



Ecole Nationale des Sciences Appliquées



## RAPPORT DE PROJET DE FIN D'ÉTUDES

Filière : Réseaux et systèmes de télécommunications

# Etude et implémentation d'une initiative Zero Trust basé sur MFA et IGA

Effectué à :

Orange Cyberdefense

Réalisé par :

ZANNOUTI Hamza

Encadré par :

Encadrant Pédagogique : Pr MADINI Zhour

Maitre de Stage :

Mme AIT EL HADJ Sana

Mr BENNANI Hamza

Soutenu le 14 juin 2023      Devant le jury :

Pr. MADINI Zhour : Professeur de l'enseignement supérieur, ENSA Kénitra

Pr. MAZRI Tomader : Professeur de l'enseignement supérieur, ENSA Kénitra

Pr. SAAD Aouatif : Professeur de l'enseignement supérieur, ENSA Kénitra

Pr. ZIAD Nadia : Professeur de l'enseignement supérieur, ENSA Kénitra

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ  
قَالَ رَبِّي شَرِحَ لِي مَرِيدٌ وَسِيرَلَاهُ مَرِيدٌ  
وَلَمْ يَلْعَجْ عَقْدَكَ فَرِسْبَانِي فَقَهْلَاهُ مَرِيدٌ

## DÉDICACES

À ALLAH le tout puissant, le miséricordieux, seul détenteur  
du savoir et maître du destin.

À mes oncles, tantes, cousins et cousines :

*Dédicaces*

Que cette thèse soit pour vous le témoignage de mes sentiments les plus sincères et  
les plus affectueux. Je vous souhaite à tous longue vie pleine de bonheur et de  
prospérité

**À tous mes amis, qui ont toujours été là pour moi à mes côtés :**

Je vous souhaite un avenir plein de réussite.

*Remerciements*

## **REMERCIEMENTS**

Je tiens à exprimer ma profonde gratitude envers la **Professeure MADINI Zhour**, notre chef de filière, et mon encadrante pédagogique pour ses précieuses recommandations, critiques et conseils tout au

long de l'élaboration de ce rapport. Je souhaite également remercier chaleureusement les membres du jury pour avoir accepté d'évaluer mon travail.

Je tiens à remercier tout particulièrement et à témoigner toute ma reconnaissance à mes encadrants professionnels : **Mme AIT EL HADJ Sana**, team leader build&run Maroc & Afrique francophone, **M. BENNANI Hamza**, Consultant en cybersécurité chez Orange Cyberdefense, **M. BENZAIM Naoufal**, Directeur Solution de Confiance Maroc & Afrique francophone, pour leurs conseils précieux et leur aide tout au long de mon stage. Je les remercie également de m'avoir intégré rapidement au sein de l'entreprise et de m'avoir accordé leur confiance, pour le temps qu'ils ont bien voulu me consacrer afin de répondre à mes interrogations, et pour leurs conseils pertinents qui m'ont énormément aidé à mener à bien ma mission.

Je tiens également à remercier l'ensemble des collaborateurs de la société Orange Cyberdefense, et tout particulièrement l'équipe Solution de Confiance, pour leur aimable accueil et leur sympathie.

Je souhaite exprimer ma sincère gratitude envers toute l'équipe pédagogique de la filière "Réseaux et Systèmes de Télécommunications" ainsi que le corps professoral de l'École Nationale des Sciences Appliquées de Kénitra pour leur formation de qualité et leur encadrement répondant aux attentes des futurs ingénieurs. Mes remerciements vont également à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce travail. Qu'ils trouvent ici l'expression de ma plus profonde gratitude.

## Table des matières

DÉDICACES.....	3
REMERCIEMENTS .....	6
LISTE DES TABLEAUX ET FIGURES .....	9
LISTE DES NOTATIONS ET ACRONYMES .....	11
RÉSUMÉ .....	13
ABSTRACT .....	14
INTRODUCTION GENERALE .....	15
CHAPITRE I – Contexte Général du Projet .....	16
INTRODUCTION.....	17
1. Présentation de l'entreprise d'accueil et du stage .....	17
1.1. Orange Cyberdefense au sein du groupe Orange .....	17
1.2. Orange Cyberdefense en quelques chiffres .....	18
1.4 Expertises et offres .....	18
1.5 Appartenance d'OCD Maroc au Groupe Orange.....	23
1.6 Partenaires locaux et étrangers .....	23
2. Contexte du projet .....	24
2.1. Contexte général .....	24
2.2. Problématique .....	24
2.3. Objectifs du projet .....	24
2.4. Organisation et plan du projet .....	25
2.5. Plan de projet .....	25
CONCLUSION .....	27
CHAPITRE 2 – État de l'Art .....	28
INTRODUCTION.....	29
1. Zero Trust .....	29
1.1. Historique .....	29

1.2.	Définition .....	29
1.3.	Avantages de Zero Trust .....	30
1.4.	Principes du Zero Trust .....	30
1.5.	Composants clés de Zero Trust .....	31
1.6.	Architecture Zero Trust selon NIST .....	32
1.7.	Limites de Zero Trust .....	34
2.	Identity and Access Management .....	35
2.1.	Définition .....	35

*Table des matières*

2.2.	Eléments de l'IAM .....	35
2.2.1	Magasin d'identité .....	36
2.2.2	Cycle de vie de l'identité .....	38
2.2.3	Gestion d'accès .....	39
	CONCLUSION .....	41
	CHAPITRE 3 – Etude comparatif et présentation des solutions .....	42
	INTRODUCTION.....	43
1.	Multiple Factor Authentication (MFA) .....	43
1.1	Définition : .....	43
1.2	Avantages : .....	43
1.3	Les type de la MFA : .....	43
1.4	MFA et Zero Trust : .....	44
2.	Identity Governance and Administration (IGA) .....	44
2.1	Définition .....	44
2.2	Avantages .....	45
2.3	IGA et Zero Trust .....	46
3.	Benchmark des solutions MFA et IGA .....	47
3.1	Solutions MFA .....	47
3.2	Solutions IGA .....	50
4.	Présentation des solutions choisies .....	51

4.1	SafeNet Authentication Service Private Cloud Edition (SAS PCE) .....	51
4.2	SailPoint IdentityIQ .....	53
4.3	Architecture de la solution .....	55
	CONCLUSION .....	56
	Chapitre 4 Implémentation et test des solutions .....	58
	INTRODUCTION.....	59
1.	Présentation du laboratoire .....	59
2.	Architecture des solutions choisies .....	60
3.	Prérequis pour le déploiement .....	63
4.	Implémentation de SAS PCE : .....	64
5.	Simulation de la MFA : .....	70
6.	Mise en place de SailPoint IdentityIQ : .....	72
	CONCLUSION .....	82
	Conclusion Générale et perspectives.....	83
	BIBLIOGRAPHIE .....	84

*Liste des tableaux et figures*

## LISTE DES TABLEAUX ET FIGURES

Tableau **4.1** : Prérequis systèmes de SAS PCE

Tableau **4.2** : Prérequis logiciels de SAS PCE

Tableau **4.3** : Matrice des flux Réseau

Figure **1.1** : Logo Orange Cyberdefense

Figure **1.2** : Orange Cyberdefense en quelque chiffres

Figure **1.3** : Business Units

Figure **1.4** : Les huits pôles de compétence d'audit et conseil

Figure **1.5** : Une couverture complète

Figure **1.6** : Groupe Orange

Figure **1.7** : Partenaires d'Orange Cyberdefense

Figure **1.8** : Diagramme de Gantt

Figure **2.1** : Principes du Zero Trust

Figure **2.2** : Architecture Zero Trust propose par la NIST

Figure **2.3** : Les éléments d'un système IAM

Figure **2.4** : Cycle de vie d'un utilisateur

Figure 3.1 : MFA  
Figure 3.2 : IGA  
Figure 3.3 : Méthodes d'authentification supporté par SAS PCE  
Figure 3.4 : Workflow automatisé  
Figure 3.5 : Vision globale sur la solution  
Figure 3.6 : Architecture de la solution SailPoint IdentityIQ

Figure 4.1 : Architecture du lab  
Figure 4.2 : Architecture du SAS PCE  
Figure 4.3 : Architecture globale de SailPointIQ  
Figure 4.4 : Installation du rôle IIS  
Figure 4.5 : Installation de MySQL  
Figure 4.6 : Création des utilisateurs sur chacune des bases de données  
Figure 4.7 : Liste des utilisateurs sur MySQL  
Figure 4.8 : Configuration de database  
Figure 4.9 : Création du compte OCD  
Figure 4.10 : Site export  
Figure 4.11 : Rôle NPS dans Windows Server  
Figure 4.12 : Installation de l'agent SafeNet pour NPS  
Figure 4.13 : Page de Self Enrollment  
Figure 4.14 : Les étapes d'authentification

*Liste des tableaux et figures*

Figure 4.15 : Processus de l'authentification à l'aide de OTP  
Figure 4.16 : Authentification avec succès  
Figure 4.17 : Page d'accueil de SailPoint IdentityIQ  
Figure 4.18 : Définition des deux applications de référence  
Figure 4.19 : Résultat de la tâche d'agrégation  
Figure 4.20 : Identity Warehouse  
Figure 4.21 : adam Kennedy cube d'identité  
Figure 4.22 : On-Boarding des deux applications de référence  
Figure 4.23 : Résultat de rapport des utilisateurs non corrélé  
Figure 4.24 : Résolution manuelle des comptes non corrélé  
Figure 4.25 : Mise en place du policy de séparation des tâches  
Figure 4.26 : La règle de séparation des tâches  
Figure 4.27 : Résultat dela policy SoD  
Figure 4.28 : Mail de violation envoyé au manager  
Figure 4.29 : Policy violations  
Figure 4.30 : Correct violation  
Figure 4.31 : Création de la compagne de certification d'accès  
Figure 4.32 : Exécution de la compagne  
Figure 4.33 : Examen d'accès

*Liste des notations et acronymes*

## **LISTE DES NOTATIONS ET ACRONYMES**

MFA	Multi-Factor Authentication
IGA	Identity Governance and Administration
OCD	Orange CyberDefense
JIT	Just In-time Access
JEA	Just Enough Access
IDaaS	Identity As A Service
IETF	Internet Engineering Task Force
API	Application Programming Interface
RFC	Request for Comments

IAM	Identity and Access Management
LDAP	Lightweight Directory Access Protocol
PA	Policy Administration
ZTA	Zero Trust Access
ZTX	Zero Trust eXtended
NIST	National Institute of Standards and Technology
SSO	Single Sign-On
USB	Universal Serial Bus
BU	Business Unit
RADIUS	Remote Authentication Dial-In User Service
SAML	Security Assertion Markup Language
OAuth2	Open Authentication 2
<i>Liste des notations et acronymes</i>	
OIDC	Open ID Connect
FIDO	Fast Identity Online
PAM	Privileged Access Management
NGFW	Next Generation Firewall
UEBA	User & Entity Behaviour Analytics
DLP	Data Loss Prevention
MS SQL	Microsoft SQL
SAS PCE	SafeNet Authentication Service Private Cloud Edition
OCD	Orange Cyberdefense
HR	Human Resources
CSV	Comma-separated Values

PKI	Public Key Infrastructure
XML	Extensible Markup Language
HTTP	HyperText Transfer Protocol
2FA	Two Factor Authentication
OTP	One Time Password
PIN	Personal Identification Number
VLAN	Virtual Local Area Network
DMZ	Demilitarized Zone
ESG	Environmental Social Governance
RGPD	Règlement Général pour la Protection des données

#### *Résumé*

Avec l'évolution rapide des travailleurs mobiles et distants, du BYOD et des services cloud, ainsi que l'impact des pandémies, les entreprises sont confrontées à de nouveaux défis en matière de sécurité, notamment face aux attaques sophistiquées perpétrées par des cybercriminels, que la sécurité traditionnelle est incapable de les adresser.

Dans ce contexte, le modèle de sécurité Zero Trust se positionne comme une approche prometteuse pour contrer ces menaces. Fondé sur le principe de "ne jamais faire confiance, toujours vérifier", il renforce la protection des données sensibles en mettant en place des mécanismes d'authentification rigoureux et une surveillance continue des activités suspectes.

Dans le cadre de ce projet de stage, notre objectif était d'étudier en profondeur ce modèle et de proposer une architecture basée sur les technologies MFA et IGA pour aider les entreprises à renforcer leur posture de sécurité et à se prémunir contre les cyberattaques.

Mots clés : BYOD, Zero Trust, authentification, surveillance continue, MFA, IGA

*Abstract*

## **ABSTRACT**

With the rapid evolution of mobile and remote workers, BYOD, and cloud services, as well as the impact of pandemics, businesses are facing new security challenges, particularly in the face of sophisticated attacks by cybercriminals.

In this context, the Zero Trust security model emerges as a promising approach to counter these threats. Based on the principle of "never trust, always verify," it strengthens the protection of sensitive data by implementing rigorous authentication mechanisms and continuous monitoring of suspicious activities.

In the scope of this internship project, our goal was to deeply study this model and propose an architecture based on MFA (Multi-Factor Authentication) and IGA (Identity Governance and Administration) technologies to help businesses enhance their security posture and defend against cyberattacks.

Keywords: BYOD, Zero Trust, authentication, continuous monitoring, MFA, IGA.

*Introduction générale*

## **INTRODUCTION GENERALE**

Alors que les organisations déplacent la plupart de leurs charges de travail vers le Cloud et que le travail à distance devient de plus en plus courant, les réseaux d'entreprise sont confrontés à des menaces croissantes, tant internes qu'externes. Le modèle de sécurité périmétrique traditionnel, qui suppose que les attaques proviennent principalement de l'extérieur, est de plus en plus remis en question. Dans ce contexte, le modèle Zero Trust se positionne comme une approche prometteuse pour renforcer la sécurité des réseaux.

Le modèle Zero Trust repose sur le principe fondamental selon lequel aucune entité, qu'elle soit interne ou externe, ne peut être automatiquement digne de confiance. Au lieu de cela, il adopte une approche de "ne jamais faire confiance, toujours vérifier". Cette approche renforce la protection des données sensibles en mettant en place des mécanismes d'authentification rigoureux et en surveillant en permanence les activités suspectes.

Dans le cadre de mon projet de stage, je me suis concentré sur l'étude approfondie du modèle Zero Trust et la proposition d'une initiative visant à mettre en œuvre un système IAM (Identity and Access Management) robuste. Un système IAM solide est une composante essentielle de tout projet Zero Trust, car il permet de gérer de manière centralisée les identités et les accès, de renforcer les mécanismes d'authentification, de contrôler les autorisations et de surveiller les activités des utilisateurs.

Ce rapport présente une synthèse des différentes étapes du travail réalisé, structuré en quatre chapitres. Le premier chapitre introduit le contexte général du projet, en mettant en évidence les défis actuels liés au déplacement vers le Cloud et au travail à distance. Le deuxième chapitre se concentre sur l'étude approfondie du modèle Zero Trust et de ses principes fondamentaux. Le troisième chapitre explore les solutions IAM disponibles sur le marché et propose une évaluation comparative pour choisir la solution la plus adaptée. Enfin, le quatrième chapitre présente l'implémentation des solutions choisis.

## **CHAPITRE I – Contexte Général du Projet**

## **CHAPITRE I – Contexte Général du Projet**

Dans ce chapitre, nous allons présenter de l'entreprise d'accueil en précisant ses chiffres clés, ses offres et expertises en plus des objectifs et l'organisation du projet et un planning sous forme de diagramme de Gantt.

## INTRODUCTION

Dans ce premier chapitre, nous allons présenter l'activité principale de l'organisation d'accueil, et de contextualiser notre projet. A cet égard, une description de l'entreprise sera faite, puis une définition détaillée du cadre de travail, avec une clarification des objectifs du projet ainsi que la démarche que nous avons opté pour réaliser le présent projet.

### 1. Présentation de l'entreprise d'accueil et du stage



Figure 1.1 : Logo Orange Cyberdefense

Dans un contexte où les menaces sont en progression et toujours plus ciblées, la sécurité est un enjeu partagé par toutes les directions au sein de l'entreprise. Convaincus que la cyber sécurité est un des axes prioritaires de croissance, Orange fait le choix à travers son entité Orange Cyberdefense de développer une approche globale et proactive de la sécurité.<sup>[1]</sup>

#### 1.1. Orange Cyberdefense au sein du groupe Orange

Le Groupe Orange a des préoccupations et des enjeux similaires à ceux de ses clients. Il est également la cible d'attaques, de malveillances informatiques et de fuites de données. En qualité d'opérateur Télécoms et d'hébergeur, il est soumis à des obligations de continuité de services et doit protéger à la fois ses données et celles de ses clients. Orange Business a défini la cyber sécurité comme un de ses axes stratégiques prioritaires ; c'est pourquoi les expertises en cyber sécurité ont été réunies au sein d'Orange Cyberdefense, filiale à 100 % du groupe Orange. Ainsi, fort de son appartenance à un opérateur télécoms mondial, Orange Cyberdefense dispose d'une position privilégiée sur le marché de la sécurité numérique notamment pour détecter les signaux faibles et les attaques des SI des organismes qu'elle

## CHAPITRE I – Contexte Général du Projet

supervise. Elle dispose de capacités uniques pour neutraliser des attaques de types dénis de service et intervient largement dans la protection des SI d'Orange et dans la protection des données personnelles de ses abonnés.

### 1.2 Orange Cyberdefense en quelques chiffres



Figure 1.2 : Orange Cyberdefense en quelque chiffres

### 1.4 Expertises et offres

Chacune des attentes clients étant singulière, Orange Cyberdefense a la capacité de proposer différents modèles de services (intégré, managé et/ou hébergé). Orange Cyberdefense est partenaire des acteurs incontournables du marché et s'associe également à des éditeurs technologiques innovants et ambitieux. L'expertise Orange Cyberdefense est partagée en 3 Business Units



Figure 1.3 : Business Units

#### □ Business unit « Conseil & Audit »

##### Les expertises :

Les clients d'Orange Cyberdefense bénéficient d'une expertise accumulée au cours des 20 dernières années dans le domaine du conseil et de l'audit, ce qui leur permet de réussir leur transformation digitale. Une approche pragmatique est développée en prenant en compte en amont les objectifs de sécurité, en les alignant sur les enjeux, le contexte et la stratégie de chaque entreprise. Les pratiques et les usages sont également pris en compte, cherchant à trouver un équilibre entre ce qui est souhaitable et ce qui est réalisable. Cet accompagnement est enrichi par les retours terrain partagés par les collègues d'autres directions d'Orange Cyberdefense, qui déploient et analysent quotidiennement des solutions de sécurité pour les clients. L'objectif est de construire des relations durables avec les clients en mettant en place un système de gestion de la sécurité évolutif et adapté à l'organisation et à la structure de l'entreprise. La volonté est de s'inscrire dans une démarche d'amélioration continue de la sécurité chez les clients.

##### Les offres :

Le business Unit Conseil & Audit d'Orange Cyberdefense est organisée en 8 pôles de compétence :

## CHAPITRE I – Contexte Général du Projet



Figure 1.4 : les huits pôles de compétence de la bu audit et conseil

### □ Business unit « Solutions de confiance » Les expertises :

La sécurité des communications exige de s'appuyer sur des solutions et des équipements de confiance. Nous vous apportons les technologies et les analyses les plus performantes en la matière en fonction de vos besoins. A travers les 500 collaborateurs de sa BU solutions de confiance, Orange Cyberdefense accompagne la transformation digitale des entreprises et ainsi vise à :

- ✓ Sécuriser les migrations vers le Cloud
- ✓ Sécuriser les infrastructures tout en assurant leur performance et leur optimisation
- ✓ Faciliter l'évolution des organisations en anticipant les impacts organisationnels et SI
- ✓ Accélérer les projets d'ouverture du SI à des partenaires de confiance
- ✓ Déléguer l'attribution et le cycle de vie des habilitations aux responsables métiers

### Les offres :

#### Sécurisation du Datacenter :

A travers des solutions de virtualisation ou des équipements dédiés, nous mettons en œuvre des Systèmes de protection des intrusions, des pare-feux hauts débits, des pare-feux applicatifs, des produits protégeant des dénis de service.

