Document Identifier: DSP2038

Date: 2014-09-16

Version: 1.0.0

Cloud Audit Data Federation - OpenStack Profile (CADF-OpenStack)

A CADF Representation for OpenStack

Document Type: White Paper

Document Status: DMTF Informational

Document Language: en-US

Contents

Figures

Tables

Foreword

This document is a deliverable from the DMTF Cloud Auditing Data Federation (CADF) Working Group. It defines a CADF representation for use with the OpenStack Cloud Management Platform. This document assumes that the reader is familiar with the concepts in the CADF Specification 1.0 (DSP0262).

Acknowledgments

The authors wish to acknowledge the following people.

Editors:

- Rick Cohen – IBM
- Gordon Chung - IBM
- Matt Rutkowski - IBM

Cloud Audit Data Federation - OpenStack Profile (CADF-OpenStack)

1 Scope

This document makes use of the common meta-model used by CADF, the Cloud Audit Data Federation to describe the events used by the OpenStack Cloud Management Platform. The document DSP0262 defines the CADF model.

2 References

The following referenced documents are indispensable for the application of this document. For dated or versioned references, only the edition cited (including any corrigenda or DMTF update versions) applies. For references without a date or version, the latest published edition of the referenced document (including any corrigenda or DMTF update versions) applies.

DMTF DSP0262, Cloud Audit Data Federation (CADF) - Data Format and Interface Definitions Specification version 1.0.0, http://dmtf.org/sites/default/files/standards/documents/DSP0262_1.0.0.pdf

OpenStack Core API Specifications: http://docs.openstack.org/api/api-specs.html

pyCADF developer documentation: http://docs.openstack.org/developer/pycadf/

pyCADF Python library – provides API to create CADF events: https://github.com/openstack/pycadf

3 Terms and definitions

3.1
CADF

CADF (Cloud Audit Data Federation) defined by DSP02626 as:

1. The name of the meta-model used to define cloud audit data
2. The name of the schema published by the DMTF

This specification describes the translation of OpenStack Audit data into the CADF data model

3.2
OpenStack

The OpenStack cloud management platform

3.3
JSON

A representation format used to describe CADF events in this profile.

4 CADF background

4.1 Overview

The Cloud Audit Data Federation (CADF) specification defines a normative event data model along with a compatible set of interfaces for federating events, logs and reports between cloud providers and customers.

CADF provides several benefits to customers of cloud services. Audit event data can be represented in a common format to allow for consistent reporting of this data across different cloud providers. Cloud customers will also be able to aggregate data from different cloud providers to provide a more complete and consistent picture of all audit data. Also with audit data coming in from different providers in the same format, customers will be able to use common audit tools and processes for all their audit data.

The ability to federate date from different sources will also provide benefits to users of OpenStack with an audit data format that will be consistent across a collection of disparate cloud (IaaS) services with some common components such as Keystone and Oslo libraries. These components will need to share audit data.

4.2 Event model

The CADF specification applies semantics to activities on resources within a cloud environment using a common data model using the concept of an event. CADF provides for multiple event types, and the model is common to all of them (i.e., activity, monitor and control events).

The event model uses the concept of a resource which is used within multiple defined event components. A resource is an entity that can provide or consume services or information within the context of a cloud infrastructure. Examples of resources include traditional IT infrastructure components like servers and network devices, software components such as databases and applications, operation and business entities used for security such as accounts, users and roles.

The event model defines both required and optional components. The required components guarantee that all events have essential data and optional components are event type dependent and add additional context to the event information.

CADF allows the event model to be extended to include new event types that can be used for other domains. Profiles of the base specification can be published to describe proper usage of the event model and extension in the other domains.

Included in the event model are taxonomies for specific field values. The taxonomies ensure that event field values are consistent when the events come from different sources (e.g., different cloud providers). The taxonomies include:

- **Resource Taxonomy** - used to classify the event by the logical IT or cloud resources that are related to the event's action. For example, values of this taxonomy could be used to classify the resource that observed the action or the resource that was the (intended) target of the action.
- **Action Taxonomy** - used to classify the event by the activity that caused it to be generated.
- **Outcome Taxonomy** - used to describe the outcome of the attempted action of the event.

Additional features are included in the CADF Event model to enable federation from hybrid cloud deployments. Resources are uniquely tracked using UUIDS and are not dependent on relative IP addresses. Event timestamps are timezone aware and the specification describes how to create events with different timezones. Events can have a geolocation component that can track geolocation of resources using international standards. This is important to enable tracking enforcement of regional policies for data and application hosting. Events can be classified using "tagging". This allows the creation of different views of the same set of data to be used for multiple domains of interest. For example some

events from the same set of events may be tagged for use in PCI compliance and other events may be tagged for SOX compliance, and an overlapping set of events can be tagged for use in corporate policy compliance. Using tags allows reports to be generated over these different views.

4.3 Required model components

Table 1 describes the event model components and the semantics for each component

Table 1 – Required CADF event model components

Model Component	CADF Definition
OBSERVER	The RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event.
INITIATOR	The RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER.
ACTION	The operation or activity the INITIATOR has performed, attempted to perform or has pending against the event's TARGET, according to the OBSERVER.
TARGET	The RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER. *Note: a TARGET (in the CADF Event Model) can represent a plurality of target resources.*
OUTCOME	The result or status of the ACTION against the TARGET, according to the OBSERVER.

The OBSERVER is a RESOURCE that observes the actual event and creates a CADF event record based on the information known and its purpose. The OBSERVER does its best to identify and classify all other required model components (e.g., INITIATOR, TARGET, ACTION, etc.) along with any relevant data.

The conceptual diagram in Figure 1 shows basic components of the CADF Event Model and their interactions:

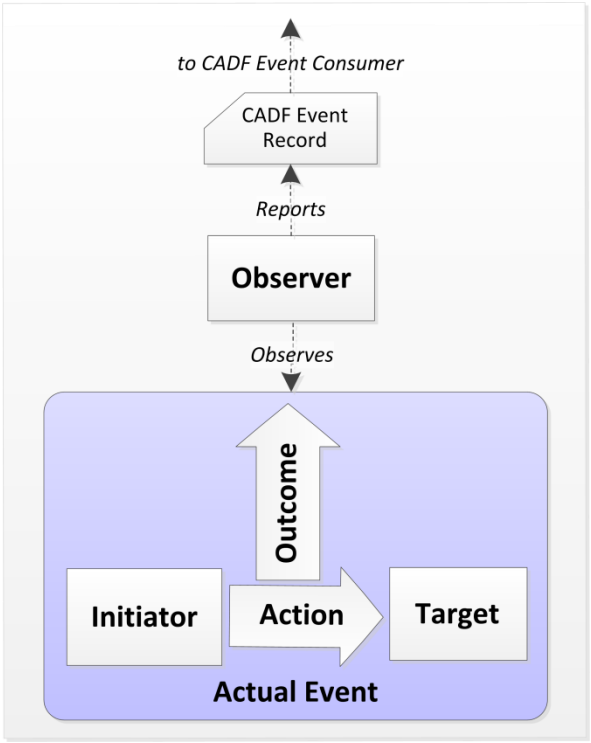


Figure 1 – CADF event model: Basic components

4.4 Using CADF for audit

The CADF data model is designed to provide information auditors are looking for to track activities in cloud environments. The data in an event can record the WHO, WHAT, WHEN, WHERE, FROM WHERE and WHERE TO of an activity. This is also referred to as the 7 “W”s of audit and compliance.

181

182 **Table 2 – CADF – the 7 "W"s of audit**

"W" Component	CADF Mandatory Properties	CADF Optional Properties (where applicable)	Description
What	event.action event.outcome event.type	event.reason *(e.g., severity, reason code, policy id)*	"what" activity occurred; "what" was the result
When	event.eventTime	reporter.timestamp (detailed), *for each reporter* event.duration	"when" did it happen • Any granularity via ISO 8601 format
Who	initiator.id initiator.type	initiator.id (id, name): (basic) initiator.credential (token): (detailed) initiator.credential.assertions (precise)	"who" (person or service) initiated the action
FromWhere		initiator.addresses (basic) initiator.host (agents, platforms, …) (detailed) Initiator.geolocation (precise)	FromWhere provides information describ ing where the action was initiated from. May include • logical/physical addresses • ISO-6709-2008, precise geolocations
OnWhat	target.id target.type		"onWhat" resource did the activity target
Where	observer.id observer.type	reporterstep.role (detailed) reporterstep.reporterTime (detailed)	"where" did the activity get observed (reported), or modified in some way.
ToWhere		target.addresses (basic) target.host (agents, platforms, …) (detailed) target.geolocation (precise)	ToWhere provides information describing where the target resource that is affected by the action is located. For example, this can be as simple as an IP address or server name.

