云学堂中毒导致服务器CPU利用率居高不下降

吴铖 2021-01-23 发表

组网及说明

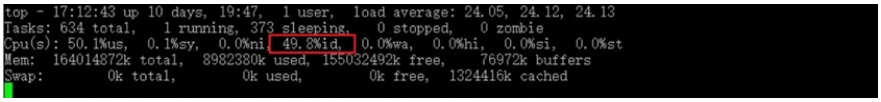
现场部署了6套云学堂，每个教室一套，各自独立使用。

问题描述

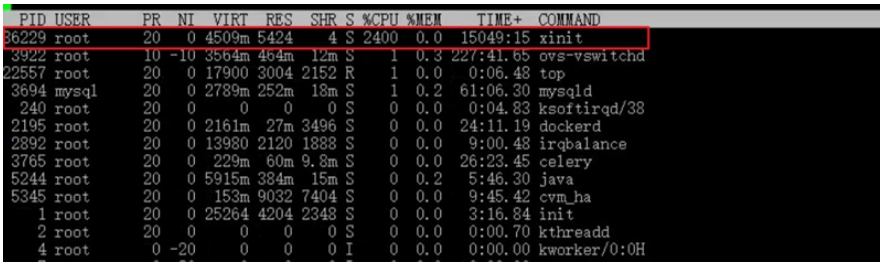
反馈6个教室全部发现前台云学堂CPU利用率都是40多%，有过重启的记录，还是如此。

过程分析

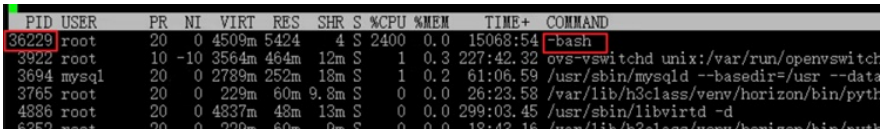
一、使用top命令确认后台的CPU使用率情况是否与前台前面显示的一致，接近50%的空闲情况，50%的使用。



二、使用top命令，按键盘P或者shift+p，将进程按照CPU利用率从大到小排序，确认什么进程占用CPU利用率进而不释放。



三、如上图可以看到xinit进程占用CPU利用率，后续键盘小写的c查看进程的文件路径情况。



四、xinit进程初步判断非云学堂环境正常进程，并且是一个脚本在进行运行，初步判断是中毒表现。

五、查看历史操作日志/var/log/operation记录，分析病毒脚本存放位置及相关操作。

六、如上图可以看到于凌晨六点进行下载，重命名，运行脚本等操作，最终脚本存在在/etc目录下。

解决方法

一、按照操作日志进行一一清理，rm -rf xinit 删除/etc/目录下脚本

```
root@cvknode5:/etc# ll | grep xin
-rwxr-xr-x   1 root root   993016 Nov 18 07:13 xinit*
You have new mail in /var/mail/root
root@cvknode5:/etc#
```

二、vi命令修改/etc/host的参数变动。

```
root@cvknode5:/etc# cat /etc/hosts
10.12.1.70 cvknode5
127.0.0.1 localhost

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
86.106.181.102 bash.fail
root@cvknode5:/etc#
```

三、使用命令kill -9 xxx 杀死脚本运行（进程号参照前面top命令查看）。

```
You have new mail in /var/mail/root
root@cvknode1:~# ps -ef | grep 31864
root     15632  9641  0 17:47 pts/5    00:00:00 grep --color=auto 31864
root     31864     1 99 06:45 ?        11-00:23:30 -bash
root@cvknode1:~# kill -9 31864
root@cvknode1:~# ps -ef | grep 31864
root     15870  9641  0 17:47 pts/5    00:00:00 grep --color=auto 31864
You have new mail in /var/mail/root
root@cvknode1:~#
```

四、至此CPU利用率正常释放掉，后续仍需加强root密码强度，及物理防火墙加强控制。