Review and Experiences with Several Clouds from GEANT Framework

Jiri Navratil jiri@cesnet.cz

EaPEC 2018 Conference CHISINAU, Moldova
Cloud workshop 18.10.2018

What is goal of this presentation

- To show implementation steps linked with the process working in the cloud
- Describe different levels of users and role of IT architects and administrators
- Show several basic technical details
- Help with decision which provider or cloud is best for my/yours solution (respecting company IT culture, style and tradition)

What commercial partners offer

Three groups of IaaS

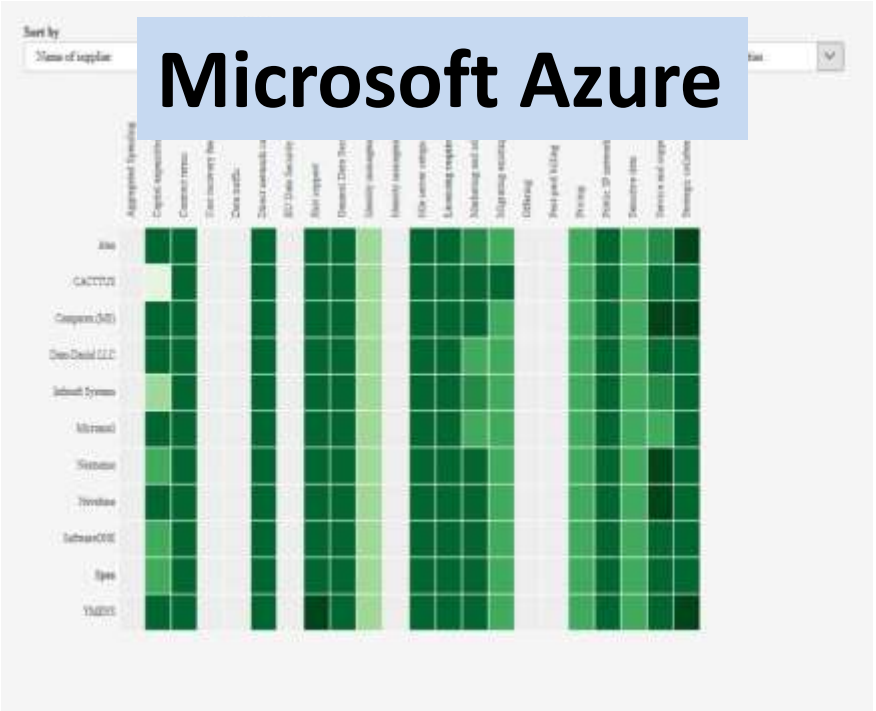
Framework Matrix in
https://catalogue.geant.org/reports/

Amazon - AWS

IaaS on own HW infrastructure

IaaS and wide spectrum of services

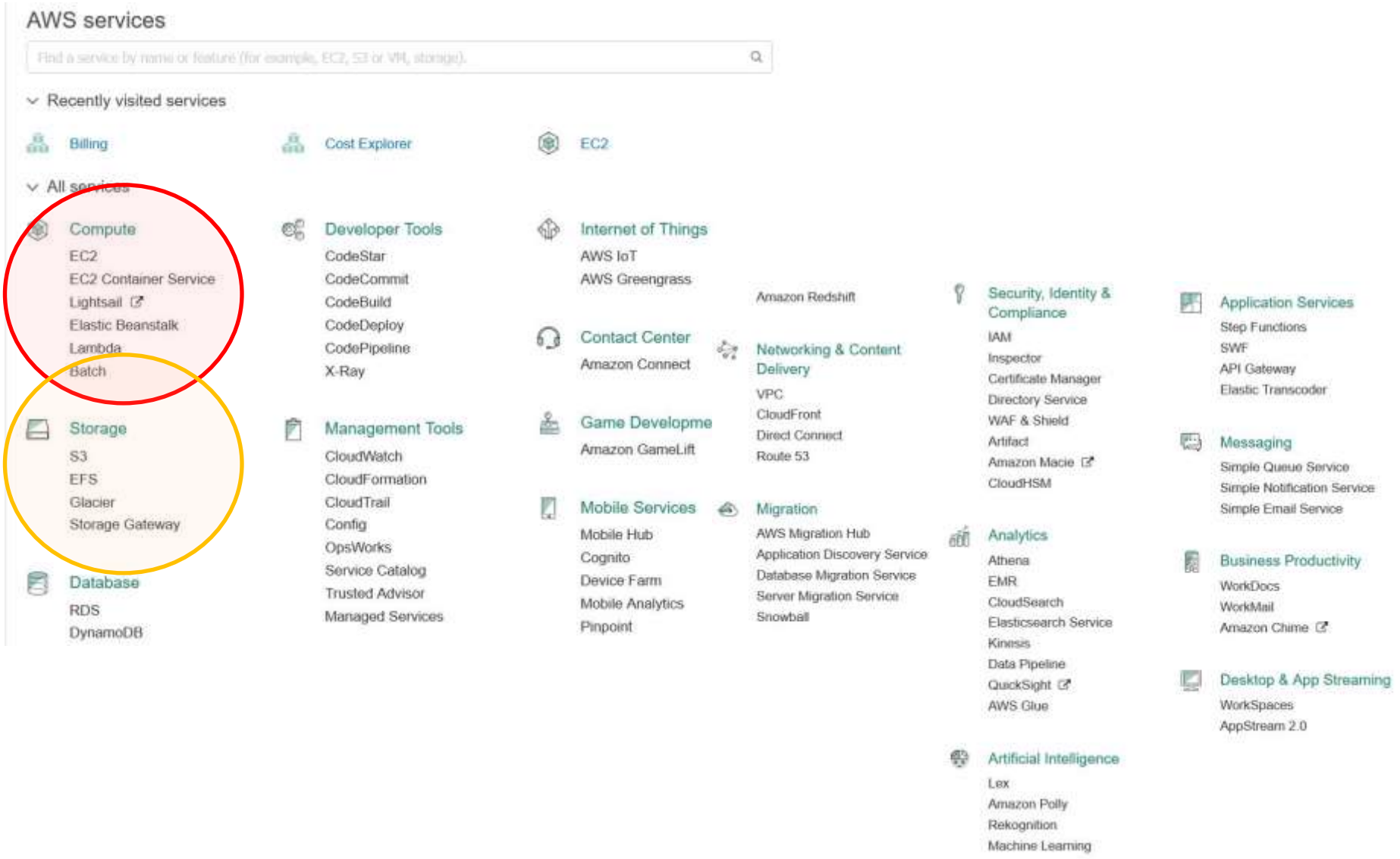
Microsoft Azure



Big Vendors offer wide spectrum of services

Big Vendors offer wide spectrum of services

Review of all AWS Services



How to become cloud user

(Individual researcher or user as a part of the team)

- Go to particular company WEB and make registration
  - Credentials Received by email
- Login to particular cloud WEB

  Microsoft https://azure.microsoft.com/en-us/

  AWS https://www.amazon.com/ap/signin?

  CloudSigma https://zrh.cloudsigma.com
- Work **in cloud DASHBOARD** (Define and control VM) as ***L1* user**

  - Define resource requests for CPU, Memory, disk, network
  - Generate or register your private SSH keys or password
  - Create VM
  - Start VM (start/stop/delete)

Users category:

L1 cloud owner /company main admin / superuser / cloud architect(not provider)

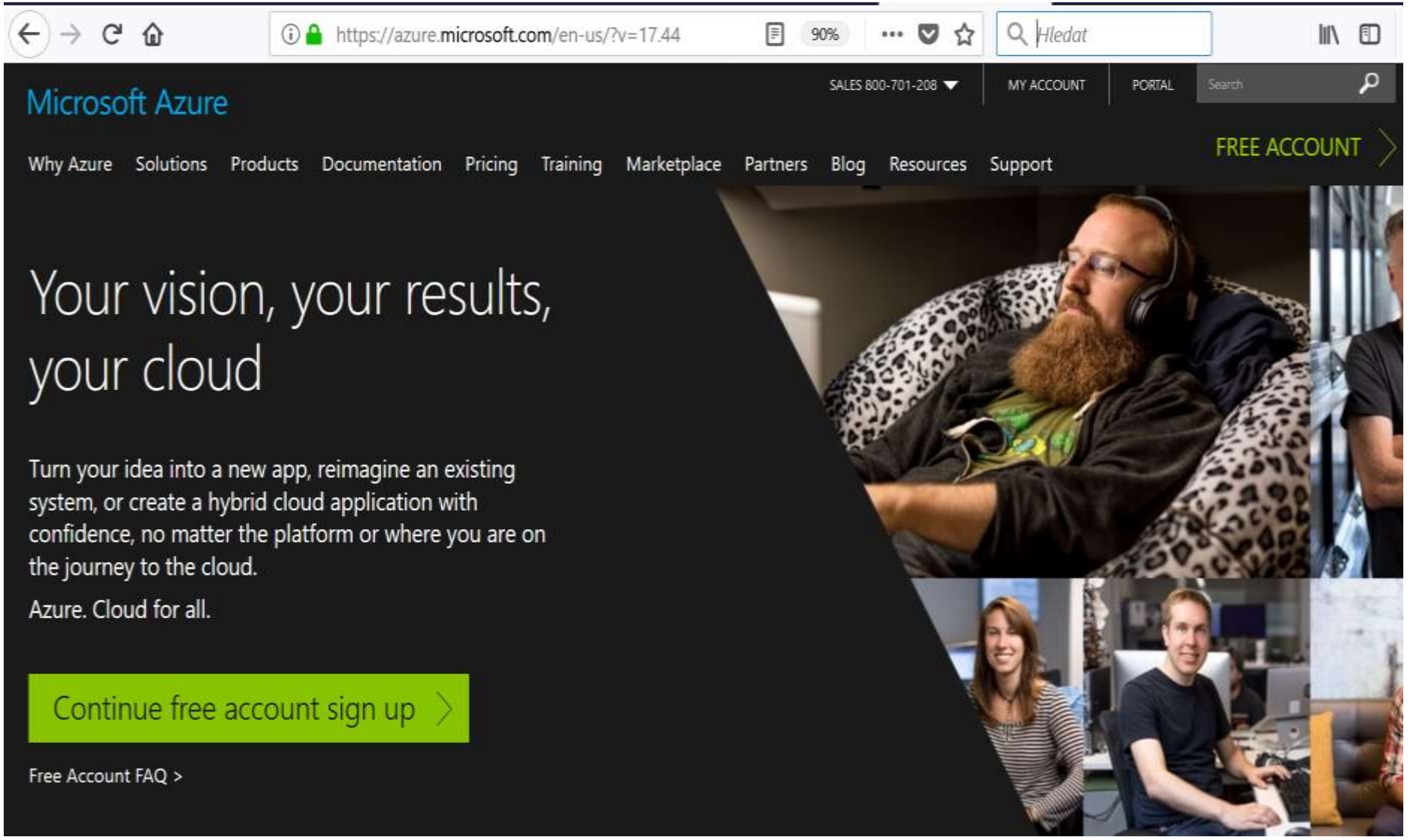
L2 user with rights to use VM as admin (with knowledge linux or MS server)

L3 application users and designers . They are using VM as at home.

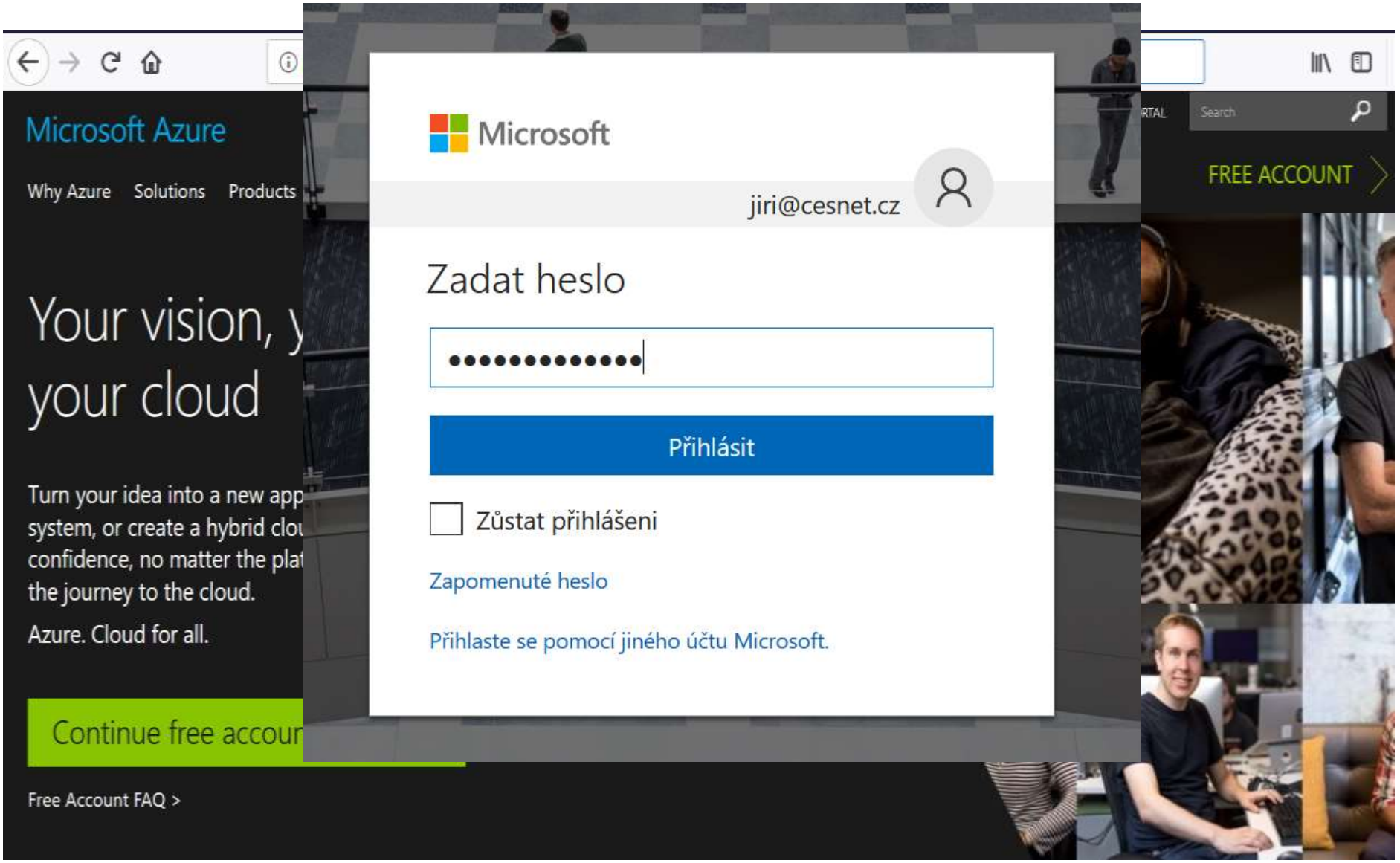
(Mathematical modelling, Wordpress, Moodle , Office365)

