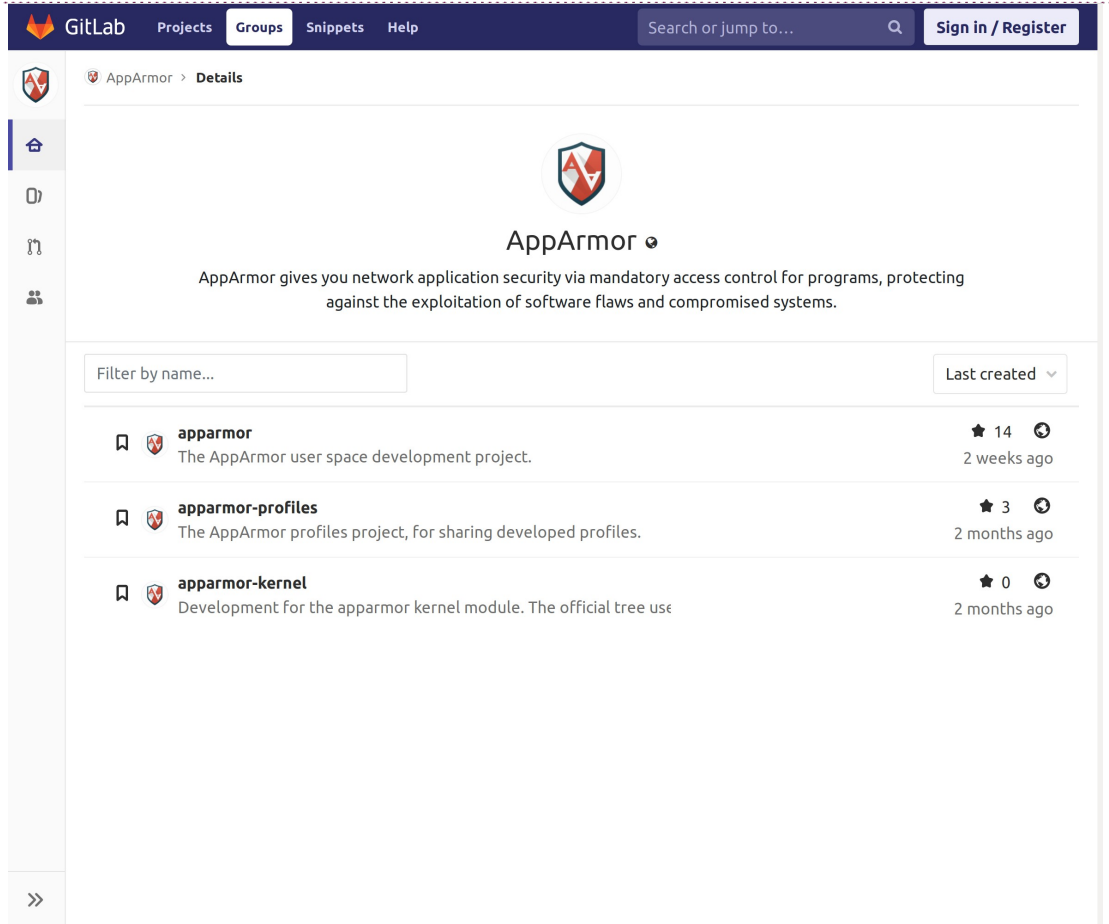
Overview and Recent Developments AppArmor

2018 Linux Security Summit – Europe

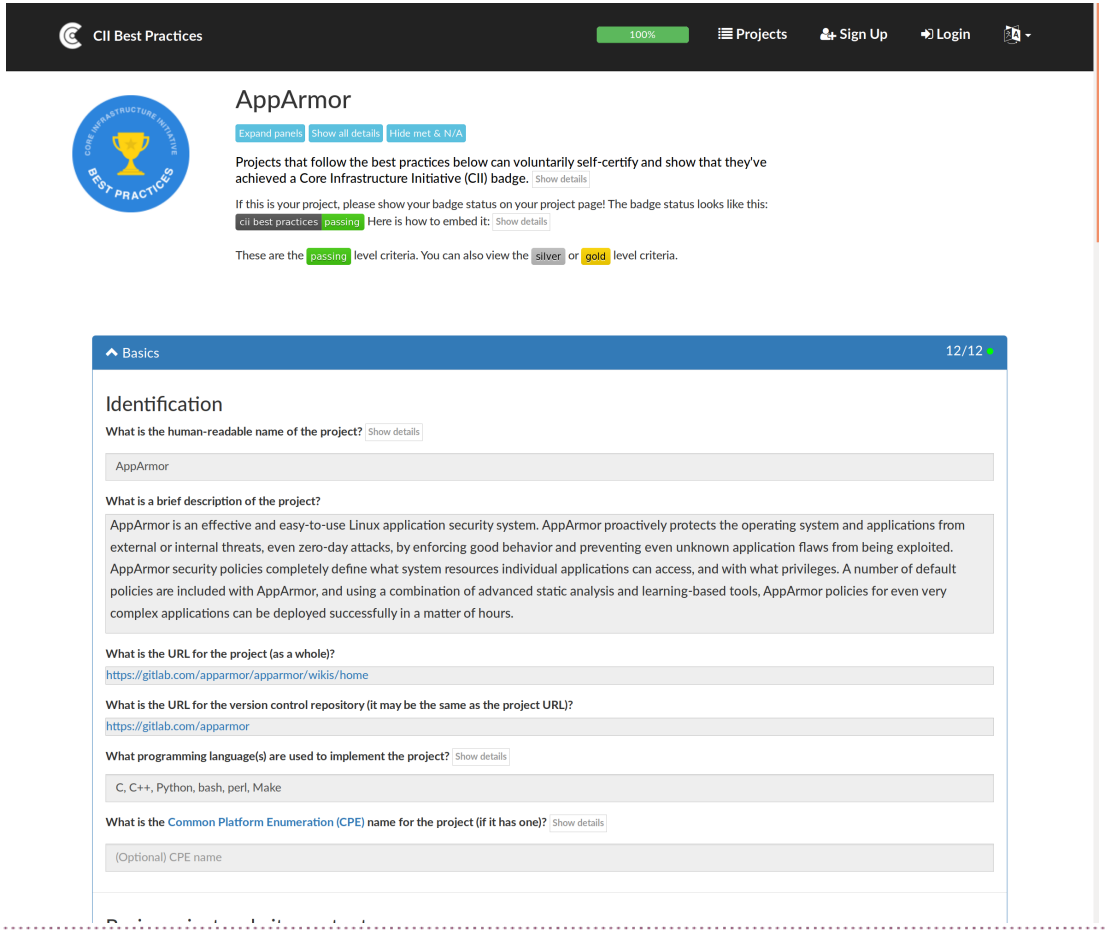
Presentation by
John Johansen
john.johansen@canonical.com
www.canonical.com
October 2018

CANONICAL

Now hosted on gitlab



CII Best Practices



CANONICAL

Overview

A Modified Domain Type Enforcement (DTE)

A Modified Domain Type Enforcement (DTE)

