THE QUICK GUIDE FOR LINUX UBUNTU OF

QVD 4.2 installation

QVD DOCUMENTATION

<documentation@theqvd.com>

June 16, 2023

Contents

Warnings

Important
The current guide contains the necessary commands to make a **mononode** QVD installation, where all the components will installed into the same machine. In a multinode installation will exist 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 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 Ubuntu 22.04 you can go directly to the website ubuntu.com to its section downloads or directly from Manual server installation.

1.2 Hardware

- 2 CPU cores
- 4 GB of RAM
- Hard disc at least 32GB

1.3 Database

- PostgreSQL 14 or higher

1.4 HKD

- x86_64 architecture.

Chapter 2

Pre-installation

```
wget -qO - https://www.theqvd.com/packages/key/public.key | sudo apt-key add -
echo "deb http://theqvd.com/packages/ubuntu-jammy QVD-4.2.0 main" > /etc/apt/sources.list.d ↩
    /qvd.list
apt-get update
```

Install firewall

```
apt-get install -y firewalld
```

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

```
firewall-cmd --zone=public --add-service=ssh --permanent
firewall-cmd --zone=public --add-service=https --permanent
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o  ↩
    $NETWORK_INTERFACE -j MASQUERADE -s 10.3.15.0/24
firewall-cmd --add-forward-port=port=8443:proto=tcp:toport=8443:toaddr=10.3.15.1 -- ↩
    permanent
firewall-cmd --reload
```

Important
Be sure to replace **$NETWORK_INTERFACE** with the name of your server's network interface.

Chapter 3

Database installation and configuration

```
apt-get install postgresql
service postgresql start
```

3.1 Create a user account

Login as postgres user:

```
su - postgres
```

Once logged in, create a user and assign a password:

```
createuser -SDRP qvd
```

Note
You will be asked to enter your password and confirm:

```
Enter password for new role: passw0rd
Enter it again: passw0rd
```

3.2 Create the QVD database

Important
The database is created with the postgres user, then the user must be logged out.

```
createdb -O qvd qvddb
exit
```

3.3 Change the PostgreSQL configuration

Edit the file **/etc/postgresql/14/main/pg_hba.conf**

Find the section that contains:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD
```

and add after that line the following:

```
host    qvddb           qvd             127.0.0.0/24            md5
```

Note
Make sure to replace the default network 127.0.0.0/24 with the network that your platform uses.

Edit the file **/etc/postgresql/14/main/postgresql.conf** and set the following parameters:

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

Restart PostgreSQL.

```
service postgresql restart
```

Chapter 4

HKD installation

```
apt-get install perl-qvd-hkd
```

4.1 Basic configuration

Copy the example configuration file to the path `/etc/qvd/`, 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=$NODE_NAME
database.host=localhost
database.name=qvddb
database.user=qvd
database.password=passw0rd
```

Important
Change the variable **$NODE_NAME** to the server name

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

```
apt-get install -y openssl
mkdir /etc/qvd/certs
cd /etc/qvd/certs
```

In **/etc/qvd/certs** generate a private key.

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

Create an auto signed certificate.

```
openssl req -new -x509 -nodes -sha256 -days 3650 -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 $HOST_NAME ($HOSTNAME) which will run your QVD node as shown below.

```
Common Name (e.g. server FQDN or YOUR name) []: $NODE_NAME
```

5.2 API

```
apt-get install -y perl-qvd-api
```

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

```
database.host=localhost
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 or the WAT we must enable the API.

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

```
apt-get 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
```

Important
Be sure to keep the spaces between the variable, the = sign and the value, and make sure there are no blank spaces at the end of the lines.

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

```
apt-get install -y qvd-wat
```

Executing the WAT

Visit https://localhost:443

Credentials:

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

Get lxc version

```
lxc-start --version
```

Once QVD WAT has been accessed, in the Section **Start\QVD Management\WAT Configuration** look for the following parameters, modify and save the values:

- **vm.network.use_dhcp = 0**
- **command.version.lxc = 5.0**

Note
The value obtained from lxc-start --version is the one that will replace the value of **command.version.lxc**.

Chapter 6

Basic and indispensable configuration

6.1 Network configuration

6.1.1 Set dnsmasq to be controlled by QVD

Check if dnsmasq is installed:

```
dpkg -s dnsmasq
```

If it is not installed, run:

```
apt-get 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.conf` and uncomment the line:

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

Execute:

```
sysctl -p
```

6.1.3 Configure a network bridge

Edit the file `/etc/netplan/00-installer-config.yaml` and add the following lines:

```
bridges:
    qvdnet0:
      addresses: [10.3.15.1/24]
      mtu: 1500
      parameters:
          stp: true
          forward-delay: 4
      dhcp4: no
      dhcp6: no
```

the file should be similar to the following:

```
network:
  ethernets:
    $NETWORK_INTERFACE_NAME:
      dhcp4:true
  version: 2
  bridges:
    qvdnet0:
      addresses: [10.3.15.1/24]
      mtu: 1500
      parameters:
          stp: true
          forward-delay: 4
      dhcp4: no
      dhcp6: no
```

Important
$NETWORK_INTERFACE_NAME must match the network interface name

Note
In case the file already exists, the **bridges:** section must be aligned with the **ethernets:** section

Note
The range **10.3.15.0/24** should be unique within your infrastructure.

Generate and apply changes

```
netplan generate
netplan apply
```

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: "/usr/lib/ssl"

Note
If other directory is returned, use it instead `/usr/lib/ssl` for the following steps.

The trusted certificates are stored in `/usr/lib/ssl/certs`.

```
trusted_ssl_path=/usr/lib/ssl/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=$(echo $HOSTNAME),address=10.3.15.1
```

Edit the /etc/default/grub file and add/modify the following line:

```
GRUB_CMDLINE_LINUX="cgroup_enable=memory swapaccount=1 systemd.unified_cgroup_hierarchy= ↩
    false"
```

run:

```
/usr/sbin/update-grub2
```

Enable the HKD service:

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

And restart the server

```
shutdown -r now
```

Chapter 7

And now, what?

If you have had any problem, consult the **Complete 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 that you follow the **WAT Guide** to perform 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.