



THE QUICK GUIDE FOR LINUX UBUNTU OF

---

# **QVD 4.2 installation**

---

QVD DOCUMENTATION

<documentation@theqvd.com>

May 30, 2022

# Contents

<b>1</b>	<b>Requirements</b>	<b>1</b>
1.1	Operating System . . . . .	1
1.2	Hardware . . . . .	1
1.3	Database . . . . .	1
1.4	HKD . . . . .	1
<b>2</b>	<b>Pre-installation</b>	<b>2</b>
<b>3</b>	<b>Database installation and configuration</b>	<b>3</b>
3.1	Create a user account . . . . .	3
3.2	Create the QVD database . . . . .	3
3.3	Change the PostgreSQL configuration . . . . .	3
<b>4</b>	<b>HKD installation</b>	<b>4</b>
4.1	Basic configuration . . . . .	4
4.2	QVD tables population . . . . .	4
<b>5</b>	<b>Administration tools installation</b>	<b>5</b>
5.1	SSL Configuration . . . . .	5
5.2	API . . . . .	5
5.3	CLI . . . . .	6
5.4	WAT . . . . .	7
<b>6</b>	<b>Basic and indispensable configuration</b>	<b>8</b>
6.1	Network configuration . . . . .	8
6.1.1	Set dnsmasq to be controlled by QVD . . . . .	8
6.1.2	Configure IP forwarding . . . . .	8
6.1.3	Configure a network bridge . . . . .	8
6.1.4	Configure QVD for your network . . . . .	9
6.2	Configure QVD to use the SSL certificates . . . . .	9
6.3	Configure HKD Node . . . . .	9
<b>7</b>	<b>And now, what?</b>	<b>10</b>

# Warnings

**Important**

The current guide contains the necessary commands to make a **mononode** QVD installation, where all the components will be installed into the same machine. In a multinode installation, there will be additional steps and network configuration may be different.

---

**Important**

During the process, some packages will be installed and the network configuration will be affected. It is recommended to use a testing environment.

---

**Important**

For practical purposes, the hostname will be identified with the name **qvdhost**, in your case you must replace it with the name corresponding to your server.

---

# Chapter 1

## Requirements

### 1.1 Operating System

To download Rocky Linux 8.5 you can go directly to the website [rockylinux.org/](https://rockylinux.org/) to its section [downloads](#). It is recommended to use the **minimal** version.

### 1.2 Hardware

- 2 CPU cores
- 2 GB of RAM
- Hard disk at least 20GB

### 1.3 Database

- PostgreSQL 13 or higher

### 1.4 HKD

- [x86\\_64](#) architecture.

## Chapter 2

# Pre-installation

Open the ports that will be necessary to perform the configuration:

```
firewall-cmd --zone=public --add-service=ssh --permanent
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --reload
```

**Note**

If the server has a graphical environment and the tests are going to be carried out on it, it is not necessary to open these ports.

---

```
rpm --import https://www.theqvd.com/packages/key/public.key
dnf install -y yum-utils
yum-config-manager --add-repo https://www.theqvd.com/packages/rockylinux/8.5/QVD-4.2.0/
dnf update -y
```

Install the necessary tools

```
dnf install -y bridge-utils
```

## Chapter 3

# Database installation and configuration

```
dnf install -y https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-x86_64/pgdg- ↵
    redhat-repo-latest.noarch.rpm
dnf install -y postgresql-server postgresql-contrib
/usr/bin/postgresql-setup initdb
systemctl enable --now postgresql
```

### 3.1 Create a user account

```
su - postgres
postgres@qvdhost:~$ createuser -SDRP qvd
Enter password for new role: passw0rd
Enter it again: passw0rd
```

### 3.2 Create the QVD database

```
postgres@qvdhost:~$ createdb -O qvd qvddb
postgres@qvdhost:~$ exit
```

### 3.3 Change the PostgreSQL configuration

Edit the file `/var/lib/pgsql/data/pg_hba.conf` and add the following line **to the beginning** of the section:

#	TYPE	DATABASE	USER	ADDRESS	METHOD
host		qvddb	qvd	127.0.0.1/32	md5

Edit the file `/var/lib/pgsql/data/postgresql.conf` and set the following parameters:

```
listen_addresses = '*'
default_transaction_isolation = 'serializable'
```

Restart PostgreSQL.

```
systemctl restart postgresql
```

## Chapter 4

# HKD installation

```
dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
dnf install -y perl-QVD-HKD
```

Enable HKD service:

```
systemctl enable --now qvd-hkd
```

### 4.1 Basic configuration

Disable SELINUX

```
setenforce 0
sed -i 's/^SELINUX=enforcing$/SELINUX=permissive/' /etc/selinux/config
```

Copy the example configuration file to the `/etc/qvd/` directory, save it as `node.conf`, and modify the permissions on it:

```
cp -v /usr/lib/qvd/config/sample-node.conf /etc/qvd/node.conf
chown root:root /etc/qvd/node.conf
chmod 0640 /etc/qvd/node.conf
```

Edit the file `/etc/qvd/node.conf` and modify/add the following entries:

```
nodename=qvdhost
database.host=127.0.0.1
database.name=qvddb
database.user=qvd
database.password=passw0rd
```

### 4.2 QVD tables population

```
/usr/lib/qvd/bin/qvd-deploy-db.pl
```

## Chapter 5

# Administration tools installation

### 5.1 SSL Configuration

**Note**

If you already have a certificate signed by a third party, you can skip the auto signed certificate creation and use your signed certificate instead.

