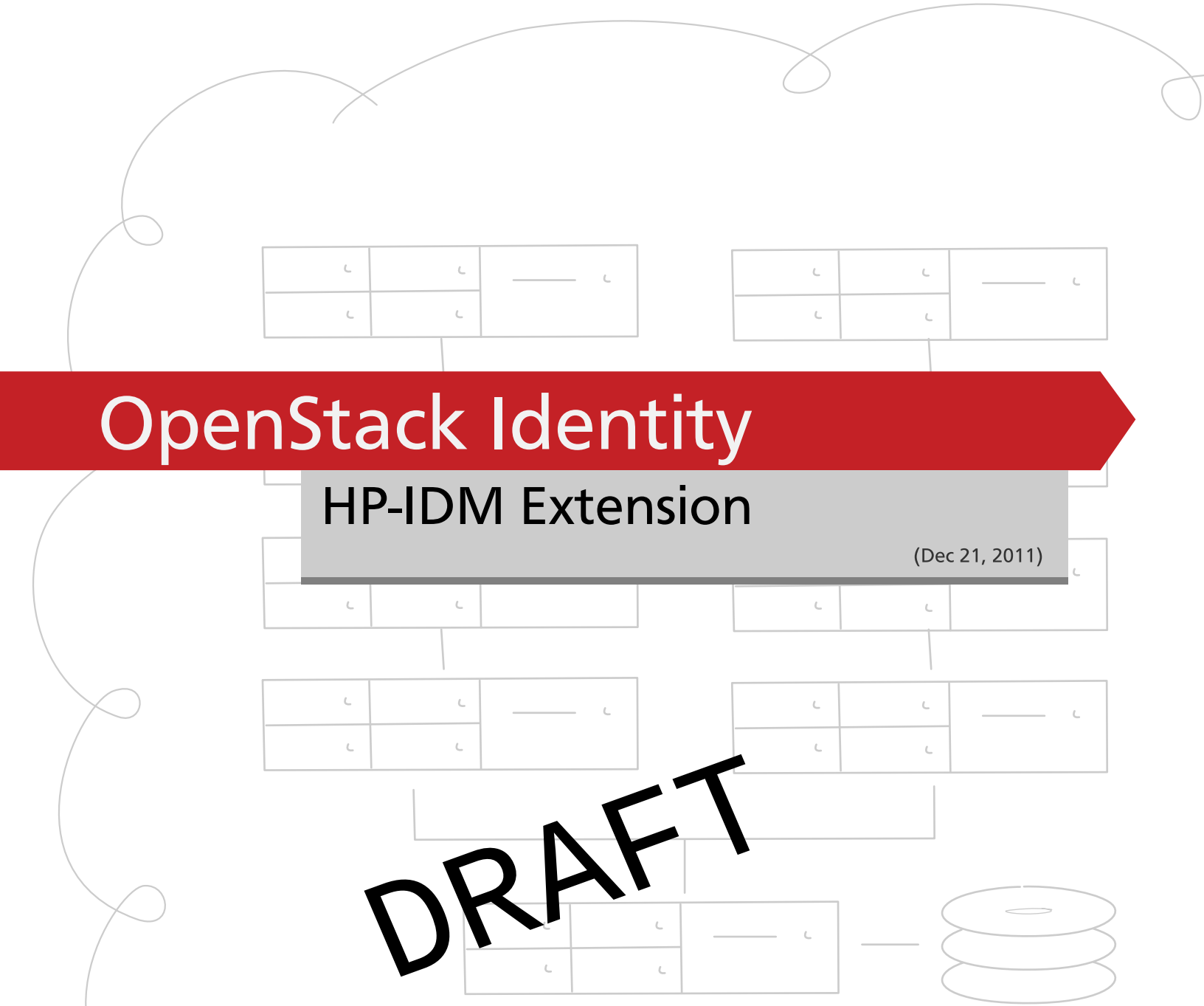
OpenStack Identity

HP-IDM Extension

(Dec 21, 2011)



openstack™

docs.openstack.org

OpenStack Identity HP-IDM Extension

HP-IDM Extension For Token Validation.

