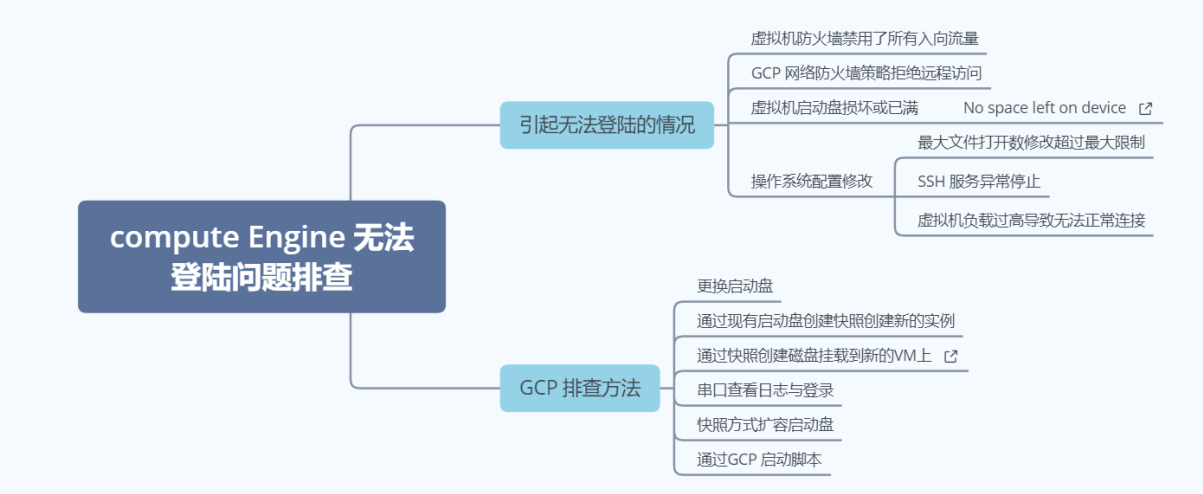
GCE 无法连接问题排查

Created @December 20, 2021 3:39 PM



引起 Compute Engine CentOS 7 无法正常SSH的情况

1. VM 防火墙规则未正常启用SSH服务
2. GCP 防火墙规则未正常放行SSH 端口
3. 系统启动盘磁盘损坏或启动磁盘空间已满
4. 系统文件打开数修改后无法正常SSH

解决办法：

由于排查过程中，需要对虚拟机进行重启，因此， 如果虚拟机挂载了 local SSD，会导Local SSD 中的数据丢失，请注意。下面的解决方法，更多适用于未挂载SSD的虚拟机无法连接的问题。

1、VM防火墙未正常放行，或是通过Xshell 连接工具进行防火墙配置时，禁用了所有INPUT 流量，导致所有的流量被丢掉。

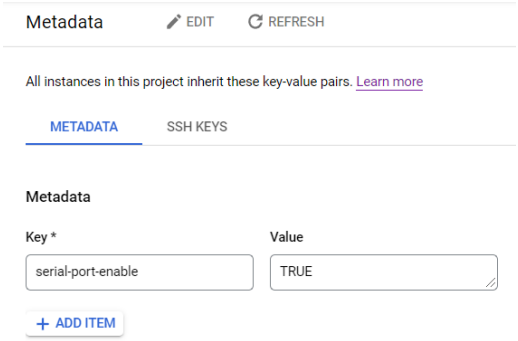
```
[root@instance-3 ~]# iptables -P INPUT DROP
[root@instance-3 ~]#
Network error: Software caused connection abort
```

