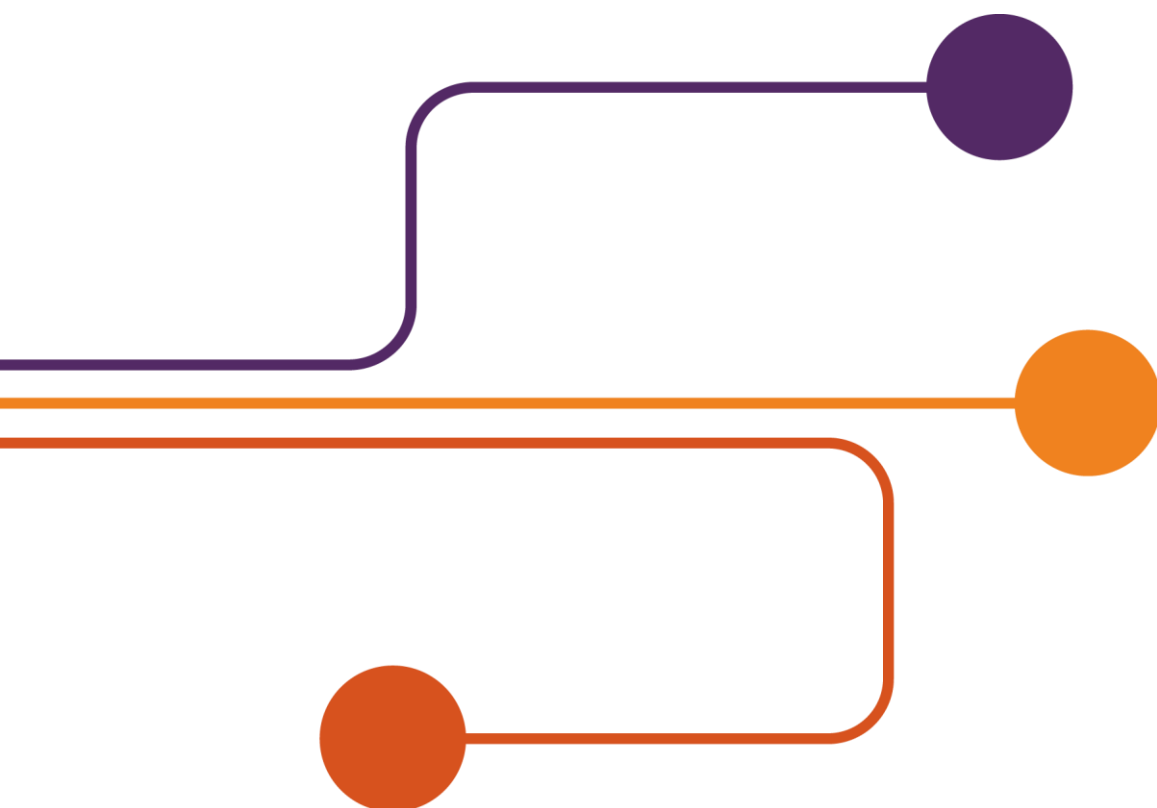


Przewodnik użytkownika  
Atman Cloud



**ATM S.A.**, ul. Grochowska 21a, 04-186 Warszawa

tel. 22 51 56 100, [info@atman.pl](mailto:info@atman.pl)

NIP: 113-00-59-989, KRS: 0000034947

(Sąd Rejonowy dla m.st. Warszawy, XIII Wydział KRS), REGON: 012677986, kapitał zakładowy: 34 526 176,80 zł w całości wpłacony

[www.atman.pl](http://www.atman.pl)

## Spis treści

Wstęp .....	3
Logowanie do panelu i zmiana hasła .....	3
Wolumeny (przestrzeń dyskowa) .....	5
Tworzenie wolumenu .....	5
Kasowanie wolumenu .....	7
Edycja wolumenu .....	7
Zmiana typu .....	7
Instancje (wirtualne maszyny) .....	8
Tworzenie instancji .....	8
Usuwanie instancji .....	14
Zmiana parametrów RAM i vCPU .....	14
Opis stanów instancji .....	15
Praktyczne uwagi .....	15
Obrazy .....	16
Tworzenie obrazu .....	16
Kasowanie obrazu .....	17
Praktyczne uwagi .....	17
Kopie migawkowe (snapshots) .....	17
Wykonanie kopii migawkowej instancji .....	17
Powrót instancji do stanu kopii migawkowej .....	18
Klucze SSH .....	18
Tworzenie pary kluczy SSH .....	18
Przygotowanie instancji do korzystania z klucza SSH .....	19
Użycie klucza do logowania .....	20
Hasło administratora do instancji .....	25
Router .....	27
Tworzenie routera .....	27
Dodanie interfejsu LAN .....	27
Usunięcie routera .....	28
Sieci wewnętrzne .....	30
Tworzenie sieci wewnętrznej .....	30
Edycja sieci i podsieci .....	32
Statyczne prywatne adresy IP, ręczne przydzielanie adresów .....	32
Praktyczne uwagi .....	33
Firewall .....	35

Utworzenie zapory ogniowej.....	35
Dodanie reguły do polityki.....	40
Usunięcie reguły z polityki.....	41
Usunięcie zapory ogniowej.....	42
Praktyczne uwagi.....	42
Grupy zabezpieczeń.....	42
Tworzenie grupy.....	42
Zmiana przypisania grupy do instancji.....	45
VPN.....	46
Adresy IP.....	46
Stałe publiczne.....	46
Pływające publiczne.....	47
Prywatne.....	48
API.....	49
Przygotowanie środowiska do korzystania z API.....	49
Szczegółowy opis przygotowania na przykładzie lokalnej maszyny Linux-Ubuntu.....	49
1. Instalacja środowiska python.....	49
2. Instalacja python-openstackclient.....	49
3. Konfiguracja python-openstackclient.....	49
Inne.....	51
Konwersja obrazów.....	51
Upload (import) pliku do chmury.....	53
Download (export) pliku z chmury.....	57
Utworzenie maszyny z własnego (zaimportowanego obrazu).....	58

## Wstęp.

Niniejszy dokument stanowi rozszerzenie dokumentu „Quick Start Guide” (w którym opisane jest krok po kroku przygotowanie do użytku jednej wirtualnej maszyny) i ma on charakter gruntownego opisu dostępnych dla użytkownika funkcjonalności. Poza możliwościami panelu Horizon opisane są także możliwości API, zwłaszcza w miejscach gdzie poprzez panel Horizon dana czynność nie jest możliwa do wykonania. Rozdziały przewodnika podzielone są tematycznie, według obszarów funkcjonalnych narzędzi dostępnych dla potrzeb użytkownika/administratora wirtualnej infrastruktury serwerowej.

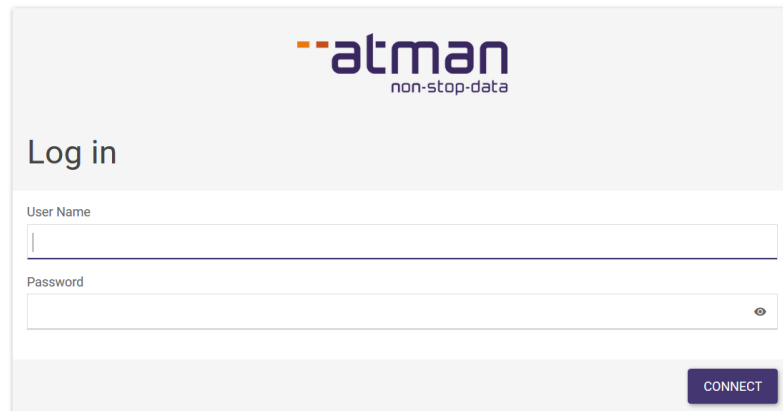
## Logowanie do panelu i zmiana hasła

### KROK 1

W oknie przeglądarki należy wpisać adres <https://panel.cloud.atman.pl>

### KROK 2

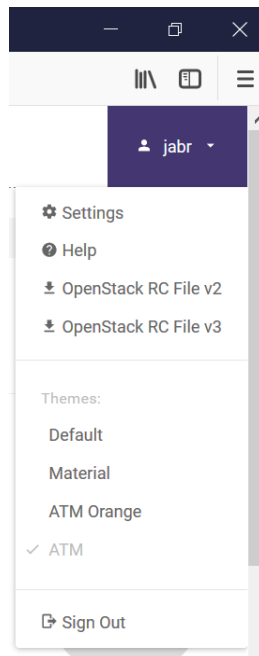
W formularzu logowania użytkownik podaje login oraz hasło, które otrzymał od Atmana.



The image shows a login form for the 'atman non-stop-data' system. At the top, the logo 'atman non-stop-data' is displayed. Below it, the text 'Log in' is centered. There are two input fields: 'User Name' and 'Password'. The 'Password' field has a small eye icon on the right side to toggle visibility. At the bottom right of the form, there is a blue button labeled 'CONNECT'.

### KROK 3

W prawym górnym rogu panelu należy rozwinąć listę klikając na nazwę użytkownika (tu: jabr), a następnie kliknąć Settings.



### KROK 4

W głównym menu panelu, po lewej stronie ekranu pojawi się na samym dole listy zakładka Settings, pod którą należy wybrać Change Password.

### KROK 5

W głównej części ekranu użytkownik dokonuje zmiany hasła, zatwierdzając zmianę przyciskiem Change.

Settings / Change Password

## Change Password

**Change Password**

Current password \*


New password \*

Confirm new password \*

**Description:**  
Change your password. We highly recommend you create a strong one.

**CHANGE**

Następuje automatyczne wylogowanie z konta z informacją o potrzebie zalogowania się przy użyciu nowego hasła:



## Log in

Password changed. Please log in again to continue.

User Name

Password

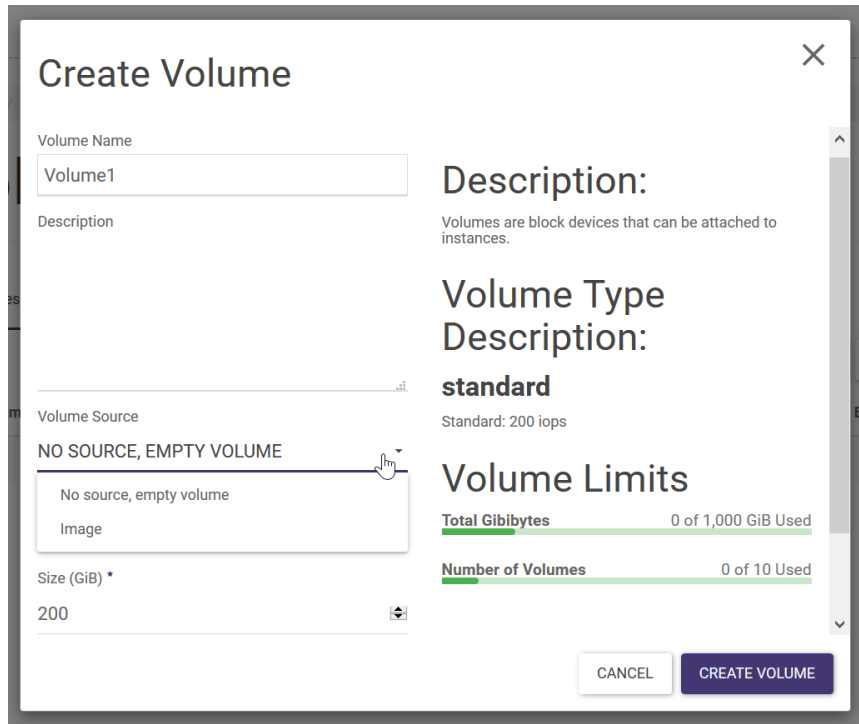
**CONNECT**

## Wolumeny (przestrzeń dyskowa)

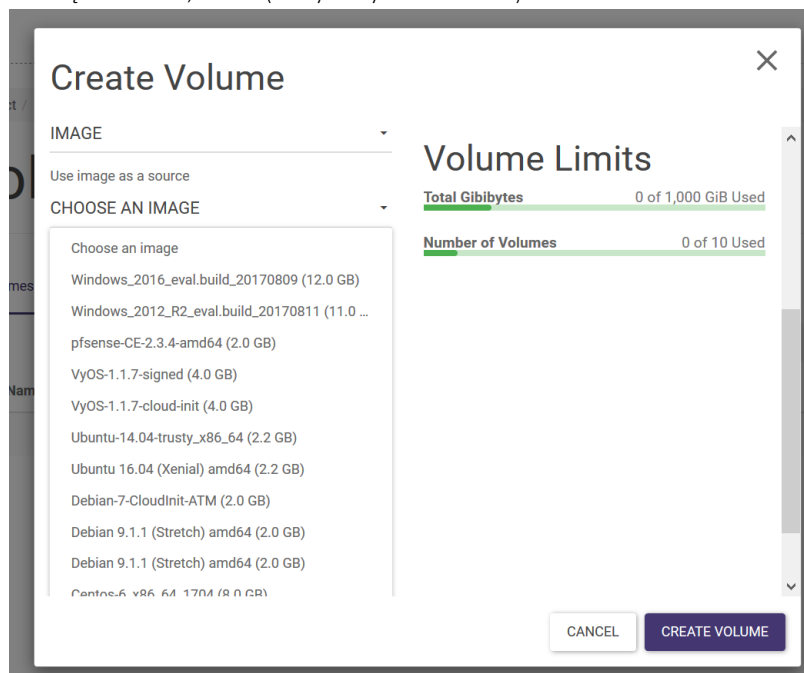
### Tworzenie wolumenu

#### KROK 1

Z głównego menu (lewa strona ekranu), należy rozwinąć Compute a następnie kliknąć Volumes. W centralnej części ekranu należy kliknąć +Create Volume. Pojawi się kreator:



Kolejno określamy w nim nazwę wolumenu, źródło (tu wybrany Linux Ubuntu)...



... a następnie rozmiar i typ. Zasoby przestrzeni dyskowej oferowane są przez Atmana w 2 wariantach: standardowy i szybki, różniące się wydajnością (iops – patrz: umowa, zamówienie). W zależności od zamówionej i udostępnionej przestrzeni Użytkownik określa tu pożądany typ przestrzeni:

Type

STANDARD

fast

standard

Availability Zone

NOVA

## KROK 2

Po kliknięciu przycisku Create Volume na liście wolumenów pojawi się nowo utworzony.

<input type="checkbox"/>	Name	Description	Size	Status	Type	Attached To	Availability Zone	Bootable	Encrypted	Actions
<input type="checkbox"/>	Volume1	-	10GiB	Available	standard		nova	Yes	No	EDIT VOLUME

## Kasowanie wolumenu

Na ekranie Project→Compute→Volumes po prawej stronie wolumenu należy wybrać akcję DELETE VOLUME. Można usunąć tylko wolumen, który nie jest przypisany do maszyny.

## Edycja wolumenu

Na ekranie Project→Compute→Volumes po prawej stronie wolumenu należy wybrać akcję EDIT VOLUME. Możliwa jest zmiana nazwy a także określenie flagi bootowalny dla danego wolumenu.

### Edit Volume

Volume Name

Description

**Description:**

Modify name and description of a volume.

The "Bootable" flag specifies that this volume can be used to launch an instance.

Bootable

## Zmiana typu

Można zmienić typ wolumenu (standard <-> fast) wybierając na ekranie Project→Compute→Volumes po prawej stronie wolumenu akcję CHANGE VOLUME TYPE. Zmiana może zająć znaczącą ilość czasu w zależności od rozmiaru wolumenu oraz rodzaju danych. Typ wolumenu można zmienić w przypadku gdy wolumen jest dodatkowy i nie podłączony do instancji. Typu wolumenu nie można zmienić dla:

- głównego wolumenu instancji
  - wolumenu dodatkowego, ale podłączonego do działającej instancji
- W kreatorze zmiany typu Migration Policy należy ustawić na wartość ON DEMAND

### Change Volume Type ✕

Volume Name \*

Type \*

FAST

Select a new volume type

standard

#### Description:

Change the volume type of a volume after its creation. This is equivalent to the `cinder retype` command.

The "Volume Type" selected must be different from the current volume type.

The "Migration Policy" is only used if the volume retype cannot be completed. If the "Migration Policy" is "On Demand", the back end will perform volume migration. Note that migration may take a significant amount of time to complete, in some cases hours.