Table of Contents

1. About This Extension 1
1.1. Document Change History 3
2. Summary of Changes 4
2.1. New Headers 4
2.2. New Faults 4
2.3. New Resources 4
2.3.1. Validate Tokens With The New Optional HP-IDM-serviceId Parameter 4
2.4. New Actions 7
2.5. New States 7

List of Tables

2.1. Validate Token Request Parameters ... 5
2.2. Check Token Request Parameters ... 7

List of Examples

1.1. Sample Valid Token Request ... 2
1.2. Sample Valid Token Request With Global Service ID Specified ... 2
1.3. Extension Query Response: XML ... 2
1.4. Extension Query Response: JSON ... 2
2.1. Validate Token Response: XML ... 5
2.2. Validate Token Response: JSON ... 5

1. About This Extension

Name	HP-IDM Extension
Namespace	http://docs.openstack.org/identity/api/ext/HP-IDM/v1.0
Alias	HP-IDM
Contact	Guang Yee <`guang.yee@hp.com`>
Status	ALPHA
Last Update	2011-12-21
Dependencies	Keystone API v2.0 (2011-12-21)
Doc Link (PDF)	https://github.com/openstack/keystone/raw/master/content/admin/HP-IDM-admin-devguide.pdf
Doc Link (WADL)	https://raw.github.com/openstack/keystone/master/keystone/content/admin/HP-IDM-admin.wadl
Short Description	HP-IDM Admin Extension to Keystone V2.0 API adds capability to filter roles with optional service IDs for token validation to mitigate security risks with role name conflicts.

Example 1.1. Sample Valid Token Request

```
GET /v2.0/tokens/ab48a9efdfedb23ty3494?belongsTo=1&HP-IDM-serviceId=1,2 HTTP/
1.1
X-Auth-Token: 999888777666
Host: identity.api.openstack.org
Accept: application/json
```

Example 1.2. Sample Valid Token Request With Global Service ID Specified

```
GET /v2.0/tokens/ab48a9efdfedb23ty3494?belongsTo=1&HP-IDM-serviceId=1,2,global
 HTTP/1.1
X-Auth-Token: 999888777666
Host: identity.api.openstack.org
Accept: application/json
```

Example 1.3. Extension Query Response: XML


```
<?xml version="1.0" encoding="UTF-8"?>
    <extension
        xmlns="http://docs.openstack.org/common/api/v1.0"
        xmlns:atom="http://www.w3.org/2005/Atom"
        name="HP Token Validation Extension"
        namespace="http://docs.openstack.org/identity/api/ext/HP-IDM/v1.0"
        alias="HP-IDM"
        updated="2011-12-06T17:00:00-00:00">

        <description>
              Validate token with the optional HP-IDM-serviceId parameter so
 that only the roles associated with the given service IDs are returned. See
 https://bugs.launchpad.net/keystone/+bug/890411 for more details.
        </description>

        <atom:link rel="describedby"
                   type="application/pdf"
                   href="https://github.com/openstack/keystone/raw/master/
keystone/content/admin/HP-IDM-admin-devguide.pdf"/>
        <atom:link rel="describedby"
                   type="application/vnd.sun.wadl+xml"
                   href="https://raw.github.com/openstack/keystone/master/
keystone/content/admin/HP-IDM-admin.wadl"/>
</extension>
```


Example 1.4. Extension Query Response: JSON


```
{
  "extension": {
    "name": "HP Token Validation Extension",
    "namespace": "http://docs.openstack.org/identity/api/ext/HP-IDM/v1.0",
    "alias": "HP-IDM",
    "updated": "2011-12-06T19:00:00-00:00",
    "description": "Validate token with the optional HP-IDM-serviceId
 parameter so that only the roles associated with the given service IDs
 are returned. See https://bugs.launchpad.net/keystone/+bug/890411 for more
 details.",
    "links": [
      {
        "rel": "describedby",
```

```
        "type": "application/pdf",
        "href": "https://github.com/openstack/keystone/raw/master/keystone/
content/admin/HP-IDM-admin-devguide.pdf"
      },
      {
        "rel": "describedby",
        "type": "application/vnd.sun.wadl+xml",
        "href": "https://raw.github.com/openstack/keystone/master/keystone/
content/admin/HP-IDM-admin.wadl"
      }
    ]
  }
}
```


1.1. Document Change History

The most recent changes to this document are described below.

Revision Date	Summary of Changes
Dec 21, 2011	• Initial version.

2. Summary of Changes

HP-IDM Admin Extension to Keystone V2.0 API adds capability to filter roles with optional service IDs for token validation to mitigate security risks with role name conflicts. See https://bugs.launchpad.net/keystone/+bug/890411 for more details.

2.1. New Headers

None.

2.2. New Faults

None.

2.3. New Resources

No new resource. HP-IDM Extension merely introduced a new optional HP-IDM-serviceId parameter for the validate token operations. The following APIs are affected.

