State of AppArmor

2017 Linux Security Summit

Presentation by
John Johansen
john.johansen@canonical.com
www.canonical.com
September 2017

CANONICAL

Finally

Upstreaming!

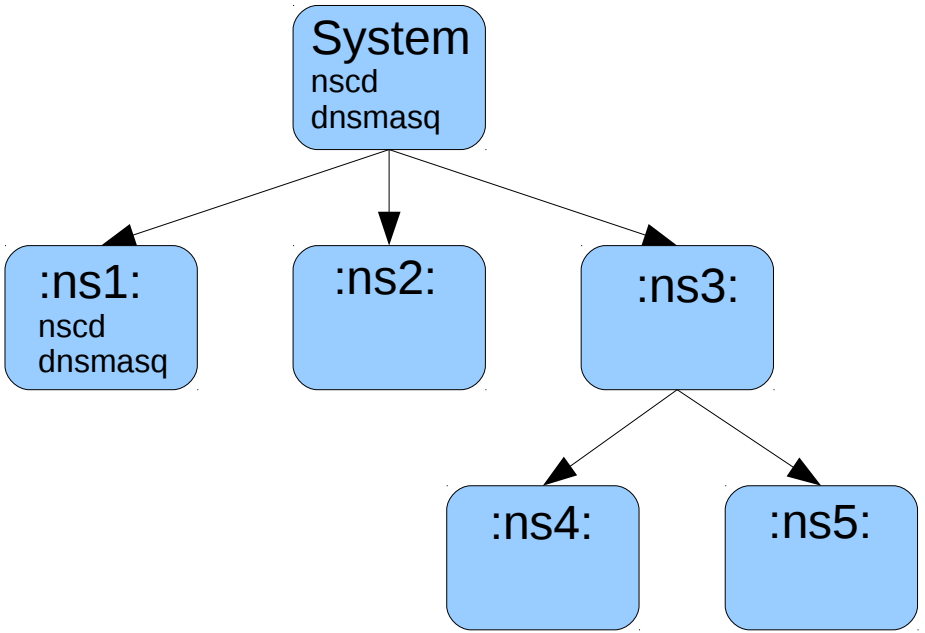
Except Full Networking

- Upstream basic AF socket controls (4.14)

