SACM Architecture Redux

IETF 101

Adam Montville

Center for Internet Security

An assertion…

…SACM ideally intends to enable a cooperative ecosystem of tools from disparate sources with minimal operator configuration.

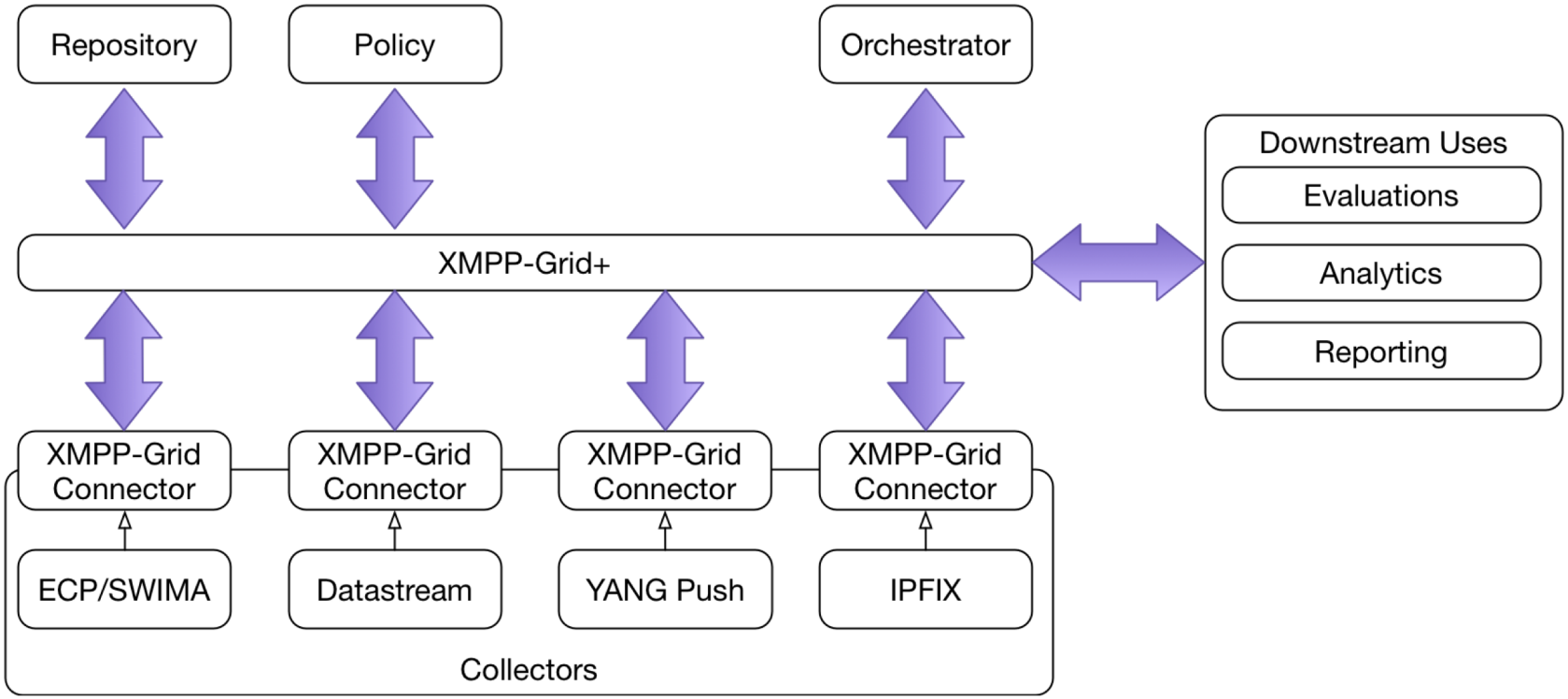
Another assertion…

…[our architectural solution] approaches [are] sometimes thought to be at odds with each other - specifically ECP and XMPP-grid.

