

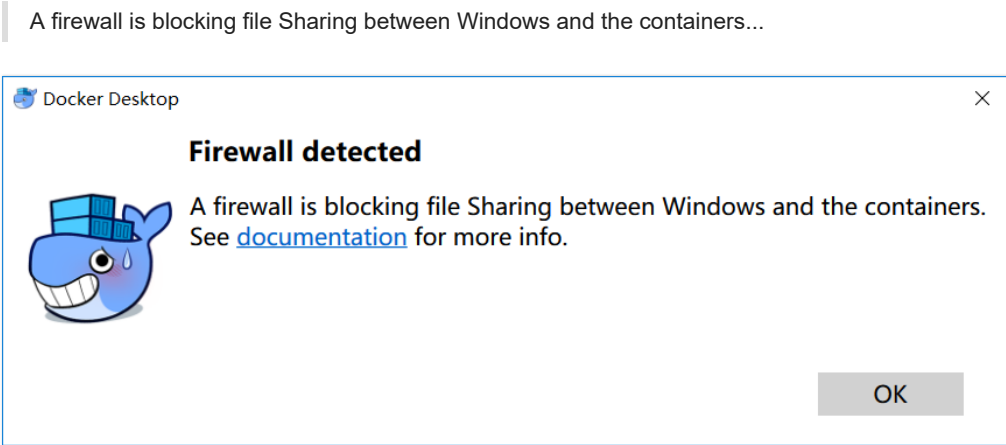


解决Docker for Windows无法共享磁盘的问题

yaxin 发表于 kuka的专栏

37

Docker for Windows 简化了windows下使用docker的流程，而且其有一项非常好的功能就是共享本地磁盘给docker（docker mount），但在实际使用中发现无法共享磁盘给docker，报错为：



0x01 错因分析

错误提示很明确，因为防火墙的问题导致无法正常共享磁盘。这里要提一下，Docker for Windows本质也是通过一个运行在hyper-v上Linux虚拟机来实现的，而其共享磁盘的方案也是通过 samba 来，也就是说，Windows作为samba服务器，然后运行docker的虚拟机通过smbclient访问Windows的samba服务。samba服务使用的是445端口，也就是说，docker虚拟机无法访问主机的445端口。可以通过下面的命令来验证：

```
docker run --rm -it --net=host alpine /bin/sh
nc -vz 10.0.75.1 445
```

```
run.png
```

上图中10.0.75.1为docker网络设置的网关，可以看到，如果端口无法访问，会在等待一段时间超时后报错。

那为什么防火墙会拦截samba服务了。首先我们要先分析一下防火墙的规则了。打开控制面板，依次选择“系统和安全”->“Windows Defender 防火墙”，然后打开左侧“高级设置”中的“入站规则”



可以看到进站规则中有很多“阻止的规则”，但是也有一条明确放通 10.0.75.1 对 445 端口的访问，可为什么还是不行呢？

通过Google，发现Windows的防火墙规则并不是按照规则先后顺序执行的，而是“**阻止规则**”优先级大于“**放通规则**”，参见：[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755191\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755191(v=ws.10))。

0x02 解决方法

那如何处理呢？当然可以通过关闭防火墙来直接验证。但是这只是一种临时的验证方式，因为关闭防火墙很不安全而且公司本身也不允许。

分析一下阻止规格，并不是所有源IP都被禁止了访问445端口，这就给我们提供了一个解决方式，找一个没有被禁止访问445端口IP端作为Docker for Windows的subnet address。

首先打开cmd，使用下面命令将所有入站的规则导出到文件中：

```
netsh advfirewall firewall show rule name=all dir=in type=dynamic status=enabled > d:/fir
```

