Document Identifier: DSP2038

Date: 2015-04-16

Version: 1.1.0

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

A CADF Representation for OpenStack

Supersedes: 1.0.0

Document Class: Informative

Document Status: Published

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
- Steve Martinelli, IBM
- Mariam John, 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, 1.0*, 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 DSP0262 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.

3.4
Federation

The concept that users are managed by an Identity Provider (IdP) and OpenStack's Identity Service (Keystone) can establish a set of rules to map federation protocol attributes to Identity API attributes.

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 data 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

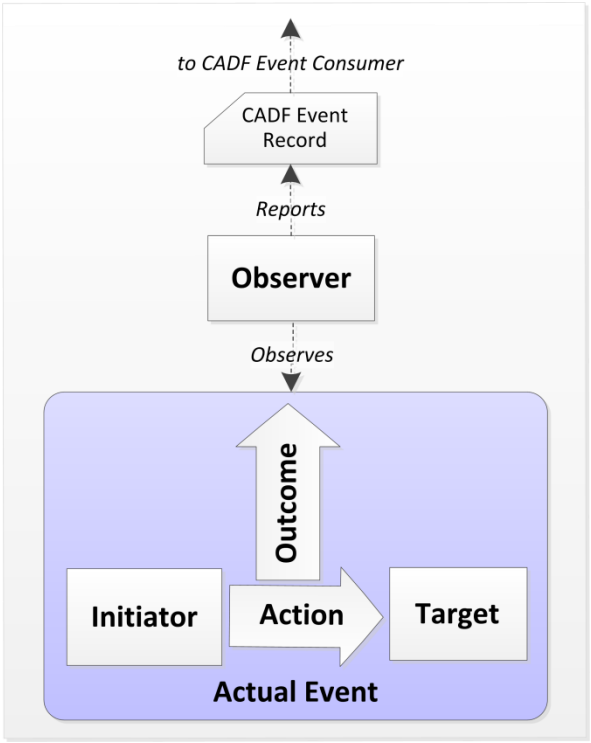
Table 1 describes the event model components and the semantics for each component

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.

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

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



194

195 **Figure 1 – CADF event model: Basic components**

196

197 4.4 Using CADF for audit

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

201

202 **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.

203 # 5 CADF with OpenStack

204 ## 5.1 OpenStack overview

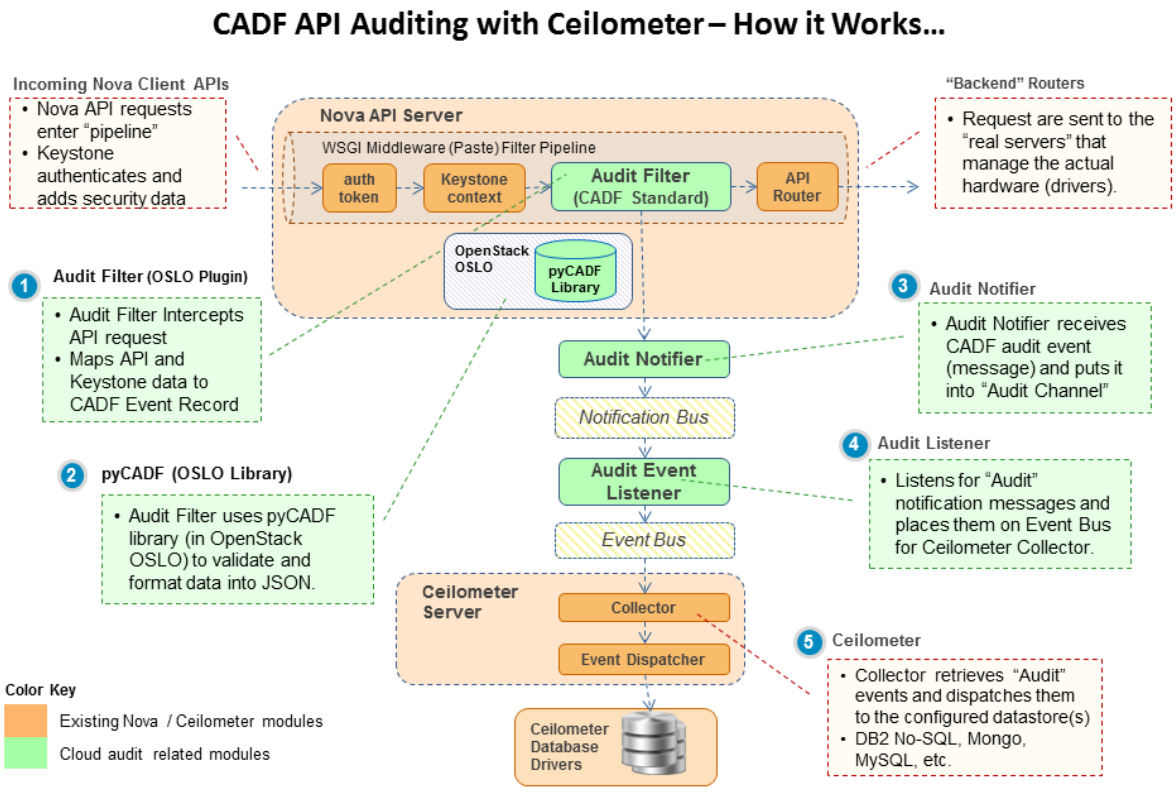
205 OpenStack is an open source project that seeks to provide a cloud computing platform that can be used
206 with public and private clouds. The technology consists of a series of interrelated projects delivering
207 various components for a cloud infrastructure solution.

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 6.3 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, then show what a CADF audit event will look like that records the execution of that REST API.

6.1 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',
   }
}
```

6.2 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.

6.2.1 GET server details

6.2.1.1 Request:

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

6.2.1.2 Field mappings:

Using the request 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
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

CADF Field	Value	Description
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.
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

CADF Field	Value	Description
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.

6.2.2 Deallocate floating IP address

6.2.2.1 Request:

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

6.2.2.2 Field mappings:

Using the request 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

CADF Field	Value	Description
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
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.

CADF Field	Value	Description
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.
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.

6.2.3 Embedded Action - Resize Instance

6.2.3.1 Request:

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"}}
```

6.2.3.2 Field mappings:

Using the request 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

CADF Field	Value	Description
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/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

CADF Field	Value	Description
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.

6.3 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.

