RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE SAAD DAHLEB BLIDA

FACULTE DES SCIENCES

Mémoire de fin d'études

Pour l'obtention de diplôme en Master en Informatique

Option : Sécurité des systèmes d'informations / Systèmes d'informatique et réseau

Etude et Mise en place d'un PAM (Privilège Access Management)

Organisme d'accueil : La Banque CPA

Réalisé par :

- Hadj Sadok Yacine
- Haioun Abderahmen

Encadré Par :

- Mme Hireche Célia
- M. Haddad Razik

Jury :

- Mme Boustia Narhimene	Présidente
- M. Cherif Zahar Amine	Examinateur
- Mme Hireche Célia	Promotrice

Promotion: 2022/2023
Date de soutenance: 26/06/2023

Remerciement

En préface de ce briefing, nous remercions Allah qui nous a aidé et nous a donné la patience et le courage durant ces longues études.

Nous tenons à remercier toutes les personnes qui ont contribué au succès de notre stage et qui nous ont aidée lors de la rédaction de ce mémoire.

Nous tenons à exprimer toute notre reconnaissance à note Promotrice Madame Hireche Célia, Nous la remercions de nous avoir encadré, orienté, aidé et conseillé.

Nous tenons à remercier vivement notre maitre de stage, Mr Haddad Razik, Responsable de sécurité des systèmes d'informations au sein de la Bank CPA, pour son accueil, le temps passé ensemble et le partage de son expertise au quotidien. Grâce aussi à sa confiance on a pu accomplir nos missions. Il fut d'une aide précieuse dans les moments les plus délicats.

Nous remercions également Mr Ziani Hamid et toute l'équipe pour leur accueil, leur esprit d'équipe.

Notre Jurys qui ont accepté de nous consacrer leurs temps en examinant le mémoire. Nous sommes honorés et on leur exprimetoute notre profonde reconnaissance

Nous remercions nos très chers parents, qui ont toujours été là pour nous, « Vous avez tout sacrifié pour vos enfants n'épargnant ni santé ni efforts. Vous m'avez donné un magnifique modèle de labeur et de persévérance. Nous vous sommes redevables d'une éducation dont nous sommes fiers ».

Nous tenons à exprimer notre profond respect et notre gratitude particulière à tous les enseignants de l'Université Saad Dahleb de Blida, et les remercier pour leurs contributions exceptionnelles à ce travail.

Pour tous nos amis qui nous ont apporté leur soutien moral pendant ces années d'études, nous vous remercions sincèrement.

Résumé :

Notre projet porte sur la recherche, la conception et la mise en place d'outils de gestion des accès privilégiés (PAM) pour la banque CPA afin d'augmenter le niveau de sécurité de leurs systèmes d'information et d'enrichir toujours plus ces moyens contre les dangers de la cybercriminalité et des salariés mécontents.

L'objectif principal du projet est le contrôle d'accès et la traçabilité globale des utilisateurs aux ressources clés de son système d'information.

Mots clés : Systèmes d'information, utilisateur, Sécurité, Traçabilité, Cybercriminalité, Contrôle d'accès, PAM, CPA.

Abstract:

Our project involves the research, design and implementation of privileged access management (PAM) tools for the CPA bank in order to increase the level of security of their information systems and further enhance these resources against the dangers of cybercrime and disgruntled employees.

The main objective of the project is to access control and the overall traceability of users to the key resources of its information system.

Keywords: Information system, User, Security, Traceability, Cybercrime, Access control, CPA, PAM.

الملخص:

يتعلق مشروعنا بالبحث والتصميم والتنفيذ لأدوات إدارة الوصول المتميزة لحساب الخاص بالبنك CPA من أجل زيادة مستوى أمان أنظمة المعلومات الخاصة بهم وزيادة إثراء هذه الوسائل ضد مخاطر الجرائم الإلكترونية والموظفين الساخطين.

الهدف الرئيسي للمشروع هو التحكم في الوصول وتتبع المستخدمين إلى الموارد الرئيسية لنظام المعلومات الخاص به.

الكلمات المفتاحية: أنظمة المعلومات، المستخدمين، أمان، تتبع، الجرائم الإلكترونية، إدارة الوصول، CPA، إدارة الوصول المتميزة.

Table des matières

Table des figures

Liste des tableaux

Acronymes et abréviations

A2F	Authentification à deux facteurs
AD	Active Directory
CPA	Crédit Populaire D'Algérie
DB	Database
DNS	Domain Name System
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IIS	Internet Information Services
IPS	Intrusion Prevention System
IT	Information Technology
JIT	Just-In-Time
LDAP	Lightweight Directory Access Protocol
MFA	Multifactor Authentication
OTP	One-Time Password
PAM	Privileged Access Management
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
SGBDR	Système de Gestion de Bases de Données Relationnelles
SIEM	Security Information and Event Management
SMB	Server Message Block
SMS	Short Message Service
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single-Sign-Out
TOTP	Time-based One-Time Password
U2F	Universal Second Factor
VNC	Virtual Network Computing
VPN	Virtual Private Network

Introduction Générale

La plupart des organisations s'appuient sur leurs ressources de données pour exécuter leurs fonctions. Par exemple, les institutions financières utilisent les informations de carte de crédit des clients pour effectuer diverses transactions, les hôpitaux utilisent à leur tour les informations sur la santé des patients pour fournir les soins nécessaires, etc. Par conséquent, sans informations, les entreprises ne pourraient plus fonctionner ; la sécurité de l'information est considérée comme un support métier, de sorte que la valorisation et la protection des informations sont des tâches cruciales pour toutes les organisations. La gestion de la sécurité de l'information est le processus par lequel la valeur des actifs informationnels d'une organisation est évaluée et protégée.

La sécurité de l'information est un ensemble de mesures, politiques, procédures, lignes directrices, ressources et activités associées, gérées collectivement dans le but de protéger les actifs informationnels, cela peut être résumé dans la triade CIA, confidentialité, intégrité et disponibilité.

La confidentialité consiste à protéger l'accessibilité des informations uniquement aux personnes autorisées. Si une personne non autorisée a l'accès à l'information, la confidentialité est compromise.

La disponibilité est le principe de disponibilité signifie que l'information est accessible et utilisable à la demande par une entité autorisée.

L'intégrité fait référence à la qualité des données et des systèmes qui sont inaltérés, complets et exacts. Elle garantit que les données n'ont pas été modifiées ou altérées de manière non autorisée ou involontaire.

Vulnérabilité est une faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces. En soi, la présence d'une vulnérabilité ne produit pas de dommage ; une menace doit exister pour l'exploiter.

Menace est une cause potentielle d'un incident lié à la sécurité de l'information qui peut entraîner des dommages aux actifs informationnels.

Le risque est lié à la sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et nuisent donc à un organisme.

La sécurité de l'information inclut plusieurs domaines, tels que la gouvernance de la sécurité de l'information et gestion des risques, la planification de la continuité des activités et de la

reprise après sinistre, le contrôle d'accès, la télécommunications et sécurité des réseaux, la cryptographie, la sécurité opérationnelle, le développement logiciel sécurisé, la sécurité dès la conception, les juridiques, réglementations, investigation et conformité et la sécurité physique et environnementale.

Ce projet intitulé « Etude et mise en place d'une solution PAM (Privileged Access Management) » est inclus dans le domaine du contrôle d'accès.

Objectif :

Pour vraiment réduire les risques, une entreprise doit aller au-delà des simples contrôles d'accès à ses comptes hautement privilégiés : elle peut notamment utiliser des contrôles d'accès très granulaires pour pouvoir contrôler ce que peut faire toute personne qui réussit à se connecter à un compte. Il peut également utiliser des contrôles d'identité pour appliquer les règles d'accès "principe du moindre privilège" et "séparation des tâches". Le suivi des actions entreprises sous des comptes partagés et leur association à des utilisateurs spécifiques permet également d'autonomiser des utilisateurs souvent anonymes.

Notre objectif est de concevoir et de mettre en œuvre une application (solution) de traçabilité, d'audit et de contrôle d'accès logique des ressources critiques par les administrateurs sans les utiliser pour modifier leurs méthodes de travail quotidiennes.

Structure du mémoire :

Le présent document est structuré comme suit :

- **Chapitre 1 : "Contrôle d'accès et solution PAM" :** Des informations générales sur le contrôle d'accès et ses principes, la gestion des accès privilégiés et ses composa, étude et comparaison entre les solutions PAM.
- **Chapitre 2 : "Choix et conception de la solution" :** Spécification des besoins d'organisme d'accueil, présentation de la solution que nous avons choisie et description des détails de la conception de notre solution.
- **Chapitre 3 : "Mise en œuvre" :** Dédiés à la mise en œuvre et les tests de notre solution

Chapitre 1 : Contrôle d’accès et solution PAM

1. Introduction :

Dans ce chapitre, on va définir l'accès, le contrôle d'accès, le compte privilégié, l'authentification, sécurité du dernier kilomètre, le coffre-fort, la politique de sécurité, l'Active Directory et enfin le Privileged Access Management (PAM).

2. Accès et contrôle d'accès :

L'accès, dans le contexte de la sécurité de l'information, fait référence à la permission ou l'autorisation accordée à un utilisateur ou à une entité pour accéder à une ressource ou à un système d'information. Cela peut inclure l'accès à des fichiers, des réseaux, des bases de données, des applications, des périphériques ou des services informatiques. [1]

Le contrôle d'accès, quant à lui, consiste à déterminer quelles activités sont autorisées aux utilisateurs légitimes en arbitrant la tentative de chaque utilisateur d'accéder aux ressources système. Une infrastructure informatique donnée peut implémenter des systèmes de contrôle d'accès à de nombreux endroits et à différents niveaux. [15,23]

Les objectifs des systèmes de contrôle d'accès sont de protéger les ressources informationnelles contre l'accès inapproprié ou indésirable. Lorsqu'ils sont mis en œuvre efficacement, ils atténuent le risque d'accès à des informations sans l'autorisation appropriée, illégalement et le risque de violation de données. [15]

Le contrôle d'accès utilise plusieurs outils pour gérer et l'accès à ces ressources, parmi lesquels les plus utilisés sont :

- Les mots de passe
- Les cartes d'identité et les badges d'accès
- Les systèmes de reconnaissance biométrique
- Les pares-feux (Firewalls)
- Les VPN
- Les systèmes d'authentification à deux facteurs

La figure 1 représente un schéma d'un contrôle d'accès.

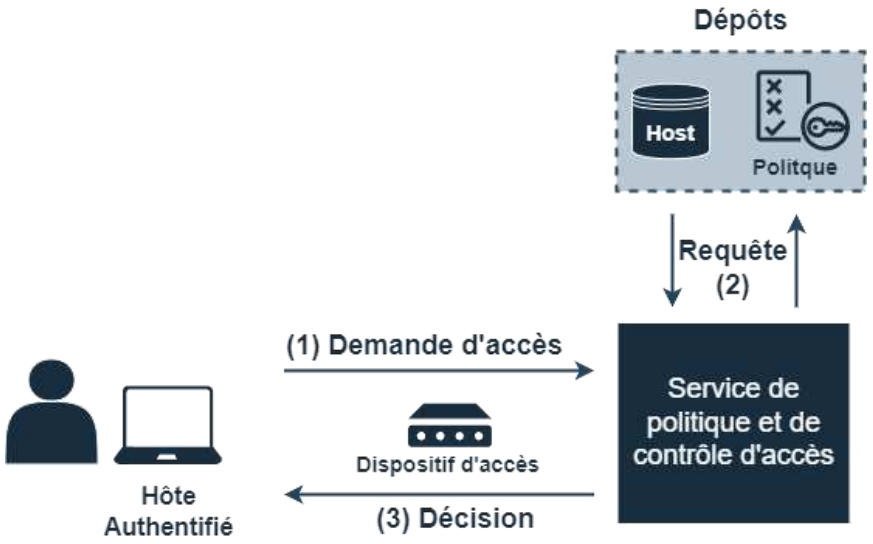

Figure 1 Contrôle d'accès

3. Compte privilégié :

Un compte d'utilisateur est une identité créée pour une personne dans un ordinateur ou un système informatique. Des comptes d'utilisateurs peuvent également être créés pour des entités machine, tels que des comptes de service pour l'exécution de programmes, des comptes système pour stocker des fichiers et des processus système, et des comptes racine et administrateur pour l'administration système. [7]

Les comptes privilégiés offrent un accès élevé et non restrictif à la plate-forme sous-jacente à laquelle les comptes non privilégiés n'ont pas accès. Ces comptes sont conçus pour être utilisés par des personnes, des applications et des machines pour déployer et gérer des technologies informatiques, telles que des systèmes d'exploitation, des périphériques réseau, des applications, etc. Ils sont les clés de l'infrastructure, donnant accès à tout, y compris souvent les données réelles résidant sur les systèmes - c'est pourquoi ils sont la première chose que les attaquants et les initiés malveillants cherchent à compromettre. [20]

L'utilisateur d'un compte privilégié est un administrateur système responsable de la gestion d'un environnement ou un administrateur informatique d'un logiciel ou d'un matériel spécifique. Il peut effectuer les opérations suivantes [7,17] :

- Installer des matériels et des logiciels du système
- Accéder à des données sensibles
- Réinitialiser les mots de passe d'autres utilisateurs
- Se connecter à toutes les machines de l’environnement

- Utiliser des privilèges élevés pour effectuer des changements dans les systèmes d'infrastructure informatique

Les autres utilisateurs informatiques comprennent les utilisateurs standard et les utilisateurs intensifs.

Utilisateurs standard : Il s'agit d'utilisateurs réguliers qui ont des comptes non puissants leur permettant d'accéder quotidiennement aux applications de l'entreprise pour effectuer des opérations de routine. Les utilisateurs standard n'ont normalement pas accès aux systèmes d'information sensibles. [20]

Utilisateurs intensifs : Les utilisateurs intensifs disposent d'autorisations supplémentaires par rapport aux utilisateurs standard. Comme un personnel informatique interne qui aide à la gestion des postes de travail des utilisateurs. Ces utilisateurs bénéficient d'une élévation d'accès au compte privilégié, qui leur donne des autorisations spécifiques, comme l'accès à distance aux postes de travail locaux et aux bases de données. [20]

La figure 2 illustre les types des utilisateurs d'Information Technology (IT).

