TP3 Report

LOAD BALANCERS

By: Nadia FRIKHA and Rania MIDAOUI, RT4-G2

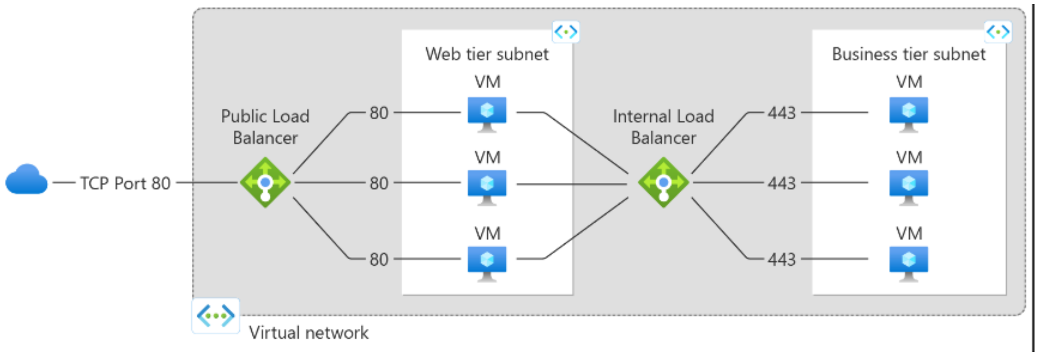
Introduction:

Azure load balancers are considered a critical component of Microsoft Azure's cloud infrastructure. They play a crucial role in ensuring high availability, scalability, and performance of applications by distributing incoming network traffic across multiple servers or virtual machines.

Azure load balancers are especially useful in scenarios where there is a high volume of traffic to an application or service. Overall, this TP will demonstrate how Azure load balancers can help improve the reliability and performance of applications in Microsoft Azure's cloud infrastructure.

Azure load balancers :

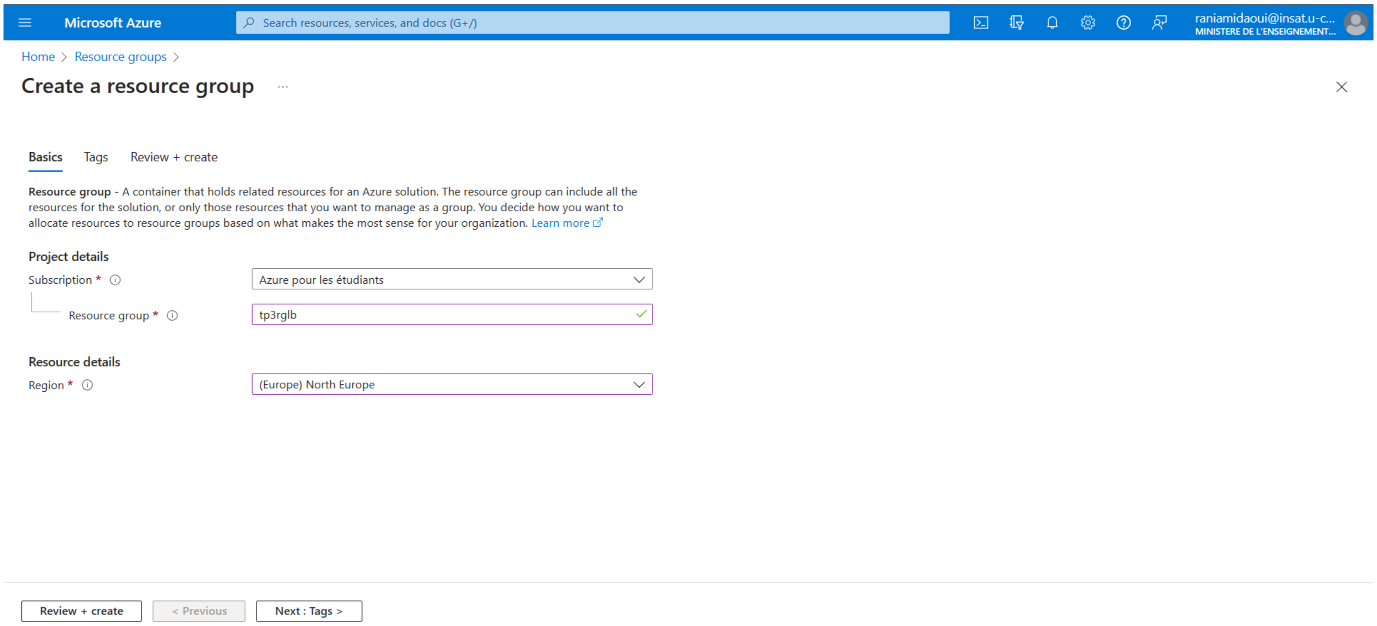
Load balancing evenly distributes incoming network traffic across a group of backend resources or servers. In Azure, the Load Balancer operates at layer 4 of the OSI model and acts as the single point of contact for clients. It uses configured load-balancing rules and health probes to distribute inbound flows to backend pool instances, which can be Azure Virtual Machines or instances in a Virtual Machine Scale Set.
A Public Load Balancer in Azure can provide outbound connections for virtual machines inside your virtual network by translating their private IP addresses to public IP addresses. This type of load balancer is commonly used to balance internet traffic to virtual machines.
On the other hand, an Internal (or Private) Load Balancer is used where private IPs are needed at the frontend only. It is used to balance traffic inside a virtual network and its frontend can be accessed from an on-premises network in a hybrid scenario.

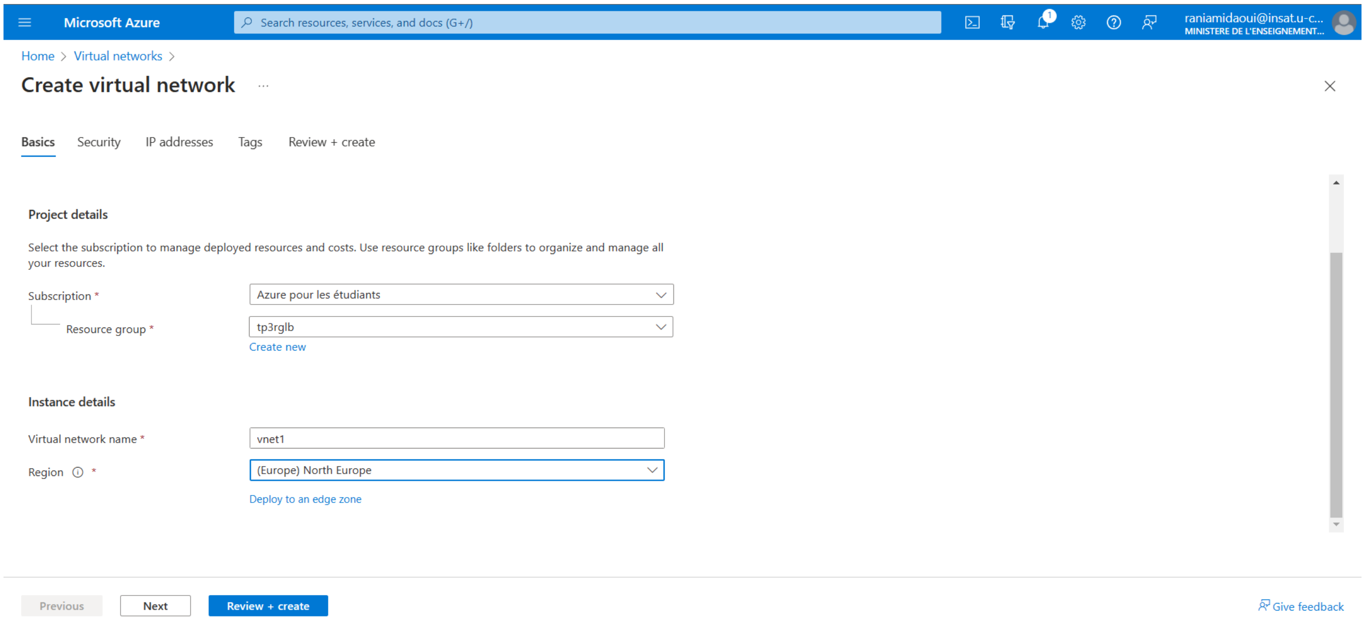


Questions:

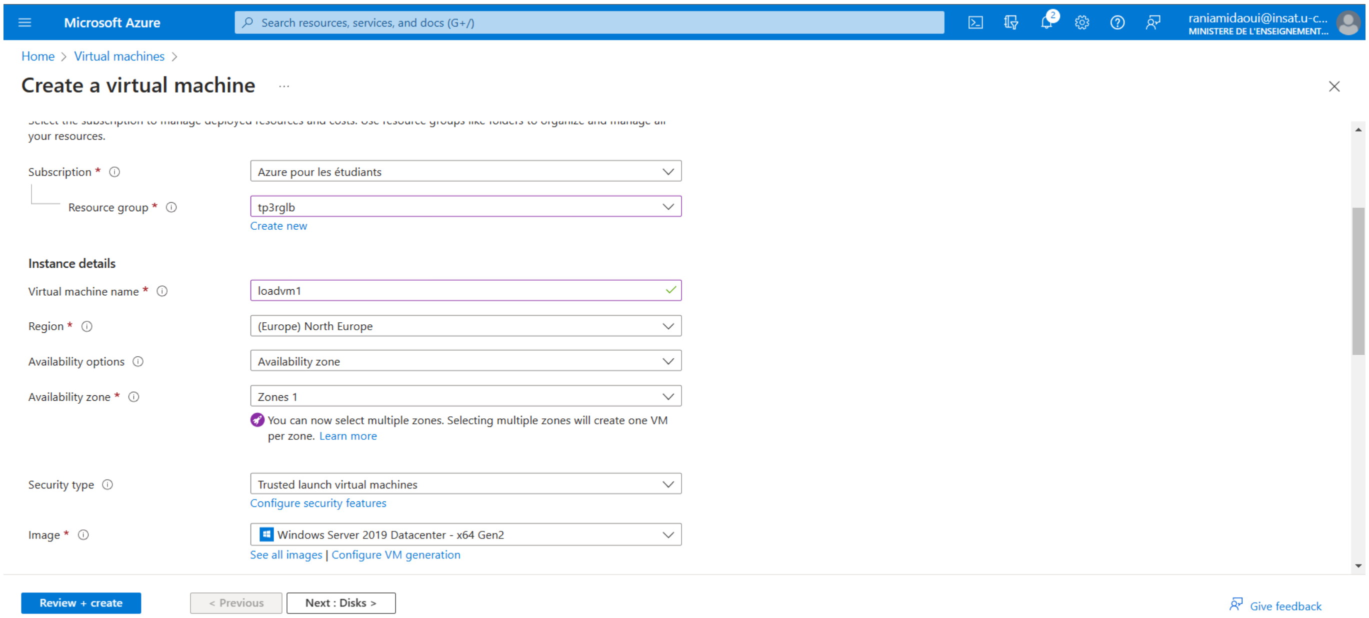
Task 1: Standard load balancer

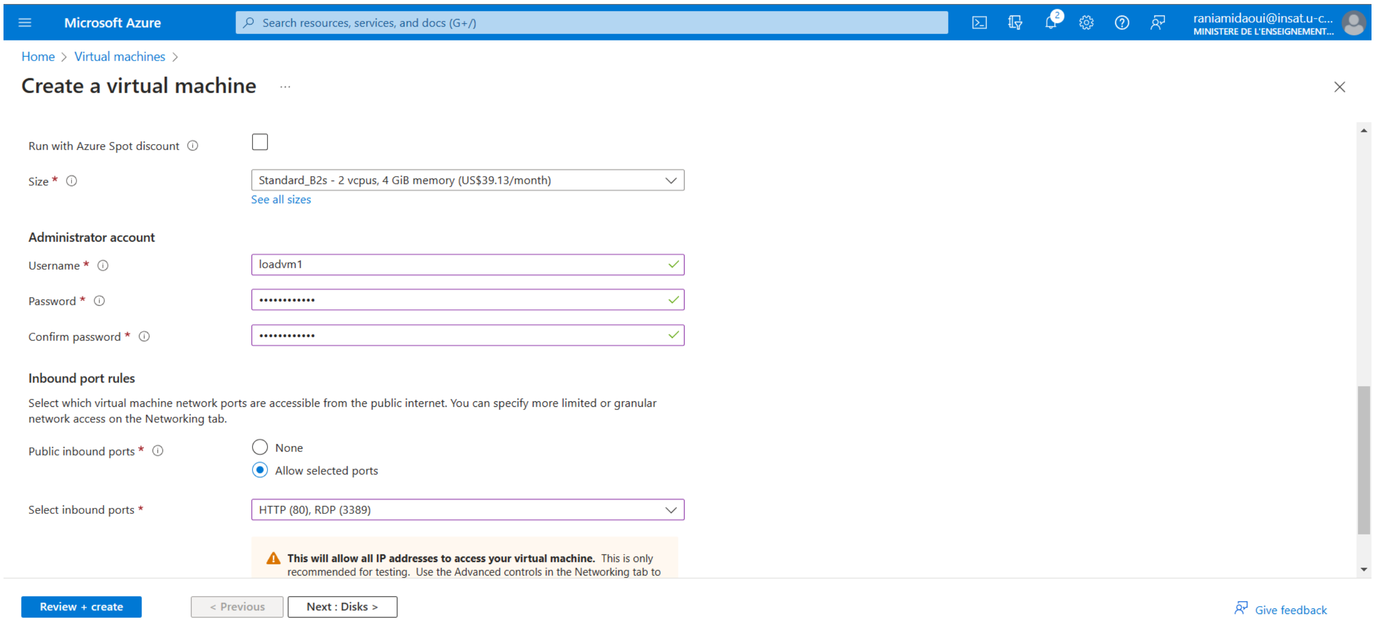
1- We create a resource group named tp3rglb then a virtual network named vnet0:



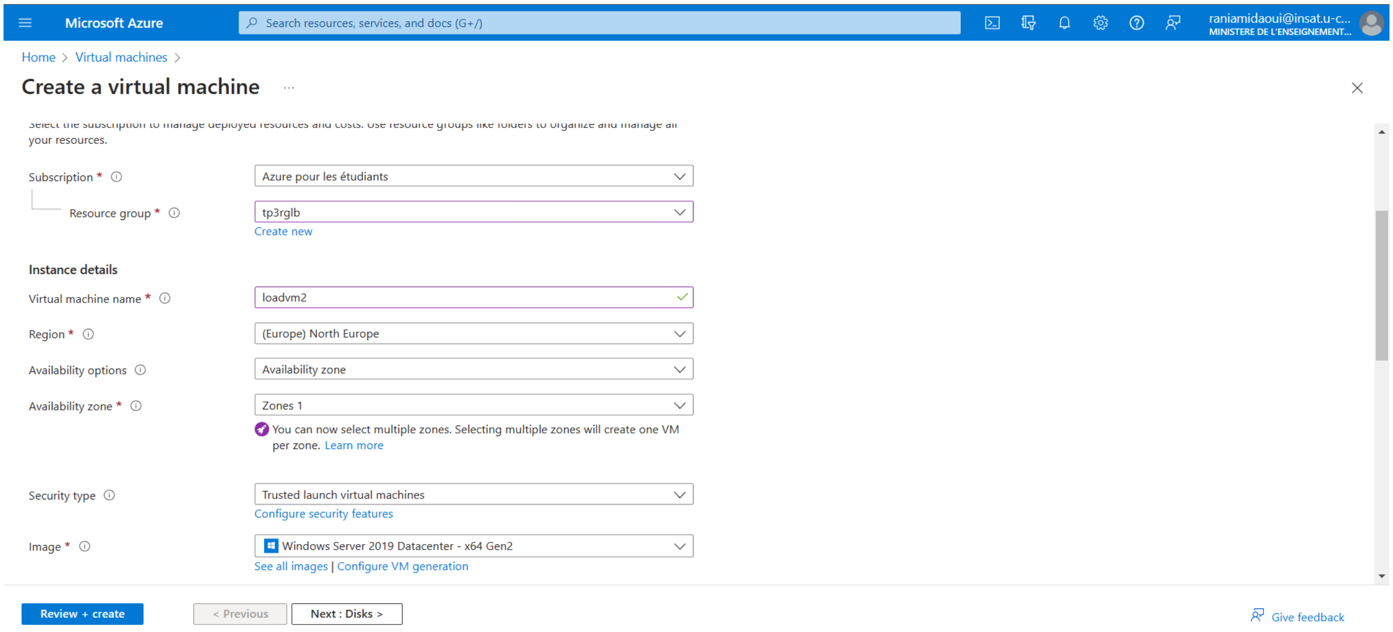


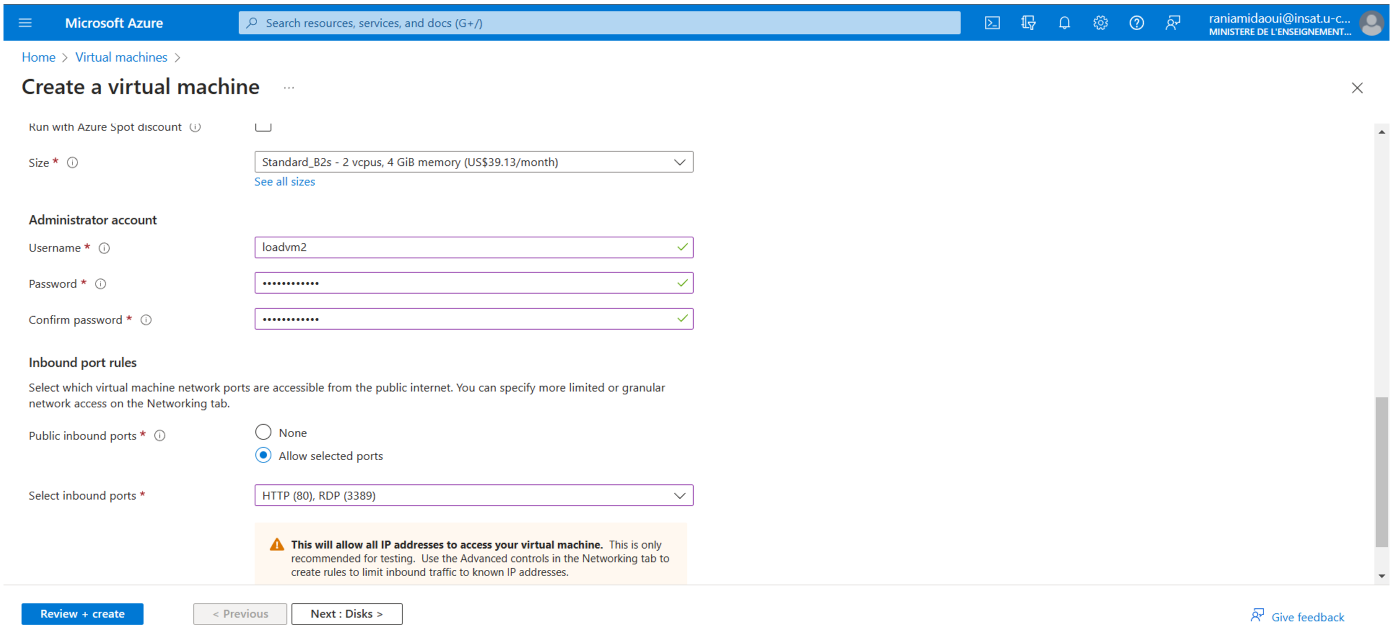
2- We create the first virtual machine loadvm1:



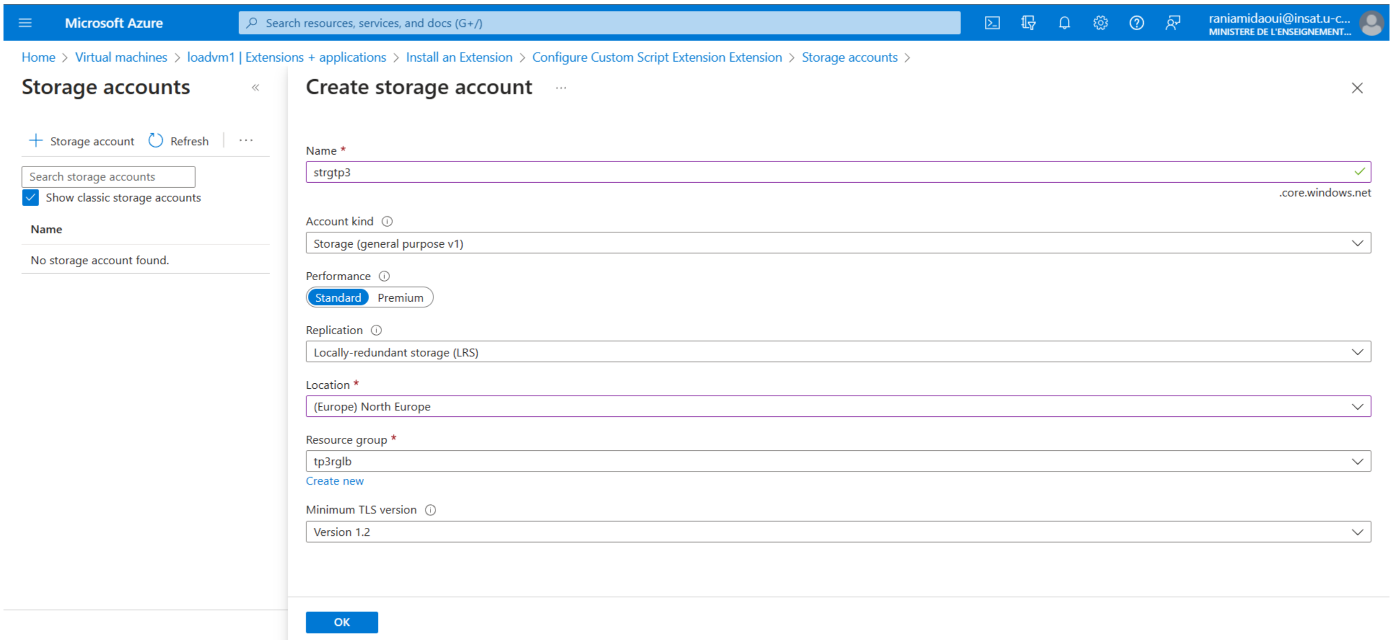


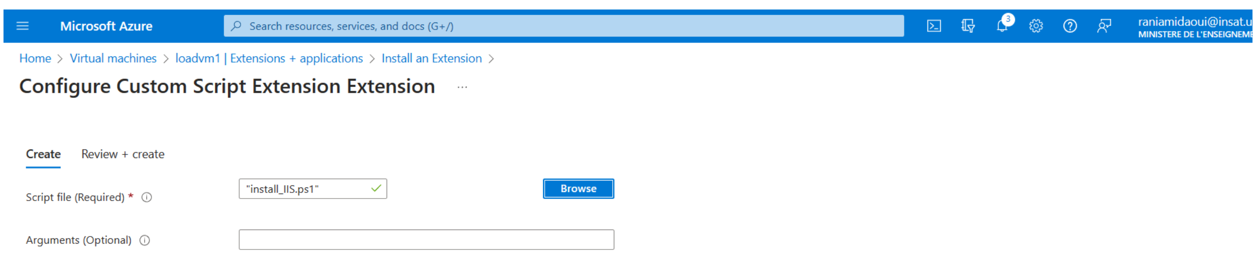
3- We create the second virtual machine loadvm2:

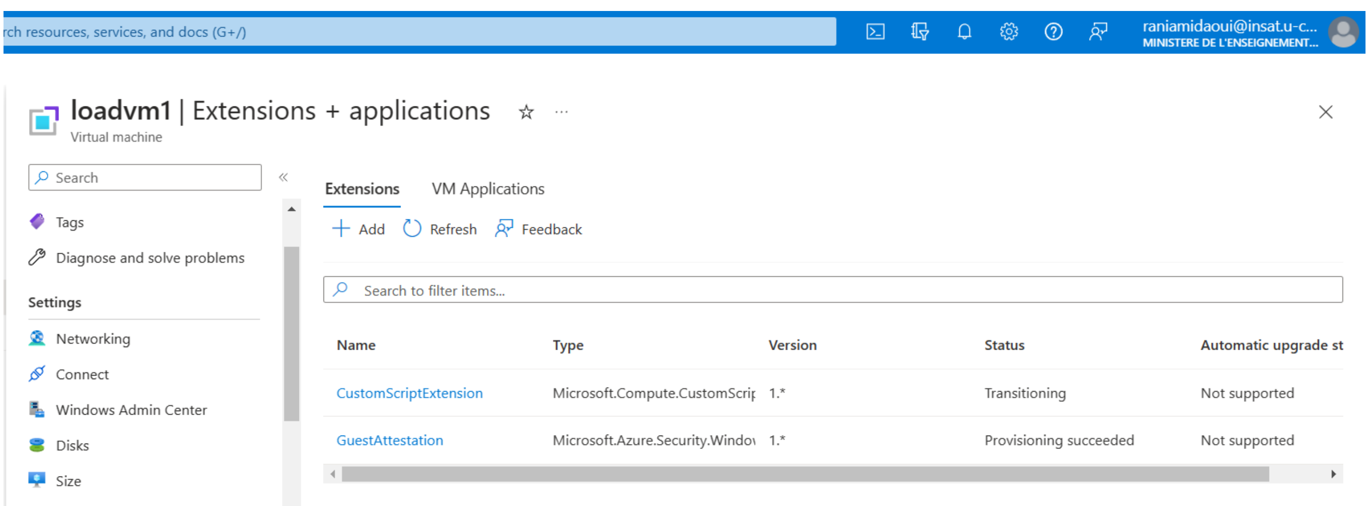




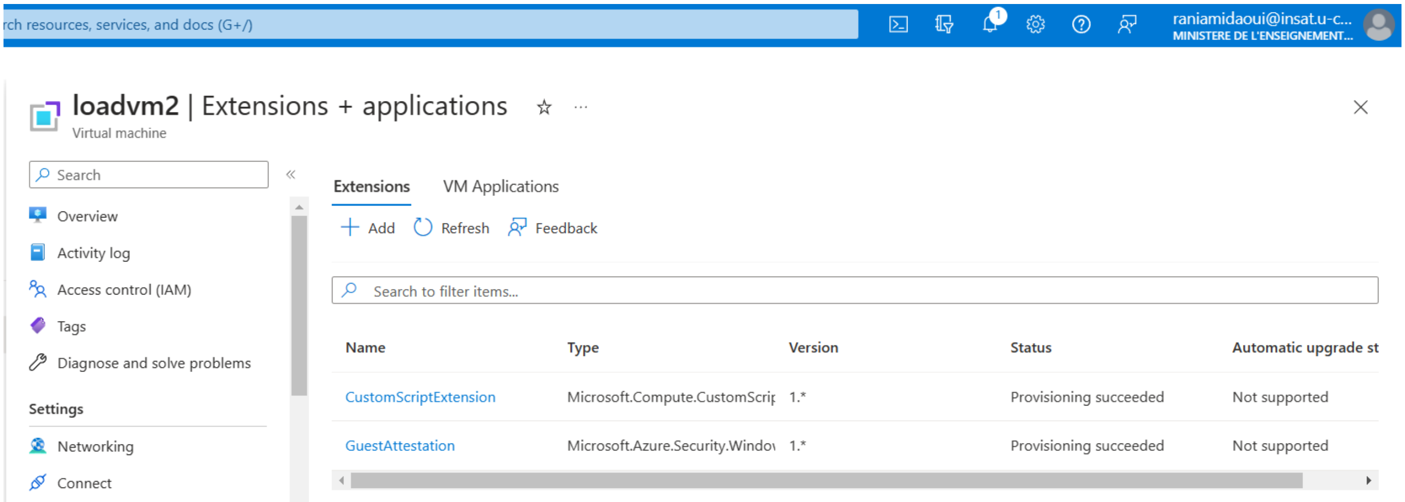
4 - We add a Custom Script Extension to install IIS server in loadvm1:



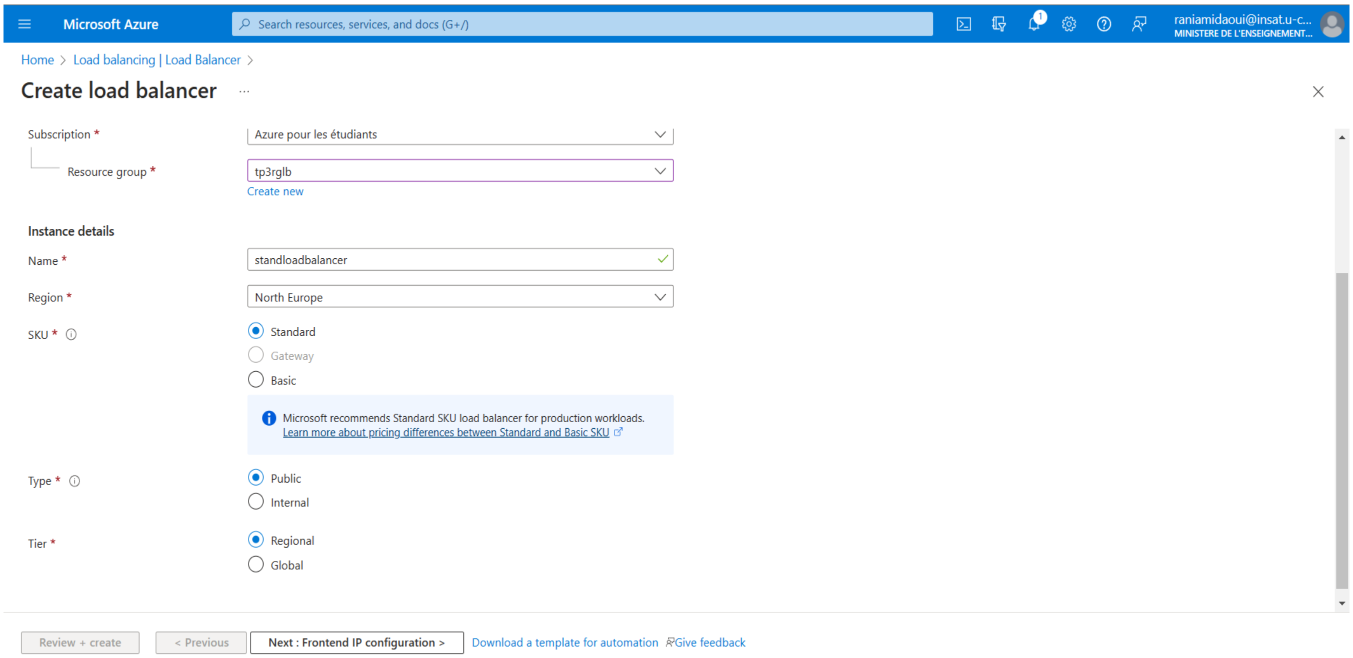


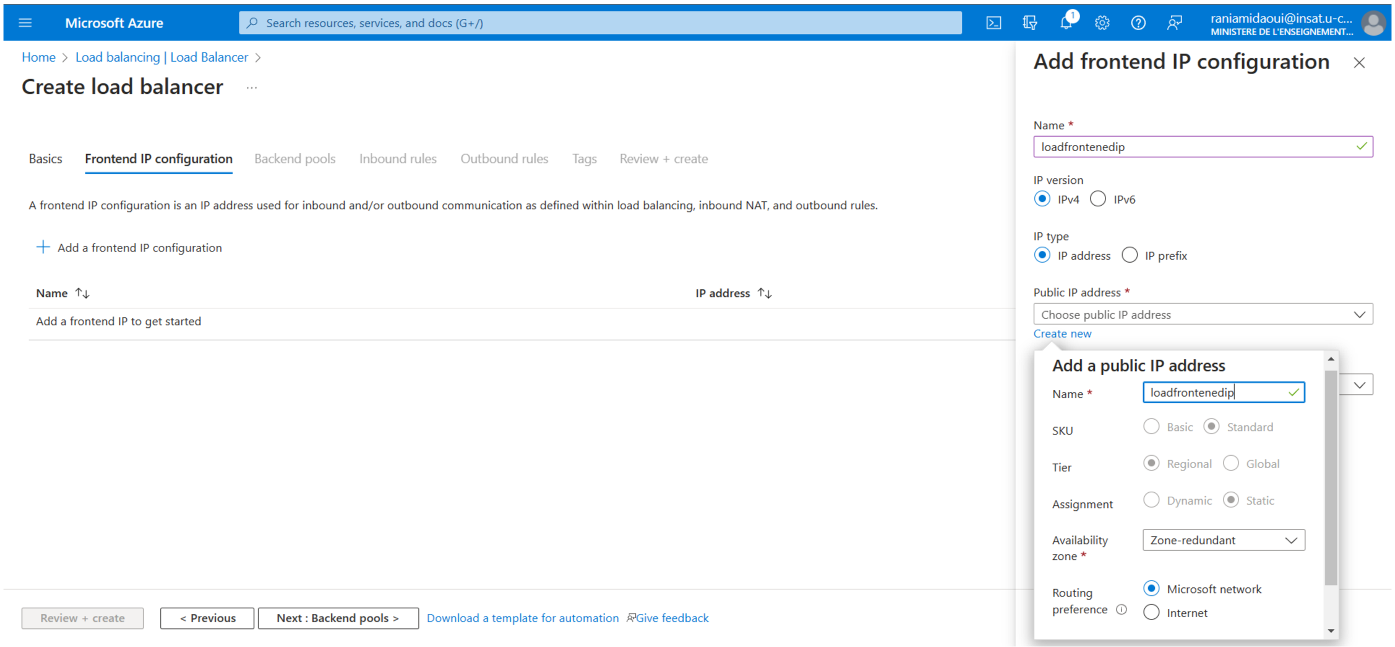


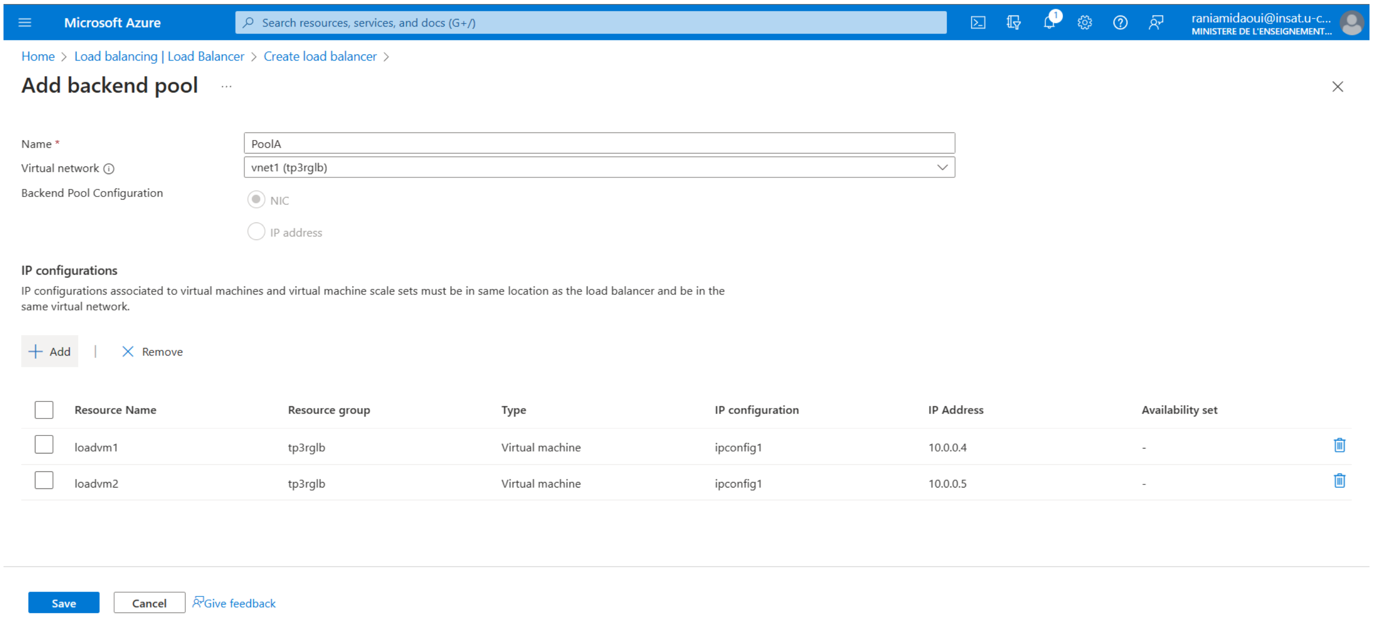
5- We add a Custom Script Extension to install IIS server in loadvm2:

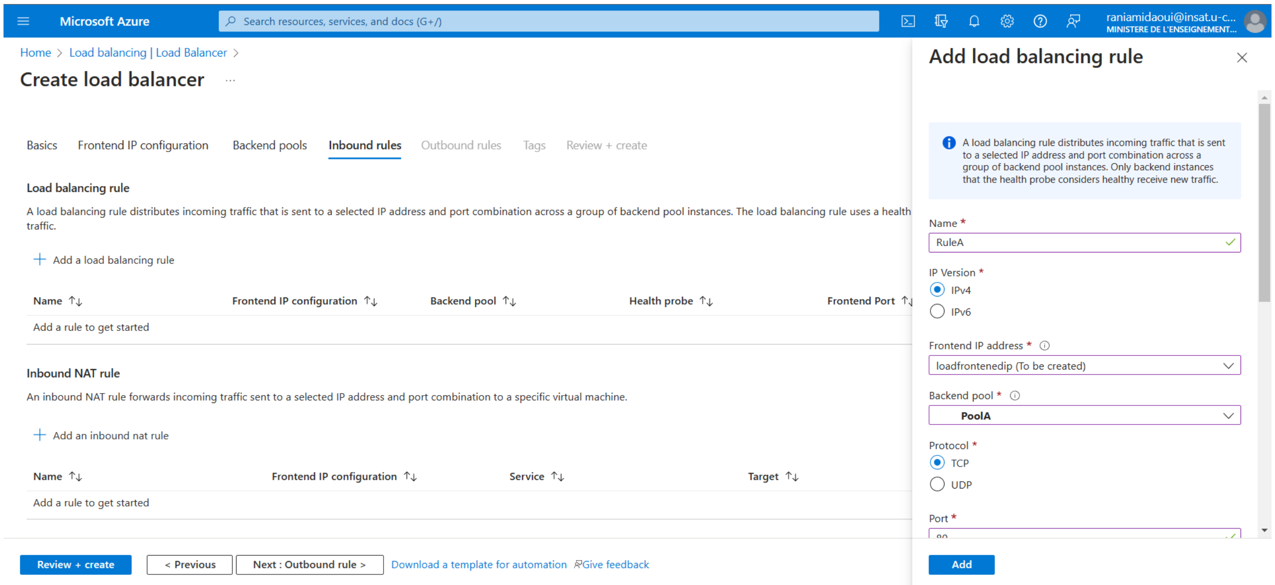


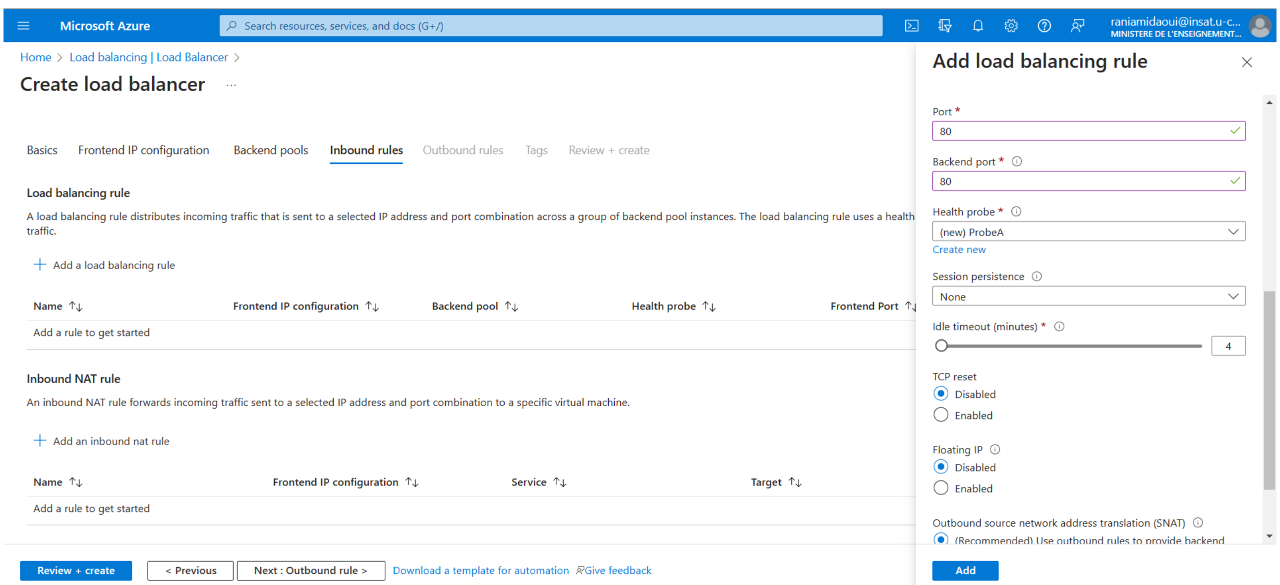
6- We create a standard SKU load balancer:

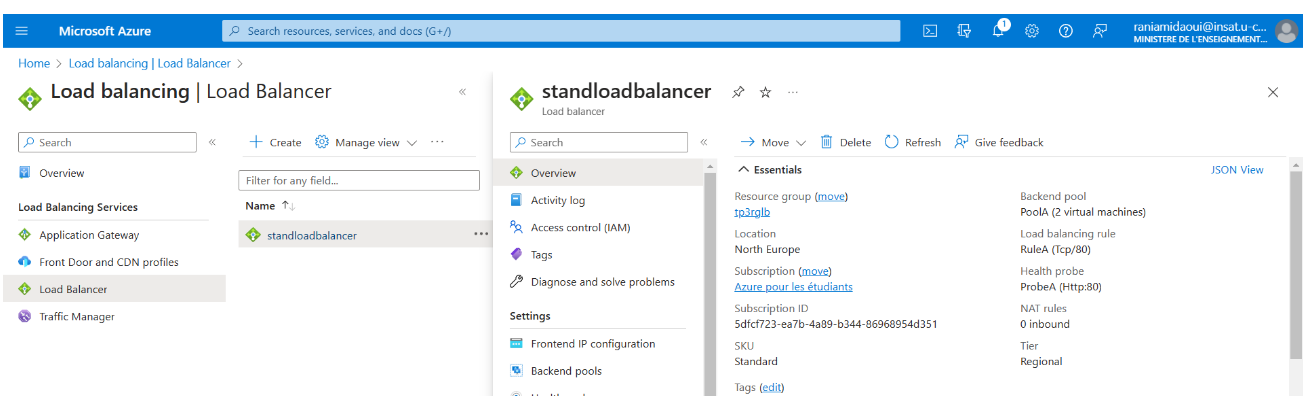



Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Load Balancer >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.
Add a frontend IP configuration
Name
IP address
Add a frontend IP to get started
Review + create
< Previous
Next : Backend pools >
Download a template for automation
Give feedback
Add frontend IP configuration
Name *
loadfrontendip
IP version
IPv4
IPv6
IP type
IP address
IP prefix
Public IP address *
Choose public IP address
Create new
Add a public IP address
Name *
loadfrontendip
SKU
Basic
Standard
Tier
Regional
Global
Assignment
Dynamic
Static
Availability zone *
Zone-redundant
Routing preference
Microsoft network
Internet

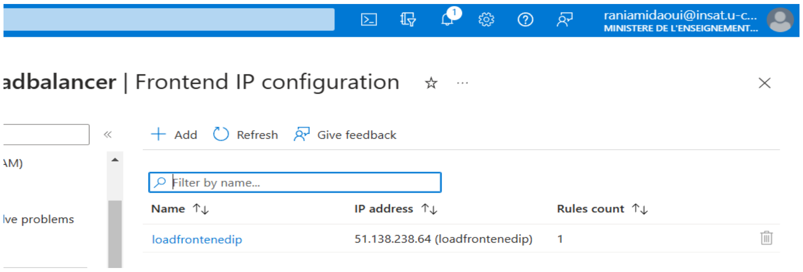

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Load Balancer > Create load balancer >
Add backend pool
Name *
PoolA
Virtual network
vnet1 (tp3rglb)
Backend Pool Configuration
NIC
IP address
IP configurations
IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.
Add
Remove
Resource Name
Resource group
Type
IP configuration
IP Address
Availability set
loadvm1
tp3rglb
Virtual machine
ipconfig1
10.0.0.4
-
loadvm2
tp3rglb
Virtual machine
ipconfig1
10.0.0.5
-
Save
Cancel
Give feedback


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Load Balancer >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
Load balancing rule
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. The load balancing rule uses a health
traffic.
Add a load balancing rule
Name
Frontend IP configuration
Backend pool
Health probe
Frontend Port
Add a rule to get started
Inbound NAT rule
An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.
Add an inbound nat rule
Name
Frontend IP configuration
Service
Target
Add a rule to get started
Review + create
< Previous
Next : Outbound rule >
Download a template for automation
Give feedback
Add load balancing rule
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. Only backend instances that the health probe considers healthy receive new traffic.
Name *
RuleA
IP Version *
IPv4
IPv6
Frontend IP address *
loadfrontenedip (To be created)
Backend pool *
PoolA
Protocol *
TCP
UDP
Port *
Add

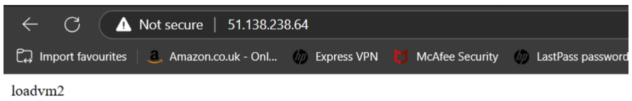

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Load Balancer >
Create load balancer
Basics
Frontend IP configuration
Backend pools
Inbound rules
Outbound rules
Tags
Review + create
Load balancing rule
A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. The load balancing rule uses a health
traffic.
Add a load balancing rule
Name
Frontend IP configuration
Backend pool
Health probe
Frontend Port
Add a rule to get started
Inbound NAT rule
An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.
Add an inbound nat rule
Name
Frontend IP configuration
Service
Target
Add a rule to get started
Review + create
< Previous
Next : Outbound rule >
Download a template for automation
Give feedback
Add load balancing rule
Port *
80
Backend port *
80
Health probe *
(new) ProbeA
Create new
Session persistence
None
Idle timeout (minutes) *
4
TCP reset
Disabled
Enabled
Floating IP
Disabled
Enabled
Outbound source network address translation (SNAT)
(Recommended) Use outbound rules to provide backend
Add


Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Load Balancer >
Load balancing | Load Balancer
Search
Overview
Load Balancing Services
Application Gateway
Front Door and CDN profiles
Load Balancer
Traffic Manager
Create
Manage view
Filter for any field...
Name
standloadbalancer
standloadbalancer
Load balancer
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Frontend IP configuration
Backend pools
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move)
tp3rglb
Location
North Europe
Subscription (move)
Azure pour les étudiants
Subscription ID
5dfcf723-ea7b-4a89-b344-86968954d351
SKU
Standard
Tags (edit)
Backend pool
PoolA (2 virtual machines)
Load balancing rule
RuleA (Tcp/80)
Health probe
ProbeA (Http:80)
NAT rules
0 inbound
Tier
Regional

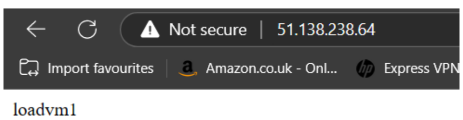
7- We try the public IP address of the load balancer:



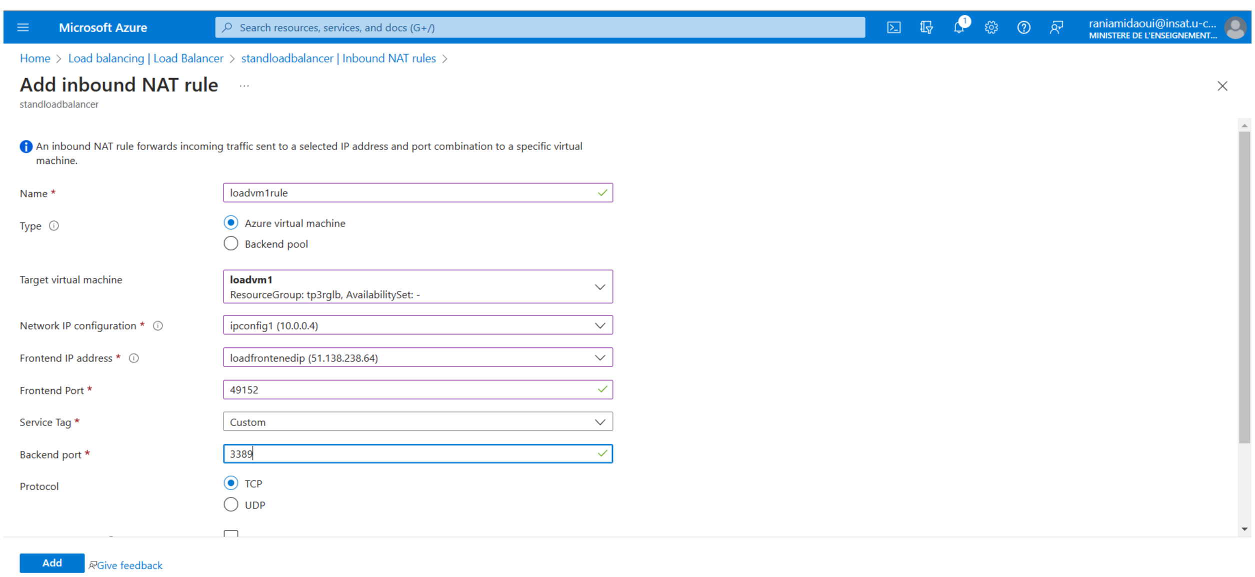
First try, we were redirected to loadvm2:



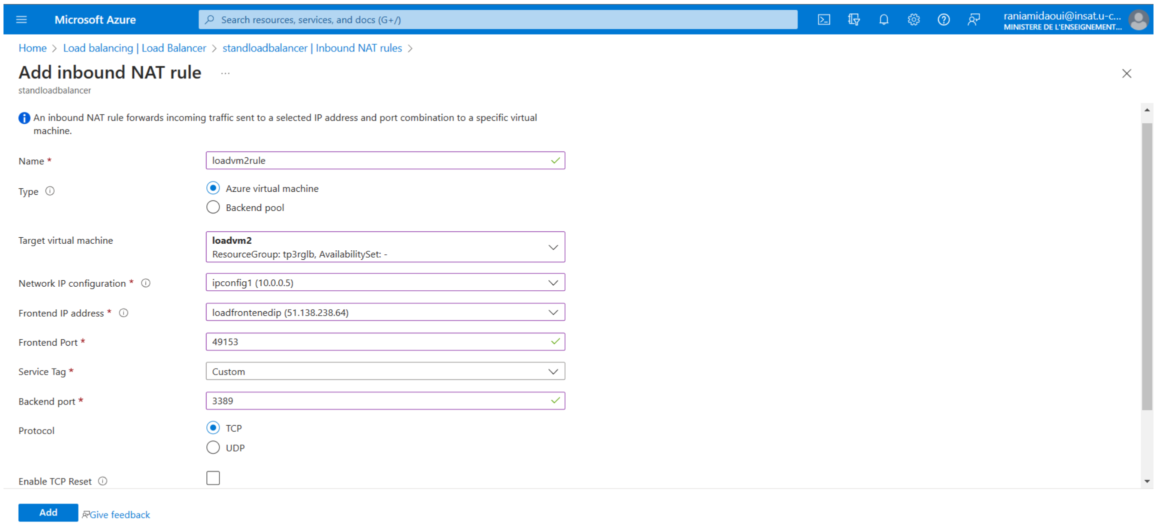
If we refresh the page, we may be redirected to loadvm1 too, our load balancer works perfectly!



8- We add an Inbound NAT rule to loadvm1 connect to a particular service on the virtual machine:

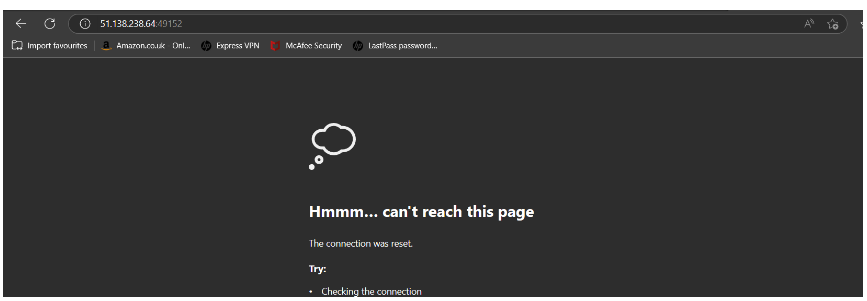


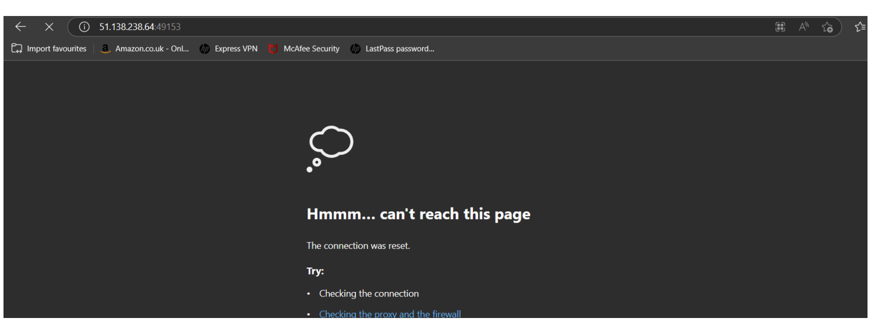
9- We add an Inbound NAT rule to loadvm2:



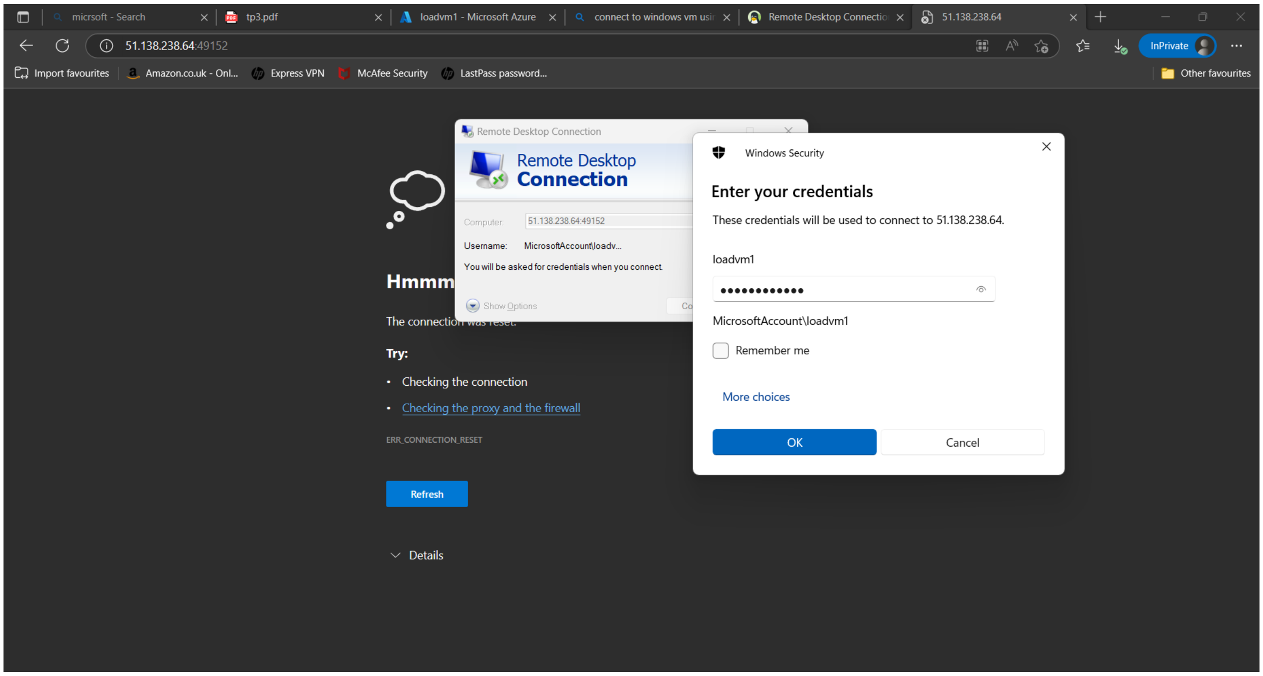
10- In this question, we were asked to open the browser and type the load balancer's public IP address using the mapped ports that we created the Inbound NAT rule with.

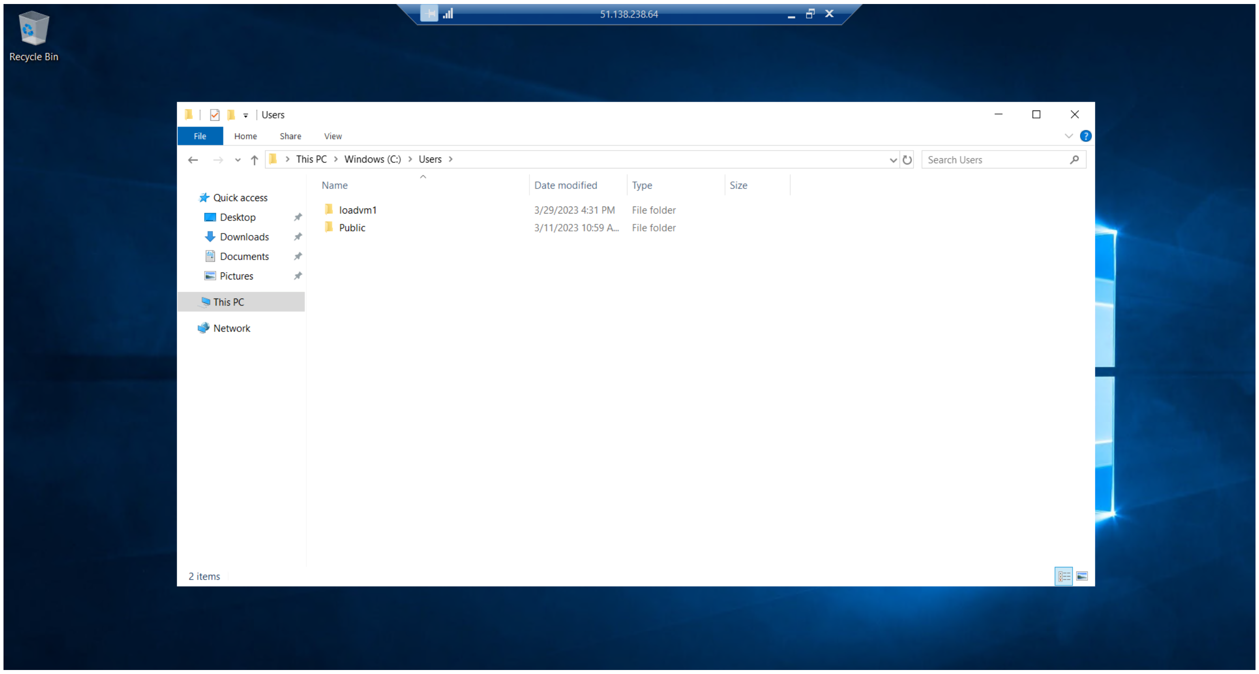
This however, didn't work in the browser because, in the rules created, we mapped the ports 49152 of loadvm1 and 49153 of loadvm2 to the port 3389 (the RDP port) of each vm, so both 51.138.238.64:49152 and 51.138.238.64:49153 should be used in a RDP client as the IP addresses of the machines to demonstrate how the two inbound Nat rules worked .

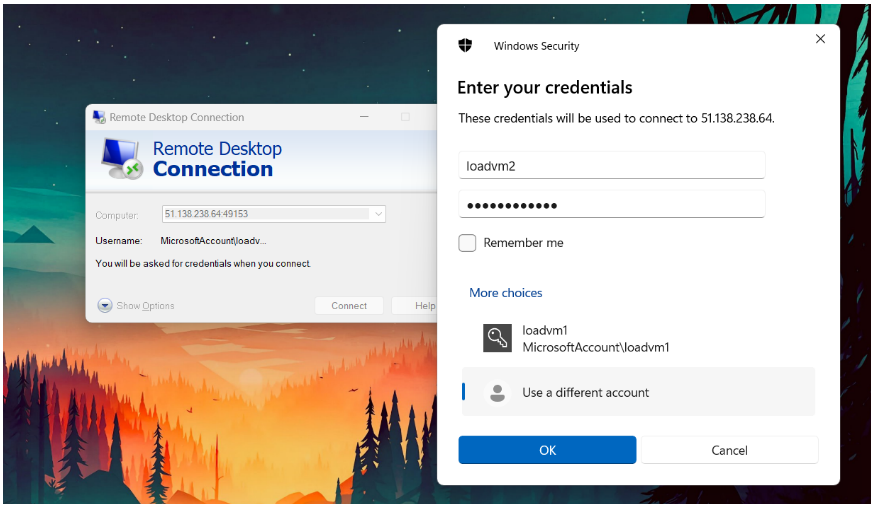


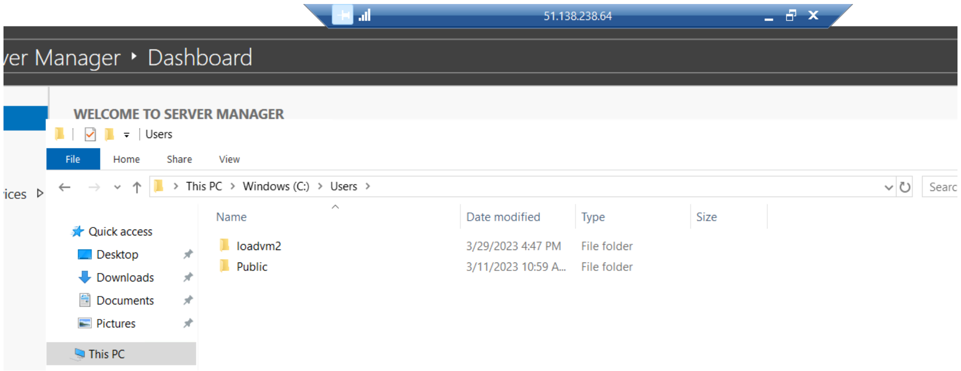


We used both 51.138.238.64:49152 and 51.138.238.64:49153 in the Remote Desktop Protocol client of our Windows machines:



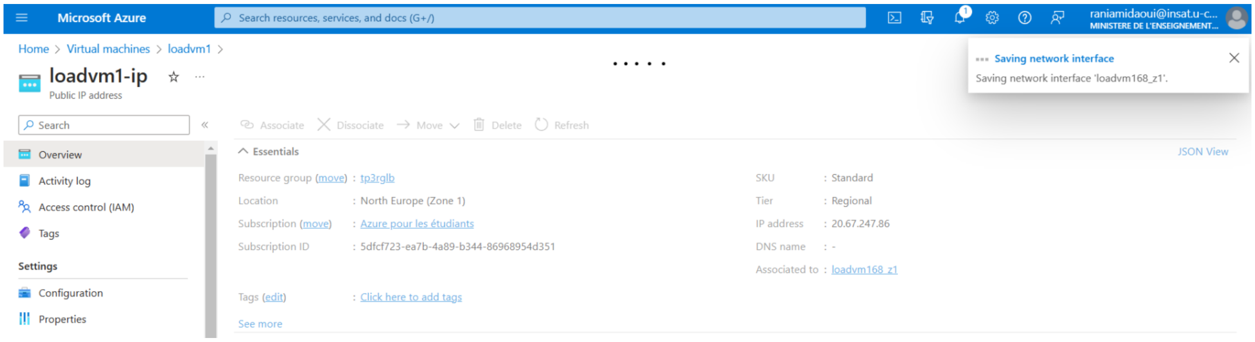


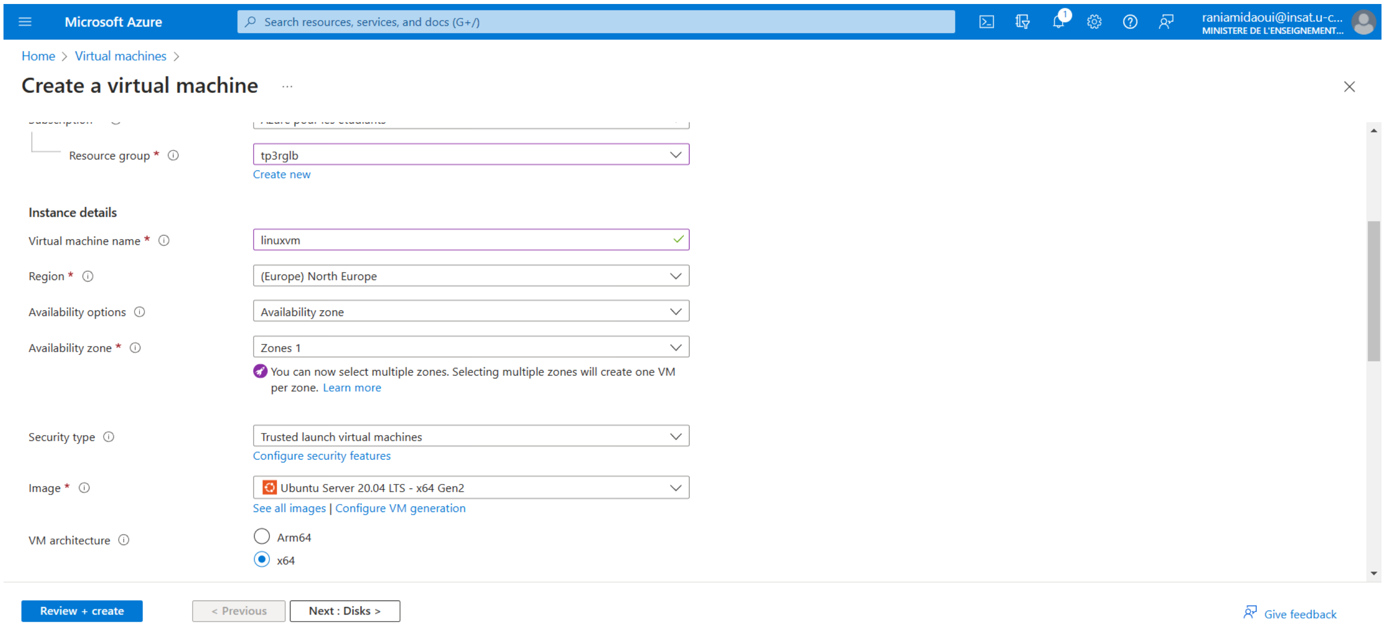


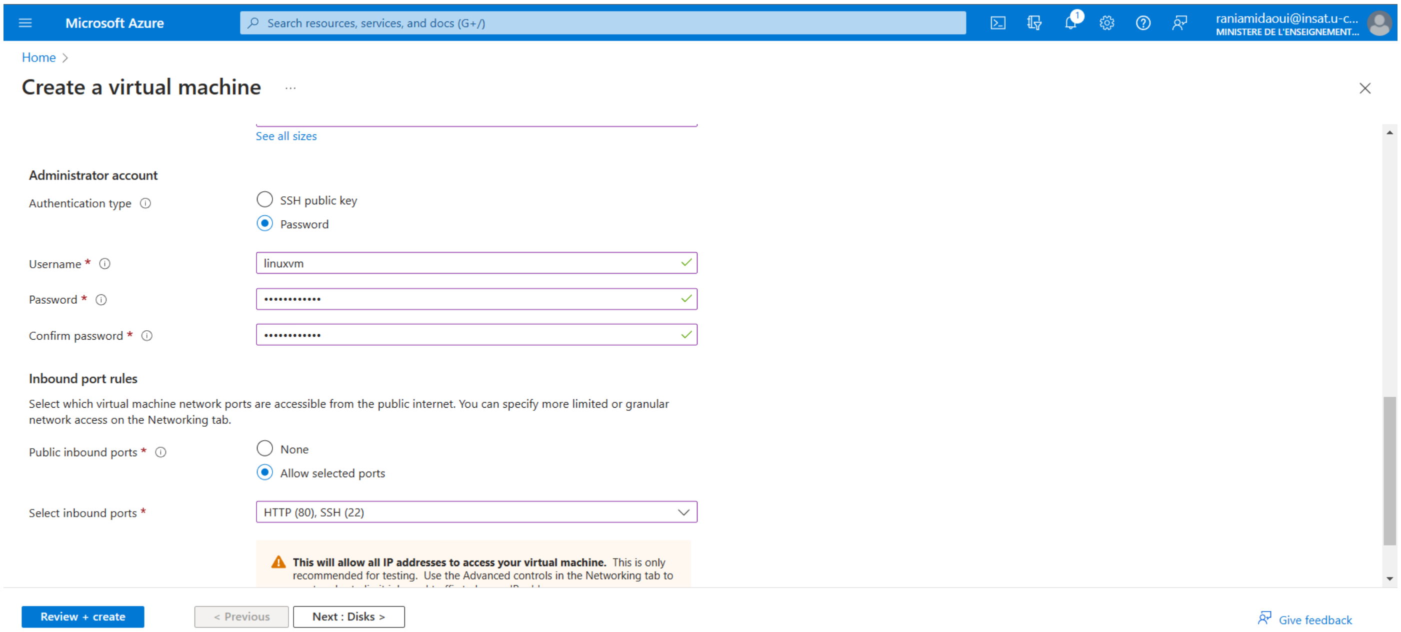


It works perfectly!

11- We disassociate the public IP address of loadvm1 and create a Linux virtual machine:







12- Since it's a Ubuntu server and we don't have a Desktop anyways, we will be using WSL to connect to the VM instead of PuTTY.

```
linuxvm@linuxvm: ~
└─$ ^C

┌──(midaoui㉿midaoui)-[~]
└─$ ssh linuxvm@20.244.0.133
linuxvm@20.244.0.133's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1035-azure x86_64)

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

  System information as of Wed Mar 29 17:06:19 UTC 2023

  System load:  0.05              Processes:             121
  Usage of /:   5.2% of 28.89GB   Users logged in:       0
  Memory usage: 8%                IPv4 address for eth0: 10.1.0.4
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

linuxvm@linuxvm:~$
```

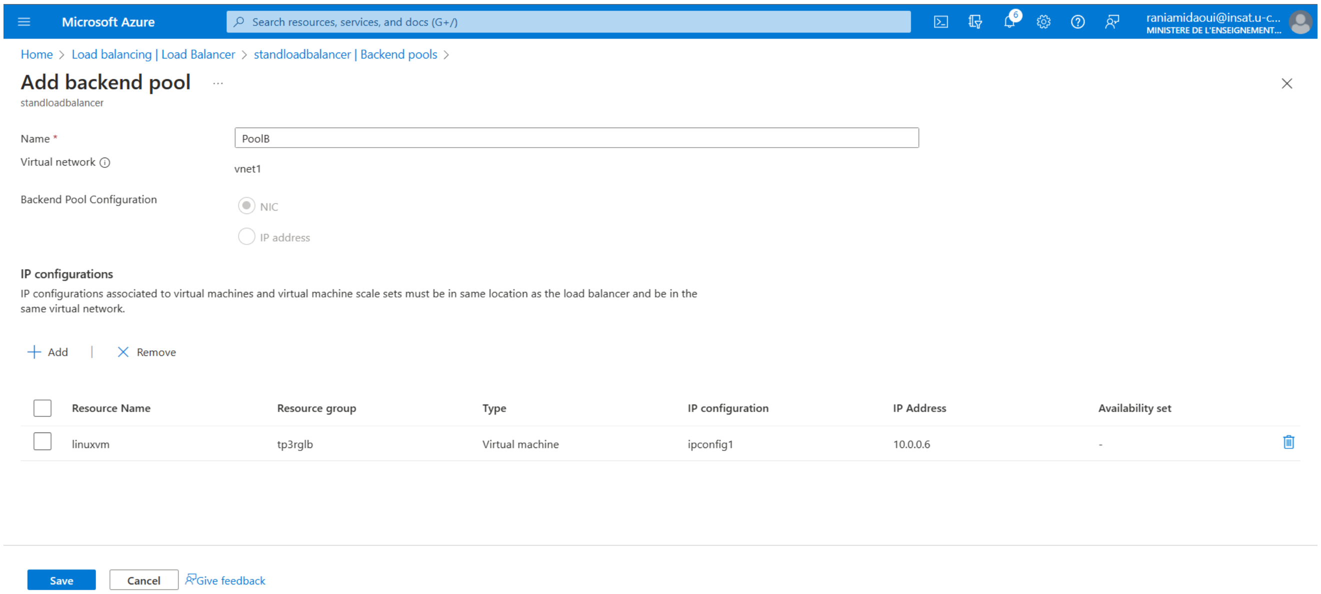
We then install Nginx and verify the installation:

```
linuxvm@linuxvm:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://azure.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://azure.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://azure.archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:6 http://azure.archive.ubuntu.com/ubuntu focal/universe Translation-en [5124 kB]
Get:7 http://azure.archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:8 http://azure.archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:9 http://azure.archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:10 http://azure.archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:11 http://azure.archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2463 kB]
Get:12 http://azure.archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [16.4 kB]
```

```
linuxvm@linuxvm:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
  libnginx-mod-mail libnginx-mod-stream libtiff5 libwebp6 libxpm4 nginx-common nginx-core
Suggested packages:
  libgd-tools fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter
```

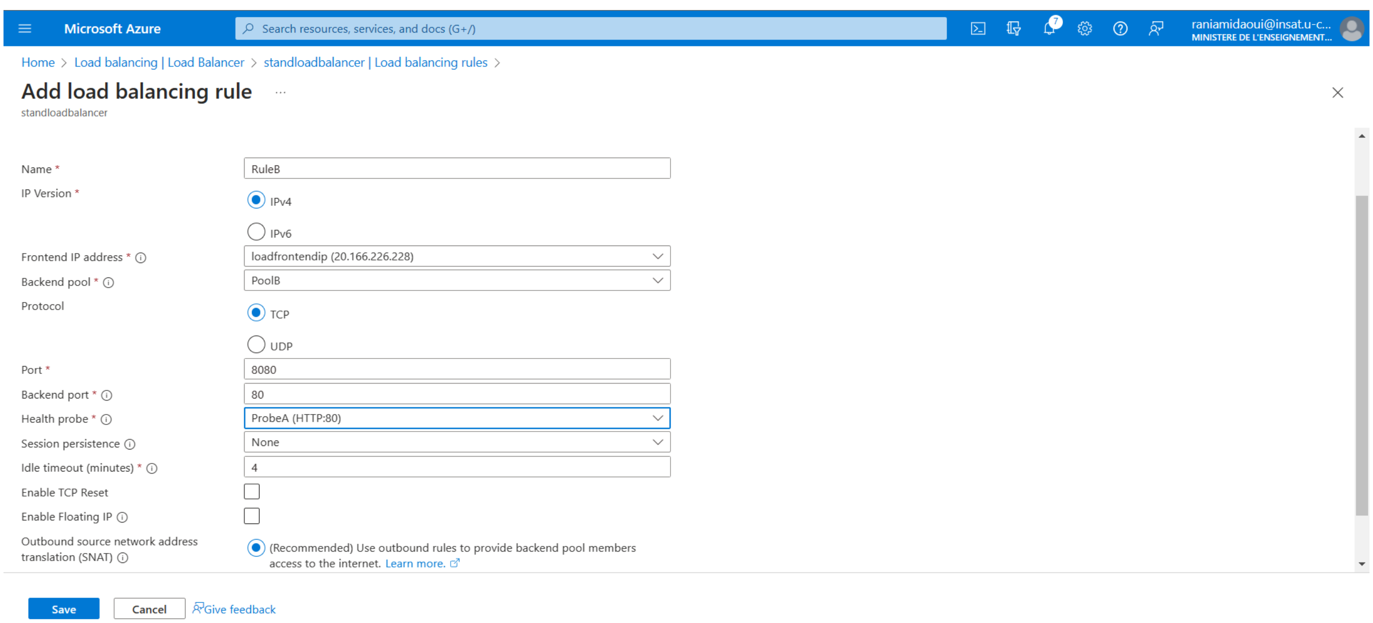
```
linuxvm@linuxvm:~$ ls /etc/nginx
conf.d        fastcgi_params  koi-win     modules-available  nginx.conf    scgi_params      sites-enabled  uwsgi_params
fastcgi.conf  koi-utf         mime.types  modules-enabled    proxy_params  sites-available  snippets       win-utf
```

13- We create a new backend pool and add the linux vm to that pool:

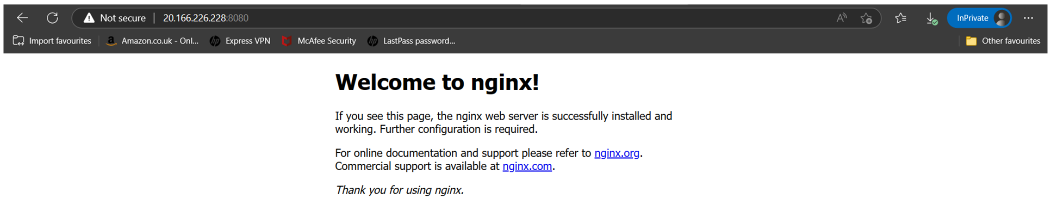


14 - We create a new load balancing rule:

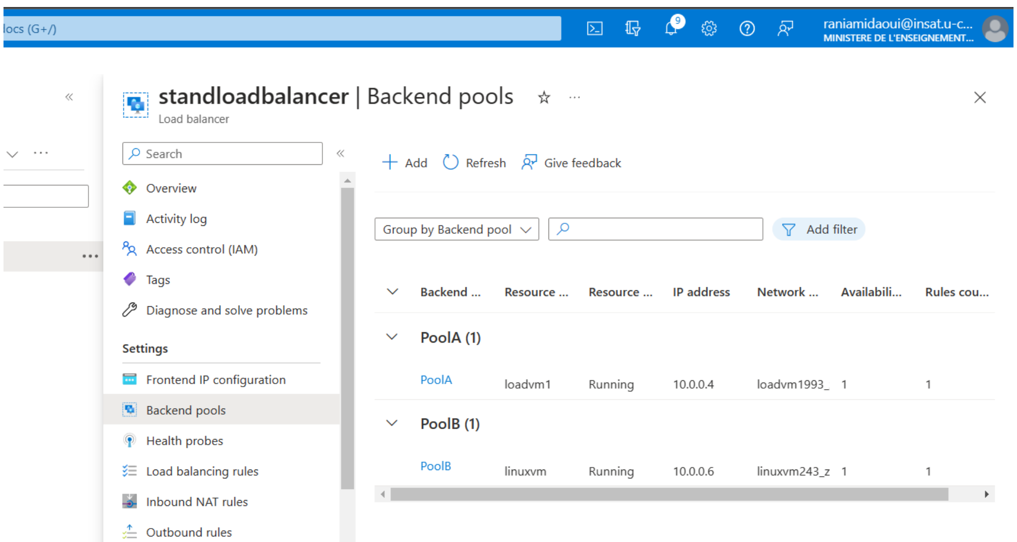
(We removed the resource group and made a new one so the ip address of the load balancer changed.)



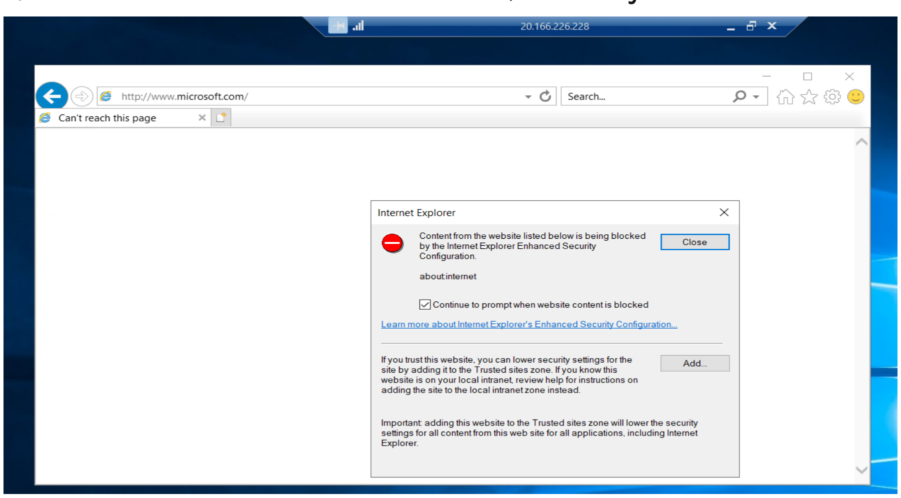
15- We try the public address of the load balancer using the port 8080, we get redirected to the Ubuntu server:



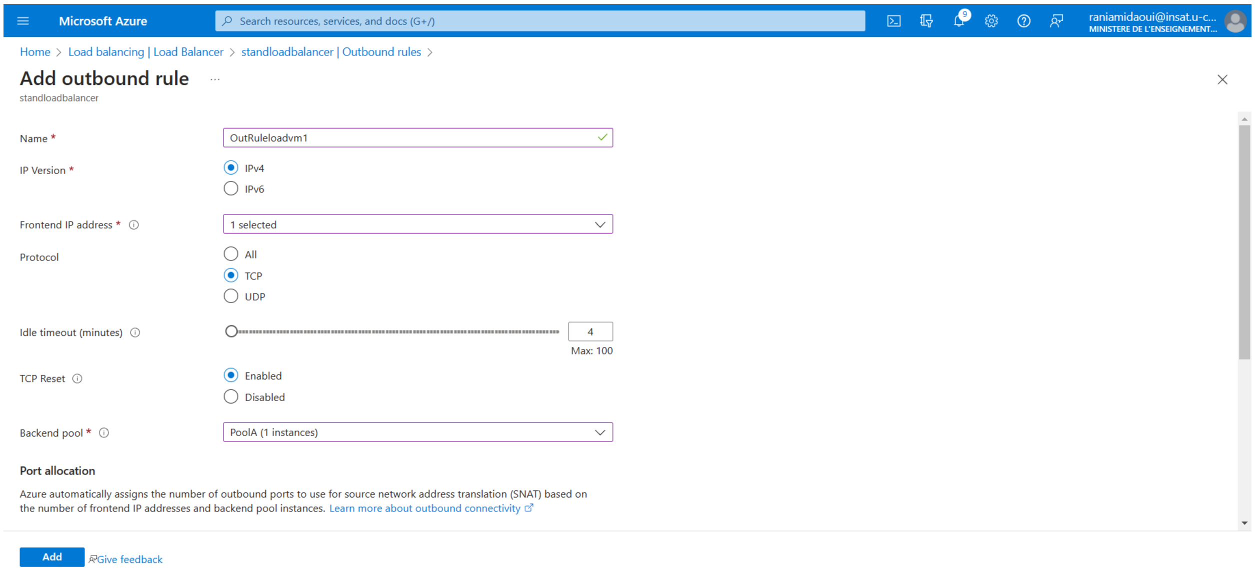
16- We remove the virtual machine loadvm2 from the PoolA:

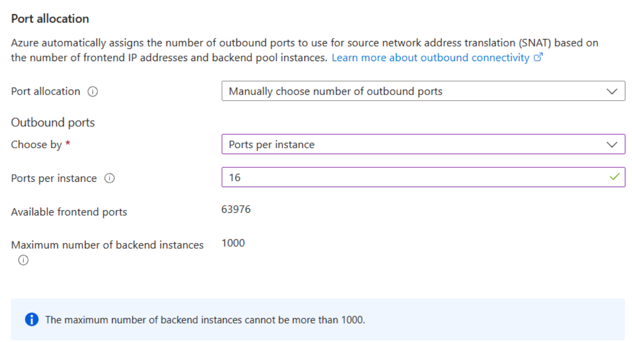


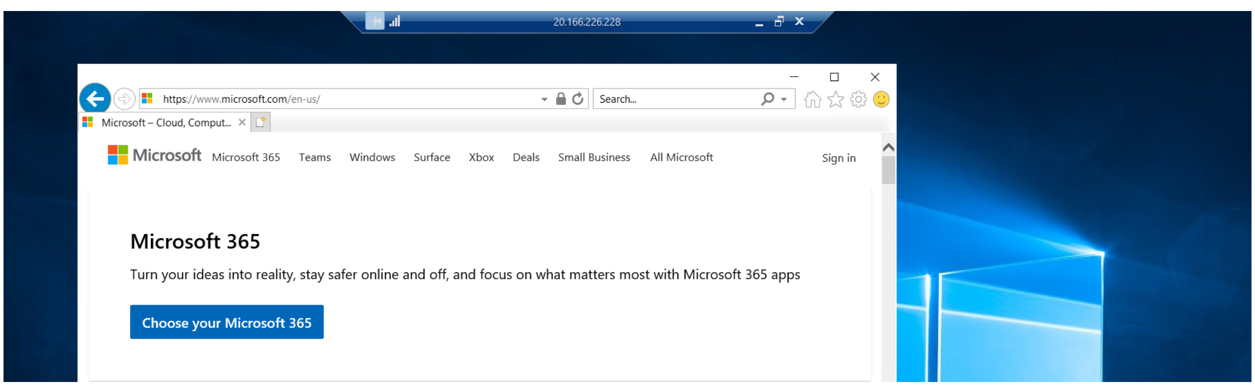
17- We connect to loadvm1 from a RDP client, and we try to access ww.microsoft.com:



We configure the outbound rules:

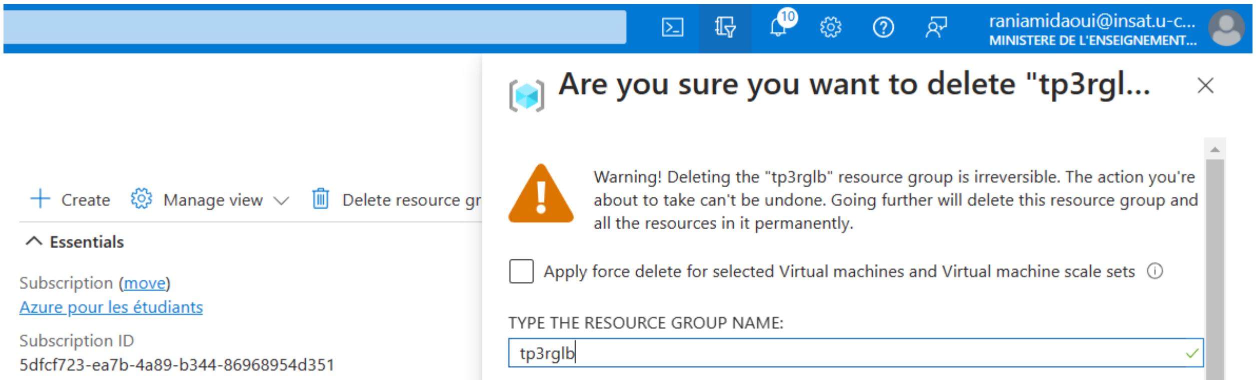






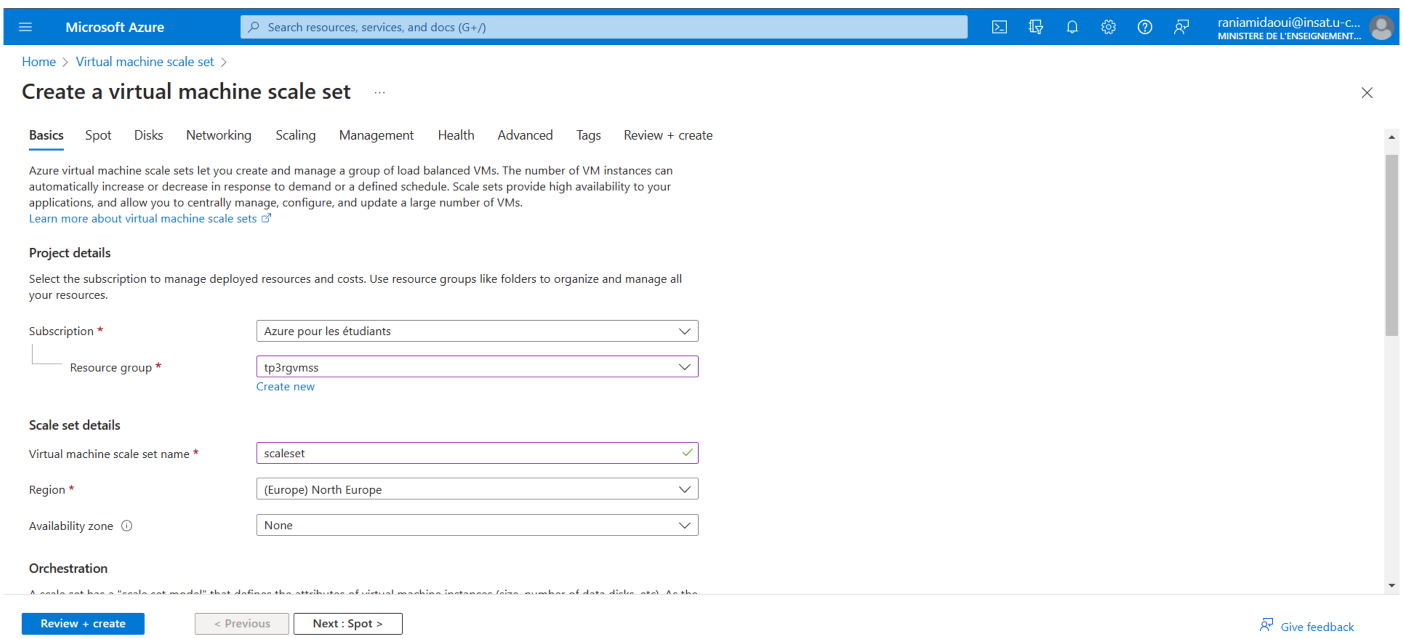
Rule successfully created!

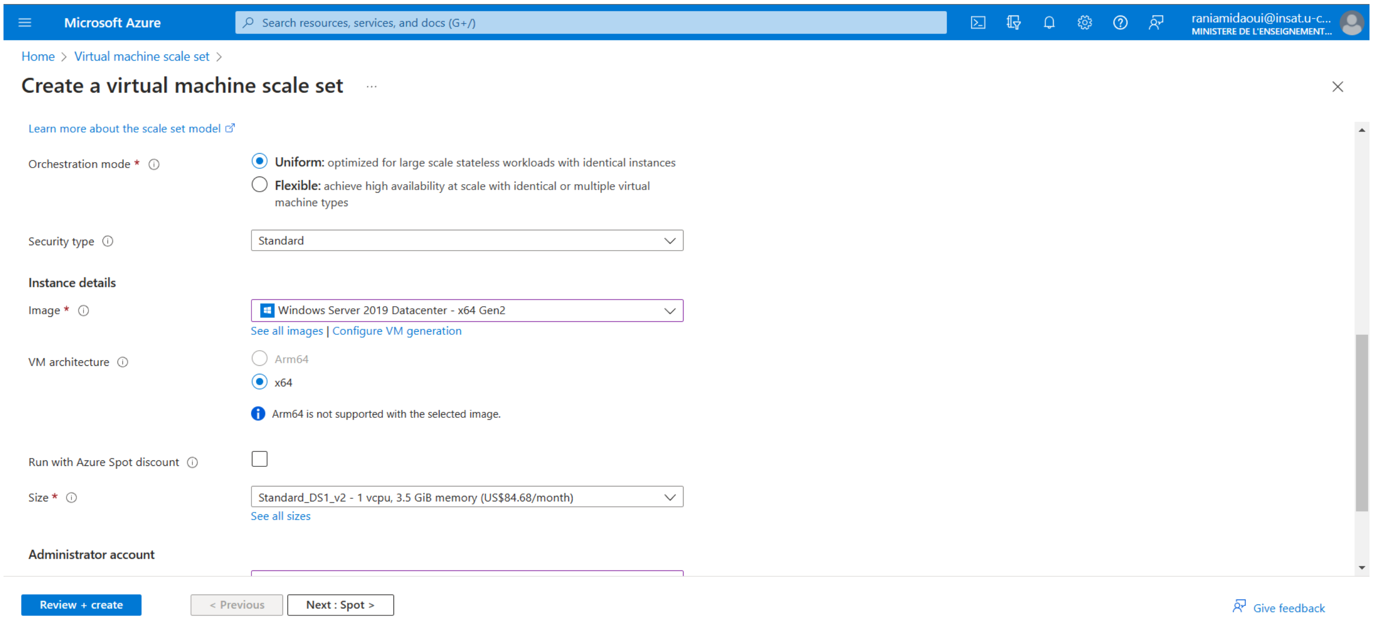
18- We delete the resource group:

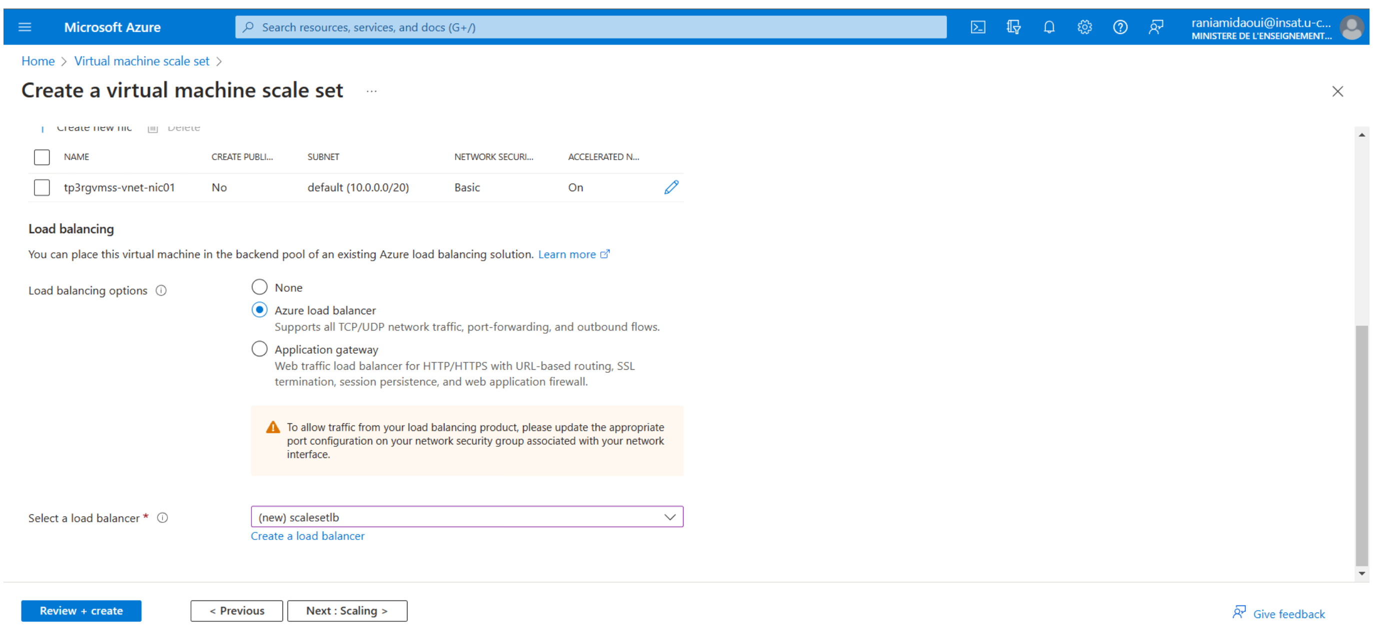


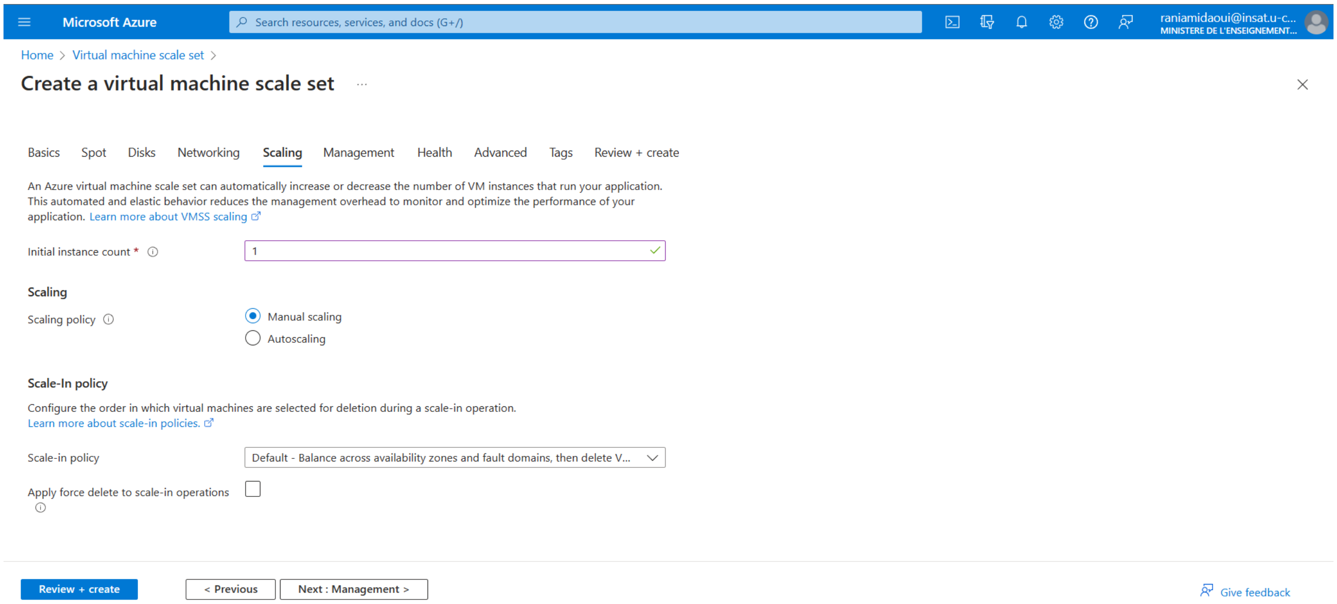
Task 2: standard load balancer and VMSS

1- We create a virtual machine scale set and configure its load balancing:

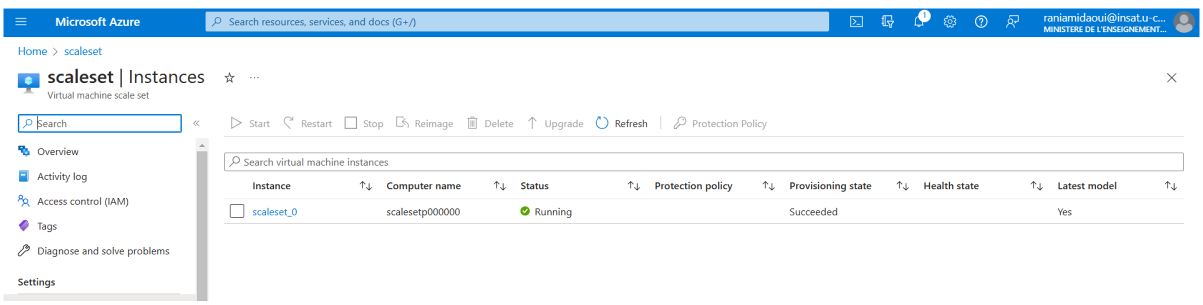


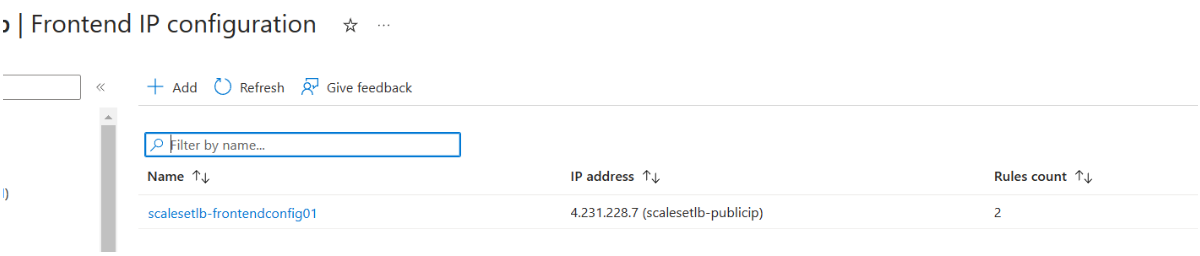

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Virtual machine scale set >
Create a virtual machine scale set
Learn more about the scale set model
Orchestration mode *
Uniform: optimized for large scale stateless workloads with identical instances
Flexible: achieve high availability at scale with identical or multiple virtual machine types
Security type
Standard
Instance details
Image *
Windows Server 2019 Datacenter - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
Size *
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (US$84.68/month)
See all sizes
Administrator account
Review + create
< Previous
Next : Spot >
Give feedback

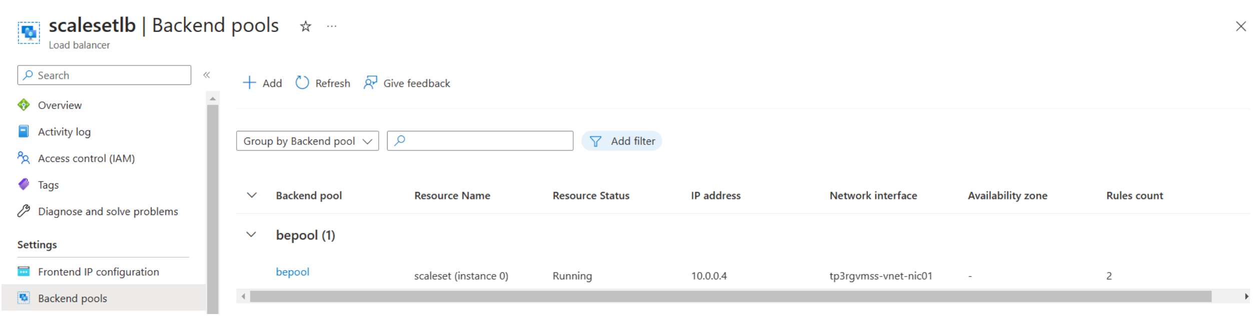

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Virtual machine scale set >
Create a virtual machine scale set
NAME
CREATE PUBLI...
SUBNET
NETWORK SECURI...
ACCELERATED N...
tp3rgvmss-vnet-nic01
No
default (10.0.0.0/20)
Basic
On
Load balancing
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. Learn more
Load balancing options
None
Azure load balancer
Supports all TCP/UDP network traffic, port-forwarding, and outbound flows.
Application gateway
Web traffic load balancer for HTTP/HTTPS with URL-based routing, SSL termination, session persistence, and web application firewall.
To allow traffic from your load balancing product, please update the appropriate port configuration on your network security group associated with your network interface.
Select a load balancer *
(new) scalesetlb
Create a load balancer
Review + create
< Previous
Next : Scaling >
Give feedback



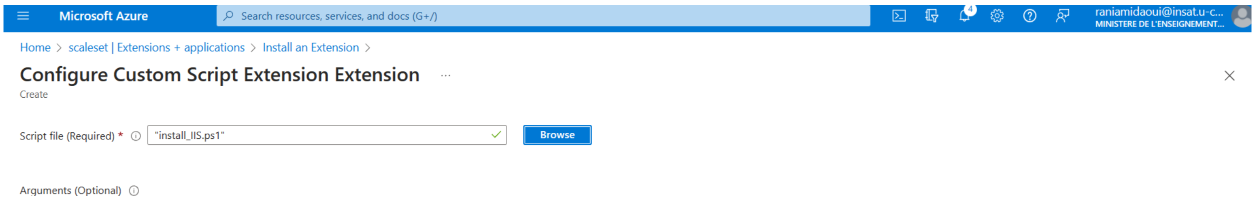
2- All the resources have been created successfully:

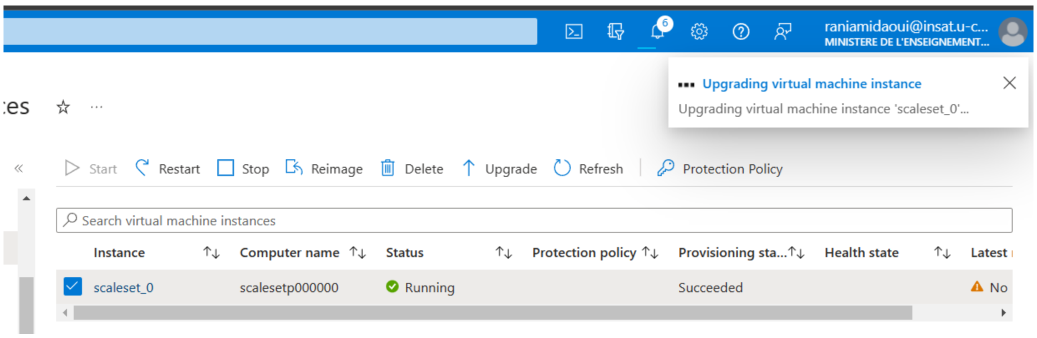




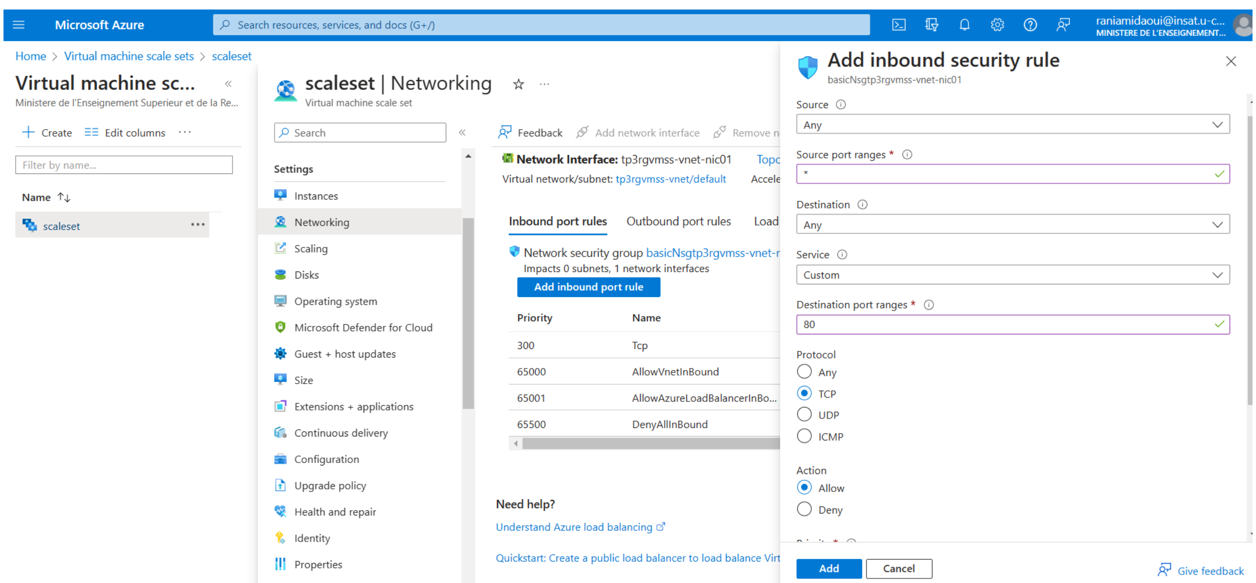


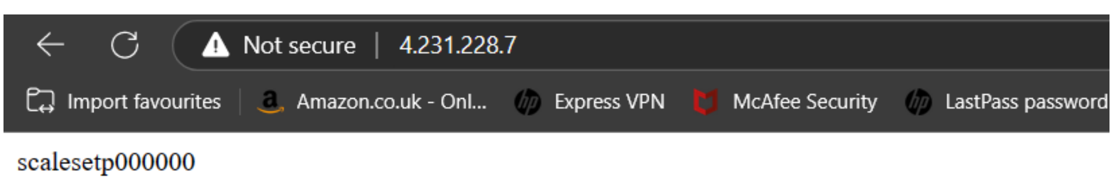
3- We add a Custom Script Extension to install IIS server and use it to upgrade the scaleset:



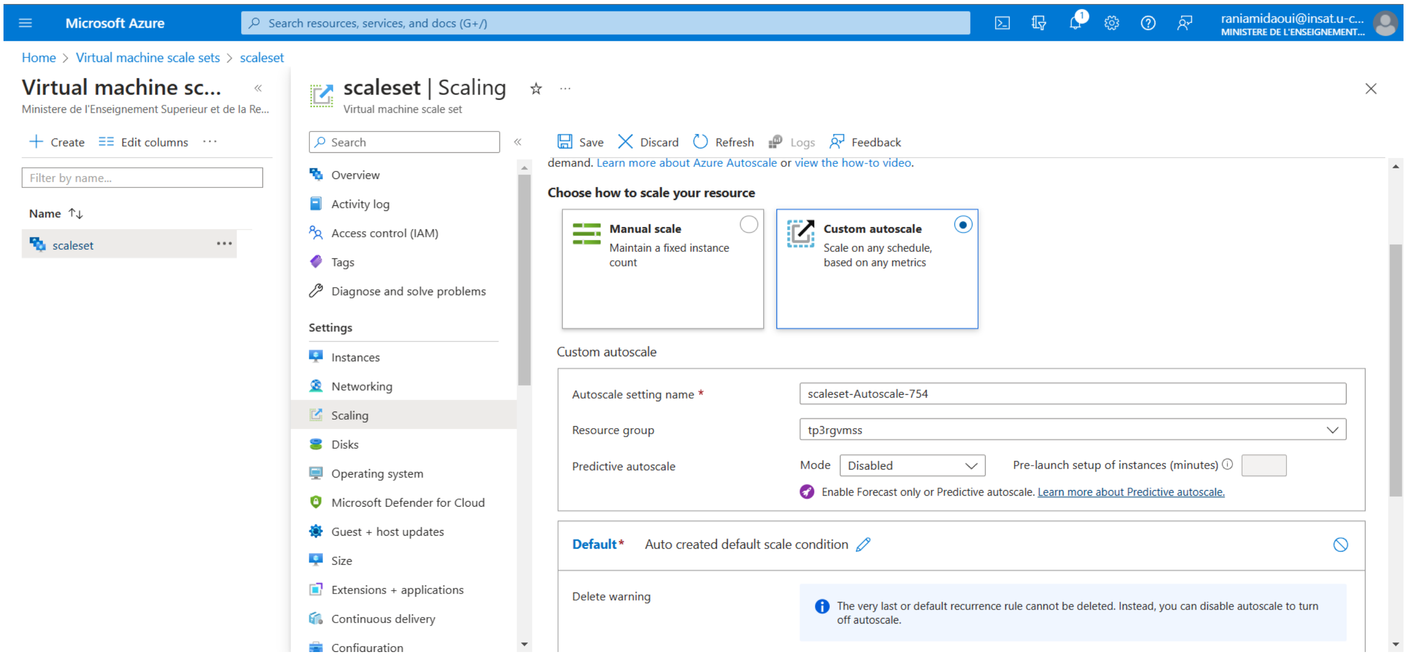


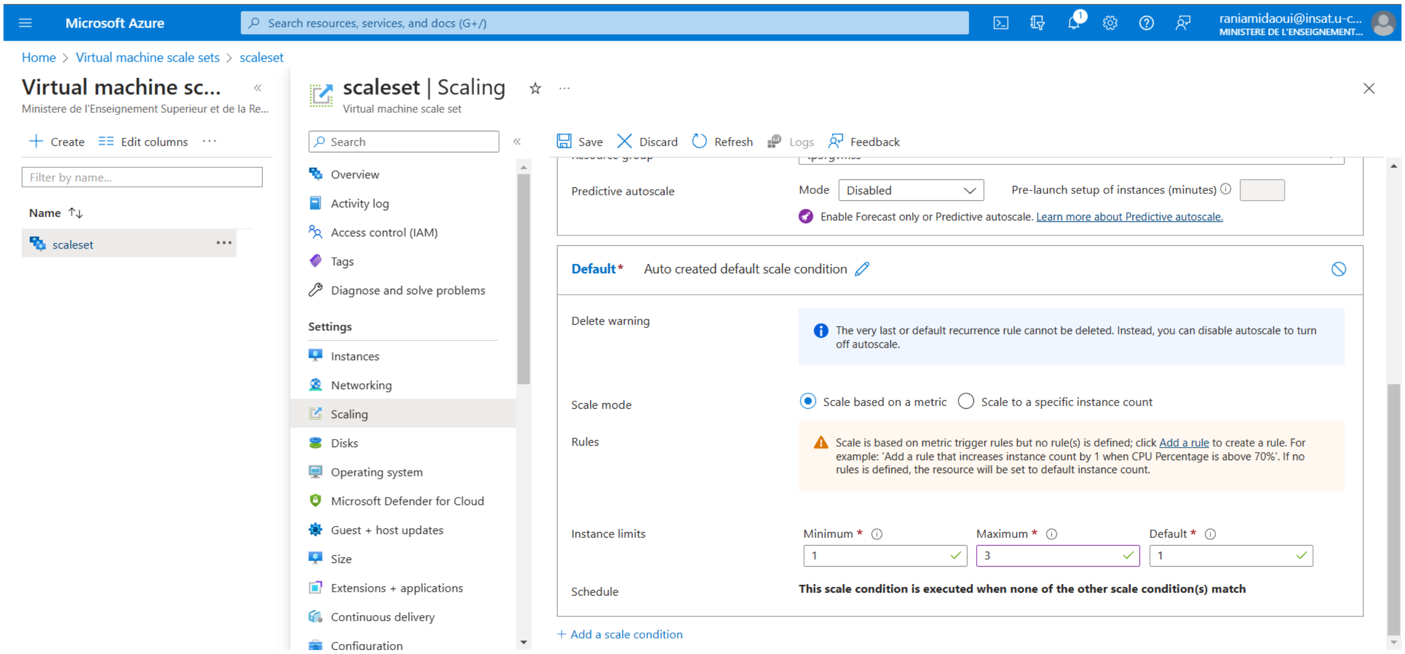
4 - Adding inbound security rule to allow traffic on port 80 and testing the load balancer:

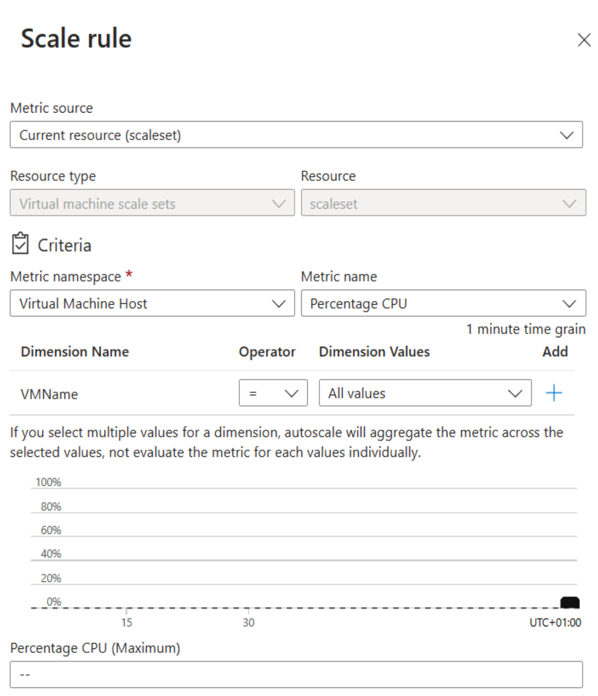


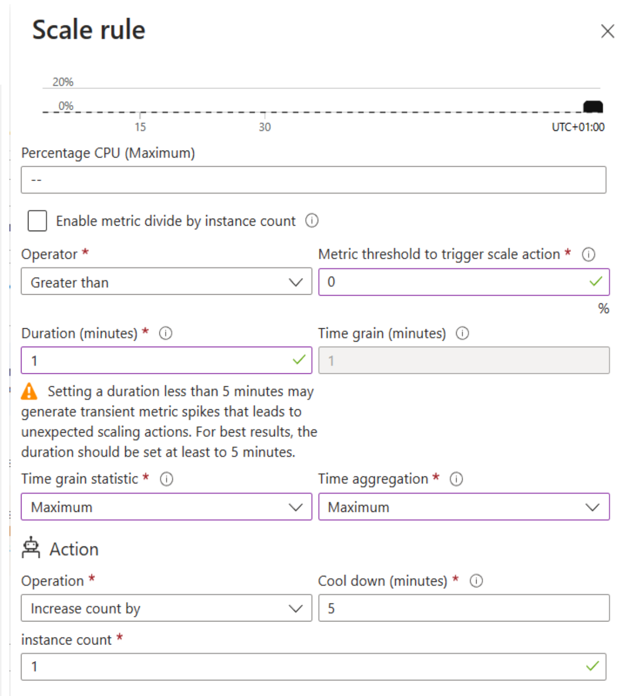


5- We set up custom autoscale:

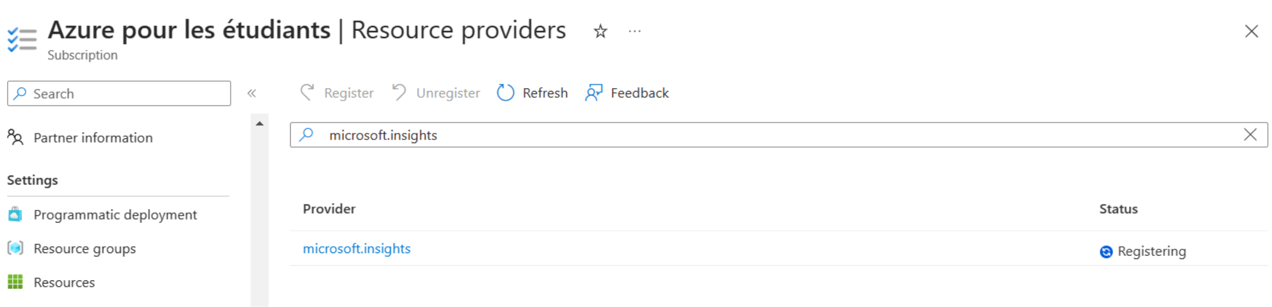


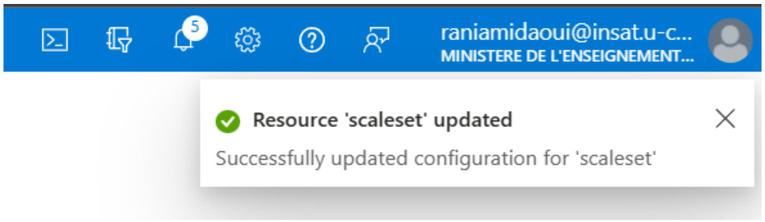




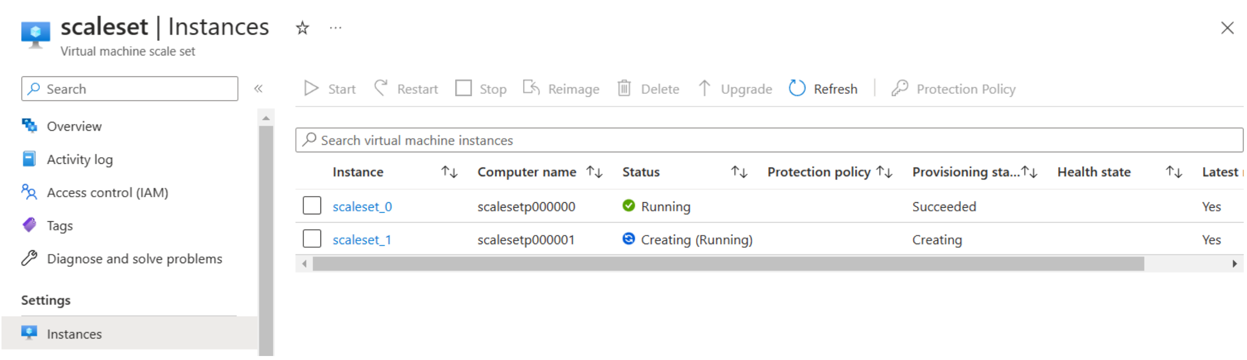


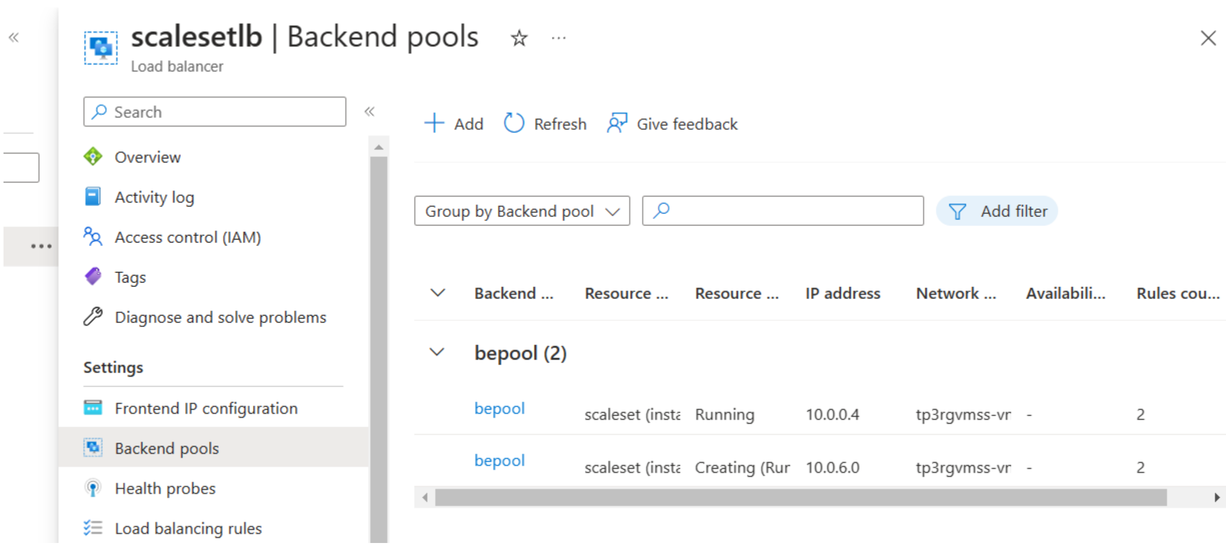
6- To save the auto-scaling we had to register microsoft.insights in our subscription:

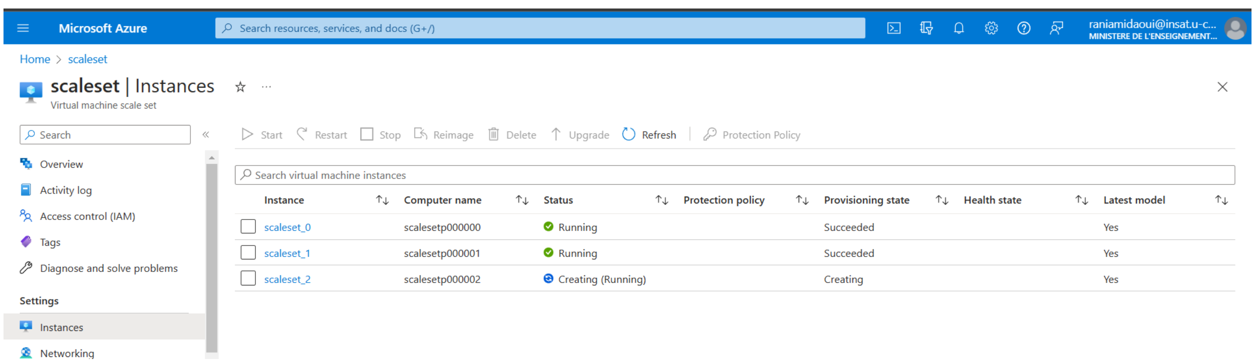


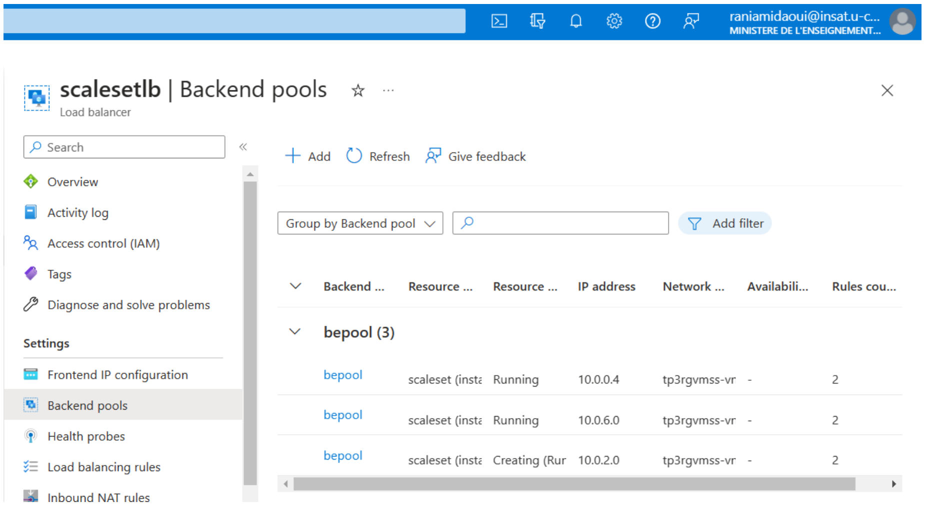


All good, the autoscaling is working perfectly:

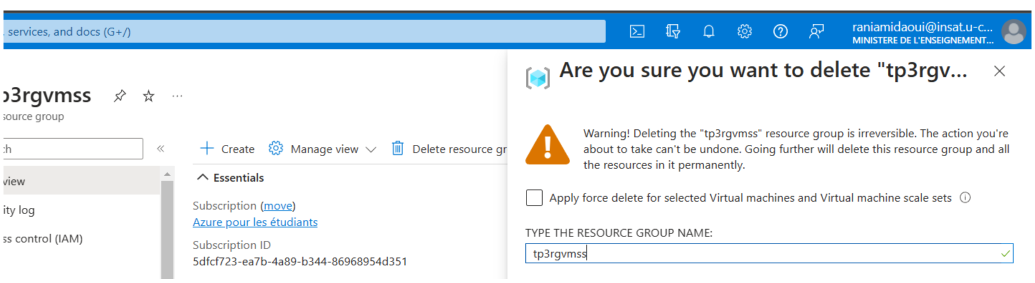








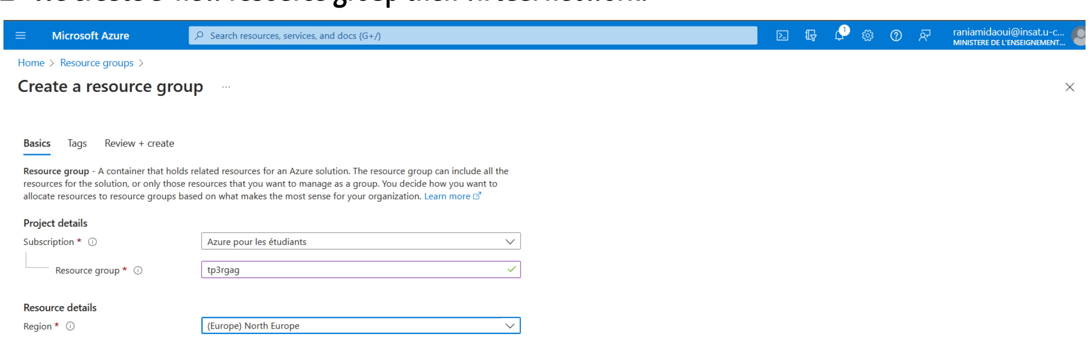
7- We delete the resource group:

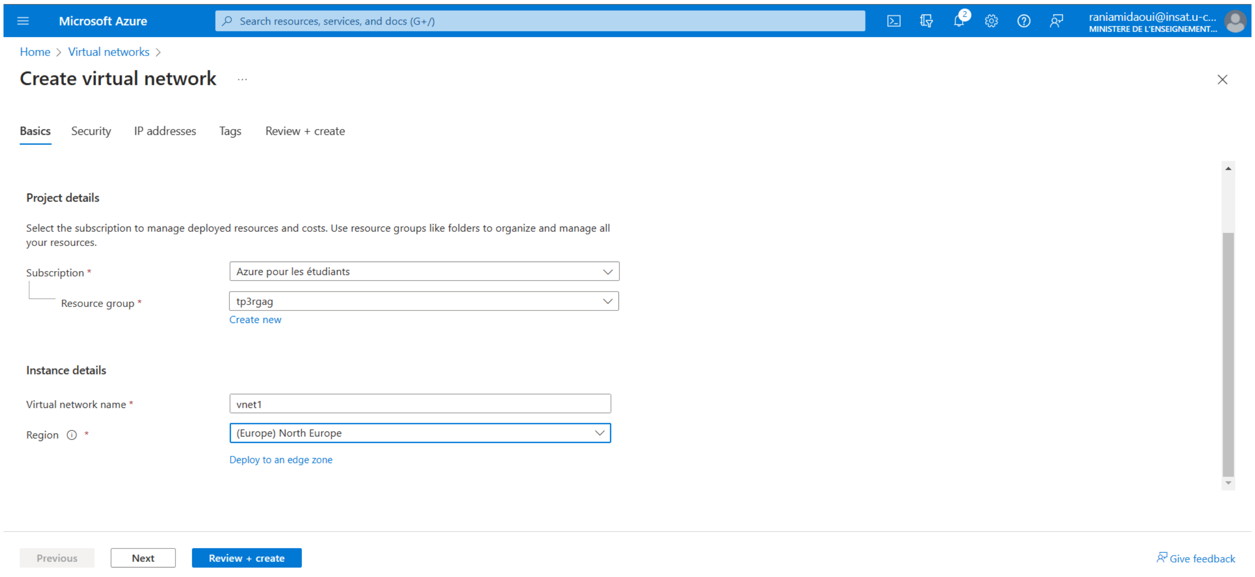


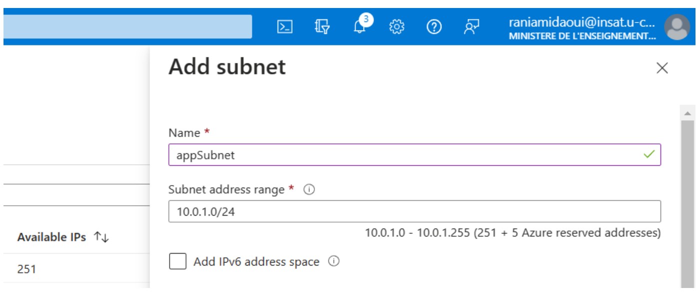
Task 3: Azure Application Gateway

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

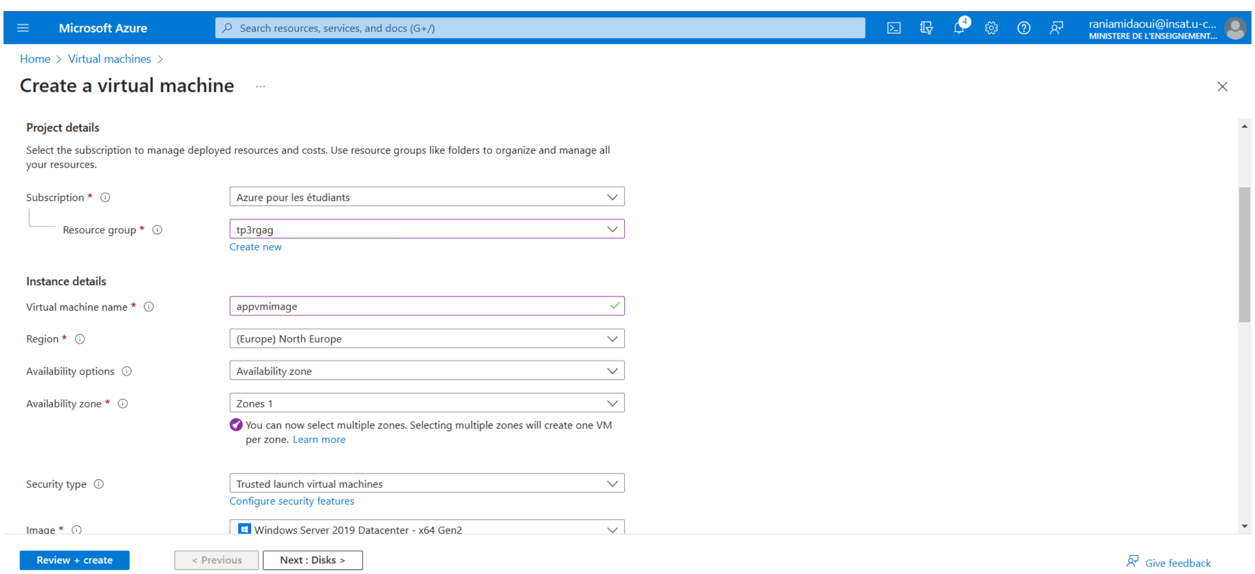
1- We create a new resource group then virtual network:

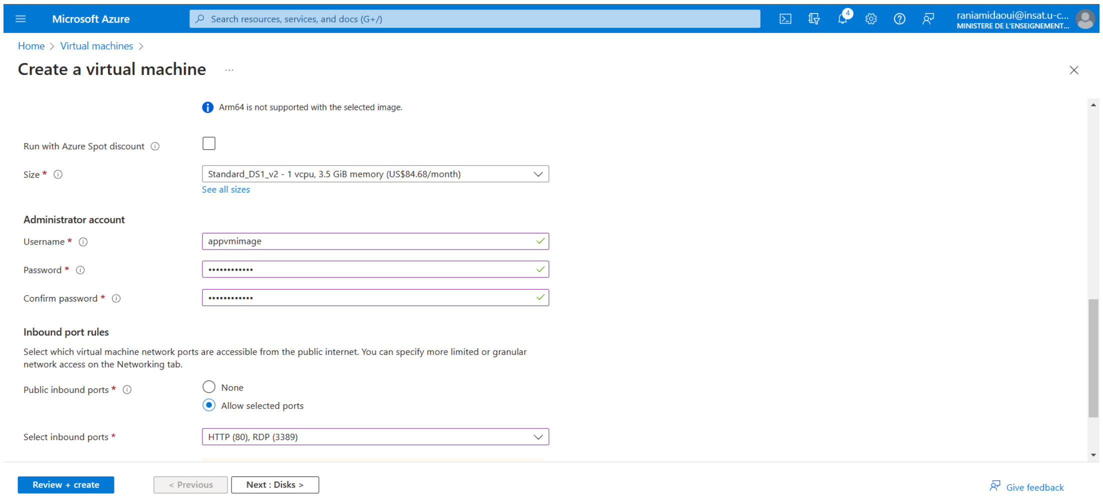


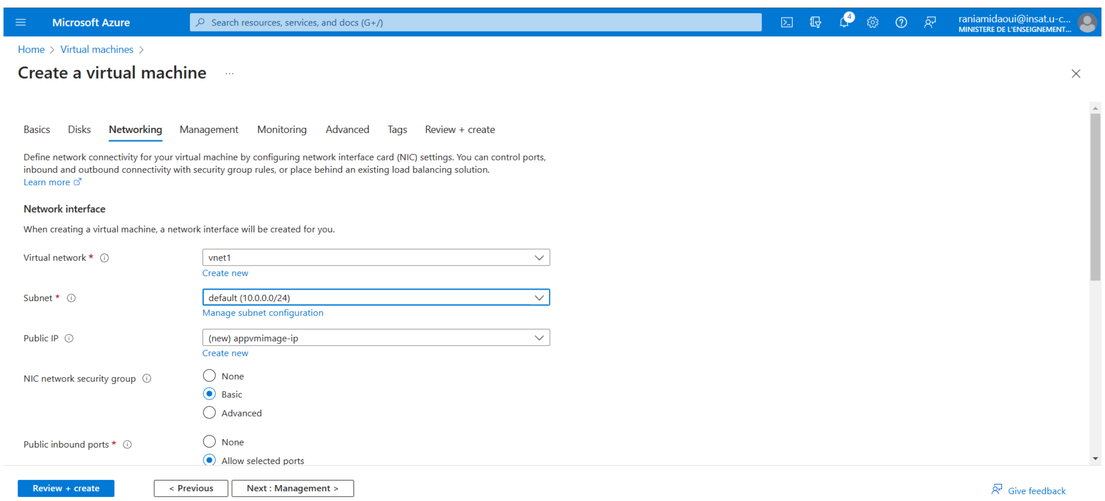


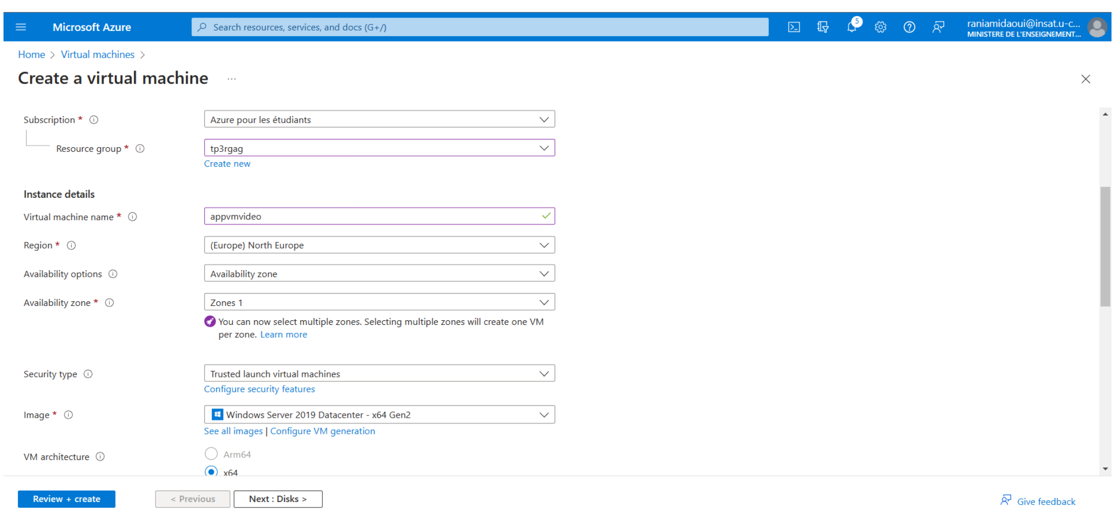


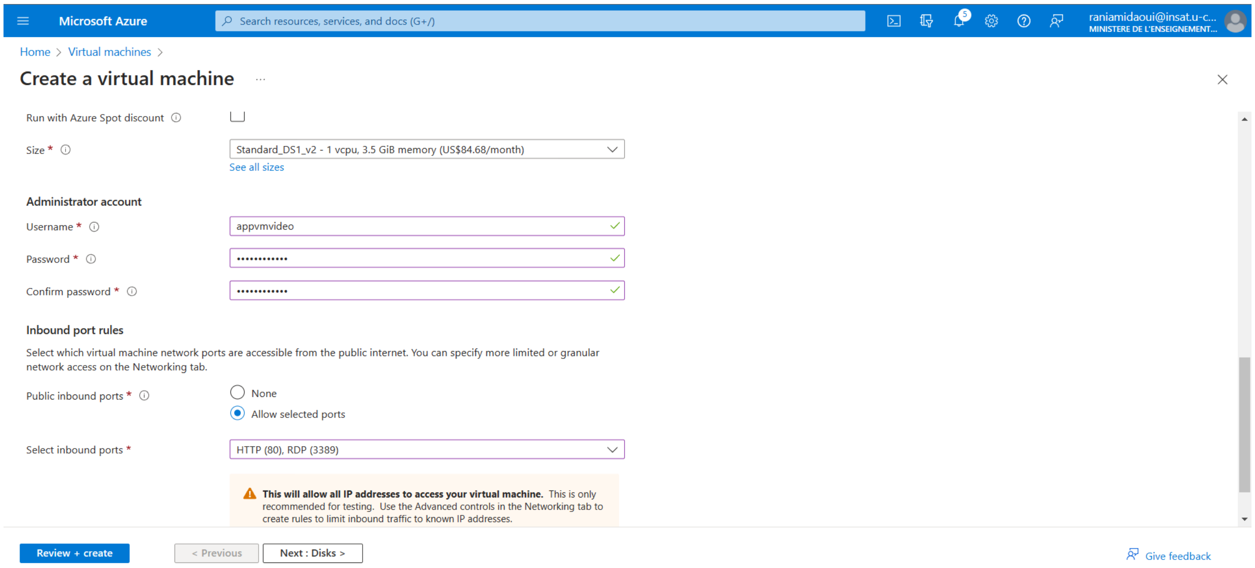
2- We create two virtual machines appvmimage and appvmvideo as a part of the default subnet:

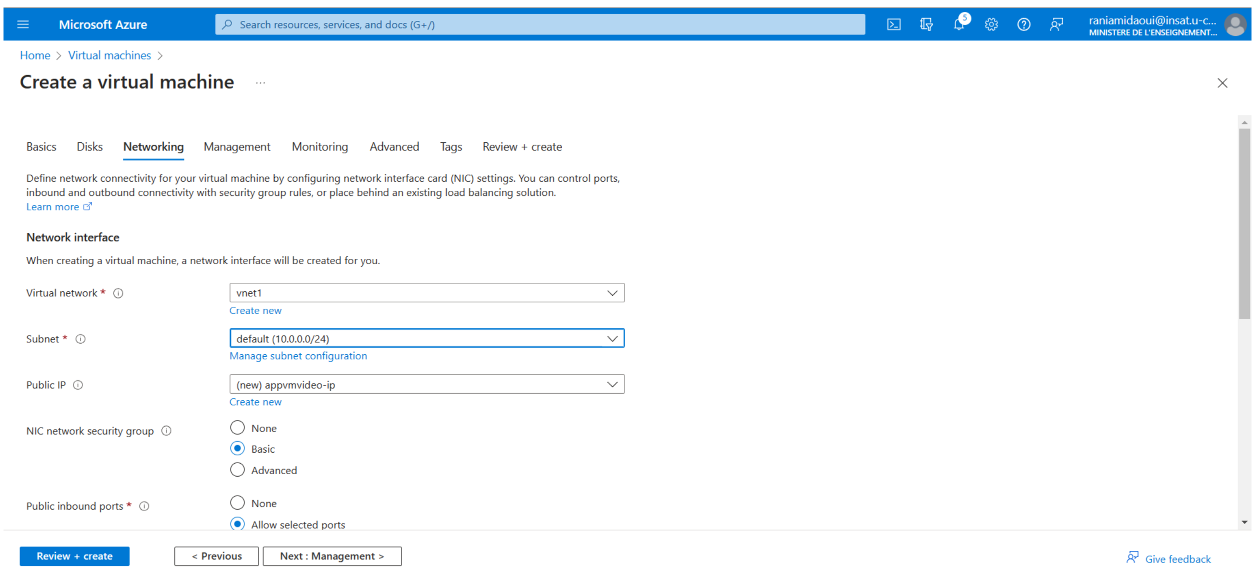



Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Virtual machines >
Create a virtual machine
Arm64 is not supported with the selected image.
Run with Azure Spot discount
Size *
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (US$84.68/month)
See all sizes
Administrator account
Username *
appvmimage
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
Select inbound ports *
HTTP (80), RDP (3389)
Review + create
< Previous
Next : Disks >
Give feedback

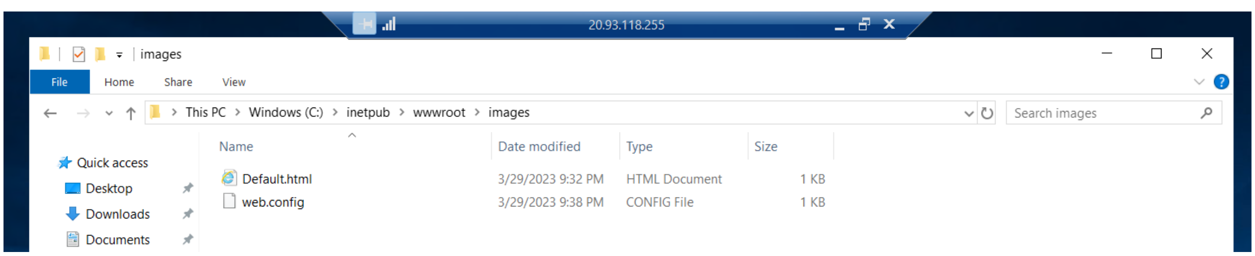

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Virtual machines >
Create a virtual machine
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
vnet1
Create new
Subnet *
default (10.0.0.0/24)
Manage subnet configuration
Public IP
(new) appvmimage-ip
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
Allow selected ports
Review + create
< Previous
Next : Management >
Give feedback

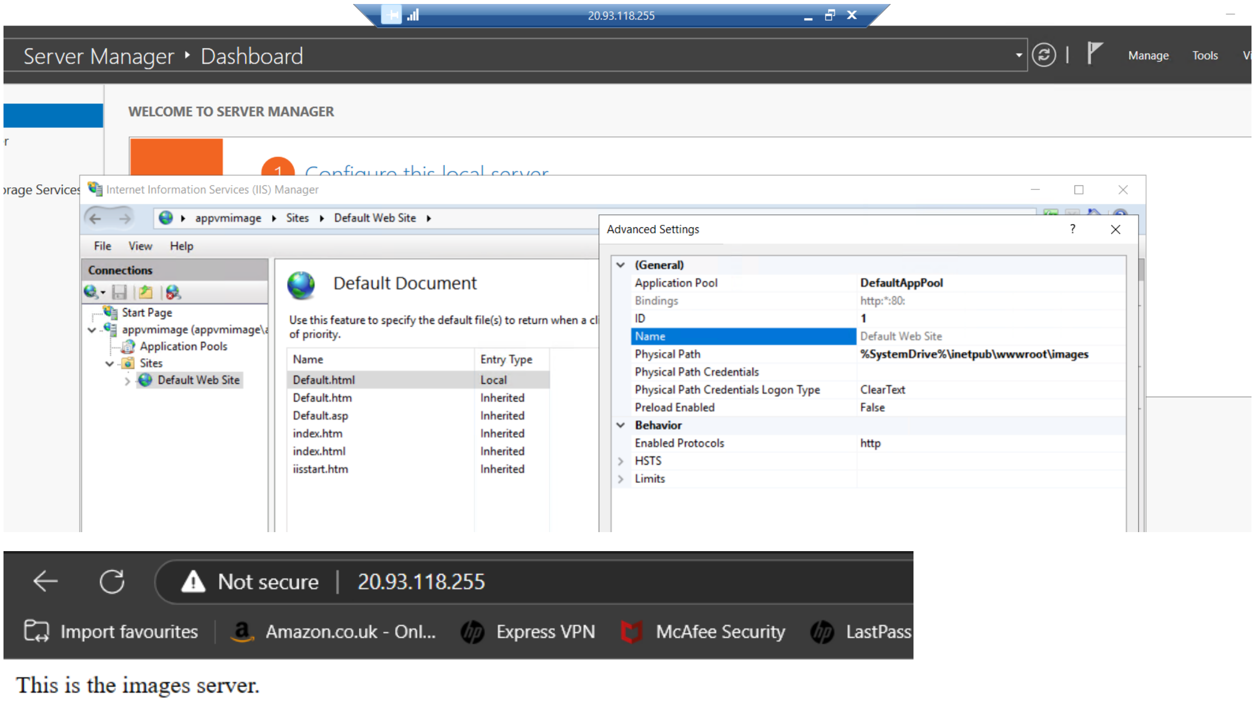

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Virtual machines >
Create a virtual machine
Subscription *
Azure pour les étudiants
Resource group *
tp3rgag
Create new
Instance details
Virtual machine name *
appvmvideo
Region *
(Europe) North Europe
Availability options
Availability zone
Availability zone *
Zones 1
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
Security type
Trusted launch virtual machines
Configure security features
Image *
Windows Server 2019 Datacenter - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Review + create
< Previous
Next : Disks >
Give feedback



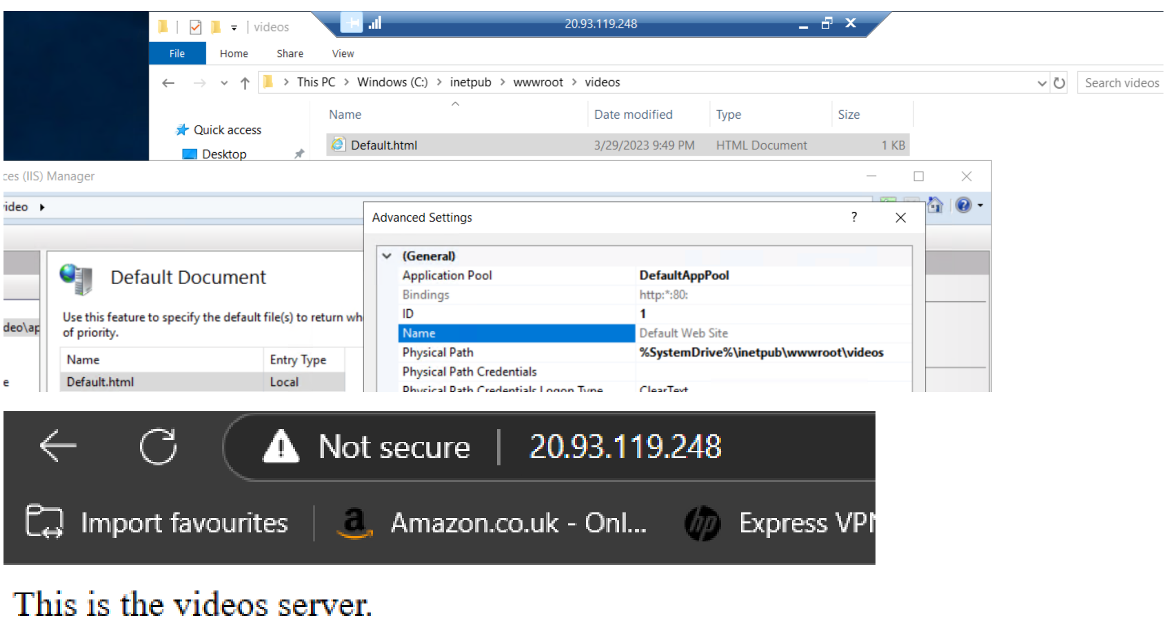


1- We install IIS server role and change the default website page of the image's server:

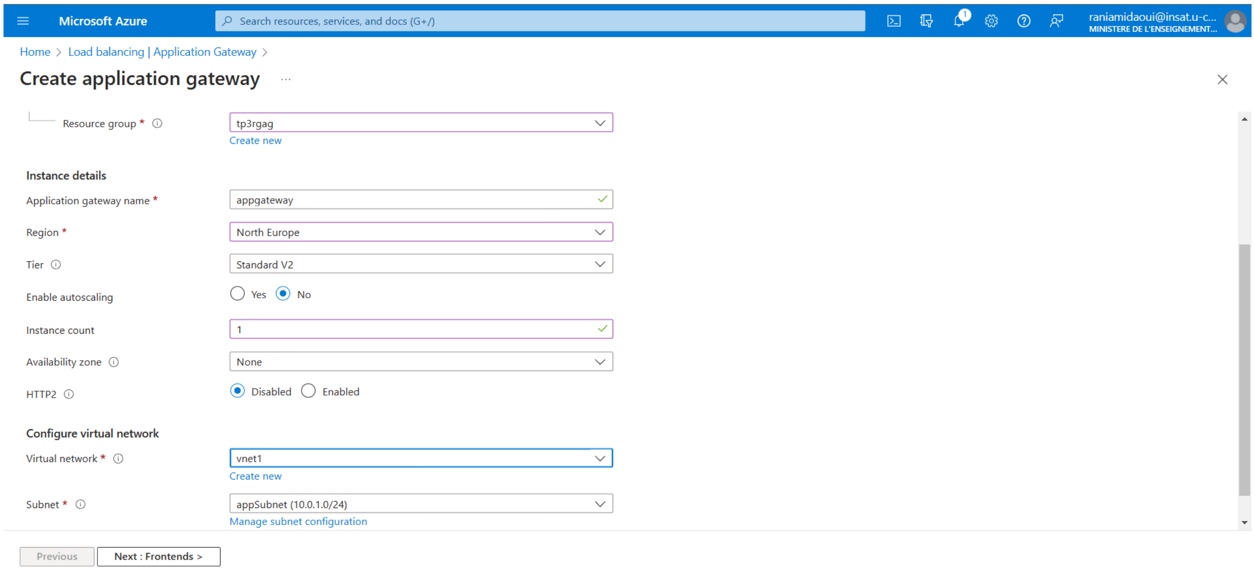


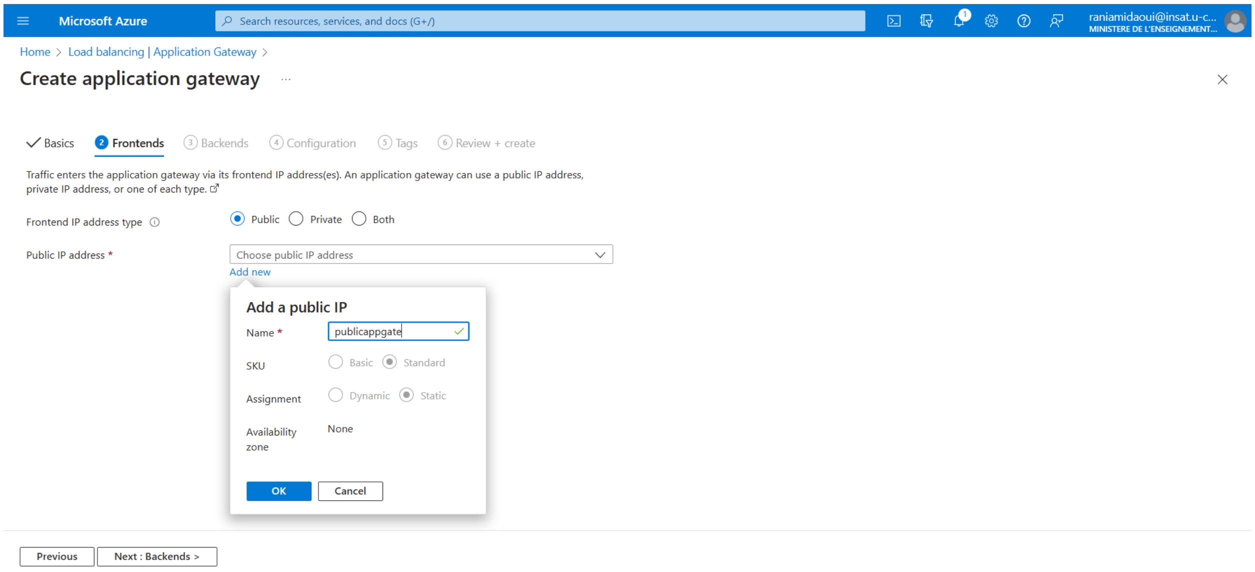


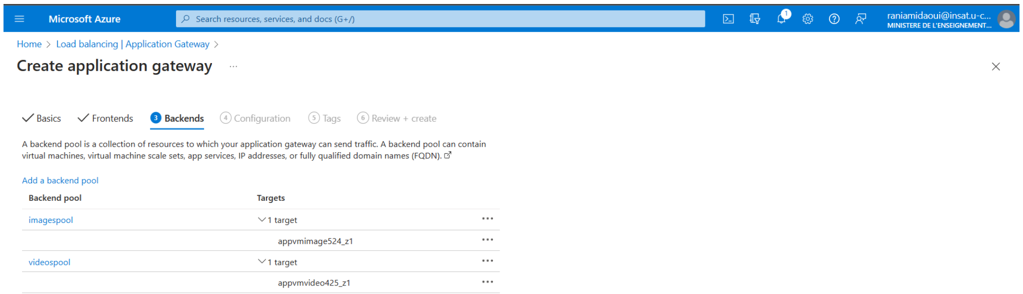
We apply the same steps to change the video's server default page:

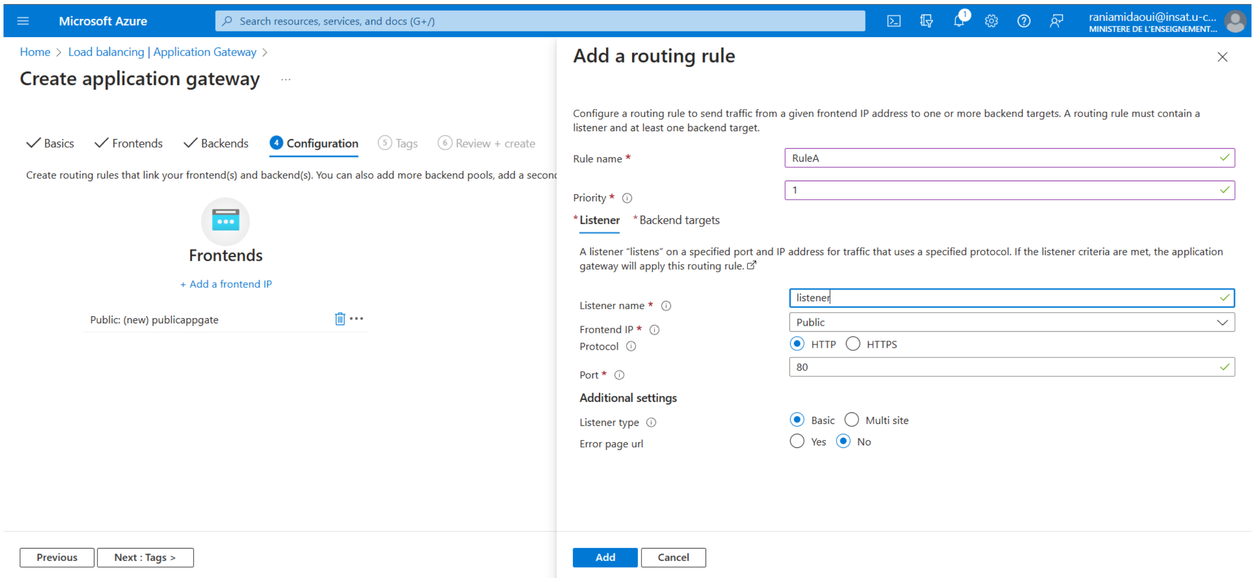


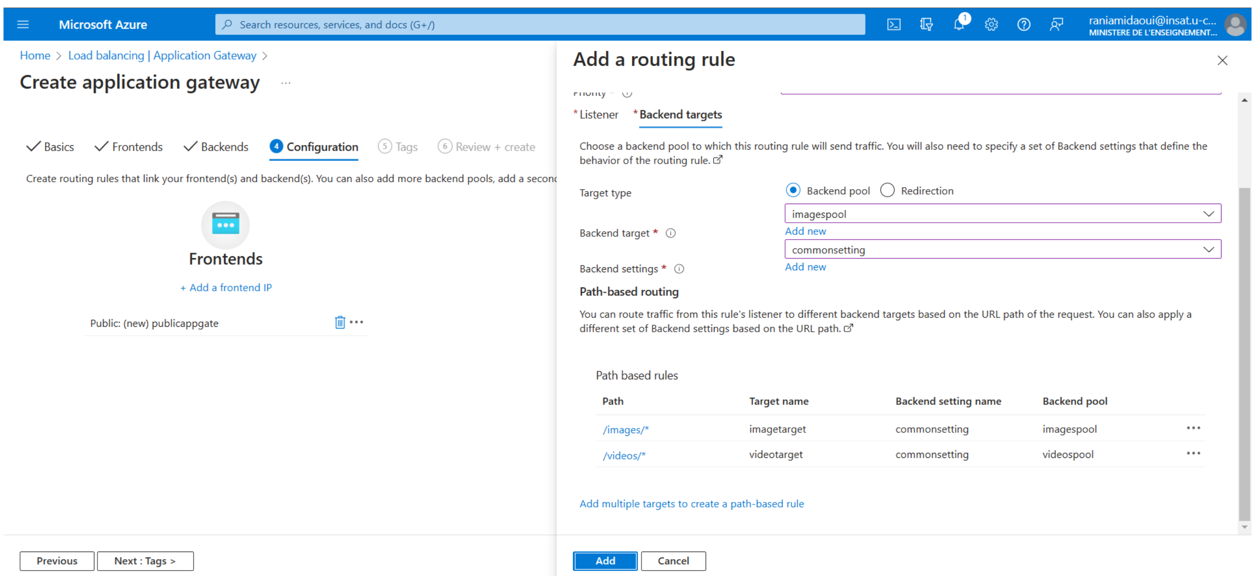
2- We create an Application gateway:

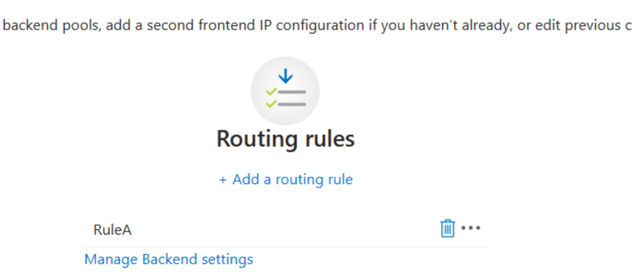




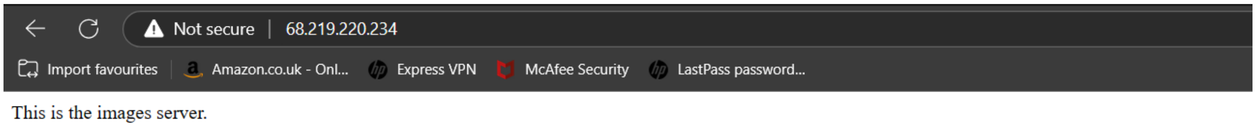


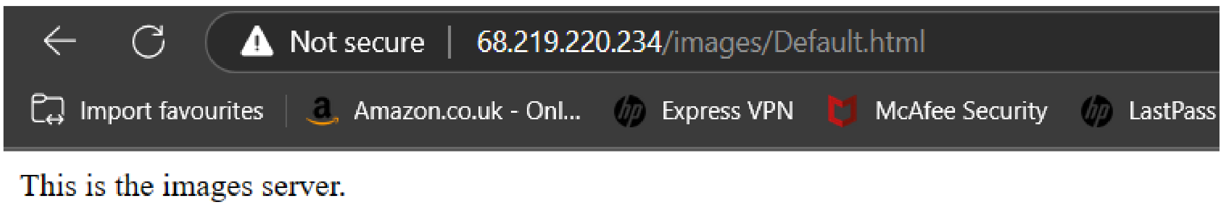

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Application Gateway >
Create application gateway
Basics
Frontends
Backends
Configuration
Tags
Review + create
Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second
Frontends
+ Add a frontend IP
Public: (new) publicappgate
Previous
Next : Tags >
Add a routing rule
Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.
Rule name *
RuleA
Priority *
1
*Listener
*Backend targets
A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.
Listener name *
listener
Frontend IP *
Public
Protocol
HTTP
HTTPS
Port *
80
Additional settings
Listener type
Basic
Multi site
Error page url
Yes
No
Add
Cancel

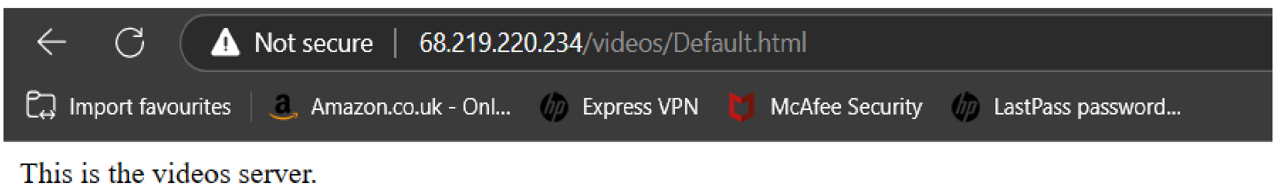

Microsoft Azure
Search resources, services, and docs (G+/)
raniamidaoui@insat.u-c...
MINISTERE DE L'ENSEIGNEMENT...
Home > Load balancing | Application Gateway >
Create application gateway
Basics
Frontends
Backends
Configuration
Tags
Review + create
Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second
Frontends
+ Add a frontend IP
Public: (new) publicappgate
Previous
Next : Tags >
Add a routing rule
*Listener
*Backend targets
Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of Backend settings that define the behavior of the routing rule.
Target type
Backend pool
Redirection
Backend target *
imagespool
Add new
Backend settings *
commonsetting
Add new
Path-based routing
You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of Backend settings based on the URL path.
Path based rules
Path
Target name
Backend setting name
Backend pool
/images/*
imagetarget
commonsetting
imagespool
/videos/*
videotarget
commonsetting
videospool
Add multiple targets to create a path-based rule
Add
Cancel


backend pools, add a second frontend IP configuration if you haven't already, or edit previous c
Routing rules
+ Add a routing rule
RuleA
Manage Backend settings

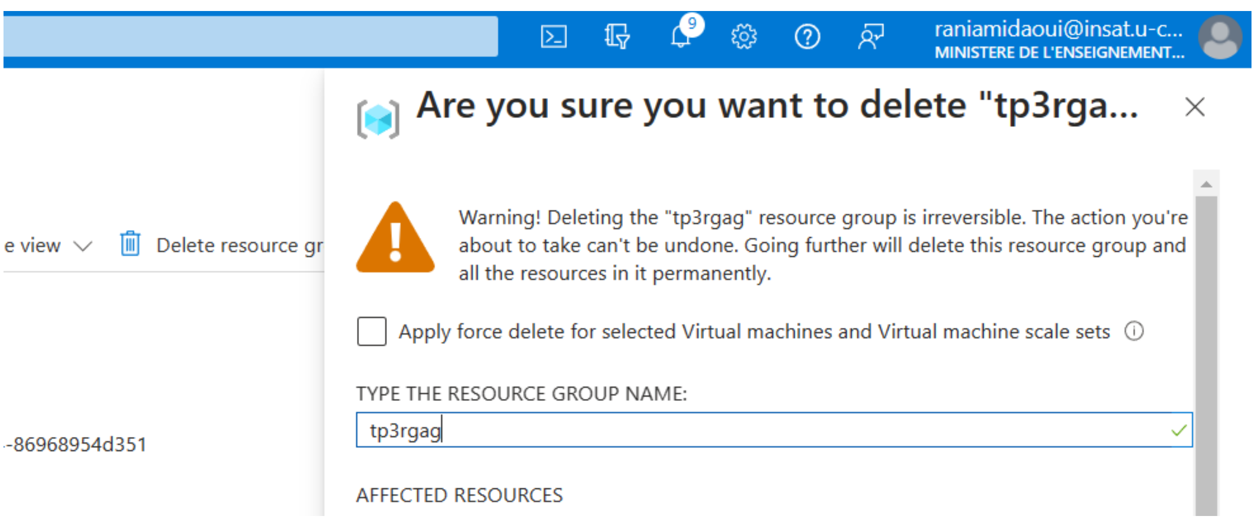
3- We test the Application Gateway:







4 - We remove the resource group:



Conclusion:

This TP showcases the various capabilities and benefits of Azure load balancers used with different implementations that we can encounter. It has enabled us to gain hands-on experience with Azure Load Balancers, which play a crucial role in ensuring high availability, scalability, and performance of applications in Microsoft Azure's cloud infrastructure.

An Azure Load Balancer is a critical component that distributes incoming network traffic across multiple servers or virtual machines, preventing any one server from becoming overwhelmed and causing a bottleneck.