

Formateur : Ihab ABADI

TP Azure AZ 104

- Créez un réseau virtuel Azure.
- Créez deux sous-réseaux dans le réseau virtuel.
- Créez un groupe de sécurité réseau (NSG) et associez-le à l'un des sous-réseaux.
- Ajoutez des règles entrantes et sortantes pour autoriser/défendre le trafic (par exemple, autoriser le trafic HTTP et HTTPS et bloquer le trafic SSH).
- Créez deux machines virtuelles, chacune dans un sous-réseau différent.
- Testez la connectivité entre les machines virtuelles et vérifiez que les règles de sécurité sont appliquées correctement.

Création Virtual Network :

Créer un réseau virtuel

Informations de base

Sécurité

Adresses IP

Étiquettes

Vérifier + créer

Réseau virtuel Azure (VNet) est le composant fondamental de votre réseau privé dans Azure. VNet permet à de nombreux types de ressources Azure, notamment des machines virtuelles Azure, de communiquer de manière sécurisée entre elles, avec Internet et sur les réseaux locaux. VNet est similaire à un réseau traditionnel que vous opérez dans votre propre centre de données, avec en plus les avantages de l'infrastructure Azure comme la mise à l'échelle, la disponibilité et l'isolation.

[En savoir plus](#)

Détails du projet

Sélectionnez l'abonnement pour gérer les ressources déployées et les coûts. Utilisez des groupes de ressources comme des dossiers pour organiser et gérer toutes vos ressources.

Subscription *

Abonnement Azure 1

Resource group *

m2i-formation

[Créer nouveau](#)

Détails de l'instance

Nom du réseau virtuel *

benoit_network

Région ⓘ *

(Asia Pacific) Japan East

[Déployer sur une zone périphérique](#)

Ajouter un sous-réseau

Sélectionnez un espace d'adressage et configurez votre sous-réseau. Vous pouvez personnaliser un sous-réseau par défaut ou effectuer une sélection à partir de modèles de sous-réseau si vous prévoyez d'ajouter des services sélectionnés plus tard. [En savoir plus](#)

Espace d'adressage IP ⓘ

10.0.0.0/16

10.0.0.0 - 10.0.255.255 (65536 adresses)

Détails du sous-réseau

Modèle de sous-réseau ⓘ

Default

Nom *

subnet_1

Adresse de début *

10.0.1.0

Taille de l'adresse IP ⓘ

/24 (256 adresses)

Espace d'adressage IP ⓘ

10.0.1.0 - 10.0.1.255 (256 adresses)

Espace d'adressage IP ⓘ 10.0.1.0 - 10.0.1.255 (256 adresses)

Sécurité

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [En savoir plus](#) ⓘ

Passerelle NAT ⓘ

Aucun

[Créer](#)

Groupe de sécurité réseau ⓘ

Aucun

[Créer](#)

Table de routage

Aucun

10.0.0.0/16 [Ajouter un sous-réseau](#) ...

10.0.0.0 - 10.0.255.255 (65536 adresses)

Sous-réseaux	Plage d'adresses IP	Taille	Passerelle NAT
subnet_0	10.0.0.0 - 10.0.0.255	/24 (256 adresses)	-
subnet_1	10.0.1.0 - 10.0.1.255	/24 (256 adresses)	-

benoit_network Réseau virtuel

Rechercher

[Vue d'ensemble](#)
[Journal d'activité](#)
[Contrôle d'accès \(IAM\)](#)
[Étiquettes](#)
[Diagnostiquer et résoudre les problèmes](#)

[Déplacer](#) [Supprimer](#) [Actualiser](#) [Envoyer des commentaires](#)

Bases
Groupe de ressources ([déplacer](#)) : m2i-formation
Emplacement ([déplacer](#)) : Japan East
Abonnement ([déplacer](#)) : Abonnement Azure 1
ID d'abonnement : c49e632f-5dd4-4c37-b1a6-578c7faa36fd

Espace d'adressage : 10.0.0.0/16
Serveurs DNS : Service DNS
Délai d'expiration du flux : Configurer
Chaine de communauté BGP : Configurer
ID réseau virtuel : 30b5d9e7

Création Security Group :