解决办法：

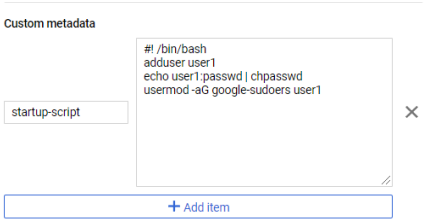
在GCP上，启用串口登录，添加特权用户，然后修改VM 防火墙策略。

实现过程

1、在GCP 控制台，启用VM 的串口登录方式，编辑【metadata】，添加如下Key-Value



2、通过VM start-script 自启脚本，添加用户，然后通过串口登录VM



在自定义元数据【custom medata】，添加新的项，如上所示：

```
在密钥字段中，输入 startup-script。
在值字段中，输入以下内容：

#! /bin/bash
adduser user1
echo USERNAME:PASSWORD | chpasswd
usermod -aG google-sudoers USERNAME

USERNAME：您要添加的用户名
PASSWORD：用户名的密码
```

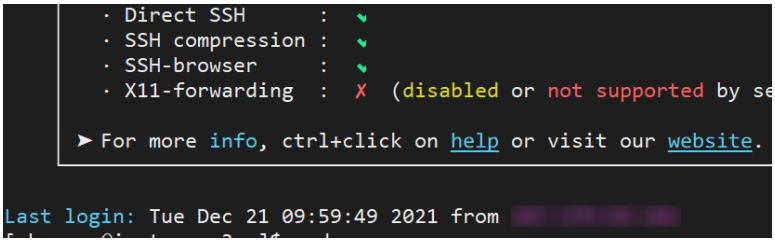
点击【保存】，然后通过reset【重置】实现VM 重启，

连接【串行端口】进行VM 防火墙配置：

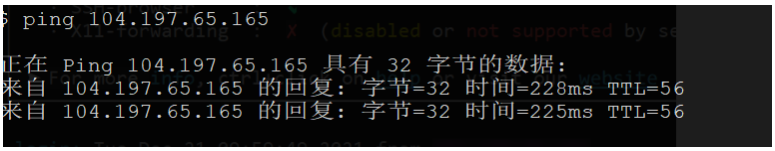
```
instance-3 login: user1
Password:
Dec 21 11:08:36 instance-3 systemd: Created slice User Slice of user1.
Dec 21 11:08:36 instance-3 systemd: Started Session 1 of user user1.
Last failed login: Sat Dec 18 18:09:02 UTC 2021 from 116.110.92.217 on ssh:notty
There were 4 failed login attempts since the last successful login.
[user1@instance-3 ~]$
```

```
允许ICMP 协议
# iptables -I INPUT  -p icmp  -j ACCEPT

允许SSH 服务：
# iptables -I INPUT  -p tcp --dport 22  -j ACCEPT

## 清楚所有防火墙策略
# iptables -F

### 保存防火墙规则
# iptables-save
```

