

LIBVIRT: Mise en réseau pontée virtualisée avec MacVTap

Table of Contents

- [LIBVIRT: Mise en réseau pontée virtualisée avec MacVTap](#)
- [Présentation de l'interface Macvtap](#)
 - [Notions générales](#)
 - [Modes de fonctionnement](#)
 - [Mode d'agrégateur de ports Ethernet virtuels \(VEPA\)](#)
 - [Mode pont](#)
 - [Mode privé](#)
- [Utilisation de KVM avec les interfaces Libvirt et macvtap](#)
 - [Création d'un interface Macvtap](#)
 - [Vérifier le noyau linux](#)
 - [Définir un réseau macvtap](#)
 - [Utilisation de l'interface](#)

Cet article, explique comment utiliser KVM avec les interfaces Libvirt et macvtap pour la mise en réseau (par opposition à un pont Linux ou à Open vSwitch).

Présentation de l'interface Macvtap

Notions générales

Une machine virtuelle doit généralement être connectée à un réseau pour être utile. Étant donné qu'une machine virtuelle s'exécute en tant qu'application sur l'ordinateur hôte, sa connexion au monde extérieur nécessite le support du système d'exploitation hôte. Il existe un certain nombre d'options pour la mise en réseau d'une machine virtuelle, à la fois sur la couche liaison et la couche réseau.

MacVTap est un pilote de périphérique Linux relativement nouveau, conçu pour faciliter la mise en réseau des machines virtuelles. Macvtap est essentiellement une combinaison du pilote Macvlan et d'un périphérique Tap:

- **Le pilote Macvlan** est un pilote de noyau Linux distinct dont dépend le pilote Macvtap. Macvlan permet de créer des interfaces réseau virtuelles qui «s'accrochent» à une interface réseau physique. Chaque interface virtuelle a sa propre adresse MAC distincte de l'adresse MAC de l'interface physique. Les trames envoyées vers ou depuis les interfaces virtuelles sont mappées sur l'interface physique, appelée interface inférieure .
- **Interfaces Tap** Une interface Tap est une interface exclusivement logicielle. Au lieu de passer des trames vers et depuis une carte Ethernet physique, les trames sont lues et écrites par un

programme d'espace utilisateur. Le noyau rend l'interface Tap disponible via le fichier de périphérique `/dev/tapN`, où N est l'index de l'interface réseau.

Une interface Macvtap combine les propriétés de ces deux éléments. c'est une interface virtuelle avec une interface logicielle de type tap. Une interface Macvtap peut être créée à l'aide de la commande `ip`:

```
$ sudo ip link add link eth0 name macvtap0 type macvtap
```

Cela ajoute une nouvelle interface appelée `macvtap0`, comme le montre la liste suivante:

```
$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16384 qdisc noqueue state UNKNOWN mode
DEFAULT
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
UP mode DEFAULT qlen 1000
    link/ether 00:1f:d0:15:7b:e6 brd ff:ff:ff:ff:ff:ff
3: macvtap0@eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT qlen 500
    link/ether 42:96:80:ee:2d:23 brd ff:ff:ff:ff:ff:ff
```

Le fichier de périphérique correspondant à la nouvelle interface `macvtap` avec l'index 3 est `/dev/tap3`. Ce fichier de périphérique est créé par `udev`.

```
$ ls -l /dev/tap3
crw----- 1 root root 252, 1 Oct 21 12:10 /dev/tap3
```

Un programme d'espace utilisateur peut ouvrir ce fichier de périphérique et l'utiliser pour envoyer et recevoir des trames Ethernet par dessus. Lorsque le noyau transmet une trame via l'interface `macvtap0`, au lieu de l'envoyer sur une carte Ethernet physique, il le rend disponible pour la lecture de ce fichier par le programme d'espace utilisateur. De même, lorsque le programme d'espace utilisateur écrit le contenu d'une trame Ethernet dans le fichier `/dev/tap3`, le code réseau du noyau voit la trame comme si elle avait été reçue via le périphérique `macvtap0`.

Le programme d'espace utilisateur est normalement un émulateur tel que QEMU, qui virtualise les cartes réseau sur les systèmes d'exploitation invités. Lorsque QEMU lit une trame Ethernet à l'aide du descripteur de fichier, il émule le comportement d'une vraie carte réseau. Généralement, il déclenche une interruption dans la machine virtuelle et le système d'exploitation invité peut alors lire la trame à partir de la carte réseau émulée.

Macvtap est implémenté dans le noyau Linux et doit être configuré lors de la compilation du noyau, en tant que module ou en tant que fonctionnalité intégrée.

