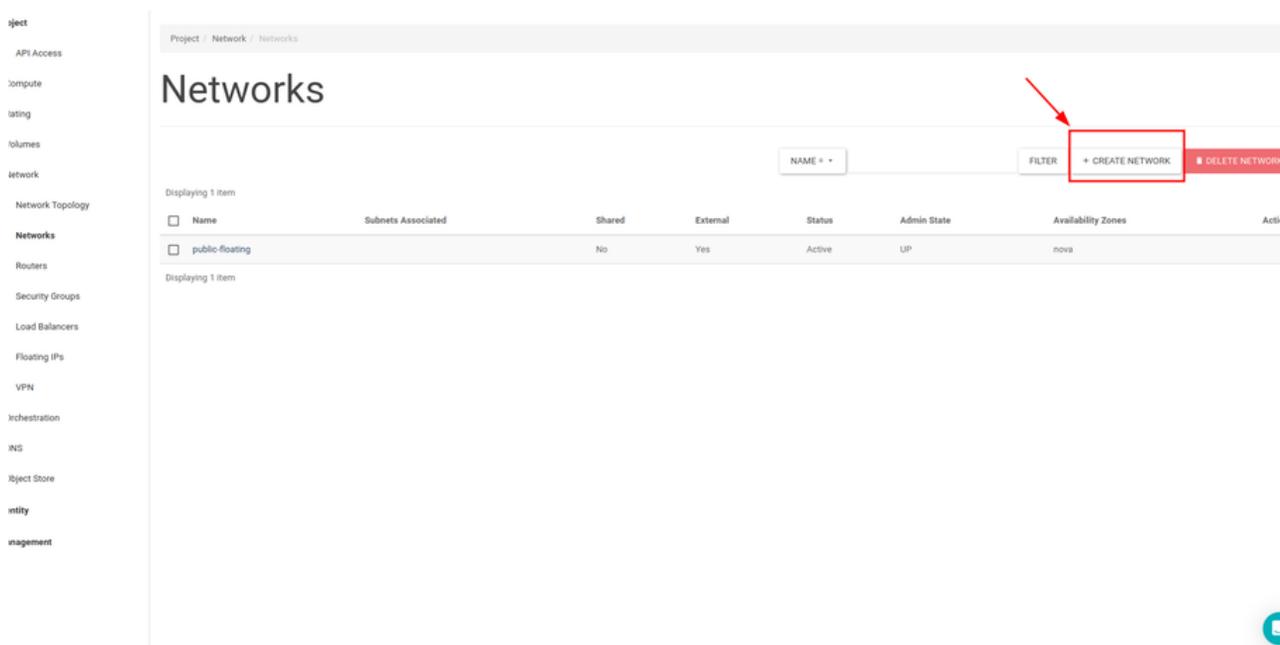


How Network Is Created?

You can create not only server that is not accessible from the outside but also server that is accessible from the outside by using Skyatlas Horizon. For instance your web server can be worked in the isolated network which is accessible from the outside. At the same time your database server is not accessible from the outside.

Creating New Network

Page is opened via Network Menu located at under the Network heading at the left of the panel in the Horizon interface. If there is any network created before it is listed in here. In order to create network click the Create Network button at the top-right.



Features of the network is entered via opened pop-up. Appropriate name should be given at the first tab.

Create Network



- Network**
- Subnet
- Subnet Details

Network Name

Create a new network. In addition, a subnet associated with the network can be created in the following steps of this wizard.

Enable Admin State

Create Subnet

Availability Zone Hints

nova

MTU

- CANCEL
- « BACK
- NEXT »

Creating Subnet

At the second tab, Subnet details should be entered as shown in screenshot.

Create Network



Network

Subnet

Subnet Details

Subnet Name

Network Address

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 »

Adding DNS

At the final tab, DNS addresses should be entered same as shown in screenshot and then click Create button at the right down to complete process.

Create Network



Network

Subnet

Subnet Details

Enable DHCP

Specify additional attributes for the subnet.

Allocation Pools [?](#)

DNS Name Servers [?](#)

Host Routes [?](#)

CANCEL

« BACK

CREATE

Created network is listed at the Network page.

Project / Network / Networks

Networks

Displaying 2 items

<input type="checkbox"/>	Name	Subnets Associated	Shared	External	Status	Admin State	Availability Zones	Actions
<input type="checkbox"/>	support Network		No	No	Active	UP	nova	EDIT NETWORK
<input type="checkbox"/>	public-floating		No	Yes	Active	UP	nova	

Displaying 2 items

Creating New Router

Page is opened via Routers menu located under the Network heading at the left of the panel. If there is any router created before it is listed here. In order to create new router, click the Create Router button at the top-right.

Project / Network / Routers

Routers

ROUTER NAME = *

Name	Status	External Network	Admin State	Availability Zones	Actions
No items to display.					

An appropriate name should be given to the router via opened pop-up.

Create Router ✕

Router Name

Enable Admin State ?

External Network

SELECT NETWORK ▼

Availability Zone Hints ?

nova ▲

Created router is listed at the Routers page.

- ject
- API Access
- ompute
- ating
- olumes
- etwork
- Network Topology
- Networks
- Routers**
- Security Groups
- Load Balancers
- Floating IPs
- VPN
- rchestration
- NS
- bject Store
- ntity
- inagement

Project / Network / Routers

Routers

ROUTER NAME = -
FILTER
+ CREATE ROUTER
DELETE ROUTER

Displaying 1 item

	Name	Status	External Network	Admin State	Availability Zones	Actions
<input type="checkbox"/>	SUPPORT Router	Active	public-floating	UP	nova	CLEAR GATEWAY

Displaying 1 item

Adding Interface

Click the router name button at the Routers page to open the page including router's details. Click the Add Interface button at the right.

Project / Network / Routers

Routers

ROUTER NAME ▾ FILTER + CREATE ROUTER DELETE Routers

Displaying 1 item

<input type="checkbox"/>	Name	Status	External Network	Admin State	Availability Zones	Actions
<input type="checkbox"/>	SUPPORT Router	Active	public-floating	UP	nova	CLEAR GATEWAY

Displaying 1 item

Project / Network / Routers / SUPPORT Router

SUPPORT Router

CLEAR GATEWAY ▾

Overview **Interfaces** Static Routes

+ ADD INTERFACE

Name	Fixed IPs	Status	Type	Admin State	Actions
No items to display					

Added Interface is listed at the router details page.

Selecting Gateway

After the steps mentioned above router at the Router page should be chosen as a gateway. Click the Set Gateway button at the end of the router line to choose gateway.

Project / Network / Routers

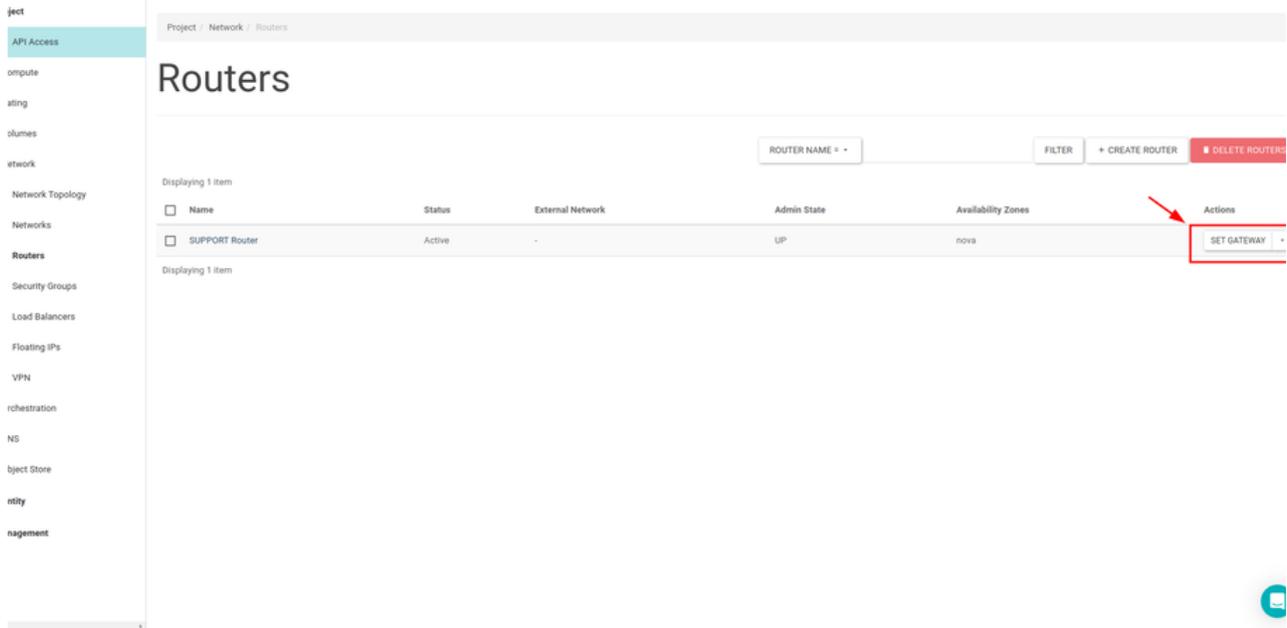
Routers

Displaying 1 item

ROUTER NAME ▾ FILTER + CREATE ROUTER DELETE ROUTERS

<input type="checkbox"/>	Name	Status	External Network	Admin State	Availability Zones	Actions
<input type="checkbox"/>	SUPPORT Router	Active	-	UP	nova	SET GATEWAY ▾

Displaying 1 item



After that gateway selection is completed.

Project / Network / Routers

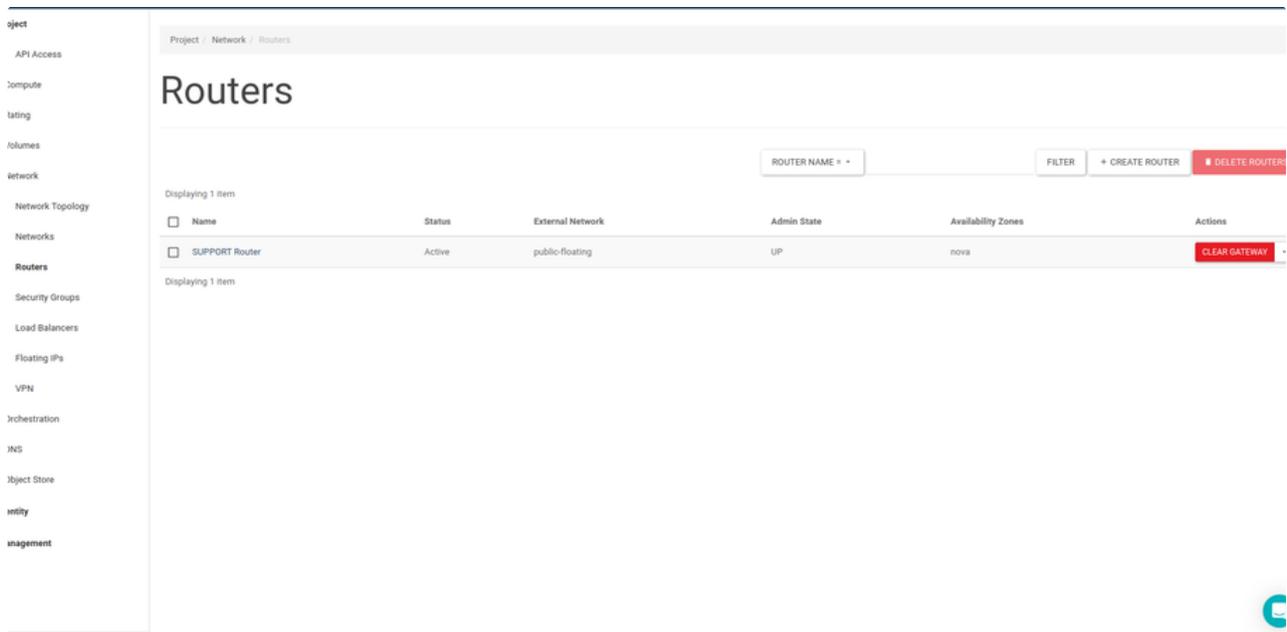
Routers

Displaying 1 item

ROUTER NAME ▾ FILTER + CREATE ROUTER DELETE ROUTERS

<input type="checkbox"/>	Name	Status	External Network	Admin State	Availability Zones	Actions
<input type="checkbox"/>	SUPPORT Router	Active	public-floating	UP	nova	CLEAR GATEWAY ▾

Displaying 1 item

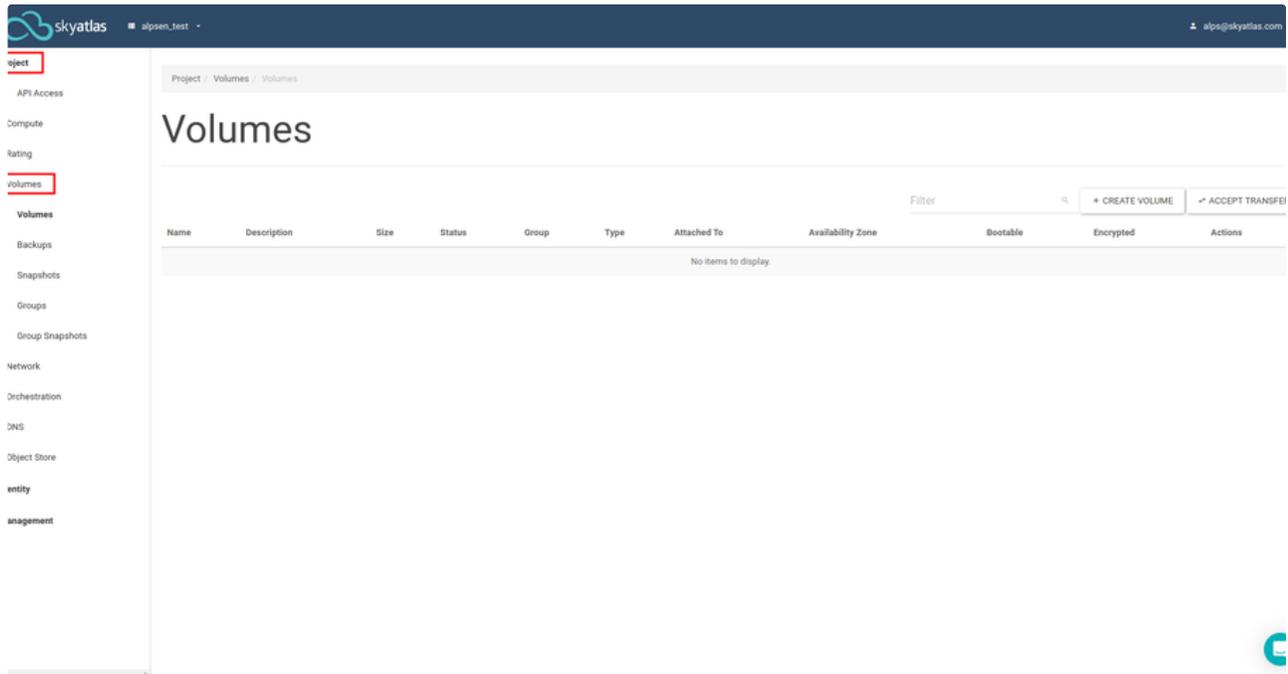


How to Create Volume?