183 # 5 CADF with OpenStack

184 ## 5.1 OpenStack overview

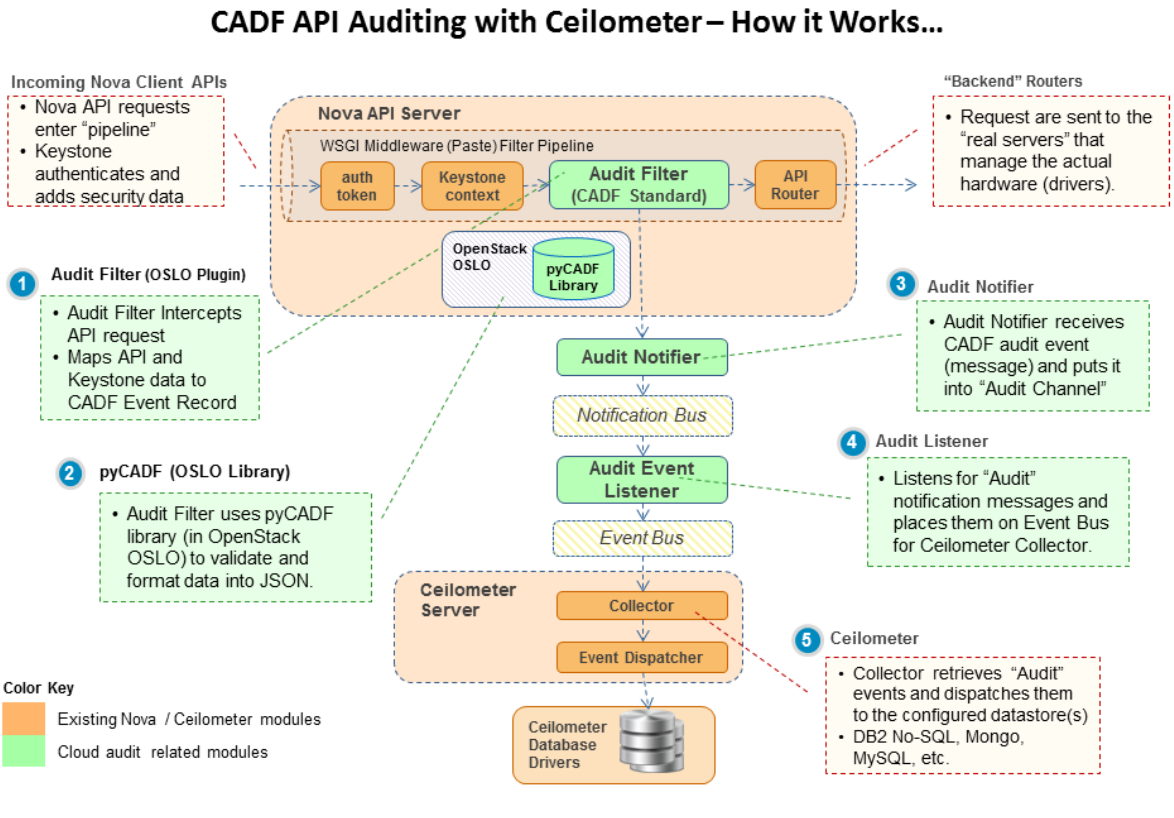
185 OpenStack is an open source project that seeks to provide a cloud computing platform that can be used
186 with public and private clouds. The technology consists of a series of interrelated projects delivering
187 various components for a cloud infrastructure solution.

5.2 Use of CADF

Representing OpenStack audit data using the CADF data model enables OpenStack customers to take advantage of all the benefits described above. Customers using multiple OpenStack environments can provide a consistent view of their audit data using CADF. Cloud environments using the OpenStack framework will also be able to federate audit data with other cloud environments that support CADF.

All CADF events in OpenStack are expressed in JSON serialization format. An example of how CADF events are conveyed in OpenStack can be seen in clause 6.4 below.

5.2.1 CADF API Auditing with Ceilometer



1

6 Examples

By walking through a detailed example, step by step, this clause will show how to use CADF to audit OpenStack operations. The example will start with an OpenStack REST API, and then show what a CADF audit event will look like that records the execution of that REST API.

6.1 Nova examples

A list of APIs that are audited by the middleware filter can be found in the appendices. They all feature the same mapping scheme described in the following examples.

6.1.1 GET server details

The HTTP request represents an OpenStack API call to the Compute Service (nova) to lists IDs, names, and links for all servers (*v2/?{tenant_id}?/servers*).

```
Method:   GET
Address:  9.26.27.109:8774
URI:      v2/e55b158759854ea6a7852aa76632c6c1/servers
```

CADF events are produced when OpenStack component API calls are made. The OpenStack CADF mapping uses the segments parsed out of the ReSTful API calls to map into the different CADF properties.

First, the HTTP Request is parsed into the following segments:

Value	Description
9.26.27.109:8774	Indicates the target service of api request
v2	Version
e55b158759854ea6a7852aa76632c6c1	Tenant id
Servers	Indicates the action will be against a Compute instance

Using this information, the segment values are mapped into CADF fields:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:a80dc5ee-be83-48ad-ad5e-6577f2217637‘	CADF generated event id
eventType	activity	Characterizes events that provide information about actions having occurred or intended to occur, and initiated by some resource or done against some resource, Such events typically report on regular operations of a Cloud infrastructure or services.
action	read/list	CADF action mapping for GET call on a OpenStack compute (nova) REST API
outcome	success	Generated by CADF filter for incoming requests, indicates that the OpenStack compute (nova) REST API call succeeded

CADF Field	Value	Description
reason	'reasonCode': '200', 'reasonType': 'HTTP'	Standard response for successful HTTP requests.
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
initiator		CADF component that contains the RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER.
initiator:id	openstack:95f12d248a234a969f456cd2c794f29a	OpenStack initiator id
initiator:typeURI	service/security/account/user	Indicates that the initiator is a user (from the CADF resource taxonomy)
initiator:name	*<user_name>*	User name of the authenticated user on the OpenStack Nova API call based on given name in Keystone
initiator:project_id	openstack:e55b158759854ea6a7852aa76632c6c1	The tenant id of the initiator
initiator:credential	token: MIIQBgYJKoZIhvcNAQcCoIIP9z …… identity_status: Confirmed	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	agent:python-novaclient address:9.26.27.109	Initiator host information where the OpenStack compute service request came from
target		CADF component that contains the RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER.
target.id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id
target.typeURI	service/compute/servers	Indicates that the target is a compute service specifically targeting servers(from the CADF resource taxonomy)
target.name	nova	Name of event target.

CADF Field	Value	Description
target.addresses	url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: admin url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: private url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: public	Addresses of event target
requestPath	v2/e55b158759854ea6a7852aa76632c6c1/servers	Request path on the OpenStack compute service REST API call
Observer		CADF component that contains the RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event
observer:id	target	Indicates that the CADF target observed this event
Reporterchain	reporterTime': '2014-01-17T23:23:38.154152+0000 role': '**modifier**', reporter': {'id': '**target**'}}],	The reporterchain is used to record additional reporters that modify the event. In this example, the event is initially created on request and the outcome and reason are modified the observer on response
Tags	**correlation_id**?value=openstack:bcac04dc-e0be-4110-862c-347088a7836a	Correlation id that can be used to correlate this event with other events “down the execution chain” to allow creation of a complete event chain for this action. Tags can be used for multiple purposes to classify events for different contexts.

