PROJEKT
Multitenantné operačné centrum kybernetickej bezpečnosti riešené
ako otvorená cloudová služba s prvkami strojového učenia

Previazané s balíkom KPB1 – Návrh virt. riešenia

Previazané s výstupom
V3 – Popis vybraného riešenia spĺňajúceho stanovené kritéria

typ – dokumentácia

Úvod

Cloud a cloudové služby sú neodlučiteľnou súčasťou dnešnej doby. Nepochybne sa o tom presvedčujeme v situáciách, kedy veľké firmy presúvajú väčšinovú časť svojej infraštruktúry na cloud. Pre klienta je častokrát všetko jednoduchšie, rýchlejšie a finančne výhodnejšie. Príkladom sú služby Amazon Web Services, Google Cloud Platform, Microsoft Azure alebo IBM Services. V posledných rokoch sa do cloud-u preniesli nielen výpočtový výkon a dáta ale aj herné odvetvie (gaming-as-a-service), medzi ktoré patria GeForce Now, Google Stadia, Playstation Now a iné.

V roku 2010 začal projekt s pôvodnými autormi National Aeronautics and Space Administration (NASA) a Rackspace Hosting v dnešnej dobe známy ako OpenStack. Väčšinou sa nasadzuje ako „infraštruktúra ako služba“ (IaaS) vo verejných aj súkromných cloudoch, kde sú používateľom sprístupnené virtuálne servery a ďalšie zdroje. Softvérová platforma pozostáva so vzájomne prepojených komponentov, ktoré riadia rôznorodé hardvérové oblasti spracovania, ukladania a sieťových zdrojov viacerých dodávateľov v celom dátovom centre. Používatelia ho spravujú buď prostredníctvom webového ovládacieho panela alebo nástrojov príkazového riadka. OpenStack má modulárnu architektúru s rôznymi názvami svojich komponentov ako sú: Compute (Nova), Networking (Neutron), Block storage (Cinder), Identity (Keystone), Object storage (Swift), Dashboard (Horizon). S každou novou verziou pribúdali nové a nové komponenty, oproti prvotnej verzii s dvomi komponentami Nova a Swift je v akutálnej verzií s názvom Yoga (Janurár 2023) možnosť inštalácie 38 komponentov. Existujú viaceré možnosti inštalácie OpenStack-u: OpenStack Charms, OpenStack „kolla-ansible“, OpenStack-Ansible alebo TripleO.

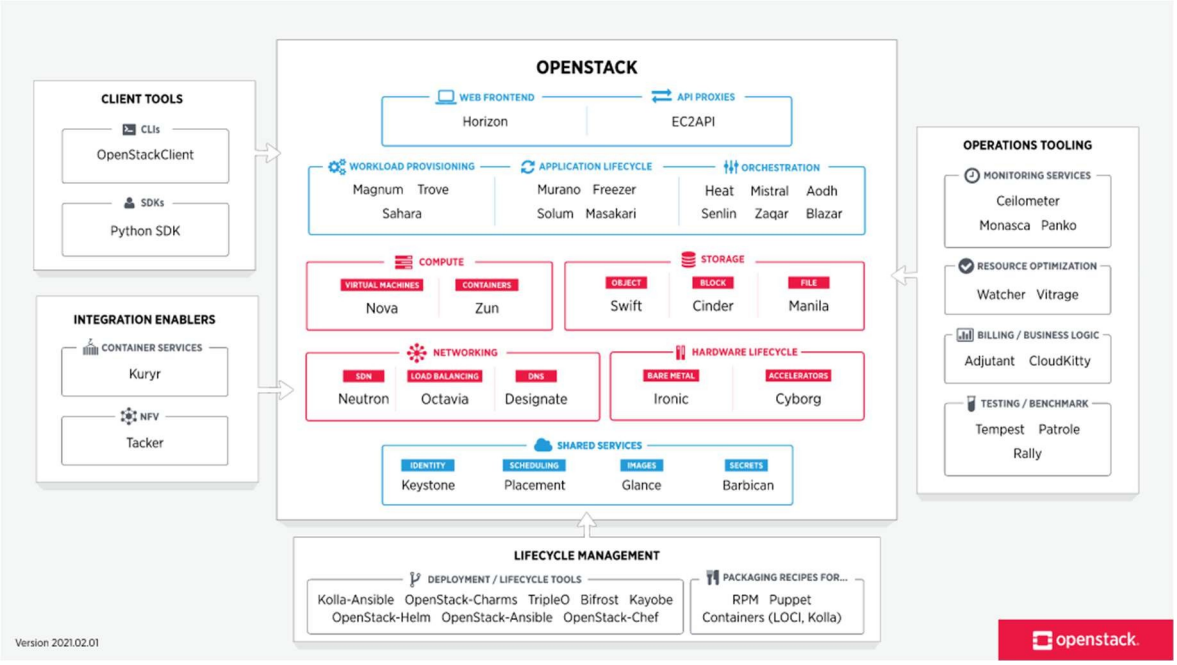
Práve na túto bezplatnú open-source platformu cloud computing-u sa v tejto práci zameriame.

1 OpenStack cloudová platforma

1.1 Čo je OpenStack?

OpenStack je cloudový operačný systém, ktorý riadi veľké skupiny výpočtových, úložných a sieťových zdrojov v rámci dátového centra, pričom všetky sú spravované a poskytované prostredníctvom rozhraní API so spoločnými mechanizmami autentifikácie. K dispozícii je aj webový panel, ktorý správcom poskytuje kontrolu a zároveň umožňuje používateľom poskytovať zdroje prostredníctvom webového rozhrania. Okrem štandardnej funkčnosti infraštruktúry ako služby poskytujú ďalšie komponenty okrem iných služieb aj orchestráciu, správu porúch a správu služieb, aby sa zabezpečila vysoká dostupnosť používateľských aplikácií.

OpenStack je rozdelený na služby, ktoré umožňujú pripojiť komponenty v závislosti od potrieb používateľa. Mapa OpenStacku poskytuje pohľad na životný cyklus OpenStacku, aby používateľ videl, kam sa tieto služby hodia a ako môžu spolupracovať [2].



Obrázok 1 – Mapa OpenStack-u

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

1.2 Inštalácia KIS OpenStack Yoga [7]

1.2.1 Na čo slúži server Metal-as-a-Service(MAAS)?

Metal-as-a-Service (MAAS) poskytuje kompletnú automatizáciu fyzických serverov pre efektívnosť prevádzky serverov/dátového centra. Softvér je open-source a je zastrešovaný firmou Canonical, ktorá stojí za distribúciou Linux Ubuntu. MAAS zaobchádza s fyzickými servermi ako s virtuálnymi strojmi (inštanciami) v cloude. Toto riešenie umožňuje spravovať niekoľko serverov naraz a z jedného miesta, aby sa nemuseli spravovať jednotlivo a komplikovane. Na diaľku je teda možné nasadenie štandardných alebo upravených operačných systémov na fyzické alebo virtuálne stroje. MAAS komplexne spĺňa potrebu rýchleho nasadenia, zničenia a rekonfigurácie operačného systému. V súčasnosti je nasadzovaný v bankovom, telekomunikačnom a priemyselnom prostredí, ako aj na špecializované účely, ako je overovanie front-end superpočítačov, streamingové hudobné služby, obnova po havárii a analýza rizík počítačovej bezpečnosti. Hlavnou kľúčovou funkciou serveru MAAS pre naše účely bude automatizácia, kedy pomocou Intelligent Platform Management Interface (IPMI) si MAAS zapne/reštartuje daný stroj a pomocou Preboot eXecution Environment (PXE) buď cez sieť IPv4 alebo IPv6 nainštaluje požadovaný alebo predvolený operačný systém na tento úkon. Ďalšími užitočnými funkciami je konfigurácia úložiska, sieťových rozhraní a manažment IP adries pomocou Dynamic Host Configuration Protocol (DHCP) [8].

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

1.2.2 Na čo slúži server Juju?

Juju je open-source framework, ktorý využíva Charmed Operatorov alebo „Charms“ na nasadenie cloudovej infraštruktúry, aplikácií a správu ich operácií od spustenia. S Juju je možné inštalovať, udržiavať, upgradovať a integrovať aplikácie naprieč klastrami, kontajnermi Kubernetes, virtuálnymi a fyzickými strojmi na verejných alebo súkromných cloudoch. Výrobcovia opisujú Juju ako softvér, ktorý riadi váš softvér. Pomáha vám prevziať kontrolu nad všetkými vašimi aplikáciami, infraštruktúrou a prostrediami. Použitie tohto softvéru by malo zabezpečiť:

- ušetrenie času stráveného nad správou skriptov
- minimalizovať náklady
- zabezpečiť redundanciu a odolnosť
- monitorovať všetky aktivity naprieč infraštruktúrou
- maximalizovať architektúru hybridného cloudu

Charmy sú malé aplikácie, ktoré obsahujú bežné sady inštrukcií funkcií, aby zabezpečili opakovateľný a spoľahlivý kód. Toto umožňuje spravovať aplikácie a scenáre namiesto konfigurácií, avšak v prípade potreby je tu stále možnosť ponoriť sa do konfiguračných súborov YAML (YAML Ain’t Markup Language). Charmed Operators sa nevyužívajú len na nasadzovanie a spravovanie jednotlivých aplikácií, ale aj na ich spájanie medzi sebou v modeloch. Aplikačný model definuje, ktoré aplikácie poskytujú službu a ako spolu súvisia. Riadenie Juju je možné pomocou príkazové riadku (CLI) alebo pomocou grafického webového rozhrania (GUI) ako je Juju GUI [9].

1.2.3 Typ inštalácie OpenStack-u

Pre samotnú inštaláciu OpenStack-u bola zvolená ako najvhodnejšia metóda OpenStack-Charms, Charmed Operators alebo tiež nazývane „Charms“ sa používajú na nasadenie a správu cloudov OpenStack pomocou Metal-as-a-Service (MAAS) a Juju. Ako prvé bude potrebné nainštalovať server MAAS a nasadiť pomocou neho server Juju. Následne budeme môcť pomocou bundle konfiguračného súboru postaviť OpenStack metódou Charms. Na inštaláciu máme k dispozícii virtuálne servery, ktoré budú slúžiť na inštaláciu MAAS, Juju a ako

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Controller Node. Ďalšie fyzické servery budú slúžiť primárne na beh virtuálnych inštancií v OpenStack-u pomocou komponentu Nova. Nižšie v tabuľkách nájdeme rozdelenie jednotlivých komponentov, privátne IP adresy, ktoré sú pre servery určené a značkovanie, ktoré dostanú v systéme MAAS.

Stroj	Komponenty
controller	Ceph-radosgw, Cinder, Designate, Glance, Heat, Keystone, MySQL (x3), Neutron- api, Nova cloud controller, Openstack- dashboard, Ovn-central (x3), Placement, RabbitMQ, Vault
compute-1	Nova, NTP, Ovn-chassis
compute-2	Nova, NTP, Ovn-chassis
compute-3	Nova, NTP, Ovn-chassis
compute-4	Nova, NTP, Ovn-chassis
compute-7	Nova, NTP, Ovn-chassis, Ovn-Central, Ceph-Osd, Ceph-Mon, Manila, Manila- Ganesha, Ceph-FS
compute-8	Nova, NTP, Ovn-chassis, Ovn-Central, Ceph-Osd, Ceph-Mon, Manila, Manila- Ganesha, Ceph-FS
compute-9	Nova, NTP, Ovn-chassis, Ovn-Central, Ceph-Osd, Ceph-Mon, Manila, Manila- Ganesha, Ceph-FS
compute-10	Nova, NTP, Ovn-chassis, Ovn-Central, Ceph-Osd, Ceph-Mon, Manila, Manila- Ganesha, Ceph-FS
compute-11	Nova, NTP, Ovn-chassis, Ovn-Central, Ceph-Osd, Ceph-Mon, Manila, Manila- Ganesha, Ceph-FS

Tabuľka 1 **– Rozdelenie komponentov na jednotlivé stroje**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

IP adresa	Účel	Virtuálny/fyzický stroj
10.11.0.1	Predvolená brána	-

10.11.0.2	MAAS	maas1 (VMWare)
10.11.0.3	Juju	juju1 (VMWare)
10.11.0.11	Controller Node	controller1 (VMWare)
10.11.0.21	Compute Node 1	IBM X3650M5
10.11.0.22	Compute Node 2	IBM X3650M5
10.11.0.23	Compute Node 3	IBM X3650M3
10.11.0.24	Compute Node 4	IBM X3650M5
10.11.0.27	Compute Node 7	HP DL380G9 iLO
10.11.0.28	Compute Node 8	HP DL380G9 iLO
10.11.0.29	Compute Node 9	HP DL380G9 iLO
10.11.0.30	Compute Node 10	Dell R720 iDRAC
10.11.0.31	Compute Node 11	IBM X3650M3

Tabuľka 2 – IP adresový rozsah pre stroje OpenStacku

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Označenie server v MAAS	Značka(Tag) v MAAS
juju.maas	juju
controller.maas	controller
compute-1.maas	compute1
compute-2.maas	compute2
compute-3.maas	compute3
compute-4.maas	compute4
compute-7.maas	compute7
compute-8.maas	compute8
compute-9.maas	compute9
compute-10.maas	compute10
compute-11.maas	compute11

Tabuľka 3 – Značkovenie(Tagy) pre stroje v MAAS

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

1.2.4 Inštalácia servera MAAS

Pre server MAAS bol v našej infraštruktúre vytvorený virtuálny stroj so 4 vCPU (virtual central processing units), 8GB operačnej pamäte a 50GB diskom. V tomto prípade bolo ešte potrebné ručne nainštalovať operačný systém a to konkrétne Linux Ubuntu vo verzii 22.04.1 LTS. Počas inštalácie operačného systému bola nakonfigurovaná statická IP adresa 10.11.0.2, predvolená brána 10.11.0.1, DNS servery nastavené na katedrové s IP adresami 158.193.152.4 a 158.193.152.11. Meno servera bolo nastavené na „maas“ a vytvorený používateľský účet „student“ s dohodnutým heslom. Ako prvý krok boli vygenerované secure shell (SSH) kľúče, ktoré neskôr využijeme pri inicializácii. Pomocou príkazu vygenerujeme nové SSH kľúče do súboru /home/student/.ssh/student:

```
ssh-keygen -t rsa
```

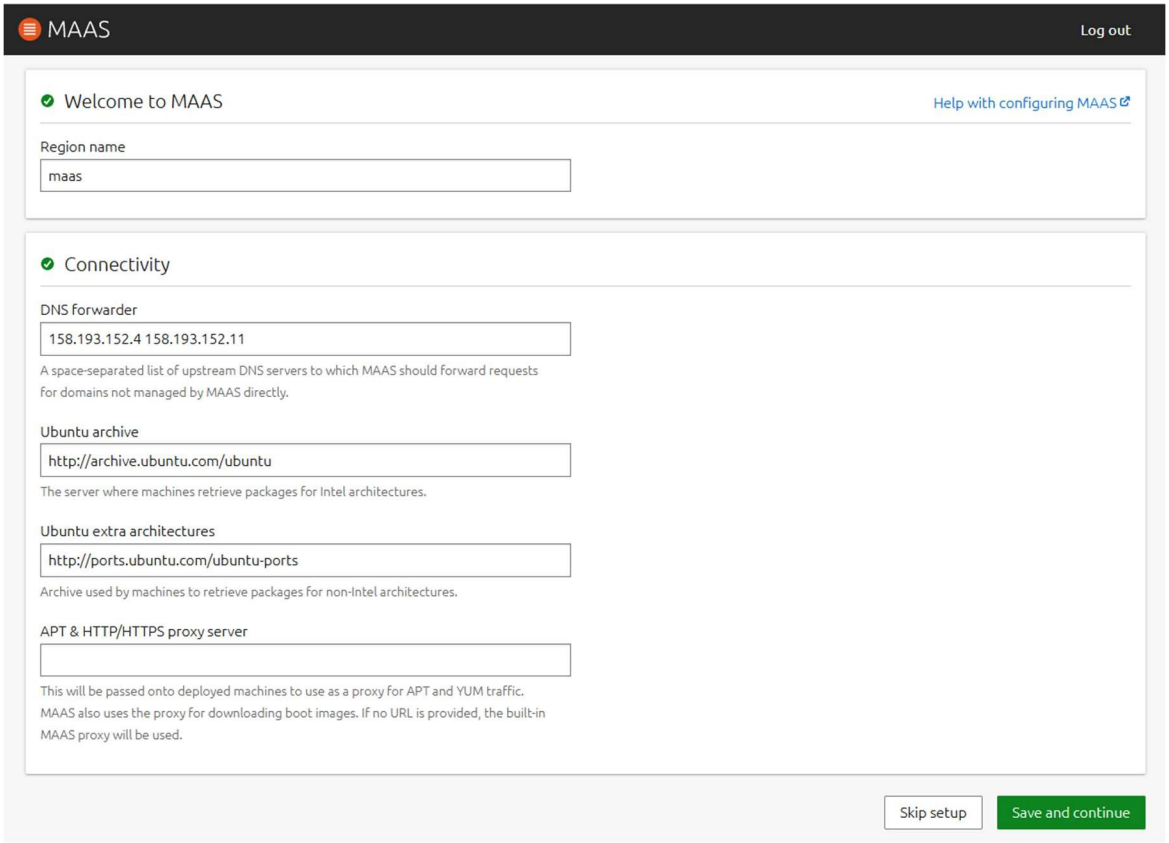
Následne môžeme začať s inštaláciou MAAS. MAAS nainštalujeme vo verzii 3.1, IP adresu pri príkaze init použijeme, ktorú sme konfigurovali počas inštalácie operačného systému. Pri príkaze createadmin vytvoríme používateľské konto s menom „student“,

<PASSWORD> nahradíme reálnym heslom a email nastavíme „student@kis.fri.uniza.sk.

```
sudo snap install maas-test-db
sudo snap install maas --channel=3.1/stable
sudo maas init region+rack --maas-url http://10.11.0.2:5240/MAAS --database-uri
maas-test-db:///
sudo maas createadmin --username student --password <PASSWORD> --email
student@kis.fri.uniza.sk
sudo maas apikey --username student > maas-api-key #ulozenie api kluca do suboru
```

Následne môžeme pokračovať v inicializácií MAAS priamo v prehliadači a to na adrese z inicializácie: http://10.11.0.2:5240/MAAS. Po prvotnom prihlásení je potrebné urobiť základnú konfiguráciu. V prvom kroku nastavíme meno regiónu na „maas“ a uvedieme DNS servery na katedrové DNS servery s IP adresami 158.193.152.4 a 158.193.152.11.

