THREE BIG
USABILITY IMPROVEMENTS
in SELinux tooling

AGENDA

- SELinux improvements from 2015

AGENDA

- SELinux improvements from 2015
- SELinux team at Red Hat

AGENDA

- SELinux improvements from 2015
- SELinux team at Red Hat
- What can SELinux do for you?

AGENDA

- SELinux improvements from 2015
- SELinux team at Red Hat
- What can SELinux do for you?
- SELinux improvements from 2016?

AGENDA

- SELinux improvements from 2015
- SELinux team at Red Hat
- What can SELinux do for you?
- SELinux improvements from 2016?
- Summary

AGENDA

- SELinux improvements from 2015
- SELinux team at Red Hat
- What can SELinux do for you?
- SELinux improvements from 2016?
- Summary
- Discussion

SELINUX IMPROVEMENTS FROM 2015

- performance gains

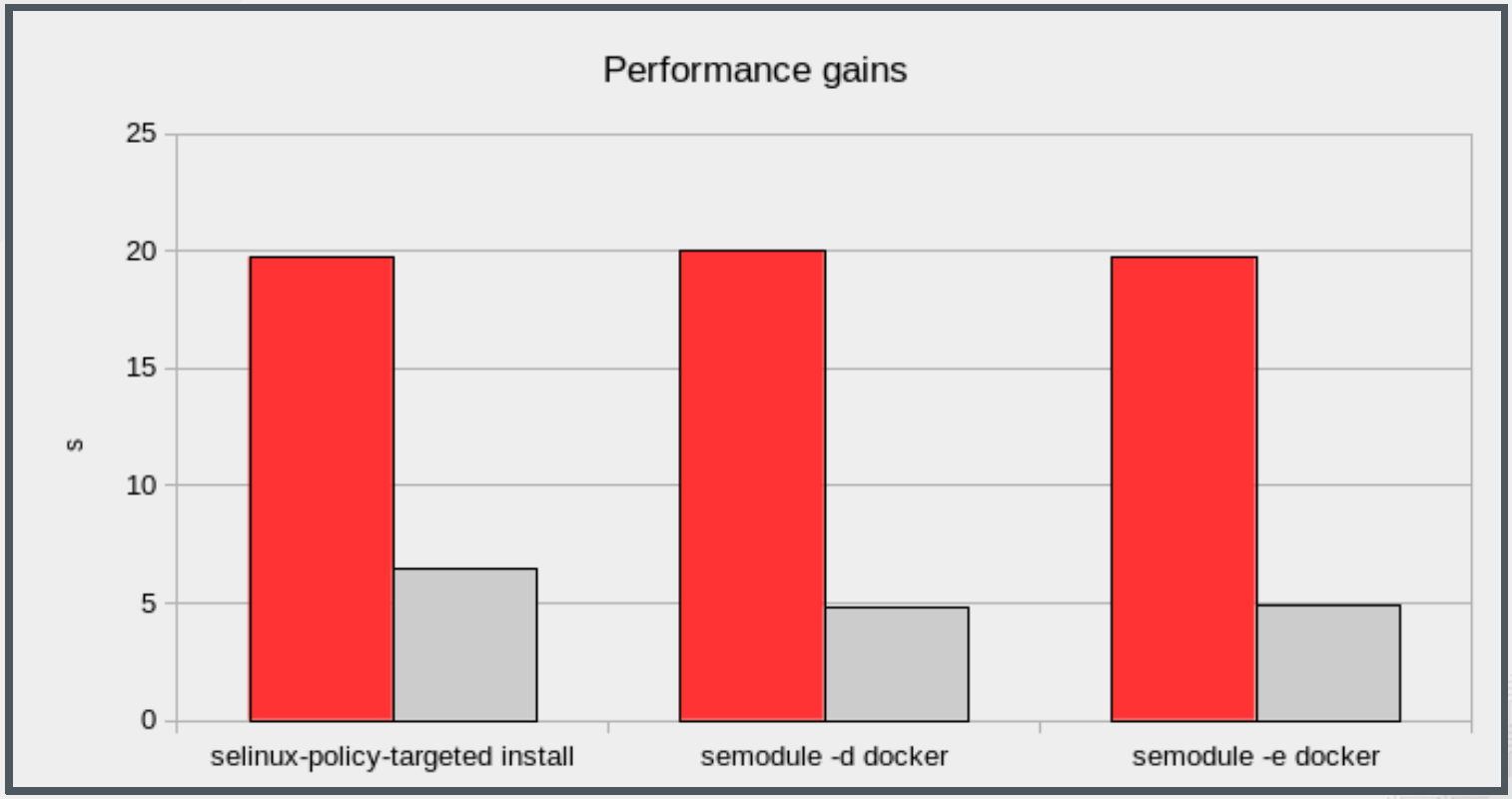
SELINUX IMPROVEMENTS FROM 2015

```
# dnf install selinux-policy-targeted
# semodule -d docker
# semodule -e docker
```

SELINUX IMPROVEMENTS FROM 2015

~ 15 seconds for

SELINUX IMPROVEMENTS FROM 2015



SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management

SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management
- **easier to provide your own SELinux policies**

