DOCUMENTATION / SUPPORT DE FORMATION

Table des matières

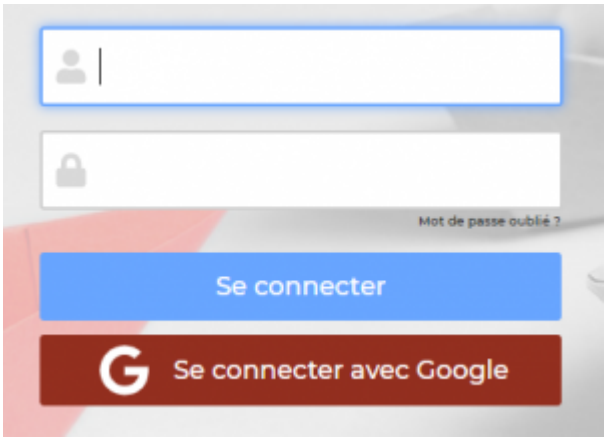
Authentifications externes

L'application vous permet d'utiliser un système externe pour l'authentification de vos utilisateurs.

Plusieurs modes d'authentification sont disponibles

- Authentification Google Apps
- Authentification Office 365 directe
- Authentification Azure Active Directory (fonctionne avec Office 365 enterprise)

Authentification Google Apps



https://image.noelshack.com/fichiers/2020/02/1/1578303860-2020-01-06-10-46-03-accueil-microsoft-azure.png

L'application vous permet d'utiliser Google Apps pour authentifier les utilisateurs. Cette méthode est possible uniquement si vous disposez d'un domain Google Apps pour gérer vos email d'entreprise.

Cette méthode permet à vos utilisateur de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Google via le protocole oauth 2.0.

Pour activer l'authentification Google Apps

1. Contacter le support Veryswing directement depuis l'application en demandant l'activation de ce mode d'authentification dans votre environnement.
2. Nous faisons ensuite l'activation pour vous et nous faisons le nécessaire auprès de Google
3. Une fois ce mode d'authentification activée, une image rouge “Se connecter avec Google” apparait sur l'écran de connexion
4. Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Google dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur

plusieurs utilisateurs en même temps.

Une fois l'authentification Google activée sur un utilisateur, il doit obligatoire cliquer sur le bouton “Se connecter avec Google” pour accéder à l'application. Il sera alors redirigé vers le site Google qui gère l'authentification puis redirigé vers l'application.

Authentification Azure Active Directory (Office 365 enterprise)

Si vous disposez d'un abonnement Azure avec Active Directory ou Office 365 enterprise, vous pouvez disposer d'une authentification sécurisée via Azure Active Directory.

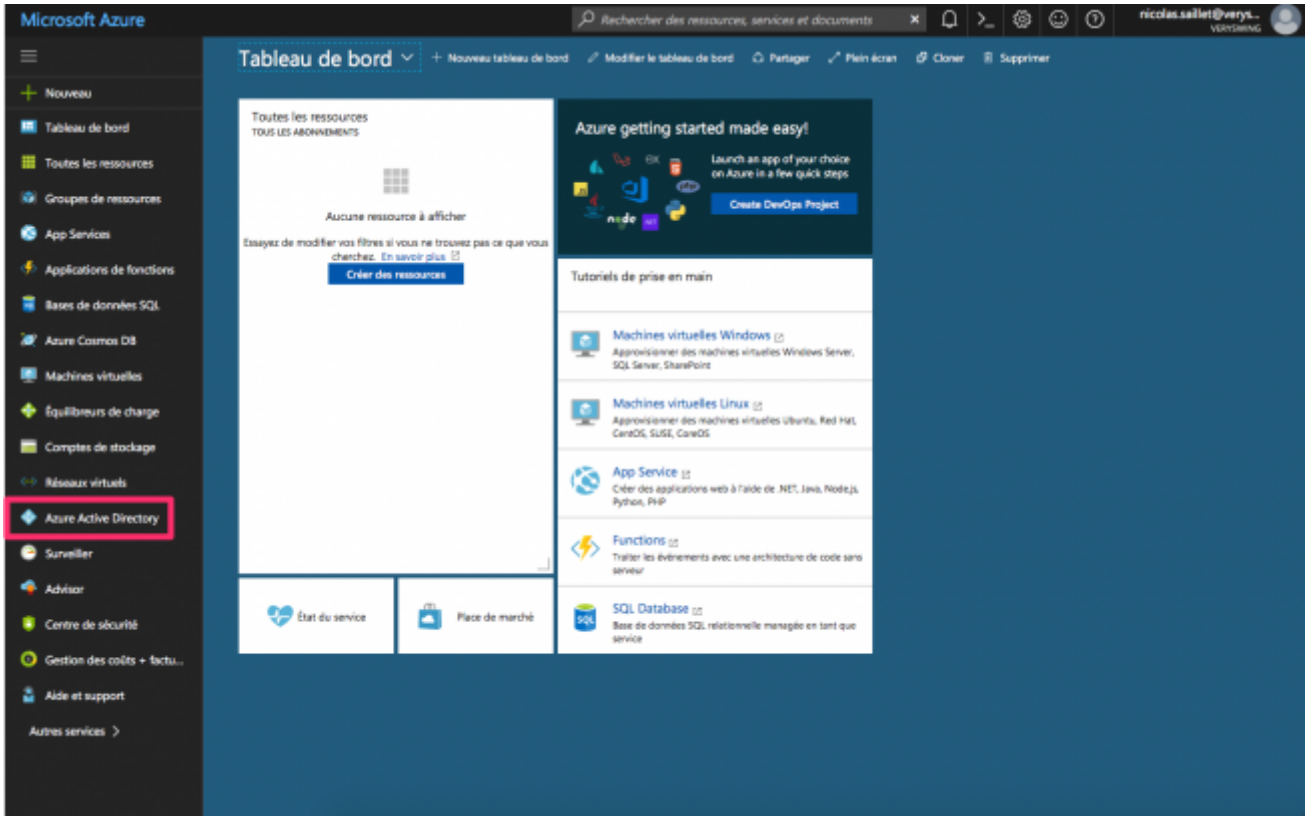
Cette méthode permet à vos utilisateurs de ne pas avoir à mémoriser ou gérer un autre identifiant et mot de passe pour l'accès à l'application.

L'authentification est intégralement gérée par Microsoft via le protocole oauth 2.0 sur la plateforme Azure.

Vous trouverez ci-dessous les différentes étapes pour activer ce mode d'authentification pour le portail Web et ensuite pour les applications mobiles.

