Architectural Reference Working Group

Meeting Minutes

20 May 2021

Attendees: Russ Warren, Adam Montville, Mitch Thomas, David Kemp, Andrew Beard, Bill Munyan, Mudit Tyagi

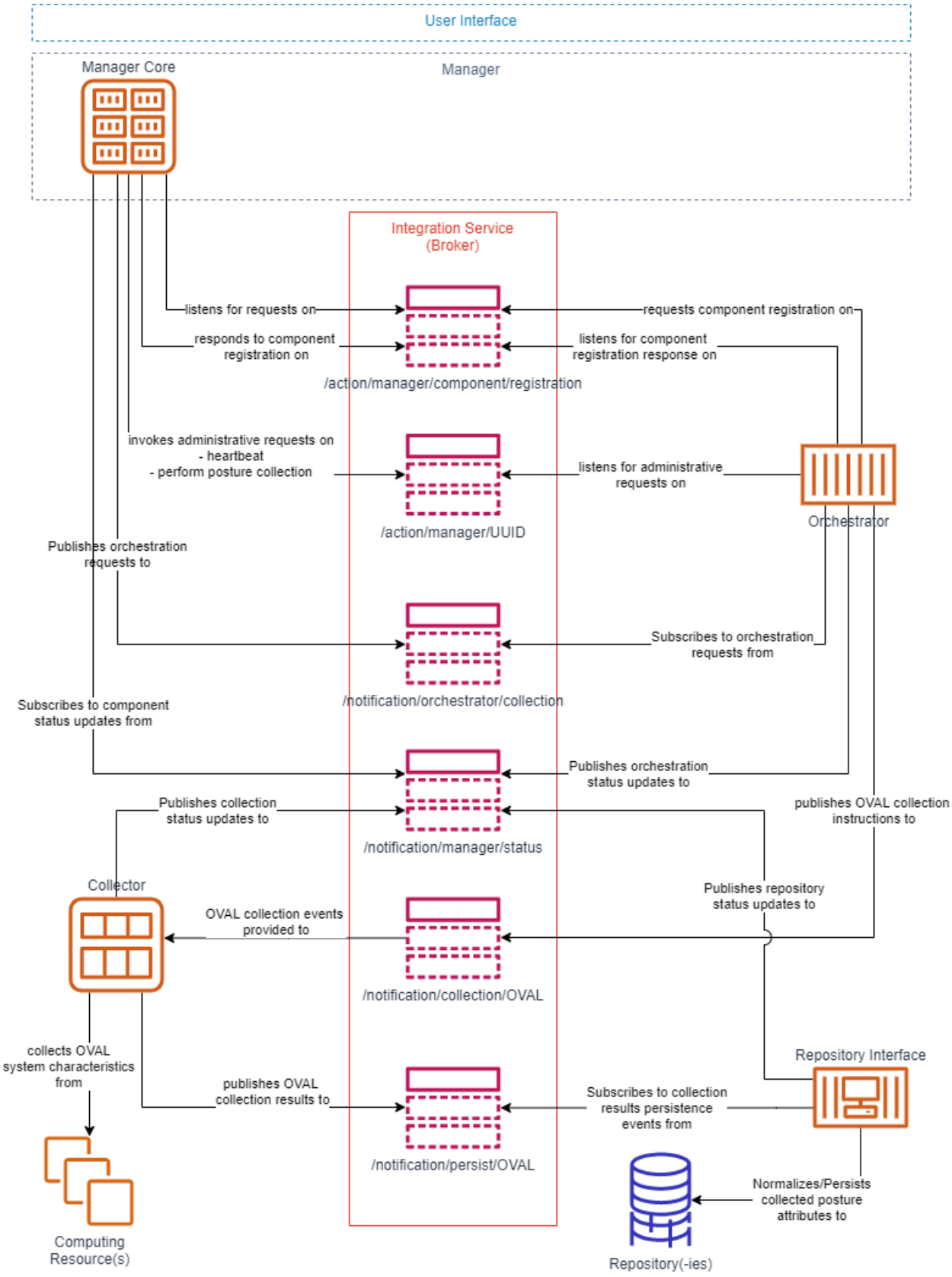
Agenda:

Here is the agenda for our call Thursday.
1 - Bill Munyan has sent out the following diagram and note on what he will cover:

I can present on the work we've been doing in the SACM working group in the IETF (on par with SCAP work -- my example uses SCAP content/tooling) and an example component, topic, and workflow diagram.