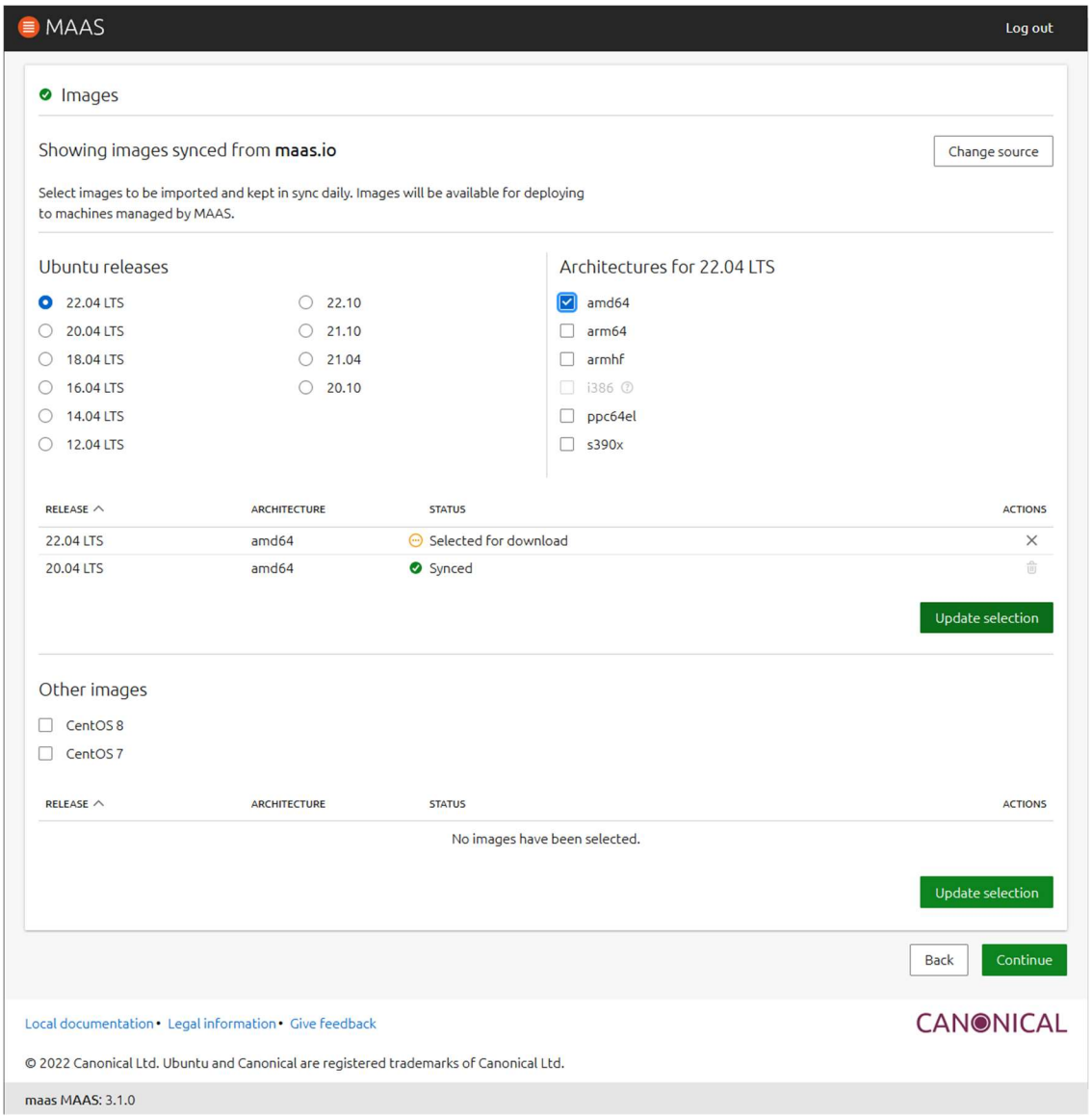
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



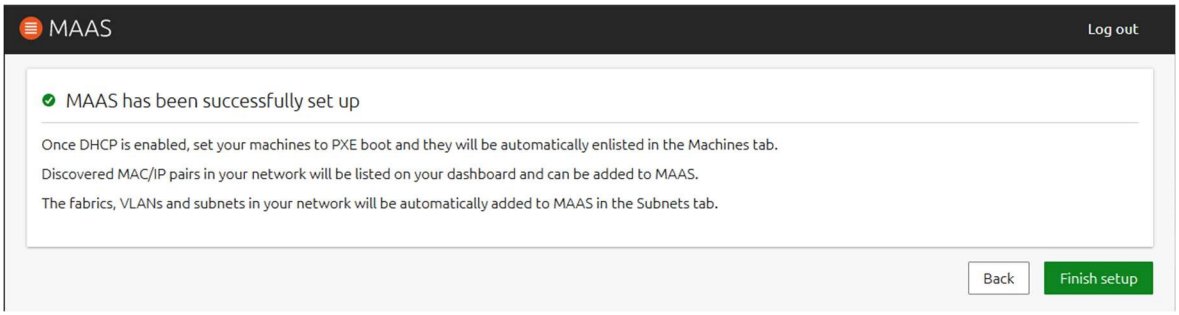
Obrázok 2 - Prvotné nastavenie MAAS – meno regiónu + DNS špeditéri

V druhom kroku je možné stiahnuť ďalšie obrazy na bootovanie okrem základnej verzie 20.04 LTS s architektúrou amd64, vzhľadom k tomu, že chceme verziu OpenStack Yoga, je potrebné stiahnuť aj obraz 22.04 LTS s architektúrou amd64 a potvrdiť pomocou tlačidla „Update selection“.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 3 - Prvotné nastavenie MAAS – Obrazy na bootovanie



Obrázok 4 - Prvotné nastavenie MAAS – úspešné dokončenie

V ďalšom kroku je potrebné naimportovať vygenerovaný SSH kľúč, ktorý sme vygenerovali pri inštalácií. Ako zdroj vyberieme typ „Upload“ a verejný SSH kľúč vypísaný napríklad príkazom cat vložíme do poľa „Public key“.

```
cat /home/student/.ssh/student.pub
```


Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

1.2.5 Základne nastavenie DHCP v MAAS

Jednou z výhod, ktoré boli spomenuté pri funkciách MAAS je DHCP server, ktorým disponuje. Tento DHCP server musíme po nainštalovaní a inicializácií nakonfigurovať. Všetky tieto zmeny budeme vykonávať pomocou MAAS CLI a preto ako prvé je potrebné sa prihlásiť pomocou používateľského účtu a API kľúča MAAS na MAAS serveri.

```
maas login student http://10.11.0.2:5240/MAAS - <  maas-api-key
```

Keďže chceme, aby kontajnery v OpenStack-u dostávali IP adresy z rozsahu 10.11.1.0 – 10.11.1.255, musíme vytvoriť dve rezervácie rozsahov pre statické IP adresy a potom dynamický rozsah pre zvyšok, ktorý sa môže používať na DHCP. Rezervovaný rozsah pre statické IP (10.11.0.1 - 10.11.0.255), čo chceme my používať a dynamický rozsah pre DHCP (10.11.2.0 - 10.11.255.254) a tým pádom bude kontajnerom v OpenStack-u priradzovať rozsah 10.11.1.0 - 10.11.1.255

```
maas student ipranges create type=dynamic \
    start_ip=10.11.2.0 end_ip=10.11.255.254

maas student ipranges create type=reserved \
    start_ip=10.11.0.1 end_ip=10.11.0.255 \
    comment='Static IPs'
```

Následne môžeme zapnúť DHCP v neznačkovanej miestnej sieti (VLAN) vo „fabric-0“.

„Fabric“ vytvorí MAAS počas inštalácie pre každú zistenú podsieť, je to niečo ako spojka medzi VLAN sieťami. V prípade, že by MAAS server bol pripojený do viacerých VLAN sietí, tak fabric umožní spojenie, je to niečo ako prepínač alebo kombinácia prepínačov využívajúce trunking.

```
maas student vlan update 0 untagged dhcp_on=True \
    primary_rack=maas
```

1.2.6 Upgrade MAAS

Tak ako každý softvér je možné upgradovať aj verziu MAAS, pri inštalácií bola použitá verzia 3.1 a medzičasom vyšla stabilná verzia 3.2. Upgrade je možné vykonať jediným príkazom v prípade použitia „region+rack“ (možnosť vyčítať z inštalácie pri init príkaze):

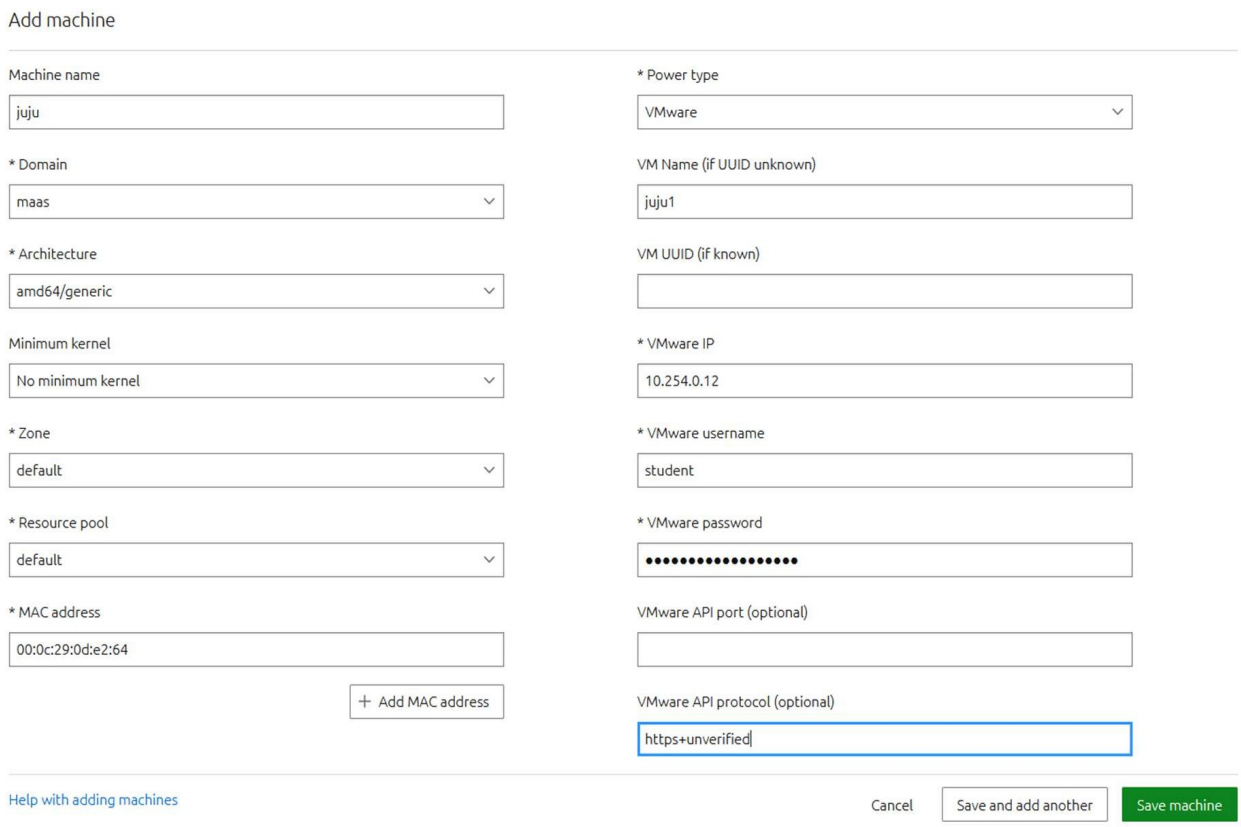
```
sudo snap refresh --channel=3.2 maas
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Za prepínačom „--channel“ uvedemie verziu. Po spustení a zadaní hesla nie je nutné reinicializovať MAAS.

1.2.7 Nasadenie servera Juju

V tomto bode už nasadzovanie už môžeme využiť funkcie servera MAAS, ktorý nám inštaláciu Juju servera uľahčí. Ako prvé bude potrebné pridať server juju1 (VMWare), pre ktorý bolo vyhradených 4 vCPUs, 4 GB operačnej pamäte a 50 GB disku. Pridať virtuálny alebo fyzický stroj do MAAS je možné dvomi spôsobmi. Prvý spôsob je zapnúť server a pokiaľ má povolené bootovanie pomocou PXE, tak MAAS mu priradí IP adresu a následne poskytne obraz na bootovanie. Po načítaní obrazu si MAAS zozbiera základné informácie o stroji a zobrazí v zozname vo webovom prehliadači. Teraz je možné upraviť premenné ako názov, IP adresu a IPMI podľa potreby. Druhým spôsobom je vyplniť vo webovom rozhraní MAAS potrebné údaje pre pridanie stroja a zahájiť uvedenie do prevádzky (commissioning).

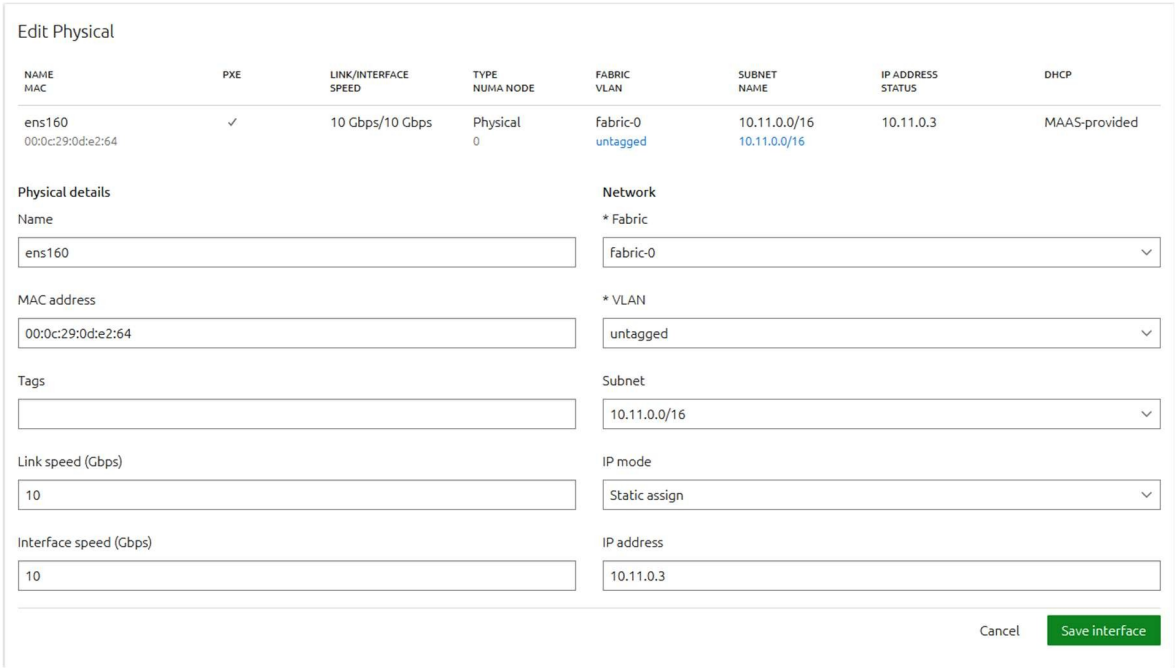


Obrázok 5 – Pridanie stroja Juju do MAAS pomocou webového rozhrania

Po úspešnom uvedení do prevádzky, bude potrebné ešte vykonať zmeny v konfigurácii pre tento stroj a to IP adresu na statickú 10.11.0.3 a vytvorenie označenia tzv. tagu. Všetky tieto zmeny sa budú vykonávať vo webovom rozhraní. Po rozkliknutí „juju.maas“ ako prvé v záložke „Network“, v našom prípade pri rozhraní ens160 klikneme na šípku smerujúcu dole pod sekciou „Actions“ a vyberieme možnosť „Edit physical“. Následne sa nám otvorí okno s možnosťou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

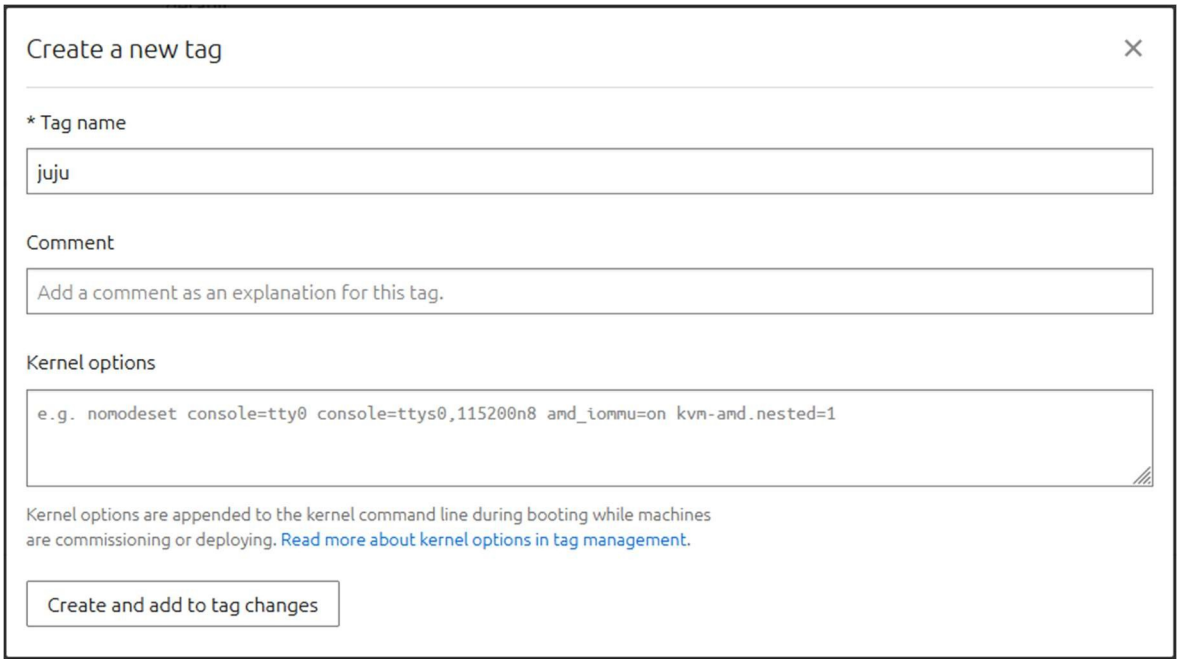
úpravy. Pre nastavenie statickej IP adresy je nutné len nastaviť „IP mode“ na „Static assign“ a do poľa „IP address“ vypísať potrebnú IP adresu a to 10.11.0.3 a už len uložiť rozhranie pomocou zeleného tlačidla „Save interface“.



Obrázok 6 – Nastavenie statickej IP adresy v MAAS webovom rozhraní

Označenie vytvoríme v záložke „Configuration“ v sekcií Tags, kde klikneme na „Edit“. Následne pomocou vyhľadávacieho poľa, ktoré sa nám zobrazilo, vytvoríme označenie „juju“ a to tak, že ho do poľa vpíšeme a následne sa zobrazí možnosť „*Create tag* „juju““ a kliknutím na túto možnosť sa zobrazí okno na vytvorenie označenia, kde môžeme napísať aj komentár alebo určiť možnosti pre Kernel. Následne už len dokončíme pomocou tlačidla „Create and add to tag changes“. Kde v upravovanej sekcii „Tags“ vidíme, že sa pridalo označenie juju a už len uložíme pomocou „Save“.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 7 – Vytvorenie označenia(tag) pre server Juju v MAAS webovom rozhraní

Ďalej budeme pokračovať v CLI priamo na MAAS serveri. Ako prvé je potreba doinštalovať juju.

