



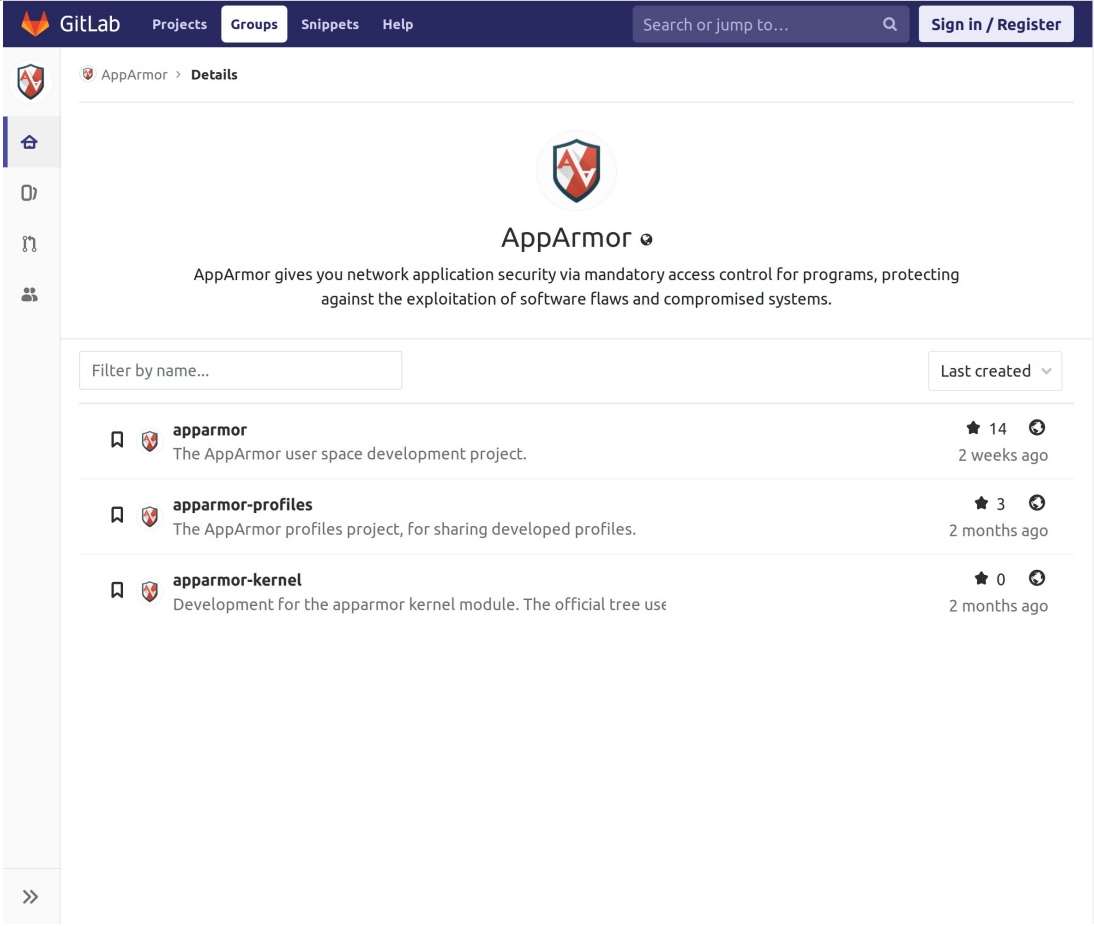
Overview and Recent Developments

AppArmor

2018 Linux Security Summit – Europe

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

Now hosted on gitlab



The screenshot shows the GitLab interface for the AppArmor group. The top navigation bar includes 'GitLab', 'Projects', 'Groups', 'Snippets', and 'Help'. A search bar and 'Sign in / Register' button are also present. The main content area displays the AppArmor logo and a description: 'AppArmor gives you network application security via mandatory access control for programs, protecting against the exploitation of software flaws and compromised systems.' Below this is a filter box and a dropdown menu set to 'Last created'. A list of three projects is shown:

Project Name	Description	Stars	Created
apparmor	The AppArmor user space development project.	14	2 weeks ago
apparmor-profiles	The AppArmor profiles project, for sharing developed profiles.	3	2 months ago
apparmor-kernel	Development for the apparmor kernel module. The official tree use	0	2 months ago



CII Best Practices 100% [Projects](#) [Sign Up](#) [Login](#)

AppArmor

[Expand panels](#) [Show all details](#) [Hide met & N/A](#)

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved a Core Infrastructure Initiative (CII) badge. [Show details](#)

If this is your project, please show your badge status on your project page! The badge status looks like this: [cii best practices: passing](#) Here is how to embed it: [Show details](#)

These are the [passing](#) level criteria. You can also view the [silver](#) or [gold](#) level criteria.

Basics 12/12

Identification

What is the human-readable name of the project? [Show details](#)

AppArmor

What is a brief description of the project?

AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing even unknown application flaws from being exploited. AppArmor security policies completely define what system resources individual applications can access, and with what privileges. A number of default policies are included with AppArmor, and using a combination of advanced static analysis and learning-based tools, AppArmor policies for even very complex applications can be deployed successfully in a matter of hours.

What is the URL for the project (as a whole)?

<https://gitlab.com/apparmor/apparmor/wikis/home>

What is the URL for the version control repository (it may be the same as the project URL)?