#### Plateforme d'accès internet :

## *CHAPITRE I – Contexte Général du Projet*

Ces plateformes garantissent la protection des accès à internet, via des pare-feux de nouvelles générations, des solutions de protection des mails et du Web.

### Protection des réseaux :

Ces solutions contrôlent l'accès des postes de travail et des utilisateurs aux réseaux et aux applications et permettent la segmentation des flux.

### Traitement de la mobilité sécurisée :

Nous assurons la sécurité des terminaux, la confidentialité des communications et l'accès distant des collaborateurs en mobilité à leur environnement de travail.

### Sécurisation des postes de travail :

Nous déployons différentes technologies de protection des endpoints contre les nombreux vecteurs d'attaques (emails, clés USB, intrusions ciblées...).

### Sécurisation de l'utilisateur :

Nous proposons des formations et des outils de sensibilisation des utilisateurs aux risques de sécurité.

### Gestion de l'Identité :

- ✓ Gestion du cycle de vie des identités (arrivée, départ, mutation, etc.)
- ✓ Gestion des modèles et demandes d'habilitations (définition des comptes applicatifs et des droits associés)
- ✓ Contrôles, revue des droits et séparation de pouvoirs (campagne de recertification des droits et comptes)
- ✓ Fédération d'identité & signature unique (SSO) pour l'ouverture du SI à des tiers de confiance et améliorer l'expérience utilisateur

### **Business unit « Contrôle, Surveillance et réactivité » :**

## **Une couverture complète et cohérente de la cybermane 24/7 365**

Fort de la première base de threat intelligence d'Europe, nous anticipons les menaces et opérons les défenses de nos clients pour perturber, contenir, et répondre aux attaques visant les actifs sensibles que nous surveillons.



Figure 1.5 : Une couverture complète

Orange Cyberdefense dispose de :

- ✓ 2 CyberSocs qui rassemblent la meilleure expertise en analyse de menace,
- ✓ 6 SOC répartis dans le monde qui surveillent et réagissent aux événements 24/7/365,
- ✓ 3 CERT qui mobilisent ses experts en intervention d'urgence et en cyber intelligence afin d'anticiper et de riposter aux attaques, dont un CSIRT (Computer Security Incident Response Team)
- ✓ 2 scrubbing centers pour réduire les attaques DDoS

## 1.5 Appartenance d'OCD Maroc au Groupe Orange

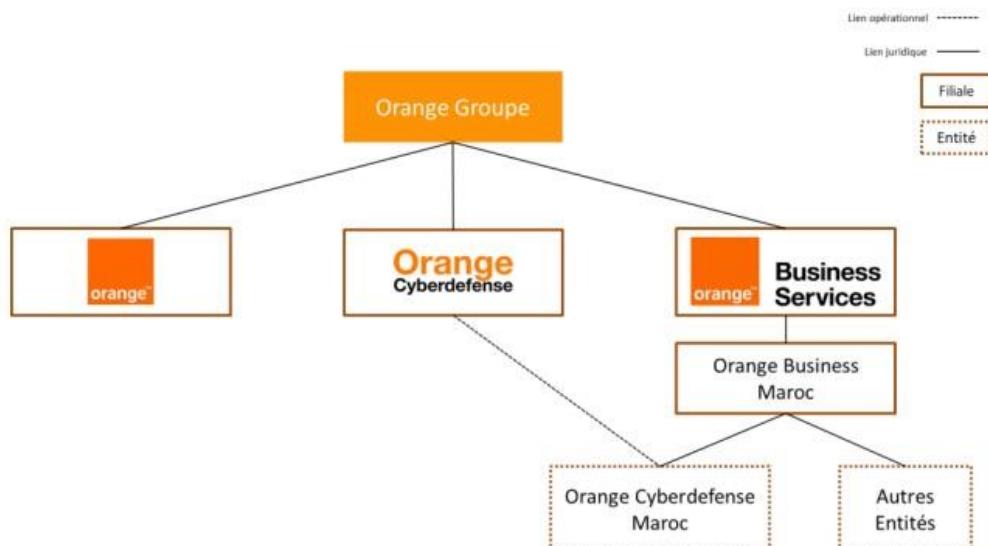


Figure 1.6 : Groupe Orange

## 1.6 Partenaires locaux et étrangers



Figure 1.7 : Partenaires Orange Cyberdefense

## 2. Contexte du projet

### 2.1. Contexte général

Ce travail de stage vise à créer une initiative pour une entreprise souhaitant mettre en œuvre une architecture Zero Trust (ZTA). L'objectif principal est de commencer par l'implémentation d'un système IAM robuste intégrant les technologies MFA (Authentification à Facteurs Multiples) et IGA (Gouvernance et Administration des Identités).

L'entreprise, Orange Cyberdefense, désire satisfaire les besoins de ses clients en améliorant les solutions et les équipements de confiance utilisés, et en adoptant une approche Zero Trust. Nous allons aider l'entreprise à renforcer sa sécurité et à améliorer son niveau de maturité en cybersécurité.

En intégrant les technologies MFA et IGA dans le système d'information du client, nous garantirons une authentification plus solide en exigeant plusieurs facteurs d'authentification et une gestion centralisée des droits d'accès et des autorisations des utilisateurs.

## **2.2. Problématique**

L'infrastructure d'une entreprise est devenue de plus en plus complexe. Une seule entreprise peut exploiter plusieurs réseaux internes, des bureaux distants avec leur propre locaux, des individus distants et/ou mobiles, et des services Cloud. Cette complexité a dépassé les anciennes méthodes de sécurité réseau basée sur le périmètre, car il n'existe pas de périmètre unique et facilement identifiable pour l'entreprise. La sécurité du réseau basée sur le périmètre s'est également avérée insuffisante car une fois que les attaquants ont franchi le périmètre, tout autre mouvement latéral est libre. Raisons pour lesquelles, la majorité des entreprises ont pensé à remplacer la sécurité réseau basée sur le périmètre par le modèle de sécurité Zero Trust.

## **2.3 Objectifs du projet**

Ce projet a pour objectif de proposer et de mettre en place un modèle de sécurité Zero Trust qui fournit un accès sécurisé aux applications et aux ressources, avec une protection intégrée contre les menaces et la compromission des données, non plus au périmètre du réseau, mais au niveau de l'utilisateur individuel pareille. Et qui permet aux employés pour accéder aux applications dans le Cloud ou sur site et travailler de n'importe où, sans avoir besoin d'un VPN d'accès à distance traditionnel, et l'accès dépend uniquement de l'appareil et des informations d'identification de l'utilisateur, quel que soit l'emplacement réseau de l'utilisateur, qu'il s'agisse de l'emplacement de l'entreprise, du réseau domestique, d'un hôtel ou d'un café. Tous les accès aux ressources de l'entreprise sont entièrement authentifiés, entièrement autorisés et entièrement chiffrés en fonction de l'état de l'appareil et des informations d'identification de l'utilisateur.

Le présent Projet s'est déroulé au sein de l'entreprise Orange Cyberdefense avec les missions principales suivantes :

- ✓ Bien maîtriser le concept Zero trust.
- ✓ Préparer pour une initiative Zero trust.
- ✓ Conception et implémentation des solutions choisis.
- ✓ Simulation des cas d'utilisation.

## **2.4 Organisation et plan du projet**

- Du côté d'Orange Cyberdefense, l'organisation du projet est la suivante : ✓ AIT  
EL HADJ Sana: Team leader Build & Run -Maroc et Afrique francophone ✓  
BENNANI Hamza : Consultant en cybersécurité.
- Du côté d'ENSAK, l'organisation du projet est la suivante :  
✓ ZANNOUTI Hamza : Élève ingénieur.  
✓ Pr MADINI Zhour : Encadrante pédagogique

## **2.5 Plan de projet**

## CHAPITRE I – Contexte Général du Projet

### Planning Prévisionnel PFE OCD

TIFFER DU PROJET	Mise en place d'une architecture BIM pour améliorer l'assurance de qualité et l'autonomisation
Sigle	ZANONI_HAND
NOM DE L'ENTREPRISE	Orange Défense
DATE D'ENTRÉE	mardi 7 Février 2023
Responsible	Madame ATEL HOUZONO

TACHE	TACHE	DATE	DATE	PREMIÈRE PHASE			DEUXIÈME PHASE			TROISIÈME PHASE			QUATRIÈME PHASE										
				DÉBUT	FIN	SEMANNE 1	SEMANNE 2	SEMANNE 3	SEMANNE 4	SEMANNE 5	SEMANNE 6	SEMANNE 7	SEMANNE 8	SEMANNE 9	SEMANNE 10	SEMANNE 11	SEMANNE 12	SEMANNE 13	SEMANNE 14	SEMANNE 15	SEMANNE 16	SEMANNE 17	SEMANNE 17
1	Etupe et planification																						
1.1	Etupe globale sur BIM	07/02/23	13/02/23	5																			
1.2	Etupe des différentes briques de BIM	14/02/23	14/02/23	5																			
1.3	Etupe sur l'architecte globale de BIM	15/02/23	21/02/23	5																			
1.4	Élaboration du planning prévisionnel	22/02/23	24/02/23	3																			
2	Design et architecture																						
2.1	Design d'une architecture basée sur GAF et M&A	27/02/23	03/03/23	5																			
2.2	Concevoir les processus, politiques et procédures de gouvernance de l'entreprise	04/03/23	10/03/23	5																			
2.3	Élaboration d'une approche pour le déploiement des solutions GAF et M&A dans l'entreprise	11/03/23	14/03/23	2																			
3	Formation sur la solution GAF et M&A																						
3.1	Formation sur la solution GAF et M&A	15/03/23	24/03/23	8																			
3.2	Formation sur la solution M&A Gambo (phase 1)	27/03/23	03/04/23	8																			
4	Déploiement de la solution GAF et M&A																						
4.1	Déploiement de la solution GAF et M&A	04/04/23	21/04/23	12																			
4.2	Intégration de la solution M&A sur les différentes composantes de l'architecture	24/04/23	28/04/23	5																			
4.3	Déploiement de la solution GAF et M&A	01/05/23	12/05/23	10																			
5	Test et validation																						
5.1	Test et vérification	24/05/23	26/05/23	5																			
5.2	Amélioration	01/05/23	05/05/23	5																			
6	Rédaction du rapport et préparation de la séquence																						
6.1	Rédaction du rapport PFE	08/05/23	05/06/23	21																			
6.2	Préparation de la présentation finale	04/06/23	13/06/23	7																			

Figure 1.8 : Diagramme de Gantt

## **CONCLUSION**

Dans ce chapitre, nous avons présenté l'organisme d'accueil, le contexte du travail et l'approche à porter présentée sous la forme d'un diagramme de Gantt. Dans le chapitre suivant, nous allons entamer une étude sur le concept Zero-Trust et l'IAM.

## **CHAPITRE 2 – État de l’Art**

## **CHAPITRE II – État de l’Art**

Dans ce chapitre, nous allons discuter du Zero Trust notamment de son historique, ses avantages, ses principes, ses composants ainsi de ses limites.

Nous allons également discuter de l’IAM, ses éléments et sa nécessité pour réussir un projet zéro trust

## **INTRODUCTION**

Avant d'entrer dans notre sujet, il faut d'abord clarifier les définitions des principaux concepts liés à notre projet, ce qui est l'objet de ce chapitre, où nous présenterons l'historique, la définition et les avantages de Zero-Trust. Ce chapitre donne également un aperçu des différentes briques sécuritaires du Zero-Trust, ainsi que de l'architecture de ZT proposée par le NIST.

### **1. Zero Trust**

#### **1.1. Historique**

Traditionnellement, les limites de sécurité étaient placées à la périphérie du réseau de l'entreprise selon une approche classique de type "muraille et douves" du château. Cependant, avec l'évolution de la technologie, les travailleurs distants et les charges de travail distantes sont devenus plus courants. Les limites de sécurité ont donc nécessairement suivi et se sont étendues non seulement à la périphérie de l'entreprise, mais également aux appareils et réseaux auxquels l'utilisateur distant était connecté, ainsi qu'aux ressources auxquelles il accédait. Cela a contraint les équipes de sécurité et de réseau à adapter les modèles de sécurité et d'accès appliqués par les organisations pour répondre à ces exigences commerciales, avec des degrés de succès mitigés. En 2010, l'analyste de Forrester John Kindervag a introduit le terme "Zero Trust" dans l'influent document "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security". Ce document a capturé des idées qui avaient été discutées dans l'industrie depuis quelques années, en particulier celles promues par le Forum Jericho. Le document de Forrester a décrit le passage d'une périphérie dure à une approche qui exigeait d'inspecter et de comprendre les éléments d'un réseau avant qu'ils puissent gagner un niveau de confiance et d'accès. Avec le temps, Forrester a développé ce concept en ce qui est maintenant connu sous le nom de cadre Zero Trust eXtended (ZTX), qui comprend les données, les charges de travail et l'identité comme composants clés de Zero Trust.<sup>[2]</sup>

#### **1.2. Définition**

Zero Trust est un modèle complet de sécurité pour protéger les ressources de réseau, d'application et de données. Il se concentre sur l'utilisation d'un modèle de politique centré sur l'identité pour contrôler l'accès. Bien que chaque entreprise ait des outils informatiques

et de sécurité en place, Zero Trust exige une approche holistique, avec l'identité au centre, afin d'appliquer des politiques de sécurité qui tiennent compte du contexte et des attributs dans tout l'environnement. [3]

### 1.3. Avantages de Zero Trust

Visibilité accrue de l'accès aux ressources : l'approche de la sécurité Zero trust exige que vous déterminiez et classiez toutes les ressources du réseau. Cela permet aux entreprises de mieux voir qui accède à quelles ressources pour quelles raisons et de comprendre les mesures à appliquer pour sécuriser les ressources.

Diminution de la surface d'attaque : en mettant l'accent sur la sécurisation des ressources individuelles, les entreprises qui appliquent les principes de Zero trust sont confrontées à une réduction des risques d'attaques de pirates visant le périmètre du réseau.

Amélioration du contrôle : la mise en œuvre d'une stratégie de sécurité Zero trust est associée au déploiement d'une solution de surveillance et de journalisation continues de l'état des ressources et de l'activité des utilisateurs. Cela permet aux entreprises de mieux détecter les menaces potentielles et d'y répondre en temps utile[3]

### 1.4. Principes du Zero Trust

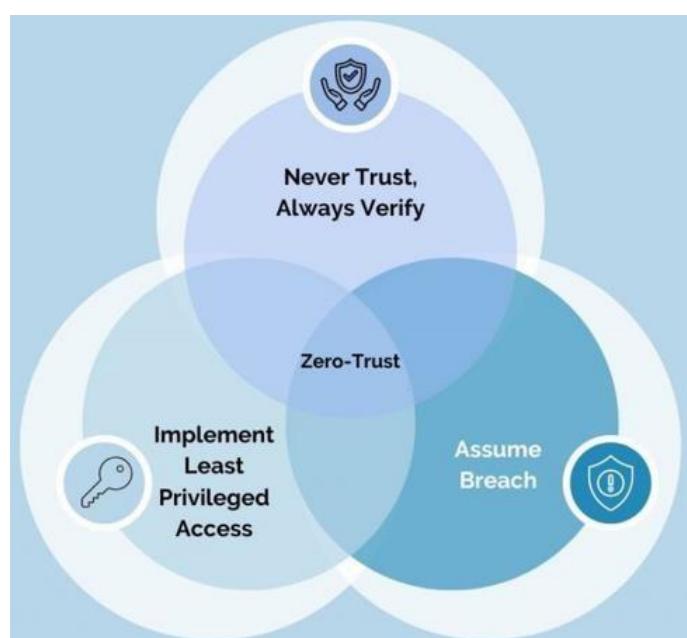


Figure 2.1 : Principes du Zero Trust

*Chapitre II – Etat de l’Art*

Le modèle Zero Trust obéit à trois principes qui guident et étayent l’implémentation de la sécurité. Ces principes sont les suivants :

**Vérification explicite** : Chaque accès est vérifié et autorisé en fonctions de plusieurs critères : identité, emplacement, état de santé de l'équipement

**Accès selon le privilège minimum** : Le principe du privilège minimum dans le modèle Zero Trust est souvent utilisé en conjonction avec deux autres principes : Just-In-Time Access (JIA) et Just Enough Access (JEA).

- Le principe JIA permet de limiter l'accès des utilisateurs et des dispositifs à des ressources sensibles pendant une période définie. Par exemple, un utilisateur peut être autorisé à accéder à une ressource critique pendant une période spécifique pour accomplir une tâche, après quoi l'accès est automatiquement révoqué. Cette mesure réduit le risque d'utilisation non autorisée de ressources sensibles.
- Le principe JEA permet de limiter l'accès des utilisateurs et des dispositifs à un niveau spécifique de privilège, en ne leur donnant accès qu'aux fonctions et aux informations nécessaires pour accomplir leur travail, et rien de plus. De cette manière, les utilisateurs ne peuvent pas accéder à des données sensibles ou des fonctions qui ne sont pas nécessaires à leur travail.

En combinant les principes du privilège minimum, du Just-In-Time Access et du Just Enough Access, les entreprises peuvent mettre en place des politiques de sécurité efficaces pour minimiser les risques de violation de données, tout en permettant aux utilisateurs et aux dispositifs de travailler de manière productive.

**Supposition de violation.** Le principe de supposition de violation dans le cadre du modèle de sécurité Zero Trust implique d'adopter une approche proactive pour la sécurité des systèmes d'information. Ce principe suppose que les menaces existent en permanence et vise à détecter et à répondre aux violations de sécurité potentielles avant qu'elles ne causent des dommages considérables. Pour y parvenir, il est crucial de procéder à une vérification constante des utilisateurs, des dispositifs et des connexions, afin de minimiser les risques de violation de données et de limiter les effets d'une telle violation. [4]

## **1.5. Composants clés de Zero Trust**

Pour mettre en place une architecture Zero Trust efficace, plusieurs composants clés doivent être pris en compte :

**Authentification forte** : pour s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être.

**Micro-segmentation** : pour diviser le réseau en zones distinctes et contrôler les accès entre ces zones.

**Visibilité en temps réel** : pour surveiller les activités du réseau et détecter les éventuelles anomalies.

**Contrôle d'accès basé sur le contexte** : pour prendre en compte les caractéristiques de chaque session et déterminer les permissions d'accès appropriées.

**Chiffrement bout en bout** : pour garantir la confidentialité des données.

**Validation continue** : pour vérifier que tous les composants fonctionnent correctement.

**Automatisation et orchestration** : pour gérer l'ensemble de ces composants de manière cohérente et efficace.

## 1.6 Architecture Zero Trust selon NIST

Le choix du NIST comme référence pour la présentation de l'architecture Zero Trust repose sur sa réputation en tant qu'autorité respectée dans le domaine de la cybersécurité. Grâce à son expertise et à sa rigueur scientifique, ce dernier a pu identifier les composants essentiels et fournir des lignes directrices précises pour la construction d'une architecture Zero Trust.

