domain of their email address. This domain must be a trusted domain, meaning it should be listed in the trusted domains list of exactly one organization.



Attempts to sign up / sign in to the portal with an email address of an untrusted domain will be rejected.

GitHub

GitHub allows users to create new accounts for free. A user must declare their company email address as the public email in their GitHub profile to enable the portal to read the email address during the OpenID/Connect authentication process.



A user cannot sign up / sign in to the portal if the portal is not allowed to read the user's email address.

Google

The user must confirm that the portal has permission to access the email address from their user profile for the sign-up process. After the initial sign-up, subsequent logins will not require the user to grant access to their profile again.

Microsoft

Microsoft allows domain administrators to decide which sites can delegate authentication to the Microsoft's OpenID/Connect authorization services. This adds an additional level of security, because a user can not accidentally share profile data with an untrusted site.

A user will only be prompted for granting the portal access to its profile if the domain administrator has allowed the portal to delegate the login to Microsoft for its organization. In case the portal is not allowed to delegate authentication to Microsoft for the particular organization, the user attempting to sign-up to the portal will be prompted to request a domain administrator to grant the portal access to Microsoft authentication services.

In large enterprises with strict security processes granting the portal access to Microsoft authentication service might take a considerable amount of time. An alternative would be to create a GitHub account.

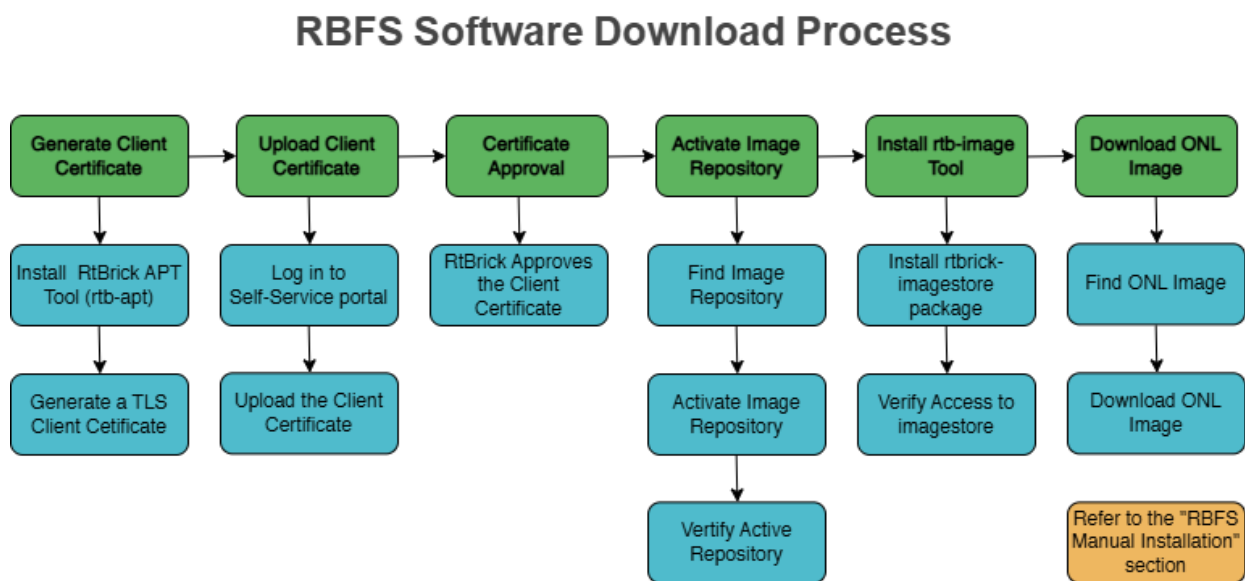
1.5.1. Using the Self-Service Portal

The Self-Service Portal can be used for generating and uploading client certificates. Also, it is required for obtaining new RBFS licenses or extend the existing licenses. For more information, see the [Uploading the Certificate to the Self-Service Portal](#) section of the RBFS Image Download Guide and [Managing Licenses via Self-Service Portal](#) section of the RBFS Licensing Guide.

2. RBFS Image Download

The RtBrick image download functionality enables authenticated users to download and install the RtBrick software (packages or images). Access to *image stores* and *Debian package repositories* on [/https://releases.rtbrick.com/](https://releases.rtbrick.com/) is **restricted** through the use of mutual TLS authentication with TLS client certificates (TLS client certificates can be self-signed).

The diagram below provides an overview of the RBFS software download process.



The process of downloading software involves the following tasks:

- 2.1. Generating a Client Certificate
- 2.2. Uploading the Certificate to the Self-Service Portal
- 2.3. Obtaining Approval and Verification of Client Certificate
- 2.4. Identifying and Activating the Image Repository
- 2.5. Installing the rtb-image Tool and Verifying Access to Image Stores
- 2.6. Downloading the ONL Image

2.1. Generating a Client Certificate

RtBrick provides the `rtb-apt` tool to generate a client certificate. This section contains the following topics:

- 2.1.1. About the RtBrick APT Tool (rtb-apt)
- 2.1.2. Installing the rtb-apt Tool

2..3. Generating a TLS Client Certificate

2.1.1. About the RtBrick APT Tool (rtb-apt)

The **rtb-apt** tool is an **APT** utility application that provides an easier way for managing the system configuration of **RtBrick package repositories** which can be used with the usual **apt** commands to install RtBrick software.

Some RtBrick package repositories require authentication via TLS client certificates and the **rtb-apt** tool provides commands for managing those repositories and the required **apt** authentication configuration.

The **rtb-apt** tool is a statically compiled Linux 64-bit executable file. Currently, it is verified to run on **Ubuntu 22.04**.

2.1.2. Installing the rtb-apt Tool

This section contains the following topics:

2.1.2.1. Prerequisites to Install the rtb-apt Tool

2.1.2.2. Downloading and Installing the rtb-apt Tool

2.1.2.3. Verifying the Version of the rtb-apt Tool

Prerequisites to Install the rtb-apt Tool

Before you install **rtb-apt**, ensure that you have installed the following software:

- GNU Privacy Guard (GPG), which is used by **apt** to validate package repositories. To install GPG, enter the following command:

```
sudo apt install gnupg
```

- HTTPS support for **apt** is required to access the package repositories via HTTPS. To do this, enter the following command:

```
sudo apt install apt-transport-https ca-certificates
```

Downloading and Installing the rtb-apt Tool

The following example shows how to download and install the **rtb-apt** tool. It

shows the URL where the latest version of the **rtb-apt** tool is available for download:

```
~ curl -o /tmp/rtb-apt https://releases.rtbrick.com/_/dl/sw/rtb-apt/latest/linux_amd64/rtb-apt \
&& sudo mv /tmp/rtb-apt /usr/local/bin/ \
&& sudo chown root:root /usr/local/bin/rtb-apt \
&& sudo chmod 0755 /usr/local/bin/rtb-apt
```

Verifying the Version of the rtb-apt Tool

The following example shows the **rtb-apt** tool version. The **rtb-apt** version 2.1.2 or later is required.

```
~ rtb-apt --version
2.1.2
```

2.1.3. Generating a TLS Client Certificate

The following example shows how to generate a TLS client certificate using the **rtb-apt** tool.

```
~ sudo rtb-apt auth generate
A new self-signed TLS client certificate has been generated for this system:

Subject:      CN=bb59a25d-6b38-4f3c-81e0-065e525c8335,OU=rtb-apt
Valid until:  2024-09-06 10:30:26 +0000 UTC

The following additional auto-generated information is included in the certificate
and can be used to uniquely identify this system:

DNS names:      [hostname.example.net]
Email addresses: [root@hostname.example.net user@hostname.example.net]
< ..... >

If you already have a working account on https://portal.rtbrick.com then you can
use the Self-Service section to upload this certificate. If you DO NOT yet have an
account on https://portal.rtbrick.com, send the certificate to your RtBrick
support contact:

-----BEGIN CERTIFICATE-----
MIIHHZCCBYegAwIBAgIRAJcI5pqSK9O+g6yJGB15i7YwDQYJKoZIhvcNAQELBQAw
QTEQMA4GA1UECxmHcnRlJrRw0zofxX4rFcMmJReNqOV0obP5r7TCtnWtAqkFx/
7JJJa
-----END CERTIFICATE-----
```

After generating the TLS Client Certificate, you need to upload it to the **Certificates** section on <https://portal.rtbrick.com>. For details about uploading a certificate, see section [Upload the Certificate to the Self-Service Portal](#) below.

2.2. Uploading the Client Certificate to the Self-Service Portal



If your domain is registered with <https://portal.rtbrick.com>, you will be able to log into your account. If not, reach out to your sales/partner contact to initially have your domain registered with the portal.

To upload a new client certificate, perform the following steps:

1. Log in to [Self-Service Portal](#).

The screenshot shows the RtBrick Customer Portal interface. At the top, there's a green header with the RtBrick logo and 'Customer Portal' text. On the right of the header, there's a 'Self-Service' link (annotated with a red circle 1) and a 'Logout' button. Below the header, on the left, is a navigation menu with 'Certificates' highlighted (annotated with a red circle 2). The main content area is titled 'Certificates' and has a 'Filter by DN' dropdown. Below this is a table of certificates. The table has columns: 'Distinguished Name', 'Description', and 'Until'. Each row shows a certificate with its name, a description, and an expiration date. There are 'Approved' and 'Valid' status buttons for each certificate. On the right side of the table, there are three filter icons: a triangle for 'Show/hide expired or revoked certificates', a circle with a checkmark for 'Show/hide valid certificates', and a circle with a plus sign for 'Show/hide certificates to be approved'. At the bottom right of the table, there's a 'Filter' button and an 'Upload certificate' button (annotated with a red circle 3).

| Distinguished Name | Description | Until |
|--------------------|-------------|-------------|
| rtbrick.com | rtbrick.com | 21-JUN-2024 |
| rtbrick.com | rtbrick.com | 06-SEP-2024 |
| rtbrick.com | rtbrick.com | 16-SEP-2024 |
| rtbrick.com | rtbrick.com | 15-MAI-2024 |

2. Click **Certificates** on the left navigation panel. The Certificates list page appears. The organization's certificate list shows all certificates of that particular organization.