CANCEL
CHANGE VOLUME TYPE

### Change Volume Type ✕

Volume Name \*

Type \*

FAST

Migration Policy

ON DEMAND

#### Description:

Change the volume type of a volume after its creation. This is equivalent to the `cinder retype` command.

The "Volume Type" selected must be different from the current volume type.

The "Migration Policy" is only used if the volume retype cannot be completed. If the "Migration Policy" is "On Demand", the back end will perform volume migration. Note that migration may take a significant amount of time to complete, in some cases hours.

CANCEL
CHANGE VOLUME TYPE

## Instancje (wirtualne maszyny)

### Tworzenie instancji

#### KROK 1

Z ekranu Project → Compute → Instances należy kliknąć LAUNCH INSTANCE.

Project / Compute / Instances

# Instances

INSTANCE ID = ▾

FILTER

🔍 LAUNCH INSTANCE

#### KROK 2

W zakładce Details należy podać nazwę instancji, a także określić ile sztuk takich instancji ma zostać wykreowanych. Dodatkowo można ograniczyć występowanie/działanie instancji do konkretnej strefy dostępności, tzw. Availability Zone (więcej: patrz praktyczne uwagi).



### 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.

Instance Name \*

Availability Zone

Any Availability Zone

Count \*

1

Total Instances (10 Max)

10%

0 Current Usage  
1 Added  
9 Remaining

← BACK    NEXT →    LAUNCH INSTANCE

#### Availability Zone

Any Availability Zone

Any Availability Zone

AZ3

AZ2

AZ1

#### KROK 3

W zakładce Source należy wybrać źródło bootowania. Wybór wartości Image pozwala na szybkie uruchomienie maszyny w jednym etapie używając tylko omawianego tu kreatora. Wybór wartości Volume jest bardziej uniwersalnym sposobem, wymaga on jednak uprzedniego utworzenia wolumenu. Patrz również praktyczne uwagi. Warto również zaznaczyć opcję NO przy „Delete Volume ...”, dzięki temu po usunięciu instancji wolumen będzie można ponownie wykorzystać. W przypadku wybrania Image jako źródła bootowania, w sekcji Available należy wybrać obraz systemu poprzez kliknięcie przycisku ze strzałką skierowaną w górę.

### Launch Instance

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

Image

Instance Snapshot

Volume

Volume Snapshot

Create New Volume

YES

Delete Volume on Instance Delete

YES NO

Allocated

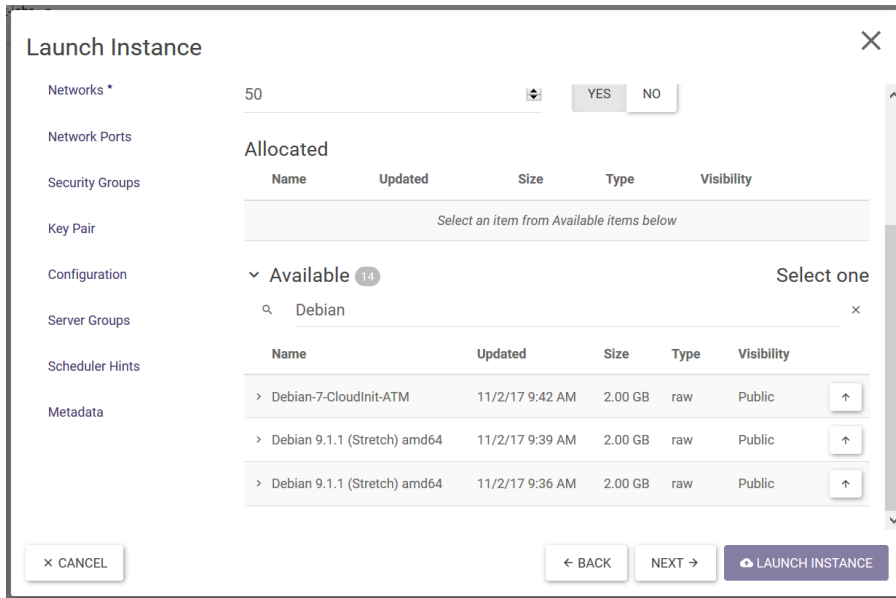
Name	Updated	Size	Type	Visibility
Select an item from Available items below				

Available 14

Select one

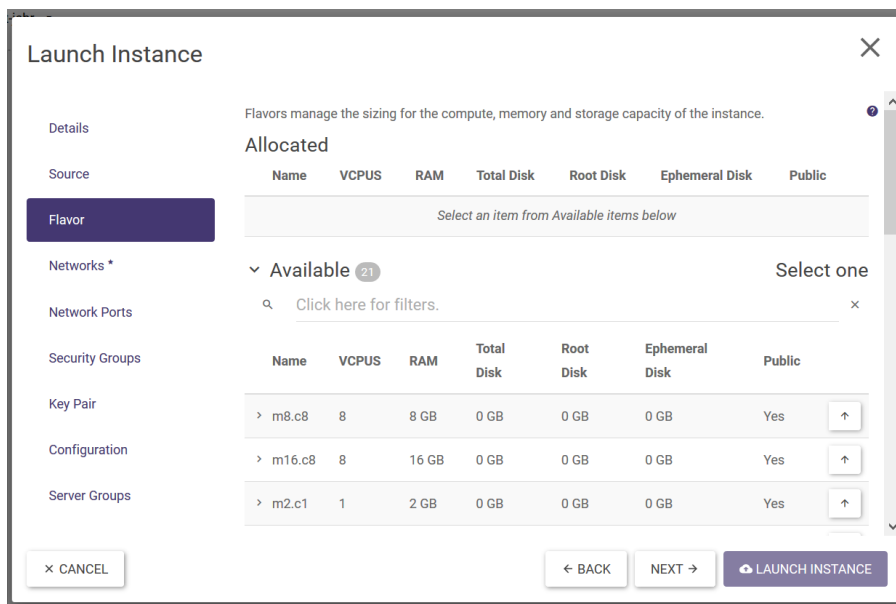
Click here for filters.

← BACK    NEXT →    LAUNCH INSTANCE



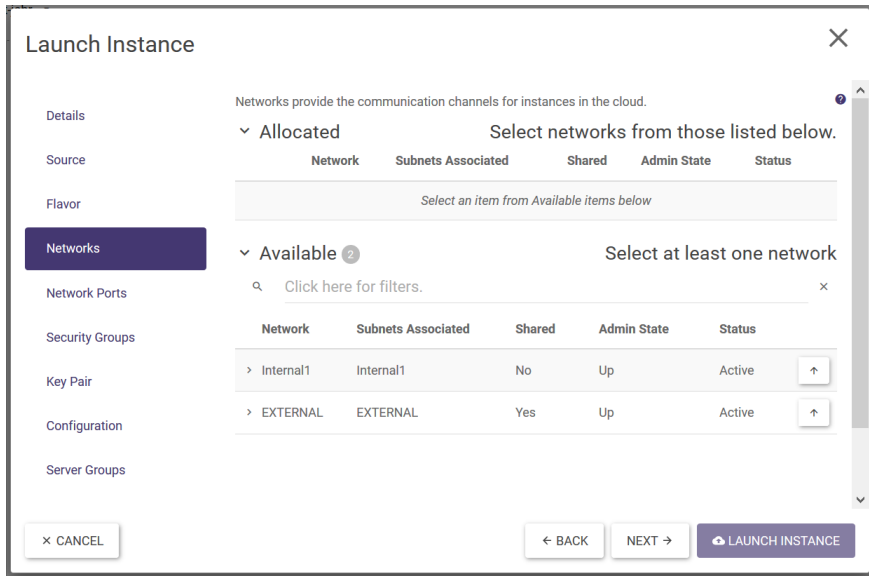
#### KROK 4

W zakładce Flavors należy wybrać (poprzez kliknięcie przycisku z symbolem strzałki w górę) flavor – czyli kombinację liczby vCPU (rdzeni) oraz ilości pamięci operacyjnej RAM.



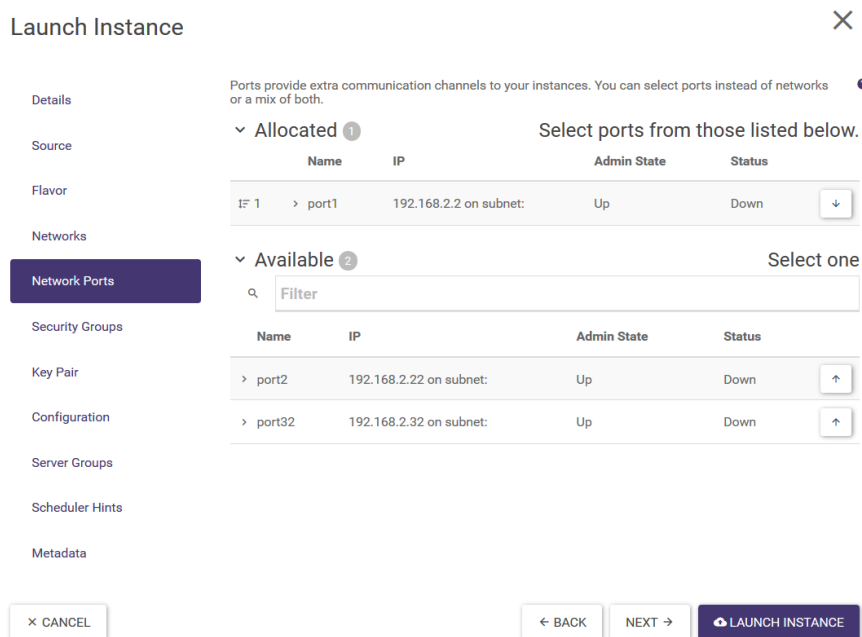
#### KROK 5

W zakładce Networks można przypisać (poprzez kliknięcie przycisku z symbolem strzałki w górę) sieć.



### KROK 6

W zakładce Network Ports można przypisać port (poprzez kliknięcie przycisku z symbolem strzałki w górę). Aby pomyślnie zakończyć tworzenie instancji, jedna z zakładek sieciowych musi zostać uzupełniona: Networks lub Network Ports.



### KROK 7

W zakładce Security Groups należy wybrać pożądaną grupę zabezpieczeń. Domyślny stan zakładki:

## Launch Instance



- Details
- Source
- Flavor
- Networks
- Network Ports
- Security Groups
- Key Pair
- Configuration

Select the security groups to launch the instance in.

▼ **Allocated** 1

Name	Description	
> default	Default security group	↓

▼ **Available** 2 Select one or more

🔍  ×

Name	Description	
> AllOpen		↑
> AllowSSH		↑

× CANCEL

← BACK

NEXT →

▶ LAUNCH INSTANCE

Używając przycisków z symbolami strzałek należy przypisać pożądaną grupę zabezpieczeń:

## Launch Instance



- Details
- Source
- Flavor
- Networks
- Network Ports
- Security Groups
- Key Pair
- Configuration

Select the security groups to launch the instance in.

▼ **Allocated** 1

Name	Description	
> AllowSSH		↓

▼ **Available** 2 Select one or more

🔍  ×

Name	Description	
> AllOpen		↑
> default	Default security group	↑

× CANCEL

← BACK

NEXT →

▶ LAUNCH INSTANCE

## Launch Instance



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

Select the security groups to launch the instance in.

▼ Allocated 1

Name	Description	
> default	Default security group	↓

▼ Available 2 Select one or more

🔍  ×

Name	Description	
> AllOpen		↑
> AllowSSH		↑

× CANCEL

← BACK

NEXT →

🔒 LAUNCH INSTANCE

### KROK 8

W zakładce Key Pair można ustawić klucze SSH, jeśli życzeniem użytkownika jest logowanie do instancji w ten sposób. Należy wybrać wcześniej stworzony klucz lub utworzyć go uruchamiając +CREATE KEY PAIR lub też importując swój własny klucz (IMPORT KEY PAIR).

## Launch Instance

×

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	
> KP-Deb1	9d.f6.bd:8e:be:fb:1a:07:0f:bf:43:68:a2:6a:54:9d	↓

**Available** 0 Select one

🔍  ×

× CANCEL

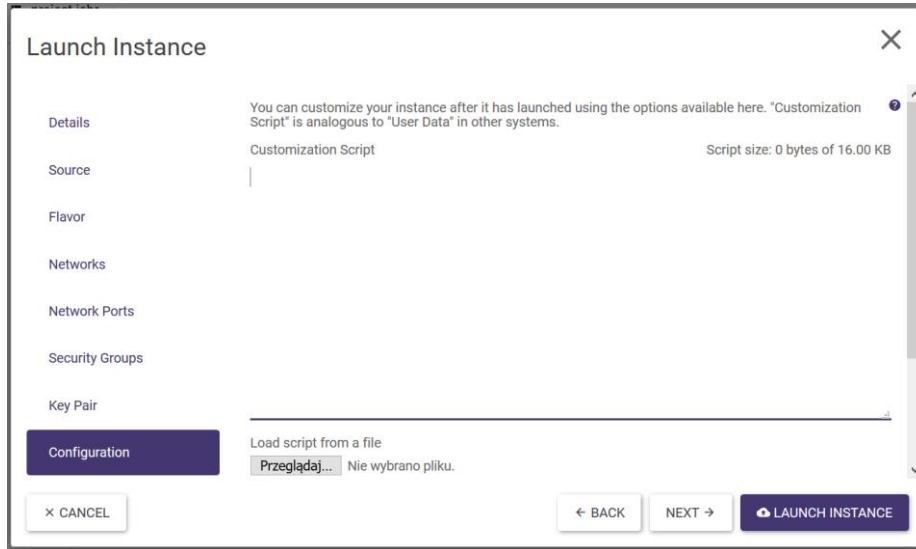
← BACK

NEXT →

🔒 LAUNCH INSTANCE

### KROK 9

Zakładka Configuration daje możliwość customizacji skryptem. Jedno z praktycznych zastosowań polega na ustawieniu hasła dla domyślnego użytkownika (patrz: praktyczne uwagi).



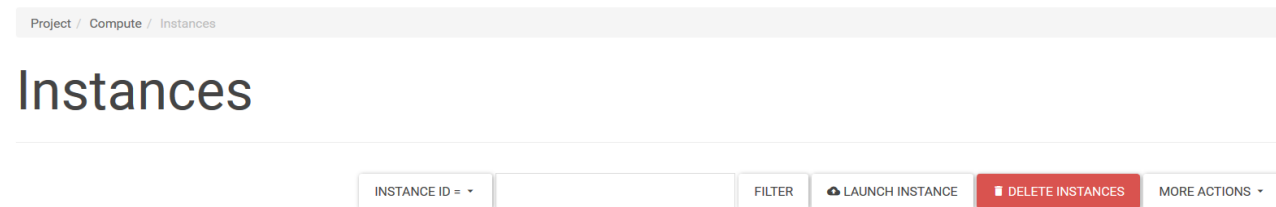
#### KROK 10

Zakładki Server Groups, Scheduler Hints oraz Metadata niniejszy przewodnik zostawia do samodzielnej eksploracji bardzo zaawansowanym użytkownikom. Można je pominąć podczas tworzenia instancji. Instancja zostaje wykreowana po kliknięciu na przycisk Launch Instance i pojawia się na liście ekranu Instances.

