Créer une App pour Azure (partie 5)

Cloud, CSS, Docker, HTML, PHP

Langage Compétences : 5

La transition digitale a poussé les éditeurs de logiciels et les entreprises à migrer leurs applications sur le web. Les services du cloud Azure ont offert la plateforme idéale, les services adéquats, ainsi que les outils, pour réaliser un développement vers le tout numérique en gardant le contrôle total sur les données. Cette publication propose la création d'une application simple en découvrant certains de ces services et outils.

Publié mercredi 22 juin 2022, 18h14
Modifié lundi 26 août 2024, 10h04

By Olivier Paudex

Sécurité sur Azure

Contrairement au machines virtuelles (VM), les services dans Azure sont publics. C'est-à-dire qu'ils sont partagés par plusieurs personnes. On les appelle aussi des **PaaS**, pour **"Plateforme as a Service"**, ou encore des **"tenants"**, parce qu'ils ne sont qu'une instance applicative d'un serveur global.

> Cette publication est composée de plusieurs partie. Ceci étant la 5ème partie.

Il y a néanmoins des possibilités de rendre ces services privatifs. Cette publication va parler de plusieurs éléments :

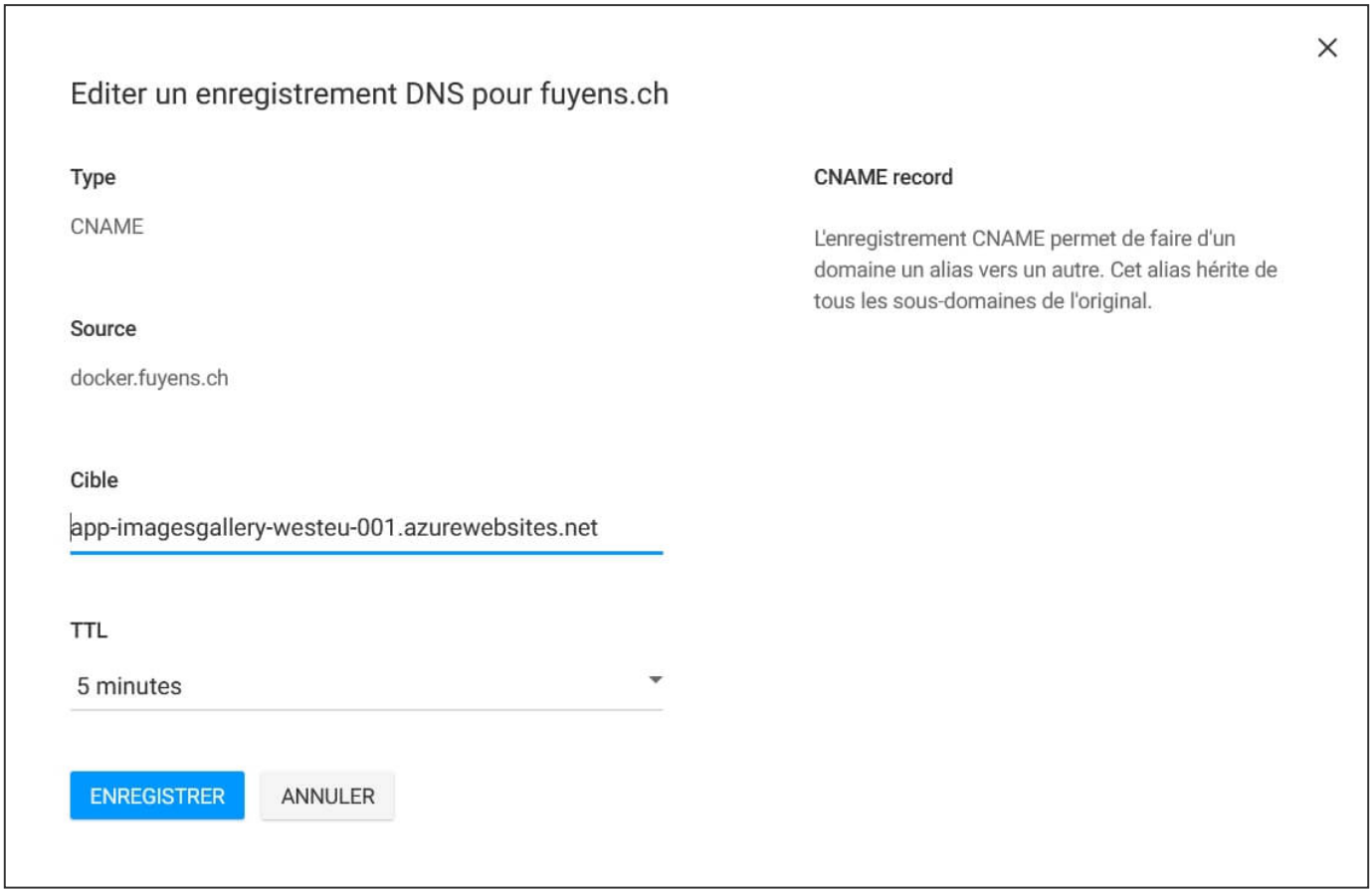
- Le DNS.
- Les certificats SSL.
- Les virtuals networks.
- Les points de terminaison privés.
- Le service **"Application Gateway"**.

DNS

Jusqu'à présent, l'application répond à l'URL suivante : **"https://[nom de l'app].azurewebsites.net/"**.

Ce n'est pas très pratique. La plupart du temps, une application devrait répondre à un nom de domaine personnalisé. Pour réaliser ceci, rien de plus simple.

- Réservez un nom de domaine
- Créez un enregistrement dans votre domaine de type **CNAME**
- L'application, dans cet exemple, prendra le nom de **"docker.fuyens.ch"**.
- Sa cible est l'URL donné par Azure.



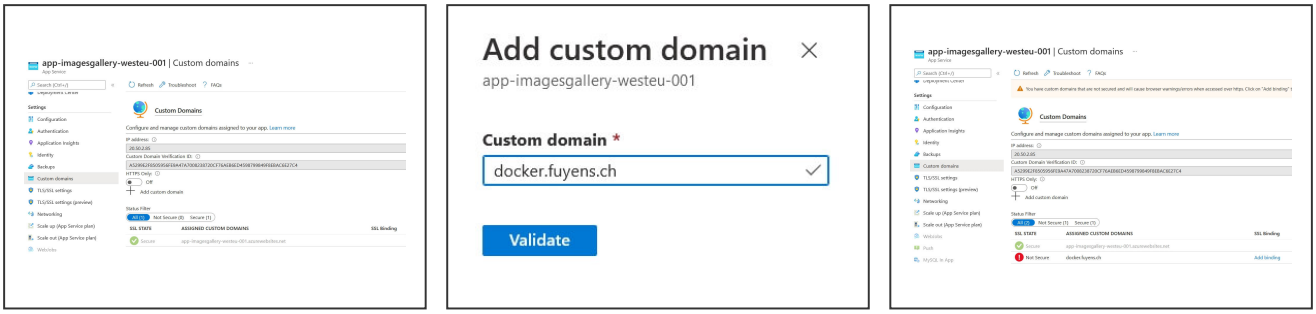
L'enregistrement du CNAME

Retournez dans l'application et ajoutez votre nouveau nom de domaine personnalisé.

