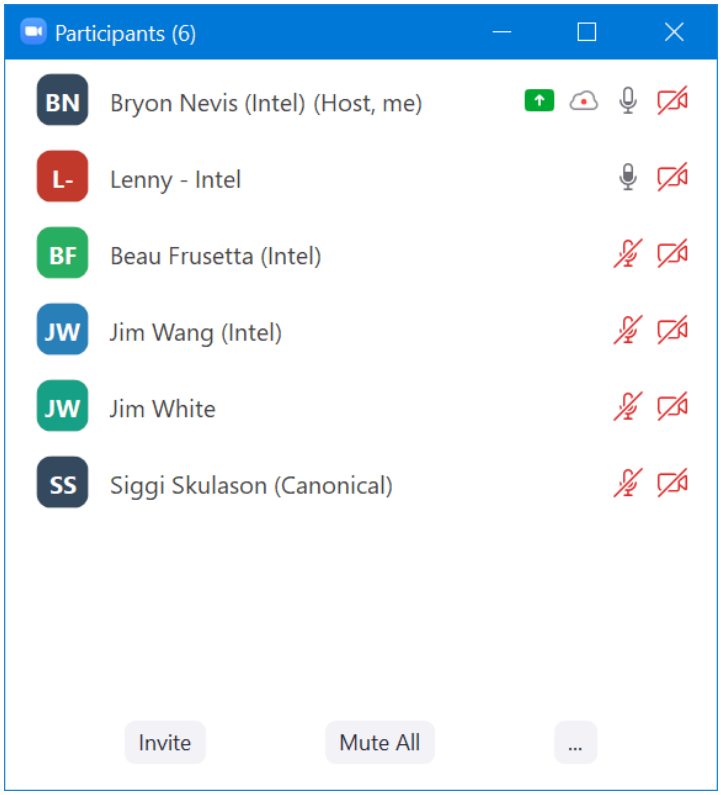
EdgeX Security WG Meeting

https://wiki.edgexfoundry.org/display/FA/Security+Working+Group

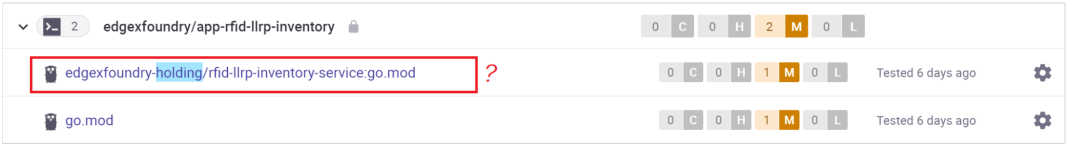
October 13, 2021

Attendees



Standing Agenda

- Review Security Board
- Securing Consul Board
- Review CIS docker scan (will skip unless something changes) (click latest run, go to classic, view console output).
- Review Snyk (Jenkins) (will skip unless something changes) (Imagelist)
  Notable issues:
  - Vulnerable openssh-client-common for sys-mgmt-agent (just patched sys-mgmt-agent last week!)
  - Device-coap libcrypto vulnerability (alpine 3.12) (Didn't we update base?)
  - Where is this inventory-service go.mod coming from below?



- Review action items from previous week

Agenda

- Broken crypto in app-functions-sdk-go
  https://github.com/edgexfoundry/app-functions-sdk-go/issues/963
  https://github.com/edgexfoundry/app-functions-sdk-go/issues/968
  Suggestions:
    - Deprecate the current function (add warning to log)
    - Plan to remove in EdgeX 3.0
    - Desire from the community to have a fixed version of the function for a LTS dot release
    - See if AlexCuse is willing to implement an improved version.
- Brainstorm: GUI in secure mode will need both an API gateway token and a Consul token. Any way to economize?
  https://github.com/edgexfoundry/edgex-ui-go/issues/448
    - Reply: “Consul API is already forwarded through the gateway with the access token appended -- just call it with the API gateway token and it will work.”
- On exposing Consul UI directly in secure mode (to resolve issue of not being able to use Consul via API gateway)
    - Was a problem to now expose it in docker-compose because there was a base restriction to localhost, and attempting to remove it caused two exports of the same port.
    - Decision: Remove restriction to localhost in nonsecure mode. Will be automatically secured in secure mode.
- Standard agenda
    - CORS implementation: to be brought up in Core WG to check scheduling
    - ONVIF ticket: descope for Jakarta; but will exclude for LTS
    - Device SDK C: Will bring up in device WG.
- Postpone: more data on being able to switch in- and out- of insecure Consul mode in snaps

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.

- 9/15: Bryon: Go back and check with users who requested remote gateway user management and see if they are OK with installing a persistent key of their choice to do this? If not, may have to not rotate kong admin key every boot.