Procédure rédigée par : Vassenet-Guihot Romain

# *<b>DPENCLASSROOMS*

#### Table des matières

I -Introduction :	2
II -Construire le Réseau AWS :	3
III -Systèmes EC2, RDS, S3	5
IV -Load Balancer & Mise à l'échelle	12
V -VPN site à site & Intranet isolé :	16
VI -Script Cloud Formation :	20

## I - Introduction :

#### a) - Présentation du scénario

« Vous travaillez dans une petite entreprise qui se développe à l'international. L'entreprise ne dispose que de quelques machines pour la gestion de ses outils internes et pour héberger son site internet. Des incidents matériels sur le serveur de messagerie ont pénalisé l'entreprise le mois dernier. Le directeur veut éviter que la situation ne se reproduise mais réalise que fiabiliser les services en interne coûterait très cher.

L'entreprise décide donc de migrer l'ensemble de son SI vers le cloud. Les outils collaboratifs seront migrés vers Google Apps et le site de l'entreprise sera hébergé sur AWS.

L'entreprise garde simplement un serveur de fichiers dans ses locaux pour profiter de la vitesse du réseau local pour le transfert de fichiers volumineux. Ce serveur est également accessible par une liaison VPN depuis un site intranet privé hébergé sur AWS »



#### Schéma indicatif de l'infrastructure

#### b) – Instructions d'architecture

- Installez un serveur WordPress (le site de l'entreprise) sur AWS en utilisant :
  - RDS pour le stockage de la base de données
  - S3 pour le stockage des médias (via le plugin amazon-web-services)
  - EC2 et Docker pour le serveur web
  - ELB pour distribuer les requêtes sur les instances EC2
  - CloudFormation pour automatiser la création de l'infrastructure
- Tous les éléments de votre infrastructure publique devront être répartis sur plusieurs zones de disponibilité (multi-AZ). Vous utiliserez le service ELB pour la répartition des requêtes vers les différentes zones de disponibilité (AZ).
- Vous monterez une instance EC2 destinée à héberger l'application intranet sur un sous-réseau privé. Dans le cadre de ce cours, le contenu de l'intranet sera une simple page web HTML.
- En local sur votre machine, vous créerez deux machines virtuelles Linux : une pour le serveur de fichiers et une pour le serveur VPN.
- Vous établirez une liaison VPN entre votre serveur VPN local et le sous-réseau privé AWS via une instance EC2.
- Vous mettrez en place de l'auto-scaling sur les instances EC2 pour augmenter le nombre de machines dès que la charge CPU des serveurs atteint 80% en moyenne sur 5 minutes et vous veillerez à être informé par un mail à chaque fois que l'événement survient.
- Vous évaluerez les coûts de votre infrastructure AWS à partir de différentes hypothèses d'usage que vous formulerez.

### II - Construire le Réseau AWS :

a) Choisir sa région :

Il est nécessaire de définir une région dans laquelle notre infrastructure devra être installée et déployée c'est pourquoi il est recommandé de répondre à différents critères comme la région des utilisateurs finaux (temps de réponse), les coûts horaires entre les régions, les lois du droit international ( ex : respect des normes en vigueur en fonction du pays pour la prestation de service gratuite ou payante par application.) Dans ce projet nous choisirons la zone « Ohio » pour laquelle le coût horaire des machines est le plus intéressant.

1

Pour en savoir plus sur les tarifications amazon : <u>https://aws.amazon.com/fr/emr/pricing/</u> <u>https://aws.amazon.com/fr/ec2/pricing/on-demand/</u>

#### b) VPC & Sous-Réseaux

Un VPC (Virtual Private Cloud) est un réseau privé virtuel. Il s'agit d'une section réseau isolée, dans laquelle nous pourrons mettre en place les machines. Un VPC réside dans une région AWS.

Un VPC couvre toutes les zones de disponibilité de la région. Au sein d'un VPC, nous pourrons déployer un ou plusieurs **sous-réseaux** dans chaque zone de disponibilité.

**Un sous-réseau est une portion d'un VPC**, et par conséquent correspond à un sous-ensemble du bloc CIDR du VPC. C'est pourquoi il est fortement recommandé d'adresser au VPC un masque de sous réseau plus large que des masques des sous réseaux. Par exemple un VPC en /16 et ses sous réseaux en /24.

Vos VPC (2) Infos Q. Filtrer les VPC							C Actions	▼ Créer un VPC < 1 > ③
Name	$\nabla$	ID due VPC 🗸	État	$\bigtriangledown$	CIDR IPv4	CIDR IPv6	Groupe IPv6	Jeu d'options
docker-wp-vpc		vpc-fbb26590	⊘ Available		172.31.0.0/16	-	-	dopt-905cf5fb
intranet-vpn-vpc		vpc-046620c905a51ed30	🕗 Available		172.16.0.0/16	-	-	dopt-905cf5fb
4								÷
/pc-fbb26590 / docker-wp-vpc								
Détails Blocs CIDR Jou Détails	rnaux de flux	Balises						
ID du VPC		État			Noms d'hôte DNS		Résolution DNS	
D vpc-fbb26590		⊘ Available			Activé		Activé	
Location		leu d'options DHCP			Table de routage			
Default		dopt-905cf5fb			rtb-3c73ef57		acl-d5aa18be	
		Dias CIDD ID: 4			Creves ID.C			
Oui		172.31.0.0/16			Groupe IPV6		-	

Créer le sous-réseau Actions	*									<del>ତ ବ ଡ</del>
Q Filtrer par balises et attributs ou r	echercher par mot clé								K <	1 à 4 sur 4 > >
Name	✓ ID de so ✓	État -	VPC	· Bloc CIDR IPv·	Adresses IPv4 -	Le b	Zone de disponil 🔺	ID de zone de dispor-	Table de routage	ACL réseau
docker-wp-subnet-public-za	subnet	available	vpc-fbb26590   docker-w	172.31.0.0/20	4089	-	us-east-2a	use2-az1	rtb-3c73ef57	acl-d5aa18be
docker-wp-subnet-public-zb	subnet	available	vpc-fbb26590   docker-w	172.31.16.0/20	4088	-	us-east-2b	use2-az2	rtb-3c73ef57	acl-d5aa18be
intranet-vpn-subnet-privé-zc	subnet	available	vpc-046620c905a51ed30	. 172.16.1.0/24	250	-	us-east-2c	use2-az3	rtb-0c17eacc082b8a8e4   intra	acl-0285d4fceed12d
intranet-vpn-subnet-public-zc	-optionnel subnet	available	vpc-046620c905a51ed30	. 172.16.0.0/24	251	-	us-east-2c	use2-az3	rtb-0fdbc0bb23e1983f2	acl-0285d4fceed12c
Sous-réseau: subnet-06ad7e1e6a3     Description Journaux de	flux Table de routage	ACL réseau	Balises	Partage						
ID de sous-réseau VPC	subnet-06ad7e1e6a3508ca4 vpc-046620c905a51ed30   intrar	net-vpn-vpc			E	Bloc CIDR	État available IPv4 172.16.1.0/24			
Adresses IPv4 disponibles	250				Le bloc d'adre	sse CIDR	IPv6 -			
Zone de disponibilité	us-east-2c (use2-az3)				Ta	ble de rou	tage rtb-0c17eacc08	32b8a8e4   intranet-vpn-priv	-sub-route	
ACL réseau	acl-0285d4fceed12cc20				Sous-réseau (sub	net) par dé	éfaut Non			
Attribuer automatiquement une adresse IPv4 publique	Non				Auto-assign cu	stomer-ow IPv4 add	vned No			
Customer-owned IPv4 pool					Attribuer automa	tiquement	tune Non			
						adresse	IPv6			
Outpost ID	-					Proprié	taire 784822470424			

Il est également possible de louer une adresse IP publique statique appelée « elastic ip » que nous pourrons si nécessaire attacher à une instance ou à une interface réseau.