- Cliquez sur l'onglet **"Custom Domains"**.
- Ajoutez votre nom de domaine personnalisé.

Le nom est maintenant lié à l'application, mais n'est pas encore sécurisé. On peut voir l'avertissement **"Not Secure"** en rouge.

Vous pouvez essayer d'entrer l'URL, dans mon exemple : **http://docker.fuyens.ch**. Ceci fonctionne, mais le navigateur vous avertira que le site n'est pas sécurisé.

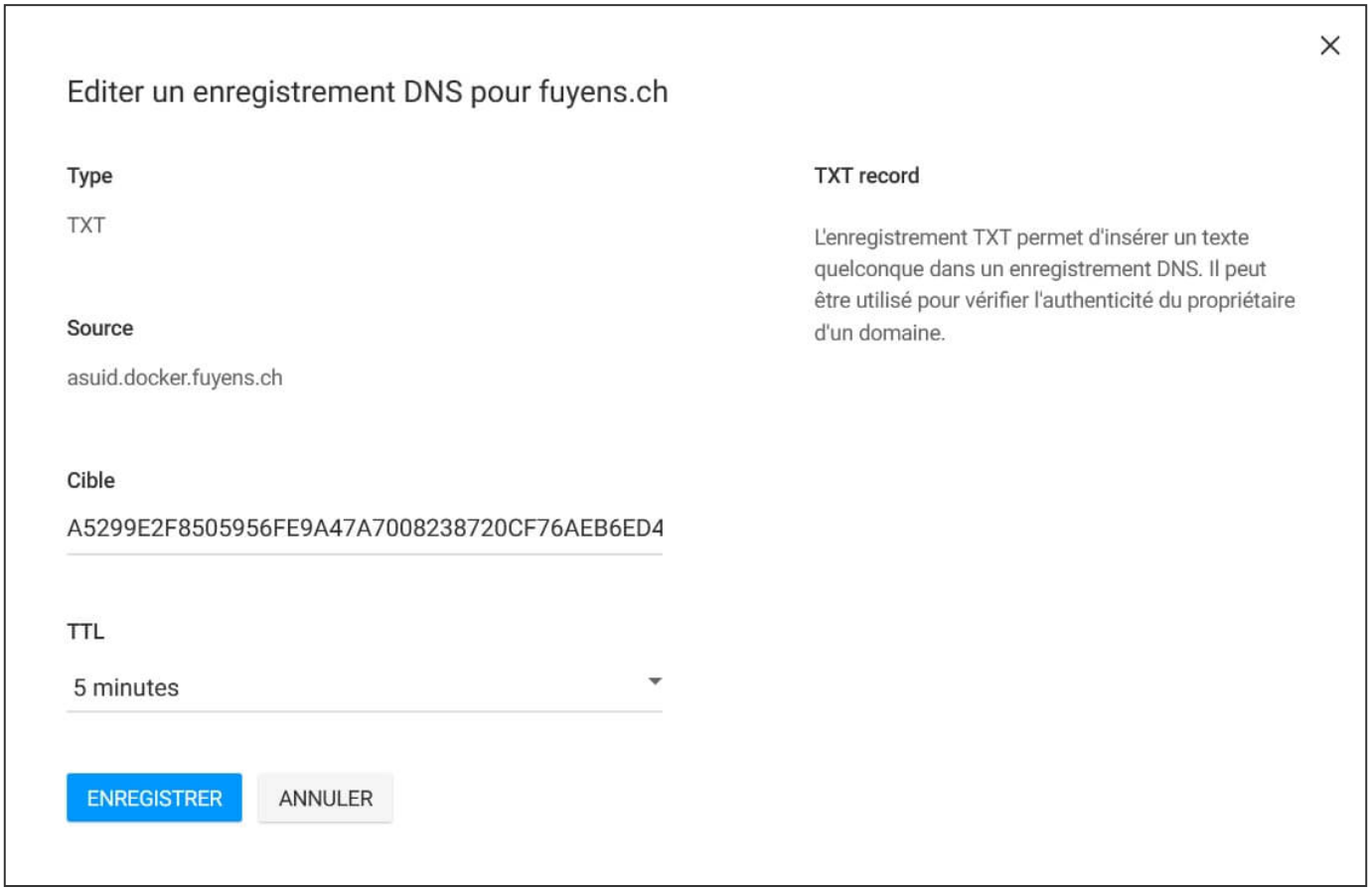


Ajouter un nom de domaine personnalisé

Le certificat SSL

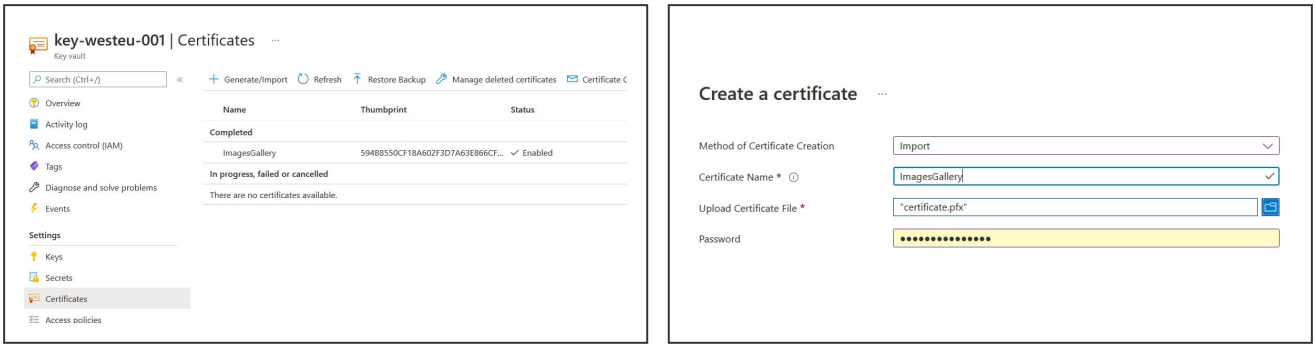
Pour remédier à ce problème, il faut souscrire à un certificat SSL.

