Fédération EntraID / PREVIST

Table des matières

1. Délégation de l'authentification PREVIST à EntraID

Ce document complète la notice Intégration sélective EntraID / PREVIST via Azure Functions. Il ne la remplace pas : le provisioning des comptes (création / mise à jour / suppression dans l'IAM PREVIST) reste géré par l'Application de Fonction décrite dans cette autre notice. Le présent document couvre uniquement l'authentification — le mécanisme par lequel un compte déjà provisionné dans PREVIST se connecte via son identité EntraID plutôt que par un mot de passe dédié.

Scénario :
Sans fédération, chaque compte dispose d'un mot de passe propre à PREVIST, distinct de celui du poste de travail / de la messagerie de l'établissement. Cela multiplie les mots de passe à retenir pour l'utilisateur final, et laisse à l'application la responsabilité de la robustesse de ce mot de passe, indépendamment de la politique de sécurité interne à l'établissement.

Principe de Fédération :
EntraID devient l'unique maître de l'identité pour l'authentification. L'utilisateur ne saisit plus de mot de passe PREVIST : sa connexion est entièrement déléguée à EntraID via un échange SAML. L'IAM conserve un mot de passe en base pour chaque compte, mais celui-ci n'est jamais utilisé ni présenté à l'utilisateur — l'authentification est redirigée systématiquement vers EntraID.

Vue d'ensemble :
- L'utilisateur final souhaite se connecter à PREVIST → l'IAM le redirige vers la page de connexion EntraID de l'établissement.
- EntraID authentifie l'utilisateur selon la politique de l'établissement (mot de passe, MFA, Windows Hello, etc.) et renvoie à l'IAM une assertion SAML signée.
- L'IAM vérifie la signature de cette assertion à l'aide du certificat public d'EntraID, puis recherche un compte correspondant déjà provisionné.
- Aucun provisioning « just-in-time » (JIT) n'est effectué à cette étape : si le compte n'existe pas dans PREVIST, la connexion échoue, quelle que soit la validité de l'authentification EntraID. Le compte doit avoir été créé au préalable par le flux de provisioning quotidien (AD ou Entra)
- Une fois authentifié auprès de PREVIST, l'accès à l'application finale (Curebot) est à son tour délégué à l'IAM — Okta agit alors comme fournisseur d'identité pour Curebot, de la même façon qu'EntraID agit comme fournisseur d'identité pour Okta.

Bénéfices :
- Aucun mot de passe supplémentaire à retenir.
- Si une session EntraID est déjà active dans le navigateur, l'authentification est automatiquement validée.
- Le cas contraire, l'utilisateur final reconnait la page d'authentification Office 365 et connait son mot de passe.
- La politique de sécurité est déléguée à l'établissement.

