

Cloud Computing – Amazon Web Services

Objectifs :

- Utiliser des services de cloud computing
- Déployer des sites web sur internet

Contenu

1. Qu'est-ce que le cloud computing ?.....	2
2. AWS Educate	2
2.1. Connection à AWS via AWS Educate	3
2.2. Les services d'AWS à utiliser pour l'activité	4
2.2.1. Le service S3	4
2.2.2. Le service EC2	5
3. Informations importantes concernant EC2.....	5
3.1. Lancement d'une machine virtuelle EC2	5
3.2. Se connecter à une machine virtuelle EC2	6

1. Qu'est-ce que le cloud computing ?

C'est la fourniture de services informatiques:

- De manière automatisée (on accède aux services commandés dans les minutes suivant la commande)
- En self-service (au travers d'un portail web)
- A la demande (on obtient les services quand on en a besoin, et on les arrête quand on n'en a plus besoin)

Les services informatiques fournis par un fournisseur de services cloud sont, pour les plus connus :

- Des machines virtuelles (avec différentes technologies : virtualisation, « containerisation »)
- Du stockage
- Des bases de données
- Une plateforme de développement complète
- Un logiciel complet (exemple : un logiciel de comptabilité)

... mais un fournisseur de cloud en fournit beaucoup plus.

Les différents types de cloud se définissent par le genre de services fournis :


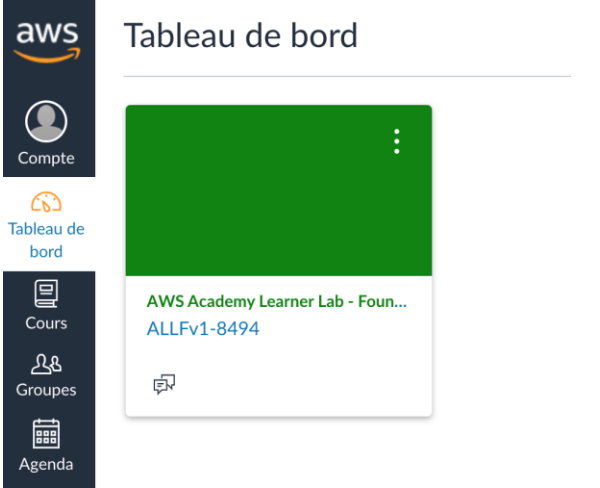
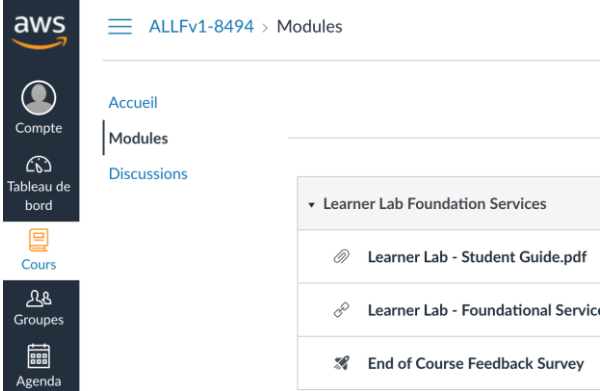
- IaaS : Infrastructure as a Service → le fournisseur de cloud fournit des services d'infrastructure comme des machines virtuelles, du stockage ou des bases de données, et le client gère le reste (il installe les logiciels/applications lui-même)
- PaaS : Platform as a Service → le fournisseur de cloud fournit comme service une plateforme complète sur laquelle le client installe ou déploie son application. Le client, ici, ne se soucie pas des serveurs, bases de données ou autre.
- SaaS : Software as a Service → le fournisseur de cloud fournit un logiciel complet, et gère tout, de l'infrastructure à l'application.

