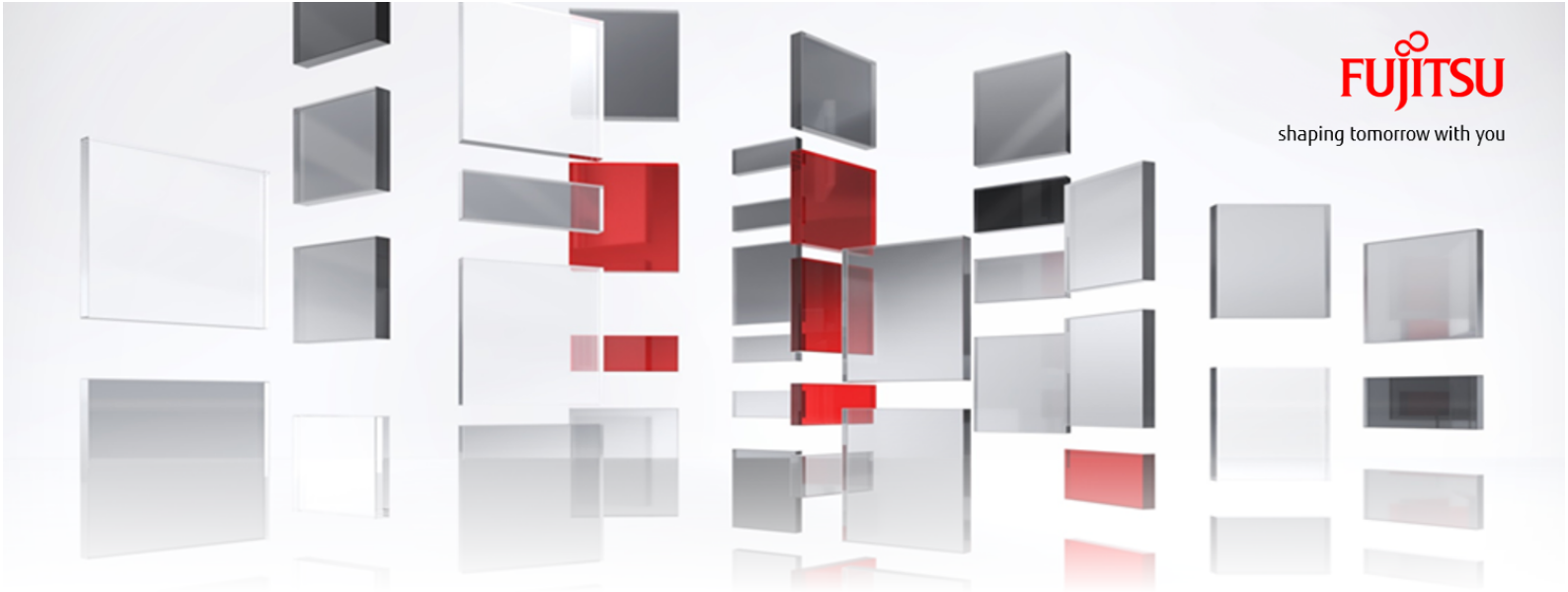

FUJITSU
shaping tomorrow with you

FUJITSU Cloud Service K5 IaaS

API reference (Network)

Version 1.8
FUJITSU LIMITED

K5IA-DC-M-001-001E

Preface

Structure of the manuals

Manual Title	Purposes and Methods of Use
IaaS API Reference • Foundation Service • Network (this document) • Application Platform Service • Management Administration • Contract Management	Detailed reference for using the REST API.
IaaS Features Handbook	Explains the features provided by this service.
IaaS API User Guide	Explains how to use the REST API, how to build the API runtime environment, and sample scripts according to usage sequences, etc.
IaaS Heat Template Specifications	This document explains the format of the Heat Orchestration Template (HOT) that you create in order to use the orchestration function.
IaaS Service Portal User Guide	This document explains how to use the functions provided by this service via Service Portal (Web GUI).
K5 Portal User Guide	This document explains how to use the functions, including registration and user information management, provided by K5 Portal.

Trademarks

- Adobe, the Adobe logo, Acrobat, and Adobe Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.
- Apache and Tomcat are either registered trademarks or trademarks of The Apache Software Foundation in the United States and/or other countries.
- Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- VMware, the VMware logo and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and other countries.
- The OpenStack Word Mark is either a registered trademark/service mark or trademark/service mark of the OpenStack Foundation, in the United States and other countries and is used with the OpenStack Foundation's permission.
- Oracle and Java are registered trademarks of Oracle and/or its affiliates.
- Red Hat is a registered trademark of Red Hat, Inc. in the U.S. and other countries.
- UNIX is a registered trademark of The Open Group.

Note that trademark symbols (™ or ®) are not appended to system names or product names used in this document.

Export restrictions

Exportation/release of this document may require necessary procedures in accordance with the regulations of your resident country and/or US export control laws.

Notice

- Information in this document may be subject to change without prior notice.
- No part of the content of this document may be reproduced without the written permission of Fujitsu Limited.
- Information in this document is the latest information as of the date of revision.
- Fujitsu assumes no responsibility for infringement of any patent rights or other rights of third parties arising from the use of information in this document.

Revision History

Edition	Date of Update	Location	Overview
1.6	July 1, 2016	*Common Parameters* on page 158	Description modified
		LoadBalancerAttributes on page 164	Description modified
		CreateLoadBalancerListeners on page 181	Description modified
1.7	July 29, 2016	*API list* on page 155	Description modified
		Create/delete record (POST v1.0/hostedzone/{zoneId}/rrset) on page 238	Description modified
1.8	November 4, 2016	*API list* on page 155	Description modified
		PolicyAttribute on page 167	Article added
		PolicyAttributeDescription on page 168	Article added
		PolicyDescription on page 168	Article added
		CreateLBCookieStickinessPolicy on page 176	Description modified
		CreateLoadBalancer on page 178	Description modified
		CreateLoadBalancerPolicy on page 182	Article added
		CreateSorryServerRedirectionPolicy on page 185	Description modified
		DeleteLoadBalancerPolicy on page 189	Article added
		DescribeLoadBalancerPolicies on page 195	Article added
		DescribeLoadBalancers on page 197	Description modified
		SetLoadBalancerPoliciesOfListener on page 209	Description modified

Contents

Part 1: Network

Topics:

1.1 Global IP delivery service

1.1.1 API list

Layer-3 networking (floatingips)

Item	API	Description
1	GET /v2.0/floatingips List floating IPs	Lists floating IPs.
2	POST /v2.0/floatingips Create floating IP	Creates a floating IP. When port information is specified, associates the floating IP with the specified port.
3	GET /v2.0/floatingips/{floatingip_id} Show floating IP details	Shows details of the specified floating IP.
4	PUT /v2.0/floatingips/{floatingip_id} Update floating IP	Updates the specified floating IP and its association with an internal port.
5	DELETE /v2.0/floatingips/{floatingip_id} Delete floating IP	Deletes a floating IP and, if present, its associated port.

subnets

Item	API	Description
1	GET /v2.0/subnets List subnets	Lists subnets to which the specified tenant has access.
2	POST /v2.0/subnets Create subnet	Creates a subnet on the specified network
3	GET /v2.0/subnets/{subnet_id} Show subnet	Shows information on the specified subnet.
4	PUT /v2.0/subnets/{subnet_id} Update subnet	Updates the specified subnet.
5	DELETE /v2.0/subnets/{subnet_id} Delete subnet	Deletes the specified subnet.

1.1.2 General requirements

This section describes general requirements to use this API.

- Specify the name and description input parameters using up to 255 characters.

- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.
- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.1.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.1.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType

Caution

- If the user has insufficient privileges to issue the target API when issuing the API for showing (Show), updating (Update), or deleting (Delete) resources, the status code 404 may be returned.
- If the user has insufficient privileges to issue the target API when issuing the API for listing (List) resources, the status code 200 will be returned and a null array will be set in the body. If there are resources with the shared attribute set to "True", information on the target resources only will be returned.

1.1.5 API options

1.1.5.1 API options

Two options are available for APIs that retrieve resource information (List, Show).

1.1.5.2 filter

Filters can be specified to retrieve only resources matching the specified attributes from the list of resource information to be retrieved.

Multiple attributes can be specified using AND as a condition.

This option can only be used for the List API.

Execution example:

- Retrieve the network with the name "private"

  GET /v2.0/networks?name=private
- To filter using multiple attributes with AND. Retrieve the network with the name "private" and that belongs to the AZ1 availability zone.

  GET /v2.0/networks?name=private?availability_zone=AZ1

1.1.5.3 Column Selection

The attributes that are retrieved from the resource information can be restricted.

This option can only be used for the List and Show APIs.

Execution example:

- List only the id attribute of networks

  GET /v2.0/networks?fields=id
- To retrieve multiple attributes (id and name)

  GET /v2.0/networks?fields=id&fields=name

1.1.5.4 APIs that do not support these options

These options are not supported by the following APIs.

- *Show Network Connector Pool* on page 31
- *List Network Connector Pools* on page 32
- *Show Network Connector* on page 35
- *List Network Connectors* on page 36

- *Show Network Connector Endpoint* on page 43
- *List Network Connector Endpoints* on page 44
- *List Connected Interfaces of Network Connector Endpoint* on page 50

1.1.6 API details

1.1.6.1 List floating IPs

Lists floating IPs that are accessible to the tenant who submits the request.

URI

/v2.0/floatingips

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "floatingips": [
        {
            "router_id": "d23abc8d-2991-4a55-ba98-2aaea84cc72f",
            "tenant_id": "4969c491a3c74ee4af974e6d800c62de",
            "floating_network_id": "376da547-b977-4cfe-9cba-275c80debf57",
            "fixed_ip_address": "10.0.0.3",
            "floating_ip_address": "172.24.4.228",
            "port_id": "ce705c24-c1ef-408a-bda3-7bbd946164ab",
            "id": "2f245a7b-796b-4f26-9cf9-9e82d248fda7",
            "status": "ACTIVE",
            "availability_zone": "AZ1"
        },
        {
            "router_id": null,
            "tenant_id": "4969c491a3c74ee4af974e6d800c62de",
            "floating_network_id": "376da547-b977-4cfe-9cba-275c80debf57",
            "fixed_ip_address": null,
            "floating_ip_address": "172.24.4.227",
            "port_id": null,
            "id": "61cea855-49cb-4846-997d-801b70c71bdd",
            "status": "DOWN",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
floatingip	A floatingip object.
tenant_id	The tenant ID.
router_id	The router ID.
status	The floatingip status.
floating_network_id	The ID of the network associated with the floating IP.
fixed_ip_address	The fixed IP address associated with the floating IP.
floating_ip_address	The floating IP address.
port_id	The port ID.
id	The floating IP ID.
availability_zone	The Availability Zone name.

1.1.6.2 Create floating IP

Creates a floating IP, and, if you specify port information, associates the floating IP with an internal port.

URI

/v2.0/floatingips

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
floatingip	A floatingip object.	xsd:string	Required
tenant_id	The tenant ID.	xsd:string	Optional
floating_network_id	The ID of the network associated with the floating IP.	csapi:uuid	Required
fixed_ip_address	The fixed IP address associated with the floating IP.	xsd:string	Optional
port_id	The port ID.	csapi:uuid	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
    "floatingip": {
```

```
        "floating_network_id": "376da547-b977-4cfe-9cba-275c80debf57",
        "port_id": "ce705c24-c1ef-408a-bda3-7bbd946164ab",
        "availability_zone": "AZ1"
    },
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "floatingip": {
        "router_id": "d23abc8d-2991-4a55-ba98-2aaea84cc72f",
        "status": "DOWN",
        "tenant_id": "4969c491a3c74ee4af974e6d800c62de",
        "floating_network_id": "376da547-b977-4cfe-9cba-275c80debf57",
        "fixed_ip_address": "10.0.0.3",
        "floating_ip_address": "172.24.4.228",
        "port_id": "ce705c24-c1ef-408a-bda3-7bbd946164ab",
        "id": "2f245a7b-796b-4f26-9cf9-9e82d248fda7",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
floatingip	A floatingip object.
router_id	The router ID.
status	The floatingip status.
tenant_id	The tenant ID.
floating_network_id	The ID of the network associated with the floating IP.
fixed_ip_address	The fixed IP address associated with the floating IP.
floating_ip_address	The floating IP address.
port_id	The port ID.
id	The floating IP ID.
availability_zone	The Availability Zone name.

1.1.6.3 Show floating IP details

Shows details for a specified floating IP.

URI

/v2.0/floatingips/{floatingip_id}

Description of the URI:

{floatingip_id} UUID The UUID of the floating IP.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "floatingip": {
        "fixed_ip_address": "10.0.0.3",
        "floating_ip_address": "172.24.4.228",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
floatingip	A floatingip object.
tenant_id	The tenant ID.
router_id	The router ID.
status	The floatingip status.
floating_network_id	The ID of the network associated with the floating IP.
fixed_ip_address	The fixed IP address associated with the floating IP.
floating_ip_address	The floating IP address.
port_id	The port ID.
id	The floating IP ID.
availability_zone	The Availability Zone name.

1.1.6.4 Update floating IP

Updates a floating IP and its association with an internal port.

URI

/v2.0/floatingips/{floatingip_id}

Description of the URI:

{floatingip_id} UUID The UUID of the floating IP.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
port_id	The port ID.	csapi:uuid	Required
fixed_ip_address	The fixed IP address associated with the floating IP.	xsd:string	Optional

Example request

```
{
    "floatingip": {
        "port_id": "fc861431-0e6c-4842-a0ed-e2363f9bc3a8"
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes Confirm the following two points when floating IP exists. Caution1. Subnet that the specified port belongs must be attached to router. 2. External network must be attached to same router described in 1.
conflict (409)	Error response codes

Response body (normal status)

```
{
    "floatingip": {
        "router_id": "d23abc8d-2991-4a55-ba98-2aaea84cc72f",
        "tenant_id": "4969c491a3c74ee4af974e6d800c62de",
        "floating_network_id": "376da547-b977-4cfe-9cba-275c80debf57",
        "fixed_ip_address": "10.0.0.4",
```

```
        "floating_ip_address": "172.24.4.228",
        "port_id": "fc861431-0e6c-4842-a0ed-e2363f9bc3a8",
        "id": "2f245a7b-796b-4f26-9cf9-9e82d248fda7",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
floatingip	A floatingip object.
tenant_id	The tenant ID.
router_id	The router ID.
status	The floatingip status.
floating_network_id	The ID of the network associated with the floating IP.
fixed_ip_address	The fixed IP address associated with the floating IP.
floating_ip_address	The floating IP address.
port_id	The port ID.
id	The floating IP ID.
availability_zone	The Availability Zone name.

1.1.6.5 Delete floating IP

Deletes a floating IP.

URI

/v2.0/floatingips/{floatingip_id}

Description of the URI:

{floatingip_id} UUID The UUID of the floating IP.

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

1.1.6.6 List subnets

Lists subnets to which the specified tenant has access.

URI

/v2.0/subnets

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)


```
{
    "subnets": [
        {
            "name": "private-subnet",
            "enable_dhcp": true,
            "network_id": "db193ab3-96e3-4cb3-8fc5-05f4296d0324",
            "tenant_id": "26a7980765d0414dbc1fc1f88cdb7e6e",
            "dns_nameservers": [],
            "allocation_pools": [
                {
                    "start": "10.0.0.2",
                    "end": "10.0.0.254"
                }
            ],
            "host_routes": [],
            "ip_version": 4,
            "gateway_ip": "10.0.0.1",
            "cidr": "10.0.0.0/24",
            "id": "08eae331-0402-425a-923c-34f7cfe39c1b",
            "availability_zone": "AZ1"
        },
        {
            "name": "my_subnet",
            "enable_dhcp": true,
            "network_id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
            "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
            "dns_nameservers": [],
            "allocation_pools": [
                {
                    "start": "192.0.0.2",
                    "end": "192.255.255.254"
                }
            ],
            "host_routes": [],
            "ip_version": 4,
            "gateway_ip": "192.0.0.1",
            "cidr": "192.0.0.0/8",
            "id": "54d6f61d-db07-451c-9ab3-b9609b6b6f0b",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
name	The subnet name.
enable_dhcp	Set to true if DHCP is enabled and false if DHCP is disabled.
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
dns_nameservers	A list of DNS name servers for the subnet. For example ["8.8.8.7", "8.8.8.8"]. specified IP addresses are displayed in sorted order in ascending order. lowest IP address will be primary DNS address.
allocation_pools	The start and end addresses for the allocation pools.
host_routes	A list of host route dictionaries for the subnet. For example: `"host_routes":[ { "destination":"0.0.0.0/0", "nexthop":"172.16.1.254" }, { "destination":"192.168.0.0/24", "nexthop":"192.168.0.1" } ]`
ip_version	The IP version, which is 4.
gateway_ip	The gateway IP address.
cidr	The CIDR.
id	The ID of the subnet.
availability_zone	The Availability Zone name.

1.1.6.7 Create subnet

Creates a subnet on the specified network.

URI

/v2.0/subnets

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
name	The subnet name.	xsd:string	Optional

Key	Description	Type	Required/ optional
network_id	The ID of the attached network.	csapi:uuid	required
allocation_pools	The start and end addresses for the allocation pools.	xsd:dict	Optional
dns_nameservers	A list of DNS name servers for the subnet. Specify each name server as an IP address enclosed by double quotation marks and separate multiple entries with commas. For example ["8.8.8.7", "8.8.8.8"]. Specify the IP addresses in ascending order. The lowest IP address will be primary DNS address.	xsd:string	Optional
host_routes	A list of host route dictionaries for the subnet. For example: `"host_routes":[ { "destination":"0.0.0.0/0", "nexthop":"172.16.1.254" }, { "destination":"192.168.0.0/24", "nexthop":"192.168.0.1" } ]`	xsd:list	Optional
gateway_ip	The gateway IP address.	xsd:string	Optional
ip_version	The IP version, which can be 4 or 6.	xsd:string	Required
cidr	The CIDR.	xsd:bool	required
enable_dhcp	Set to "true" if DHCP is enabled, or "false" otherwise.	xsd:boolean	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Caution

- Do not specify an ISP shared address (100.64.0.0/10 or a subnet address of that subnet when divided).
- One subnet is associated with one network.

Caution

Note the following when creating a subnet that uses the Windows virtual server for SAP service or physical server for SAP HANA service.

- Create a subnet with the following string assigned to the beginning of the name parameter.

Windows virtual server for SAP service: fcx_subnet-w:

Physical server for SAP HANA service: fcx_subnet-b:

- The mask value that you can specify using CIDR is 16 to 29.
- Other than the IP address specified for allocation_pools and gateway_ip, is the IP address assigned to the server (VM) that was created using the Windows virtual server for SAP service or physical server for SAP HANA service.

  For allocation_pools, specify an IP address outside of the IP address range used by the Windows virtual server for SAP service or physical server for SAP HANA service.
- For ip_version, specify 4.
- The information specified for host_routes, enable_dhcp, and dns_nameservers is not set for the server (VM) created using the Windows virtual server for SAP service or physical server for SAP HANA service.

Example request

```
{
    "subnet": {
        "network_id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
        "ip_version": 4,
        "cidr": "192.168.199.0/24",
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "subnet": {
        "name": "",
        "enable_dhcp": true,
        "network_id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
        "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
        "dns_nameservers": [],
        "allocation_pools": [
            {
                "start": "192.168.199.2",
                "end": "192.168.199.254"
            }
        ],
        "host_routes": [],
        "ip_version": 4,
```

```
        "gateway_ip": "192.168.199.1",
        "cidr": "192.168.199.0/24",
        "id": "3b80198d-4f7b-4f77-9ef5-774d54e17126",
        "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
name	The subnet name.
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
dns_nameservers	A list of DNS name servers for the subnet. Specify each name server as an IP address enclosed by double quotation marks and separate multiple entries with commas. For example ["8.8.8.7", "8.8.8.8"].
allocation_pools	The start and end addresses for the allocation pools.
host_routes	A list of host route dictionaries for the subnet. For example: `"host_routes":[ { "destination":"0.0.0.0/0", "nexthop":"172.16.1.254" }, { "destination":"192.168.0.0/24", "nexthop":"192.168.0.1" } ]`
gateway_ip	The gateway IP address.
ip_version	The IP version, which is 4.
cidr	The CIDR.
id	The ID of the subnet.
enable_dhcp	Set to true if DHCP is enabled and false if DHCP is disabled.
availability_zone	The Availability Zone name.

1.1.6.8 Show subnet

Shows information for a specified subnet.

URI

/v2.0/subnets/{subnet_id}

Description of the URI:

{subnet_id} UUID The UUID for the subnet of interest to you.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "subnet": {
        "name": "my_subnet",
        "enable_dhcp": true,
        "network_id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
        "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
        "dns_nameservers": [],
        "allocation_pools": [
            {
                "start": "192.0.0.2",
                "end": "192.255.255.254"
            }
        ],
        "host_routes": [],
        "ip_version": 4,
        "gateway_ip": "192.0.0.1",
        "cidr": "192.0.0.0/8",
        "id": "54d6f61d-db07-451c-9ab3-b9609b6b6f0b",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
name	The subnet name.
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
dns_nameservers	A list of DNS name servers for the subnet. Specify each name server as an IP address enclosed by double quotation marks and separate multiple entries with commas. For example ["8.8.8.7", "8.8.8.8"]. specified IP addresses are displayed in sorted order in ascending order. lowest IP address will be primary DNS address.
allocation_pools	The start and end addresses for the allocation pools.
host_routes	A list of host route dictionaries for the subnet. For example: `"host_routes":[`

Item	Description

	<pre>{
	"destination":"0.0.0.0/0",
	"nexthop":"172.16.1.254"
	},
	{
	"destination":"192.168.0.0/24",
	"nexthop":"192.168.0.1"
	}
	]</pre>

gateway_ip	The gateway IP address.
ip_version	The IP version, which is 4 or 6.
cidr	The CIDR.
id	The ID of the subnet.
enable_dhcp	Set to true if DHCP is enabled and false if DHCP is disabled.
availability_zone	The Availability Zone name.

1.1.6.9 Update subnet

Updates the specified subnet.

URI

/v2.0/subnets/{subnet_id}

Description of the URI:

{subnet_id}: The UUID of the subnet.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/ optional
name	The subnet name.	xsd:string	Optional
gateway_ip	The gateway IP address.	xsd:string	Optional
enable_dhcp	Set to true if DHCP is enabled and false if DHCP is disabled.	xsd:boolean	Optional
dns_nameservers	A list of DNS name servers for the subnet. Specify each name server as an IP address enclosed by double quotation marks and separate multiple entries with commas. For example ["8.8.8.7", "8.8.8.8"].	xsd:string	Optional
host_routes	A list of host route dictionaries for the subnet. For example: <pre>"host_routes":[</pre>	xsd:list	Optional

Key	Description	Type	Required/ optional

	<pre>{
	"destination":"0.0.0.0/0",
	"nexthop":"172.16.1.254"
	},
	{
	"destination":"192.168.0.0/24",
	"nexthop":"192.168.0.1"
	}
	]</pre>		

Caution Note the following when updating a subnet that uses the Windows virtual server for SAP service or physical server for SAP HANA service.

- The "fcx_subnet-w:" or "fcx_subnet-b:" string at the beginning of the name parameter cannot be changed.
- gateway_ip cannot be changed.
- The information specified for host_routes, enable_dhcp, and dns_nameservers is not set for the server (VM) created using the Windows virtual server for SAP service or physical server for SAP HANA service.

Example request

```
{
    "subnet": {
        "name": "my_subnet"
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "subnet": {
        "name": "private-subnet",
        "enable_dhcp": true,
        "network_id": "db193ab3-96e3-4cb3-8fc5-05f4296d0324",
        "tenant_id": "26a7980765d0414dbc1fc1f88cdb7e6e",
        "dns_nameservers": [],
        "allocation_pools": [
            {
                "start": "10.0.0.2",
                "end": "10.0.0.254"
```

```
            }
        ],
        "host_routes": [],
        "ip_version": 4,
        "gateway_ip": "10.0.0.1",
        "cidr": "10.0.0.0/24",
        "id": "08eae331-0402-425a-923c-34f7cfe39c1b",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
name	The subnet name.
enable_dhcp	Set to true if DHCP is enabled and false if DHCP is disabled.
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
dns_nameservers	A list of DNS name servers for the subnet. Specify each name server as an IP address enclosed by double quotation marks and separate multiple entries with commas. For example ["8.8.8.7", "8.8.8.8"].
allocation_pools	The start and end addresses for the allocation pools.
host_routes	A list of host route dictionaries for the subnet. For example: `"host_routes":[ { "destination":"0.0.0.0/0", "nexthop":"172.16.1.254" }, { "destination":"192.168.0.0/24", "nexthop":"192.168.0.1" } ]`
ip_version	The IP version, which is 4 or 6.
gateway_ip	The gateway IP address.
cidr	The CIDR.
id	The ID of the subnet.
availability_zone	The Availability Zone name.

1.1.6.10 Delete subnet

Deletes the specified subnet.

URI

/v2.0/subnets/{subnet_id}

Description of the URI:

{subnet_id} UUID The UUID for the subnet of interest to you.

HTTP method

DELETE

Request parameter


Caution When a subnet is deleted, DHCP can no longer be used in the network where it was it was created. If using DHCP, the subnet alone cannot be deleted- the network must be deleted as well.


Caution Before deleting a subnet that uses the Windows virtual server for SAP service or physical server for SAP HANA service, it is necessary to delete the network resources using it.

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

1.2 Private network service

1.2.1 API list

networks

Item	API	Description
1	GET /v2.0/networks List networks	Lists networks to which the tenant has access
2	POST /v2.0/networks Create network	Creates a network
3	GET /v2.0/networks/{network_id} Show network	Shows details of the specified network
4	PUT /v2.0/networks/{network_id} Update network	Updates the specified network
5	DELETE /v2.0/networks/{network_id} Delete network	Deletes the specified network and its associated resources

Network Connector

Item	API	Description
1	GET /v2.0/network_connector_pools/{network_connector_pool_id} Show network connector pool	Shows the specified network connector pool
2	GET /v2.0/network_connector_pools List network connector pools	Lists network connector pools
3	POST /v2.0/network_connectors Create Network Connector	Creates a network connector
4	GET /v2.0/network_connectors/{network_connector_id} Show network connector	Shows information about the specified network connector
5	GET /v2.0/network_connectors List Network Connectors	Lists network connectors
6	PUT /v2.0/network_connectors/{network connector id} Update Network Connector	Updates the specified network connector
7	DELETE /v2.0/network_connector/{network connector id}	Deletes the specified network connector

Item	API	Description
	Deletes Network Connector	
8	POST /v2.0/network_connector_endpoints Create Network Connector Endpoint	Creates a network connector endpoint
9	GET /v2.0/network_connector_endpoints/{network_connector_endpoint_id} Show Network Connector Endpoint	Shows information about the specified network connector endpoint
10	GET /v2.0/network_connector_endpoints List Network Connector Endpoints	Lists network connector endpoints
11	PUT /v2.0/network_connector_endpoints/{network connector endpoint id} Update Network Connector Endpoint	Updates the specified network connector endpoint
12	DELETE /v2.0/network_connector_endpoints/{network connector endpoint id} Deletes Network Connector Endpoint	Deletes the specified network connector endpoint
13	PUT /v2.0/network_connector_endpoints/{network connector endpoint id}/connect Connect Network Connector Endpoint	Connects interface to the specified network connector endpoint
14	PUT /v2.0/network_connector_endpoints/{network connector endpoint id}/disconnect Disconnect Network Connector Endpoint	Disconnects interface from the specified network connector endpoint
15	GET /v2.0/network_connector_endpoints/{network connector endpoint id}/interfaces List Connected Interfaces of Network Connector Endpoint	Lists the interfaces connected to the specified network connector endpoint

1.2.2 General requirements

This section describes general requirements to use this API.

- Specify the name and description input parameters using up to 255 characters.
- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.
- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.2.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.2.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType


Caution

- If the user has insufficient privileges to issue the target API when issuing the API for showing (Show), updating (Update), or deleting (Delete) resources, the status code 404 may be returned.
- If the user has insufficient privileges to issue the target API when issuing the retrieve resource list (List) API, the status code 200 may be returned. If this happen, a null

array will be returned in the body section. Also, if there are resources with the shared attribute set to "True", information on the target resources only will be returned.

1.2.5 API options

1.2.5.1 API options

Two options are available for APIs that retrieve resource information (List, Show).

1.2.5.2 filter

Filters can be specified to retrieve only resources matching the specified attributes from the list of resource information to be retrieved.

Multiple attributes can be specified using AND as a condition.

This option can only be used for the List API.

Execution example:

- Retrieve the network with the name "private"

  GET /v2.0/networks?name=private
- To filter using multiple attributes with AND. Retrieve the network with the name "private" and that belongs to the AZ1 availability zone.

  GET /v2.0/networks?name=private?availability_zone=AZ1

1.2.5.3 Column Selection

The attributes that are retrieved from the resource information can be restricted.

This option can only be used for the List and Show APIs.

Execution example:

- List only the id attribute of networks

  GET /v2.0/networks?fields=id
- To retrieve multiple attributes (id and name)

  GET /v2.0/networks?fields=id&fields=name

1.2.5.4 APIs that do not support these options

These options are not supported by the following APIs.

- *Show Network Connector Pool* on page 31
- *List Network Connector Pools* on page 32
- *Show Network Connector* on page 35
- *List Network Connectors* on page 36
- *Show Network Connector Endpoint* on page 43
- *List Network Connector Endpoints* on page 44
- *List Connected Interfaces of Network Connector Endpoint* on page 50

1.2.6 API details

1.2.6.1 List networks

Lists networks to which the specified tenant has access.

URI

/v2.0/networks

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)


```
{
    "networks": [
        {
            "status": "ACTIVE",
            "subnets": [
                "54d6f61d-db07-451c-9ab3-b9609b6b6f0b"
            ],
            "name": "private-network",
            "admin_state_up": true,
            "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
            "router:external": true,
            "shared": true,
            "id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
            "availability_zone": "AZ1"
        },
        {
            "status": "ACTIVE",
            "subnets": [
                "08eae331-0402-425a-923c-34f7cfe39c1b"
            ],
            "name": "private",
            "admin_state_up": true,
            "tenant_id": "26a7980765d0414dbc1fc1f88cdb7e6e",
            "router:external": true,
            "shared": true,
            "id": "db193ab3-96e3-4cb3-8fc5-05f4296d0324",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
admin_state_up	The administrative state of the network, which is up (true) or down (false).
id	The network ID.
name	The network name.
shared	Indicates whether this network is shared across all tenants.
status	The network status.
subnets	The associated subnets.
tenant_id	The tenant ID.
router:external	Specifies whether the network is an external network or not.
availability_zone	The Availability Zone name

1.2.6.2 Create network

Creates a network.

URI

/v2.0/networks

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
admin_state_up	The administrative state of the network, which is up (true) or down (false).	xsd:bool	Optional
name	The network name. A request body is optional: If you include it, it can specify this optional attribute.	xsd:string	Optional
shared	Indicates whether this network is shared across all tenants. By default, only administrative users can change this value.	xsd:bool	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
 "network": {
```

```
  "name": "sample_network",
  "admin_state_up": true,
  "availability_zone": "AZ1"
 }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "network": {
        "status": "ACTIVE",
        "subnets": [],
        "name": "net1",
        "admin_state_up": true,
        "tenant_id": "9bacb3c5d39d41a79512987f338cf177",
        "segments": [
            {
                "provider:segmentation_id": 2,
                "provider:physical_network": "8bab8453-1bc9-45af-8c70-
f83aa9b50453",
                "provider:network_type": "vlan"
            },
            {
                "provider:segmentation_id": null,
                "provider:physical_network": "8bab8453-1bc9-45af-8c70-
f83aa9b50453",
                "provider:network_type": "stt"
            }
        ],
        "shared": false,
        "port_security_enabled": true,
        "id": "4e8e5957-649f-477b-9e5b-f1f75b21c03c",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
admin_state_up	The administrative state of the network, which is up (true) or down (false).
id	The network ID.
name	The network name.
shared	Indicates whether this network is shared across all tenants.
status	The network status.
subnets	The associated subnets.