After logging panel.skyatlas.com, click on the Project tab on the left hand side to create a volume. You can follow steps:

1 Project → Volumes

After that, you should see **Volumes** page.



For creating a volume, you should click on the Create Volume button. Now, you should see Create Volume pop-up page.

Create Volume ✕

Volume Name

Description

Volume Source
NO SOURCE, EMPTY VOLUME ▾

Type
FAST ▾

Size (GiB) *
1 +

Availability Zone
NOVA ▾

Group 
NO GROUP ▾

Description:
Volumes are block devices that can be attached to instances.

Volume Type Description:
fast
No description available.

Volume Limits

Total Gibibytes 0 of 1,000 GiB Used

Number of Volumes 0 of 10 Used

In the Volume Name field, enter the name you want to give the new volume. You can write explanations about the new volume in the Description field. You need to select "No source, empty volume " from Volume Source list. Also, you need to specify Size in gigabytes for the new volume.

After filling the corresponding fields, you can complete creating volume by clicking the **Create Volume** button. You can see information about the new volume in the **Volume** tab.

Project

API Access

Compute

Rating

Volumes

Volumes

Backups

Snapshots

Groups

Group Snapshots

Network

Orchestration

DNS

Object Store

Identity

Management

Project / Volumes / Volumes

Volumes

Filter

[+ CREATE VOLUME](#)[ACCEPT TRANSFER](#)[DELETE VOLUMES](#)

Displaying 1 item

<input type="checkbox"/>	Name	Description	Size	Status	Group	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
<input type="checkbox"/>	SUPPORT	Support Volume	1GiB	Available	-	fast		nova	No	No	EDIT VOLUME

Displaying 1 item



Access and Security Settings

Certain procedures should be followed at the Horizon interface to remote access to your server before creating it.

Security Rules

You can create and regulate security rules in order to access Instance.

In order to see these rules, open the Security Groups tab at “ Network → Security Groups “ page and click the Manage Rules button.

The screenshot displays the OpenStack Horizon interface for the 'Security Groups' page. The breadcrumb navigation at the top reads 'Project / Network / Security Groups'. The main heading is 'Security Groups'. Below the heading, there are two buttons: '+ CREATE SECURITY GROUP' and 'DELETE SECURITY GROUP'. A table lists the security groups, with one entry: 'default' with ID 'ab90afd2-b026-41b8-8932-e638ac2be400' and description 'Default security group'. The 'Actions' column for this entry contains a 'MANAGE RULES' button, which is highlighted with a red border. The left sidebar shows a navigation menu with 'Security Groups' selected.

Name	Security Group ID	Description	Actions
default	ab90afd2-b026-41b8-8932-e638ac2be400	Default security group	MANAGE RULES

Rules can be deleted or new rules can be added from the page in which security rules are listed. To add new rule, click the Add Rule button at the page.

Project / Network / Security Groups / Manage Security Group Rule...

Manage Security Group Rules: default (ab90afd2-b026-41b8-8932-eb38ae2be400)

+ ADD RULE DELETED RULES

Displaying 8 items

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Description	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	-	DELETE RULE
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	Any	Any	-	default	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	TCP	80 (HTTP)	0.0.0.0/0	-	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	TCP	443 (HTTPS)	0.0.0.0/0	-	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv6	Any	Any	-	default	-	DELETE RULE

Displaying 8 items

From the opened page, rules that provide accessibility of the instance can be added by choosing.

Add Rule ✕

Rule *

CUSTOM TCP RULE

- Custom TCP Rule
- Custom UDP Rule
- Custom ICMP Rule
- Other Protocol
- All ICMP
- All TCP
- All UDP
- DNS
- HTTP
- HTTPS
- IMAP
- IMAPS
- LDAP
- MS SQL
- MYSQL
- POP3
- POP3S
- RDP
- SMTP
- SMTPS
- SSH

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

About SSH Connection

SSH rule should be added to access Linux instance by SSH via port 22.

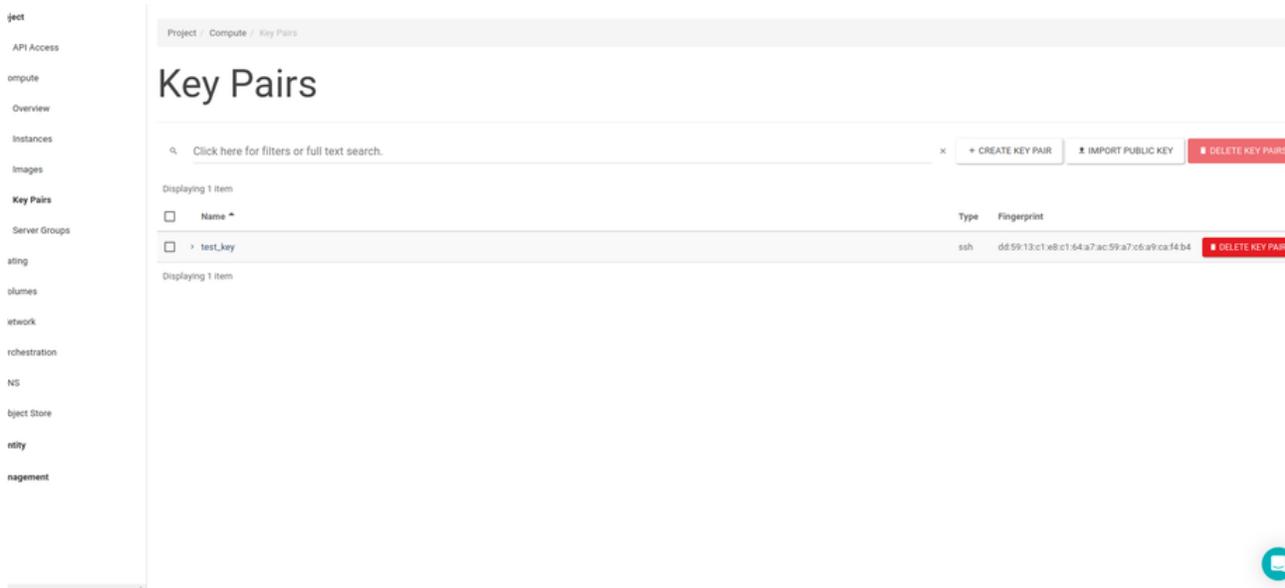
About RDP Connection

RDP rule should be added to access Windows instance by RDP via port 3389.

Creating Key Pair

In order to see these rules, open the Key Pairs tab at Compute → Key Pairs

If there is any key created before it is listed here. Click the Create Key Pair button at the top-right to create new key.



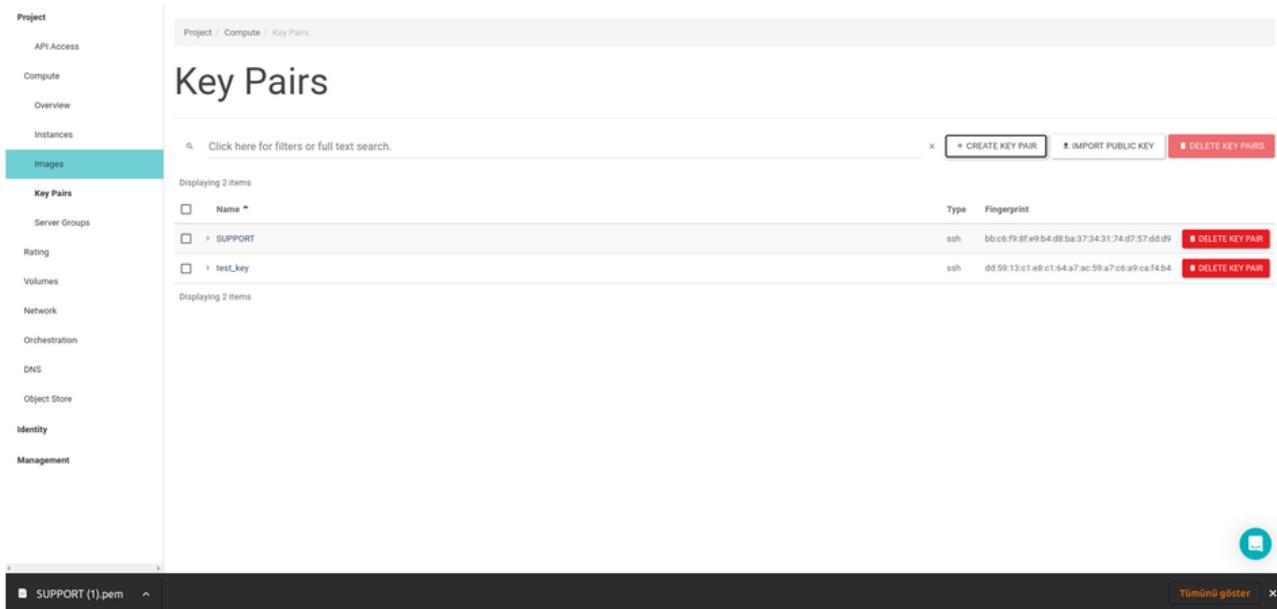
An appropriate name is given to the key that will be used for access to instances at the opened pop-up. Click the Create Key Pair button.

The 'Create Key Pair' dialog box is shown. It has a title bar with a close button (X) and a help icon (?). The form contains two fields:

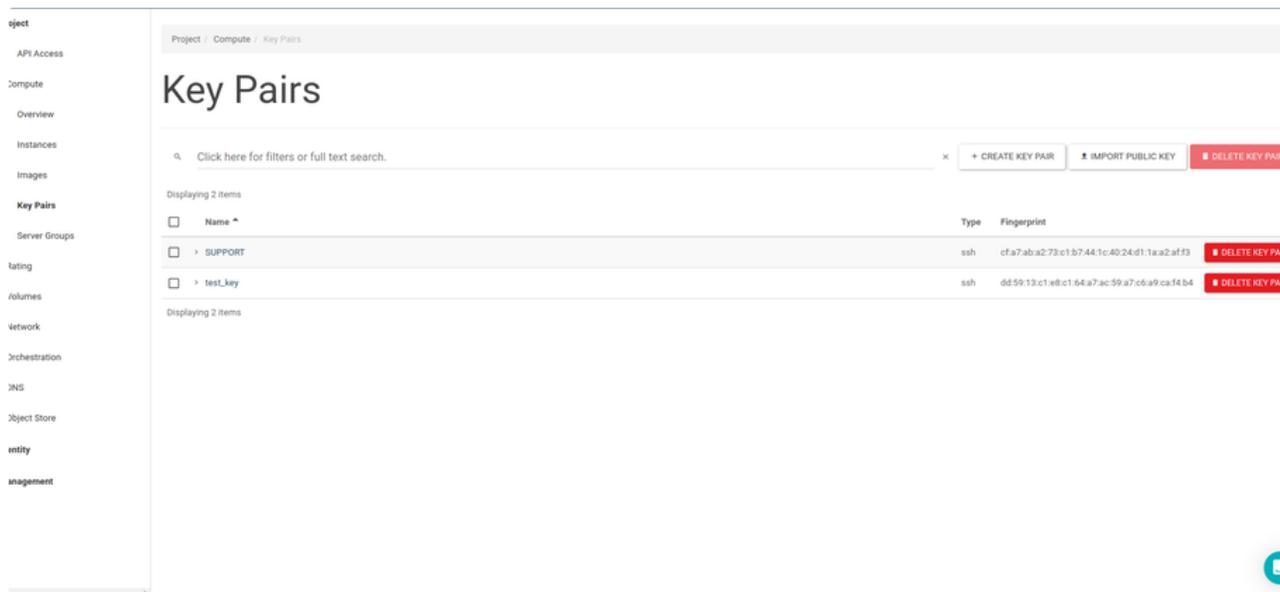
- Key Pair Name**: A text input field containing 'SUPPORT' with a green checkmark on the right.
- Key Type**: A dropdown menu currently set to 'SSH Key'.

At the bottom of the dialog are two buttons: 'X CANCEL' and '+ CREATE KEY PAIR'.

After that, download the file that has .pem extension and has a name given for the key. Then downloaded file will be used to connect to public IP given Instance via SSH.



Created Key is listed at the Key Pairs tab in the Key Pairs page.



Permission change should be done as mentioned below for .pem file to be capable of making connection to instance.
`chmod 600 <path/to/file.pem>`

Adding Key Pair

A new key can be created on the system in which Instance connection will be made.
In order to do this, firstly a new key is created via console on the local system by command line mentioned below.

