THE QUICK GUIDE FOR LINUX UBUNTU OF

QVD 4.2 installation

QVD DOCUMENTATION

<documentation@theqvd.com>

July 28, 2020

Contents

Product QVD 4.2 Virtual Deckard
QVD Docs Team <documentation@theqvd.com>
Legal notice

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.

Requirements

Database

- 2 CPU cores
- 2 GB of RAM
- PostgreSQL 10 or higher

HKD

- x86_64 architecture.

Pre-installation

```
root@qvdnode:~# yum install yum-utils
root@qvdnode:~# rpm --import https://www.theqvd.com/packages/key/public.key
root@qvdnode:~# yum-config-manager --add-repo http://theqvd.com/packages/centos/7.8/QVD ↩
    -4.2.0/
root@qvdnode:~# yum update
```

For commercial packages:

```
root@qvdnode:~# echo "[QVD-4.2.0]" > /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "name=QVD-4.2.0" >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "baseurl=http://$USER:$PASSWORD@theqvd.com/commercial-packages/centos ↩
    /7.8/QVD-4.2.0/" | sed 's/@\(.*@\)/%40\1/' >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "enabled=1" >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# yum update
```

Note
$USER and $PASSWORD are the credentials received when the suscription is purchased.

Database installation and configuration

```
root@qvdnode:~# yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-7- ↩
    x86_64/pgdg-redhat-repo-latest.noarch.rpm
root@qvdnode:~# yum install postgresql10-server postgresql10-contrib
root@qvdnode:~# /usr/pgsql-10/bin/postgresql-10-setup initd
root@qvdnode:~# systemctl enable --now postgresql-10.service
```

Create a user account

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

Create the QVD database

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

Change the PostgreSQL configuration

Edit the file **/var/lib/pgsql/10/data/postgresql.conf** and set the following parameters:

```
listen_addresses = '0.0.0.0'
default_transaction_isolation = 'serializable'
```

Edit the file **/var/lib/pgsql/10/data/pg_hba.conf** and add the following line **to the beginning**:

```
host qvddb qvd 192.168.0.0/24 md5
```

Note
Make sure to replace the default network 192.168.0.0/24 with the network that your platform uses.

Restart PostgreSQL.

```
root@qvdnode:~# systemctl restart postgresql-10.service
```

Installation of the HKD

```
root@qvdnode:~# yum install perl-QVD-HKD
```

Basic configuration

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

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

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

path.log=/var/log/qvd
log.filename=${path.log}/qvd.log
log.level=INFO
```

QVD tables population

```
root@qvdnode:~# /usr/lib/qvd/bin/qvd-deploy-db.pl
```

Administration tools installation

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

```
root@qvdnode:~# yum install openssl
root@qvdnode:~# mkdir /etc/qvd/certs
root@qvdnode:~# cd /etc/qvd/certs
```

Generate a private key.

```
root@qvdnode:/etc/qvd/certs# openssl genrsa 2048 > key.pem
```

Create an auto signed certificate.

```
root@qvdnode:/etc/qvd/certs# 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.

API

```
root@qvdnode:~# yum install perl-QVD-API
```

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

```
database.host=qvdnode
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 start the API.

```
root@qvdnode:~# 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.

```
root@qvdnode:~# curl -k https://localhost:443/api/info
```

It should return a JSON with system information.

CLI

```
root@qvdnode:~# yum install 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.

```
root@qvdnode:~# qa4 admin get
```

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

WAT

```
root@qvdnode:~# yum install QVD-WAT
```

Executing the WAT

Visit https://localhost:443

Credentials:

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

Basic and indispensable configuration

Network configuration

Set dnsmasq to be controlled by QVD

- Firstly, check dnsmasq status service:

```
root@qvdnode:~# systemctl is-enabled dnsmasq
```

- By default, it starts the process that is executed as a daemon in the background, so you should avoid it starting automatically. This is done with the following commands:

```
root@qvdnode:~# systemctl stop dnsmasq
root@qvdnode:~# systemctl disable dnsmasq
```

Configure IP forwarding

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

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

Execute:

```
root@qvdnode:~# sysctl -p
```

Configure a network bridge

- Install the necessary tools

```
root@qvdnode:~# yum install bridge-utils -y
```

- Verify that the bridge module is loaded with the command:

```
root@qvdnode:~# modinfo bridge
```

  - If it is not loaded, run:

```
root@qvdnode:~# modprobe --first-time bridge
```

- To create the interface configuration file to be used for QVD run:

```
root@qvdnode:~# vi /etc/sysconfig/network-scripts/ifcfg-qvdnet0
```

– Add the following lines:

```
DEVICE="qvdnet0"
BOOTPROTO="static"
IPADDR="10.3.15.1"
NETMASK="255.255.255.0"
ONBOOT="yes"
TYPE="Bridge"
NM_CONTROLLED="no"
```

- **Firewall Configuration in CentOS**

  Enable NAT for container navigation, for this, 2 zones are required, internal and external. The internal zone will use the container network 10.3.15.0/24 or whatever chosen with interface **qvdnet0** previously created. And the external zone should use the interface **eth0** (replace with external network interface), for this we do the following:

```
root@qvdnode:~# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING ↩
     -o eth0 -j MASQUERADE -s 10.3.15.0/24
root@qvdnode:~# firewall-cmd --change-interface=eth0 --zone=external --permanent
root@qvdnode:~# firewall-cmd --set-default-zone=external
root@qvdnode:~# firewall-cmd --change-interface=qvdnet0 --zone=internal --permanent
```

  You must make a "port forwarding" of port 8443 in external network to port 8443 in internal network to the bridge ip qvdnet0 10.3.15.1.

```
root@qvdnode:~# firewall-cmd --zone=external --add-forward-port=port=8443:proto=tcp:toport ↩
    =8443:toaddr=10.3.15.1 --permanent
```

  Open in the external network the connection ports that QVD uses, 8443 to connect to the sessions and 443 to connect to WAT.

```
root@qvdnode:~# firewall-cmd --add-port=8443/tcp --permanent --zone=external
root@qvdnode:~# firewall-cmd --add-service=https --permanent --zone=external
```

  Reload the rules to apply the changes made:

```
root@qvdnode:~# firewall-cmd --complete-reload
```

- Restart the network service:

```
root@qvdnode:~# systemctl restart network
```

Configure QVD for your network

```
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.use_dhcp,value=0
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.ip.start,value=10.3.15.50
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.netmask,value=24
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.gateway,value=10.3.15.1
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.dns_server,value=10.3.15.254
root@qvdnode:~# qa4 config set tenant_id=-1,key=vm.network.bridge,value=qvdnet0
```

Configure QVD to use the SSL certificates

```
root@qvdnode:~# qa4 config ssl key=/etc/qvd/certs/key.pem, cert=/etc/qvd/certs/cert.pem
root@qvdnode:~# 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`.

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

Configure HKD node

- Now, add the node to the solution by running:

```
root@qvdnode:~# qa4 host new name=qvdnode,address=10.3.15.1
```

- And restart HKD service:

```
root@qvdnode:~# systemctl restart qvd-hkd
```

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

Note
We recommend to you to continue with the **Web Administration Tool (WAT) Manual** to do these steps.

Once finished, you will only have to:

- Connect and try the solution
- Check the **Quick Installation Guides** to choose your client and install it on your system.

–

If you have any questions or need additional support, visit our Web Site or contact us.

Main Menu