某局点CAS有两台CVK主机无法弹出修改虚拟机操作界面

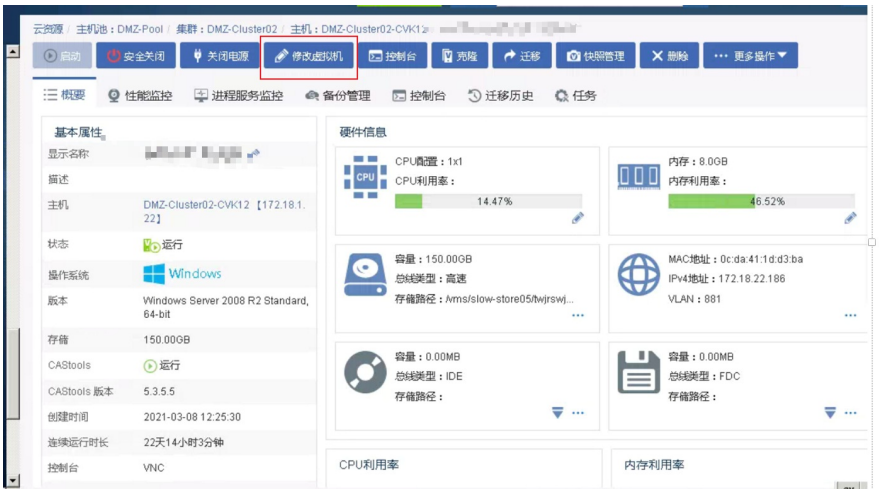
母鑫 2021-04-29 发表

组网及说明

略

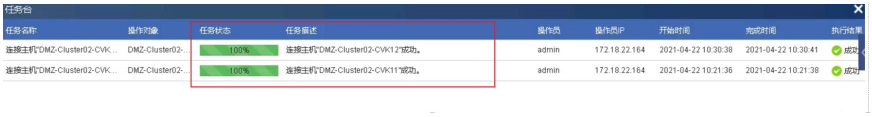
问题描述

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。

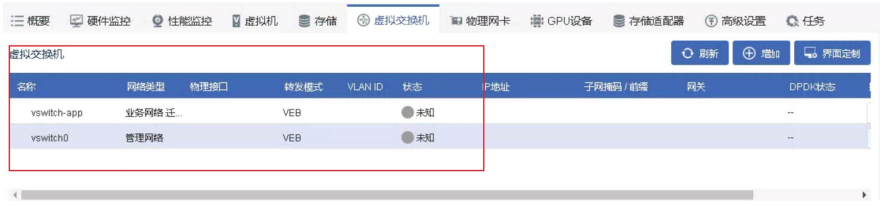


过程分析

1. 尝试手动连接两台cvk主机，发现均正常。



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。



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 0cda41ld0364 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