CONTAINERS TODAY

27-6-2019

The Hague

Powered by Amazic
Market Development
Hot, hotter, hottest

running a compliant container platform
for the banking industry

Containers Today (27-06-2019)
ABN AMRO
Roland Schijvenaars & Wiebe de Roos
About us – Wiebe de Roos

Wiebe de Roos
CI/CD Consultant & Engineer
https://www.linkedin.com/in/wiebe-de-roos

ABN·AMRO
About us – Roland Schijvenaars

Roland Schijvenaars
Cloud native consultant
[LinkedIn profile link]

ABN·AMRO
Table of Contents

1 Introduction

2 Recap Containers Today 2018

3 Container Security

4 Managed Container Platform

5 Compliance as Code

6 Containers Tomorrow
ABN AMRO is a leading bank with an operating income of EUR 8.588 million. Headquartered in Amsterdam, ABN AMRO has 22,000 employees servicing retail, private, and corporate finances worldwide. 5,000 associates work in IT, and there are 350+ agile teams. The image also shows a cartoon character with the text "Agile Dev + IT Ops = DevOps!" suggesting a focus on collaboration, communication, integration, and automation in the context of Agile Development and IT Operations.
1. Container Journey

- Jenkins Core in AWS
- Container platform EKS
- Container platform AKS

- 2017: First Docker PoCs
- 2018: Twistlock
- 2019 Q1: Open Policy Agent
- 2019 Q2
- 2019 Q3
- 2019 Q4?
2. Container Initiatives – 2017-2018

- **First Docker PoCs**
  - **2017**
- **Jenkins Core in AWS**
  - **2018**
- **Container platform EKS**
  - **2019 Q1**
- **Container platform AKS**
  - **2019 Q2**
  - **2019 Q3**
  - **2019 Q4?**

- **Twistlock**
- **Open Policy Agent**
2. Recap – Containers Today 2018

Dockerizing the Enterprise – fast & secure

✓ Docker use cases
✓ Docker (image) pipelines
✓ CI platform: from VMs to Containers
✓ Containers in the enterprise
✓ Container security
3. Container Security - Twistlock

- Jenkins Core in AWS
- Container platform EKS
- Container platform AKS

- 2017: First Docker PoCs
- 2018: Twistlock
- 2019 Q1: Twistlock
- 2019 Q2
- 2019 Q3: Open Policy Agent
- 2019 Q4?
3. Container Security Journey

2018H2
- Container Security RFP
- Twistlock selected

2019Q1
- Twistlock in Production
- Docker image pipeline + Twistlock scans
- Scanning 3rd party Docker Images

2019Q2
- Standards & guidelines
- Rollout for all teams
- Container scanning in current way of working

2019Q3
- Fix critical issues
- Runtime protection
- Triage process in place

Communication, knowledge sharing, training
3. Context of Twistlock

Main features:
- Vulnerability scanning
- Runtime protection
3. Vulnerability Scanning Example

Scan details

<table>
<thead>
<tr>
<th>Image</th>
<th>ataf/apache-jmeter-5.1.1.v1.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>sha256:5216e36c758416c75ea6f717ef1f4d36054411cb0c3ec7def8a5927e8ad9f4</td>
</tr>
<tr>
<td>OS distribution</td>
<td>Alpine Linux v3.8</td>
</tr>
<tr>
<td>Scan Status</td>
<td>Failed</td>
</tr>
<tr>
<td>Vulnerability threshold</td>
<td>low</td>
</tr>
<tr>
<td>Compliance threshold</td>
<td>low</td>
</tr>
</tbody>
</table>

Vulnerabilities

<table>
<thead>
<tr>
<th>Id</th>
<th>Type</th>
<th>Highest Severity</th>
<th>Description</th>
<th>Show details</th>
</tr>
</thead>
<tbody>
<tr>
<td>411</td>
<td>Binary</td>
<td>critical</td>
<td>java version 1.8.0.181 has 18 vulnerabilities.</td>
<td>Show details</td>
</tr>
<tr>
<td>46</td>
<td>OS</td>
<td>critical</td>
<td>openjdk8 (used in openjdk8.jre, openjdk8.jre-base, openjdk8.jre-lib, openjdk8) version 8.181.13-r0 has 12 vulnerabilities.</td>
<td>Show details</td>
</tr>
<tr>
<td>49</td>
<td>nodejs</td>
<td>high</td>
<td>jquery version 2.1.3 has 2 vulnerabilities.</td>
<td>Show details</td>
</tr>
<tr>
<td>47</td>
<td>jar</td>
<td>high</td>
<td>com.fasterxml.jackson.core.jackson.databind version 2.9.8 has 1 vulnerability.</td>
<td>Show details</td>
</tr>
</tbody>
</table>