6.3.1 Download binary image data

6.3.1.1 Request:

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

340 **6.3.1.2 Field mappings:**

341 Using the request 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)
initiator:name	*<user_name>*	User name of the authenticated user on the OpenStack Glance 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-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
observer:id	target	Indicates that the CADF target observed this event

CADF Field	Value	Description
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.

6.4 Keystone examples

6.4.1 Authenticating a user

6.4.1.1 Field mappings:

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.
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.

CADF Field	Value	Description
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 observer ID (i.e., the Keystone service's ID).

6.4.2 Authenticating a federated user

6.4.2.1 Field mappings:

The CADF audit event for federated user authentication is generated within the Keystone service. Since information about a federated user is stored on an external Identity Provider a credential object is attached to the initiator to include more information about the origins of the user. 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

CADF Field	Value	Description
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.
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
initiator.credential		CADF component that represents data on how the user authenticated
initiator.credential.type	http://docs.oasis-open.org/security/saml/v2.0	The specification of the type of federation protocol used during authentication
initiator.credential.token	671da331c47d4e29bb6ea1d270154ec3	Audit token ID value, represents the token the user provided before authenticated, may be None
initiator.credential.identity_provider	<*idp_name* >	Identity provider name that authenticated the user, as defined in Keystone
initiator.credential.user	<*user_name*>	User name of the authenticated user defined by the Identity provider

CADF Field	Value	Description
initiator.credential.groups	*[<group_name>]*	List of Keystone group names that the user is a member of.
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 observer ID (i.e., the Keystone service's ID).

6.4.3 Adding a role assignment to an actor and target

6.4.3.1 Field mappings:

The CADF audit event for role assignment creation and deletion is generated within the Keystone service. A role assignment comprises of three parts, the role being granted or revoked, an actor receiving the role (either a user or group), and a target upon which the role may be used (a project or domain). 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.

CADF Field	Value	Description
action	created.role_assignment <OR> deleted.role_assignment	CADF action mapped to user authentication
outcome	success	Generated by Keystone service to indicate successful authentication of credentials.
eventTime	2013-08-20T20:52:57.048554+0000	CADF generated timestamp
role	*<role_id>*	ID of the role assignment being created or deleted, as defined by Keystone.
group	*<group_id>*	ID of the group being granted the role assignment, as defined by Keystone. Either group or user will appear, not both.
user	*<user_id>*	ID of the user being granted the role assignment, as defined by Keystone. Either group or user will appear, not both.
project	*<project_id>*	ID of the project on which the user or group is being granted the role assignment, as defined by Keystone. Either project or domain will appear, not both.
domain	*<domain_id>*	ID of the domain on which the user or group is being granted the role assignment, as defined by Keystone. Either project or domain will appear, not both.
inherited_to_projects	Boolean value	Indicated whether a role assignment is inherited to projects of a domain
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

CADF Field	Value	Description
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 observer ID (i.e., the Keystone service's ID).

6.4.4 Keystone extensions to the CADF Resource Taxonomy

The following resource extensions to the CADF Data subtree have been introduced by Keystone:

- data/security/domain
- data/security/endpoint
- data/security/project
- data/security/region
- data/security/trust

6.5 Trove examples

6.5.1 Trove extensions to the CADF Resource Taxonomy

The complete list of APIs that are audited by the audit middleware can be found in the appendices.

6.5.2 Create a database server instance

6.5.2.1 Request:

Method	POST
Address	http://9.30.182.116:8779
URI	/v1.0/70ea121d43cd431ba60617792327f36e/instances

This request provisions a new database server instance based on the parameters (flavor, volume size, datastore type and version) specified in the body of the request. The CADF audit event for this request is shown as below:

6.5.2.2 Field mappings:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	'openstack:ddc0a2172bdb4f5cabaac998a8b30e35'	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	create	CADF action mapping for GET call targeting the Trove API
outcome	success	Generated by CADF filter for incoming requests, indicates that the Trove REST API call succeeded
eventTime	2015-03-08T06:56:34.765681+0000	CADF generated timestamp
reason	{'reasonCode': '200', 'reasonType': 'HTTP'}	Standard response for successful HTTP requests
initiator		
initiator:id	openstack:ddc0a2172bdb4f5cabaac998a8b30e35	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 Trove API call based on given name in Keystone
initiator:project_id	openstack:70ea121d43cd431ba60617792327f36e	The tenant id of the initiator
initiator:credential	'token': '819c xxxxxxxx 6bc8', 'identity_status': 'Confirmed'	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	'agent': 'python-keystoneclient', 'address': '9.30.182.116'	Initiator host information where the OpenStack compute service request came from
target		
target.id	openstack:trove	OpenStack target id
target:typeURI	service/database/instances	Indicates that the target is a compute service specifically targeting servers (from the CADF resource taxonomy)
target:name	trove	Name of event target

CADF Field	Value	Description
target:addresses	'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'admin'}, {'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'private'}, {'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'public'}]	Addresses of event target
requestPath	/v1.0/70ea121d43cd431ba60617792327f36e/instances	Request path on the Trove REST API call
observer		
observer:id	target	Indicates that the CADF target observed this event
reporterchain	'reporterTime': '2015-03-08T06:56:35.022826+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:bcf634a5-a270-413a-b1f6-f60ade183bac'	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.

6.5.3 List of status and information for all database server instances

6.5.3.1 Request:

Method	GET
Address	http://9.30.182.116:8779
URI	/v1.0/70ea121d43cd431ba60617792327f36e/instances

This request lists all the database instances provisioned and managed by Trove. The CADF audit event for this request is shown as below:

6.5.3.2 Field mappings:

CADF Field	Value	Description
typeURI	http://schemas.dmtf.org/cloud/audit/1.0/event	CADF event schema
id	openstack:trove	CADF generated event id

CADF Field	Value	Description
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 targeting the Trove API
outcome	success	Generated by CADF filter for incoming requests, indicates that the Trove REST API call succeeded
eventTime	2015-03-06T16:00:26.198797+0000	CADF generated timestamp
reason	{'reasonCode': '200', 'reasonType': 'HTTP'}	Standard response for successful HTTP requests
initiator		
initiator:id	openstack:ddc0a2172bdb4f5cabaac998a8b30e35	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 Trove API call based on given name in Keystone
initiator:project_id	openstack:70ea121d43cd431ba60617792327f36e	The tenant id of the initiator
initiator:credential	'token': 'aa1b xxxxxxxx 8079', 'identity_status': 'Confirmed'	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	'agent': 'python-keystoneclient', 'address': '9.30.182.116'	Initiator host information where the OpenStack compute service request came from
target		
target.id	openstack:trove	OpenStack target id
target:typeURI	service/database/instances	Indicates that the target is a compute service specifically targeting servers(from the CADF resource taxonomy)
target:name	trove	Name of event target
target:addresses	'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'admin'}, {'url': 'http://9.30.182.116:8779/v1.0/70ea1	Addresses of event target

CADF Field	Value	Description
	21d43cd431ba60617792327f36e', 'name': 'private'}, {'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'public'}]	
requestPath	/v1.0/70ea121d43cd431ba60617792327f36e/instances	Request path on the Trove REST API call
observer		
observer:id	target	Indicates that the CADF target observed this event
reporterchain	{'reporterTime': '2015-03-06T15:23:50.854762+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:e19e767f-40a7-4dc6-9baf-7ce09e99b915	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.