Adre	sses IP Elastic (2)							С	Actions <b>v</b>	Allou	ier l'adresse IP Elasti	ic
QF	Filtrer les adresses IP Elastic										< 1 >	۲
	Name	$\nabla$	Adresse IPv4 allouée ⊽	Туре	$\nabla$	ID d'allocation 🗸	ID d'instance associée	$\nabla$	Adresse IP privée	$\nabla$	ID d'association	
	-		3.13.18.100	Adresse IP publique		eipalloc-000ad2cebd275165b	i-02ccda7fbd5488b25 🗹		172.31.15.5		eipassoc-0f7f95e9	90aa71
	-		3.130.232.188	Adresse IP publique		eipalloc-0dcad052127918a5e	-		-		-	

Afin de communiquer avec l'extérieur, AWS met en place des passerelles de sortie ; il en existe deux sortes :

- les passerelles Internet, permettant de router du trafic réseau dans et hors de votre VPC. Les passerelles Internet supportent l'IPv4 et l'IPv6 ;
- les **passerelles de sortie** uniquement, permettant de router du trafic réseau uniquement en sortie de votre VPC. Cela peut être une alternative à la création d'une instance NAT ou d'une passerelle NAT. Les passerelles de sortie uniquement ne supportent que l'IPv6.

Après avoir créé une passerelle internet, nous devons l'attacher à notre VPC.

VPC > Passerelles Internet > igw-b3bccddb				
igw-b3bccddb / infra-gw-	wp			Actions <b>v</b>
Détails Infos				
ID de passerelle Internet 🗗 igw-b3bccddb	État ④ Attached	ID du VPC vpc-fbb26590   docker-wp-vpc	Propriétaire 🗗 784822470424	

### III - Systèmes EC2, RDS, S3

a) Installation & Sécurité

Les machines ou instances de distribution (AMI) Linux ou Windows s'installe et se paramètre grâce au service « EC2 »

Un ensemble d'options peuvent être configurés afin de répondre à différents besoins (Type d'instance : mémoire, cpu, stockage ; groupe de sécurité, zone de disponibilité)

Dans ce projet nous utiliserons l'offre gratuite disponible (t2.micro)

1. Choisir IA Étape 2 Amazon EC réseau, et v	AMI 2. Choisir un type d'instance 3 2 : Choisir un type d'ins 2 fournit un vaste éventail de types d'ins rous offrent une flexibilité dans le choix d	Configurer Fir tance stances optin de l'associatio	istance hisés pour in de resso	4. Ajout différen ources	er le stockage 5. Ajouter Its cas d'utilisation. Les in adaptées à vos application	des balises istances s ns. En sa	<ol> <li>6. Configurer le groupe de séc ont des serveurs virtuels qui pe voir plus à propos des types d'</li> </ol>	untó 7. Vérification euvent exècuter des applications. Les types instances et de la manière dont ils peuvent	d'instances se composent de différentes comb répondre à vos besoins informatiques.	inaisons de processeur, de mémoire, de	stockage et de capacité
Filtrer par:	All instance families  Gér Gér nent sélectionné : 12 micro (- ECU, 1 vi	nération acti CPU, 2.5 GH	z, 1 Gio	Affic	her / Masquer les colon	nes					
	Famille	•	Туре	*	VCPU (j)	v	Mémoire (Gio) -	Stockage d'instance (Go) (i) -	Disponible en version optimisée pour EBS ①	Performances réseau (j)	• Prise en charge IPv6 ① •
	12		t2.nano		1		0.5	EBS uniquement		Faibles à modèrées	Oui
•	12	Eligibi	t2.micro e à l'offre gr	atute	1		1	EBS uniquement		Falbles à modérées	Oul
	12		t2.small		1		2	EBS uniquement	*	Faibles à modérées	Oui

#### De la même façon nous paramétrons la base de donnée dans le service « RDS »

RDS > Ba	ases de données										
Bases o	de données			C Re	ssources de groupe	C Mod	ifier Action	s 🔻 Restaur	er à partir de S3	Créer une base de donné	ées
Q Filt	rer bases de données									$\langle 1 \rangle$	0
E	<ul> <li>Identifiant de base de données</li> </ul>	•	Rôle ⊽	Moteur ⊽	Région et AZ 🔻	Taille ⊽	Statut 🗸	Processeur	Activité actuelle	Maintenance $\triangledown$	VPC
0	database-1		Principale	MariaDB	us-east-2a	db.t2.micro	O Disponible	1.69%	1 Connexion	s	vpc-fbl
	replicadb		Réplica	MariaDB	us-east-2b	db.t2.micro	⊘ Disponible	1.17%	0 Connexion	ŝ	vpc-fbl
4											- F

Il est également important d'apporter un maximum de sécurité en filtrant le Trafic entrant/sortant.

C'est pourquoi nous devons également configurer les groupes de sécurité en fonction des besoins comme accepter les requêtes HTTP/HTTPS (80 / 443) pour les réseaux publics ou sera installé le docker wp en zone multi a-z ou bien autoriser l'écoute unique du port 3306 pour le GS base de donnée de manière à éviter la découverte du réseau par icmp par exemple et autoriser uniquement la connexion des machines EC2 Docker/Wordpress à la BDD.

Grou	pes de sécurité (1/6)	Infor	nations				C Acti	ions 🔻	Créer un groupe de sécu	rité
Q	Filter les groupes de sécurité								< 1 >	۲
	Name	V	ID du groupe de sécu… ⊽	Nom du groupe de 🔻	ID de VPC 🛛 🗢	Description $\bigtriangledown$	Propriétaire	$\nabla$	Nombre de règles e ⊽	Nomb
	Security-Load-Balancer		sg-0573a1f3b3035693f	load-balancer-wizard-1	vpc-fbb26590	load-balancer-wizard	784822470424		6 Entrées d'autorisation	1 Entré
	Security-WP-AutoScalling	)	sg-05c75729845f8f769	launch-wizard-1	vpc-fbb26590	launch-wizard-1 create	784822470424		5 Entrées d'autorisation	1 Entré
	Security-WP-za		sg-06e44c3dc9af8a98f	Docker-WP-za	vpc-fbb26590	launch-wizard-2 create	784822470424		5 Entrées d'autorisation	1 Entré
	Security-Intranet		sg-0938df59c8c28eeac	default	vpc-046620c905a51ed30	default VPC security gr	784822470424		8 Entrées d'autorisation	1 Entré
	Security-WP-zb		sg-0de53e964872108c1	Docker-WP-zb	vpc-fbb26590	launch-wizard-2 create	784822470424		5 Entrées d'autorisation	1 Entré
	Security-BDD		sg-e448c79d	default	vpc-fbb26590	default VPC security gr	784822470424		2 Entrées d'autorisation	1 Entré
g-e448 Détai	c79d - default Is Règles entrantes	Ré	gles sortantes Balises		=					
Règl	es entrantes	Р	rotocole P	lage de ports	Source			Descriptio	Modifier les règles entr	rantes
	1 (0	т	CD 7	706	so-05c75720845f8f769 (Jaune	h-wizard-1)				
MYSQ	L/Aurora		LP 5	300	3g-05c75725045101705 (taune	(1-wizaru-1)		-		

b) Configuration Docker & Wordpress :

Voici la liste des commandes utilisées afin d'installer docker composer et la création d'une base de données sécurisé avec un utilisateur non root.

Installation de Docker :

### sudo apt-get update sudo apt install apt-transport-https ca-certificates curl software-properties-common curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/debian stretch stable" apt-cache policy docker-ce sudo apt install docker-ce sudo curl -L https://github.com/docker/compose/releases/download/1.25.5/docker-compose-`uname -s`-`uname -m` -o /usr/local/bin/docker-compose sudo chmod +x /usr/local/bin/docker-compose *Création d'une base de donnée dédiée à Wordpress avec utilisateurs spécifique* apt-get install mariadb-client

mysql -h database-1.czq2xzhlagls.us-east-2.rds.amazonaws.com -u admin -p (cnx à la bdd rds parent : mot de passe : awsawsocrocr)

CREATE DATABASE wordpress CHARACTER SET utf8 COLLATE utf8\_general\_ci; (creation de la bdd "wordpress" dans la bdd parent)

GRANT ALL PRIVILEGES ON wordpress.\* TO 'wpuser'@'%' identified by 'wppassword';

mysql -h 172.31.13.203 -u wpuser -p ( connection a la BDD RDS )

(wppassword)



nano docker-compose.yml ( creation de l'installation manuel wordpress docker )

Configuration de docker afin de connecter automatiquement le service cms wordpress sous conteneur à sa bdd via Docker-compose.yml





Les connexions HTTP sont désactivé dans le VPC par default. Il faut donc les autoriser à partir du groupe de sécurité et en modifiant les règles de connexions entrantes en ajoutant le protocol http



c) Snapshots & AMI personnalisée(s)

De manière à reproduire facilement notre machine ec2 de la zone A sur la zone B sans avoir à refaire l'ensemble des configurations précédentes (système uniquement. Certains paramètres devront être ajouter à cette nouvelle instance comme le groupe de sécurité ou la modification des instances à intégrer dans l'auto-scalling groupe ) il faut créer une sauvegarde à un instant t du notre disque dur aussi appelé snapshot.