Item	Description
tenant_id	The tenant ID.
availability_zone	The Availability Zone name

1.2.6.3 Show network

Shows information for a specified network.

URI

/v2.0/networks/{network_id}

Description of the URI:

{network_id} UUID The UUID for the network of interest to you.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "network": {
        "status": "ACTIVE",
        "subnets": [
            "54d6f61d-db07-451c-9ab3-b9609b6b6f0b"
        ],
        "name": "private-network",
        "admin_state_up": true,
        "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
        "router:external": true,
        "shared": true,
        "id": "d32019d3-bc6e-4319-9c1d-6722fc136a22",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
admin_state_up	The administrative state of the network, which is up (true) or down (false).
id	The network ID.
name	The network name.

Item	Description
shared	Indicates whether this network is shared across all tenants.
status	The network status.
subnets	The associated subnets.
tenant_id	The tenant ID.
availability_zone	The Availability Zone name
router:external	Specifies whether the network is an external network or not.

1.2.6.4 Update network

Updates a specified network.

URI

/v2.0/networks/{network_id}

Description of the URI:

{network_id} UUID The UUID for the network of interest to you.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
admin_state_up	The administrative state of the network, which is up (true) or down (false).	xsd:bool	Optional
name	The network name.	xsd:string	Optional

Example request

```
{
    "network": {
        "name": "sample_network_5_updated"
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "network": {
        "status": "ACTIVE",
        "subnets": [],
        "name": "sample_network_5_updated",
        "admin_state_up": true,
        "tenant_id": "4fd44f30292945e481c7b8a0c8908869",
        "router:external": false,
        "shared": false,
        "id": "1f370095-98f6-4079-be64-6d3d4a6adcc6",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
status	The network status.
subnets	The associated subnets.
name	The network name.
admin_state_up	The administrative state of the network, which is up (true) or down (false).
tenant_id	The tenant ID.
router:external	Specifies whether the network is an external network or not.
shared	Indicates whether this network is shared across all tenants. By default, only administrative users can change this value.
id	The network ID.
provider:segmentation_id	
availability_zone	The Availability Zone name

1.2.6.5 Delete network

Deletes the specified network and its associated resources.

URI

/v2.0/networks/{network_id}

Description of the URI:

{network_id} UUID The UUID for the network of interest to you.

HTTP method

DELETE

Request parameter

Caution Before deleting a network that is specified for subnets that use the Windows virtual server for SAP service or physical server for SAP HANA service, it is necessary to delete the network resources using the subnet.

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

1.2.6.6 Show Network Connector Pool

Shows a specified network connector pool.

Request

URI

GET <network service endpoint>/v2.0/network_connector_pools/<network connector pool id>

Example:

GET http://192.168.122.1:9696/v2.0/network_connector_pools/78380271-954a-4c1a-a76d-43033c7fc9bf

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

```
{
 "network_connector_pool" : {
  "id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "name" : "mpls-vpn-pool1"
 }
}
```

Body Elements

- id:

  id for this network connector pool

  - Type: String
- name:

  name for network connector pool

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.
- 404: Specified Network Connector Pool not found

1.2.6.7 List Network Connector Pools

Lists network connector pools.

Request

URI

GET <network service endpoint>/v2.0/network_connector_pools

Example:

GET http://192.168.122.1:9696/v2.0/network_connector_pools/78380271-954a-4c1a-a76d-43033c7fc9bf

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

```
{
 "network_connector_pools" : [
  {
   "id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
   "name" : "mpls-vpn-pool1",
  },
  {
   "id" : "ddd0271-954a-4c1a-a76d-43033c7fc9bf",
   "name" : "mpls-vpn-pool2"
```

```
    }
  ]
}
```

Elements

- id:

  id for this network connector pool

  - Type: String
- name:

  name for network connector pool

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.

1.2.6.8 Create Network Connector

Creates a network connector.

Request

URI

POST <network service endpoint>/v2.0/network_connectors

Example:

POST http://192.168.122.1:9696/v2.0/network_connectors

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "network_connector" : {
  "name" : "connector1",
  "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Parameters

- name:

  name for network connector

  - Type: String

  - Constraints: Up to 255 characters in length
  - Constraints: a-z, A-Z, 0-9, and _-
  - Required: Yes
- network_connector_pool_id:

  A network connector pool id for this network connector. When this value not specified and only one pool exists, use it.
  - Type: String
  - Required: No
- tenant_id:

  The tenant's ID to which this network connector belongs.

  This parameter is restricted for tenant in which requester joins.
  - Type: String
  - Required: No

Response

Status code

- 201

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector" : {
  "id" : "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "name" : "connector1",
  "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "network_connector_endpoints" : [],
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Elements

- id:

  ID for this network connector
  - Type: String
- name:

  name for network connector
  - Type: String
- network_connector_pool_id:

  A network connector pool id for this network connector.
  - Type: String
- network_connector_endpoints:

ID of network connector endpoints belonging to this network connector. Immediate after creation, this value must be empty array.

  - Type: Array of String
- tenant_id:

  tenant's ID to which this network connector belongs

  - Type: String

Errors

- 400: Invalid parameter in request body
- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.
- 404: Network Connector Pool not found.
- 409: Operation conflicts with another one.
- 503: No resource remains in the network connector pool

1.2.6.9 Show Network Connector

Shows information for a specified network connector.

Request

URI

GET <network service endpoint>/v2.0/network_connectors/<network connector id>

Example:

GET http://192.168.122.1:9696/v2.0/network_connectors/07993b1c-79e1-4cf6-a663-dc42b9ce37d4

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

```
{
 "network_connector" : {
  "id" : "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "name" : "connector1",
  "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "network_connector_endpoints" : [
```

```
   "0e521ed5-62d0-44c9-9c04-2e880b5add21"
  ],
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Elements

- id:

  ID for this network connector

  - Type: String
- name:

  name for network connector

  - Type: String
- network_connector_pool_id:

  A network connector pool id for this network connector.

  - Type: String
- network_connector_endpoints:

  ID of network connector endpoints belonging to this network connector. Immediate after creation, this value must be empty array.

  - Type: Array of String
- tenant_id:

  tenant's ID to which this network connector belongs

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.
- 404: Specified network connector not found

1.2.6.10 List Network Connectors

Lists network connectors.

Request

URI

GET <network service endpoint>/v2.0/network_connectors

Example:

GET http://192.168.122.1:9696/v2.0/network_connectors

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200 (OK)

Headers

- Content-Type: application/json

Body

```
{
 "network_connectors" : [
  {
   "id" : "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
   "name" : "connector1",
   "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
   "network_connector_endpoints" : [
    "0e521ed5-62d0-44c9-9c04-2e880b5add21"
   ],
   "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
  },
  {
  "id" : "ddecde23-fbf7-460d-b895-6f190b1890ec",
  "name" : "connector1",
  "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "network_connector_endpoints" : [
   "d001c289-e7ba-4db9-90d8-ee70785852b4"
  ],
  "tenant_id" : "d827860a-f3dc-4c65-9e22-78142582a12c"
  }
 ]
}
```

Elements

- id:

  ID for this network connector

  - Type: String
- name:

  name for network connector

  - Type: String
- network_connector_pool_id:

  A network connector pool id for this network connector.

  - Type: String
- network_connector_endpoints:

  ID of network connector endpoints belonging to this network connector. Immediate after creation, this value must be empty array.

  - Type: Array of String
- tenant_id:

  tenant's ID to which this network connector belongs

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.

1.2.6.11 Update Network Connector

Updates a specified network connector.

Request

URI

PUT <network service endpoint>/v2.0/network_connectors/<network connector id>

Example:

PUT http://192.168.122.1:9696/v2.0/network_connectors/07993b1c-79e1-4cf6-a663-dc42b9ce37d4

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "network_connector" : {
  "name" : "connector2"
 }
}
```

Request parameters

Update only specified parameter.

- name:

  name for network connector

  - Type: String
  - Constraints: Up to 255 characters in length
  - Constraints: a-z, A-Z, 0-9, and _-

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector" : {
  "id" : "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "name" : "connector2",
  "network_connector_pool_id" : "78380271-954a-4c1a-a76d-43033c7fc9bf",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03",
  "network_connector_endpoints" : [
   "0e521ed5-62d0-44c9-9c04-2e880b5add21"
  ]
 }
}
```

Elements

- id:

  ID for this network connector

  - Type: String
- name:

  name for network connector

  - Type: String
- network_connector_pool_id:

  A network connector pool id for this network connector.

  - Type: String
- network_connector_endpoints:

  ID of network connector endpoints belonging to this network connector. Immediate after creation, this value must be empty array.

  - Type: Array of String
- tenant_id:

  tenant's ID to which this network connector belongs

  - Type: String

Errors

- 400:
  - Invalid parameter in request body
  - Not updatable parameter is specified in request body
- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate
- 404: Specified network connector not found

1.2.6.12 Deletes Network Connector

Deletes a specified network connector.

Request

URI

DELETE <network service endpoint>/v2.0/network_connector/<network connector id>

Example:

DELETE http://192.168.122.1:9696/v2.0/network_connectors/07993b1c-79e1-4cf6-a663-dc42b9ce37d4

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 204

Headers

- Content-Type: text/plain

Errors

- 401: Token is not specified or not authorized
- 403: Token is not permitted to operate
- 404: Specified network connector not found
- 409:
  - Specified network connector in use.
  - Operation conflicts with another one.

1.2.6.13 Create Network Connector Endpoint

Creates a network connector endpoint.

Request

URI

POST <network service endpoint>/v2.0/network_connector_endpoints

Example:

POST http://192.168.122.1:9696/v2.0/network_connector_endpoints

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "network_connector_endpoint" : {
  "name": "endponit_for_az1",
  "network_connector_id": "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "endpoint_type": "availability_zone",
  "location" : "east-jp-az1",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Request parameters

- name:

  Name for this network connector endpoint.

  - Type: String
  - Constraints: Up to 255 characters in length
  - Constraints: a-z, A-Z, 0-9, and _-
  - Required: Yes
- network_connector_id:

  ID of network connector to which this network connector endpoint belongs.

  - Type: String
  - Required: Yes
- endpoint_type:

  type of this network connector endpoint.

  - Type: String
  - Constraints: "availability_zone" or "remote"
  - Required: Yes
- location:

  location of this network connector endpoint in the endpoint_type.

  - Type: String
  - Required: Yes
  - Constraints: When type is "availability_zone", this value must be one of availability zone name. When type is "remote", this value express label of location, such as 'intra'.
- tenant_id:

  The tenant's ID to which this network connector belongs.

  This parameter is restricted for tenant in which requester joins.

  - Type: String
  - Required: No

Response

Status code

- 201

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector_endpoint" : {
  "id": "6ed3561f-087f-43f9-9a51-bf71f666b80f",
  "name": "endponit_for_az1",
  "network_connector_id": "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "endpoint_type": "availability_zone",
  "location" : "east-jp-az1",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Elements

- id:

  ID for this network connector endpoint

  - Type: String
- name:

  Name for this network connector endpoint

  - Type: String
- network_connector_id:

  ID of network connector to which this network connector endpoint belongs.

  - Type: String
- endpoint_type:

  Type of this network connector endpoint. This value must be one of "availability_zone" or "remote"

  - Type: String
- location:

  Location of this network connector endpoint in the endpoint_type. When endpoint_type is "availability_zone", this value is availability_zone name. When endpoint_type is "remote", this value expresses label of location, such as 'intra'.

  - Type: String
- tenant_id:

  Tenant's ID to which this network connector belongs

  - Type: String

Errors

- 400: Invalid parameter in request body
- 401: Token is not specified or not authorized
- 403: Token is not permitted to operate
- 404: Network connector not found for specified ID
- 409: A network endpoint already exists for same condition with combination of endpoint_type and location.
- 503: Any available resource for network connector endpoint does not remain.

1.2.6.14 Show Network Connector Endpoint

Shows a specified network connector endpoint.

Request

URI

GET <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>

Example:

GET http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector_endpoint" : {
  "id": "6ed3561f-087f-43f9-9a51-bf71f666b80f",
  "name": "endponit_for_az1",
  "network_connector_id": "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "endpoint_type": "availability_zone",
  "location" : "east-jp-az1",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Elements

- id:

  ID for this network connector endpoint

  - Type: String
- name:

  Name for this network connector endpoint

  - Type: String
- network_connector_id:

ID of network connector to which this network connector endpoint belongs.

  - Type: String
- endpoint_type:

  Type of this network connector endpoint. This value must be one of "availability_zone" or "remote"

  - Type: String
- location:

  Location of this network connector endpoint in the endpoint_type. When endpoint_type is "availability_zone", this value is availability_zone name. When endpoint_type is "remote", this value expresses label of location, such as 'intra'.

  - Type: String
- tenant_id:

  Tenant's ID to which this network connector belongs

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate
- 404: Network connector endpoint not found for specified ID

1.2.6.15 List Network Connector Endpoints

Lists network connector endpoints.

Request

URI

GET <network service endpoint>/v2.0/network_connector_endpoints

Example:

GET http://192.168.122.1:9696/v2.0/network_connector_endpoints

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector_endpoints" :[
  {
   "id": "6ed3561f-087f-43f9-9a51-bf71f666b80f",
   "name": "endponit_for_az1",
   "network_connector_id": "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
   "endpoint_type": "availability_zone",
   "location" : "east-jp-az1",
   "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
  },
  {
   "id": "1e71eee6-a7e5-4b05-93c6-e6e8bf02f2e5",
   "name": "endponit_for_az2",
   "network_connector_id": "75e3507f-8fb6-4b0f-9f0c-00ce011e4a51",
   "endpoint_type": "availability_zone",
   "location" : "east-jp-az2",
   "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
  }
 ]
}
```

Elements

- id:

  ID for this network connector endpoint

  - Type: String
- name:

  Name for this network connector endpoint

  - Type: String
- network_connector_id:

  ID of network connector to which this network connector endpoint belongs.

  - Type: String
- endpoint_type:

  Type of this network connector endpoint. This value must be one of "availability_zone" or "remote"

  - Type: String
- location:

  Location of this network connector endpoint in the endpoint_type. When endpoint_type is "availability_zone", this value is availability_zone name. When endpoint_type is "remote", this value expresses label of location, such as 'intra'.

  - Type: String
- tenant_id:

  Tenant's ID to which this network connector belongs

  - Type: String

Errors

- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate

1.2.6.16 Update Network Connector Endpoint

Updates a specified network connector endpoint.

Request

URI

PUT <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>

Example:

PUT http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "network_connector_endpoint" : {
  "name": "endponit2_for_az1"
 }
}
```

Request parameters

- name:

  Name for this network connector endpoint.

  - Type: String
  - Constraints: Up to 255 characters in length
  - Constraints: a-z, A-Z, 0-9, and _-

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector_endpoint" : {
  "id": "6ed3561f-087f-43f9-9a51-bf71f666b80f",
```

```
  "name": "endponit2_for_az1",
  "network_connector_id": "07993b1c-79e1-4cf6-a663-dc42b9ce37d4",
  "endpoint_type": "availability_zone",
  "location" : "east-jp-az1",
  "tenant_id" : "29320d5e-dd29-425c-b386-3cbb2754ad03"
 }
}
```

Elements

- id:

  ID for this network connector endpoint

  - Type: String
- name:

  Name for this network connector endpoint

  - Type: String
- network_connector_id:

  ID of network connector to which this network connector endpoint belongs.

  - Type: String
- endpoint_type:

  Type of this network connector endpoint. This value must be one of "availability_zone" or "remote"

  - Type: String
- location:

  Location of this network connector endpoint in the endpoint_type. When endpoint_type is "availability_zone", this value is availability_zone name. When endpoint_type is "remote", this value expresses label of location, such as 'intra'.

  - Type: String
- tenant_id:

  Tenant's ID to which this network connector belongs

  - Type: String

Errors

- 400:
  - Invalid parameter in request body
  - Not updatable parameter is specified in request body
- 401: Token is not specified or not authorized
- 403: Token is not permitted to operate
- 404: Network connector endpoint not found for specified ID
- 409: Operation conflicts with another one.

1.2.6.17 Deletes Network Connector Endpoint

Deletes a specified network connector endpoint.

Request

URI

DELETE <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>

Example:

DELETE http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 204

Errors

- 401: Token is not specified or not authorized
- 403: Token is not permitted to operate
- 404: Network connector endpoint not found for specified ID
- 409:
  - Some interfaces still connect to the network connector endpoint.
  - Operation conflicts with another one.

1.2.6.18 Connect Network Connector Endpoint

Connects interface to a specified network connector endpoint.

Request

URI

PUT <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>/connect

Example:

PUT http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f/connect

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "interface" : {
```

```
  "port_id": "5fd5b822-c400-46dc-bc68-ea8c0dd20876"
 }
}
```

Parameters

- interface:

  Resource information for connection to the network connector endpoint. Value depends on network connector endpoint type. When endpoint_type is availability_zone:

  - Type: Map
  - Required: Yes
- port_id:

  Port resource on the availability zone.

  - Type: String
  - Required: Yes

Response

Status code

- 200

Errors

- 400: Invalid parameter in request body
- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.
- 404: Network connector endpoint not found for specified ID
- 409:
  - Resource can't be connected to network connector endpoint.
  - Operation conflicts with another one.

Caution ID for internal control is displayed in device_id of port information after the port connected to Network Connector Endpoint.

1.2.6.19 Disconnect Network Connector Endpoint

Disconnect interface to a specified network connector endpoint.

Request

URI

PUT <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>/disconnect

Example:

PUT http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f/disconnect

Headers

- X-Auth-Token: token delivered by identity service
- Content-Type: application/json

Body syntax

```
{
 "interface" : {
  "port_id": "5fd5b822-c400-46dc-bc68-ea8c0dd20876"
 }
}
```

Parameters

- interface:

  Resource information for disconnection to the network connector endpoint Value depends on network connector endpoint type. When endpoint_type is availability_zone:

  - Type: Map
  - Required: Yes
- port_id:

  Port resource on the availability zone. The port's device_owner must be 'network:router_interface'

  - Type: String
  - Required: Yes

Response

Status code

- 200

Errors

- 400: Invalid parameter in request body
- 401: Token is not specified or not authorized.
- 403: Token is not permitted to operate.
- 404:
  - Network connector endpoint not found for specified ID.
  - Specified interface is not connected.
- 409: Operation conflicts with another one.

1.2.6.20 List Connected Interfaces of Network Connector Endpoint

Lists interfaces which connects to a specified network connector endpoint.

Request

URI

GET <network service endpoint>/v2.0/network_connector_endpoints/<network connector endpoint id>/interfaces

Example:

GET http://192.168.122.1:9696/v2.0/network_connector_endpoints/6ed3561f-087f-43f9-9a51-bf71f666b80f/interfaces

Headers

- X-Auth-Token: token delivered by identity service

Response

Status code

- 200

Headers

- Content-Type: application/json

Body

Example:

```
{
 "network_connector_endpoint" : {
  "interfaces" : [
  {
   "port_id": "5fd5b822-c400-46dc-bc68-ea8c0dd20876"
  },
  {
   "port_id": "8df2a059-2851-4938-b989-51ce156d6b29"
  }
 ]
}
```

Elements

- interfaces:

  Information of interfaces connecting to specified network connector endpoint.

  - Type: Array of Map

For availability_zone:

- port_id:

  Port resource in the availability zone.

  - Type: String

Errors

- 401: Token is not specified or not authorized.

- 403: Token is not permitted to operate.
- 404: Network connector endpoint not found for specified ID

1.3 Network adapter

1.3.1 API list

ports

Item	API	Description
1	GET /v2.0/ports List ports	Lists ports to which the tenant has access
2	POST /v2.0/ports Create port	Creates a port on the specified network
3	GET /v2.0/ports/{port_id} Show port	Shows details for the specified port
4	PUT /v2.0/ports/{port_id} Update port	Updates the specified port
5	DELETE /v2.0/ports/{port_id} Delete port	Deletes the specified port

Security groups and rules

Item	API	Description
1	POST /v2.0/security-groups Create security group	Creates a security group
2	GET /v2.0/security-groups/ {security_group_id} Show security group	Shows the specified security group
3	PUT /v2.0/security-groups/ {security_group_id} Update security group	Updates information about the specified security group
4	DELETE /v2.0/security-groups/ {security_group_id} Delete security group	Deletes the specified security group
5	POST /v2.0/security-group-rules Create security group rule	Creates security group rules
6	DELETE /v2.0/security-group-rules/ {rules-security-groups-id} Delete security group rule	Deletes the specified rule from a security group
7	GET /v2.0/security-groups	Lists security groups

Item	API	Description
	List security groups	
8	GET /v2.0/security-group-rules List security group rules	Lists security group rules
9	GET /v2.0/security-group-rules/{rules-security-groups-id} Show security group rule	Shows details about the specified security group rule

- If the security group is omitted when creating the port (Port) of an instance, the default security group of the project will be used. The default security group rules of the initial state are as follows.

Direction	IP version	Communication destination	Protocol number	Protocol-specific information
Egress	IPv6	All	All	All
Egress	IPv4	All	All	All
Ingress	IPv6	Default security group	All	All
Ingress	IPv4	Default security group	All	All

- The rules of the initial state during security group creation are as follows.

Direction	IP version	Communication destination	Protocol number	Protocol-specific information
Egress	IPv6	All	All	All
Egress	IPv4	All	All	All

1.3.2 General requirements

This section describes general requirements to use this API.

- Specify the name and description input parameters using up to 255 characters.
- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.
- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.3.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.3.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType

Caution

- If the user has insufficient privileges to issue the target API when issuing the API for showing (Show), updating (Update), or deleting (Delete) resources, the status code 404 may be returned.
- If the user has insufficient privileges to issue the target API when issuing the API for listing (List) resources, the status code 200 will be returned and a null array will be set

in the body. If there are resources with the shared attribute set to "True", information on the target resources only will be returned.

1.3.5 API options

1.3.5.1 API options

Two options are available for APIs that retrieve resource information (List, Show).

1.3.5.2 filter

Filters can be specified to retrieve only resources matching the specified attributes from the list of resource information to be retrieved.

Multiple attributes can be specified using AND as a condition.

This option can only be used for the List API.

Execution example:

- Retrieve the network with the name "private"

  GET /v2.0/networks?name=private
- To filter using multiple attributes with AND. Retrieve the network with the name "private" and that belongs to the AZ1 availability zone.

  GET /v2.0/networks?name=private?availability_zone=AZ1

1.3.5.3 Column Selection

The attributes that are retrieved from the resource information can be restricted.

This option can only be used for the List and Show APIs.

Execution example:

- List only the id attribute of networks

  GET /v2.0/networks?fields=id
- To retrieve multiple attributes (id and name)

  GET /v2.0/networks?fields=id&fields=name

1.3.5.4 APIs that do not support these options

These options are not supported by the following APIs.

- *Show Network Connector Pool* on page 31
- *List Network Connector Pools* on page 32
- *Show Network Connector* on page 35
- *List Network Connectors* on page 36
- *Show Network Connector Endpoint* on page 43
- *List Network Connector Endpoints* on page 44
- *List Connected Interfaces of Network Connector Endpoint* on page 50

1.3.6 API details

1.3.6.1 List ports

Lists ports to which the tenant has access.

URI

/v2.0/ports

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)


```
{
    "ports": [
        {
            "status": "ACTIVE",
            "name": "",
            "allowed_address_pairs": [],
            "admin_state_up": true,
            "network_id": "70c1db1f-b701-45bd-96e0-a313ee3430b3",
            "tenant_id": " d397de8a63f341818f198abb0966f6f3",
            "extra_dhcp_opts": [],
            "device_owner": " network:router_interface ",
            "mac_address": "fa:16:3e:58:42:ed",
            "binding:vnic_type": "normal",
            "fixed_ips": [
                {
                    "subnet_id": "008ba151-0b8c-4a67-98b5-0d2b87666062",
                    "ip_address": "172.24.4.2"
                }
            ],
            "id": "d80b1a3b-4fc1-49f3-952e-1e2ab7081d8b",
            "security_groups": [],
            "device_id": "9ae135f4-b6e0-4dad-9e91-3c223e385824",
            "availability_zone": "AZ1"
        },
        {
            "status": "ACTIVE",
            "name": "",
            "allowed_address_pairs": [],
            "admin_state_up": true,
            "network_id": "f27aa545-cbdd-4907-b0c6-c9e8b039dcc2",
            "tenant_id": "d397de8a63f341818f198abb0966f6f3",
            "extra_dhcp_opts": [],
            "device_owner": "network:router_interface",
            "mac_address": "fa:16:3e:bb:3c:e4",
            "binding:vnic_type": "normal",
            "fixed_ips": [
```

```
                {
                    "subnet_id": "288bf4a1-51ba-43b6-9d0a-520e9005db17",
                    "ip_address": "10.0.0.1"
                }
            ],
            "id": "f71a6703-d6de-4be1-a91a-a570ede1d159",
            "security_groups": [],
            "device_id": "9ae135f4-b6e0-4dad-9e91-3c223e385824",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
status	The port status. Value is ACTIVE or DOWN.
name	The port name.
allowed_address_pairs	Allowed address pairs.
admin_state_up	The administrative state of the port, which is up (true) or down (false).
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
extra_dhcp_opts	Extra DHCP options.
device_owner	The ID of the entity that uses this port. For example, a dhcp agent.
mac_address	The MAC address of the port.
fixed_ips	IP addresses for the port. Includes the IP address and subnet ID.
id	The ID of the port.
security_groups	The IDs of any attached security groups.
device_id	The ID of the device that uses this port. For example, a virtual server.
binding:vnic_type (Optional)	The vnic type that is bound to the neutron port. This value is one of followings: • normal(virtual nic) • direct(pci passthrough) • macvtap(virtual interface with a tap-like software interface)
availability_zone	The Availability Zone name

1.3.6.2 Create port

Creates a port on a specified network.

URI

/v2.0/ports

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
name	A symbolic name for the port.	xsd:string	Optional
allowed_address_pairs	Allowed address pairs	xsd:dict	Optional
admin_state_up	The administrative status of the port, which is up (true) or down (false).	xsd:bool	Optional
mac_address	The MAC address. If you specify an address that is not valid, a 400 Bad Request error is returned. If you do not specify a MAC address, OpenStack Networking tries to allocate one. If a failure occurs, a 503 Service Unavailable error is returned.	xsd:string	Optional
fixed_ips	If you specify only a subnet ID, OpenStack Networking allocates an available IP from that subnet to the port. If you specify both a subnet ID and an IP address, OpenStack Networking tries to allocate the specified address to the port.	xsd:dict	Optional
security_groups	Security groups. Specify one or more security group IDs.	csapi:uuid	Optional (Note)
network_id	The ID of the the network.	csapi:uuid	Required
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional


Caution For ports used by the Windows virtual server for SAP service or physical server for SAP HANA service, the IP address specified in allocation_pools and gateway_ip of the subnet associated with network_id can be specified for fixed_ips.

Example request

```
{
    "port": {
        "network_id": "a87cc70a-3e15-4acf-8205-9b711a3531b7",
        "name": "private-port",
        "admin_state_up": true,
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes
macGenerationFailure (503)	Error response codes
serviceUnavailable (503)	Error response codes

Response body (normal status)

```
{
    "port": {
        "status": "DOWN",
        "name": "private-port",
        "allowed_address_pairs": [],
        "admin_state_up": true,
        "network_id": "a87cc70a-3e15-4acf-8205-9b711a3531b7",
        "tenant_id": "d6700c0c9ffa4f1cb322cd4a1f3906fa",
        "binding:vnic_type": "normal",
        "device_owner": "",
        "mac_address": "fa:16:3e:c9:cb:f0",
        "fixed_ips": [
            {
                "subnet_id": "a0304c3a-4f08-4c43-88af-d796509c97d2",
                "ip_address": "10.0.0.2"
            }
        ],
        "id": "65c0ee9f-d634-4522-8954-51021b570b0d",
        "security_groups": [
            "f0ac4394-7e4a-4409-9701-ba8be283dbc3"
        ],
        "device_id": "",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
status	The port status. Value is ACTIVE or DOWN.
name	The port name.
allowed_address_pairs	Allowed address pairs.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
extra_dhcp_opts	Extra DHCP options.

Item	Description
device_owner	The ID of the entity that uses this port. For example, a dhcp agent.
mac_address	The MAC address of the port.
fixed_ips	IP addresses for the port. Includes the IP address and subnet ID.
id	The ID of the port.
security_groups	The IDs of any attached security groups.
device_id	The ID of the device that uses this port. For example, a virtual server.
binding:vnic_type	The vnic type that is bound to the neutron port. This value is one of followings: • normal(virtual nic) • direct(pci passthrough) • macvtap(virtual interface with a tap-like software interface)
availability_zone	The Availability Zone name

Caution

If security_groups is omitted, the default security group of the project will be used.

1.3.6.3 Show port

Shows information for a specified port.

URI

/v2.0/ports/{port_id}

Description of the URI:

{port_id} UUID The UUID for the port.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "port": {
```

```
        "status": "ACTIVE",
        "name": "",
        "allowed_address_pairs": [],
        "admin_state_up": true,
        "network_id": "a87cc70a-3e15-4acf-8205-9b711a3531b7",
        "tenant_id": "7e02058126cc4950b75f9970368ba177",
        "extra_dhcp_opts": [],
        "device_owner": "network:router_interface",
        "mac_address": "fa:16:3e:23:fd:d7",
        "binding:vnic_type": "normal",
        "fixed_ips": [
            {
                "subnet_id": "a0304c3a-4f08-4c43-88af-d796509c97d2",
                "ip_address": "10.0.0.1"
            }
        ],
        "id": "46d4bfb9-b26e-41f3-bd2e-e6dcc1ccedb2",
        "security_groups": [],
        "device_id": "5e3898d7-11be-483e-9732-b2f5eccd2b2e",
        "availability_zone": "AZ1"
    }
}
```


Description of response body (normal status)

Item	Description
status	The port status. Value is ACTIVE or DOWN.
name	The port name.
allowed_address_pairs	Allowed address pairs.
admin_state_up	The administrative state of the port, which is up (true) or down (false).
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
extra_dhcp_opts	Extra DHCP options.
device_owner	The ID of the entity that uses this port. For example, a dhcp agent.
mac_address	The MAC address of the port.
fixed_ips	IP addresses for the port. Includes the IP address and subnet ID.
id	The ID of the port.
security_groups	The IDs of any attached security groups.
device_id	The ID of the device that uses this port. For example, a virtual server.
binding:vnic_type	The vnic type that is bound to the neutron port. This value is one of followings: • normal(virtual nic) • direct(pci passthrough) • macvtap(virtual interface with a tap-like software interface)
availability_zone	The Availability Zone name

1.3.6.4 Update port

Updates a specified port.

URI

/v2.0/ports/{port_id}

Description of the URI:

{port_id} UUID The UUID for the port.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
name	A symbolic name for the port.	xsd:string	Optional
admin_state_up	The administrative status of the port, which is up (true) or down (false).	xsd:bool	Optional
fixed_ips	If you specify only a subnet ID, OpenStack Networking allocates an available IP from that subnet to the port. If you specify both a subnet ID and an IP address, OpenStack Networking tries to allocate the specified address to the port. Caution Do not specify this parameter when the port is associated with floating IP.	xsd:dict	Optional
security_groups	Security groups. Specify one or more security group IDs.	csapi:uuid	Optional

Caution For ports used by the Windows virtual server for SAP service or physical server for SAP HANA service, the IP address specified in allocation_pools and gateway_ip of the subnet associated with network_id can be specified for fixed_ips.

