



Enabling RHEL Security:

SELinux, Fapolicyd and Auditd

Joshua Loscar

Senior Technical Marketing Manager

Red Hat

Brian Hoppus

Senior Technical Account Manager

Red Hat

Nate Lager

Senior Technical Marketing Manager

Red Hat



Joshua Loscar
Senior Marketing Account Manager



Brian Hoppus
Senior Technical Account Manager



Nate Lager
Senior Technical Marketing
Manager - RHEL



Joshua Loscar
Senior Marketing Account Manager

- **12+ Years In IT**
 - 6 Years as a Red Hat Technical Account Manager
 - Built 200+ Pc's
 - Homelab Enthusiast
 - 48 Raspberry Pi & counting
 - Worked with early Containers back in 2017
- **6 Years With The DoD**
 - Hardening Via STIGs
 - Risk Management (RMF)
- **11 Years Attending & Contributing To Cyber Security Conferences**
 - DEF CON
 - BSides
 - Southern California Linux Expo
- **10 Years Running A Hackerspace**
 - Tutor Security+
 - Online Security & Privacy
- **Content Creator**
 - Host 4 Year Podcast on Cybersecurity
 - Guest Host on Infosec Podcast
 - Publishing Videos for online training



Brian Hoppus


Senior Technical Account Manager

- **Why**
 - First distro was Fedora Core 2
 - Passion for open source
 - Community as an enabler for advancing technology
- **Prior Experience**
 - 12+ years as Linux sysadmin
 - Civil service for the US Navy's NAWC and NUWC
- **Work at Red Hat**
 - Technical Account Manager for 3+ years
 - Started with Platform (RHEL + Satellite)
 - Now focused on Ansible Automation Platform



Nate Lager

Senior Technical Marketing
Manager - RHEL

 @gangrif@undrground.org

- IT Generalist
 - I've worked in hosting, higher ed, and ISP.
 - Networking, operating systems, even some datacenter design
 - But I specialize in Linux
- DEF CON group admin
 - I help run and organize a local DEF CON group since 2017
 - I keep a toe in the IT Security industry
- Creator
 - These days I spend my time creating content around Red Hat Enterprise Linux as a Technical Marketing Manager
 - Come see me at the RHEL booth!

Today's Agenda

- ▶ Whoami
- ▶ Definitions
- ▶ SELinux
- ▶ Fapolicyd
- ▶ Auditd

Enabling RHEL Security:

Lab Password

securerhel6

Lab layout

Presentation (5-7) minutes

Hands on Lab (10-15) Minutes

How Many Of You Use SELinux?

How Many Of You Turn Off SELinux?

What Is SELinux?

Security Enhanced Linux



Can help proactively **mitigate** systems from the consequences of exploits during the window of vulnerability

Why use SELinux?

- ▶ Limits damage from compromised services
- ▶ Enforces least privilege
- ▶ Your boss says you have to

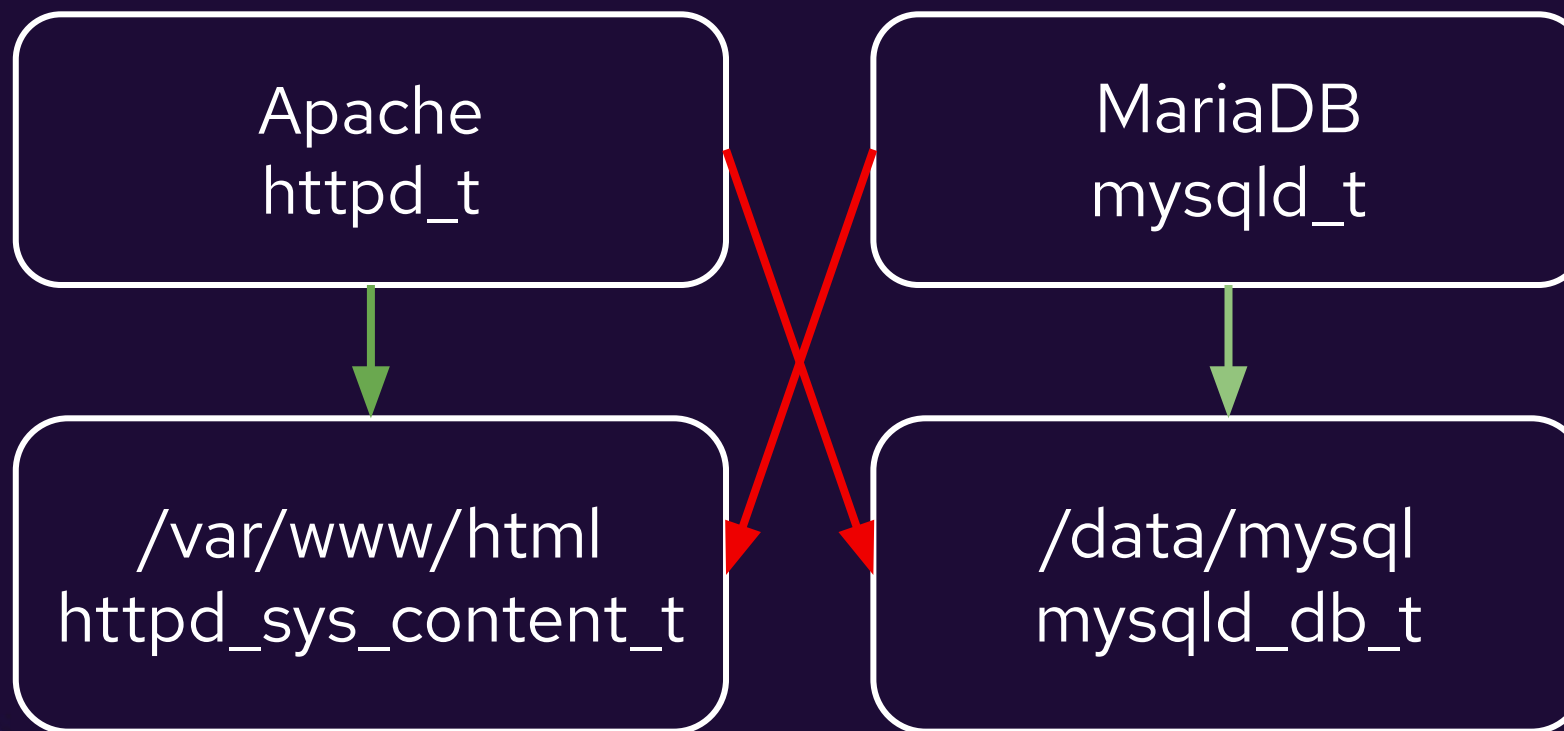
Key Concepts

- ▶ Subjects: usually processes
- ▶ Objects: files, sockets, devices
- ▶ Labels: **everything** has a security context
- ▶ Policies: define allowed interactions
- ▶ Booleans: on/off switches for policy parts

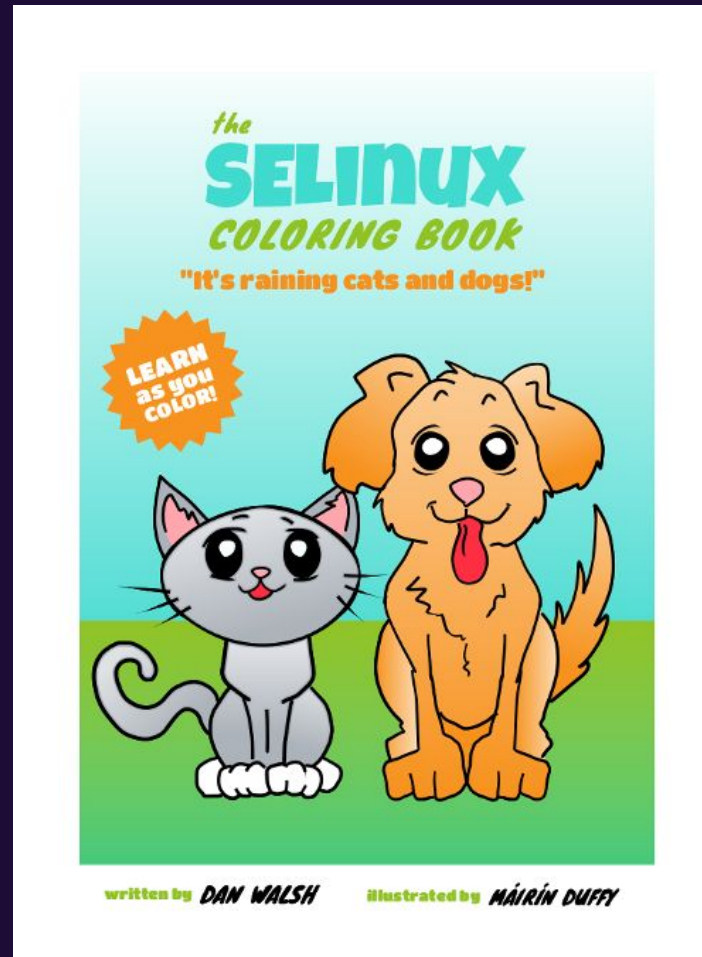
SELinux Types

```
[root@summit ~]# ls -Z /etc/shadow  
system_u:object_r:shadow_t:s0 /etc/shadow
```


