

July, 2013



Portland

Cloud Monitoring and Auditing with CADF (Cloud Auditing and Data Federation)

Jacques Durand (Fujitsu)
Matt Rutkowski (IBM)

Disclaimer

- ▶ The information in this presentation represents a snapshot of work in progress within the DMTF.
- ▶ This information is subject to change. The Standard Specifications remain the normative reference for all information.
- ▶ For additional information, see the Distributed Management Task Force (DMTF) Web site.



The DMTF was formed to lead the development, adoption and unification of management standards and initiatives for desktop, enterprise and internet environments

Agenda

- ▶ **Motivation**
- ▶ **Standard Overview**
- ▶ **Data Model – Events, Logs**
- ▶ **Taxonomies Overview**
- ▶ **Interfaces and Querying**
- ▶ **Challenges**

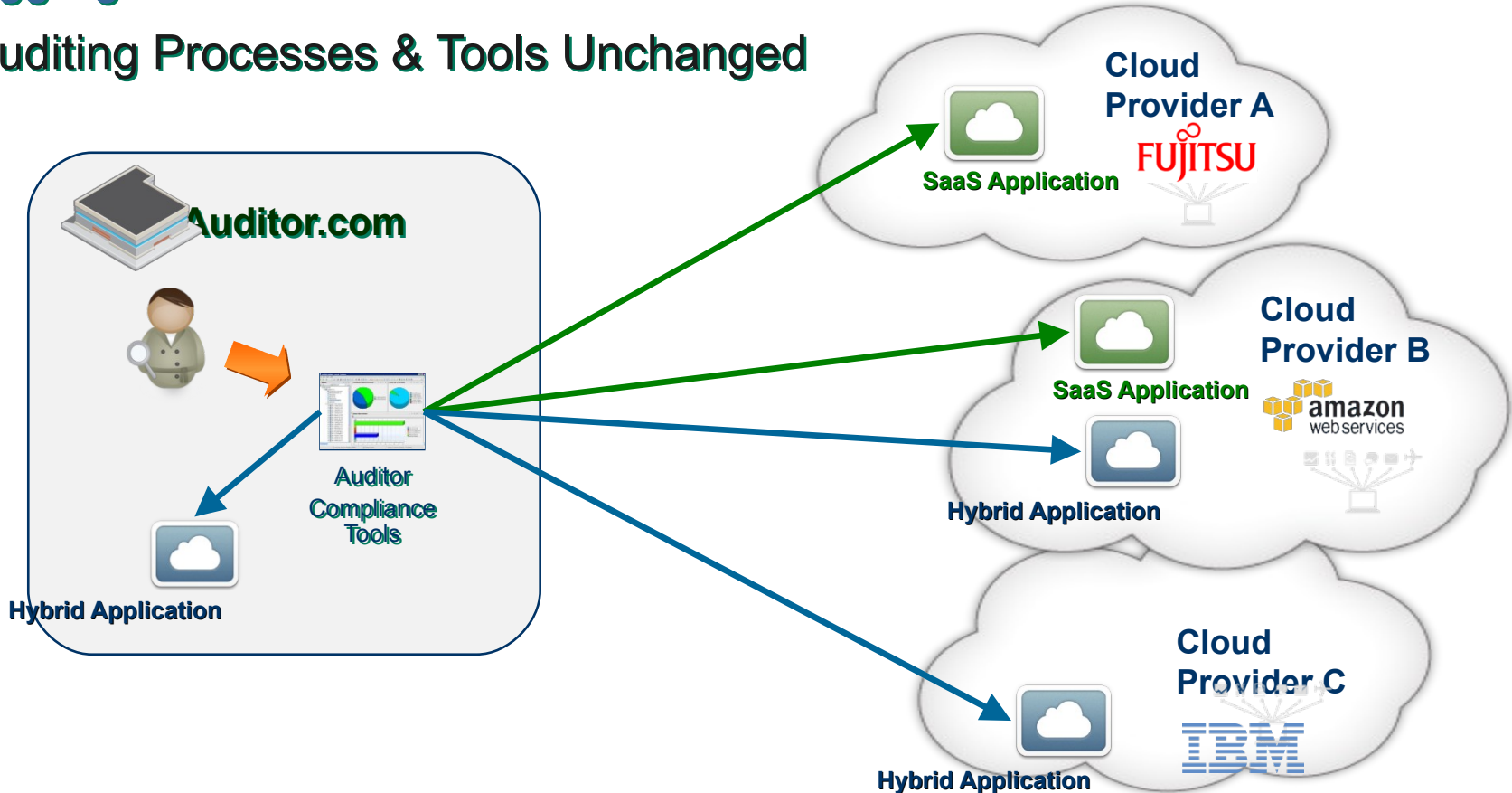
- ▶ **Need for more Visibility of Cloud Operations**
 - **Consumers: Control of Operating Expenses**
 - ✦ Understanding Cloud consumption patterns.
 - ✦ Per-Tenant Event Logs
 - **Virtualized resources, Multi-tenant**
 - ✦ Need to understand how workloads affect each other
 - ✦ Predictability of performances, or consumption

- ▶ **Contractual Nature of Cloud Operations**
 - **Cloud Providers have obligations to various Entities**
 - ✦ *Regulatory / Government*
 - ✦ *Company (Policies)*
 - ✦ *Customer SLA, SLO*
 - ✦ *Brokers*

Why an Audit Standard ?

General Scenario: Managing Auditing Data on (Hybrid) Clouds

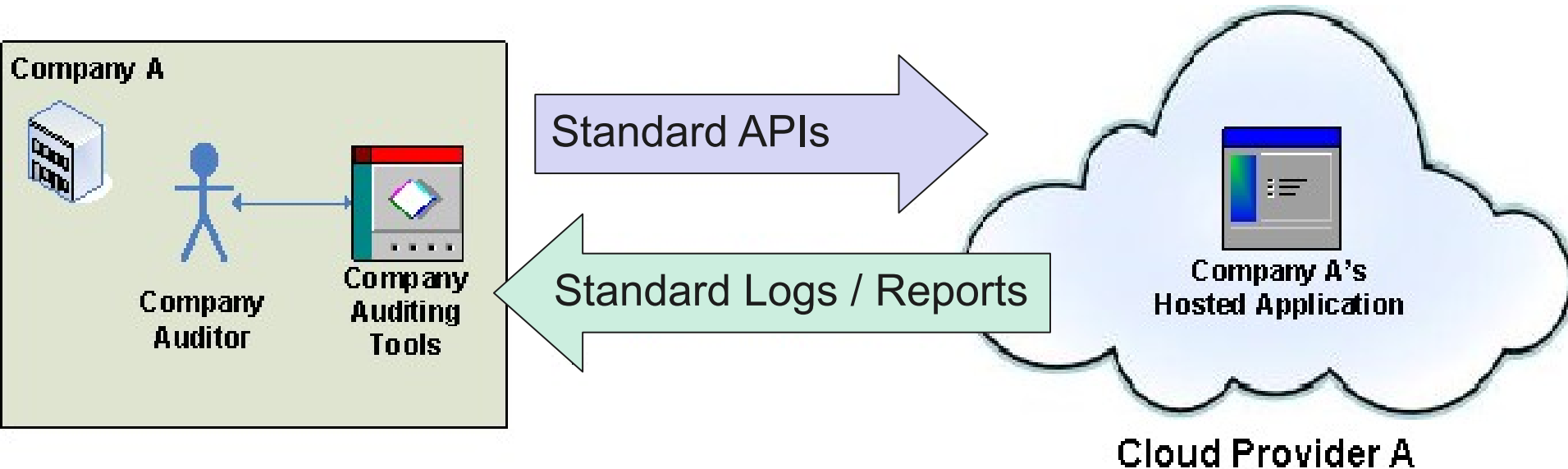
- Similar Reports from different Clouds
- Aggregate Audit Data from Different Clouds / Partners
- Auditing Processes & Tools Unchanged