Many application users NO NEED to contact PROVIDERs or work with DASHBOARD

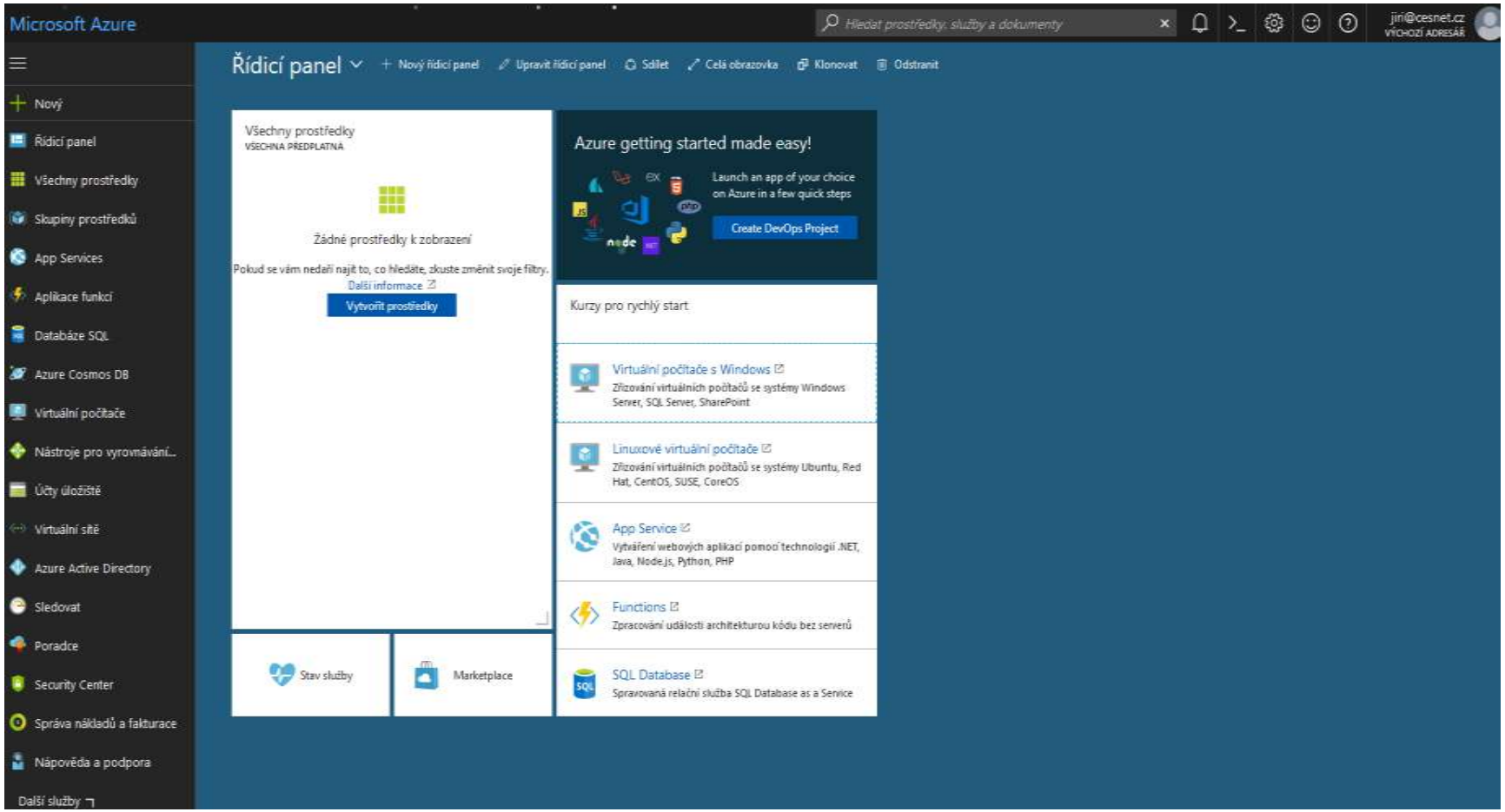
Microsoft Azure



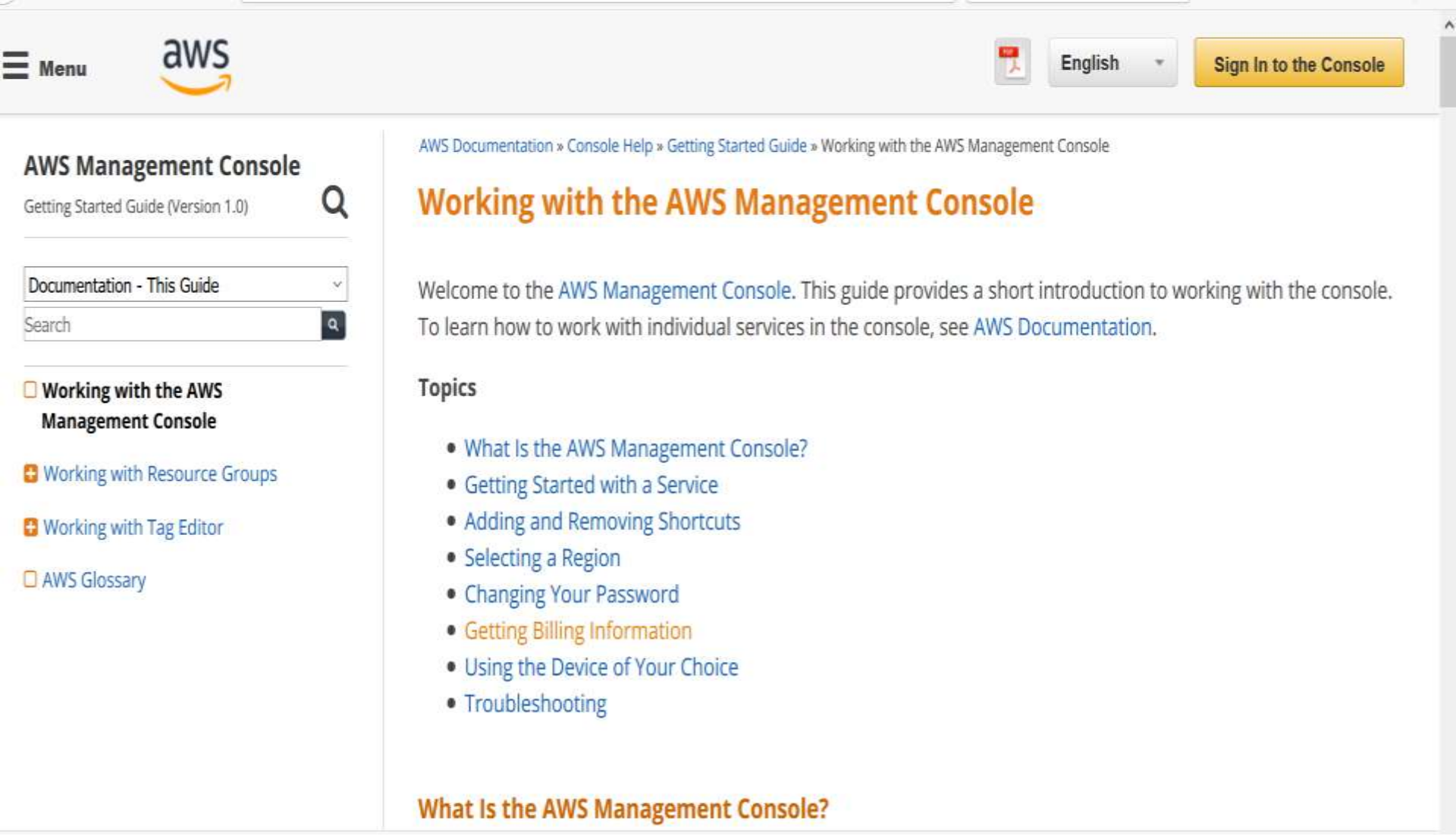
Microsoft Azure



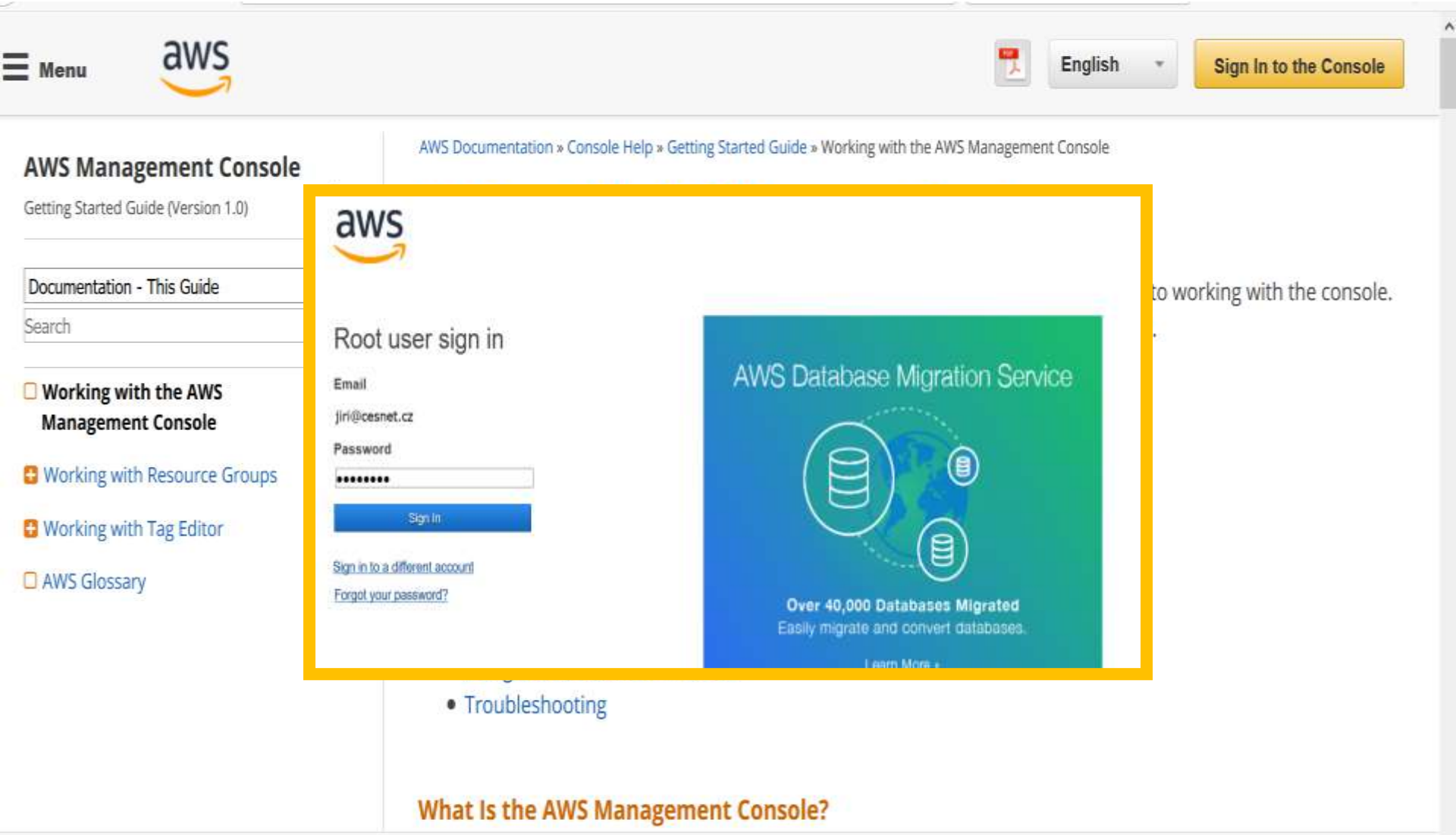
L1 cloud user - Azure Management - Dashboard



