

# TPS Labs Azure Lundi

## TP le service de compte de stockage Azure

Le service Azure Compte de stockage, également connu sous le nom de Azure Storage Account inclut le stockage d'objets blob, de fichiers, de files d'attente et de tables. Le stockage blob est idéal pour la mise à disposition d'images ou de documents qui vont être distribués directement dans un navigateur. C'est également idéal pour le stockage de fichiers, pour un accès distribué, la diffusion en continu de vidéos et d'audio, le stockage de données pour la sauvegarde et la restauration, la récupération d'urgence et l'archivage.

### Créer un compte de stockage :

Connectez vous sur le portail Azure, puis cliquez sur Tous les services. Saisissez Ressources, puis Groupes de ressources. Sélectionnez le groupe de ressources dans lequel vous allez souhaiter stocker votre compte de stockage.

Ajouter et saisissez Stockage, sélectionnez Compte de stockage : blob, fichier, table, file d'attente. Cliquez sur Créer. Nous allons dès à présent donner un nom à notre compte de stockage. Je tiens à attirer votre attention sur le fait qu'il faut que ce nom soit unique. Dans notre exemple, nous allons

#### Créer un compte de stockage ...

Informations de base

Avancé

Réseau

Protection des données

Chiffrement

Étiquettes

Vérifier + crée

Détails du projet

Sélectionnez l'abonnement dans lequel créer le compte de stockage. Choisissez un groupe de ressources nouveau ou existant pour organiser et gérer votre compte de stockage avec d'autres ressources.

Abonnement \*

Paiement à l'utilisation

Groupe de ressources \*

Formation

Créer nouveau

Détails de l'instance

Si vous devez créer un type de compte de stockage hérité, cliquez [ici](#).

Nom du compte de stockage ⓘ \*

demoformation2022

Région ⓘ \*

(US) East US

Performances ⓘ \*

☒ Standard: Recommandé pour la plupart des scénarios (compte universel v2)

☐ Premium: Recommandé pour les scénarios nécessitant une faible latence.

Redondance ⓘ \*

Stockage géoredondant (GRS)

☒ Proposez l'accès en lecture sur les données en cas d'indisponibilité régionale.

saisir Demoformation2024.

Nous allons sélectionner le modèle de déploiement. Je vous invite toujours à utiliser Ressource Manager, puis le type de compte, Stockage (v1 à usage général), son emplacement. Donc dans notre exemple, Est des états unis, puis réplication.

Dans la réplication, nous avons trois options. Nous pouvons avoir du stockage local redondant, du stockage géo-redondant ou du stockage géo-redondant avec accès en lecture. Dans notre exemple, nous choisissons du stockage géo-redondant avec accès en lecture. Pour les étapes suivant, laissez les options par défaut.

### Charger un document dans un compte de stockage

Pour uploader un document dans un compte de stockage Azure ; Nous allons créer un conteneur qui va être public, donc accessible à n'importe qui sur internet, dans lequel nous allons uploader un document. Je vous invite à vous connecter sur le portail Azure, puis à cliquer sur Tous les services. Vous pouvez chercher Stockage, Comptes de stockage. Nous pouvons voir que nous avons notre comptes de stockage. Dans notre exemple, le compte de stockage qui nous intéresse est le compte DemoFormation2022.

Je vous invite à cliquer dessus, puis à vous rendre dans la partie Service Blob, Conteneurs, et créer un nouveau Conteneur. Vous pouvez lui donner un nom.

### Nouveau conteneur

Nom \*

demo

Niveau d'accès public ⓘ

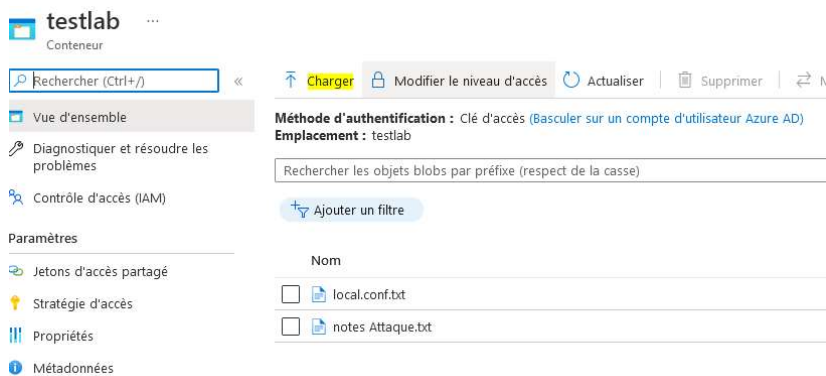
Conteneur (accès en lecture anonyme pour les conteneurs ...)

Toutes les données des conteneurs et des objets blob peuvent être lues par requête anonyme. Les clients peuvent énumérer les objets blob dans le conteneur par requête anonyme, mais ne peuvent pas énumérer les conteneurs dans le compte de stockage.

