Subject: Auditd and openz

Posted by bvan on Thu, 22 Oct 2009 12:53:22 GMT

View Forum Message <> Reply to Message

Hello,

I have setup auditd on an openvz hostserver and it correctly logs events for both the host server and the containers. The problem I have however is that auditd does not display the full pathnames of event triggered in the container. I.e. if I add a rule

```
auditctl -w /vz/root/101/etc/shadow -k CFG_shadow
```

to put a file watch on /etc/shadow in VE 101, this will create an audit log when I touch the file:

```
type=SYSCALL msg=audit(1256215471.392:699910): arch=c000003e syscall=2 success=yes
exit=0 a0=7fff362acc8b a1=941 a2=1b6 a3=0 items=1 ppid=5126 pid=22744 auid=0 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=535 comm="touch" exe="/bin/touch"
key="CFG_shadow"
type=CWD msg=audit(1256215471.392:699910):  cwd="/"
type=PATH msg=audit(1256215471.392:699910): item=0 name="/etc/shadow" inode=16965399
dev=fd:00 mode=0100400 ouid=0 ogid=0 rdev=00:00
```

The problem is that this audit entry points to /etc/shadow instead of /vz/root/101/etc/shadow, even though the inode mentioned in the log points to /vz/root/101/etc/shadow.
This is a problem because now you can not see from which container the event was triggered. Do you have any ideas how to make the auditd container aware ?