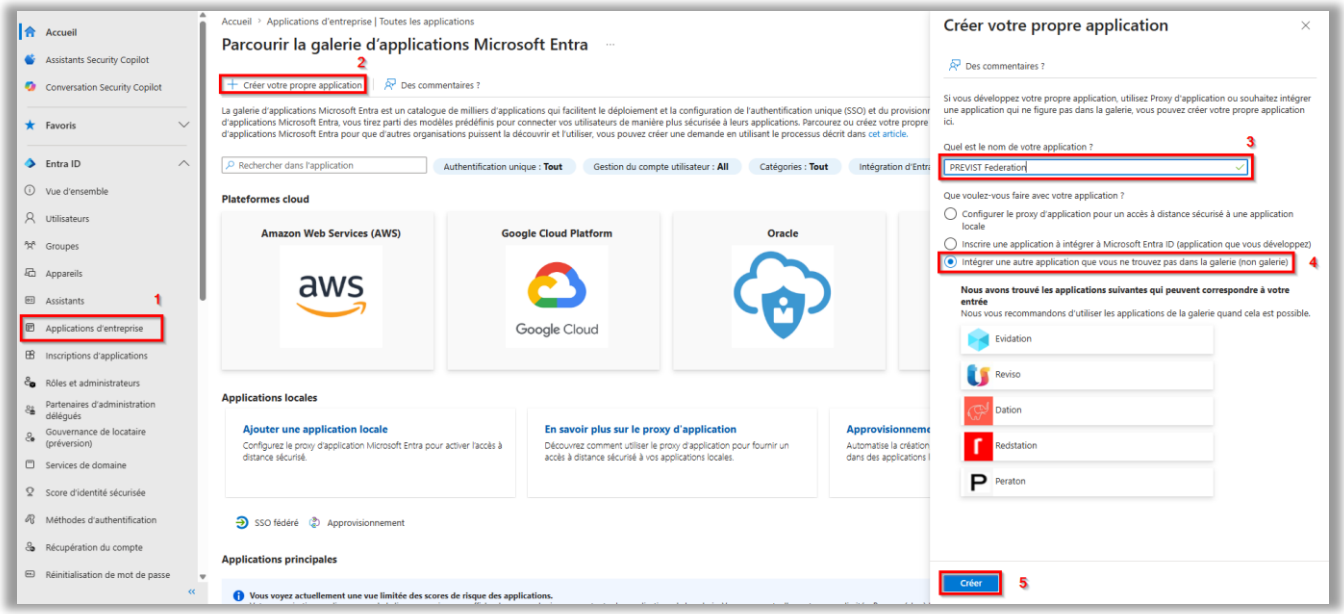
Durée de session :
La politique de session PREVIST s'appliquant lors de l'échange de jeton SAML garde la session active 24h maximum, 2h si aucune activité n'est enregistrée sur la session. Aucun cookie de session global n'est partagé entre les applications.

Nb - Intégration AD :
Dans le cadre d'une intégration par AD dans un environnement Azure AD Connect, la fédération par Entra n'est pas exclue, les comptes étant identiques dans les deux annuaires.

2. Création de l'application d'entreprise Entra

Créer une application dans le centre d'administration Microsoft Entra :

1- Applications d'entreprise - Nouvelle application
2- Créer votre propre application
3- Nom : PREVIST Federation (recommandé)
4- Intégrer une autre application que vous ne trouvez pas dans la galerie
5- Créer



Affectation de l'application :

Par défaut, les applications Microsoft doivent être affectées. Pour gérer l'affectation, il est possible de le faire :

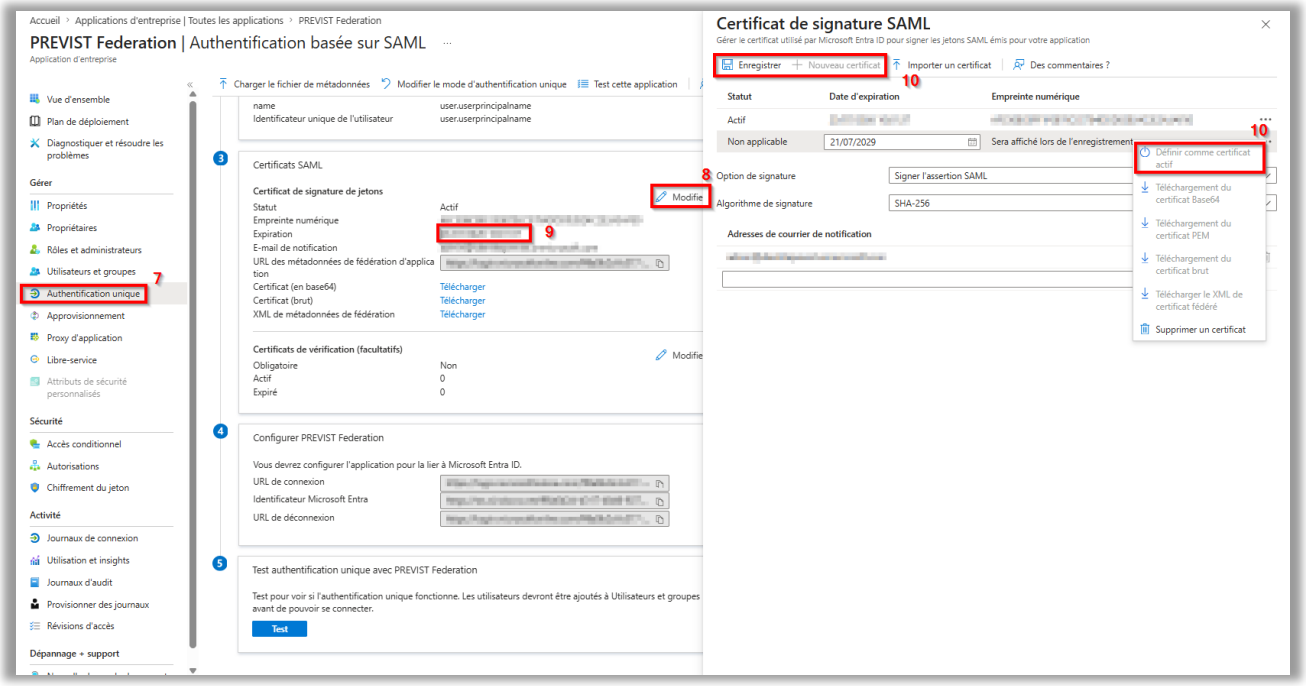
- Par compte (P1, P2, P3) : chaque compte doit manuellement être assigné à l'application.
- Par groupe (P2, P3) : l'accès à l'application peut être affecté par groupe (par exemple, le groupe utilisé dans l'intégration).
- Sans affectation requise (P1, P2, P3) : tous les comptes du tenant peuvent accéder à l'application.
- Il est également possible de donner ou de bloquer la possibilité pour les utilisateurs de demander l'accès à l'application (un responsable du traitement de ces demandes doit être assigné).

Cette option est parallèle à la création des comptes dans l'IAM PREVIST. L'accès à cette application ne donne pas l'accès à la plateforme, juste la possibilité de valider l'authentification vers l'IAM. Si le compte n'est pas intégré côté PREVIST, la connexion sera validée par Entra, mais refusée par PREVIST (pas de JIT).

Il est recommandé de désactiver l'affectation requise (actif par défaut), ou dans le cas d'un abonnement P2 ou P3 sur Entra, d'y inclure le groupe utilisé pour le Provisioning vers PREVIST.

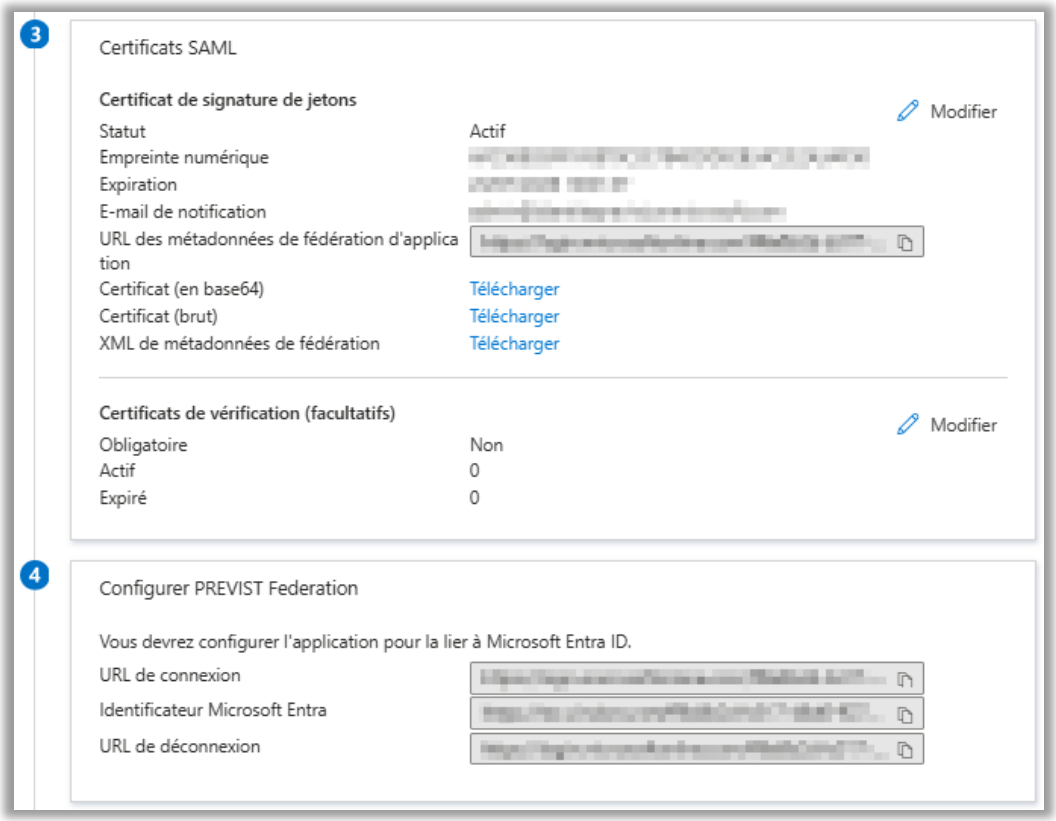
6- Pour désactiver la nécessité d'affecter l'application : Propriété – Affectation requise – Non
6bis- Pour affecter par compte ou par groupe : Utilisateurs et groupes – Ajouter un utilisateur / groupe
Important : ces comptes ou groupes doivent inclure au minimum tous les groupes déjà utilisés côté provisioning - un compte provisionné dans PREVIST mais non affecté à cette application serait bloqué par EntraID avant même d'atteindre PREVIST.

7- Authentification unique – SAML
8- Certificats SAML – Certificat de signature de jetons - Modifier
9- Vérifier la date d'expiration du certificat généré automatiquement, si celle-ci est supérieure à 3 ans, alors le certificat ne sera pas valable.
10- Si le certificat n'est pas valable : Nouveau certificat – Enregistrer – Définir comme certificat actif
Il est possible de renseigner une adresse mail pour recevoir une notification avant l'expiration du certificat.



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

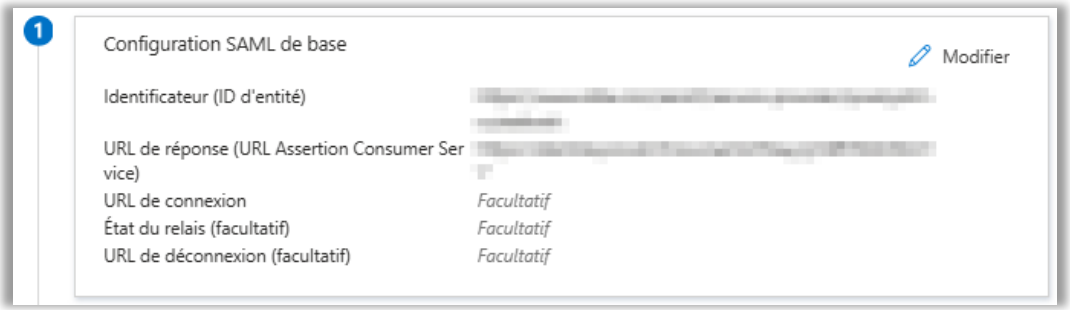
- URL de connexion (encart 4 – Configurer PREVIST Federation)
- Identificateur Microsoft Entra (encart 4 – Configurer PREVIST Federation)
- Certificat en base64 (encart 3 – Certificats SAML)
- URL des métadonnées de fédération d'application (encart 3 – Certificats SAML)



A l'aide de ces éléments, PREVIST acceptera Microsoft comme source de fédération.
L'IAM sera en mesure de récupérer automatiquement le certificat actif depuis les métadonnées à la suite d'une mise à jour sur votre Tenant. Le certificat ne sera pas automatiquement renouvelé (cf §3).

