Subject: Re: Scientific Linux 5.7 OS Templates in contrib
Posted by kir on Wed, 14 Sep 2011 21:36:07 GMT
View Forum Message <> Reply to Message

Indeed there is a specific set of actions to be performed on a newly created container which is to be used to make a template. This includes:
- log files truncation;
- yum/apt database cleanup;
- adjustments to cron jobs and init.d services;
- making sure ssh keys are unique (this is specific to Debian, maybe Ubuntu -- they generate key pairs on SSH package installation not the first run);
- disabling root login (usermod -L root should be sufficient, although it's always better to check);
- removing getty entries from inittab (or its upstart/systemd analog) — since there are no terminals in CT;
- making sure syslogd don't do sync () for each log line written (this ruins I/O performance if you have tens or hundreds of CTs);
- proper software repository configuration;
- (optional) removal of unneeded packages (like kernel) just for the sake of disk space savings (this is usually done by creating stub "dummy" packages that virtually provide the stuff required by other packages but not really needed;
- (optional) removal of some extra stuff like locale data;
- linking /etc/mtab to /proc/mounts (although it might not be needed);
- something else I can't remember at the moment.

Then, some things are performed by vzctl's postcteate.sh script which is run during vzctl create. This, among other things, include crontab times randomization, to prevent all CTs to run say cron.daily jobs at the same time.

Hope that helps,
  Kir.

--
Sent from my Android phone
On Sep 15, 2011 12:57 AM, "Kelvin Raywood" <kray@triumf.ca> wrote:
> Scott Dowdle wrote:
>> ...
>> The final products are a i386 and an x86_64 contributed SL 5.7 OS Template.
>
> Thanks very much for these Scott. This is much appreciated.
>
> I just wanted to mention one thing that I got bitten by recently with a
> template from contrib.
>
> In the official templates, /etc/shadow has * in the encrypted-password

> field for root so that you can't login as root using a password.
> In April, an early SL-6.0 template was contributed
> (scientificlinux-6.0-x86.tar.gz Apr-11-2011) which has an encrypted
> password string for root.
>
> We normally disable password access to root in /etc/ssh/sshd_config via
> "PermitRootLogin without-password" and use ssh keys or "vzctl enter" to
> get root access so didn't notice that the machine had a root password
> enabled. Also, since it was our first SL-6 container, we didn't have
> our deployment procedure sorted out properly and this was the
> sshd_config part.
>
> It didn't take long for some spider to find the machine and guess the
> password. An IRC robot was installed and /root/.ssh/authorized_keys was
> overwritten. We noticed fairly quickly and then cracked the password
> string.
>
> Anyway, we learned our lesson but I think it would also be good practice
> for contributors to check that their template does not have a root
password.
>
> Oh yeah - the cracked password ... password
>
> --
> Kel Raywood
> TRIUMF
> Vancouver BC
>