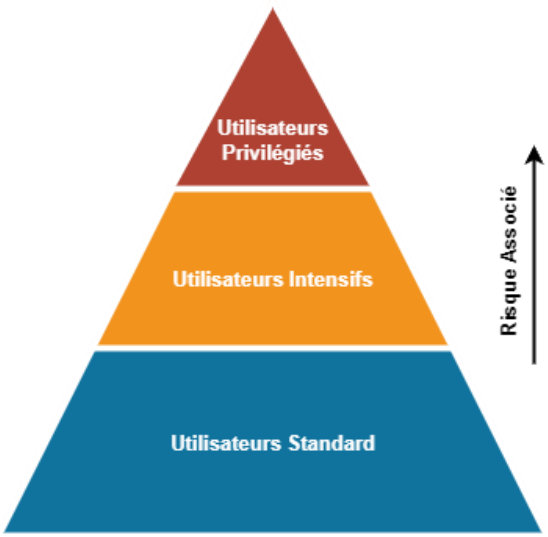

Figure 2 Types des utilisateurs d'IT

4. Authentification :

L'authentification est le processus de vérification de l'identité d'un utilisateur, d'un appareil ou d'un système. Elle garantit que seuls les utilisateurs ou systèmes autorisés peuvent accéder aux informations ou ressources sensibles. [2]

4.1. Authentification à deux facteurs :

L'authentification à deux facteurs (A2F) est utilisée pour les cibles les plus probables, Remote Desktop Protocol (RDP), Secure Shell (SSH) et l'exécution des opérations privilégiées. [2,12]

L'authentification à deux facteurs implique généralement l'utilisation d'un mot de passe, les méthodes d'authentification à deux facteurs les plus utilisées [4,5] :

- Clé de sécurité U2F (Universal Second Factor)
- Mot de passe à usage unique (OTP)
- Mot de passe à usage unique basé sur le temps (TOTP)
- Carte à puce
- Applications mobiles
- Message court (SMS), e-mail ou appel vocal
- Certificat logiciel
- Notification push
- Clé de sécurité U2F/WebAuthn
- QR Code
- Biométrie (empreintes digitales, reconnaissance faciale, etc.)

En vue de leurs utilisations dans le reste du mémoire, nous détaillons ici les authentifications à deux facteurs suivants :

4.2. Mot de passe à usage unique (OTP) :

Le mot de passe à usage unique (OTP) est un algorithme qui génère un mot de passe valide pour une seule session de connexion ou un seul accès au compte pour garantir la confidentialité des données grâce à des processus d'authentification et de sécurité. [18,27]

4.3. Mot de passe à usage unique basé sur le temps (TOTP) :

Le mot de passe à usage unique basé sur le temps (TOTP) est un algorithme qui a le même but que le OTP et qui fournit des mots de passe courts qui changent toutes les 30 ou 60 secondes. En raison de ses changements rapides des mots de passe généré par TOTP Il est pratiquement impossible de prédire le prochain mot de passe. [18]

5. Sécurité du dernier kilomètre « Last Mile » :

Le "dernier kilomètre" ou "Last Mile" désigne tous les composants du réseau qui sont physiquement situés en dehors du siège ou des succursales d'une organisation et qui sont utilisés par les travailleurs à distance pour se connecter aux systèmes et aux ressources de l'entreprise.

L'utilisation d'un mot de passe fort et sa mise à jour régulière ne suffisent plus. L'authentification à deux facteurs est désormais une exigence obligatoire lorsqu'il s'agit de protéger l'accès aux actifs de l'entreprise, en particulier lorsqu'il s'agit d'accéder par le biais du RDP.

6. Coffre-fort des mots de passe :

Coffre-fort de mots de passe est une application qui aide les utilisateurs à stocker leur mot de passe sur un serveur pour le conserver en toute sécurité par un des mots de passe cryptés, et leur suggère un nouveau mot de passe fort. Son objectif est d'empêcher l'oubli ou la fuite des mots de passe. [6,8,28]

6.1. Etat de coffre-fort :

Le coffre a deux états :

- **Non initialisé :** après l'installation, le coffre-fort est dans l'état non initialisé, et l'administrateur doit l'initialiser et enregistrer les clés de décryptage les conserver en toute sécurité.
- **Initialisé :**
  - **Décrypté :** lorsque le coffre-fort est initialisé, le coffre-fort se trouve dans l'état Décrypté, auquel cas le coffre-fort est prêt à être utilisé
  - **Crypté :** le coffre-fort est dans un état crypté, lors du redémarrage du service coffre-fort. Dans ce cas, l'administrateur doit le décrypter en utilisant les codes de décryptage précédemment enregistrés.

La figure 3 illustre le principe de coffre-fort.

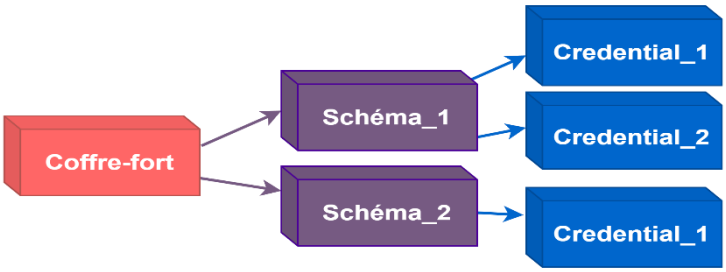

Figure 3 Coffre-fort des mots de passe

7. Politique de sécurité :

La politique de sécurité est un ensemble de lois, de règles et de pratiques régissant la gestion, l'accès et la protection des informations et des ressources sensibles contre une utilisation non autorisée. [10,11,14]

Cette politique est enregistrée dans le système de gestion des accès et doit être attribuée aux utilisateurs.

Un utilisateur demande l'accès à un service particulier. Si l'utilisateur n'est pas autorisé à accéder au service, le système refusera la demande d'accès et répondra à l'utilisateur. Si l'utilisateur est autorisé à accéder au service, le système fait correspondre les règles de restriction d'accès aux règles de politique et accorde finalement l'accès à l'utilisateur.

8. Active Directory :

Active Directory est un service d'annuaire extensible développé par Microsoft qui permet une gestion centralisée des équipements réseau. Il permet d'ajouter, de supprimer ou de déplacer facilement des comptes d'utilisateurs, de groupes et d'ordinateurs ainsi que des autres équipements. [13]

Active Directory est basé sur des protocoles Internet standard et a une conception qui aide à identifier clairement les composants physiques et logiques de la structure de votre réseau.

Il utilise en principe quatre protocoles [13] :

- LDAP (Lightweight Directory Access Protocol)

- Kerberos
- SMB (Server Message Block)
- DNS (Domain Name System)

9. Privileged Access Management (PAM) :

Privileged Access Management (PAM) ou la gestion des accès privilégiés est une solution automatisée de gestion des mots de passe et des sessions qui fournit un contrôle d'accès sécurisé, un audit, des alertes et une journalisation pour tous les comptes privilégiés. La technologie est conçue pour gérer les comptes d'administrateurs locaux ou partagés dans un domaine, les comptes d'administrateur individuels des utilisateurs, les services, les systèmes d'exploitation, les périphériques réseau, les bases de données et de serveur ainsi que les applications et les clés SSH. [9,17,21]

La figure 4 illustre l'Architecture PAM.

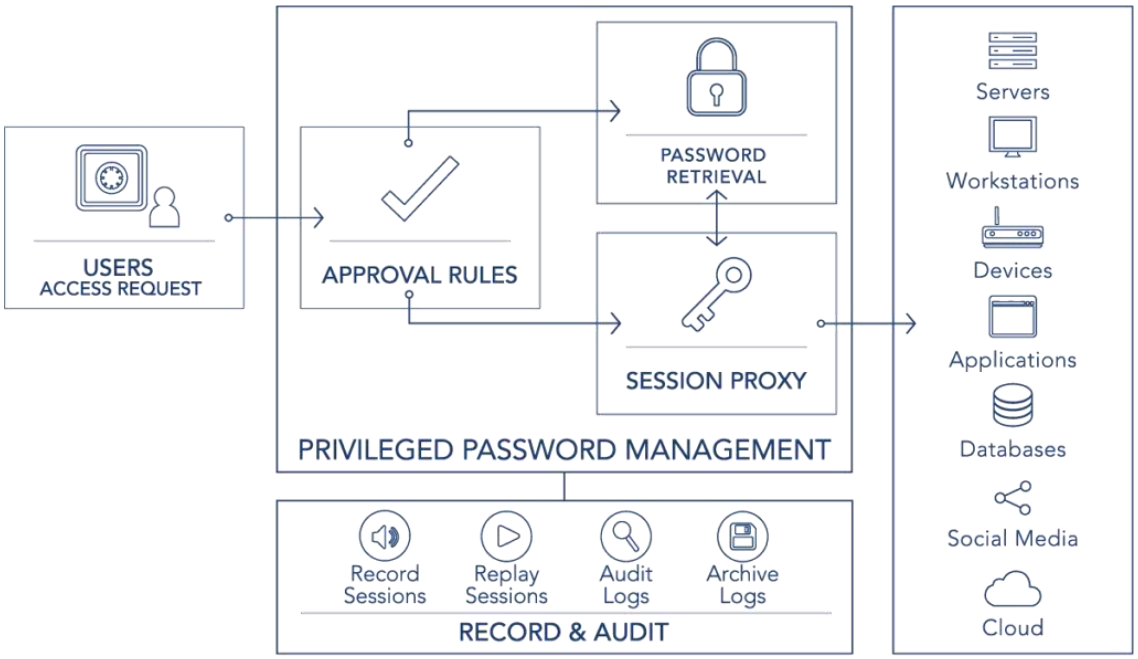

Figure 4 Architecture PAM

10.Composants de PAM :

La gestion des accès privilégiés (PAM) comprend généralement un ensemble de composants qui fonctionnent ensemble pour contrôler et surveiller l'accès privilégié aux systèmes, applications et données critiques [17] :

- Stockage du mot de passe
- Gouvernance
- Gestion des sessions

- Analyses et rapports
- Système d'intégration
- Gestion des mots de passe
- Gestion privilégiée

La figure 5 présente les composants de PAM.

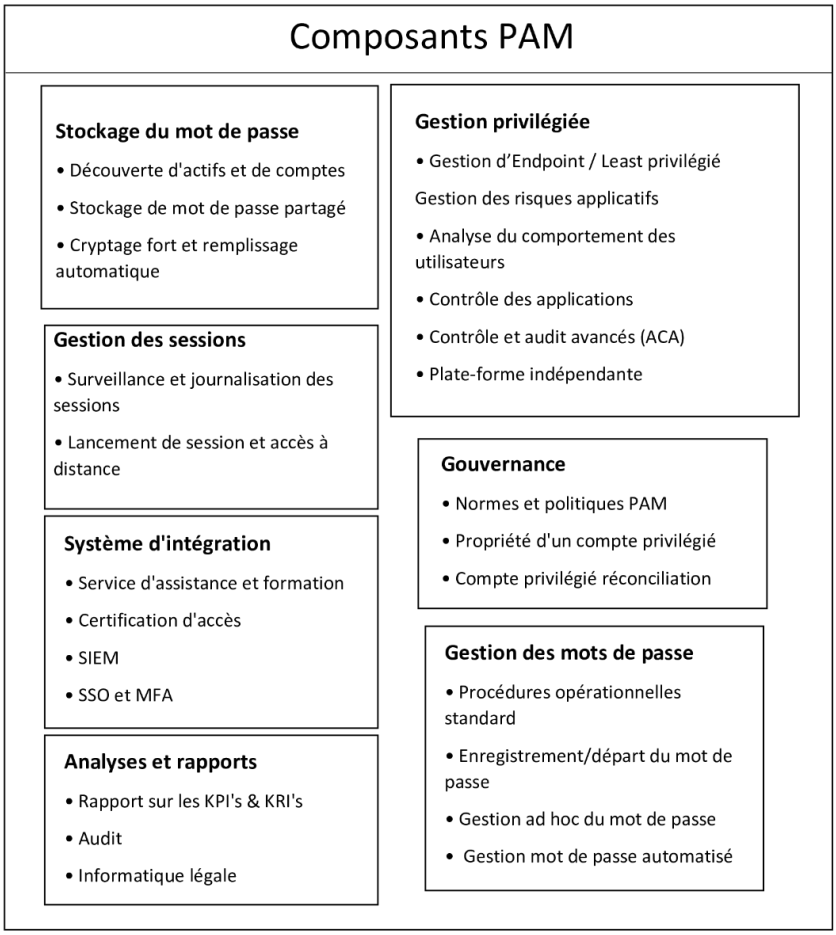

Figure 5 Composants de PAM

11.Comparaison entre différentes solutions PAM existantes :

11.1. Teleport :

Teleport est une plateforme d'accès open-source utilisée pour SSH, Kubernetes, les bases de données, les applications web internes et Windows. Elle prévient le phishing en s'appuyant sur la biométrie et l'identité de la machine, arrête les pivots des attaquants avec l'architecture Zero Trust. [25]

11.1.1. Principales caractéristiques :

- **Gestion de l'accès :** pour définir des politiques précises et déterminer qui peut effectuer certaines actions sur des ressources spécifiques. [25]

- **Authentification et autorisation :** pour prouver l'identité d'un utilisateur ou d'un service avant de permettre l'utilisateur à accéder aux services. [25]
- **Enregistrement des sessions :** Les sessions SSH et kubectl, les requêtes DB, les sessions de RDP windows, les sessions web et les requêtes API sont enregistrées. [25]

11.1.2. Limites :

La version open-source et la version Team de téléport sont très limitées, car la solution ne dispose pas des caractéristiques importantes de PAM et qui sont les suivantes : le contrôle d'accès basé sur les rôles (RBAC), demande d'accès juste-à-temps, Single-Sign-On (SSO) et l'option de appareils de confiance.