Le modèle de sécurité Zero Trust est un concept plutôt qu'une solution clé en main qu'une entreprise peut simplement adopter. Cependant, le NIST a identifié les composants clés qui peuvent aider à construire une architecture Zero Trust à travers son état de l'art. Une architecture Zero Trust est généralement composée de deux parties : le Control Plane et le Data Plane. [5]

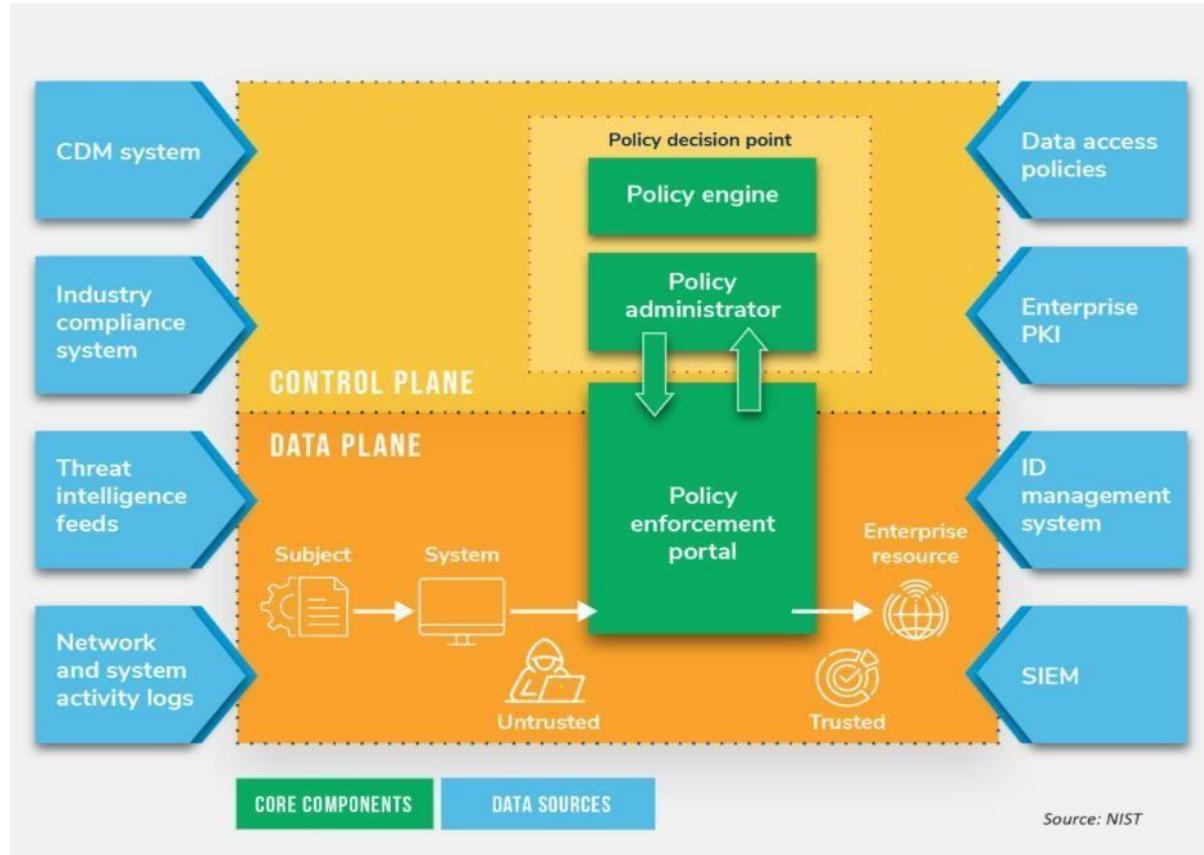


Figure 2.2: Architecture Zero Trust propose par NIST

### 1.6.1 Control Plane

Le control plane représente l'ensemble des composants chargés de collecter les informations nécessaires à la retranscription du contexte et chargés de la prise de décision. Il est composé du « policy decision point », lui-même composé du « policy engine » et du « policy administrator ».

#### Policy engine :

Ce composant est responsable de la décision finale d'accorder l'accès à une ressource pour un sujet donné. Le PE utilise la politique de l'entreprise ainsi que des données provenant de sources externes pour alimenter un algorithme de confiance afin d'accorder, de refuser ou de révoquer l'accès à la ressource.

#### Policy administrator :

Ce composant est chargé d'établir et/ou de fermer le chemin de communication entre un sujet et une ressource. Il génère toute authentification spécifique à une session et tout jeton ou justificatif d'authentification utilisé par un client pour accéder à une ressource d'entreprise. Il

*Chapitre II – Etat de l'Art*  
est étroitement lié à la PE et s'appuie sur sa décision d'autoriser ou de refuser finalement une session.

### **1.6.2 Data plane**

Le reste des composants se trouve dans le data plane. Le data plane représente l'ensemble des composants avec lesquels l'utilisateur peut interagir. L'utilisateur peut interagir avec le policy enforcement point mais pas avec le policy decision point qui est dans le control plane.

#### **Policy Enforcement Point :**

Ce système est chargé d'activer, de surveiller et, éventuellement, de mettre fin aux connexions entre un sujet et une ressource d'entreprise. Le pep communique avec le PA pour transmettre des demandes et/ou recevoir des mises à jour de politiques de la part du PA. Il s'agit d'un seul composant logique dans ZTA, mais il peut être divisé en deux composants différents : le côté client et le côté ressource.

## **1.7 Limites de Zero Trust**

Le modèle de sécurité Zero Trust a été présenté comme une défense ultra-sécurisée contre les menaces émergentes et non reconnues. Contrairement à la sécurité périphérique, il ne part pas du principe que les personnes à l'intérieur d'une organisation sont automatiquement en sécurité. Au contraire, il exige que chaque utilisateur - interne et externe - soit autorisé avant tout accès.

Une approche fragmentaire de la cybersécurité zéro confiance peut créer des lacunes : La cybersécurité à confiance zéro peut éventuellement conduire à une sécurité supérieure, mais en cours de route, elle peut exposer les entreprises à un risque accru. La plupart des entreprises personnalisent leurs propres stratégies en utilisant une approche fragmentaire, mais des lacunes ou des fissures peuvent se développer et rendre la confiance zéro moins solide qu'annoncé. Dans le même temps, le démantèlement d'une solution existante peut créer des failles de sécurité inattendues.

La cybersécurité "zéro confiance" exige un engagement d'administration permanente :

Un autre obstacle souvent négligé au passage à un modèle de cybersécurité à confiance zéro est la nécessité d'une administration permanente. Les modèles de confiance zéro reposent sur un vaste réseau de permissions strictement définies, mais les entreprises sont en

## *Chapitre II – Etat de l'Art*

constante évolution. Les personnes occupent de nouveaux rôles et changent de site. Les contrôles d'accès doivent être mis à jour à chaque fois pour garantir que les bonnes personnes ont accès à des informations spécifiques. Le maintien de l'exactitude et de la mise à jour des autorisations nécessite une saisie permanente.

### Impacte de Zero Trust sur la productivité :

L'introduction d'une approche de la cybersécurité fondée sur la confiance zéro peut également affecter la productivité. Le défi principal de la confiance zéro est de verrouiller l'accès sans interrompre les flux de travail. Les gens ont besoin d'accéder à des données sensibles pour travailler, communiquer et collaborer. Si une personne change de rôle et se retrouve bloquée pendant une semaine pour accéder à des fichiers ou des applications, sa productivité peut chuter. Dans le pire des cas, la perte de productivité devient un problème plus important que la cybersécurité elle-même.

## **2. Identity and Access Management**

### **2.1. Définition**

Identity and Access Management (IAM) est un vaste domaine de la sécurité de l'information qui englobe à la fois les aspects techniques et les processus métier de contrôle d'accès en fournissant le bon accès à la bonne personne au bon moment."

L'IAM implique la gestion des identités (personnes et entités non personnelles) et sert de source d'information fiable concernant ces identités. Il agit comme le système "clé de voûte" pour de nombreuses intégrations techniques et processus métier. L'IAM est fondamental pour les discussions sur la Zero Trust et joue un rôle crucial dans la mise en œuvre d'un programme Zero Trust. [6]

### **2.2. Eléments de l'IAM**

Bien que chaque système de gestion des identités soit différent, en fonction de la combinaison unique de chaque entreprise et de son ensemble de technologies choisies, les systèmes de gestion des identités contiennent des éléments communs qu'on va les détailler dans cette partie en s'appuient sur la figure ci-dessous :

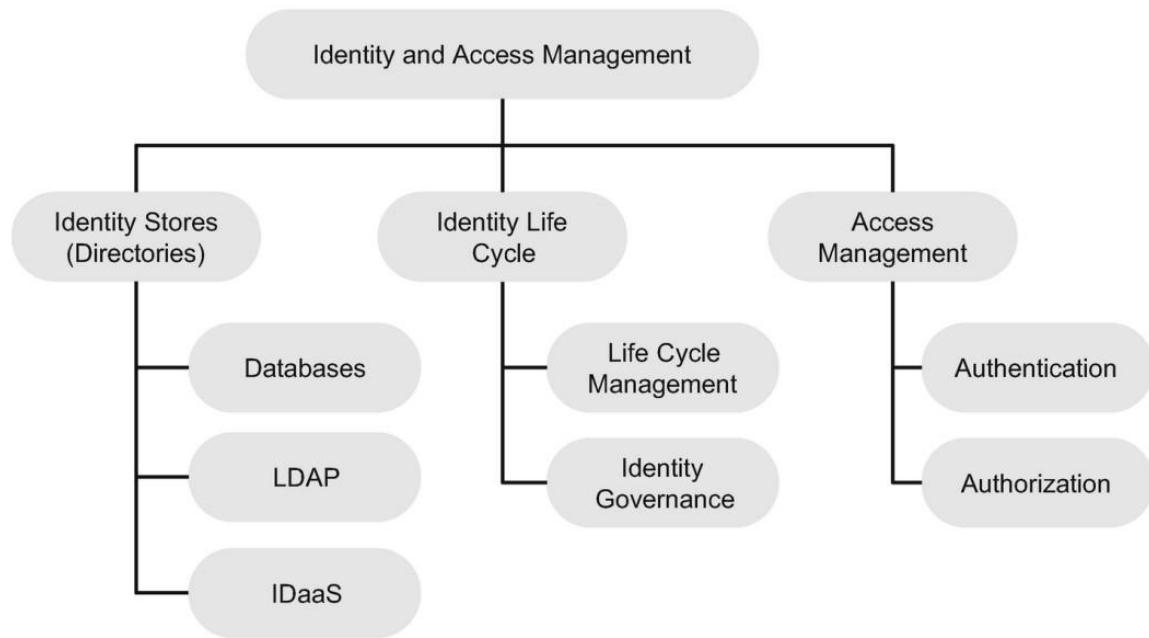


Figure 2.3: Les éléments d'un système IAM

### 2.2.1 Magasin d'identité

L'élément central de tout système de gestion des identités est son magasin d'identités, souvent appelé un répertoire (plus formellement, un service de répertoire). C'est là, de manière logique, que les informations de référence sur les entités sont stockées - les attributs qui décrivent l'entité et fournissent des données significatives destinées à être utilisées par les utilisateurs humains et les consommateurs automatisés de ces informations."

Dans le contexte de la Zero Trust et de la gestion des identités et des accès (IAM), les "magasins d'identités" sont des référentiels ou des bases de données où les informations de référence sur les entités sont stockées. Ces magasins contiennent des attributs qui décrivent l'entité et fournissent des données pertinentes à la fois pour les utilisateurs humains et les systèmes automatisés. Le magasin d'identités est souvent appelé un répertoire ou un service de répertoire.

#### Bases de données :

Les bases de données peuvent techniquement servir de magasin d'identités centralisé accessible via un réseau. Cependant, la plupart des entreprises modernes évitent d'utiliser directement des bases de données brutes en tant que répertoires pour plusieurs raisons. Il n'est pas recommandé de donner aux applications distantes un accès à la base de données contenant les informations sur les utilisateurs, en particulier les informations d'identification, même en lecture seule.

## *Chapitre II – Etat de l'Art*

Il est important de noter que, même si les répertoires basés sur des normes utilisent inévitablement une base de données sous-jacente, il existe une différence significative entre l'accès direct à une base de données brute et l'utilisation de protocoles normalisés et d'interfaces de programmation d'applications (API) pour interagir avec les répertoires. Il est donc nécessaire d'éviter ces types de magasins d'identités personnalisés et, s'ils sont déjà en place, ils devraient être progressivement éliminés dans le cadre d'une initiative Zero Trust.

### **LDAP :**

Le protocole Lightweight Directory Access Protocol (LDAP) est une spécification qui définit un ensemble de messages (effectivement une API) pour interagir avec des services de répertoire à travers un réseau. Il s'agit d'une norme bien établie décrite dans des RFCs du groupe de travail Internet Engineering Task Force (IETF). LDAP v3, publié initialement en 1997, est particulièrement réussi, car de nombreux fournisseurs de répertoire (open source et commerciaux) le prennent en charge, permettant une interopérabilité entre composants de différents fournisseurs.

LDAP offre une API simple pour effectuer des opérations sur les entités du répertoire. Il est largement utilisé pour l'authentification des utilisateurs (mots de passe) et bénéficie d'un large déploiement et d'un soutien important de la part des fournisseurs d'identité, de sécurité, d'applications et d'infrastructures. Par exemple, le service Active Directory de Microsoft, qui est largement déployé dans l'industrie, est compatible avec l'API LDAP.

### **Identity As A Service (IDaaS):**

Au sein de l'ère numérique actuelle, Identity-as-a-Service (IDaaS) est apparu comme une solution essentielle tant pour les entreprises que pour les particuliers. L'IDaaS fait référence à un service basé sur le cloud qui permet aux organisations de gérer et d'authentifier de manière sécurisée les identités des utilisateurs sur différentes applications et systèmes. Il offre un ensemble complet d'outils et de protocoles pour la fourniture d'utilisateurs, la connexion unique, la gestion des accès et la gouvernance des identités. En tirant parti de l'IDaaS, les entreprises peuvent rationaliser leurs processus de gestion des identités, renforcer la sécurité et améliorer l'expérience utilisateur, tout en réduisant les complexités et les coûts associés aux solutions traditionnelles sur site.

## 2.2.2 Cycle de vie de l'identité

Chaque identité possède un cycle de vie, qu'il soit explicitement et formellement défini ou non. Les identités sont créées, elles existent pendant une période, elles peuvent potentiellement changer de rôles au fil du temps, et finalement elles sont détruites. Les organisations doivent disposer d'outils techniques et de processus métier/IT pour gérer et contrôler les cycles de vie des identités. Ces domaines au sein de l'IAM, connus sous le nom de gestion du cycle de vie et de gouvernance des identités, font indirectement partie d'une initiative Zero Trust

### Gestion du cycle de vie :

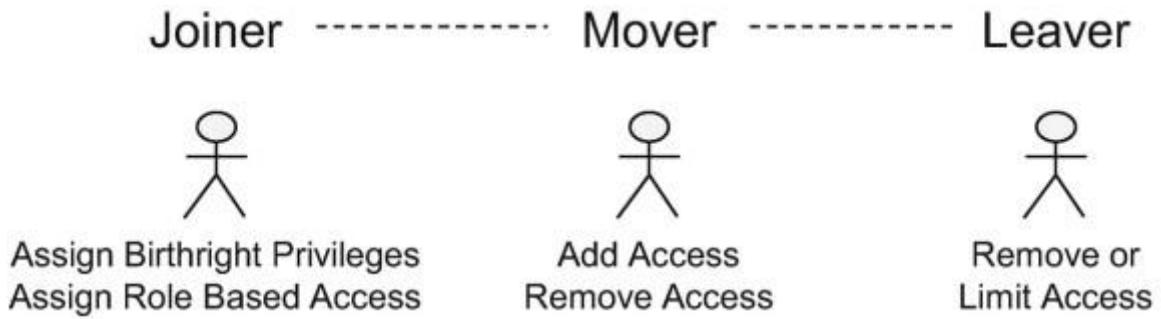


Figure 2.4: Cycle de vie d'un utilisateur

Le management de cycle de vie des identités revient à la gestion complète des identités des utilisateurs, y compris leur création, leur modification, leur attribution de droits d'accès, leur surveillance et leur désactivation lorsqu'elles ne sont plus nécessaires. Cela englobe également la gestion des comptes de service, des priviléges et des rôles associés.

L'objectif c'est de garantir que les identités et les accès sont gérés de manière sécurisée et efficace tout au long de leur existence, en minimisant les risques de sécurité et en assurant la conformité aux politiques et aux réglementations.

### Gouvernance des identités

La gouvernance des identités, qui détermine "qui doit avoir accès à quoi" dans le cadre du cycle de vie des identités, est une partie intégrante des programmes de gestion des accès et des identités (IAM). La gouvernance est généralement motivée par des exigences de conformité et de sécurité, avec souvent une plus grande importance accordée à la conformité. Les entreprises déploient souvent des solutions de gouvernance des identités pour répondre

à ces exigences de conformité, notamment dans le domaine des applications financières et des contrôles, notamment pour les entreprises cotées en bourse.

Ces décisions de gouvernance des identités peuvent être mises en œuvre de manière automatisée par le biais d'un système de provisionnement ou être gérées par des processus informatiques et métier manuels. Dans les deux cas, les politiques de gouvernance des identités doivent être alignées sur les politiques de confiance zéro (Zero Trust).

### **2.2.3 Gestion d'accès**

La gestion des accès est au cœur de la gestion des identités et se compose de deux composantes principales : premièrement, les moyens par lesquels les entités prouvent qu'elles sont qui elles prétendent être, l'authentification, et deuxièmement, le modèle permettant de définir et d'exprimer l'ensemble des actions qu'une entité donnée est autorisée à effectuer, l'autorisation. Examinons chacune de ces composantes à tour de rôle.

#### **Authentification**

Dans cette section, nous fournissons une introduction aux protocoles, mécanismes, normes et tendances courants en matière d'authentification. Nous le faisons afin d'explorer leur pertinence dans le cadre des déploiements Zero Trust. Commençons par quelques définitions de base, incluses pour plus de clarté :

- **Nom d'utilisateur/mot de passe** : une authentification simple, utilisée depuis des décennies. Cela consiste à valider quelque chose que vous connaissez.
- **Authentification multi-facteurs (MFA)** : l'utilisation de plus d'un facteur d'authentification dans le cadre d'un processus d'authentification. Cela utilise souvent un jeton physique, une application pour smartphone ou un mécanisme biométrique pour valider quelque chose que vous possédez ou quelque chose que vous êtes.
- **Authentification sans mot de passe** : c'est un principe général consistant à utiliser des facteurs autres que des mots de passe pour l'authentification initiale. Nous encourageons ce changement, car cela élimine les risques bien connus liés aux mots de passe faibles, au vol de mots de passe et à la réutilisation des mots de passe. Ces solutions utilisent souvent les types de mécanismes énumérés précédemment dans le cadre du MFA.

Maintenant, examinons plusieurs protocoles et mécanismes d'authentification couramment utilisés :

- **LDAP** : un API utilisé à la fois pour interagir avec les répertoires et pour l'authentification des utilisateurs. Il prend en charge nativement l'authentification basée sur le nom d'utilisateur et le mot de passe.
- **RADIUS** : un autre protocole d'authentification plus ancien, utilisé pour l'authentification à distance des utilisateurs. Il est largement utilisé et prend en charge différents mécanismes d'authentification au-delà du simple nom d'utilisateur et mot de passe.
- **SAML** : un langage de balisage des assertions de sécurité qui permet l'authentification unique (SSO) pour les applications web à partir de fournisseurs différents. Il définit une représentation XML et un protocole basé sur HTTP pour permettre aux applications web (fournisseurs de services) de consommer les informations d'authentification et d'attributs utilisateur à partir d'un fournisseur d'identité distinct.
- **OAuth2** : un mécanisme permettant à une application tierce d'accéder à un ensemble limité de fonctions ou de ressources au sein d'une application web, au nom de l'utilisateur. Il s'agit d'un protocole d'autorisation qui repose sur les permissions accordées par l'utilisateur.
- **OIDC** : construit sur OAuth2, il ajoute l'authentification à l'autorisation OAuth et est couramment utilisé par les applications web pour fournir l'authentification et l'autorisation en utilisant le framework OAuth sous-jacent.
- **Authentification basée sur des certificats** : utilisée pour valider l'identité des utilisateurs et des appareils, en se basant sur la possession d'un certificat valide. Les certificats peuvent être installés sur les appareils des utilisateurs ou utilisés par des serveurs et des appareils IoT.
- **FIDO2** : une norme émergente qui offre une expérience "sans mot de passe" aux utilisateurs en utilisant des protocoles basés sur l'infrastructure à clé publique (PKI). Il

prend en charge les navigateurs, les appareils mobiles et les dispositifs matériels comme moyens d'authentification.

- **Authentification mobile et biométrique** : bien qu'il ne s'agisse pas de normes d'authentification à proprement parler, les méthodes d'authentification modernes utilisent de plus en plus des technologies conviviales basées sur les appareils mobiles pour l'authentification des utilisateurs, telles que la reconnaissance d'empreintes digitales ou faciale. [7]

### **Autorisation :**

Dans le contexte de la gestion des identités et des accès (IAM) et du Zero Trust, l'autorisation concerne la détermination des droits et des priviléges accordés à un utilisateur ou à une entité après leur authentification. Elle contrôle l'accès aux ressources en fonction des permissions attribuées.

