链滴

11、高级网络配置

作者：sunjvhui

原文链接：https://ld246.com/article/1562826670800

来源网站：链滴

高级网络配置

Docker 网络

当docekr 启动时，会自动在主机上创建docker0虚拟网桥，实际上是liunx的一个bridge，可以理解一个软件交换机。它还会挂载到它的网口之间进行转发。

同时,docker随机分配一个本地未占用的私有网段（在RFC1918中定义）中的一个地址给docker0接，比如典型的 127.17.42.1 ,掩码为255.255.0.0。此后启动的容器内的网口也会自动分配一个同一网（172.17.0.0/16）的地址。

当创建一个Docker容器的时候，同时会创建了一对veth pair 接口，（当数据包发送到一个接口时，外一个接口也可以收到相同的数据包）。这对接口一端在容器内，即 eth0；另一端在本地并被挂载docker0网桥，名称以 veth 开头，（例如 vethAAQI2QT）。通过这种方式，主机可以跟容器通信容器之间也可以互相通信。Docker就创建了在主机和所有容器之间一个虚拟共享网络。

快速配置指南

跟 Docker 网络相关的命令列表。

其中有些命令选项只有在 Docker 服务启动的时候才能配置，而且不能马上生效。

- -b BRIDGE 或 --bridge=BRIDGE 指定容器挂载的网桥
- --bip=CIDR 定制 docker0 的掩码

- -H SOCKET... 或 --host=SOCKET... Docker 服务端接收命令的通道
- --icc=true|false 是否支持容器之间进行通信
- --ip-forward=true|false 请看下文容器之间的通信
- --iptables=true|false 是否允许 Docker 添加 iptables 规则
- --mtu=BYTES 容器网络中的 MTU

下面2个命令选项既可以在启动服务时指定，也可以在启动容器时指定。在 Docker 服务启动的时候定则会成为默认值，后面执行 docker run 时可以覆盖设置的默认值。

- --dns=IP_ADDRESS... 使用指定的DNS服务器
- --dns-search=DOMAIN... 指定DNS搜索域

最后这些选项只有在 docker run 执行时使用，因为它是针对容器的特性内容。

- -h HOSTNAME 或 --hostname=HOSTNAME 配置容器主机名
- --link=CONTAINER_NAME:ALIAS 添加到另一个容器的连接
- --net=bridge|none|container:NAME_or_ID|host 配置容器的桥接模式
- -p SPEC 或 --publish=SPEC 映射容器端口到宿主主机
- -P or --publish-all=true|false 映射容器所有端口到宿主主机

容器访问控制

容器的访问控制，主要通过 Linux 上的 iptables 防火墙来进行管理和实现。iptables 是 Linux 上默的防火墙软件，在大部分发行版中都自带。

容器访问外部网络

容器要想访问外部网络，需要本地系统的转发支持。在Linux 系统中，检查转发是否打开。

```
$sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
```

如果为 0，说明没有开启转发，则需要手动打开。

```
$sysctl -w net.ipv4.ip_forward=1
```

如果在启动 Docker 服务的时候设定 --ip-forward=true, Docker 就会自动设定系统的 ip_forward 数为 1。

容器之间互相访问

需要两方面支持

- 容器的网络拓扑是否已经互联。默认情况下，所有容器都会被连接到 docker0 网桥上。
- 本地系统的防火墙软件 — iptables 是否允许通过

访问所有端口

当启动Docker服务时，默认会添加一条转发策略到iptables的FORWARD链上，策略为通过（ACCEP）还是禁止（DROP）取决于配置--icc=true（缺省值）还是 --icc=false。当然，如果手动指定 --iptables=false 则不会添加 iptables 规则。

可见，默认情况下，不同容器之间是允许网络互通的。如果为了安全考虑，可以在 /etc/default/docker 文件中配置 DOCKER_OPTS=--icc=false 来禁止它。

访问指定端口

在通过 -icc=false关闭网络访问后，还可以通过 --link=CONTAINER_NAME:ALLAS 选项来访问容的开放端口。

例如，在启动 Docker 服务时，可以同时使用 icc=false --iptables=true 参数来关闭允许相互的网访问，并让 Docker 可以修改系统中的 iptables 规则。

此时，系统中的 iptables 规则可能是类似

```
$ sudo iptables -nL
...
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  0.0.0.0/0            0.0.0.0/0
...
```

注意：--link=CONTAINER_NAME:ALIAS 中的 CONTAINER_NAME 目前必须是 Docker 分配名字，或使用 --name 参数指定的名字。主机名则不会被识别。