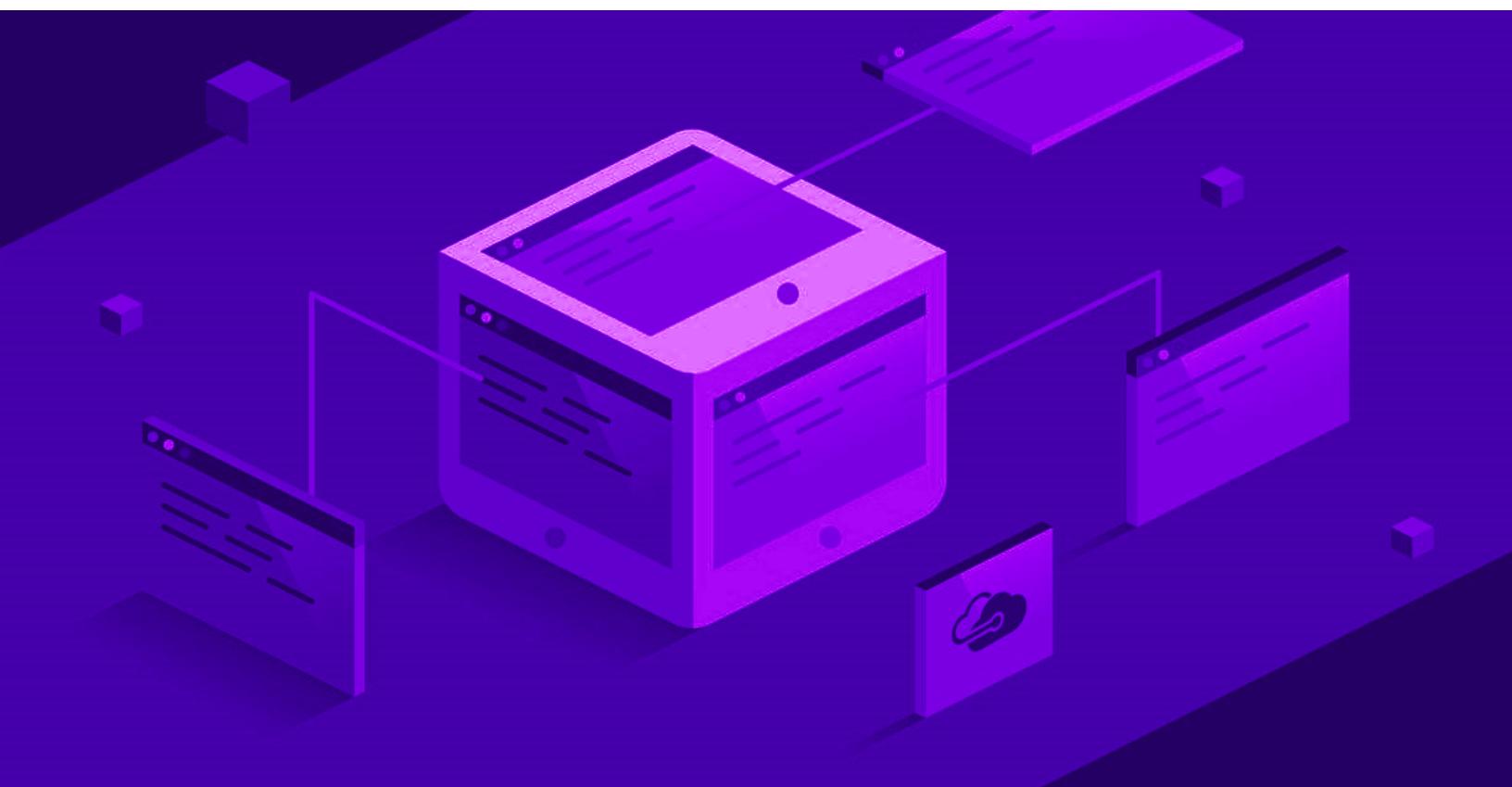


TP3 Report

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.

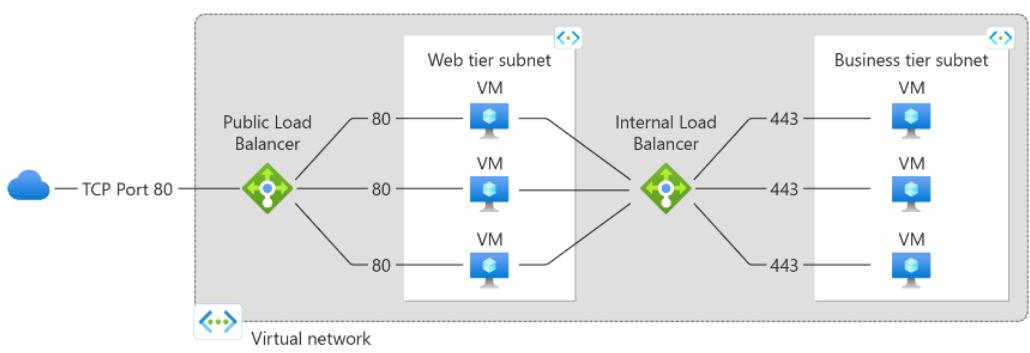
Azure load balancers are especially useful in scenarios where there is a high volume of traffic to an application or service. Overall, this TP will demonstrate how Azure load balancers can help improve the reliability and performance of applications in Microsoft Azure's cloud infrastructure.

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:

The screenshot shows two sequential steps in the Microsoft Azure portal:

Step 1: Create a resource group

- Basics** tab selected.
- Subscription**: Azure pour les étudiants
- Resource group**: tp3rglb
- Region**: (Europe) North Europe

Step 2: Create virtual network

- Basics** tab selected.
- Subscription**: Azure pour les étudiants
- Resource group**: tp3rglb
- Virtual network name**: vnet1
- Region**: (Europe) North Europe

Both screenshots include standard Azure navigation and status bars at the top.

