
Amazon Virtual Private Cloud

Manuel de mise en route

API Version 2012-12-01



Amazon Web Services

Amazon Virtual Private Cloud: Manuel de mise en route

Amazon Web Services

Copyright © 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The following are trademarks or registered trademarks of Amazon: Amazon, Amazon.com, Amazon.com Design, Amazon DevPay, Amazon EC2, Amazon Web Services Design, AWS, CloudFront, EC2, Elastic Compute Cloud, Kindle, and Mechanical Turk. In addition, Amazon.com graphics, logos, page headers, button icons, scripts, and service names are trademarks, or trade dress of Amazon in the U.S. and/or other countries. Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon.

All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

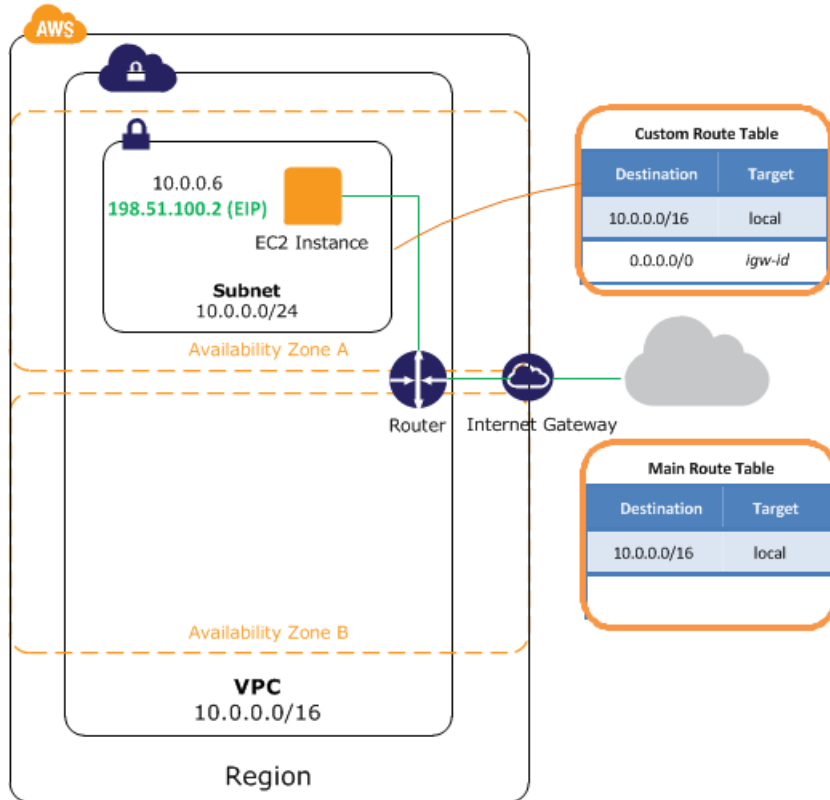
Présentation de l'exercice	1
Mise en route	4
Etape 1 : S'inscrire à Amazon VPC	4
Etape 2 : Configurer le VPC et la passerelle Internet	5
Etape 3 : Configurer un groupe de sécurité pour votre VPC	8
Etape 4 : Lancer une instance dans votre VPC	13
Etape 5 : Affecter une adresse IP élastique à l'instance	14
Comment procéder ensuite ?	16
Faites-nous part de vos commentaires	20

Présentation de l'exercice

Un nuage privé virtuel (VPC) est un réseau virtuel qui s'apparente à un réseau classique que vous pourriez exploiter dans votre propre centre de données, avec les avantages de l'infrastructure évolutive d'Amazon Web Services (AWS). Une fois les différentes étapes de cet exercice accomplies, vous disposerez d'une instance Amazon EC2 en cours d'exécution au sein d'un nondefault VPC, à laquelle vous pourrez accéder via Internet à l'aide du protocole SSH (pour les instances Linux) ou RDP (pour les instances Windows).

Pour lire une présentation d'Amazon VPC, consultez la section [What is Amazon VPC?](#) du manuel *Amazon Virtual Private Cloud User Guide*.

Le schéma suivant illustre l'architecture que vous allez créer en effectuant les différentes étapes de l'exercice proposé dans ce manuel. Le groupe de sécurité que vous configurez et associez à cette instance autorise uniquement le trafic à transiter via des ports spécifiques, verrouillant la communication avec l'instance conformément aux règles que vous définissez. Par le biais d'une adresse IP élastique (EIP), il est possible d'accéder, depuis Internet, à une instance du VPC normalement privée. Pour cela, vous utilisez une passerelle Internet (agissant, par exemple, en tant que serveur Web).



Le tableau suivant récapitule les tâches que vous allez effectuer à mesure que vous réalisez les différentes étapes de l'exercice proposé dans ce manuel.

<p>Étape 1 : Saisie à Amazon VPC (4)</p>	<p>Inscrivez-vous à Amazon VPC, si ce n'est pas déjà fait.</p>
<p>Étape 2 : Configurer le VPC et la passerelle Internet (5)</p>	<p>Utilisez l'assistant VPC pour les opérations suivantes :</p> <ol style="list-style-type: none"> 1. Créer un VPC, c'est-à-dire une portion isolée du nuage AWS 2. Créer et associer une passerelle Internet, afin de connecter directement votre VPC à Internet et pouvoir accéder à d'autres produits AWS tels qu'Amazon Simple Storage Service (Amazon S3) 3. Créer un sous-réseau Amazon VPC, c'est-à-dire un segment d'une plage d'adresses IP du VPC, dans lequel vous pouvez exécuter des instances Amazon EC2 Les sous-réseaux vous permettent de regrouper des instances en fonction de vos besoins opérationnels et de vos exigences de sécurité. 4. Définissez le routage dans le VPC afin de permettre le trafic entre le sous-réseau et Internet. Votre VPC dispose d'un routeur implicite, comme illustré sur le schéma.