L'autorisation repose sur le principe de n'accorder qu'un accès minimal nécessaire aux ressources, en fonction du contexte et des besoins spécifiques de chaque utilisateur. Les politiques d'autorisation sont appliquées de manière granulaire, prenant en compte des facteurs tels que l'identité de l'utilisateur, le niveau de confiance de l'appareil utilisé, le lieu, l'heure, etc. Elles décident si l'accès à une ressource spécifique doit être accordé, refusé ou s'il nécessite une authentification supplémentaire.

L'objectif de l'autorisation est de limiter les risques d'accès non autorisés en s'assurant que seules les personnes et les entités de confiance peuvent accéder aux ressources appropriées. En combinant l'authentification et l'autorisation, on crée un environnement sécurisé où l'accès est contrôlé de manière stricte et adaptative, en fonction du contexte de chaque demande d'accès.

## **CONCLUSION**

En conclusion de ce chapitre, nous avons exploré en détail le concept de Zero Trust, son historique, ses avantages, ses principes ainsi que ses composants et son architecture selon le NIST. Nous avons également entamé notre exploration de la brique de l'IAM, en fournissant une définition claire et en définissant son scope, qui comprend le magasin d'identité, le cycle de vie de l'identité et la gestion des accès. Ces deux domaines sont des éléments essentiels pour renforcer la sécurité des systèmes d'information et garantir un niveau de confiance

*Chapitre II – Etat de l'Art*  
approprié. Dans les prochains chapitres, nous approfondirons davantage ces sujets et explorerons leurs interactions pour construire une infrastructure de confiance solide.

## **CHAPITRE III – Etude comparatif et présentation des solutions**

Dans ce chapitre, nous allons définir les deux technologies MFA et IGA, comparer trois solutions dominantes dans le marché pour les deux briques, et de présenter les solutions choisis.

*Etude comparatif et présentation des solutions*

## INTRODUCTION

Dans ce chapitre nous allons découvrir les deux technologies MFA et IGA en détail en présentant leurs avantages et leurs contributions dans une architecture Zero Trust, nous allons aussi comparer les éditeur leader dans les deux briques, et finalement présenter les solutions choisies.

### 1. Multiple Factor Authentication (MFA)

#### 1.1 Définition :

L'authentification multifactorielle (MFA) est une méthode de sécurité qui exige des utilisateurs de fournir plusieurs formes d'identification pour accéder à un système ou à des ressources sensibles. En utilisant divers facteurs d'authentification, tels que des mots de passe, des jetons, des empreintes digitales ou des codes générés, le MFA renforce considérablement la sécurité en ajoutant une couche supplémentaire de vérification [14].



Figure 3.1: MFA

#### 1.2. Avantages :

Les avantages de l'authentification multifactorielle sont nombreux. Tout d'abord, elle réduit considérablement les risques d'usurpation d'identité et de compromission des comptes utilisateurs. Même si un facteur d'authentification est compromis, les autres facteurs requis pour accéder aux ressources protégées assurent une sécurité renforcée.

### 1.3. Les types de la MFA :

Il existe plusieurs types de facteurs d'authentification utilisés dans le cadre du MFA. Parmi les plus courants, on trouve :

**Type 1 – Quelque chose que vous connaissez :** Il s'agit de facteurs basés sur des informations que l'utilisateur connaît, comme les mots de passe, les codes PIN ou les réponses à des questions de sécurité préétablies.

**Type 2 – Quelque chose que vous avez :** Ces facteurs s'appuient sur des objets physiques que l'utilisateur possède, tels qu'une carte à puce, un jeton matériel ou un téléphone mobile.

**Type 3 – Quelque chose que vous êtes :** Ces facteurs utilisent les caractéristiques physiques ou comportementales uniques de l'utilisateur, comme les empreintes digitales, la reconnaissance faciale ou vocale, le balayage de la paume de la main, les scans de la rétine....

### 1.4 MFA et Zero Trust :

Le concept de Zero Trust repose sur le principe selon lequel toute tentative d'accès doit être vérifiée et autorisée, quel que soit le niveau de confiance préalable accordé. En intégrant le MFA, les organisations peuvent appliquer une vérification continue de l'identité de l'utilisateur, renforçant ainsi les contrôles de sécurité dans un environnement Zero Trust. L'utilisation du MFA en combinaison avec d'autres mesures de sécurité renforce la protection des ressources critiques, des données sensibles et des systèmes informatiques.

## 2. Identity Governance and Administration (IGA)

### 2.1. Définition



**Figure 3.2: IGA**

L'IGA est une discipline cruciale pour la gestion des identités et des accès au sein d'une organisation. Elle vise à garantir que seules les bonnes personnes ont accès aux bonnes ressources au bon moment. L'IGA se concentre sur la gestion centralisée des identités des utilisateurs, des priviléges et des droits d'accès. Elle assure l'exactitude des informations d'identification tout en facilitant la création, la modification et la suppression des identités. Elle contrôle également les accès en fonction des rôles, des responsabilités et des besoins opérationnels, prévenant les menaces internes et externes. De plus, elle surveille les activités des utilisateurs à priviléges élevés et effectue des revues d'accès régulières pour minimiser les risques de violation de sécurité.

## **2.2. Avantages**

L'adoption d'une solution d'IGA présente plusieurs avantages significatifs pour les organisations :

### **2.2.1. Gestion centralisée des identités et des accès**

L'IGA permet une gestion centralisée des identités des utilisateurs, des priviléges et des droits d'accès aux ressources.

Cela simplifie la gestion des utilisateurs en regroupant toutes les informations d'identification et les autorisations au même endroit, facilitant ainsi les opérations de provisionnement, de modification et de révocation des droits d'accès.

### **2.2.2. Renforcement de la sécurité**

L'IGA aide à renforcer la sécurité de l'organisation en garantissant que seules les bonnes personnes ont accès aux ressources appropriées.

En établissant des politiques de contrôle d'accès strictes et en suivant les principes du moindre privilège, l'IGA réduit les risques de violations de sécurité internes et externes, notamment les accès non autorisés et les abus de priviléges.

### **2.2.3. Conformité réglementaire améliorée**

L'IGA facilite la conformité aux réglementations et aux normes de sécurité en assurant une gestion rigoureuse des identités et des accès.

En mettant en place des processus de certification, de suivi des accès et de génération de rapports, l'IGA aide les organisations à démontrer leur conformité aux exigences réglementaires telles que le RGPD, HIPAA, PCI DSS, etc.

### **2.2.4. Réduction des coûts et de la complexité**

Grâce à une gestion centralisée et automatisée des identités et des accès, l'IGA permet de réduire les coûts opérationnels liés à la création, à la modification et à la suppression manuelles des comptes utilisateurs.

De plus, en évitant les accès non autorisés et les violations de sécurité, l'IGA peut réduire les coûts liés aux incidents de sécurité et aux pertes de données.

### **2.2.5. Amélioration de la productivité**

En fournissant un accès rapide et sécurisé aux ressources appropriées, l'IGA améliore la productivité des utilisateurs en leur permettant de se concentrer sur leurs tâches essentielles plutôt que de gérer manuellement leurs droits d'accès.

De plus, grâce aux workflows de gestion des identités, l'IGA rationalise les processus de demande et d'approbation des droits d'accès, réduisant ainsi les délais et les frictions.

## **2.3. IGA et Zero Trust**

Une approche moderne de la gouvernance et de l'administration des identités fournit des informations essentielles sur l'identité et le contexte métier, ce qui aide à la mise en place d'un modèle de confiance zéro. Pour prendre des décisions efficaces dans un modèle de

confiance zéro, il est nécessaire de mieux comprendre les utilisateurs et le contexte dans lesquels ils évoluent.

De plus en plus d'organisations profitent des avantages de la gouvernance des identités pour réussir la mise en œuvre du modèle de confiance zéro. En fait, selon ESG, 81 % des personnes interrogées considèrent que la gouvernance des identités est un élément clé des efforts de mise en œuvre du modèle de confiance zéro. De plus, 84 % d'entre elles prévoient une augmentation des dépenses de gestion des identités et des accès au cours des 12 prochains mois.

Le modèle de confiance zéro ne concerne pas uniquement le service informatique, il profite à l'ensemble de l'organisation. C'est pourquoi les parties prenantes clés doivent être impliquées dans le processus. Elles doivent comprendre les avantages cruciaux offerts par ce modèle, ainsi que les conséquences possibles si rien ne change.

### 3. Benchmark des solutions MFA et IGA

#### 3.1 Solutions MFA

Le tableau suivant présente les trois éditeurs leader dans le côté MFA et des informations sur l'entreprise et les fonctionnalités de la solution qu'ils offrent. [8], [9], [10]

		<b>THALES</b>	 Microsoft	 Okta
Entreprise	Date de création de l'entreprise	6 décembre 2000, France	4 avril 1975, États-Unis	janvier 2009, États-Unis
	Siège social	Paris, France	Redmond, Washington, États-Unis	San Francisco, Californie, États-Unis
	Nombre du personnel	80 000	182 268	2 379
	Revenus	17 milliards EUR	168 milliards USD	835 Million USD
	Nom de la solution	SafeNet Authentication Service PCE	Microsoft Multi-Factor Authentication	Okta Adaptive Multi-factor Authentication
Note selon Gartner (Peers reviews)		3.9/5	4.5/5	4.6/5

Déploiement	Type de déploiement	On-Premise / Cloud / SaaS	Cloud / SaaS / Web	SaaS
	Disponibilité	Un load-balancer est à mettre en place	Utilisation de la norme RADIUS Load Balancer	F5 BigIP Load Balancer
	Systèmes d'exploitation supportés	Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016 (GUI), et 2019(GUI)	Azure	--
	Annuaires LDAP supportés	Active Directory, Novell eDirectory 8. x et SUNOne 5.3	Active Directory	Active Directory, Novell eDirectory 8. x et SUNOne 5.5
Sizing	Configuration pour utilisateur	<10000: 16GB RAM, 2 Cores 10000-20000: 32GB RAM, 4 Cores >20000: 64GB, 6 Cores	--	--
	Configuration moyenne pour authentications par seconde	70: 16GB RAM, 2 Cores 73: 32GB RAM, 2 Cores 82: 16GB RAM, 4 Cores 88: 32GB RAM, 4 Cores	--	--
Base clientèle	Taille de l'entreprise cliente	<50M USD(20%), 50M-1B USD(20%), 1B-19B USD(40%), GOV/PS(20%)	<50M USD(17%), 50M-1B USD(40%), 1B-19B USD(21%), 10B+ USD(5%), GOV/PS(17%)	<50M USD(12%), 50M-1B USD(58%), 1B-19B USD(19%), 10B+ USD(5%), GOV/PS(5%)
	L'industrie	Services (20%), Finance (20%), Manufacturing (10%), Healthcare (10%), Other (40%)	Services (24%), Finance (7%), Manufacturing (10%), Healthcare (10%), Other (48%)	Services (35%), Finance (9%), Manufacturing (9%), Healthcare (5%), Other (42%)
	Région de déploiement	Europe, Middle East and Africa (38%), North America(38%), Asia/Pacific (15%), Latin America (8%)	Europe, Middle East and Africa (27%), North America(55%), Asia/Pacific (15%), Latin America (3%)	Europe, Middle East and Africa (17%), North America(54%), Asia/Pacific (21%), Latin America (9%)
Expérience utilisateur	Gestion centralisée des règles	Selon: des adresses IP, des groupes d'utilisateurs, des dates/heures ...	Selon: l'état de utilisateurs, stratégies des groupes, ...	Selon: des adresses IP, des profils d'utilisateurs, ...
	Workflows automatisés	Synchronisation LDAP, la génération automatique des rapports/alertes, standards/customisés ...	Verrouillage de compte, Blocage/déblocage des utilisateurs, Alerte de fraude, Notifications....	Conforme
	Rapports programmés automatisée	Génération des logs de manière programmée depuis l'interface administrateur	Conforme	Conforme
	Alertes	Emails, SMS	Emails	Emails, SMS

	Configuration du Token	Configurer les politiques de sécurités de différents types de tokens	Utilisé dans les environnements Azure AD pour gérer les jetons	Conforme
Personnalisation	Logos	Conforme	Conforme	Conforme

	Les emails envoyés aux utilisateurs	Conforme	Conforme	Conforme
	Pages web	Conforme	Conforme	Conforme
	Alertes	Conforme	Conforme	Conforme
	URLs	Conforme	Conforme	Conforme
	Token avec les exigences de sécurité	Conforme	Conforme	Conforme
	Authentification	OTP (physiques/logiciels), OOB (SMS, Emails), Grid. KBA (Kerberos) & l'authentification contextuelle	OTP (physiques/logiciels), OOB (SMS, Emails), Grid. KBA (Kerberos) & l'authentification contextuelle	OTP (physiques/logiciels), OOB (SMS, Emails), Grid. KBA (Kerberos) & l'authentification contextuelle
	Types d'authentification	Hardware, 3rd Party, OTP Push, Pattern Based, Voice, Biometric, SMS, eMail, Password, Google Authenticator, Passwordless	Hardware Tokens OPT, Software Tokens OPT, Microsoft Authenticator, Voice, SMS, Password, Windows Hello Entreprise, Passwordless, Clé de sécurité FIDO2	SMS, Voice, Email, OTP, 3rd Party, Hardware Tokens, Biometric factors
	Attributs Return de RADIUS	Serveur RADIUS (NPS ou FreeRADIUS)	Serveur RADIUS	Serveur RADIUS
	Conformité	Tokens certifiés FIPS 140-2 Tokens DSKPP sécurisé Racine de confiance matérielle	ISO 27001:2013 NIST SP 800-171 R2 NIST SP 800-53 Rév. 4	ISO 27001:2013 SOC 2 Type II FIPS 140-2
	Compatibilité	VPN	Conforme	Conforme
	Outlook	Conforme	Conforme	Conforme
	Serveurs web etd'applications	IIS, Apache, Apache Tomcat.....	IIS, Apache, Apache Tomcat.....	IIS, Apache, Apache Tomcat.....
	Plates-formes, environnements deprogrammation et langages	JAVA, C++, .NET.....	JAVA, C++, .NET.....	JAVA, C++, .NET.....

	Base de données	PostgreSQL, MS SQL, MySQL	PostgreSQL, Oracle, MySQL.....	Database.com, Frac Database, Oracle....
	Serveurs Windows	Conforme	Conforme	Conforme
	Solution PAM	CyberArk	CyberArk, WALLIX, OneIdentity,....	CyberArk
	Solution SOAR	CORTEX XSOAR	SPLUNK SOAR, CORTEX XSOAR,...	CORTEX XSOAR
Support	Type	24/24, 7/7	24/24, 7/7	24/24, 7/7
	Adresse	Belcamp, Maryland 21017, USA	--	--
	Numero de telephone	1-410-931-7520	+1 (866) 539 4191, +1 (855) 330 8653	+1-800-425-1267
Protection contre les attaques		Conforme	Conforme	Conforme
Déploiement des softstoken		Mobile pass, Mobile pass+	Microsoft Authenticator	OKTA Verify
Traçabilité		Snapshot	Les rapports des connexions	Logs
Tarification		35,64 \$ pour 1 license de 3ans	Prix sur demande	250 \$ pour 5 licenses de 2ans

### 3.2 Solutions IGA

		 SailPoint	 ORACLE	 SAVIYNT
Entreprise	Date de création de l'entreprise	2005, États-Unis	16 juin 1977, États-Unis	2010, États-Unis
	Siège social	Austin, Texas, États-Unis	Redwood City, Californie, États-Unis	El Segundo, États-Unis
	Nombre du personnel	1400	137000	1000
	Revenus	300 Million USD	39.1 milliards USD	90 Million USD
	Nom de la solution	SailPointIdentityNow / SailPoint IdentityIQ	Oracle Identity Governance	Saviynt Identity Governance and Administration
Note selon Gartner (Peers reviews)		4.4/5	4.5/5	4.5/5

Déploiement	Type de déploiement	On-Premise / Cloud / SaaS	On-Premise / Cloud / SaaS	On-prem / cloud /SaaS
	Systèmes d'exploitation supportés	Windows linux,unix,solaris	Windows linux,unix,solaris	Windows linux,unix,solaris --
	Annuaires LDAP supportés	Active Directory, Novell eDirectory 8. x et SUNOne 5.3	Active Directory, Novell eDirectory 8. x et SUNOne 5.3	Active Directory, Novell eDirectory 8. x et SUNOne 5.5
Base clientèle	Taille de l'entreprise cliente	Entreprise de taille moyenne à grande	Entreprise de taille Moyenne à grande	Entreprise de taille Moyenne à grande
	L'industrie	Services (20%), Finance (20%), Manufacturing (10%), Healthcare (10%), Other (40%)	Services (24%), Finance (7%), Manufacturing (10%), Healthcare (10%), Other (48%)	Services (35%), Finance (9%), Manufacturing (9%), Healthcare (5%), Other (42%)
	Région de déploiement	Europe, Middle East and Africa (38%), North America(38%), Asia/Pacific (15%), Latin America (8%)	Europe, Middle East and Africa (27%), North America(55%), Asia/Pacific (15%), Latin America (3%)	Europe, Middle East and Africa (17%), North America(54%), Asia/Pacific (21%), Latin America (9%)
Fonctionnalités		Gestion des identités et des accès, gouvernance des identités, automatisation des processus, certification des accès ...	Gestion des identités et des accès, gouvernance des identités, automatisation des processus, certification des accès ....	Gestion des identités et des accès, gouvernance des identités, gestion des accès privilégiés, gestion des risques

	Alertes	Emails, SMS teams	Emails	Emails, SMS
Personnalisation	Logos	Conforme	Conforme	Conforme

[11,12,13]

## **4. Présentation des solutions choisies**

### **4.1 SafeNet Authentication Service Private Cloud Edition (SAS PCE)**

SAS PCE est un système sur site fournissant une solution d'authentification forte sécurisée et entièrement automatisée, avec des options de jetons flexibles adaptées aux besoins uniques de votre organisation, ce qui réduit considérablement le coût total de fonctionnement. L'authentification forte est facilitée par la flexibilité et l'évolutivité des workflows automatisés de SafeNet Authentication Service, des intégrations de jetons indépendantes des fournisseurs et des API étendues. En outre, les capacités et les processus de gestion sont entièrement automatisés et personnalisables, offrant une expérience utilisateur transparente et améliorée. SafeNet Authentication Service permet une migration rapide vers un environnement cloud multiniveau et mutualisé, protégeant tout, des applications cloud et sur site aux réseaux, utilisateurs et appareils.

- Il s'agit d'une solution 2FA qui s'intègre facilement dans l'existant infrastructure
- Dispose d'une interface de gestion simple
- Offre une large gamme de jetons pour répondre aux demandes / besoins des utilisateurs

#### **Méthodes d'authentification :**

SAS propose une large gamme de méthodes d'authentification prêtées à l'emploi qui peuvent être utilisées pour gérer les risques via le gestionnaire de politiques. Les méthodes sont indiquées ci-dessous :



Figure 3.3: Méthodes d'authentification supporté par la solution

#### Avantages de la solution :

SAS PCE est utilisée par des centaines d'organisations et entreprises commerciales et gouvernementales dans le monde entier en tant qu'élément central de leur stratégie de gestion d'identité et des accès pour les raisons suivantes :

- Une authentification forte peut être fournie n'importe où, à toute personne où un mot de passe est utilisé et grâce à la prise en charge des normes de l'industrie telles que RADIUS et SAML et la disponibilité des API et des agents pour d'autres applications.
- La solution prend en charge la plus large gamme de méthodes d'authentification offrant la flexibilité de choisir le bon type de jeton pour les besoins de chaque individu.
- La solution prend en charge les jetons tiers garantissant que les investissements existants dans les jetons sont maintenus et fournissent une migration transparente pour les utilisateurs finaux.
- Le degré d'automatisation complet réduit considérablement les coûts de gestion et d'administration, conduisant dans la plupart des cas à une économie de TCO allant jusqu'à 60%.
- Les jetons n'expirent pas et peuvent être réémis à de nouveaux utilisateurs, ce qui réduit encore les coûts et la charge administrative.
- Les utilisateurs peuvent avoir plus d'un jeton sans frais supplémentaires au-delà du coût du jeton, offrant une assistance aux utilisateurs disposant de plusieurs appareils.