+

Capability System*

AppArmor Design

- Start with a target policy
  - Make it easy to confine applications
  - Controlled sharing
    - Allow sandboxes to be built on top
  - Allow confining more than just applications
- The user is the biggest problem
  - Try to make it easy to use
    - Let tooling do the work
  - Get out of the way of admin or any improvements will get turned off
    - Unconfined
- Work towards supporting strict confinement

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

Profile – attachment specification

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
             interface=org.freedesktop.Upower
             member="{Device,}Changed",
        ...
}
```

Profile – flags that modify behavior

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

Profile – rule block

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
             interface=org.freedesktop.Upower
             member="{Device,}Changed",
        ...
}
```

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
             interface=org.freedesktop.Upower
             member="{Device,}Changed",
        ...
}
```

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        allow dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

```
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
        include <abstractions/audio>
        include <abstractions/cups-client>
        include <abstractions/dbus-strict>
        include <abstractions/dbus-session-strict>

        allow file r /etc/firefox*/,
        allow file r /etc/firefox*/**,
        allow ixr /usr/bin/basename,

        dbus bus=system path="/org/freedesktop/UPower"
                interface=org.freedesktop.Upower
                member="{Device,}Changed",
        ...
}
```

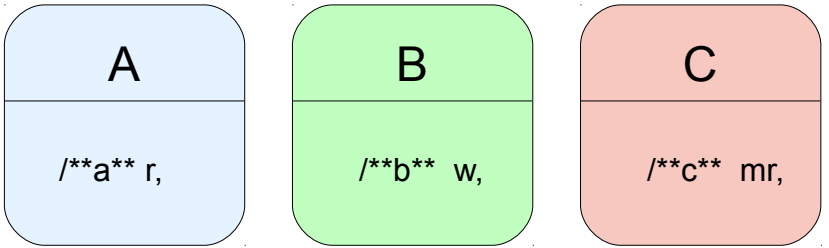
Policy

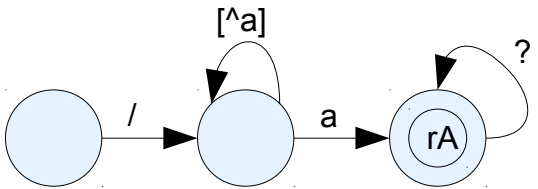
```
profile ping /{usr/,}bin/ping {
  #include <abstractions/base>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>

  capability net_raw,
  capability setuid,
  network inet raw,
  network inet6 raw,

  /{,usr/}bin/ping mixr,
  /etc/modules.conf r,

  ...
```

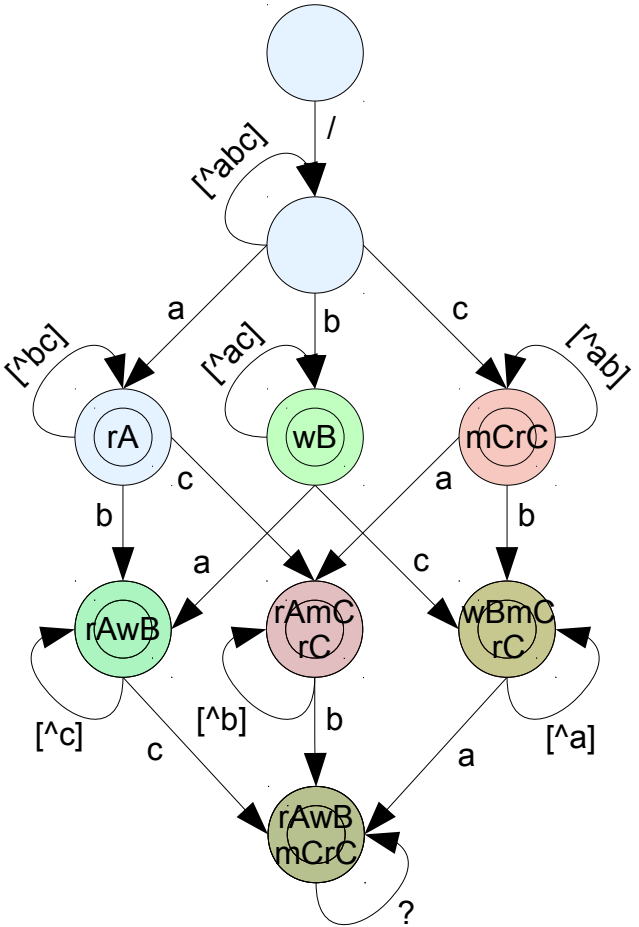
```
/sbin/dhclient  {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/openssl>

  capability net_bind_service,
  capability net_raw,
  capability dac_override,
  capability net_admin,

  network packet,
  network raw,

  @{PROC}/[0-9]*/net/ r,
  @{PROC}/[0-9]*/net/** r,

  /sbin/dhclient mr,


  ...
```

```
profile syslogd /{usr/,}sbin/syslogd  {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/consoles>

  capability sys_tty_config,
  capability dac_override,
  capability dac_read_search,
  capability setuid,
  capability setgid,
  capability syslog,

