Information Model Update

SACM Virtual Interim Meeting

09/24/2015

Agenda

- Status

- Open issues

- Next steps

Status

- IM restructuring available on GitHub123
    - Framework, assets, and elements

- Working on a proposal to use triples4 for defining IM elements
    - Network interface [subject] has a [predicate] IPv4 address [object]

- Working on a proposal with options for representing IM elements

```
Container NetworkInterface {
    Container IPv4Address{
        type string;
    }
}
```

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/22
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03186.html
3. https://github.com/sacmwg/draft-ietf-sacm-information-model/commit/4918789e86936cd53a1340830803ae74eb02d63e
4. See Endpoint ID Design Team Meeting recording for 8/21 in Dropbox

Standards track or not?

- IM is currently listed in the charter as a standards track document1, however, the corresponding milestone2 says the IM is informational

- So far, consensus on the list says the IM should be standards track
  - Standards track means normative guidance for implementations

- Can we update the milestone to say the IM is standards track?

1. https://datatracker.ietf.org/wg/sacm/charter/
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03180.html

How to handle discrepancies between -01 and -02?

- From -01 to -02, some sections went missing[1]
  - E.g. Section 1.1 listing changes in -01 disappeared

- It is not clear whether the changes were intentional or accidental

- How should we address this issue?
  - Received feedback on the list to re-integrate the missing sections[2]

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/20
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03295.html

What do we call a logical grouping of information?

- Currently use "container" to describe logical groupings of attributes, metadata, and other containers
  - There is concern that this term implies a hierarchy

- Alternative terms might be "construct" "class", or "object"

  - Is "container" good enough? Or, would we prefer something else?

Should reports be out of scope?

- Reports contain provenance information and summarize endpoint attributes 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?

SACM Components must have time sync?

- Reliable and trustworthy time synchronization[1,2] 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

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/25
2. http://www.ietf.org/mail-archive/web/sacm/current/msg03175.html

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?

Short-term path forward?

- Is there a need for a short-term change in direction1?
    - There is still a lot of work to be done on the core WG documents
    - A handful of editors are spread across multiple WG documents
    - We need more contributors

- One approach is to focus on solutions drafts that may attract new contributors
    - So far, consensus is leaning towards a shift to solutions drafts
    - There is concern that it will be difficult to evaluate solutions without complete WG documents

1. http://www.ietf.org/mail-archive/web/sacm/current/msg03163.html

Next steps

- Send outcome of open issues discussion to the list for last call

- Finish triples proposal and send it to the list for discussion

- Send options for representing IM elements to the list for discussion

- Specify one or two IM elements to serve as a template

- From there, it depends on our short-term path forward