- Un portail en libre-service complet permet aux utilisateurs d'exécuter de nombreuses fonctions qui nécessitaient traditionnellement l'assistance du service d'assistance.

### Workflow automatisé déclenché par les changements liés aux utilisateurs :

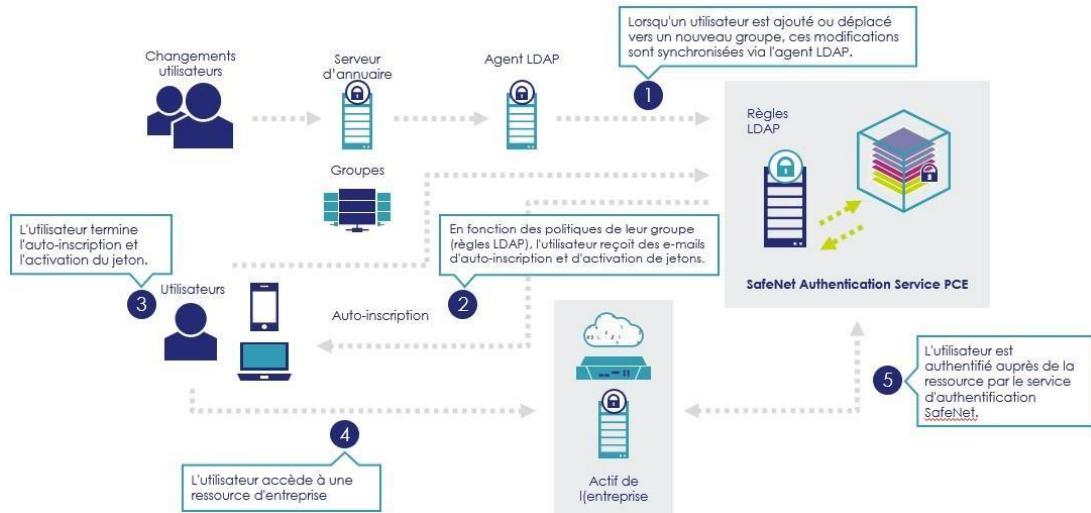


Figure 3.3: Workflow automatisé

## 4.2. SailPoint IdentityIQ

SailPoint IdentityIQ est une solution de gouvernance des identités et des accès sur site qui aide les organisations à gérer de manière centralisée les identités des utilisateurs, les accès aux systèmes et les priviléges. En tant que plateforme IGA, SailPoint IdentityIQ vise à renforcer la sécurité, à garantir la conformité aux réglementations et à améliorer l'efficacité opérationnelle de l'entreprise.



Figure 3.4: Vision globale sur la solution

SailPoint IdentityIQ offre plusieurs fonctionnalités parmi lesquelles :

#### **4.2.1 Gestion des identités :**

IdentityIQ permet de créer, modifier et supprimer des comptes utilisateurs, d'attribuer des rôles et des priviléges, et de gérer le cycle de vie des identités de manière cohérente.

#### **4.2.2 Gestion des accès :**

La solution offre des fonctionnalités avancées de contrôle d'accès, de gestion des droits et de certification des accès. Elle permet de garantir que seules les personnes autorisées ont accès aux ressources appropriées.

#### **4.2.3 Automatisation des processus :**

IdentityIQ automatise les processus de gestion des identités et des accès, ce qui permet de réduire les erreurs et d'améliorer l'efficacité opérationnelle.

#### **4.2.3 Sécurité renforcée :**

La solution intègre des mécanismes de sécurité avancés, tels que l'authentification multifactorielle et la détection des anomalies, afin de protéger les données sensibles et de prévenir les intrusions.

### 4.3 Architecture de la solution

La solution SailPoint IdentityIQ se compose de plusieurs éléments importants chacun aide à des cas d'utilisation bien spécifique.

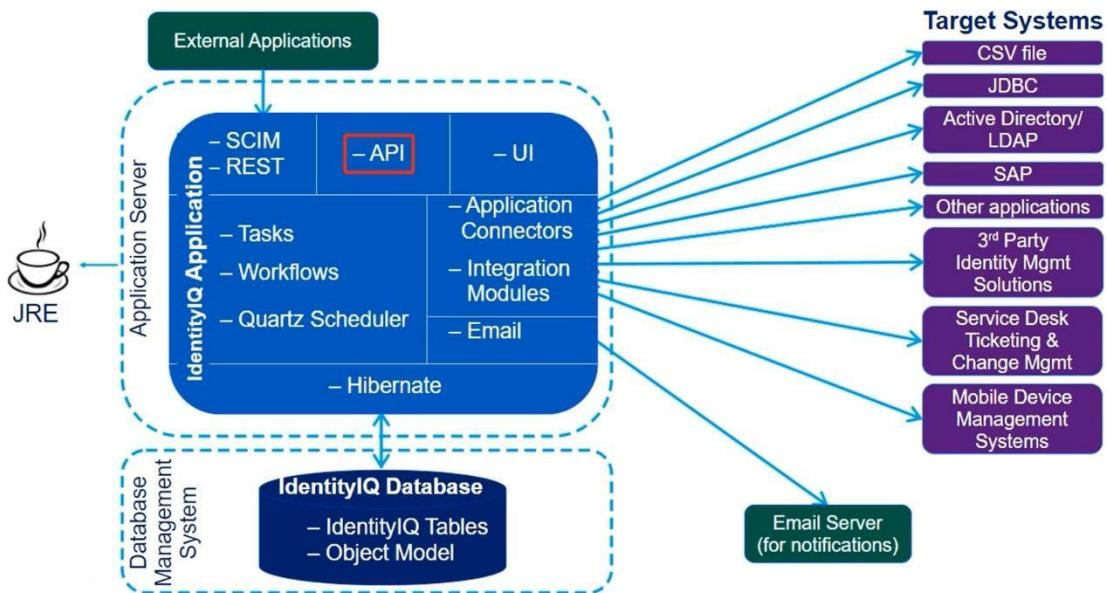


Figure 3.5: Architecture de la solution SailPoint IdentityIQ

- [Java Runtime Environment \(JRE\)](#) : SailPoint IdentityIQ est basé sur la plateforme Java et utilise le JRE pour exécuter ses différentes fonctionnalités.
- [Interface utilisateur \(UI\)](#) : L'interface utilisateur de SailPoint IdentityIQ offre aux administrateurs et aux utilisateurs finaux une interface conviviale pour gérer les identités, les accès et les tâches liées à la gouvernance des identités.
- [Tâches \(Tasks\)](#) : Les tâches dans IdentityIQ sont des processus automatisés qui effectuent des actions spécifiques, comme la provision de comptes utilisateurs, la certification des accès ou la génération de rapports. Les tâches peuvent être planifiées ou déclenchées manuellement.
- [Workflow](#) : Les workflows sont des flux de travail qui définissent les étapes et les approbations nécessaires pour des processus spécifiques dans IdentityIQ. Par exemple, un workflow peut être utilisé pour gérer le processus d'approbation des demandes d'accès ou des demandes de modification des priviléges.

- Quartz Scheduler : IdentityIQ utilise Quartz Scheduler pour la planification et l'exécution des tâches automatiques. Cela permet de programmer des tâches récurrentes, telles que la génération de rapports ou la mise à jour des données.
- Connecteurs d'applications : SailPoint IdentityIQ propose une large gamme de connecteurs d'applications préconfigurés qui permettent d'intégrer et de gérer les accès aux différentes applications et systèmes de l'entreprise. Ces connecteurs facilitent la collecte des données d'identité, la gestion des comptes utilisateurs et la synchronisation des autorisations.
- E-mail : IdentityIQ utilise la fonctionnalité d'e-mail pour envoyer des notifications et des alertes aux utilisateurs et aux administrateurs. Cela permet de tenir les parties prenantes informées des actions à effectuer ou des événements importants liés à la gestion des identités.
- La base de données de SailPoint : IdentityIQ utilise la fonctionnalité d'e-mail pour envoyer des notifications et des alertes aux utilisateurs et aux administrateurs. Cela permet de tenir les parties prenantes informées des actions à effectuer ou des événements importants liés à la gestion des identités.
- Systèmes cibles : Les systèmes cibles font référence aux applications, aux systèmes et aux ressources auxquels IdentityIQ permet de gérer les accès. Il peut s'agir de systèmes sur site ou de services cloud, tels que des applications métier, des bases de données, des serveurs, des services web, etc.

## **CONCLUSION**

Dans ce chapitre, nous avons examiné en détail deux technologies clés : MFA et IGA. Nous avons effectué une évaluation comparative des différentes solutions disponibles sur le marché et présenté en particulier les deux solutions choisis qui était imposé par le besoin interne de l'entreprise d'accueil : SafeNet Authentication Service Private Cloud Edition et SailPoint IdentityIQ. Dans le prochain chapitre, nous procéderons à l'implémentation de ces solutions et nous les mettrons en pratique à travers des cas d'utilisation spécifiques.

## **CHAPITRE IV – Implémentation et test des solutions**

Dans ce chapitre nous allons présenter l'environnement de déploiement des solutions choisis, leurs architectures ainsi de leurs processus d'installation et d'établir des use-case pour les deux solutions

## INTRODUCTION

Ce chapitre sera dédié pour présenter l'environnement de test d'Orange Cyberdefense ainsi des prérequis d'installation et l'architecture des solutions et de leurs processus d'installation ensuite on va simuler des cas d'utilisation pour chaque solution.

### 1. Présentation du laboratoire

L'architecture réseau de l'entreprise cliente est basée sur les quatre composants principaux suivants :

- **FortiGate Firewall** : Pour le contrôle du flux entrant et sortant ainsi que pour l'accès VPN à distance.
- Check Point Firewall : Pour filtrer la communication interne de l'entreprise.
- **Les Switchs :**
  - Switch Users : Pour l'équipe de sécurité.
  - Switch Infra : Diviser en trois VLAN, un VLAN pour le département IT, et un VLAN pour les autres départements.
- **Zone DMZ** : Une zone réseau démilitarisée sécurisée qui héberge les serveurs et les ressources exposées de lab.

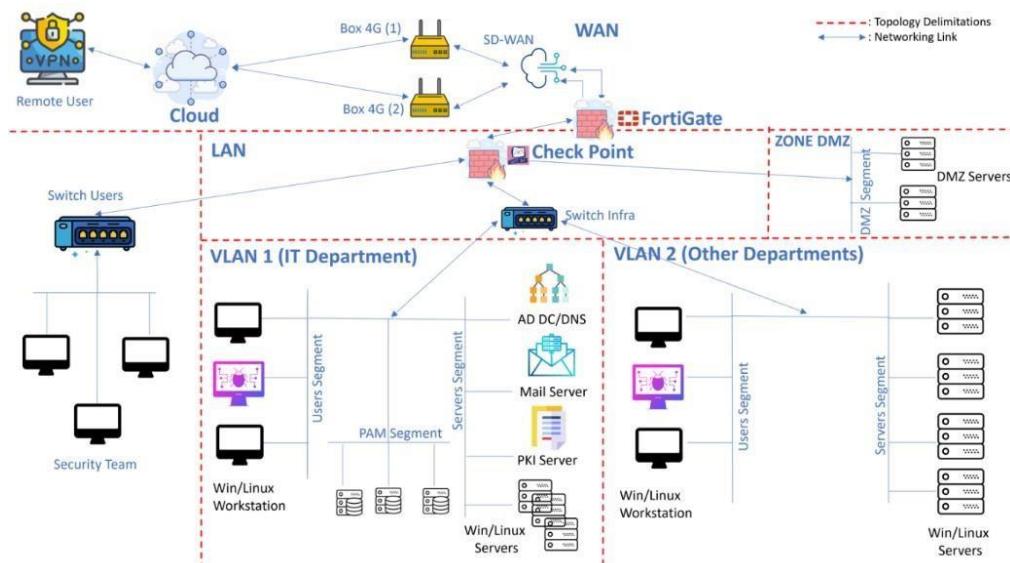


Figure 4.1: Architecture du lab

## 2. Architecture des solutions choisies

### 2.1 SAS PCE :

L'architecture proposé correspond à l'architecture de forte disponibilité pour les entreprises de petite et taille moyenne qui est recommandé par Thales, composé par : Deux serveurs SAS PCE (un primaire et un autre secondaire), base de données MySQL (Master, Slave), Rôle NPS.

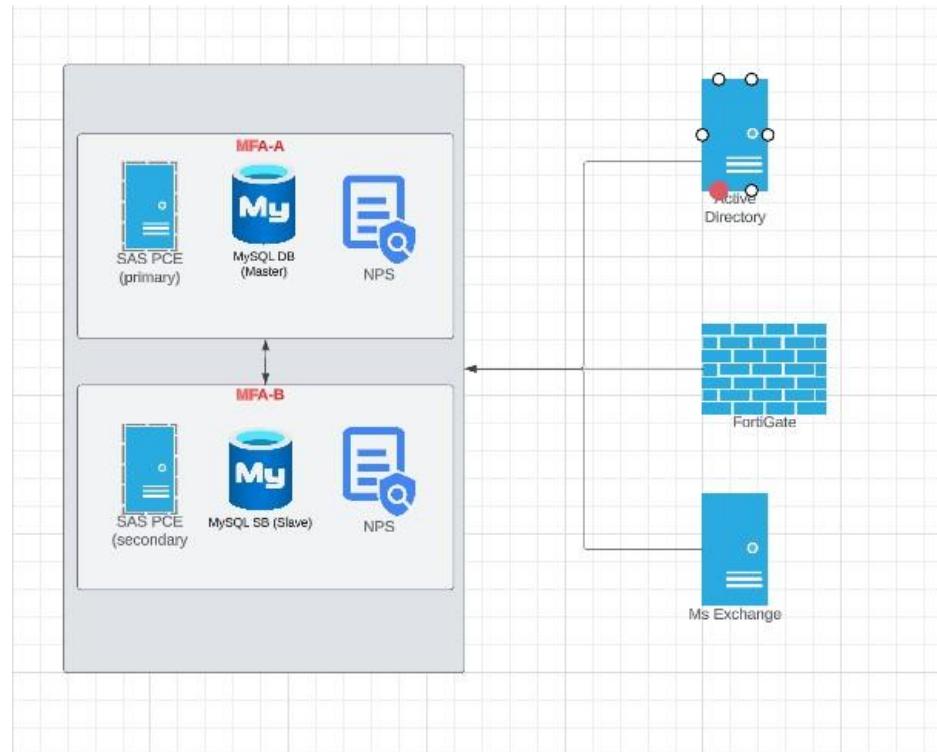


Figure 4.2: Architecture du SAS PCE

- **MFA-A et MFA-B :**
  - ✓ Il s'agit des serveurs Windows sur lesquels les composants de la solution seront installés ainsi que les bases de données qui seront utilisées par la solution.
  - ✓ Le rôle NPS est installé sur les deux pour supporter les équipements qui font l'authentification à base de RADIUS
  - ✓ Dans le cadre de ce projet, les bases de données utilisées sont du MySQL.
- **Base de données :**

- ✓ Le système de base de données utilisé est MySQL en versions 8.0.12 community.  
Les bases de données contiennent toutes les données de configuration, des politiques de sécurité et d'évènement de la solution SAS PCE.
- ✓ Toutes les instances SAS PCE accède à une seule base de données à la fois, il s'agit de la base de données déclarée Master.
- ✓ L'intégrité de la solution repose principalement sur la sécurisation des bases de données. De ce fait, la Haute disponibilité de la plateforme consiste à assurer à la réPLICATION de celle-ci (Flux « RéPLICATION BD ») ainsi que le basculement automatique en cas de défaillance depuis la BD Master vers la Slave (Flux « Accès à la BD Slave en cas de bascule »). La haute disponibilité est gérée nativement par la solution à travers le composant SAS HA Controller Service. □ **SAS-HA Controller Service**
- ✓ Il s'agit d'un composant logiciel installé sur le serveur 2 et qui est responsable de la configuration et de la gestion de la réPLICATION MySQL. Il configure les serveurs MySQL en mode primaire-secondaire. Il s'assure également que la base de données est hautement disponible pour SAS.
- ✓ Si le serveur MySQL primaire n'est pas accessible à SAS, après avoir essayé 5 fois de se connecter au serveur MySQL primaire, le SAS HA Controller Service promeut un serveur MySQL secondaire approprié comme nouveau serveur primaire.

- **Active Directory :**

Il s'agit de l'active directory du lab, où les différentes données sur les utilisateurs sont localisées, donc l'intégration de la solution avec l'AD est une nécessité pour ne pas refaire le processus d'une façon manuel dans l'interface □ **Microsoft Exchange :**

C'est le serveur mail de l'environnement, avant l'implémentation de la solution MFA, l'authentification se faisait en entrant seulement le login et mot de passe, l'objectif c'est d'ajouter un autre facteur de vérification qui va être le token généré par l'application de vérification de Thales appelé MobilePASS, disponible dans plusieurs systèmes d'exploitation comme : Android, iOS et Windows

## 2.2 SailPoint IdentityIQ :

#### Chapitre IV – Implémentation des solutions

Avant de présenter l'architecture de SailPoint IdentityIQ, il est important de noter que compte tenu des limitations de ressources dans l'environnement de laboratoire, l'architecture proposée sera installée sur une machine hébergée dans le cloud. Cette approche me permettra d'effectuer les cas d'utilisation et les configurations nécessaires pendant que le laboratoire sera étendu en termes de ressources RAM.

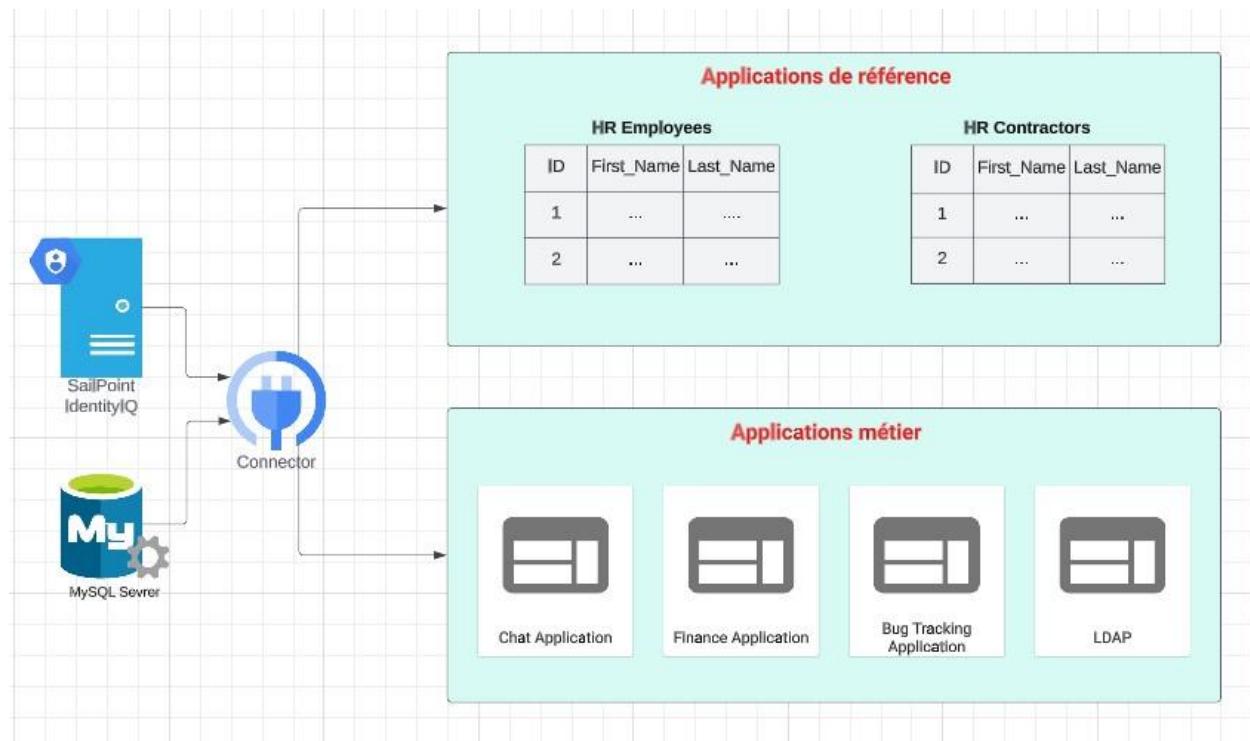


Figure 4.3: Architecture de la solution SailPoint IdentityIQ

- **Applications de référence :**

Les applications de référence sont les applications qui sont la source primaire des données liées aux utilisateurs de l'entreprise, chaque fois SailPoint détecte qu'une nouvelle identité (un nouvel employé qui vient d'intégrer l'entreprise) a été ajouté, il crée un nouveau cube d'identité propre à cet utilisateur, ce cube va être appelé cube d'autorité, parce qu'il a été créé depuis une application de référence

- **Application métier**

Les applications métier font référence aux logiciels ou systèmes spécifiques utilisés par une organisation pour soutenir ses opérations quotidiennes.

