



# CAHIER DE CHARGE

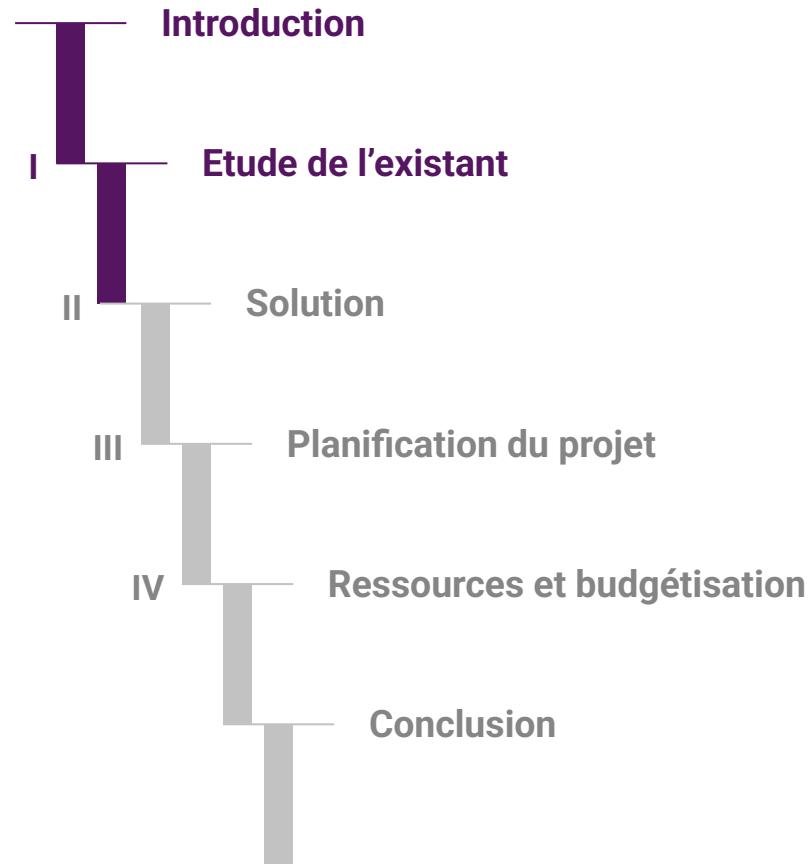
Projet : Gestion des secrets avec Barbican

Groupe 6 :

- ANABA NGOUMOU Rachel
- HARVIS LANDRY Fotseu Fonkwa

Sous la supervision de :  
M. NGUIMBUS Emmanuel

# PLAN



# Introduction

## Pratiques couramment observées



## Risques liés à ces pratiques



# I. Etude de l'existant

## Présentation générale de Barbican

Barbican est le service natif d'OpenStack dédié à la gestion centralisée des secrets à savoir :

- les clés de chiffrement
- les mots de passe
- les certificats
- les données sensibles

## Modes de fonctionnement

- **Synchrone** : Pour les actions simples et rapides, principalement la lecture d'un secret.
- **Asynchrone** : Pour les actions longues ou complexes, comme la création d'un nouveau secret.



# I. Etude de l'existant

## Fonctionnalités de Barbican

### Gestion du cycle de vie des secrets

- Création/ajout
- Lecture/récupération
- Mis à jour/modification
- Suppression
- Stockage
- Gestion des métadonnées associées aux secrets (nom, type, mode, dates d'expiration, etc.).

### Chiffrement et déchiffrement

- Chiffrement avant stockage dans la base de données.
- Déchiffrement à la récupération.

### Accès et administration

- Exposition d'une API, permettant la gestion des secrets par programmation.
- Interaction avec Barbican via des clients Python et des outils en ligne de commande.



### Conteneurisation des secrets

Regroupement des secrets liés dans un conteneur selon des types prédéfinis :

- Certificat
- RSA
- Générique

### Gestion des accès et sécurité

Contrôle des accès aux secrets à partir des listes de contrôles d'accès.

# I. Etude de l'existant

## Services de Barbican



**Barbican-API**

Ce service est une interface simple qui permet à d'autres applications d'interagir avec Barbican. En bref, c'est une porte d'entrée sécurisée pour gérer les secrets.



**Barbican-worker**

Il est en charge de l'exécution des ordres passés à l'API barbican.