11.2. StrongDM :

StrongDM est une plateforme de gestion des accès fournie sous forme de logiciel en tant que service (SaaS). StrongDM combine l'authentification, l'autorisation, la mise en réseau, l'audit et l'observabilité en une seule plateforme, ce qui permet aux entreprises de gérer et d'auditer facilement l'accès à l'ensemble de leur infrastructure. [24]

11.2.1. Principales caractéristiques :

- **Authentification et fédération d'identité :** Des contre-mesures pour lutter contre les attaques de compte par brute force. Un mot de passe est exigé pour tous les utilisateurs, tous les mots de passe sont cryptés par l'algorithme de hachage *bcrypt, une* authentification multi-facteur et permet aux clients de se fédérer avec une variété de fournisseurs d'identité pour gérer l'identité et l'authentification des utilisateurs, comme Okta et Azure AD. [24]
- **Protection des données :** Les données des périphériques et des utilisateurs sont protégées et les connections entre le client et la destination sont cryptées. [24]
- **L'audit généralisé :** Chaque authentification d'utilisateur, requête SSH et commande RDP ainsi que les actions des administrateurs telles que les changements de permission sont enregistrés dans un référentiel inviolable. Grâce à un outil de commande les administrateurs peuvent voir l'historique des audits de n'importe quel moment et ils peuvent l'exporter dans un certain nombre de format. [24]
- **Gestion des logs :** Les activités de l'utilisateur sont enregistrées localement ou sur cloud, selon la configuration de l'administrateur. [24]

11.2.2. Limites :

StrongDM ne dispose pas d'une version open source, donc les clients ne peuvent pas ajouter des nouvelles fonctionnalités selon les besoins de l'entreprise, de plus l'installation et la configuration de cette solution n'est pas facile et demande de résoudre de nombreux problèmes et créer beaucoup de code.

11.3. JumpServer :

JumpServer est un système sur un réseau utilisé pour accéder et gérer des dispositifs dans une zone de sécurité séparée. [16]

11.3.1. Principales caractéristiques :

- **Authentification :** Utilise différents types d'authentification tels que LDAP/AD, RADIUS, Single-Sign-On et authentification multi-facteurs avec Google Authenticator. [16]
- **Autorisation :** Les utilisateurs, les groupes d'utilisateurs, les actifs, les nœuds d'actifs, les applications et les utilisateurs du système peuvent être autorisés. Les autorisations de la base de données et le temps accessible des ressources autorisées sont supervisés et contrôlé. [16]
- **Gestion des accès :** Prise en charge de la gestion des utilisateurs de la gestion et des utilisateurs du système, la gestion basée sur les rôles (5 rôles). Un service de gestion des mots de passe des actifs ; génération automatique du mot de passe, envoi automatique du mot de passe, réglage de l'expiration du mot de passe. [16]
- **Audit :** Contrôle en temps réel et l'audit du contenu des sessions en ligne et l'audit du contenu des sessions historiques. [16]

11.3.2. Limites :

JumpServer ne dispose pas des fonctionnalités importantes de PAM, le coffre-fort des mots de passe pour stocker les identifiants de connexion et de faciliter l'authentification aux services.

La version open-source de JumpServer ne possède pas la connexion d'une base de données via l'interface Web.

11.4. Trasa :

TRASA est un projet open source qui fournit des fonctionnalités de sécurité PAM modernes et permet d'appliquer les meilleures pratiques de sécurité pour protéger l'infrastructure interne : Web, SSH, RDP, et les bases de données contre les accès non autorisés ou malveillants. [26]

Ses principales caractéristiques sont :

- **Open-source :** Permettra d'ajouter de nouvelles fonctionnalités à l'avenir.
- **Sécuriser l'accès local et à distance :** Une combinaison d'outils pour sécuriser l'accès aux services à distance et l'accès aux comptes locaux, tels que TOTP, Universal Second Factor (U2F) et l'authentification à deux facteurs YubiKey, des politiques de sécurité strictes pour les utilisateurs afin de restreindre l'accès à leurs services. [26]
- **Surveillance de l'accès sécurisé :** La visibilité d'une session autorisée active doit être totale afin que toute intention malveillante cachée dans l'accès de confiance puisse être vérifiée en temps réel ou à l'avenir. [26]
- **Coffre-fort des mots de passe :** Un coffre-fort qui sauvegarde les identifiants de connexion des services et facilite les accès à ces services.
- **Intégration avec les fournisseurs d'identités et de secrets :** Intégration direct avec les fournisseurs d'identité de service et à des gestionnaires de secrets pour protéger une infrastructure dynamique. [26]

11.4.1. Limites :

Trasa ne dispose pas d'une équipe de soutien qui pourrait aider les organisations à résoudre les problèmes.

12.Comparaison :

Le tableau 1 illustre une comparaison entre ces trois solutions.

Tableau 1 Comparaison entre les solutions

	Teleport	StrongDM	JumpServer	Trasa
Système d'exploitation	Docker, Windows, MAC and Linux	Linux	Docker, Linux	Docker
Interface WEB sécurisée	Oui	Oui	Oui	Oui
Accès client natif sécurisé (RDP, SSH...)	Oui	Oui	Oui	Oui
Coffre-fort des mots de passe	Oui	Oui	Non	Oui
Authentification Multi-facteur (MFA)	Oui	Oui	Oui	Oui
La haute disponibilité	Oui	Oui	Oui	Oui
Surveillance	Session en direct et enregistrée	Session en direct et enregistrée	Session en direct et enregistrée	Session en direct et enregistrée
Version Open-source	Oui, mais elle ne dispose pas des fonctionnalités les plus importantes de PAM.	Non	Oui, mais elle est limitée	Oui, avec toutes les caractéristiques de PAM

13.Conclusion :

A travers ce chapitre, on a étudié l'accès, le contrôle d'accès et ses différentes fondamentales. Ensuite on a analysé et comparé entre différentes solutions PAM.

Dans le prochain chapitre, on va présenter l'organisme d'accueil, spécifier les besoins de l'entreprise et enfin présenter que nous avons choisie.

Chapitre 2 : Choix et conception de la solution

1. Introduction :

La spécification des besoins et la conception sont des étapes fondamentales du processus de développement d'un logiciel, et nous commençons ce chapitre en abordant les différents besoins définis par l'organisme d'accueil.

Nous passons ensuite à la phase de conception, où nous élaborons des diagrammes de cas d'utilisation et des diagrammes de séquence associés.

2. Présentation de l'organisme d'accueil

2.1. Présentation du CPA :

Le Crédit Populaire d'Algérie (CPA) est une banque publique algérienne créée le 29 décembre 1966, par l'ordonnance N°66-366 et ses statuts ont été arrêtés par l'ordonnance n°67/78 du 11 Mars 1967. C'est une Société par action, dont l'Etat Algérien est actionnaire à 100%.

Dans les dispositions générales de ses statuts, le CPA est conçu comme une banque générale et universelle.

2.2. Les missions du Direction de la sécurité des systèmes d'information (DSSI) :

A ce titre, elle est, notamment, chargée :

De définir et proposer aux organes de décision habilités de la banque les stratégies et les politiques de développement et de sécurité des systèmes d'information ;

- D'élaborer les plans de développement liés aux systèmes d'information de la banque et conduire les projets informatiques et de modernisation qui en découlent ;
- D'assurer la veille technologique dans les domaines relevant de ses attributions ;
- D'assister les structures métiers dans la conception et la mise en œuvre des systèmes d'informations spécifiques à leurs activités, tout en veillant au respect des normes et standards, leur cohérence et leur compatibilité ;

De développer la maîtrise d'œuvre à travers la conception, la réalisation et la maintenance des solutions informatiques ;

- D'élaborer les programmes d'investissement en matière d'équipements informatiques et doter les utilisateurs de moyens performants ;
- D'assurer la gestion de l'ensemble des composantes de l'infrastructure informatique : Equipements, Réseaux de transmission de données, logiciels, etc.. ; d'élaborer et de mettre en œuvre les plans de reprise d'activité de manière à garantir la continuité

d'exploitation des systèmes informatiques, notamment les sites de production informatiques.

3. Spécification des Besoins :

3.1. Fonctionnalités :

- Accès client natif sécurisé : L'application doit supporter les protocoles de connexion à distance (RDP, SSH, HTTPS) avec la possibilité de créer des accès personnalisés à des utilisateurs privilégiés avec des politiques personnalisée.
- Contrôle d'accès : La solution doit offrir la possibilité de créer des sessions en fonction du niveau d'autorisation et du statut de l'utilisateur (un utilisateur ne peut accéder qu'à la plateforme définie par son niveau d'attribut).
- Un coffre-fort des mots de passe : L'application doit contenir un coffre-fort qui stocke les identifiants de connexion.
- L'Authentification Multi-facteur (MFA) : L'application doit offrir une protection Multi facteur qui offre au moins deux informations d'identification indépendantes sur ce que l'utilisateur sait (son mot de passe), sur ce qu'il possède (un ticket ou un mail) et sur ce qu'il est.
- Cryptage des mots de passe : La solution doit Utiliser un cryptage fort pour les mots de passe.
- La haute disponibilité : La solution doit prendre en compte la haute disponibilité.
- Surveillance : L'application doit faire un enregistrement et une capture de session à distance et localement en temps réel. Elle doit offrir, également, la possibilité de voir les sessions déjà enregistrées.
- Sauvegarde et restauration : La solution doit offrir un système de sauvegarde et de restauration de la configuration qui doit être à la disposition des administrateurs.

3.2. Exigences techniques :

Le tableau 2 illustre l'environnement technologique existant.

Tableau 2 Environnement technologique existant

Système d'exploitation	Bases de données	Serveurs WEB	Equipements réseau	Outils sécurité	Rôles
Windows Ubuntu Windows server	Informix SQL server Oracle MySQL PostgreSQL …	IIS APACHE TOMCAT SAP NetWeaver Glassfish Ingex	CISCO POLO ALTO STONESOFT FORTINET …	Firewall, Antivirus (Kaspersky et autres) Proxy IPS / IDS…	AD Exchange SharePoint Lync SIEM…

La solution doit :

- Présenter une interface Web sécurisée, qui permet aux utilisateurs une bonne gestion des accès aux différentes plateformes existantes au niveau de la banque.
- Être hébergée par la Banque, dans ses locaux et sur ses plateformes.
- Prendre en charge une gestion centralisée.

4. Choix de solutions :

Suite à l'étude des différentes solutions disponibles (section 9 chapitre 1) compte tenu des caractéristiques de chaque solution, présentant ces limites et en s'inspirant du tableau comparatif, nous avons choisi de mettre en œuvre ce projet en utilisant la solution Trasa. Cette solution offre toutes les fonctionnalités de la gestion des accès privilégiés.

La figure 6 présente l'architecture de la solution Trasa.

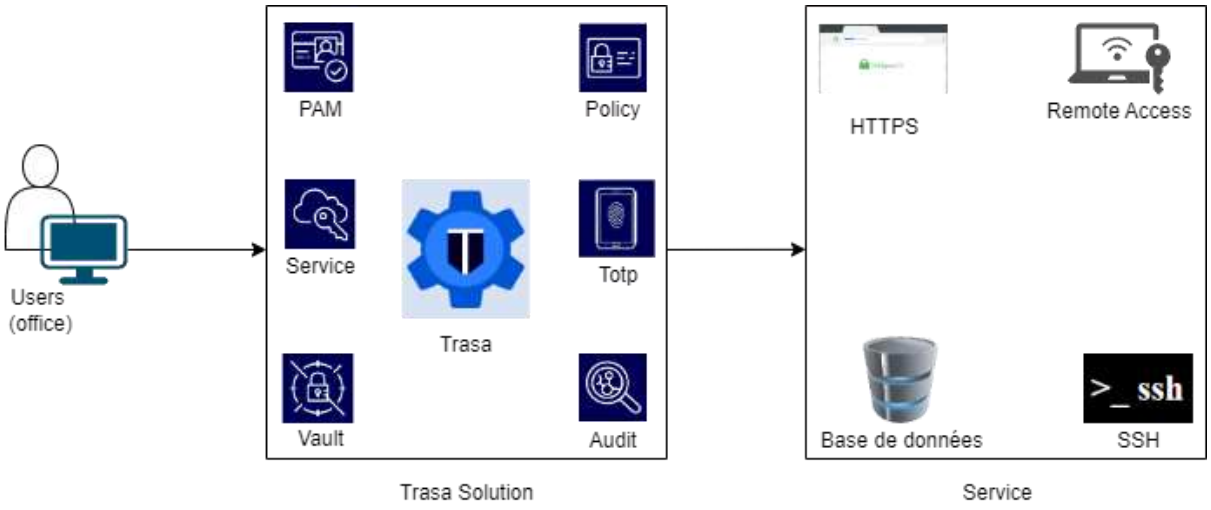

Figure 6 Architecture de la solution Trasa

5. Diagrammes de conception :

Cette section présente le fonctionnement de la solution à travers des diagrammes de cas d'utilisation et diagrammes de séquences.

La figure 7 présente le diagramme de cas d'utilisation générale.

