ONAP Multi-Architecture Support Challenges
Migrating to Docker Hub

Brian Hedstrom, OAM Technology Consulting

Paul Vaduva, ENEA

Representing arm

2019-05-13

Background Information

Principle of the ONAP Technical Charter

"ONAP will include product / service / resource agnostic platform modules for lifecycle management (from definition, deployment, monitor / manage to retirement) of cloud centric, software controlled network functions."

Section 1b above can be found in both the original and revised LFN series charters.
It is unchanged since originally being adopted and placed into effect on March 9, 2017.
https://www.onap.org/wp-content/uploads/sites/20/2018/01/ONAP-Project-a-Series-of-LF-Projects-LLC-Technical-Charter-12-22-2017-FINAL.pdf

ONAP
OPEN NETWORK AUTOMATION PLATFORM

ONAP Architecture Principles

ONAP Architecture Principles include:

ONAP Scope
Vendor & Service Agnostic: ONAP Platform must be VNF, Resources, Products, and Service agnostic. Each service provider or integrator that uses ONAP can manage their specific environment (Resources, VNFs, Products, and services) by creating necessary metadata / artifacts using Design Studio to support their needs / environment.

ONAP Deployment / resiliency / scalability Support
Cloud Environment Support: All components in ONAP should be virtualized, preferably with support for both virtual machines and containers. All components should be software-based with no requirement on a specific hardware platform.
Availability & Resiliency: ONAP must support various deployment and configuration options to meet varying availability and resiliency needs of various service providers.

See https://wiki.onap.org/display/DW/Architecture+Principles

ONAP Platform Maturity Requirements (S3P)

ONAP S3P (Stability, Security, Scalability, Performance) requirements include:

Manageability

Level 1:

- All ONAP components will use a single logging system.
- Instantiation of a simple ONAP system should be accomplished in <1 hour with a minimal footprint

Level 2:

- A component can be independently upgraded (for bug fixes only) without impacting the operation of interacting components
- Component configuration to be externalized in a common fashion across ONAP projects
- All application logging to adhere to ONAP Application Logging Specification v1.2
- Implement guidelines for a minimal container footprint

Level 3:

- Transaction tracing across components

Starting with the ONAP Dublin Release, all projects required to meet a minimum Level 2.

Footprint minimization considered a Must Have for Dublin

The footprint minimization effort is introducing multi-arch support base images.

Multi-arch support proposal was vetted by ARCH in Casablanca release timeframe

See https://wiki.onap.org/display/DW/Manageability

Container Images - Best Practices & Tools (CIA)

ONAP Container Optimization (CIA) project goals:

This project will deliver re-usable artifacts & tooling to help ONAP projects simplify the development of vendor-agnostic container images using build templates that implement industry best practices.

- Enable Multi-Architecture support while reducing the container image footprint.
- Recommends using Alpine base images

Scalability

- Resource-constrained images (small & fast) improve horizontal scalability of ONAP deployments

Manageability

- Efficient, small images reduce transport, deployment, upgrade and recovery time

Usability

- Re-usable templates & reusable base images
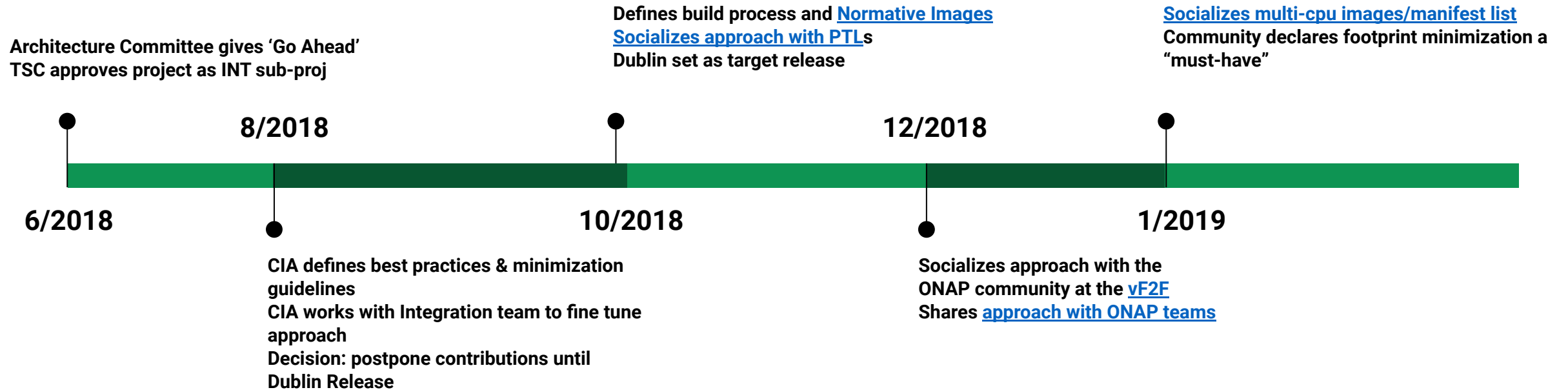- Multi-platform images offer operators more deployment options

