

知 某局点CAS有两台CVK主机无法弹出修改虚拟机操作界面

母鑫 2021-04-29 发表

组网及说明

略

问题描述

某局点现场反馈有两台主机均无法弹出修改虚拟机的操作界面，其他界面操作正常，其余主机均正常。现场反馈之前有中过挖矿病毒，后续进行过杀毒操作。



过程分析

1. 尝试手动连接两台cvk主机，发现均正常。

任务名称	操作对象	任务状态	任务描述	操作员	操作IP	开始时间	完成时间	执行结果
连接主机DMZ-Cluster02-CVK08	DMZ-Cluster02-CVK08	100%	连接主机DMZ-Cluster02-CVK12成功。	admin	172.18.22.184	2021-04-22 10:30:38	2021-04-22 10:30:41	成功
连接主机DMZ-Cluster02-CVK11	DMZ-Cluster02-CVK11	100%	连接主机DMZ-Cluster02-CVK11成功。	admin	172.18.22.184	2021-04-22 10:21:38	2021-04-22 10:21:38	成功

2. 查看主机的虚拟交换机网络时发现，两台主机的虚拟交换机的状态都是未知。

名称	网络类型	物理接口	转发模式	VLAN ID	状态	IP地址	子网掩码 / 前缀	网关	DPDK状态
vswitch-app	业务网络迁...	VEB			未知				--
vswitch0	管理网络	VEB			未知				--

3. 在两台主机后台执行“ovs_dbg_listports”查看虚拟交换机的状态，提示无权执行。这种问题一般是病毒导致的文件权限问题。

```
vnet0 0cda411d0364 172.18.22.2          3/7          899x          150
0      clglpt_001 5900
root@DMZ-Cluster02-CVK08:~# ssh DMZ-Cluster02-CVK11
Authorized users only. All activity may be monitored and reported
Last login: Thu Apr 22 10:41:02 2021 from 172.18.1.18
root@DMZ-Cluster02-CVK11:~# ovs_dbg_listports
/opt/bin/ovs_dbg_listports: 2: exec: /usr/bin/python: Permission denied
root@DMZ-Cluster02-CVK11:~#
```

解决方法

1. 此问题为病毒文件导致文件权限问题，主机无法读取相关文件导致。
2. 如果现场频繁出现病毒引起的问题，推荐重装环境。
3. 如果无法重装，可通过以下进行相应文件提权，并定期修改root密码。

lsattr xxxx //显示文件的隐藏属性，‘i’参数代表无法对文件进行修改

chattr -i xxx //移除相关参数属性

chmod //对文件进行提权

```
root@09M2-Cluster02-CVK12:~# lsattr /usr/bin/python2.7
----i-----e- /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~# chattr -i /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~# lsattr /usr/bin/python2.7
-----e- /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~# chmod 755 /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~#
root@09M2-Cluster02-CVK12:~# lsattr /usr/bin/python2.7
-----e- /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~# ls -al /usr/bin/python2.7
-rwxr-xr-x 1 root root 2993560 Apr 21 2012 /usr/bin/python2.7
root@09M2-Cluster02-CVK12:~# ls -al /usr/bin/python
lrwxrwxrwx 1 root root 9 Apr 18 2012 /usr/bin/python -> python2.7
root@09M2-Cluster02-CVK12:~# ovs_db_listports
PCI  NAME  LF  IO  BU  SRIO  MTU  &L  SPEED  MAC  IP  VEN:DEV  DESC  SUBSYS  DRIVER  FIRMWARE
3d:00:0 eth2  0  0/32 1500 u/u  1000 08688d6972df 8086:37d1 X722 0000 140e 3.33 0x80000f0c 1.1767.0
3d:00:1 eth3  0  0/32 1500 u/u  1000 08688d6972e0 8086:37d1 X722 0000 140e 3.33 0x80000f0c 1.1767.0
3d:00:2 eth4  0  0/32 1500 u/d  0 08688d6972e1 8086:37d1 X722 0000 140e 3.33 0x80000f0c 1.1767.0
3d:00:3 eth5  0  0/32 1500 u/d  0 08688d6972e2 8086:37d1 X722 0000 140e 3.33 0x80000f0c 1.1767.0
5f:00:0 eth0  0  1500 u/u  10000 4ce9e4ca0770 14e4:168e ECMS7810 5006 bnx2x bc 7.13.0
5f:00:1 eth1  0  1500 u/u  10000 4ce9e4ca0772 14e4:168e ECMS7810 5006 bnx2x bc 7.13.0
=====
Type      Name MAC      IPv4      OffPort  Vlanx  MTU  VName  VNC
vswitch0  inc      vswitch0 08688d6972df 172.18.1.22 65534/1 1500
```