<https://gitlab.com/apparmor>

What programming language(s) are used to implement the project? [Show details](#)

C, C++, Python, bash, perl, Make

What is the Common Platform Enumeration (CPE) name for the project (if it has one)? [Show details](#)

(Optional) CPE name



Overview



A Modified Domain Type Enforcement (DTE)



A Modified Domain Type Enforcement (DTE)

+

Capability System*



- 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",  
    ...  
}
```



```
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",
```

```
    ...
```

```
}
```



```
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",
```

```
    ...
```

```
}
```



```
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,
```

```
  ...
```

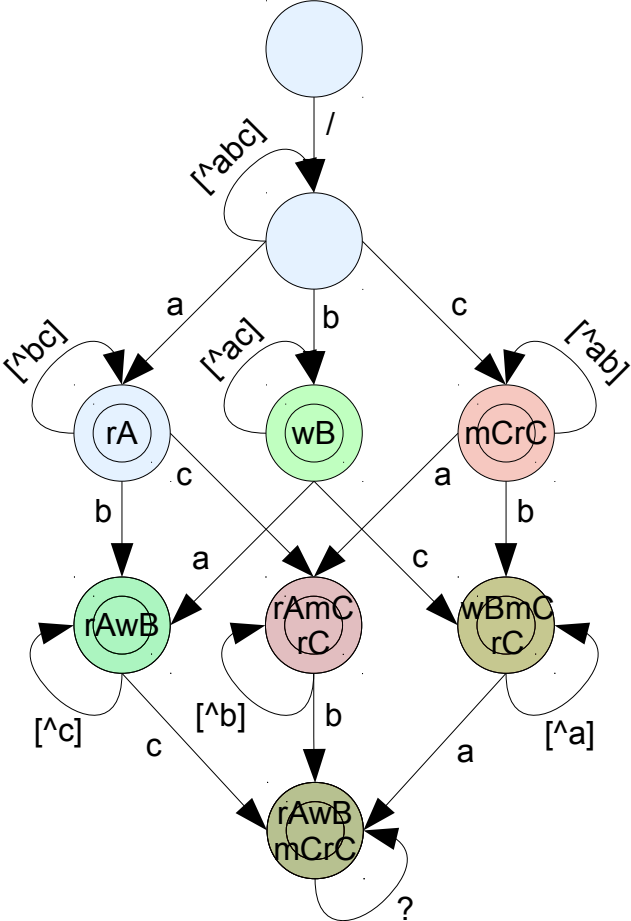
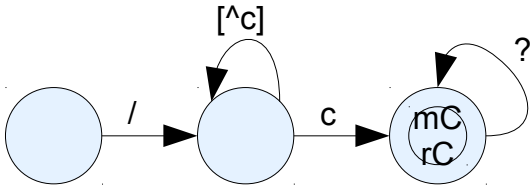
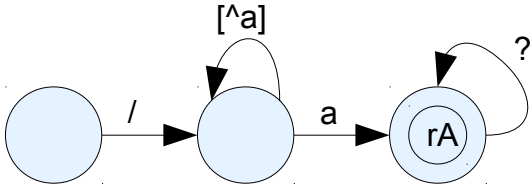
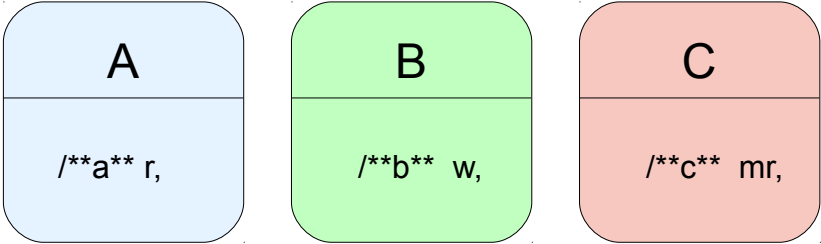
```
profile syslogd /{usr/,}sbin/syslogd {  
  #include <abstractions/base>  
  #include <abstractions/nameservice>  
  #include <abstractions/consoles>
```

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

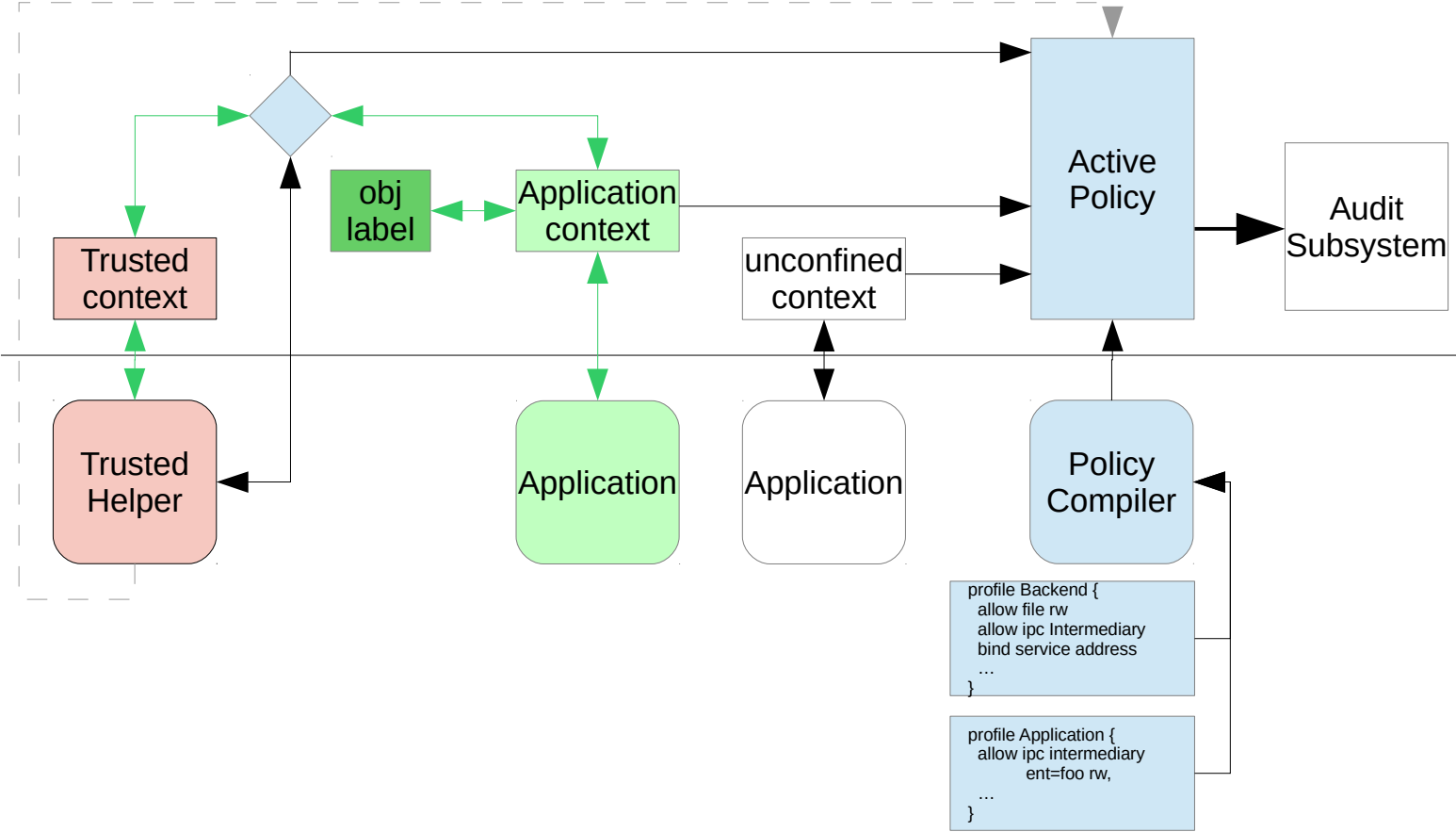
```
  /dev/log wl,  
  /var/lib/*/dev/log wl,
```