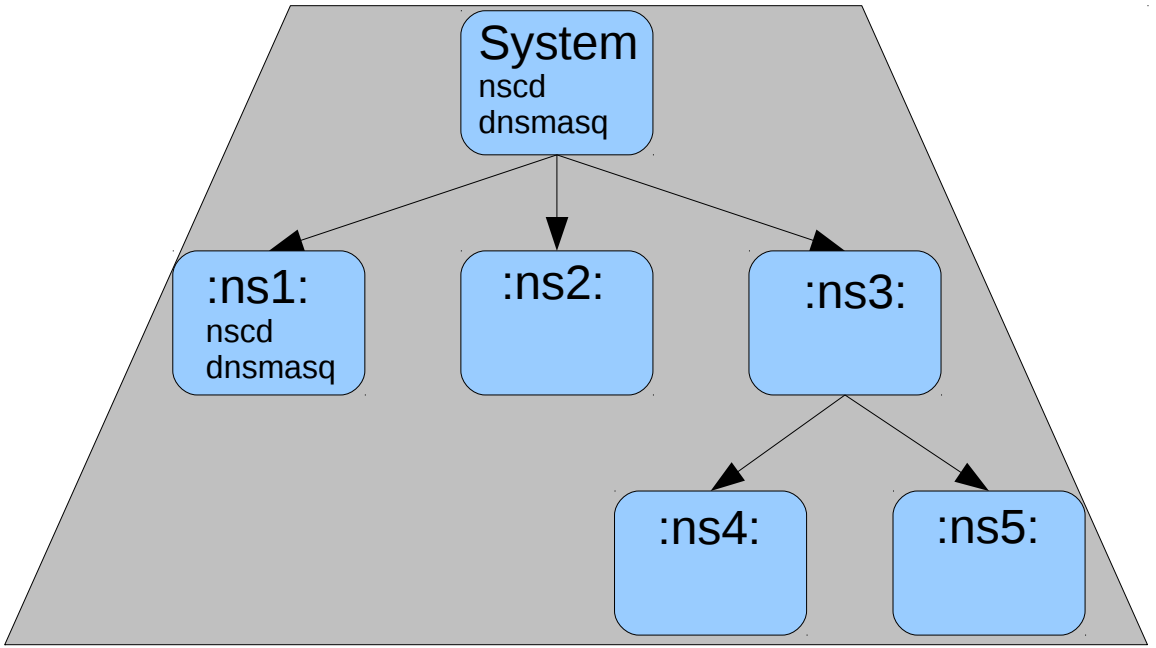
  network inet,

  network packet,
- Full network controls (WIP)
  - Needs to work with apparmor stacking
  - Internal type splitting (required by: AF_UNIX, dbus, ...)
  - SECIDS
    - Map to dynamic policy
    - Support stacking
  - Secmark, userspace (iptable rule) view can be different from that of the stack

