DevOps Working Group

Thursday October 29, 2020

Agenda

| Time	Topic	Owner
10 Min	DevOps Updates (Hanoi)	Ernesto
10 Min	CIS Docker Benchmark	Ernesto/Venkat
5 Min	Hanoi DevOps Deliverables	All
5 Min	AOB / Opens	All

Attendees
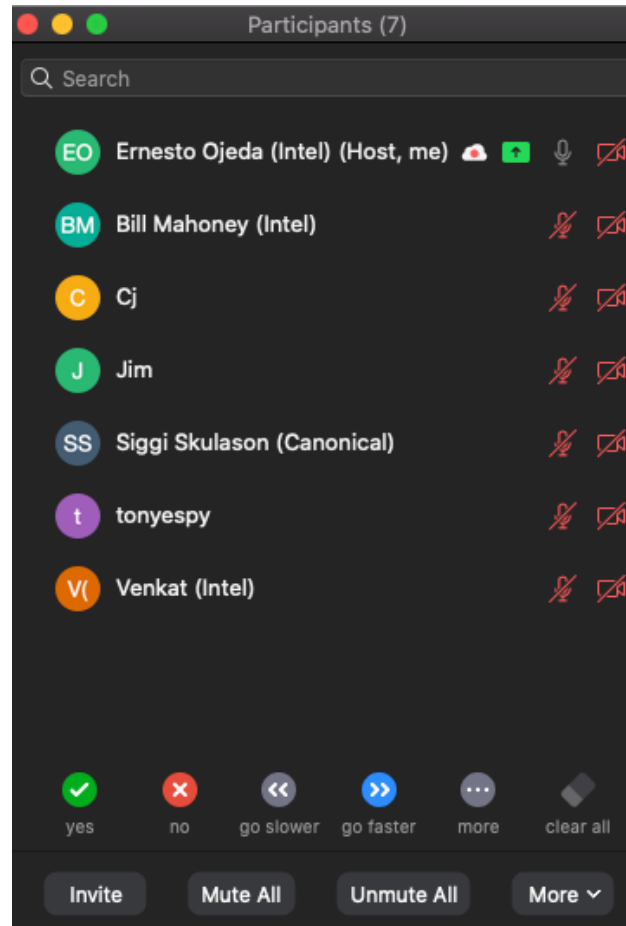
DevOps WG Update (Hanoi)

- **Pipeline Enhancements**
  - #252 [Watching] Build Snaps natively on Ubuntu
    - Build time increased, still testing
    - Open question about disabling all snap arm64 checks
  - #260 [Complete] CodeCov results not uploading
  - #261 [In Progress] Snyk scan docker images pre release
  - #137 [In Progress] Spike: CIS Docker Security Benchmark for EdgeX
  - [In Progress] New Global library for publishing GitHub pages content
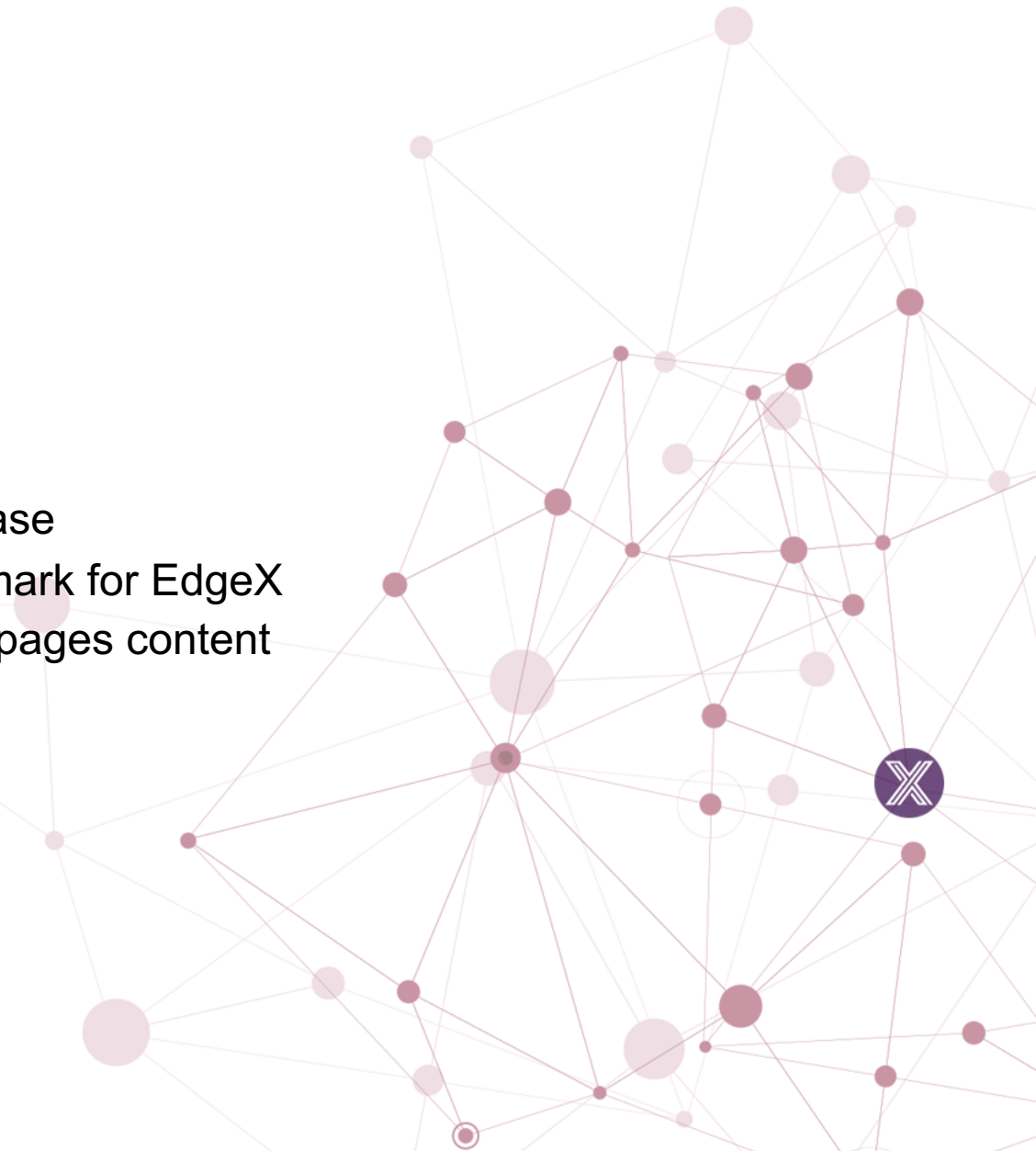
Inline Snyk Docker Image Scan

- Snyk CLI offers the `snyk test` command which shows scan results inline

- Pipeline requirements:
  - implement on-demand testing of docker images (after pushed to nexus i.e. master builds)
  - Notify distribution list of users when vulnerabilities are found
    - security-issues@lists.edgexfoundry.org
  - filter only on **high** severity findings
  - allow ignoring of Snyk findings via the .snyk policy file
    - Policy file will be stored in new repo **edgexfoundry/security-pipeline-policies** (Colin, Bryon, Jim)
  - Will use default fail-on option
    - --fail-on=**all**
  - Will Mark the build unstable but allow creation of the artifact:
    https://jenkins.edgexfoundry.org/blue/organizations/jenkins/edgexfoundry%2Fsample-service/detail/PR-77/16/pipeline

Hanoi DevOps Deliverables

- New faster build pipeline for edgex-go (build images in parallel)
- New edgex-cli build pipeline, create and publish edgex-cli binaries
- Snyk scanning pre-release docker images
- Snap build speed improvements for amd64 and arm64
- Auto generation of documentation for edgex-global-pipelines
- Linting of groovy code in pipeline to avoid syntax failures
- Cleanup and standardization of Mocking in unit tests
- Implement mocking of transitive functions in edgex-global-pipelines
- Introduce concept of "build commits" to trigger rebuild of artifacts
- Standardization use of `env.` across all pipelines
- Complete re-write of sample-service to enable full end-to-end testing of pipeline features
- EdgeX Release optimization (rebuild artifacts)
- Introduce process for vetting of OSS dependencies
- EdgeX AWS ECS reference stack deployment

- DevOps World presentation of edgex-global-pipelines
- Facilitate the upgrade to Go 1.15
- Implement workaround for race condition testing for Go prior to v1.15
- git-semver bug fixes and more robust unit tests
- GitHub Release automation
- GitHub prune stale/pre-release git tags
- GitHub label/milestone sync (with throttling)
- Generate report for stale docker images
- Released 8 device services
- Geneva Dot release
- SwaggerHub API global function
- Standardization of ENTRYPOINT across all Dockerfiles in all repos

Notes

- Core WG would like a way to sync image names in developer-scripts with the actual image names being generated by Jenkins pipelines. For examples in edgex-go, docker-**edgex**-secrets-setup-go was changed to docker-secrets-setup-go and that change was never promoted to developer-scripts. Need a way to do sync image names across all repos to developer-scripts