The filter options allows filtering certificates by their distinguished name or lifecycle status.

3. Click the **Upload certificate** button in the organization's certificate list view to upload a new client certificate.

RtBrick Customer Portal

Self-Service Logout

RtBrick

Certificates

Licenses

Members

Resources

Journal

New Certificate

Description

Playground VM

Description for the certificate to distinguish.

Certificate

-----END CERTIFICATE-----

X.509 certificate plain text.

Upload certificate

4. Copy the certificate content in PEM format into the text area. The description field is optional, but it can be used to provide additional information about the certificate.
5. Click the **Upload certificate** button to upload a new certificate.

2.3. Obtaining Approval and verification of the Client Certificate

1. RtBrick reviews and approves the client's certificate that is uploaded on the Self-Service portal.
2. After RtBrick approves the certificate, verify it by entering the command "sudo rtb-apt auth check".

```

~ sudo rtb-apt auth check
Repository: releases/latest/rtbrick-tools ... restricted ... TLS client
certificate accepted

```

If the client certificate is not accepted by RtBrick, the following message will appear. Please contact the customer support team.

```

~ sudo rtb-apt auth check
Repository: releases/latest/rtbrick-tools ... restricted ... TLS client
certificate NOT accepted

```

2.4. Identifying and Activating the Image Repository



You can install additional RtBrick Tools that help simplifying tasks related to debian package repositories. For details see [Installing the rtb-image Tool and Verifying Access to Image Stores](#)

This section contains the following topics:

[2.4.1. Finding the Image Repository](#)

[2.4.2. Activating the Repository](#)

[2.4.3. Verifying Active Repositories](#)

2.4.1. Finding the Image Repositories

To find the available repositories, enter the "sudo rtb-apt repo list" command.

The following example shows how to find the available repositories:

```

~ sudo rtb-apt repo list
Group           Repository      Distribution    Release Active Restricted
releases/latest rtbrick-tools   ubuntu         jammy         No         No
< ..... >

```

2.4.2. Activating an Image Repository

To activate an image repository, enter the "sudo rtb-apt repo activate" command.

The following example shows how to activate the "releases/latest/rtbrick-tools" repository.

```

~ sudo rtb-apt repo activate releases/latest/rtbrick-tools

```

rtb-apt activated repository is added to /etc/apt/sources.list.d/rtbrick.list so that the repository can then be used with commands such as **apt update** and **apt install** to install the RtBrick Debian tool packages.

```

~ cat /etc/apt/sources.list.d/rtbrick.list
deb [arch=amd64 signed-by=/etc/rtbrick/RtBrick-Support.pubkey.asc]
https://releases.rtbrick.com/_/latest/ubuntu/jammy/rtbrick-tools jammy
rtbrick-tools

```

2.4.3. Verifying the Active Repositories

To verify the active repositories, use the "sudo rtb-apt repo list" command. For example in the below output **releases/latest** repository is active because its status is set to YES.

```

~ sudo rtb-apt repo list
Group           Repository      Distribution    Release Active Restricted
releases/latest rtbrick-tools   ubuntu         jammy   Yes     Yes
< ..... >

```

2.5. Installing the rtb-image Tool and Verifying Access to Image Stores

Once the TLS client certificate for the current system is trusted by RtBrick and once RtBrick package repositories have been activated with rtb-apt, the apt commands can be used to install the RtBrick software contained in those package repositories.



rtb-image version 3.11.0 or later is required to correctly work with managed downloads.

This section contains the following topics:

[2.5.1. Installing the rtbrick-imgstore Package](#)

[2.5.2. Verifying access \(authentication\) to Image Stores](#)

2.5.1. Installing the rtbrick-imgstore Package



If you have any existing RtBrick tools packages, it is essential to upgrade to the latest version because some of the RtBrick tools Debian packages have changed and have been upgraded several times. You can remove the existing RtBrick tools package using the below command:

```

apt list --installed | egrep -i rtbrick-imgstore | awk -F '/' '{print $1;}'
| xargs sudo apt remove -y

```


The following shows the installation of the **rtbrick-imgstore** package which provides the **rtb-image** CLI tool.

```

~ sudo apt update
Hit:1 https://releases.rtbbrick.com/_/latest/ubuntu/jammy/rtbrick-tools jammy
InRelease
Hit:3 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:4 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:7 http://archive.ubuntu.com/ubuntu jammy-backports InRelease [109 kB]
Get:8 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:9 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [970 kB]
Get:10 http://archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [979
kB]
< ..... >

```

```

~ sudo apt install rtbrick-imgstore
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  rtbrick-imgstore
0 upgraded, 1 newly installed, 0 to remove and 46 not upgraded.
Need to get 7,731 kB of archives.
After this operation, 26.3 MB of additional disk space will be used.
Get:1 https://releases.rtbbrick.com/_/latest/ubuntu/jammy/rtbrick-tools
jammy/rtbrick-tools amd64 rtbrick-imgstore amd64 3.3.0 [7,731 kB]
Fetched 7,731 kB in 0s (41.4 MB/s)
Selecting previously unselected package rtbrick-imgstore.
< ..... >

```

2.5.2. Verifying Access (Authentication) to Image Stores

The **rtb-image** command (CLI tool) provided by the **rtbrick-imgstore** package is used to interact with "image stores". The "image stores" are used for delivery of RBFS container images and RtBrick ONL installer images.

Similarly to package repositories some of the image stores are *restricted* meaning that they require the client application (**rtb-image** in this case) to authenticate with a TLS client certificate. **rtb-image** re-uses the TLS client certificate already generated by **rtb-apt** for the current system.

This section contains the following topics:

2.5.1. Viewing Available Image Stores

2.5.2. Activating a Restricted Image Store

2.5.3. Verifying Access to Image Stores

Viewing Available Image Stores

The following example shows how to view the available image stores:

```

~ sudo rtb-image stores list

```

| Index | UUID | Name | RemoteURL |
|-----------|--|-----------|-----------|
| Active | Restricted | | |
| 0 | af73c0a6-40e7-4775-b74b-aadafeabe86d | latest | |
| | https://releases.rtbrick.com/_/images/latest | Yes | No |
| 1 | c4c896b0-52c5-4343-8a21-e2ca3ea440f1 | resources | |
| | https://releases.rtbrick.com/_/resources | No | No |
| 2 | | 22.5.1 | |
| | https://releases.rtbrick.com/_/images/22.5.1 | No | No |
| 3 | | 22.6.1 | |
| | https://releases.rtbrick.com/_/images/22.6.1 | No | No |
| 4 | | 22.7.1 | |
| | https://releases.rtbrick.com/_/images/22.7.1 | No | No |
| < > | | | |

Activating a Restricted Image Store

The following example shows how to activate a (possibly restricted) image store:

```

~ sudo rtb-image stores activate 0

```

Verifying Access to Image Stores

If the TLS client certificate for the current system is already trusted by RtBrick, you can use **rtb-image** to download the images. Before downloading the image, you can verify the access to the image stores using the **sudo rtb-image auth check** command.

The following example shows how to verify the access to the image stores:

```

~ sudo rtb-image auth check
Image store: latest (af73c0a6-40e7-4775-b74b-aadafeabe86d) ... restricted ... TLS
client certificate accepted

```

2.6. Downloading the ONL Image

Image stores contain the ONL installer images.

To download ONL installer images, perform the following steps:

2.6.1. Updating the Local Cached Copy of the Remote Image Store

2.6.2. Finding the ONL Image

2.6.3. Pulling the ONL Image

2.6.4. Verifying the Location of the Downloaded Image

2.6.1. Updating the Local Cached Copy of the Remote Image Store

Enter the following command to update the local cached copy of remote image store for RBFS container and ONL images.

```

~ sudo rtb-image update
Local image store cached copy updated to: Store:
/var/cache/rtbrick/imagestores/847c6ecd-df58-462e-a447-38c620a12fe1 Version:
2.4.60878 ValidUntil: 2180-12-25 11:58:44

```

2.6.2. Finding the ONL Image

To find the ONL image, enter the "sudo rtb-image list" command with the following options.

```
-f, --format=FORMAT      Filter images with a specific format. This must be an
exact match of the image format attribute.
-r, --role=ROLE          Filter images with a specific role. This must be an
exact match of the image role attribute.
-p, --platform=PLATFORM  Filter images for a specific platform. This must be
an exact match of the image platform attribute.
-m, --model=MODEL        Filter images for a specific model. This must be an
exact match of the image model attribute.
-v, --ver-range=VER-RANGE Filter images with versions that fall in the provided
version range. See the syntax for version ranges at
```

The following example shows how to find the ONL image details for UfiSpace S9510-28DC Multiservice Edge image.

```
$ sudo rtb-image list --format onl-installer --platform q2a --role multiservice-  
edge --ver-range latest --model s9510-28dc
```

```
Store: /var/cache/rtbrick/imagestores/847c6ecd-df58-462e-a447-38c620a12fe1
Version: 2.4.81241 ValidUntil: 2274-03-18 11:58:44
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
|                                                                                               |
|                                                                                               |
|                                                                                               |
| UUID                                                                                           |
|                                                                                               |
| Role                Model                Platform  Format                Cached ~           |
|-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

```

#####
#####
- d196be23-6cdd-4b50-afd3-fa9ef65532ad 25.1.1-pre-release.9
multiservice-edge      s9510-28dc      q2a      onl-installer  false  -
#####
#####
#####
#####

```

2.6.3. Pulling the ONL Image

There are two options available for downloading the ONL image:

- Option 1: Downloading the image to the current working directory
- Option 2: Downloading the image to a specific directory

Option 1: Downloading the image to the current working directory

To download the ONL image, use the UUID (for example, d196be23-6cdd-4b50-afd3-fa9ef65532ad) of the ONL image in the "sudo rtb-image pull" command. Use the "--here" option to download the image to the current working directory.