Avancé

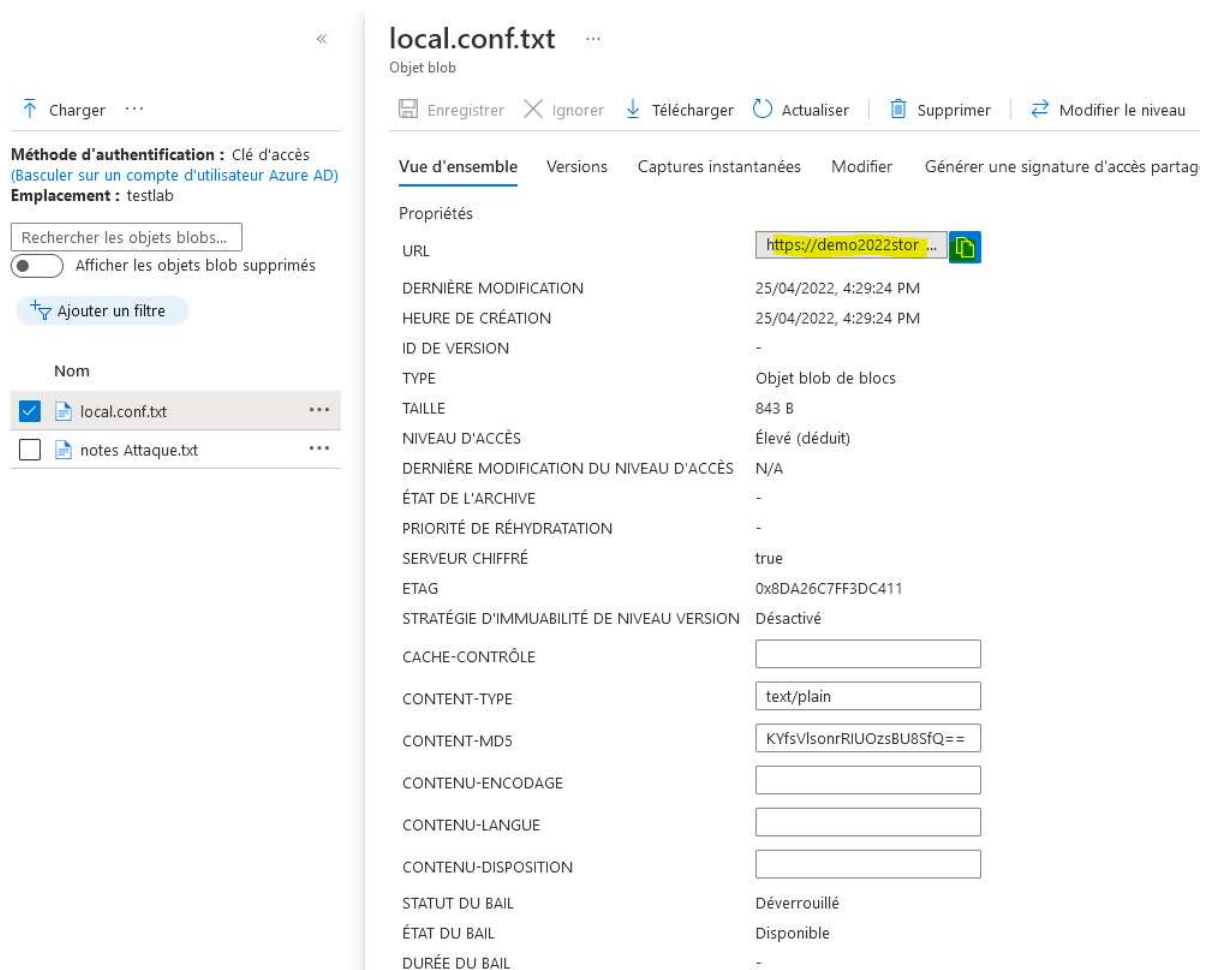
Dans cet exemple, je vais l'appeler demo, puis vous allez pouvoir définir un niveau d'accès. Par défaut, quand vous créez un conteneur, son niveau d'accès est privé. Personne d'autre que vous peut accéder à ce conteneur-là. Néanmoins, si vous souhaitez exposer ce conteneur publiquement sur internet, vous pouvez, par exemple, sélectionner Conteneur avec un accès en lecture anonyme pour les conteneurs et les objets blob, puis cliquer sur OK.

Le conteneur de stockage est désormais créé. Nous avons un conteneur qui se nomme demo. Nous pouvons cliquer dessus pour rentrer dedans, puis cliquer sur Charger, afin d'uploader un document, sélectionner votre fichier à uploader



Une fois l'upload terminé, Je clique sur les propriété du fichier.

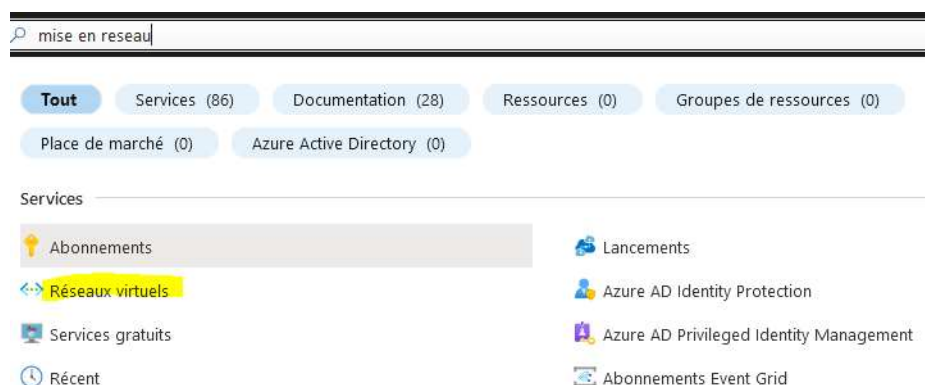
Je peux récupérer son URL, puis ouvrir un autre navigateur, en navigation privée, par exemple, coller mon URL et je peux constater que je peux accéder publiquement au fichier que je viens d'uploader sur internet.



Donc avec cette configuration, n'importe qui sur internet, connaissant cette URL-là, peut accéder à votre fichier. Dans le cas où vous utilisez un conteneur qui est exposé publiquement sur internet, faites attention à ne pas stocker des informations pouvant être sensibles. N'importe qui va alors pouvoir avoir accès aux fichiers contenus dans ce conteneur.

## Créer un réseau virtuel

La création d'un réseau virtuel dans Azure, plus souvent appelé Virtual Network ou encore VNet. Mais avant de commencer, prenons le temps de définir qu'est-ce qu'un réseau virtuel dans Azure. Un réseau virtuel dans Azure est un réseau privé qui va vous permettre d'interconnecter vos machines virtuelles et vos services Azure. Pour cela je vous invite à vous rendre dans le portail, sur "portal.azure.com", puis à cliquer sur "Tous les services". Je vous invite à aller dans la catégorie "Mise en réseau" puis à cliquer sur "Réseaux virtuels".



Comme nous pouvons le constater nous avons déjà des réseaux virtuels

Pour ajouter nouveau réseau virtuel, je vous invite à cliquer sur "Ajouter". Notre première étape va être de donner un nom à ce réseau virtuel. Dans notre exemple nous allons nommer notre réseau

[Accueil](#) > [Groupes de ressources](#) > [Formation](#) > [Créer une ressource](#) >

### Créer un réseau virtuel ...

[De base](#) [Adresses IP](#) [Sécurité](#) [Étiquettes](#) [Vérifier + créer](#)

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

#### Détails du projet

Abonnement \* ⓘ

Groupes de ressources \* ⓘ   
[Créer nouveau](#)

#### Détails de l'instance

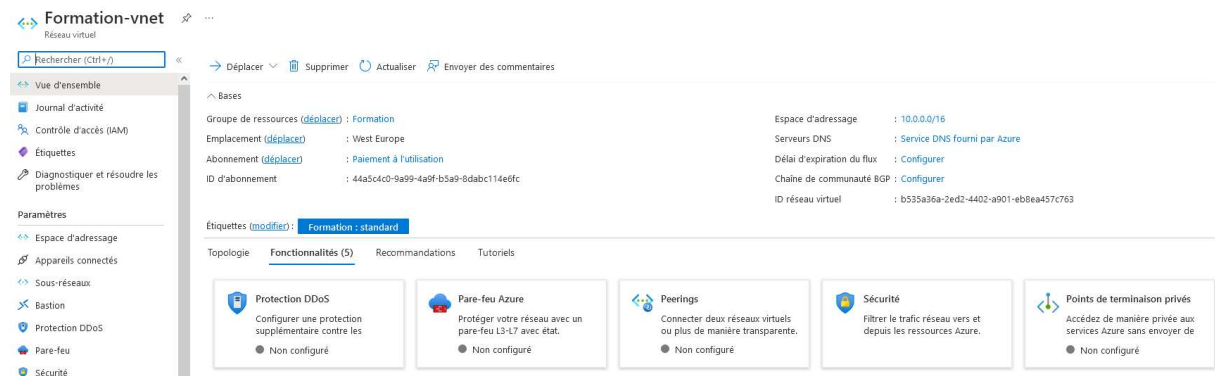
Nom \*

Région \*

virtuel "VnetFormation".

Comme nous pouvons le constater, l'espace d'adressage est 10.1.0.0/16. Il s'agit alors d'un espace

d'adressage d'IP privée. Nous sélectionnons notre abonnement Azure, puis nous sélectionnons le groupe de ressources dans lequel nous souhaitons créer notre réseau. Nous souhaitons que ce réseau soit créé dans l'est des États-Unis (ou west europe si vous avez choisis ce dernier). Un premier sous-réseau va être créé, il portera le nom de "default". Son plan d'adressage est 10.1.0.0/24. Nous souhaitons activer une protection contre les dénis de service, donc une protection de base, et nous souhaitons désactiver les points de terminaison de service. Enfin, il nous restera uniquement à cliquer sur le bouton "Créer" pour lancer la création de notre réseau virtuel.

