EDGEXFOUNDRY™

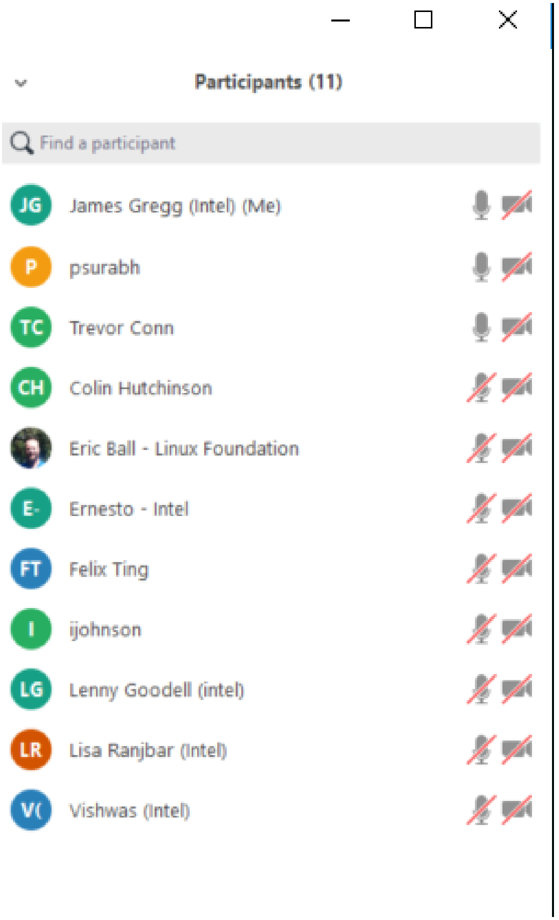
DevOps Working Group

Thursday May 16, 2019

Agenda

Time	Topic	Owner
10 min	Work Review (GitHub Project)	James Gregg
10 min	Backlog Review	James Gregg
10-15 min	Config Options Discussion	Trevor Conn
10 min	Explore Update: Clair / Klar Docker Image Scanning	James Gregg / Pradeep
	Opens	All

Attendees



Participants (11)

Find a participant

- JG James Gregg (Intel) (Me)
- P psurabh
- TC Trevor Conn
- CH Colin Hutchinson
- Eric Ball - Linux Foundation
- E- Ernesto - Intel
- FT Felix Ting
- I ijohnson
- LG Lenny Goodell (intel)
- LR Lisa Ranjbar (Intel)
- V(Vishwas (Intel)

