Delhi TSC F2F
Working Agenda and Deck

Palo Alto, CA
June 5-6
Delhi F2F Meeting

• Agenda
  • Day 1 – Delhi planning day
    • Welcome and intro by Mike McDonough (VMWare): 9-9:45am
    • Architecture day tee-up: 10-noon
      • Review and explanation of upcoming items
    • Delhi Planning – what’s in/out: 1-3:30pm
      • Scope definition
    • Testbed and organization liaising: 3:30-4:30pm
      • IIC Testbeds, IIC coordination, etc.
    • Vertical Solution Group update/actions: 4:30pm-5:15pm
  • TSC & WG chair upcoming voting: 5:15-5:30pm
    • LF review of rules and procedures for upcoming voting
  • Day 2 – Architecture issues day
    • TBD architecture discussion and decisions: 9am-2:30pm
    • Business Issues/Discussion: 2:30-3:30pm
    • Wrap up and action items: 3:30-4:30pm
Architecture Issues Tee-up – Technical Debt

• Technical Debt (things that need fixed)
  • Rearchitect Go Export Distro – Move to Application Services concept(s)
  • Protecting micro service secrets with Vault (export distro, others?)
  • Upgrade Consul & master/slave configuration
  • Automate API documentation (move to alternate format?)
  • Search for Mongo replacements/alternatives (offer for Edinburg)
  • Steps toward truly distributed EdgeX (multiple machines, reverse proxy impact, commands across hosts, etc.)
  • Device discovery, onboarding and removal
  • Renew threat modeling
Architecture Issues Tee-up - Enhancements

- ARM 32 support
- Device services that downsample (scale back readings sent when data is pumped to fast)
- Min/Max limit on accepting command
- Data transformation and/or filtering at DS level
- Additional DS connectivity (ex: CANBus, Profinet, …)
- Alternate deployment / orchestration (ex: adding Kubernetes support)
- User Interface (review/adopt for Delhi)
- How to deal with device security
- Load balancing of requests to multiple service instances
- Support for an alternate message bus (Point to point between services or at large)
- Introduce new category for microservices: “Sharing Services” for East/West data exchange with non-EdgeX entities
- Protobuf or lighter weight messaging (Hitachi submission)
- Address data privacy concerns (GDPR, HIP-A, …)
- Additional export connectors (ex: Greengrass, …)
- Scheduling – service or library approach?
Cadence Check

- April & Oct remain target release months
  - California release an aberration due need to get Go code
- F2F planning around time of completion of each release
  - Edinburgh – Oct 2018
  - Korea – April 2019
- Conferences
  - At least 2 x large marketing/promotional events (Hannover Messe, IoT SWC)
  - At least 1 x developer focused event
Delhi Scope

• Lot of desires for Delhi
  • Too many potential work items
  • Must be realistic
• Delivery schedule is only 3-4 months out
  • Summer vacations
  • IoT SWC target in October (16-18th)
• Must sharpen the focus and make hard choices
• Suggest 4 main implementation targets
  • Initial System Management APIs and agent
  • DS SDKs (Go/C) & some replacement DSs
  • Next wave of security features
    • Suggest ACL, secure non-HTTP comms
  • Improve testing
    • Better/more unit, complete black box and performance
Delhi Planning – System Management

**In**
- System management API
- Sys mgmt agent
- Base service (started with refactor)
  - Service naming
  - Availability
  - Common config/reg
  - Service tracing (OpenTracing API)
- Service outage & notifications
  - Resiliency in face of non-availability of services

**Out**
- Gateway management
- Consul replacement
- Multi-instance management
- Alt. deployment or orchestration (beyond Compose)
  - Ex: Kubernetes
- Load balancing; east/west comms/RAS
System Management Roadmap for reference
<table>
<thead>
<tr>
<th>Delhi Planning - Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>In</strong></td>
</tr>
<tr>
<td>• ACL (for reverse proxy use)</td>
</tr>
<tr>
<td>• Secure non-Http comms</td>
</tr>
<tr>
<td>• MQTT outbound/inbound</td>
</tr>
<tr>
<td>• 0MQ outbound</td>
</tr>
<tr>
<td><strong>Out</strong></td>
</tr>
<tr>
<td>• CA</td>
</tr>
<tr>
<td>• Service-to-service security</td>
</tr>
<tr>
<td>• Device security</td>
</tr>
<tr>
<td>• Threat modeling</td>
</tr>
<tr>
<td>• Code signing</td>
</tr>
<tr>
<td>• Use of Hyperledger</td>
</tr>
</tbody>
</table>
Security Roadmap for reference

Data Protection
- DAR Encrypted Storage
- Key Management
- DIT Encrypted Comms
- Data Protection Policy
- Guidelines
  - Privacy

Identity and Access
- Access Management (Least Privilege)
- Administration Local and Remote
- Authentication
- Identity and Access Policy
- Identity Management

Operational Security
- Security Monitoring
- Audit
- SW Update Management
- Attestation
- Chain of Trust
- Operational Security Policy
- Inbound Secure Reverse Proxy
- Secure Auto-configuration

Elements in purple to be partially completed in California release.
Delhi Planning – DS & SDK

In
• Results/Actions of June 4 meeting
• Complete the initial SDKs
  • Go & C
• Complete new virtual device service
• Refactor some existing DS
  • Modbus
  • BACNet
  • MQTT

Out
• Device discovery
  • Onboarding/removing
Delhi Planning – Testing

**In**
- Unit tests coverage of a majority of the code
  - Core/support service refactors as examples
- Blackbox testing for all services
  - Integrate in CI
  - Reporting on failed tests
  - Remaining services not completed for CA
  - DS/SDK
- Performance Tests
  - Meeting RP3 targets?
  - RP3 targets realistic?

**Out**
- Security Testing???
Delhi Planning - Misc

**In**
- Replace any remaining Java services
  - Scheduler (review/cleanup contribution)
  - Rules Engine
- Refactor per DT work
  - Better interfacing/loose coupling/isolation
  - Better organization
  - Better testing
- Configuration categorized/grouped
  - Settings/configuration standardization
- Begin work on Application Services
  - Eventual replacement for Export Services
  - Target Edinburgh release?
- Review and incorporate all the outstanding code contributions
  - UI
  - Scheduler
  - Samsung code
  - EdgeX-UI

**Out**
- Additional OS Support
  - Arm 32?
  - Windows
- DB replacement
- Monitor config changes and apply dynamically
  - Persist settings on clean shutdown
- Services respond to native init process
  - Ex: systemd
- Commands / exported northside
Vertical Solutions Group

• 3 features from Smart Factory Project, might be also along with the existing Core architectures.
• OPC UA Device Service (Java, C) : Also validation completed from OPC UA CTT, discussion with TSC Chair
• ezMQ (realtime messaging framework) : Brokerless transmission
• Pharos (System managementt) : We have a video clip to demonstrate how it works)
Architecture – Tech Debt/Readdress

- Rearchitect Go Export Distro – Move to Application Services concept(s)
  - More modular/SDK like
  - More scalable solution
- Protecting micro service secrets with Vault (export distro, others?)
- Upgrade Consul &/or move to master/slave configuration
  - Based on conversation with HashiCorp
- Automate API documentation
  - Replace or augment RAML with Swagger, TOML, etc.
- Search for Mongo replacements/alternatives (offer for Edinburg)
  - Errors and warnings on startup
  - Mongo replacement/alternates (no Arm32 support, MongoDB light, etc.)
  - Use of DB Ids in objects

---

- Steps toward truly distributed EdgeX
  - Services running on different host machines
  - Security impact with re: reverse proxy
  - Command calling across hosts
- Device discovery, onboarding and removal
- Renew threat modeling

Discuss as potentially part of Delhi

Discuss time permitting and proposed for Edinburgh or beyond
Architecture – Desired Enhancements

• ARM 32 support
• Device services that downsample (scale back readings sent when data is pumped to fast)
• Min/Max limit on accepting command
• Data transformation and/or filtering at DS level
• Additional DS connectivity
  • CANBus
  • Profinet
• Alternate deployment / orchestration
  • Kubernetes vs Compose or Snaps
• User Interface
  • Review/accept VMWare donation as EdgeX UI
  • Preview by end of summer

Discuss as potentially part of Delhi
Architecture – Desired Enhancements (Cont.)

• How to deal with device security
• Load balancing of requests to multiple service instances
• Support for an alternate message bus
  • Point to point between services or at large
• Introduce new category for microservices: “Sharing Services” for East/West data exchange with non-Edgex entities
• Protobuf or lighter weight messaging (Hitachi submission)
• Address data privacy concerns
  • EU laws and affirmation about data use/storage/etc.
  • HIP-A
• Additional export connectors (depends on Export Service refactor)
  • AWS Greengrass
• Scheduling – service or library approach?
  • Make it consistent across services

Discussed time permitting and proposed for Edinburgh or beyond
Business Issues

• Marketplace for value-add microservices and its implications (will we need a new EdgeX microservice acting as license server?)

• Certification process
  • When do we start to outline?
  • Levels
  • What does it incorporate?
    • What gets certified? Micro services, EdgeX extensions (ex: real time?)
  • Security certification

• Samsung is about to extend EdgeX related project from the internal manufacturing infrastructure (as Smart Factory) to consumer electronics and mobiles.