Deployability

- With platform-agnostic images, operators and VNF vendors may choose among a variety of hardware/server providers with different OS and CPU architectures
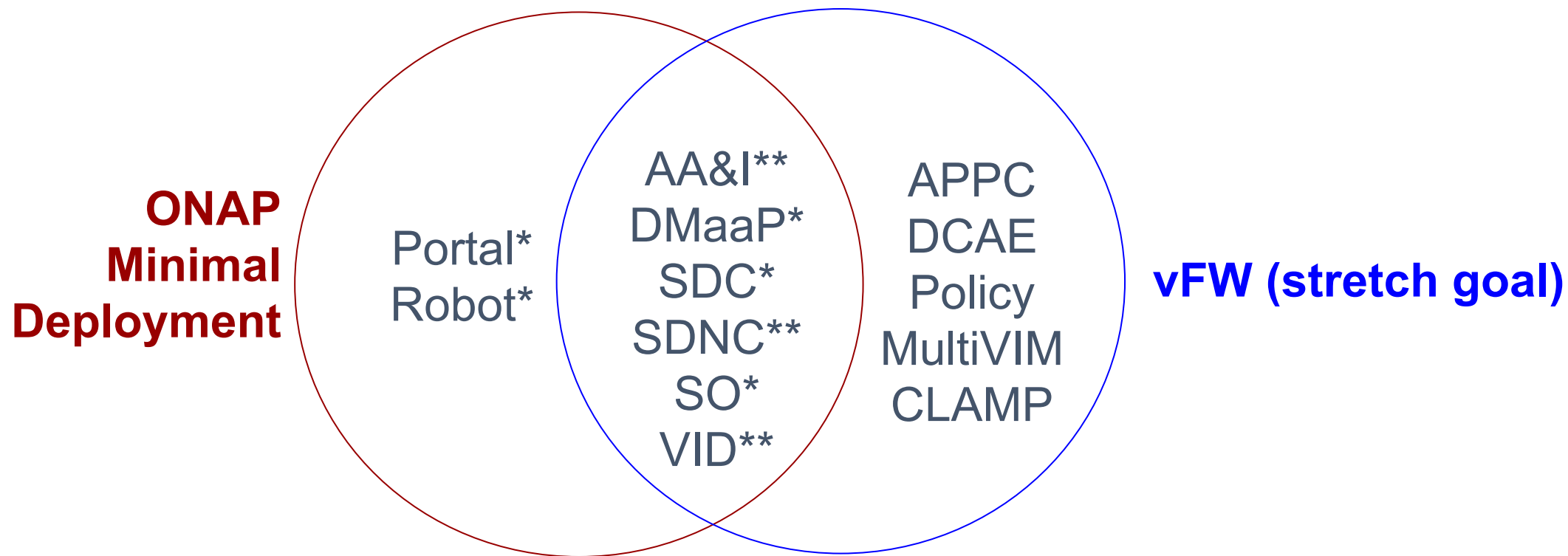
See https://wiki.onap.org/pages/viewpage.action?pageId=34375682

Project being led by ARM

Container Optimization Timeline

Architecture Committee gives 'Go Ahead'
TSC approves project as INT sub-proj

Defines build process and Normative Images
Socializes approach with PTLs
Dublin set as target release

Socializes multi-cpu images/manifest list
Community declares footprint minimization a
"must-have"

8/2018

12/2018

6/2018

10/2018

1/2019

CIA defines best practices & minimization
guidelines
CIA works with Integration team to fine tune
approach
Decision: postpone contributions until
Dublin Release

Socializes approach with the
ONAP community at the vF2F
Shares approach with ONAP teams

CIA Dublin Scope

ONAP Minimal Deployment

Portal*
Robot*

AA&I**
DMaaP*
SDC*
SDNC**
SO*
VID**

APPC
DCAE
Policy
MultiVIM
CLAMP

vFW (stretch goal)

vFW Source: https://wiki.onap.org/pages/viewpage.action?pageId=3246170

Problem Statement & Solution Proposal

Multi-Arch Support: Parallel CI/CD Pipeline

The following blocking issue was raised to LF Help Desk Jan 17:

- ONAP Nexus3 registry doesn't support manifest lists (Image Manifest v2)
- Current ONAP Nexus3 registry does not support manifest lists
- Ticket #67224
- ARM resources have been working toward a CI/CD pipeline that supports multi-cpu with no resolution
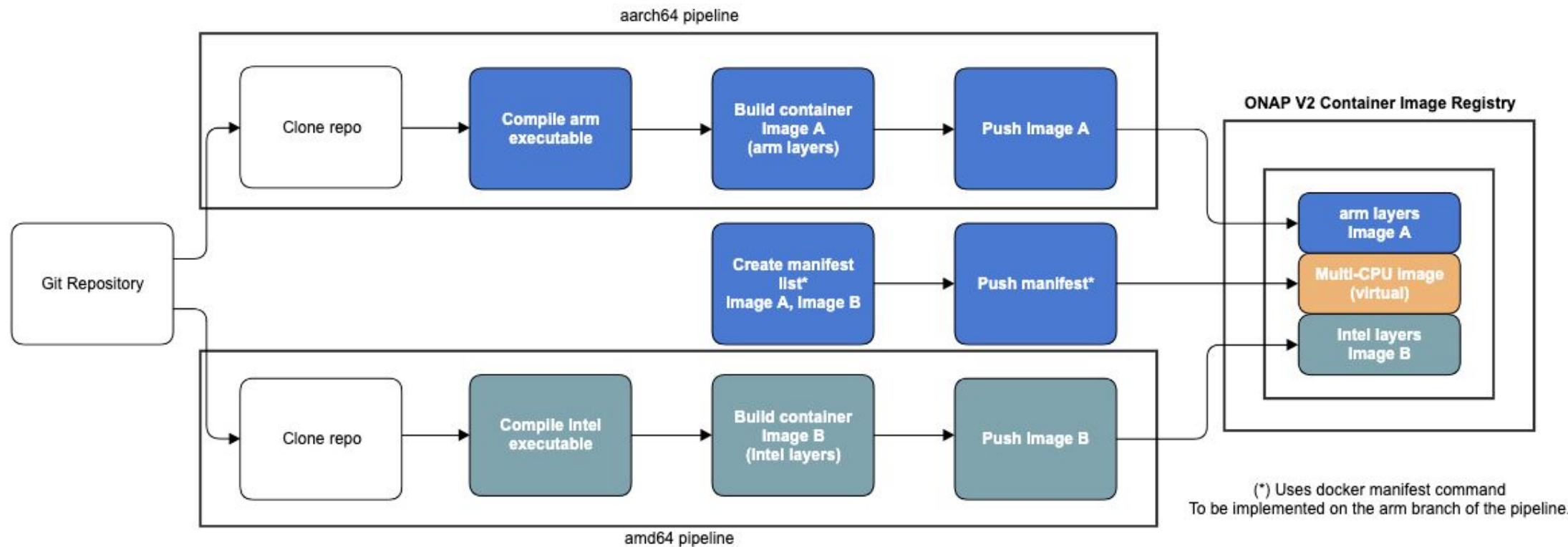
LF Infrastructure Upgrade Challenges

LF Infrastructure Team Priority:

1. CIMAN-234: Nexus2 - Migrate to Global-jjb gerrit-maven-stage job (opened 1/29/19)
2. CIMAN-229: Multi-cpu docker build jobs (opened 1/4/19)
3. CIMAN-239: Nexus3 - Migrate teams to start deploying images in DockerHub (opened 2/13/19)

The goal for the Dublin timeframe was to use Nexus 3 with the necessary changes requested by the ARM team. This effort was abandoned as not possible after parallel efforts to make it work.

ONAP El Alto proposed release includes a shorter technical debt release

Request is to include DockerHub Migration in El Alto as part of the "Test Automation & CI/CD Pipeline and Deployment procedure"

See
https://wiki.onap.org/display/DW/TSC+2019-04-18?preview=/60889264/63996004/2019-04-18%20ONAP%20Cadence%20Release_V5.pptx
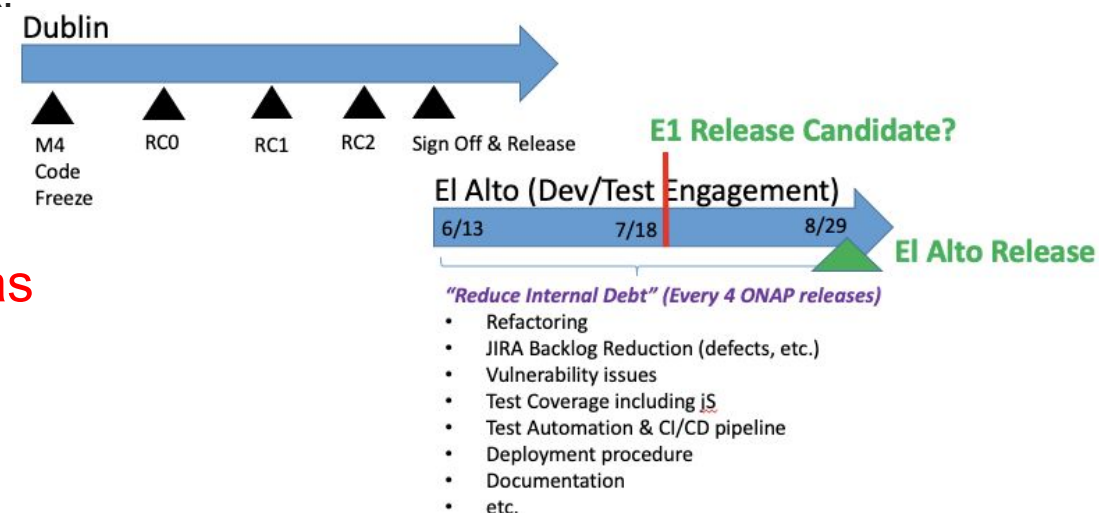
So what's the problem with Nexus docker registry?

- Nexus3 docker registry implementation does not allow the creation of manifest-list (multiarch images)
  - https://issues.sonatype.org/browse/NEXUS-18546
- Nexus3 docker caching registry does not allow to pull and cache a multiarch docker image (caches only the x86_64 image).

Docker Trusted Registry

This storage solution is available but currently out of the picture as a possible solution:

- Additional cost for ONAP which hasn't been proposed yet
  - Will need additional planning and analysis to provide the exact numbers
- Extra cost for running operations to support it
- Availability of resources from the Infrastructure team will need to be acquired
- Requires about 6+ weeks for implementation if approved

Requirements for the multi-arch CI/CD pipeline.

1. Switching from Nexus3 docker registries to DockerHub.
2. Tagging convention is still not consistent across components. Requires a fix.
3. Rename all docker images to contain a suffix (a reference to arch of the image) to have different names for each architecture.
4. Create additional jobs for building each container on new architecture e.g. arm64 (under works to support it)
5. Create an additional job for building the manifest list (multi-arch image) out of the existent arch specific images e.g. aarch64 and amd64.
   a. This step will require additional research as it is still a concept LF has not worked on before.
6. ONAP teams to provide a component dependency chart to plan for an effective migration.
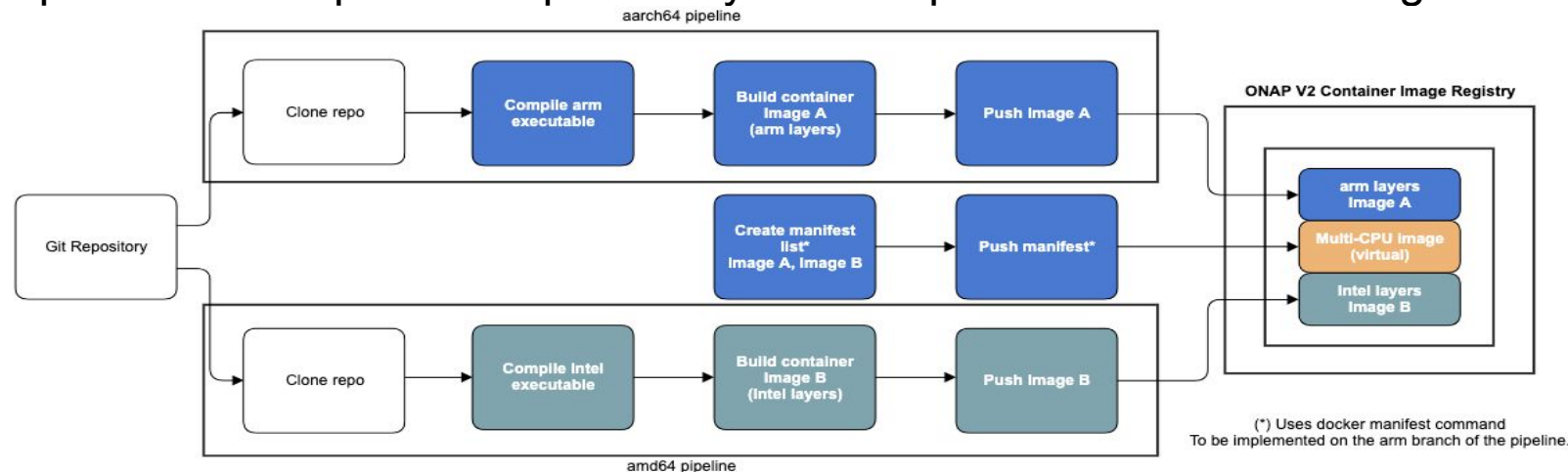
Performance concerns using DockerHub.