  /dev/log                    wl,
  /var/lib/*/dev/log          wl,


  ...
```

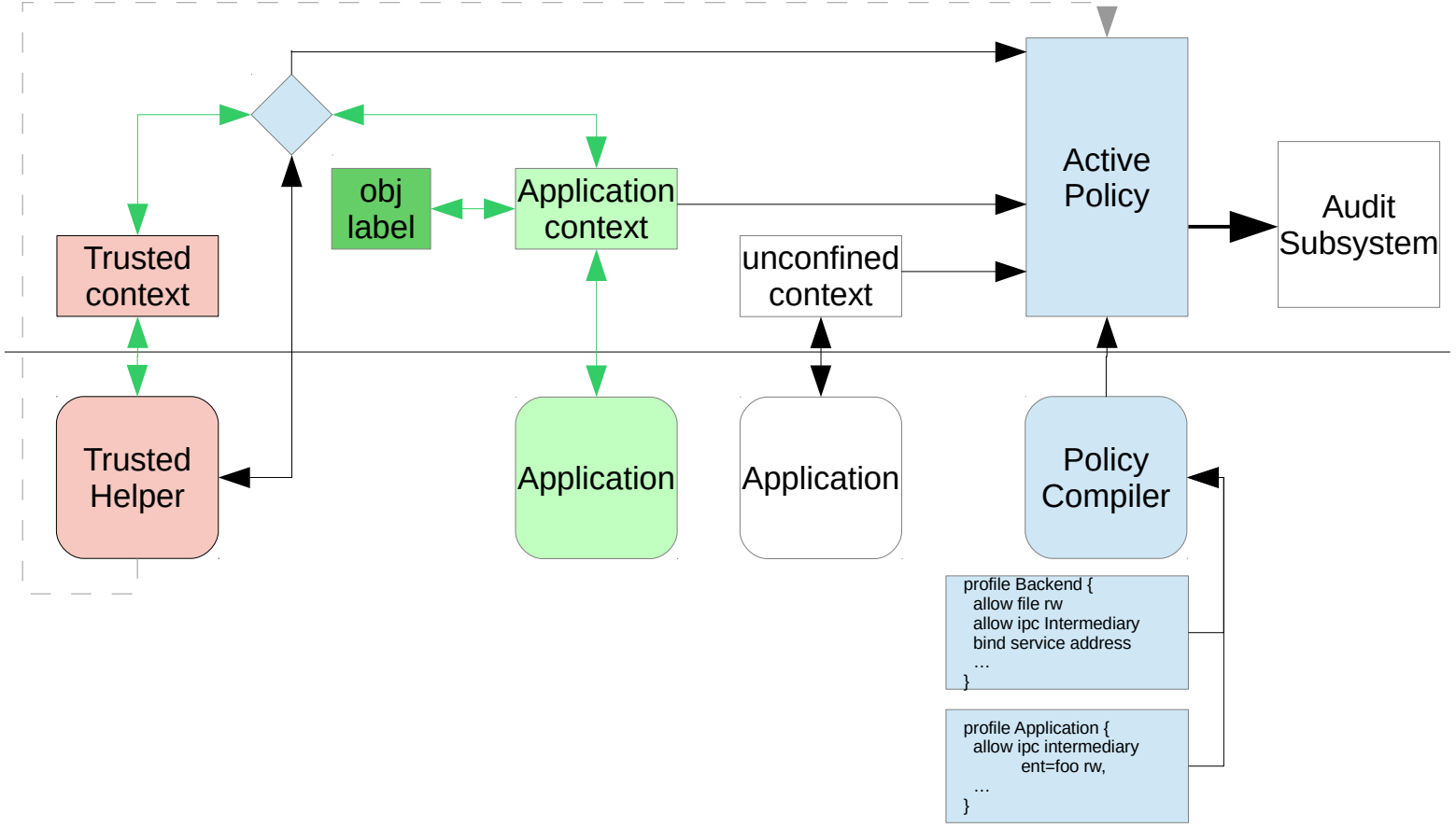
Handling Pattern matching







Basic Policy Summary



Policy Namespaces

Policy Namespaces

Namespace 1

/usr/sbin/libvirtd (enforce)
/usr/sbin/mdnsd (complain)
/usr/sbin/ippusbxd (enforce)
/usr/sbin/dovecot (complain)
/usr/lib/snapd/snap-confine (enforce)
/usr/lib/telepathy/telepathy-ofono (enforce)