Example request

```
{
    "port": {
        "name": "private-port",
        "admin_state_up": true
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "port": {
        "status": "DOWN",
        "name": "private-port",
        "allowed_address_pairs": [],
        "admin_state_up": true,
        "network_id": "a87cc70a-3e15-4acf-8205-9b711a3531b7",
        "tenant_id": "d6700c0c9ffa4f1cb322cd4a1f3906fa",
        "binding:vnic_type": "normal",
        "device_owner": "",
        "mac_address": "fa:16:3e:c9:cb:f0",
        "fixed_ips": [
            {
                "subnet_id": "a0304c3a-4f08-4c43-88af-d796509c97d2",
                "ip_address": "10.0.0.2"
            }
        ],
        "id": "65c0ee9f-d634-4522-8954-51021b570b0d",
        "security_groups": [
            "f0ac4394-7e4a-4409-9701-ba8be283dbc3"
        ],
        "device_id": "",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
status	The port status. Value is ACTIVE or DOWN.
name	The port name.
allowed_address_pairs	Allowed address pairs.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
network_id	The ID of the attached network.
tenant_id	The ID of the tenant who owns the network.
extra_dhcp_opts	Extra DHCP options.
device_owner	The ID of the entity that uses this port. For example, a dhcp agent.

Item	Description
mac_address	The MAC address of the port.
fixed_ips	IP addresses for the port. Includes the IP address and subnet ID.
id	The ID of the port.
security_groups	The IDs of any attached security groups.
device_id	The ID of the device that uses this port. For example, a virtual server.
binding:vnic_type	This value is one of followings: • normal(virtual nic) • direct(pci passthrough) • macvtap(virtual interface with a tap-like software interface)
availability_zone	The Availability Zone name

1.3.6.5 Delete port

Deletes a specified port.

URI

/v2.0/ports/{port_id}

Description of the URI:

{port_id} UUID The UUID for the port.

HTTP method

DELETE

Request parameter

Notes

- Do not delete ports attached to virtual servers.

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

1.3.6.6 Create security group

Creates an OpenStack Networking security group.

URI

/v2.0/security-groups

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
name	A symbolic name for the security group. Not required to be unique.	xsd:string	Optional
description	Describes the security group.	xsd:string	Optional

Example request

```
{
    "security_group": {
        "name": "new-webservers",
        "description": "security group for webservers"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "security_group": {
        "description": "security group for webservers",
        "id": "2076db17-a522-4506-91de-c6dd8e837028",
        "name": "new-webservers",
        "security_group_rules": [
            {
                "direction": "egress",
                "ethertype": "IPv4",
                "id": "38ce2d8e-e8f1-48bd-83c2-d33cb9f50c3d",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "2076db17-a522-4506-91de-c6dd8e837028",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            },
            {
                "direction": "egress",
                "ethertype": "IPv6",
```

```
                "id": "565b9502-12de-4ffd-91e9-68885cff6ae1",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "2076db17-a522-4506-91de-c6dd8e837028",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            }
        ],
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
    }
}
```

Description of response body (normal status)

Item	Description
description	The security group description.
id	The UUID for the security group.
name	The security group name.
tenant_id	The tenant ID.
security_group_rules	The security group rule objects to associate with this security group.

1.3.6.7 Show security group

Shows information for a specified security group.

URI

/v2.0/security-groups/{security_group_id}

Description of the URI:

{security_group_id} UUID The UUID of the security group IP.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "security_group": {
        "description": "default",
```

```
        "id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "name": "default",
        "security_group_rules": [
            {
                "direction": "egress",
                "ethertype": "IPv6",
                "id": "3c0e45ff-adaf-4124-b083-bf390e5482ff",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            },
            {
                "direction": "egress",
                "ethertype": "IPv4",
                "id": "93aa42e5-80db-4581-9391-3a608bd0e448",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            },
            {
                "direction": "ingress",
                "ethertype": "IPv6",
                "id": "c0b09f00-1d49-4e64-a0a7-8a186d928138",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "remote_ip_prefix": null,
                "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            },
            {
                "direction": "ingress",
                "ethertype": "IPv4",
                "id": "f7d45c89-008e-4bab-88ad-d6811724c51c",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "remote_ip_prefix": null,
                "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            }
        ],
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
    }
}
```


Description of response body (normal status)

Item	Description
security_group	Security group object.
description	The security group description.
id	The UUID for the security group.
name	The security group name.

Item	Description
tenant_id	The tenant ID.
security_group_rules	The security group rule objects to associate with this security group.

1.3.6.8 Update security group

Updates an OpenStack Networking security group.

URI

/v2.0/security-groups/{security_group_id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
name	The security group name.	xsd:string	Optional
description	The security group description.	xsd:string	Optional

Example request

```
{
    "security_group": {
        "name": "new-webservers",
        "description": "security group for webservers"
    }
}
```

Response codes

Status code	Description
200	Normal response codes
Bad Request (400)	Error response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "security_group": {
        "description": "security group for webservers",
        "id": "2076db17-a522-4506-91de-c6dd8e837028",
        "name": "new-webservers",
        "security_group_rules": [
            {
```

```
                "direction": "egress",
                "ethertype": "IPv4",
                "id": "38ce2d8e-e8f1-48bd-83c2-d33cb9f50c3d",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "2076db17-a522-4506-91de-c6dd8e837028",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            },
            {
                "direction": "egress",
                "ethertype": "IPv6",
                "id": "565b9502-12de-4ffd-91e9-68885cff6ae1",
                "port_range_max": null,
                "port_range_min": null,
                "protocol": null,
                "remote_group_id": null,
                "remote_ip_prefix": null,
                "security_group_id": "2076db17-a522-4506-91de-c6dd8e837028",
                "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
            }
        ],
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
    }
}
```


Description of response body (normal status)

Item	Description
description	The security group description.
id	The UUID for the security group.
name	The security group name.
tenant_id	The tenant ID.
security_group_rules	The security group rule objects to associate with this security group.

1.3.6.9 Delete security group

Deletes an OpenStack Networking security group.

URI

/v2.0/security-groups/{security_group_id}

Description of the URI:

{security_group_id} UUID The UUID of the security group IP.

HTTP method

DELETE

Response codes

Status code	Description
201	Normal response codes
204	No Content
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

1.3.6.10 Create security group rule

Creates an OpenStack Networking security group rule.

URI

/v2.0/security-group-rules

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
direction	Ingress or egress: The direction in which the security group rule is applied. For a compute instance, an ingress security group rule is applied to incoming (ingress) traffic for that instance. An egress rule is applied to traffic leaving the instance.	xsd:string	Required
port_range_min	The minimum port number in the range that is matched by the security group rule. When the protocol is TCP or UDP, this value must be less than or equal to the value of the port_range_max attribute. If this value is not specified, the security group rule matches all numbers of port. If port_range_min is 0, all port numbers are allowed regardless of port_range_max. When the protocol is ICMP, this value must be an ICMP type. If this value is not specified, the security group rule matches all ICMP types.	xsd:int	Optional

Key	Description	Type	Required/optional
ethertype	Must be IPv4, and addresses represented in CIDR must match the ingress or egress rules. If this values is not specified, IPv4 is set.	xsd:string	Optional
port_range_max	The maximum port number in the range that is matched by the security group rule. When the protocol is TCP or UDP , the port_range_min attribute constrains the port_range_max attribute. When the protocol is ICMP, this value must be an ICMP code. If this value is not specified, the security group rule matches all ICMP codes.	xsd:int	Optional
protocol	The protocol that is matched by the security group rule. Valid values are null, tcp, udp, icmp, and digits between 0-and 255	xsd:string	Optional
remote_group_id	The remote group ID to be associated with this security group rule. You can specify either remote_group_id or remote_ip_prefix in the request body.	csapi:uuid	Optional
security_group_id	The security group ID to associate with this security group rule.	csapi:uuid	Required
remote_ip_prefix	The remote IP prefix to be associated with this security group rule. You can specify either remote_group_id or remote_ip_prefix in the request body. This attribute matches the specified IP prefix as the source or destination IP address of the IP packet. if direction is ingress matches source, otherwise matches destination.	xsd:string	Optional

Example request

```
{
    "security_group_rule": {
        "direction": "ingress",
        "port_range_min": "80",
        "ethertype": "IPv4",
        "port_range_max": "80",
        "protocol": "tcp",
        "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a"
```

```
    }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
buildInProgress (409)	Error response codes

Response body (normal status)

```
{
    "security_group_rule": {
        "direction": "ingress",
        "ethertype": "IPv4",
        "id": "2bc0accf-312e-429a-956e-e4407625eb62",
        "port_range_max": 80,
        "port_range_min": 80,
        "protocol": "tcp",
        "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "remote_ip_prefix": null,
        "security_group_id": "a7734e61-b545-452d-a3cd-0189cbd9747a",
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
    }
}
```

Description of response body (normal status)

Item	Description
id	The security group rule ID.
direction	Ingress or egress: The direction in which the security group rule is applied. For a compute instance, an ingress security group rule is applied to incoming (ingress) traffic for that instance. An egress rule is applied to traffic leaving the instance.
port_range_min	The minimum port number in the range that is matched by the security group rule. When the protocol is TCP or UDP, If this value is not specified, the security group rule matches all numbers of port. If port_range_min is 0, all port numbers are allowed regardless of port_range_max. When the protocol is ICMP, this value must be an ICMP type. If this value is null, the security group rule matches all ICMP types.
ethertype	Must be IPv4 or IPv6, and addresses represented in CIDR must match the ingress or egress rules.
port_range_max	The maximum port number in the range that is matched by the security group rule.

Item	Description
	When the protocol is ICMP, If this value is not specified, the security group rule matches all ICMP codes.
protocol	The protocol that is matched by the security group rule. Valid values are null, tcp, udp, icmp, and digits between 0-and 255
remote_group_id	The remote group ID to be associated with this security group rule.
security_group_id	The security group ID to associate with this security group rule.
remote_ip_prefix	The remote IP prefix to be associated with this security group rule. This attribute matches the specified IP prefix as the source or destination IP address of the IP packet. if direction is ingress matches source, otherwise matches destination.

1.3.6.11 Delete security group rule

Deletes a specified rule from a OpenStack Networking security group.

URI

/v2.0/security-group-rules/{rules-security-groups-id}

Description of the URI:

{rules-security-groups-id} UUID The UUID of the security group rule IP.

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

1.3.6.12 List security groups

Lists all OpenStack Networking security groups to which the specified tenant has access.

URI

/v2.0/security-groups

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes

Response body (normal status)


```
{
    "security_groups": [
        {
            "description": "default",
            "id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "name": "default",
            "security_group_rules": [
                {
                    "direction": "egress",
                    "ethertype": "IPv6",
                    "id": "3c0e45ff-adaf-4124-b083-bf390e5482ff",
                    "port_range_max": null,
                    "port_range_min": null,
                    "protocol": null,
                    "remote_group_id": null,
                    "remote_ip_prefix": null,
                    "security_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
                    "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
                },
                {
                    "direction": "egress",
                    "ethertype": "IPv4",
                    "id": "93aa42e5-80db-4581-9391-3a608bd0e448",
                    "port_range_max": null,
                    "port_range_min": null,
                    "protocol": null,
                    "remote_group_id": null,
                    "remote_ip_prefix": null,
                    "security_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
                    "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
                },
                {
                    "direction": "ingress",
                    "ethertype": "IPv6",
                    "id": "c0b09f00-1d49-4e64-a0a7-8a186d928138",
                    "port_range_max": null,
                    "port_range_min": null,
                    "protocol": null,
                    "remote_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
                    "remote_ip_prefix": null,
                    "security_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
                    "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
                },
                {
                    "direction": "ingress",
                    "ethertype": "IPv4",
                    "id": "f7d45c89-008e-4bab-88ad-d6811724c51c",
                    "port_range_max": null,
                    "port_range_min": null,
                    "protocol": null,
                    "remote_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
```

```
                    "remote_ip_prefix": null,
                    "security_group_id": "85cc3048-
abc3-43cc-89b3-377341426ac5",
                    "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
                }
            ],
            "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
security_group	Security group object.
description	The security group description.
id	The UUID for the security group.
name	The security group name.

1.3.6.13 List security group rules

Lists a summary of all OpenStack Networking security group rules that the specified tenant can access.

URI

/v2.0/security-group-rules

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "security_group_rules": [
        {
            "direction": "egress",
            "ethertype": "IPv6",
            "id": "3c0e45ff-adaf-4124-b083-bf390e5482ff",
            "port_range_max": null,
            "port_range_min": null,
            "protocol": null,
            "remote_group_id": null,
            "remote_ip_prefix": null,
            "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
```

```
        },
        {
            "direction": "egress",
            "ethertype": "IPv4",
            "id": "93aa42e5-80db-4581-9391-3a608bd0e448",
            "port_range_max": null,
            "port_range_min": null,
            "protocol": null,
            "remote_group_id": null,
            "remote_ip_prefix": null,
            "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
        },
        {
            "direction": "ingress",
            "ethertype": "IPv6",
            "id": "c0b09f00-1d49-4e64-a0a7-8a186d928138",
            "port_range_max": null,
            "port_range_min": null,
            "protocol": null,
            "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "remote_ip_prefix": null,
            "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
        },
        {
            "direction": "ingress",
            "ethertype": "IPv4",
            "id": "f7d45c89-008e-4bab-88ad-d6811724c51c",
            "port_range_max": null,
            "port_range_min": null,
            "protocol": null,
            "remote_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "remote_ip_prefix": null,
            "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
            "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
        }
    ]
}
```


Description of response body (normal status)

Item	Description
direction	Ingress or egress: The direction in which the security group rule is applied. For a compute instance, an ingress security group rule is applied to incoming (ingress) traffic for that instance. An egress rule is applied to traffic leaving the instance.
ethertype	Must be IPv4 or IPv6, and addresses represented in CIDR must match the ingress or egress rules.
security_group_id	The security group ID to associate with this security group rule.
port_range_min	The minimum port number in the range that is matched by the security group rule. When the protocol is TCP or UDP, If this value is not specified, the security group rule matches all numbers of port. If port_range_min is 0, all port numbers are allowed regardless of port_range_max. When the protocol is ICMP, this value must be an ICMP type. If this value is null, the security group rule matches all ICMP types.

Item	Description
port_range_max	The maximum port number in the range that is matched by the security group rule. When the protocol is ICMP, If this value is not specified, the security group rule matches all ICMP codes.
protocol	The protocol that is matched by the security group rule. Valid values are null, tcp, udp, icmp, and digits between 0 and 255.
remote_group_id	The remote group ID to be associated with this security group rule.
remote_ip_prefix	The remote IP prefix to be associated with this security group rule. This attribute matches the specified IP prefix as the source or destination IP address of the IP packet. if direction is ingress matches source, otherwise matches destination.

1.3.6.14 Show security group rule

Shows detailed information for a specified security group rule.

URI

/v2.0/security-group-rules/{rules-security-groups-id}

Description of the URI:

{rules-security-groups-id} UUID The UUID of the security group rule IP.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)


```
{
    "security_group_rule": {
        "direction": "egress",
        "ethertype": "IPv6",
        "id": "3c0e45ff-adaf-4124-b083-bf390e5482ff",
        "port_range_max": null,
        "port_range_min": null,
        "protocol": null,
        "remote_group_id": null,
        "remote_ip_prefix": null,
        "security_group_id": "85cc3048-abc3-43cc-89b3-377341426ac5",
        "tenant_id": "e4f50856753b4dc6afee5fa6b9b6c550"
    }
}
```

Description of response body (normal status)

Item	Description
direction	Ingress or egress: The direction in which the security group rule is applied. For a compute instance, an ingress security group rule is applied to incoming (ingress) traffic for that instance. An egress rule is applied to traffic leaving the instance.
ethertype	Must be IPv4 or IPv6, and addresses represented in CIDR must match the ingress or egress rules.
id	The security group rule ID.
port_range_max	The maximum port number in the range that is matched by the security group rule. When the protocol is ICMP, If this value is not specified, the security group rule matches all ICMP codes.
port_range_min	The minimum port number in the range that is matched by the security group rule. When the protocol is TCP or UDP, If this value is not specified, the security group rule matches all numbers of port. If port_range_min is 0, all port numbers are allowed regardless of port_range_max. When the protocol is ICMP, this value must be an ICMP type. If this value is null, the security group rule matches all ICMP types.
protocol	The protocol that is matched by the security group rule. Valid values are null, tcp, udp, icmp, and digits between 0 and 255.
remote_group_id	The remote group ID to be associated with this security group rule.
remote_ip_prefix	The remote IP prefix to be associated with this security group rule. This attribute matches the specified IP prefix as the source or destination IP address of the IP packet. if direction is ingress matches source, otherwise matches destination.
security_group_id	The security group ID to associate with this security group rule.

1.4 Network connector service

1.4.1 API list

Layer-3 networking (routers)

Item	API	Description
1	POST /v2.0/routers Create router	Creates a logical router
2	GET /v2.0/routers/{router_id} Show router details	Shows details about the specified router
3	DELETE /v2.0/routers/{router_id} Delete router	Deletes a logical router If present, also deletes its external gateway interface
4	PUT /v2.0/routers/{router_id} Update router	Updates the specified logical router
5	PUT /v2.0/routers/{router_id}/add_router_interface Add interface to router	Adds an internal interface to the specified logical router
6	PUT /v2.0/routers/{router_id}/remove_router_interface Remove interface from router	Deletes an internal interface from the specified logical router
7	GET /v2.0/routers List routers	Lists routers that the tenant who submits the request can access

Extra routes

Item	API	Description
1	PUT /v2.0/routers/{router_id} Update extra route	Updates routing information

Virtual Private Network as a Service

Item	API	Description
1	GET /v2.0/vpn/ipsecpolicies List IPSec policies	Lists all IPsec policies
2	GET /v2.0/vpn/ipsecpolicies/{ipsecpolicy-id} Show IPSec policy details	Shows details about the specified IPsec policy

Item	API	Description
3	POST /v2.0/vpn/ipsecpolicies Create IPSec Policy	Creates an IPsec policy
4	PUT /v2.0/vpn/ipsecpolicies/{ipsecpolicy-id} Update IPSec Policy	Updates the specified IPsec policy
5	DELETE /v2.0/vpn/ipsecpolicies/{ipsecpolicy-id} Delete IPSec policy	Deletes an IPsec policy
6	GET /v2.0/vpn/ipsec-site-connections List IPSec site connections	Lists all connections between IPsec sites
7	GET /v2.0/vpn/ipsec-site-connections/{connection-id} Show IPSec site connection details	Shows details about the connection between specified IPsec sites
8	POST /v2.0/vpn/ipsec-site-connections Create IPSec site connection	Creates an IPsec site connection
9	PUT /v2.0/vpn/ipsec-site-connections/{connection-id} Update IPSec site connection	Updates a connection between IPsec sites that is not in a PENDING state
10	DELETE /v2.0/vpn/ipsec-site-connections/{connection-id} Delete IPSec site connection	Deletes a connection between IPsec sites
11	GET /v2.0/vpn/vpnservices List VPN services	Lists VPN services
12	GET /v2.0/vpn/vpnservices/{service-id} Show VPN service details	Shows details about the specified VPN service
13	POST /v2.0/vpn/vpnservices Create VPN service	Creates a VPN service
14	PUT /v2.0/vpn/vpnservices/{service-id} Update VPN service	Updates the specified VPN service that is not in a PENDING state
15	DELETE /v2.0/vpn/vpnservices/{service-id} Delete VPN service	Deletes the specified VPN service
16	GET /v2.0/vpn/ikepolicies List IKE policies	Lists IKE policies
17	GET /v2.0/vpn/ikepolicies/{ikepolicy-id} Show IKE policy details	Shows details about the specified IKE policy
18	POST /v2.0/vpn/ikepolicies Create IKE policy	Creates an IKE policy

Item	API	Description
19	PUT /v2.0/vpn/ikepolicies/{ikepolicy-id} Update IKE policy	Updates the specified IKE policy
20	DELETE /v2.0/vpn/ikepolicies/{ikepolicy-id} Delete IKE policy	Deletes the specified IKE policy

1.4.2 General requirements

This section describes general requirements to use this API.

- Specify the name and description input parameters using up to 255 characters.
- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.
- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.4.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.4.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized

Status code	Description
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType


Caution

- If the user has insufficient privileges to issue the target API when issuing the API for showing (Show), updating (Update), or deleting (Delete) resources, the status code 404 may be returned.
- If the user has insufficient privileges to issue the target API when issuing the API for listing (List) resources, the status code 200 will be returned and a null array will be set in the body. If there are resources with the shared attribute set to "True", information on the target resources only will be returned.

1.4.5 API options

1.4.5.1 API options

Two options are available for APIs that retrieve resource information (List, Show).

1.4.5.2 filter

Filters can be specified to retrieve only resources matching the specified attributes from the list of resource information to be retrieved.

Multiple attributes can be specified using AND as a condition.

This option can only be used for the List API.

Execution example:

- Retrieve the network with the name "private"

  GET /v2.0/networks?name=private
- To filter using multiple attributes with AND. Retrieve the network with the name "private" and that belongs to the AZ1 availability zone.

  GET /v2.0/networks?name=private?availability_zone=AZ1

1.4.5.3 Column Selection

The attributes that are retrieved from the resource information can be restricted.

This option can only be used for the List and Show APIs.

Execution example:

- List only the id attribute of networks

  GET /v2.0/networks?fields=id
- To retrieve multiple attributes (id and name)

  GET /v2.0/networks?fields=id&fields=name

1.4.5.4 APIs that do not support these options

These options are not supported by the following APIs.

- *Show Network Connector Pool* on page 31
- *List Network Connector Pools* on page 32
- *Show Network Connector* on page 35
- *List Network Connectors* on page 36
- *Show Network Connector Endpoint* on page 43
- *List Network Connector Endpoints* on page 44
- *List Connected Interfaces of Network Connector Endpoint* on page 50

1.4.6 API details

1.4.6.1 Create router

Creates a logical router.

URI

/v2.0/routers

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
name	The router name.	xsd:string	Optional
admin_state_up	The administrative state of the router, which is up (true) or down (false).	xsd:bool	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Caution

Do not specify external_gateway_info.

Example request

```
{
    "router": {
        "name": "another_router",
        "admin_state_up": true,
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "router": {
        "status": "ACTIVE",
        "external_gateway_info": null,
        "name": "another_router",
        "admin_state_up": true,
        "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
        "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
router	A router object.
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
id	The router ID.
availability_zone	The Availability Zone name

1.4.6.2 Show router details

Shows details for a specified router.

URI

/v2.0/routers/{router_id}

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "router": {
        "status": "ACTIVE",
        "external_gateway_info": null,
        "name": "another_router",
        "admin_state_up": true,
        "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
        "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
        "routes": [
            {
                "nexthop": "10.1.0.10",
                "destination": "40.0.1.0/24"
            }
        ],
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
router	A router object.
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
id	The router ID.
routes	List of dictionary(static route definitions) in this format:

Item	Description

	<pre>[
	  {
	  "nexthop":"IPADDRESS",
	  "destination":"CIDR"
	  }
	]</pre>
	Static route definitions:
	next_hop is the IP address of the next hop.
	destination is the destination CIDR.

availability_zone	The Availability Zone name

1.4.6.3 Delete router

Deletes a logical router and, if present, its external gateway interface.

URI

/v2.0/routers/{router_id}

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes
serviceUnavailable (503)	Error response codes Caution If 503 error message returned, when external gateway is being configured. Please try it again about 2 minutes later.

1.4.6.4 Update router

Updates a logical router.

URI

/v2.0/routers/{router_id}

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/ optional
external_gateway_info	The network_id, for the external gateway.	xsd:dict	Optional
name	The router name.	xsd:string	Optional
admin_state_up	The administrative state of the router, which is up (true) or down (false).	xsd:bool	Optional

Caution

Do not specify external_gateway_info.

Example request

```
{
    "router": {
        "external_gateway_info": {
            "network_id": "8ca37218-28ff-41cb-9b10-039601ea7e6b"
        }
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
serviceUnavailable (503)	Error response codes Caution If 503 error message returned, when external gateway is being configured. Please try it again about 2 minutes later.

Response body (normal status)

```
{
```

```
    "router": {
        "status": "ACTIVE",
        "external_gateway_info": {
            "network_id": "8ca37218-28ff-41cb-9b10-039601ea7e6b"
        },
        "name": "another_router",
        "admin_state_up": true,
        "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
        "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
        "routes": [
            {
                "nexthop": "10.1.0.10",
                "destination": "40.0.1.0/24"
            }
        ],
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
router	A router object.
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
id	The router ID.
routes	List of dictionary(static route definitions) in this format: `[ { "nexthop":"IPADDRESS", "destination":"CIDR" } ]` Static route definitions: next_hop is the IP address of the next hop. destination is the destination CIDR.
availability_zone	The Availability Zone name

1.4.6.5 Add interface to router

Adds an internal interface to a logical router.

URI

/v2.0/routers/{router_id}/add_router_interface

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
subnet_id	The subnet ID. (exclusive with port_id)	csapi:UUID	Optional
port_id	The port ID. (exclusive with subnet_id)	csapi:UUID	Optional

You must specify either subnet_id or port_id

Caution

Example request

```
{
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1"
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1",
    "port_id": "3a44f4e5-1694-493a-a1fb-393881c673a4",
    "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
    "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
    "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
subnet_id	The subnet ID.

Item	Description
port_id	The port ID.
tenant_id	The tenant ID.
id	The router ID.
availability_zone	The Availability Zone name

1.4.6.6 Remove interface from router

Removes an internal interface from a logical router.

URI

/v2.0/routers/{router_id}/remove_router_interface

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
subnet_id	The subnet ID.	csapi:UUID	Optional
port_id	The port ID.	csapi:UUID	Optional

You must specify either subnet_id or port_id

Caution

Example request

```
{
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1"
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
    "tenant_id": "2f245a7b-796b-4f26-9cf9-9e82d248fda7",
    "port_id": "3a44f4e5-1694-493a-a1fb-393881c673a4",
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1",
    "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
id	The router ID.
tenant_id	The tenant ID.
port_id	The port ID.
subnet_id	The subnet ID.
availability_zone	The Availability Zone name

1.4.6.7 List routers

Lists logical routers that are accessible to the tenant who submits the request.

URI

/v2.0/routers

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)

```
{
 "routers": [
  {
   "status": "ACTIVE",
   "external_gateway_info": null,
   "name": "second_routers",
   "admin_state_up": true,
   "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
   "id": "7177abc4-5ae9-4bb7-b0d4-89e94a4abf3b",
   "routes": [
    {
     "nexthop": "10.1.0.10",
     "destination": "40.0.1.0/24"
```

```
    }
   ],
   "availability_zone": "AZ1"
  },
  {
  "status": "ACTIVE",
  "external_gateway_info": {
   "network_id": "3c5bcddd-6af9-4e6b-9c3e-c153e521cab8"
  },
  "name": "router1",
  "admin_state_up": true,
  "tenant_id": "33a40233088643acb66ff6eb0ebea679",
  "id": "a9254bdb-2613-4a13-ac4c-adc581fba50d",
   "routes": [
    {
     "nexthop": "11.1.0.10",
     "destination": "41.0.1.0/24"
    }
   ],
   "availability_zone": "AZ1"
  }
 ]
}
```

Description of response body (normal status)

Item	Description
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
id	The router ID.
routes	List of dictionary(static route definitions) in this format: `[ { "nexthop":"IPADDRESS", "destination":"CIDR" } ]` Static route definitions: next_hop is the IP address of the next hop. destination is the destination CIDR.
availability_zone	The Availability Zone name

1.4.6.8 Update extra route

Updates logical router with routes attribute.

URI

/v2.0/routers/{router_id}

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
routes	Extra route configuration		
nexthop	The IP address of the next hop.	xsd:string	Optional
destination	The destination CIDR.  Caution Don't specify same CIDR that the router interface belongs to.	xsd:string	Optional

Example request

```
{
   "router":{
      "routes":[
         {
            "nexthop":"10.1.0.10",
            "destination":"40.0.1.0/24"
         }
      ]
   }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes

Response body (normal status)

```
{"router":
    {"status": "ACTIVE",
     "external_gateway_info": {"network_id": "5c26e0bb-
a9a9-429c-9703-5c417a221096"},
```

```
    "name": "router1",
    "admin_state_up": true,
    "tenant_id": "936fa220b2c24a87af51026439af7a3e",
    "routes": [{"nexthop": "10.1.0.10", "destination": "40.0.1.0/24"}],
    "id": "babc8173-46f6-4b6f-8b95-38c1683a4e22"},
    "availability_zone": "AZ1"}
}
```

Description of response body (normal status)

Item	Description
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
routes	
id	The router ID.
availability_zone	The Availability Zone name.

1.4.6.9 List IPSec policies

Lists IPSec policies.

URI

/v2.0/vpn/ipsecpolicies

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)

```
{
  "ipsecpolicies": [
    {
      "name": "ipsecpolicy1",
      "transform_protocol": "esp",
      "auth_algorithm": "sha1",
      "encapsulation_mode": "tunnel",
```

```
      "encryption_algorithm": "aes-128",
      "pfs": "group14",
      "tenant_id": "ccb81365fe36411a9011e90491fe1330",
      "lifetime": {
        "units": "seconds",
        "value": 3600
      },
      "id": "5291b189-fd84-46e5-84bd-78f40c05d69c",
      "description": "",
      "availability_zone": "AZ1"
    }
  ]
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IPsec policy.
transform_protocol	Transform protocol used: esp.
auth_algorithm	Authentication algorithm: sha1.
encapsulation_mode	Encapsulation mode: tunnel.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, or aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
tenant_id	Unique identifier for owner of the VPN service.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
id	Unique identifier for the IPsec policy.
description	Description of the IPSec policy.
availability_zone	The Availability Zone name.

Response body (error status)

```
{
  "NeutronError": "network service is unavailable in
 availability_zone(AZ1)",
  "request_id": "73b014c9-10ab-4e3b-b281-05feae513c02"
}
```

Description of response body (error status)

Item	Description
NeutronError	Error messages
request_id	Request ID

1.4.6.10 Show IPSec policy details

Shows details for a specified IPSec policy.

URI

/v2.0/vpn/ipsecpolicies/{ipsecpolicy-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "ipsecpolicy": {
    "name": "ipsecpolicy1",
    "transform_protocol": "esp",
    "auth_algorithm": "sha1",
    "encapsulation_mode": "tunnel",
    "encryption_algorithm": "aes-128",
    "pfs": "group14",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "lifetime": {
      "units": "seconds",
      "value": 3600
    },
    "id": "5291b189-fd84-46e5-84bd-78f40c05d69c",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IPsec policy.
transform_protocol	Transform protocol used: esp.
auth_algorithm	Authentication algorithm: sha1.
encapsulation_mode	Encapsulation mode: tunnel.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, or aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
tenant_id	Unique identifier for owner of the VPN service.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
id	Unique identifier for the IPsec policy.

Item	Description
description	Description of the IPSec policy.
availability_zone	The Availability Zone name.

1.4.6.11 Create IPSec Policy

Creates an IPSec policy.

URI

/v2.0/vpn/ipsecpolicies

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
name	Friendly name for the IPsec policy.	string	Optional
transform_protocol	Transform protocol used: esp. (default: esp)	string	Optional
auth_algorithm	Authentication algorithm: sha1. (default: sha1)	string	Optional
encapsulation_mode	Encapsulation mode: tunnel. (default: tunnel)	string	Optional
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, or aes-192. (default: aes-128)	string	Optional
pfs	Perfect Forward Secrecy: group2, group5, or group14. (default: group5)	string	Optional
lifetime	Lifetime of the SA. Units in 'seconds'. The time should be from 60 seconds to 86400 seconds. Either units or value may be omitted. (default: {'units' : 'seconds', 'value' : 3600})	dict	Optional
description	Description of the IPSec policy.	string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
  "ipsecpolicy": {
    "name": "ipsecpolicy1",
    "transform_protocol": "esp",
    "auth_algorithm": "sha1",
    "encapsulation_mode": "tunnel",
    "encryption_algorithm": "aes-128",
    "pfs": "group5",
    "lifetime": {
      "units": "seconds",
      "value": 7200    },
    "availability_zone": "AZ1"
  }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes

Response body (normal status)

```
{
  "ipsecpolicy": {
    "name": "ipsecpolicy1",
    "transform_protocol": "esp",
    "auth_algorithm": "sha1",
    "encapsulation_mode": "tunnel",
    "encryption_algorithm": "aes-128",
    "pfs": "group5",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "lifetime": {
      "units": "seconds",
      "value": 7200
    },
    "id": "5291b189-fd84-46e5-84bd-78f40c05d69c",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IPsec policy.
transform_protocol	Transform protocol used: esp.
auth_algorithm	Authentication algorithm: sha1.
encapsulation_mode	Encapsulation mode: tunnel.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, or aes-192.