<p>Étape 3 : Configurer un groupe de sécurité pour votre VPC</p>	<p>Utilisez la console Amazon VPC pour configurer un groupe de sécurité afin de contrôler le trafic entrant et sortant pour l'instance.</p>
<p>Étape 4 : Lancer une instance dans votre VPC</p>	<p>Utilisez la console Amazon EC2 pour lancer une instance au sein du sous-réseau. Cette instance est associée à une adresse IP privée figurant dans la plage d'adresses du sous-réseau.</p>
<p>Étape 5 : Affecter une adresse IP élastique à l'instance</p>	<p>Utilisez la console Amazon VPC pour affecter une adresse IP élastique à l'instance. Avec l'adresse IP élastique, l'instance dispose, en plus de son adresse privée, d'une adresse IP publique qui permet d'y accéder via Internet.</p>
<p>Étape finale: Supprimer le VPC</p>	<p>Utilisez la console Amazon EC2 pour mettre fin à votre instance et la console Amazon VPC pour supprimer votre VPC.</p>

Mise en route sur Amazon VPC

Ce manuel fournit une introduction pratique à l'utilisation d'Amazon VPC par le biais d'AWS Management Console. L'exercice proposé vous guide à travers un scénario simple dans lequel vous allez configurer un VPC avec un sous-réseau public unique contenant une instance EC2 en cours d'exécution dotée d'une adresse IP élastique.

Topics

- [Etape 1 : S'inscrire à Amazon VPC \(p. 4\)](#)
- [Etape 2 : Configurer le VPC et la passerelle Internet \(p. 5\)](#)
- [Etape 3 : Configurer un groupe de sécurité pour votre VPC \(p. 8\)](#)
- [Etape 4 : Lancer une instance dans votre VPC \(p. 13\)](#)
- [Etape 5 : Affecter une adresse IP élastique à l'instance \(p. 14\)](#)

Pour avoir un aperçu de l'exercice que vous devrez effectuer, consultez la section [Présentation de l'exercice \(p. 1\)](#). Pour lire une présentation basique d'Amazon VPC, consultez la section [What is Amazon VPC?](#) du manuel *Amazon Virtual Private Cloud User Guide*.

Etape 1 : S'inscrire à Amazon VPC

Lorsque vous créez un compte AWS, nous y souscrivons automatiquement tous les services AWS, y compris Amazon EC2 et Amazon VPC. Vous payez des frais uniquement en fonction des services que vous utilisez réellement. Pour réaliser l'exemple donné ici, les frais facturés resteront modiques.

Si vous possédez déjà un compte AWS, vous pouvez ignorer la prochaine étape. Si tel n'est pas le cas, observez la procédure suivante pour en créer un.

Pour créer un compte AWS

1. Rendez-vous sur <http://aws.amazon.com> et cliquez sur Inscrivez-vous.
2. Suivez les instructions à l'écran.
Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code PIN en utilisant le clavier numérique de votre téléphone.

Nous vous informerons par e-mail dès que votre compte sera activé et prêt à l'emploi.

Etape 2 : Configurer le VPC et la passerelle Internet

Pour cette étape, nous allons utiliser l'assistant VPC afin de créer un VPC. L'assistant effectue automatiquement les étapes suivantes :



Tip

Si vous le souhaitez, vous pouvez réaliser ces étapes manuellement à l'aide d'AWS Management Console.


- Création d'un VPC de taille /16 (un réseau comprenant 65 536 adresses IP privées)
- Association d'une passerelle Internet au VPC
- Ajout d'un sous-réseau de taille /24 (une plage de 256 adresses IP privées)
- Configuration du routage de votre VPC de façon à permettre le trafic entre le sous-réseau et la passerelle Internet

Pour créer un VPC à l'aide de l'assistant VPC dans AWS Management Console

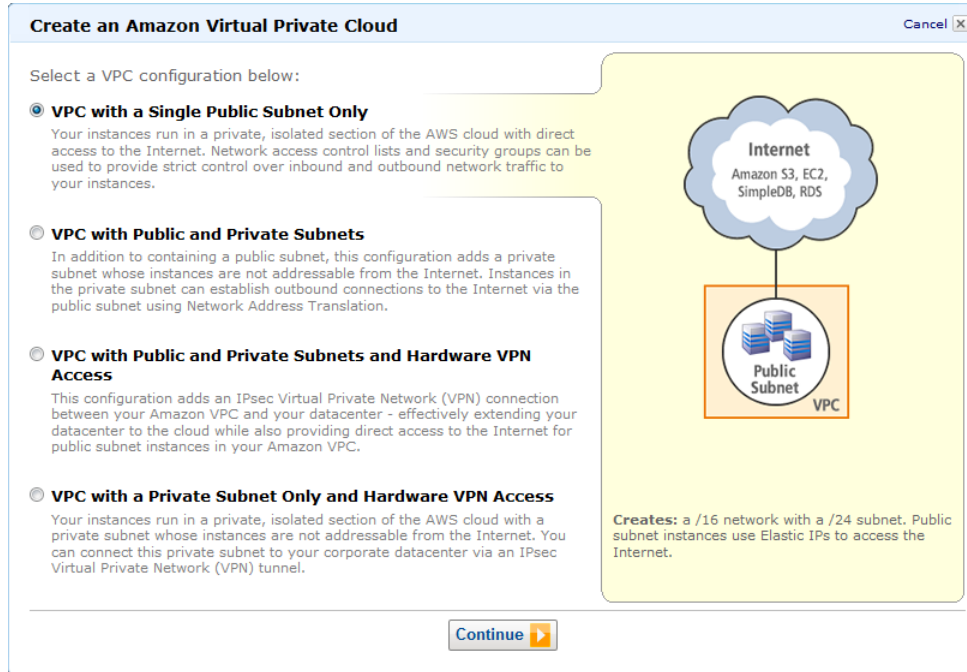
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon VPC à partir de l'adresse <https://console.aws.amazon.com/vpc/>.
2. A partir du tableau de bord VPC, cliquez sur Get started creating a VPC.