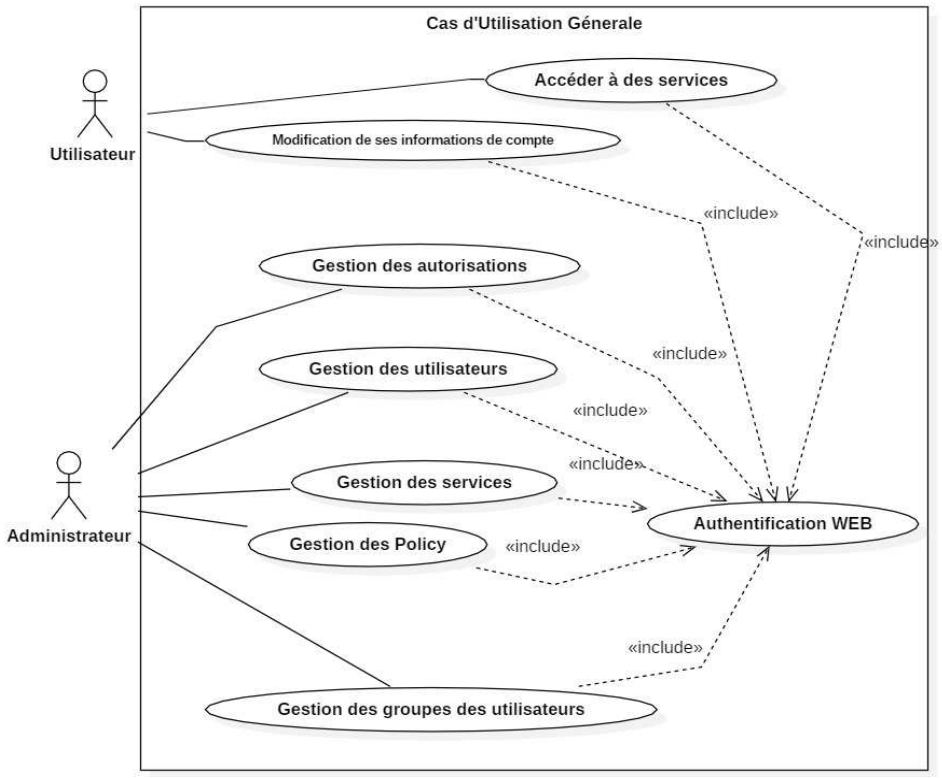

Figure 7 Cas d'utilisation <<Générale>>

La figure 8 illustre le cas d'utilisation d'accès à un service.

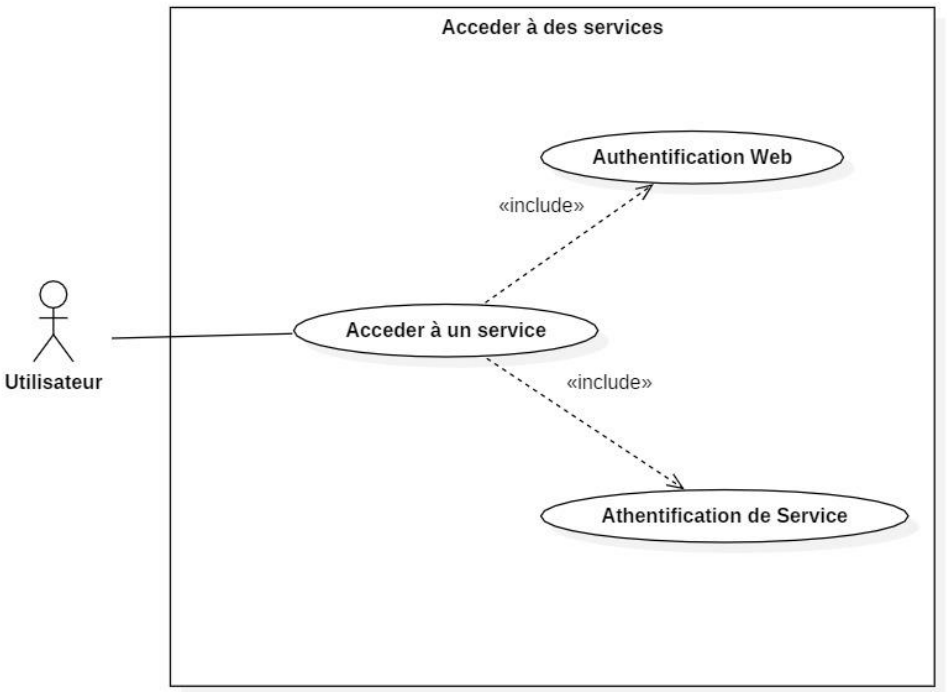

Figure 8 cas d'utilisation <<Accéder à un service>>

Ce diagramme (figure 8), explique comment l'utilisateur fait pour accéder à un service d'accès à distance et les étapes à suivre.

1. L'utilisateur va demander la connexion RDP
2. L'application va demander les données d'authentification
3. L'utilisateur va envoyer ses données d'authentification
4. Le système va vérifier ses données d'authentification avec le système de base de données
5. Si les données sont vérifiées, l'application demande à l'utilisateur de choisir, la connexion ciblée
6. Quand l'utilisateur choisis, la connexion ciblée le système de l'application va vérifier l'autorisation de l'utilisateur
7. Si l'autorisation est vérifiée donc l'application va lancer l'enregistrement de session et ouvrir la session à l'utilisateur
8. Sinon l'application va afficher un message, erreur d'identifiant de connexion.
9. Si les données d'authentification ne sont pas vérifiées, donc l'application va afficher un message. Erreur d'authentification.

La figure 9 présente le cas d'utilisation de gestion des utilisateurs

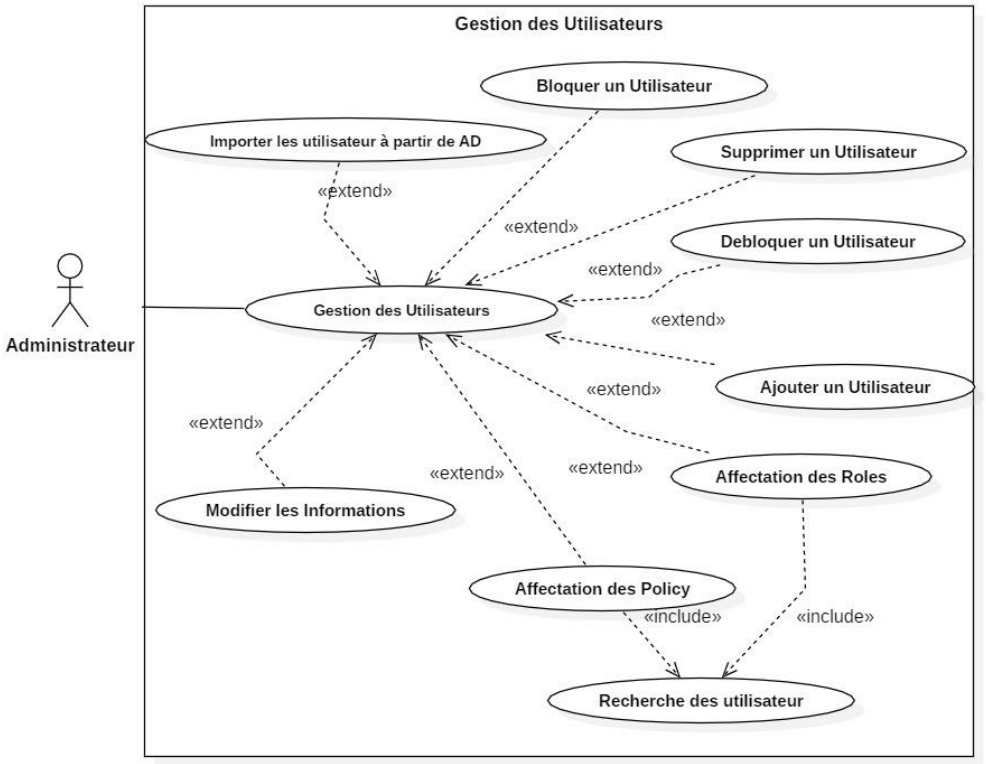

Figure 9 cas d'utilisation <<Gestion des Utilisateurs>>

Ce diagramme (figure 9), explique comment l'administrateur va faire la gestion des utilisateurs à l'application.

L'administrateur doit d'abord s'authentifier à l'application.

Ajouter un utilisateur :

1. L'administrateur va choisir l'opération d'ajout d'un utilisateur.
2. Le système d'application va afficher le formulaire d'ajout d'un utilisateur.
3. L'administrateur va remplir le formulaire et valider l'opération.
4. L'application va vérifier les le formulaire et exécuter l'opération et envoyer un token à l'administrateur.
5. Le token va être envoyer par l'administrateur à l'utilisateur pour configurer son mot de passe.

Modifier et supprimer un utilisateur

1. L'administrateur choisis l'opération de modifier ou supprimer un utilisateur.
2. Le système va afficher un formulaire à l'administrateur.
3. L'administrateur va remplir le formulaire.

Affectation des Rôles :

1. L'administrateur va choisi l'opération affectation des rôles.
2. Le système va afficher le formulaire.
3. L'administrateur va remplir le formulaire et affecter les rôles aux utilisateurs.

Affectation des Politiques :

1. L'administrateur va choisir l'opération affectation des Policy.
2. Le système va afficher le formulaire à remplir.
3. L'administrateur va rempli le formulaire et affecter les politiques aux utilisateurs.

La figure 10 présente le diagramme de séquence de création d'un service.

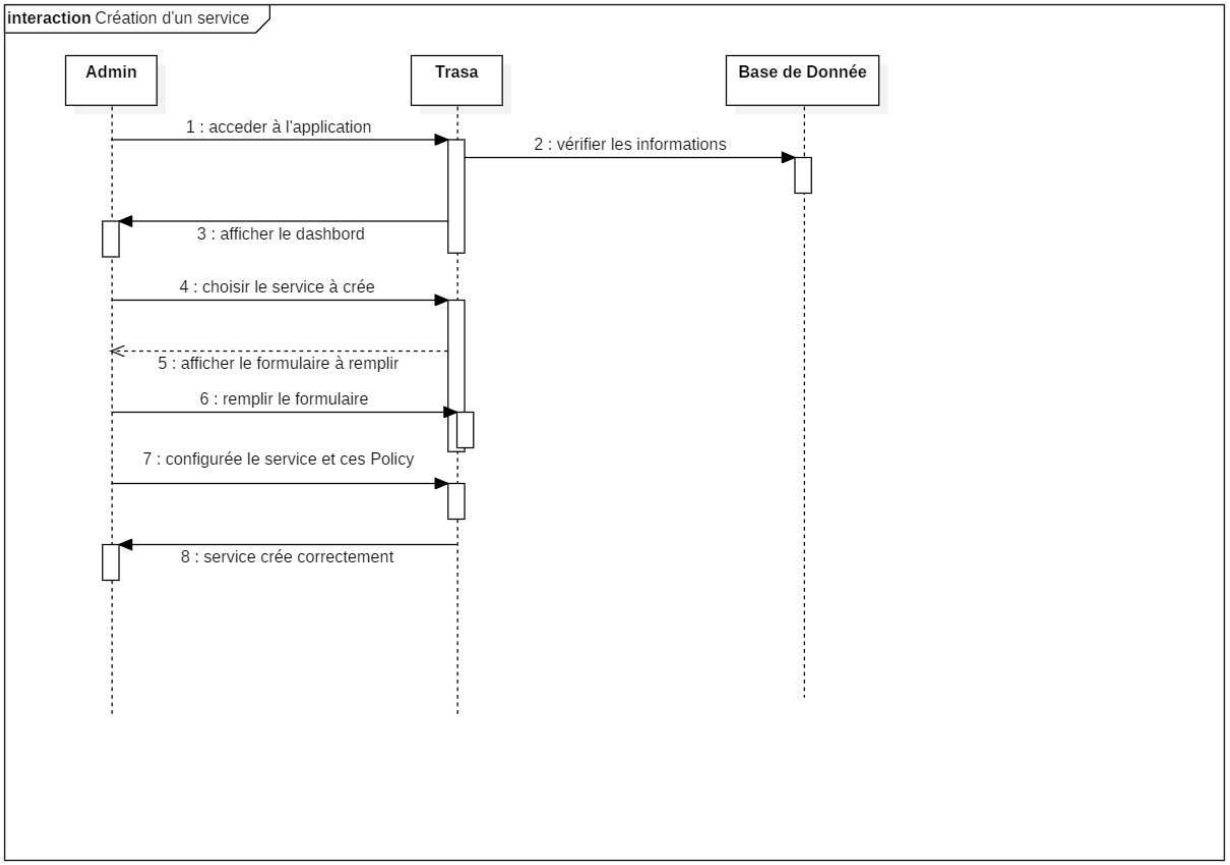

Figure 10 Diagramme de séquence <<création d'un service >>

Ce diagramme (figure 10), explique comment l'administrateur crée un service.

Tout d'abord, l'administrateur accède à son compte, puis choisit le service à créer, le système lui affiche un formulaire à remplir, il remplit ce formulaire et poursuit les procédures de configuration de ce service, d'affectation des utilisateurs et des politiques et enfin il valide la création.