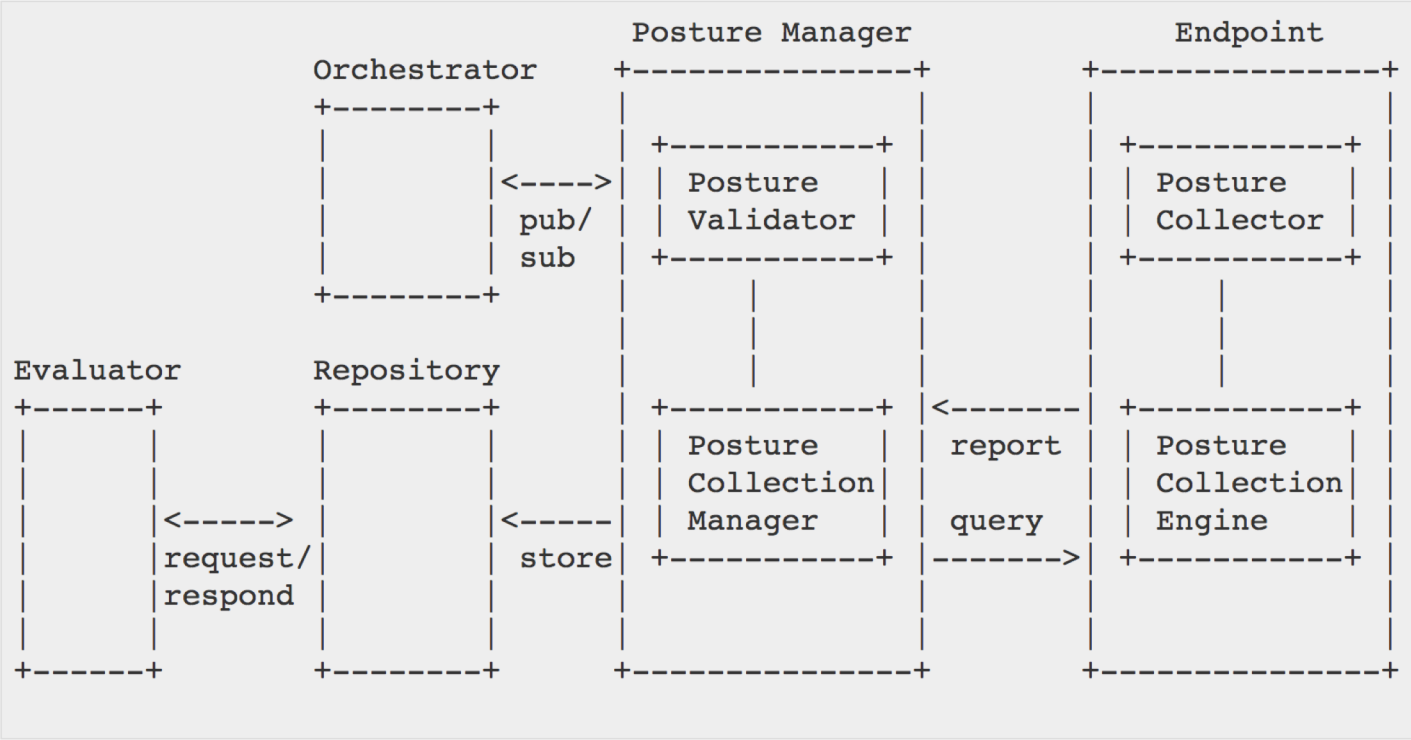
What if…

…both are relevant to us?

