

Rackspace API Key Authentication

EXT v1.0 (Aug 26, 2011)

DRAFT



EXT v1.0 (2011-08-26)

This document is intended for client developers interested in using the Rackspace API Key Authentication Service Extension along with the Keystone - OpenStack Identity (API). The document is for informational purposes only and is provided "AS IS."

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

ii

Table of Contents

1. About This Extension	1
1.1. Document Change History	2
2. Summary of Changes	3
2.1. New Headers	3
2.2. New Faults	3
2.3. New Resources	3
2.4. New Actions	3
2.5. New Element	3
2.5.1. Rackspace extensions to Keystone v2.0 API enabling API Key authentication.	3

List of Examples

1.1. Extension Query Request: XML	2
1.2. Extension Query Request: JSON	2
2.1. XML Auth Request using apiKeyCredentials	4
2.2. JSON Auth Request using apiKeyCredentials	4
2.3. XML Auth Response	4
2.4. JSON Auth Response	5

1. About This Extension

Name	Rackspace API Key Authentication Service Extension
Namespace	http://docs.rackspace.com/identity/api/ext/RAX-KSKEY/v1.0
Alias	RAX-KSKEY-service
Dependencies	Keystone - OpenStack Identity
Doc Link (PDF)	https://github.com/openstack/keystone/raw/master/keystone/content/service/RAX-KSKEY-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/service/xsd/RAX-KSKEY-credentials.xsd
Short Description	Rackspace extensions to Keystone v2.0 API enabling API Key authentication.

Example 1.1. Extension Query Request: XML

```
<?xml version="1.0" encoding="UTF-8"?>
<extension xmlns="http://docs.openstack.org/common/api/v2.0"
  xmlns:atom="http://www.w3.org/2005/Atom"
  name="Rackspace API Key authentication" namespace="http://docs.
rackspace.com/identity/api/ext/RAX-KSKEY/v1.0"
  alias="RAX-KSKEY-service"
  updated="2011-08-14T13:25:27-06:00">
  <description>
    Rackspace extensions to Keystone v2.0 API
    enabling API Key authentication.
  </description>
  <atom:link rel="describedby" type="application/pdf"
    href="https://github.com/openstack/keystone/raw/
master/keystone/content/service/identitydevguide.pdf" />
</extension>
```

Example 1.2. Extension Query Request: JSON

```
{
  "extension": {
    "name": "Rackspace API Key Authentication",
    "namespace": "http://docs.rackspace.com/identity/api/ext/RAX-KSKEY/v1.0",
    "alias": "RAX-KSKEY",
    "updated": "2011-08-14T13:25:27-06:00",
    "description": "Rackspace extensions to Keystone v2.0 API enabling API Key
authentication.",
    "links": [ {
      "rel": "describedby",
      "type": "application/pdf",
      "href": "http://docs.rackspacecloud.com/identity/api/ext/RAX-KSKEY-
service.pdf"
    } ]
  }
}
```

1.1. Document Change History

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

2. Summary of Changes

The Rackspace API Key Authentication Service Extension allows authenticate call to happen using *apikeyCredentials*.

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. Rackspace extensions to Keystone v2.0 API enabling API Key authentication.

2.5.1.1. Authenticate

This extension allows authentication calls to accept new type of credentials *apikeyCredentials*. These are additional type of credentials defined to support rackspace style authentication. The usage of *apikeyCredentials* 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 apikeyCredentials

```
<?xml version="1.0" encoding="UTF-8"?>
<auth xmlns="http://docs.openstack.org/identity/api/v2.0">
  <apikeyCredentials
    xmlns="http://docs.rackspace.com/identity/api/ext/RAX-KSKEY/v1.0"
    username="testuser"
    apikey="aaaaa-bbbbb-cccc-12345678"/>
</auth>
```

Example 2.2. JSON Auth Request using apikeyCredentials

```
{
  "auth": {
    "RAX-KSKEY:apikeyCredentials": {
      "username": "test_user",
      "apikey": "aaaaa-bbbbb-cccc-12345678"
    }
  }
}
```

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

```

{
  "auth": {
    "token": {
      "id": "asdasdasd-adsasdadads-asdasdasd-adsadsasd",
      "expires": "2010-11-01T03:32:15-05:00"
    },
    "serviceCatalog": [
      {
        "name": "Cloud Servers",
        "type": "compute",
        "endpoints": [
          {
            "publicURL": "https://compute.north.host/v1/1234",
            "internalURL": "https://compute.north.host/v1/1234",
            "region": "North",
            "tenantId": "1234",
            "versionId": "1.0",
            "versionInfo": "https://compute.north.host/v1.0/",
            "versionList": "https://compute.north.host/"
          }, {
            "publicURL": "https://compute.north.host/v1.1/3456",
            "internalURL": "https://compute.north.host/v1.1/3456",
            "region": "North",
            "tenantId": "3456",
            "versionId": "1.1",

```

```
        "versionInfo": "https://compute.north.host/v1.1/",
        "versionList": "https://compute.north.host/"
    }
  ],
  {
    "name": "Cloud Files",
    "type": "object-store",
    "endpoints": [
      {
        "publicURL": "https://compute.north.host/v1/blah-blah",
        "internalURL": "https://compute.north.host/v1/blah-blah",
        "region": "South",
        "tenantId": "1234",
        "versionId": "1.0",
        "versionInfo": "uri",
        "versionList": "uri"
      },
      {
        "publicURL": "https://compute.north.host/v1.1/blah-blah",
        "internalURL": "https://compute.north.host/v1.1/blah-blah",
        "region": "South",
        "tenantId": "3456",
        "versionId": "1.1",
        "versionInfo": "https://compute.north.host/v1.1/",
        "versionList": "https://compute.north.host/"
      }
    ],
    "endpoint_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"
    }
  ]
}
```