LA GUÍA PARA PRINCIPIANTES DE

Instalación de QVD 4.2

QVD DOCUMENTATION

<documentation@theqvd.com>

February 23, 2022

Contents

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 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 versión 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 *Uso de LXC Virtualization en 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.

Part I

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 **SUSE**, **Ubuntu**, **CentOS** y **Rocky Linux**.

Esta guía asumirá que usted está instalando los paquetes en **Rocky 8.5**.

En resumen:

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

0.1 Rocky Linux

Los paquetes para el entorno del nodo HKD están disponibles en

```
http://theqvd.com/packages/sles/12SP1/stable
```

En primer lugar, agregue la clave pública de los paquetes QVD a sus claves de confianza (como root):

```
# rpm --import https://www.theqvd.com/packages/key/public.key
```

Ahora, agregue el repositorio:

```
# yum-config-manager --add-repo http://theqvd.com/packages/centos/7.2/QVD-4.2.0/
```

Para paquetes comerciales:

```
# echo "[QVD-4.2.0]" > /etc/yum.repos.d/QVD-4.2.0.repo
# echo "name=QVD-4.2.0" >> /etc/yum.repos.d/QVD-4.2.0.repo
# echo "baseurl=http://$USUARIO:$PASSWORD@theqvd.com/commercial-packages/centos/7.2/QVD ↩
    -4.2.0/" | sed 's/@\(.*@\)/%40\1/' >> /etc/yum.repos.d/QVD-4.2.0.repo
# echo "enabled=1" >> /etc/yum.repos.d/QVD-4.2.0.repo
```

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

El repositorio QVD 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

Como anteriormente, los componentes de código abierto requeridos por QVD son los que siguen:

- El RSGBD de PostgreSQL.
- KVM: Hipervisor.
- NX: protocolo que maneja las conexiones de escritorio remoto.
- Ebtables: una utilidad de cortafuegos basada en IP para puentes ethernet

0.2 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 2 GB de RAM. Esto debe ser suficiente para un máximo de 4 usuarios.
- **Espacio en disco**: Al menos 4 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 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. También clientes beta para Android e iOS.

0.3 Red

Los nodos HKD utilizan interfaces de puente de red y de red virtual para facilitar la interconexión en red de cada una de las máquinas virtuales que se ejecutan en el nodo. Con el fin de proporcionar automáticamente direcciones IP a las máquinas virtuales, QVD también ejecuta un servidor DHCP que asignará 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 cualquier otra de su infraestructura existente.

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.

Los pasos de conexión en red se tratan con más detalle más adelante en este documento, sin embargo lo más importante a tener en cuenta en este momento es que debe asegurarse de que tiene un rango de IP de red dedicado que se puede utilizar para las máquinas virtuales que se ejecutarán dentro de QVD.

Además, en una instalación mononodo, como la que estamos describiendo aquí, 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.

Important
Hay una funcionalidad en el Panel de Administración Web (WAT) llamada Espía de Sesión utilizada para dar soporte a los usuarios conectándonos a sus escritorios VNC. Esta herramienta funciona estableciendo una conexión desde la QVD API hacia el servidor x11vnc que se encuentra instalado y escuchando en las máquinas virtuales. Por esta razón, la máquina donde se encuentre instalada la QVD API, deberá tener conectividad con la subred donde se encuentren las máquinas virtuales de QVD por el puerto 3030.

Chapter 1

Instalación y configuración de QVD DB

Dado que uno de los componentes más fundamentales de la solución QVD es la base de datos, le sugerimos que instale esto primero. La base de datos se utilizará para vincular todos los demás componentes y para permitirles interactuar. El software QVD tiene una base de datos PostgreSQL en su núcleo. Toda la información de configuración y tiempo de ejecución se almacena en la base de datos y si falla, la plataforma al completo dejará de funcionar.

