Subject: VPS users interfere with HN ones
Posted by dagr on Sun, 07 Jan 2007 16:38:19 GMT
View Forum Message <> Reply to Message

2.6.9-023stab037.3-smp -RHEL4 x86 vzctl 3.0.13

First of all i noticed 1 thing, dont know is it bug or else . I can see proccesses inside different VPSs beeing outside them (in VE 0) under unprivileged user. It happens when user id inside VPS coincides with user_id inside HN. Just like this

[openvz@ws3-ca vps_dev]$ ps -ef| grep dagr

dagr 12391 12364 0 16:07 ? 00:00:00 /vps_core/mysql/libexec/mysqld --basedir=/vps_core/mysql --datadir=/vps_core/mysql/var --user=mysql --pid-file=/vps_core/mysql/var/vps-10121.super.vz.pid --skip-external-locking --port=3306 --socket=/tmp/mysql.sock
dagr 14835 14808 0 16:07 ? 00:00:00 /vps_core/mysql/libexec/mysqld --basedir=/vps_core/mysql --datadir=/vps_core/mysql/var --user=mysql --pid-file=/vps_core/mysql/var/vps-101221.super.vz.pid --skip-external-locking --port=3306 --socket=/tmp/mysql.sock
dagr 15325 15298 0 16:07 ? 00:00:00 /vps_core/mysql/libexec/mysqld --basedir=/vps_core/mysql --datadir=/vps_core/mysql/var --user=mysql --pid-file=/vps_core/mysql/var/vps-101257.super.vz.pid --skip-external-locking --port=3306 --socket=/tmp/mysql.sock
dagr 14597 14569 0 16:20 ? 00:00:00 /vps_core/mysql/libexec/mysqld --basedir=/vps_core/mysql --datadir=/vps_core/mysql/var --user=mysql --pid-file=/vps_core/mysql/var/vps-101262.super.vz.pid --skip-external-locking --port=3306 --socket=/tmp/mysql.sock

They are shown as running under dagr user, actually they are all in different VPSs under user mysql. It wouldnt bother me much if i didnt encountered 1 problem. I cant run mc or mcedit in HN under user dagr and root anymore , its just hangs, at the same time its ok under different user. Its obvious for me that its because dagr id coincides with mysql in vpss and root with many others inside them. Somehow even /etc/init.d/vz stop doesnt help. Didnt try reboot yet. If you have any ideas, please share.

Subject: Re: VPS users interfere with HN ones
Posted by rickb on Sun, 07 Jan 2007 17:47:23 GMT
View Forum Message <> Reply to Message

I think many people will wonder about this, so I will explain in detail.

The HN's /proc has directories for each PID in the system, even those which are created in the VE context. So, when you run programs like ps, lsof on the HN, "ps" thinks that all the pids belong to

the HN. The normal userspace tools which read /proc know nothing about openvz or virtualization. Many tools which read the uid will reference /etc/passwd to find the username because its easier for the user to see the username rather then the UID. In your case, the UIDs happen to clash. This is pure chance. If you run only lsof for example, you will see many of these:

lsof: no pwd entry for UID XXX

This means XXX is not present in /etc/passwd, but it is present in a VE's /etc/passwd. In conclusion, there is nothing "wrong" or "bugged" here, its just that the normal userspace tools like ps, lsof, etc do not have a concept of virtualization. In the future, when PID contexts get finalized in the linux kernel, the userspace tools will recognize that the PID does not belong to the HN and take a more intelligent action in displaying the username.

Rick Blundell

Subject: Re: VPS users interfere with HN ones
Posted by kir on Sun, 07 Jan 2007 21:05:25 GMT
View Forum Message <> Reply to Message

To add to what Rick just said:

(1) VE0, i.e. the host system itself, is considered to be «a parent» to all the VEs, thus it sees all the processes in all VEs. Sometimes this is handy for debugging VE-related problems. You can find out that VE a process with a given PID belongs to by checking the envID field in /proc/PID/status file.

(2) It is not recommended to run in VE0 anything but OpenVZ management-related tasks. I.e. it is not a good idea to have, say, MySQL installed in VE0 (just create a separate VE for it), or have ordinary users for the purposes other than OpenVZ HN administration tasks. The only networking daemon that you should run in VE0 should be sshd. If you will follow this recommendation you will not have problems with global process visibility. If you will not follow this recommendation, you could have severe security flaws/problems.
