GUÍAS RÁPIDAS

Guía de Instalación de QVD 4.2

DOCUMENTACIÓN DE QVD

<documentation@theqvd.com>

Contents

List of Figures

Producto QVD 4.2 Virtual Deckard
Equipo QVD Docs <documentation@theqvd.com>
Aviso legal

Introducción

Esta guía tiene la intención de ayudarle a instalar una solución QVD por sí mismo. Se pretende que este documento sea lo más sencillo de seguir posible y que usted pueda prácticamente copiar y pegar los comandos de la documentación a la consola.

En este sentido, hemos obviado cualquier referencia a la arquitectura del producto, y se da por hecho que usted ha leido previamente el **Manual de Arquitectura**.

Note

Tenga en cuenta que mientras las versiones de QVD desde la 3.1, son capaces de soportar la virtualización LXC, esta guía solo explica cómo configurar el entorno para la virtualización predeterminada KVM, para que las cosas sean lo más simples posible.

Si está interesado en configurar su instalación de QVD para aprovechar LXC, consulte el capítulo titulado **Virtualización LXC dentro de QVD** en el **Manual de administración de QVD**.

QVD está en desarrollo continuo. Si bien tratamos de mantener toda nuestra documentación actualizada con la versión actual, es posible que se proporcione alguna nueva funcionalidad antes de actualizar la documentación. Si hay secciones en este documento que se han vuelto obsoletas, o si encuentra que algunas de las instrucciones proporcionadas no funcionan como se esperaba, no dude en ponerse en contacto con nosotros.

Chapter 1

El método fácil y rápido

Instalación de la máquina virtual de demostración QVD QVD proporciona un dispositivo VirtualBox de demostración en forma de una imagen OVF que puede descargar y ejecutar con un mínimo de esfuerzo dentro del software VirtualBox disponible gratuitamente. Si no tiene VirtualBox instalado, puede descargarlo desde el sitio web https://www.virtualbox.org/-wiki/Downloads o seguir las instrucciones allí obtenerlo para su sistema operativo particular. Dado que usted va a estar ejecutando la demostración de un entorno puramente virtualizado, esto significa que usted será capaz de probar el software de una amplia gama de entornos diferentes y sin tener que hacer cambios sustanciales a su propia configuración.

La imagen VM se puede encontrar aquí (Apartado Appliances):

http://theqvd.com/download/disk-images

Una vez descargado, inicie el software VirtualBox y seleccione "Importar servicio virtualizado" en el menú Archivo. Elija la demostración de QVD que ha descargado y haga clic en Siguiente. Esto le llevará a la pantalla Configuración de importación de dispositivos.

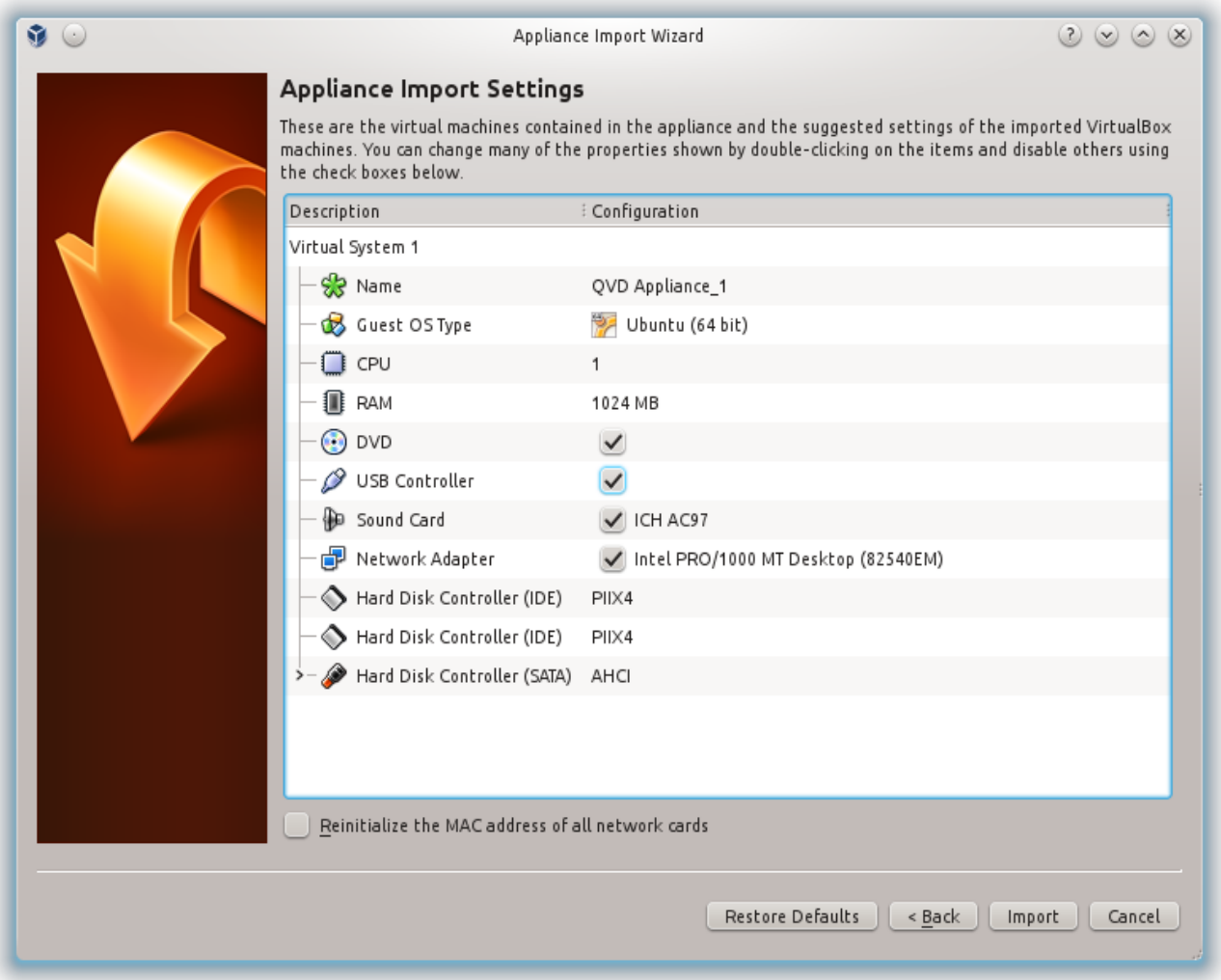

Figure 1.1: VirtualBox Configuración de Importación de Dispositivos

No recomendamos que cambie nada en esta pantalla, así que haga clic en el botón Importar y dé a VirtualBox un par de minutos para completar la importación. De vuelta en la pantalla principal de VirtualBox, ahora debe tener la nueva máquina "QVD Appliance".

