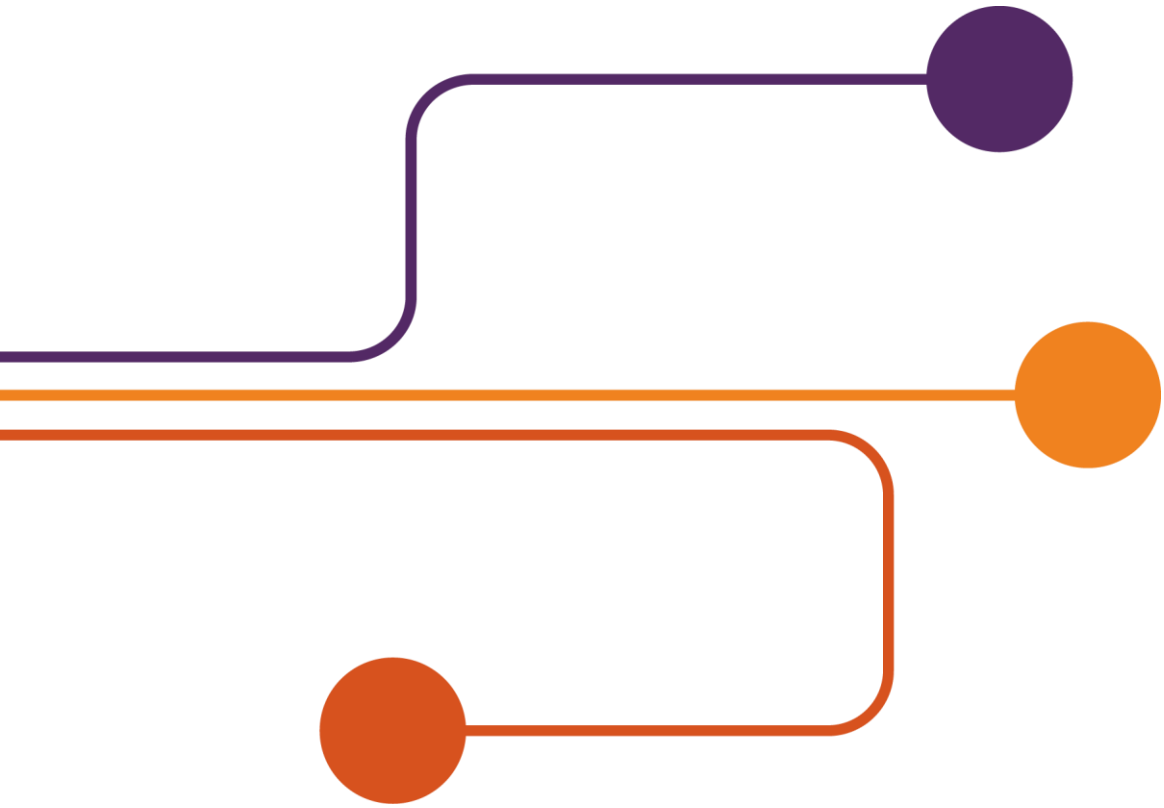
# Przewodnik użytkownika
# Atman Cloud



**ATM S.A.,** ul. Grochowska 21a, 04-186 Warszawa
tel. 22 51 56 100, 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**

# Spis treści

# 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.

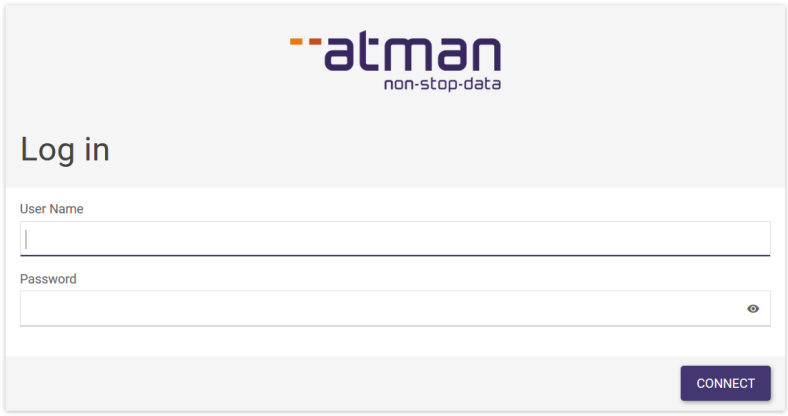
# Logowanie do panelu i zmiana hasła

KROK 1

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

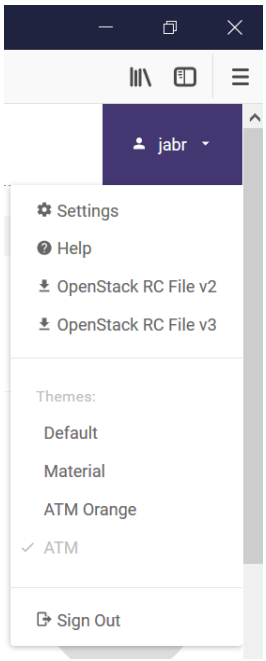
KROK 2

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




KROK 3

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

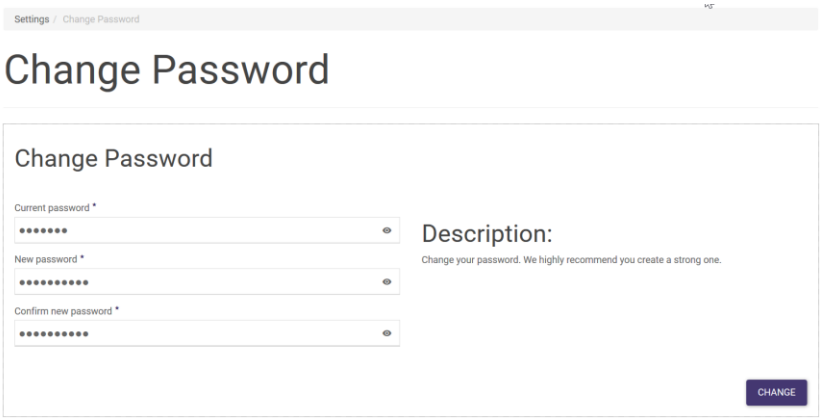



KROK 4

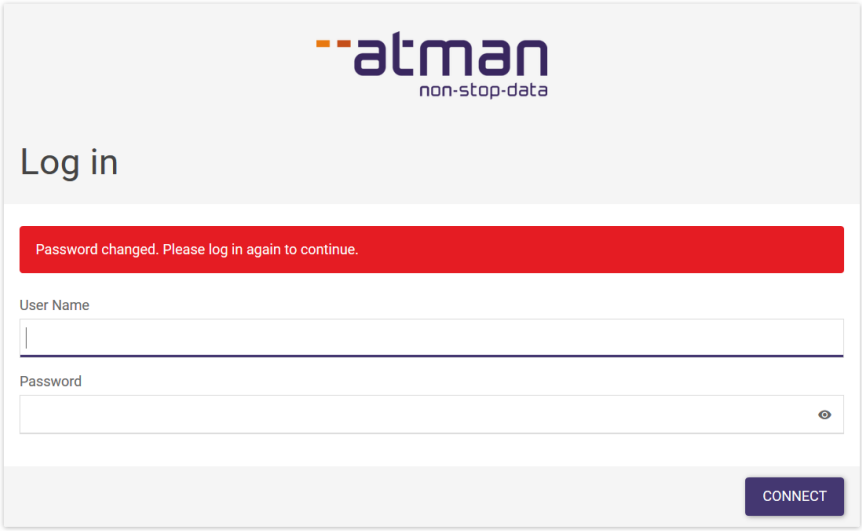
W głównym menu panelu, po lewej stronie ekranu pojawi się na samym dole listy zakładka Settings, pod którą należy wybrać Change Password.

KROK 5

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




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

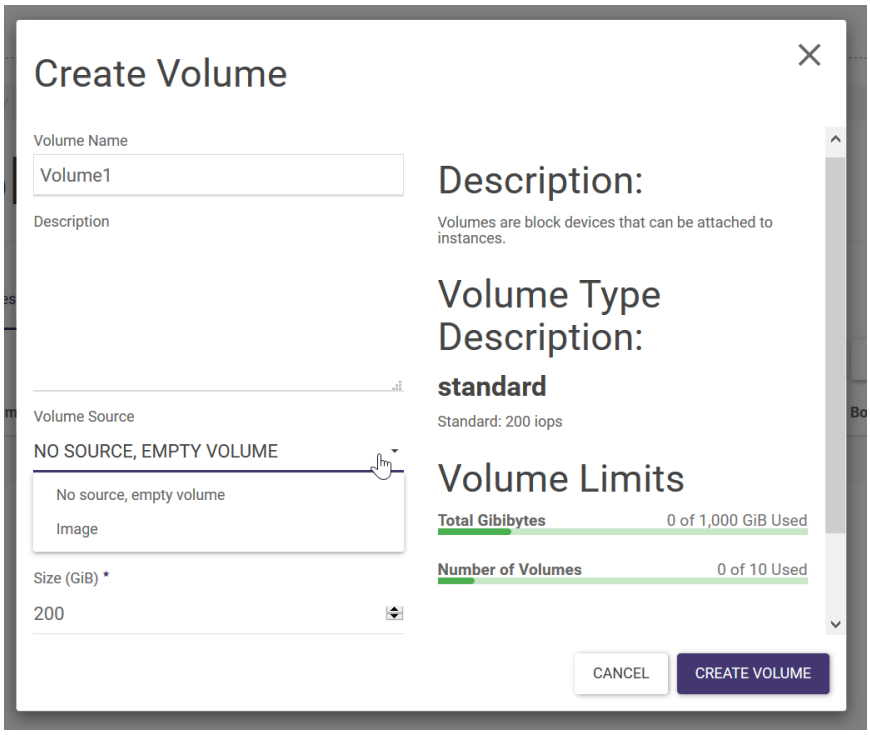



# Wolumeny (przestrzeń dyskowa)

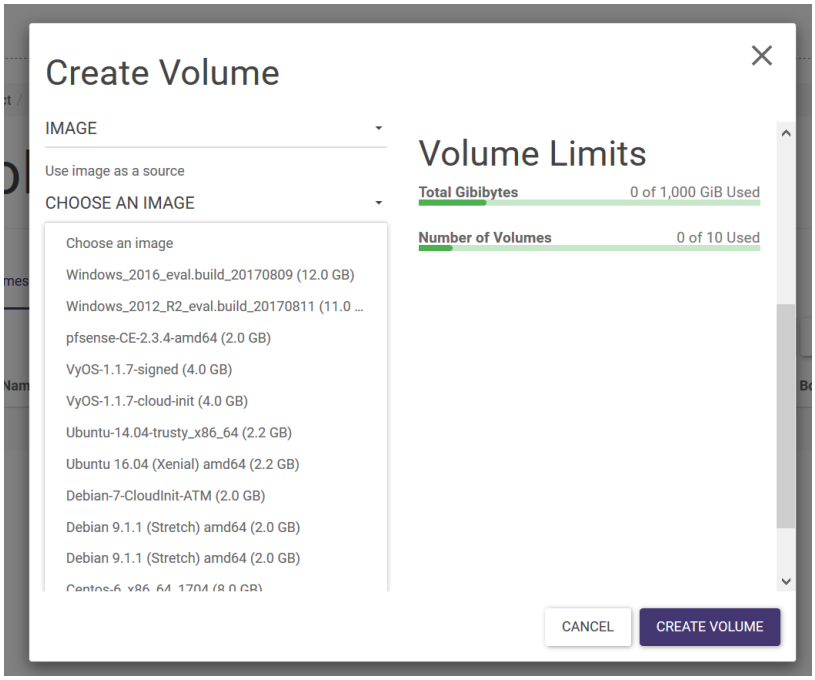
## Tworzenie wolumenu

KROK 1

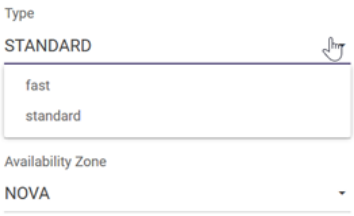
Z głównego menu (lewa strona ekranu), należy rozwinąć Compute a następnie kliknąć Volumes. W centralnej części ekranu należy kliknąć +Create Volume. Pojawi się kreator:




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:




KROK 2

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

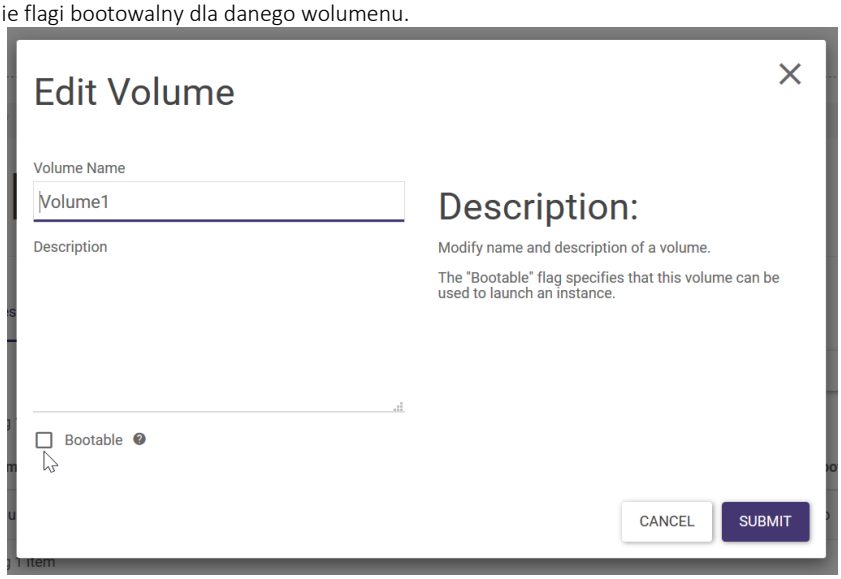
| Name | Description | Size | Status | Type | Attached To | Availability Zone | Bootable | Encrypted | Actions |
|---|---|---|---|---|---|---|---|---|---|
| Volume1 | - | 10GiB | Available | standard | | nova | Yes | No | EDIT VOLUME |

## 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.



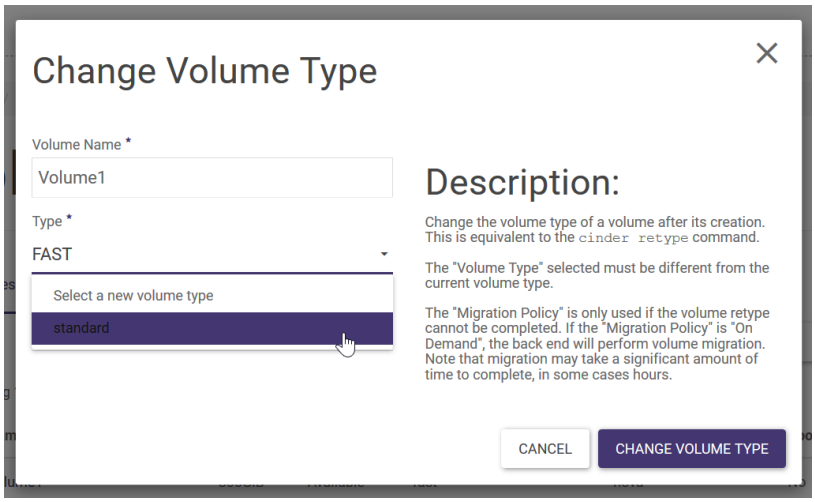

## Zmiana typu

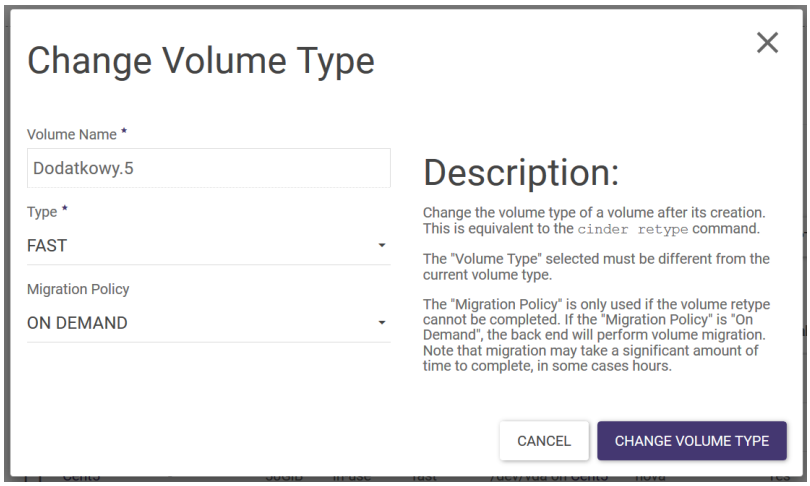
Można zmienić typ wolumeny (standard <-> fast) wybierając na ekranie Project→Compute→Volumes po prawej stronie wolumenu akcję CHANGE VOLUME TYPE. Zmiana może zająć znaczącą ilość czasu w zależności od rozmiaru wolumenu oraz rodzaju danych. Typ wolumenu można zmienić w przypadku gdy wolumen jest dodatkowy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

a) głównego wolumenu instancji

b) wolumenu dodatkowego, ale podłączonego do działającej instancji

W kreatorze zmiany typu Migration Policy należy ustawić na wartość ON DEMAND

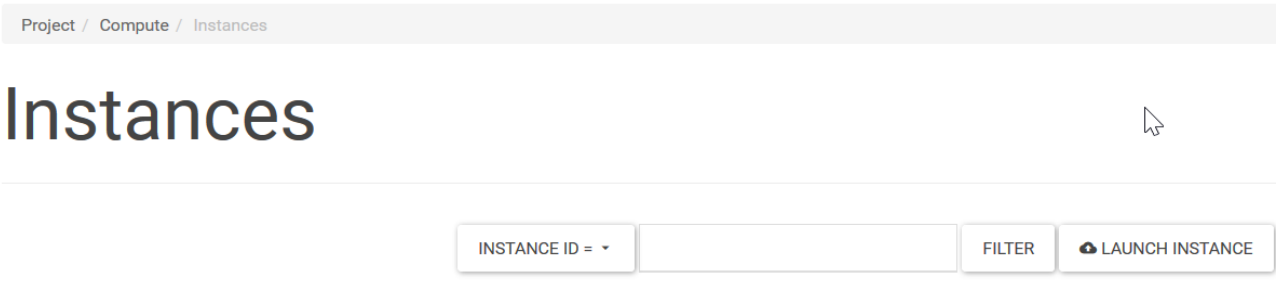


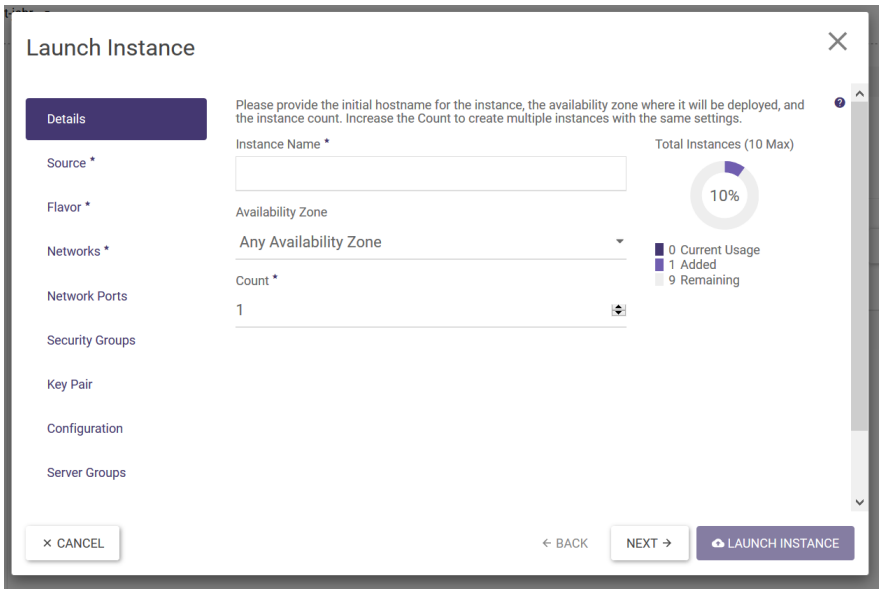

# Instancje (wirtualne maszyny)

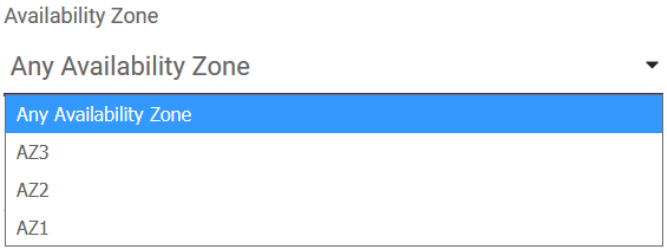
## Tworzenie instancji

KROK 1
Z ekranu Project→Compute→Instances należy kliknąć LAUNCH INSTANCE.



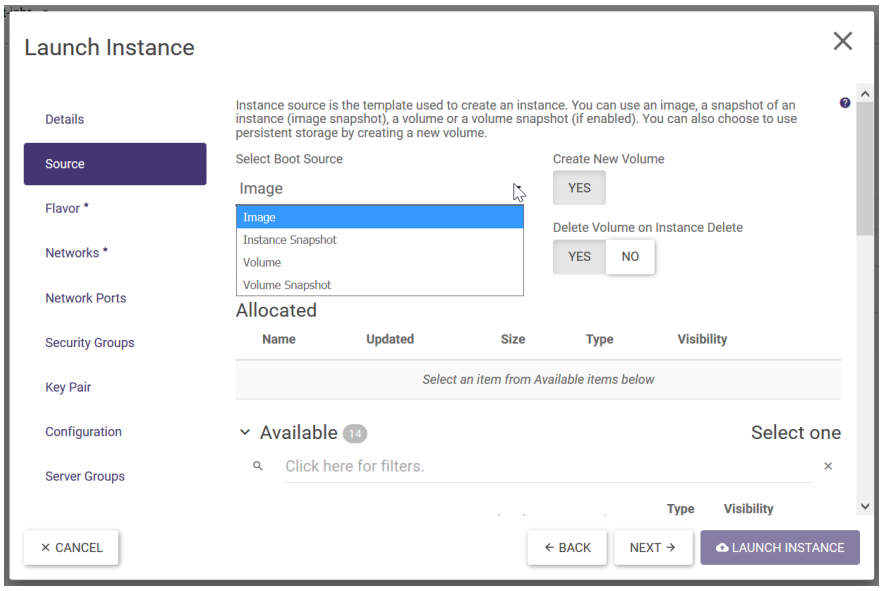

KROK 2
W zakładce Details należy podać nazwę instancji, a także określić ile sztuk takich instancji ma zostać wykreowanych. Dodatkowo można ograniczyć występowanie/działanie instancji do konkretnej strefy dostępności, tzw. Availability Zone (więcej: patrz praktyczne uwagi).