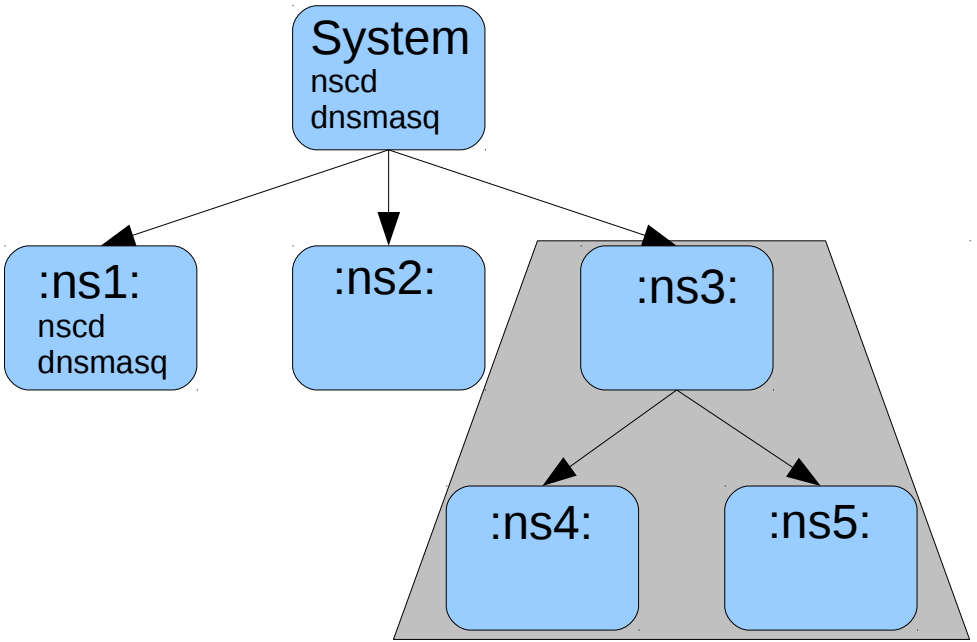
Policy Namespaces & Stacking



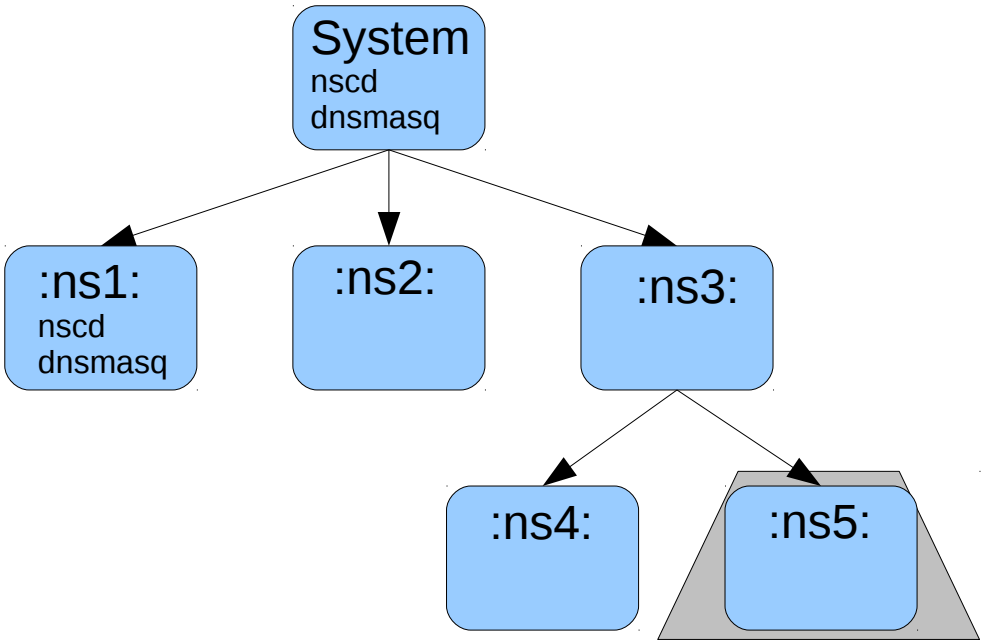
Policy Namespaces & Stacking



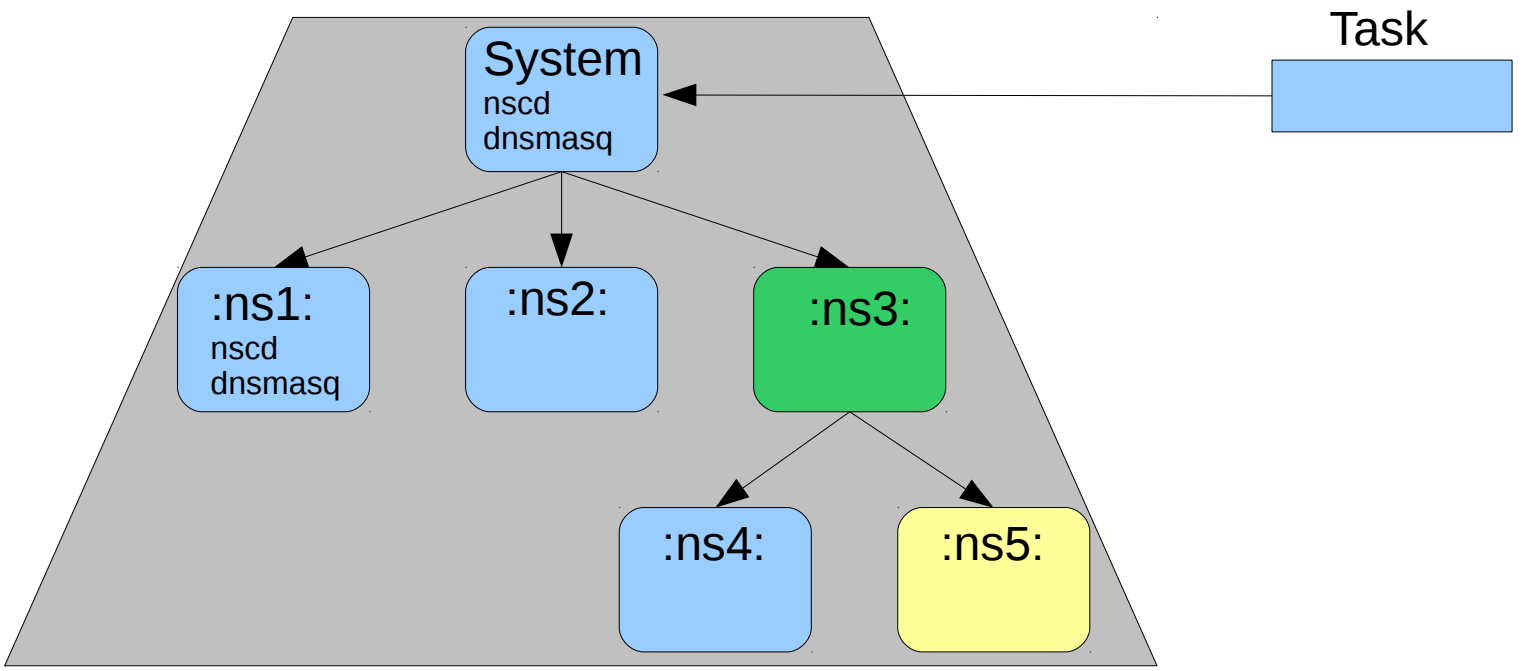
Policy Namespaces & Stacking



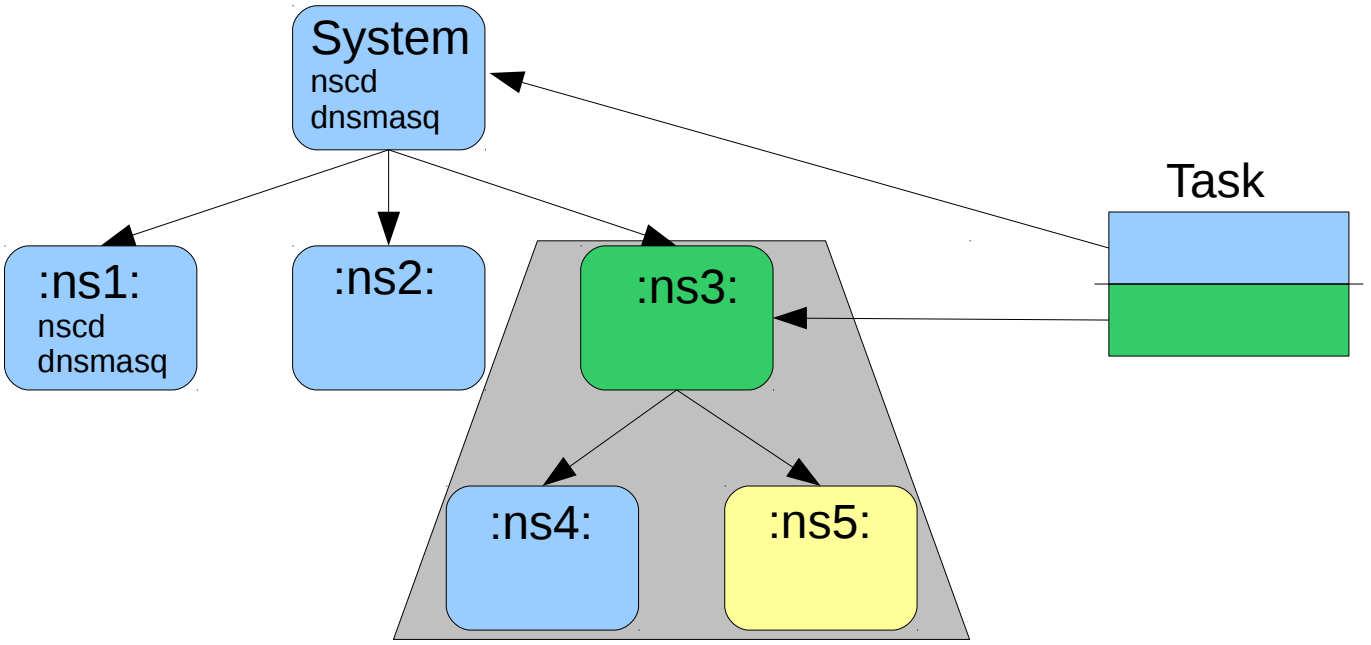
Policy Namespaces & Stacking



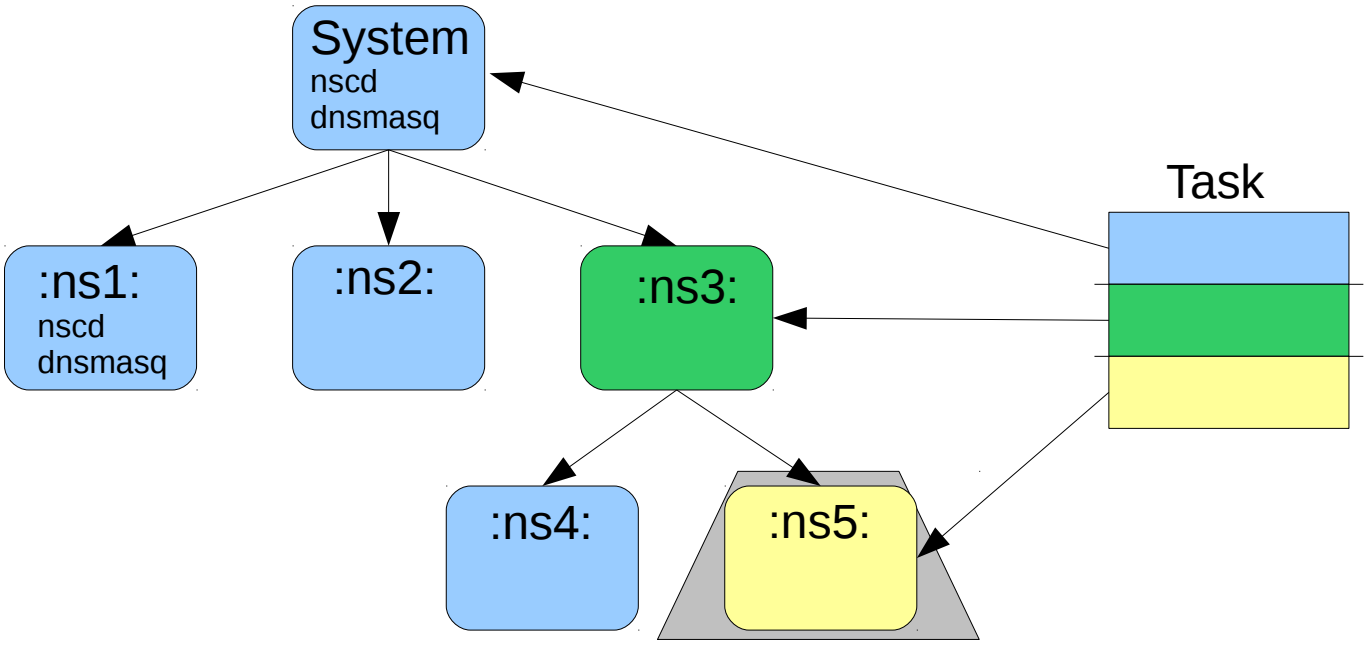
Policy Namespaces & Stacking



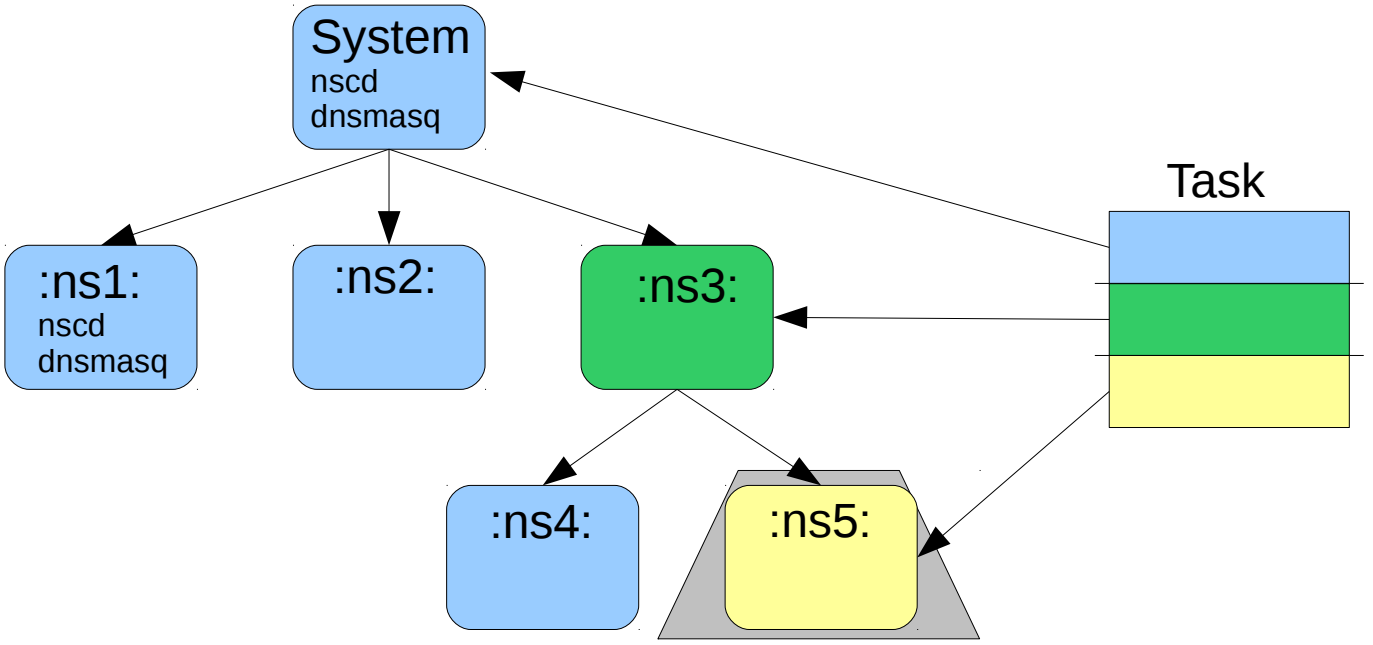
Policy Namespaces & Stacking



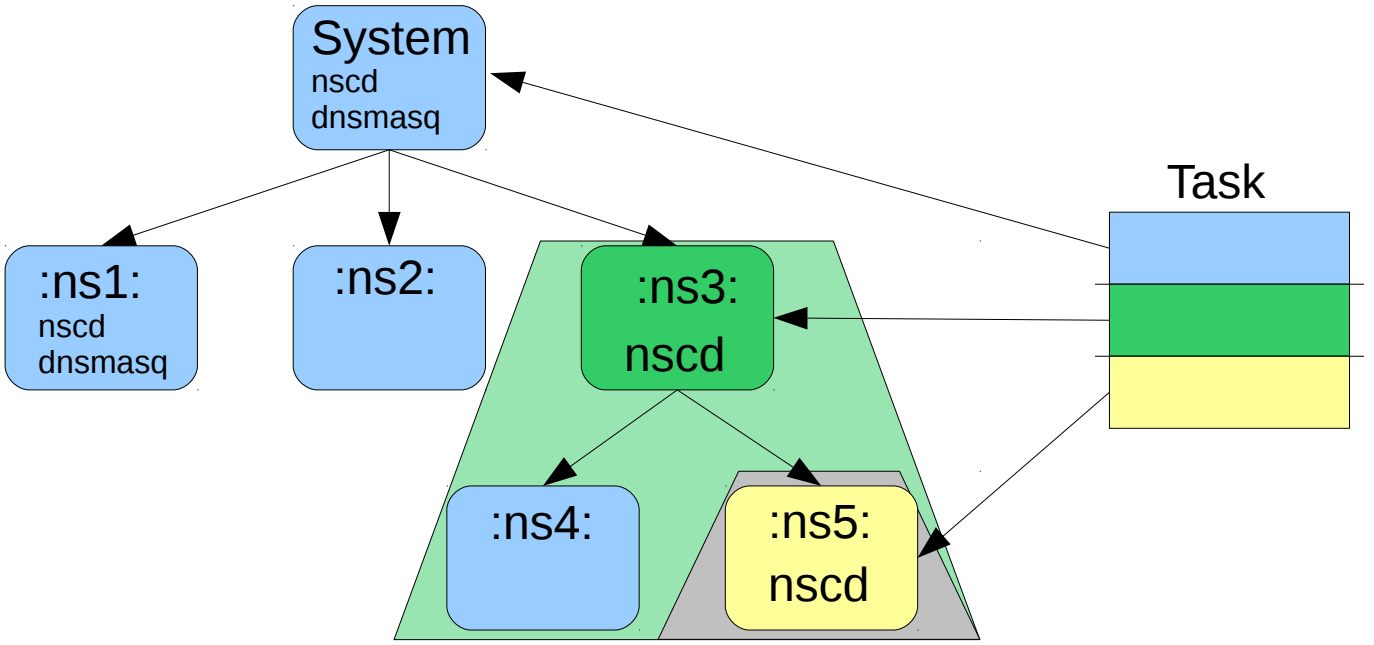
Policy Namespaces & Stacking



- View