6.1.2 Deallocate floating IP address

The HTTP request represents an OpenStack API call to the Compute Service (nova) to deallocate a floating IP address from the IP list (v2/?{tenant_id}?/os-floating-ips/?{id}?).

```
Method:   GET
Address:  9.26.27.109:8774
URI:      v2/e55b158759854ea6a7852aa76632c6c1/os-floating-
ips/e55b167823124ea6a7852aa76123d9m2
```

Similarly, the HTTP Request is parsed into the following segments

Value	Description
9.26.27.109:8774	Indicates the target service of api request
v2	Version
e55b158759854ea6a7852aa76632c6c1	Tenant id
os-floating-ips	Indicates the action will be against floating IPs associated to an account
e55b167823124ea6a7852aa76123d9m2	Floating IP id

Using this information, the segment values are mapped into CADF fields:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:a80dc5ee-be83-48ad-ad5e-1324aew923kj‘	CADF generated event id
eventType	activity	Characterizes events that provide information about actions having occurred or intended to occur, and initiated by some resource or done against some resource, Such events typically report on regular operations of a Cloud infrastructure or services.
action	delete	CADF action mapping for DELETE call on a OpenStack compute (nova) REST API
outcome	success	Generated by CADF filter for incoming requests, indicates that the OpenStack compute (nova) REST API call succeeded

CADF Field	Value	Description
reason	'reasonCode': '200', 'reasonType': 'HTTP'	Standard response for successful HTTP requests.
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
initiator		CADF component that contains the RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER.
initiator:id	openstack:95f12d248a234a969f456cd2c794f29a	OpenStack initiator id
initiator:typeURI	service/security/account/user	Indicates that the initiator is a user (from the CADF resource taxonomy)
initiator:name	*<user_name>*	User name of the authenticated user on the OpenStack Nova API call based on given name in Keystone
initiator:project_id	openstack:e55b158759854ea6a7852aa76632c6c1	The tenant id of the initiator
initiator:credential	token: MIIQBgYJKoZIhvcNAQcCoIIP9z …… identity_status: Confirmed	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	agent:python-novaclient address:9.26.27.109	Initiator host information where the OpenStack compute service request came from
target		CADF component that contains the RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER.
target.id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id
target.typeURI	service/compute/os-floating-ips/floating-ip	Indicates that the target is a compute service specifically targeting a specific floating-ip(from the CADF resource taxonomy)
target.name	nova	Name of event target.

CADF Field	Value	Description
target.addresses	url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: admin url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: private url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: public	Addresses of event target
requestPath	v2/e55b158759854ea6a7852aa76632c6c1/os-floating-ips/e55b167823124ea6a7852aa76123d9m2	Request path on the OpenStack compute service REST API call
Observer		CADF component that contains the RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event
observer:id	target	Indicates that the CADF target observed this event
Reporterchain	reporterTime': '2014-01-17T23:23:38.154152+0000 role': '**modifier**', reporter': {'id': **'target**'}}],	The reporterchain is used to record additional reporters that modify the event. In this example, the event is initially created on request and the outcome and reason are modified the observer on response
Tags	**correlation_id**?value=openstack:bcac04dc-e0be-4110-862c-347088a7836a	Correlation id that can be used to correlate this event with other events “down the execution chain” to allow creation of a complete event chain for this action. Tags can be used for multiple purposes to classify events for different contexts.

6.1.3 Embedded action - Resize instance

The HTTP request represents an OpenStack API call to the Compute Service (nova) to execute an action against a specific instance (v2/?{tenant_id}?/servers/?{server_id}?/action). The actual action is defined in the body of the request. In this case, the action is to resize the instance.

```
Method:   GET
Address:  9.26.27.109:8774
URI:
   v2/e55b158759854ea6a7852aa76632c6c1/servers/e55b167823124ea6a7852aa76123d9m2/action
REQ BODY: {"resize" : {"flavorRef" : "2"}}
```

Using this information, the segment values are mapped into CADF fields:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:a80dc5ee-be83-48ad-ad5e-1324aew923kj‘	CADF generated event id
eventType	activity	Characterizes events that provide information about actions having occurred or intended to occur, and initiated by some resource or done against some resource, Such events typically report on regular operations of a Cloud infrastructure or services.
action	update/resize	CADF action maps Nova actions to an update action, specifically a resize action.
outcome	success	Generated by CADF filter for incoming requests, indicates that the OpenStack compute (nova) REST API call succeeded
reason	'reasonCode': '200', 'reasonType': 'HTTP'	Standard response for successful HTTP requests.
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
initiator		CADF component that contains the RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER.
initiator:id	openstack:95f12d248a234a969f456cd2c794f29a	OpenStack initiator id
initiator:typeURI	service/security/account/user	Indicates that the initiator is a user (from the CADF resource taxonomy)
initiator:name	*<user_name>*	User name of the authenticated user on the OpenStack Nova API call based on given name in Keystone

CADF Field	Value	Description
initiator:project_id	openstack:e55b158759854ea6a7852aa76632c6c1	The tenant id of the initiator
initiator:credential	token: MIIQBgYJKoZIhvcNAQcCoIIP9z …… identity_status: Confirmed	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	agent:python-novaclient address:9.26.27.109	Initiator host information where the OpenStack compute service request came from
target		CADF component that contains the RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER.
target.id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id
target.typeURI	service/compute/servers/action	Indicates that the target is a compute service specifically targeting a specific instance to apply an action against(from the CADF resource taxonomy)
target.name	nova	Name of event target.
target.addresses	url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: admin url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: private url:http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1 name: public	Addresses of event target
requestPath	v2/e55b158759854ea6a7852aa76632c6c1/os-floating-ips/e55b167823124ea6a7852aa76123d9m2	Request path on the OpenStack compute service REST API call

CADF Field	Value	Description
Observer		CADF component that contains the RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event
observer:id	target	Indicates that the CADF target observed this event
Reporterchain	reporterTime': '2014-01-17T23:23:38.154152+0000 role': '**modifier**', reporter': {'id': '**target**'}}],	The reporterchain is used to record additional reporters that modify the event. In this example, the event is initially created on request and the outcome and reason are modified the observer on response
Tags	**correlation_id**?value=openstack:bcac04dc-e0be-4110-862c-347088a7836a	Correlation id that can be used to correlate this event with other events “down the execution chain” to allow creation of a complete event chain for this action. Tags can be used for multiple purposes to classify events for different contexts.

6.2 Glance examples

Audit events for the Glance service use the same middleware process described for Nova. As such, many of the values for Glance audit events are similarly prescribed as Nova audit events.

6.2.1 Download binary image data

The HTTP request represents an OpenStack API call to the Image Service (glance) to download data for a specific image file (*v2/ images/?{image_id}?/file*).

```
Method:   GET
Address:  9.26.27.109:8777
URI:      v2/images/e55b158759854ea6a7852aa76632c6c1/file
```

The HTTP Request is parsed into the following segments

Value	Description
9.26.27.109:8777	Indicates the glance service
v2	Version
images	Indicates the target is an image

Value	Description
e55b158759854ea6a7852aa76632c6c1	Image id
file	Indicates the action will be against the image file

245 Using this information, the segment values are mapped into CADF fields:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:a80dc5ee-be83-48ad-ad5e-6577f2217637‘	CADF generated event id
eventType	activity	Characterizes events that provide information about actions having occurred or intended to occur, and initiated by some resource or done against some resource Such events typically report on regular operations of a Cloud infrastructure or services.
action	read	CADF action mapping for GET request targeting Glance API
outcome	success	Generated by CADF filter for incoming requests, indicates that the OpenStack image (glance) REST API call succeeded
reason	'reasonCode': '200', 'reasonType': 'HTTP'	Standard response for successful HTTP requests
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
initiator		CADF component that contains the RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER
initiator:id	openstack:95f12d248a234a969f456cd2c794f29a	OpenStack initiator id
initiator:typeURI	service/security/account/user	Indicates that the initiator is a user (from the CADF resource taxonomy)