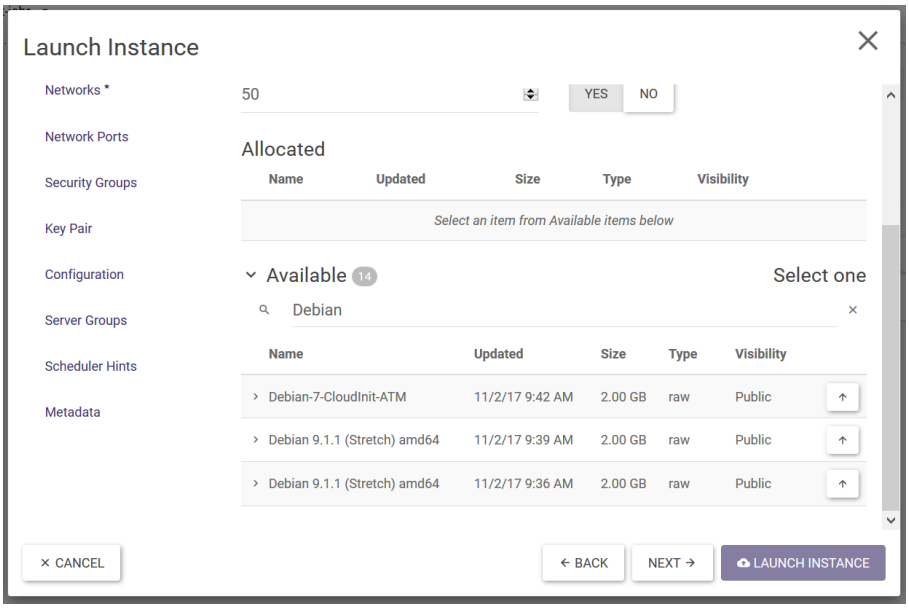



KROK 3

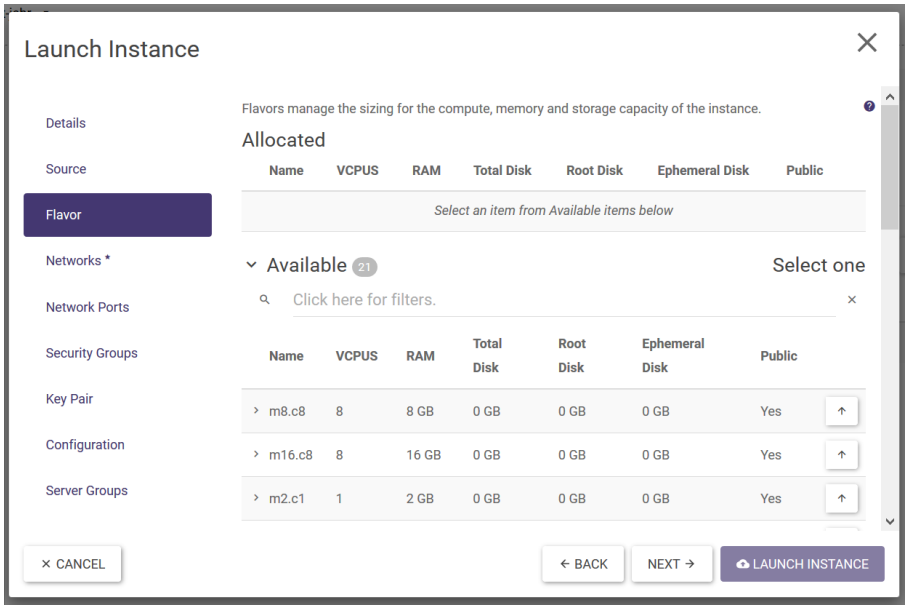
W zakładce Source należy wybrać źródło bootowania. Wybór wartości Image pozwala na szybkie uruchomienie maszyny w jednym etapie używając tylko omawianego tu kreatora. Wybór wartości Volume jest bardziej uniwersalnym sposobem, wymaga on jednak uprzedniego utworzenia wolumenu. Patrz również praktyczne 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.





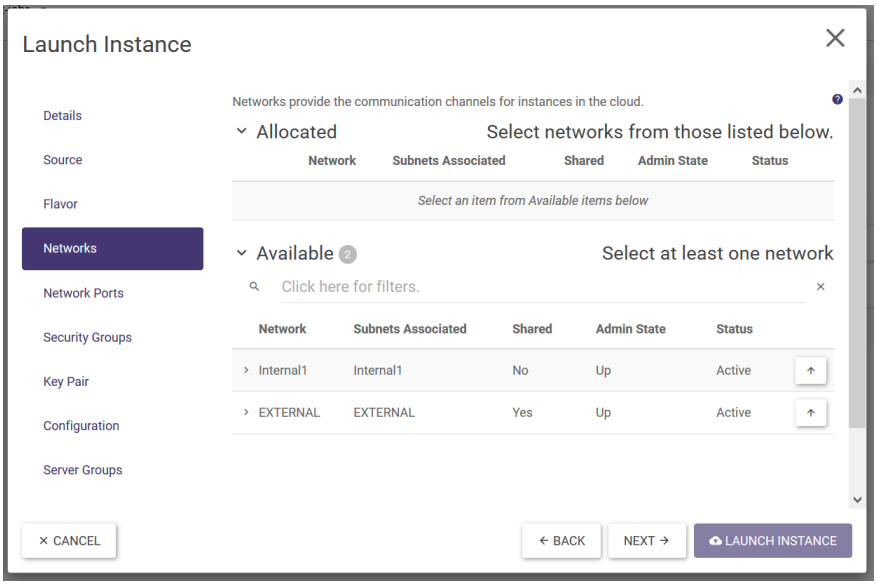

KROK 4

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



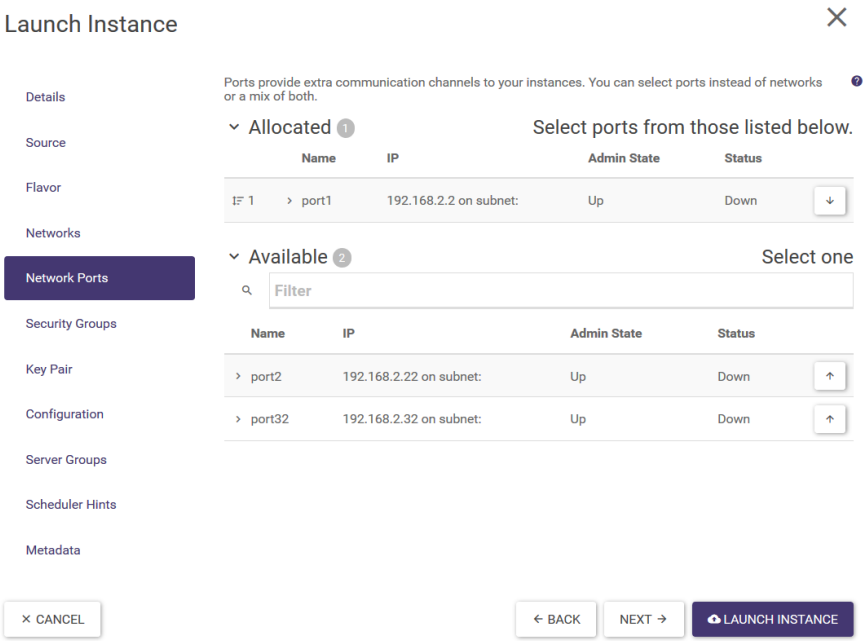

KROK 5

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



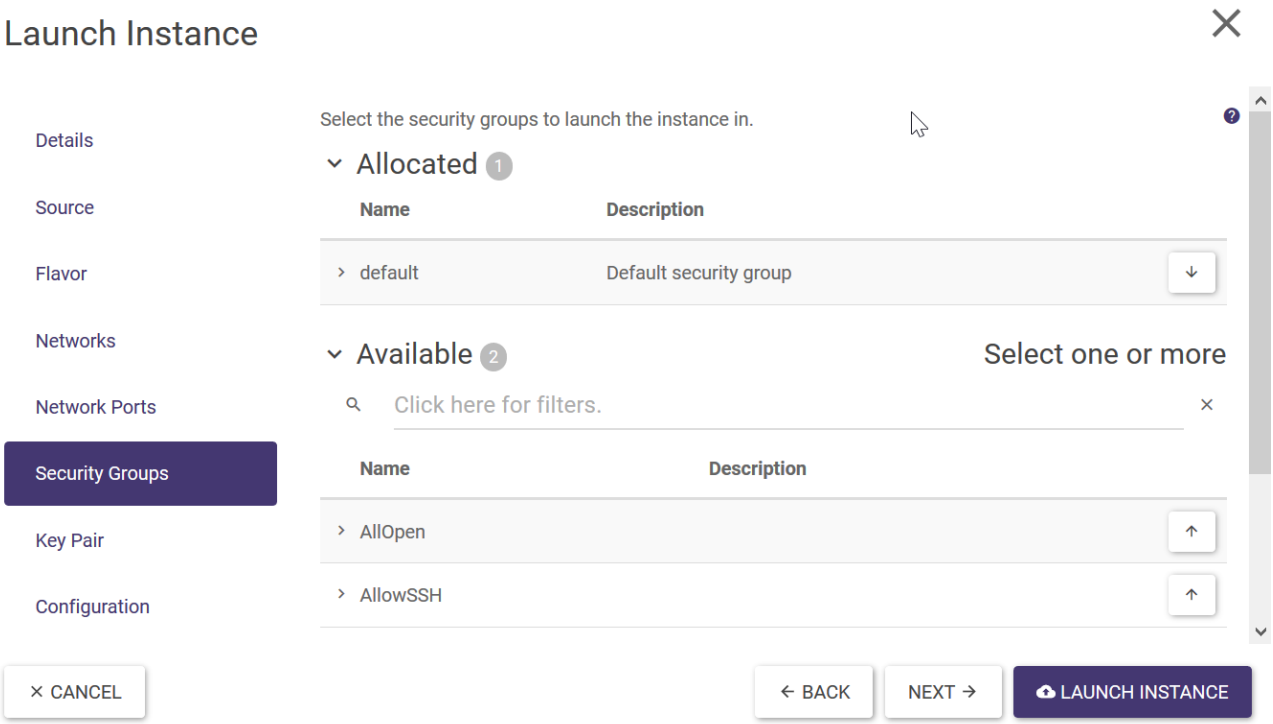

KROK 6

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.

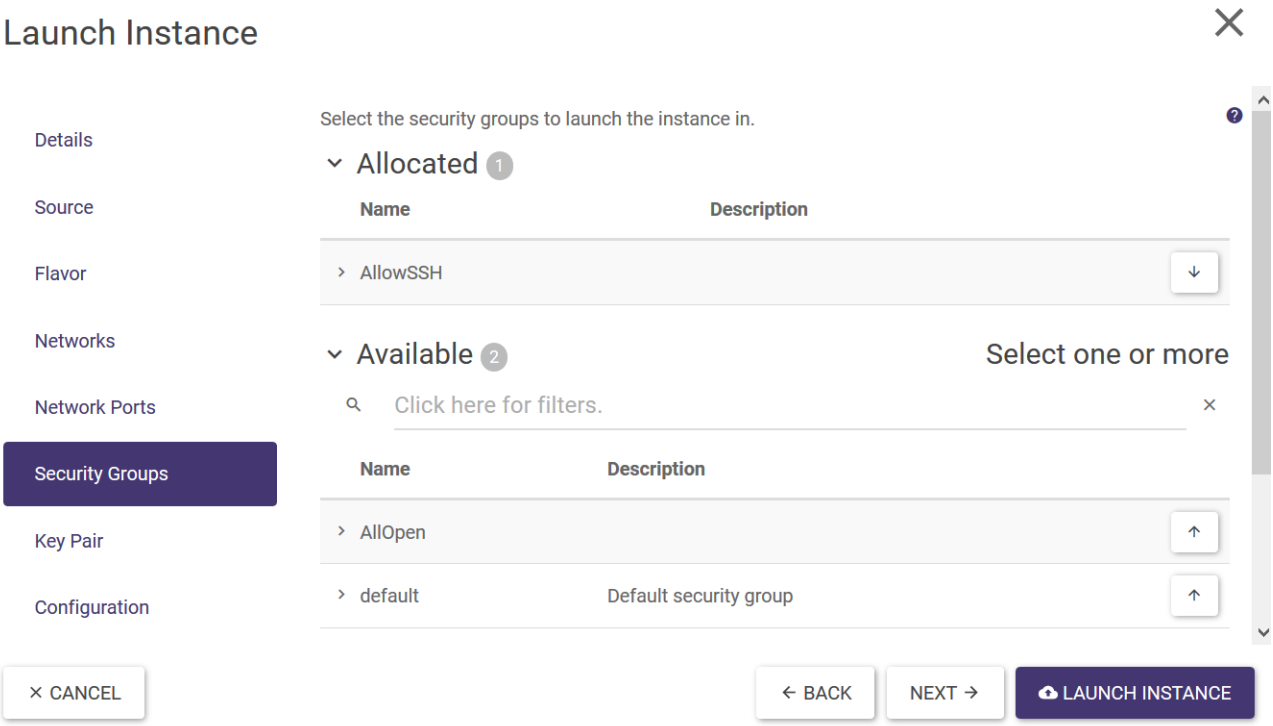


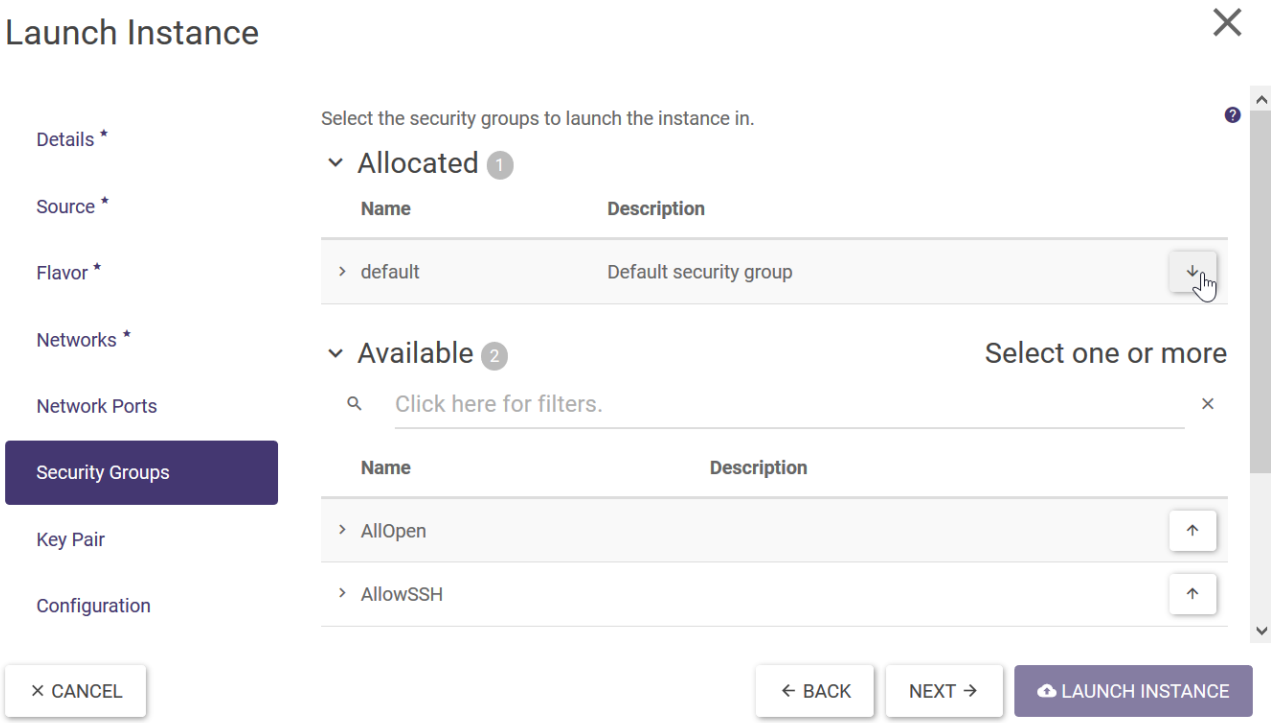

KROK 7

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



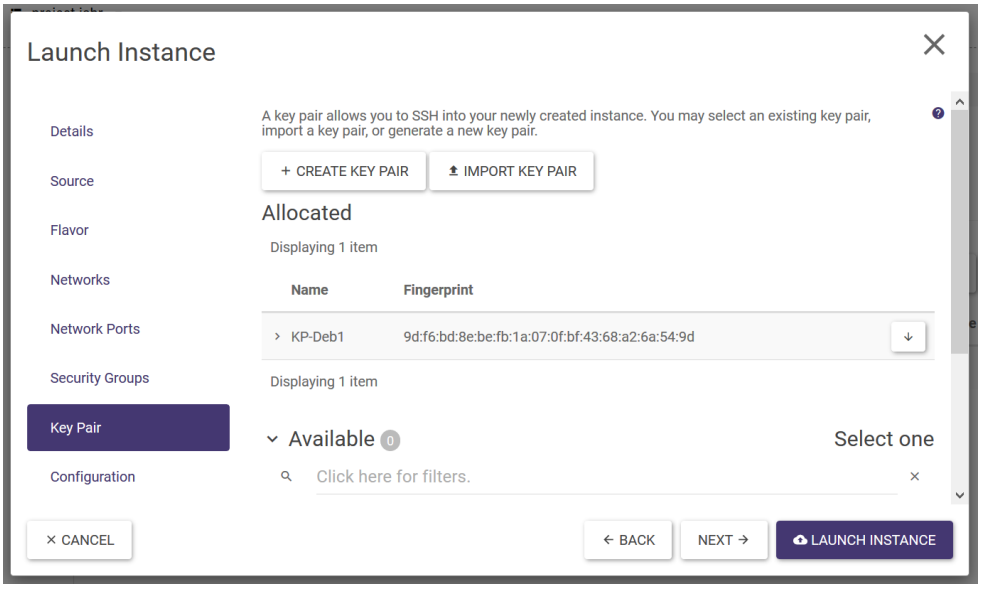

Używając przycisków z symbolami strzałek należy przypisać pożądaną grupę zabezpieczeń:





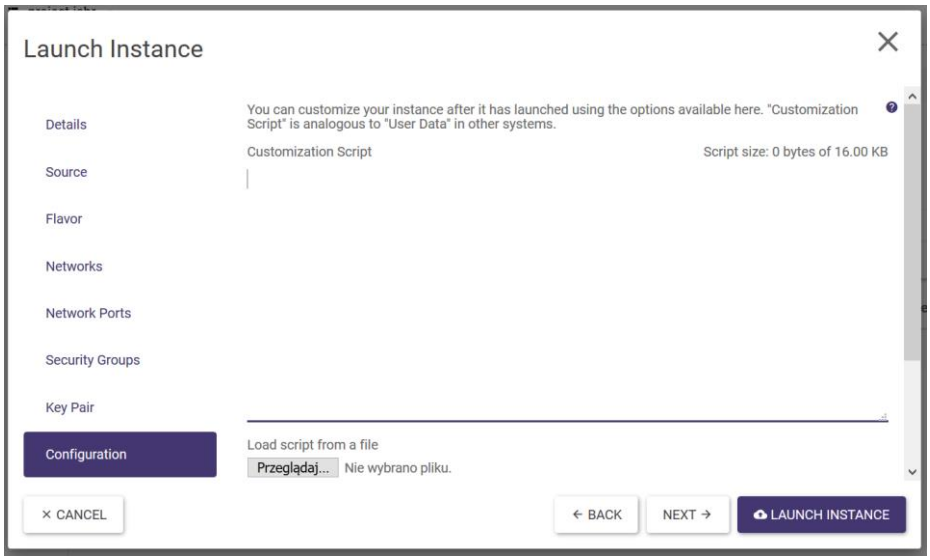

KROK 8

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).




KROK 9

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



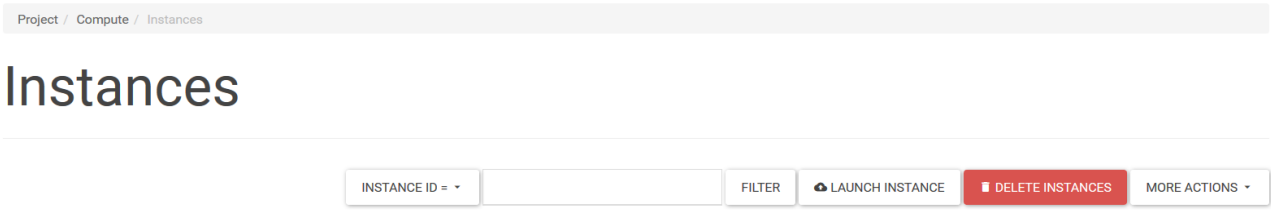

KROK 10

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.

| Instance Name | Image Name | IP Address | Flavor | Key Pair | Status | Availability Zone | Task | Power State | Time since created | Actions |
|---|---|---|---|---|---|---|---|---|---|---|
| Ubu1 | - | 195.167.156.60 | m8.c8 | - | Active | AZ1 | None | Running | 1 week | CREATE SNAPSHOT |

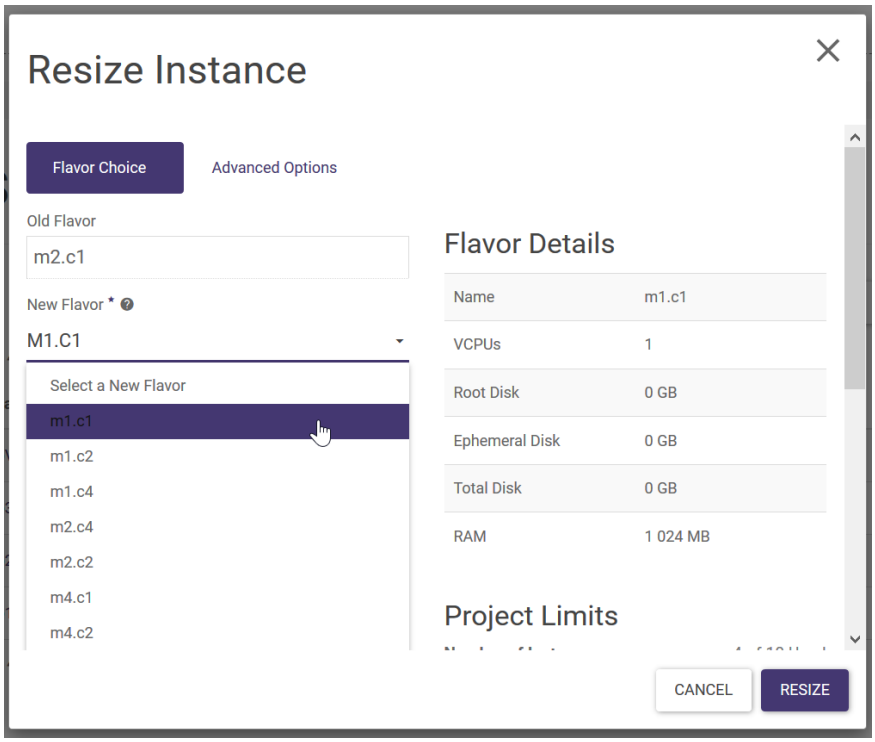
## Usuwanie instancji

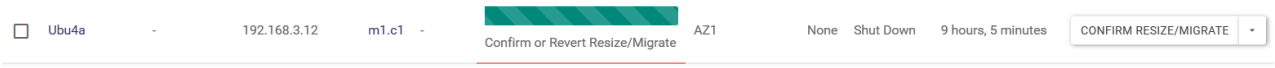
Instancję można usunąć uruchamiając akcję DELETE INSTANCE na wybranej instancji na liście ekranu Project → Compute → Instances. Większą liczbę instancji można usunąć zaznaczając instancje przeznaczone do usunięcia na liście a następnie kliknięcie przycisku DELETE INSTANCES.