```
$ sudo rtb-image pull --here d196be23-6cdd-4b50-afd3-fa9ef65532ad
rtbrick-onl-installer-multiservice-edge-q2a-s9510-28dc-25.1.1-pre-
release.9.d.sha512 240 B / 240 B
[=====] 100.00%
0s
rtbrick-onl-installer-multiservice-edge-q2a-s9510-28dc-25.1.1-pre-release.9.d.asc
833 B / 833 B
[=====]
100.00% 0s
rtbrick-onl-installer-multiservice-edge-q2a-s9510-28dc-25.1.1-pre-release.9.d 1.22
GiB / 1.22 GiB
[=====] 100.00%
31s
rtbrick-onl-installer-multiservice-edge-q2a-s9510-28dc-25.1.1-pre-release.9.d:
decompressing 100 B / 100 B
[=====] 100.00% 27s
```

The image will be downloaded to the current working directory under the `rtbrick-onl-installer` directory as shown below:

```
$ ls -al
total 36
drwxrwxr-x  6 rtbuser rtbuser 4096 Jan  9 05:18 .
drwxr-xr-x 16 rtbuser rtbuser 4096 Jan  9 05:17 ..
drwxr-xr-x  2 rtbuser rtbuser 4096 Jan  9 05:18 rtbrick-onl-installer

$ cd rtbrick-onl-installer/

$ ls -al
```

```
total 1227848
drwxr-xr-x 2 rtbuser rtbuser      4096 Jan  9 05:18 .
drwxrwxr-x 6 rtbuser rtbuser      4096 Jan  9 05:18 ..
-rw-r--r-- 1 rtbuser rtbuser 1257294496 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d
-rw-r--r-- 1 rtbuser rtbuser      833 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.asc
-rw-r--r-- 1 rtbuser rtbuser      233 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.sha512
```

Option 2: Downloading the image to a specific directory

Another method to save the image to a specific directory is shown below:

```
$ sudo rtb-image pull --dst=/home/supervisor 7f52060d-4af4-4ca7-8fe7-3619ee7f6bfb
rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.sha512 233
B / 233 B
[=====]
100.00% 0s
rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.asc 833 B /
833 B
[=====]
] 100.00% 0s
rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d 1.17 GiB /
1.17 GiB
[=====]
100.00% 11s
rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d:
decompressing 100 B / 100 B
[=====] 100.00%
0s
7f52060d-4af4-4ca7-8fe7-3619ee7f6bfb downloaded as /home/supervisor

$ cd /home/supervisor

$ ls -al
total 36
drwxrwxr-x 6 rtbuser rtbuser 4096 Jan  9 05:18 .
drwxr-xr-x 16 rtbuser rtbuser 4096 Jan  9 05:17 ..
drwxr-xr-x 2 rtbuser rtbuser 4096 Jan  9 05:18 rtbrick-onl-installer

$ cd rtbrick-onl-installer/

$ ls -al
total 1227848
drwxr-xr-x 2 rtbuser rtbuser      4096 Jan  9 05:18 .
drwxrwxr-x 6 rtbuser rtbuser      4096 Jan  9 05:18 ..
-rw-r--r-- 1 rtbuser rtbuser 1257294496 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d
-rw-r--r-- 1 rtbuser rtbuser      833 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.asc
-rw-r--r-- 1 rtbuser rtbuser      233 Jan  9 05:18 rtbrick-onl-installer-
accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d.sha512
```

2.6.4. Displaying the Location of the Downloaded Image

The details of the downloaded image can be viewed using the following command:

```
$ sudo rtb-image show d196be23-6cdd-4b50-afd3-fa9ef65532ad

Store: /var/cache/rtbrick/imagestores/847c6ecd-df58-462e-a447-38c620a12fe1
Version: 2.4.81241 ValidUntil: 2274-03-18 11:58:44

UUID:          d196be23-6cdd-4b50-afd3-fa9ef65532ad
Version:       25.1.1-pre-release.9
Extra versions:
Tags:
Creation Date: 2025-02-26 05:48:12 +0000 UTC (3 hours ago)
Role:          multiservice-edge
Platform:      q2a
Model:         s9510-28dc
Format:        onl-installer
Architecture:  amd64
Filename:      rtbrick-onl-installer/rtbrick-onl-installer-multiservice-
edge-q2a-s9510-28dc-25.1.1-pre-release.9.d
FullPath/URL:  /var/cache/rtbrick/imagestores/847c6ecd-df58-462e-a447-
38c620a12fe1/rtbrick-onl-installer/rtbrick-onl-installer-multiservice-edge-q2a-
s9510-28dc-25.1.1-pre-rel...
SHA512:
f1604b22881409f3ec28c9abac6406fad6bc6c7fe52168ff26eb8cb0086c64ae5195a60c83a1420c9a
b5f01b9d2ddba25e9b39d673daf3bd4a4c6dd506079846
Base Image:    00953e7c-151a-4c46-847c-3a3541b01e4a
Embedded Packages: 16
Embedded Images:   1
IsLayered:         false
Cached:            false
ExtractedPath:
```



The `sudo rtb-image show` command displays only symlink information, so you need to copy the source file.

Once the image has been downloaded successfully, proceed to install it using ONIE. For details, see [Installing ONL Manually](#) downloaded

3. RBFS Manual Installation

You can install open network Linux (ONL) manually on an OCP-compliant **bare-metal switch**. The Open Network Install Environment (ONIE) is an open-source utility that provides an installation environment for OCP-compliant bare-metal switches. ONIE is used to install different network operating systems (NOS) on a device.

ONIE provides several methods for locating a Network Operating System (NOS) installer image. Detailed information about these methods can be found in the **ONIE User Guide**. The RBFS ONL image can be installed using any of these methods.



- If you are upgrading your existing RBFS installation, please refer to the section **Upgrading the RBFS Image**.
- When installing ONL, any existing configurations on the switch will be deleted.
- The current RBFS configurations can be retrieved via a REST call from the RESTCONF endpoint. If you have saved the RBFS configuration using this method, you can load it onto the switch through a RESTCONF endpoint. For more information, refer to the following sections of the RtBrick documentation.

Using the Proxy Endpoint

RESTCONF API: Use Cases and Examples

3.1. Prerequisites for Manual Installation

- Ensure that you have downloaded the RBFS ONL image as described in the **RBFS Image Download** section.
- Provision the out-of-band management interface with an IP address either via DHCP or manual configuration (as described in **Manual Configuration of the Management Interface IP**).

3.2. Installing RBFS Using a USB Thumb Drive

This section describes how to install image using a USB thumb drive.

3.2.1. Prerequisites

- Format the USB drive with the FAT32 file system format because we need to place the RBFS image on the root directory of the USB drive.
- Ensure that you have downloaded the RBFS ONL image as described in the [RBFS Image Download](#) section.

3.2.2. Installation Procedure



You can also find instructions for installing via a USB thumb drive in the [ONIE User Guide](#).

To install via USB, insert the USB drive to your computer and assume the USB drive appears as `/dev/sda1` and is mounted at `/media/rtbuser/4356-00B1` on Linux. This may vary depending on your system and operating system.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       29G   16K   29G   1% /media/rtbuser/4356-00B1
```

It is crucial to rename the RBFS ONL image to `onie-installer`, as ONIE only recognizes images with this name at the root of the USB drive.

To install via USB, simply copy the installer image (in this example, the image name is `rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d`) to the root directory of the USB thumb drive, as shown below:

```
$ cp rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d
/media/rtbuser/4356-00B1/onie-installer

$ ls -al /media/rtbuser/4356-00B1/
total 1256820
drwxr-xr-x  2 rtbuser rtbuser      16384 Jan  1  1970 .
drwxr-x---+ 3 root    root         4096 Jan  9 11:49 ..
-rw-r--r--  1 rtbuser rtbuser 1286955159 Jan  9 11:49 onie-installer
```

- Remove the USB drive from your computer and insert it into one of the USB ports on the front or rear panel of your ONIE-enabled device.
- Insert the cable into the console port and connect to the console port of the device.
- Power on the device and reboot it. ONIE will automatically detect the onie-

installer file located at the root of the USB drive and execute it.

```
root@b11-pod1:~# reboot
```

- Wait for the device to show the "login:" prompt after installing the image. You can then log in and check the image version.

3.2.3. Manual Configuration of the Management Interface IP

If DHCP is not available, you need to manually configure the IP address, subnet mask, and default gateway for the device's management port while still logged in from its console port.

1. Identify the management port. Check the device documentation to determine which network interface is designated as the management interface (labeled "ma1").
2. Modify the **ma1** interface network parameters by adding IP address, Netmask, and gateway using your preferred editor. The example below shows how to modify these parameters using the Vim editor.

```
supervisor@onl:/etc/network/interfaces.d $ vim ma1
auto ma1
iface ma1 inet static          <----- modify ma1 inet assignment as static
    address 192.0.2.187        <----- ma1 management interface ip address
    netmask 255.255.255.0      <----- subnet mask
    gateway 192.0.2.10         <----- configure gateway
```

3. Restart the networking service by disabling and enabling the **ma1** interface, as shown in the example below. By default, the default route will point to the gateway IP address.

```
sudo ifdown ma1
sudo ifup ma1
```

3.3. Installing over the Network

For all network installation scenarios, ONIE expects the NOS installer image to be available on the network via HTTP.

3.3.1. Prerequisites

- Ensure that you have downloaded the RBFS ONL image as described in the [RBFS Image Download](#) section.
- Ensure that you have set up an HTTP server that will make available the downloaded images for ONIE to use.