- Copiez l'adresse IP de l'application (voir l'image ci-dessus).
- Copiez l'ID de vérification du domaine personnalisé.
- Retournez sur votre DNS.
- Créez un enregistrement de type **TXT** et nommez-le **"asuid.docker.fuyens.ch"**, dans mon exemple.
- Collez-y l'ID de vérification.



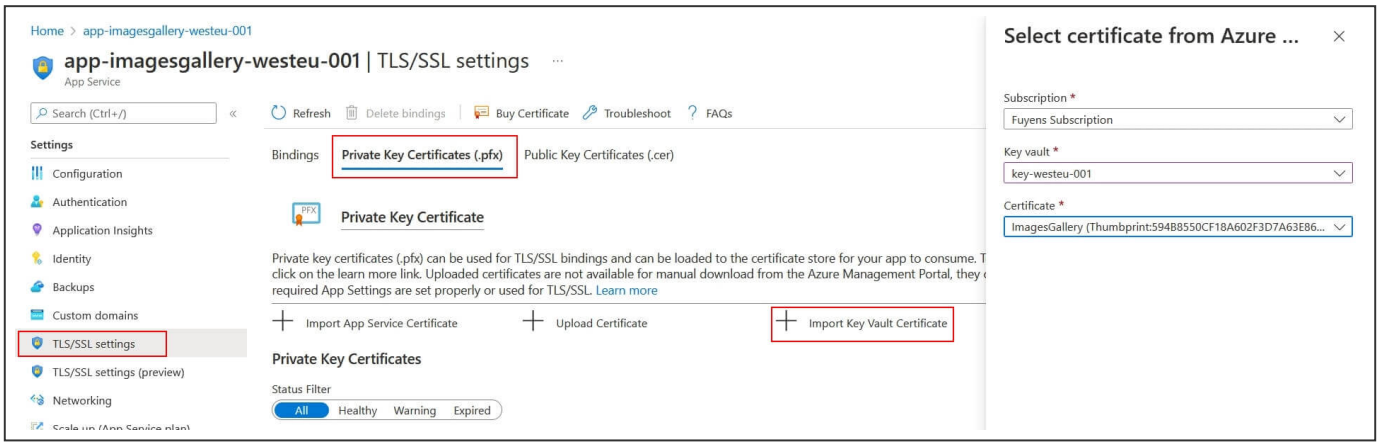
L'enregistrement TXT pour la vérification du domaine personnalisé

- Créez un certificat en choisissant l'un des nombreux fournisseurs sur le marché.
- Convertissez votre certificat au format **PFX**, si nécessaire (avec SSLShopper ou OpenSSL, si vous êtes plus branché ligne de commandes).
- Retournez dans le KeyVault.
- Cliquez sur l'onglet **"Certificates"**.
- Cliquez sur **"Generate/Import"**.
- Sélectionnez **"Import"**.
- Entrez un nom pour le certificat.
- Sélectionnez votre certificat au format PFX.
- Entrez le mot de passe donné lors de la création du certificat.



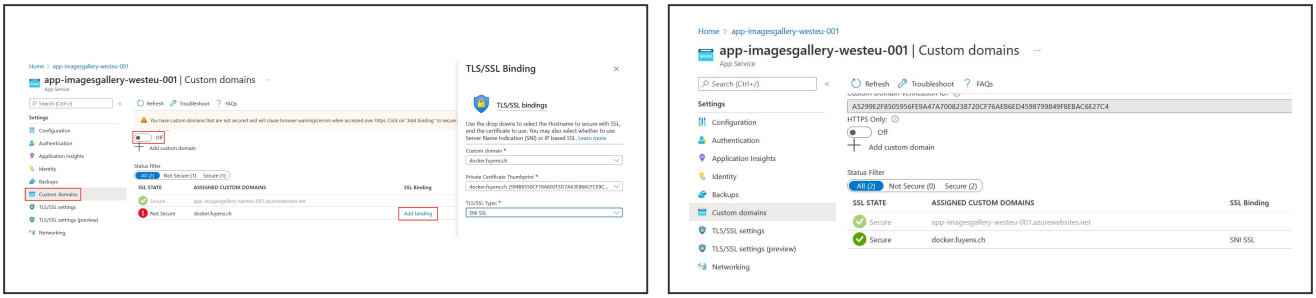
Importation du certificat dans le KeyVault

- Retournez dans l'application.
- Cliquez sur l'onglet **"TLS/SSL settings"**.
- Cliquez sur **"Private Key Certificates (.pfx)**.
- CLiquez sur **"Import Key Vault Certificate"**.
- Sélectionnez le certificat.



Importation d'un certificat depuis le KeyVault

- Cliquez sur l'onglet **"Custom Domains"**.
- Cliquez sur **"Add binding"**.
- Sélectionnez le certificat.



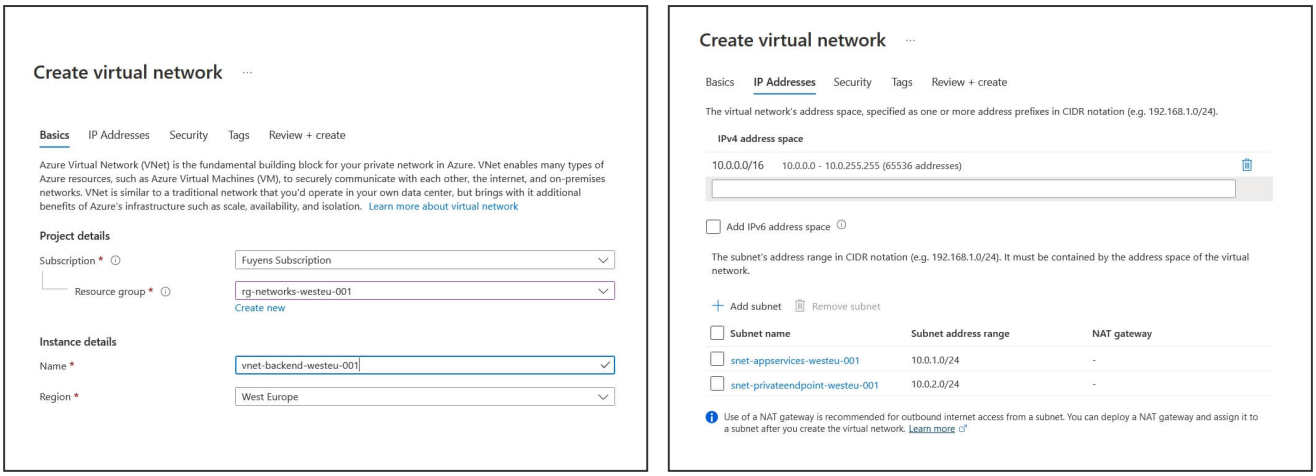
Liaison du certificat avec l'application

Cette fois-ci, notre application est validée par un certificat.