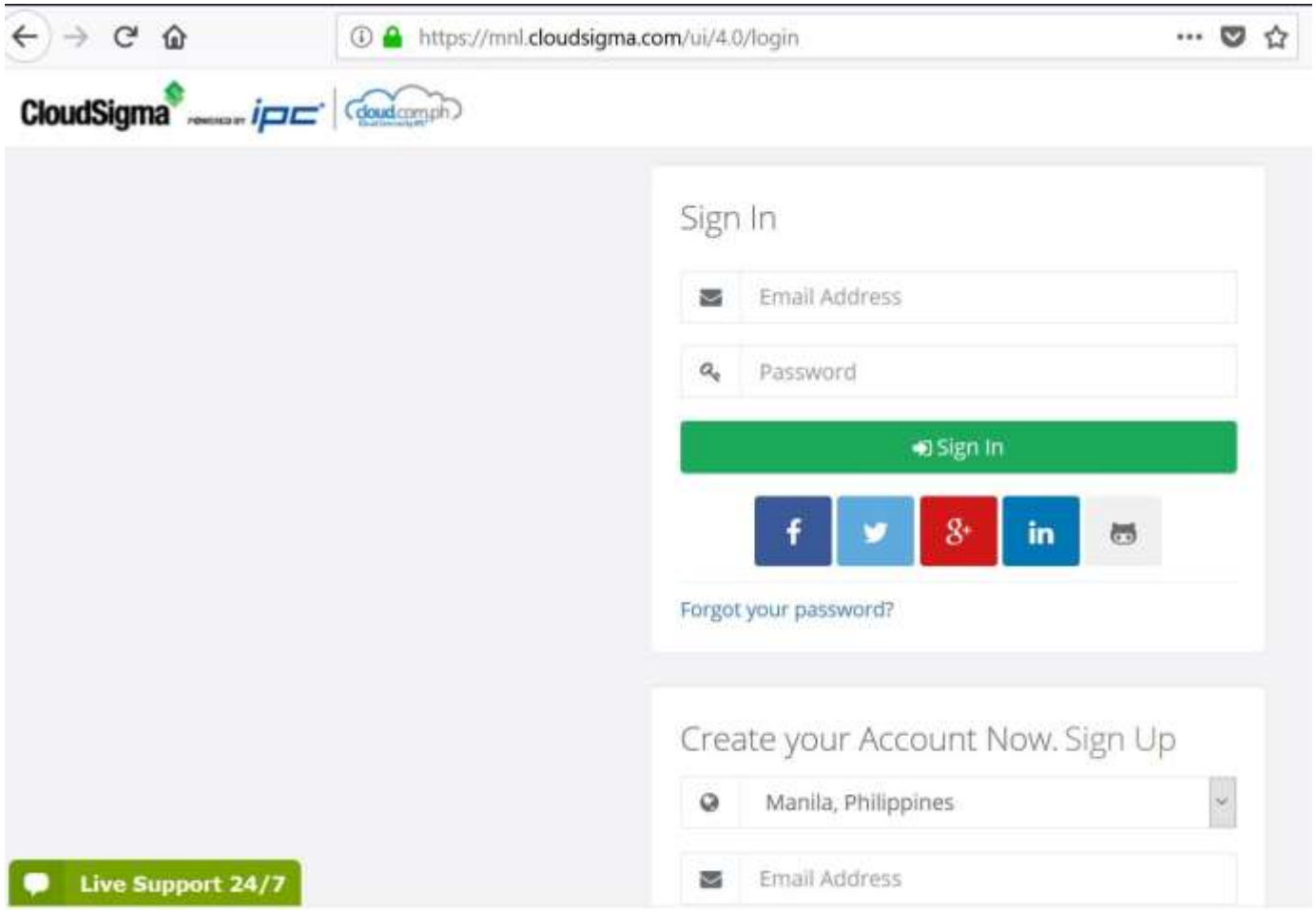
Amazon Web Services



Amazon Web Services



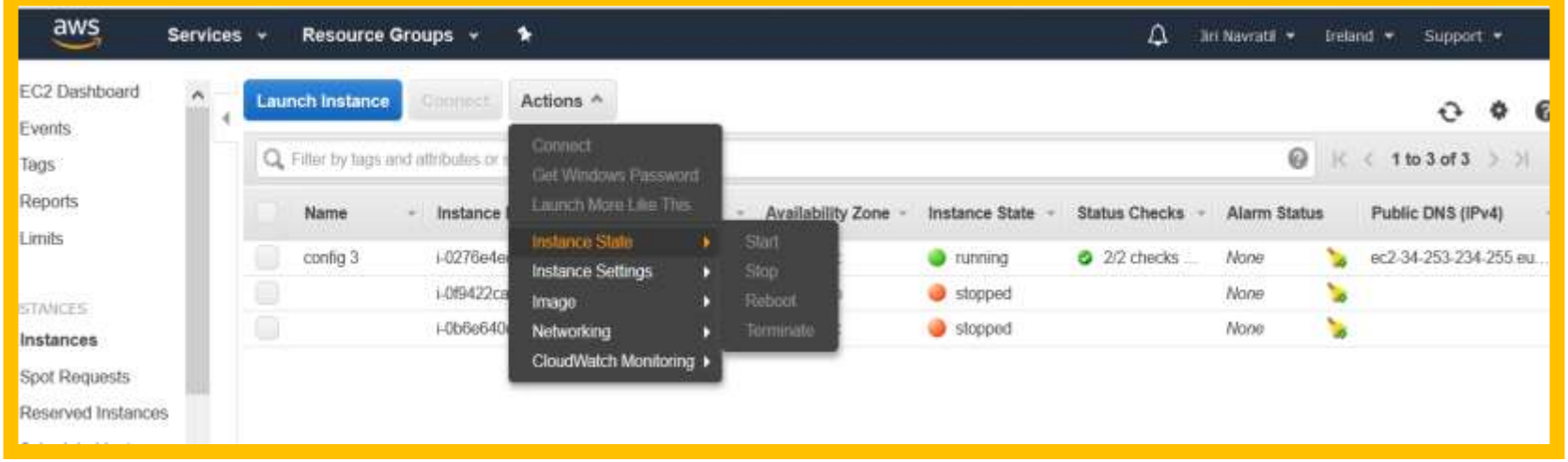
CloudSigma IaaS



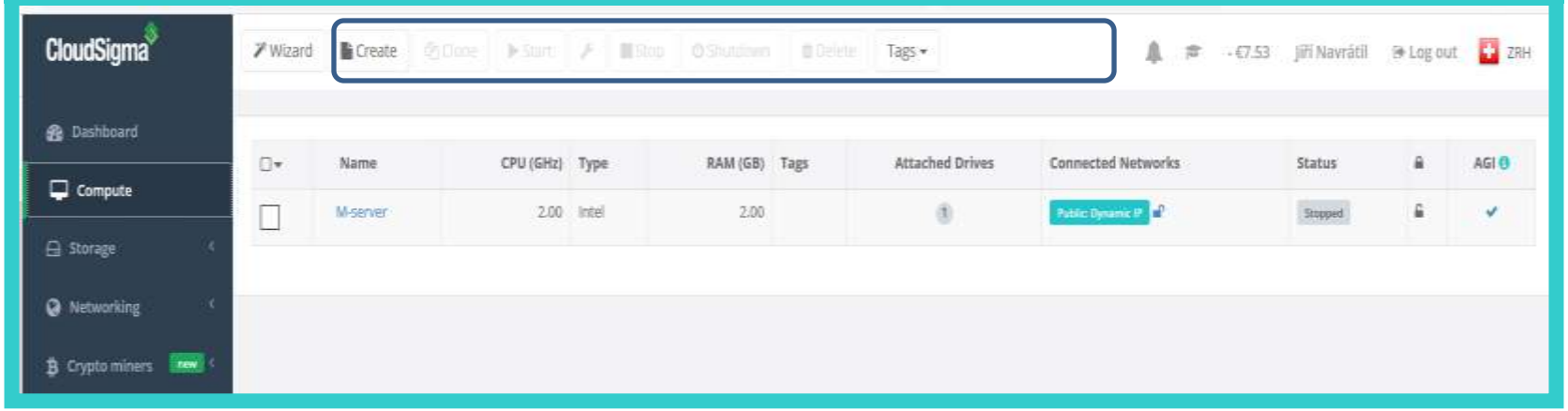
Dashboards = control panels

Different form, terminology, different icons, etc.

AWS

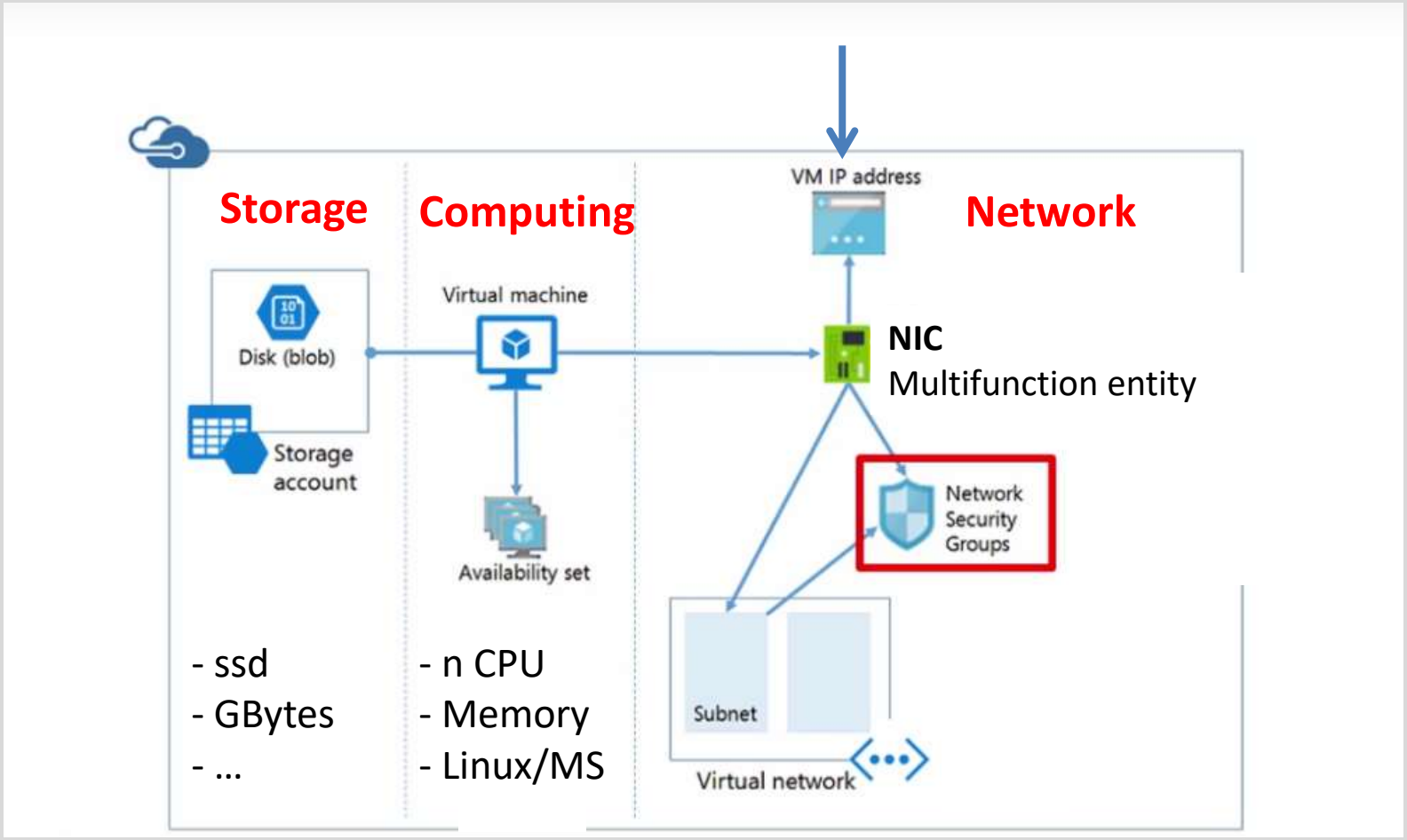


CloudSigma



Resource allocation

(Storage, Computing power, Networking)



Networking is important part of the cloud infrastructure

IP addressing:

Private IP	IP access to VM from private network
Public IP Dynamic (DHCP)	direct access from anywhere, after each **Stop/ Restart** different IP
Public IP Static	**for extra $**

(example: CloudSigma - 2 CHF per Public Static IP)

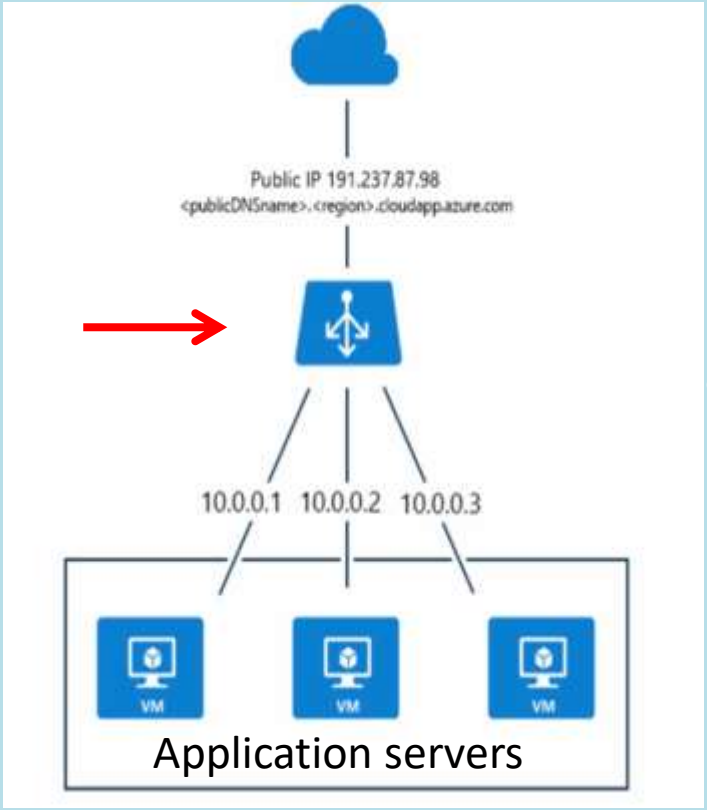
Definition of policies (Firewalls)

to Enable or to Block access from or to VM
In CloudSigma policy, in Amazon AWS, Microsoft Security groups

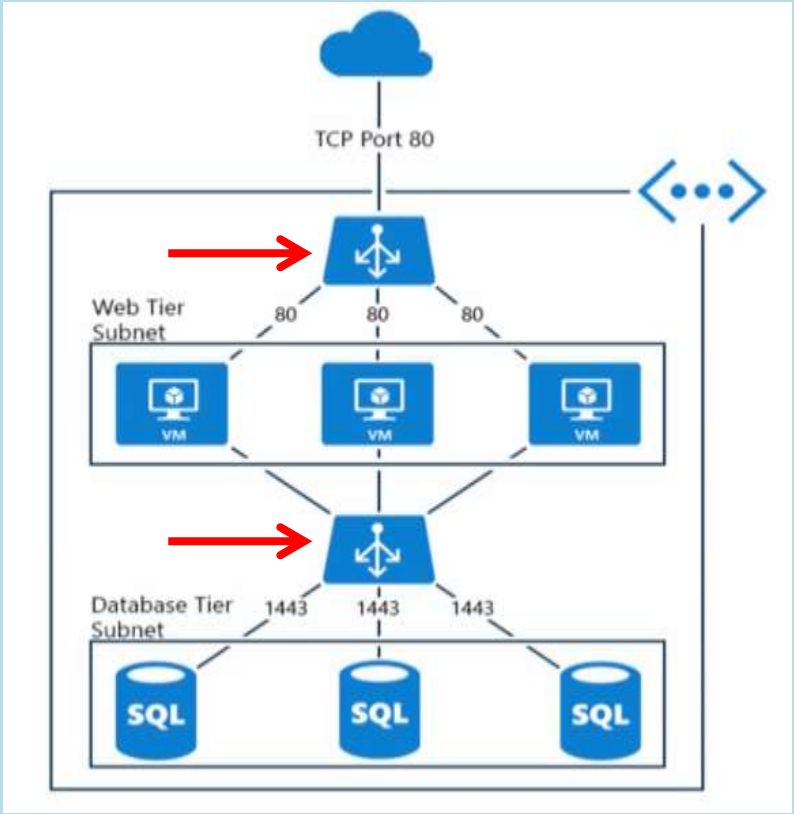
What is main difference compare to non cloud solution:
Strong rules for access as default. Only SSH no other traffic