3.3.2. Installation Procedure



You can also find instructions for installing the ONL image over the network in the [ONIE User Guide](#).

To install the ONL image over the network, perform the following steps:



On a fresh box, **ONL prompt** is not available, so skip to **ONIE prompt** section.

ONL prompt section:

Option 1: Manually select ONIE boot mode

1. Connect to the console port
2. Reboot the device

```
root@b11-pod1:~# reboot
```

3. Once the selection menu appears as shown in the selection menu below, select "**ONIE**" and press enter.

```
GNU GRUB version 2.02
```

```
+-----+
| Open Network Linux |
| *ONIE  <----- Select this one |
+-----+
```

```
Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

4. Select "**ONIE: Install OS**" from the next selection menu displayed.

```

                        GNU GRUB  version 2.02
+-----+
|*ONIE: Install OS   <----- Select this one|
| ONIE: Rescue      |
| ONIE: Uninstall OS|
| ONIE: Update ONIE|
| ONIE: Embed ONIE  |
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.

```

5. Wait for the "ONIE:/ #" prompt.

```

NOTICE: ONIE started in NOS install mode.  Install mode persists
NOTICE: until a NOS installer runs successfully.

** Installer Mode Enabled **
ONIE:/ #
ONIE:/ #
ONIE:/ #

```

Provide the URL of the ONL installer image location.

```

ONIE:/ # onie-nos-install http://server.example.net/_/images/latest/rtbrick-onl-
ins
taller/rtbrick-onl-installer-spine-q2c-21.9.1.d

```

Wait until the device displays the "**login:**" prompt after the image upgrade completes. You can then log into the device and verify the image version.

Option 2: Preselect ONIE boot mode

1. Connect to the console port
2. Select ONIE boot mode

```

root@onl>bll-pod1:~ # onl-onie-boot-mode --help
usage: onl-onie-boot-mode [-h] [--onie-only]
                        {install,rescue,uninstall,update,embed,diag,none}

positional arguments:
  {install,rescue,uninstall,update,embed,diag,none}

optional arguments:
  -h, --help            show this help message and exit
  --onie-only           Do not set ONIE boot menu option.
root@onl>bll-pod1:~ #

root@onl>bll-pod1:~ # onl-onie-boot-mode install

```

```
The system will boot into ONIE install mode at the next restart.
root@onl>bl1-pod1:~ #
```



To preselect ONIE boot mode, run the commands using sudo. For example, "sudo onl-onie-boot-mode install."

3. Reboot switch

```
root@onl>bl1-pod1:~ # reboot
```

ONIE prompt section:

You must update the URL of the ONL installer image location as per your specific HTTP server configuration.

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover... done.

ONIE:/ # onie-nos-install http://server.example.net/_/images/latest/rtbrick-onl-
ins
taller/rtbrick-onl-installer-spine-q2c-21.9.1.d

discover: installer mode detected.
Stopping: discover... done.

Info: Attempting http://server.example.net/_/images/latest/rtbrick-onl-
installer/rtbrick-onl-installer-spine-q2c-21.9.1.d ...

Connecting to server.example.net (198.51.100.125)
installer 100% |*****| 1176M 0:00:00 ETA

ONIE: Executing installer: http://server.example.net/_/images/latest/rtbrick-onl-
installer/rtbrick-onl-installer-spine-q2c-21.9.1.d
```

3.4. Upgrading RBFS

This section describes the process for upgrading your current version of RBFS.



If you are performing a fresh installation on an OCP-compliant bare-metal switch, refer to the section [RBFS Manual Installation](#).

3.4.1. Guidelines

- When installing ONL, any existing configurations on the switch will be deleted.
- The current RBFS configurations can be retrieved via a REST call from the

RESTCONF endpoint. If you have saved the RBFS configuration using this method, you can load it onto the switch through a RESTCONF endpoint. For more information, refer to the following sections of the RtBrick documentation.

[Using the Proxy Endpoint](#)

[RESTCONF API: Use Cases and Examples](#)

3.4.2. Upgrading RBFS Using a Thumb Drive

Prerequisites

- Format the USB drive with the FAT32 file system format because we need to place the RBFS image on the root directory of the USB drive.
- Ensure you have downloaded the RBFS ONL image described in the RBFS Image Download section.



You can also find instructions for installing via a USB thumb drive in the [ONIE User Guide](#).

To install via USB, perform the following steps:

- Insert the USB drive to your computer and assume the USB drive appears as `/dev/sda1` and is mounted at `/media/rtbuser/4356-00B1` on Linux. This may vary depending on your system and operating system.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1       29G   16K   29G   1% /media/rtbuser/4356-00B1
```



Ensure that you rename the RBFS ONL image to **onie-installer**, as ONIE only recognizes images with this name at the root of the USB drive.

- Copy the RBFS image (in this example, the RBFS image name is `rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d`) to the root directory of the USB thumb drive, as shown below:

```
$ cp rtbrick-onl-installer-accessleaf-q2c-s9600-102xc-24.9.1-candidate.16.d
/media/rtbuser/4356-00B1/onie-installer
```

```
$ ls -al /media/rtbuser/4356-00B1/
total 1256820
drwxr-xr-x  2 rtbuser rtbuser      16384 Jan  1  1970 .
drwxr-x---+ 3 root    root        4096 Jan  9 11:49 ..
-rw-r--r--  1 rtbuser rtbuser 1286955159 Jan  9 11:49 onie-installer
```

- Remove the USB drive from your computer and insert it into one of the USB ports on the front or rear panel of your ONIE-enabled device.
- Connect to the console port.
- Reboot the device.

```
root@b11-pod1:~# reboot
```

Once the selection menu appears as shown in the selection menu below, select "ONIE" and press enter.

```
GNU GRUB  version 2.02

+-----+
| Open Network Linux                                     |
| *ONIE  <----- Select this one                       |
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

Select "ONIE: Install OS" from the next selection menu displayed.

```
GNU GRUB  version 2.02

+-----+
| *ONIE: Install OS  <----- Select this one           |
| ONIE: Rescue                                              |
| ONIE: Uninstall OS                                       |
| ONIE: Update ONIE                                       |
| ONIE: Embed ONIE                                         |
+-----+

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
```

ONIE will automatically detect the onie-installer file located at the root of the USB drive and execute it.

- Wait until the device displays the "login:" prompt after the image upgrade

completes. You can then log into the device and verify the image version.

The default username is “supervisor”, and the password is “supervisor”.

3.4.3. Upgrading RBFS over the Network

For all network installation scenarios, ONIE expects the NOS installer image to be available on the network via HTTP.

Prerequisites

- Ensure that you have downloaded the RBFS ONL image as described in the RBFS Image Download section.
- Ensure that you have set up an HTTP server that will make available the downloaded images for ONIE to use.

Procedure to Upgrade RBFS over the Network

You can also find instructions for installing the ONL image over the network in the [ONIE User Guide](#).

- Connect to the console port.
- Select ONIE boot mode.

```
root@onl>b11-pod1:~ # onl-onie-boot-mode --help
usage: onl-onie-boot-mode [-h] [--onie-only]
                        {install,rescue,uninstall,update,embed,diag,none}

positional arguments:
  {install,rescue,uninstall,update,embed,diag,none}

optional arguments:
  -h, --help            show this help message and exit
  --onie-only           Do not set ONIE boot menu option.
root@onl>b11-pod1:~ #

root@onl>b11-pod1:~ # onl-onie-boot-mode install
The system will boot into ONIE install mode at the next restart.
root@onl>b11-pod1:~ #
```



To preselect ONIE boot mode, run the commands using sudo. For example, "sudo onl-onie-boot-mode install".

- Reboot switch

```
root@onl>b1l-pod1:~ # reboot
```

ONIE prompt section:

You must update the URL of the ONL installer image location as per your specific HTTP server configuration.

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover... done.

ONIE:/ # onie-nos-install http://server.example.net/_/images/latest/rtbrick-onl-
ins
taller/rtbrick-onl-installer-spine-q2c-21.9.1.d

discover: installer mode detected.
Stopping: discover... done.

Info: Attempting http://server.example.net/_/images/latest/rtbrick-onl-
installer/rtbrick-onl-installer-spine-q2c-21.9.1.d ...

Connecting to server.example.net (198.51.100.125)
installer 100% |*****| 1176M 0:00:00 ETA