Why an Audit Standard ?

Use Cases:

- Client-side **Auditing Tools** accessing **any** Cloud Provider
- Customers **Changing** Cloud Providers, want a consistent way to track compliance
- Aggregating Audits from **Hybrid Clouds**



Monitoring vs. Auditing (1)

Distinction between “Monitoring” material and “Audit” material is blurred

- ▶ **The Objectives are as diverse as**
 - Tracking and Enforcing all aspects of Security
 - Ensuring Service Levels
 - Enforcing Best Practices and Policies
- ▶ **All Operations may be subject to Audit**
 - Cloud Auditing involves real-time events beyond traditional security concerns and reflect on all kinds of operations,
 - ✦ resource lifecycle, data migrations, performance

Comprehensive Monitoring Model needed for Auditing

- ▶ Basic construct: **Events**
- ▶ Very Diverse Events are fair game for Auditing
 - Remote **user access** and requests
 - Virtual resources allocation and **lifecycle** management
 - Regular monitoring of **workloads**
 - **Usage** metering
 - System **alerts**
 - **Notifications** to users

Granular Audit Event

Some Use Case Categories

Category	Demonstrates Audit Requirements for
Binary and Metadata	Inclusion of binary and meta data within format
Compliance Control Based	Explore representation of common Control Based auditing frameworks (e.g. HIPAA, PCI, COBIT, etc)
Correlation	Correlating related events that span service, infrastructure and deployment boundaries (e.g. monetary transactions, network routes, etc.)
Data Tagging	Tagging events with domain and non-domain based classification values to achieve custom reports/views
Informational Events	Multiple language considerations, character encoding needs
Location Based	Representing physical location of event resources (e.g. geo or regional) and representation of location data.
Network	Representation of network events and their characteristics such as location and protocol representations
Operational	Treatment, demarcation and representation of audit report (event) data filtered by query parameters

Granular Audit Event

Some Use Case Categories, Continued

Category	Demonstrates Audit Requirements for
Obfuscation	Treatment, demarcation and representation of Personally Identifiable Information (PII)
Report Chaining	tracking and identifying the resources that create, modify or surface auditable events
Security	Exhibit the needs of security related events; e.g. normalized representation of identity, tokens, policy, etc
Service Level Agreement (SLA)	Representation of SLA monitoring events, their metrics and rule representations
Service License Management (SLM)	Representation of SLM monitoring events, their metrics and rule representations
Signature	The need to sign audit information at various granularities (e.g. event, report and log level)
Summarizing	representation of repeated events that are collapsed into a single event for reporting (for compactness)
Temporal	Attributing event actions with time-based information (e.g. granularity of measurement observed time, best time, modification time, etc.)

A Generic **Model** for Events and Logs

- A comprehensive Event , Log and Report model, that serves both operational and auditing objectives.

Interfaces

- Protocol & Service Methods to Manage and Federate Events, Logs and Reports

Taxonomies

- Normalize the Classification of Audit Events, (resources, operations, outcomes).

CADF Standard Overview

Events (1)

- ▶ **Distinction between:**
 - Actual (physical) Event
 - Event Record (a representation, ~ *CIM Indication*)
 - CADF Event Record (CADF-compliant Event Record)

- ▶ **Not a 1-1 relationship between**
 - Actual Evt $\leftarrow \rightarrow$ Event Record
 - Different aspects of same physical event
 - Aggregation / summarization of many actual evts

▶ Yet Another Event Standard?

■ Previous Efforts:

- ✦ CEE (MITRE),
- ✦ XDAS (X/Open Distributed Audit Service)
- ✦ ...

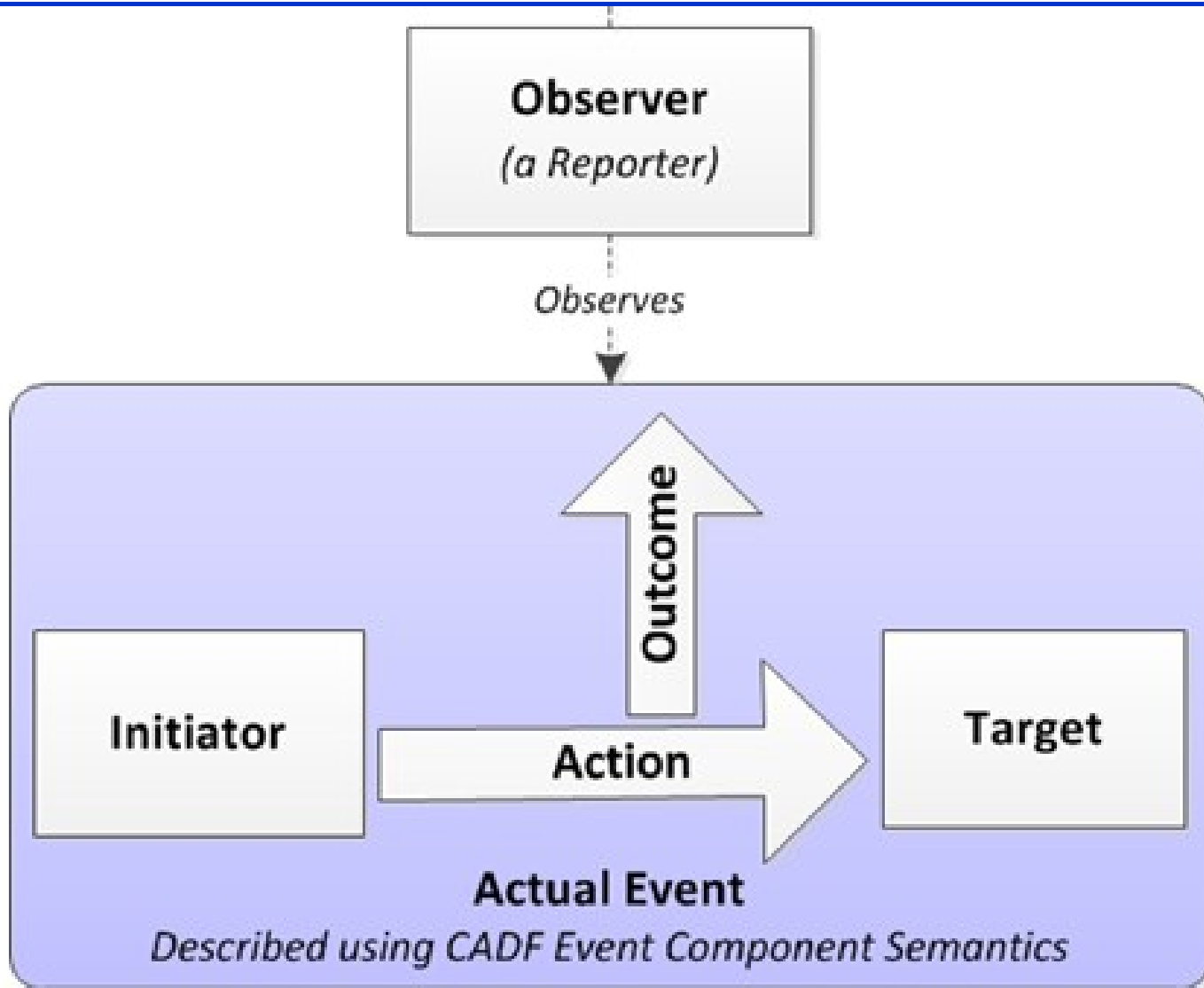
■ Under DMTF:

- ✦ CIM Indications,
- ✦ CIMI Events

▶ Inputs from existing event models and use cases analysis → versatile event model.

CADF Standard Overview

Events (3)



Three major event classes have been identified:

- (a) **activity** (tracking operations),
- (b) **monitoring** (resource status),
- (c) **control** (policy-based decisions).

CADF Standard Overview

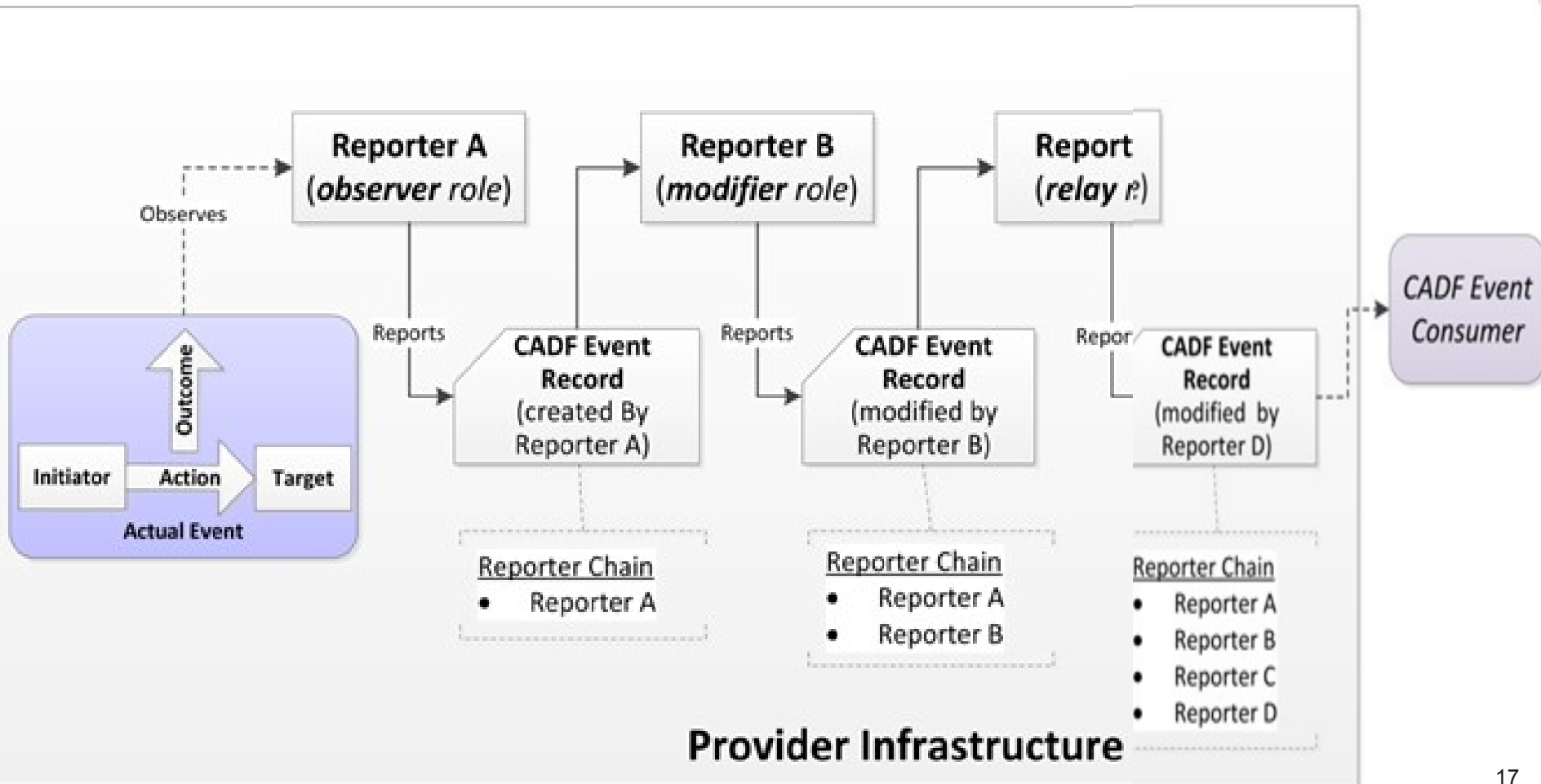
Events (5)

OBSERVER	EVENT TYPE	INITIATOR	ACTION	TARGET	OUTCOME	MEASUREMENT
identity management service	activity	user (connecting from some client)	login (for security compliance purposes)	server (a CADF Resource value)	Any valid CADF Outcome value (e.g., success, failure, etc.)	N/A (not required for activity type events)
monitoring server	monitor	monitoring server	monitor	cpu	(success, failure, pending.)	70% (Average CPU utilization)
server monitoring agent	activity	server monitoring agent	read	cpu	(success, failure, pending.)	Optional Value (e.g.,80%)
Policy enforcement point	control	Policy enforcement point	deny	User request (e.g., access to a server)	(success, failure, pending.)	REASON (rationale for control action)

CADF Standard Overview

Events (6)

The genesis of an event record may involve several entities or “reporters” starting from the initial “observer”.