Item	Description
pfs	Perfect Forward Secrecy: group2, group5, or group14.
tenant_id	Unique identifier for owner of the VPN service.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
id	Unique identifier for the IPsec policy.
description	Description of the IPSec policy.
availability_zone	The Availability Zone name.

1.4.6.12 Update IPSec Policy

Updates an IPSec policy.

URI

/v2.0/vpn/ipsecpolicies/{ipsecpolicy-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/ optional
name	Friendly name for the IPsec policy.	string	Optional
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.	string	Optional
pfs	Perfect Forward Secrecy: group2, group5, or group14.	string	Optional
lifetime	Lifetime of the SA. Units in 'seconds'. The time should be from 60 seconds to 86400 seconds. Either units or value may be omitted. (default: {'units' : 'seconds', 'value' : 3600})	dict	Optional
description	Description of the IPSec policy.	string	Optional

Example request

```
{
  "ipsecpolicy": {
    "pfs": "group14"
  }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)


```
{
  "ipsecpolicy": {
    "name": "ipsecpolicy1",
    "transform_protocol": "esp",
    "auth_algorithm": "sha1",
    "encapsulation_mode": "tunnel",
    "encryption_algorithm": "aes-128",
    "pfs": "group14",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "lifetime": {
      "units": "seconds",
      "value": 3600
    },
    "id": "5291b189-fd84-46e5-84bd-78f40c05d69c",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```


Description of response body (normal status)

Item	Description
name	Friendly name for the IPsec policy.
transform_protocol	Transform protocol used: esp.
auth_algorithm	Authentication algorithm: sha1.
encapsulation_mode	Encapsulation mode: tunnel.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, or aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
tenant_id	Unique identifier for owner of the VPN service.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
id	Unique identifier for the IPsec policy.
description	Description of the IPSec policy.
availability_zone	The Availability Zone name.

1.4.6.13 Delete IPSec policy

Deletes an IPSec policy.

URI

/v2.0/vpn/ipsecpolicies/{ipsecpolicy-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes

1.4.6.14 List IPSec site connections

Lists IPSec site-to-site connections.

URI

/v2.0/vpn/ipsec-site-connections

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)


```
{
  "ipsec_site_connections": [
    {
      "status": "PENDING_CREATE",
      "psk": "secret",
      "initiator": "bi-directional",
      "name": "vpnconnection1",
      "admin_state_up": true,
      "tenant_id": "ccb81365fe36411a9011e90491fe1330",
      "description": "",
      "auth_mode": "psk",
      "peer_cidrs": [
        "10.1.0.0/24"
      ],
      "mtu": 1500,
      "ikepolicy_id": "bf5612ac-15fb-460c-9b3d-6453da2fafa2",
```

```
      "dpd": {
        "action": "hold",
        "interval": 30,
        "timeout": 120
      },
      "route_mode": "static",
      "vpnservice_id": "c2f3178d-5530-4c4a-89fc-050ecd552636",
      "peer_address": "172.24.4.226",
      "peer_id": "172.24.4.226",
      "id": "cbc152a0-7e93-4f98-9f04-b085a4bf2511",
      "ipsecpolicy_id": "8ba867b2-67eb-4835-bb61-c226804a1584",
      "availability_zone": "AZ1"
    }
  ]
}
```


Description of response body (normal status)

Item	Description
status	Indicates whether VPN connection is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
psk	Pre Shared Key: any string.
initiator	Whether this VPN can only respond to connections or can initiate as well.
name	Name for IPSec site-to-site connection.
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets.
tenant_id	Unique identifier for owner of the VPN service.
description	Description of the IPSec site-to-site connection.
auth_mode	Authentication mode: psk.
peer_cidrs	Peer private CIDRs.
mtu	Maximum Transmission Unit to address fragmentation.
ikepolicy_id	Unique identifier of IKE policy.
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds.
route_mode	Route mode: static. This will be extended in the future.
vpnservice_id	Unique identifier of VPN service.
peer_address	Peer gateway public IPv4 address.
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.
id	Unique identifier for the IPSec site-to-site connection.
ipsecpolicy_id	Unique identifier of IPSec policy.
availability_zone	The Availability Zone name.

Caution If the status does not become ACTIVE after creating resources, even though the connection destination settings have been completed, check if the following parameters match the information of the connection destination.

- IKE Policy
  - encryption_algorithm
  - pfs
  - lifetime
- IPSec Policy
  - encryption_algorithm
  - pfs
  - lifetime
- IPSec site connection
  - psk
  - peer_cidrs
  - peer_address
  - peer_id

1.4.6.15 Show IPSec site connection details

Shows details about a specified IPSec site-to-site connection.

URI

/v2.0/vpn/ipsec-site-connections/{connection-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)


```
{
  "ipsec_site_connection": {
    "status": "PENDING_CREATE",
    "psk": "secret",
    "initiator": "bi-directional",
    "name": "vpnconnection1",
    "admin_state_up": true,
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "description": "",
    "auth_mode": "psk",
    "peer_cidrs": [
      "10.1.0.0/24"
    ],
    "mtu": 1500,
    "ikepolicy_id": "bf5612ac-15fb-460c-9b3d-6453da2fafa2",
```

```
    "dpd": {
      "action": "hold",
      "interval": 30,
      "timeout": 120
    },
    "route_mode": "static",
    "vpnservice_id": "c2f3178d-5530-4c4a-89fc-050ecd552636",
    "peer_address": "172.24.4.226",
    "peer_id": "172.24.4.226",
    "id": "cbc152a0-7e93-4f98-9f04-b085a4bf2511",
    "ipsecpolicy_id": "8ba867b2-67eb-4835-bb61-c226804a1584",
    "availability_zone": "AZ1"
  }
}
```


Description of response body (normal status)

Item	Description
status	Indicates whether VPN connection is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
psk	Pre Shared Key: any string.
initiator	Whether this VPN can only respond to connections or can initiate as well.
name	Name for IPSec site-to-site connection.
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets.
tenant_id	Unique identifier for owner of the VPN service.
description	Description of the IPSec site-to-site connection.
auth_mode	Authentication mode: psk.
peer_cidrs	Peer private CIDRs.
mtu	Maximum Transmission Unit to address fragmentation.
ikepolicy_id	Unique identifier of IKE policy.
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds.
route_mode	Route mode: static. This will be extended in the future.Unique identifier of VPN service.
vpnservice_id	Unique identifier of VPN service.
peer_address	Peer gateway public IPv4 address.
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.
id	Unique identifier for the IPSec site-to-site connection.
ipsecpolicy_id	Unique identifier of IPSec policy.
availability_zone	The Availability Zone name.

Caution If the status does not become ACTIVE after creating resources, even though the connection destination settings have been completed, check the items in the notes in "*List IPSec site connections* on page 102".

1.4.6.16 Create IPSec site connection

Creates an IPSec site connection.

URI

/v2.0/vpn/ipsec-site-connections

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
psk	Pre Shared Key: any string.	string	Required
initiator	Whether this VPN can only respond to connections or can initiate as well. Select bi-directional or response-only (default: bi-directional)	string	Optional
ipsecpolicy_id	Unique identifier of IPSec policy.	uuid-str	Required
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets. (default: true)	bool	Optional
peer_cidrs	Peer private CIDRs. unique list of valid cidr in the form <net_address>/<prefix>. Only one cidr can be specifed.	list	Required
ikepolicy_id	Unique identifier of IKE policy.	uuid-str	Required
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds. (default: {'action' : 'hold', 'interval' : 30, 'timeout' : 120)	dict	Optional
vpnservice_id	Unique identifier of VPN service.	uuid-str	Required
peer_address	Peer gateway public IPv4 address.	string	Required
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.	string	Required

Key	Description	Type	Required/optional
name	Name for IPSec site-to-site connection.	string	Optional
description	Description of the IPSec site-to-site connection.	string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
  "ipsec_site_connection": {
    "psk": "secret",
    "initiator": "bi-directional",
    "ipsecpolicy_id": "22b8abdc-e822-45b3-90dd-f2c8512acfa5",
    "admin_state_up": true,
    "peer_cidrs": [
      "10.2.0.0/24"
    ],
    "ikepolicy_id": "d3f373dc-0708-4224-b6f8-676adf27dab8",
    "dpd": {
      "action": "hold",
      "interval": 60,
      "timeout": 240
    },
    "vpnservice_id": "7b347d20-6fa3-4e22-b744-c49ee235ae4f",
    "peer_address": "172.24.4.233",
    "peer_id": "172.24.4.233",
    "name": "vpnconnection1",
    "availability_zone": "AZ1"
  }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes

Response body (normal status)

```
{
  "ipsec_site_connection": {
    "status": "PENDING_CREATE",
    "psk": "secret",
    "initiator": "bi-directional",
    "name": "vpnconnection1",
    "admin_state_up": true,
    "tenant_id": "b6887d0b45b54a249b2ce3dee01caa47",
    "description": "",
    "auth_mode": "psk",
    "peer_cidrs": [
      "10.2.0.0/24"
```

```
    ],
    "mtu": 1500,
    "ikepolicy_id": "d3f373dc-0708-4224-b6f8-676adf27dab8",
    "dpd": {
      "action": "hold",
      "interval": 60,
      "timeout": 240
    },
    "route_mode": "static",
    "vpnservice_id": "7b347d20-6fa3-4e22-b744-c49ee235ae4f",
    "peer_address": "172.24.4.233",
    "peer_id": "172.24.4.233",
    "id": "af44dfd7-cf91-4451-be57-cd4fdd96b5dc",
    "ipsecpolicy_id": "22b8abdc-e822-45b3-90dd-f2c8512acfa5",
    "availability_zone": "AZ1"
  }
}
```


Description of response body (normal status)

Item	Description
status	Indicates whether VPN connection is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
psk	Pre Shared Key: any string.
initiator	Whether this VPN can only respond to connections or can initiate as well.
name	Name for IPSec site-to-site connection.
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets.
tenant_id	Unique identifier for owner of the VPN service.
description	Description of the IPSec site-to-site connection.
auth_mode	Authentication mode: psk.
peer_cidrs	Peer private CIDRs.
mtu	Maximum Transmission Unit to address fragmentation.
ikepolicy_id	Unique identifier of IKE policy.
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds.
route_mode	Route mode: static. This will be extended in the future.
vpnservice_id	Unique identifier of VPN service.
peer_address	Peer gateway public IPv4 address.
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.
id	Unique identifier for the IPSec site-to-site connection.
ipsecpolicy_id	Unique identifier of IPSec policy.
availability_zone	The Availability Zone name.

Caution If the status does not become ACTIVE after creating resources, even though the connection destination settings have been completed, check the items in the notes in "*List IPSec site connections* on page 102".

1.4.6.17 Update IPSec site connection

Updates an IPSec site-to-site connection, provided status is not indicating a PENDING_* state.

URI

/v2.0/vpn/ipsec-site-connections/{connection-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
psk	Pre Shared Key: any string.	string	Optional
initiator	Whether this VPN can only respond to connections or can initiate as well. Select bi-directional or response-only (default: bi-directional)	string	Optional
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets.	bool	Optional
peer_cidrs	Peer private CIDRs. unique list of valid cidr in the form <net_address>/<prefix>. Only one cidr can be specifed.	list	Optional
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds. (default: {'action' : 'hold', 'interval' : 30, 'timeout' : 120)	dict	Optional
peer_address	Peer gateway public IPv4 address.	string	Optional
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.	string	Optional
name	Name for IPSec site-to-site connection.	string	Optional
description	Description of the IPSec site-to-site connection.	string	Optional

Example request

```
{
  "ipsec_site_connection": {
    "description": "to datacenter2"
  }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "ipsec_site_connection": {
    "status": "DOWN",
    "psk": "secret",
    "initiator": "bi-directional",
    "name": "vpnconnection1",
    "admin_state_up": true,
    "tenant_id": "26de9cd6cae94c8cb9f79d660d628e1f",
    "description": " to datacenter2",
    "auth_mode": "psk",
    "peer_cidrs": [
      "10.2.0.0/24"
    ],
    "mtu": 1500,
    "ikepolicy_id": "771f081c-5ec8-4f9a-b041-015dfb7fbbe2",
    "dpd": {
      "action": "hold",
      "interval": 30,
      "timeout": 120
    },
    "route_mode": "static",
    "vpnservice_id": "41bfef97-af4e-4f6b-a5d3-4678859d2485",
    "peer_address": "172.24.4.233",
    "peer_id": "172.24.4.233",
    "id": "f7cf7305-f491-45f4-ad9c-8e7240fe3d72",
    "ipsecpolicy_id": "9958d4fe-3719-4e8c-84e7-9893895b76b4",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
status	Indicates whether VPN connection is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
psk	Pre Shared Key: any string.

Item	Description
initiator	Whether this VPN can only respond to connections or can initiate as well.
name	Name for IPSec site-to-site connection.
admin_state_up	Administrative state of VPN connection. If false (down), VPN connection does not forward packets.
tenant_id	Unique identifier for owner of the VPN service.
description	Description of the IPSec site-to-site connection.
auth_mode	Authentication mode: psk.
peer_cidrs	Peer private CIDRs.
mtu	Maximum Transmission Unit to address fragmentation.
ikepolicy_id	Unique identifier of IKE policy.
dpd	Dead Peer Detection protocol controls. Action: hold or restart. Interval and timeout in seconds.
route_mode	Route mode: static. This will be extended in the future.
vpnservice_id	Unique identifier of VPN service.
peer_address	Peer gateway public IPv4 address.
peer_id	Peer router identity for authentication. Can be IPv4/IPv6 address, e-mail address, key id, or FQDN.
id	Unique identifier for the IPSec site-to-site connection.
ipsecpolicy_id	Unique identifier of IPSec policy.
availability_zone	The Availability Zone name.

Caution If the status does not become ACTIVE after updating resources, even though the connection destination settings have been completed, check the items in the notes in "*List IPSec site connections* on page 102".

1.4.6.18 Delete IPSec site connection

Deletes an IPSec site-to-site connection.

URI

/v2.0/vpn/ipsec-site-connections/{connection-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes

Status code	Description
Not Found (404)	Error response codes
Conflict (409)	Error response codes

1.4.6.19 List VPN services

Lists VPN services.

URI

/v2.0/vpn/vpnservices

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)

```
{
  "vpnservices": [
    {
      "router_id": "ec8619be-0ba8-4955-8835-3b49ddb76f89",
      "status": "PENDING_CREATE",
      "name": "myservice",
      "admin_state_up": true,
      "subnet_id": "f4fb4528-ed93-467c-a57b-11c7ea9f963e",
      "tenant_id": "ccb81365fe36411a9011e90491fe1330",
      "id": "9faaf49f-dd89-4e39-a8c6-101839aa49bc",
      "description": "",
      "availability_zone": "AZ1"
    }
  ]
}
```

Description of response body (normal status)

Item	Description
router_id	Router ID to which the VPN service is inserted.
status	Indicates whether IPsec VPN service is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
name	Human readable name for the VPN service. Does not have to be unique.

Item	Description
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.
subnet_id	The subnet on which the tenant wants the VPN service.
tenant_id	Owner of the VPN service. Only admin users can specify a tenant identifier other than their own.
id	Unique identifier for the VPN Service object.
description	Human readable description for the VPN service.
availability_zone	The Availability Zone name.

1.4.6.20 Show VPN service details

Shows details about a specified VPN service.

URI

/v2.0/vpn/vpnservices/{service-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "vpnservice": {
    "router_id": "ec8619be-0ba8-4955-8835-3b49ddb76f89",
    "status": "PENDING_CREATE",
    "name": "myservice",
    "admin_state_up": true,
    "subnet_id": "f4fb4528-ed93-467c-a57b-11c7ea9f963e",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "id": "9faaf49f-dd89-4e39-a8c6-101839aa49bc",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
router_id	Router ID to which the VPN service is inserted.
status	Indicates whether IPsec VPN service is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
name	Human readable name for the VPN service. Does not have to be unique.
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.
subnet_id	The subnet on which the tenant wants the VPN service.
tenant_id	Owner of the VPN service. Only admin users can specify a tenant identifier other than their own.
id	Unique identifier for the VPN Service object.
description	Human readable description for the VPN service.
availability_zone	The Availability Zone name

1.4.6.21 Create VPN service

Creates a VPN service.

URI

/v2.0/vpn/vpnservices

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
subnet_id	The subnet on which the tenant wants the VPN service.	uuid-str	Required
router_id	Router ID to which the VPN service is inserted.	uuid-str	Required
name	Human readable name for the VPN service. Does not have to be unique.	string	Optional
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.	bool	Optional
description	Human readable description for the VPN service.	string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
  "vpnservice": {
    "subnet_id": "f4fb4528-ed93-467c-a57b-11c7ea9f963e",
    "router_id": "ec8619be-0ba8-4955-8835-3b49ddb76f89",
    "name": "myservice",
    "admin_state_up": true,
    "availability_zone": "AZ1"
  }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes

Response body (normal status)

```
{
  "vpnservice": {
    "router_id": "ec8619be-0ba8-4955-8835-3b49ddb76f89",
    "status": "PENDING_CREATE",
    "name": "myservice",
    "admin_state_up": true,
    "subnet_id": "f4fb4528-ed93-467c-a57b-11c7ea9f963e",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "id": "9faaf49f-dd89-4e39-a8c6-101839aa49bc",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
router_id	Router ID to which the VPN service is inserted.
status	Indicates whether IPsec VPN service is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
name	Human readable name for the VPN service. Does not have to be unique.
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.
subnet_id	The subnet on which the tenant wants the VPN service.
tenant_id	Owner of the VPN service. Only admin users can specify a tenant identifier other than their own.
id	Unique identifier for the VPN Service object.

Item	Description
description	Human readable description for the VPN service.
availability_zone	The Availability Zone name

1.4.6.22 Update VPN service

Updates a VPN service, provided status is not indicating a PENDING_* state.

URI

/v2.0/vpn/vpnservices/{service-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
name	Human readable name for the VPN service. Does not have to be unique.	string	Optional
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.	bool	Optional
description	Human readable description for the VPN service.	string	Optional

Example request

```
{
  "vpnservice": {
    "description": "Updated description"
  }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "vpnservice": {
```

```
    "router_id": "881b7b30-4efb-407e-a162-5630a7af3595",
    "status": "ACTIVE",
    "name": "myvpn",
    "admin_state_up": true,
    "subnet_id": "25f8a35c-82d5-4f55-a45b-6965936b33f6",
    "tenant_id": "26de9cd6cae94c8cb9f79d660d628e1f",
    "id": "41bfef97-af4e-4f6b-a5d3-4678859d2485",
    "description": "Updated description",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
router_id	Router ID to which the VPN service is inserted.
status	Indicates whether IPsec VPN service is currently operational. Possible values include: ACTIVE, DOWN, BUILD, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
name	Human readable name for the VPN service. Does not have to be unique.
admin_state_up	Administrative state of the vpnservice. If false (down), port does not forward packets.
subnet_id	The subnet on which the tenant wants the VPN service.
tenant_id	Owner of the VPN service. Only admin users can specify a tenant identifier other than their own.
id	Unique identifier for the VPN Service object.
description	Human readable description for the VPN service.
availability_zone	The Availability Zone name.

1.4.6.23 Delete VPN service

Deletes a VPN service.

URI

/v2.0/vpn/vpnservices/{service-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes

1.4.6.24 List IKE policies

Lists IKE policies.

URI

/v2.0/vpn/ikepolicies

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)

```
{
  "ikepolicies": [
    {
      "name": "ikepolicy1",
      "tenant_id": "ccb81365fe36411a9011e90491fe1330",
      "auth_algorithm": "sha1",
      "encryption_algorithm": "aes-256",
      "pfs": "group5",
      "phase1_negotiation_mode": "main",
      "lifetime": {
        "units": "seconds",
        "value": 3600
      },
      "ike_version": "v1",
      "id": "5522aff7-1b3c-48dd-9c3c-b50f016b73db",
      "description": "",
      "availability_zone": "AZ1"
    }
  ]
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IKE policy.
tenant_id	Unique identifier for owner of the VPN service.
auth_algorithm	Authentication Hash algorithms: sha1.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
phase1_negotiation_mode	IKE mode: main.

Item	Description
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
ike_version	Version: v1.
id	Unique identifier for the IKE policy.
description	Description of the IKE policy.
availability_zone	The Availability Zone name.

1.4.6.25 Show IKE policy details

Shows details for a specified IKE policy.

URI

/v2.0/vpn/ikepolicies/{ikepolicy-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)


```
{
  "ikepolicy": {
    "name": "ikepolicy1",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "auth_algorithm": "sha1",
    "encryption_algorithm": "aes-256",
    "pfs": "group5",
    "phase1_negotiation_mode": "main",
    "lifetime": {
      "units": "seconds",
      "value": 3600
    },
    "ike_version": "v1",
    "id": "5522aff7-1b3c-48dd-9c3c-b50f016b73db",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IKE policy.
tenant_id	Unique identifier for owner of the VPN service.
auth_algorithm	Authentication Hash algorithms: sha1.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
phase1_negotiation_mode	IKE mode: main.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
ike_version	Version: v1.
id	Unique identifier for the IKE policy.
description	Description of the IKE policy.
availability_zone	The Availability Zone name.

1.4.6.26 Create IKE policy

Creates an IKE policy.

URI

/v2.0/vpn/ikepolicies

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
phase1_negotiation_mode	IKE mode: main. (default: main)	string	Optional
auth_algorithm	Authentication Hash algorithms: sha1. (default: sha1)	string	Optional
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192 (default: aes-128)	string	Optional
pfs	Perfect Forward Secrecy: group2, group5, or group14. (default: group5)	string	Optional
lifetime	Lifetime of the SA. Units in 'seconds'. The time should be from	dict	Optional

Key	Description	Type	Required/ optional
	60 seconds to 86400 seconds. Either units or value may be omitted. (default: {'units' : 'seconds', 'value' : 2000})		
ike_version	Version: v1. (default: v1)	string	Optional
name	Friendly name for the IKE policy.	string	Optional
description	Description of the IKE policy.	string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
  "ikepolicy": {
    "phase1_negotiation_mode": "main",
    "auth_algorithm": "sha1",
    "encryption_algorithm": "aes-128",
    "pfs": "group5",
    "lifetime": {
      "units": "seconds",
      "value": 7200
    },
    "ike_version": "v1",
    "name": "ikepolicy1",
    "availability_zone": "AZ1"
  }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes

Response body (normal status)

```
{
  "ikepolicy": {
    "name": "ikepolicy1",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "auth_algorithm": "sha1",
    "encryption_algorithm": "aes-128",
    "pfs": "group5",
    "phase1_negotiation_mode": "main",
    "lifetime": {
```

```
      "units": "seconds",
      "value": 7200
    },
    "ike_version": "v1",
    "id": "5522aff7-1b3c-48dd-9c3c-b50f016b73db",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IKE policy.
tenant_id	Unique identifier for owner of the VPN service.
auth_algorithm	Authentication Hash algorithms: sha1.
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
phase1_negotiation_mode	IKE mode: main.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
ike_version	Version: v1.
id	Unique identifier for the IKE policy.
description	Description of the IKE policy.
availability_zone	The Availability Zone name.

1.4.6.27 Update IKE policy

Updates an IKE policy.

URI

/v2.0/vpn/ikepolicies/{ikepolicy-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/ optional
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.	string	Optional
pfs	Perfect Forward Secrecy: group2, group5, group14.	string	Optional
lifetime	Lifetime of the SA. Units in 'seconds'. The time should be from 60 seconds	dict	Optional

Key	Description	Type	Required/ optional
	to 86400 seconds. Either units or value may be omitted.		
name	Friendly name for the IKE policy.	string	Optional
description	Description of the IKE policy.	string	Optional

Example request

```
{
  "ikepolicy": {
    "encryption_algorithm": "aes-256"
  }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "ikepolicy": {
    "name": "ikepolicy1",
    "tenant_id": "ccb81365fe36411a9011e90491fe1330",
    "auth_algorithm": "sha1",
    "encryption_algorithm": "aes-256",
    "pfs": "group5",
    "phase1_negotiation_mode": "main",
    "lifetime": {
      "units": "seconds",
      "value": 3600
    },
    "ike_version": "v1",
    "id": "5522aff7-1b3c-48dd-9c3c-b50f016b73db",
    "description": "",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
name	Friendly name for the IKE policy.
tenant_id	Unique identifier for owner of the VPN service.
auth_algorithm	Authentication Hash algorithms: sha1.

Item	Description
encryption_algorithm	Encryption Algorithms: aes-128, aes-256, aes-192.
pfs	Perfect Forward Secrecy: group2, group5, or group14.
phase1_negotiation_mode	IKE mode: main.
lifetime	Lifetime of the SA. Units in 'seconds'. Either units or value may be omitted.
ike_version	Version: v1.
id	Unique identifier for the IKE policy.
description	Description of the IKE policy.
availability_zone	The Availability Zone name.

1.4.6.28 Delete IKE policy

Deletes an IKE policy.

URI

/v2.0/vpn/ikepolicies/{ikepolicy-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes

1.5 Firewall

1.5.1 API list

FWaaS

Item	API	Description
1	GET /v2.0/fw/firewall_rules List firewall rules	Lists all firewall rules
2	GET /v2.0/fw/firewall_rules/{firewall_rule_id} Show firewall rule details	Shows details about the specified firewall rule
3	POST /v2.0/fw/firewall_rules Create firewall rule	Creates a firewall rule
4	PUT /v2.0/fw/firewall_rules/{firewall_rule_id} Update firewall rule	Updates the specified firewall rule
5	DELETE /v2.0/fw/firewall_rules/{firewall_rule_id} Delete firewall rule	Deletes the specified firewall rule
6	GET /v2.0/fw/firewall_policies List firewall policies	Lists all firewall policies
7	GET /v2.0/fw/firewall_policies/{firewall_policy_id} Shows firewall policy details.	Shows details about the specified firewall policy
8	POST /v2.0/fw/firewall_policies Create firewall policy	Creates a firewall policy
9	PUT /v2.0/fw/firewall_policies/{firewall_policy_id} Update firewall policy	Updates the specified firewall policy
10	DELETE /v2.0/fw/firewall_policies/{firewall_policy_id} Delete firewall policy	Deletes the specified firewall policy
11	PUT /v2.0/fw/firewall_policies/{firewall_policy-id}/insert_rule Insert firewall rule in firewall policy	Inserts a firewall rule into the specified firewall policy
12	PUT /v2.0/fw/firewall_policies/{firewall_policy-id}/remove_rule Remove firewall rule from firewall policy	Removes firewall rule from the specified firewall policy

Item	API	Description
13	GET /v2.0/fw/firewalls List firewalls	Lists all firewalls
14	GET /v2.0/fw/firewalls/{firewall-id} Shows firewall details.	Shows details about the specified firewall
15	POST /v2.0/fw/firewalls Create firewall	Creates a firewall
16	PUT /v2.0/fw/firewalls/{firewall-id} Update firewall	Updates the specified firewall
17	PUT /v2.0/fw/firewalls/{firewall-id}/reset_connections Update firewall(Connection reset)	Deletes all connections managed by the specified firewall
18	DELETE /v2.0/fw/firewalls/{firewall-id} Delete firewall	Deletes the specified firewall

1.5.2 General requirements

This section describes general requirements to use this API.

- Specify the name and description input parameters using up to 255 characters.
- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.
- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.5.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.5.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType


Caution

- If the user has insufficient privileges to issue the target API when issuing the API for showing (Show), updating (Update), or deleting (Delete) resources, the status code 404 may be returned.
- If the user has insufficient privileges to issue the target API when issuing the API for listing (List) resources, the status code 200 will be returned and a null array will be set in the body. If there are resources with the shared attribute set to "True", information on the target resources only will be returned.

1.5.5 API options

1.5.5.1 API options

Two options are available for APIs that retrieve resource information (List, Show).

1.5.5.2 filter

Filters can be specified to retrieve only resources matching the specified attributes from the list of resource information to be retrieved.

Multiple attributes can be specified using AND as a condition.

This option can only be used for the List API.

Execution example:

- Retrieve the network with the name "private"

GET /v2.0/networks?name=private

- To filter using multiple attributes with AND. Retrieve the network with the name "private" and that belongs to the AZ1 availability zone.

  GET /v2.0/networks?name=private?availability_zone=AZ1

1.5.5.3 Column Selection

The attributes that are retrieved from the resource information can be restricted.

This option can only be used for the List and Show APIs.

Execution example:

- List only the id attribute of networks

  GET /v2.0/networks?fields=id

- To retrieve multiple attributes (id and name)

  GET /v2.0/networks?fields=id&fields=name

1.5.5.4 APIs that do not support these options

These options are not supported by the following APIs.

- *Show Network Connector Pool* on page 31
- *List Network Connector Pools* on page 32
- *Show Network Connector* on page 35
- *List Network Connectors* on page 36
- *Show Network Connector Endpoint* on page 43
- *List Network Connector Endpoints* on page 44
- *List Connected Interfaces of Network Connector Endpoint* on page 50

1.5.6 API details

1.5.6.1 List firewall rules

Lists firewall rules.

URI

/v2.0/fw/firewall_rules

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
unauthorized (401)	Error response codes

Response body (normal status)


```
{
    "firewall_rules": [
        {
            "action": "allow",
            "description": "",
            "destination_ip_address": null,
            "destination_port": "80",
            "enabled": true,
            "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
            "id": "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
            "ip_version": 4,
            "name": "ALLOW_HTTP",
            "position": 1,
            "protocol": "tcp",
            "shared": false,
            "source_ip_address": null,
            "source_port": null,
            "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
            "availability_zone": "AZ1"
        }
    ]
}
```


Description of response body (normal status)

Item	Description
action	Action to be performed on the traffic matching the rule (allow, deny).
description	Human readable description for the firewall Rule (1024 characters limit).
destination_ip_address	Destination IP address or CIDR.
destination_port	Destination port number or a range. If range, port numbers are separated by colon.
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy.
firewall_policy_id	This is a read-only attribute which gets populated with the uuid of the firewall policy when this firewall rule is associated with a firewall policy. A firewall rule can be associated with one firewall policy at a time. The association can however be updated to a different firewall policy. This attribute can be "null" if the rule is not associated with any firewall policy.
id	Unique identifier for the firewall rule object.
ip_version	IP Protocol Version.
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.
position	This is a read-only attribute that gets assigned to this rule when the rule is associated with a firewall policy. It indicates the position of this rule in that firewall policy. This position number starts at 1. The position can be "null" if the firewall rule is not associated with any policy.

Item	Description
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
source_ip_address	Source IP address or CIDR.
source_port	Source port number or a range. If range, port numbers are separated by colon.
tenant_id	Owner of the firewall rule. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.2 Show firewall rule details

Shows firewall rule details.

URI

/v2.0/fw/firewall_rules/{firewall_rule-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)


```
{
    "firewall_rule": {
        "action": "allow",
        "description": "",
        "destination_ip_address": null,
        "destination_port": "80",
        "enabled": true,
        "firewall_policy_id": null,
        "id": "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
        "ip_version": 4,
        "name": "ALLOW_HTTP",
        "position": null,
        "protocol": "tcp",
        "shared": false,
        "source_ip_address": null,
        "source_port": null,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
```

```
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
action	Action to be performed on the traffic matching the rule (allow, deny).
description	Human readable description for the firewall Rule (1024 characters limit).
destination_ip_address	Destination IP address or CIDR.
destination_port	Destination port number or a range. If range, port numbers are separated by colon.
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy.
firewall_policy_id	This is a read-only attribute which gets populated with the uuid of the firewall policy when this firewall rule is associated with a firewall policy. A firewall rule can be associated with one firewall policy at a time. The association can however be updated to a different firewall policy. This attribute can be "null" if the rule is not associated with any firewall policy.
id	Unique identifier for the firewall rule object.
ip_version	IP Protocol Version.
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.
position	This is a read-only attribute that gets assigned to this rule when the rule is associated with a firewall policy. It indicates the position of this rule in that firewall policy. This position number starts at 1. The position can be "null" if the firewall rule is not associated with any policy.
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
source_ip_address	Source IP address or CIDR.
source_port	Source port number or a range. If range, port numbers are separated by colon.
tenant_id	Owner of the firewall rule. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.3 Create firewall rule

Creates a firewall rule.

