

Intégration sélective EntraID / PREVIST via Azure Functions

Table des matières

1. Objectif & principe de sécurité « moindre privilège »	2
2. Données exposées à Okta	3
3. Pré-Requis.....	5
4. Abonnement Azure	6
5. Application Microsoft Graph	8
6. Création de l'Application de Fonction (Windows)	10
7. Paramètres & variables d'environnement	11
8. Import de la Fonction Node.js (zip)	12
9. Intégration PREVIST (et test appel HTTP trigger)	13
10. (Optionnel) Filtrage IP : Restriction d'accès.....	14
11. (Optionnel) Monitoring.....	16
12. (Optionnel) Gestion & renouvellement du secret Graph	18
13. Annexes.....	25

1. Objectif & principe de sécurité « moindre privilège »

Risque initial :

Pour l'intégration des comptes EntraID dans PREVIST (IAM Okta), Microsoft Graph ne permet pas de limiter finement la portée des autorisations de lecture (« User.Read.All » et « Group.Read.All » donnent accès à tout le tenant). *L'établissement doit rester maître des données présentées.*

Solution :

Une fonction HTTPS (publiée sur Azure Functions) lit MgGraph en interne de façon contrôlée (groupe cible) et expose seulement les comptes désirés à Okta par le biais d'une variable (groupe de sécurité) paramétrable par l'établissement, avec authentification par clé et filtrage IP côté Application de Fonction.

Différentes variables sont paramétrables en interface graphique par l'établissement (secret, groupe à partager, paramètres à exposer).

Vue d'ensemble :

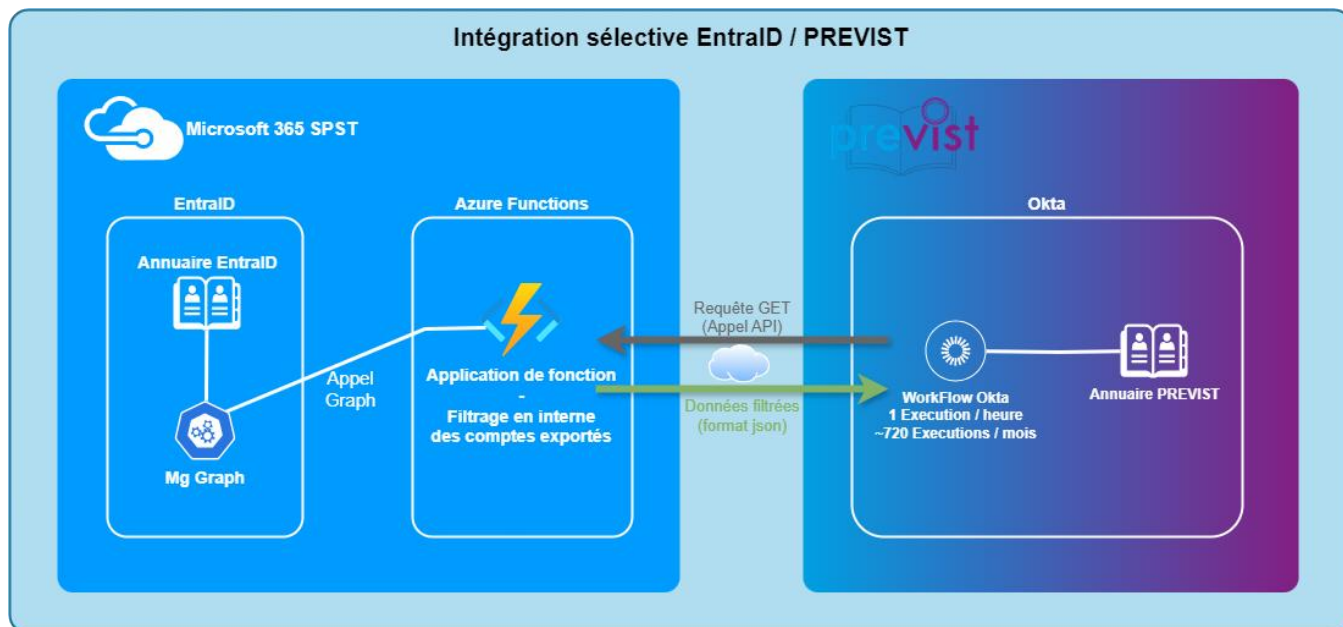
L'Application de Fonction appelle Microsoft Graph en interne sur un groupe racine défini, explore les sous-groupes, concatène les utilisateurs, et retourne un payload JSON strict.

PREVIST vient consommer l'Endpoint HTTPS (auth niveau fonction, clé secrète paramétrable requise) et intègre les utilisateurs via des Workflows. Possibilité de limiter l'accès à la fonction par filtrage IP.

Bénéfices :

L'établissement conserve la main (paramétrage, activation/blocage, scope fonctionnel) sans exposer l'ensemble du tenant à PREVIST.

L'application de fonction Azure exclut le maintien d'un environnement serveur.



2. Données exposées à Okta

L'application exposera le groupe racine paramétré par l'établissement en variable d'environnement. Il affichera en sortie les comptes présents dans ce groupe (N0), rangés par sous-groupe (N1).

Les comptes présents dans le N0 accéderont à PREVIST (SSO Okta), les comptes présents dans le sous-groupe N1 accéderont aux applications avec les accès liés à ce groupe.

Nb : Pour les accès Curebot, retrouver la matrice des groupes dans l'annexe [Annexe Matrice Metiers Curebot.pdf](#).

Nb2 : Les groupes modernes « Microsoft 365 » ne peuvent être imbriqués, il est nécessaire d'utiliser des groupes de sécurité.

Les comptes présents dans les sous-groupes (N2/3/4/etc...) seront affichés en sortie dans le sous-groupe N1. Les noms de groupes N1/2/3/4/etc... ne seront pas affichés. Une sécurité est en place pour éviter les boucles infinies.

Les paramètres exportés par défaut (non paramétrables) sont : id, userPrincipalName, surname, givenName.

Il s'agit des paramètres nécessaires au cycle de vie du compte dans l'IAM.

- ID : permet de prendre en compte en cas de renommage du compte.
- UPN : login PREVIST (nécessaire pour le SSO).
- Nom et Prénom : pour la complétion des templates.

D'autres attributs à exporter peuvent être paramétrés par l'établissement dans une variable d'environnement au besoin (attributs MgGraph).

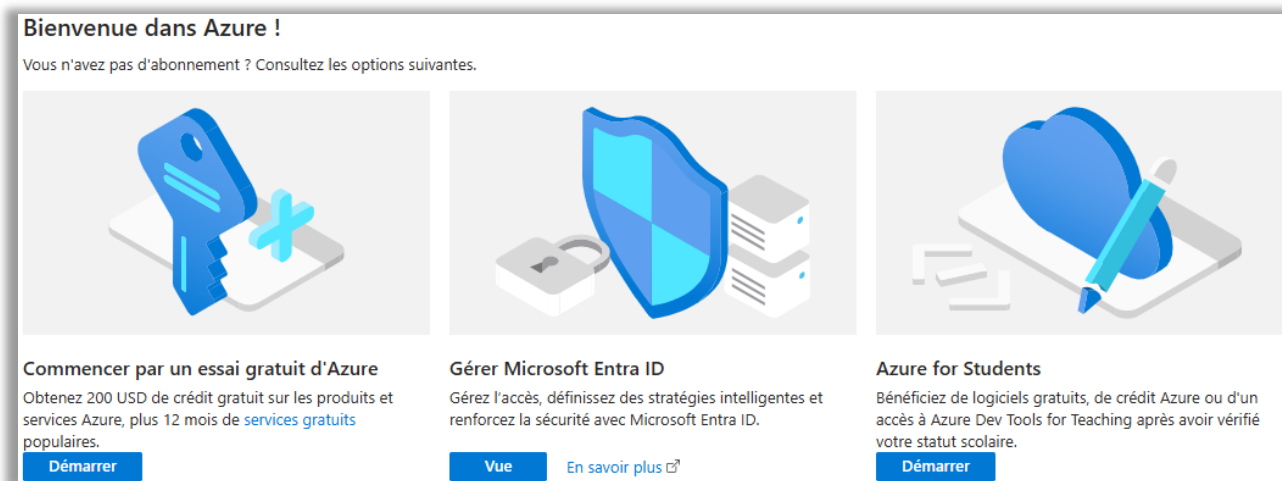
Exemple de sortie :

```
{
  "success": true,
  "groupName": "GRP_PREVIST",
  "groupId": "*****_****_****_****_*****",
  "count": 3,
  "users": [
    {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test6@previst.fr", "surname": "TEST6", "givenName": "Utilisateur"}
  ],
  "groups": [
    {
      "@odata.type": "#microsoft.graph.group",
      "displayName": "GRP_PREVIST_Curebot_Medecin",
      "userPrincipalName": null,
      "users": [
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test4@previst.fr", "surname": "TEST4", "givenName": "Utilisateur"},
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test1@previst.fr", "surname": "TEST1", "givenName": "Utilisateur"}
      ]
    },
    {
      "@odata.type": "#microsoft.graph.group",
      "displayName": "GRP_PREVIST_Curebot_Infirmier",
      "userPrincipalName": null,
      "users": [
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test5@previst.fr", "surname": "TEST5", "givenName": "Utilisateur"},
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test2@previst.fr", "surname": "TEST2", "givenName": "Utilisateur"}
      ]
    },
    {
      "@odata.type": "#microsoft.graph.group",
      "displayName": "GRP_PREVIST_Curebot_Qualite",
      "userPrincipalName": null,
      "users": [
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test10@previst.fr", "surname": "TEST10", "givenName": "Utilisateur"},
        {"@odata.type": "#microsoft.graph.user", "id": "*****_****_****_****_*****", "userPrincipalName":
"utilisateur.test2@previst.fr", "surname": "TEST2", "givenName": "Utilisateur"}
      ]
    }
  ]
}
```

3. Pré-Requis

→ Abonnement Azure

Pour vérifier s'il existe un abonnement en cours, se rendre sur portal.azure.com, si l'encart ci-dessous s'affiche, alors il n'existe pas d'abonnement en cours lié au compte utilisé et il ne sera pas possible de créer d'application sur le portail Azure :



Bienvenue dans Azure !
Vous n'avez pas d'abonnement ? Consultez les options suivantes.

