Subject: *DISCUSSED* Does OpenVZ have support for GrSecurity?
Posted by joelee on Sun, 15 Jul 2007 19:26:55 GMT
View Forum Message <> Reply to Message

Hi All,

I've search the forum and noticed some past discussion for GrSecurity support in OVZ. I wanted to know if OVZ have support for it and if not is there plans to support this in near future.

If this feature is already being supported, I would appreciate any comments on its use with OVZ.

Joe

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by dev on Tue, 17 Jul 2007 10:32:37 GMT
View Forum Message <> Reply to Message

we have experimental grsecurity patch on top of 2.6.18 stable OVZ kernel, but it is unstable and I'm not sure will become stable one day... :/

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by joelee on Tue, 17 Jul 2007 18:19:05 GMT
View Forum Message <> Reply to Message

Quote:we have experimental grsecurity patch on top of 2.6.18 stable OVZ kernel, but it is unstable and I'm not sure will become stable one day... :/

Hmm, not to optimistic. Can you elaborate a bit as to why you feel it will not be stable one day. I am understanding if one wants to provides various chroot protection and other aspect to kernel security GrSecurity like solutions would be essential to be patch in the kernel. Also, if it can't be supported in a stable way are there other options besides GrSecurity?

Joe

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by dev on Wed, 18 Jul 2007 07:42:36 GMT
View Forum Message <> Reply to Message

grsecurity does conflict much with openvz changes, so it requires some efforts to resolve/fix them. Also grsecurity patch looks to be poorly documented and thus it's hard to dig into it. If there is a volunteer we can give him a patch we already have for doing this job. Surely, it is not impossible, it is just what we have no resources for :/

Next, there are some concerns about security. RHEL5 kernel provides
execshield and randomization of address spaces. So the major feature is available out of the box.
Many other features of grsecurity look like a fake security (just giving you a feeling of safeness),
e.g. users which can't see other user processes in the /proc. It doesn't help security and a little bit
experienced user can still easily find all the other PIDs in the system.

And the main question is why someone wants grsecurity? To protect users from each other? Then
use dedicated VE for each of them (which is a much hardened chroot protection even compared
to grsec) and be happy. If I miss something and you need some particular feature of grsec, then
plz give me to know. We'll do our best to bring it.

---

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by joelee on Wed, 18 Jul 2007 15:44:54 GMT
View Forum Message <> Reply to Message

Dev, I thank you for your comments below. However, I must say that I don't share your views to
saying:
Quote:
Then use dedicated VE for each of them (which is a much hardened chroot protection even
compared to grsec) and be happy.

That statement is not practical to give each user dedicated VE. While OpenVZ VE is great I don't
think its designed to give each user VE to improve security. VE are used mainly to consolidate
servers and offering isolation for those servers. That's why there's tools like GrSecurity, SELinux,
IPtables and such to provide additional layer of security for users.

I am not much of an expert in this area and respect your other comments implying GrSecurity is
not much of help. So, how about SElinux, RBAC, Running tools like Bastille to harnend the OS.
Will they not prove helpful either.

IMO, I think it would be best for someone who can fix the issues regarding GrSecurity and
perhaps other tools so that they can be used by used properly with OVZ.

Joe

---

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by dev on Wed, 18 Jul 2007 16:15:13 GMT
View Forum Message <> Reply to Message

Ouch, I definetely didn't mean to say that any of these technologies is useless  Sure, not.

What I meant to say is that VEs are designed to be fully isolated - in resource management, in
networking (can't sniff etc.), file systems, etc. So 2 users in 2 different VEs are isolated in many

regards better that on a signle machine using 2 different users with SELinux IMHO. It's my imho. Why? because SELinux doesn't try to solve DoS issues, resource management issues and so on. It solves only accessibility issues.

What VEs do not try to solve at all - protection from the other world. Sure, iptables and firewalls do it's job here.

And I fully support your statement that it would be fine if OpenVZ could support all of them. I guess SELinux must be the first one, as it is a part of mainstream kernel.

---

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by joelee on Wed, 18 Jul 2007 22:28:24 GMT
View Forum Message <> Reply to Message

Dev, your point is well made and I am much in agreement. But, the example you gave about the 2 users being more protected if they are on different VE as appose to being on one with SELinux or GrSecurity is correct.

However, as you know, in a real world environment a VE will be supporting many many users. And, a one will still want to find ways to further secure/protect users or apps from each other - That's where SElinux and GrSecurity tools come into play and serve there purpose.

Therefore if OpenVZ has some technical issues to support those tools then it would make sense for OVZ to put some effort to getting those fix - Hope you agree!

I initially made this post because I wanted to be able to chroot users in SSH, FTP, etc... And, that the Grsecurity like tool is recommended to be patch to kernel to enhance the chrooting capabiltiy. And, I've come to learn that OVZ had problems with GrSecurity.

I hope some attention can be placed on this by OVZ team to fix what can be fix in order to support GrSecurity and/or SElinux.
Hope you get my point! Anyway, thanks for your comments...

Joe

---

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by dev on Thu, 19 Jul 2007 06:48:48 GMT
View Forum Message <> Reply to Message

Yep. I got your point too :@) So we are in agreement
SELinux support is on TODO list, though I can't say timeline yet.

Thanks for your feedback!

---

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by joelee on Thu, 19 Jul 2007 13:59:04 GMT
View Forum Message <> Reply to Message

One question came to mind and hope you can clarify for me. The issues with OVZ not supporting GrSecurity or SElinux currently - Is that only a issue for the HN or VE's as well.

Is there an issue to install GrSecurity on the VE itself.

Joe

Subject: Re: Does OpenVZ have support for GrSecurity?
Posted by dev on Thu, 19 Jul 2007 14:37:24 GMT
View Forum Message <> Reply to Message

it's kernel patches which can't be easily added or enabled. So the answer is: both HN and VE