DMTF Cloud Audit Data Federation Working Group (CADF) Charter

Dated 04/29/2011

Version: 1.0.7

Problem Space and Environment

Concerns over cloud provider security remain one of the top inhibitors to adoption of cloud deployment models. Potential consumers of cloud deployments understand and need assurance that the security policies they require on their applications are consistently managed and enforced "in the cloud" as they would be in their enterprise.

A cloud provider's ability to provide specific audit event, log and report information on a per-tenant and application basis is essential. It is apparent that in order to meet these customer expectations, cloud providers must provide standard mechanisms for their tenant customers to self-manage & self-audit application security that includes information about the provider's hardware, software and network infrastructure used to run specific tenant applications.

We propose that the best way to address these requirements is by developing open standards for cloud auditing. These standards would support the submission and retrieval of normative audit event data from cloud providers in the form of customized reports and logs that can be dynamically generated for cloud customers using their criteria. Adoption of such open standards by cloud providers' management platforms would go far to instill greater trust in "cloud hosted applications" and be a significant step forward in fulfilling the promise of an open cloud marketplace.

WG Scope & Charter

The Cloud Audit Data Federation WG will develop an audit event data model and a compatible interaction model that is able to describe interactions between IT resources suitable for cloud deployment models, including real and virtual resources contained within cloud providers' IT infrastructures and convey them in a federated manner.

The working groups will accept member use cases as input to profile development in order to make the data and interface models specified by the working group consumable by different customer scenarios and implementations.

In Scope

This section describes areas that are "in scope" for the CADF along with basic goals and/or requirements for each area.

- Data Model – that defines a normative, prescriptive audit event record and is composable into compatible log and record formats.
    - Extensible Event Taxonomies – normative, prescriptive taxonomies used to categorize event resources, actions and outcomes.
- Exemplary Interface Model – that defines service methods for management and federation of the audit data model.
    - Interfaces would include consideration for event Submission, Import and Export, Query and Subscription.
- Exemplary Component and Interaction Model - that demonstrates how the data and interfaces could be used by cloud providers and consumers to support general cloud auditing use cases.
- Profiles - that extends the core data and interface specifications developed to accommodate particular methods of consumption.

Out of Scope

IT systems such as those that comprise cloud deployments may report a wide variety of information in many different ways. This standard is focused on the proper federation or exchange of normative auditable events across cloud deployment models and between cloud and enterprises.

The following items are considered "Out of Scope"

- Translation of event notation from other domains
- Non-federated, low-level event generation
- Message and transport protocols
- Persistence and storage of audit events, reports, and logs will not be considered.
- Inclusion of Trace, Debug and Forensic Information

Business Justification

This effort will provide a standard means for customers that wish to utilize cloud deployment models for hosting distributed applications and services to federate audit event data in the form of records, logs and reports.

Specifications, profiles, and whitepapers produced by this working group will serve to protect the investments of companies seeking to move their applications to cloud deployment models while preserving the auditability of their business and operational processes regardless of chosen provider.

Expected WG Input

The following reference materials and documents will be of interest to the CADF for their activities:

1. Use Cases and Interactions for Cloud Auditing as provided by members
2. Data Model Requirements from The Open Group (TOG) XDAS v2 Update Project
3. Data Model Requirements from Cloud Management WG
4. Consideration and possible incorporation of and alignment with IETF Syslog protocol
5. Consideration and possible incorporation of and alignment with MITRE CEE format

WG Deliverables

1. Cloud Audit Event Data Model Specification
    a. Including Resource, Action and Outcome Taxonomies
    b. Including Guidance and Best Practices for Use of the Data Model.
2. Cloud Audit Event API Specification
    a. Including an exemplary Component Model
    b. Including Use Cases
3. Profiles of the Cloud Audit Event Data Model and Event API Specifications which the CADF deems necessary.
4. Protocol requirements delivered to the CMWG (or other groups if they exist)
5. Other documents and whitepapers which the Cloud Audit Working Group deems necessary.

WG Timeline

The CADF is expected to complete the above deliverables within 12-18 months from approval of the charter by the board.

Alliance Partnerships

1 Cloud Security Alliance (CSA)

2 The Open Group (TOG)

2.1 Consideration and possible incorporation of and alignment with XDAS v2 Update Drafts

Reliance/Coordination with other Subcommittees or Working Groups

1 Coordination with the DMTF Cloud Management WG (CMWG)

1.1 Specifically, any reference to protocols or protocol requirements must be coordinated with the CMWG.

2 Review with the DMTF Platform Management SC (PMSC), Infrastructure SC and Schema SC.

3 Coordination with the DMTF Security WG.