THE QUICK GUIDE FOR LINUX SLES 12 OF

QVD 4.2 installation

QVD DOCUMENTATION

<documentation@theqvd.com>

May 30, 2022

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

Requierements

1.1 Operating System

To download SLES 15 SP3 you can go directly to the website www.suse.com to its section downloads.

> **Important**
> To download the iso it is necessary to have a suse account, you can register with a free account which will allow you to download an evaluation copy for a period of 60 days (The duration of this period depends directly on SUSE).

1.2 Hardware

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

1.3 Databases

- PostgreSQL 13.6 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.

Add the repository to download the commercial packages, a username and password will be requested:

```
rpm --import https://www.theqvd.com/packages/key/public.key
zypper ar http://theqvd.com/commercial-packages/sles/15SP3/QVD-4.2.0 QVD-4.2
 User Name: []
 password: []
zypper ref
```

Note
$USER and $PASSWORD are the credentials received when purchasing the subscription.

Note
It is possible that you have to provide your installation disk to finish the operation.

Install the necessary tools

```
zypper install -y bridge-utils
```

Chapter 3

Database installation and configuration

```
zypper install -y postgresql-server
systemctl start postgresql.service
```

Enable the postgres service to start at server startup

```
systemctl enable --now postgresql.service
```

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.service
```

Chapter 4

Installation of HKD

```
zypper install -y perl-QVD-HKD
```

4.1 Basic configuration

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
```

Enable HKD service:

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

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

```
zypper install openssl
mkdir /etc/qvd/certs
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.

5.2 API

```
zypper 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 or 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

```
zypper 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 verify 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

```
zypper install -y qvd-wat
```

Executing the WAT

Visit https://localhost:443

Credentials:

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

Chapter 6

Basic and essential configuration

6.1 Network configuration

6.1.1 Set dnsmasq to be controlled by QVD

```
rpm -q dnsmasq
```

If it is not installed:

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

6.1.2 Configure IP forwarding

Look in the **.conf** files inside `/etc/sysctl.d/` and add/uncomment the line:

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

Execute:

```
sysctl -p
```

6.1.3 Configure a network bridge

Open Yast and go to System → Network Settings

```
yast
```

images/QVDInstallationSLES_Yast_step1.png

- Select Add option.

images/QVDInstallationSLES_Yast_step2.png

Select the type **Bridge** and Select **Next**

images/QVDInstallationSLES_Yast_step3.png

Set the following options:

General tab

- Configuration name: **qvdnet0**
- Activate device\Activate device: **During boot**
- Firewall zone\Assign interfaces… **public**
- Maximum Transmission Unit (MTU)\Define MTU: **0**

images/QVDInstallationSLES_Yast_step4.png

Address Tab

- (x) Statically assigned IP address
- IP address: **10.3.15.1**
- Subnet mask: **/24**
- Hostname: **qvdhost**

images/QVDInstallationSLES_Yast_step5.png

Select Next * The network device will be automatically configured in a few seconds. * Choose Ok to save the configuration. * Exit from Yast

Execute the following commands too:

```
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING -o eth0 -j  ↩
    MASQUERADE -s 10.3.15.0/24
firewall-cmd --change-interface=eth0 --zone=external --permanent
firewall-cmd --set-default-zone=external
firewall-cmd --change-interface=qvdnet0 --zone=internal --permanent
firewall-cmd --zone=external --add-forward-port=port=8443:proto=tcp:toport=8443:toaddr ↩
    =10.3.15.1 --permanent
```

Note
The range **10.3.15.0/24** should be unique within your infrastructure. NOTE: change the interface eth0 for the one corresponding to your server

Bring up the network bridge:

```
ifup qvdnet0
```

6.1.4 Configura 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/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=/etc/ssl
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

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 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.