Unprivileged singularity

Dave Dykstra

WLCG Containers WG Meeting

3 July 2019

Proposal for unprivileged singularity

- Goal: convert as much as possible of WLCG to unprivileged singularity
  - Preferably running out of cvmfs instead of rpm for easier upgrades
- My suggested plan:
  - Make baseline be new singularity version with unprivileged read-only bind-mount fix
  - Convert VOs that are using singularity in production to try running singularity out of cvmfs at least if not found in $PATH
    - CMS probably already has this if they have upgraded GlideinWMS lately
  - Announcement from security teams to enable unprivileged namespaces and encourage removing singularity rpm (preferably) or set ‘allow setuid = no’