42-Cloud-1 Project:

1. Diagramme

Cf. piece jointe

1. Security Tables
2. myVpcBastionSecurityGroup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | All | All | 0.0.0.0/0 | Pour tester |
| SSH | TCP | 22 | 0.0.0.0/0 | J’accepte toutes les addresses IP sources qui se connectent a moi. Je peux aussi faire en sorte que je n’accepte que les addresses IP source provenant de l ecole 42 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Outbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Destination** | **Description** |
| All | All | All | 0.0.0.0/0 | Default: c est pareil que ci-dessus |
|  |  |  |  |  |

1. myVpcDatabaseSecurityGroup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| MYSQL/Aurora | TCP | 3306 | myVpcWebSecurityGroup | Je n’accepte que ce que le traffic qui provient de myVpcWebSecurityGroup, i.e. des instances Wordpress  Je n ouvre que le port 3306 puisque les instances se connectent a moi en ‘mySQL’ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Outbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Destination** | **Description** |
| All | All | All | 0.0.0.0/0 | Default: c est pareil que ci-dessus |
|  |  |  |  |  |

1. myVpcEfsMountTargetSecurityGroup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| NFS | TCP | 2049 | myVpcWebSecurityGroup | Je n’accepte que ce que le traffic qui provient de myVpcWebSecurityGroup, i.e. des instances Wordpress  Je n ouvre que le port 2049 puisque les instances se connectent a moi en ‘NFS’ |
| NFS | TCP | 2049 | myVpcEfsMountTargetSecurityGroup | !!! |
| SSH | TCP | 22 | myVpcBastionSecurityGroup | !!! |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Outbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Destination** | **Description** |
| All | All | All | 0.0.0.0/0 | Default: c est pareil que ci-dessus |
|  |  |  |  |  |

1. myVpcLoadBalancerSecurityGroup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | J accepte tout le trafic ip provenant de mes clients  Je n ouvre que le port 80 puisque les clients se connectent a moi en ‘http’ |
| HTTPS | TCP | 443 | 0.0.0.0/0 | !!! TBDr |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Outbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Destination** | **Description** |
| All | All | All | 0.0.0.0/0 | Default: c est pareil que ci-dessus |
|  |  |  |  |  |

1. myVpcWebSecurityGroup:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | myVpcLoadBalancerSecurityGroup | Je ne suis pas accessible depuis l exterieur et le suis pour le trafic provenant du Load Balancer |
| HTTPS | TCP | 443 | myVpcEfsMountTargetSecurityGroup | !!! |
| SSH | TCP | 22 | myVpcBastionSecurityGroup | L instance Bastion pourra se connecter a moi |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Outbound** | | | | |
| **Type** | **Protocol** | **Port Range** | **Destination** | **Description** |
| All | All | All | 0.0.0.0/0 | Default: c est pareil que ci-dessus |
|  |  |  |  |  |

1. Route Tables
2. myVpcPublicSubnetRouteTable:

|  |  |  |  |
| --- | --- | --- | --- |
| **myVpcPublicSubnetRouteTable** | | | |
| **Destination** | **Target** | **Propagated** | **Description** |
| 10.0.0.0/16 | Local |  |  |
| 0.0.0.0/0 | myVpcInternetGateway |  | Pour se connecter a l exterieur du reseau local |

1. myVpcWebAndDataSubnet1**a**RouteTable:

|  |  |  |  |
| --- | --- | --- | --- |
| **myVpcWebAndDataSubnet1aRouteTable** | | | |
| **Destination** | **Target** | **Propagated** | **Description** |
| 10.0.0.0/16 | Local |  |  |
| 0.0.0.0/0 | myVpcNatGateway1**a** |  | Je peux me connecter a l exterieur mais personne ne pourra pas se connecter a moi directement  Par exple, je veux upgrader Wordpress ou bien ma BD |

1. myVpcWebAndDataSubnet1**b**RouteTable:

|  |  |  |  |
| --- | --- | --- | --- |
| **myVpcWebAndDataSubnet1aRouteTable** | | | |
| **Destination** | **Target** | **Propagated** | **Description** |
| 10.0.0.0/16 | Local |  |  |
| 0.0.0.0/0 | myVpcNatGateway1**b** |  | Je peux me connecter a l exterieur mais personne ne pourra pas se connecter a moi directement  Par exple, je veux upgrader Wordpress ou bien ma BD |

1. Load test instance

C est une AMI classique (Free Tiers) ou l on installe ce script, qui permet de lancer des requetes http su le load balancer pour tester le ‘scaling’

e1r12p13% cat loadTest.sh

#!/bin/bash -ex

yum -y update

yum install -y httpd24-tools

ab -n 500000 -c 15 -t 600 -s 120 -r http://myVpcLoadBalancer-1118744953.eu-central-1.elb.amazonaws.com/

e1r12p13%

1. Wordpress First Install

C est un script a ameliorer :

* On update l instance
* On installe :
  + Httpd24 : apache
  + php70 : version de php
  + php70-mysqlnd : extension requise par php afin de se connecter a la BD
* On attend que le filesystem NFS (EFS) soit monté
* On installe wordpress sur le montage NFS ainsi il sera ‘vu’ par toutes les instances de toutes le ‘availability zones’
* On configure wordpress
* On configure opcache afin que le site web wordpress soit plus responsif

#!/bin/bash -x

bash -ex << "TRY"

EFS\_ENDPOINT="fs-27f9217e.efs.eu-central-1.amazonaws.com"

# update

yum -y update

# install httpd v2.4, php7. php70-mysqlnd (extension required by php to connect to mysql db), php70-opcach (optimise)

yum -y install httpd24 php70 php70-mysqlnd php70-opcache

# wait until EFS file system is available

while ! nc -z ${EFS\_ENDPOINT} 2049; do sleep 10; done

sleep 10

# mount EFS file system

echo "${EFS\_ENDPOINT}:/ /var/www/ nfs4 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,\_netdev 0 0" >> /etc/fstab

mount -a

# install wordpress

cd /var/www/html

wget https://wordpress.org/latest.zip

chown -R apache:apache /var/www/html/

chmod 2775 /var/www

find /var/www -type d -exec chmod 2755 {} \;

# config opcache

sed -i 's/;opcache.revalidate\_freq=2/opcache.revalidate\_freq=300/g' /etc/php-7.0.d/10-opcache.ini

# config httpd

perl -i -0pe 's/<Directory "\/var\/www">\n\s\*AllowOverride None\n/<Directory "\/var\/www">\n AllowOverride All\n/' /etc/httpd/conf/httpd.conf

chkconfig httpd on

# config opcache

sed -i 's/;opcache.revalidate\_freq=2/opcache.revalidate\_freq=300/g' /etc/php-7.0.d/10-opcache.ini

# config httpd

perl -i -0pe 's/<Directory "\/var\/www">\n\s\*AllowOverride None\n/<Directory "\/var\/www">\n AllowOverride All\n/' /etc/httpd/conf/httpd.conf

chkconfig httpd on

# start httpd

service httpd start

TRY

1. AutoScaling : *userdata*

Lorsque l AutoScaling va créer des nouvelles instances, il faut lui donner de la ‘matiere’ afin qu il puisse configurer ces nouvelles instances au ‘bootstrap’

Pas grande chose :

* On installe ce dont a besoin
* On configure
* Puis on demarre les services

# userdata

#!/bin/bash -x

bash -ex << "TRY"

EFS\_ENDPOINT="fs-27f9217e.efs.eu-central-1.amazonaws.com"

#---------------------------------------------------

# Logs are stored in /var/log/cloud-init-output.log

#---------------------------------------------------

# update

yum -y update

# install httpd v2.4, php7. php70-mysqlnd (extension required by php to connect to mysql db), php70-opcach (optimise)

yum -y install httpd24 php70 php70-mysqlnd php70-opcache

# wait until EFS file system is available

while ! nc -z ${EFS\_ENDPOINT} 2049; do sleep 10; done

sleep 10

# mount EFS file system

echo "${EFS\_ENDPOINT}:/ /var/www/ nfs4 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,\_netdev 0 0" >> /etc/fstab

mount -a

# config opcache

sed -i 's/;opcache.revalidate\_freq=2/opcache.revalidate\_freq=300/g' /etc/php-7.0.d/10-opcache.ini

# config httpd

perl -i -0pe 's/<Directory "\/var\/www">\n\s\*AllowOverride None\n/<Directory "\/var\/www">\n AllowOverride All\n/' /etc/httpd/conf/httpd.conf

chkconfig httpd on

# start httpd

service httpd start

TRY

1. Divers
2. Se connecter au Bastion

# Utiliser l agent ssh

ssh-add –K myFranckfurtKey.pem

ssh-add –L

# Se connecter a l instance Bastion :

# Copier l adresse IP public de cette instance

ssh –A ec2-user@<adresse IP public de l instance Bastion>

<Bastion prompt $> ssh ec2-user@<address ip privee de l instance de votre choix>

1. Afficher l adresse ip de l instance Web sur le site Web

J ai ajoute le plugin ‘What the file’

* Cela me permet de reperer directement le fichier php que je dois modifier
* J ai choisi de modifier le fichier ‘partials/header/logo.php’ et d ajouter ces instructions php a l endroit ou le site afficher le nom du site

PS. J ai aussi utilise un plugin Elementor afin de configurer wordpress. Donc il se peut que le fichier a modifier soit different

$server\_ip = getHostByName(getHostName());

echo esc\_html( get\_bloginfo( 'name' ) . ": " . $server\_ip);

1. Sauvegarder en format fichier yaml l infrastructure configuree sur le cloud AWS

J ai utilise CloudFormer de AWS

PS : Je n ai pas tester le re-deploiement a l identique a partir de ce fichier. Car la correction de ce projet n est pas encore faite

Cf. fichier : *42-cloud-1.project.by.cloudformer.yaml*