## 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 siecie wewnętrznej, musi być włączone DHCP – patrz również rozdział „Sieci wewnętrzne”.

UWAGA 2. Strefy dostępności.

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 winnej 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
```

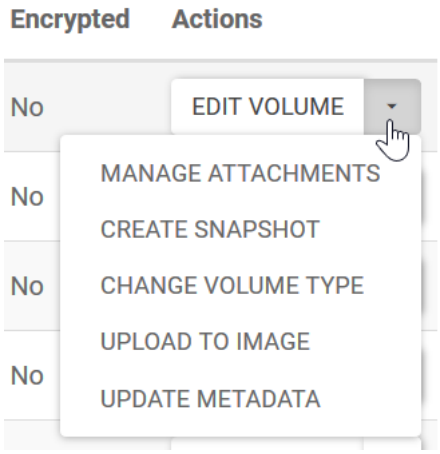
W przypadku systemu Linux Debian należy takiego użytkownika stworzyć – tu: debian. W polu Customization Script należy wpisać:

```
#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
```

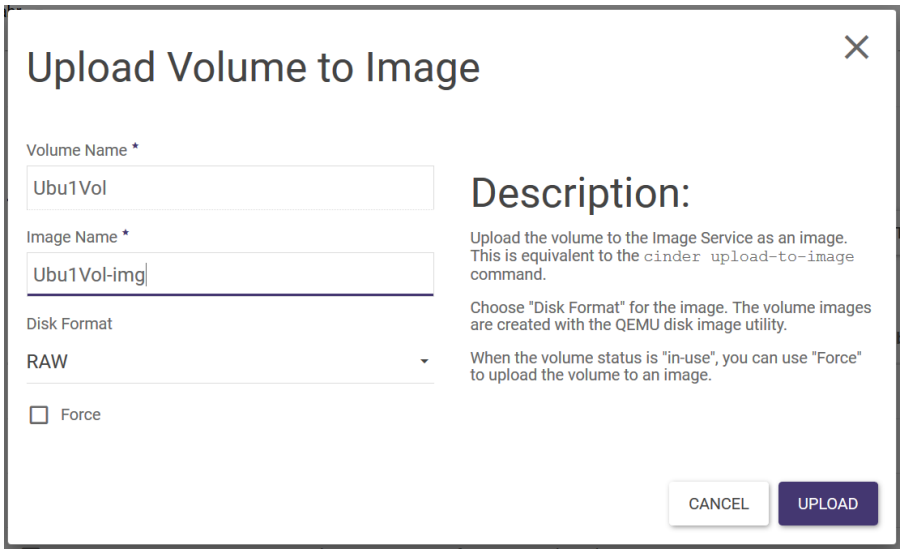
# Obrazy

## Tworzenie obrazu

KROK 1
Z ekranu Project→Compute→Volumes z akcji dla wybranego wolumenu należy wybrać UPLOAD TO IMAGE:

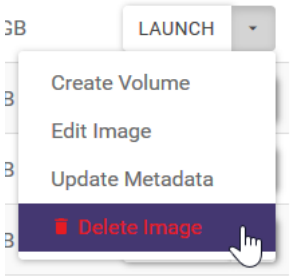



KROK 2
W kreatorze należy wpisać nazwę obrazu i potwierdzić tworzenie przyciskiem UPLOAD.




## 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).

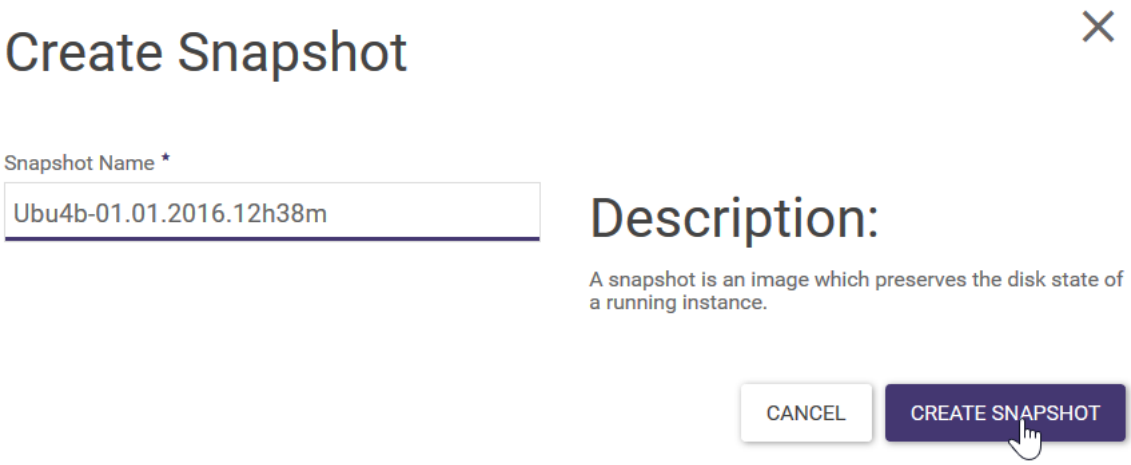
UWAGA 2
Nie można usunąć obrazu z ustawieniami VISIBILITY = PUBLIC.

UWAGA 3
Tworzenie obrazów działa tylko dla wolumenów nieprzypiętych 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.

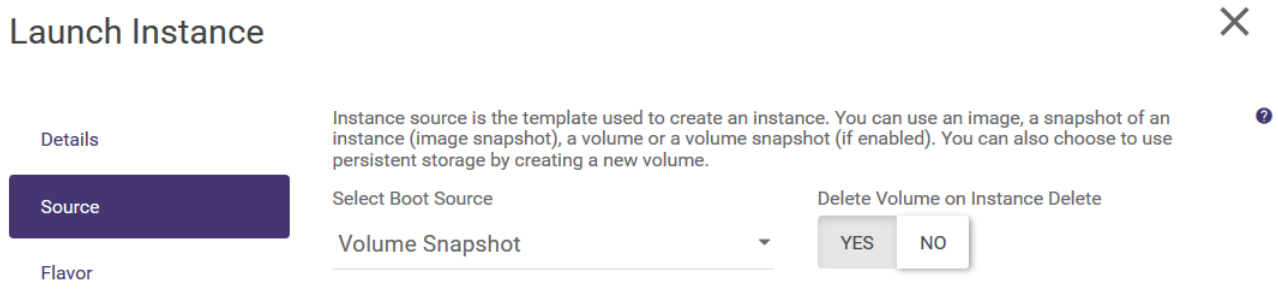



KROK 2
Po kliknięciu CREATE SNAPSHOT zostanie utworzona kopia migawkowa, która od razu pojawia się na liście Project→Compute→Images

## 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 ekranui Project→Compute→Images przyciskiem LAUNCH po prawej stronie dla wybranego obrazu – kopii migawkowej

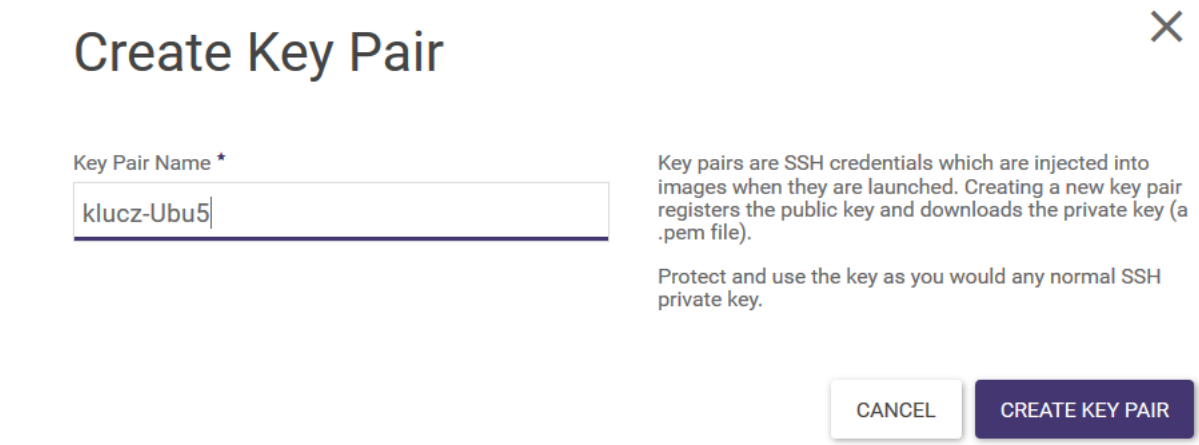
W przypadku sposobu (a) należy pamiętać o wybraniu odpowiedniego źródła source boot, które z kolei dla ścieżki (b) automatycznie jest ustawiane:



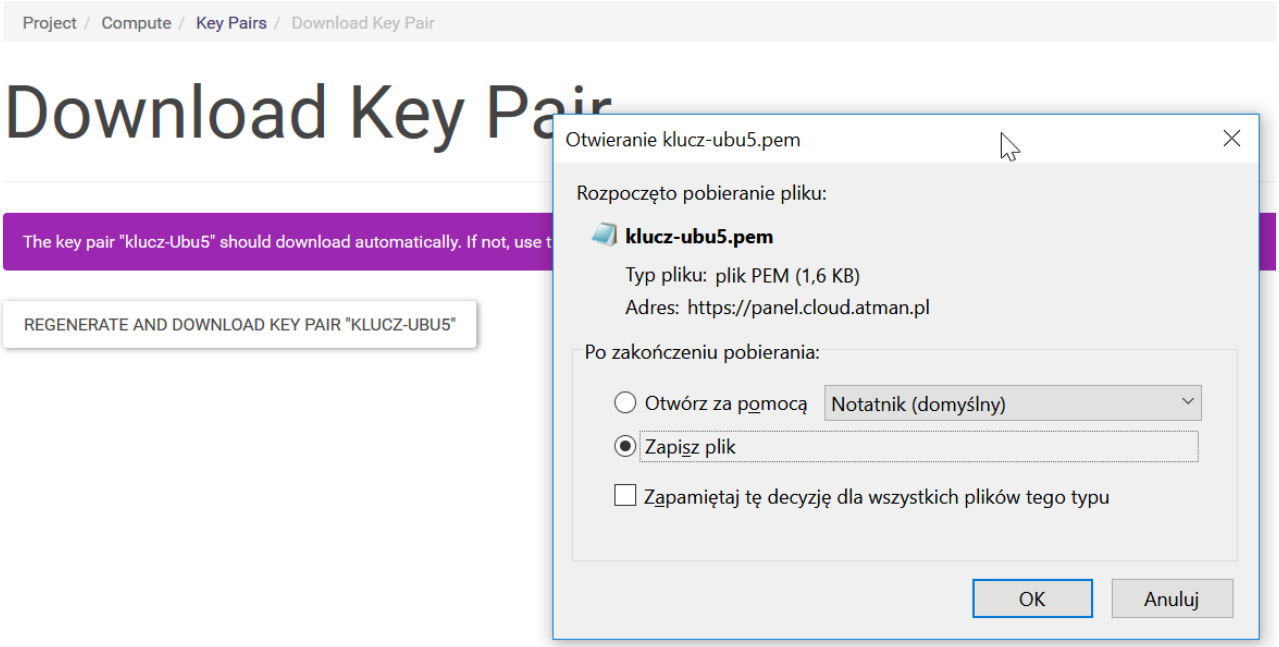

# Klucze SSH

## 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):

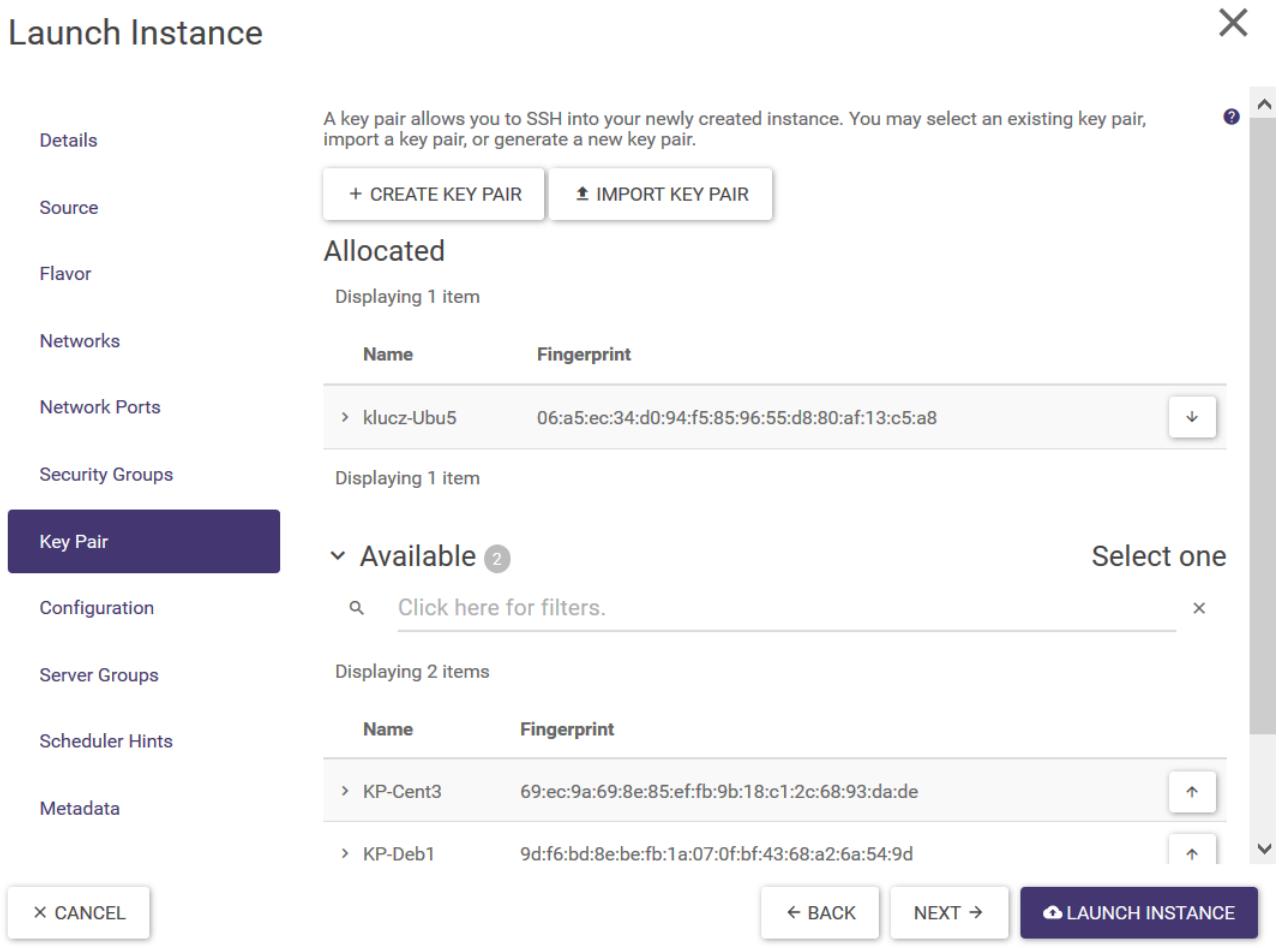



KROK 2
Po potwierdzeniu przyciskiem CREATE KEY PAIR, pojawi się okno pobierania klucza prywatnego który należy zapisać na lokalnej maszynie:




## 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 strzełek. Widać również że poprzednio wykonany krok można również wykonać w kreatorze:




## 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

| Instance Name | Image Name | IP Address | Flavor | Key Pair | Status | Availability Zone | Task | Power State | Time since created |
|---|---|---|---|---|---|---|---|---|---|
| Ubu5 | - | 195.167.156.24 | m1.c1 | klucz-Ubu5 | Active | AZ2 | None | Running | 0 minutes |

KROK 2

Dla systemów Linux:

Przejście 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-----
MIIEpQIBAAKCAQEAyIlDrgqtRyYZkzIrlMXXok+R4slynKyB6H1NjrB1RW+zq4Gk
jUy/hRKrNkFtQnelLhPPTIcVPASz0ZuxCFFnct/7OuUo6EPhhrLXMwdZjTTBlz0L
Zm0nNyb4aioC07XLVxFgMIpPkzCntmWLalQRu3ljWP5xehxETYz1nd+Th0vlZKa8
727MjDwE7nXZXsj4Gw+PfmQVqavxo3l9jvGcq3YWyt+qSQbKwW0/I6xdGv3e8Wnj
L8pLqVVb2nLPSiD7Z4W90j72QaiNwOqGt5t/ddLlonWdhw9TToixOKGdHVDiL5bf
QQIp8pCkrIK9m458+LWqsgrEQ8y4R5Yq02SerQIDAQABAoIBAAvZ2M8TQHRA8yf4
wgyTuI+WBjgR0Z0isLatmQTCttt4o3SSP8g97d+OX+Hf8fYInhFgCFMsdHvMh1fu
zIKCVQu74tvzKPy47j4ImaEhYRBwOrSWXfMapkOjIPEdNHeQecjWdQnJUrSPHoov
7BJHj5i1rsJWnxwpSXwPxYAj81L+dXF0ext/7CDK9uInACqx87BErLcPRMozlzMp
GzPHXk+RpwDSsFpO3Jy/ZRCv/06vAXihJ6NjuWj5/zBNF5+O8QV5iant46GSNnN8
PcykioxwTAiBWnE7tAY42P7RflQ2FyJT9pX6fLgFtwvY67vFP3+EwGRMX88MNXqX
C6QqkiECgYEA59w3QiBVQqWw0//sgcvRD2y+1NLYMm1DqAi9NF+FbhEISYT4R9q6
VxDNCPnC3CLyHgVnZ6BKdy6W9DL7KRKidjDHABMzk7Y+y0nBqBPJwlli0z9vHlr5
eMOw73vU6jgXcy4gUl8bDHojeaBMTAZdma8TpILOJp9wz51Pl216BYkCgYEA3Woq
1QjvIMGnkaBZdzB5PRMGkU9XBMhx+jyGU05Rq6p+SedWSVBGkwvoVmoW+uA6zjta
T17kk9rTBEnJfAC6K0rNVv+FKuzaUvofEXo4gmq1cbbQGd7OczwxovUmQLJM+dnt
/wnjPD0bdzjlw9RyliZA7mK+OmZsZhFJ7nfQqwUCgYEA0YzvCD2usRiM812nBDwQ
C2/OHQ0eRp0H+7NCRTZbonmUUtXxiwd9SDkwBf+thEW1KzrZFQgCpSqfVb9JzfpA
iK9W+5NfFw4sPJDBjMWtoJAmyCPZqsawF9xNanQxnynoz7mNjsTT7nfo3gDpVACg
0cgw6YsrBC8vxwQ3LfXMxXkCgYEAtX6md5RoOAil7EhtrbbtWrPyyUApC4GndEES
tszXQ4lxFfFsmJIWF8lF/TffeGw/p/edErytT8mq+bPmViBeeshJQ8wWg9Y9LJFc
0D3Ifpcr/nelY99wiaNI6NRdM+E0GgabAVlAjItmrTbVmM3YCFS5Gu+UEVkN+Cip
2rEaOmUCgYEAlh32lrWeRen3KbZJ/VQ8mjnbzodc+157TQS8ttoomr5smjZPLpRs
4na1qWLZI6W/naUAvou7VO2IULOTs9HSpwKkePZ7evivXNKGP55j6gB/Jd2VwX0H
Ej+mQ2UmdLKSeYCdwV0VwSrJrk23HYnnGy8u5b+L4hmR8QWxSSqAh/g=
-----END RSA PRIVATE KEY-----

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

Następnie zmiana uprawnień:

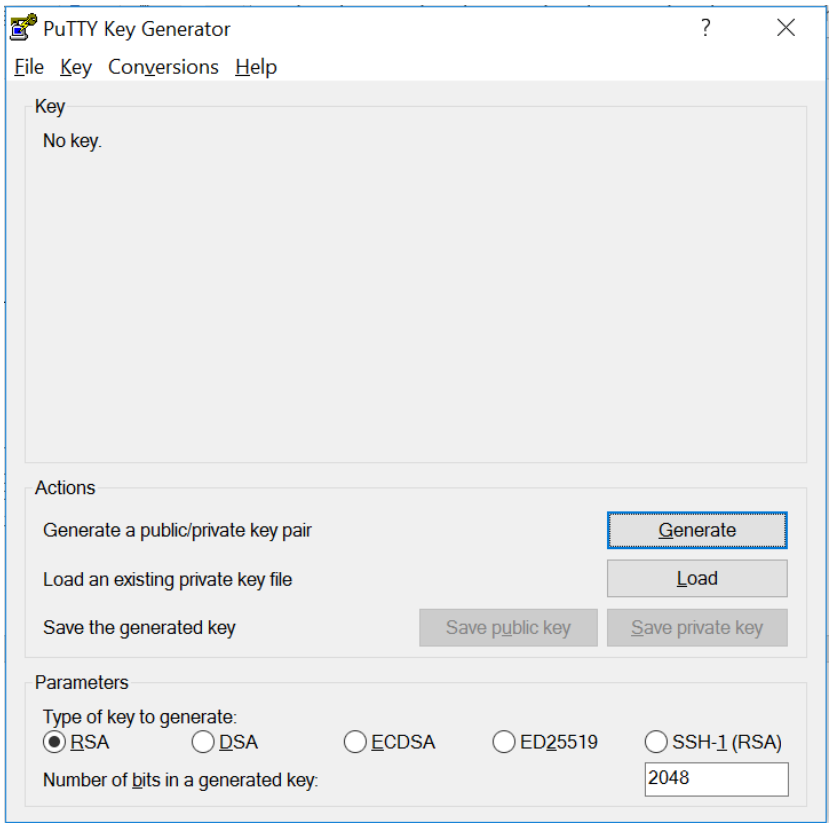
ubuntu@ubu1: ~/.ssh