- Scope
- Admin

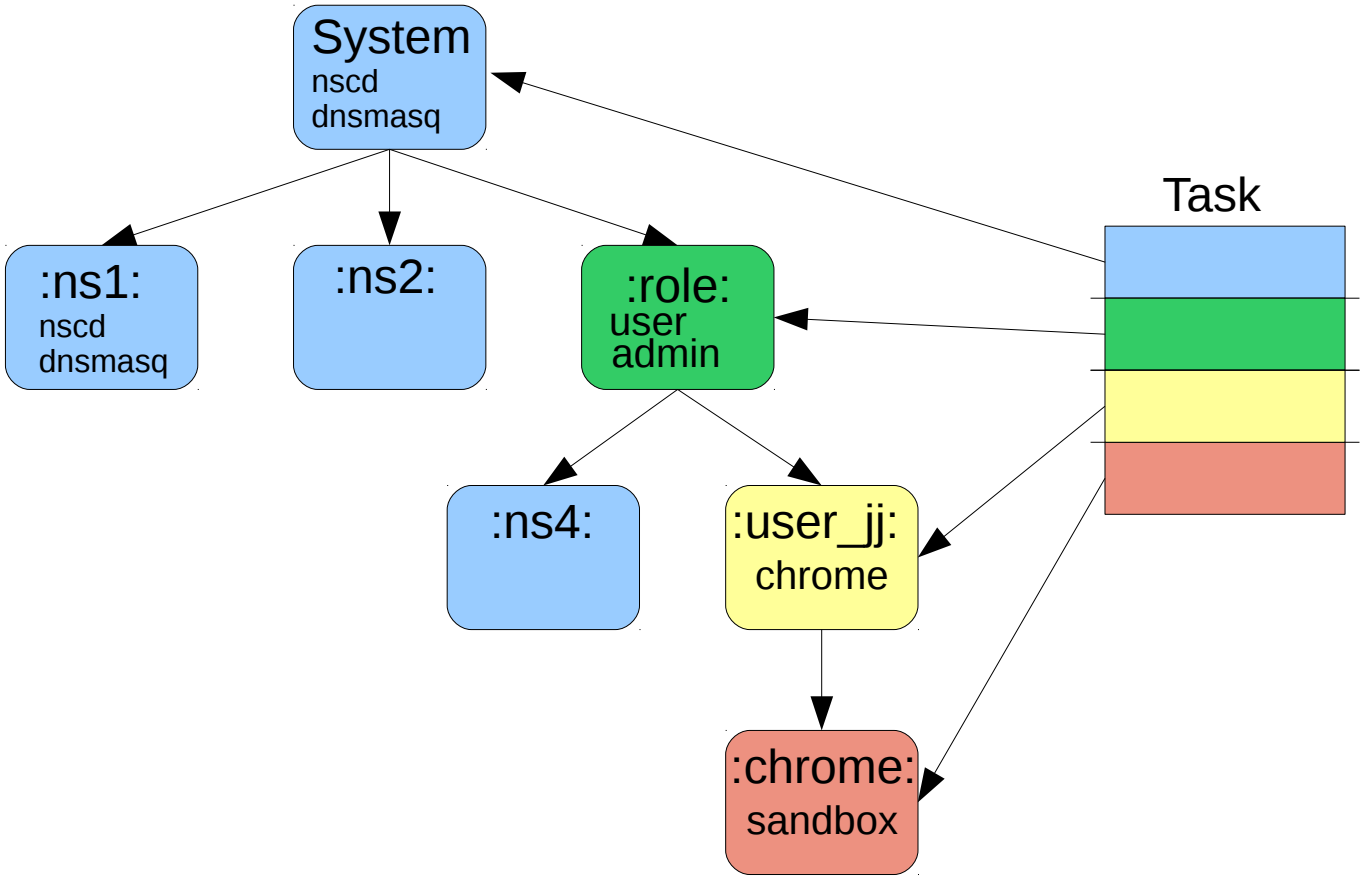


- View
- Scope
- Admin



User sees: nscd :ns5:nscd

Not just about LSM stacking or Containers



Stacking & Policy Namespaces

- Control policy namespace Scope and View (not yet)
  - Open up namespaces to other uses than containers
    - Sort of apparmor version of MCS
    - Roles
    - Unprivileged user defined policy
    - Application defined policy
- Virtualized apparmorfs policy/ directory (4.13)
- Create/destroy policy namespaces with mkdir/rmdir (4.13)
