

SACM
Internet-Draft
Intended status: Informational
Expires: December 10, 2014

N. Cam-Winget
Cisco Systems
June 8, 2014

Secure Automation and Continuous Monitoring (SACM) Requirements
draft-camwinget-sacm-requirements-04

Abstract

This document defines the scope and set of requirements for the Secure Automation and Continuous Monitoring working group. The requirements and scope are based on the agreed upon use cases.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 10, 2014.

Copyright Notice

Copyright (c) 2014 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

Abbreviated Title

June 2014

Table of Contents

1.	Introduction	2
2.	Requirements	2
2.1.	General SACM requirements	2
2.2.	Requirements based on Use Cases	4
3.	Acknowledgements	5
4.	IANA Considerations	5
5.	Security Considerations	5
6.	References	5
6.1.	Normative References	5
6.2.	Informative References	6
	Author's Address	6

[1.](#) Introduction

Today's challenges of evolving threats and improved analytics to address such threats highlight a need to automate the securing of both information and the systems that store, process and transmit the information. SACM's charter focuses on addressing some of these challenges in a narrower scope by bounding the task to address use cases that pertain to the posture assessment of endpoints.

This document focuses on describing the requirements for facilitating the exchange of posture assessment information, in particular, for the use cases as exemplified in [[I-D.ietf-sacm-use-cases](#)]. Also, this document uses terminology defined in [[I-D.ietf-sacm-terminology](#)].

[2.](#) Requirements

This document defines requirements based on the SACM use cases defined in [[I-D.ietf-sacm-use-cases](#)]. This section describes the requirements used by SACM to assess and compare candidate information models and protocols to suit the architecture. These requirements express characteristics or features that a candidate protocol or data model must be capable of offering so as to ensure security and interoperability.

[2.1.](#) General SACM requirements

The use cases defined in [[I-D.ietf-sacm-use-cases](#)] apply to many deployment scenarios. To ensure interoperability, scalability and flexibility in any of these deployments, the following requirements

are defined for all use cases:

G-001 Extensibility: the data models, protocols and transports defined by SACM must be extensible to allow support for non-standard and future extensions. The transport protocol must support easily

adding new operations while maintaining backwards compatibility. The query language must allow general inquiries as well as expression of specific paths to follow; retrieval of specific information based on an event, as well as on a continuous basis; and the ability to retrieve specific pieces of information, specific classes of information, and/or the entirety of available information. The information model must accommodate the addition of new data types and/or schemas in a backwards compatible fashion.

G-002 Interoperability: The data models, protocols and transports must be specified with enough details and state machine to ensure interoperability.

G-003 Scalability: The data models, protocols and transports must be scalable. SACM must support a broad set of deployment scenarios. As such, it is possible that the size or posture assessment information can vary from a single assessment that is small in (record or datagram) size to a very large datagram or a very large set of assessments and must be addressed by the SACM specifications defined.

G-004 Agility: The agility requirement is to ensure that the data model, protocols, transports and its implementations are suitable to fit in different deployment models and scenarios. Considerations for the lightweight implementations of data models and transports is required. Use cases, especially in the vulnerability assessment and threat defense applications require time criticality in both obtaining the information as well as consuming (e.g. parsing) the data.

G-005 Transport variability: Different transports must be supported to address different deployment and time constraints. Supporting transports at the Layer 2, Layer 3 and higher application layers.

G-006 Extensibility: a method for expressing both standard and non-standard (implementer-specific) data attributes while avoiding

collisions should be defined. For interoperability and scope boundary, an explicit set of data attributes as mandatory to implement should be defined and focused on Posture Assessment should be described to allow for interoperability too.

G-007 Access Control: To address security and privacy considerations, the data model, protocols and transport must consider authorization based on roles to only allow authorized requestors and publishers to access the information being requested or published.