SELINUX IMPROVEMENTS FROM 2015

```
# dnf install docker-selinux
```

SELINUX IMPROVEMENTS FROM 2015

```
# dnf install docker-selinux

libsepol.scope_copy_callback:docker Duplicate
declaration in module
```

SELINUX IMPROVEMENTS FROM 2015

```
# dnf install docker-selinux
# semodule --list=full | grep docker
400 docker
100 docker
```

SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management
- **easier to provide your own SELinux policies**
  - assigning **priorities** to modules

SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management
- **easier to provide your own SELinux policies**
  - assigning **priorities** to modules
- **new Common Intermediate Language - CIL**

SELINUX IMPROVEMENTS FROM 2015

- HLL vs. CIL

```
# cat mysandbox.te

policy_module(mysandbox,1.0)

require{
 type sandbox_web_t;
  attribute userdomain;
 }

allow sandbox_web_t userdomain:unix_stream_socket co
nnectto;
```

SELINUX IMPROVEMENTS FROM 2015

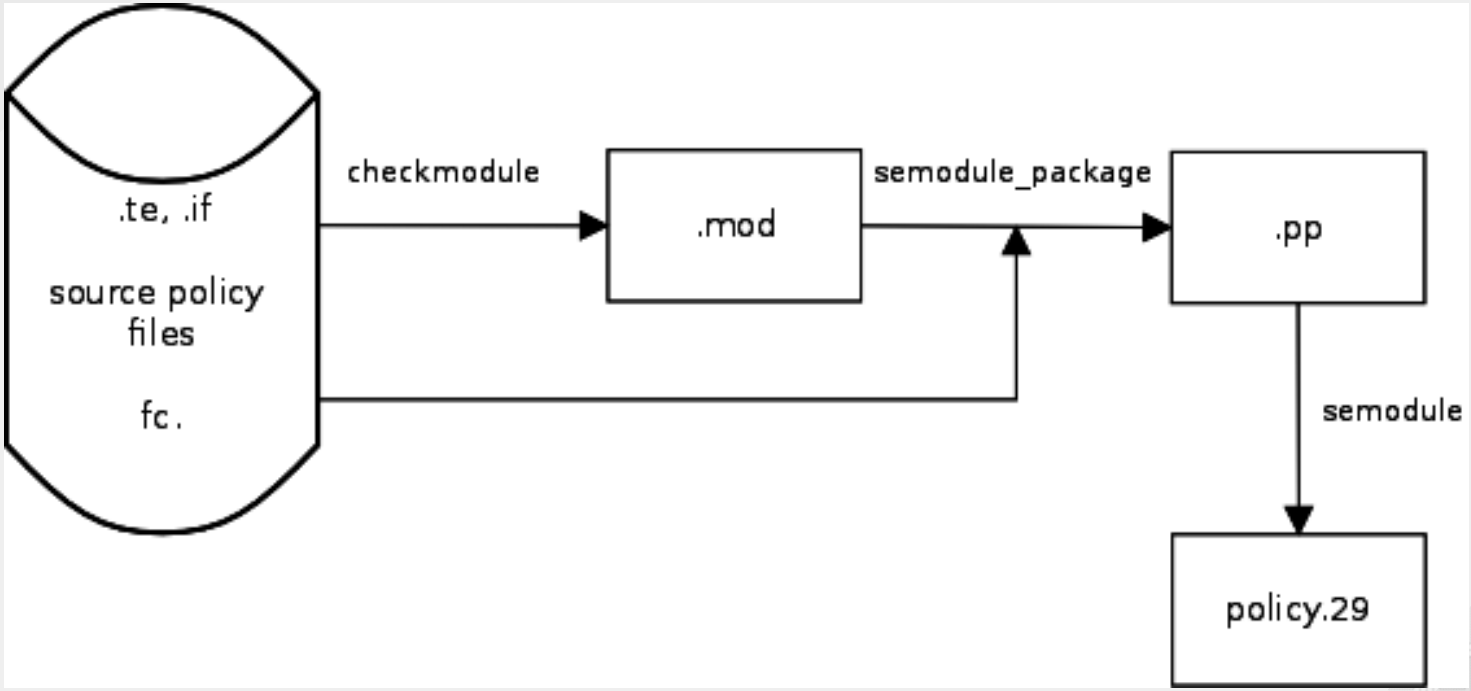
- HLL vs. CIL

```
# make -f ../Makefile mysandbox.pp

# semodule -i mysandbox.pp
```

SELINUX IMPROVEMENTS FROM 2015

- HLL vs. CIL



SELINUX IMPROVEMENTS FROM 2015

- CIL

```
# cat mysandbox.cil

(allow sandbox_web_t unconfined_t (unix_stream_socket (con
nectto)))

# semodule -i mysandbox.cil
```

SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management
- **easier to provide your own SELinux policies**
  - assigning **priorities** to modules
- **new Common Intermidiate Language - CIL**
  - readable intermediate policy language

SELINUX IMPROVEMENTS FROM 2015

- **performance gains**
  - **75% speed-up** of tools that perform SELinux policy management
- **easier to provide your own SELinux policies**
  - assigning **priorities** to modules
- **new Common Intermidiate Language - CIL**
  - readable intermediate policy language
  - potential for new High Level Languages (in Java Script?)