Créer un groupe de sécurité réseau

✓ Validation réussie

De base

Étiquettes

Vérifier + créer

De base

Abonnement

Groupe de ressources

Région

nom

Abonnement Azure 1

m2i-formation

Japan East

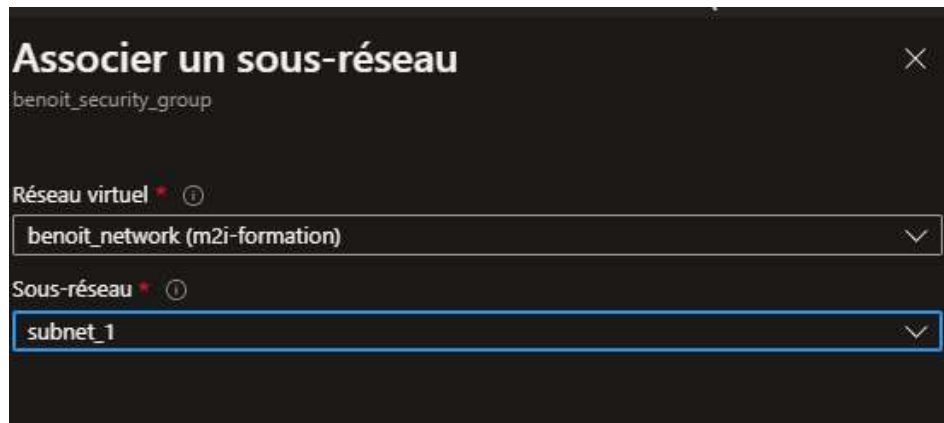
benoit_security_group

Étiquettes

Name

Benoit_Security_Group

Associer Security Group à un Subnet :



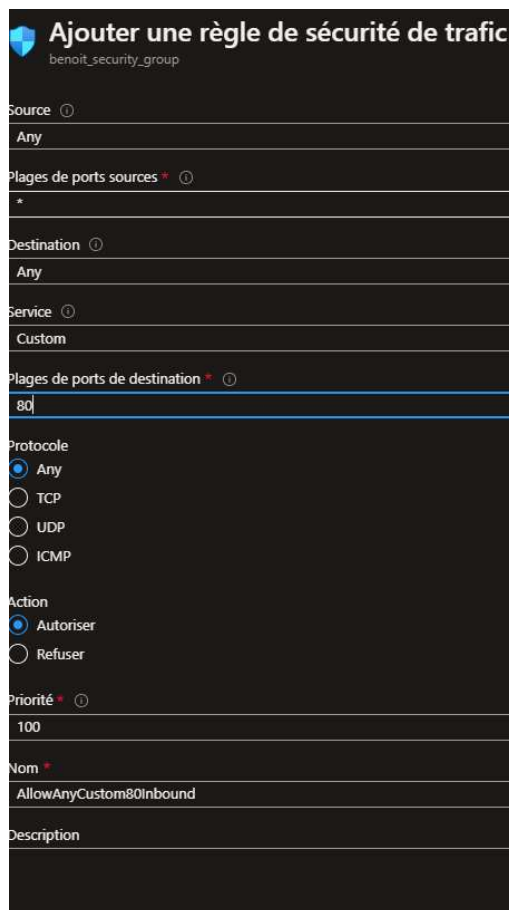
Associer un sous-réseau

benoit_security_group

Réseau virtuel * ⓘ
benoit_network (m2i-formation) ▼

Sous-réseau * ⓘ
subnet_1 ▼

Autoriser port 80 et 443 (HTTP & HTTPS)



Ajouter une règle de sécurité de trafic

benoit_security_group

Source ⓘ
Any

Plages de ports sources * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Plages de ports de destination * ⓘ
80

Protocole
☒ Any
☐ TCP
☐ UDP
☐ ICMP

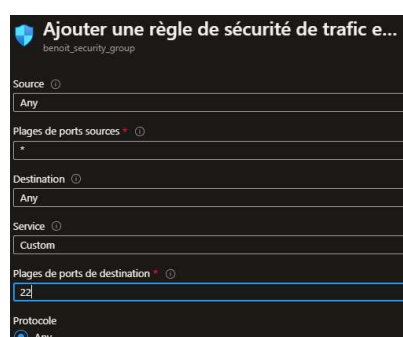
Action
☒ Autoriser
☐ Refuser

Priorité * ⓘ
100

Nom *
AllowAnyCustom80Inbound

Description

Bloquer port 22 (SSH) :



Ajouter une règle de sécurité de trafic e...

benoit_security_group

Source ⓘ
Any

Plages de ports sources * ⓘ
*

Destination ⓘ
Any

Service ⓘ
Custom

Plages de ports de destination * ⓘ
22

Protocole
☒ Any

TCP

UDP

ICMP

Action

Autoriser

Refuser

Priorité

120

Nom

DenyAnyCustom22Inbound

Description

Résultat des opérations :

cloud | Règles de sécurité de trafic entrant

Ajouter

Masquer les règles par défaut

Actualiser

Supprimer

Fournir des commentaires

Les règles de sécurité du groupe de sécurité réseau sont évaluées par priorité à l'aide de la combinaison de la source, du port source, de la destination, du port de destination et du protocole pour autoriser ou refuser le trafic. Une règle de sécurité ne peut pas être supprimée si elle est la seule règle existante. Vous ne pouvez pas supprimer les règles de sécurité par défaut, mais vous pouvez les remplacer par des règles ayant une priorité plus élevée. [En savoir plus](#)

