



链滴

SSH 被爆了

作者: [Eddie](#)

原文链接: <https://ld246.com/article/1542245583412>

来源网站: [链滴](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

起因

前几天我更新网站的证书，就是那个[Let's Encrypt](#) 现在提供免费泛域名 SSL 证书
突然弹出个No space left on device 磁盘突然就满了。肯定有鬼。

定位问题

```
root@iz280f4j9s3z:/opt# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            487M   4.0K   487M   1% /dev
tmpfs           100M   816K    99M   1% /run
/dev/vda1       20G    19G    68M 100% /
none            4.0K     0   4.0K   0% /sys/fs/cgroup
none            5.0M     0   5.0M   0% /run/lock
none            497M     0   497M   0% /run/shm
none            100M     0   100M   0% /run/user
overflow        1.0M     0   1.0M   0% /tmp

root@iz280f4j9s3z:/var# du -sh *
8.0K    ax25
3.7M    backups
971M    cache
517M    lib
4.0K    local
0       lock
9.0G    log
4.0K    mail
4.0K    opt
7.1M    resin
0       run
1.7M    spool
11M     tmp
218M    www
```

发现log目录非常大!

```
root@iz280f4j9s3z:/var/log# du -sh *
4.0K    alternatives.log
4.0K    alternatives.log.1
4.0K    alternatives.log.10.gz
4.0K    alternatives.log.11.gz
4.0K    alternatives.log.12.gz
4.0K    alternatives.log.2.gz
4.0K    alternatives.log.3.gz
4.0K    alternatives.log.4.gz
4.0K    alternatives.log.5.gz
4.0K    alternatives.log.6.gz
4.0K    alternatives.log.7.gz
4.0K    alternatives.log.8.gz
4.0K    alternatives.log.9.gz
500K    apache2
136K    apt
3.6G    auth.log
400K    auth.log.1
0       auth.log.1.gz
52K     auth.log.2.gz
64K     auth.log.3.gz
64K     auth.log.4.gz
8.0K    boot.log
4.2G    btmp
57M     btmp.1
```

其中 auth.log 、 btmp 占空间最多

发生了啥？

auth.log btmp 都记录了ssh的登录情况，突然变大，应该是ssh被扫了。

解决办法？

我们暂时将 auth.log、 btmp 备份，然后删除。（阿里云删除了以后不知道为什么要重启服务器）

将ufw reset，禁止所有端口访问，允许指定ip访问特定端口，将ssh端口从默认的22，21 修改为其端口，将auth.log 中登录失败的ip加入黑名单中。

get help from :

<http://blog.chinaunix.net/uid-20329764-id-5016539.html>

<https://moecclub.org/2017/03/20/70/>