/usr/lib/telepathy/telepathy-* (enforce)
/usr/lib/telepathy/mission-control-5 (enforce)
/usr/sbin/identd (complain)
/usr/sbin/cupsd (enforce)

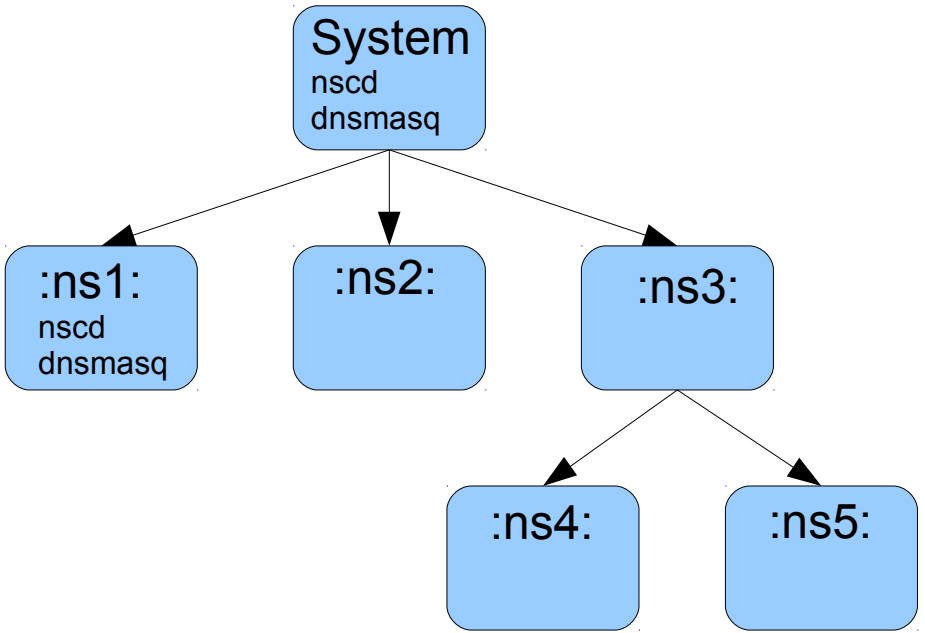
Namespace 2

/usr/sbin/libvirtd (enforce)
/usr/sbin/mdnsd (complain)
/usr/sbin/identd (complain)
/usr/sbin/cupsd (enforce)
firefox (enforce)
firefox//sanitized_helper (enforce)
firefox//lsb_release (enforce)
firefox//browser_openjdk (enforce)
firefox//browser_java (enforce)