2- We create the first virtual machine loadvm1:

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The user is on the first step, 'Set instance details'. The form includes fields for Subscription (selected: 'Azure pour les étudiants'), Resource group (selected: 'tp3rglb'), and Virtual machine name ('loadvm1'). Other settings like Region ('(Europe) North Europe'), Availability options ('Availability zone'), and Security type ('Trusted launch virtual machines') are also visible. The 'Image' dropdown shows 'Windows Server 2019 Datacenter - x64 Gen2'. Navigation buttons at the bottom include 'Review + create', '< Previous', 'Next : Disks >', and 'Give feedback'.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The user is on the second step, which involves configuring the administrator account and inbound port rules. Under 'Administrator account', the 'Username' is set to 'loadvm1'. Under 'Inbound port rules', the 'Public inbound ports' section has 'Allow selected ports' selected, and 'HTTP (80), RDP (3389)' is listed. A warning message states: '⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to...' Navigation buttons at the bottom include 'Review + create', '< Previous', 'Next : Disks >', and 'Give feedback'.

3- We create the second virtual machine loadvm2:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine ...

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Azure pour les étudiants

Resource group * ⓘ tp3rglib

Create new

Instance details

Virtual machine name * ⓘ loadvm2

Region * ⓘ (Europe) North Europe

Availability options ⓘ

Availability zone *

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

Review + create < Previous Next : Disks > Give feedback

Microsoft Azure

Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine ...

Run with Azure Spot discount ⓘ

Size * ⓘ Standard_B2s - 2 vcpus, 4 GiB memory (US\$39.13/month)

See all sizes

Administrator account

Username * ⓘ loadvm2

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)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create < Previous Next : Disks > Give feedback

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

Create storage account

Name *: strgtp3

Account kind: Storage (general purpose v1)

Performance: Standard

Replication: Locally-redundant storage (LRS)

Location: (Europe) North Europe

Resource group: tp3rglb

Minimum TLS version: Version 1.2

OK

Configure Custom Script Extension Extension

Create Review + create

Script file (Required): `install_IIS.ps1`

Arguments (Optional):

loadvm1 | Extensions + applications

Virtual machine

Extensions VM Applications

Name	Type	Version	Status	Automatic upgrade st
CustomScriptExtension	Microsoft.Compute.CustomScript	1.*	Transitioning	Not supported
GuestAttestation	Microsoft.Azure.Security.Windows	1.*	Provisioning succeeded	Not supported

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

loadvm2 | Extensions + applications

Virtual machine

Search resources, services, and docs (G+/)

Extensions VM Applications

+ Add Refresh Feedback

Name	Type	Version	Status	Automatic upgrade st
CustomScriptExtension	Microsoft.Compute.CustomScript	1.*	Provisioning succeeded	Not supported
GuestAttestation	Microsoft.Azure.Security.Windo	1.*	Provisioning succeeded	Not supported

6- We create a standard SKU load balancer:

Microsoft Azure

Home > Load balancing | Load Balancer >

Create load balancer

Subscription * Azure pour les étudiants

Resource group * tp3rglb

Instance details

Name * standloadbalancer

Region * North Europe

SKU * Standard

Type * Public

Tier * Regional

Review + create < Previous Next : Frontend IP configuration > Download a template for automation Give feedback

Microsoft recommends Standard SKU load balancer for production workloads. Learn more about pricing differences between Standard and Basic SKU

Microsoft Azure Search resources, services, and docs (G+)

Home > Load balancing | Load Balancer > Create load balancer ...

Frontend IP configuration

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	

Add fronted IP configuration

Name * loadfrontenedip

IP version IPv4

IP type IP address

Public IP address * Choose public IP address Create new

Add a public IP address

Name * loadfrontenedip

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+)

Home > Load balancing | Load Balancer > Create load balancer > Add backend pool ...

Add backend pool

Name * PoolA

Virtual network vnet1 (tp3rglb)

Backend Pool Configuration NIC

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.

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

Create load balancer

Inbound rules

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

Frontend IP address *: loadfrontenedip (To be created)

Backend pool *: PoolA

Protocol *: TCP

Port *: 80

Add

Add load balancing rule

Port *: 80

Backend port *: 80

Health probe *: (new) ProbeA

Session persistence: None

Idle timeout (minutes): 4

TCP reset: Disabled

Floating IP: Disabled

Outbound source network address translation (SNAT): (Recommended) Use outbound rules to provide backend

Add

Load balancing | Load Balancer

standloadbalancer

Overview

Essentials

- Resource group (move): tp2rglb
- Location: North Europe
- Subscription (move): Azure pour les étudiants
- Subscription ID: Sdfc723-ea7b-4a89-b344-86968954d351
- SKU: Standard
- Tags (edit): Tags
- 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:

The screenshot shows the Azure portal interface for managing a load balancer. The top navigation bar includes icons for file, settings, and user profile. The main title is 'loadbalancer | Frontend IP configuration'. Below the title, there's a toolbar with '+ Add', 'Refresh', and 'Give feedback' buttons. A search bar labeled 'Filter by name...' is present. A table lists the frontend IP configuration rules. The first rule is 'loadfrontenedip' with IP address '51.138.238.64 (loadfrontenedip)' and a 'Rules count' of 1.

First try, we were redirected to loadvm2:

The screenshot shows a browser window with a warning message: 'Not secure | 51.138.238.64'. The address bar shows 'loadvm2'. The page content is mostly blank, indicating a redirect or loading issue.

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

The screenshot shows a browser window with a warning message: 'Not secure | 51.138.238.64'. The address bar shows 'loadvm1'. The page content is visible and readable.

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

The screenshot shows the Microsoft Azure portal for adding an inbound NAT rule. The top navigation bar includes icons for file, settings, and user profile. The main title is 'Add inbound NAT rule'. The form fields are as follows:

- Name: (highlighted)
- Type: Azure virtual machine
- Target virtual machine:
- Network IP configuration:
- Frontend IP address:
- Frontend Port:
- Service Tag:
- Backend port:
- Protocol: TCP

At the bottom, there are 'Add' and 'Give feedback' buttons.

