System Management WG Agenda: 09/3/19

Attendees: (Attendees who may have joined after the start of the meeting may not have been captured and listed)
Note: Discussion and action items as a result of meeting in RED

Old Business

- Open Horizon sub-project
  - State of current POC
- Fuji Work
  - Metrics collection – implemented (thanks Akram); refactoring and unit test coverage ongoing (thanks Michael)
  - Set Configuration – currently being worked
  - Start/stop/restart
    - Issue: how to return response and not break compatibility
      - Dell team did meet later in the day to discuss SMA and several design / implementation issues.

      - Security – SMA access: The SMA API is unsecured and therefore creates a significant security risk especially given setting configuration or starting/stopping/restarting services could result in catastrophic operations.
      - On this issue, the decision was that the API Gateway will suffice for the Fuji release to protect the APIs just as it does other services. In Geneva, however, we want a more fine-grained access control. In particular, we want the API Gateway to allow access only to some elevated privileage user to be able to access and use the SMA APIs (today there is only one general purpose user that the API Gateway uses). To that end, there should be more fine-grained access/user controls for all services so this should be implemented in Geneva as a more general improvement to security access via the API Gateway that just happens to also apply to the SMA. In the future (Geneva or later) we actually like to allow access to be controlled not just by service but by API (example: allow access to some users to get config but not set config).

      - Security – executor access: Because the executor is just an executable that is calling on services to do things like start/stop/restart, it presents itself as another big security risk if someone has access to the EdgeX environment and can invoke the executor operations. For Fuji, this is a risk mitigated to some extent by proper platform access controls. In the future, the executor's access should also be control (ACL/user/role-based access) and the executor should probably check credentials when it is invoked (since the executor is not triggered by a REST API). In Geneva, this risk and potential security exploitation needs to be more heavily examined and dealt with.

      - SMA start/stop/restart:
      - Overall, the initial design to have the SMA API be a synchronous and blocking call from the client was not prudent. In general, this call needs to be asynchronous and non-blocking. This is regardless of the new requirement to also start/stop/restart the SMA as just another service. To fix this would require adding a new set of APIs in order to maintain backward

compatibility (which is to be avoided for Fuji). So for now, this feature will not be implemented and the existing start/stop/restart functionality (which excludes SMA as just another service and uses blocking calls) will remain, but be marked deprecated to warn the community that change is coming.

- In Geneva, we'll change this API to be asynchronous and include a callback to which the SMA can respond when the start/stop/restart activity is completed.

- Further, in the case of SMA as just another service to start/stop/restart, the desire is to keep executors free of having to maintain any state, persistence or other information about the services and their state. So the SMA will have to have some sort of persistence that can be used to track the results of the SMA operation, and it will have to be the first service started/stopped/etc. in order for the executor to provide results of the other operations on the other services. This begs the question as to whether the SMA is now special again, with regard to the other services, and how to handle this.

- So before implementing start/stop/restart of the SMA for Geneva, it is suggested we capture more real requirements for this and determine if there is really need to make other changes in order to be able to even offer start/stop/restart of the SMA itself and/or if so should this be accomplished by special means such as a separate and different API call.

New Business

- none