FreeNAS - Bug #22961

Cannot add passphrase component to initiallly key encrypted volume

03/30/2017 12:39 PM - Wojciech Kloska

Status:	Resolved		
Priority:	Important		
Assignee:	Alexander Motin		
Category:	OS		
Target version:	11.0-RC		
Seen in:	9.10.2-U2	**Needs Merging:**	Yes
Severity:	New	**Needs Automation:**	No
Reason for Closing:		**Support Suite Ticket:**	n/a
Reason for Blocked:		**Hardware Configuration:**	
Needs QA:	Yes	**ChangeLog Required:**	No
Needs Doc:	Yes		

Description

This looks like a probable GELI issue, or some kind of misinterpretation of configuration knobs - when volume is created as key encrypted later attempts to rekey it using password or password+key components fail (rekey with key is working fine). GELI seems sad about `-i` switch being used somewhere, but there's nothing in the middleware using that switch - need further investigation.

Associated revisions

Revision 3467132c - 04/21/2017 01:08 AM - Alexander Motin

Always allow setting number of iterations for the first time.

Before this change it was impossible to set number of PKCS#5v2 iterations,
required to set passphrase, if it has two keys and never had any passphrase.
Due to present metadata format limitations there are still cases when number
of iterations can not be changed, but now it works in cases when it can.

PR: 218512
MFC after: 2 weeks
Sponsored by: iXsystems, Inc.
Differential Revision: https://reviews.freebsd.org/D10338

(cherry picked from commit 1fbe8b4c28a7aacc43ccb204ac2e9fb17485c490)

Ticket: #22961

Revision 3467132c - 04/21/2017 01:08 AM - Alexander Motin

Always allow setting number of iterations for the first time.

Before this change it was impossible to set number of PKCS#5v2 iterations,
required to set passphrase, if it has two keys and never had any passphrase.
Due to present metadata format limitations there are still cases when number

of iterations can not be changed, but now it works in cases when it can.

PR: 218512
MFC after: 2 weeks
Sponsored by: iXsystems, Inc.
Differential Revision: https://reviews.freebsd.org/D10338

(cherry picked from commit 1fbe8b4c28a7aacc43ccb204ac2e9fb17485c490)

Ticket: #22961

History

#1 - 03/31/2017 12:30 PM - Frank Riley

This is indeed a geli restriction. -i is on by default when you specify a passphrase. For whatever reason, geli won't let you add a passphrased key if an existing key is set.

#2 - 03/31/2017 02:52 PM - Wojciech Kloska

Frank Riley wrote:

> This is indeed a geli restriction. -i is on by default when you specify a passphrase. For whatever reason, geli won't let you add a passphrased key if an existing key is set.

That seems to be a bug in GELI, because if I create a password or passowrd+key protected volume, I can then rekey between any of possible security combinations (key, key+password, password). That limitation does not seem to make much sense as `-i` is a default always when protection by password is a thing - not only during geli init, but also geli setkey - setkey reevaluates iterations value automatically even if `-i` wasn't provided via command line.

#3 - 04/04/2017 02:48 PM - Wojciech Kloska

- Assignee changed from Wojciech Kloska to Alexander Motin

Over to Sasha for investigation.

So far I have found out that there are two places containing functions for setting GELI user key:

- https://github.com/freenas/os/blob/freebsd11/sbin/geom/class/eli/geom_eli.c#L1164
- https://github.com/freenas/os/blob/freebsd11/sys/geom/eli/g_eli_ctl.c#L559

Both contain very similar check:

```
        if (bitcount32(md.md_keys) != 1) {
            gctl_error(req, "To be able to use '-i' option, only "
                "one key can be defined.");
            return;
        }
```

The main difference is that part in kernel performs this check always, while the other only for detached providers.

Even if there's any reason why this should fail when using setkey with explicit -i switch being set, we're not setting -i nowhere and it still does fail.

I smell some inconsistency here, because when iterations (-i) are calculated automatically inside of GELI (geli init with passphrase and key components active, but no -i specified) I can then rekey as much as I want using any slot I want. According to man page GELI is always using PKCS#5v2 during processing passphrase component of the user key, unless explicitly disabled.

I can't find anywhere in the documentation that rekey from key encryption to key+password encryption is prohibited - that's why I think that's a bug.

During my tests I have removed check (https://github.com/freenas/os/blob/freebsd11/sys/geom/eli/g_eli_ctl.c#L617) completely and rebuilt the kernel. After that things seem to be working well and I cannot reproduce the failing scenario anymore (or find any other issues introduced by that change).

There are two main questions here IMO: can these checks be completely removed as I did? If not, how we should modify them to allow at least this particular use case of switching between encryption types with no issues?

#4 - 04/06/2017 03:45 AM - Alexander Motin

- Status changed from Screened to Fix In Progress

Those checks should not be removed, since they are protecting against situation when changing number of iteration for one key would invalidate the other one, since there is only one md_iterations field in metadata. I think correct solution could be to check present value of md_iterations, and allow changing it if it is -1. But I'll take deeper look in case if there are some other better options.

#5 - 04/09/2017 03:58 PM - Frank Riley

Wojciech Kloska wrote:

> Even if there's any reason why this should fail when using setkey with explicit -i switch being set, we're not setting -i nowhere and it still does fail.

If you're not setting it, you're using it. It calculates how many iterations it can do in 2 seconds and uses that.

Anyway, I've been frustrated by this restriction before so I fixed it. You can see my bug report here and my pull request here. Hopefully they will pull it in.

#6 - 04/10/2017 12:09 AM - Alexander Motin

I written my own patch over the weekend: https://reviews.freebsd.org/D10338

#7 - 04/17/2017 12:38 PM - Alexander Motin

- Project changed from 9 to FreeNAS

- Category changed from 534 to 137

- Target version changed from 384 to 9.10.4

- Seen in changed from to 9.10.2-U2

#8 - 04/18/2017 01:30 AM - Alexander Motin

- Priority changed from Regression to Important

Its not a regression. It never worked properly.

#9 - 04/19/2017 07:57 AM - Kris Moore

- Target version changed from 9.10.4 to 11.1

#10 - 04/21/2017 01:09 AM - Alexander Motin

- Status changed from Fix In Progress to Resolved

- Target version changed from 11.1 to 11.0

#12 - 05/03/2017 10:57 PM - Vaibhav Chauhan

- Target version changed from 11.0 to 11.0-RC