- Before opening up to more user
  - Finish virtualization of interfaces
  - Ownership of unprivileged policy namespaces
  - Resource controls on policy
  - Reaping of policy

Stacking & Namespacing - Issues

- Currently policy namespaces in conjunction with user namespaces
  - Restriction: single level of nesting
- Partially revive Lukasz Pawelczyk smack namespaces patch
  - Allows labeling user namespace
  - Extend with extra hooks to allow LSM to update state
  - New policy namespace for every user namespace?
    - Not 1-to-1 mapping. AppArmor policy namespaces have other uses
- LSM/security namespacing integration
  - Standardized interface to request new namespace?
- LSM Stacking integration
  - How/where does the apparmor stack integrate?
- SECIDs and networking (stacking)

Other Kernel Changes

- Check point/restore support
  - compression of policy to reduce size
- Improvements to the Query interface
  - Speed
  - multiple queries
  - Different types of queries (permissions, data, ...)
- Moving state machine from DFA → HFA
  - More flexible (dynamic variables, backreferences, counting constraints)
  - Smaller policy (choke points on DFA state explosion)
  - Still bounded, and verifiable in userspace
- Moving away from /proc/<pid>/attr/ interfaces
  - LSM stacking

Misc

- Userspace 2.11 release, 4.0 release this fall
- Documentation of stacking and policy namespaces
- User space utils cleanup
- Under the hood compiler improvements – parallel compiles (2.11)
- Policy versioning
- Work towards using new interfaces over /proc when available
- And Lots of bug fixing, and revision of …

Backlog

Backlog

- Complete the model
  - Delegation
  - security.apparmor xattr support
- Better LXD/snappy integration
- Better systemd integration
- Ioctl white listing
- Overlayfs support
- Extended permissions
- Kernel conditionals
- Environment filtering
- Performance improvements
- Learning mode improvements
- Bring-up mode improvements
- Tool improvements
- ...

Questions please
Thank you

John Johansen
john.johansen@canonical.com
www.canonical.com