La figure 11 présente le diagramme de séquence pour accéder à un service

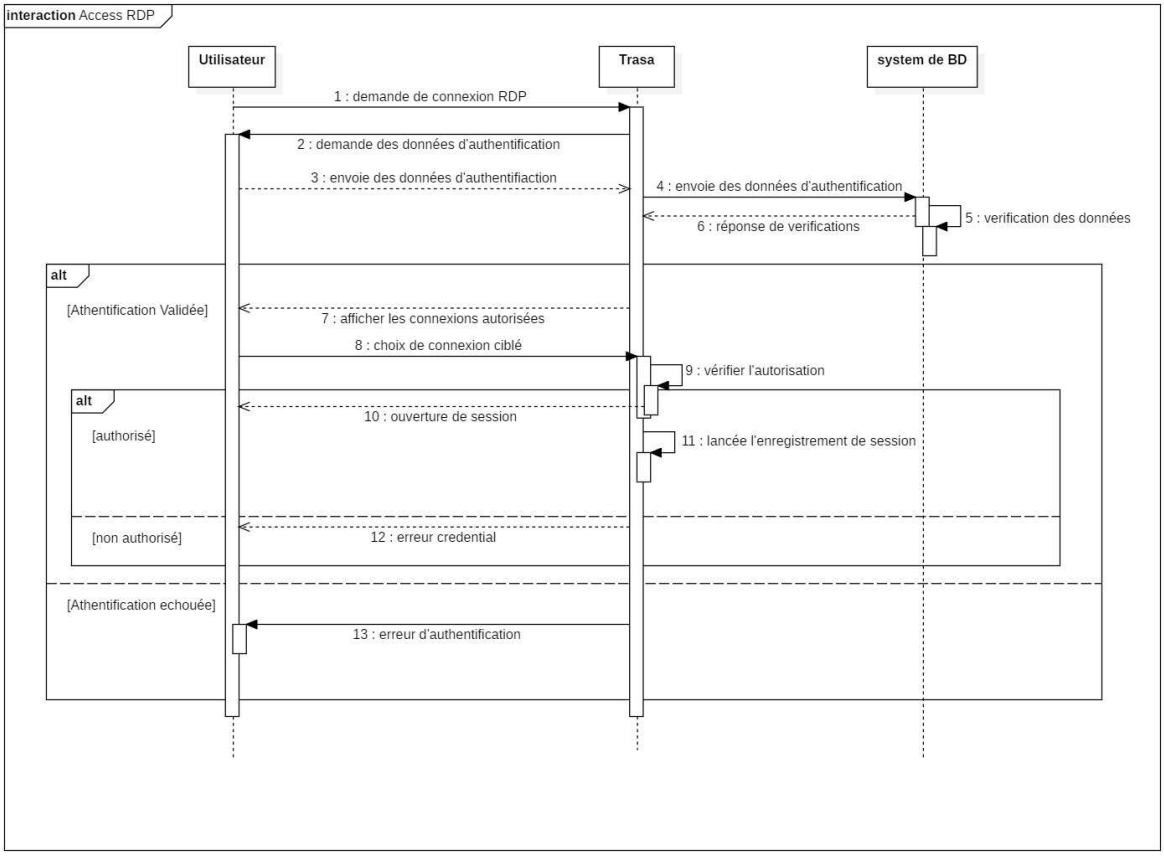

Figure 11 Diagramme de séquence <<Accéder à un service >>

Ce diagramme (figure 11), explique comment l'utilisateur accède à un service.

Premièrement, l'administrateur demande l'accès au service, puis le système vérifie les données entrantes et répond à l'utilisateur en lui indiquant le résultat de la vérification.

Si les informations d'identification ne sont pas valides, l'accès au service échoue, sinon il passe à l'étape de vérification d'authentification. Si l'authentification n'est pas valide, l'accès est refusé. Dans le cas contraire, le système ouvre la session pour l'utilisateur et démarre l'enregistrement vidéo.

6. Conclusion :

Dans ce chapitre, nous avons énuméré les différents besoins auxquels notre système doit répondre, puis nous avons présenté la phase de conception de notre système, qui contient des diagrammes de cas d'utilisation et des diagrammes de séquence, qui nous ont aidés à décrire en détail le fonctionnement du système et à faciliter sa réalisation.

Dans le chapitre suivant, nous passons à l'étape finale de notre projet, à savoir la mise en œuvre de la solution.

Chapitre 3 : Mise en œuvre

1. Introduction :

Ce chapitre est la dernière partie de notre mémoire et traite de la phase de mise en œuvre de notre solution. Nous décrivons d'abord l'environnement matériel et logiciel utilisé pour la solution. Enfin, nous testons les fonctionnalités de la solution.

2. Installation de solution :

2.1. Environnement de travail :

Pour réaliser notre projet, on a utilisé une machine DELL équipée de :

- Processeur : Intel i5-8350U
- RAM : 16 Go
- Système d'exploitation : Windows 11
- Stockage : 2 Go

Deux machines virtuelles ont été déployées sur cet hôte

- Serveur principal :

Hébergeant la solution Trasa, il est équipé de :

- Processeur : intel i5-8350U (2 Threads)
- Système d'exploitation : Ubuntu 20.04
- RAM : 4 Go
- Stockage : 50 Go

- Serveur secondaire :

Serveur pour les tests, équipé de :

- Processeur : intel i5-8350U (1 Thread)
- Système d'exploitation : Windows Server 2019
- RAM : 2 Go
- Stockage : 25 Go

Pour le déploiement de notre solution, on a utilisé les logiciels suivants dans notre hôte :

- **Oracle VM VirtualBox :** est un logiciel de virtualisation gratuit, fonctionnant actuellement sous Windows, Linux, MacOs, etc. Il se compose d'une machine hôte et d'une machine invitée.

- **Kernel-based Virtual Machine (KVM) :** est une solution de virtualisation complète pour Linux sur du matériel x86 contenant des extensions de virtualisation (Intel VT ou AMD-V). Il est composé d'un module de noyau chargeable, kvm.ko, qui fournit l'infrastructure de virtualisation de base et d'un module spécifique au processeur, kvm-intel.ko ou kvm-amd.ko.
- **Docker Compose :** est une technologie de conteneurisation développée par Docker Ins pour permettre la création et l'utilisation de conteneurs Linux, et aider les machines virtuelles à devenir très légères et modulaires.
- **PostgreSQL :** est un système de gestion de bases de données relationnelles (SGBDR) orienté objet puissant et open source et qui donne la priorité à la conformité et à l'extensibilité SQL. [19]
- **Redis :** est un système de gestion de base de données, créé en langage C et faisant partie de la famille NoSQL. [22]
- **Apache Guacamole Server (Guacd) :** est une passerelle pour les accès à distance en utilisant un navigateur WEB. Il prend en charge les protocoles standard tels que VNC, RDP et SSH. [3]

2.2. Installation de la solution Trasa :

Afin d'installer la solution Trasa, les étapes suivantes sont nécessaires ;

- **Installation de Redis :**

sudo docker run -d -p 6379:6379 --name redis redis:6.0.8

```
pam-server@pam-server:~$ sudo docker run -d -p 6379:6379 --name redis redis:6.0.8
d7f9a410ef1df16d232605e772bf5896ac2dc08ec81607fc1de5db8b20a5571f
```

Figure 12 Installation de Redis

- **Installation de Postgresql :**

sudo docker run -d -p 5432:5432 --name db \
-e POSTGRES_PASSWORD=trasauser \
-e POSTGRES_USER=trasauser \
-e POSTGRES_DB=trasadb postgres:13.0

```
pam-server@pam-server:~$ sudo docker run -d -p 5432:5432 --name db \
> -e POSTGRES_PASSWORD=trasauser \
> -e POSTGRES_USER=trasauser \
> -e POSTGRES_DB=trasadb postgres:13.0
883233d9b90a44bdfe44b4332f98f8e08fbc47fe1a85afe921bf5d861cf7b81d
```

Figure 13 Installation de Postgresql

- **Installation de Apache Guacamole Server :**

```
sudo docker run -d --name guacd \
-p 127.0.0.1:4822:4822 \
-v /tmp/trasa/accessproxy/guac:/tmp/trasa/accessproxy/guac \
--user root seknox/guacd:v0.0.1
```

```
pam-server@pam-server:~$ sudo docker run -d --name guacd \
> -p 127.0.0.1:4822:4822 \
> -v /tmp/trasa/accessproxy/guac:/tmp/trasa/accessproxy/guac \
> --user root  seknox/guacd:v0.0.1
f32f355f9b6cbaf351439384dd45b42c463ef5d24a550a55d59fd04ca32db541
```

Figure 14 Installation de Apache Guacamole Server

- **Installation de Trasa :**

```
sudo docker run -d --name trasa --link db:db \
--link guacd:guacd \
--link redis:redis \
-p 443:443 \
-p 80:80 \
-p 8022:8022 \
-e TRASA.LISTENADDR=192.168.1.200 \
-e TRASA.AUTOCERT="false" \
-v /tmp/trasa/accessproxy/guac:/tmp/trasa/accessproxy/guac \
seknox/trasa:v1.1.4
```

```
pam-server@pam-server:~$ sudo docker run -d --name trasa --link db:db \
> --link guacd:guacd \
> --link redis:redis \
> -p 443:443 \
> -p 80:80 \
> -p 8022:8022 \
> -e TRASA.LISTENADDR=192.168.1.200 \
> -e TRASA.AUTOCERT="false" \
> -v /tmp/trasa/accessproxy/guac:/tmp/trasa/accessproxy/guac \
> seknox/trasa:v1.1.4
fbf4fa6ef9fe61673bde7f4cf22ac53db48c0cf7dbacd7d04962285d4d49871f
```

Figure 15 Installation de Trasa

3. Configuration de la solution :

3.1. Configuration de compte admin :

Après avoir installé le serveur Trasa, on peut y accéder via le lien qu'on a fourni. Une connexion au tableau de bord est requise en insérant nom d'utilisateur et mot de passe.

La figure 16 illustre la connexion au tableau de bord.

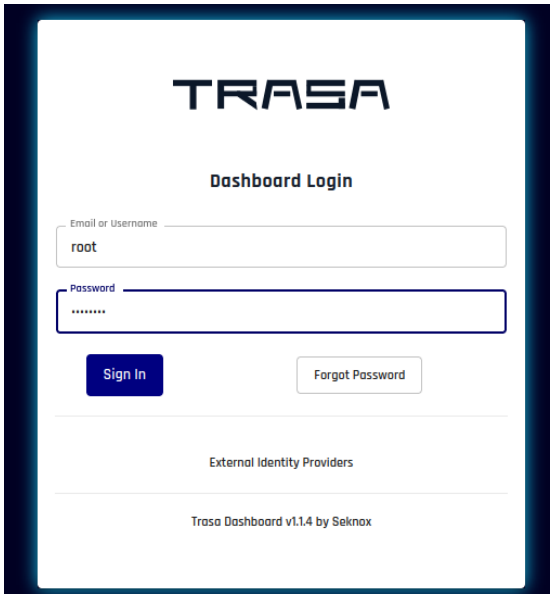

Figure 16 Connexion au tableau de bord

Après s'être connecté, une page de changement de mot de passe s'affiche, dans laquelle nous saisissons un mot de passe fort, un mélange d'alphabets majuscules et minuscules, de caractères spéciaux et de chiffres.

La figure 17 illustre un formulaire pour mettre un mot de passe fort.

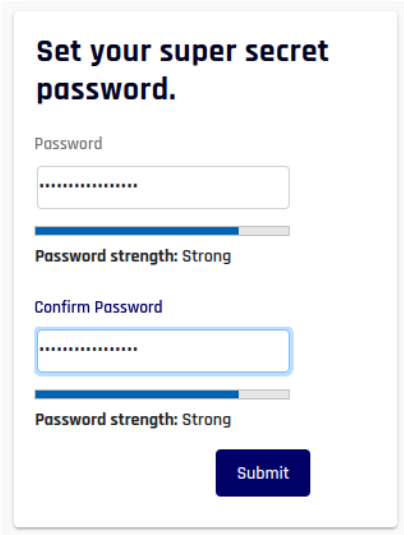

Figure 17 Mettre un mot de passe fort

Par la suite, un premier appareil est inscrit en scannant le code QR lors de la connexion de l'appareil mobile avec Google Authenticator et en saisissant le code TOTP.

La figure 18 présente le code QR à scanner et la saisie du code TOTP pour inscrire un appareil mobile.

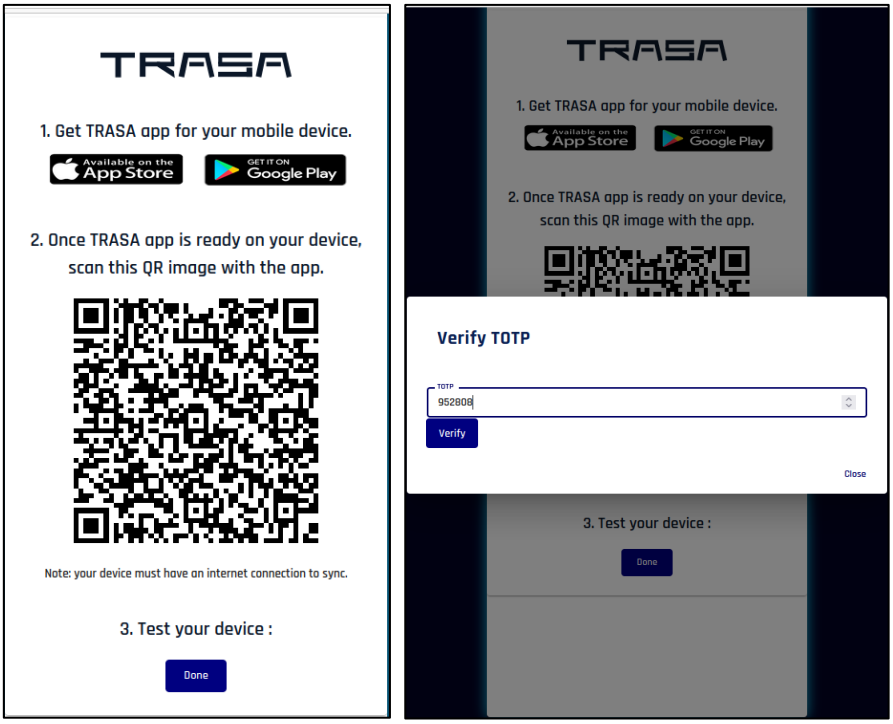

Figure 18 Inscrire un appareil mobile

Enfin, la configuration du compte administrateur est terminée et la page de tableau de bord apparaît.

La figure 19 présente le tableau de bord de l'administrateur.