- Since DockerHub registry is not in the proximity of the build infra, one could have concerns regarding bandwidth and performance for the docker build / push jobs.
- LF has given assurances that if such an issue arises they will provide docker images caching in the proximity of the build infrastructure.

ONAP
OPEN NETWORK AUTOMATION PLATFORM
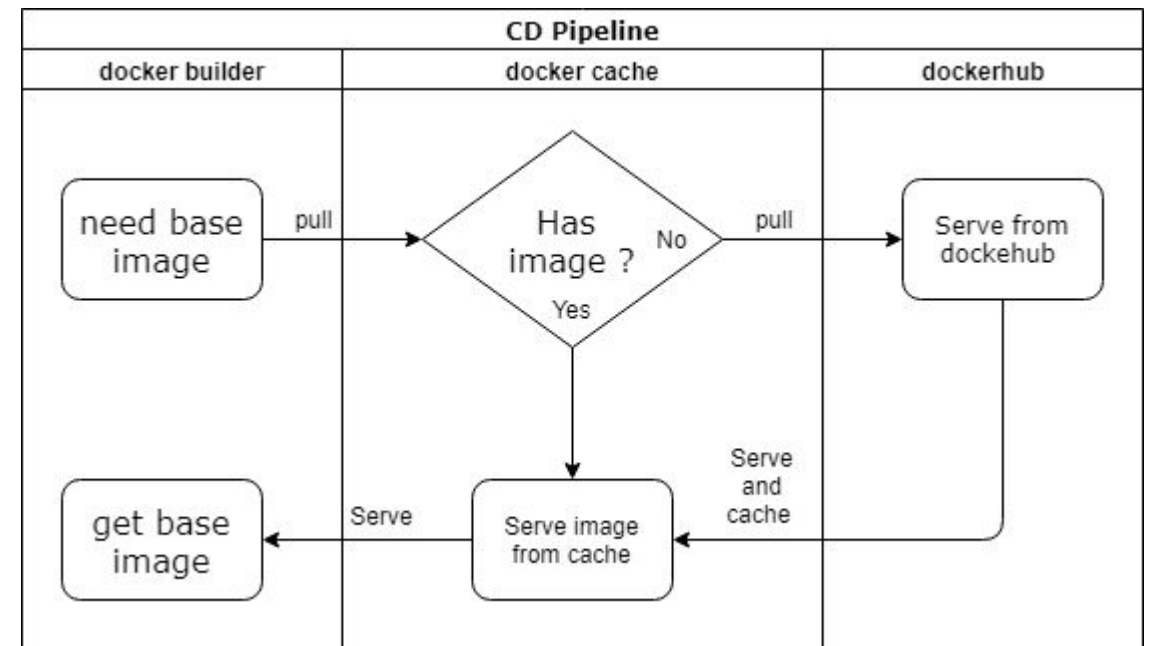
Security concerns using DockerHub.

- The recent security breach refers to a database of Dockerhub accounts whose account information have been stolen
  - https://motherboard.vice.com/en_us/article/7xgbzb/docker-hub-breach-hackers-stole-private-keys-tokens
- The impact of this incident is
  - Proprietary code of companies could have been hacked
    - Not applicable to ONAP as all code is open source
  - Images build with Docker autobuild system might contain injected code
    - Not applicable to ONAP as it uses its own build servers

- The conclusion is that this incident does not affect ONAP in any way, nor will possible future similar incidents

Summary

ONAP Platform mandates support for any CPU architecture (e.g., Resource agnostic) to allow deployments on any hardware infrastructure

Nexus3 docker registry does not support multi-arch images

Request is to include DockerHub Migration in El Alto as a Non-Functional Requirement