En los sistemas de producción, se recomienda encarecidamente que la base de datos se instale en una configuración de alta disponibilidad, de modo que no se convierta en un posible punto de fallo para su solución VDI. En general, los requisitos reales de hardware son muy modestos, cualquier servidor moderno con sólo dos núcleos de CPU y 2 GB de RAM será capaz de soportar la carga de la base de datos.

En esta configuración de demostración, es poco probable que genere mucha carga y asumiremos que su plataforma de prueba será capaz de hacer frente a los requisitos.

1.1 Instalación

La forma recomendada de instalar la base de datos central es con el paquete perl-qvd-db. Para instalar ejecutar como root:

```
root@myserver:~# apt-get install perl-qvd-db
```

Después de instalar `perl-qvd-db`, tiene que realizar varios pasos manuales. 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.

Debido a que QVD está diseñado para ejecutarse desde uno o más nodos servidor, el paquete `perl-qvd-db` no requiere el servidor postgresql como dependencia. Sin embargo, para los propósitos de esta guía de instalación, necesitaremos el servidor instalado en la máquina local. Por supuesto, podría utilizar un servidor en otra máquina y adaptar su configuración en consecuencia. Instale lo siguiente:

```
# yum install https://download.postgresql.org/pub/repos/yum/9.3/redhat/rhel-7-x86_64/pgdg- ↩
    centos93-9.3-2.noarch.rpm
# yum install postgresql93-server postgresql93-contrib
# /usr/pgsql-9.3/bin/postgresql93-setup initdb
```

Ahora, inicie el servidor postgresql:

```
# systemctl start postgresql
```

Important
Deseamos recordarle nuevamente que la versión mínima de PostgreSQL para QVD 4.2 es la 9.3.

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):

```
# su - postgres
```

1.2 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@myserver:~$ 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.

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

1.4 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 9.3, aunque puede que necesite ajustar algunas rutas según sea necesario.

Los archivos de configuración se encuentran en `/var/lib/pgsql/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 *.

```
root@myserver:~# cd /var/lib/pgsql/data
root@myserver:/var/lib/pgsql/data # vi postgresql.conf
listen_addresses = '*'
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`. Esto será en `/var/lib/pgsql/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.

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

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

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

```
root@myserver:~# 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:

```
#
# QVD Node Configuration
#

# Name of this node in QVD. Usually the machine's hostname.
nodename = mycomputer

# Database connection information.
# database.host: where the QVD database is found
database.host=mycomputer
# database.name: the name of the QVD database
database.name=qvddb
# database.user: the user account needed to connect
database.user=qvd
# database.password: the password needed to connect
```

```
database.password=passw0rd

# Log level. One of ALL, DEBUG, INFO, WARN, ERROR, FATAL, OFF
log.level = ALL
log.filename = /var/log/qvd/qvd.log
```

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.

1.6 Instalación de las tablas 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. Esto creará la estructura de tabla que QVD necesita.

```
# /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.

1.7 Prueba de acceso

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

```
# psql -U qvd -W -h localhost -d qvddb
Password for user qvd:
psql (9.3.0)

qvd=> \d<return>
```

Chapter 2

Instalación y configuración del nodo

2.1 Instalación del HKD

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

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

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

2.2 Instalación de las herramientas de administración

2.2.1 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:

```
root@myserver:~# 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 connection information.
# database.host: where the QVD database is found
database.host=mycomputer
# database.name: the name of the QVD database
database.name=qvddb
# database.user: the user account needed to connect
database.user=qvd
# database.password: the password needed to connect
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@myserver:~# systemctl start qvd-api
```

2.2.2 CLI

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

```
root@myserver:~# 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.

2.2.3 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.

