# EdgeX Security WG Meeting, 11/13/19

Attendees: Tingyu, Anthony, Jason, Michael (DELL), Mike, Lisa, Jim Wang, Diana, Bryon, Lenny, Beau, Eno (Intel), Ian Johnson, Tony (Canonical), Malini (VMWare), Jim White (IoTech)

Others may have joined after the meeting

Agenda

* Fuji work carried into master
* Geneva release items
* ARM support issue

# Fuji works that need to be carried into master

 Under EdgeX-go:

# PR-2090: user-friendly return message if cert already exists in proxy

# PR-2075: use alpine instead of scratch to get curl

# PR-2052: change of configuration.toml – set default security key value

Trevor noticed 5 others, 2 snap related, and 3 service related.

Suggests pinging Ian, to merge over all snaps related to master.

Under developer-script:

All the changes are in master the single branch

Nothing ARM specific docker compose. Nightly build into Fuji branch.

 Under docker-edgex-mongo:

 # PR-70: add curl to base image (scratch to alpine to facilitate the dependency checks)

# PR-69: 10 retry attempts. (Diana)

# PR-64: enable mongo container work in security mode (in Fuji, need to capture in master)

 Under docker-edgex-consul: (on Fuji, , open against master and awaiting review)

 # PR-8

# PR-9

 Under docker-edgex-volume: (on Fuji, , open against master and awaiting review)

 # PR-12

 Tingyu will review all PRs to confirm list above is complete

# Geneva release working items

* Bootstrap package for security release

Michael Estrin already working on this.

Trevor: internal to every service - might need to split into modules. DI and Bootstrap modules.

Tingyu: the dependency scripts – scripts work only on some platforms, make it into executables that could be called from within the code. If successful in this, could revert to base scratch images instead of an image with curl installed.

* Injecting service specific secrets – such as for Application SDK – injecting in AWS API tokens etc.

Go-mod-secrets. Lenny brought this up

* Per service token generation & related works

Bryon working on this.

* Images split – upstream image with a separate handling of configuration

Jim Wang: mentions issue 1716 split vault image into 2.

Tingyu: Similar suggestion for proxy, executable and config/initialization.

Broader discussion – across the project – pattern - how should we deal with public images we pull and customize. Lenny – could use a volume mount where we keep customizations, cross-mount. Jim Wang testing this out. ☺

For Redis – Andre recommends not creating custom credentials – given it is behind the proxy and we have ACL there

Lenny: Docker versus snaps – any security concerns to address

 Might there be some snaps security (Tony and Ian often cite greater security out of the box with snaps)

Michael: Not securing Redis would be a mistake. What does the security team mandate for securing Redis? What if we do not have proper network isolation.

Some of us recall from F2F that Andre would be providing security for Redis.

Today we have a mongo-init script, would need something similar for Redis.

Security group recommends protecting Redis instance.

* ARM support (?)

ARM Blackbox tests fail, unstable (timeout settings).

From TSC meeting – we leave things as is for Fuji release, but going forward

Michael: why are Blackbox tests failing and what needs to be done?

Currently it’s a VM in a VM on our LF test setup – it is slower, 800 ms is the timeout setting.

If timeouts are the only test failure types, easy enough to fix through configuration.

Tingyu: Based on my debug, there are infrastructure related issues, not just timeouts.

 efore security testing phase itself there have been crashes.

1. Core data -> meta data -> rules engine (crash here), did not even get to security test.
2. Postman, the testing tool. The ARM postman-newman to be used has to be custom built. One of the issues was the postman-newman included an older version of TLS and we needed to upgrade it to work with our broader setup.

 Should we have a task force to address this, allocating some resources to this?

* ARM support issue
* local build – good for development but need a setup from LF/project.

Trevor: how much effort should we invest in our Blackbox testing given framework changing

Anthony: Pointed out that we do not really care where Postman, the driver of the tests runs.

Malini: For the manual tests – getting it up on ARM was problematic .. but why postman in the picture there – investigate with Alex.

* local testing

 From TSC meeting – we need to work around release messaging for ARM.

Additional topics:

1. Lenny – future looking for Apps Services. Retrieve storage secrets. How do we store and retrieve. Such as API keys, AWS/token. Inject into vault. A new service endpoint? SDK would expose it.