

Search

Q

KB0013881 - Latest Version



Kumu Cloud Computing Service

Revised by Siang Sheng Jheng • a day ago • 55 Views • ☆☆☆☆☆

Kumu Cloud Computing Service

Service Overview

Kumu Cloud Computing Service is a private cloud platform hosted locally at the OIST campus. The service offers researchers, students and select IT sections tools for self-deploying virtual machines at their convenience. Being hosted on-campus, we can offer high speed network access to internal sensing equipment and HPC systems such as Deigo and Bucket. Infrastructure section offers additional deployment services on top of this platform to provide production-grade systems through automation.

The platform is built on OpenStack and offers a collection of services, such as distributed storage, software defined networking and virtualization solutions to enable central allocation of server resources through a self-service web portal (<https://dashboard.kumu.oist.jp>) or through an HTTP API access for systems orchestration.

Eligibility

Faculty	Researcher	Student	RUA	Executive	Admin	Alumni	External	Innovation
✓	✓	✓	✗	✗	✗	✗	✗	✗
Vendor								
✗								

Requesting Kumu Cloud Computing service

Link to service catalog or Create direct form here <Andrew>

Add or Remove Project

Apply for API/CLI Access


Request Additional Resources

User Manual

Login to dashboard

Activate user before login to the service.

1. Visit <https://dashboard.kumu.oist.jp/> from OIST network or via OIST VPN service, and click “Connect”



openstack®

Log in

Authenticate using

Security Assertion Markup Language ▼

If you are not sure which authentication method to use, contact your administrator.

Connect

2. Sign in with your OIST account and password



Sign in with your organizational account

Sign in

Please use your OIST username followed by @oist.jp for the username field.

Example: taro1234@oist.jp

Please note that this is **NOT** your email address.

Problems with your password? Click [here!](#)

If you have any other issues, please go to the [IT Service Portal](#), call Phone# 23525, or visit us in Lab 2 B661.

Please send an email to it-help@oist.jp if unable to access the [IT Service Portal](#).

© 2013 Microsoft

3. By default, user will login with OIST user name and under the project which same name as user. For testing environment, each user has default resources as below,

- Instances (virtual machines): 10
- VCPU (virtual CPU cores): 12

- RAM (total available memory): 25GB
- Floating IPs (IP address can be connected within OIST network): 10
- Volumes (disk volumes): 10
- Volume storage (total disk storage space can be used): 250GB
- Object Storage (containers): 1GB

Instances/Virtual machines

How to create instance (virtual machine)

Before launching a new instance/virtual machine, there are two necessary steps for accessing the instance via SSH.

a. Importing/creating SSH key.

Instances/Virtual machines can be accessed from user-end via SSH connection. User can create an SSH key pair via dashboard or import existed public key to KUMU platform.

Launch Instance ×

Details *

Source *

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair. ?

+ Create Key Pair

📁 Import Key Pair

Allocated

Displaying 1 item

Name	Fingerprint
> demo	b8:8e:41:b7:89:10:b9:d5:e2:aa:e5:6a:04:e1:fb:ab

Displaying 1 item

▼ Available 2 Select one

🔍

Click here for filters.

×

Displaying 2 items

Create Key pair

Click button "Create Keypair" to generate the keys, and private credential should start to download as a file on local server automatically.

Create Key Pair ×

Key Pair Name *

demo ✓

Key Pairs are how you login to your instance after it is launched. Choose a key pair name you will recognize. Names may only include alphanumeric characters, spaces, or dashes.

✕ Cancel

+ Create Key Pair

Import SSH key pair

User can also create SSH key pair on local server and upload to KUMU platform.

Import Public Key



Key Pair Name *

Load Public Key from a file

No file chosen

Public Key *

Content size: 0 bytes of 16.00 KB

Key Pairs are how you login to your instance after it is launched. Choose a key pair name you will recognize and paste your SSH public key into the space provided.

There are two ways to generate a key pair. From a Linux system, generate the key pair with the `ssh-keygen` command:

```
ssh-keygen -t rsa -f cloud.key
```

This command generates a pair of keys: a private key (cloud.key) and a public key (cloud.key.pub).

From a Windows system, you can use PuTTYGen to create private/public keys. Use the PuTTY Key Generator to create and save the keys, then copy the public key in the red highlighted box to your `.ssh/authorized_keys` file.

Now, the generated public key is ready to be imported to the instance.

b. Create security rules for SSH (port 22).

Click tab "Project" -> "Network" -> "Security groups", click button "Create Security groups".

Name the security group.

Create Security Group



Name *

Description

Description:

Security groups are sets of IP filter rules that are applied to network interfaces of a VM. After the security group is created, you can add rules to the security group.

Select the new security group and click button "Manage Rules".

Security Groups

Displaying 10 items			
		Filter <input type="text"/>	<input type="button" value="+ Create Security Group"/> <input type="button" value="Delete Security Groups"/>
<input type="checkbox"/>	Name	Security Group ID	Description
<input checked="" type="checkbox"/>	SSH	5aae38f2-d019-4361-9cea-8e06928ad577	
			Actions <input type="button" value="Manage Rules"/>

Click the button "Add rule", and select rule "SSH".

Add Rule



Rule *

SSH

Remote * ?

CIDR

CIDR ?

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel

Add

Now we have SSH key and security rule can be applied to the instance later while creating instances. We can start to launch instance as below,

1. Visit and login to <https://dashboard.kumu.oist.jp/>
2. Click tab "Project" -> "Compute" -> "Instances", click button "Launch Instance".

openstack kumu-test01@oist.jp

Project / Compute / Instances

Instances

Instance ID = Filter Launch Instance

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
No items to display.										

3. Name the instance
4. Select 'Image' as boot source for the instance. User can choose from pre-defined images, uploaded customized images, or snapshot from existed instance.

Details *

Source *

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source

Image

Create New Volume

Yes No

Volume Size (GB) *

1

Delete Volume on Instance Delete

Yes No

Allocated

Name	Updated	Size	Type	Visibility
Select an item from Available items below				

Available 5

Select one

Q

Click here for filters.

X

Name	Updated	Size	Type	Visibility	
> CentOS-7-GenericCloud-1907	2/26/20 3:34 PM	898.75 MB	qcow2	Public	↑
> CentOS-8-GenericCloud-1911	2/25/20 2:35 PM	683.00 MB	qcow2	Public	↑
> ubuntu-16-04-amd64-cloudimg	2/26/20 3:34 PM	444.04 MB	qcow2	Public	↑
> ubuntu-18.04-amd64-cloudimg	2/26/20 3:34 PM	329.06 MB	qcow2	Public	↑
> ubuntu-20.04-amd64-cloudimg	2/26/20 5:26 PM	524.81 MB	qcow2	Public	↑

5. Choose a flavor for the instance. Flavor is an available hardware configuration for an instance (virtual machine). It defines the specification of an instance that can be launched.

Details *

Source *

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Flavors manage the sizing for the compute, memory and storage capacity of the instance.

Allocated

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public
Select an item from Available items below						

Available 27

Select one

Q

Click here for filters.

X

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> n1-highmem-4-100	4	16 GB	100 GB	100 GB	0 GB	Yes	↑
> n1-standard-8-40	8	16 GB	40 GB	40 GB	0 GB	Yes	↑
> n1-standard-4-40	4	8 GB	40 GB	40 GB	0 GB	Yes	↑
> n1-standard-1-40	1	2 GB	40 GB	40 GB	0 GB	Yes	↑
> n1-highmem-2-20	2	8 GB	20 GB	20 GB	0 GB	Yes	↑
> n1-standard-4-20	4	8 GB	20 GB	20 GB	0 GB	Yes	↑
> n1-highcpu-2-100	2	2 GB	100 GB	100 GB	0 GB	Yes	↑
> n1-highmem-2-100	2	8 GB	100 GB	100 GB	0 GB	Yes	↑

6. Choose network. By default, “Default_Network” will be assigned to the instance with a private IP address which have access to Internet and OIST network but cannot be accessed from OIST network. Detail will be described in “Network” section.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Networks provide the communication channels for instances in the cloud.

▼ Allocated 1

Select networks from those listed below.

Network	Subnets Associated	Shared	Admin State	Status
1 > Default_Network	default-subnet	Yes	Up	Active

▼ Available 0

Select at least one network

Click here for filters.

Network	Subnets Associated	Shared	Admin State	Status
No available items				

Cancel

< Back

Next >

Launch Instance

7. (Optional) Add additional security groups if needed. Security groups are sets of IP filter rules that are applied to assigned instances, which define networking access to the instance. User can create their own security groups and apply to the instance under test environment. Detail steps will be described in “Network” section.

Launch Instance

Details

Source

Flavor

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Select the security groups to launch the instance in.

▼ Allocated 1

Name	Description
> default	Default security group

▼ Available 2

Select one or more

Click here for filters.

Name	Description																		
▼ ICMP																			
	<table> <tr> <th>Direction</th> <th>Ether Type</th> <th>Protocol</th> <th>Min Port</th> <th>Max Port</th> <th>Remote</th> </tr> <tr> <td>egress</td> <td>IPv6</td> <td>-</td> <td>-</td> <td>-</td> <td>::/0</td> </tr> <tr> <td>egress</td> <td>IPv4</td> <td>-</td> <td>-</td> <td>-</td> <td>0.0.0.0/0</td> </tr> </table>	Direction	Ether Type	Protocol	Min Port	Max Port	Remote	egress	IPv6	-	-	-	::/0	egress	IPv4	-	-	-	0.0.0.0/0
Direction	Ether Type	Protocol	Min Port	Max Port	Remote														
egress	IPv6	-	-	-	::/0														
egress	IPv4	-	-	-	0.0.0.0/0														
> iperf																			

Cancel

< Back

Next >

Launch Instance

8. Insert SSH key to the instance. Instances can be access from user-end via SSH connection. User can create an SSH key pair via dashboard or import existed public key.

Launch Instance

Details *
Source *
Flavor *
Networks
Network Ports
Security Groups
Key Pair
Configuration
Server Groups

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

+ Create Key Pair

Import Key Pair

Allocated

Displaying 1 item

Name	Fingerprint
> demo	b8:8e:41:b7:89:10:b9:d5:e2:aa:e5:6a:04:e1:fb:ab

Displaying 1 item

Available 2

Select one

Click here for filters.

Displaying 2 items

Create Key pair

Click button "Create Keypair" to generate the keys, and private credential should start to download as a file on local server automatically.

Create Key Pair

Key Pair Name *

demo

Key Pairs are how you login to your instance after it is launched. Choose a key pair name you will recognize. Names may only include alphanumeric characters, spaces, or dashes.

Cancel

Create Key Pair

Now, the generated public key can be imported to the instance

Launch Instance

Details *
Source *
Flavor *
Networks
Network Ports
Security Groups
Key Pair
Configuration
Server Groups
Scheduler Hints
Metadata

A key pair allows you to SSH into your newly created instance. You may select an existing key pair, import a key pair, or generate a new key pair.

+ Create Key Pair

Import Key Pair

Allocated

Displaying 0 items

Select a key pair from the available key pairs below.

Displaying 0 items

Available 3

Select one

Click here for filters.

Displaying 3 items

Name	Fingerprint
> demo	03:7c:26:a5:46:5e:65:b9:ab:af:96:8f:17:50:fa:ea

Public Key

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDdu30y4U9FJLSBBVJ6g+rOWtAQdK10IUYA0xMRsyh+2UGcmJa+QU130EzC/7qkwLG5H65ZIBut4zuJ18qbqk21iFu7TIEdvf8cXY1mLHm/H8Yz2ciUwBxpb1cfSaw317nHbP69UGRQGI3IcPGdoN40IObQ8/csnwJMaUzd0cNgRgKdg+f/t4mkhtM93YbejodfJCmoZ+3/IYcOTTUHoqDt/YzNAGRXS1WdeOVvzhK62erNbYGYMzHGE8s/aqtBXsfQsxkC+0Xqyb6MzSn8H2x/rKI0hq0rHqL73Q8C0adSTBkD0pZwD+1Jcj/biV50Jq1iVis8X8/vjLIr0mDe5Ng2T Generated-by-Nova

9. Associate floating IP to the instance if needed. Instance (virtual machine) can be accessed directly via floating IP from OIST network.

The screenshot shows the 'Instances' page in the OpenStack dashboard. On the left is a sidebar with navigation links: Project, API Access, Compute, Overview, Instances (selected), Images, Key Pairs, Volumes, Network, Orchestration, Object Store, and Identity. The main area displays a table of instances. One instance named 'demo' is shown with IP address 192.168.81.21 and flavor n1-highcpu-2-20. A red arrow points to the 'Actions' column for this instance, where a dropdown menu is open. The menu includes options like 'Associate Floating IP', 'Attach Interface', 'Detach Interface', 'Edit Instance', 'Attach Volume', 'Detach Volume', 'Update Metadata', 'Edit Security Groups', 'Console', 'View Log', 'Pause Instance', 'Suspend Instance', 'Shelve Instance', 'Resize Instance', 'Lock Instance', and 'Soft Reboot Instance'.

Allocate floating IP, click 'plus' icon to allocate floating IP from IP pool.

Manage Floating IP Associations

IP Address *

Select an IP address ▼ +

Port to be associated *

demo: 192.168.81.21 ▼

Select the IP address you wish to associate with the selected instance or port.

Cancel Associate

Add description

Allocate Floating IP

Pool *

Default_FIP_Pool ▼

Description

Description: Allocate a floating IP from a given floating IP pool.

Project Quotas

Floating IP 0 of 10 Used

Cancel Allocate IP

Associate with instance.

Manage Floating IP Associations



IP Address *

10.155.8.23



Select the IP address you wish to associate with the selected instance or port.

Port to be associated *

demo: 192.168.81.21



Cancel

Associate

The instance will be associated with the floating IP address. User can access the instance via floating IP within OIST network.

Instances

Instance ID = Filter Launch Instance Delete Instances More Actions ▾

Displaying 1 item

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/>	demo	-	192.168.81.21 Floating IPs: 10.155.8.23	n1-highcpu-2-20	-	Active	nova	None	Running	15 minutes	Create Snapshot ▾

Displaying 1 item

10. Access the instance via SSH. The instance can be accessed via SSH if the instance had been associated with floating IP and the public key had been imported to the instance.

Default user names for different cloud images,

- CentOS cloud image, the default user name is "centos". You can access the instance via command "ssh centos@ <FLOATING_IP>" from your workstation within OIST network.
- Ubuntu cloud image, the default user name is "ubuntu". You can access the instance via command "ssh ubuntu@ <FLOATING_IP>" from your workstation within OIST network.

11. Access the instance via console.

There is no default user's password for the cloud images. User have to set the password before login via console directly. Login to instance via console first and then set the password via command, "sudo passwd <username>", e.g. "sudo passwd centos". Input the new password twice, and then you can login to the instance with the new password as below steps.

Click tab "Project" -> "Compute" -> "Instances", and then click the instance.

Project

API Access

Compute

Overview

Instances

Images

Key Pairs

Volumes

Network

Orchestration

Object Store

Identity

Project / Compute / Instances / demo

demo

Overview

Log

Console

Action Log

Name

Description

ID

Status

Locked

Availability Zone

Created

Time Since Created

demo

-

dd7448b3-6490-4238-8cc9-266bdfdea1d4

Active

False

nova

March 2, 2020, 10:48 a.m.

17 minutes

Specs

Flavor Name

Flavor ID

RAM

VCPUs

Disk

n1-highcpu-2-20

9d1a48fd-3bf8-4c6d-bb5c-e2e4739a0652

2GB

2 VCPU

20GB

IP Addresses

Default_Network

192.168.81.21, 10.155.8.23

Security Groups

ICMP

ALLOW IPv6 to ::/0
ALLOW IPv4 to 0.0.0.0/0

Click “console”. The instance can be accessed via VNC console.

Overview

Instances

Images

Key Pairs

Volumes

Network

Orchestration

Object Store

Identity

Overview

Log

Console

Action Log

Instance Console

If console is not responding to keyboard input, click the grey status bar below: [Click here to show only console](#)
To exit the fullscreen mode, click the browser's back button.

Connected (encrypted) to: DEMU (instance-000312e)

CentOS Linux 8 (Core)

Kernel 4.18.0-147.3.1.el8_1.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

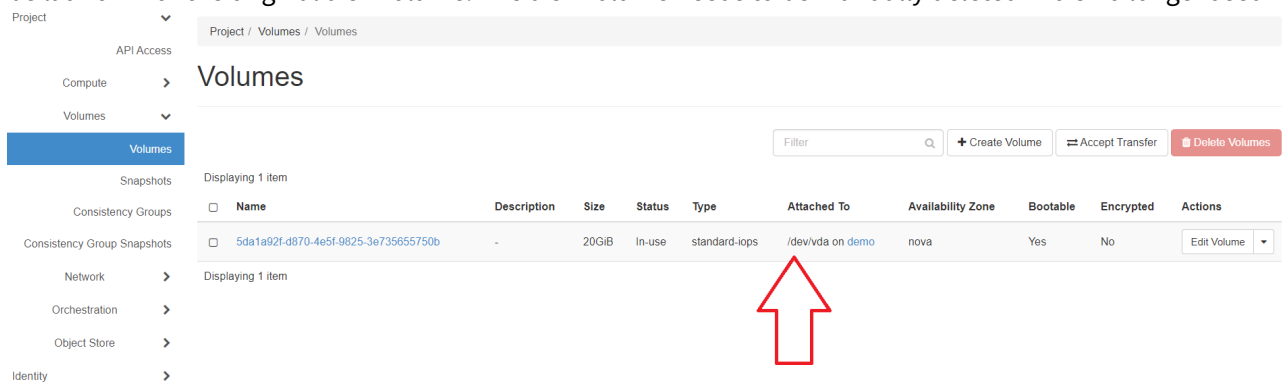
demo login:

Volumes

Manage volumes and snapshot

Once the instance has been created, it will also allocate a disk volume attached to the instance. Deleting the

instance will not delete the disk volume by design. When the old instance has been deleted, new instance can be launch with the original disk volume. The disk volume needs to be manually deleted if it is no longer used



The screenshot shows the OpenStack Volumes dashboard. On the left is a sidebar with navigation links: Project, API Access, Compute, Volumes (selected), Snapshots, Consistency Groups, Consistency Group Snapshots, Network, Orchestration, Object Store, and Identity. The main header shows the breadcrumb 'Project / Volumes / Volumes' and the title 'Volumes'. Below the header, there's a filter input, '+ Create Volume', 'Accept Transfer', and 'Delete Volumes' buttons. A table displays one volume with the following details:

Name	Description	Size	Status	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
5da1a92f-d870-4e5f-9825-3e735655750b	-	20GiB	In-use	standard-ops	/dev/vda on demo	nova	Yes	No	Edit Volume

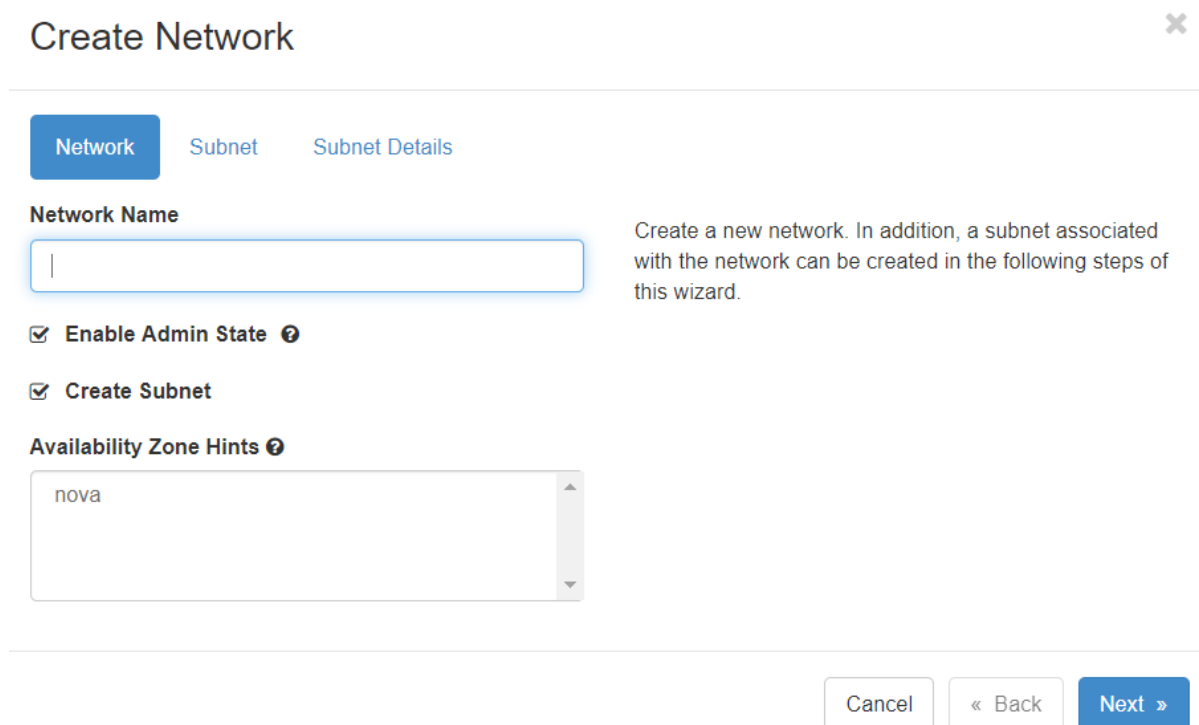
A red arrow points to the 'Attached To' column, specifically to the 'demo' instance name.

Network

Kumu cloud computing service provide "Test Network" by default for test environment which can access Internet and attached with floating IP address. User can also create private network within the project. The private network can only be used and accessed via instances within the project.

Create network

1. Click tab "Project" -> "Network" -> "Networks". Click button "+Create Network".
2. Name the network



The screenshot shows the 'Create Network' wizard. At the top, there's a title 'Create Network' and a close button. Below the title are three tabs: 'Network' (selected), 'Subnet', and 'Subnet Details'. The 'Network Name' field is empty. To the right of this field is a text box that says: 'Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.'

Below the network name field are two checked checkboxes:

- ☒ Enable Admin State ?
- ☒ Create Subnet

Below these checkboxes is a section titled 'Availability Zone Hints ?' with a dropdown menu showing 'nova'.

At the bottom right of the form are three buttons: 'Cancel', '« Back', and 'Next »'.

3. Create subnet for the network

Name the subnet

Define network address range in CIDR format. Ex.192.168.10.0/24.

Create Network



Network

Subnet

Subnet Details

Subnet Name

demo-subnet

Network Address

192.168.0.0/24

IP Version

IPv4

Gateway IP

☐ Disable Gateway

Creates a subnet associated with the network. You need to enter a valid "Network Address" and "Gateway IP". If you did not enter the "Gateway IP", the first value of a network will be assigned by default. If you do not want gateway please check the "Disable Gateway" checkbox. Advanced configuration is available by clicking on the "Subnet Details" tab.

Cancel

« Back


Next »

Security groups

Security groups are sets of IP filter rules that are applied to assigned instances, which define networking access to the instance. User can create customized security rules and assign to instance.

Project / Network / Security Groups

Security Groups

Filter  [+ Create Security Group](#) [Delete Security Groups](#)

Displaying 3 items

<input type="checkbox"/>	Name	Security Group ID	Description	Actions
<input type="checkbox"/>	ICMP	02ae1121-ce6f-4721-aa5f-ea1ca9aad28		Manage Rules
<input type="checkbox"/>	default	4a568b06-5ecd-482c-89f5-2de8269c4921	Default security group	Manage Rules
<input type="checkbox"/>	iperf	f00e0bac-8fc1-411d-80a4-daeeb277b02f		Manage Rules

Displaying 3 items

1. Click tab "Project" -> "Network" -> "Security Groups". Click button "Create Security Groups" and name it.
2. Click "Manage Rules" -> "Add Rules".

3. Choose pre-defined rules or custom rule based on need and fill port which related to the rule.

Add Rule ✕

Rule *

SSH

Remote * ?

CIDR

CIDR ?

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel

Add

Floating IPs

Each instance in KUMU cloud computing platform has a private, fixed IP address and can also have a floating IP address. Private IP addresses are used for communication between instances, and floating IP addresses are used for communication with networks outside the platform. Floating IPs can be allocated and associated to the instance while creating the instance. The floating IP address has been assigned to an instance will still be reserved even after the instance has been deleted. It needs to be manually released if the floating IP address is no longer used.

Object Store


In OpenStack Object Storage, containers provide storage for objects in a manner just like a Windows folder or Linux file directory, though they cannot be nested. An object in OpenStack consists of the file to be stored in the container and any accompanying metadata. By default, user can upload maximum 1GB files to the container in total.


Create container


1. Click tab "Project" -> "Object Store" -> "Containers"
2. Click "+container"
3. Name the container, the naming rule restrict the name of the container need to be longer than 3 character.


Copy Permalink


Attachments


- Attachments
-  Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png


 Pasted image.png






















 Pasted image.png

 Pasted image.png

 Pasted image.png

 Pasted image.png

 Pasted image.png

-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  Pasted image.png
-  imagee.png
-  Pasted image.png
-  imagef.png

Most Viewed

AnyConnect VPN

System Administrator • 1245 Views • 5d ago • ★★★★★

Working from Home for Staff and Temporary Staff During the COVID-19 Pandemic

Tim Dyce • 744 Views • 2d ago • ★★★★★

Working Off-Campus (Remote Work)

Tim Dyce • 737 Views • 2d ago • ★★★★★

Connecting to the software server

Alex Lafountain • 380 Views • 2mo ago • ★★★★★

Recommendations and Feedback on Remote Work

Tim Dyce • 316 Views • 2d ago • ★★★★★

Most Useful

Connecting to the software server

Alex Lafountain • 380 Views • 2mo ago • ★★★★★

AnyConnect VPN

System Administrator • 1245 Views • 5d ago • ★★★★★

Adobe Creative Cloud

Ryoko Abe • 83 Views • 3mo ago • ★★★★★