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

- Step 1 - Define Your Policy
- NIST 800-53 Framework

Criminal Justice Information Systems (CJIS)

- Step 2 - Follow Your Policy
- CJIS Implementation
Where Does Identity Management Fit?

NIST 800-53

AC-2 / Authorizes access to the information system based on: 1. A valid access authorization;

Request for access is approved by your manager

Identity Management

Criminal Justice Information Systems (CJIS)

Section 5.6.2.1.1 - Passwords

Identity Management
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 provides the foundation for secure, scalable containers on bare metal, on Red Hat Virtualization, in your datacenter or the public cloud. Red Hat OpenShift is dedicated and 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, Red Hat provides industry-leading responsiveness to security vulnerabilities.
Identity Management Compliance Without DevOps

User needs access to an application

User emails project owner asking for access

Project owner forwards to admin with the word “approved”

Admin creates access and stores email in special folder

Admin tells user they’re approved to access the project

Auditor asks for approval trail

Admin forwards emails

:-(
Identity Management Compliance With DevOps

User needs access to a project → Logs into IDM and requests access → Project owner clicks “Approve”

IDM system creates access and builds audit trail → IDM system notifies user of access

Auditor logs into IDM system → Auditor pulls reports
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
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/
THANK YOU

plus.google.com/+RedHat
linkedin.com/company/red-hat
youtube.com/user/RedHatVideos
facebook.com/redhatinc
twitter.com/RedHatNews

#redhat #rhsummit
How this applies to OpenShift

<table>
<thead>
<tr>
<th>Layer</th>
<th>Technology</th>
<th>In Demo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud</td>
<td>• OpenStack - Keystone</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>• Amazon - IAM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• etc</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>1. LDAP</td>
<td>Red Hat Identity Management</td>
</tr>
<tr>
<td></td>
<td>2. AD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. SSSD</td>
<td></td>
</tr>
</tbody>
</table>
# How this applies to OpenShift

<table>
<thead>
<tr>
<th>Layer</th>
<th>Technology</th>
<th>In Demo</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenShift Console and CLI</td>
<td>Authentication</td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>● LDAP</td>
<td>● Username + Password - KeyCloak</td>
</tr>
<tr>
<td></td>
<td>● Password File</td>
<td>● U2F - Unison</td>
</tr>
<tr>
<td></td>
<td>● OpenID Connect</td>
<td>● Compliance Banner - Unison</td>
</tr>
<tr>
<td></td>
<td>● Header + Reverse Proxy</td>
<td>● OpenID Connect</td>
</tr>
<tr>
<td></td>
<td>Authorization</td>
<td>Authorization</td>
</tr>
<tr>
<td></td>
<td>● Internal User and Group objects</td>
<td>● Unison self service</td>
</tr>
<tr>
<td></td>
<td>● Web services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● LDAP Sync</td>
<td></td>
</tr>
<tr>
<td>Container</td>
<td>1. External Identity Provider</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>2. External User System</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
LEARN. NETWORK. EXPERIENCE OPEN SOURCE.