Ceph - Feature #11032

selinux policy for ceph-mon

03/05/2015 04:08 PM - Sage Weil

Status:	Resolved	**% Done:**	0%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:			
Category:			
Target version:	v9.0.7		
Source:	other	**Reviewed:**	
Tags:		**Affected Versions:**	
Backport:		**Pull request ID:**	

Description

From an internal red hat discussion:

There are probably three distinct things we need to do to get cephs and SELinux to work together.

1. It should just work out of the box. If there is any issue that prevents cephs from working with SELinux in enforcing mode either on the client or server, this needs to be fixed by the SELinux team ASAP. But we need to know what is happening. Have your QE team do their testing in enforcing mode and if things break have them work in permissive and report bugs including the AVC messages. You can collect these via

```
ausearch -m avc -i -ts recent
```

Attach these to the bugzilla and work with SELinux engineers to get the policy updated.

2. Start to build policy to confine Cephs Daemons. Anything that is running on a cephs server as unconfined_service_t or initrc_t or init_t will need to have policy written for it.

```
ps -eZ | grep unconfined_service
```

Will tells us the daemons that need policy written. Open a bugzilla for any daemons that do not have policy written for them and the SELinux team will work with you and QE to write policy.

3. Does cephs support XAttrs? SELinux relies on XATTR support to label content differently. SELinux is a labeling system, we label every process and every file system object and then write rules controlling access between process labels and file labels. If a file system does not support XAttrs then we can label the entire file system with the same label via a mount "context" option, but this is not ideal since we do not get the fine grained control. For example if we wanted to have two different VM images on a cephs file system, we would want to have them labeled differently.

History

#1 - 08/04/2015 02:40 PM - Sage Weil

- Target version set to v9.0.7

#2 - 08/13/2015 06:03 PM - Sage Weil

- Status changed from New to Resolved