Les réseaux virtuels

Si notre application est publique, il en va pas de même pour tous les autres services (base de données, stockage, keyvault). Nous allons y remédier en créant des réseaux virtuels et des accès privatisés.

- Créez un **"Virtual network (Vnet)".**
- Sélectionnez le groupe de ressources du réseau.
- Entrez un nom du style **"vnet-backend-westeu-001"**.
- Ajoutez le sous-réseau **"snet-appservices-westeu-001"** et appliquez lui le réseau IP **"10.0.1.0/24"**.
- Ajoutez le sous-réseau **"snet-privateendpoint-westeu-001"** et appliquez lui le réseau IP **"10.0.2.0/24"**.



Création du Vnet "Backend"

- Recommencez avec un autre Vnet.
- Entrez un nom du style **"vnet-frontend-westeu-001"**.

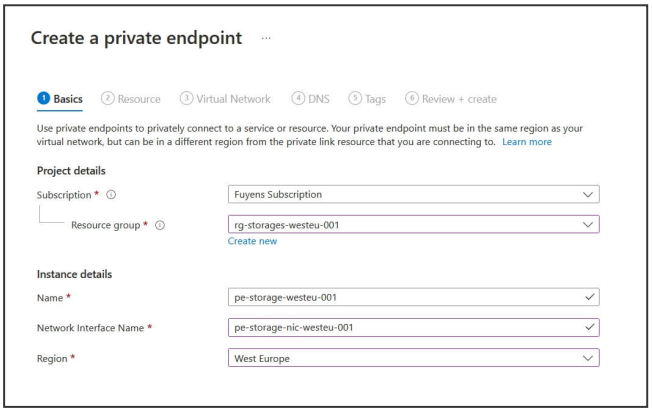
- Ajoutez le sous-réseau **"snet-appgateway-westeu-001"** et appliquez lui le réseau IP **"10.1.1.0/24"**.
- Ajoutez le sous-réseau **"snet-privateendpoint-westeu-001"** et appliquez lui le réseau IP **"10.1.2.0/24"**.

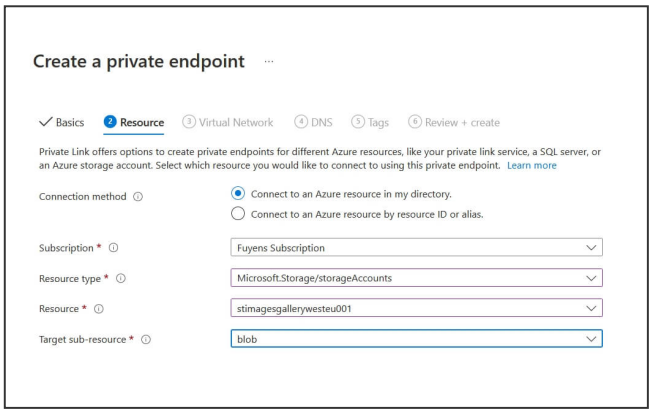
Les points de terminaison privés

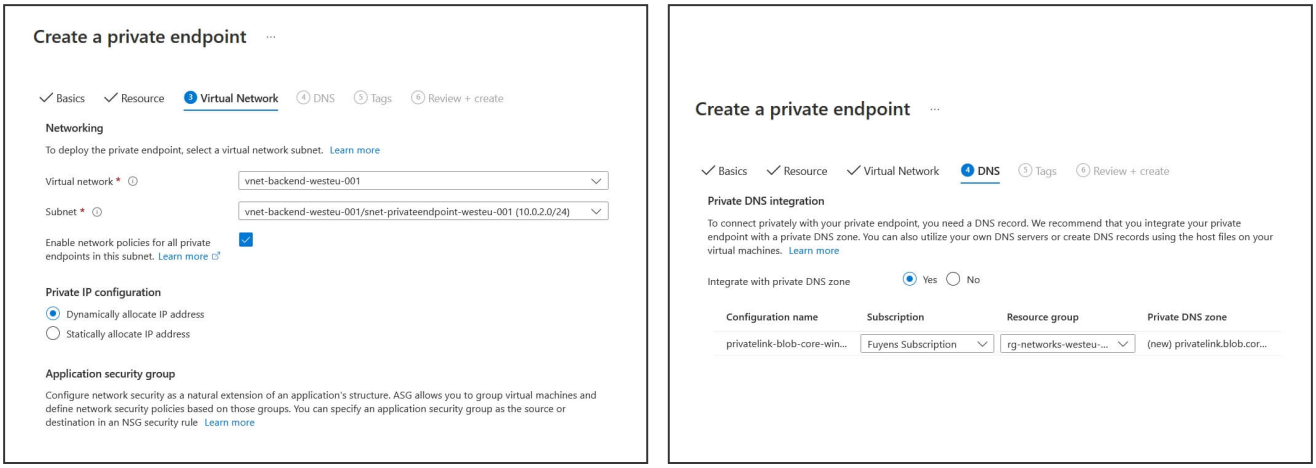
Les points de terminaison privés permettent d'ajouter une adresse IP privée à un service public, comme le stockage ou la base de données.

Le stockage

- Ajoutez un point de terminaison (private endpoint).
- Sélectionnez le groupe de ressources du stockage.
- Entrez un nom du style **"pe-storage-westeu-001"**.
- Entrez un nom pour la carte réseau du style **"pe-storage-nic-westeu-001"**.
- Sélectionnez le type de ressource **"Microsoft.Storage/storageAccounts"**.
- Sélectionnez **"blob"** pour la sous-ressource.
- Sélectionnez le subnet **"Private endpoint"**, précédemment créé.
- Sélectionnez l'intégration avec une zone DNS privée.







Configuration d'un point de terminaison privé pour le service de stockage

La base de données

- Recommencez pour la base de donnée en sélectionnant le groupe de ressources de la base de données et le type de ressource **"Microsoft.Sql/servers"**.
- Sélectionnez le subnet **"Private endpoint"**, précédemment créé.

Le coffre-fort

Le coffre-fort fait très fort !

Il possède deux points de terminaisons privés. L'un pour le **"vnet de backend"**, pour que l'application puisse retrouver les secrets. L'autre pour le **"vnet de frontend"** pour que le service **"application gateway"** puisse y retrouver le certificat SSL.

- Recommencez une troisième fois pour le KeyVault.
- Sélectionnez le type de ressource **"Microsoft.KeyVault/vaults"**.
- Sélectionnez une fois le vnet **"backend"**.
- Recommencez une dernière fois pour le Keyvault.
- Sélectionnez le type de ressource **"Microsoft.KeyVault/vaults"**.
- Sélectionnez une fois le réseau virtuel **"frontend"** et le sous-réseau **"private endpoint"**.

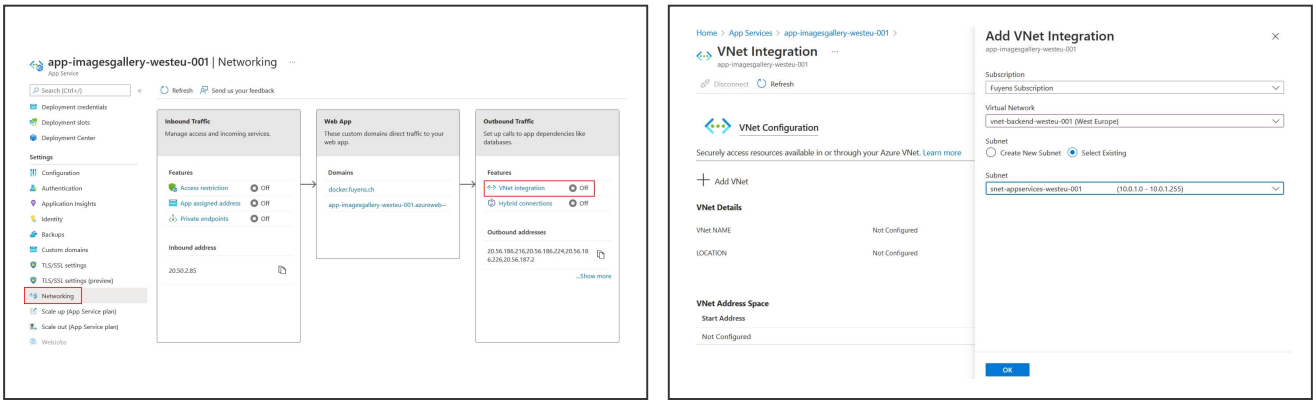
Les trois services sont maintenant liés au réseau virtuel **"Backend"**.

Le service du coffre-fort est également lié au réseau virtuel **"Frontend"**.

Intégration de l'application au réseau virtuel

Pour intégrer une application à un réseau virtuel, il suffit de le sélectionner.

- Retournez dans l'application.
- Cliquez sur l'onglet **"Networking"**.
- Cliquez sur **"Vnet Integration"**.
- Cliquez sur **"Add Vnet"**.
- Sélectionnez le vnet **"backend"**.
- Sélectionnez le sous-réseau **"appservices"**.

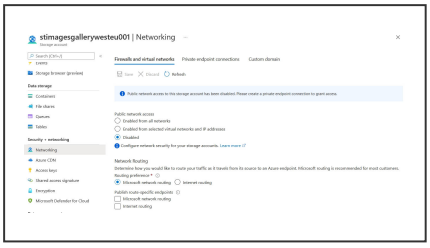
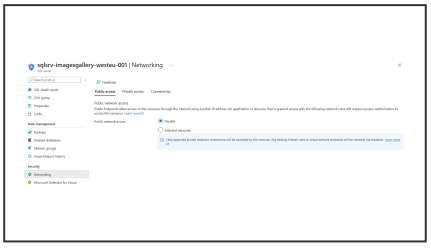
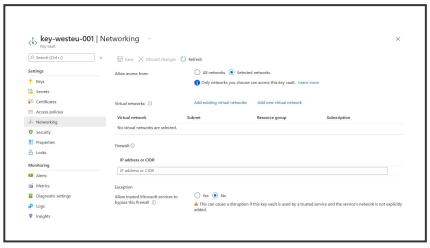


Intégrer une application dans un réseau virtuel

Désactivation des droits d'accès au différents services

Pour sécuriser l'infrastructure, faîtes le tour des trois services et désactivez l'accès au réseau public.

- Dans le compte de stockage, cliquez sur **"Networking"**, puis sélectionnez **"Désactivez l'accès au réseau public"**.
- Idem pour le serveur de base de données.
- Dans le coffre-fort, il n'y a pas de désactivation possible, alors sélectionnez **"Selected networks"** et dans les exceptions, sélectionnez **"No"** pour **"Allow trusted Microsoft services to bypass this firewall"**.

Désactivation de l'accès au réseau public

Vérification de l'accès

Vérifiez que l'application fonctionne toujours

- Essayez de vous connectez à la base de données à l'aide de **Azure Data Studio**, il devrait y avoir une erreur de connexion.
- Idem pour le stockage avec **Azure Storage Explorer**.

L'Application Gateway

L'Application Gateway permet de créer, comme son nom l'indique, une passerelle unique en entrée de l'infrastructure. Elle filtre les protocoles autorisés, et redirige le trafic vers une ou plusieurs applications ou services. Elle permet entre autres de :

- Ajouter une seule adresse IP publique en entrée de notre infrastructure.
- Ajouter de la sécurité en créant des règles d'écoute sur un protocole en particulier.
- Ajouter une option de part-feu (firewall) à notre infrastructure.
- Équilibrer les charges sur plusieurs ressources, en redirigeant le trafic vers une ressource en fonction de l'URL.

> Les ressources de sécurité font partie des éléments du cloud Azure les plus onéreux. Une passerelle frontale comme celle utilisée pour cette application de démo peut coûter environ **6 € par jour**. Donc attention de ne pas la laisser en activité plus de temps que nécessaire.

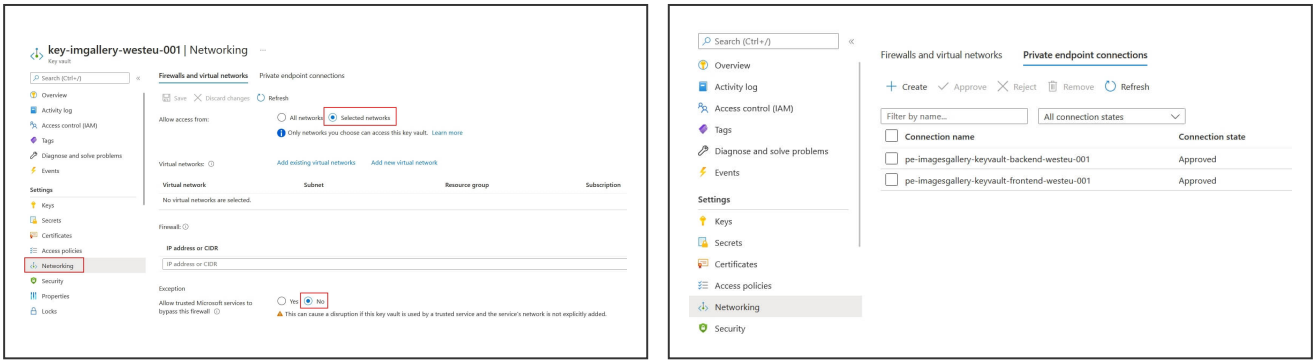
Azure Managed Identity (AMI)

