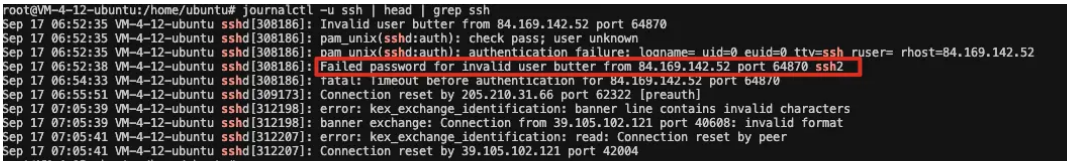
【对外】journalctl日志快速优化痕迹隐藏

前言

最近在抹除痕迹的时候，直接进行删除不太优雅，于是研究下如何快速隐藏journalctl上的日志。

journalctl日志会记录一些服务日志，其中包含ssh的日志包括登录的ip、使用密码还是密钥登录等等。

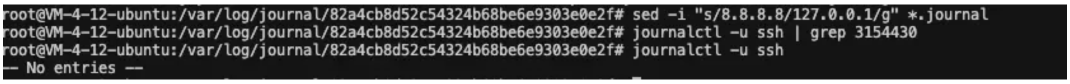


```
root@VM-4-12-ubuntu:/home/ubuntu# journalctl -u ssh | head | grep ssh
Sep 17 06:52:35 VM-4-12-ubuntu sshd[308186]: Invalid user butter from 84.169.142.52 port 64870
Sep 17 06:52:35 VM-4-12-ubuntu sshd[308186]: pam_unix(sshd:auth): check pass; user unknown
Sep 17 06:52:35 VM-4-12-ubuntu sshd[308186]: pam_unix(sshd:auth): authentication failure: logname= uid=0 euid=0 tty=ssh ruser= rhost=84.169.142.52
Sep 17 06:52:38 VM-4-12-ubuntu sshd[308186]: Failed password for invalid user butter from 84.169.142.52 port 64870 ssh2
Sep 17 06:54:33 VM-4-12-ubuntu sshd[308186]: fatal: Timeout before authentication for 84.169.142.52 port 64870
Sep 17 06:55:51 VM-4-12-ubuntu sshd[309173]: Connection reset by 205.210.31.66 port 62322 [preauth]
Sep 17 07:05:39 VM-4-12-ubuntu sshd[312198]: error: kex_exchange_identification: banner line contains invalid characters
Sep 17 07:05:39 VM-4-12-ubuntu sshd[312198]: banner exchange: Connection from 39.105.102.121 port 40608: invalid format
Sep 17 07:05:41 VM-4-12-ubuntu sshd[312207]: error: kex_exchange_identification: read: Connection reset by peer
Sep 17 07:05:41 VM-4-12-ubuntu sshd[312207]: Connection reset by 39.105.102.121 port 42004
```

如何解决?

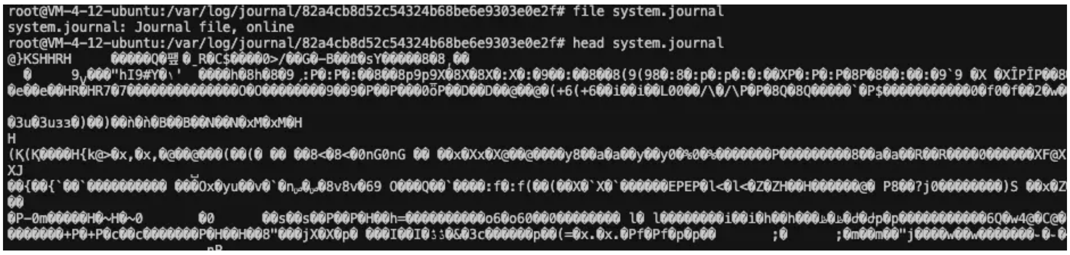
按照传统的思路，直接使用sed替换，会发现日志无法使用了。

```
sed -i "s/8.8.8.8/127.0.0.1/g" *.journal
journalctl -u ssh
```



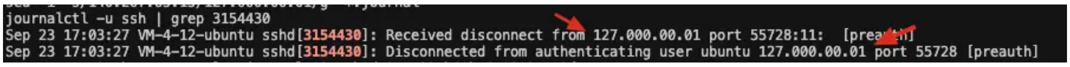
```
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# sed -i "s/8.8.8.8/127.0.0.1/g" *.journal
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# journalctl -u ssh | grep 3154430
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# journalctl -u ssh
-- No entries --
```