```
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$
```

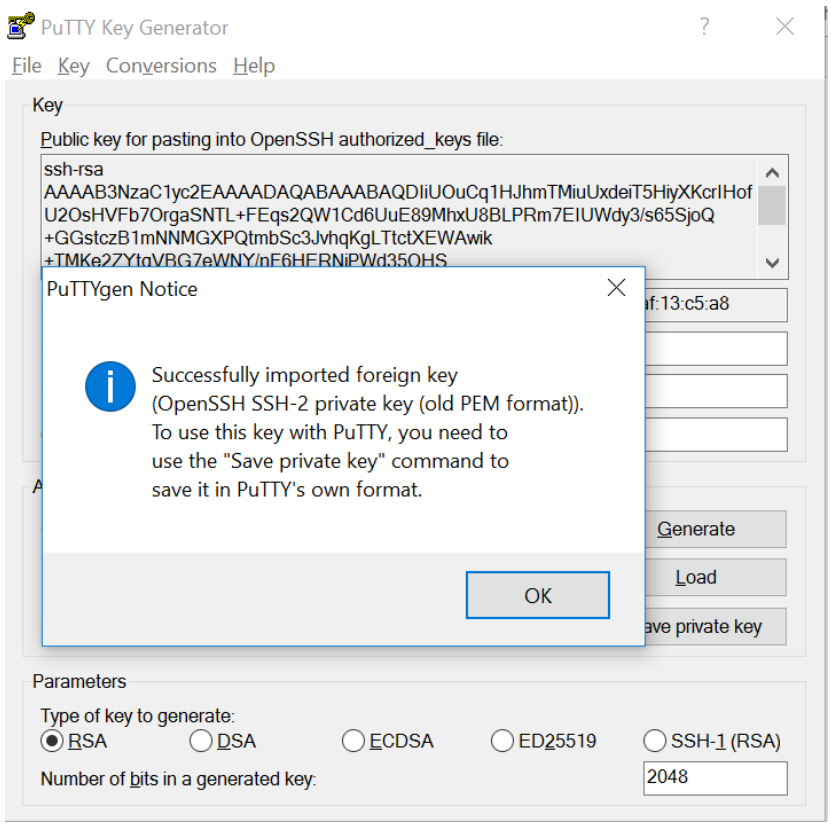
Dla systemów Windows:

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

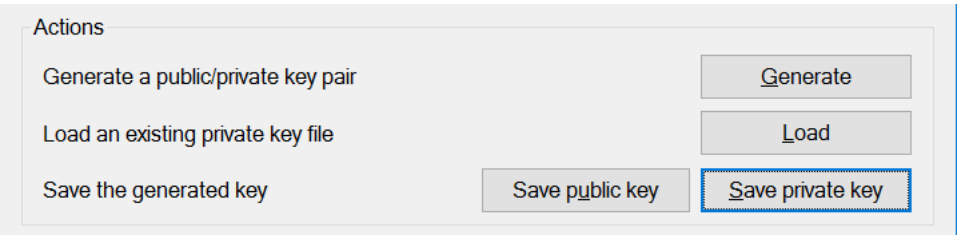
Należy uruchomić program PUTTYGEN.EXE:




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.

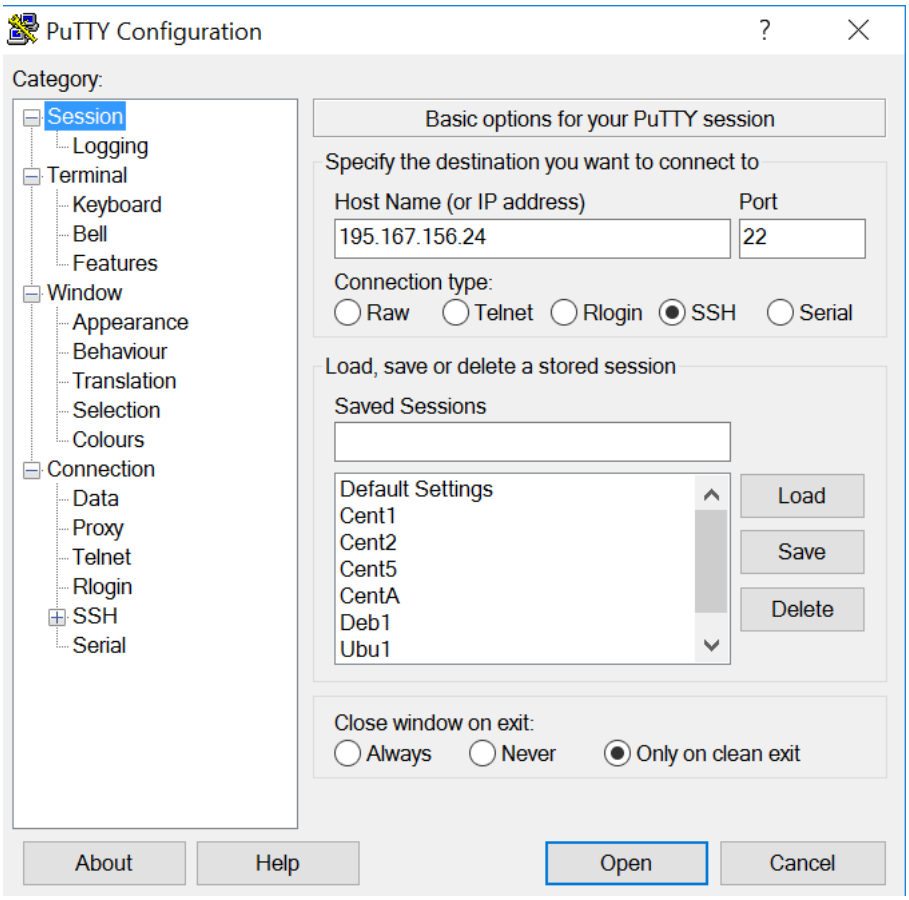
Dla systemów Linux:

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

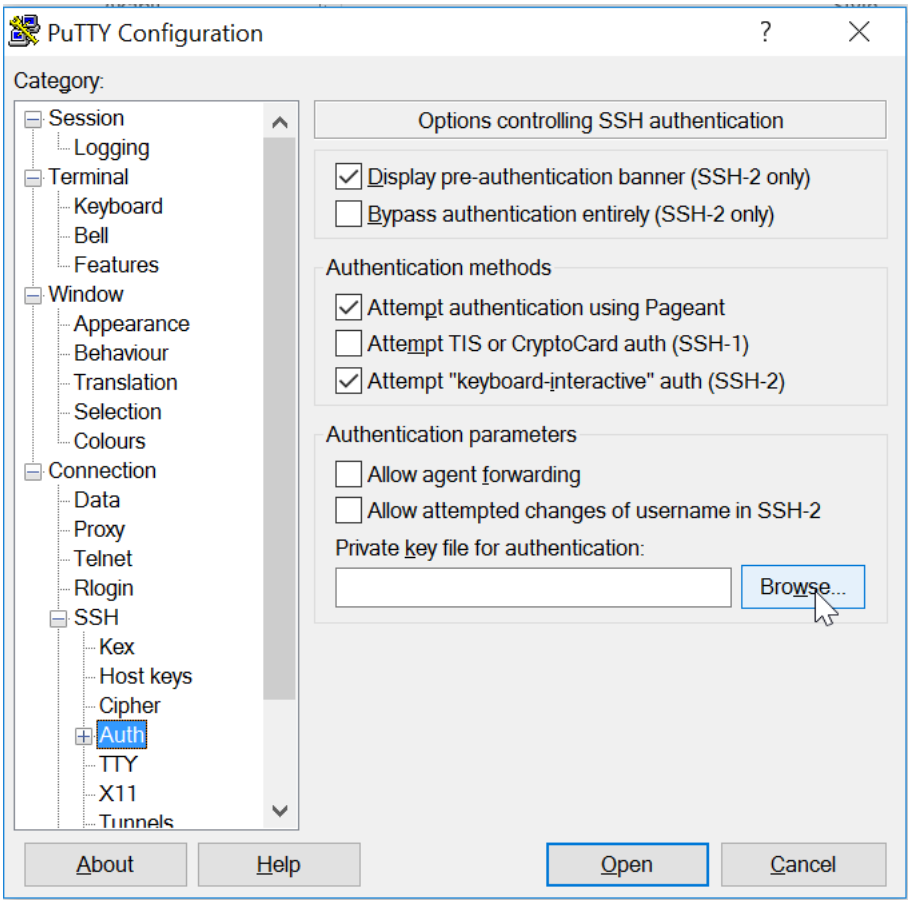

Dla systemów Windows:

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

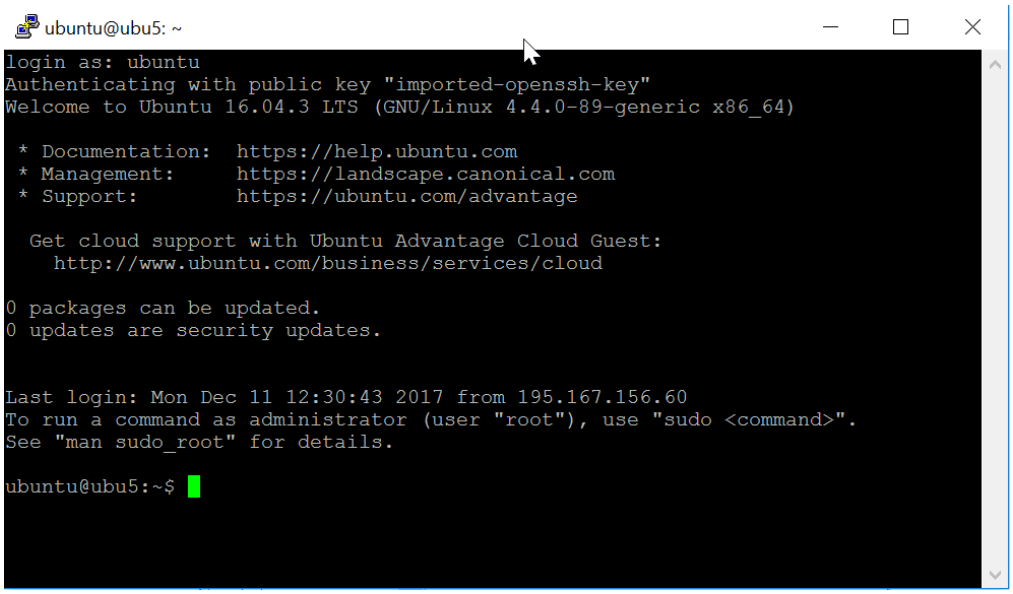
Adres IP:




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

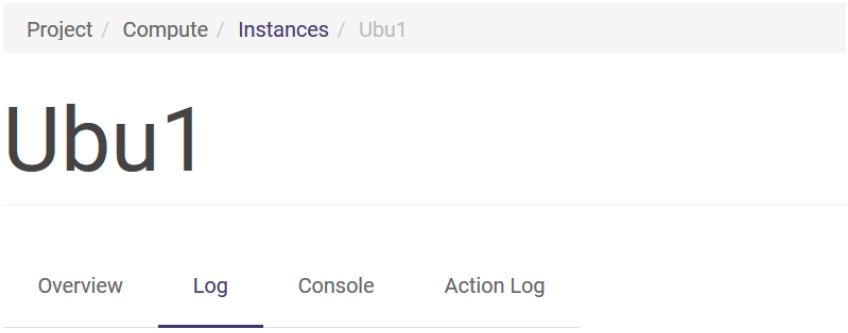



Po kliknięciu przycisku Open w oknie PuTTY Configuration, następuje otwarcie sesji. Należy wpisać użytkownika (tu, domyślnie dla Linux Ubuntu: ubuntu):

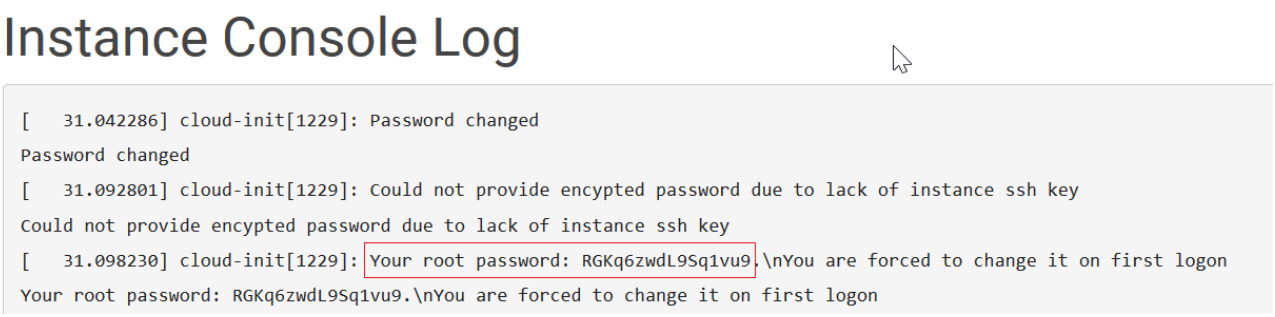



## Hasło administratora do instancji

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:

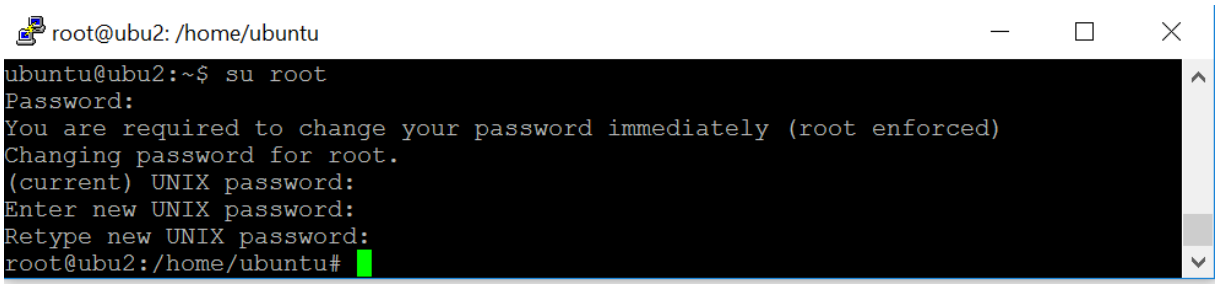



W logach znajduje się hasło root:




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 logowanie 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):



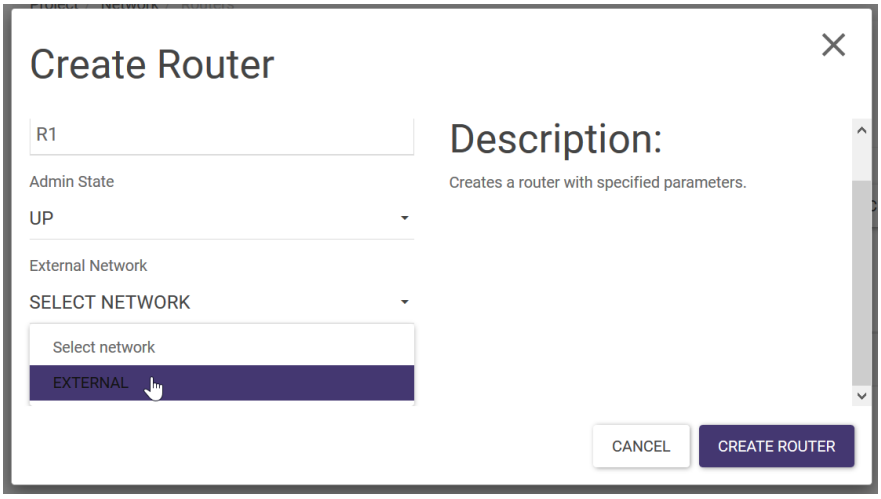

# Router

## 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 (patrze też: autogenerowanie hasła root, dhcp sieci wewnętrznej)

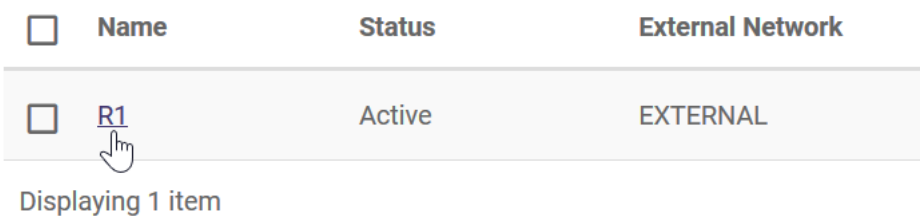
KROK 1
Na ekranie Project→Network→Routers klikamy +CREATE ROUTER

KROK 2
W kreatorze należy nadać nazwę oraz podpiąć sieć zewnętrzną, a następnie potwierdzić klikając przycisk Create Router:

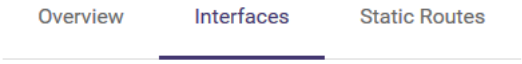



## Dodanie interfejsu LAN

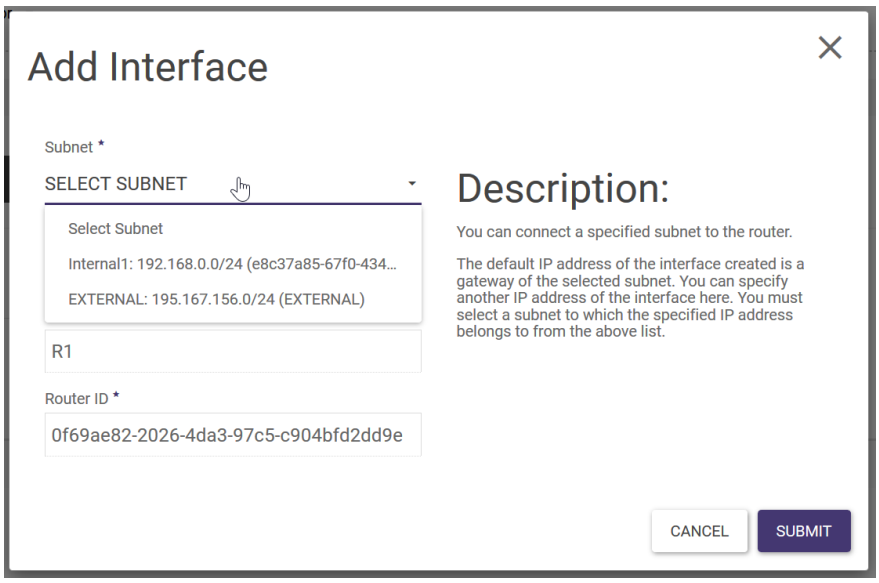
KROK 1
Należy kliknąć na nazwę routera na liście:




KROK 2
Po przejściu do zakładki Interfaces należy kliknąć +ADD INTERFACE



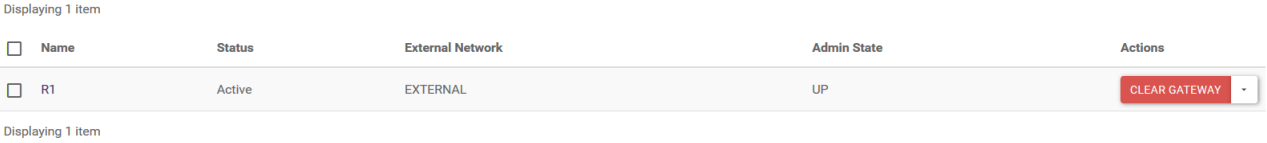

KROK 3
W kreatorze należy wybrać stworzoną wcześniej sieć wewnętrzną a następnie potwierdzić przyciskiem SUBMIT:



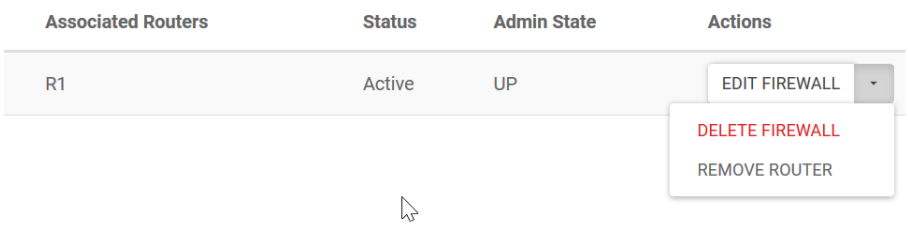

## Usunięcie routera

Aby usunąć router, należy najpierw wszystkie zależności:

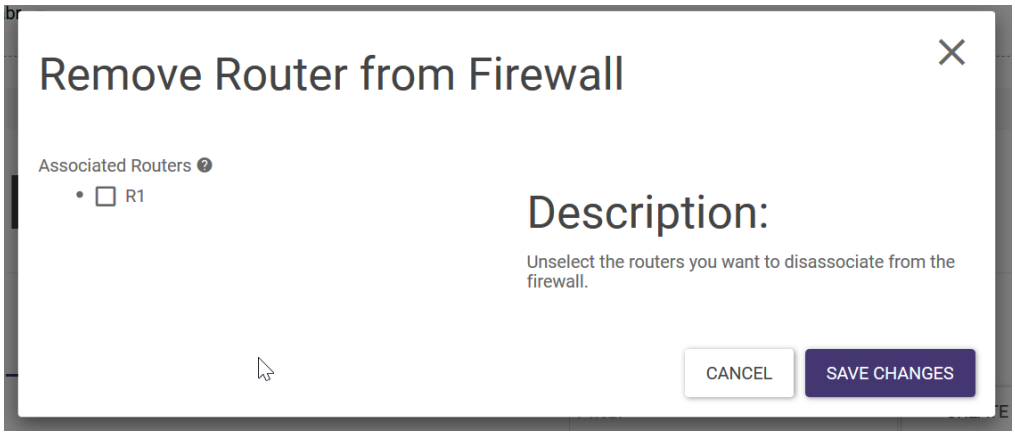
KROK 1
Po prawej stronie routera na liście aktywności należy wybrać CLEAR GATEWAY




KROK 2
Odwiązanie routera z Firewalla. Na ekranie Project→Network→Firewalls, należy z listy actions wybrać REMOVE ROUTER.

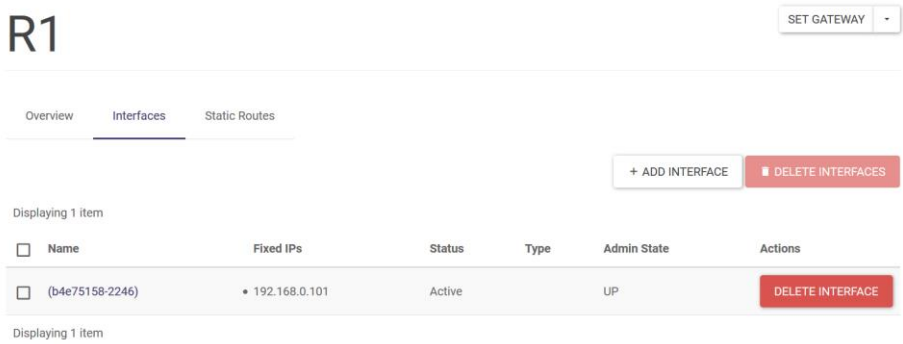



KROK 3
W kreatorze należy odznaczyć router a następnie potwierdzić zmianę przyciskiem SAVE CHANGES

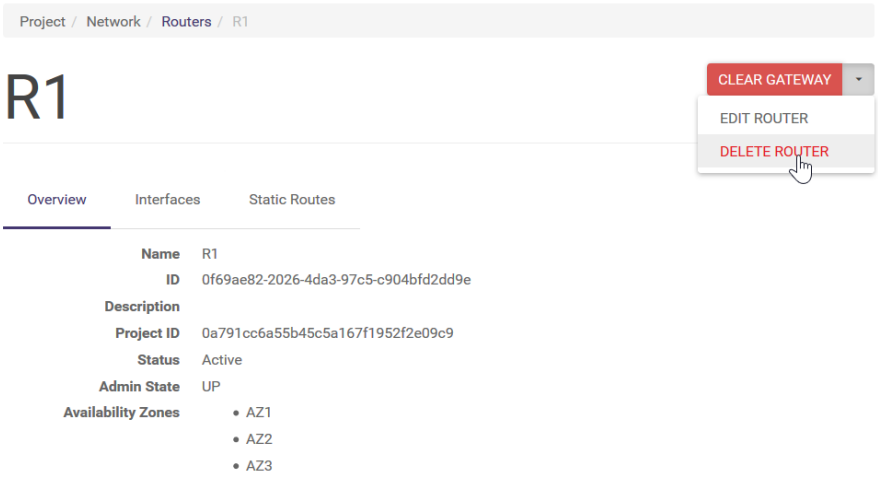



Po zmianie statusu z Pending Update na Active można przejść do następnego kroku.

KROK 4
Usunięcie interfersju LAN. Po przejściu do ekranu Project→Network→Routers a następnie kliknięciu nazwy routera, który chcemy usunąć, przechodzimy na zakładkę Interface. Usuwamy wszystkie interfejsy poprzez funkcję DELETE INTERFACE




KROK 5
Po przejściu do zakładki Overview należy wybrać DELETE ROUTER

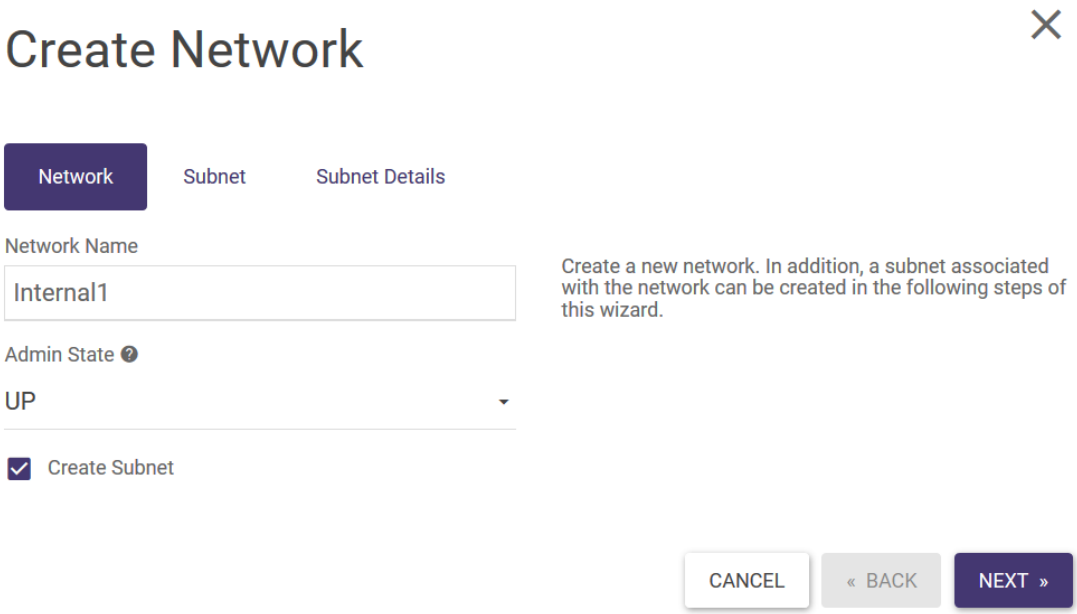


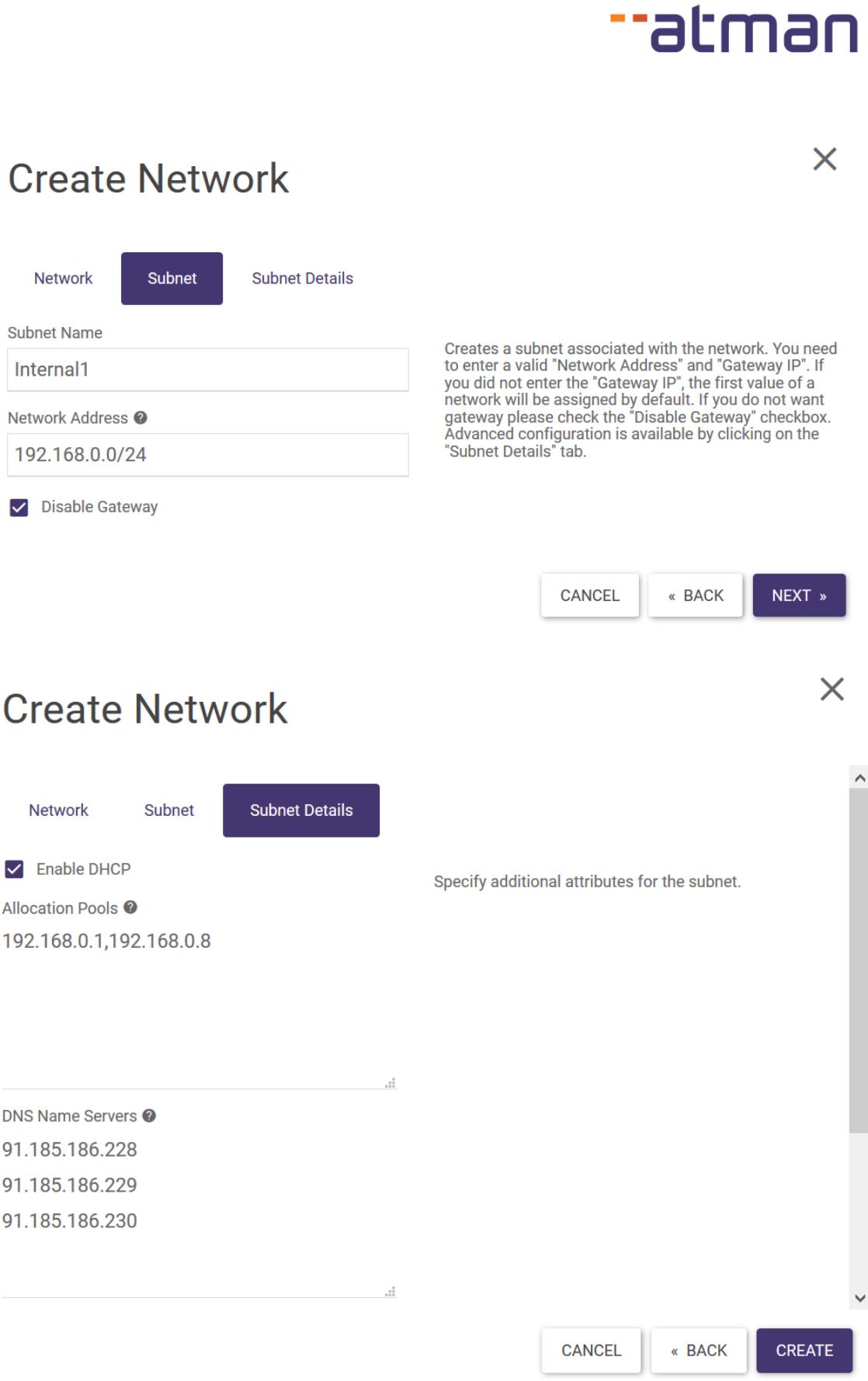

# Sieci wewnętrzne

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.

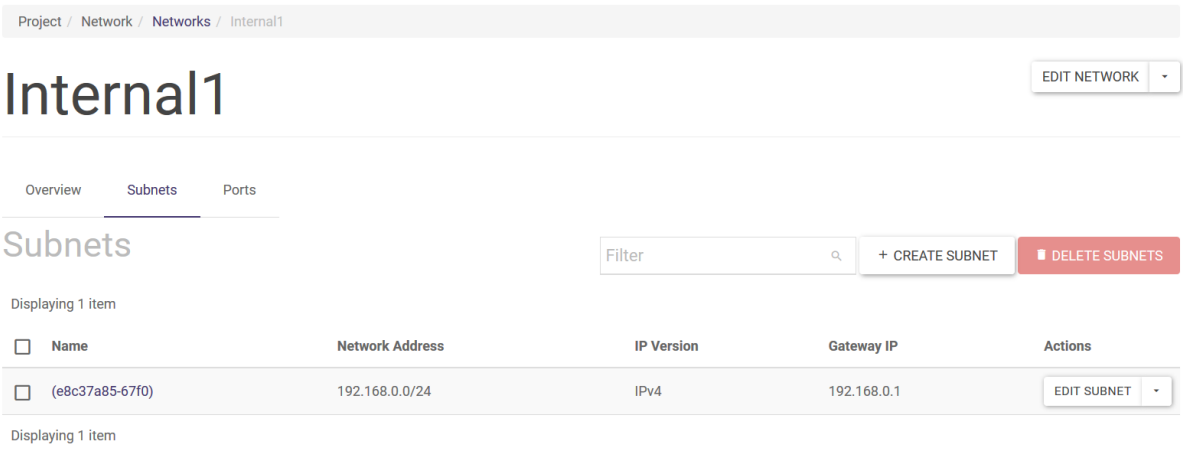





Po kliknięciu CREATE lista sieci powiększy się o nowoutworzoną sieć wewnętrzną:


## Edycja sieci i podsieci

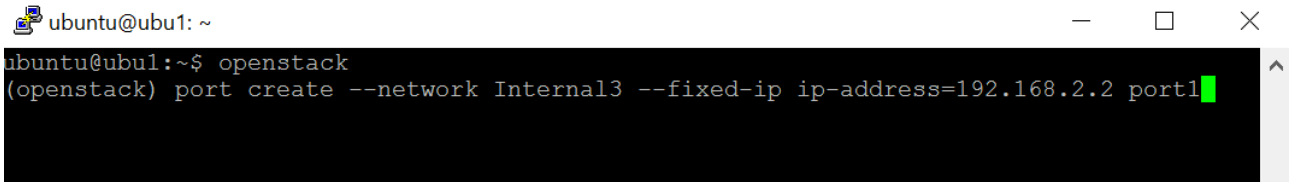
