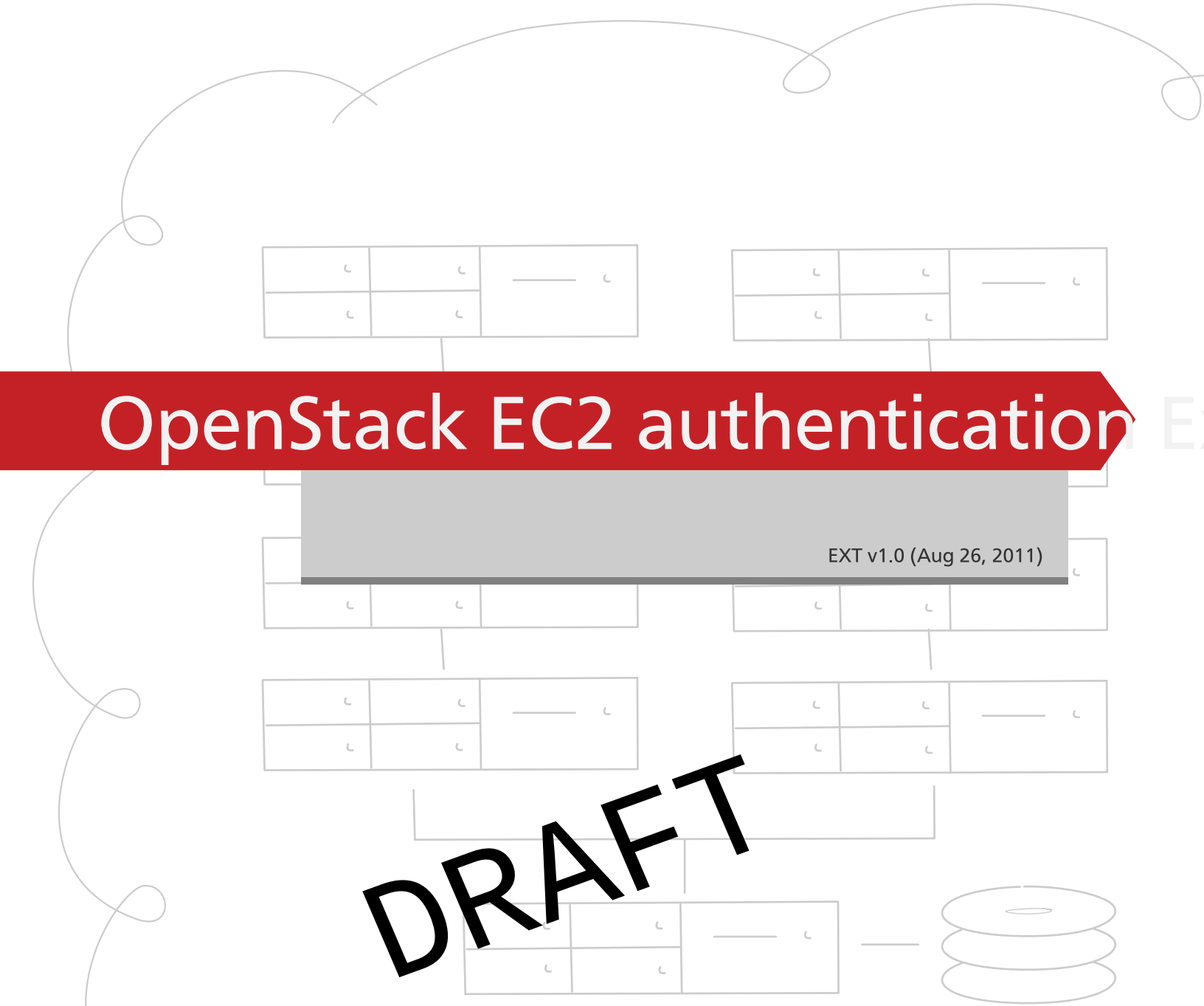
OpenStack EC2 authentication

EXT v1.0 (Aug 26, 2011)



DRAFT

openstack™

docs.openstack.org

OpenStack EC2 authentication Extension (Service Operations)

EXT v1.0 (2011-08-26)

This document is intended for client developers interested in using the OpenStack EC2 Authentication Service Extension along with the Keystone - OpenStack Identity (API).