SELINUX IMPROVEMENTS FROM 2015

- **new Common Intermidiate Level Language - CIL**
  - lolpolicy (HLL) from Joshua Brindle

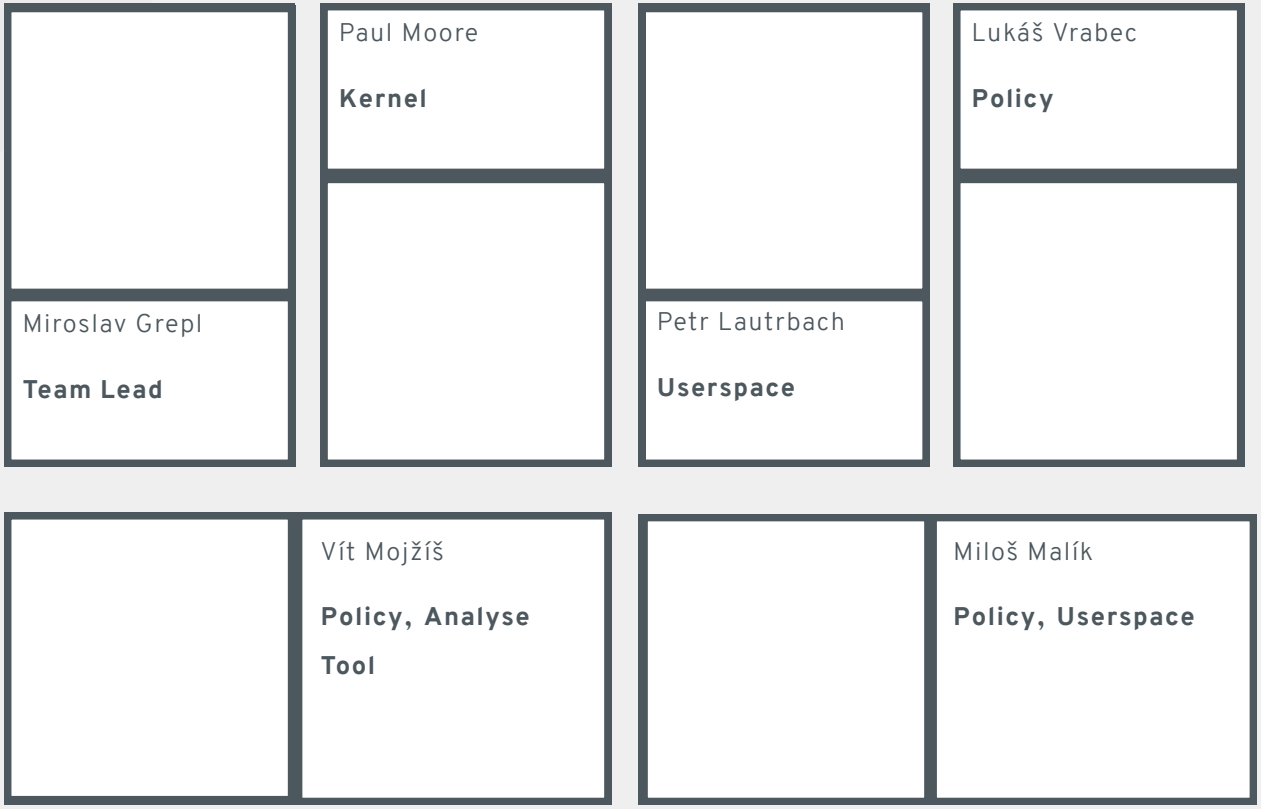
```
I iz logwatch
     in ur webserver
     reading ur logs
```

SELINUX IMPROVEMENTS FROM 2015

It is **HERE.**

FEDORA 23.

SELINUX TEAM AT RED HAT



SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

SELINUX TEAM AT RED HAT

Miroslav Grepl

Team Lead

Paul Moore

Kernel

Petr Lautrbach

Userspace

Lukáš Vrabec

Policy

Vít Mojžíš

Policy, Analyse Tool

Miloš Malík

Policy, Userspace

WHAT SELINUX CAN DO FOR YOU?

- protect your system from consequences of exploited apps

WHAT SELINUX CAN DO FOR YOU?

- **protect your system from consequences of exploited apps**
  - CVE-2015-5602 aka *Unauthorized Privilege Escalation* in *sudo*

WHAT SELINUX CAN DO FOR YOU?

[usr@localhost ~]$ ln -s /etc/shadow ~/temp/test.txt

[usr@localhost ~]$ sudo -e ~/temp/test.txt

root:$6$0m2y//leQIKDW0cg$f0wGcz/4NhfJo8VEe66SRHz9p8QaaTq8Ldby66692uO04ouqn9D93ECQVIO62Cer3ar2z.ef.365SSInyja3T.::0:99999:7:::

bin:*:16489:0:99999:7:::

daemon:*:16489:0:99999:7:::

adm:*:16489:0:99999:7:::

lp:*:16489:0:99999:7:::

sync:*:16489:0:99999:7:::

shutdown:*:16489:0:99999:7:::

WHAT SELINUX CAN DO FOR YOU?

```
[usr@localhost ~]$ ln -s /etc/shadow ~/temp/test.txt

[usr@localhost ~]$ sudo -e ~/temp/test.txt

sudoedit: /home/usr/temp/test.txt: Permission denied

[usr@localhost ~]$ getenforce

Enforcing
```

WHAT SELINUX CAN DO FOR YOU?