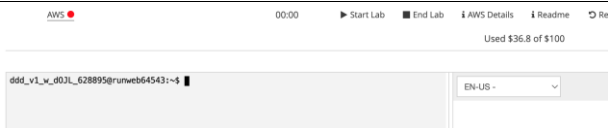



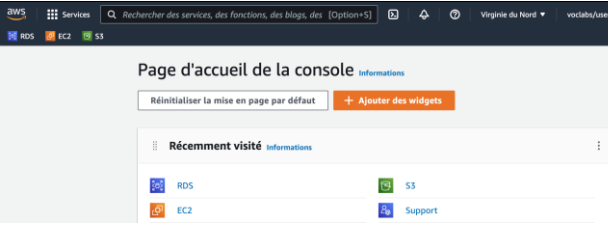
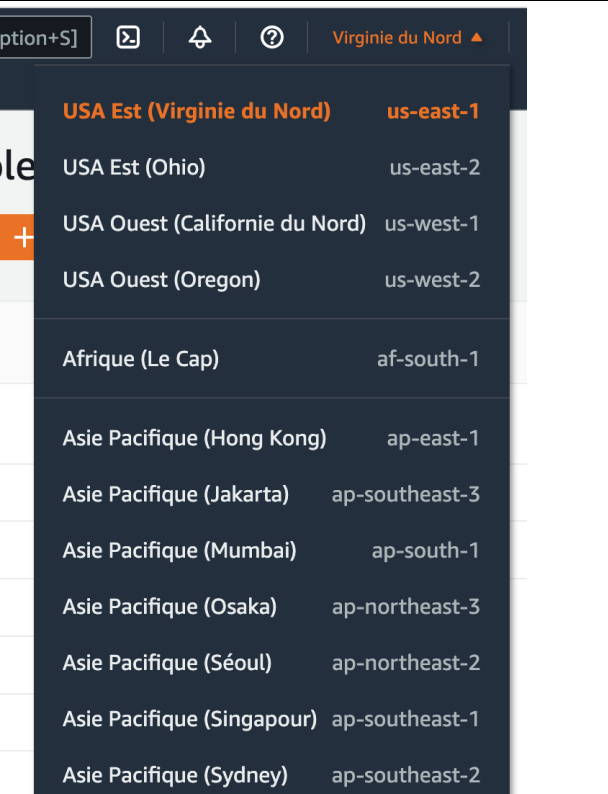
2. AWS Educate

Le lycée Saint-Michel est inscrit au programme « AWS Educate », ce qui permet aux étudiants d'avoir accès au cloud d'AWS de manière gratuite (crédit de 100\$).

L'accès au portail des services d'AWS se fait au travers de la plateforme instructure.com (plateforme d'apprentissage en ligne).

2.1. Connection à AWS via AWS Educate

<p>1- Aller sur https://www.awsacademy.com/LMS_Login</p>	
<p>2- Cliquer sur « student login » et connectez-vous avec votre email @saintmichelannecy.fr</p>	
<p>3- Vous arrivez alors dans un portail d'apprentissage en ligne sur lequel vous avez le cours « AWS Academy Learner Lab – Foundation Services »</p>	
<p>4- Aller dans le menu « Modules » puis cliquer sur « Learner Lab – Foundational Services »</p>	

<p>5- Dans le portail de votre lab, cliquer sur ► Start Lab</p>	
<p>6- Le lien AWS passe au jaune , puis au vert </p>	
<p>7- Cliquer sur  pour accéder à la console AWS qui vous permet d'utiliser les services cloud d'AWS</p>	
<p>8- Notes : vous ne pouvez provisionner des services que dans le datacenter (ou plutôt, la zone de disponibilité) de Virigine du Nord (par défaut). Vous ne devez pas modifier ceci.</p>	

2.2. Les services d'AWS à utiliser pour l'activité

2.2.1. Le service S3

S3 est un service de stockage de fichiers en ligne. Il permet de stocker des fichiers et des répertoires avec une manière très fine de gestion des droits d'accès.
C'est le service technique qui se cache sous les services iCloud d'Apple ou Dropbox.

Il permet aussi de mettre à disposition des sites web statiques, c'est-à-dire qui s'exécute avec un simple navigateur (et développés avec les langages standard du web : HTML, CSS, JavaScript). On ne peut pas héberger de sites web dynamiques construits avec des langages qui ont une exécution « côté serveur » comme PHP.

2.2.2. Le service EC2

EC2 ou Elastic Cloud Computing, est un service de fourniture de machines virtuelles. Le service EC2 permet de lancer des instances (= machines virtuelles) de différentes caractéristiques (nombre de CPUs, quantité de RAM, performance des disques, etc....) avec un système d'exploitation au choix (Linux Ubuntu, Linux Suse, Windows Server 2019, etc.....).

EC2 permet aussi le déploiement de machines virtuelles avec des applications pré-installées.

3. Informations importantes concernant EC2

3.1. Lancement d'une machine virtuelle EC2

Quand vous lancez une nouvelle instance EC2, vous devez à un moment donné, sélectionner une paire de clés. Sélectionnez la paire de clés « vockey » qui est proposée.