More complex infrastructures

knowlege of existing utilization



a load



External Load balancer

Internal Load balancer

What power I will need

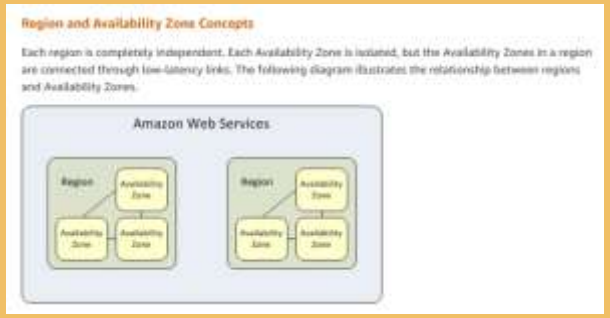
Instance Family	Some Use Cases
General purpose (T2, M5, M4)	• Low-traffic websites and web applications • Small databases and mid-size databases
Compute-optimized (C5, C4)	• High performance web servers • Video-encoding
Memory-optimized (X1e, X1, R4)	• High performance databases • Distributed memory caches
Storage-optimized (H1, I3, D2)	• Data warehousing • Log or data-processing applications
Accelerated Computing (P3, P2, G3, F1)	• 3D visualizations • Machine learning

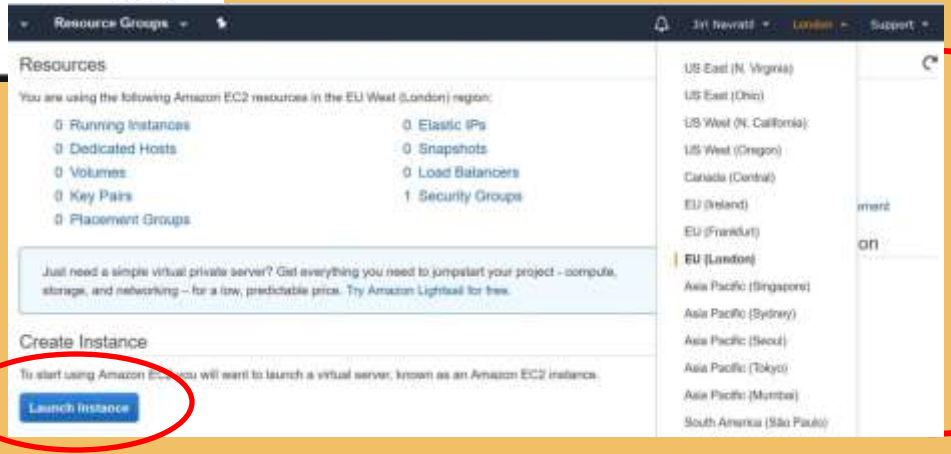
EC2 Purchasing Options

L1 Cloud user - Dashboard Management

L1 user is person who is responsible for creation infrastructure Cloud Architect

Select Regions and AZ

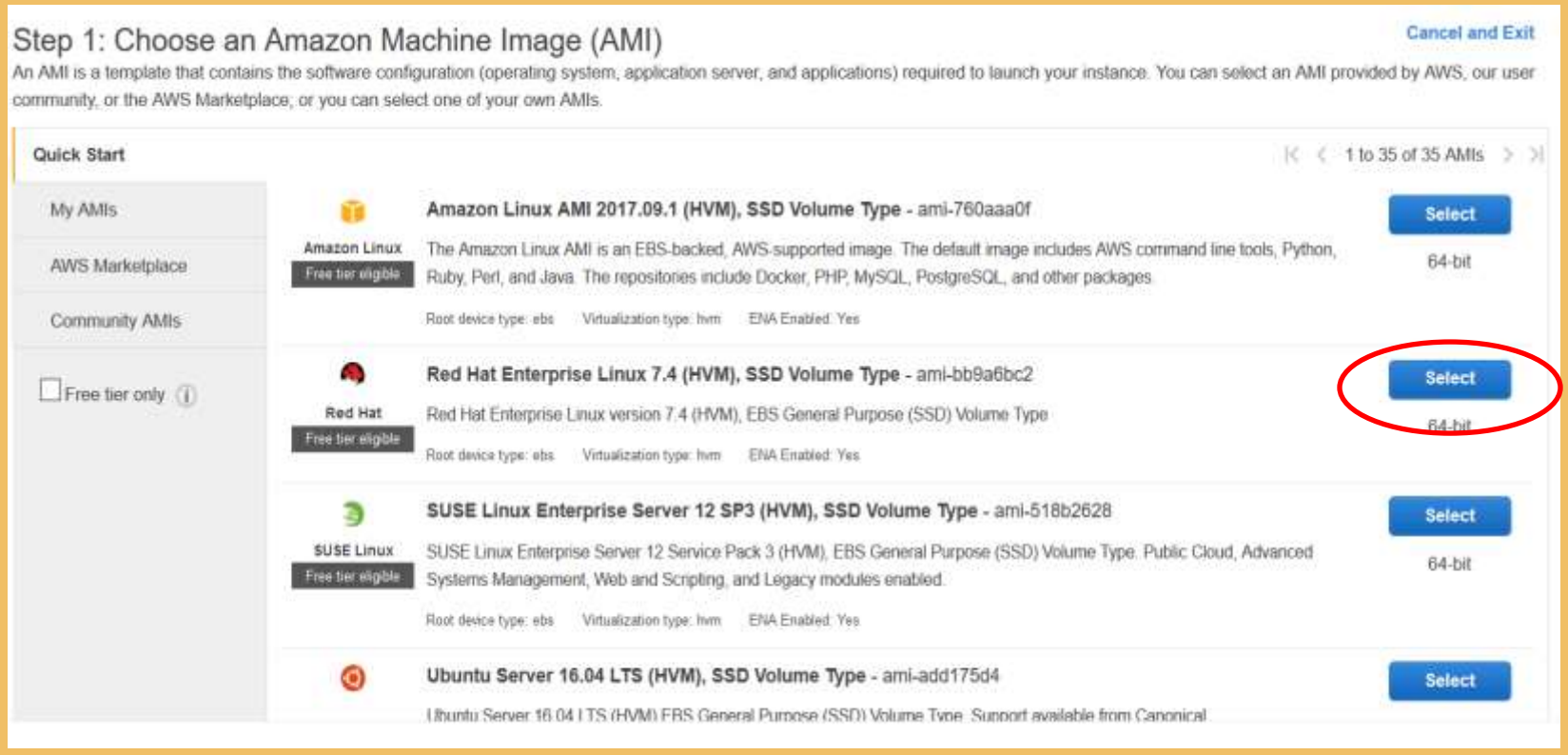




Select DC

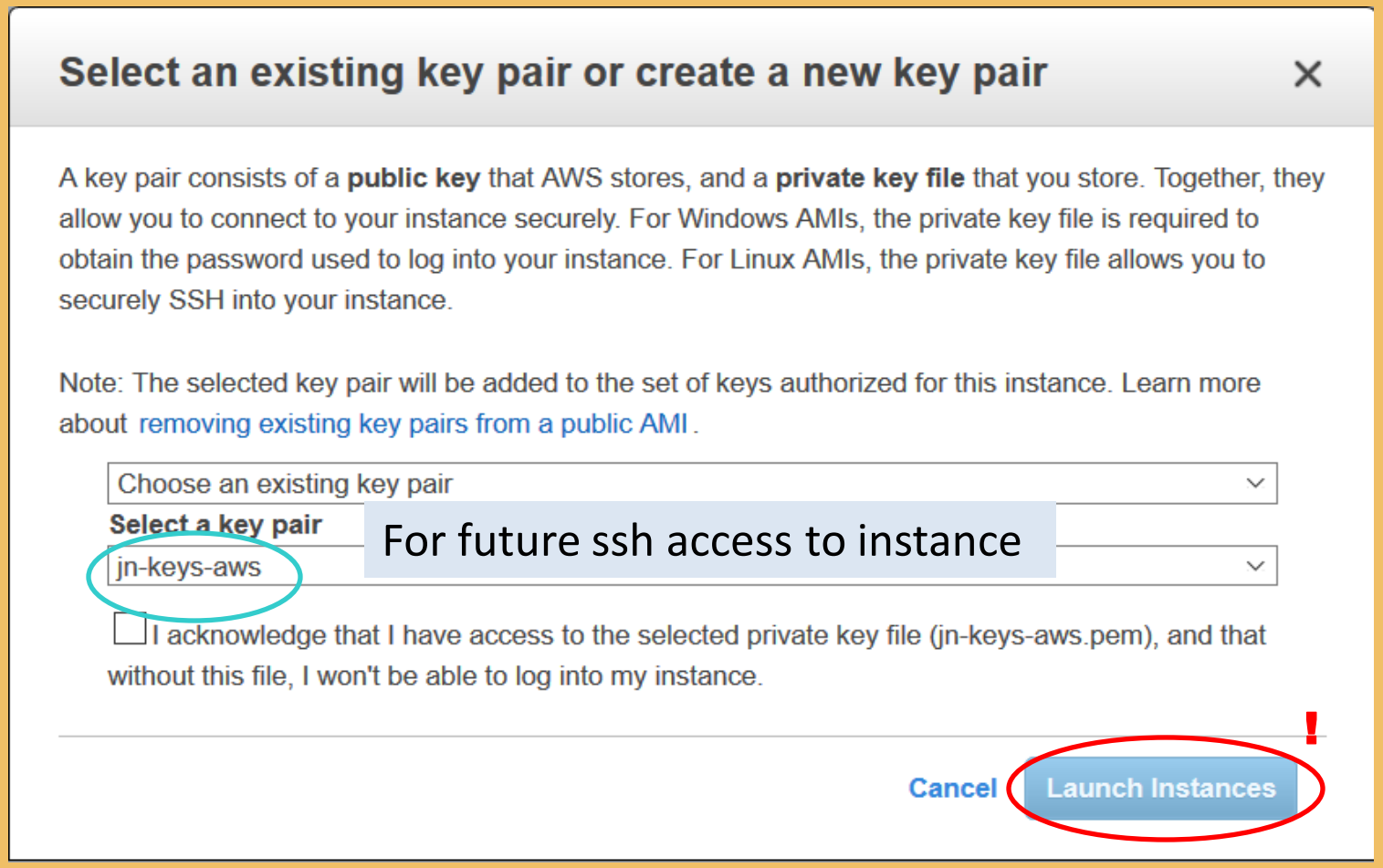
L1 Cloud user - Dashboard Management

Select Instance typa



…… etc.

L1 Cloud user - Dashboard Management

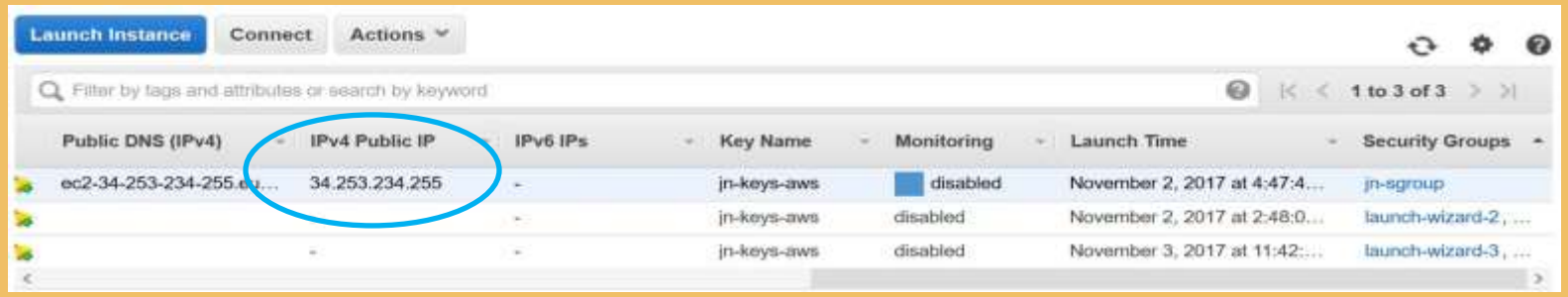


L1 Cloud user - Dashboard Management

My cloud infrastructure - Status review

Ireland

Cont.