L'application gateway va utiliser le certificat SSL en lieu et place de l'application. Pour accéder au **"Keyvault"** contenant le certificat, celui-ci doit s'enregistrer auprès du service **"Keyvault"**. Au contraire du **"Apps service"** qui utilise une identité de type **"System assigned"**, le service **"Application gateway"** va devoir utiliser une identité de type **"User assigned"**. Pour réaliser ceci, il faut passer par un **"Azure Managed Identity"** ou AMI.

- Créez un Azure User Managed Identity.
- Copiez son ID depuis la page **"Overview"**.
- Retournez dans le Keyvault.
- Ajoutez une règle d'accès.
- Ajoutez le droit **"GET"** pour les **"Secret permissions"**.
- Cliquez sur **"Select principal"**.
- Collez l'ID de l'AMI.
- Ajoutez l'accès au keyvault pour l'AMI.

Accéder au Keyvault depuis l'Application Gateway

- Cliquez sur l'onglet **"Networking"** du Keyvault.
- Sélectionnez "Selected networks".
- N'ajoutez aucun réseau virtuel.
- Sélectionnez **"No"** pour l'exception **"Allow trusted Microsoft services to bypass this firewall"**.
- Vérifiez bien que vous avez configuré deux points de terminaisons privés.



Configuration du Keyvault avec deux points de terminaisons privés

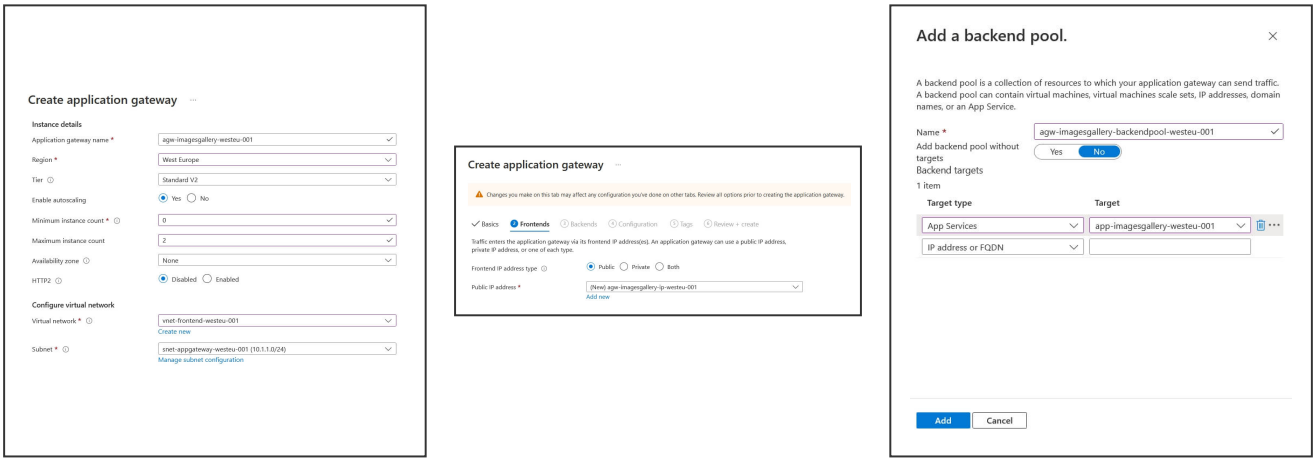
Application Gateway

Onglet Basics

- Créez une Application Gateway.
- Donnez-lui un nom.
- Laissez le nombre minimum d'instance à 0.
- Ajustez le nombre maximum d'instance à 2.
- Pour la configuration du virtual network, ajoutez le réseau virtuel **"frontend"** et le sous-réseau **"app gateway"**.

Onglet "Frontends et Backends"

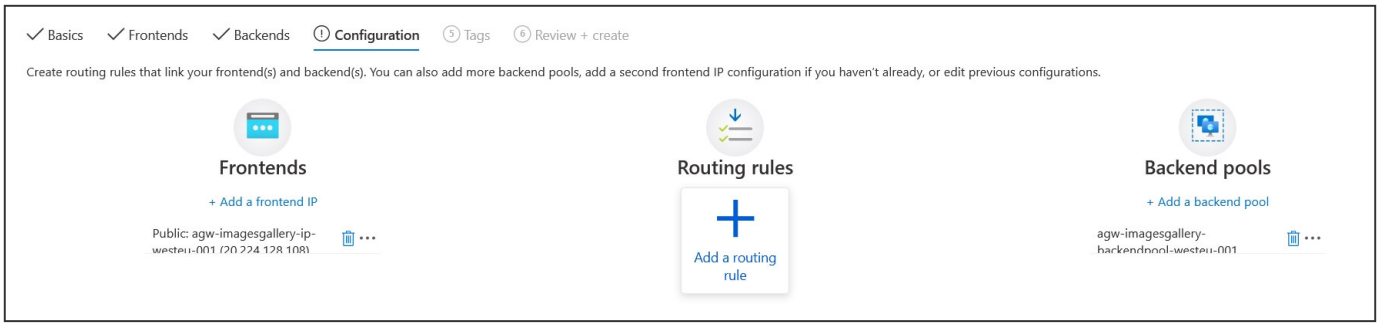
- Pour l'onglet **"Frontends"**, ajoutez une nouvelle adresse IP publique.
- Pour l'onglet **"Backends"**, ajoutez un backend pool et associez-lui l'application en tant que cible.



La création du "Frontend" et du "Backend"

Onglet Configuration

Une fois le **"Frontend"** et le **"Backend"** ajoutés, l'Application Gateway a besoin de les relier au travers de règles de routage qui vont filtrer les protocoles autorisés. On appelle ceci un**"listener"**.



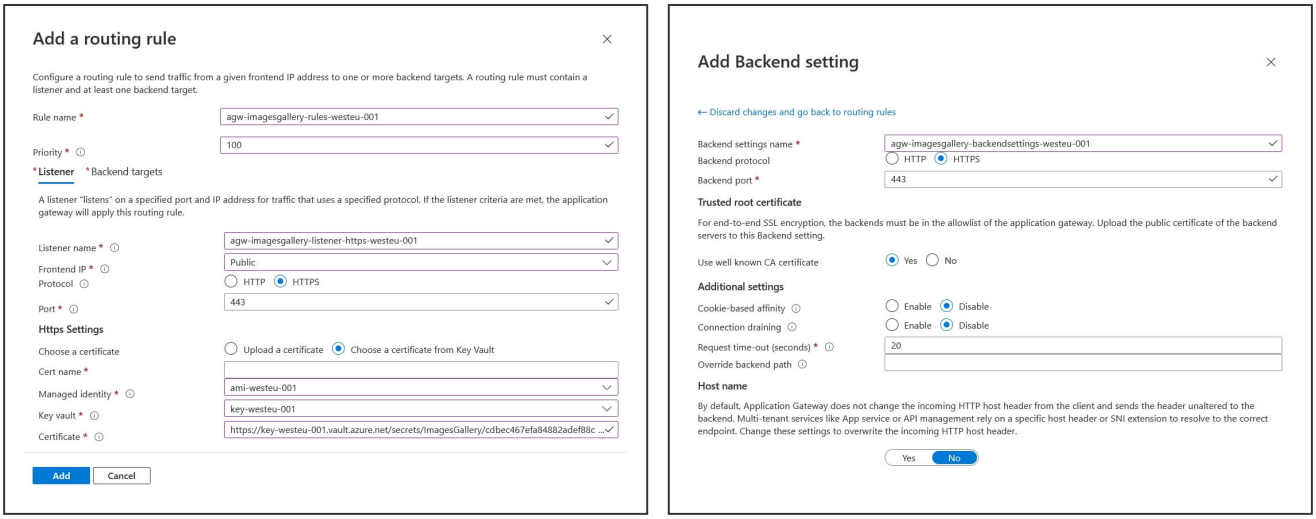
Les règles de routage

- Cliquez sur **"Add a routing rule"**.
- Nommez-la.
- Donnez-lui une priorité de 100.

- Ajoutez un **"Listener"** et associez-lui le protocole HTTPS et le port 443.
- Sélectionnez **"Choose a certificate from Key Vault"**.
- Sélectionnez l'AMI et le Keyvault.
- Collez l'URL de l'ID secrète du certificat.

> Microsoft recommande à ce propos de ne donner que le chemin du certificat, sans son ID. Ceci facilite le renouvellement du certificat.

- Créez un nouveau **"Backend setting"**.
- Nommez-le.
- Sélectionnez le protocole HTTPS et le port 443.
- Sélectionnez **"Yes"** l'option **"Use well known CA certificate"**.



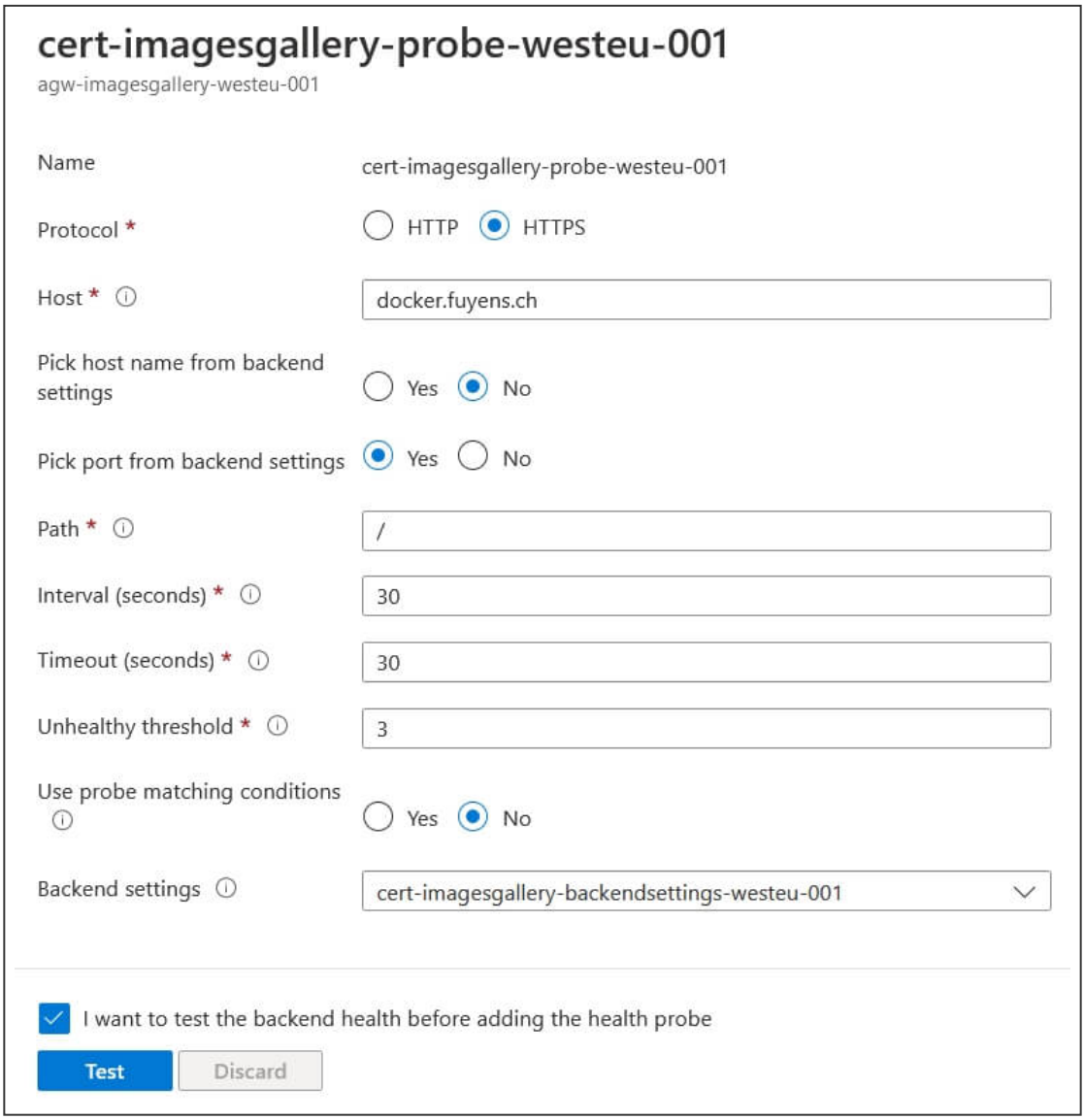
La règle de routage et ses paramètres

La sonde de santé

La sonde de santé permet de contrôler et de tester que l'application gateway fonctionne correctement.