- **protect your system from consequences of exploited apps**
  - CVE-2015-5602 aka *Unauthorized Privilege Escalation* in *sudo*

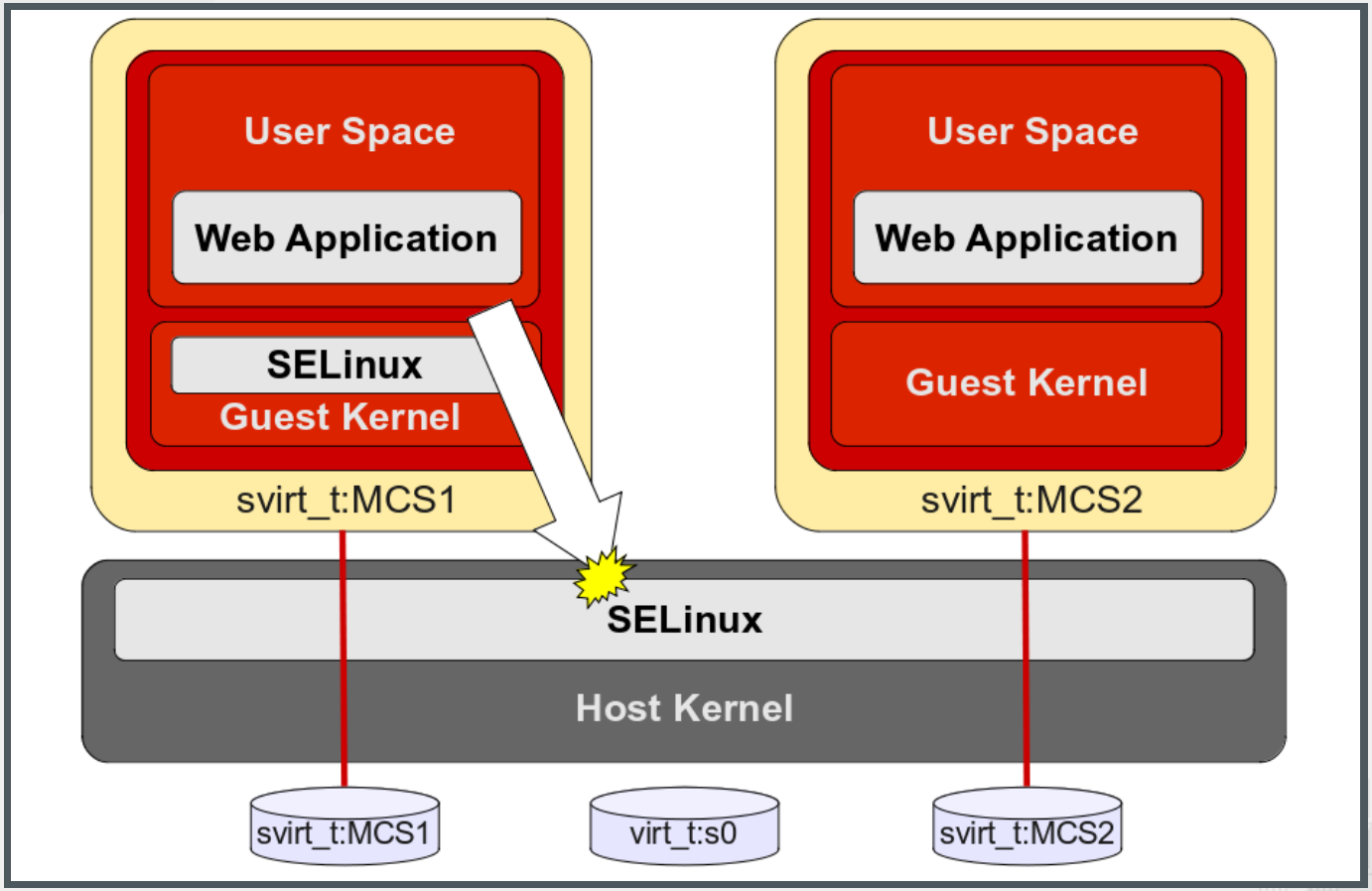
WHAT SELINUX CAN DO FOR YOU?

- **protect your system from consequences of exploited apps**
  - CVE-2015-5602 aka *Unauthorized Privilege Escalation* in *sudo*
- **protect your virtual machines**

WHAT SELINUX CAN DO FOR YOU?

- **protect your system from consequences of exploited apps**
  - CVE-2015-5602 aka *Unauthorized Privilege Escalation* in *sudo*
- **protect your virtual machines**
  - CVE-2015-3456 aka *Venom*