Créer un instan	tané Actions	v		∆ ⊕ ♦ Ø
M'appartenant	<ul> <li>Q, Filtrer par</li> </ul>	balises et attributs ou rechercher par mot clé		② K < 1 à 1 sur 1 > >
Name	- ID d'instan	tané 🔺 Taille 👻 Statut	✓ Démarré(e) ✓ Progression ✓ Chiffrement ✓ ID de clé KMS ✓ Alias de clé KN✓	
	snap-05744	3fc12ec 8 Gio 🥥 completed	28 avril 2020 02:37:26 UTC+2 disponible (100 %) Non chiffré	
Instantané: snap	o-057443fc12ec3a	683 Balises		
]	ID d'instantané Statut	snap-057443fc12ec3a683 completed	Progression 100% Capacité 8 Gio	
	Volume Démarré(e) Propriétaire	vol-04ea51370d64f7028 28 avril 2020 02:37:26 UTC+2 784822470424	Chiffenent Non chiffé ID de cié KMS Alias de cié KMS	
	Codes produit Description	- Website Zone B	ARN de clé KMS Restauration rapide d'instantanés -	

Après quoi il nous restera à créer une image système basé sur notre snapshot. Celle-ci sera utilisé pour choisir notre AMI personnalisé lorsque nous devrons déployer une nouvelle instance dans la zone B ou une mise à l'échelle automatisé en cas de Trafic élevé.

Lancer EC2 Image Builder	Actions ~		Δ 4	- <b>•</b>	0
M'appartenant 🛩 🔍 Filtrer	ar balises et attributs ou rechercher par mot clé	) I< <	1 à 1 s	ar 1 >	>
Name v Nom d'	MI 🔺 ID d'AMI 🔹 Source 🔹 Propriétaire « Visibilité « Statut » Date de création » Plateforme » Type de périp» Virtualisation »				
DockerWP E Website	- B ami-0c565851243d3/811 784822470424/ 784822470424 Privé available 28 avril 2020 02:43:03 UTC+2 Other Linux ebs hvm				
Image: ami-0c565851243d3f81					
Détails Autorisations	Balises				
				Modifie	н
ID d'AMI	ami-0c565851243d3/811 Website - B				
Propriétaire	784822470424 Source 784822470424/Website - B				
Statut	available Raison de l'état -				
Date de création	28 avril 2020 02:43:03 UTC+2 Platform details Linux/UNIX				
Architecture	x86_64 Usage operation RunInstances				
Type d'image	machine Type de virtualisation hvm				
Description	Website Zone B Nom du périphérique racine /dev/sda1				
Type de périphérique racine	ebs ID de disque RAM -				
ID du noyau	- Codes produit -				
Périphériques de stockage en mode bloc	/dev/sda1=snap-057443fc12ec3a683.8:true.gp2				

d) Bucket S3 & Role IAM

Pour connecter ses compartiments S3 depuis nos instances EC2, il nous faut : Créer et joindre un rôle de profil AWS Identity and Access Management (IAM) aux instances qui autorise l'accès à Amazon S3.

Vérifier que la stratégie de compartiment S3 ne possède pas de stratégie refusant l'accès. Confirmer la connectivité réseau entre l'instance EC2 et Amazon S3.

aws Services ▼			👃 AICGUIHOT 🔻 Global 💌 Support 🔻
Identity and Access Management (IAM)	<sup>Róles</sup> → s³ Récapitulatif		Supprimer le rôle
Tableau de bord	ARN de rôl	am:aws:lam::784822470424:roleIs3 🖨	
	Description du rôle	Allows EC2 instances to call AWS services on your behalf.   Modifier	
Groupes	ARN des profils d'instance	arn:aws:iam::784822470424:instance-profile/s3 🖉	
Utilisateurs	Chemi		
Rôles	Heure de création	2020-10-25 17:47 UTC+0100	
Stratégies	Dernière activit	2020-10-27 13:52 UTC+0100 (8 jours il y a)	
Fournisseurs d'identité	Durée maximale de la session	1 heure Modifier	
Paramètres du compte	Autorisations Relations d'approbation Balises	Access Advisor Révoquer les sessions	
	-		
Analyseur d'accès	<ul> <li>Permissions policies (1 strategie appliquee</li> </ul>		
Règles d'archivage	Attacher des stratégies		Ajouter une stratégie en ligne
Analyseurs			
Paramètres	Nom de la stratègie 👻	Type de	trategie 👻
Rapport sur les informations d'identification	AmazonS3FullAccess	Stratégie	gérée par AWS 🗶
Activité de l'organisation	<ul> <li>Permissions boundary (not set)</li> </ul>		
Politiques de contrôle des services (SCP)			

Dans notre scénario il est bien sur évident que le bucket ne doit pas être accessible depuis l'extérieur mais uniquement depuis nos instance EC2 comme serveur de média.