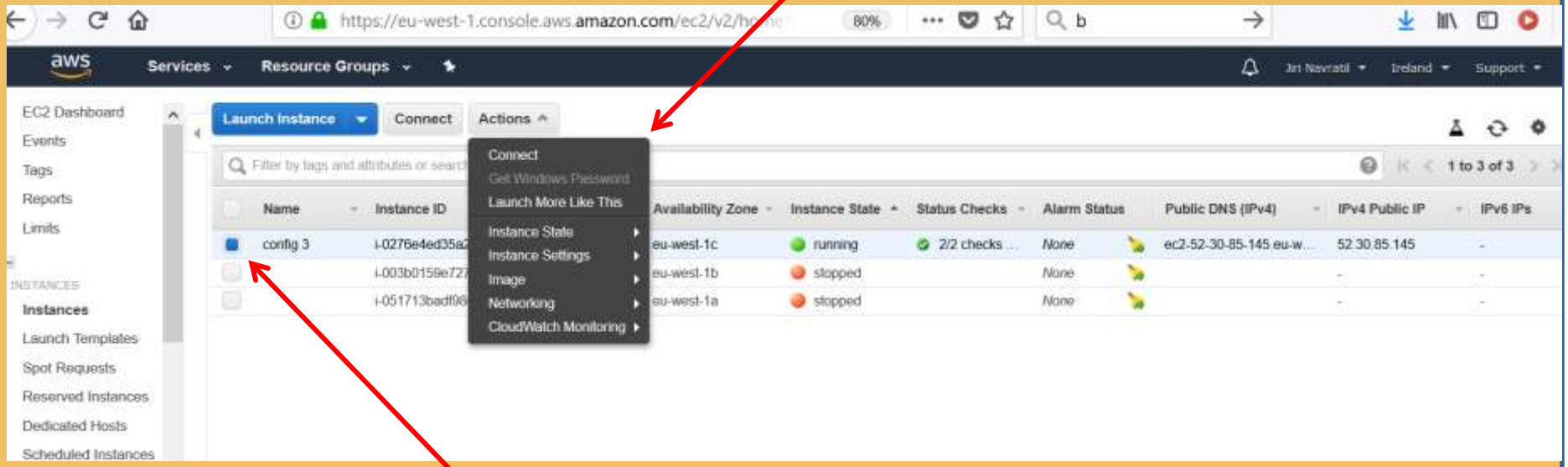


IP

keys

L1 Cloud user - Dashboard Management

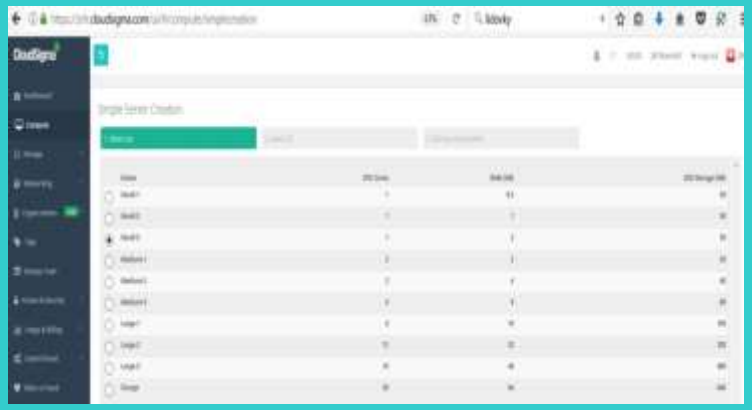
Action commands



Valid for this instance

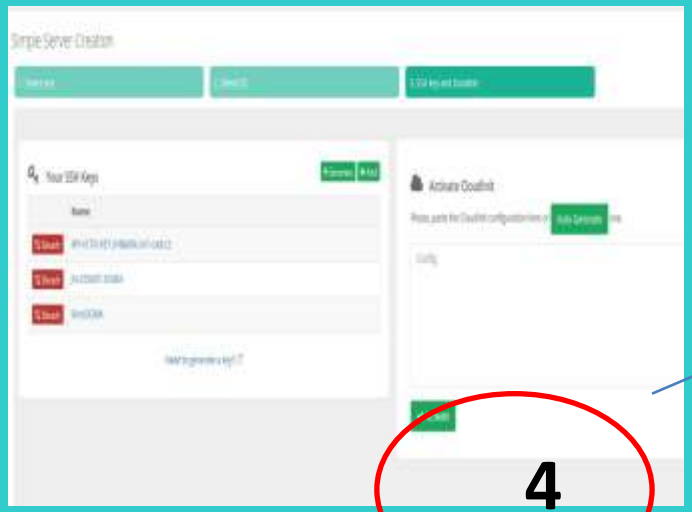
L1 Cloud user - Dashboard Management Process In CloudSIgma (step 1-5)

1



2

3

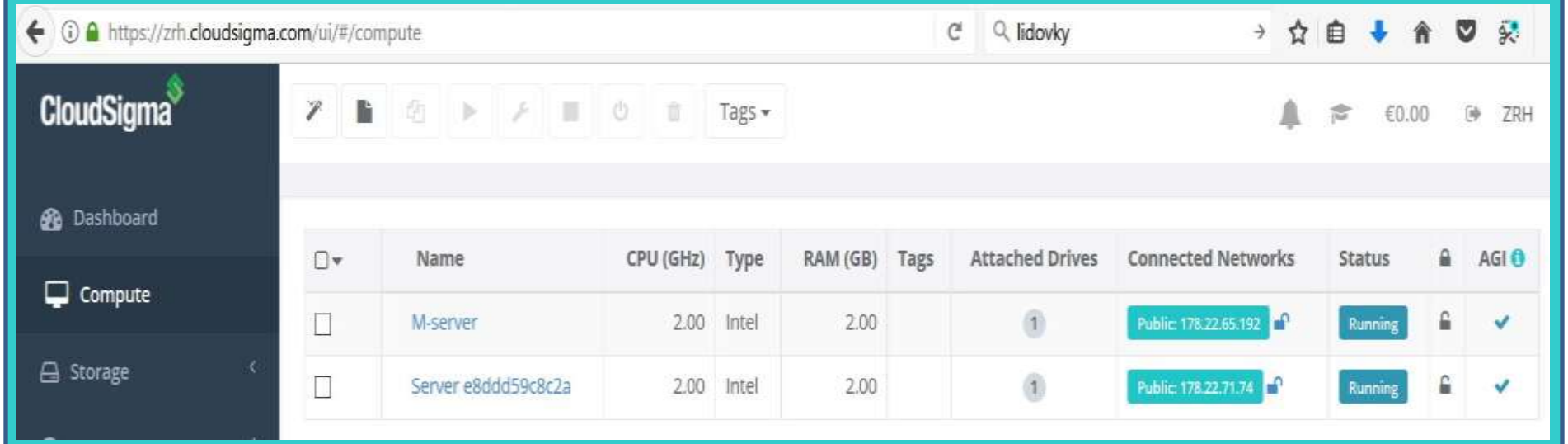


4

5

L1 Cloud user Dashboard Management

My cloud infrastructure - Status review



ssh keys

Security group

L1 user Set AWS Security groups

Security Group: sg-40d3c838

Description | **Inbound** | Outbound | Tags

Edit

Default only SSH no other traffic allowed

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

Create Security Group | Actions

search: sg-f92efa82 | Add filter

Name	Group ID	Group Name	VPC ID	Description
	sg-f92efa82	jn-sgroup	vpc-dd6928b9	ssh, web

Security Group: sg-f92efa82

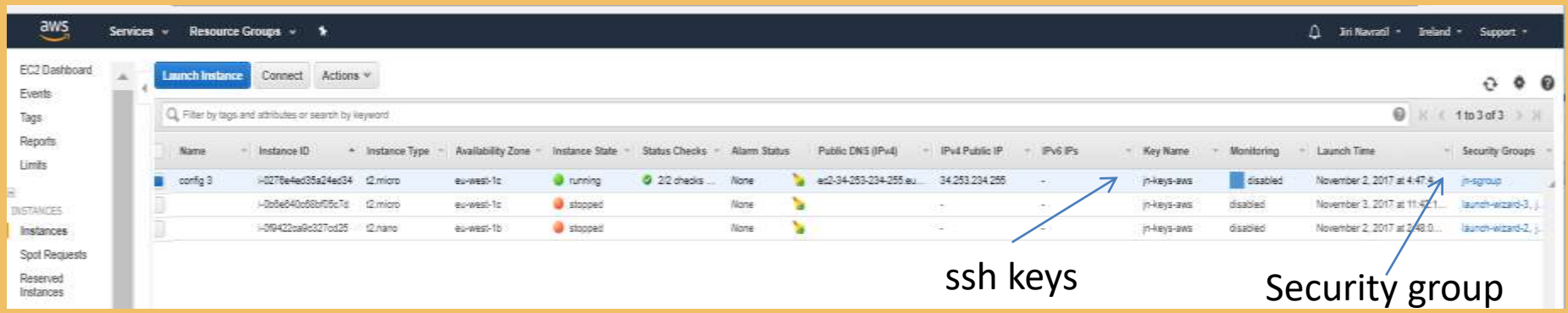
Description | **Inbound** | Outbound | Tags

Edit

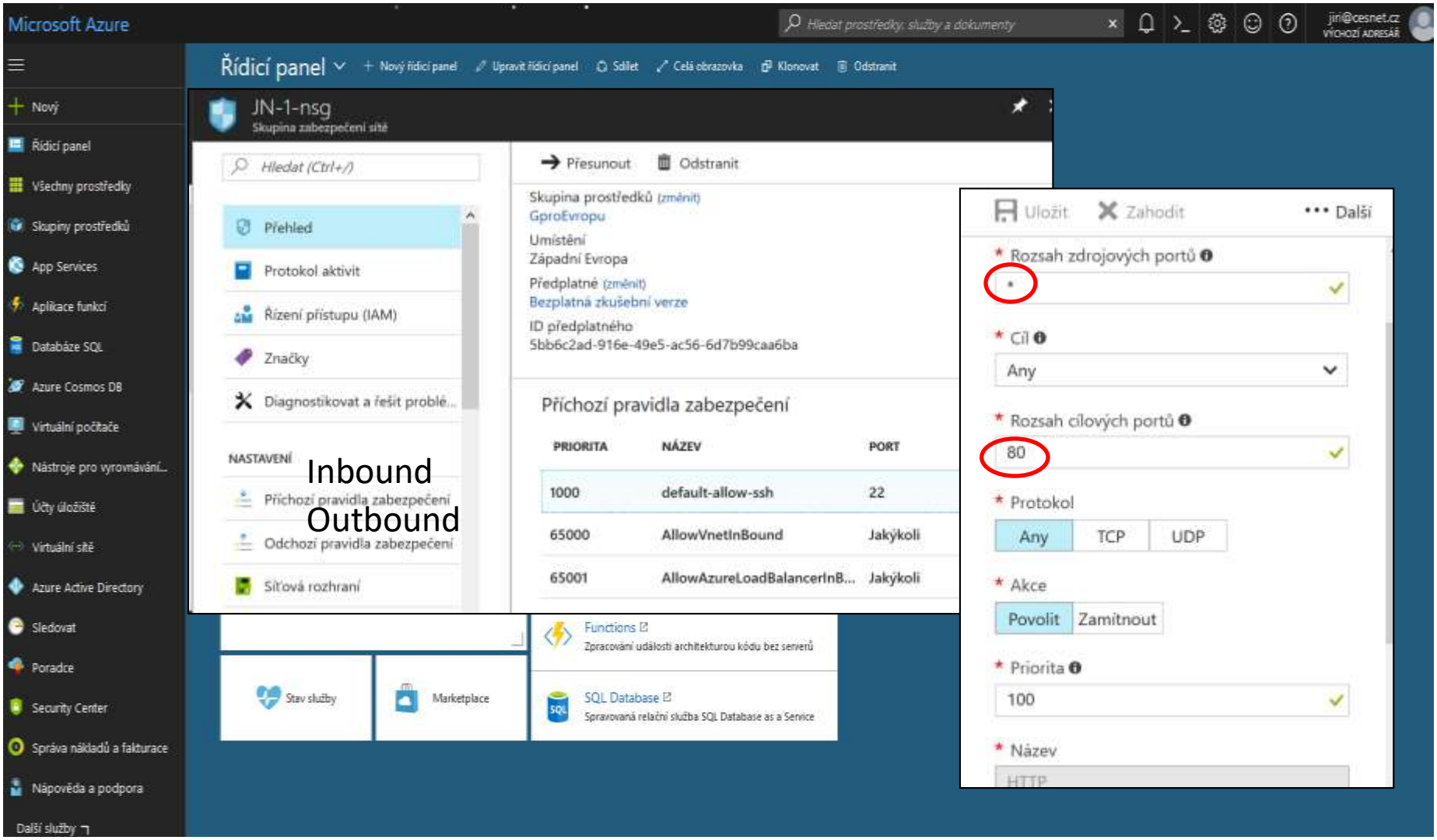
VM manager changed to open to all world for WEB

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	web http
HTTP	TCP	80	::/0	web http
Custom ICMP Rule - IPv4	Echo Reply	N/A	0.0.0.0/0	ping
Custom ICMP Rule - IPv4	Echo Reply	N/A	::/0	ping
SSH	TCP	22	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	web https
HTTPS	TCP	443	::/0	web https

L1 user - AWS Security groups

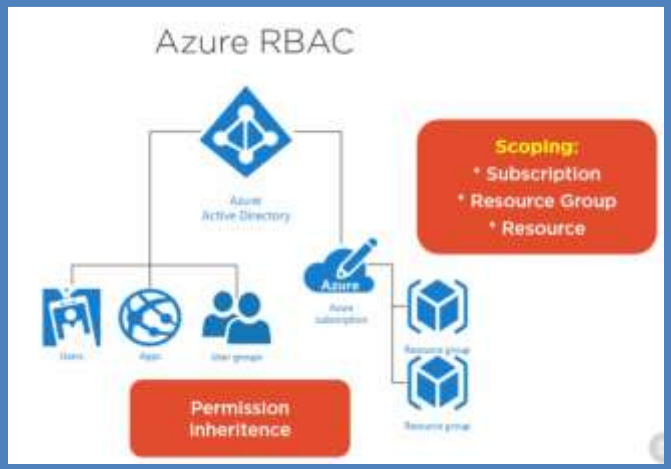


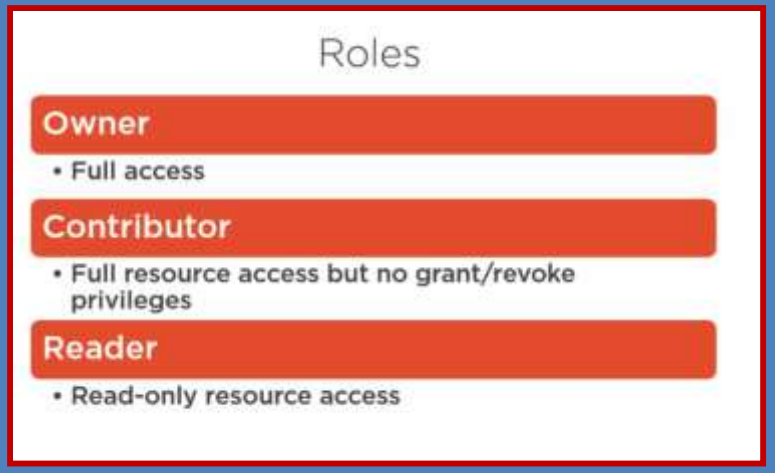
L1 user Set Azure Security groups



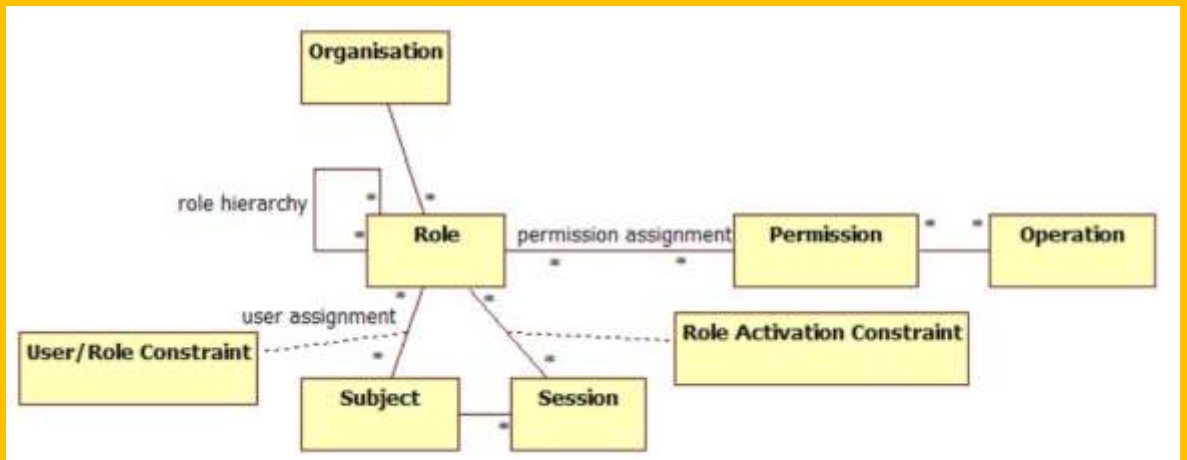
Clouds offer complex user management

Microsoft Azure example RBAC Role Based Access Control



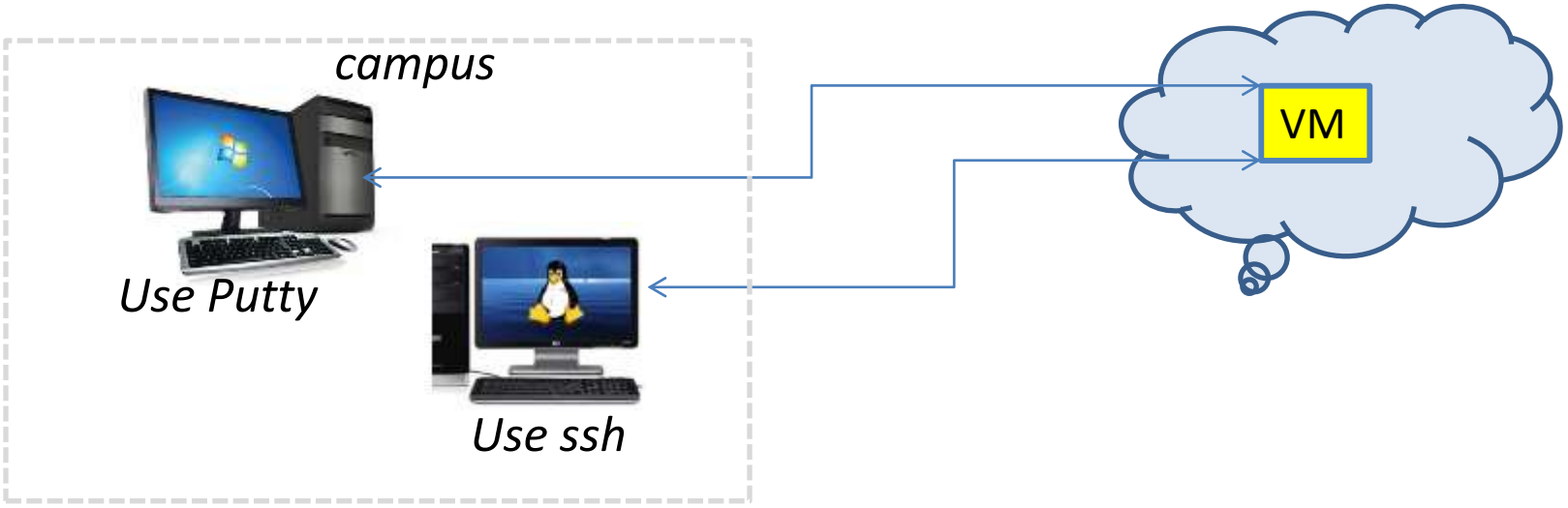


Amazon Role-Based Access Control Policy



L2 user - Login to VM from local machine

L2 user is person who will work in VM – application developer

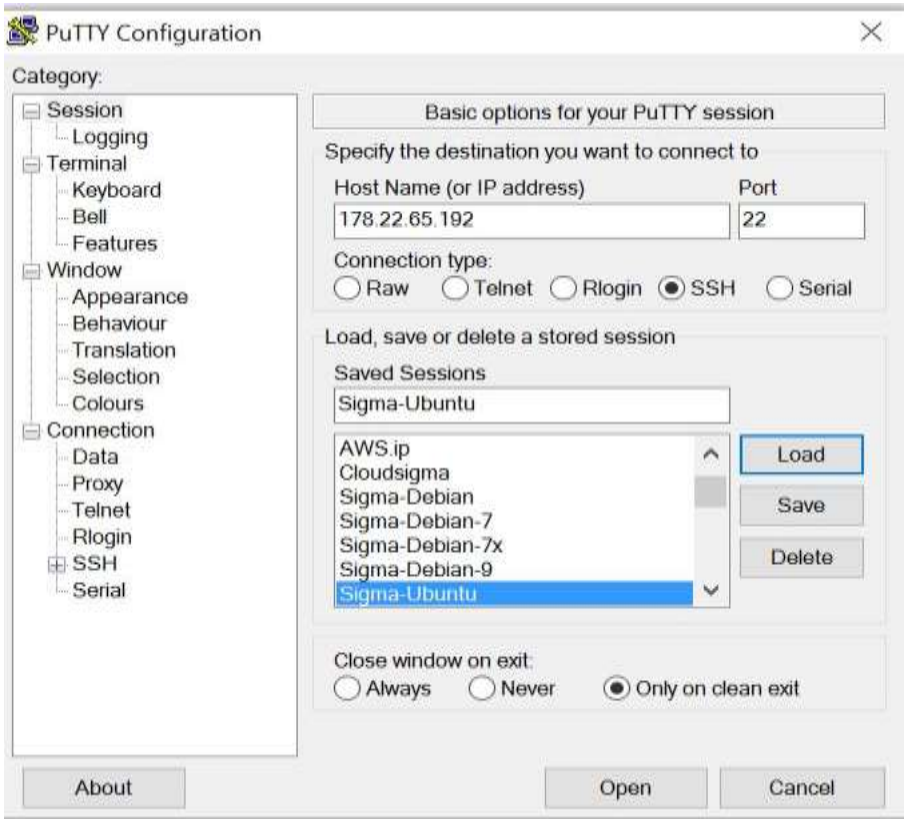


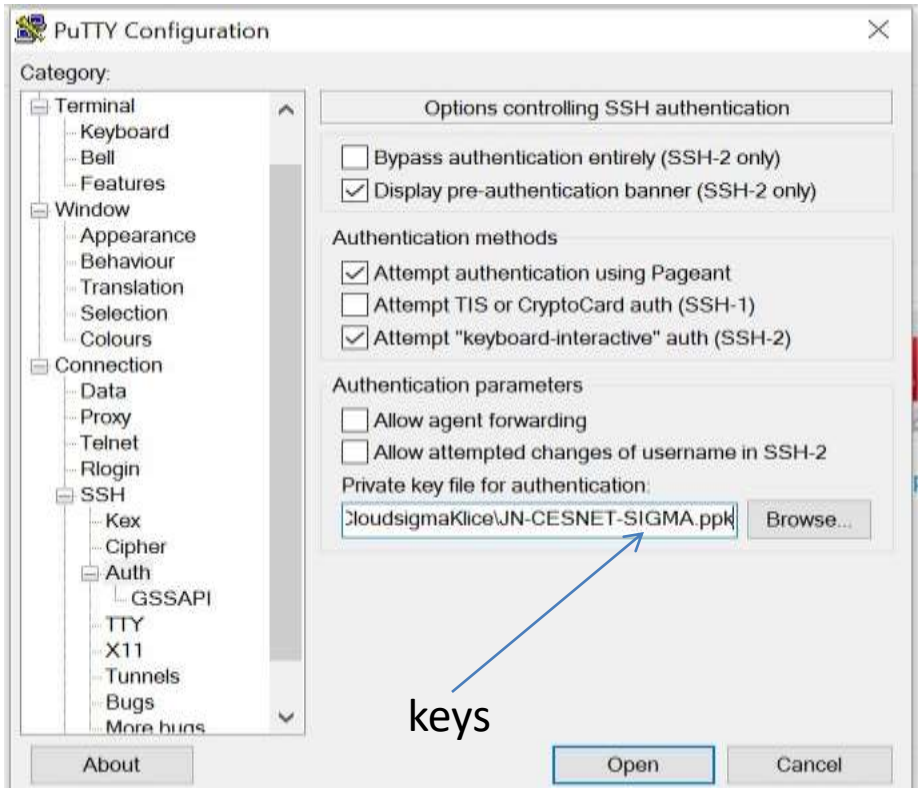
ssh –i .ssh/my_clouds-key.rsa root@xy-machine.aws.com

```
ubuntu@ip-172-31-9-117: ~
Authenticating with public key "imported-openssh-key"
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 3.13.0-133-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Nov 21 13:49:00 UTC 2017

  System load:  0.0               Processes:           109
  Usage of /:   19.7% of 7.74GB   Users logged in:     0
  Memory usage: 21%               IP address for eth0: 172.31.9.117
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

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

29 packages can be updated.
20 updates are security updates.


Last login: Fri Nov  3 08:55:22 2017 from eduroam-188.cesnet.cz
ubuntu@ip-172-31-9-117:~$
```

L2 user - Prepare to Login to VM from PC

With PUTTY, PUTTYGEN





From Windows use “putty” with Your own keys or generated keys from provider converted to ppk via PUTTYGEN

L2 user - Inside VM

Acting as System and Application administrator

(root or ubuntu/sudo, etc.)

Moodle used as testing application

- **E-learning system used in many schools and universities, widely spread all over the world**
- Quite complex system with **own users, DB, WEB**
- You must install several fundamental software tools on VM
  as L2 user
  - mySQL database or other DB
  - Apache WEB,
  - PHP5.6 or 7.0
  - Moodle 3.2

  L3 user Moodle admin to create:
  - roles for rest of users: manager, teacher, student
  - prepare content – courses
  - link to mailing server

  Make access for Moodle users, registration to courses, etc.

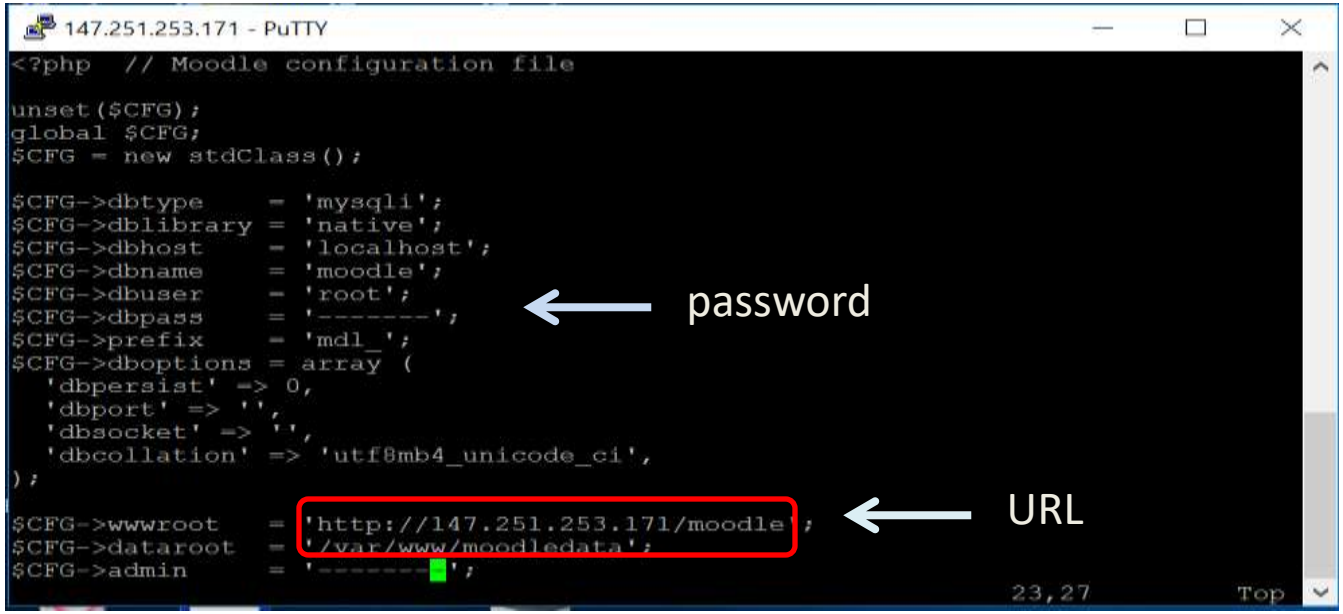
  L4 Users (lectures, preparing content in the Moodle, students attending courses)
  L3 and L4 Users running application users which doesn't know if it is on cloud on not)

