Subject: Pureftpd and Linux capabilties
Posted by christoph on Sun, 02 Jul 2006 16:02:22 GMT
View Forum Message <> Reply to Message

Hello!

I'm trying to get pureftpd running inside a Debian sarge VPS.
There seems to be a problem with Linux capabilities.

What can be done to solve that issue without recompiling pureftpd with "--without-capabilities"?

/etc/init.d/pure-ftpd-mysql start
Starting ftp server: Running: /usr/sbin/pure-ftpd-mysql -l mysql:/etc/pure-ftpd/db/mysql.conf -E -u 60 -O clf:/var/log/ftp/transfer.log -A -B
421 Unable to switch capabilities : Operation not permitted

My versions:
ii pure-ftpd-common 1.0.19-4 Pure-FTPd FTP server (Common Files)
ii pure-ftpd-mysql 1.0.19-4 Pure-FTPd FTP server with MySQL user authenticat

Thank you for any hints!
Christoph

Subject: Re: Pureftpd and Linux capabilties
Posted by dev on Sun, 02 Jul 2006 19:20:34 GMT
View Forum Message <> Reply to Message

1. you can strace pureftpd to check what capabilities it tries to set and fails.
See http://wiki.openvz.org/Stracing_a_program for information on how to strace an application.

2. after you found what's wrong with capabilities you can add missing capability to your VE with vzctl command. Check vzctl man on how to control VE capabilities (http://openvz.org/documentation/mans/vzctl.8):

#vzctl set <VEID> --capability capname:on|off

Note: changing capabilities requires VE restart.

Subject: Re: Pureftpd and Linux capabilties
Posted by christoph on Sun, 02 Jul 2006 20:50:03 GMT
View Forum Message <> Reply to Message

Hi!

Thanks for the fast (especially on Sunday) and competent answer.

I found out with strace that pureftpd likes to set the following capabilities:

CHOWN DAC_READ_SEARCH SETGID SETUID NET_BIND_SERVICE NET_ADMIN SYS_CHROOT SYS_NICE CHOWN DAC_READ_SEARCH SETGID SETUID NET_BIND_SERVICE NET_ADMIN SYS_CHROOT SYS_NICE

I activated those via vzctl and it works perfectly now!

One thing I was thinking about. What about security when all those capabilities are set?

Christoph

Subject: Re: Pureftpd and Linux capabilties
Posted by luismi on Mon, 03 Jul 2006 00:18:45 GMT
View Forum Message <> Reply to Message

Hi there,

Yes, I have the sane problem here.
You need to recompile the pure-ftpd package using the next option:

--without-capabilities: if the capabilities library (libcap) is found,
Pure-FTPd will try to use it in order to enhance security. This option
overrides the test to ignore the library. Try this if capabilities don't
work properly on your system. libcap can be downloaded from
ftp://ftp.kernel.org/pub/linux/libs/security/linux-privs/ .

From: http://download.pureftpd.org/pub/pure-ftpd/doc/README

I can send you my packages if you want, I use puredb since I have few accounts but I also created the mysql and ldap packages, for the future

I am not using the latest version 1.0.22 since I use the version from a debian stable mirror, that is, 1.0.19.

Also if you need some help recompiling pure-ftpd under debian, let me know, I will try to help you

Regards.

Subject: Re: Pureftpd and Linux capabilties

Posted by luismi on Mon, 03 Jul 2006 00:19:56 GMT
View Forum Message <> Reply to Message

Cristoph,

How do you activate those capabilities using vzctl?

I am very insterested on that.

Subject: Re: Pureftpd and Linux capabilties
Posted by christoph on Mon, 03 Jul 2006 06:39:45 GMT
View Forum Message <> Reply to Message

Hi!

Thanks for your package offering. I think I'll stick with the Debian version since it is working now after having set the capabilities.

Here is how I set the capabilities for the VPS via bash:

```
VPSID=123
for CAP in CHOWN DAC_READ_SEARCH SETGID SETUID NET_BIND_SERVICE NET_ADMIN
SYS_CHROOT SYS_NICE CHOWN DAC_READ_SEARCH SETGID SETUID
NET_BIND_SERVICE NET_ADMIN SYS_CHROOT SYS_NICE
do
  vzctl set $VPSID --capability ${CAP}:on --save
done
```

Regards
Christoph

Subject: Re: Pureftpd and Linux capabilties
Posted by dev on Mon, 03 Jul 2006 07:22:13 GMT
View Forum Message <> Reply to Message

can you confirm please that CAP_NET_ADMIN is the one to blame? i.e. remove it and recheck

if it is CAP_NET_ADMIN then it is really buggy software :/
This capability is too powerfull to give it as is. So from security point of view, sure it is not good.

Subject: Re: Pureftpd and Linux capabilties
Posted by christoph on Mon, 03 Jul 2006 18:31:43 GMT

Hi!

I removed CAP_NET_ADMIN and it doesn't work then.

