



# Identity Management and Compliance in OpenShift

Or “Use DevOps to Make Your Auditors and Suits Happy”

Marc Boorshtein  
CTO, Tremolo Security

Ellen Newlands  
Senior Security Product Manager, Cloud Business Unit at Red Hat

May 3, 2017

# Who Are We?

Marc Boorshtein - CTO Tremolo Security, Inc.

- 15+ years of identity management implementation experience
- Multiple deployments across large commercial and federal customers

Ellen Newlands - Senior Security Product Manager, Cloud Business Unit at Red Hat

- Red Hat Product Manager for Identity and Access Management
- Extensive experience in enterprise and WEB identity management and single sign-on

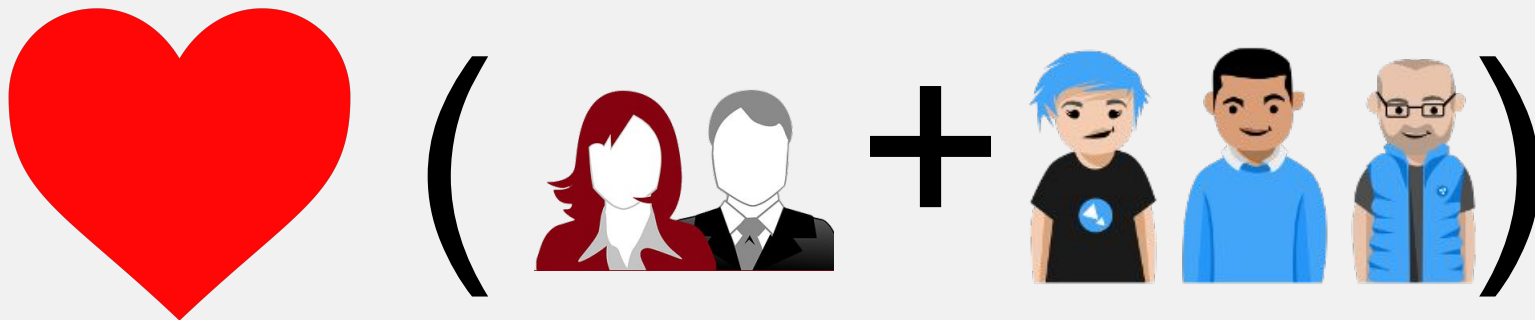
# What Will We Be Talking About?

- Why is identity management and compliance important to you?
- What is “compliance”?
- How does identity management apply to compliance?
- How does Red Hat and OpenShift manage security?
- What “compliance” looks like without and with DevOps
- How OpenShift manages it’s identities
- Demo!

# Why is Compliance Important to You?

It's not just for meetings and auditors...

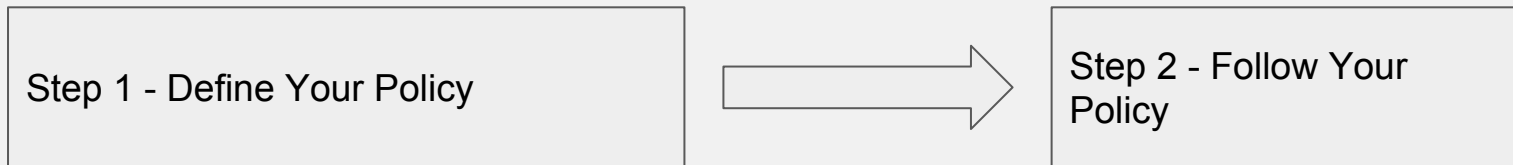
## DevOps + Identity Management =



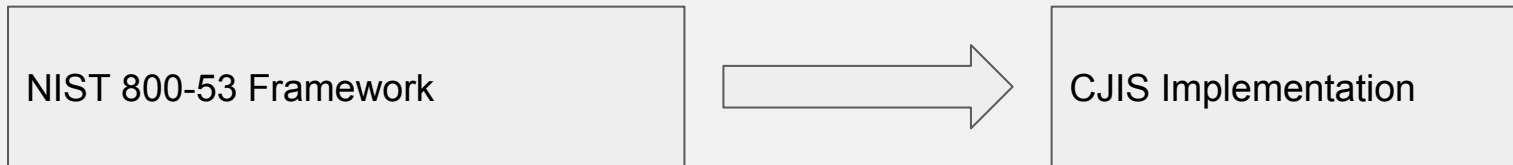
# What is Compliance?