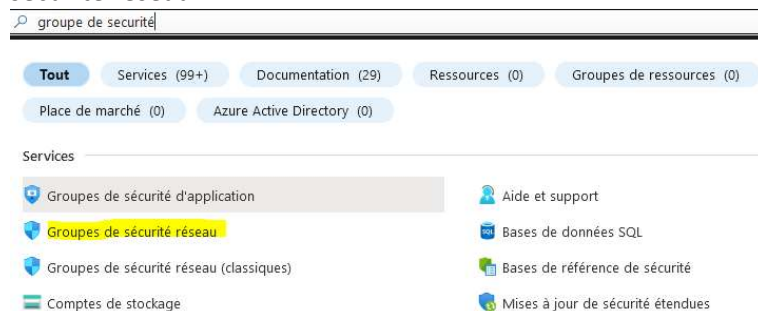


Le déploiement de notre réseau virtuel est en cours. Nous pouvons constater que le déploiement de notre réseau virtuel s'est déroulé avec succès. Si nous actualisons la liste des réseaux virtuels en cliquant sur le bouton "Actualiser", nous pouvons voir que notre réseau virtuel "VnetFormationt" est présent.

## Créer un sous-réseau dans un réseau virtuel existant

La création d'un nouveau sous-réseau dans un réseau virtuel existant est important car il permet de segmenter un réseau. Que cela soit un réseau dit classique, un réseau d'entreprise ou encore un réseau virtuel dans Azure, il est important de segmenter son réseau avec des sous-réseaux, ceci afin d'isoler certains groupes de machines ou encore certaines parties de son réseau. Plus concrètement, nous ne souhaitons pas forcément que nos bases de données puissent être accessibles directement depuis notre DMZ. Afin de conserver un niveau de sécurité adéquat dans son infrastructure Azure, je vous recommande fortement de segmenter votre réseau en divers sous-réseaux. Pour cela je vous invite à vous rendre sur le portail.

Nous allons dans un premier temps créer un groupe de sécurité réseau, un Network Security Group qui va nous permettre de filtrer le trafic de notre futur sous-réseau, autant le trafic entrant que le trafic sortant. Pour cela je vous invite à cliquer sur "Tous les services" puis saisir "nsg". "Groupes de sécurité réseau"



je vous invite à cliquer dessus. Comme vous pouvez le voir, nous avons déjà des groupes de sécurité réseau qui sont présents. Nous allons en ajouter un nouveau. Pour cela, cliquez sur "Ajouter". Nous allons donner un nom à notre groupe de sécurité, dans notre exemple "dmz-nsg". Nous sélectionnons l'abonnement, puis nous sélectionnons le groupe de ressources, le ressources group dans lequel nous allons stocker notre groupe de sécurité réseau.

### Créer un groupe de sécurité réseau ...

De base   Étiquettes   Vérifier + créer

Détails du projet

Abonnement \* Païement à l'utilisation

Groupe de ressources \* Formation  
[Créer nouveau](#)

Détails de l'instance

Nom \* dmz-nsg

Région \* West Europe

Dans notre scénario, nous souhaitons utiliser un groupe de ressources existant donc nous cochons "Utiliser existant". Sélectionnez votre groupe de ressource, son emplacement dans l'est des États-Unis (ou autre, en fonction de ce que vous avez choisis) et nous cliquons sur "Créer".

Notre groupe de sécurité est alors en déploiement. Nous pouvons constater que la création de notre groupe de sécurité s'est déroulée avec succès. Pour cela, je vous invite à passer à la seconde étape qui va être la création de notre sous-réseau dans un réseau virtuel existant.

Cliquez sur "Tous les services", à vous rendre dans la catégorie "Mise en réseau" puis cliquer sur "Réseaux virtuels". Je vous invite à sélectionner votre réseau, dans notre exemple "VnetFormation" puis à vous rendre dans la catégorie "Paramètres" puis "Sous-réseaux".

Accueil > Réseaux virtuels > Formation-vnet

### Réseaux virtuels

Répertoire par défaut

+ Créer   Gérer la vue

Filtrer un champ...

Nom
Formation-vnet
Formation-vnet-asr

### Formation-vnet | Sous-réseaux

Réseau virtuel

Rechercher (Ctrl+/)

+ Sous-réseau   + Sous-réseau de passerelle   Actualiser

Rechercher dans les sous-réseaux

Nom	IPv4	IP
default	10.0.0.0/24	-

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Diagnostiquer et résoudre les problèmes

Paramètres

Espace d'adressage

Appareils connectés

Sous-réseaux

Bastion

Nous pouvons constater qu'un sous-réseau est déjà présent. Nous allons en créer un deuxième en cliquant sur "Sous-réseaux". Nous allons définir un nom à ce sous-réseau, dans notre exemple "dmz". Nous pouvons voir que la plage d'adresse est 10.0.2.0/24. Nous allons associer le groupe de sécurité réseau que nous avons créé précédemment, dans notre exemple "dmz-nsg" puis je vous invite à cliquer sur "Ok".

