Gestion des Habilitations SailPoint

Gildas CHERAUD BOISTEAU

BTS Service Informatique aux Organisations option SISR

Sommaire

1. Descriptif

1.1 Description du service

Le service de gestion des habilitations permet de contrôler, attribuer et révoquer les accès aux ressources informatiques de l'entreprise, afin de garantir que chaque utilisateur dispose uniquement des droits nécessaires à ses missions.

1.2 Descriptif Technique et Gouvernance

La gestion des habilitations chez Nickel repose sur une solution d'**IAM (Identity and Access Management)** nommée SailPoint. Dans un environnement bancaire régi par une politique **"Zero Trust"**, aucun accès n'est accordé par défaut.

Le rôle du technicien :

Provisioning : Je participe à la mise à disposition des ressources applicatives en fonction des besoins réels des collaborateurs.

Workflow d'approbation : Chaque demande d'accès supplémentaire doit être initiée par un manager via SailPoint, garantissant une validation métier systématique avant toute intervention technique.

Moindre privilège : En tant que Technicien IT Workplace, je dispose moi-même d'un ensemble de droits spécifiques et limités, nécessaires à l'exercice de mes missions.

1.3 Objectif du service

L'objectif du service est d'assurer un accès sécurisé et maîtrisé aux applications et aux ressources du système d'information, tout en respectant les exigences de sécurité et de conformité.

1.4 Utilisateurs concernés

Ce service concerne l'ensemble des collaborateurs de l'entreprise, ainsi que les managers responsables de la validation des demandes d'accès.

1.5 Recensement des ressources

Les ressources mobilisées pour ce service sont :

- La solution IAM SailPoint
- L’annuaire Active Directory
- Les applications métiers internes
- Les comptes utilisateurs et groupes de sécurité

2. Analyse du Processus d'Habilitation

L'interface SailPoint permet une vision consolidée de l'identité numérique d'un collaborateur à travers plusieurs onglets techniques : **Attributs**, **Droits**, et **Comptes applicatifs**.

Méthodologie d'intervention :

Réconciliation : Le système vérifie la concordance entre les droits déclarés dans SailPoint et les comptes réellement présents sur les applications cibles (comme l'Active Directory).

Gestion des comptes : La section "Comptes applicatifs" permet de suivre l'état (Statut) et la date de dernière actualisation de chaque accès, assurant ainsi une hygiène informatique constante .

Principe d'approbation unique : SailPoint fonctionne sur un modèle où chaque droit est auditable, ce qui permet de répondre aux exigences de conformité du groupe BNP Paribas.

En tant que technicien Workplace, je n’initie pas les demandes d’habilitation : celles-ci sont exclusivement créées et validées par les managers. Mon rôle intervient après validation, pour le contrôle, la cohérence, l’application et la vérification des droits.

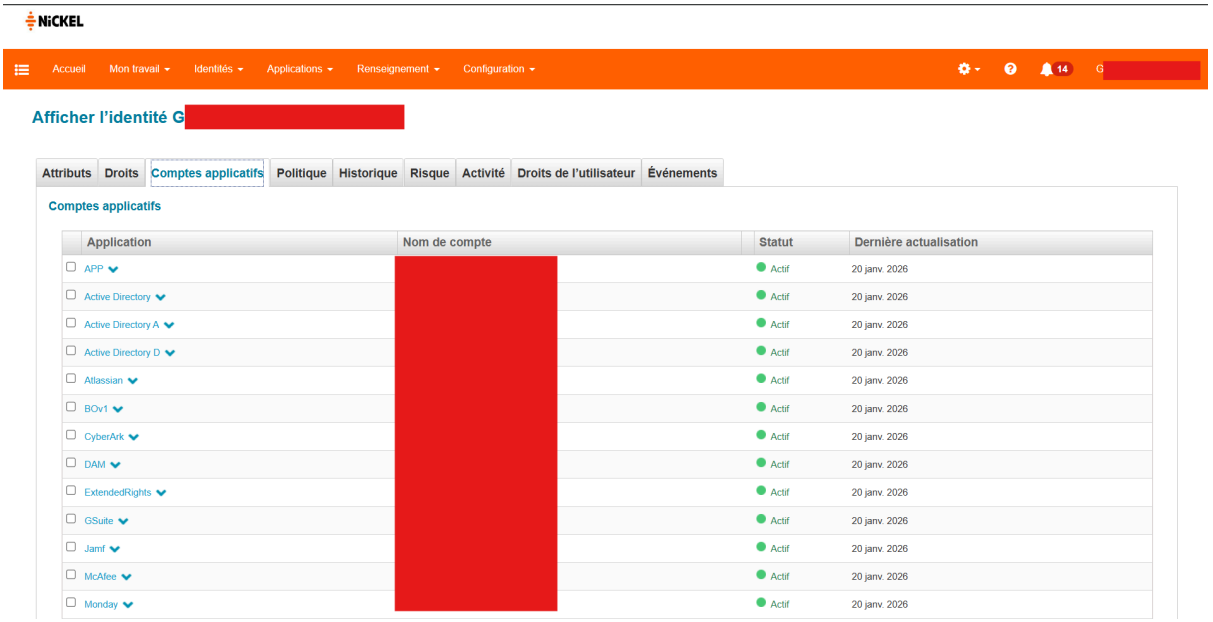
3. Sécurité et Traçabilité Bancaire

L'utilisation de SailPoint est une mesure de sécurité active visant à réduire la surface d'attaque de l'organisation :

Traçabilité : L'historique et les événements liés à une identité sont enregistrés, permettant de savoir précisément qui a autorisé un droit et quand il a été activé.

Contrôle de conformité : En cas de changement de poste ou de départ, le système facilite la révocation immédiate des accès, évitant ainsi la persistance de "comptes dormants".

Auditabilité : Le traitement des demandes d'habilitations fait l'objet d'un suivi rigoureux pour répondre aux besoins de contrôle interne propres à un établissement financier .



4. Procédure de gestion d'une habilitation

1. Une demande d'accès est initiée par le manager via SailPoint.

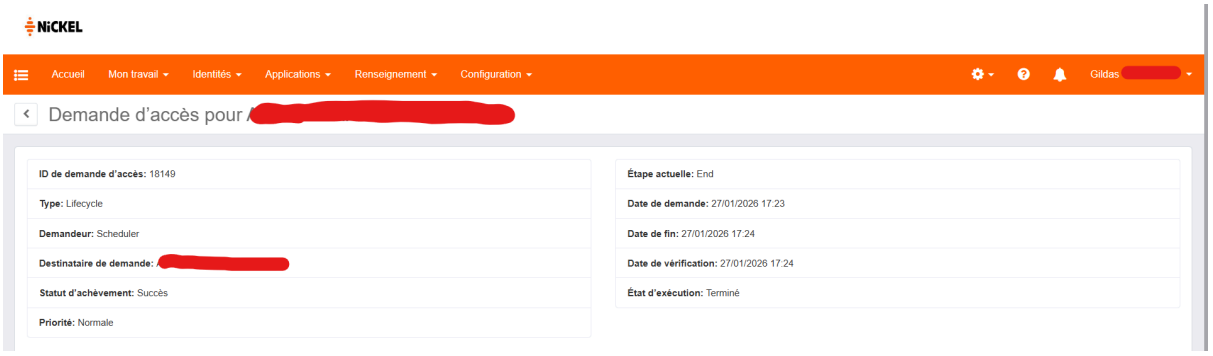
2. La demande est validée selon le workflow d'approbation défini.