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

After that created key is gotten to import to the panel.

```
cat ~/cloud.key.pub
```

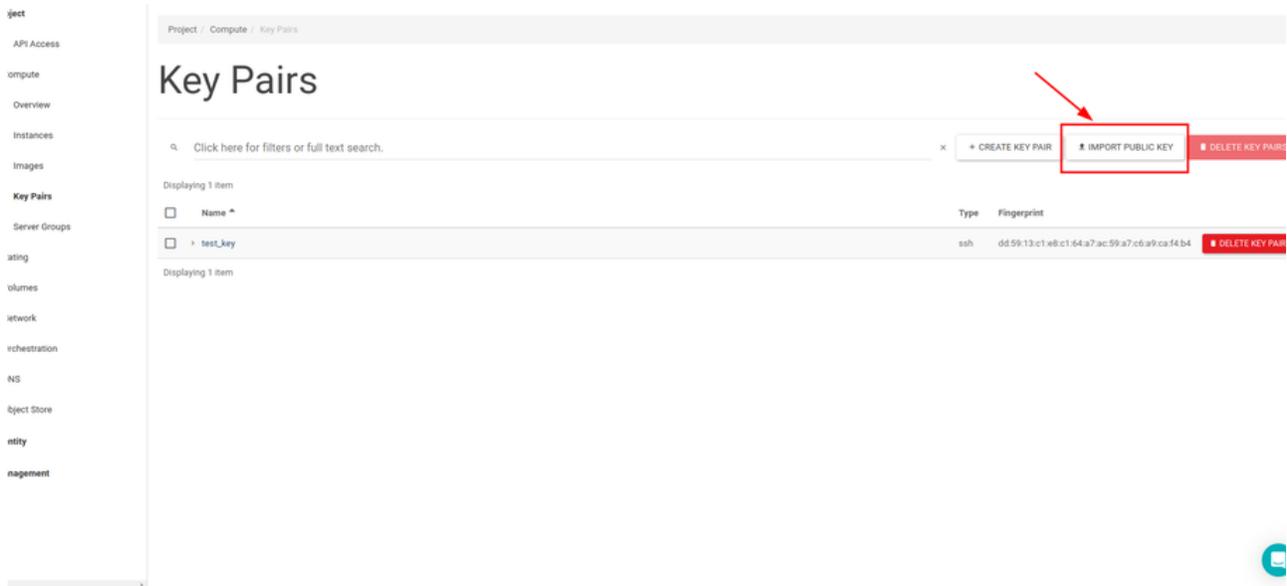
Key created as mentioned below is copied to import.

```
user@user:~$ cat ~/cloud.key.pub
```

```
ssh-rsa
```

```
AAAAB3NzaC1yc2EAAAADAQABAAQAC5pQvB/L1BO1MvI6XCKtA6raCukvUY4A7btssf1Ln/Of9/afA39Wbqc9CUZqjw6V/IWA96Fm9e1Xzh/4q7BHZgIEiLw1grpstideKq3dVUKt1UI1+c7Glp3XXlpo3+QtxA5pZyi30l2nDrkbn6Wqhiwu2jhz74iMbbmAMXIK9baN2f2yC65ucUV/gj9U/tU0C/vneOtp+26ln6+roxi9TYWs9msldAQd1iK00Tj9irsbd0h0X/pQ73CMxnBz9400ss027KCjoWeJZGezn9IYoHKrFfxVAZ6oP+sjqfGy7KWJQoxsZHcn0XcMB3U7+/llkJHj199wqpY19igLL user@user
```

Text copied from ssh-rsa part to user@user(inclusive) is added by clicking Import Key Pair at the Key Pairs screen on the panel.



A key name is entered via Import Key Pair pop-up page and past the copied text here. Then click the Import Key Pair button.

Import Public Key



Key Pair Name *



SUPPORT ✓

Key Type *

SSH Key

Load Public Key from a file

Dosya seçilmedi

Public Key * (Modified)

Content size: 379 bytes of 16.00 KB

```
AAAAB3NzaC1yc2EAAAADAQABAAQBAOC5pQvB/L1B01Mvl6XCKtA6raCukvUY4A7btssf1Ln/Of9  
/afA39Wbqc9CU7...Kq3dVUKt1Ul1+c7Glp3XXlipo3  
+QtxA5pZyi30l2r...5ucUV/gj9U/tU0C/vne0tp+26ln  
6+roxi9TYWs9m...?7KCjoWeJZGezn9IYoHKrFfxVA  
Z6oP+sjqfGy7KWJQoxsZHcN0XcMB3U7+/lkiHjl99wqpY19igLL user@user
```

Created key is listed at the Key Pairs tab on the Key Pairs page.

Adding Public IP

If you want to access created Instance via Internet, public IP should be assigned. For this open the Floating IP's tab on the Network page. Click the Allocate IP To Project button at the top-right.

Pool selection at the opened pop-up remains default and click the Allocate IP button at the right down. Therefore, a new public IP is assigned to project.

Allocate Floating IP ✕

Pool ^{*}
 PUBLIC-FLOATING ▾

Description

DNS Domain

DNS Name

Description:

Allocate a floating IP from a given floating IP pool.

Project Quotas

Floating IP 0 of 50 Used

CANCEL
ALLOCATE IP

Assigned Public IPs is listed on the Floating IP's tab.

- Project
- API Access
- Compute
- Rating
- Volumes
- Network
 - Network Topology
 - Networks
 - Routers
 - Security Groups
 - Load Balancers
 - Floating IPs**
 - VPN
 - Orchestration
 - DNS
 - Object Store
- Identity
- Management

Project / Network / Floating IPs

Floating IPs

FLOATING IP ADDRESS ▾

FILTER

ALLOCATE IP TO PROJECT

RELEASE FLOATING IPs

Displaying 1 item

	IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions
<input type="checkbox"/>	213.14.226.241				-	public-floating	Down	ASSOCIATE ▾

Displaying 1 item

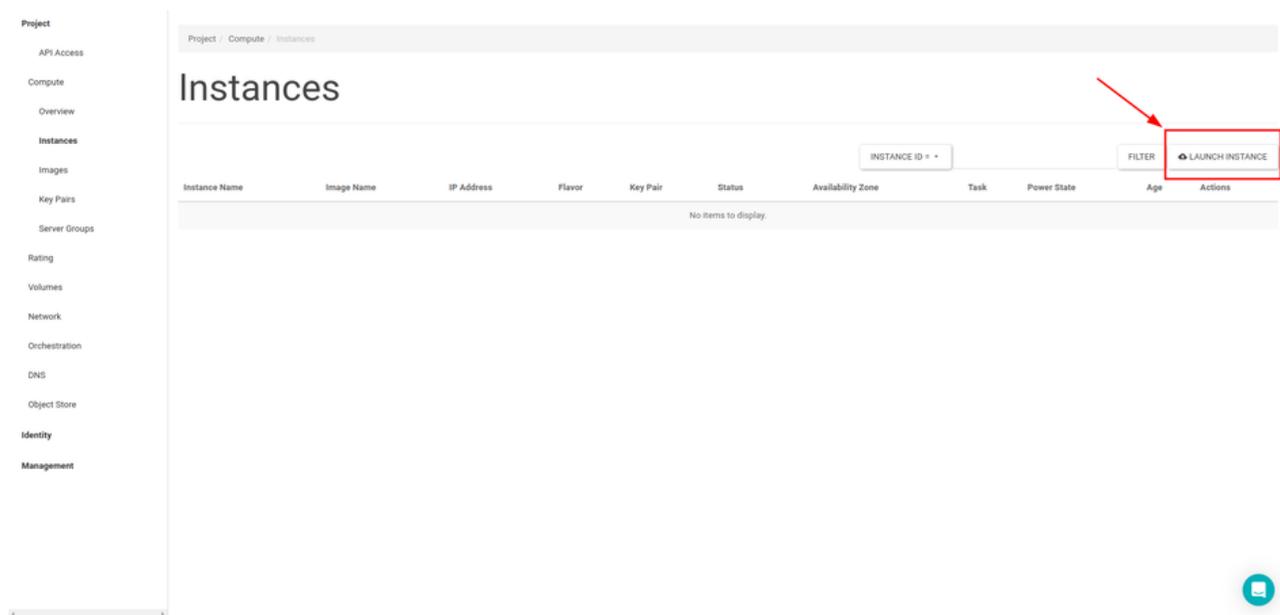
Launch Your First Server

You can create your own server in a few minutes by using SkyAtlas Horizon interface. In order to do this, first of all you should create a network and then you should set the settings of access and security. After doing previous steps, you can create your first server by following steps that will be mentioned below.

Creating Server

Cloud servers are defined as Instance in the Horizon interface.

Page is opened via Instance menu which is placed under the Compute heading located in left of the panel. If there is any instance created before it would be listed here. To create new instance you should click the Launch Instance button located in the top-right.



Firstly requested name is entered to Instance Name area. After that "Select Boot Source" is selected for instance that will be created for very first time. Then, needed operating system is chosen from the image list. Then needed flavor is chosen from the Flavor selection and Launch button at the rightdown is clicked.

Launch Instance



Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Details *

Source

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Price

Project Name

Instance Name *

Description

Availability Zone

Any Availability Zone

Count *

1

Total Instances

(10 Max)



0 Current Usage

1 Added

9 Remaining

× CANCEL

← BACK

NEXT →

LAUNCH INSTANCE

Launch Instance



Details *

Source

Flavor *

Networks

Network Ports

Security Groups

Key Pair

Configuration

Server Groups

Scheduler Hints

Metadata

Price

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

Volume Size (GB) *

Delete Volume on Instance Delete

Allocated

Displaying 0 items

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

Displaying 0 items

Available 45

Select one

Displaying 20 items | Next »

Name	Updated	Size	Type	Visibility	
> CentOS	5/9/22 2:36 PM	807.94 MB	QCOW2	Public	<input type="button" value="↑"/>
> CentOS 8	1/20/23 12:54 PM	1.22 GB	QCOW2	Public	<input type="button" value="↑"/>
> Debian 10 Buster	1/20/23 12:54 PM	556.65 MB	QCOW2	Public	<input type="button" value="↑"/>
> Debian 10 Buster + Bugzilla	1/20/23 12:49 PM	1.56 GB	QCOW2	Public	<input type="button" value="↑"/>
> Debian 10 Buster + CakePHP	1/20/23 12:53 PM	1.26 GB	QCOW2	Public	<input type="button" value="↑"/>

Launch Instance ✕

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

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

Allocated

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

▼ Available 15 Select one

🔍 ✕

Name	VCPUS	RAM	Total Disk	Root Disk	Ephemeral Disk	Public	
> B1-Small	1	2 GB	0 GB	0 GB	0 GB	Yes	↑
> E1-Small	1	4 GB	0 GB	0 GB	0 GB	Yes	↑
> B1-Medium	2	4 GB	0 GB	0 GB	0 GB	Yes	↑
> B1-Large	4	8 GB	0 GB	0 GB	0 GB	Yes	↑
> E1-Medium	2	8 GB	0 GB	0 GB	0 GB	Yes	↑
> X1-Small	1	8 GB	0 GB	0 GB	0 GB	Yes	↑
> B1-XLarge	8	16 GB	0 GB	0 GB	0 GB	Yes	↑
> X1-Medium	2	16 GB	0 GB	0 GB	0 GB	Yes	↑
> E1-Large	4	16 GB	0 GB	0 GB	0 GB	Yes	↑
> E1-XLarge	8	32 GB	0 GB	0 GB	0 GB	Yes	↑
> X1-Large	4	32 GB	0 GB	0 GB	0 GB	Yes	↑

Observe that created instance's status is running.

- object
- API Access
- compute
- Overview
- Instances
- Images
- Key Pairs
- Server Groups
- Networking
- Volumes
- Network
- Orchestration
- INS
- Object Store
- Identity
- Management

Project / Compute / Instances

Instances

INSTANCE ID ▾

FILTER

LAUNCH INSTANCES

DELETE INSTANCES

MORE ACTIONS ▾

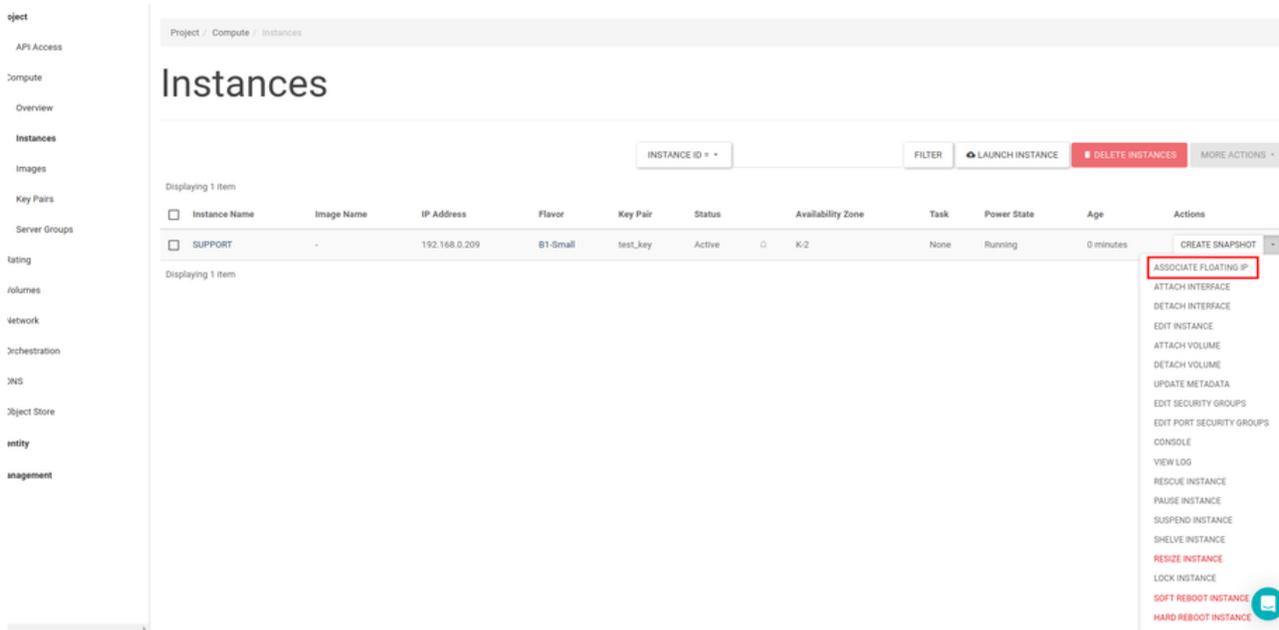
Displaying 1 item

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
<input type="checkbox"/>	SUPPORT	-	10.0.0.1	B1-Small	test_key	Active	K-2	None	Running	0 minutes	CREATE SNAPSHOT ▾

Displaying 1 item

Adding Public IP

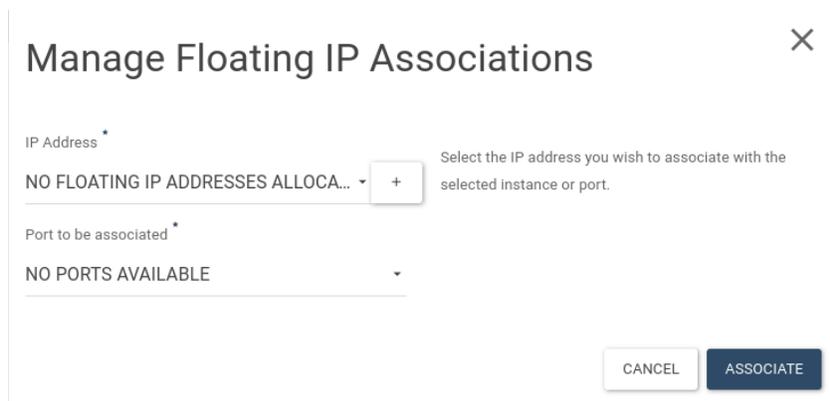
In order to access created instance via Internet, public IP should be given at first. So as to do this, "Associate Floating IP" option is selected from list at the end of the Instance line which public IP will be given.