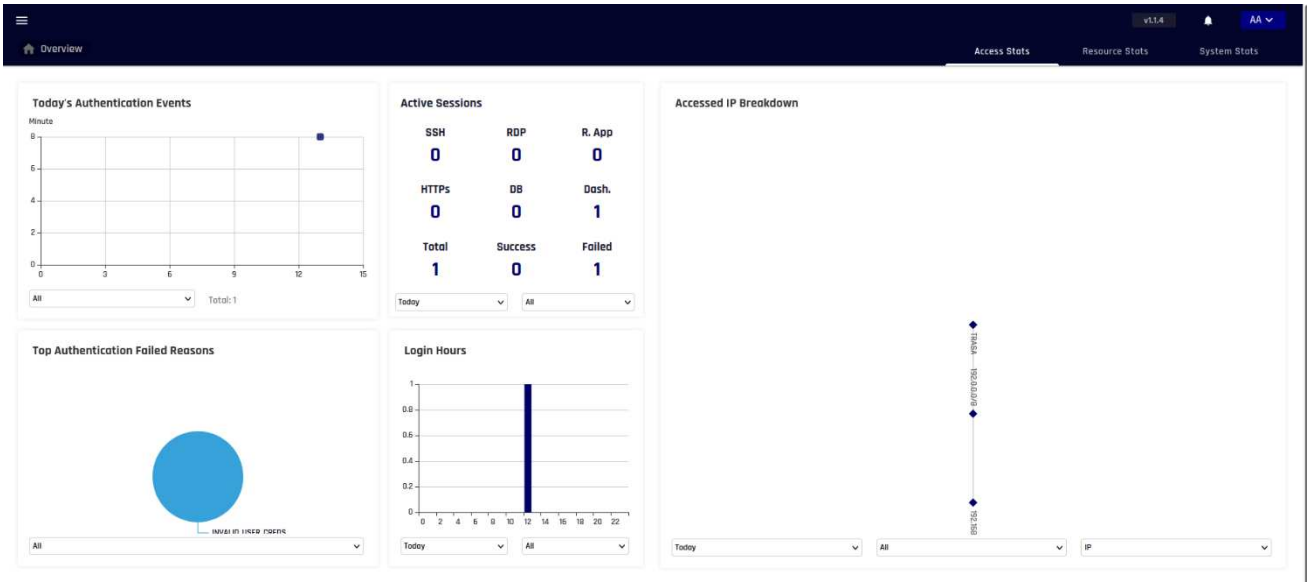

Figure 19 Tableau de bord de l'administrateur

3.2. Création d’un utilisateur :

Pour créer un utilisateur, l'administrateur se connecte à son compte, clique sur le bouton des tr Après avoir cliqué sur Create User et avoir rempli le formulaire avec les coordonnées de l'utilisateur et choisi son type ; administrateur ou simple utilisateur simple, l’administrateur clique sur Submit. Enfin, un lien s'affiche pour poursuivre la configuration du compte.

La figure 20 présente comment créer un utilisateur.

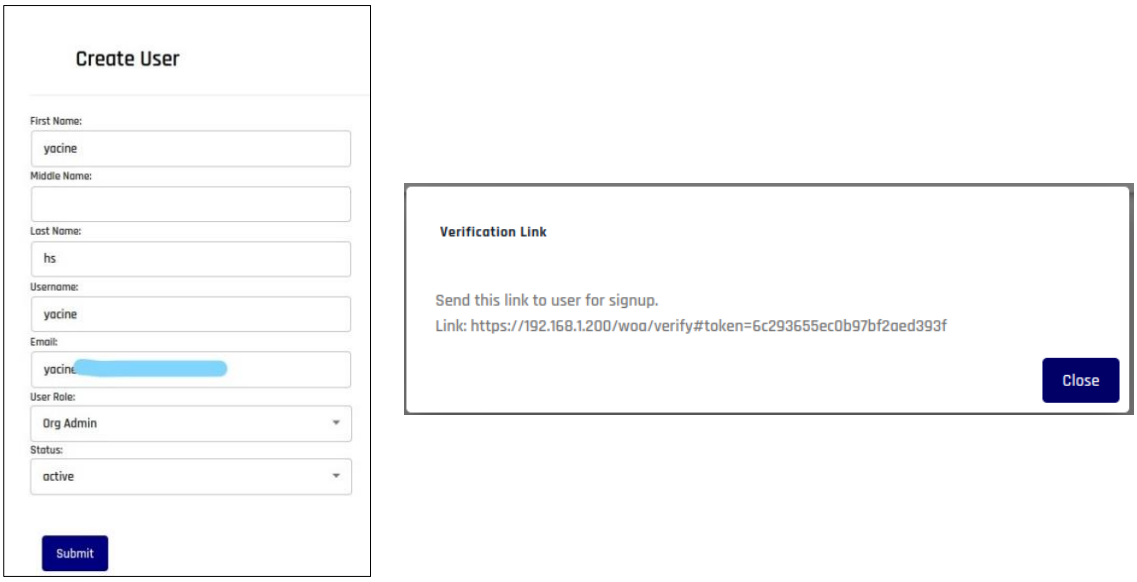

Figure 20 Créer un utilisateur

3.3. Création d’une politique :

L’administrateur clique sur le bouton des trois barres et ensuite sur *Control*, puis sur *Create New Policy*. La création d'une politique se compose de trois parties : donner un nom à la politique, ajouter des autorisations et réviser et créer la politique.

La phase d'ajout d'autorisations consiste à :

- Politique de base : Prise en charge de la politique basée sur l'heure et l'emplacement ainsi que du contrôle de l'authentification à deux facteurs, de l'option d'enregistrement des sessions et de l'autorisation des transferts de fichiers.
- Hygiène des appareils : Contrôle de l'accès en fonction de l'hygiène de sécurité des appareils de l'utilisateur.

La figure 21 illustre comment créer une politique.

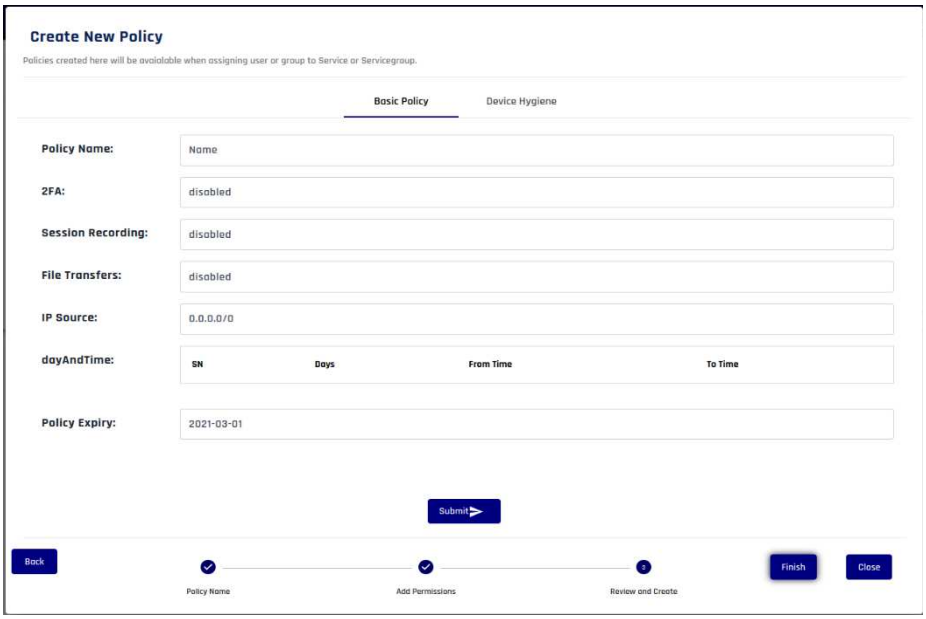

Figure 21 Créer une politique

3.4. Création d'un service :

L'administrateur clique sur le bouton des trois barres et ensuite sur *Services*, puis sur *Create New Service* remplit les détails et sélectionne le type de service.

La figure 22 présente comment créer un service.

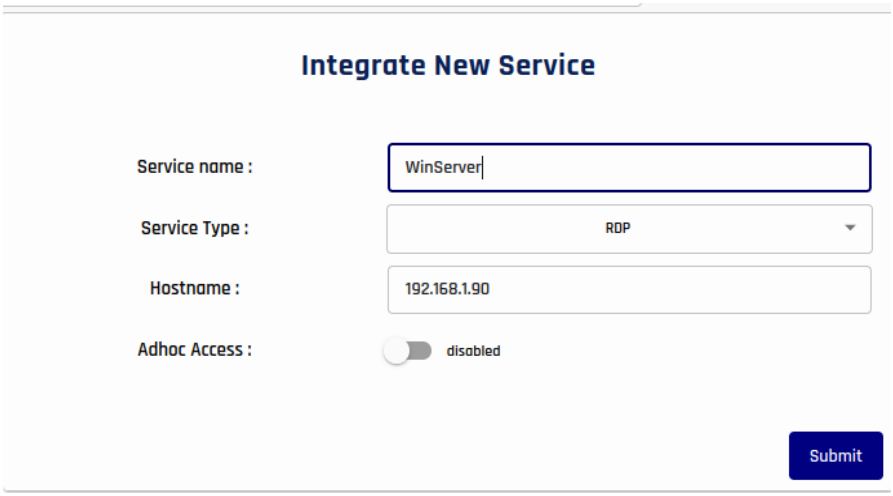

Figure 22 Créer un service

La page sera redirigée vers la page du service nouvellement créé, puis clique sur *Access Map,* ensuite sur *Assign User*. Il faut maintenant assigner les utilisateurs qui ont accès à ce service, sélectionner une politique pour ces utilisateurs et taper le nom d'utilisateur RDP.

La figure 23 présente comment assigner un utilisateur à un service.

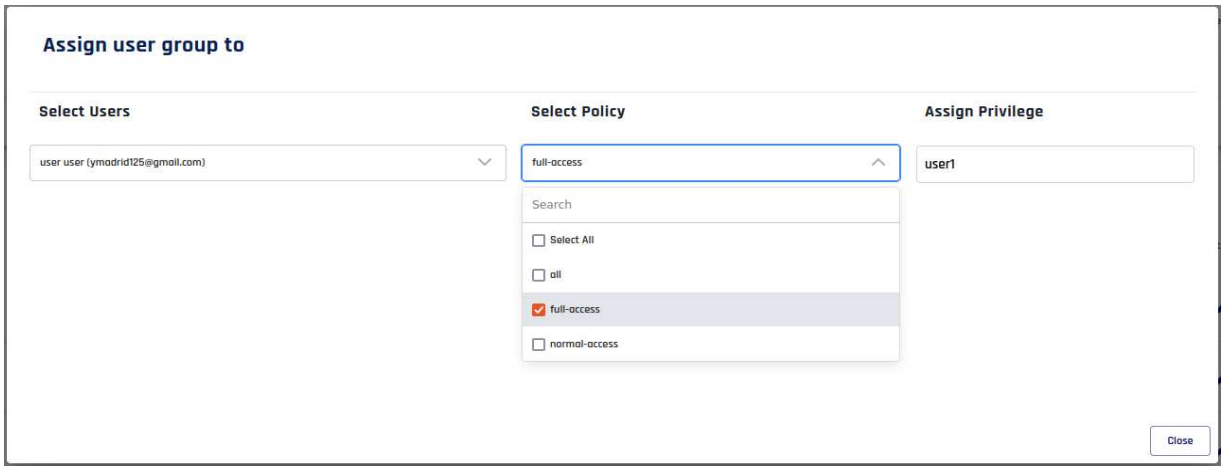

Figure 23 Assigner un utilisateur

Après avoir assigné les utilisateurs, il faut ajouter les identifiants de connexion RDP en cliquant sur *Manage Credentials* dans la barre des tâches, puis ajouter le nom d'utilisateur et le mot de passe et cliquer sur "+" pour les stocker dans le coffre-fort.

La figure 24 présente comment stocker les identifiants de connexion dans le coffre-fort.

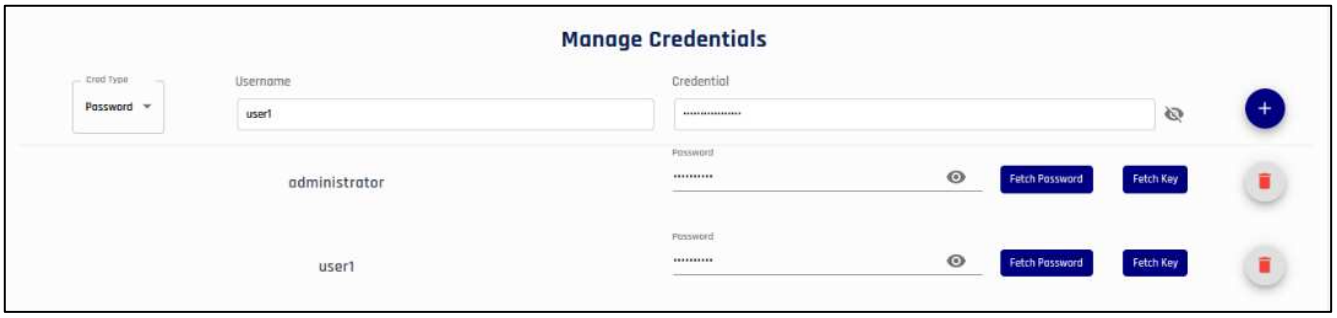

Figure 24 Stocker les identifiants de connexion dans le coffre-fort

4. Test et Evaluation :

4.1. Accéder au service RDP :

Pour accéder au service RDP, l'utilisateur doit se connecter à son compte. La première page qui apparaît est *My Route*, où il trouve tous les services attribués, sélectionne le service RDP auquel il veut accéder et clique sur *Connect*, puis sur le nom d'utilisateur qui apparaît.

La figure 25 présente comment accéder à un service.

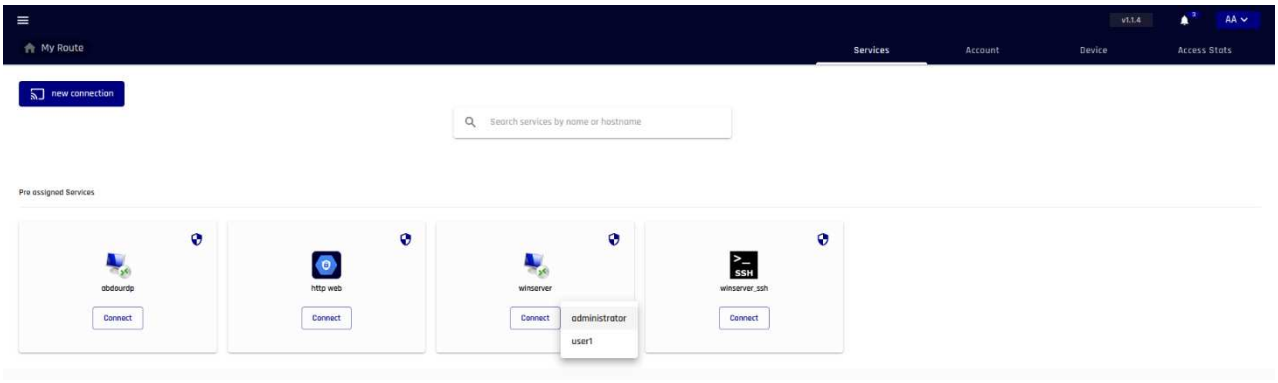

Figure 25 Accéder à un service

Ensuite, un nouvel onglet s'ouvre, demandant à l'utilisateur de choisir le type d'authentification à deux facteurs. L'utilisateur doit sélectionner une méthode et procéder à la vérification de son identité.

Une fois la vérification effectuée, l'utilisateur se voit accorder l'accès à son service.

La figure 26 présente l'accès à RDP.

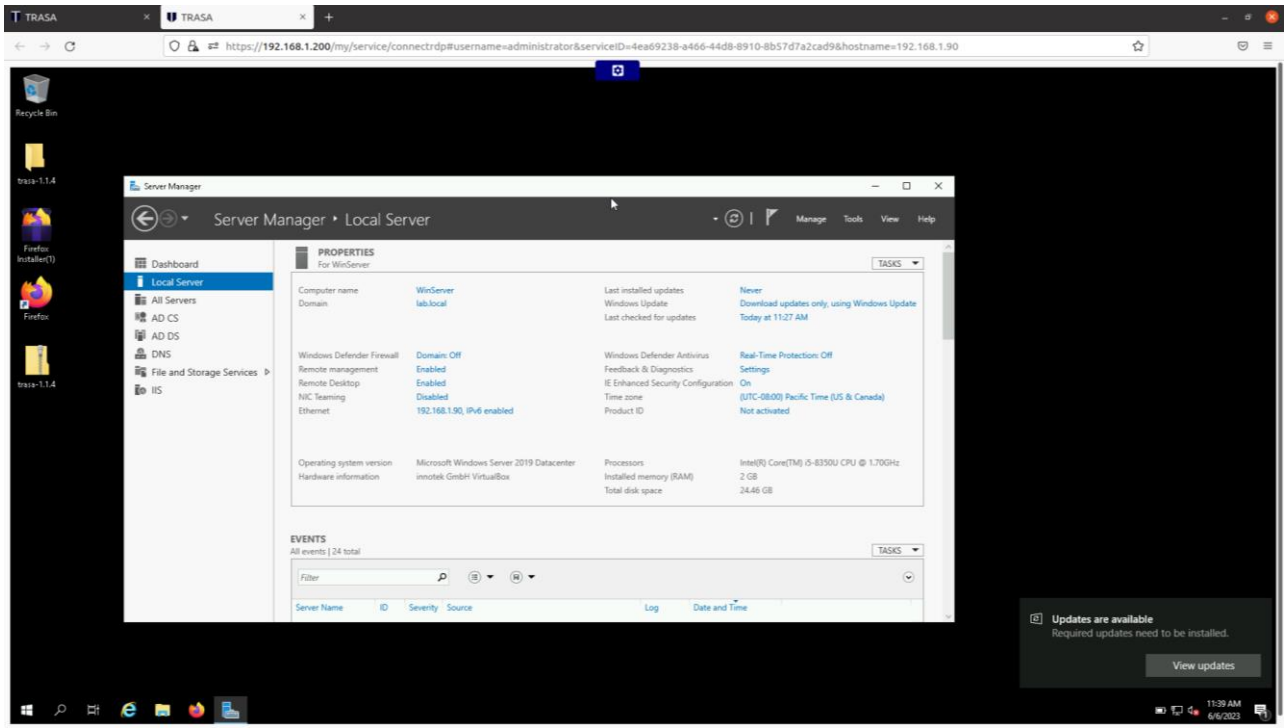

Figure 26 Accès à RDP

4.1. Accéder au service SSH :

De la même manière que dans la figure 25, mais en cliquant sur *Connect* dans le SSH service, puis en vérifiant l'identité et enfin en accédant au service SSH.

La figure 27 présente l'accès à SSH.

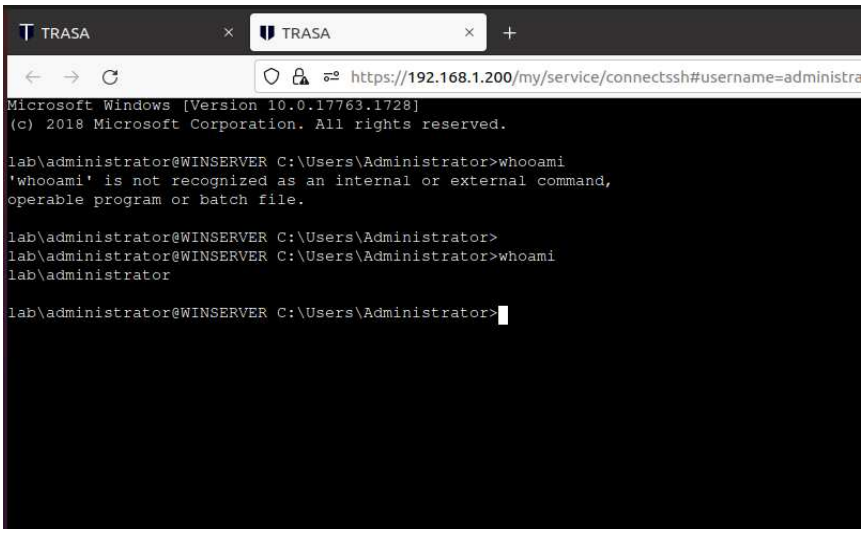

Figure 27 Accès à SSH

4.2. Accéder au service non autorisé :

Après avoir créé les services RDP et ajouté les utilisateurs, nous créons une politique appelée Normal-Access. Elle restreint l'accès pendant les week-ends.

La figure 28 présente la nouvelle politique créée.

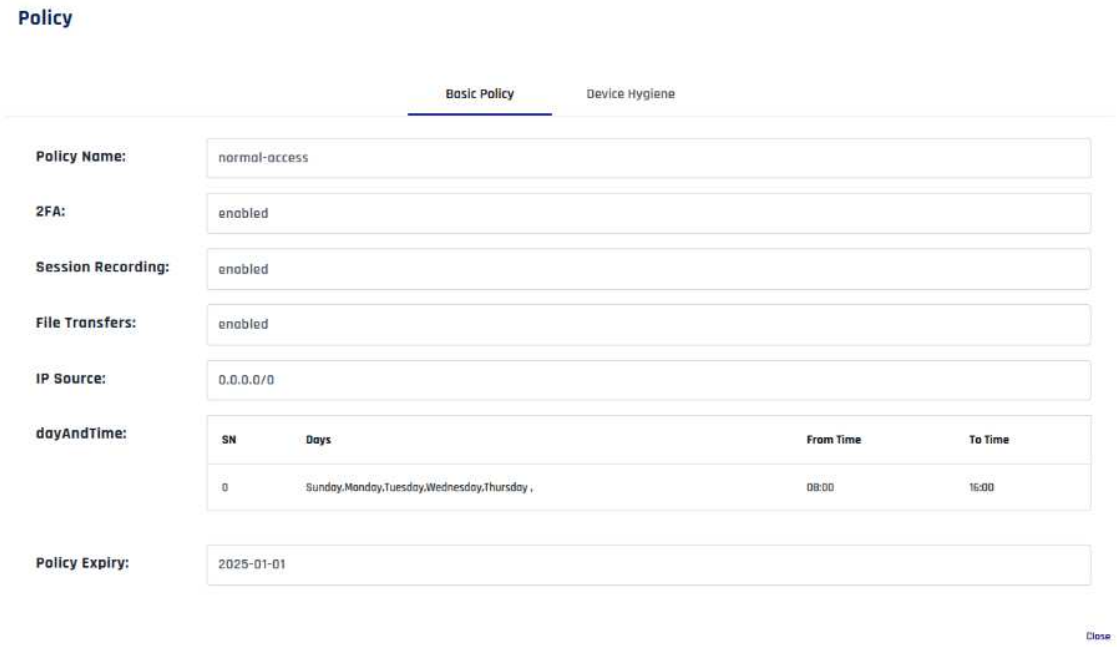

Figure 28 Politique accès normal

Cette stratégie doit être attribuée à un utilisateur non privilégié du service RDP de Windows Server.

La figure 29 montre les utilisateurs affectés au service RDP et leurs politiques.

Figure 29 Utilisateurs et politiques assignés

L'utilisateur se connecte à son compte, puis accède à la page de ses services.

Il constate que l'icône de son service est en rouge, ce qui signifie qu'il n'a pas accès à ce service pour l'instant.

La figure 30 illustre un accès non autorisé d'un service d'un utilisateur non privilégié.

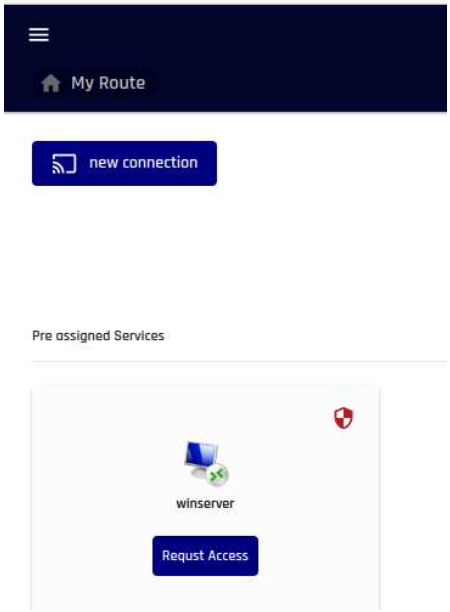

Figure 30 Accès non autorisé

Enfin, il doit cliquer sur *Request Access* pour demander l'accès à un administrateur.

La figure 31 présente la demande d'un accès.

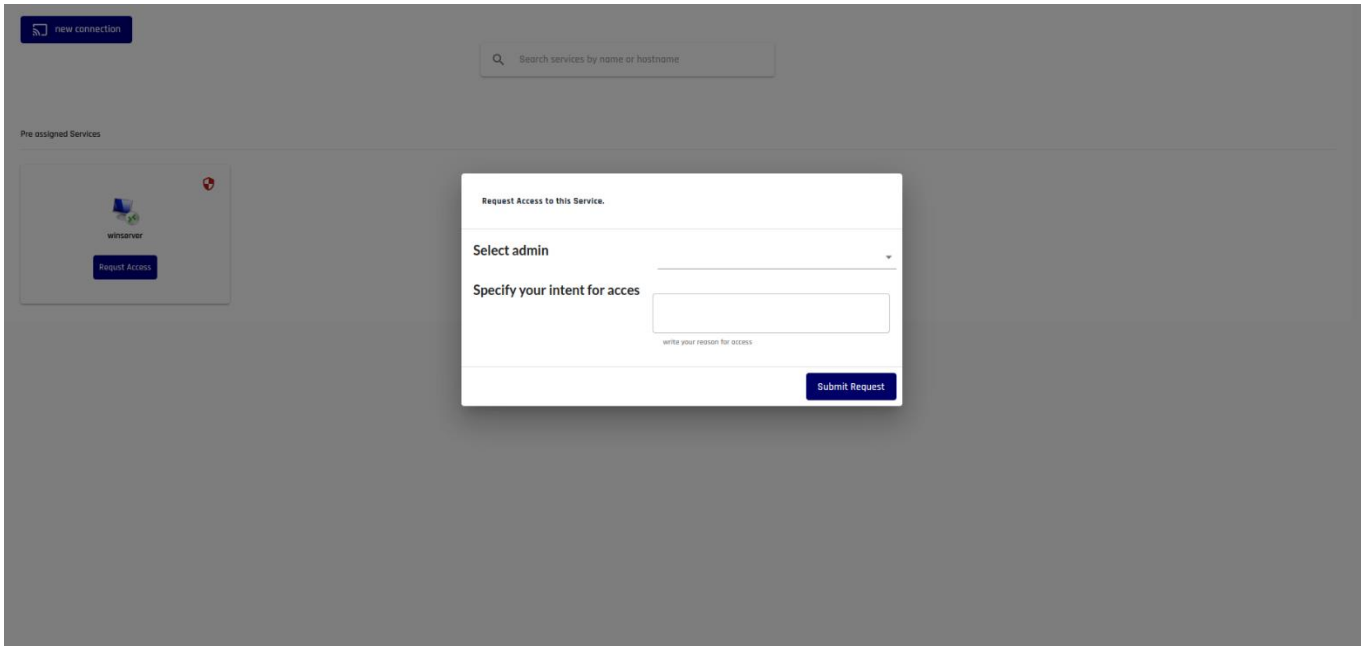

Figure 31 Demande d'accès

4.3. Transfert de fichiers :

Pour transférer des fichiers de la machine de l'utilisateur vers un service RDP, il doit être dans une session en direct, puis clique sur le bouton bleu en haut.

Sélectionne ensuite le fichier qu'il souhaite transférer et cliquez sur *Upload*.

La figure 32 présente comment transférer un fichier vers un service RDP.

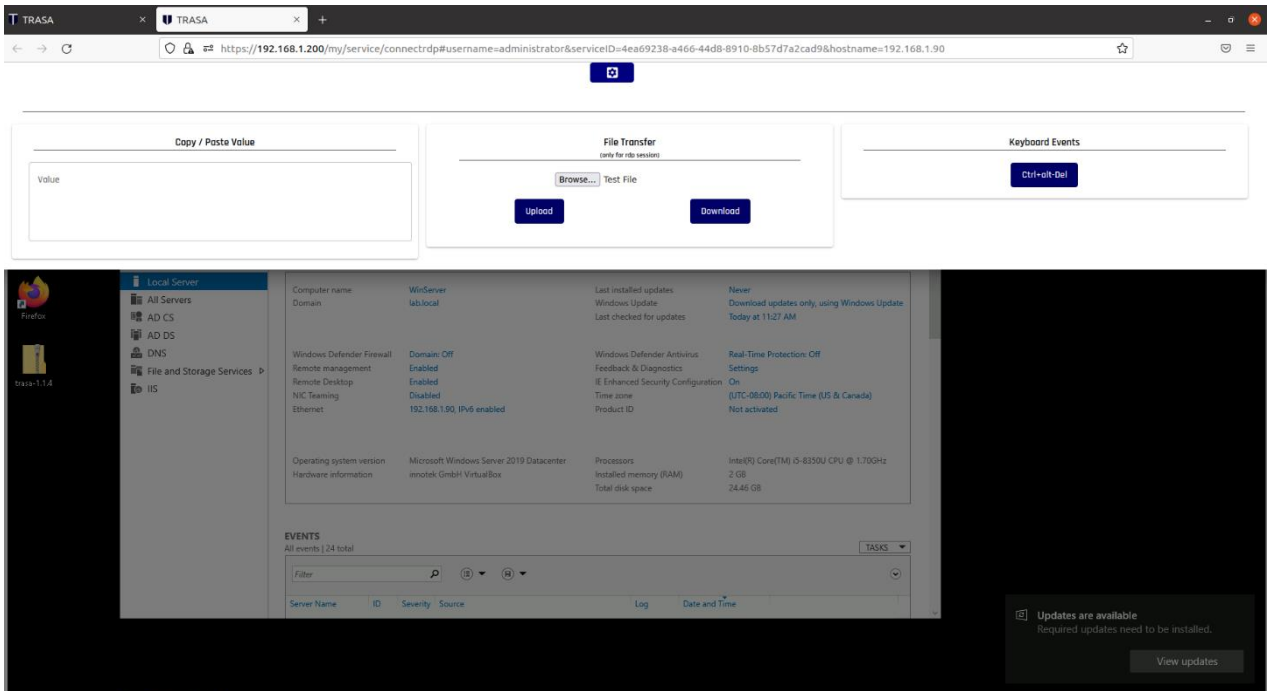

Figure 32 Transférer un fichier vers un service RDP

Il consulte son fichier transféré sur le service RDP.

La figure 33 présente le fichier transféré au service RDP.

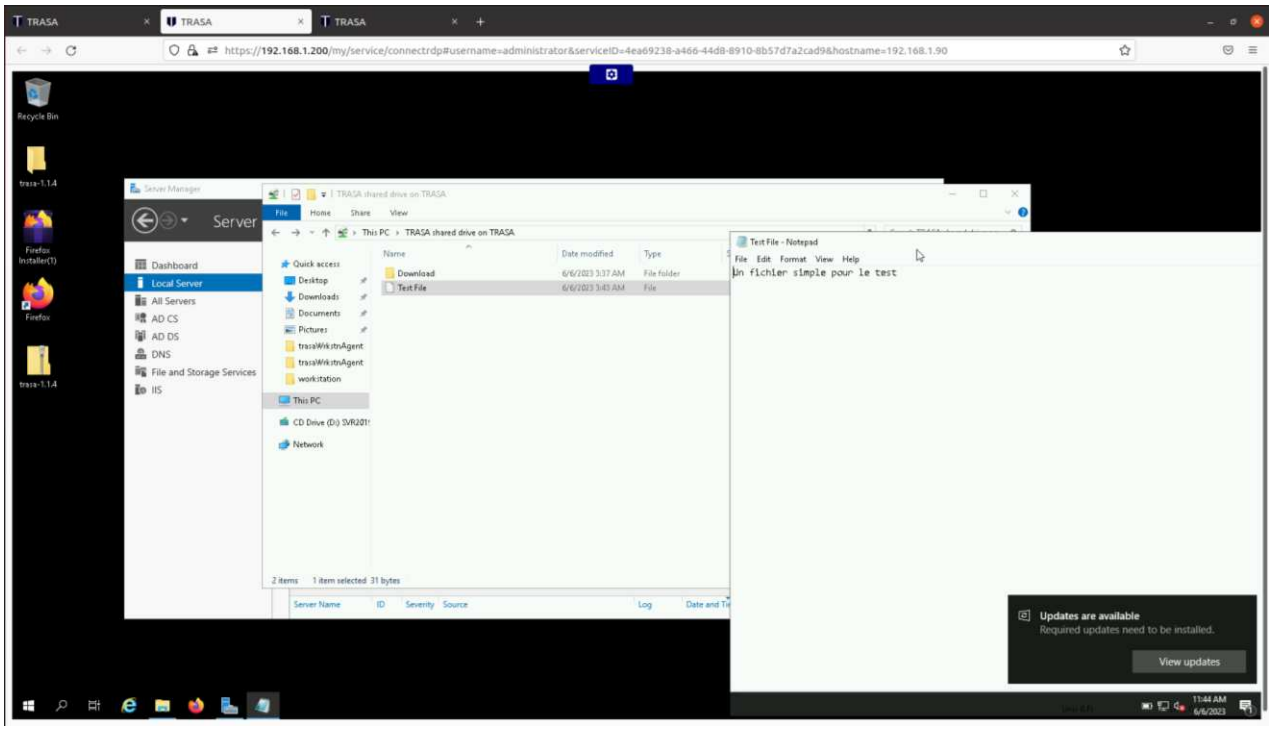

Figure 33 Fichier transféré au service RDP

Pour transférer un fichier qui est dans la machine de service RDP vers la machine de l'utilisateur, il doit copier le fichier qu'il souhaite à transférer et le coller dans le dossier partagé nommé *"Trasa shared drive on Trasa"*.

Ensuite, clique sur le bouton bleu en haut et clique sur *Download*.

La figure 34 présente comment transférer un fichier vers la machine hôte de l'utilisateur.

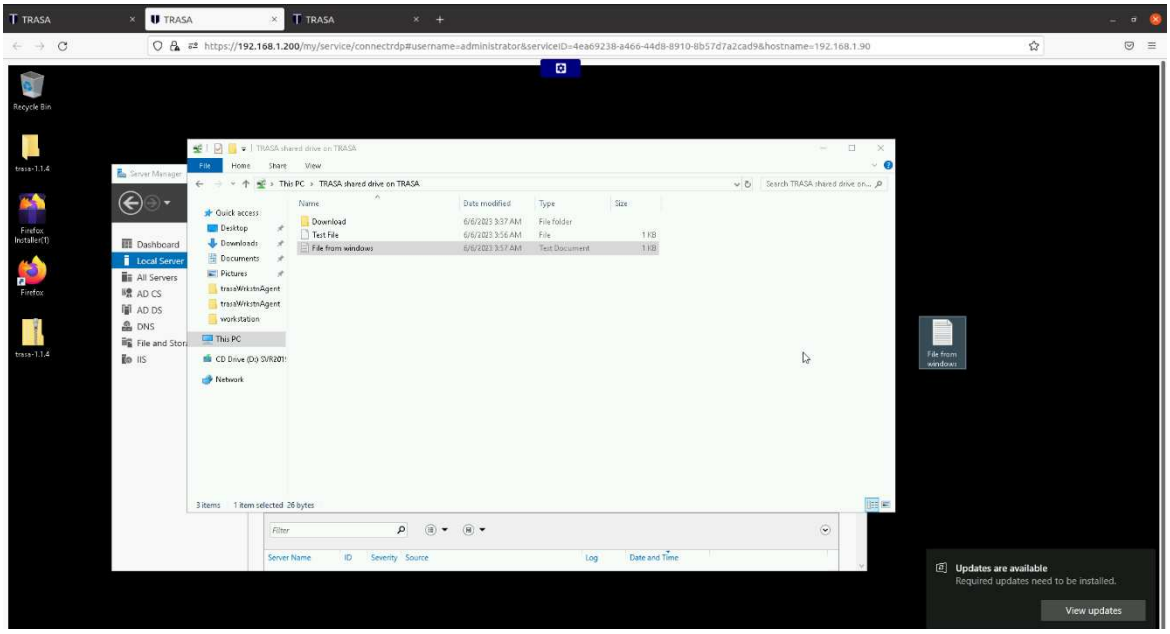

Figure 34 Transférer un fichier vers la machine hôte de l'utilisateur

Enfin, il trouve ce fichier transféré dans l'explorateur de fichiers sur Trasa, qui contient tous les fichiers transférés.

La figure 35 montre l'explorateur de fichiers.

Figure 35 Explorateur de fichiers

5. Conclusion :

Dans ce chapitre, nous avons présenté l'environnement de travail, la mise en œuvre et la configuration de la solution que nous avons choisie, puis nous avons testé quelques fonctionnalités.

Conclusion Générale

En règle générale, les utilisateurs les plus expérimentés du service informatique sont responsables du déploiement et de la gestion des fonctionnalités dont dépend l'entreprise.

Mais avec ce pouvoir vient le risque, La complexité de l'informatique est telle que les modifications apportées, même par le personnel le plus expérimenté, peuvent avoir des impacts inattendus et graves sur la disponibilité, les performances et/ou l'intégrité des ressources.

L'accès au niveau administrateur peut être exploité par des acteurs malveillants à l'intérieur ou à l'extérieur d'une entreprise pour causer de graves dommages à cette dernière.

Ce présent rapport a été réalisé dans le but d'étudier et mettre en place d'une solution **PAM** pour remédier à ce type de menaces, notre solution proposée répond totalement aux exigences demandées par l'organisme d'accueil en terme de centralisation des gestions de ces accès locaux et à distance. Elle répond également aux points suivants :

- Accès client natif sécurisé
- Contrôle d'accès
- Un coffre-fort des mots de passe
- L'Authentification Multi-facteur (MFA)
- Surveillance

A travers ce mémoire, nous avons présenté les principales lignes sur les accès privilégiés, une étude comparative de différentes solutions PAM et avant de ce fait le choix qui répond le mieux aux exigences de l'organisme d'accueil.

En termes de sécurité notre solution est basée sur plusieurs mécanismes tels que :

- Le cryptage des mots de passe.
- Cryptage des sessions entre les utilisateurs.
- Aussi utilisant les protocoles SSH, HTTPS.

Bibliographie

[1] Al Kukhun, D., Codreanu, D., Manzat, A.-M., & Sèdes, F. (2013). Une vision pervasive d'un système multimédia distribué : extention en vue d'un contrôle d'accès adaptatif. *OATAO*.

[2] Ali, G., Dida, M. A., & Sam, A. (2020). Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*, *12*(10), 160. https://doi.org/10.3390/fi12100160

[3] Apache GuacamoleTM. (n.d.). https://guacamole.apache.org

[4] Australian Cyber Security Centre [ACSC]. (n.d.-a). Implementing Multi-Factor Authentication. *cyber.gov.au*.

[5] Australian Cyber Security Centre [ACSC]. (n.d.-b). Strategies to Mitigate Cyber Security Incidents – Mitigation Details. In *cyber.gov.au*.

[6] Blasko, G., Narayanaswami, C., & Raghunath, M. (2005). *A Wristwatch-Computer Based Password-Vault*.

[7] Carson, J. (2017). Privileged Account Management For Dummies. *Thycotic*.

[8] Cheng, H., Li, W., Wang, P., Chu, C., & Liang, K. (2021). Incrementally updateable honey password vaults. In *USENIX Security Symposium* (pp. 857–874).

[9] Cobia, A. (2019). *Privileged Access Management*. La Salle University.

[10] Computers at risk: safe computing in the information age. (1991). *Choice Reviews Online*.

[11] Crook, R., Ince, D. C., & Nuseibeh, B. (2003). Modelling access policies using roles in requirements engineering. *Computer Science Web*, 979–991.

[12] De Cristofaro, E., Du, H., Freudiger, J., & Norcie, G. (2014). *A Comparative Usability Study of Two-Factor Authentication*.

[13] Desmond, B., Richards, J., Allen, R., & Lowe-Norris, A. (2013). *Active Directory: Designing, Deploying, and Running Active Directory*. O'Reilly Media, Incorporated.

[14] Fernandes, T. (2001). *Les politiques de sécurité* [Rapport de recherche DIUL-RR-0103]. Université Laval.

[15] Hu, V. C., Ferraiolo, D. F., & Kuhn, D. (2006). *Assessment of access control systems*. https://doi.org/10.6028/nist.ir.7316

[16] JumpServer. (n.d.). JumpServer. https://www.jumpserver.org

[17] Kuokkanen, A. (2020). *Newcomer's introduction to Privileged Access Management* [Bachelor's thesis]. JAMK.

[18] MAUDOUX, C. (2018). *Implémentation de l'authentification à double facteur dans la solution de SSO AAA LemonLDAP::NG 2.0* [INGÉNIEUR CNAM].

[19] PostgreSQL. (n.d.). PostgreSQL. https://www.postgresql.org

[20] Privileged access management 101: A comprehensive guide to building a sound PAM strategy for your enterprise. (n.d.). *ManageEngine*.

[21] Purba, A., & Soetomo, M. A. (2019). Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control. *Annual Conference on Management and Information Technology*.

[22] Redis. (n.d.). Redis. https://redis.io

[23] Sandhu, R. S., & Samarati, P. (1994). Access control: Principles and Practice. *IEEE*.

[24] StrongDM | Dynamic Access That Puts Your People First. (n.d.). strongDM. https://www.strongdm.com

[25] Teleport. (n.d.). Teleport: Identity-Native Infrastructure Access. Faster. More Secure. Teleport. https://goteleport.com

[26] TRASA: zero trust service access. | TRASA: zero trust service access. (n.d.). https://www.trasa.io/

[27] Uymatiao, M. L. T., & Zhang, Y. (2014). *Time-based OTP authentication via secure tunnel (TOAST): A mobile TOTP scheme using TLS seed exchange and encrypted offline keystore*. https://doi.org/10.1109/icist.2014.6920371

[28] Vishwakarma, S., Khera, H., & Manchanda, K. (2021). Password Vault. *EasyChair Preprint*.