URI

/v2.0/fw/firewall_rules

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
action	Action to be performed on the traffic matching the rule (allow, deny).	xsd:string	Optional
destination_ip_address	Destination IP address or CIDR.	xsd:string	Optional
destination_port	Destination port number or a range. If range, port numbers are separated by colon. Specify a small port number first.	xsd:string	Optional
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy.	xsd:bool	Optional
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.	xsd:string	Optional
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp. (Avoid the use of null when specifying the protocol for Neutron FWaaS rules. Instead, create multiple rules for both 'tcp' and 'udp' protocols independently.)	xsd:string	Optional
source_ip_address	Source IP address or CIDR.	xsd:string	Optional
source_port	Source port number or a range. If range, port numbers are separated by colon.	xsd:string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
    "firewall_rule": {
        "action": "allow",
        "destination_port": "80",
        "enabled": true,
        "name": "ALLOW_HTTP",
        "protocol": "tcp",
```

```
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes

Response body (normal status)

```
{
    "firewall_rule": {
        "action": "allow",
        "description": "",
        "destination_ip_address": null,
        "destination_port": "80",
        "enabled": true,
        "firewall_policy_id": null,
        "id": "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
        "ip_version": 4,
        "name": "ALLOW_HTTP",
        "position": null,
        "protocol": "tcp",
        "shared": false,
        "source_ip_address": null,
        "source_port": null,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
action	Action to be performed on the traffic matching the rule (allow, deny).
description	Human readable description for the firewall Rule (1024 characters limit).
destination_ip_address	Destination IP address or CIDR.
destination_port	Destination port number or a range
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy
firewall_policy_id	This is a read-only attribute which gets populated with the uuid of the firewall policy when this firewall rule is associated with a firewall policy. A firewall rule can be associated with one firewall policy at a time. The association can however be updated to a different firewall policy. This attribute can be "null" if the rule is not associated with any firewall policy.

Item	Description
id	Unique identifier for the firewall rule object.
ip_version	IP Protocol Version.
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.
position	This is a read-only attribute that gets assigned to this rule when the rule is associated with a firewall policy. It indicates the position of this rule in that firewall policy. This position number starts at 1. The position can be "null" if the firewall rule is not associated with any policy.
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
source_ip_address	Source IP address or CIDR.
source_port	Source port number or a range.
availability_zone	The Availability Zone name.

1.5.6.4 Update firewall rule

Updates a firewall rule.

URI

/v2.0/fw/firewall_rules/{firewall_rule-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/ optional
action	Action to be performed on the traffic matching the rule (allow, deny).	xsd:string	Optional
destination_ip_address	Destination IP address or CIDR.	xsd:string	Optional
destination_port	Destination port number or a range. If range, port numbers are separated by colon.	xsd:string	Optional
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy.	xsd:bool	Optional

Key	Description	Type	Required/ optional
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.	xsd:string	Optional
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp. (Avoid the use of null when specifying the protocol for Neutron FWaaS rules. Instead, create multiple rules for both 'tcp' and 'udp' protocols independently.)	xsd:string	Optional
source_ip_address	Source IP address or CIDR.	xsd:string	Optional
source_port	Source port number or a range. If range, port numbers are separated by colon.	xsd:string	Optional

Example request

```
{
    "firewall_rule": {
        "enabled": true
    }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Bad Request (400)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "firewall_rule": {
        "action": "allow",
        "description": "",
        "destination_ip_address": null,
        "destination_port": "80",
        "enabled": true,
        "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "id": "8722e0e0-9cc9-4490-9660-8c9a5732fbb0",
        "ip_version": 4,
        "name": "ALLOW_HTTP",
        "position": 1,
        "protocol": "tcp",
        "shared": false,
        "source_ip_address": null,
        "source_port": null,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "availability_zone": "AZ1"
```

```
        }
}
```

Description of response body (normal status)

Item	Description
action	Action to be performed on the traffic matching the rule (allow, deny).
description	Human readable description for the firewall Rule (1024 characters limit).
destination_ip_address	Destination IP address or CIDR.
destination_port	Destination port number or a range
enabled	When set to False will disable this rule in the firewall policy. Facilitates selectively turning off rules without having to disassociate the rule from the firewall policy
firewall_policy_id	This is a read-only attribute which gets populated with the uuid of the firewall policy when this firewall rule is associated with a firewall policy. A firewall rule can be associated with one firewall policy at a time. The association can however be updated to a different firewall policy. This attribute can be "null" if the rule is not associated with any firewall policy.
id	Unique identifier for the firewall rule object.
ip_version	IP Protocol Version
name	Human readable name for the firewall rule (255 characters limit). Does not have to be unique.
position	This is a read-only attribute that gets assigned to this rule when the rule is associated with a firewall policy. It indicates the position of this rule in that firewall policy. This position number starts at 1. The position can be "null" if the firewall rule is not associated with any policy.
protocol	The protocol that is matched by the firewall rule. Valid values are null, tcp, udp, and icmp.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
source_ip_address	Source IP address or CIDR.
source_port	Source port number or a range.
tenant_id	Owner of the firewall rule. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.5 Delete firewall rule

Deletes a firewall rule.

URI

/v2.0/fw/firewall_rules/{firewall_rule-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes The Conflict error response is returned when an operation is performed while the firewall is in a PENDING state.

1.5.6.6 List firewall policies

Lists firewall policies.

URI

/v2.0/fw/firewall_policies

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)

```
{
    "firewall_policies": [
        {
            "audited": false,
            "description": "",
            "firewall_rules": [
                "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
            ],
            "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
            "name": "test-policy",
            "shared": false,
            "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.7 Shows firewall policy details.

Shows firewall policy details.

URI

/v2.0/fw/firewall_policies/{firewall_policy-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)


```
{
    "firewall_policy": {
        "audited": false,
        "description": "",
        "firewall_rules": [
            "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
        ],
```

```
        "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "name": "test-policy",
        "shared": false,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.8 Create firewall policy

Creates a firewall policy.

URI

/v2.0/fw/firewall_policies

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are	xsd:bool	Optional

Key	Description	Type	Required/optional
	changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.		
description	Human readable description for the firewall policy (1024 characters limit).	xsd:string	Optional
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.	xsd:list	Optional
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.	xsd:string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
    "firewall_policy": {
        "firewall_rules": [
            "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
        ],
        "name": "test-policy",
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
Unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "firewall_policy": {
        "audited": false,
        "description": "",
        "firewall_rules": [
            "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
        ],
        "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "name": "test-policy",
        "shared": false,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "availability_zone": "AZ1"
    }
```

```
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.9 Update firewall policy

Updates a firewall policy.

URI

/v2.0/fw/firewall_policies/{firewall_policy-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.	xsd:bool	Optional

Key	Description	Type	Required/optional
description	Human readable description for the firewall policy (1024 characters limit).	xsd:string	Optional
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.	xsd:list	Optional
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.	xsd:string	Optional

Example request

```
{
    "firewall_policy": {
        "firewall_rules": [
            "a08ef905-0ff6-4784-8374-175fffe7dade",
            "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
        ]
    }
}
```

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "firewall_policy": {
        "audited": false,
        "description": "",
        "firewall_rules": [
            "a08ef905-0ff6-4784-8374-175fffe7dade",
            "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
        ],
        "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "name": "test-policy",
        "shared": false,
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.10 Delete firewall policy

Deletes a firewall policy.

URI

/v2.0/fw/firewall_policies/{firewall_policy-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
Conflict (409)	Error response codes Conflict error code is returned the firewall policy is in use.

1.5.6.11 Insert firewall rule in firewall policy

Inserts a firewall rule in a firewall policy relative to the position of other rules.

URI

/v2.0/fw/firewall_policies/{firewall_policy-id}/insert_rule

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
firewall_rule_id	uuid of firewall rule for insertion.	xsd:uuid	Required
insert_after	Insert the specified firewall rule on firewall_rule_id after this rule.	xsd:uuid	Optional
insert_before	Insert the specified firewall rule on firewall_rule_id before this rule.	xsd:uuid	Optional

Example request

```
{
    "firewall_rule_id": "7bc34b8c-8d3b-4ada-a9c8-1f4c11c65692",
    "insert_after": "a08ef905-0ff6-4784-8374-175fffe7dade",
    "insert_before": ""
}
```

Response codes

Status code	Description
200	Normal response codes
Bad Request (400)	Error response codes Bad Request error is returned in the case the rule information is missing.
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "audited": false,
    "description": "",
    "firewall_list": [],
    "firewall_rules": [
        "a08ef905-0ff6-4784-8374-175fffe7dade",
        "7bc34b8c-8d3b-4ada-a9c8-1f4c11c65692",
        "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
    ],
    "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
    "name": "test-policy",
    "shared": false,
    "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
    "availability_zone": "AZ1"
```

```
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_list	The list of firewall uuid that associates with.this firewall policy These firewalls will implement the rules contained in this firewall policy.
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant identifier other than their own.
availability_zone	The Availability Zone name.

1.5.6.12 Remove firewall rule from firewall policy

Removes a firewall rule from a firewall policy.

URI

/v2.0/fw/firewall_policies/{firewall_policy-id}/remove_rule

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
firewall_rule_id	uuid of firewall rule for removal.	xsd:uuid	Required

Example request

```
{
    "firewall_rule_id": "7bc34b8c-8d3b-4ada-a9c8-1f4c11c65692"
}
```

Response codes

Status code	Description
200	Normal response codes
Bad Request (400)	Error response codes Bad Request error is returned if the rule information is missing or when a firewall rule is tried to be removed from a firewall policy to which it is not associated.
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "audited": false,
    "description": "",
    "firewall_list": [],
    "firewall_rules": [
        "a08ef905-0ff6-4784-8374-175fffe7dade",
        "8722e0e0-9cc9-4490-9660-8c9a5732fbb0"
    ],
    "id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
    "name": "test-policy",
    "shared": false,
    "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
    "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
audited	When set to True by the policy owner indicates that the firewall policy has been audited. This attribute is meant to aid in the firewall policy audit workflows. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.
description	Human readable description for the firewall policy (1024 characters limit)
firewall_list	The list of firewall uuid that associates with.this firewall policy These firewalls will implement the rules contained in this firewall policy.
firewall_rules	This is an ordered list of firewall rule uuids. The firewall applies the rules in the order in which they appear in this list.
id	Unique identifier for the firewall policy object.
shared	Indicates whether this firewall rule is shared across all tenants. This value is always False.
name	Human readable name for the firewall policy (255 characters limit). Does not have to be unique.

Item	Description
tenant_id	Owner of the firewall policy. Only admin users can specify a tenant
availability_zone	The Availability Zone name.

1.5.6.13 List firewalls

Lists firewalls.

URI

/v2.0/fw/firewalls

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "firewalls": [
        {
            "admin_state_up": true,
            "description": "",
            "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
            "id": "3b0ef8f4-82c7-44d4-a4fb-6177f9a21977",
            "name": "",
            "status": "ACTIVE",
            "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
            "router_id": "fe00194c-d73c-4b46-b94a-622bf28fc9e2",
            "availability_zone": "AZ1"
        }
    ]
}
```

Description of response body (normal status)

Item	Description
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.
description	Human readable description for the firewall (1024 characters limit)

Item	Description
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.
id	Unique identifier for the firewall object.
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.
status	Indicates whether firewall resource is currently operational. Possible values include: ACTIVE, DOWN, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
tenant_id	Owner of the firewall. Only admin users can specify a tenant identifier other than their own.
router_id	The ID of the router that this firewall applied.
availability_zone	The Availability Zone name.

1.5.6.14 Shows firewall details.

Shows firewall details.

URI

/v2.0/fw/firewalls/{firewall-id}

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
    "firewall": {
        "admin_state_up": true,
        "description": "",
        "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "id": "3b0ef8f4-82c7-44d4-a4fb-6177f9a21977",
        "name": "",
        "status": "ACTIVE",
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "router_id": "fe00194c-d73c-4b46-b94a-622bf28fc9e2",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.
description	Human readable description for the firewall (1024 characters limit)
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.
id	Unique identifier for the firewall object.
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.
status	Indicates whether firewall resource is currently operational. Possible values include: ACTIVE, DOWN, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
tenant_id	Owner of the firewall. Only admin users can specify a tenant identifier other than their own.
router_id	The ID of the router that this firewall applied.
availability_zone	The Availability Zone name.

1.5.6.15 Create firewall

Creates a firewall.

URI

/v2.0/fw/firewalls

HTTP method

POST

Request parameter

Key	Description	Type	Required/optional
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.	xsd:bool	Optional
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.	csapi:uuid	Optional

Key	Description	Type	Required/optional
router_id	The ID of the router that this firewall be applied. If you don't specify, the resource will be created at all routers in tenant.	xsd:string	Optional
description	Human readable description for the firewall (1024 characters limit).	xsd:string	Optional
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.	xsd:string	Optional
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ.	xsd:string	Optional

Example request

```
{
    "firewall": {
        "admin_state_up": true,
        "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "router_id": "fe00194c-d73c-4b46-b94a-622bf28fc9e2",
        "availability_zone": "AZ1"
    }
}
```

Response codes

Status code	Description
201	Normal response codes
itemNotFound (404)	Error response codes
forbidden (403)	Error response codes
Bad Request (400)	Error response codes
Unauthorized (401)	Error response codes

Response body (normal status)

```
{
    "firewall": {
        "admin_state_up": true,
        "description": "",
        "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "id": "3b0ef8f4-82c7-44d4-a4fb-6177f9a21977",
        "name": "",
        "status": "PENDING_CREATE",
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "router_id": "fe00194c-d73c-4b46-b94a-622bf28fc9e2",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.
description	Human readable description for the firewall (1024 characters limit)
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.
id	Unique identifier for the firewall object.
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.
status	Indicates whether firewall resource is currently operational. Possible values include: ACTIVE, DOWN, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
tenant_id	Owner of the firewall. Only admin users can specify a tenant identifier other than their own.
router_id	The ID of the router that this firewall applied.
availability_zone	The Availability Zone name.

1.5.6.16 Update firewall

Updates a firewall, provided status is not PENDING_*.

URI

/v2.0/fw/firewalls/{firewall-id}

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.	xsd:bool	Optional
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.	csapi:uuid	Optional

Key	Description	Type	Required/optional
description	Human readable description for the firewall (1024 characters limit).	xsd:string	Optional
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.	xsd:string	Optional

Example request

```
{
    "firewall": {
        "admin_state_up": "false"
    }
}
```

Response codes

Status code	Description
200	Normal response codes
Bad Request (400)	Error response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "firewall": {
        "admin_state_up": false,
        "description": "",
        "firewall_policy_id": "c69933c1-b472-44f9-8226-30dc4ffd454c",
        "id": "3b0ef8f4-82c7-44d4-a4fb-6177f9a21977",
        "name": "",
        "status": "PENDING_UPDATE",
        "tenant_id": "45977fa2dbd7482098dd68d0d8970117",
        "router_id": "fe00194c-d73c-4b46-b94a-622bf28fc9e2",
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
admin_state_up	Administrative state of the firewall. If false (down), firewall does not forward packets and will drop all traffic to/from VMs behind the firewall.
description	Human readable description for the firewall (1024 characters limit)

Item	Description
firewall_policy_id	The firewall policy uuid that this firewall is associated with. This firewall will implement the rules contained in the firewall policy represented by this uuid.
id	Unique identifier for the firewall object.
name	Human readable name for the firewall (255 characters limit). Does not have to be unique.
status	Indicates whether firewall resource is currently operational. Possible values include: ACTIVE, DOWN, ERROR, PENDING_CREATE, PENDING_UPDATE, or PENDING_DELETE.
tenant_id	Owner of the firewall. Only admin users can specify a tenant identifier other than their own.
router_id	The ID of the router that this firewall applied.
availability_zone	The Availability Zone name.

1.5.6.17 Update firewall(Connection reset)

Connection reset for applying firewall rule to the current communication immediately.

URI

/v2.0/fw/firewalls/{firewall-id}/reset_connections

Description of the URI:

All connections managed by routers that use the specified firewall will be deleted a few seconds after the API response. This reflects the rules set for the firewall to communication. Existing communications that were in progress via routers that use the specified firewall, including communications permitted by it, will be disconnected at the time. If any communication permission rules exist, the disconnection will be temporary, so communication will be resumed.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
target	null	null	Required

Example request

```
{
    "target": null
}
```

Response codes

Status code	Description
200	Normal response codes

Status code	Description
Not Found (404)	Error response codes Firewall xxx could not be found
Conflict (409)	Error response codes Operation cannot be performed since associated Firewall xxx is in (*) (*) ... PENDING_STATE or PENDING_UPDATE or PENDING_DELETE
Bad Request (400)	Error response codes

Response body (normal status)

```
{
    "target": null
}
```

Description of response body (normal status)

Item	Number of occurrences of element	Description
target	1	Connection deletion target (null indicates that all firewall connections were deleted)

1.5.6.18 Delete firewall

Deletes a firewall.

URI

/v2.0/fw/firewalls/{firewall-id}

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error Response Codes
Not Found (404)	Error Response Codes
conflict (409)	Error response codes

1.6 Load balancer

1.6.1 API list

Load balancer

Item	API	Description
1	ApplySecurityGroupsToLoadBalancer	Associates one or more security groups with the load balancer
2	AttachLoadBalancerToSubnets	Attaches one or more subnets to the load balancer
3	ConfigureHealthCheck	Specifies the health check settings to use when evaluating the health state of the distribution destination instances of the specified load balancer
4	CreateLBCookieStickinessPolicy	Generates a session stickiness policy
5	CreateLoadBalancer	Creates a load balancer
6	CreateLoadBalancerListeners	Creates one or more listeners for the port specified in the load balancer
7	CreateLoadBalancerPolicy	Creates a policy including required attributes according to its type
8	CreateSorryServerRedirectionPolicy	Creates a policy for redirecting to the SorryServer when unable to distribute due to the distribution destination instances not all being in an active state.
9	DeleteLoadBalancer	Deletes the specified load balancer
10	DeleteLoadBalancerListeners	Deletes a listener of the specified port number from the load balancer
11	DeleteLoadBalancerPolicy	Deletes a specified policy from the load balancer
12	DeregisterInstancesFromLoadBalancer	Deletes the specified instance from the load balancer
13	DescribeLoadBalancerAttributes	Retrieves attribute information of the load balancer that was created
14	DescribeLoadBalancerPolicies	Retrieves policy information from the load balancer
15	DescribeLoadBalancers	Retrieves detailed information of the load balancer that was created
16	DetachLoadBalancerFromSubnets	Detaches the subnets from the load balancer
17	ModifyLoadBalancerAttributes	Changes attribute information of the specified load balancer
18	RegisterInstancesWithLoadBalancer	Adds an instance to the load balancer
19	SetLoadBalancerListenerSSLCertificate	Sets the certificate of the end of SSL communications for the specified listener

Item	API	Description
20	SetLoadBalancerPoliciesOfListener	Registers, deregisters, and changes policies that are applied to a listener of the load balancer

1.6.2 General requirements

This section describes general requirements to use this API.

- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.6.3 API common information

1.6.3.1 Query Requests and Response

Description

This section describes query requests. A query request can be a HTTP or HTTPS request described in HTTP methods (GET or POST) containing the Action query parameter.

Contents

Query requests

A query request comprises the following.

- Endpoint

  URL that functions as the entry point of a web service.
- Action

  Action to be executed.

  This is one of the parameters, specified as Action=<*action*>.
- Parameter

  Each parameter is delimited by an ampersand (&).

  Among the parameters are list structure items.

  These lists are specified using the expression param.*n*.

  n is an integer starting from 1.

Query request example

In the example below, "https://loadbalancing.(*regionName*).cloud.global.fujitsu.com/" is the endpoint, "CreateLoadBalancer" is the action, and the remainder are the parameters.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
&Listeners.member.1.LoadBalancerPort=80
&Listeners.member.1.InstancePort=80
```

```
&Listeners.member.1.Protocol=http
&Listeners.member.1.InstanceProtocol=http
&Scheme=internal
&Subnets.member.1=subnet-3561b05d
&Version=2014-11-01
&Action=CreateLoadBalancer
```

Query response

The structure of a query response is specific to the operation.

The request ID is included in the requestId element of all responses.

The request ID is required for troubleshooting issues.

When a normal response with status code 200 is returned, check the result in "*DescribeLoadBalancers* on page 197".

When a status code other than 200 is returned, refer to "*Common Errors* on page 158" or Errors of the executed API to remove the cause of the error.

Query response example

In the example below, the request ID is "1549581b-12b7-11e3-895e-1334aEXAMPLE".

```
{
  "CreateLoadBalancerResponse": {
    "CreateLoadBalancerResult": {
      "DNSName":
 "MyLB01-3b9c2b0f028f40e09d6306887646c28b.elb.tps5.fujitsu.com"
    },
    "ResponseMetadata": {
      "RequestId": "1549581b-12b7-11e3-895e-1334aEXAMPLE"
    }
  }
}
```

1.6.3.2 Requests Headers

Description

A request header contains information used by all actions.

Contents

- X-Auth-Token

  Valid authentication token.
- Accept

  Usable application media type.

  The JSON format ("application/json") and XML format ("application/xml") can be specified.

  Responses will be converted into the specified format.
- Content-type

  Application media type of the resource content.

  The JSON format ("application/json") and XML format ("application/xml") can be specified.

  If Accept is omitted, responses will be converted into the specified format.

1.6.3.3 Common Parameters

Description

Common parameters are request parameters that can be used by all actions.

Action-specific parameters are also listed in the topic.

Contents

- Action

  Action to be executed.

  - Default: None
  - Type: String
  - Required: Yes
- Version

  API version to which a request is written.

  Specify 2014-11-01.

  Format: Expressed as YYYY-MM-DD.

  - Default: None
  - Type: String
  - Required: No

1.6.3.4 Common Errors

Description

Common errors are general errors that can be returned by all actions.

Action-specific errors are described in the explanation of each action.

Contents

- InternalFailure

  The request failed due to an error with unknown cause, exception, or failure.

  - HTTP Status Code: 400
- InvalidClientTokenId

  The request has not been approved for the specified authentication token.

  Or, a parameter that cannot be used with the specified authentication token has been specified.

  - HTTP Status Code: 403
- InvalidParameterCombination

  The request specified parameters that cannot be specified at the same time.

  - HTTP Status Code: 400
- InvalidParameterValue

  An invalid value or a value outside the range was specified for the input parameter.

  - HTTP Status Code: 400
- MalformedQueryString

The query string contained a syntax error.

- HTTP Status Code: 404

- MissingParameter

  A required parameter has not been specified for the specified action.

  - HTTP Status Code: 400

- ResourceIsBusy

  The resource is being used by another operation.

  - HTTP Status Code: 409

- UnsupportedHeaderValue

  An unsupported header value was specified.

  - HTTP Status Code: 406

- Unsupported

  The specified request is not supported.

  - HTTP Status Code: 500

- InternalError

  An internal error occurred.

  - HTTP Status Code: 500

1.6.4 API data types

1.6.4.1 BackendServerDescription

Description

Information about the configuration of a back-end server.

Contents

- InstancePort

  Port of the back-end server.

  - Default: None
  - Type: Integer
  - Required: No

- PolicyNames

  List of policies enabled for the back-end server.

  - Default: None
  - Type: String list
  - Required: No

1.6.4.2 HealthCheck

Description

Information about a health check.

Contents

- HealthyThreshold

  The number of consecutive health check successes that is to be embedded in the assignment destination after it has been deemed that the target distribution destination instance has recovered from a failure.

  Specify a value from 1 to 2147483647.

  - Type: Integer
  - Required: Yes
- Interval

  The interval, in seconds, between health checks.

  Specify a value from 1 to 2147483647.

  - Type: Integer
  - Required: Yes
- Target

  Protocol, port number, and URL of the instance targeted for a health check.

  These are to be specified using the following format:

  ```
  protocol:port<url>
  ```

  For the protocol, specify one of the following: TCP, HTTP, HTTPS, or SSL.

  For the port, specify a value from 1 to 65535.

  For the url, if the protocol is HTTP or HTTPS, then specify the URL path. (Optional)

  - Type: String
  - Required: Yes
- Timeout

  The amount of time, in seconds, during which no response means a failed health check.

  Specify a value from 1 to 2147483647.

  

  This value must be less than the Interval value.

  Caution

  - Type: Integer
  - Required: Yes
- UnhealthyThreshold

  The number of consecutive health check failures that is to be excluded from the assignment destination after it has been deemed that the target distribution destination instance failed.

  Specify a value from 1 to 2147483647.

  - Type: Integer
  - Required: Yes

1.6.4.3 ConnectionSettings

Description

Information about the ConnectionSettings attribute.

Contents

- IdleTimeout

  Time for maintaining the connection to the front and back ends in an idle state.

  This time period is set in seconds.

  - Type: Integer
  - Valid range: Minimum value of 1. Maximum value of 3600.
  - Required: Yes

1.6.4.4 Instance

Description

Information about an instance.

Contents

- InstanceId

  ID of the instance.

  - Type: String
  - Required: Yes
- PortId

  Port ID of the instance.

  Target port, where multiple ports exist for an instance.

  - Type: String
  - Required: No

1.6.4.5 InstanceDescription

Description

Information about an instance.

Contents

- InstanceId

  ID of the instance.

  - Type: String
  - Required: No
- PortId

  Port ID of the instance.

  - Type: String
  - Required: No

1.6.4.6 LBCookieStickinessPolicy

Description

Data type of LBCookieStickinessPolicy.

Contents

- CookieExpirationPeriod

  Expiration period (seconds) of the cookie.

  If this parameter is omitted, the expiration period will not be set.

  - Type: Long
  - Required: No
- PolicyName

  Name of policy.

  The name must be unique among the load balancers.

  - Type: String
  - Required: No

1.6.4.7 Listener

Description

Information about a listener.

Contents

- InstancePort

  TCP port number of distribution destination server.

  Specify a value from 1 to 65535.

  This item cannot be changed while the load balancer exists.

  Caution

  Only one InstancePort can be specified for a single load balancer.

  - Type: Integer
  - Required: Yes
- InstanceProtocol

  Protocol (HTTP, HTTPS, TCP, SSL) to be used for routing traffic to the back-end instances.

  This item cannot be changed while the load balancer exists.

  Caution

  If the front-end protocol is HTTP or HTTPS, InstanceProtocol must be set to HTTP or HTTPS.

  If the front-end protocol is TCP or SSL, InstanceProtocol must be set to TCP or SSL.

  The protocol specified for InstanceProtocol is not case-sensitive.

  If specifying more than one listener, it is necessary to match their InstanceProtocol and InstancePort values.

Caution

- Type: String
- Required: Yes

- LoadBalancerPort

  Port number of the front-end.

  Specify a value from 1 to 65535.

  This item cannot be changed while the load balancer exists.

  - Type: Integer
  - Required: Yes

- Protocol

  Transport protocol of the load balancer (HTTP, HTTPS, TCP, or SSL).

  This item cannot be changed while the load balancer exists.

  

  The protocol specified for Protocol is not case-sensitive.

  CautionIf the protocol is HTTP or HTTPS, the value of the X-Forwarded-Proto header will be the value specified for Protocol.

  - Type: String
  - Required: Yes

- SSLCertificateId

  Resource ID of the SSL certificate registered for the Key Management service.

  

  Only one SSL certificate can be specified for a single load balancer.

  CautionIf an SSL certificate that differs for each listener is specified, the last specified SSL certificate will be effective.

  If the front-end protocol is HTTP or TCP, it is not necessary to specify SSLCertificateId.

  - Type: String
  - Required: No

1.6.4.8 ListenerDescription

Description

Information about a listener.

Contents

- Listener

  Information about a listener.

  - Type: *Listener* on page 162
  - Required: No

- PolicyNames

  List of policy names.

  If there are no policies enabled, the list is empty.

  - Type: String list
  - Required: No

1.6.4.9 LoadBalancerAttributes

Description

Data type of LoadBalancerAttributes.

Contents

- ConnectionSettings

  By setting this parameter, the load balancer can maintain the connection in an idle (not sending or receiving data over the connection) state for a specified period.

  By default, it is set as follows by the combination of Protocol and InstanceProtocol of Listeners.

  - When the protocol is HTTP-HTTP, HTTPS-HTTP or HTTPS-HTTPS.

    60 seconds
  - When the protocol is TCP-TCP, SSL-TCP or SSL-SSL.

    3600 seconds

1.6.4.10 LoadBalancerDescription

Description

Normal response described in *DescribeLoadBalancers* on page 197

Contents

- AutoScaleState

  AutoScale state.

  If AutoScaleState is InService, this indicates that autoscale is enabled.

  If AutoScaleState is OutOfService, this indicates that autoscale is disabled.

  If AutoScaleState is AutoScaling, this indicates that autoscale is running.

  If AutoScaleState is Maintenance, this indicates that autoscale is disabled because maintenance is in progress.

  If AutoScaleState is Error, this indicates that autoscale has failed and is disabled.

  Refer to the AutoScaleErrorDescription information and remove the cause of the error.

  - Type: String
  - Required: No
- AutoScaleErrorDescription

  Investigation information for the time when AutoScaleState was Error.

  - Type: String
  - Required: No
- BackendServerDescriptions

  List of detailed information about the back-end servers.

  - Type: *BackendServerDescription* on page 159 list
  - Required: No
- CreatedTime

The time the load balancer was created.

- Type: DateTime
- Required: No

- DNSName

  Name of the DNS server where the load balancer name and IP address relationship is registered.

  - Type: String
  - Required: No

- ErrorDescription

  Investigation information for the time when State was Error.

  If "No more IP addresses available on Subnet '_subnet_id_'", this indicates that a subnet has insufficient IP addresses.

  If "No more Floating IP available on Network '_network_id_'", this indicates that a network has insufficient floating IPs.

  In all other cases, reexecute the operation immediately preceding the error.

  However, if the operation immediately preceding the error was *CreateLoadBalancer* on page 178 or *AttachLoadBalancerToSubnets* on page 171, follow the procedure below.

  - If the operation was *CreateLoadBalancer* on page 178, reexecute after executing *DeleteLoadBalancer* on page 186.
  - If the operation was *AttachLoadBalancerToSubnets* on page 171, reexecute after using *DetachLoadBalancerFromSubnets* on page 201 to detach the subnet that was added.

  If the value is not changed even after reexecuting the operation, notify the operation administrator of the ErrorDescription information and request an investigation.

  - Type: String
  - Required: No

- Grade

  Grade of the load balancer (performance type).

  Indicates a standard grade load balancer (Standard), medium performance-grade load balancer (Middle), or high performance-grade load balancer (High).

  - Type: String
  - Required: No

- HealthCheck

  Failure monitoring information of the load balancer.

  - Type: *HealthCheck* on page 159
  - Required: No

- Instances

  List of distribution destination instance IDs.

  - Type: *InstanceDescription* on page 161 list
  - Required: No

- ListenerDescriptions

  List of the detailed information about listeners.

  - Type: *ListenerDescription* on page 163 list
  - Required: No

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: No
- Policies

  List of policies defined for the load balancer.

  - Type: *Policies* on page 166
  - Required: No
- Scheme

  Type of the load balancer.

  If Scheme is public, the load balancer holds a DNS name that allows resolution of global IPs.

  If Scheme is internal, the load balancer holds a DNS name that allows resolution of private IPs.

  - Type: String
  - Required: No
- SecurityGroups

  Security group.

  - Type: String list
  - Required: No
- Servers

  Server information used for configuring the load balancer.
- State

  Latest status of the load balancer.

  If State is InService, this indicates that the load balancer is operating normally.

  If State is OutOfService, this indicates that an operation is being executed for the load balancer.

  If State is Error, this indicates that an operation for the load balancer has failed, and is in an error state.

  Check the ErrorDescription information.

  - Type: String
  - Required: No
- Subnets

  List of the subnet IDs of the virtual system.

  - Type: String list
  - Required: No

1.6.4.11 Policies

Description

Information about the policies.

Contents

- LBCookieStickinessPolicies

  List of *LBCookieStickinessPolicy* on page 162 created in *CreateLBCookieStickinessPolicy* on page 176

- Type: *LBCookieStickinessPolicy* on page 162 list
- Required: No

- SorryServerRedirectionPolicies

  List of *SorryServerRedirectionPolicy* on page 169 created in *CreateSorryServerRedirectionPolicy* on page 185

  - Type: *SorryServerRedirectionPolicy* on page 169 list
  - Required: No
- OtherPolicies

  List of policies other than stickiness and SorryServerRedirection policies.

