Cloud Security: Frameworks and Enforcement

SHAWN WELLS
Director, Innovation Programs, U.S. Public Sector
shawn@redhat.com || 443-534-0130

35 MINUTES, 2 GOALS

35 MINUTES, 2 GOALS

1. Cloud Security Lifecycle
    - Government Certification & Accreditation Models
    - Case Study: Westfield's MADFW/MITE

35 MINUTES, 2 GOALS

1. Cloud Security Lifecycle
   - Government Certification & Accreditation Models
   - Case Study: Westfield's MADFW/MITE

2. Enabling Security Technologies
   - Security Content Automation Protocol (SCAP)
   - Containers

WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
  - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE

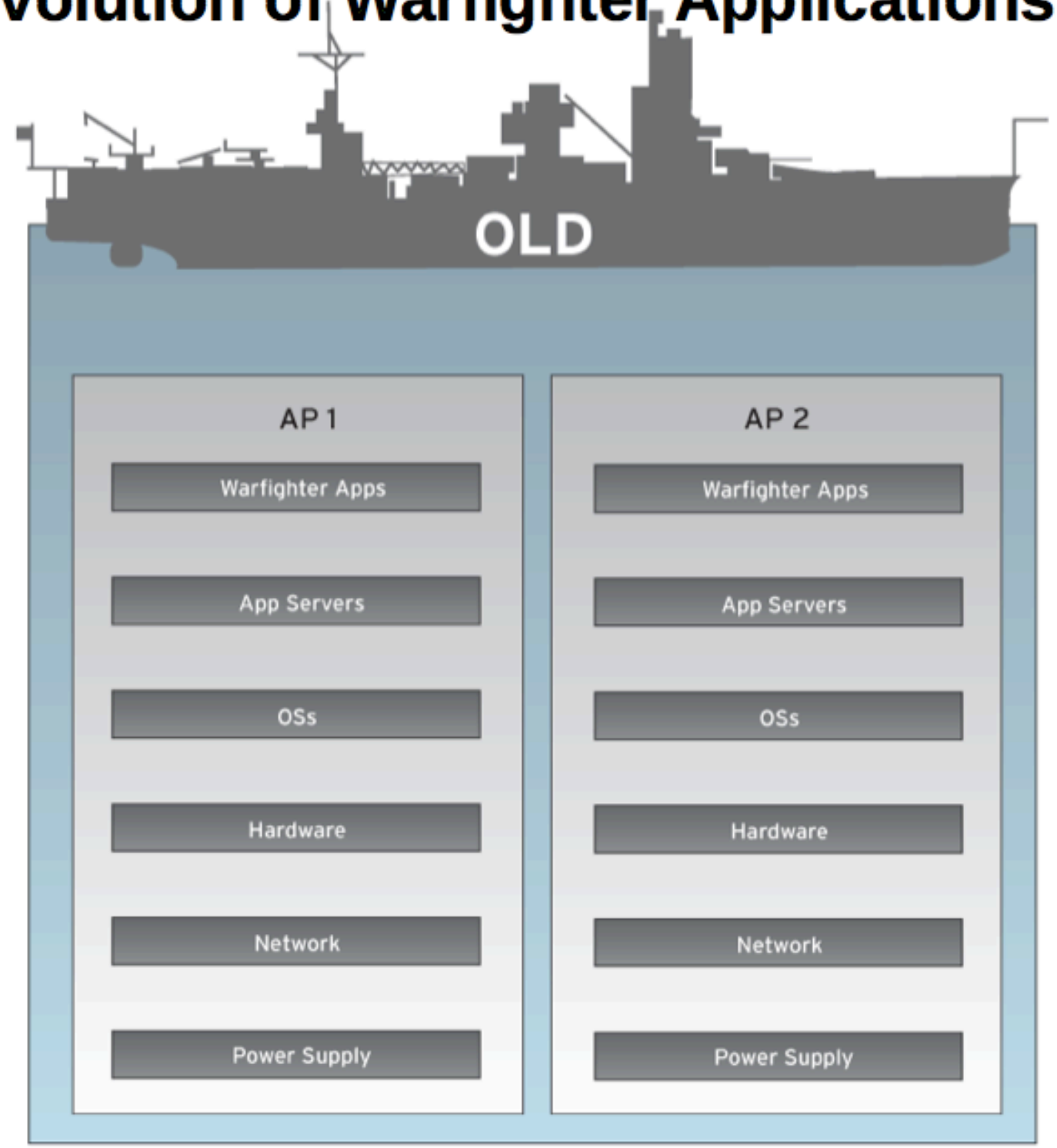
WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
  - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE
- Platform as a Service (PaaS)
  - DLT CODEvolved, Autonomic ARCWRX