Nom \*

Espace d'adressage de sous-réseau \* ⓘ  
  
 10.0.2.0 - 10.0.2.255 (251 + 5 adresses réservées Azure)

☐ Ajouter un espace d'adressage IPv6 ⓘ

Passerelle NAT ⓘ

Groupe de sécurité réseau

Table de routage

Enfin depuis votre VM Windows, ajoutez une interface réseaux lui permettant de se connecter à votre nouveau sous-réseaux DMZ et qui applique le groupe de sécurité dmz-nsg. Autorisez les flux icmp et RDP. Vous l'avez compris les groupes de sécurités sont des solution de filtrage à l'équivalence des firewalls au sein d'une entreprise.

[Accueil](#) > [Machines virtuelles](#) > [srv04](#) >

## Créer l'interface réseau ...

Détails du projet

Abonnement ⓘ

Groupe de ressources \* ⓘ  
  
[Créer nouveau](#)

Emplacement ⓘ

Interface réseau

Nom \*

Réseau virtuel ⓘ

Sous-réseau \* ⓘ

Groupe de sécurité réseau de la carte réseau ⓘ  
☐ Aucun  
☒ De base  
☐ Paramètres avancés

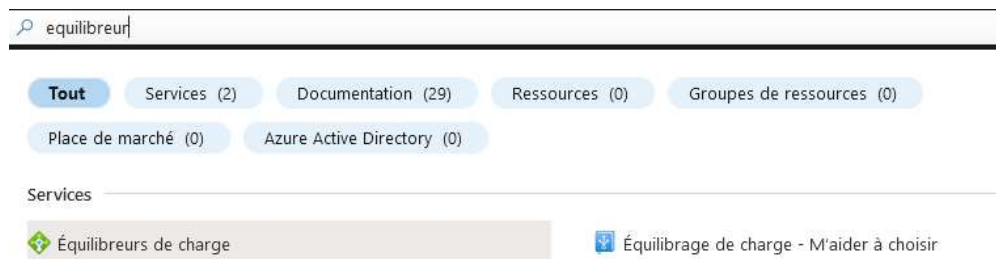
Ports d'entrée publics \* ⓘ  
☒ Aucun  
☐ Autoriser les ports sélectionnés

Sélectionner des ports d'entrée

Créer

## Intégrer un équilibreur de charge

Dans cette étape, nous allons voir comment créer un équilibreur de charge dans Azure, ou plus souvent appelé Load Balancer. Le rôle d'un équilibreur de charge est de répartir la charge sur un pool de machines. Dans notre exemple, nous avons deux serveurs web Windows composés de la machine win01 et de la machine win02. Elles sont toutes les deux membres d'un groupe de haute disponibilité nommé as-lb. Dans notre exemple, nous allons créer un équilibreur de charge travaillant sur la couche 4 du modèle OSI, la couche Transport.



Pour commencer, je vous invite à vous rendre sur le portail et à cliquer sur Tous les services. Vous pouvez saisir charge, puis cliquer sur Équilibreurs de charge. Enfin, cliquez sur Ajouter. Nous allons pouvoir définir un nom à notre équilibreur de charge, dans notre exemple lb-win. Nous souhaitons un type Public, une référence De base et nous allons créer une IP publique pour cet équilibreur de charge.



## Créer un équilibreur de charge ...

L'équilibreur de charge Azure est un équilibreur de charge de couche 4 qui répartit le trafic entrant entre plusieurs instances de machines virtuelles saines. Les équilibreurs de charge utilisent un algorithme de répartition basé sur le hachage. Ils utilisent par défaut un code de hachage composé d'un 5-uplet (adresse IP source, port source, adresse IP de destination, port de destination, type de protocole) pour mapper le trafic aux serveurs disponibles. Les équilibreurs de charge sont soit accessibles sur Internet (par l'intermédiaire d'une adresse IP publique), soit accessibles en interne (uniquement à partir d'un réseau virtuel). Les équilibreurs de charge Azure prennent également en charge la traduction d'adresses réseau (NAT) pour router le trafic entre des adresses IP publiques et privées. [En savoir plus.](#)

### Détails du projet

Abonnement \*

Groupe de ressources \*   
[Créer nouveau](#)

### Détails de l'instance

Nom \*

Région \*

RÉFÉRENCE (SKU) \* ⓘ ☒ Standard  
☐ Passerelle  
☐ De base

**i** Microsoft recommande un équilibreur de charge de référence SKU Standard pour les charges de travail de production.  
[En savoir plus sur les différences de prix entre les références SKU Standard et De base](#) ⓘ

Type \* ⓘ ☒ Public  
☐ Interne

Niveau \* ☒ Régional  
☐ Global

Cliquons sur Créer. Donnons un nom à notre iP publique, dans notre exemple lb-ip pub. Nous souhaitons que l'IP publique soit statique, donc nous cochons Statique et nous cliquons sur OK. Si nous le souhaitons, nous avons la possibilité d'ajouter une adresse IPv6 publique. Nous sélectionnons votre abonnement, votre groupe de ressources dans lequel nous allons souhaiter sauvegarder notre équilibreur de charge.

### Ajouter une configuration IP f... ✕

Nom \*

Version IP ☒ IPv4 ☐ IPv6

Type IP ☒ Adresse IP ☐ Préfixe IP

Adresse IP publique \*   
[Créer](#)

**Ajouter une adresse IP publique**

Nom \*

RÉFÉRENCE (SKU) ☐ De base ☒ Standard

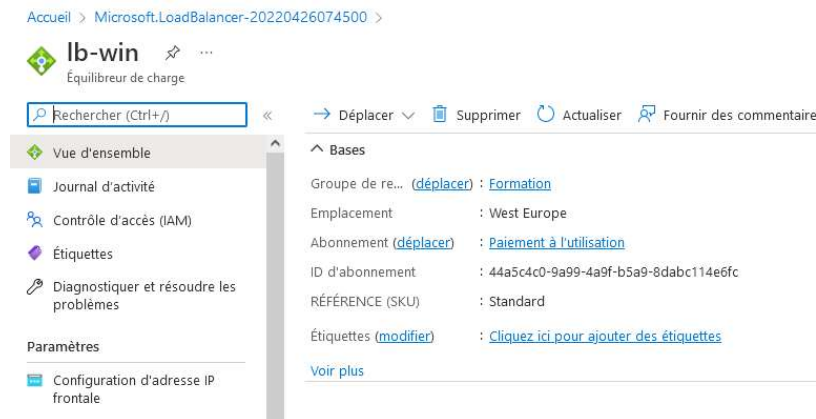
Niveau ☒ Régional ☐ Global

Affectation ☐ Dynamique  
☒ Statique

Zone de disponibilité \*

Préférence de routage ⓘ ☒ Réseau Microsoft  
☐ Internet

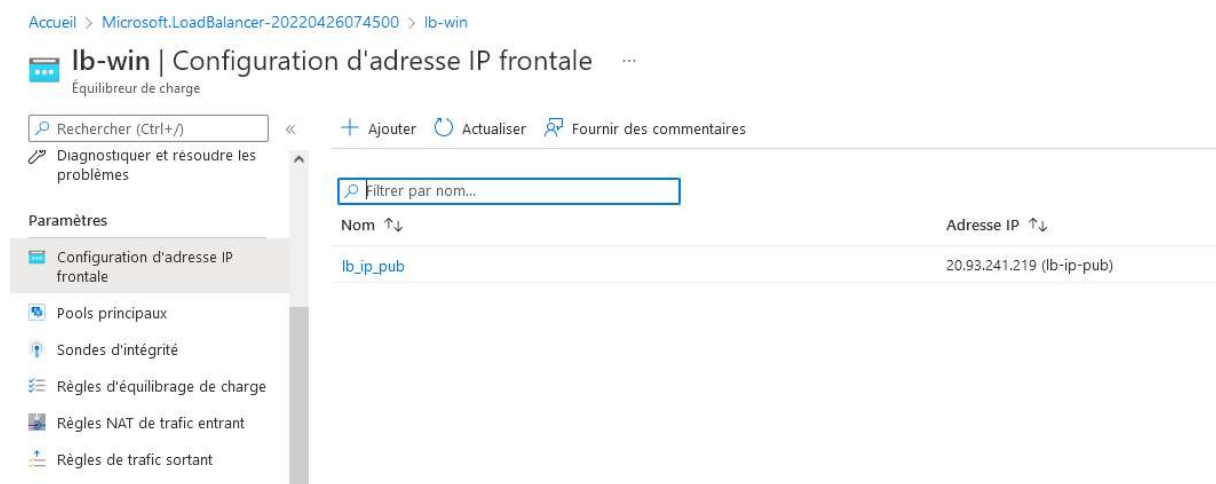
Enfin je peux définir l'emplacement, donc dans notre scénario, Est des États-Unis (ou west Europe si c'est votre choix) et je clique sur Créer. Le déploiement de notre équilibreur de charge est en cours. Nous avons désormais la confirmation que notre déploiement a réussi, notre équilibreur de charge s'est créé avec succès.



Nous pouvons cliquer sur Actualiser et nous pouvons voir que nous avons un équilibreur de charge qui se nomme lb-win.

## Configurer l'équilibreur de charge

Dans cette étape, nous allons voir comment configurer un équilibreur de charge. Pour cela, je vous invite à cliquer sur le nom de votre équilibreur de charge, dans mon exemple lb-win. Comme vous pouvez le constater, mon équilibreur de charge a l'adresse IP publique 20.93.241.219, adresse IP publique qui a été créée lors de la création de l'équilibreur de charge.



Nous allons, dans un premier temps, configurer notre pool. Pour cela, allez dans l'onglet Paramètres, puis Pools principaux. Cliquez sur Ajouter. Notre pool va contenir deux machines, nos deux serveurs web, à savoir web01 et web02 qui doivent faire partie du même groupe de haute disponibilité : as-lb. Si cela n'a pas encore été fait, déployez deux VM windows avec le rôle IIS d'installé.

Enfin modifiez le fichier iisstart.htm de chacun d'entre eux afin d'y inclure un message permettant de les identifier. Enfin la déclaration du lien avec votre load balancer peut se faire lors de la création de votre VM ou après dans la configuration du load balancer.

## Créer une machine virtuelle ...

Groupe de sécurité réseau de la carte réseau ⓘ ☐ Aucun ☐ De base ☒ Paramètres avancés

Configurer le groupe de sécurité réseau  [Créer](#)

Supprimer l'adresse IP publique et la carte réseau lors de la suppression de la machine virtuelle ⓘ ☐

Mise en réseau accélérée ⓘ ☒

**Équilibrage de charge**

Vous pouvez placer cette machine virtuelle dans le pool de back-ends d'une solution d'équilibrage de charge Azure existante. [En savoir plus](#)

Placer cette machine virtuelle derrière une solution d'équilibrage de charge existante ? ☒

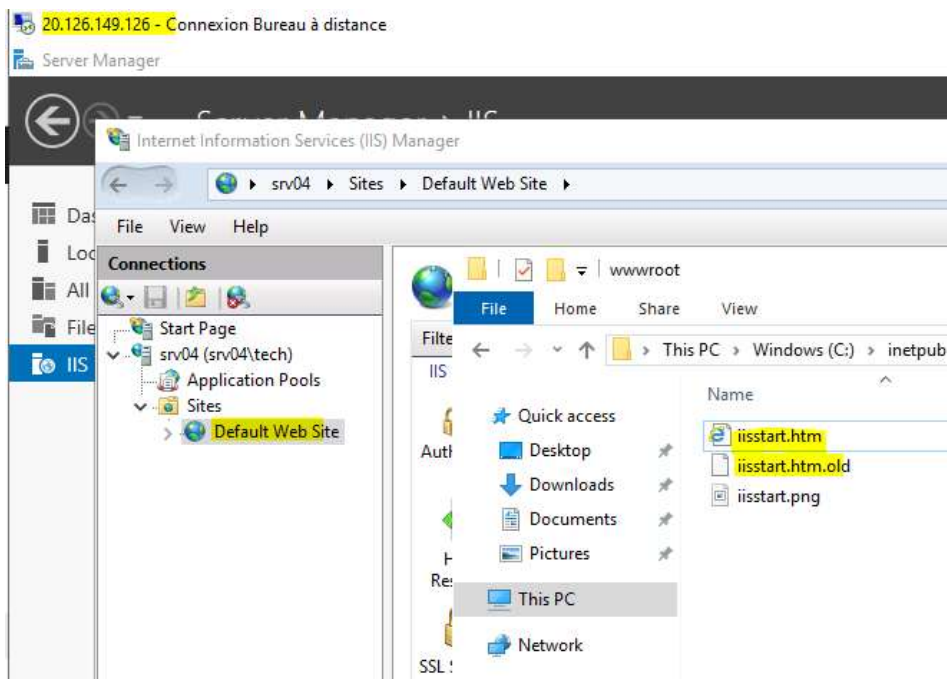
**Paramètres d'équilibrage de charge**

- **Application Gateway** est un équilibreur de charge du trafic web HTTP/HTTPS avec un routage basé sur l'URL, une résiliation SSL, une persistance de session et un pare-feu d'applications web. [En savoir plus sur Application Gateway](#)
- **Azure Load Balancer** prend en charge la totalité du trafic réseau TCP/UDP, le réacheminement de port et les flux sortants. [En savoir plus sur Azure Load Balancer](#)

Options d'équilibrage de charge \* ⓘ

Sélectionner un équilibreur de charge \* ⓘ

Sélectionner un pool de back-ends \* ⓘ  [Créer](#)



```
iisstart.htm - Notepad
File Edit Format View Help
<html>
<head>
<title>
Mon Site web
</title>
</head>
<body>
Ceci est un site de test de win01
</body>
</html>
```

Autre solution :

Dans un deuxième temps, je vais donner un nom à mon pool, à savoir pool-win. Dans l'onglet Associé à, je vais sélectionner Groupe à haute disponibilité. Je sélectionne mon groupe à haute disponibilité, à savoir le groupe as-lb contenant deux machines virtuelles, mes deux machines win01 et win02. Puis je clique sur Ajouter une configuration IP réseau cible, je sélectionne ma première machine, win01. Je sélectionne sa configuration IP réseau, puis je clique de nouveau sur Ajouter une configuration IP réseau cible. Je sélectionne ma seconde machine, win02, son interface réseau et je clique sur OK. Mon pool est actuellement en train de s'enregistrer. Nous pouvons voir qu'une première machine vient d'être ajoutée au pool.