  - Type: String list
  - Required: No

1.6.4.12 PolicyAttribute

Description

Data type of PolicyAttribute.

Composed of a pair of key and values defining the property of the specific policy.

Contents

- AttributeName

  Attribute name of the policy.

  - Type: String
  - Required: No
- AttributeValue

  Attribute name of the policy

  - Type: String
  - Required: No

Note

In the case PolicyTypeName of *CreateLoadBalancerPolicy* on page 182 is SSLNegotiationPolicyType, the following values can be set.

AttributeName	AttributeValue	Default	description
Protocol-TLSv1	true / false	false	Possibility of TLSv1 communication. True is recommended.
Protocol-SSLv3	true / false	false	Possibility of SSLv3 communication. True is recommended.
Protocol-TLSv1.1	true / false	false	Possibility of TLSv1.1 communication.
Protocol-TLSv1.2	true / false	false	Possibility of TLSv1.2 communication.

1.6.4.13 PolicyAttributeDescription

Description

Data type of PolicyAttributeDescription.

Contents

- AttributeName

  Attribute name related to the policy.

  - Type: String
  - Required: No
- AttributeValue

  Value of the attribute related to the policy.

  - Type: String
  - Required: No

Note In the case PolicyTypeName of *PolicyDescription* on page 168 is SSLNegotiationPolicyType,the following values will be set.

AttributeName	AttributeValue	Default	description
Protocol-TLSv1	true / false	false	Possibility of TLSv1 communication
Protocol-SSLv3	true / false	false	Possibility of SSLv3 communication
Protocol-TLSv1.1	true / false	false	Possibility of TLSv1.1 communication
Protocol-TLSv1.2	true / false	false	Possibility of TLSv1.2 communication
IsDefault	true / false	false	If the policy is set as default when creating a load balancer or not

1.6.4.14 PolicyDescription

Description

Data type of PolicyDescription.

Contents

- PolicyAttributeDescriptions

  List of structures of policy attributes.

  - Type: *PolicyAttributeDescription* on page 168 list
  - Required: No
- PolicyName

  Name of the policy.

- Type: String
- Required: No

- PolicyTypeName

  Type name of the policy to be created.

  - Type: String list
  - Required: No

1.6.4.15 SorryServerRedirectionPolicy

Description

Data type of SorryServerRedirectionPolicy.

Contents

- Location

  URI of the redirection destination location.

  - Type: Long
  - Required: No

- PolicyName

  Name of policy.

  The name must be unique among the load balancers.

  - Type: String
  - Required: No

1.6.4.16 SourceSecurityGroup

Description

Data type of an element of the *DescribeLoadBalancers* on page 197 response.

Contents

- GroupName

  Name of SourceSecurityGroup.

  - Type: String
  - Required: No

- OwnerAlias

  Owner of SourceSecurityGroup.

  - Type: String
  - Required: No

1.6.5 API details

1.6.5.1 ApplySecurityGroupsToLoadBalancer

Description

Associates one or more security groups with a load balancer.

The specified security groups override the previously associated security groups.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  The name must be unique among the load balancers in the projects to which the account belongs.

  - Type: String
  - Required: Yes
- SecurityGroups.member.N

  List of security group IDs to associate with the load balancer.

  It is necessary to specify security group IDs not as a security group name, but as an ID.

  - Type: String list
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the ApplySecurityGroupsToLoadBalancerResult.

- SecurityGroups

  List of security ID groups associated with the load balancer.

  - Type: String list

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400

- InvalidSecurityGroup

  One or more of the specified security groups do not exist.

  - HTTP Status Code: 400

Examples

Sample request

The example below applies the security groups MySecurityGroup-XXXXX and MySecurityGroup-YYYYY security groups to the load balancer with the name MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
SecurityGroups.member.1=MySecurityGroup-XXXXX
&SecurityGroups.member.2=MySecurityGroup-YYYYY
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=ApplySecurityGroupsToLoadBalancer
```

Sample response (XML)

```
<ApplySecurityGroupsToLoadBalancerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <ApplySecurityGroupsToLoadBalancerResult>
    <SecurityGroups>
      <member>MySecurityGroup-XXXXX</member>
      <member>MySecurityGroup-YYYYY</member>
    </SecurityGroups>
  </ApplySecurityGroupsToLoadBalancerResult>
  <ResponseMetadata>
    <RequestId>06b5decc-102a-11e3-9ad6-bf3e4EXAMPLE</RequestId>
  </ResponseMetadata>
</ApplySecurityGroupsToLoadBalancerResponse>
```

Sample response (JSON)

```
{
 "ApplySecurityGroupsToLoadBalancerResponse": {
  "ApplySecurityGroupsToLoadBalancerResult": {
   "SecurityGroups": {
    "member": [
     "MySecurityGroup-XXXXX",
     "MySecurityGroup-YYYYY"
    ]
   }
  },
  "ResponseMetadata": {
   "RequestId": "06b5decc-102a-11e3-9ad6-bf3e4EXAMPLE"
  }
 }
}
```

1.6.5.2 AttachLoadBalancerToSubnets

Description

Attaches one or more subnets to the specified load balancer.

The load balancer evenly distributes requests across all registered subnets.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  The name must be unique among the load balancers in the projects to which the account belongs.

  - Type: String
  - Required: Yes
- Subnets.member.N

  List of subnet IDs to attach to the load balancer.

  - Type: String list
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the AttachLoadBalancerToSubnetsResult.

- Subnets

  List of subnet IDs attached to the load balancer.

  - Type: String list

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409
- InvalidSubnet

  The Virtual system has no Internet gateway.

  - HTTP Status Code: 400
- SubnetNotFound

  One or more subnets were not found.

  - HTTP Status Code: 400

Examples

Sample request

The example below attaches the subnet-3561b05e to the load balancer with the name MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Subnets.member.1=subnet-3561b05e
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=AttachLoadBalancerToSubnets
```

Sample response (XML)

```
<AttachLoadBalancerToSubnetsResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <AttachLoadBalancerToSubnetsResult>
    <Subnets>
      <member>subnet-119f0078</member>
      <member>subnet-3561b05e</member>
    </Subnets>
  </AttachLoadBalancerToSubnetsResult>
  <ResponseMetadata>
    <RequestId>07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE</RequestId>
  </ResponseMetadata>
</AttachLoadBalancerToSubnetsResponse>
```

Sample response (JSON)

```
{
  "AttachLoadBalancerToSubnetsResponse": {
    "AttachLoadBalancerToSubnetsResult": {
      "Subnets": {
        "member": [
          "subnet-119f0078",
          "subnet-3561b05e"
        ]
      }
    },
    "ResponseMetadata": {
      "RequestId": "07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE"
    }
  }
}
```

1.6.5.3 ConfigureHealthCheck

Description

Specifies the health check settings to use when evaluating the health state of the distribution destination instances of the specified load balancer.

If you do not specify the health check settings in the API, the following settings will be used:

Interval:	30
Timeout:	5
HealthyThreshold:	10
UnhealthyThreshold:	2
Target:	protocol:port[url] protocol: Value of InstanceProtocol of the listener. port: Value of InstancePort of the listener. url: / when the protocol is HTTP or HTTPS.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  The name must be unique among the load balancers in the projects to which the account belongs.

  - Type: String
  - Required: Yes
- HealthCheck

  Setting information for the health check.

  The protocol and port number to be specified for the target of *HealthCheck* on page 159 must match the InstanceProtocol and InstancePort specified in *Listener* on page 162 of the load balancer with the name specified in LoadBalancerName.

  - Type: *HealthCheck* on page 159
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called ConfigureHealthCheckResult.

- HealthCheck

  Health check information that is updated for distribution destination instances

  - Type: *HealthCheck* on page 159

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found

  - HTTP Status Code: 400

Examples

Sample request

The example below configures a health check target of HTTP:80/ping, implementation interval of 30 seconds, response timeout of 3 seconds, failure decision threshold of 2 times, and restore decision threshold of 2 times, for the distribution destination instances of the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
HealthCheck.HealthyThreshold=2
&HealthCheck.UnhealthyThreshold=2
&HealthCheck.Target=HTTP:80
&HealthCheck.Interval=30
&HealthCheck.Timeout=3
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=ConfigureHealthCheck
```

Sample response (XML)

```
<ConfigureHealthCheckResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <ConfigureHealthCheckResult>
    <HealthCheck>
      <Interval>30</Interval>
      <Target>HTTP:80</Target>
      <HealthyThreshold>2</HealthyThreshold>
      <Timeout>3</Timeout>
      <UnhealthyThreshold>2</UnhealthyThreshold>
    </HealthCheck>
  </ConfigureHealthCheckResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b12EXAMPLE</RequestId>
  </ResponseMetadata>
</ConfigureHealthCheckResponse>
```

Sample response (JSON)

```
{
  "ConfigureHealthCheckResponse": {
    "ConfigureHealthCheckResult": {
      "HealthCheck": {
        "Interval": "30",
        "Target": "HTTP:80",
        "HealthyThreshold": "2",
        "Timeout": "3",
        "UnhealthyThreshold": "2"
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b12EXAMPLE"
    }
  }
}
```

1.6.5.4 CreateLBCookieStickinessPolicy

Description

Generates a session stickiness policy.

This policy can be associated only with HTTP/HTTPS listeners.

For this policy, it is necessary to configure the listener that will be applied by SetLoadBalancerPoliciesOfListener.

When this policy is specified, the load balancer specifies the cookie information for identifying distribution destination instances in the response packet.

When this cookie information is specified for requests from the client, the load balancer assigns the information to the specified instance.

Information related to the session expiration period specified in the policy is appended to the cookie information for identifying instances.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- CookieExpirationPeriod

  Maximum period for holding a session using cookies.

  The time is specified in seconds, from 1 to 2147483647.

  If this parameter is omitted, the expiration period will not be set.

  - Type: Long
  - Default: n/a
  - Required: No
- LoadBalancerName

  Name of the load balancer that will use the policies.

  - Type: String
  - Required: Yes
- PolicyName

  Name of the policy to be created.

  The name must be unique among the policies that can be used by the target load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- DuplicatePolicyName

  Policy with the same name exists for this load balancer. Please choose another name.

  - HTTP Status Code: 400
- TooManyPolicies

  Quota for number of policies for this load balancer has already been reached.

  - HTTP Status Code: 400

Examples

Sample request

The example below created a session expiration period of 60 seconds for the policy named MyLoadBalancerCookiePolicy, for the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
CookieExpirationPeriod=60
&LoadBalancerName=MyLB01&PolicyName=MyLoadBalancerCookiePolicy
&Version=2014-11-01
&Action=CreateLBCookieStickinessPolicy
```

Sample response (XML)

```
<CreateLBCookieStickinessPolicyResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
<CreateLBCookieStickinessPolicyResult/>
<ResponseMetadata>
  <RequestId>99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE</RequestId>
</ResponseMetadata>
</CreateLBCookieStickinessPolicyResponse>
```

Sample response (JSON)

```
{
  "CreateLBCookieStickinessPolicyResponse": {
    "CreateLBCookieStickinessPolicyResult": {
    },
    "ResponseMetadata": {
      "RequestId": "99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE"
    }
  }
}
```

1.6.5.5 CreateLoadBalancer

Description

Creates a load balancer.

If the call completes successfully, notification of a unique DNS name is sent.

Up to 20 load balancers can be created for projects to which the account belongs.

When creating a load balancer, SSLNegotiationPolicy is set as default.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- Listeners.member.N

  List of listeners, including LoadBalancerPort, InstancePort, and Protocol.

  - Type: *Listener* on page 162 list
  - Required: Yes
- LoadBalancerName

  Name of the load balancer.

  The name must be unique among the load balancers in the projects to which the account belongs.

  Specify the value using up to 30 characters.

  You can specify alphanumeric characters and hyphens (-).

  - Type: String
  - Required: Yes
- Scheme

  Type of the load balancer.

  Specify public to create a load balancer over the Internet.

  Specify internal to create a load balancer from a private network.

  - Type: String
  - Default: public
  - Valid values: public | internal
  - Required: No
- SecurityGroups.member.N

  List of security group IDs.

  If omitted, the default security group of the user's project will be used.

  - Type: String list
  - Required: No
- Subnets.member.N

  List of subnet IDs.

  Specify the same subnet as the distribution destination instance that is to be registered in the following cases.

  - When using the health check function for VM instance using autoscaling (AutoScaling)
  - When monitoring load balancer monitoring items using the monitoring service

  - Type: String list

  - Required: Yes
- Grade

  Grade of the load balancer (performance type).

  Select from a standard grade load balancer (Standard), medium performance grade load balancer (Middle), or high performance grade load balancer (High).

  - Type: String
  - Default: Standard
  - Valid values: Standard | Middle | High
  - Required: No

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following is returned in a structure called the CreateLoadBalancerResult.

- DNSName

  DNS name of load balancer.

  - Type: String

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- CertificateNotFound

  The specified SSL ID does not refer to a valid SSL certificate in the Key Management Service.

  - HTTP Status Code: 400
- DuplicateAccessPointName

  Load balancer name already exists for this account. Please choose another name.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409
- InvalidScheme

  Invalid value for scheme. Scheme can only be specified for load balancers in the Virtual system.

  - HTTP Status Code: 400
- InvalidSecurityGroup

  One or more specified security groups do not exist.

  - HTTP Status Code: 400
- InvalidSubnet

  The Virtual system has no Internet gateway.

  - HTTP Status Code: 400
- SubnetNotFound

  One or more subnets were not found.
  - HTTP Status Code: 400
- TooManyAccessPoints

  The quota for the number of load balancers has already been reached.
  - HTTP Status Code: 400

Examples

Sample request

The example below creates a load balancer named MyLB01 and a listener for the 80/http port/protocol for front-end and back-end connections.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
&Listeners.member.1.LoadBalancerPort=80
&Listeners.member.1.InstancePort=80
&Listeners.member.1.Protocol=http
&Listeners.member.1.InstanceProtocol=http
&Scheme=internal
&Subnets.member.1=subnet-3561b05d
&Version=2014-11-01
&Action=CreateLoadBalancer
```

Sample response (XML)

```
<CreateLoadBalancerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <CreateLoadBalancerResult>
    <DNSName>MyLB01-1234567890.aa.bbbb.cccc.dddd</DNSName>
  </CreateLoadBalancerResult>
  <ResponseMetadata>
    <RequestId>1549581b-12b7-11e3-895e-1334aEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateLoadBalancerResponse>
```

Sample response (JSON)

```
{
  "CreateLoadBalancerResponse": {
    "CreateLoadBalancerResult": {
      "DNSName": "MyLB01-1234567890.aa.bbbb.cccc.dddd"
    },
    "ResponseMetadata": {
      "RequestId": "1549581b-12b7-11e3-895e-1334aEXAMPLE"
    }
  }
}
```

1.6.5.6 CreateLoadBalancerListeners

Description

Creates one or more listeners for the port specified in the load balancer.

If a listener for the specified LoadBalancerPort exists, InstancePort,InstanceProtocol and SSLCertificateId values must match the existing listner's.

To change the InstancePort and/or Protocol for an existing listener, re-create the load balancer.

In the case specifying multiple listeners, it is necessary to match their InstanceProtocol and InstancePort values.

If combinations of InstancePort and InstanceProtocol are different, it is necessary to create a load balancer for each combination.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- Listeners.member.N

  List of listeners, including LoadBalancerPort, InstancePort, Protocol, and SSLCertificateId.

  - Type: *Listener* on page 162 list
  - Required: Yes
- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- CertificateNotFound

  The specified SSL ID does not refer to a valid SSL certificate in the Key Management Service.

  - HTTP Status Code: 400
- DuplicateListener

A listener already exists for the given LoadBalancerName and LoadBalancerPort, but with a different InstancePort, Protocol, or SSLCertificateId.

  - HTTP Status Code: 400

- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409

Examples

Sample request

The example below creates a listener for the 443/https port/protocol for the front-end connection and 80/http port/protocol for the back-end connection for the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Listeners.member.1.Protocol=https
&Listeners.member.1.LoadBalancerPort=443
&Listeners.member.1.InstancePort=80
&Listeners.member.1.InstanceProtocol=http
&Listeners.member.1.SSLCertificateId=1232d7bf-8f28-4cc7-a63d-44e218853c6d
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=CreateLoadBalancerListeners
```

Sample response (XML)

```
<CreateLoadBalancerListenersResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <CreateLoadBalancerListenersResult/>
  <ResponseMetadata>
    <RequestId>1549581b-12b7-11e3-895e-1334aEXAMPLE</RequestId>
  </ResponseMetadata>
</CreateLoadBalancerListenersResponse>
```

Sample response (JSON)

```
{
  "CreateLoadBalancerListenersResponse": {
    "CreateLoadBalancerListenersResult": {
    },
    "ResponseMetadata": {
      "RequestId": "1549581b-12b7-11e3-895e-1334aEXAMPLE"
    }
  }
}
```

1.6.5.7 CreateLoadBalancerPolicy

Description

Creates a policy including required attributes according to its type.

Policies can be created up to 100 for each load balancer.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes
- PolicyAttributes.member.N

  List of attribute related to policy.

  - Type: *PolicyAttribute* on page 167list
  - Required: Yes
- PolicyName

  Name of the policy to be created.

  The name must be unique among the policies that can be used by the target load balancer.

  - Type: String
  - Required: Yes
- PolicyTypeName

  Type name of the policy to be created.

  - Type: String
  - Required: Yes

    The following can be specified.

    SSLNegotiationPolicyType

    a SSL cryptographic protocol policy

    It is possible to set to listener which uses the protocol HTTPS and SSL.

Response

The following status code is returned.

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- DuplicatePolicyName

  Policy with the same name exists for this load balancer. Please choose another name.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.
  - HTTP Status Code: 409
- PolicyNotFound

  One or more specified policies were not found.
  - HTTP Status Code: 400
- TooManyPolicies

  Quota for number of policies for this load balancer has already been reached.
  - HTTP Status Code: 400

Examples

Sample request

The example below created the policy named MySSLNegotiationPolicy, for the load balancer named MyLB01.

```
       https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
       &PolicyAttributes.member.1.AttributeName=Protocol-TLSv1
       &PolicyAttributes.member.1.AttributeValue=false
       &PolicyAttributes.member.2.AttributeName=Protocol-SSLv3
       &PolicyAttributes.member.2.AttributeValue=true
       &PolicyAttributes.member.3.AttributeName=Protocol-TLSv1.1
       &PolicyAttributes.member.3.AttributeValue=true
       &PolicyAttributes.member.4.AttributeName=Protocol-TLSv1.2
       &PolicyAttributes.member.4.AttributeValue=true
       &PolicyName=MySSLNegotiationPolicy
       &PolicyTypeName=SSLNegotiationPolicyType
       &Version=2014-11-01
       &Action=CreateLoadBalancerPolicy
```

Sample response (XML)

```
       <CreateLoadBalancerPolicyResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
        <CreateLoadBalancerPolicyResult/>
        <ResponseMetadata>
         <RequestId>99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE</RequestId>
        </ResponseMetadata>
       </CreateLoadBalancerPolicyResponse>
```

Sample response (JSON)

```
       {
        "CreateLoadBalancerPolicyResponse": {
         "CreateLoadBalancerPolicyResult": {
         },
         "ResponseMetadata": {
          "RequestId": "99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE"
         }
        }
       }
```

1.6.5.8 CreateSorryServerRedirectionPolicy

Description

Creates a policy for redirecting to the sorry server when unable to distribute the client request because there are no distribution destination instances in active state.

This policy can be associated only with HTTP/HTTPS listeners.

For this policy, it is necessary to configure the listener that will be applied by SetLoadBalancerPoliciesOfListener.

When this policy is specified, the specified location information is set in the response packet when the load balancer is unable to assign requests to distribution destination instances.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- Location

  URI of the redirection destination location.

  - Type: String
  - Required: Yes
- LoadBalancerName

  Name of the load balancer that will use the policies.

  - Type: String
  - Required: Yes
- PolicyName

  Name of the policy to be created.

  The name must be unique among the policies that can be used by the target load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

The specified load balancer could not be found.

- HTTP Status Code: 400

- DuplicatePolicyName

  Policy with the same name exists for this load balancer. Please choose another name.

  - HTTP Status Code: 400

Examples

Sample request

The example below creates a policy named MyPolicy at the redirection destination location http://XXXXXXXX/ for the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Location=http://XXXXXXXX/
&LoadBalancerName=MyLB01&PolicyName=MyPolicy
&Version=2014-11-01
&Action=CreateSorryServerRedirectionPolicy
```

Sample response (XML)

```
<CreateSorryServerRedirectionPolicyResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <CreateSorryServerRedirectionPolicyResult/>
  <ResponseMetadata>
    <RequestId>99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE</RequestId>
  </ResponseMetadata>
</CreateSorryServerRedirectionPolicyResponse>
```

Sample response (JSON)

```
{
  "CreateSorryServerRedirectionPolicyResponse": {
    "CreateSorryServerRedirectionPolicyResult": {
    },
    "ResponseMetadata": {
      "RequestId": "99a693e9-12b8-11e3-9ad6-bf3e4EXAMPLE"
    }
  }
}
```

1.6.5.9 DeleteLoadBalancer

Description

Deletes the specified load balancer.

If re-creating a load balancer, it is necessary to reconfigure all its settings.

The DNS name associated with a deleted load balancer can no longer be used.

Once deleted, the load balancer name and the related DNS logs are erased, and the data sent to that IP address will not arrive at the distribution destination instances.

This API can be used only by users with account privileges belonging to the same project as the account used when creating the load balancer.

If the load balancer does not exist or has already been deleted, the call to this API will still be successful.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

None.

Examples

Sample request

The example below deletes the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=DeleteLoadBalancer
```

Sample response (XML)

```
<DeleteLoadBalancerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DeleteLoadBalancerResult/>
  <ResponseMetadata>
    <RequestId>f6dd8353-eb6b-6b4fd32e4f05</RequestId>
  </ResponseMetadata>
</DeleteLoadBalancerResponse>
```

Sample response (JSON)

```
{
  "DeleteLoadBalancerResponse": {
    "DeleteLoadBalancerResult": {
    },
    "ResponseMetadata": {
      "RequestId": "f6dd8353-eb6b-6b4fd32e4f05"
    }
  }
}
```

1.6.5.10 DeleteLoadBalancerListeners

Description

Deletes the listener of the specified port number from the load balancer.

This API cannot be used to set the number of listeners to 0.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes
- LoadBalancerPorts.member.N

  Front-end port number of the listener for the load balancer that is to be deleted.

  - Type: Integer list
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found

  - HTTP Status Code: 400

- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409

Examples

Sample request

The example below delete the listener of port number 22 for the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=DeleteLoadBalancerListeners
&LoadBalancerPorts.member.1=22
```

Sample response (XML)

```
<DeleteLoadBalancerListenersResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DeleteLoadBalancerListenersResult/>
  <ResponseMetadata>
    <RequestId>f6dd8353-eb6b-6b4fd32e4f05</RequestId>
  </ResponseMetadata>
</DeleteLoadBalancerListenersResponse>
```

Sample response (JSON)

```
{
  "DeleteLoadBalancerListenersResponse": {
    "DeleteLoadBalancerListenersResult": {
    },
    "ResponseMetadata": {
      "RequestId": "f6dd8353-eb6b-6b4fd32e4f05"
    }
  }
}
```

1.6.5.11 DeleteLoadBalancerPolicy

Description

Deletes a policy from the specified load balancer.

Policies not set to the listener can be deleted.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String

  - Required: Yes
- PolicyName

  >Name of the policy to be deleted.

  - Type: String
  - Required: Yes

Response

The following status code is returned.

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409
- PolicyNotFound

  One of more specified policies were not found.

  - HTTP Status Code: 400

Examples

Sample request

The example below deletes the MySSLNegotiationPolicy that was created by the load balancer named MyLB01.

```
      https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
      &PolicyName=MySSLNegotiationPolicy
      &Version=2014-11-01
      &Action=DeleteLoadBalancerPolicy
```

Sample response (XML)

```
      <DeleteLoadBalancerPolicyResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
       <DeleteLoadBalancerPolicyResult/>
       <ResponseMetadata>
```

```
    <RequestId>f6dd8353-eb6b-6b4fd32e4f05</RequestId>
  </ResponseMetadata>
</DeleteLoadBalancerPolicyResponse>
```

Sample response (JSON)

```
{
 "DeleteLoadBalancerPolicyResponse": {
  "DeleteLoadBalancerPolicyResult": {
  },
  "ResponseMetadata": {
   "RequestId": "f6dd8353-eb6b-6b4fd32e4f05"
  }
 }
}
```

1.6.5.12 DeregisterInstancesFromLoadBalancer

Description

Deregisters the specified distribution destination instances from the specified load balancer.

After a distribution destination instance is deregistered, it no longer receives traffic from the load balancer.

This API can be used only by users with account privileges belonging to the same project as the account used when creating the load balancer.

Refer to "*DescribeLoadBalancers* on page 197" to check if the distribution destination instances have been deregistered from the load balancer.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- Instances.member.N

  List of distribution destination instance IDs to deregister.

  - Type: *Instance* on page 161 list
  - Required: Yes
- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the DeregisterInstancesFromLoadBalancerResult.

- Instances

  List of remaining distribution destination instances registered with the updated load balancer.

  - Type: [InstanceDescription] list

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- InvalidEndPoint

  The specified EndPoint is not valid.

  - HTTP Status Code: 400

Examples

Sample request

The example below deregisters the distribution destination instance with the ID i-e3677ad7 from the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Instances.member.1.InstanceId=i-e3677ad7
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=DeregisterInstancesFromLoadBalancer
```

Sample response (XML)

```
<DeregisterInstancesFromLoadBalancerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DeregisterInstancesFromLoadBalancerResult>
    <Instances>
      <member>
        <InstanceId>i-6ec63d59</InstanceId>
        <PortId>p-6ec63d59</PortId>
      </member>
      <member>
        <InstanceId>i-34cde612</InstanceId>
      </member>
    </Instances>
  </DeregisterInstancesFromLoadBalancerResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b12EXAMPLE</RequestId>
  </ResponseMetadata>
</DeregisterInstancesFromLoadBalancerResponse>
```

Sample response (JSON)

```
{
  "DeregisterInstancesFromLoadBalancerResponse": {
    "DeregisterInstancesFromLoadBalancerResult": {
      "Instances": {
        "member": [
          {
           "InstanceId": "i-6ec63d59"
           "PortId": "p-6ec63d59"
          },
          {
           "InstanceId": "i-34cde612"
          }
        ]
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b12EXAMPLE"
    }
  }
}
```

1.6.5.13 DescribeLoadBalancerAttributes

Description

Describes the attributes for the specified load balancer.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the DescribeLoadBalancerAttributesResult.

- LoadBalancerAttributes

  Information about the load balancer attributes.

  - Type: *LoadBalancerAttributes* on page 164

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400

Examples

Sample request

The example below retrieves information about the attributes of the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Instances.member.1.InstanceId=i-e3677ad7
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action= DescribeLoadBalancerAttributes
```

Sample response (XML)

```
<DescribeLoadBalancerAttributesResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DescribeLoadBalancerAttributesResult>
    <LoadBalancerAttributes>
      <ConnectionSettings>
        <IdleTimeout>60</IdleTimeout>
      </ConnectionSettings>
    </LoadBalancerAttributes>
  </DescribeLoadBalancerAttributesResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b13EXAMPLE</RequestId>
  </ResponseMetadata>
</DescribeLoadBalancerAttributesResponse>
```

Sample response (JSON)

```
{
  "DescribeLoadBalancerAttributesResponse": {
    "DescribeLoadBalancerAttributesResult": {
      "LoadBalancerAttributes": {
        "ConnectionSettings": {
          "IdleTimeout": "60"
        }
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b13XAMPLE"
    }
  }
}
```

1.6.5.14 DescribeLoadBalancerPolicies

Description

Retrieves policy information from the load balancer.

Specifying the name of load balancer,all policies that can be used with load balancer are retrieved.

If omitted,all policies that the service provides will be retrieved.

Specifying the name of policy,Only that policy will be retrieved.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: No
- PolicyNames.member.N

  Name of the policy.

  - Type: String list
  - Required: No

Response

The following status code is returned.

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the DescribeLoadBalancerPoliciesResult.

- LoadBalancerPolicies

  The policy of load balancer

  - Type: *PolicyDescription* on page 168 list

Errors

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- PolicyNotFound

  One or more specified policies were not found.

  - HTTP Status Code: 400

Examples

Sample request

The example below retrieves information availavle on the load balancer named MyLB01.