- Commencer par un essai gratuit d'Azure**
Obtenez 200 USD de crédit gratuit sur les produits et services Azure, plus 12 mois de [services gratuits](#) populaires.
[Démarrer](#)
- Gérer Microsoft Entra ID**
Gérez l'accès, définissez des stratégies intelligentes et renforcez la sécurité avec Microsoft Entra ID.
[Vue](#) [En savoir plus](#)
- Azure for Students**
Bénéficiez de logiciels gratuits, de crédit Azure ou d'un accès à Azure Dev Tools for Teaching après avoir vérifié votre statut scolaire.
[Démarrer](#)

→ Carte en cours de validité

Nb : **Pour créer un abonnement Azure, il est nécessaire de renseigner une carte en cours de validité pour confirmer son identité** : cette restriction s'applique à l'essai gratuit, au paiement à la demande, et également dans le cadre de l'offre des 2000\$ de crédits Azure offerts pour les organisations à but non lucratif.

Alternativement, il est possible de contacter son revendeur Microsoft pour créer un abonnement Azure dans Open en renseignant un numéro de licence. Cette licence n'est pas proposée chez tous les revendeurs.

→ Accès admin au portail Azure pour gérer les abonnements. Différents abonnements peuvent exister au sein d'un même tenant. L'abonnement est disponible pour le compte l'ayant créé et peut être assigné à d'autres comptes par le créateur ou un compte admin.

→ Accès admin au tenant Microsoft EntraID pour créer l'Application Microsoft Graph et consentir les permissions d'application.

→ Système d'hébergement

Windows *Consommation* : support continu. (recommandé)

Linux *Consommation* : retrait le 30 septembre 2028 → migrer vers *Consommation Flexible* (Windows *Consommation* non impacté).

4. Abonnement Azure

La mise en place d'une Application de Fonction nécessite différentes ressources pour fonctionner.

La fonction utilisera un *Plan Consommation* : 1 M d'exécutions/mois gratuites et 400 000 GB-s gratuits/mois. Une exécution correspond à un appel de la fonction. PREVIST l'appellera une fois par heure, soit environ 720 exécutions/mois. Il est possible d'utiliser le plan *Consommation Flexible*, qui a des quotas différents mais garde 1 M d'exécutions gratuites.

Pour fonctionner, l'application nécessitera une ressource Storage et une ressource Application Insights (créées automatiquement).

- La ressource **Storage** nécessaire pour le fonctionnement de l'application sera facturée (<1€/mois).
- Certaines options de monitoring disponibles dans la ressource **Application Insight** seront facturées (prix variable en fonction des paramètres).
- La création d'un **Key Vault** optionnel pour le renouvellement automatique du secret sera facturée (<1€/rotation).

Nb : Il est possible de recevoir 2000\$ de crédits Azure annuels pour les organisations à but non lucratif.

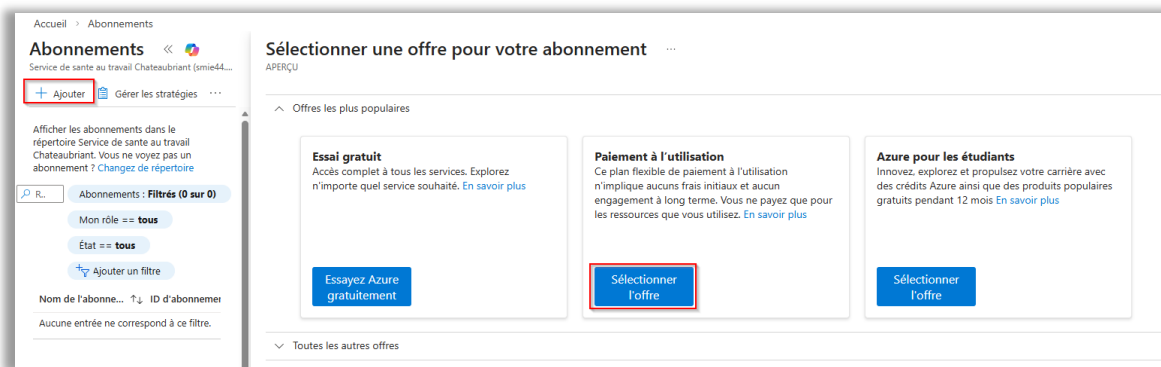
Vérifier la page de tarification la plus à jour.



Se rendre sur le [Portail Azure](#) et sélectionner le menu : Abonnements

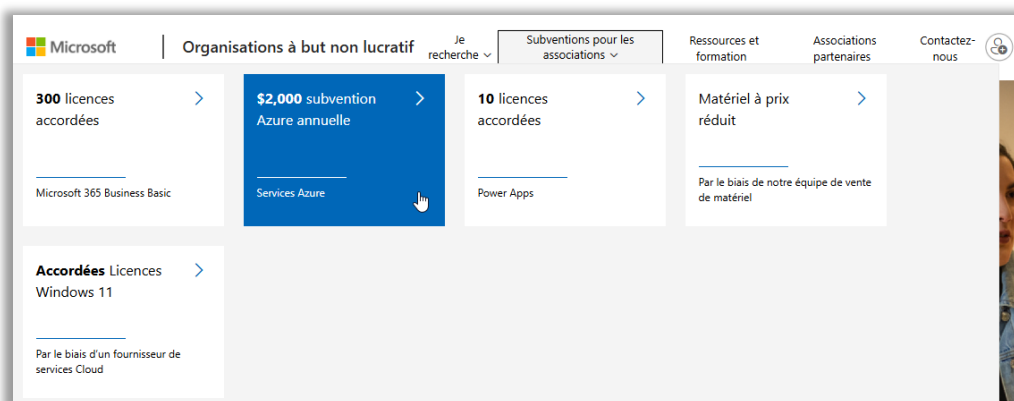
- 1- Cliquer sur [Ajouter](#)
- 2- Sélectionner l'option [Paiement à l'utilisation](#).

Pour renseigner un numéro de licence Azure dans Open (disponible auprès de certains revendeurs Microsoft), choisir « Toutes les autres offres » et sélectionner l'option Azure dans Open.



- 3- Renseigner les informations sur le propriétaire de l'abonnement et prendre connaissance des conditions d'utilisation de l'abonnement. Plusieurs abonnements peuvent exister sur un même portail Azure. Seuls le compte créateur de l'abonnement et le compte administrateur principal du Tenant sera en mesure de créer des ressources dans l'abonnement. Il sera nécessaire de donner les accès à l'abonnement aux autres comptes nécessitant l'accès aux ressources PREVIST.
- 4- Renseigner une carte en cours de validité.
Pour Azure dans Open, entrer le numéro de licence fourni.

- 5- Tenant éligible non-profit uniquement : Pour bénéficier de 2000\$ annuels de crédits Azure, se rendre sur nonprofit.microsoft.com et se connecter avec le compte propriétaire du tenant. Choisir le menu **Subventions pour les associations – Services Azure**.

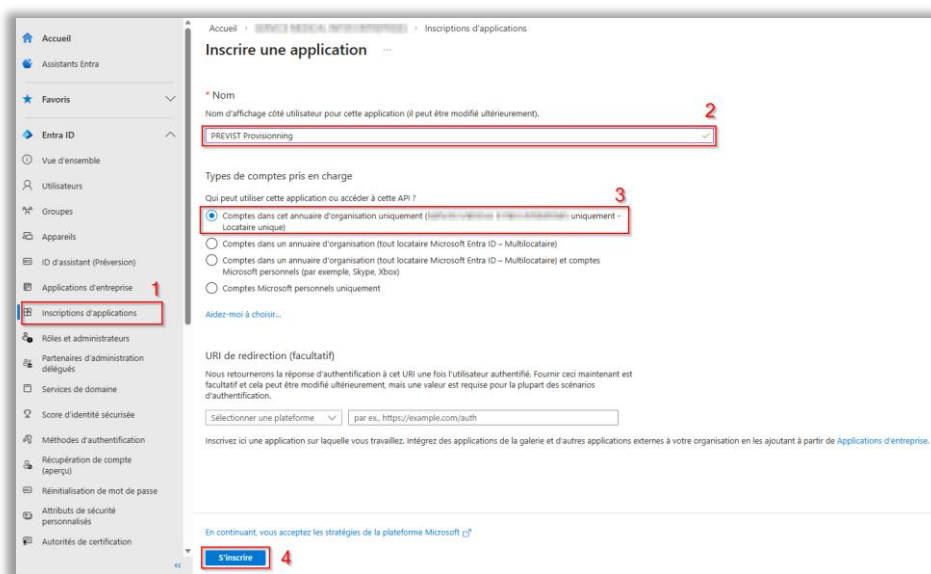


- 6- La demande sera traitée sous 48h. Une confirmation par mail (ou un refus le cas échéant) sera envoyée sur la boîte mail du propriétaire du tenant. L'activation des crédits devra se faire depuis un lien présent dans ce mail sous 90 jours.
- 7- Le propriétaire du tenant recevra une alerte de renouvellement un mois avant l'expiration des crédits. Le renouvellement peut être anticipé et ne sera pris en compte qu'à la date anniversaire.