L2 user - Inside VM

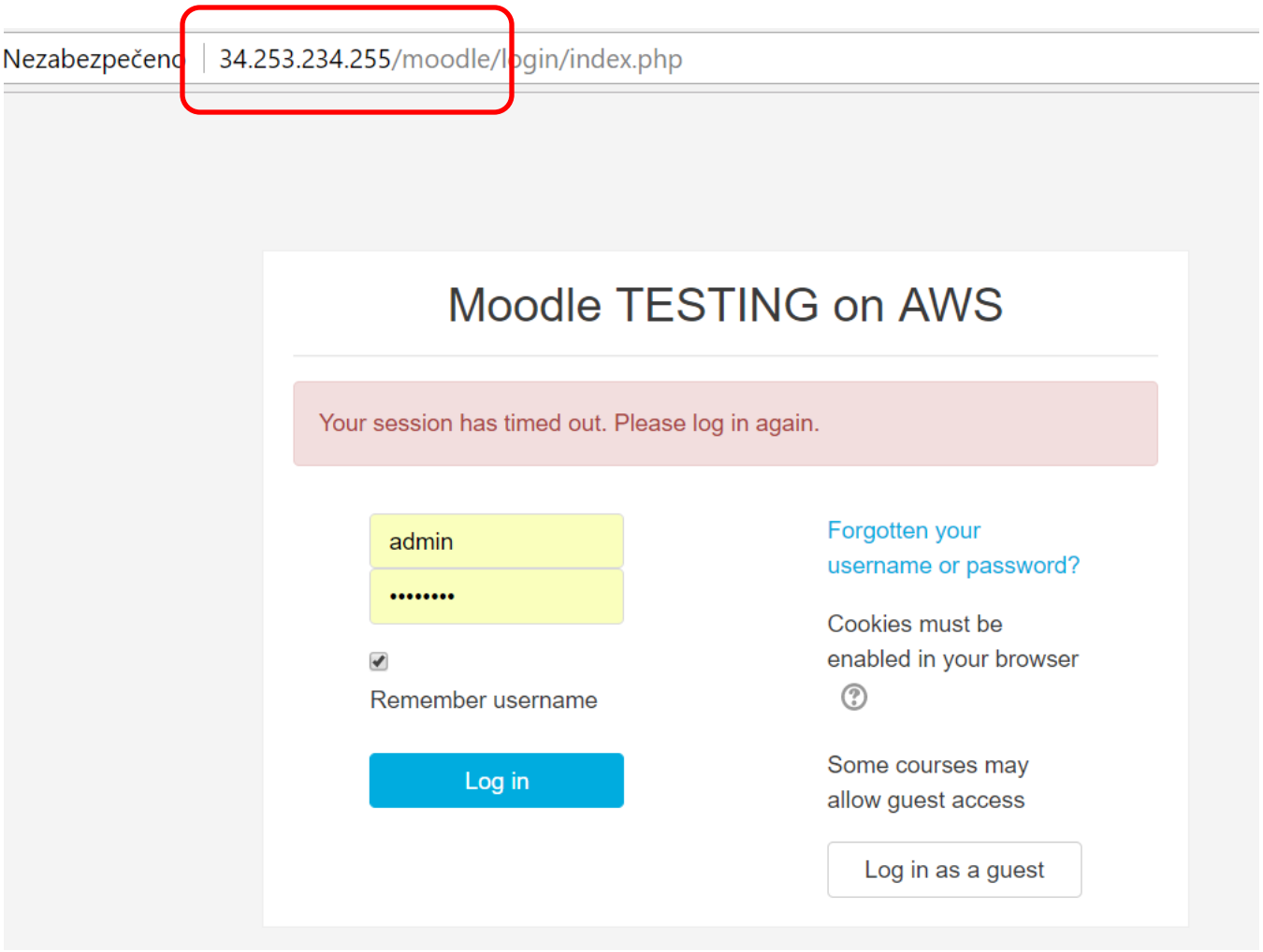
Install your application

```
sudo apt-get update

sudo apt-get install apache2 mysql-client mysql-server php5

sudo apt-get install graphviz aspell php5-pspell php5-curl php5-gd
...
```

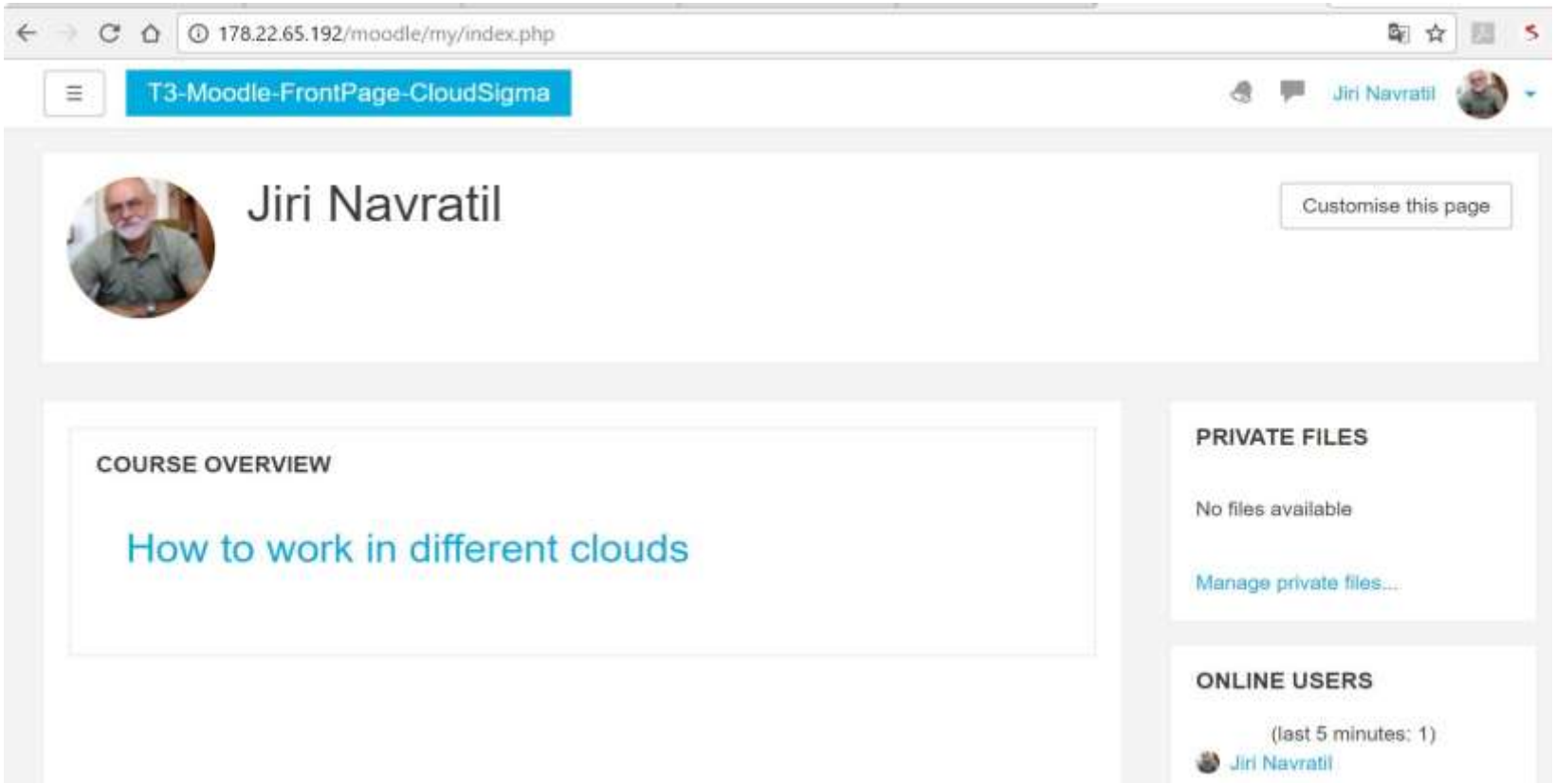
Configure Moodle



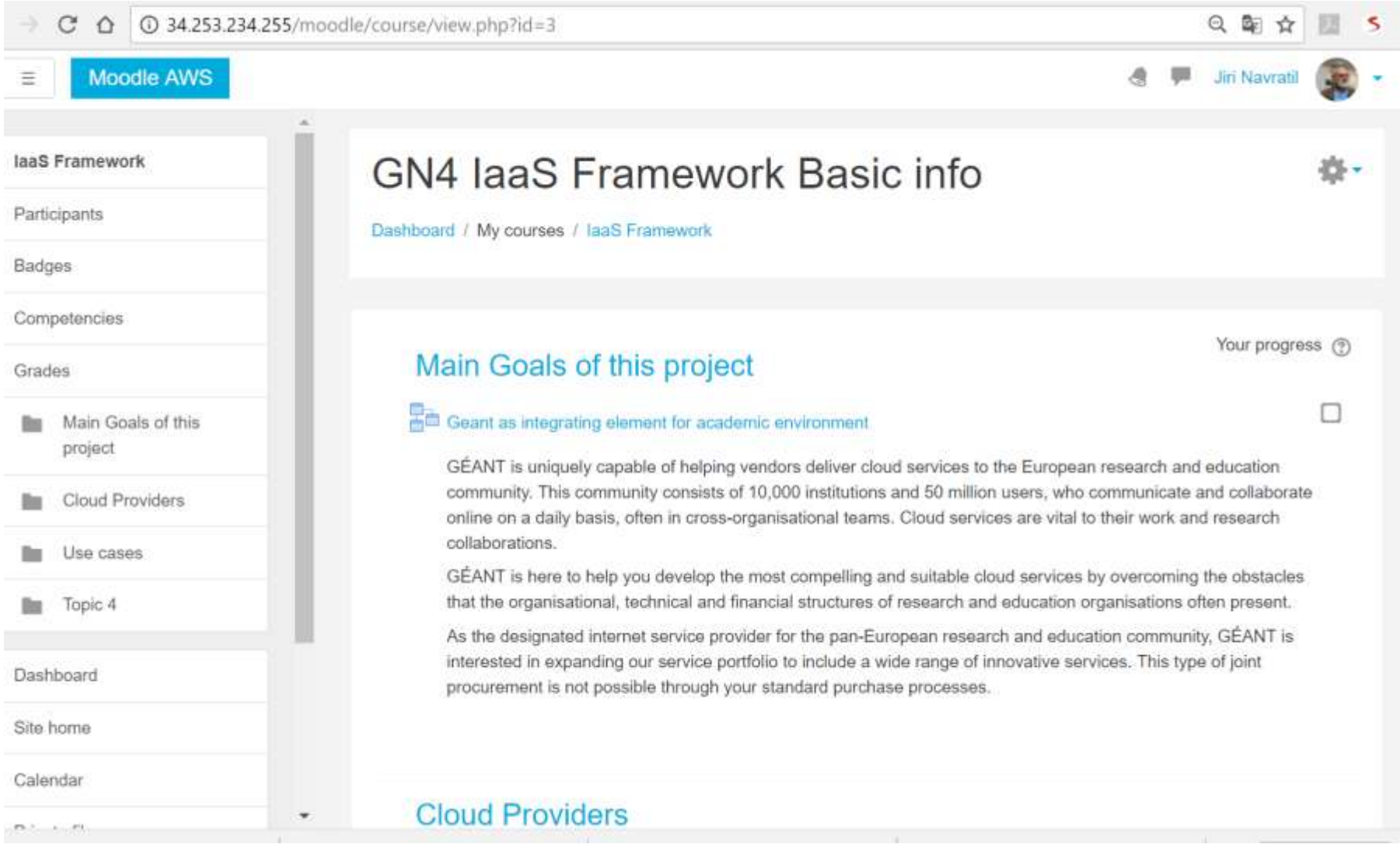
L3 user Login to Application



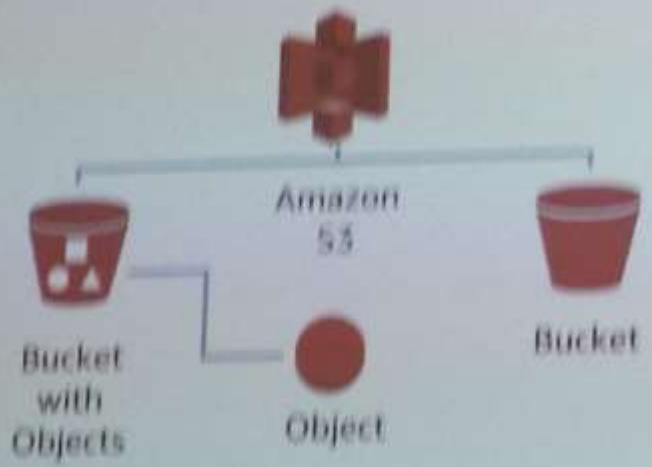
L3 user Inside Moodle



L3 user inside Moodle testing application



Amazon S3 storage concept



- Amazon S3 stores data as objects within buckets.
- An object is composed of a file and optionally any metadata that describes that file.
- You can have up to 100 buckets in each account.
- You can control access to the bucket and its objects.

An object key is the unique identifier for an object in a bucket.

http://doc.s3.amazonaws.com/2006-03-01/AmazonS3.html

Bucket

Object/Key

Amazon S3 Facts

- Can store an **unlimited** number of objects in a bucket
- Objects can be up to **5 TB**; no bucket size limit
- Designed for **99.999999999%** durability and **99.99%** availability of objects over a given year
- Can use **HTTP/S** endpoints to store and retrieve any amount of data, at any time, from anywhere on the web
- Highly scalable, reliable, fast, and inexpensive
- Can use optional server-side **encryption** using AWS or customer-managed provided client-side encryption
- Auditing is provided by access **logs**
- Provides standards-based **REST** and SOAP interfaces

Cloud Activity reports

(Billing, Pricing, Licensing)

To Open subscription for AWS, Microsoft, etc.
As individual you need valid Credit card !
OR
Your organization must sign a contract with reseler