Les deux types d'application sont connecté à SailPoint IdentityIQ via des connecteurs, SailPoint supporte par défaut plusieurs applications populaire chose qui facilite énormément la procédure d'intégration

- **Base de données :**

La base de données de SailPoint IdentityIQ sert de référentiel central pour stocker, gérer et organiser les informations essentielles relatives aux identités des utilisateurs, aux accès, aux rôles et aux politiques de sécurité. Elle permet une gouvernance efficace des identités et une gestion cohérente des accès au sein de l'organisation.

### 3. Prérequis pour le déploiement

#### 3.1 Prérequis systèmes de SAS PCE :

Pour une installation réussie, il est nécessaire de vérifier les prérequis suivant avant de commencer.

	Rôle	CPU	RAM	Stockage	OS
MFA-A	Instance SAS PCE avec DB Master Seveur NPS	2 Core 2.6 Ghz	16 Go	300 Go	Windows Server 2012 ou Windows Server 2012 R2 ou Windows Server 2016 64 bit ou Windows Server 2019 64 bit
MFA-B	Instance SAS PCE avec DB Slave + HA Controller service Serveur NPS	2 Core 2.6 Ghz	16 Go	300 Go	Windows Server 2012 ou Windows Server 2012 R2 ou Windows Server 2016 64 bit ou Windows Server 2019 64 bit

Tableau 4.1: Prérequis systèmes de SAS PCE

#### 3.2 Prérequis logiciel de SAS PCE :

*Chapitre IV – Implémentation des solutions*

Avant de plonger dans les détails de l'installation, examinons attentivement les prérequis logiciels nécessaires pour déployer avec succès l'authentification forte dans notre environnement de test

	Rôle	Prérequis
MFA-A	Instance SAS PCE avec DB Master, NPS Server	<ul style="list-style-type: none"> <li>- MySQL 8.0.18</li> <li>- MySQL Connector 6.10.7</li> <li>- Internet Information Services (IIS) 8.5</li> <li>- .NET 4.8</li> <li>- .NET Framework 3.5 Features</li> <li>- Rôle Microsoft NPS</li> </ul>
MFA-B	Instance SAS PCE avec DB Slave + HA Controller service, NPS Server	<ul style="list-style-type: none"> <li>- MySQL 8.0.18</li> <li>- MySQL Connector 6.10.7</li> <li>- Internet Information Services (IIS) 8.5</li> <li>- .NET 4.8</li> <li>- .NET Framework 3.5 Features</li> <li>- Rôle Microsoft NPS</li> </ul>

Tableau 4.2: Prérequis logiciels de SAS PCE

### 3.3 Matrice des flux réseau de SAS PCE :

Pour assurer une connectivité fluide et sécurisée, il est essentiel de prendre en compte les différents ports réseau utilisés par les serveurs SAS PCE et les composants associés.

Port	Direction	Composant concerné	Descriptif
80/443	Sortant / Entrant	Les serveurs SAS PCE	Les ports 80 et/ou 443 peuvent être utilisés pour les sessions de gestion, l'approvisionnement, l'autoinscription, le libre-service et pour le traitement des demandes d'authentification chiffrées des agents configurés. Pour des raisons de sécurité, le port 443 (SSL) est recommandé
1812/1813	Sortant	Les serveurs SAS PCE	Les ports 1812/1813 sont des ports standard pour l'authentification RADIUS et la comptabilité RADIUS respectivement
389	Sortant	Les serveurs SAS PCE	Le port 389 est le standard pour les connexions LDAP
25	Sortant	Les serveurs SAS PCE	Le port par défaut pour l'envoi des emails en SMTP
8456	Entrant	Les serveurs SAS PCE	Le numéro de port par défaut pour le trafic de synchronisation LDAP vers/dépuis SAS et LDAP
8458	Entrant	Les serveurs SAS PCE	Le numéro de port entrant par défaut pour l'agent de journalisation
11012	Sortant / Entrant	Les serveurs SAS PCE	Le port par défaut pour la communication entre SAS et SAS HA Controller Service

Tableau 4.3: Matrice des flux réseau

### 4. Implémentation de SAS PCE :

#### Chapitre IV – Implémentation des solutions

Une fois l'installation du Windows Server 2016 a terminé, nous allons commencer par l'installation des prérequis logiciels



Figure 4.4: Installation du IIS

Une fois terminer on passe à l'installation de la base de données MySQL

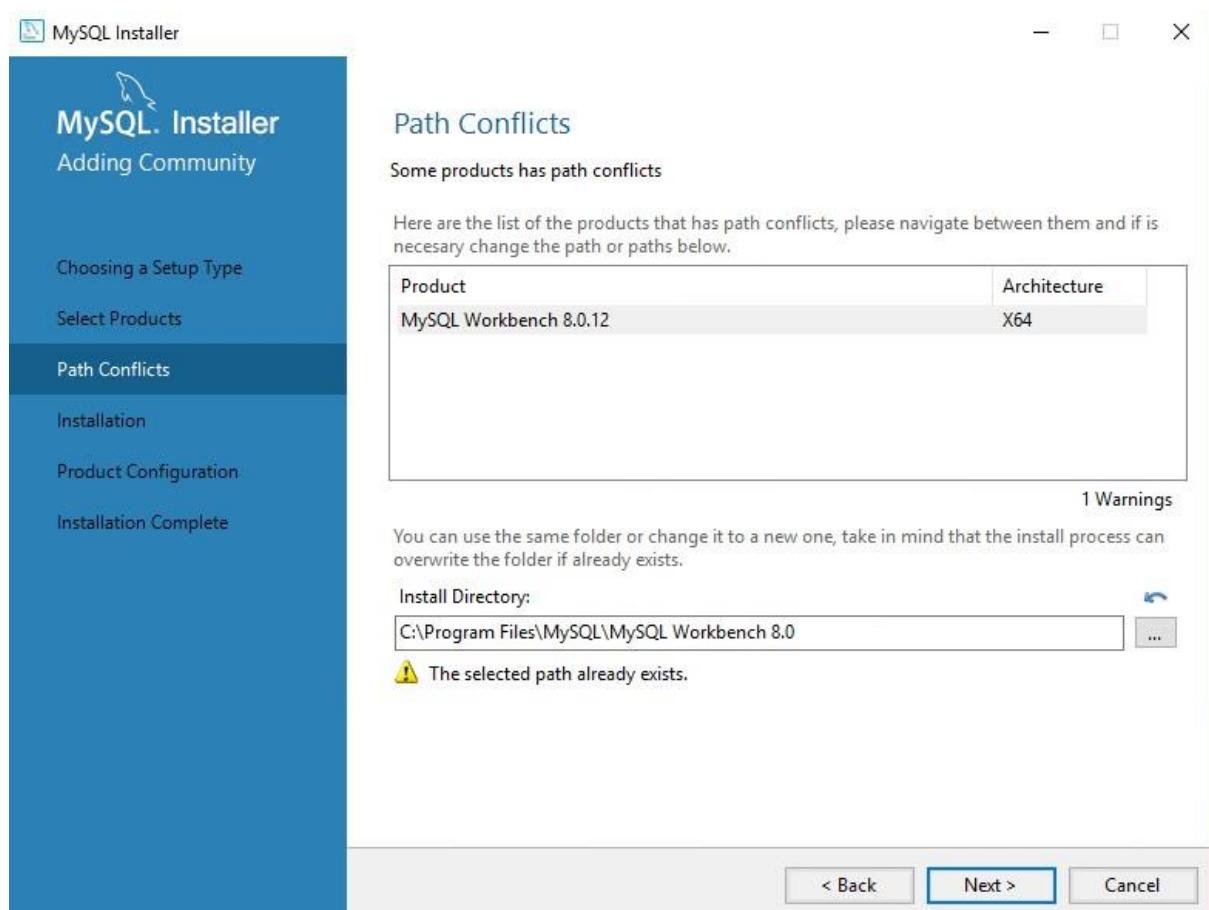
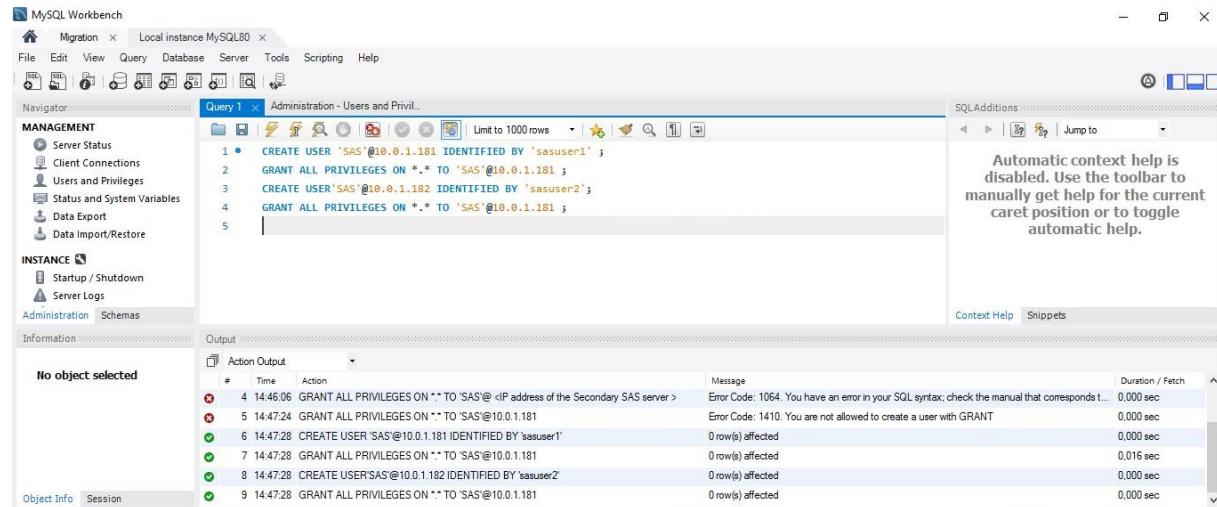


Figure 4.5: Installation de MySQL

#### Chapitre IV – Implémentation des solutions

Une fois la base de données est installée, on va créer des utilisateurs pour accéder à la base de données SAS et accorder l'accès en cas de basculement à chaque instance, la procédure va être répété pour l'autre instance aussi.



The screenshot shows the MySQL Workbench interface with the following details:

- File Bar:** Migration, Local instance MySQL80, File, Edit, View, Query, Database, Server, Tools, Scripting, Help.
- Navigator:** MANAGEMENT (Server Status, Client Connections, Users and Privileges, Status and System Variables, Data Export, Data Import/Restore), INSTANCE (Startup / Shutdown, Server Logs, Administration, Schemas), Information.
- Query Editor:** Query 1 - Administration - Users and Privil... contains the following SQL code:
 

```

1 • CREATE USER 'SAS'@'10.0.1.181' IDENTIFIED BY 'sasuser1';
2 GRANT ALL PRIVILEGES ON *.* TO 'SAS'@'10.0.1.181';
3 CREATE USER 'SAS'@'10.0.1.182' IDENTIFIED BY 'sasuser2';
4 GRANT ALL PRIVILEGES ON *.* TO 'SAS'@'10.0.1.182';
5
      
```
- Output Window:** Shows the execution log with rows 4 and 5 failing due to syntax errors (Error Code: 1064) and permission denied (Error Code: 1410).
- SQL Additions:** A note: "Automatic context help is disabled. Use the toolbar to manually get help for the current caret position or to toggle automatic help."

Figure 4.6: Création des utilisateurs dans MySQL

Le résultat de cette étape est la création de ces utilisateurs dans les deux bases de données



The screenshot shows the MySQL Workbench interface with the following details:

- File Bar:** Local instance MySQL57, File, Edit, View, Query, Database, Server, Tools, Scripting, Help.
- Navigator:** MANAGEMENT (Server Status, Client Connections, Users and Privileges, Status and System Variables, Data Export, Data Import/Restore), INSTANCE (Startup / Shutdown, Server Logs, Options File), PERFORMANCE (Dashboard), Information.
- Table View:** Local instance MySQL57 - Users and Privileges shows the following data:

User	From Host
mysql.session	localhost
mysql.sys	localhost
repuser	10.0.1.181
repuser	10.0.1.182
root	localhost
sas	10.0.1.181
sas	10.0.1.182

- Buttons:** Add Account, Delete, Refresh.

Figure 4.7: Liste des utilisateurs MySQL

L'étape suivante sera de configurer la réPLICATION de MySQL, on commence par modifier le fichier **my.ini** qui est localisé dans l'emplacement suivant **%ProgramData%\<MySQL Server>**

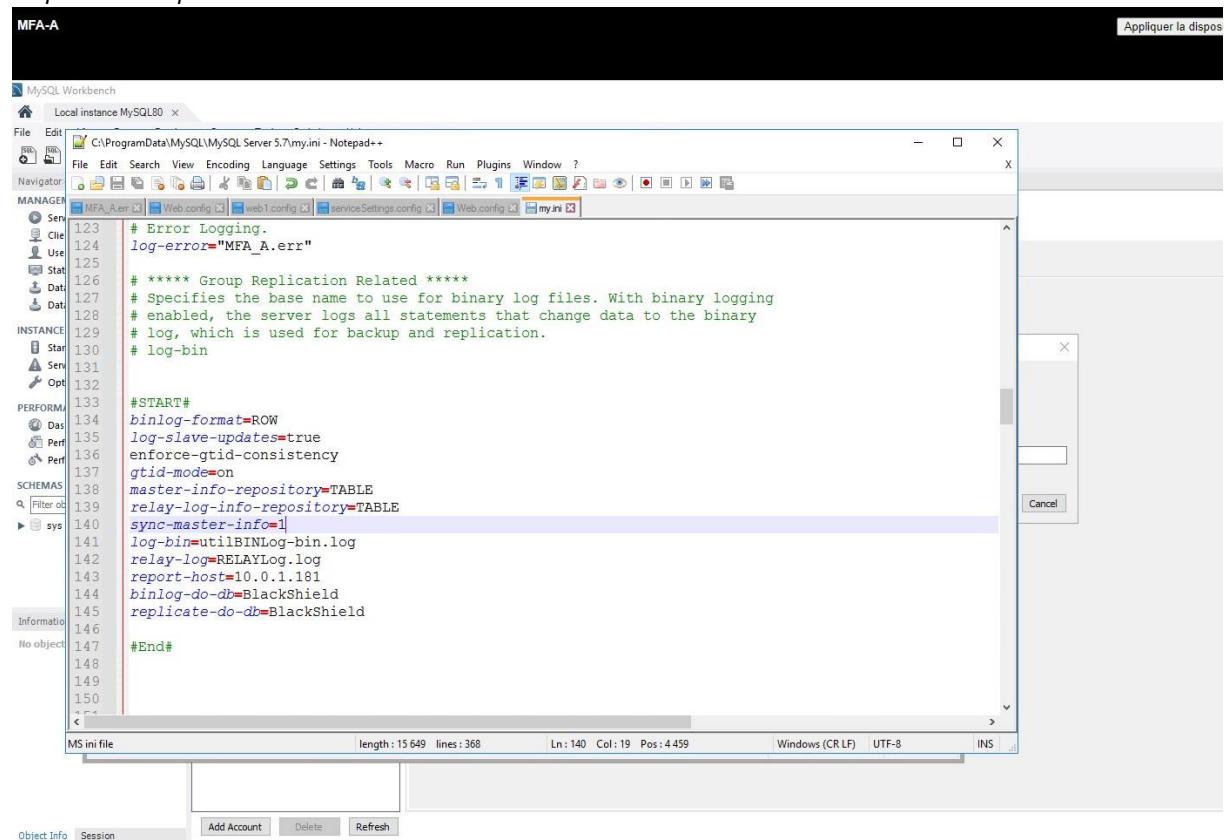


Figure 4.8: Liste des utilisateurs MySQL

Après avoir installé les autres prérequis, on exécute le fichier d’installation **BlackShield ID Service Provider Edition x 64.exe** pour procéder à l’installation de SafeNet Authentication Service.

Le reste de la configuration va se faire sur l’interface graphique de SAS PCE en tapant (<http://10.0.1.181/console>) dans le navigateur.

Une fois connecté à la plateforme, la première chose à configurer c’est la réplication base de données en naviguant vers **System>Database>SQL Database**. Par suite nous allons fournir les informations liées aux adresses IP des bases de données et les identifiant des utilisateurs qu’on vient de créer au niveau de MySQL.

Une fois la connexion est aboutie on reçoit le message de succès suivant :

## Chapitre IV – Implémentation des solutions

The screenshot shows the 'System' tab selected in the navigation bar. Under 'Database', there is a table with one row: 'SQL Database' which 'Configure connections to SQL databases'. Below the table are three buttons: 'Done', 'Back', and 'Cancel'. A note at the bottom says: 'Configuration Complete. Click Done to save.' and 'NOTE: Two files (Cipher.bak & CipherKey.b64) have been created in your SafeNet Authentication Service install directory under the CipherExport directory. These files are necessary to perform a SafeNet Authentication Service server restore.'

**Figure 4.9: Configuration de Database réussite**

Après on va créer le compte de notre entreprise en naviguant vers **On-Boarding**

The screenshot shows the 'On-boarding' tab selected. In the 'Create Account' section, an account named 'OCD\_LAB' is being created. The 'Billing Address' section contains fields for Address 1, Address 2, City, State, Country, and Postal/Zip. There are also fields for Address 1, Address 2, Custom #1, Custom #2, Custom #3, Profile, and Group. At the bottom, there are 'Save' and 'Cancel' buttons.

**Figure 4.10: Crédit du compte Orange Cyberdefense**

Après la finalisation de celle-ci, on effectue une exportation du site (de toutes les config de MFA-A) vers le site MFA-B pour ne pas refaire les mêmes étapes

Depuis MFA-A on navigue vers **Setup > Site > Site export**

The screenshot shows the 'Site Export' configuration page. It includes fields for 'File Key' (containing '185ebf8783b4df11ef399dd0b71ba'), 'Site File', and two 'Save' buttons. A note at the bottom states: 'Important: If you have configured SafeNet Authentication Service to use a database or LDAP server using "localhost" or a loopback IP, your site export will not work. You must reconfigure your system to use either hostnames.'

**Figure 4.11: Site export**

On importe le fichier « **Site File** » ainsi de la clé du fichier dans MFA-B



Dans les deux serveurs, nous allons installer le serveur NPS et l'agent SafeNet for NPS qui vont gérer les requêtes d'authentification via le protocole RADIUS.

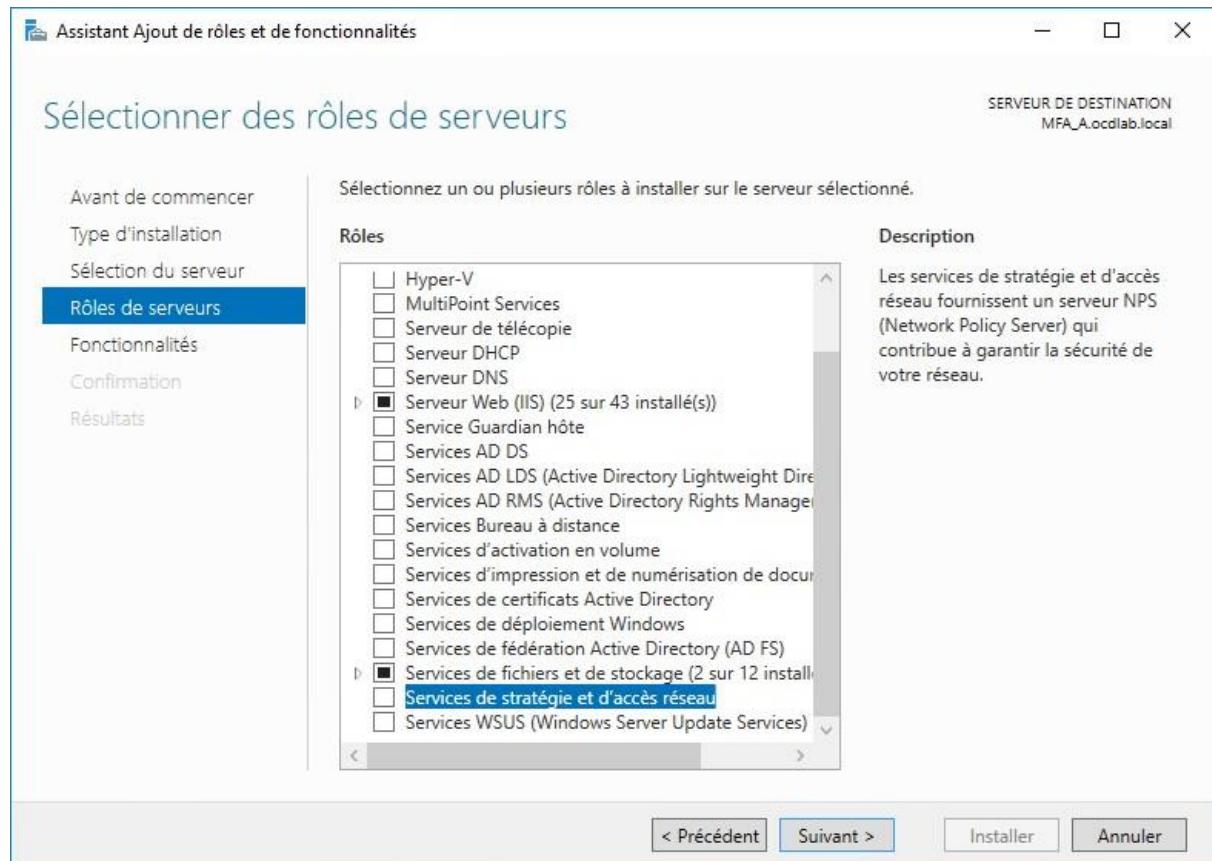


Figure 4.12: Rôle NPS dans Windows Server



Figure 4.13: Installation de l'agent SafeNet pour NPS

L'étape qui suit s'agit de la configuration du compte « Operator », qui est responsable de la gestion du compte de l'entreprise ou « Virtual Server » qui n'est autre que OCD dans notre cas. L'opérateur de compte reçoit alors un mail de « Self Enrollment » qui va activer son compte ainsi que sa token.

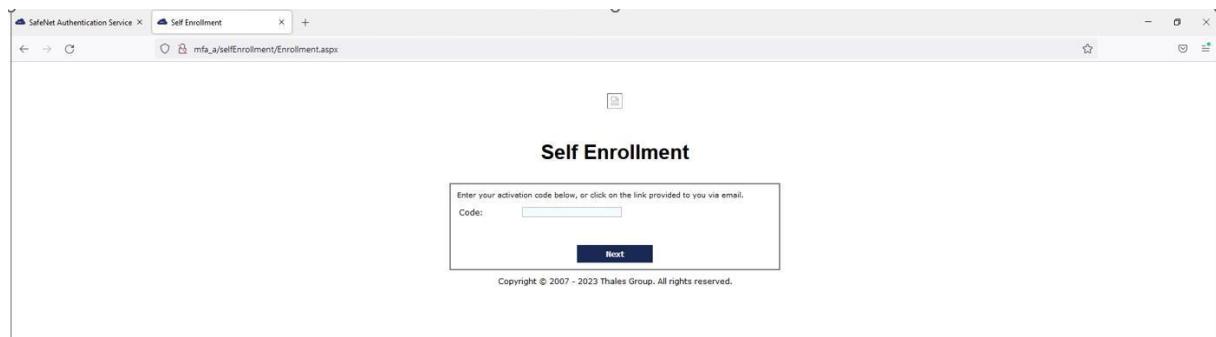


Figure 4.14: Page de Self Enrollment

## 5. Simulation de la MFA :

### Présentation du cas d'utilisation :

La figure suivante décrit le cas d'utilisation que nous allons établir, ainsi de la démarche de la double authentification assuré par SAS PCE :

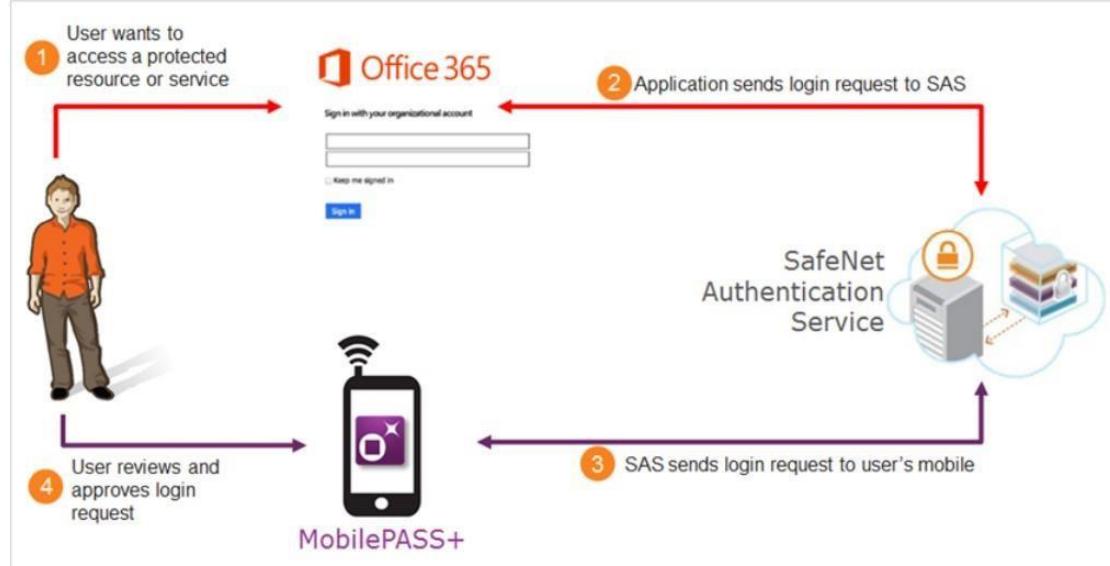


Figure 4.15: Les étapes d'authentification

1. L'utilisateur souhaite accéder à une application qui nécessite une authentification à deux facteurs (par exemple, Office 365). Il fournit son nom d'utilisateur et son mot de passe, puis clique sur le bouton Se connecter.
2. L'application envoie les demandes de connexion au serveur, qui identifie l'utilisateur et son appareil mobile.
3. Le serveur déclenche directement une demande d'authentification en mode "on-the-go". Si le mode "push" est utilisé, l'utilisateur reçoit une notification "push" sur son appareil mobile pour indiquer qu'une demande de connexion est en attente.
4. L'utilisateur tape sur la notification pour afficher les détails de la demande de connexion, et répond par une tape pour approuver ou refuser la demande. (Dans certains cas, l'utilisateur devra fournir un code PIN supplémentaire avant d'être autorisé à afficher et à répondre à la demande de connexion). La réponse (à laquelle est joint un code d'accès) est renvoyée au serveur, où elle est validée. Lorsque l'authentification réussit, l'application est automatiquement actualisée et l'accès est accordé à l'utilisateur.

#### Simulation avec le serveur Outlook de l'environnement de test

Une fois l'intégration avec Outlook est terminée, nous allons utiliser SAS PCE pour authentifier, à l'aide de l'application mobile passe pour avoir un OTP. Donc comme montrer

*Chapitre IV – Implémentation des solutions*  
dans les figures suivantes, l'utilisateur entre son identifiant et son mot de passe, et puis, il prend l'OTP.



Figure 4.16: Processus de l'authentification à l'aide de l'OTP

Et donc, l'authentification va être vérifier et l'accès est garantie

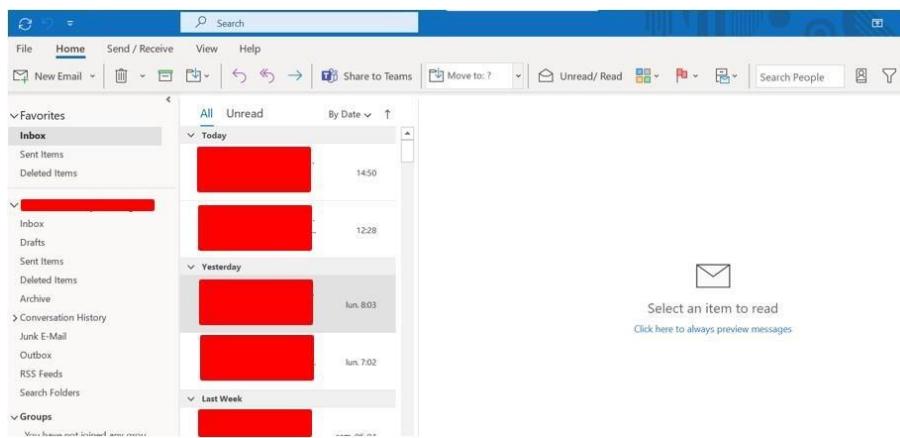


Figure 4.17: Authentification avec succès

## 6. Mise en place de SailPoint IdentityIQ :

Après une installation réussite de la solution, on accède à l'interface graphique de la solution, c'est dans cette interface où la majorité de notre configuration va être effectué :

#### Chapitre IV – Implémentation des solutions

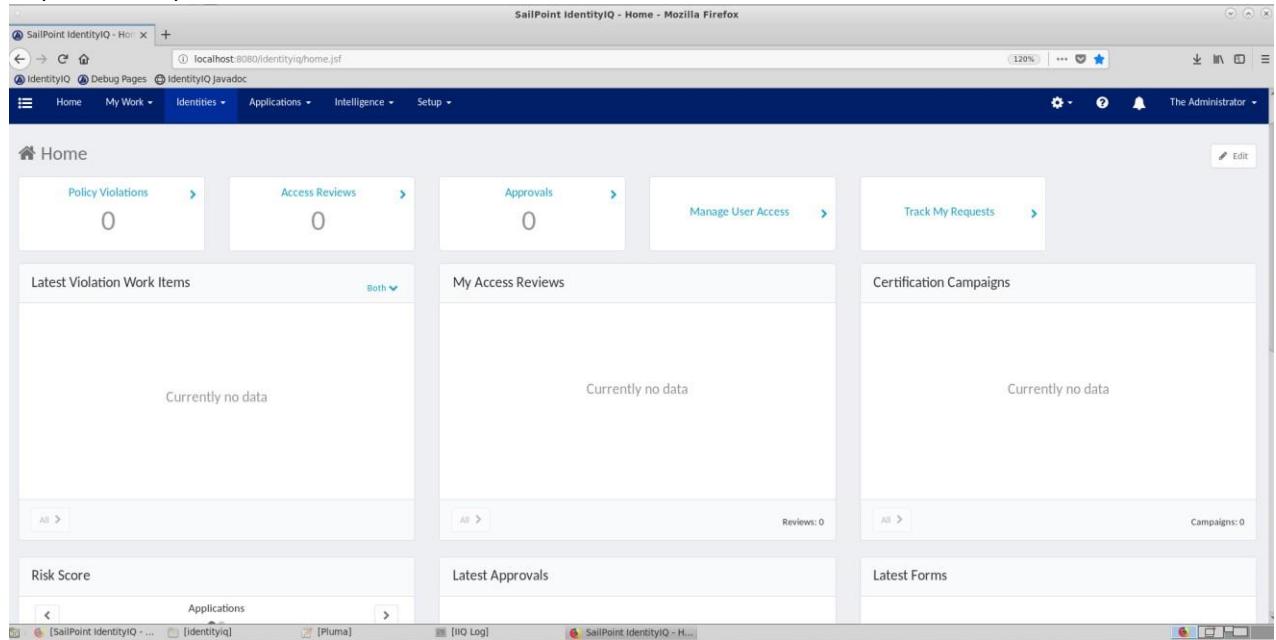


Figure 4.18: Page d'accueil de SailPoint IdentityIQ

#### Plan de configuration et simulation de la solution :

En ce qui concerne l'intégration et la configuration de la solution, nous allons diviser le travail en deux phases :

Une première phase où nous allons ajouter les applications de référence qui sont deux fichiers CSV qui contiennent les informations de tous les employés et tous les sous-traitants de l'entreprise, ainsi de quatre applications métier.

La deuxième phase sera consacrée à l'amélioration des données et les informations des utilisateurs dans la solution en faisant des rapports qui vont détecter les cubes d'identité non corrélé lors de l'agrégation des applications métier, nous allons aussi créer une policy de séparation des tâches et finalement nous allons créer une campagne de certification pour établir un examen d'accès pour tous les employés qui ont accès à l'application de finance

#### Phase 1 :

Nous allons commencer par l'onboarding des applications de référence et les connecter à SailPoint, les figures suivantes montrent les étapes à suivre :

## Chapitre IV – Implémentation des solutions

The screenshot shows the SailPoint IdentityIQ - Application Definition page. At the top, there is a browser header with the URL [localhost:8080/identityiq/define/applications/applications.jsf](http://localhost:8080/identityiq/define/applications/applications.jsf). Below the header, the main interface has a dark blue header bar with navigation links: Home, My Work, Identities, Applications, Intelligence, and Setup. On the right side of the header, it says "The Administrator". The main content area is titled "Application Definition". A yellow banner at the top states: "No authoritative applications defined in the system, all identities will be marked uncorrelated." Below this, there is a search bar labeled "Filter by Application Name" and a button labeled "Add New Application". A table lists applications with columns: Name, Host, Type, Aggregation Types, and Modified. The table is currently empty. At the bottom of the table, there are pagination controls (Page 0 of 0), a dropdown for items per page (Show 25), and a note: "No data to display". The footer contains the copyright notice: "© Copyright 2011 IdentityIQ Technologies. All rights reserved."

The screenshot shows the "Edit Application HR Employees" configuration page. The top navigation bar includes "Details", "Configuration", "Correlation", "Risk", "Activity Data Sources", "Rules", and "Password Policy". The "Configuration" tab is selected. The "Settings" sub-tab is also selected. The main form fields include "Name" (HR Employees), "Owner" (The Administrator), "Application Type" (DelimitedFile), "Revoker", "Proxy Application", and "Profile Class". There is a rich text editor for "Description" and a section for "Authoritative Application" settings with checkboxes for "Case Insensitive", "Native Change Detection", and "Maintenance Enabled". The "Authoritative Application" checkbox is checked.

The screenshot shows the "Edit Application HR Employees" schema configuration page. The top navigation bar includes "Details", "Configuration", "Correlation", "Risk", "Activity Data Sources", "Rules", and "Password Policy". The "Settings" sub-tab is selected. The "Schema" sub-tab is also selected. The "Object Type: account" section includes tabs for "File", "Filtering", "Merging", and "Iteration Partitioning". Configuration options for "File Path" (set to "/home/spadmin/impl/identity/training/data/AuthEmployee"), "File Encoding" (empty), "File Transport" (set to "Local"), "Parsing Type" (set to "Delimited"), "Delimiter" (empty), and "Columns" (empty) are shown. A "Test Connection" button is at the bottom.

## Chapitre IV – Implémentation des solutions

The screenshot shows the configuration interface for the 'account' object type. It includes sections for 'Details' and 'Attributes'. In the 'Details' section, fields include 'Native Object Type' (account), 'Display Attribute' (fullName), 'Identity Attribute' (employeeId), and 'Instance Attribute' (empty). Under 'Attributes', there is a table listing attributes like employeeId, firstName, lastName, managerId, and fullName, each with a string type and edit button.

Name	Description	Type	Properties
employeeId		string	
firstName		string	
lastName		string	
managerId		string	
fullName		string	

Figure 4.20: Définition de l'application HR Employees

Après la finalisation de ses étapes, on refait la même procédure pour l'application « **HR Contractors** »

The screenshot shows the 'Application Definition' page in the SailPoint interface. It lists two applications: 'HR Contractors' and 'HR Employees', both of which are of type 'DelimitedFile' and have 'account' as their aggregation type. The 'HR Contractors' application was modified on 5/22/2023 at 04:03:01 am, while 'HR Employees' was modified on 5/21/2023 at 04:08:23 pm.

Name	Host	Type	Aggregation Types	Modified
HR Contractors	localhost	DelimitedFile	account	5/22/2023 04:03:01 am
HR Employees	localhost	DelimitedFile	account	5/21/2023 04:08:23 pm

Figure 4.19: Définition des deux applications de référence

Les données ne seront pas lues tant qu'on n'a pas exécuter une tâche d'agrégation, pour faire ce, on navigue vers : **Setup > Tasks > New Task > Account Aggregation**



Après la création de cette tache en précisant l'application cible (HR Employees), nous allons l'exécuter

#### Chapitre IV – Implémentation des solutions

Attributes				
Attribute	Value			
Applications scanned	HR Employees			
Accounts scanned	162			
Identities created	162			

Application	Account	Action	Identity	Attribute
HR Employees	1a	Create	James.Smith	
HR Employees	1b	Create	Jakob.Brouwer	
HR Employees	1c	Create	Aaron.Nichols	
HR Employees	1a2ax	Create	DeShaun.Harris	
HR Employees	1a2a	Create	Mary.Johnson	
HR Employees	1a2b	Create	Jose.Silva	
HR Employees	1a2c	Create	Amy.Chen	
HR Employees	1a2a3d	Create	Barbara.Wilson	
HR Employees	1a2a3b	Create	Linda.Davis	
HR Employees	1a2a3c	Create	Michael.Miller	
HR Employees	1a2a3a	Create	Robert.Brown	

Figure 4.20: Résultat de la tâche d'agrégation

On refait la même chose pour l'autre application, en naviguant vers Identity Warehouse on trouve que les utilisateurs ont été bien créer, et les attributs de chaque identité ont été bien importé

#### Identity Warehouse

User Name	First Name	Last Name	Manager	Assigned Role Summary	Detected Role Summary	Risk Score	Last Refresh	Type
Adam.Kennedy	Adam	Kennedy	Douglas.Flores	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Aditi.Anand	Aditi	Anand	Howard.Rose	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Akina.Date	Akina	Date	Yiro.Ito	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Alan.Bradley	Alan	Bradley	Eugene.Hawkins	● 0	● 0	● 0	5/22/23 8:04 AM	Contractor
Albert.Visser	Albert	Visser	Patrick.Jenkins	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Alice.Fribourg	Alice	Fribourg	Sophie.Comans	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Allen.Burton	Allen	Burton	Sara.Berry	● 0	● 0	● 0	5/22/23 8:04 AM	Contractor
Amanda.Ross	Amanda	Ross	Jakob.Brouwer	● 0	● 0	● 0	5/22/23 8:04 AM	Employee
Amie.Wong	Amie	Wong	Howard.Rose	● 0	● 0	● 0	5/22/23 8:04 AM	Employee

Displaying 1 - 50 of 235

Figure 4.21: Identity Warehouse

Si on clique sur un utilisateur (Adam Kennedy) nous allons accéder à son cube d'identité, qui est une interface qui contient toutes les informations d'un utilisateur (nom, prénom, manager, département, permissions, ses comptes, les policy...)

## Chapitre IV – Implémentation des solutions

[View Identity Adam.Kennedy](#)

The screenshot shows a table of user attributes for Adam Kennedy. The columns include User Name, First Name, Last Name, Email, Manager, Type, Department, Location, Employee ID, Region, Job Title, and Cost Center. The data is as follows:

User Name	Adam.Kennedy
First Name	Adam
Last Name	Kennedy
Email	
Manager	Douglas.Flores
Type	Employee
Department	Accounting
Location	London
Employee ID	1b2c3a4e
Region	Europe
Job Title	Payroll Analyst II
Cost Center	R01e L03e

Figure 4.22: Adam Kennedy cube d'identité

On refait la même procédure, uniquement cette fois pour des applications métier, la grande différence c'est lorsque SailPointIQ va scannée les utilisateurs de ces applications, il ne va pas créer de nouveaux cubes d'identité, mais d'ajouter les comptes trouvés sur le cube de l'employé déjà existant.

