

# SACM Architecture

Next Actions and Open Questions

July 25, 2019 – IETF 105

Adam Montville

# Pending Changes: Simple Draft Reorganization

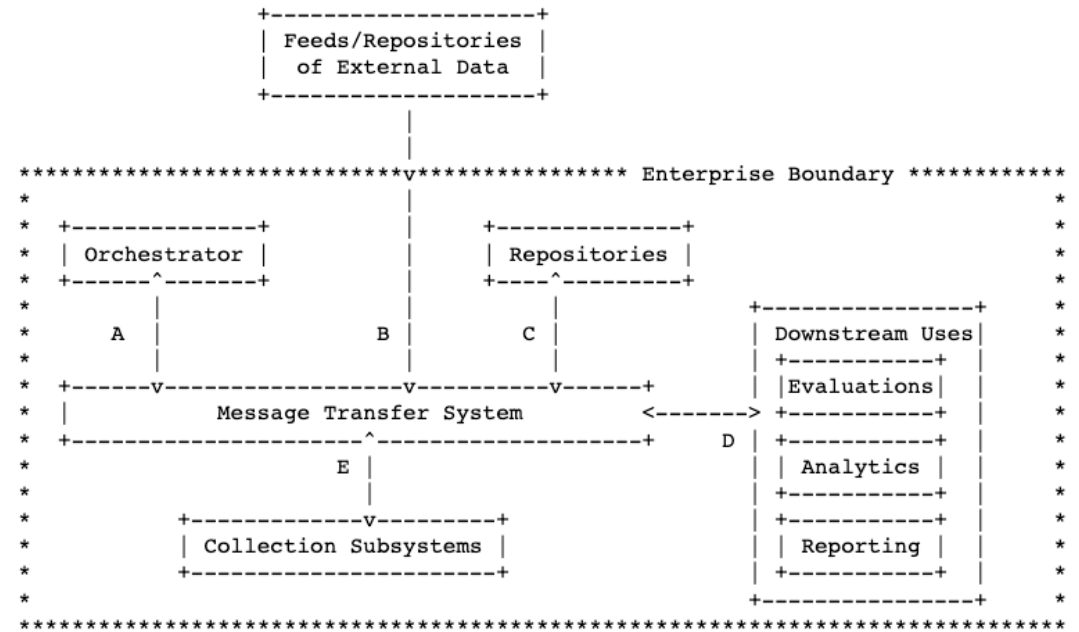
- Remove XMPP-based solution from the draft entirely – separate draft
- Combine current Section 3.1 with current Section 4 (becomes new Section 3)
- Narrow focus to single workflow – configuration assessment
- Clarifications (covered on subsequent slides)

## Table of Contents

1. Introduction . . . . .	2
1.1. Open Questions . . . . .	3
1.2. Requirements notation . . . . .	3
2. Terms and Definitions . . . . .	4
3. Architectural Overview . . . . .	4
3.1. SACM Roles . . . . .	5
3.2. Exploring An XMPP-based Solution . . . . .	5
3.3. Example Architecture using XMPP-Grid and Endpoint Posture Collection Protocol . . . . .	8
4. Components, Capabilities, Interfaces, and Workflows . . . . .	10
4.1. Components . . . . .	10
4.2. Capabilities . . . . .	11
4.3. Interfaces . . . . .	11
4.4. Workflows . . . . .	12
4.4.1. IT Asset Management . . . . .	12
4.4.2. Vulnerability Management . . . . .	12
4.4.3. Configuration Management . . . . .	14
5. Privacy Considerations . . . . .	15
6. Security Considerations . . . . .	15
7. IANA Considerations . . . . .	16
8. References . . . . .	16
8.1. Normative References . . . . .	16
8.2. Informative References . . . . .	16
Appendix A. Mapping to RFC8248 . . . . .	18
Appendix B. Example Components . . . . .	21
B.1. Policy Services . . . . .	21
B.2. Software Inventory . . . . .	22
B.3. Datastream Collection . . . . .	23
B.4. Network Configuration Collection . . . . .	23
Authors' Addresses . . . . .	24

# Clarification: Enterprise Boundary

- Intent was not to imply on-prem
- Inclusive of off-prem
  - Cloud-based services/accounts