6.5.4 Create backup of a database server instance

6.5.4.1 Request:

Method	POST
Address	http://9.30.182.116:8779
URI	/v1.0/70ea121d43cd431ba60617792327f36e/backups

This request creates a backup of the database server instance specified in the body of the request. The CADF audit event for this request is shown as below:

6.5.4.2 Field mappings:

CADF Field	Value	Description
type URI	http://schemas.dmtf.org/cloud/audit/1.0/event/	CADF event schema
id	openstack:trove	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

CADF Field	Value	Description
		operations of a Cloud infrastructure or services.
action	create	CADF action mapping for GET call targeting the Trove API
outcome	success	Generated by CADF filter for incoming requests, indicates that the Trove REST API call succeeded
eventTime	2015-03-06T17:18:37.139257+0000	CADF generated timestamp
reason	{'reasonCode': '200', 'reasonType': 'HTTP'}	Standard response for successful HTTP requests
initiator		
initiator:id	openstack:ddc0a2172bdb4f5cabaac998a8b30e35	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 Trove API call based on given name in Keystone
initiator:project_id	openstack:70ea121d43cd431ba60617792327f36e	The tenant id of the initiator
initiator:credential	'token': '8921 xxxxxxxx 3494', 'identity_status': 'Confirmed'	Credential information on the OpenStack compute service request. Value is an obfuscated OpenStack Keystone token
initiator:host	'agent': 'python-keystoneclient', 'address': '9.30.182.116'	Initiator host information where the OpenStack compute service request came from
target		
target.id	openstack:trove	OpenStack target id
target:TypeURI	service/database/backups	Indicates that the target is a compute service specifically targeting servers(from the CADF resource taxonomy)
target:name	trove	Name of event target
target:addresses	'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'admin' 'url': 'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'private' 'url':	Addresses of event target

CADF Field	Value	Description
	'http://9.30.182.116:8779/v1.0/70ea121d43cd431ba60617792327f36e', 'name': 'public'	
requestPath	/v1.0/70ea121d43cd431ba60617792327f36e/backups	Request path on the Trove REST API call
observer		
observer:id	target	Indicates that the CADF target observed this event
reporterchain	{'reporterTime': '2015-03-06T15:23:50.854762+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:d38000e1-9169-4e8f-b675-f493414b91c5'	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.

7 OpenStack API mappings by project

7.1 Keystone - Identity Service

Group APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	groups	data/security/group	create	Creates a new group.
PATCH	groups/?{group_id}?	data/security/group	update	Update group.
DELETE	groups/?{group_id}?	data/security/group	delete	Delete group.
Project APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	projects	data/security/project	create	Creates a new project.
PATCH	projects/?{project_id}?	data/security/project	update	Update project.
DELETE	projects/?{project_id}?	data/security/project	delete	Delete project.
Role APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	roles	data/security/role	create	Creates a new role.
PATCH	roles/?{role_id}?	data/security/role	update	Update role.
DELETE	roles/?{role_id}?	data/security/role	delete	Delete role.

Domain APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	domains	data/security/domain	create	Creates a new domain.
PATCH	domains/?{domain_id}?	data/security/domain	update	Update domain.
DELETE	domains/?{domain_id}?	data/security/domain	delete	Delete domain.
User APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	users	data/security/account/user	create	Creates a new user.
PATCH	users/?{user_id}?	data/security/account/user	update	Update user.
DELETE	users/?{user_id}?	data/security/account/user	delete	Delete user.
Trust APIs				
Method	**API Path Extension** Base Path: /v3/OS-TRUST	**Type URI**	**Action**	**Description**
POST	trusts	data/security/trust	create	Creates a new trust.
DELETE	trusts/?{trust_id}?	data/security/trust	delete	Delete trust.
Region APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	regions	data/security/region	create	Creates a new region.
PATCH	regions/?{region_id}?	data/security/region	update	Update region.
DELETE	regions/?{region_id}?	data/security/region	delete	Delete region.
Endpoint APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	endpoints	data/security/endpoint	create	Creates a new endpoint.
PATCH	endpoints/?{endpoint_id}?	data/security/endpoint	update	Update endpoint.
DELETE	endpoints/?{endpoint_id}?	data/security/endpoint	delete	Delete endpoint.
Service APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	services	data/security/service	create	Creates a new service.
PATCH	services/?{service_id}?	data/security/service	update	Update service.
DELETE	services/?{service_id}?	data/security/service	delete	Delete service.
Policy APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	policies	data/security/group	create	Creates a new policy.
PATCH	policies/?{ policy_id}?	data/security/policy	update	Update policy.
DELETE	policies/?{ policy_id}?	data/security/policy	delete	Delete policy.