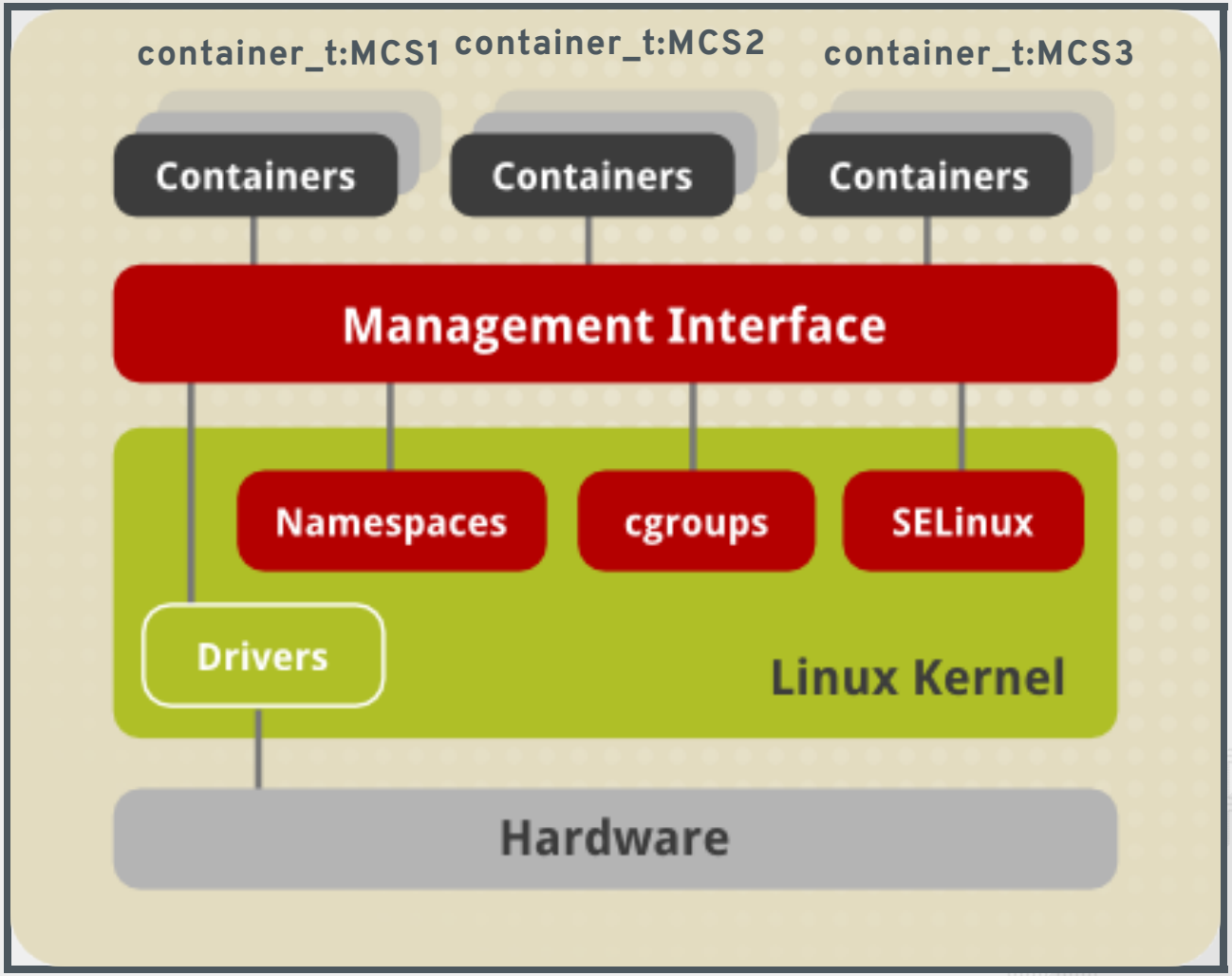
WHAT SELINUX CAN DO FOR YOU?



WHAT SELINUX CAN DO FOR YOU?

- keeps your container in its own space

WHAT SELINUX CAN DO FOR YOU?



WHAT SELINUX CAN DO FOR YOU?

- keeps your container in its own space
- advanced security for Multitenant Environments

WHAT SELINUX CAN DO FOR YOU?

- **keeps your container in its own space**
- **advanced security for Multitenant Environments**
  - running thousands processes
  - gears in OpenShift
  - containers in OpenShift v3

WHAT SELINUX CAN DO FOR YOU?

Security **WINS**
with **SELINUX**

SELINUX IMPROVEMENTS IN 2016?