<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"/>	Ubu1	-	195.167.156.60	m8.c8	-	Active	AZ1	None	Running	1 week	CREATE SNAPSHOT -

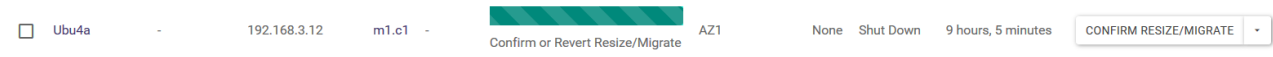
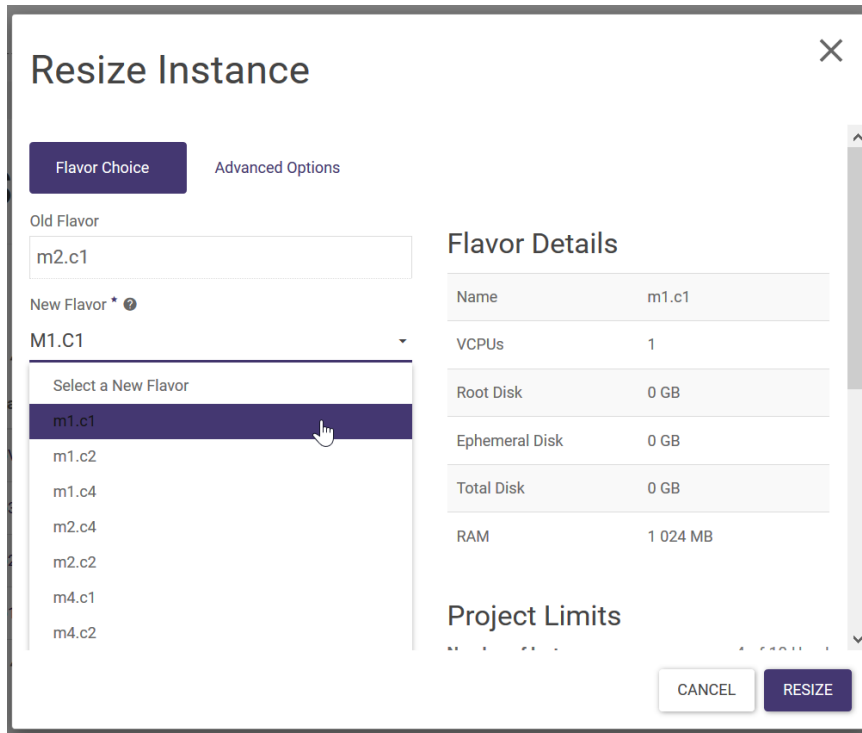
## Usuwanie instancji

Instancję można usunąć uruchamiając akcję DELETE INSTANCE na wybranej instancji na liście ekranu Project → Compute → Instances. Większą liczbę instancji można usunąć zaznaczając instancje przeznaczone do usunięcia na liście a następnie kliknięcie przycisku DELETE INSTANCES.



## Zmiana parametrów RAM i vCPU

Parametry można zmienić poprzez zmianę flavor'a. Na ekranie Project → Compute → Instances należy wybrać akcję RESIZE INSTANCE. W kreatorze należy wybrać nowy flavor i zatwierdzić przyciskiem RESIZE. Na liście instancji w polu TASK pojawi się pasek stanu z informacją o zadaniu. Po wykonaniu należy kliknąć CONFIRM RESIZE/MIGRATE.



## Opis stanów instancji

Na liście instancji po prawej stronie ekranu Project → Compute → Instances użytkownik ma możliwość wykonania szeregu akcji dotyczących ich stanu. Poniższy opis przedstawia znaczenie stanów.

AKCJA	OPIS
PAUSE INSTANCE	Stan maszyny zapisywany jest w pamięci RAM. Instancja staje się nieaktywna.
SUSPEND INSTANCE	Wejście w stan podobny do hibernacji – stan instancji wraz z pamięcią zapisywany jest na dysku, RAM i rdzenie zostają zwolnione – można zaalokować do innych instancji. Instancja zostaje wyłączona.
RESUME INSTANCE	Powrót do stanu sprzed akcji SUSPEND lub PAUSE.
SHELVE INSTANCE	Instancja zostaje wyłączona, zasoby zwolnione. Stan instancji nie jest zapisywany.
UNSHelve INSTANCE	Tworzy i bootuje instancję od nowa.
LOCK INSTANCE	Instancja jest zabezpieczona przed usunięciem.
UNLOCK INSTANCE	Instancja jest podatna na usunięcie.
SOFT / HARD REBOOT	Ponowne uruchomienie instancji.
SHUT OFF INSTANCE	Wyłączenie instancji.
START INSTANCE	Włączenie instancji.

## Praktyczne uwagi

### UWAGA 1. Autogenerowanie hasła root.

Hasło administratora generowane jest automatycznie. Aby hasło zostało nadane i było widoczne w logach instancji należy pamiętać, że w przypadku używania sieci wewnętrznej, musi być włączone DHCP – patrz również rozdział „Sieci wewnętrzne”.

### UWAGA 2. Strefy dostępności.

© ATM S.A.	Szablon	Strona
Atman Cloud. Quick Start Guide.	wersja 2.0	15 z 60
Wszystkie prawa zastrzeżone. Ujawnianie niniejszego dokumentu stronom trzecim bez pisemnej zgody ATM S.A. jest zabronione.		

Platforma chmurowa w zakresie węzłów obliczeniowych podzielona jest na trzy strefy (AZ – Availability Zones). Każda strefa stanowi osobną grupę szaf węzłów (fizycznych serwerów). Ograniczając instancję do danej strefy użytkownik ma pewność, że instancja (wirtualna maszyna) nie znajdzie się w innej strefie. Taka funkcjonalność umożliwia użytkownikowi – jeśli jest to potrzebne – dodatkową separację od siebie grup instancji.

UWAGA 3. Źródło bootowania.

Wybór wartości Image w źródle bootowania domyślnie stosuje typ przestrzeni dyskowej STANDARD. Jeśli użytkownik potrzebuje uruchomić instancję z dyskiem systemowym o typie FAST, powinien uprzednio utworzyć wolumen. Wybór wartości Volume jest bardziej uniwersalnym sposobem – na etapie tworzenia wolumenu można jawnie określić typ: STANDARD lub FAST.

UWAGA 4. Customization Script.

Dla systemów operacyjnych linux można w łatwy sposób wygenerować przy tworzeniu maszyny samodzielnie określone hasło dla domyślnego użytkownika. W przypadku systemu Linux Ubuntu domyślnym użytkownikiem jest ubuntu, dla systemu Linux CentOS – użytkownik centos. W polu Customization Script należy wpisać:

```
#cloud-config
password: mysecret
chpasswd: { expire: False }
ssh_pwauth: True
```

W przypadku systemu Linux Debian należy takiego użytkownika stworzyć – tu: debian. W polu Customization Script należy wpisać:

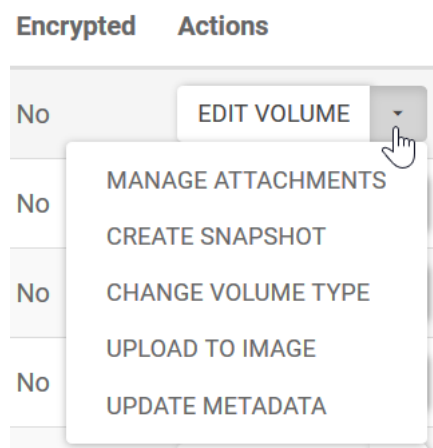
```
#cloud-config
password: mysecret
ssh_pwauth: True
chpasswd: { expire: False }
system_info:
  default_user:
    name: debian
    lock_passwd: true
  sudo: ["ALL=(ALL) NOPASSWD:ALL"]
  shell: /bin/bash
```

## Obrazy

### Tworzenie obrazu

KROK 1

Z ekranu Project → Compute → Volumes z akcji dla wybranego wolumenu należy wybrać UPLOAD TO IMAGE:



KROK 2

W kreatorze należy wpisać nazwę obrazu i potwierdzić tworzenie przyciskiem UPLOAD.



## Upload Volume to Image ✕

Volume Name \*

Image Name \*

Disk Format

RAW ▾

Force

### Description:

Upload the volume to the Image Service as an image. This is equivalent to the `cinder upload-to-image` command.

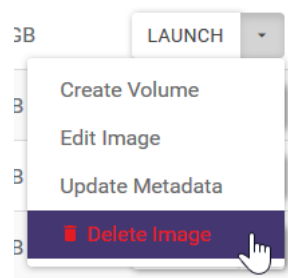
Choose "Disk Format" for the image. The volume images are created with the QEMU disk image utility.

When the volume status is "in-use", you can use "Force" to upload the volume to an image.

CANCEL
UPLOAD

## Kasowanie obrazu

Z ekranu Project → Compute → Images z prawej strony w akcji dla wybranego obrazu należy wybrać Delete Image:



## Praktyczne uwagi

### UWAGA 1

Nie można usunąć obrazu z ustawieniami PROTECTED = YES (tę wartość można zmienić na NO edytując obraz → akcja Edit Image).

### UWAGA 2

Nie można usunąć obrazu z ustawieniami VISIBILITY = PUBLIC.

### UWAGA 3

Tworzenie obrazów działa tylko dla wolumenów nieprzyjętych do instancji.

## Kopie migawkowe (snapshots)

### Wykonanie kopii migawkowej instancji

#### KROK 1

Z ekranu Project → Compute → Instances na liście akcji należy kliknąć CREATE SNAPSHOT. Pojawi się okno, w którym należy podać nazwę którą chcemy nadać kopii.

## Create Snapshot ×


Snapshot Name \*

Ubu4b-01.01.2016.12h38m

### Description:

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

CANCEL

CREATE SNAPSHOT 

#### KROK 2

Po kliknięciu CREATE SNAPSHOT zostanie utworzona kopia migawkowa, która od razu pojawia się na liście Project → Compute → Images

### Powrót instancji do stanu kopii migawkowej

Nie można bezpośrednio odtworzyć (cofnąć) bieżącego stanu instancji do stanu kopii migawkowej. Można natomiast z kopii migawkowej utworzyć kolejną maszynę. Tworzenie polega na uruchomieniu kreatora tworzenia instancji:

a) z ekranu Project → Compute → Instances przyciskiem LAUNCH INSTANCE

lub

b) z ekranu Project → Compute → Images przyciskiem LAUNCH po prawej stronie dla wybranego obrazu – kopii migawkowej

W przypadku sposobu (a) należy pamiętać o wybraniu odpowiedniego źródła source boot, które z kolei dla ścieżki (b) automatycznie jest ustawiane:

## Launch Instance ×

Details

Source

Flavor

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

Volume Snapshot

Delete Volume on Instance Delete

YES

NO

## Klucze SSH

### Tworzenie pary kluczy SSH

#### KROK 1

Na ekranie Project → Key Pairs należy kliknąć przycisk CREATE KEY PAIR (alternatywnie: można zaimportować stworzony przez siebie lokalnie klucz publiczny – przycisk IMPORT KEY PAIR):

## Create Key Pair ✕

Key Pair Name \*

Key pairs are SSH credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

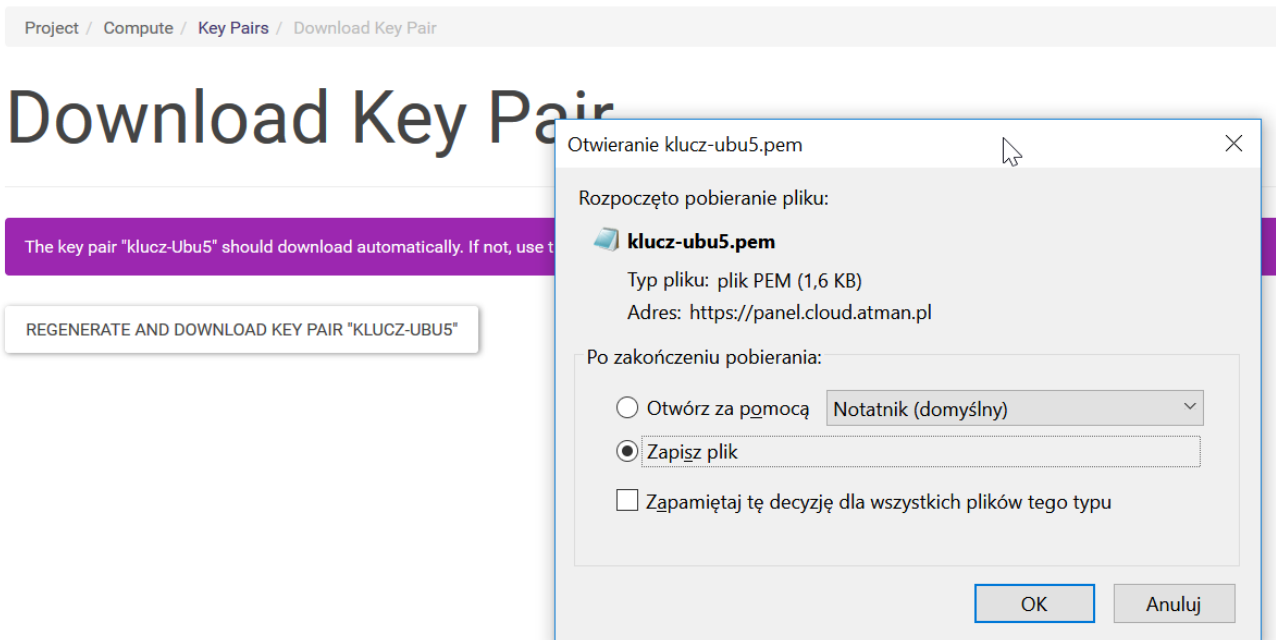
Protect and use the key as you would any normal SSH private key.

CANCEL

CREATE KEY PAIR

### KROK 2

Po potwierdzeniu przyciskiem CREATE KEY PAIR, pojawi się okno pobierania klucza prywatnego który należy zapisać na lokalnej maszynie:



### Przygotowanie instancji do korzystania z klucza SSH

W kreatorze tworzenia instancji w zakładce Key Pair należy wybrać klucz który chcemy zastosować dla tej maszyny – używając przycisków z symbolem strzałek. Widać również że poprzednio wykonany krok można również wykonać w kreatorze:

## 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 1 item

Name	Fingerprint
> klucz-Ubu5	06:a5:ec:34:d0:94:f5:85:96:55:d8:80:af:13:c5:a8

Displaying 1 item

### Available 2

Select one

Displaying 2 items

Name	Fingerprint
> KP-Cent3	69:ec:9a:69:8e:85:ef:fb:9b:18:c1:2c:68:93:da:de
> KP-Deb1	9d:f6:bd:8e:be:fb:1a:07:0f:bf:43:68:a2:6a:54:9d

× CANCEL
← BACK
NEXT →
LAUNCH INSTANCE

## Użycie klucza do logowania

### KROK 1

Na liście instancji ekranu Project → Compute → Instances przy utworzonej instancji pojawi się również informacja o stosowanym kluczu:

Displaying 7 items

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Time since created
<input type="checkbox"/>	Ubu5	-	195.167.156.24	m1.c1	klucz-Ubu5	Active	AZ2	None	Running	0 minutes

### KROK 2

Dla systemów Linux:

Przejdźcie do katalogu .ssh lokalnej maszyny i zapisanie/utworzenie/skopiowanie do niej prywatnego klucza (tu nazwa pliku to klucz-Ubu5-priv.pem)

```
ubuntu@ubu1: ~/ssh
```

```
ubuntu@ubu1:~$ cd .ssh/
ubuntu@ubu1:~/ssh$ cat klucz-Ubu5-priv.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAYlDrgqtRyYZkzIrlMXXok+R4slynKyB6H1NjrB1RW+zq4Gk
jUy/hRKRnKfTQnelLhPPTIcVPASz0ZuxCFFncf/7OuUo6EPhhrLXMwdZjTTB1z0L
Zm0nNyb4aioC07XLVxFgMIpPkzCntmWLalQRu3ljWP5xehxETYz1nd+Th0v1ZKa8
727MjDwE7nXZXsj4Gw+PfmQVqavxo3l9jvGcq3YWyt+qSQbKwW0/I6xdGv3e8Wnj
L8pLqVVb2nLPSid7Z4W90j72QainwOqGt5t/ddLlonWdhw9TToixOKGdHVDiL5bf
QQIp8pCkrIK9m458+LWqsgreQ8y4R5Yq02SerQIDAQABAoIBAAvZ2M8TQHRA8yf4
wgyTuI+WBjgR0Z0isLatmQTcttt4o3SSP8g97d+OX+Hf8fYInhFgCFMsdHvMh1fu
zIKCVQu74tvzKPy47j4ImaEhYRBwOrSWXfMapkOjIPEdNHeQecjWdQnJUrsPHoov
7BJHj5ilrsJWnxwpSXwPxYAj81L+dXF0ext/7CDK9uInAcqx87BERLcPRMoz1zMp
GzPHXk+RpwDSsFpO3Jy/ZRCv/06vAXihJ6NjuWj5/zBNF5+O8QV5iant46GSNN8
PcykioxwTAiBwnE7tAY42P7RflQ2FyJT9pX6fLgFtwvY67vFP3+EwGRMX88MNXqX
C6QqkiECgYEA59w3QiBVQqWw0//sgcvRD2y+1NLYMm1DqAi9NF+FbhEISYT4R9q6
VxDNCPnC3CLyHgVnZ6BKdy6W9DL7KRKIdjDHABMzk7Y+y0nBqBPJwll10z9vH1r5
eM0w73vU6jgXcy4gU18bDHojeaBMTAZdma8TpILOJp9wz51Pl216BYkCgYEA3Woq
1QjvIMGnkaBZdzB5PRMGkU9XBMhx+jyGU05Rq6p+SedWSVBGkwvoVmoW+uA6zjta
T17kk9rTBenJfAC6K0rNVv+FKuzaUvofEXo4gmq1cbbQGd7OczwxovUmQLJM+dnt
/wnjPD0bdzjlw9Ry1iZA7mK+OmZsZhFJ7nfQqWUCgYEA0YzvCD2usRiM812nBDwQ
C2/OHQ0eRp0H+7NCRtZbonmUUtXxiwd9SDkwBf+thEW1KzrZFQgCpSqfVb9JzfpA
iK9W+5NfFw4sPJDBjMWtoJAmyCPZqsawF9xNanQxnynoz7mNjstT7nfo3gDpVACg
0cgw6YsrBC8vxwQ3LfxMxXkCgYEAAtX6md5RoOAil7EhtrbhtWrPyyUApC4GndEES
tszXQ4lxFffsmJIWF81F/TffeGw/p/edErytT8mq+bPmViBeeshJQ8wWg9Y9LJFc
0D3Ifpocr/nely99wiani6NRdM+E0GgabAVlAjItmrTbVmM3YCFS5Gu+UEVkn+Cip
2rEaOmUCgYEAh32lrWeRen3KbZJ/VQ8mjnbzodc+157TQS8ttoomr5smjZPLpRs
4nalqWLZI6W/naUavou7VO2IULOTs9HSpwKkePZ7evivXNKGP55j6gB/Jd2VwX0H
Ej+mQ2UmdlKSeYCdW0VwSrJrk23HYnnGy8u5b+L4hmR8QWxSSqAh/g=
-----END RSA PRIVATE KEY-----

ubuntu@ubu1:~/ssh$
```