Modes de fonctionnement

Un périphérique Macvtap peut fonctionner dans l'un des trois modes suivants: mode VEPA (Virtual Ethernet Port Aggregator), mode Bridge et mode Private. Les modes déterminent la manière dont les extrémités du tap communiquent entre elles.

Mode d'agrégateur de ports Ethernet virtuels (VEPA)

Dans ce mode, qui est le mode par défaut, les données entre les extrémités du même périphérique inférieur sont envoyées via le périphérique inférieur (carte Ethernet) au commutateur physique auquel le périphérique inférieur est connecté.

Le mode VEPA simplifie la tâche de l'ordinateur hôte en laissant le commutateur physique effectuer la commutation, pour laquelle le commutateur est très performant. Un autre avantage est que les administrateurs réseau peuvent surveiller le trafic entre des machines virtuelles à l'aide d'outils connus sur un commutateur géré, ce qui ne serait pas possible si les données ne sont jamais entrées dans le commutateur.

Ce mode nécessite que le commutateur prenne en charge le mode «Reflective Relay», également appelé mode «Hairpin». Reflective Relay signifie que le commutateur peut renvoyer une image sur le même port que celui sur lequel il l'a reçu. Malheureusement, la plupart des commutateurs actuels ne prennent pas encore en charge le mode Reflective Relay, car le protocole STP (Spanning Tree Protocol) l'empêche et, avant l'avènement de la virtualisation, il n'était pas logique qu'une frame passe par le même port.

Mode pont

Lorsque le périphérique MacVTap est en mode Bridge, les ordinateurs d'extrémité peuvent communiquer directement sans envoyer les données via le périphérique inférieur. Lorsqu'on utilise ce mode, le commutateur physique n'a pas besoin de prendre en charge le mode Reflective Relay.

Mode privé

En mode privé, les nœuds du même périphérique MacVTap ne peuvent jamais se parler, que le commutateur physique prenne en charge le mode de Reflective Relay ou non. On utilise ce mode lorsqu'on souhaite isoler les machines virtuelles connectées aux ordinateurs d'extrémité, mais pas du réseau extérieur.

Utilisation de KVM avec les interfaces Libvirt et macvtap

Avec le toolkit libvirt (libvirt.org) pour gérer vos machines virtuelles, ajouter une définition d'interface réseau semblable à celle-ci dans le fichier XML de votre domaine:

Création d'un interface Macvtap

Vérifier le noyau linux

Les interfaces Macvtap sont liées aux interfaces macvlan (elles partagent le même pilote de noyau). Par conséquent, il faut d'abord s'assurer que le noyau Linux prend en charge le pilote macvlan. Ces commandes aideront à savoir si le noyau est prêt à fonctionner:

```
modprobe macvlan  
lsmod | grep macvlan
```

Définir un réseau macvtap

Une fois que KVM et Libvirt sont installés et fonctionnent correctement, commencer par définir un réseau Libvirt auquel les ordinateurs virtuels créés seront connectés.

Cet extrait de code XML définit un réseau Libvirt qui utilise les interfaces macvtap associées à l'interface physique eth1 :

```
<network>  
  <name>macvtap-net</name>  
  <forward mode="bridge">  
    <interface dev="eth1"/>  
  </forward>  
</network>
```

Utiliser la commande virsh net-define avec ce XML pour définir le réseau Libvirt actuel. En supposant que le code XML ci-dessus soit stocké dans un fichier nommé macvtap-def.xml, exécuter cette commande:

```
virsh net-define macvtap-def.xml
```

Ensuite, définir le démarrage automatique du réseau Libvirt résultant et le démarrer:

```
virsh net-autostart macvtap-net  
virsh net-start macvtap-net
```

Utilisation de l'interface

Maintenant on peut l'utiliser avec virt-install utilisant une commande comme celle-ci (avec une ligne encapsulée pour la lisibilité):

```
virt-install --name=cirros --ram=256 --vcpus=1 \ --disk  
path=/home/user/cirros-0.3.2-x86_64-disk.img,format=qcow2 \ --import --  
network network:macvtap-net,model=virtio --vnc
```

Une fois cette commande terminée, un domaine invité KVM sera exécuté et associé à une interface macvtap. On peut voir la nouvelle interface macvtap en exécutant ip link list :

```
5: macvtap0@eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc  
pfifo_fast state UNKNOWN mode DEFAULT group default qlen 500 link/ether  
52:54:00:5c:15:d6 brd ff:ff:ff:ff:ff:ff
```

From:

<http://www.ouarte.garden/> - **dwndoc**

Permanent link:

<http://www.ouarte.garden/doku.php?id=virtualisation:libvirt-macvtap>

Last update: **2025/02/19 10:59**

