



THE QUICK GUIDE FOR LINUX SLES 12 OF

QVD 4.1 installation

QVD DOCUMENTATION

<documentation@theqvd.com>

November 5, 2018

Contents

1	Requiereements	1
1.1	Database	1
1.2	HKD	1
2	Pre-installation	2
3	HKD installation	3
4	Database installation and configuration	4
4.1	Create a user account	4
4.2	Create the QVD database	4
4.3	Change the PostgreSQL configuration	4
4.4	Basic configuration	5
4.5	QVD tables population	5
5	Administration tools installation	6
5.1	SSL Configuration	6
5.2	API	6
5.3	CLI	7
5.4	WAT	7
6	Basic and indispensable configuration	8
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	Configura QVD for your network	11
6.2	Configure QVD to use the SSL certificates	11
6.3	Configure HKD Node	12
7	And now, what?	13

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.

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
# zypper ar http://theqvd.com/packages/sles/12SP1/QVD-4.1.0 QVD
# zypper ref
```

**Note**

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

For commercial packages:

```
# rpm --import https://www.theqvd.com/packages/key/public.key
# zypper ar http://theqvd.com/commercial-packages/sles/12SP1/QVD-4.1.0 QVD
User Name: $USER
Password: $PASSWORD
# zypper ref
```

**Note**

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

Chapter 3

HKD installation

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

Chapter 4

Database installation and configuration

```
root@myserver:~# zypper install postgresql-server
# service postgresql start
```

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/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/data/postgresql.conf` and set the following parameters:

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

Restart PostgreSQL.

```
root@myserver:~# service postgresql restart
```

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:~# zypper 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:~# zypper 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.

```
service qvd-api start
```

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:~# zypper 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

```
# zypper 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:

```
# zypper install dnsmasq
# chkconfig dnsmasq off
```

Configure IP forwarding

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

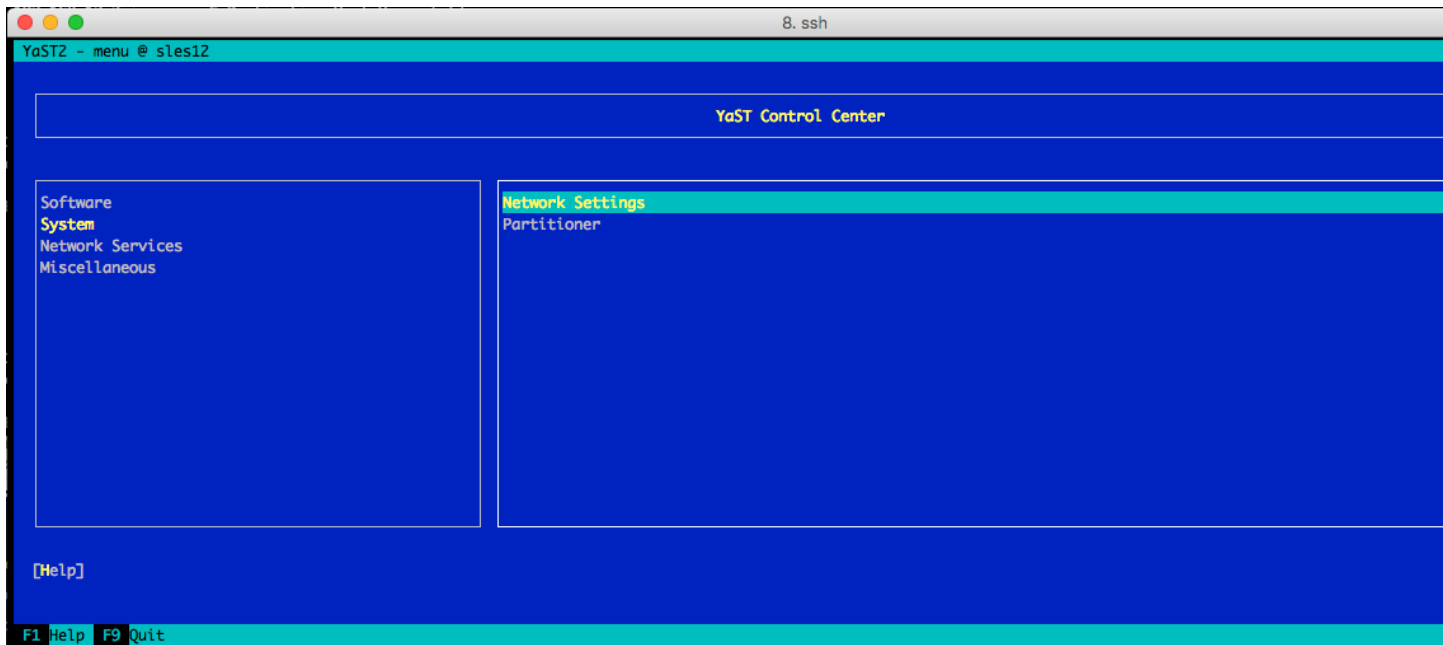
```
net.ipv4.ip_forward=1
```

Execute:

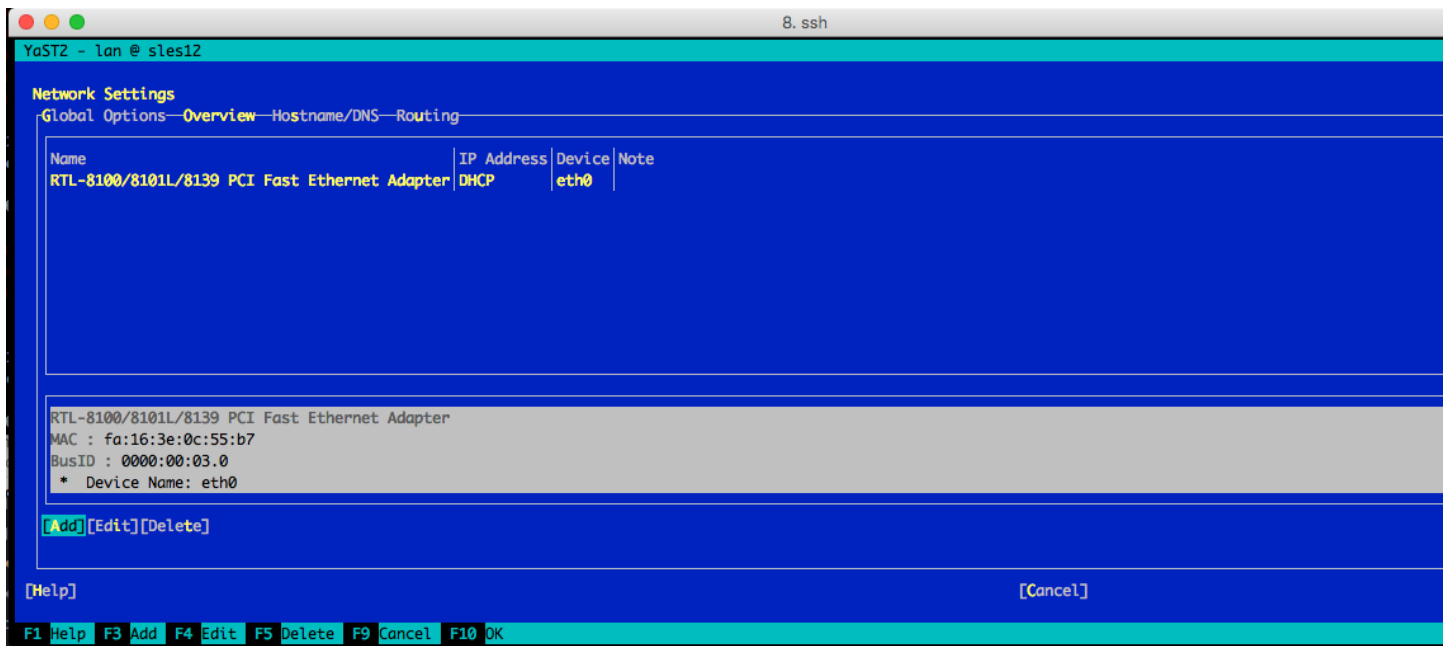
```
# sysctl -p
```

Configure a network bridge

Open Yast and go to System → Network Settings

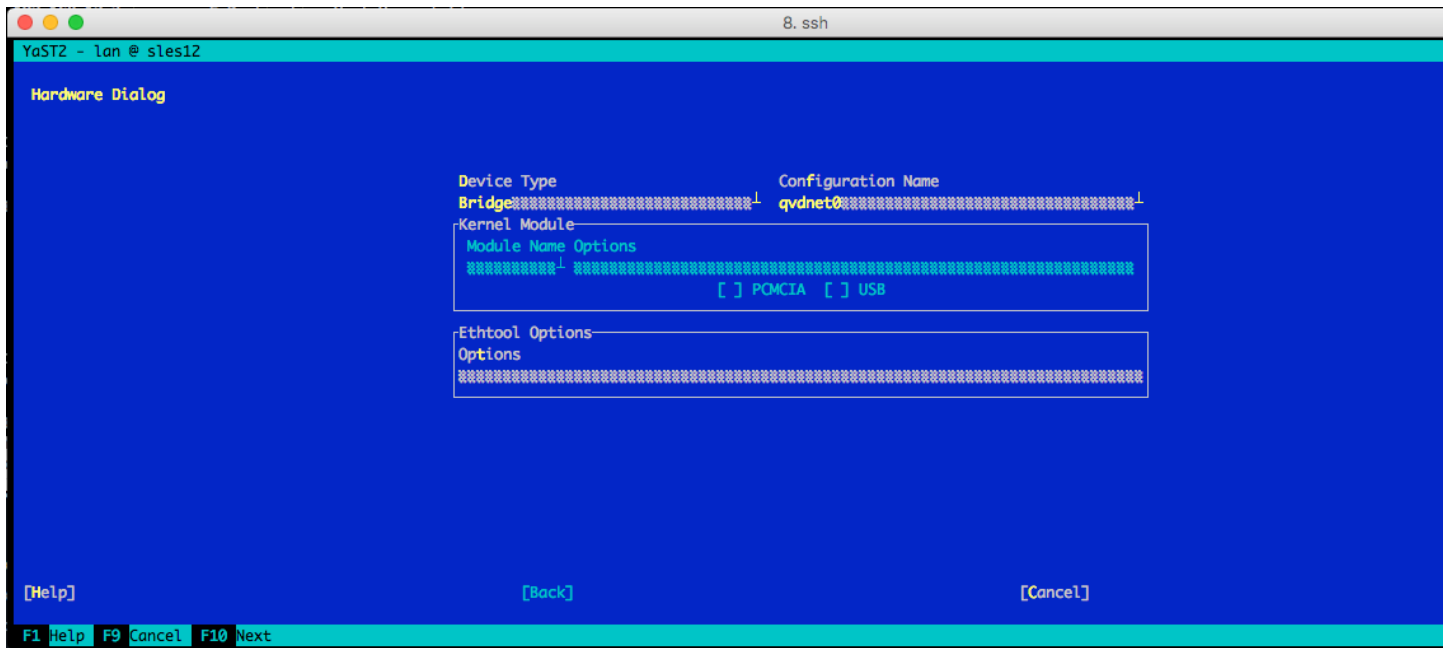


- Select Add option.



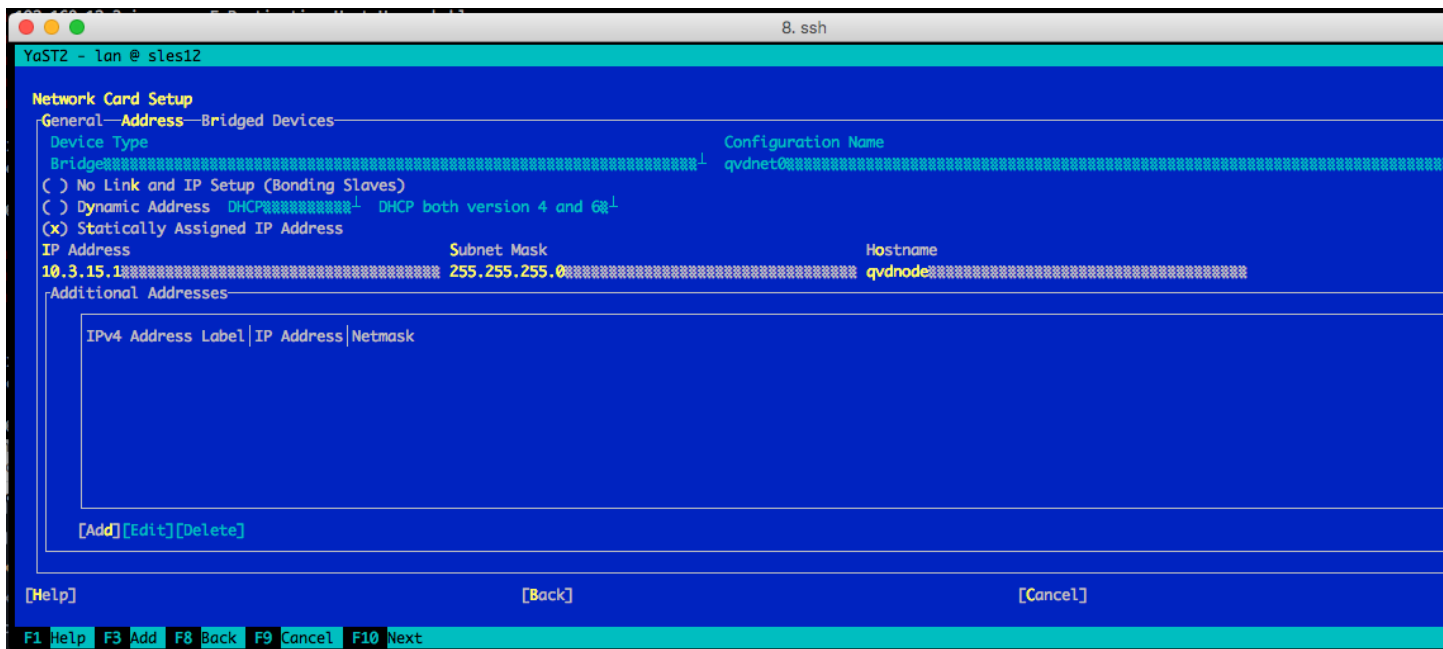
Set the following options:

- Device Type:"Bridge"
- Configuration name:"qvdnet0"
- Leave all the remainig fields as they are.
- Choose Next.



In the following screen set the options:

- IP Address:"10.3.15.1"
- Subnet Mask:"255.255.255.0"
- Hostname:"qvdrnode"
- Choose 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:

```
iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.0.2
iptables -t nat -A PREROUTING -d 192.168.0.2 -p tcp --dport 8443 -j DNAT --to-destination ←
10.3.15.1
```

**Note**

You will need to change the IP address **192.168.0.2** to the IP address of the network interface that you intend your clients to connect to.

**Note**

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

Bring up the network bridge:

```
# ifup qvdnet0
```

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
```

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
```

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 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.