## Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Min</td>
<td>DevOps WG Update (Fuji)</td>
<td>James</td>
</tr>
<tr>
<td>10 Min</td>
<td>SonarCloud Issues</td>
<td>Trevor</td>
</tr>
<tr>
<td>30 Min</td>
<td>Release Update / Geneva Planning</td>
<td>Lisa / Jim</td>
</tr>
<tr>
<td>10 Min</td>
<td>Opens</td>
<td></td>
</tr>
</tbody>
</table>
Attendees
DevOps WG Update

Fuji Scope

Static Code Analysis Tools

- Snyk Integration with Jenkins - **DONE**
- GitHub Repo / Snyk Integration
  - Integrate GitHub Organization – Snyk set up as ‘edgex-Jenkins’
  - Integration with the repo (app-service-configurable) - **DONE**
    - Added Scan stage to Jenkinsfile (app-service-configurable)
    - Modified the Snyk global library to call monitor method as part of the Jenkins Pipeline
  - Add additional integration for ongoing Docker image scan - Docker Hub
    - Issue with docker-edgex-mongo image identified
    - Weekly scans now report NEW vulnerabilities if found
  - Configure notifications to SIR team members – **DONE**
    *Note: several invitations pending*
    - Slack integration with Snyk – new scope **DONE**
  - Email notifications in the Free plan go to Snyk Administrator – Everyone added has the same role.
  - Budget request for Standard plan
    - Supports additional reporting and RBAC for Collaborator role
- New device services – **BLOCKED**
- git-semver bug - **WIP**
Follow Up – WW38

• Action Items
• Help Needed - support-rules engine
  • Issue needs to be created for support-rules engine
  • May require additional support from DevOps

Is this still an open - Yes
Latest image isn’t including the java code – something in the build
Image gets tagged with latest commit, but code doesn’t match that.
- Create a new Issue to address / pull in
Snyk Dashboard
Slack integration - #snyk-reports

snyk-bot 7:41 AM

CVE-2019-5094
New vulnerability in package e2fsprogs/e2fsprogs at the edgex-jenkins organization.

Severity: Low
Package: e2fsprogs/e2fsprogs

Issue ID: SNYK LINUX-E2FSPROGS-468973

Affected projects:
- edgexfoundry/docker-edgex-mongo:1.0.1
  Package version: 1.42.12-2+b1
- edgexfoundry/docker-edgex-mongo:latest
### Helpdesk Ticket # | Description | Details | Status
--- | --- | --- | ---
IT-17609 | IT-17609 Add additional contacts to a JSD ticket | Unable to add Lisa to the JSD tickets using LFID or GitHub ID | RESOLVED

---

#### Help Center

**Requests**

- Open requests
- **EdgeX**
- Any request type
- Search for requests

No requests were found.

Try modifying your search criteria or create a request.
Backlog Review
SonarCloud – Duplicated Code

- Edgex-go PR with a single character change introduced MAJOR issue with identification of Duplicated Code
  - Trevor created custom Sonar profile for EdgeX Way to remove assessment of any Duplicated Code

Discussion / Help Needed

AR: Open ticket up with Sonar and try to figure out what caused it?
Fuji Release Update (Lisa)

Current Developer Experience

• Currently with the CI infrastructure developers have to make changes in several repositories; ci-management and their own repositories
• The builds maintained in ci-management are versioned separately from the code they are building causing potential problems
• Developers have to understand JJB and the sandbox to update their job
  • In most cases this is too big of a heavy lift for developers to engage
Geneva Transformation: Architecture
How long does it take? Is this all Geneva scope?