CADF Field	Value	Description
initiator:name	*<user_name>*	User name of the authenticated user on the OpenStack Glance API call based on given name in Keystone
initiator:project_id	openstack:e55b158759854ea6a7852aa76632c6c1	The tenant id of the initiator
initiator:credential	token: MIIQBgYJKoZIhvcNAQcCoIIP9z …… identity_status: Confirmed	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	agent:python-glanceclient address:9.26.27.109	Initiator host information where the OpenStack image service request came from
target		CADF component that contains the RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER
target.id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id
target.typeURI	service/storage/image/images/image/file	Indicates that the target is an image service specifically targeting an image file(from the CADF resource taxonomy)
target.name	nova	Name of event target
target.addresses	url:http://9.26.27.109:8777/v2 name: admin url:http://9.26.27.109:8777/v2 name: private url:http://9.26.27.109:8777/v2/ name: public	Addresses of event target
requestPath	v2/images/e55b158759854ea6a7852aa76632c6c1/file	Request path on the OpenStack image service REST API call
Observer		CADF component that contains the RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event

CADF Field	Value	Description
observer:id	target	Indicates that the CADF target observed this event
Reporterchain	reporterTime': '2014-01-17T23:23:38.154152+0000 role': '**modifier**', reporter': {'id': **'target**'}}],	The reporterchain is used to record additional reporters that modify the event. In this example, the event is initially created on request and the outcome and reason are modified the observer on response
Tags	**correlation_id**?value=openstack:bcac04dc-e0be-4110-862c-347088a7836a	Correlation id that can be used to correlate this event with other events “down the execution chain” to allow creation of a complete event chain for this action. Tags can be used for multiple purposes to classify events for different contexts.

6.3 Keystone example

6.3.1 Authenticating a user

The CADF audit event for user authentication is generated within the Keystone service. As the event is observed from a location other than the middleware, some of the CADF event details are different. The Keystone observer generates the values as follows:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:a80dc5ee-be83-48ad-ad5e-1324aew923kj‘	CADF generated event id
eventType	activity	Characterizes events that provide information about actions having occurred or intended to occur, and initiated by some resource or done against some resource Such events typically report on regular operations of a Cloud infrastructure or services.
action	authenticate	CADF action mapped to user authentication
outcome	success	Generated by Keystone service to indicate successful authentication of credentials

CADF Field	Value	Description
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
initiator		CADF component that contains the RESOURCE that initiated, originated, or instigated the event's ACTION, according to the OBSERVER
initiator:id	openstack:95f12d248a234a969f456cd2c794f29a	OpenStack initiator id
initiator:typeURI	service/security/account/user	Indicates that the initiator is a user (from the CADF resource taxonomy)
initiator:name	*<user_name>*	User name of the authenticated user defined in Keystone
initiator:host	agent:python-novaclient address:9.26.27.109	Initiator host information where the OpenStack authentication request came from
target		CADF component that contains the RESOURCE against which the ACTION of a CADF Event Record was performed, was attempted, or is pending, according to the OBSERVER
target.id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id
target.typeURI	service/security/account/user	Indicates that the target is the user account in Keystone service
observer		CADF component that contains the RESOURCE that generates the CADF Event Record based on its observation (directly or indirectly) of the Actual Event
observer.typeURI	service/security	Indicates the observer is the Keystone service
observer:id	openstack:0f126160203748a5b4923f2eb6e3b7db	OpenStack target id

6.4 Sample OpenStack CADF event

A sample OpenStack CADF audit event generated by middleware:

```
{
   'typeURI': 'http://schemas.dmtf.org/cloud/audit/1.0/event',
   'id': 'openstack:a80dc5ee-be83-48ad-ad5e-6577f2217637‘
```

```
    'eventType': 'activity',
    'action': 'read/list',
    'outcome': 'success',
    'reason': {'reasonCode': '200', 'reasonType': 'HTTP'},
    'eventTime': '2014-01-17T23:23:38.109989+0000',
    'initiator': {
          'id': 'openstack:95f12d248a234a969f456cd2c794f29a'
          'typeURI': 'service/security/account/user',
          'name': `<user name>',
          'project_id': 'openstack:e55b158759854ea6a7852aa76632c6c1',
           'credential': {
                  'token': `MIIQBgYJKoZIhvcNAQcCoIIP9z …… `,
                  'identity_status': 'Confirmed'            },
           'host': {
                  'agent': 'python-novaclient',
                  'address': '9.26.27.109'},
    },
    'target': {
         'id': 'openstack:0f126160203748a5b4923f2eb6e3b7db',
         'typeURI': `service/compute/servers',
         'name': 'nova`
         'addresses': [
              { 'url': 'http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1',
                'name': 'admin'},
              { 'url': 'http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1',
                'name': 'private'},
              { 'url': 'http://9.26.27.109:8774/v2/e55b158759854ea6a7852aa76632c6c1',
                'name': 'public'}
          ],
    },
    'observer': { 'id': 'target'},
    'reporterchain': [
        { 'reporterTime': '2014-01-17T23:23:38.154152+0000',
          'role': 'modifier',
          'reporter': {'id': 'target'}}
     ],
    'requestPath': '/v2/56600971-90f3-4370-807f-ab79339381a9/servers',
    'tags': ['correlation_id?value=openstack:bcac04dc-e0be-4110-862c-347088a7836a'],
}
```

A sample OpenStack CADF audit evented generated by Keystone service:

```
{
   'typeURI': 'http://schemas.dmtf.org/cloud/audit/1.0/event',
   'id': 'openstack:a80dc5ee-be83-48ad-ad5e-6577f2217637`
    'eventType': 'activity',
    'action': 'authenticate',
    'outcome': 'success',
    'eventTime': '2014-01-17T23:23:38.109989+0000',
```

```
    'initiator': {
          'id': 'openstack:95f12d248a234a969f456cd2c794f29a'
          'typeURI': 'service/security/account/user',
          'name': '<user name>',
           'host': {
                  'agent': 'python-novaclient',
                  'address': '9.26.27.109'},
    },
    'target': {
         'id': 'openstack:0f126160203748a5b4923f2eb6e3b7db',
         'typeURI': 'service/security/account/user',
    },
    'observer': { 'id': 'openstack:95f12d248a234a969f456aw0ju0cw09j'
                'typeURI': 'service/security',
   }
}
```

ANNEX A
Compute service

URL	TypeURI	Action	Description
POST v1.1/?{tenant_id}?/os-snapshots	service/compute/os-snapshots	create	Creates a snapshot.
GET v1.1/?{tenant_id}?/os-snapshots	service/compute/os-snapshots	read/list	Lists snapshots.
GET v1.1/?{tenant_id}?/os-snapshots/?{snapshot_id}?	service/compute/os-snapshots/snapshot	read	Shows information for a specified snapshot.
DELETE v1.1/?{tenant_id}?/os-snapshots/?{snapshot_id}?	service/compute/os-snapshots/snapshot	delete	Deletes a specified snapshot from the account. The operation does not require a request body and does not return a response body. This operation is asynchronous. You must list snapshots repeatedly to determine whether the snapshot was deleted.
GET v1.1/?{tenant_id}?/os-snapshots/detail	service/compute/os-snapshots/detail	read/list	Lists details for a specified snapshot. The operation does not require a request body.
GET v1.1/?{tenant_id}?/os-volumes	service/compute/os-volumes	read/list	Lists the volumes associated with the account. The operation does not require a request body.
POST v1.1/?{tenant_id}?/os-volumes/?{volume_id}?	service/compute/os-volumes/volume	create	Creates a volume. The operation requires a request body.
GET v1.1/?{tenant_id}?/os-volumes/?{volume_id}?	service/compute/os-volumes/volume	read	Shows information for a specified volume.
DELETE v1.1/?{tenant_id}?/os-volumes/?{volume_id}?	service/compute/os-volumes/volume	delete	Deletes a specified volume.
GET v1.1/?{tenant_id}?/os-volumes/detail	service/compute/os-volumes/detail	read/list	Lists details for a specified volume. The operation does not require a request body.
GET v1.1/?{tenant_id}?/os-volume-types	service/compute/os-volume-types	read/list	Lists volume types.
GET v1.1/?{tenant_id}?/os-volume-types/?{volume_type_id}?	service/compute/os-volume-types/volume-type	read	Shows information for a specified volume type.
POST v2/?{tenant_id}?	service/compute/os-networks	update	Creates a network.
GET v2/?{tenant_id}?/extensions	service/compute/extensions	read/list	Lists all available extensions.
GET v2/?{tenant_id}?/extensions/?{alias}?	service/compute/extensions/alias	read	Gets details about the specified extension.
GET v2/?{tenant_id}?/flavors	service/compute/flavors	read/list	Lists all flavors. Includes the access type, which is public or private.
POST v2/?{tenant_id}?/flavors	service/compute/flavors	create	Creates a flavor.