Następnie zmiana uprawnień:

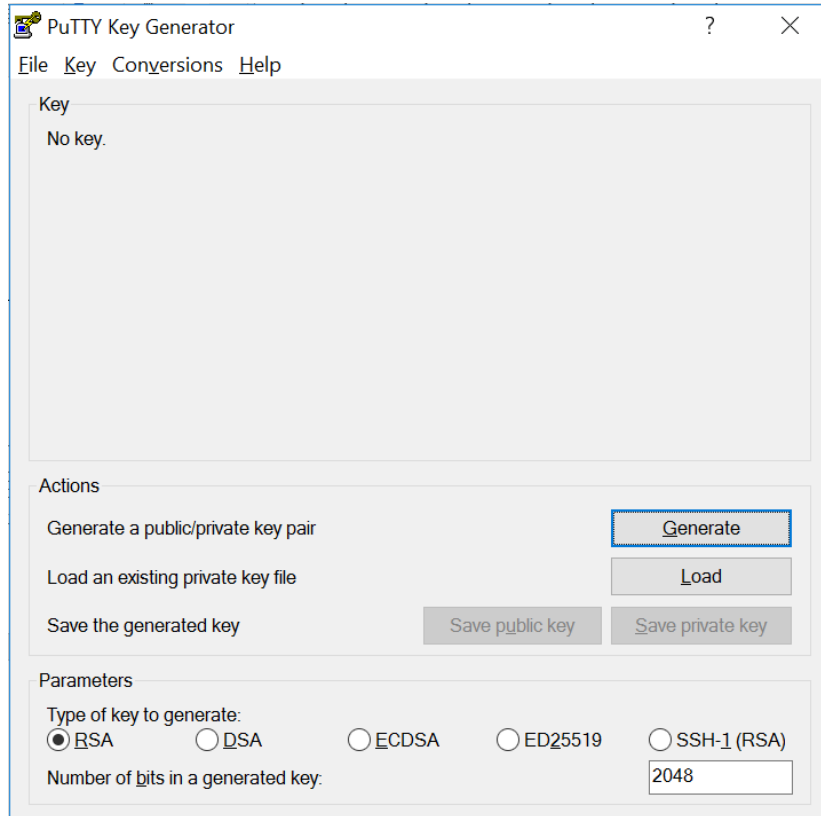
```
ubuntu@ubu1: ~/ssh
```

```
ubuntu@ubu1:~/ssh$ chmod 600 klucz-Ubu5-priv.pem
ubuntu@ubu1:~/ssh$ ls -hall klucz-Ubu5-priv.pem
-rw----- 1 ubuntu ubuntu 1.7K Dec 11 12:21 klucz-Ubu5-priv.pem
ubuntu@ubu1:~/ssh$
```

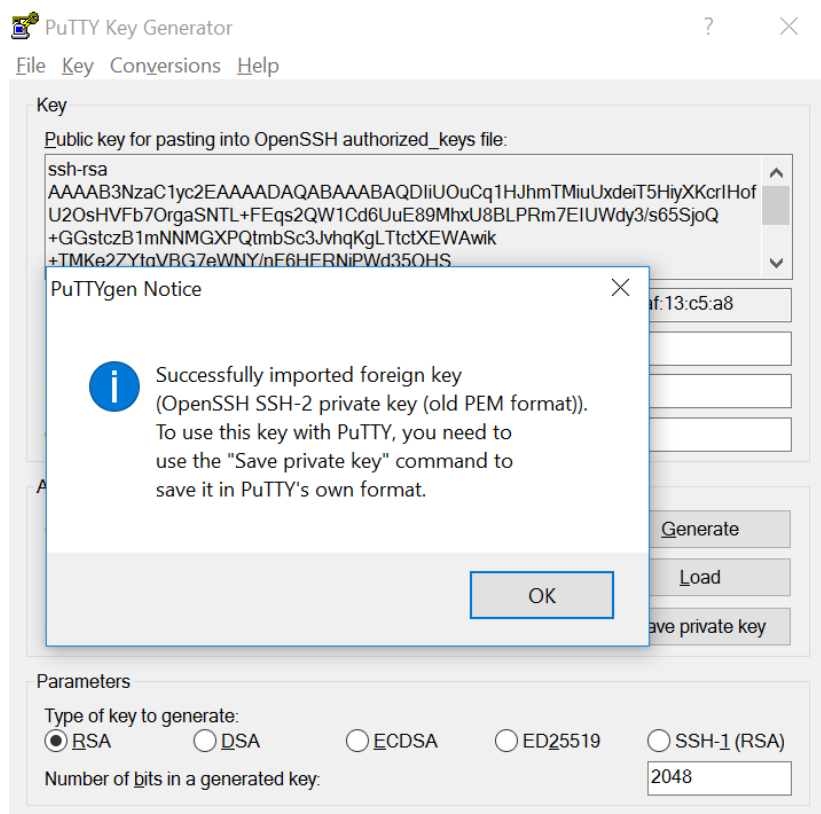
Dla systemów Windows:

Najpopularniejszym narzędziem jest Putty w którym uprzednio należy przekonwertować plik z formatu pem na ppk.

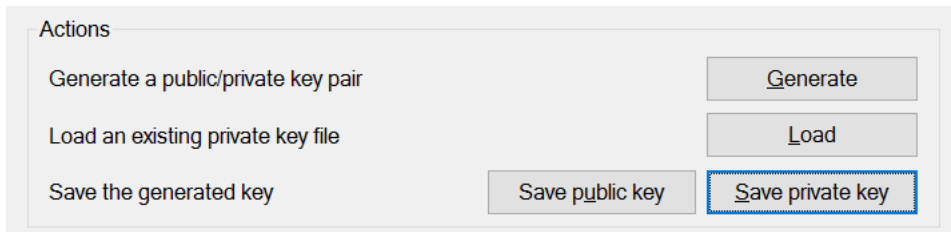
Należy uruchomić program PUTTYGEN.EXE:



załadować (przycisk Load → wybór prywatnego klucza – w tym przykładzie: klucz-Ubu5-priv.pem)



Z poziomu tego samego okna PUTTYGEN zapisać klucz jako ppk przyciskiem „Save private key”




### KROK 3

Logowanie.

Dla systemów Linux:

Przy pomocy polecenia `ssh -i <plik-klucza> <uzytkownik>@<adres ip>` logujemy się do maszyny

 ubuntu@ubu5: ~

```
ubuntu@ubu1:~/.ssh$ ssh -i klucz-Ubu5-priv.pem ubuntu@195.167.156.24
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-89-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
  http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

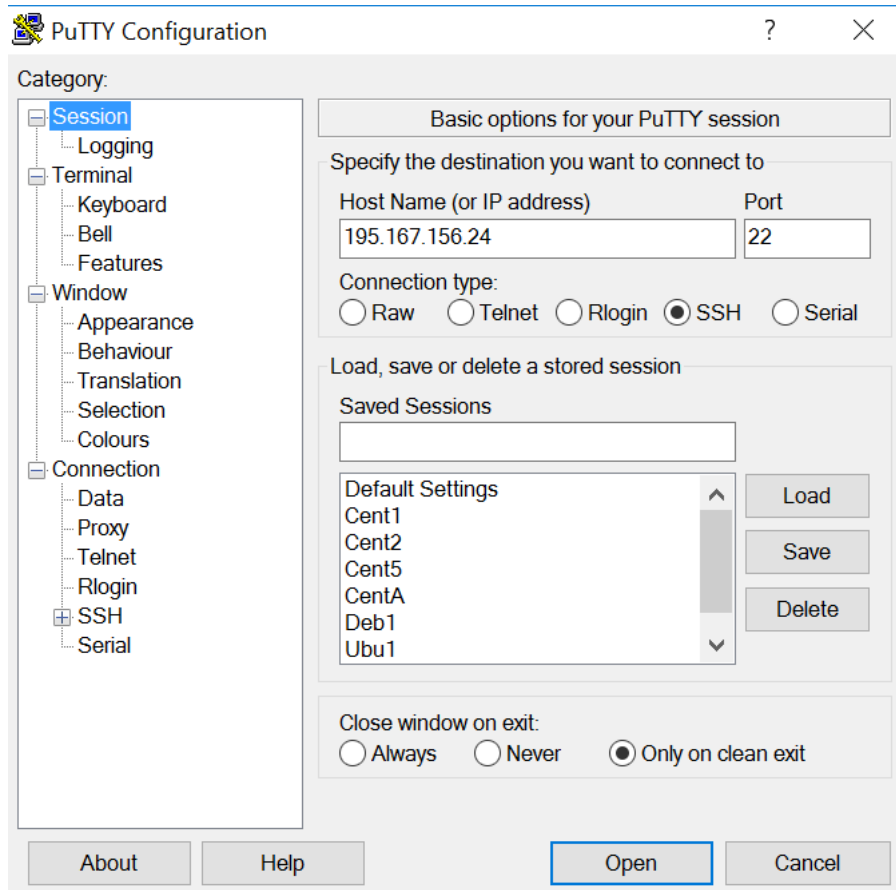
Last login: Mon Dec 11 12:23:44 2017 from 195.167.156.60
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubu5:~$ █
```

Dla systemów Windows:

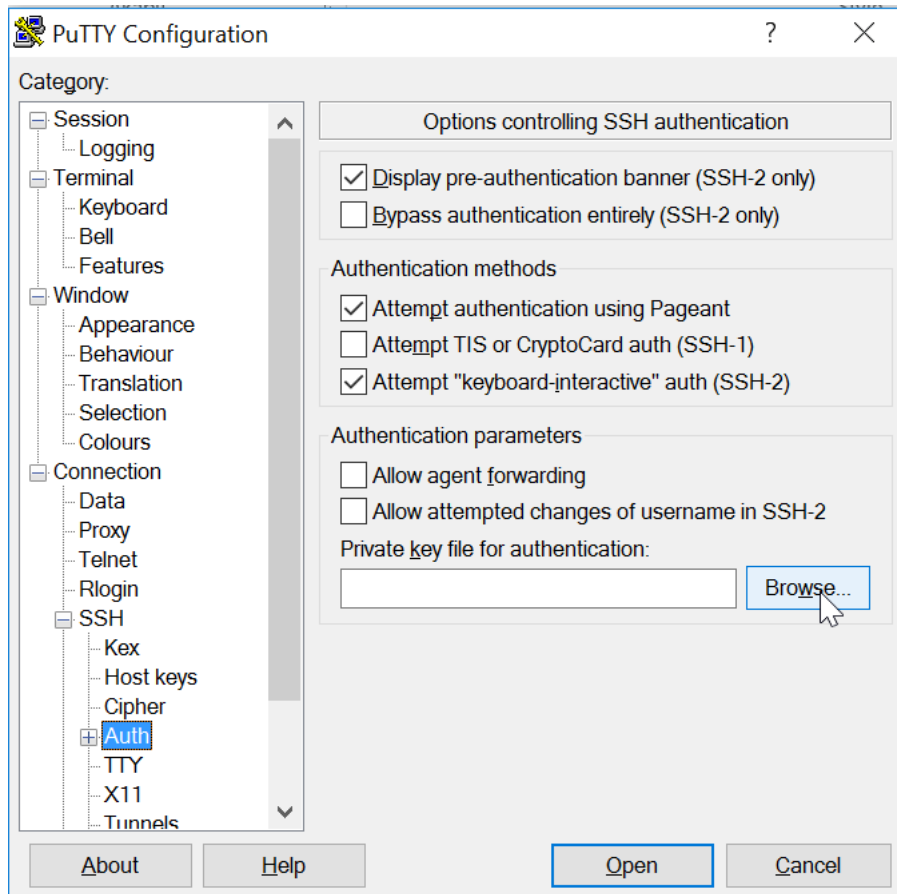
Używając oprogramowania PUTTY.EXE należy skonfigurować połączenie podając adres IP oraz klucz ppk wygenerowane w poprzednim kroku.