```
  ...
```

Handling Pattern matching



Basic Policy Summary





Policy Namespaces



Namespace 1

/usr/sbin/libvirt (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)

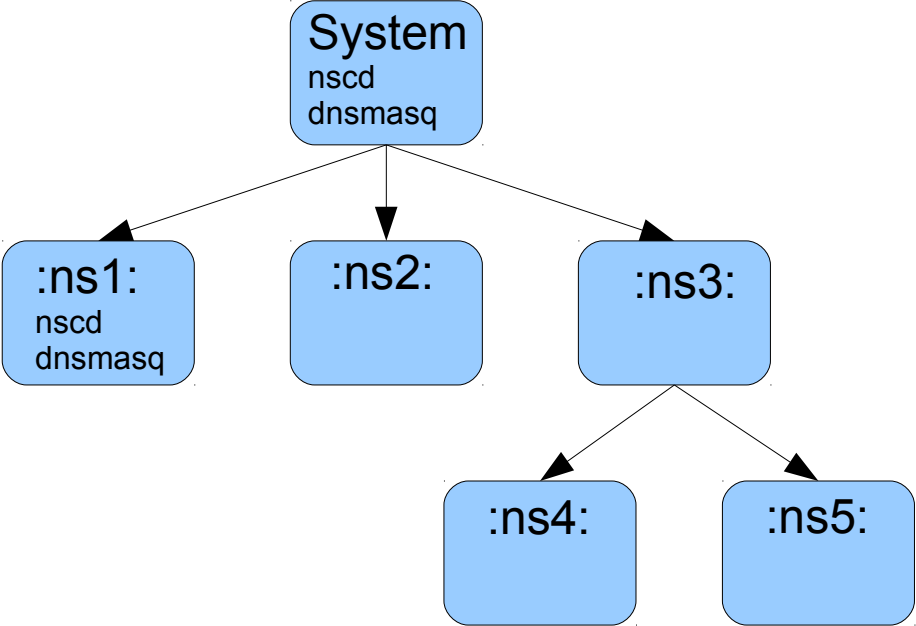
Namespace 2

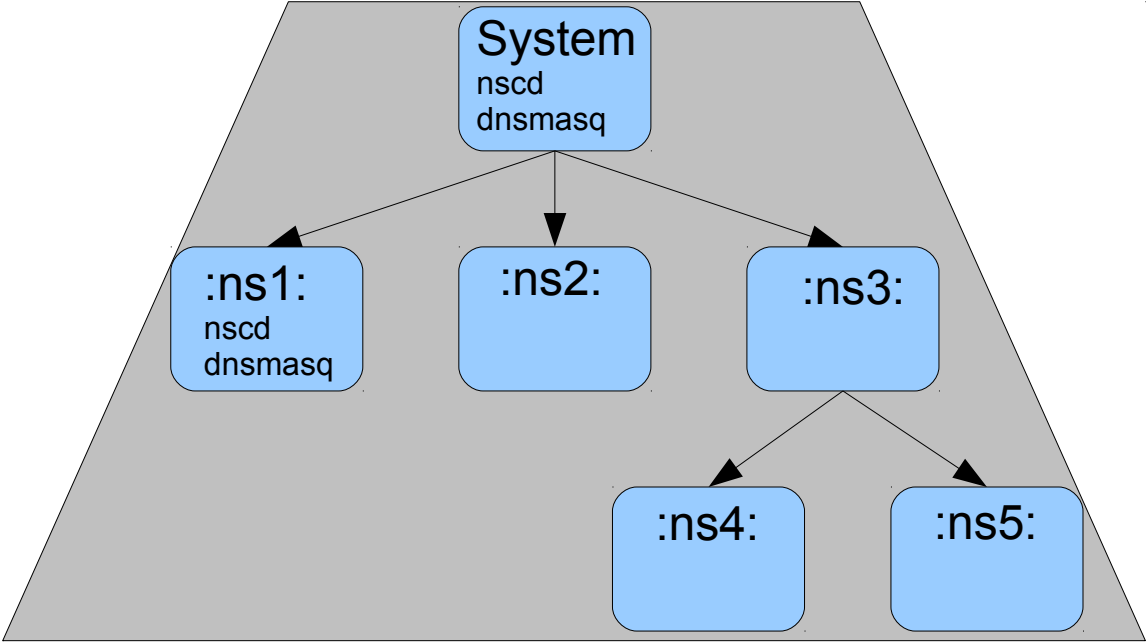
/usr/sbin/libvirt (enforce)
/usr/sbin/mdnsd (complain)
/usr/sbin/identd (complain)
/usr/sbin/cupsd (enforce)
firefox (enforce)