测试SSH 远程连接：

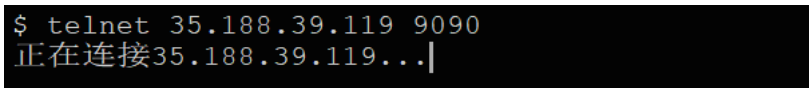


测试网络连通性：



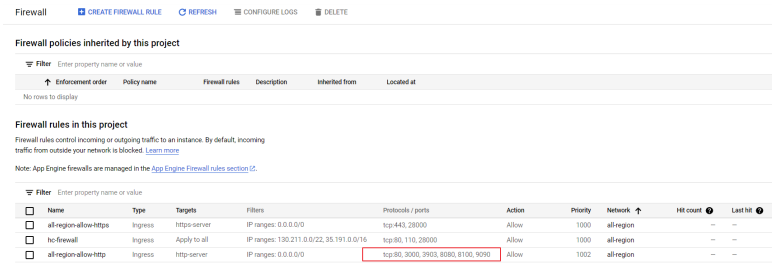
2、GCP 防火墙规则未正常放行SSH 端口

这种情况是由于GCP 的Global 防火墙导致SSH 请求流量无法正常进入到GCP 网络中导致请求被拒绝，如下错误提示：



解决办法：

登录GCP的控制台添加对应端口的防火墙策略：

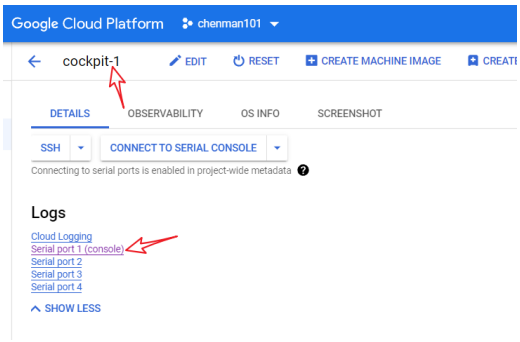


3、系统启动盘磁盘损坏或启动磁盘空间已满

如果虚拟机启动磁盘已满，则您可能无法访问虚拟机。此情况可能很难进行问题排查，因为虚拟机连接问题是由于启动磁盘已满导致时，这种情况并不总是显而易见。

- `Network error: Software caused connection abort`
- `ERROR: (gcloud.compute.ssh) Could not SSH into the instance.  It is possible that your SSH key has not propagated to the instance yet. Try running this command again.  If you still cannot connect, verify that the firewall and instance are set to accept ssh traffic.`
- `You cannot connect to the VM instance because of an unexpected error. Wait a few moments and then try again.`
- `No space left on device`
- `ERROR Exception calling the response handler. [Errno 2] No usable temporary directory found in ['/tmp', '/var/tmp', '/usr/tmp', '/']...`

1. 确认虚拟机的 SSH 故障是否因启动磁盘已满导致,在控制台中找到VM 实例，点击【VM 名称】，然后找到串口：




```
# 通过gcloud 查看串口日志输出
$ gcloud compute instances tail-serial-port-output VM_NAME
```

在串口日志中查找`No space left on device`，如下所示，意味着启动盘因为日志数据的持续写入或不断产生数据文件，已经将启动盘空间占用满，导致无法正常的SSH 登录

```
Dec 23 04:18:14 cockpit-1 systemd[1]: systemd-hostnamed.service: Failed to run 'start' task: No space left on device
Dec 23 04:18:14 cockpit-1 systemd[1]: systemd-hostnamed.service: Failed with result 'resources'.
Dec 23 04:18:14 cockpit-1 systemd[1]: Failed to start Hostname Service.
Dec 23 04:18:39 cockpit-1 dhclient[317]: bound to 10.1.2.10 -- renewal in 1542 seconds.
Dec 23 04:19:07 cockpit-1 systemd[1]: session-157.scope: Succeeded.
Dec 23 04:19:12 cockpit-1 systemd[1]: Started Session 160 of user chenman.
[76325.734790] kworker/1:3: page allocation failure: order:0, mode:0x6310ca(GFP_HIGHUSER_MOVABLE|__GFP_NORETRY|__GFP_NOWARN|__GFP_NOMEMALLOC), nodem
```

如果启动磁盘已满，则生成的输出将包含消息`No space left on device`。

解决办法：

方法一：

1、创建磁盘的快照，用于将已满的磁盘挂载到其他的VM上进行扩容

2、停止虚拟机，并增加磁盘容量

a. 停止虚拟机

```
gcloud compute instances stop VM_NAME  --zone=

VM_NAME：有问题的VM 实例名称
```

b. 增加启动盘容量：重新调整虚拟机启动磁盘的大小后，大多数虚拟机会自动调整根文件系统的大小并重启虚拟机。

调整前的磁盘容量：

```
root@cockpit-1:~# df -Th
Filesystem     Type      Size  Used Avail Use% Mounted on
udev           devtmpfs  484M     0  484M   0% /dev
tmpfs          tmpfs      99M   11M   89M  11% /run
/dev/sda1      ext4      9.7G  9.6G     0 100% /
tmpfs          tmpfs     493M     0  493M   0% /dev/shm
tmpfs          tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs          tmpfs     493M     0  493M   0% /sys/fs/cgroup
/dev/sda15     vfat      124M  5.7M  119M   5% /boot/efi
tmpfs          tmpfs      99M     0   99M   0% /run/user/1002
```

```
gcloud compute disks resize BOOT_DISK_NAME --size DISK_SIZE

BOOT_DISK_NAME：虚拟机的启动磁盘的名称
DISK_SIZE：启动磁盘新的更大大小（以 GB 为单位）
```