Adres IP:

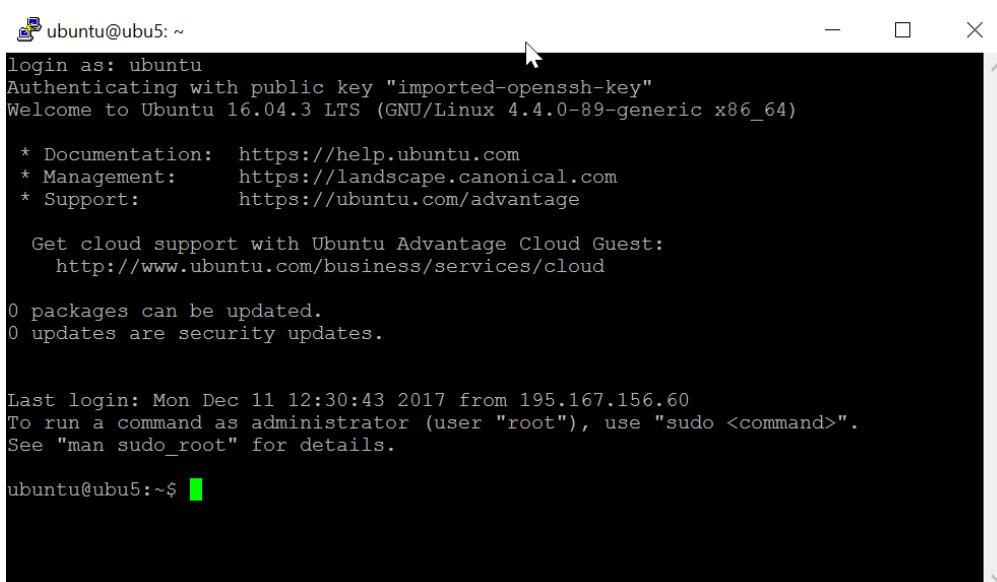


W kategorii Connection → SSH → Auth po kliknięciu przycisku Browse należy podać klucz prywatny ppk:



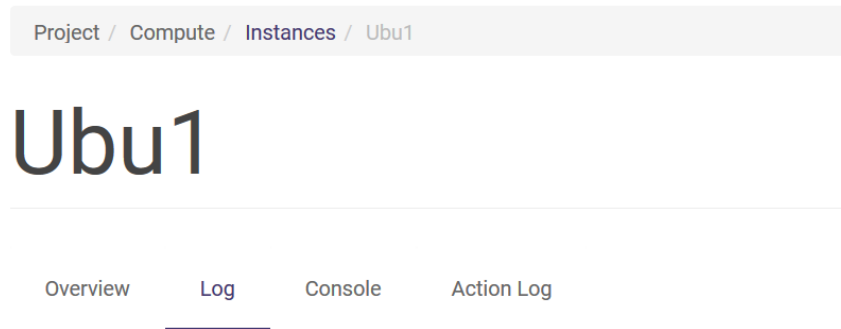


Po kliknięciu przycisku Open w oknie PuTTY Configuration, następuje otwarcie sesji. Należy wpisać użytkownika (tu, domyślnie dla Linux Ubuntu: ubuntu):



## Hasło administratora do instancji

Hasło root/administratora generuje się automatycznie podczas tworzenia maszyny (patrz również rozdział „Sieci wewnętrzne” → praktyczne uwagi). Hasło to można odczytać z logów. Na liście instancji należy kliknąć na nazwę instancji, a po pojawieniu się nowego ekranu – na zakładkę Log:



W logach znajduje się hasło root:

## Instance Console Log

```
[ 31.042286] cloud-init[1229]: Password changed
Password changed
[ 31.092801] cloud-init[1229]: Could not provide encrypted password due to lack of instance ssh key
Could not provide encrypted password due to lack of instance ssh key
[ 31.098230] cloud-init[1229]: Your root password: RGKq6zwdL9Sq1vu9.\nYou are forced to change it on first logon
Your root password: RGKq6zwdL9Sq1vu9.\nYou are forced to change it on first logon
```

Hasła tego można użyć do pierwszego logowania jako root – można je wykonać z wewnątrz panelu. Po kliknięciu na nazwę instancji, należy przejść do zakładki Console:



Przy pierwszym logowaniu trzeba przejść standardową procedurę zmiany hasła, podając najpierw bieżące (z logów) a następnie dwa razy nowe hasło. Wpisywanie hasła znak po znaku jest bardzo niewygodne – w wbudowanej w panel Horizon konsoli nie zadziała kopiuj-wklej. Inne, bardzo wygodne podejście bazuje na logowaniu zdalnym z konsoli wspierającej kopiuj-wklej. Może to być terminal lokalnej maszyny lub narzędzie typu putty w przypadku użytkowników systemu operacyjnego Windows. Po zdalnym zalogowaniu się przez ssh (uprzednio najlepiej mieć stworzonego użytkownika – np. sposobem opisanym w UWAGA 4 praktycznych uwag tego rozdziału), należy wykonać polecenie switch user (su) – użytkownik wejdzie w standardową procedurę zmiany hasła podczas której można już użyć w kopiuj-wklej (tu: ctrl+c standardowo = kopiuj, następnie prawy przycisk myszy w konsoli putty):

```

root@ubu2: /home/ubuntu
ubuntu@ubu2:~$ su root
Password:
You are required to change your password immediately (root enforced)
Changing password for root.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
root@ubu2: /home/ubuntu#
  
```

## Router

### Tworzenie routera

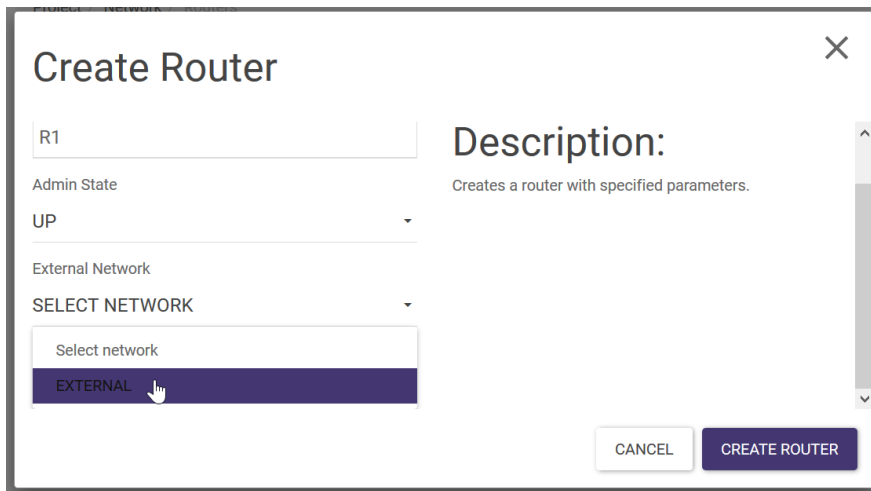
Przy przygotowaniu środowiska składającego się z routera, sieci wewnętrznej i maszyn, warto pamiętać o kolejności tworzenia, tzw. (1) utworzenie routera, (2) utworzenie sieci wewnętrznej i podłączenie jej do routera, (3) utworzenie sieci wewnętrznej (patrz też: autogenerowanie hasła root, dhcp sieci wewnętrznej)

#### KROK 1

Na ekranie Project → Network → Routers klikamy +CREATE ROUTER

#### KROK 2

W kreatorze należy nadać nazwę oraz podpiąć sieć zewnętrzną, a następnie potwierdzić klikając przycisk Create Router:



### Dodanie interfejsu LAN

#### KROK 1

Należy kliknąć na nazwę routera na liście:

<input type="checkbox"/>	Name	Status	External Network
<input type="checkbox"/>	R1	Active	EXTERNAL

Displaying 1 item

### KROK 2

Po przejściu do zakładki Interfaces należy kliknąć +ADD INTERFACE



### KROK 3

W kreatorze należy wybrać stworzoną wcześniej sieć wewnętrzną a następnie potwierdzić przyciskiem SUBMIT:

## Add Interface ✕

Subnet \*

SELECT SUBNET ▼

Select Subnet

Internal1: 192.168.0.0/24 (e8c37a85-67f0-434...)

EXTERNAL: 195.167.156.0/24 (EXTERNAL)

R1

### Description:

You can connect a specified subnet to the router.

The default IP address of the interface created is a gateway of the selected subnet. You can specify another IP address of the interface here. You must select a subnet to which the specified IP address belongs to from the above list.

Router ID \*

0f69ae82-2026-4da3-97c5-c904bfd2dd9e

CANCEL SUBMIT

## Usunięcie routera

Aby usunąć router, należy najpierw wszystkie zależności:

### KROK 1

Po prawej stronie routera na liście aktywności należy wybrać CLEAR GATEWAY

Displaying 1 item

<input type="checkbox"/>	Name	Status	External Network	Admin State	Actions
<input type="checkbox"/>	R1	Active	EXTERNAL	UP	CLEAR GATEWAY <span style="font-size: 0.8em;">▼</span>

Displaying 1 item

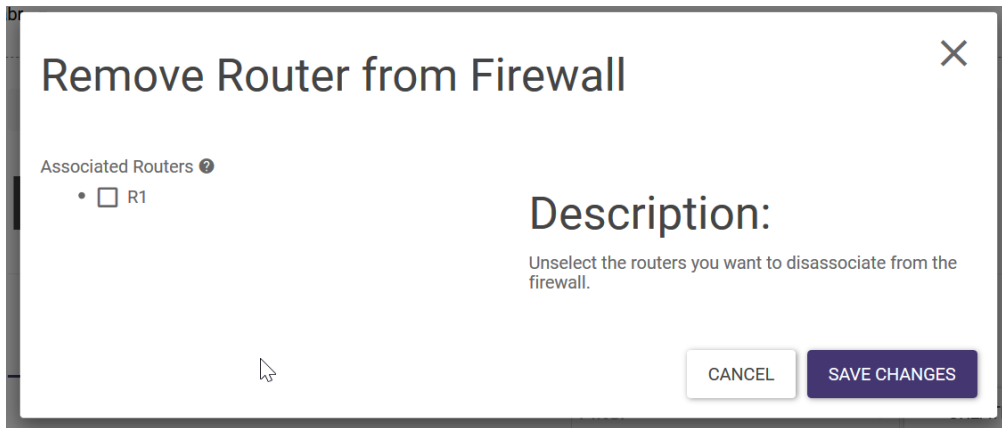
### KROK 2

Odwiązanie routera z Firewalla. Na ekranie Project → Network → Firewalls, należy z listy actions wybrać REMOVE ROUTER.

Associated Routers	Status	Admin State	Actions
R1	Active	UP	EDIT FIREWALL DELETE FIREWALL REMOVE ROUTER

### KROK 3

W kreatorze należy odznaczyć router a następnie potwierdzić zmianę przyciskiem SAVE CHANGES



Po zmianie statusu z Pending Update na Active można przejść do następnego kroku.

### KROK 4

Usunięcie interfejsu LAN. Po przejściu do ekranu Project → Network → Routers a następnie kliknięciu nazwy routera, który chcemy usunąć, przechodzimy na zakładkę Interface. Usuujemy wszystkie interfejsy poprzez funkcję DELETE INTERFACE

## R1

SET GATEWAY

Overview Interfaces Static Routes

+ ADD INTERFACE DELETE INTERFACES

Displaying 1 item

<input type="checkbox"/>	Name	Fixed IPs	Status	Type	Admin State	Actions
<input type="checkbox"/>	(b4e75158-2246)	• 192.168.0.101	Active		UP	DELETE INTERFACE

Displaying 1 item

### KROK 5

Po przejściu do zakładki Overview należy wybrać DELETE ROUTER

Project / Network / Routers / R1

# R1

CLEAR GATEWAY ▾  
EDIT ROUTER  
DELETE ROUTER

---

Overview   Interfaces   Static Routes

<b>Name</b>	R1
<b>ID</b>	0f69ae82-2026-4da3-97c5-c904bfd2dd9e
<b>Description</b>	
<b>Project ID</b>	0a791cc6a55b45c5a167f1952f2e09c9
<b>Status</b>	Active
<b>Admin State</b>	UP
<b>Availability Zones</b>	<ul style="list-style-type: none"> <li>• AZ1</li> <li>• AZ2</li> <li>• AZ3</li> </ul>

## Sieci wewnętrzne

Użytkownik ma możliwość samodzielnego tworzenia sieci wewnętrznych.

### Tworzenie sieci wewnętrznej

#### KROK 1

Po przejściu na ekran Project → Network → Networks, należy kliknąć +CREATE NETWORK a następnie przejść przez 3 zakładki kreatora. Poniższe trzy ekrany przedstawiają przykładowo uzupełnione pola.

✕

## Create Network

Network

Subnet

Subnet Details

Network Name

Admin State ?

UP ▾

Create Subnet

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

CANCEL

« BACK

NEXT »

# Create Network



Network

**Subnet**

Subnet Details

Subnet Name

Internal1

Network Address 

192.168.0.0/24

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 »

# Create Network



Network

Subnet


**Subnet Details**

Enable DHCP

Allocation Pools 

192.168.0.1,192.168.0.8

Specify additional attributes for the subnet.

DNS Name Servers 

91.185.186.228

91.185.186.229

91.185.186.230

CANCEL

« BACK

CREATE

Po kliknięciu CREATE lista sieci powiększy się o nowoutworzoną sieć wewnętrzną:

Displaying 2 items

<input type="checkbox"/>	Name	Subnets Associated	Shared	External	Status	Admin State
<input type="checkbox"/>	Internal1	192.168.0.0/24	No	No	Active	UP
<input type="checkbox"/>	EXTERNAL	EXTERNAL 195.167.156.0/24	Yes	Yes	Active	UP

Displaying 2 items

## Edycja sieci i podsieci

Edycja sieci i parametrów podsieci możliwa jest po kliknięciu na nazwę sieci. Pojawi się ekran, z którego można użyć dwóch akcji: EDIT NETWORK oraz EDIT SUBNET.

Project / Network / Networks / Internal1

# Internal1

EDIT NETWORK

Overview Subnets Ports

## Subnets

Filter  + CREATE SUBNET DELETE SUBNETS

Displaying 1 item

<input type="checkbox"/>	Name	Network Address	IP Version	Gateway IP	Actions
<input type="checkbox"/>	(e8c37a85-67f0)	192.168.0.0/24	IPv4	192.168.0.1	EDIT SUBNET

Displaying 1 item

## Statyczne prywatne adresy IP, ręczne przydzielanie adresów

Ręczne nadanie prywatnego adresu IP jest możliwe z wykorzystaniem API. Należy wykonać następujące kroki:

### KROK 1

Utworzenie portu, korzystając z komendy

```
(openstack) port create --network Internal3 --fixed-ip ip-address=192.168.2.2 port1
```

Gdzie: Internal3 to nazwa utworzonej uprzednio sieci wewnętrznej, port1 nadawana nazwa portu, a 192.168.2.2 to adres IP który chcemy przypisać.

```
ubuntu@ubu1: ~
ubuntu@ubu1:~$ openstack
(openstack) port create --network Internal3 --fixed-ip ip-address=192.168.2.2 port1
```



# Internal3

EDIT NETWORK

Overview Subnets Ports

## Ports

Filter

Displaying 4 items

<input type="checkbox"/>	Name	Fixed IPs	Attached Device	Status	Admin State	Actions
<input type="checkbox"/>	(4bca6b69-c1eb)	• 192.168.2.5	network:dhcp	Active	UP	EDIT PORT
<input type="checkbox"/>	(78afa6a0-258a)	• 192.168.2.3	network:dhcp	Active	UP	EDIT PORT
<input type="checkbox"/>	port1	• 192.168.2.2	Detached	Down	UP	EDIT PORT
<input type="checkbox"/>	(cfe5791d-8c74)	• 192.168.2.4	network:dhcp	Active	UP	EDIT PORT

Displaying 4 items

### KROK 2

Przypisanie portu do instancji Podczas tworzenia maszyny w kreatorze w zakładce Network Ports należy wybrać port z adresem IP, który chcemy przypisać do instancji. Patr: screenshot z UWAGI 1 sekcji „Praktyczne uwagi”.

## Praktyczne uwagi

UWAGA 1. Sieci wewnętrzne a hasło root.

Autogenerowanie hasła root podczas tworzenia maszyny odbywa się po sieci tylko przy włączonym DHCP. W przypadku potrzeby stworzenia sieci wewnętrznej z maszynami ze statycznymi adresami IP należy skorzystać z następującej procedury działania:

1. Utworzenie sieci wewnętrznej z włączonym DHCP. Atman zaleca kreowanie sieci wewnętrznych z zawsze włączonym DHCP.
2. Utworzenie portów wg sposobu opisanego w podrozdziale wyżej „Statyczne prywatne adresy IP”.
3. W trakcie tworzenia maszyny z kreatora, przypisanie portu do maszyny w zakładce Network Ports. Zakładka Networks powinna pozostać wtedy nieuzupełniona.

# Launch Instance



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

Ports provide extra communication channels to your instances. You can select ports instead of networks or a mix of both. ?

▼ Allocated <sup>1</sup>

Select ports from those listed below.

Name	IP	Admin State	Status
> port1	192.168.2.2 on subnet:	Up	Down

▼ Available <sup>2</sup>

Select one

Name	IP	Admin State	Status
> port2	192.168.2.22 on subnet:	Up	Down
> port32	192.168.2.32 on subnet:	Up	Down

× CANCEL

← BACK

NEXT →

🔥 LAUNCH INSTANCE

**UWAGA 2. Gateway.**

Przy tworzeniu samodzielnej sieci wewnętrznej, należy w kreatorze zaznaczyć opcję Disable Gateway. W przypadku potrzeby podłączenia sieci do routera, należy włączyć tą opcję co pozwoli na dodanie do routera interfejsu tej sieć. Przed uruchomieniem maszyny sieć powinna być wpięta do routera. Ekran kreatora edycji/tworzenia sieci:

# Edit Subnet




Subnet Subnet Details

Subnet Name

Update a subnet associated with the network. Advanced configuration are available at "Subnet Details" tab.

Network Address 

Gateway IP 

Disable Gateway

CANCEL « BACK NEXT »

## Firewall

Funkcjonalność zapory ogniowej dostępna jest w ekranie Project → Network → Firewalls (w menu po lewej części panelu Horizon). Należy pamiętać, że Firewall związany jest z routerem, zatem aby był on aktywny, uprzednio należy mieć utworzony router.

Tworzenie reguł odbywa się w kolejności: (1) Zdefiniowanie reguł (zakładka Firewall Rules), (2) Utworzenie polityk (zakładka Firewall Policies), (3) Utworzenie obiektu firewall (zakładka Firewalls).