```
       https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
       &Version=2014-11-01
       &Action=DescribeLoadBalancerPolicies
```

Sample response (XML)

```
       <DescribeLoadBalancerPoliciesResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">R
        <DescribeLoadBalancerPoliciesResult>
         <PolicyDescriptions>
          <member>
           <PolicyName>MyLBStickinessPolicy</PolicyName>
           <PolicyTypeName>LBCookieStickinessPolicyType</PolicyTypeName>
           <PolicyAttributeDescriptions>
            <member>
             <AttributeName>CookieExpirationPeriod</AttributeName>
             <AttributeValue>60</AttributeValue>
            </member>
           </PolicyAttributeDescriptions>
          </member>
          <member>
           <PolicyName>ServiceSSLNegotiationPolicy</PolicyName>
           <PolicyTypeName>SSLNegotiationPolicyType</PolicyTypeName>
           <PolicyAttributeDescriptions>
            <member>
             <AttributeName>Protocol-TLSv1</AttributeName>
             <AttributeValue>false</AttributeValue>
            </member>
            <member>
             <AttributeName>Protocol-SSLv3</AttributeName>
             <AttributeValue>false</AttributeValue>
            </member>
            <member>
             <AttributeName>Protocol-TLSv1.1</AttributeName>
             <AttributeValue>true</AttributeValue>
            </member>
            <member>
             <AttributeName>Protocol-TLSv1.2</AttributeName>
             <AttributeValue>true</AttributeValue>
            </member>
            <member>
             <AttributeName>IsDefault</AttributeName>
             <AttributeValue>true</AttributeValue>
            </member>
           </PolicyAttributeDescriptions>
          </member>
         </PolicyDescriptions>
        </DescribeLoadBalancerPoliciesResult>
        <ResponseMetadata>
         <RequestId>83c88b9d-12b7-11e3-8b82-87b13EXAMPLE</RequestId>
        </ResponseMetadata>
       </DescribeLoadBalancerPoliciesResponse>
```

Sample response (JSON)

```
{
 "DescribeLoadBalancerPoliciesResponse": {
  "DescribeLoadBalancerPoliciesResult": {
   "PolicyDescription": [
    {
     "PolicyName": "MyLBStickinessPolicy",
     "PolicyTypeName": "LBCookieSticknessPolicyType",
     "PolicyAttributeDescriptions": [
      {
       "AttributeName": "CookieExpirationPeriod",
       "AttributeValue": "60"
      }]
    },
    {
     "PolicyName": "ServiceSSLNegotiationPolicy",
     "PolicyTypeName": "SSLNegotiationPolicyType",
     "PolicyAttributeDescriptions": [
      {
       "AttributeName": "Protocol-TLSv1",
       "AttributeValue": "false"
      },
      {
       "AttributeName": "Protocol-SSLv3",
       "AttributeValue": "false"
      },
      {
       "AttributeName": "Protocol-TLSv1.1",
       "AttributeValue": "true"
      },
      {
       "AttributeName": "Protocol-TLSv1.2",
       "AttributeValue": "true"
      },
      {
       "AttributeName": "IsDefault",
       "AttributeValue": "true"
      }]
    }
  ]}
  "ResponseMetadata": {
    "RequestId": "83c88b9d-12b7-11e3-8b82-87b13XAMPLE"
   }
  }
}
```

1.6.5.15 DescribeLoadBalancers

Description

Describes the specified the load balancers.

If a load balancer is specified, the call describes the specified load balancer.

If no load balancers are specified, the call describes the load balancers created using an account belonging to the same project as the account that issued this API.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerNames.member.N

  List of load balancers created by an account belonging to the project.

  - Type: String list
  - Required: No
- Marker

  Reserved parameter.
  - Type: String
  - Required: No

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.
  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the DescribeLoadBalancersResult.

- LoadBalancerDescriptions

  List of detailed information of a load balancer.
  - Type: *LoadBalancerDescription* on page 164 list
- NextMarker

  Reserved parameter
  - Type: String

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.
  - HTTP Status Code: 400

Examples

Sample request

The example below retrieves information about the attributes of the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerNames.member.1=MyLB01
&Version=2014-11-01
&Action=DescribeLoadBalancers
```

Sample response (XML)

```
<DescribeLoadBalancersResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DescribeLoadBalancersResult>
```

```
    <LoadBalancerDescriptions>
      <member>
        <LoadBalancerName>MyLB01</LoadBalancerName>
        <DNSName>MyLB01-3b9c2b0f028f40e09d6306887646c28b.loadbalancing-jp-
east-1.cloud.global.fujitsu.com</DNSName>
        <State>InService</State>
        <ListenerDescriptions>
          <member>
            <Listener>
              <Protocol>HTTPS</Protocol>
              <LoadBalancerPort>443</LoadBalancerPort>
              <InstanceProtocol>HTTP</InstanceProtocol>
              <InstancePort>80</InstancePort>
              <SSLCertificateId>1232d7bf-8f28-4cc7-a63d-44e218853c6d</
SSLCertificateId>
            </Listener>
            <PolicyNames>
              <member>MyPolicy</member>
            </PolicyNames>
          </member>
        </ListenerDescriptions>
        <Policies>
          <LBCookieStickinessPolicies>
            <member>
              <PolicyName>MyLoadBalancerCookieStickinessPolicy</PolicyName>
              <CookieExpirationPeriod>60</CookieExpirationPeriod>
            </member>
          </LBCookieStickinessPolicies>
          <OtherPolicies>
           <member>MyPolicy</member>
          </OtherPolicies>
        </Policies>
        <Subnets>
          <member>MySubnet</member>
        </Subnets>
        <Instances>
          <member>
            <InstanceId>i-e4cbe38d</InstanceId>
            <PortId>p-e4cbe38d</PortId>
          </member>
        </Instances>
        <HealthCheck>
          <Target>HTTP:80</Target>
          <Interval>90</Interval>
          <Timeout>60</Timeout>
          <UnhealthyThreshold>10</UnhealthyThreshold>
          <HealthyThreshold>2</HealthyThreshold>
        </HealthCheck>
        <SecurityGroups>
          <member>MySecurityGroup</member>
        </SecurityGroups>
        <CreatedTime>2014-06-01T21:15:31.280Z</CreatedTime>
        <Scheme>Internal</Scheme>
        <Grade>Standard</Grade>
      </member>
    </LoadBalancerDescriptions>
    <NextMarker></NextMarker>
  </DescribeLoadBalancersResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b12EXAMPLE</RequestId>
  </ResponseMetadata>
</DescribeLoadBalancersResponse>
```

Sample response (JSON)

```
{
  "DescribeLoadBalancersResponse": {
    "DescribeLoadBalancersResult": {
      "LoadBalancerDescriptions": {
        "member": [
          {
            "LoadBalancerName": "MyLB01",
            "DNSName":
 "MyLB01-3b9c2b0f028f40e09d6306887646c28b.loadbalancing-jp-
east-1.cloud.global.fujitsu.com",
            "State": "InService",
            "ListenerDescriptions": {
              "member": {
                "Listener": {
                  "Protocol": "HTTPS",
                  "LoadBalancerPort": "443",
                  "InstanceProtocol": "HTTP",
                  "InstancePort": "80",
                  "SSLCertificateId": "1232d7bf-8f28-4cc7-a63d-44e218853c6d"
                },
                "PolicyNames": {
                  "member": "MyPolicy"
                }
              }
            },
            "Policies": {
              "LBCookieStickinessPolicies": {
                "member": {
                  "PolicyName": "MyLoadBalancerCookieStickinessPolicy",
                  "CookieExpirationPeriod": "60"
                }
              }
              "OtherPolicies": [
               {
                "member": "MyPolicy"
               }
              ]
            },
            "Subnets": {
              "member": "MySubnet"
            },
            "Instances": {
              "member": {
                "InstanceId": "i-e4cbe38d"
                "PortId": "p-e4cbe38d"
              }
            },
            "HealthCheck": {
              "Target": "HTTP:80",
              "Interval": "90",
              "Timeout": "60",
              "UnhealthyThreshold": "10",
              "HealthyThreshold": "2"
            },
            "SecurityGroups": {
              "member": "MySecurityGroup"
            },
            "CreatedTime": "2014-06-01T21:15:31.280Z",
            "Scheme": "Internal",
            "Grade": "Standard"
          }
        ]
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b12EXAMPLE"
    }
  }
```

```
}
```

1.6.5.16 DetachLoadBalancerFromSubnets

Description

Detaches the specified subnets from the set of configured subnets for the specified load balancer.

After a subnet is detached, the load balancer balances the requests among the remaining subnets.

If the subnet does not exist or has already been deleted, the call to this API will still be successful.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer to detach from.

  - Type: String
  - Required: Yes
- Subnets.member.N

  List of subnet IDs to detach from the load balancer.

  - Type: String list
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the DetachLoadBalancerFromSubnetsResult.

- Subnets

  List of subnet IDs attached to the load balancer.

  - Type: String list

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400

- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409

Examples

Sample request

The example below detaches the subnet with the ID MySubnet-XXXXX from the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Subnets.member.1=MySubnet-XXXXX
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=DetachLoadBalancerFromSubnets
```

Sample response (XML)

```
<DetachLoadBalancerFromSubnetsResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <DetachLoadBalancerFromSubnetsResult>
    <Subnets>
      <member>subnet-159f007c</member>
      <member>subnet-3561b05e</member>
    </Subnets>
  </DetachLoadBalancerFromSubnetsResult>
  <ResponseMetadata>
     <RequestId>07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE</RequestId>
  </ResponseMetadata>
</DetachLoadBalancerFromSubnetsResponse>
```

Sample response (JSON)

```
{
  "DetachLoadBalancerFromSubnetsResponse": {
    "DetachLoadBalancerFromSubnetsResult": {
      "Subnets": {
        "member": [
          "subnet-159f007c",
          "subnet-3561b05e"
        ]
      }
    },
   "ResponseMetadata": {
      "RequestId": "07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE"
    }
  }
}
```

1.6.5.17 ModifyLoadBalancerAttributes

Description

Modifies the attributes of the specified load balancer.

You can modify the period for maintaining the connection to the front and back ends of a load balancer in an idle state.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerAttributes

  Information about the load balancer attributes.

  - Type: *LoadBalancerAttributes* on page 164
  - Required: Yes
- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the ModifyLoadBalancerAttributesResult.

- LoadBalancerAttributes

  Information about the load balancer attributes.

  - Type: *LoadBalancerAttributes* on page 164
- LoadBalancerName

  Name of the load balancer.

  - Type: String

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400

Examples

Sample request

The example below modifies the ConnectionSettings attribute of the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerAttributes.ConnectionSettings.IdleTimeout=30
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action= ModifyLoadBalancerAttributes
```

Sample response (XML)

```
<ModifyLoadBalancerAttributesResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <ModifyLoadBalancerAttributesResult>
    <LoadBalancerName>MyLB01</LoadBalancerName>
    <LoadBalancerAttributes>
      <ConnectionSettings>
        <IdleTimeout>30</IdleTimeout>
      </ConnectionSettings>
    </LoadBalancerAttributes>
  </ModifyLoadBalancerAttributesResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b13EXAMPLE</RequestId>
  </ResponseMetadata>
</ModifyLoadBalancerAttributesResponse>
```

Sample response (JSON)

```
{
  "ModifyLoadBalancerAttributesResponse": {
    "ModifyLoadBalancerAttributesResult": {
      "LoadBalancerName": "MyLB01",
      "LoadBalancerAttributes": {
        "ConnectionSettings": {
          "IdleTimeout": "30"
        }
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b13XAMPLE"
    }
  }
}
```

1.6.5.18 RegisterInstancesWithLoadBalancer

Description

Adds the specified instances as distribution destinations to the specified load balancer.

After the instance is registered, the load will be distributed among it and the other existing instances.

Even if an IP address of a distribution destination instance registered to the load balancer is changed, the load will not be distributed to the new IP address.

The distribution destination instances registered to the load balancer are restarted, and the IP addresses are changed.

Distribution destination instances must be stopped before being deleted from a load balancer.

Distribution destination instances must be started before being registered to a load balancer.

Refer to "*DeregisterInstancesFromLoadBalancer* on page 191" for details on how to delete registered distribution destination instances from a load balancer.

This API can be used only by users with account privileges belonging to the same project as the account used when creating the load balancer.

Refer to "*DescribeLoadBalancers* on page 197" for details on how to check the status of registered distribution destination instances.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- Instances.member.N

  List of instance IDs to register to the load balancer.

  - Type: Instance list
  - Required: Yes
- LoadBalancerName

  Name of the load balancer to register the instances to.

  The name must be unique among the load balancers in the projects to which the account belongs.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

The following element is returned in a structure called the RegisterInstancesWithLoadBalancerResult.

- Instances

  List of updated distribution destination instances of the load balancer.

  - Type: *InstanceDescription* on page 161 list

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- InvalidEndPoint

  The specified EndPoint is not valid.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

Requested configuration change is invalid.

- HTTP Status Code: 409

Examples

Sample request

The example below registers the distribution destination instance with the ID i-315b7e51 to the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Instances.member.1.InstanceId=i-315b7e51
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=RegisterInstancesWithLoadBalancer
```

The example below registers the distribution destination instance with the ID i-315b7e51 and port ID p-315b7e51 to the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
Instances.member.1.InstanceId=i-315b7e51
&Instances.member.1.PortId=p-315b7e51
&LoadBalancerName=MyLB01
&Version=2014-11-01
&Action=RegisterInstancesWithLoadBalancer
```

Sample response (XML)

```
<RegisterInstancesWithLoadBalancerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <RegisterInstancesWithLoadBalancerResult>
    <Instances>
      <member>
        <InstanceId>i-712cde1e</InstanceId>
      </member>
      <member>
        <InstanceId>i-315b7e51</InstanceId>
        <PortId>p-315b7e51</PortId>
      </member>
    </Instances>
  </RegisterInstancesWithLoadBalancerResult>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b12EXAMPLE</RequestId>
  </ResponseMetadata>
</RegisterInstancesWithLoadBalancerResponse>
```

Sample response (JSON)

```
{
  "RegisterInstancesWithLoadBalancerResponse": {
    "RegisterInstancesWithLoadBalancerResult": {
      "Instances": {
        "member": [
          {
           "InstanceId": "i-712cde1e"
          },
          {
```

```
            "InstanceId": "i-315b7e51"
            "PortId": "p-315b7e51"
          }
        ]
      }
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b12EXAMPLE"
    }
  }
}
```

1.6.5.19 SetLoadBalancerListenerSSLCertificate

Description

Sets the certificate that terminates the specified listener's SSL connections.

The specified certificate replaces any prior certificate that was being used on the specified load balancer and port.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes
- LoadBalancerPort

  Port of the listener that uses the specified SSL certificate.

  - Type: Integer
  - Required: Yes
- SSLCertificateId

  Resource ID of the SSL certificate registered for the Key Management service.

  - Type: String
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- CertificateNotFound

  The specified SSL ID does not refer to a valid SSL certificate in the Key Management Service.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409
- ListenerNotFound

  Load balancer does not have a listener configured at the specified port.

  - HTTP Status Code: 400

Examples

Sample request

The example below sets the SSL certificate with ID 5c349f63-a874-47ed-b09e-9da913cbbbde for port 443 and the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
LoadBalancerName=MyLB01
&SSLCertificateId=5c349f63-a874-47ed-b09e-9da913cbbbde
&LoadBalancerPort=443
&Version=2014-11-01
&Action=SetLoadBalancerListenerSSLCertificate
```

Sample response (XML)

```
<SetLoadBalancerListenerSSLCertificateResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <SetLoadBalancerListenerSSLCertificateResult/>
  <ResponseMetadata>
    <RequestId>83c88b9d-12b7-11e3-8b82-87b12EXAMPLE</RequestId>
  </ResponseMetadata>
</SetLoadBalancerListenerSSLCertificateResponse>
```

Sample response (JSON)

```
{
  "SetLoadBalancerListenerSSLCertificateResponse": {
    "SetLoadBalancerListenerSSLCertificateResult": {
    },
    "ResponseMetadata": {
      "RequestId": "83c88b9d-12b7-11e3-8b82-87b12EXAMPLE"
    }
  }
}
```

1.6.5.20 SetLoadBalancerPoliciesOfListener

Description

Registers, deregisters, or changes policies applied to a listener of the load balancer.

If multiple listeners are set to ELB, all listeners apply a session stickiness policy and a SSL cryptographic protocol policy which are last registered.

Request parameters

Refer to "*Common Parameters* on page 158" for details on standard parameter information used by all actions.

- LoadBalancerName

  Name of the load balancer.

  - Type: String
  - Required: Yes
- LoadBalancerPort

  Port number of front-end connections for the listeners using the policies.

  - Type: Integer
  - Required: Yes
- PolicyNames.member.N

  List of policies to be applied to the listeners.

  If the list is empty, all current policies will be removed from the listener.

  - Type: String list
  - Required: Yes

Response

The following status code is returned:

- Normal response code

  This operation was accepted normally.

  - HTTP Status Code: 200

Response elements

n/a

Errors

Refer to "*Common Errors* on page 158" for details on error information common to all operations.

- AccessPointNotFound

  The specified load balancer could not be found.

  - HTTP Status Code: 400
- InvalidConfigurationRequest

  Requested configuration change is invalid.

  - HTTP Status Code: 409

- ListenerNotFound

  Load balancer does not have a listener configured at the specified port.

  - HTTP Status Code: 400
- PolicyNotFound

  One or more of the specified policies were not found.

  - HTTP Status Code: 400

Examples

Sample request

The example below applies the policy named MyLoadBalancerCookiePolicy to the listener in port 80 of the load balancer named MyLB01.

```
https://loadbalancing.(regionName).cloud.global.fujitsu.com/?
PolicyNames.member.1=MyLoadBalancerCookiePolicy
&LoadBalancerName=MyLB01
&LoadBalancerPort=80
&Version=2014-11-01
&Action=SetLoadBalancerPoliciesOfListener
```

Sample response (XML)

```
<SetLoadBalancerPoliciesOfListenerResponse xmlns=" http://
docs.cloudcommunity.global.fujitsu.com/loadbalancing/api/v1.0">
  <SetLoadBalancerPoliciesOfListenerResult/>
  <ResponseMetadata>
    <RequestId>07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE</RequestId>
  </ResponseMetadata>
</SetLoadBalancerPoliciesOfListenerResponse>
```

Sample response (JSON)

```
{
  "SetLoadBalancerPoliciesOfListenerResponse": {
    "SetLoadBalancerPoliciesOfListenerResult": {
    },
    "ResponseMetadata": {
      "RequestId": "07b1ecbc-1100-11e3-acaf-dd7edEXAMPLE"
    }
  }
}
```

1.7 SSL-VPN connection

1.7.1 API list

SSL-VPN

Item	API	Description
1	GET /v2.0/vpn/ssl-vpn-connections List SSL VPN Connections	Lists SSL-VPN connections
2	GET /v2.0/vpn/ ssl-vpn-connections / {sslvpnconnection-id} Shows details for a specified SSL VPN Connection	Shows details for the specified SSL-VPN connection
3	POST /v2.0/vpn/ssl-vpn-connections Create SSL VPN Connection	Creates SSL-VPN connections
4	PUT /v2.0/vpn/ ssl-vpn-connections / {sslvpnconnection-id} Update SSL VPN Connection	Updates the specified SSL-VPN connection
5	DELETE /v2.0/vpn/ ssl-vpn-connections / {sslvpnconnection-id} Delete SSL VPN Connection	Deletes the specified SSL-VPN connection

1.7.2 General requirements

This section describes general requirements to use this API.

- When executing the API that lists the resources, only some of the availability zone information may be returned. If this happens, it is assumed that infrastructure maintenance is in progress, so wait for a few moments (at least one minute) and then execute the API again.

1.7.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.7.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType

1.7.5 Notes

Note the following when using the SSL-VPN feature:

- Install OpenVPN client on the client.
- Obtain the following certificates, required for building SSL-VPN connection environments and setting up clients:
  - CA certificate of the server
  - Certificate of the client
  - Secret key of the client

1.7.6 API details

1.7.6.1 List SSL VPN Connections

Lists SSL VPN Connection

URI

/v2.0/vpn/ssl-vpn-connections

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Forbidden (403)	Error response codes

Response body (normal status)

```
{
  "ssl_vpn_connections":[
    {
      "id":"2322fdea-783d-923b-cc4e-abc023ed874f"
      "tenant_id": "1219ecaa01e0254dac4f08c9123aefcd",
      "name":"conn1",
      "status":"DOWN",
      "client_address_pool_cidr":"10.8.0.0/24",
      "credential_id": "434a9843-ecc0-4653-8f3a-e604d9d7aadc",
      "admin_state_up": true,
      "vpnservice_id":"cc91b7af-8304-4aff-ad07-86bdbaae2e93",
      "availability_zone": "AZ1"
    }
    {
      "id": "86445a53-c95c-4203-8382-6c88b768c4a0",
      "tenant_id": "1219ecaa01e0254dac4f08c9123aefcd ",
      "name": "conn2",
      "status": "ACTIVE",
      "client_address_pool_cidr": "10.8.1.0/24",
      "credential_id": "434a9843-ecc0-4653-8f3a-e604d9d7aadc ",
      "admin_state_up": true,
      "vpnservice_id": "2b0cff45-af8f-4605-8f0b-ad06517474d5",
      "availability_zone": "AZ2"
    }
  ]
}
```

Description of response body (normal status)

Item	Description
tenant_id	Unique identifier for owner of the SSL VPN connection.
name	name of the SSL VPN connection.
admin_state_up	Administrative state of the SSL VPN connection. If false (down), port does not forward packets.
client_address_pool_cidr	Client address pool subnet which will be used by sslvpn client
credential_id	UUID for VPNCredential Container on keymanagement.

Item	Description
	When you didn't specify this parameter at creating the resource, this value returns 'null'.
vpnservice_id	UUID for VPNService
id	UUID for SSL VPN connection Object.
status	Indicates whether the SSL VPN connection is currently operational. Possible values include: ACTIVE DOWN PENDING_CREATE ERROR
availability_zone	The Availability Zone name

1.7.6.2 Shows details for a specified SSL VPN Connection

Shows details for a specified SSL VPN Connection.

URI

/v2.0/vpn/ ssl-vpn-connections /{sslvpnconnection-id}

Description of the URI:

{sslvpnconnection-id} : Unique identifier for the SSL VPN Connection.

HTTP method

GET

Response codes

Status code	Description
200	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "ssl_vpn_connection":{
    "id":"2322fdea-783d-923b-cc4e-abc023ed874f",
    "tenant_id":"1219ecaa01e0254dac4f-08c9123aefcd",
    "name":"conn1",
    "status":"DOWN",
    "client_address_pool_cidr":"10.8.0.0/24",
    "credential_id": "434a9843-ecc0-4653-8f3a-e604d9d7aadc",
    "admin_state_up": true,
    "vpnservice_id":"cc91b7af-8304-4aff-ad07-86bdbaae2e93",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
tenant_id	Unique identifier for owner of the SSL VPN connection.
name	name of the SSL VPN connection.
admin_state_up	Administrative state of the SSL VPN connection. If false (down), port does not forward packets.
client_address_pool_cidr	Client address pool subnet which will be used by sslvpn client
credential_id	UUID for VPNCredential Container on keymanagement. When you didn't specify this parameter at creating the resource, this value returns 'null'.
vpnservice_id	UUID for VPNService
id	UUID for SSL VPN connection Object.
status	Indicates whether the SSL VPN connection is currently operational. Possible values include: ACTIVE DOWN PENDING_CREATE ERROR
availability_zone	The Availability Zone name

1.7.6.3 Create SSL VPN Connection

Creates an SSL VPN Connection.

URI

/v2.0/vpn/ssl-vpn-connections

HTTP method

POST

Request parameter

Key	Description	Type	Required/ optional
name	name of the SSL VPN connection (default: "")	string	Optional
admin_state_up	Administrative state of the SSL VPN connection. If false (down), port does not forward packets (default: true)	bool	Optional
client_address_pool_cidr	Client address pool subnet which will be used by sslvpn client	cidr	Required
credential_id	UUID for VPNCredential Container on keymanagement	uuid-str	Optional

Key	Description	Type	Required/ optional
	When you use client certificate offered by K5 to connect SSL-VPN, please omit this parameter.		
vpnservice_id	UUID for VPNService	uuid-str	Required
availability_zone	The Availability Zone name. If you don't specify, the resource will be created in default AZ. (default: default AZ selected)	string	Optional
protocol	Communication protocol used by VPN connection: tcp (only tcp can be specified but this parameter cannot be commited)	string	Required

Example request

```
{
  "ssl_vpn_connection":{
    "name":"conn1",
    "client_address_pool_cidr":"10.8.0.0/24",
    "admin_state_up": true,
    "credential_id": "434a9843-ecc0-4653-8f3a-e604d9d7aadc",
    "vpnservice_id":"cc91b7af-8304-4aff-ad07-86bdbaae2e93",
    "availability_zone": "AZ1"
    "protocol": "tcp"
  }
}
```

Response codes

Status code	Description
201	Normal response codes
Bad Request (400)	Error response codes
Unauthorized (401)	Error response codes

Response body (normal status)

```
{
  "ssl_vpn_connection":{
    "id":"76ee7216-5eef-470c-a7d2-ce4a7461b046",
    "name":"conn1",
    "status":"DOWN",
    "client_address_pool_cidr":"10.8.0.0/24",
    "credential_id": "434a9843-ecc0-4653-8f3a-e604d9d7aadc",
    "admin_state_up": true,
    "tenant_id":"1219ecaa01e0254dac4f08c9123aefcd",
    "vpnservice_id":"cc91b7af-8304-4aff-ad07-86bdbaae2e93",
    "availability_zone": "AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
tenant_id	Unique identifier for owner of the SSL VPN connection.
name	name of the SSL VPN connection.
admin_state_up	Administrative state of the SSL VPN connection. If false (down), port does not forward packets.
client_address_pool_cidr	Client address pool subnet which will be used by sslvpn client
credential_id	UUID for VPNCredential Container on keymanagement. When you didn't specify this parameter at creating the resource, this value returns 'null'.
vpnservice_id	UUID for VPNService
id	UUID for SSL VPN connection Object.
status	Indicates whether the SSL VPN connection is currently operational. Possible values include: ACTIVE DOWN PENDING_CREATE ERROR
availability_zone	The Availability Zone name

1.7.6.4 Update SSL VPN Connection

Updates an SSL VPN Connection.

URI

/v2.0/vpn/ ssl-vpn-connections /{sslvpnconnection-id}

Description of the URI:

{sslvpnconnection-id} : Unique identifier for the SSL VPN Connection.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
name	name of the vpn service	string	Optional
admin_state_up	Administrative state of vpnservice. If false (down), port does not forward packets.	bool	Optional

Example request

```
{
  "ssl_vpn_connection":{
    "name":"conn1A",
    "admin_state_up":false
```

```
  }
}
```

Response codes

Status code	Description
200	Normal response codes
Bad Request (400)	Error response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

Response body (normal status)

```
{
  "ssl_vpn_connection":{
    "id":"2322fdea-783d-923b-cc4e-abc023ed874f",
    "tenant_id":"1219ecaa01e0254dac4f08c9123aefcd",
    "name":"conn1A",
    "status":"DOWN",
    "client_address_pool_cidr":"10.8.0.0/24",
    "credential_id":"434a9843-ecc0-4653-8f3a-e604d9d7aadc",
    "admin_state_up":false,
    "vpnservice_id":"cc91b7af-8304-4aff-ad07-86bdbaae2e93",
    "availability_zone":"AZ1"
  }
}
```

Description of response body (normal status)

Item	Description
tenant_id	Unique identifier for owner of the SSL VPN connection.
name	name of the SSL VPN connection.
admin_state_up	Administrative state of the SSL VPN connection. If false (down), port does not forward packets.
client_address_pool_cidr	Client address pool subnet which will be used by sslvpn client
credential_id	UUID for VPNCredential Container on keymanagement. When you didn't specify this parameter at creating the resource, this value returns 'null'.
vpnservice_id	UUID for VPNService
id	UUID for SSL VPN connection Object.
status	Indicates whether the SSL VPN connection is currently operational. Possible values include: ACTIVE DOWN PENDING_CREATE ERROR
availability_zone	The Availability Zone name

1.7.6.5 Delete SSL VPN Connection

Deletes an SSL VPN Connection.

URI

/v2.0/vpn/ ssl-vpn-connections /{sslvpnconnection-id}

Description of the URI:

{sslvpnconnection-id} : Unique identifier for the SSL VPN Connection.

HTTP method

DELETE

Response codes

Status code	Description
204	Normal response codes
Unauthorized (401)	Error response codes
Not Found (404)	Error response codes

1.8 DNS service

1.8.1 API list

Item	API	Description
1	CreateHostedZone Create zone	Creates a zone
2	GetHostedZone Get zone information	Gets zone information
3	ListHostedZones List zone information	Lists zone information
4	DeleteHostedZone Delete zone	Deletes a zone
5	ChangeResourceRecordSets Create/delete record	Creates/deletes a record
6	ListResourceRecordSets List record information	Lists record information
7	GetChange Get update request information	Gets update request information

1.8.2 General requirements

This section describes general requirements to use this API.

- Unless otherwise stated, the request parameters must be sent by using HTTP GET or HTTP PUT.
- If a value in the request parameter contains a character that cannot be used as is in the URL, it must be encoded using UTF-8.

The following values are also required for this service:

- The user agent (User-Agent) string for the request of this service must be "FGCP-OS-API-CLIENT".

1.8.3 Common API request headers

Request headers

X-Auth-Token

Token to retrieve when user authentication is performed

Data type	Cardinality
String	1..1

Content-Type

This can only be specified for POST requests

Specify "application/xml"

Data type	Cardinality
String	0..1

Accept

Specify "application/xml"

Data type	Cardinality
String	0..1

1.8.4 Common API response headers

Response headers

x-fj-request-id

ID that uniquely identifies the request.

This is required when contacting support staff to troubleshoot an issue.

UUID format (example: 647cd254-e0d1-44a9-af61-1d6d86ea6b77)

Data type	Cardinality
String	1..1

1.8.5 Common API errors

- Authentication error

HTTP status

Status

The following error codes can be returned for the request.

401: Authentication error

Data type	Cardinality
Int	1..1

Response elements

n/a

Example of response

```
HTTP/1.1 401 Unauthorized
Date: Fri, 06 Jun 2014 11:00:38 GMT
```

- Access denied

HTTP status

Status

The following error codes can be returned for the request.

403: Access denied

Data type	Cardinality
Int	1..1

Response elements

AccessDeniedException

Envelope of error response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	Message

Message

Error message.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	AccessDeniedException	None

Example of response

```
HTTP/1.1 403 Forbidden
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<AccessDeniedException>
  <Message>Access Denied</Message>
</AccessDeniedException>
```

- Errors other than authentication error/access denied

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

400:	XML format of request is incorrect
500:	Internal server error
5xx:	Error when an AZ goes down The query sent by the user varies depending on when the AZ goes down, resulting in various behaviors. Therefore, (5xx) returned by the HTTP status code prompts the user to retry.

Data type	Cardinality
Int	1..1

Response elements

ErrorResponse

Envelope of error response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	Error RequestId

Error

Envelope of error information.

Data type	Cardinality	Parent element	Child element
-	1..1	ErrorResponse	Type Code Message

Type

Sender or Receiver.

Indicates whether the error was caused by the sender or the receiver.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	Error	None

Code

Error code.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	Error	None

Message

Error message (English).

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	Error	None

RequestId

ID that uniquely identifies the request.

This is required when contacting support staff to troubleshoot an issue.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ErrorResponse	None

Example of response

```
HTTP/1.1 400 Bad Request
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: 2844de70-360d-488d-bd63-0cd88fd94be1
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< ErrorResponse xmlns="http://docs.cloudcommunity.global.fujitsu.com/dns/
api/v1.0/">
  <Error>
    <Type>Sender</Type>
    <Code>InvalidInput</Code>
    <Message>The specified Action is not valid</Message>
    </Error>
    <RequestId>2844de70-360d-488d-bd63-0cd88fd94be1</RequestId>
</ErrorResponse>
```

1.8.6 API details

1.8.6.1 Create zone (POST /v1.0/hostedzone)

Creates a zone.

Specify the necessary information in the request body, and a zone will be created based on that information.

Up to 100 zones can be registered.

When the API is executed, authentication is performed using a confirmation code in order to confirm the ownership rights of the domain.

When this API is executed for the first time, an Unauthorised error occurs. When an Unauthorized error occurs, set the confirmation code in the error message of the response in the registrar or DNS, and reexecute this API.

If a create zone API of the same name is executed concurrently with a zone that is being created, a 500 Internal Error will occur, so retry the operation.

Request headers

n/a

Request parameters

n/a

Request elements

CreateHostedZoneRequest

Request envelope.

Data type	Cardinality	Parent element	Child element
-	1..1	None	Name HostedZoneConfig

Name

Zone name. FQDN format.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	CreateHostedZoneRequest	None

HostedZoneConfig

Envelope of appended information.

Data type	Cardinality	Parent element	Child element
-	0..1	CreateHostedZoneRequest	Comment

Comment

Comment. Specify up to 255 fullwidth characters.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	HostedZoneConfig	None

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

201:	Normal completion
400:	Authentication required/invalid zone name
404:	Invalid zone name was specified
409:	Existing zone name was specified

Data type	Cardinality
Int	1..1

Response elements (normal completion)

CreateHostedZoneResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	HostedZone ChangeInfo DelegationSet

HostedZone

Envelope of the zone information.

Data type	Cardinality	Parent element	Child element
-	1..1	CreateHostedZoneResponse	Id Name CallerReference Config ResourceRecordSetCount

Id

ID of the zone that was created. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Name

Name of the zone that was created. Normalized value.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

CallerReference

Identifier of the zone that was created. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Config

Envelope of appended information.

Data type	Cardinality	Parent element	Child element
-	1..1	HostedZone	Comment

Comment

Comment.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	Config	None

ResourceRecordSetCount

Number of records registered in the host zone.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

ChangeInfo

Envelope of the update request information.

Data type	Cardinality	Parent element	Child element
-	1..1	CreateHostedZoneResponse	Id Status SubmittedAt

Id

Update request ID.

The ID is used by the GetChange API to retrieve update request information.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Status

Current status of an update request.

PENDING or INSYNC.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

SubmittedAt

Datetime when update request was issued. Format: YYYY-MM-DDThh:mm:ss.SSSZ

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

DelegationSet

Envelope of the name server information.

Data type	Cardinality	Parent element	Child element
-	1..1	CreateHostedZoneResponse	NameServers

NameServers

Envelope of the name server list.

Data type	Cardinality	Parent element	Child element
-	1..1	DelegationSet	NameServer

NameServer

Name server allocated to the zone.

Data type	Cardinality	Parent element	Child element
xsd:string	1..n	NameServers	None

Example of request

```
POST /v1.0/hostedzone HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Content-Type: application/xml
Accept: application/xml
X-Auth-Token: MIIFvgY...

<?xml version="1.0" encoding="UTF-8"?>
< CreateHostedZoneRequest xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <Name>example.com</Name>
  <HostedZoneConfig>
    <Comment>comment</Comment>
  </HostedZoneConfig>
</CreateHostedZoneRequest>
```

Example of response

```
HTTP/1.1 201 Created
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< CreateHostedZoneResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <HostedZone>
    <Id>example.com</Id>
    <Name>example.com<Name>
    <CallerReference>example.com</CallerReference>
    <Config>
      <Comment>comment</Comment>
    </Config>
    <ResourceRecordSetCount>0</ResourceRecordSetCount>
  </HostedZone>
  <ChangeInfo>
    <Id>cb7faf29ae2bb2bd489d0d27b36e28fc</Id>
    <Status>INSYNC</Status>
    <SubmittedAt>2014-06-06T11:00:38.370Z</SubmittedAt>
  </ChangeInfo>
  <DelegationSet>
    <NameServers>
      <NameServer>cdns0.nifty.ad.jp</NameServer>
      <NameServer>cdns1.nifty.ad.jp</NameServer>
    </NameServers>
  </DelegationSet>
</CreateHostedZoneResponse>
```

Flow of authentication using a confirmation code to confirm ownership rights of a domain

- When using the CreateHostedZone API, authentication using a confirmation code is required to confirm if the domain of the zone to be created is the domain owned by the user who executed the API.