ONIE: Executing installer: http://server.example.net/_/images/latest/rtbrick-onl-
installer/rtbrick-onl-installer-spine-q2c-21.9.1.d
```


4. RBFS Automated Installation (ZTP)

4.1. Overview

Zero Touch Provisioning (ZTP) automates the tasks of installing software images. It is a method for setting up and configuring devices automatically. ZTP installs or upgrades the RBFS software image on your hardware platforms without any manual intervention.

ZTP automatically provisions routers newly installed in the network and it is very useful in deploying routers in a large-scale environment as it eliminates much of the manual intervention. ZTP is also used to automate the software upgrade process and help with a high level of network automation.

4.2. ZTP Workflow

A new hardware platform comes pre-installed with the ONIE (Open Network Installation Environment). ONIE is an open-source installation environment that acts as an enhanced boot loader utilizing capabilities in a Linux or BusyBox environment. ONIE allows users and channel partners to install the Network Operating System as part of provisioning.

ONIE requires a management LAN to obtain the configuration and software image information through the management interface. ONIE can access only the management interface. It starts a Dynamic Host Configuration Protocol (DHCP) based discovery process to obtain basic configuration information, such as the management IP address and the URL of the image to install on the bare-metal switch.

Then ONIE pulls the image and boots it.

Even after ONIE boots the image, the switch is not configured. This leads to questions about how to configure the switch.

The RtBrick images come with some pre-installed daemons. The pre-installed Control Daemon (CtrlD) is responsible for the management of the switch, and takes over after the image is activated.

The Control Daemon is responsible for configuring the switch. To do this, the hardware platform must be connected to the DHCP server and the management server through a management LAN.

The management server is responsible for providing the image binaries and the configuration of each device.

In the ZTP, ONIE performs the role of discovering, downloading and activating the image from the image registry.

In essence, the following is the high-level workflow of ZTP process:

ONIE performs the following tasks:

- DHCP discovery
- Image download
- Image activation

Control Daemon performs the following tasks:

- DHCP discovery
- Switch configuration

ONIE allows to automate the firmware update. The image request to the management server is slightly different, and the management server needs to provide the firmware update image that the device vendor provides.

This section provides information about the NOS installation and firmware (FW) update.

4.2.1. ZTP Process

This section provides information about ZTP process. Figure. 1 illustrates the ZTP process at a high level.

The ZTP process is divided into two main parts:

Software Image Discovery and Installation

The ONIE in the device uses information that you have defined on the Dynamic Host Configuration Protocol (DHCP) server to locate the IP address and image

download URL.

- ONIE uses different ways to pull the image from the repository for downloading. In the ZTP process, HTTP is used to pull the image because ONIE conveys the serial number as the HTTP header. This serial number allows the image registry to identify the switch and select the appropriate image.

Along with the serial number, ONIE also sends the **onie-operation** that allows to distinguish between an **os-install** and **onie-update**, and select the correct image for either NOS install or firmware upgrade.

- See the ONIE image discovery for further information (/ONIE/)
- CtrlD configuration discovery and application.
- CtrlD sends DHCPINFORM to request all options required for configuration discovery.
- The configurations are downloaded from the management server (**httpd**) and applied.

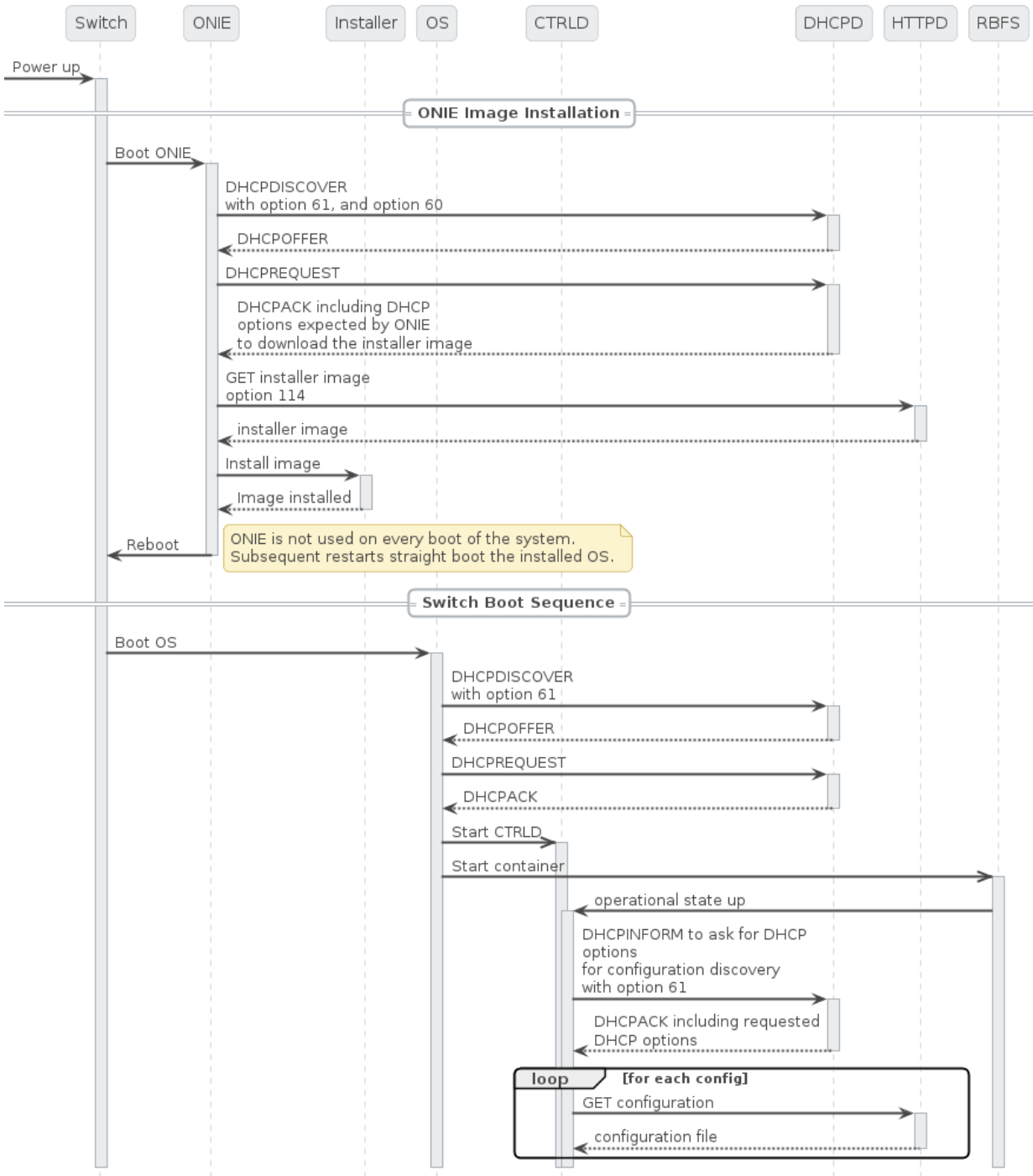


Figure 1. The ZTP Process

Figure 2. depicts the relationship between the fabric, the DHCP server, and the management server.

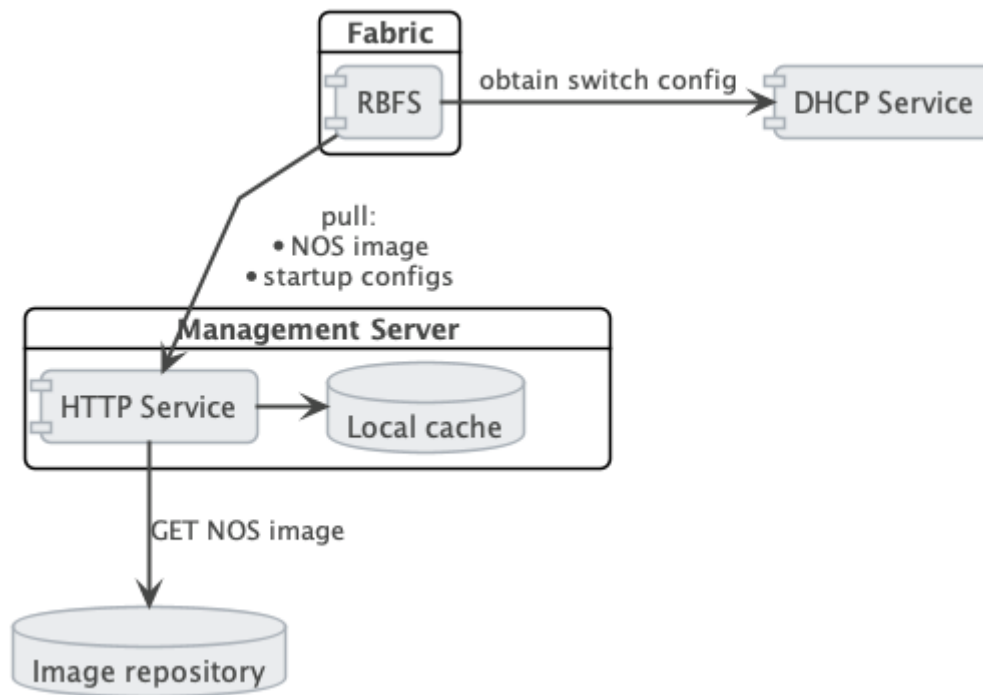


Figure 2. The Management Server Architecture

4.3. DHCP Service

Because of its low set of requirements, the default DHCP server shipped with ubuntu, `isc-dhcp`, is used to run the DHCP service.

The following code shows an example configuration of a DHCP server and hardware box (**`dhcp.conf`**).

dhcp.conf

```

authoritative;
default-lease-time 600;
max-lease-time 720000;

# This is only needed if the version is lower than 4.4
option loader-pathprefix code 210 = text;

subnet 10.0.0.0 netmask 255.255.255.0 {
    range 10.0.0.200 10.0.0.250;
    option routers 10.0.0.138;
    option domain-name-servers 10.0.0.210;
    option domain-name "local";
    host LEAF01 {
        # Identify client by MAC address.
        hardware ethernet 48:65:ee:11:da:85;
        # Identify client by serial number
        option dhcp-client-identifier "\000WLC1C27L00003P2";
        fixed-address 10.0.0.250;
        option host-name LEAF01;
    }
}
  
```

```
# Set DHCP option 114 (default-url) to set the installer image URL.
# ONIE loads the installer image from the specified URL.
option default-url "http://managementserver/ztp/image";
# Set DHCP option 210 (path prefix) to set the configuration base URL.
# CTRLD loads all configuration files from this base URL.
option loader-pathprefix "http://managementserver";
}
}
```

Most of the used options are already predefined in the ISC-DHCP server. You can see the reference under [/ISCKB/](#), the [loader-pathprefix](#) is defined since DHCP 4.4, so if you use an older one, define it as described above.

4.4. HTTP Service (Management Server)

The HTTP daemon ([httpd](#)) is responsible for providing the NOS installer and the configuration files.

Therefore, a self-implemented Golang HTTP server is used, which reads the [ONIE_SERIAL_NUMBER](#) and [ONIE-OPERATION](#) HTTP header and maps them to the NOS/FW installer image download path, and maps the serial number to the ZTP configuration files. For more details about the configuration files, see the following section.

The [ONIE-OPERATION](#) header can have the following values:

- install nos: [os-install](#)
- update firmware: [onie-update](#)

The following sections provide information about the installation and configuration of the server.

4.4.1. ZTP installation

For the installation, you can choose any one of the following two options:

ZTP Installation with the Debian Package

You must perform the following steps for ZTP installation using the Debian package.

- Ensure that you have added the [rtrbick](#) repository to your [apt.sources](#) list and updated the cache.

- Ensure that the port **80** is available and not in use on your device.
- Install the package **rtbrick-fabric-ztp**.
- The package installs a **systemd** service named **rtbrick-fabric-ztp**.
- Ensure that the service is running with **sudo systemctl status rtbrick-fabric-ztp**.
- The default location for the ZTP configuration files is **/var/rtbrick/ztp/configs/** where you need to copy your configuration files.

If you want to override server settings, perform the following:

- Edit the service configuration file **/etc/systemd/system/rtbrick-fabric-ztp.service** and add parameters to the **ExecStart** command.
- Parameter **--addr**: the listen address of the server, default is **0.0.0.0:80**.
- Parameter **--requestTimeout**: the request timeout server in seconds, default is **600**, must possibly be increased depending on the connection speed and image file sizes.
- Parameter **--filePath**: the location for the ZTP configuration files, the default location is **/var/rtbrick/ztp/configs/**.

ZTP Installation as Docker Container

You must perform the following steps for ZTP installation as a docker container.

- Ensure that you have access to the **rtbrick** docker registry.
- Ensure that the port **80** is available and not in use on your device.
- Create a compose file **docker-compose.yml**. The following is a sample compose file.