```
Sudo snap install juju –classic
```

Vytvoríme YAML konfiguračný súbor s následnými premennými. IP adresa je systému MAAS a po vytvorení súboru pridáme cloud s názvom „maas-one“.

```
Nano maas-cloud.yaml #vytvorenie a otvorenie súboru

#začiatok súboru maas-cloud.yaml
clouds:
  maas-one:
    type: maas
    auth-types: [oauth1]
    endpoint: http://10.11.0.2:5240/MAAS
#koniec súboru maas-cloud.yaml

#pridanie cloudu s konfiguračným súborom maas-cloud.yaml s názvom maas-one
juju add-cloud –client -f maas-cloud.yaml maas-one
```

Pridáme poverenia z MAAS, aby mohla Juju integrovať s novo pridaným cloudom. Na import opäť použijeme konfiguračný súbor YAML s názvom maas-creds.yaml (názov môže byť ľubovoľný) a pomocou príkazu „juju add-credential“ pridáme.

```
#maas-oauth je maas-api-key kľúč z inštalácie, ktorý nájdeme v súbore rovnako
pomenovamo a to maas-api-key

nano maas-creds.yaml #vytvorenie a otvorenie súboru

#začiatok súboru maas-creds.yaml
```


Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

```
credentials:
  maas-one:
    anyuser:
      auth-type: oauth1
      maas-oauth:
VcLNh2986dQcHD3fCt:t9gpGYeNjTKEFfjQgj:uLeqhLZZ4UlcghArpNWe9yRueGCpX2n4
#koniec súboru maas-creds.yaml

#pridanie poverení s konfiguračným súborom maas-creds.yaml do cloudu maas-one
juju add-credential -client -f maas-creds.yaml maas-one
```

Teraz môžeme spustiť inštaláciu Juju kontroléra na server. Dôležité je v prepínači „– constraints“ uviesť „tags=juju“, ktorý sme pri konfigurácií v MAAS priradili serveru, aby bolo možné označiť server, na ktorý sa má nainštalovať. Ďalej je uvedené meno cloudu a teda „maas-one“ a pomenovanie kontroléra „maas-controller“.

```
Juju bootstrap -bootstrap-series=focal -constraints tags=juju maas-one maas-
controller
```

Po zadaní tohto príkazu by sme mali vidieť vo webovom rozhraní zapnutie daného servera a už len počkať, kým bude všetko nainštalované a dokončené. Po úspešnej inštalácií pridáme administrátorské konto „student“ kvôli jednotnému prístupu.

```
#vytvorenie konta, následný výpis budeme ignorovať juju add-user
student

#priradenie superuser privilégií pre konto student juju grant
student superuser

#vytvorenie hesla pre konto student
juju change-user-password student

#overenie vo výpise juju
users
```

```
student@maas:~$ juju users
Controller: maas-controller

Name      Display name  Access     Date created  Last connection
admin*    admin         superuser  2022-10-27    just now
student                 superuser  2022-10-27    2022-11-09

student@maas:~$
```

Obrázok 8 – Overenie pridaného konta student pre Juju

Následne si môžeme vypísať adresu umiestnenia stránky (URL) a to buď s povereniami pre admin konto alebo len samotnú URL.

```
#výpis URL + admin povereniami
juju dashboard
```


Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

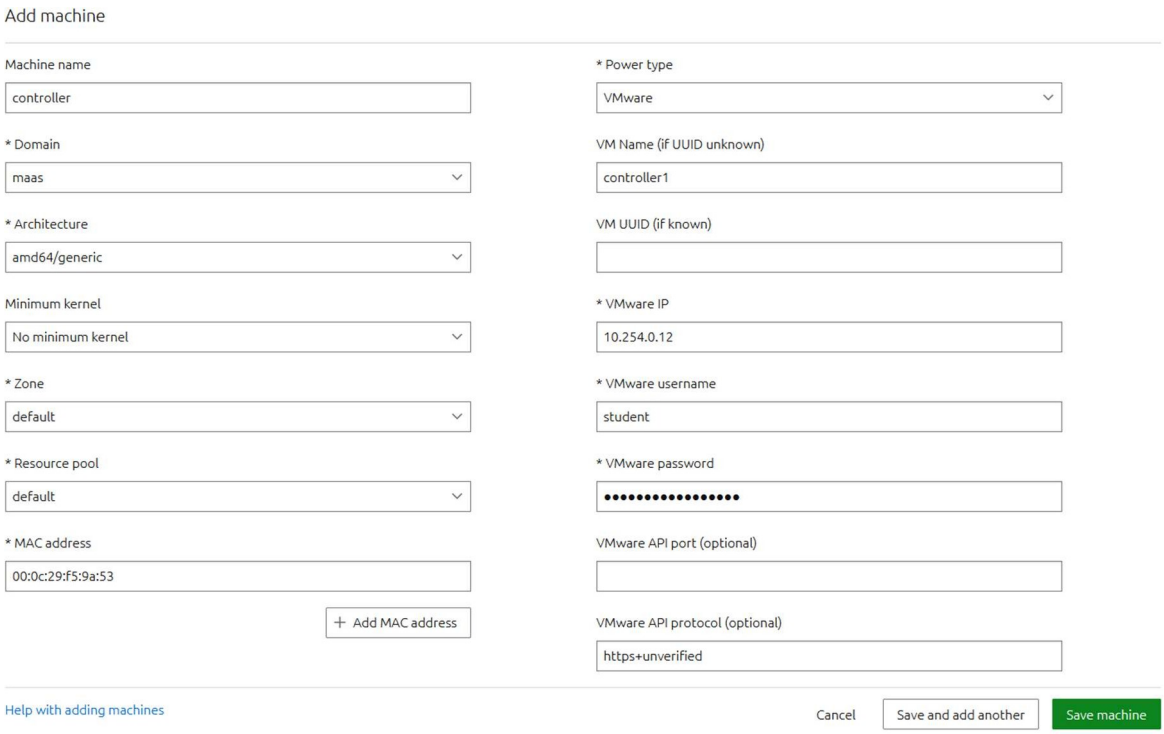
```
#výpis URL bez poverení
juju dashboard -hide-credential
```

Keďže sme priradili statickú IP adresu stroju pre Juju, tak adresa na umiestnenie stránky bude: https://10.11.0.3:17070/dashboard. Následne sa môžeme prihlásiť a uvidíme webové rozhranie pre Juju. Prístup priamo na server je potom možný pomocou SSH s použitím SSH kľúča.

```
Ssh ubuntu@10.11.0.3 -i /home/student/.local/share/juju/ssh/juju_id_rsa
```

1.2.8 Pridanie serverov určených pre beh OpenStack-u

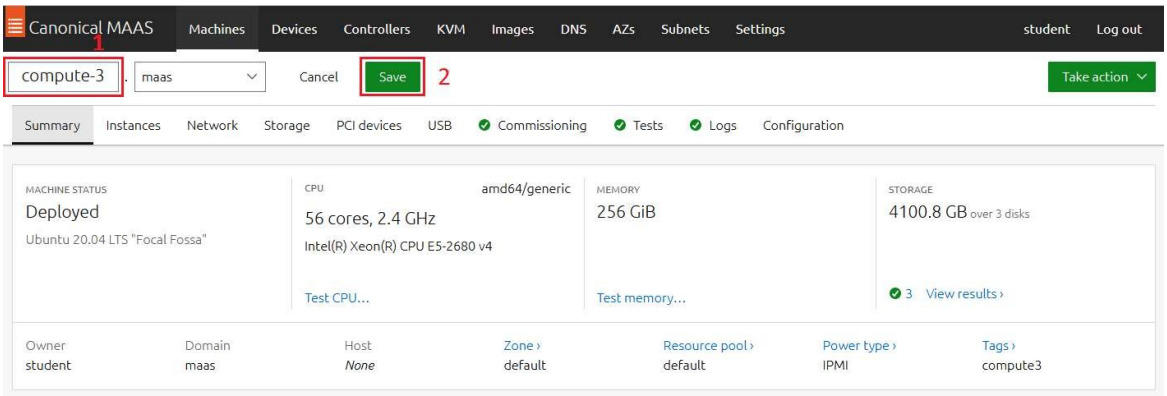
Tak ako v prípade Juju servera, aby sme mohli využiť funkciu automatizácie, pridáme servery, na ktorých bude nainštalovaný OpenStack do MAAS. Bude sa jednať o jeden ovládací uzol tzv. Controller Node a tri výpočtové uzly tzv. Compute Nody. Controller Node je virtuálny stroj, ktorý beží na rovnakom fyzickom serveri ako MAAS a Juju s 32 vCPUs, 64GB operačnej pamäti a 100GB miesta na disku. Ten bude možné pridať rovnakým spôsobom ako Juju server. Taktiež mu následne rovnakým spôsobom vytvoríme značku (Tag) podľa tabuľky „Tabuľka 2 – Značkovanie (Tagy) pre stroje v MAAS“. IP adresu zatiaľ nebude potrebné konfigurovať z dôvodu, že budeme robiť zmeny v sieťovom nastavení v neskoršej fáze.



Obrázok 9 - Pridanie Controller Node do MAAS pomocou webového rozhrania

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Pre Compute Nody použijeme druhý spôsob. Najskôr na jednotlivých serveroch bude potrebné nastaviť ako prioritu bootovanie cez PXE a následne po zapnutí si MAAS tieto servery priradí a zistí informácie. V tomto prípade nebude potrebné nastavovať IPMI, nakoľko to MAAS spraví za nás. Použitím tohto spôsobu pridania bude potrebné rozlíšiť jednotlivé servery, pretože MAAS im predvolené zvolí náhodné meno a toto bude potrebné upraviť aj s vytvorením značky (Tagu). Pre tieto servery tiež nebudeme konfigurovať IP adresy. Meno servera zmeníme tak, že po rozkliknutí servera klikneme v ľavom hornom rohu na meno a následne vpíšeme požadované a uložíme pomocou tlačidla „Save“.



Obrázok 10 – Zmena mena servera v MAAS webovom rozhraní

1.2.9 Konfigurácia siete v systéme MAAS

Ako prvú zmenu a predprípravu pre konfigurácie rozhraní na serveroch musíme upraviť podsiete v systéme MAAS. Ako prvé vytvoríme priestory (Spaces), ktoré slúžia ako zoskupenie podsieti a umožňuje im komunikovať medzi sebou. Ďalej upravíme priestor pre „fabric-0“, vytvoríme vlany a podsiete. Všetky tieto zmeny budeme vykonávať pomocou MAAS CLI a preto ako prvé je potrebné sa prihlásiť pomocou používateľského účtu a API kľúča MAAS na MAAS serveri.

```
maas login student http://10.11.0.2:5240/MAAS - <  maas-api-key
```

Následne môžeme vytvoriť priestory. Po každom príkaze dostaneme informáciu, či vytvorenie prebehlo úspešne v podobe výpisu „Success“ a informácia o danej štruktúre ako napríklad meno a identifikátor. My budeme potrebovať dva priestory s názvami „openstack-mgmt“ a „openstack-vxlan“, ktoré uvedieme pri vytváraní ako požadovaný parameter.