Instale el paquete:

```
# 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 Parámetros de configuración internos de QVD

Si bien es posible agregar otros parámetros de configuración al archivo de configuración de nodo QVD que hemos editado anteriormente, este archivo simplemente se utiliza para arrancar el servidor y posteriormente el servidor se referirá a la base de datos para encontrar cualquier otra entrada de configuración, por lo que es mejor práctica establecer los parámetros de configuración QVD dentro de la base de datos.

Hay algunos parámetros que deben definirse para informar a QVD acerca de su entorno (por ejemplo, el rango de direcciones IP disponibles para las máquinas virtuales o su puerta de enlace predeterminada). Estos parámetros son obligatorios y los demonios QVD se negarán a iniciarse a menos que estén definidos. Son los siguientes:

- `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.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:

```
# 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.bridge,value=qvdnet0
```

3.2 Requisitos 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.

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.

3.2.1 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, compruebe que dnsmasq está instalado. En Ubuntu, ejecute los siguientes comandos y compruebe el estado:

```
# dpkg -s dnsmasq
```

En SUSE:

```
# rpm -q dnsmasq
```

Si no está instalado, hágalo ahora utilizando su gestor de paquetes, ya sea `apt-get install dnsmasq`, o `zypper install dnsmasq`.

De forma predeterminada, el paquete Ubuntu inicia el proceso que se ejecuta como un demonio en segundo plano, así que debe evitar que comience automáticamente. Esto se hace con los siguientes comandos en Ubuntu:

```
# service dnsmasq stop
# sed -i s/ENABLED=1/ENABLED=0/ /etc/default/dnsmasq
```

En SLES dnsmasq se gestiona bajo el comando chkconfig y se deshabilita de forma predeterminada, por lo que no debería necesito hacer nada. Sin embargo, en caso de que dnsmasq se haya habilitado o por asegurarse, puede comprobar que está desactivado ejecutando el siguiente comando como root:

```
# chkconfig dnsmasq off
```

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.

3.2.2 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.

```
# 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:

```
# sysctl -p
```

3.2.3 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.

Para configurar su red en 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
```

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 escrito la configuración de red en un archivo, debe levantar la interfaz de puente de red.

```
# ifup qvdnet0
```

Configurar un puente de red en SLES

Si utiliza SLES, le recomendamos que utilice Yast2 para configurar su puente de red.

Abra Yast y vaya a Dispositivos de red → Configuración de red → Agregar.

Defina las opciones siguientes:

- Tipo de dispositivo:"bridge"
- Nombre de configuración:"0" (La cadena será un sufijo de br, así que aquí el nombre del puente será br0).
- Deje todos los campos restantes como están.
- Seleccione Siguiente.
- Seleccione el dispositivo físico que desea que forme parte del puente. (Marque eth0 por ejemplo).
- Seleccione Siguiente.
- Seleccione Aceptar.
- El dispositivo de red se configurará automáticamente en unos segundos.

3.2.4 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.

```
# 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
```

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**.

3.3 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. Si ya tiene un certificado firmado por un tercero, puede omitir este paso y utilizar su certificado firmado.

3.3.1 Creación de un certificado autofirmado

La herramienta openssl es necesaria para crear un certificado autofirmado. Si aún no lo ha instalado, puede hacerlo de la siguiente forma:

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

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

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

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

```
root@myserver:~# openssl genrsa 2048 > key.pem
```

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

```
root@myserver:~# openssl req -new -x509 -nodes -sha256 -days 60 -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) []:qvd.qindel.com
Email Address []:documentation@theqvd.com
```

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

3.3.2 Configurar QVD para usar los certificados SSL

En el paso anterior 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@myserver:~# 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@myserver:~# 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:

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

Esto indicaría que los certificados de confianza se almacenan en `/etc/ssl/certs`. 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.

```
# trusted_ssl_path=/usr/lib/ssl/certs
# 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
```

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.

Part II

¿Y ahora qué?

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

- Agregar su nodo HKD a la solución
- 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.

También necesitará instalar el cliente QVD. En la guía de Administración encontrará un apartado sobre su instalación y uso.

Part III

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 o necesita soporte adicional, visite nuestro sitio web en http://theqvd.com/ o póngase en contacto con nosotros en info@theqvd.com.