Here is a part of the strace with CAP_NET_ADMIN disabled.
strace /usr/sbin/pure-ftpd-mysql:

capset(0x19980330, 0,
{CAP_CHOWN|CAP_DAC_READ_SEARCH|CAP_SETGID|CAP_SETUID|CAP_NET_BIND_SERVICE|CAP_NET_ADMIN|CAP_SYS_CHROOT|CAP_SYS_NICE,
CAP_CHOWN|CAP_DAC_READ_SEARCH|CAP_SETGID|CAP_SETUID|CAP_NET_BIND_SERVICE|CAP_NET_ADMIN|CAP_SYS_CHROOT|CAP_SYS_NICE, }) = -1 EPERM (Operation not permitted)
rt_sigprocmask(SIG_BLOCK, ~[RTMIN], [], 8) = 0
fstat64(1, {st_mode=S_IFCHR|0600, st_rdev=makedev(136, 0), ...}) = 0
mmap2(NULL, 4096, PROT_READ|PROT_WRITE, MAP_PRIVATE|MAP_ANONYMOUS, -1, 0) = 0x40018000
write(1, "421 Unable to switch capabilitie"..., 61421 Unable to switch capabilities : Operation not permitted
) = 61

Christoph

Subject: Re: Pureftpd and Linux capabilties
Posted by christoph on Tue, 04 Jul 2006 14:15:20 GMT

Hi!

I now checked the source code of pureftpd.
It seems that it always keeps CAP_NET_ADMIN.

What should one think about that?

Christoph

caps.c:
 http://pureftpd.cvs.sourceforge.net/pureftpd/pureftpd/src/ca ps.c?view=markup

...
```
void set_initial_caps(void)
{
    apply_caps(cap_keep_startup,
            sizeof(cap_keep_startup) / sizeof(cap_value_t));
```

}
...

caps_p.h:
http://pureftpd.cvs.sourceforge.net/pureftpd/pureftpd/src/ca ps_p.h?view=markup

...
```
cap_value_t cap_keep_startup[] = {
    CAP_SETGID,
    CAP_SETUID,
    CAP_CHOWN,
    CAP_NET_BIND_SERVICE,
    CAP_SYS_CHROOT,
    CAP_SYS_NICE,
    CAP_NET_ADMIN,
    CAP_DAC_READ_SEARCH
};

cap_value_t cap_keep_login[] = {
# ifndef WITH_PRIVSEP
#  ifndef HAVE_SYS_FSUID_H
    CAP_SETUID,
#  endif
    CAP_NET_BIND_SERVICE,
# endif
    CAP_NET_ADMIN
};
```
...

Subject: Re: Pureftpd and Linux capabilties
Posted by dev on Tue, 04 Jul 2006 14:26:46 GMT
View Forum Message <> Reply to Message

You can try to contact pureftpd authors.
First, I can't imagine why CAP_NET_ADMIN can be required for FTP daemon

Next, it looks wrong to fail if this capability is not currently available. why it doesn't try to apply AND mask on current capabilities available via capget()?

Subject: Re: Pureftpd and Linux capabilties
Posted by rema on Wed, 14 Mar 2007 14:04:48 GMT
View Forum Message <> Reply to Message

luismi wrote on Sun, 02 July 2006 20:18Hi there,
Also if you need some help recompiling pure-ftpd under debian, let me know, I will try to help you

Regards.

could you give some hints here how this could be done using sarge?

best rema

Subject: Re: Pureftpd and Linux capabilties
Posted by Valmont on Thu, 15 Mar 2007 09:11:46 GMT
View Forum Message <> Reply to Message

//some offtop

The best way - is to use vsftpd. It is fast,secure and doesn't need these caps.

Subject: Re: Pureftpd and Linux capabilties
Posted by rema on Thu, 15 Mar 2007 12:03:51 GMT
View Forum Message <> Reply to Message

hmm, but i need an mysql backend ....

Subject: Re: Pureftpd and Linux capabilties
Posted by Valmont on Thu, 15 Mar 2007 12:14:36 GMT
View Forum Message <> Reply to Message

At least now - only with pam_mysql.

Subject: Re: Pureftpd and Linux capabilties
Posted by xdanx on Fri, 25 Nov 2011 00:55:30 GMT
View Forum Message <> Reply to Message

So.. is it a major security risk if I can't recompile pureftp-d and I'm forced to use those capabilities ?

Would those capabilities turned on for the container help affect in any way the node, in case the container gets rooted ? In other words, can those extra added capabilities for the container

represent a security hole (for the container and/or node)?

I'm thinking that even without running OpenVZ, on a normal [for example] Ubuntu installation those capabilities are required by the ftp server and people don't panic that much about it.

Thanks,
Dan

Subject: Re: Pureftpd and Linux capabilties
Posted by dev on Fri, 25 Nov 2011 08:24:36 GMT
View Forum Message <> Reply to Message

Quote:Would those capabilities turned on for the container help affect in any way the node, in case the container gets rooted ? In other words, can those extra added capabilities for the container represent a security hole (for the container and/or node)?

These capabilities represent a security hole for a container, not for the whole node.

Quote:
I'm thinking that even without running OpenVZ, on a normal [for example] Ubuntu installation those capabilities are required by the ftp server and people don't panic that much about it.

Well, people typically never panic when they do not know much about it

I will ask kir@, maybe he will contact pureftpd and get it fixed.

Subject: Re: Pureftpd and Linux capabilties
Posted by xdanx on Fri, 25 Nov 2011 15:39:24 GMT
View Forum Message <> Reply to Message

I see. Thanks for the info.
And I agree with you: it is a bit strange for pure-ftpd to ask for that many capabilities (including NET_ADMIN)

For anyone who wants to know what they do exactly, go to http : //linux.die.net/man/7/capabilities

OR in linux

man capabilities

Cheers,
Dan