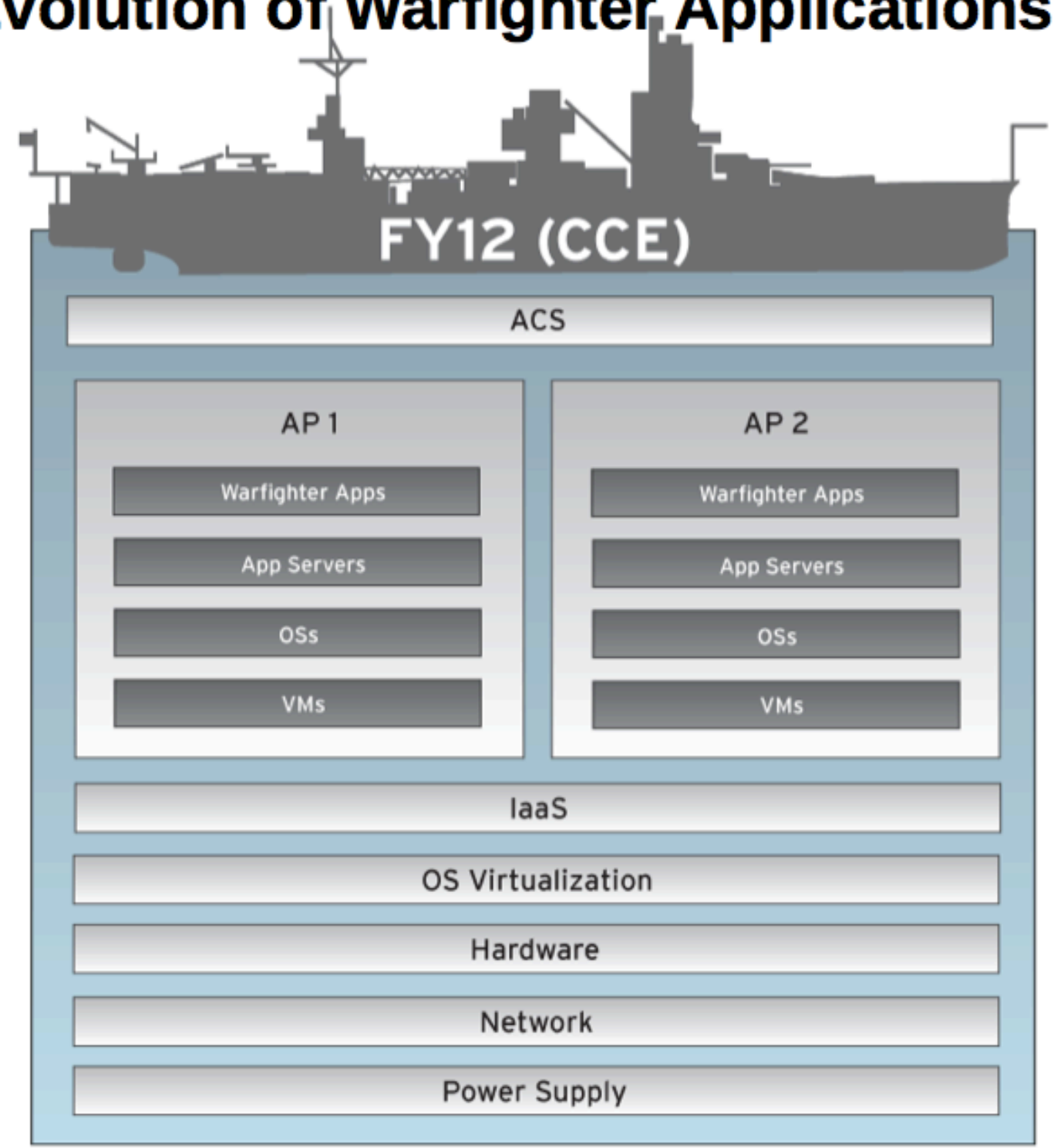
WHAT IS THE CLOUD?