URL	TypeURI	Action	Description
GET v2/?{tenant_id}?/flavors/?{flavor_id}?	service/compute/flavors/flavor	read	Gets the flavor access type, which is either public or private.
DELETE v2/?{tenant_id}?/flavors/?{flavor_id}?	service/compute/flavors/flavor	delete	Deletes a flavor.
GET v2/?{tenant_id}?/flavors/?{flavor_id}?/os-extra_specs	service/compute/flavors/flavor/os-extra_specs	read/list	Lists the extra-specs or keys for the specified flavor.
POST v2/?{tenant_id}?/flavors/?{flavor_id}?/os-extra_specs	service/compute/flavors/flavor/os-extra_specs	create	Creates extra-specs or keys for the specified flavor.
GET v2/?{tenant_id}?/flavors/?{flavor_id}?/os-extra_specs/?{key_id}?	service/compute/flavors/flavor/os-extra_specs/key	read	Gets the value of the specified key.
DELETE v2/?{tenant_id}?/flavors/?{flavor_id}?/os-extra_specs/?{key_id}?	service/compute/flavors/flavor/os-extra_specs/key	delete	Delete a specified extra-spec by key.
GET v2/?{tenant_id}?/flavors/?{flavor_id}?/os-flavor-access	service/compute/flavors/flavor/os-flavor-access	read/list	Lists tenants with access to the specified private flavor.
GET v2/?{tenant_id}?/flavors/detail	service/compute/flavors/detail	read/list	Lists details for available flavors. Includes the rxtx_factor extended attribute.
GET v2/?{tenant_id}?/images/?{image_id}?	service/compute/images/image	read	Describes a specific image.
GET v2/?{tenant_id}?/images/detail	service/compute/images/detail	read/list	Lists images.
GET v2/?{tenant_id}?/limits	service/compute/limits	read/list	Returns current limits for the account.
GET v2/?{tenant_id}?/limits/tenant_id=?{customer_tenant_id}?	service/compute/limits/tenant	read	Enables administrators to get absolute and rate limit information, including information on currently used absolute limits, for the specified customer tenant ID.
GET v2/?{tenant_id}?/os-agents	service/compute/os-agents	read/list	Lists all agent builds.
POST v2/?{tenant_id}?/os-agents	service/compute/os-agents	create	Creates an agent build.
DELETE v2/?{tenant_id}?/os-agents	service/compute/os-agents	delete	Deletes an existing agent build.
PUT v2/?{tenant_id}?/os-agents/?{id}?	service/compute/os-agents/os-agent	update	Updates an agent build.
GET v2/?{tenant_id}?/os-aggregates	service/compute/os-aggregates	read/list	Lists all aggregates.

URL	TypeURI	Action	Description
POST v2/?{tenant_id}?/os-aggregates	service/compute/os-aggregates	create	Creates an aggregate.
DELETE v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	delete	Deletes an aggregate.
GET v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	read	Gets details about a specified aggregate.
PUT v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	update	Updates the name, and optionally the availability zone, for a specified aggregate.
POST v2/?{tenant_id}?/os-certificates	service/compute/os-certificates	create	Creates a root certificate.
GET v2/?{tenant_id}?/os-certificates	service/compute/os-certificates	read/list	Lists root certificates owned by a specified tenant ID.
GET v2/?{tenant_id}?/os-cloudpipe	service/compute/os-cloudpipe	read/list	Lists cloudpipes.
POST v2/?{tenant_id}?/os-cloudpipe	service/compute/os-cloudpipe	create	Creates a cloudpipe.
POST v2/?{tenant_id}?/os-cloudpipe/configure-project	service/compute/os-cloudpipe/configure-project	update	Updates the virtual private network (VPN) IP address and port for a specified cloudpipe instance.
GET v2/?{tenant_id}?/os-fixed-ips/?{fixed_ip}?	service/compute/os-fixed-ips/ip	read	Gets data about a specified fixed IP address.
GET v2/?{tenant_id}?/os-floating-ip-dns	service/compute/os-floating-ip-dns	read/list	Lists registered DNS domains published by the DNS drivers.
PUT v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?	service/compute/os-floating-ip-dns/domain	update	Creates or updates a DNS domain.
DELETE v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?	service/compute/os-floating-ip-dns/domain	delete	Deletes a DNS domain and all associated host entries.
GET v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?/entries/?{ip}?	service/compute/os-floating-ip-dns/domain/entries/entry	read/list	Lists DNS entries for a specified domain and IP.
PUT v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?/entries/?{name}?	service/compute/os-floating-ip-dns/domain/entries/entry	update	Creates or updates a DNS entry.
GET v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?/entries/?{name}?	service/compute/os-floating-ip-dns/domain/entries/entry	read	Finds a unique DNS entry for a specified domain and name.
DELETE v2/?{tenant_id}?/os-floating-ip-dns/?{domain}?/entries/?{na	service/compute/os-floating-ip-dns/domain/entries/entry	delete	Deletes a specified DNS entry.

URL	TypeURI	Action	Description
me}?			
GET v2/?{tenant_id}?/os-floating-ip-pools	service/compute/os-floating-ip-pools	read/list	Lists floating IP pools.
GET v2/?{tenant_id}?/os-floating-ips	service/compute/os-floating-ips	read/list	Lists floating IP addresses associated with the tenant or account.
POST v2/?{tenant_id}?/os-floating-ips	service/compute/os-floating-ips	create	Allocates a new floating IP address to a tenant or account.
GET v2/?{tenant_id}?/os-floating-ips/?{id}?	service/compute/os-floating-ips/floating-ip	read	Lists details of the floating IP address associated with floating_IP_address_ID.
DELETE v2/?{tenant_id}?/os-floating-ips/?{id}?	service/compute/os-floating-ips/floating-ip	delete	Deallocates the floating IP address associated with floating_IP_address_ID.
GET v2/?{tenant_id}?/os-floating-ips-bulk	service/compute/os-floating-ips-bulk	read/list	Lists all floating IPs.
POST v2/?{tenant_id}?/os-floating-ips-bulk	service/compute/os-floating-ips-bulk	create	Bulk-creates floating IPs.
GET v2/?{tenant_id}?/os-floating-ips-bulk/?{host_name}?	service/compute/os-floating-ips-bulk/host	read	Lists all floating IPs for a specified host.
POST v2/?{tenant_id}?/os-floating-ips-bulk/delete	service/compute/os-floating-ips-bulk/delete	delete	Bulk-deletes floating IPs.
GET v2/?{tenant_id}?/os-hosts	service/compute/os-hosts	read/list	Lists all hosts.
GET v2/?{tenant_id}?/os-hosts/?{host_name}?	service/compute/os-hosts/host	read	Shows information for a specified host.
PUT v2/?{tenant_id}?/os-hosts/?{host_name}?	service/compute/os-hosts/host	update	Enables a host or puts it in maintenance mode.
GET v2/?{tenant_id}?/os-hosts/?{host_name}?/reboot	service/compute/os-hosts/host/reboot	start/reboot	Reboots a host.
GET v2/?{tenant_id}?/os-hosts/?{host_name}?/shutdown	service/compute/os-hosts/host/shutdown	stop/shutdown	Shuts down a host.
GET v2/?{tenant_id}?/os-hosts/?{host_name}?/startup	service/compute/os-hosts/host/startup	start/startup	Starts a host.
GET v2/?{tenant_id}?/os-hypervisors	service/compute/os-hypervisors	read/list	Lists hypervisors information for each server obtained through the hypervisor-specific API, such as libvirt or XenAPI.
GET v2/?{tenant_id}?/os-hypervisors/?{hypervisor_hostname}?	service/compute/os-hypervisors/hypervisor	read	Shows the uptime for a specified hypervisor.
GET v2/?{tenant_id}?/os-hypervisors/?{hypervisor_hostname}?/servers	service/compute/os-hypervisors/hypervisor/servers	read/list	Lists instances that belong to specific hypervisors.
GET v2/?{tenant_id}?/os-hypervisors/detail	service/compute/os-hypervisors/detail	read/list	Shows information for a specified hypervisor. Typically configured as an admin-only extension by using policy.json settings.