Verb	URI	Description
Validate Tokens With The New Optional HP-IDM-serviceId Parameter		
GET	`/tokens/{tokenId}`	Check that a token is valid and that it belongs to a supplied tenant and services and return the permissions relevant to a particular client.
HEAD	`/tokens/{tokenId}`	Check that a token is valid and that it belongs to a particular tenant and services (For performance).

2.3.1. Validate Tokens With The New Optional HP-IDM-serviceId Parameter

The following are a list of operations on templates.

Verb	URI	Description
GET	`/tokens/{tokenId}`	Check that a token is valid and that it belongs to a supplied tenant and services and return the permissions relevant to a particular client.
HEAD	`/tokens/{tokenId}`	Check that a token is valid and that it belongs to a particular tenant and services (For performance).

2.3.1.1. Validate Token

Verb	URI	Description
GET	`/tokens/{tokenId}?belongsTo=`*`string`*`&HP-IDM-serviceId=`*`string`*	Check that a token is valid and that it belongs to a supplied tenant and services and return the permissions relevant to a particular client.

Normal Response Code(s): 200, 203

Error Response Code(s): identityFault (400, 500, …), badRequest (400), unauthorized (401), forbidden (403), badMethod (405), overLimit (413), serviceUnavailable (503), itemNotFound (404)

Valid tokens will exist in the `/tokens/{tokenId}` path and invalid tokens will not. In other words, a user should expect an itemNotFound (`404`) fault for an invalid token.

If 'HP-IDM-serviceId' is provided, it must be a comma-separated string of service IDs. If any of the service IDs is invalid or if there are no roles associated with the service IDs, a user should expect a 401.

Table 2.1. Validate Token Request Parameters

Name	Style	Type	Description
`X-Auth-Token`	header	String	You need a valid admin token for access. The `X-Auth-Token` header should always be supplied.
`belongsTo`	query	String	Validates a token has the supplied tenant in scope. The `belongsTo` parameter is optional.
`HP-IDM-serviceId`	query	String	If provided, filter the roles to be returned by the given service IDs. The `HP-IDM-serviceId` parameter is optional.
`tokenId`	template	String	

Example 2.1. Validate Token Response: XML

```
<?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"/>
 <user username="jqsmith">
  <roles xmlns="http://docs.openstack.org/identity/api/v2.0">
   <role xmlns="http://docs.openstack.org/identity/api/v2.0"
    id="Admin" tenantId="one"/>
   <role xmlns="http://docs.openstack.org/identity/api/v2.0"
    id="compute:cloud_admin"/>
  </roles>
 </user>
</auth>
```

Example 2.2. Validate Token Response: JSON

```
{
```

```
  "auth": {
    "token": {
      "expires": "2010-11-01T03:32:15-05:00",
      "id": "ab48a9efdfedb23ty3494"
    },
    "user": {
      "username": "jqsmith",
      "roles": [
        {
          "id": "Admin",
          "tenantId": "one"
        }, {
          "id": "compute:cloud_admin"
        }
      ]
    }
  }
}
```

2.3.1.2. Check Token

Verb	URI	Description
HEAD	`/tokens/{tokenId}?belongsTo=`*`string`*`&HP-IDM-serviceId=`*`string`*	Check that a token is valid and that it belongs to a particular tenant and services (For performance).

Normal Response Code(s): 200, 203

Error Response Code(s): identityFault (400, 500, ...), badRequest (400), unauthorized (401), forbidden (403), badMethod (405), overLimit (413), serviceUnavailable (503), itemNotFound (404)

Valid tokens will exist in the `/tokens/{tokenId}` path and invalid tokens will not. In other words, a user should expect an itemNotFound (`404`) fault for an invalid token.

If `belongsTo` is provided, validates that a token has a specific tenant in scope.

If 'HP-IDM-serviceId' is provided, it must be a comma-separated string of service IDs. If any of the service ID is invalid or if there are no roles associated with the service IDs, a user should expect a 401.

No response body is returned for this method.

Table 2.2. Check Token Request Parameters

Name	Style	Type	Description
`X-Auth-Token`	header	String	You need a valid admin token for access. The `X-Auth-Token` header should always be supplied.
`belongsTo`	query	String	Validates a token has the supplied tenant in scope. (for performance). The `belongsTo` parameter is optional.
`HP-IDM-serviceId`	query	String	Check the roles against the given service IDs. The `HP-IDM-serviceId` parameter is optional.
`tokenId`	template	String	

This operation does not return a response body.

2.4. New Actions

None.

2.5. New States

None.