Role Assignment APIs				
Method	**API Path Extension** Base Path: /v3//**?**{tenant_id}?/	**Type URI**	**Action**	**Description**
PUT	domains/{domain_id}/users/{user_id}/roles/{role_id}	data/security/account/user	update	Grant a role to a user on a domain.
PUT	domains/{domain_id}/groups/{group_id}/roles/{role_id}	data/security/account/user	update	Grant a role to a group on a domain.
PUT	projects/{project_id}/users/{user_id}/roles/{role_id}	data/security/account/user	update	Grant a role to a user on a project.
PUT	projects/{project_id}/groups/{group_id}/roles/{role_id}	data/security/account/user	update	Grant a role to a group on a project.
DELETE	domains/{domain_id}/users/{user_id}/roles/{role_id}	data/security/account/user	delete	Revoke a role from a user on a domain.
DELETE	domains/{domain_id}/groups/{group_id}/roles/{role_id}	data/security/account/user	delete	Revoke a role from a group on a domain.
DELETE	projects/{project_id}/users/{user_id}/roles/{role_id}	data/security/account/user	delete	Revoke a role from a user on a project.
DELETE	projects/{project_id}/groups/{group_id}/roles/{role_id}	data/security/account/user	delete	Revoke a role from a group on a project.
OAuth 1.0 APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	OS-OAUTH1/consumers	data/security/account	create	Creates a new consumer.
PATCH	OS-OAUTH1/consumers/?{consumer_id}?	data/security/account	update	Update consumer.
DELETE	OS-OAUTH1/consumers/?{consumer_id}?	data/security/account	delete	Delete consumer.
POST	OS-OAUTH1/request_token	data/security/credential	create	Creates a new request token.
POST	OS-OAUTH1/access_token	data/security/credential	create	Creates a new access token.
DELETE	users/{user_id}/OS-OAUTH1/access_tokens/{access_token_id}	data/security/credential	delete	Delete access token.
Authentication APIs				
Method	**API Path Extension** Base Path: /v3/	**Type URI**	**Action**	**Description**
POST	auth/tokens	data/security/account/user	authenticate	User authenticates, and retrieves a token.

7.2 Nova - Compute Service

Note: text in red indicates a special case mapping.

7.2.1 Version 1.1 APIs

Snapshot APIs				
Method	**API Path Extension** Base Path: /v1.1/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	os-snapshots	service/compute/os-snapshots	create	Creates a snapshot.
GET	os-snapshots	service/compute/os-snapshots	read/list	Lists snapshots.
GET	os-snapshots/?{snapshot_id}?	service/compute/os-snapshots/snapshot	read	Shows information for a specified snapshot.
DELETE	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	os-snapshots/detail	service/compute/os-snapshots/detail	read/list	Lists details for a specified snapshot. The operation does not require a request body.
Volume APIs				
Method	**API Path Extension** Base Path: /v1.1/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-volumes	service/compute/os-volumes	read/list	Lists the volumes associated with the account. The operation does not require a request body.
POST	os-volumes/?{volume_id}?	service/compute/os-volumes/volume	create	Creates a volume. The operation requires a request body.
GET	os-volumes/?{volume_id}?	service/compute/os-volumes/volume	read	Shows information for a specified volume.
DELETE	os-volumes/?{volume_id}?	service/compute/os-volumes/volume	delete	Deletes a specified volume.
GET	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	os-volume-types	service/compute/os-volume-types	read/list	Lists volume types.
GET	os-volume-types/?{volume_type_id}?	service/compute/os-volume-types/volume-type	read	Shows information for a specified volume type.

7.2.2 Version 2 APIs

- Reference: http://developer.openstack.org/api-ref-compute-v2.html

Extension APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	extensions	service/compute/extensions	read/list	Lists all available extensions.
GET	extensions/?{alias}?	service/compute/extensions/alias	read	Gets details about the specified extension.
Servers APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	servers	service/compute/servers	read/list	Lists IDs, names, and links for all servers.
POST	servers	service/compute/servers	create	Creates a server.
GET	servers/detail	service/compute/servers/detail	read/list	Lists details for all servers.
GET	servers/?{server_id}?	service/compute/servers/server	read	Gets details for a specified server.
PUT	servers/?{server_id}?	service/compute/servers/server	update	Updates the editable attributes of the specified server.
DELETE	servers/?{server_id}?	service/compute/servers/server	delete	Deletes a specified server.
Server Metadata APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	servers/?{server_id}?/metadata	service/compute/servers/server/metadata	read/list	Lists metadata for the specified resource.
PUT	servers/?{server_id}?/metadata	service/compute/servers/server/metadata	update	Sets metadata for the specified resource.
POST	servers/?{server_id}?/metadata	service/compute/servers/server/metadata	create	Updates metadata items by key for the specified resource.
GET	servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	read	Gets a metadata item by key for the specified resource.
PUT	servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	update	Sets a metadata item by key for the specified resource.
DELETE	servers/?{server_id}?/metadata/?{key}?	service/compute/servers/server/metadata/key	delete	Deletes a metadata item by key for the specified resource.

Server Addresses APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	servers/?{server_id}?/ips	service/compute/servers/server/ips	read/list	Lists networks and addresses for a specified tenant and server.
GET	servers/?{server_id}?/ips/?{network_label}?	service/compute/servers/server/ips/label	read/list	Lists addresses for a specified tenant, server, and network.
Server Action APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/action	service/compute/servers/action	update/changePassword	Changes the password for a server. Specify the changePassword action in the request body.
POST	servers/action	service/compute/servers/action	update/reboot	Reboots the specified server. Specify the reboot action in the request body.
POST	servers/action	service/compute/servers/action	update/rebuild	Rebuilds the specified server. Specify the rebuild action in the request body.
POST	servers/action	service/compute/servers/action	update/resize	Resizes the specified server. Specify the resize action in the request body.
POST	servers/action	service/compute/servers/action	update/confirmResize	Confirms a pending resize action. Specify the confirmResize action in the request body.
POST	servers/action	service/compute/servers/action	update/revertResize	Cancels and reverts a pending resize action. Specify the revertResize action in the request body.
POST	servers/action	service/compute/servers/action	update/createImage	Creates a new image. Specify the createImage action in the request body.
Flavors APIs				
Method	**API Path Extension** Base Path: /v2/{tenant_id}/	**TypeURI**	**Action**	**Description**
GET	flavors	service/compute/flavors	read/list	Lists IDs, names, and links for available flavors.
GET	flavors/detail	service/compute/flavors/detail	read/list	Lists all details for available flavors.
GET	flavors/?{flavor_id}?	service/compute/flavors/flavor	read	Gets details for a specified flavor.
Images APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	images	service/compute/images	read/list	Lists IDs, names, and links for available images.
GET	images/detail	service/compute/images/detail	read/list	Lists details for available images. Includes the image size.
GET	images/?{image_id}?	service/compute/images/image	read	Gets details for a specified image.
DELETE	images/?{image_id}?	service/compute/images/image	delete	Deletes a specified image.