于是查看了下journal的日志，发现属于特定格式



```
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# file system.journal
system.journal: Journal file, online
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# head system.journal
@}KSHHRH     �����Q�땦�_R�C$�����>/��G�-B��sY������8�8,��
  �     9,���"hI9#Y�\'  ����h�8h�8�9 ;P�:P�:���8��8p9p9X�8X�8X�:X�:�9��:���8��8(9(98�:8�:p�:p�:�:��XP�:P�:P�8P�8��:��:�9`9 �X �XÎPÎP���8
�e��e��HR�HR7�7����������������O�O����������9���9�P��P����õP��D���D���@���@�(+6(+6��i��i��L����/\�/\P�P��8Q��8Q�����`�P$�������������f��f���2�w�

�3u�3u33�)��)��ǹ�ǹ�B��B��N��N�xM�xM�H
H
(K(K����H{k@>�x,�x,�@��@���(��(� �� ��8<�8<��nG�nG �� ��x�Xx�X@��@����y8��a�a��y��y�0�%�0�%�������P����������8��a�a��R��R�����������XF@X
XJ
��{��{`��`���������� ���Ox�yu��v�`�n��8v8v�69 O����Q��`����:f�:f(��(��X�`X�`������EPEP�l<�l<�Z�ZH��H�������@� P8��?j���������)S ��x�Z
��
�P-�m������H�~H�~0       ��      ��s��s��P��P�H��h=����������o6�o6������������ l� l��������i��i�h��h�����d�dp�p������������6Q�w4@�C@
�������+P�+P�c��c��������P�H��H��8"���jX�X�p� ���I��I�3&�3c�������p��(=�x.�x.�Pf�Pf�p�p��      ;�      ;�m��m��"j����w��w�������-�-�
```



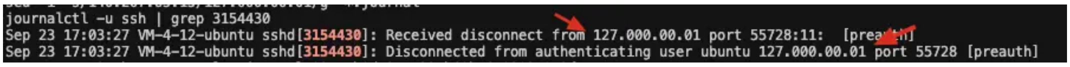
```
journalctl -u ssh | grep 3154430
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: Received disconnect from 127.000.00.01 port 55728:11:  [preauth]
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: Disconnected from authenticating user ubuntu 127.000.00.01 port 55728 [preauth]
```

仅仅格式校验之长度

根据之前修改java反序列化包的经验，这些一般都是规范了长度，而非byte的md5，尝试保持长度

```
sed -i "s/111.111.11.11/127.000.00.01/g" *.journal
```

```
journalctl -u ssh | grep 3154430
```



```
journalctl -u ssh | grep 3154430
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: Received disconnect from 127.000.00.01 port 55728:11:  [preauth]
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: Disconnected from authenticating user ubuntu 127.000.00.01 port 55728 [preauth]
```

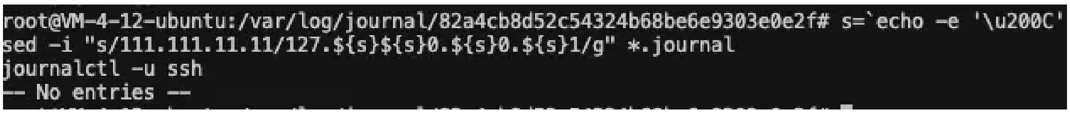
显然不是很优雅

零宽字符尝试

虽然我们能修改成一个随机的ip了，但是防御方可以通过日志对比发现踪迹。

于是想到了零宽字符，比如127.000.00.01，就是在视觉效果上显示127.0.0.1，但是可惜的是不支持。

```
s=`echo -e '\u200C'`
sed -i "s/111.111.11.11/127.${s}${s}0.${s}0.${s}1/g" *.journal
journalctl -u ssh | grep 3154430
```



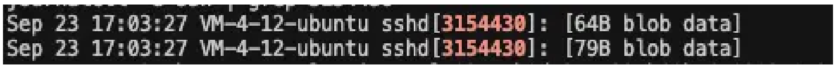
```
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# s=`echo -e '\u200C'
sed -i "s/111.111.11.11/127.${s}${s}0.${s}0.${s}1/g" *.journal
journalctl -u ssh
-- No entries --
```

fuzz之blob data

于是对字符fuzz，发现对不可见的字符，journal就不直接显示，而事显示blob data。

```
s=`echo -e '\u007F'`
sed -i "s/111.111.11.11/127.${s}${s}0.${s}0.${s}1/g" *.journal
journalctl -u ssh | grep 3154430

```

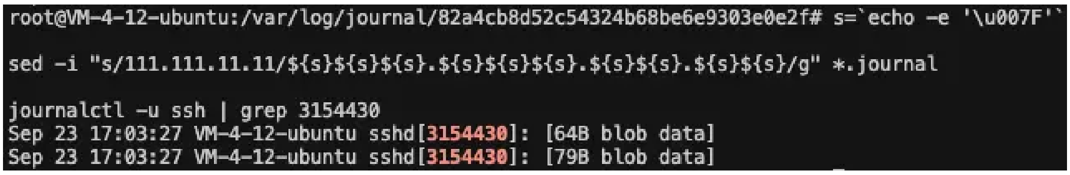


```
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: [64B blob data]
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: [79B blob data]
```

结合利用

显示的时候是blob data，直接去查看journal日志文件也找不到真实的IP

```
s=`echo -e '\u007F'`
sed -i "s/111.111.11.11/${s}${s}${s}.${s}${s}${s}.${s}${s}.${s}${s}/g" *
journalctl -u ssh | grep 3154430
```



```
root@VM-4-12-ubuntu:/var/log/journal/82a4cb8d52c54324b68be6e9303e0e2f# s=`echo -e '\u007F'`

sed -i "s/111.111.11.11/${s}${s}${s}.${s}${s}${s}.${s}${s}.${s}${s}/g" *.journal

journalctl -u ssh | grep 3154430
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: [64B blob data]
Sep 23 17:03:27 VM-4-12-ubuntu sshd[3154430]: [79B blob data]
```

总结

其实还不是很完美，理想状态是直接修改IP而非隐藏。如果有更好的方法，欢迎一起交流。