```
maas student spaces create name="openstack-mgmt"
maas student spaces create name="openstack-vxlan"
```


Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Po vytvorení priestorov môžeme vytvoriť VLAN siete a upraviť neznačkovanú VLAN sieť vo „fabric-0“. Najskôr upravíme neznačkovanú VLAN sieť a to tak, že jej priradíme priestor „openstack-mgmt“.

```
maas student vlan update 0 untagged space="openstack-mgmt"
```

VLAN siete, ktoré ďalej vytvoríme budú mať všetky požadované parametre „fabric“ identifikátor 0 a vid podľa potrebnej hodnoty. Využijeme aj voliteľný parameter pre lepšiu identifikáciu a to meno. Ku VLAN sieti s identifikátorom 500 a menom „brVXLAN“ priradíme aj druhý vytvorený priestor „openstack-vxlan“.

```
maas student vlans create 0 name="brEX" vid=153
maas student vlans create 0 name="brEX2" vid=154
maas student vlans create 0 name="brVXLAN" vid=500 space="openstack-vxlan"
```

Následne už stačí len vytvoriť podsiete s beztriednym smerovaním medzi doménami (CIDR), menom, „fabric“ identifikátor a identifikátorom VLAN siete.

```
maas student subnets create cidr="158.193.153.0/24" name="EXT1" fabric=0 vid=153 maas student
subnets create cidr="158.193.154.0/24" name="EXT2" fabric=0 vid=154
maas student subnets create cidr="10.12.0.0/24" name="VXLAN" fabric=0 vid=500
```

1.2.10 Zmena konfigurácie siete pre Controller Node

Pre potreby OpenStack-u potrebujeme zabezpečiť rovnaké sieťové konfigurácie rozhraní naprieč všetkými uzlami. Pri Controller Node je konfigurácia trošku odlišná, nakoľko sa jedná o virtuálny server a má len jedno sieťové rozhranie. Toto rozhranie premenujeme a vytvoríme mosty s príslušnými VLAN sieťami a IP adresami. Zmeniť konfiguráciu sa dá pomocou CLI, tak aj pomocou webového rozhrania GUI. Pre efektívnosť a možnosti automatizácie tohto kroku budeme pracovať v CLI na serveri MAAS, ale v prílohách bude návod aj pre GUI. V prvom kroku, pokiaľ tomu tak nie je sa prihlásime na serveri MAAS pod účtom student.

```
maas login student http://10.11.0.2:5240/MAAS - <  maas-api-key
```

Počas tohto kroku aj nasledujúceho budeme potrebovať identifikátory(ID) serverov, ktoré im MAAS priradilo. Tie si vypíšeme pomocou nasledujúceho príkazu.

```
maas student machines read | jq '.[] | .hostname, .system_id'
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Názov	ID
juju	7ckx7w
controller	kgseyr
compute-1	8gsdnw
compute-2	nn7n7k
compute-3	bt8cge
compute-4	xkhy38
compute-7	anhqyc
compute-8	hhshym
compute-9	c6xpxx
compute-10	ncwf6s
compute-11	eyttr6

Tabuľka 4 – Zoznam identifikátorov serverov v MAAS

Keď už poznáme ID jednotlivých serverov, tak pomocou príkazu read si vypíšeme aj ID sieťových rozhraní na Controller Node.

```
maas student interfaces read pbpdab | jq '.[] | .id, .name'
```

Z výpisu sme zistili, že jediné rozhranie s názvom ens160 má ID 5. Toto ID a ID servera v systéme MAAS využijeme pri premenovaní sieťového rozhrania ens160 na názov „bond“.

```
maas student interface update kgseyr 5 name=bond
```

Tomuto sieťovému rozhraniu teraz priradíme VLAN siete, ktoré sme vytvárali v predchádzajúcom kroku. Opätovne budeme musieť zistiť aj ID pre tieto VLAN siete, ktoré im priradil systém MAAS v našom Fabric-0.

```
maas student vlans read 0
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

VLAN	ID
untagged	5001
153(brEX)	5007
154(brEX2)	5009
500(brVXLAN)	5008

Tabuľka 5 – Zoznam identifikátorov VLAN v MAAS

Následne môžeme vytvoriť jednotlivé VLAN siete nad týmto rozhraním a to s pomocou ID servera, ID VLAN a ID tohto sieťového rozhrania. Pri úspešnom vytváraní VLAN bude v rámci výstupu vypísané aj ID, ktoré je potrebné zapísať. Stačí ID prvého nakoľko číslovanie je sekvenčné. Teda ak prvá pridaná VLAN sieť má ID 520, tak nasledujúca bude mať ID 521.

```
maas student interfaces create-vlan kgseyr vlan=5007 parent=5 maas student
interfaces create-vlan kgseyr vlan=5009 parent=5
maas student interfaces create-vlan kgseyr vlan=5008 parent=5
```

Teraz vytvoríme nad jednotlivými VLAN sieťami a samotným sieťovým rozhraním mosty typu Open vSwitch(OVS). Pri tomto kroku je potrebné tiež odsledovať nové ID pre posledný krok.

```
maas student interfaces create-bridge kgseyr name=brEX vlan=5007 parent=520
bridge_type=ovs
maas student interfaces create-bridge kgseyr name=brEX2 vlan=5009 parent=521
bridge_type=ovs
maas student interfaces create-bridge kgseyr name=brVXLAN vlan=5008 parent=522
bridge_type=ovs
maas student interfaces create-bridge kgseyr name=brMGMT vlan=5001 parent=5
bridge_type=ovs
```

Posledným krokom je pridanie podsietí pre novovytvorené sieťové rozhrania, avšak najskôr budeme potrebovať ID jednotlivých podsietí.

```
maas student subnets read
```

Názov podsiete	ID
10.11.0.0/16	1
EXT1	3
EXT2	5
VXLAN	2

Tabuľka 6 – Zoznam identifikátorov podsietí v MAAS

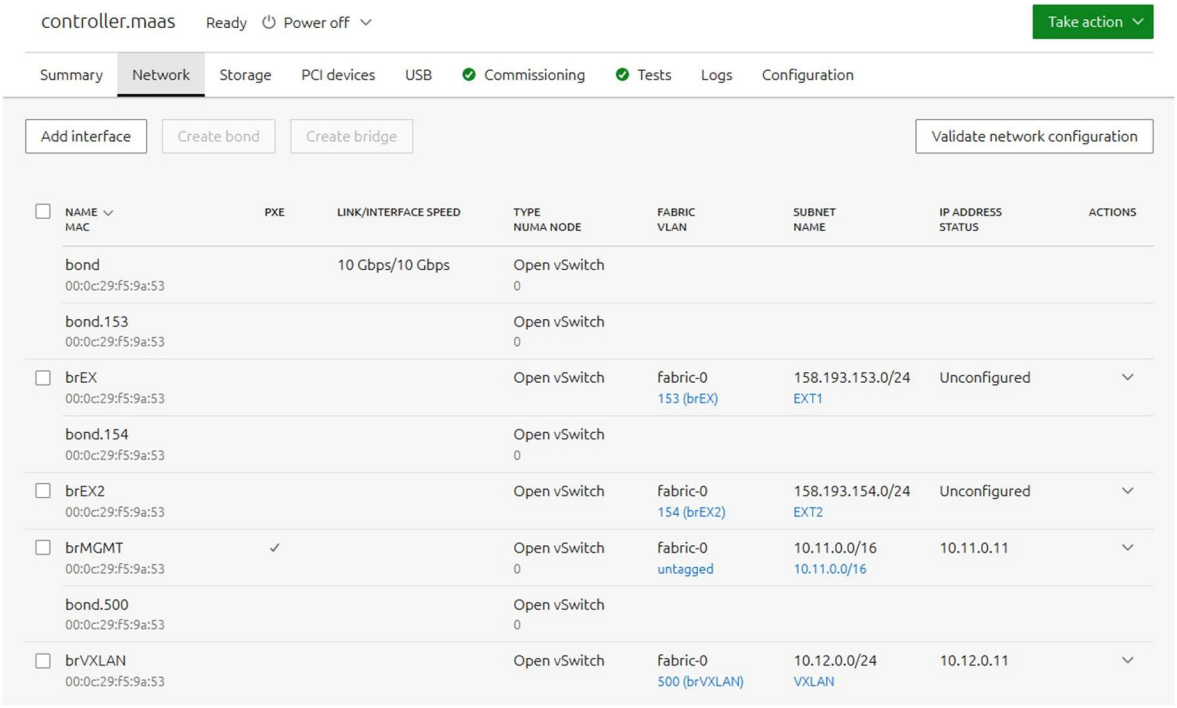
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Rozhraniam pre VLAN siete 153(brEX) a 154(brEX2) priradíme len podsieť a mód nastavíme na „LINK_UP“, čo značí, že sa rozhranie zapne len pre danú podsieť a nepriradí sa IP adresa.

```
maas student interface link-subnet kgseyr 524 mode=LINK_UP subnet=3
maas student interface link-subnet kgseyr 525 mode=LINK_UP subnet=5
```

Pre rozhranie manažmentu (neznačkovaná prevádzka) a VLAN siete 500 (brVXLAN), použijeme mód statický a nastavíme statické IP adresy.

```
maas student interface link-subnet kgseyr 526 mode=STATIC subnet=2
ip_address=10.12.0.11
maas student interface link-subnet kgseyr 527 mode=STATIC subnet=1
ip_address=10.11.0.11
```



Obrázok 11 – Zobrazenie celej sieťovej konfigurácie pre Controller Node v GUI

1.2.11 Zmena konfigurácie siete pre Compute Nody

V prípade Compute Nodov budeme postupovať podobne ako v predchádzajúcom kroku, až na pár zmien. Hneď v prvom kroku nebude len premenovávať sieťové rozhranie, ale dve fyzické rozhrania spojíme do jedného pomocou bondu. V tomto prípade budeme potrebovať aj MAC (Media Access Control) adresu jedného z rozhraní, my zvolíme prvú v poradí.

```
maas student interfaces read xpxd4w | jq '.[] | .id, .mac_adress, .name'
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Z výpisu sme zistili, že naše dve rozhrania majú ID 38 (enp68s0f0) a 43 (enp68s0f1) a MAC adresa, ktorú použijeme z rozhrania enp68s0f0 je 00:1b:21:d4:62:3c. Bond mód použijeme 802.3ad a hash politiku nastavíme na „layer2+3“.

```
maas student interfaces create-bond xpxd4w name=bond parents=38
mac_address=00:1b:21:d4:62:3c parents=43 bond_mode=802.3ad
bond_xmit_hash_policy=layer2+3
```

Nezabudneme si zapísať ID vytvorené bondu a pridáme VLAN siete.

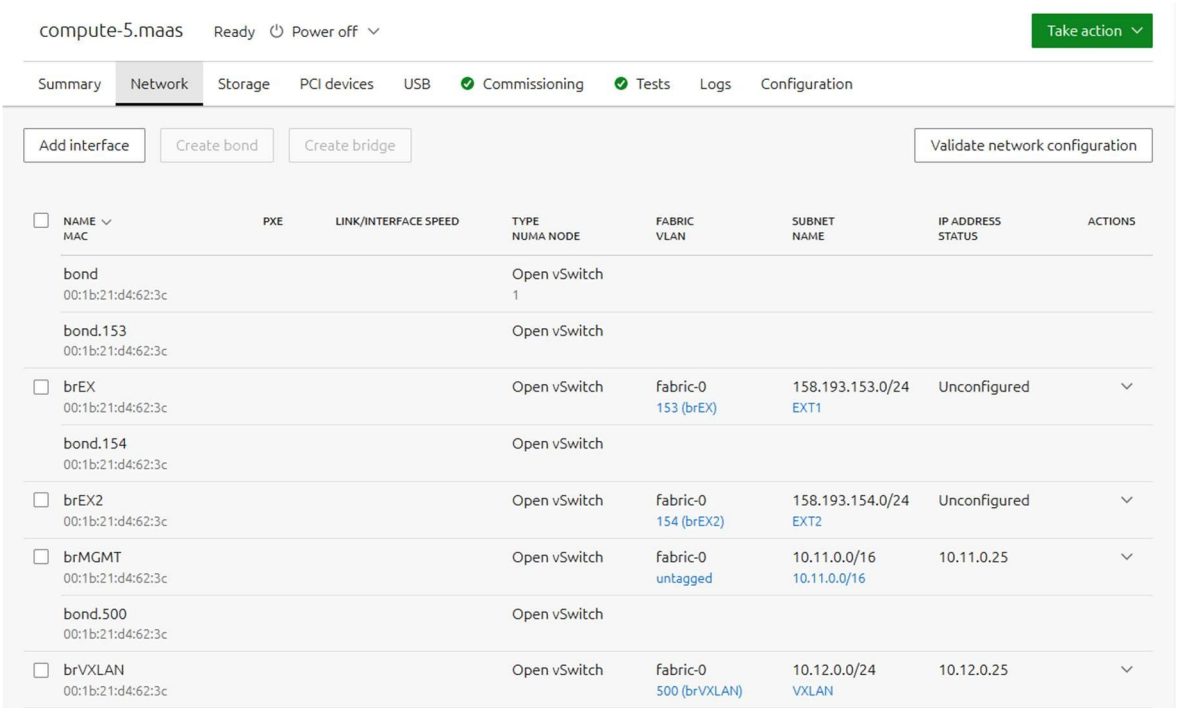
```
maas student interfaces create-vlan xpxd4w vlan=5007 parent=529 maas student
interfaces create-vlan xpxd4w vlan=5009 parent=529
maas student interfaces create-vlan xpxd4w vlan=5008 parent=529
```

A už pokračujeme ako v prípade Controller Nodu, vytvoríme mosty a priradíme podsiete.

```
maas student interfaces create-bridge xpxd4w name=brEX vlan=5007 parent=530
bridge_type=ovs
maas student interfaces create-bridge xpxd4w name=brEX2 vlan=5009 parent=531
bridge_type=ovs
maas student interfaces create-bridge xpxd4w name=brVXLAN vlan=5008 parent=532
bridge_type=ovs
maas student interfaces create-bridge xpxd4w name=brMGMT vlan=5001 parent=529
bridge_type=ovs
```

```
maas student interface link-subnet xpxd4w 533 mode=LINK_UP subnet=3
maas student interface link-subnet xpxd4w 534 mode=LINK_UP subnet=5
maas student interface link-subnet xpxd4w 535 mode=STATIC subnet=2
ip_address=10.12.0.25
maas student interface link-subnet xpxd4w 536 mode=STATIC subnet=1
ip_address=10.11.0.25
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 12 - Zobrazenie celej sieťovej konfigurácie pre Compute Node v GUI

1.2.12 Zmena konfigurácie diskov pre Compute Nody

Po pridaní servera do systému MAAS nie je jednoznačné, ktorý disk zo servera zvolí ako systémový. Preto je nutné túto konfiguráciu skontrolovať a poprípade upraviť. Budeme postupovať podobne ako v prípade konfigurácie sieťových rozhraní a taktiež pomocou CLI. Využijeme už získané ID jednotlivých serverov a vypíšeme si disky, ktorými disponujú. Konkrétne si vypíšeme len veľkosti diskov a ich ID.

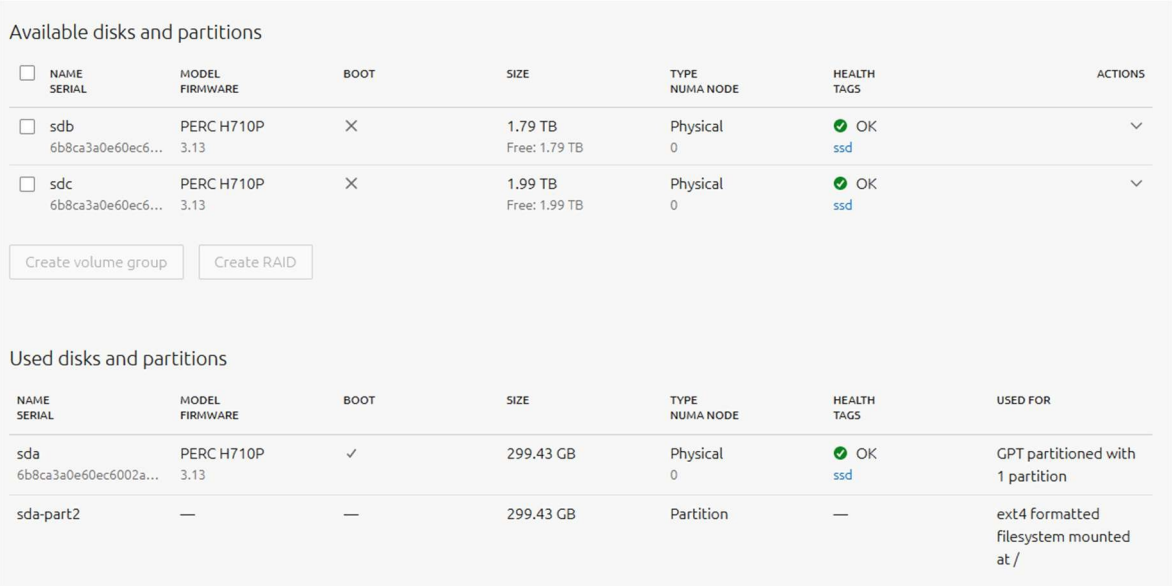
```
maas student block-devices read xpxd4w | jq '.[] | .size, .id'
```

Vieme, že servery sú osadené diskami o veľkosti 300GB, 1.8TB a 2TB. My chceme ako systémový disk použiť práve najmenší 300GB disk. V tomto prípade má tento disk ID 13. Nastavenie systémového disku spočíva len v jednom príkaze a to určenie ID servera a ID disku.