Edycja sieci i parametrów podsieci możliwa jest po kliknięciu na nazwę sieci. Pojawi się ekran, z którego można użyć dwóch akcji: EDIT NETWORK oraz EDIT SUBNET.

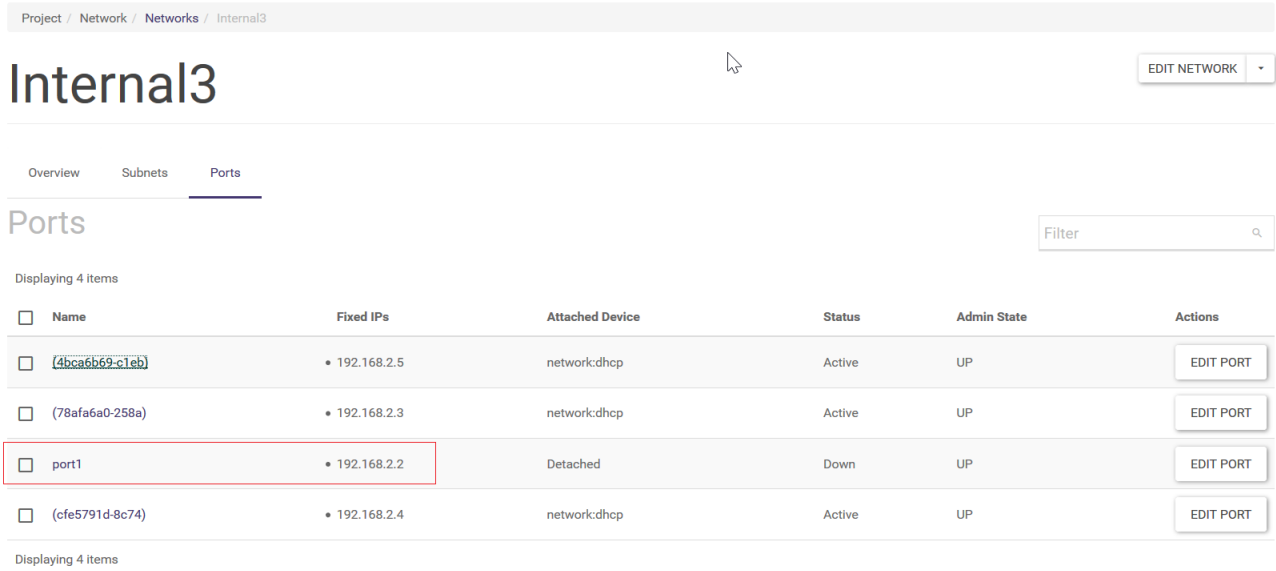



## Statyczne prywatne adresy IP, ręczne przydzielanie adresów

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.



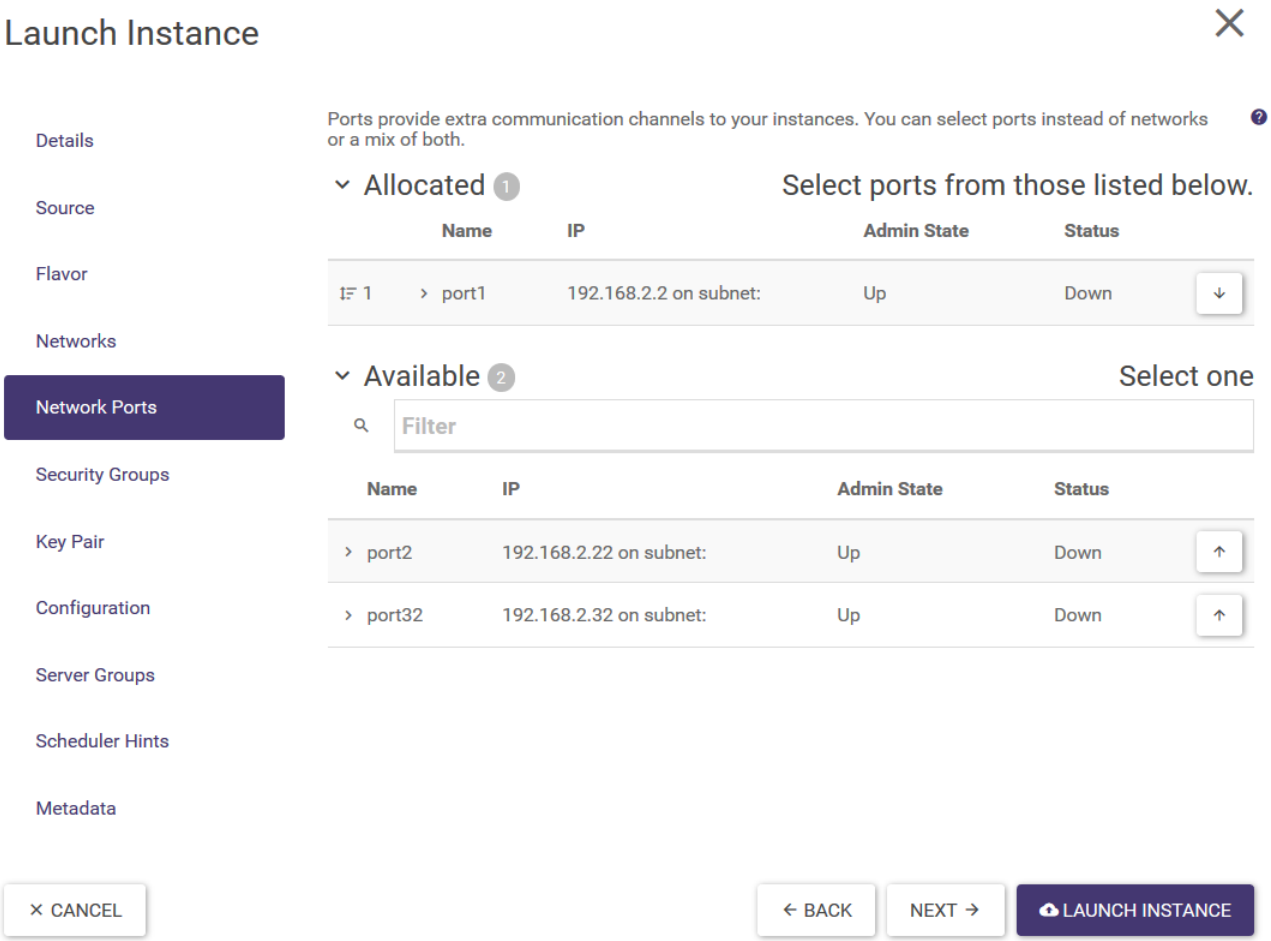



KROK 2
Przypisanie portu do instancji Podczas tworzenia maszyny w kreatorze w zakładce Network Ports należy wybrać port z adresem IP, który chcemy przypisać do instancji. Patrz: screenshot z UWAGI 1 sekcji „Praktyczne uwagi".

## Praktyczne uwagi

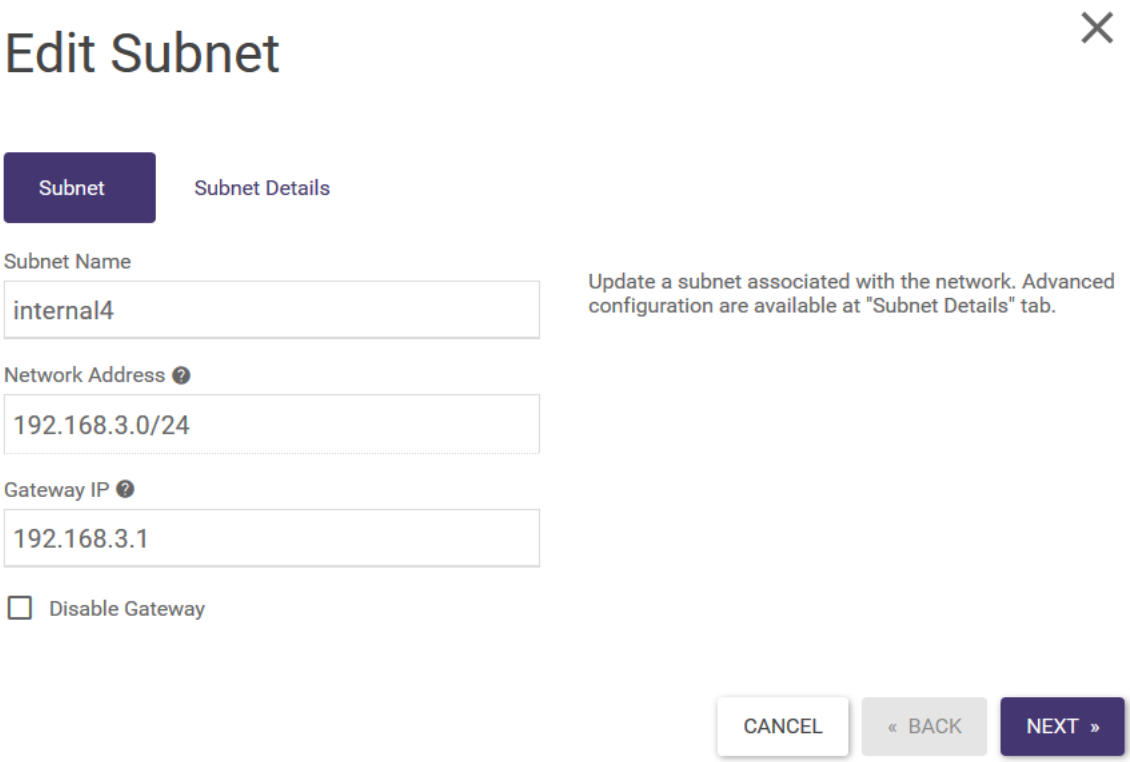
UWAGA 1. Sieci wewnętrzne a hasło root.
Autogenerowanie hasła root podczas tworzenia maszyny odbywa się po sieci tylko przy włączonym DHCP. W przypadku potrzeby stworzenia sieci wewnętrznej z maszynami ze statycznymi adresami IP należy skorzystać z następującej procedury działania:

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.




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 siec. Przed uruchomieniem maszyny sieć powinna być wpięta do routera. Ekran kreatora edycji/tworzenia sieci:




# Firewall

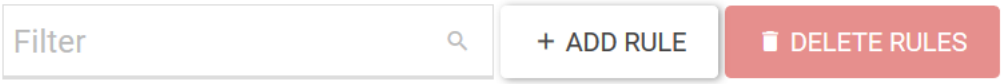
Funkcjonalność zapory ogniowej dostępna jest w ekranie Project → Network → Firewalls (w menu po lewej części panelu Horizon). Należy pamiętać, że Firewall związany jest z routerem, zatem aby był on aktywny, uprzednio należy mieć utworzony router.

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

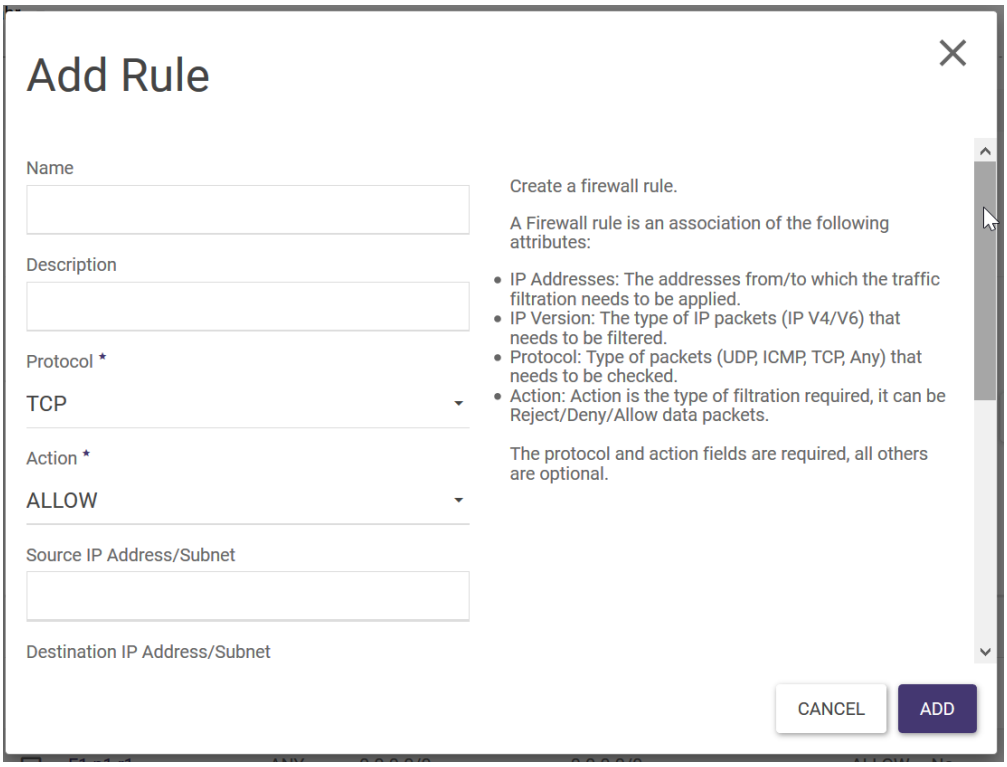
## Utworzenie zapory ogniowej.

KROK 1

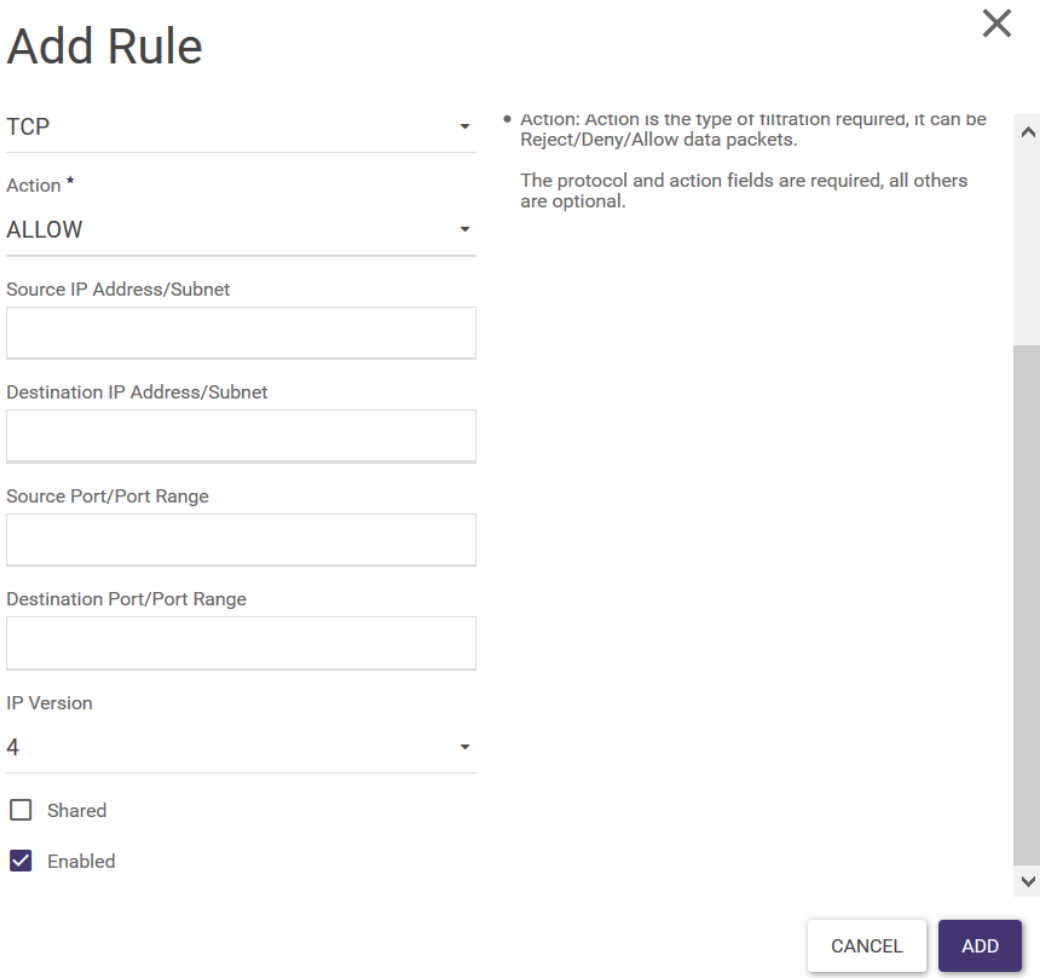
Regułę należy utworzyć klikając przycisk Add Rule w zakładce Firewall Rules, a następnie definiując reguły za pomocą kreatora.




Górna część ekranu kreatora:




Dolna część ekranu kreatora:

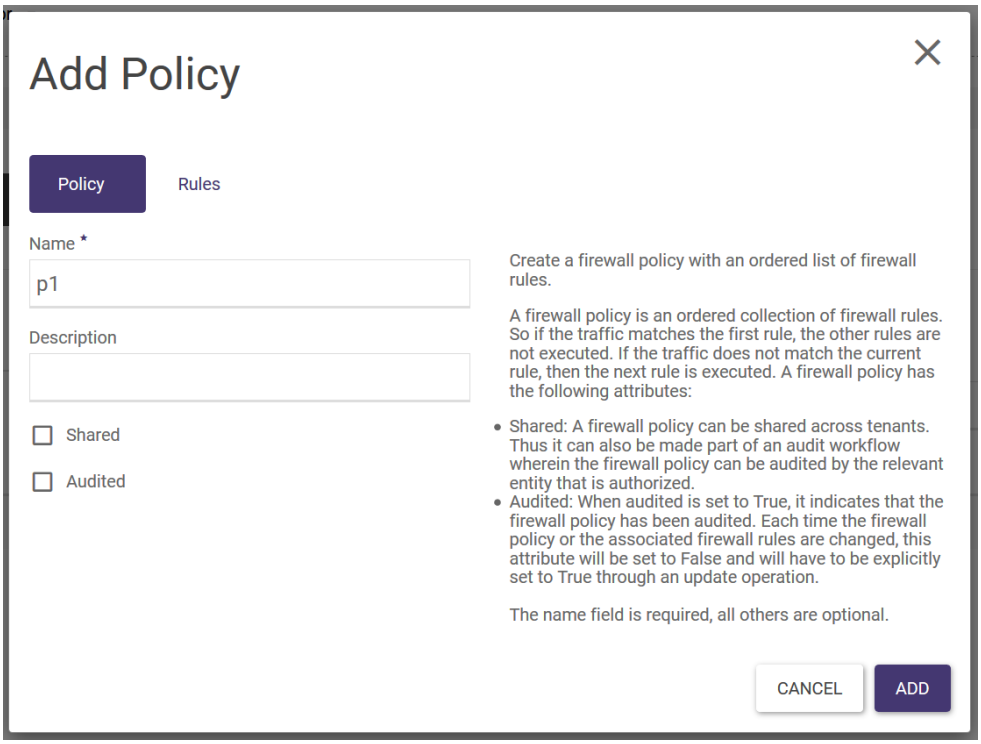


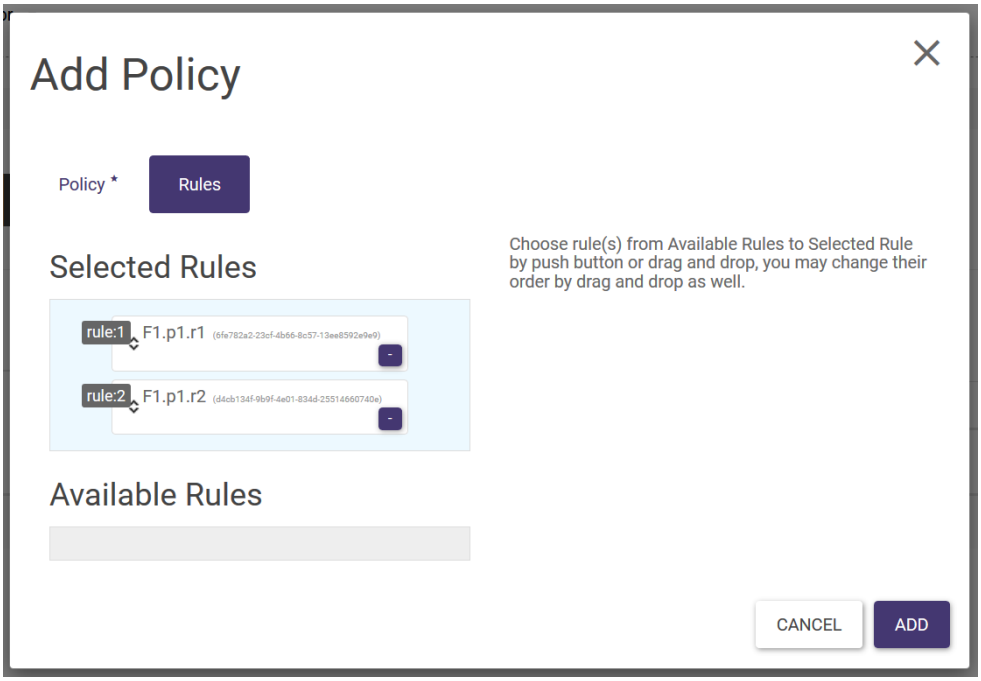

Oto 3 przykłady pozwalające zorientować się w jaki sposób konfigurować regułu

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

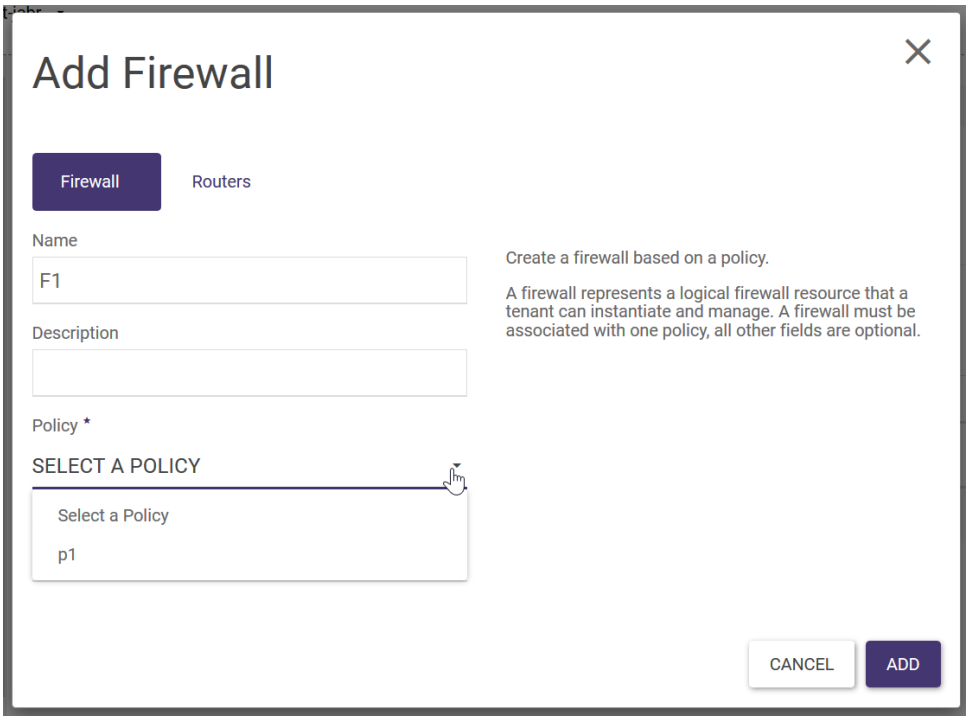
| Name | Description | Protocol | Source IP | Source Port | Destination IP | Destination Port | Action | Shared | Enabled | In Policy | Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|
| F1.p1.r3 | | TCP | - | - | - | 22 | DENY | No | Yes | p1 | EDIT RULE |
| F1.p1.r2 | | ICMP | - | - | -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

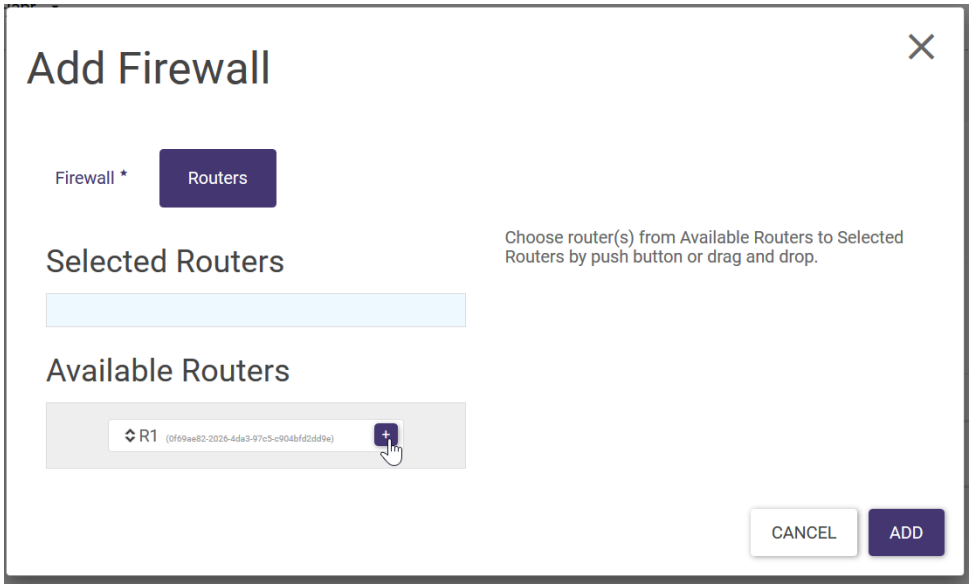
KROK 2
W zakładce Firewall Policies należy klinąć przycisk +ADD POLICY i za pomocą kreatora dodać politykę, wpisując jej nazwę oraz dodając wcześniej zdefiniowane reguły. UWAGA: ważna jest kolejność reguł.

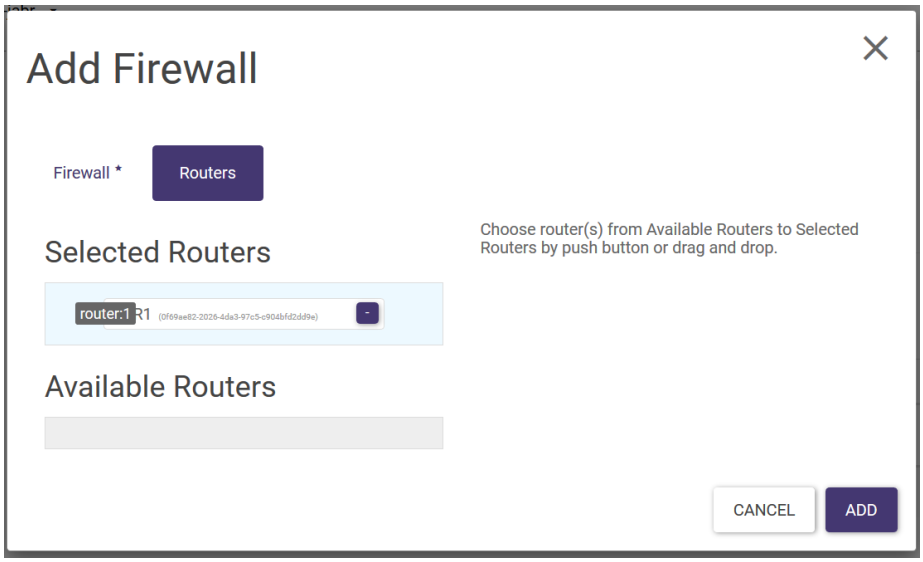


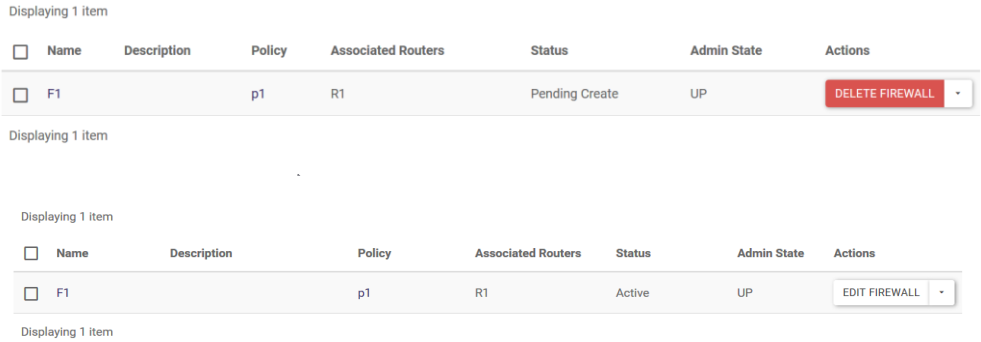

KROK 3
W zakładce Firewalls należy kliknąć przycisk +CREATE FIREWALL i uzupełnić pola w kreatorze, podając politykę i wiążąc Firewall z Routerem.



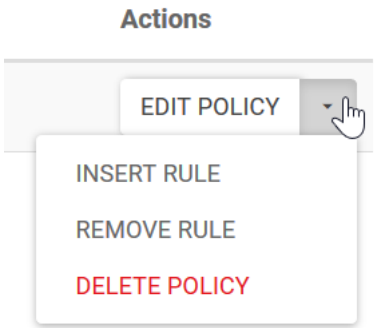



Teraz należy poczekać aż status zmieni się z Pending Create na Active. Jeśli w ciągu kilku sekund zmiana nie nastąpi, należy kliknąć w głównym menu po lewej stroni panelu Horizon na inną zakładkę po czym wrócić do zakładki Firewalls lub odświeżyć widok – status będzie zmieniony.

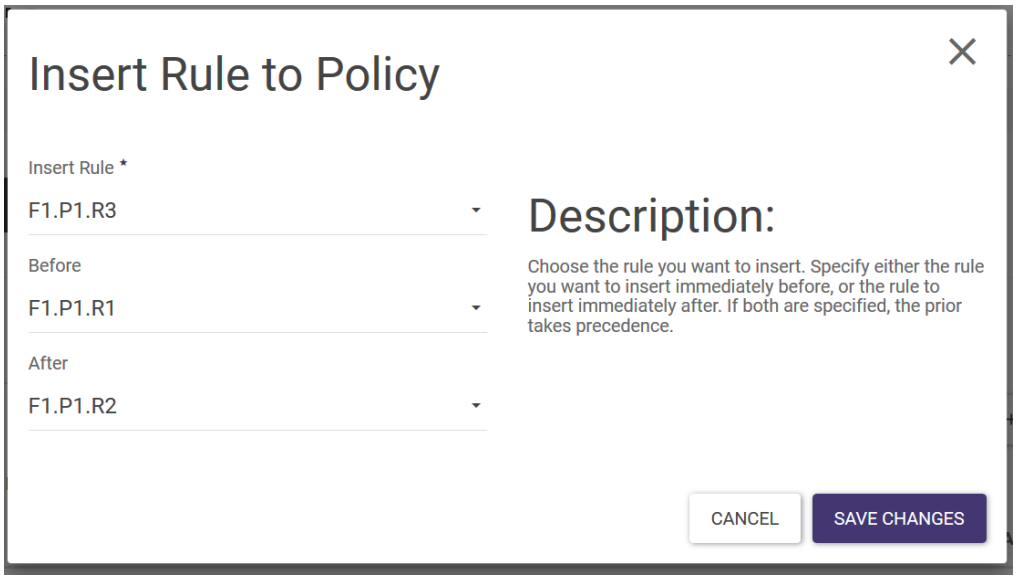



## Dodanie reguły do polityki.

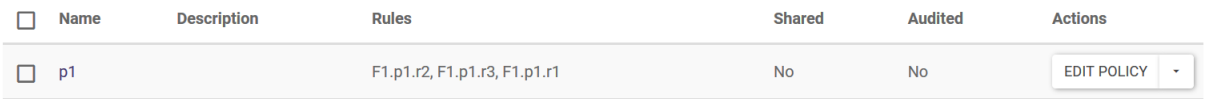
KROK 1
Po prawej stronie polityki do której chcemy dodać regułę należy rozwinąć listę aktywności i kliknąć Insert Rule.