▼ **Paire de clés (connexion)** Informations

Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

Nom de la paire de clés - obligatoire

Sélectionner

Q

Continuer sans paire de clés (Non recommandé) Valeur par défaut

vockey
Type : rsa

Créer une paire de clés

Modifier

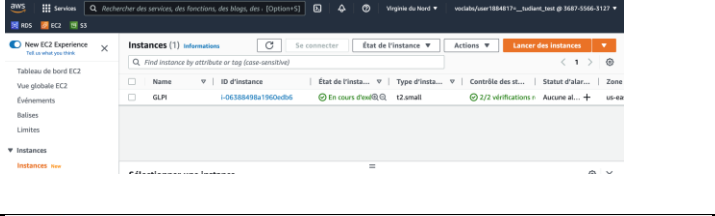
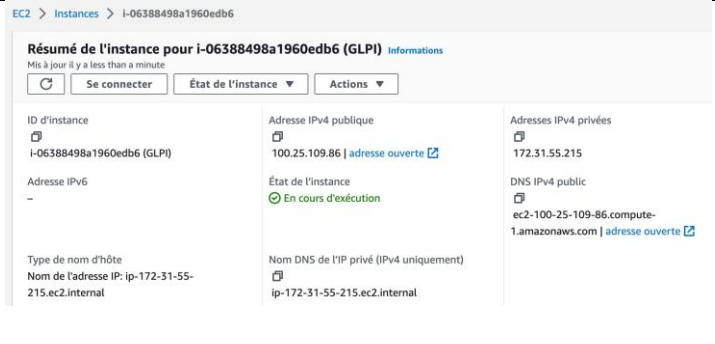
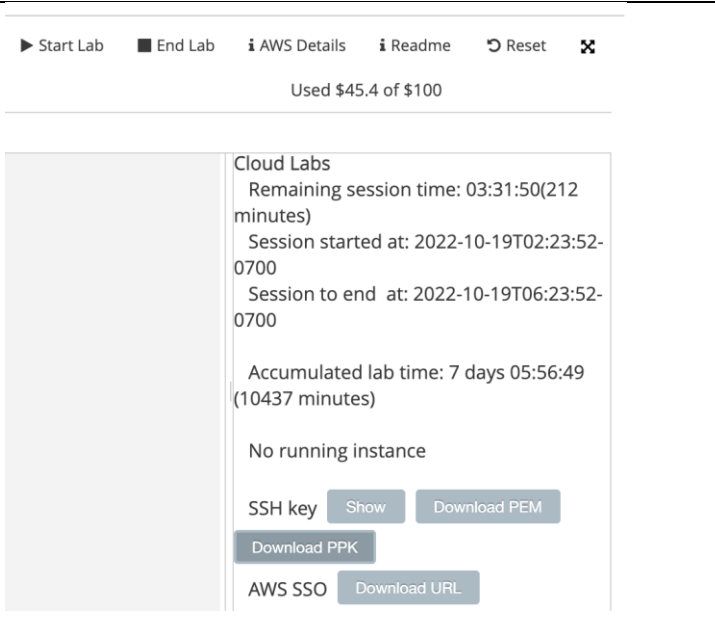
La clé privée correspondant est téléchargeable depuis la page de démarrage de votre Lab AWS Educate.

The screenshot shows the AWS Educate interface. On the left is a sidebar with navigation links: Compte, Tableau de bord, Cours, Agenda, Boîte de réception, and Historique. The main content area shows the 'Learner Lab - Foundational Services' page. At the top, there's a status bar with 'AWS' and a green dot, a timer '03:24', and buttons for 'Start Lab', 'End Lab', 'AWS Details', 'Readme', 'Reset', and a close icon. Below this, it says 'Used \$45.4 of \$100'. The main area is divided into two sections. The left section shows a terminal window with the prompt 'ddd_v1_w_zR9_1125837@runweb64547:~\$'. The right section shows 'Cloud Labs' session details: 'Remaining session time: 03:31:50(212 minutes)', 'Session started at: 2022-10-19T02:23:52-0700', 'Session to end at: 2022-10-19T06:23:52-0700', 'Accumulated lab time: 7 days 05:56:49 (10437 minutes)', and 'No running instance'. At the bottom right, there are two buttons: 'Download PPK' (circled in red) and 'Download PEM'.

3.2. Se connecter à une machine virtuelle EC2

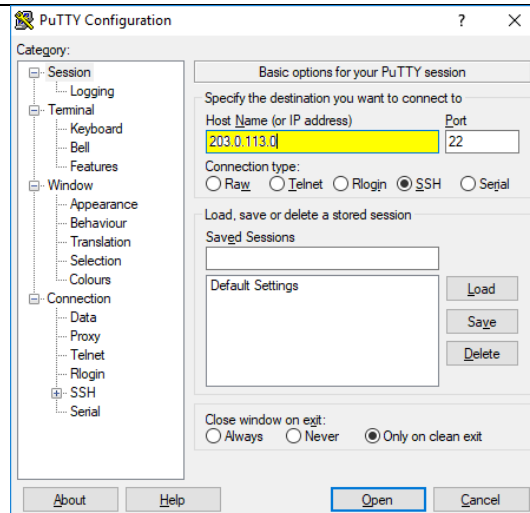
Vous aurez besoin d'accéder à la machine virtuelle linux que vous aurez déployé pour installer la « stack » LAMP (= Linux Apache MySQL PHP).

Ci-dessous, un guide pour vous connecter à une machine virtuelle Linux :

<p>Aller dans la liste de vos instances EC2</p>	
<p>Cliquer sur l'ID de l'instance pour obtenir les détails de l'instance. Vous y trouvez l'adresse IP publique de votre machine ainsi que son nom DNS publique.</p>	
<p>Dans la page de démarrage de votre Lab AWS Educate, cliquer sur AWS Details puis cliquer sur Download PPK pour télécharger le fichier de clé privée qui vous permettra de vous connecter à votre instance EC2.</p>	

Sur votre PC, lancer l'application Putty.

Dans la zone « Host Name (or IP address), entrer l'adresse IP publique ou le nom DNS publique.