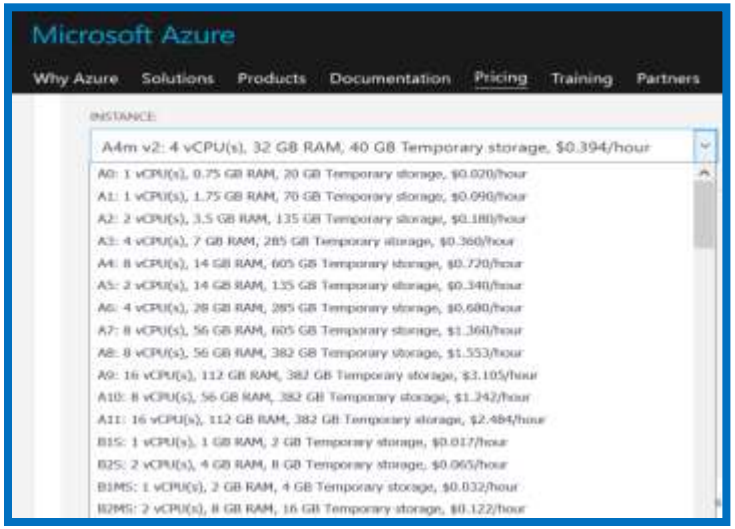
Pricing models

AWS - used resources for my testing cca 15 US/month

CloudSigma – allocated resources cca 60 EURO/per month

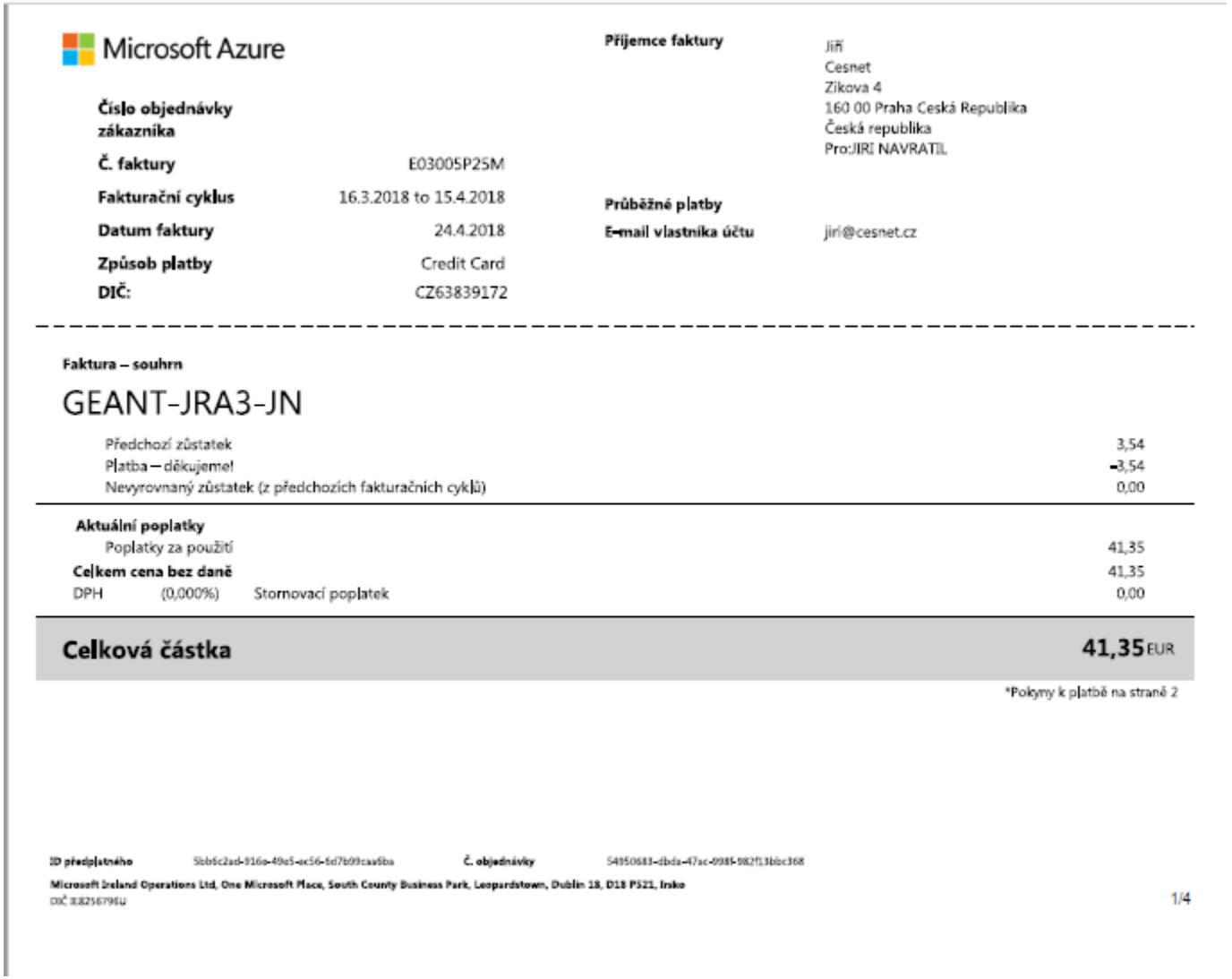
Microsoft

- http://azure.microsoft.com/en-us/pricing/calculator/
- https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/



Linear price to used resource or not ?

Microsoft Invoice



Microsoft Azure

Číslo objednávky zákazníka	
Č. faktury	E03005P25M
Fakturační cyklus	16.3.2018 to 15.4.2018
Datum faktury	24.4.2018
Způsob platby	Credit Card
DIČ:	CZ63839172

Příjemce faktury

Jiří
Cesnet
Zikova 4
160 00 Praha Ceská Republika
Česká republika
Pro:JIRI NAVRATIL

Průběžné platby

E-mail vlastníka účtu jiri@cesnet.cz

Faktura – souhrn

GEANT-JRA3-JN

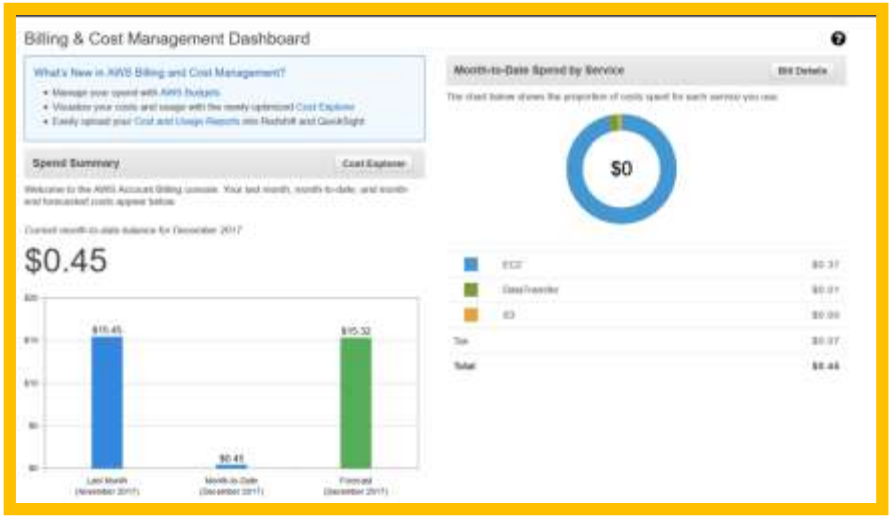
Předchozí zůstatek	3,54
Platba – děkujeme!	-3,54
Nevyrovnaný zůstatek (z předchozích fakturačních cyklů)	0,00
Aktuální poplatky	
Poplatky za použití	41,35
Celkem cena bez daně	41,35
DPH (0,000%) Stornovací poplatek	0,00
Celková částka	**41,35** EUR

*Pokyny k platbě na straně 2

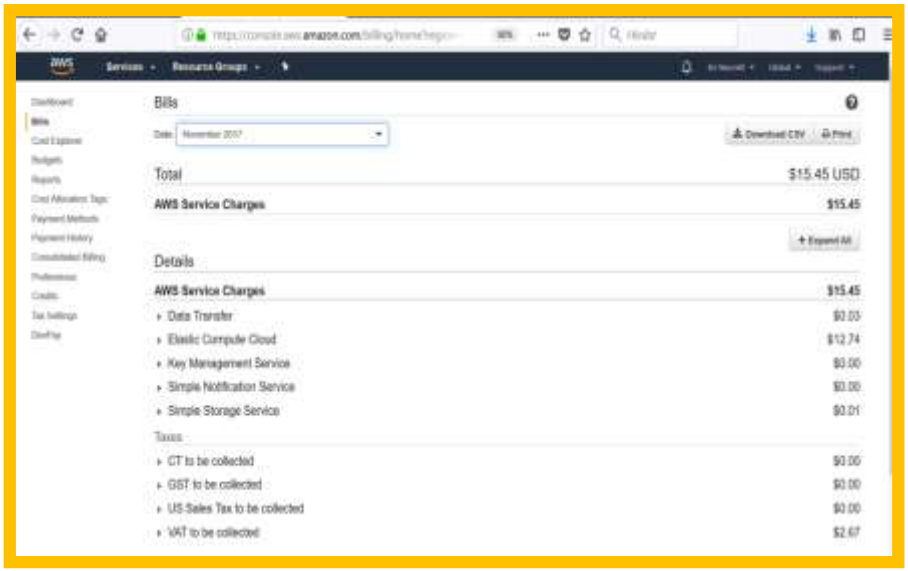
ID předplatného 5bb6c2ad-916a-49e5-ac56-6d7b09caa5ba **Č. objednávky** 54950683-dbda-47ac-0985-982f13bbc368

Microsoft Ireland Operations Ltd, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irsko
DIČ IE8256796U

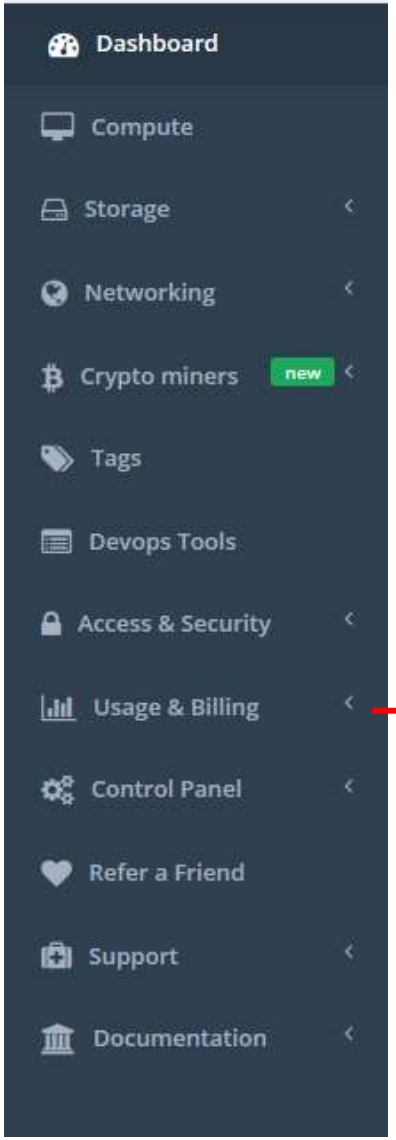
AWS Billing console

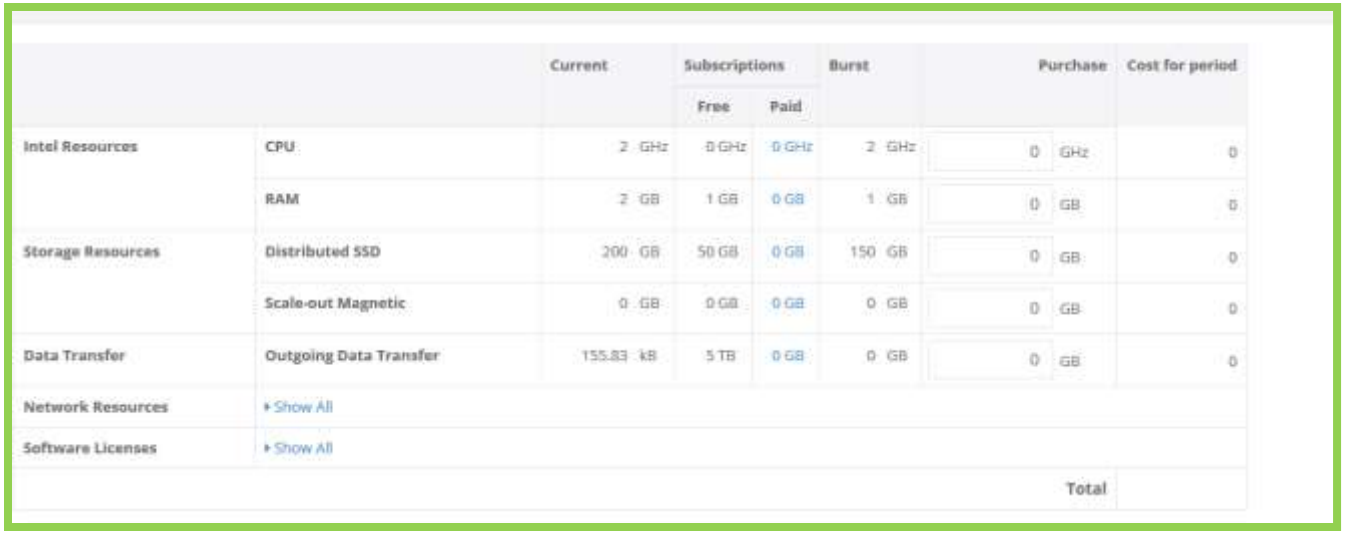


AWS Monthly Invoice

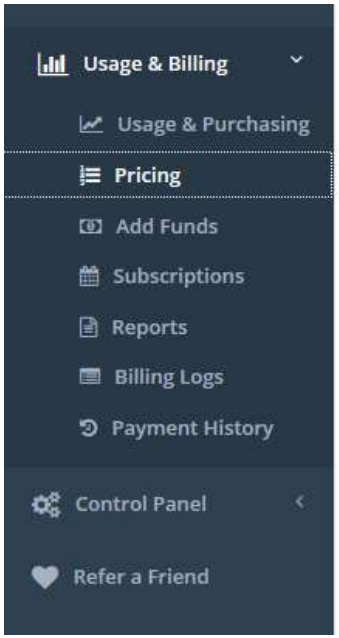


CloudSigma Usage review





		Current	Subscriptions		Burst	Purchase	Cost for period
			Free	Paid			
Intel Resources	CPU	2 GHz	0 GHz	0 GHz	2 GHz	0 GHz	0
	RAM	2 GB	1 GB	0 GB	1 GB	0 GB	0
Storage Resources	Distributed SSD	200 GB	50 GB	0 GB	150 GB	0 GB	0
	Scale-out Magnetic	0 GB	0 GB	0 GB	0 GB	0 GB	0
Data Transfer	Outgoing Data Transfer	155.83 kB	5 TB	0 GB	0 GB	0 GB	0
Network Resources	▸ Show All						
Software Licenses	▸ Show All						
						Total	



Summary

Existing infrastructures were built gradually during long period by different specialists (system engineers, technicians, networkers) connecting together many HW pieces with wired network.

On clouds you can create your new environment on remote infrastructure exactly as on your home infrastructure without touching HW and wires. You can apply programmatically all types of rights, restrictions and limitations. IT architects in large infrastructures appears as very important role.

No needs extra space, no HW no wiring. Work can be done in parallel to existing infrastructure in couple of weeks.

You should trust to cloud providers same way as you trust to your own DC staff or partners. There are principally same dangers - INTERNET.

You need experienced IT staff who know how to do it or
to rent special contractors ! It is not task for cloud providers support !

Thank you for your attention

Q ?