- Infrastructure as a Service (IaaS)
  - CIA C2S, NSA MACHINESHOP, ARC-P, Westfield's MITE
- Platform as a Service (PaaS)
  - DLT CODEvolved, Autonomic ARCWRX
- Software as a Service (SaaS)
  - salesforce.com

Evolution of Warfighter Applications



Evolution of Warfighter Applications



Evolution of Warfighter Applications

FY12 (ACS)

ACS Enterprise Services

AP 1

Warfighter Apps

ACS Platform Services

AP 2

Warfighter Apps

ACS Platform Services

IaaS

OS Virtualization

Hardware

Network

Power Supply

Evolution of Warfighter Applications

PLATFORM SERVICES	PAAS
App providers build to vendor products	App providers build to DoD standard
Changing middleware vendor requires work from all app providers	Changing middleware vendor is invisible to all app providers
Static scaling	Dynamic scaling
Makes it easier for app providers to build C&A'd environments	Removes need for app provider to build C&A'd environments
Build / deploy apps in months / years	Build / deploy apps in days
RHEL+JBoss, Windows+BEA Solaris+Oracle	Google AppEngine

Evolution of Warfighter Applications

PROPOSED

ACS Enterprise Services

AP 1

Warfighter Apps

AP 2

Warfighter Apps

DoD AppEngine (PaaS)

AS

DB

??

IaaS

OS Virtualization

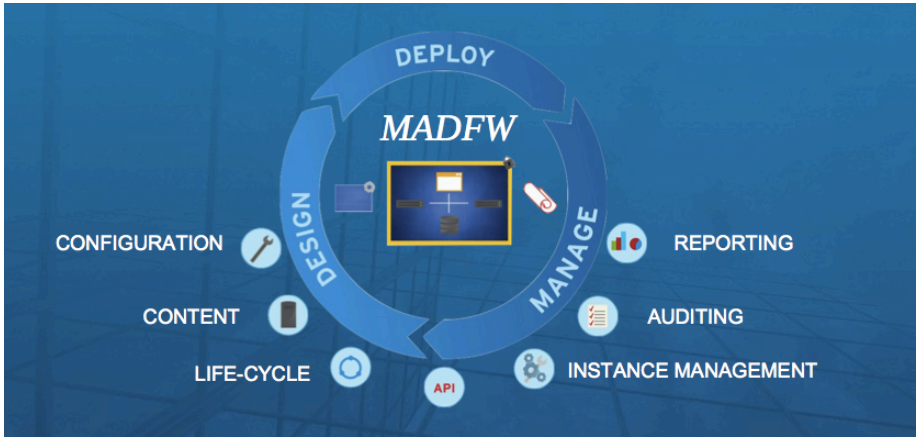
Hardware

Network

Power Supply

IaaS Case Study: Westfield's MADFW

- Also known as MITE, falls under MID
- Development environment for ~117 tenants
- Anything beyond operating system is responsibility of tenant (applications, continuous monitoring, etc)
- ICD 503, High/Low/Low



