THE QUICK GUIDE FOR LINUX CENTOS OF

QVD 4.1 installation

QVD DOCUMENTATION

<documentation@theqvd.com>

November 5, 2018

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.

Chapter 1

Requirements

Database

- 2 CPU cores

- 2 GB of RAM

- PostgreSQL 9.3 or higher

HKD

- x86_64 architecture.

Chapter 2

Pre-installation

```
# rpm --import https://www.theqvd.com/packages/key/public.key
# yum install yum-utils
# yum-config-manager --add-repo http://theqvd.com/packages/centos/7.2/QVD-4.1.0/
# yum update
```

For commercial packages:

```
# rpm --import https://www.theqvd.com/packages/key/public.key
# echo "[QVD-4.1.0]" > /etc/yum.repos.d/QVD-4.1.0.repo
# echo "name=QVD-4.1.0" >> /etc/yum.repos.d/QVD-4.1.0.repo
# echo "baseurl=http://$USER:$PASSWORD@theqvd.com/commercial-packages/centos/7.2/QVD ↩
   -4.1.0/" | sed 's/@\(.*@\)/%40\1/' >> /etc/yum.repos.d/QVD-4.1.0.repo
# echo "enabled=1" >> /etc/yum.repos.d/QVD-4.1.0.repo
# yum update
```

Note

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

Chapter 3

Database installation and configuration

```
# yum install https://download.postgresql.org/pub/repos/yum/9.3/redhat/rhel-7-x86_64/pgdg- ↩
    centos93-9.3-2.noarch.rpm
# yum install postgresql93-server postgresql93-contrib
# /usr/pgsql-9.3/bin/postgresql93-setup initdb
# systemctl start postgresql-9.3
```

Chapter 4

HKD installation

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

Create a user account

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

Create the QVD database

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

Change the PostgreSQL configuration

Edit the file /var/lib/pgsql/9.3/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.

Edit the file /var/lib/pgsql/9.3/data/postgresql.conf and set the following parameters:

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

Restart PostgreSQL.

```
root@myserver:~# systemctl restart postgresql-9.3
```

Basic configuration

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

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

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

QVD tables population

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

Chapter 5

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@myserver:~# yum install openssl
root@myserver:~# mkdir /etc/qvd/certs
root@myserver:~# cd /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 that will be running your QVD node.

API

```
root@myserver:~# yum install 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 start the 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.

CLI

```
root@myserver:~# 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.

```
# qa4 admin get
```

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

WAT

```
# yum install qvd-wat
```

Executing the WAT

Visit https://localhost:443

Credentials:

- **username**: superadmin@*

- **password**: superadmin

Chapter 6

Basic and indispensable configuration

Network configuration

Set dnsmasq to be controlled by QVD

```
# rpm -q dnsmasq
```

If it is not installed:

```
# yum install dnsmasq
# chkconfig dnsmasq off
```

Configure IP forwarding

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

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

Execute:

```
# sysctl -p
```

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
```

Install the needed tools

```
# yum install bridge-utils -y
```

To create the configuration file of the interface that will be used for QVD, execute:

```
# 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"
GATEWAY="10.3.15.10"
DNS1=10.3.15.10
ONBOOT="yes"
TYPE="Bridge"
NM_CONTROLLED="no"
```

Edit the configuration file of the adapter that will be used as bridge. Replace *eth0* by yours.

```
# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Place the following information:

```
DEVICE=eth0
TYPE=Ethernet
BOOTPROTO=none
ONBOOT=yes
NM_CONTROLLED=no
BRIDGE=qvdnet0
```

Restart the network:

```
# systemctl restart network
```

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
```

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
```

Configure HKD Node

Edit file /etc/qvd/node.conf with this contents:

```
nodename = node1
database.host = localhost
database.name = qvddb
database.user = qvd
database.password = passw0rd
```

Now, add the node to the solution by running:

```
# qa4 host new name=node1,address=10.3.15.1
```

And start HKD service:

```
# systemctl start qvd-hkd
```

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 fist 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.