c. 重新启动虚拟机

```
gcloud compute instances start VM_NAME
```

3、尝试通过 SSH 连接到虚拟机

a. 可以正常连接，虚拟机自动调整跟文件系统，可以通过串口日志查看，如下所示：

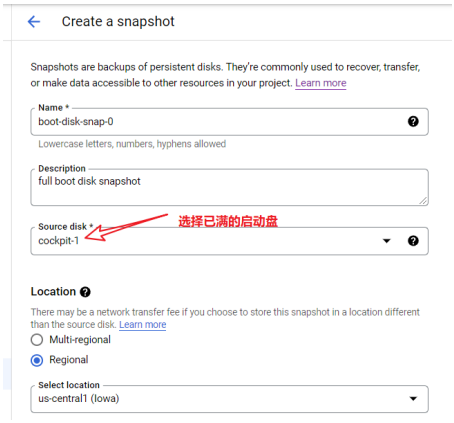
```
Begin: Running /scripts/init-premount ... done.
Begin: Mounting root file system ... Begin: Run[    2.296140] gce-disk-expand: Resizing partition on
ning /scripts/local-top ... done.
Begin: Running /scripts/local-premount ... [    2.326327] gce-disk-expand: Moving GPT header for /dev/sda with sgdisk.
[    3.341616]  sda: sda1 sda14 sda15
[    3.343580] gce-disk-expand: Resizing /dev/sda partition 1 with parted.
[    3.403658] gce-disk-expand: Done
done.
```

登录虚拟机后 通过 `df -Th` 来检查是否有可用的磁盘空间，即自动调整文件系统大小成功。

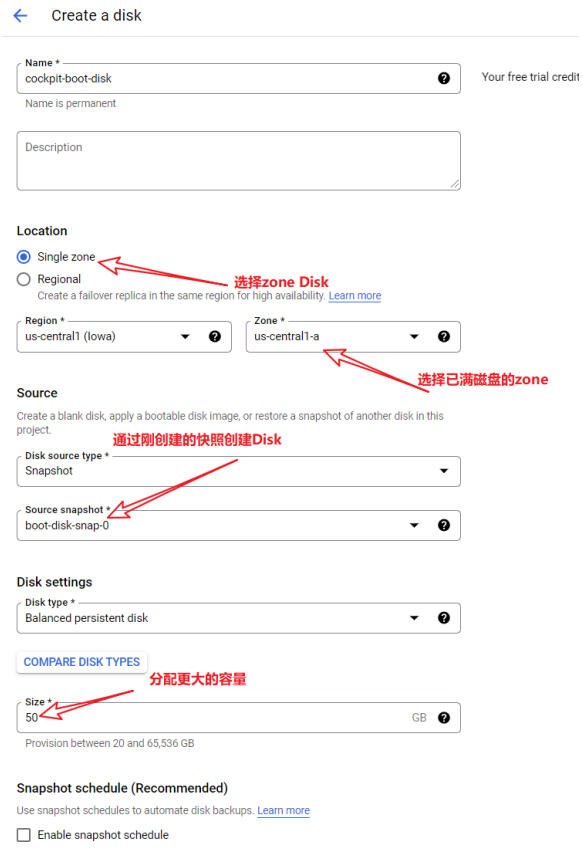
```
Last login: Thu Dec 23 04:13:37 2021 from [redacted]
user2@cockpit-1:~$ df -Th
Filesystem     Type      Size  Used Avail Use% Mounted on
udev           devtmpfs  484M     0  484M   0% /dev
tmpfs          tmpfs      99M  3.2M   96M   4% /run
/dev/sda1      ext4       20G  9.6G  9.1G  52% /
tmpfs          tmpfs     493M     0  493M   0% /dev/shm
tmpfs          tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs          tmpfs     493M     0  493M   0% /sys/fs/cgroup
/dev/sda15     vfat      124M  5.7M  119M   5% /boot/efi
tmpfs          tmpfs      99M     0   99M   0% /run/user/1002
```