Dans le volet **Catégorie**, développez **Connexion**, développez **SSH**, puis choisissez **Auth**. Suivez les instructions suivantes :

- a. Choisissez **Parcourir**.
- b. Sélectionnez le fichier .ppk que vous avez téléchargé précédemment

Cliquer sur Open pour se connecter à la machine Linux.

Installation de WordPress sur un serveur AWS Linux 2

Compléments aux didacticiels

Suivre les indications détaillées dans <https://fr.wordpress.org/support/article/how-to-install-wordpress/>, mais attention aux détails suivants :

- 1- Exécuter les commandes « `wget https://wordpress.org/latest.tar.gz` » et « `tar -xzf latest.tar.gz` » dans le répertoire `/var/www/html/` **sans sudo**
- 2- Puis, ré-exécuter les commandes du tutoriel d'installation de LAMP sur AWS EC2 Linux 2 :
 - a. `sudo chmod 2775 /var/www && find /var/www -type d -exec sudo chmod 2775 {} \;`
 - b. `find /var/www -type f -exec sudo chmod 0664 {} \;`

Si vous avez exécuté la commande `tar` avec `sudo`, réexécuter la commande suivante :
`sudo chown -R ec2-user:apache /var/www`

Vous pouvez ensuite continuer la procédure d'installation de Wordpress normalement (création de base de données, puis exécuter l'application wordpress dans le navigateur qui permet de lancer le wizzard d'installation).

Une fois wordpress installé, vous devez modifier le fichier `/var/www/html/wordpress/wp-config.php` et ajouter juste après la ligne :
`define('NONCE_SALT', 'put your unique phrase here');`

la ligne:

`define('FS_METHOD', 'direct');`

Pour modifier le fichier `/var/www/html/wordpress/wp-config.php`, utiliser l'utilitaire **nano**. (taper `nano` suivi du nom du fichier à modifier).

Dans nano, au fois votre fichier modifié, faites Ctrl+o suivi d'un appui sur la touche « entrée » puis Ctrl+x pour fermer le fichier.

Dernière modification pour autoriser wordpress à uploader des fichiers de 100 Mo, vous devez passer les paramètres `upload_max_filesize` et `post_max_size` dans le fichier `/etc/php.ini` à 100M


```
; Maximum allowed size for uploaded files.  
; http://php.net/upload-max-filesize  
upload_max_filesize = 100M  
  
; Maximum size of POST data that PHP will accept.  
; Its value may be 0 to disable the limit. It is ignored if POST data reading  
; is disabled through enable_post_data_reading.  
; https://php.net/post-max-size  
post_max_size = 100M
```

Pour modifier le fichier `/etc/php.ini`, utiliser l'utilitaire **nano avec sudo**. (taper *sudo nano* suivi du nom du fichier à modifier)

Et finalement, redémarrer le serveur web avec ces 2 commandes :

sudo systemctl restart httpd

sudo service php-fpm restart

Atelier : Création de votre VPC et lancement d'un serveur web

Version 4.6.6 (TESS1)

Dans cet atelier, vous allez utiliser Amazon Virtual Private Cloud (VPC) pour créer votre propre VPC et y ajouter des composants supplémentaires pour obtenir un réseau personnalisé. Vous allez également créer des groupes de sécurité pour votre instance EC2. Ensuite, vous allez configurer et personnaliser une instance EC2 pour exécuter un serveur web et lancer ce dernier dans le VPC.

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources Amazon Web Services (AWS) dans un réseau virtuel que vous avez défini. Ce réseau virtuel ressemble beaucoup à un réseau classique que vous utiliseriez dans votre propre centre de données, avec l'avantage d'utiliser l'infrastructure évolutive d'AWS. Vous pouvez créer un VPC couvrant plusieurs zones de disponibilité.

Scénario

Dans cet atelier, vous allez créer l'infrastructure suivante :

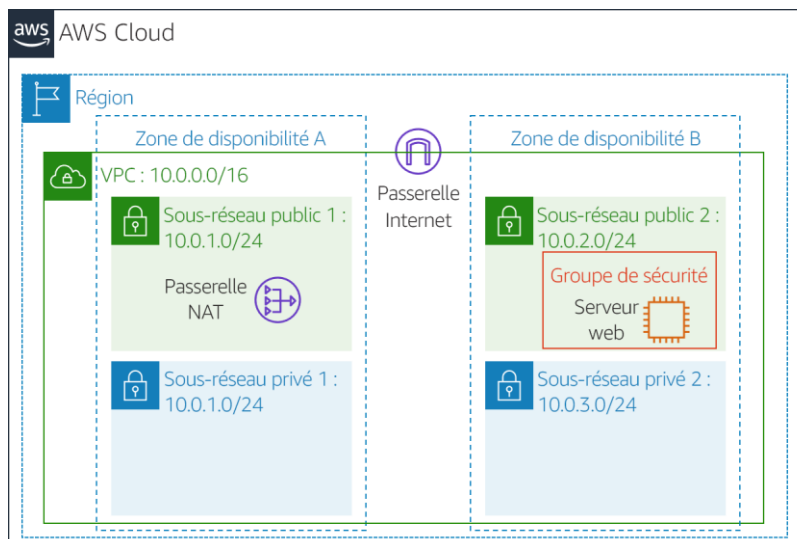


Table de routage publique

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle Internet

Table de routage privée

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle NAT

Objectifs

À la fin de cet atelier, vous serez en mesure d'effectuer les opérations suivantes :