					AICGUIHOT 🔻	Global 🔻 Supp
Amazon S3 ×	Amazon S3 > stockage-aws-s3					
Compartiments	stockage-aws-s3					
Points d'accès						
Opérations par lot	Présentation des compartiments					
Access analyzer (Analyseur d'accès) pour S3	Région USA Est (Ohio) us-east-2	Nom de la ressource Amazon (ARP	) Date de 24 Oct y	création 02:08:07 PM CEST	Accéder Compartiment et objets non publics	
Paramètres du compte relatifs à Block Public Access						
Fonctionnalité spot 3	Objets Propriétés Autorisations	Métriques Gestion Points d'au	cès			
	Lacto public au compartiments et defets ett acor tous les accio publics - Ces parariettes spoplagen sen accio public Si vous avez besein d'un certain ni Modifier Bioquer tous les accès publics O Activé Bioquer Taccès public aux compartimer O Activé	di va des listes de comblé d'accès LACL), des stratégies d uniquement à compartiment et les points d'accès. No neau d'accès public à son compartiment su objets, vous s ets et aux objets, accordé via de nouvelles listes c ets et aux objets, accordé via n'importe quelles lis tes et aux objets, accordé via de nouvelles stratégi aux compartiments et objets via n'importe quelle	e compartiment, des stratégies de point recommande d'activer « Biogean tous iouver personnaliser les paramètres indi e contrôle d'accès (ACL) les de comtrôle d'accès (ACL) les de compartiment ou de point s stratégies de compartiment ou	d'accès ou tour ces éléments à la fois. Pour ble es accès publics ». Toutefois, want d'applique réduels d'dessous en function de vos cas d'util d'accès public point d'accès public	quer Tacols public à tous vos compartiments et objets 55, es paramètres, vivifier que vos applications functionner auton de stackage spécifiques. En servir plan	activez + Bloquer nt correctement
Instances (1/3) Informations			C Se c	onnecter État de l'instance	Actions V Lancer des in	stances ▼ 1 > ⊚
Instances (1/3)     Informations       Q     Filtrer les instances	: D. d'instance État de l'instance	Tune d'inst T	C Se c	onnecter État de l'instance	Actions V Lancer des in	stances ▼ 1 > @
Instances (1/3) Informations          Q. Filtrer les instances         Name       V         Image: Constraint of the standard s	b D d'instance État de l'instance Dacida 70%45480635 O En cours d'avieu	▼ Type d'inst ▼ Co	C Se c	onnecter État de l'instance Statut des Zone de d	Actions      Lancer des in     Construction     Actions      DNS IPv4 public      v	stances ▼ 1  2  3  13  18  100
Instances (1/3) Informations           Q. Filtrer les instances           Image: I	D d'instance État de l'instance 02ccda7fbd5488b25 ② En cours d'exécu	v Type d'inst v Co tion @Q t2.micro € tion @Q t2.micro €	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Statut des Zone de d Aucune + us-east-22	▼         Actions         ▼         Lancer des in                  ispo         ▲         DNS IPv4 public         ▼            ec2-3-13-18-100.us-e         ∞	stances ▼ 1  Adresse IPv 3.13.18.100 18.222.128.1
Instances (1/3) Informations          Q. Filtrer les instances         Name       V         Docker-WP-ZA       III         Docker-WP-ZB       III         Intranet-ZC       III	D d'instance État de l'instance 02ccda7/fbd5488b25 ⊘ En cours d'exécu 007ba53ba5da79fda ⊘ En cours d'exécu 080707491ed5faf96 ⊖ Arrêté(e)	▼         Type d'inst ▼         Cc           tion         QQ         t2.micro         C           tion         QQ         t2.micro         C           tion         QQ         t2.micro         C           QQ         t2.micro         C         C	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Statut des     Zone de d       Aucune +     us-east-2t       Aucune +     us-east-2t       Aucune +     us-east-2t       Aucune +     us-east-2t	▼         Actions         Lancer des in           ispo         ▲         DNS IPv4 public         ▼           ec2.3-13-18-100.us-e         ●         ec2.4-18-222-128-158.u	stances         ▼           1         >         Image: Constraint of the standard standa
Instances (1/3) Informations          Ritter les instances         Name         Docker-WP-ZA         Docker-WP-ZB         Intranet-ZC	D d'instance État de l'instance 02ccda7/bd5488b25	▼     Type d'Inst ▼     Cc       tion     QQ     t2.micro     Cc       tion     QQ     t2.micro     Cc       QQ     t2.micro     Cc	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Statut des     Zone de d       Aucune +     us-east-2c       Aucune +     us-east-2c	Actions         Lancer des in           ispo         ▲         DNS IPv4 public         ▼           ec2-3-13-18-100.us-e         ∞         −	stances         V           1         >         Image: Constraint of the standard standar
Instances (1/3) Informations          Image: Construction of the image of	D d'instance État de l'instance 02ccda7fbd5488b25	▼     Type d'inst ▼     Cr       ton     QQ     t2.micro     Cr       tion     QQ     t2.micro     Cr       QQ     t2.micro     Cr       QQ     t2.micro     Cr	C Se o ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Statut des     Zone de d       Aucune +     us-east-2t       Aucune +     us-east-2t       Aucune +     us-east-2t	▼         Actions ▼         Lancer des in           ispo         ▲         DNS IPv4 public         ▼           ec2.3-13-18-100.us-e         ●         ec2.18-222.128-158.u           -         −	stances V 1 > @ Adresse IPv 3.13.18.100 18.222.128.13 -
Instances (1/3) Informations          Image: Construction of the image: Construc	D d'instance État de l'instance O2ccda7/bd5488b25 ⓒ En cours d'exécu 007ba53ba5da79fda ⓒ En cours d'exécu 080707491ed5faf96 ⓒ Arrêté(e)	v     Type d'inst v     Cr       tion     QQ     t2.micro     Cr       tion     QQ     t2.micro     Cr       QQ     t2.micro     -	C Se o ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Etat de l'instance       Statut des     Zone de d       Aucune +     us-east-2t       Aucune +     us-east-2t       Aucune +     us-east-2t       ID de VPC     ID de VPC	▼       Actions ▼       Lancer des in         ispo       ▲       DNS IPv4 public       ▼         ec23-13-18-100.us-e       ●       •         ec218-222-128-158.u       −	stances V 1 > © Adresse IPv 3.13.18.100 18.222.128.19 -
Instances (1/3) Informations          Ritter les instances         Name       II         Docker-WP-ZA       II         Docker-WP-ZB       II         Intranet-ZC       II         Type d'instance       t2.micro	D d'instance État de l'instance 02ccda7fbd5488b25	▼       Type d'inst       ▼       Cr         tion       QQ       t2.micro       C         tion       QQ       t2.micro       C         QQ       t2.micro       C         QQ       t2.micro       -	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Statut des       Zone de d         Aucune +       us-east-2t         Aucune +       us-east-2t         Aucune +       us-east-2t         D de VPC           ID de VPC	▼       Actions ▼       Lancer des in         ispo       ▲       DNS IPv4 public       ▼         ec2.3-13.18-100.us-e       ●       ec2.18-222.128-158.u         -       -       −         ocker-wp-vpc]       [2]	stances         V           1         >         ©           Adresse IPv         3.13.18.100           18.222.128.11         -
Instances (1/3) Informations C. Filtrer les instances Name V II Docker-WP-ZA I- Docker-WP-ZB I- Intranet-ZC I- Type d'instance t2.micro Rôle IAM	n D d'instance État de l'instance 02ccda7/bd5488b25	▼       Type d'Inst ▼       Cc         tion       QQ       t2.micro       Q         tion       QQ       t2.micro       Q         QQ       t2.micro       -         Adresses IP Elastic       □       3.13.18.100 [Adresse IP publique]         ID de sous-réseau       ID de sous-réseau	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies	Etat de l'instance         Statut des       Zone de d         Aucune +       us-east-2t         Aucune +       us-east-2t         Aucune +       us-east-2t         Aucune +       us-east-2t         ID de VPC       ID de VPC         ID de VPC       ID de VPC	Actions         Lancer des in           (spo         DNS IPv4 public         (           ecc2-3-13-18-100.us-e         (           ecc2-18-222-128-158.u         (           -         (	stances         V           1         >         ©           Adresse         IPv         3.13.18.100           18.222.128.11         -         -
Instances (1/3) Informations	D d'instance État de l'instance 02ccda7fbd5488b25 ② En cours d'exécu 007ba55ba5da79fda ③ En cours d'exécu 080707491ed5faf96 ④ Arrêté(e)	v       Type d'inst v       Cc         tion       QQ       t2.micro       Cc         tion       QQ       t2.micro       Cc         QQ       t2.micro       C         QQ       t2.micro       -         Adresses IP Elastic       ID       3.13.18.100 [Adresse IP publique]         ID de sous-réseau       ID       subnet-9cf20df7 (docker-wp-subnet)	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies +t-public-za)	Etat de l'instance         Statut des       Zone de d         Aucune +       us-east-2c         Aucune +       us-east-2c         Aucune +       us-east-2c         ID de VPC       ID de VPC         ID de VPC       Vpc-fbb26590 (c	Actions     Lancer des in       ispo     NS IPv4 public     v       ec2-3-13-18-100 us-e     v       ec2-18-222-128-158.u       ocker-wp-vpc)	stances V 1 > ③ Adresse IPv 3.13.18.100 18.222.128.11 -
Instances (1/3) Informations          Filtrer les instances         Name         Docker-WP-ZA         Docker-WP-ZB         Intranet-ZC         Intranet-ZC         Type d'instance         t2.micro         Rôle IAM         Is 3 2         Détails de Linstance       Informations	nmations	v     Type d'inst v     Co       tion     QQ     t2.micro     Co       ition     QQ     t2.micro     Co       QQ     t2.micro     -	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies 	Statut des Zone de d Aucune + us-east-2c Aucune + us-east-2c Aucune + us-east-2c ID de VPC Vpc-fbb26590 (c Surveillance	Actions     Lancer des in       ispo     DNS IPv4 public     v       ec2-3-13-18-100 us-e     v       ec2-18-222-128-158.u       ocker-wp-vpc	stances
Instances (1/3) Informations C. Filtrer les instances Docker-WP-ZA II Docker-WP-ZA II Docker-WP-ZB II Intranet-ZC II Type d'instance t2.micro Rôle IAM S 5 2 Plateforme C Linux/UNIX	n D d'instance État de l'instance 02ccda7fbd5488b25	v       Type d'Inst v       Cc         tion       QQ       t2.micro       Q         tion       QQ       t2.micro       Q         QQ       t2.micro       -         Adresses IP Elastic       -       -         ID de sous-réseau       -       -         ID de t/AMI       -       -	C Se c ntrôle des statuts 2/2 vérifications réussies 2/2 vérifications réussies tr-public-za) C vP EC2 - ZA/B)	Etat de l'instance         Statut des       Zone de d         Aucune +       us-east-2c         Aucune +       us-east-2c         Aucune +       us-east-2c         Jucune +       us-east-2c         Surveillance       G         Surveillance       désactivé	Actions     Lancer des in       ispo     NDNS IPv4 public        ecc2-313-18-100.us-e        ecc2-18-222-128-158.u   ocker-wp-vpc) [2]	stances

Puis nous pouvons vérifier l'accès du compartiment S3 (crée depuis la console via le service s3) depuis nos instances EC2 de la zone A/B



### IV - Load Balancer & Mise à l'échelle

AWS fournit un **service d'équilibrage de charge** ou *Load Balancer*, c'est-à-dire un composant qui va distribuer les requêtes réseau vers différentes machines, afin de **répartir** la charge sur plusieurs éléments de l'infrastructure, permettant de paralléliser les traitements.

Équilibreur de charge d'application
HTTP HTTPS Créer
Choisissez un équilibreur de charge d'application quand vous avez besoin d'un ensemble de fonctions flexible pour vos applications web avec un trafic HTTP et HTTPS. En opérant au niveau des demandes, les équilibreurs de charge d'application fournissent des fonctions avancées de routage et de visibilité ciblant les architectures d'application, y compris les microservices et les conteneurs.
En savoir plus >

a) Configuration du Load Balancing

Les options indispensables dans notre cas sont d'ajouter la disponibilité multi a-z grâce à leurs sous-réseaux respectif de manière à équilibrer la charge entre les machines EC2 des deux zones.

Créer un équilit	breur de charge	Actions *				<del>0</del> ¢	0
Q Filtrer par ba	lises et attributs ou r	echercher par mot clé				< < 1 à 1 sur 1 >	>
Nom		Nom du DNS	<ul> <li>État</li> </ul>	<ul> <li>ID de VPC</li> </ul>	<ul> <li>Zones de disponibilité - Type</li> </ul>	<ul> <li>Créé le</li></ul>	
ELB		ELB-275071419.us-east-2.elb.amaz	zonaws.com active	vpc-fbb26590	us-east-2b, us-east-2a application	26 octobre 2020 15:25:46 U	
Équilibreur de c	harge: ELB					880	5
Description	Écouteurs S	urveillance Services intégrés	Balises				1
Configuratio	on de base						Т
	Nom	ELB					
	ARN	arn:aws:elasticloadbalancing:us	-east-2:784822470424:loadbala	incer/app/ELB/39693293922bfe6c 🖨			
	Nom du DNS	ELB-275071419.us-east-2.elb.a (Enregistrement A)	imazonaws.com 省				l
	État	active					
	Туре	application					
	Méthode	internet-facing					
	Type d'adresse IP	ipv4					
		Modifier le type d'adresse IP	2				
	VPC	vpc-fbb26590 🗷					
Zone	es de disponibilité	subnet-7de9dc07 - us-east-2b ( Adresse IPv4: Attribuées pa	Z ar AWS				
		subnet-9cf20df7 - us-east-2a Adresse IPv4: Attribuées pa	ar AWS				
		Modifier les sous-réseaux (s	subnets)				
	Zone hébergée	Z3AADJGX6KTTL2					
ł	Heure de création	26 octobre 2020 15:25:46 UTC+	+1				

EC2 > Groupes cibles > site Internet				
site Internet				Supprimer
🗗 am: aws: elasticloadbalancing: us-east-2: 7848224704	124: groupe cible / site web / 37ed6	b66416f8e9f		
Configuration de base				
Type de cible instance d'instance	Protocole: Port HTTP : 80 Version du protocole HTTP1		VPC vpc-fbb26590 🔀	Équilibreur de charge ELB 🕻
Attributs				Modificateur
Permanence Activée Durée de la permanence 4 heures Algorithme d'équilibrage de charge Tourniquet (round robin)			Retard d'annulation d'enreg 300 secondes Durée de démarrage lent O seconde	listrement
Détails du groupe Cibles Surveillance	Balises			
Cibles enregistrées (2) Q. Filtrer les ressources par propriété au valeur				C     Enregistrer les cibles       < 1     >
ID d'instance	Nom	♥ Port ♥	Zone 🗸	Détails du statut
i-02ccda7fbd5488b25	Docker-WP-ZA	80	us-east-2a	Target is in the stopped state
i-007ba53ba5da79fda	Docker-WP-ZB	80	us-east-2b	Target is in the stopped state

Vérification du fonctionnement ELB avec algorithme du tourniquet & permanence de 4H/Session



b) Configuration de la mise à l'échelle automatique (auto scalling)

Le but de la mise à l'échelle automatisé est de lancée un nombre x d'instance temporaire et de même image (AMI) afin de supporter les charges de Trafic importantes selon certains critères ( dans notre cas lorsque la charge CPU>80%). Par définition, l'élasticité de notre infrastructure adaptera d'ellemême son nombres d'instances en zone multi a-z selon une stratégie de mise à l'échelle que nous allons configurer dans notre groupe autoscalling.

Tout d'abord nous devons configurer un groupe de lancement afin de paramétrer les différentes options de lancement des futures instances. Ce groupe de lancement est indépendant du groupe de mise à l'échelle car c'est lui qui est en charge de répondre à des critères comme : OU & QUOI, QUI & COMMENT ( ces deux derniers points pourront être modifier dans le groupe autoscalling )

( Définition des Zones de lancement, groupe de sécurité, sans oublier l'image ( AMI ) à utiliser et le type d'instance ( t2.micro dans notre cas ) )

Configurations de lancement (1)	Info		C Actions <b>v</b>	Créer une configuration de lancement
<b>Q</b> Rechercher des configurations de lancem	ent			< 1 >
Nom	▼ ID d'AMI	▼ Type d'instance	▼ Heure de création	

Il nous faut donc crée un groupe de mise à l'échelle et associé nos instances EC2 de la zone A & B afin que ces dernières fassent partie intégrante de ce groupe. On définira également une stratégie

de mise à l'échelle selon des alarmes basées sur des métriques d'instance, la capacité souhaitée, minimal & maximal de notre déploiement automatisé.

Groupes Auto Scaling (1/1)			C Modifier Supprimer Créer un groupe Auto S	icaling		
Q Rechercher vos groupes Auto Scaling			< 1	>		
Nom V Modèle/configuration	de lance ⊽ Instances ⊽ Statut	▼ Capacité s	souh $ abla M abla M abla Zones de disponibilité$			
Architecture OC P10 Groupe de Lancement -	AutoScalling 0 💮 Mise à j	our de la capacité 2	2 4 us-east-2a, us-east-2b			
	_					
tails Activité Mise à l'échelle automatique Ges	stion des instances Surveillance Actua	lisation d'instance				
étails du groupe			Mo	difier		
pacité souhaitée	Nom du groupe Auto Scaling					
	Architecture OC P10					
pacité minimale	Date de création	٥ (المحمد محمد الم				
	Mon May 11 2020 15:44:02 GM1+020	o (neure d'ete d'Europe centrale)				
pacite maximale	Amazon Resource Name (ARN) arn:aws:autoscaling:us-east-2:784822	470424:autoScalingGroup:43fa9d16-				
	c44e-42cc-ad34-c9035d6701e2:auto P10	ScalingGroupName/Architecture OC				
onfiguration de lancement			Mo	difier		
nfiguration de lancement	ID d'AMI	Groupes de sécurité				
oupe de Lancement - AutoScalling	ami-0c565851243d3f811		sg-06e44c3dc9af8a98f 🖾 sg-0de53e964872108c1 🖾 sg-e448c7	9d 🔼		
oupe de Lancement - AutoScalling pe d'instance	ami-0c565851243d3f811 Nom de la paire de clés		sg-06e44c3dc9af8a98f 🕻 sg-0de53e964872108c1 🕻 sg-e448c7 Heure de création	9d 🔼		
oupe de Lancement - AutoScalling pe d'instance           Groupes Auto Scaling         Architecture OC P10	ami-0c565851243d3f811 Nom de la paire de clés		sg-06e44c3dc9af8a98f ⊠sg-0de53e964872108c1 ⊠sg-e448c7 Heure de création	9d 🖸		
oupe de Lancement - AutoScalling pe d'instance > Groupes Auto Scaling > Architecture OC P10 2étails Activité Mise à l'échelle automatique G	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f 🖄 sg-0de53e964872108c1 🖄 sg-e448c7 Heure de création	9d 🔼		
oupe de Lancement - AutoScalling pe d'instance > Groupes Auto Scaling > Architecture OC P10 Détails Activité Mise à l'échelle automatique G	ami-Oc565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f 🖄 sg-0de53e964872108c1 🖄 sg-e448c7 Heure de création	9d 🗹		
oupe de Lancement - AutoScalling pe d'instance > Groupes Auto Scaling > Architecture OC P10 Détails Activité Mise à l'échelle automatique G itratégies de mise à l'échelle (2) Info	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f ≧sg-0de55e964872108c1 ≧sg-e448c7 Heure de création           C         Actions ▼         Ajouter une stratégie	9d 🔀		
upe de Lancement - AutoScalling se d'instance > Groupes Auto Scaling > Architecture OC P10 Détails Activité Mise à l'échelle automatique G Stratégies de mise à l'échelle (2) Info	ami-Oc565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f ≧sg-0de55e964872108c1 ≧sg-e448c7 Heure de création           C         Actions ▼         Ajouter une stratégie	9d 🖸		
uppe de Lancement - AutoScalling         be d'instance         Stroupes Auto Scaling > Architecture OC P10         Détails       Activité         Mise à l'échelle automatique       G         Stratégies de mise à l'échelle (2) Info         AutoScalling_WP_ZA         Stratégies	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB	sg-06e44c3dc9af8a98f [2sg-0de53e964872108c1 [2sg-e448c7 Heure de création C Actions ▼ Ajouter une stratégie <	9d 🗹		
uppe de Lancement - AutoScalling         se d'instance         > Groupes Auto Scaling > Architecture OC P10         Détails       Activité         Mise à l'échelle automatique       G         Stratégies de mise à l'échelle (2) Info         AutoScalling_WP_ZA         ype de stratégie:         dise à l'échelle simple	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple	sg-06e44c3dc9af8a98f [2sg-0de53e964872108c1 [2sg-e448c7] Heure de création           C         Actions ▼         Ajouter une stratégie	9d 🗹		
Stratégies de mise à l'échelle automatique         AutoScalling_WP_ZA         Ype de stratégie:         Hise à l'échelle suitomatique	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple Activé ou désactivé? Activée	sg-06e44c3dc9af8a98f ≧sg-0de55e964872108c1 ≧sg-e448c7 Heure de création	9d 🗹		
oupe de Lancement - AutoScalling pe d'instance    Groupes Auto Scaling > Architecture OC P10  Détails Activité Mise à l'échelle automatique G  Stratégies de mise à l'échelle (2) Info  AutoScalling_WP_ZA  Type de stratégie:  We à l'échelle simple  Activé ou désactivé?  Désactivée  Exécuter la stratégie quand:	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f ≧sg-0de55e964872108c1 Èsg-e448c7 Heure de création           C         Actions ▼         Ajouter une stratégie	9d 🗹		
oupe de Lancement - AutoScalling pe d'instance	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance	sg-06e44c3dc9af8a98f [2sg-0de53e964872108c1 [2sg-e448c7 Heure de création           C         Actions ▼         Ajouter une stratégie            Jillization >= 80 pendant 1 périodes conséruitives de 300 serondes nour	9d 🗹 1		
uppe de Lancement - AutoScalling         > Groupes Auto Scaling > Architecture OC P10         Détails       Activité       Mise à l'échelle automatique       C         Stratégies de mise à l'échelle (2) Info         AutoScalling_WP_ZA         ype de stratégie:         tise à l'échelle simple         ctrivée         xécuter la stratégie quand:         IV>80%_WPZA         épasse le seuil de falarme : CPUUtilization >= 80 pendant 1 pério         imensions de métrique :         Instrated = 1-202cda7h95488b25	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple Activé ou désactivé? Activé Exécuter la stratégie quand: CPU>80%_WPZB dépasse le seuil de l'alarme : CPUL dimensions de métrique : Instanced = 1-0070ba53ba5da7	sg-06e44c3dc9af8a98f [2sg-0de55e964872108c1 [2sg-e448c7] Heure de création           C         Actions ▼         Ajouter une stratégie            Jtilization >= 80 pendant 1 périodes consécutives de 300 secondes pour         9fda	9d 🗹 1		
oupe de Lancement - AutoScalling pe d'instance   Groupes Auto Scaling > Architecture OC P10  Détails Activité Mise à l'échelle automatique  Stratégies de mise à l'échelle (2) info  AutoScalling_WP_ZA  ype de stratégie: Aise à l'échelle simple  kctivé ou désactivé?  Pésactivée  ixécuter la stratégie quand: :PU>80%_WPZA lépasse le seuil de l'alame : CPUUtilization >= 80 pendant 1 péric limensions de mérique: Instanceld = I-02ccda7/bd5488b25  Yenez la mesure suivante:	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple Activé ou désactivé? Activée Exécuter la stratégie quand: CPU>80%_WPZB dépasse le seui de l'alarme : CPUL dimensions de métrique : Instanceld = 1-0070a53ba5da7: Prenez la mesure suivante:	sg-06e44c3dc9af8a98f ≧sg-0de55e964872108c1 ≧sg-e448c7 Heure de création           C         Actions         ▼         Ajouter une stratégie            Jtilization >= 80 pendant 1 périodes consécutives de 300 secondes pour         9fda         9fda	1		
oupe de Lancement - AutoScalling pe d'instance	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple Activé ou désactivé? Activée Exécuter la stratégie quand: CPU>80%_WPZB dépasse le seui de l'alarme : CPUL dimensions de métrique : Instanceld = i-007ba55ba5da7: Prenez la mesure suivante: Ajouter 1 unités de capacité	sg-06e44c3dc9af8a98f [2sg-0de55e964872108c1 [2sg-e448c7 Heure de création           C         Actions ▼         Ajouter une stratégie            Jtilization >= 80 pendant 1 périodes consécutives de 300 secondes pour         9fda	9d 🗹		
oupe de Lancement - AutoScalling pe d'instance	ami-0c565851243d3f811 Nom de la paire de clés iestion des instances Surveillance Act	ualisation d'instance AutoScalling_WP_ZB Type de stratégie: Mise à l'échelle simple Activée Exécuter la stratégie quand: CPU>80%_WPZB dépasse le seuil de t'alarme : CPUL dimensions de métrique : Instanceld = i-007ba53ba5da7 Prenez la mesure suivante: Ajouter 1 unités de capacité	sg-06e44c3dc9af8a98f [2sg-0de53e964872108c1 [2sg-e448c7] Heure de création           C         Actions ▼         Ajouter une stratégie            Jtilization >= 80 pendant 1 périodes consécutives de 300 secondes pour         9fda	9d 🕻		

Enfin nous veillerons à être averti par notification email dès qu'une machine est lancée par effet de mise à l'échelle selon notre stratégie de CPU>80%.

Ces stratégies nécessitent la création d'alarmes « cloudwatch » avec action. Cette prise de mesure ou action est activé dès lors que le seuil de l'alarme est dépassé afin d'ajouter une unité de capacité supplémentaire à notre groupe de mise à l'échelle.

C'est à dire dimensionner de façon automatisée et donc « scaller » notre infrastructure (élastique) pour répondre aux besoins croissants d'une application qui fonctionne et qui obtient toujours plus de trafic, ou simplement des « pics » à des moments clés.