Note

De forma predeterminada, la versión de QVD del appliance utiliza los puertos 8443 para el enrutador de capa 7, el puerto 7443 para la herramienta de administración Web y el puerto 6443 para el portal de usuario. Además, el puerto 2222 se utiliza para el acceso ssh. Proporcionar el acceso a estos puertos en un sistema operativo invitado en VirtualBox puede lograrse mediante NAT y establecer el motor de red VirtualBox para asignar estos puertos al invitado. Esto ya está configurado en el QVD Appliance. Es importante tener en cuenta que estos puertos **no** deben estar ya en uso en la máquina local o esto no funcionará correctamente.

Para iniciar el dispositivo QVD, simplemente selecciónelo en la lista de máquinas virtuales en VirtualBox y haga clic en el botón Inicio. Esto arrancará la máquina y lo llevará a una pantalla de inicio de sesión de la consola. El nombre de usuario y la contraseña predeterminados son `qvd`, aunque no debería tener que iniciar sesión todavía para probar el software. Puede conectarse al puerto 8443 de su máquina local con el cliente de QVD para verificar directamente el funcionamiento del producto

como usuario. También puede conectarse a los puertos 7443 y 6443 con un navegador web para ver la interfaz de administración WAT y el Portal de Usuario respectivamente.

Le dejamos los datos del appliance para que pueda experimentar con libertad:

SYSTEM	USER	PASSWORD
Console	qvd	qvd
Console	root	root
Web Administration Tool (https://localhost:7443)	superadmin@*	superadmin
User Portal (https://localhost:6443)	qvd-demo@default	qvd-demo

Si lo desea, puede usar el cliente QVD para conectarse a la máquina virtual pre-configurada con los siguientes datos:

HOST	USER	PASSWORD
localhost	qvd-demo@default	qvd-demo

Note

Por defecto no hay acceso como root a los escritorios virtuales. Si necesita hacer pruebas de este tipo, puede cambiar la contraseña desde el filesystem de la vm que está montado sobre el filesystem del appliance QVD:

```
Acceda como root a la consola del appliance QVD y ejecute lo siguiente:
$ chroot /var/lib/qvd/storage/rootfs/10000-fs
$ passwd
Enter new UNIX password: root
Retype new UNIX password: root
passwd: password updated successfully
$ exit
$ cd /
Ahora puede usar el usuario root, con contraseña root en la VM de demostración.
```

Important

Si decide utilizar el dispositivo de demostración QVD, puede omitir una gran parte de este documento. Tenga en cuenta, sin embargo, que esta demo no tiene soporte y de ninguna manera proporciona una solución preparada para producción. Para entender completamente cómo funcionan los componentes de QVD, recomendamos encarecidamente que continúe leyendo este documento, pero si simplemente desea ver el software funcionando, debería ser capaz de seguir la demo en Instalando y configurando QVD Client.

Chapter 2

Guía de instalación de QVD

2.1 Requisitos para esta guía

En esta guía, suponemos que desea configurar su primer entorno de demostración de QVD. Por este motivo, asumiremos que los componentes del lado del servidor dentro de la solución se hospedarán en el mismo servidor físico. Llamamos a esto una instalación *mononodo*. Con el fin de mantener las cosas lo más simple posible, también asumiremos que probará la solución utilizando el Cliente QVD instalado en una estación de trabajo independiente. Aunque es posible tener todos los componentes incluyendo el cliente en ejecución en la misma máquina, es más fácil demostrar las capacidades de la VDI si se conecta desde una estación de trabajo distinta.

Dado que todos los componentes se ejecutarán en el mismo sistema, no estaremos demasiado preocupados por el almacenamiento compartido. Sin embargo, es importante entender que QVD hace uso de algún almacenamiento común entre los diferentes componentes de la solución y que para maximizar el potencial de su solución, es probable que algunos de estos directorios de almacenamiento se ubiquen en un recurso compartido de archivos de red en un NAS o SAN.

Con todo esto en mente, seguiremos construyendo esta solución en un solo host para mantener las cosas lo más simples posible. En realidad, es más que probable que un entorno de producción mantenga cada uno de los diferentes componentes en diferentes sistemas y el almacenamiento se gestione a través de cada uno de ellos. Si se siente cómodo configurando las comparticiones NFS y construyendo e instalando cada componente en una máquina diferente, no dude en hacerlo.

Actualmente, QVD tiene paquetes para los componentes de servidor disponibles para las distribuciones de CentOS 7.8 y Ubuntu 18.04. En esta guía se proporcionarán de manera conjunta todas las instrucciones de instalación que son similares en ambas distribuciones y, en donde sea necesario, se proporcionarán los comandos que difieren entre las mismas.

En resumen:

- Un único nodo con todos los componentes (Ubuntu o CentOS)
- Una máquina cliente para probar
- Sin almacenamiento compartido
- Muy sencillo
- Listo para producción

2.2 Hardware del sistema

Los componentes del nodo HKD normalmente se deben ejecutar en sistemas independientes para garantizar que cuentan con recursos adecuados para ejecutarse y los requisitos de hardware variarán en función del número de usuarios que desee servicio, el número de imágenes de disco del sistema operativo que desee y varios factores más.

Por lo que respecta a esta guía, que supone que está evaluando QVD que sólo instalará una imagen y configurará uno o dos usuarios como máximo, le recomendamos los siguientes requisitos de hardware del sistema como guía:

- **Procesador del sistema**: Procesador de 64 bits, preferiblemente multi-core. Puede soportar alrededor de 8 usuarios por núcleo. Los paquetes de 32 bits están disponibles para pruebas, pero la limitación de 4 GB de RAM para los modos no PAE de los procesadores x86 significa que sólo una cantidad limitada de clientes será posible, y ciertamente no es viable para un entorno de producción.
- **Memoria del sistema**: Al menos 4 GB de RAM. Esto debe ser suficiente para un máximo de 4 usuarios.
- **Espacio en disco**: Al menos 20 GB de espacio en disco deben estar disponibles para contener la imagen del sistema operativo, etc. Muy probablemente, deberá tratar de duplicar esto para trabajar cómodamente con las herramientas implicadas en la importación de una imagen.
- **Interfaz de red**: Necesitará al menos una interfaz de red disponible. Un NIC Ethernet 10/100/1000 debe ser perfectamente suficiente. Hemos tenido éxito en servir los escritorios sobre conexiones inalámbricas también.