The screenshot shows the OpenStack 'Instances' page. A table lists one instance with the following details:

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
SUPPORT	-	192.168.0.209	B1-Small	test_key	Active	K-2	None	Running	0 minutes	CREATE SNAPSHOT, ASSOCIATE FLOATING IP, ATTACH INTERFACE, DETACH INTERFACE, EDIT INSTANCE, ATTACH VOLUME, DETACH VOLUME, UPDATE METADATA, EDIT SECURITY GROUPS, EDIT PORT SECURITY GROUPS, CONSOLE, VIEW LOG, RESCUE INSTANCE, PAUSE INSTANCE, SUSPEND INSTANCE, SHelve INSTANCE, RESIZE INSTANCE, LOCK INSTANCE, SOFT REBOOT INSTANCE, HARD REBOOT INSTANCE

IP gotten before is chosen from the opened pop-up and Associate button at the right down is clicked.



The dialog box titled 'Manage Floating IP Associations' contains the following fields and controls:

- IP Address ***: A dropdown menu currently showing 'NO FLOATING IP ADDRESSES ALLOCA...' with a '+' button to its right. A tooltip below it reads: 'Select the IP address you wish to associate with the selected instance or port.'
- Port to be associated ***: A dropdown menu currently showing 'NO PORTS AVAILABLE'.
- Buttons**: 'CANCEL' and 'ASSOCIATE' buttons at the bottom right.

IP information is viewed at the IP Address location. This location is belong to the instance that IP is assigned in the Instance page.

Project

API Access

Compute

Overview

Instances

Images

Key Pairs

Server Groups

Rating

Volumes

Network

Orchestration

DNS

Object Store

Identity

Management

Project / Compute / Instances

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	Age	Actions
<input type="checkbox"/>	SUPPORT	Ubuntu-20.04	192.168.1.17	B1-Small	test_key	Active	K-2	None	Running	3 minutes	CREATE SNAPSHOT ▾

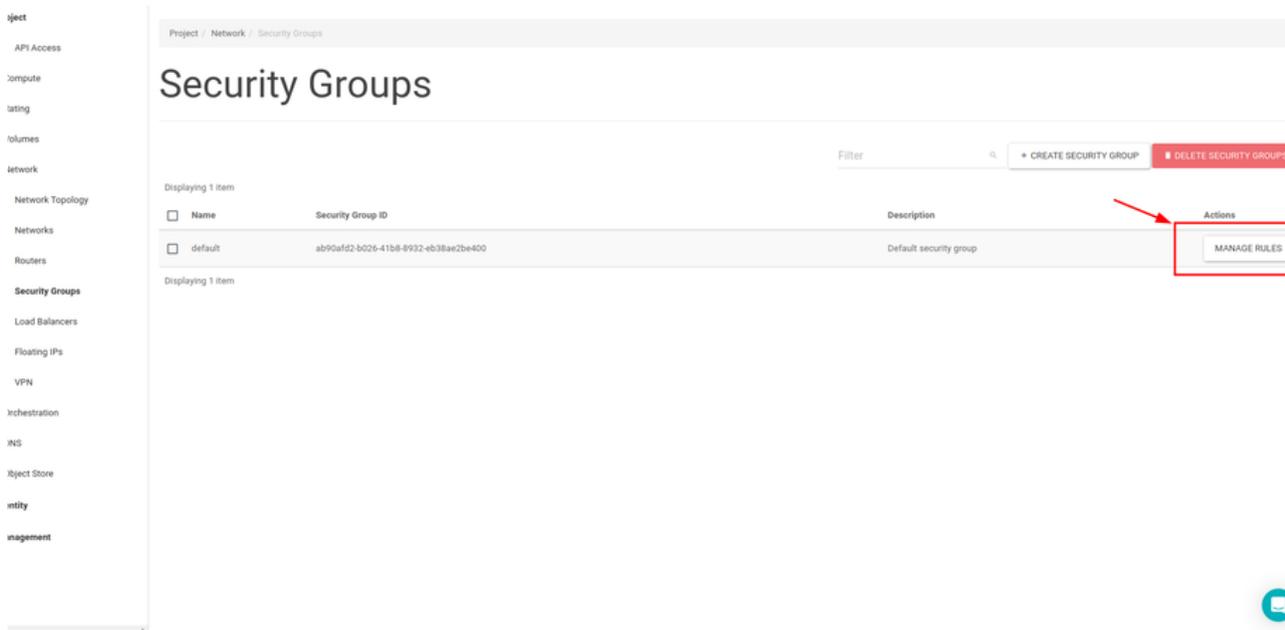
Displaying 1 item



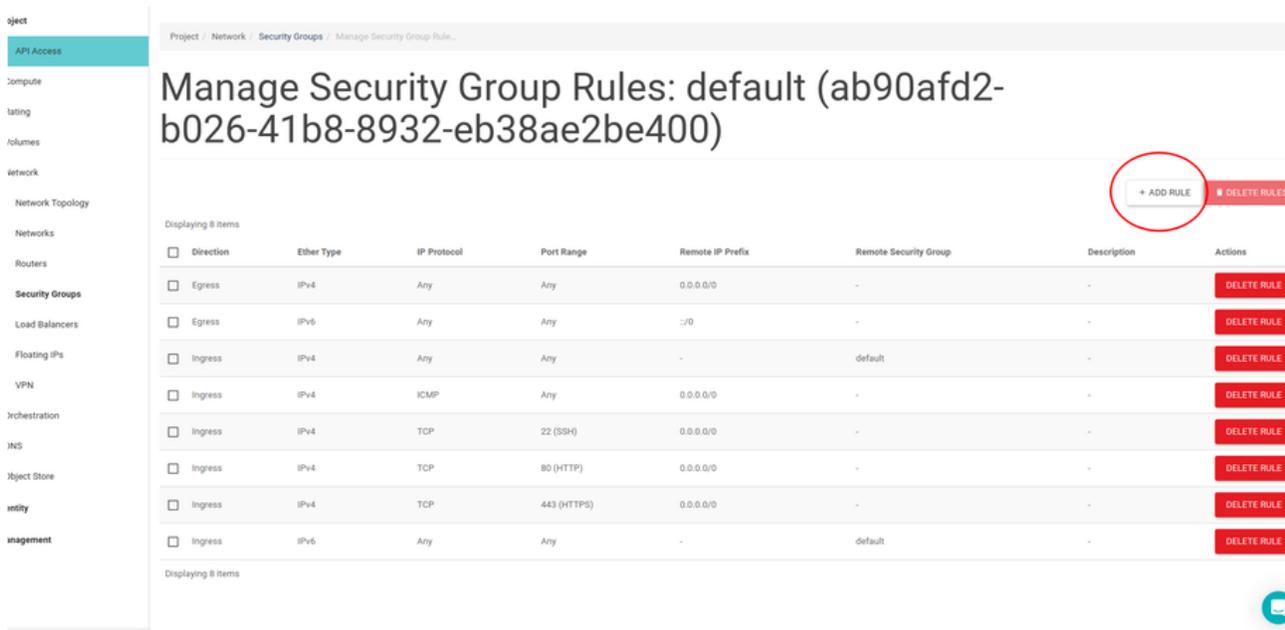
SSH Connection From Specific Public IP Address to Your Instance

If you want access to your server from certain IP address, you can do this in the Access & Security settings from Skyatlas panel. You can follow the sections:

1 Network -> Security Groups -> MANAGE RULES



After that, you should see the **Add Rule** pop-up page.



Add Rule ✕

Rule *

CUSTOM TCP RULE

Description ?

Direction

INGRESS

Open Port *

PORT

Port ?

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.

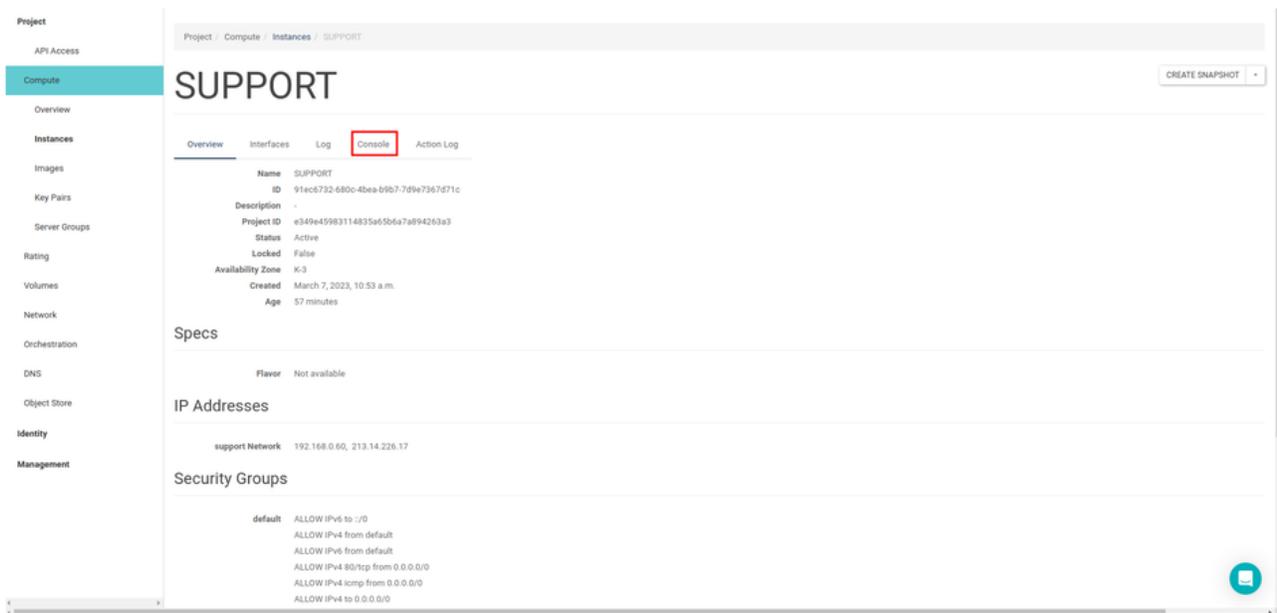
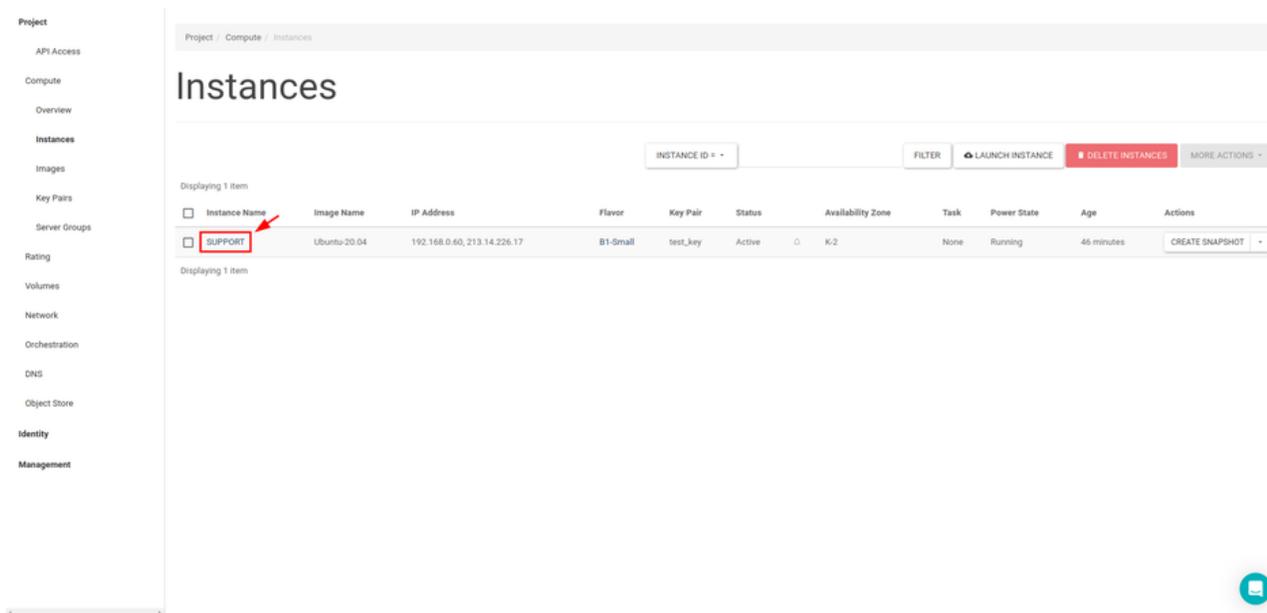
Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance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

Fill in the blanks as follows. Replace **CIDR** text box to your **Public IP Address** and click **Add** button.