  The method for setting up the confirmation code is shown below.

  The setup method is different depending on whether the domain to be specified is a newly retrieved domain (not managed by any DNS yet) or an existing domain (already managed by another DNS).
- Confirmation code retrieval method:

  Specify the same parameters as the zone scheduled for creation, and execute the CreateHostedZone API. Execution of the API will result in an Unauthorized error, so retrieve the confirmation code that is output to the error message.

```
Response Body:
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< ErrorResponse xmlns="http://docs.cloudcommunity.global.fujitsu.com/dns/
api/v1.0/">
<Error><Type>Sender</Type><Code>Unauthorized</Code>
<Message>name_server:f0094d76e096551441d24af257488a6a.cdns-
verify.nifty.ad.jp,txt:nifty-dns-
verify=f0094d76e096551441d24af257488a6a</Message>
</Error><RequestId>req-ac1ac325-2880-4cf5-8e5f-42dc9097b5d4</RequestId></
ErrorResponse>
```

- Confirmation code setup method for a newly retrieved domain:

  Set a name server in the registrar.

```
name_server:f0094d76e096551441d24af257488a6a.cdns-verify.nifty.ad.jp
```

- Confirmation code setup method for an existing domain:

  Set a text record in the DNS.

```
txt:nifty-dns-verify=f0094d76e096551441d24af257488a6a
```

1.8.6.2 Retrieve zone information (GET /v1.0/hostedzone/{*zoneId* })

Retrieves zone information.

Specification of the zone information to be retrieved is performed using the zone ID which is included in the request URL.

Zone and name server information are retrieved

*The zone ID is the same value as the zone name.

Request headers

n/a

Request parameters

n/a

Request elements

n/a

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

200:	Normal completion
400:	Invalid zone ID
404:	A zone with the specified ID does not exist

Data type	Cardinality
Int	1..1

Response elements (normal completion)

GetHostedZoneResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	HostedZone DelegationSet

HostedZone

Envelope of the zone information.

Data type	Cardinality	Parent element	Child element
-	1..1	GetHostedZoneResponse	Id Name CallerReference Config ResourceRecordSetCount

Id

Zone ID. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Name

Zone name. Normalized value.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

CallerReference

Zone identifier. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Config

Envelope of appended information.

Data type	Cardinality	Parent element	Child element
-	1..1	HostedZone	Comment

Comment

Comment.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	Config	None

ResourceRecordSetCount

Number of records registered in the host zone.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

DelegationSet

Envelope of the name server information.

Data type	Cardinality	Parent element	Child element
-	1..1	GetHostedZoneResponse	NameServers

NameServers

Envelope of the name server list.

Data type	Cardinality	Parent element	Child element
-	1..1	DelegationSet	NameServer

NameServer

Name server allocated to the zone.

Data type	Cardinality	Parent element	Child element
xsd:string	1..n	NameServers	None

Example of request

```
GET /hostedzone/example.com HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
```

```
X-Auth-Token: MIIFvgY...
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< GetHostedZoneResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <HostedZone>
    <Id>example.com</Id>
    <Name>example.com</Name>
    <CallerReference>example.com</CallerReference>
    <Config>
      <Comment>comment</Comment>
    </Config>
    <ResourceRecordSetCount>0</ResourceRecordSetCount>
  </HostedZone>
  <DelegationSet>
    <NameServers>
      <NameServer>cdns0.nifty.ad.jp</NameServer>
      <NameServer>cdns1.nifty.ad.jp</NameServer>
    </NameServers>
  </DelegationSet>
</GetHostedZoneResponse>
```

1.8.6.3 List zone information (GET /v1.0/hostedzone)

Lists zone information.

You can use the URL parameters in the request to specify the first zone ID for which information is to be retrieved, and the maximum number of records to be retrieved.

*The zone ID is the same value as the zone name.

Request headers

n/a

Request parameters

marker

Retrieval start zone ID.

If omitted, zone information will be retrieved from the beginning.

Data type	Cardinality
String	0..1

maxitems

Maximum number of records to retrieve. Up to 100.

If omitted, 100 will be used.

Data type	Cardinality
String	0..1

Request elements

n/a

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

200:	Normal completion
400:	The zone ID specified in "marker" does not exist, or the values specified in "maxitems" is outside the range of 1 to 100

Data type	Cardinality
Int	1..1

Response elements (normal completion)

ListHostedZonesResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	HostedZones Marker IsTruncated NextMarker MaxItems

HostedZones

Envelope of the zone information list.

Data type	Cardinality	Parent element	Child element
-	1..1	ListHostedZonesResponse	HostedZone

HostedZone

Envelope of the zone information.

Data type	Cardinality	Parent element	Child element
-	1..n	HostedZones	Id Name CallerReference Config

Data type	Cardinality	Parent element	Child element
			ResourceRecordSetCount

Id

Zone ID. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Name

Zone name. Normalized value.

Data Type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

CallerReference

Zone identifier. Same value as the zone name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Config

Envelope of appended information.

Data type	Cardinality	Parent element	Child element
-	1..1	HostedZone	Comment

Comment

Comment.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	Config	None

ResourceRecordSetCount

Number of records registered in the host zone.

Data Type	Cardinality	Parent element	Child element
xsd:string	1..1	HostedZone	None

Marker

Retrieval start zone ID specified in the request.

Data Type	Cardinality	Parent element	Child element
xsd:string	0..1	ListHostedZonesResponse	None

IsTruncated

Indicates whether there is zone information that has not been returned.

true or false.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ListHostedZonesResponse	None

NextMarker

Retrieval start zone ID of zone information that has not been returned.

This is returned when IsTruncated is true.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ListHostedZonesResponse	None

MaxItems

Maximum number of records for retrieval specified in request.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ListHostedZonesResponse	None

Example of request

```
GET /hostedzone HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
X-Auth-Token: MIIFvgY...
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< ListHostedZonesResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <HostedZones>
    <HostedZone>
      <Id>example.com</Id>
      <Name>example.com</Name>
      <CallerReference>example.com</CallerReference>
      <Config>
        <Comment>comment</Comment>
      </Config>
      <ResourceRecordSetCount>0</ResourceRecordSetCount>
    </HostedZone>
  <HostedZone>
...
  </HostedZone>
  </HostedZones>
  <IsTruncated>false</IsTruncated>
  <MaxItems>100</MaxItems>
</ListHostedZonesResponse>
```

1.8.6.4 Delete zone (DELETE /v1.0/hostedzone/{*zoneId* })

- Deletes a zone.
- Specify the zone to be deleted by using the zone ID in the request.
- When a zone is deleted, all records that have been set for that zone are also deleted.
- Even if a zone is deleted, the domain will not be discontinued.
- If a delete zone API is executed concurrently with operation of the record update API in the same zone, a 500 Internal Error will occur, so retry the operation.

*The zone ID is the same value as the zone name.

Request headers

n/a

Request parameters

n/a

Request elements

n/a

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

200:	Normal completion
400:	Invalid input parameter
404:	The zone of the specified zone ID does not exist

Data type	Cardinality
Int	1..1

Response elements (normal completion)

DeleteHostedZoneResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	ChangeInfo

ChangeInfo

Envelope of the update request information.

Data type	Cardinality	Parent element	Child element
-	1..1	ListHostedZonesResponse	Id Status

Data type	Cardinality	Parent element	Child element
			SubmittedAt

Id

Update request ID.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Status

Update status.

PENDING or INSYNC.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

SubmittedAt

Datetime of update request. Format: YYYY-MM-DDThh:mm:ss.SSSZ

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Example of request

```
DELETE /hostedzone/example.com HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
X-Auth-Token: MIIFvgY...
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< DeleteHostedZoneResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <ChangeInfo>
    <Id>d36956475553d655cf70a293adeb155c</Id>
    <Status>INSYNC</Status>
    <SubmittedAt>2014-06-06T11:00:38.178Z</SubmittedAt>
  </ChangeInfo>
</DeleteHostedZoneResponse>
```

1.8.6.5 Create/delete record (POST v1.0/hostedzone/{*zoneId*}/rrset)

- Creates and deletes records.
- The types of records that can be registered are NS, A, AAAA, CNAME, MX, TXT, and LBR (for latency-based routing).
- The SOA record settings cannot be changed.
- Create/delete operations can be specified for multiple records in a single request. They are handled as a single transaction, so are not reflected in parts.
- Because record creation/deletion is not reflected immediately, the response will return the update request information.

  The update will be complete when the update status changes from PENDING to INSYNC.
- Up to 10,000 records can be registered for each zone.
- When a record is deleted, the data with matching Name, Type, and Value is erased.
- If create or delete record APIs are executed concurrently in the same zone, a 500 Internal Error will occur, so retry the operation.

*The zone ID is the same value as the zone name.

Request headers

n/a

Request parameters

n/a

Request elements

ChangeResourceRecordSetsRequest

Request envelope.

Data type	Cardinality	Parent element	Child element
-	1..1	None	ChangeBatch

ChangeBatch

Envelope of record transaction.

Data type	Cardinality	Parent element	Child element
-	1..1	ChangeResourceRecordSetsRequest	Comment Changes

Comment

Comment for the record transaction.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ChangeBatch	None

Changes

Envelope of change content list.

Data type	Cardinality	Parent element	Child element
-	1..1	ChangeBatch	Change

Change

Envelope of change content.

Data type	Cardinality	Parent element	Child element
-	1..n	Changes	Action ResourceRecordSet

Action

Type of record operation. CREATE or DELETE.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	Change	None

ResourceRecordSet

Envelope of the record information.

Data type	Cardinality	Parent element	Child element
-	1..1	Change	Name Type SetIdentifier Weight XniftyDefaultHost Failover XniftyHealthCheckConfig TTL ResourceRecords XniftyComment

Name

Record name.

Input limitation:

Alphanumeric character (a-z,0-9) , Wild-card (*) , At mark (@) and Hyphen(-) are available.

Specify 1 or more and 63 or less character

Wildcards can be specified for A, AAAA, MX, and CNAME records, as long as Weight and Failover are not specified.

The at mark (@) can be specified for A, AAAA, MX, and TXT records, as long as Failover is not specified.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

Type

Record type.

NS, A, AAAA, CNAME, MX, TXT, LBR.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

SetIdentifier

Record identification information.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

Weight

Weighting value. 0 to 100.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

XniftyDefaultHost

Default host information.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

Failover

Failover type. PRIMARY or SECONDARY.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

XniftyHealthCheckConfig

Envelope of health check information.

Data type	Cardinality	Parent element	Child element
-	0..1	ResourceRecordSet	IPAddress Port Protocol ResourcePath FullyQualifiedDomainName

IPAddress

Health check destination IP address.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

Port

Health check destination port.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

Protocol

Health check type. HTTP, HTTPS, TCP.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

ResourcePath

Health check destination path.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	XniftyHealthCheckConfig	None

FullyQualifiedDomainName

Health check destination domain name.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	XniftyHealthCheckConfig	None

TTL

TTL value. 60 to 86400 seconds. If omitted, the zone TTL will be used.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

ResourceRecords

Envelope of record response information list.

Data type	Cardinality	Parent element	Child element
-	1..1	ResourceRecordSet	ResourceRecord

ResourceRecord

Envelope of record response information.

Data type	Cardinality	Parent element	Child element
-	1..n	ResourceRecords	Value

Value

Record response value. Multibyte domains can be set for CNAME, MX and NS records.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecord	None

XniftyComment

Comment. Specify up to 255 fullwidth characters.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

200:	Normal completion
400:	Invalid input parameter
404:	A zone with the specified ID does not exist

Data type	Cardinality
Int	1..1

Response elements (normal completion)

ChangeResourceRecordSetsResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	ChangeInfo

ChangeInfo

Envelope of the update request information.

Data type	Cardinality	Parent element	Child element
-	1..1	ChangeResourceRecordSetsResponse	Id Status SubmittedAt

Id

Update request ID.

The ID is used by the GetChange API to retrieve update request information.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Status

Current status of an update request.

PENDING or INSYNC.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

SubmittedAt

Datetime when update request was issued. Format: YYYY-MM-DDThh:mm:ss.SSSZ

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Example of request

```
POST /hostedzone/example.com/rrset HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
X-Auth-Token: MIIFvgY...
<?xml version="1.0" encoding="UTF-8"?>
< ChangeResourceRecordSetsRequest xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <ChangeBatch>
    <Changes>
      <Change>
        <Action>CREATE</Action>
        <ResourceRecordSet>
          <Name>server.example.com</Name>
          <Type>A</Type>
          <TTL>60</TTL>
          <ResourceRecords>
             <ResourceRecord>
               <Value>222.158.xxx.yyy</Value>
             </ResourceRecord>
          </ResourceRecords>
        </ResourceRecordSet>
      </Change>
    </Changes>
  </ChangeBatch>
</ChangeResourceRecordSetsRequest>
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< ChangeResourceRecordSetsResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <ChangeInfo>
    <Id>7a782d43939d7ff538ff1ee19dbdd5a0</Id>
    <Status>INSYNC</Status>
    <SubmittedAt>2014-06-06T11:00:38.178Z</SubmittedAt>
  </ChangeInfo>
</ChangeResourceRecordSetsResponse>
```

Failover settings

- Failover settings

  The failover settings are specified using Failover tags. They can only be specified for A and AAAA records.

- PRIMARY: Only 1 record can be set.
- SECONDARY: Multiple settings are possible.

- Heath check

  Health checks are to be specified in the failover settings.

  This is set using the XniftyHealthCheckConfig tag.

  Health check rules

  - Individual health checks specified for each record are executed.
  - The switch target for failover is executed with the same host/same record type as 1 group.
  - If multiple records are specified for secondary, they will be prioritized in order of registration.

```
<XniftyHealthCheckConfig>
  <IPAddress>targetIpAddr</IPAddress>
  <Port>targetPortNum</Port>
  <Protocol>targetProtocol</Protocol>
  <ResourcePath>targetUrlPathSection</ResourcePath>
  <FullyQualifiedDomainName>httpHeaderHostInfo</FullyQualifiedDomainName>
</XniftyHealthCheckConfig>
```

  Caution

  When using failover, it is recommended to set the record TTL to 60 seconds.

- Example failover settings (ResourceRecordSet)

```
<ResourceRecordSet>
  <Name>server1.example.com</Name>
  <Type>A</Type>
  <Failover>PRIMARY</Failover>
  <XniftyHealthCheckConfig>
    <IPAddress>222.158.xxx.yyy</IPAddress>
    <Port>80</Port>
    <Protocol>HTTP</Protocol>
  </XniftyHealthCheckConfig>
  <ResourceRecords>
    <ResourceRecord>
      <Value>222.158.xxx.yyy</Value>
    </ResourceRecord>
  </ResourceRecords>
</ResourceRecordSet>
<ResourceRecordSet>
  <Name>server2.example.com</Name>
  <Type>A</Type>
  <Failover>SECONDARY</Failover>
  <XniftyHealthCheckConfig>
    <IPAddress>222.158.xxx.zzz</IPAddress>
    <Port>80</Port>
    <Protocol>HTTP</Protocol>
  </XniftyHealthCheckConfig>
  <ResourceRecords>
    <ResourceRecord>
      <Value>222.158.xxx.zzz</Value>
    </ResourceRecord>
  </ResourceRecords>
</ResourceRecordSet>
```

LBR settings

- Settings for latency-based routing (LBR)

For the LBR settings, set the type to "LBR".

Inside the Value tags, the area and host are delimited by a halfwidth space.

```
<Value>area host<Value>
```

For *area*, specify the nearest area.

10:	Japan
20:	Asia
30:	North America

For *host*, specify the value to be returned when there is access from the specified area. Registered A/AAAA records can be specified in the same zone.

Use sub-domain notation instead of FQDN for the host.

(in the LBR setting example below, www.example.com is specified as the default zone and registered in Japan, while www2.example.com is registered in Asia.)

Inside the XniftyDefaultHost tags, specify the value to be returned when there is access from outside the specified area.

- Example LBR settings (ResourceRecordSet)

```
<Changes>
  <Change>
    <Action>CREATE</Action>
    <ResourceRecordSet>
      <Name>server.example.com</Name>
      <Type>LBR</Type>
      <XniftyDefaultHost>www</XniftyDefaultHost>
      <ResourceRecords>
        <ResourceRecord>
          <Value>10 www,20 www2</Value>
        </ResourceRecord>
      </ResourceRecords>
    </ResourceRecordSet>
  </Change>
</Changes>
```

LBR settings

- Settings for a weighted round robin

  Specify the weighting value in the Weight tags. They can only be specified for A and AAAA records.

  The record hit rate varies according to the specified weighting value.
- Notes
  - If there are no records with a weighting of 100 in the weighting setting value, the target record may not be returned when resolving the name.
  - When the weighting setting value is set to 0, the hit rate will be 0, so no value will be returned.
  - For normal record registration, when records of the same host/same record type are registered, they are handled as a weighting of 100.
- Example weighted round robin settings (ResourceRecordSet)

```
<ResourceRecordSet>
  <Name>server.example.com</Name>
  <Type>A</Type>
```

```
  <Weight>100</Weight>
  <TTL>60</TTL>
  <ResourceRecords>
    <ResourceRecord>
      <Value>222.158.xxx.yyy</Value>
    </ResourceRecord>
  </ResourceRecords>
</ResourceRecordSet>
<ResourceRecordSet>
  <Name>server.example.com</Name>
  <Type>A</Type>
  <Weight>100</Weight>
  <TTL>60</TTL>
  <ResourceRecords>
    <ResourceRecord>
      <Value>222.158.xxx.zzz</Value>
    </ResourceRecord>
  </ResourceRecords>
</ResourceRecordSet>
```

MX record settings

- MX record settings

  Separate the priority from the host using a halfwidth space in the Value tag inside the ResourceRecord.

  ```
  <Value>priority host</Value>
  ```

- Example MX record settings

Priority:	10
Host:	mail.example.com

  ```
  <ResourceRecordSet>
    <Name>@</Name>
    <Type>MX</Type>
    <TTL>60</TTL>
    <ResourceRecords>
      <ResourceRecord>
        <Value>10 mail.example.com</Value>
      </ResourceRecord>
    </ResourceRecords>
  </ResourceRecordSet>
  ```

PTR record settings

- PTR record settings

  Currently, PTR records cannot be set.

1.8.6.6 List record information (GET /v1.0/hostedzone/{*zoneId*}/rrset)

Lists the record information.

Specify the URL request parameters to determine the record position (name, type, identification information) where retrieval starts from, and the maximum number of records to be retrieved.

By specifying the record position, a search is performed as follows:

- Record position not specified: Retrieval will start from the first record in the zone.
- Only the name is specified: Retrieval will start from the first record that matches the name.
- The name and type are specified: Retrieval will start from the first record that matches the name and type.
- The name, type, and identification information are specified: Retrieval will start from the first record that matches the name, type, and identification information.

If a record position combination other than the above is specified, an error will occur.

*The zone ID is the same value as the zone name.

Request headers

n/a

Request parameters

name

Record name (domain). FQDN format.

Data type	Cardinality
String	0..1

type

Record type.

NS, A, AAAA, CNAME, MX, TXT, LBR.

Data type	Cardinality
String	0..1

identifer

Record identification information.

Random string created by the system during registration.

Data type	Cardinality
String	0..1

maxitems

Maximum number of records to retrieve. Up to 100.

If omitted, 100 will be used.

Data type	Cardinality
String	0..1

Request elements

n/a

HTTP status

Status

The following error codes can be returned for the request.
One of the following values will be returned:

200:	Normal completion
400:	maxitems is outside the range of 1 to 100
404:	A zone with the specified ID does not exist

Data type	Cardinality
Int	1..1

Response elements (normal completion)

ListResourceRecordSetsResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	ResourceRecordSets IsTruncated MaxItems NextRecordName NextRecordType NextRecordIdentifier

ResourceRecordSets

Envelope of the record information list.

Data type	Cardinality	Parent element	Child element
-	1..1	ListResourceRecordSetsResponse	ResourceRecordSet

ResourceRecordSet

Envelope of the record information.

Data type	Cardinality	Parent element	Child element
-	1..n	ResourceRecordSets	Name Type SetIdentifier Weight XniftyDefaultHost Failover XniftyHealthCheckConfig TTL ResourceRecords XniftyComment

Name

Record name.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

Type

Record type.

NS, A, AAAA, CNAME, MX, TXT, LBR.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

SetIdentifier

Record identification information.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

Weight

Weighting value.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

XniftyDefaultHost

Default host information.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

Failover

Failover type. PRIMARY or SECONDARY.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

XniftyHealthCheckConfig

Envelope of health check information.

Data type	Cardinality	Parent element	Child element
-	0..1	ResourceRecordSet	IPAddress Port Protocol ResourcePath FullyQualifiedDomainName

IPAddress

Health check destination IP address.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

Port

Health check destination port.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

Protocol

Health check type.

HTTP, HTTPS, TCP.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	XniftyHealthCheckConfig	None

ResourcePath

Health check destination path.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	XniftyHealthCheckConfig	None

FullyQualifiedDomainName

Health check destination domain name.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	XniftyHealthCheckConfig	None

TTL

TTL value.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ResourceRecordSet	None

ResourceRecords

Envelope of the record response information list.

Data type	Cardinality	Parent element	Child element
-	1..1	ResourceRecordSet	ResourceRecord

ResourceRecord

Envelope of record response information.

Data type	Cardinality	Parent element	Child element
-	1..n	ResourceRecords	Value

Value

Record response value.

Data type	Cardinality	Parent element	Child Element(s)
xsd:string	1..1	ResourceRecord	None

XniftyComment

Comment.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ResourceRecordSet	None

IsTruncated

Indicates whether there is zone information that has not been returned. true or false.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ListResourceRecordSetsResponse	None

MaxItems

Maximum number of records for retrieval specified in request.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ListResourceRecordSetsResponse	None

NextRecordName

Retrieval start record name of record information that has not been returned.
This is returned when IsTruncated is true.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ListResourceRecordSetsResponse	None

NextRecordType

Retrieval start record name of record information that has not been returned.
This is returned when IsTruncated is true.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ListResourceRecordSetsResponse	None

NextRecordIdentifier

Retrieval start record name of record information that has not been returned.
This is returned when IsTruncated is true.

Data type	Cardinality	Parent element	Child element
xsd:string	0..1	ListResourceRecordSetsResponse	None

Example of request

```
GET /hostedzone/example.com/rrset HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
X-Auth-Token: MIIFvgY...
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< ListResourceRecordSetsResponse xmlns="http://
docs.cloudcommunity.global.fujitsu.com/dns/api/v1.0/">
  <ResourceRecordSets>
    <ResourceRecordSet>
      <Name>example.com</Name>
      <Type>MX</Type>
      <SetIdentifier>uLrNgSC4yzg=</SetIdentifier>
      <TTL>60</TTL>
      <ResourceRecords>
        <ResourceRecord>
          <Value>10 mail.example.com</Value>
        </ResourceRecord>
      </ResourceRecords>
    </ResourceRecordSet>
    <ResourceRecordSet>
    ...
    </ResourceRecordSet>
  </ResourceRecordSets>
  <IsTruncated>false</IsTruncated>
  <MaxItems>100</MaxItems>
</ListResourceRecordSetsResponse>
```

1.8.6.7 Retrieve update request information (GET /v1.0/change/{*updateRequestId* })

Retrieves update request information.

Update request information is retrieved by specifying the update request ID in the request.

The update request ID is set in the response body of the update system API.

*This API only supports update request IDs when the update system API is successful. The update system API is as follows:

- CreateHostedZone
- DeleteHostedZone
- ChangeResourceRecordSets

Request headers

n/a

Request parameters

n/a

Request elements

n/a

HTTP status

Status

The following error codes can be returned for the request.

One of the following values will be returned:

200:	Normal completion
404:	The update request ID does not exist

Data type	Cardinality
Int	1..1

Response elements (normal completion)

GetChangeResponse

Envelope of the response.

Data type	Cardinality	Parent element	Child element
-	1..1	None	ChangeInfo

ChangeInfo

Envelope of the update request information.

Data type	Cardinality	Parent element	Child element
-	1..1	ListHostedZonesResponse	Id Status SubmittedAt

Id

Update request ID.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Status

Update status.

PENDING or INSYNC.

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

SubmittedAt

Datetime of update request. Format: YYYY-MM-DDThh:mm:ss.SSSZ

Data type	Cardinality	Parent element	Child element
xsd:string	1..1	ChangeInfo	None

Example of request

```
GET /change/d36956475553d655cf70a293adeb155c HTTP/1.1
Date: Fri, 06 Jun 2014 11:00:37 GMT
Content-Length: ...
Host: dns.gls.cloud.global.fujitsu.com
Accept: application/xml
X-Auth-Token: MIIFvgY...
```

Example of response

```
HTTP/1.1 200 OK
Date: Fri, 06 Jun 2014 11:00:38 GMT
Content-Length: ...
Content-Type: application/xml
x-fj-request-id: d96bd874-9bf2-11e1-8ee7-c98a0037a2b6
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
< GetChangeResponse xmlns="http://docs.cloudcommunity.global.fujitsu.com/
dns/api/v1.0/">
  <ChangeInfo>
    <Id>dcd102450ad397f197cb9f09755964f7</Id>
    <Status>INSYNC</Status>
    <SubmittedAt>2014-06-06T11:00:38.178Z</SubmittedAt>
  </ChangeInfo>
</GetChangeResponse>
```

1.9 Network connector expansion

1.9.1 API list

Layer-3 networking (routers)

Item	API	Description
1	PUT /v2.0/routers/{router_id}/ add_cross_project_router_interface Adds an internal interface to a logical router.	Specify a port on the network of a tenant that is different to the logical router within the same domain, and create the connection interface.
2	PUT /v2.0/routers/{router_id}/ remove_cross_project_router_interface Removes an internal interface from a logical router.	Specify a port on the network of a tenant that is different to the logical router within the same domain, and delete the connection interface.
3	PUT /v2.0/routers/{router_id} Updates a logical router.	Updates the routing information between different tenants within the same domain.

1.9.2 General requirements

This section describes general requirements to use this API.

- Set the version of the IP address to be specified in the request parameter to "4" ("ip_version": 4), and specify the IP address (XXX_ip_address) in IPv4 format.

1.9.3 Common API items

Request header

Parameter	Description	Remarks
Content-Type	application/json	-
Accept	application/json	-
X-Auth-Token	authentication token	-

1.9.4 Common API error codes

Examples of common API error codes

Response codes

Status code	Description
500,400,other codes possible	computeFault
501	notImplemented
503	serverCapacityUnavailable
503	serviceUnavailable
400	badRequest
401	unauthorized
403	forbidden
403	resizeNotAllowed
404	itemNotFound
405	badMethod
409	backupOrResizeInProgress
409	buildInProgress
409	conflictingRequest
413	overLimit
413	badMediaType

1.9.5 API details

1.9.5.1 Add interface to router (Create connection interface)

Adds an internal interface to a logical router.

Specify a port on the network of a tenant that is different to the logical router within the same domain, and create the connection interface.

URI

/v2.0/routers/{router_id}/add_cross_project_router_interface

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
port_id	The port ID.	csapi:UUID	MUST

Example request

```
{
   "port_id": "a2f1f29d-571b-4533-907f-5803ab96ead1"
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1",
    "port_id": " 1accb5ac-b258-483e-af3a-f41f6df8190c",
    "tenant_id": " e10f4ade5a7649c49e1a6817196516ad",
    "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
    "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
subnet_id	The subnet ID.
port_id	The port ID.
tenant_id	The tenant ID.
id	The router ID.
availability_zone	The Availability Zone name

Notes

If a port on the network of the same tenant as the logical router is specified, an error will occur. (response code: 400)

If a logical router outside of the domain to which the user belongs is specified, an error will occur. (response code: 403)

If a port on a network outside of the domain to which the user belongs is specified, an error will occur. (response code: 404)

1.9.5.2 Remove interface from router (Delete connection interface)

Removes an internal interface from a logical router.

Specify a port on the network of a tenant that is different to the logical router within the same domain, and delete the connection interface.

URI

/v2.0/routers/{router_id}/remove_cross_project_router_interface

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
port_id	The port ID.	csapi:uuid	MUST

Example request

```
{
   "port_id": "1accb5ac-b258-483e-af3a-f41f6df8190c"
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes
conflict (409)	Error response codes

Response body (normal status)

```
{
    "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
    "tenant_id": " e10f4ade5a7649c49e1a6817196516ad",
    "port_id": "1accb5ac-b258-483e-af3a-f41f6df8190c",
    "subnet_id": "a2f1f29d-571b-4533-907f-5803ab96ead1",
    "availability_zone": "AZ1"
}
```

Description of response body (normal status)

Item	Description
id	The router ID.
tenant_id	The tenant ID.
port_id	The port ID.
subnet_id	The subnet ID.
availability_zone	The Availability Zone name

Notes

If a port on the network of the same tenant as the logical router is specified, an error will occur. (response code: 400)

If a logical router outside the domain to which the user belongs is specified, an error will occur. (response code: 403)

If a port on a network outside the domain to which the user belongs is specified, an error will occur. (response code: 404)

1.9.5.3 Update router (Update routing information)

Updates a logical router.

Updates the routing information between different tenants within the same domain.

URI

/v2.0/routers/{router_id}

Description of the URI:

{router_id} UUID The UUID of the router.

HTTP method

PUT

Request parameter

Key	Description	Type	Required/optional
routes	List of dictionary(static route definitions) in this format: `[ { "nexthop":"IPADDRESS", "destination":"CIDR" } ]` Static route definitions: next_hop is the IP address of the next hop.	xsd:list	MUST

Key	Description	Type	Required/optional
	destination is the destination CIDR.		

Example request

```
{
    "router": {
        "routes": [
            {
                "nextop":"10.54.249.65",
                "destination":"0.0.0.0/0"
            },
            {
                "nextop":"10.54.249.65",
                "destination":"10.54.249.128/26"
            }
        ]
    }
}
```

Response codes

Status code	Description
200	Normal response codes
badRequest (400)	Error response codes
unauthorized (401)	Error response codes
forbidden (403)	Error response codes
itemNotFound (404)	Error response codes

Response body (normal status)

```
{
    "router": {
        "status": "ACTIVE",
        "external_gateway_info": {
            "network_id": "8ca37218-28ff-41cb-9b10-039601ea7e6b"
        },
        "name": "another_router",
        "admin_state_up": true,
        "tenant_id": "6b96ff0cb17a4b859e1e575d221683d3",
        "id": "8604a0de-7f6b-409a-a47c-a1cc7bc77b2e",
        "routes": [
            {
                "nextop":"10.54.249.65",
                "destination":"0.0.0.0/0"
            },
            {
                "nextop":"10.54.249.65",
                "destination":"10.54.249.128/26"
            }
        ],
        "availability_zone": "AZ1"
    }
}
```

Description of response body (normal status)

Item	Description
router	A routers object.
status	The router status.
external_gateway_info	The network_id, for the external gateway.
name	The router name.
admin_state_up	The administrative state of the router, which is up (true) or down (false).
tenant_id	The tenant ID.
id	The router ID.
routes	List of dictionary(static route definitions) in this format: `[ { "nexthop":"IPADDRESS", "destination":"CIDR" } ]` Static route definitions: next_hop is the IP address of the next hop. destination is the destination CIDR.
availability_zone	The Availability Zone name

Notes

If a logical router outside the domain to which the user belongs is specified, an error will occur. (response code: 403)

FUJITSU Cloud Service K5 IaaS

API reference (Network) 1.8Revision

Published Date November 2016