EC2 > Groupes Auto Scaling	
Groupes Auto Scaling (1/1)	C Modifier Supprimer Créer un groupe Auto Scaling
Q. Rechercher vos groupes Auto Scaling	< 1 > ©
✓ Nom	Capacité souh… ♥ M… ♥ M… ♥ Zones de disponibilité
Architecture OC P10 Groupe de Lancement - AutoScalling 0 💬 Mise à jour de la capacité	2 2 4 us-east-2a, us-east-2b
Détails Activité Mise à l'échelle automatique Gestion des instances Surveillance Actualisation d'instance	
Notifications d'activité (1)	C Actions V Créer une notification
Q Filtrer les notifications	< 1 > @
Envoyer à	⊽
my-sns-topic (romain.guihot@gmail.com)	

Un test a été réalisé avec la création d'une stratégie pour CPU>0,1% de manière à vérifier la scalabilité, et les notifications ③

	Q	Rechercher dans les	messages						•									?	() ()
	÷	001	<b>e</b>	¢,	D		:										15	i sur 1 188	<
		AWS Notifications <n À moi 👻</n 	no-reply@sns.a	mazonaw	s.com>										dim. 15 r	iov. 10:10 (il	l y a 10 jou	irs) 🟠	4
		🛪 Détecter la lang	gue ▾ > t	rançais	- Trad	uire le me	essage										Désac	tiver pour	anglais
		You are receiving this e 09:04:00)] was greater View this alarm in the A https://us-east-2.consol	email because than the thresi AWS Managem le.aws.amazor	your Ama hold (0.01 ient Cons	zon Clou )." at "Su ole: udwatch/f	dWatch A nday 15 I nome?reg	Narm "CPU>0,1% November, 2020 gion=us-east-2#s	_TEST" in the I 09:10:37 UTC".	US East (Ohi ) )=CPU%3E09	nio) region h	has entered th	e ALARM state, I	ecause "Thresh	hold Cros	ssed: 1 dat	apoint [0.16	661572659	9071966 (1	5/11/20
ńc		Alarm Detailis: - Name: ( - Description: - State Change: - Reason for State Cha - Timestamp: - AWS Account: - Alarm Arn:	CPU>0,1%_TE CPU>0,1% W INSUFFICIE inge: Thresh Sunday 15 N 784822470 arn:aws:cloud	EST P ZA ALE NT_DAT/ old Cross ovember, 424 watch:us-	:RTE + Al A -> ALAF ed: 1 data 2020 09: east-2:78	UTOSCAI M spoint [0.1 10:37 UT 4822470	LLING ACTION A 16615726590719 FC 424:alarm:CPU>	JOUTE 1 UNIT 66 (15/11/20 09 0,1%_TEST	rÉ 9:04:00)] was	s greater th	ian the thresh	old (0.01).							
		Threshold: - The alarm is in the AL	ARM state wh	en the me	etric is Gr	eaterTha	nThreshold 0.01	or 60 seconds.											
		Monitored Metric: - MetricNamespace: - MetricName: - Dimensions: - Period: - Statistic: - Unit:	AWS CPUUM [Instand 60 second Average not specifie	S/EC2 illization celd = i-0: ls id	2ccda7fbo	15488b25	5]												
		State Change Actions: - OK:																	

V - VPN site à site & Intranet isolé :

Le but étant de faire communiquer notre réseau d'entreprise locale (simulé par des VM de distribution debian sur mon réseau privé) à l'intranet hébergé chez aws dans un sous réseau privé isolé et inaccessible autrement que par le tunnel VPN.



Coté AWS, il est indispensable de créer un sous réseau privée et un sous réseau public qui sera utilisé uniquement afin de sortir sur internet provisoirement pour installer les packets d'un frontal web (apache, php : service httpd )

On pensera également à créer un groupe de sécurité pour n'autoriser que notre réseau privée d'entreprise à communiquer et définir les routes associées.

🔪 Filtrer par balises et attributs ou re	chercher par mot clé								I< <	1 à 4 sur 4 > >
Name	✓ ID de so	État -	VPC -	Bloc CIDR IPv~	Adresses IPv4 ~	Le b	Zone de disponil 🗕	ID de zone de dispoi~	Table de routage	ACL réseau
docker-wp-subnet-public-za	subnet	available	vpc-fbb26590   docker-w	172.31.0.0/20	4088	-	us-east-2a	use2-az1	rtb-3c73ef57	acl-d5aa18be
docker-wp-subnet-public-zb	subnet	available	vpc-fbb26590   docker-w	172.31.16.0/20	4088	-	us-east-2b	use2-az2	rtb-3c73ef57	acl-d5aa18be
intranet-vpn-subnet-privé-zc	subnet	available	vpc-046620c905a51ed30	172.16.1.0/24	250	-	us-east-2c	use2-az3	rtb-0c17eacc082b8a8e4   intra	acl-0285d4fceed
intranet-vpn-subnet-public-zc-o	optionnel subnet	available	vpc-046620c905a51ed30	172.16.0.0/24	251	-	us-east-2c	use2-az3	rtb-0fdbc0bb23e1983f2	acl-0285d4fcee
Description Journaux de R	market and a second second	0.01	Deliana	Destage						
Description Journaux de fl	Table de routage	ACL résea	au Balises	Partage						
Description Journaux de fi Modifier une association de tab able de routage: rlb-0c17eacc082	UX Table de routage Ne de routage 2068a8e4   intranet-vpn-priv-s	ACL résea	au Balises	Partage						
Description Journaux de fi Modifier une association de tab able de routage:rtb-0c17eacc082	ux Table de routage ne de routage 208a8e4   intranet-vpn-priv-s  < < 1 à 2 s	ACL réseauterent automotion autom	au Balises	Partage						
Description Journaux de fi Modifier une association de tab able de routage: rtb-0c17eacC082 Destination C	ux Table de routage Ile de routage 2068a6e4   intranet-vpn-priv-s K < 1 à 2 s Sible	ACL résea ub-route aur 2 > >	au Balises	Partage						
Description Journaux de fi Modifier une association de tab fable de routage: rtb-0c17eacc082 Destination C 192,168,1.024 v	ux Table de routage le de routage 26888e4   intranet-vpn-priv-s K < 1 à 2 s Sible gw-01ad971f696ec61fa	ACL réseauter ACL réseauter AC	au Balises	Partage						

Comme pour AWS, notre serveur VPN local de distribution debian devra être en mode routeur.

En editant le fichier /etc/sysctl.conf

net.ipv4.ip\_forward = 1

Explication de l'installation de Strongswan sur notre serveur VPN local avec la commande suivante :

apt-get install strongswan -y

Ensuite on va préparer la configuration de la future liaison VPN. En éditant le fichier /etc/ipsec.conf

conn	aws
	type=tunnel
	authby=secret
	left=192.168.1.10 # Addresse IP Du serveur VPN Local
	leftid=31.35.80.99 # Addresse Public Local Entreprise ( Fournit par mon FAI )
	right=3.15.75.58 # Addresse Public AWS
	leftauth=psk
	rightauth=psk
	keyexchange=ikev1
	ike=aes128-sha1-modp1024
	ikelifetime=8h
I	esp=aes128-sha1-modp1024
	lifetime=1h
	keyingtries=%forever
	leftsubnet=192.168.1.0/24 # Réseau Privé Local Entreprise
	rightsubnet=172.16.1.0/24 # Réseau Privé AWS Zone C
I	dpddelay=10s
	dpdtimeout=30s
	dpdaction=restart
	auto=start

On edite également le fichier /etc/ipsec.secrets afin de procéder à l'échange de clé entre nos deux points de terminaison.