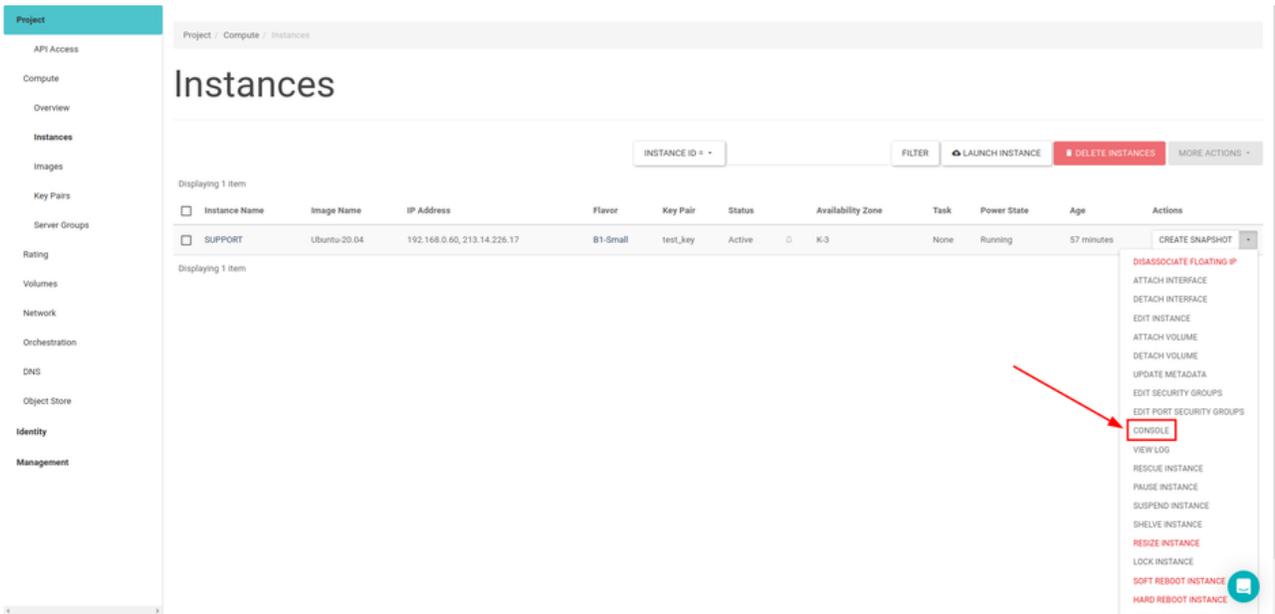
After this process, your instance will only be accessible from your public IP address. Feel free to add more IP address.

Accessing Console And Code 1006 Error

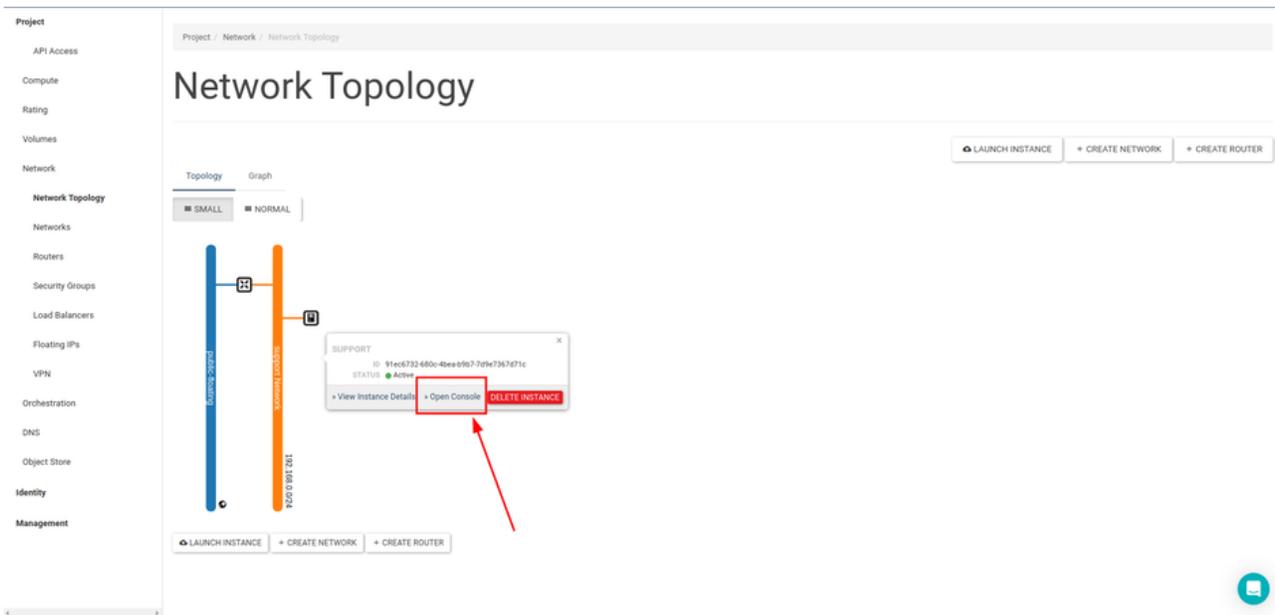
1- First, list your current servers by going to the **Compute > Instances** tab on the panel on the left. Then click on the server whose console you want to access. By selecting the console from the tabs above, you can access the console to which the server is connected. You can also easily view general information and logs about your server from this screen.



2- In order to reach it more practically, you can go to **Compute > Instances** tab on the left panel and instead of clicking on the server you want to access the console, you can directly access the console by selecting the console from the "drop box" menu on the far right.



3- If you wish, you can access the console by clicking on the server you want from the Network Topology screen and clicking the "Open Console" text on the bubble that opens.



Code 1006 Error

It is possible to get a Code 1006 error when accessing the console. You can access the console by solving this error quite easily.

Click on the "Click here to show console" text on the console.

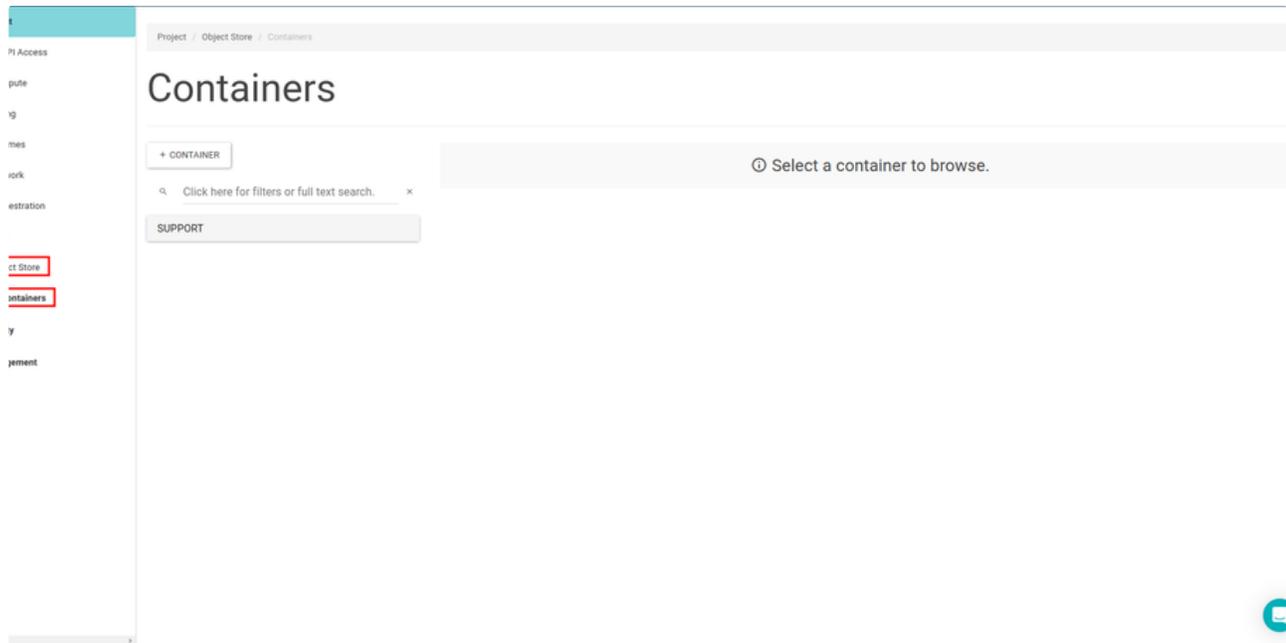


When you refresh the opened page by clicking the **refresh button** on your browser or by pressing the "**F5**" key, you will see the console screen come up.

How to Create Container For Object Storage on SkyAtlas Panel

For the object storage operations, you can follow sections :

1 Project -> Object Store -> Containers



To create a new container, you should click on the **Container** button. On the **Create Container** pop-up page, you must specify the container name from **Container Name** text field.

Note: If you choose the Public option, you allow anyone with the public URL to gain access to your objects in the container.

Create Container ✕

Container Name ^{*} ?

Container name must not contain "/".

Storage Policy ^{*}

default-placement ▼

Container Access

A Public Container will allow anyone with the Public URL to gain access to your objects in the container.

After creating container, you can see the new container on the **Containers** screen.

Project / Object Store / Containers

Containers

Object Count: 0
Size: 0 bytes
Date Created: Mar 2, 2023
Storage Policy: default-placement
 Public Access: Disabled

Displaying 0 items

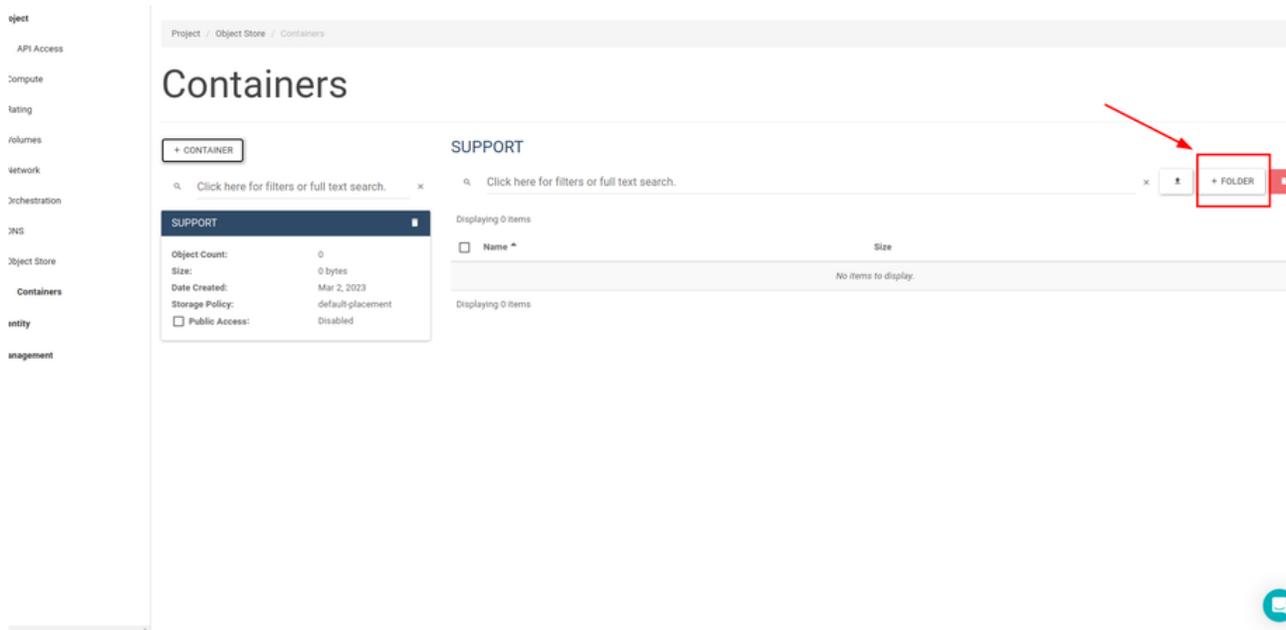
Name	Size
No items to display.	

Displaying 0 items

If you click on the container, you will see information about the container.

How to Upload My File into Container?

Click **Upload File** button to upload any file in the container.



From the **Upload File** pop-up page, you can choose files to upload into container.



After uploading file, you will see information about the your objects on the screen.

- Object
- API Access
- Compute
- Logging
- Volumes
- Network
- Orchestration
- INS
- Object Store
- Containers
- Identity
- Management

Containers

CONTAINER

SUPPORT

Click here for filters or full text search.

Click here for filters or full text search.

FOLDER

SUPPORT

Object Count: 1
Size: 0 bytes
Date Created: Mar 2, 2023
Storage Policy: default placement
 Public Access: Disabled

Displaying 1 item

<input type="checkbox"/>	Name *	Size	
<input type="checkbox"/>	SUPPORT	Folder	DELETE



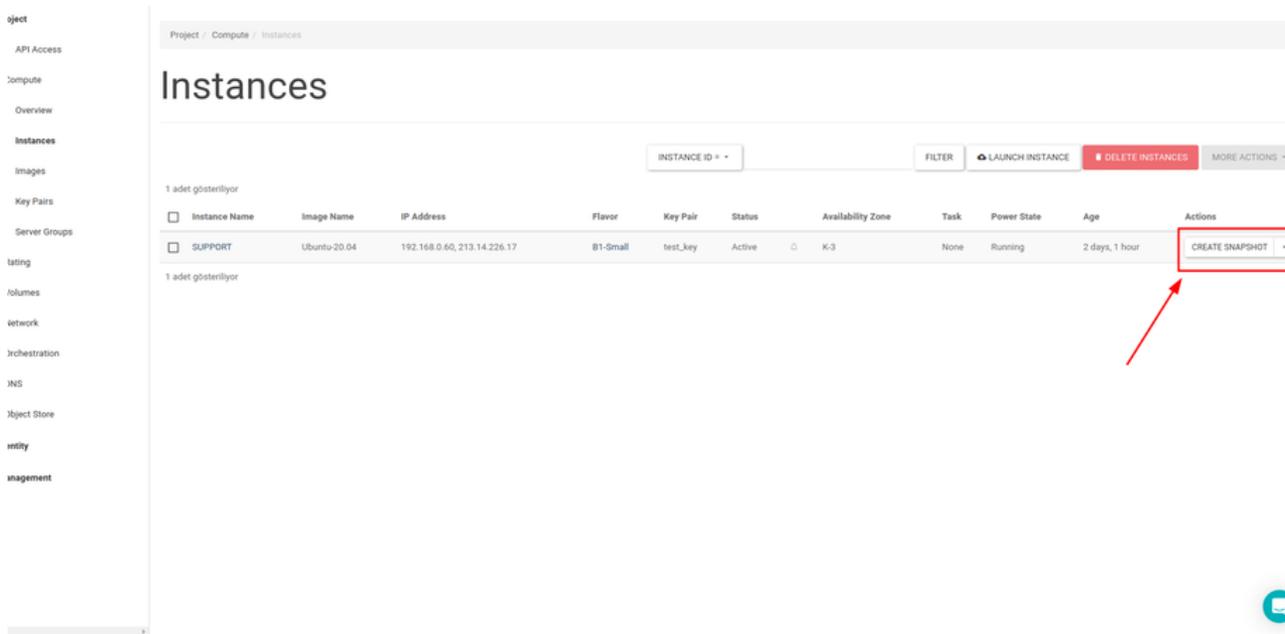
How to Create Snapshot on SkyAtlas Panel

A snapshot represents a frozen image of a volume. The source of a snapshot is called an "original." When a snapshot is created, it looks exactly like the original at that point in time. As changes are made to the original, the snapshot remains the same and looks exactly like the original at the time the snapshot was created. Also you create an instance from this snapshot that identically same to your original instance.

If you want to create snapshot, you must have a instance that runs on SkyAtlas Panel.

Launch Your First Server

To perform the snapshot operation, you must click the **Create Snapshot** button on the **Actions** tab of your server.



You will create a snapshot on the **Create Snapshot** pop-up page. Fill the **Snapshot Name** text field and click the **Create Snapshot** button.

Create Snapshot

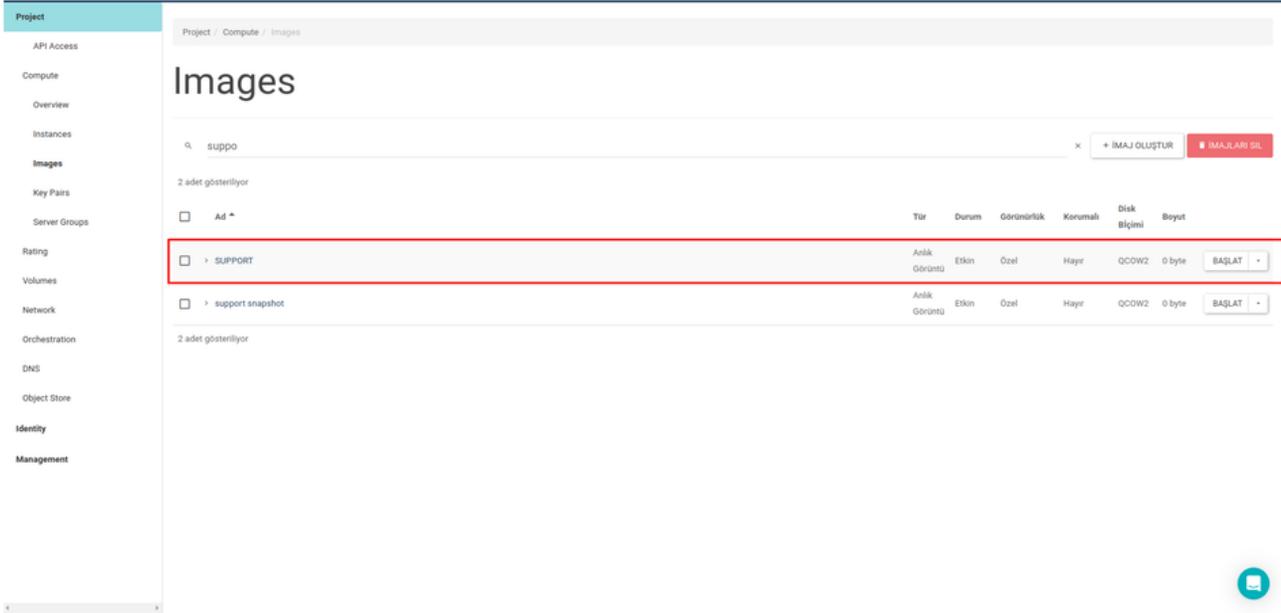
Snapshot Name *

Description:

A snapshot is an image which preserves the disk state of a running instance.

CANCEL CREATE SNAPSHOT

After these operations, you will see your snapshot, that created by you , in the **Images** section.



Creating a New Server from Snapshot

If you want to create an instance from the snapshot, click the **Launch** button that located at **Actions** tab. You must fill sections that **Details**, **Flavor** and **Key Pairs**. After that, in the **Source** section, please select **Instance Snapshot** from **Select Boot Source** list. At the bottom you will see your snapshot, that created by you. Please choose image name from this list and click the **Launch Instance** button.

Sanal Makine Başlat



Detaylar *

Kaynak

Şablon *

Ağlar

Ağ Bağlantı Noktaları

Güvenlik Grupları

Key Pair

Yapılandırma

Sunucu Grupları

Zamanlayıcı İpuçları

Metaveri

Price

Sunucu kaynağı, sunucu oluşturmak için kullanılacak şablondur. Bir imaj, sunucu anlık görüntüsü (imaj anlık görüntüsü), birim anlık görüntüsü üstünde bir birim (etkinse) seçebilirsiniz. Ayrıca yeni bir birim oluşturarak kalıcı depolama da kullanabilirsiniz.

Başlatma Kaynağını Seçin

Sanal Makine Anlık Görüntüsü

Yeni Birim Oluştur

EVET

HAYIR

Birim Boyutu(GB) *

1

Birimi Sanal Makineyi Silinince Sil

EVET

HAYIR

Ayrılmış

0 adet gösteriliyor

Ad	Güncellendi	Boyut	Tür	Görünürlük
----	-------------	-------	-----	------------

Aşağıdaki kullanılabilir öğelerden birini seçin.

0 adet gösteriliyor

Uygun 1

Birini seçin

Click here for filters or full text search.

1 adet gösteriliyor

Ad	Güncellendi	Boyut	Tür	Görünürlük
----	-------------	-------	-----	------------

> Support Snapshot	3/9/23 12:33 PM	0 byte	QCOW2	Özel
--------------------	-----------------	--------	-------	------

1 adet gösteriliyor

× İPTAL

← GERİ

İLERİ →

SANAL MAKINE BAŞLAT

You will see your instance that created from a snapshot in the **Instances** section.

- object
- API Access
- Compute
- Overview
- Instances**
- Images
- Key Pairs
- Server Groups
- Routing
- Volumes
- Network
- Orchestration
- DNS
- Object Store
- entity
- management

Instances

INSTANCE ID FILTER [LAUNCH INSTANCE](#) [DELETE INSTANCES](#) [MORE ACTIONS](#)

2 adet gösteriliyor

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
<input type="checkbox"/>	SUPPORT From Snapshot	-	192.168.0.9	B1-Small	test_key	Build	K-2	Block Device Mapping	No State	0 minutes	ASSOCIATE FLOATING IP
<input type="checkbox"/>	SUPPORT	Ubuntu-20.04	192.168.0.60, 213.14.226.17	B1-Small	test_key	Active	K-3	None	Running	2 days, 1 hour	CREATE SNAPSHOT

2 adet gösteriliyor

How to Create Stack on SktAtlas Panel

Stack allows you deploying multipli instance at the same time.

In this article, we will create a simple stack.

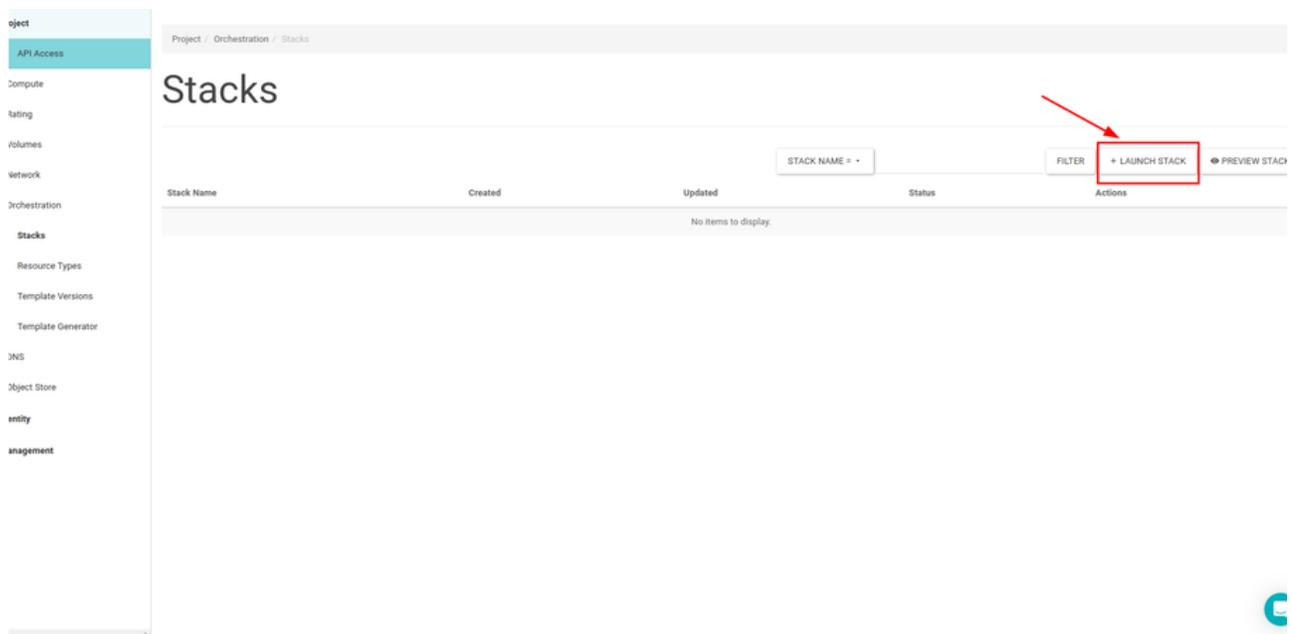
Firstly, you need to create a template file with **.yaml** extension and add the following lines into it.

```
1 # vim stack.yaml
2
3 heat_template_version: 2016-04-08
4
5 description: Simple template to deploy a single compute instance
6
7 parameters:
8   key_name:
9     type: string
10    label: Key Name
11 #   default: cloudkey
12    description: Name of key-pair to be used for compute instance
13
14   image_id:
15     type: string
16    label: Image ID
17 #   default: Ubuntu 16.04 Xenial
18   constraints:
19     - allowed_values: [CentOS Linux release 6.6 (Final) ,
20                       CentOS Linux release 7.0.1406 (Core),
21                       Debian Jessie 8.2,
22                       Debian Wheezy 7.8 ,
23                       Ubuntu 16.04 Xenial ,
24                       Ubuntu Trusty ]
25    description: Image to be used for compute instance
26
27   instance_type:
28     type: string
29    label: Instance Type
30   constraints:
31     - allowed_values: [ General S ,
32                       Compute S ,
33                       General M ,
34                       Compute M ,
35                       General L ,
36                       Extreme S ,
37                       Compute L ,
38                       Extreme M ,
39                       General XL,
40                       Compute XL,
41                       Extreme L,
42                       General XXL,
43                       Extreme XL,
44                       Compute XXL,
45                       Extreme XXL ]
46    description: Type of instance (flavor) to be used
47
48 resources:
```

```
49 Test_Instance1:
50   type: OS::Nova::Server
51   properties:
52     key_name: { get_param: key_name }
53     image: { get_param: image_id }
54     flavor: { get_param: instance_type}
55 Test_Instance2:
56   type: OS::Nova::Server
57   properties:
58     key_name: { get_param: key_name }
59     image: { get_param: image_id }
60     flavor: { get_param: instance_type}
```

You will follow these steps for create a stack:

1 Orchestration → Stack → Launch Stack



Choose the File option from the Template Source for uploading stack.yaml file and click the Next button.

Select Template



Template Source *

Template File ⓘ

 stack.yaml

Environment Source

Environment File ⓘ

 No file selected.

Description:

Use one of the available template source options to specify the template to be used in creating this stack.

Cancel

Next

On the **Launch Stack** pop-up page :

Stack Name: please enter stack name

password for user : please enter your account name

Image ID: please choose image for your instances

Instance Type : please choose flavor type for your instances

Key Name : please enter your private key

after these operations, click the Launch button.

Launch Stack



Stack Name *

Creation Timeout (minutes) *

60 - +

Rollback On Failure

Password for user "alps@skyatlas.com" *

Image ID *

CentOS Linux release 6.6 (Final) ▼

Instance Type *

General S ▼

Key Name *

Description:

Create a new stack with the provided values.

CANCEL

LAUNCH

After creating stack, you will see your **Test_Stack** on the **Stacks** section.

Stack Name	Created	Updated	Status	Actions
Test_Stack	0 minutes	Never	Create Complete	Check Stack

Also, you will see your instances that creating by stacks in the **Instances** tab.

Instances

Instance Name	Image Name	IP Address	Size	Key Pair	Status	Availability Zone	Task	Power State	Time since created	Actions
<input type="checkbox"/> Test_Stack-Test_Instance2-273pnr15qo4d	Ubuntu 16.04 Xenial	10.0.0.204	General M	cloudkey	Active	istanbul-1a	None	Running	2 minutes	Create Snapshot
<input type="checkbox"/> Test_Stack-Test_Instance1-vav76dx04lqx	Ubuntu 16.04 Xenial	10.0.0.203	General M	cloudkey	Active	istanbul-1b	None	Running	2 minutes	Create Snapshot

Displaying 2 items

For further reading about Heat Stack :

[Heat Orchestration Template \(HOT\) Guide](#)

[Heat Orchestration Template \(HOT\) specification](#)

Remote Access to Your Instance

You can access to created instance with different username informations according to selected image. When you connect to Instance you should enter username information that is belong to image to the <username> part.

These are:

- CentOS Linux release 6.6 (Final) → username: **cloud-user**
CentOS Linux release 7.0.1406 (Core) → username: **centos**
Debian Wheezy 7.8 → username: **debian**
- Fedora 21 → username:
- SUSE Linux Enterprise Server 11 SP3 → username: **root**
Turnkey Magento 13.0 → username: **root**
Ubuntu Trusty → username: **ubuntu**
Linux CoreOS 1855.40 → username: **core**

In case of Instances opened with Windows image, you should access Instance after Instance starts via console at the panel and you should generate a password from the Windows Login screen.

Afterwards you can connect the public IP assigned instance via RDP (Remote Desktop Protocol).

- Windows Server 2008 R2 Standard SP1
- Windows Server 2012 R2 Standard (2)

Connection via Created Key

Command line mentioned below should be written to consol screen in order to connect Instance according to method used in Creating Key Pair.

```
ssh -i <path/to/file.pem> <username>@<instance_public_ip>
```

Connection via Added Key

Command line mentioned below should be written to consol screen in order to connect Instance according to method used in Adding Key Pair.

```
ssh -i cloud.key <username>@<instance_public_ip>
```

Instance Connection via Windows

3rd party applications should be used in order to connect and manage Linux Instance via Windows. **PuTTY** is one of the applications. Steps that explain how to connect Linux instance created via **PuTTY** are mentioned below.

PuTTY

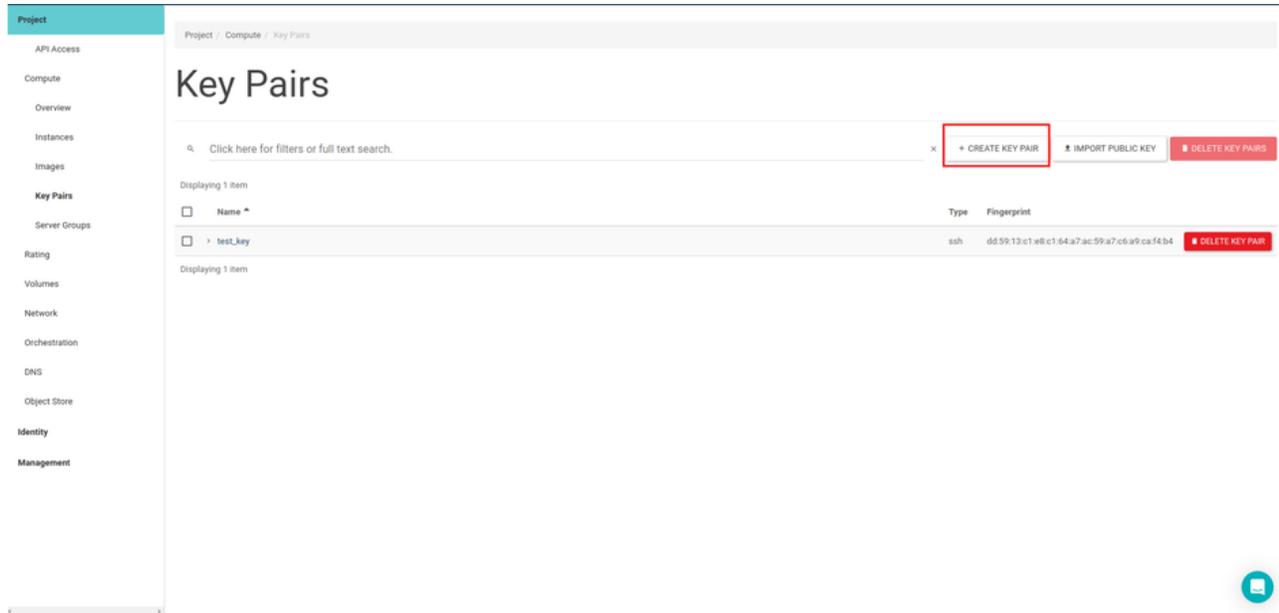
First of all, PuTTY application should be downloaded to Windows. You can download application from the link:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

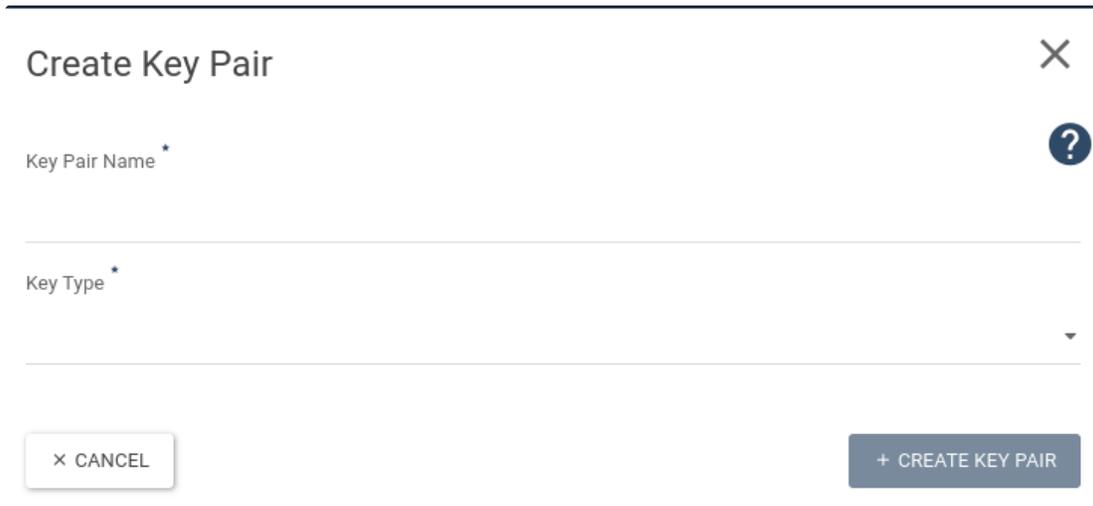
Click to download PuTTY

Creating Key Pair

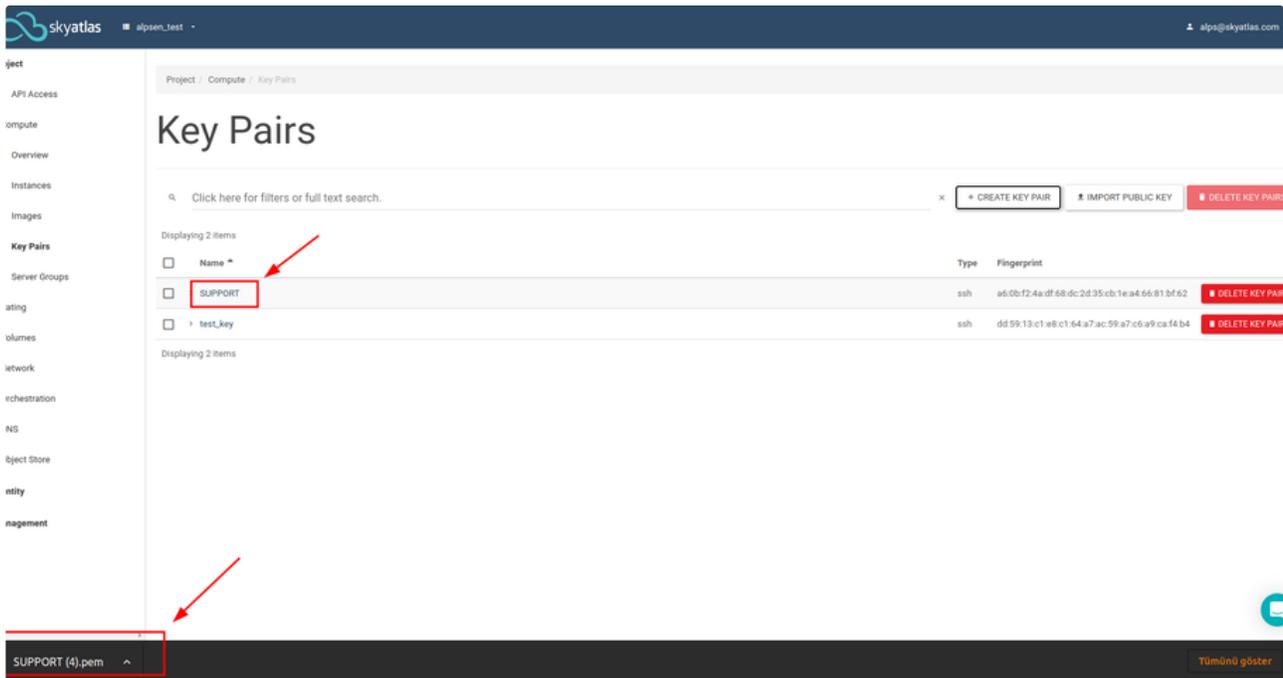
Open the page via Key Pairs menu located under the Compute heading at left of the panel. If there is any key created before it is listed here. In order to create new Key, click the Create Key Pair button.



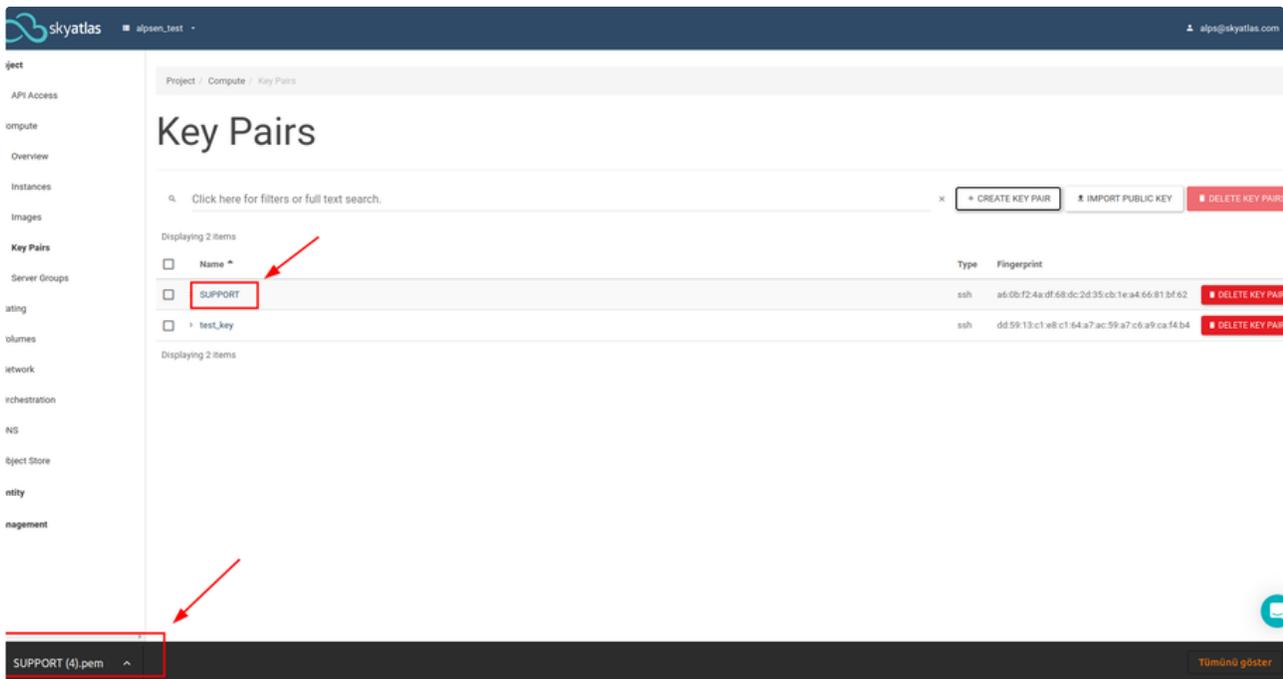
An appropriate name is given to the key that will be used for access to instances at the opened pop-up. Click the Create Key Pair button.

A screenshot of the 'Create Key Pair' dialog box. The dialog has a title bar with a close button (X) and a help button (?). It contains two input fields: 'Key Pair Name' and 'Key Type'. At the bottom, there are two buttons: 'CANCEL' and '+ CREATE KEY PAIR'.

After that, download the file that has .pem extension and has a name given for the key. Then downloaded file will be used to connect to instance via SSH.



Created Key is listed at the Key Pairs tab in the Key Pairs page

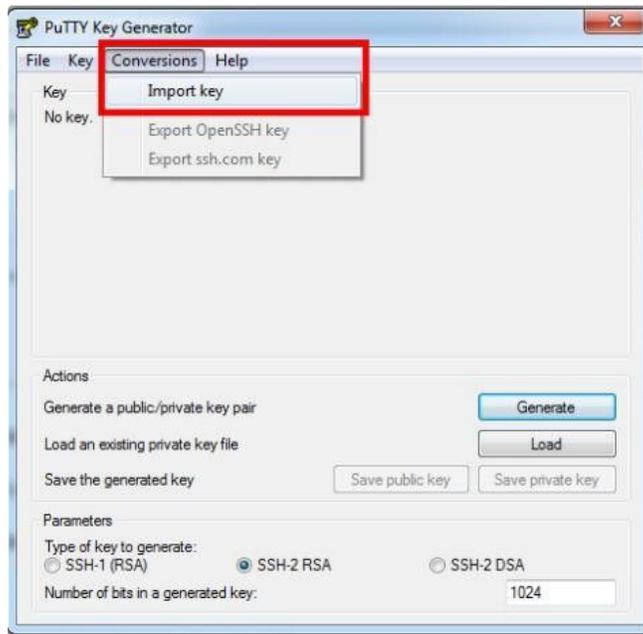


PuTTYgen

In order to add .pem extension file which is generated and downloaded via PuTTYgen panel to the PuTTY, it should be converted to .ppk extension file via PuTTYgen.

[Click to download PuTTYgen.](#)

.pem extension file downloaded from panel is imported to PuTTYgen as shown in screenshot.

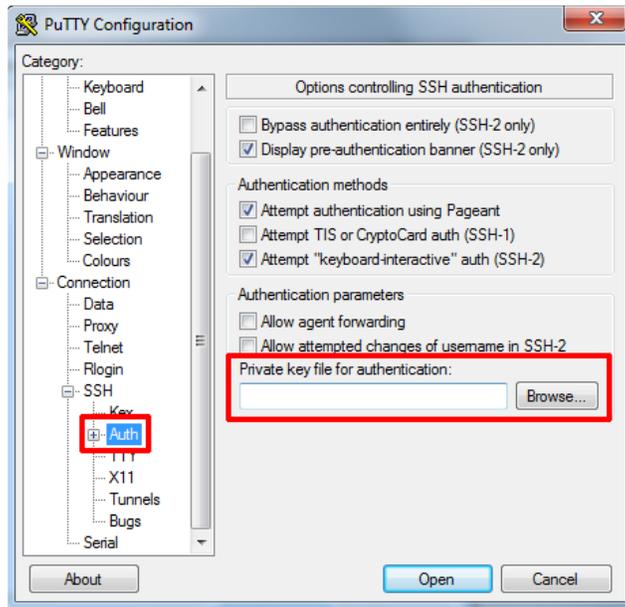


Afterwards a password that will be used to connect to Instance is entered to the **Key passphrase** and **Confirm passphrase** area as shown in screenshot.

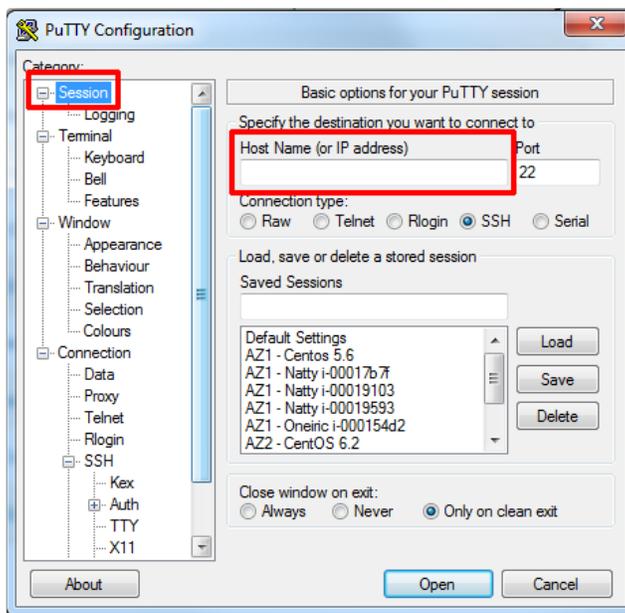
After password is entered click the **Save private key** button and save the .ppk extension file by giving name to it.



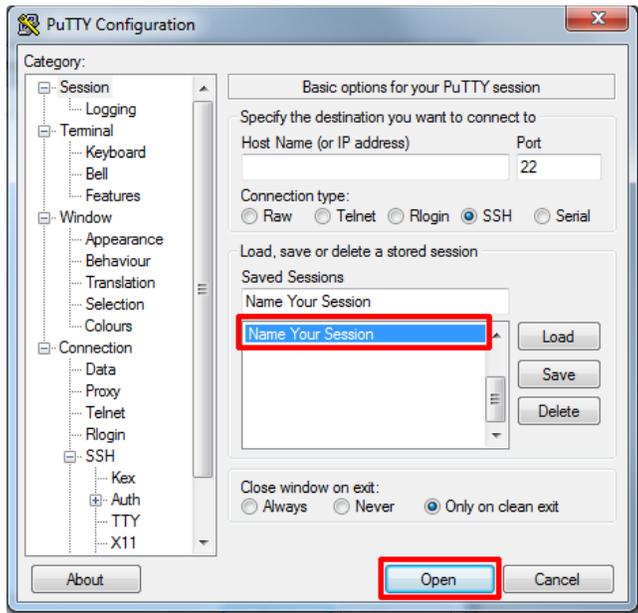
.ppk extension file is added by starting downloaded application PuTTY as shown in screenshot. After this step you can connect to Instance which has public IP defined via Windows.



In order to connect to Instance, public IP of the Instance is written to Host Name (or IP address) area as shown in screenshot and this registration is saved to be used in the future.

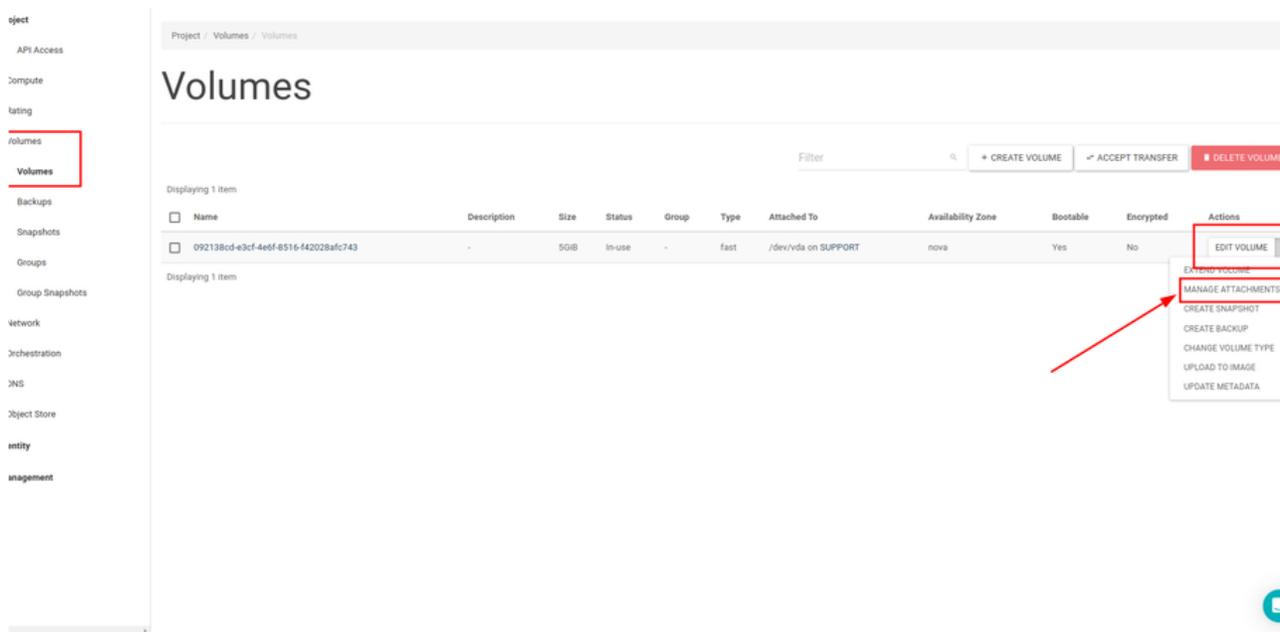


Open a console screen by clicking Open after selecting this registered session. Username information is entered according to image that Instance has via this console (**See:Instance ion (SSH)**) and after that register with passphrase that is given via PuTTYgen. After connection success, Instance is ready to use and access.



How to Attach Volume to Instance?

Before attaching volume to your instance, you should follow the instructions on pages [Launch Your First Instance](#) and [How to Create Volume?](#) .

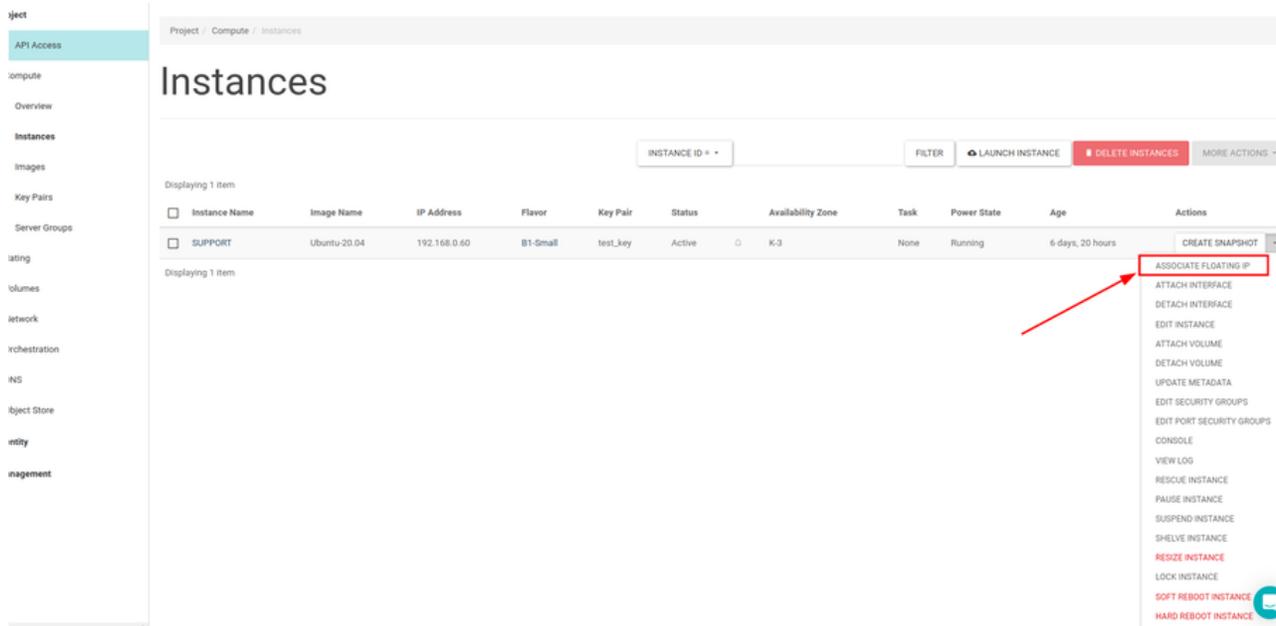


Then click on the Manage Attachments button on the Edit Volume button for the volume you created from the Volume tab. From the Manage Volume Attachments pop-up page that opens, you must select the server on which you want to add the volume and click the Attach Volume button.

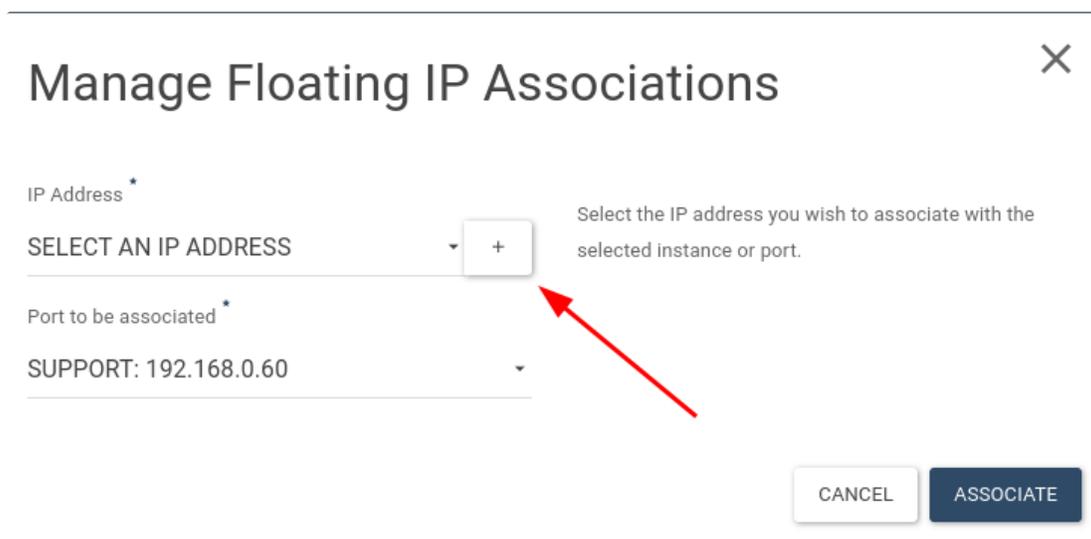
Adding IP Address to Server

To access an instance on the Internet we must be given first. a public IP address.

First the "Associate Floating IP" option is selected from the list at the end of the line belonging to the instance that will be public IP on the Instances page.



If there is no floating IP defined on your project when you click on Associate floating IP button, you can assign new floating IPs to your project by click the + button.



You see the floating_net pool is selected in the menu. You can add new IP by click the Allocate IP button.

Allocate Floating IP ×

Pool *
PUBLIC-FLOATING ▾

Description
|

DNS Domain

DNS Name

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

Project Quotas

Floating IP 1 of 50 Used

CANCEL ALLOCATE IP

You see the Instances IP information on the Instances page in the IP Address field.

Project / Compute / Instances

Instances

Displaying 1 item

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
<input type="checkbox"/> SUPPORT	Ubuntu-20.04	192.168.0.60, 213.14.226.17	B1-Small	test_key	Active	K-3	None	Running	6 days, 20 hours	<input type="button" value="CREATE SNAPSHOT"/>

Displaying 1 item

Unused IP addresses must be released from your project to avoid charging by the system.

By clicking on the Floating IPs tab under Network, you can list all the floating IPs your project has and delete the floating IP addresses that you don't use.

Project / Network / Floating IPs

Floating IPs

FLOATING IP ADDRESS = -

FILTER ALLOCATE IP TO PROJECT RELEASE FLOATING IP

Displaying 1 item

<input type="checkbox"/> IP Address	Description	DNS Name	DNS Domain	Mapped Fixed IP Address	Pool	Status	Actions
<input type="checkbox"/> 213.14.226.17				SUPPORT 192.168.0.60	public-floating	Active	DISASSOCIATE

Displaying 1 item