1. 仍然无法访问虚拟机，文件系统问题。该虚拟机不支持自动调整根文件系统大小，需要通过上面的快照重新创建新的更大容量的启动盘，然后重新挂载，

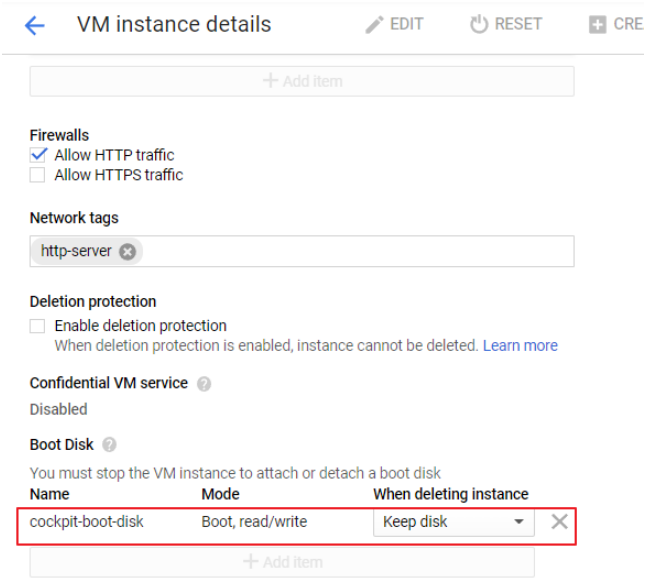
a. 为已满的启动盘创建快照：



b. 通过快照创建新的启动盘增加磁盘容量，通过创建好的快照来创建更大容量已满启动盘的副本，然后将创建的磁盘挂载到虚拟机上，



c. 停止虚拟机，移除已满的启动盘，挂载增加容量后新的启动盘



d. 重启虚拟机，登录虚拟机通过 df -Th 检查扩容后的容量。

```
Last login: Thu Dec 23 04:44:34 2021 from
user2@cockpit-1:~$ df -Th
Filesystem     Type      Size  Used Avail Use% Mounted on
udev           devtmpfs  484M     0  484M   0% /dev
tmpfs          tmpfs      99M  3.2M   96M   4% /run
/dev/sda1      ext4       30G  9.6G   19G  35% /
tmpfs          tmpfs     493M     0  493M   0% /dev/shm
tmpfs          tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs          tmpfs     493M     0  493M   0% /sys/fs/cgroup
/dev/sda15     vfat      124M  5.7M  119M   5% /boot/efi
tmpfs          tmpfs      99M     0   99M   0% /run/user/1002
```

4、系统文件打开数修改超限后无法正常SSH 连接

linux下open_file的值默认是1024，在实际工作中，这个值严重不能满足实际需求，因此我们会根据需求修改系统默认的文件打开数（openfile），通常还会修改到很大的数值，

检查磁盘容量、网络防火墙等都是正常运行的。

```
root@cockpit-1:~# cat /proc/sys/fs/nr_open
1048576
```

直接通过命令修改文件打开数，发生了系统的错误提示：

```
root@cockpit-1:~# ulimit -n 65536000
-bash: ulimit: open files: cannot modify limit: Operation not permitted
root@cockpit-1:~#
```

```
# ulimit -n 1048576  # 最大上限值
root@cockpit-1:~# ulimit -n 1048577  # 修改超出上限值，临时配置会发生错误
-bash: ulimit: open files: cannot modify limit: Operation not permitted
```