31.35.80.99 3.15.75.58 : PSK "NBr3REZUHoC8pgjooi6C0VNoHuToX\_Oq"

Après un redémarrage du vpn client/serveur notre tunnel vpn est montée et nous pouvons le vérifier des deux côtés de notre infrastructure (nous constatons également que nos routes & groupes de sécurité fonctionne correctement puisque depuis le routeur vpn local nous accédons aux travers du tunnel à notre intranet en 172.16.1.80 :

Q Filtrer par balises et att	tributs ou rechercher par mo	ot clé							   K < 1 i	1sur1 > >∣
Name VID	O d'VPN	▲ État →	Passerelle privée virtuelle	<ul> <li>Transit Gateway</li> </ul>	- Passe	relle client - Adre	sse de passerelle clier	nt 👻 Inside Ip Version	- Type	<ul> <li>Catégori</li> </ul>
vpn-to-lan vp	pn-Da6f1e6efc8Dab397	disponible	vgw-01ad971f696ec61fa   infra	a	cgw-0	23a0dbed2a17fab7   aws 31.35	.80.99	IPv4	ipsec.1	VPN
Connexion VPN: vpn-0a6	offe6efc80ab397	Balises			0.0.0					880
Tunnel State								Γ.	/ 1 è 0 aur	
Tunnel Number	En dehors de l'adress	A l'intérieur du	CIDR IF Inside IPv6 CIDR		Statut	Dernier statut modifié	Détails	Certificate AR	< 1 a 2 sur:	2 > >
Tunnel 1	3 15 75 58	169 254 82 248/	30 -		HAUT	4 novembre 2020 17:46:08 LITC+	1 .			
Tunnel 2	3.138.42.120	169.254.199.244	4/30 -		BAS	20 octobre 2020 05:19:33 UTC+2	-			
generat sending receive parsed connect root@Cl PING 17 64 byte 64 byte 64 byte 64 byte 64 byte 7C 172 4 packe rtt min root@Cl	ing QUICK packet: QUICK_MOI ion 'aws ient-VPN- 2.16.1.80 s from 17 s from 17	<pre>(_MODE from 1 from 1 estab OE resp estab (172. 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1 72.16.1</pre>	me/ocr# 1p request 29 .92.168.1.1 3.15.75.58 onse 29898 lished suc ome/ocr# pi 16.1.80) 5 .80: icmp_ .80: icmp	sec up aw 89813632 0[4500] to 13632 [ H/ cessfully ng 172.16 6(84) byt seq=1 ttl: seq=2 ttl: seq=3 ttl: seq=4 ttl:  d, 0% pacl 22.116/120	s [ HASH 9 0 3.15.7 192.164 ASH SA 1 .1.80 es of da =254 tin =254 tin =254 tin =254 tin =254 tin sket loss 6.497/2	SA No KE ID 75.58[4500] 8.1.10[4500] No KE ID ID ata. me=120 ms me=126 ms me=120 ms me=120 ms s, time 3007 .572 ms	ID ] (316 byt (316 by ]	ces) (tes)		

Il nous faudra bien sur définir à notre serveur de fichier local (192.168.1.20) comme passerelle par défault l'addresse ip de notre serveur vpn local (192.168.1.10)

De ce fait nos postes clients ou tout autre serveur d'entreprises pourront traverser le tunnel VPN à condition d'avoir toujours comme route par défault le serveur VPN local en mode routeur.

PING 172.16.1.80	0 (172.16.1.80)	56(84) bytes of (	data.							
From 192.168.1.1	L0: icmp_seq=1 Re	edirect Host(New	nextho	op: 192.	168.1.2	254)				
64 bytes from 17	72.16.1.80: icmp	_seq=1 ttl=253 t:	ime=120	ms						
From 192.168.1.1	L0: icmp_seq=2 Re	edirect Host(New	nextho	op: 192.	168.1.2	254)				
64 bytes from 17	72.16.1.80: icmp	_seq=2 ttl=253 t:	ime=120	) ms						
From 192.168.1.1	L0: icmp_seq=3 Re	edirect Host(New	nextho	op: 192.	168.1.2	254)				
64 bytes from 17	72.16.1.80: icmp	_seq=3 ttl=253 t:	ime=120	) ms						
From 192.168.1.1	L0: icmp_seq=4 Re	edirect Host(New	nextho	op: 192.	168.1.2	254)				
64 bytes from 172.16.1.80: icmp_seq=4 ttl=253 time=121 ms										
From 192.168.1.10: icmp_seq=5 Redirect Host(New nexthop: 192.168.1.254)										
64 bytes from 17	/2.16.1.80: icmp_	_seq=5 ttl=253 t:	ime=121	lms						
From 192.168.1.1	LO: icmp_seq=6 Re	edirect Host(New	nextho	op: 192.	168.1.2	254)				
64 bytes from 17	/2.16.1.80: icmp_	_seq=6 ttl=253 t:	ime=121	lms						
^C										
172.16.1.80	ping statistics									
6 packets transm	nitted, 6 receive	ed, 0% packet los	ss, tin	ne 5007n	ns					
rtt min/avg/max/	/mdev = 120.524/1	120.993/121.355/0	ð.306 m	ıs						
<pre>root@Client-VPN·</pre>	-VM:/home/ocr# ro	oute -n								
Table de routage	a IP du noyau									
Destination	Passerelle	Genmask	Indic	Metric	Ref	Use	Iface			
0.0.0.0	192.168.1.10	0.0.0.0	UG	0	0	0	enp0s3			
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	enp0s3			

Il nous reste à vérifier que l'on accède via le service web de notre serveur de fichier à la page intranet de notre serveur sur le réseau privé aws au travers du tunnel ipsec 🐵

Mozilla Fir	efox	
173163 AN 4		
← → ℃ ₪ 0 % 172.16.1.80	···· © ☆ III\ 🗊 🛎 🗏	
Félicitation ! Vous êtes désormais connecté sur notre intranet hé	bergé chez aws & accessible uniquement grâce au tunnel	
vpn ipsec depuis le reseau prive de l'entreprise.		
Menu		

```
ec2-user@ip-172-16-1-80:~
                                                                            root@Client-VPN-VM:/home/ocr# ssh -i "awsocr.pem" ec2-user@172.16.1.80
Last login: Wed Nov 4 17:07:35 2020 from 192.168.1.10
                      Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-16-1-80 ~]$ ping 192.168.1.20
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.
4 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=120 ms
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=121 ms
64 bytes from 192.168.1.20: icmp_seq=3 ttl=63 time=121 ms
64 bytes from 192.168.1.20: icmp_seq=4 ttl=63 time=121 ms
64 bytes from 192.168.1.20: icmp_seq=5 ttl=63 time=121 ms
<mark>`</mark>C
--- 192.168.1.20 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 120.931/121.159/121.289/0.400 ms
[ec2-user@ip-172-16-1-80 ~]$
```

### **VI - Script Cloud Formation :**

La force de ce projet est également la capacité à concevoir entièrement son architecture grâce à la programmation avec la création de modèle aussi appelé « pile ».

Ces piles au format json ou yaml regroupes l'ensembles des ressources et dépendances nécessaires à la création complète d'une infrastructure répondant à divers besoins.

Coinbase utilise par exemple la puissance de L'IaC AWS pour centraliser, maitriser, tester, concevoir et déployer en production toutes les ressources de l'infrastructure hébergeant l'application de portefeuilles numériques basé sur les technologies de la blockchain.

• Veuillez consulter le fichier .yaml afin de prendre connaissance du modèle complet pour la création totale de l'infrastructure du projet.

```
Description: "Architecture Projet 10 OCR"
Resources:
    EC2VPC:
3
         Type: "AWS::EC2::VPC"
3
         Properties:
             CidrBlock: "172.31.0.0/16"
             EnableDnsSupport: true
             EnableDnsHostnames: true
             InstanceTenancy: "default"
3
             Tags:
3
                 Key: "Name"
                 Value: "docker-wp-vpc"
3
    EC2VPC2:
         Type: "AWS::EC2::VPC"
3
         Properties:
             CidrBlock: "172.16.0.0/16"
             EnableDnsSupport: true
             EnableDnsHostnames: false
             InstanceTenancy: "default"
Ξ
             Tags:
3
                 Key: "Name"
                 Value: "intranet-vpn-vpc"
3
    EC2Subnet:
         Type: "AWS::EC2::Subnet"
-
         Properties:
             AvailabilityZone: !GetAtt EC2Instance3.AvailabilityZone
             CidrBlock: "172.31.0.0/20"
             VpcId: !Ref EC2VPC
             MapPublicIpOnLaunch: true
3
             Tags:
3
                 Key: "Name"
                 Value: "docker-wp-subnet-public-za"
Ξ
    EC2Subnet2:
         Type: "AWS::EC2::Subnet"
3
         Properties:
             AvailabilityZone: !GetAtt EC2Instance.AvailabilityZone
             CidrBlock: "172.31.16.0/20"
             VpcId: !Ref EC2VPC
             MapPublicIpOnLaunch: true
Ξ
             Tags:
3
                 Key: "Name"
                 Value: "docker-wp-subnet-public-zb"
```