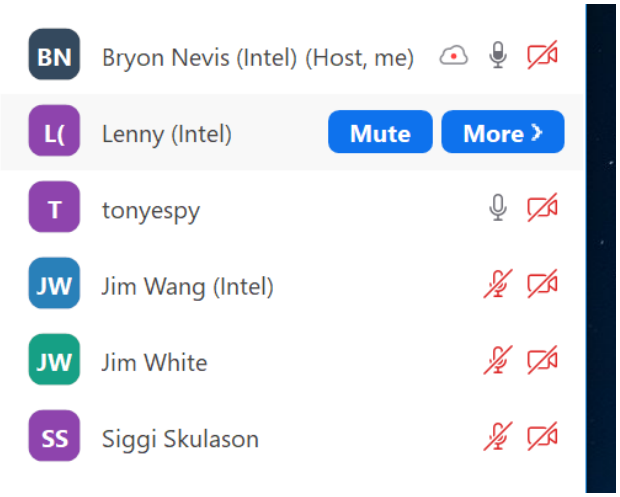
EdgeX Security WG Meeting

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

September 15, 2021

Attendees



BN Bryon Nevis (Intel) (Host, me)

L(Lenny (Intel)

T tonyespy

JW Jim Wang (Intel)

JW Jim White

SS Siggi Skulason

Standing Agenda

- Review Security Board
  - HELP needed for documentation!

Icebox	New	Backlog	WIP	Done
9	1	4	1 / 7	11

- Securing Consul Board

Ph-3 ToDo	Ph-2 ToDo	WIP	Done
4	1 / 2	0 / 0	3

- 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)

Critical	High	Medium	Low
36!	28	23	2

  - Wait for DevOps alpine upgrade.

- Review action items from previous week

Agenda

- Backport fix for remote gateway user management?
  - Decision: Don’t backport to Ireland
  - Discussion: Do we rotate the key every boot?
  - Go back and check with users who requested this and see if they are OK with installing a persistent key of their choice to do this?
  - UI will want this feature.
- CORS double-dipping (Lenny)
  - Originated as a request for device-sdk to add CORS capability in the insecure configuration. Currently, we can enable this globally via Kong if security is enabled.
  - Do we remove it from Kong and enable it in the common service middleware? Would also have to enable it in the C SDK as well.
  - Also: don’t talk to devices services directly: go via core-command
  - Scope this local to device-sdk only?
  - If enable in the service, would need new set of settings in the ServiceInfo that is repeated across services. (But could override with a common environment variable, but still need it to be applied to each service -- would need to regenerate the docker-compose. For snaps, can add to configure hook.)
  - Security recommendation: push this down to individual microservices and remove from Kong (due to desire to run in non-secure).
  - Continue discussion at architect meeting.
- Technical discussion on Consul after-the-fact disable of ACL system
  - Experimented with changing acl_enable flag in the Consul json config and restart Consul. Tried both flipping the flag and deleting the config.
  - Result was that there is still an error accessing the KV API in Consul

    As requested by the Security WG, I’ve tested editing the `consul_acl.json` file (found in `$SNAP_DATA/consul/config`) to set `acl.enabled=false` to see if this will disable ACL checking in Consul (after a restart), and unfortunately the answer seems to be no.
    Here are the steps I’ve tried (`SNAP_DATA=/var/snap/edgexfoundry/current`):

    ```
    sudo snap install edgexfoundry --channel=2.0
    ```

`sudo snap set edgexfoundry security-secret-store=off` (this halts kong, postgres, and vault, and sets the env var `EDGEX_SECURITY_SECRET_STORE=false` for all of the services (except for device-virtual and app-service-configurable which aren't configured in `snapcraft.yaml` to use the required command chain script which handles this var).

individually stop (using `snap stop …`) core-data, core-command, core-metadata, redis, and consul

`sudo rm $SNAP_DATA/redis/conf/*.conf`, `sudo touch $SNAP_DATA/redis/conf/redis.conf`

set `acl.enable=false` in `$SNAP_DATA/consul/config/consul_acl.json`

`rm $SNAP_DATA/consul/data/acl_tokens.json`

`sudo snap start edgexfoundry.redis` (and same for consul and core-metatadata)

This almost works as both consul and redis start, however when I start core-metadata, it fails trying to read its configuration from consul:

```
level=INFO app=core-metadata source=config.go:359 msg="Loaded service configuration from /var/snap/edgexfoundry/3196/config/core-metadata/res/configuration.toml"
level=INFO app=core-metadata source=variables.go:352 msg="Variables override of 'SecretStore.TokenFile' by environment variable: SECRETSTORE_TOKENFILE=/var/snap/edgexfoundry/3196/secrets/core-metadata/secrets-token.json"
level=INFO app=core-metadata source=config.go:156 msg="Using Config Provider access token of length 0"
level=INFO app=core-metadata source=config.go:334 msg="Using Configuration provider (consul) from: http://localhost:8500 with base path of edgex/core/2.0/core-metadata"
2021-09-08T16:56:28.874-0400 [ERROR] agent.http: Request error: method=GET url=/v1/kv/edgex/core/2.0/core-metadata/Notifications/Description from=127.0.0.1:48296 error="Permission denied"
```

NOTE - I also tried deleting the file `$SNAP_DATA/consul/config/consul_acl.json` with similar results.

I think the problem may be that in addition to configuring consul to require ACLs, it's also configured to use vault as the backend for its key store, but this is just a theory for now.

  - Will file an issue on inability to revert secure/insecure modes on next framework startup. Would like to understand why Consul is behaving this way (is the setting persisted inside of Consul?)

- Secrets seeding https://github.com/edgexfoundry/edgex-go/issues/3709
- Verbal discussion on Consul token and service resiliency. Lenny to file issue.
- POSTPONED to 9/29: ADR for delay start service secret store token https://github.com/edgexfoundry/edgex-docs/issues/278

- No meeting next week.

Action Items

- 7/14: Bryon: Update security policy documentation w.r.t. when to use GitHub security advisories to notify users of issues.
- ~~8/25: Jim/Tony: Report back progress on Consul security after-the-fact disable. (Look at a snap configure hook to see if it will work to modify ACL config.)~~
- 9/15: Bryon: Update Makefile in edgex-go to tell user how to install golangci-lint if it is not installed.
- 9/15: Bryon: Back out CORS changes.
- 9/15: Bryon: File an issue on Consul because of the reversion issue. (could also apply to Redis too). Tony to add additional data. Should be able to switch between secure and non-secure modes at startup.
- 9/15: ALL: Review #3709 proposal
- 9/15: Lenny: Submit issue for resiliency on Consul token