SACM
IETF 99

July 20, 2017

Adam Montville

Karen O'Donoghue

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Administrative Tasks

- Note takers
- Jabber Scribe

Agenda

1. WG status – chairs – 5m
2. Hackathon results – David Waltermire 15m
3. Hackathon results – Henk Birkholz 15m
4. Existing Work Disposition/Open Issues (total: 40m)
    1. SWIMA – Charles Schmidt 15m
    2. Terminology – Henk Birkholz 15m
    3. CoSWID - Henk Birkholz 10m
5. TNC 2.0 Update - Charles Schmidt 15m
6. ROLIE Software Descriptor Extension - Stephen Banghart - 20m
7. ROLIE Checklist Extension - Bill Munyan - 5m
8. Charter Discussion / Way Forward - Chairs/AD - remaining time
    1. Information Model
    2. Architecture
    3. Existing WG drafts
    4. Existing individual drafts
    5. Charter
    6. Milestones

Status

- Updates to CoSWID, IM, SWIMA, Requirements, and Terminology
- Requirements has a DISCUSS in IESG
- New submission: ROLIE Extension - Configuration Checklist
- Charter
- Milestones
- Hackathon

Way Forward

- <for discussion>

The Three Things

1. Collection
2. Evaluation
3. Messaging

Collection

The WG will define a way to provide to provide two types of imperative guidance to the correct SACM collectors:1) Which target endpoints to collect from and 2) what to collect fromthis target endpoints. When classified, a set of instructions, such as VDD or YANG filter expressions, can be brokered to the appropriate collectors. Alas, detecting and classifying beforehand might require orchestrating functions that go beyond the set of capabilities a SACM collector can provide. Manual configuration of targets and corresponding collection profiles will not scale and does not seem to be a viable option."

Evaluation

The working group will produce a standards track document that describes a criteria language capable of being evaluated against endpoint posture information to produce a standardized result. The language will support complex Boolean statements, comparison operators, and functions for string manipulation; and will be extensible enough to be applicable to the full range of collected posture attributes. Additionally, this document will define an approach that allows data from any posture collection mechanism to be evaluated.

Messaging

The WG will define a control plane function to enable the discovery and orchestration between devices that can provide the requisite information sought by posture collectors, posture evaluators or both. As an example, a document that describes an instance of such a control plane and transfer protocol for data, is through the use of XMPP and extensions as needed to demonstrate XMPP's applicability to SACM.