KROK 2
Przy pomocy kreatora określamy regułę do dodania wraz kolejnością jej stosowania przez Firewall.

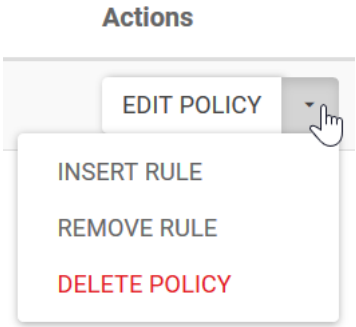



KROK 3
Należy zatwierdzić dodanie klikając przycisk Save Changes. Polityka zostaje zaktualizowana.

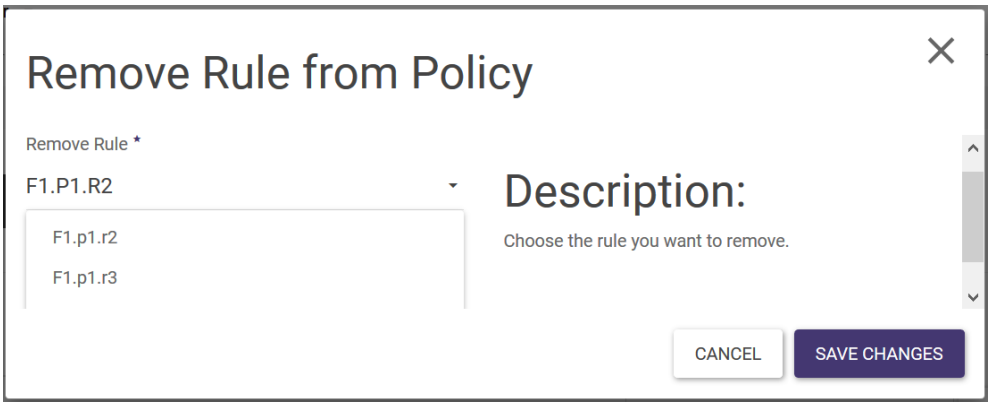



## Usunięcie reguły z polityki.

KROK 1
Po prawej stronie polityki z której chcemy usunąć regułę należy rozwinąć listę aktywności i kliknąć Remove Rule.



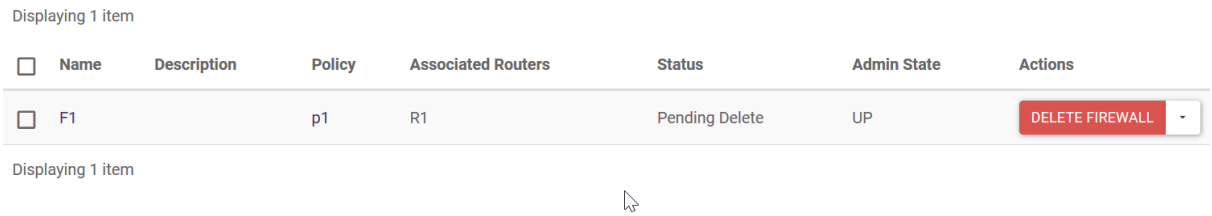

KROK 2
Po zaznaczeniu reguły, którą chcemy usunąć, należy kliknąć przycisk „Save Changes”.




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:




(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

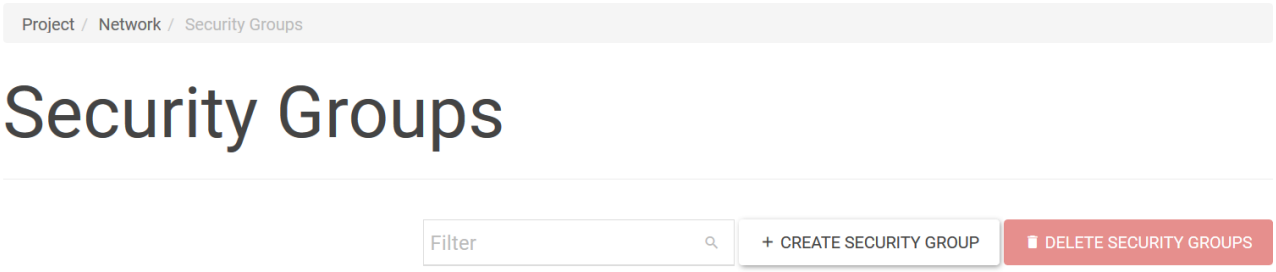
Grupa zabezpieczeń (Security Group) jest bardzo wygodnym narzędziem, umożliwiającym szczegółowe zdefiniowanie reguł bezpieczeństwa. Reguły określają jaki ruch jest dozwolony w ramach grupy zabezpieczeń. Jedna grupa zabezpieczeń może zostać przypisana do wielu wirtualnych maszyn. Do jednej wirtualnej 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):

| Direction | Ether Type | IP Protocol | Port Range | Remote IP Prefix | Remote Security Group | Actions |
|---|---|---|---|---|---|---|
| Egress | IPv4 | Any | Any | 0.0.0.0/0 | - | DELETE RULE |
| Ingress | IPv6 | Any | Any | - | default | DELETE RULE |
| Ingress | IPv4 | Any | Any | - | default | DELETE RULE |
| Egress | IPv6 | Any | Any | ::/0 | - | DELETE RULE |

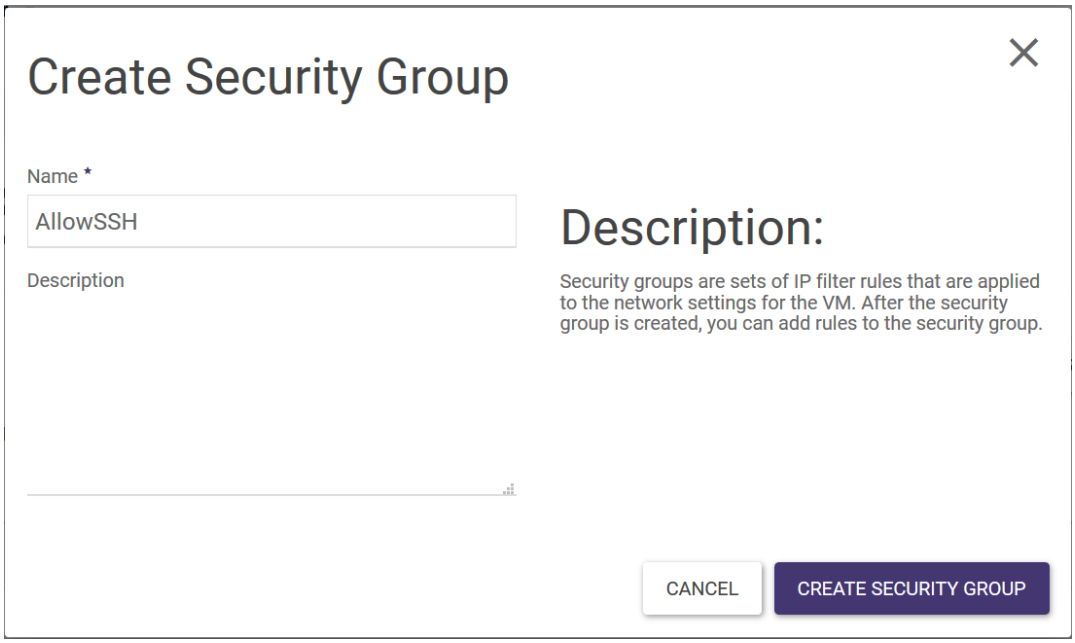
Displaying 4 items

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:

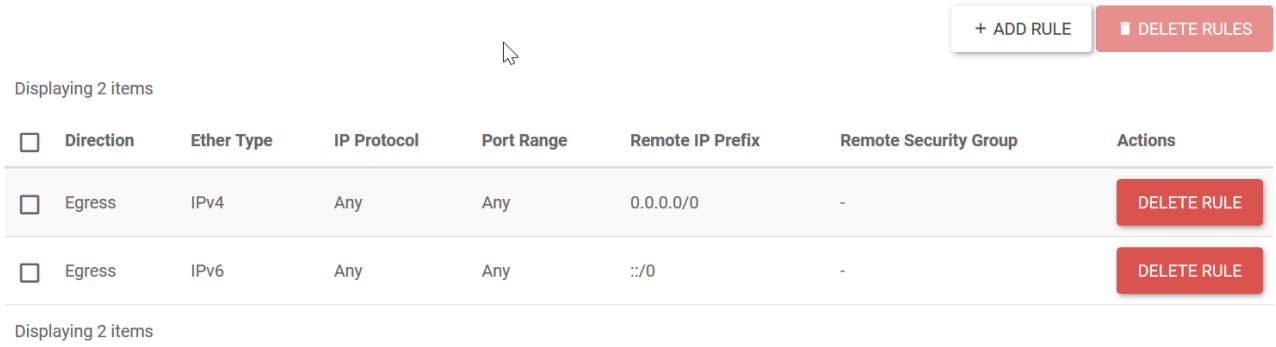



KROK 2
Pojawi się kreator, w którym należy nadać nazwę grupy zabezpieczeń (tu: AllowSSH), a następnie kliknąć Create Security Group:



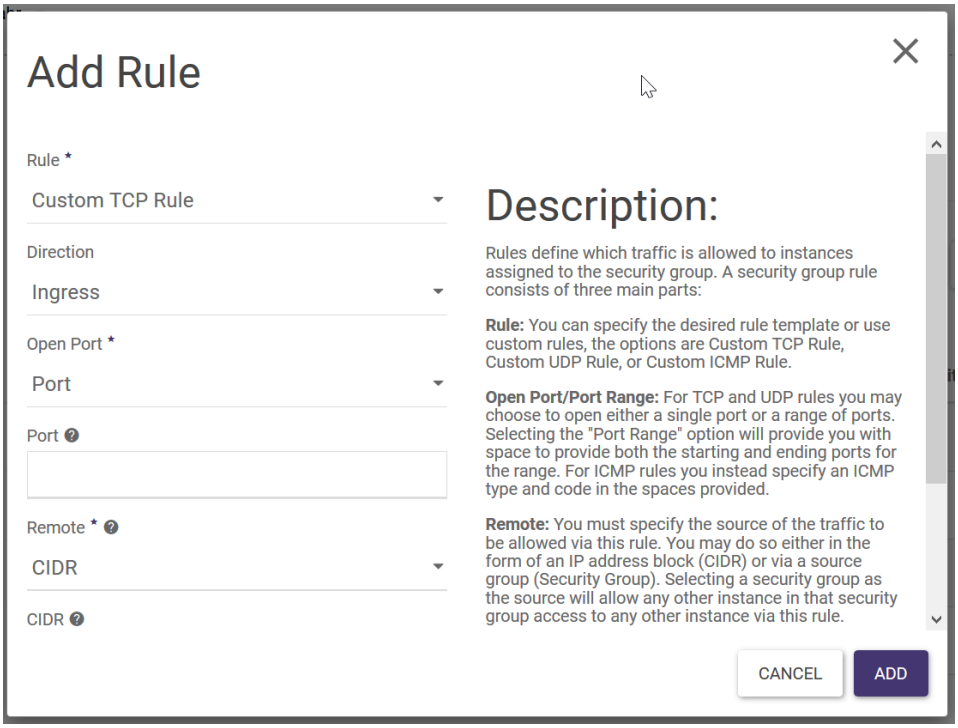
KROK 3

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:




KROK 4

Nową regułę 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 reguł, należy je zatwierdzić w kreatorze klikając przycisk Add.




KROK 5

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

Displaying 4 items

| Direction | Ether Type | IP Protocol | Port Range | Remote IP Prefix | Remote Security Group | Actions |
|---|---|---|---|---|---|---|
| Egress | IPv4 | Any | Any | 0.0.0.0/0 | - | DELETE RULE |
| Egress | IPv6 | Any | Any | ::/0 | - | DELETE RULE |
| Ingress | IPv4 | ICMP | Any | 0.0.0.0/0 | - | DELETE RULE |
| 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:

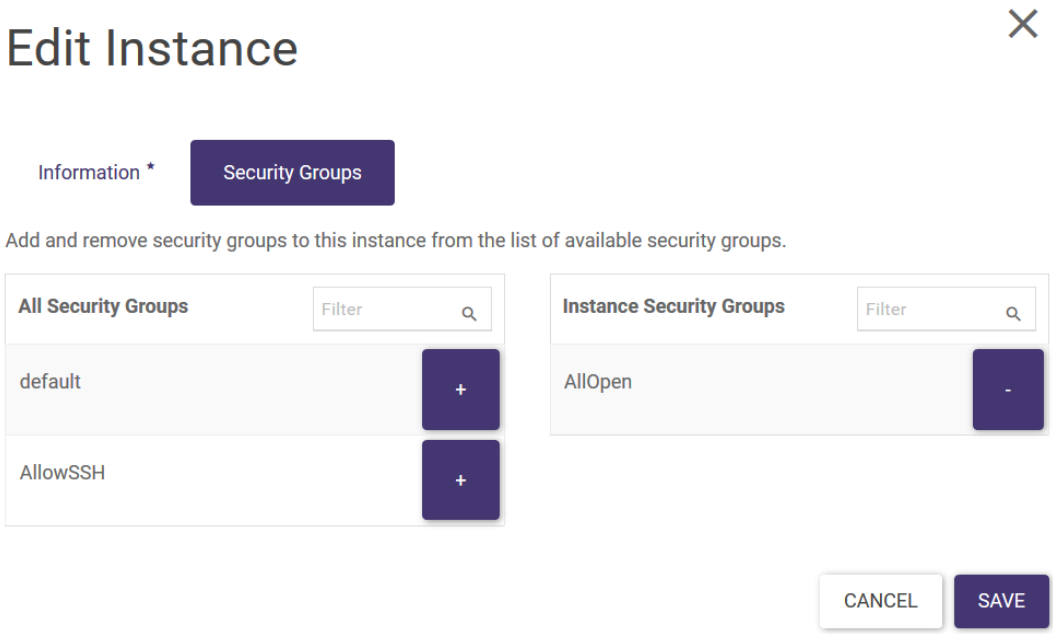
| Direction | Ether Type | IP Protocol | Port Range | Remote IP Prefix | Remote Security Group | Actions |
|---|---|---|---|---|---|---|
| Egress | IPv6 | Any | Any | ::/0 | - | DELETE RULE |
| Egress | IPv4 | Any | Any | 0.0.0.0/0 | - | DELETE RULE |
| Ingress | IPv4 | TCP | 1 - 65535 | 0.0.0.0/0 | - | 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. Odbywa 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.




# 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.

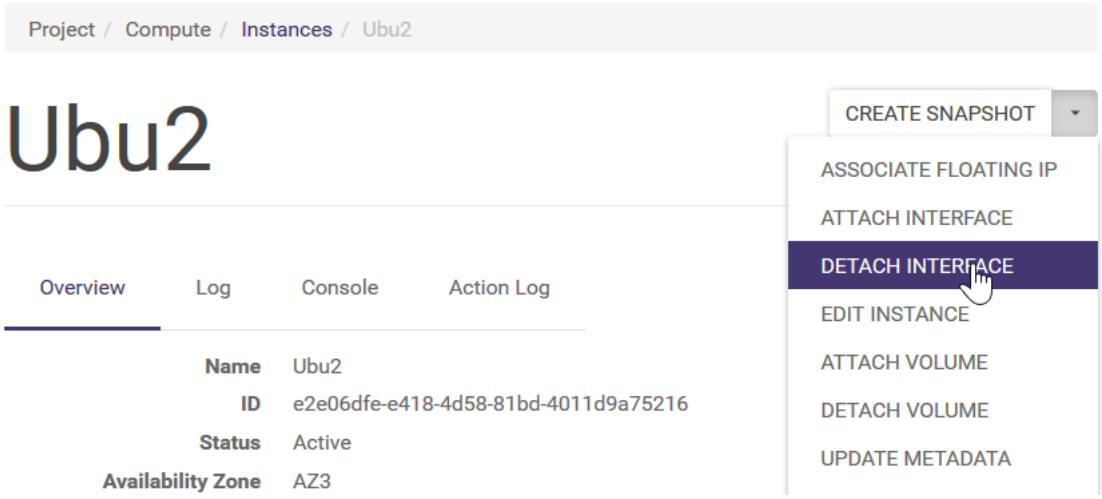
# Adresy IP

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:

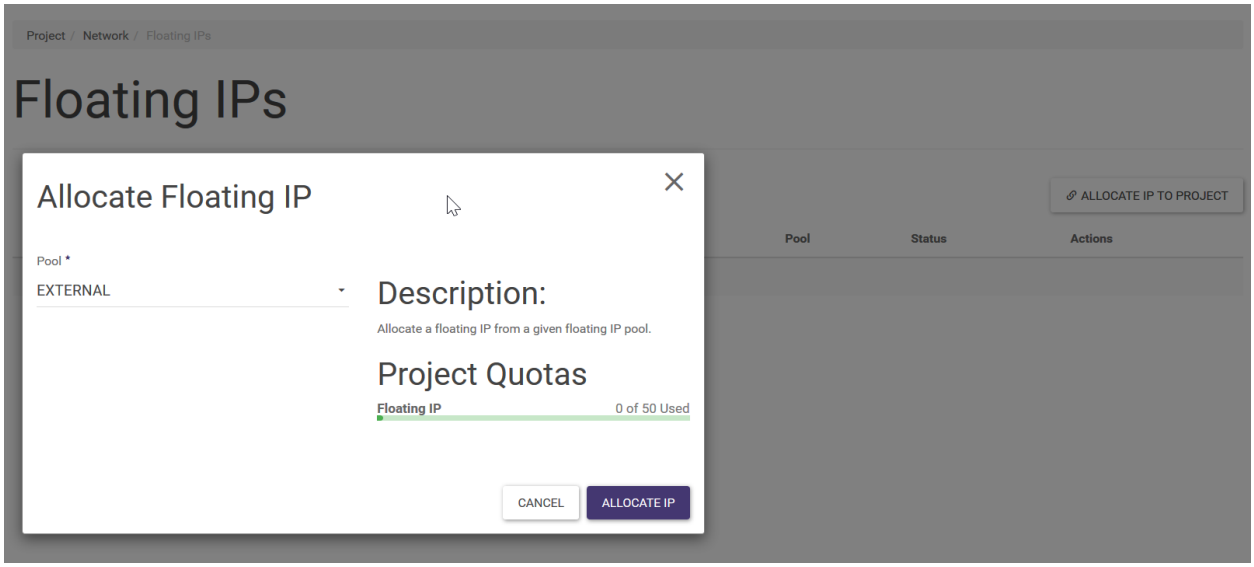



Należy pamiętać że ponowna alokacja tego samego publicznego adresu IP może oczywiście nastąpić ale z bardzo małym prawdopodobieństwem. Bardzo wygodnym i zalecanym przez Atmana podejściem dla instancji produkcyjnych jest korzystanie z pływających adresów IP.

