Information Model Update

IETF 94
11/03/2015
Agenda

• Status

• Open issues

• Next steps
Status

• Discussed changes\(^1\) and issues during the last virtual interim meeting\(^2\)
  • Closed \#22\(^3\) and \#29\(^4\)
  • Discussed \#20\(^5\) and \#32\(^6\), but, they remain open
  • Received a request for a list of tasks and the required skillsets

• New thoughts on the triples example work\(^7\)

• Interest around developing a matching algorithm\(^8\)

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/commit/4918789e86936cd53a1340830803ae74eb02d63e
Representing elements in the IM

• Need a modeling syntax for representing IM elements¹

• Approaches mentioned on the list²
  • RFC7326³
  • draft-ietf- imap-information-model⁴
  • Unified Modeling Language (UML)⁵
  • Entity-Relationship (E-R) diagrams⁶

• Thoughts on these approaches? Are there others to consider?

Example¹ (RFC7326 and lmap-info-model)

1. Please note that I used this example because it was very convenient :). It does not represent any agreed upon model for a network interface. Furthermore, it does not mean a decision has been made around whether or not a network interface is a hardware component, software component, both, or something else. That decision is currently being worked out on the list (https://www.ietf.org/mail-archive/web/sacm/current/msg03199.html).
1. Please note that I used this example because it was very convenient :). It does not represent any agreed upon model for a network interface. Furthermore, it does not mean a decision has been made around whether or not a network interface is a hardware component, software component, both, or something else. That decision is currently being worked out on the list (https://www.ietf.org/mail-archive/web/sacm/current/msg03199.html).
Task descriptions and required skillsets

• Tasks so far\(^1\)
  • Survey of mandatory to implement information
  • IM modeler
  • Data model reviewer
  • Developer
  • Transport reviewer (TBD)

• Are there other tasks that we want to consider? Where would we want to put this information?

---

Should reports be out of scope\(^1\)?

• Reports contain provenance information and summarize endpoint attribute assertions, evaluation results, etc.

• Metrics and presentation vary greatly depending on the needs of an organization

• Do we really need to develop a standard for reports? Or, can we just provide the information necessary to generate reports?

\(^1\) [https://github.com/sacmgw/draft-ietf-sacm-information-model/issues/30](https://github.com/sacmgw/draft-ietf-sacm-information-model/issues/30)
Should SACM Components be defined in the IM?

- The IM contains a section that describes various SACM Components
  - External collector, evaluator, and report generator

- The IM should focus on modeling the information needed by the SACM Components and not the actual SACM Components

- Can we remove this text from the IM and include it in the Architecture as the editors see fit?

SACM Components must have time sync?

• Reliable and trustworthy time synchronization\(^{12}\) is needed to support:
  • Authentication
  • Association of timestamps with collected attributes
  • Correlation of events

• Different types of timestamps include:
  • Creation
  • Observation / collection
  • Publish
  • Relay
  • Storage

• Include the following normative requirements for data models?
  • SACM Components residing on target endpoints SHOULD implement time sync and correct timestamps
  • SACM Components that do not reside on target endpoints MUST implement time sync and add correct timestamps

Next steps

- Send outcome of open issues discussion to the list for last call
- Further discuss the new thoughts around the triples example
- Determine how to handle algorithms
- From there, it depends on our path forward