DevOps Working Group

Thursday May 14, 2020
# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Topic</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 Min</td>
<td>Geneva Release - Opens</td>
<td></td>
</tr>
<tr>
<td>10 Min</td>
<td>Hanoi / DevOps Updates</td>
<td></td>
</tr>
<tr>
<td>10 Min</td>
<td>Snaps Discussion</td>
<td>All</td>
</tr>
<tr>
<td>10 Min</td>
<td>AOB / Opens</td>
<td>All</td>
</tr>
</tbody>
</table>
Attendees
DevOps WG Recap (Geneva)

Geneva (May 2020):

• DevOps Jenkins Pipeline Transformation
  • Introduced new Jenkins Global Libraries for build automation
    • Includes test framework for Groovy code
    • Explore underway to look into code coverage of Groovy code using Codecov.io
  • Semantic Versioning using Intel contributed utility (git-semver) enhanced to include test framework
  • Continuous Delivery via "release-kraken"
  • Developer Enablement – GitHub Project Tracker, GitHub Issue label creation automated, gitcommit linter implemented *
  • New ci-build images and global libraries developed to support Jenkins Pipelines
  • New life cycle policies implemented on Linux Foundation Nexus repositories
  • Automation of the labels across the project
  • GitHub Tracker (Kanban board) – utilized weekly with built in workflow
  • Developer Documentation created for new Jenkins Pipelines
  • Improved performance of all builds to include collaboration with Linux Foundation to drive performance improvements for ARM builds (~15 mins build performance improvements using a new flavor of LF build nodes)
    • X86 build nodes (VM) uses 4cpu – 2gb
    • Arm64 build nodes (VM) now uses 4 cpu – 16gb

DevSecOps scope includes:
• Snyk Advanced Reporting via Community Bridge - $8K savings on licensing for developer licenses
• Snyk Docker Hub image scans with weekly reports of new vulnerabilities
• Snyk CLI of Go integrated into scan stage of Jenkins Pipelines
• Clair image scans within scan stage of Jenkins Pipelines
• DevOps contributed code fixes to address CVEs found in images based on Snyk reporting
• Lftools updated to use latest version – code signing, git tag signing, Docker image signing
Geneva Freeze and Release

TSC approved

- Freeze: 12pm GMT, April 22 (Wed, week before planning meeting)
- Release: 12pm GMT, May 13 (Wed two weeks after planning meeting)

See Geneva release notes for details (on Slack)

**REMINDER:**
We will NOT be branching off master for the Geneva release.

Includes EVERYTHING

Will not be versioning go modules

Do we need blackbox tests to be an “artifact” of a release?

- QA/ Test WG doesn’t require signed tags, but since release kraken can be used to automate the creation of the tag, it would be a signed tag
- If there’s a need to patch Geneva, the tagged blackbox tests would be used
- Since blackbox tests wasn’t previously considered a “release artifact” does it get tagged? – YES it does

Decision: We now need to consider blackbox tests as a formal artifact. Tag would be generated at the time of the formal release
Geneva Release Schedule

Timeline to be reviewed for Geneva Retrospective

New scope – consider blackbox tests as artifact of the release
- should have been considered within review of ADR007

Green light decision to release
- TSC meeting late in the day
- Multiple issues worked throughout the day

support-rules-engine

Snap label / promotion issue identified
Geneva Retrospective – Next week

What went right? What could be improved?
DevOps WG Update

Hanoi

- **Performance Optimizations**
  - Build Optimizations for edgex-go
    - Explore completed and demo’d by Ernesto Ojeda with observable performance improvements in the build time
    - Trevor Conn / Core WG chair – gave green light in TSC call 05/13/20
      - Comments on review of last week’s DevOps WG meeting in Slack – #core channel

  ![Meeting Photo]

- **DevSecOps**
  - Community Bridge Feature Requests
    - Changes coming to the UI - removing export functionality of LICENSE data
  - Updated Snyk CLI to address incorrect version of Go on Snyk portal
  - Completed SDL milestones to allow for contribution of ghmetrics (automation of the paper study - Issue #1947)
  - Identified that Linux Foundation offers new tool - Nexus IQ (requires go.sum for all dependencies)
    - Next steps: Continue Discussion next week in Architect’s meeting

- **Other**
  - LFTools / Sigul latest version that supports Python 3.x
    - Need input from LF on alternative signing tool – LF to create a release and test, not looking at a replacement - is sigul project abandoned?
  - GitHub Issue Labels - ghsynch – Refactor to Python Script #26
    - Refactored code and enhancements to include Milestones
    - Optimized to address API throttling issue
Geneva release