- ▶ Three extensions mechanisms:
- ▶ (1) Attachments
 - allows attachments of any kind to both events and logs
- ▶ (2) Derivation (OO-style sub-typing)
 - E,g, attributes specific to some Resource types
- ▶ (3) Tags
 - For categorizing / labeling events

CADF Data Model Overview

Event Element Example

```

<event>
  id="myscheme://mydomain/event/id/1234"
  eventType="activity"
  eventTime="2012-03-22T13:00:00-04:00"
  action="create"
  outcome="dmtf:cadf:0262:0100:success">
  <initiator typeURI="resource/security/account/user ">
    </user id="provider-domain:user1234">
  </initiator>
</target typeURI="resource/service/database">
  <account type="subscriber" id="CIM:account-id"/>
    // Optionally embed provider specific account data here
  </account>
</target>
<reportchain>
  <reporterstep role="observer" id="provider-domain:observer-id"/>
  <reporterstep role="modifier" id="provider-domain:modifier-id"/>
</reportchain>
<tag>provider-domain:grouping:PCI?value=a123</tag>
<tag>//myobserver/correlationID?value=1234</tag>
</event>

```

Classify Event Using DMTF CADF Taxonomy Values
(Normative for Federation)

Domain Specific Identifiers
(e.g. Provider Domain and DMTF CIM)

Optionally Embed Format Specific Data Objects
(e.g. CIM_Account)

Report Chain
Track resources that contributed to event data

Optional "Tags" to Enable Profile Specific Views on Data
(e.g. "Show All PCI Related Events")

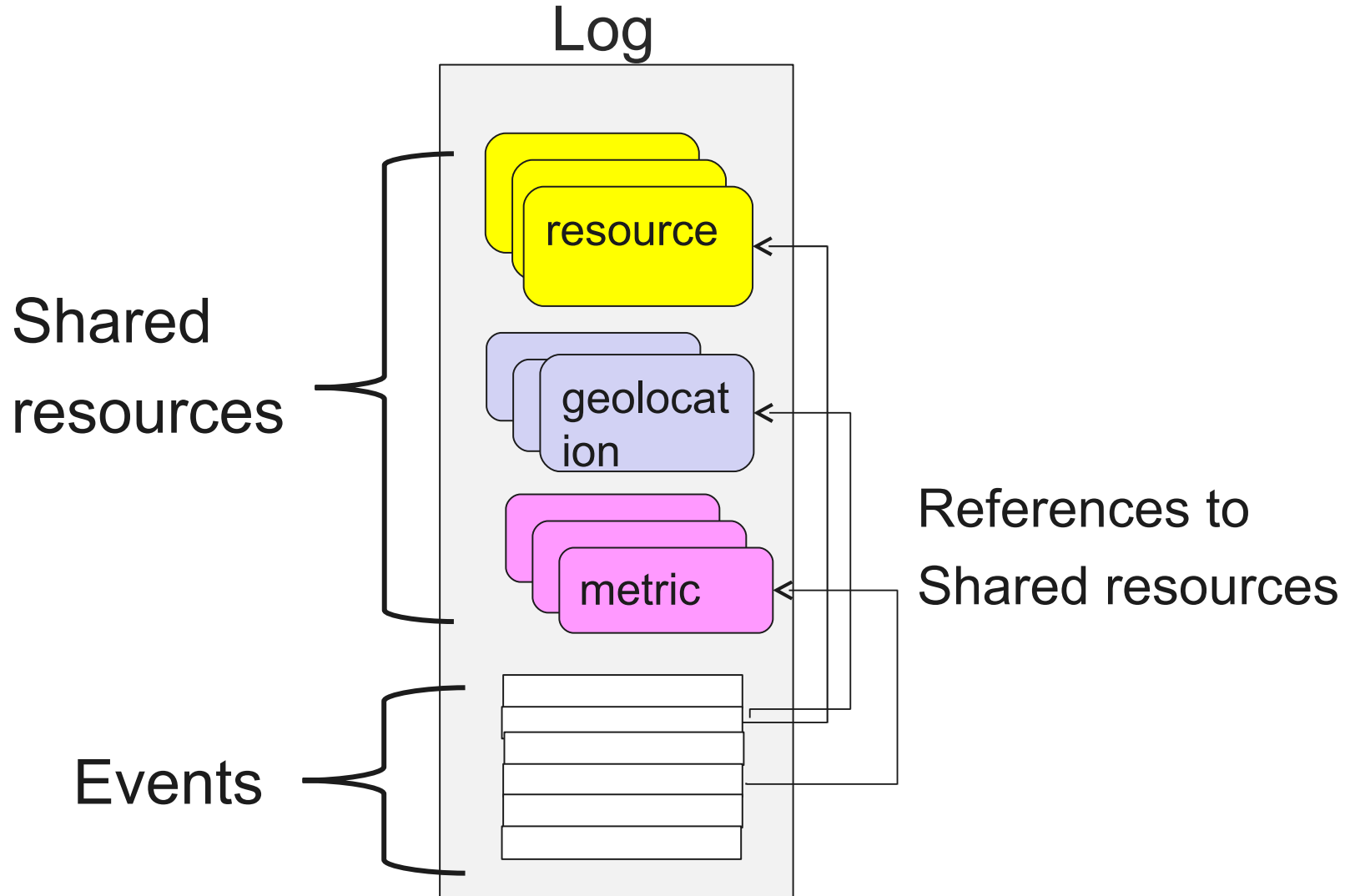
CADF Standard Overview

Logs (1)

- ▶ LOG: more than just a collection of Events: an Event Container
 - must support merging, transfer, event selection,
- ▶ Has additional, contextual Information typically shared by many Events:
 - Description/State of Cloud resources involved,
 - User data,
 - geolocations
 - metrics
- ▶ Extensibility: attachments

CADF Standard Overview

Logs (2)



A Generic Model for Events and Logs

- A comprehensive Event , Log and Report model, that serves both operational and auditing objectives.

Interfaces

- Protocol & Service Methods to Manage and Federate Events, Logs and Reports

Taxonomies

- Normalize the Classification of Audit Events, (resources, operations, outcomes).