直接修改配置文件，永久生效，退出重新登录生效；

```
#@student        -       maxlogins       4
* soft  nofile 1048577
* hard  nofile 1048579
```

登录返回无法正常登录，

```
[chenman@instance-3 ~]$ sudo su -
sudo: pam_open_session: Permission denied
sudo: policy plugin failed session initialization
```

尝试通过串口登录，无法正常登录，同时查看串口日志，没有发现磁盘满的错误：

```
instance-3 login: user1
Password:
Dec 23 09:46:30 instance-3 systemd: Started Session 46 of user user1.

Permission denied
```

通过启动脚本修改 open_file 文件打开数，

```
/usr/bin/sed -i '/nofile/d' /etc/security/limits.conf
```

重启虚拟机，运行启动脚本，来修改系统配置文件，重新远程登录，可以正常登录，问题得到解决：

```
[chenman@instance-3 ~]$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 3658
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 3658
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

补充 通过gcloud troubleshot：

```
$ gcloud beta compute ssh cockpit-1 --zone=us-central1-a --troubleshoot

Starting ssh troubleshooting for instance https://compute.googleapis.com/compute/beta/projects/yunion-test-286209/zones/us-central1-a/
Start time: 2021-12-23 10:10:43.350588

---- Checking network connectivity ----
The troubleshooting tool needs permission to check the VM's network connectivity.

Is it OK to run this test? (Y/n)?  y

Enabling service [networkmanagement.googleapis.com] on project [yunion-test-286209]...
Your source IP address is 34.80.131.230
Network Connectivity Test Result: REACHABLE
EndpointInfo <EndpointInfo
 destinationIp: '10.1.2.10'
 destinationNetworkUri: 'projects/yunion-test-286209/global/networks/default'
 destinationPort: 22
 protocol: 'TCP'
 sourceIp: '34.80.131.230'
 sourcePort: 51103>
Initial state: packet originating from Internet.
START_FROM_INTERNET
Forwarding state: arriving at a Compute Engine instance.
ARRIVE_AT_INSTANCE
Config checking state: verify INGRESS firewall rule.
APPLY_INGRESS_FIREWALL_RULE
```

```
Final state: packet delivered to instance.
DELIVER
---- Checking user permissions ----
User permissions: 0 issue(s) found.

---- Checking VPC settings ----
VPC settings: 0 issue(s) found.

---- Checking VM status ----
VM status: 0 issue(s) found.

---- Checking VM boot status ----
VM boot: 0 issue(s) found.
```

获取所有GCP的IP：

```
$ dig +qr +short txt `dig +short TXT _spf.google.com | grep -oE 'include:\S*' | cut -d':' -f2 | xargs` | grep -oE 'ip[46]:\S*' | sort
ip4:108.177.8.0/21
ip4:108.177.96.0/19
ip4:130.211.0.0/22
ip4:172.217.0.0/19
ip4:172.217.128.0/19
ip4:172.217.160.0/20
ip4:172.217.192.0/19
ip4:172.217.32.0/20
ip4:172.253.112.0/20
ip4:172.253.56.0/21
ip4:173.194.0.0/16
ip4:209.85.128.0/17
ip4:216.239.32.0/19
ip4:216.58.192.0/19
ip4:35.190.247.0/24
ip4:35.191.0.0/16
ip4:64.233.160.0/19
ip4:66.102.0.0/20
ip4:66.249.80.0/20
ip4:72.14.192.0/18
ip4:74.125.0.0/16
ip6:2001:4860:4000::/36
ip6:2404:6800:4000::/36
ip6:2607:f8b0:4000::/36
ip6:2800:3f0:4000::/36
ip6:2a00:1450:4000::/36
ip6:2c0f:fb50:4000::/36

参考：https://www.runoob.com/regexp/regexp-syntax.html
```