```
version: '3.3'
services:
  ztp:
    image: 'docker.rtbrick.com/rbms-fabric-ztp:latest'
    container_name: rbms-fabric-ztp
    restart: unless-stopped
    ports:
      - '80:80'
    volumes:
      - './configs:/var/rtbrick/ztp/configs'
```

- The compose setup uses a 'bind mound' method for the ZTP configuration

folder. Therefore, the `docker-compose.yml` must be placed in the same location together with the `./configs` folder for the ZTP configurations. To know the details of the configuration files, see the following sections.

- If required, adapt the compose file for a different image version, port binding or different configuration folder location.
- Start the container using the `docker-compose up -d` command.

4.4.2. ZTP configuration

The HTTP service matches the `ONIE-SERIAL-NUMBER` header to the configuration files. Therefore, the configuration folder should contain a JSON file for the serial number (`<serial_number>.json`) for each supported serial number.

This file contains settings for locations of all additional configuration files that have to be delivered for the specific device and settings for the NOS installer image and the firmware update image.

Example `sample.json` file for a serial number 'sample':

/var/rtbrick/ztp/configs/sample.json

```
{
  "description": "192.168.202.116",
  "ctrlld": "ctrlld.json",
  "ctrlldrbac": "ctrlldrbac.json",
  "startup": "sample_startup.json",
  "accessjwks": "sample_accessjwks.json",
  "apigwd": "sample_apigwd.json",
  "tls": "sample_tls.pem",
  "image": "http://pkg.rtbrick.net/_/images/latest/rtbrick-onl-installer/rtbrick-onl-installer-accessleaf-qmx-20.4.0-g8daily.20200415051734+Bmaster.C059a09ea",
  "update_image": "http://pkg.rtbrick.net/firmwares/onie-firmware-x86_64-ufispace_s9600_32x_ufispace_s9600_64x-r0_v0.3.0.updater"
}
```

Image Location Configuration

For the configuration entries `"image"` and `"update_image"` you have three possibilities:

- Redirect URL: Configuration value must start with `http`, the server redirects the request to download the image from the URL. For example, `"http://pkg.rtbrick.net/_/images/latest/rtbrick-onl-installer/rtbrick-onl-installer-accessleaf-qmx-20.4.0-g8daily.20200415051734+Bmaster.C059a09ea"`

- **Absolute File Location:** config value must start with `/`, can point to any file on the local disk, example `/usr/share/images/rtbrick-onl-installer.img`.
- **Relative File Location:** config value must be a filename and not start with `/`, points to any file in the `<ztpath>/configs/images/` folder, example "rtbrick-onl-installer.img"

4.4.3. ZTP APIs

For information about ZTP REST APIs, refer to the </resources/techdocs/development/api/rbms-apis.html> [ZTP Management Server API].

4.5. Control Daemon

Once the RBFS image is activated by ONIE, Control Daemon (CtrlD) is responsible for executing the remaining tasks and configuring the switch. CtrlD acts as a post-ZTP daemon, it runs after the image is activated.

There are various configuration files that CtrlD can load from a management server and apply to the system.

- **CtrlD config:** This is the base configuration for CtrlD. There the RBMS and Graylog can be specified, but also the authentication and authorization mechanism can be controlled.
- **CtrlD rbac policy:** The Role Based Access Control (RBAC) policy of CtrlD is defined in this configuration file.
- **Startup Config:** This is the file for RBFS switch configuration.
- **TLS pem file:** This file is intended for the API Gateway (ApiGwD). The file is an X509 public/private key file in PEM format defined in the [RFC7468](#).
- **Access JWKS file:** This file is intended for the ApiGwD. The JSON Web Key Set (JWKS) is described in the [RFC 7517](#).

4.5.1. Trigger the ZTP process

The ZTP process in CtrlD is triggered for a specific container (LXC) on the switch. This can be triggered in the following ways.

- By the switch (RBFS Linux container) itself by sending the *operational state up* to

CtrlD.

- By sending a REST request to trigger the ZTP process to CtrlD (/api/v1/ctrlid/ztp/_run).

If 'load-last-config' option is set to true, ZTP is in the disabled state. ZTP is enabled if load-last-config is false.

By default, 'load-last-config' is false and ZTP is enabled. You must set to 'load-last-config' true to disable ZTP.

4.5.2. Trigger the reinstall

The reinstall of a switch can be triggered by sending a POST request to CtrlD (/api/v1/ctrlid/system/_reinstall)

4.5.3. Trigger Firmware Update

The firmware update of a switch can be triggered by sending a POST request to CtrlD (/api/v1/ctrlid/system/_update)

4.5.4. Management Server URL Discovery

CtrlD has to discover the management server URL to download the configuration files from the management server. Therefore, a management interface, that allows sending an DHCPINFORM request to the DHCP server, is defined.

The request contains **DHCP option 60**, that conveys the vendor class identifier "rtbrick", which informs the DHCP server about the vendor information.

The request contains the **DHCP option 61** that conveys the client identifier. The client identifier is either omitted or contains the serial number. The serial number is gathered from the ONIE file system information file [/lib/platform-config/current/onl/onie-info.json](#). If that does not result in a valuable result the following command is executed `dmidecode -s system-serial-number` (see [/RFC2131/](#) and [/RFC2132/](#) for further information).

There are at least two DHCP options requested, **DHCP option 54** that conveys the IP address of the DHCP server (see [/RFC2132/](#) for further information), and **DHCP option 210** that conveys the path prefix for all configuration files (see [/RFC5071/](#) for further information).

If the DHCP option 210 is not returned, CtrlD attempts to read the configurations from the IP address of the ZTP server. Otherwise, CtrlD attempts to read the configurations from the base URL specified in DHCP option 210.

4.5.5. Request configurations

The request to the Management server contains the following HTTP headers:

- ONIE-SERIAL-NUMBER: This serial number is either the onie serial number or empty string.
- CONTAINER-NAME: Container that triggered the ZTP process.
- ELEMENT-NAME: Element name that triggered the ZTP process.
- HOST-NAME: Host name of the device that triggered the ZTP process.



All this information can be used to select the right configurations for the container. This also allows the use of ZTP Configuration Process for virtual environments.

The requested URL:

- CtrlD Config: <management server url>/ztp/config/ctrlD