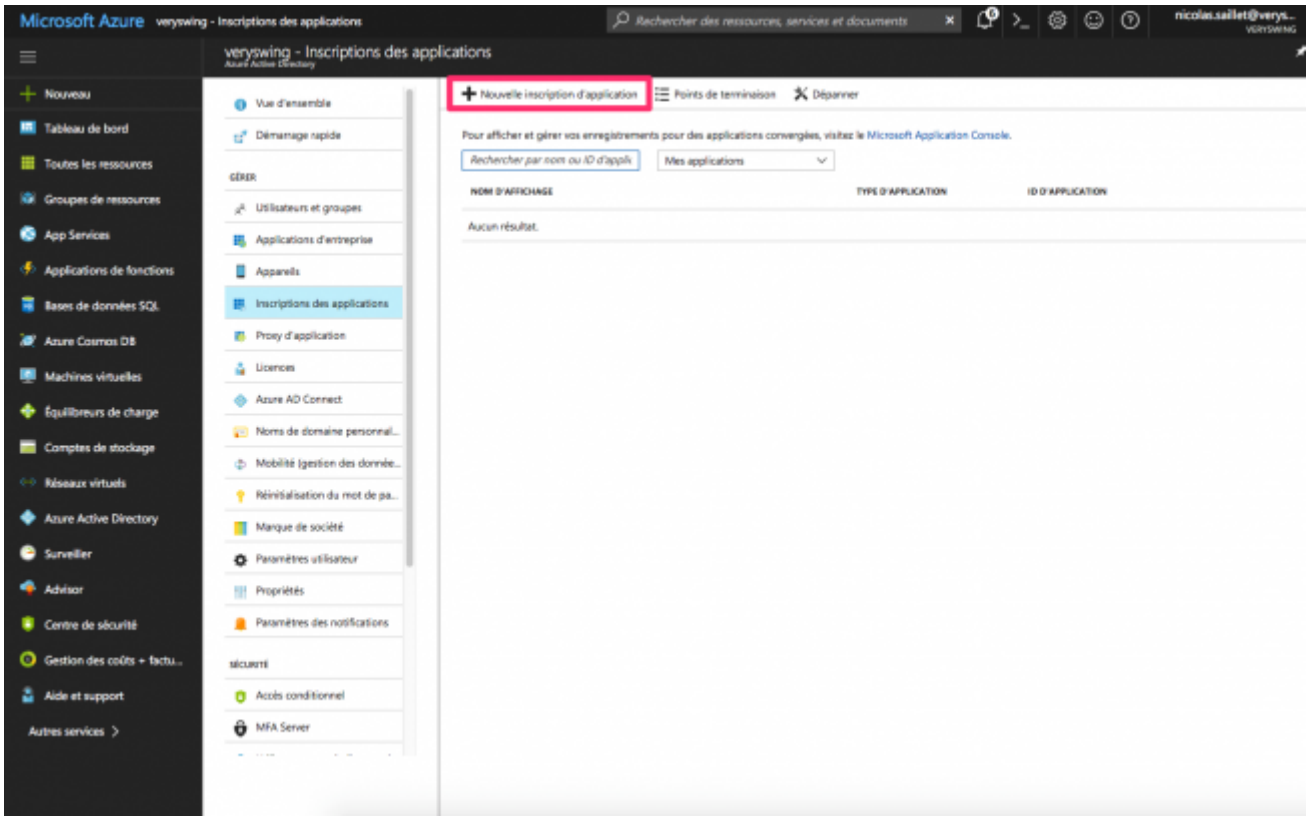
Authentification via le portail Web

Depuis la console Microsoft Azure

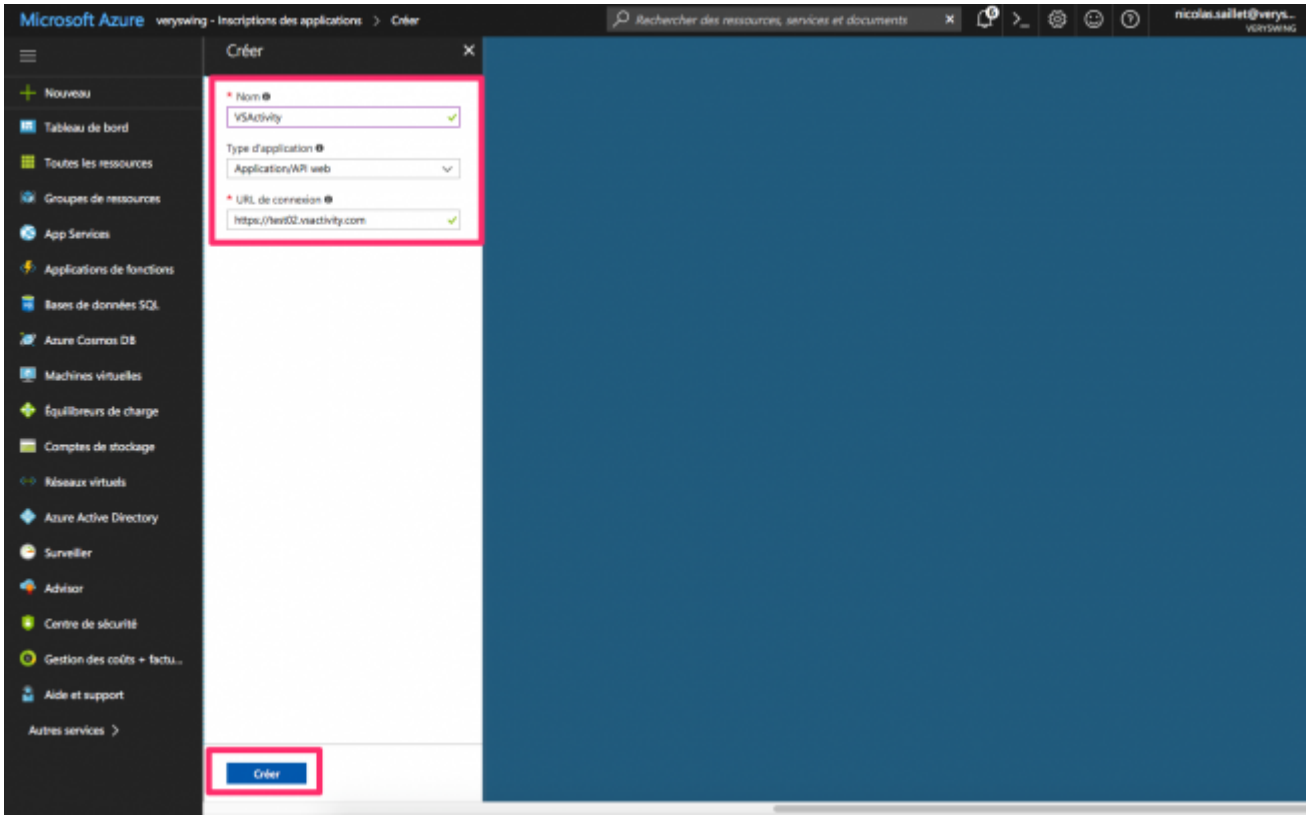


Depuis votre console Azure, cliquez sur Azure Active Directory dans les items à gauche.

Cliquez ensuite sur l'onglet Inscriptions des applications.



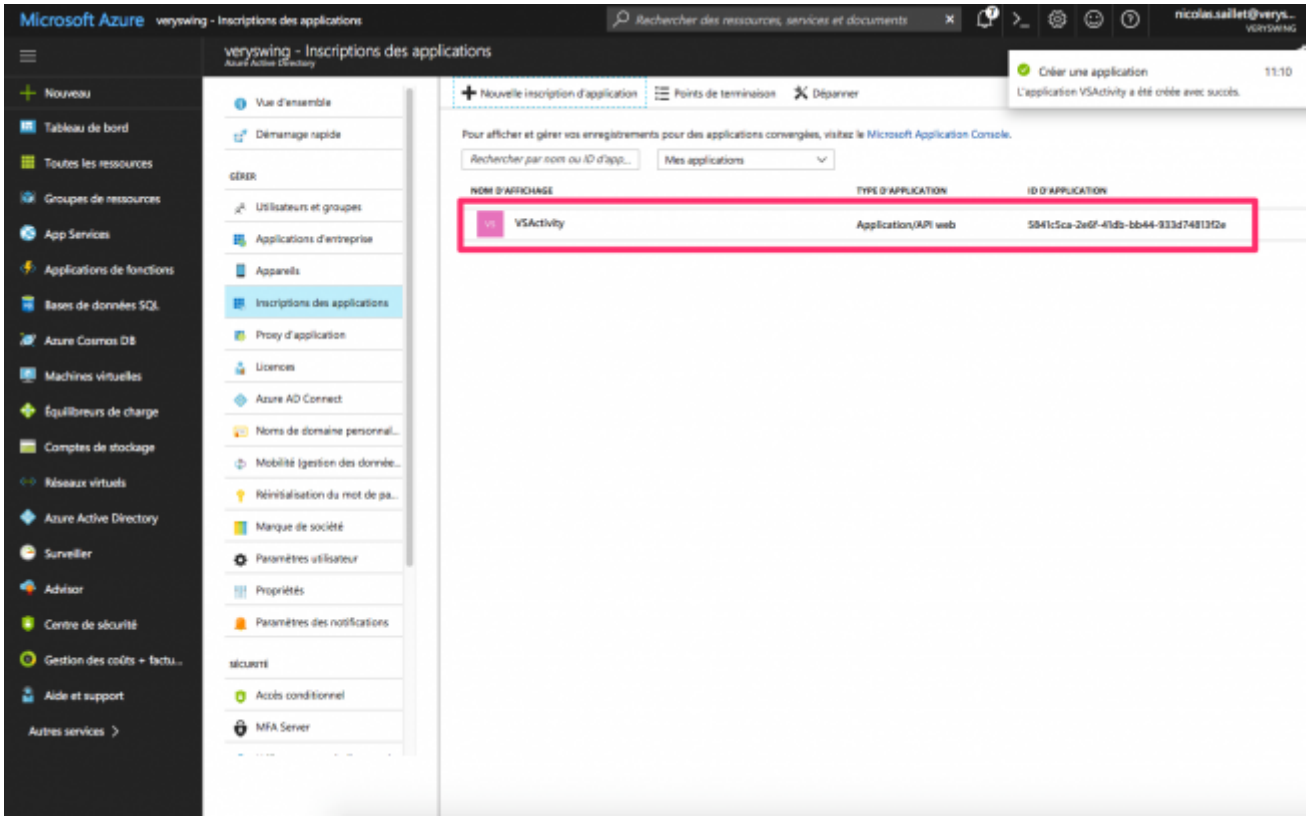
Cliquez sur + Nouvelle Inscription d'application en haut de l'interface pour ajouter une application à votre tenant Azure AD.



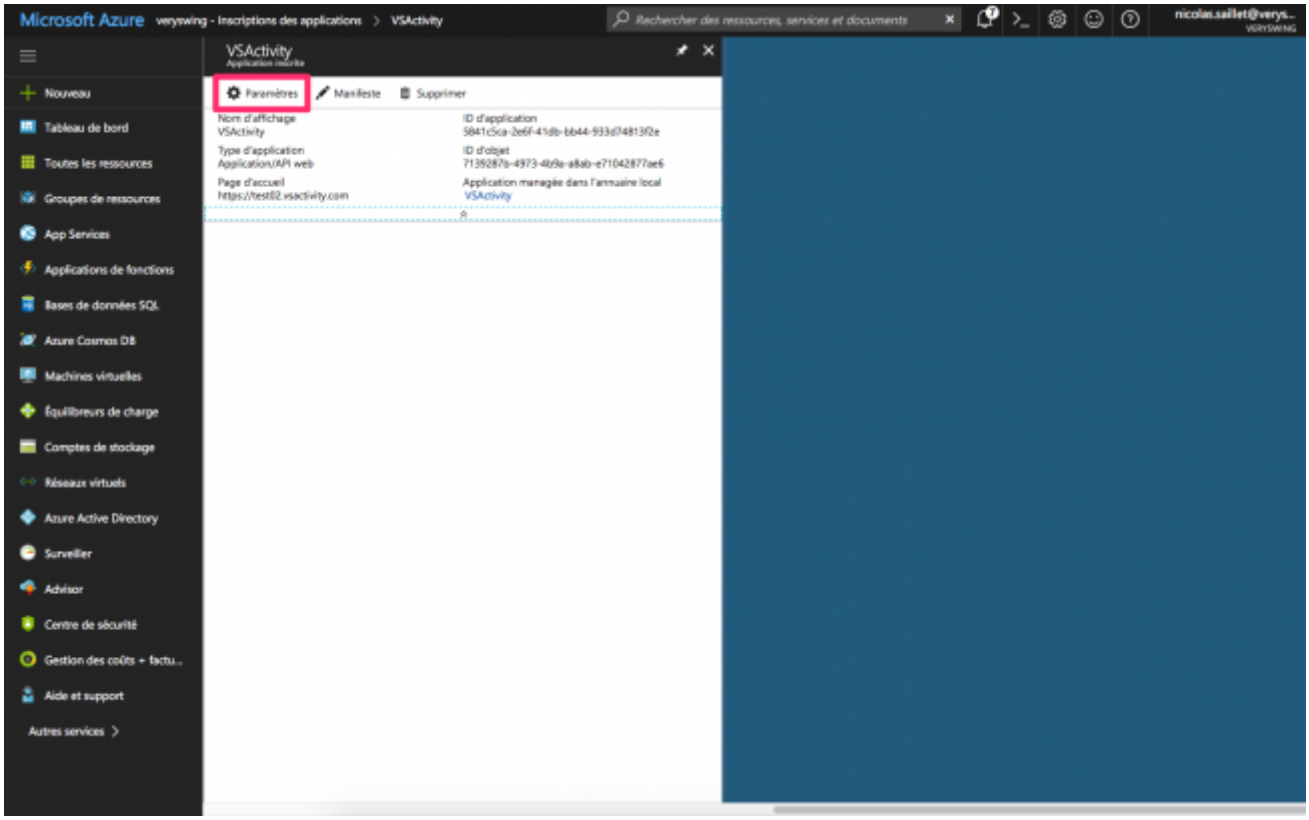
Remplissez les informations demandées

- Nom : VSActivity ou VSPortage
- Type d'application : Application/API Web
- URL de connexion : https://ENTREPRISE.vsactivity.com

Remplacez ENTREPRISE par le préfixe de l'url d'accès à votre environnement.