Table of Contents

List of Examples

1. About This Extension

Name	OpenStack EC2 authentication Extension
Namespace	http://docs.openstack.org/identity/api/ext/OS-KSEC2/v1.0
Alias	OS-KSEC2
Dependencies	Keystone - OpenStack Identity
Doc Link (PDF)	https://github.com/openstack/keystone/raw/master/keystone/content/service/OS-KSEC2-service-devguide.pdf
Doc Link (WADL)	None, the extension makes no modification to the API WADL.
Doc Link (XSD)	https://raw.github.com/openstack/keystone/master/keystone/content/common/xsd/OS-KSEC2-credentials.xsd
Short Description	OpenStack EC2 authentication Service Extension to Keystone v2.0 API adds the capability to support EC2 style authentication..

Example 1.1. Extension Query Response: XML


```
<?xml version="1.0" encoding="UTF-8"?>
    <extension
        name="OpenStack EC2 authentication Extension"
        namespace="http://docs.openstack.org/identity/api/ext/OS-KSEC2/v1.0"
        alias="OS-KSEC2-service"
        updated="2011-08-25T09:50:00-00:00">

        <description>
              Adds the capability to support EC2 style authentication.
        </description>

        <atom:link rel="describedby"
                   type="application/pdf"
                   href="https://github.com/openstack/keystone/raw/master/
keystone/content/service/OS-KSEC2-service-devguide.pdf"/>
    </extension>
```


Example 1.2. Extension Query Response: JSON


```
{
  "extension":{
        "name": "OpenStack EC2 authentication Extension",
        "namespace": "http://docs.openstack.org/identity/api/ext/OS-KSEC2/v1.
0",
        "alias": "OS-KSEC2",
        "updated": "2011-08-25T09:50:00-00:00",
        "description": "Adds the capability to support EC2 style
 authentication.",
        "links": [
          {
            "rel": "describedby",
            "type": "application/pdf",
            "href": "https://github.com/openstack/keystone/raw/master/
keystone/content/service/OS-KSEC2-service-devguide.pdf"
          }
        ]
 }
}
```


1.1. Document Change History

Revision Date	Summary of Changes
Aug. 24, 2011	• Initial release.

2. Summary of Changes

The OpenStack EC2 authentication Service Extension allows authenticate call using ec2Credentials.

2.1. New Headers

None.

2.2. New Faults

None.

2.3. New Resources

None.

2.4. New Actions

None.

2.5. New Element

2.5.1. Openstack extension to Keystone v2.0 API enabling EC2 style authentication.

2.5.1.1. Authenticate

This extension allows authentication calls to accept new type of credentials *`ec2Credentials`*. These are additional type of credentials defined to support EC2 style authentication. The usage of *`ec2Credentials`* on a existing call to authenticate is illustrated below

Verb	URI	Description
POST	/tokens	Authenticate to generate a token.

Normal Response Code(s):200, 203

Error Response Code(s): unauthorized (401), userDisabled (403), badRequest (400), identityFault (500), serviceUnavailable(503)

This call will return a token if successful. Clients obtain this token, along with the URL to other service APIs, by first authenticating against the Keystone Service and supplying valid credentials. This extension provides support for Rackspace Style API Key credentials.

Client authentication is provided via a ReST interface using the POST method, with v2.0/tokens supplied as the path. A payload of credentials must be included in the body.

The Keystone Service is a ReSTful web service. It is the entry point to all service APIs. To access the Keystone Service, you must know URL of the Keystone service.

Example 2.1. XML Auth Request using EC2CREDENTIALS

```
<?xml version="1.0" encoding="UTF-8"?>
<auth
  xmlns="http://docs.openstack.org/identity/api/v2.0"
  tenantId="1234">
  <ec2Credentials
    xmlns="http://docs.openstack.org/identity/api/ext/OS-KSEC2/v1.0"
    username="testuser"
    key="aaaaa"
    signature="bbbbb"/>
</auth>
```

Example 2.2. JSON Auth Request using EC2CREDENTIALS

```
{
    "auth":{
        "OS-KSEC2-ec2Credentials":{
            "username":"test_user",
            "secret":"aaaaa",
            "signature":"bbb"
        },
        "tenantId":"77654"
    }
}
```

Example 2.3. XML Auth Response

```
<?xml version="1.0" encoding="UTF-8"?>
<auth xmlns="http://docs.openstack.org/identity/api/v2.0">
 <token expires="2010-11-01T03:32:15-05:00"
           id="ab48a9efdfedb23ty3494"/>
    <serviceCatalog>
        <service type="compute" name="Computers in the Cloud">
            <endpoint
                    region="North"
                    tenantId="1234"
          publicURL="https://north.compute.public.com/v2.0/1234"
                    internalURL="https://north.compute.internal.com/v2.0/
1234">
       <version
           id="2.0"
           info="https://north.compute.public.com/v2.0/"
           list="https://north.compute.public.com/" />
      </endpoint>
            <endpoint
                    region="South"
                    tenantId="3456"
                    publicURL="https://south.compute.public.com/v2.0/3456"
                    internalURL="https://south.compute.internal.com/v2.0/
3456">
          <version
           id="2.0"
           info="https://south.compute.public.com/v2.0/"
           list="https://south.compute.public.com/" />
      </endpoint>
        </service>
```

```
        <service type="object-store" name="HTTP Object Store">
            <endpoint
                    region="North"
                    tenantId="1234"
                    publicURL="https://north.object-store.public.com/v1/1234"
                    internalURL="https://north.object-store.internal.com/v1/
1234">
       <version
           id="1"
           info="https://north.object-store.public.com/v1/"
           list="https://north.object-store.public.com/" />
      </endpoint>
            <endpoint
                    region="South"
                    tenantId="3456"
                    publicURL="https://south.object-store.public.com/v2.0/
3456"
                    internalURL="https://south.object-store.internal.com/v2.0/
3456">
          <version
           id="2.0"
           info="https://south.object-store.public.com/v1/"
           list="https://south.object-store.public.com/" />
      </endpoint>
        </service>
        <service type="dns" name="DNS-as-a-Service">
            <endpoint
                    publicURL="https://dns.public.com/v2.0/blah-blah">
        <version
           id="2.0"
           info="https://dns.public.com/v2.0/"
           list="https://dns.public.com/" />
      </endpoint>
        </service>
    </serviceCatalog>
</auth>
```

Example 2.4. JSON Auth Response

```
{
    "access":{
        "token":{
            "id":"ab48a9efdfedb23ty3494",
            "expires":"2010-11-01T03:32:15-05:00",
            "tenant":{
                "id": "345",
                "name": "My Project"
            }
        },
        "user":{
            "id":"123",
            "name":"jqsmith",
            "roles":[{
                    "id":"234",
                    "name":"compute:admin"
                },
    {
                    "id":"235",
                    "name":"object-store:admin",
                    "tenantId":"1"
```

```
                }
            ],
            "roles_links":[]
        },
        "serviceCatalog":[{
                "name":"Cloud Servers",
                "type":"compute",
                "endpoints":[{
                        "tenantId":"1",
                        "publicURL":"https://compute.north.host/v1/1234",
                        "internalURL":"https://compute.north.host/v1/1234",
                        "region":"North",
                        "versionId":"1.0",
                        "versionInfo":"https://compute.north.host/v1.0/",
                        "versionList":"https://compute.north.host/"
                    },
                    {
                        "tenantId":"2",
                        "publicURL":"https://compute.north.host/v1.1/3456",
                        "internalURL":"https://compute.north.host/v1.1/3456",
                        "region":"North",
                        "versionId":"1.1",
                        "versionInfo":"https://compute.north.host/v1.1/",
                        "versionList":"https://compute.north.host/"
                    }
                ],
                "endpoints_links":[]
            },
            {
                "name":"Cloud Files",
                "type":"object-store",
                "endpoints":[{
                        "tenantId":"11",
                        "publicURL":"https://compute.north.host/v1/blah-blah",
                        "internalURL":"https://compute.north.host/v1/blah-
blah",
                        "region":"South",
                        "versionId":"1.0",
                        "versionInfo":"uri",
                        "versionList":"uri"
                    },
                    {
                        "tenantId":"2",
                        "publicURL":"https://compute.north.host/v1.1/blah-
blah",
                        "internalURL":"https://compute.north.host/v1.1/blah-
blah",
                        "region":"South",
                        "versionId":"1.1",
                        "versionInfo":"https://compute.north.host/v1.1/",
                        "versionList":"https://compute.north.host/"
                    }
                ],
                "endpoints_links":[{
                        "rel":"next",
                        "href":"https://identity.north.host/v2.0/endpoints?
marker=2"
                    }
                ]
            }
```

```
        ],
        "serviceCatalog_links":[{
                "rel":"next",
                "href":"https://identity.host/v2.0/endpoints?session=2hfh8Ar&
marker=2"
            }
        ]
    }
}
```