



Contribution ID: 70

Type: **not specified**

User namespaces with host-isolated UID/GIDs

Monday, 13 November 2023 15:00 (30 minutes)

This talk aims to move forward the discussion about an extension of user namespaces that allows the usage of host-isolated (non-mapped) UID/GID. This topic was raised by Stéphane Graber and Christian Brauner originally in [1] and [2]. Stéphane and I would like to share some new results and discuss difficulties with the Linux kernel community.

Some highlights:

- extension of kuid_t/kgid_t to 64-bit wide
- VFS permission model for unmapped UID/GIDs

[1] Isolated dynamic user namespaces <https://lpc.events/event/7/contributions/836/>

[2] Simplified user namespace allocation <https://lpc.events/event/11/contributions/982/>

Primary authors: MIKHALITSYN, Aleksandr; GRABER, Stéphane (Canonical Ltd.)

Presenters: MIKHALITSYN, Aleksandr; GRABER, Stéphane (Canonical Ltd.)

Session Classification: Containers and checkpoint/restore MC

Track Classification: LPC Microconference: Containers and checkpoint/restore MC