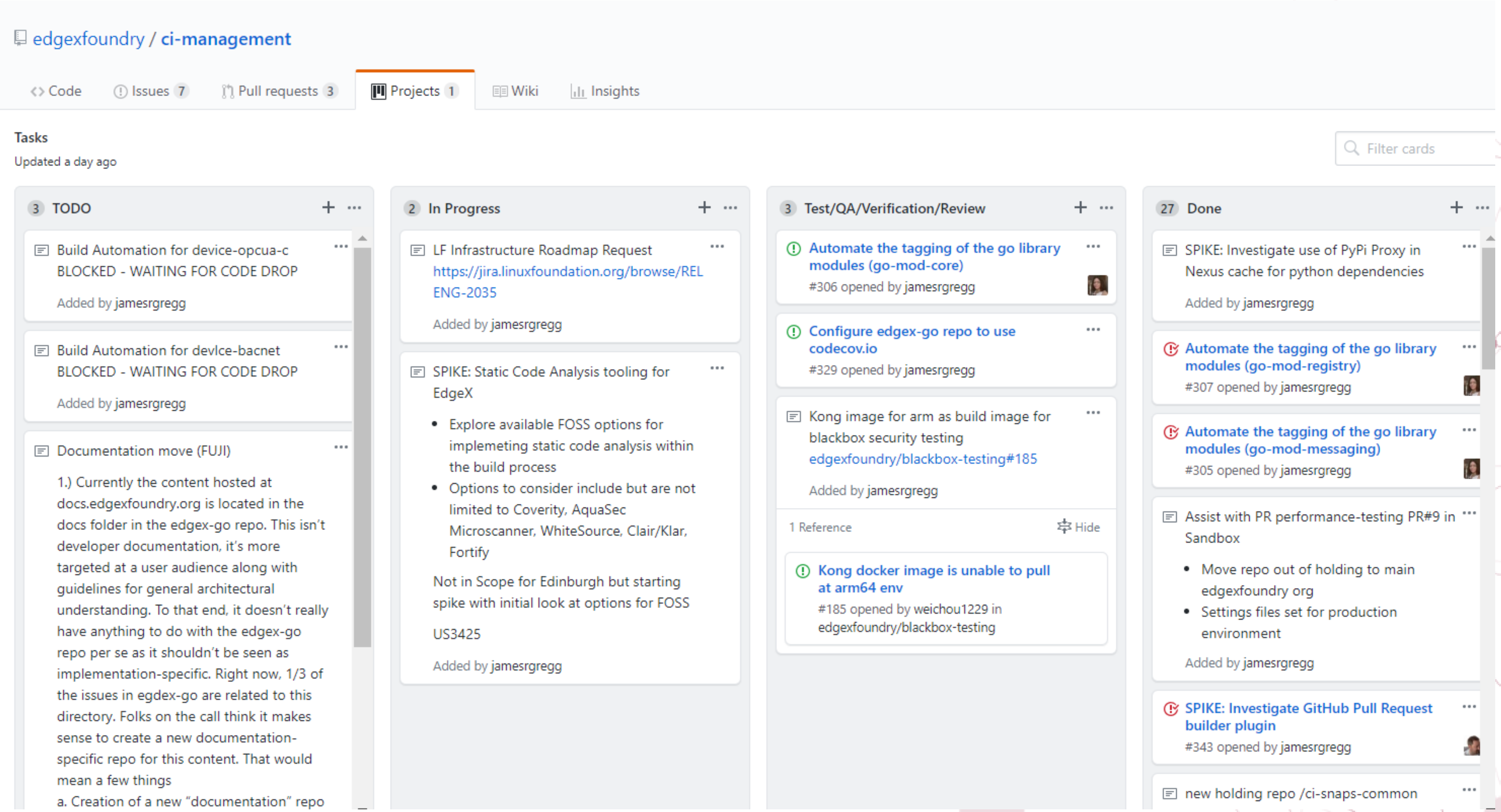
EdgeX DevOps WG Update

- Jenkins Pipelines built for go-mod-core, go-mod-messaging, go-registry-core - PR#95 PR#10   PR#15
  - Note: Pipelines were created without LFTOOLS / Sigul
- Catalog of Basebuild Docker images now being built using Jenkins Pipelines with images successfully pushed to Nexus
  - Includes Kong-ARM64 basebuild image for blackbox security testing
- New automation built to take the human factor out of needing LF infrastructure team’s help for manually creating Jenkins Pipelines webhooks
- Issues:
  - LFTOOLS / Sigul defects not addressed by Linux Foundation
  - Roadmap for addressing technical debt not understood by Linux Foundation for build dependencies (python version)

Work Review

Helpdesk Ticket #	Description	Details	Status
69830	codecov.io config needed for edgex-go repo	Eric Ball has implemented codecov.io for edgex-go repo as of WW20 Additional repos identified to include SDK repos – hold off on additional repos for now until we have it working with edgex-go	WIP (Eric)
68377	failed job related to timeout waiting for SSH	Eric Ball follow up with the team that owns VEXHOST – no progress Issue is with building new arm images – doesn't affect edgex builds decision to leave it open for now.. Circle back with VEXHOST team	WIP (Eric) Possible look at using a different OS for the builds Proposal to use Ubuntu instead of Centos ARM image
71119	need to extend sigul to include additional functionality – bugs identified with lftools / sigul	– sigul enhancements included in release last Thursday LFTOOLS release v0.23.1 Lisa identified some defects Sigul enhancements being worked by LF resources with PR in Gerrit WW20	WIP (Eric)
71025	TIG Performance Issues identified during testing on Sandbox	Tests are working in Sandbox but introduced OMM problems with AWS hosted TIG stack Redeployed the solution LF Infrastructure team engaged to resize the instances.	Resolved (Jordan) THANK YOU JORDAN CONWAY !! Outstanding PR for ci-management #338
71084	Enable PyPI for EdgeX Jenkins caching of python dependencies	SPIKE to see what it would take to enable the PyPI Proxy for caching dependencies on Nexus	Resolved THANK YOU ERIC BALL !! Pulled in Fuji scope!!!