Amazon VPC enables you to create a virtual network topology - including subnets and route tables - for your EC2 resources.

Click the button below to create a Virtual Private Cloud.

[Get started creating a VPC](#) 

3. Sélectionnez la première option, VPC with a Single Public Subnet Only, puis cliquez sur Continue.

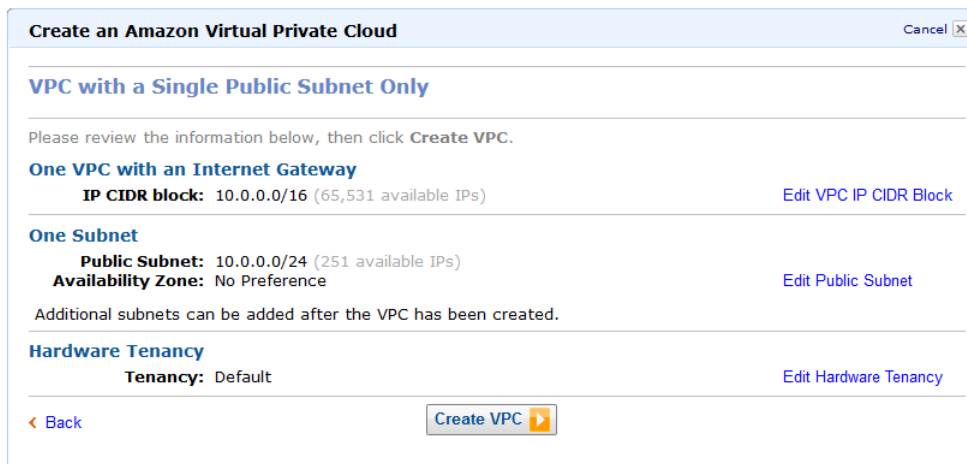


4. La page de confirmation indique les plages CIDR que nous allons utiliser pour le VPC et le sous-réseau (10.0.0.0/16 et 10.0.0.0/24, respectivement), ainsi que les paramètres de location du matériel. Modifiez ces paramètres selon vos besoins, puis cliquez sur **Create VPC** afin de créer le VPC, la passerelle Internet, le sous-réseau et la table de routage.



Note

Pour en savoir plus sur la notation CIDR, consultez [l'article Wikipédia concernant le routage interdomaine sans classe \(CIDR\)](#). Pour en savoir plus sur la location du matériel, consultez la section [Using EC2 Dedicated Instances](#) dans le manuel *Amazon Virtual Private Cloud User Guide*



5. Une fenêtre d'état indique la progression de ces tâches. Une fois ces tâches terminées, une fenêtre d'état confirme la réussite de la création du VPC. Cliquez sur Close afin de fermer la fenêtre d'état et de revenir au tableau de bord VPC.

Vérification des éléments constitutifs de votre VPC

Vous pouvez utiliser les paramètres par défaut pour les éléments créés par l'assistant VPC dans le cadre de la réalisation de l'exercice proposé dans ce manuel. Cette section explique comment afficher ces éléments et leurs paramètres à l'aide de la console VPC.

Dans le volet de navigation, cliquez sur Your VPCs, puis sélectionnez le VPC que vous venez de créer.



Tip

Vous devrez peut-être actualiser la page pour que le VPC s'affiche.

La console affiche , ainsi que le VPC que vous venez de créer. Chaque VPC dispose d'un jeu d'options DHCP, d'une table de routage principale et d'une LCA réseau par défaut. Pour en savoir plus sur, consultez les sections [DHCP Options Sets](#), [Route Tables](#) et [Network ACLs](#) dans le manuel *Amazon Virtual Private Cloud User Guide*.

Viewing: All Virtual Private Clouds

	VPC ID	State	CIDR	DHCP Options	Main Route Table	Default Network ACL
<input type="checkbox"/>	vpc-09ab8662	● available	172.31.0.0/16	dopt-00ab866b	rtb-02ab8669	acl-03ab8668
<input checked="" type="checkbox"/>	vpc-071db56d	● available	10.0.0.0/16	dopt-00ab866b	rtb-1a1db570	acl-051db56f

Pour consulter les informations relatives à vos passerelles Internet, cliquez sur Internet Gateways dans le volet de navigation.

Viewing: All Internet Gateways

	ID	State	VPC
<input type="checkbox"/>	igw-0eab8665	● available	vpc-09ab8662 (172.31.0.0/16)
<input checked="" type="checkbox"/>	igw-041db56e	● available	vpc-071db56d (10.0.0.0/16)

Le VPC créé possède deux tables de routage. Le VPC possède une table de routage principale fournie par défaut et l'assistant VPC a permis, en plus, de créer une table de routage personnalisée. Votre sous-réseau est associé à la table de routage personnalisée, ce qui signifie que nous utilisons les routages de cette table pour déterminer l'acheminement du trafic au niveau du sous-réseau. Si vous choisissez d'ajouter un nouveau sous-réseau à votre VPC, il utilisera la table de routage principale par défaut.

Pour consulter vos tables de routage


1. Cliquez sur Route Tables dans le volet de navigation.
2. Sélectionnez la table de routage personnalisée (celle dont la colonne Main présente la valeur No) afin d'afficher les informations de routage dans le volet de détails.

Viewing: All Route Tables



	Route Table ID	Associated With	Main	VPC
<input type="checkbox"/>	rtb-02ab8669	0 Subnets	Yes	vpc-09ab8662 (172.31.0.0/16)
<input checked="" type="checkbox"/>	rtb-ed1db587	1 Subnet	No	vpc-071db56d (10.0.0.0/16)
<input type="checkbox"/>	rtb-1a1db570	0 Subnets	Yes	vpc-071db56d (10.0.0.0/16)

3. La première ligne de la table correspond au routage local, qui permet la communication des instances figurant au sein du VPC. Ce routage est présent par défaut dans toutes les tables de routage et ne peut pas être supprimé.


La deuxième ligne indique le routage ajouté via l'assistant pour permettre au trafic destiné aux adresses IP hors du VPC (soit 0.0.0.0/0) d'être acheminé du sous-réseau vers la passerelle Internet. Ce sous-réseau est désigné comme *public*, car l'ensemble du trafic qui en est issu est acheminé vers la passerelle Internet.

 **Route Table: rtb-ed1db587**


Routes Associations Route Propagation

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	 active	No	<input type="button" value="Remove"/>
0.0.0.0/0	igw-041db56e	 active	No	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text" value="select a target"/>			<input type="button" value="Add"/>

4. Sélectionnez la table de routage principale. La table de routage principale comporte un routage local, mais pas d'autres routages. Par conséquent, les sous-réseaux que vous créez ne sont, au départ, pas exposés à Internet : ils sont *privés*. Pour exposer un nouveau sous-réseau en tant que sous-réseau public, vous pouvez soit modifier le routage dans la table de routage principale, soit associer ce sous-réseau à une table de routage personnalisée.

 **Route Table: rtb-1a1db570**

Routes Associations Route Propagation

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	 active	No	<input type="button" value="Remove"/>
<input type="text"/>	<input type="text" value="select a target"/>			<input type="button" value="Add"/>

Etape 3 : Configurer un groupe de sécurité pour votre VPC

Un *groupe de sécurité* fonctionne comme un pare-feu virtuel contrôlant le trafic autorisé à accéder aux instances qui lui sont associées. Pour bénéficier des fonctions offertes par les groupes de sécurité, vous

devez créer un groupe, y ajouter les règles de trafic entrant et sortant souhaitées, puis associer vos instances à ce groupe de sécurité lorsque vous les lancez. Lorsque vous ajoutez ou supprimez des règles dans votre groupe de sécurité, ces changements sont automatiquement appliqués aux instances associées au groupe.

Votre VPC est associé à un *groupe de sécurité par défaut*. Toute instance qui n'est pas spécifiquement associée à un autre groupe est affectée au groupe de sécurité par défaut. Dans le cadre de cet exercice, nous pourrions utiliser le groupe de sécurité par défaut, mais nous préférons créer le groupe `WebServerSG`. Vous définirez ce groupe de sécurité lorsque vous lancerez une instance dans votre VPC.

Topics

- [Règles du groupe de sécurité WebServerSG \(p. 9\)](#)
- [Création du groupe de sécurité WebServerSG \(p. 10\)](#)
- [Ajout de règles au groupe de sécurité WebServerSG \(p. 10\)](#)

Règles du groupe de sécurité WebServerSG

Les règles de trafic entrant régulent le trafic autorisé à accéder aux instances associées au groupe de sécurité (c'est-à-dire, l'origine du trafic et le port d'écoute sur l'instance). L'ensemble du trafic généré en retour est automatiquement autorisé à accéder aux instances. Par exemple, si un client sur Internet envoie une requête à un serveur Web de votre VPC associé au groupe `WebServerSG`, l'instance peut répondre, quelles que soient les règles de trafic sortant au niveau du groupe. Ainsi, les groupes de sécurité sont dynamiques.

Les règles de trafic sortant déterminent les destinations auxquelles les instances associées au groupe peuvent envoyer le trafic (à savoir, la destination du trafic et le port de destination). La totalité du trafic retour (par exemple, la réponse de l'hôte qui reçoit le trafic) est automatiquement autorisée à accéder aux instances, quelles que soient les règles de trafic entrant au niveau du groupe de sécurité.

Le tableau suivant répertorie les règles de trafic entrant et sortant pour le groupe de sécurité `WebServerSG` et leur impact.



Note

Si votre entreprise utilise uniquement Linux ou uniquement Windows, vous n'avez pas besoin d'ajouter à la fois les accès SSH et RDP.

Entrant			
IP Source	Protocole	Plage de ports	Commentaires
0.0.0.0/0	TCP	80	Autoriser l'accès HTTP entrant depuis n'importe quelle origine
0.0.0.0/0	TCP	443	Autoriser l'accès HTTPS entrant depuis n'importe quelle origine
Plage d'adresses IP publiques de votre réseau domestique	TCP	22	Autoriser l'accès SSH entrant depuis votre réseau domestique (Linux/UNIX uniquement)

Plage d'adresses IP publiques de votre réseau domestique	TCP	3389	Autoriser l'accès RDP entrant depuis votre réseau domestique (Windows uniquement)
Sortant			
IP Dest	Protocole	Plage de ports	Commentaires
0.0.0.0/0	TCP	80	Autoriser l'accès HTTP sortant aux serveurs sur Internet (par exemple, pour les mises à jour logicielles)
0.0.0.0/0	TCP	443	Autoriser l'accès HTTPS sortant aux serveurs sur Internet (par exemple, pour les mises à jour logicielles)

Dans cet exercice, nous n'allons pas ajouter de règle pour permettre la communication entre les différentes instances associées au groupe de sécurité. Pour ce type de communication, vous devez ajouter une règle au groupe de sécurité avec cet objectif précis. Pour en savoir plus, consultez la section [Security Groups](#) dans le manuel *Amazon Virtual Private Cloud User Guide*.

Création du groupe de sécurité WebServerSG

Pour créer le groupe de sécurité WebServerSG

1. Ouvrez la console Amazon VPC à partir de l'adresse <https://console.aws.amazon.com/vpc/>.
2. Cliquez sur Security Groups dans le volet de navigation.
3. Cliquez sur le bouton Create Security Group.
4. Indiquez `WebServerSG` comme nom du groupe de sécurité et fournissez une description. Sélectionnez l'ID de votre VPC dans le menu VPC, puis cliquez sur Yes, Create.

Par défaut, les nouveaux groupes de sécurité commencent avec seulement une règle de trafic sortant, qui permet à la totalité du trafic de quitter les instances. Vous devez ajouter des règles pour activer un trafic entrant ou limiter le trafic sortant.

Ajout de règles au groupe de sécurité WebServerSG

Pour ajouter des règles au groupe de sécurité WebServerSG

1. Cliquez sur Security Groups dans le volet de navigation afin d'afficher vos groupes de sécurité.
2. Sélectionnez le groupe de sécurité `WebServerSG` que vous venez de créer. Le volet de détails inclut un onglet présentant les informations relatives au groupe de sécurité, ainsi que des onglets pour configurer les règles de trafic entrant et sortant.
3. Ajoutez des règles pour l'accès HTTP et HTTPS entrant, depuis n'importe quelle origine :
 - a. Dans l'onglet Inbound, sélectionnez `HTTP` dans la liste déroulante Create a new rule et vérifiez que la valeur Source est `0.0.0.0/0`.
 - b. Cliquez sur Add Rule. Une règle autorisant tout accès HTTP, quelle qu'en soit l'origine, est ainsi ajoutée. Notez que le bouton Apply Rule Changes est disponible et que la mention « Your changes have not been applied yet » figure au-dessus. Cliquez sur ce bouton pour appliquer les changements, une fois toutes les règles de trafic entrant ajoutées.

Security Group: WebServerSG

Details Inbound* Outbound

Create a new rule: Custom TCP rule

Port range: 80 (HTTP)
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

+ Add Rule

Your changes have not been applied yet.

Apply Rule Changes

TCP	Port (Service)	Source	Action
	80 (HTTP)	0.0.0.0/0	Delete

- c. Sélectionnez `HTTPS` à partir de la liste déroulante `Create a new rule` et vérifiez que la valeur `Source` est `0.0.0.0/0`.
 - d. Cliquez sur `Add Rule`. Une règle autorisant tout accès `HTTPS`, quelle qu'en soit l'origine, est ainsi ajoutée.
4. Ajoutez des règles pour l'accès `SSH` et `RDP` (bureau à distance) entrant dans le groupe depuis la plage d'adresses IP publiques de votre réseau :



Caution

Si vous utilisez la plage `0.0.0.0/0`, vous autorisez toutes les adresses IP à accéder à votre instance via `SSH` ou `RDP`. Cette méthode est acceptable dans le cadre de cet exercice, mais n'est pas sécurisée pour les environnements de production. Dans un environnement de production, vous autoriserez uniquement l'accès à votre instance pour une adresse IP ou une plage d'adresses spécifiques.



Tip

Vous pouvez également utiliser un service pour obtenir l'adresse IP de votre ordinateur local. Pour trouver un service qui affichera votre adresse IP, indiquez « what is my IP address » (quelle est mon adresse IP) dans votre recherche. Si votre connexion s'effectue via un `FAI` ou derrière un pare-feu, sans adresse IP statique, vous devez déterminer la plage d'adresses IP utilisée par les ordinateurs clients.

- a. Dans l'onglet `Inbound`, sélectionnez `SSH` dans la liste déroulante `Create a new rule`.
 - b. Dans le champ `Source`, saisissez la plage d'adresses IP publiques de votre réseau (par exemple, `192.0.2.0/24`). Si vous ne connaissez pas la plage d'adresses, vous pouvez utiliser `0.0.0.0/0` dans le cadre de cet exercice (consultez l'avertissement et le conseil précisés pour cette étape).
 - c. Cliquez sur `Add Rule`.
 - d. Sélectionnez `RDP` dans la liste déroulante `Create a new rule`.
 - e. Dans le champ `Source`, indiquez la plage d'adresses IP publiques de votre réseau domestique. Si vous ne connaissez pas la plage d'adresses, vous pouvez utiliser `0.0.0.0/0` dans le cadre de cet exercice (consultez l'avertissement et le conseil précisés pour cette étape).
 - f. Cliquez sur `Add Rule`.
5. Cliquez sur `Apply Rule Changes` afin d'appliquer ces règles de trafic entrant.

Security Group: WebServerSG

Details **Inbound** Outbound

Create a new rule: Custom TCP rule

Port range: (e.g., 80 or 49152-65535)

Source: 0.0.0.0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

TCP Port (Service)	Source	Action
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
22 (SSH)	0.0.0.0/0	Delete
3389 (RDP)	0.0.0.0/0	Delete

6. Limitez l'accès sortant au trafic HTTP et HTTPS à partir du groupe, vers n'importe quelle destination :

- Dans l'onglet Outbound, identifiez la règle par défaut autorisant la totalité du trafic sortant, puis cliquez sur Delete. Cette règle est marquée pour suppression. Toutefois, la suppression n'interviendra que lorsque vous aurez cliqué sur Apply Rule Changes, ce que vous ferez après avoir ajouté les règles de trafic sortant pour les protocoles HTTP et HTTPS.

Security Group: WebServerSG

Details Inbound **Outbound***

Create a new rule: Custom TCP rule

Port range: (e.g., 80 or 49152-65535)

Destination: 0.0.0.0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

Your changes have not been applied yet.

ALL Port (Service)	Destination	Action
ALL	0.0.0.0/0	Undelete

- Sélectionnez HTTP dans la liste déroulante Create a new rule, puis cliquez sur Add Rule. Une règle autorisant tout trafic HTTP sortant, quelle qu'en soit la destination, est ainsi ajoutée.
- Sélectionnez HTTPS dans la liste déroulante Create a new rule, puis cliquez sur Add Rule. Une règle autorisant tout trafic HTTPS sortant, quelle qu'en soit la destination, est ainsi ajoutée.

7. Cliquez sur Apply Rule Changes afin d'appliquer ces règles de trafic sortant.

Security Group: WebServerSG

Details Inbound **Outbound**

Create a new rule: Custom TCP rule

Port range: (e.g., 80 or 49152-65535)

Destination: 0.0.0.0 (e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

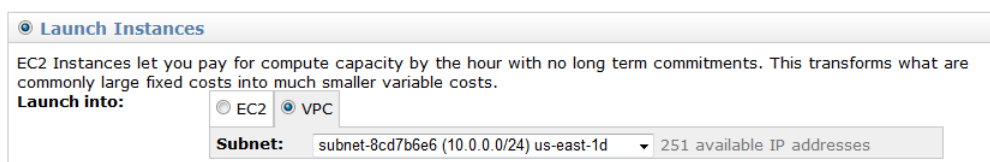
TCP Port (Service)	Destination	Action
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete

Etape 4 : Lancer une instance dans votre VPC

Lorsque vous lancez une instance EC2 dans un VPC, vous devez préciser l'ID d'un sous-réseau au sein du VPC.

Pour lancer une instance EC2 dans un VPC

1. Ouvrez la console Amazon EC2 à partir de l'adresse <https://console.aws.amazon.com/ec2/>.
2. A partir de la barre de navigation, sélectionnez la région souhaitée pour l'instance. Dans cet exercice, vous pouvez utiliser la région par défaut. Pour en savoir plus concernant les régions et les zones de disponibilité, consultez la section [Regions and Availability Zones](#) du manuel *Amazon Elastic Compute Cloud User Guide*.
3. Dans le tableau de bord, cliquez sur le bouton Launch Instance.
4. Sur la page Create a New Instance, sélectionnez Classic Wizard, puis cliquez sur Continue.
5. Sur la page CHOOSE AN AMI, l'onglet Quick Start affiche la liste des configurations de base disponibles, appelées images machine Amazon (AMI). Choisissez l'AMI que vous souhaitez utiliser en cliquant sur le bouton Select correspondant.
6. Sur la page INSTANCE DETAILS, dans le menu Instance Type, gardez la valeur par défaut, Micro (t1.micro), afin de lancer une seule instance Micro.
7. Sous Launch Instances, vérifiez que votre sous-réseau est bien sélectionné dans la liste déroulante Subnet, puis cliquez sur Continue.



8. Sous Advanced Instance Options, vous pouvez spécifier l'adresse IP à utiliser pour l'instance. Dans le cadre de cet exercice, toutefois, laissez le champ IP Address vide et cliquez sur Continue pour accepter les paramètres par défaut.
9. Cliquez sur Continue afin d'utiliser le périphérique de stockage par défaut.
10. Définissez une étiquette pour votre instance si vous le souhaitez, puis cliquez sur Continue.
11. Sur la page Create Key Pair, vous pouvez sélectionner une paire de clés existante ou en créer une. Dans le cadre de cet exercice, nous allons créer une paire de clés.
 - a. Cliquez sur Create a new Key Pair.
 - b. Indiquez le nom de votre paire de clés (par exemple, `VPC_Keypair`), puis cliquez sur Create & Download your Key Pair. Les éléments contenus dans la clé privée sont nécessaires pour établir la connexion à votre instance après son lancement. Amazon Web Services ne conserve pas la partie privée des paires de clés.
 - c. Lorsque vous y êtes invité, enregistrez la clé privée sur un emplacement sécurisé de votre système, puis cliquez sur Continue.
12. Sur la page CONFIGURE FIREWALL, sélectionnez Choose one or more of your existing Security Groups. Sélectionnez le groupe `WebServerSG` que vous avez créé, puis cliquez sur Continue.
13. Sur la page REVIEW, vérifiez vos paramètres. Lorsque tout est correct, cliquez sur Launch afin de lancer votre instance.

Etape 5 : Affecter une adresse IP élastique à l'instance

Par défaut, toute instance figurant dans un VPC est privée. Vous pouvez rendre publique une instance figurant dans un VPC en associant une passerelle Internet au VPC et en attribuant une adresse IP publique à l'instance. Dans cet exercice, vous avez utilisé l'assistant VPC afin de créer une passerelle Internet pour votre VPC. Vous allez, à présent, créer une adresse IP élastique, c'est-à-dire une adresse IP publique rattachée à votre compte AWS, puis associer cette adresse à votre instance afin que cette dernière soit accessible via Internet.

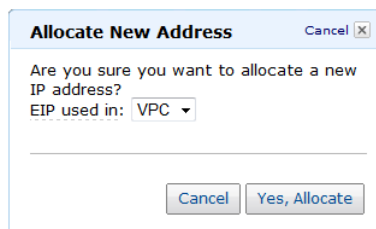
Pour en savoir plus sur les adresses IP élastiques, consultez la section [Elastic IP Addresses](#) dans le manuel *Amazon Virtual Private Cloud User Guide*.

Pour affecter une adresse IP élastique

1. Ouvrez la console Amazon VPC à partir de l'adresse <https://console.aws.amazon.com/vpc/>.
2. Cliquez sur Elastic IPs dans le volet de navigation.
3. Cliquez sur le bouton **Allocate New Address**.

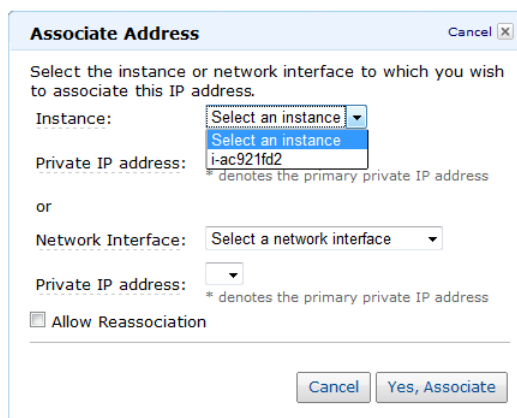


4. Dans la liste EIP used in:, sélectionnez **VPC**, puis cliquez sur **Yes, Allocate**.



The dialog box titled "Allocate New Address" has a "Cancel" button in the top right corner. The main text asks "Are you sure you want to allocate a new IP address?". Below this, there is a label "EIP used in:" followed by a dropdown menu currently showing "VPC". At the bottom of the dialog, there are two buttons: "Cancel" and "Yes, Allocate".

5. Sélectionnez l'adresse IP élastique dans la liste et cliquez sur le bouton **Associate Address**.
6. Dans la boîte de dialogue **Associate Address**, sélectionnez l'instance à laquelle associer l'adresse, puis cliquez sur **Yes, Associate**.



The dialog box titled "Associate Address" has a "Cancel" button in the top right corner. The main text says "Select the instance or network interface to which you wish to associate this IP address." There are two main sections. The first section is for "Instance:" with a dropdown menu showing "Select an instance" and a list of instances including "i-ac921fd2". Below this is a label "Private IP address:" with a note "* denotes the primary private IP address". The second section is for "Network Interface:" with a dropdown menu showing "Select a network interface" and a label "Private IP address:" with the same note. At the bottom, there is a checkbox labeled "Allow Reassociation" which is currently unchecked. At the bottom right, there are two buttons: "Cancel" and "Yes, Associate".

Votre instance est désormais accessible par Internet. Vous pouvez également accéder à l'instance via le protocole SSH ou RDP (Bureau à distance) à partir de votre réseau local, en précisant l'adresse IP élastique de l'instance comme adresse de connexion. Pour savoir comment se connecter à une instance Linux, consultez la section [Connect to Your Linux Instance](#) du manuel *Amazon Elastic Compute Cloud User Guide*. Pour savoir comment se connecter à une instance Windows, consultez la section [Connect to Your Windows Instance](#) du manuel *Amazon Elastic Compute Cloud Microsoft Windows Guide*.

Vous avez maintenant terminé l'exercice : votre VPC est configuré et vous disposez d'une instance s'exécutant dans votre VPC à laquelle vous pouvez vous connecter via Internet. Vous pouvez continuer à utiliser votre instance et votre VPC, ou choisir de mettre fin à votre instance et supprimer le VPC. Pour en savoir plus sur le nettoyage, ou pour consulter de la documentation complémentaire concernant les VPC, reportez-vous à la section [Comment procéder ensuite ?](#) (p. 16).

Comment procéder ensuite ?

Topics

- [Etape facultative : Supprimer le VPC \(p. 16\)](#)
- [Compte AWS et informations d'identification \(p. 17\)](#)
- [Sécurité renforcée pour votre VPC \(p. 17\)](#)
- [Autres scénarios pour Amazon VPC \(p. 17\)](#)
- [Méthodes d'accès à Amazon VPC \(p. 17\)](#)
- [Documentation connexe \(p. 18\)](#)
- [Pour obtenir une aide supplémentaire \(p. 19\)](#)

Si vous avez suivi l'exemple proposé dans ce manuel, vous avez configuré un VPC et lancé une instance dans ce VPC. Si vous le souhaitez, vous pouvez conserver ce VPC afin de le réutiliser par la suite. Sinon, vous pouvez le supprimer. Que vous choisissiez de le supprimer ou non, vous pouvez toujours créer d'autres VPC.

Etape facultative : Supprimer le VPC

Avant de supprimer un VPC, vous devez mettre fin à toutes les instances qui s'y exécutent. Lorsque vous supprimez un VPC, cela supprime également les ressources associées, y compris les sous-réseaux, groupes de sécurité, listes de contrôle d'accès réseau, jeux d'options DHCP, tables de routage et passerelles Internet.

Pour supprimer le VPC

1. Ouvrez la console Amazon EC2 à partir de l'adresse <https://console.aws.amazon.com/ec2/>.
2. Cliquez sur Instances dans le volet de navigation.
3. Cliquez avec le bouton droit de la souris sur l'instance en cours d'exécution dans le VPC, puis choisissez Terminate.
4. A l'invite de confirmation, cliquez sur Yes, Terminate.
5. Ouvrez la console Amazon VPC à partir de l'adresse <https://console.aws.amazon.com/vpc/>.
6. Cliquez sur Your VPCs dans le volet de navigation.
7. Sélectionnez le VPC, puis cliquez sur Delete.
8. A l'invite de confirmation, cliquez sur Yes, Delete.