firefox//sanitized_helper (enforce)
firefox//lsb_release (enforce)
firefox//browser_openjdk (enforce)
firefox//browser_java (enforce)

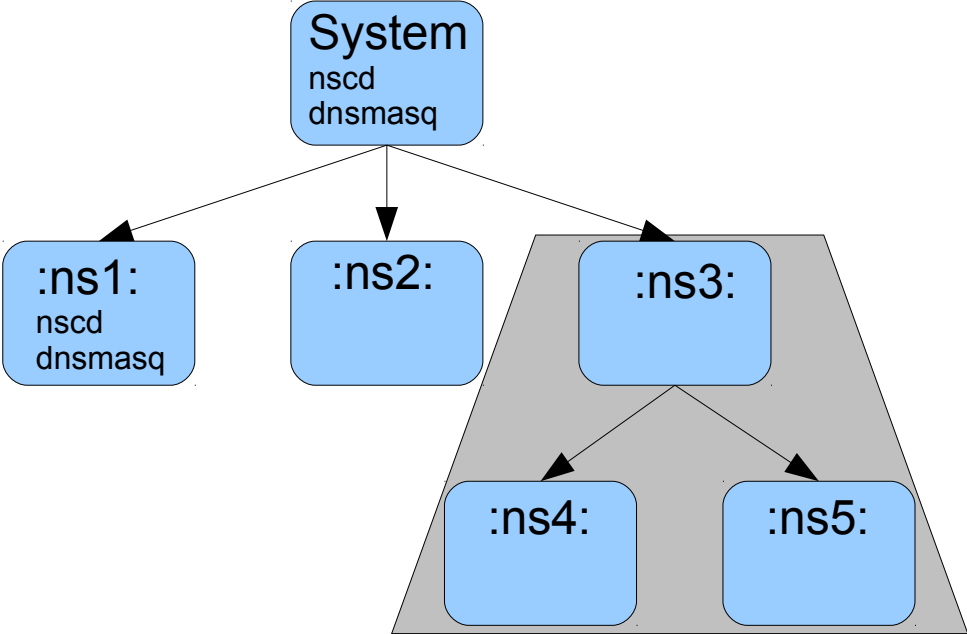


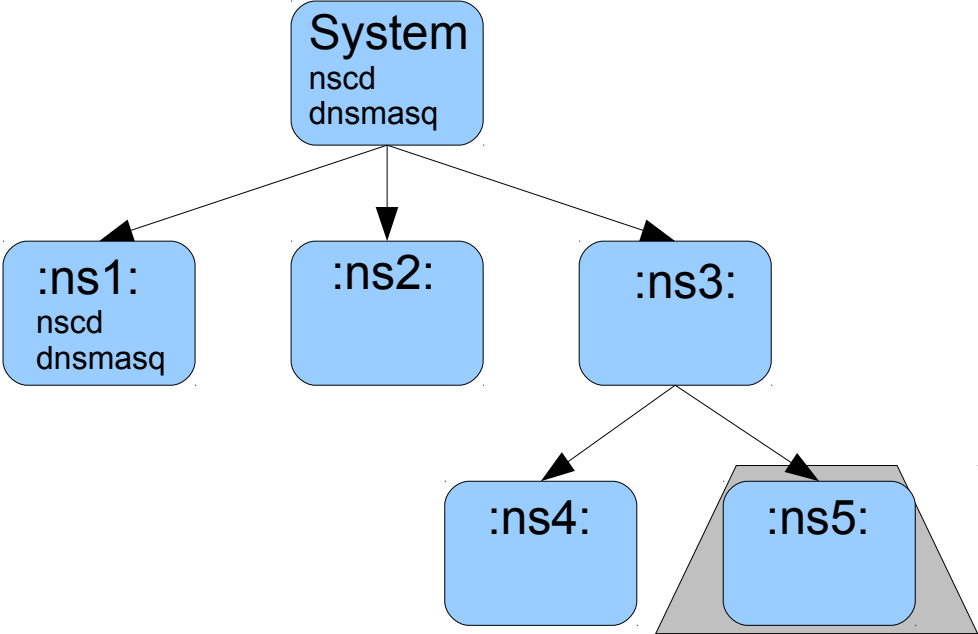
:ns:profile

:ns://profile



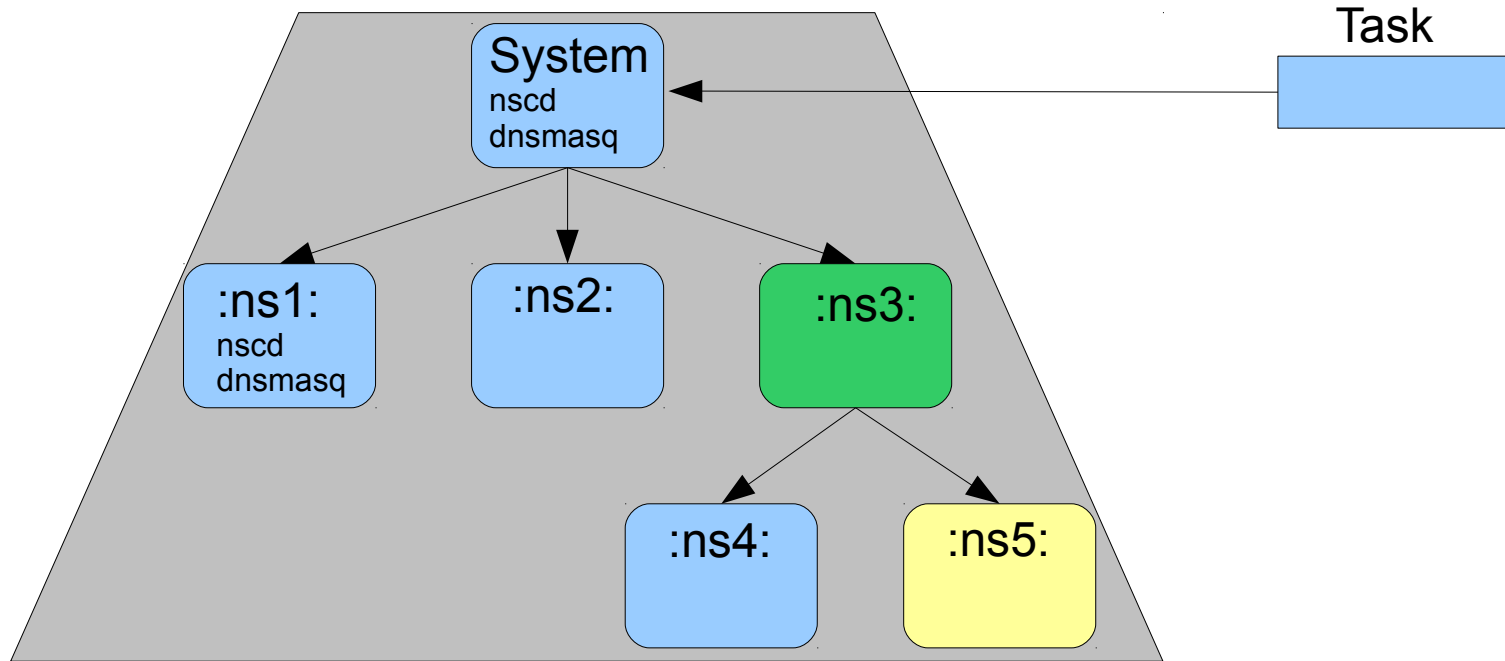




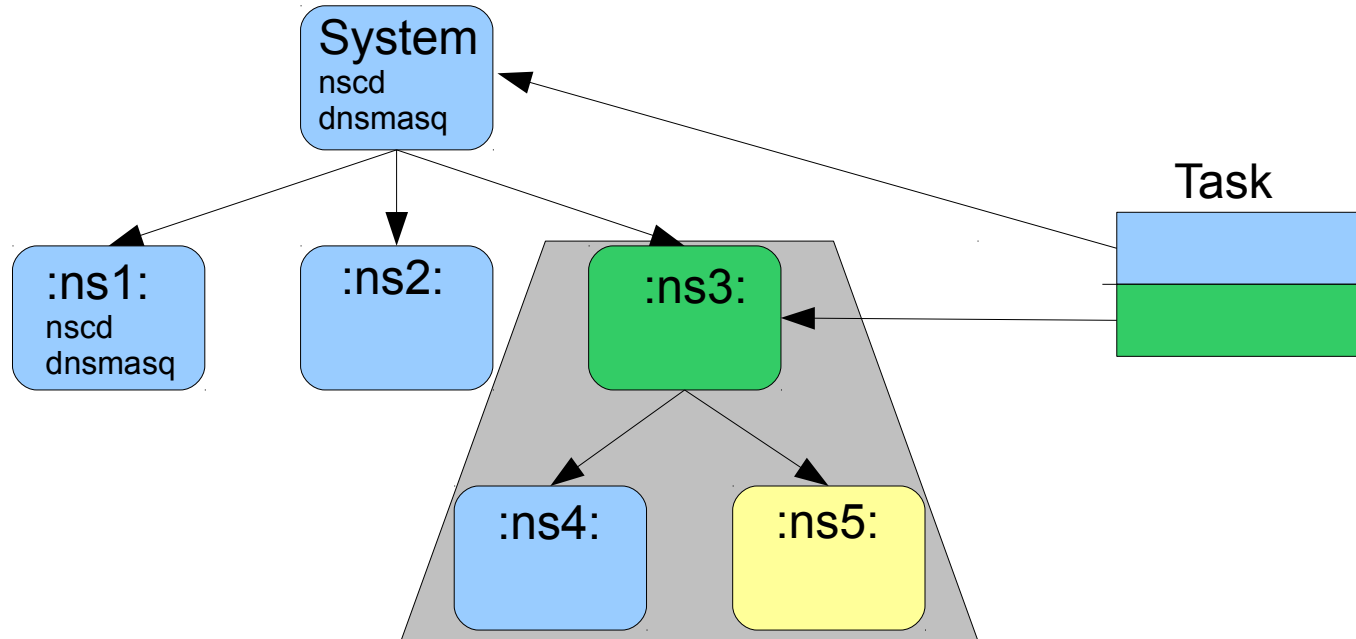


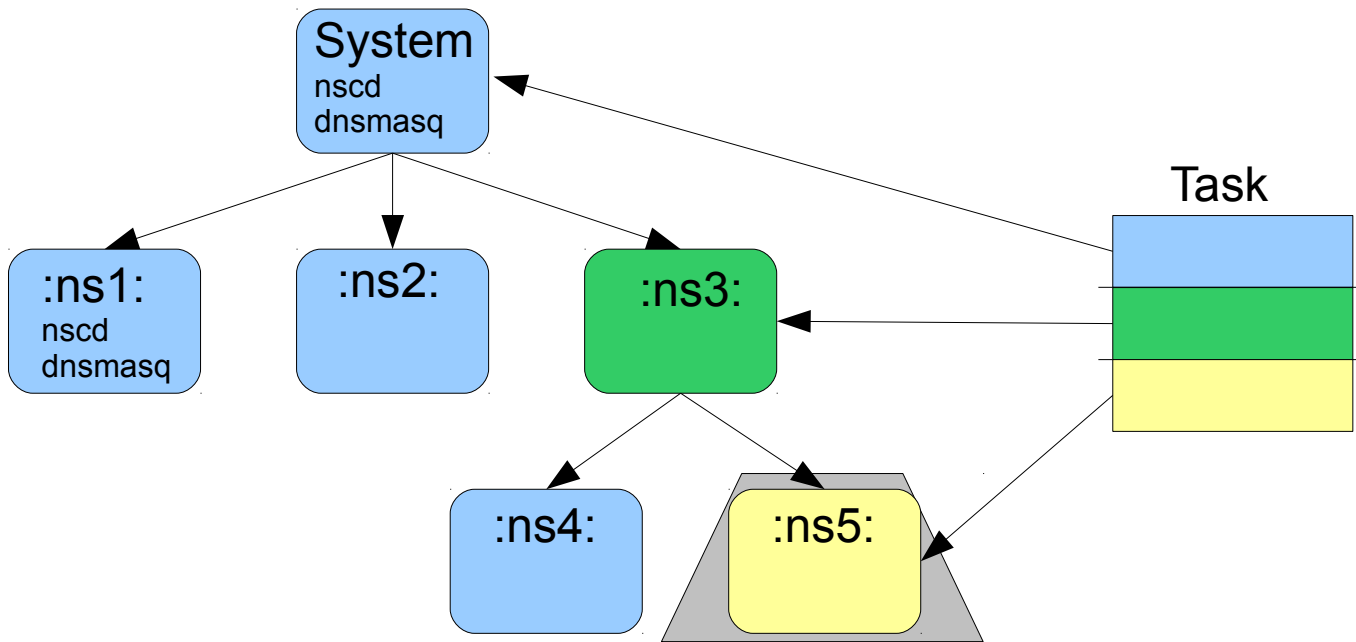