#### Auto signed certificate creation

```
mkdir /etc/qvd/certs
cd /etc/qvd/certs
```

Generate a private key.

```
openssl genrsa 2048 > key.pem
```

Create a self signed certificate.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key key.pem > cert.pem
```

**Note**

OpenSSL will prompt you to enter the various fields that it requires for the certificate. In the field **Common Name** you must insert the fully qualified domain name of the host that will be running your QVD node.

### 5.2 API

```
dnf install -y perl-QVD-API
```

Create the file `/etc/qvd/api.conf` with the following content:



```
database.host=127.0.0.1
database.name=qvddb
database.user=qvd
database.password=passw0rd
api.user=root
api.group=root
path.api.ssl=/etc/qvd/certs
```

To execute either the CLI as the WAT we must enable the API.

```
systemctl enable --now qvd-api
```

Calling to the endpoint *info* from the browser or using the following command, we will check that the API is working.

```
curl -k https://localhost:443/api/info
```

It should return a JSON with system information.

## 5.3 CLI

```
dnf install -y perl-QVD-Admin4
```

Create the file `/etc/qvd/qa.conf` with the following content:

```
qa.url=https://localhost:443/
qa.tenant=*
qa.login=superadmin
qa.password=superadmin
qa.format=TABLE
qa.insecure=1
```



### Caution

This is just a testing installation guide. Never for be using in production environment. The parameter `qa.insecure` must be replaced by the parameter `qa.ca` with your Authority certification path.

With the following command we will check that qa4 is working.

```
qa4 admin get
```

It should return the two administrators of the system: admin and superadmin.

```
.----+-----+-----+-----+
| id | name          | language | block |
+----+-----+-----+-----+
|  1 | superadmin   | auto     |   10 |
|  2 | admin        | auto     |   10 |
'----+-----+-----+-----+'
Total: 2
```

## 5.4 WAT

```
dnf install -y qvd-wat
```

### Executing the WAT

Visit <https://localhost:443>

Credentials:

- **username:** superadmin@\*
- **password:** superadmin

## Chapter 6

# Basic and indispensable configuration

### 6.1 Network configuration

#### 6.1.1 Set dnsmasq to be controlled by QVD

```
rpm -q dnsmasq
```

If it is not installed:

```
dnf install -y dnsmasq  
[ `systemctl is-enabled dnsmasq.service` == "enabled" ] && systemctl disable dnsmasq. ↔  
service || echo "success disabled"
```

#### 6.1.2 Configure IP forwarding

Edit the file `/etc/sysctl.d/qvd-sysctl.conf` and uncomment the line:

```
net.ipv4.ip_forward=1
```

Execute:

```
sysctl -p
```

#### 6.1.3 Configure a network bridge

Check if the bridge module is loaded with the command:

```
modinfo bridge
```

If it is not loaded, execute:

```
modprobe --first-time bridge
```

Creating the Network Bridge

```
nmcli connection add ifname qvdnet0 connection.type bridge ipv4.addresses 10.3.15.1/24 ipv4 ↔  
.method manual
```

### 6.1.4 Configure QVD for your network

```
qa4 config set tenant_id=-1,key=vm.network.ip.start,value=10.3.15.50
qa4 config set tenant_id=-1,key=vm.network.netmask,value=24
qa4 config set tenant_id=-1,key=vm.network.gateway,value=10.3.15.1
qa4 config set tenant_id=-1,key=vm.network.dns_server,value=10.3.15.254
qa4 config set tenant_id=-1,key=vm.network.bridge,value=qvdnet0
```

## 6.2 Configure QVD to use the SSL certificates

```
qa4 config ssl key=/etc/qvd/certs/key.pem, cert=/etc/qvd/certs/cert.pem
openssl version -d
```

The previous command may return the following response by default:

```
OPENSSLDIR: "/etc/pki/tls"
```



#### Note

If other directory is returned, use it instead `/etc/pki/tls` for the following steps.

The trusted certificates are stored in `/etc/pki/tls/certs`.

```
trusted_ssl_path=/etc/pki/tls/certs
cert_path=/etc/qvd/certs/cert.pem
cert_name=`openssl x509 -noout -hash -in $cert_path`.0
cp $cert_path $trusted_ssl_path/QVD-L7R-cert.pem
ln -s $trusted_ssl_path/QVD-L7R-cert.pem $trusted_ssl_path/$cert_name
```

## 6.3 Configure HKD Node

Now, add the node to the solution by running:

```
qa4 host new name=qvdhost,address=10.3.15.1
```

## Chapter 7

# And now, what?

Should you have any issue, please check the full QVD installation guide.

If you have already done all the steps of this guide, congratulations, you already have a solution QVD installed. Now you should:

- Configure your first OSF
- Install your first image
- Add your first user
- Add a VM for your user

We recommend to you to continue with **the WAT guide** to do these steps.

Once finished, you will only have to connect and try the solution.

Check the **Quick guide to install the QVD client** in your system.

If you have any question or need additional support, visit our website at <http://theqvd.com/> or contact with us at [info@theqvd.com](mailto:info@theqvd.com).