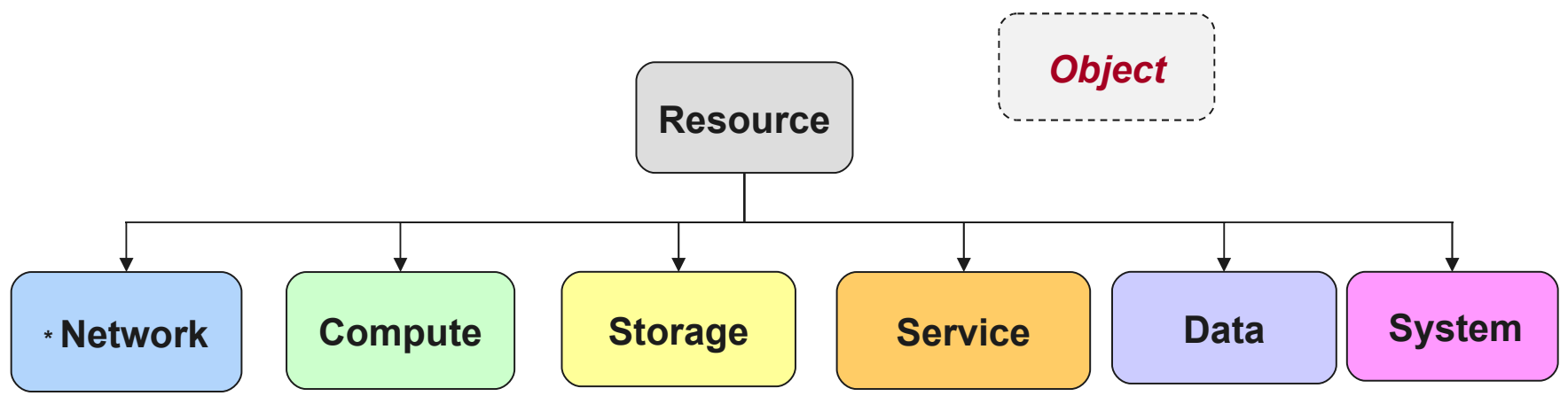
CADF Standard Overview

Taxonomies (1)

- ▶ Taxonomies allow for categorizing events in a consistent way.
- ▶ Taxonomies have been defined for
 - event actions,
 - resources
 - outcomes.
 -
- ▶ An additional tagging mechanism adds flexibility by allowing cross-categorization of events

Goal: Normalize the Classification of Audit Events Using CADF Defined Taxonomies

- ▶ *A Logical Meta-Model for Naming Cloud Resources involved*
- ▶ *Resources Compatible with other Formal Objective Inheritance models (like CIM)*



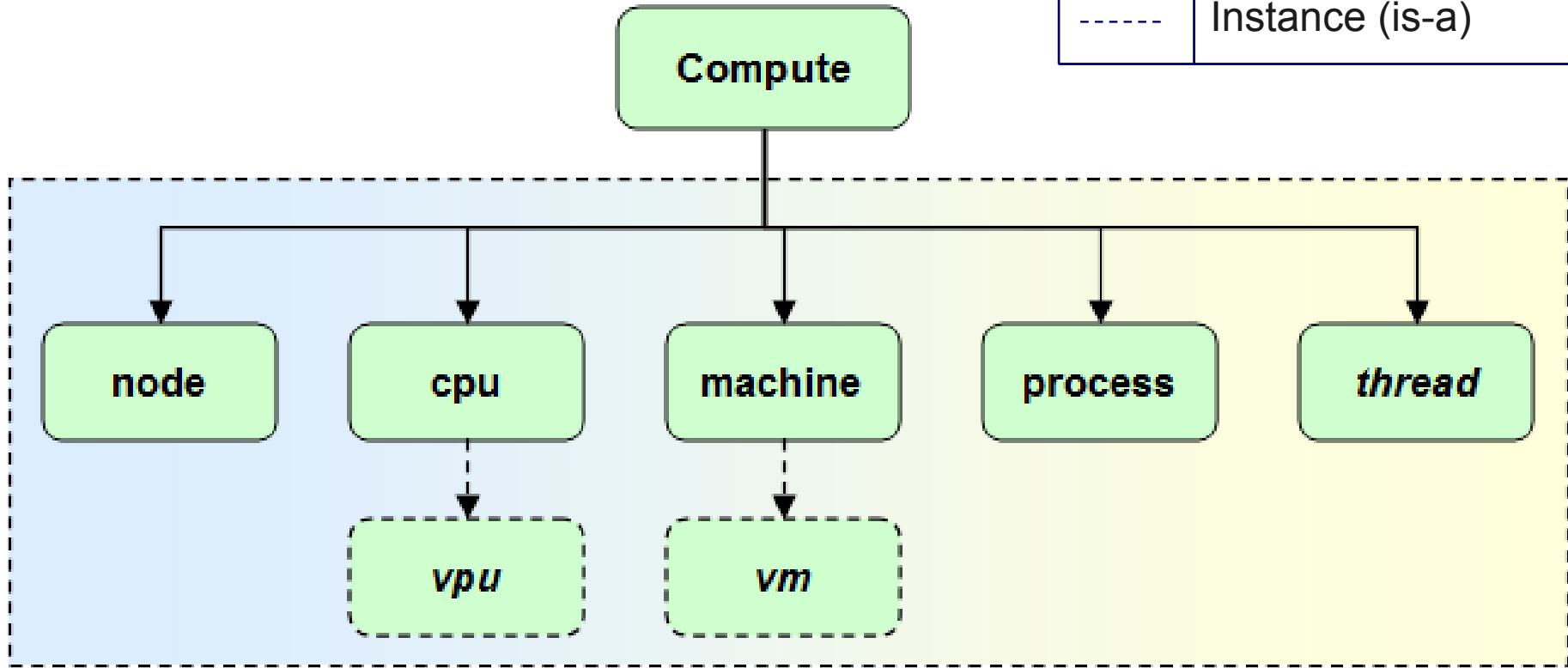
Semantic overlap is OK

Different **perspectives** on same Resource → Different taxonomy **Paths**.

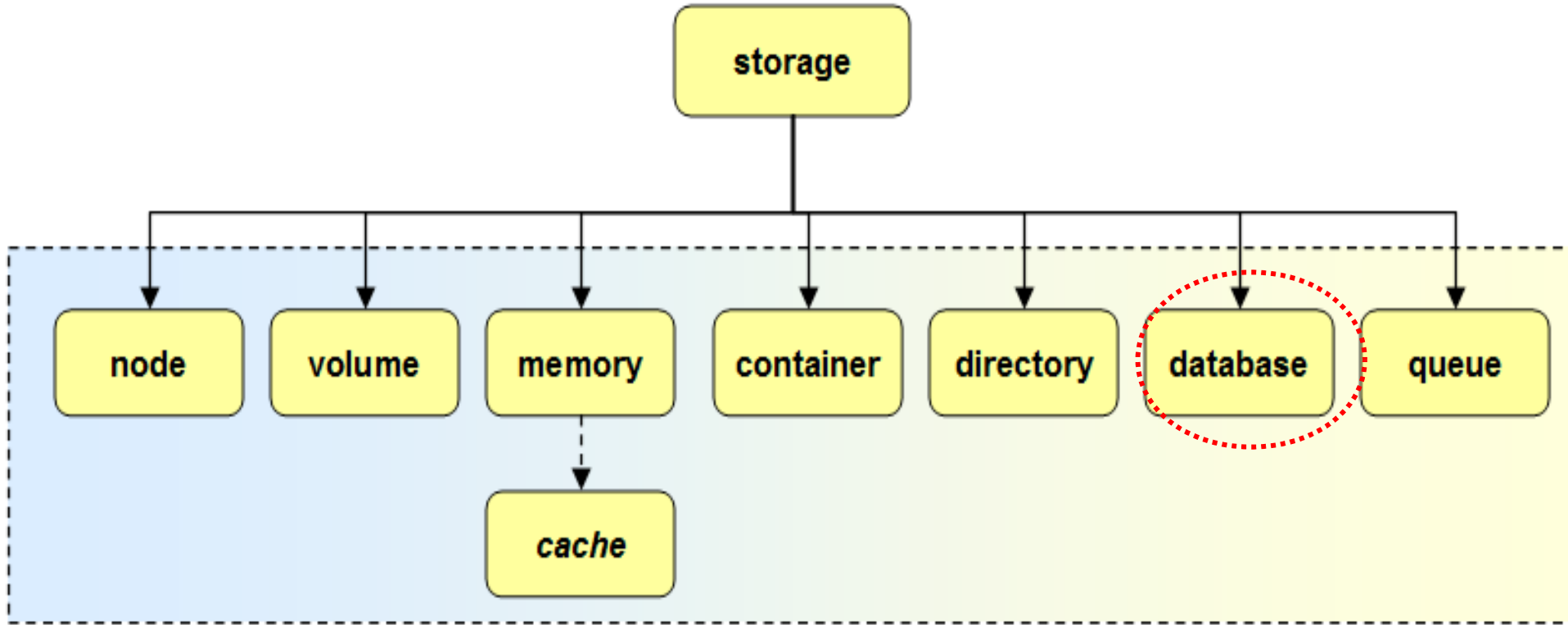
Taxonomies: Compute Subcategory Examples

- *Sample Expansion of the Compute Subtree*

——	Categorization
-----	Instance (is-a)



- *Sample Expansion of the Storage Subtree*

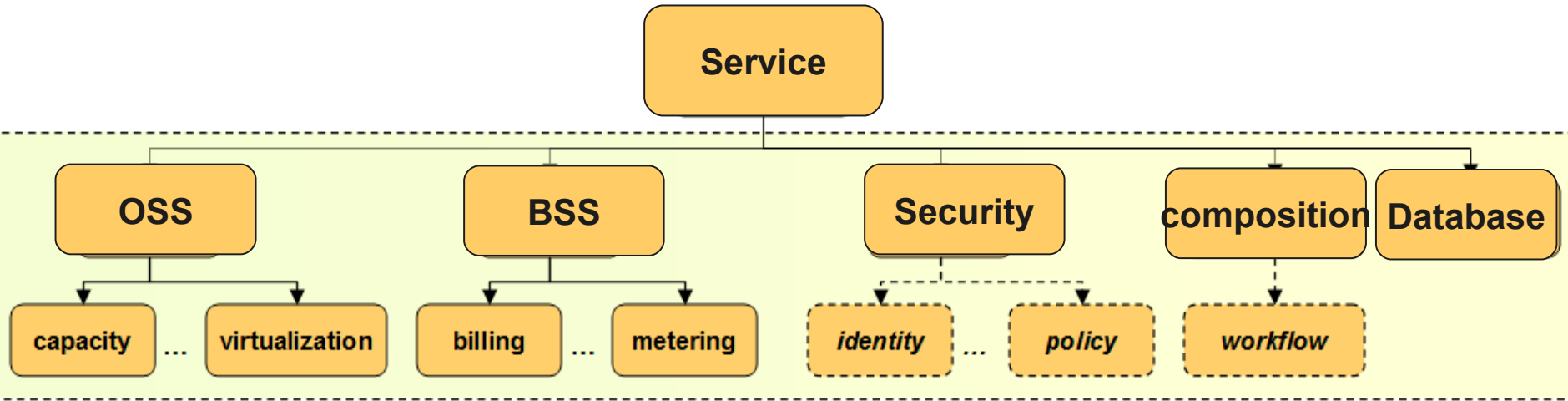


Taxonomy **Paths** vs unique names:

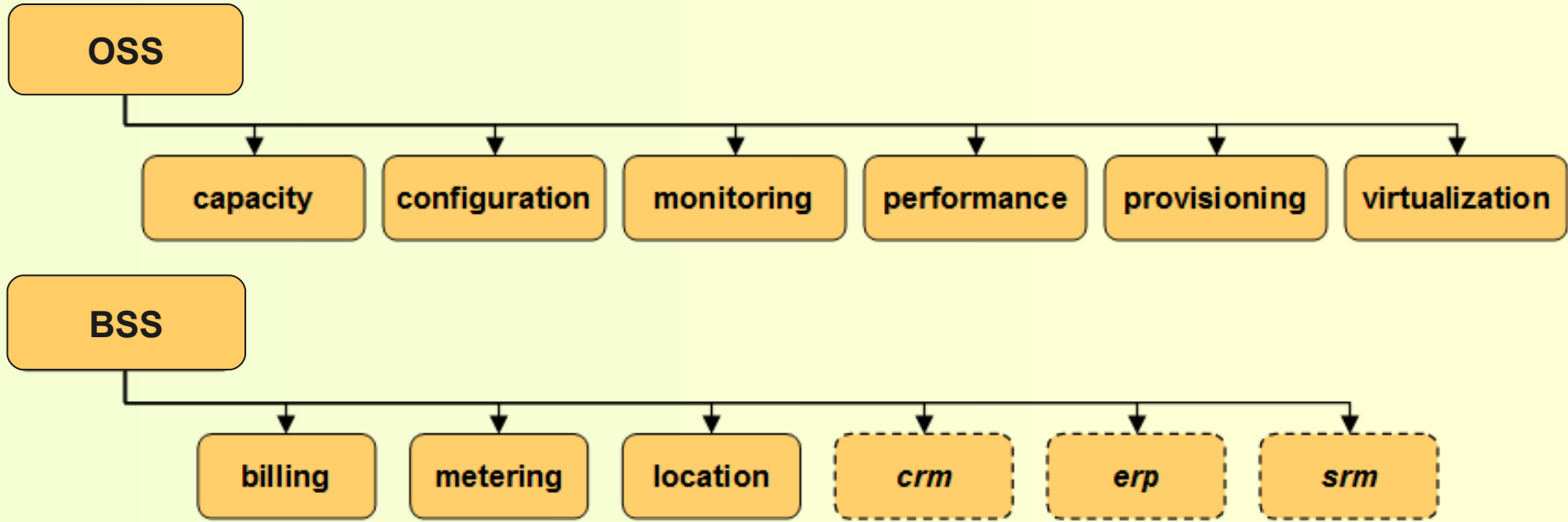
e.g. `resource/storage/database`

Taxonomies: Service Subcategory Examples

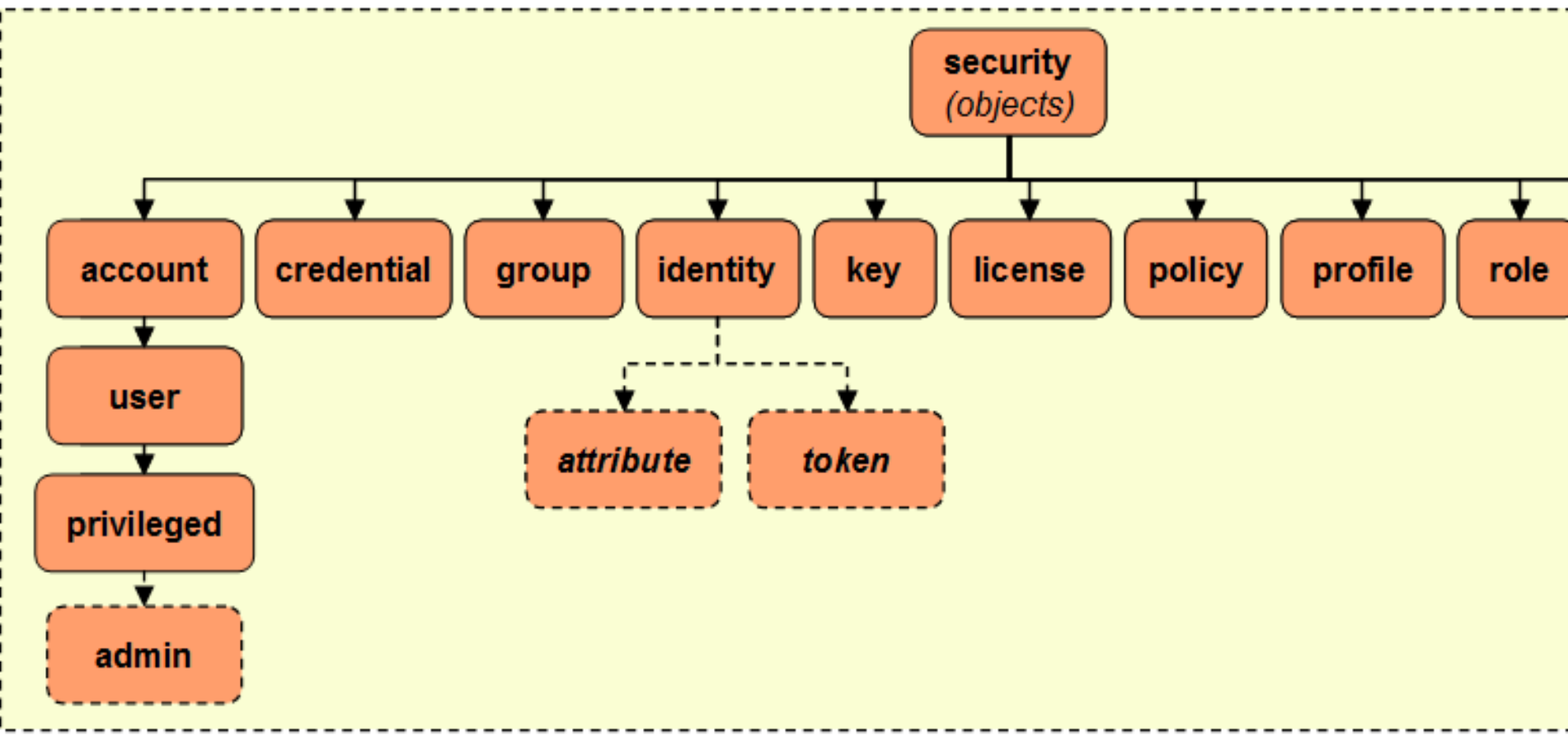
- Sample Expansion of the Service Subtree



- Sample Expansion of the Service Subtree

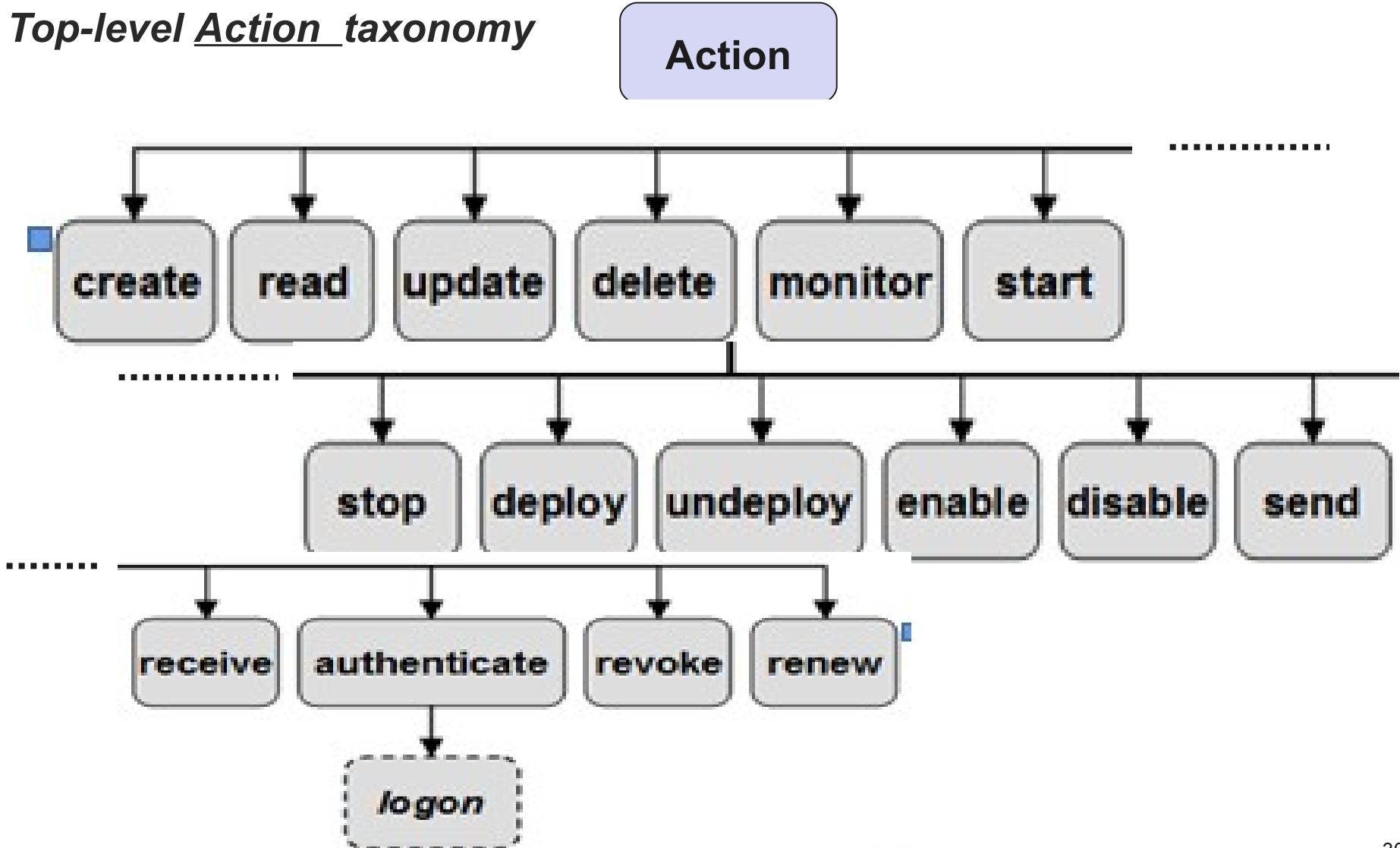


- *Sample Expansion of the Security Subtree*



Taxonomies: *Actions*

• *Top-level Action taxonomy*



A Generic Model for Events and Logs

- A comprehensive Event , Log and Report model, that serves both operational and auditing objectives.

Interfaces

- Protocol & Service Methods to Manage and Federate Events, Logs and Reports

Taxonomies

- Normalize the Classification of Audit Events, (resources, operations, outcomes).

- ▶ A REST interface for accessing event logs, reports
 - URIs for top-level resources (logs, reports)
 - XML or JSON serialization
 - Once complete, logs are not supposed to be modified (→ GET, not PUT or PATCH)
 - ✦ Processing logs (signing, consolidating) → new Log
- ▶ Events to be accessed via querying/selection in a log.
 - GET <log-URI> “?” <query>

Event Querying and Filtering (1)

- ▶ Query parameter **\$filter** appended to the URI of queried resource
- ▶ Query all Events in a Log, that report on a Resource creation

```
/events/Event?$filter=action="create"
```

- ▶ Query all Events in a Log, that have a target Resource located in Denver

```
/events/Event?  
$filter=target/geolocation/city="Denver"
```

Event Querying and Filtering (2)

- ▶ Query all Events in a Log, that report on a **failed** Resource creation

```
/events/Event?$filter=((action='create') and  
(outcome='failure'))
```

- ▶ Query all Events in a Log, that occurred on or after 2013-07-22


```
/events/Event?$filter=  
eventTime>="2013-07-22T00:00:00-02:00"
```

Event Querying and Filtering (3)

- ▶ **TAXONOMY queries**

- ▶ **Query all Events in a Log, with a target resource of type equal to “resource/service/oss/virtualization”.**

typeURI = taxonomy path



```
/events/Event?
```

```
$filter=target/typeURI="resource/service/oss/virtualization"
```

- ▶ **Query all Events in a Log, that have a target Resource of type equal or under “resource/service/oss**

```
/events/Event?
```

```
$filter=target/typeURI="resource/service/oss/*"
```

Event Querying and Filtering (4)

▶ TAXONOMY queries

- ▶ Query all Events in a Log, with a target resource of type ending with “security/profile”.

```
/events/Event?$filter=  
target/typeURI="resource//security/profile"
```

- ▶ Query all Events in a Log, that have at least one of their tags of value “//GRC20.gov/cloud/security/pci-dss”

```
/events/Event?$filter=  
tags[*]="//GRC20.gov/cloud/security/pci-dss"
```

Event Querying and Filtering (5)

- ▶ Other query parameters

- ▶ Limiting returned results

```
/events/Event?$limit=100
```

```
/events/Event?$offset=800
```

- ▶ Pagination

```
/events/Event?$first
```

```
/events/Event?$last
```

```
/events/Event?$previous
```

Particularly Useful “CADF” Data Types

▶ Identifier

- A kind of URI – for all kinds of CADF Resources
- "scheme ":" hier-part ["?" query] ["#" fragment]

▶ Path

- A kind of URI, used for taxonomies
- "cadf://schemas.dmtf.org/cloud/audit/1.0/**resource/storage/database**"

▶ Tag

- A kind of URI
- “//GRC20.gov/cloud/**auditplan**?value=audit101”

▶ Timestamp

- A profile of UTC time: “2012-02-25T09:00:00-05:00”
- based upon the xs:dateTime as per [XMLSchema2](#)

▶ Attachment

- A container type for any extended content

Challenges: Event Correlations (1)

- ▶ Request-Responses (sync, async)
- ▶ Causality (action+reaction)
- ▶ Split: a single Actual Event on Multiple Resources
 - → Multiple event records
- ▶ A single User request crossing several system layers
 - (gateway, authorization, resource manager...)
 - System components may not act as ‘reporters’ on the same event – Instead, generate their own event record.

Challenges: Event Correlations (2)

► Use of correlation tags

- E.g. deletion of all files in a subdirectory
- (A Single Actual Event on Multiple Resources → Multiple events)

```

<Event id="myscheme://mydomain/id/1234" action="delete" >
  ... <target id="myscheme://mydomain/resource/id/0001"
name="file01.txt" typeURI="data/file"></target>
  <tags>
    <tag>//myobserver/correlationID?value=1234</tag>
  </tags>
</Event>
<Event id="myscheme://mydomain/id/1235" action="delete" >
  ...<target id="myscheme://mydomain/resource/id/0002"
name="file02.txt" typeURI="data/file"></target>
  <tags>
    <tag>//myobserver/correlationID?value=1234</tag>
  </tags>
</Event>
  
```


- ▶ Use of explicit Event reference lists, in attachments
 - E.g. summarizing event, inability to tag

```

<Event id="myscheme://mydomain/id/1234">
  ...
  <attachments
    <attachment name="correlatedEvents">
      <content><events>
        <Eventref eventId="myscheme://mydomain/event/id/AAA" />
        <Eventref eventId="myscheme://mydomain/event/id/BBB" />
      </events>
    </content>
  </attachment>
</attachments>
</Event>
  
```

July, 2013



Portland

**Cloud Monitoring and Auditing
with CADF
(Cloud Auditing and Data Federation)**

Questions ?