3. Je vérifie la cohérence du droit demandé avec le poste de l'utilisateur.

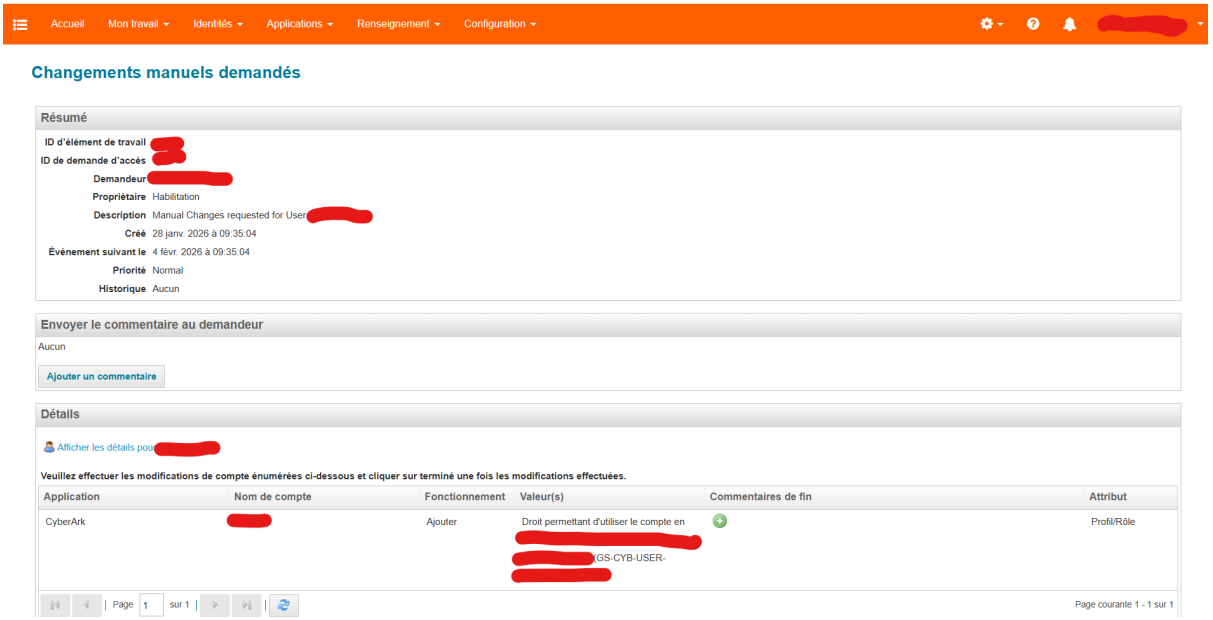
4. Le droit est attribué ou révoqué via SailPoint.

5. Je vérifie l'application effective du droit sur l'annuaire ou l'application cible.

6. L'opération est tracée et historisée.



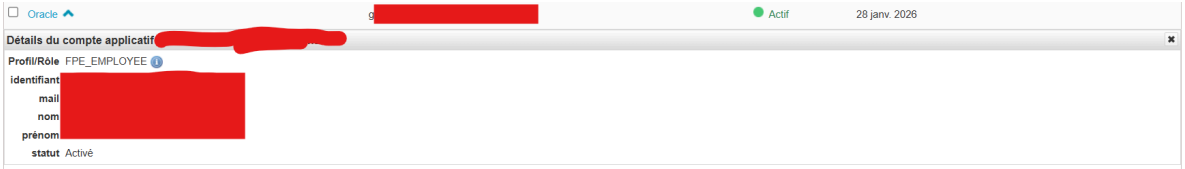
Demande d’accès validée dans SailPoint. Cette vue permet de vérifier l’origine de la demande, le type de workflow (lifecycle), son statut d’achèvement et les dates de traitement.



Détail des modifications d’habilitation à effectuer. Cette vue permet de contrôler l’application concernée, le rôle demandé et le type d’action (ajout ou retrait de droit) avant exécution.

5. Vérification, sécurité et traçabilité

Après chaque modification, je vérifie que les droits montrent uniquement les accès nécessaires, conformément au principe du moindre privilège. Les actions réalisées sont historisées afin de permettre des contrôles ultérieurs et des audits de conformité.



Vérification de l’application effective de l’habilitation. Le compte applicatif est actif et le rôle attribué correspond à la demande validée.

6. Exploitation et continuité du service

Le service de gestion des habilitations est utilisé quotidiennement pour les arrivées, mobilités et départs des collaborateurs. En cas de dysfonctionnement, une intervention rapide permet d’éviter tout blocage d’accès aux outils de travail.

7. Lien avec le support

En cas de problème d’accès ou de droits insuffisants, une demande est prise en charge par le support afin de restaurer rapidement l’accès nécessaire à l’utilisateur.

8. Conclusion

Cette réalisation démontre ma capacité à **gérer des services informatiques** dans un cadre hautement sécurisé. En maîtrisant l'outil **SailPoint**, je garantis que le patrimoine applicatif de **Nickel** est protégé par une gestion granulaire des accès. Cette compétence est fondamentale pour assurer la confidentialité et l'intégrité des données au sein du **Système d'Information**.