



LA GUÍA PARA PRINCIPIANTES DE

Instalación de QVD 4.1

QVD DOCUMENTATION

<documentation@theqvd.com>

November 5, 2018

Contents

1	Requisitos	1
1.1	Base de datos	1
1.2	HKD	1
2	Pre-instalación	2
3	Instalación del HKD	3
4	Instalación y configuración de la base de datos	4
4.1	Crear una cuenta de usuario	4
4.2	Crear la base de datos QVD	4
4.3	Cambiar la configuración de PostgreSQL	4
4.4	Configuración básica	5
4.5	Población de las tablas de QVD	5
5	Instalación de las herramientas de administración	6
5.1	Configuración de SSL	6
5.2	API	6
5.3	CLI	7
5.4	WAT	7
6	Configuración básica e indispensable	8
6.1	Configuración de red	8
6.1.1	Establecer dnsmasq para ser controlado por QVD	8
6.1.2	Configurar el reenvío IP	8
6.1.3	Configurar un puente de red	8
6.1.4	Configurar QVD para su red	11
6.2	Configurar QVD para usar los certificados SSL	11
6.3	Configurar nodo HKD	12
7	¿Y ahora qué?	13

Advertencias

**Important**

La presente guía contiene los comandos necesarios para realizar una instalación de QVD **mononodo**, en la cual se instalarán todos los componentes en la misma máquina. En una instalación multinodo existirán pasos adicionales y la configuración de red varía.

**Important**

Durante el proceso se instalarán paquetes y se realizarán modificaciones de la configuración de red. Se recomienda utilizar un entorno de pruebas.

Chapter 1

Requisitos

Base de datos

- 2 núcleos de CPU
- 2 GB de RAM
- PostgreSQL 9.3 o superior

HKD

- Arquitectura [x86_64](#).

Chapter 2

Pre-instalación

```
# 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**

Es posible que deba proporcionar su disco de instalación para completar la operación.

Para paquetes comerciales:

```
# 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: $USUARIO
Password: $PASSWORD
# zypper ref
```

**Note**

\$USUARIO y \$PASSWORD son las credenciales recibidas al comprar la suscripción.

Chapter 3

Instalación del HKD

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

Chapter 4

Instalación y configuración de la base de datos

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

Crear una cuenta de usuario

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

Crear la base de datos QVD

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

Cambiar la configuración de PostgreSQL

Edite el archivo `/var/lib/pgsql/data/pg_hba.conf` y agregue **al principio** la línea siguiente:

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

**Note**

Asegúrese de reemplazar la red predeterminada 192.168.0.0/24 con la red que utiliza su plataforma.

Edite el archivo `/var/lib/pgsql/data/postgresql.conf` y establezca los siguientes parámetros:

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

Reinicie PostgreSQL.

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

Configuración básica

```
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
```

Edite el archivo `/etc/qvd/node.conf` y modifique/incluya las siguientes entradas:

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

Población de las tablas de QVD

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


Chapter 5

Instalación de las herramientas de administración

Configuración de SSL



Note

Si ya tiene un certificado firmado por un tercero, puede omitir la creación de un certificado autofirmado y utilizar su certificado firmado.

Creación de un certificado autofirmado

```
root@myserver:~# zypper install openssl
root@myserver:~# mkdir /etc/qvd/certs
root@myserver:~# cd /etc/qvd/certs
```

Genere una clave privada.

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

Cree un certificado autofirmado.

```
# openssl req -new -x509 -nodes -sha256 -days 3650 -key key.pem > cert.pem
```



Note

OpenSSL le pedirá que ingrese varios campos que requiere para el certificado. En el campo **Nombre común** debe insertar el nombre de dominio completo del host que ejecutará su nodo QVD.

API

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

Cree el fichero `/etc/qvd/api.conf` con el siguiente contenido:

```
database.host=localhost
database.name=qvddb
database.user=qvd
database.password=passw0rd
api.user=root
api.group=root
path.api.ssl=/etc/qvd/certs
```

Para ejecutar tanto el CLI como el WAT deberemos arrancar la API.