Image metadata APIs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	images/?{image_id}?/metadata	service/compute/images/image/metadata	read/list	Lists metadata for the specified resource.
PUT	images/?{image_id}?/metadata	service/compute/images/image/metadata	update	Set metadata for the specified resource.
POST	images/?{image_id}?/metadata	service/compute/images/image/metadata	create	Updates metadata items by key for the specified resource.
GET	images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	read	Gets a metadata item by key for the specified resource.
PUT	images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	update	Sets a metadata item by key for the specified resource.
DELETE	images/?{image_id}?/metadata/?{key}?	service/compute/images/image/metadata/key	delete	Deletes a metadata item by key for the specified resource.

7.2.3 Version 2 Extensions APIs

Extensions add features, MIME types, actions, states, headers, parameters, and resources to the core Compute API without requiring a version change.

- The following API requests are based on the “actions” (values) provided in the body of the HTTP request.

Reference: http://developer.openstack.org/api-ref-compute-v2-ext.html

Method	API Path Extension Base Path: /v2/?{tenant_id}?/	TypeURI	Action	Description
Server Admin Actions				
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/pause	Pauses a server. Changes its status to PAUSED.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/unpause	Unpauses a PAUSED server and changes its status to ACTIVE.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/suspend	Suspends a server and changes its status to SUSPENDED.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/resume	Resumes a SUSPENDED server and changes its status to ACTIVE.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/migrate	Migrates a server to a host. The scheduler chooses the host.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/resetNetwork	Resets networking on a server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/injectNetworkInfo	Injects network information into a server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/lock	Locks a server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/unlock	Unlocks a server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/createBackup	Backs up a server instance.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-migrateLive	Live-migrates a server to a new host without rebooting.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-resetState	Resets the state of a server to a specified state.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/evacuate	Evacuates a server from failed host.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/addSecurityGroup	Assigns the specified security group to the server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/removeSecurityGroup	Removes the specified security group from the server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/addFloatingIp	Adds a floating IP address to an instance.

Flavor Access				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	flavors	service/compute/flavors	read/list	Lists all flavors. Includes the access type, which is public or private.
POST	flavors	service/compute/flavors	create	Creates a flavor.
GET	flavors/?{flavor_id}?	service/compute/flavors/flavor	read	Gets the flavor access type, which is either public or private.
GET	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	flavors/detail	service/compute/flavors/detail	read/list	Lists details for available flavors. • Includes extended attributes.
DELETE	flavors/?{flavor_id}?	service/compute/flavors/flavor	delete	Deletes a flavor.
POST	flavors/?{flavor_id}?/action	service/compute/flavours/flavor/action	update/addTenantAccess	Gives the specified tenant access to the specified private flavor.
DELETE	flavors/?{flavor_id}?/action	service/compute/flavours/flavor/action	delete	Revokes access from the specified tenant for the specified private flavor.
Flavor extra-specs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	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	flavors/?{flavor_id}?/os-extra_specs	service/compute/flavors/flavor/os-extra_specs	create	Creates extra-specs or keys for the specified flavor.
GET	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	flavors/?{flavor_id}?/os-extra_specs/?{key_id}?	service/compute/flavors/flavor/os-extra_specs/key	delete	Delete a specified extra-spec by key.
Images (with Size attribute)				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	images/?{image_id}?	service/compute/images/image	read	Describes a specific image.
GET	images/detail	service/compute/images/detail	read/list	Lists images.
Limits				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	limits	service/compute/limits	read/list	Returns current limits for the account.
GET	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.

Guest Agent				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-agents	service/compute/os-agents	read/list	Lists all agent builds.
POST	os-agents	service/compute/os-agents	create	Creates an agent build.
DELETE	os-agents	service/compute/os-agents	delete	Deletes an existing agent build.
PUT	os-agents/?{id}?	service/compute/os-agents/os-agent	update	Updates an agent build.
Host Aggregates				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-aggregates	service/compute/os-aggregates	read/list	Lists all aggregates.
POST	os-aggregates	service/compute/os-aggregates	create	Creates an aggregate.
DELETE	os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	delete	Deletes an aggregate.
GET	os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	read	Gets details about a specified aggregate.
PUT	os-aggregates/?{aggregate_id}?	service/compute/os-aggregates/os-aggregate	update	Updates the name, and optionally the availability zone, for a specified aggregate.
POST	os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/set_metadata	Sets metadata for an aggregate.
POST	os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/add_host	Adds a host to an aggregate.
POST	os-aggregates/?{aggregate_id}?/action	service/compute/os-aggregates/os-aggregate/action	update/remove_host	Removes a host from an aggregate.
Root Certificate				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	os-certificates	service/compute/os-certificates	create	Creates a root certificate.
GET	os-certificates	service/compute/os-certificates	read/list	Lists root certificates owned by a specified tenant ID.
Cloud Pipe				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-cloudpipe	service/compute/os-cloudpipe	read/list	Lists cloudpipes.
POST	os-cloudpipe	service/compute/os-cloudpipe	create	Creates a cloudpipe.
POST	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.
Server Console				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-getConsoleOutput	Gets console output.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-getVNCConsole	Gets a console.

Coverage Report				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	os-coverage/action	service/compute/os-coverage/action	update/report	Generates a coverage report.
POST	os-coverage/action	service/compute/os-coverage/action	update/start	Starts Nova coverage reporting.
POST	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	os-coverage/action	service/compute/os-coverage/action	update/stop	Stops Nova coverage reporting.
Server Deferred Delete				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/forceDelete	Force-deletes a server.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/restore	Reverses the deletion of a server.
Fixed IPs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-fixed-ips/?{fixed_ip}?	service/compute/os-fixed-ips/ip	read	Gets data about a specified fixed IP address.
POST	os-fixed-ips/?{fixed_ip}?/action	service/compute/os-fixed-ips/ip/action	update/reserve	Reserves or releases a fixed IP.
Floating IP DNS Records				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-floating-ip-dns	service/compute/os-floating-ip-dns	read/list	Lists registered DNS domains published by the DNS drivers.
PUT	os-floating-ip-dns/?{domain}?	service/compute/os-floating-ip-dns/domain	update	Creates or updates a DNS domain.
DELETE	os-floating-ip-dns/?{domain}?	service/compute/os-floating-ip-dns/domain	delete	Deletes a DNS domain and all associated host entries.
PUT	os-floating-ip-dns/?{domain}?/entries/?{name}?	service/compute/os-floating-ip-dns/domain/entries/entry	update	Creates or updates a DNS entry.
GET	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	os-floating-ip-dns/?{domain}?/entries/?{name}?	service/compute/os-floating-ip-dns/domain/entries/entry	delete	Deletes a specified DNS entry.
GET	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.
Floating IP Pools				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-floating-ip-pools	service/compute/os-floating-ip-pools	read/list	Lists floating IP pools.