Filter par nom

Port == tout

Protocole == tout

Source == tout

Destination == tout

Action == tout

Priorité	Nom	Port	Protocole	Source	Destination	Action
100	AllowAnyCustom80Inbound	80	N'importe lequel	N'importe lequel	N'importe lequel	Allow
110	AllowAnyCustom443Inbound	443	N'importe lequel	N'importe lequel	N'importe lequel	Allow
120	DenyAnyCustom22Inbound	22	N'importe lequel	N'importe lequel	N'importe lequel	Deny

Création VM :

Supprimer

Annuler

Redéployer

Télécharger

Actualiser

Le déploiement est en cours

Nom du déploiement : CreateVm-canonical.0001-com-ubuntu-serv...

Abonnement : [Abonnement Azure 1](#)

Groupe de ressources : [m2i-formation](#)

Heure de début : 31/03/2023 11:45:16

ID de corrélation : c91ba665-57c2-4b23-a0db-12baea9f42d1

Détails du déploiement

Ressource	Type	Statut
Aucun résultat.		

Vérification de la création :

Actualiser

Rechercher sur les appareils connectés

Appareil	Type	Adresse IP
benoit-vm-1093	Interface réseau	10.0.1.4
benoit-test-0677	Interface réseau	10.0.0.4

Test de ping sur une VM vers l'autre VM :

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

vel@benoit-test-0:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:22:48:05:72:80 brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.4/24 brd 10.0.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::222:48ff:fe05:7280/64 scope link
        valid_lft forever preferred_lft forever
vel@benoit-test-0:~$ ping 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
 64 bytes from 10.0.1.4: icmp_seq=1 ttl=64 time=0.874 ms
 64 bytes from 10.0.1.4: icmp_seq=2 ttl=64 time=1.40 ms
^C
10.0.1.4 ping statistics:
```

```
--- 10.0.1.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.874/1.138/1.402/0.264 ms
```

Même exercice en powershell :

Objet avec Les informations de L'adresse IP

```
$ip = @{
    Name = 'publicIpAzPowershell1Benoit'
    ResourceGroupName = 'm2i-formation'
    AllocationMethod = 'Static'
    IpAddressVersion = 'IPv4'
    Location = "koreacentral"
}
```

Création de L'adresse ip

```
$ipConfig = New-AzPublicIpAddress @ip
```

Objet avec Les informations de L'adresse IP

```
$ip2 = @{
    Name = 'publicIpAzPowershell2Benoit'
    ResourceGroupName = 'm2i-formation'
    AllocationMethod = 'Static'
    IpAddressVersion = 'IPv4'
    Location = "koreacentral"
}
```

Création de L'adresse ip

```
$ipConfig2 = New-AzPublicIpAddress @ip2
```

#Objet avec Les informations du VNET

```
$vnet = @{
    Name = 'VNet-benoit'
    ResourceGroupName = 'm2i-formation'
    Location = 'koreacentral'
    AddressPrefix = '10.0.0.0/16'
}
```

#Objet Subnet

```
$frontendSubnet = New-AzVirtualNetworkSubnetConfig -Name frontendSubnet -AddressPrefix "10.0.1.0/24"
$backendSubnet = New-AzVirtualNetworkSubnetConfig -Name backendSubnet -AddressPrefix "10.0.2.0/24"
```

```
$virtualNetwork = New-AzVirtualNetwork @vnet -Subnet $frontendSubnet,$backendSubnet
```

#Objet avec Les informations du groupe de sécurité

```
$netSecurityGroup = @{
    Name = "security-group-az-powershell-benoit-2"
    ResourceGroupName = "m2i-formation"
    Location = "koreacentral"
}
```

Création d'un security group

```
$nsc = New-AzNetworkSecurityGroup @netSecurityGroup
```

Création des règles de sécurité

```
$nsc | Add-AzNetworkSecurityRuleConfig -Name web-rule-2 -Description "Allow HTTP" `
    -Access Allow -Protocol Tcp -Direction Inbound -Priority 102 -SourceAddressPrefix `
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 80 | Set-AzNetworkSecurityGroup
```

```
$nsc | Add-AzNetworkSecurityRuleConfig -Name ssh-rule-2 -Description "Allow SSH" `
-Access Allow -Protocol Tcp -Direction Inbound -Priority 101 -SourceAddressPrefix `
185.31.149.99 -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 22 | Set-AzNetworkSecurityGroup
```

```
$nsc | Add-AzNetworkSecurityRuleConfig -Name web-rule-3 -Description "Allow HTTPS" `
-Access Allow -Protocol Tcp -Direction Inbound -Priority 103 -SourceAddressPrefix `
Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 443 | Set-AzNetworkSecurityGroup
```

Création d'une vm

```
$infoVm = @{
    Name = 'vm-az-powershell-benoit'
    ResourceGroupName = 'm2i-formation'
    Location = "koreacentral"
    SecurityGroupName = $nsc
    Image = "UbuntuLTS"
    PublicIpAddressName = "publicIpAzPowershell1Benoit"
    PublicIpSku = "Standard"
    SubnetName = "frontendSubnet"
    VirtualNetworkName = "VNet-benoit"
}
```

```
$vm = New-AzVM @infoVm -Credential (Get-Credential)
```

Création d'une vm

```
$infoVm2 = @{
    Name = 'vm-az-powershell-benoit-2'
    ResourceGroupName = 'm2i-formation'
    Location = "koreacentral"
    SecurityGroupName = $nsc
    Image = "UbuntuLTS"
    PublicIpAddressName = "publicIpAzPowershell2Benoit"
    PublicIpSku = "Standard"
    SubnetName = "backendSubnet"
    VirtualNetworkName = "VNet-benoit"
}
```

```
$vm = New-AzVM @infoVm2 -Credential (Get-Credential)
```

Correction TP 1 :

Version Powershell :

```
# Variables
$ResourceGroupName = "m2i-formation"
$VNetName = "VNetBenoitVirtual"
$Subnet1Name = "SousReseau1"
$Subnet2Name = "SousReseau2"
$NSGName = "NSGBenoit"
$Location = "koreacentral"
$VM1Name = "VM1"
$VM2Name = "VM2"
$Username = "WorkBenoitUtilisateur"
$Password = "WorkBenoitPasse"

# Créez un réseau virtuel Azure
$VNet = New-AzVirtualNetwork -ResourceGroupName $ResourceGroupName -Name $VNetName -AddressPrefix 10.0.0.0/16 -Location $Location

# Créez deux sous-réseaux dans le réseau virtuel
$Subnet1 = Add-AzVirtualNetworkSubnetConfig -Name $Subnet1Name -AddressPrefix 10.0.1.0/24 -VirtualNetwork $VNet
$Subnet2 = Add-AzVirtualNetworkSubnetConfig -Name $Subnet2Name -AddressPrefix 10.0.2.0/24 -VirtualNetwork $VNet
$VNet | Set-AzVirtualNetwork

# Créez un groupe de sécurité réseau (NSG) et associez-le au premier sous-réseau
$NSG = New-AzNetworkSecurityGroup -ResourceGroupName $ResourceGroupName -Location $Location -Name $NSGName
$Subnet1 = Set-AzVirtualNetworkSubnetConfig -Name $Subnet1Name -AddressPrefix 10.0.1.0/24 -VirtualNetwork $VNet -NetworkSecurityGroup $NSG
$VNet | Set-AzVirtualNetwork

# Ajoutez des règles entrantes et sortantes pour autoriser/défendre le trafic
$HTTPRule = New-AzNetworkSecurityRuleConfig -Name "AutoriserHTTP" -Description "Autoriser le trafic HTTP" -Access "Allow" -Protocol "Tcp" -Direction "Inbound" -Priority 100 -SourceAddressPrefix "Internet" -SourcePortRange "*" -DestinationAddressPrefix "*"
$HTTPSRule = New-AzNetworkSecurityRuleConfig -Name "AutoriserHTTPS" -Description "Autoriser le trafic HTTPS" -Access "Allow" -Protocol "Tcp" -Direction "Inbound" -Priority 110 -SourceAddressPrefix "Internet" -SourcePortRange "*" -DestinationAddressPrefix "*"
$SSHRule = New-AzNetworkSecurityRuleConfig -Name "BloquerSSH" -Description "Bloquer le trafic SSH" -Access "Deny" -Protocol "Tcp" -Direction "Inbound" -Priority 120 -SourceAddressPrefix "Internet" -SourcePortRange "*" -DestinationAddressPrefix "*"

$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $HTTPRule
$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $HTTPSRule
$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $SSHRule
$NSG | Set-AzNetworkSecurityGroup

# Créez deux machines virtuelles, chacune dans un sous-réseau différent
New-AzVm -ResourceGroupName $ResourceGroupName -Name $VM1Name -Location $Location -VirtualNetworkName $VNetName -SubnetName $Subnet1Name -AdminUsername $Username -AdminPassword $Password -SecurityGroupName $NSGName -OpenPorts 80,443 -Image "Canonical:UbuntuServer:18.04-LTS"
New-AzVm -ResourceGroupName $ResourceGroupName -Name $VM2Name -Location $Location -VirtualNetworkName $VNetName -SubnetName $Subnet2Name -AdminUsername $Username -AdminPassword $Password -OpenPorts 80,443 -Image "Canonical:UbuntuServer:18.04-LTS"

# Testez la connectivité entre les machines virtuelles et vérifiez que les règles de sécurité sont appliquées correctement
$VM1 = Get-AzVM -ResourceGroupName $ResourceGroupName -Name $VM1Name
$VM2 = Get-AzVM -ResourceGroupName $ResourceGroupName -Name $VM2Name

$VM1PublicIP = (Get-AzPublicIpAddress -ResourceGroupName $ResourceGroupName -Name "$($VM1.Name)PublicIP").IpAddress
$VM1PrivateIP = (Get-AzNetworkInterface -ResourceGroupName $ResourceGroupName -Name "$($VM1.Name)NIC").IpConfigurations.PrivateIpAddress
Write-Host "Adresse IP publique de la VM1: $VM1PublicIP"
Write-Host "Adresse IP privée de la VM1: $VM1PrivateIP"
```

Variables

```
$ResourceGroupName = "m2i-formation"
```



```

$VNetName = "MonReseauVirtuel"
$Subnet1Name = "SousReseau1"
$Subnet2Name = "SousReseau2"
$NSGName = "MonNSG"
$Location = "eastus"
$VM1Name = "VM1"
$VM2Name = "VM2"
$Username = "MonNomUtilisateur"
$Password = "MonMotDePasse"

# Créez un réseau virtuel Azure
$VNet = New-AzVirtualNetwork -ResourceGroupName $ResourceGroupName -Name $VNetName -AddressPrefix 10.0.0.0/16 -Location $Location

# Créez deux sous-réseaux dans le réseau virtuel
$Subnet1 = Add-AzVirtualNetworkSubnetConfig -Name $Subnet1Name -AddressPrefix 10.0.1.0/24 -VirtualNetwork $VNet
$Subnet2 = Add-AzVirtualNetworkSubnetConfig -Name $Subnet2Name -AddressPrefix 10.0.2.0/24 -VirtualNetwork $VNet
$VNet | Set-AzVirtualNetwork

# Créez un groupe de sécurité réseau (NSG) et associez-le au premier sous-réseau
$NSG = New-AzNetworkSecurityGroup -ResourceGroupName $ResourceGroupName -Location $Location -Name $NSGName
$Subnet1 = Set-AzVirtualNetworkSubnetConfig -Name $Subnet1Name -AddressPrefix 10.0.1.0/24 -VirtualNetwork $VNet -NetworkSecurityGroup $NSG
$VNet | Set-AzVirtualNetwork

# Ajoutez des règles entrantes et sortantes pour autoriser/défendre le trafic
$HTTPRule = New-AzNetworkSecurityRuleConfig -Name "AutoriserHTTP" -Description "Autoriser le trafic HTTP" -Access "Allow" -Protocol "Tcp" -Direction "Inbound" -Priority 100 -DestinationAddressPrefix "*" -DestinationPortRange 80
$HTTPsRule = New-AzNetworkSecurityRuleConfig -Name "AutoriserHTTPS" -Description "Autoriser le trafic HTTPS" -Access "Allow" -Protocol "Tcp" -Direction "Inbound" -Priority 110 -DestinationAddressPrefix "*" -DestinationPortRange 443
$SSHRule = New-AzNetworkSecurityRuleConfig -Name "BloquerSSH" -Description "Bloquer le trafic SSH" -Access "Deny" -Protocol "Tcp" -Direction "Inbound" -Priority 120 -DestinationAddressPrefix "*" -DestinationPortRange 22
$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $HTTPRule
$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $HTTPsRule
$NSG | Add-AzNetworkSecurityRuleConfig -NetworkSecurityRule $SSHRule
$NSG | Set-AzNetworkSecurityGroup

# Créez deux machines virtuelles, chacune dans un sous-réseau différent
New-AzVm -ResourceGroupName $ResourceGroupName -Name $VM1Name -Location $Location -VirtualNetworkName $VNetName -SubnetName $Subnet1Name -AdminUsername $Username -OpenPorts 80,443 -Image "Canonical:UbuntuServer:18.04-LTS:latest"

New-AzVm -ResourceGroupName $ResourceGroupName -Name $VM2Name -Location $Location -VirtualNetworkName $VNetName -SubnetName $Subnet2Name -AdminUsername $Username -OpenPorts 80,443 -Image "Canonical:UbuntuServer:18.04-LTS:latest"

# Testez la connectivité entre les machines virtuelles et vérifiez que les règles de sécurité sont appliquées correctement

$VM1 = Get-AzVm -ResourceGroupName $ResourceGroupName -Name $VM1Name
$VM2 = Get-AzVm -ResourceGroupName $ResourceGroupName -Name $VM2Name

$VM1PublicIP = (Get-AzPublicIpAddress -ResourceGroupName $ResourceGroupName -Name "{$($VM1.Name)PublicIP}").IpAddress
$VM2PrivateIP = (Get-AzNetworkInterface -ResourceGroupName $ResourceGroupName -Name "{$($VM2.Name)VMNic}").IpConfigurations.PrivateIpAddress

Write-Host "Adresse IP publique de la VM1: $VM1PublicIP"
Write-Host "Adresse IP privée de la VM2: $VM2PrivateIP"

```

Version CLI :

```

#!/bin/bash

# Variables
RESOURCE_GROUP="RG1-Formation"
LOCATION="us-east-1"
VNET_NAME="MonReseauVirtuel"
SUBNET1_NAME="SousReseau1"
SUBNET2_NAME="SousReseau2"
NSG_NAME="MonNSG"
VM1_NAME="VM1"
VM2_NAME="VM2"
USERNAME="MonNomUtilisateur"
PASSWORD="MonMotDePasse"

# Créez un réseau virtuel Azure
az network vnet create --resource-group $RESOURCE_GROUP --name $VNET_NAME --address-prefix 10.0.0.0/16 --location $LOCATION

# Créez deux sous-réseaux dans le réseau virtuel
az network vnet subnet create --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET1_NAME --address-prefix 10.0.1.0/24
az network vnet subnet create --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET2_NAME --address-prefix 10.0.2.0/24

# Créez un groupe de sécurité réseau (NSG) et associez-le au premier sous-réseau
az network nsg create --resource-group $RESOURCE_GROUP --name $NSG_NAME --location $LOCATION
az network vnet subnet update --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET1_NAME --network-security-group $NSG_NAME

# Ajoutez des règles entrantes et sortantes pour autoriser/défendre le trafic
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name AutoriserHTTP --priority 100 --source-address-prefixes Internet --source-port-ranges * --destination-address-prefixes * --destination-port-ranges 80 --access Allow --protocol Tcp --description Autoriser le trafic HTTP
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name AutoriserHTTPS --priority 110 --source-address-prefixes Internet --source-port-ranges * --destination-address-prefixes * --destination-port-ranges 443 --access Allow --protocol Tcp --description Autoriser le trafic HTTPS
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name BloquerSSH --priority 120 --source-address-prefixes Internet --source-port-ranges * --destination-address-prefixes * --destination-port-ranges 22 --access Deny --protocol Tcp --description Bloquer le trafic SSH

# Créez deux machines virtuelles, chacune dans un sous-réseau différent (suite)
az vm create --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --subnet $SUBNET1_NAME --public-ip-address-allocation static --image Canonical:UbuntuServer:18.04-LTS:latest --admin-username $USERNAME --admin-password $PASSWORD
az vm open-port --resource-group $RESOURCE_GROUP --name $VM1_NAME --port 80
az vm open-port --resource-group $RESOURCE_GROUP --name $VM1_NAME --port 443

# Testez la connectivité entre les machines virtuelles et vérifiez que les règles de sécurité sont appliquées correctement
VM1_PUBLIC_IP=$(az vm show --resource-group $RESOURCE_GROUP --name $VM1_NAME --show-details --query publicIpAddress --output tsv)
VM2_PRIVATE_IP=$(az vm show --resource-group $RESOURCE_GROUP --name $VM2_NAME --show-details --query privateIpAddress --output tsv)

echo "Adresse IP publique de la VM1: $VM1_PUBLIC_IP"
echo "Adresse IP privée de la VM2: $VM2_PRIVATE_IP"

```

#!/bin/bash

Variables

```

RESOURCE_GROUP="m2i-formation"
LOCATION="eastus"
VNET_NAME="MonReseauVirtuel"
SUBNET1_NAME="SousReseau1"
SUBNET2_NAME="SousReseau2"
NSG_NAME="MonNSG"
VM1_NAME="VM1"
VM2_NAME="VM2"
USERNAME="MonNomUtilisateur"
PASSWORD="MonMotDePasse"

# Créez un réseau virtuel Azure
az network vnet create --resource-group $RESOURCE_GROUP --name $VNET_NAME --address-prefix 10.0.0.0/16 --location $LOCATION

# Créez deux sous-réseaux dans le réseau virtuel
az network vnet subnet create --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET1_NAME --address-prefix 10.0.1.0/24
az network vnet subnet create --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET2_NAME --address-prefix 10.0.2.0/24

# Créez un groupe de sécurité réseau (NSG) et associez-le au premier sous-réseau
az network nsg create --resource-group $RESOURCE_GROUP --name $NSG_NAME --location $LOCATION
az network vnet subnet update --resource-group $RESOURCE_GROUP --vnet-name $VNET_NAME --name $SUBNET1_NAME --network-security-group $NSG_NAME

# Ajoutez des règles entrantes et sortantes pour autoriser/défendre le trafic
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name AutoriserHTTP --priority 100 --source-address-prefixes "Internet" --source-destination-port-ranges 80 --access Allow --protocol Tcp --description "Autoriser le trafic HTTP" --direction Inbound
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name AutoriserHTTPS --priority 110 --source-address-prefixes "Internet" --source-destination-port-ranges 443 --access Allow --protocol Tcp --description "Autoriser le trafic HTTPS" --direction Inbound
az network nsg rule create --resource-group $RESOURCE_GROUP --nsg-name $NSG_NAME --name BloquerSSH --priority 120 --source-address-prefixes "Internet" --source-port-ranges 22 --access Deny --protocol Tcp --description "Bloquer le trafic SSH" --direction Inbound

# Créez deux machines virtuelles, chacune dans un sous-réseau différent (suite)
az vm create --resource-group $RESOURCE_GROUP --name $VM2_NAME --location $LOCATION --vnet-name $VNET_NAME --subnet $SUBNET2_NAME --public-ip-address-allocation-method Manual --admin-username $USERNAME --admin-password $PASSWORD

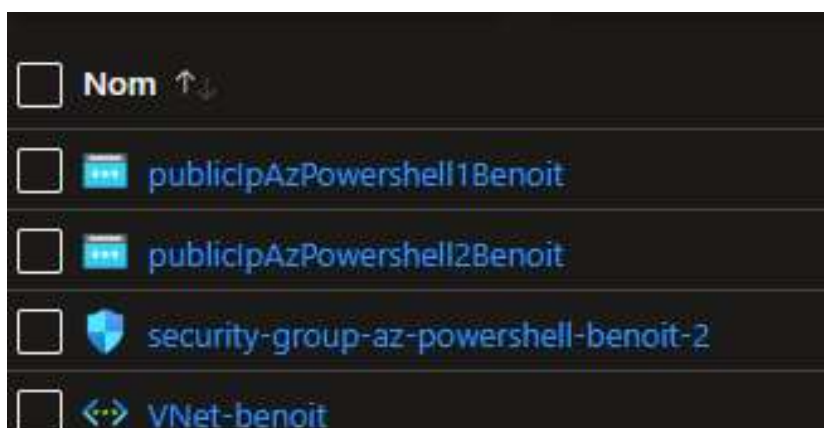
az vm open-port --resource-group $RESOURCE_GROUP --name $VM2_NAME --port 80
az vm open-port --resource-group $RESOURCE_GROUP --name $VM2_NAME --port 443