然后将所有**操作为阻止，协议为TCP**的规则中的远程IP全部复制出来。然后上 `python` 处理，这里使用了**IPy库**进行网关的判断和处理。

```
from IPy import IP
# netsh advfirewall firewall show rule name=all dir=in type=dynamic status=enabled > d:/f
firewall_rules = """
169.254.2.0/24
10.3.128.0/17
9.19.161.0/26,9.19.161.64/26,10.3.224.0/19
"""

net_sets = []
for line in firewall_rules.strip().split('\n'):
    line = line.strip()
    line_seg = line.split(',')
    for net_string in line_seg:
        print(net_string)
        net_sets.append(IP(str(net_string)))

for net in net_sets:
    for l2 in range(0, 255):
        for l3 in range(0, 255):
            ip_net = "10.%s.%s.0" % (l2, l3)
            if ip_net in net:
                continue
            print("Net %s is available" % ip_net)
```

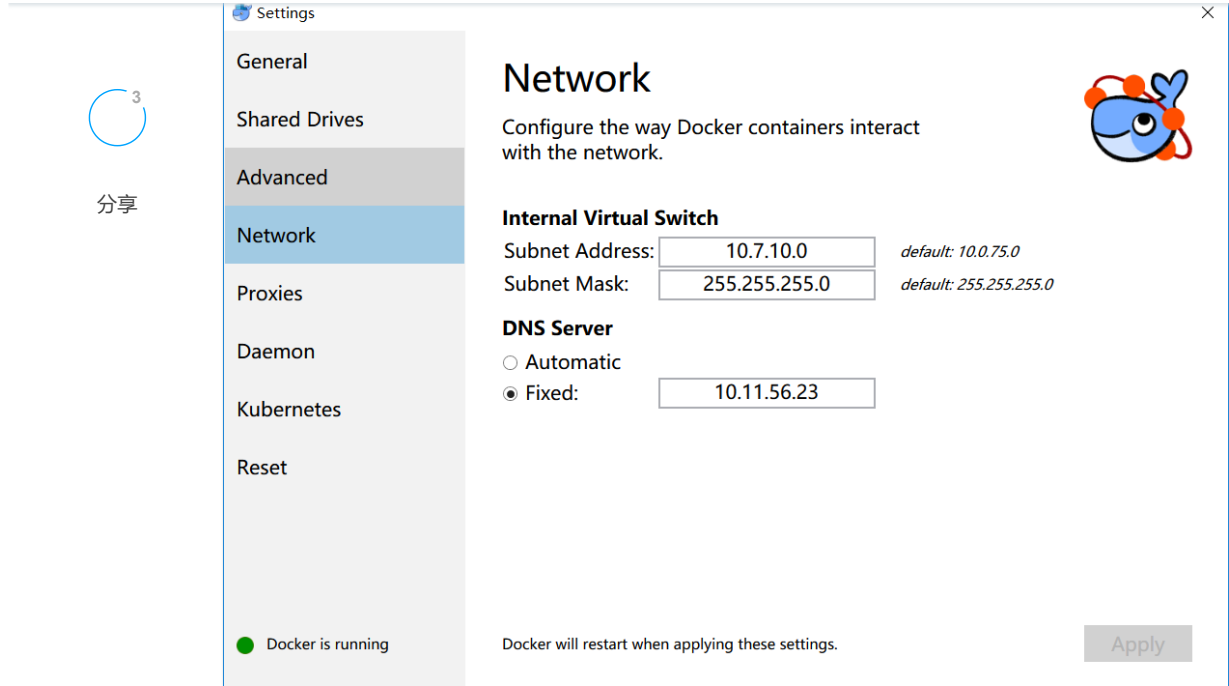



Image.png

原创声明，本文系作者授权云+社区发表，未经许可，不得转载。
如有侵权，请联系 yunjia_community@tencent.com 删除。

发表于 1 天前

容器网络安全DockerWindows

举报



kuka的专栏

1 篇文章 1 人订阅

订阅专栏

我来说两句

0 条评论

登录后参与评论

上一篇：[让Windows,Linux或OSX上的Chrome像ChromeOS一样运行Android Apps](#)
下一篇：[空间不够来折腾：手机系统备份到电脑](#)



分享

🔍

0

0