### Utworzenie zapory ogniowej.

KROK 1

Regułę należy utworzyć klikając przycisk Add Rule w zakładce Firewall Rules, a następnie definiując reguły za pomocą kreatora.



Górna część ekranu kreatora:

## Add Rule ✕

Name

Description

Protocol \*  
TCP ▾

Action \*  
ALLOW ▾

Source IP Address/Subnet

Destination IP Address/Subnet

Create a firewall rule.

A Firewall rule is an association of the following attributes:

- IP Addresses: The addresses from/to which the traffic filtration needs to be applied.
- IP Version: The type of IP packets (IP V4/V6) that needs to be filtered.
- Protocol: Type of packets (UDP, ICMP, TCP, Any) that needs to be checked.
- Action: Action is the type of filtration required, it can be Reject/Deny/Allow data packets.

The protocol and action fields are required, all others are optional.

CANCEL
ADD

Dolna część ekranu kreatora:

## Add Rule



TCP

Action \*

ALLOW

Source IP Address/Subnet

Destination IP Address/Subnet

Source Port/Port Range

Destination Port/Port Range

IP Version

4

Shared

Enabled

• Action: Action is the type of filtration required, it can be Reject/Deny/Allow data packets.

The protocol and action fields are required, all others are optional.

CANCEL ADD

Oto 3 przykłady pozwalające zorientować się w jaki sposób konfigurować regułu

- F1.p1.r3 – odrzucenie SSH
- F1.p1.r2 – odrzucenie ping
- F1.p1.r1 – wszystko otwarte

<input type="checkbox"/>	Name	Description	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Shared	Enabled	In Policy	Actions
<input type="checkbox"/>	F1.p1.r3		TCP	-	-	-	22	DENY	No	Yes	p1	EDIT RULE
<input type="checkbox"/>	F1.p1.r2		ICMP	-	-	-	-	DENY	No	Yes	p1	EDIT RULE
<input type="checkbox"/>	F1.p1.r1		ANY	0.0.0.0/0	-	0.0.0.0/0	-	ALLOW	No	Yes	p1	EDIT RULE

### KROK 2

W zakładce Firewall Policies należy kliknąć przycisk +ADD POLICY i za pomocą kreatora dodać politykę, wpisując jej nazwę oraz dodając wcześniej zdefiniowane reguły. UWAGA: ważna jest kolejność reguł.

## Add Policy ✕

Policy

Rules

Name \*

Description

Shared  
 Audited

Create a firewall policy with an ordered list of firewall rules.

A firewall policy is an ordered collection of firewall rules. So if the traffic matches the first rule, the other rules are not executed. If the traffic does not match the current rule, then the next rule is executed. A firewall policy has the following attributes:

- Shared: A firewall policy can be shared across tenants. Thus it can also be made part of an audit workflow wherein the firewall policy can be audited by the relevant entity that is authorized.
- Audited: When audited is set to True, it indicates that the firewall policy has been audited. Each time the firewall policy or the associated firewall rules are changed, this attribute will be set to False and will have to be explicitly set to True through an update operation.

The name field is required, all others are optional.

CANCEL

ADD

## Add Policy ✕

Policy \*

Rules

Selected Rules

rule:1

F1.p1.r1

(6f6782a2-23cf-4b66-8c57-13ae8592e9e9)

-

rule:2

F1.p1.r2

(d4cb134f-9b9f-4ae01-8344-25514660740e)

-

Available Rules

CANCEL

ADD

### KROK 3

W zakładce Firewalls należy kliknąć przycisk +CREATE FIREWALL i uzupełnić pola w kreatorze, podając politykę i wiążąc Firewall z Routerem.

## Add Firewall ✕

Firewall
Routers

Name

Description

Policy \*  
SELECT A POLICY

Select a Policy  
 p1

Create a firewall based on a policy.  
 A firewall represents a logical firewall resource that a tenant can instantiate and manage. A firewall must be associated with one policy, all other fields are optional.

CANCEL
ADD

## Add Firewall ✕

Firewall \*
Routers

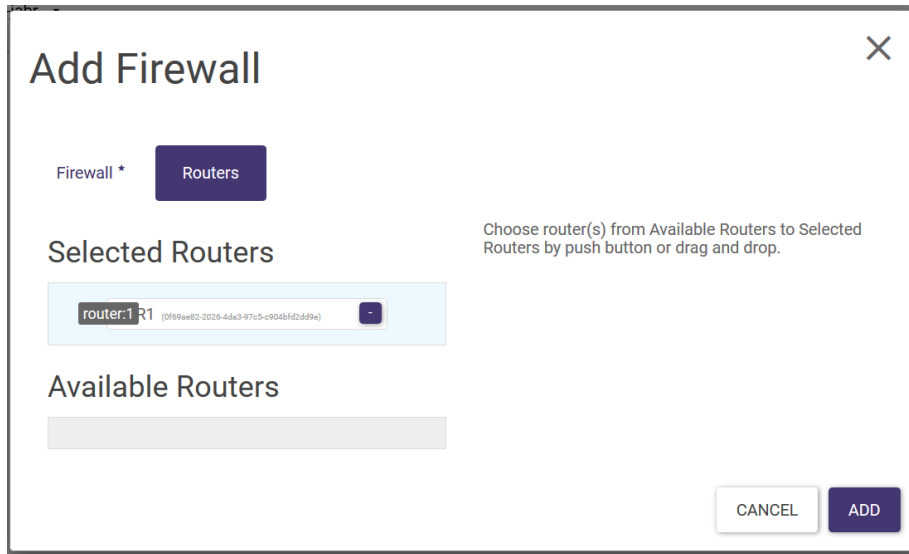
Selected Routers

Available Routers

↕ R1 (0f69ae82-2026-4da3-97c5-c904bffd2d89e)
+

Choose router(s) from Available Routers to Selected Routers by push button or drag and drop.

CANCEL
ADD



Teraz należy poczekać aż status zmieni się z Pending Create na Active. Jeśli w ciągu kilku sekund zmiana nie nastąpi, należy kliknąć w głównym menu po lewej stronie panelu Horizon na inną zakładkę po czym wrócić do zakładki Firewalls lub odświeżyć widok – status będzie zmieniony.

Displaying 1 item

<input type="checkbox"/>	Name	Description	Policy	Associated Routers	Status	Admin State	Actions
<input type="checkbox"/>	F1		p1	R1	Pending Create	UP	DELETE FIREWALL

Displaying 1 item

Displaying 1 item

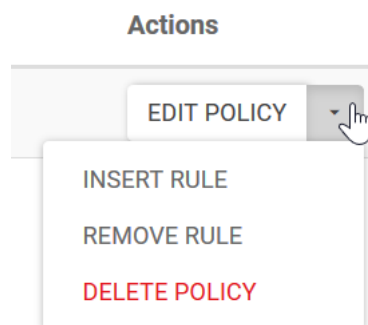
<input type="checkbox"/>	Name	Description	Policy	Associated Routers	Status	Admin State	Actions
<input type="checkbox"/>	F1		p1	R1	Active	UP	EDIT FIREWALL

Displaying 1 item

## Dodanie reguły do polityki.

### KROK 1

Po prawej stronie polityki do której chcemy dodać regułę należy rozwinąć listę aktywności i kliknąć Insert Rule.



### KROK 2

Przy pomocy kreatora określamy regułę do dodania wraz kolejnością jej stosowania przez Firewall.



## Insert Rule to Policy ✕

Insert Rule \*

F1.P1.R3 ▼

---

Before

F1.P1.R1 ▼

---

After

F1.P1.R2 ▼

---

CANCEL SAVE CHANGES

**Description:**

Choose the rule you want to insert. Specify either the rule you want to insert immediately before, or the rule to insert immediately after. If both are specified, the prior takes precedence.

### KROK 3

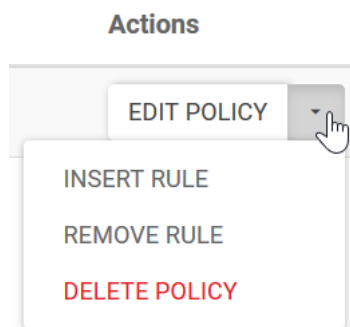
Należy zatwierdzić dodanie klikając przycisk Save Changes. Polityka zostaje zaktualizowana.

<input type="checkbox"/>	Name	Description	Rules	Shared	Audited	Actions
<input type="checkbox"/>	p1		F1.p1.r2, F1.p1.r3, F1.p1.r1	No	No	EDIT POLICY ▼

## Usunięcie reguły z polityki.

### KROK 1

Po prawej stronie polityki z której chcemy usunąć regułę należy rozwinąć listę aktywności i kliknąć Remove Rule.



### KROK 2

Po zaznaczeniu reguły, którą chcemy usunąć, należy kliknąć przycisk „Save Changes”.

## Remove Rule from Policy ✕

Remove Rule \*

F1.P1.R2

F1.p1.r2

F1.p1.r3

### Description:

Choose the rule you want to remove.

CANCEL
SAVE CHANGES

Oba kroki powtarza się tyle razy ile reguł jest do usunięcia.

## Usunięcie zapory ogniowej.

Aby usunąć Firewall należy wykonać czynności w odwrotnej kolejności niż przy jego tworzeniu:

(1) usunięcie obiektu Firewall – na liście usuwanego FW pojawi się status Pending Delete, po chwili FW powinien zniknąć z listy:

Displaying 1 item

	Name	Description	Policy	Associated Routers	Status	Admin State	Actions
<input type="checkbox"/>	F1		p1	R1	Pending Delete	UP	<span style="background-color: #e74c3c; color: white; padding: 2px 5px; border-radius: 3px;">DELETE FIREWALL</span> -

Displaying 1 item

(2) Usunięcie polityk (zakładka Firewall Policies)

(3) Usunięcie reguł (zakładka Firewall Rules)

## Praktyczne uwagi

UWAGA 1. Edycja reguł.

Wprawdzie panel Horizon sugeruje akcję EDIT RULE, jednakże nie jest możliwa edycja reguły. W przypadku potrzeby zmiany należy regułę usunąć i utworzyć nową.

## Grupy zabezpieczeń

### Tworzenie grupy

Grupa zabezpieczeń (Security Group) jest bardzo wygodnym narzędziem, umożliwiającym szczegółowe zdefiniowanie reguł bezpieczeństwa. Reguły określają jaki ruch jest dozwolony w ramach grupy zabezpieczeń. Jedna grupa zabezpieczeń może zostać przypisana do wielu wirtualnych maszyn. Do jednej wirtualnej maszyny może zostać przypisanych wiele grup zabezpieczeń. Domyślna grupa zabezpieczeń stosowana do wszystkich wirtualnych maszyn (które nie mają przypisanej żadnej innej grupy zabezpieczeń) odrzuca każdy przychodzący ruch, natomiast pozwala na ruch wychodzący z maszyny. Dopuszcza także ruch z obrębu tej samej grupy zabezpieczeń (tzn. wszystkich maszyn które mają tę grupę przypisaną):

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv6	Any	Any	-	default	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	Any	Any	-	default	DELETE RULE
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	DELETE RULE

Displaying 4 items

W przypadku potrzeby komunikacji z zewnątrz, np. zarządzania wirtualną maszyną przez ssh, należy dodać regułę na to pozwalającą. Najwygodniejszym sposobem jest utworzenie kolejnej grupy zabezpieczeń – niezależnej od grupy default – i zdefiniowanie w niej wymaganych reguł.

#### KROK 1

W menu po lewej stronie panelu Horizon, należy kliknąć Security Groups, a następnie w głównej części ekranu uruchomić + Create Security Group:

Project / Network / Security Groups

## Security Groups

Filter  + CREATE SECURITY GROUP

#### KROK 2

Pojawi się kreator, w którym należy nadać nazwę grupy zabezpieczeń (tu: AllowSSH), a następnie kliknąć Create Security Group:

### Create Security Group ✕

Name \*

Description:

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

Description

---

### KROK 3

Po pojawieniu się grupy na liście w głównym oknie ekranu, należy kliknąć przycisk Manage Rules w prawej części ekranu, dla tej grupy. Pojawi się nowy ekran z dwiema domyślnymi regułami, przepuszczającymi ruch wychodzący z maszyny:

+ ADD RULE DELETED RULES

Displaying 2 items

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	DELETED RULE
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	DELETED RULE

Displaying 2 items

### KROK 4

Nową regułą dodaje się poprzez kliknięcie +Add Rule. Poniższy zrzut ekranu pokazuje jakie wartości należy wybrać, aby pozwalać na SSH z dowolnego źródłowego adresu IP. Po określeniu reguły, należy je zatwierdzić w kreatorze klikając przycisk Add.

## Add Rule

Rule \*
Description:

Custom TCP Rule

---

Direction

Ingress

---

Open Port \*

Port

---

Port ?



---

Remote \* ?

CIDR

---

CIDR ?

**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

### KROK 5

Można w ten sposób dodać więcej reguły, w tym przykładzie dodana została w analogiczny sposób jak w kroku 4 reguła przepuszczająca ICMP (ping). Pełna lista reguły stworzonej grupy zabezpieczeń:

Displaying 4 items

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	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	ICMP	Any	0.0.0.0/0	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	DELETE RULE

Displaying 4 items

Oto przykład reguł innej grupy zabezpieczeń, która w sposób całkowicie otwarty przepuszcza ruch TCP:

<input type="checkbox"/>	Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
<input type="checkbox"/>	Egress	IPv6	Any	Any	::/0	-	DELETE RULE
<input type="checkbox"/>	Egress	IPv4	Any	Any	0.0.0.0/0	-	DELETE RULE
<input type="checkbox"/>	Ingress	IPv4	TCP	1 - 65535	0.0.0.0/0	-	DELETE RULE

Displaying 3 items

Grupy zabezpieczeń stanowią uzupełnienie, rozszerzenie możliwości dostępnych poprzez Firewall w zakresie zarządzania dozwolonym ruchem w wirtualnym środowisku serwerowym. Umożliwiają zorganizowanie łatwo zarządzalnych i przejrzystych polityk bezpieczeństwa dla różnych grup maszyn.

UWAGA: grupy zabezpieczeń działają niezależnie od reguł Firewalla.

## Zmiana przypisania grupy do instancji

Raz przypisaną do instancji (wirtualnej maszyny) grupę zabezpieczeń można zmienić, zmiany automatycznie stosowane są do wszystkich instancji mających przypisanie do tej grupy. Można również zmienić przypisanie grupy do instancji. Odbyna się to poprzez uruchomienie akcji EDIT INSTANCE na ekranie Project → Compute → Instances. Pojawi się kreator, którego można użyć do dodawania i usuwania przypisani instancja – grupa zabezpieczeń.

## Edit Instance ✕

Information \*

Security Groups

Add and remove security groups to this instance from the list of available security groups.

All Security Groups	Filter	Instance Security Groups	Filter
default	<input type="text"/>	AllOpen	<input type="text"/>
+		-	
AllowSSH			
+			

## VPN

Panel Horizon umożliwia wygodne zestawienie połączenie VPN typu site-to-site przy użyciu protokołu IPSec. Kanały IPSec można zestawiać pomiędzy środowiskiem serwerowym użytkownika w Atman Cloud a routerem fizycznym, routerem systemowym (np. VyOS) lub innym środowiskiem z tą funkcjonalnością (bazującym na narzędziach OpenStack).

Po stronie środowiska serwerowego użytkownika należy z panelu Horizon na ekranie Project → Network → VPN zdefiniować wszystkie komponenty połączenia IPSec. Analogiczne czynności należy wykonać po drugiej stronie połączenia VPN.