Backlog Review



edgexfoundry / ci-management

Tasks
Updated a day ago

3 TODO

Build Automation for device-opcua-c
BLOCKED - WAITING FOR CODE DROP
Added by jamesrgregg

Build Automation for devlce-bacnet
BLOCKED - WAITING FOR CODE DROP
Added by jamesrgregg

Documentation move (FUJI)

1.) Currently the content hosted at docs.edgexfoundry.org is located in the docs folder in the edgex-go repo. This isn't developer documentation, it's more targeted at a user audience along with guidelines for general architectural understanding. To that end, it doesn't really have anything to do with the edgex-go repo per se as it shouldn't be seen as implementation-specific. Right now, 1/3 of the issues in egdex-go are related to this directory. Folks on the call think it makes sense to create a new documentation-specific repo for this content. That would mean a few things

a. Creation of a new "documentation" repo

2 In Progress

LF Infrastructure Roadmap Request
https://jira.linuxfoundation.org/browse/RELENG-2035
Added by jamesrgregg

SPIKE: Static Code Analysis tooling for EdgeX

- Explore available FOSS options for implemeting static code analysis within the build process
- Options to consider include but are not limited to Coverity, AquaSec Microscanner, WhiteSource, Clair/Klar, Fortify

Not in Scope for Edinburgh but starting spike with initial look at options for FOSS

US3425

Added by jamesrgregg

3 Test/QA/Verification/Review

Automate the tagging of the go library modules (go-mod-core)
#306 opened by jamesrgregg

Configure edgex-go repo to use codecov.io
#329 opened by jamesrgregg

Kong image for arm as build image for blackbox security testing
edgexfoundry/blackbox-testing#185
Added by jamesrgregg

1 Reference

Kong docker image is unable to pull at arm64 env
#185 opened by weichou1229 in edgexfoundry/blackbox-testing

27 Done

SPIKE: Investigate use of PyPi Proxy in Nexus cache for python dependencies
Added by jamesrgregg

Automate the tagging of the go library modules (go-mod-registry)
#307 opened by jamesrgregg

Automate the tagging of the go library modules (go-mod-messaging)
#305 opened by jamesrgregg

Assist with PR performance-testing PR#9 in Sandbox

- Move repo out of holding to main edgexfoundry org
- Settings files set for production environment

Added by jamesrgregg

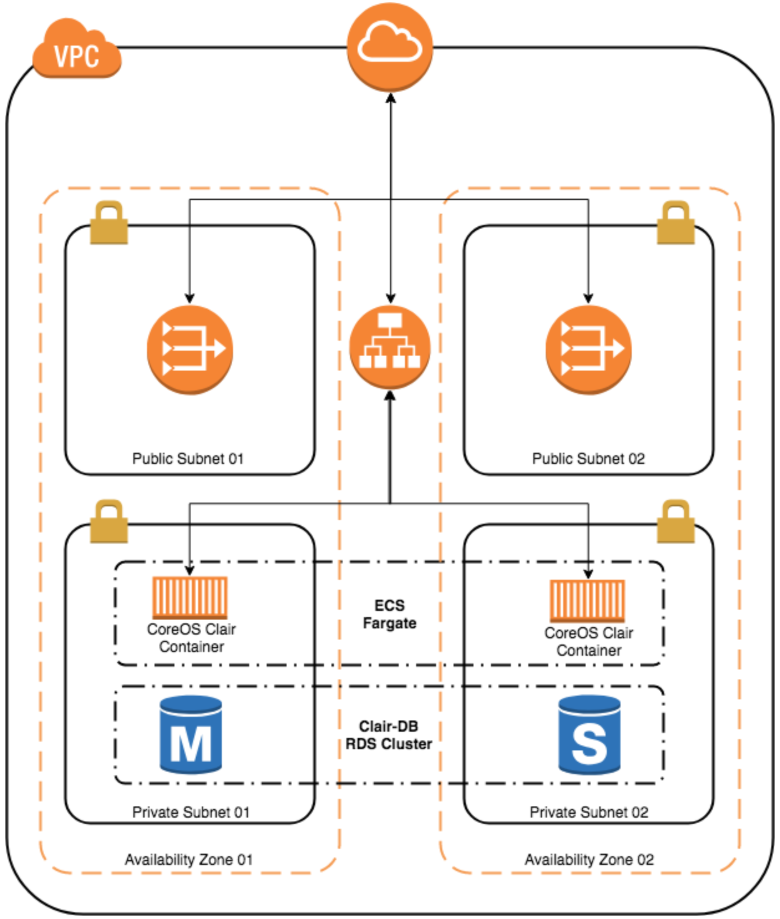
SPIKE: Investigate GitHub Pull Request builder plugin
#343 opened by jamesrgregg