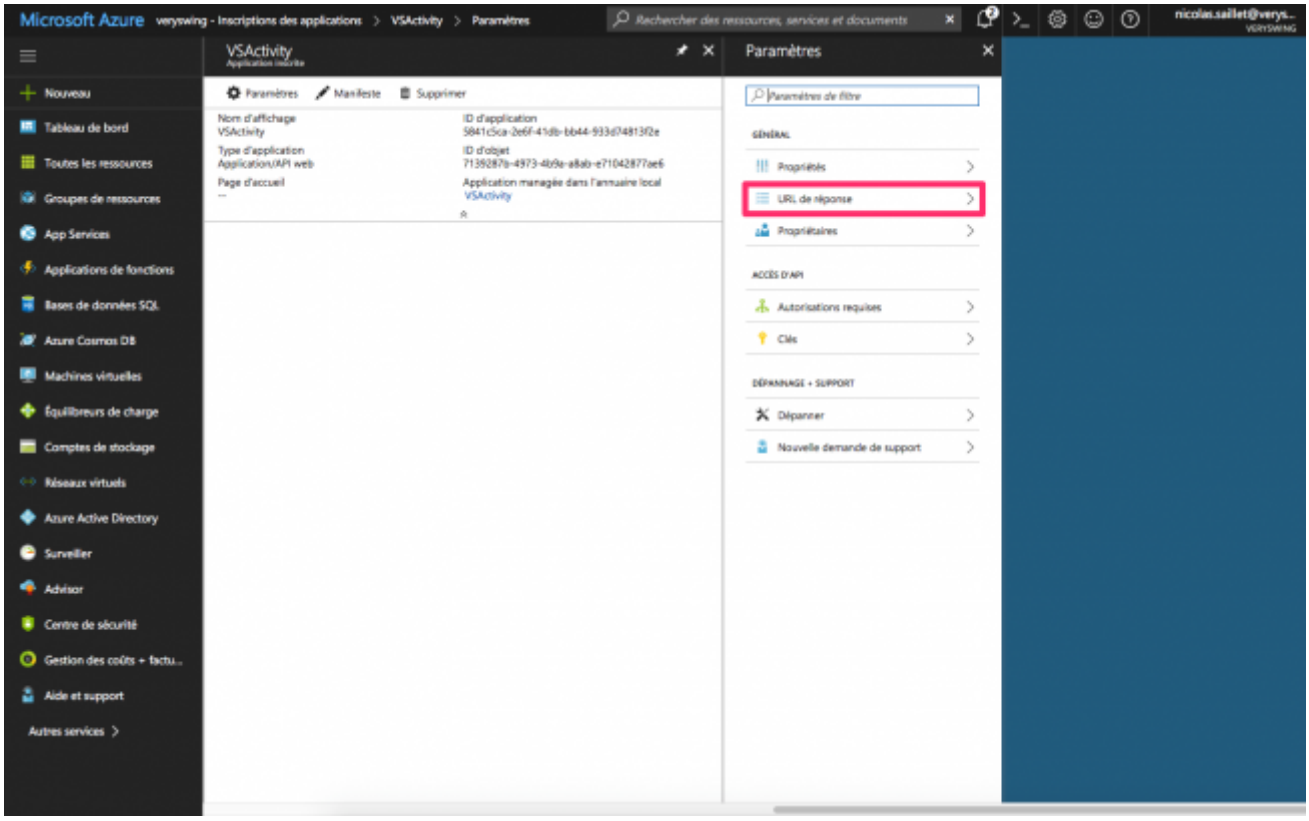


Une fois l'application créée, cliquez sur la ligne de l'application nouvelle créée.

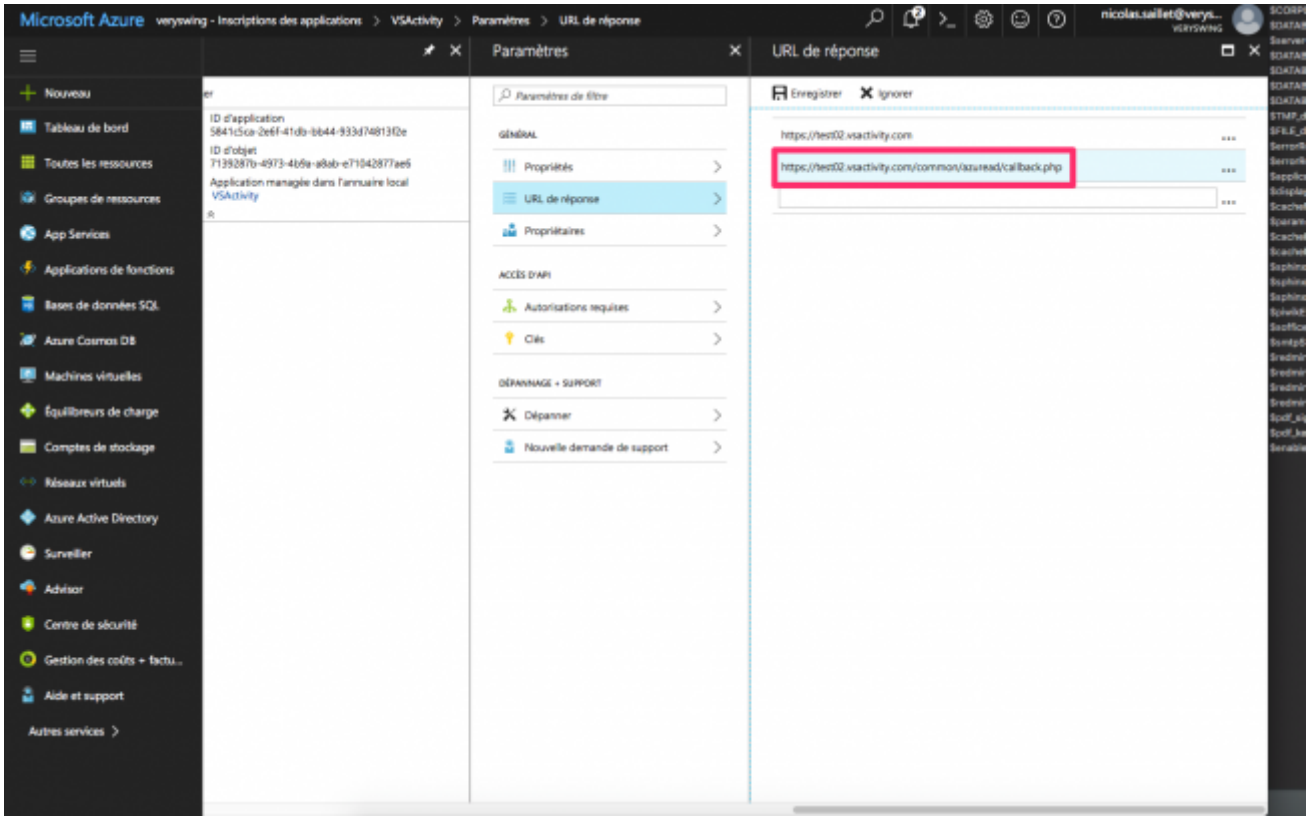


A ce stade, vous pouvez conserver l'ID de l'application qui apparait. Il sera nécessaire de nous le transmettre une fois l'application créée et totalement paramètrée.

Une fois le panneau de l'application ouvert, cliquez sur Paramètres en haut à coté de la roue dentée.

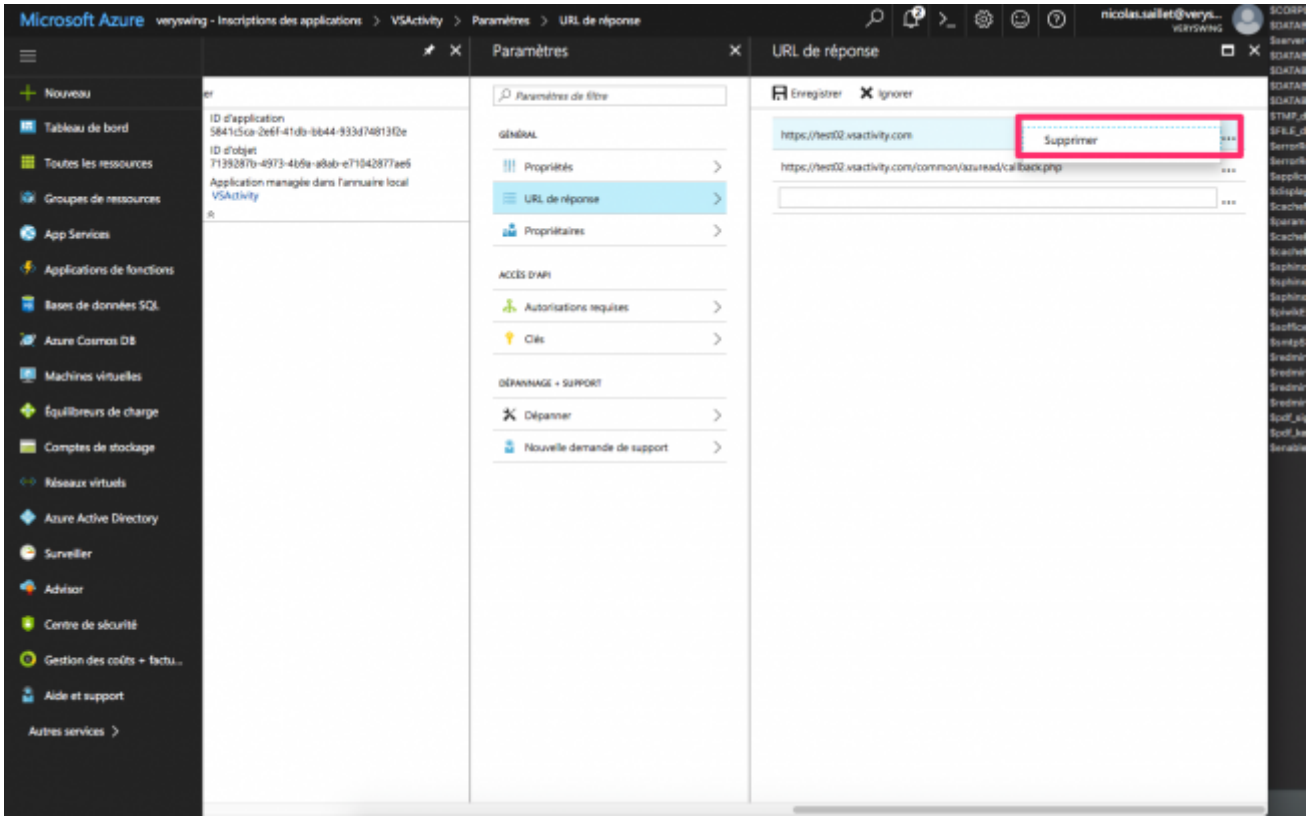


Cliquez sur URL de réponse dans le panneau de droite.

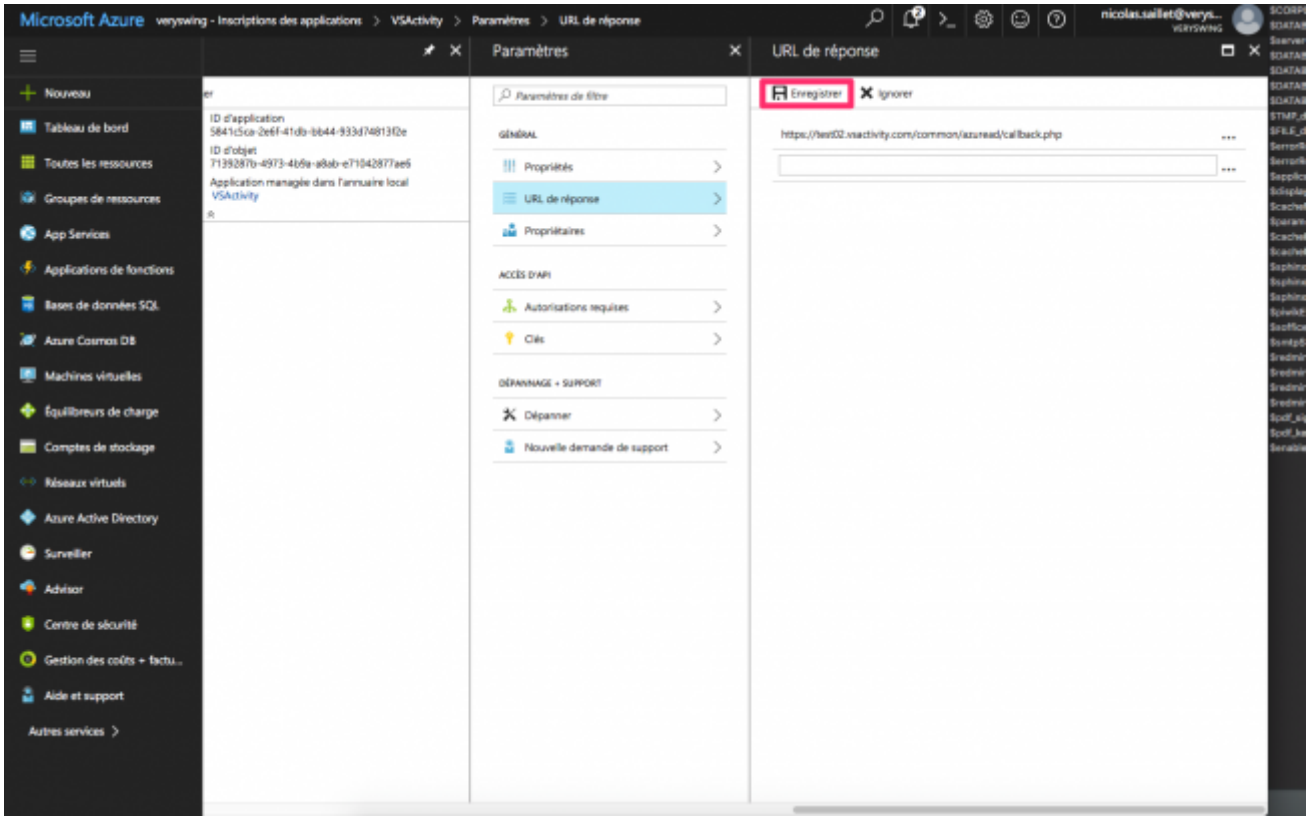


Saisissez l'url de réponse : https://ENTREPRISE.vsactivity.com/common/azuread/callback.php

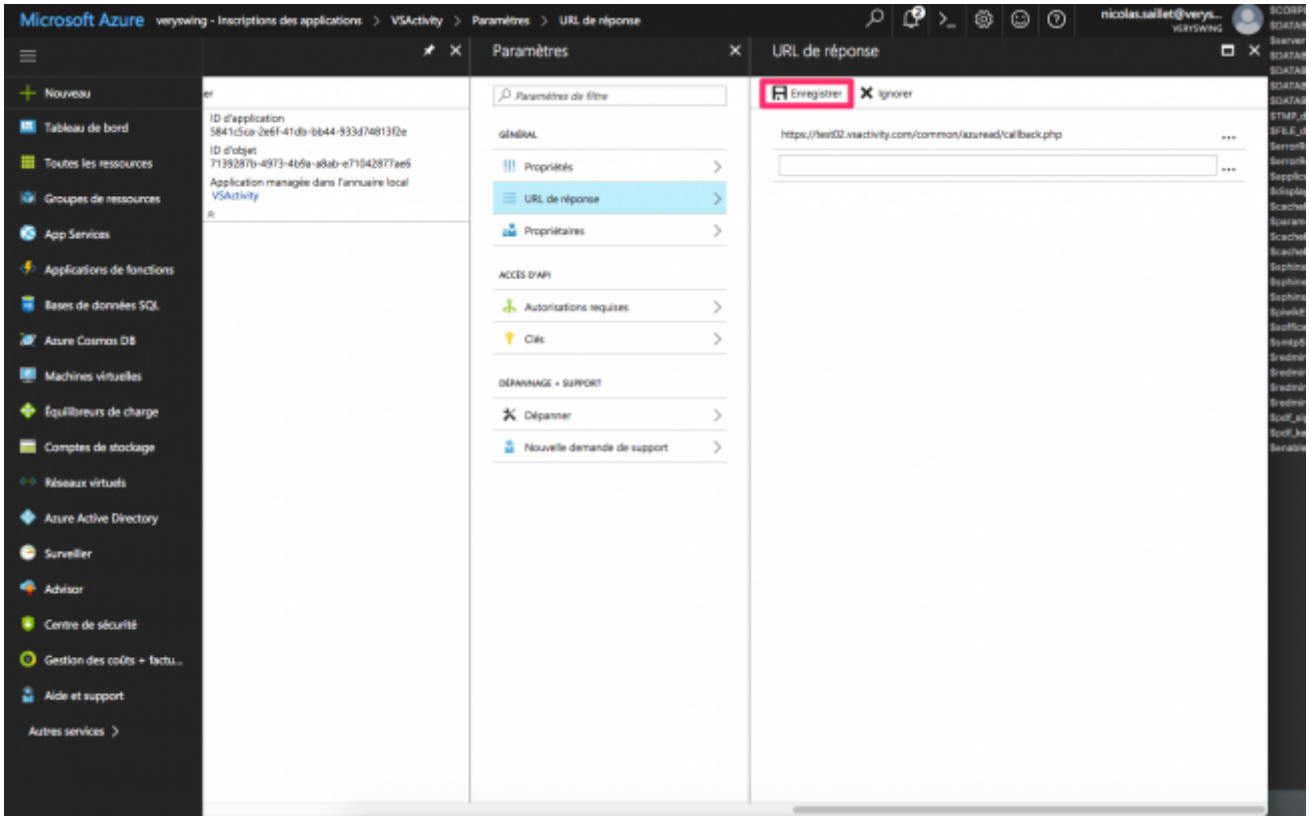
Remplacez ENTREPRISE par le préfixe de l'url d'accès à votre environnement.



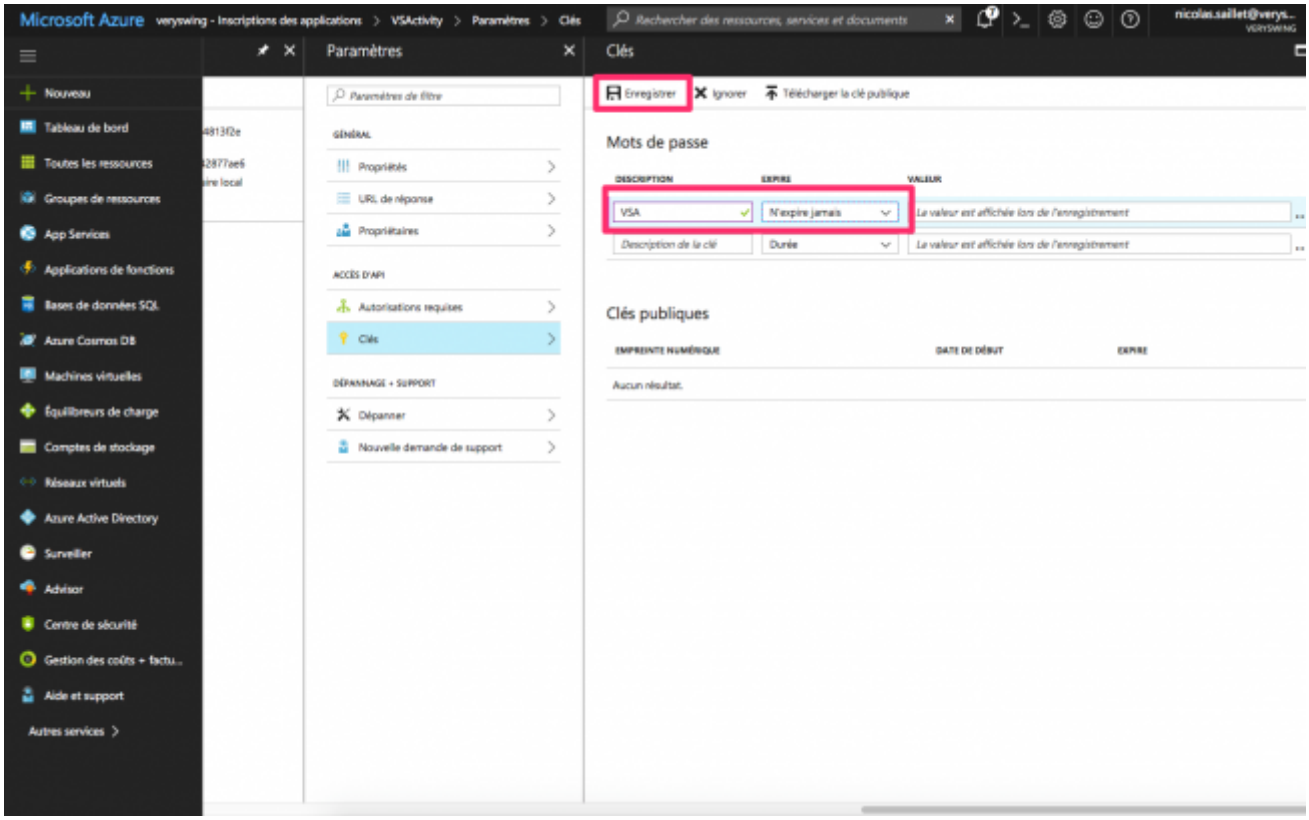
Supprimez l'entrée créée automatiquement avec l'url https://ENTREPRISE.vsactivity.com



Cliquez sur Enregistrer.