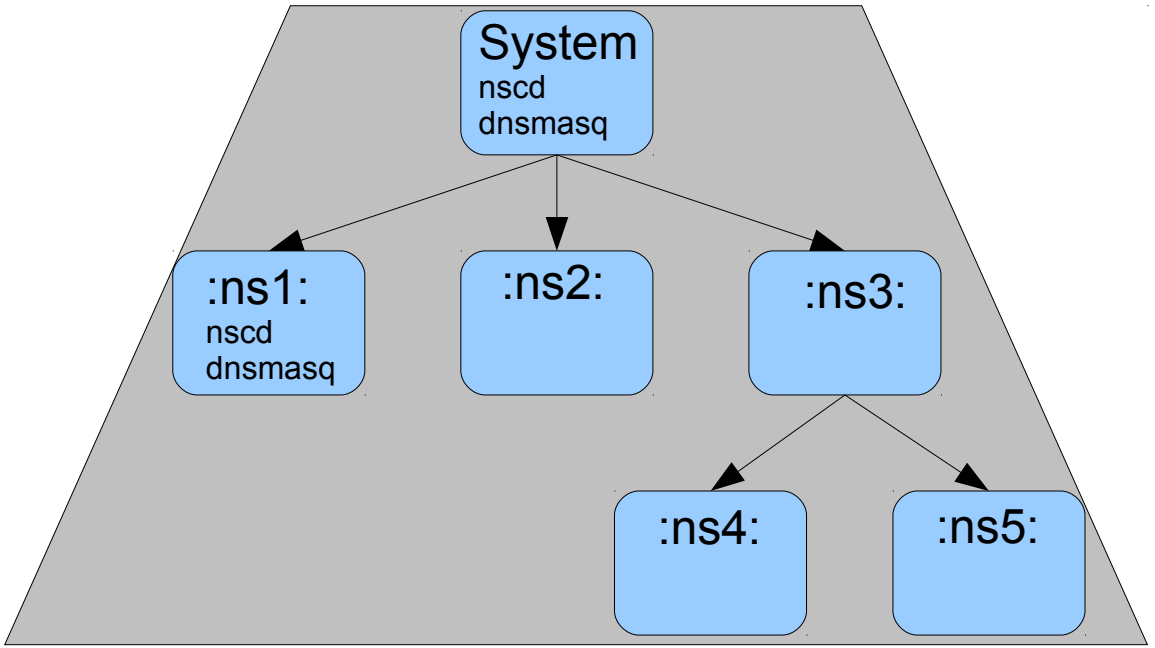
:ns:profile

:ns://profile

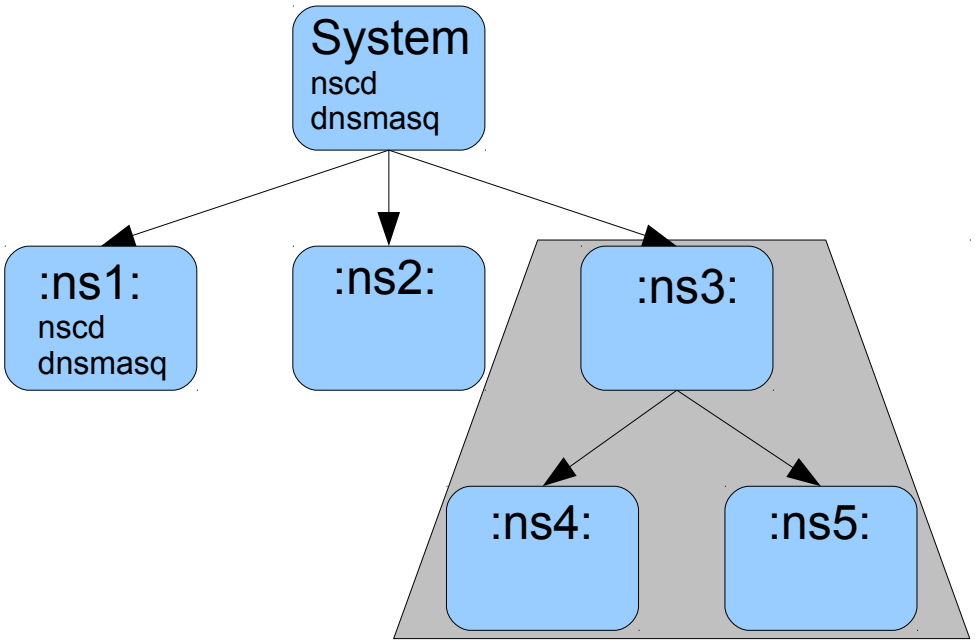
Policy Namespaces - Hierarchical



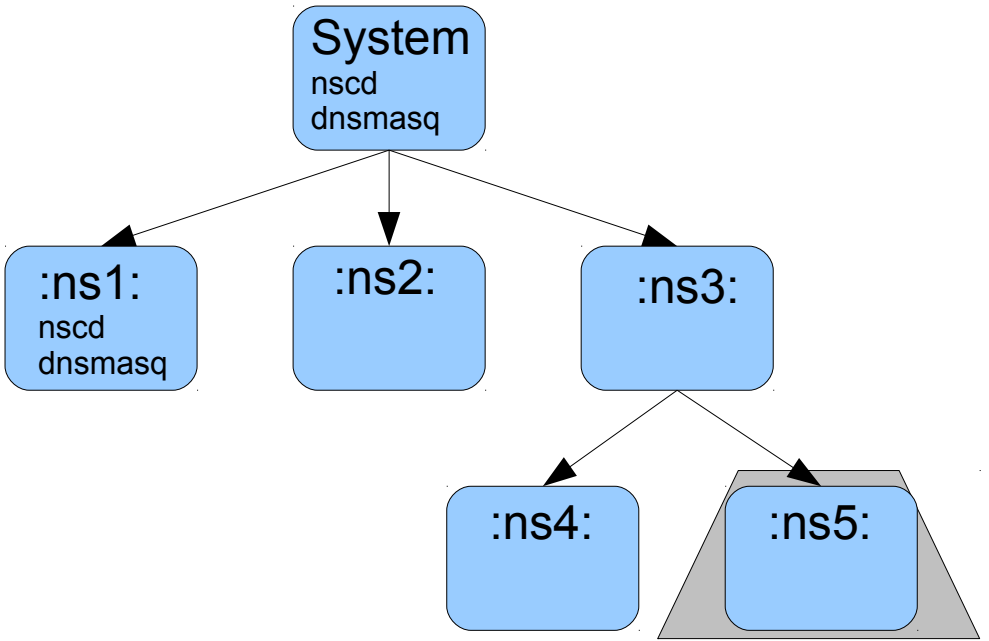
Policy Namespace - View



Policy Namespaces – Child NS View

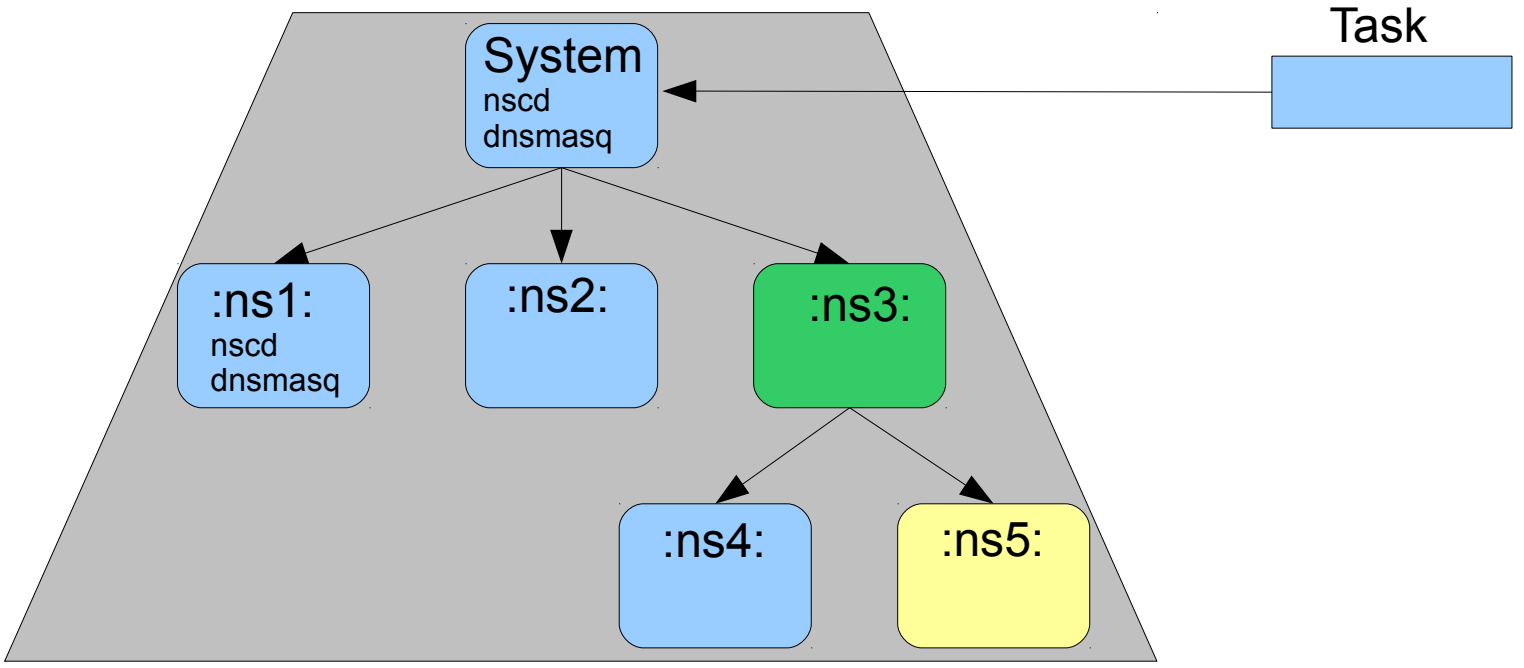


Policy Namespaces – Grand Child NS View

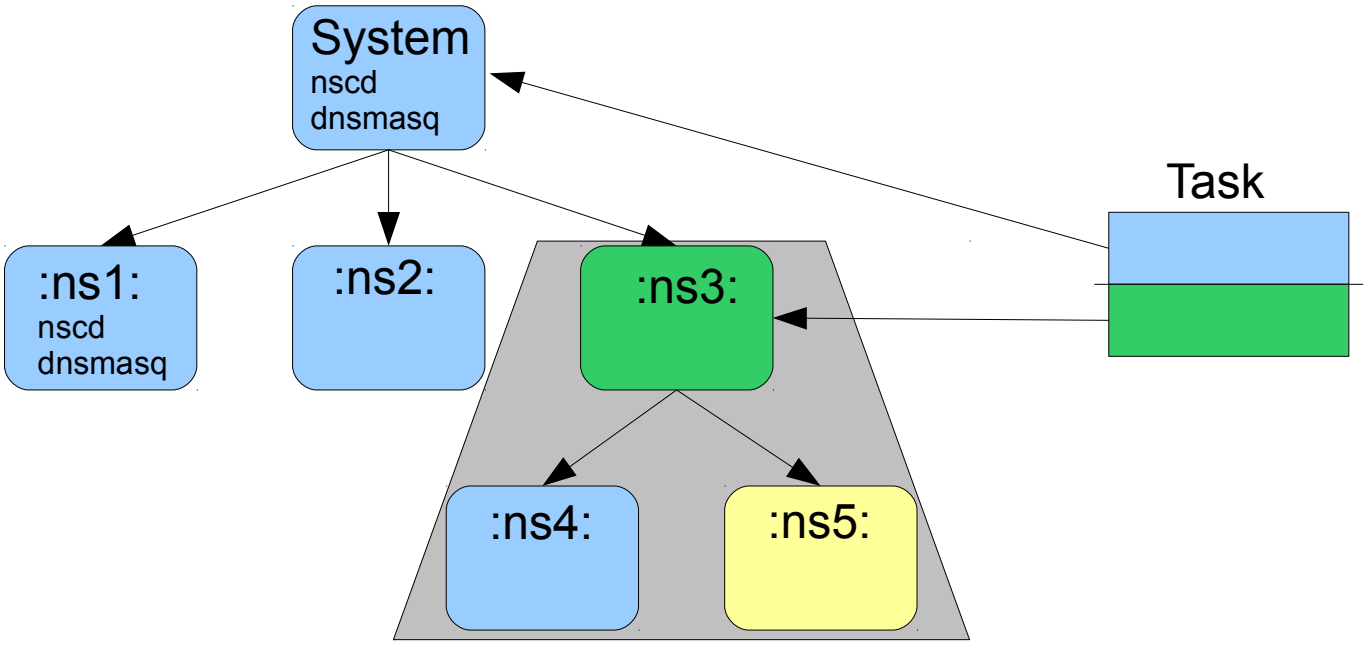


Policy Stacking
&
Dynamic Policy

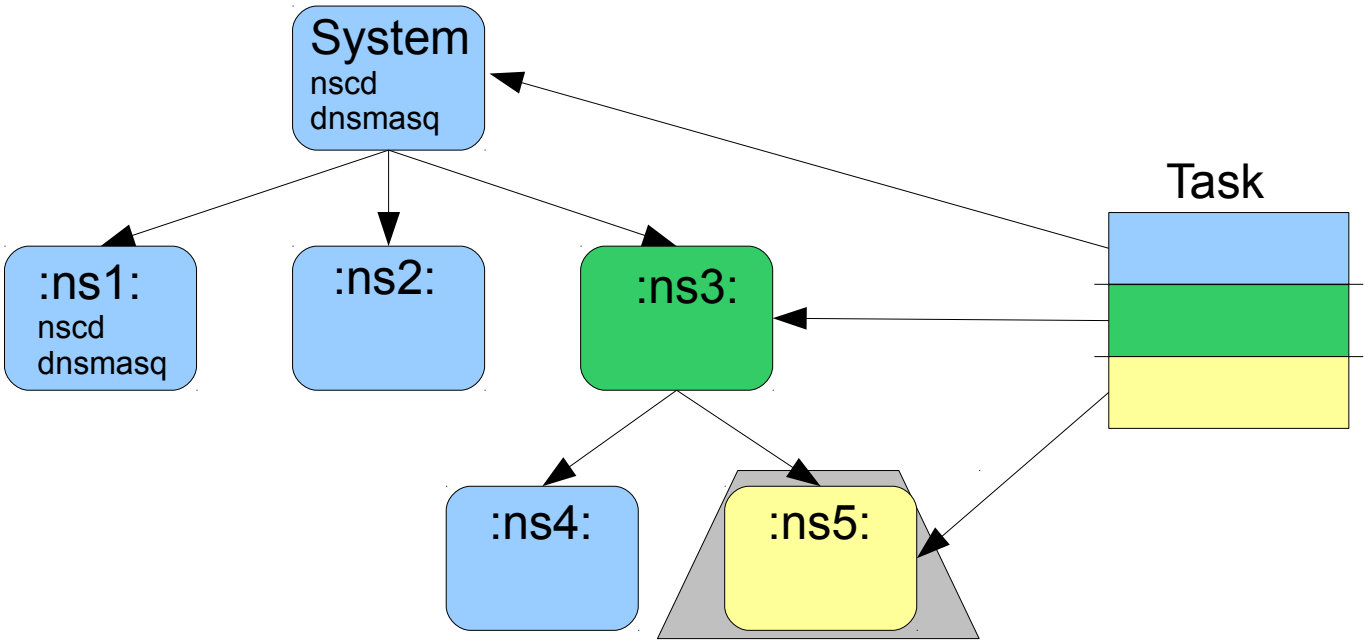