new holding repo /ci-snaps-common

Config Options Discussion / Trevor Conn

- Expectation of enabling Redis
  - Propose to use the Docker Compose override to avoid having to create a new image

Architecture diagram of Clair hosted on AWS



- Clair uses PostgreSQL, so use Aurora PostgreSQL to host the Clair database. You deploy Clair as an ECS service with the Fargate launch type behind an Application Load Balancer.

- The Clair container is deployed in a private subnet behind the Application Load Balancer that is hosted in the public subnets. The private subnets must have a route to the internet using the NAT gateway, as Clair fetches the latest vulnerability information from multiple online sources.

Options to scan docker images for CVE detection

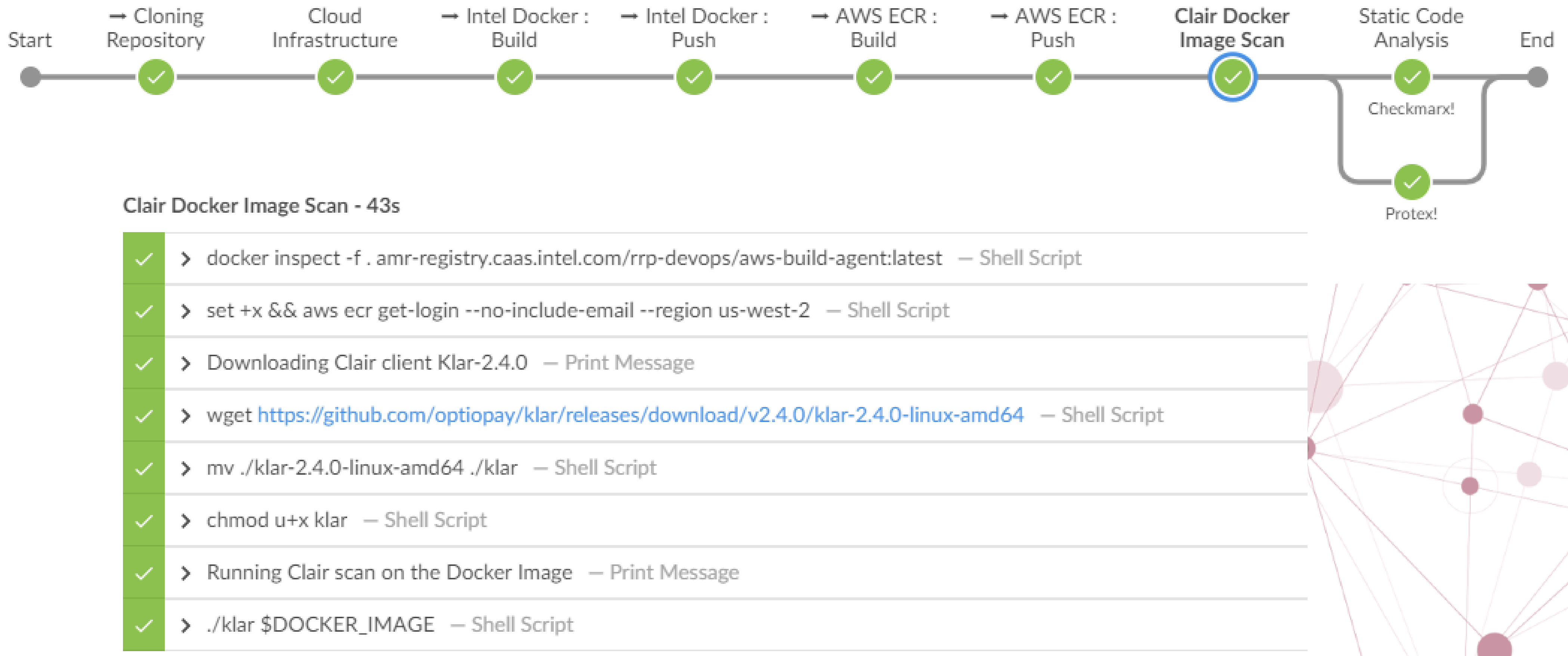
- Option #1 : Clair hosted on AWS
  Clair server and Postgres DB is hosted on AWS & Klar runs within the Jenkins pipeline. Ideally the Jenkins job would be configured to include a state which scans the Docker images published in the EdgeX Nexus repo. A report of Critical CVEs is generated with detailed information within the Jenkins build log.