Puede utilizar cualquier sistema cliente soportado para ejecutar el software QVD Client. Actualmente soportamos Linux , Microsoft Windows y OSX.

2.3 Requerimientos de los sistemas operativos

2.3.1 Ubuntu 18.04

PRE-INSTALACIÓN EN UBUNTU

- Verificar que los puertos requeridos (443 y 8443) esten 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.

2.3.2 CentOS 7.8

PREINSTALACIÓN EN CENTOS

- Instalar los paquetes adicionales

```
root@qvdnode:~# yum install yum-utils
```

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

```
root@qvdnode:~# rpm --import https://www.theqvd.com/packages/key/public.key
```

- Agregar el repositorio y actualizar:

```
root@qvdnode:~# yum-config-manager --add-repo http://theqvd.com/packages/centos/7.8/QVD ↩
    -4.2.0/
root@qvdnode:~# yum update
```

  - Para paquetes comerciales:

```
root@qvdnode:~# echo "[QVD-4.2.0]" > /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "name=QVD-4.2.0" >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "baseurl=http://$USER:$PASSWORD@theqvd.com/commercial-packages/ ↩
    centos/7.8/QVD-4.2.0/" | sed 's/@\(.*@\)/%40\1/' >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# echo "enabled=1" >> /etc/yum.repos.d/QVD-4.2.0.repo
root@qvdnode:~# yum update
```

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

El repositorio QVD, en ambas distribuciones, proporciona los siguientes paquetes:

- **perl-qvd-client**: software de cliente de QVD GUI
- **perl-qvd-hkd**: demonio de mantenimiento
- **perl-qvd-admin4**: herramientas de línea de comandos para administrar usuarios, máquinas virtuales, sistema operativo
- **perl-qvd-db**: base de datos central para la plataforma

Cada uno de estos paquetes tendrá varias dependencias que pueden ser satisfechas por otros paquetes provistos por los repositorios usuales de Ubuntu. A continuación se muestra un resumen de otros componentes de código abierto requeridos por QVD:

- El **RSGBD** de PostgreSQL.
- **KVM**: Hipervisor.
- **LXC**: Contenedores Linux basados en las herramientas de espacio de usuario de los Kernels recientes
- **libvirt0**: una biblioteca para la interfaz con diferentes sistemas de virtualización
- **NX**: protocolo que maneja las conexiones de escritorio remoto.
- **Ebtables**: una utilidad de cortafuegos basada en IP para puentes ethernet

2.4 Instalación y configuración del motor de base de datos

Instale lo siguiente

Ubuntu:

```
root@qvdnode:~# apt-get install postgresql
```

CentOS:

```
root@qvdnode:~# yum install https://download.postgresql.org/pub/repos/yum/reporpms/EL-7- ↩
    x86_64/pgdg-redhat-repo-latest.noarch.rpm
root@qvdnode:~# yum install postgresql10-server postgresql10-contrib
root@qvdnode:~# /usr/pgsql-10/bin/postgresql-10-setup initdb
```

Ahora, habilite/inicie el servidor postgresql:

Ubuntu

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

CentOS

```
root@qvdnode:~# systemctl enable --now postgresql-10.service
```

Despues de la instalación, se deben realizar algunos pasos de forma manual. Estos son:

1. Crear una cuenta de usuario,
2. Crear una base de datos,
3. Cambiar la configuración de la base de datos, y
4. Desplegar el esquema de la base de datos de QVD.

Necesitará crear una cuenta de usuario y una base de datos en postgres, así que haga `su` a la cuenta de postgres (use `sudo` si no es root):

```
root@qvdnode:~# su - postgres
```

2.4.1 Crear una cuenta de usuario

Si desea utilizar una cuenta de usuario existente, puede saltarse este paso.

Una vez que tenga acceso a la base de datos, puede crear cuentas de usuario con el comando createuser. Se le pedirá una contraseña para el nuevo usuario y algunos detalles sobre la cuenta de usuario. Puede responder *n* a todo.

Por ejemplo, para crear un usuario llamado qvd, utilice el siguiente comando.

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

El nuevo usuario ahora puede ser asignado como propietario de una base de datos. Primero tenemos que crear la base de datos QVD.

2.4.2 Creación de la base de datos QVD

Utilice el comando createdb para crear una base de datos para QVD. Utilice el modificador -O para establecer el propietario de la base de datos a la cuenta que desea utilizar. En este caso, estableceremos el propietario en el nuevo usuario que creamos en el paso anterior.

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

2.4.3 Cambiar la configuración de PostgreSQL

En un entorno en producción en el que múltiples sistemas interactúan con la base de datos QVD, QVD utiliza transacciones de forma extensiva y requiere un nivel de aislamiento de transacciones superior al configurado por defecto. Además, por lo general, necesita que PostgreSQL sea accesible por otros hosts de su red. Si bien este paso es opcional en la solución independiente que estamos creando en esta guía, quizás desee realizar esta configuración para asegurarse de que su sistema esté preparado para gestionar nodos HKD adicionales. Para ello debe editar el archivo de configuración PostgreSQL `postgresql.conf`. Asumiremos que está utilizando PostgreSQL 10 aunque puede que necesite ajustar algunas rutas según sea necesario.

En Ubuntu los archivos de configuración se encuentran en **/etc/postgresql/10/main/**, en CentOS se encuentran en **/var/lib/pgsql/10/data**.

El nivel de aislamiento de la transacción se controla con la configuración default_transaction_isolation. Para habilitar el acceso de red a PostgreSQL en general, cambie la configuración listen_addresses de *localhost* a *0.0.0.0*.

UBUNTU:

- Archivo de configuración: **/etc/postgresql/10/main/postgresql.conf**

CENTOS:

- Archivo de configuración: **/var/lib/pgsql/10/data/postgresql.conf**

editar

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

Important
Aunque el paso anterior era opcional para una configuración independiente, el siguiente paso no lo es. Deberá configurar el acceso de red para el usuario de QVD que haya creado.

Para habilitar el acceso de red para el usuario qvd, busque el archivo `pg_hba.conf`. Para Ubuntu esto será en **/etc/postgresql/10/main** y para CentOS en **/var/lib/pgsql/10/data**. Editar este archivo y agregar 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. El formato es el siguiente: `[host] [base de datos] [usuario] [CIDR-address] [auth-method] [auth-options]`

Reinicie PostgreSQL para que los cambios surtan efecto.

