sepia - Bug #45009

https://download.ceph.com/keys/release.asc: ignored as the file has an unsupported filetype.

04/09/2020 07:47 AM - Sebastian Wagner

Status:	Need More Info	**% Done:**	0%
Priority:	Normal		
Assignee:	David Galloway		
Category:			
Target version:			
Source:		**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:		**ceph-qa-suite:**	
Regression:	No	**Crash signature:**	
Severity:	3 - minor		

Description

https://download.ceph.com/keys/release.asc is a file format that is not understood by apt:

```
root@buster:~# wget https://download.ceph.com/keys/release.asc
root@buster:~# file release.asc 
release.asc: PGP public key block Public-Key (old)
root@buster:~# cp release.asc /etc/apt/trusted.gpg
root@buster:~# apt update
Hit:1 http://httpredir.debian.org/debian buster InRelease
Hit:2 https://download.ceph.com/debian-octopus buster InRelease
Err:2 https://download.ceph.com/debian-octopus buster InRelease
  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY E84AC2C0460F3994
Reading package lists... Done
Building dependency tree       
Reading state information... Done
All packages are up to date.
W: http://httpredir.debian.org/debian/dists/buster/InRelease: The key(s) in the keyring /etc/apt/trusted.gpg are ignored as the file has an unsupported filetype.
W: https://download.ceph.com/debian-octopus/dists/buster/InRelease: The key(s) in the keyring /etc/apt/trusted.gpg are ignored as the file has an unsupported filetype.
W: An error occurred during the signature verification. The repository is not updated and the previous index files will be used. GPG error: https://download.ceph.com/debian-octopus buster InRelease: The following signatures couldn't be verified because the public key is not available: NO_PUBKEY E84AC2C0460F3994
W: Failed to fetch https://download.ceph.com/debian-octopus/dists/buster/InRelease  The following signatures couldn't be verified because the public key is not available: NO_PUBKEY E84AC2C0460F3994
W: Some index files failed to download. They have been ignored, or old ones used instead.
```

However, when converting this to GPG v4, it works:

```
root@buster:~# apt-key add release.asc
root@buster:~# file /etc/apt/trusted.gpg
/etc/apt/trusted.gpg: PGP/GPG key public ring (v4) created Tue Sep 15 20:56:41 2015 RSA (Encrypt or Sign) 4096 bits MPI=0xcbaa7e8ef94169f9...
root@buster:~# apt update
Hit:1 http://httpredir.debian.org/debian buster InRelease
Get:2 https://download.ceph.com/debian-octopus buster InRelease [8557 B]
Get:3 https://download.ceph.com/debian-octopus buster/main amd64 Packages [15.7 kB]
Fetched 24.2 kB in 4s (6765 B/s)
Reading package lists... Done
```

```
Building dependency tree       
Reading state information... Done
All packages are up to date.
root@buster:~# apt-key list
/etc/apt/trusted.gpg
--------------------
pub   rsa4096 2015-09-15 [SC]
      08B7 3419 AC32 B4E9 66C1  A330 E84A C2C0 460F 3994
uid           [ unknown] Ceph.com (release key) <security@ceph.com>
```

This has an impact on cephadm, which needs to install gnupg on **all** cluster machines in order to convert the key to GPG v4.

Can we provide a key in the correct format?

Related issues:

Blocks Orchestrator - Bug #44972: cephadm: add-repo on ubuntu broken **New**

History

#1 - 04/09/2020 07:48 AM - Sebastian Wagner

- Blocks Bug #44972: cephadm: add-repo on ubuntu broken added

#2 - 04/16/2020 09:50 PM - David Galloway

- Assignee set to David Galloway

How do you convert it? I'm not finding anything that even indicates gpg has a version 4.

#3 - 04/23/2020 11:06 AM - Sebastian Wagner

```
apt-key add release.asc
```

automatically converts it to the correct format.

#4 - 04/28/2020 02:05 PM - David Galloway

Is the resulting /etc/apt/trusted.gpg file something that should be reused though? It's not ascii.

This works fine on Debian 10: wget -q -O- 'https://download.ceph.com/keys/release.asc' | sudo apt-key add - as our docs suggest.

I tried importing the key then exporting it using apt-key export but it just outputs the same public key block (minus Version: GnuPG v1)

#5 - 05/04/2020 01:37 PM - Sebastian Wagner

yes, `apt-key` works, but would require to add gnupg as a dependency for cephadm on all hosts.

#6 - 05/04/2020 05:28 PM - David Galloway

What I'm getting at is, is /etc/apt/trusted.gpg after apt converts the key portable? Can we just throw trusted.gpg on download.ceph.com and it'll work universally?