PREVIST vous fournira en retour les éléments à renseigner dans l'encart 1 – Configuration SAML de base :

- Identificateur (ID d'entité)
- URL de réponse (URL Assertion Consumer Service)



3. (Optionnel) Gestion & renouvellement du certificat SAML

Le certificat de signature SAML généré au §2 est valable 3 ans maximum sur EntraID. Ce chapitre propose une solution d'automatisation de son renouvellement pour ne pas dépendre d'une action manuelle (bien que ponctuelle).

PREVIST sera en mesure de récupérer un nouveau certificat paramétré sur le tenant dès lors que les métadonnées auront été communiquées.
PREVIST vérifie quotidiennement l'état des certificats d'après les métadonnées, et intègre automatiquement le certificat actif le cas échéant. Cette action passe par un workflow tournant tous les jours à 5h du matin. Il est recommandé de planifier le renouvellement de votre certificat en fin de journée afin de limiter l'éventuel impact sur les connexions.
Ce workflow enverra une notification par mail à l'admin de l'établissement si le certificat est expiré. L'établissement reste seul maitre de la validité des certificats et peut être notifié par Microsoft de l'approche de la date d'expiration (cf §2 – 10).

Ce chapitre se base sur les paramètres déjà établis dans le renouvellement automatique du secret MGGraph présenté en §12 de la notice Intégration sélective EntraID / PREVIST via Azure Functions.
A ce titre, un abonnement sur le Portail Azure est requis.
Ce chapitre réutilise les accès précédemment paramétrés sur le compte Automation (*§12 b et c).*

Il est possible de générer le renouvellement du certificat par d'autres procédés (Portail Azure, Manuel après notification par Microsoft, Office 365 Power Automate, etc…).

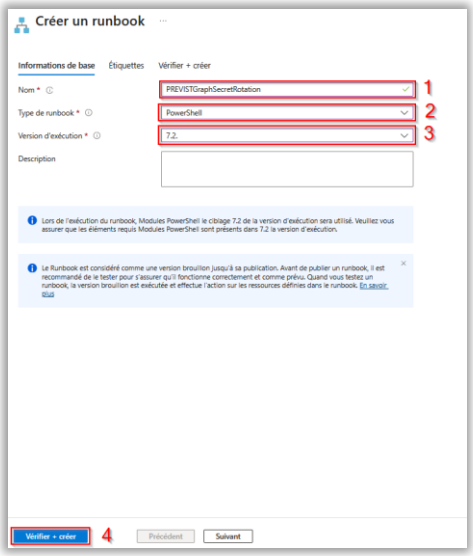
a- Relever l'ID d'Objet de l'application de fédération

Depuis la console Entra – Application d'entreprise, ouvrir l'application PREVIST Federation et copier l' « ID d'objet » dans l'onglet « Vue d'ensemble ».

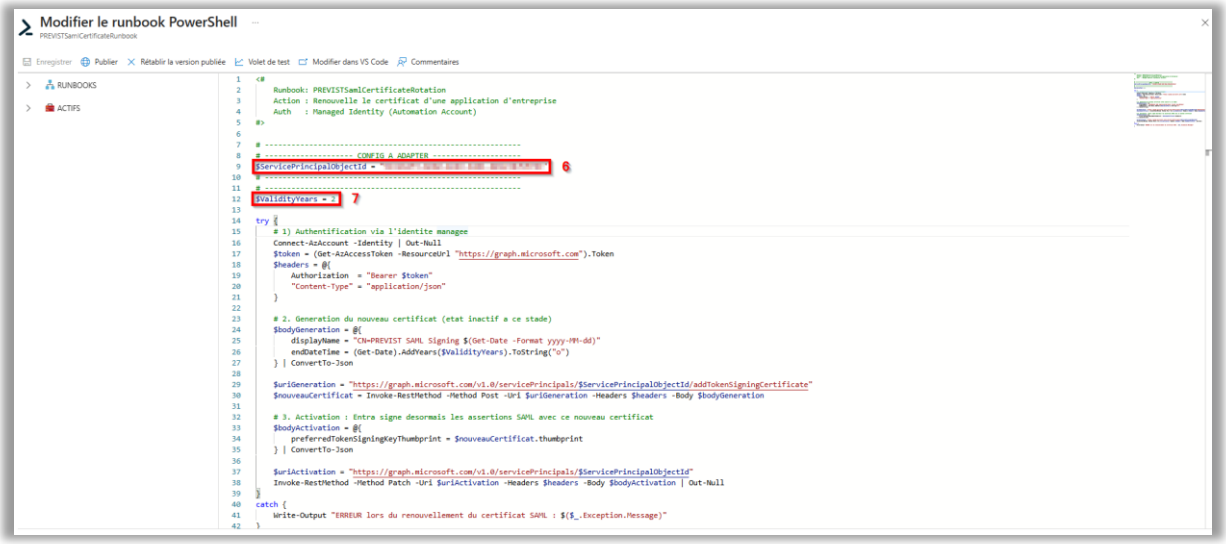
b- Création du Runbook

Depuis le Portail Azure – ouvrir le Compte Automation PREVISTSecretRotation précédemment créé.
Dans le menu Automatisation des processus – Runbooks – Créer un runbook

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



5- Copier le contenu du script PREVISTSamlCertificateRotation.ps1
6- Renseigner l'ID d'objet de l'application d'entreprise retenu en « a- »
7- (Optionnel) Modifier la période de validité du certificat (en années)
8- Enregistrer + Publier

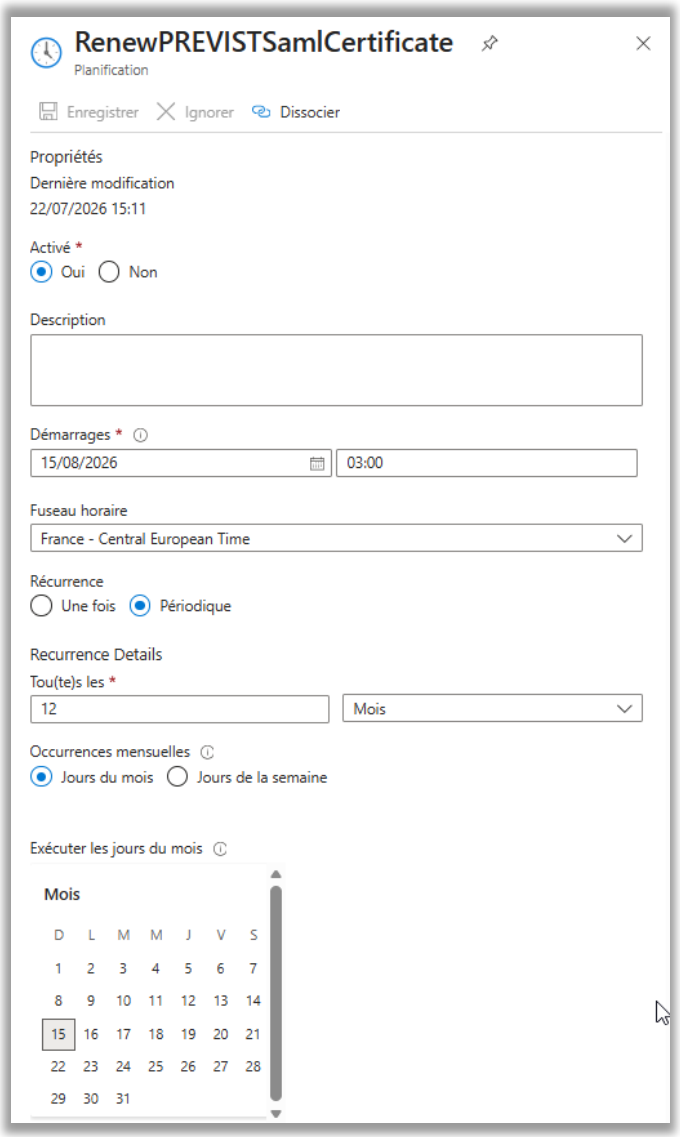


Nb : Le certificat ne peut être utilisé que depuis Okta. Il n'est pas nécessaire de le changer régulièrement.

c- Planification du Runbook

Dans le Runbook en cours, menu Ressources – Planifications – Ajouter une planification

Azure ne permet pas de créer de planification à plus de 500 jours d'écart. Dans le scenario proposé, une planification annuelle offre une marge confortable au regard des 2 ans de validité. Privilégier un horaire hors activité de l'établissement (nuit ou week-end) : PREVIST vérifie l'état des certificats tous les jours à 5h du matin.
Dans cet exemple, le secret sera renouvelé le 15 du mois, tous les 12 mois, à 03h du matin.

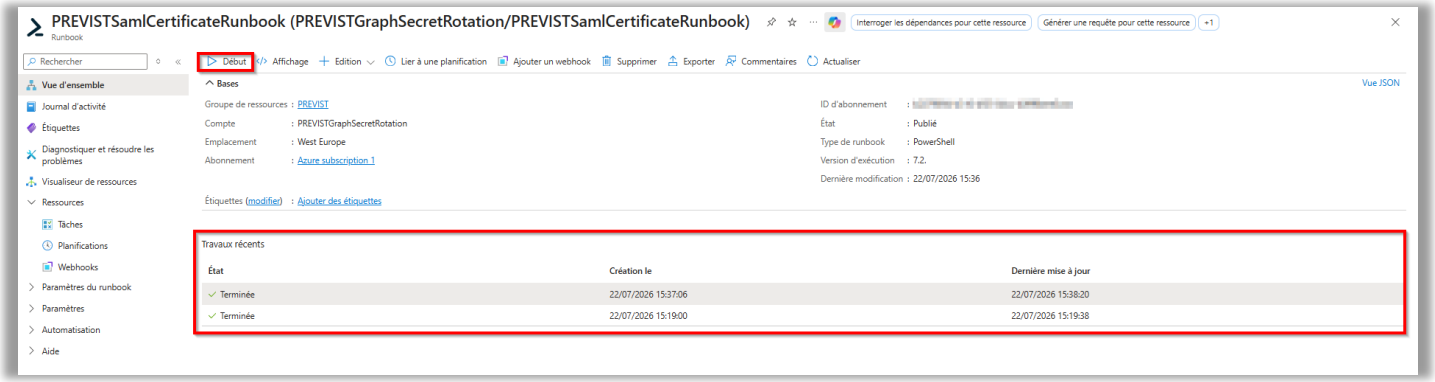


d- Test du Runbook

Le test du Runbook générera un nouveau certificat et invalidera le certificat actif, rendant la connexion sur la plateforme impossible jusqu'à la prochaine vérification des métadonnées par PREVIST (à 5h du matin). Penser à planifier ce test de manière à limiter son impact, ou à rendre le certificat initial actif par la suite.

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.



À la suite du test, vérifier :

- Les logs de sortie de l'exécution
- La création et activation du certificat dans EntraID (cf §2)

4. Annexes

- *Integration_selective_EntraID_PREVIST_via_Azure_Functions_V2.pdf : Notice de paramétrage de l'outil d'intégration des comptes dans PREVIST par EntraID.*
- *Federation_EntraID_PREVIST.pdf: Notice de paramétrage de la Fédération (SSO) par jeton SAML.*
- *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.*
- *WebApp_previst-provisionning.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.*
- *PREVISTSamlCertificateRotation.ps1 : Script permettant la rotation du certificat SAML.*
- *Notice générale PREVIST.pdf*
- *Notice Informatique PREVIST-V2.pdf*
- *Notice RGPD PREVIST_v2.pdf*