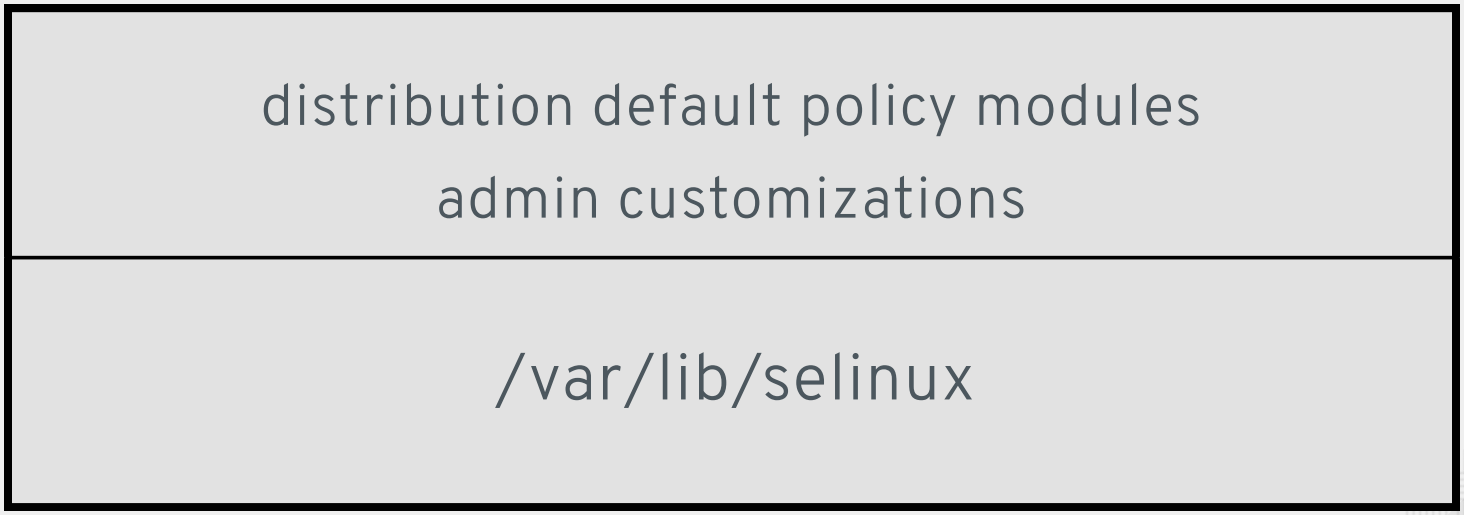
- "a new SELinux" on Atomic - seatomic

SELINUX IMPROVEMENTS IN 2016?

- **"a new SELinux" on Atomic - seatomic**
  - support for "factory reset"

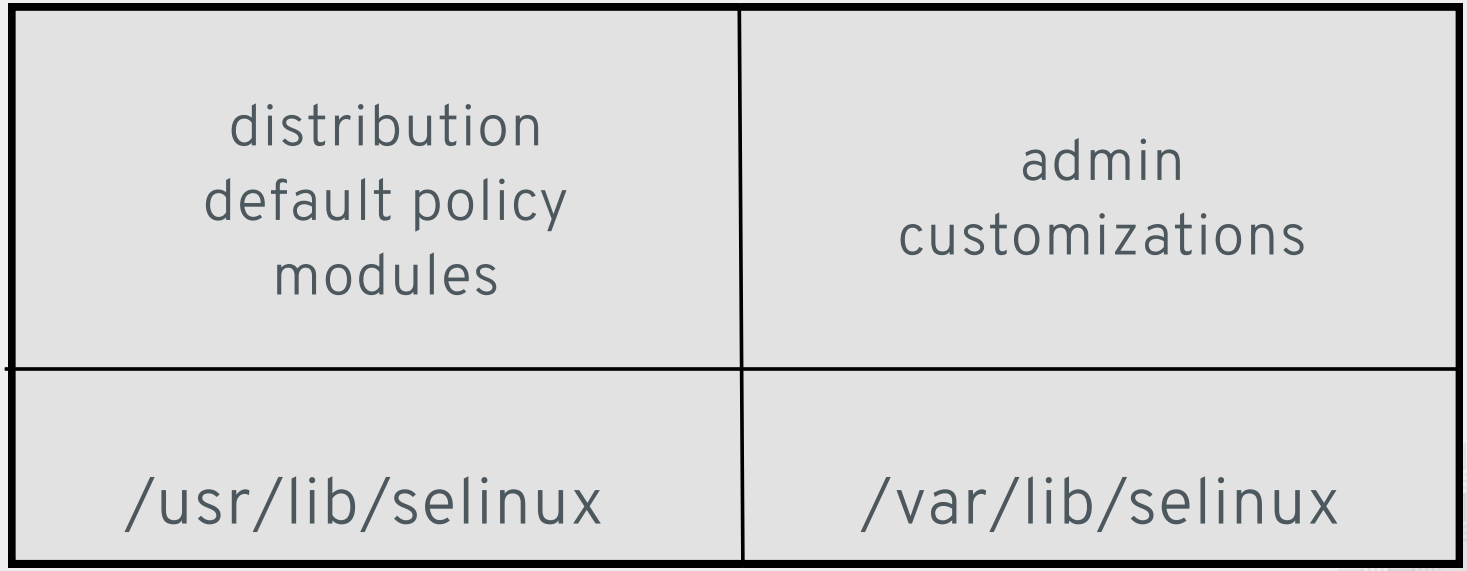
SELINUX IMPROVEMENTS IN 2016?

- **"a new SELinux" on Atomic - seatomic**
  - support for "factory reset"



SELINUX IMPROVEMENTS IN 2016?

- **"a new SELinux" on Atomic - seatomic**
  - support for "factory reset"



SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**

SELINUX IMPROVEMENTS IN 2016?

```
$ sestatus
Loaded policy name:                targeted
$ seinfo
Types:               4665
Allow:             100393
```

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**
    - **a new concept of policy - "lightweight" policy**

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**
    - **a new concept of policy - "lightweight" policy**
      - reduction of process/file types - **thousands** vs. **tens**

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**
    - **a new concept of policy - "lightweight" policy**
      - reduction of process/file types - **thousands** vs. **tens**
      - reduction of policy rules - **tens thousands** vs. **thousands**

SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**
    - **a new concept of policy - "lightweight" policy**
      - reduction of process/file types - **thousands** vs. **tens**
      - reduction of policy rules - **tens thousands** vs. **thousands**
      - simplified and understandable policy

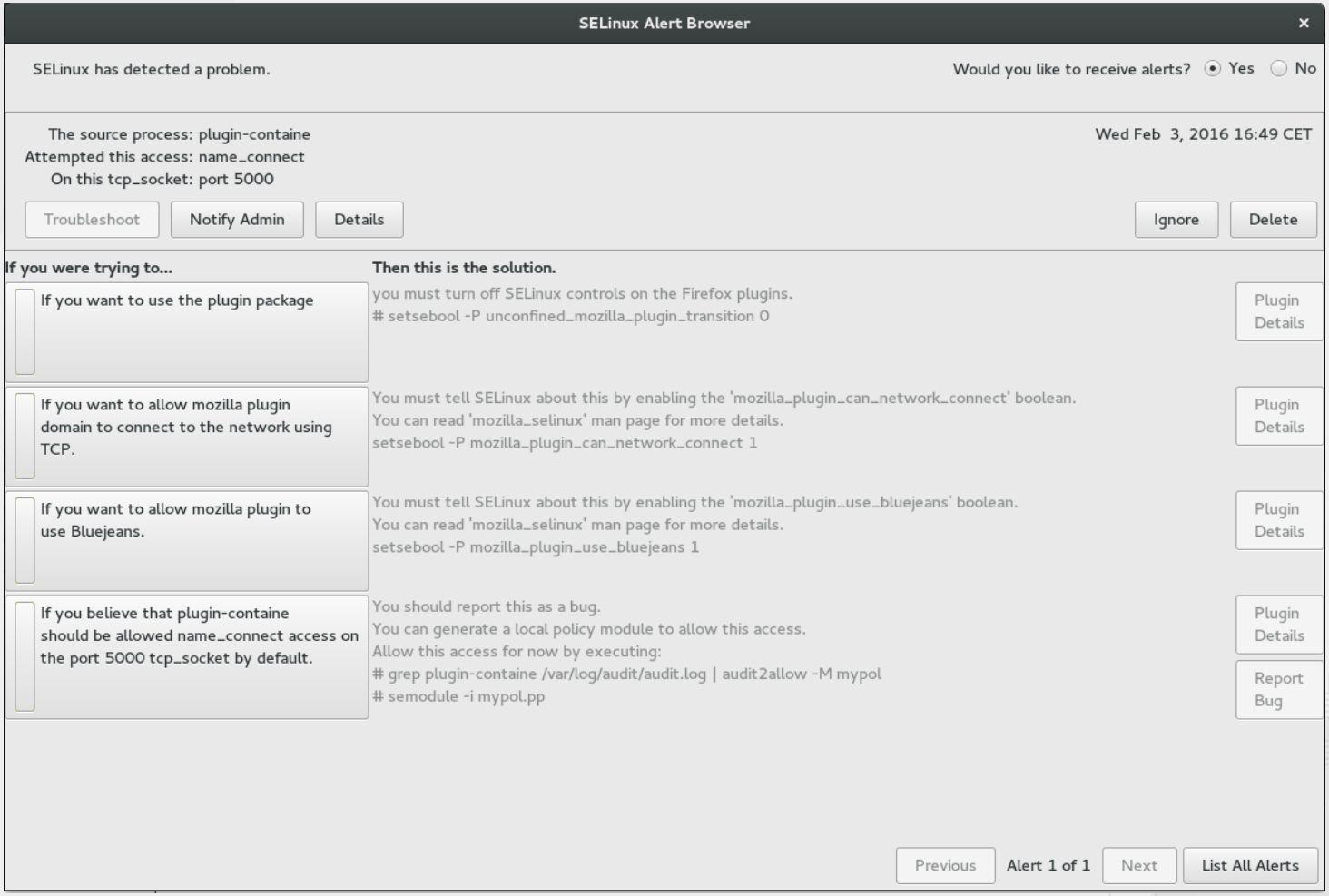
SELINUX IMPROVEMENTS IN 2016?

- **seatomic "SELinux on Atomic"**
  - policy reflecting Atomic Host requirements
    - containers with services around containers
    - the current huge "workstation" policy - **Targeted**
    - **a new concept of policy - "lightweight" policy**
      - reduction of process/file types - **thousands** vs. **tens**
      - reduction of policy rules - **tens thousands** vs. **thousands**
      - simplified and understandable policy
      - **significant speed-up** of tools that performs SELinux policy management

SELINUX IMPROVEMENTS IN 2016?

- SELinux troubleshooting

SELINUX IMPROVEMENTS IN 2016?



SELINUX IMPROVEMENTS IN 2016?

- **SELinux troubleshooting**
  - improved **best practises** suggested by SEAlert
  - SELinux troubleshooting **in Cockpit**

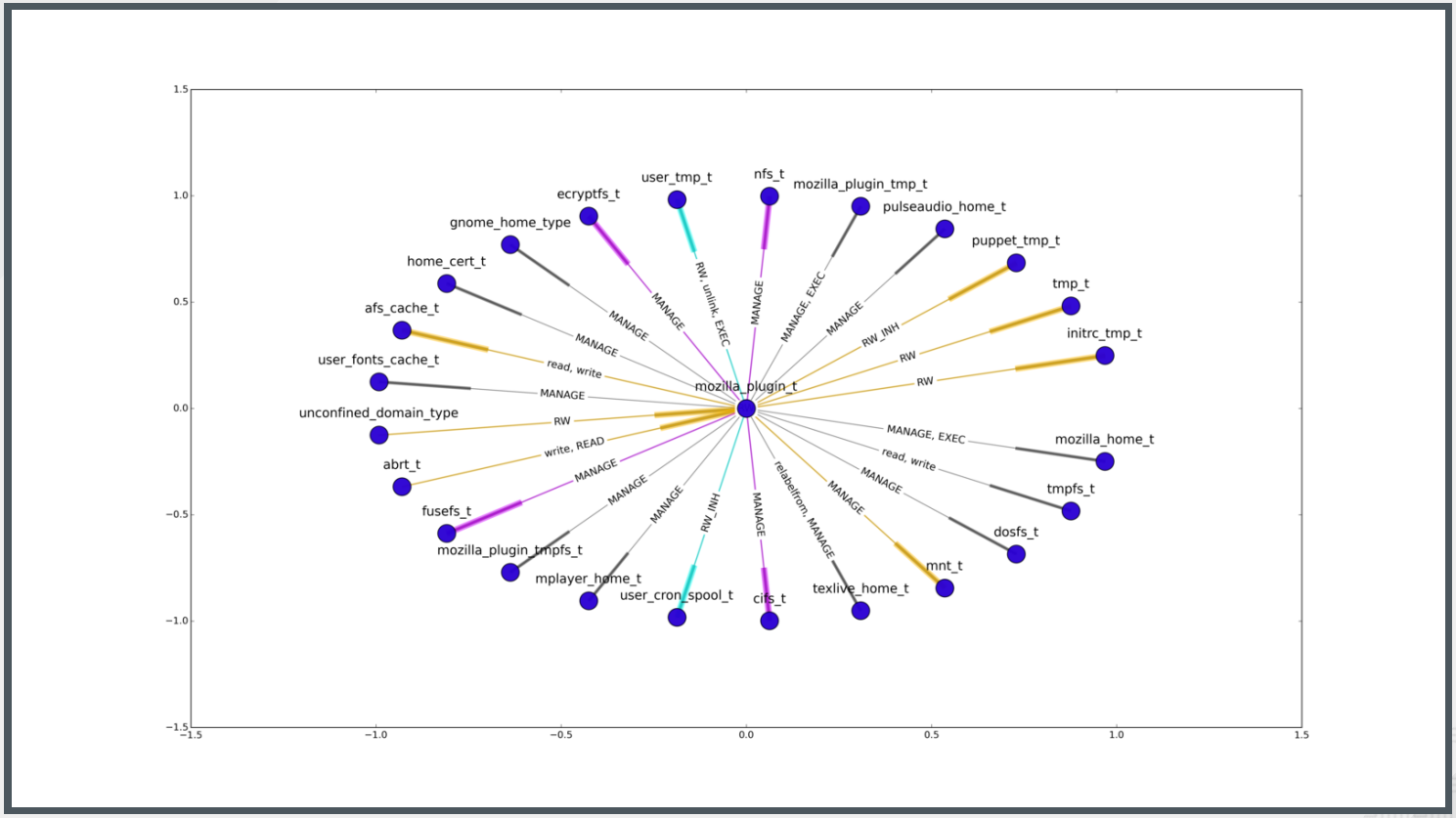
SELINUX IMPROVEMENTS IN 2016?

- **SELinux troubleshooting**
  - improved **best practises** suggested by SEAlert
  - SELinux troubleshooting **in Cockpit**
- **SELinux policy analysis tool**

SELINUX IMPROVEMENTS IN 2016?

- **SELinux troubleshooting**
  - improved **best practises** suggested by SEAlert
  - SELinux troubleshooting **in Cockpit**
- **SELinux policy analysis tool**
  - human readable **big picture** of policy

SELINUX IMPROVEMENTS IN 2016?



SELINUX IMPROVEMENTS IN 2016?

- **SELinux troubleshooting**
  - improved **best practises** by SEAlert
  - SELinux troubleshooting **in Cockpit**
- **SELinux policy analysis tool**
  - human readable **big picture** of policy
  - SELinux policy integrity

SUMMARY

- **75% speed** of tools that perform SELinux policy management

SUMMARY

- **75% speed** of tools that perform SELinux policy management
- easier to provide your **own** SELinux policies

SUMMARY

- **75% speed** of tools that perform SELinux policy management
- easier to provide your **own** SELinux policies
- **CIL** as a new Intermediate Language

SUMMARY

- **75% speed** of tools that perform SELinux policy management
- easier to provide your **own** SELinux policies
- **CIL** as a new Intermediate Language
- SELinux helps **mitigate** consequences of exploits

SUMMARY

- **75% speed** of tools that perform SELinux policy management
- easier to provide your **own** SELinux policies
- **CIL** as a new Intermediate Language
- SELinux helps **mitigate** consequences of exploits
- new SELinux for Atomic Hosts aka **seatomic** is coming soon

SUMMARY

- SELinux troubleshooting integrated with Cockpit

SUMMARY

- SELinux troubleshooting integrated with Cockpit
- Visualization of policy

DISCUSSION AND Q&A

and **THANK YOU!**

mgrepl@redhat.com