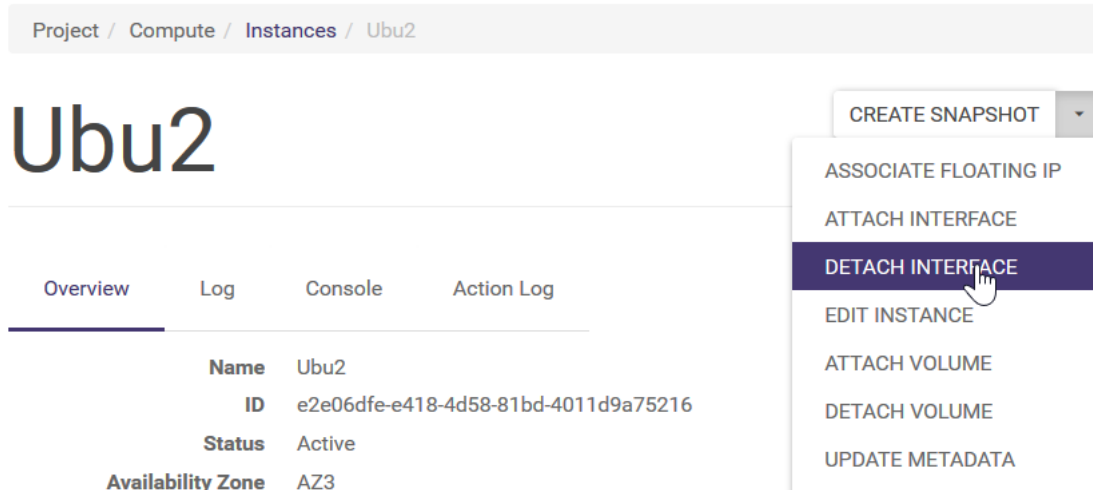
## Adresy IP

W ramach Atman Cloud, użytkownik ma możliwość operowania trzema typami adresów: stałymi publicznymi, pływającymi publicznymi (floating) oraz prywatnymi. Adresy publiczne dostępne są w liczbie określonej w umowie (zamówieniu). Limit wykupionych adresów publicznych osiągany jest poprzez przydzielanie zarówno publicznych stałych jak i publicznych pływających adresów IP.

### Stałe publiczne

Taki adres przypisywany jest do instancji (wirtualnej maszyny), gdy bezpośrednio jest ona wpinana do sieci EXTERNAL. Adres inicjalnie przydzielany jest z DHCP, jednakże póty będzie on niezmiennie przypisany do interfejsu maszyny aż interfejs ten zostanie skasowany lub maszyna usunięta.

Usunięcie interfejsu odbywa się poprzez wybranie funkcji DETATCH INTERFACE z poziomu instancji:



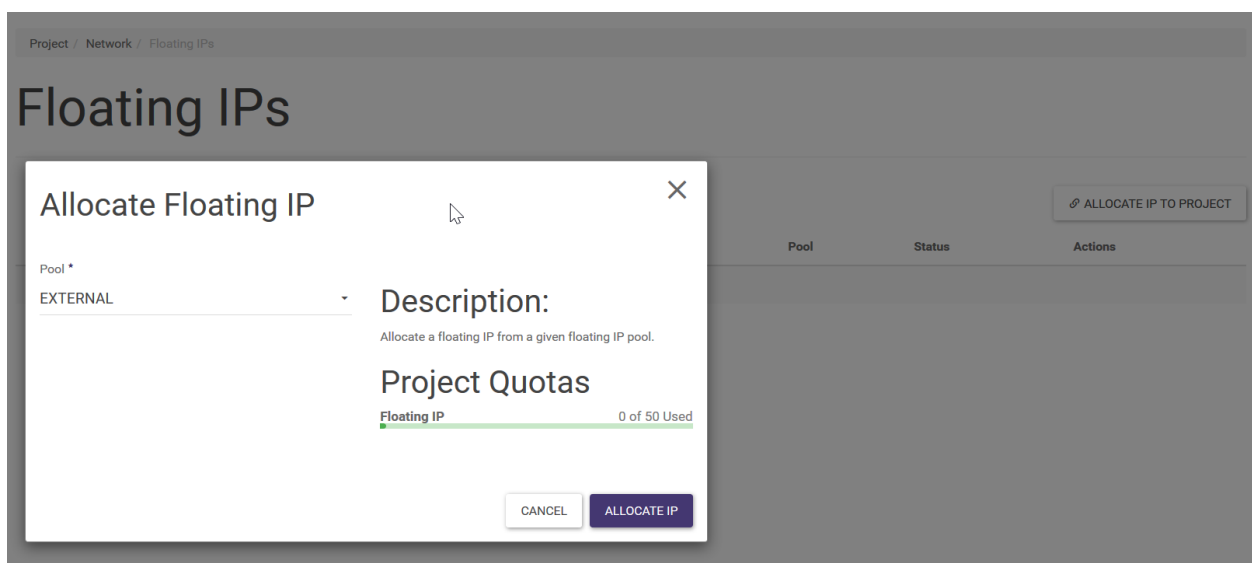
Należy pamiętać że ponowna alokacja tego samego publicznego adresu IP może oczywiście nastąpić ale z bardzo małym prawdopodobieństwem. Bardzo wygodnym i zalecanym przez Atmana podejściem dla instancji produkcyjnych jest korzystanie z pływających adresów IP.

## Pływające publiczne

Cechą pływających publicznych adresów IP jest to, że po zaalokowaniu ich przez użytkownika do środowiska, pozostają one przydzielone „na własność” tego środowiska do momentu świadomego uwolnienia ich przez użytkownika (usunięcia ze środowiska). Takie adresy inicjalnie przydzielane są z DHCP i pozostają niezienne przez cały ich cykl życia aż do ich uwolnienia. Pływające adresy IP można w sposób dowolny wiązać z instancjami (wirtualnymi maszynami), zmieniać ich przypisanie między instancjami w trakcie życia instancji lub pozostawiać nieprzypisanymi. Idea polega na powiązaniu publicznego pływającego adresu IP do interfejsu/portu z prywatną adresacją, zapewniając w ten sposób automatyczną translację tych adresów.

### KROK 1

Przydzielenie pływającego publicznego adresu IP do środowiska. Na ekranie Project → Network → Floating IPs należy wybrać akcję ALLOCATE IP TO PROJECT. Pojawi się okno, na którym należy kliknąć przycisk ALLOCATE IP.

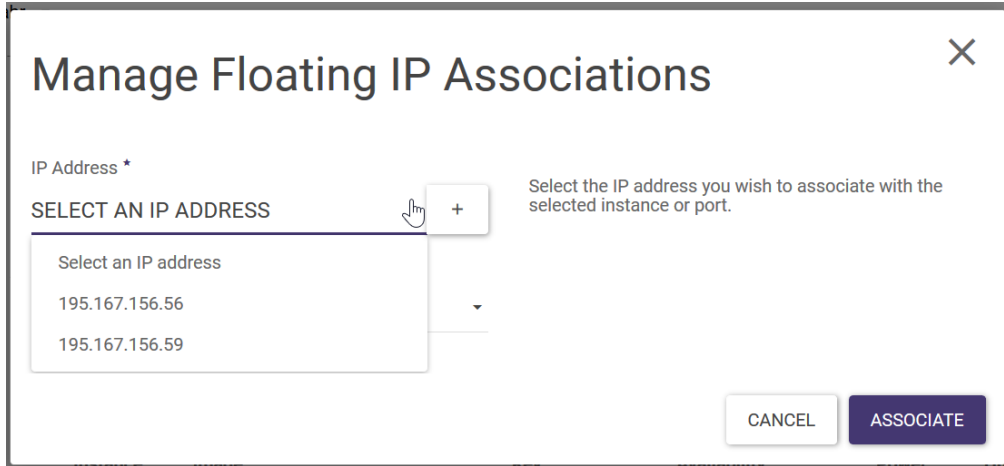


### KROK 2

Przydzielenie pływającego adresu IP do środowiska odbywa się poprzez:

- uruchomienie akcji ASSOCIATE dla danego pływającego adresu IP na ekranie Project→Network→Floating IPs
- uruchomienie akcji ASSOCIATE FLOATING IP dla danej instancji na ekranie Project→Compute→Instances

Z kreatora należy wybrać pływający adres IP a następnie port z którym ma zostać skojarzony.



**Manage Floating IP Associations**

IP Address \*

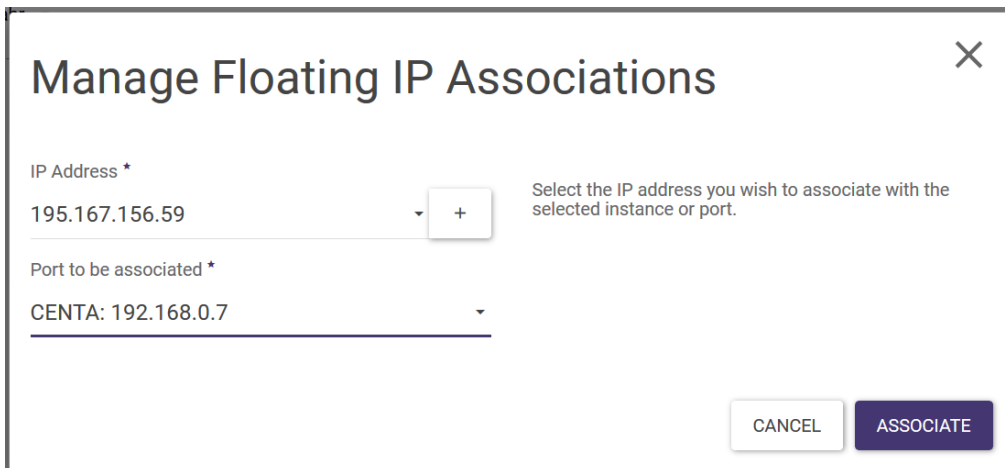
SELECT AN IP ADDRESS

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

195.167.156.56

195.167.156.59

CANCEL ASSOCIATE



**Manage Floating IP Associations**

IP Address \*

195.167.156.59

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

Port to be associated \*

CENTA: 192.168.0.7

CANCEL ASSOCIATE

Po przydzieleniu adresu na liście instancji będzie to odzwierciedlone w następujący sposób:

<input type="checkbox"/>	Instance Name	Image Name	IP Address	Flavor	Key	ir	Status
			192.168.0.5				
<input type="checkbox"/>	CentB	-	<b>Floating IPs:</b>	m1.c1	-		Active
			195.167.156.59				

## Prywatne

Użytkownik ma możliwość nadawania i przypisywania adresów prywatnych – więcej informacji w rozdziale Sieć.



## API

### Przygotowanie środowiska do korzystania z API

Atman rekomenduje klienta api: python-openstackclient.

Pełną dokumentację online można znaleźć pod adresem: <https://docs.openstack.org/python-openstackclient/latest/>

Kolejność działań:

1. Instalacja środowiska python
2. Instalacja python-openstackclient
3. Konfiguracja python-openstackclient
  - a. Pobranie pliku rc z panelu Horizon
  - b. Eksport zmiennych środowiskowych

### Szczegółowy opis przygotowania na przykładzie lokalnej maszyny Linux-Ubuntu:

1. Instalacja środowiska python. Na maszynie, z której administrator będzie zarządzał środowiskiem poprzez api, należy uruchomić polecenie:

```
ubuntu@ubu1: ~  
ubuntu@ubu1:~$ sudo apt install python-dev python-pip
```

2. Instalacja python-openstackclient.

W następnej kolejności uruchamiane jest polecenie:

```
ubuntu@ubu1: ~  
ubuntu@ubu1:~$ pip install python-openstackclient
```

3. Konfiguracja python-openstackclient.

- a. Pobranie pliku rc. Należy zalogować się do panelu Horizon i przejść do zakładki Project->Compute->API Access:

### Project

Compute

Overview

Instances

Volumes

Images

Key Pairs

API Access

Network

Orchestration

DNS

### Identity

W następnym kroku należy kliknąć „DOWNLOAD OPENSTACK RC FILE V3”:

Project / Compute / API Access

## API Access

DOWNLOAD OPENSTACK RC FILE V2.0

DOWNLOAD OPENSTACK RC FILE V3

VIEW CREDENTIALS

Pobrany plik należy zapisać w katalogu domowym użytkownika:

```
ubuntu@ubu1: ~  
ubuntu@ubu1:~$ pwd  
/home/ubuntu  
ubuntu@ubu1:~$ ls project-jabr-openrc.sh  
project-jabr-openrc.sh  
ubuntu@ubu1:~$ █
```

- b. Eksport zmiennych środowiskowych

Pobrano plik jest skryptem bash'owym, a jego działanie opiera się na ustawieniu 9 zmiennych środowiskowych, które używane są przez klienta API (python-openstackclient) do komunikacji z wirtualnym środowiskiem serwerowym (projektem) na chmurze Atman Cloud.

W środowisku Linux, eksport tych zmiennych uzyskuje się poprzez uruchomienie skryptu (komenda `source <plik-który-został-pobrano>`):

```
ubuntu@ubu1: ~  
ubuntu@ubu1:~$ source project-jabr-openrc.sh
```

Po podaniu hasła ustawione są już wszystkie zmienne niezbędne do użycia API:

```
ubuntu@ubu1: ~  
ubuntu@ubu1:~$ printenv | grep OS  
OS_PROJECT_ID=0a791cc6a55b45c5a167f1952f2e09c9  
OS_REGION_NAME=Waw01  
OS_USER_DOMAIN_NAME=Default  
OS_PROJECT_NAME=project-jabr  
OS_IDENTITY_API_VERSION=3  
OS_PASSWORD=  
OS_AUTH_URL=https://api.cloud.atman.pl:5000/v3  
OS_USERNAME=jabr  
OS_INTERFACE=public  
ubuntu@ubu1:~$
```

Każdorazowo przy nowej sesji należy w ten sam sposób ustawić zmienne.

Komunikacja pomiędzy środowiskiem na Atman Cloud a terminalem, z którego administrator zarządza poprzez API, odbywa się w formie szyfrowanej transmisji (protokół HTTPS).

W przypadku terminalu administracyjnego obsługiwanego przez inny system operacyjny (inna dystrybucja Linux, Mac OS X, Windows) – szczególnie opisanych kroków będą się różnić, przy czym koncepcja pozostaje ta sama: instalacja środowiska python, instalacja klienta python-openstackclient, pobranie wartości dla zmiennych środowiskowych z panelu Horizon.

Klient/API jest przygotowany do użycia.

Lista wszystkich poleceń dostępna jest pod adresem:

<https://docs.openstack.org/python-openstackclient/latest/cli/command-list.html>

## Inne

### Konwersja obrazów

W celu zaimportowania maszyny z zewnątrz do wirtualnego środowiska serwerowego do Atman Cloud, należy uprzednio przekonwertować ją do formatu raw. Poniższy przykład obrazuje proces konwersji pliku vmdk na raw przy użyciu rekomendowanego przez Atman narzędzia – `qemu`.