Ubuntu

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

CentOS

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

2.5 Instalación del HKD

Ahora es el momento de instalar el HKD. Para ello, asegúrese de tener privilegios de root:

Ubuntu

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

CentOS:

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

Esto instalará el HKD, así como todas las dependencias necesarias para ejecutar un nodo HKD.

2.5.1 Configuración básica

Cada nodo QVD utiliza un archivo de configuración `/etc/qvd/node.conf` desde donde se obtiene, entre otros ajustes que cubriremos más adelante, las credenciales de la base de datos y el nombre del host. Una vez que haya terminado de configurar postgresql, necesitará crear este archivo de configuración de nodo. Debe tener `perl-qvd-config-core` instalado en este punto como una dependencia. Contiene un archivo de muestra `node.conf`. Cree la carpeta `qvd` en /etc, y copie esta configuración de plantilla allí:

```
root@qvdnode:~# cp -v /usr/lib/qvd/config/sample-node.conf /etc/qvd/node.conf
```

Obviamente, los permisos en este archivo deben ser tan restrictivos como sea posible.

```
root@qvdnode:~# chown root:root /etc/qvd/node.conf
```

Ahora, haga el archivo ilegible por cualquier persona fuera del propietario y del grupo:

```
root@qvdnode:~# chmod 0640 /etc/qvd/node.conf
```

Ahora necesitará editar el archivo `/etc/qvd/node.conf` para incluir los detalles necesarios para acceder a la base de datos. El archivo de configuración debería tener este aspecto:

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

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

En primer lugar, la entrada `nodename` y la entrada `database.host` deben coincidir con el nombre de su máquina, por lo que el ejemplo anterior necesitará algún tipo de edición.

El host de base de datos también debe coincidir con el nombre de host o la dirección IP del sistema en el que se encuentra su base de datos. De forma predeterminada, el nombre de la base de datos se establece normalmente en *qvddb*, pero para instalaciones personalizadas, esto puede ser diferente. También deberá establecer el nombre de usuario y la contraseña de la base de datos que configuró al crear la base de datos.

Finalmente, podría también agregar un nivel de logging para propósitos de depuración de problemas.

Una vez finalizadas las configuraciones deberá Iniciar/Habilitar el servicio de HKD:

+

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

2.6 Implementación del esquema de la base de datos de QVD

Ahora es el momento de poblar la base de datos con las tablas que se utilizarán para almacenar datos para QVD. Antes de poder usar cualquiera de las herramientas de QVD, tendremos que configurar la base de datos, el nombre de usuario y la contraseña en los archivos de configuración de QVD.

Una vez hecho, ejecute **qvd-deploy-db.pl**, este script creará la estructura de la base de datos con las tabla que QVD necesita.

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

Note
En este punto obtendrá un error de autenticación si no ha utilizado la combinación de nombre de usuario y contraseña como el ejemplo anterior. Para cambiar los detalles para que coincidan con los que ha utilizado, edite el archivo **/etc/qvd/node.conf**. Entraremos en más detalles sobre este archivo en breve.

2.6.1 Prueba de acceso

Inicie sesión en postgresql e introduzca el siguiente comando para enumerar las tablas utilizadas por QVD:

```
root@qvdnode:~# psql -U qvd -W -h localhost -d qvddb
Password for user qvd:
psql (10)
```

2.7 Configuración de SSL

El nodo HKD necesita un certificado x509 y una clave privada para asegurar las conexiones de red. Para una instalación de producción, debe utilizar un certificado emitido por una autoridad de certificación reconocida, como Verisign o Thawte. Para fines de prueba puede utilizar un certificado autofirmado. En esta demostración, vamos paso a paso a través de la creación de un certificado auto-firmado, y utilizaremos esto dentro de nuestra configuración.

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

2.7.1 Creación de un certificado autofirmado

La herramienta openssl es necesaria para crear un certificado autofirmado. Si aún no lo ha instalado, puede hacerlo utilizando los repositorios

Ubuntu:

```
root@qvdnode:~# apt-get install openssl
```

CentOS:

```
root@qvdnode:~# yum install openssl
```

Recomendamos que para trabajar con los certificados, cree un subdirectorio en `/etc/qvd`.

```
root@qvdnode:~# mkdir /etc/qvd/certs
root@qvdnode:~# cd /etc/qvd/certs
```

Para crear su certificado, primero debe generar una clave privada.

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

Dada la clave privada, se crea un certificado autofirmado con el siguiente comando.

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

OpenSSL le pedirá que ingrese los varios campos que requiere para el certificado. Debe introducir información relevante en estos campos. El campo más importante es el campo **Nombre común** que debe coincidir con el nombre de dominio completo del host que ejecutará su nodo QVD.

```
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
++++------+++
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Madrid
Locality Name (eg, city) []:Madrid
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Qindel Group
Organizational Unit Name (eg, section) []:QVD Team
Common Name (eg, YOUR name) []:qvdnode
Email Address []:documentation@theqvd.com
```

Ahora tendrá un certificado auto-firmado y su correspondiente clave privada.

2.8 API

La API es un pre-requisito para los dos siguientes componentes, por lo que debe ser lo primero que instale. Puede hacerlo mediante el siguiente comando:

Ubuntu:

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

CentOS:

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

Al instalar la API, necesitará configurarla. Para ello, debe crear el fichero `/etc/qvd/api.conf` y añadir las siguientes líneas:

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

api.user = root
api.group = root

path.api.ssl=/etc/qvd/certs
```

Obsérvese que hemos repetido aquí los datos de configuración de la base de datos, ya que la API requiere este acceso. Además, hemos añadido las dos líneas que marcan el usuario con el que se ejecutará la API (root en este caso siguiendo con el ejemplo anterior), y una línea más con la ruta donde están los certificados que la API necesita para arrancar. Si no dispone de un certificado, puede ver como crear uno en la sección Creación de un certificado autofirmado de la presente guía.

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.

2.9 CLI

La utilidad de administración en línea de comandos de QVD se incluye en el paquete **perl-qvd-admin**.

Ubuntu:

```
root@qvdnode:~# apt-get install perl-qvd-admin4
```

CentOS:

```
root@qvdnode:~# yum install perl-QVD-Admin4
```

Esta útil herramienta permite realizar en línea de comandos todas las operaciones que se pueden realizar usando la herramienta de administración web del paquete **qvd-wat**. Puede instalarlo en cualquier host que desee utilizar para administrar su instalación de QVD. Por ejemplo, es posible que desee integrar QVD con una herramienta de supervisión externa como Nagios, por lo que la instalación de la utilidad QVD CLI Administration en este host haría esto posible.

La utilidad de Administración de QVD requiere un archivo de configuración que le diga dónde está instalada la API QVD. Vamos a configurar esto en el siguiente paso, pero vale la pena tener en cuenta que si desea instalar esta utilidad en cualquier otro host, el acceso a la API sigue siendo necesario para su funcionamiento.

Cree el fichero `/etc/qvd/qa.conf`:

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

En este ejemplo hemos asumido que la API ha sido configurada para escuchar en localhost en el puerto 443. También hemos asumido cuál es la contraseña del usuario superadmin e incluso que la configuración SSL ya se ha llevado a cabo. Además, hemos configurado `qa.tenant = *`, por lo que veríamos todos los tenants de la plataforma en caso de que estuviese configurada como multitenant. Veremos cómo se configuran algunas de estas cosas más adelante en esta misma guía. Para más información sobre el concepto de multitenant refiérase también al manual de configuración del CLI y el WAT. 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**.

2.10 WAT

La Herramienta de Administración de Web de QVD (QVD-WAT) es una interfaz sencilla que facilita la administración de los nodos HKD y el monitoreo de sesiones activas de clientes dentro de su infraestructura. También le ofrece la posibilidad de administrar nodos HKD desde ubicaciones remotas.

Aunque no es estrictamente necesario para ejecutar QVD, sin duda le ayudará a empezar con el producto, por lo que lo instalaremos y configuraremos en nuestro nodo servidor.

Ubuntu:

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

CentOS:

```
root@qvdnode:~# yum install qvd-wat
```

El WAT se instala en `/usr/lib/qvd/lib/wat/`. Dentro de esta localización se encuentra su fichero de configuración: `config.json`, que mostramos a continuación:

```
{
   "apiUrl": ""
}
```

Note
Cuando el parámetro apiUrl está vacío el sistema localiza la API en la misma URL donde está el WAT.

Para el ejemplo mononodo que estamos preparando, no es necesario cambiar este fichero. Tan solo asegúrese de que está ahí.

Si se quisiese desplegar la API en otra URL habría que reflejarlo en este fichero. Por ejemplo:

```
{
   "apiUrl": "https://api.yourqvdserver.com:443"
}
```

Ejecutando el WAT

El WAT es independiente de la API en cuanto a instalación. Se pueden instalar en máquinas distintas y funcionar sin problemas, siempre que el WAT tenga en su configuración la dirección de la API. No obstante, y puesto que también se pueden instalar juntos, como es nuestro caso en mononodo, la API sirve por defecto el WAT, no siendo necesario configurar ningún servidor apache o nginx que lo sirva.

Para arrancar el WAT en nuestro ejemplo por tanto solo es necesario tener la API arrancada. Pruebe la conexión en su navegador, visitando https://localhost:443

Para iniciar sesión, puede usar el nombre de usuario y la contraseña predeterminados:

- **user**: superadmin@*
- **password**: superadmin

Puede cambiar esta contraseña desde el propio WAT.

Chapter 3

Configuración básica e indispensable

Ahora que tiene instaladas las herramientas administrativas, vamos a utilizarlas para configurar su nodo.

3.1 Configuración de red

Los nodos servidor QVD hacen uso de un puente de red y de interfaces de red virtuales para facilitar interfaces de red a cada una de las máquinas virtuales que se ejecutan en el nodo. Con el fin de proporcionar direcciones IP a máquinas virtuales, QVD también ejecuta un servidor DHCP que asignará las direcciones IP dentro del rango de la red virtual a los hosts virtuales a medida que se inician. Por lo tanto es muy importante que elija un rango de red que sea poco probable que entre en conflicto con cualquiera de sus otras infraestructuras existentes para este fin.

Note
Los servicios que se ejecutan en sistemas de la misma red IP pueden verse afectados por QVD o cualquiera de las máquinas virtuales que se ejecutan en QVD.

En una instalación mononodo necesitará configurar algún tipo de NAT para que las máquinas virtuales tengan acceso a la red. Esto se logra generalmente configurando reglas *iptables* en el host. En este documento le proporcionaremos un ejemplo, pero usted puede encontrar que un enfoque alternativo es más adecuado para su entorno.

Hay una serie de pasos de configuración que puede ser necesario realizar manualmente para configurar correctamente la red para un nodo servidor QVD. A menudo hay otras maneras de lograr una configuración de red apropiada, por lo que los proporcionamos sólo como directrices.

3.1.1 Establecer dnsmasq para ser controlado por QVD

QVD utiliza dnsmasq como servidor DHCP y DNS para las máquinas virtuales que se ejecutan en un nodo. Para funcionar correctamente, dnsmasq necesita ser ejecutado por el proceso HKD.

- En primer lugar, verifique el estado del servicio:

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

- De forma predeterminada, cuando dnsmasq esta instalado, se inicia como un demonio en segundo plano, así que debe evitar que comience automáticamente. Esto se hace con los siguientes comandos:

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

Note
Este paso es esencial para que QVD funcione utilizando la virtualización KVM. Para LXC es posible especificar si se debe o no hacer uso de DHCP para configurar la red dentro de sus máquinas virtuales.

3.1.2 Configurar el reenvío IP

La redirección IP (IP Forwarding) es necesaria para encaminar a los clientes a la ubicación correcta. Puede habilitarla rápidamente ejecutando el siguiente comando.

```
root@qvdnode:~# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Desafortunadamente, al reiniciar el sistema host, este cambio se perderá. Para que sea permanente, puede editar `/etc/sysctl.conf` y descomentar la línea:

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

Puede obligar a sysctl a recargar su configuración después de haber editado este archivo ejecutando:

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

3.1.3 Configurar un puente de red

Hay varias formas de configurar el puente de red y el enrutamiento apropiado para asegurarse de que un cliente QVD se enruta a la máquina virtual correcta.

El método más fácil es configurar una interfaz de red estática y un conjunto de reglas de enrutamiento **iptables** para realizar el NAT necesario para traducir las direcciones IP entre su red real y virtual.