[2.2.](#) Requirements based on Use Cases

This section describes the requirements that may apply to information models, data models, protocols or transports as identified by the use cases in [[I-D.ietf-sacm-use-cases](#)] and referenced by the section numbers from that draft.

REQ-001 Attribute Dictionary: Use Cases in the whole of [Section 2](#) describe the need for an Attribute Dictionary. With SACM's scope focused on Posture Assessment, the attribute collection and aggregation must have a well understood set of attributes inclusive of their meaning or usage intent.

REQ-002 Information Model: Use Case 2.1.1 describes the need for an Information Model to drive content definition. As SACM endeavors to reuse already existing standards which may have their own data models defined by instantiating an information model, the data models can be mapped to SACM's information model. See [[RFC3444](#)] for a description and distinctions between an information and data model.

REQ-003 Data Model to Protocol mapping: Use Case 2.1.1 describes the need to instantiate a data model that can map to the SACM protocols for posture content operations such as publication, query, change detection and asynchronous notifications.

REQ-004 Endpoint Discovery: Use Case 2.1.2 describes the need to discover endpoints and their composition.

REQ-005 Attribute based query: Use Case 2.1.2 describes the need for the data model to support a query operation based on a set of attributes to facilitate collection of information such as posture assessment, inventory (of endpoints or endpoint components) and configuration checklist. .

REQ-006 Information based query with filtering: Use Case 2.1.3 describes the need for the data model to support the means for the information to be collected through a query mechanism. Furthermore, the query operation requires filtering capabilities to allow for only a subset of information to be retrieved. The query operation may be a synchronous request or asynchronous request.

REQ-007 Asynchronous publication, updates or change modifications with filtering: Use Cases 2.1.3, 2.1.4 and 2.1.5 describe the need for the data model to support the means for the information to be published asynchronously. Similarly, the data model must support the means for a requestor to obtain updates or change modifications asynchronously. Like the query operation, these update

notifications can be set up with a filter to allow for only a subset of posture assessment information to be obtained.

REQ-008 Data model scalability: Use Cases 2.1.4 and 2.1.5 describes the need for the data model to support scalability. For example, the query operation may result in a very large set of attributes as well as a large set of targets.

REQ-009 Separation of Collection Request and Collection Action: the data model must distinguish the means to request for a data item to include enough information to properly identify the item to collect but the request could be separate and distinct from the actual method or process used to fulfill the request.

[3.](#) Acknowledgements

The authors would like to thank Barbara Fraser, Jim Bieda and Adam Montville for reviewing and contributing to this draft.

[4.](#) IANA Considerations

This memo includes no request to IANA.

[5.](#) Security Considerations

This document defines the requirements for SACM. As such, it is expected that several data models, protocols and transports may be defined or reused from already existing standards. This section will highlight security considerations that may apply to SACM based on the architecture and standards applied in SACM.

[6.](#) References

[6.1.](#) Normative References

[I-D.ietf-sacm-terminology]

Waltermire, D., Montville, A., Harrington, D., and N. Cam-Winget, "Terminology for Security Assessment", [draft-ietf-sacm-terminology-04](#) (work in progress), May 2014.

[I-D.ietf-sacm-use-cases]

Waltermire, D. and D. Harrington, "Endpoint Security Posture Assessment - Enterprise Use Cases", [draft-ietf-sacm-use-cases-07](#) (work in progress), April 2014.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

Cam-Winget

Expires December 10, 2014

[Page 5]

Internet-Draft

Abbreviated Title

June 2014

[6.2.](#) Informative References

[RFC3444] Pras, A. and J. Schoenwaelder, "On the Difference between Information Models and Data Models", [RFC 3444](#), January 2003.

[RFC5209] Sangster, P., Khosravi, H., Mani, M., Narayan, K., and J. Tardo, "Network Endpoint Assessment (NEA): Overview and Requirements", [RFC 5209](#), June 2008.

Author's Address

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way

San Jose, CA 95134
US

Email: ncamwing@cisco.com