URL	TypeURI	Action	Description
GET v2/?{tenant_id}?/os-hypervisors/statistics	service/compute/os-hypervisors/statistics	read/list	Shows hypervisor statistics over all compute nodes.
GET v2/?{tenant_id}?/os-keypairs	service/compute/os-keypairs	read/list	Lists keypairs associated with the account.
POST v2/?{tenant_id}?/os-keypairs	service/compute/os-keypairs	create	Generates or imports a keypair.
DELETE v2/?{tenant_id}?/os-keypairs/?{keypair_name}?	service/compute/os-keypairs/keypair	delete	Deletes a keypair.
GET v2/?{tenant_id}?/os-keypairs/?{keypair_name}?	service/compute/os-keypairs/keypair	read	Shows a keypair associated with the account.
GET v2/?{tenant_id}?/os-migrations	service/compute/os-migrations	read	Enables an administrative user to fetch in-progress migrations for a region or specified cell in a region.
GET v2/?{tenant_id}?/os-networks	service/compute/os-networks	read/list	Lists all networks that are available to the tenant.
GET v2/?{tenant_id}?/os-networks/?{id}?	service/compute/os-networks/network	read	Gets information about a specified network.
DELETE v2/?{tenant_id}?/os-networks/?{id}?	service/compute/os-networks/network	delete	Deletes a specified network.
POST v2/?{tenant_id}?/os-networks/add	service/compute/os-networks/add	create	Adds a specified network to a project.
GET v2/?{tenant_id}?/os-quota-sets	service/compute/os-quota-sets	read/list	Shows quotas for a tenant.
PUT v2/?{tenant_id}?/os-quota-sets	service/compute/os-quota-sets	update	Updates quotas for a tenant.
GET v2/?{tenant_id}?/os-quota-sets/defaults	service/compute/os-quota-sets/defaults	read	Gets default quotas for a tenant.
GET v2/?{tenant_id}?/os-quota-sets/user_id=?{user_id}?	service/compute/os-quota-sets	read	Shows quotas for a specified tenant and user.
POST v2/?{tenant_id}?/os-quota-sets/user_id=?{user_id}?	service/compute/os-quota-sets	update	Updates quotas for a specified tenant and user.
POST v2/?{tenant_id}?/os-security-group-rules	service/compute/os-security-group-rules	create	Creates a security group rule.
DELETE v2/?{tenant_id}?/os-security-group-rules/?{security_group_rule_id}?	service/compute/os-security-groups-rules/rule	delete	Deletes a security group rule.
GET v2/?{tenant_id}?/os-security-groups	service/compute/os-security-groups	read/list	Lists security groups.
POST v2/?{tenant_id}?/os-security-groups	service/compute/os-security-groups	create	Creates a security group.

URL	TypeURI	Action	Description
GET v2/?{tenant_id}?/os-security-groups/?{security_group_id}?	service/compute/os-security-groups/security_group	read	Gets information for a specified security group.
DELETE v2/?{tenant_id}?/os-security-groups/?{security_group_id}?	service/compute/os-security-groups/security_group	delete	Deletes a specified security group.
GET v2/?{tenant_id}?/os-services	service/compute/os-services	read/list	Lists all running services.
PUT v2/?{tenant_id}?/os-services/disable	service/compute/os-services/disable	disable	Disables scheduling for a service.
PUT v2/?{tenant_id}?/os-services/enable	service/compute/os-services/enable	enable	Enables scheduling for a service.
GET v2/?{tenant_id}?/os-simple-tenant-usage	service/compute/os-simple-tenant-usage	read/list	Lists usage information for all tenants.
GET v2/?{tenant_id}?/os-simple-tenant-usage/?{tenant_id}?	service/compute/os-simple-tenant-usage/tenant	read	Gets usage information for a tenant.
GET v2/?{tenant_id}?/servers	service/compute/servers	read/list	Lists IDs, names, and links for all servers.
POST v2/?{tenant_id}?/servers	service/compute/servers	create	Creates a server.
GET v2/?{tenant_id}?/servers/?{server_id}?	service/compute/servers/server	read	Gets details for a specified server.
PUT v2/?{tenant_id}?/servers/?{server_id}?	service/compute/servers/server	update	Updates the editable attributes of the specified server.
DELETE v2/?{tenant_id}?/servers/?{server_id}?	service/compute/servers/server	delete	Deletes a specified server.
GET v2/?{tenant_id}?/servers/?{server_id}?/diagnostics	service/compute/servers/server/diagnostics	read	Gets basic usage data for a specified server.
GET v2/?{tenant_id}?/servers/?{server_id}?/ips	service/compute/servers/server/ips	read/list	Lists networks and addresses for a specified tenant and server.
GET v2/?{tenant_id}?/servers/?{server_id}?/ips/?{network_label}?	service/compute/servers/server/ips/label	read/list	Lists addresses for a specified tenant, server, and network.
GET v2/?{tenant_id}?/servers/?{server_id}?/metadata	service/compute/servers/server/metadata	read/list	Lists metadata for the specified resource.
POST v2/?{tenant_id}?/servers/?{server_id}?/metadata	service/compute/servers/server/metadata	create	Updates metadata items by key for the specified resource.

URL	TypeURI	Action	Description
PUT v2/?{tenant_id}?/servers/?{server_id}?/metadata	service/compute/servers/server/metadata	update	Sets metadata for the specified resource.
GET v2/?{tenant_id}?/servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	read	Gets a metadata item by key for the specified resource.
PUT v2/?{tenant_id}?/servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	update	Sets a metadata item by key for the specified resource.
DELETE v2/?{tenant_id}?/servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	delete	Deletes a metadata item by key for the specified resource.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-instance-actions	service/compute/servers/server/os-instance-actions	read/list	Lists available actions for a specified server. Deployers set permissions for this request in the policy.json file. By default, all users can list actions.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-instance-actions/?{action_id}?	service/compute/servers/server/os-instance-actions/instance-action	read	Gets details for a specified action for a specified server instance. Deployers set permissions for this request in the policy.json file. By default, only administrators can get details for an action.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-security-groups	service/compute/servers/server/os-security-groups	read/list	Lists security groups for a specified server.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-virtual-interfaces	service/compute/servers/server/os-virtual-interfaces	read/list	Lists the virtual interfaces for a specified instance.
POST v2/?{tenant_id}?/servers/?{server_id}?/os-volume_attachments	service/compute/servers/server/os-volume_attachments	create	Attaches a volume to the specified server.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-volume_attachments	service/compute/servers/server/os-volume_attachments	read/list	Lists the volume attachments for the specified server.
GET v2/?{tenant_id}?/servers/?{server_id}?/os-volume_attachments/?{attachment_id}?	service/compute/servers/server/os-volume_attachments/attachment	read	Lists volume details for the specified volume attachment ID.
DELETE v2/?{tenant_id}?/servers/?{server_id}?/os-volume_attachments/?{attachment_id}?	service/compute/servers/server/os-volume_attachments/attachment	delete	Deletes the specified volume attachment from the specified server.
GET v2/?{tenant_id}?/servers/detail	service/compute/servers/detail	read/list	Lists details for all servers.

URL	TypeURI	Action	Description
GET v2/?{tenant_id}?/v2/images/?{image_id}?	service/compute/images/image	read	Gets details for a specified image. Includes the image size.
GET v2/?{tenant_id}?/v2/images/detail	service/compute/images/detail	read/list	Lists details for available images. Includes the image size.
GET v2/flavors	service/compute/flavors	read/list	Lists IDs, names, and links for available flavors.
GET v2/flavors/?{flavor_id}?	service/compute/flavors/flavor	read	Gets details for a specified flavor.
GET v2/flavors/detail	service/compute/flavors/detail	read/list	Lists all details for available flavors.
GET v2/images	service/compute/images	read/list	Lists IDs, names, and links for available images.
GET v2/images/?{image_id}?	service/compute/images/image	read	Gets details for a specified image.
DELETE v2/images/?{image_id}?	service/compute/images/image	delete	Deletes a specified image.
GET v2/images/?{image_id}?/metadata	service/compute/images/image/metadata	read/list	Lists metadata for the specified resource.
POST v2/images/?{image_id}?/metadata	service/compute/images/image/metadata	create	Updates metadata items by key for the specified resource.
PUT v2/images/?{image_id}?/metadata	service/compute/images/image/metadata	update	Sets metadata for the specified resource.
GET v2/images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	read	Gets a metadata item by key for the specified resource.
PUT v2/images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	update	Sets a metadata item by key for the specified resource.
DELETE v2/images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	delete	Deletes a metadata item by key for the specified resource.
GET v2/images/detail	service/compute/images/detail	read/list	Lists all details for available images.
GET v2/servers	service/compute/servers	read/list	Shows detailed extended server attribute information for all servers.
GET v2/servers/?{server_id}?	service/compute/servers/server	read	Shows extended server attributes for a specified server.
GET v2/servers/?{server_id}?/os-server-password	service/compute/servers/server/os-server-password	read	Gets the administrative password for a specified server.
POST v2/servers/?{server_id}?/os-server-password	service/compute/servers/server/os-server-password	update	Resets the administrative password for a specified server.

ANNEX B
Compute service (Action)

The following api requests are based on the values provided in the body of the request.

URL	TypeURI	Action	Description
POST v2/?{tenant_id}?/flavors/?{flavor_id}?/action	service/compute/flavours/flavor/action	update/addTenantAccess	Gives the specified tenant access to the specified private flavor.
DELETE v2/?{tenant_id}?/flavors/?{flavor_id}?/action	service/compute/flavours/flavor/action	delete	Revokes access from the specified tenant for the specified private flavor.
POST v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/set_metadata	Sets metadata for an aggregate.
POST v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/add_host	Adds a host to an aggregate.
POST v2/?{tenant_id}?/os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/remove_host	Removes a host from an aggregate.
POST v2/?{tenant_id}?/os-coverage/action	service/compute/os-coverage/action	update/report	Generates a coverage report.
POST v2/?{tenant_id}?/os-coverage/action	service/compute/os-coverage/action	update/start	Starts Nova coverage reporting.
POST v2/?{tenant_id}?/os-coverage/action	service/compute/os-coverage/action	update/start	Starts coverage reporting for all services. All reports are combined into a single report.
POST v2/?{tenant_id}?/os-coverage/action	service/compute/os-coverage/action	update/stop	Stops Nova coverage reporting.
POST v2/?{tenant_id}?/os-fixed-ips/?{fixed_ip}?/action	service/compute/os-fixed-ips/ip/action	update/reserve	Reserves or releases a fixed IP.
POST v2/?{tenant_id}?/os-networks/?{id}?/action	service/compute/os-networks/network/action	update/associate_host	Associates a specified network with a host.
POST v2/?{tenant_id}?/os-networks/?{id}?/action	service/compute/os-networks/network/action	update/disassociate_host	Disassociates the host from a specified network.
POST v2/?{tenant_id}?/os-networks/?{id}?/action	service/compute/os-networks/network/action	update/disassociate	Disassociates a specified network from a project so that the network can be reused.
POST v2/?{tenant_id}?/os-networks/?{id}?/action	service/compute/os-networks/network/action	update/disassociate_project	Disassociates the project from a specified network.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/pause	Pauses a server. Changes its status to PAUSED.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/unpause	Unpauses a PAUSED server and changes its status to ACTIVE.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/suspend	Suspends a server and changes its status to SUSPENDED.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/resume	Resumes a SUSPENDED server and changes its status to ACTIVE.
POST v2/?{tenant_id}?/servers/?{s	service/compute/servers/server/action	update/migrate	Migrates a server to a host. The scheduler chooses the host.

URL	TypeURI	Action	Description
erver_id}?/action			
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/resetNetwork	Resets networking on a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/injectNetworkInfo	Injects network information into a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/lock	Locks a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/unlock	Unlocks a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/createBackup	Backs up a server instance.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/os-migrateLive	Live-migrates a server to a new host without rebooting.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/os-resetState	Resets the state of a server to a specified state.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/evacuate	Evacuates a server from failed host.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/addSecurityGroup	Assigns the specified security group to the server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/removeSecurityGroup	Removes the specified security group from the server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/addFloatingIp	Adds a floating IP address to an instance.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/os-getConsoleOutput	Gets console output.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/os-getVNCConsole	Gets a console.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/forceDelete	Force-deletes a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/restore	Reverses the deletion of a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/rescue	Puts a server in rescue mode. Changes status to RESCUE.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/unrescue	Returns a server to its state before being rescued.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/os-stop	Halts a running server. Changes status to STOPPED.
POST v2/?{tenant_id}?/servers/?{s	service/compute/servers/server/action	update/os-start	Returns a STOPPED server to ACTIVE status.

URL	TypeURI	Action	Description
erver_id}?/action			
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/pool	Adds a floating IP address to an instance.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/removeFloatingIp	Removes a floating IP from an instance.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/resize	Resizes a server.
POST v2/?{tenant_id}?/servers/?{server_id}?/action	service/compute/servers/server/action	update/rebuild	Rebuilds a specified server.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/changePassword	Changes the password for a server. Specify the changePassword action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/reboot	Reboots the specified server. Specify the reboot action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/rebuild	Rebuilds the specified server. Specify the rebuild action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/resize	Resizes the specified server. Specify the resize action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/confirmResize	Confirms a pending resize action. Specify the confirmResize action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/revertResize	Cancels and reverts a pending resize action. Specify the revertResize action in the request body.
POST v2/?{tenant_id}?/servers/action	service/compute/servers/action	update/createImage	Creates a new image. Specify the createImage action in the request body.

ANNEX C
Network service

URL	TypeURI	Action	Description
GET v2/?{tenant_id}?/networks	service/network/networks	read/list	Lists networks to which the specified tenant has access.
POST v2/?{tenant_id}?/networks	service/network/networks	create	Creates a network.
GET v2/?{tenant_id}?/networks/?{network_id}?	service/network/networks/network	read	Shows information for the specified network.
PUT v2/?{tenant_id}?/networks/?{network_id}?	service/network/networks/network	update	Updates the specified network.
DELETE v2/?{tenant_id}?/networks/?{network_id}?	service/network/networks/network	delete	Deletes the specified network and its associated resources.
GET v2/?{tenant_id}?/ports	service/network/ports	read/list	Lists ports to which the tenant has access.
POST v2/?{tenant_id}?/ports	service/network/ports	create	Creates a port on a specified network.
GET v2/?{tenant_id}?/ports/?{port_id}?	service/network/ports/port	read	Shows information for a specified port.
PUT v2/?{tenant_id}?/ports/?{port_id}?	service/network/ports/port	update	Updates a specified port.
DELETE v2/?{tenant_id}?/ports/?{port_id}?	service/network/ports/port	delete	Deletes a specified port.
GET v2/?{tenant_id}?/quotas	service/network/quotas	read/list	Lists quotas for tenants who have non-default quota values.
GET v2/?{tenant_id}?/quotas/?{quota_id}?	service/network/quotas/quota	read	Shows information for a specified quota.
PUT v2/?{tenant_id}?/quotas/?{quota_id}?	service/network/quotas/quota	update	Updates quotas for a specified tenant. Use when non-default quotas are desired.
DELETE v2/?{tenant_id}?/quotas/?{quota_id}?	service/network/quotas/quota	delete	Resets quotas to default values for a specified tenant.
GET v2/?{tenant_id}?/subnets	service/network/subnets	read/list	Lists subnets to which the specified tenant has access.
POST v2/?{tenant_id}?/subnets	service/network/subnets	create	Creates a subnet on a specified network.
GET v2/?{tenant_id}?/subnets/?{subnet_id}?	service/network/subnets/subnet	read	Shows information for a specified subnet.
PUT v2/?{tenant_id}?/subnets/?{subnet_id}?	service/network/subnets/subnet	update	Updates a specified subnet.
DELETE v2/?{tenant_id}?/subnets/?{subnet_id}?	service/network/subnets/subnet	delete	Deletes a specified subnet.

ANNEX D
Object storage service

URL	TypeURI	Action	Description
GET v1/?{account}?	service/storage/object/account	read/list	Lists storage containers, sorted by name.
HEAD v1/?{account}?	service/storage/object/account	read	Gets container metadata, such as the number of containers and the total bytes stored in OpenStack Object Storage, for the tenant.
POST v1/?{account}?	service/storage/object/account	update	Creates or updates account metadata by associating custom metadata headers with the account level URI. These headers must have the format, X-Account-Meta-*.
GET v1/?{account}?/?{container}?	service/storage/object/account/container	read/list	Lists the objects stored in the container.
PUT v1/?{account}?/?{container}?	service/storage/object/account/container	update	Creates a container.
DELETE v1/?{account}?/?{container}?	service/storage/object/account/container	delete	Deletes an empty container.
HEAD v1/?{account}?/?{container}?	service/storage/object/account/container	read	Gets container metadata, including the number of objects and the total bytes of all objects stored in the container.
POST v1/?{account}?/?{container}?	service/storage/object/account/container	update	Creates or updates the arbitrary container metadata by associating custom metadata headers with the container level URI. These headers must have the format, X-Container-Meta-*.
GET v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	read	Gets data for the specified object.
PUT v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	update	Creates or updates the content and metadata for a specified object.
DELETE v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	delete	Permanently deletes an object from the OpenStack Object Storage system. In combination with the COPY command, you can use COPY and then DELETE to effectively move an object.
COPY v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	create/copy	Copies an object to another object with a new name in the OpenStack Object Storage system.
HEAD v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	read	Gets object metadata and other standard HTTP headers.
POST v1/?{account}?/?{container}?/?{object}?	service/storage/object/account/container/object	update	Updates arbitrary key/value metadata. Metadata must be in the format X-Object-Meta-*. You can also assign X-Delete-At or X-Delete-After to expiring objects. You cannot use this operation to change other headers, such as Content-Type.

ANNEX E
Block storage service

URL	TypeURI	Action	Description
POST v2/?{tenant_id}?/snapshots	service/storage/block/snapshots	create	Creates a snapshot, which is a point-in-time copy of a volume. You can create a new volume from the snapshot.
GET v2/?{tenant_id}?/snapshots	service/storage/block/snapshots	read/list	Lists summary information for all Cinder snapshots that are accessible to the tenant who submits the request.
GET v2/?{tenant_id}?/snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	read	Shows information for a specified snapshot.
PUT v2/?{tenant_id}?/snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	update	Updates a specified snapshot.
DELETE v2/?{tenant_id}?/snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	delete	Deletes a specified snapshot.
GET v2/?{tenant_id}?/snapshots/detail	service/storage/block/snapshots/detail	read/list	Lists detailed information for all Cinder snapshots that are accessible to the tenant who submits the request.
GET v2/?{tenant_id}?/types	service/storage/block/types	read/list	Lists volume types.
GET v2/?{tenant_id}?/types/?{volume_type_id}?	service/storage/block/types/type	read	Shows information about a specified volume type.
POST v2/?{tenant_id}?/volumes	service/storage/block/volumes	create	Creates a volume.
GET v2/?{tenant_id}?/volumes	service/storage/block/volumes	read/list	Lists summary information for all Cinder volumes that are accessible to the tenant who submits the request.
GET v2/?{tenant_id}?/volumes/?{volume_id}?	service/storage/block/volumes/volume	read	Shows information about a specified volume.
PUT v2/?{tenant_id}?/volumes/?{volume_id}?	service/storage/block/volumes/volume	update	Updates a volume.
DELETE v2/?{tenant_id}?/volumes/?{volume_id}?	service/storage/block/volumes/volume	delete	Deletes a specified volume.
GET v2/?{tenant_id}?/volumes/detail	service/storage/block/volumes/detail	read/list	Lists detailed information for all Cinder volumes that are accessible to the tenant who submits the request.

339 # ANNEX F
340 # Image service

341

URL	TypeURI	Action	Description
GET v1/images	service/storage/image/images	read/list	Lists public VM images.
POST v1/images	service/storage/image/images	create	Registers a virtual machine (VM) image.
GET v1/images/?{image_id}?	service/storage/image/images/image	read	Shows details for the specified image.
PUT v1/images/?{image_id}?	service/storage/image/images/image	update	Updates an image, uploads an image file, or updates metadata for an image.
DELETE v1/images/?{image_id}?	service/storage/image/images/image	delete	Deletes the specified image.
PUT v1/images/?{image_id}?/members	service/storage/image/images/image/members	update	Replaces a membership list for an image.
PUT v1/images/?{image_id}?/members/?{owner}?	service/storage/image/images/image/members/member	update	Adds a member to an image. If you omit the request body from this call, this request adds the membership to the image, leaves the existing memberships unmodified, and defaults new memberships to have can_share set to false.
DELETE v1/images/?{image_id}?/members/?{owner}?	service/storage/image/images/image/members/member	delete	Removes a member from an image.
GET v1/images/detail	service/storage/image/images/detail	read	Lists all details for available images.
GET v1/shared-images/?{owner}?	service/storage/image/shared-images/member	read/list	Lists the VM images shared with a specified owner. The owner ID is the tenant ID.
GET v2/images	service/storage/image/images	read/list	Lists public virtual machine (VM) images.
POST v2/images	service/storage/image/images	create	Creates a virtual machine (VM) image.
GET v2/images/?{image_id}?	service/storage/image/images/image	read	Gets details for a specified image.
PATCH v2/images/?{image_id}?	service/storage/image/images/image	update	Updates a specified image.
DELETE v2/images/?{image_id}?	service/storage/image/images/image	delete	Deletes a specified image.
PUT v2/images/?{image_id}?/file	service/storage/image/images/image/file	update	Uploads binary image data.
GET v2/images/?{image_id}?/file	service/storage/image/images/image/file	read	Downloads binary image data.
POST v2/images/?{image_id}?/members	service/storage/image/images/image/members	update	Adds a specified tenant ID as an image member.
DELETE v2/images/?{image_id}?/members/?{member_id}?	service/storage/image/images/image/members/member	delete	Deletes a specified tenant ID from the member list of the specified image.
PUT v2/images/?{image_id}?/members/?{member_id}?	service/storage/image/images/image/members/member	update	Sets the specified status for the specified member of the specified image.
PUT v2/images/?{image_id}?/tags/?{tag}?	service/storage/image/images/image/tags/tag	update	Adds a specified tag to a specified image.

URL	TypeURI	Action	Description
DELETE v2/images/?{image_id}?/tags/?{tag}?	service/storage/image/images/image/tags/tag	delete	Deletes a specified tag from a specified image.
GET v2/schemas/image	service/storage/image/schemas/image	read	Gets a json-schema document that represents an image entity.
GET v2/schemas/images	service/storage/image/schemas/images	read	Gets a json-schema document that represents an images entity
GET v2/schemas/member	service/storage/image/schemas/member	read	Gets a json-schema document that represents an image member entity.
GET v2/schemas/members	service/storage/image/schemas/members	read	Gets a json-schema document that represents an image members entity

342

ANNEX G
(informative)

Change log

Version	Date	Description
1.0.0	2014-09-16	

Bibliography

DMTF DSP-IS0102, Distributed Management Task Force, Inc., *Architecture for Managing Clouds White Paper 1.0*, http://dmtf.org/sites/default/files/standards/documents/DSP-IS0102_1.0.0.pdf

DMTF DSP-ISO103, Distributed Management Task Force, Inc., *Use Cases and Interactions for Managing Clouds 1.0.0*, http://www.dmtf.org/sites/default/files/standards/documents/DSP-IS0103_1.0.0.pdf