Contribution ID: **265** Type: **not specified**

Using kernel keyrings with containers

Tuesday, 10 September 2019 18:40 (30 minutes)

The kernel contains a keyrings facility for handling tokens for filesystems and other kernel services to use. These are frequently disabled for container environments, however, because they were not made namespace aware by the authors of the user-namespace and others.

Unfortunately, this lack prevents various things from working inside containers. To get around this, keys are now being tagged with a namespace tag that allows keys operating in different namespaces to coexist in the same keyring and restrictions have been placed on joining session keyrings across namespaces.

This still isn't sufficient to make them truly useful here. Intended future developments include: granting a permit to use a key to a container; adding per-container keyrings; request-key upcall namespacing.

I agree to abide by the anti-harassment policy

Yes

I confirm that I am already registered for LPC 2019

Primary author: Mr HOWELLS, David (Red Hat)

Presenter: Mr HOWELLS, David (Red Hat)

Session Classification: Containers and Checkpoint/Restore MC