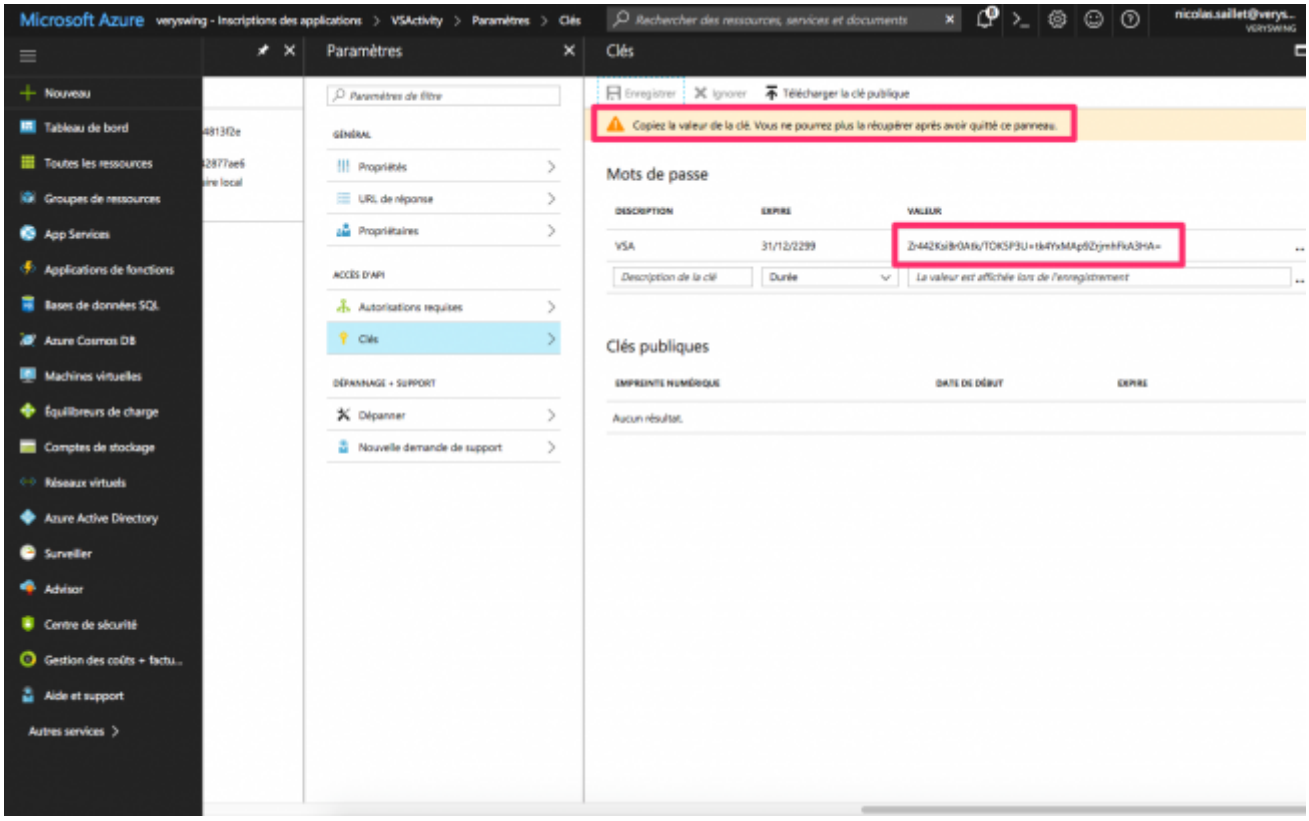


Cliquez sur Clé.



Créez une nouvelle clé. Indiquez comme description VSA ou VSP. Choisissez N'expire jamais dans la colonne EXPIRE.

Cliquez sur Enregistrer.

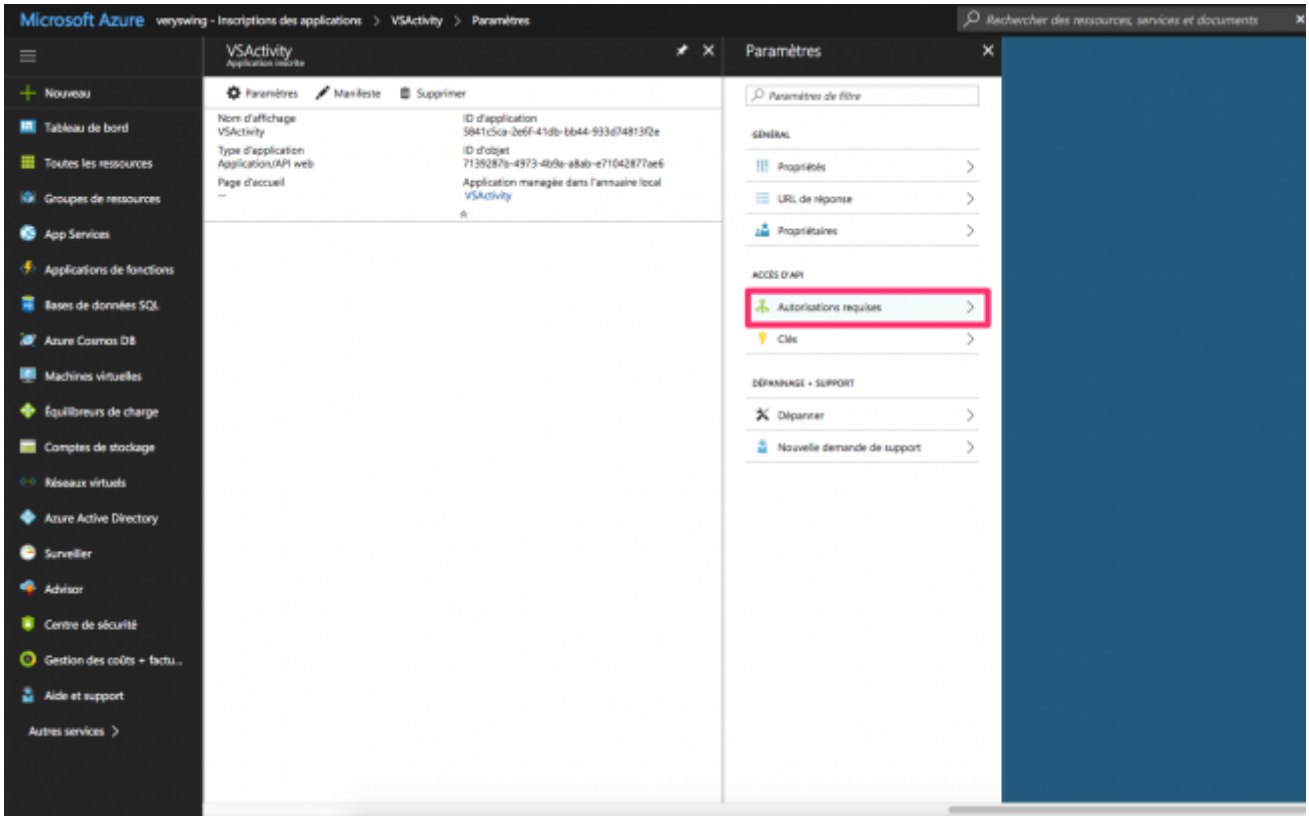


Attention la clé sera générée à l'enregistrement et n'apparaitra qu'une seule fois. Il sera nécessaire de la sauvegarder pour nous la communiquer. Il sera ensuite impossible de la voir à nouveau.

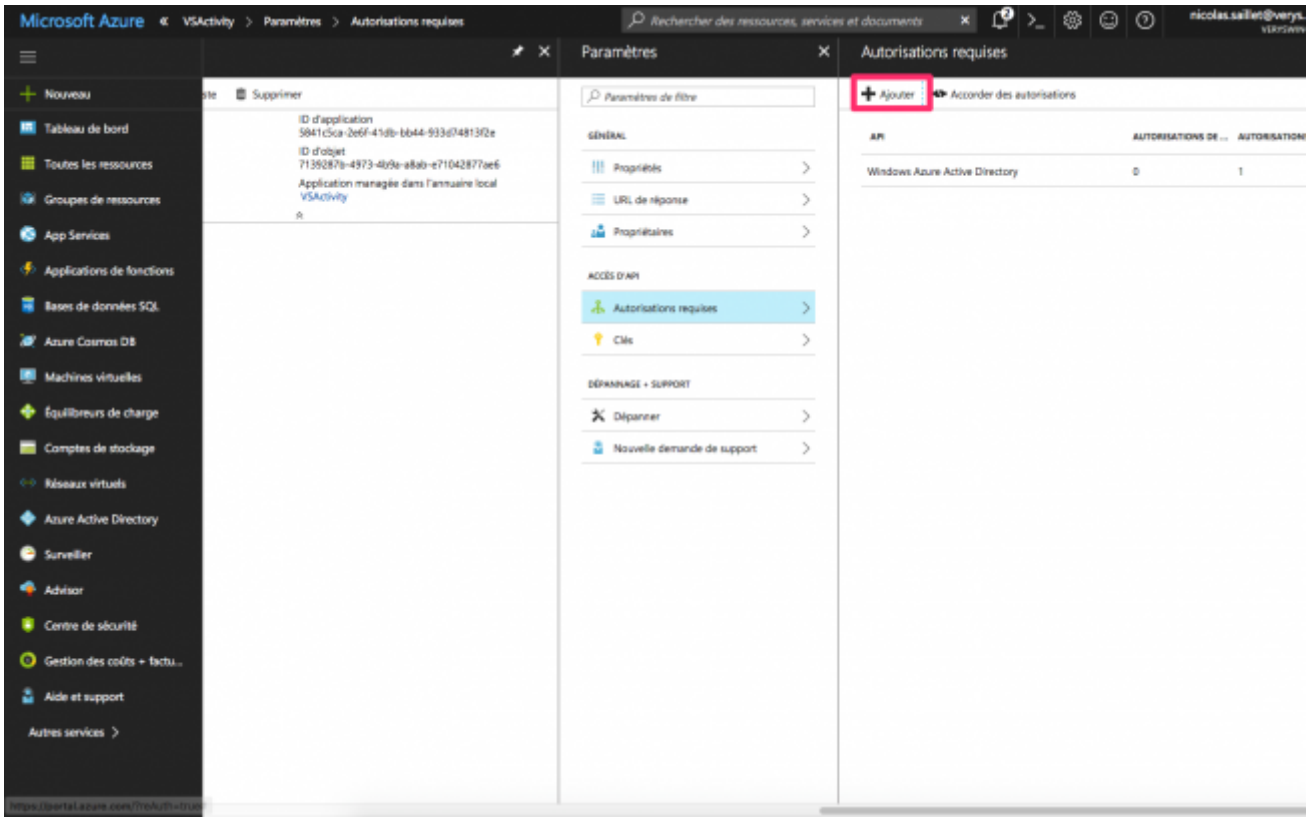
Si vous avez raté la clé, vous pouvez en générer une nouvelle et supprimer l'ancienne.

La sécurité et les autorisations d'accès

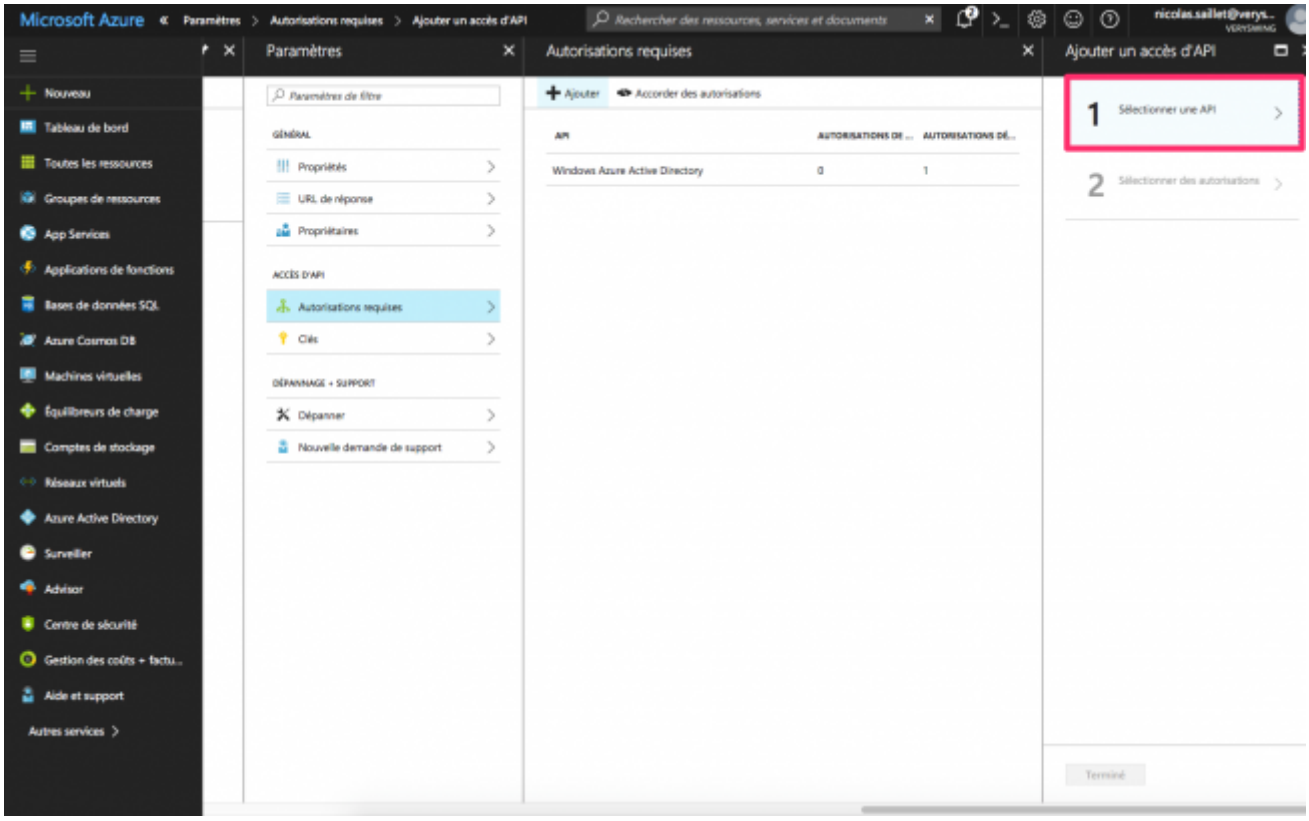
Une fois l'application créée, il est nécessaire d'ajouter des autorisations pour que vos utilisateurs puissent se connecter à l'application depuis votre tenant Azure AD.



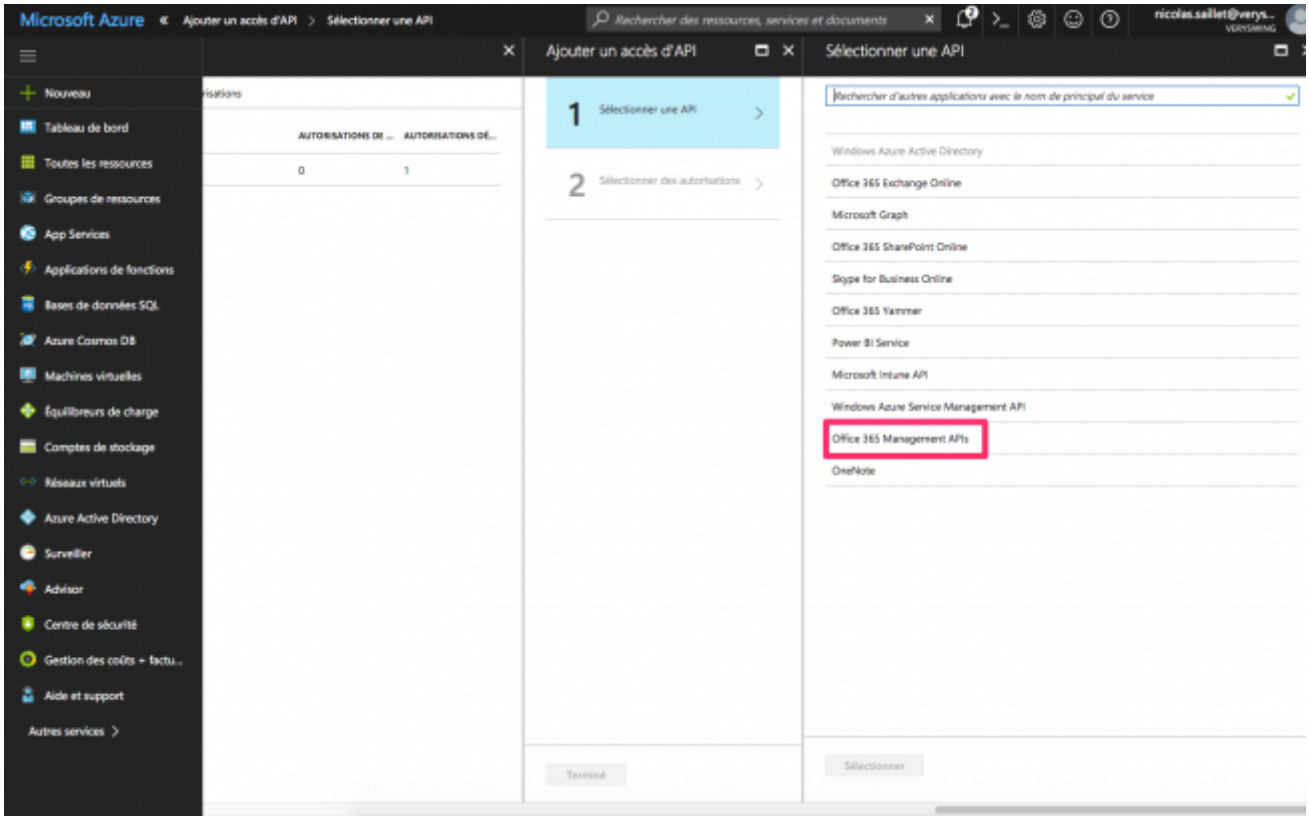
Cliquez sur Autorisation requises, depuis le panneau de configuration de l'application dans votre console Azure AD.



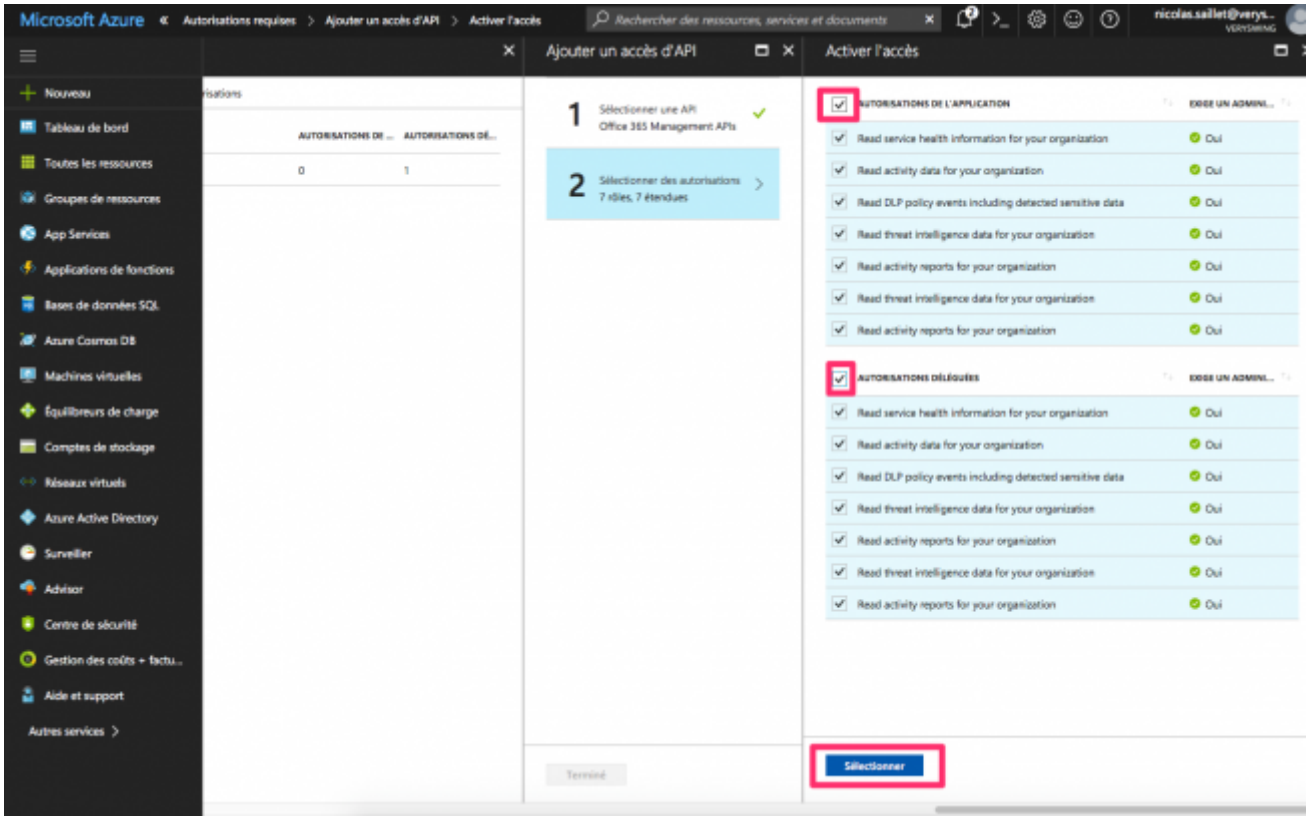
Cliquez sur + Ajouter.



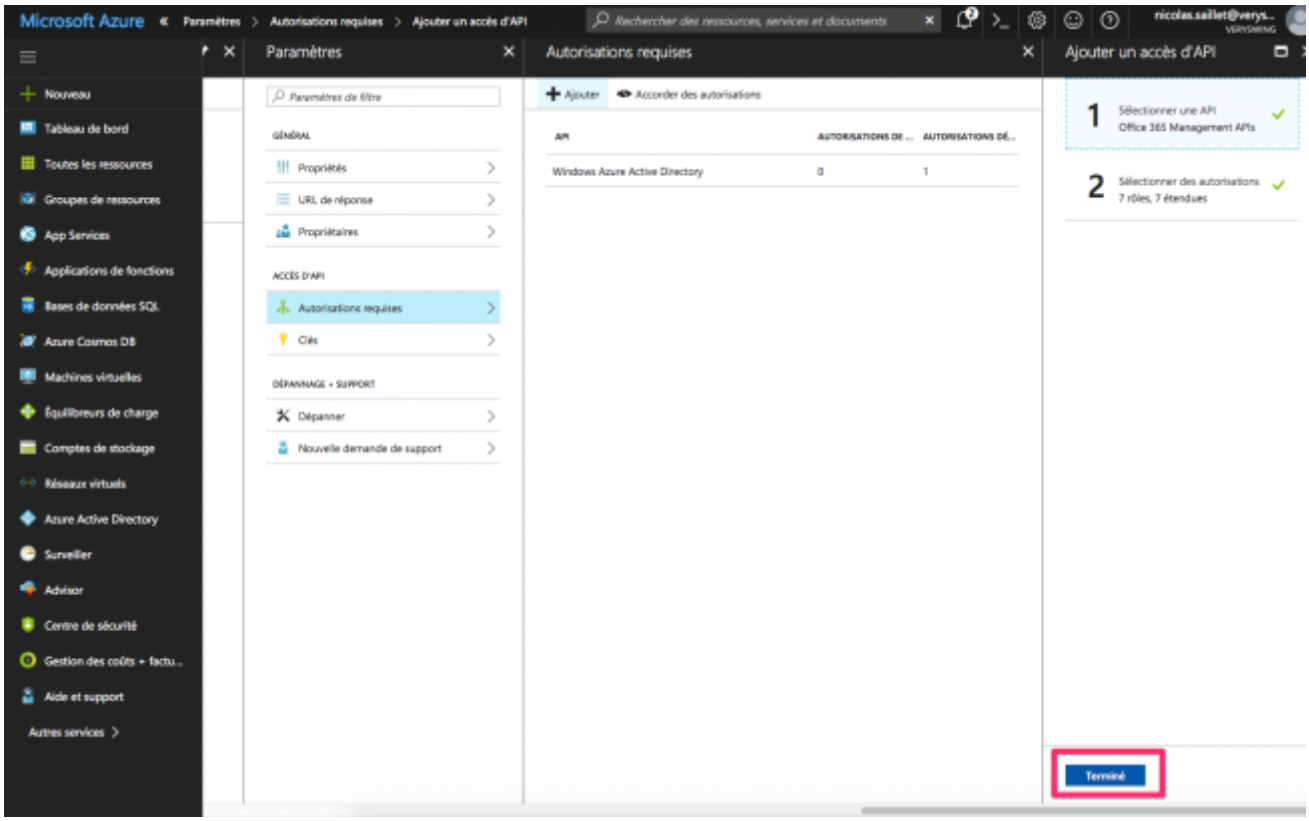
Cliquez sur 1 Sélectionnez une API.



Cliquez sur Office 365 Management Apis.



Cliquez sur Autorisations de l'application et Autorisations déléguées pour donner l'accès en lecture. Puis cliquez sur Sélectionner en bas.



Cliquez sur Terminé.

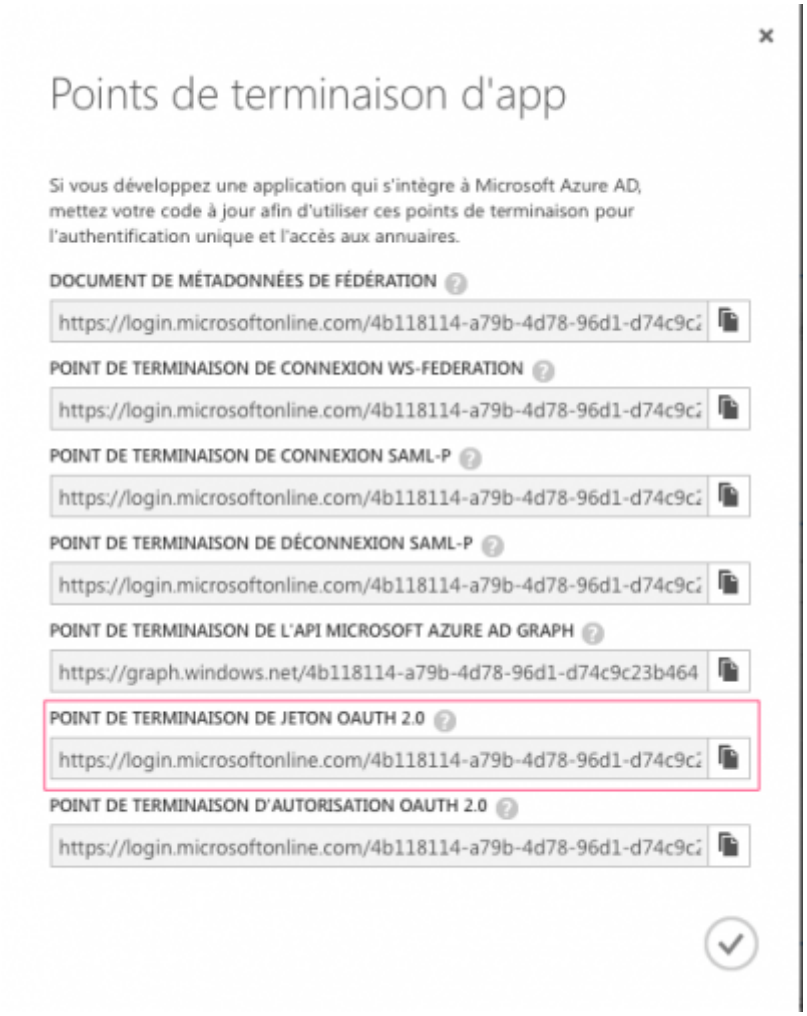
Répétez l'opération 2 fois pour ajouter les APIs “**Windows Azure Service Management API**” et

“**Windows Azure Active Directory**”

Les informations à nous communiquer

Une fois l'application ajoutée dans votre console Azure, il est nécessaire de nous communiquer :

- L'id de l'application disponible dans le panneau de l'application en cliquant sur Priopriétés
- La clé secrète que vous avez générée
- Le tenant ID, le point de terminaison de jeton oauth 2.0, il est disponible en cliquant sur **POINT DE TERMINAISON** en base de l'interface quand vous êtes dans l'onglet CONFIGURER de l'application

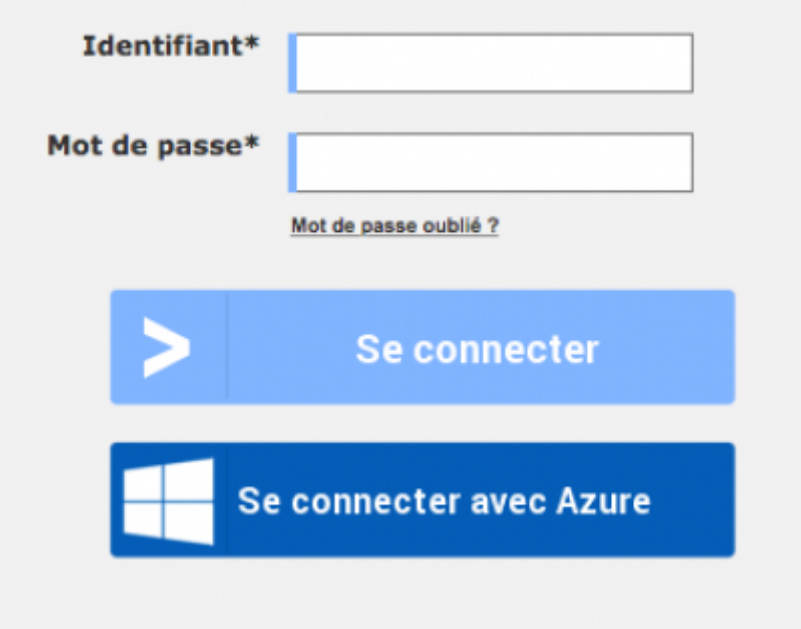


Une fois que le mode d'authentification Azure AD est activé

Il est nécessaire de changer le mode d'authentification de vos utilisateurs depuis l'écran Administration > Utilisateur

Dans le formulaire, vous devez choisir explicitement le mode d'authentification Azure Active Directory dans le formulaire de gestion de l'utilisateur. Il existe également une action de masse pour le faire sur plusieurs utilisateurs en même temps.