Continuous Monitoring

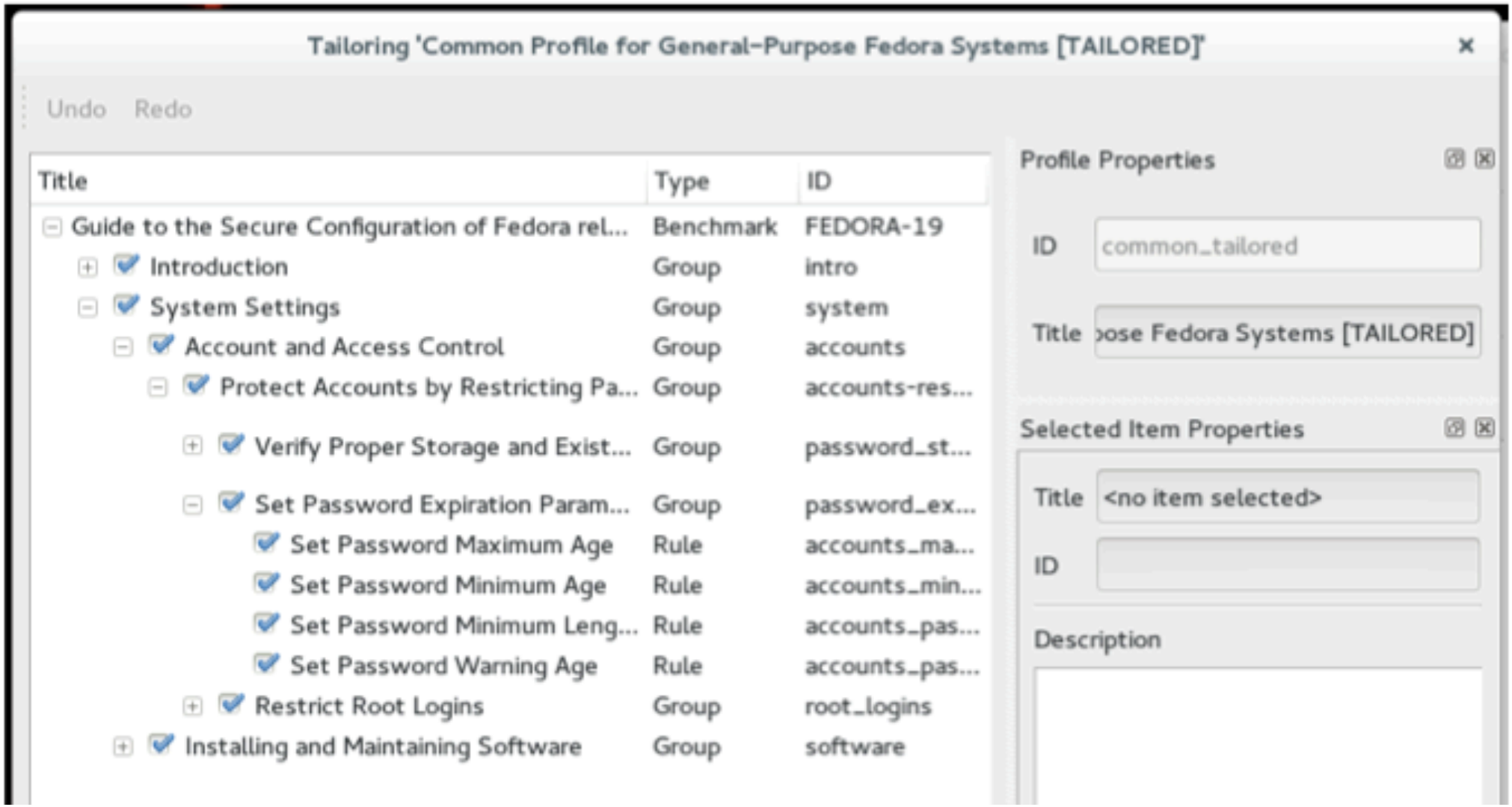
- NIST 800-53, 800-137, and many other regulations require continuous monitoring

- We've been using the SCAP Security Guide
  - Large body of Linux security controls
  - Logically grouped into profiles (e.g. DoD STIG, FISMA Moderate, C2S…)