Stacking - System View



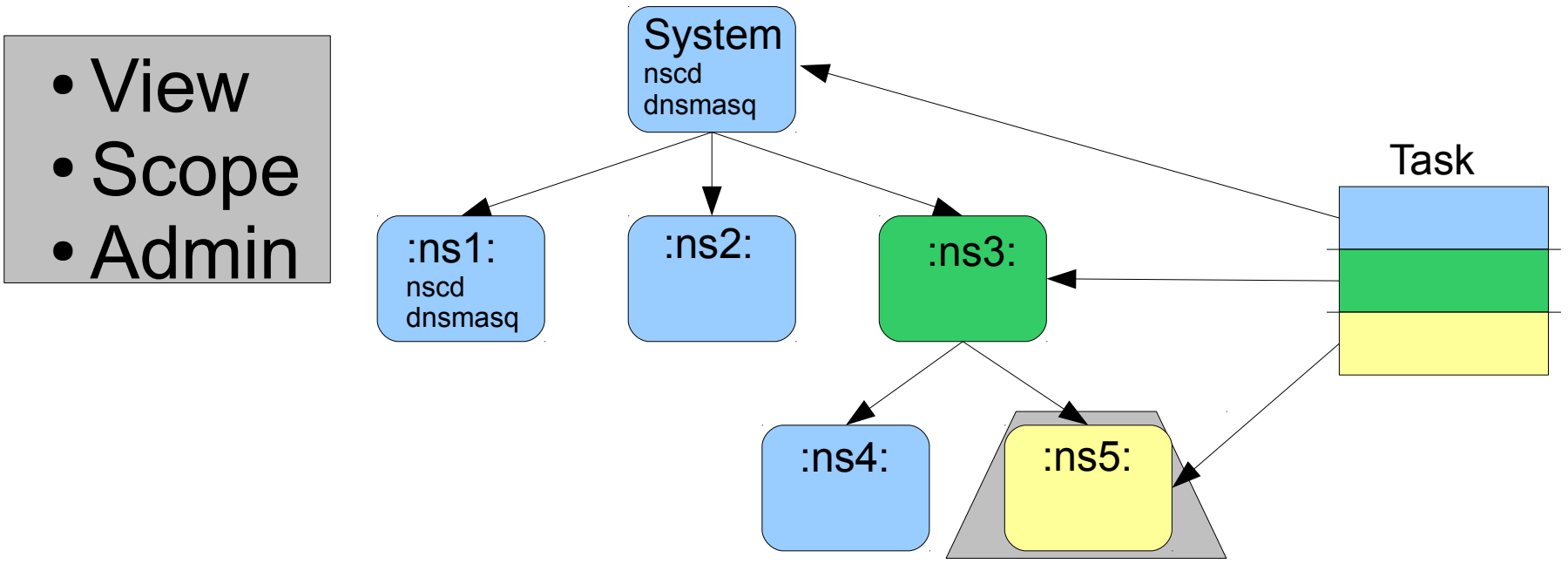
Stacking Across Policy NS can Reduce View



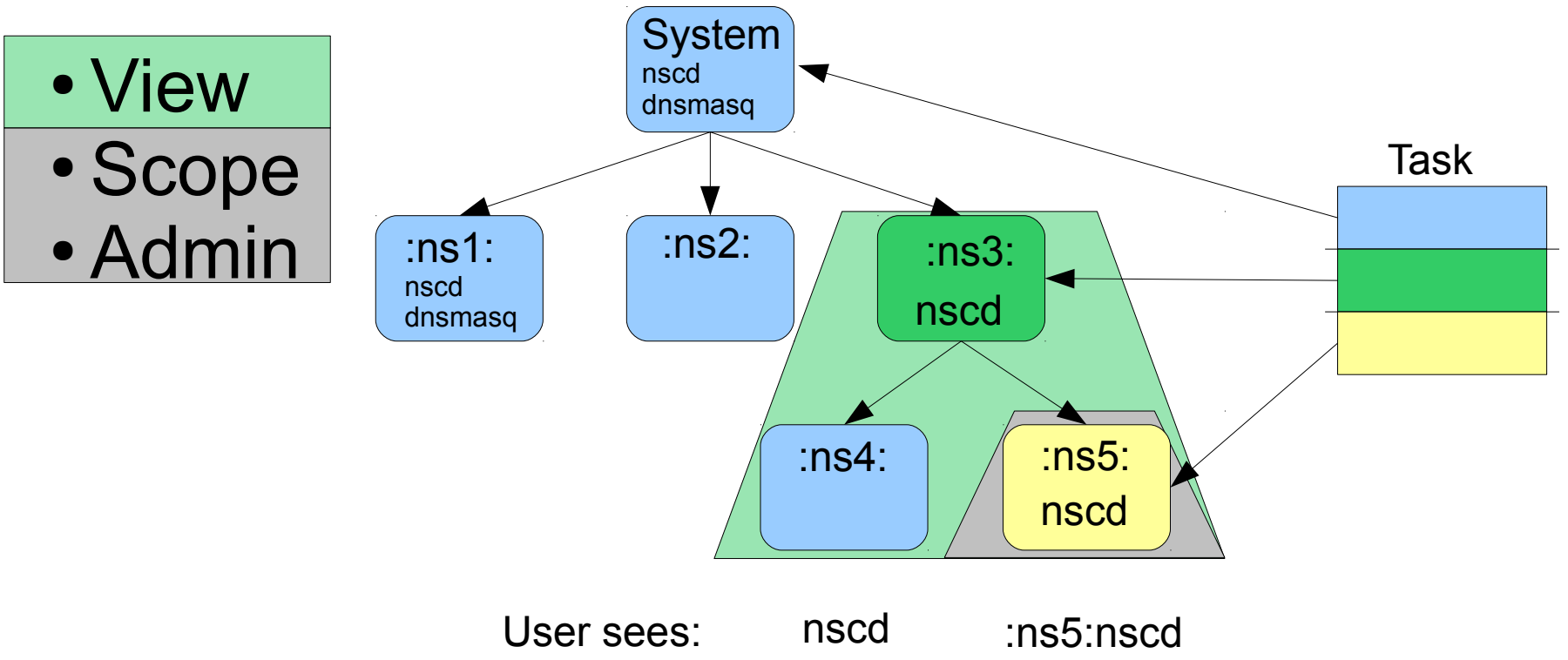
Stacking – Further Reduced View



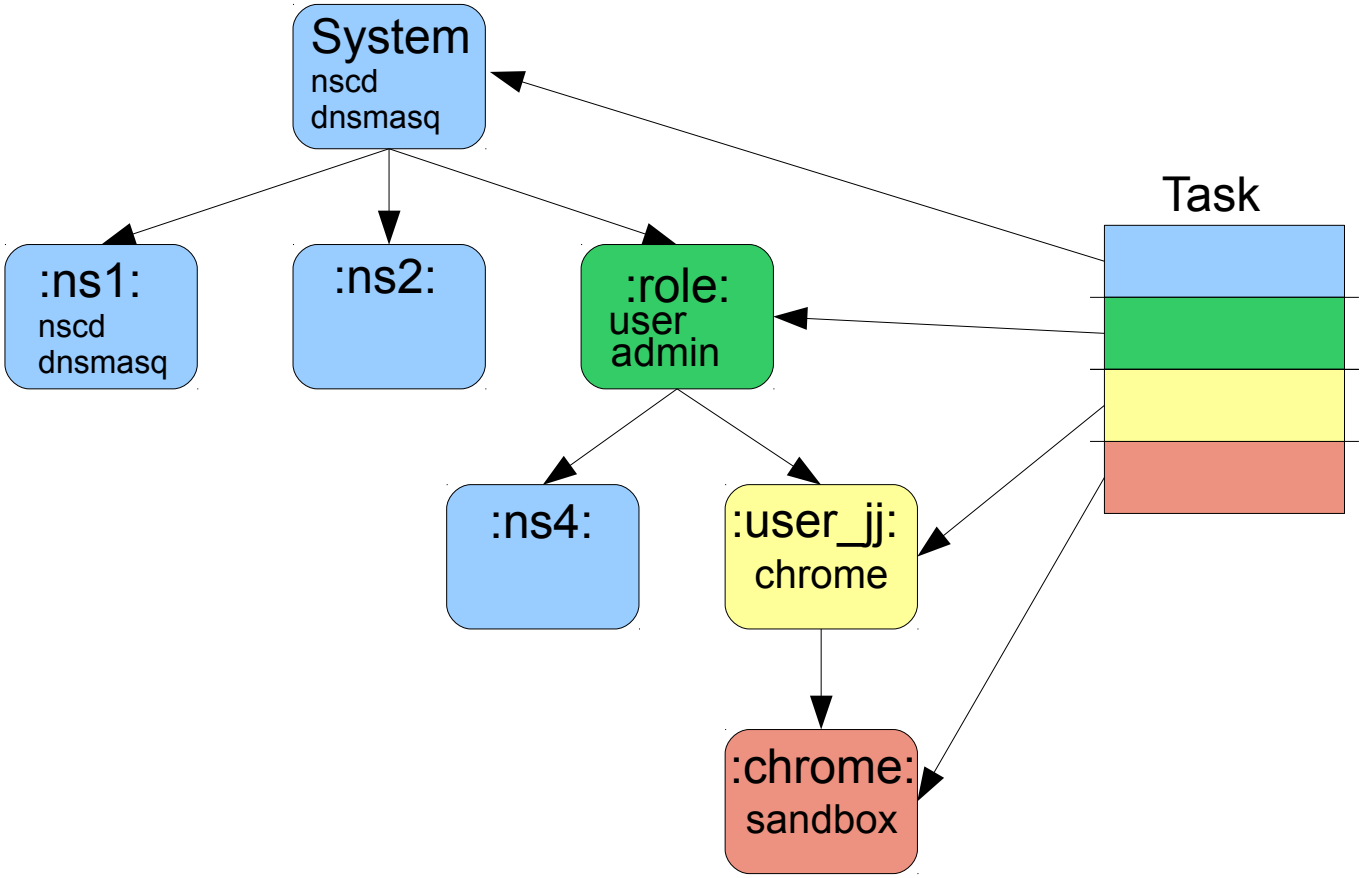
Policy NS & Stacking – Scope & View



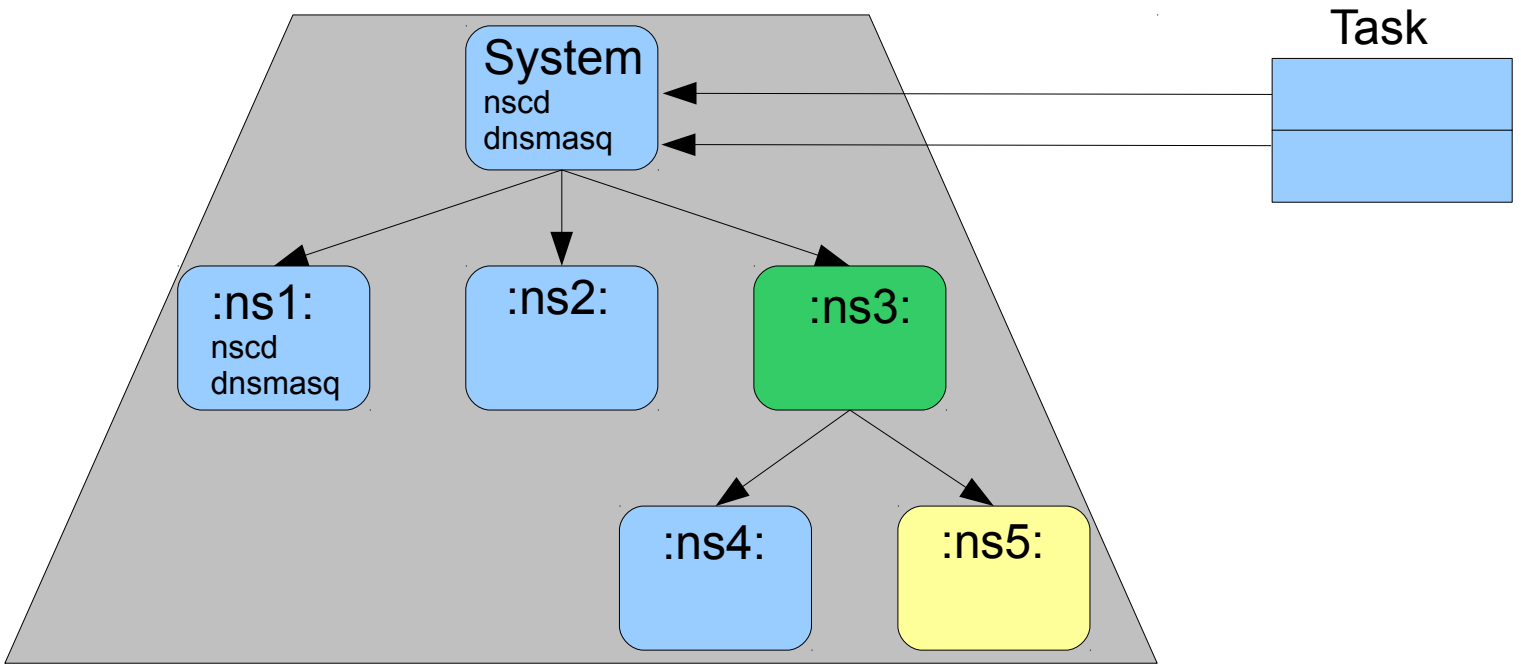
Policy NS & Stacking – Scope & View* - NOT yet available



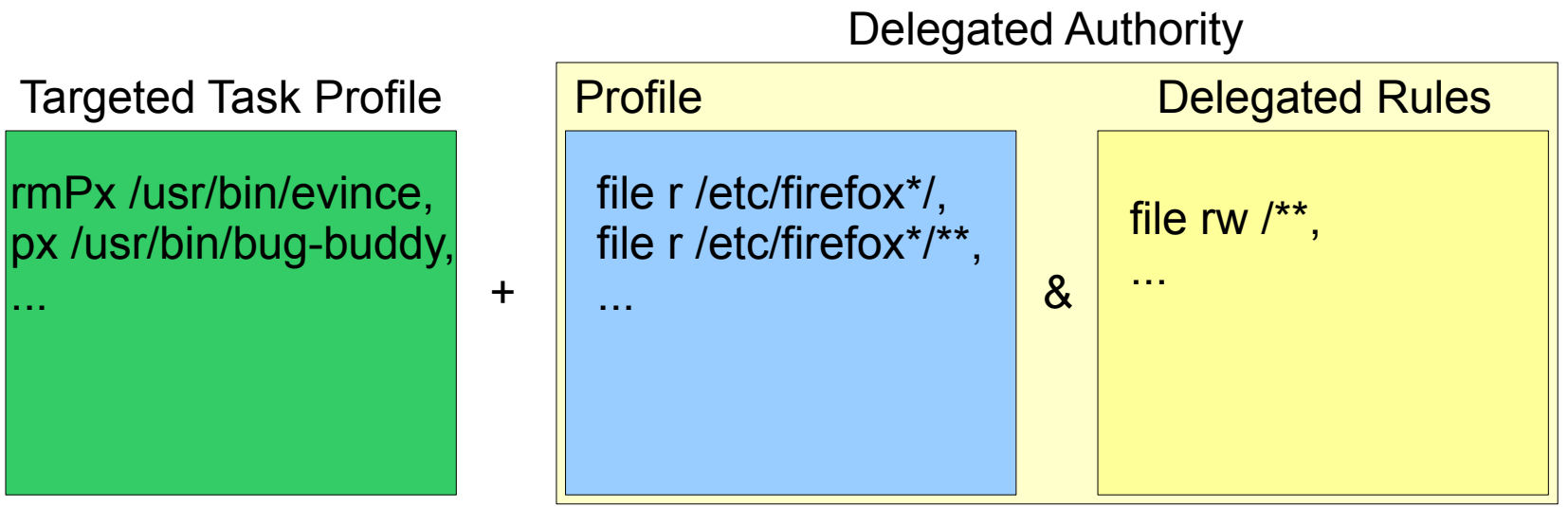
Application and User Defined Policy* - NOT yet available



Stacking – not just across namespaces



Delegation of Authority* - NOT yet available



firefox//&evince

Recent Developments

Everything except

af_unix

Upstreaming cont.

- Secids – 4.18
- audit rule filtering (SUBJ_ROLE) – 4.18
- socket mediation – 4.17
- Profile attachment – 4.17
  - EVM
  - Improved overlapping exec attachment resolution
  - nnp subset test

Policy tagged with ABI info