Accueil > lb-win >

### Pool\_LB ...

lb-win

Nom	Pool_LB
Réseau virtuel	Formation-vnet (Formation)
Configuration du pool de back-ends	<input checked="" type="radio"/> Carte réseau <input type="radio"/> Adresse IP
Version IP	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6

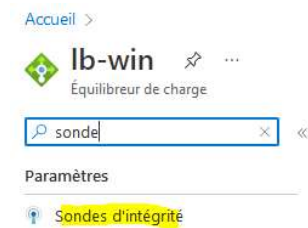
**Machines virtuelles**

Vous pouvez uniquement attacher des machines virtuelles dans westeurope si elles ont une configuration IP publique avec une référence SKU standard ou aucune configuration IP publique. Toutes les configurations IP doivent être dans le même réseau virtuel.

<input type="checkbox"/> Machine virtuelle	Configuration IP	Groupe à haute disponibilité
<input type="checkbox"/> win01	ipconfig1 (10.0.0.7)	-
<input type="checkbox"/> vm03	ipconfig1 (10.0.0.9)	-

Ajoute de la sonde d'intégrité

## Mise en œuvre de la sonde d'intégrité

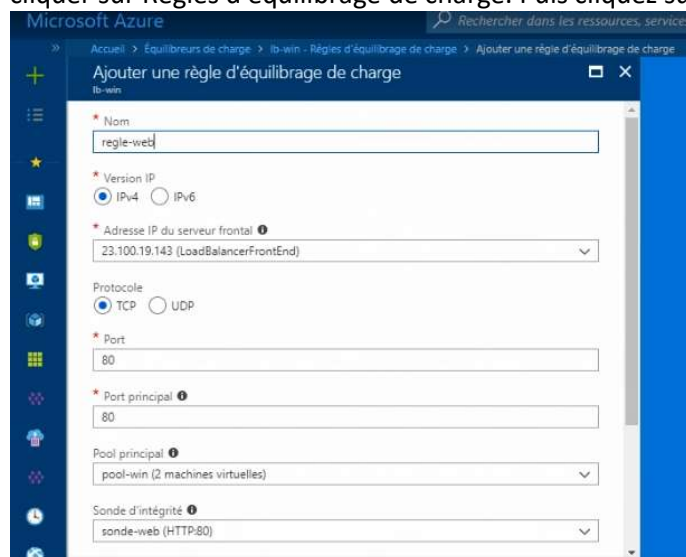


Notre prochaine étape va être de configurer notre sonde d'intégrité. Pour cela, je vous invite à cliquer sur **Sondes d'intégrité**. Puis cliquez sur **Ajouter**. Je vous invite à donner un nom à cette sonde, dans notre exemple sonde-web. Étant donné que dans notre pool, nous avons des serveurs web, je vous invite à cocher **Protocole HTTP**.



Dans **Port** nous avons 80. **Chemin d'accès**, nous avons la racine. **Intervalle**, nous avons 5 secondes. **Seuil de défaillance sur le plan de l'intégrité**, nous avons deux échecs consécutifs. Nous confirmons la création de notre sonde en cliquant sur **OK**. Notre sonde est actuellement en train de se créer. Notre sonde a bien été créée.

La dernière étape va être la création d'une règle d'équilibrage de charge. Pour cela, je vous invite à cliquer sur **Règles d'équilibrage de charge**. Puis cliquez sur **Ajouter**.



Nous allons donner un nom à notre règle d'équilibrage de charge, à savoir **regle-web**. **Version IP**, **IPv4**. Nous avons l'adresse IP du serveur frontal qui correspond à l'adresse IP publique de notre

équilibreur de charge. Protocole, TCP. Port, 80. Port principal, 80. Pool principal, il s'agit du pool que nous avons créé précédemment, pool-win, composé de deux machines, win01 et win02. Sonde d'intégrité, nous avons bien sonde-web. Persistance de session, nous n'en avons pas. Délai d'inactivité, nous avons 4 minutes. Nous pouvons dès à présent cliquer sur OK. L'enregistrement de la règle d'équilibrage de charge est en cours. Notre règle d'équilibrage de charge vient d'être ajoutée.

La configuration de notre Load Balancer est désormais terminée. Je vous invite à cliquer sur Vue d'ensemble, puis à copier l'adresse IP publique de notre Load Balancer, ouvrir un nouvel onglet et coller. Nous pouvons dès à présent cliquer sur Entrée. Nous sommes directement redirigés vers une de nos machines, soit web01, soit web02. Notre Load Balancer fonctionne.

Faite le test d'accès web.