When someone asks if you're compliant...

NIST 800-53

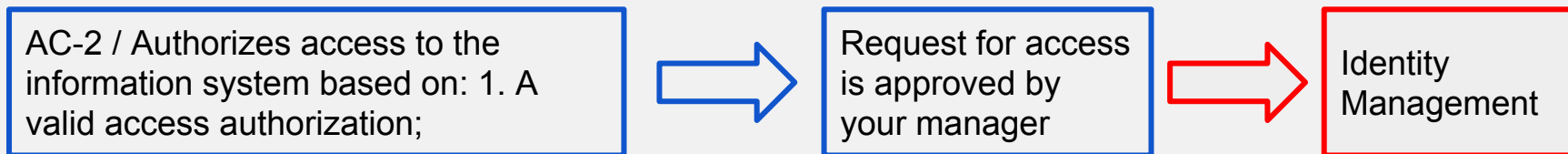


Criminal Justice Information Systems (CJIS)

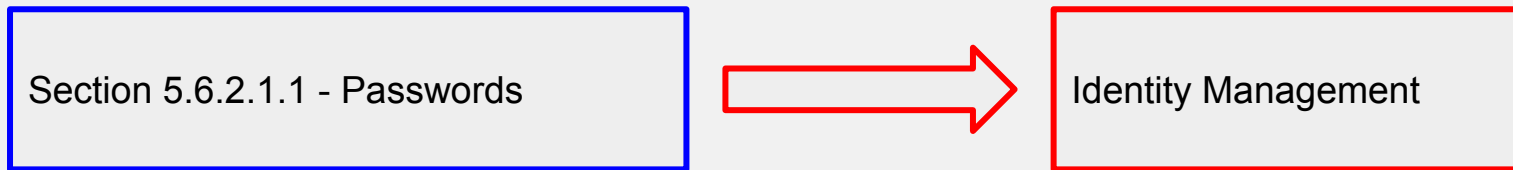


# Where Does Identity Management Fit?

NIST 800-53



Criminal Justice Information Systems (CJIS)



# OpenShift Container Platform Security

Integrated security features including

- Role-based Access Controls with LDAP and OAuth integration
- Privilege access management
- Automated certificate management
- Scalable secrets management
- Private data and logins exchanged with OpenShift are transmitted over SSL
- Application passwords are filtered from OpenShift log files and encrypted.
- Pushing and pulling of private data is done over SSH
  - Authenticated with keys, not passwords,
  - This helps prevent brute force cracking
  - Tools are available for users to deploy similar steps for their applications

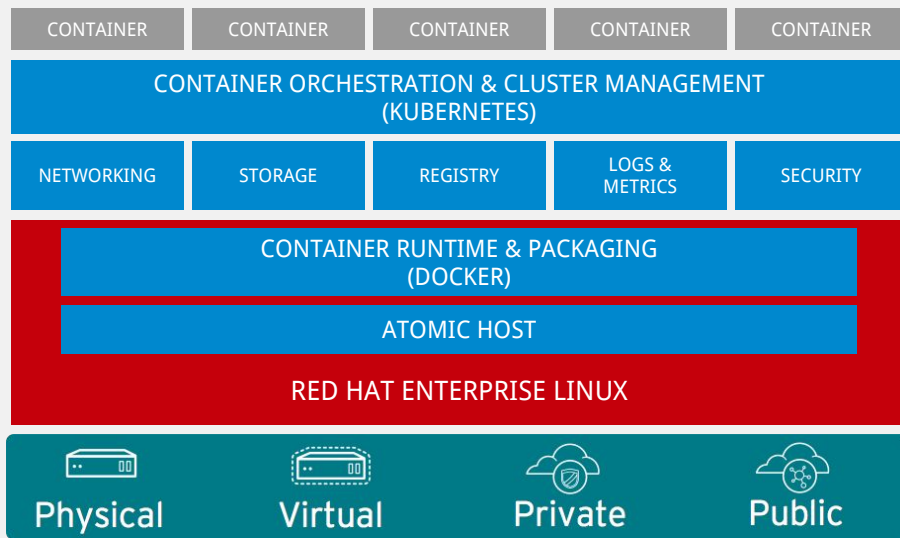
Visit the Security zone in the Red Hat booth for more information on OpenShift & container security