# Testez la connectivité entre les machines virtuelles et vérifiez que les règles de sécurité sont appliquées correctement
VM1_PUBLIC_IP=$(az vm show --resource-group $RESOURCE_GROUP --name $VM1_NAME --show-details --query publicIps --output tsv)
VM2_PRIVATE_IP=$(az vm show --resource-group $RESOURCE_GROUP --name $VM2_NAME --show-details --query privateIps --output tsv)
echo "Adresse IP publique de la VM1: $VM1_PUBLIC_IP"
echo "Adresse IP privée de la VM2: $VM2_PRIVATE_IP"

```

TP Azure AZ 104

- Créez un réseau virtuel Azure avec deux sous-réseaux.
- Créez un groupe de disponibilité et ajoutez-y deux machines virtuelles (VMs) avec IIS (Internet Information Services) installé.
- Configurez les machines virtuelles pour afficher un message personnalisé sur la page d'accueil d'IIS.
- Créez un équilibreur de charge (Load Balancer) et configurez-le pour répartir le trafic entre les deux VMs.
- Créez des règles de sonde pour surveiller la santé des VMs.
- Testez l'équilibrage de charge en accédant à l'adresse IP publique de l'équilibreur de charge. Vous devriez voir les messages personnalisés des deux VMs.



Créer un groupe à haute disponibilité

✓ Validation réussie

De base

Paramètres avancés

Étiquettes

Vérifier + créer

De base

Abonnement

Abonnement Azure 1

Groupe de ressources

m2i-formation

Région

Korea Central

Nom

IIS_Benoit

Nombre de domaines d'erreur

2

Nombre de domaines de mise à jour

5

Utiliser des disques managés

Non (classique)

Paramètres avancés


Groupe de placement de proximité

Aucun

Étiquettes

Name

IIS_Benoit



IIS_Benoit

Groupe à haute disponibilité

[Déplacer](#) [Supprimer](#) [Actualiser](#)

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Paramètres

Configuration

Bases

Groupe de res... [\(déplacer\)](#) : [m2i-formation](#)

Emplacement : Korea Central

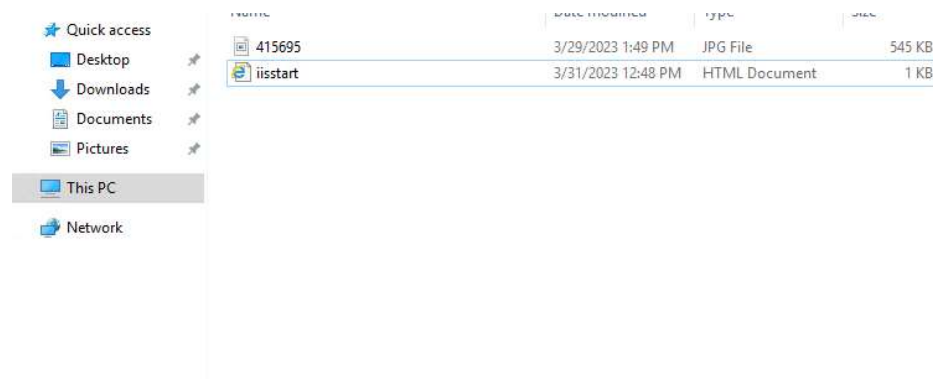
Abonnement [\(déplacer\)](#) : [Abonnement Azure 1](#)

ID d'abonnement : c49e632f-5dd4-4c37-b

We recommend that new customers choose virtual machines to decrease the number of VM instances in response to demand.

Installation rôle IIS :





Création d'une image du serveur :

Créer une image

De base Étiquettes Vérifier + créer

Créez une image à partir de cette machine virtuelle pour déployer des machines virtuelles et groupes de machines virtuelles identiques supplémentaires. Avec une image partagée, vous pouvez facilement répliquer l'image dans les régions Azure du monde entier et en gérer les versions. Certaines informations de la machine virtuelle sont reportées dans l'image, notamment le type de système d'exploitation, la génération de VM, le plan et les détails de publication. [En savoir plus](#)

Détails du projet

Abonnement: Abonnement Azure 1

Groupe de ressources *: m2i-formation

Détails de l'instance

Région: (Asia Pacific) Korea Central

Partager l'image dans Azure Compute Gallery: ☒ Oui, la partager dans une galerie sous forme de version d'image de machine virtuelle. ☐ Non, capturer uniquement une image managée.

Supprimer automatiquement cette machine virtuelle après avoir créé l'image: ☐

Détails de la galerie

Galerie de calcul Azure cible *: (nouveau) galerie_benoit [Créer](#)

État du système d'exploitation: ☒ Généralisée : les machines virtuelles créées à partir de cette image nécessitent la configuration du nom d'hôte, de l'utilisateur administrateur et d'autres configurations de machine virtuelle au premier démarrage. ☐ Spécialisée : les machines virtuelles créées à partir de cette image sont entièrement configurées et n'ont pas besoin de paramètres comme le nom d'hôte et l'utilisateur/le mot de passe administrateur.

Créer une image

De base Étiquettes **Vérifier + créer**

De base

Abonnement	Abonnement Azure 1
Groupe de ressources	m2i-formation
Région	Korea Central
Partager l'image dans Azure Compute Gallery	Oui
Supprimer automatiquement cette machine virtuelle après avoir créé l'image	Non
Galerie de calcul Azure	(nouveau) galerie_benoit
État du système d'exploitation	Generalized
Définition d'image de machine virtuelle cible	(nouveau) srv_benoit_iss
Numéro de version	1.0.0
Machine virtuelle source	iis-benoit-1

Exclure de la plus récente	Non
Date de fin de vie	Aucun
Réplication	
Nombre de répliquas par défaut	1
Réplication	Korea Central: 1
Balises	
Name	srv_benoit_iss

Une fois exécuté, cette option arrête la machine virtuelle pour créer l'image :

Le déploiement est en cours

Nom du déploiement : Microsoft.Compute-CaptureVM-202303311...

Abonnement : [Abonnement Azure 1](#)

Groupe de ressources : [m2i-formation](#)

Heure de début : 31/03/2023 16:13:37

ID de corrélation : 0ce1c419-eee2-4059-9528-e817a2efe86f

^

Détails du déploiement

Ressource	Type	Statut
 galerie_benoit/srv_benoit_iss/1.0.0	Microsoft.Compute/galleries/images/versions	Created
 galerie_benoit/srv_benoit_iss	Microsoft.Compute/galleries/images	OK
 galerie_benoit	Microsoft.Compute/galleries	OK

TP Azure AZ 104

- Créez un nouvel annuaire Azure AD.
- Ajoutez un utilisateur personnalisé et attribuez-lui un rôle administrateur dans l'annuaire.
- Créez et configurez un groupe de sécurité et ajoutez l'utilisateur personnalisé au groupe.
- Enregistrez une application dans Azure AD et configurez l'authentification en utilisant OAuth 2.0.
- Accordez des autorisations à l'application pour accéder à l'API Microsoft Graph.
- Utilisez l'API Microsoft Graph pour récupérer des informations sur les utilisateurs et les groupes de votre annuaire Azure AD.