Floating IPs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-floating-ips	service/compute/os-floating-ips	read/list	Lists floating IP addresses associated with the tenant or account.
POST	os-floating-ips	service/compute/os-floating-ips	create	Allocates a new floating IP address to a tenant or account.
GET	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	os-floating-ips/?{id}?	service/compute/os-floating-ips/floating-ip	delete	Deallocates the floating IP address associated with floating_IP_address_ID.
POST	servers/?{server_id}?/action `"addFloatingIp": { "address": "" }`	service/compute/servers/server/action	update/pool	Adds a floating IP address to an instance.
POST	servers/?{server_id}?/action `"removeFloatingIp": { "address": "" }`	service/compute/servers/server/action	update/removeFloatingIp	Removes a floating IP from an instance.
Floating IPs Bulk				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-floating-ips-bulk	service/compute/os-floating-ips-bulk	read/list	Lists all floating IPs.
POST	os-floating-ips-bulk	service/compute/os-floating-ips-bulk	create	Bulk-creates floating IPs.
POST	os-floating-ips-bulk/delete	service/compute/os-floating-ips-bulk/delete	delete	Bulk-deletes floating IPs.
GET	os-floating-ips-bulk/?{host_name}?	service/compute/os-floating-ips-bulk/host	read	Lists all floating IPs for a specified host.
Hosts				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-hosts	service/compute/os-hosts	read/list	Lists all hosts.
GET	os-hosts/?{host_name}?	service/compute/os-hosts/host	read	Shows information for a specified host.
PUT	os-hosts/?{host_name}?	service/compute/os-hosts/host	update	Enables a host or puts it in maintenance mode.
GET	os-hosts/?{host_name}?/startup	service/compute/os-hosts/host/startup	start/startup	Starts a host.
GET	os-hosts/?{host_name}?/shutdown	service/compute/os-hosts/host/shutdown	stop/shutdown	Shuts down a host.
GET	os-hosts/?{host_name}?/reboot	service/compute/os-hosts/host/reboot	start/reboot	Reboots a host.

Hypervisors				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	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	os-hypervisors/?{hypervisor_hostname}?	service/compute/os-hypervisors/hypervisor	read	Shows the uptime for a specified hypervisor.
GET	os-hypervisors/?{hypervisor_hostname}?/servers	service/compute/os-hypervisors/hypervisor/servers	read/list	Lists instances that belong to specific hypervisors.
GET	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.
GET	os-hypervisors/statistics	service/compute/os-hypervisors/statistics	read/list	Shows hypervisor statistics over all compute nodes.
Server (instance) actions				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	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	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.
Key Pairs				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-keypairs	service/compute/os-keypairs	read/list	Lists keypairs associated with the account.
POST	os-keypairs	service/compute/os-keypairs	create	Generates or imports a keypair.
DELETE	os-keypairs/?{keypair_name}?	service/compute/os-keypairs/keypair	delete	Deletes a keypair.
GET	os-keypairs/?{keypair_name}?	service/compute/os-keypairs/keypair	read	Shows a keypair associated with the account.
Migrations				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	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.

Networks				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	<no path>	service/compute/os-networks	update	Creates a network.
GET	os-networks	service/compute/os-networks	read/list	Lists all networks that are available to the tenant.
POST	os-networks/add	service/compute/os-networks/add	create	Adds a specified network to a project.
GET	os-networks/?{id}?	service/compute/os-networks/network	read	Gets information about a specified network.
DELETE	os-networks/?{id}?	service/compute/os-networks/network	delete	Deletes a specified network.
POST	os-networks/?{id}?/action `"associate_host": ""`	service/compute/os-networks/network/action	update/associate_host	Associates a specified network with a host.
POST	os-networks/?{id}?/action `"disassociate_host": null`	service/compute/os-networks/network/action	update/disassociate_host	Disassociates the host from a specified network.
POST	os-networks/?{id}?/action `"disassociate": null`	service/compute/os-networks/network/action	update/disassociate	Disassociates a specified network from a project so that the network can be reused.
POST	os-networks/?{id}?/action `"disassociate_project": null`	service/compute/os-networks/network/action	update/disassociate_project	Disassociates the project from a specified network.
Quota Sets				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-quota-sets	service/compute/os-quota-sets	read/list	Shows quotas for a tenant.
PUT	os-quota-sets	service/compute/os-quota-sets	update	Updates quotas for a tenant.
GET	os-quota-sets/defaults	service/compute/os-quota-sets/defaults	read	Gets default quotas for a tenant.
GET	os-quota-sets/user_id=?{user_id}?	service/compute/os-quota-sets	read	Shows quotas for a specified tenant and user.
POST	os-quota-sets/user_id=?{user_id}?	service/compute/os-quota-sets	update	Updates quotas for a specified tenant and user.
Security Group Rules				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	os-security-group-rules	service/compute/os-security-group-rules	create	Creates a security group rule.
DELETE	os-security-group-rules/?{security_group_rule_id}?	service/compute/os-security-groups-rules/rule	delete	Deletes a security group rule.

Security Groups				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-security-groups	service/compute/os-security-groups	read/list	Lists security groups.
POST	os-security-groups	service/compute/os-security-groups	create	Creates a security group.
GET	os-security-groups/?{security_group_id}?	service/compute/os-security-groups/security_group	read	Gets information for a specified security group.
DELETE	os-security-groups/?{security_group_id}?	service/compute/os-security-groups/security_group	delete	Deletes a specified security group.
GET	servers/?{server_id}?/os-security-groups	service/compute/servers/server/os-security-groups	read/list	Lists security groups for a specified server.
Server Password				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	/servers/?{server_id}?/os-server-password	service/compute/servers/server/os-server-password	read	Gets the administrative password for a specified server.
POST	/servers/?{server_id}?/os-server-password	service/compute/servers/server/os-server-password	update	Resets the administrative password for a specified server.
Server Start and Stop				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-stop	Halts a running server. Changes status to STOPPED.
POST	servers/?{server_id}?/action	service/compute/servers/server/action	update/os-start	Returns a STOPPED server to ACTIVE status.
Manages Services				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-services	service/compute/os-services	read/list	Lists all running services.
PUT	os-services/enable	service/compute/os-services/enable	enable	Enables scheduling for a service.
PUT	os-services/disable	service/compute/os-services/disable	disable	Disables scheduling for a service.
Usage Reports				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	os-simple-tenant-usage	service/compute/os-simple-tenant-usage	read/list	Lists usage information for all tenants.
GET	os-simple-tenant-usage/?{tenant_id}?	service/compute/os-simple-tenant-usage/tenant	read	Gets usage information for a tenant.
Virtual Interfaces				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	servers/?{server_id}?/os-virtual-interfaces	service/compute/servers/server/os-virtual-interfaces	read/list	Lists the virtual interfaces for a specified instance.