Ubuntu 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
```

CENTOS

- Instalar las herramientas necesarias

```
root@qvdnode:~# yum install bridge-utils -y
```

- Comprobar que el modulo de puente está cargado con el comando:

```
root@qvdnode:~# modinfo bridge
```

  - Si no está cargado ejecutar:

```
root@qvdnode:~# modprobe --first-time bridge
```

- Para crear el fichero de configuración de la interfaz que se utilizará para QVD ejecute:

```
root@qvdnode:~# vi /etc/sysconfig/network-scripts/ifcfg-qvdnet0
```

– Agregue las líneas siguientes:

```
DEVICE="qvdnet0"
BOOTPROTO="static"
IPADDR="10.3.15.1"
NETMASK="255.255.255.0"
ONBOOT="yes"
TYPE="Bridge"
NM_CONTROLLED="no"
```

- **Configuracion de Cortafuegos en CentOS**

  Habilitar el NAT para la navegacion de los contenedores, para ello se requiere de 2 zonas, internal y external. La zona internal usara la red de contenedores 10.3.15.0/24 o la que haya sido elegida con interface **`qvdnet0`** previamente creada. Y la zona external debera usar la interface **`eth0`** (sustituir por interface de red externa), para ello hacemos lo siguiente:

```
root@qvdnode:~# firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTING ↩
     -o eth0 -j MASQUERADE -s 10.3.15.0/24
root@qvdnode:~# firewall-cmd --change-interface=eth0 --zone=external --permanent
root@qvdnode:~# firewall-cmd --set-default-zone=external
root@qvdnode:~# firewall-cmd --change-interface=qvdnet0 --zone=internal --permanent
```

  Hacer un "port forwarding" del puerto 8443 en red external al puerto 8443 en red internal a la ip del bridge qvdnet0 10.3.15.1.

```
root@qvdnode:~# firewall-cmd --zone=external --add-forward-port=port=8443:proto=tcp:toport ↩
    =8443:toaddr=10.3.15.1 --permanent
```

  Abrir en la red external los puertos de conexion que utiliza QVD, 8443 para la conexion a las sesiones y 443 para conectar con WAT.

```
root@qvdnode:~# firewall-cmd --add-port=8443/tcp --permanent --zone=external
root@qvdnode:~# firewall-cmd --add-service=https --permanent --zone=external
```

  Recargar las reglas para aplicar los cambios realizados:

```
root@qvdnode:~# firewall-cmd --complete-reload
```

Es importante señalar que en el ejemplo anterior 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. En el ejemplo de arriba usamos el rango **10.3.15.0/24** para la red virtual utilizada por QVD. Este rango debe ser único dentro de su infraestructura y debe dedicarse al uso de QVD, de modo que los servicios que arranquen en QVD no interfieran en otros sistemas dentro de su red.

Si bien hay otros enfoques más limpios para configurar su red, estos a veces tienen problemas con interfaces de red particulares tales como WIFI. El enfoque mencionado anteriormente debería funcionar para la mayoría de los sistemas.

Una vez que haya realizado la configuración de red:

En Ubuntu, deberá levantar la interfaz de puente de red.

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

En CentOS, deberá reiniciar el servicio de red:

```
root@qvdnode:~# systemctl restart network
```

3.1.4 Configurar QVD para su red

Para que QVD administre correctamente la configuración de la máquina virtual y el enrutamiento subsiguiente, necesitará cambiar algunos ajustes de configuración dentro de QVD-DB. Se recomienda que utilice la Utilidad de Administración CLI de QVD para hacer esto. También puede utilizar el WAT si ya lo ha configurado.

Estos ajustes se utilizan para proporcionar un entorno de red dedicado para las Máquinas virtuales. Debe utilizar direcciones IP y rangos de red que no entren en conflicto con su infraestructura de red existente. En el ejemplo a continuación se utiliza el rango **10.3.15.0/24** para la red virtual utilizada por QVD.

Estos parámetros son obligatorios y los demonios QVD se negarán a iniciarse a menos que estén definidos. Son los siguientes:

- **`vm.network.use_dhcp,value`**: Habilitar/deshabilitar servicio dhcp
- **`vm.network.ip.start`**: Primera IP del rango reservado para máquinas virtuales
- **`vm.network.netmask`**: Máscara de red del rango
- **`vm.network.gateway`**: IP del router que permite acceder al exterior. Será transmitido por DHCP a las máquinas virtuales
- **`vm.network.dns_server`**: Sistema de nombres de dominio
- **`vm.network.bridge`**: Nombre de la interfaz puente reservada para QVD

Estas entradas se pueden establecer en la base de datos utilizando el comando `qa` disponible en el paquete `perl-qvd-admin` de la siguiente manera:

```
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
```

Important
Si está ejecutando **AppArmor** en su máquina host, podrá comprobar que evita que las máquinas host accedan a Internet. Tenemos un perfil de AppArmor para QVD que está disponible en los paquetes. En cualquier caso, también es posible deshabilitar AppArmor con `/etc/init.d/apparmor teardown`. Esto detendrá AppArmor y permitirá ejecutar normalmente QVD. Si esto es inaceptable en el entorno en producción, utilice el perfil referido y pida ayuda al equipo de soporte QVD si es necesario.

Estos ajustes se describen con más detalle en la sección del **Manual de administración de QVD** titulado **Virtual Machine Options** en el capítulo **Configuración básica de QVD**.

3.2 Configurar QVD para usar los certificados SSL

Anteriormente, creamos un directorio `/etc/qvd/certs` para almacenar nuestro certificado autofirmado. Si está utilizando un certificado firmado por una entidad emisora reconocida, es posible que desee colocar sus certificados en el mismo lugar para que las siguientes instrucciones tengan sentido.

En este paso, configuraremos QVD para que utilice el certificado del servidor y la clave privada. Para ello, utilizaremos la herramienta qvd-admin.