## 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 niezmienne 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.

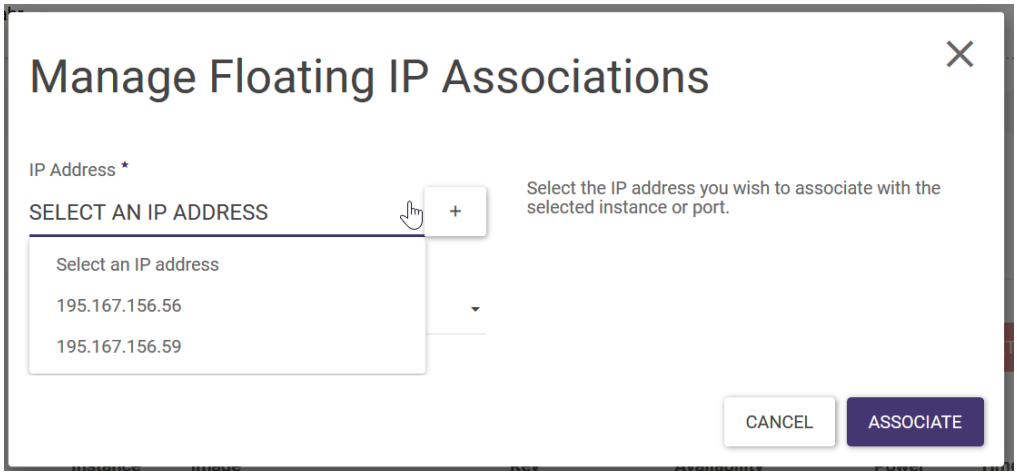


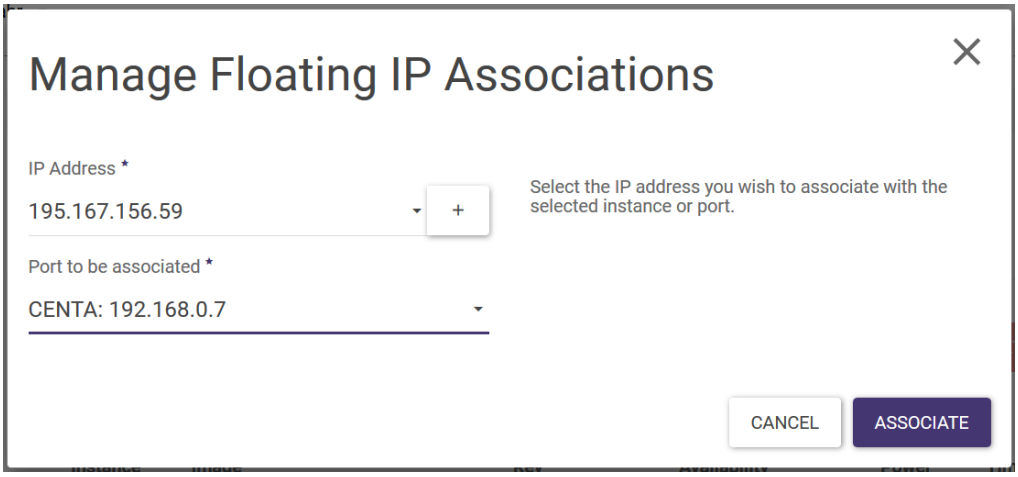

KROK 2

Przydzielenie pływającego adresu IP do środowiska odbywa się poprzez:

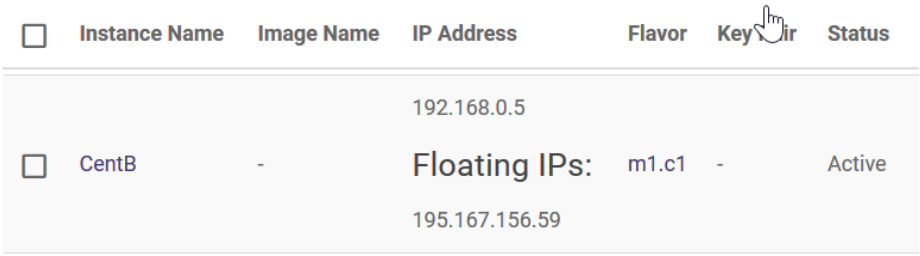
a) uruchomienie akcji ASSOCIATE dla danego pływającego adresu IP na ekranie Project→Network→Floating IPs
b) uruchomienie akcji ASSOCIATE FLOATING IP dla danej instancji na ekranie Project→Compute→Instances

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




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




## Prywatne

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

# API

## Przygotowanie środowiska do korzystania z API

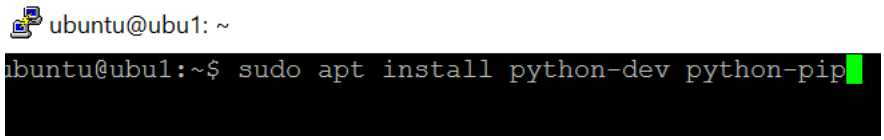
Atman rekomenduje klienta api: python-openstackclient.
Pełną dokumentację online można znaleźć pod adresem: https://docs.openstack.org/python-openstackclient/latest/

Kolejność działań:

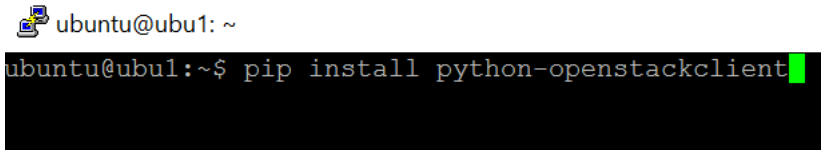
1. Instalacja środowiska python
2. Instalacja python-openstackclient
3. Konfiguracja python-openstackclient
    a. Pobranie pliku rc z panelu Horizon
    b. Eksport zmiennych środowiskowych

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

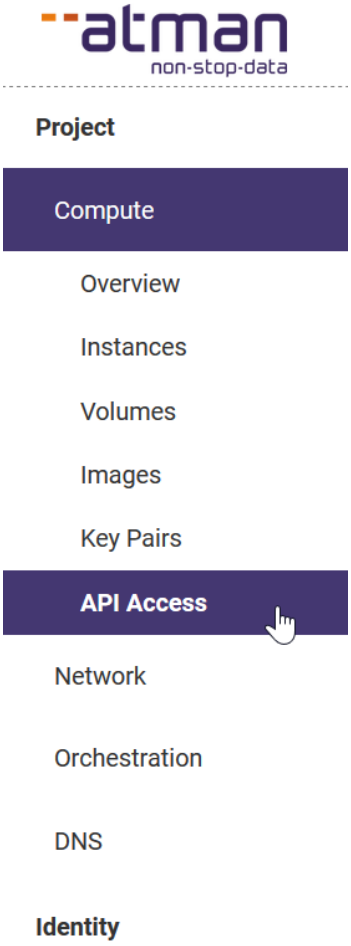
1. Instalacja środowiska python. Na maszynie, z której administrator będzie zarządzał środowiskiem poprzez api, należy uruchomić polecenie:



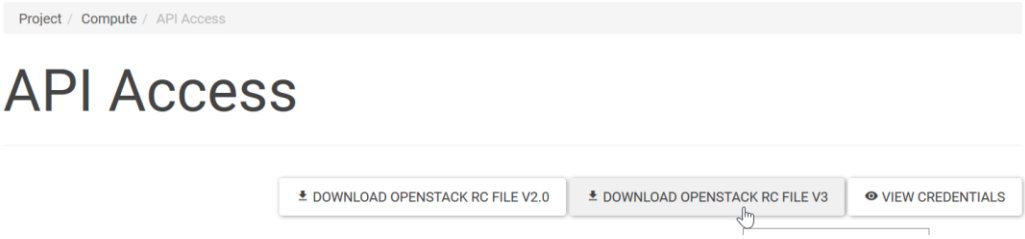

2. Instalacja python-openstackclient.
   W następnej kolejności uruchamiane jest polecenie:



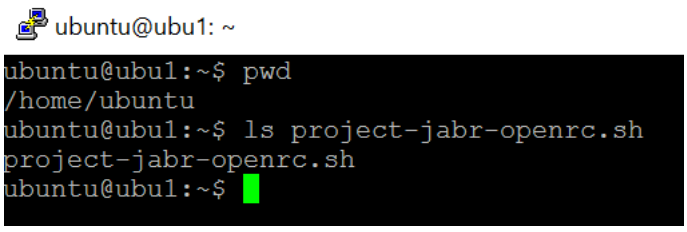

3. Konfiguracja python-openstackclient.
    a. Pobranie pliku rc. Należy zalogować się do panelu Horizon i przejść do zakładki Project->Compute->API Access:




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



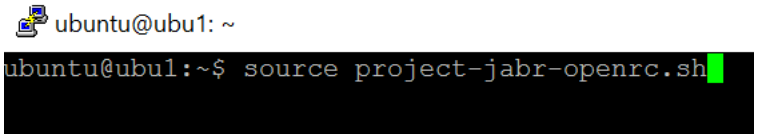

Pobrany plik należy zapisać w katalogu domowym użytkownika:



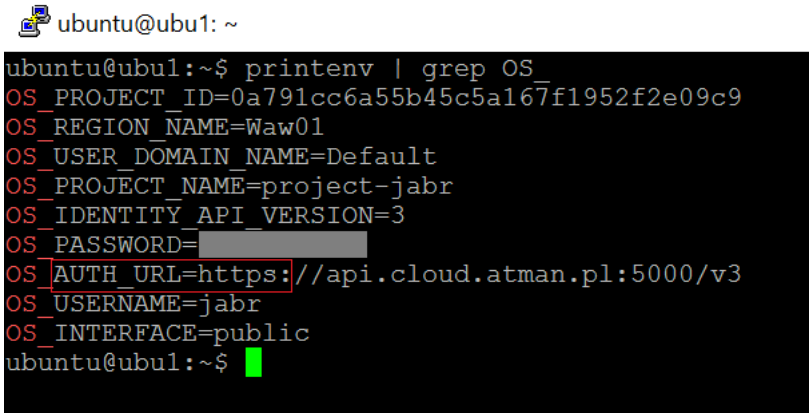

b. Eksport zmiennych środowiskowych

Pobrany 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-pobrany>):




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




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) – szczegóły 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:

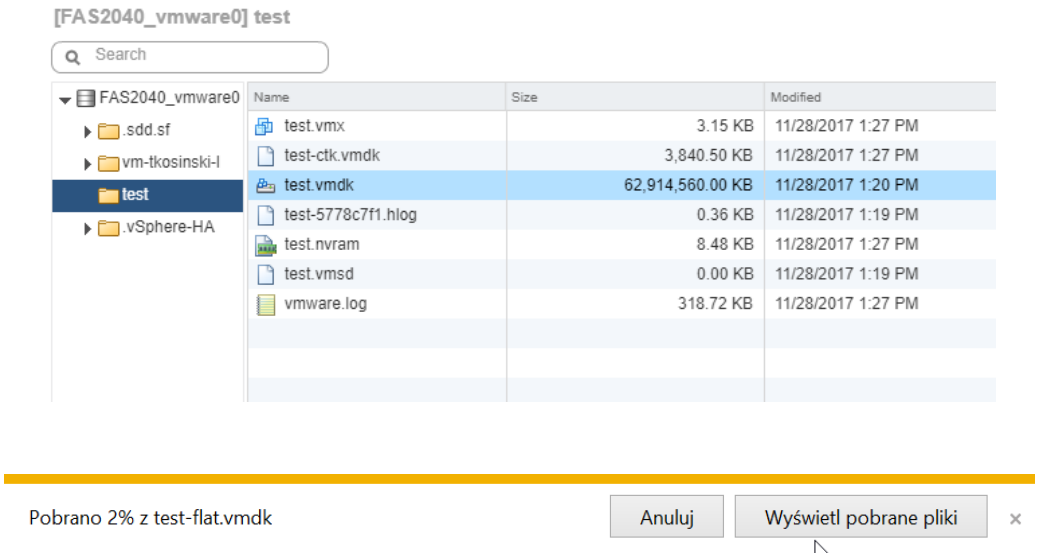
https://docs.openstack.org/python-openstackclient/latest/cli/command-list.html

# Inne

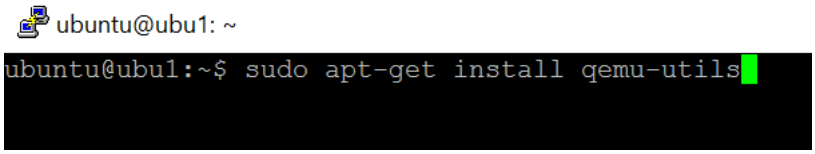
## Konwersja obrazów

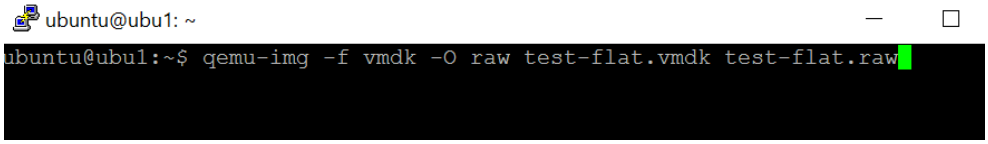
W celu zaimportowania maszyny z zewnątrz do wirtualnego środowiska serwerowego do Atman Cloud, należy uprzednio przekonwertować ją do formatu raw. Poniższy przykład obrazuje proces konwersji pliku vmdk na raw przy użyciu rekomendowanego przez Atman narzędzia – qemu.

KROK 1
Zapisanie obrazu maszyny
Z poziomu VMWare vSphere Web Client pobieramy plik (tu: jako  test-flat.vmdk)



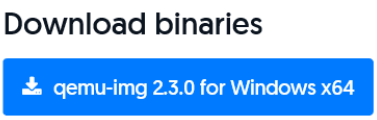

KROK 2
Konwersja. Linux:



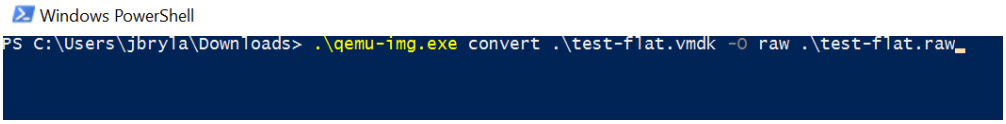




Windows:

1. Należy pobrać oprogramowanie qemu:

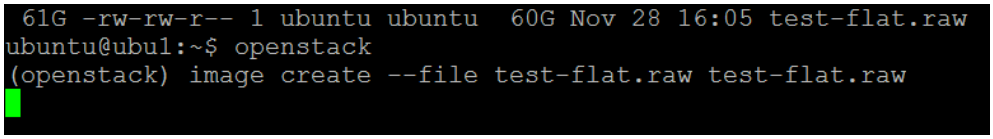



2. Po rozpakowaniu oprogramowanie gotowe jest do użycia – z terminala PowerShell należy uruchamiać z miejsca w którym plik qemu-img.exe jest zapisany.
3. Poniższe polecenie konwertuje plik vmdk do formatu raw:

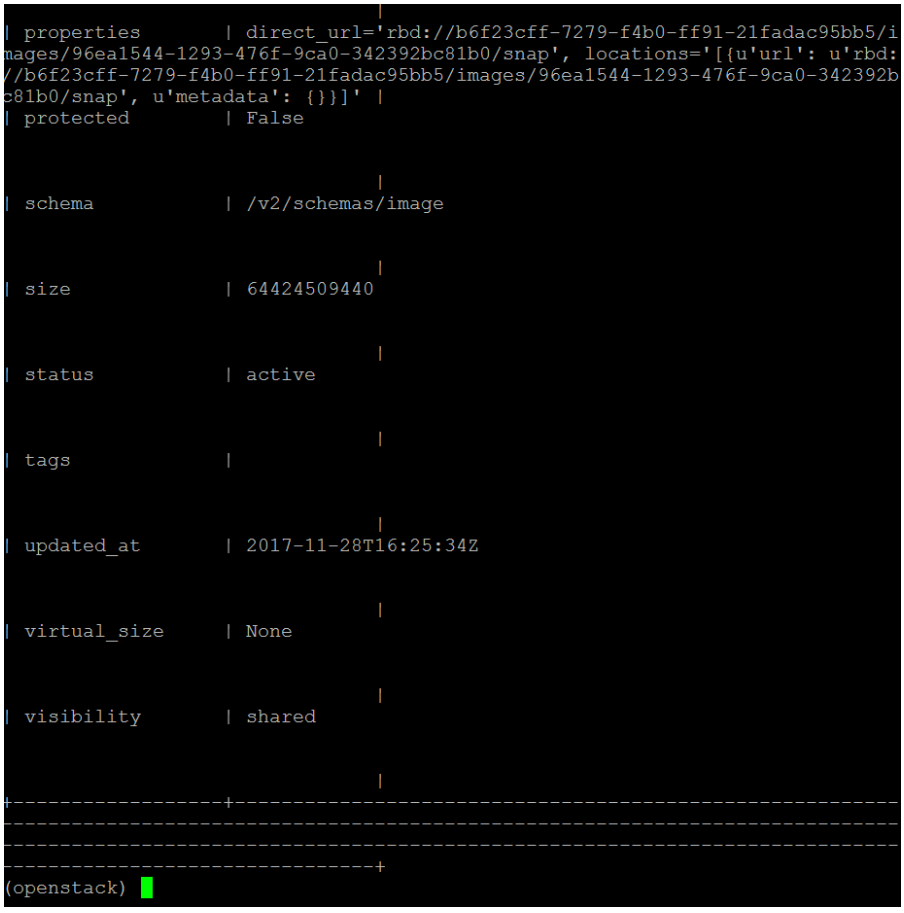