- Créer un VPC
- Créer des sous-réseaux
- Configurer un groupe de sécurité
- Lancer une instance EC2 dans un VPC

Durée

Cet atelier dure environ **30 minutes**.

Accès à AWS Management Console

1. Accéder à la console AWS à partir du cours AWS Leaner Lab, comme vu précédemment.

AWS Management Console s'ouvre dans un nouvel onglet. Le système vous y connecte automatiquement.

Conseil : Si le nouvel onglet de navigateur ne s'ouvre pas, une bannière ou une icône s'affiche généralement en haut de votre navigateur pour indiquer que celui-ci bloque l'ouverture des fenêtres contextuelles du site. Choisissez la bannière ou l'icône et choisissez « Allow pop ups » (Autoriser les fenêtres contextuelles).

2. Disposez l'onglet AWS Management Console de façon à l'afficher à côté de ces instructions. Dans l'idéal, vous devez pouvoir voir les deux onglets en même temps, pour suivre plus facilement les étapes de l'atelier.

Tâche 1 : Création de votre VPC

Dans cette tâche, vous allez utiliser l'Assistant VPC pour créer un VPC, une passerelle Internet et deux sous-réseaux dans une seule zone de disponibilité. Une **passerelle Internet (IGW)** est un composant VPC qui autorise la communication entre les instances de votre VPC et Internet.

Après avoir créé un VPC, vous pouvez y ajouter des **sous-réseaux**. Chaque sous-réseau doit résider entièrement dans une zone de disponibilité et ne peut pas

s'étendre sur plusieurs zones. Si le trafic de votre sous-réseau est acheminé vers une passerelle Internet, le sous-réseau est reconnu comme un *sous-réseau public*. Si un sous-réseau ne possède pas de route vers la passerelle Internet, il est appelé *sous-réseau privé*.

L'assistant créera également une *passerelle NAT*, qui sert à fournir une connectivité Internet aux instances EC2 dans les sous-réseaux privés.

5. Dans la **Console de gestion AWS**, dans le menu **Services**, choisissez **VPC**.
6. Choisissez **Launch VPC Wizard** (Démarrer l'assistant VPC).
7. Dans le panneau de navigation de gauche, choisissez **VPC with Public and Private Subnets** (VPC avec des sous-réseaux publics et privés) (la deuxième option).
8. Choisissez **Select** (Sélectionner), puis configurez les paramètres suivants :
 - **VPC name** (Nom du VPC) : `picasso-expo` (VPC dédié à l'infrastructure pour l'expo Picasso)
 - **Availability Zone** (Zone de disponibilité) : sélectionnez la *première* zone de disponibilité.
 - **Public subnet name** (Nom du sous-réseau public) : `Public Subnet 1` (Sous-réseau public 1)
 - **Availability Zone** (Zone de disponibilité) : sélectionnez la *première* zone de disponibilité (identique à celle utilisée ci-dessus).
 - **Private subnet name** (Nom du sous-réseau privé) : `Private Subnet 1` (Sous-réseau privé 1)
 - **Elastic IP Allocation ID** (ID d'allocation d'adresse IP Elastic) : cliquez dans la zone et sélectionnez l'adresse IP affichée.
9. Choisissez **Create VPC** (Créer un VPC).

L'Assistant va créer votre VPC.

10. Une fois l'opération terminée, choisissez **OK**.

L'Assistant a mis en service un VPC avec un sous-réseau public et un sous-réseau privé dans la même zone de disponibilité, ainsi que des tables de routage pour chaque sous-réseau :

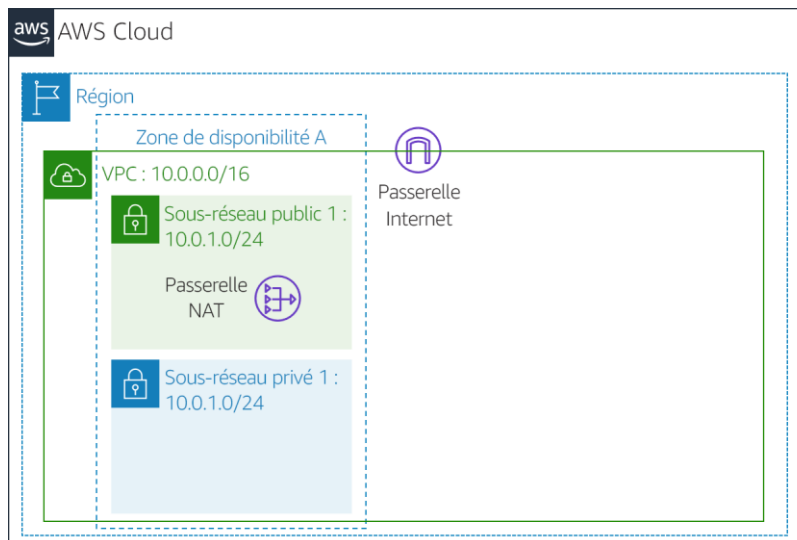


Table de routage publique

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle Internet

Table de routage privée

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	NAT gateway

Le sous-réseau public possède le bloc d'adresses CIDR **10.0.0.0/24**, ce qui signifie qu'il contient toutes les adresses IP commençant par **10.0.0.x**.

Le sous-réseau privé possède le bloc d'adresses CIDR **10.0.1.0/24**, ce qui signifie qu'il contient toutes les adresses IP commençant par **10.0.1.x**.

Tâche 2 : Création de sous-réseaux supplémentaires

Avec cette tâche, vous allez créer deux sous-réseaux supplémentaires dans une deuxième zone de disponibilité. Ceci vous permet de créer des ressources dans plusieurs zones de disponibilité afin de fournir une *haute disponibilité*.

11. Dans le panneau de navigation de gauche, choisissez **Subnets** (Sous-réseaux).

Tout d'abord, vous allez créer un second sous-réseau public.

12. Choisissez **Create subnet** (Créer un sous-réseau), puis configurez les éléments suivants :

- **VPC ID** (ID de VPC) : `picasso-expo`
- **Subnet name** (Nom du sous-réseau) : `picasso-expo-subnet-public2` (Sous-réseau public 2)
- **Availability Zone** (Zone de disponibilité) : sélectionnez la *deuxième* zone de disponibilité.
- **IPv4 CIDR block** (Bloc d'adresses CIDR IPv4) : `10.0.2.0/24`

Toutes les adresses IP du sous-réseau commenceront par **10.0.2.x**.

13. Choisissez **Create subnet** (Créer un sous-réseau).

Vous allez maintenant créer un second sous-réseau privé.

14. Choisissez **Create subnet** (Créer un sous-réseau), puis configurez les éléments suivants :

- **VPC ID** (ID de VPC) : `picasso-expo`
- **Subnet name** (Nom du sous-réseau) : `picasso-expo-subnet-private2` (Sous réseau privé 2)
- **Availability Zone** (Zone de disponibilité) : sélectionnez la *deuxième* zone de disponibilité.
- **CIDR block** (Bloc d'adresses CIDR) : `10.0.3.0/24`

Toutes les adresses IP du sous-réseau commenceront par **10.0.3.x**.

15. Choisissez **Create subnet** (Créer un sous-réseau).

Vous allez maintenant configurer les sous-réseaux privés pour acheminer le trafic lié à Internet vers la passerelle NAT afin que les ressources du sous-réseau privé puissent se connecter à Internet, tout en conservant les ressources privées. Pour ce faire, vous devez configurer une *table de routage*.

Une *table de routage* contient un ensemble de règles, appelées *routes*, qui sont utilisées pour déterminer où le trafic réseau est dirigé. Chaque sous-réseau d'un VPC doit être associé à une table de routage. Cette table de routage contrôle le routage pour le sous-réseau.

16. Dans le panneau de navigation de gauche, choisissez **Route Tables** (Tables de routage).
17. Sélectionnez la table de routage avec la configuration suivante : **Main = Yes** et **VPC = Lab VPC**. (Développez la colonne *VPC ID* (ID de VPC) si nécessaire pour afficher le nom du VPC.)
18. Dans la colonne **Name** (Nom) de cette table de routage, choisissez l'icône de crayon , saisissez `Private Route Table` (Table de routage privée), puis choisissez **Save** (Enregistrer).
19. Dans le volet inférieur, choisissez l'onglet **Routes**.

Notez que **Destination 0.0.0.0/0** est configuré sur **Target nat-xxxxxxx**. Cela signifie que le trafic destiné à Internet (0.0.0.0/0) sera envoyé à la passerelle NAT. La passerelle NAT transférera ensuite le trafic vers Internet.

Cette table de routage est donc utilisée pour acheminer le trafic à partir de sous-réseaux privés. Vous allez maintenant ajouter un nom à la table de routage pour la rendre plus reconnaissable par la suite.

20. Dans le volet inférieur, choisissez l'onglet **Subnet Associations** (Associations de sous-réseau).

Vous allez maintenant associer cette table de routage aux sous-réseaux privés.

21. Choisissez **Edit subnet associations** (Modifier les associations de sous-réseau).
22. Sélectionnez à la fois **Private Subnet 1** (Sous-réseau privé 1) et **Private Subnet 2** (Sous-réseau privé 2).

Vous pouvez développer la colonne *Subnet ID* (ID de sous-réseau) pour afficher les noms de sous-réseau.

23. Choisissez **Save associations** (Enregistrer les associations).

Vous allez maintenant configurer la table de routage utilisée par les sous-réseaux publics.

24. Sélectionnez la table de routage avec la configuration suivante : **Principal = Non** et **VPC = picasso-expo-vpc** (et désélectionnez les autres sous-réseaux).
25. Dans la colonne **Name** (Nom) de cette table de routage, choisissez l'icône de crayon , saisissez **Private Route Table** (Table de routage privée), puis choisissez **Save** (Enregistrer).
26. Dans le volet inférieur, choisissez l'onglet **Routes**.

Notez que **Destination 0.0.0.0/0** est configuré sur **Target igw-xxxxxxx**, c'est-à-dire la passerelle Internet. Cela signifie que le trafic lié à Internet sera envoyé directement à Internet via la passerelle Internet.

Vous allez maintenant associer cette table de routage aux sous-réseaux publics.

27. Choisissez l'onglet **Subnet Associations** (Associations de sous-réseau).
28. Choisissez **Edit subnet associations** (Modifier les associations de sous-réseau).
29. Sélectionnez à la fois **Public Subnet 1** (Sous-réseau public 1) et **Public Subnet 2** (Sous-réseau public 2).
30. Choisissez **Save associations** (Enregistrer les associations).

Votre VPC dispose désormais de sous-réseaux publics et privés configurés dans deux zones de disponibilité :

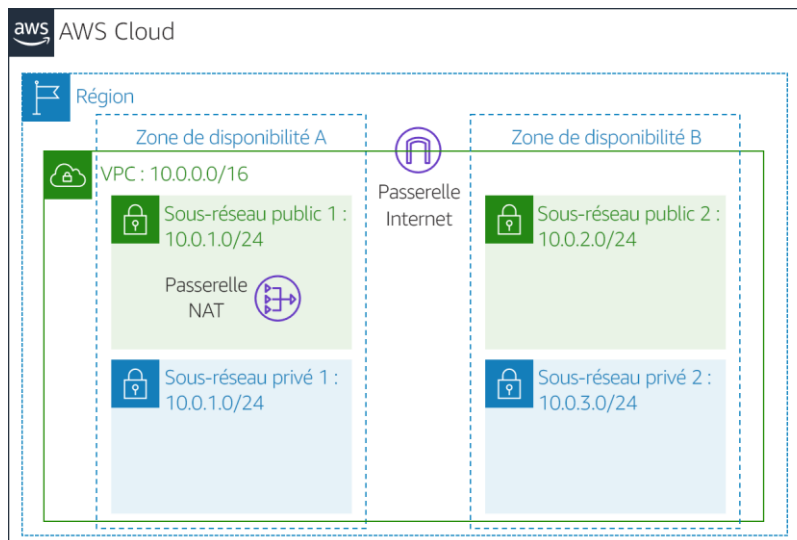


Table de routage publique

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle Internet

Table de routage privée

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle NAT

Tâche 3 : Création d'un groupe de sécurité de VPC

Avec cette tâche, vous allez créer un groupe de sécurité de VPC qui agit comme un pare-feu virtuel. Lorsque vous lancez une instance, vous lui associez un ou plusieurs groupes de sécurité. Vous pouvez ajouter des règles à chaque groupe de sécurité pour autoriser le trafic vers ou depuis ses instances associées.

31. Dans le panneau de navigation de gauche, choisissez **Security Groups** (Groupes de sécurité).
32. Choisissez **Create security group** (Créer un groupe de sécurité), puis configurez les paramètres suivants :
 - **Security group name** (Nom du groupe de sécurité) : `Web Security Group` (Groupe de sécurité web)
 - **Description** : `Enable HTTP access` (Autoriser l'accès HTTP)
 - **VPC** : `picasso-expo-vpc`
35. Dans le volet **Inbound rules** (Règles entrantes), choisissez **Add rule** (Ajouter une règle).
36. Configurez les paramètres suivants :
 - **Type** : `HTTP`
 - **Source** : `Anywhere-IPv4`
 - **Description** : `Permit web requests` (Autoriser les demandes web)
38. Faites défiler l'affichage jusqu'au bas de la page, puis choisissez **Create security group** (Créer un groupe de sécurité).

Vous utiliserez ce groupe de sécurité dans le cadre de la prochaine tâche, lors du lancement d'une instance Amazon EC2.

Tâche 4 : Lancement d'une instance de serveur web

Dans cette tâche, vous allez lancer une instance Amazon EC2 dans le nouveau VPC. Vous allez configurer l'instance pour qu'elle fonctionne en tant que serveur web.

39. Dans le menu **Services**, choisissez **EC2**.

40. Choisissez **Launch Instance** (Lancer une instance), puis choisissez **Launch Instance** (Lancer l'instance).

Tout d'abord, vous allez sélectionner une *Amazon Machine Image (AMI)* qui contient le système d'exploitation souhaité.