- CtrlD rbac policy: <management server url>/ztp/config/ctrlDrbac
- Startup Config: <management server url>/ztp/config/startup
- TLS pem file: <management server url>/ztp/config/tls
- Access JWKS file: <management server url>/ztp/config/accessjwks

If any of the file is not found, the process still goes forward.

4.5.6. Business Events

During the ZTP Process log messages are sent to the configured **ztp** graylog endpoint.

For more information, see the switch API documentation.

4.5.7. Overall Process Flow

The following two figures show the CtrlD ZTP process flow.

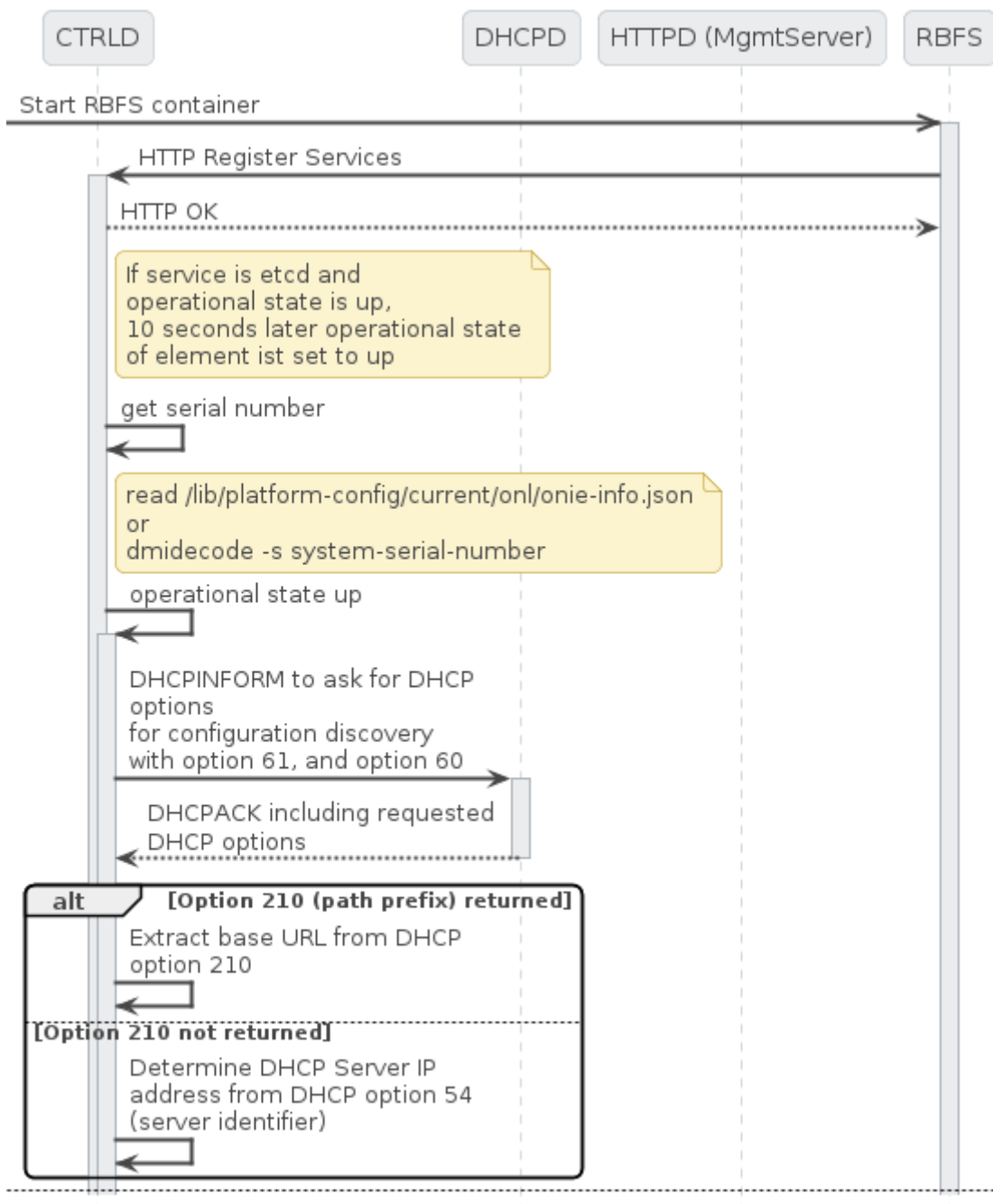


Figure 3. CTRLD ZTP process flow (Part 1/2)

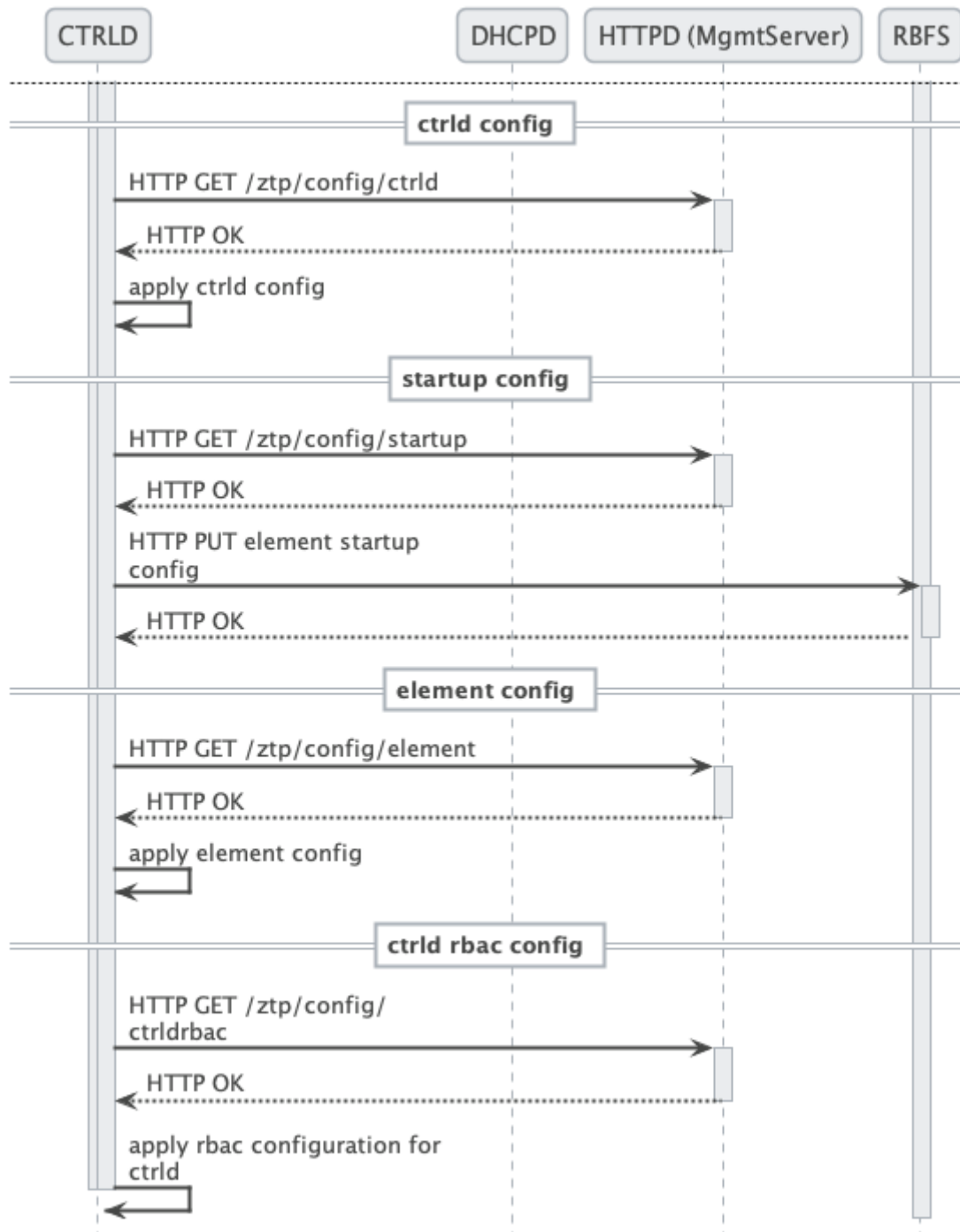


Figure 4. CTRLD ZTP process flow (Part 2/2)

4.6. References

References

| | |
|-----------|---|
| /ONIE/ | Open Network Installation Environment Image Discovery |
| /RFC2131/ | RFC2131 - Dynamic Host Configuration Protocol |
| /RFC2132/ | RFC2132 - DHCP Options and BOOTP Vendor Extensions https://tools.ietf.org/html/rfc2132 |

| | |
|-----------|--|
| /RFC5071/ | RFC5071 - Dynamic Host Configuration Protocol Options Used by PXELINUX |
| /ISCKB/ | ISC Default DHCP Options |

5. RBFS Licensing

5.1. Overview

RBFS Licensing allows you to access the full functionality of your RtBrick FullStack (RBFS) installation. Rtbrick provides a 28-day evaluation license on request. It is not allowed to be used in production. Use a permanent or subscription license that has been purchased through RtBrick Sales. If you want to extend the evaluation period and get additional licenses, contact RtBrick Support.

Without any license installed on your system, you can evaluate RBFS for 7 days. You need to get an evaluation license or purchase an actual license within 7 days to use the full functionality of RBFS.

5.2. Obtaining or Extending Licenses

To obtain new RBFS licenses or extend the existing licenses, go to <https://portal.rtbrick.com/>, click **Licenses** in the left-side menu, and then select the **Request license** link. For details, see the [Managing Licenses via Self-Service Portal](#) section below.

5.3. Managing Licenses via Self-Service Portal

The RtBrick Self-Service portal enables users to view existing license keys, request new licenses, and renew licenses that are about to expire.

5.3.1. Accessing the license key

To access the license key, click on **Licenses** in the left-side menu. This page lists your available licenses. Select the license you want to view.

RtBrick

Certificates

Licenses

Members

Resources

Journal

Licenses

Filter by name

⚠️ ⓘ ⚙️

Filter

Request license

| License Name | Scope | Valid From | Until | Days Left |
|------------------------------------|------------|-------------|-------------|-----------|
| lab Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| lab Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| lab Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| lab_license Valid | Evaluation | 28-FEB-2023 | 04-MÄR-2024 | 134 |
| test-license Valid | Evaluation | 22-OKT-2023 | 11-NOV-2023 | 20 |

The detail view shows the license details including the license key.

RtBrick

Certificates

Licenses

Members


Resources

Journal

test-license evaluation license

Valid

License Key



Copy license key

Name

test-license

Unique license name.

License Scope

Evaluation license

Scope of application the license is intended for.

Valid From

22-OCT-2023

Date from when the license should be valid from.

Valid Until

11-NOV-2023

Date until the license is valid (exclusive)

Valid For (Days)

20

Number of days the license is valid for.

Click **Copy license key** to add the license key to the clipboard.

5.3.2. Working with the license list view

The license list view allows filtering licenses by their names and lifecycle status.

RtBrick

Certificates

Licenses

Members

Resources

Journal

Licenses

lab.*

license name pattern

Show/hide expired

Show/hide approved

Show/hide unapproved requests

⚠️ ⓘ ⚙️

Filter

Request license

| License Name | Scope | Valid From | Until | Days Left |
|--|------------|-------------|-------------|-----------|
| lab eval Expired Expiry acknowledged | Evaluation | 21-JUL-2022 | 18-UNI-2022 | - |
| lab_license Valid | Evaluation | 28-FEB-2023 | 04-MÄR-2024 | 133 |

The name filter is a regular expression. The icons next to the filter allow including or excluding expired licenses, unapproved license requests and approved licenses from the license list.

5.3.3. Requesting a new license

To request a new license, proceed to licenses on the left-side menu and click the **Request license** button to request a new license.

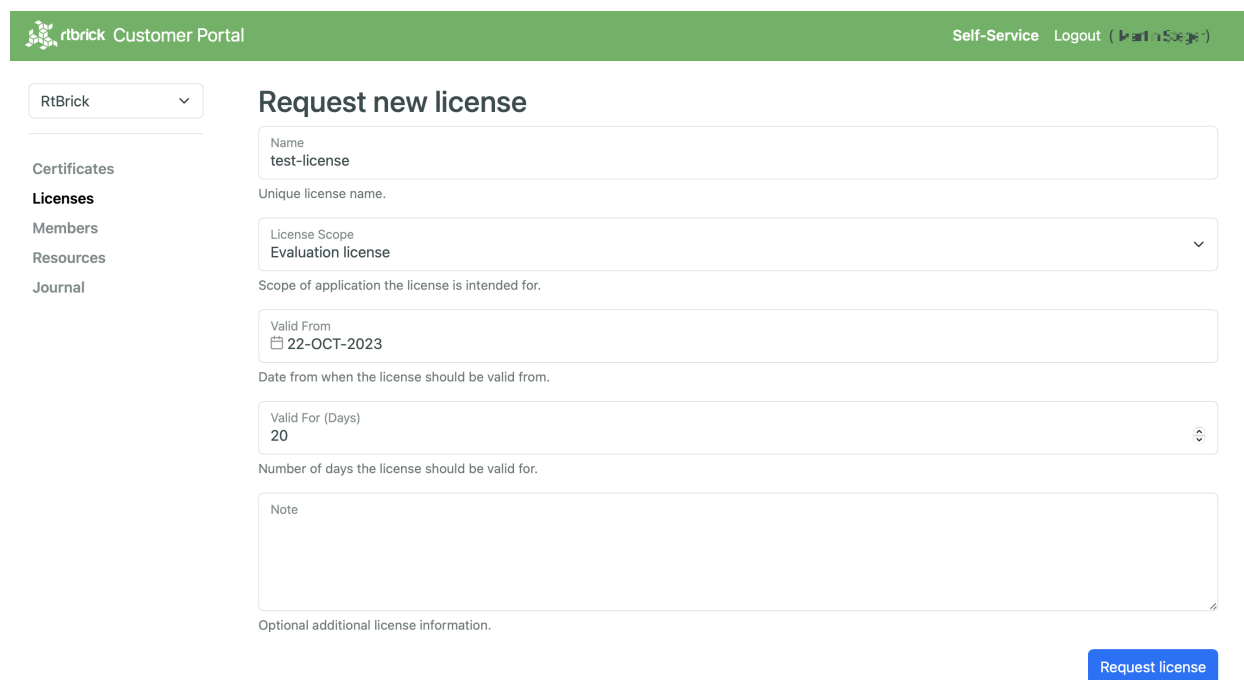


Licenses

Filter by name

| License Name | Scope | Valid From | Until | Days Left |
|------------------------------------|------------|-------------|-------------|-----------|
| RT Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| H Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| JP Valid | Evaluation | 05-JUN-2023 | 02-DEZ-2023 | 41 |
| lab_license Valid | Evaluation | 28-FEB-2023 | 04-MÄR-2024 | 134 |
| test-license Valid | Evaluation | 22-OKT-2023 | 11-NOV-2023 | 20 |

Fill the license request form with all relevant data.



Request new license

Name
test-license

Unique license name.

License Scope
Evaluation license

Scope of application the license is intended for.

Valid From
22-OCT-2023

Date from when the license should be valid from.

Valid For (Days)
20

Number of days the license should be valid for.

Note

Optional additional license information.

Request license

Click the **Request license** button to submit the license request.

5.3.4. Renewing an existing license

The portal reports when a license is about to expire. Click the **Renew** button to create a license request from the current license and copy all relevant data from the license to the license request. Once the license request has been approved, the new license and the license about to expire are both valid to give some time for deploying the new license key to the RBFS instances.

Click the **No renew** button if a license is supposed to expire and shall not be included in the expiry notifications anymore.

5.4. Installing a License

You can install a license by using the RBFS CLI or via the RESTCONF API. You should get a license encrypted string from Rtbrick and configure the same via CLI.



When you upgrade your RBFS installation, the existing license should either get restored via saved configuration or it needs to be installed again.

To install a license, enter the following command:

Syntax