Criticals should be fixed or mitigated
3. Container Runtime Protection Example

docker: Error response from daemon: OCI runtime create failed: [Twistlock] Image operation blocked by policy: allow-whitelisted-images-only, has 1 compliance issues:

This container is not allowed, since the image is not whitelisted by ABNAMRO. Only images from ABN AMRO NEXUS are allowed.
Container platform team

Stratus

“low-level clouds characterized by horizontal layering with a uniform base.”
4. Managed Container Platform

- Jenkins Core in AWS
- Container platform EKS
- Container platform AKS

- 2017
  - First Docker PoCs

- 2018
  - Twistlock

- 2019 Q1
  - Open Policy Agent

- 2019 Q2
- 2019 Q3
- 2019 Q4?
4. Main Objectives

Build a platform which is:

- **Easy to use**
  - Provision in minutes
  - One stop shop for developers
  - All workloads supported

- **Secure**
  - Security framework in place
  - Vulnerability & Compliance detection
  - Container protection

- **Portable**
  - Workloads can run on AWS and Azure
  - Loose coupling cloud native components

- **Reusable**
  - Everything as code
  - Compliance framework
  - Knowledge of containers, Kubernetes etc.
4. Conceptual Framework

- Application
- Pipeline
- Platform
- Governance
- Managed Container Platform
- Go Live

Assessment
## 4. Component overview

<table>
<thead>
<tr>
<th>Level</th>
<th>Application</th>
<th>Orchestration</th>
<th>Runtime</th>
<th>Provisioning</th>
<th>Infra</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>App definition &amp; Image build</td>
<td>CI/CD</td>
<td>Scanning</td>
<td>Persistent storage</td>
<td>Network</td>
</tr>
<tr>
<td>APPLICATION</td>
<td>Helm</td>
<td>cloudbees</td>
<td>Azure DevOps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ORCHESTRATION</td>
<td>Amazon EKS</td>
<td>Azure AKS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RUNTIME</td>
<td>To be determined</td>
<td>Docker</td>
<td>CN</td>
<td></td>
<td>Secrets</td>
</tr>
<tr>
<td>PROVISIONING</td>
<td>Automation &amp; Config</td>
<td>Docker Registry</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INFRA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. Compliance as Code - Open Policy Agent (OPA)

- Jenkins Core in AWS
- Container platform EKS
- Container platform AKS

- First Docker PoCs
- Twistlock
- Open Policy Agent

Timeline:
- 2017
- 2018
- 2019 Q1
- 2019 Q2
- 2019 Q3
- 2019 Q4?
5. Policy Enforcement with OPA

Compliance Officers

Container Platform Team

OPA Policies

Cluster Policies

Docker Pipeline

Helm Pipeline

Infra as Code Pipeline
5. OPA Policy Enforcement Example

Prevent deployments of containers with a public facing endpoint, applications can only be accessed via the ABN AMRO internal network.

```rego
package kubernetes.admission
import data.kubernetes.namespaces
import input.request.object.metadata.annotations as annotations
deny[msg] {
  input.request.kind.kind = "Service"
  input.request.operation = "CREATE"
  input.request.object.spec.type = "LoadBalancer"
  missing_required_annotations[msg]
}
# Require annotation which matches an annotation on the target namespace
missing_required_annotations[msg] {
  namespace_sg := namespaces[input.request.namespace].metadata.annotations["elb-security-group"]
  not annotations["service.beta.kubernetes.io/aws-load-balancer-security-groups"] = namespace_sg
  msg = sprintf("LoadBalancer Services in namespace %q must use security group %q", [input.request.namespace, namespace_sg])
}
```
6. Containers Tomorrow

- **First Docker PoCs** (2017)
- **Jenkins Core in AWS** (2018)
- **Twistlock** (2019 Q1)
- **Container platform EKS** (2019 Q2)
- **Open Policy Agent** (2019 Q3)
- **Container platform AKS** (2019 Q4?)
6. Reuse for AKS

Goal:

• Support workloads on Microsoft Azure while re-using as much as possible.

Advantages of Container Platform:

• Build once – run in AWS and Azure
• One source of truth for (code) compliance
• Security is maintained centrally
• Workloads are truly portable
• Kubernetes knowledge is spread at the organization
The Stratus Container Platform is:

- Easy to use
- Secure
- Portable
- Reusable
Questions?

Wiebe de Roos
https://www.linkedin.com/in/wiebe-de-roos

Roland Schijvenaars
https://nl.linkedin.com/in/rschijvenaars