Subject: Re: sudo audit log
Posted by zoom on Tue, 25 Nov 2008 16:09:10 GMT
View Forum Message <> Reply to Message

I was thinking the same thing, however the audit libs are the same for a container which doesn't get the message.

audit-libs-python-1.6.5-9.el5
audit-libs-1.6.5-9.el5

I did notice that the host system does contain an audit.log in /var/log/audit. I tried creating a similar directory in the /var/log directory of the container with the same permissions, still no luck.

Looking at the strace it seems that it can't find it "Illegal seek", however I'm not 100% sure. But as you can see the "chmod" does get executed for the sudo command "sudo chmod 777 htaccess.tmp"

```
fcntl64(4, F_GETFL)                     = 0x8002 (flags O_RDWR|O_LARGEFILE)
fstat64(4, {st_mode=S_IFCHR|0620, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) =
0xb7fc2000
_llseek(4, 0, 0xbfede224, SEEK_CUR)     = -1 ESPIPE (Illegal seek)
write(4, "audit_log_user_command(): Connec"..., 45) = 45
close(4)                                = 0
munmap(0xb7fc2000, 4096)                = 0
execve("/bin/chmod", ["chmod"..., "777"..., "htaccess.tmp"...], [/* 24 vars */]) = 0
```

I did notice that the host is running a audit daemon. Could this be what is missing in the container?

```
root      8436  0.0  0.0  83916   824 ?        S<sl Sep29   0:22 auditd
```