```
maas student block-device set-boot-disk xpxd4w 13
```

Kontrolu nastavenia systémového disku môžeme vykonať pomocou GUI, po rozkliknutí daného servera, záložka „Storage“ a následne hľadáme symbol fajky v stĺpci „Boot“.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 13 – Zobrazenie nastavenie systémového disku v GUI

1.2.13 Nastavenie minimálneho jadra (kernel-u)

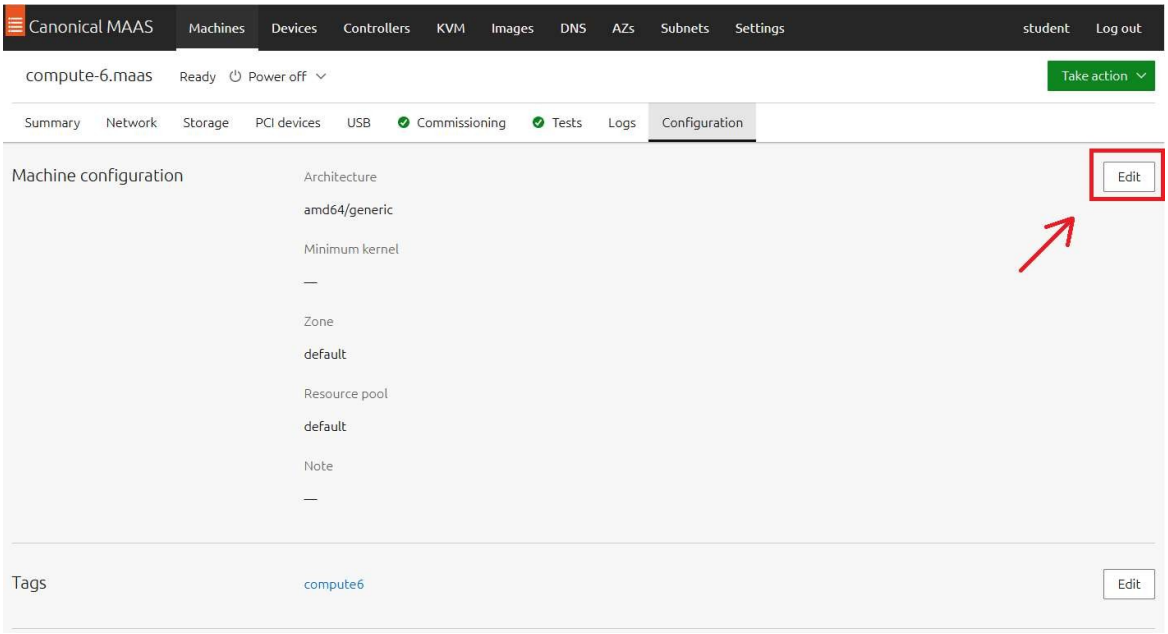
Pri skúšobnom nasadení OpenStack-u nastal problém komunikácie MAAS a jedného z compute nodov, konkrétne compute-6. Problém spočíval v komunikácií medzi serverom a MAAS po nainštalovaní operačného systému. Pri spustení inštalácie príkazy z MAAS-u na zapnutie a následne nahratie operačného systému prebehli v poriadku, ale ďalej už serveru zlyhala komunikácia, podľa chybovej hlášky nemal sieťovú konektivitu. Vzhľadom k nášmu heterogénnemu zloženiu serverov môže nastať aj takáto skutočnosť, kedy compute-6 je rovnaký typ servera ako compute-3 a compute-4, ale má inú sieťovú kartu. Riešenie spočívalo v nastavení minimálneho jadra pre operačný systém, ktoré obsahovalo aj ovládač pre sieťovú kartu, ktorá bola osadená v serveri compute-6. Za zistenie tejto skutočnosti ďakujem Ing. Martinovi Kontšekovi, PhD. Nastavenie minimálneho jadra operačného systému môžeme nastaviť ako cez CLI, tak aj vo webovom rozhraní. Cez CLI sa prihlásime do MAAS, pokiaľ už tak nie je a pomocou príkazu na nastavenie minimálneho jadra a systémového ID pre server nastavíme požadovanú hodnotu. V tomto prípade si schováme výstup, ktorý by bol vypísaný pomocou „> /dev/null“ nakoľko je príliš dlhý. Na overenie použijeme príkaz len na vypísanie položky, ktorá obsahuje našu kontrolovanú hodnotu.

```
maas login student http://10.11.0.2:5240/MAAS - < /home/student/maas-api-key

maas student machine update 8h7kbn min_hwe_kernel=hwe-20.04 > /dev/null

maas student machine read 8h7kbn | jq '.hostname, .min_hwe_kernel'
```

```
student@maas:~$ maas student machine read 8h7kbn | jq '.hostname, .min_hwe_kernel'
"compute-6"
"hwe-20.04"
student@maas:~$
```

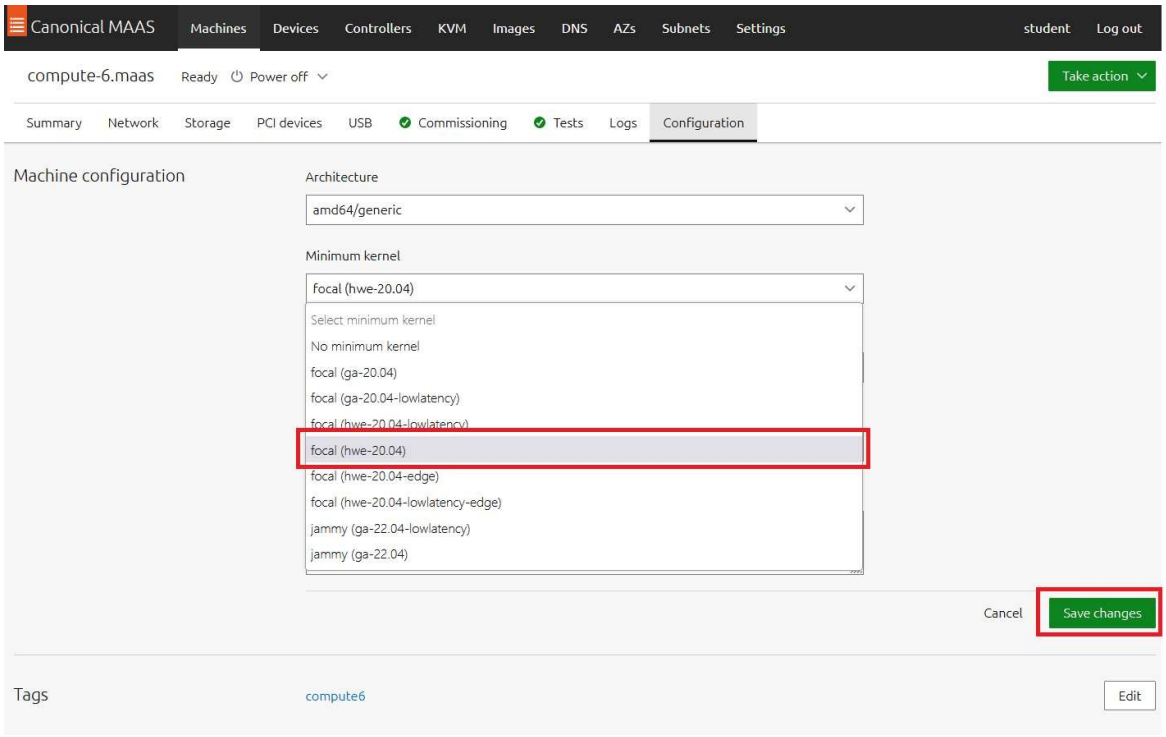
Obrázok 14 - Príklad výpisu kontrolnej hodnoty pri zmene minimálneho jadra

V prípade nastavenia cez webové rozhranie si v záložke „Machines“ otvoríme „compute-6.maas“. V záložke „Configuration“ klikneme na tlačidlo „Edit“, ktoré sa nachádza v sekcií „Machine configuration“. Otvoríme si rozbaľovacie menu „Minimum kernel“ a zvolíme požadovanú hodnotu, v našom prípade „focal (hwe-20.04) a klikneme na tlačidlo „Save changes“. Po vykonaní týchto úkonov môžeme skontrolovať, že predtým hodnota „Minimum kernel“ bola nastavená na „—“ a teraz tam už je naša požadovaná hodnota „hwe- 20.04“.

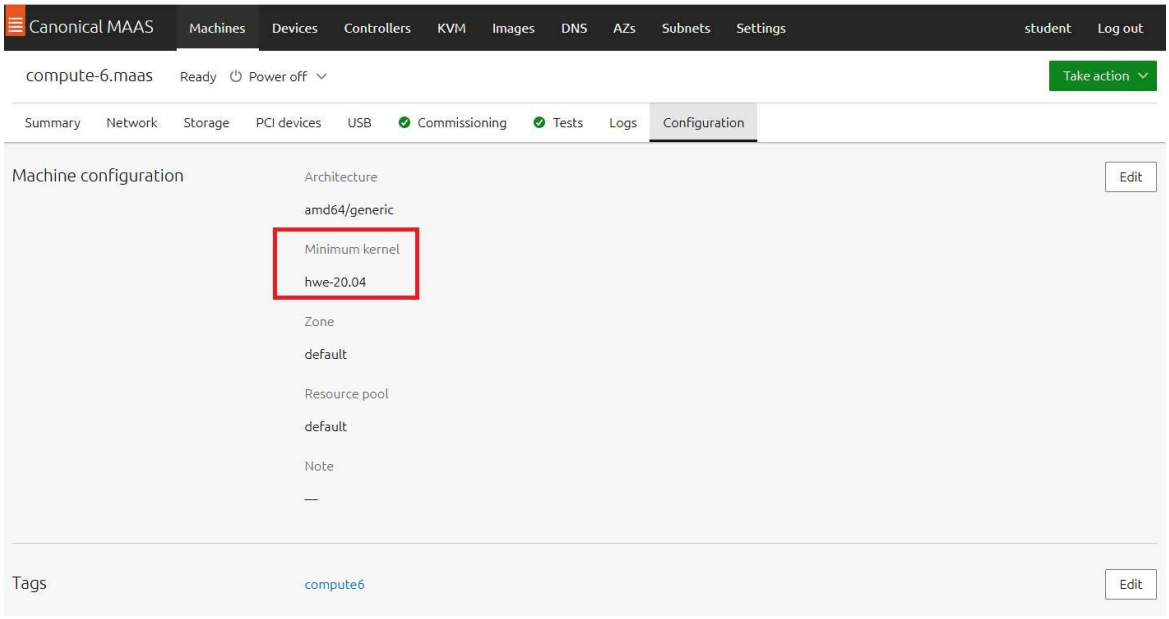


Obrázok 15 - Nastavenie minimálneho jadra vo webovom rozhraní MAAS

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 16 - Nastavenie minimálneho jadra vo webovom rozhraní MAAS



Obrázok 17 - Nastavenie minimálneho jadra vo webovom rozhraní MAAS

1.2.14 Inštalačný balíček (bundle) pre OpenStack

Ako už bolo spomínané, na samotnú inštaláciu OpenStack-u použijeme inštalačný balíček tzv. bundle, ktorý bude súčasťou príloh. Oproti ručnej inštalácií sú hlavne výhody v tom, že nie je potrebné každý príkaz kopírovať alebo vytvárať konfiguračné súbory pre komponenty a všetko je pekne zrozumiteľne a prehľadne v

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

jednom súbore. To znamená, že po otvorení a prezretí takéhoto súboru daný čitateľ zistí, aké komponenty budú nainštalované, aké vzťahy budú vytvorené alebo použité sieťové rozhrania a iné. Bundle sa skladá z piatich častí: hlavička, premenné, stroje (servery), vzťahy a aplikácie. V hlavičke sa uvádza meno a séria, v našom prípade je názov „openstack-base“ a budeme používať sériu „focal“ na operačné systémy Linux Ubuntu:

```
name: openstack-base
series: focal
```

Ďalej je sekcia premenných, v nej je ako prvé určené opäť séria „focal“, použitá na určenie operačného systému na serveroch spolu s verziou OpenStack-u. Data-port určuje, ktoré sieťové mosty (bridge) budú namapované, na ktoré sieťové rozhrania. V našom prípade táto sekcia bude obsahovať aj premenné pre komponent Ceph Osd a to:

- pevné disky, ktoré budú použité pre tento komponent
- počet serverov, na ktorých bude tento komponent nainštalovaný
- počet serverov, na ktorých bude nainštalovaný monitorovací komponent

Okrem hlavičkovej sekcie, každá sekcia má svoj názov a informácie v nej sú odsadené tabulátorom alebo v prípade sekcie vzťahov pomlčkou.

```
variables:
  openstack-origin: &openstack-origin cloud:focal-yoga
  data-port: &data-port brEX:bond.153 brEX2:bond.154 brVXLAN:bond.500
  osd-devices: &osd-devices /dev/sdb /dev/sdc
  expected-osd-count: &expected-osd-count 5
  expected-mon-count: &expected-mon-count 5
```

V sekcií strojov (serverov) je možné si očíslovať stroje podľa vlastnej konvencie a priradiť im v prípade potreby označkovanie (tag) zo systému MAAS.