<table>
<thead>
<tr>
<th>Completed</th>
<th>Work In Progress</th>
<th>Release Backlog</th>
</tr>
</thead>
<tbody>
<tr>
<td>217 (G wrap-up /H new)</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
Meeting Minutes

• Snaps release needs some rework – can’t manually retag in snapcraft
  • Need to fix labels - add story to backlog for Hanoi scope
  • Need to get cd to push to beta first - add story to backlog for Hanoi scope

• Issue identified with labels – cd is including the dev tag
Hanoi Planning

Scope Discussions
DevOps Scope of Work - Hanoi

• **Performance Optimizations**
  - Jenkins Pipeline optimizations for edgex-go
  - Explore options from LF for supporting Jenkins on K8s – completed roadmap review within Geneva
  - Explore alternatives to containerization within the builds
    - Explore use of BuildKit to simplify creation of x86/ARM build images so they share a single manifest when published to Docker Hub / Nexus
    - Explore use of Kanico
      - Explore Complete – **Will not Work**
        - Requires use of K8s persistent volumes and dedicated build agents which are long lived

• **Performance of the Build Environment**
  - Monitoring / Alerting optimizations (Continuous Improvement Opportunity)

• **Technical Debt**
  - Caching Dependencies – speed it up (upstream dependencies)

• **Open Horizons Enablement**
  - Shared Infra with Open Horizons
  - Build Automation for OH

• **Stretch Goals**
  - Code Coverage for Jenkins Global Libraries (codecov.io)
  - Snap improvements – build optimizations
  - Support for `--race` flag with goals to address with Go 1.15 …*but there are options*
Geneva Planning

Scope Discussions
# Fuji Release

- **Freeze:** Oct 23rd (Wednesday)
- **Release:** Nov 15th (Friday)

<table>
<thead>
<tr>
<th>Start Date: 10/23/19 (with extension)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>week 1</th>
<th>week 2</th>
<th>week 3</th>
<th>week 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>oct</td>
<td>nov</td>
<td>nov</td>
<td>nov</td>
</tr>
<tr>
<td>wed</td>
<td>wed</td>
<td>wed</td>
<td>wed</td>
</tr>
<tr>
<td>23</td>
<td>30</td>
<td>6</td>
<td>13</td>
</tr>
<tr>
<td>24</td>
<td>31</td>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>8</td>
<td>15</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>27</td>
<td>3</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>28</td>
<td>4</td>
<td>11</td>
<td>18</td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>12</td>
<td>19</td>
</tr>
</tbody>
</table>

- **Code Freeze**
- **EdgeX F2F in Phoenix**
- **Update Documentation, Compose Files and Bug Fixes**
- **Cut Fuji Branches**
- **GitHub Issues: Close / Mark for Geneva**
- **Create Fuji Jobs For Existing Repos**
- **Scan of EdgeX Images**
- **Open Tickets with LF for release on 11/15/19**
- **Finalize Release Notes**
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
- Code signing / Artifact signing **
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
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)**

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

<table>
<thead>
<tr>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size change to use Ubuntu / Debian base build images to support –race flag for Go Lang</td>
<td></td>
</tr>
<tr>
<td>Clair scan findings – Discussion developer community if we want to break the build when there’s findings</td>
<td>Bring into Security WG for discussion</td>
</tr>
<tr>
<td>Open Horizons enablement</td>
<td></td>
</tr>
<tr>
<td>Alignment to new LF roadmap self-service offerings – EdgeX use case for handling holding repositories</td>
<td></td>
</tr>
<tr>
<td>Release automation - key learnings and sharing with LF</td>
<td></td>
</tr>
<tr>
<td>Explore use of Buildkit</td>
<td></td>
</tr>
<tr>
<td>Explore use of Kanico</td>
<td></td>
</tr>
<tr>
<td>Snyk Dashboard Review</td>
<td></td>
</tr>
</tbody>
</table>
Attendees & Community Participation – ww14
Attendees & Community Participation – ww15
Attendees & Community Participation – ww16

Attendees

Participants (5 of 6)
- James Gregg (Intel) (Me)
- Ernesto Ojeda (Intel)
- tony espy
- Emilio Reyes (Intel)
- Jim White
- Lisa Rashidi-Ranjbar

Community Participation

- Intel
- IoTech
- Dell
- VMWare
- ARM
- Canonical
- LF
- Kong
Attendees & Community Participation – ww17

Community Participation

- Intel
- IoTech
- Dell
- VMWare
- ARM
- Canonical
- LF
- Kong