



CVK修改密码后无法SSH登陆

张昊 2022-06-30 发表

告警信息

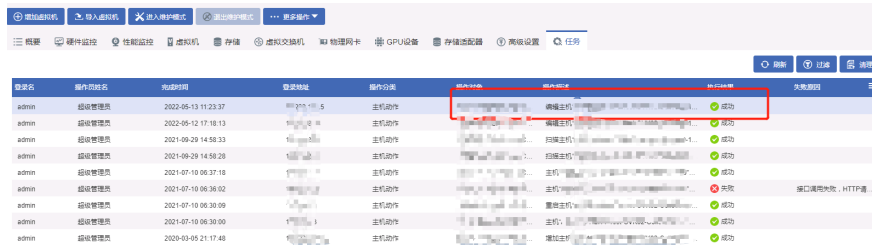
后台SSH登录CVK，输入用户名密码后提示无法登录

问题描述

CVK主机在修改密码后无法直接SSH登录，但可以通过其他节点进行跳转或xconsole界面直接登录

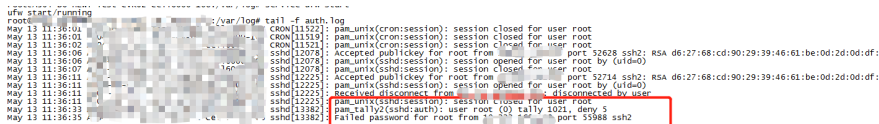
过程分析

1、首先查看CAS前台进行的修改任务，任务显示修改成功，且尝试将密码再次进行修改后，仍无法正常SSH登录



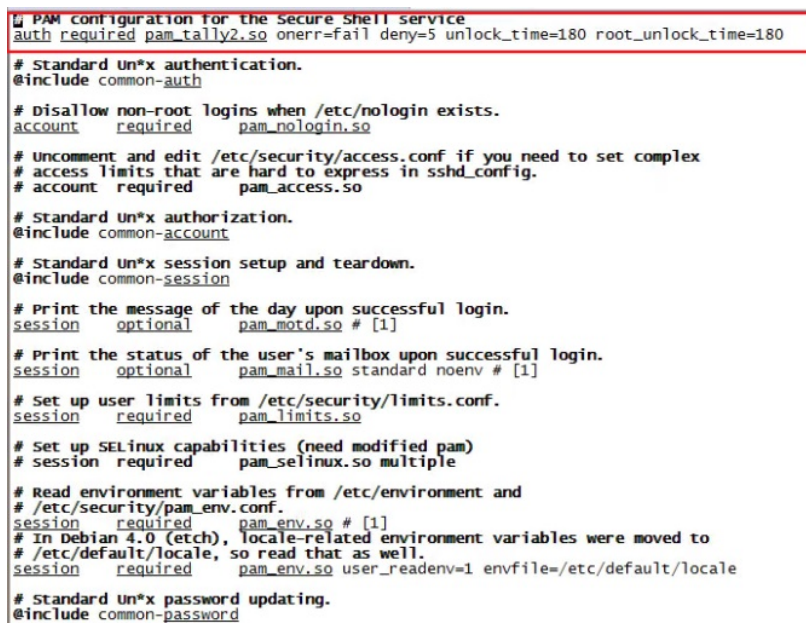
任务名	操作任务名	开始时间	结束时间	操作内容	操作结果	操作人	失败原因
admin	密码管理	2022-05-13 11:23:37	成功		成功		
admin	密码管理	2022-05-12 17:18:13	成功		成功		
admin	密码管理	2021-09-29 14:58:23	成功		成功		
admin	密码管理	2021-09-29 14:58:28	成功		成功		
admin	密码管理	2021-07-10 00:37:18	成功		成功		
admin	密码管理	2021-07-10 00:36:02	成功		成功		
admin	密码管理	2021-07-10 00:30:09	成功		成功		
admin	密码管理	2021-07-10 00:30:00	成功		成功		
admin	密码管理	2020-03-05 21:17:48	成功		成功		

2、通过其他CVK主机跳转到该CVK后台，检查登录日志auth.log，发现pam_tally2的相关打印：



```
May 13 11:36:04 ... cron[11322]: pam_unix(cron:session): session closed for user root
May 13 11:36:02 ... cron[11321]: pam_unix(cron:session): session closed for user root
May 13 11:36:06 ... sshd[12078]: Accepted publickey for root from ... port 52628 ssh: RSA d6:27:68:cd:90:29:39:46:61:be:0d:2d:0d:df:7
May 13 11:36:06 ... sshd[12078]: pam_unix(sshd:session): session opened for user root by (uid=0)
May 13 11:36:11 ... sshd[12225]: Accepted publickey for root from ... port 52714 ssh: RSA d6:27:68:cd:90:29:39:46:61:be:0d:2d:0d:df:7
May 13 11:36:11 ... sshd[12225]: pam_unix(sshd:session): session opened for user root by (uid=0)
May 13 11:36:11 ... sshd[12225]: Received disconnect from ... user root
May 13 11:36:13 ... pam_tally2(sshd:auth): user root (0) tally 1021, deny 5
May 13 11:36:35 ... sshd[13382]: Called password for root from ... port 55988 ssh2
```

3、通过该报错，怀疑与现场的SSH配置中的加固项有关，查看/etc/pam.d/ssh文件，确实存在登录失败锁定的相关设置：



```
# PAM configuration for the Secure Shell service
auth required pam_tally2.so onerr=fail deny=5 unlock_time=180 root_unlock_time=180

# Standard un*x authentication.
@include common-auth

# Disallow non-root logins when /etc/nologin exists.
account required pam_nologin.so

# Uncomment and edit /etc/security/access.conf if you need to set complex
# access limits that are hard to express in sshd_config.
# account required pam_access.so

# Standard un*x authorization.
@include common-account

# Standard un*x session setup and teardown.
@include common-session

# Print the message of the day upon successful login.
session optional pam_motd.so # [1]

# Print the status of the user's mailbox upon successful login.
session optional pam_mail.so standard noenv # [1]

# Set up user limits from /etc/security/limits.conf.
session required pam_limits.so

# Set up SELinux capabilities (need modified pam)
# session required pam_selinux.so multiple

# Read environment variables from /etc/environment and
# /etc/security/pam_env.conf.
session required pam_env.so # [1]
# In Debian 4.0 (etch), locale-related environment variables were moved to
# /etc/default/locale, so read that as well.
session required pam_env.so user_readenv=1 envfile=/etc/default/locale

# Standard un*x password updating.
@include common-password
```

该限制默认是没有添加的，现场做过等保加固相关的操作所致。添加后即会对ssh登录进行限制，如果连续登录失败5次，就会锁定登录180s。

4、通过命令pam_tally2 -u root检查root用户的登录失败锁定次数，发现现场有1300多次登录失败的记录。

5、分析锁定的原因，现场CAS对接了监控平台，对接时需要用到CVK的root用户，修改密码后监控平台侧未及时修改对接配置，导致频繁使用错误密码访问该CVK，进而导致root被持续锁定。

解决方法

使用命令 `pam_tally2 -r -u root` 可以手动解除锁定状态。或在CAS前台直接修改CVK的密码为原密码，可避免ssh登录被锁定。

建议修改CVK主机密码时，及时关注并同步修改与CAS对接平台的对应密码，避免访问或监控出现异常。