41. Dans la ligne correspondant à **Debian** (en haut), choisissez **Select** (Sélectionner).

Le paramètre *Instance Type* (Type d'instance) définit les ressources matérielles affectées à l'instance.

42. Sélectionnez **t2.micro** (affiché dans la colonne *Type*).

43. Choisissez **Next: Configure Instance Details** (Étape suivante : Configuration des détails de l'instance)

Vous allez maintenant configurer l'instance à lancer dans un sous-réseau public du nouveau VPC.

44. Configurez les paramètres suivants :

- **Network** (Réseau) : *picasso-expo-vpc*
- **Subnet** (Sous-réseau) : *Public Subnet 2* (Sous-réseau public 2) (*et non Private* (Privé) !)
- **Auto-assign Public IP** (Attribuer automatiquement l'adresse IP publique) : *Enable* (Activer)

47. Choisissez **Next: Add Storage** (Étape suivante : Ajout de stockage)

Vous allez utiliser les paramètres par défaut pour le stockage.

48. Choisissez **Étape suivante : Ajout de balises**.

Les identifications peuvent être utilisées pour identifier les ressources. Vous utiliserez une balise pour attribuer un nom à l'instance.

49. Choisissez **Add Tag** (Ajouter une balise), puis configurez les paramètres suivants :

- **Key** (Clé) : **Name** (Nom)
- **Value** (Valeur) : **Web Server 1** (Serveur web 1)

50. Choisissez **Next: Configure Security Group** (Étape suivante : Configuration d'un groupe de sécurité)

Vous allez configurer l'instance de manière à utiliser le paramètre *Web Security Group* (Groupe de sécurité web) que vous avez créé précédemment.

51. Sélectionnez **Select an existing security group** (Sélectionner un groupe de sécurité existant).

52. Sélectionnez **Web Security Group** (Groupe de sécurité web).

Il s'agit du groupe de sécurité que vous avez créé avec la tâche précédente. Il permettra un accès HTTP à l'instance.

53. Choisissez **Review and Launch** (Vérifier et lancer).

54. Lorsqu'un message d'*avertissement* vous informe que vous ne pourrez plus vous connecter à l'instance via le port 22, choisissez **Continue** (Continuer).

55. Vérifiez les informations liées à l'instance, puis choisissez **Launch** (Lancer).

56. Dans la boîte de dialogue **Select an existing keypair** (Sélectionner une paire de clés existante), sélectionnez **I acknowledge...** (Je reconnais...).

57. Choisissez **Launch Instances** (Lancer des instances), puis **View Instances** (Afficher les instances).

58. Attendez que **Web Server 1** (Serveur web 1) affiche *2/2 checks passed* (2/2 contrôles réussis) dans la colonne **Status Checks** (Contrôles des statuts).

Cela peut prendre quelques minutes. Choisissez d'actualiser en haut à droite toutes les 30 secondes pour mettre à jour la page.

Vous allez maintenant vous connecter au serveur web s'exécutant sur l'instance EC2.

59. Sélectionnez **Web Server 1** (Serveur web 1).

60. Copiez la valeur **Public DNS (IPv4)** (DNS public (IPv4)) affichée dans l'onglet **Description** en bas de la page.

61. Ouvrez un nouvel onglet de navigateur web, collez la valeur **Public DNS** (DNS public) et appuyez sur Entrée.

L'architecture complète que vous avez déployée est la suivante :

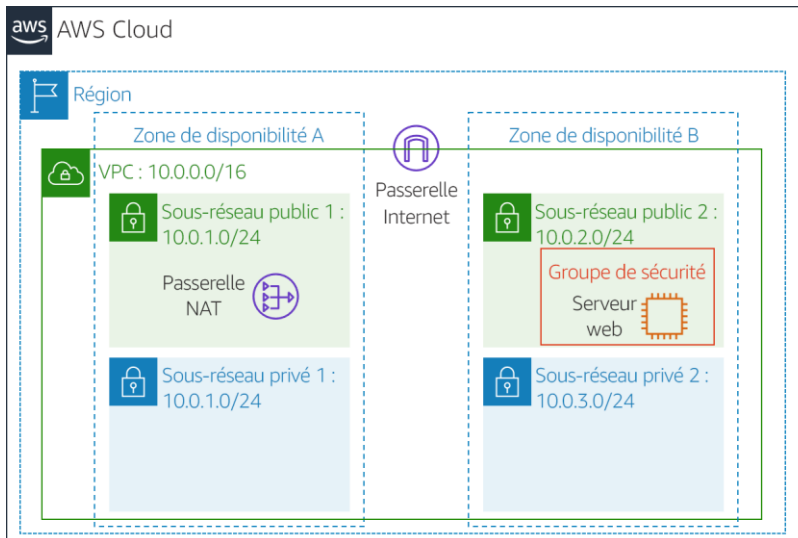


Table de routage publique

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle Internet

Table de routage privée

Destination	Cible
10.0.0.0/16	Local
0.0.0.0/0	Passerelle NAT