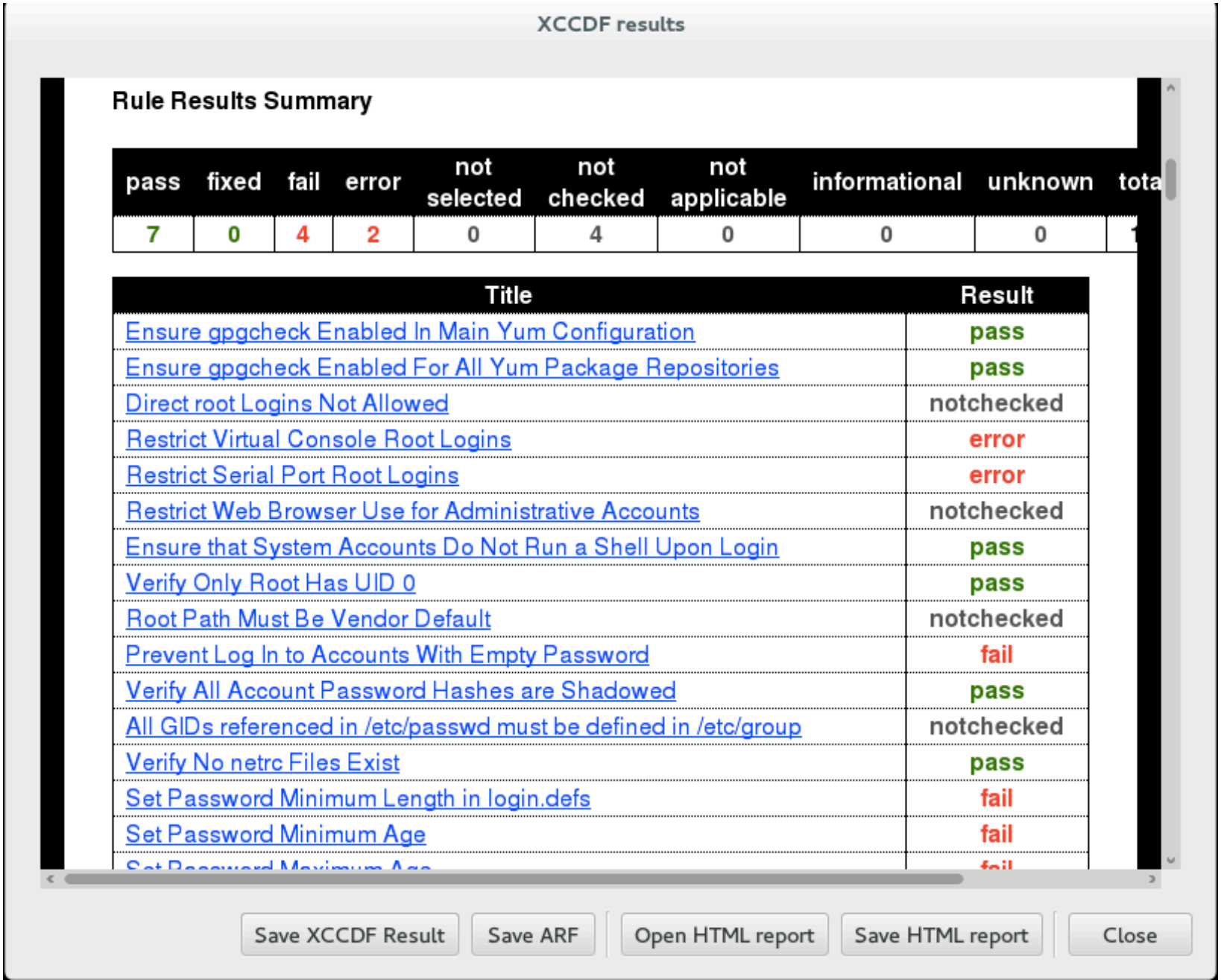
  https://fedorahosted.org/scap-security-guide/

Contributors Include . . .

Control Tailoring



Sample Output



SCAP Content Repositories

NIST maintains SCAP content repository for U.S. Government. Plenty of non-Linux content!

http://web.nvd.nist.gov/view/ncp/repository

MADFW v2: PaaS (via containers)

- Think of the containers as boxes, nodes as the truck
- We don’t care what’s inside the box, it’s just cargo

Multi-tenancy

RHEL

HYPERVISOR (RHEV, OpenStack, KVM, even VMWare…)

