



GUÍAS RÁPIDAS

Instalación de QVD 4.2 en Ubuntu 18.04

DOCUMENTACIÓN DE QVD

<documentation@theqvd.com>

Contents

1	Requisitos	1
1.1	Base de datos	1
1.2	HKD	1
2	Pre-instalación	2
3	Instalación y configuración de la base de datos	3
3.1	Crear una cuenta de usuario	3
3.2	Crear la base de datos QVD	3
3.3	Cambiar la configuración de PostgreSQL	3
4	Instalación del HKD	4
4.1	Configuración básica	4
4.2	Despliegue del esquema de la base de datos 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	9
6.2	Configurar QVD para usar los certificados SSL	9
6.3	Configurar nodo HKD	10

Producto QVD 4.2 Virtual Deckard
Equipo QVD Docs <documentation@theqvd.com>
[Aviso legal](#)

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

1.1 Base de datos

- 2 núcleos de CPU
- 2 GB de RAM
- PostgreSQL 10 o superior

1.2 HKD

- Arquitectura [x86_64](#).

Chapter 2

Pre-instalación

- Verificar que los puertos requeridos (443 y 8443) estén abiertos

```
root@qvdnode:~# firewall-cmd --list-all
```

- En caso de que no se encuentren a la escucha, realizar la siguiente configuración:

```
root@qvdnode:~# firewall-cmd --permanent --add-service https
root@qvdnode:~# firewall-cmd --permanent --add-port 8443/tcp
root@qvdnode:~# systemctl restart firewalld
root@qvdnode:~# firewall-cmd --list-all
```

- Agregar la clave pública de los paquetes QVD a sus claves de confianza (como root):

```
root@qvdnode:~# wget -qO - https://www.theqvd.com/packages/key/public.key | sudo apt-key ←
add -
```

- Agregar el repositorio y actualizar:

```
root@qvdnode:~# echo "deb http://theqvd.com/packages/ubuntu-bionic QVD-4.2.0 main" > \
/etc/apt/sources.list.d/qvd.list
root@qvdnode:~# apt-get update
```

- Para paquetes comerciales:

```
root@qvdnode:~# echo "deb http://$USUARIO:$PASSWORD@theqvd.com/packages/ubuntu-bionic ←
QVD-4.2.0 main" > \
/etc/apt/sources.list.d/qvd.list
root@qvdnode:~# apt-get update
```

**Note**

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

Chapter 3

Instalación y configuración de la base de datos

```
root@qvdnode:~# apt-get install postgresql
root@qvdnode:~# systemctl enable --now postgresql@10-main.service
```

3.1 Crear una cuenta de usuario

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

3.2 Crear la base de datos QVD

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

3.3 Cambiar la configuración de PostgreSQL

Edite el archivo `/etc/postgresql/10/main/postgresql.conf` y establezca los siguientes parámetros:

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

Edite el archivo `/etc/postgresql/10/main/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.

Reinicie PostgreSQL.

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

Chapter 4

Instalación del HKD

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

4.1 Configuración básica

- Copie el archivo de ejemplo **sample-node.conf** a su configuración:

```
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
```

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

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

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

– Donde

- * **nodename**: Nombre del nodo, normalmente es el mismo nombre del servidor
- * **database.host**: Servidor donde reside la base de datos de QVD
- * **database.name**: Nombre de la base de datos de QVD
- * **database.user**: Cuenta de usuario necesaria para conectar
- * **database.password**: Contraseña del usuario anteriormente especificado

– También debe agregar un nivel de log para fines de depuración.

– Las entradas relacionadas con el log se deben establecer aquí, debido a que los componentes de QVD se inicializan antes de conectarse a la base de datos.



Note

Debe asegurarse de que el **nodename**, **database.host**, **database.name**, **database.user** y **database.password** contienen valores que coinciden con los que haya configurado. Una vez que estos ajustes estén en su lugar, cualquier utilidad que requiera acceso a la base de datos tendrá los detalles de configuración apropiados para hacerlo.

- Iniciar/Habilitar el servicio de HKD

```
root@qvdnode:~# systemctl enable --now qvd-hkd
```

4.2 Despliegue del esquema de la base de datos de QVD

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

Chapter 5

Instalación de las herramientas de administración

5.1 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@qvdnode:~# apt-get install openssl
root@qvdnode:~# mkdir /etc/qvd/certs
root@qvdnode:~# cd /etc/qvd/certs
```

Genere una clave privada.

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

Cree un certificado autofirmado.

```
root@qvdnode:/etc/qvd/certs# openssl req -new -x509 -nodes -sha256 -days 365 -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.

5.2 API

```
root@qvdnode:~# apt-get install perl-qvd-api
```

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

```
database.host=qvdnode
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.

```
root@qvdnode:~# systemctl enable --now qvd-api
```

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

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

Nos deberá devolver un JSON con datos del sistema.

5.3 CLI

```
root@qvdnode:~# apt-get 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.

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

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

5.4 WAT

```
root@qvdnode:~# apt-get install qvd-wat
```

Ejecutando el WAT

Visite <https://localhost:443>

Credenciales:

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

Chapter 6

Configuración básica e indispensable

6.1 Configuración de red

6.1.1 Establecer dnsmasq para ser controlado por QVD

- Verificar el estado del servicio:

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

- En caso de que este activo, es necesario deshabilitarlo:

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

6.1.2 Configurar el reenvío IP

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

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

- Ejecute:

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

6.1.3 Configurar un puente de red

Edite el archivo `/etc/network/interfaces` y agregue las líneas siguientes:

```
auto qvdnet0
iface qvdnet0 inet static
    pre-up brctl addbr qvdnet0
    pre-up iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 192.168.0.2
    pre-up iptables -t nat -A PREROUTING -d 192.168.0.2 -p tcp --dport 8443 -j DNAT --to- ↵
        destination 10.3.15.1
    post-down brctl delbr qvdnet0
    address 10.3.15.1
    netmask 255.255.255.0
```

**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:

```
root@qvdnode:~# ifup qvdnet0
```

6.1.4 Configurar QVD para su red

```
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
```

6.2 Configurar QVD para usar los certificados SSL

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

El directorio devuelto por el comando anterior devuelve por defecto:

```
OPENSSLDIR: "/usr/lib/ssl"
```

**Note**

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

Los certificados de confianza se almacenan en `/usr/lib/ssl/certs`

```
root@qvdnode:~# trusted_ssl_path=/usr/lib/ssl/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
```

6.3 Configurar nodo HKD

- Una vez que se ha realizado toda la configuración, añade el nodo a la solución ejecutando:

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

- Y reinicie el servicio HKD:

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

¿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



Note

Le recomendamos que consulte el [Manual de la herramienta de administración Web \(WAT\)](#) para realizar estos pasos.

Una vez finalizado solo le quedará:

- Conectarse y probar la solución
- Consultar las [Guías rápidas de instalación](#) para elegir su cliente e instalarlo en su sistema.

—

Si tiene alguna pregunta ó necesita soporte adicional, visite nuestro [sitio web](#) ó póngase en [contacto](#) con nosotros.

[Menú Principal](#)