### Application Definition

The screenshot shows a table of registered applications. The columns are Name, Host, Type, Aggregation Types, and Modified. The data is as follows:

Name	Host	Type	Aggregation Types	Modified
Bug Tracking	localhost	JDBC	account	
Chat Application	localhost	JDBC	account, group	
Finance	localhost	DelimitedFile	account, group	
HR Contractors	localhost	DelimitedFile	account	5/22/2023 09:25:27 am
HR Employees	localhost	DelimitedFile	account	5/22/2023 09:25:39 am
LDAP	training.sailpoint.com	OpenLDAP - Direct	account, group	5/22/2023 11:17:01 am
Time Tracking	localhost	JDBC	account	5/22/2023 11:27:53 am

Figure 4.23: On-boarding des applications métier

### Phase 2 :

Dans cette phase nous allons commencer par un rapport qui va détecter les identités qui n'ont pas été proprement corrélé et affecté aux cubes de référence.

On navigue vers **Intelligence > reports > uncorrelated accounts reports** et on clique sur execute

The screenshot shows the Reports interface with the 'Reports' tab selected. A search bar at the top contains the text 'uncorrelated'. Below it, a table lists a single report: 'Uncorrelated Accounts Report'. The table has columns for Name and Description. The description for this report is: 'A detailed view of the uncorrelated user accounts in the system.' At the bottom of the report card, there are four buttons: 'Save As New Report', 'Schedule', 'Execute', and 'Delete'.

## Uncorrelated Accounts Report

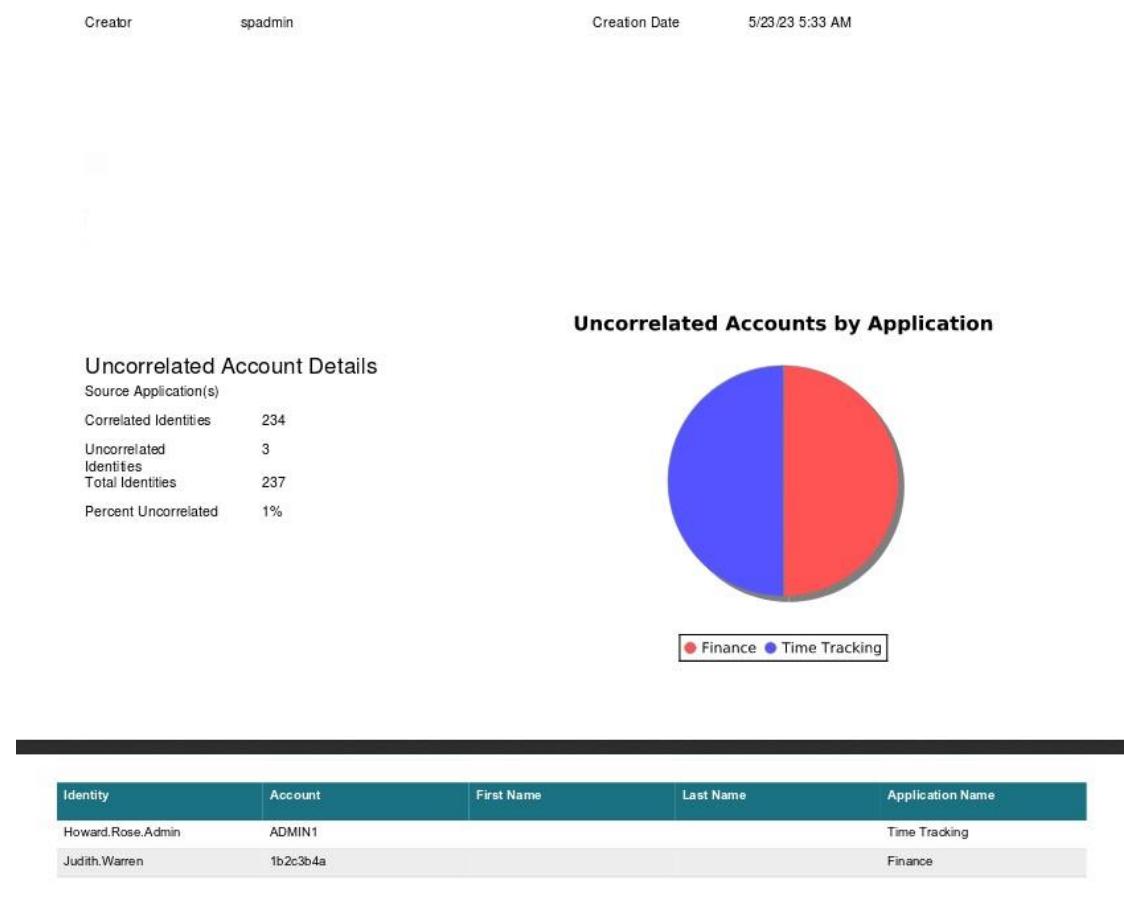


Figure 4.24: Résultat de rapport des utilisateurs non corrélé

Pour fixer ce problème, on navigue vers **identities>identity Correlation** et on spécifie l’application où on a eu ce problème (time tracking, finance) et on sélectionne le compte non corrélé, ainsi de l’utilisateur qui a eu ce problème (Howard Rose, Judith Warren) et on clique sur merge

The screenshot shows two main panels: "Select Unrelated Accounts" and "Select Target Identity".

**Select Unrelated Accounts:** This panel lists accounts from the "Time Tracking" application. Two accounts are selected: "Howard.Rose.Admin" and "Judith.Warren".

Account	Type
Howard.Rose.Admin	Time Tracking
Judith.Warren	Finance

**Select Target Identity:** This panel lists identities from both "Time Tracking" and "Finance" applications. The "Howard.Rose" identity is selected.

Identity	First Name	Last Name	Correlated	Manager	Email	Created Date	Last Modified	Type
Howard.Rose	Howard	Rose	Yes	Maria White	How.Rose@democracygrid.com	2023-05-23 10:00:22	2023-05-23 10:00:22	Employee
Judith.Warren	Judith	Warren	No	John Smith	Judith.Warren@democracygrid.com	2023-05-23 11:00:27	2023-05-23 11:00:27	Employee
Howard.Rose	Howard	Rose	No	Vince Foster	Howard.Rose@democracygrid.com	2023-05-23 11:00:45	2023-05-23 11:00:45	Employee

Figure 4.25: Résolution manuelle des comptes non corrélé

### Séparation des tâches :

Le but de cet use-case est de détecter et restreindre les utilisateurs de l'application finance qui ont les permissions d'approuver et de payer un fournisseur, donc ces deux permissions ne doivent pas être porté par la même personne

Pour créer cette policy, on navigue vers **Setup > policies > new policy > Entitlement SOD Policy**

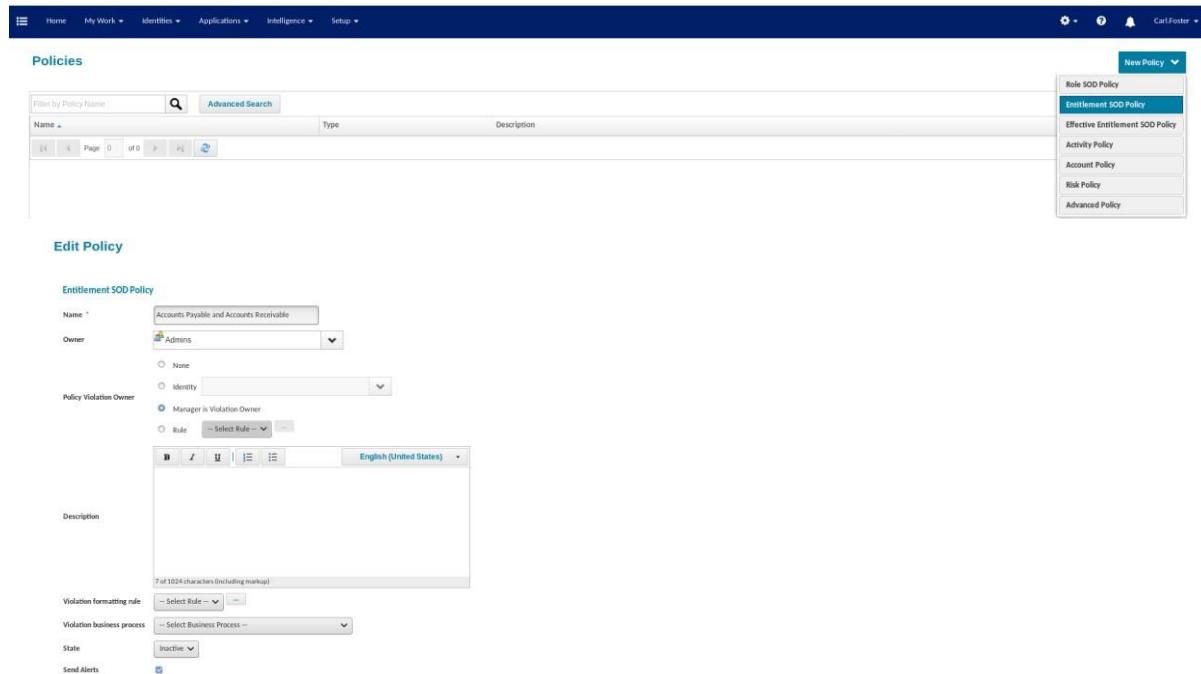


Figure 4.26: Mise en place du policy de séparation des tâches

On doit créer la règle de notre cas d'utilisation, et l'ajouter par suite du policy.

The screenshot shows the 'Edit Entitlement SOD Rule' screen. A rule named 'Cannot have access to Accounts Payable and Account Receivable at the same time' is listed. This rule is currently disabled. Below the rule, there are two 'Entitlement Set' sections. The first entitlement set applies to the 'Finance' application item and checks if the user has 'Account Payable' or 'Account Receivable'. The second entitlement set also applies to the 'Finance' application item and checks if the user has 'Account Receivable'. Both sets use 'Or' logic and are configured with 'Attribute' type and 'Permission Group' source. The 'Is Null' checkbox is checked for both sets.

Figure 4.27: La règle de séparation des tâches

#### Chapitre IV – Implémentation des solutions

On exécute la policy, dans le cas de violation le manager de l'employé qui porte ces deux permissions va être notifié via email pour lui informer et pour qu'il puisse agir par suite.

Policy simulation for Accounts Payable and Accounts Receivable	
Rule Name	Number of violations
Cannot have access to Accounts Payable and Accounts Receivable at the same time	1

Figure 4.28: Résultat de la policy SoD

```
From iga@example.com Wed May 24 16:03:34 2023
Date: Wed, 24 May 2023 16:03:34 -0500 (CDT)
From: iga@example.com
To: Amy.Chen@demoxample.com
Message-ID: <359108092501466ebd9601ac16d9e198@example.com>
Subject: Policy violation by Richard.Jackson
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_Part_2_2077716332.1684962214926"
X-Mailer: smptsend

-----=_Part_2_2077716332.1684962214926
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 7bit

A violation of policy 'Accounts Payable and Accounts Receivable' rule 'Cannot have access to Accounts Payable and Accounts Receivable at the same time' was detected on user 'Richard.Jackson'.
```

Figure 4.29: Mail de violation envoyé au manager

L'administrateur SailPoint peut aussi voir les violations des politiques en allant vers **My Work** > **Policy Violations**. L'administrateur peut soit approuver la violation s'il s'agit d'une exception ou bien de révoqué l'une des deux permissions

Policy Violations					
	Identity	Policy Name	Rule	Owner	Description
	Richard.Jackson	Accounts Payable and Accounts Receivable	Cannot have access to Accounts Payable and Accounts Receivable at the same time	Amy.Chen	

Figure 4.30: Policy Violations

Correct Violation

Violation: Cannot have access to Accounts Payable and Accounts Receivable at the same time

Violation Description:

Remove a set of entitlements to correct the violation.

Entitlements	Conflicting Entitlements
<input checked="" type="checkbox"/> Account Receivable	<input checked="" type="checkbox"/> Account Payable
Accounts Receivable Group for Finance Application	Accounts Payable Group for Finance Application
Application: Finance Attribute: Permission Group	Application: Finance Attribute: Permission Group

Cancel  Revoke

Figure 4.31: Correct Violation

### Certification d'accès :

Le dernier cas d'utilisation que nous allons présenter dans ce rapport est la certification d'accès qui aide les entreprises à garantir et à vérifier d'une façon régulière que les utilisateurs disposent uniquement des accès nécessaires pour effectuer leurs tâches.

On navigue vers **Setup > Certification > New Certification > targeted**

The screenshot shows the SailPoint interface with the following details:

- Who to Certify:** 1 Filters applied.
- What to Certify:** All Additional Entitlements, All Target Permissions.
- Choose Certifier:** Manager selected.
- Schedule:** 5/24/23.
- Additional Settings:** Includes a section for defining items to certify, with 'Additional Entitlements' checked. A filter is applied: Application Equals Finance.

**Figure 4.32: Crédation de la campagne de certification d'accès**

On va spécifier que le certificateur primaire est le propriétaire d'application finance et les admins sont le backup

The screenshot shows the 'Choose Certifier' step with the following details:

- Primary Certifier:** Owner selected.
- Additional Entitlements will be certified by the:** Entitlement Owner selected.
- Backup Certifier:** Admins selected.

On clique sur **Run Now** pour programmer la certification à s'exécuter sur le champ

The screenshot shows the 'Certifications' page with the following details:

- A green banner at the top indicates: Targeted certification scheduled successfully.
- The 'Certifications' tab is selected.
- A table lists the scheduled certification:
 

Name	Owner	Status	Percent Complete	Create Date	Tags
Targeted Certification [5/24/23 5:38:06 PM CDT]	Dennis.Barnes	Pending	Pending	5/24/2023 05:38:07 pm	

**Figure 4.33: Exécution de la certification**

Quand le certificateur se connecte à SailPoint, il peut commencer à certifier les accès depuis **My Work> Access Reviews**

The screenshot shows the 'My Access Reviews' section of a software application. At the top, there's a progress bar indicating 0% completion, due on 6/24/23. The status is 'Completed: 0 / 1' and it was 'Requested By: Dennis Barnes'. Below this, there's a table with one row:

Type	Display Name	Description	Application	Account Name	Identity	Decision
Entitlement	ACCOUNTING on Permission Group	Accounting Group for Finance Application	Finance	Judith.Warren	Howard.Rose	<button>Approve</button> <button>Revoke</button>

Figure 4.34: Examen d'accès

## CONCLUSION

Ce chapitre avait pour but de présenter l'environnement de test d'OCD, les architectures des solutions choisis ainsi des simulations des cas d'utilisation de ces technologies pour mettre en jeu une bonne visibilité sur l'ensemble des utilisateurs et leurs accès et l'implémentation de l'authentification forte.

## **Conclusion Générale et perspectives**

Durant mon stage au sein de l'entreprise Orange Cyberdefense, j'ai eu l'opportunité de participer à un projet passionnant axé sur l'étude et l'implémentation d'une initiative Zero Trust, en mettant en place les technologies d'IGA et de MFA. Ce projet m'a permis de découvrir la complexité et la diversité des compétences requises dans le domaine de la sécurité informatique.

J'ai rapidement réalisé l'importance cruciale de l'approche Zero Trust en matière de sécurité des réseaux. Cette approche gagne en popularité, et de plus en plus d'entreprises reconnaissent la nécessité de mettre en œuvre tout ou partie de ses principes. En adoptant une architecture Zero Trust, les organisations peuvent réduire les risques liés aux accès non autorisés, aux priviléges excessifs et aux attaques d'usurpation d'identité.

L'implémentation des technologies d'IGA et de MFA assure un départ réussi pour une entreprise souhaitant adopter le modèle Zero Trust. L'IGA a permis de renforcer la gestion des identités et des accès, en fournissant une visibilité et un contrôle plus granulaires sur les droits et les priviléges des utilisateurs. Quant au MFA, il a ajouté une couche supplémentaire de sécurité en exigeant des utilisateurs une authentification à plusieurs facteurs, réduisant ainsi les risques d'intrusion.

En termes de perspectives, la suite du projet c'est d'implémenter l'IGA au sein de l'environnement du test et l'intégrer avec les applications déjà présente dans ce dernier une fois assez de ressources sont disponible. Migrer la base de données de la solution SAS PCE du MySQL vers MS SQL reste une option valable pour améliorer la haute disponibilité de la solution car celle-ci est plus stable avec cette base de données. Une fois que le système IAM a atteint un niveau de maturité opérationnel, la voie est ouverte pour intégrer d'autres briques telles que DLP, UEBA, NGFW, PAM, ZTNA...

En conclusion, ce projet a été une occasion précieuse pour moi de progresser professionnellement et personnellement. Il m'a permis d'élargir mes horizons, de me familiariser avec les réalités du monde du travail et d'améliorer mes compétences en matière de sécurité et de solutions de confiance. Je suis reconnaissant d'avoir eu l'opportunité de

participer à ce projet et je suis convaincu que les connaissances et les compétences acquises me seront utiles dans ma carrière future dans le domaine de la sécurité informatique.

#### *Bibliographie*

## **BIBLIOGRAPHIE**

[1] : Orange Cyberdefense [en ligne] [Consulté le 12/02/2023] disponible à l'adresse : <<https://www.orangecyberdefense.com/>>

[2] : Akamai,Modèle de sécurité Zero Trust , [en ligne] [Consulté le 14/02/2023] disponible à l'adresse <<https://www.akamai.com/fr/glossary/what-is-zero-trust#:~:text=Fonctionnement%20de%20mod%C3%A8le%20Zero%20Trust&text=Le%20mod%C3%A8le%20Zero%20Trust%20repose,ext%C3%A9rieur%20de%20ce%20p%C3%A9rim%C3%A8tre%20r%C3%A9seau>>

[3] : Gartner, Zero Trust Network Access, [en ligne] [Consulté le 18/02/2023] disponible à l'adresse : <<https://www.gartner.com/en/information-technology/glossary/zero-trustnetwork-access-ztna>>

[4] : Octa, the state of Zero Trust Security 2032, [en ligne] [Consulté le 21/02/2023] disponible à l'adresse : <<https://www.okta.com/resources/whitepaper-the-state-of-zero-trust-security2021-report>>

[5] : National Institute of Standards and Technology (NIST). Zero Trust Architecture. NIST Special Publication 800-207 (2020). [En ligne] [Consulté le 05/03/2023] Disponible à l'adresse : <<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>>

[6] : Multifactor authentication and how does it work , the state of Zero Trust Security 2032 ,

[en ligne] [Consulté le 12/03/2023] disponible à l'adresse :  
<<https://www.techtarget.com/searchsecurity/definition/multifactor-authentication-MFA>>

**[7]** : Jason Garbis , Jerry W. Chapman. Zero Trust Security. Edition :1ère edition, Année de publication : 2021, Lieu d'édition : Boston, MA, USA ;Atlanta.GA,USA

#### *Bibliographie*

**[8]** : Thales, About Thales, [en ligne] [Consulté le 18/03/2023] disponible à l'adresse : <<https://www.thalesgroup.com/en/global/group>>

**[9]** : Microsoft,Multifactor Authentication , [en ligne] [Consulté le 20/03/2023] disponible à l'adresse : <<https://www.microsoft.com/en-us/security/business/identity-access/azureactive-directory-mfa-multi-factor-authentication>>

**[10]** : Octa, Adaptive Multi-Factor Authentication, [en ligne] [Consulté le 21/03/2023] disponible à l'adresse : <<https://www.okta.com/products/adaptive-multi-factorauthentication/>>

**[11]** : SailPoint,Transform your identity security program , [en ligne] [Consulté le 22/03/2023] disponible à l'adresse : <<https://www.sailpoint.com/>>

**[12]** : Oracle,Oracle Identity Governance , [en ligne] [Consulté le 23/05/2023] disponible à l'adresse : <<https://www.oracle.com/security/identity-management/governance/>>

**[13]** : Saviynt,Identity Governance & Administration , [en ligne] [Consulté le 24/05/2023] disponible à l'adresse : <<https://saviynt.com/solutions/identity-governance-andadministration/>>