Multi-tenancy

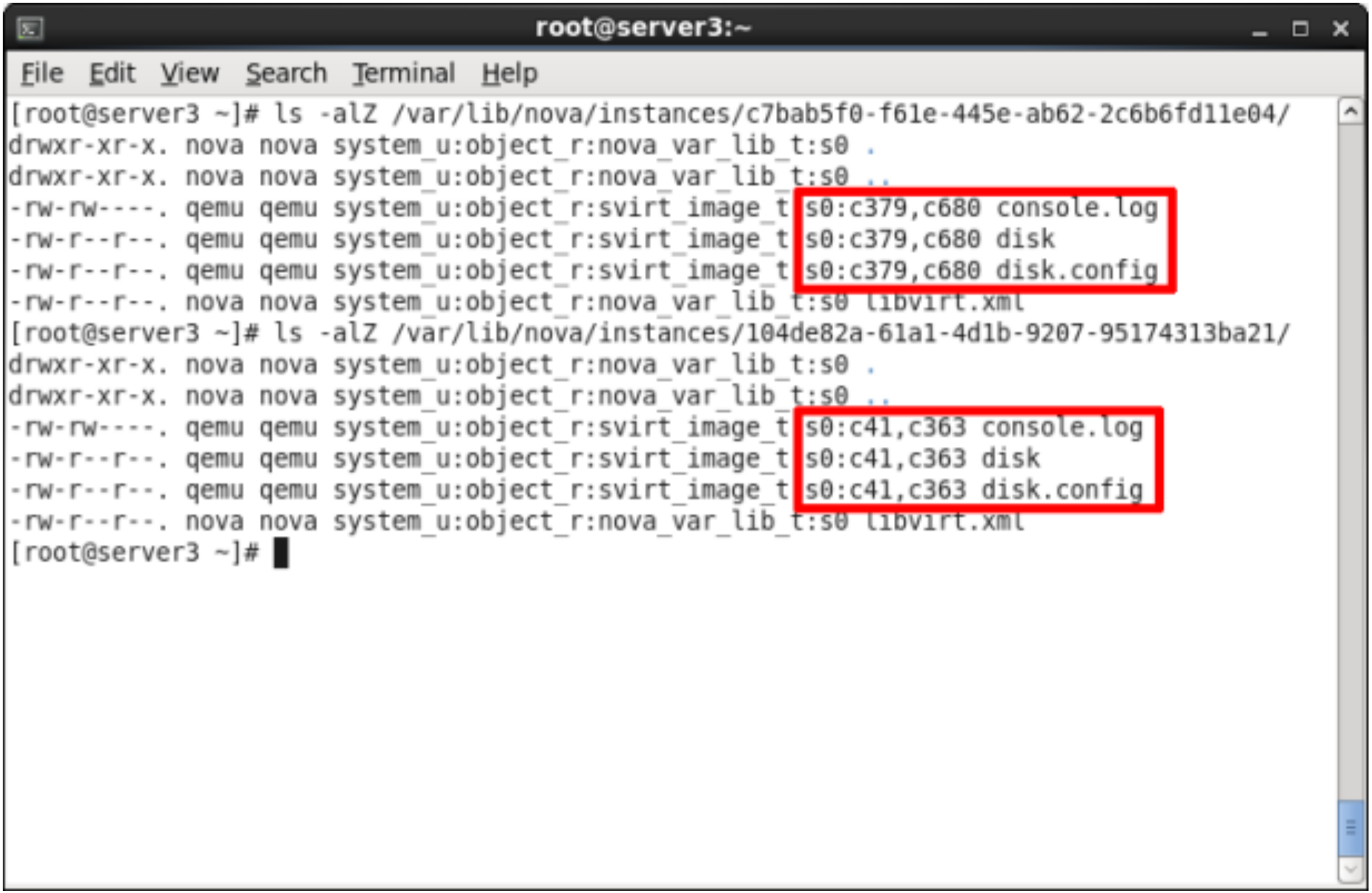
system_u:system_r:svirt_t:s0:c379,c680

system_u:system_r:svirt_t:s0:c41,c368

RHEL

HYPERVISOR (RHEV, OpenStack, KVM, even VMWare…)

Multi-tenancy




WE CAN DO MORE
WHEN WE WORK
TOGETHER