Policy Stacking & Dynamic Policy



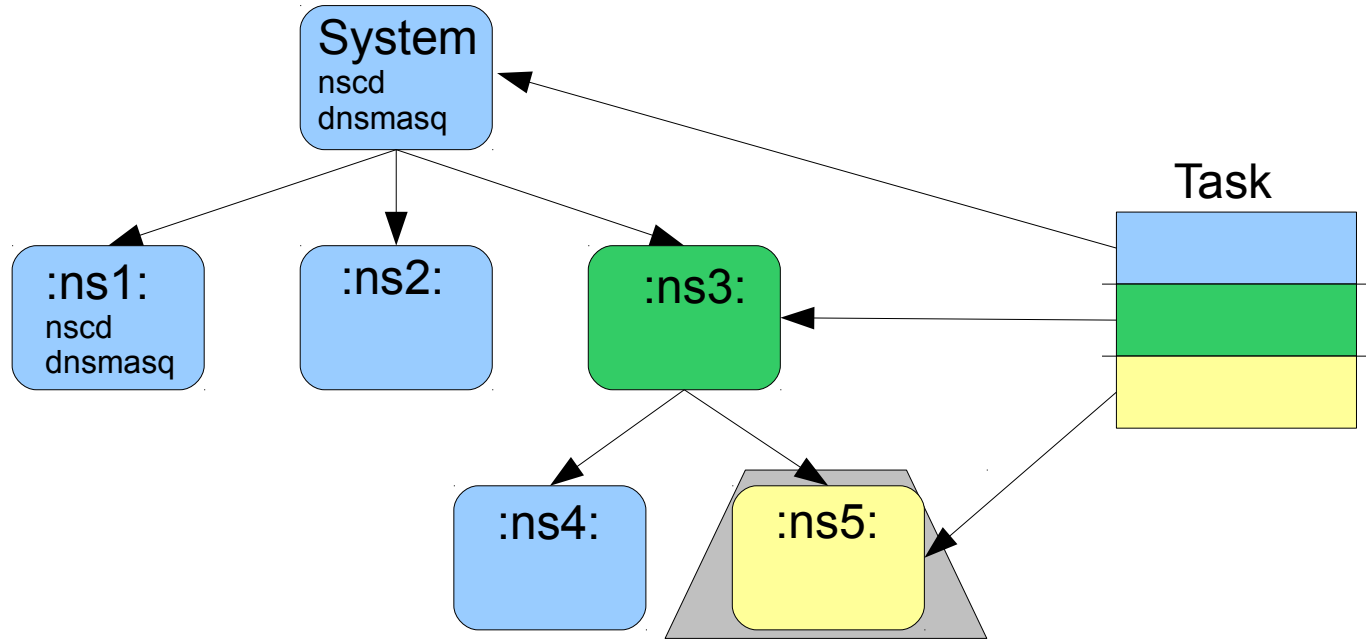
Stacking Across Policy NS can Reduce View





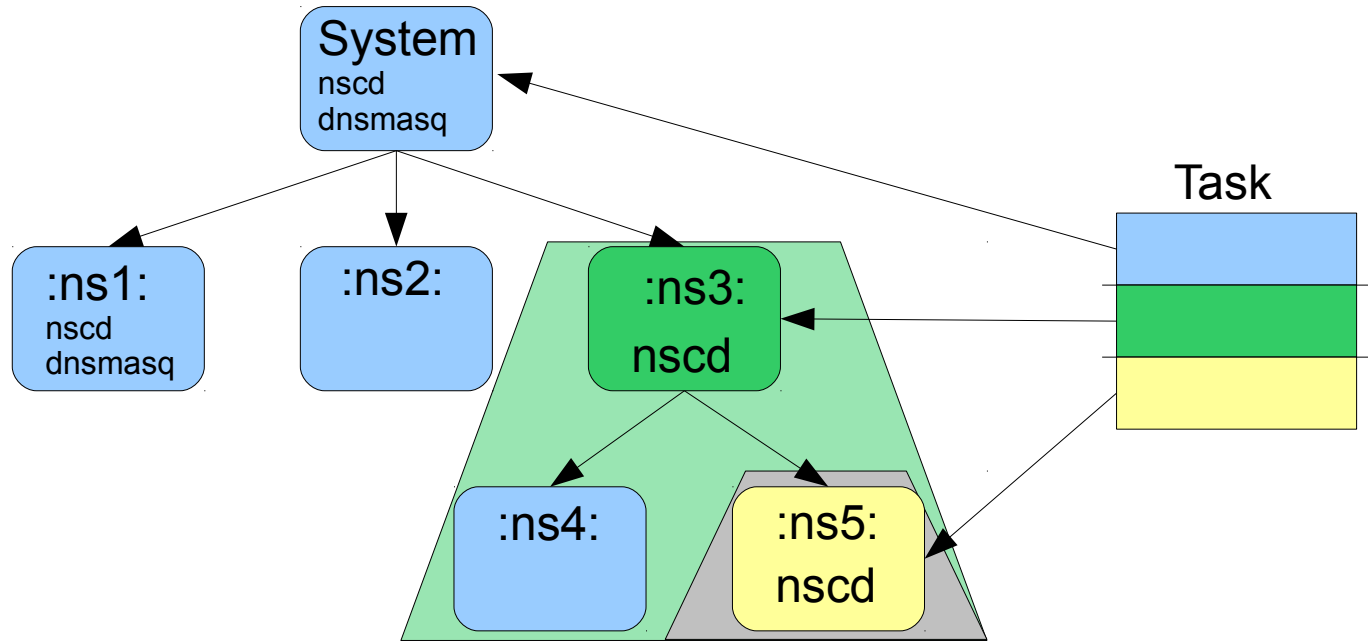


- View
- Scope
- Admin

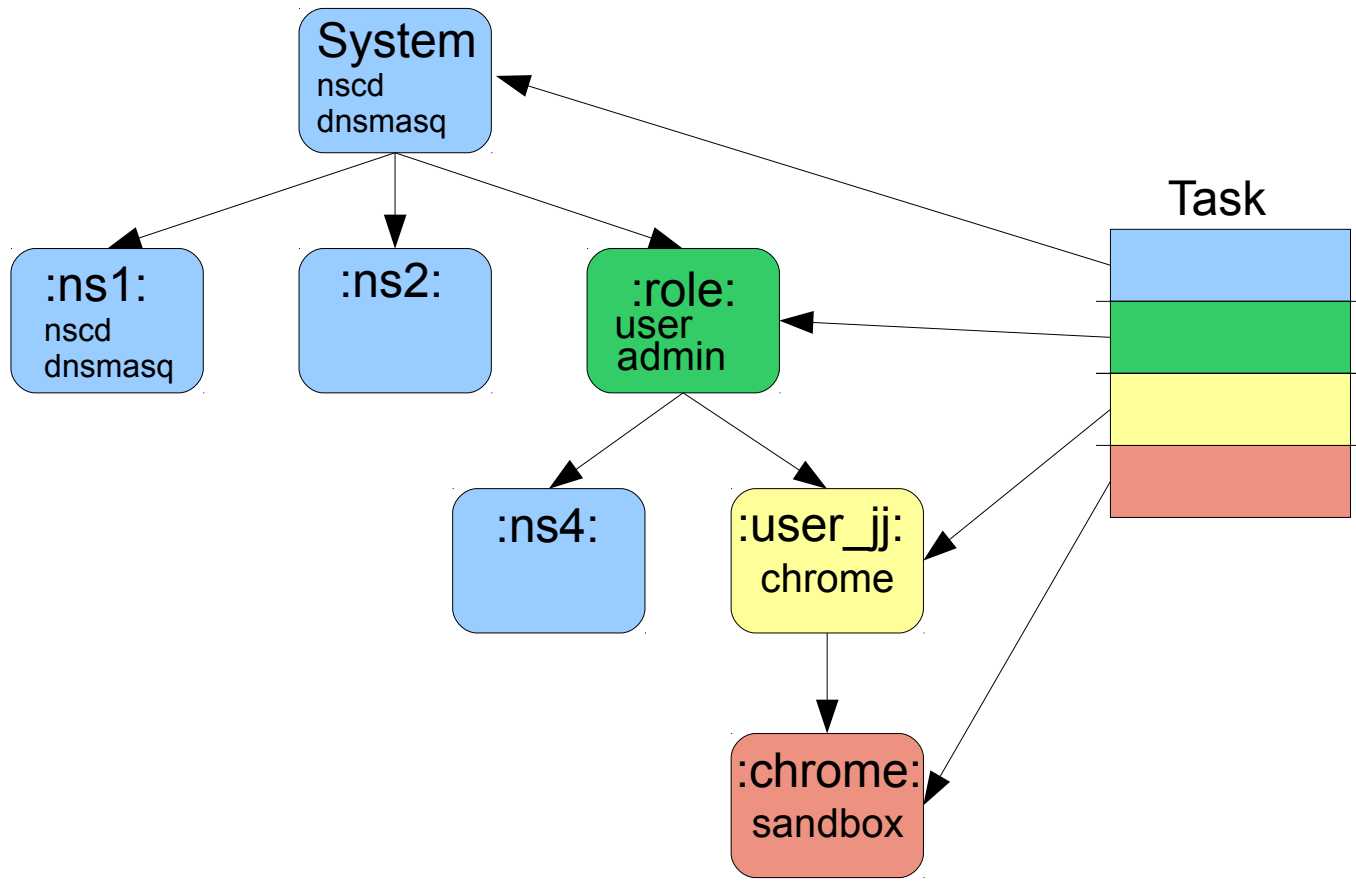




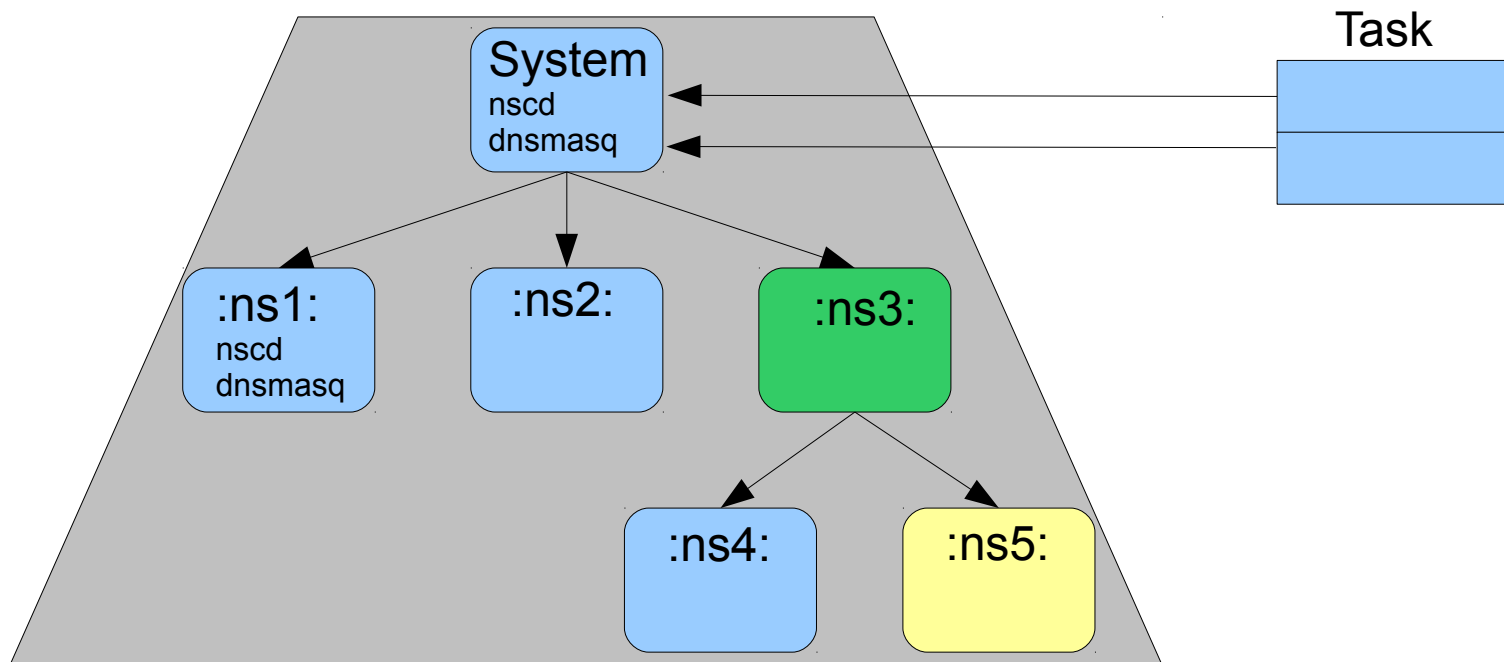
- View
- Scope
- Admin



User sees: nscd :ns5:nscd



Stacking – not just across namespaces





Targeted Task Profile

```
rmPx /usr/bin/evince,  
px /usr/bin/bug-buddy,  
...
```

+

Delegated Authority

Profile

```
file r /etc/firefox*/,  
file r /etc/firefox*/**,  
...
```

&

Delegated Rules

```
file rw /**,  
...
```



firefox//&evince



Recent Developments



Everything except

af_unix



- 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



```
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,
```




```
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,
```



/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  
...
```



`$(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
...
```



\$(loc1)/7f01cf2e.0

\$(loc2)/7f01cf2e.0

skype
usr.bin.evince
usr.bin.firefox

usr.sbin.cupsd

...

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

...

\$(loc1)/a035ea11.0

\$(loc2)/a035ea11.0

skype
usr.bin.evince
usr.bin.firefox

usr.sbin.cupsd

...

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

...



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
 - ...
-



- 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
-



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



Questions please
Thank you

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