  Option #2 : Clair hosted on LF infrastructure
  Similar solution to Option #1 but the Clair Server and DB are hosted on dedicated Linux Foundation infrastructure.

  Option #3: Clair hosted on existing AWS TIG infrastructure

  Need cost associated with options if hosted on AWS

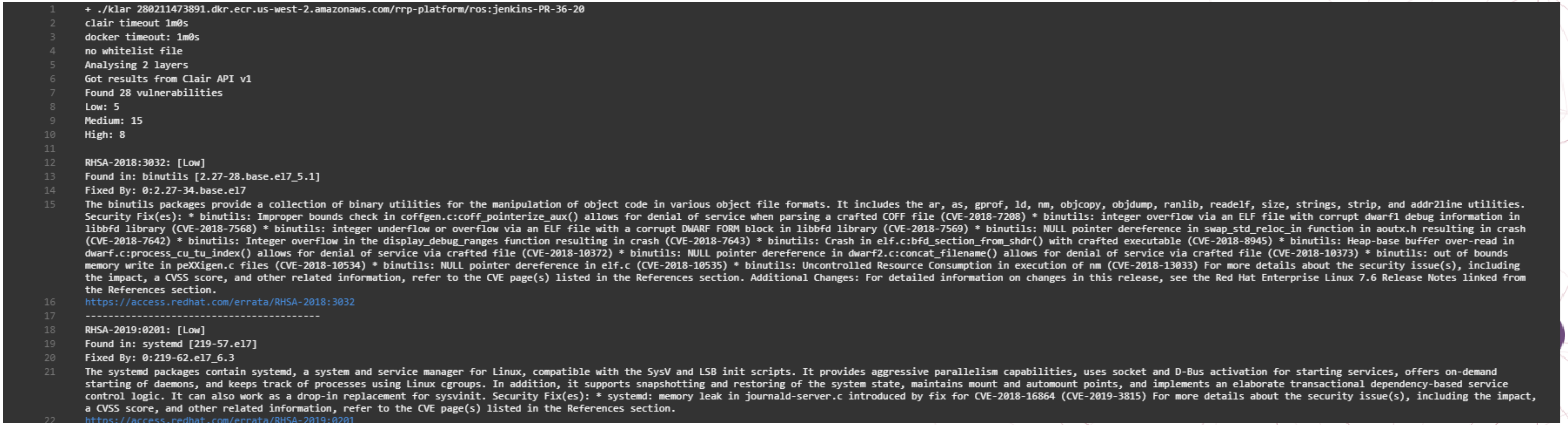
Jenkins Pipeline job with Clair Image Scan Stage



Clair Docker Image Scan - 43s

- ✓ > docker inspect -f . amr-registry.caas.intel.com/rrp-devops/aws-build-agent:latest — Shell Script
- ✓ > set +x && aws ecr get-login --no-include-email --region us-west-2 — Shell Script
- ✓ > Downloading Clair client Klar-2.4.0 — Print Message
- ✓ > wget https://github.com/optiopay/klar/releases/download/v2.4.0/klar-2.4.0-linux-amd64 — Shell Script
- ✓ > mv ./klar-2.4.0-linux-amd64 ./klar — Shell Script
- ✓ > chmod u+x klar — Shell Script
- ✓ > Running Clair scan on the Docker Image — Print Message
- ✓ > ./klar $DOCKER_IMAGE — Shell Script