```
machines:
  '11':
    constraints: tags=controller
  '23':
    constraints: tags=compute3
  '24':
    constraints: tags=compute4
```

Pri vzťahoch sa na odlíšenie používajú pomlčky a to nasledovne:

- prvý komponent, s ktorým sa má vytvoriť vzťah je označený dvomi pomlčkami s medzerou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

- druhý komponent, s ktorým sa má vytvoriť vzťah je najskôr odsadený tabulátorom a až potom nasleduje jedna pomlčka

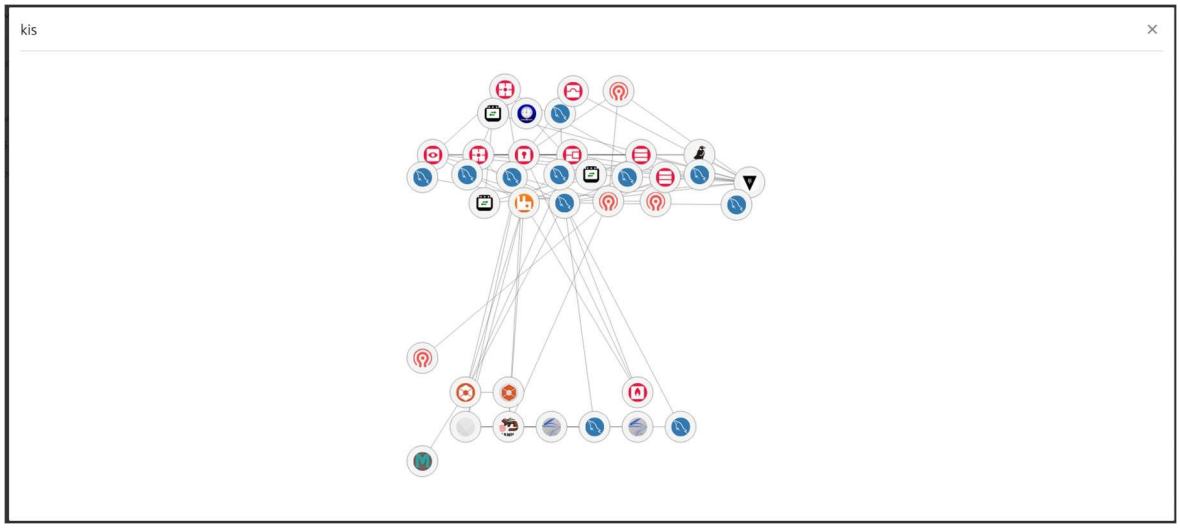
```
relations:
- - nova-compute:amqp
  - rabbitmq-server:amqp
- - nova-cloud-controller:identity-service
  - keystone:identity-service
- - glance:identity-service
  - keystone:identity-service
```

V poslednej sekcií aplikácií (komponentov) je to pri rôznych aplikáciách rôznorodé, pretože nie všetky majú rovnaké možnosti, ale základ majú rovnaký. Konkrétne si rozoberieme komponent Nova. Ako prvé sú väzby (bindings), ktoré sú voliteľným prvkom a uvádzajú, ktoré dáta z daného komponentu budú využívať daný priestor (space) z MAAS-u. Anotácie určujú bod podľa súradníc X a Y, kde bude umiestnená ikona komponentu v Juju webovom grafickom rozhraní znázorňujúci daný model. Charm a kanál (channel) určujú aká verzia daného komponentu bude nainštalovaná, kompletný zoznam verzií a kanálov môžeme nájsť na charmhub.io, napr. https://charmhub.io/nova-compute. Počet jednotiek (num_units) uvádza koľkokrát bude komponent nainštalovaný. Možnosti (options) sa líšia komponent od komponentu, zoznam a významy jednotlivých možností nájdeme taktiež na stránke charmhub.io. Ako posledné je opäť voliteľná možnosť, kedy môžeme určiť na ktoré stroje bude komponent nainštalovaný, v opačnom prípade to Juju spraví automaticky. V prípade komponentov, ktoré sú inštalované v kontajneroch je potrebné uvádzať pred číslom stroja „lxd:“.

```
applications:
  nova-compute:
    bindings:
      "": openstack-mgmt
      internal: openstack-mgmt
      migration: openstack-mgmt
    annotations:
      gui-x: '190'
      gui-y: '890'
    charm: ch:nova-compute
    channel: yoga/stable
    num_units: 5
    options:
      config-flags: default_ephemeral_format=ext4
      enable-live-migration: true
      enable-resize: true
      migration-auth-type: ssh
      openstack-origin: *openstack-origin
    to:
    - '23'
    - '24'
    - '25'
    - '26'
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

```
    - '27'
  mysql-innodb-cluster:
    bindings:
      "": openstack-mgmt
      shared-db: openstack-mgmt
    annotations:
      gui-x: '535'
      gui-y: '1550'
    charm: ch:mysql-innodb-cluster
    channel: 8.0/stable
    num_units: 3
    to:
    - lxd:11
    - lxd:11
    - lxd:11
```



Obrázok 18 - Príklad zobrazenia modelu kis v Juju webovom rozhraní pomocou ikon komponentov a prepojení (vzťahov) medzi nimi

1.2.15 Inštalácia OpenStacku Yoga

V tomto momente máme pripravené a nakonfigurované všetko potrebné pre spustenie inštalácie platformy OpenStack Yoga pomocou balíčka (bundle). Začneme nahraním tohto súboru vo formáte YAML na server MAAS. Budeme pokračovať v CLI na serveri MAAS pomocou príkazu na vytvorenie modelu s názvom „kis“ a majiteľom konta „student“. Následne už len stačí spustiť inštaláciu pomocou príkazu „deploy“ a cestou k bundle.

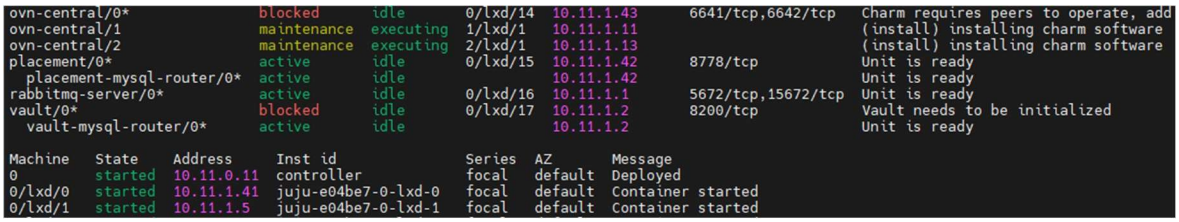
```
juju add-model kis

juju deploy ./bundleKIS.yaml
```

Po určitom čase (15-20 minút) môžeme skontrolovať stav inštalácie pomocou príkazu:

```
juju status
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

V prípade že komponent s názvom Vault je v stave „Idle“ a status je „Vault needs to be initialized“ bude treba vykonať posledný krok a to odpečatiť ho. Predtým ako začneme musíme ešte nainštalovať softvér na to potrebný.



Obrázok 19 – Zapečatený a neinicializovaný trezor (Vault) pri inštalácii

```
sudo snap install vault
```

Vyexportujeme IP adresu kontajnera, kde je nainštalovaný modul Vault (juju status).

```
export VAULT_ADDR=http://10.11.1.30:8200
```

Zahájime inicializáciu pomocou „init“ príkazu a uvedieme počet kľúčov, ktoré sa vypíšu a počet kľúčov, ktoré budú potrebné na odpečatenie. Z výstupu je potrebné si uchovať najlepšie všetky kľúče alebo počet potrebný na odpečatenie. Taktiež si uložíme „Initial Root Token“.

```
vault operator init -key-shares=5 -key-threshold=3
```

Výstup:

```
Unseal Key 1: 9xCIrnapVFY5QKWPx6UcrZAL0f2l7Gl2cZ2y2/ydZA+u Unseal Key
2: Ahs6PAEwSosNki7W0+idDCaD4rnUy+FmzGQsN/0yopLB
Unseal Key 3: Ac0hWoHGqxRev9SWlvzrNlgUxtng3YHbqFWQTJJWr2CP
Unseal Key 4: mGVNmEW7MvBJAqP4VJ8wv452Ls949Tl9V+/6gMXl15lB
Unseal Key 5: yALNYeOBllNrg77Ws67xKznmA9mylxeGJ/aNXQExpzGF

Initial Root Token: s.Un84Rz15EjUmfb9uk3uQRhqb

Vault initialized with 5 key shares and a key threshold of 3. Please securely distribute the key
shares printed above. When the Vault is re-sealed, restarted, or stopped, you must supply at least 3
of these keys to unseal it before it can start servicing requests.

Vault does not store the generated master key. Without at least 3 key to

reconstruct the master key, Vault will remain permanently sealed!

It is possible to generate new unseal keys, provided you have a quorum of
existing unseal keys shares. See "vault operator rekey" for more information.
```


Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Zoberieme počet kľúčov z „-key-threshold=“ a použijeme v príkazoch „vault operator unseal“.

```
vault operator unseal 9xClrnapVFY5QKWPx6UcrZAL0f2l7Gl2cZ2y2/ydZA+u vault
operator unseal Ahs6PAEwSosNki7W0+idDCaD4rnUy+FmzGQsN/0yopLB
vault operator unseal Ac0hWoHGqxRev9SWlvzrNlgUxtng3YHbqFWQTJJWr2CP
```

V príkaze export VAULT_TOKEN použijeme Initial Root Token z predchádzajúceho výpisu.

```
export VAULT_TOKEN=s.Un84Rz15EjUmfb9uk3uQRhqb
vault token create -ttl=10m
```

Výstup:

```
Key                  Value
---                  -----
token                s.KFrGIuaSB9JuioHaCttgFRAN
token_accessor       gkG8YIMYg6j2DYjWgAxCADnC
token_duration       10m
token_renewable      true
token_policies       ["root"]
identity_policies    []
policies             ["root"]
root@openstackmaas:~#
```

Token použijeme v nasledujúcom príkaze:

```
 juju run-action --wait vault/leader authorize-charm
token=s.KFrGIuaSB9JuioHaCttgFRAN
```

Posledný príkaz na vygenerovanie koreňových certifikátov:

```
juju run-action --wait vault/leader generate-root-ca
```

Po vygenerovaní certifikátov je potrebné ešte nejakú dobu počkať až kým všetky komponenty nebudú v stave „active“ a „idle“. Následne si môžeme vypísať heslo od administrátorského konta pomocou príkazu:

```
juju run --unit keystone/leader leader-get admin_passwd
```

Prístup na webové rozhranie je na IP adrese komponentu Openstack-dashboard: https://<IP_ADRESA>/horizon. Prihlasovacie údaje sú:

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

User Name: admin
Password: <PASSWORD>
Domain: admin_domain

Pre prístup odkiaľkoľvek na konzolu virtuálnych inštancií v OpenStack-u, nakoľko sa všade používajú privátne IP adresy, nakonfigurujeme proxy IP adresu.

```
juju config nova-cloud-controller console-proxy-ip=158.193.152.130
```

A pre nastavenie predvolenej domény pre prihlasovanie, aby sa nemusela zakaždým vypisovať.

```
juju config openstack-dashboard default-domain="admin_domain"
```

1.2.16 Konfigurácia MAAS servera pre automatickú autentifikáciu pre OpenStack CLI klienta

Po úspešnej inštalácii OpenStack-u je možné konfigurovať túto platformu buď cez webové grafické rozhranie, ktoré zabezpečuje komponent Horizon, alebo pomocou OpenStack klienta vo forme CLI. Pre niektoré úkony je lepšie práve webové grafické rozhranie, pre iné zasa forma CLI, ako napr. vytvorenie externých sietí, ktoré bude menej časovo náročné. OpenStack klient nainštalujeme na server MAAS pomocou jednoduchého príkazu:

```
sudo snap install openstackclients
```

Následne treba vykonať autentifikáciu pomocou exportov a aby nebolo nutné túto autentifikáciu robiť zakaždým ručne, pridáme do súboru „.bashrc“ kód na automatickú autentifikáciu. Tento súbor sa spúšťa pri každom prihlásení na server. V prvej časti sa nakopírujú certifikáty na správne miesta, následne sa do premenných _keystone_ip a _password pomocou Juju príkazov uložia IP adresa komponentu Keystone a administrátorské heslo. Pomocou exportov sa nastavia potrebné premenné a ako overenie sa vypíše tabuľka prístupových bodov OpenStack-u [10].

```
#Login OpenStack CLI Client
JUJU_MODEL=kis
if [ -d ~/snap/openstackclients/common/ ]; then
  # When using the openstackclients confined snap the certificate has to be
  # placed in a location reachable by the clients in the snap.
  _root_ca=~/snap/openstackclients/common/${JUJU_MODEL-""}root-ca.crt
else
  _root_ca=/tmp/${JUJU_MODEL-""}root-ca.crt
fi
```


Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

```
juju run $_juju_model_arg --unit vault/leader 'leader-get root-ca' | tee
$_root_ca >/dev/null 2>&1

_keystone_ip=$(juju run -m kis --unit keystone/leader -- 'network-get --bind-
address public')
_password=$(juju run -m kis --unit keystone/leader 'leader-get admin_passwd')

export OS_REGION_NAME=RegionOne
export OS_AUTH_VERSION=3
export OS_CACERT=/home/student/snap/openstackclients/common/root-ca.crt
export OS_AUTH_URL=https://${_keystone_ip}:5000/v3
export OS_PROJECT_DOMAIN_NAME=admin_domain
export OS_AUTH_PROTOCOL=https
export OS_USERNAME=admin
export OS_AUTH_TYPE=password
export OS_USER_DOMAIN_NAME=admin_domain
export OS_PROJECT_NAME=admin
export OS_PASSWORD=${_password}
export OS_IDENTITY_API_VERSION=3

echo "--- Testing exports to initialize OpenStack CLI Client ---"
echo "--- Printing endpoints of OpenStack ---"
openstack endpoint list --interface admin
#End of login OpenStack CLI Client
```

```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-53-generic x86_64)

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

  System information as of Fri Dec  2 08:50:26 AM UTC 2022

  System load:  0.0029296875      Processes:               287
  Usage of /:   67.6% of 23.45GB  Users logged in:         0
  Memory usage: 27%               IPv4 address for ens160: 10.11.0.2
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

18 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Fri Dec  2 08:31:27 2022 from 10.11.0.1
--- Testing exports to initialize OpenStack CLI Client ---
--- Printing endpoints of OpenStack ---
+----------------------------------+-----------+--------------+--------------+---------+-----------+-----------------------------------------+
| ID                               | Region    | Service Name | Service Type | Enabled | Interface | URL                                     |
+----------------------------------+-----------+--------------+--------------+---------+-----------+-----------------------------------------+
| 02baecf0cd314b4aa1bbbfce4efc1790 | RegionOne | placement    | placement    | True    | admin     | https://10.11.1.30:8778                 |
| 339f4b046c554dd3ad6c1591837fb02b | RegionOne | keystone     | identity     | True    | admin     | https://10.11.1.20:35357/v3             |
| 3d59654f31be4fdfa71d5263c4bb8817 | RegionOne | neutron      | network      | True    | admin     | https://10.11.1.22:9696                 |
| 3ed243be17df4e64a49f43e0092db1ea | RegionOne | glance       | image        | True    | admin     | https://10.11.1.33:9292                 |
| 86a9db4b118b4460855e828c14a3bd26 | RegionOne | swift        | object-store | True    | admin     | https://10.11.1.26:443/swift            |
| 9a9c237931154479a3bc1badc0524e79 | RegionOne | nova         | compute      | True    | admin     | https://10.11.1.31:8774/v2.1            |
| be42141354344daaa28f9d537b37f3d8 | RegionOne | cinderv3     | volumev3     | True    | admin     | https://10.11.1.27:8776/v3/$(tenant_id)s |
| eaa421d7ce0349d8b6c43cc6b499b6fb | RegionOne | s3           | s3           | True    | admin     | https://10.11.1.26:443/                 |
+----------------------------------+-----------+--------------+--------------+---------+-----------+-----------------------------------------+
student@maas:~$
```

Obrázok 20 – Ukážka autentifikácie po prihlásení na server MAAS

1.2.17 Vytvorenie externých sietí pre OpenStack

Platforma OpenStack používa na komunikáciu virtuálnych inštancií s vonkajšími sieťami tzv. externú siete. V našom prípade máme aktuálne k dispozícii dva IP adresové rozsahy, ktoré môžeme použiť pre prideľovanie verejných IP adries virtuálnym inštanciám. Vytvorenie takejto externej siete je možné pomocou webového rozhrania OpenStack-u, alebo my sme zvolili možnosť pomocou CLI OpenStack klienta. Keďže disponujeme dvomi adresovými rozsahmi a to 158.193.153.0/24 a 158.193.154.0/24, potrebujeme vytvoriť dve externé siete. Prvú externú sieť vytvoríme s názvom „ext-net-153“ ako „provider-network- type“ zvolíme možnosť „flat“, aby pakety boli zasielané neupravené. Ako „provider-physical-

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

network“ uvedieme „physnet1“, ktorú sme v inštalačnom balíčku uviedli ako „flat-network-providers“ a následne namapovali na most brEX a ten na fyzické rozhranie bond.153. Pre túto externú sieť „ext-net-153“ vytvoríme aj podsieť s prideľovaním IP adries v rozsahu 158.193.153.2 – 158.193.153.254, katedrovým DNS serverom s IP adresou 158.193.152.4, predvolenou bránou 158.193.153.1 a názvom EXT1.

```
openstack network create --external --share \
   --provider-network-type flat --provider-physical-network physnet1 \
   ext-net-153

openstack subnet create --network ext-net-153 \
  --allocation-pool start=158.193.153.2,end=158.193.153.254 \
  --dns-nameserver 158.193.152.4 --gateway 158.193.153.1 \
  --subnet-range 158.193.153.0/24 EXT1
```

V prípade druhej externej siete „ext-net-154“ budeme postupovať rovnakým spôsobom, až na zmenu názvu a pre „provider-physical-network“ uvedieme „physnet2“, ktorý je v inštalačnom balíčku namapovaný ďalej na most brEX2 a fyzické rozhranie bond.154. Pri vytváraní podsiete samozrejme tiež vymeníme IP adresný rozsah v treťom oktete na 154 a pomenujeme EXT2.