#7 - 07/14/2020 02:05 PM - Jon Spriggs

For those trying to follow along, I ended up doing this:

curl https://download.ceph.com/keys/release.asc | gpg --no-default-keyring --keyring /tmp/fix.gpg --import - && gpg --no-default-keyring --keyring /tmp/fix.gpg --export > /etc/apt/trusted.gpg.d/ceph.release.gpg && rm /tmp/fix.gpg

The key import itself works fine, it's just that the Debian repo it matches against can't process the type 1 GPG key.

The output files in /etc/apt/trusted.gpg.d/ (e.g. debian-archive-buster-stable.gpg) are also not ascii files, they're data blobs.

#8 - 07/14/2020 03:09 PM - David Galloway

Jon Spriggs wrote:

> The output files in /etc/apt/trusted.gpg.d/ (e.g. debian-archive-buster-stable.gpg) are also not ascii files, they're data blobs.

Are the data blobs portable? Could I just upload those to download.ceph.com and have our tooling pull the new keys if the OS is using the newer GPG version?

#9 - 08/01/2020 01:24 PM - Mohammed Naser

I am running into this issue on Debian buster. I'm happy to contribute the changes if someone wants to upload things on the Ceph side.

#10 - 08/03/2020 02:59 PM - David Galloway

Mohammed Naser wrote:

> I am running into this issue on Debian buster. I'm happy to contribute the changes if someone wants to upload things on the Ceph side.

I'd be happy to upload a patched key. I just still haven't gotten confirmation that a patched key is portable. i.e., if a key you've imported on your machine can be imported to any machine.

#11 - 08/03/2020 03:33 PM - Mohammed Naser

Cool. I decided to run a little experiment in that case:

```
docker run -it --rm debian:buster
apt update
apt install curl gnupg
curl https://download.ceph.com/keys/release.asc | gpg --no-default-keyring --keyring /tmp/fix.gpg --import - &
& gpg --no-default-keyring --keyring /tmp/fix.gpg --export > /etc/apt/trusted.gpg.d/ceph.release.gpg && rm /tm
p/fix.gpg
md5sum /etc/apt/trusted.gpg.d/ceph.release.gpg
```

The md5sum was 86c50270e710a52ba54922f8959bb253. I reran the same exact thing in another Docker container and ended up with the same md5sum. Now, to test the theory that it's portable, I uploaded that file here:

https://bashupload.com/rPoHl/nYBR_.gpg

I launched a new container again, but this time using the consumed key:

```
docker run -it --rm debian:buster
apt update
apt install curl
curl https://bashupload.com/rPoHl/nYBR_.gpg > /etc/apt/trusted.gpg.d/ceph.release.gpg
echo deb https://download.ceph.com/debian-octopus/ buster main | tee /etc/apt/sources.list.d/ceph.list
apt update
apt install librados2
apt info librados2
```

The result returns

```
# apt info librados2
Package: librados2
Version: 15.2.4-1~bpo10+1
Priority: optional
Section: libs
Source: ceph
Maintainer: Ceph Maintainers <ceph-maintainers@lists.ceph.com>
Installed-Size: 13.4 MB
Depends: libblkid1 (>= 2.17.2), libc6 (>= 2.28), libgcc1 (>= 1:3.0), libibverbs1 (>= 1.1.6), liblttng-ust0 (>=
 2.5.0), librdmacm1 (>= 1.0.15), libssl1.1 (>= 1.1.0), libstdc++6 (>= 6), libudev1 (>= 183), zlib1g (>= 1:1.1.
4)
Conflicts: librados
Replaces: librados
Homepage: http://ceph.com/
Download-Size: 3110 kB
APT-Manual-Installed: yes
APT-Sources: https://download.ceph.com/debian-octopus buster/main amd64 Packages
Description: RADOS distributed object store client library

N: There is 1 additional record. Please use the '-a' switch to see it
```

So, my little experiment confirms that it works and feel free to reproduce it with the instructions above. :)

#12 - 08/21/2020 04:33 PM - David Galloway

Mohammed Naser wrote:

> Cool. I decided to run a little experiment in that case:

Thanks so much for this!

@Sebastian, can we have cephadm start using http://download.ceph.com/keys/release.gpg instead of release.asc?

#13 - 08/21/2020 04:34 PM - David Galloway

- Status changed from New to Fix Under Review

#14 - 08/21/2020 05:24 PM - Mohammed Naser

I believe that the following section must be updated:

https://github.com/ceph/ceph/blob/cb529acaf485a62c48df557341a88d3092823ee2/src/cephadm/cephadm#L4289-L4290

#15 - 09/16/2020 09:04 PM - Nathan Cutler

David Galloway wrote:

> @Sebastian, can we have cephadm start using http://download.ceph.com/keys/release.gpg instead of release.asc?

I don't know the answer to that, but I tried simply replacing 'release.asc' with 'release.gpg' in the cephadm source code and that doesn't work.

#16 - 09/16/2020 09:11 PM - David Galloway

- Status changed from Fix Under Review to Need More Info

Okay, well I did what was asked. If there's another format I need to upload, let me know.