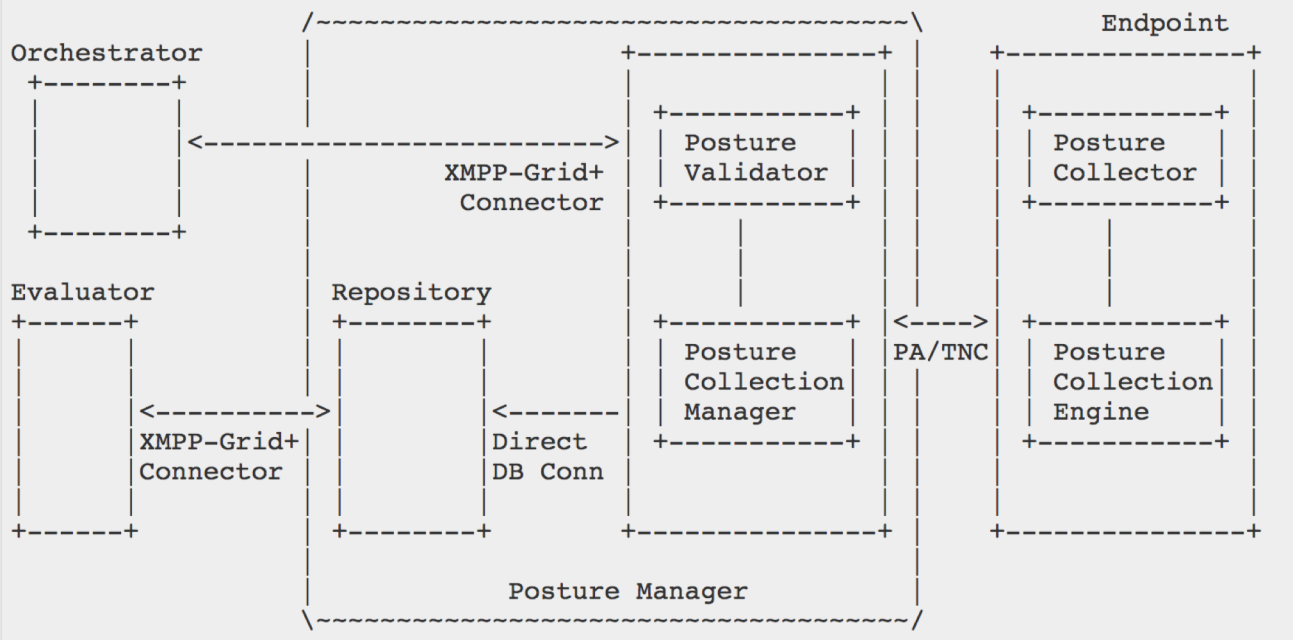
The Gist


Repository
Policy
Orchestrator
Downstream Uses
Evaluations
Analytics
Reporting
XMPP-Grid+
XMPP-Grid Connector
XMPP-Grid Connector
XMPP-Grid Connector
XMPP-Grid Connector
ECP/SWIMA
Datastream
YANG Push
IPFIX
Collectors

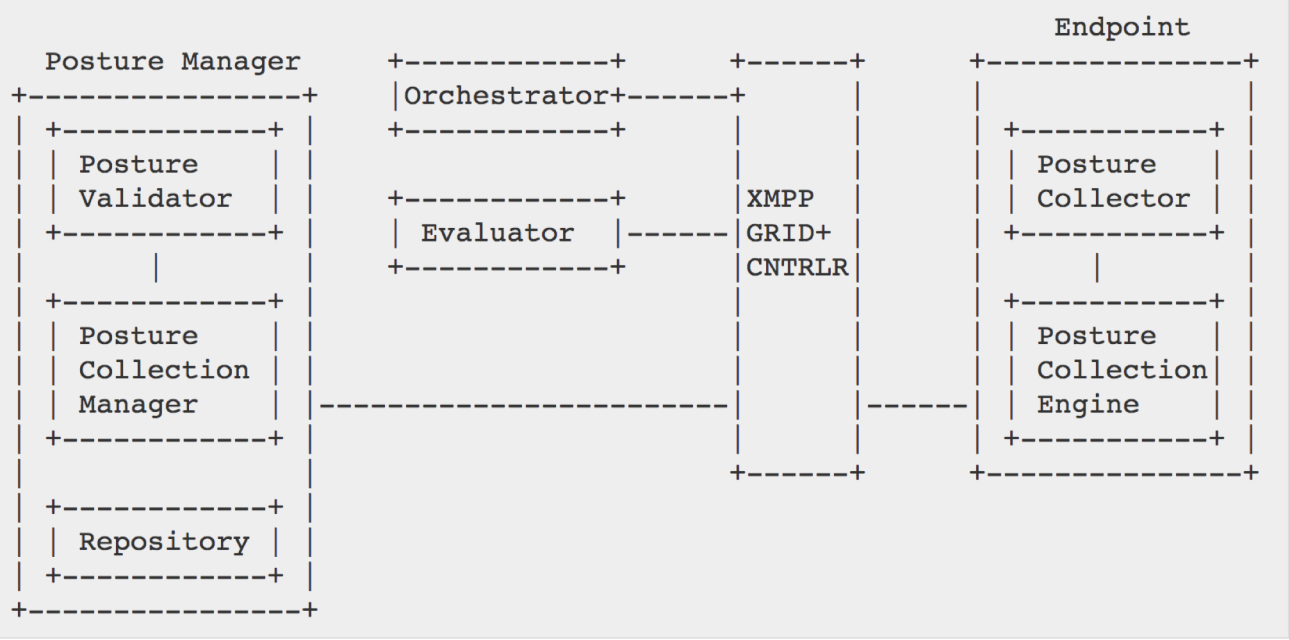
ECP 1


Posture Manager
Endpoint
Orchestrator
pub/
sub
Posture
Validator
Posture
Collector
Evaluator
Repository
request/
respond
store
Posture
Collection
Manager
report
query
Posture
Collection
Engine

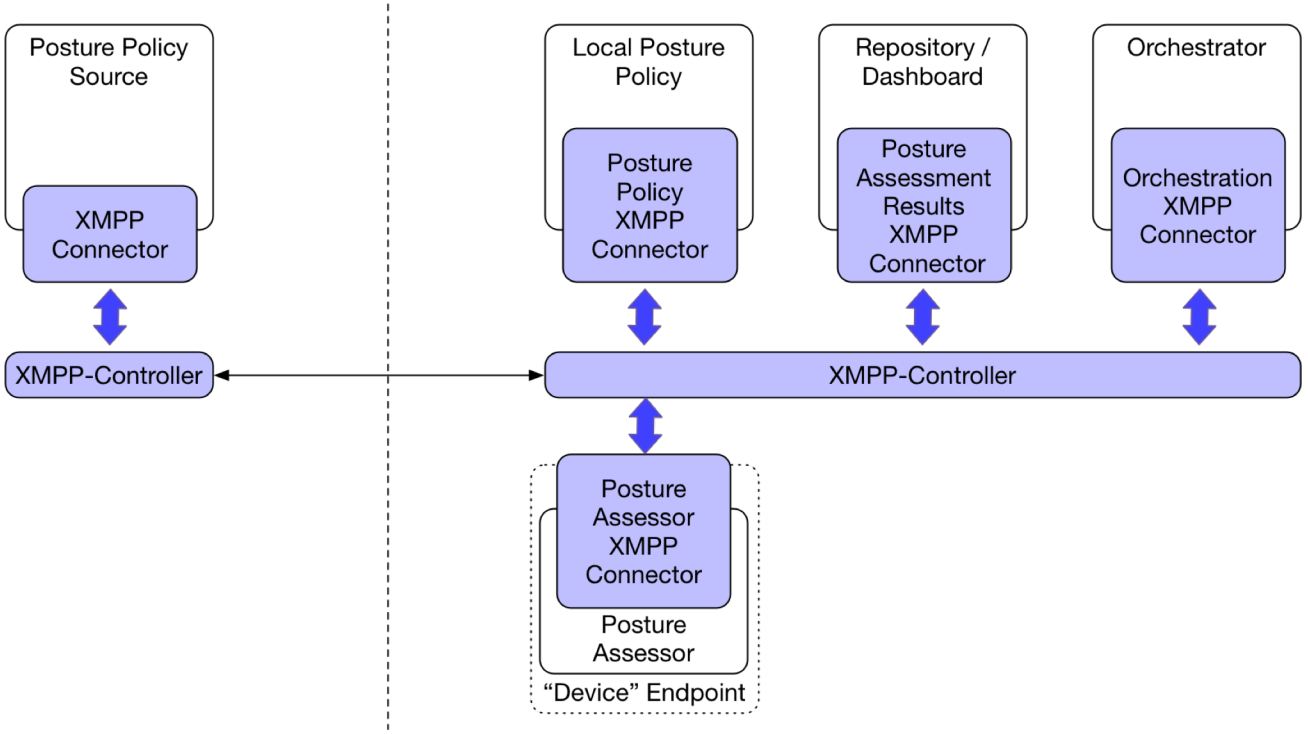
ECP 2


Endpoint
Orchestrator
XMPP-Grid+
Connector
Posture
Validator
Posture
Collector
Evaluator
Repository
Posture
Collection
Manager
PA/TNC
Posture
Collection
Engine
XMPP-Grid+
Connector
Direct
DB Conn
Posture Manager

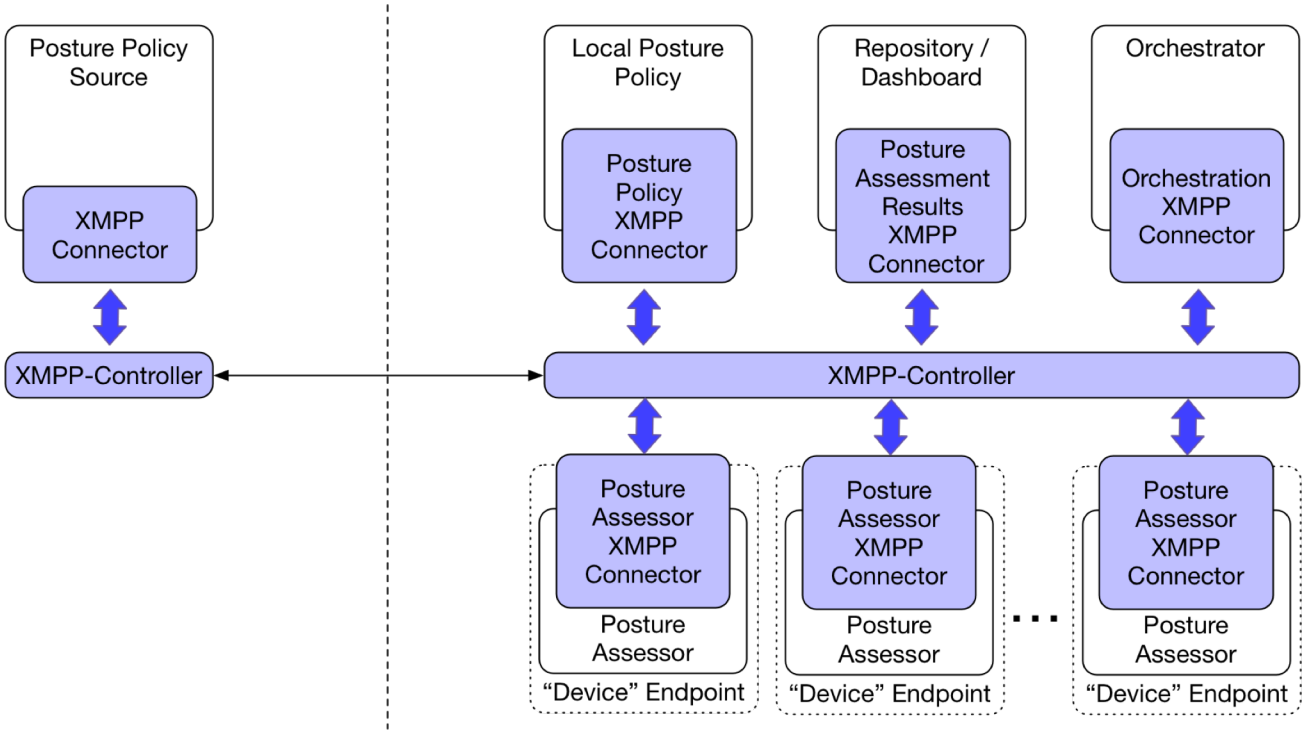
ECP 3


Posture Manager
Posture Validator
Posture Collection Manager
Repository
Orchestrator
Evaluator
XMPP GRID+ CNTRLR
Endpoint
Posture Collector
Posture Collection Engine

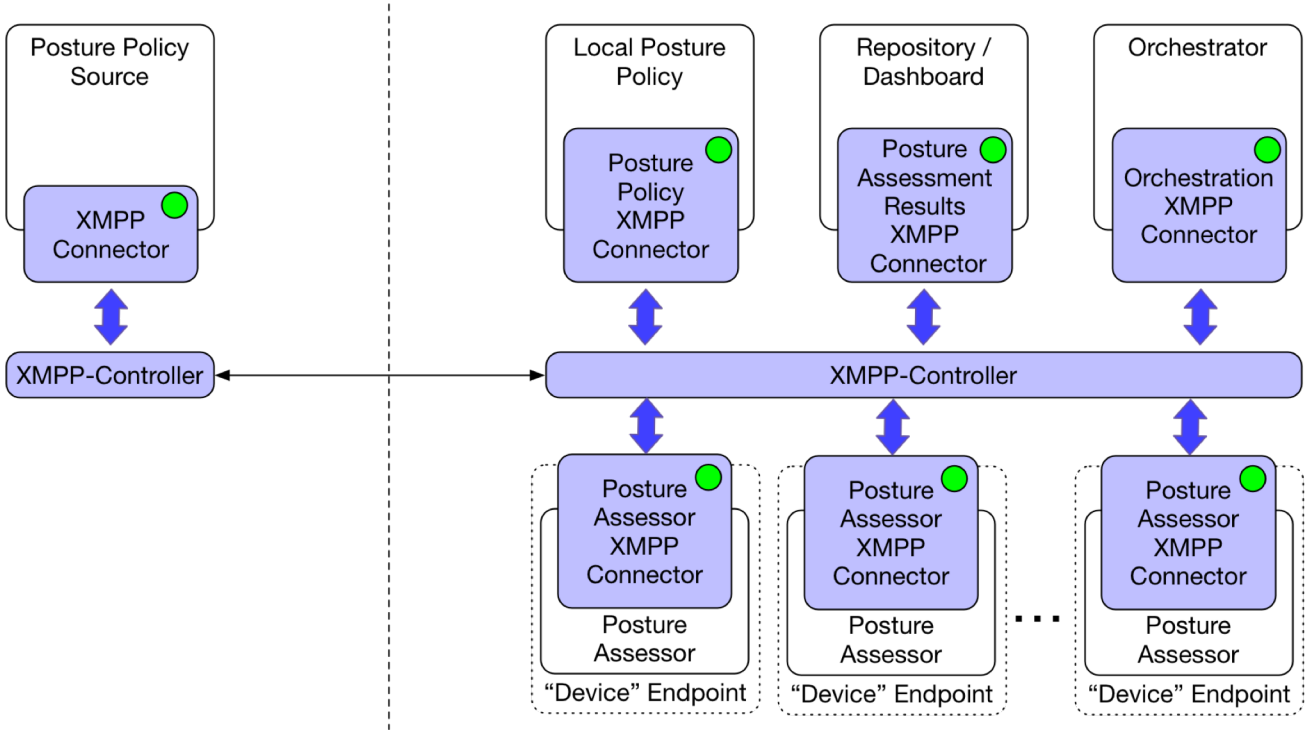
Next…


Posture Policy Source
XMPP Connector
XMPP-Controller
Local Posture Policy
Posture Policy XMPP Connector
Repository / Dashboard
Posture Assessment Results XMPP Connector
Orchestrator
Orchestration XMPP Connector
XMPP-Controller
Posture Assessor XMPP Connector
Posture Assessor
"Device" Endpoint

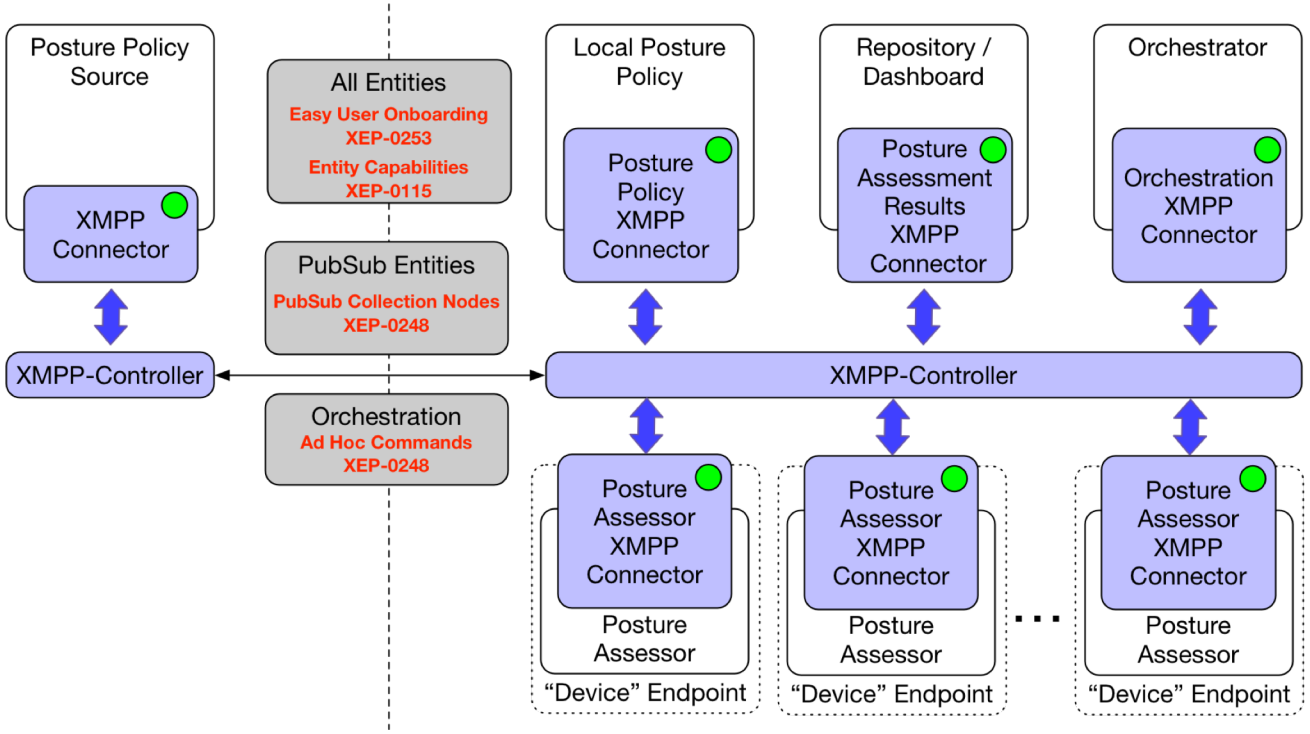
Agents as XMPP Clients



XMPP Presence Opens Doors



Potential XMPP Extensions



Possible SACM Components

Repository
- Vulnerability Information
- Software Inventory
- Configuration Policy
- Configuration State

Collector
- Software Inventory Collector
- Vulnerability State Collector
- Configuration State Collector

Evaluator
- Software Inventory
- Vulnerability State
- Configuration State

Orchestrator
- Vulnerability Management
- Configuration Management
- Asset Management

Going Forward…

Welcome contributions.

Continue exploration and hackathons.

Pick one or two capabilities and associated components for focus.

AND

Consider contributions to XMPP-Grid in MILE

Or…Create XMPP-Grid+ here in SACM

Or…Do something else for message transfer