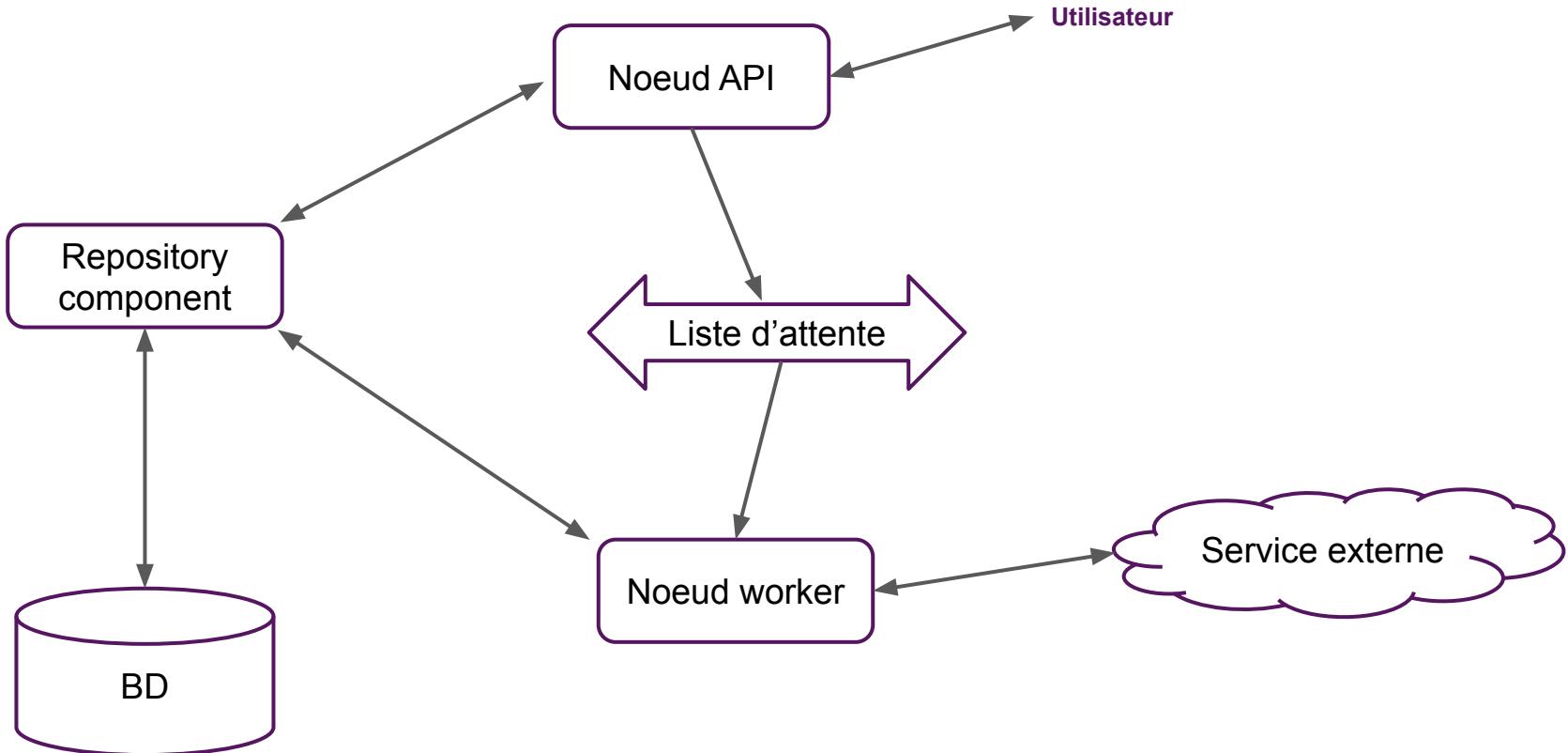


**Barbican-keyston listener  
(optionnel)**

Il met à jour automatiquement la base de données de secrets pour refléter les changements d'utilisateurs et de projets, en s'assurant que seuls les propriétaires ou les personnes autorisées peuvent accéder aux secrets.

# I. Etude de l'existant

## Architecture de Barbican



# I. Etude de l'existant

## Limites de Barbican



### Pas de contrôle d'accès

Barbican ne connaît pas le concept d'application, il donne accès à tous les secrets ou rien.



### Authentification trop complexe

Barbican impose une authentification Keystone complexe, inadaptée et trop lourde pour des applications tierces qui ont besoin d'un accès simple et sécurisé à leurs seuls secrets. Seuls les utilisateurs/services OpenStack ont des comptes



### Renouvellement manuel des secrets

Barbican ne peut pas décider de renouveler un secret lui-même. Il attend qu'on lui donne l'ordre de générer un nouveau secret pour le mettre à jour.