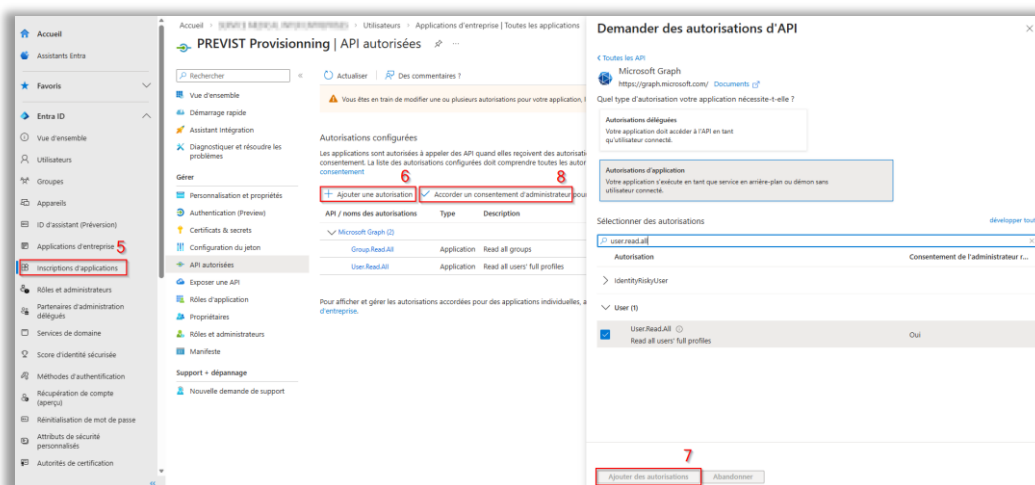
5. Application Microsoft Graph

Créer une application dans le Centre d'administration [Microsoft Entra](#) :

- 1- Inscriptions d'applications – Nouvelle Inscription
- 2- Nom : PREVIST Provisioning (recommandé)
- 3- Types de comptes pris en charge : Comptes dans cet annuaire d'organisation uniquement
- 4- S'inscrire



- 5- Menu *API autorisées*
- 6- Ajouter une autorisation – Microsoft Graph – Autorisation d'application.
- 7- Autorisations d'application à accorder :
 - o *User.Read.All* (Application)
 - o *Group.Read.All* (Application)
- 8- Accorder un consentement d'administrateur pour <Tenant>.



Ces permissions ouvrent la lecture des utilisateurs et des groupes au niveau annuaire pour la fonction.
 Nb : la valeur « User.Read » (Déléguée) accordée par défaut n'est pas nécessaire.

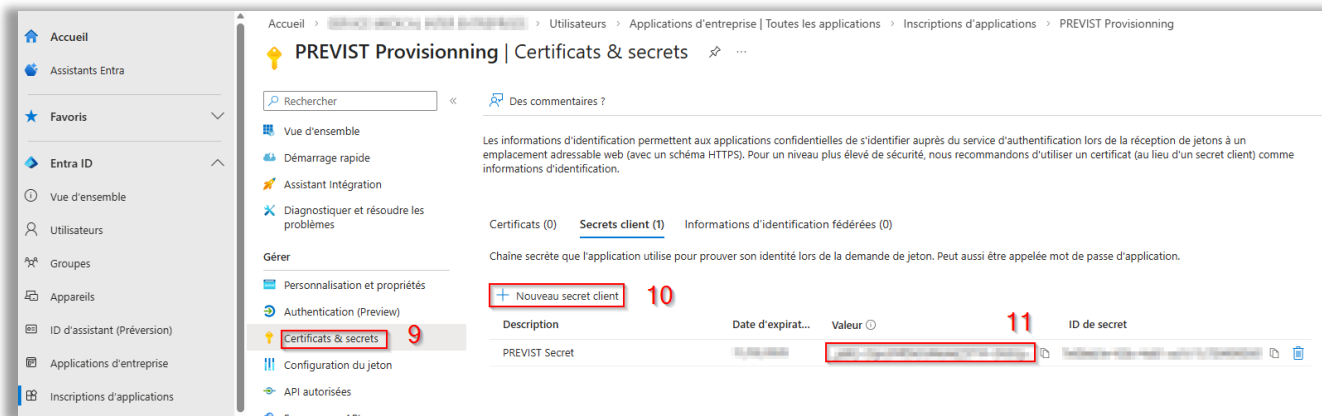
9- Menu **Certificats & secrets - Secret client**

10- Créer un **Nouveau secret client** – PREVIST Secret

Durée maximale désormais de 2 ans (Microsoft a supprimé les secrets « N'expire jamais »).

Cette clé ne sera utilisée qu'en interne. Elle sera donc à renouveler tous les deux ans sans intervention de PREVIST.

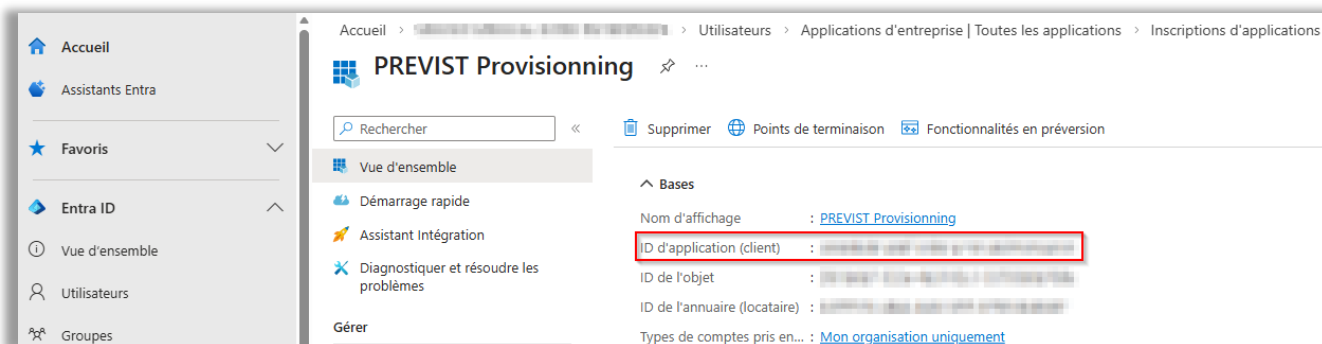
11- **Noter la Valeur** : elle ne pourra plus être consultée par la suite.



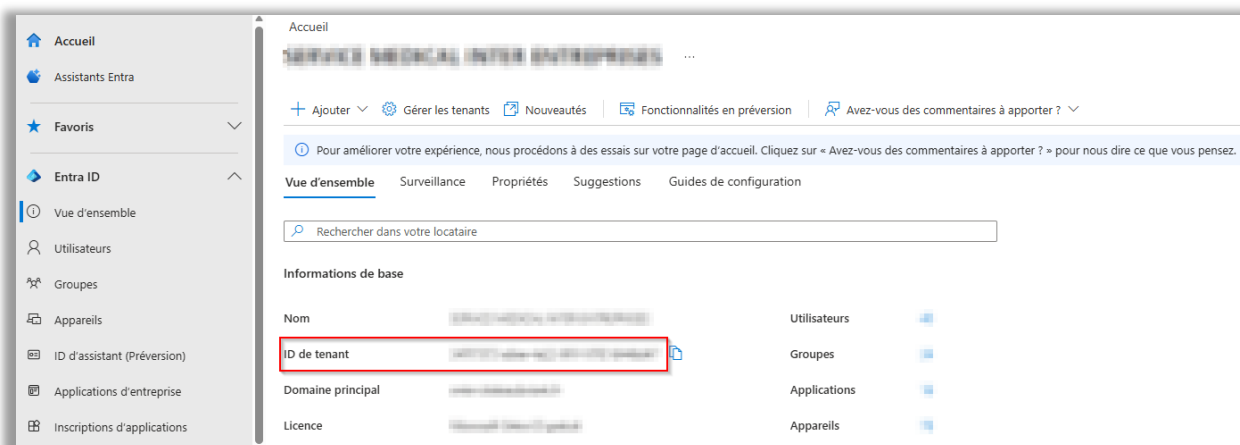
Nb : Il sera possible d'automatiser la rotation du secret (cf. §12).

Pour les chapitres suivants, retenir les valeurs suivantes qui seront à renseigner dans l'application web :

- **Valeur secret client** : cf point 11 ci-dessus
- **ID d'application (client)** : menu **Vue d'ensemble** de l'application
- **Pour l'automatisation du renouvellement du secret (§12, optionnel)**, retenir également l'**ID de l'objet**



- **ID de Tenant** : menu **Vue d'ensemble** d'EntraID



6. Création de l'Application de Fonction (Windows)



Créer une ressource sur le [Portail Azure](#) : Application de fonction
Sélectionner une option d'hébergement : Consommation (recommandé)

- 1- **Abonnement** : Choisir une suscription Azure en cours.
- 2- **Groupe de ressources** : **Créer nouveau** (recommandé : PREVIST)
- 3- **Nom de l'application de fonction** : `previstProvisioning<SPST>` (recommandé)
- 4- **Système d'exploitation** : **Windows** (recommandé)
- 5- **Pile d'exécution** : **Node.js**
- 6- **Version** : **22 LTS**
- 7- **Région** : **West Europe** (recommandé)
- 8- **Vérifier + créer - Créer**

The screenshot shows the 'Créer une application de fonction (Consommation)' page in the Azure portal. The page is titled 'Créer une application de fonction (Consommation)' and has a breadcrumb trail: 'Accueil > Créer une ressource > Créer une application de fonction'. Below the title, there are tabs for 'De base', 'Stockage', 'Réseau', 'Surveillance', 'Durable Functions', 'Déploiement', 'Authentification', 'Balises', and 'Vérifier + créer'. The main content area is titled 'Détails du projet' and contains the following fields and options:

- Abonnement ***: A dropdown menu with a red box around it and the number '1' to its right.
- Groupe de ressources ***: A dropdown menu with '(Nouveau) PREVIST' selected and a 'Créer nouveau' link below it. A red box is around the dropdown and the number '2' is to its right.
- Détails de l'instance**:
 - Nom de l'application de fonction ***: A text input field containing 'PREVISTprovisioning' with a checkmark icon. A red box is around the field and the number '3' is to its right.
 - Système d'exploitation ***: Radio buttons for 'Linux (hérité)' and 'Windows'. The 'Windows' option is selected and circled in red with the number '4' to its right.
- Pile d'exécution ***: A dropdown menu with 'Node.js' selected. A red box is around the dropdown and the number '5' is to its right.
- Version ***: A dropdown menu with '22 LTS' selected. A red box is around the dropdown and the number '6' is to its right.
- Région ***: A dropdown menu with 'West Europe' selected. A red box is around the dropdown and the number '7' is to its right.

At the bottom of the form, there is a 'Vérifier + créer' button with a red box around it and the number '8' to its right, along with '< Précédent' and 'Suivant : Stockage >' buttons.

Nb : Patienter quelques instant le temps que l'application de fonction ainsi que ses dépendances se génèrent.

... Le déploiement est en cours

7. Paramètres & variables d'environnement

Depuis l'étape précédente, ouvrir

[Accéder à la ressource](#)

ou depuis le [Portail Azure](#), ouvrir l'application



Ajouter les variables suivantes dans Paramètres → Variables d'environnement.