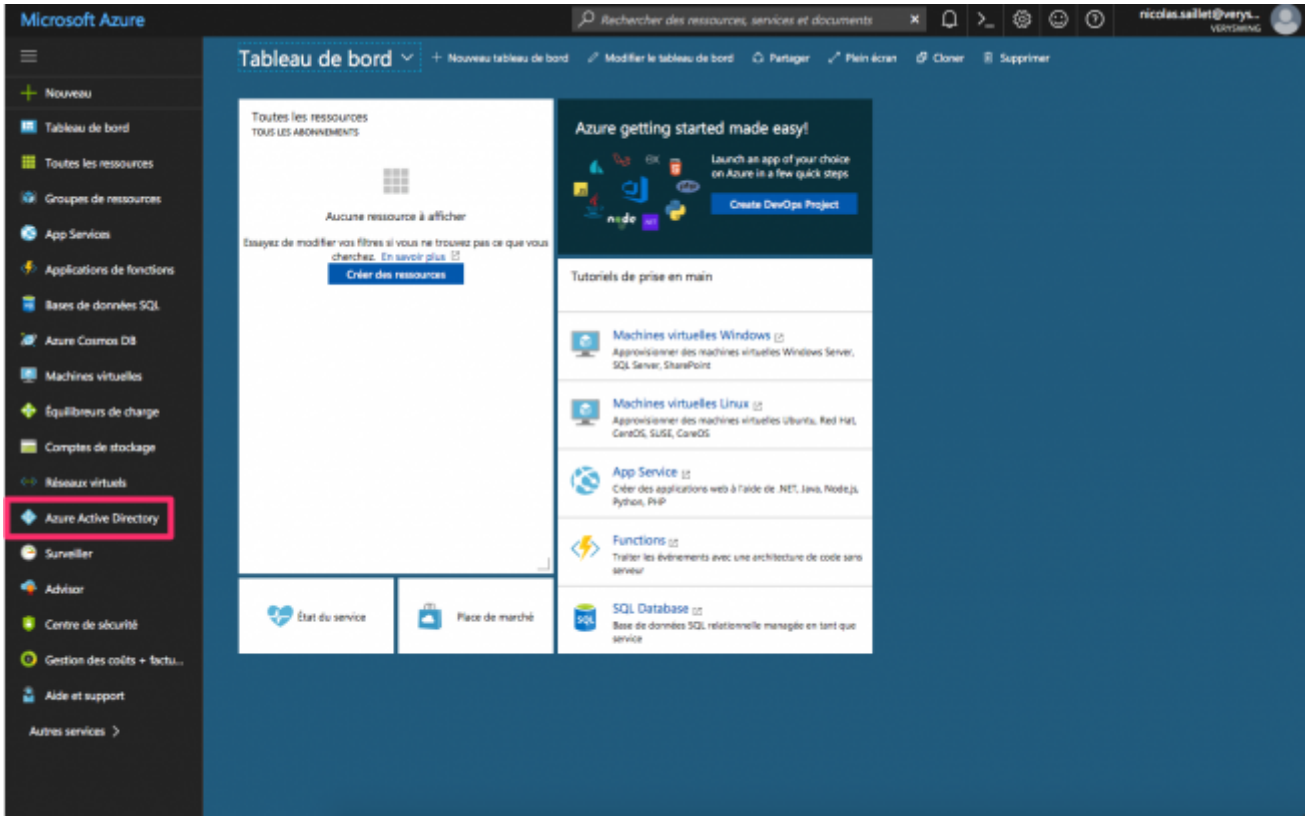
Une fois l'authentification Azure Active Directory activée sur un utilisateur, il doit obligatoirement cliquer sur le bouton “Se connecter avec Azure” pour accéder à l'application. Il sera alors redirigé vers le site Microsoft qui gère l'authentification puis redirigé vers l'application.



Authentification via les applications mobile

Avant d'activer l'authentification Azure Active Directory pour les applications mobiles VSActivity, il est essentiel d'avoir tout d'abord activer l'authentification pour l'interface Web.

Depuis la console Azure Management



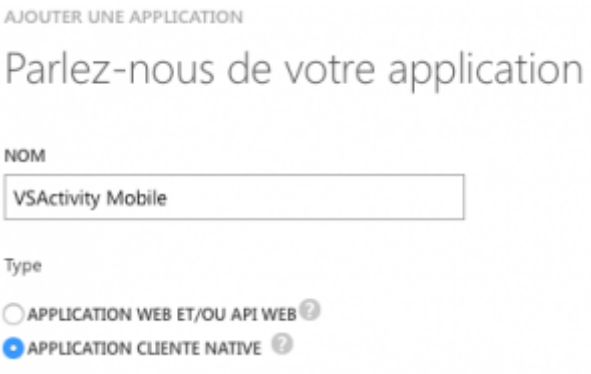
Depuis votre console Azure, cliquez sur ACTIVE DIRECTORY dans les items à gauche.

Une fois dans la zone active directory, cliquez sur le tenant **où vous avez ajouter l'authentification Azure Active Directory pour la partie Web**.

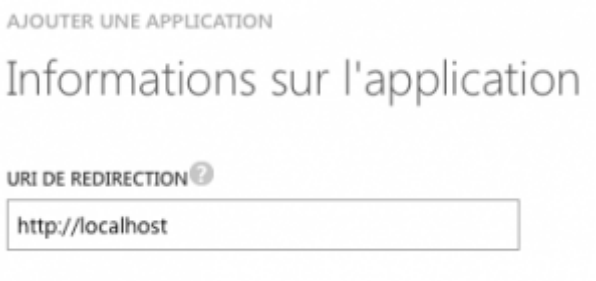
Cliquez ensuite sur l'onglet APPLICATIONS.

Cliquez sur AJOUTER+ en bas de l'interface pour ajouter une application à votre tenant Azure AD. Choisir “Ajouter une application développée par mon organisation”.

Indiquez le nom de l'application, VSActivity Mobile. Cocher la case “APPLICATION CLIENTE NATIVE”.

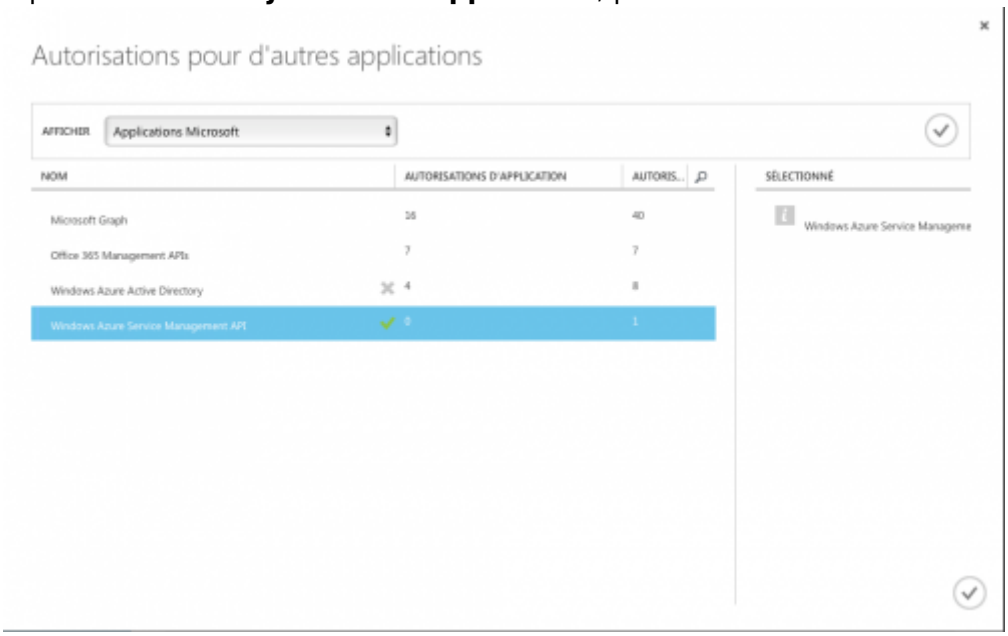


Indiquez l'url suivant dans le formulaire : http://localhost



Une fois l'application créée, cliquez sur l'onglet CONFIGURER.

Cliquez ensuite sur **Ajouter une application**, puis cochez Windows Azure Services Management API



:

Cliquez ensuite ENREGISTRER en bas de l'interface. Le console va travailler quelques secondes.

Les informations à nous communiquer

Une fois l'application ajoutée dans votre console Azure, il est nécessaire de nous communiquer :

- L'id de l'application disponible dans l'onglet CONFIGURER **ID CLIENT**

Une fois que le mode d'authentification Azure AD est activé

Une fois activé, tous les utilisateurs ayant le mode d'authentification “Azure Active Directory” pourront s'authentifier avec leurs comptes Microsoft Azure Active Directory sur nos applications mobiles. L'utilisateur devra obligatoirement cliquer sur le bouton “Se connecter avec Azure” pour accéder à l'application. Il sera alors redirigé vers le site Microsoft qui gère l'authentification puis redirigé vers l'application.