9- We add an Inbound NAT rule to loadvm2:

The screenshot shows the Microsoft Azure portal interface for creating an inbound NAT rule. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. The main page title is 'Add inbound NAT rule ...' under 'standloadbalancer'. A descriptive note states: 'An inbound NAT rule forwards incoming traffic sent to a selected IP address and port combination to a specific virtual machine.' The configuration form fields are as follows:

- Name ***: loadvm2rule
- Type**: Azure virtual machine
- Target virtual machine**: loadvm2 (ResourceGroup: tp3rglb, AvailabilitySet: -)
- Network IP configuration ***: ipconfig1 (10.0.0.5)
- Frontend IP address ***: loadfrontenedip (51.138.238.64)
- Frontend Port ***: 49153
- Service Tag ***: Custom
- Backend port ***: 3389
- Protocol**: TCP
- Enable TCP Reset**: Unchecked

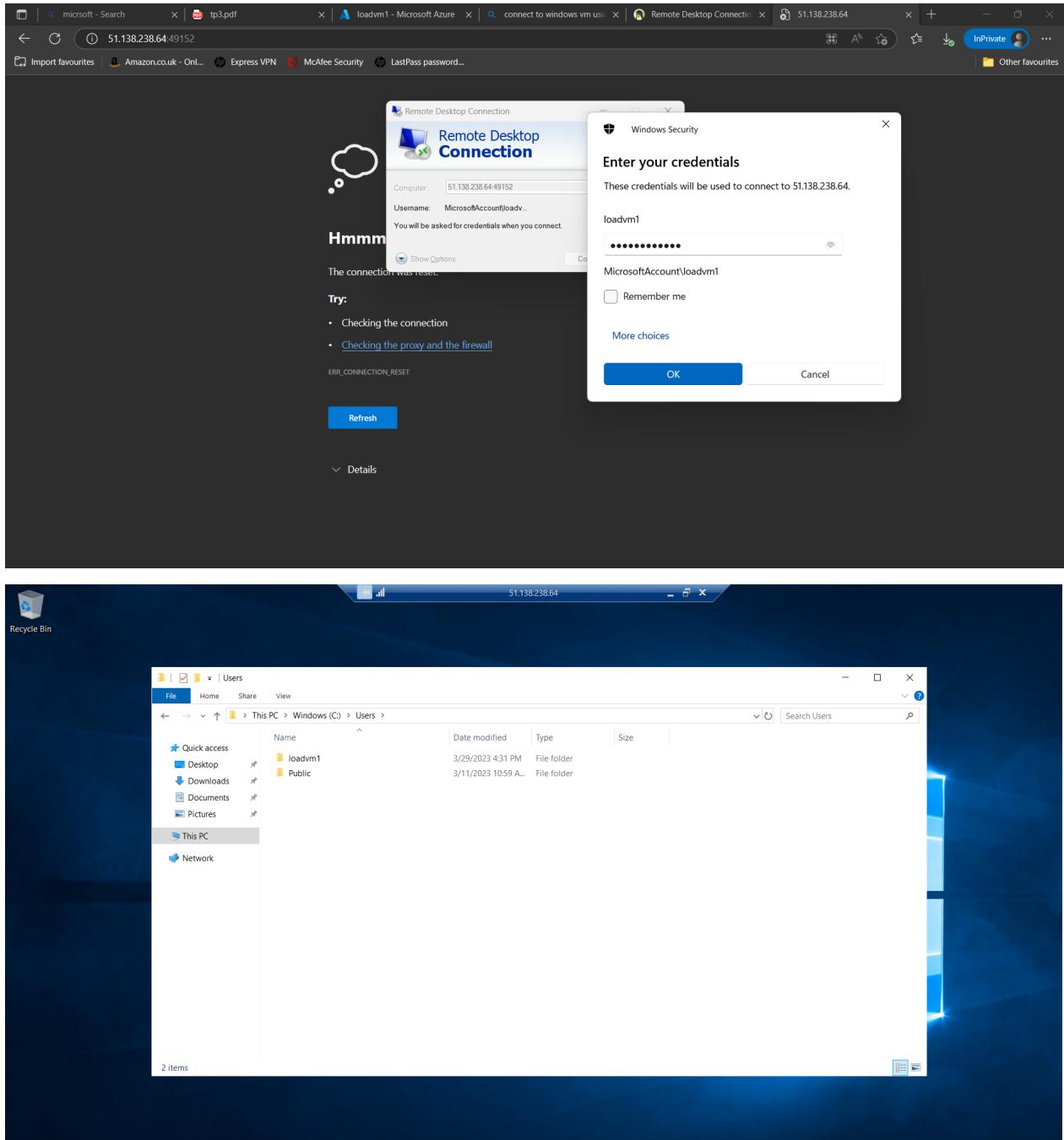
At the bottom right are 'Add' and 'Give feedback' buttons.

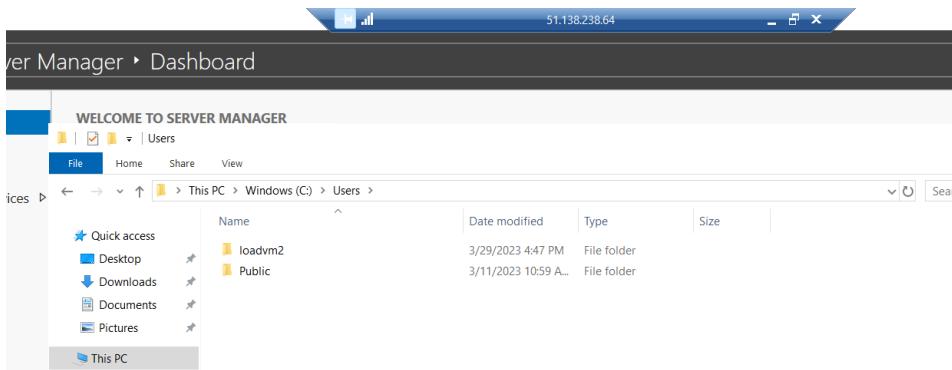
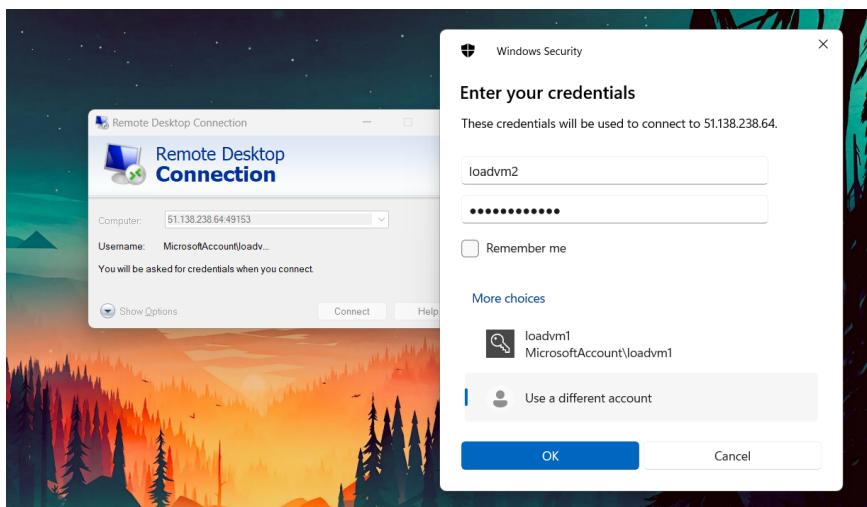
10- In this question, we were asked to open the browser and type the load balancer's public IP address using the mapped ports that we created the Inbound NAT rule with.

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 .

The image contains two side-by-side browser windows. Both show a dark grey page with a white cloud icon and the text 'Hmmm... can't reach this page'. Below it says 'The connection was reset.' and 'Try:' followed by a bulleted list: 'Checking the connection' and 'Checking the proxy and the firewall'. The top window has a URL of '51.138.238.64:49152' and the bottom window has a URL of '51.138.238.64:49153'. The browser interface includes a back button, forward button, and a menu bar with various icons.

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:

Setting	Value
Resource group (move)	tp2rglb
Location	North Europe (Zone 1)
Subscription (move)	Azure pour les étudiants
Subscription ID	5dpcf723-ea7b-4a89-b344-86968954d351
Tags (edit)	Click here to add tags

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines > Create a virtual machine

Instance details

Virtual machine name * Available

Region *

Availability options

Availability zone * You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type Configure security features

Image * See all images | Configure VM generation

VM architecture x64

Review + create < Previous Next : Disks > Give feedback

Microsoft Azure Search resources, services, and docs (G+)

Home > Create a virtual machine

Administrator account

Authentication type Password

Username * Available

Password * Available

Confirm password * Available

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 * Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to

Review + create < Previous Next : Disks > Give feedback

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:~ x + ~
└$ ^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:

The screenshot shows the 'Add backend pool' page in the Microsoft Azure portal. The 'Name' field is set to 'PoolB'. The 'Virtual network' is 'vnet1'. Under 'Backend Pool Configuration', 'NIC' is selected. In the 'IP configurations' section, there is a note about IP configurations associated with virtual machines and virtual machine scale sets. Below this, there are 'Add' and 'Remove' buttons. A table lists the backend pool members: 'linuxvm' (Resource Name), 'tp3rglb' (Resource group), 'Virtual machine' (Type), 'ipconfig1' (IP configuration), '10.0.0.6' (IP Address), and '-' (Availability set). At the bottom are 'Save', 'Cancel', and 'Give feedback' buttons.

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.)

The screenshot shows the 'Add load balancing rule' page in the Microsoft Azure portal. The 'Name' field is 'RuleB'. The 'IP Version' is 'IPv4'. The 'Frontend IP address' is 'loadfrontendip (20.166.226.228)'. The 'Backend pool' is 'PoolB'. The 'Protocol' is 'TCP'. The 'Port' is '8080' and the 'Backend port' is '80'. The 'Health probe' is 'ProbeA (HTTP:80)'. The 'Session persistence' is 'None'. The 'Idle timeout (minutes)' is '4'. The 'Enable TCP Reset' and 'Enable Floating IP' checkboxes are unchecked. The 'Outbound source network address translation (SNAT)' checkbox is checked. A note at the bottom says '(Recommended) Use outbound rules to provide backend pool members access to the internet.' At the bottom are 'Save', 'Cancel', and 'Give feedback' buttons.

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

The screenshot shows a Microsoft Edge browser window. The address bar displays "Not secure | 20.166.226.228:8080". Below the address bar, there are several icons for bookmarks and security. The main content area shows the "Welcome to nginx!" page. The page includes a message: "If you see this page, the nginx web server is successfully installed and working. Further configuration is required.", links to "nginx.org" and "nginx.com", and a "Thank you for using nginx." message.

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

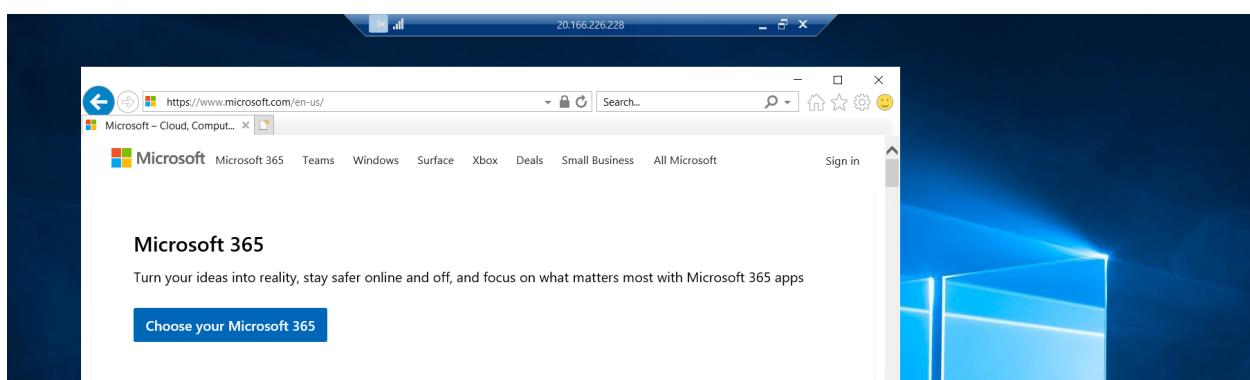
The screenshot shows the Azure portal interface for managing a load balancer. The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, the "Backend pools" option is selected. The main content area displays the "standloadbalancer | Backend pools" blade. It shows two backend pools: "PoolA (1)" and "PoolB (1)". "PoolA (1)" contains one member: "loadvm1" (Status: Running, IP: 10.0.0.4). "PoolB (1)" contains one member: "linuxvm" (Status: Running, IP: 10.0.0.6).

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

The screenshot shows an Internet Explorer window with the URL "http://www.microsoft.com". The status bar indicates the connection is to "20.166.226.228". A modal dialog box titled "Internet Explorer" is displayed, stating: "Content from the website listed below is being blocked by the Internet Explorer Enhanced Security Configuration." It includes a "Close" button and a checkbox for "Continue to prompt when website content is blocked". Below the dialog, a message says: "If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead." At the bottom, it says: "Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer."

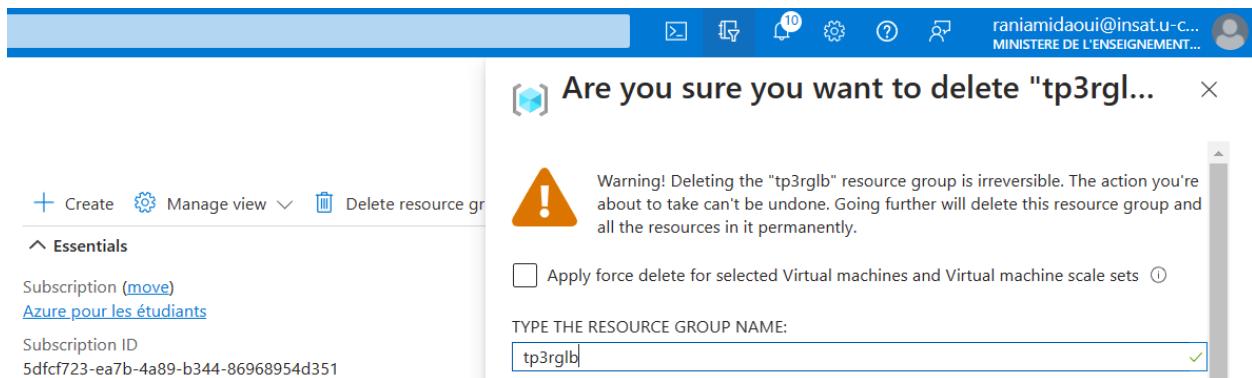
We configure the outbound rules:

The screenshot shows the Microsoft Azure portal interface for configuring an outbound rule. The top navigation bar includes 'Microsoft Azure', a search bar, and user information. The main page title is 'Load balancing | Load Balancer | standloadbalancer | Outbound rules > Add outbound rule'. The configuration form includes fields for 'Name' (OutRuleloadvm1), 'IP Version' (IPv4 selected), 'Frontend IP address' (1 selected), 'Protocol' (TCP selected), 'Idle timeout (minutes)' (4), 'TCP Reset' (Enabled selected), and 'Backend pool' (PoolA (1 instances)). A note about port allocation states: 'Azure automatically assigns the number of outbound ports to use for source network address translation (SNAT) based on the number of frontend IP addresses and backend pool instances.' Below this, there's a section for 'Port allocation' with options for 'Manually choose number of outbound ports' (selected), 'Choose by' (Ports per instance selected), and 'Ports per instance' (16). A note at the bottom states: 'The maximum number of backend instances cannot be more than 1000.'



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:

The screenshot shows the Azure portal interface for creating a new virtual machine scale set. At the top, there's a navigation bar with the Microsoft Azure logo, a search bar, and the user's name 'raniamidaoui@insat.u-c...' and 'MINISTERE DE L'ENSEIGNEMENT...'. Below the navigation bar, the URL 'Home > Virtual machine scale set >' is visible. The main page title is 'Create a virtual machine scale set ...'. Below the title, there are tabs for 'Basics', 'Spot', 'Disks', 'Networking', 'Scaling', 'Management', 'Health', 'Advanced', 'Tags', and 'Review + create'. The 'Basics' tab is selected. A descriptive text explains that Azure virtual machine scale sets let you create and manage a group of load balanced VMs. It mentions that the number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs. A link 'Learn more about virtual machine scale sets' is provided. The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'Azure pour les étudiants' and the 'Resource group' dropdown is set to 'tp3rgvmss'. The 'Scale set details' section requires a 'Virtual machine scale set name' ('scaleset') and a 'Region' ('(Europe) North Europe'). The 'Availability zone' dropdown is set to 'None'. The 'Orchestration' section is partially visible at the bottom. At the bottom of the page, there are buttons for 'Review + create', '< Previous' (disabled), 'Next : Spot >', and 'Give feedback'.

Create a virtual machine scale set

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

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 *
[See all sizes](#)

Administrator account

[Review + create](#) [< Previous](#) [Next : Spot >](#) [Give feedback](#)

Create a virtual machine scale set

NAME	CREATE PUBLIC IP	SUBNET	NETWORK SECURITY GROUP	ACCELERATED NETWORKING
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.

Select a load balancer *
[Create a load balancer](#)

[Review + create](#) [< Previous](#) [Next : Scaling >](#) [Give feedback](#)

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Scaling

Scaling policy Manual scaling Autoscaling

Scale-In policy

Configure the order in which virtual machines are selected for deletion during a scale-in operation. [Learn more about scale-in policies](#)

Scale-in policy: Default - Balance across availability zones and fault domains, then delete V...

Apply force delete to scale-in operations

2- All the resources have been created successfully:

scaleset | Instances

Instance	Computer name	Status	Protection policy	Provisioning state	Health state	Latest model
scaleset_0	scalesetp000000	Running		Succeeded		Yes

Frontend IP configuration

Name	IP address	Rules count
scalesetlb-frontendconfig01	4.231.228.7 (scalesetlb-publicip)	2

scalesetlb | Backend pools

Backend pool	Resource Name	Resource Status	IP address	Network interface	Availability zone	Rules count
bepool (1)	scaleset (instance 0)	Running	10.0.0.4	tp3rgvmss-vnet-nic01	-	2

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

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure', a search bar, and user information ('raniamidaoui@insat.u-c... MINISTÈRE DE L'ENSEIGNEMENT...'). Below the navigation bar, the URL is 'Home > scaleset | Extensions + applications > Install an Extension > Configure Custom Script Extension Extension'. A 'Script file (Required)' input field contains 'install_IIS.ps1', with a 'Browse' button next to it. An 'Arguments (Optional)' input field is below. In the main content area, a progress bar indicates 'Upgrading virtual machine instance' for 'scaleset_0'. Below the progress bar is a table listing VM instances, showing 'scaleset_0' as running and succeeded. At the bottom, there are buttons for Start, Restart, Stop, Reimage, Delete, Upgrade, Refresh, and Protection Policy.

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

The screenshot shows the Microsoft Azure portal interface. On the left, the 'Virtual machine scale sets' blade is open, showing a list of scalesets with 'scaleset' selected. The right side shows the 'Networking' blade for the 'scaleset' scale set. Under 'Inbound port rules', a new rule is being added: 'Add inbound security rule' for 'basicNsgtp3rgvmss-vnet-nic01'. The configuration includes: Source 'Any', Source port ranges '80', Destination 'Any', Service 'Custom', Destination port ranges '80', Protocol 'TCP', and Action 'Allow'. At the bottom right of the blade are 'Add' and 'Cancel' buttons. Below the blade, a browser screenshot shows a test of the load balancer. The address bar says 'Not secure | 4.231.228.7'. The page content displays 'Import favourites | Amazon.co.uk - Onl... | Express VPN | McAfee Security | LastPass password' and the text 'scalesetp000000'.

5- We set up custom autoscale:

scaleset | Scaling

Virtual machine scale set

Choose how to scale your resource

- Manual scale
- Custom autoscale (selected)

Custom autoscale

Autoscale setting name: scaleset-Autoscale-754

Resource group: tp3rgvmss

Predictive autoscale: Mode: Disabled

Note: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

scaleset | Scaling

Virtual machine scale set

Predictive autoscale

Mode: Enabled

Default

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode

Rules: Scale is based on metric trigger rules but no rule(s) is defined; click Add a rule to create a rule. For example: 'Add a rule that increases instance count by 1 when CPU Percentage is above 70%'. If no rules is defined, the resource will be set to default instance count.

Instance limits

Minimum: 1

Maximum: 3

Default: 1

This scale condition is executed when none of the other scale condition(s) match

Scale rule

Metric source: Current resource (scaleset)

Resource type: Virtual machine scale sets Resource: scaleset

Criteria

Metric namespace *: Virtual Machine Host Metric name: Percentage CPU

Dimension Name Operator Dimension Values Add

VMName = All values +

If you select multiple values for a dimension, autoscale will aggregate the metric across the selected values, not evaluate the metric for each value individually.

Percentage CPU (Maximum): 0% - 100% UTC+01:00

Scale rule

Percentage CPU (Maximum): 0% - 20% UTC+01:00

Enable metric divide by instance count ⓘ

Operator *: Greater than Metric threshold to trigger scale action * ⓘ

0 %

Duration (minutes) * ⓘ Time grain (minutes) ⓘ

1 1

⚠ Setting a duration less than 5 minutes may generate transient metric spikes that leads to unexpected scaling actions. For best results, the duration should be set at least to 5 minutes.

Time grain statistic * ⓘ Time aggregation * ⓘ

Maximum Maximum

Action

Operation *: Increase count by Cool down (minutes) * ⓘ

5

instance count *:

1

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

Azure pour les étudiants | Resource providers ⚙ ...

Subscription

Search Register Unregister Refresh Feedback

Partner information

Programmatic deployment

Resource groups

Resources

microsoft.insights

Provider	Status
microsoft.insights	Registering

Resource 'scaleset' updated

Successfully updated configuration for 'scaleset'

All good, the autoscaling is working perfectly:

scaleset | Instances

Virtual machine scale set

Search

Start, Restart, Stop, Reimage, Delete, Upgrade, Refresh, Protection Policy

Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems

Settings

Instances

Instance	Computer name	Status	Protection policy	Provisioning state	Health state	Latest model
scaleset_0	scalesetp000000	Running	Succeeded		Yes	
scaleset_1	scalesetp000001	Creating (Running)		Creating	Yes	

scalesetlb | Backend pools

Load balancer

Search

Add, Refresh, Give feedback

Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems

Settings

Frontend IP configuration, Backend pools, Health probes, Load balancing rules

Group by Backend pool

bepool (2)

Backend pool	VM instance ID	Status	IP address	Network security group	Availability zone	Rules count
bepool	scaleset (insta...)	Running	10.0.0.4	tp3rgvmss-vr	-	2
bepool	scaleset (insta...)	Creating (Run...	10.0.6.0	tp3rgvmss-vr	-	2

Microsoft Azure

Home > scaleset

scaleset | Instances

Virtual machine scale set

Search

Start, Restart, Stop, Reimage, Delete, Upgrade, Refresh, Protection Policy

Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems

Settings

Instances, Networking

Search virtual machine instances

Instance	Computer name	Status	Protection policy	Provisioning state	Health state	Latest model
scaleset_0	scalesetp000000	Running	Succeeded		Yes	
scaleset_1	scalesetp000001	Running	Succeeded		Yes	
scaleset_2	scalesetp000002	Creating (Running)		Creating	Yes	

Backend pool	scaleset (inst)	Status	IP address	Network security group	Ports
bepool	scaleset (inst)	Running	10.0.0.4	tp3rgvmss-vr	-
bepool	scaleset (inst)	Running	10.0.6.0	tp3rgvmss-vr	-
bepool	scaleset (inst)	Creating (Runn)	10.0.2.0	tp3rgvmss-vr	-

7- We delete the resource group:

Are you sure you want to delete "tp3rgv..."

Warning! Deleting the "tp3rgvmss" resource group is irreversible. The action you're about to take can't be undone. Going further will delete this resource group and all the resources in it permanently.

Apply force delete for selected Virtual machines and Virtual machine scale sets

TYPE THE RESOURCE GROUP NAME:
tp3rgvmss

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:

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * Azure pour les étudiants

Resource group * tp3ragag

Resource details

Region * (Europe) North Europe

Create virtual network

Basics

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure pour les étudiants

Resource group * tp3rag

Virtual network name * vnet1

Region * (Europe) North Europe

Deploy to an edge zone

Previous Next Review + create Give feedback

Add subnet

Name * appSubnet

Subnet address range * 10.0.1.0/24

Available IPs 251

Add IPv6 address space

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

Create a virtual machine

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure pour les étudiants

Resource group * tp3rag

Virtual machine name * appvmimage

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

Image * Windows Server 2019 Datacenter - x64 Gen2

Review + create < Previous Next : Disks > Give feedback

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

Run with Azure Spot discount

Size * Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (US\$84.68/month)

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 * Allow selected ports None

Select inbound ports * HTTP (80), RDP (3389)

Review + create **< Previous** **Next : Disks >** **Give feedback**

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

Networking Basics Disks 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

Subnet * default (10.0.0.0/24)

Public IP * (new) appvmimage-ip

NIC network security group * Basic Advanced

Public inbound ports * Allow selected ports None

Review + create **< Previous** **Next : Management >** **Give feedback**

Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual machines > Create a virtual machine

Subscription * Azure pour les étudiants

Resource group * tp3rgaq

Instance details

Virtual machine name * appvmvideo

Region * (Europe) North Europe

Availability options * Availability zone

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Availability zone *

Security type * Trusted launch virtual machines

Image * Windows Server 2019 Datacenter - x64 Gen2

VM architecture * Arm64 x64

Review + create **< Previous** **Next : Disks >** **Give feedback**

Microsoft Azure Search resources, services, and docs (G+)

Home > Virtual machines >

Create a virtual machine

Run with Azure Spot discount

Size *

Administrator account

Username * ✓

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 *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Review + create < Previous Next : Disks > Give feedback

Microsoft Azure Search resources, services, and docs (G+)

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 * Create new

Subnet * Manage subnet configuration

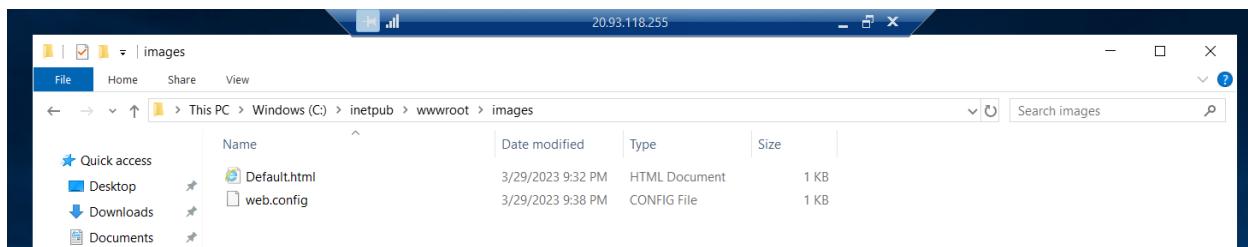
Public IP Create new

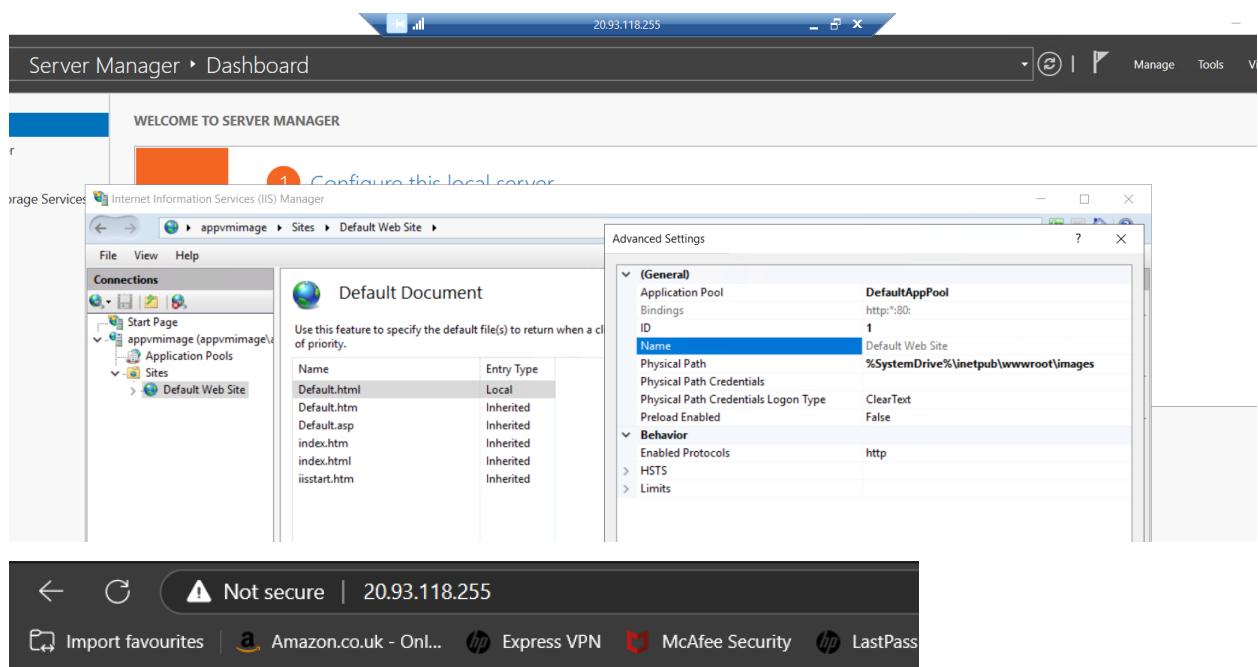
NIC network security group None Basic Advanced

Public inbound ports * None Allow selected ports

Review + create < Previous Next : Management > Give feedback

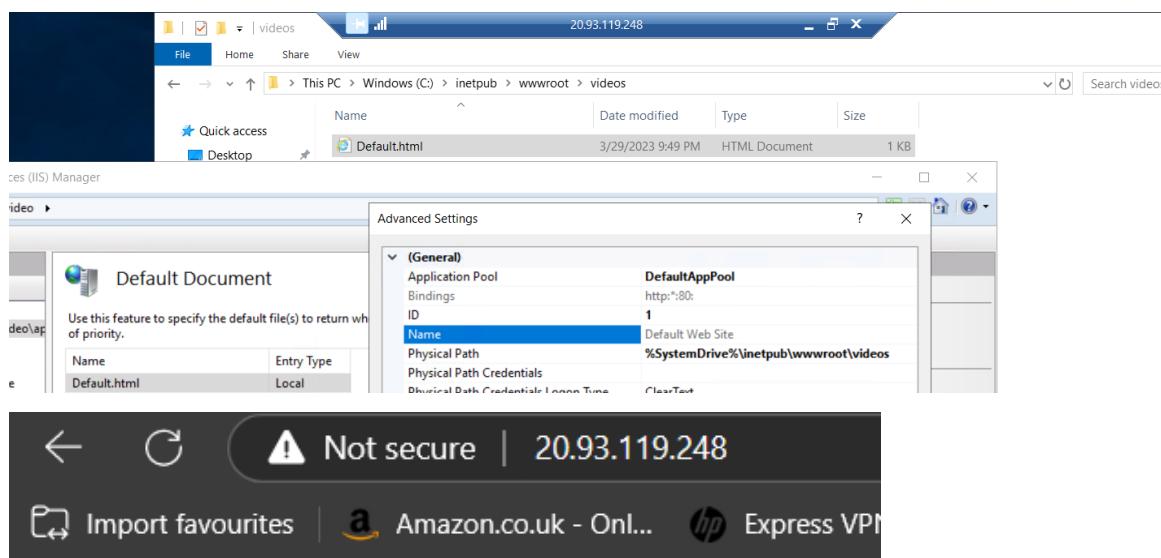
1- We install IIS server role and change the default website page of the image's server:





This is the images server.

