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

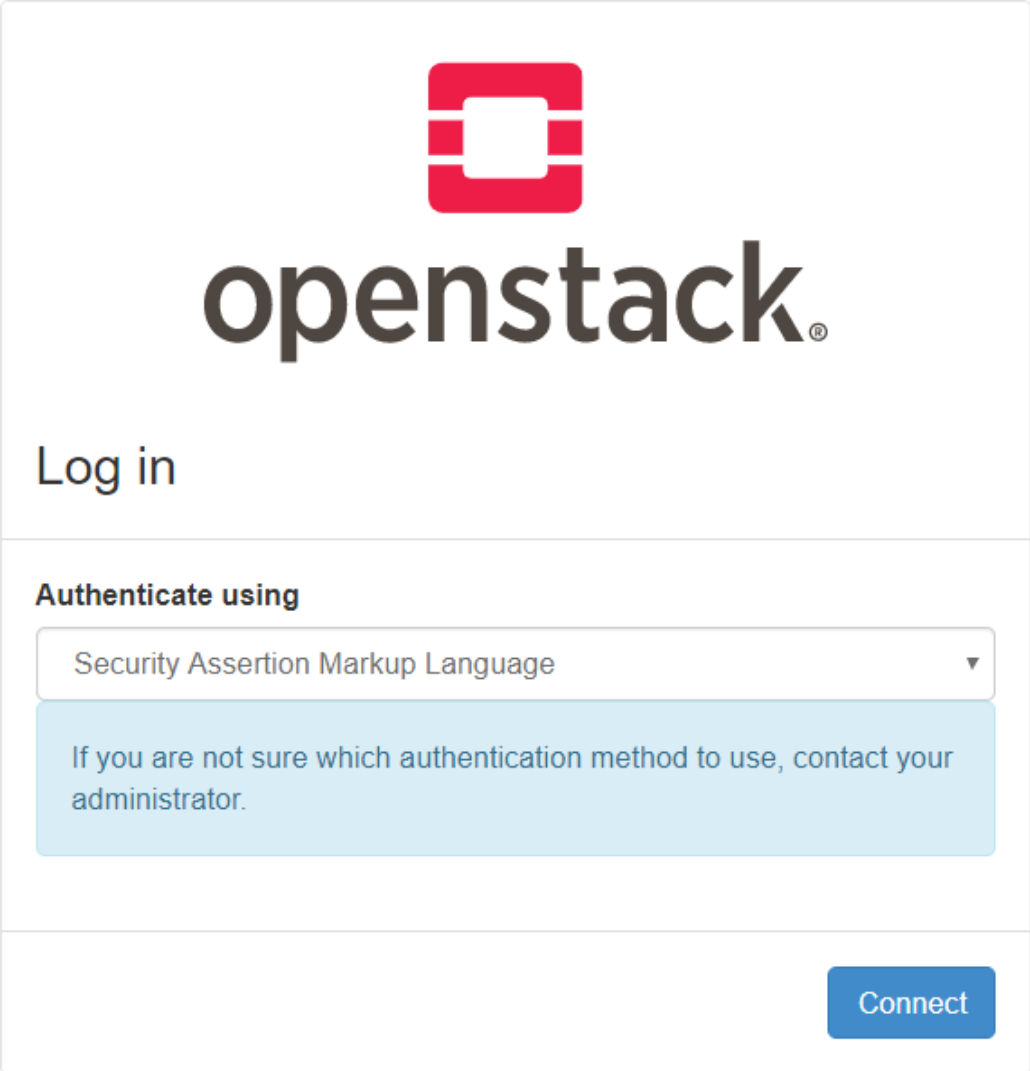
Request Additional Resources

User Manual

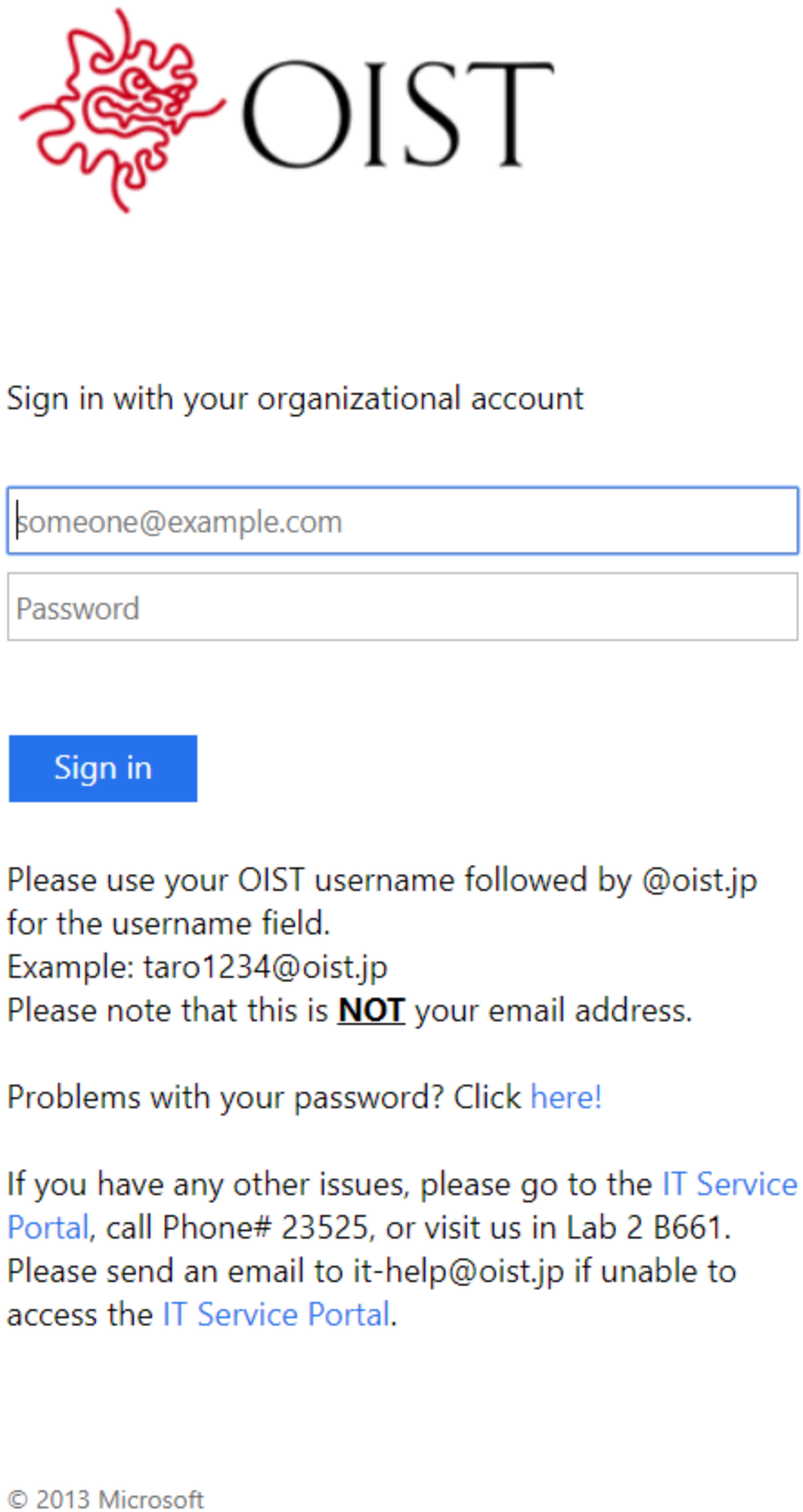
Login to dashboard

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”



2. Sign in with your OIST account and password



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

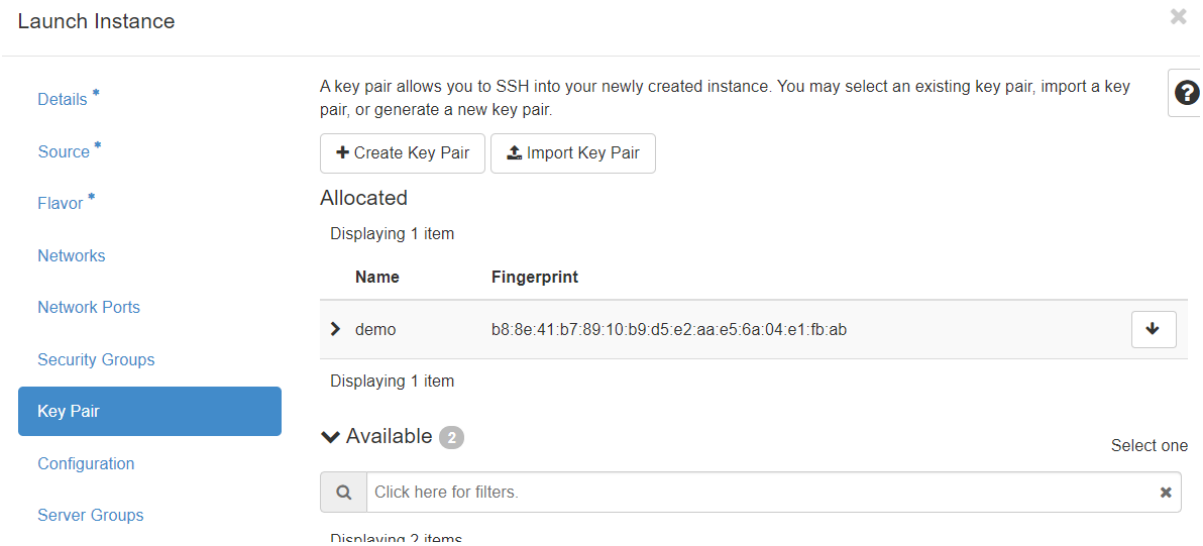
Instances/Virtual machines

How to create instance (virtual machine)

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

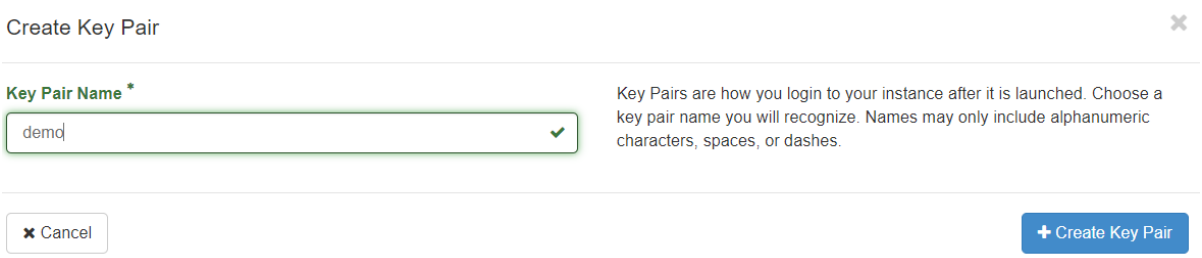
a. Importing/creating SSH key.

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.



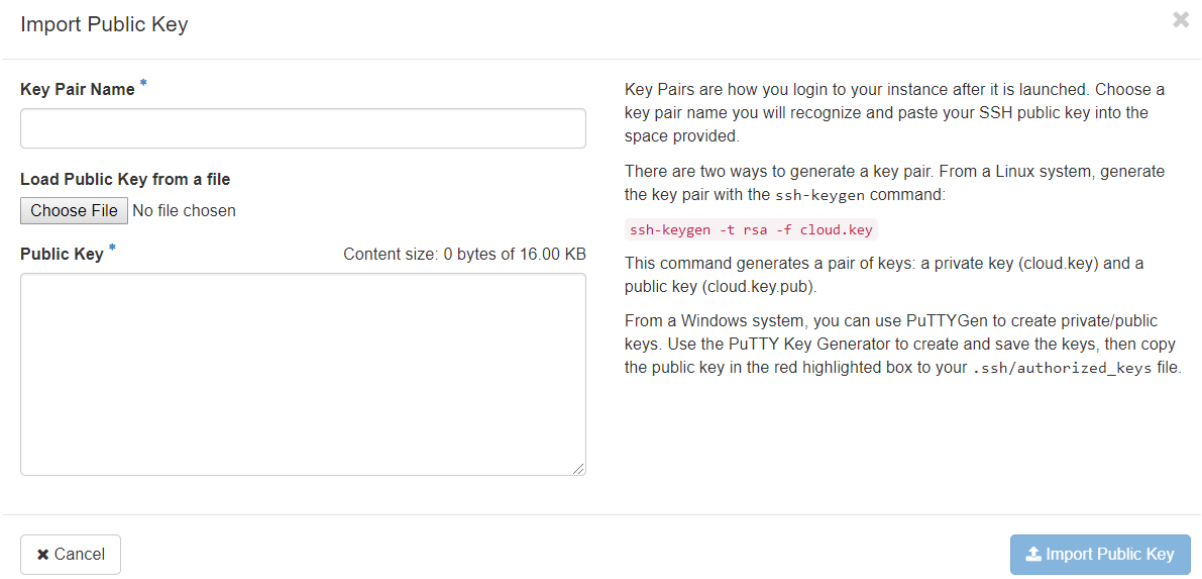
Create Key pair

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



Import SSH key pair

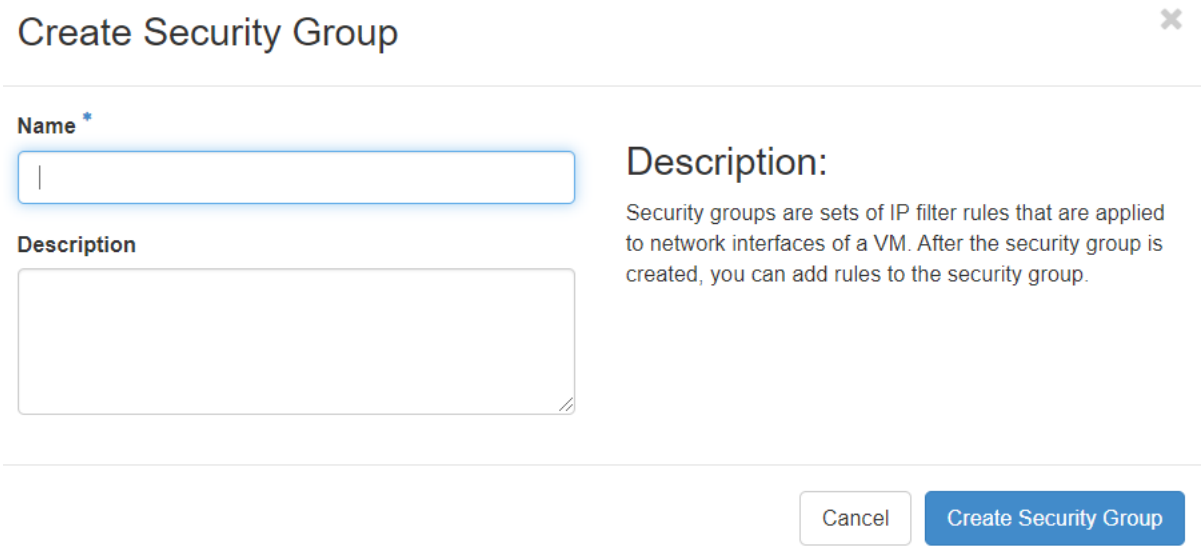
User can also create SSH key pair on local server and upload to KUMU platform.



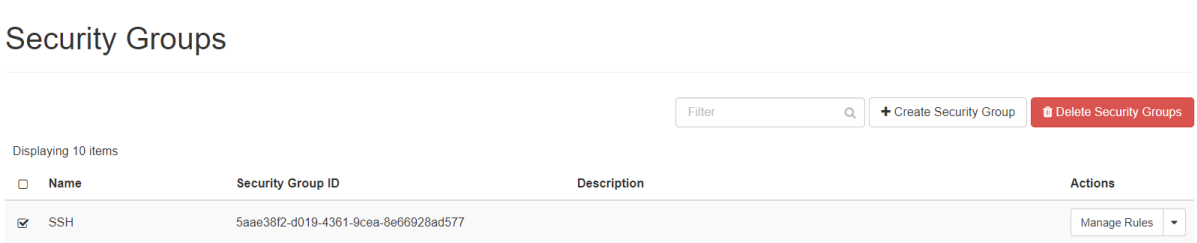
Now, the generated public key is ready to be imported to the instance.

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

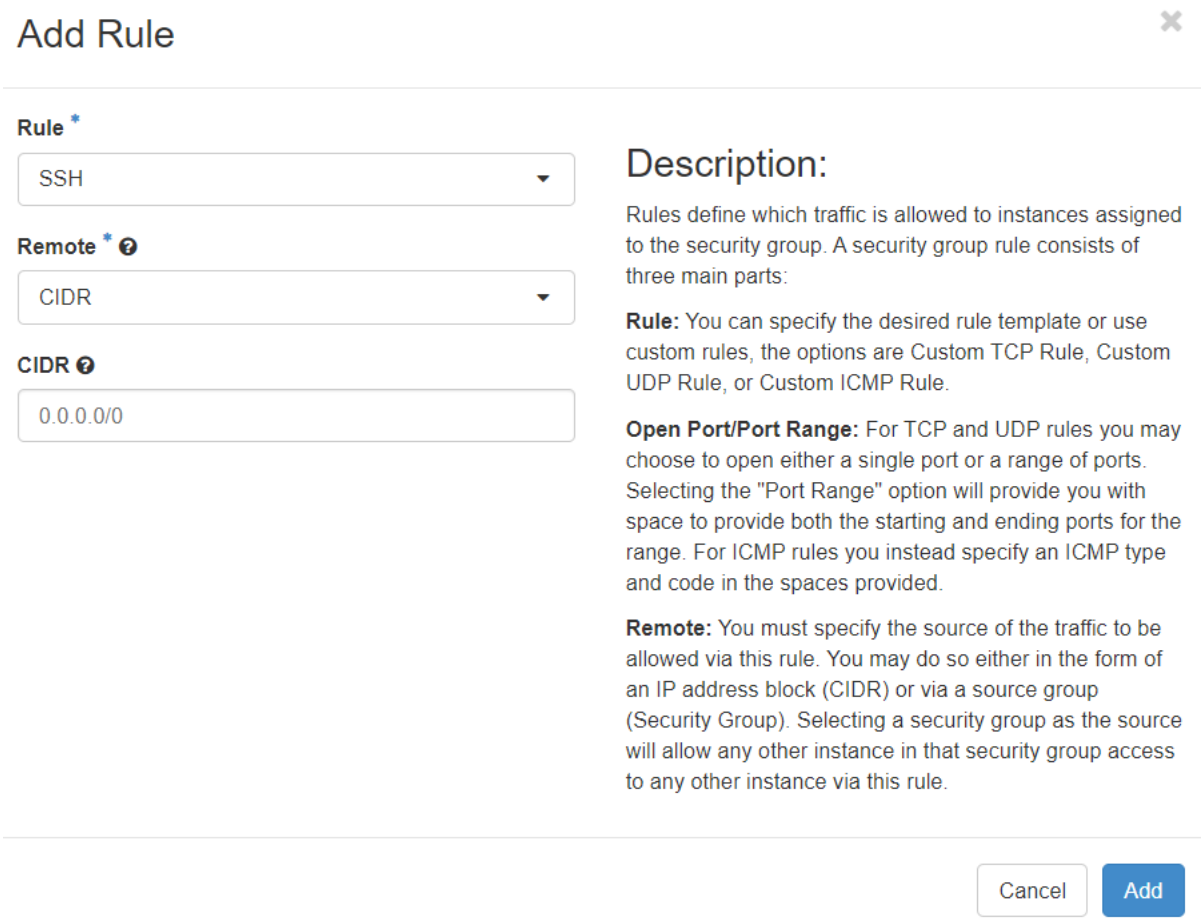
Click tab “Project” -> “Network” -> “Security groups”, click button “Create Security groups”.
Name the security group.



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

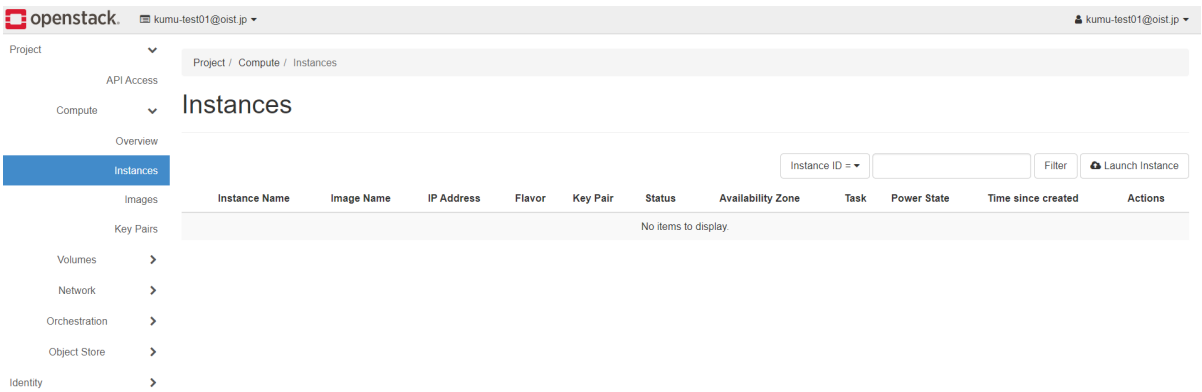


Click the button " Add rule", and select rule "SSH".

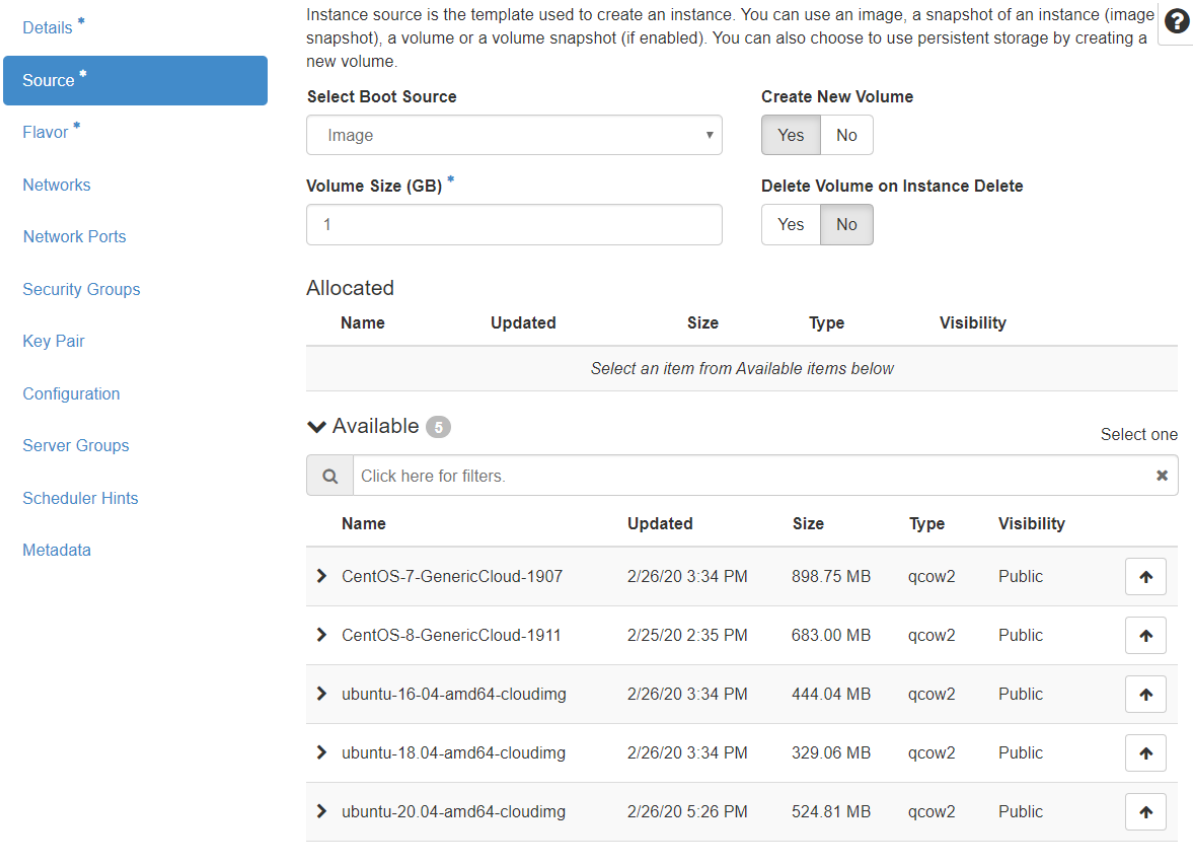


Now we have SSH key and security rule can be applied to the instance later while creating instances. We can start to launch instance as below,

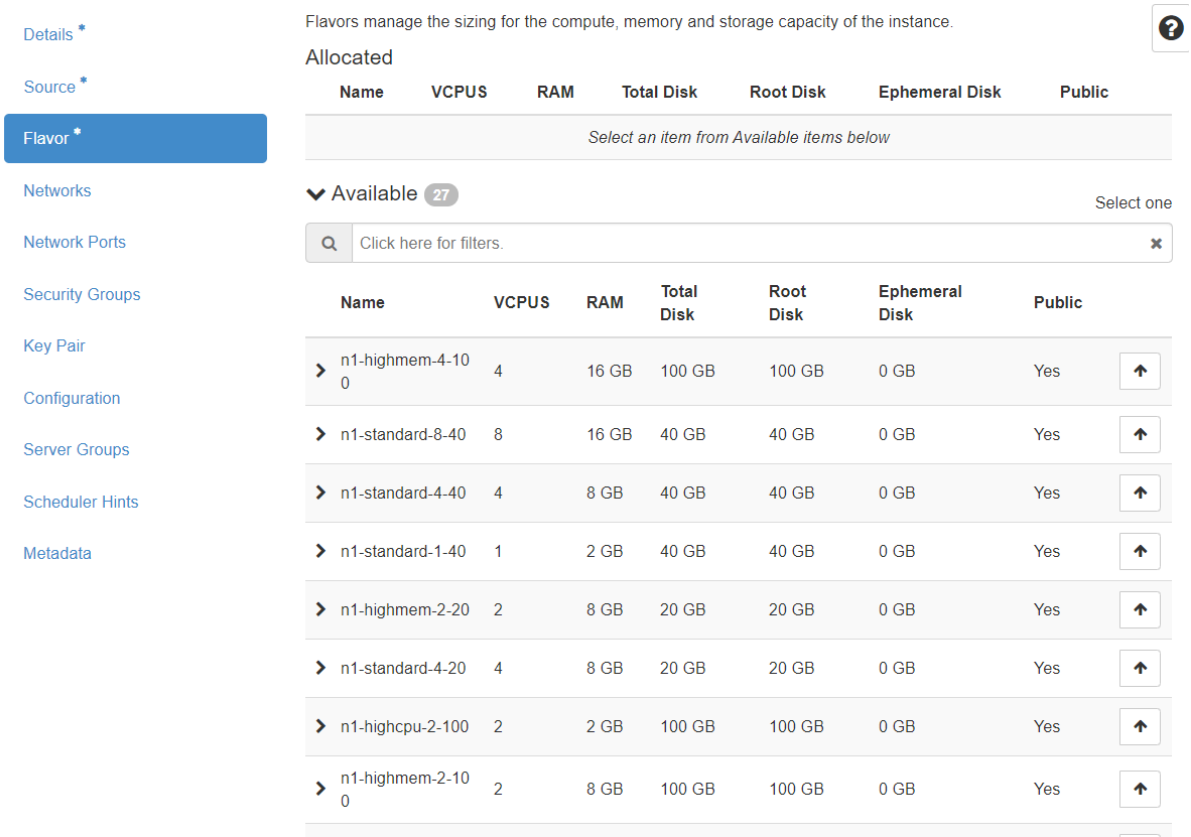
1. Visit and login to https://dashboard.kumu.oist.jp/
2. Click tab “Project” -> “Compute” -> “Instances”, click button “Launch Instance” .



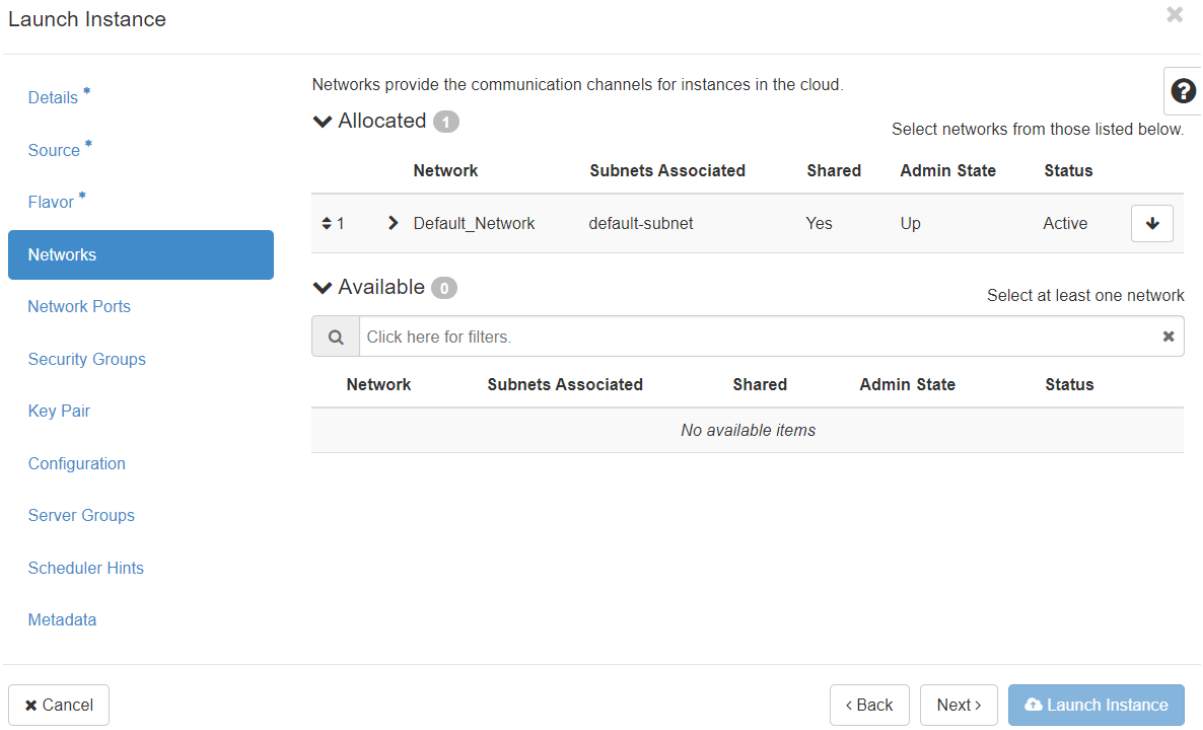
3. Name the instance
4. Select 'Image' as boot source for the instance. User can choose from pre-defined images, uploaded customized images, or snapshot from existed instance.



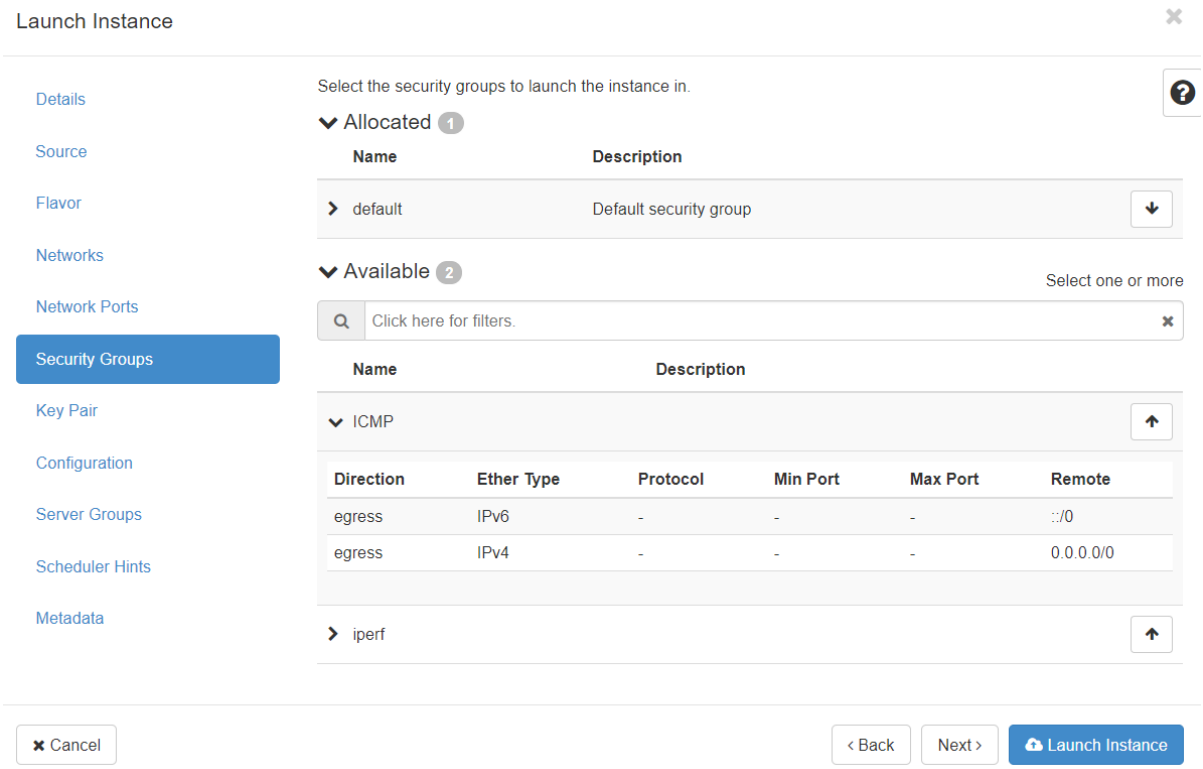
5. Choose a flavor for the instance. Flavor is an available hardware configuration for an instance (virtual machine). It defines the specification of an instance that can be launched.



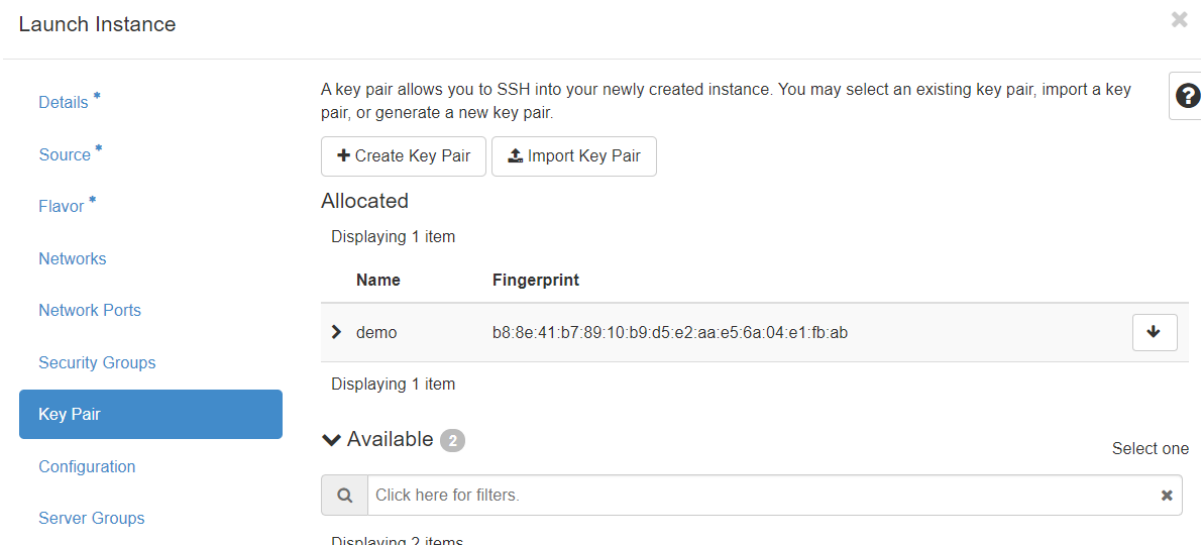
6. Choose network. By default, “Default_Network” will be assigned to the instance with a private IP address which have access to Internet and OIST network but cannot be accessed from OIST network. Detail will be described in “Network” section.



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.

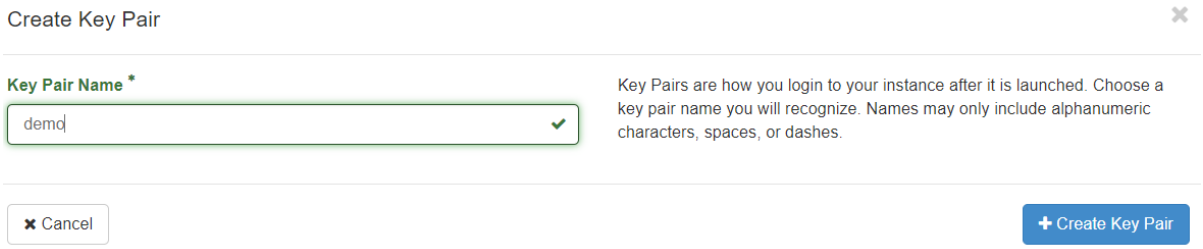


8. Insert SSH key to the instance. Instances can be access from user-end via SSH connection. User can create an SSH key pair via dashboard or import existed public key.

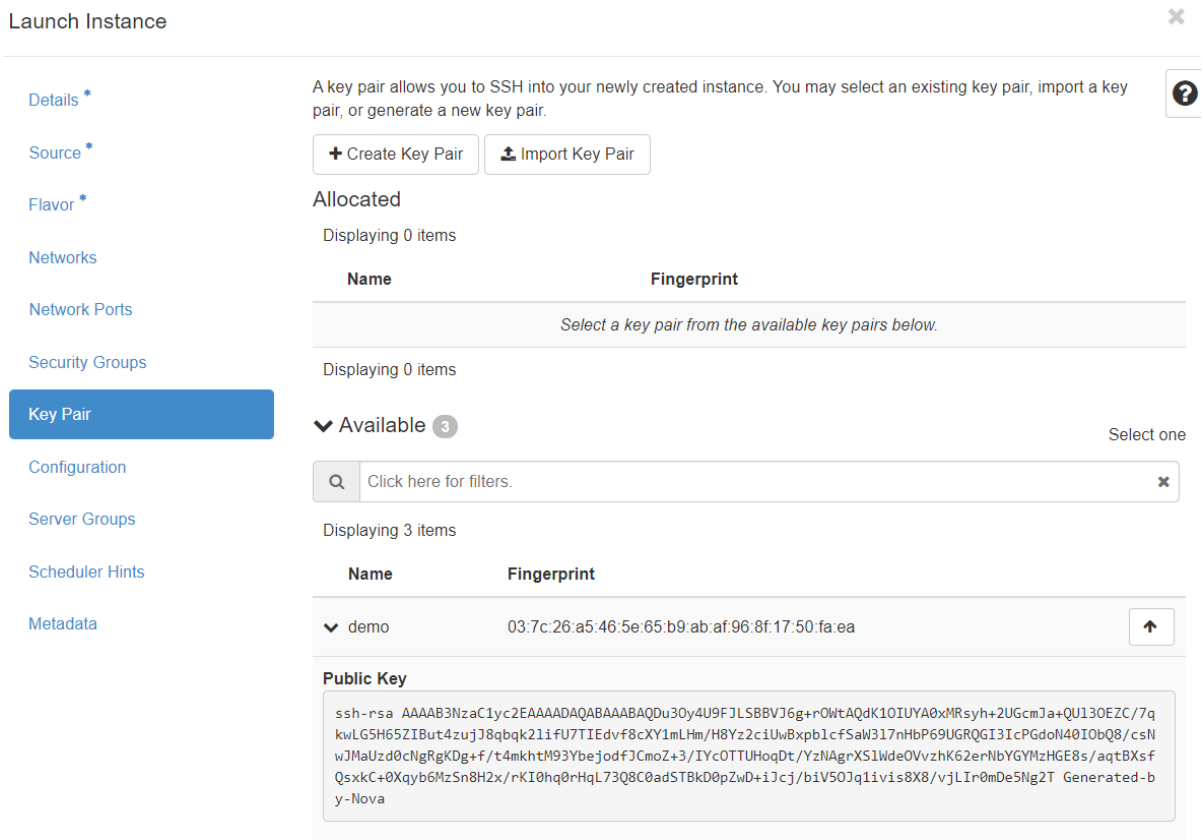


Create Key pair

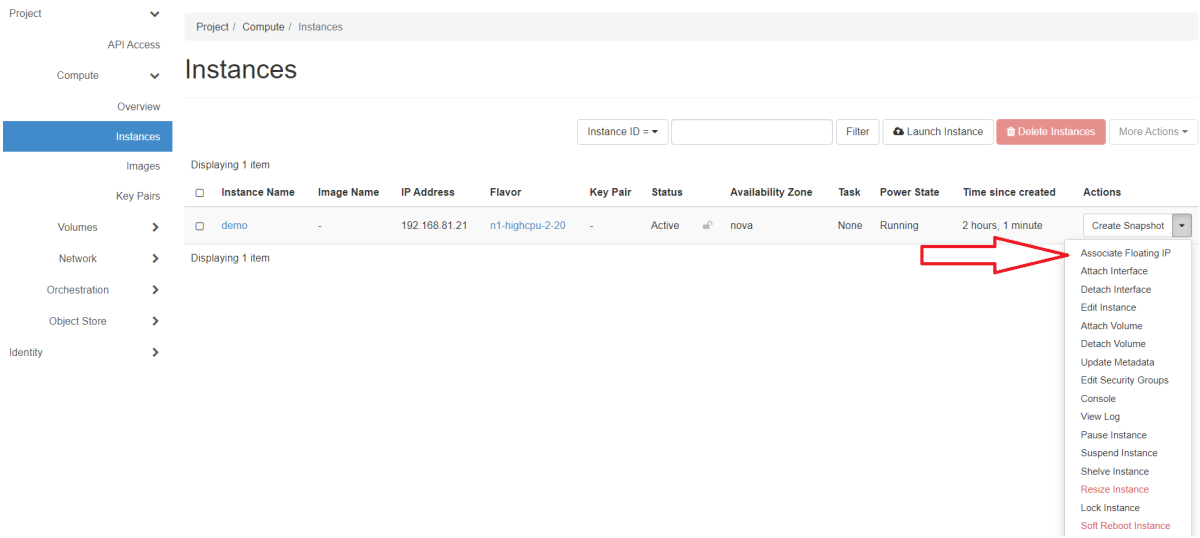
Click button "Create Keypair" to generate the keys, and private credential should start to download as a file on local server automatically.



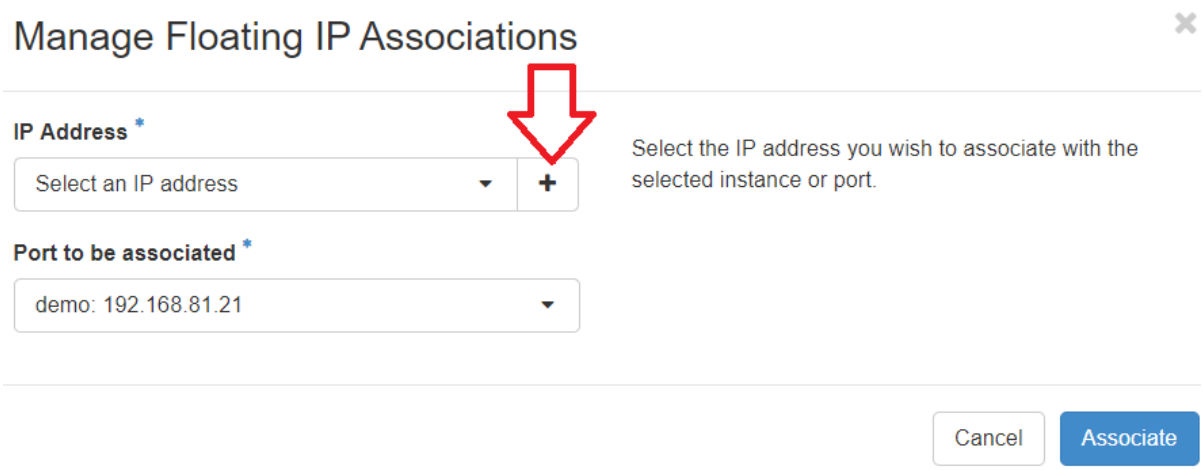
Now, the generated public key can be imported to the instance



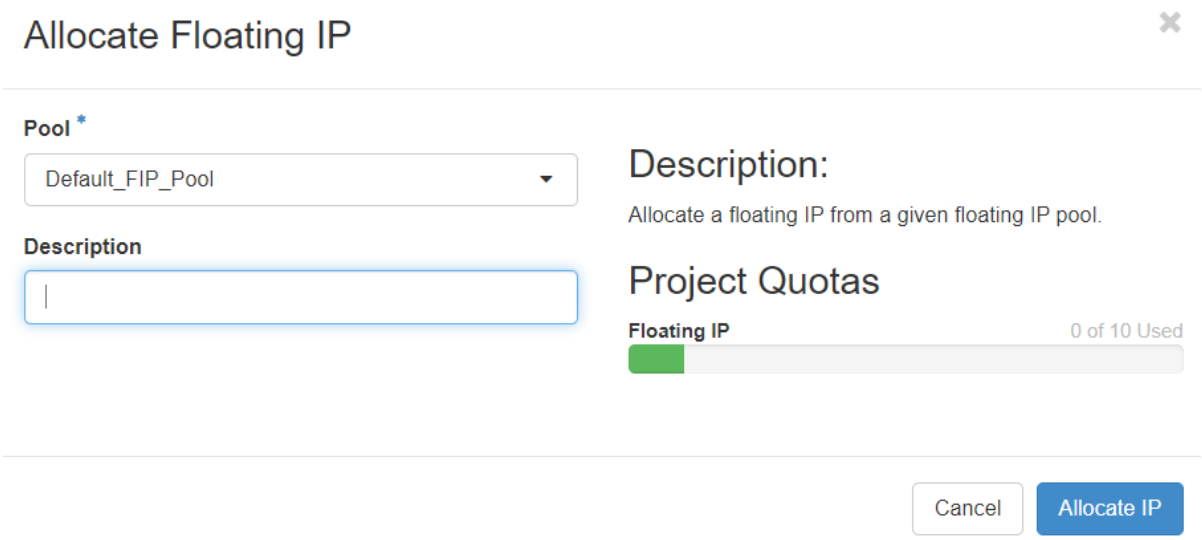
9. Associate floating IP to the instance if needed. Instance (virtual machine) can be accessed directly via floating IP from OIST network.



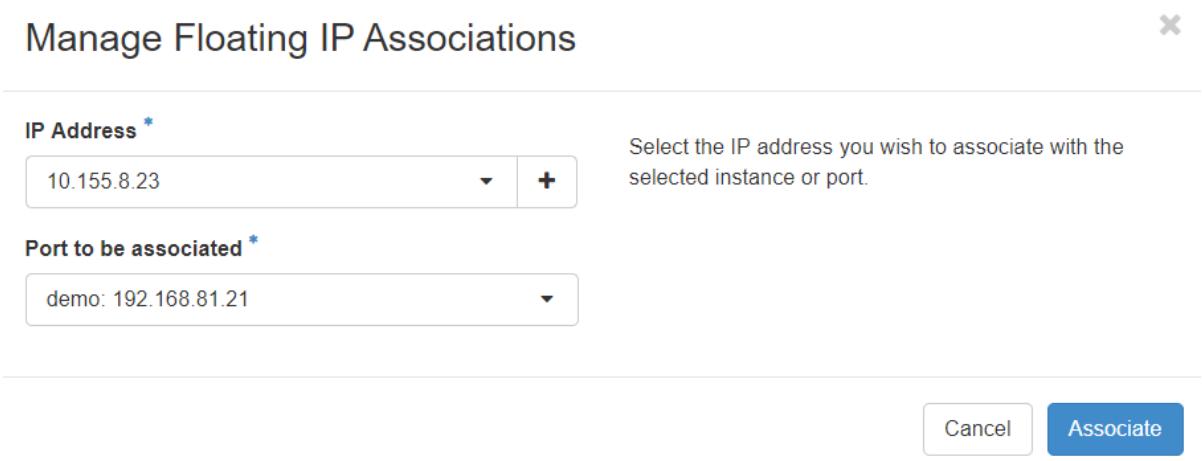
Allocate floating IP, click 'plus' icon to allocate floating IP from IP pool.



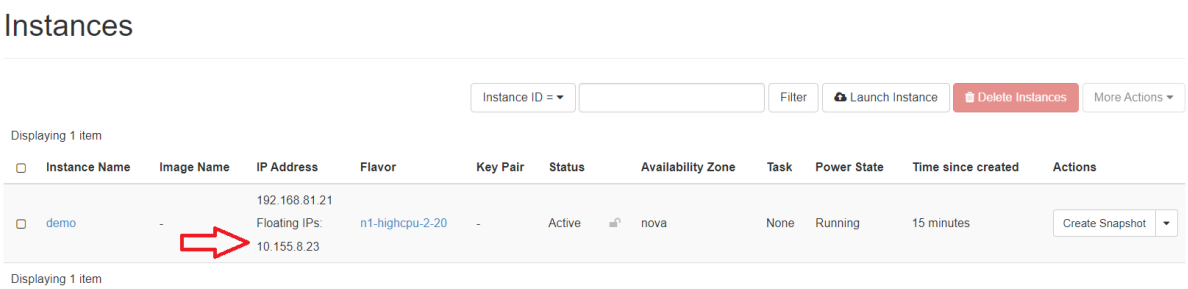
Add description



Associate with instance.



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



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	demo
Description	-
ID	dd7448b3-6490-4238-8cc9-266bdfdea1d4
Status	Active
Locked	False
Availability Zone	nova
Created	March 2, 2020, 10:48 a.m.
Time Since Created	17 minutes

Specs

Flavor Name	n1-highcpu-2-20
Flavor ID	9d1a48fd-3bf8-4c6d-bb5c-e2e4739a0652
RAM	2GB
VCPUs	2 VCPU
Disk	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: QEMU (instance-0000312e) | Send CtrlAltDel

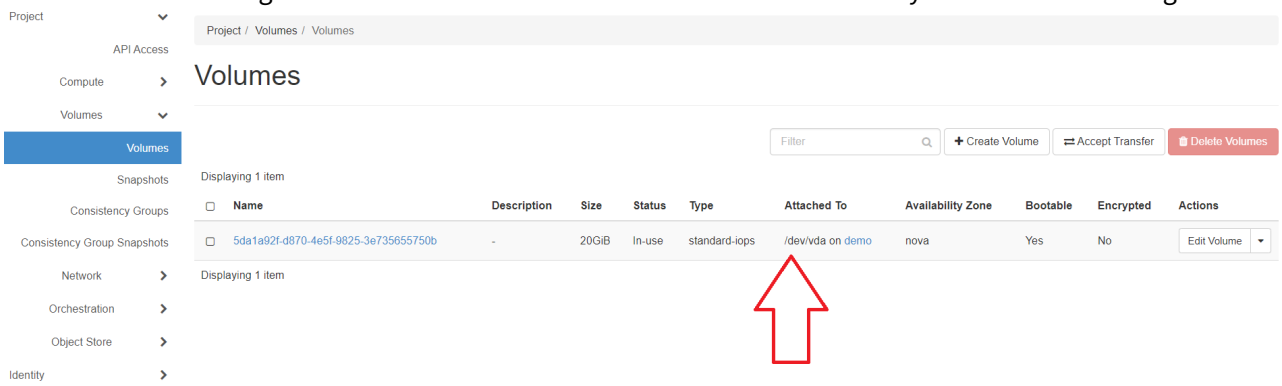
```
CentOS Linux 8 (Core)
Kernel 4.18.0-147.3.1.el8_1.x86_64 on an x86_64

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

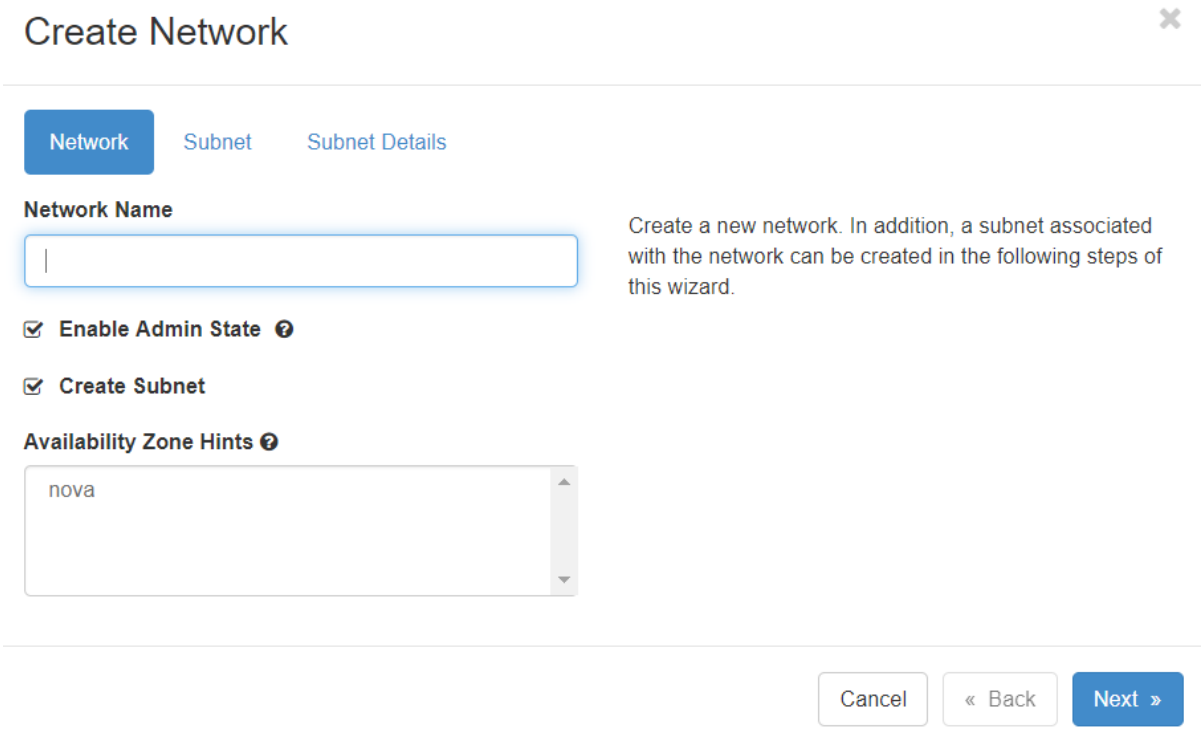


Network

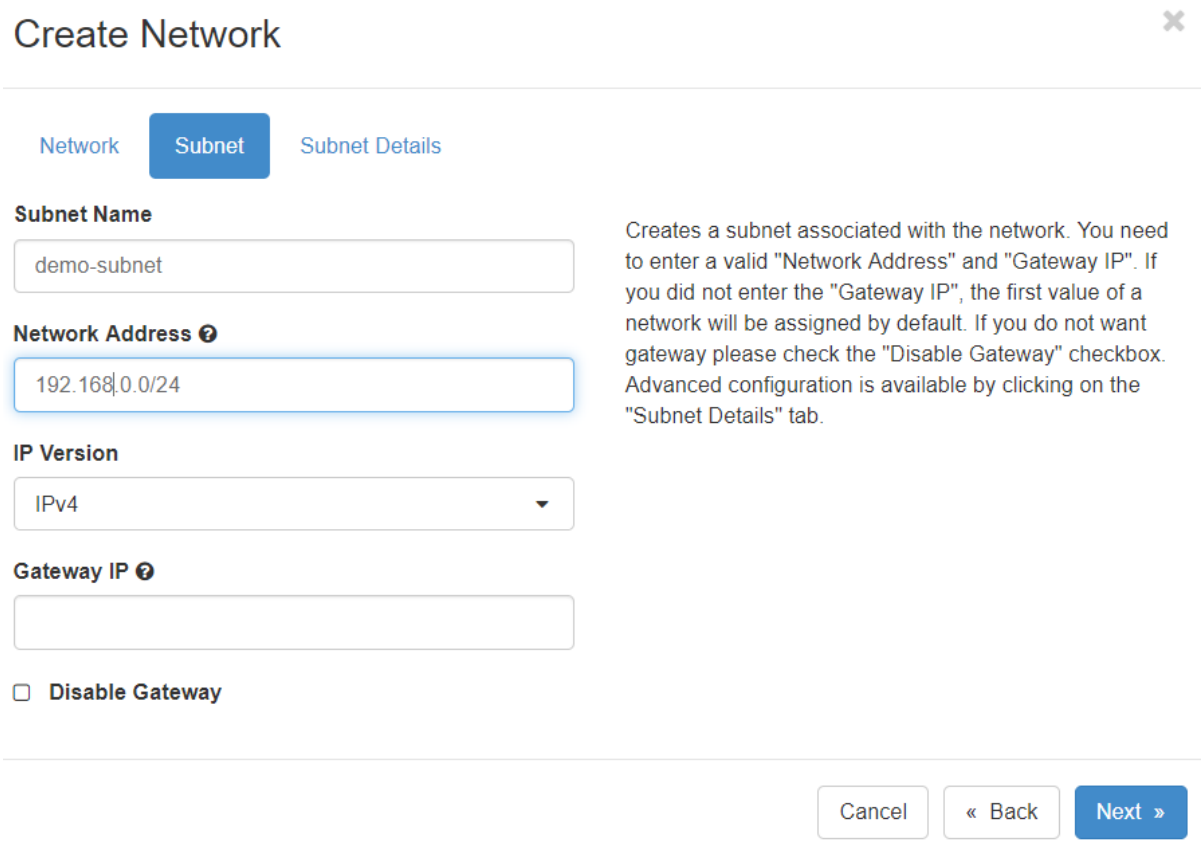
Kumu cloud computing service provide "Test Network" by default for test environment which can access Internet and attached with floating IP address. User can also create private network within the project. The private network can only be used and accessed via instances within the project.

Create network

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

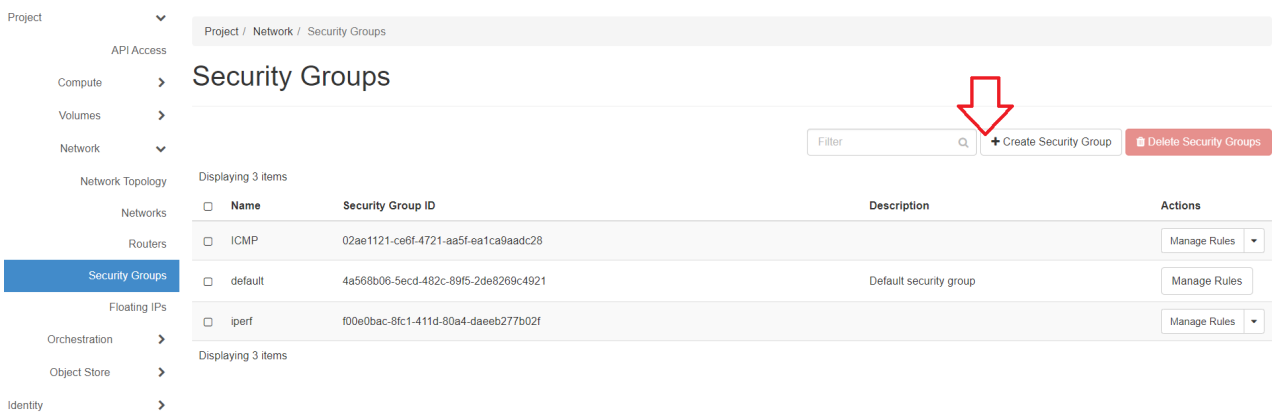


3. Create subnet for the network
Name the subnet
Define network address range in CIDR format. Ex.192.168.10.0/24.



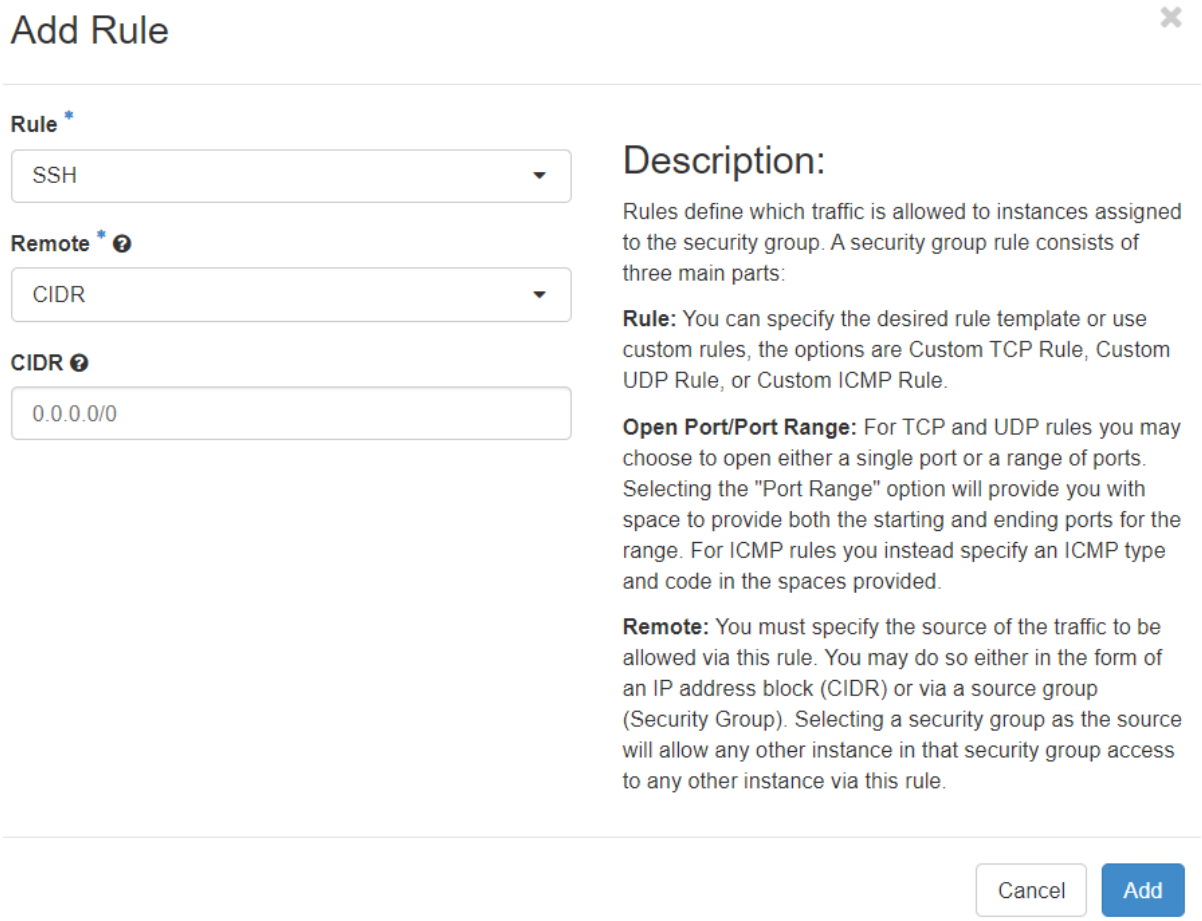
Security groups

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.



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.



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.

Helpful? Yes No

100% found this useful

Rate this article ★★★★★

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

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 • ★★★★★