```
profile ping /{usr/,}bin/ping  {
    include <abstractions/base>
    include <abstractions/consoles>
    include <abstractions/nameservice>

    capability net_raw,
    capability setuid,
    network inet raw,
    network inet6 raw,

    file mixr /{,usr/}bin/ping,
    file r /etc/modules.conf,
```

Policy tagged with ABI info

```
abi=<features/upstream-4.18>

profile ping /{usr/,}bin/ping  {
    include <abstractions/base>
    include <abstractions/consoles>
    include <abstractions/nameservice>

    capability net_raw,
    capability setuid,
    network inet raw,
    network inet6 raw,

    file mixr /{,usr/}bin/ping,
    file r /etc/modules.conf,
```

Single Binary Policy Cache

/etc/apparmor.d/cache

bin.ping
sbin.klogd
sbin.syslogd
sbin.syslog-ng
skype
usr.bin.evince
usr.bin.firefox
usr.bin.pidgin
usr.sbin.cupsd
usr.sbin.dnsmasq
usr.sbin.dovecot
...

Per Kernel binary policy

$(location)/7f01cf2e.0

bin.ping
sbin.klogd
sbin.syslogd
sbin.syslog-ng
skype
usr.bin.evince
usr.bin.firefox
usr.bin.pidgin
usr.sbin.cupsd
usr.sbin.dnsmasq
usr.sbin.dovecot
...

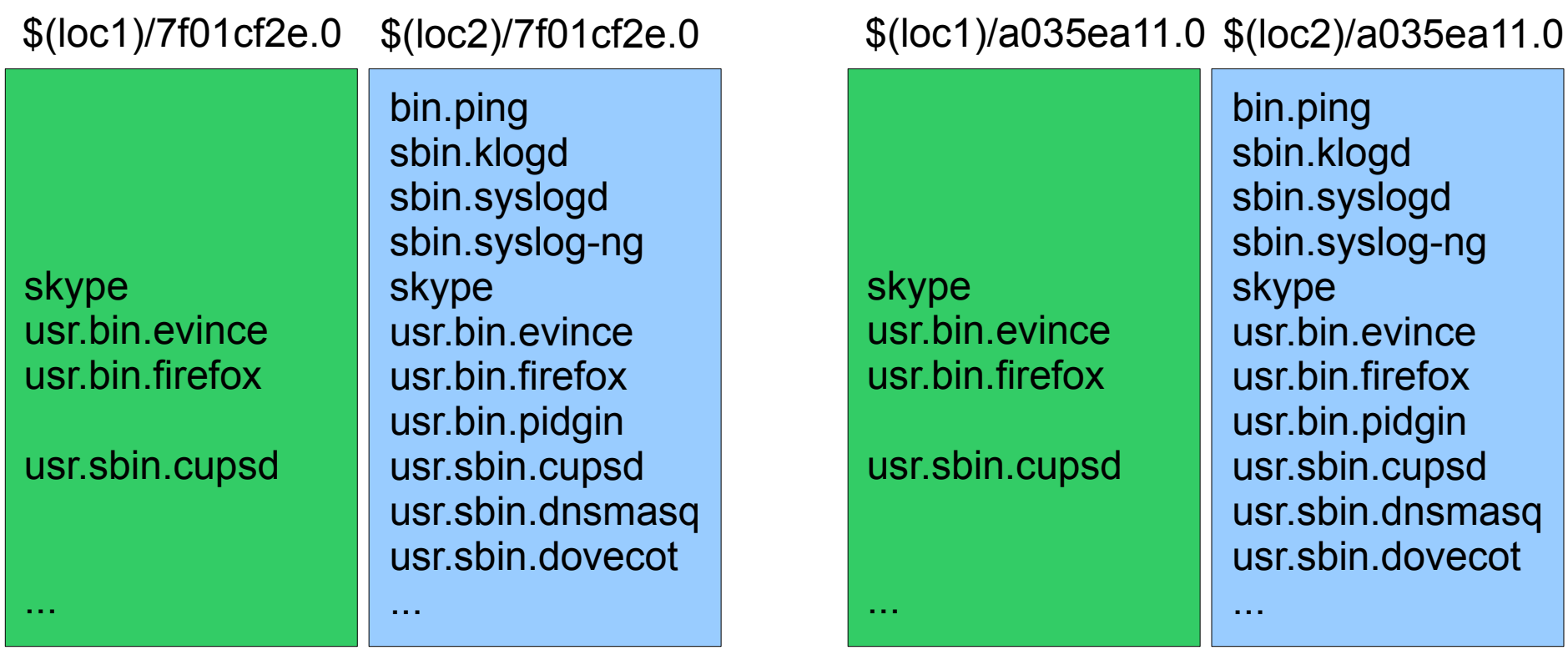
$(location)/cache/7f01cf2e.1

bin.ping
sbin.klogd
sbin.syslogd
sbin.syslog-ng
skype
usr.bin.evince
usr.bin.firefox
usr.bin.pidgin
usr.sbin.cupsd
usr.sbin.dnsmasq
usr.sbin.dovecot
...

$(location)/cache/a035ea11.0

bin.ping
sbin.klogd
sbin.syslogd
sbin.syslog-ng
skype
usr.bin.evince
usr.bin.firefox
usr.bin.pidgin
usr.sbin.cupsd
usr.sbin.dnsmasq
usr.sbin.dovecot
...

Binary Policy Overlay



WIP

Current WIP

- Internal cleanups and improvements
- Rework early policy loading
  - Systemd integration
  - Default profile
  - initrd/initramfs hooks
- Fine grained networking
  - af_unix
  - ipv4/ipv6
- Improved mount mediation
- Missing mediation
  - Keys mediation
  - ioctl mediation
  - ...

WIP continued

- Improvements to auditing
  - Get audit data off the stack
  - Caching and grouping
- Improvements to complain/learning
  - Caching of recently audited events
  - Direct to daemon logging
  - Daemon interaction, similar to the seccomp notify work
- Further attachment conditionals (user, …)
- Extended conditionals, and permissions
- Policy namespaces
  - Separate scope & view work
  - Open up policy to users and applications
- Delegation

WIP continued

- no_new_priv improvements
- pam_apparmor
- Interaction with system namespaces
- Documentation
-

Questions please
Thank you

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