## Upload (import) pliku do chmury

1. Upload przy użyciu API.




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

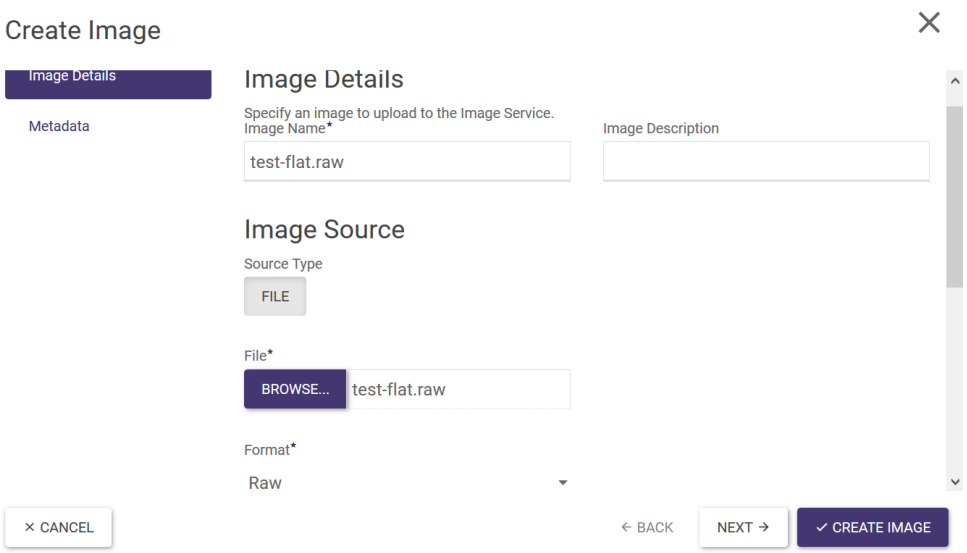



Sprawdzenie czy plik został zaimportowany na chmurę:

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 |
| 0bfbedd0-8016-40df-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-d0ce076edff0 | 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:



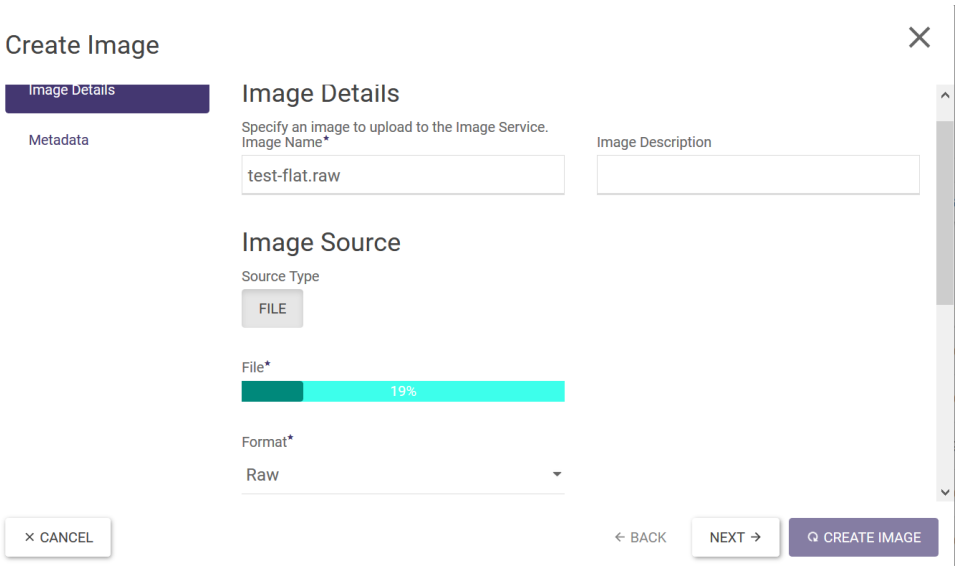

W dolnej części kreatora należy ustawić parametry:

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

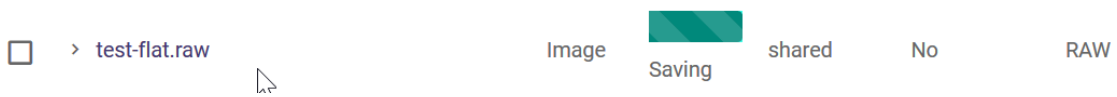

Znaczenie parametrów:

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

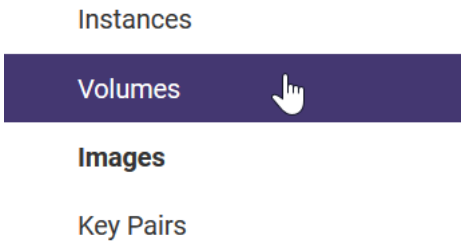
W trakcie uploadu obrazu w kreatorze pojawi się pasek stanu, na którym widać postęp pracy:



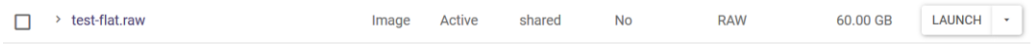

Po utworzeniu kreatorem obrazu należy odświeżyć widok…




…poprzez kliknięcie w menu na inną zakładką i ponowne kliknięcie na zakładkę Images:




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

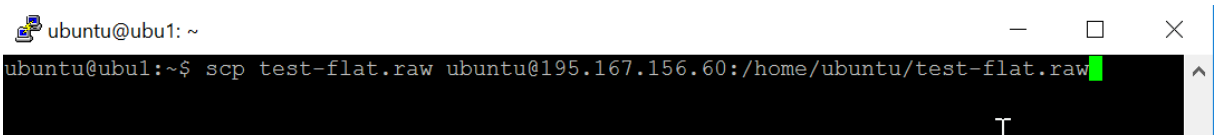



3. Trzecia droga:

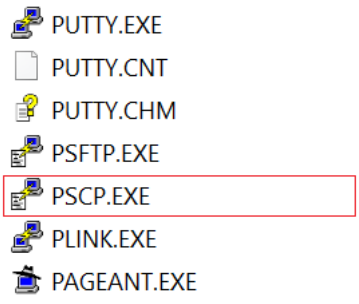
W przypadku bardzo dużych plików, słabego łącza, zrywania sesji, itp. – alternatywną, dobrze działającą ścieżką jest skopiowanie obrazu z lokalnej maszyny na zdalną maszynę uruchomioną na Atman Cloud, a następnie użycie API do uploadu obrazu.

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).

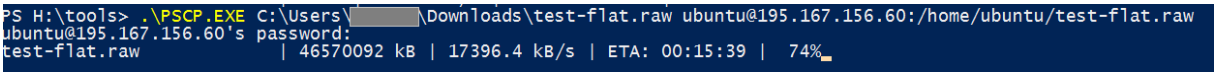
Linux:




Windows:



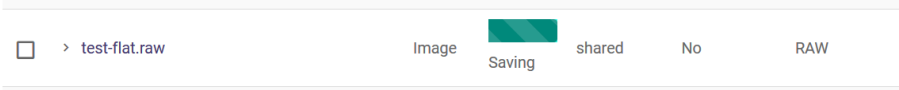

Sposób użycia z PowerShell Windowsa:




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

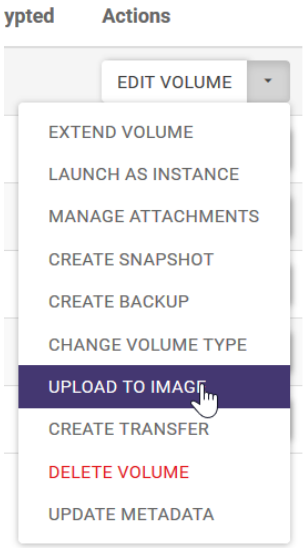
```
 61G -rw-rw-r-- 1 ubuntu ubuntu  60G Nov 28 16:05 test-flat.raw
ubuntu@ubu1:~$ openstack
(openstack) image create --file test-flat.raw test-flat.raw
```

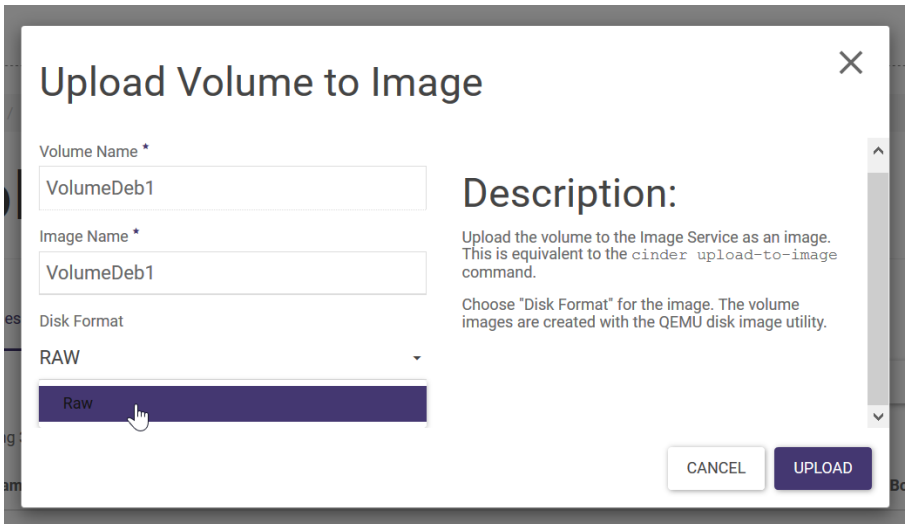
Można zaobserwować, że jednocześnie w panelu Horizon w zakładce Images pojawi się nowa pozycja na liście z informacją o zapisywaniu:



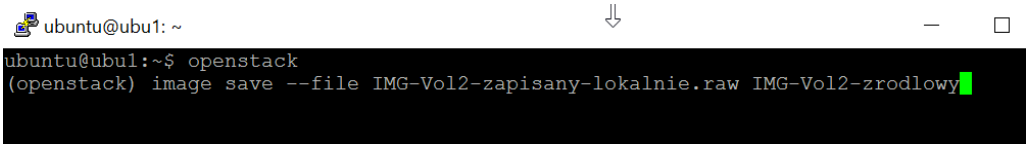

## Download (export) pliku z chmury.

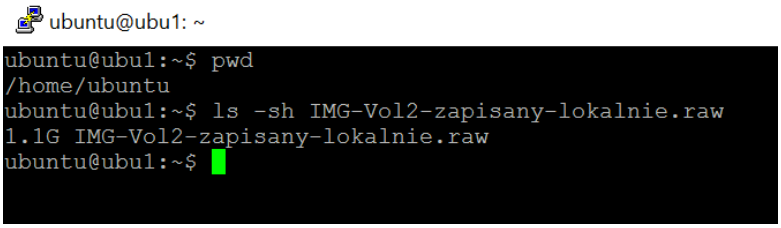
Aby wyeksportować obraz z chmury na lokalną stację roboczą, uprzednio należy utworzyć obraz wolumenu (zakładka Volumes, akcja dla wybranego wolumenu „upload to image”):






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



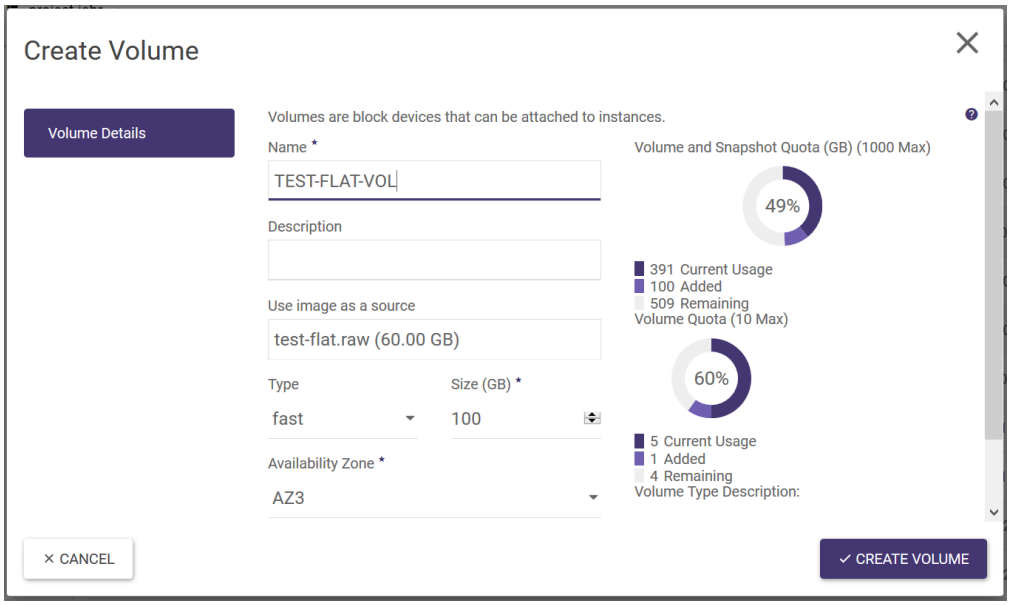




## Utworzenie maszyny z własnego (zaimportowanego obrazu)

Należy wykonać następujące kroki:

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

KROK 1. Utworzenie wolumenu z obrazu.
Z poziomu panelu Horizon:



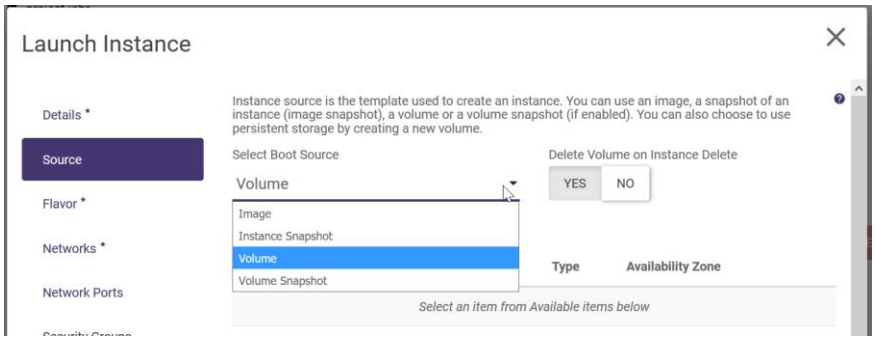

Przy użyciu API:

```
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             | 3c459b2cbbeb49ea8b5f30317f5fbcc4     |
+---------------------+--------------------------------------+
(openstack)
```

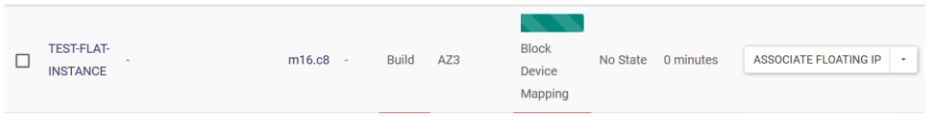
Komenda „volume type list” – listuje dostępne profile storage’owe. W tym przypadku użyty został profil szybki.
Komenda „volume create” – tworzy wolumen. Właściwość –size określa rozmiar w GB, --type to rodzaj storage’u (patrz wyżej), -- image to nazwa obrazu użytego do tworzenia wolumenu, --bootable (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 volumenie.




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




A po chwili – maszyna gotowa: