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
[2] https://www.ietf.org/proceedings/interim/2015/09/24/sacm/minutes/minutes-interim-2015-sacm-5
[3] https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/22
[4] https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/29
[5] https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/20
[6] https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/32
[7] http://www.ietf.org/mail-archive/web/sacm/current/msg03404.html
[8] http://www.ietf.org/mail-archive/web/sacm/current/msg03397.html

Representing elements in the IM

- Need a modeling syntax for representing IM elements[1]
- Approaches mentioned on the list[2]
  - RFC7326[3]
  - draft-ietf-lmap-information-model[4]
  - Unified Modeling Language (UML)[5]
  - Entity-Relationship (E-R) diagrams[6]
- Thoughts on these approaches? Are there others to consider?

[1] https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/27
[2] https://tools.ietf.org/rfc/rfc7326.txt
[3] https://tools.ietf.org/id/draft-ietf-lmap-information-model-07.txt
[4] http://www.uml-diagrams.org/
[5] https://en.wikipedia.org/wiki/Entity%E2%80%93relationship_model
[6] http://www.ietf.org/mail-archive/web/sacm/current/msg03290.html

Example[1] (RFC7326 and lmap-info-model)

```
CLASS NetworkInterface EXTENDS HardwareComponent {

    name            : string

    index           : int

    hardwareAddress : MACAddress

    type            : enum {ether, fddi, loopback, …}

    flags [0..n]    : enum {up, broadcast, debug, …}

}


Network Interface (Class):

name             string       The name of the interface.

index            int          The index of the interface.

hardwareAddress  MACAddress   The IEEE 802 MAC address.

type             Enumeration  Describes the type of the network
                              interface.

flags [0..n]     Enumeration  Describes the flags set on the
                              interface.
```

```
Definition of network-interface-obj


object {

    string              name;

    int                 index;

    mac-address-obj     hardware-address;

    string              type;

    string              flags<0..n>;

} network-interface-obj;


A network-interface-object consists of the following elements:

name:                The name of the interface.

index:               The index of the interface.

hardwareAddress:     The IEEE 802 MAC address.

type:                Describes the type of the network interface. The
                     value 'ether' indicates…

flags:               Describes the flags set on the interface. The
                     value 'up' indicates…
```

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).

Example[1] (UML and E-R Diagram)

```
+--------------------+

| HardwareComponent |

+--------------------+

| …                  |

+--------------------+

          ^

          |

+----------------------+

| NetworkInterface    |

+----------------------+

| string name          |

| int    index         |

| enum   type          |

| enum   flags [0..n] |<>-

+----------------------+  |

                          |

         [ MACAddress ]--|
```

```
The aggregate class that constitutes a
NetworkInterface is:

MACAddress
    One. The IEEE 802 MAC address.

The Network Interface class has four
attributes:

name
    Required.  String. The name of
    the interface.

index
    Required. Int. The index of the
    interface.

type
    Required. Enum. Describes the
    type of network interface.

flags
  Optional. 0..n. Describes the flags
  set on the interface.
```

```
+--------------------+

| HardwareComponent |

+--------------------+

         |

    < IS-A >

         |

+-------------------+

| NetworkInterface |----

+-------------------+   |

 |----( name )          |

 |----( index )         |

 |----( type )          |

 |----(( flags ))       |

                        |

+-------------+         |

| MACAddress |----< HAS-A >

+-------------+
```

```
The NetworkInterface entity IS-A
HardwareComponent and HAS-A MACAddress.

It has four attributes:

name
    Required.  String. The name of
    the interface.

index
    Required. Int. The index of the
    interface.

type
    Required. Enum. Describes the
    type of network interface.

flags
  Optional. 0..n. Describes the flags
  set on the interface.
```

[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?

[1] http://www.ietf.org/mail-archive/web/sacm/current/msg03397.html

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/sacmwg/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?

1. https://github.com/sacmwg/draft-ietf-sacm-information-model/issues/33

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

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

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[1]

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