Paramètres de l'application Microsoft Graph (retenus en §5) :

TENANT_ID = <ID de tenant>

CLIENT_ID = <ID d'application (client)>

CLIENT_SECRET = <Valeur secret>

Build (Oryx) pour déploiement Zip :

SCM_DO_BUILD_DURING_DEPLOYMENT = true

ENABLE_ORYX_BUILD = true

Remarque : Oryx est le builder App Service; le couple SCM_DO_BUILD_DURING_DEPLOYMENT + zip-deploy déclenche le build (npm install) côté Kudu. Selon historique de déploiement, Oryx peut s'invoquer même si désactivé ; nettoyer Kudu si comportement inattendu.

Paramétrage fonctionnel :

INBOUND_SHARED_SECRET : Clé de chiffrement « Secret » utilisée en header lors de l'appel de la fonction.

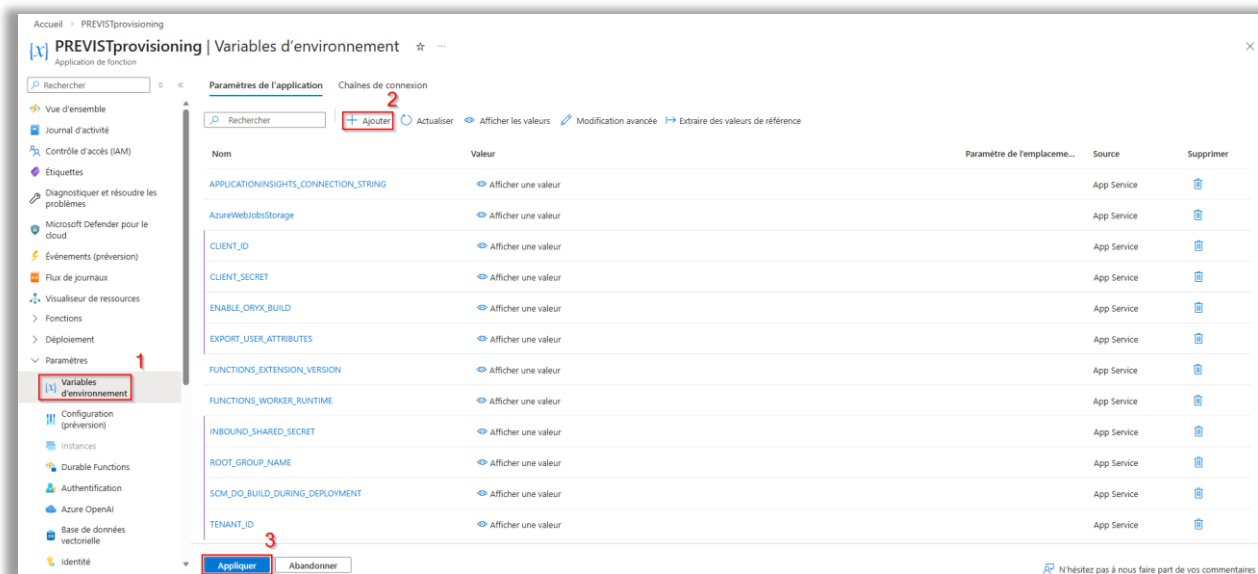
Cette valeur personnalisée sera à communiquer à PREVIST. (Caractères autorisés : « a-z », « A-Z », « 0-9 », « - »)

ROOT_GROUP_NAME : Nom du groupe racine (displayName) dans EntraID (recommandé GRP_PREVIST)

La fonction résout ce groupe par displayName et n'affiche que ses membres directs (utilisateurs) + tous les utilisateurs (directs + imbriqués) pour chaque sous-groupe direct. (cf §2)

EXPORT_USER_ATTRIBUTES : liste CSV d'attributs utilisateurs Graph à exporter en plus de id, userPrincipalName, surname, givenName (ex. mail,department,jobTitle).

Cette variable peut rester vide, mais doit être créée.



Nom	Valeur	Paramètre de l'emplacement...	Source	Supprimer
APPLICATIONINSIGHTS_CONNECTION_STRING	Afficher une valeur		App Service	
AzureWebJobsStorage	Afficher une valeur		App Service	
CLIENT_ID	Afficher une valeur		App Service	
CLIENT_SECRET	Afficher une valeur		App Service	
ENABLE_ORYX_BUILD	Afficher une valeur		App Service	
EXPORT_USER_ATTRIBUTES	Afficher une valeur		App Service	
FUNCTIONS_EXTENSION_VERSION	Afficher une valeur		App Service	
FUNCTIONS_WORKER_RUNTIME	Afficher une valeur		App Service	
INBOUND_SHARED_SECRET	Afficher une valeur		App Service	
ROOT_GROUP_NAME	Afficher une valeur		App Service	
SCM_DO_BUILD_DURING_DEPLOYMENT	Afficher une valeur		App Service	
TENANT_ID	Afficher une valeur		App Service	

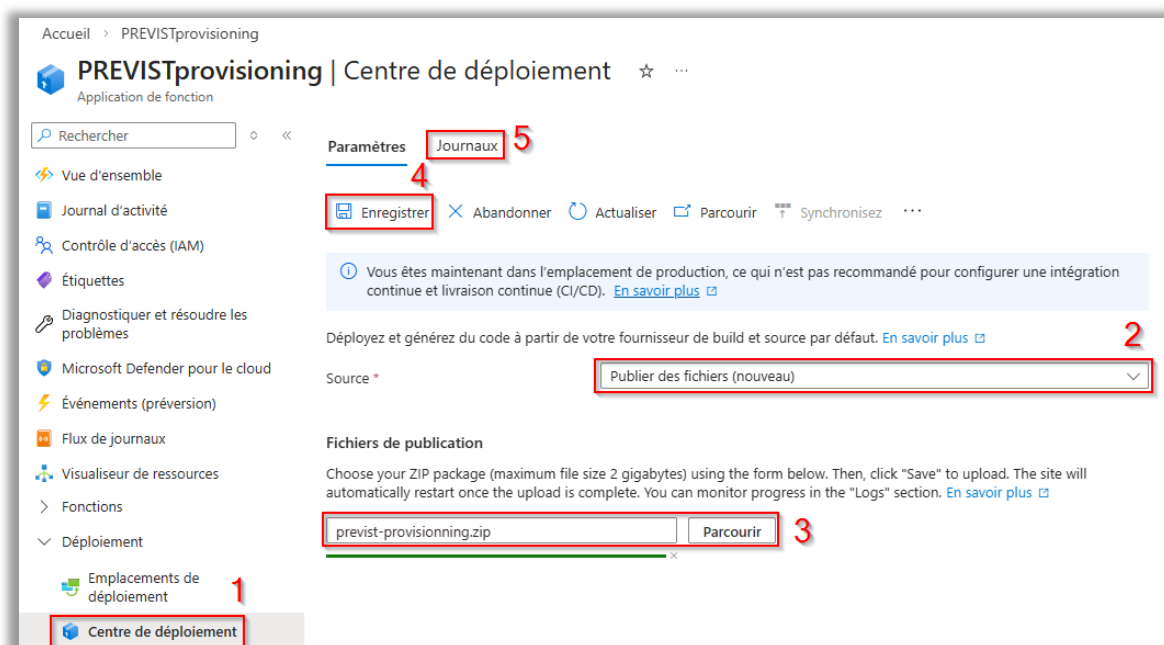
Appliquer les modifications et Confirmer.

Les variables présentes par défaut doivent être conservées en l'état.

8. Import de la Fonction Node.js (zip)

Importer le projet « [previst-provisioning.zip](#) » contenant la fonction node.js.

- 1- Déploiement - Centre de déploiement
- 2- Source : Publier des fichiers
- 3- Fichiers de publication : Cliquer sur **Parcourir** et sélectionner le projet `previst-provisioning.zip` fourni
- 4- Enregistrer
- 5- Journaux : Cet onglet permet de vérifier l'état du déploiement. Patienter que la colonne « Etat » passe en « Opération réussie (Actif) »



Optionnel : Vérifier les dépendances côté Kudu Console/SSH :

```
npm ls @azure/functions  
npm ls @microsoft/microsoft-graph-client  
npm ls @azure/identity
```

Ces packages sont utilisés par le handler HTTP et par le client Graph authentifié via Client Credentials.

NB : Des outils de diagnostics avancés sont disponibles dans le menu *Outils de développement* tels qu'une console (sans élévation), les outils Kudu+, et un éditeur de fichiers.

9. Intégration PREVIST (et test appel HTTP trigger)

Sécurité de l'Endpoint (auth = fonction):

Le handler GetPrevistUsers est défini en HTTP GET, authLevel: 'function', route previst-users.

L'appel requiert deux clés (fonction ou host) via « x-functions-key » ou « ?code=* », et via « X-Previst-Secret » ou « &secret=* ».

Il est possible de tester l'appel de la fonction directement dans un navigateur par l'URL :

https://<app>.azurewebsites.net/api/previst-users?code=<FUNCTION_KEY>&secret=<INBOUND_SHARED_SECRET>

A cette étape, merci de fournir à PREVIST les éléments suivants :

- **<app> & <FUNCTION_KEY>** : Menu « [Vue d'ensemble - GetPrevistUsers - Obtenir une URL de fonction - default \(Clé de fonction\)](#) »
- **<INBOUND_SHARED_SECRET>** : Menu « [Variables environment](#) »

Ces éléments (*à titre informatif*) permettront d'intégrer les comptes filtrés dans PREVIST à l'aide de Workflows (côté PREVIST). Ces Workflows sont paramétrés dans l'IAM Okta.

Endpoint :

GET <https://<app>.azurewebsites.net/api/previst-users>

Headers:

x-functions-key: <FUNCTION_KEY> (ou ?code=<FUNCTION_KEY> en query)

X-Previst-Secret: <INBOUND_SHARED_SECRET> (ou &secret=<INBOUND_SHARED_SECRET> en query)

Exemple cURL:

```
curl -s \ -H "x-functions-key: <FUNCTION_KEY>" \ -H "X-Previst-Secret: <INBOUND_SHARED_SECRET>" \ "https://<app>.azurewebsites.net/api/previst-users"
```

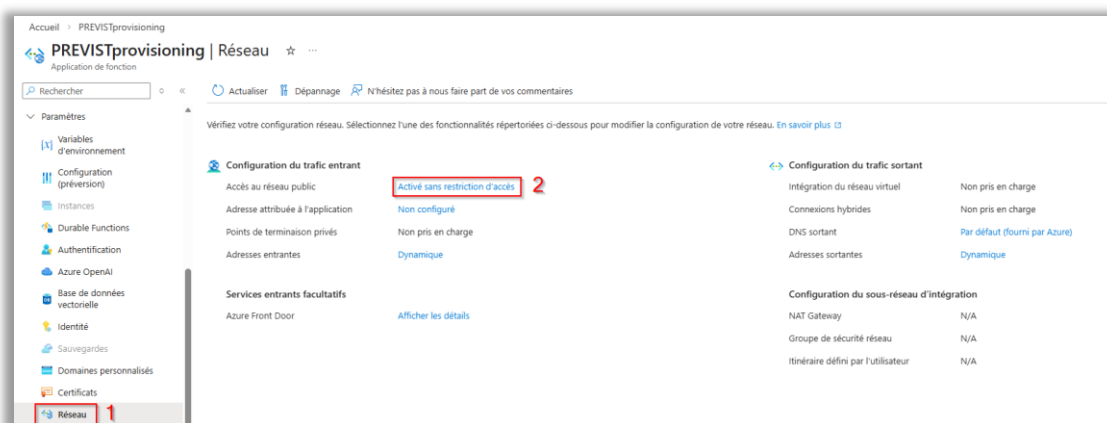
Test query:

https://<app>.azurewebsites.net/api/previst-users?code=<FUNCTION_KEY>&secret=<INBOUND_SHARED_SECRET>

10. (Optionnel) Filtrage IP : Restriction d'accès

Pour mettre en place un filtre par IP afin de sécuriser les appels sur l'application de fonction (en plus nom d'hôte sécurisé, du header function, et du secret) :

- 1- Menu Paramètres – Réseau
- 2- Accès au réseau public : cliquer sur **Activé sans restriction d'accès**

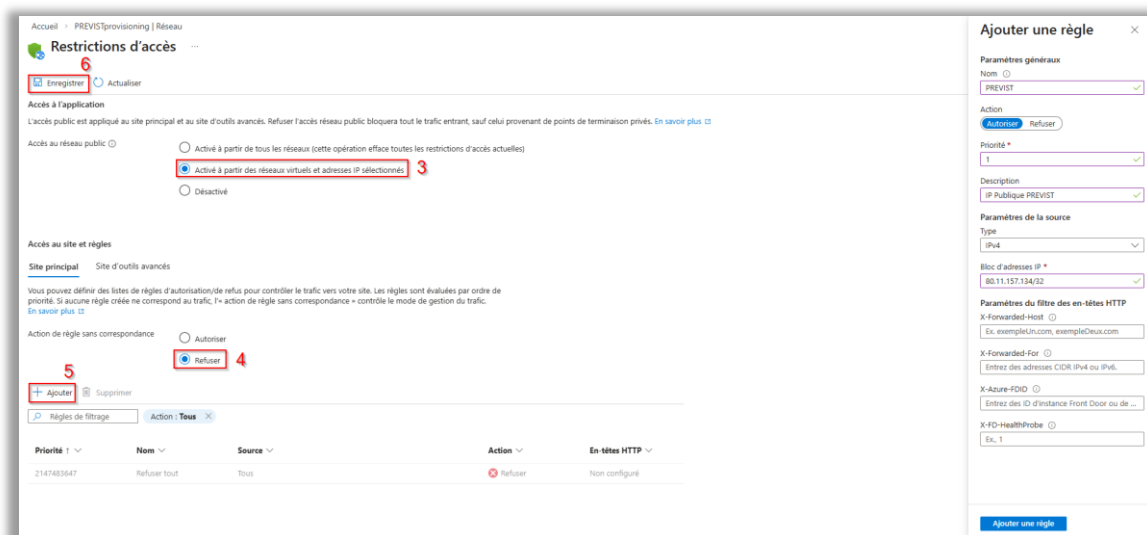


- 3- Accès au réseau public : Activé à partir des réseaux virtuels et adresses IP sélectionnés
- 4- Action de règle sans correspondance : Refuser, permettra de refuser la connexion de la fonction depuis toutes les IPs, sauf celles autorisées manuellement.

5- Ajouter la liste d'IPs suivantes :

Nom	Action	Priorité	Description	Bloc d'adresses IP
Okta_n	Autoriser	1	IPs Publiques Okta	Le pool d'IPs publiques d'Okta est disponible sur la page Allow access to Okta IP addresses . PREVIST est hébergé dans la cellule « Production Ireland : emea_cell_2 » composée de 180 adresses IP. L'outil de restriction ne permet d'ajouter des IP que par groupe de 8, il sera donc nécessaire de créer plusieurs pools pour autoriser la totalité des IPs d'Okta.
Admins PREVIST (optionnel)	Autoriser	1	IP Publique Admins PREVIST	80.11.157.134/32, 5.39.48.130/32 (pour tests d'appels par les admins PREVIST)
<SPST> (optionnel)	Autoriser	1	IPs Publique du SPST	Pool d'IPs publiques du SPST (pour tests d'appels de la fonction en interne)


6- Enregistrer, Accepter la mise à jour et Continuer



The screenshot shows the 'Restrictions d'accès' configuration page. The main content area includes sections for 'Accès à l'application', 'Accès au réseau public', 'Accès au site et règles', and 'Action de règle sans correspondance'. The 'Action de règle sans correspondance' section has 'Autoriser' and 'Refuser' radio buttons, with 'Refuser' selected. A table below shows a rule with ID 2147483647, action 'Refuser tout', source 'Tous', and HTTP headers 'Non configuré'. The right sidebar, titled 'Ajouter une règle', contains fields for 'Nom' (PREVIST), 'Action' (Autoriser/Refuser), 'Priorité' (1), 'Description' (IP Publique PREVIST), 'Type' (IPv4), 'Bloc d'adresses IP' (80.11.157.134/32), and various HTTP header settings. Red boxes and numbers 1 through 6 highlight the 'Enregistrer' button, the 'Activer à partir de tous les réseaux' radio button, the 'Activer à partir des réseaux virtuels et adresses IP sélectionnés' radio button, the 'Refuser' radio button, the 'Ajouter' button, and another 'Enregistrer' button respectively.

11. (Optionnel) Monitoring

Il est possible de créer des alertes de supervision depuis le menu **Supervision – Alertes** dans l'application de fonction.

Des options plus poussées sont disponibles dans la ressource Application Insights  **PREVISTprovisioning** générée automatiquement sur le [Portail Azure](#).

Certaines de ces ressources de supervision sont facturées. Les tarifs sont ajustés et affichés en temps réels lors de la préparation des alertes. Si une offre de crédits non-profit est liée à l'abonnement en cours, ces alertes en seront déduites.

Métriques :

Le menu **Supervision – Métriques** permet de consulter les différentes statistiques sur l'utilisation de la fonction tel que le nombre d'exécution sur une période donnée (FunctionExecutionCount) ou les tentatives de connexion depuis une IP non autorisée (http 403).

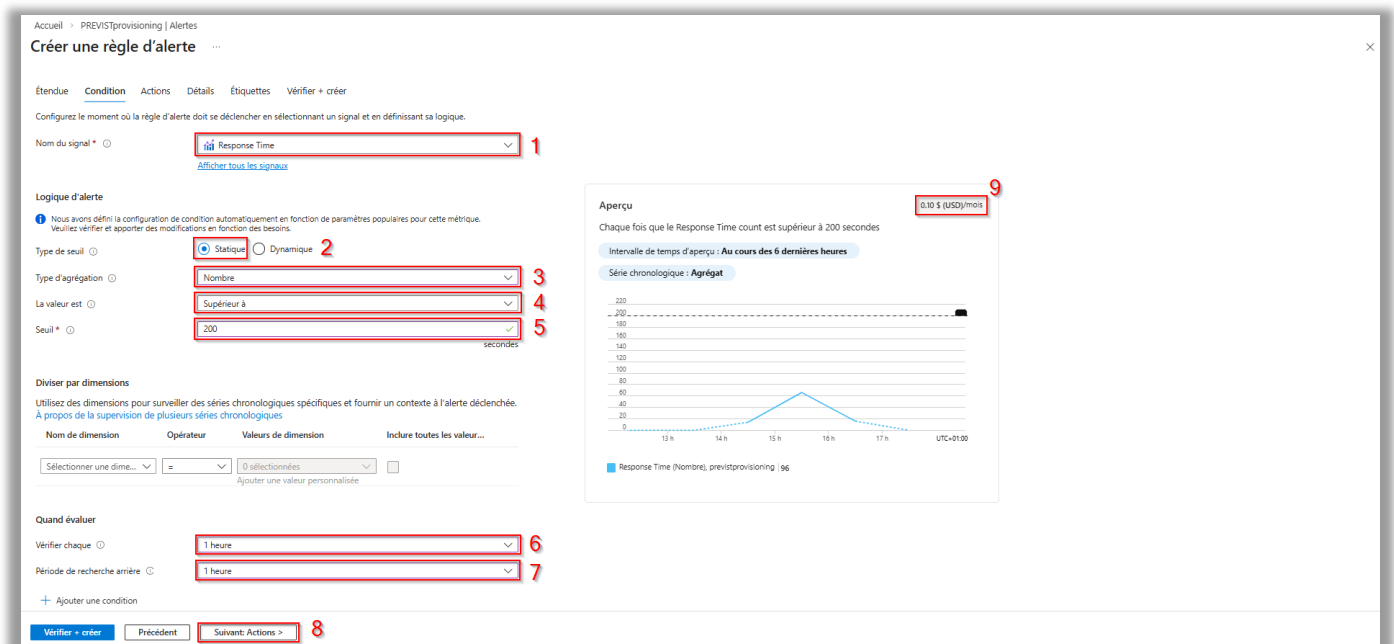
Alertes personnalisées :

Pour monitorer le temps de réponse de la fonction (timeout par défaut non paramétrable de 240 secondes) et recevoir un mail en cas de dépassement d'un seuil paramétré à 200 secondes.

Depuis le menu **Supervisions – Alertes – Créer**.

- 1- **Nom du signal** : [Afficher tous les signaux](#) - Response Time
- 2- **Type de seuil** : Statique
- 3- **Type d'agrégation** : Nombre
- 4- **La valeur est** : Supérieur à
- 5- **Seuil** : 200
- 6- **Vérifier chaque** : 1 heure
- 7- **Période de recherche arrière** : 1 heure
- 8- **Suivant** : Actions >

Nb : Un graph affichera en temps réel les résultats de cette alerte, ainsi que le tarif (10cts/mois) de la mise en place (9).



The screenshot displays the 'Créer une règle d'alerte' (Create alert rule) configuration page. The interface is divided into several sections:

- Nom du signal**: A dropdown menu showing 'Response Time' (highlighted with a red box and '1').
- Logique d'alerte**: A section with a note about automatic configuration. It includes a 'Type de seuil' (Threshold type) section with 'Statique' (Static) selected (highlighted with a red box and '2').
- Type d'agrégation**: A dropdown menu showing 'Nombre' (Count) (highlighted with a red box and '3').
- La valeur est**: A dropdown menu showing 'Supérieur à' (Greater than) (highlighted with a red box and '4').
- Seuil**: A text input field containing '200' (highlighted with a red box and '5').
- Diviser par dimensions**: A section for dimension-based alerting, currently showing '0 sélectionnées'.
- Quand évaluer**: A section for evaluation frequency, with 'Vérifier chaque' (Check every) set to '1 heure' (highlighted with a red box and '6') and 'Période de recherche arrière' (Back search period) set to '1 heure' (highlighted with a red box and '7').
- Actions**: A dropdown menu showing 'Suivant: Actions >' (highlighted with a red box and '8').
- Aperçu**: A preview section showing a graph of 'Response Time (Nombre, previstprovisioning | 96)' over time. A price tag of '0.10 \$ (USD)/mois' is displayed (highlighted with a red box and '9').

Onglets Actions :

- 9- Sélectionner des actions : Utiliser des actions rapides (préversion)
- 10- Nom du groupe d'actions : Envoi mail Alerte Response Time
- 11- Nom d'affichage : ResponseTime
- 12- E-mail : l'adresse mail recevant l'alerte
- 13- Enregistrer
- 14- Vérifier + créer

Accueil > PREVISTprovisioning | Alertes

Créer une règle d'alerte

Étendue Condition **Actions** Détails Étiquettes Vérifier + créer

Un groupe d'actions est un ensemble d'actions qui peuvent être appliquées à une règle d'alerte. [En savoir plus](#)

Sélectionner des actions

- Utiliser des actions rapides (préversion)
Sélectionnez une ou plusieurs des actions rapides. **9**
- Utiliser des groupes d'actions
Ajoutez un groupe d'actions existant ou en créez-en un.
- Aucun

Actions rapides

Les actions rapides ne sont pas encore configurées
[Gérer les actions rapides](#)

Utiliser des actions rapides (préversion)

Détails

Nom du groupe d'actions * **10** Envoi mail Alerte Response Time

Nom d'affichage * **11** ResponseTime

Actions

E-mail **12** antoine.panhelleu@keysource.eu

Envoyer un e-mail au rôle Azure Resource Manager
Sélectionner un rôle Azure Resource M... Manage

Notification d'Azure mobile app **13** antoine.panhelleu@keysource.eu

14 Vérifier + créer Précédent Suivant: Détails >

13 Enregistrer Annuler

12. (Optionnel) Gestion & renouvellement du secret Graph

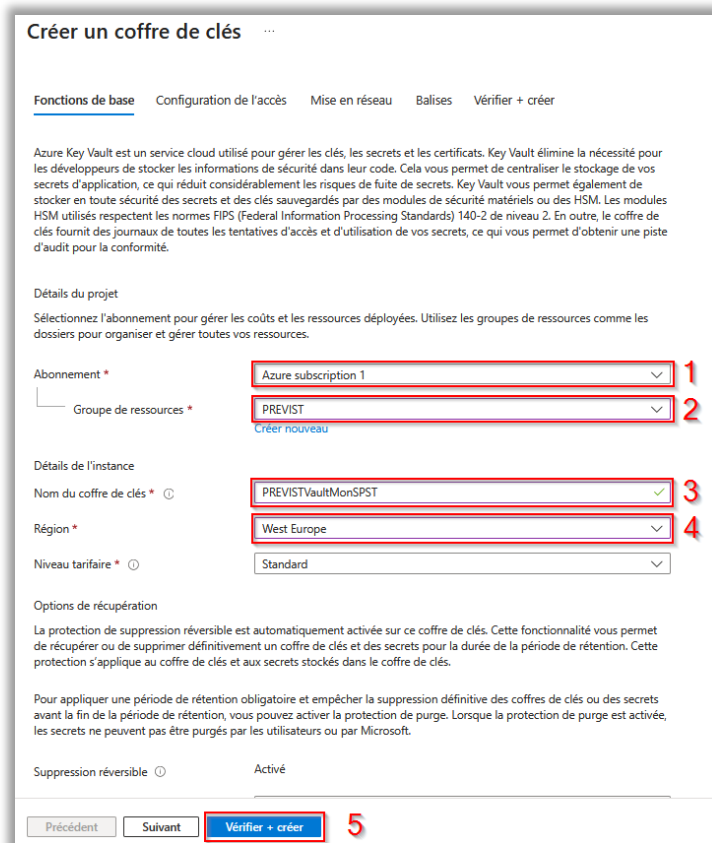
Le Secret de l'application Graph créé en §5 sera stocké dans un Key Vault sur le portail Azure. Ce secret sera appelé en lieu et place de la variable d'environnement `<CLIENT_SECRET>` paramétrée en §7.

Un compte Azure Automation renouvelera le secret dans un Runbook.

a- Création d'une ressource Key Vault Azure : (stockage du secret)

Créer une ressource sur le [Portail Azure](#) : Key Vault (ou Coffre de clés) 

- 1- **Abonnement** : Choisir une suscription Azure en cours.
- 2- **Groupe de ressources** : PREVIST (recommandé)
- 3- **Nom du coffre de clés** : PREVISTVault<SPST> (recommandé)
- 4- **Région** : West Europe (recommandé)
- 5- **Vérifier + créer** – Créer



Créer un coffre de clés ...

Fonctions de base Configuration de l'accès Mise en réseau Balises Vérifier + créer

Azure Key Vault est un service cloud utilisé pour gérer les clés, les secrets et les certificats. Key Vault élimine la nécessité pour les développeurs de stocker les informations de sécurité dans leur code. Cela vous permet de centraliser le stockage de vos secrets d'application, ce qui réduit considérablement les risques de fuite de secrets. Key Vault vous permet également de stocker en toute sécurité des secrets et des clés sauvegardés par des modules de sécurité matériels ou des HSM. Les modules HSM utilisés respectent les normes FIPS (Federal Information Processing Standards) 140-2 de niveau 2. En outre, le coffre de clés fournit des journaux de toutes les tentatives d'accès et d'utilisation de vos secrets, ce qui vous permet d'obtenir une piste d'audit pour la conformité.

Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * Azure subscription 1 **1**

Groupe de ressources * PREVIST **2**
[Créer nouveau](#)

Détails de l'instance

Nom du coffre de clés * PREVISTVaultMorSPST **3**

Région * West Europe **4**

Niveau tarifaire * Standard

Options de récupération

La protection de suppression réversible est automatiquement activée sur ce coffre de clés. Cette fonctionnalité vous permet de récupérer ou de supprimer définitivement un coffre de clés et des secrets pour la durée de la période de rétention. Cette protection s'applique au coffre de clés et aux secrets stockés dans le coffre de clés.

Pour appliquer une période de rétention obligatoire et empêcher la suppression définitive des coffres de clés ou des secrets avant la fin de la période de rétention, vous pouvez activer la protection de purge. Lorsque la protection de purge est activée, les secrets ne peuvent pas être purgés par les utilisateurs ou par Microsoft.

Suppression réversible Activé

Précédent Suivant **Vérifier + créer** **5**

NB : Le compte utilisé pour créer le coffre sera automatiquement paramétré comme Propriétaire. Le rôle propriétaire ne donne pas l'accès aux ressources du Vault, mais la possibilité d'éditer ces accès. Il est donc nécessaire de s'accorder le rôle **Agent des secrets Key Vault** (cf « Accorder les permissions » ci-dessous).

b- **Création d'un Compte Automation** : (renouvellement du secret)

Ce compte aura accès à l'application MgGraph et au Key Vault et se chargera de renouveler le Secret et de le mettra à jour dans le Key Vault.



Créer une ressource sur le [Portail Azure](#) : **Compte Automation**

- 1- **Abonnement** : Choisir une suscription Azure en cours.
- 2- **Groupe de ressources** : PREVIST
- 3- **Nom du compte d'automatisation** : PREVISTGraphSecretRotation (recommandé)
- 4- **Région** : West Europe
- 5- **Vérifier + créer** - **Créer**

Créer un compte Automation ...

Informations de base | Avancé | Réseau | Étiquettes | Vérifier + créer

Créez un compte Automation pour détenir les runbooks et la configuration Automation utilisés pour automatiser les opérations et les tâches de gestion autour des ressources Azure et non-Azure. Vous pouvez exécuter des tâches en nuage dans un environnement sans serveur ou utiliser des tâches hybrides sur votre ordinateur via des machines virtuelles Azure ou des serveurs compatibles avec Arc ou des serveurs à arc activé de la machine virtuelle VMWare (préversion). [En savoir plus](#)

Abonnement * 1

Groupe de ressources * 2
[Créer nouveau](#)

Détails de l'instance

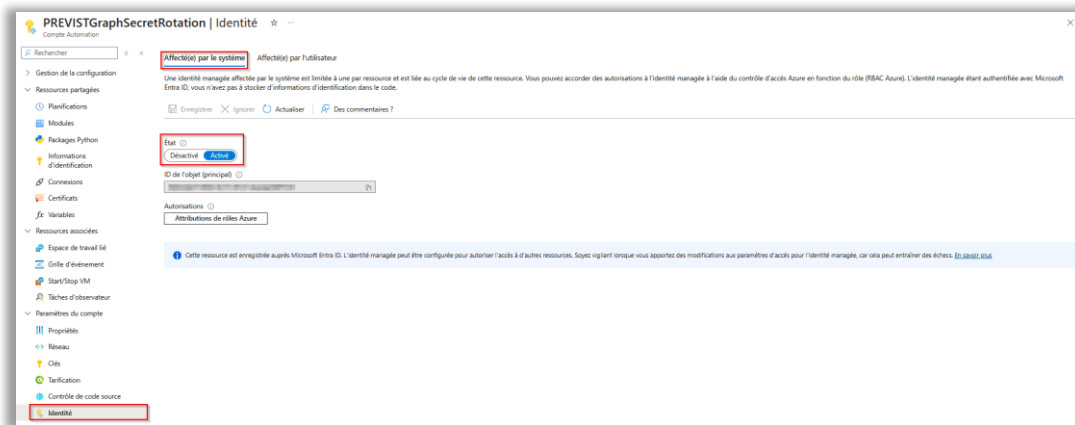
Nom du compte d'automatisation * 3

Région * 4

5


c- Accorder les permissions :

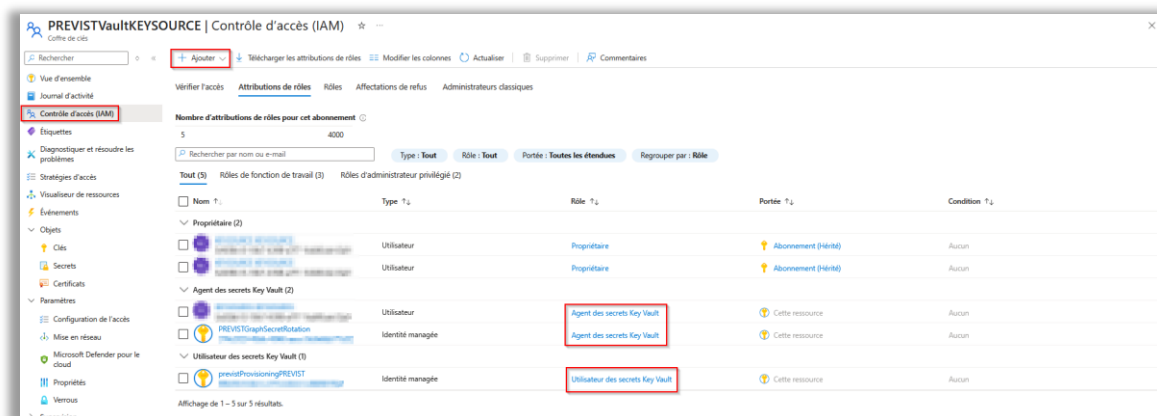
- ➔ Depuis le [Portail Azure](#), ouvrir le Compte Automation  **PREVISTGraphSecretRotation**.
Dans le menu **Paramètres du compte - Identité**, onglet **Affecté(e) par le système**, vérifier que l'état soit activé.



- ➔ Depuis le [Portail Azure](#), ouvrir l'Application de Fonction **PREVISTProvisioning<SPST>**.
Dans le menu **Paramètres - Identité**, onglet **Affecté(e) par le système**, vérifier que l'état soit activé.

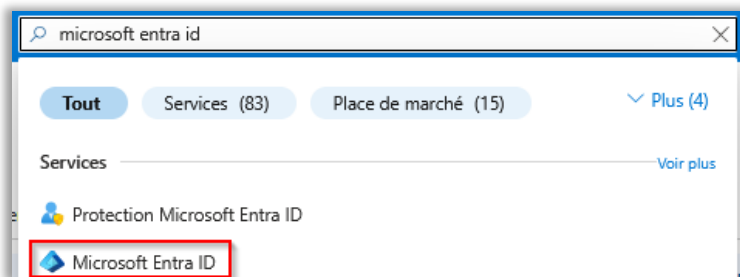
Nb : ce paramétrage permettra de donner les accès au secret enregistré dans le vault.


- ➔ Depuis le [Portail Azure](#), ouvrir le Key Vault **PREVISTVault<SPST>** précédemment créée.
Dans le menu **Contrôle d'accès (IAM) - Ajouter une attribution de rôle** :
 - Attribuer le rôle **Agent des secrets Key Vault** au compte actuellement utilisé ainsi qu'au compte Automation  **PREVISTGraphSecretRotation** précédemment créé (optionnel : aux autres comptes pouvant nécessiter l'accès à ce secret).
 - Attribuer le rôle **Utilisateur des secrets Key Vault** à l'Application de Fonction **PREVISTProvisioning<SPST>**

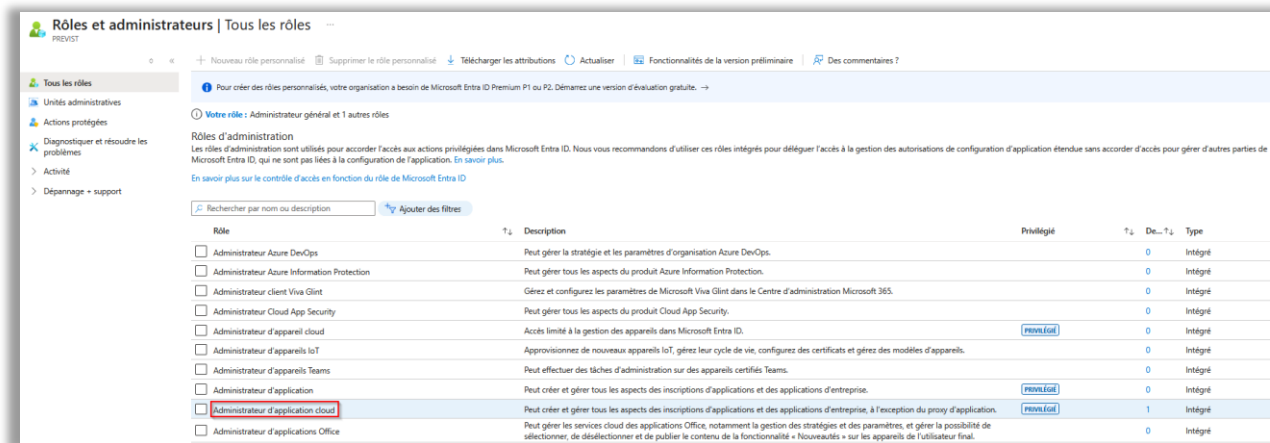


Nb : Ces rôles permettront l'écriture ou la lecture des secrets enregistrés dans le Vault.

→ Depuis le [Portail Azure](#), rechercher « Microsoft Entra ID » et l'ouvrir.



Dans le menu de gauche, choisir **Gérer – Rôles et administrateurs**. Ouvrir le rôle **Administrateur d'application cloud** et y ajouter le compte Automation  **PREVISTGraphSecretRotation** précédemment créé.



Nb : Cette option permettra au compte Automation de créer un secret dans l'application Graph.

d- Création du Runbook

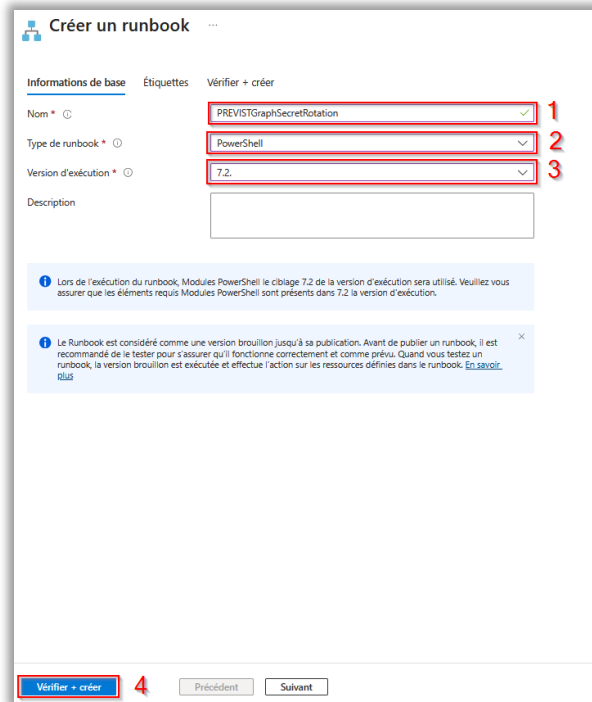
Depuis le Portail Azure, ouvrir le Compte Automation



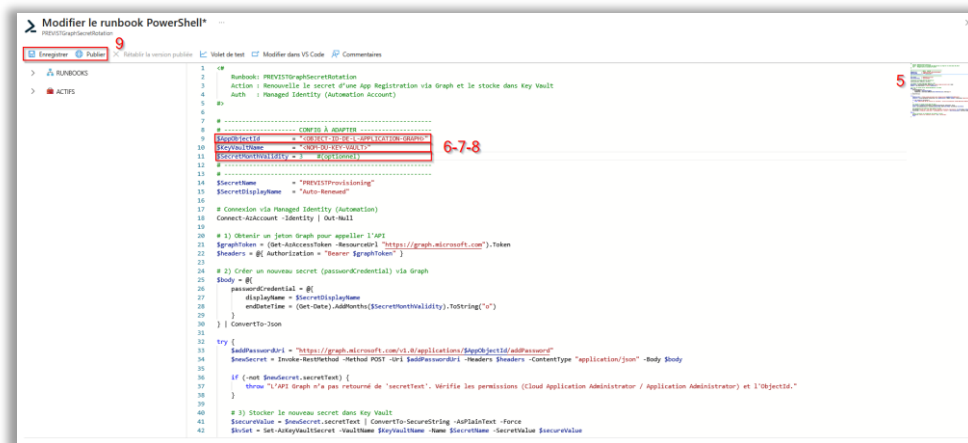
précédemment créé.

Dans le menu **Automatisation des processus – Runbooks – Créer un runbook**

- 1- **Nom** : PREVISTGraphSecretRunbook (recommandé)
- 2- **Type de runbook** : Powershell
- 3- **Version d'exécution** : 7.2
- 4- **Vérifier + créer** – Créer



- 5- Copier le contenu du script [PREVISTGraphSecretRotation.ps1](#)
- 6- Renseigner l'ID d'objet de l'application Graph retenu en \$5
- 7- Renseigner le nom du Key Vault créé précédemment PREVISTVault<SPST>
- 8- (Optionnel) Modifier la période de validité du secret (en mois)
- 9- Enregistrer + Publier



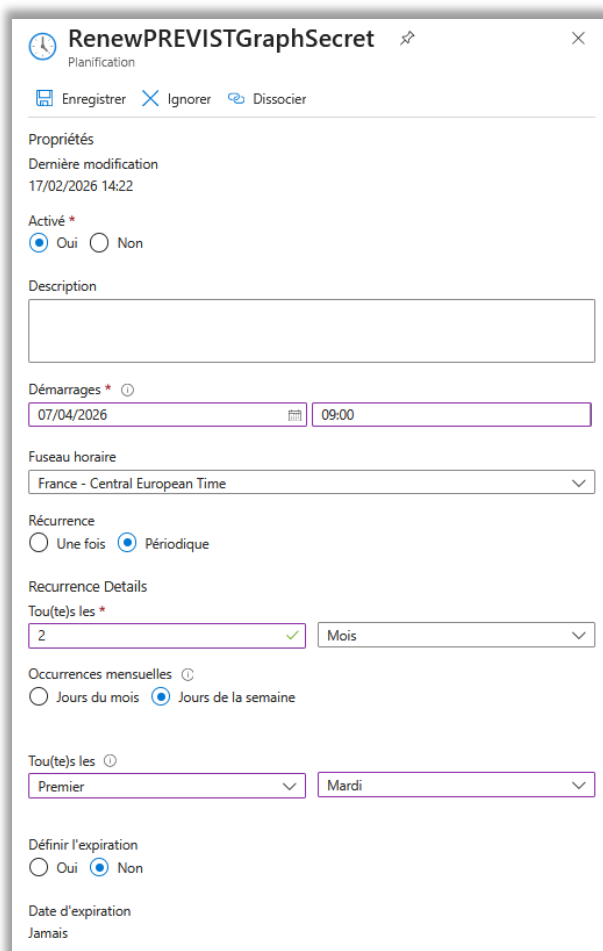
Nb : Dans le scenario par défaut, le secret expirera au bout de 3 mois.

e- Planification du Runbook

Dans le Runbook en cours, menu [Ressources – Planifications – Ajouter une planification](#)

Dans le scénario proposé, le secret expirant au bout de 3 mois, il est recommandé de planifier le renouvellement tous les 2 mois.

Dans cet exemple, le secret sera renouvelé à partir du 07 avril 2026, tous les 2 mois, le premier mardi du mois à 9h.

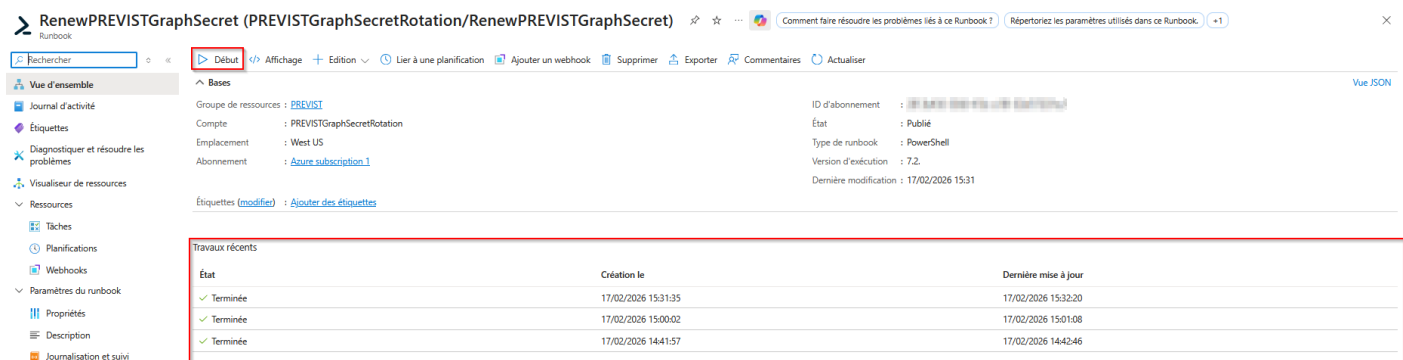


The screenshot shows a configuration window for a cron job named 'RenewPREVISTGraphSecret'. The window title is 'RenewPREVISTGraphSecret' with a clock icon and a close button. Below the title, there are three buttons: 'Enregistrer' (Save), 'Ignorer' (Cancel), and 'Dissocier' (Unlink). The 'Propriétés' (Properties) section shows 'Dernière modification' (Last modified) as '17/02/2026 14:22'. The 'Activé *' (Enabled) section has a radio button for 'Oui' (Yes) selected. The 'Description' field is empty. The 'Démarrages *' (Starts) section has a date field set to '07/04/2026' and a time field set to '09:00'. The 'Fuseau horaire' (Time zone) is set to 'France - Central European Time'. The 'Récurrence' (Recurrence) section has a radio button for 'Périodique' (Periodic) selected. The 'Recurrence Details' section has 'Tou(te)s les *' (Every) set to '2' and 'Mois' (Months). The 'Occurrences mensuelles' (Monthly occurrences) section has a radio button for 'Jours de la semaine' (Days of the week) selected. The 'Tou(te)s les' (Every) section has 'Premier' (First) and 'Mardi' (Tuesday) selected. The 'Définir l'expiration' (Define expiration) section has a radio button for 'Non' (No) selected. The 'Date d'expiration' (Expiration date) is set to 'Jamais' (Never).

f- Test du Runbook

Dans le menu [Vue d'ensemble](#) du Runbook, cliquer sur [Début](#)

Les logs de sortie des exécutions manuelles et planifiées sont disponibles sur cette page.



RenewPREVISTGraphSecret (PREVISTGraphSecretRotation/RenewPREVISTGraphSecret)

Vue d'ensemble

Groupes de ressources : PREVIST

Compte : PREVISTGraphSecretRotation

Emplacement : West US

Abonnement : Azure_subscription_1

ID d'abonnement : [redacted]

État : Publié

Type de runbook : PowerShell

Version d'exécution : 7.2

Dernière modification : 17/02/2026 15:31

État	Création le	Dernière mise à jour
Terminée	17/02/2026 15:31:35	17/02/2026 15:32:20
Terminée	17/02/2026 15:00:02	17/02/2026 15:01:08
Terminée	17/02/2026 14:41:57	17/02/2026 14:42:46

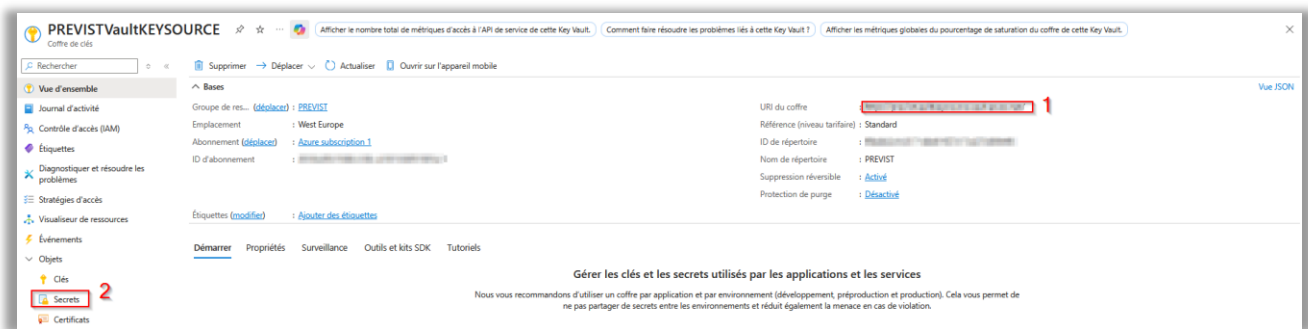
À la suite du test, vérifier :

- Les logs de sortie de l'exécution
- La création du secret Graph « Auto-Renew » dans EntraID (cf §4)
- La création du secret dans le vault (cf point 2 ci-dessous)

g- Connecter la Fonction d'application au Key Vault :

Depuis le [Portail Azure](#), ouvrir le Key Vault [PREVISTVault<SPST>](#) précédemment créée.

- 1- Dans le menu [Vue d'ensemble](#), collecter l'URL du coffre / Vault.
- 2- Dans le menu [Objets - Secrets](#), retrouver le secret généré automatiquement par le Runbook.



PREVISTVaultKEYSOURCE

URI du coffre : [redacted] 1

Référence (niveau tarifaire) : Standard

ID de répertoire : [redacted]

Nom de répertoire : PREVIST

Suppression réversible : Actif

Protection de purge : Désactivé

Objets

Clés 2

Secrets

Gérer les clés et les secrets utilisés par les applications et les services

Nous vous recommandons d'utiliser un coffre par application et par environnement (développement, préproduction et production). Cela vous permet de ne pas partager de secrets entre les environnements et réduit également la menace en cas de violation.

- 3- Dans l'application de fonction, remplacer la valeur de la variable `<CLIENT_SECRET>` (cf §7) par : `@Microsoft.KeyVault(SecretUri=https://<URL_DU_VAULT>.vault.azure.net/secrets/PREVISTProvisioning/)`

Le secret est désormais appelé depuis le Vault lors de l'exécution de la fonction. Un nouveau secret sera généré tous les deux mois, et mis à jour automatiquement dans le Vault.

13. Annexes

- [Annexe Matrice Metiers Curebot.pdf](#) : Liste des groupes de sécurité recommandés pour l'attribution des rôles métiers sur l'application finale Curebot.
- [previst-provisioning.zip](#) : Script Node.js prêt à uploader dans l'application de fonction. (cf §8)
- [WebApp_previst-provisioning.zip](#) : Version Web App du script Node.js pour installation sur VM on-premise.
- [PREVISTGraphSecretRotation.ps1](#) : Script permettant la rotation du secret d'appel de l'application MgGraph. (cf §12)
- [Notice générale PREVIST.pdf](#)
- [Notice Informatique PREVIST-V2.pdf](#)
- [Notice RGPD PREVIST v2.pdf](#)