Installing Rancher (Docker)

Unit 2.1.1

Installing Rancher

Rancher offers two methods for installation, the sandbox method that uses a single Docker container for everything, and the HA method that installs into RKE.

In addition to not being highly available, the Docker method is also not compatible with the HA method. At the moment there is no supported way to migrate from one to the other, so if you deploy production clusters and later want to migrate to the HA version, you'll have to recreate all of your downstream clusters and configuration.

For that reason, it's important to consider what the Rancher installation is going to become. If you're taking it for a test drive but you think you might use it in production, it's best to start with the HA method and use the single-node install.

Common Parameters

When you start the container, you'll pass it, at the minimum, the following options:

- -d to daemonize
- -p 80:80 -p 443:443 to pass through ports 80 and 443
- --restart=unless-stopped - you want this because the backup and upgrade processes require stopping the container. If you use **always** then you won't ever be able to stop it. You'll have to kill it, and then you can't restart it.

SSL Considerations

You have four options for how to secure access to the Rancher server.

Rancher-Generated Self-Signed Certs

The default option is the easiest and doesn't require anything from you. When Rancher first starts, if there are no SSL configuration options

provided to it, it will generate a self-signed certificate and use this to secure access.

BYO Self-Signed Certs

You can also generate your own certificates and attach them to the container as Docker volumes. You'll need three files:

- Private Key
- Full Chain Certificate
- CA Certificate

BYO Real Certs

If you're running Rancher in a public environment where it's accessed by others, you may want to secure it with real certificates to avoid the security warnings that come from certificates signed by an unknown authority. For this you'll only need two files:

- Private Key
- Full Chain Certificate

The steps are the same as bringing your own self-signed cert, except that you don't need to create a volume for the CA certificate. Rancher will use the CA certificate from the certificate store that ships with the container.

Auto-Generated Let's Encrypt Certificate

Rancher can request a certificate directly from Let's Encrypt via the http-01 challenge format. This works in environments where the Rancher server can be reached from the Internet, either directly, through port-forwarding, or through a public-facing load balancer.

The Rancher server must have a DNS name that points to the IP of the Rancher server host, and it must be reachable on port 80. The challenge can come from anywhere, so port 80 has to be open to the world.

To initiate the certificate request from Let's Encrypt, provide --acme-domain as a startup option to the Rancher server container, ***after*** the container image. This isn't a flag to Docker, so by placing it after the image, the flag is passed to the Rancher server container entrypoint, and Rancher makes the request.

Advanced Options

There are other advanced options you can pass to the container startup process, enabling things like API audit logging, custom CA certificates, modified TLS settings, air gap environments, and persistent data. These are covered in detail in the documentation, but we'll address one of them here.

Bind-Mounted Volume for Persistent Data

Rancher creates a Docker volume for its persistent data and mounts it at /var/lib/rancher inside of the container. If you prefer, you can bind-mount a directory from the host to this location instead. By using a bind-mounted directory, backups and restores are easier than when using the Docker volume.

References

Single-node Docker Installation - https://rancher.com/docs/rancher/v2.x/en/installation/other-installation-methods/single-node-docker/

Advanced Installation Options - https://rancher.com/docs/rancher/v2.x/en/installation/other-installation-methods/single-node-docker/advanced/