I've attached the diagram I will go through:
The orange-colored icons represent components in the ecosystem
The blue ones represent data repositories
The red/pink ones down the middle of the diagram represent topics (an example implementation of which would be, OpenDXL topics with payload specifications outlined in the "OCA ontology")

2 – Andrew Beard will review his work on Threat Intelligence and the ontology.


User Interface
Manager
Manager Core
Integration Service
(Broker)
listens for requests on
responds to component
registration on
requests component registration on
listens for component
registration response on
/action/manager/component/registration
invokes administrative requests on
- heartbeat
- perform posture collection
listens for administrative
requests on
/action/manager/UUID
Orchestrator
Publishes orchestration
requests to
Subscribes to orchestration
requests from
/notification/orchestrator/collection
Subscribes to component
status updates from
Publishes orchestration
status updates to
Publishes collection
status updates to
publishes OVAL collection
instructions to
/notification/manager/status
Collector
Publishes repository
status updates to
OVAL collection events
provided to
/notification/collection/OVAL
collects OVAL
system characteristics
from
publishes OVAL
collection results to
Repository Interface
Subscribes to collection
results persistence
events from
/notification/persist/OVAL
Normalizes/Persists
collected posture
attributes to
Computing
Resource(s)
Repository(-ies)

Topic 1 – Discuss SACM working group (IETF) – Lead by Bill Munyan

Bill discussed the IETF work group working with the SACM (Security Automated and Continuous Monitoring). The focus is on Posture Attribute Collection and Evaluation. An architecture draft is available at

- https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/

The SCAP group has been focused on architecture (SACM and SCAP). 2 are similar on what they are trying to accomplish. SACM is more content agnostic. Hackathons and POCs have been done. XMPP messaging framework and OVAL definitions have been used. Draft is focus on capabilities and operations. Capabilities is what the component can do. Capability advertisement/service directory is used to publish the capabilities on the components. OpenDXL can be used as the integration service and the OCA ontology describes the topic actions and payloads. Operations such as registration, notifications, posture collection, posture evaluation, and an admin interface.

Diagram shows the Manager, SACM producer and consumers exchanging messages over the integration services (OpenDXL). Posture collection can be done via an agent or via a posture collection service (not on the endpoint). (see meeting recording for slides). Orchestration would collect the posture information from the posture collection services. Manager, orchestrator, collector, repository, and endpoints are the components. Manager listens to a predefined topic for requests. The manager works with the orchestrator to collect the posture information.

+++ We lost Bill to a power outage +++ We will continue the discussion on our next call.

Topic 2 – Discuss Threat Intelligence and the ontology – Lead by Andrew Beard

There is a Build issue on the OCA Ontology GitHub. We need Chris Smith's (Ontology maintainer) to help fix this. Andrew has a Pull request for his input on the threat intelligence ontology. The threat intelligence will be a passive role (answers requests from SIEM/SOAR, receives data from threat intelligence source). We can use STIX patterns to interact with the Threat Intelligence system. Andrew created a list of attributes. We should support IPV4 and IPV6 with common type.

Andrew will capture the use cases for the user of the threat intelligence system. Data gets put into and out of the threat intelligence system (like a library). STIX can handle a lot of the communication. Project Kestrel can be relevant to this discussion. C4 diagrams also need to be added for this system.

OpenC2 is a graph-based interface, and we will need to map to the ontology.