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



This is the videos server.

2- We create an Application gateway:

Instance details

- Application gateway name *: appgateway
- Region *: North Europe
- Tier: Standard V2
- Enable autoscaling: No
- Instance count: 1
- Availability zone: None
- HTTP2: Disabled

Configure virtual network

- Virtual network *: vnet1
- Subnet *: appSubnet (10.0.1.0/24)

Buttons: Previous, Next : Frontends >

Frontends

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type: Public

Add a public IP

Name *	publicappgate
SKU	Standard
Assignment	Static
Availability zone	None

Buttons: Previous, Next : Backends >

Backends

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN).

Add a backend pool

Backend pool	Targets
imagespool	appvmimage524_z1
videospool	appvmvideo425_21

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.³

Listener name * Listener

Frontend IP * Public

Protocol HTTP

Port * 80

Additional settings

Listener type Basic

Error page url No

Previous **Next : Tags >** **Add** **Cancel**

Add a routing rule

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.³

Target type Backend pool

Backend target * imagespool

Backend settings * commonsetting

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.³

Path	Target name	Backend setting name	Backend pool
/images/*	imagetarget	commonsetting	imagespool
/videos/*	videotarget	commonsetting	videospool

Previous **Next : Tags >** **Add** **Cancel**

backend pools, add a second frontend IP configuration if you haven't already, or edit previous c

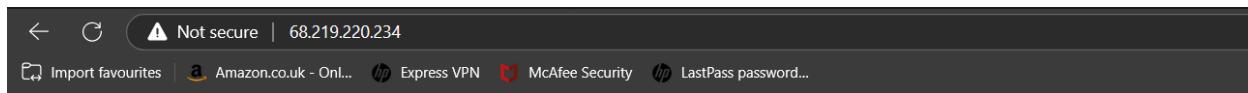
Routing rules

+ Add a routing rule

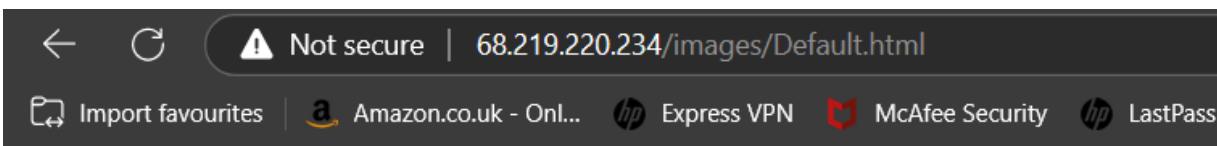
RuleA

Manage Backend settings

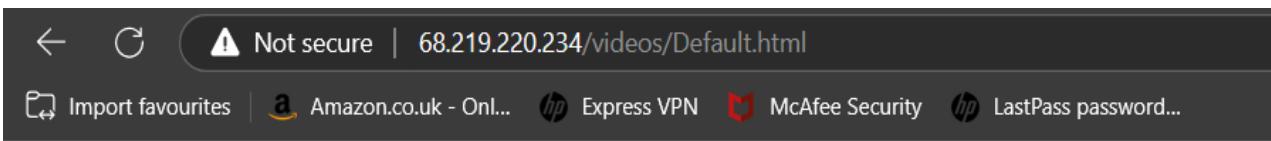
3- We test the Application Gateway:



This is the images server.

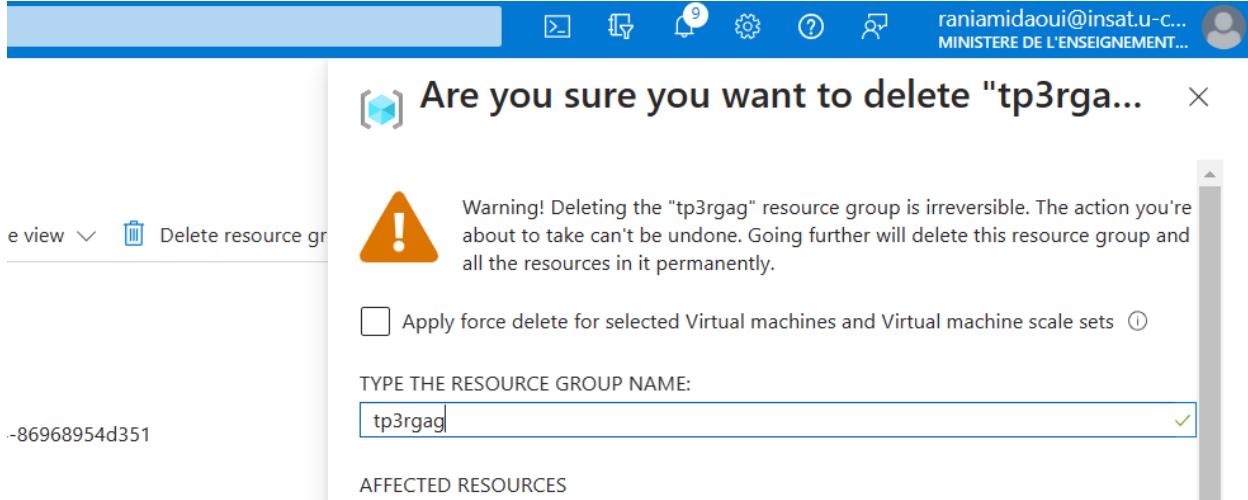


This is the images server.



This is the videos server.

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.