## KROK 1

Zapisanie obrazu maszyny

Z poziomu VMWare vSphere Web Client pobieramy plik (tu: jako test-flat.vmdk)

[FAS2040\_vmware0] test

Search

Name	Size	Modified
test.vmx	3.15 KB	11/28/2017 1:27 PM
test-ctk.vmdk	3,840.50 KB	11/28/2017 1:27 PM
test.vmdk	62,914,560.00 KB	11/28/2017 1:20 PM
test-5778c7f1.hlog	0.36 KB	11/28/2017 1:19 PM
test.nvram	8.48 KB	11/28/2017 1:27 PM
test.vmsd	0.00 KB	11/28/2017 1:19 PM
vmware.log	318.72 KB	11/28/2017 1:27 PM

Pobrano 2% z test-flat.vmdk

Anuluj

Wyświetl pobrane pliki

## KROK 2

Konwersja. Linux:

```
ubuntu@ubu1: ~
```

```
ubuntu@ubu1:~$ sudo apt-get install qemu-utils
```

```
ubuntu@ubu1: ~
```

```
ubuntu@ubu1:~$ qemu-img -f vmdk -O raw test-flat.vmdk test-flat.raw
```

Windows:

1. Należy pobrać oprogramowanie qemu:

### Download binaries

[qemu-img 2.3.0 for Windows x64](#)

2. Po rozpakowaniu oprogramowanie gotowe jest do użycia – z terminala PowerShell należy uruchamiać z miejsca w którym plik qemu-img.exe jest zapisany.
3. Poniższe polecenie konwertuje plik vmdk do formatu raw:

```
Windows PowerShell
PS C:\Users\jbryla\Downloads> .\qemu-img.exe convert .\test-flat.vmdk -o raw .\test-flat.raw
```

## Upload (import) pliku do chmury

1. Upload przy użyciu API.

```
61G -rw-rw-r-- 1 ubuntu ubuntu 60G Nov 28 16:05 test-flat.raw
ubuntu@ubul:~$ openstack
(openstack) image create --file test-flat.raw test-flat.raw
```

Po ukończeniu w terminalu pojawiają się właściwości stworzonego/uploadowanego obrazu:

```

| properties | direct_url='rbd://b6f23cff-7279-f4b0-ff91-21fadac95bb5/i
| images/96ea1544-1293-476f-9ca0-342392bc81b0/snap', locations='[[u'url': u'rbd:
| //b6f23cff-7279-f4b0-ff91-21fadac95bb5/images/96ea1544-1293-476f-9ca0-342392b
| c81b0/snap', u'metadata': {}]]' |
| protected | False
|
| schema | /v2/schemas/image
|
| size | 64424509440
|
| status | active
|
| tags |
|
| updated_at | 2017-11-28T16:25:34Z
|
| virtual_size | None
|
| visibility | shared
|
+-----+
+-----+
(openstack) █
```

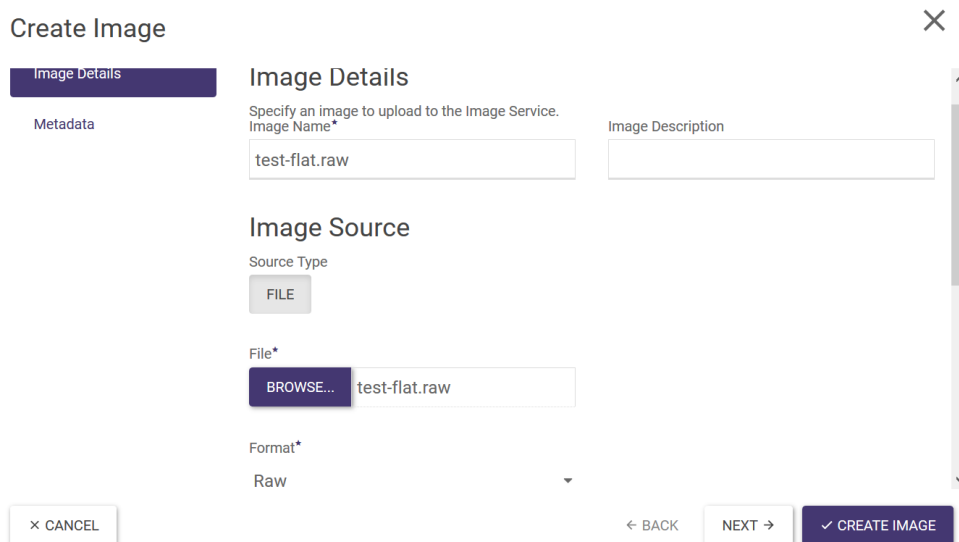
Sprawdzenie czy plik został zaimportowany na chmurę:

```

ubuntu@ubu1: ~
ubuntu@ubu1:~$ openstack
(openstack) image list
+-----+-----+-----+
| ID | Name | Status |
+-----+-----+-----+
| bc33dc53-9e99-47fa-8604-f245e9a9bfb6 | CentOS-7_x86_64_1702 | active |
| 668efd69-4d57-4d0d-8c55-0dc119cdf592 | Centos-6_x86_64_1704 | active |
| 0bfbbedd0-8016-40df-92b4-95f960eb765a | Cirros | active |
| 43937403-8356-47a4-8cfe-be59e4ccd43c | Debian 9.1.1 (Stretch) amd64 | active |
| a0ab4b87-1113-4c9e-b406-debc1ecdc658 | Debian 9.1.1 (Stretch) amd64 | active |
| 4eec2b2e-ca56-44d0-a5d9-4dc454e25ce5 | Debian-7-CloudInit-ATM | active |
| 8f8783d3-1a6f-410a-8e03-8cb9a31a90e2 | IMG-VOL1 | active |
| f8ffbe2f-5626-426c-b5d6-a482fc46c8f1 | IMG-Vol2 | active |
| b749d985-7053-4b88-91e3-226378006454 | Ubuntu 16.04 (Xenial) amd64 | active |
| 1322afa1-8106-42aa-86f7-d0ce076eddf0 | Ubuntu-14.04-trusty_x86_64 | active |
| f83d8ff7-3f53-46d0-a535-363d39f5e285 | VyOS-1.1.7-cloud-init | active |
| 08c2d30f-02d3-455e-b95e-9be90dc34a3c | VyOS-1.1.7-signed | active |
| 80f202af-8361-4ab7-b986-5038d2dc53af | Windows_2012_R2_eval.build_20170811 | active |
| 7bb2964c-9eca-4b53-afb3-f1821d43d163 | Windows_2016_eval.build_20170809 | active |
| 7c3947cb-19a5-4ab8-8937-83161062f775 | pfsense-CE-2.3.4-amd64 | active |
| 96ea1544-1293-476f-9ca0-342392bc81b0 | test-flat.raw | active |
+-----+-----+-----+
(openstack) █

```

2. Upload z lokalnej maszyny na chmurę przy użyciu panelu Horizon:



W dolnej części kreatora należy ustawić parametry:

- a) Visibility=Private
- b) Protected=Yes lub Protected=No.

## Image Sharing

Visibility

PUBLIC

PRIVATE

Protected

YES

NO

← BACK

NEXT →

CREATE IMAGE

Znaczenie parametrów:

- Private – obraz będzie widoczny tylko w ramach danego środowiska, niewidoczny dla innych (tę opcję należy wybrać)
- Public – takie obrazy tworzone są tylko przez administratorów Atman Cloud. Opcja niedostępna dla użytkownika.
- Protected – nie będzie można usunąć takiego obrazu
- Unprotected – dozwolone jest usuwanie obrazu

W trakcie uploadu obrazu w kreatorze pojawi się pasek stanu, na którym widać postęp pracy:

### Create Image

Image Details

Metadata

#### Image Details

Specify an image to upload to the Image Service.

Image Name\*

Image Description

#### Image Source

Source Type

FILE

File\*

19%

Format\*

Raw


× CANCEL
← BACK
NEXT →
CREATE IMAGE

Po utworzeniu kreatorem obrazu należy odświeżyć widok...

<input type="checkbox"/>	> test-flat.raw	Image	<div style="background-color: #0070c0; width: 20px; height: 10px; display: inline-block;"></div> Saving	shared	No	RAW
--------------------------	-----------------	-------	---	--------	----	-----

...poprzez kliknięcie w menu na inną zakładkę i ponowne kliknięcie na zakładkę Images:

Instances

Volumes 

Images

Key Pairs

Po odświeżeniu widoku – obraz jest zaimportowany do środowiska i gotowy do użycia.

<input type="checkbox"/>	> test-flat.raw	Image	Active	shared	No	RAW	60.00 GB	LAUNCH	-
--------------------------	-----------------	-------	--------	--------	----	-----	----------	--------	---

### 3. Trzecia droga:

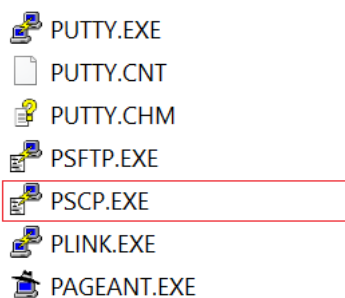
W przypadku bardzo dużych plików, słabego łącza, zrywania sesji, itp. – alternatywną, dobrze działającą ścieżką jest skopiowanie obrazu z lokalnej maszyny na zdalną maszynę uruchomioną na Atman Cloud, a następnie użycie API do uploadu obrazu.

W kolejnym kroku przyjmujemy założenie, że na Atman Cloud znajduje się maszyna Linux Ubuntu (IP:195.167.156.60) z wystarczająco dużą przestrzenią do pomieszczenia obrazu. Do przekopiowania najłatwiej użyć komendy scp lub jej odpowiednika Windowsowego w postaci pscp (to narzędzie jest częścią standardowego pakietu oprogramowania Putty).

Linux:

```
ubuntu@ubu1: ~
ubuntu@ubu1:~$ scp test-flat.raw ubuntu@195.167.156.60:/home/ubuntu/test-flat.raw
```

Windows:



Sposób użycia z PowerShell Windowsa:

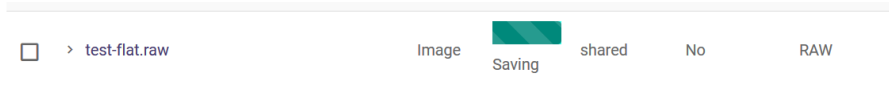
```
PS H:\tools> .\PSCP.EXE C:\Users\...Downloads\test-flat.raw ubuntu@195.167.156.60:/home/ubuntu/test-flat.raw
ubuntu@195.167.156.60's password:
test-flat.raw | 46570092 kB | 17396.4 kB/s | ETA: 00:15:39 | 74%
```

Po przekopiowaniu obrazu należy z poziomu wirtualnej maszyny, na którą obraz został skopiowany, wykonać polecenie:



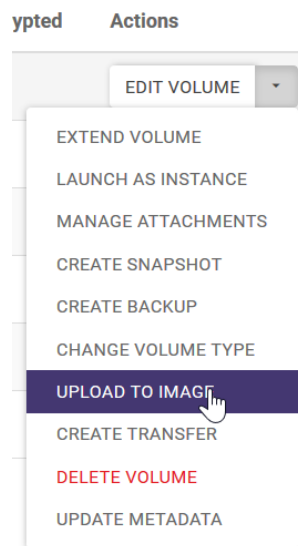
```
61G -rw-rw-r-- 1 ubuntu ubuntu 60G Nov 28 16:05 test-flat.raw
ubuntu@ubul:~$ openstack
(openstack) image create --file test-flat.raw test-flat.raw
```

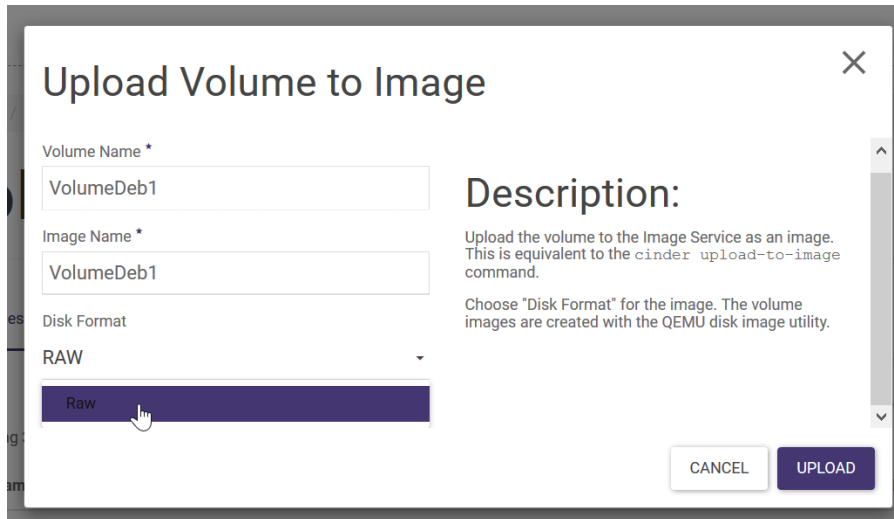
Można zaobserwować, że jednocześnie w panelu Horizon w zakładce Images pojawi się nowa pozycja na liście z informacją o zapisywaniu:



## Download (export) pliku z chmury.

Aby wyeksportować obraz z chmury na lokalną stację roboczą, uprzednio należy utworzyć obraz wolumenu (zakładka Volumes, akcja dla wybranego wolumenu „upload to image”):





Gdy już obraz zostanie stworzony, używając API można zapisać lokalnie obraz wykonując polecenie:

```
ubuntu@ubu1: ~
ubuntu@ubu1:~$ openstack
(openstack) image save --file IMG-Vol2-zapisany-lokalnie.raw IMG-Vol2-zrodlowy
```

```
ubuntu@ubu1: ~
ubuntu@ubu1:~$ pwd
/home/ubuntu
ubuntu@ubu1:~$ ls -sh IMG-Vol2-zapisany-lokalnie.raw
1.1G IMG-Vol2-zapisany-lokalnie.raw
ubuntu@ubu1:~$
```

## Utworzenie maszyny z własnego (zaimportowanego obrazu)

Należy wykonać następujące kroki:

- i. utworzenie wolumenu z obrazu
- ii. utworzenie instancji (wirtualnej maszyny)

KROK 1. Utworzenie wolumenu z obrazu.

Z poziomu panelu Horizon:

### Create Volume

**Volume Details**

Name \*

Description

Use image as a source

Type: fast      Size (GB) \*: 100

Availability Zone \*: AZ3

Volumes are block devices that can be attached to instances.

Volume and Snapshot Quota (GB) (1000 Max)  
49%

391 Current Usage  
100 Added  
509 Remaining  
Volume Quota (10 Max)

60%

5 Current Usage  
1 Added  
4 Remaining  
Volume Type Description:

✕ CANCEL
✓ CREATE VOLUME

Przy użyciu API:

```

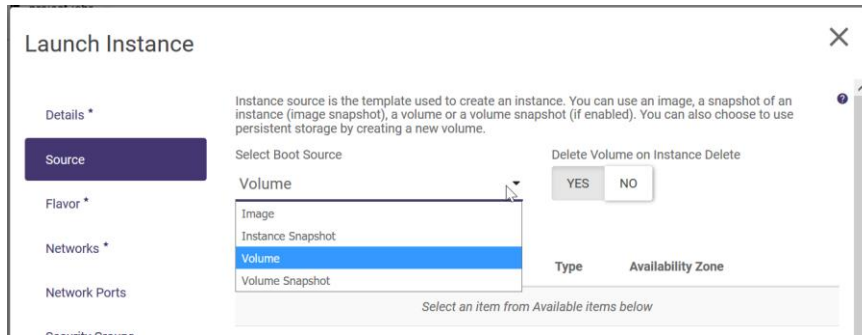
ubuntu@ubu1: ~
ubuntu@ubu1:~$ openstack
(openstack) volume type list
+-----+-----+-----+
| ID          | Name      | Is Public |
+-----+-----+-----+
| 7c2c5e13-0562-4bdd-bf04-2ef3796382fb | fast      | True      |
| 70f78038-911e-48d2-966a-3e3a8af37caf | standard  | True      |
+-----+-----+-----+
(openstack) volume create --size 100 --type fast --image test-flat.raw --bootable test-flat-volume
+-----+-----+
| Field      | Value                                           |
+-----+-----+
| attachments | []                                              |
| availability_zone | nova                                           |
| bootable    | false                                          |
| consistencygroup_id | None                                           |
| created_at  | 2017-12-01T08:33:50.092752                    |
| description | None                                           |
| encrypted   | False                                          |
| id          | 26f12a2d-0a71-4943-afff-3051a709dbae         |
| multiattach | False                                          |
| name        | test-flat-volume                              |
| properties  |                                                 |
| replication_status | None                                           |
| size        | 100                                            |
| snapshot_id | None                                           |
| source_volid | None                                           |
| status      | creating                                       |
| type        | fast                                           |
| updated_at  | None                                           |
| user_id     | 3c459b2cbb49ea8b5f30317f5fbcc4              |
+-----+-----+
(openstack)
  
```

Komenda „volume type list” – listuje dostępne profile storage’owe. W tym przypadku użyty został profil szybki.

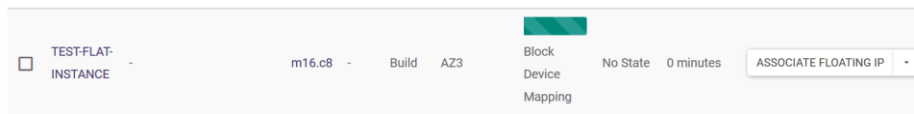
Komenda „volume create” – tworzy wolumen. Właściwość –size określa rozmiar w GB, --type to rodzaj storage’u (patrz wyżej), --image to nazwa obrazu użytego do tworzenia wolumenu, --bootable (bez podawania wartości) ustawią flagę wolumenu na bootowalny. Na końcu należy podać nazwę nowo tworzonego wolumenu.

KROK 2. Utworzenie instancji z wolumenu.

Standardowa ścieżka w panelu Horizon polega na użyciu kreatora. Należy wybrać Volume jako źródło i wskazać utworzony z obrazu wolumen. Warto zaznaczyć opcję „NO” dla właściwości „Delete Volume on Instance Delete” – ułatwia to wiele późniejszych potencjalnych operacji na wolumenie.



Tworzenie instancji – w zakładce Instances widać progres – tworzenie maszyny.



A po chwili – maszyna gotowa:

