Compte rendu TP4

Traffic manager, Front door and Firewall

RT4 _ Groupe 1

- Réalisé par :

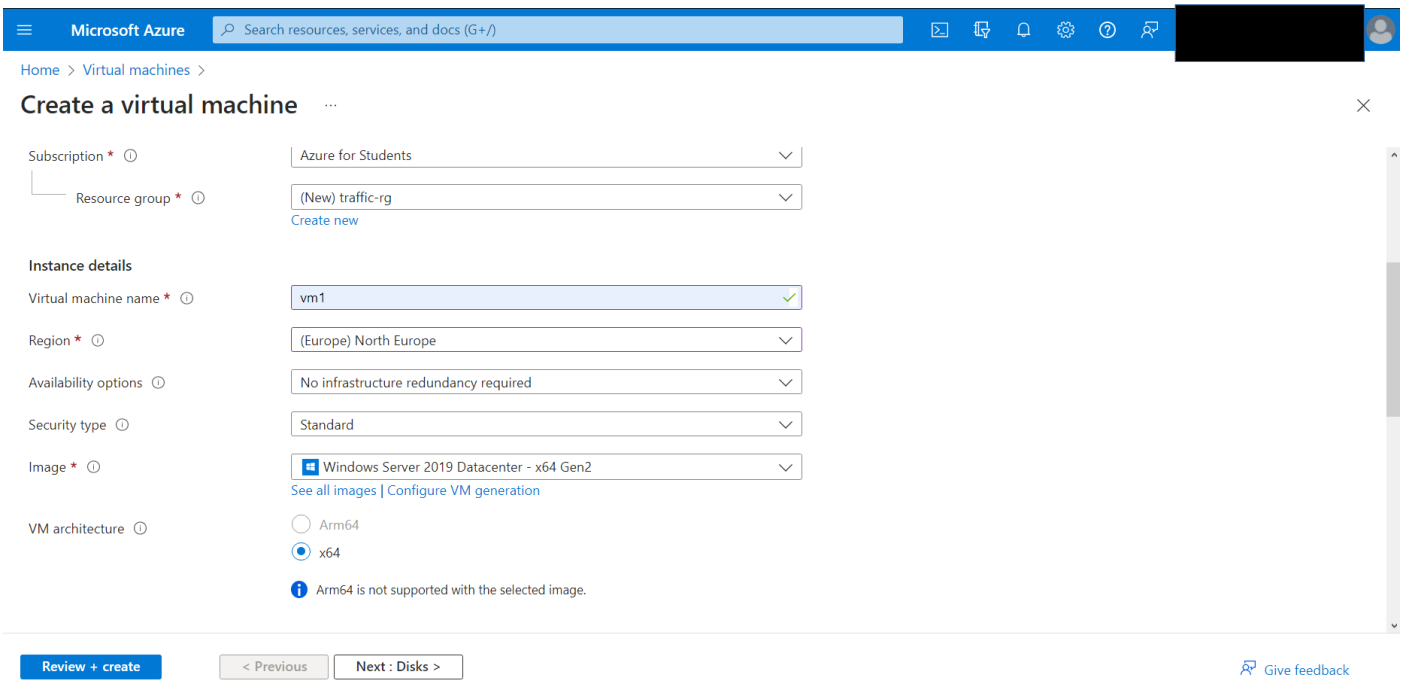
- Loulou Souha

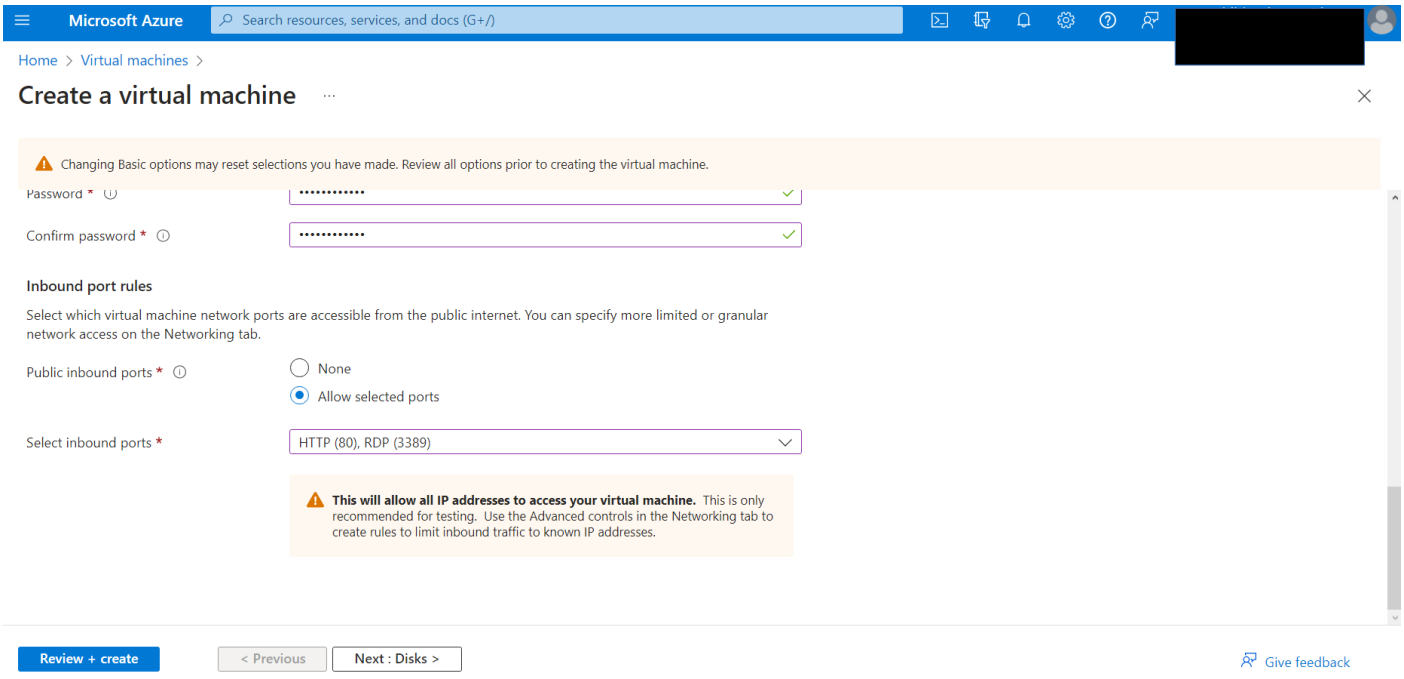
- Ben Jemaa Mouhib

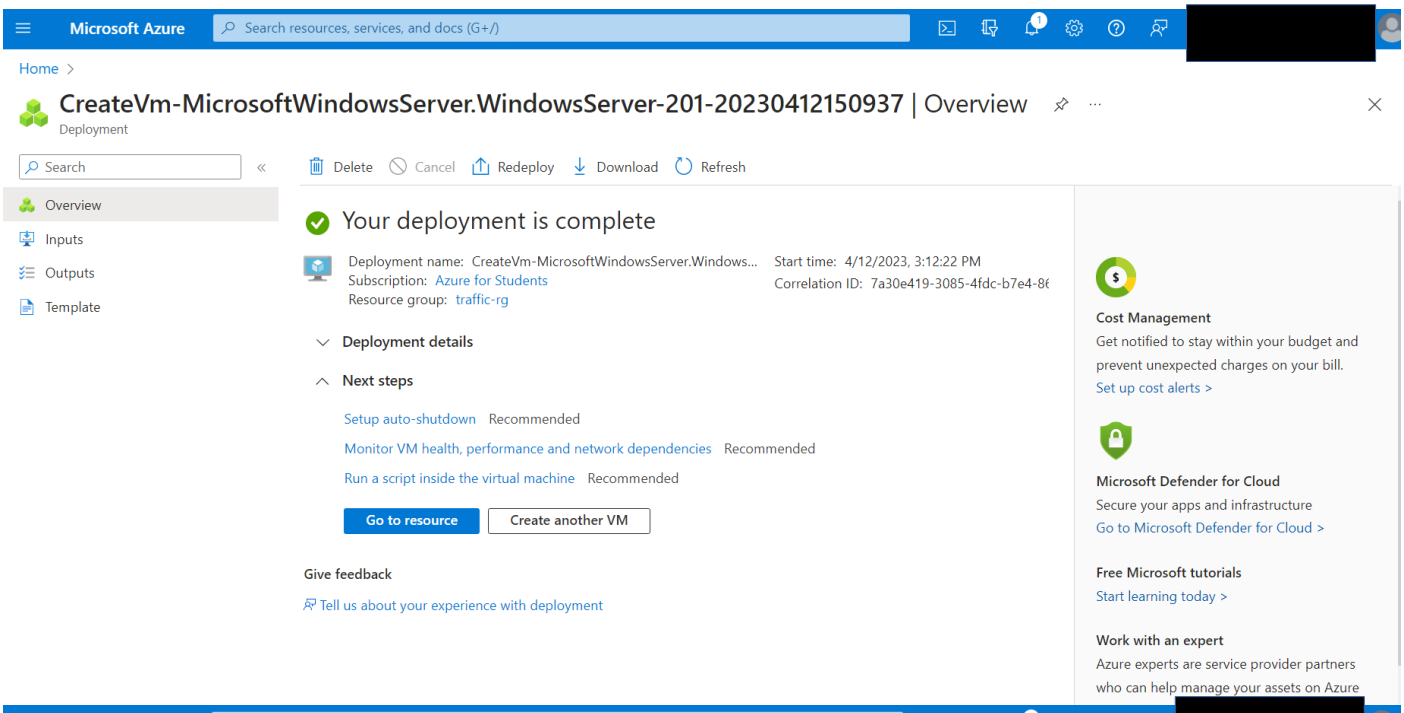
Année universitaire : 2022 - 2023

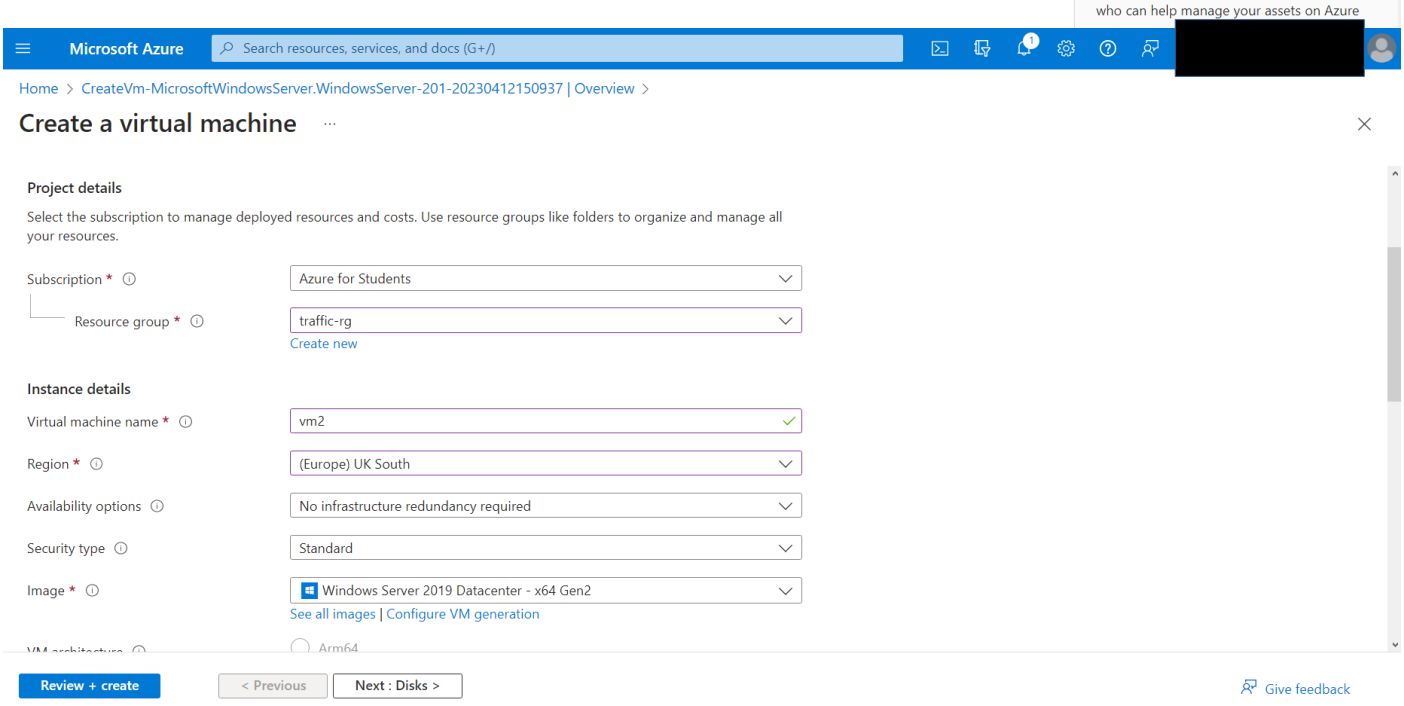
Task 1 : Azure traffic manager profile

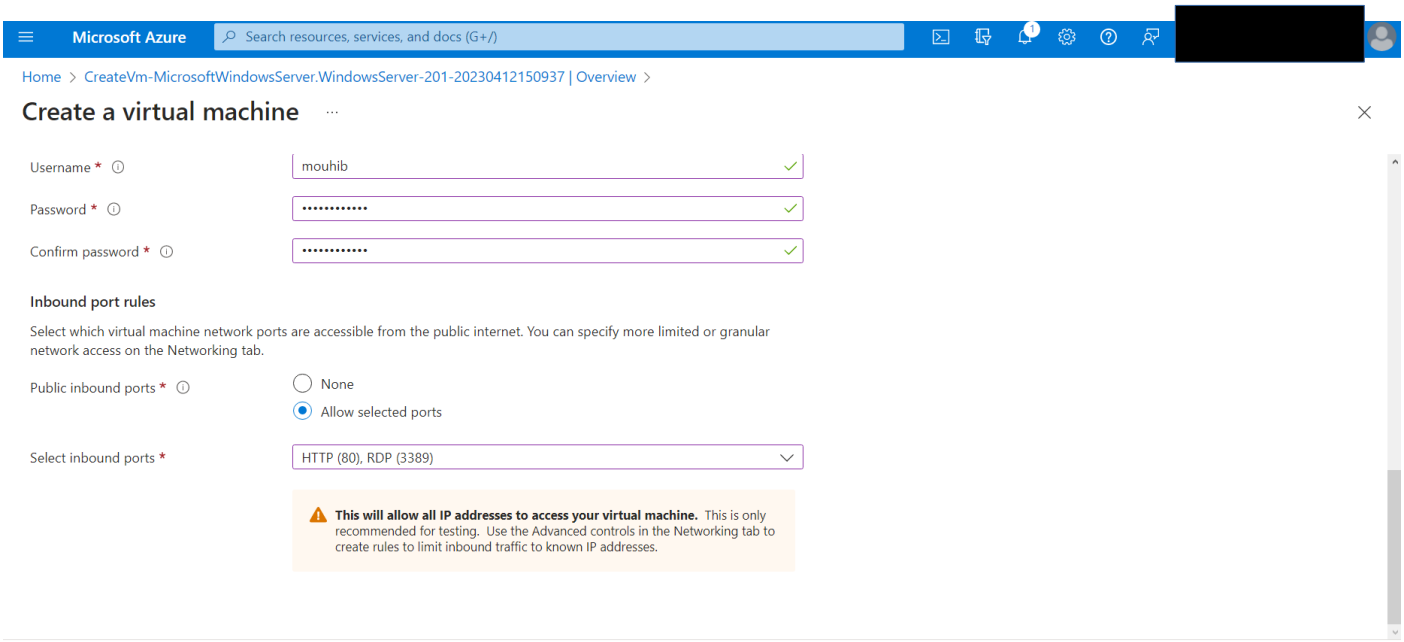
1- A-

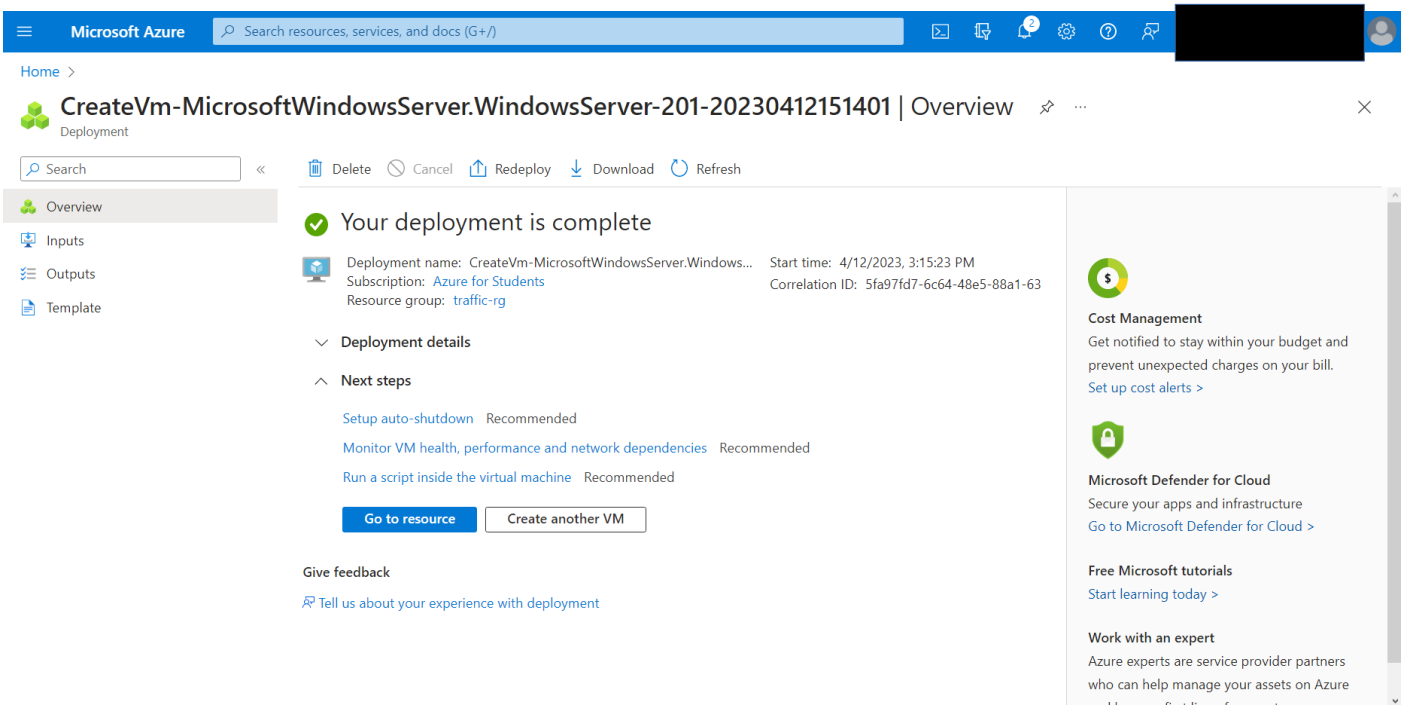




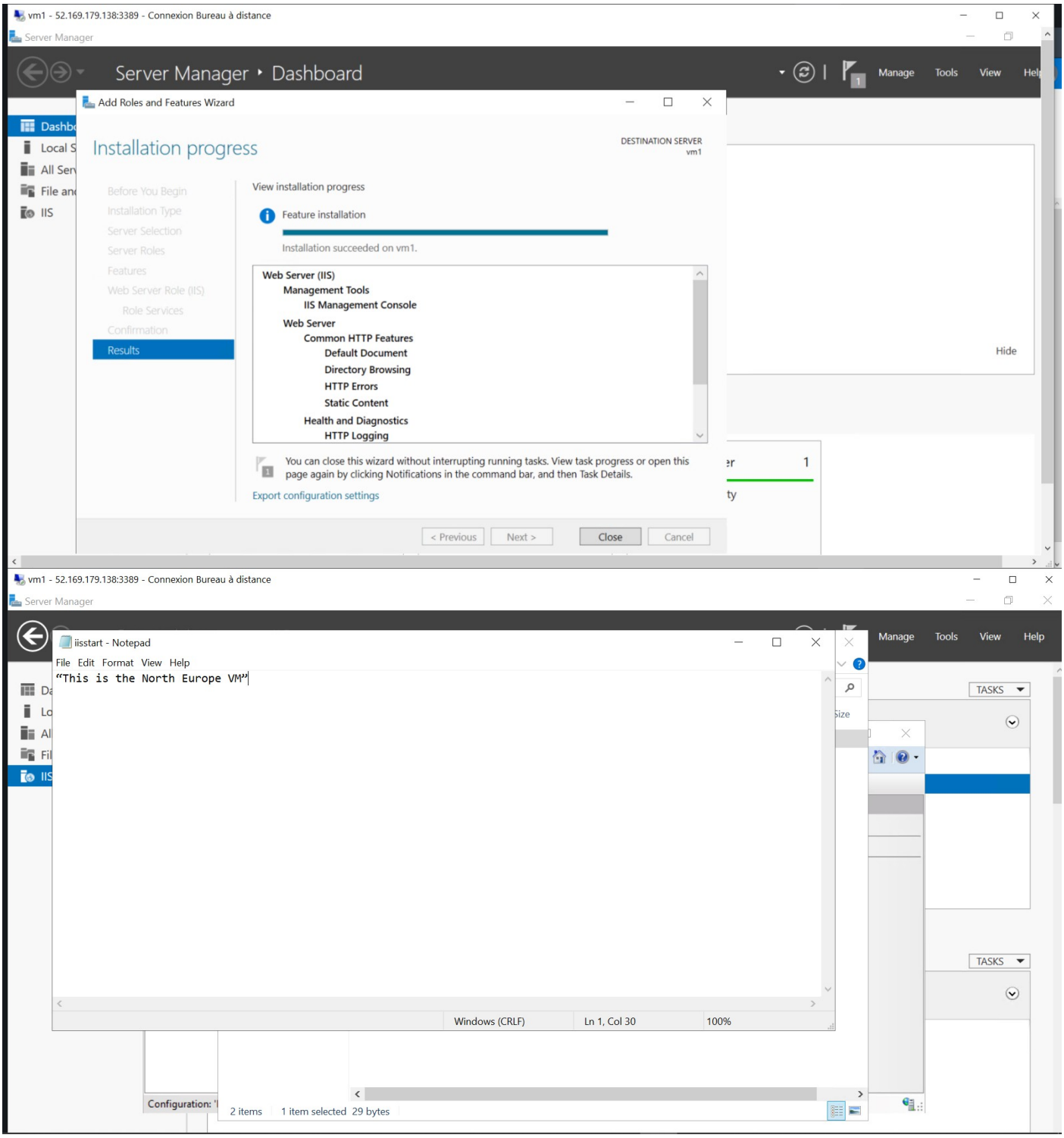

Microsoft Azure
Search resources, services, and docs (G+/)
Home
CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230412150937 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-MicrosoftWindowsServer.Windows...
Subscription: Azure for Students
Resource group: traffic-rg
Start time: 4/12/2023, 3:12:22 PM
Correlation ID: 7a30e419-3085-4fdc-b7e4-8
Deployment details
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure

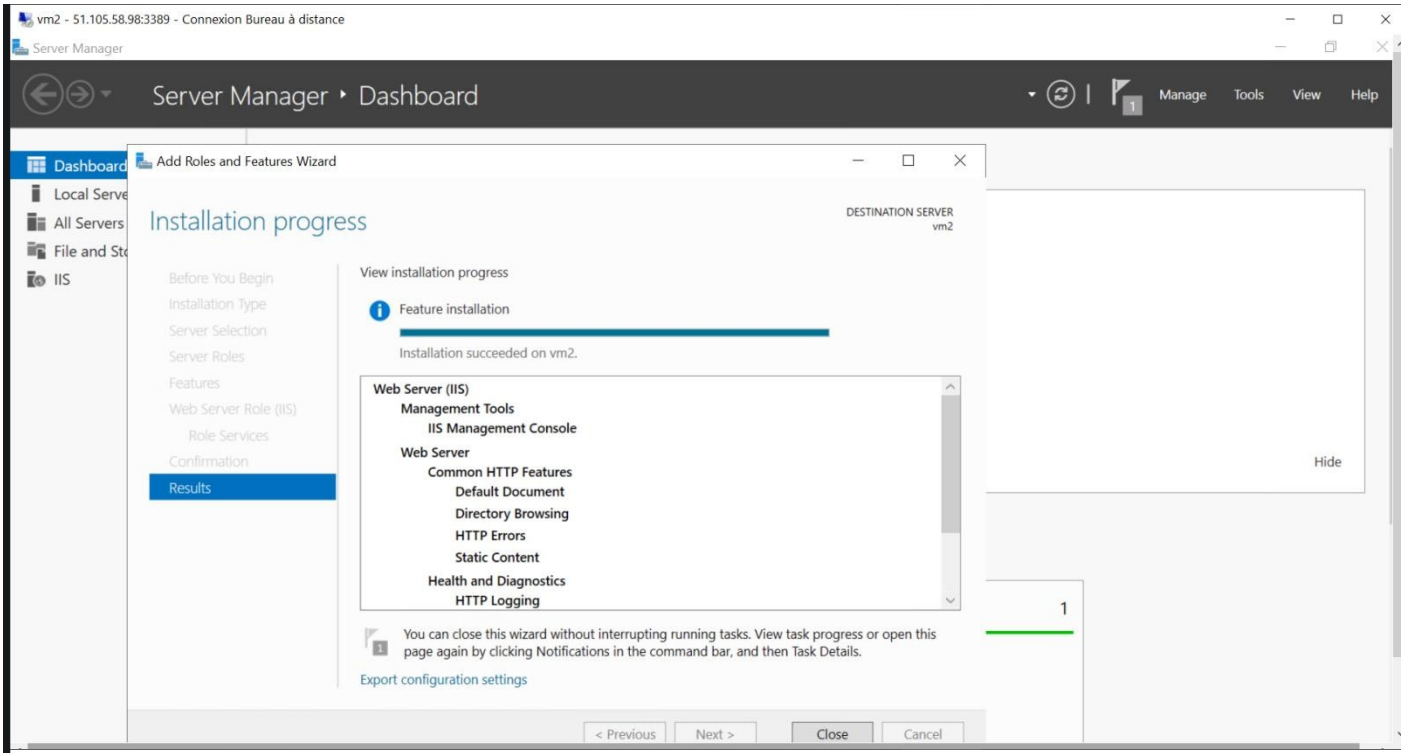

Microsoft Azure
Search resources, services, and docs (G+/)
Home
CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230412150937 | Overview
Create a virtual machine
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
traffic-rg
Create new
Instance details
Virtual machine name *
vm2
Region *
(Europe) UK South
Availability options
No infrastructure redundancy required
Security type
Standard
Image *
Windows Server 2019 Datacenter - x64 Gen2
See all images | Configure VM generation
Arm64
Review + create
< Previous
Next : Disks >
Give feedback

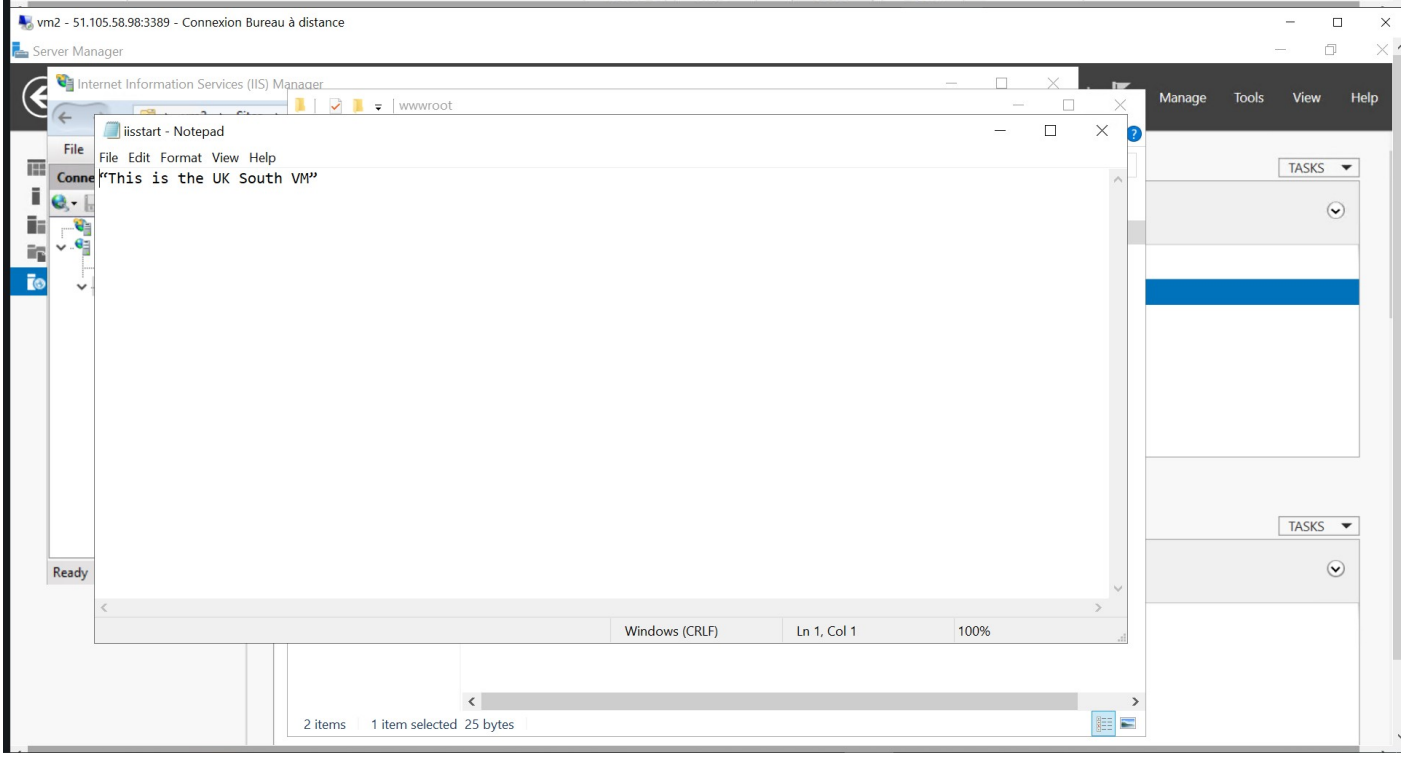

Microsoft Azure
Search resources, services, and docs (G+/)
Home > CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230412150937 | Overview >
Create a virtual machine
Username * mouhib
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the 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


Microsoft Azure
Search resources, services, and docs (G+/)
Home >
CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230412151401 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-MicrosoftWindowsServer.Windows...
Subscription: Azure for Students
Resource group: traffic-rg
Start time: 4/12/2023, 3:15:23 PM
Correlation ID: 5fa97fd7-6c64-48e5-88a1-63
Deployment details
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure

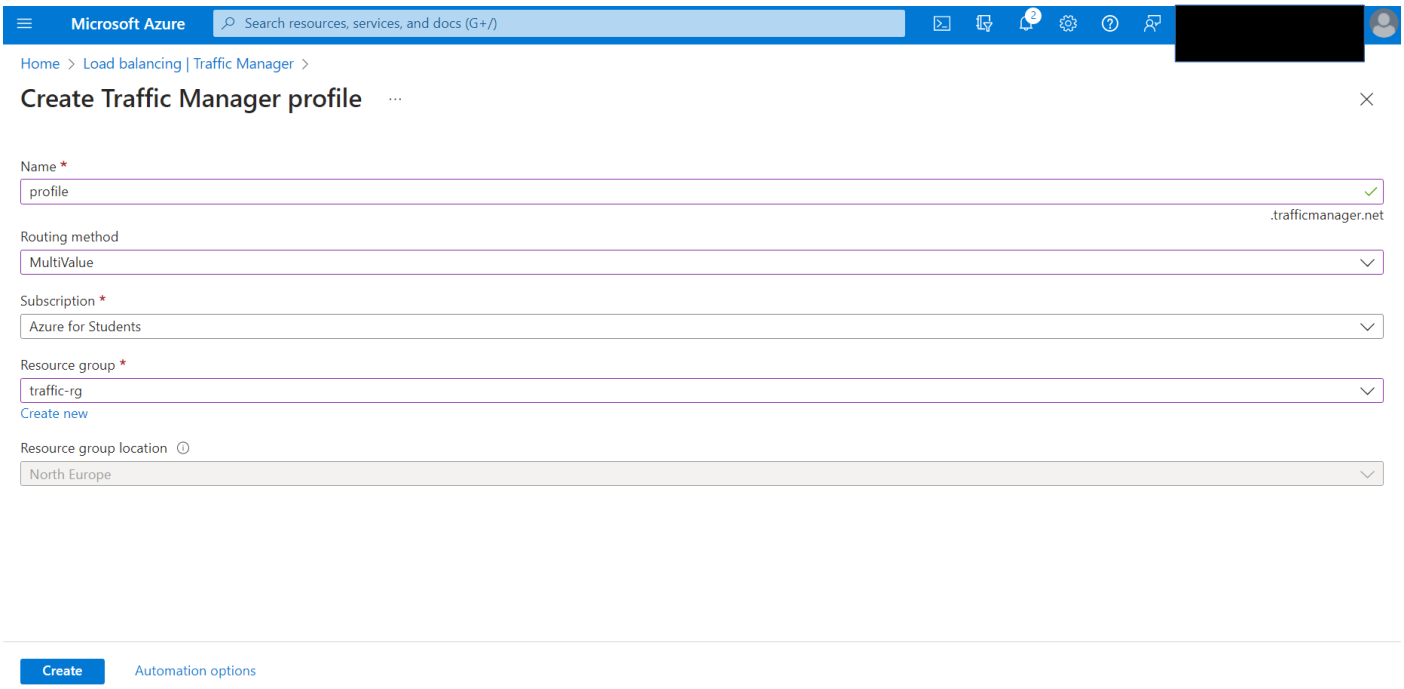
b-

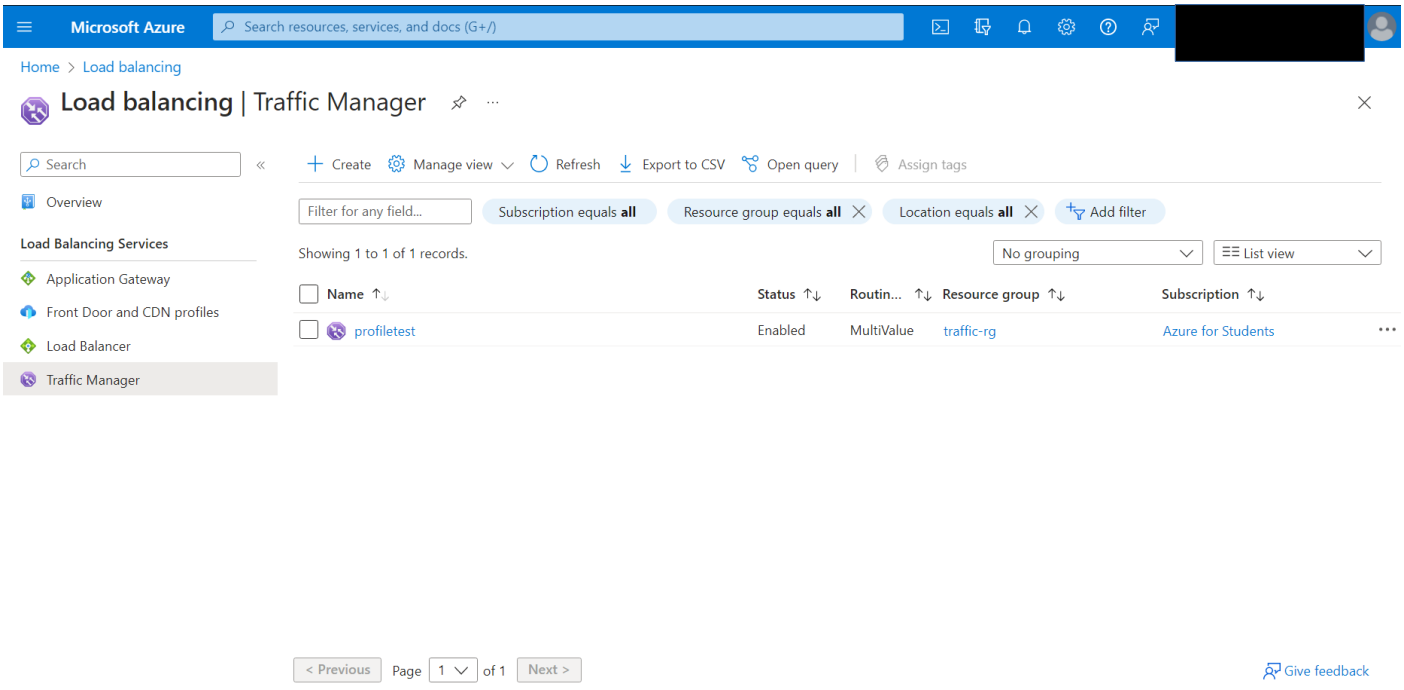

vm1 - 52.169.179.138:3389 - Connexion Bureau à distance
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
vm1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on vm1.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
Hide
vm1 - 52.169.179.138:3389 - Connexion Bureau à distance
Server Manager
Manage
Tools
View
Help
iisstart - Notepad
File Edit Format View Help
"This is the North Europe VM"
Windows (CRLF)
Ln 1, Col 30
100%
TASKS
TASKS
2 items
1 item selected 29 bytes


vm2 - 51.105.58.98:3389 - Connexion Bureau à distance
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Serve
All Servers
File and St
IIS
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
vm2
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on vm2.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel
Hide
1

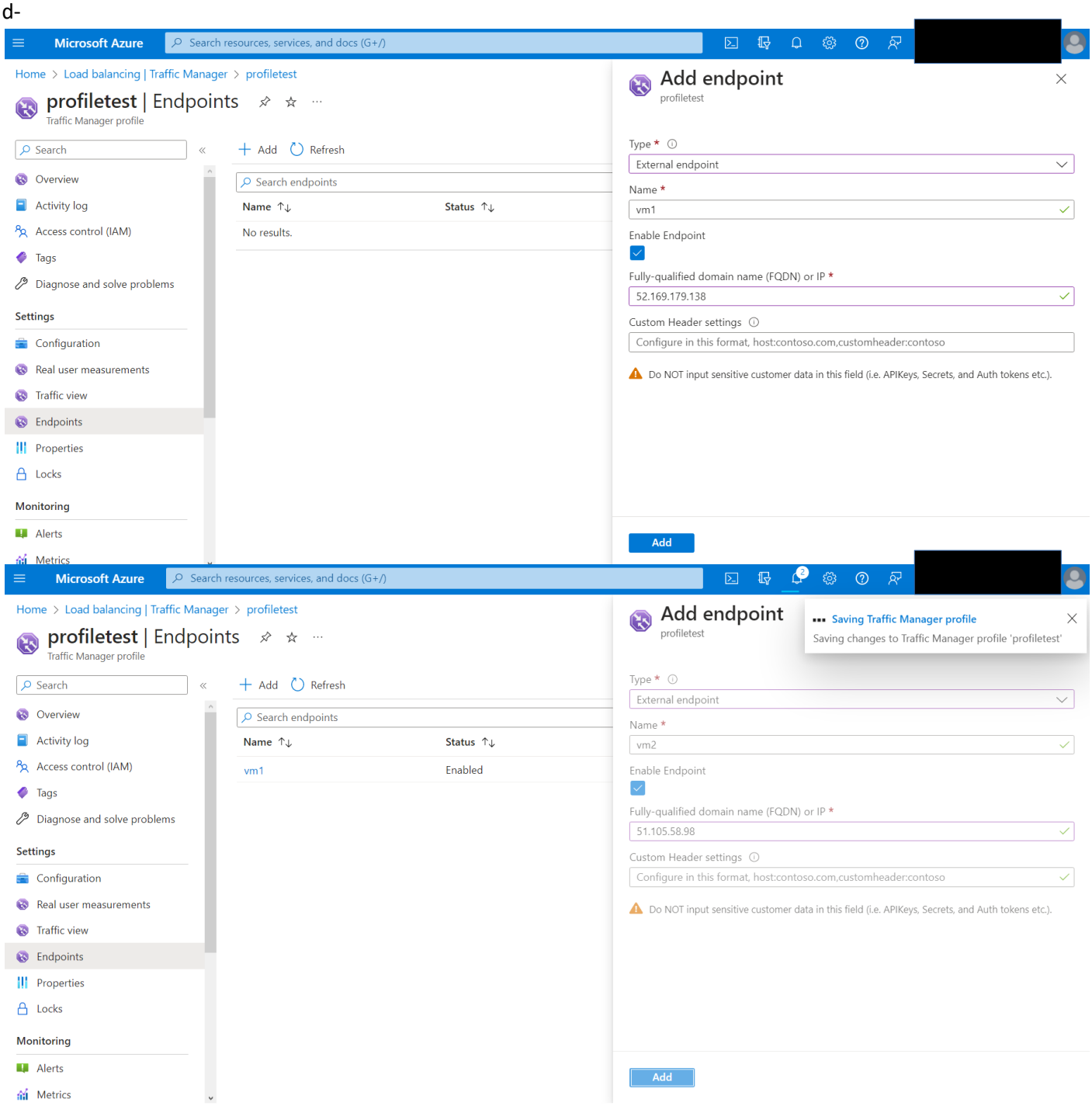

vm2 - 51.105.58.98:3389 - Connexion Bureau à distance
Server Manager
Internet Information Services (IIS) Manager
wwwroot
iisstart - Notepad
File Edit Format View Help
"This is the UK South VM"
Windows (CRLF)
Ln 1, Col 1
100%
Manage
Tools
View
Help
TASKS
Ready
2 items
1 item selected 25 bytes

C-

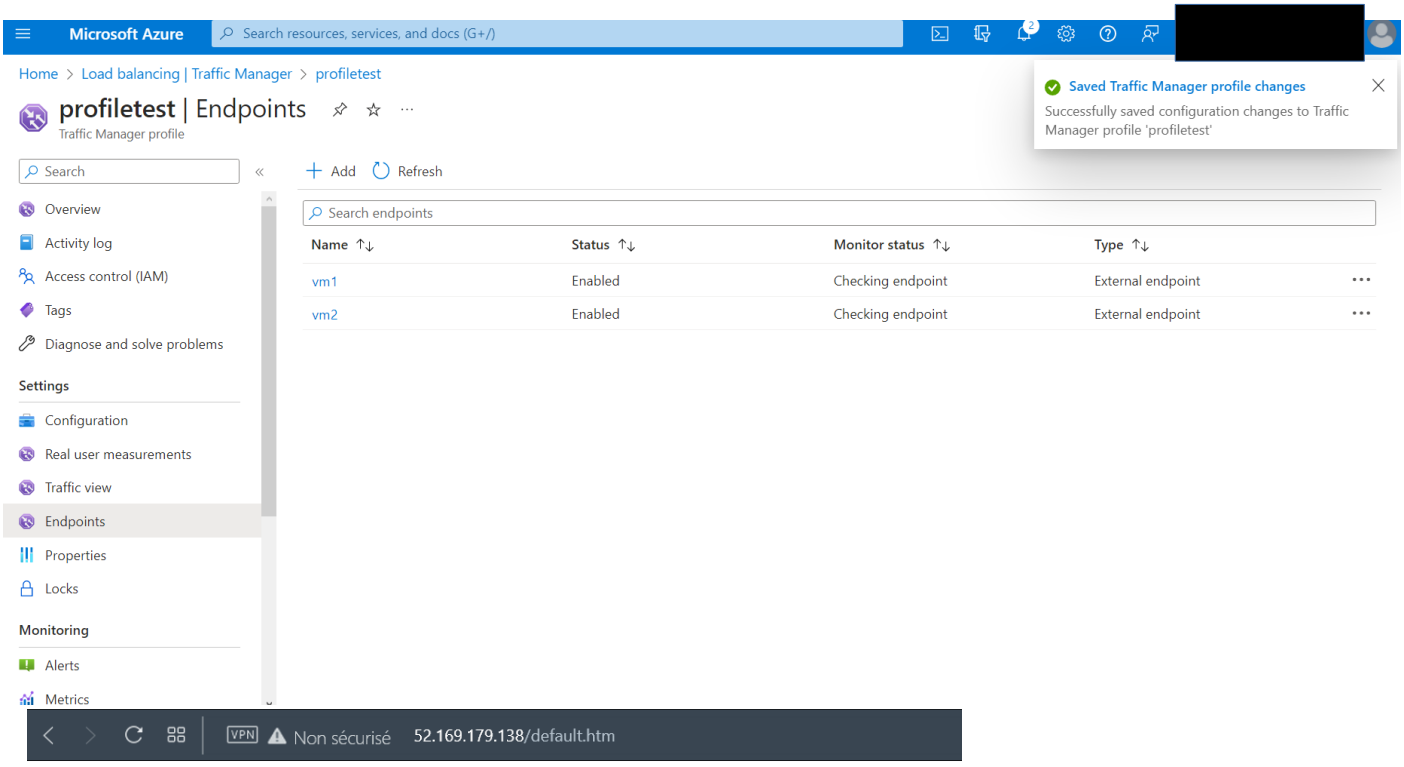

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing | Traffic Manager >
Create Traffic Manager profile
Name *
profile
.trafficmanager.net
Routing method
MultiValue
Subscription *
Azure for Students
Resource group *
traffic-rg
Create new
Resource group location
North Europe
Create
Automation options


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing
Load balancing | Traffic Manager
Search
Overview
Load Balancing Services
Application Gateway
Front Door and CDN profiles
Load Balancer
Traffic Manager
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Filter for any field...
Subscription equals all
Resource group equals all
Location equals all
Add filter
Showing 1 to 1 of 1 records.
No grouping
List view
Name
Status
Routin...
Resource group
Subscription
profiletest
Enabled
MultiValue
traffic-rg
Azure for Students
< Previous
Page 1 of 1
Next >
Give feedback

d-

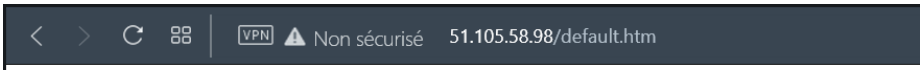

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing | Traffic Manager > profiletest
profiletest | Endpoints
Traffic Manager profile
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Real user measurements
Traffic view
Endpoints
Properties
Locks
Monitoring
Alerts
Metrics
Add
Refresh
Search endpoints
Name
Status
No results.
Add endpoint
profiletest
Type *
External endpoint
Name *
vm1
Enable Endpoint
Fully-qualified domain name (FQDN) or IP *
52.169.179.138
Custom Header settings
Configure in this format, host:contoso.com,customheader:contoso
Do NOT input sensitive customer data in this field (i.e. APIKeys, Secrets, and Auth tokens etc.).
Add

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Load balancing | Traffic Manager > profiletest
profiletest | Endpoints
Traffic Manager profile
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Real user measurements
Traffic view
Endpoints
Properties
Locks
Monitoring
Alerts
Metrics
Add
Refresh
Search endpoints
Name
Status
vm1
Enabled
Add endpoint
profiletest
Saving Traffic Manager profile
Saving changes to Traffic Manager profile 'profiletest'
Type *
External endpoint
Name *
vm2
Enable Endpoint
Fully-qualified domain name (FQDN) or IP *
51.105.58.98
Custom Header settings
Configure in this format, host:contoso.com,customheader:contoso
Do NOT input sensitive customer data in this field (i.e. APIKeys, Secrets, and Auth tokens etc.).
Add

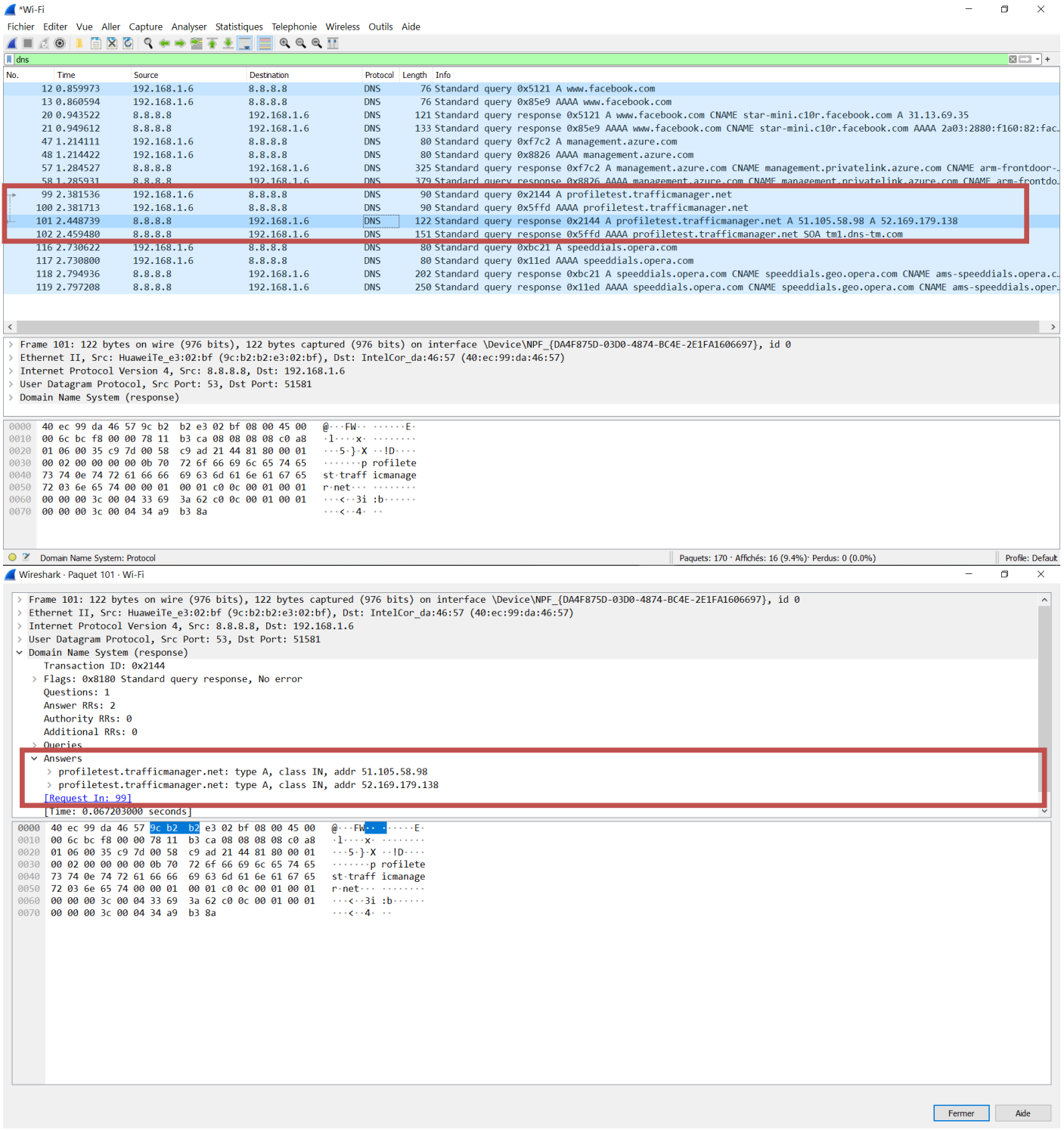


"This is the North Europe VM"

e-



"This is the UK South VM□


*Wi-Fi
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
dns
No. Time Source Destination Protocol Length Info
12 0.859973 192.168.1.6 8.8.8.8 DNS 76 Standard query 0x5121 A www.facebook.com
13 0.860594 192.168.1.6 8.8.8.8 DNS 76 Standard query 0x85e9 AAAA www.facebook.com
20 0.943522 8.8.8.8 192.168.1.6 DNS 121 Standard query response 0x5121 A www.facebook.com CNAME star-mini.c10r.facebook.com A 31.13.69.35
21 0.949612 8.8.8.8 192.168.1.6 DNS 133 Standard query response 0x85e9 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f160:82:fac
47 1.214111 192.168.1.6 8.8.8.8 DNS 80 Standard query 0xf7c2 A management.azure.com
48 1.214422 192.168.1.6 8.8.8.8 DNS 80 Standard query 0x8826 AAAA management.azure.com
57 1.284527 8.8.8.8 192.168.1.6 DNS 325 Standard query response 0xf7c2 A management.azure.com CNAME management.privatelink.azure.com CNAME arm-frontdoor-
58 1.285931 8.8.8.8 192.168.1.6 DNS 379 Standard query response 0x8826 AAAA management.azure.com CNAME management.privatelink.azure.com CNAME arm-frontdo
99 2.381536 192.168.1.6 8.8.8.8 DNS 90 Standard query 0x2144 A profiletest.trafficmanager.net
100 2.381713 192.168.1.6 8.8.8.8 DNS 90 Standard query 0x5ffd AAAA profiletest.trafficmanager.net
101 2.448739 8.8.8.8 192.168.1.6 DNS 122 Standard query response 0x2144 A profiletest.trafficmanager.net A 51.105.58.98 A 52.169.179.138
102 2.459480 8.8.8.8 192.168.1.6 DNS 151 Standard query response 0x5ffd AAAA profiletest.trafficmanager.net SOA tm1.dns-tm.com
116 2.730622 192.168.1.6 8.8.8.8 DNS 80 Standard query 0xbc21 A speeddials.opera.com
117 2.730800 192.168.1.6 8.8.8.8 DNS 80 Standard query 0x11ed AAAA speeddials.opera.com
118 2.794936 8.8.8.8 192.168.1.6 DNS 202 Standard query response 0xbc21 A speeddials.opera.com CNAME speeddials.geo.opera.com CNAME ams-speeddials.opera.c
119 2.797208 8.8.8.8 192.168.1.6 DNS 250 Standard query response 0x11ed AAAA speeddials.opera.com CNAME speeddials.geo.opera.com CNAME ams-speeddials.oper
Frame 101: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{DA4F875D-03D0-4874-BC4E-2E1FA1606697}, id 0
Ethernet II, Src: HuaweiTe_e3:02:bf (9c:b2:b2:e3:02:bf), Dst: IntelCor_da:46:57 (40:ec:99:da:46:57)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.6
User Datagram Protocol, Src Port: 53, Dst Port: 51581
Domain Name System (response)
0000 40 ec 99 da 46 57 9c b2 b2 e3 02 bf 08 00 45 00 @···FW·· ·····E·
0010 00 6c bc f8 00 00 78 11 b3 ca 08 08 08 08 c0 a8 ·l····x· ····
0020 01 06 00 35 c9 7d 00 58 c9 ad 21 44 81 80 00 01 ···5·}·X ··!D····
0030 00 02 00 00 00 00 0b 70 72 6f 66 69 6c 65 74 65 ·····p rofilete
0040 73 74 0e 74 72 61 66 66 69 63 6d 61 6e 61 67 65 st·traff icmanage
0050 72 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 01 r·net··· ····
0060 00 00 00 3c 00 04 33 69 3a 62 c0 0c 00 01 00 01 ···<··3i :b·····
0070 00 00 00 3c 00 04 34 a9 b3 8a ···<··4· ··
Domain Name System: Protocol
Paquets: 170 · Affichés: 16 (9.4%) · Perdus: 0 (0.0%)
Profile: Default
Wireshark · Paquet 101 · Wi-Fi
Frame 101: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{DA4F875D-03D0-4874-BC4E-2E1FA1606697}, id 0
Ethernet II, Src: HuaweiTe_e3:02:bf (9c:b2:b2:e3:02:bf), Dst: IntelCor_da:46:57 (40:ec:99:da:46:57)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.1.6
User Datagram Protocol, Src Port: 53, Dst Port: 51581
Domain Name System (response)
Transaction ID: 0x2144
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
Answers
profiletest.trafficmanager.net: type A, class IN, addr 51.105.58.98
profiletest.trafficmanager.net: type A, class IN, addr 52.169.179.138
[Request In: 99]
[Time: 0.067203000 seconds]
0000 40 ec 99 da 46 57 9c b2 b2 e3 02 bf 08 00 45 00 @···FW·· ·····E·
0010 00 6c bc f8 00 00 78 11 b3 ca 08 08 08 08 c0 a8 ·l····x· ····
0020 01 06 00 35 c9 7d 00 58 c9 ad 21 44 81 80 00 01 ···5·}·X ··!D····
0030 00 02 00 00 00 00 0b 70 72 6f 66 69 6c 65 74 65 ·····p rofilete
0040 73 74 0e 74 72 61 66 66 69 63 6d 61 6e 61 67 65 st·traff icmanage
0050 72 03 6e 65 74 00 00 01 00 01 c0 0c 00 01 00 01 r·net··· ····
0060 00 00 00 3c 00 04 33 69 3a 62 c0 0c 00 01 00 01 ···<··3i :b·····
0070 00 00 00 3c 00 04 34 a9 b3 8a ···<··4· ··
Fermer
Aide

2-

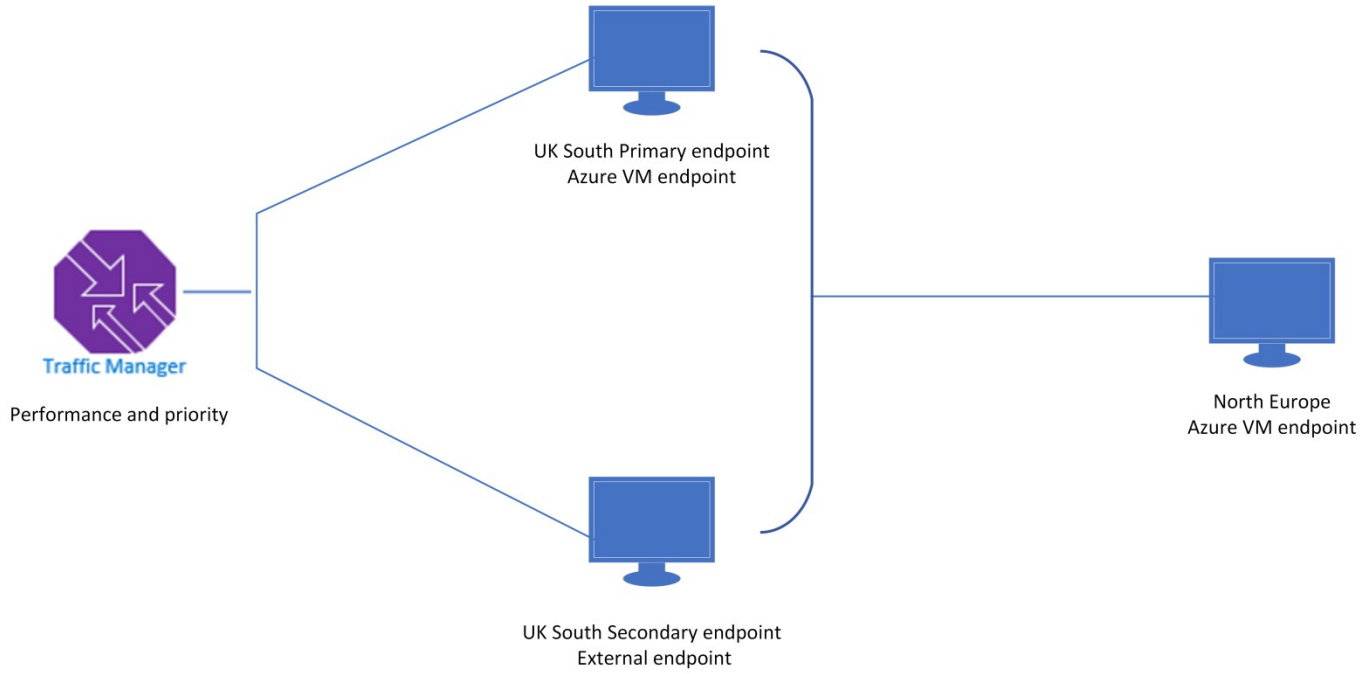
Scenario:

- one Azure virtual machine in North Europe
- two other Azure virtual machines in UK South.
- users directed to ➔ endpoints in the UK South location
  ➔ or to ➔ endpoint in the North Europe location,
  (based on the location that is closest to the users)

But, in the UK South location:

Method that helps to direct traffic to ➔ secondary endpoint
(if the primary one is not available)

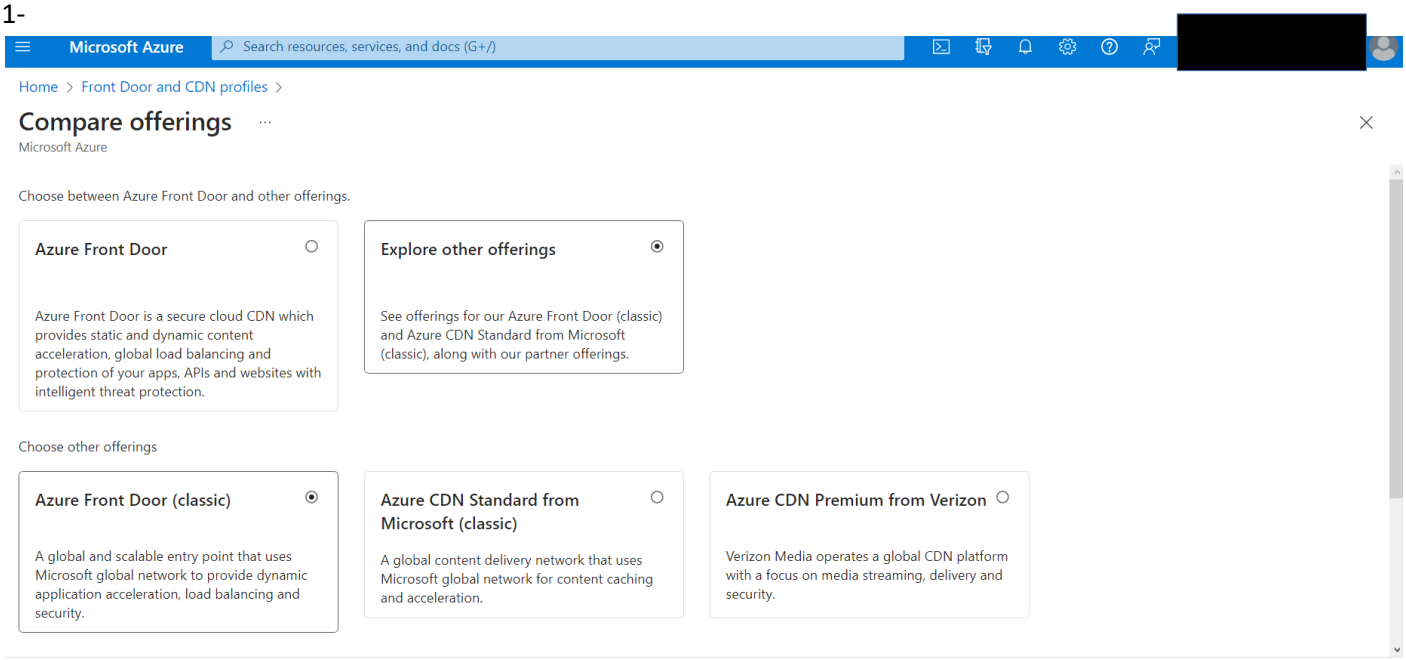
- Schéma d'architecture du scenario proposé :

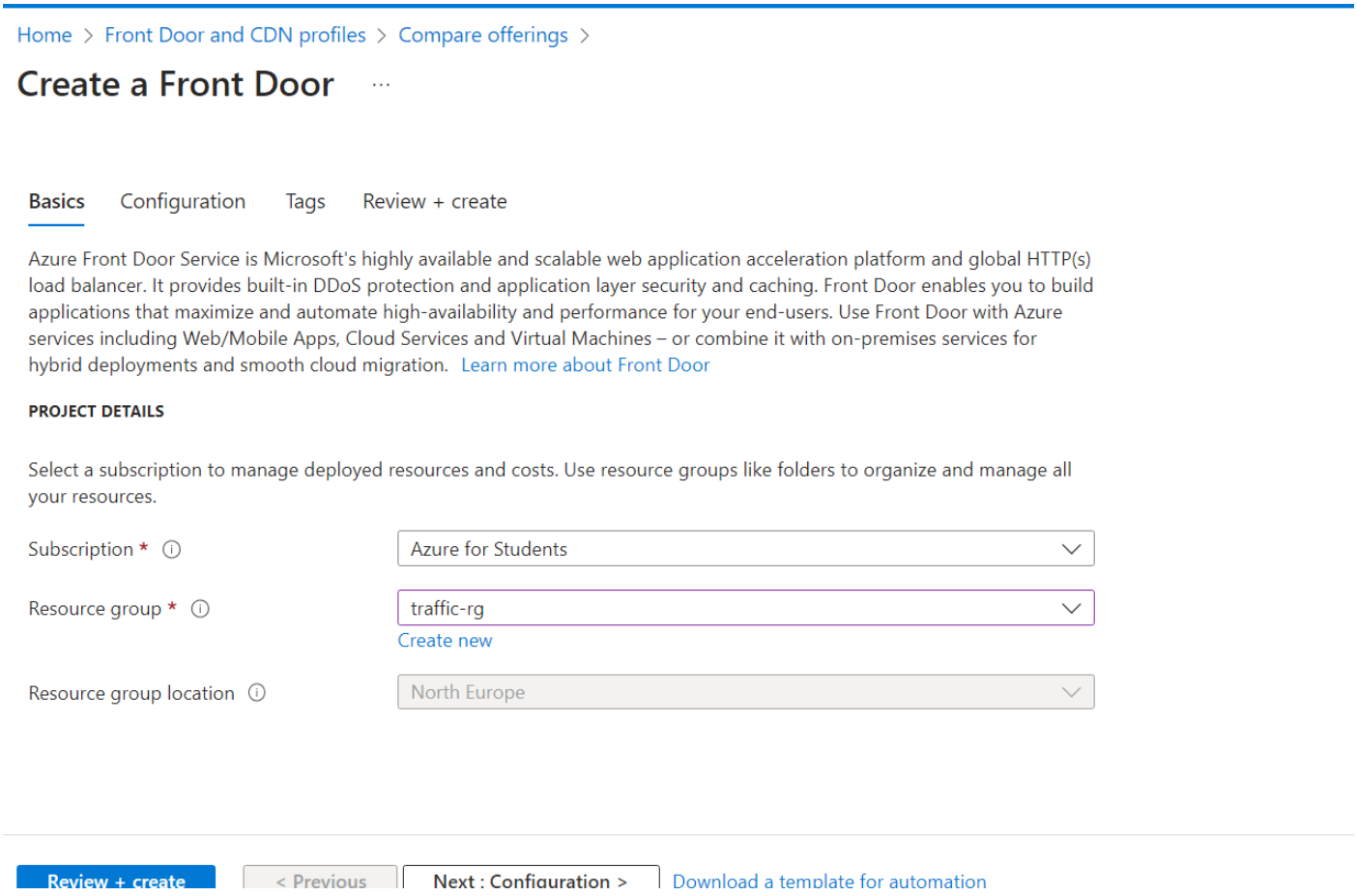


- En effet, pour établir le routage basé sur la location la plus proche aux utilisateurs, le 'Trafic manager' va utiliser la méthode de routage « Performance » (où on fait le routage en mesurant la latency la plus petite des utilisateurs).
- Pour établir le routage vers le secondaire endpoint d'UK south si le primaire n'est pas joignable, le 'Traffic Manager Profile' va utiliser la méthode de routage « Priority » en routant le traffic vers le primaire endpoint. S'il n'est pas joignable il va ensuite router le traffic vers le secondaire endpoint.

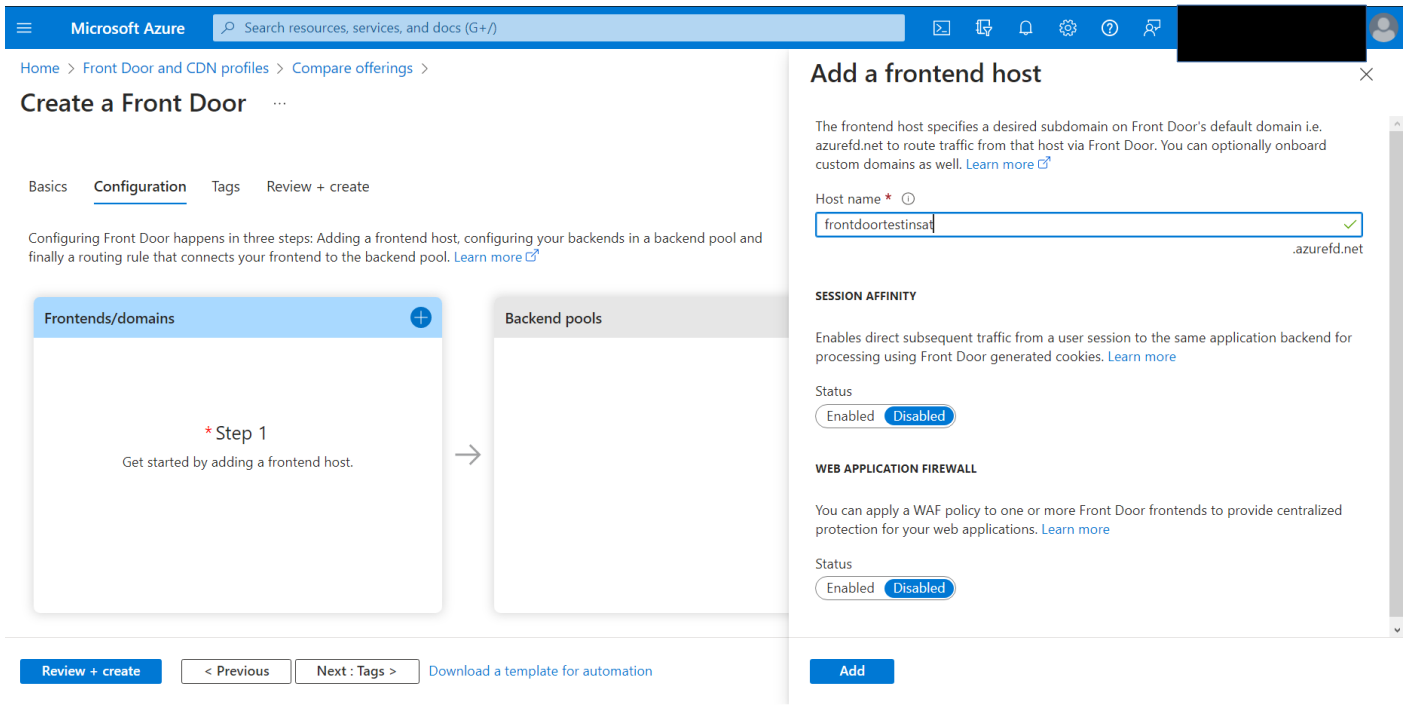
Task 2 : Azure front door

1-

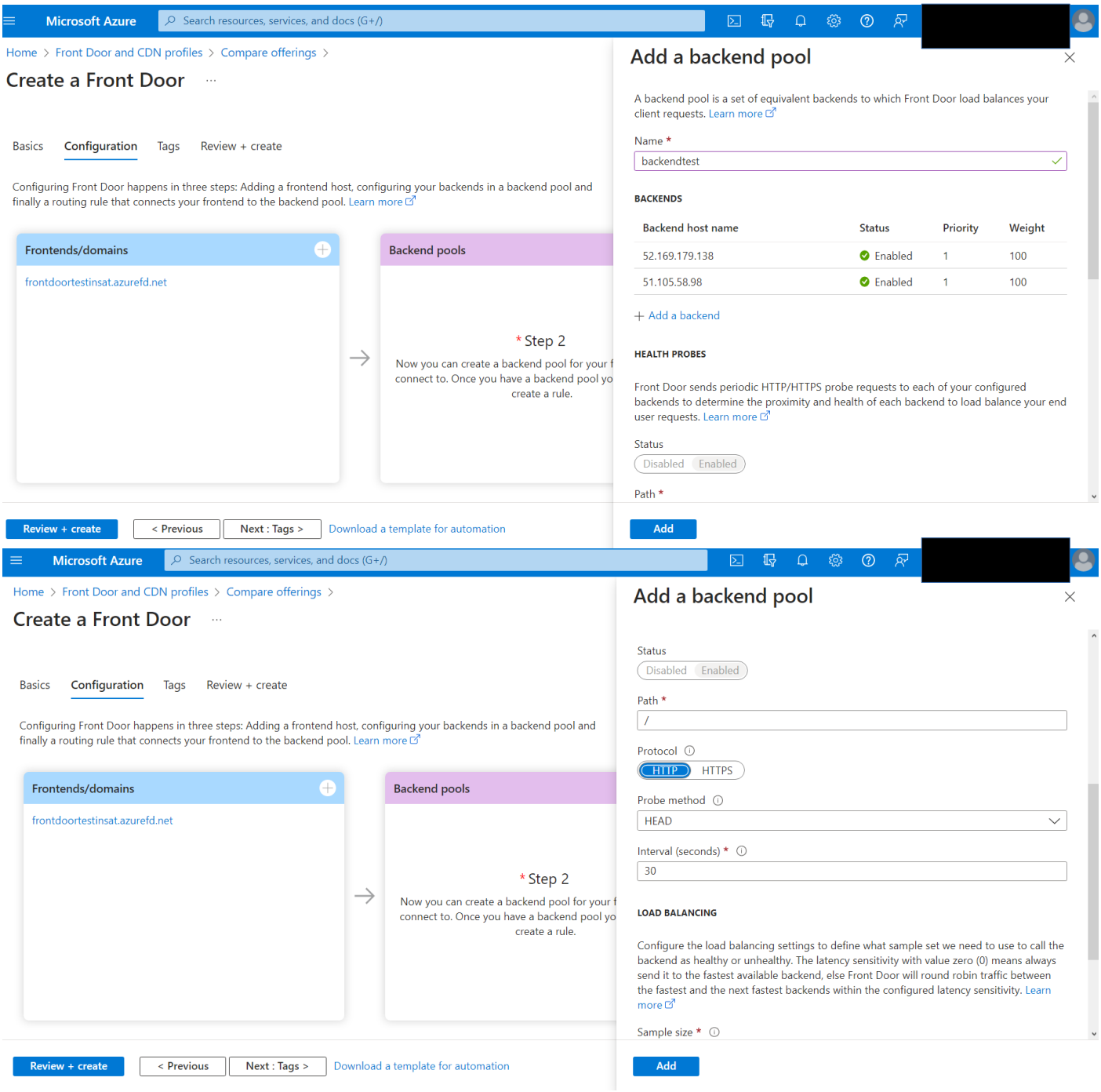




a-

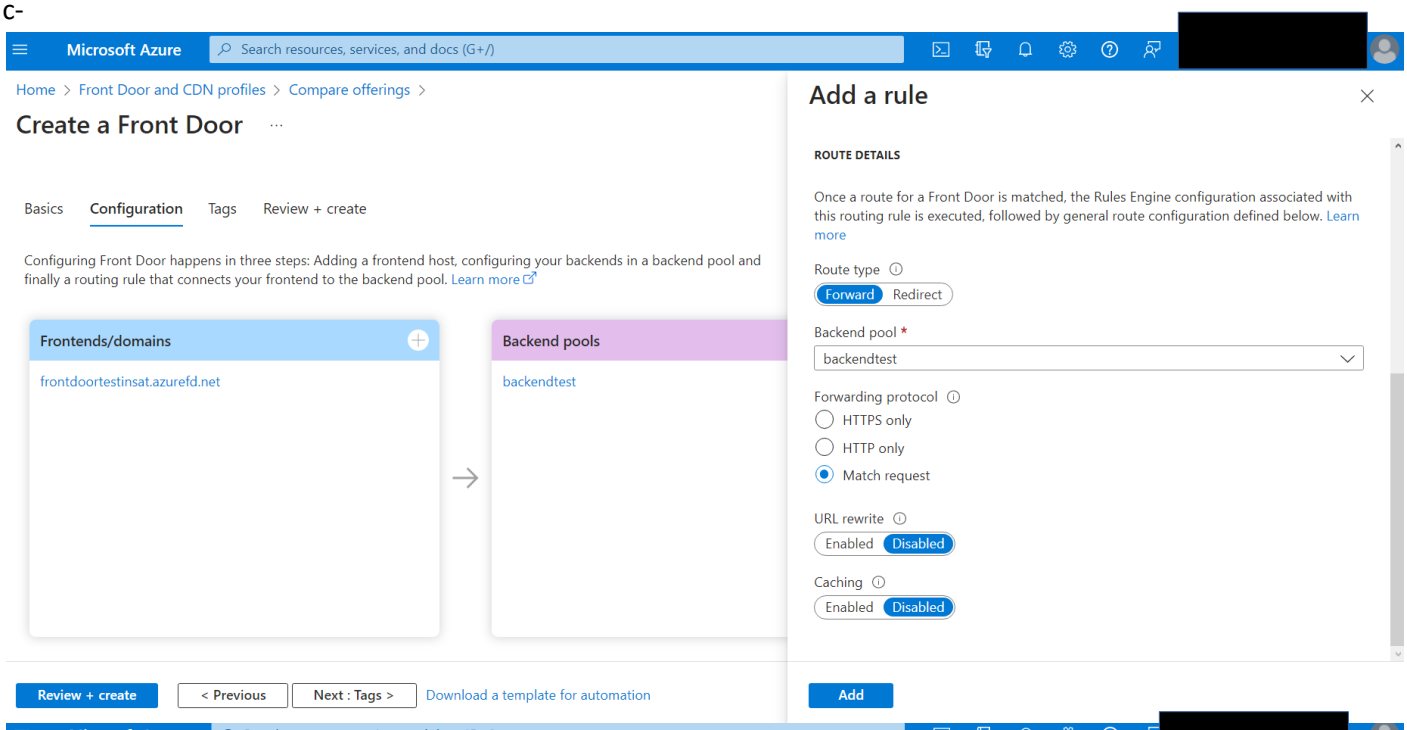

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
Frontends/domains
Backend pools
* Step 1
Get started by adding a frontend host.
Review + create
< Previous
Next : Tags >
Download a template for automation
Add a frontend host
The frontend host specifies a desired subdomain on Front Door's default domain i.e. azurefd.net to route traffic from that host via Front Door. You can optionally onboard custom domains as well. Learn more
Host name *
frontdoortestinsat
.azurefd.net
SESSION AFFINITY
Enables direct subsequent traffic from a user session to the same application backend for processing using Front Door generated cookies. Learn more
Status
Enabled
Disabled
WEB APPLICATION FIREWALL
You can apply a WAF policy to one or more Front Door frontends to provide centralized protection for your web applications. Learn more
Status
Enabled
Disabled
Add

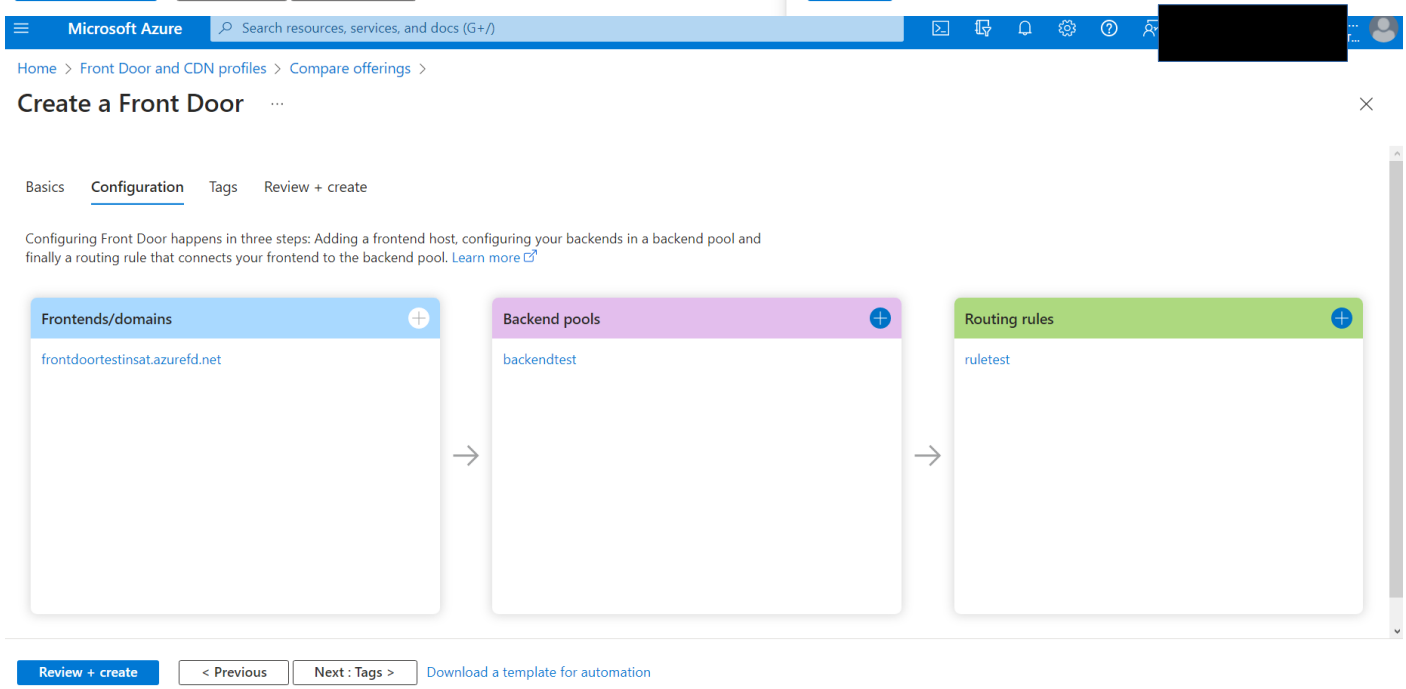
b-

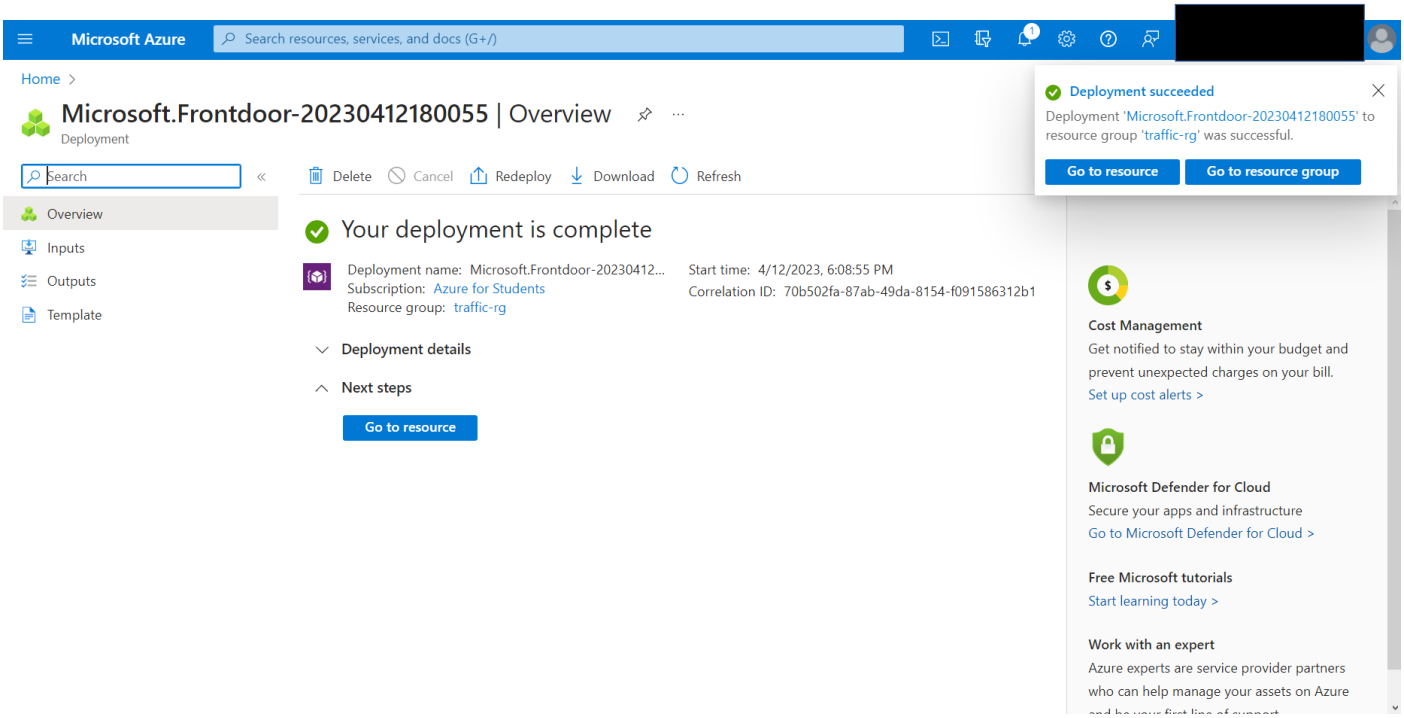

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
Frontends/domains
frontdoortestinsat.azurefd.net
Backend pools
* Step 2
Now you can create a backend pool for your f
connect to. Once you have a backend pool yo
create a rule.
Review + create
< Previous
Next : Tags >
Download a template for automation
Add a backend pool
A backend pool is a set of equivalent backends to which Front Door load balances your client requests. Learn more
Name *
backendtest
BACKENDS
Backend host name
Status
Priority
Weight
52.169.179.138
Enabled
1
100
51.105.58.98
Enabled
1
100
Add a backend
HEALTH PROBES
Front Door sends periodic HTTP/HTTPS probe requests to each of your configured backends to determine the proximity and health of each backend to load balance your end user requests. Learn more
Status
Disabled
Enabled
Path *
Add

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
Frontends/domains
frontdoortestinsat.azurefd.net
Backend pools
* Step 2
Now you can create a backend pool for your f
connect to. Once you have a backend pool yo
create a rule.
Review + create
< Previous
Next : Tags >
Download a template for automation
Add a backend pool
Status
Disabled
Enabled
Path *
/
Protocol
HTTP
HTTPS
Probe method
HEAD
Interval (seconds) *
30
LOAD BALANCING
Configure the load balancing settings to define what sample set we need to use to call the backend as healthy or unhealthy. The latency sensitivity with value zero (0) means always send it to the fastest available backend, else Front Door will round robin traffic between the fastest and the next fastest backends within the configured latency sensitivity. Learn more
Sample size *
Add

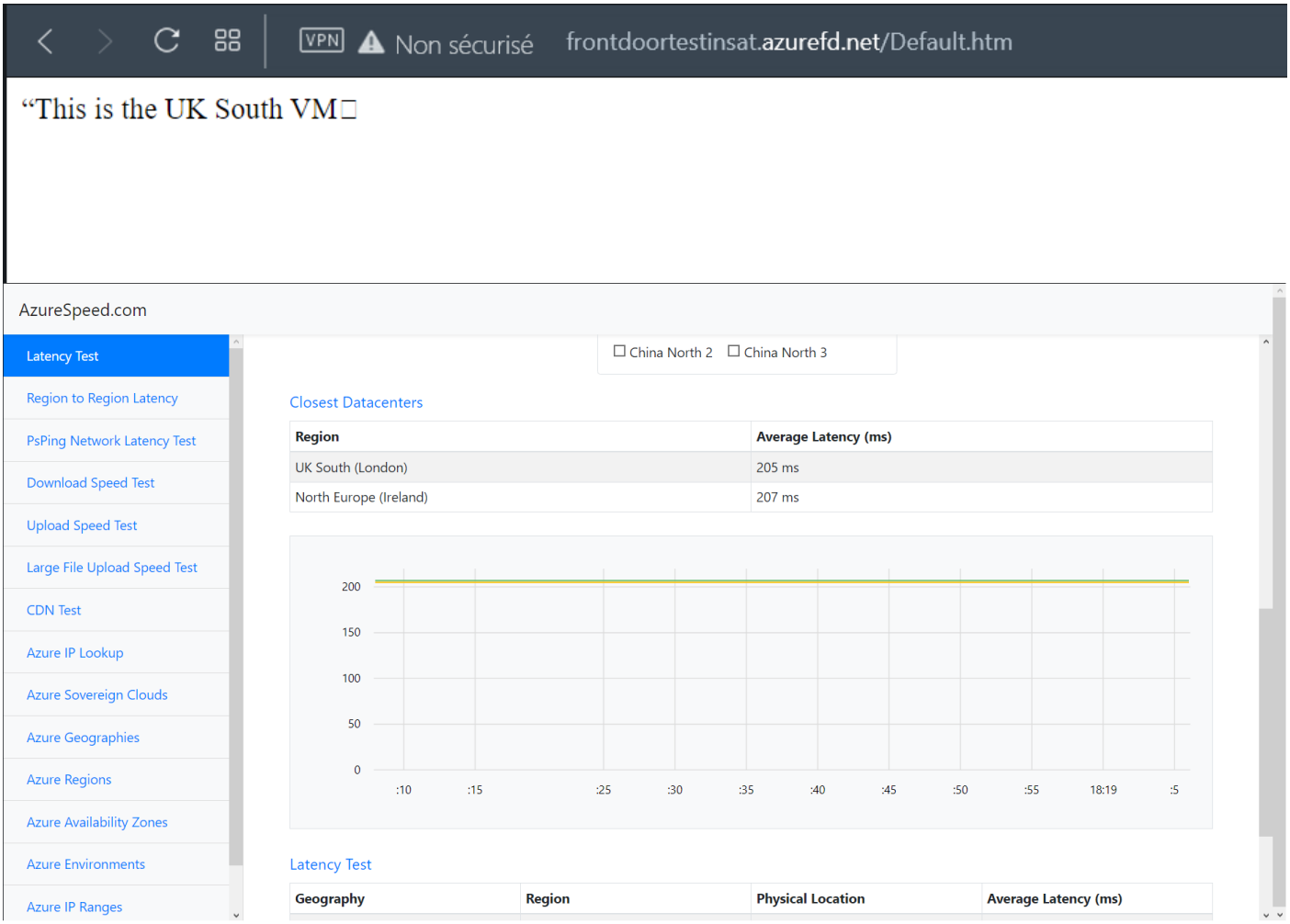
C-


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
Frontends/domains
frontdoortestinsat.azurefd.net
Backend pools
backendtest
Review + create
< Previous
Next : Tags >
Download a template for automation
Add a rule
ROUTE DETAILS
Once a route for a Front Door is matched, the Rules Engine configuration associated with this routing rule is executed, followed by general route configuration defined below. Learn more
Route type
Forward
Redirect
Backend pool *
backendtest
Forwarding protocol
HTTPS only
HTTP only
Match request
URL rewrite
Enabled
Disabled
Caching
Enabled
Disabled
Add


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Front Door and CDN profiles > Compare offerings >
Create a Front Door
Basics
Configuration
Tags
Review + create
Configuring Front Door happens in three steps: Adding a frontend host, configuring your backends in a backend pool and finally a routing rule that connects your frontend to the backend pool. Learn more
Frontends/domains
frontdoortestinsat.azurefd.net
Backend pools
backendtest
Routing rules
ruletest
Review + create
< Previous
Next : Tags >
Download a template for automation



2-

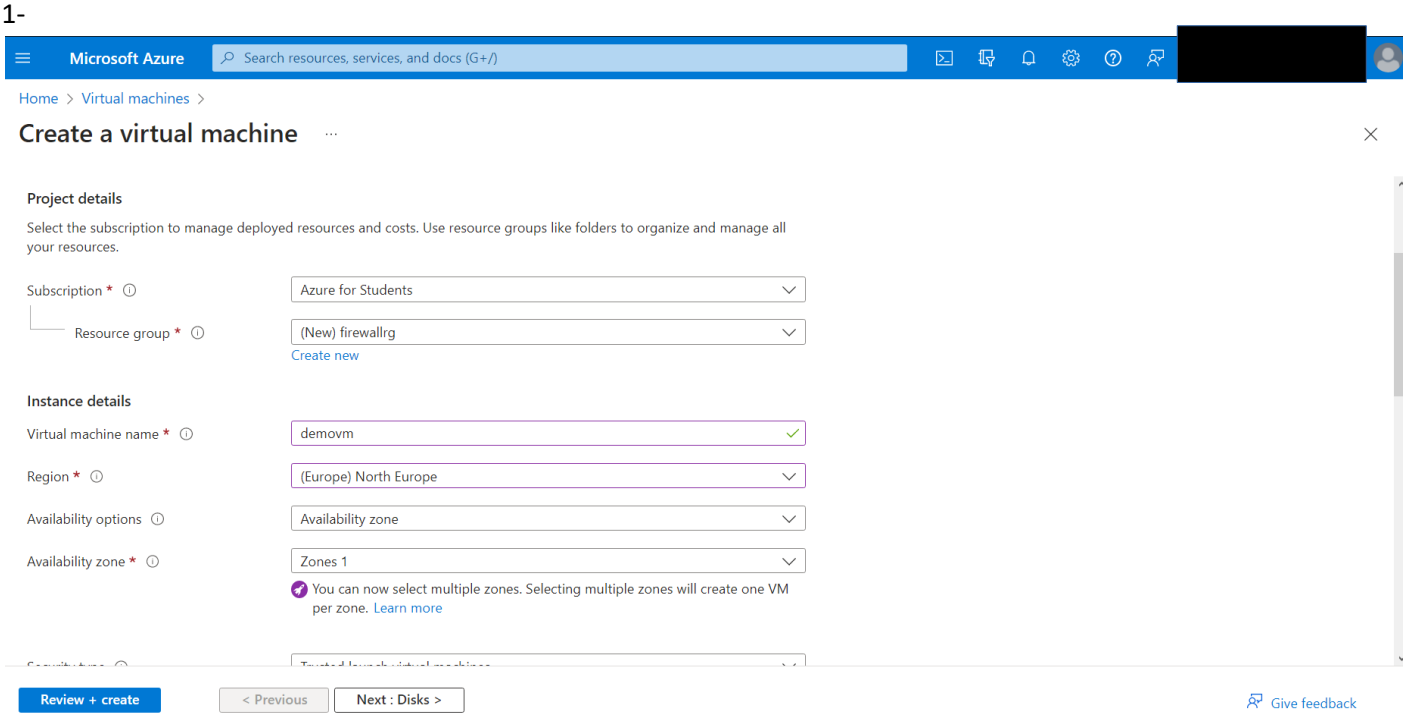


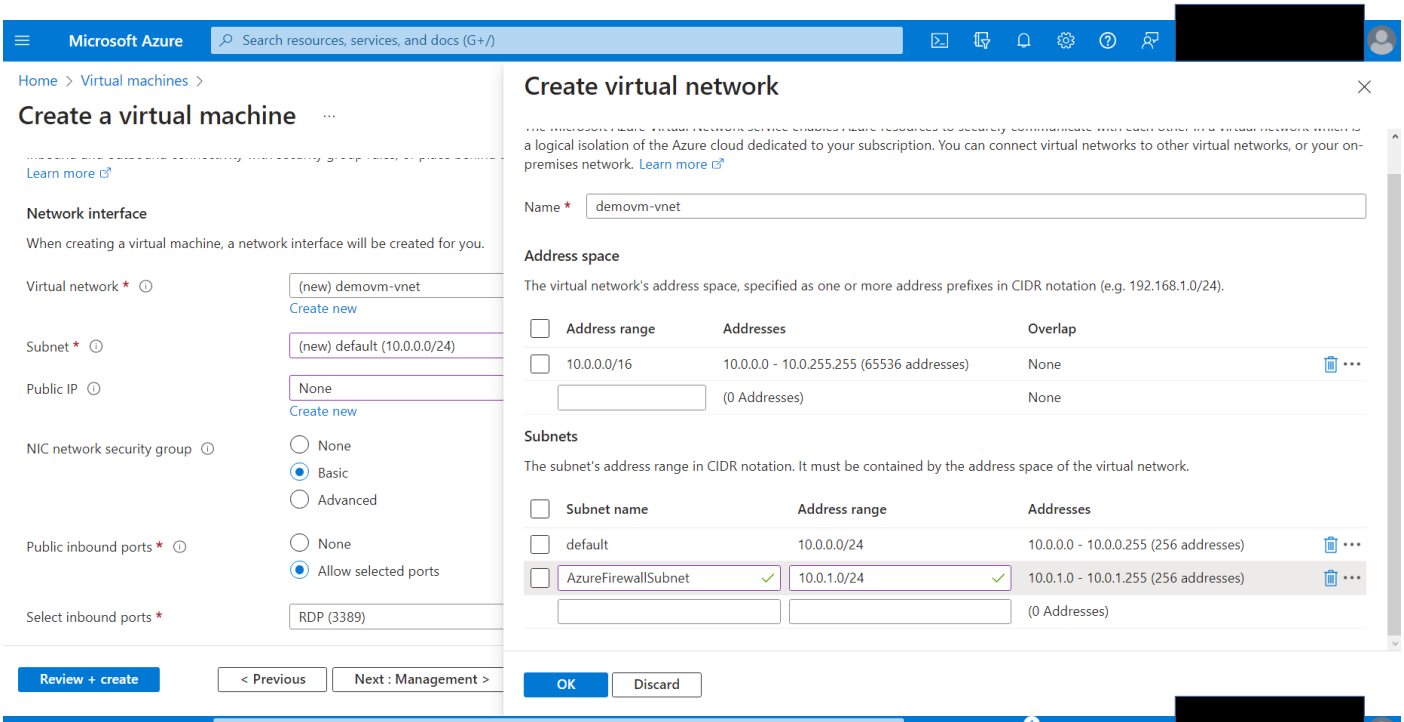
➔ Le VM localize en "UK south" a été choisi car le "Front Door a utilisé son algorithme de routage intelligent pour faire le routage du traffic http issu par un client vers le « Backend » ayant la plus petite valeur de « latency » qui varie selon la location du client. Pour ce cas, on a « UK south » Latency vaut 205ms et « North Europe » Latency vaut 207ms donc il est logique de choisir « UK south » (205 ms < 207 ms). Si on parle avec plus de détails, lors de la réception d'une requête du client, le « Front Door » vérifie la location du client et sélectionne le « Backend » ayant

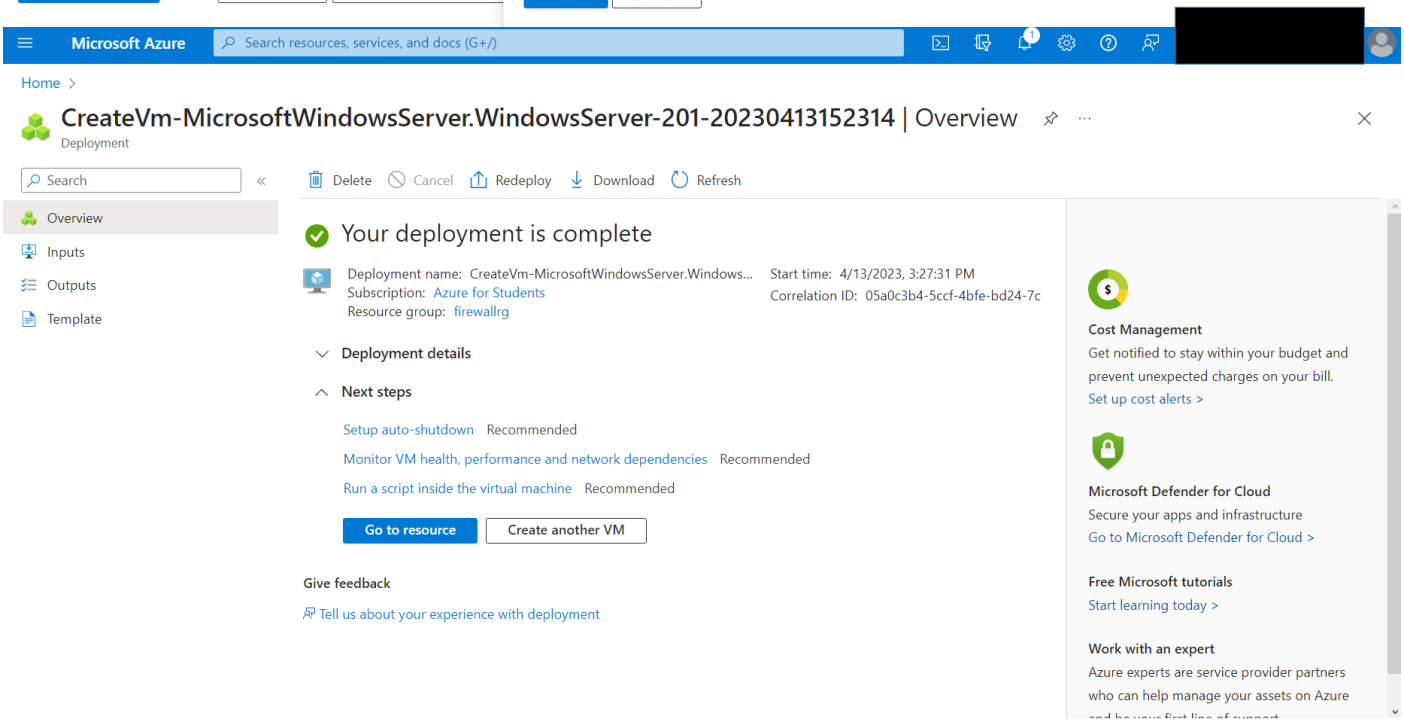
la plus faible « Latency ». Ceci est en effet réalisable en se basant sur le « POP – Nearest point of presence » qui signifie un point ou une location physique où deux appareils de communications se connectent d'un emplacement vers le reste de l'internet, en utilisant une technologie de routage « anycast » qui fait le routage vers le « POP ». La technologie « Anycast » signifie une méthode d'adressage et de routage où les requêtes peuvent être routés vers une variété de locations ou nœuds différents (si on parle d'un contexte de CDN, elle signifie alors le routage du traffic entrant vers le plus proche 'data center' qui peut traiter les requêtes convenablement).

Task 3 : Azure Firewall

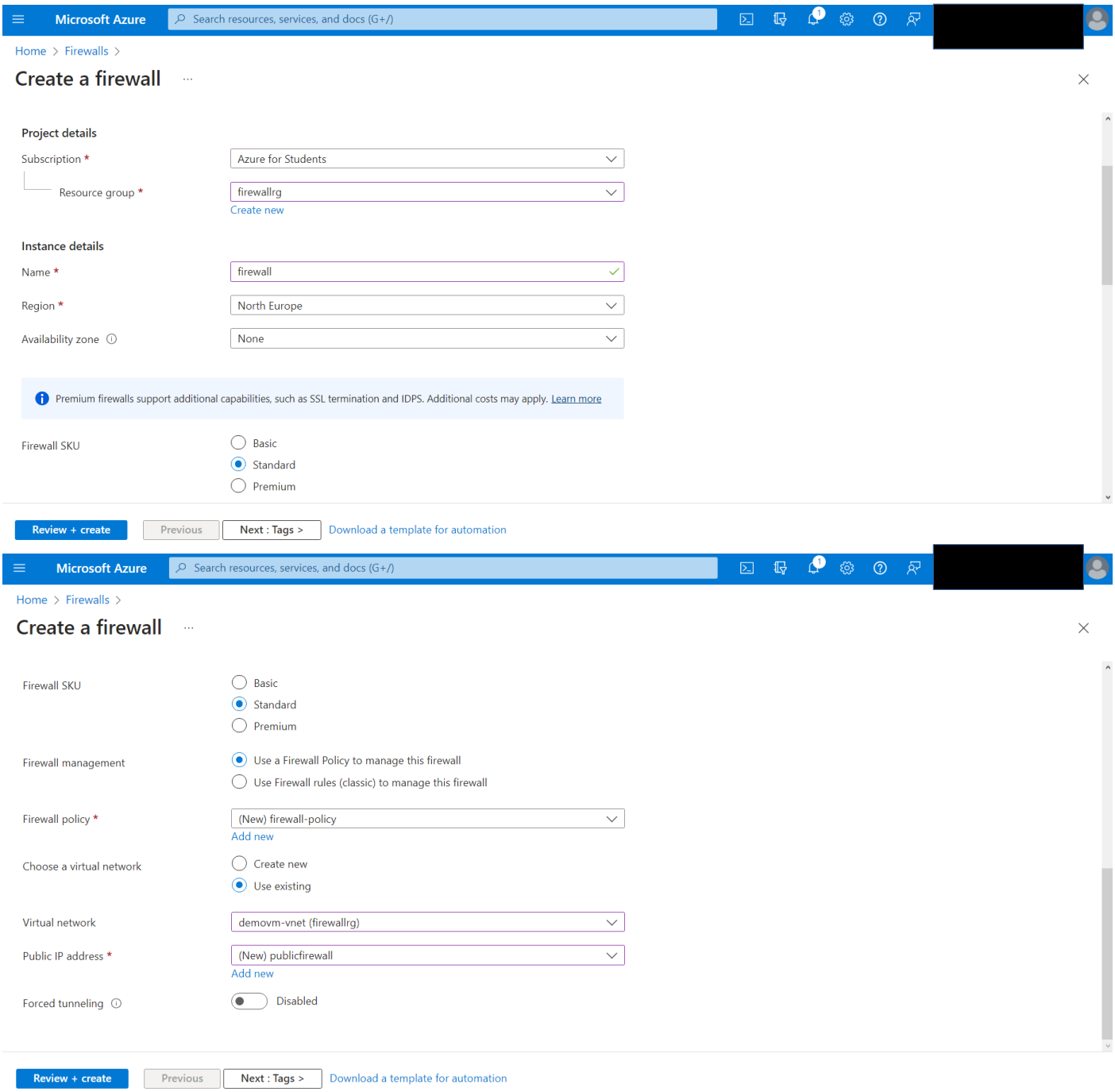
1-



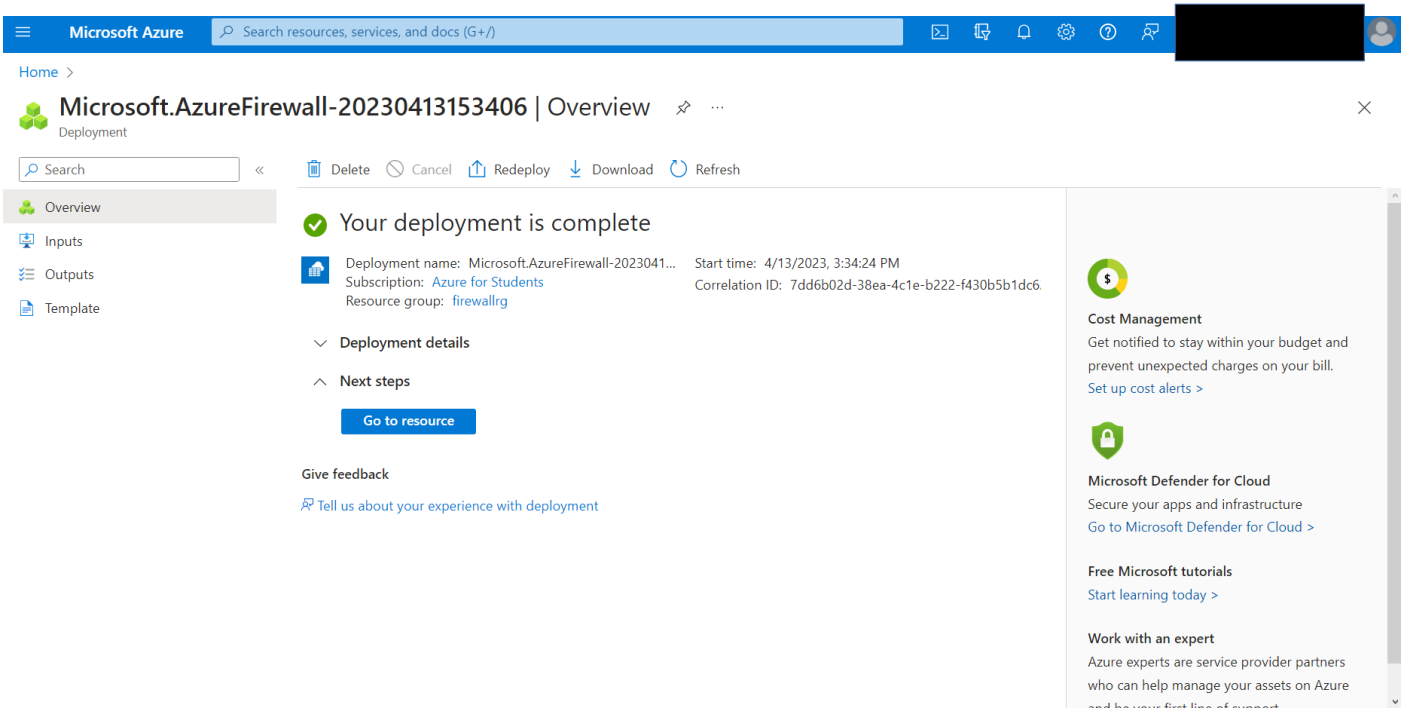

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual machines >
Create a virtual machine
Learn more
Network interface
When creating a virtual machine, a network interface will be created for you.
Virtual network *
(new) demovm-vnet
Create new
Subnet *
(new) default (10.0.0.0/24)
Public IP
None
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
Allow selected ports
Select inbound ports *
RDP (3389)
Review + create
< Previous
Next : Management >
Create virtual network
a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more
Name *
demovm-vnet
Address space
The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).
Address range
Addresses
Overlap
10.0.0.0/16
10.0.0.0 - 10.0.255.255 (65536 addresses)
None
(0 Addresses)
None
Subnets
The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.
Subnet name
Address range
Addresses
default
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (256 addresses)
AzureFirewallSubnet
10.0.1.0/24
10.0.1.0 - 10.0.1.255 (256 addresses)
(0 Addresses)
OK
Discard


Microsoft Azure
Search resources, services, and docs (G+/)
Home >
CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230413152314 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: CreateVm-MicrosoftWindowsServer.Windows...
Subscription: Azure for Students
Resource group: firewallrg
Start time: 4/13/2023, 3:27:31 PM
Correlation ID: 05a0c3b4-5ccf-4bfe-bd24-7c
Deployment details
Next steps
Setup auto-shutdown Recommended
Monitor VM health, performance and network dependencies Recommended
Run a script inside the virtual machine Recommended
Go to resource
Create another VM
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure

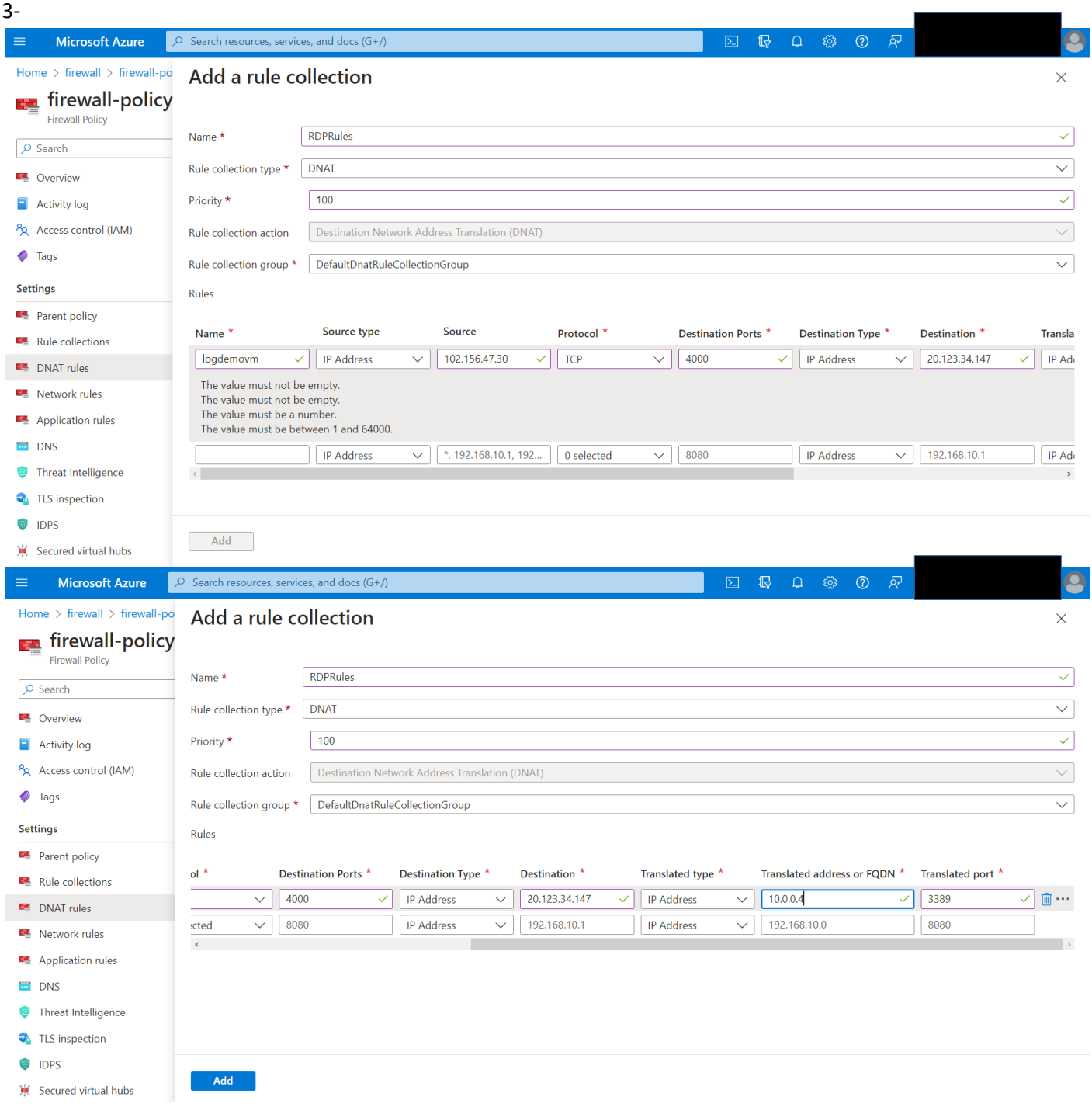
2-


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Firewalls >
Create a firewall
Project details
Subscription *
Azure for Students
Resource group *
firewallrg
Create new
Instance details
Name *
firewall
Region *
North Europe
Availability zone
None
Premium firewalls support additional capabilities, such as SSL termination and IDPS. Additional costs may apply. Learn more
Firewall SKU
Basic
Standard
Premium
Review + create
Previous
Next : Tags >
Download a template for automation

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Firewalls >
Create a firewall
Firewall SKU
Basic
Standard
Premium
Firewall management
Use a Firewall Policy to manage this firewall
Use Firewall rules (classic) to manage this firewall
Firewall policy *
(New) firewall-policy
Add new
Choose a virtual network
Create new
Use existing
Virtual network
demovm-vnet (firewallrg)
Public IP address *
(New) publicfirewall
Add new
Forced tunneling
Disabled
Review + create
Previous
Next : Tags >
Download a template for automation


Microsoft Azure
Search resources, services, and docs (G+/)
Home
Microsoft.AzureFirewall-20230413153406 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: Microsoft.AzureFirewall-2023041...
Subscription: Azure for Students
Resource group: firewallrg
Start time: 4/13/2023, 3:34:24 PM
Correlation ID: 7dd6b02d-38ea-4c1e-b222-f430b5b1dc6
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners who can help manage your assets on Azure

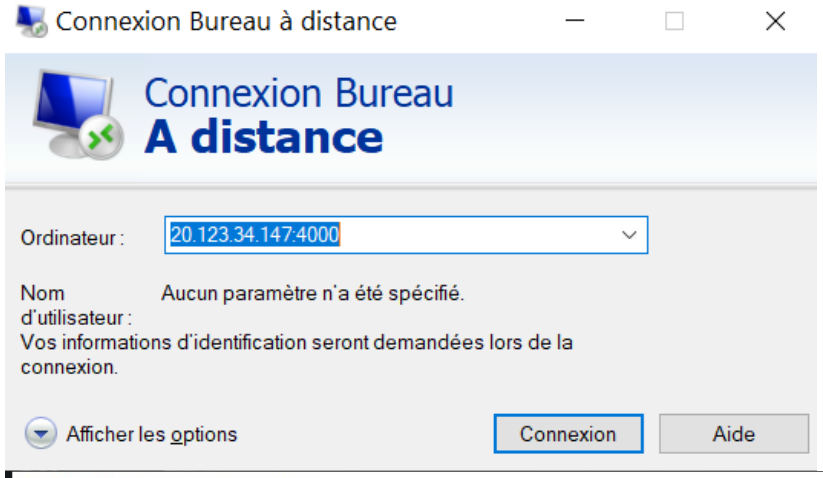
3-

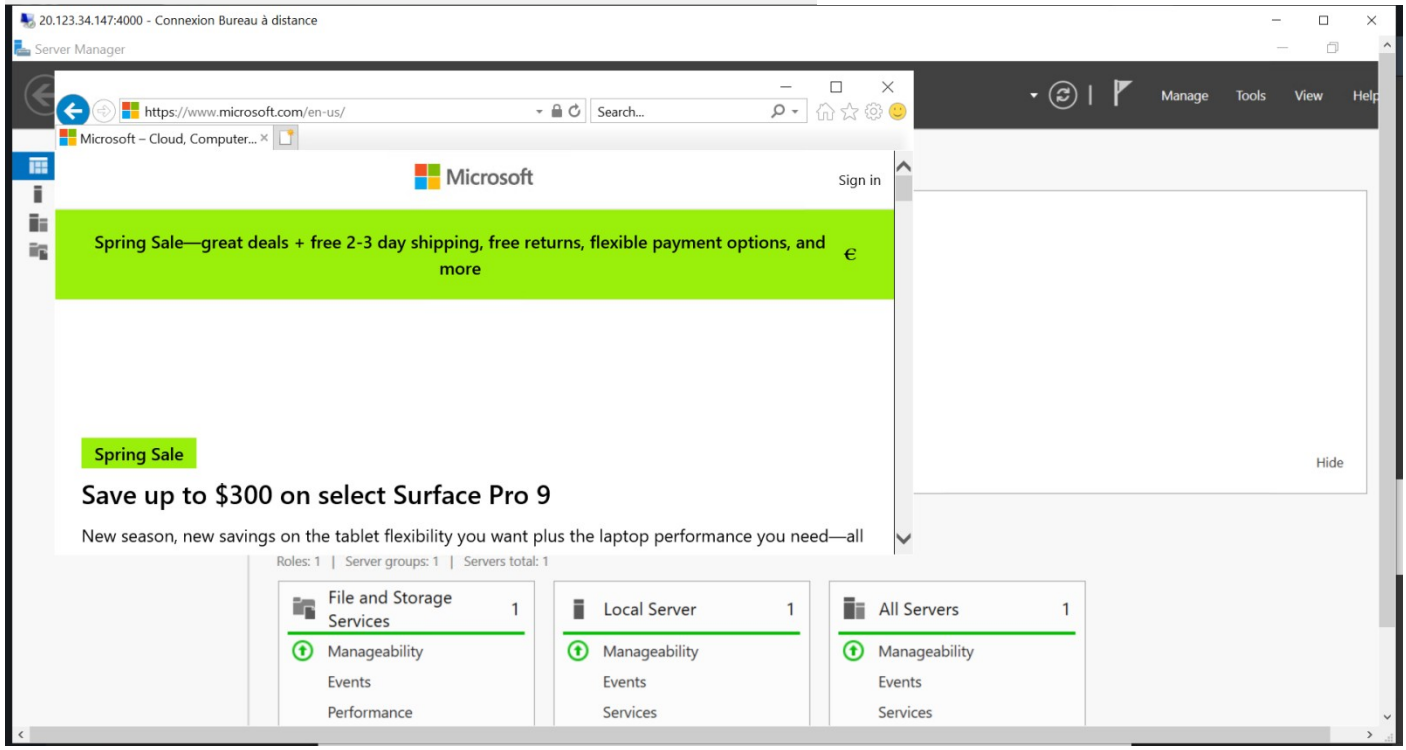

Microsoft Azure
Search resources, services, and docs (G+/)
Home > firewall > firewall-po
firewall-policy
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Add a rule collection
Name *
RDPRules
Rule collection type *
DNAT
Priority *
100
Rule collection action
Destination Network Address Translation (DNAT)
Rule collection group *
DefaultDnatRuleCollectionGroup
Rules
Name *
Source type
Source
Protocol *
Destination Ports *
Destination Type *
Destination *
Transla
logdemovm
IP Address
102.156.47.30
TCP
4000
IP Address
20.123.34.147
The value must not be empty.
The value must not be empty.
The value must be a number.
The value must be between 1 and 64000.
IP Address
*, 192.168.10.1, 192...
0 selected
8080
IP Address
192.168.10.1
Add

Microsoft Azure
Search resources, services, and docs (G+/)
Home > firewall > firewall-po
firewall-policy
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Add a rule collection
Name *
RDPRules
Rule collection type *
DNAT
Priority *
100
Rule collection action
Destination Network Address Translation (DNAT)
Rule collection group *
DefaultDnatRuleCollectionGroup
Rules
Destination Ports *
Destination Type *
Destination *
Translated type *
Translated address or FQDN *
Translated port *
4000
IP Address
20.123.34.147
IP Address
10.0.0.4
3389
8080
IP Address
192.168.10.1
IP Address
192.168.10.0
8080
Add

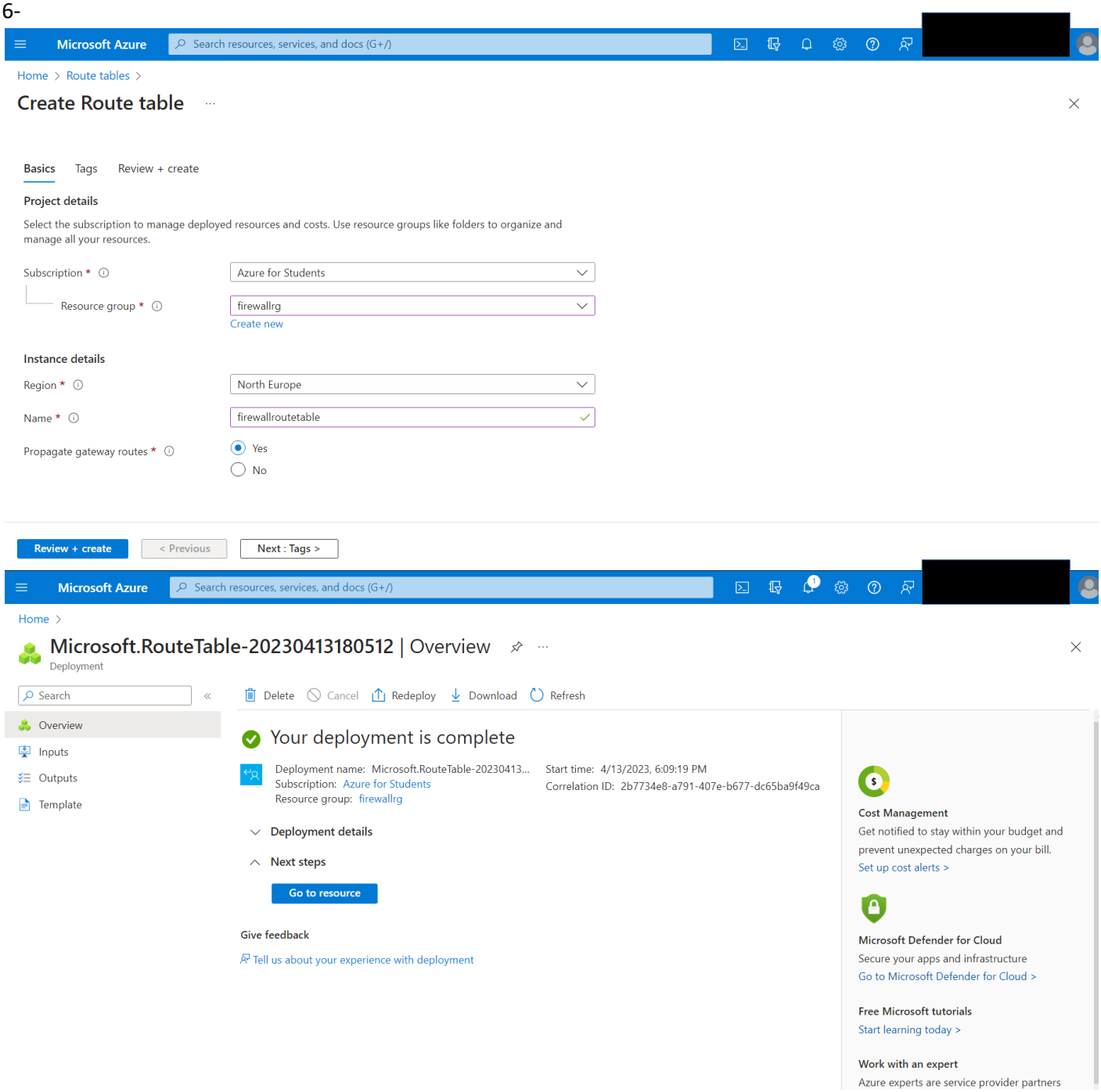
4-

5-


Connexion Bureau à distance
Connexion Bureau
A distance
Ordinateur :
20.123.34.147:4000
Nom d'utilisateur :
Aucun paramètre n'a été spécifié.
Vos informations d'identification seront demandées lors de la connexion.
Afficher les options
Connexion
Aide

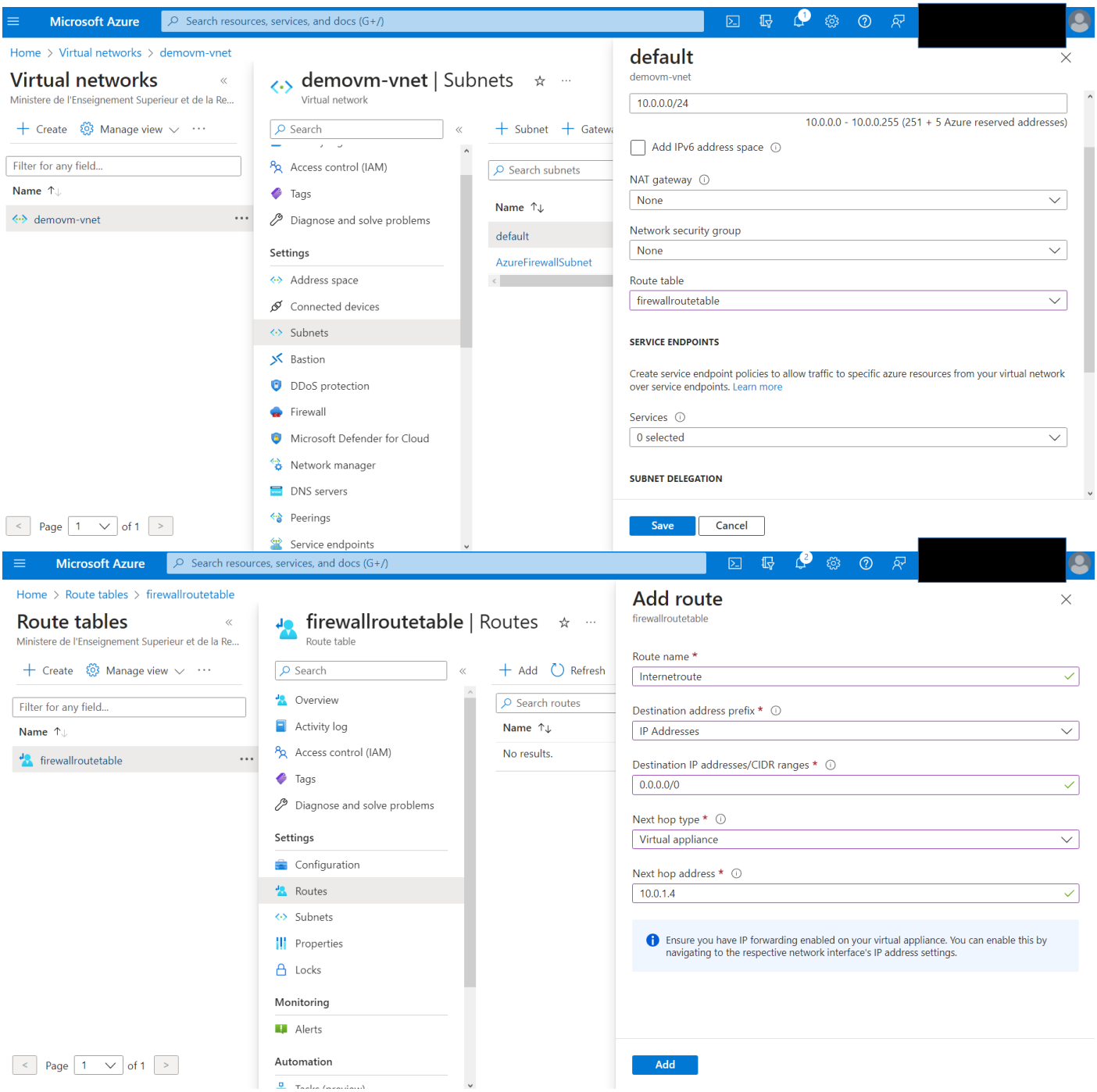

20.123.34.147:4000 - Connexion Bureau à distance
Server Manager
Manage
Tools
View
Help
https://www.microsoft.com/en-us/
Search...
Microsoft – Cloud, Computer...
Microsoft
Sign in
Spring Sale—great deals + free 2-3 day shipping, free returns, flexible payment options, and more
Spring Sale
Save up to $300 on select Surface Pro 9
New season, new savings on the tablet flexibility you want plus the laptop performance you need—all
Hide
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services
1
Manageability
Events
Performance
Local Server
1
Manageability
Events
Services
All Servers
1
Manageability
Events
Services

6-

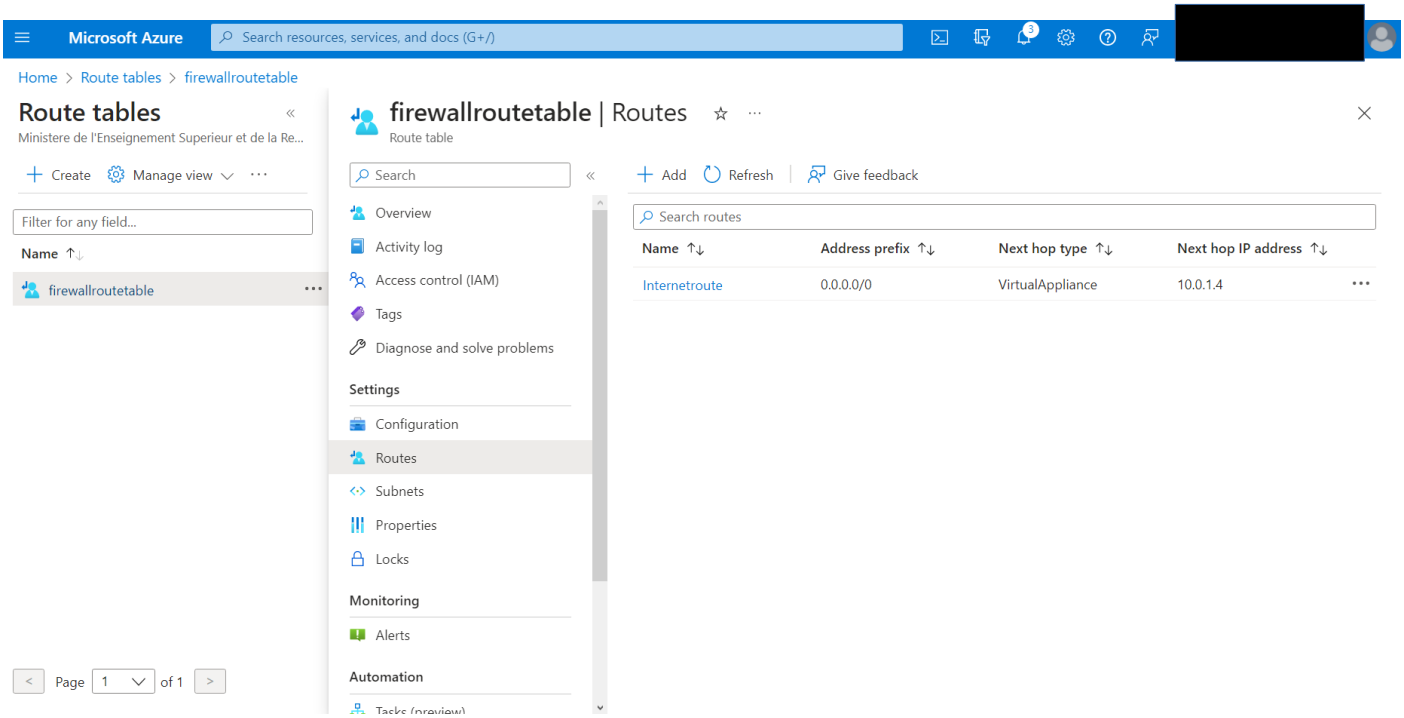

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Route tables >
Create Route table
Basics
Tags
Review + create
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
Azure for Students
Resource group *
firewallrg
Create new
Instance details
Region *
North Europe
Name *
firewallroutetable
Propagate gateway routes *
Yes
No
Review + create
< Previous
Next : Tags >

Microsoft Azure
Search resources, services, and docs (G+/)
Home >
Microsoft.RouteTable-20230413180512 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Your deployment is complete
Deployment name: Microsoft.RouteTable-20230413...
Subscription: Azure for Students
Resource group: firewallrg
Start time: 4/13/2023, 6:09:19 PM
Correlation ID: 2b7734e8-a791-407e-b677-dc65ba9f49ca
Deployment details
Next steps
Go to resource
Give feedback
Tell us about your experience with deployment
Cost Management
Get notified to stay within your budget and prevent unexpected charges on your bill.
Set up cost alerts >
Microsoft Defender for Cloud
Secure your apps and infrastructure
Go to Microsoft Defender for Cloud >
Free Microsoft tutorials
Start learning today >
Work with an expert
Azure experts are service provider partners

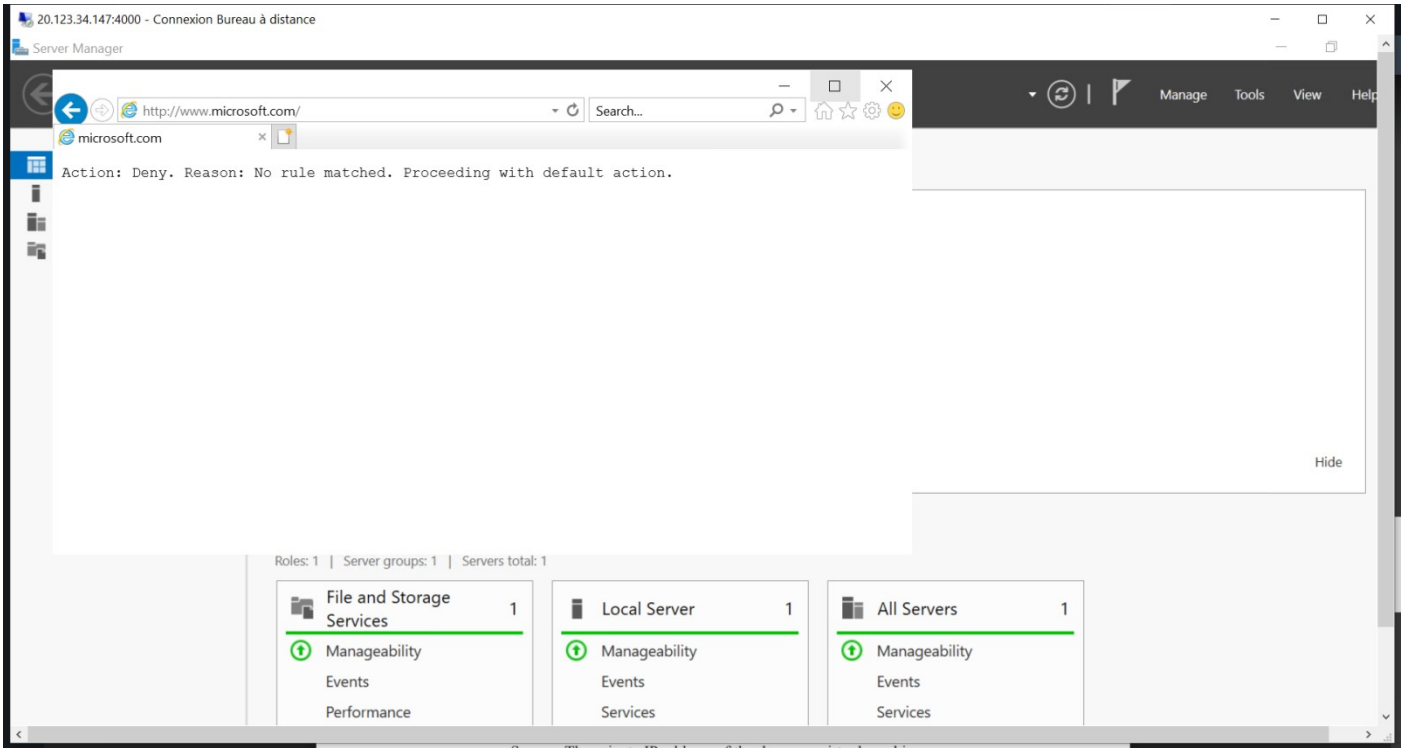
7-


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks > demovm-vnet
Virtual networks
Ministere de l'Enseignement Superieur et de la Re...
Create
Manage view
Filter for any field...
Name
demovm-vnet
Page 1 of 1
demovm-vnet | Subnets
Virtual network
Search
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS servers
Peerings
Service endpoints
Subnet
Search subnets
Name
default
AzureFirewallSubnet
default
demovm-vnet
10.0.0.0/24
10.0.0.0 - 10.0.0.255 (251 + 5 Azure reserved addresses)
Add IPv6 address space
NAT gateway
None
Network security group
None
Route table
firewallroutetable
SERVICE ENDPOINTS
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Services
0 selected
SUBNET DELEGATION
Save
Cancel

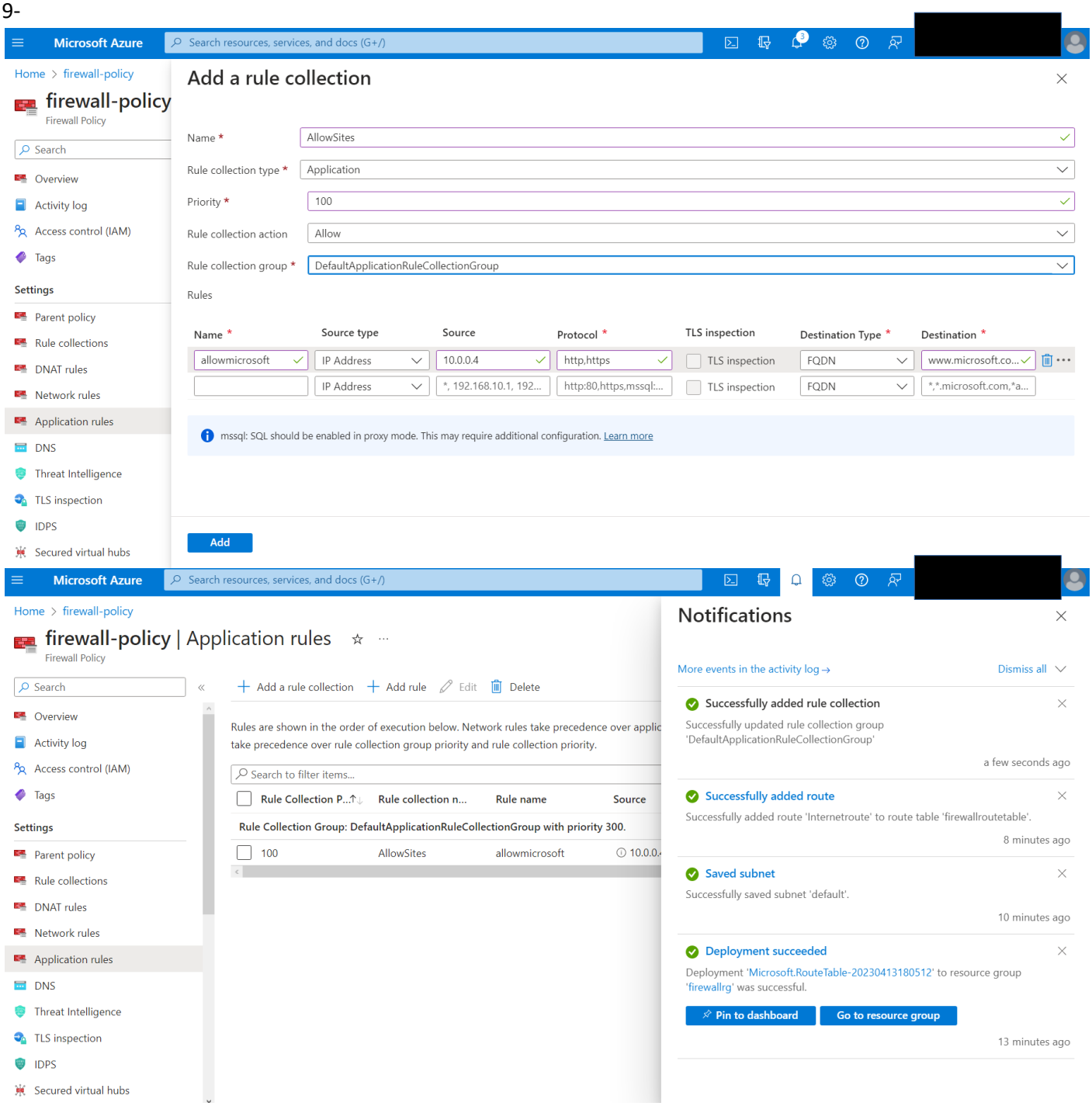
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Route tables > firewallroutetable
Route tables
Ministere de l'Enseignement Superieur et de la Re...
Create
Manage view
Filter for any field...
Name
firewallroutetable
Page 1 of 1
firewallroutetable | Routes
Route table
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Locks
Monitoring
Alerts
Automation
Add
Refresh
Search routes
Name
No results.
Add route
firewallroutetable
Route name *
Internetroute
Destination address prefix *
IP Addresses
Destination IP addresses/CIDR ranges *
0.0.0.0/0
Next hop type *
Virtual appliance
Next hop address *
10.0.1.4
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.
Add


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Route tables > firewallroutetable
Route tables
Ministere de l'Enseignement Superieur et de la Re...
Create
Manage view
Filter for any field...
Name
firewallroutetable
Page 1 of 1
firewallroutetable | Routes
Route table
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Locks
Monitoring
Alerts
Automation
Add
Refresh
Give feedback
Search routes
Name
Address prefix
Next hop type
Next hop IP address
Internetroute
0.0.0.0/0
VirtualAppliance
10.0.1.4

8-

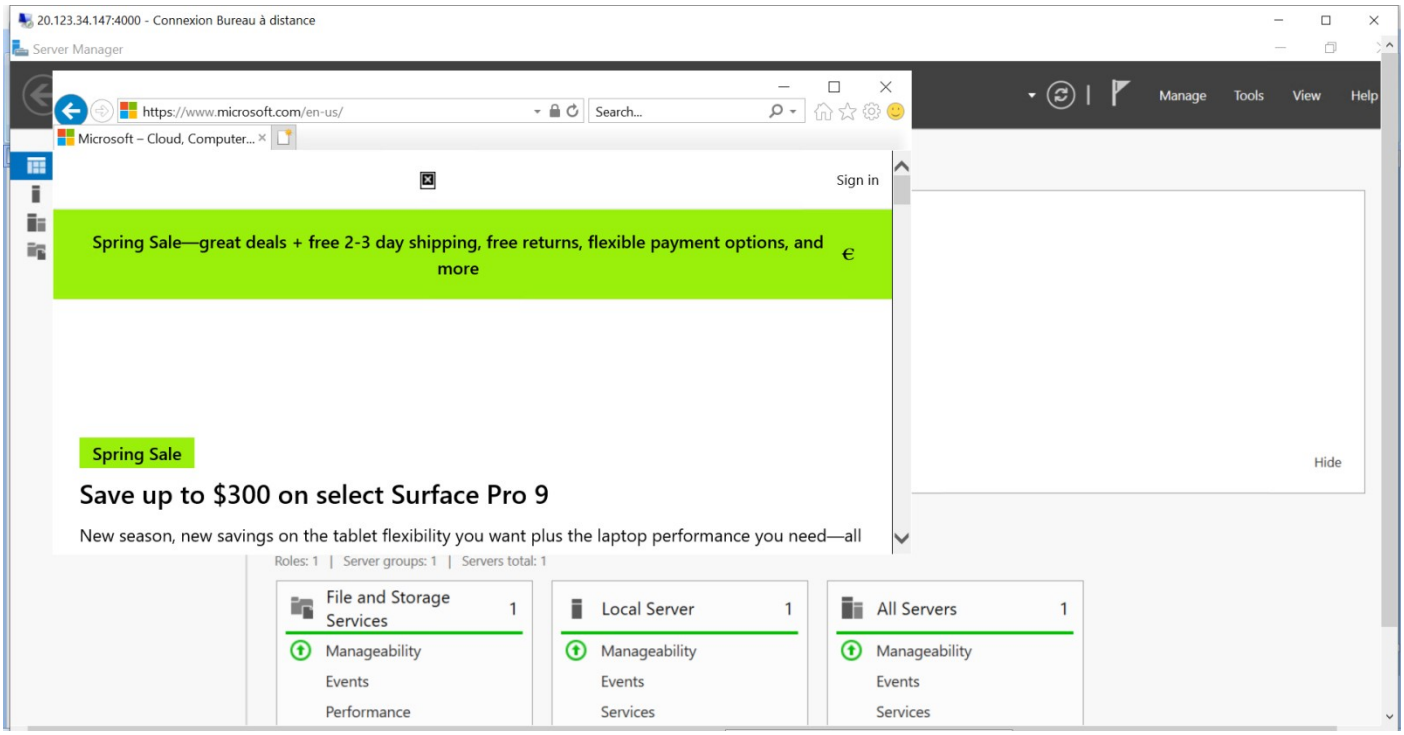

20.123.34.147:4000 - Connexion Bureau à distance
Server Manager
http://www.microsoft.com/
Search...
microsoft.com
Action: Deny. Reason: No rule matched. Proceeding with default action.
Manage
Tools
View
Hide
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services
Manageability
Events
Performance
Local Server
Manageability
Events
Services
All Servers
Manageability
Events
Services

9-

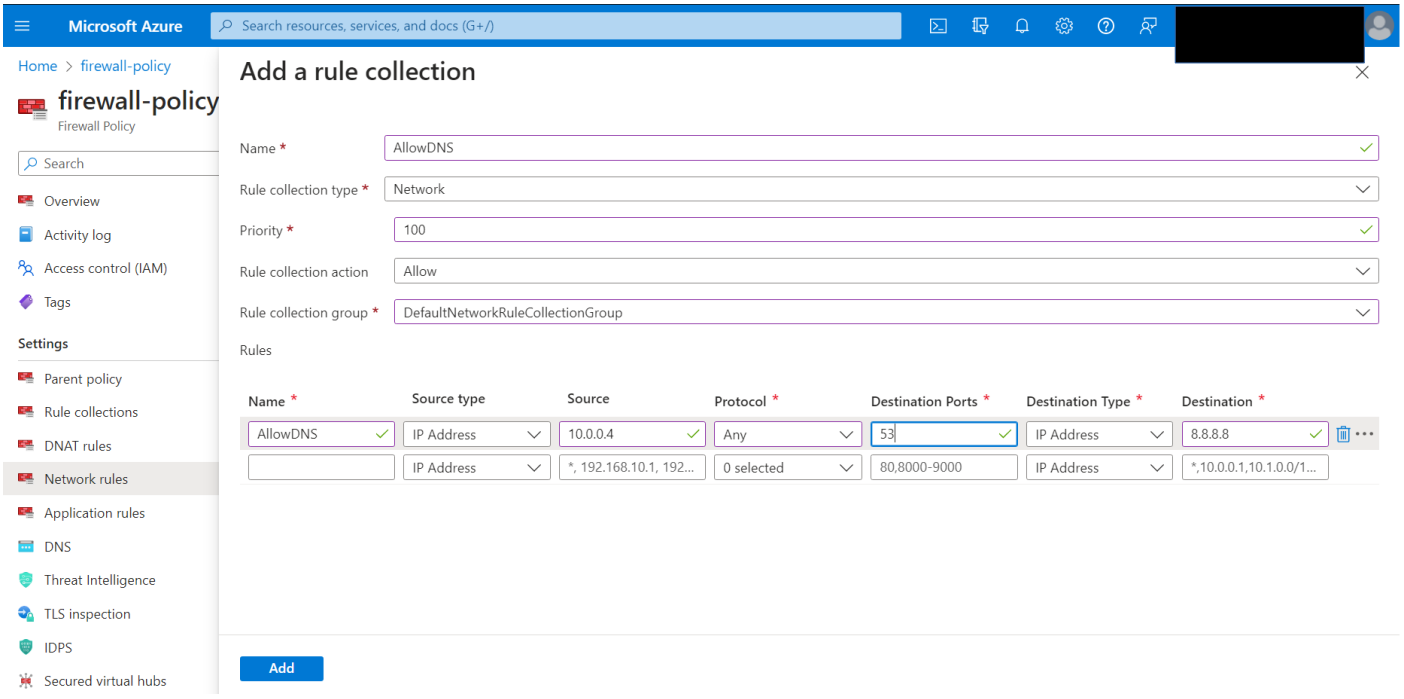

Microsoft Azure
Search resources, services, and docs (G+/)
Home > firewall-policy
firewall-policy
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Add a rule collection
Name * AllowSites
Rule collection type * Application
Priority * 100
Rule collection action Allow
Rule collection group * DefaultApplicationRuleCollectionGroup
Rules
Name * Source type Source Protocol * TLS inspection Destination Type * Destination *
allowmicrosoft IP Address 10.0.0.4 http,https TLS inspection FQDN www.microsoft.co...
IP Address *, 192.168.10.1, 192... http:80,https,mssql:... TLS inspection FQDN *,*.microsoft.com,*a...
mssql: SQL should be enabled in proxy mode. This may require additional configuration. Learn more
Add

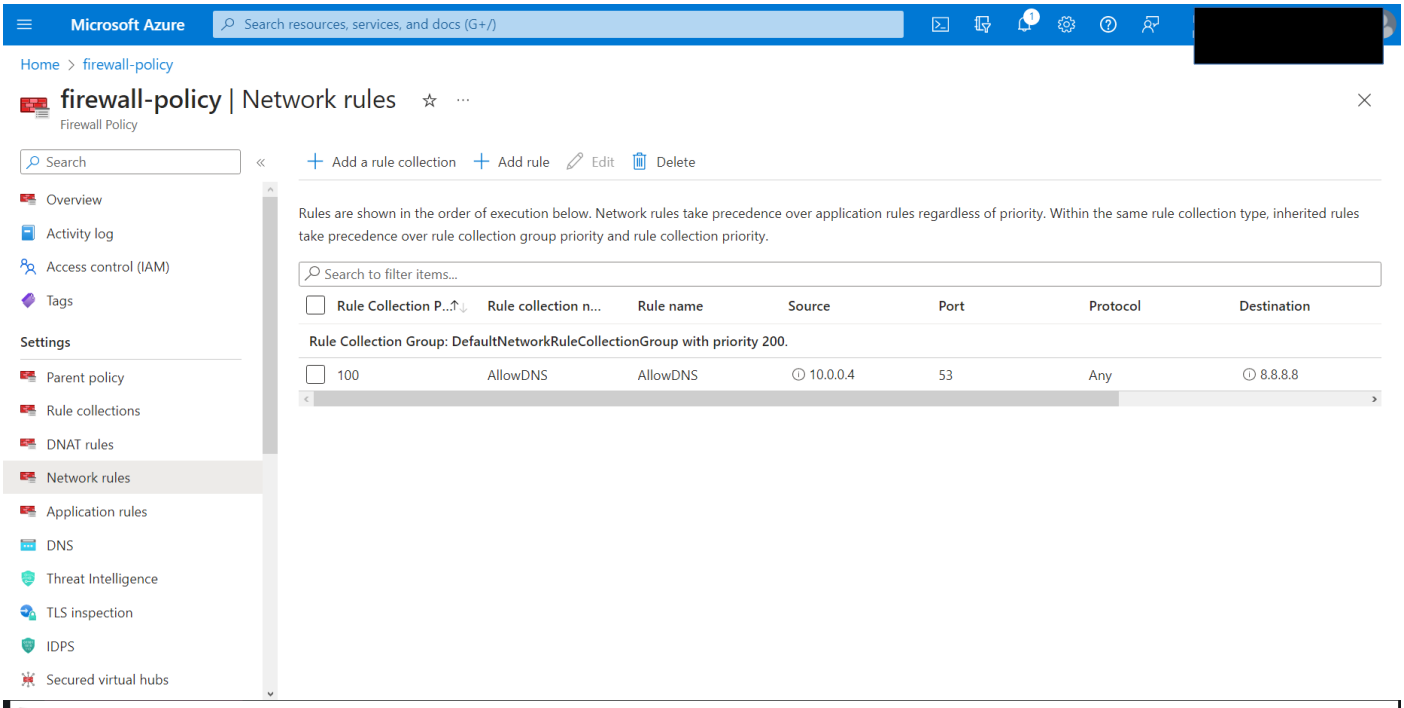
Microsoft Azure
Search resources, services, and docs (G+/)
Home > firewall-policy
firewall-policy | Application rules
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Add a rule collection
Add rule
Edit
Delete
Rules are shown in the order of execution below. Network rules take precedence over applic
take precedence over rule collection group priority and rule collection priority.
Search to filter items...
Rule Collection P...
Rule collection n...
Rule name
Source
Rule Collection Group: DefaultApplicationRuleCollectionGroup with priority 300.
100 AllowSites allowmicrosoft
Notifications
More events in the activity log →
Dismiss all
Successfully added rule collection
Successfully updated rule collection group 'DefaultApplicationRuleCollectionGroup'
a few seconds ago
Successfully added route
Successfully added route 'Internetroute' to route table 'firewallroutetable'.
8 minutes ago
Saved subnet
Successfully saved subnet 'default'.
10 minutes ago
Deployment succeeded
Deployment 'Microsoft.RouteTable-20230413180512' to resource group 'firewallrg' was successful.
Pin to dashboard
Go to resource group
13 minutes ago

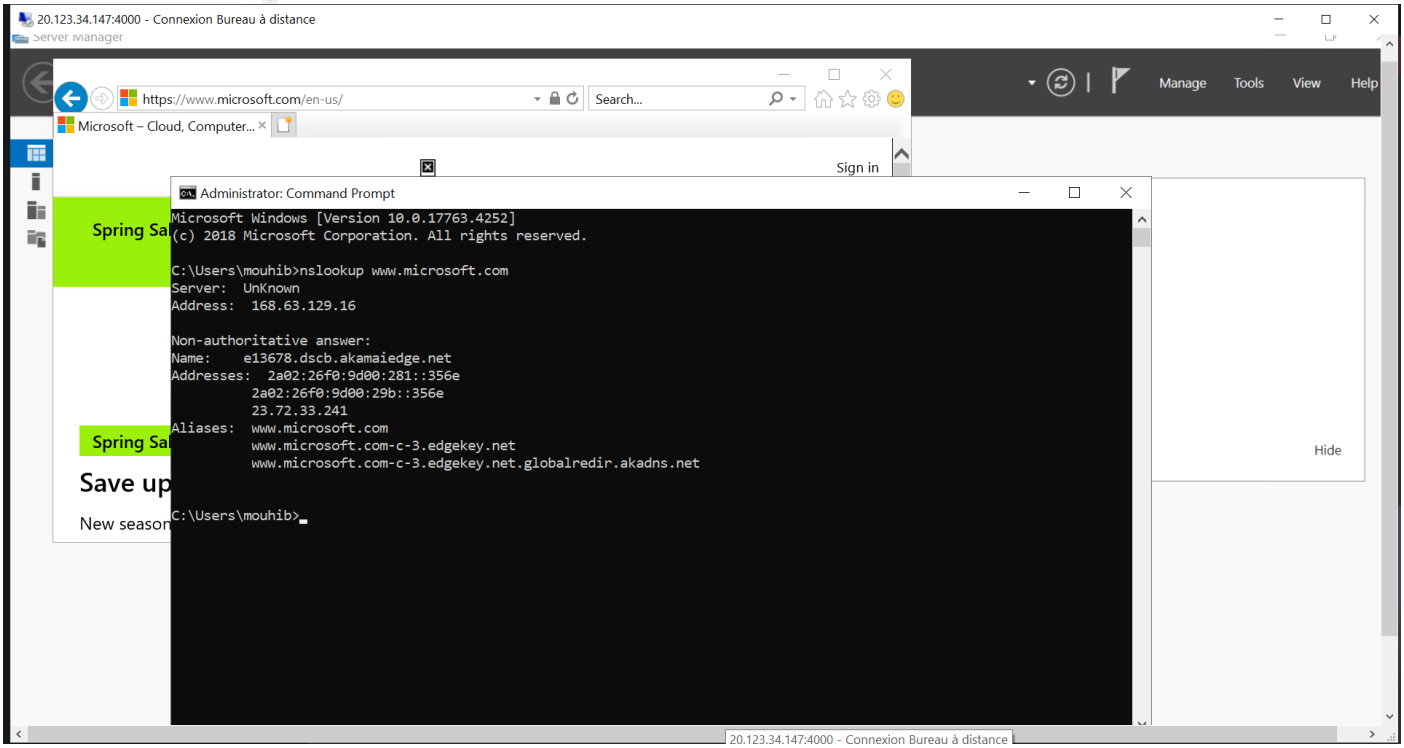
10-


20.123.34.147:4000 - Connexion Bureau à distance
Server Manager
https://www.microsoft.com/en-us/
Search...
Microsoft – Cloud, Computer...
Manage
Tools
View
Help
Sign in
Spring Sale—great deals + free 2-3 day shipping, free returns, flexible payment options, and more
Spring Sale
Save up to $300 on select Surface Pro 9
New season, new savings on the tablet flexibility you want plus the laptop performance you need—all
Hide
Roles: 1 | Server groups: 1 | Servers total: 1
File and Storage Services 1
Manageability
Events
Performance
Local Server 1
Manageability
Events
Services
All Servers 1
Manageability
Events
Services

11-


Microsoft Azure
Search resources, services, and docs (G+/)
Home > firewall-policy
firewall-policy
Firewall Policy
Search
Overview
Activity log
Access control (IAM)
Tags
Settings
Parent policy
Rule collections
DNAT rules
Network rules
Application rules
DNS
Threat Intelligence
TLS inspection
IDPS
Secured virtual hubs
Add a rule collection
Name * AllowDNS
Rule collection type * Network
Priority * 100
Rule collection action Allow
Rule collection group * DefaultNetworkRuleCollectionGroup
Rules
Name * | Source type | Source | Protocol * | Destination Ports * | Destination Type * | Destination *
AllowDNS | IP Address | 10.0.0.4 | Any | 53 | IP Address | 8.8.8.8
IP Address | *, 192.168.10.1, 192... | 0 selected | 80,8000-9000 | IP Address | *,10.0.0.1,10.1.0.0/1...
Add





➔ Afin de vérifier si on peut accéder au serveur DNS 8.8.8.8 depuis la machine demovm à travers le firewall, on a utilisé la commande « nslookup » qui permet de faire la résolution du nom du domaine (DNS) d'un URL (site web) pour retourner son adresse IP publique.

Comme on peut voir dans cette capture d'écran, « nslookup www.microsoft.com » a retourné la valeur d'adresse IP de ce site web « 138.63.129.16 » ce qui signifie que la machine demovm a pu accéder au serveur DNS 8.8.8.8 à travers le firewall. Tout est grâce à la règle du firewall policy qui s'appelle « AllowDNS ».

Interprétations :

I. Azure traffic manager :

Il s'agit d'un service qui permet la distribution du trafic Internet vers les applications déployés d'une façon publique dans une région Azure globale. En choisissant une méthode de routage adéquate, il permet de router ce trafic en utilisant le DNS vers un point de terminaison qui peut être hébergé en dehors d'Azure. Globalement, il permet d'améliorer la haute disponibilité des applications, améliorer les performances des applications et combiner plusieurs méthodes de routage afin de faciliter l'implémentation de n'importe quelle architecture complexe de règles du trafic.

Azure Trafic manager prend en charge 6 méthodes de routage du trafic :

- **Priority :** Pour fournir un point de terminaison principal et d'autres secondaires qui prennent la relève en cas de panne
- **Weighted :** La distribution du trafic sera faite en fonction du poids d'un ensemble de points de terminaisons (il doit être défini rigoureusement pour qu'il soit uniforme entre tous les points de terminaison)
- **Performance :** Dans le cas où on a plusieurs points de terminaisons qui se situent dans des emplacements géographiques différents où on route le trafic vers le point le plus proche aux utilisateurs, c'est-à-dire, le point ayant la « Latency » la plus faible
- **Géographic :** En fonction de l'origine géographique des requêtes DNS, on route l'utilisateur vers des points de terminaison spécifiques
- **Valeurs Multiples :** Les points de terminaison sont toujours des adresses IPv4 et IPv6.
- **Subnet :** Utilisé lorsqu'on veut relier des plages d'adresses IP d'utilisateur à un point de terminaison spécifique.

  ➔ Dans le cadre de ce TP dans Task 1, nous avons utilisé le type de routage « Multivalue » (valeurs multiples) où on a relié la machine du client vers des points de terminaison multiples via une requête DNS (DNS query response qu'on a vu avec wireshark où on a vu les adresses publiques des deux machines).

II. Azure front door :

Tout d'abord on défini CDN, il s'agit d'un réseau de diffusion de contenu (content delivery network / content distribution network). C'est un réseau très large contant un très grand nombre de serveurs qui sont connectés entre eux et permettent d'accélérer le chargement des pages Web pour les applications avec des données massives.

Dans ce contexte, on introduit Azure Front Door qui s'agit du Cloud réseau de distribution de contenu de Microsoft. Il permet d'avoir un accès sécurisé tout en améliorant la rapidité, la fiabilité et la sécurité aux applications entre les applications et le contenu web statique et dynamique. Il fait le routage du trafic en utilisant un réseau massive de centaines de points de présences (PoPs) globaux et locaux qui sont distribués dans le monde entier pour fournir les besoins des entreprises et des utilisateurs finaux.

Dans le contexte de ce TP nous avons défini le Front End Door en 3 étapes :

1- **Définition du front end host :**
   Il s'agit d'un nom de domaine qui est utilisé pour faire le routage des requêtes vers un ou plusieurs backend pool. Son URL est utilisé par les clients pour y accéder et utiliser ses services ou applications. Pour chaque front end host, on peut configurer une ou plusieurs règles de routage des requêtes vers le backend pool approprié.
2- **Définition du backend pool :**
   Il s'agit d'un groupe de ressources qui ne sont accessibles qu'à travers le load balanceur du Front Door et ses options de gestion du trafic. Chaque pool peut contenir plusieurs backends (par

exemple ; des machines virtuelles, des applications web, ou n'importe quelle point de terminaison accessible de façon publique par Internet).
Le trafic peut être distribué pour ces pools en utilisant les règles de routage où on peut router le trafic selon l'URL, le nom du host ou d'autres critères. Ce qui permettra d'améliorer les performances, la scalabilité et l'availabilité de l'application.

3- **Définition de la règle de routage :**
Il s'agit d'une configuration dans le Front Door d'Azure qui permet de spécifier la manière avec la quelle les requêtes doivent être routées vers les backend pools. Elle se compose d'une partie « left-hand » (qui indique les requêtes qui vont être liées et elle peut être configurée selon des critères bien précis comme le hostname, le chemin, http header… etc), et d'une partie « right-hand » qui indique les backends pools qui doivent recevoir ces requêtes.
Il s'agit donc d'un outil puissant et très important pour le load balanceur et la gestion du trafic.

III. Azure Firewall :

Il s'agit d'un service Firewall puissant puisqu'il possède une protection contre les menaces en filtrant le trafic et en générant une alerte si les adresses IP des requêtes (envoyées ou reçues) sont malveillantes. Il est important de noter aussi qu'Azure Firewall fait la mise à jour à temps réel de sa base de données sur les listes de domaines et d'adresses IP malveillante pour que la protection soit toujours efficace contre les nouvelles attaques. Pour la version premium, plusieurs autres services peuvent être valables comme l'inspection TLS (l'inspection du trafic encrypté du Transport layer security – TLS, tout en le déchiffrant afin de vérifier s'il y a du contenu malveillant. En effet, pour l'activer il faut installer un certificat d'autorité intermédiaire.), IDPS (Intrusion Detection and Prevention System qui s'agit d'un système de signature pour établir le monitoring et le logging des activités de réseau en temps réel pour prévenir les attaques le plus tôt possible), filtrage URL… etc.
Dans le cadre de ce TP, nous avons utilisé le Firewall pour bloquer l'accès au site www.microsoft.com puis nous avons libérer l'accès à ce site en utilisant la définition d'une route table et les règles de firewall policy et puis nous avons donné l'accès au serveur dns 8.8.8.8 pour notre VM. (en utilisant ; DNAT rules, network rules, application rules).
En effet, firewall policy est une ressource qui contient des options de sécurité configurables et peut être utilisé sur plusieurs instances de Firewall dans la même région. On peut définir plusieurs Network Security Groups et plusieurs instances de Firewall pour les gérer tous en utilisant firewall policy. Il nous permet de définir les règles de sécurité, des configurations pour le DNS, des règles de NAT, un traitement intelligent contre les menaces, des règles d'application… etc.
On ajoute qu'Azure firewall offre aussi une fonctionnalité qui s'appelle « Policy Analytics » qui aide à étudier les policies du Firewall au cours du temps pour qu'elles soient toujours à jour et sécurisées.

- DNAT rule (Destination Network Address Translation) ; Ce sont des règles utilisées pour bloquer ou laisser passer le traffic à travers l'adresse publique du Firewall. Elle permet donc la redirection du trafic vers une destination spécifique (adresse IP et port spécifiques en faisant la traduction de la destination originale vers une destination différente). Implicitement, cette règle ajoute aussi une règle de réseau (Network rule) correspondante pour accepter le trafic traduit. Pour des raisons de sécurité il faut toujours ajouter une 'application rule collections' après chaque 'DNAT rule' pour que l'accès soit restreint pour l'application uniquement (c'est presque ce qu'on a fait dans le TP lorsqu'on a activé l'accès au site www.microsoft.com)
- Network rule ; Elle spécifie le trafic bloqué et accepté en utilisant les adresses IP de la source et de la destination, les ports et les protocoles (http par exemple). On peut les organiser dans une collections de policies qui peuvent aussi être combinées en une collections de collections (afin de créer une structure hiérarchique de groupes de règles, pour offrir une meilleure visibilité et gestion de règles).

- Application rules ; On spécifie l'acceptation ou le refus du trafic en se basant sur la couche application (Layer 7). Par exemple, on peut accepter le trafic ou le bloquer en se basant sur un protocole spécifié de la couche applicative comme HTTP, HTTPS, FTP… etc. Ou en se basant sur des attributs du trafic (chemin URL, version du protocole, le port…etc).