```
service qvd-api start
```

Haciendo una llamada al endpoint *info* desde el navegador o con el siguiente comando comprobaremos que la API está funcionando.

```
# curl -k https://localhost:443/api/info
```

Nos deberá devolver un JSON con datos del sistema.

CLI

```
root@myserver:~# zypper install perl-QVD-Admin4
```

Cree el fichero `/etc/qvd/qa.conf` con el siguiente contenido:

```
qa.url = https://localhost:443/
qa.tenant = *
qa.login = superadmin
qa.password = superadmin
qa.format = TABLE
qa.insecure = 1
```



Caution

Esto es solo una guía de instalación para pruebas. Nunca para su uso en un entorno de producción. El parámetro `qa.insecure` deberá ser sustituido por el parámetro `qa.ca` con la ruta de su Autoridad de certificación.

Con el siguiente comando comprobaremos que el QA4 está funcionando.

```
# qa4 admin get
```

Nos deberá devolver los 2 administradores del sistema: admin y superadmin.

WAT

```
# zypper install qvd-wat
```

Ejecutando el WAT

Visite <https://localhost:443>

Credenciales:

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

Chapter 6

Configuración básica e indispensable

Configuración de red

Establecer dnsmasq para ser controlado por QVD

```
# rpm -q dnsmasq
```

Si no está instalado:

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

Configurar el reenvío IP

Edite el fichero `/etc/sysctl.conf` y añada la línea:

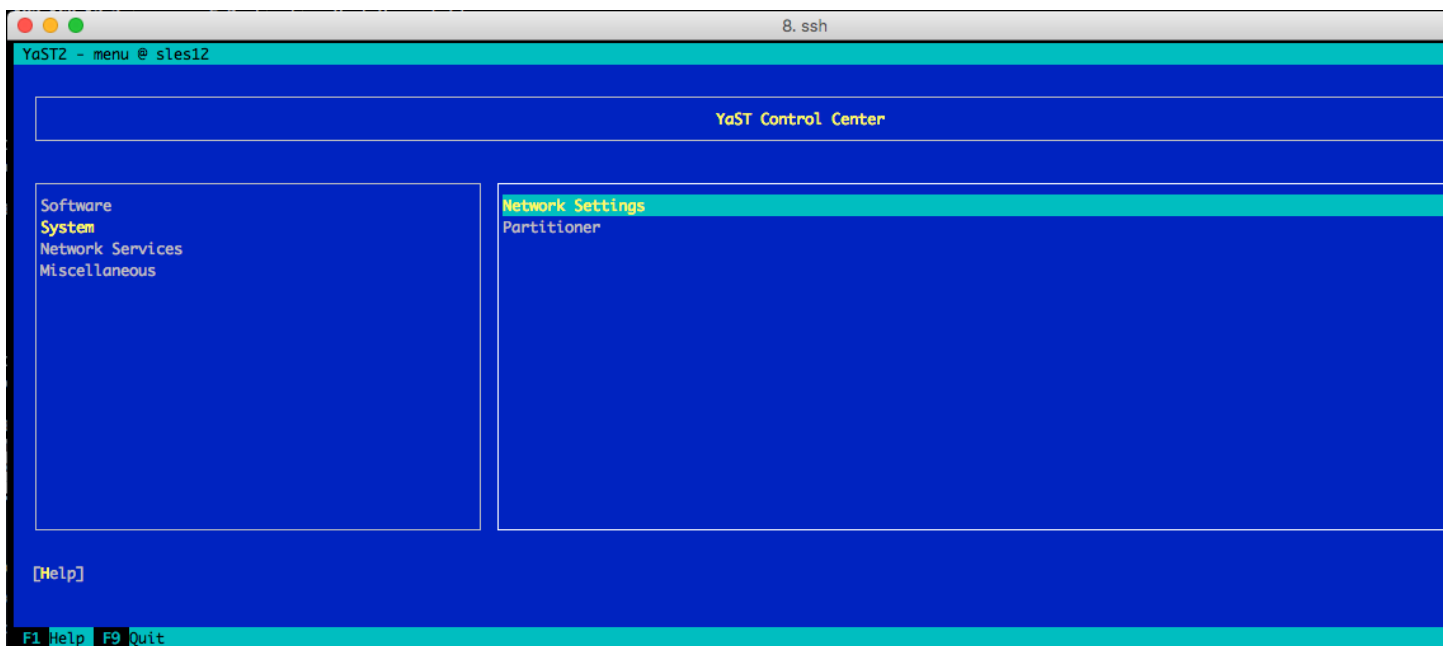
```
net.ipv4.ip_forward=1
```

Ejecute:

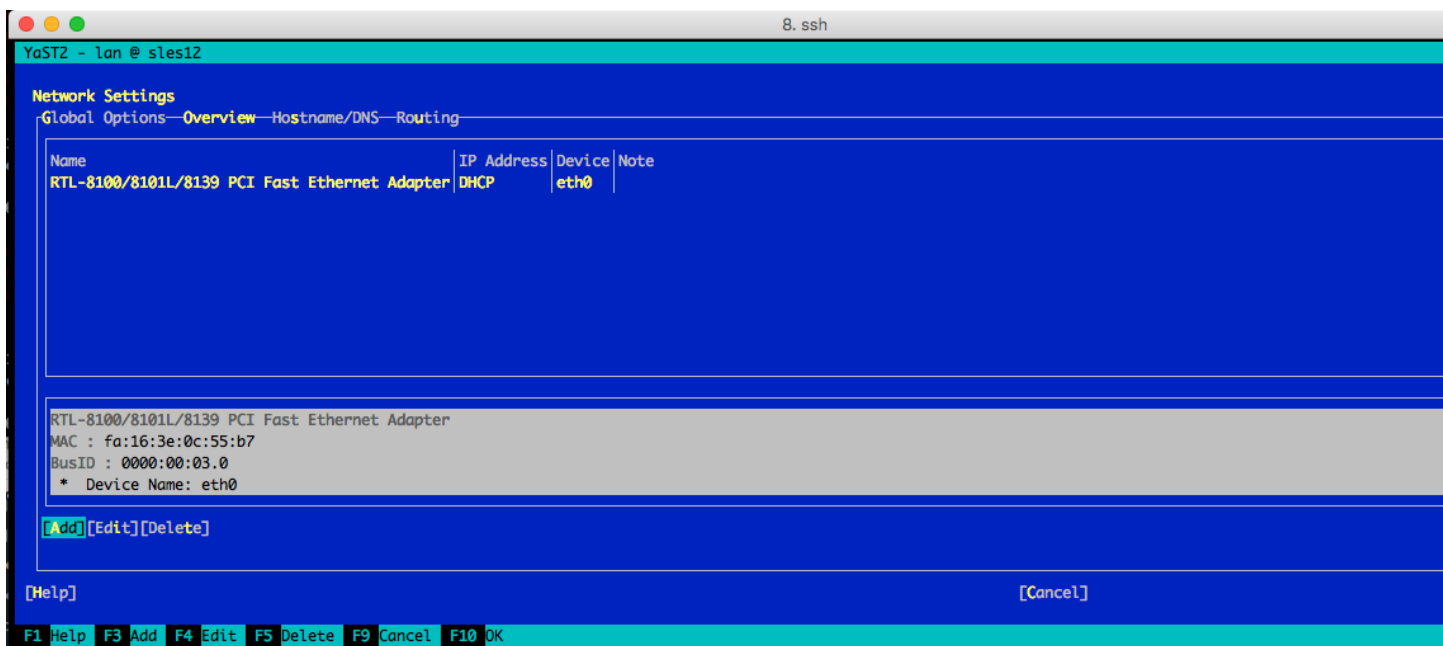
```
# sysctl -p
```

Configurar un puente de red

Abra Yast y vaya a System → Network Settings

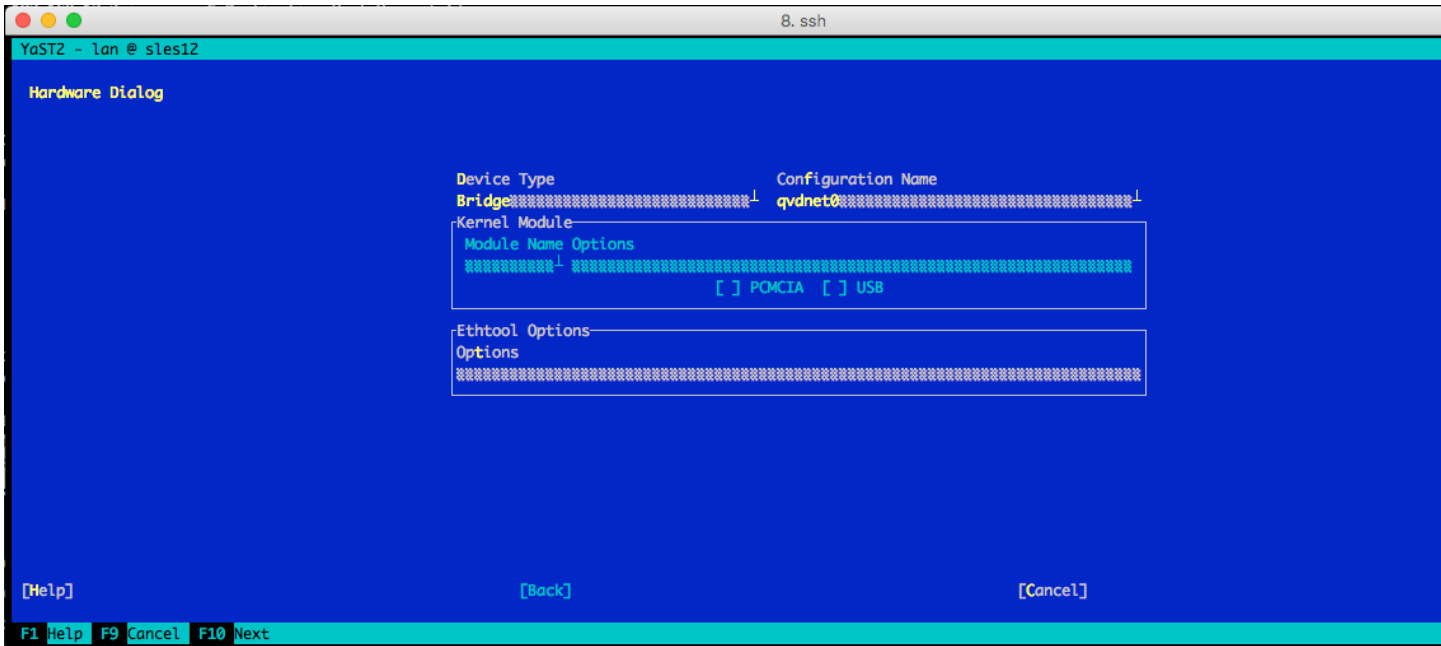


- Seleccione la opción Add.



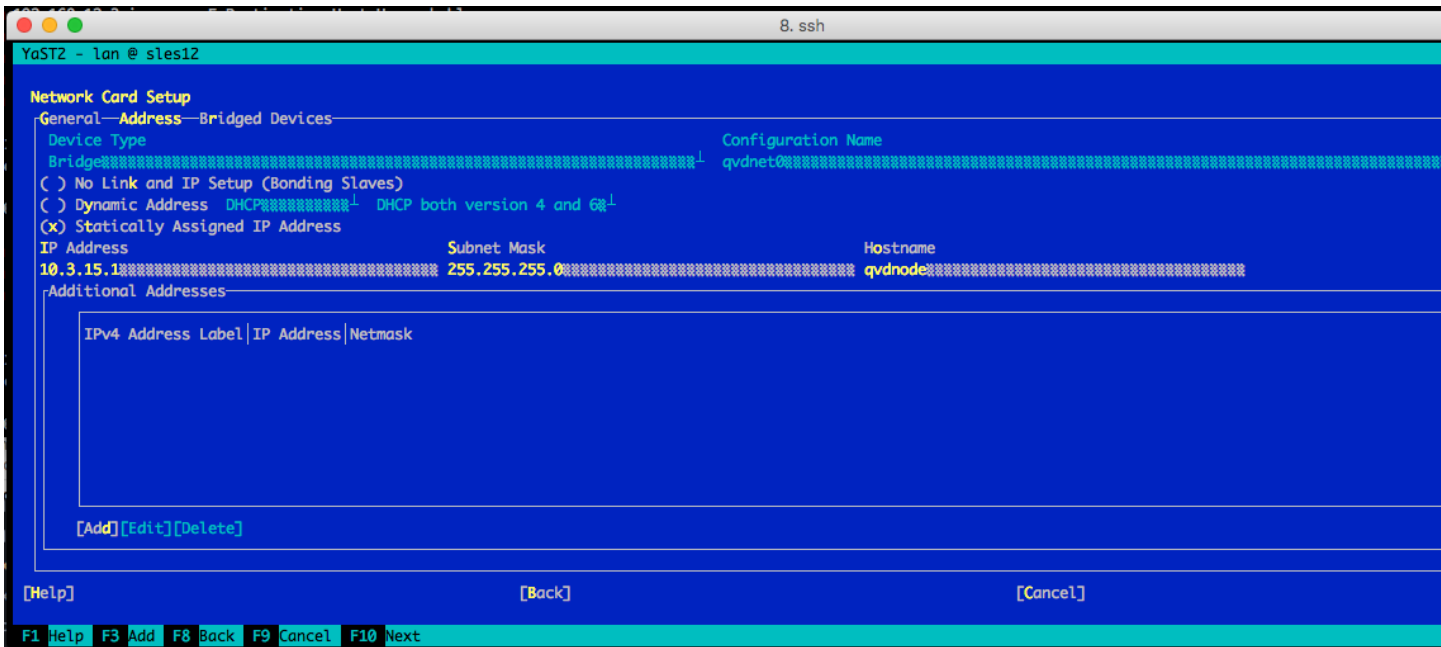
Defina las opciones siguientes:

- Device Type:"Bridge"
- Configuration name:"qvdnet0"
- Deje todos los campos restantes como están
- Seleccione Next.



En la siguiente pantalla defina las siguientes opciones:

- IP Address:"10.3.15.1"
- Subnet Mask:"255.255.255.0"
- Hostname:"qvdrnode"
- Seleccione Next.



- El dispositivo de red se configurará automáticamente en unos segundos.
- Seleccione Ok para salvar la configuración.
- Salga de Yast

Ejecute también los siguientes comandos:

```
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**

Necesitará cambiar la dirección IP **192.168.0.2** a la dirección IP de la interfaz de red a la que desea que sus clientes se conecten.

**Note**

El rango **10.3.15.0/24** debe ser único dentro de su infraestructura.

Levante la interfaz de red:

```
# ifup qvdnet0
```

Configurar QVD para su red

```
# 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
```

Configurar QVD para usar los certificados SSL

```
# qa4 config ssl key=/etc/qvd/certs/key.pem, cert=/etc/qvd/certs/cert.pem
# openssl version -d
```

El directorio devuelto por el comando anterior devuelve por defecto:

```
OPENSSLDIR: "/etc/ssl"
```

**Note**

Si en su caso devuelve otro directorio, utilícelo en lugar de `/etc/ssl` para los siguientes pasos.

Los certificados de confianza se almacenan en `/etc/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
```

Configurar nodo HKD

Edite el fichero `/etc/qvd/node.conf` con este contenido:

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

Ahora añade el nodo a la solución ejecutando:

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

Y arranque el servicio HKD:

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

Chapter 7

¿Y ahora qué?

Si ha tenido algún problema consulte la guía de instalación completa de QVD.

Si ya ha realizado todos los pasos de esta guía con éxito, enhorabuena, ya tiene una solución QVD instalada. A continuación debería de:

- Configurar su primer OSF
- Instalar su primera imagen
- Agregar su primer usuario
- Añadir una VM para su usuario

Le recomendamos que siga con **la guía del WAT** para realizar estos pasos.

Una vez finalizado solo le quedará:

- Conectarse y probar la solución

Consulte **la guía rápida para instalar el cliente QVD** en su sistema.

Si tiene alguna pregunta o necesita soporte adicional, visite nuestro sitio web en <http://theqvd.com/> o póngase en contacto con nosotros en info@theqvd.com.