```
openstack network create --external --share \
   --provider-network-type flat --provider-physical-network physnet2 \
   ext-net-154

openstack subnet create --network ext-net-154 \
  --allocation-pool start=158.193.154.2,end=158.193.154.254 \
  --dns-nameserver 158.193.152.4 --gateway 158.193.154.1 \
  --subnet-range 158.193.154.0/24 EXT2
```

Na overenie môžeme použiť príkazy na výpis sietí a podsietí v OpenStack-u.

```
openstack network list
openstack subnet list
```

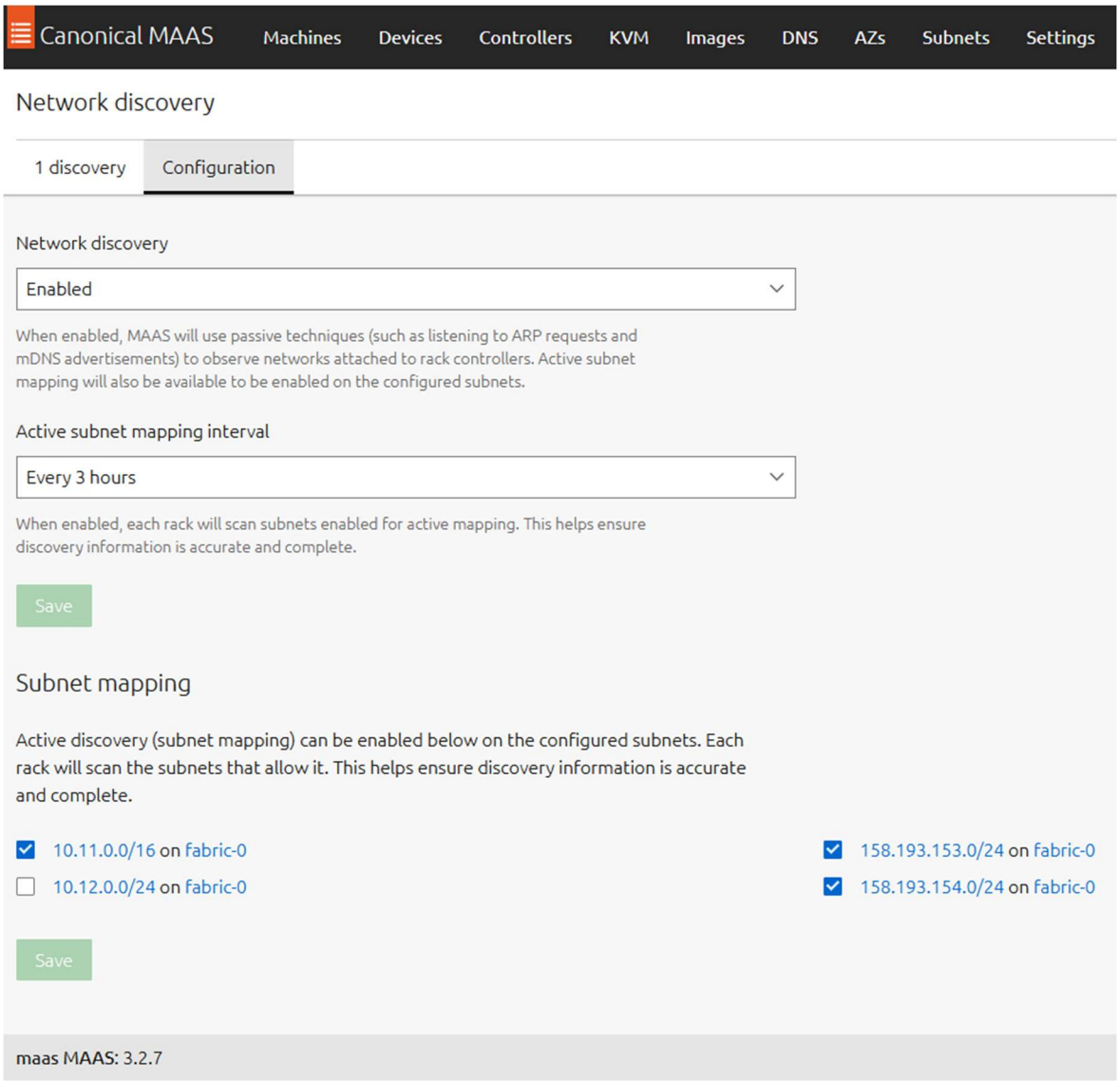
```
student@maas:~$ openstack network list
+--------------------------------------+-------------+--------------------------------------+
| ID                                   | Name        | Subnets                              |
+--------------------------------------+-------------+--------------------------------------+
| 3e7591c8-c85f-4447-a7ba-0deb2cbe8860 | ext-net-153 | 86e73eb3-2743-48b7-9f84-a75e2634b009 |
| c8bed010-e42e-4f98-9651-6aa7562aff85 | ext-net-154 | 87d41c69-9eb5-4ce6-af29-7791eeda550c |
+--------------------------------------+-------------+--------------------------------------+
student@maas:~$ openstack subnet list
+--------------------------------------+------+--------------------------------------+------------------+
| ID                                   | Name | Network                              | Subnet           |
+--------------------------------------+------+--------------------------------------+------------------+
| 86e73eb3-2743-48b7-9f84-a75e2634b009 | EXT1 | 3e7591c8-c85f-4447-a7ba-0deb2cbe8860 | 158.193.153.0/24 |
| 87d41c69-9eb5-4ce6-af29-7791eeda550c | EXT2 | c8bed010-e42e-4f98-9651-6aa7562aff85 | 158.193.154.0/24 |
+--------------------------------------+------+--------------------------------------+------------------+
student@maas:~$
```

Obrázok 21 – Výpis sietí a podsietí v OpenStacku na serveri MAAS

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

1.2.18 Vymazanie IP adries komponentov v MAAS

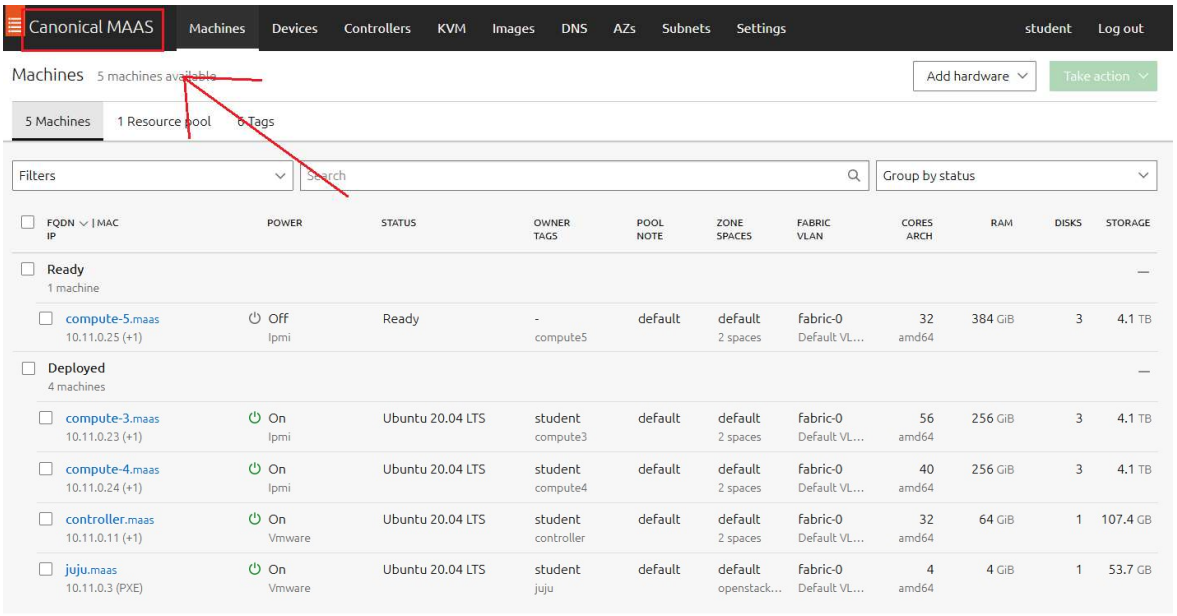
Systém MAAS disponuje aj funkcionalitou objavovania siete, teda v určitých intervaloch vie zmapovať podsiete, do ktorých je pripojený. Táto funkcionalita sa dá vypnúť všeobecne alebo konkrétne na jednotlivé podsiete.



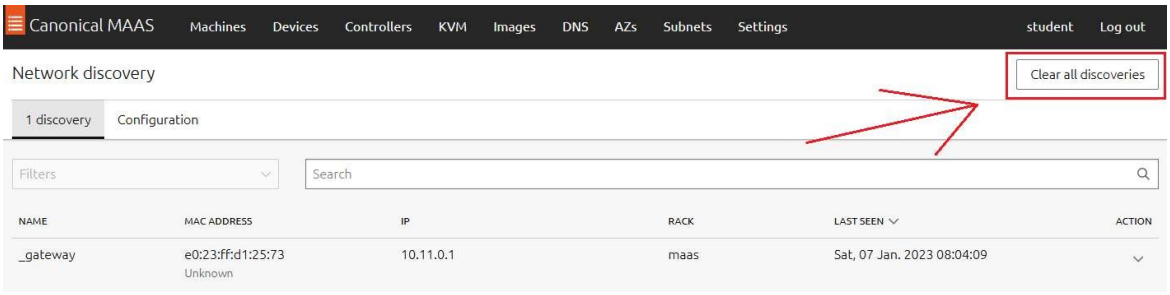
Obrázok 22 – Ukážka nastavení mapovania siete v MAAS webovom rozhraní

V prípade, že potrebujeme zmazať model a použiť rovnaký rozsah IP adries, ktoré sme vyčlenili pre komponenty OpenStack-u, tak je nutné vymazať objavené IP adresy v tomto zozname. Túto akciu možno vykonať ako v GUI, tak aj pomocou CLI. Vo webovom rozhraní ako prvé klikneme na názov „Canonical MAAS“ v ľavom hornom rohu a následne sa nám zobrazí menu „Network discovery“, kde v pravej hornej časti klikneme na „Clear all discoveries“ a teda vyčistenie všetkých objavených zariadení.

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 23 – Navigácie v MAAS webovom rozhraní pre Network discovery menu



Obrázok 24 – Vyčistenie zoznamu objavených zariadení v Network discovery

Pre CLI opäť platí, že ak nie sme prihlásený do MAAS, tak ako prvé sa prihlásime do MAAS pod používateľským kontom student.

```
maas login student http://10.11.0.2:5240/MAAS - <  maas-api-key
```

A následne pomocou jedného príkazu taktiež vymažeme celý zoznam objavených zariadení. Možnosť „all“ je možné ešte nahradiť za „mdns“, ktoré vymaže všetky mDNS objavy alebo „neighbours“, ktoré vymaže všetky záznamy od susedov.