```
root@qvdnode:~# qa config ssl key=/etc/qvd/certs/key.pem cert=/etc/qvd/certs/cert.pem
```

Si el certificado no está firmado por una autoridad de confianza, debe agregarse al directorio de certificados de confianza del sistema para que la capa SSL lo pueda validar. Para averiguar cual es ese directorio, ejecute el siguiente comando:

```
root@qvdnode:~# openssl version -d
```

El directorio de certificados de confianza siempre es un subdirectorio llamado **certs** dentro del directorio devuelto por el comando anterior.

Por ejemplo, el comando puede devolver la respuesta siguiente:

Ubuntu:

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

CentOS:

```
OPENSSLDIR: "/etc/pki/tls"
```

Esto indicaría que los certificados de confianza se almacenan en `/usr/lib/ssl/certs` en Ubuntu y en `/etc/pki/tls/certs` en CentOS. En la mayoría de los casos esto es realmente un enlace simbólico a otro lugar, pero esta ruta debe ser suficiente para trabajar con los certificados.

Para que SSL reconozca el certificado, debe ser nombrado correctamente. Los siguientes comandos le ayudarán a asegurarse de que el certificado se denomina correctamente.

Ubuntu:

```
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
```

CentOS

```
root@qvdnode:~# trusted_ssl_path=/etc/pki/tls/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
```

Por supuesto, independientemente de su distribución, es importante que compruebe el **trusted_ssl_path** y el **cert_path** en los comandos enumerados anteriormente. Si es necesario, cámbielos para que coincidan con su entorno.

Los comandos enumerados anteriormente se asegurarán primero de que obtengamos el nombre correcto para su certificado y, a continuación, copiaremos el certificado a la ruta donde se almacenarán los certificados de confianza, renombrándolo a `QVD-L7R-cert.pem` de manera que tenga un nombre que tenga sentido para usted más adelante. Finalmente, creamos un enlace simbólico desde el certificado hasta el nombre que OpenSSL espera para usar el archivo de certificado.

3.2.1 Configuración del nodo HKD

- Una vez que se ha realizado toda la configuración, añada 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
```

Chapter 4

Instalación y configuración del cliente QVD

El cliente QVD está disponible para plataformas Linux, Microsoft Windows y Mac OSX.

Sea cual sea su elección de plataforma para ejecutar la aplicación cliente, lo mejor es que la ejecute en un sistema diferente del que está utilizando para ejecutar componentes del servidor. Esto le dará una imagen mucho mejor de cómo funciona todo el entorno.

4.1 Cliente Windows

Si utiliza Microsoft Windows como su plataforma base para ejecutar la aplicación cliente QVD, deberá descargar manualmente el instalador del cliente QVD. Puede descargar el instalador de:

http://theqvd.com/download#windows

Una vez que haya terminado de descargar el instalador, ejecútelo como un archivo ejecutable normal y siga el asistente durante el proceso de instalación.

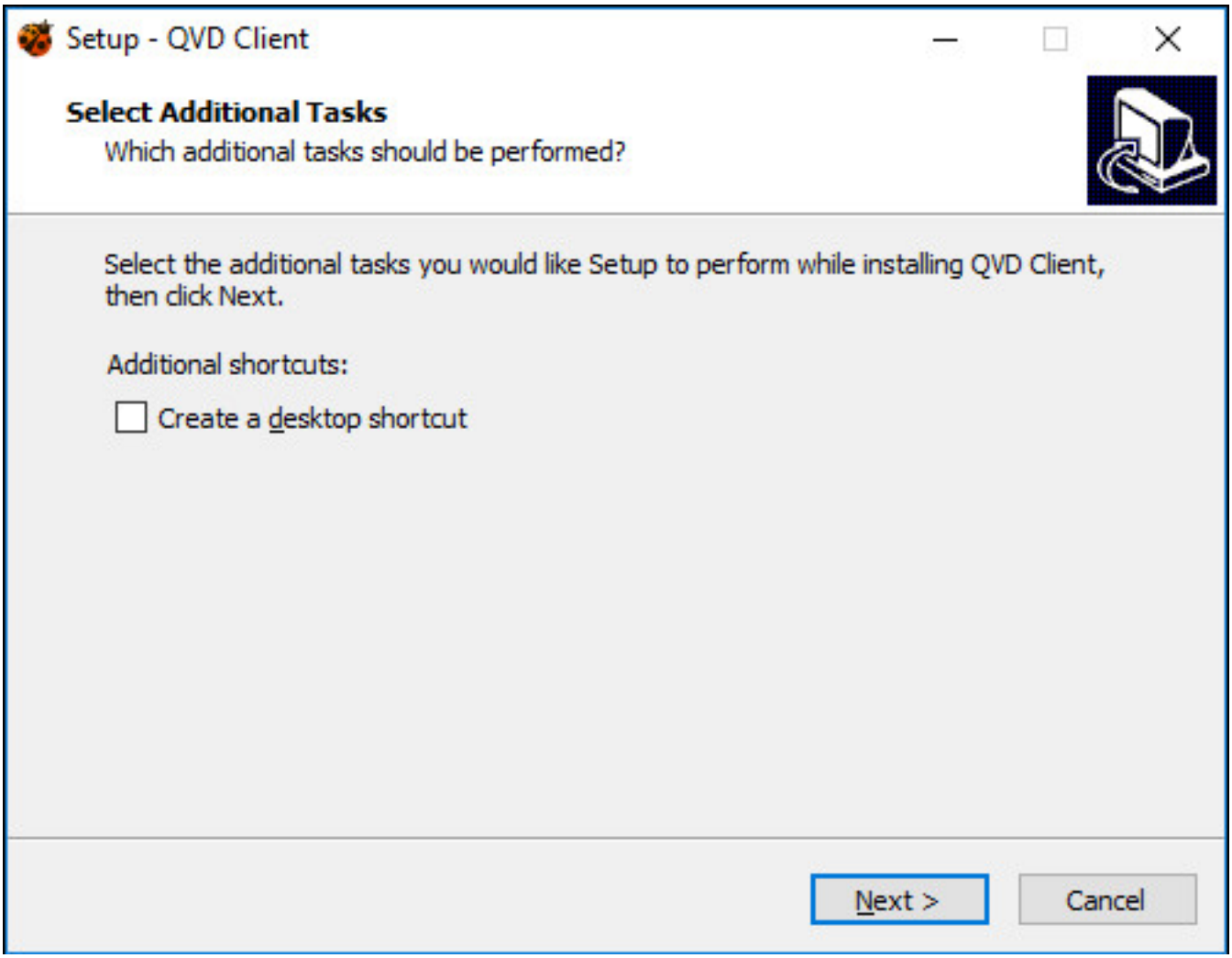

Figure 4.1: El Asistente de instalación de Windows QVD Client

Una vez que haya terminado la instalación, puede ejecutar el cliente desde el acceso directo en el escritorio de Windows (si ha seleccionado agregar el acceso directo) o desde el menú QVD en el menú Aplicaciones. Esto abrirá el cliente para que esté listo para conectarse.