Tying It All Together



Next Steps



<https://developers.redhat.com/e-books/selinux-coloring-book>

Enabling RHEL Security:

Lab: SELinux

Enabling RHEL Security:

Who has heard of Fapolicd?

Have you ever...

Had a server compromised, and some unknown
malicious binary was running from some crazy
location?

What is Fapolicyd?

Fapolicyd is a tool for managing and enforcing file access policies on Linux systems.

It allows administrators to define policies that control who can access which files and directories, and how they can do so.

How FAPolicyD Works

Fapolicyd works by intercepting file access requests and checking them against the defined policies.

If a request matches a policy, fapolicyd allows or denies the request accordingly.

Fapolicyd framework components

- ▶ fapolicyd service
- ▶ fapolicyd command-line utilities
- ▶ fapolicyd RPM plugin
- ▶ fapolicyd rule language
- ▶ fagenrules script

Benefits of Fapolicyd

Fapolicyd offers several benefits

- ▶ Improved security
- ▶ Compliance
- ▶ Simplified management
- ▶ Flexibility

Lab: FAPolicyd

Enabling RHEL Security:

AuditD

Enabling RHEL Security:

Who has heard of AuditD?

Enabling RHEL Security:

Who is using AuditD?

What is AuditD?

The Linux Audit system provides a way to track security-relevant information about your system.

Then, you can prevent future such violations by configuring additional security measures such as SELinux.

Use cases for AuditD

- ▶ Watching file access
- ▶ Monitoring system calls
- ▶ Recording
 - commands run by a user
 - execution of system pathnames
 - security events
- ▶ Searching for events
- ▶ Running summary reports
- ▶ Monitoring network access

Audit System Components

**The kernel-side
system call processing**

**The user-space
applications and utilities**

Kernel-side system call processing

The kernel component receives system calls from user-space applications and filters them through one of the following filters: user, task, fstype, or exit.

After a system call passes the exclude filter, it is sent through one of the aforementioned filters, which, based on the Audit rule configuration, sends it to the Audit daemon for further processing.

User-space applications and utilities

- ▶ The user-space Audit daemon collects the information from the kernel and creates entries in a log file.
- ▶ Other Audit user-space utilities interact with the Audit daemon, the kernel Audit component, or the Audit log files

Benefits of AuditD: Tools

Fapolicyd offers several benefits for RHEL 9 administrators, including:

- ▶ **auditctl**
- ▶ **aureport**
- ▶ **audisp**

Configuring auditd for a secure environment

Have 10 different configurations across 4 Categories

- ▶ **File**
- ▶ **Space**
- ▶ **Disk**
- ▶ **Flush**

Enabling RHEL Security:

Lab: AuditD

Enabling RHEL Security:



TL;DR



Fapolicyd

is a user-space application that controls file access based on rules, offering a simpler approach to access control.



SELinux

is a kernel-level MAC system that provides fine-grained access control based on labels.



Auditd

is a logging tool that records security-related events, providing an audit trail for forensic analysis.



Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



twitter.com/RedHat