Subject: sudo audit log
Posted by zoom on Tue, 25 Nov 2008 14:49:24 GMT
View Forum Message <> Reply to Message

Yesterday I decided to run yum update in one of my containers. After successfully updating the container I noticed a strange message when using the sudo command.

audit_log_user_command(): Connection refused

This doesn't prevent me from making use of the sudo command to perform root level duties, however I'm wonder why I'm getting this message. After searching around on the web I found something about the message indicating that audit logging isn't enabled in the kernel.

Container: CentOS release 5.2 (Final)
Host: RHEL 5 (openvz kernel)
OpenVZ Kernel: 2.6.18-92.1.1.el5.028stab057.2
sudo: sudo-1.6.8p12-12.el5

How can I determine if audit logging is enabled? Does the latest OpenVZ kernel have it enabled?

Thanks.

Subject: Re: sudo audit log
Posted by maratrus on Tue, 25 Nov 2008 15:32:24 GMT
View Forum Message <> Reply to Message

Hello,

probably that after you've updated the VE some audit* packet has installed (please check it).

But it might be that a particular functionality is prohibited inside VE so you get such message.
You can strace "sudo" command to find out the syscall that is fails.
http://wiki.openvz.org/Stracing_a_program

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
```

Subject: Re: sudo audit log
Posted by maratrus on Tue, 25 Nov 2008 16:11:44 GMT
View Forum Message <> Reply to Message

Hello,

could you please show the full output.

Subject: Re: sudo audit log
Posted by zoom on Tue, 25 Nov 2008 16:29:39 GMT
View Forum Message <> Reply to Message

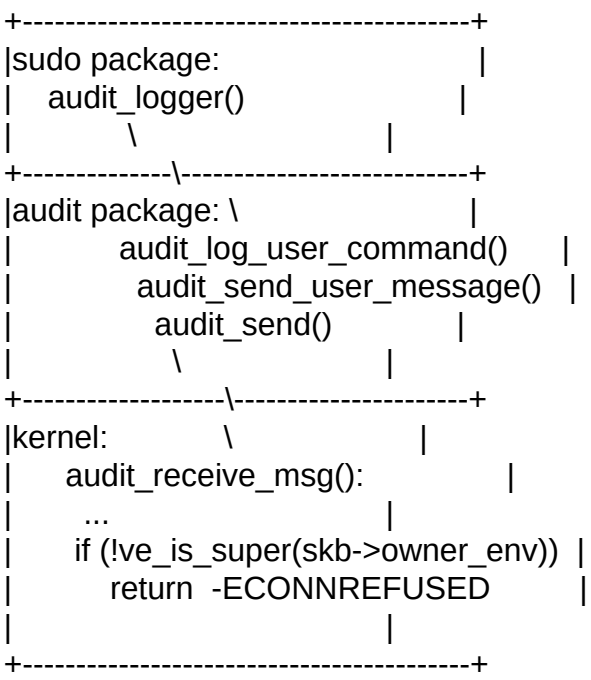
Sure.

Please see the attached file.

File Attachments
1) sudo-strace.txt, downloaded 572 times

Subject: Re: sudo audit log
Posted by maratrus on Tue, 25 Nov 2008 17:07:23 GMT
View Forum Message <> Reply to Message

Seems like here is the chain of calls:



So, it is prohibited to use audit inside VE (and sudo is build with audit support).
The patch from
https://bugzilla.redhat.com/show_bug.cgi?id=401201

should resolve this issue (but the problems are different)

Subject: Re: sudo audit log
Posted by zoom on Tue, 25 Nov 2008 17:22:03 GMT
View Forum Message <> Reply to Message

maratrus,

Thanks for taking the time to track this one down.

Much Appreciated!!