Compte AWS et informations d'identification

Ce manuel vous a présenté la procédure détaillée d'inscription au service et d'obtention d'un compte AWS, ainsi qu'un court exercice de mise en pratique. Maintenant que vous avez terminé l'exercice, nous vous recommandons de vérifier, avec un administrateur ou un collègue de votre entreprise, s'il possède déjà un compte AWS et des informations d'identification que vous pourrez utiliser lors de vos interactions futures avec AWS.

Si vous êtes le propriétaire du compte ou l'administrateur et souhaitez en savoir plus sur AWS Identity and Access Management, consultez les pages <http://aws.amazon.com/fr/iam> et [Using AWS Identity and Access Management](#).

Sécurité renforcée pour votre VPC

Si, en plus de votre groupe de sécurité, vous voulez une autre couche de sécurité, vous pouvez utiliser une liste de contrôle d'accès (LCA) réseau. Les LCA réseau contrôlent le trafic au niveau du sous-réseau. Cet exercice utilise uniquement des groupes de sécurité, qui contrôlent le trafic au niveau de l'instance. Pour en savoir plus sur les LCA réseau, consultez la section [Network ACLs](#) dans le manuel *Amazon Virtual Private Cloud User Guide*.

Autres scénarios pour Amazon VPC

Ce manuel présente un scénario simple d'utilisation d'Amazon VPC. Toutefois, l'assistant VPC fournit d'autres scénarios. Pour plus de détails sur ces scénarios, consultez la section [Scenarios for Amazon VPC](#) dans le manuel *Amazon Virtual Private Cloud User Guide*.

Méthodes d'accès à Amazon VPC

Le présent manuel vous a présenté comment utiliser Amazon VPC via AWS Management Console. Vous pouvez continuer à l'utiliser par le biais de la console ou essayer l'une des autres interfaces.

Continuer avec la console

Pour en savoir plus sur l'utilisation d'Amazon VPC à l'aide de la console, consultez le manuel [Amazon Virtual Private Cloud User Guide](#).

Utiliser l'interface de ligne de commande

Amazon EC2 et Amazon VPC partagent une interface de ligne de commande Java commune. Ces outils de ligne de commande sont un moyen rapide d'exécuter Amazon EC2 et VPC sans codage sur l'API ou recours à une bibliothèque. Pour savoir comment faire vos premiers pas avec les outils de ligne de commande, consultez la section [Getting Started with the Command Line Tools](#) du manuel *Amazon Elastic Compute Cloud User Guide*. Pour consulter une description complète de ces commandes, reportez-vous au document [Amazon Elastic Compute Cloud Command Line Reference](#).

Utiliser une bibliothèque existante

Amazon EC2 and Amazon VPC partagent une interface de programmation commune. Si vous préférez utiliser Amazon VPC via une API, des bibliothèques et des ressources sont disponibles pour les langages suivants :

- [Java](#)
- [PHP](#)
- [Python](#)
- [Ruby](#)
- [Windows et .NET](#)

Pour connaître les bibliothèques et les exemples de code dans tous les langages, accédez à la page [Exemples de codes et bibliothèques Amazon EC2](#).

Ecrire du code directement sur l'API de service Web

Si vous voulez écrire du code directement sur l'API pour Amazon EC2 et Amazon VPC, consultez la section [Making Requests](#) du manuel *Amazon Elastic Compute Cloud User Guide*. Ce manuel décrit comment créer et authentifier des demandes d'API, et explique comment utiliser Amazon EC2 et Amazon VPC par le biais des API. Pour une description complète des actions des API, consultez le document [Amazon Elastic Compute Cloud API Reference](#).

Documentation connexe

Ce manuel de mise en route pour Amazon VPC décrit les rudiments pour utiliser Amazon VPC. Le tableau suivant récapitule les autres documents disponibles concernant Amazon VPC.

Description	Documentation
Informations concernant l'utilisation d'Amazon VPC	Amazon Virtual Private Cloud User Guide
Informations concernant la configuration de la passerelle client (si vous choisissez d'utiliser une connexion VPN avec votre VPC)	Amazon Virtual Private Cloud Network Administrator Guide
Introduction pratique à Amazon EC2	Mise en route sur Amazon EC2
Informations concernant l'utilisation d'Amazon EC2	Amazon Elastic Compute Cloud User Guide
Description des commandes pour Amazon EC2 et Amazon VPC	Amazon Elastic Compute Cloud Command Line Reference
Description des actions de l'API, des types de données et des erreurs pour Amazon EC2 et Amazon VPC	Amazon Elastic Compute Cloud API Reference
Brève description des commandes les plus couramment utilisées pour Amazon VPC	Amazon Virtual Private Cloud Quick Reference Card

Pour obtenir une aide supplémentaire

Nous vous conseillons de consulter les forums de discussion d'AWS. Ce sont des forums communautaires destinés aux utilisateurs qui ont des questions techniques concernant les services AWS. Pour consulter le forum dédié à Amazon VPC, accédez à la page <https://forums.aws.amazon.com/forum.jspa?forumID=58>.

Vous pouvez également obtenir de l'aide en adhérant au programme AWS Premium Support. Il s'agit d'un service d'assistance individuelle rapide. Pour en savoir plus, consultez la page <http://aws.amazon.com/premiumsupport>.

Faites-nous part de vos commentaires

Votre retour est important pour nous aider à rendre notre documentation utile et facile à utiliser. Faites-nous part de vos premières impressions concernant Amazon VPC en remplissant notre [enquête sur la mise en route](#).

Merci.