Clair Output – Jenkins log



```
+ ./klar 280211473891.dkr.ecr.us-west-2.amazonaws.com/rrp-platform/ros:jenkins-PR-36-20
clair timeout 1m0s
docker timeout: 1m0s
no whitelist file
Analysing 2 layers
Got results from Clair API v1
Found 28 vulnerabilities
Low: 5
Medium: 15
High: 8

RHSA-2018:3032: [Low]
Found in: binutils [2.27-28.base.el7_5.1]
Fixed By: 0:2.27-34.base.el7
The binutils packages provide a collection of binary utilities for the manipulation of object code in various object file formats. It includes the ar, as, gprof, ld, nm, objcopy, objdump, ranlib, readelf, size, strings, strip, and addr2line utilities.
Security Fix(es): * binutils: Improper bounds check in coffgen.c:coff_pointerize_aux() allows for denial of service when parsing a crafted COFF file (CVE-2018-7208) * binutils: integer overflow via an ELF file with corrupt dwarf1 debug information in
libbfd library (CVE-2018-7568) * binutils: integer underflow or overflow via an ELF file with a corrupt DWARF FORM block in libbfd library (CVE-2018-7569) * binutils: NULL pointer dereference in swap_std_reloc_in function in aoutx.h resulting in crash
(CVE-2018-7642) * binutils: Integer overflow in the display_debug_ranges function resulting in crash (CVE-2018-7643) * binutils: Crash in elf.c:bfd_section_from_shdr() with crafted executable (CVE-2018-8945) * binutils: Heap-base buffer over-read in
dwarf.c:process_cu_tu_index() allows for denial of service via crafted file (CVE-2018-10372) * binutils: NULL pointer dereference in dwarf2.c:concat_filename() allows for denial of service via crafted file (CVE-2018-10373) * binutils: out of bounds
memory write in peXXigen.c files (CVE-2018-10534) * binutils: NULL pointer dereference in elf.c (CVE-2018-10535) * binutils: Uncontrolled Resource Consumption in execution of nm (CVE-2018-13033) For more details about the security issue(s), including
the impact, a CVSS score, and other related information, refer to the CVE page(s) listed in the References section. Additional Changes: For detailed information on changes in this release, see the Red Hat Enterprise Linux 7.6 Release Notes linked from
the References section.
https://access.redhat.com/errata/RHSA-2018:3032
-----------------------------------------
RHSA-2019:0201: [Low]
Found in: systemd [219-57.el7]
Fixed By: 0:219-62.el7_6.3
The systemd packages contain systemd, a system and service manager for Linux, compatible with the SysV and LSB init scripts. It provides aggressive parallelism capabilities, uses socket and D-Bus activation for starting services, offers on-demand
starting of daemons, and keeps track of processes using Linux cgroups. In addition, it supports snapshotting and restoring of the system state, maintains mount and automount points, and implements an elaborate transactional dependency-based service
control logic. It can also work as a drop-in replacement for sysvinit. Security Fix(es): * systemd: memory leak in journald-server.c introduced by fix for CVE-2018-16864 (CVE-2019-3815) For more details about the security issue(s), including the impact,
a CVSS score, and other related information, refer to the CVE page(s) listed in the References section.
https://access.redhat.com/errata/RHSA-2019:0201
```

Meeting Minutes

- Pradeep presented the material related to Clair / Klar explore.
    - Next Steps:
        - Need Cost associated with proposed Options
        - Need to review best option with LF Infrastructure team
        - Need to take the proposed solution forward to the TSC for a vote if there are additional costs / overhead to implement

EDGEXFOUNDRY™

Fuji Planning

Scope Discussions

Fuji – DevOps

In

- Static code analysis tool identified and integrated into the EdgeX Jenkins Pipeline for Docker image scanning

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 FOUNDRY™

Edinburgh Release

Release Planning

Edinburgh Dates

- Freeze Date – May 28
- Release Date – June 20

EDGEXFOUNDRY™

Future Agenda Topics

WW14	Documentation migration – edgex-go user documentation
WW14	Topics for Fuji F2F Jenkins Pipelines for EdgeX services
WW15	Review Aqua Microscanner – Image scanning tool for Vulnerabilities
WW16	NVIDIA – Security tooling within CodePipeline (Trevor request) 4/18/19
WW17	
WW18	
	Demo Clair / Klar
	Athens Project – proxy server for go package dependencies
	Community Involvement