菜单 腾讯云首页 云市场 云+社区 备案 控制台



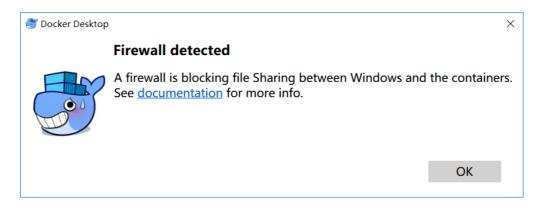
分享

解决Docker for Windows无法共享磁盘的问题

yaxin 发表于 kuka的专栏

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:

A firewall is blocking file Sharing between Windows and the containers...



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
```

```
~]$
/ # nc -vz 10.0.75.1 445
nc: 10.0.75.1 (10.0.75.1:445): Operation timed out
/ # nc -vz 10.14.40.12 80
10.14.40.12 (10.14.40.12:80) open
/ #
```

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"

在 0 0

37

专栏	问答	沙龙	快讯	团队主页	开发者	手册	}	굸	学		找文章	: / 抄	答案	/ 找抗	大术支	牛		写文章	章
	出站规则 连接安全规则		grandman, sand		所有	是	阻止	杏	任何	任何	B-1000	TCP	entire.	任何	任何	任何	任何		
	- 基 监视	Or -	Silver (Stable) (1999)		所有	是	阻止	否	任何	任何	48,000	UDP	10000	任何	任何	任何	任何		
		⊘ • • • • • • • • • • • • • • • • • • •	Street Street, Street,		所有	是	阻止	否	任何	任何	B4109	TCP	10,000	任何	任何	任何	任何		
			100 中央中央の発展		所有	是	阻止	否	任何	任何	26 5 600	TCP	7 (Sec.)		任何	任何	任何		1
		⊘ +	Alban Pekin Mila		所有	是	阻止	否	任何	任何	100 A 100 A	TCP	1.00	任何	任何	任何	任何		
			STATE OF THE PARTY.		所有	是	阻止	否	任何	任何	440,000	TCP	1.000	任何	任何	任何	任何		
3			Marie Beller, P. S. St.		所有	是	阻止	否	任何	任何	MARKET .		11,000	任何	任何	任何	任何		(
()		⊘ =□	the philipped		所有	是	阻止	否	任何	任何	200,000	UDP	100	任何	任何	任何	任何		,
			make before the party		所有	是	阻止	否	任何	任何	PO0000	UDP	767.00		任何	任何	任何		
			Million William Admin		所有	是	阻止	否	任何	任何	747 (20)	UDP	100	任何	任何	任何	任何		
			Steam Johnson Steam		所有	是	阻止	否	任何	任何	19/3/29	TCP	548000	任何	任何	任何	任何		(
			A Professional		所有	是	允许	否	C:\Pr	任何	任何	任何	任何	任何	任何	任何	任何		
		Ø m.	A Company		所有	是	允许	否	D:\pr	任何	任何	TCP	任何	任何	任何	任何	任何		
八亩		9.11	ACCUPATION OF		所有	是	允许	否	D:\pr	任何	任何	UDP	任何	任何	任何	任何	任何		
分享		O Doc	kerProxy		所有	是	允许	否	C:\Pr	任何	任何	任何	任何	任何	任何	任何	任何		
		⊘ Doc	kerSmbMount		所有	是	允许	否	任何	10.0.75.1	10.0.75.2	TCP	445	任何	任何	任何	任何		
		Ø-,	er tely		所有	是	允许	否	D:\pr	任何	任何	TCP	任何	任何	任何	任何	任何		
		-				_	4.34	_		And Alex				440,000	440,000				
						£													
						fire	vaii.	png											

可以看到入站规则中有很多"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)。

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\ adv firewall\ firewall\ show\ rule\ name=all\ dir=in\ type=dynamic\ status=enabled\ >\ d:/firewall\ show\ rule\ name=all\ show\ rule\ name=all\ show\ rule\ show\ rule\ name=all\ show\ rule\ name=all\$

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 12 in range(0, 255):
        for 13 in range(0, 255):
           ip_net = "10.%s.%s.0" % (12, 13)
            if ip_net in net:
                continue
            print("Net %s is available" % ip_net)
```



团队主页

开发者手册

扫码关注云+社区

Copyright © 2013-2019

Tencent Cloud. All Rights Reserved.

专栏 问答 沙龙 快讯 团队主页 开发者手册 云学| 找文章 / 找答案 / 找技术大牛

写文章

在 0 0



公言

https://cloud.tencent.com/developer/article/1397357