Geneva Transformation

Phase 1
- Research Spikes
- Plugin Setup and Configuration
  - Jenkinsfile
  - Jenkinsfile.sandbox

Phase 2
- Jenkinsfile templates
- Implementation details get solidified
- Refactor existing pipelines to use new templates

Phase 3
- Existing Job Migration

Full Transformation by Geneva Release - April 2020
Meeting Minutes

• Expect Fuji Release date by EOW next week
  • Tracking to November

• Open issue related to - support-rules engine
  • Issue created in ci-management – Issue #492

• Sample-Service Discussion
  • AR: Email to TSC to vote on moving sample-service out of holding for DevOps test / validation of Pipelines and git-semver

• No existing policy that discusses what artifacts must get signed with sigul
  • AR: Need to Discuss with Jeremy Phelps - PR #318 for signing go-modules with sigul

• Feedback – Geneva Scope of Work
  • Streamlined Pipeline removes verification phase
  • Offers better Developer Experience
  • 3 Phases
    • Currently in Phase 1 - planning and pre-work
  • AR: Open JSD for help needed from LF to configure the Jenkins GitHub Org Plugin
    • Need to create required webhooks for top level Org
Geneva Planning

Scope Discussions
Geneva – DevOps

**In**
- Full Pipeline transformation for EdgeX services
  - Convert Jenkins JJB Freestyle jobs to Jenkins Pipelines
- Introduce GitHub Org Plugin
- Simplified Jenkinsfile
- Global Libraries to support Jenkins Pipeline transformation
- Add Unit testing to global-libraries (uncommitted) **
- Snyk integration for edgex services
  - As part of Jenkins Pipeline conversion
- Slack integration with Jenkins pipelines
- Nexus Cleanup / Lifecycle Policy

**Out**
- Alternate deployment/orchestration
  - Beyond Docker/Snaps
  - Kubernetes
  - Kata Containers
  - …
- Integration Test Pipelines
Fuji Planning

Scope Discussions
Fuji – DevOps

In
- Static code analysis tool identified and integrated into the EdgeX Jenkins Pipeline for Docker image scanning (Clair Server)
- Explore SAST for true static code analysis to include additional tooling such as Fortify / Coverity
- Code and artifact signing with semantic versioning
- Fix Documentation – edgex-go
  - Create a new repo for edgex-docs
- Build Performance Optimizations
  - Pipelines for EdgeX Foundry base build images
  - Basebuild images managed locally within Nexus
  - Leverage PyPi Proxy for local pip dependencies
  - ARM builds – optimization leveraging different high CPU build nodes / OS (ARM Team)

Out
- Alternate deployment/orchestration
  - Beyond Docker/Snaps
  - Kubernetes
  - Kata Containers
  - …
- SonarQube – SonarCloud is already in play in the LF
  - Decision: wait to see what codecov.io offers
- Suggestion to rename all of the Jenkins “arm” jobs so as to differentiate 32bit / 64bit architectures
- Full Pipeline transformation for EdgeX services
## EdgeX DevOps Commitments (Fuji)

### Scope of Work

<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add static artifact analysis into the EdgeX Jenkins Pipeline</td>
<td></td>
</tr>
<tr>
<td>(analysis of Docker /runtime artifacts, not the source code)</td>
<td></td>
</tr>
<tr>
<td>Add code and artifact signing with semantic versioning</td>
<td></td>
</tr>
<tr>
<td>Conduct build performance optimizations by:</td>
<td></td>
</tr>
<tr>
<td>• Adding Pipelines for EdgeX Foundry base build images</td>
<td></td>
</tr>
<tr>
<td>• Allow base build images to be managed locally within Nexus</td>
<td></td>
</tr>
<tr>
<td>• Leverage PyPi Proxy for local pip dependencies</td>
<td></td>
</tr>
<tr>
<td>Explore static code analysis like Checkmarx, Coverity, GuardRails, Synk, SonarQube</td>
<td></td>
</tr>
</tbody>
</table>

- Clair Server landing no longer at risk for Fuji
  - LF committed to implement on AWS and fund with expected completion next week
- gitsemver along with lftools used for artifact signing and semantic versioning
- Jenkins build performance optimizations for base build images completed
- All base build images will now be stored in Nexus (Snapshot):10003
- PyPi enabled as part of Edinburgh scope
- Initial review of GuardRails showed that the product was identifying issues which were not applicable for microservices architecture
# Past / Future Agenda Topics

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>WW36</td>
<td></td>
</tr>
<tr>
<td>WW37</td>
<td></td>
</tr>
</tbody>
</table>