# Red Hat Enterprise Linux: Support Compliance for OpenShift

Red Hat Enterprise Linux provides the foundation for secure, scalable containers

On bare metal, on Red Hat Virtualization

In your datacenter or the public cloud



Red Hat provides industry-leading responsiveness to security vulnerabilities

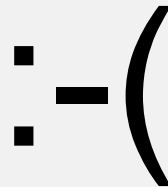
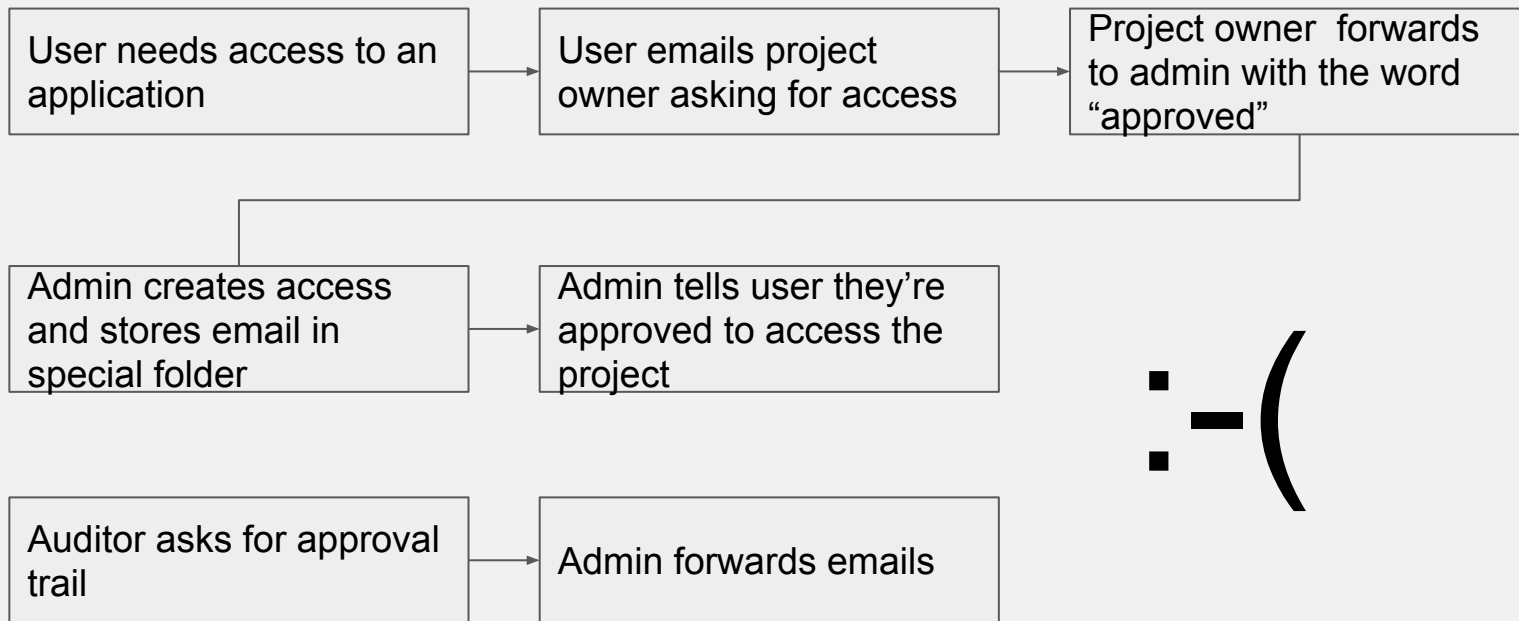
Red Hat OpenShift Dedicated available on both AWS & GCP

OpenShift on public cloud inherits the security features of your public cloud provider

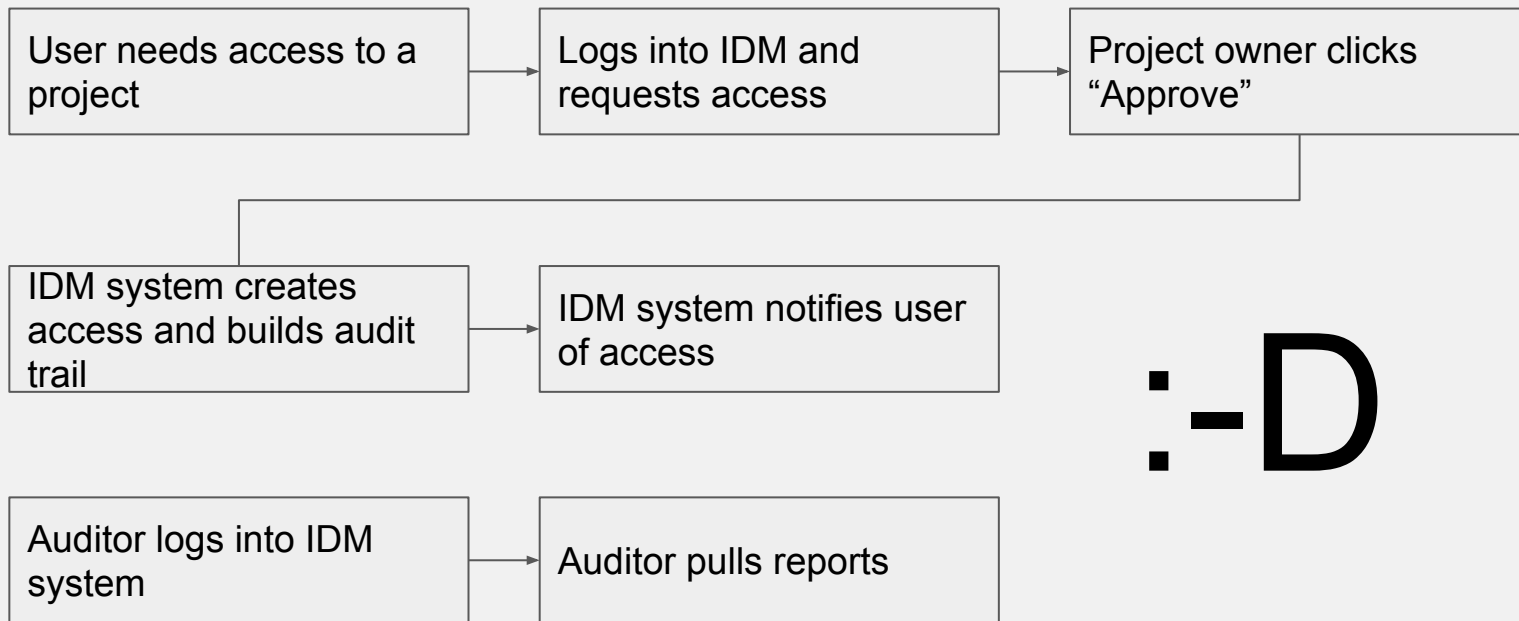
For example, to know more about [the security of Amazon EC2](#)



# Identity Management Compliance Without DevOps



# Identity Management Compliance With DevOps



:-D

# How this applies to OpenShift

## WHO?

- User Object in EtcD
- LDAP
- OpenID Connect
- Reverse Proxy + Header

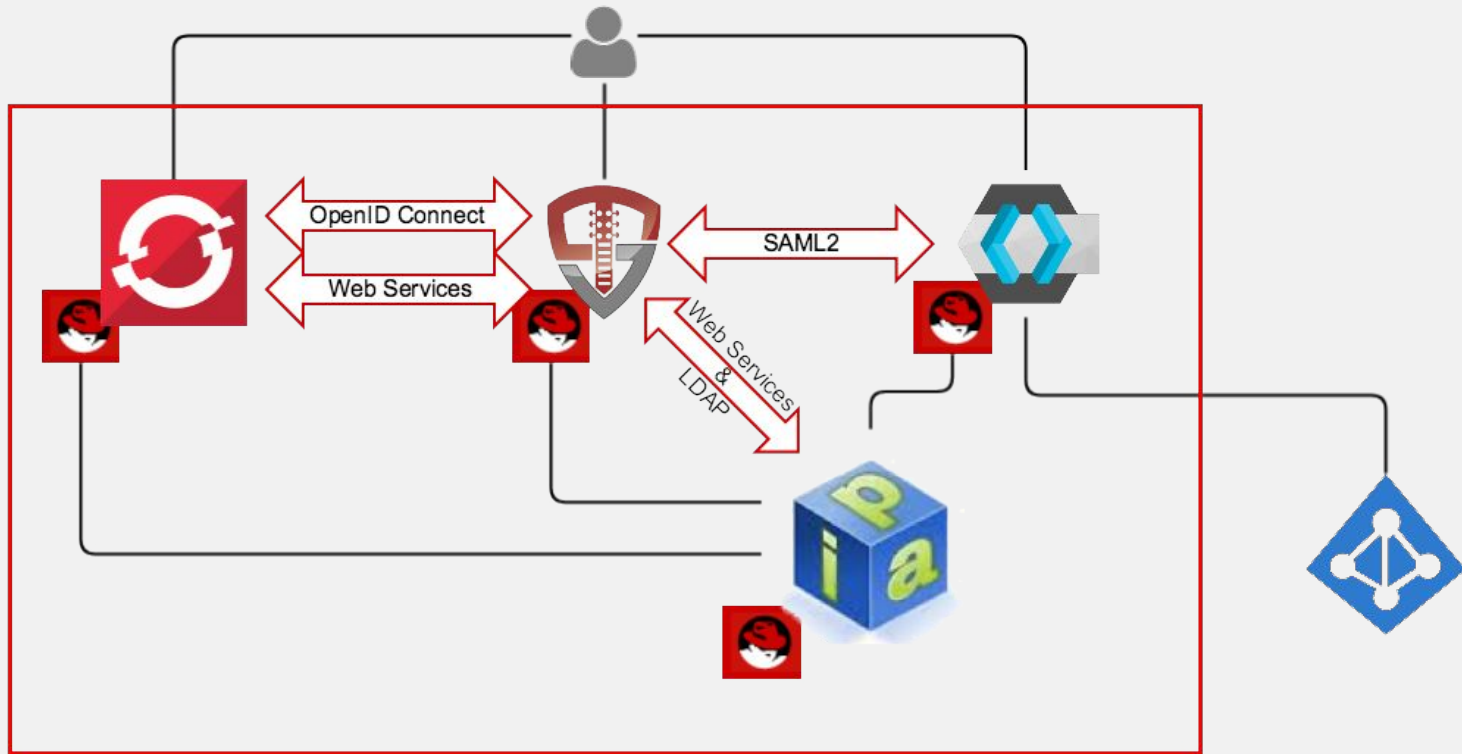
## WHAT?

- Subject + Role + Project = RoleBinding
- Local Objects
- Management
  - OpenShift Console
  - LDAP Sync
  - oadm
  - Web services

## WHY?

- External Workflow

# Demo



# DEMO

# Shameless Self Promotion



- Booth 145
  - Mobile Battery Chargers
  - Screen Cleaners
- Web - <http://tremolo.io>
- Twitter - @tremolosecurity / @mlbiam
- Github - <https://www.github.com/tremolosecurity/>
- Blog this session is based on - <https://www.tremolosecurity.com/openshift-compliance-and-identity-management/>

RED HAT  
**SUMMIT**

# THANK YOU



[plus.google.com/+RedHat](https://plus.google.com/+RedHat)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)







[twitter.com/RedHatNews](https://twitter.com/RedHatNews)





[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)

# How this applies to OpenShift

Layer	Technology	In Demo
Cloud   	<ul style="list-style-type: none"><li>• OpenStack - Keystone</li><li>• Amazon - IAM</li><li>• etc</li></ul>	N/A
Operating System  redhat	<ol style="list-style-type: none"><li>1. LDAP</li><li>2. AD</li><li>3. SSSD</li></ol>	Red Hat Identity Management



# How this applies to OpenShift

Layer	Technology	In Demo
OpenShift Console and CLI 	Authentication <ul style="list-style-type: none"><li>• LDAP</li><li>• Password File</li><li>• OpenID Connect</li><li>• Header + Reverse Proxy</li></ul> Authorization <ul style="list-style-type: none"><li>• Internal User and Group objects</li><li>• Web services</li><li>• LDAP Sync</li></ul>	Authentication <ul style="list-style-type: none"><li>• Username + Password - KeyCloak</li><li>• U2F - Unison</li><li>• Compliance Banner - Unison</li><li>• OpenID Connect</li></ul> Authorization <ul style="list-style-type: none"><li>• Unison self service</li></ul>
Container 	<ol style="list-style-type: none"><li>1. External Identity Provider</li><li>2. External User System</li></ol>	N/A

The Red Hat Summit logo is a red speech bubble shape with the words "RED HAT" in a smaller font above the word "SUMMIT" in a larger font, both in white.

**RED HAT**  
**SUMMIT**

**LEARN. NETWORK.  
EXPERIENCE  
OPEN SOURCE.**