```
maas student discoveries clear all=True
```

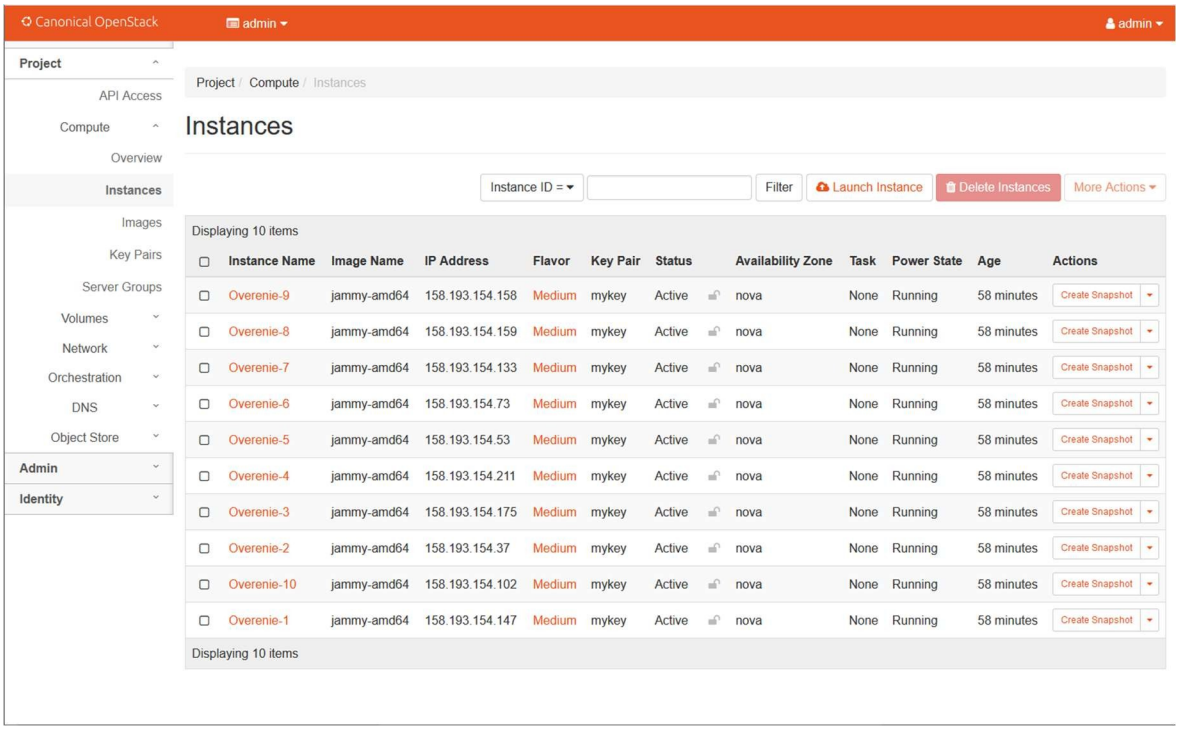

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

2 Overenie

Overenie prebiehalo vytváraním prvkov a tým aj overená ich funkčnosť:

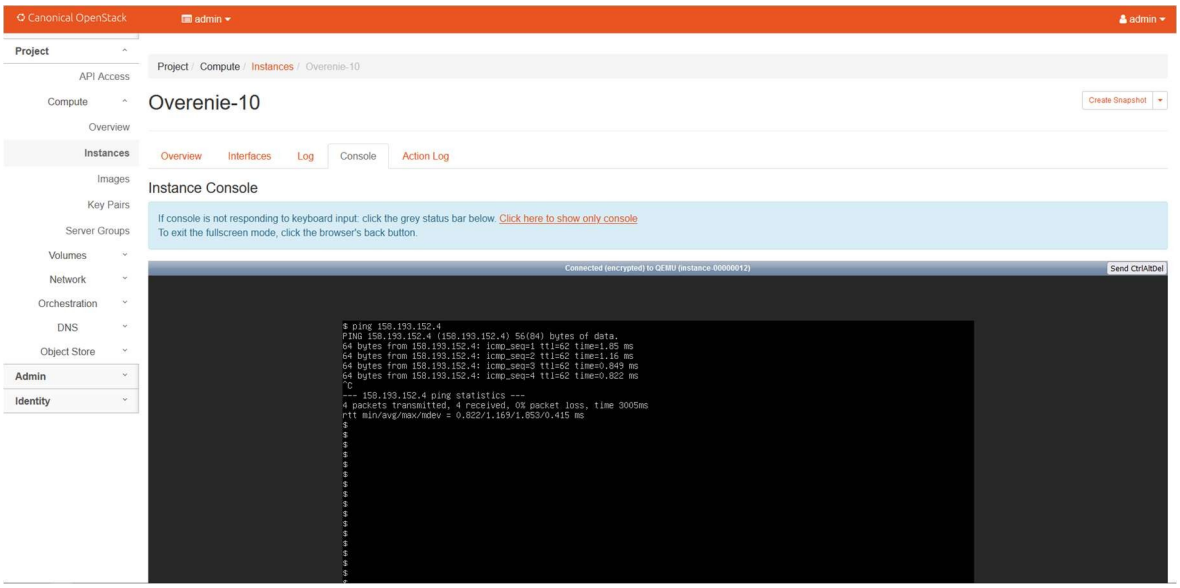
- vytvorenie inštancií
- konzola vo webovom rozhraní
- pripojenie na konzolu pomocou terminálu
- nahranie obrazu na bootovanie
- vytváranie flavor-ov (zdroje pre inštancie)
- vytvorenie sietí
- vytvorenie a nahranie SSH kľúčov

Taktiež všetky komponenty po nainštalovaní pomocou výpisu „juju status“ boli bez chybový hlášok v aktívnom stave.

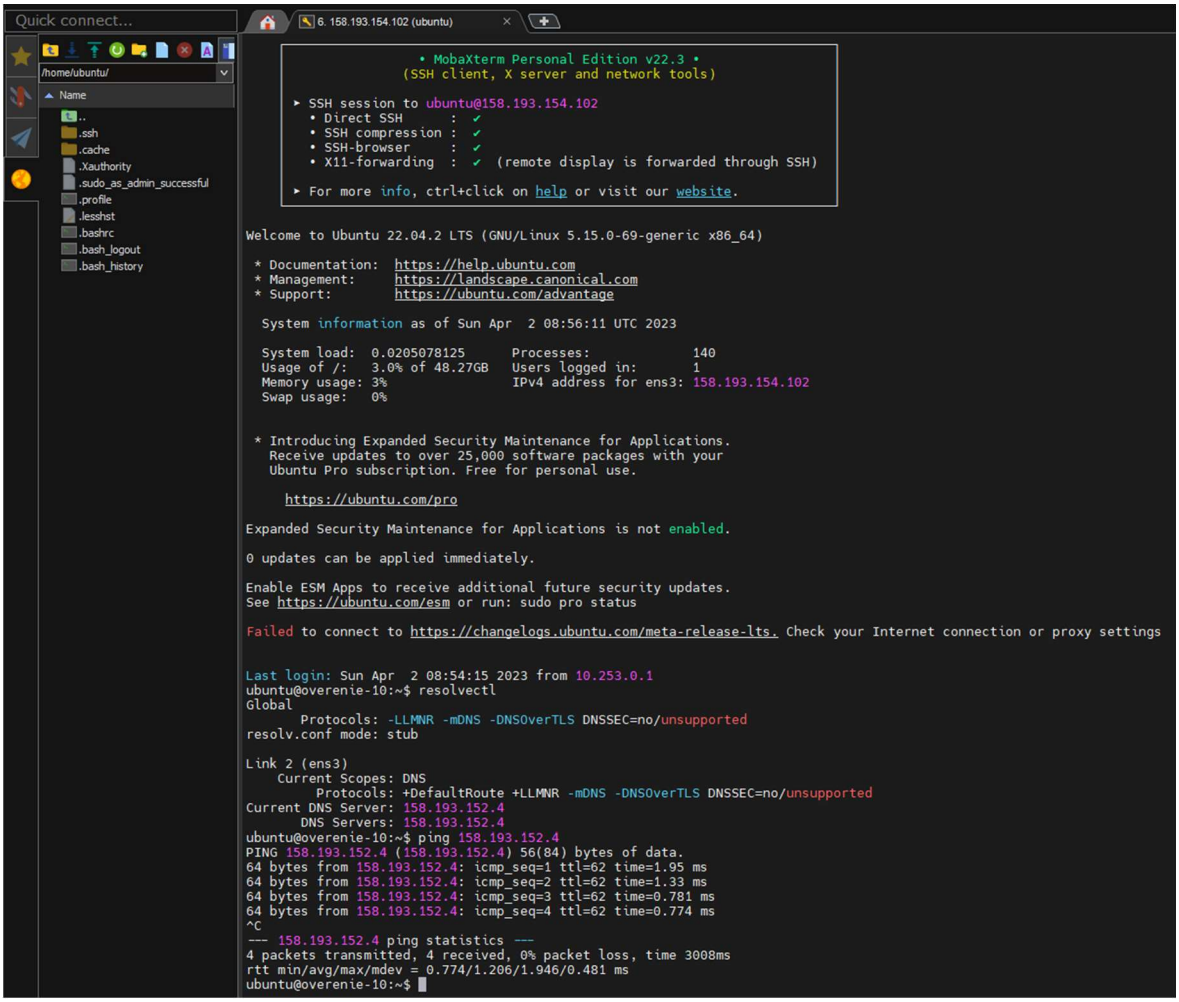


Obrázok 29 - Virtuálne inštancie pre overenie funkčnosti

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

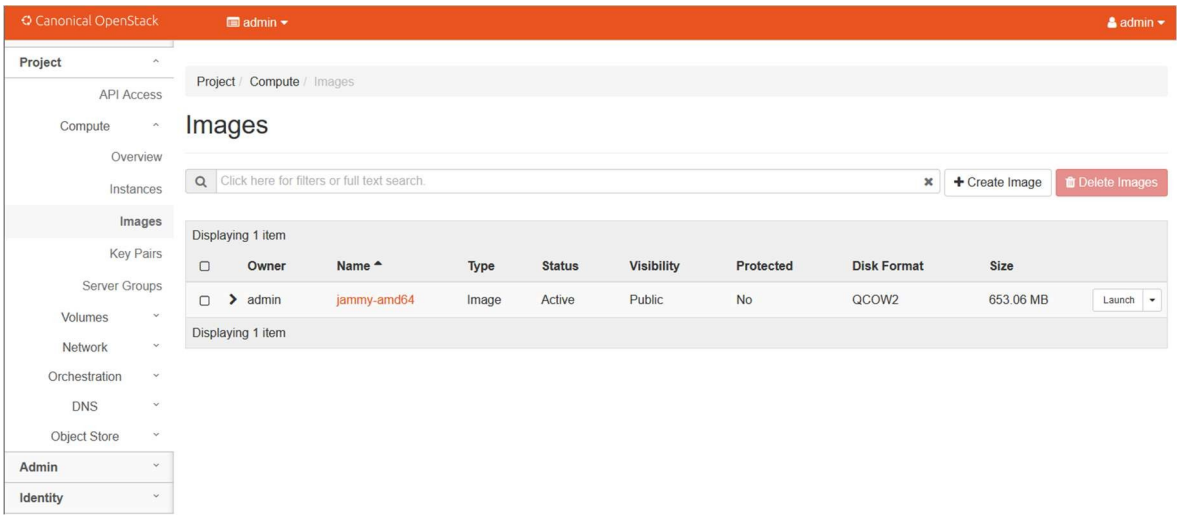


Obrázok 30 - Konzola vo webovom rozhraní

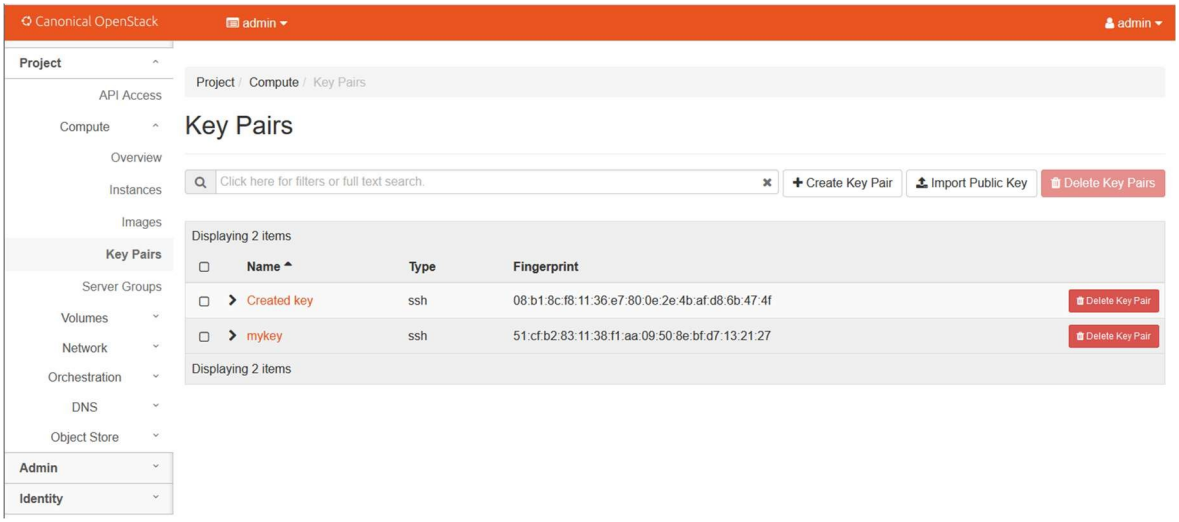


Obrázok 31 - Pripojenie na konzolu cez terminál

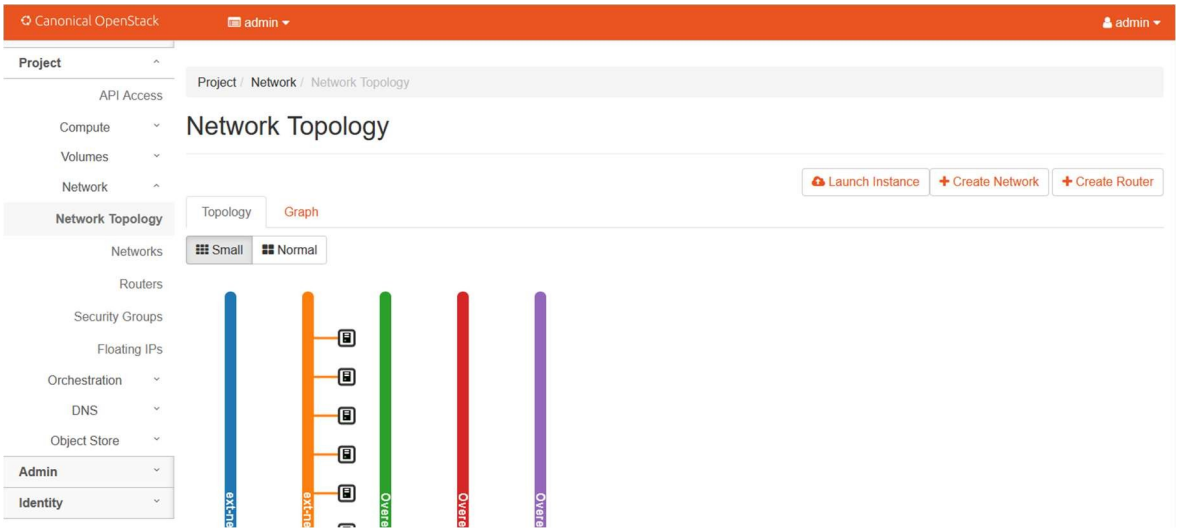
Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 32 - Zoznam nahraných obrazov na bootovanie

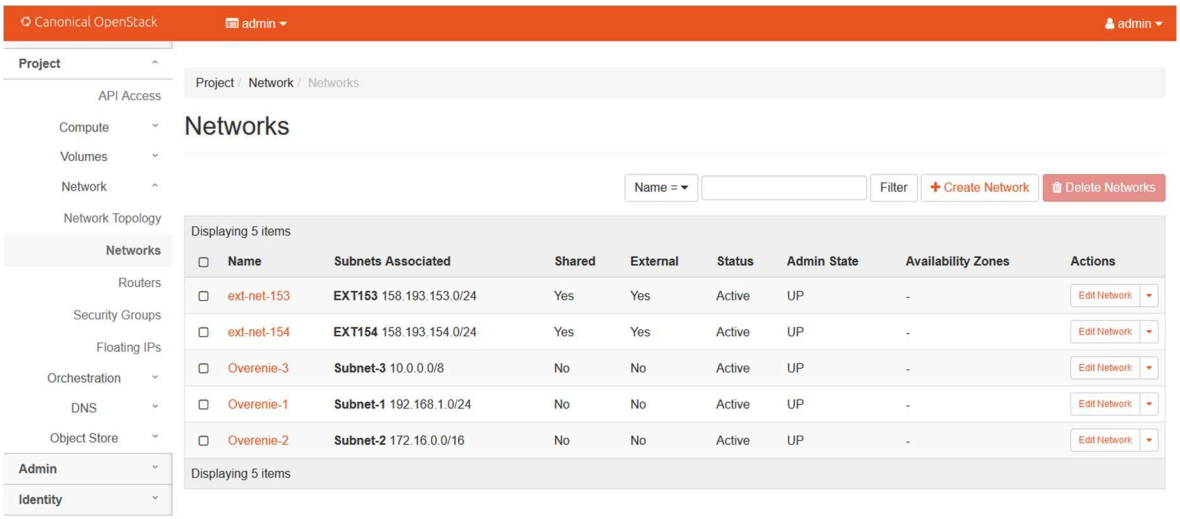


Obrázok 33 - SSH kľúče vytvorený/nahraný



Obrázok 34 - Sieťová topológia

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY



Obrázok 35 - Zoznam vytvorených sietí na overenie

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Záver

Hlavným cieľom implementácie bolo nasadenie cloudovej platformy OpenStack s využitím nástrojov Charms na fyzickej a virtuálnej infraštruktúre. Okrem nasadenia OpenStack-u na fyzické servery bola zrealizovaná aj príprava a inštalácia virtuálnych serverov určených pre prevádzku systémov MAAS a Juju, pričom zostávajúca výpočtová kapacita bola využitá na nasadenie kontroléra cloudovej platformy.

Po zadefinovaní technických požiadaviek boli identifikované komponenty potrebné na prevádzku platformy. Následne sa pristúpilo k implementácii v preddefinovanej postupnosti – iniciálne nasadenie systému MAAS, ktorý zabezpečuje efektívne a automatizované provisionovanie ďalších serverov. V rámci MAAS bol následne inštalovaný aj server Juju, ktorý predstavuje framework pre nasadzovanie aplikačných služieb prostredníctvom Charms.

Fyzické servery boli nakonfigurované v prostredí MAAS, vrátane ich sieťovej topológie a značiek, ktoré sú nevyhnutné pre správne rozloženie komponentov. Na základe zoznamu požadovaných služieb bol vytvorený inštalačný balíček (bundle), v ktorom bolo definované priradenie jednotlivých komponentov. Riadiace komponenty boli alokované na kontrolér, výpočtové komponenty na compute uzly. V priebehu konfigurácie boli postupne integrované aj ďalšie servery, pričom sa vykonali potrebné úpravy sieťovej komunikácie a testovanie dostupnosti služieb.

Pre zefektívnenie procesu boli vytvorené skripty na automatizáciu inštalácie a správy prostredia. Súčasťou technickej dokumentácie je rozsiahla administrátorská príručka obsahujúca podrobné inštrukcie k jednotlivým častiam systému, vrátane nasadenia webového rozhrania Skyline. Používateľská dokumentácia poskytuje základné návody pre interakciu s prostredím OpenStack, vrátane postupov na vytvorenie a konfiguráciu:

- virtuálnej inštancie,
- bootovacieho obrazu,
- SSH kľúča,
- siete,
- smerovača.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
ÚRAD VLÁDY SLOVENSKEJ REPUBLIKY

Zoznam použitej literatúry

[1] **vexxhost.com**. 2023. Cloud Orchestration with OpenStack Heat - An Introduction. 2023. Dostupné na internete: https://vexxhost.com/blog/cloud-orchestration-with-openstack-heat/

[2] **openstack.org**. 2022. What is OpenStack?. [online]. 2022. Dostupné na internete: https://www.openstack.org/software/

[3] **openstack.org**. 2023. OpenStack Deployment Tools. [online]. 2023. Dostupné na internete: https://www.openstack.org/software/project-navigator/deployment-tools

[4] **openstack.org**. 2022. OpenStack Components. [online]. 2022. Dostupné na internete: https://www.openstack.org/software/project-navigator/openstack-components

[5] **Juju Charm – RabbitMQ**. 2022. charm-rabbitmq-server. [online]. 2022. Dostupné na internete: https://github.com/openstack/charm-rabbitmq-server

[6] **OpenStack Charmers.** 2022. Vault. [online]. 2022. Dostupné na internete: https://charmhub.io/vault

[7] **openstack.org**. 2022. OpenStack Charms Deployment Guide. [online]. 2022. Dostupné na internete: https://docs.openstack.org/project-deploy-guide/charm-deployment- guide/yoga/index.html

[8] **maas.io**. 2022. Canonical MAAS. [online]. 2022. Dostupné na internete: https://maas.io/

[9] **juju.is**. 2022. Take control of..... [online]. 2022. Dostupné na internete: https://juju.is/

[10] **github.com**. 2022. openstack-charmers / openstack-bundles. [online]. 2022. Dostupné na internete: https://github.com/openstack-charmers/openstack- bundles/tree/master/stable/shared

[11] **Zaira Hira**. 2023. Shell Scripting for Beginners – How to Write Bash Scripts in Linux. [online]. 2023. Dostupné na internete: https://www.freecodecamp.org/news/shell-scripting- crash-course-how-to-write-bash-scripts-in-linux/