Security Automation & IETF SACM

Workshop on Security Incident Information Sharing (SIIS)

David Waltermire

7/26/2013

What is Security Automation?

"We need a much greater focus on standardization and automation to allow humans to get out of the loop of manual defense and focus instead on human-worthy activities" – Tony Sager

- Carrying out well-understood security and security-related operational activities using computer assisted mechanisms
- Applying technologies and techniques that support security-oriented risk-based decision making

Why Automate Security?

- Constrained fiscal environment
  - Increase efficiency
  - Maximize the use of scalable, enterprise-level technology
- Reduce knowledge deficit
  - Rapid information sharing across the entire enterprise
  - Use of machine-readable, standard forms
  - Integrate multiple endpoint perspectives
- Establishing standards of due diligence
  - For buying products
  - For administering hosts and networks safely
  - For detecting attacks
  - For sharing information

Same Information / Different Views

Systems/Network Operations

Are we healthy?

- Verify compliance
- Remediate

- Authorized software
- Compliance with organizational configuration policies
- Proper user and device behavior

Prevent

Security Operations/Network Defense

Are we under attack?

- Observe activity
- Respond

- Unauthorized or malicious software
- Unauthorized changes to configurations
- Unauthorized user and device behavior

Detect

What is needed?

- Integration of Technologies
  - Integrate security and operational endpoint perspectives through use of common standards
  - Scalable, standardized architecture for endpoint data collection
- Interoperability
  - Standardized protocols, data models, identifiers that support the architecture
  - Modular security components
- Consensus Standards
  - Broaden agreement on approaches
  - Work to insure international adoption

IETF Security Automation & Continuous Monitoring (SACM)

Scope: Assessment of endpoint posture

Endpoint: Any computing device that can be connected to a network. This includes: laptops, desktops, servers, cell phones, or any device that may have an IP address.

Posture: Configuration and/or status of hardware or software on an endpoint as it pertains to an organization's security policy.

Proposed Use Cases

- Departmental Software Policy Compliance
- Vulnerable Endpoint Identification
- Suspicious Endpoint Behavior
- Compromised Endpoint Identification

Departmental Software Policy Compliance

Description: Limit software used on an endpoint to software that is organizationally approved; ensure approved software is appropriately configured according to organizational policy.

Dependencies:

- Definition of organizationally approved software whitelist and configuration settings
- Computer configured to download and install software patches each night
- Know what endpoints exist and who is responsible for them

Activities:

- Check computer against organizational policies when it connects to a network and regularly thereafter (perhaps as posture changes are detected)
- Assess the posture of the computer and report compliance with policy
- Block execution of unauthorized / misconfigured software
- Endpoint owners remedy non-compliant software

Post Conditions:

- Appropriate individuals understand what software is in use on endpoints they are responsible for
- Unauthorized and improperly configured software is prevented from executing
- Appropriate individuals are taking action to remove or properly configure software

Vulnerable Endpoint Identification

Description: When a zero-day exploit is detected in the wild, a security engineer needs to determine how exposed an organization is or has been to it.

Preconditions:

- Understand the vulnerability (e.g., vulnerable software components, vulnerable software ids, exploit characteristics)
- Know what endpoints exist and who is responsible for them

Activities:

- Identify vulnerable conditions on endpoints (e.g., presence of vulnerable software components)
- Report findings to stakeholders
- Prioritize remedies based on endpoint characteristics and organizational risk management decisions

Post Conditions:

- Appropriate individuals understand of the organization's exposure to and potential impact of the identified 0-day
- Appropriate individuals are taking action to further assess or mitigate the organization's posture regarding this 0-day

Compromised Endpoint Identification

Description: Use knowledge of specific indicators of compromise to identify compromised endpoints.

Preconditions:

- Know what endpoints exist and who is responsible for them
- Identify indicators of compromise through shared information or organizational experience

Activities:

- Identify compromised endpoints and understand the scope of the compromise
- Report findings to stakeholders
- Prioritize remedies based on endpoint characteristics and organizational risk management decisions

Post Conditions:

- Appropriate individuals understand the nature and extent of the compromise
- Appropriate individuals are taking action to further assess or mitigate the organization's posture regarding the compromise

Suspicious Endpoint Behavior

Description: Detecting a connection attempt to a known-bad Internet host by a botnet zombie that has made its way onto an organization's IT systems.

Preconditions:

- Maintenance of a list of known-bad internet hosts
- Know what endpoints exist and who is responsible for them

Activities:

- Detect C^2 traffic using network monitoring capabilities
- Identify changes to the endpoints software inventory and configuration; determine if changes represent a compromise

Post Conditions

- Appropriate individuals understand the nature and extent of the compromise
- Appropriate individuals are taking informed action to further assess or remedy affected endpoint posture relating to the compromise
- Measures are put in place to avoid future compromise

Use Case Discussion

- Are these the right use cases to consider?
- Are there missing dimensions within a specific use case?
- Are there other important use cases to consider?

Architecture - General Thoughts

- Vendor Independent
  - Device Types – computing hosts (e.g., clients, servers), network infrastructure, virtualized, mobile
  - Software Distribution Models – User installed, black box, app store, virtual images
- Scalable
  - Support for small to large organizations
  - Network segmentation
  - Security zones
  - Batch vs. Incremental data
  - Reuse / tailoring of content across organizations / tools
- Timely
  - Event-based endpoint state data publication
  - On-demand/request-driven state collection
- Extensible
  - Flexible collection of device state using name/value tuples (e.g., configuration item, software inventory)
  - Allow linking to underlying collection mechanism for greater context
  - Endpoint identification (e.g., hardware/software sources, network info)
- Secure
  - Tie endpoint state to endpoint identity
  - Data integrity (e.g., XMLDSig, TLS)
  - Data confidentiality (e.g., XML Encryption, TLS)

Current Architecture Proposals

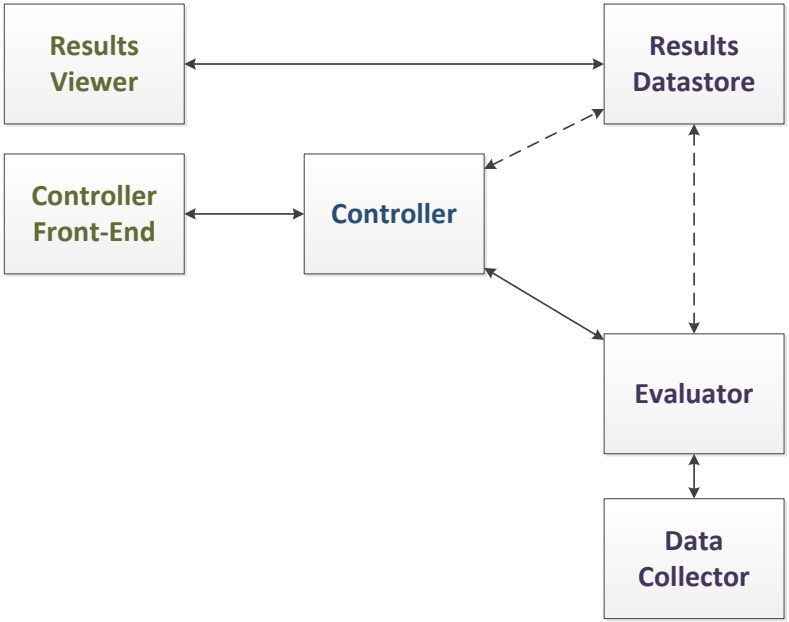
- Gunner Engelbach – SACM Email List
- draft-waltermire-sacm-architecture-00
- draft-handt-sacm-alternate-architecture-01

Gunner Engelbach – SACM Email List

Source: Gunnar Engelbach

- Each “entity” exposes an interface

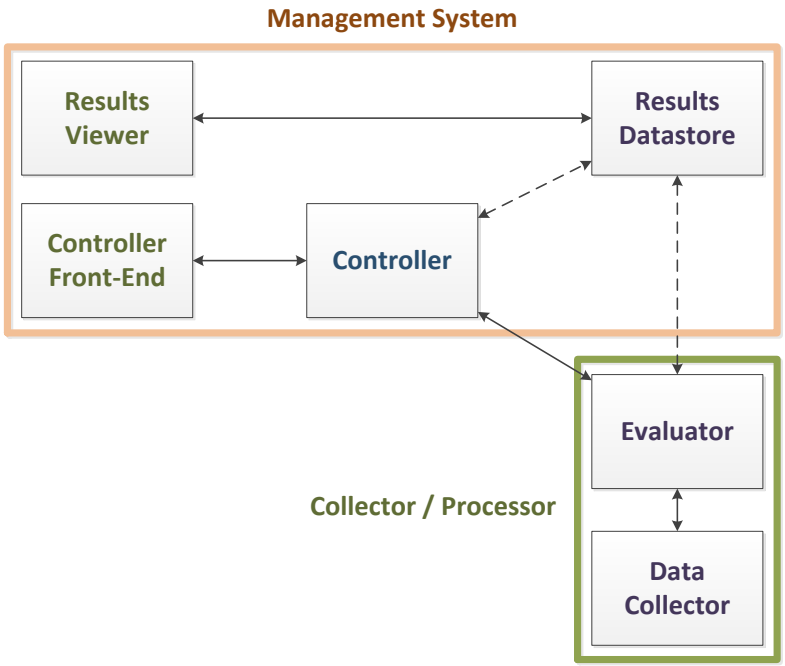
- **Data Collector**
  - Receive requests to collect data
  - Return collected data
- **Evaluator**
  - Receive/responds evaluation requests
  - Sends/receives data collection requests
  - Interacts with data store (optional)
- **Controller** – Central Management
- **Controller Front-End**
  - Configure associations with evaluators
  - Manage evaluation requests
- **Results Datastore** – Manages generated results
- **Results Viewer** – Presents data



Gunner Engelbach – SACM Email List (Cont'd)

Source: Gunnar Engelbach

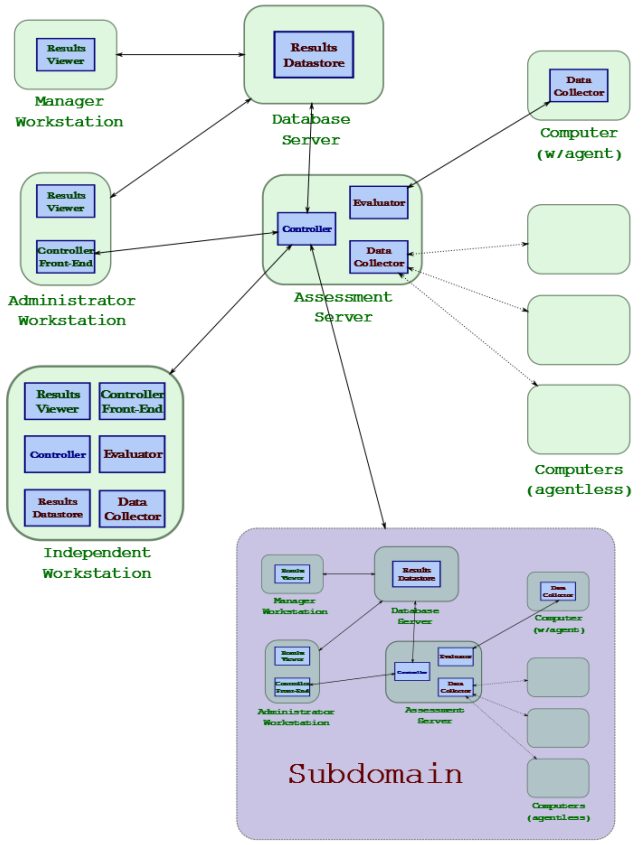
- **Management System**
  - Provides user interface
  - Supports queries to any number of evaluators
- **Collector / Processor**
  - Responsible for local data collection
  - Evaluator could support data collector interface, allowing it to be used by other evaluators



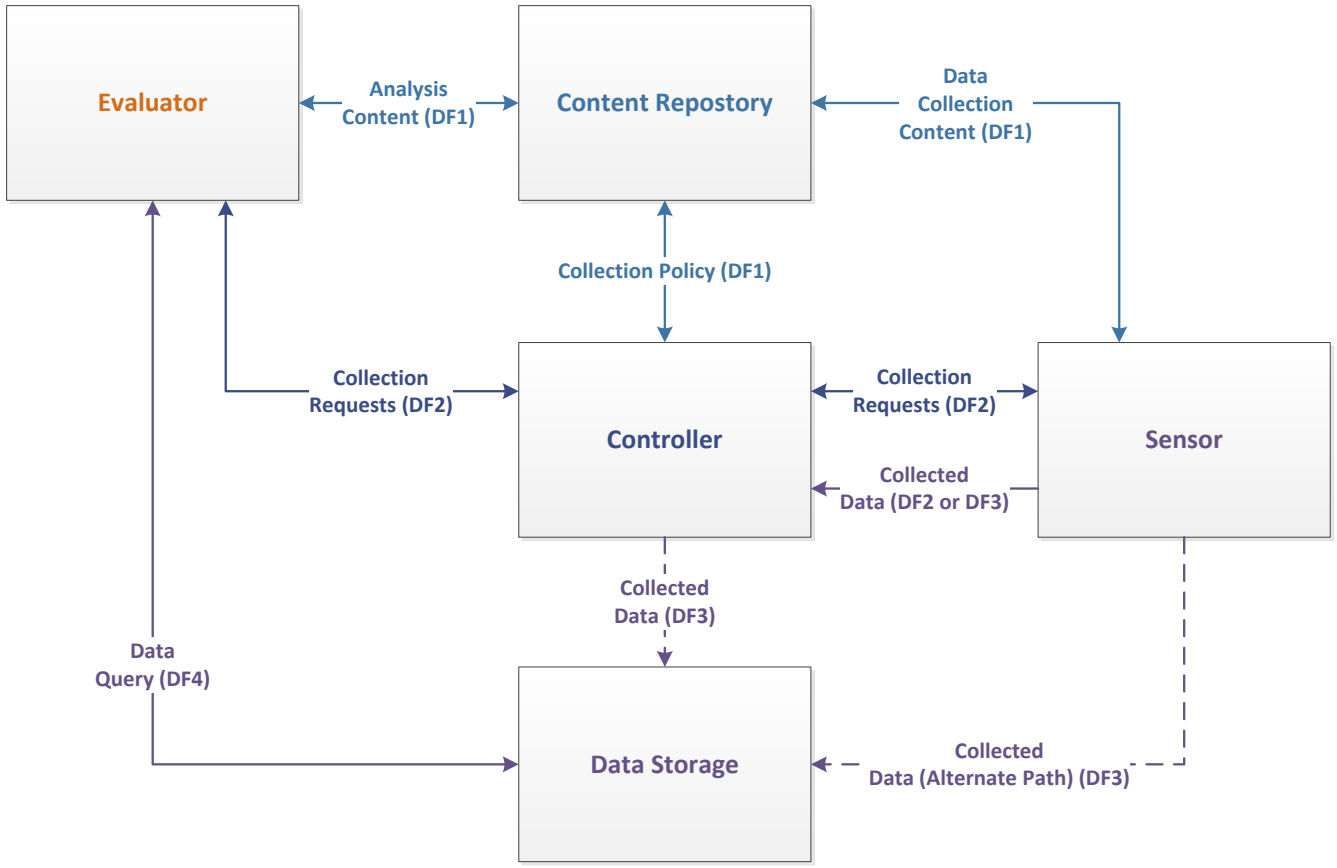
Gunner Engelbach – SACM Email List (Cont'd)

Source: Gunnar Engelbach

- Green boxes represent hosts
  - Necessary interfaces exposed
  - Internal interfaces are not shown
- Assessment server contains entities to:
  - Perform scheduled tasks
  - Evaluate data collected from agents
  - Use of internal data collectors (agentless)
  - Retrieving data from a separate, independent enclave
- Independent workstation can perform and display assessments, but can be linked to enterprise management system
- Inter-connections between domains enable a more comprehensive view of the enterprise



draft-waltermire-sacm-architecture-00



draft-waltermire-sacm-architecture-00 (Cont'd)

Represents an "abstraction" of different functional components

Controller

- Collection task management
- Sensor management
- Marshalling sensor data to data storage

Content Repository

- Manages metadata used for data collection and analysis – supports a data-driven approach

Sensor/Collector

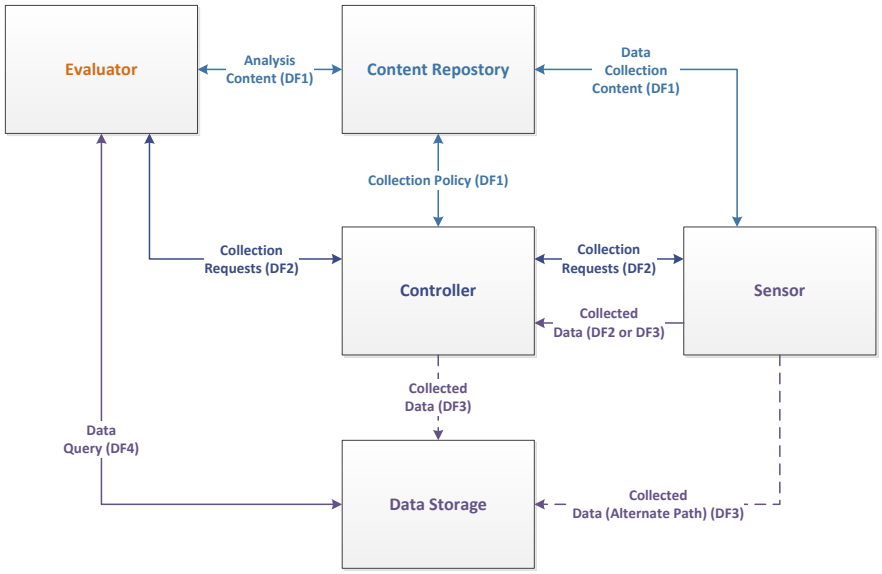
- Performs data collection based on events or tasks

Evaluator

- Performs requested analysis based on collected data

Data Storage

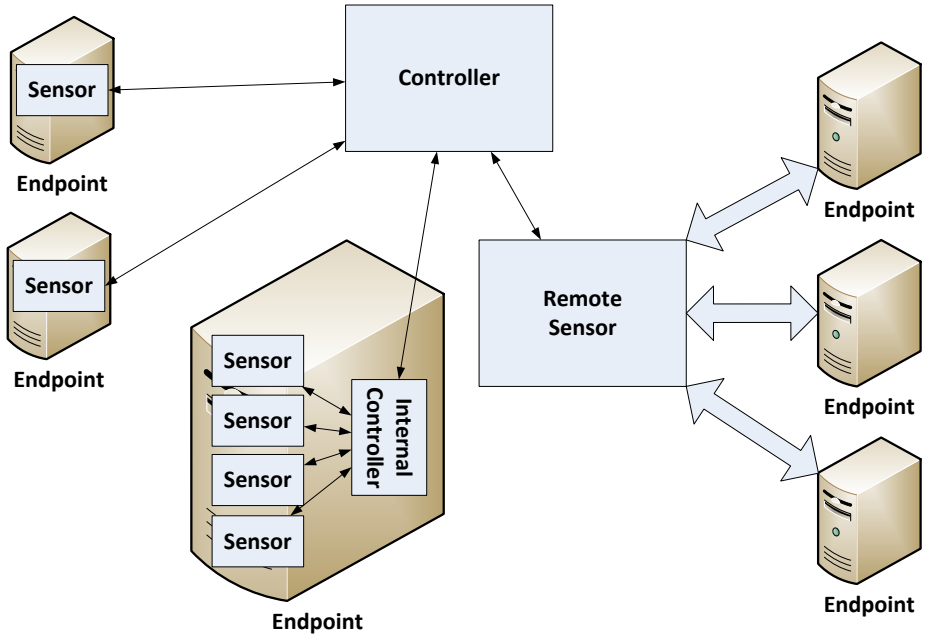
- Manages collected data
- Supports directed queries



draft-waltermire-sacm-architecture-00 (Cont'd)

Controllers may:

- Delegate to other controllers
- Manage remote, "agentless" sensors
- Manage a collection of sensor "agents"
- Manage an internal controller that manages many internal sensors



draft-handt-sacm-alternate-architecture-01

A concrete architecture example:

Border Protection Device (BPD)

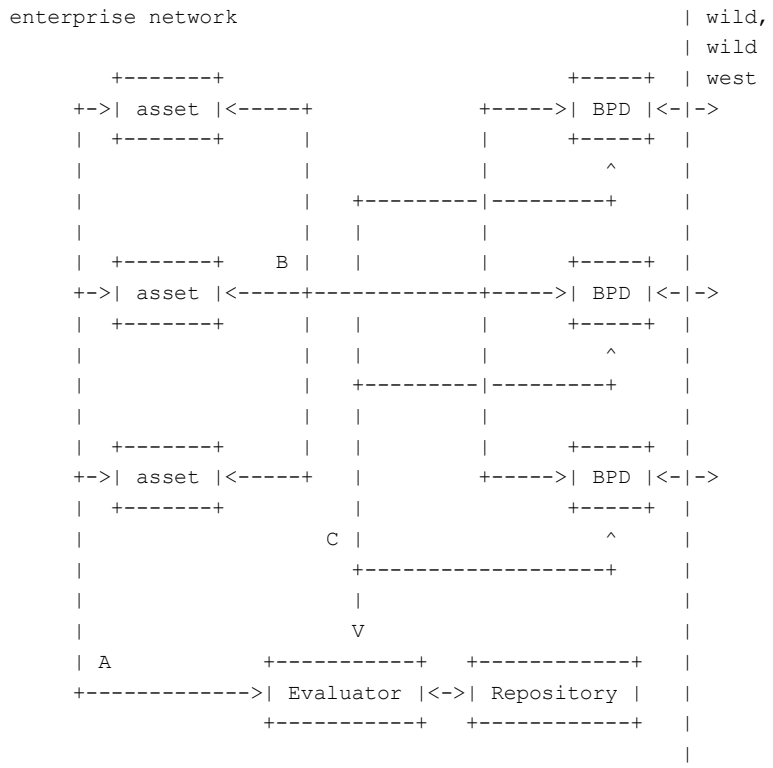
- A firewall and IDS (Intrusion Detection System) all rolled in to one.

Asset

- Either a host or a client

Evaluator

- Determines whether the asset is allowed access to the network



draft-handt-sacm-alternate-architecture-01 (Cont'd)

A lines

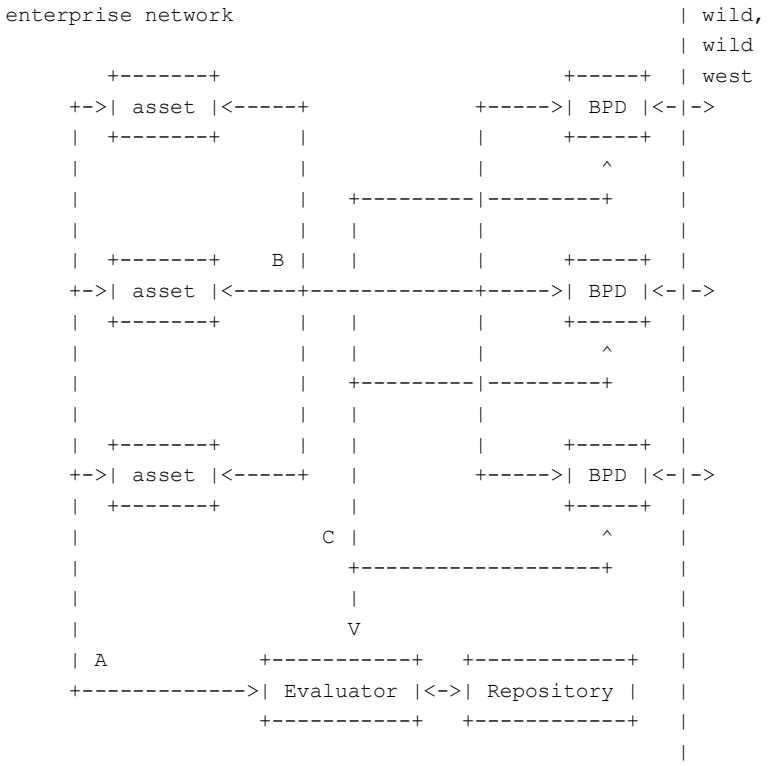
- NEA client/server performing posture collection, brokering, and exchange
- Asset has NEA client with one or more collectors performing posture collection
- Evaluator has NEA server with one or more evaluators performing posture evaluation
- Initial posture assessment when asset connects to network
- Ongoing maintenance of posture as well

B lines

- Network traffic
- BPDs insure assets are action appropriately

C lines

- Insure BPDs know how the asset should be acting



Architectural Themes

- Collection of endpoint posture across multiple perspectives (e.g., software inventory, configurations, vulnerability, unauthorized/malicious activity)
- Functional separation of data collection and analysis
- Use of content repositories to support data-driven data collection and analysis
- Central management of analysis and collection tasking
- Composition of multiple instances

Wrapping Up

- The SACM effort is still working through the process of identifying use cases, requirements, and architectural approaches
  - Common themes are starting to form
  - More work is needed
- We need your help to insure we are focusing on the appropriate dimensions of the problem
  - Contribute to the mailing list discussion
  - Submit use cases, requirements, and architectural drafts

Additional Information

IETF WG Page: http://datatracker.ietf.org/wg/sacm/

- Charter, drafts, mailing list info

Initial SACM WG Meeting @ IETF 87

Friday, August 2nd, 2013

11:20a – 1:30p

InterContinental Berlin - Tiergarten ½

Agenda:
https://datatracker.ietf.org/meeting/87/agenda/sacm/