## **Compte Rendu du Workshop sur la Migration vers HVault**

**Participants :**

* Sébastien Connor
* Franck Gabon
* Philippe
* Enrique
* Max
* Nevado
* Bryan

**Date :** [À préciser]  
**Sujet :** Migration vers HVault et présentation des solutions possibles

### **Présentation des Quatre Solutions Proposées**

Lors du workshop, un PowerPoint présentant quatre solutions pour la migration vers HVault a été exposé. Voici le récapitulatif des solutions discutées, avec leurs avantages et contraintes.

#### **1. Consultation Humaine via l'Interface HVault**

**Description :**

* Les utilisateurs récupèrent les secrets via l’interface HVault et les partagent manuellement avec les membres des projets Domino.

**Avantages :**

* Simplicité de mise en place.
* Pas de coût supplémentaire.
* Rapidité de mise en œuvre.
* Aucun changement par rapport au processus existant sur la plateforme Domino legacy.

**Contraintes :**

* Interventions humaines nécessaires.
* Accès aux interfaces HVault nécessite des privilèges.
* Moins sécurisé : risque d’échange de mots de passe et secrets via des canaux non sécurisés (Teams, e-mails).

#### **2. Projet dédié à l'Extraction des Secrets**

**Description :**

* Création d’un projet spécifique qui lance des jobs pour récupérer les secrets depuis HVault et les stocker dans un emplacement partagé sur Domino.

#### **3. Projet ou Librairie de Code Source**

**Description :**

* Un projet ou une librairie contenant le code source nécessaire pour se connecter à HVault et récupérer les secrets.
* Les projets Domino incluent cette librairie pour accéder aux secrets.

#### **4. Autonomie des Projets**

**Description :**

* Chaque projet se connecte de manière autonome à HVault via un certificat pour récupérer ses propres secrets et se connecter aux systèmes tiers.

### **Schémas Applicatifs Disponibles**

Des schémas applicatifs illustrant les différentes solutions sont disponibles pour consultation.

### **Processus d'Ajout des Comptes**

* **Processus classique via TOR** pour l’ajout des comptes.
* **Validation managériale obligatoire** pour accéder à HVault (staging et production).
* **Rôles et permissions :**
  + Les membres ayant accès à HVault peuvent créer et sauvegarder des secrets.
  + Les secrets relatifs aux instances tierces (fournis par les équipes d’infrastructure) sont en lecture seule.

### **Secrets REDIS et COS/Bucket**

* Les secrets pour Redis et COS/Bucket sont statiques pour le moment, ce qui favorise le choix de la **solution 1**.
* **Environnements HVault :**
  + **Staging :** Stocke les secrets de DEV et HPROD.
  + **Production :** Stocke les secrets de PROD.
  + Aucun changement prévu pour COS et Redis (toujours 3 environnements).

### **Décision Finale**

À l’issue de la réunion, une **convention commune** a été adoptée pour utiliser la **solution 1** en tant que solution transitoire. Cette décision prend en compte :

* La durée de migration actuelle.
* Les contraintes des projets en cours.

Une transition vers une **utilisation plus mature des API HVault** est prévue pour le **2ème semestre 2025**.

Cette convention nécessite de prévoir des **exceptions** pour permettre des accès HVault en production pour certains comptes.

**Prochaines étapes :**

* Mettre en place les accès nécessaires pour les comptes identifiés.
* Suivre le processus de validation managériale pour ces accès.
* Documenter les étapes pour se connecter et exploiter HVault depuis les pipelines GitLab.

**Fin du compte rendu**.