Subject: Re: TinyVZ 0.7 released
Posted by Solar Designer on Mon, 22 Aug 2011 16:12:18 GMT
View Forum Message <> Reply to Message

On Sat, Aug 20, 2011 at 06:36:28PM -0400, Sam Trenholme wrote:
> TinyVZ 0.7 is a tiny little OpenVZ template for making OpenVZ
> containers that use the lowest amount of memory and hard disk space
> possible.
>
> This is a self-hosting template with all source code; it is possible
> to compile the entire system inside of the template. Look in the
> build/ directory (inside the template) for source code.

This is very nice. My concern, though, is that things such as uClibc were not built with security in mind. I am pretty sure that uClibc is problematic when used in conjunction with SUID/SGID programs. Does uClibc ensure that fd 0-2 are open on program startup (opening them to /dev/null / /dev/full if not)? I doubt it. I admit I haven't checked, though.

I think a better libc to use for this purpose would be musl:

http://www.etalabs.net/musl/

It also lacks some of those highly desirable security measures, but I think it will gain those soon.

While uClibc is primarily for embedded systems, musl is primarily for typical/full systems - just without glibc's bloat.

Meanwhile, the sad truth may be that under Linux we need to use (e)glibc (or other clones of it) for SUIDs/SGIDs. <plug>BTW, the full Owl userland, with development/build tools, is just 112 MB under .tar.gz:
http://mirrors.kernel.org/openwall/Owl/current/vztemplate/
It is also able to rebuild itself, although the source code is not part of the .tar.gz (just the development/build tools/libs are). With the source tarballs added, the size increases a lot indeed... to 280 MB if we exclude just the Linux kernel, which is not installed in an OpenVZ container anyway.
</plug>

Alexander