```
set system license <license_key>
```

Example

```
supervisor@rtbrick: cfg> set system license
"eyJzdGFydF9kYXRlIjogMTYxNTg3MTE3MCwgImVuZGF9kYXRlIjogMTYxNTk1NzU3MH0=.Yx/XiFDFRzAt
XPU0aIoh5GqiXa+kOJBWp3LgDeJooVrl88mpPs2ZRMPC+k5HvoZDXvsreqRrqoFR3vk7S2PlqmLxYf0bNB
ly4dlhrloBwwFkFuJaiU/M+ZGPExgILdVyXumI88VYx8m/Z5SxEj0bFQGUy8UHRUYW/Ay8fhPfYe jWuSgp
v3OrIThH9CVjlDmrp/k4yOuHyTz5gLgq4A0h33vB5O99aOIJW5UX4XDKvQqmQX5kytRlR1SseWuAbWKjUd
VOKf2Mk36IbF9/xAKier++LzXESpLMI+MT63AybSDHOBZydoMjLH9C6cPEfGHzWTIBNtT3679Tokf25EK1
Jw=="
```

The following example shows the running configuration.

```
supervisor@rtbrick: cfg> show config system
{
  "rtbrick-config:system": {
    "license": [
```

```
{
  "license-key":
    "eyJzdGFyZD9kYXRlIjogMTYxNTg3MTE3MCwgImVuZGF9kYXRlIjogMTYxNTk1NzU3MH0=.Yx/XiFDFRzAt
    XPUOaIoh5GqiXa+kOJBWp3LgDeJooVr188mpPs2ZRMPC+k5HvoZDXvsreqRrqrFR3vk7S2PlqmLxYf0bNB
    ly4dlhrloBwwFkFuJaiU/M+ZGPExgILdVyXumI88VYx8m/Z5SxEj0bFQGUy8UHRUYW/Ay8fhPfYeJWuSgp
    v3OrIThH9CVjlDmrp/k4yOuHyTz5gLgq4A0h33vB5O99aOIJW5UX4XDKvQqmqX5kytRlR1SseWuAbWKjUd
    VOkf2Mk36IbF9/xAKier++LzXESpLMI+MT63AybSDHOBZydomjLH9C6cPEfGHZWTIBNtT3679Tokf25EK1
    Jw=="
}
```

5.5. Installing Multiple Licenses

You can install multiple licenses. Additional licenses can be installed even when you have existing license(s). The license with the maximum evaluation period will be prioritised over others. When you have multiple evaluation licenses installed, the one that expires later takes higher priority compared to the other licenses.

5.6. Viewing the installed license

Syntax

```
show system license
```

Example

```
root@rtbrick: cfg> show system license
License Validity:
  License 1:
    Start date : Tue Mar 16 05:06:10 GMT +0000 2021
    End date   : Wed Mar 17 05:06:10 GMT +0000 2021
root@rtbrick: cfg>
```

After verifying the validity of the license, the license file will be installed at the following location:

```
/etc/rtbrick/license/rtbrick-license
```

5.7. Deleting a License

To delete a license, enter the following command:

Syntax

```
delete system license <license_key>
```

Example

```
supervisor@rtbrick: cfg> delete system license  
"eyJzdGFydF9kYXRlIjogMTYxNTg3MTE3MCwgImVuZGF9kYXRlIjogMTYxNTk1NzU3MH0=.Yx/XiFDFRzAt  
XPU0aIoh5GqiXa+k0JBWp3LgDeJooVrl88mpPs2ZRMPC+k5HvoZDXvsreqRrqrFR3vk7S2PlqmLxYf0bNB  
ly4dlhrloBwwFkFuJaiU/M+ZGPExgILdVyXumI88VYx8m/Z5SxEj0bFQGUy8UHRUYW/Ay8fhPfYeJWuSgp  
v3OrIThH9CVjlDmrp/k4yOuHyTz5gLgq4A0h33vB5O99aOIJW5UX4XDKvQgmqX5kytRlR1SseWuAbWKjUd  
VOKf2Mk36IbF9/xAKier++LzXESpLMI+MT63AybSDHOBZydoMjLH9C6cPEfGHZWTIBNtT3679Tokf25EK1  
Jw=="
```

5.8. License Expiry

When a license expires, you will not be able to see the operational state of the system via CLI or BDS API.

5.8.1. License Validation

The process of verifying the validity of the software license is known as license validation. If no license is installed, a 7-day evaluation period will be provided. During this time, there will be no license validation. After the evaluation period ends, the system will check and perform license validation every 12 hours. If a valid license is not found, access to the operational state of the system via CLI or BDS API will not be available.

Once a license is installed on the device, it will be validated every 12 hours. If a license is installed within 7 days of evaluation, it is considered the end of the evaluation period, and the license validation will start from that point onward.

Relevant warning or error messages will be generated based on the license validation:

- A warning is generated if the license validity is less than seven days.

- An error message is generated if the license validity is less than one day.
- A critical message is generated if the license has already expired.

Both BDS and file logs are generated for license expiry, and if the Graylog plugin is configured, they are sent to the Graylog. For a list the logs related to license expiry, refer to the section [License Log Messages](#).

To find out the details about the license installed on your system, run the “show system license” command as explained in the section [Viewing the installed license](#).

| Registered Address | Support | Sales |
|---|--|--|
| 40268, Dolerita Avenue Fremont CA 94539 | | |
| +1-650-351-2251 | | +91 80 4850 5445 |
| http://www.rtbrick.com | support@rtbrick.com | sales@rtbrick.com |

©Copyright 2024 RtBrick, Inc. All rights reserved. The information contained herein is subject to change without notice. The trademarks, logos and service marks ("Marks") displayed in this documentation are the property of RtBrick in the United States and other countries. Use of the Marks are subject to RtBrick's Term of Use Policy, available at <https://www.rtbrick.com/privacy>. Use of marks belonging to other parties is for informational purposes only.