- Créez une sonde de santé (**"probe-health"**).
- Nommez-la.
- **Très important !** Donnez au **"host"**, le nom de votre application sur le certificat. Dans mon cas, celui-ci est **"docker.fuyens.ch"**.

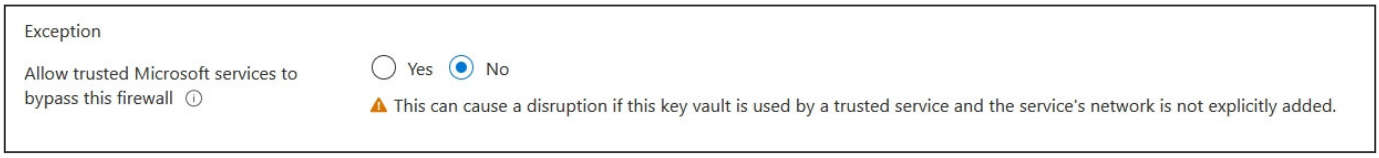
- Sélectionnez **"No"** pour l'option **"Pick host name from backend settings"**.
- Sélectionnez **"Yes"** pour l'option **"Pick port from backend settings"**.
- Entrez **"/"** pour le chemin **("path")**.
- Sélectionnez le backend settings.
- Laissez les autres options par défaut.
- Cochez **"I want to test the backend health before adding the health probe"**.
- Cliquez sur **"Test"**.



Création de la sonde de santé

Le résultat doit être une coche verte.

> Si ce n'est pas le cas, vérifiez le nom de votre certificat, qui doit correspondre à la sonde. Si vous n'y arrivez toujours pas, retournez au Keyvault et autorisez temporairement les services de Microsoft d'y accéder.



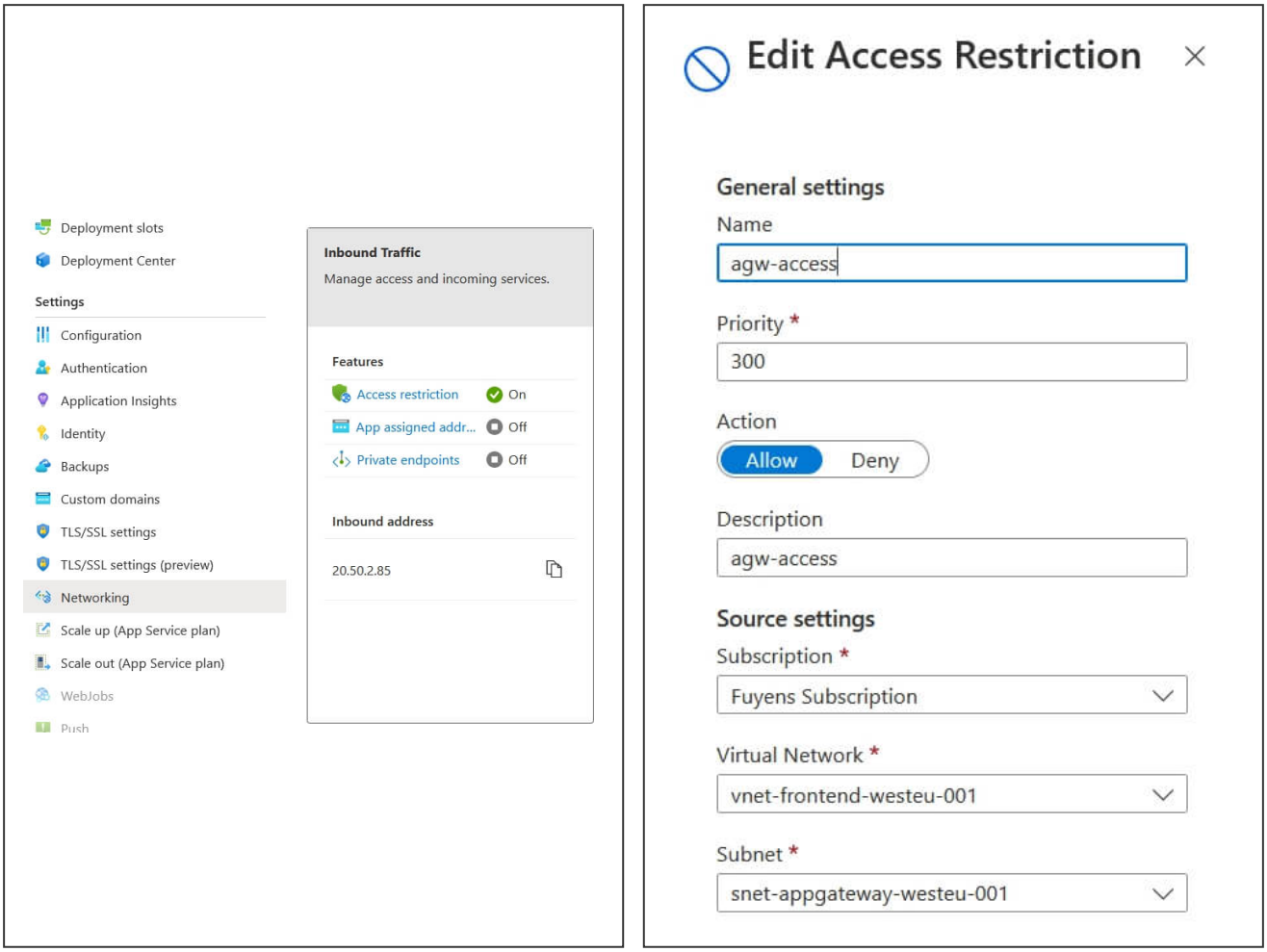
L'exception de sécurité devrait toujours être sur "No" quand on utilise un point de terminaison privé

- Testez une dernière fois la sonde en cliquant sur **"backend health"** et vérifiez que vous avez bien la coche verte.

Restriction d'accès à l'application.

Maintenant que l'infrastructure possède une **"application gateway"**, on peut fermer l'accès public à l'application.

- Retournez sur **"App services"**.
- Cliquez sur **"Networking"**.
- Cliquez sur **"Access restriction"**.
- Ajoutez une règle qui n'autorise que le sous-réseau de l'application gateway d'accéder à l'application.



La restriction d'accès au niveau de l'application

Conclusion

Voilà, cette longue publication est maintenant terminée. Elle valide toutes mes recherches et mes différents tests que j'ai entrepris afin de réaliser une infrastructure sécurisée autour d'une application qui utilise des services **"PaaS"** sur le cloud Azure de Microsoft. J'ai également couvert l'utilisation des containers avec Docker et l'utilisation des certificats SSL.