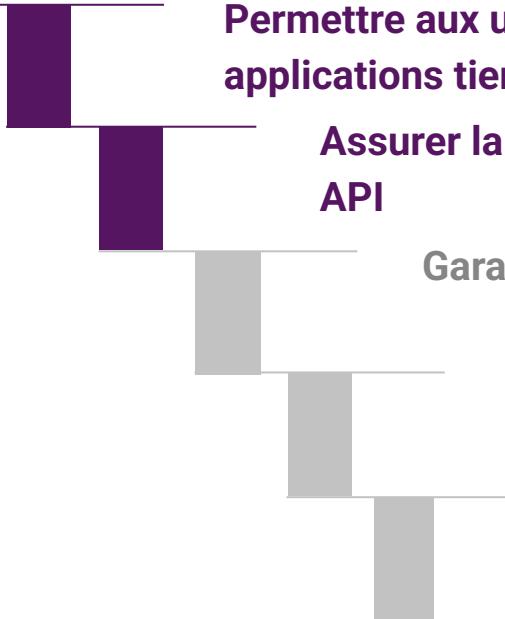


### Absence de notification

Barbican ne dispose pas d'un système de notification intégré pour signaler aux applications et aux utilisateurs que la valeur d'un secret a changé ou pour informer les utilisateurs sur des problèmes rencontrés.

## II. Solution

### Objectifs spécifiques à atteindre



Permettre aux utilisateurs d'intégrer Barbican avec leurs applications tierces

Assurer la validité permanente des certificats SSL/TLS et des clés API

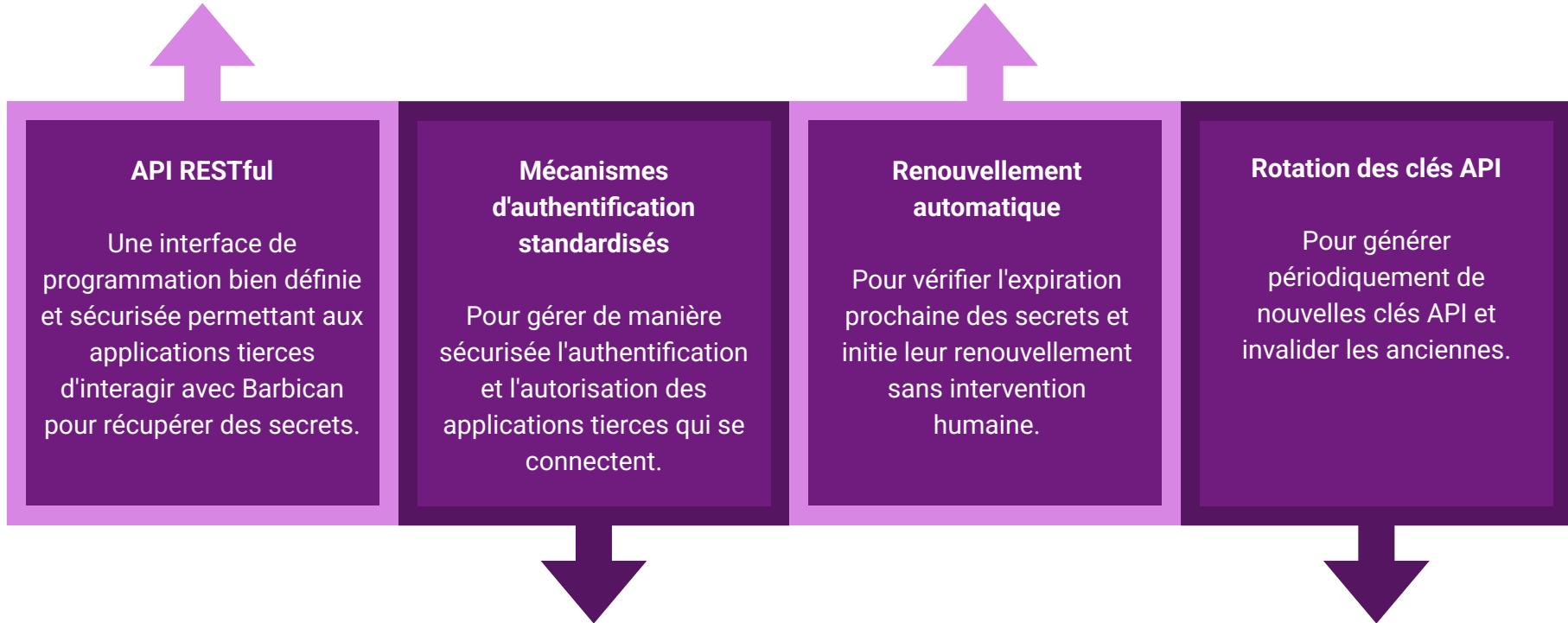
Garantir la traçabilité des événements qui ont lieu dans le système

Permettre aux utilisateurs de manager leurs applications tierces

Informer les utilisateurs sur les événements concernant leurs secrets

# II. Solution

## Fonctionnalités à implémenter



# II. Solution

## Fonctionnalités à implémenter

### Journalisation (Logging) complète

Enregistrement automatique de chaque action effectuée.

### Portail Utilisateur (UI) et tableau de bord

Une interface graphique où les utilisateurs peuvent visualiser, ajouter, supprimer ou révoquer l'accès de leurs applications tierces. Aussi, visualiser les événements récents et l'état de santé des secrets.

### Gestion des permissions

Fonctionnalité permettant à l'utilisateur de définir exactement ce à quoi une application tierce a le droit d'accéder (ex: "accès en lecture seule aux certificats").

### Système d'alertes et de notifications

Fonctionnalité pour envoyer des notifications automatiques (email, SMS) aux utilisateurs lorsque des événements critiques surviennent

# II. Solution

## Livrables attendus

Une plateforme d'intégration

Un orchestrateur

Un guide d'utilisation

Une API

Une application web qui permet à des utilisateurs d'intégrer Barbican à leurs applications et de manager leurs secrets.

Un service qui surveille en permanence les clés API et les certificats SSL/TLS, détecte ceux qui vont expirer, les renouvelle automatiquement, et notifie les utilisateurs les actions menées ou les problèmes rencontrés.

Un guide non-technique, simple et bien structuré expliquant pas à pas comment déployer et utiliser notre solution.

Il s'agit de l'API de notre solution. Elle permettra aux applications tierces de communiquer avec notre solution pour interagir avec Barbican.

## II. Solution

### Comparaison des fonctionnalités

Version actuelle de Barbican	Optimisation
Gestion du cycle de vie des secrets	API RESTful
Conteneurisation des secrets	Mécanismes d'authentification standardisés
Chiffrement et déchiffrement des secrets	Renouvellement automatique
Gestion des accès et sécurité	Rotation des clés API
Accès et administration	Journalisation (Logging) complète
	Portail Utilisateur (UI) et tableau de bord
	Gestion des permissions
	Système d'alertes et de notifications

# III. Planification du projet



▲ LOREM

***Le projet s'étend sur 4 mois, du 04 Octobre 2025 au 30 Janvier 2026.***

# IV. Ressources et budgétisation

## Ressources humaines

Poste	Nombre de personne	salaire jour/homme (en F CFA)	Nombre de jours de travail	Salaire total
Chef de projet	1	10000	12	120 000,00
Analyste	2	10000	7	140 000,00
Concepteurs	2	15000	7	210 000,00
Développeur	2	10000	66	1 320 000,00
Déployeur	1	5000	14	70 000,00
Rédacteur technique	2	5000	14	140 000,00
Monteur de power-points	1	7000	10	70 000,00
<b>TOTAL</b>				<b>2 070 000,00</b>

# IV. Ressources et budgétisation

## Ressources logicielles

Logiciel	Cout
Logiciel de traitement de texte	20 000,00
Logiciel de présentation	20 000,00
Logiciel de conception	50 000,00
Environnement de développement intégrée	25 000,00
<b>Total</b>	<b>115 000,00</b>

# IV. Ressources et budgétisation

## Ressources matérielles

Matériel	Quantité	Coût unitaire / journalier	Nombre de jour d'utilisation	Coût total
Ordinateur performant	2	575 000	/	1 150 000,00
Connexion internet (en Go)	10	3 000	115	345 000,00
<b>TOTAL</b>				<b>1 495 000,00</b>

# Conclusion

Barbican est le service de gestion des secrets d'Openstack. Il est très efficace mais également limité au niveau :

- du contrôle d'accès
- de l'authentification
- du renouvellement des secrets
- des notifications

Les livrables attendus sont :

- Une plateforme d'intégration
- Un orchestrateur
- Un guide d'utilisation
- Une API



Pour palier à ces limites, notre solution devra :

- Fournir une interface graphique pour l'intégration de Barbican avec des applications tierces et pour la gestion de leurs secrets
- Assurer la validité permanente des certificats SSL/TLS et des clés API
- Notifier les utilisateurs sur les événements qui surviennent

La réalisation de ce projet se déroulera sur 4 mois allant du 04 Octobre 2025 au 30 Janvier 2026.