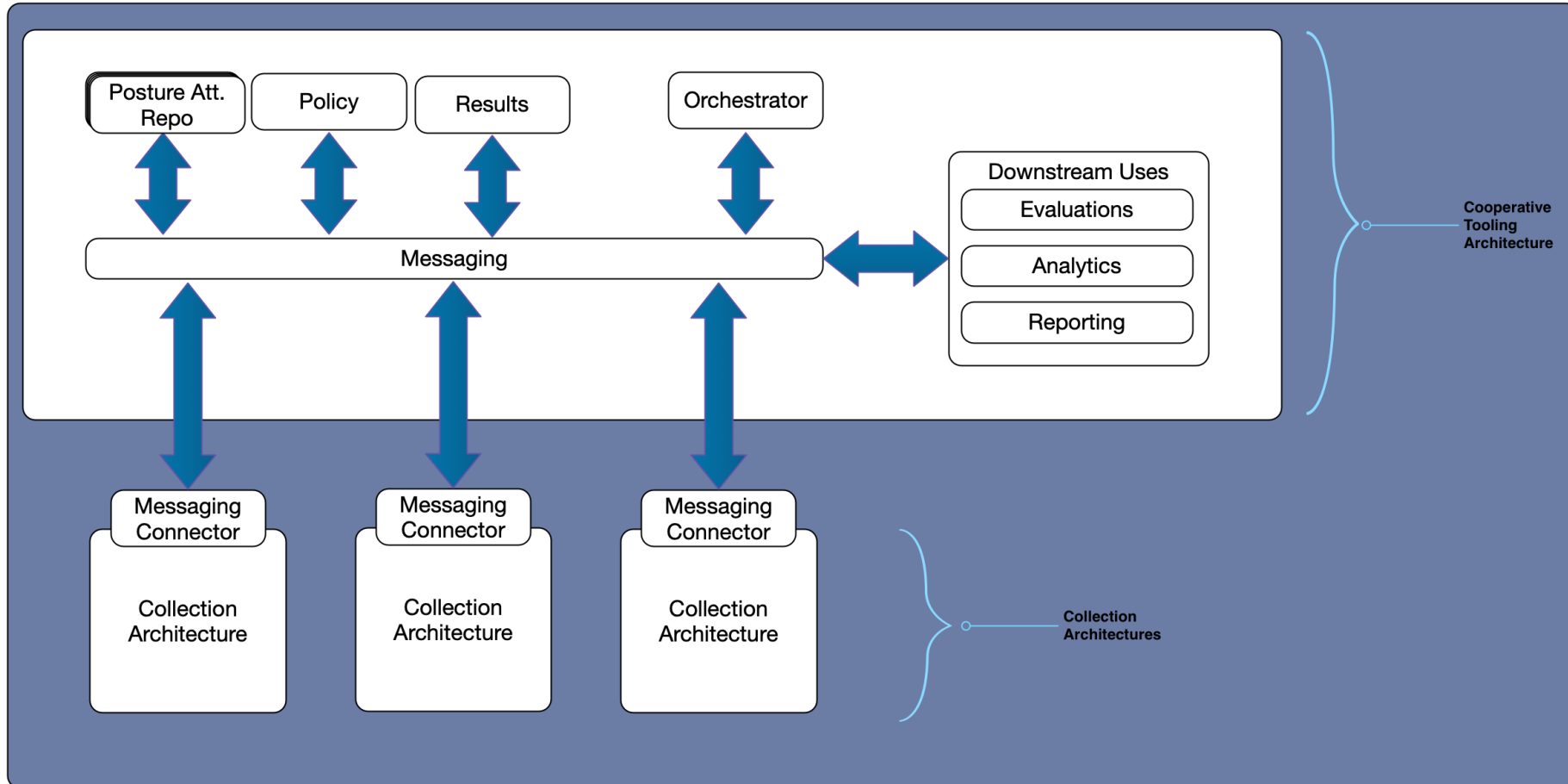


# Clarification: Capability vs. Interface vs. Operations

- **Capability:** Component  $X$  can assess configurations for target system classes  $A$ ,  $B$ , and  $C$  using dialect  $L$  of data model  $M$ 
  - Product Foo can assess configuration for Windows, MacOS, and AWS using OVAL 5.11.2
- **Interface:** Component  $X$  implements the SACM-standard operations to carry out a capability
  - Configuration assessment of Windows 10 using OVAL 5.11.2
- **Operation:** Component  $X$  can *collect* data from target system  $Y$ 
  - Gather system characteristics from Windows 10

***Interaction??***

# Clarification: Sub-architectures



# Clarification: Components

- Initially focus on configuration management
- Propose components
- Provide descriptive details for each proposed component
  - Capabilities
  - Interfaces
  - Required/supported operations

# Answers to Open Questions

- Should workflows be documented in this draft or in separate drafts?
  - Start in the draft, and create a new draft only when necessary
- Should interfaces be documented in this draft or in separate drafts?
  - Start in the draft, and create a new draft only when necessary