

知 CAS主机配置密码策略密码由于过期导致CVK主机异常的一种解决方案

孙亚华 2021-04-13 发表

组网及说明

CAS5.0的版本。

问题描述

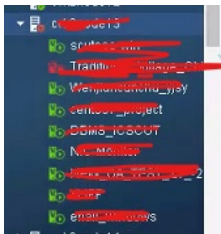
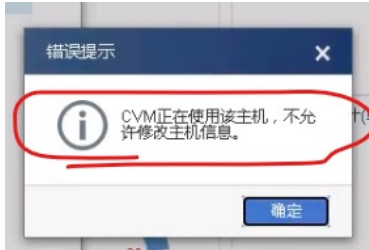
现场之前做过等保配置，配置了CVK主机的密码90天到期需要更换且配置了密码输入错误次数超出后锁定的限制。

现场在主机密码超期之后在CVM前台进行修改主机密码的配置，提示“CVM正在使用该主机，不允许修改主机信息”。

点击连接该主机提示“主机异常”。

后台从其他正常的cvk上SSH登录该主机时，提示需要修改密码。

其上的虚拟机业务正常。



```
root@cvknode10:~# ssh 202.20.100.04
You are required to change your password immediately (password aged)
Last login: Mon Apr 12 21:30:34 2021 from 202.20.100.04
Changing password for root.
(current) UNIX password:
```

过程分析

登录CVM后台，查看界面上报错时刻对应的cas.log的日志，有如下报错；

```
at org.apache.tomcat.util.threadpool.ThreadPool$TaskThread$HeaptingRunnable.run(ThreadThread.java:61) [tomcat8-util-8.0.14.jar:8.0.14]
at java.lang.Thread.run(Thread.java:745) [?:1.7.0_121]
2021-04-12 21:32:42 [ERROR] [http-nio-8080-exec-49] [com.Virtual.plat.server.rs.nova.func.RsNovaMgrImpl:queryNodeStorage] null
com.Virtual.plat.server.vm.vmm.HypervisorException: End of file while reading data: WARNING: Your password has expired.
password change required but no tty available.: Input/output error
at com.Virtual.plat.server.vm.vmm.LibvirtExceptionMapper.mapException(vmc:66) [LibvirtExceptionMapper.class:?]
at com.Virtual.plat.server.vm.vmm.LibvirtExceptionMapper.mapException(vmc:25) [LibvirtExceptionMapper.class:?]
```

从正常的CVK上ssh跳转到该异常的cvk上，按照提示将密码更新一下（前提是现场还有记录原来的密码）

登录到CVM后台，使用mysql -uroot -p命令进入数据库，使用select * from TBL_HOST 查看这个cvm数据库中记录的这个主机的密码，如下

```
id 5118 CPU @ 2.30GHz | Lenovo ThinkSystem S3550 -[7X16CT01W]-
| 7C:D3:0A:61:09:F8 | 1 | 00 | NULL | NULL | NULL | NULL
| 32 | 1 | cvk2node14 | 202.38.193.26 | root | 44116
id 5118 CPU @ 2.30GHz | Lenovo ThinkSystem S3550 -[7X16CT01W]-
| 7C:D3:0A:60:6F:B8 | 1 | 00 | NULL | NULL | NULL | NULL
| 33 | 1 | cvk2node1 | 202.38.193.19 | root | 44116
id 5118 CPU @ 2.30GHz | Lenovo ThinkSystem S3550 -[7X16CT01W]-
| 7C:D3:0A:67:3B:C0 | 1 | 00 | NULL | NULL | NULL | NULL
```

利用 update TBL_HOST set PW="XX" WHERE ID=X;命令将数据库中记录的密码改为现场异常cvk后台当前的真实密码。

一般如果是由于忘记了密码导致上述问题的，搞这一步就可以解决了。但是现场将数据库密码和cvk的真实密码改为一致之后连接主机还是显示异常。

继续做如下排查，登录进去之后，查看该主机的/var/log/auth.log看，有如下报错。

```
23:22:39 cvk2node13 sudo: java: TTY=unknown : PWD=/var/opt/ds/agent/slowpath : USER=root
23:22:39 cvk2node13 sudo: pam_unix(sudo:session): session opened for user root by (uid=)
23:22:39 cvk2node13 sudo: pam_unix(sudo:session): session closed for user root
23:22:41 cvk2node13 sshd[1400]: pam_tally2(sshd:auth): user root ( ) tally 155, deny
23:22:43 cvk2node13 sshd[1400]: Failed password for root from 202.38.193.7 port 44116 ssh2
```

应该是现场配置了密码输入错误次数超出锁定的策略，导致目前登录锁住，需要解锁才能恢复

解决方法

在异常cvk后台执行pam_tally2 -r 命令，解除锁定之后，再次连接主机之后恢复正常。

```
root@cvk2node13:~# pam_tally2 -u root
Login          Failures Latest failure    From
root           1429    04/12/21 23:27:36    202.38.193.7
root@cvk2node13:~# pam_tally2 -t
Login          Failures Latest failure    From
root           1430    04/12/21 23:27:38    202.38.193.7
root@cvk2node13:~# pam_tally2 -u root
```

任务名称	操作对象	任务状态	任务描述
连接主机:cvk2node13	cvk2node13	100%	连接主机cvk2node13成功。