Volume Attachments				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/os-volume_attachments	service/compute/servers/server/os-volume_attachments	create	Attaches a volume to the specified server.
GET	servers/?{server_id}?/os-volume_attachments	service/compute/servers/server/os-volume_attachments	read/list	Lists the volume attachments for the specified server.
GET	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	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.
Servers and images with disk config				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/action `"resize": { ... }`	service/compute/servers/server/action	update/resize	Resizes a server.
POST	servers/?{server_id}?/action `"rebuild": { ... }`	service/compute/servers/server/action	update/rebuild	Rebuilds a specified server.
Server Rescue, Unrescue				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
POST	servers/?{server_id}?/action `"rescue": { }`	service/compute/servers/server/action	update/rescue	Puts a server in rescue mode. Changes status to RESCUE.
POST	servers/?{server_id}?/action `"unrescue": null`	service/compute/servers/server/action	update/unrescue	Returns a server to its state before being rescued.
Server Extended Attributes				
Method	**API Path Extension** Base Path: /v2/?{tenant_id}?/	**TypeURI**	**Action**	**Description**
GET	/servers `"servers"` (... }	service/compute/servers	read/list	Shows detailed extended server attribute information for all servers.
GET	/servers/?{server_id}? `"servers"` (... }	service/compute/servers/server	read	Shows extended server attributes for a specified server.

7.3 Neutron - Network Service

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

7.4 Swift - Object Storage Service

Method	API Path Extension Base Path: /v1/?{account}?/	TypeURI	Action	Description
GET	<none>	service/storage/object/account	read/list	Lists storage containers, sorted by name.
HEAD	<none>	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.

Method	API Path Extension Base Path: /v1/?{account}?/	TypeURI	Action	Description
POST	<none>	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-*.
Container				
GET	?{container}?	service/storage/object/account/container	read/list	Lists the objects stored in the container.
PUT	?{container}?	service/storage/object/account/container	update	Creates a container.
DELETE	?container}?	service/storage/object/account/container	delete	Deletes an empty container.
HEAD	?{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	?{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-*.
Container Object				
GET	?{container}?/?{object}?	service/storage/object/account/container/object	read	Gets data for the specified object.
PUT	?{container}?/?{object}?	service/storage/object/account/container/object	update	Creates or updates the content and metadata for a specified object.
DELETE	?{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	?{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	?{container}?/?{object}?	service/storage/object/account/container/object	read	Gets object metadata and other standard HTTP headers.
POST	?{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.

7.5 Cinder - Block Storage Service

Method	API Path Extension Base Path: /v2/?{tenant_id}?/	TypeURI	Action	Description
Snapshots				
POST	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	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	snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	read	Shows information for a specified snapshot.
PUT	snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	update	Updates a specified snapshot.
DELETE	snapshots/?{snapshot_id}?	service/storage/block/snapshots/snapshot	delete	Deletes a specified snapshot.
GET	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.
Volumes				
GET	types	service/storage/block/types	read/list	Lists volume types.
GET	types/?{volume_type_id}?	service/storage/block/types/type	read	Shows information about a specified volume type.
POST	volumes	service/storage/block/volumes	create	Creates a volume.
GET	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	volumes/?{volume_id}?	service/storage/block/volumes/volume	read	Shows information about a specified volume.
PUT	volumes/?{volume_id}?	service/storage/block/volumes/volume	update	Updates a volume.
DELETE	volumes/?{volume_id}?	service/storage/block/volumes/volume	delete	Deletes a specified volume.
GET	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.

7.6 Glance - Image Service

Version 1 and 2 APIs

Method	API Path Extension Base Path: /v1/	TypeURI	Action	Description
Images				
GET	images	service/storage/image/images	read/list	Lists public VM images.
POST	images	service/storage/image/images	create	Registers a virtual machine (VM) image.
GET	images/?{image_id}?	service/storage/image/images/image	read	Shows details for the specified image.
PUT	images/?{image_id}?	service/storage/image/images/image	update	Updates an image, uploads an image file, or updates metadata for an image.
DELETE	images/?{image_id}?	service/storage/image/images/image	delete	Deletes the specified image.
Membership				
PUT	images/?{image_id}?/members	service/storage/image/images/image/members	update	Replaces a membership list for an image.
PUT	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	images/?{image_id}?/members/?{owner}?	service/storage/image/images/image/members/member	delete	Removes a member from an image.
GET	images/detail	service/storage/image/images/detail	read	Lists all details for available images.
GET	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.
Method	**API Path Extension** Base Path: /v2/	**TypeURI**	**Action**	**Description**
Images				
GET	images	service/storage/image/images	read/list	Lists public virtual machine (VM) images.
POST	images	service/storage/image/images	create	Creates a virtual machine (VM) image.
GET	images/?{image_id}?	service/storage/image/images/image	read	Gets details for a specified image.
PATCH	images/?{image_id}?	service/storage/image/images/image	update	Updates a specified image.
DELETE	images/?{image_id}?	service/storage/image/images/image	delete	Deletes a specified image.
PUT	images/?{image_id}?/file	service/storage/image/images/image/file	update	Uploads binary image data.
GET	images/?{image_id}?/file	service/storage/image/images/image/file	read	Downloads binary image data.

Membership				
POST	images/?{image_id}?/members	service/storage/image/images/image/members	update	Adds a specified tenant ID as an image member.
DELETE	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	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	images/?{image_id}?/tags/?{tag}?	service/storage/image/images/image/tags/tag	update	Adds a specified tag to a specified image.
DELETE	images/?{image_id}?/tags/?{tag}?	service/storage/image/images/image/tags/tag	delete	Deletes a specified tag from a specified image.
Schemas				
GET	schemas/image	service/storage/image/schemas/image	read	Gets a json-schema document that represents an image entity.
GET	schemas/images	service/storage/image/schemas/images	read	Gets a json-schema document that represents an images entity
GET	schemas/member	service/storage/image/schemas/member	read	Gets a json-schema document that represents an image member entity.
GET	schemas/members	service/storage/image/schemas/members	read	Gets a json-schema document that represents an image members entity

7.7 Trove - Database Service

Database Instance APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
POST	/instances	service/database/instances/instance	create	Creates a new database instance.
GET	/instances	service/database/instances	read/list	Lists all database instances.
PUT	/instances/?{instance_id}?	service/database/instances/instance	update	Update database instance.
GET	/instances/?{instance_id}?	service/database/instances/instance	read/list	List database instance status and details.
DELETE	/instances/?{instance_id}?	service/database/instances/instance	delete	Delete database instance.
GET	/instances/?{instance_id}?/configuration	service/database/instances/instance/configuration	read/list	Get default configuration.
POST	/instances/?{instance_id}?/root	service/database/instances/instance/root	update	Enable root user.
GET	/instances/?{instance_id}?/root	service/database/instances/instance/root	read/list	List root-enabled status

Database Instance Action APIs *(action in message body)*				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
POST	/instances/?{instance_id}?/action `"restart": {}`	service/database/instances/instance/action	update/restart	Restart instance
POST	/instances/?{instance_id}?/action `"resize": { "flavorRef": "" }`	service/database/instances/instance/action	update/resize	Resize the instance
POST	/instances/?{instance_id}?/action `"resize": { "volume":""}`	service/database/instances/instance/action	update/resize	Resize the instance volume
Database APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
POST	/instances/?{instance_id}?/databases	service/database/instances/instance/databases	create	Create database
GET	/instances/?{instance_id}?/databases	service/database/instances/instance/databases	read/list	List database for instance
DELETE	/instances/?{instance_id}?/databases/?{database_name}?	service/database/instances/instance/databases/database	delete	Delete database

User APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
POST	/instances/?{instance_id}?/users	service/database/instances/instance/users	create	Create user (in database instance)
GET	/instances/?{instance_id}?/users	service/database/instances/instance/users	read/list	List users in database instance.
PUT	/instances/?{instance_id}?/users `"users": [ { "name": "", "password": "" } ]`	service/database/instances/instance/users	update	Change user password
PUT	/instances/?{instance_id}?/users/?{user}?	service/database/instances/instance/users/user	update	Modify user attributes
GET	/instances/?{instance_id}?/users/?{user}?	service/database/instances/instance/users/user	read/list	List user
DELETE	/instances/?{instance_id}?/users/?{user}?	service/database/instances/instance/users/user	delete	Delete user
GET	/instances/{instanceId}/users/{name}/databases	service/database/instances/instance/users/user/databases	read/list	List user access (all databases)
PUT	/instances/?{instance_id}?/users/?{user}?/databases	service/database/instances/instance/users/user/databases	update	Grant user access (to one or more databases on instance)
DELETE	/instances/?{instance_id}?/users/?{user}?/databases/?{database}?	service/database/instances/instance/users/user/databases/database	delete	Revoke user access (to one database)
Flavor APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
GET	/flavors	service/database/flavors	read/list	List flavors
GET	/flavors/?{flavor}?	service/database/flavors/flavor	read/list	List flavors by ID
Backup APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
POST	/backups	service/database/backups	create	Create backup
GET	/backups	service/database/backups	read/list	List backups
GET	/backups/?{backup}?	service/database/backups/backup	read/list	List backups by ID
DELETE	/backups/?{backup}?	service/database/backups/backup	delete	Delete backup
GET	/instances/?{instance_id}?/backups	service/database/instances/instance/backups	read/list	List backups by instance.
POST	/instances	service/database/instances	create	Restore backup

Configuration APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
GET	/configurations	service/database/configurations	read/list	List configurations
POST	/configurations	service/database/configurations	create	Create configuration
GET	/configurations/?{configuration}?	service/database/configurations/configuration	read/list	List configuration details
PATCH	/configurations/?{configuration}?	service/database/configurations/configuration	update	Update (some) configuration parameters
PUT	/configurations/?{configuration}?	service/database/configurations/configuration	update	Replace all configuration parameters
DELETE	/configurations/?{configuration}?	service/database/configurations/configuration	delete	Delete configuration group
GET	/configurations/?{configuration}?/instances	service/database/configurations/configuration/instances	read/list	List instances for configuration
GET	/datastores/versions/{versionId}/parameters	/service/database/datastores/versions/{version}/parameters	read/list	List Configuration parameters (regardless of datastore)
GET	/datastores/versions/{versionId}/parameters/{parameterId}	/service/database/datastores/versions/{version}/parameters/parameter	read/list	List Configuration parameter details (regardless of datastore)
Datastore Type APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
GET	/datastores	service/database/datastores	read/list	List all datastore types
GET	/datastores/?{datastore}?	service/database/datastores/datastore	read/list	List datastore type
GET	/datastores/?{datastore}?/versions	service/database/datastores/datastore/versions	read/list	List all datastore versions
GET	/datastores/?{datastore}?/versions/?{version}?	service/database/datastores/datastore/versions/version	read/list	list datastore version
Replication APIs				
Method	**API Path Extension** Base Path: v1.0/?{tenant_id}?/	**Type URI**	**Action**	**Description**
PATCH	/instances/instance_id	/service/database/instances/instance_id	update/detach	Detach a replica from its source.

ANNEX A
(informative)

Change log

Version	Date	Description
1.0.0	2014-07-15	
1.1.0	2015-04-16	Release includes the following updates: • Added new Keystone examples (Juno release update) • Added listing of Keystone and Trove extensions to CADF Resource Taxonomy. Added Annex for Trove APIs (draft) with API listing • Re-authored the Trove API tables to include complete API for Kilo release, the previous table was outdated and contained an old (and inaccurate subset). OpenStack Trove project acknowledges that it should update its own public API docs. • Merged in and verified Trove API mapping updates (tables) for appendix. Fixed missing or questionable entries that were in “red” text in previous revision. • Merged in Keystone API mapping table and final Trove updates. These now reflect OpenStack Kilo release APIs.

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-IS0103, 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

Python CADF library (pyCADF), Pypi open source (latest), https://pypi.python.org/pypi/pycadf

OpenStack API Reference, http://developer.openstack.org/api-ref.html