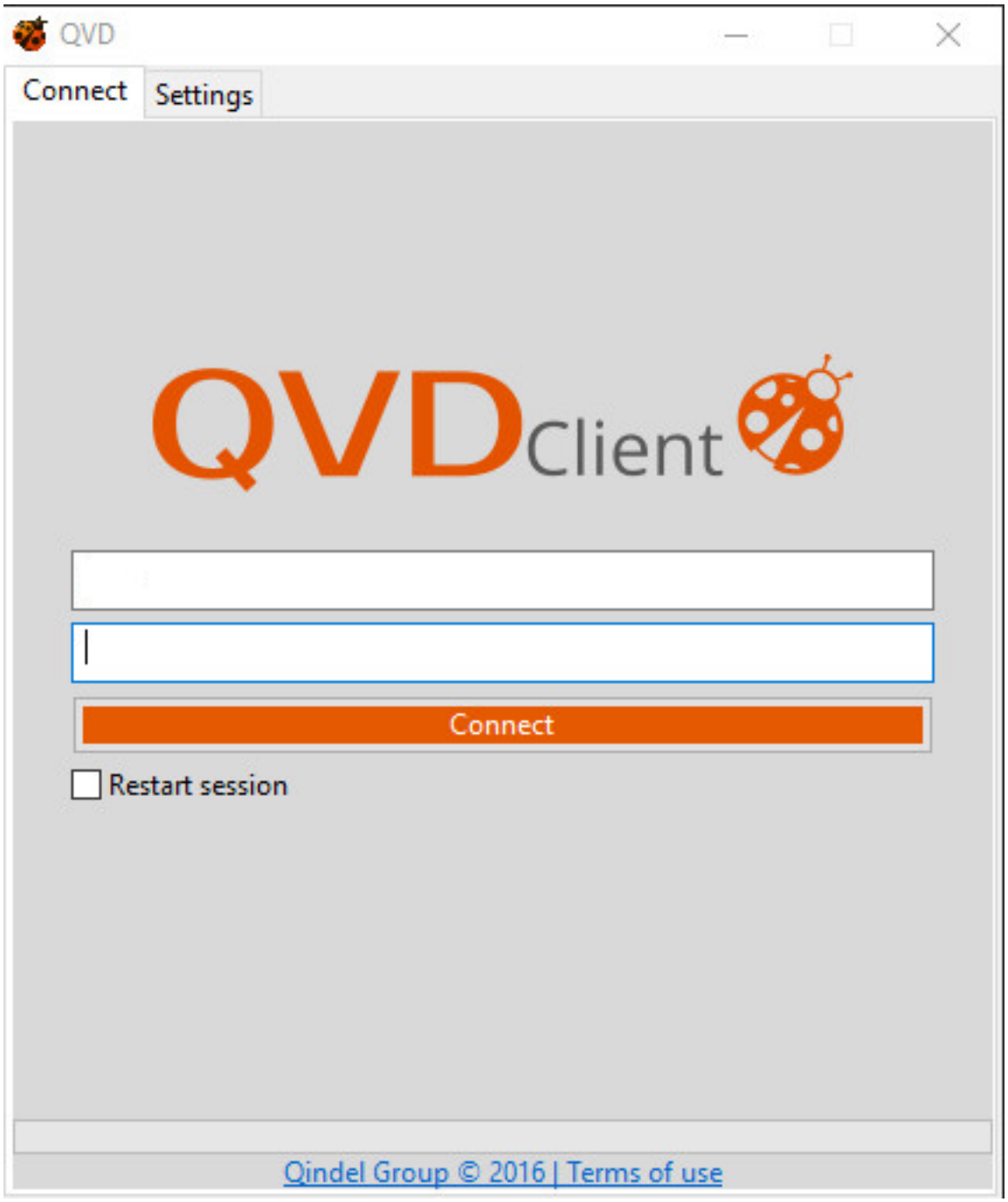

Figure 4.2: El cliente de Windows QVD

Si se desean usar la impresión en VMA anteriores a 4.2 es necesario realizar los siguientes pasos:

- Compartir las impresoras
- Ir a *Administrar la configuración avanzada de uso compartido*.
- Asegúrese de que en su *perfil actual* esté activado el uso compartido de archivos e impresoras.
- En *todas las redes*, desactive el uso compartido con contraseña en la parte inferior.

4.2 Cliente OSX

Si utiliza Mac OSX como su plataforma base deberá tener instalado como prerrequisito el servidor de X **Xquartz** que ha dejado de distribuirse por defecto con Mac OS.

Xquartz

Para ejecutar la aplicación cliente QVD, deberá descargar manualmente el instalador del cliente QVD. Puede descargar el instalador de:

http://theqvd.com/download#osx

Una vez que haya terminado de descargar el instalador, ejecútelo como un archivo ejecutable normal y siga el asistente durante el proceso de instalación.

Una vez que haya terminado la instalación, puede ejecutar el cliente desde el Launcher.

4.3 Cliente Linux

Instalar el cliente de QVD en una plataforma Ubuntu Linux es simple. Debe agregar el repositorio de QVD a las fuentes del repositorio de apt si aún no lo ha hecho.

Ahora podrá instalar el cliente con el siguiente comando:

Ubuntu:

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

CentOS:

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

Dependiendo del entorno de escritorio, debería poder acceder al cliente dentro del menú "Aplicaciones", normalmente en el submenú "Internet". Como alternativa, puede ejecutar la GUI del cliente desde la consola utilizando el comando `/usr/lib/qvd/bin/qvd-gui-client.pl`.

¿Y ahora qué?

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

- Instalar su primera imagen
- Agregar su primer usuario
- Conectarse y probar la solución

Desde la versión 4.0 de QVD, el WAT se ha convertido en la herramienta de administración estándar del producto. Le recomendamos que siga con la guía del WAT para realizar estos pasos, y continuar así con su aprendizaje de QVD.

Conclusión

En esta guía, hemos pasado por una instalación básica y la configuración de todos los componentes dentro de una solución QVD. Esperamos que, siguiendo la guía haya logrado configurar su propia solución de escritorio virtual y haya sido capaz de conectarse a ella con un cliente QVD.

QVD se puede utilizar para una amplia gama de propósitos y escalas muy diferentes, por lo que es la primera opción como plataforma de virtualización de escritorio dentro de la empresa. Sus facilidades de administración remota, su capacidad de integración con otras tecnologías y las posibilidades de conexión para usuarios remotos de una manera segura le ayudarán a mejorar la administración de sus usuarios de Linux y Solaris y reducir los costos asociados con la virtualización de escritorios.

–

Si tiene alguna pregunta ó necesita soporte adicional, visite nuestro sitio web ó póngase en contacto con nosotros.

Menú Principal